ISSN 1343-2915

学術情報処理研究

No.16　　2012

JACN

学術情報処理研究編集委員会

学術情報処理研究

Journal for Academic Computing and Networking

No.16　2012

学術情報処理研究編集委員会

No.16 2012 年

学術情報処理研究

巻頭言 廿日出勇 1

論文

山口大学自己点検評価システム（YUSE）の開発と運用:第１期中期目標期間及び第２期中期目標期間前半のまとめ
市川哲彦，小柏香穂理，鈴木素之，松元隆博，内藤博夫 3

全学ポータルを用いた学生・教職員間多機能連絡システムの開発
二木恵，東昭孝，笠原禎也，高田良宏，松平拓也 15

分散キャンパスを利用したファイルバックアップシステム
野口宏，大瀧保広，鎌田賢 25

ADFS による学術認証フェデレーション対応 SharePoint サービスの構築
伊藤智博，立花和宏，奥山澄雄，高野勝美，田島靖久，吉田浩司 33

学認との融合化を視野に入れた金沢大学統合認証基盤の構築と運用
松平拓也，笠原禎也，高田良宏，東昭孝，二木恵 41

学認と学内統一認証の自動切替
松澤英之，園田誠，黒木亘，廿日出勇 51

学内の様々な運用形態に対応したコンパクトなアカウント管理システムの実現
瀬川大勝，辻澤隆彦，石橋みゆき 59

SaaS 環境によるプログラミング初学者教育の試み
田中克明，鈴木令子，山崎秀記 71

大規模 PC 実習室システムの更新及びその利用状況
右田雅裕，杉谷賢一，久保田真一郎，武藏泰雄，永井孝幸，
戸田真志，喜多敏博，松葉龍一，辻一隆，島本勝，木田健，
宇佐川毅，中野裕司 80

ISMS 導入のための情報セキュリティインシデントコスト定量化について
永井好和，市川哲彦，長谷川孝博，小河原加久治，多田村克己 86

標的型攻撃メールの予防対策
伊藤史人，高見澤秀幸，佐藤郁哉 100

大学 1 年生の情報活用能力と ICT 機器やメディアの利用状況調査
辰己丈夫，江木啓訓，瀬川大勝 111

IC カード全学導入に向けた認証基盤システム整備と評価
清水さや子，戸田勝善，吉田次郎 122

学術情報光コアネットワークにおける波長群スイッチングと
リンク通過パス数均一化の効果
高野勝美，軽部良，齋藤慶太，武田利浩，伊藤智博 131

複数認証基盤に対応する複合 SSO 環境でのユーザエクスペリエンス
松浦健二，上田哲史，佐野雅彦 138

第 16 回学術情報処理研究集会

横浜国立大学におけるウェブホスティングサービス
志村俊也，吉岡克成，徐浩源，牧田大佑，星澤裕二，松本勉 147

iSCSI 型ネットブートシステム起動性能評価システム
本田修啓 152

大震災の経験から考案した BCP 非常用サーバ
鵜川義弘，福井恵子，平井清巳，安藤明伸，小野元久，本田茂広 158

無線 LAN 接続状況の可視化と無線 LAN アクセスポイントの動作解析
内藤郁之，望月源，佐野洋 163

CMS 小テスト問題分析による授業改善の試み
和田武 167

大学導入教育としての情報教育の実践
佐々木正人，石黒克也，斎藤卓也，豊永昌彦 174

大分大学医学部キャンパスのネットワーク運用ポリシーとシステム構成について
島岡章，板倉紀子 178

ユーザと機器のオンライン申請、登録、認証システムの開発とその運用について
-- センター管理業務の削減の観点から --
板倉紀子，島岡章，小谷明義，吉田和幸 183

会議時貸し出し用 iPad における Apple Configurator を用いたセキュリティ対策
川戸聡也，本村真一 188

SINET4 への移行に伴う対外接続回線の冗長化構成の構築と評価
柳沼匠，清水さや子，吉岡諭，吉田次郎 192

ISMS 研究会

ISO 審査機関からみた国立大学法人の ISMS
山本富夫 197

大学情報系センターにおける SLA の構築
長谷川孝博 202

ISMS 認証取得後の活動について
佐野雅彦，上田哲史 205

センター紹介

福岡教育大学「学術情報センター」の発足
大坪靖直，清水紀宏 207

長崎大学情報メディア基盤センター紹介
情報教育及び e ラーニング開発支援体制を拡充
野崎剛一，藤井美知子，丹羽量久，上繁義史，古賀掲維，柳生大輔 209

報告

第 6 回国立大学法人情報系センター長会議議事要旨
宮崎大学情報基盤センター 211

第 6 回国立大学法人情報系センター研究交流・連絡会議　報告 松岡守 223

第 15 回学術情報処理研究集会　報告 松岡守 225

学術情報処理研究投稿規定 227

編集後記 松岡守 228

巻頭言

交流から連携へ

宮崎大学情報基盤センター長
廿日出　勇

大学の情報基盤をいかにすべきか、自由にいろいろなアイディアを出して議論するのは楽しいものです。しかし、実際にシステムを導入する際には、予算、利用可能な技術や製品、運用管理に必要な技術や労力など様々な制約があり、制約下で大学にとって最良と思えるシステムを構築しなければなりません。また、多くの大学では、主要なシステムを４～５年のリースで導入しているので、リース中に陳腐にならない先進性も求められます。進歩の速いＩＣＴ分野で４～５年先を見通すことになるのですから、情報系センターの関係者は、リースの更新のたびに苦労されていることと思います。

「大学の情報基盤をいかにすべきか」、この問題を難しくしている原因の一つは、コンピューティング環境が大きく変化する時期にきているからです。利用者をスムーズに新しいコンピューティング環境に移行させていくことは、大変なことですが、センターの重要な使命です。現在進行しているクラウドコンピューティングへの流れは、かつてのコンピュータのダウンサイジングやインターネットへの接続に匹敵する大きな変化であり、どのような形態のクラウドにするのか、どのサービスを外部に出すのか、難しい判断をしなければなりません。

もう一つの原因は、情報系センターを取り巻く環境の変化です。法人化以降、センターの関わる業務は広がり、図書館や事務の情報部門との連携も進んでいます。センターの業務が増える一方で、経営効率化のために業務・システム最適化が推進され、予算や人員の削減が進められています。さらに、東日本大震災を契機に、大学の情報システムの BCP 対策が真剣に検討され始めました。予算などの制約が厳しくなるなか、情報基盤に求められる要求は高くなってきています。

このような厳しい状況では、知恵を出し合うだけでなく、複数のセンターが連携して共通の問題の解決にあたることが必要ではないでしょうか。例えば、大規模災害に対応するには、遠隔地にバックアップシステムが必要ですが、同じ立場の大学ということで、重要データの相互バックアップやシステムの運用代行を行いやすいのではないでしょうか。BCP 対策をきっかけに、センター間の技術と人の交流が進み、大学間クラウドやシステムの共同開発など、連携の輪が広がっていくことを期待します。

学術情報処理研究集会は、国立大学法人情報系センター関係者の研究発表と情報交換の場です。本誌「学術情報処理研究」に掲載された情報基盤の構築と運用に関する先進的な取り組みが他センターの参考になり、集会での交流が新しい連携につながれば幸いです。

論文

山口大学自己点検評価システム (YUSE) の開発と運用: 第 1 期中期目標期間及び第 2 期中期目標期間前半のまとめ

An Overview of YUSE, Yamaguchi University Self-Evaluation System, in Relation to University Self-Evaluation Activities in the First Mid-Term Goals Period and the First Half of the Second Period

市川哲彦 [1], 小柏 香穂理 [1], 鈴木 素之 [2], 松元 隆博 [3], 内藤 博夫 [2,3]

Yoshihiko Ichikawa[1], Kahori Ogashiwa[1], Motoyuki Suzuki[2], Takahiro Matsumoto[3], Hiroo Naitoh[2,3]

山口大学メディア基盤センター [1]
山口大学大学院理工学研究科 [2]
山口大学大学評価室 [3]
Media and Information Technology Center, Yamaguchi University[1]
Graduate School of Science and Engineering, Yamaguchi University[2]
University Evaluation Department, Yamaguchi University[3]

概要

現在，大学評価は学校教育法及び国立大学法人法により義務づけられており，大学運営では評価活動のための PDCA サイクルが必須となっている．このサイクルは様々な観点に対して挙証データに基づく評価を行うため，基礎データの収集・分析が必須であり，情報システムによる効率的なサポートが必要不可欠である．そのため本学では，山口大学自己点検評価システム (YUSE) が導入されており，10 年以上にわたり利用目的に合わせた改修を行いながら運用が行われてきた．本システム自体は，平成 16 年の国立大学法人化以前に，平成 11 年の大学設置基準の変更に伴う自己点検評価の義務化を背景として平成 14 年に導入されたものであり，現時点では，第 2 期中期計画 (平成 22 年〜平成 27 年) の前半の開発計画までほぼ終了した段階である．折しも，文部科学省から大学改革実行プランが平成 24 年 6 月に公表され，評価制度の抜本的な見直し及び大学情報の公開の徹底が求められ，今後はより総合的・戦略的な institutional research (IR) に対しての情報システムによるサポートを検討すべき時期に来ていると言える．本稿では，こうした今後の活動の基礎資料として，あるいは，他大学における大学評価支援システムとの比較材料として利用されることを期待して，基礎データの収集に加えて評価活動支援機能の開発が活発となった法人化後の動きを中心に，YUSE のこれまでの開発・運用の経緯をまとめて問題点の指摘を行う．さらに，同様な PDCA が要求される情報セキュリティマネジメントシステム (ISMS) の構築経験とこれまでの YUSE の開発経緯とを比較して，PDCA サイクルの “見える化” や所謂 “評価疲れ” 等の課題について考察を行う．

キーワード

大学自己点検評価, institutional research

1 はじめに

注意

脚注ではなく尾注を利用しているので，注釈については参考文献後の「注釈」セクションを参照されたい．

平成 3 年及び平成 11 年の設置基準の改正による自己点検評価の義務化，さらに，平成 16 年の大学の法人化後の学校教育法及び国立大学法人法による法制化を受け，大学評価の PDCA サイクルは大学活動の必須事項となっており，さまざまな情報システムを活用した基礎データの収集と分析はもはや大学運営では避けて通る事はできない．筆者らの所属する山口大学では，平成 14 年 7 月に，山口大学自己点検評価システム (YUSE) の運用が開始され，以降現在にいたるまで，適宜改修を行いながら，教員の全般的自己点検評価，研究水準評価，教育貢献度評価，組織別自己点検評価などの自己点検評価活動や人事評価の試行へのシステム連携による支援などにおいて利用されている．

現在は，第 2 期中期目標期間 (平成 22 年〜平成 27 年) の前半の開発計画までほぼ終了した段階であり，中期目標 [1][1] を達成すべく活動を継続している．元々は教員の基礎情報を収集するシステムとしてスタートしているが，現在では，評価内容をまとめた山口大学活動白書作成の検討，電子シラバスや授業評価システムとの連携，教員情報の公開システム (人・知・技 [2], 研究者総覧 [3]) との連携，データ入力のポータルサイトの充実などが実施あるいは検討されており，より institutional research (以下, IR) [4, 5] 色の強いものになっている．

折しも，文部科学省から大学改革実行プラン [6] が平成 24 年 6 月に公表され，評価制度の抜本的な見直し及び大学情報の公開の徹底が求められ，今後はこうした動きを活発化させることが期待されている．そこで，本稿では YUSE のこれまでの開発・運用の経緯を，基礎データの収集に加えて評価活動支援機能の開発が活発となった平成 16 年の法人化後の動きを中心に説明する．今後の活動を計画する際の基礎資料として，大学間の評価支援システムの比較検討材料として利用されることを期待している．

本節では，まず YUSE が運用されてきた背景を法制度などの面からまとめ，次いで YUSE の利用の概略について述べる．

1.1 背景

大学の自己点検評価は平成 3 年の大学設置基準の改正 [7][2] において制度化されたのち，平成 10 年の大学審議会の答申 [8] [3]を受けて平成 11 年の大学設置基準の改正 [9] [4] において外部評価の努力目標化と共に義務化が明記された．また，平成 12 年 4 月に発足した大学評価・学位授与機構によって，第三者認証機関による評価を念頭においた試行的大学評価 [10, 11] が実施された．

その後，平成 16 年に国立大学が一斉に法人化され，同時に平成 16 年 4 月 1 日に施行された学校教育法改正 [12][5]により自己点検評価の実施及び結果の公開並びに第三者による認証評価 (機関別認証評価，専門分野別認証評価) が法制化され (認証評価の期間はそれぞれ 7 年毎以内と 5 年毎以内 [13][6])，また，国立大学法人法第 35 条 (において読み替えて準用する独立行政法人通則法) により大学法人評価委員会の評価を受けること (読替通則法第 32 条，第 34 条)[14] [7] が法制化された．こうした動きを受け，法人化後の本学においては，学則 (平成 16 年 4 月 1 日制定・施行)[15] にて，次のように自己点検評価の義務を改めて定めている:

> 第 4 条　本法人は，教育研究水準の向上を図るとともに，前条の理念及び目的を達成するため，教育研究活動等の状況について，自ら点検及び評価を行い，その結果を公表する。
> 2　前項の点検及び評価並びにその結果の公表に関し必要な事項は，別に定める。

法人化前後の自己点検評価に関する取組みについては報告 [16] に概略が述べられている．また，平成 18 年 4 月には評価室が発足し，それまでの評価委員会+評価委員会専門委員会の体制から移行している．

さらに，平成 22 年の学校教育法施行規則の改正 [17] において教育情報の公開の徹底がまた，平成 24 年の大学改革実行プラン [6] により評価制度の抜本的な見直し及び大学情報の公開の徹底がさらに求められるようになり，大学における評価活動及び教育情報の公開への要求はさらに高まっている．

1.2 YUSE の自己点検評価における利用の概略

本学の全学的自己点検評価は，当初は「山口大学の全学的自己点検評価実施要領」(平成 13 年 12 月) において定められ，法人化後は「国立大学法人山口大学全学的自己点検評価実施要領」(平成 18 年 3 月) において，また，平成 19 年 3 月からは更に細分化され「基本的考え方」,「基本方針」,「実施要領」,「実施要項」において定義されている．平成 18 年度に企画されていた評価は，

- 教員全般的活動評価 (平成 19 年度，平成 20 年度実施)
- 教育貢献度評価 (平成 20 年度実施)

- 研究水準評価 (平成 19 年度試行実施)

であり，それぞれについて YUSE データで蓄積された基礎データに基づく判定資料の生成と，部局長等による評価がなされた．また，人事評価をサポートするためのシステムも作成されている．

大学機関別認証評価については平成 21 年度に受審・認定 (認証機関: 大学評価・学位授与機構)，専門職大学院認証評価については 平成 21 年度に受審・認定 (認証機関: 大学基準協会) されている [18]．法人評価においても，第 1 期中期目標期間 (平成 16 年度〜平成 21 年度) についての業務の実績に関する評価 [18] と教育水準評価 [19] がなされている．これらはスプレッドシート形式での情報収集と実積報告書作成が行われたため，YUSE データの直接的な利用は行われていない．

その後，平成 22 年度より「教員データベース」が導入され (平成 23 年 3 月稼働開始)，基礎データの収集・公開と自己点検評価の PDCA サイクルが分離されたため，統計情報の入力と評価用プロセスのサポートを中心とした新 YUSE システムに移行している．以降区別したい場合は，移行前の YUSE を旧 YUSE システムあるいは YUSE オリジナルバージョンと，また，移行後のシステムを，新 YUSE システムまたはその開発コードで YUSE/TNG と呼ぶことにする．現在は，

- 教員による自己点検評価 (平成 23 年度実施，平成 24 年度実施予定)
- 組織活動自己点検評価 (平成 24 年度実施予定)

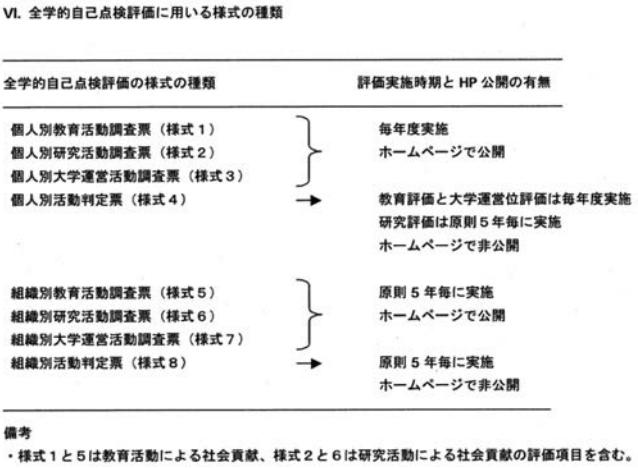
が YUSE/TNG のサポート下で進行中であり，組織単位の情報の集約・比較を行うための組織情報集約システムの開発も行っている．また，組織別自己点検評価の評価項目は，大学評価・学位授与機構が実施する機関別認証評価，選択的評価，専門職大学院認証評価 (資料は [20] を参照) において利用される基本的観点の入力とも関連しており，外部評価における基礎資料として入力されたデータが利用できるようになっている．

1.3 本稿の構成

以降は，YUSE による自己点検評価等の支援について順次説明を行い，続いて，大学評価と同じく PDCA サイクルを回す必要がある情報セキュリティマネジメントシステム (ISMS)[21] との比較について議論した上で，まとめと今後の課題を述べる．

2 YUSE を用いた自己点検評価活動支援

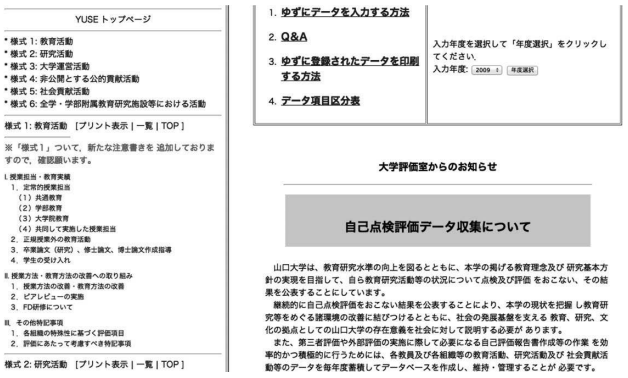
2.1 初期の評価計画と YUSE


VI. 全学的自己点検評価に用いる様式の種類

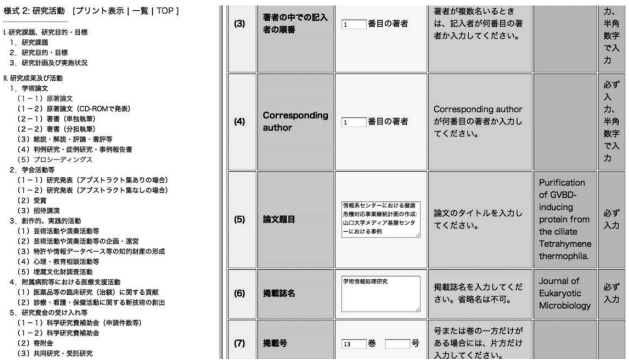
全学的自己点検評価の様式の種類		評価実施時期と HP 公開の有無
個人別教育活動調査票（様式１）		毎年度実施
個人別研究活動調査票（様式２）		ホームページで公開
個人別大学運営活動調査票（様式３）		
個人別活動判定票（様式４）	→	教育評価と大学運営位評価は毎年度実施 研究評価は原則５年毎に実施 ホームページで非公開
組織別教育活動調査票（様式５）		原則５年毎に実施
組織別研究活動調査票（様式６）		ホームページで公開
組織別大学運営活動調査票（様式７）		
組織別活動判定票（様式８）	→	原則５年毎に実施 ホームページで非公開

備考
・様式１と５は教育活動による社会貢献、様式２と６は研究活動による社会貢献の評価項目を含む。

図 1: 全学的自己点検評価に用いる様式の種類 (全学的自己点検評価実施要領 (平成 **13** 年 **12** 月 **11** 日承認) より抜粋)



(a) トップページ



(b) 研究成果入力画面

図 2: **YUSE** (オリジナルバージョン) での個人別自己点検評価のための基本データ入力画面 (平成 **21** 年度用)

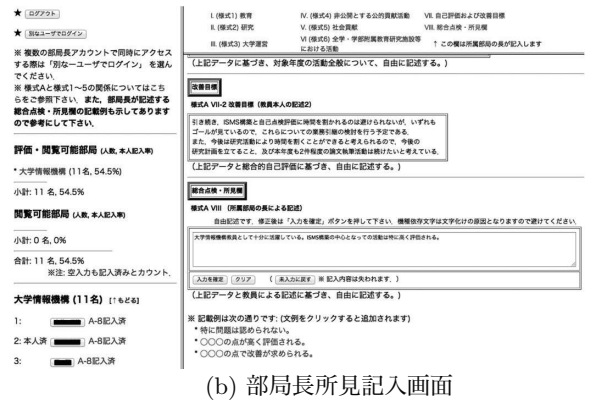
上述の通り，「山口大学の全学的自己点検評価実施要領」(平成 13 年 12 月) が自己点検評価の最初期の定義を与えている．図 1 は当初予定されていた各種記入様式と，それらの評価サイクルとの関係である．教育活動と大学運営活動に関する個人別自己点検評価は毎年，個

人の研究水準評価と組織別自己点検評価は 5 年に一度実施することが予定されていた．個人別自己点検評価で用いるデータを継続的に収集，公開するために作成されたのが YUSE であり，平成 14 年 7 月に平成 13 年度データの入力が開始された．

図 2 に YUSE の個人別自己点検評価の入力メニューを示す．(a) は様式構成を示すトップページ，(b) は研究業績の入力画面である．このスナップショットは平成 21 年度データの入力用システムのものであるため，入力内容を定義した様式の構成は図 1 とは異なっている点に注意されたい．収集内容はほぼ毎年修正が行われているため，入力画面の構成も合わせて少しずつ修正されている．ただし，データについては過去に収集したデータを新しい項目構成に合わせて再編成したものが保存されており，例えばこの図のバージョンでは，(a) の右側に示すドロップダウンメニューで選択することにより，平成 13 年度から平成 20 年度までの活動実積も閲覧編集可能である．

2.2 教員全般的活動評価

(a) 活動評価システムトップページ



(b) 部局長所見記入画面

図 3: **YUSE** (オリジナルバージョン) での教員全般的活動評価システムの記入画面 (平成 **19** 年度データを対象とした平成 **20** 年実施のもの)

自己点検評価では，実施要領 (図 1) にある通り，当初から様式 4 (後に様式構成の変更により様式 A と名称変更) のような評価用のシートがデザインされ，評価の実施が計画されていた．一方，YUSE の開発当初のバージョンにはこうした評価支援機能は含まれていなかったが，後に機能拡張を行い，平成 18 年，平成 19 年には評価シート様式 A に基づく全般的活動評価のサポートがなされた．拡張された機能には，(1) YUSE 入力データからの集計値の算出，(2) 教員個人による自己評価及び改善目標の作成，(3) 部局の長による総合点検・所見の入力，が含まれており，図 3(a) のような画面で教員個人による集計値の閲覧及び評価の入力が，また，部局長用システムでは図 3(b) に示す通り，左フレームに評価対象組織と内訳の一覧，右フレームに，選択された教員の情報と総合所見記入画面を配置している．部局長による記入結果は教員自身が図 3(a) で確認し，必要に応じて不服申立てと協議も可能としていた．

記録によると，平成 19 年度の教員の評価実施率は 52%，平成 20 年度は 65%で，周知徹底にはやや問題がある．また，スケジュールについてであるが，平成 18 年度実積の評価では，平成 19 年度年 11 月 1 日に入力が開始され，終了にあたる学長による全般的活動評価の公表が 3 月 31 日付けでなされている．翌年度実積はそれぞれ 7 月 22 日と 1 月 22 日付けで実施されている．毎年度実施される PDCA の C のフェーズ期間としてみた場合，5〜7ヶ月という期間はやや長過ぎる感がある．この点については改めて ISMS との比較で議論を行う．

なお，YUSE は CSV ファイル形式のデータの集まりとしてデータベースを記憶しているので，全般的活動評価で使われる集約処理は，SQL などの汎用言語で行うのではなく，別途専用の簡易言語を設計・実装して行っている．例えば，研究業績の集約処理の一部は次のように定義されている:

```
aggregate <A-2-1> from <2-2-1-2-1> <2-2-1-2-2> =
  <2> = "著書"
  <3> = {{ count(<*1>)+count(<*2>) }}
  <4> = {{ count(<*1>) }}
  <5> = {{ count(<*2>) }}
  <6> = ""
  <7> = ""

aggregate <A-2-1> from <2-2-1-3> =
  <2> = "総説・解説・評論・書評等"
  <3> = {{ count(<*>) }}
  <4> = ""
  <5> = ""
  <6> = {{ count(array_filter(<*>, 'eq_3_4')) }}
  <7> = {{ count(array_filter(<*>, 'eq_3_const1')) }}
```

他にも define, insert, delete, move, rename といった操作文を用いて，データベース本体のメンテナンスと，YUSE の入力項目定義の修正が行えるようになっている．また，入力画面の簡単な編集システムも準備されているので，データベースと入力画面のメンテナンスはソースプログラムレベルの改修をほとんどせずに実施されていた．

2.3 教育貢献度評価

教育貢献度評価は

> 個々の教員の担当する個々の授業の質の改善を通じて、学部・研究科等の教育水準の向上と質の改善に資することを目的とする。
> (教員の全学自己点検評価実施要領 (平成 19 年 5 月 14 日決定) より抜粋)

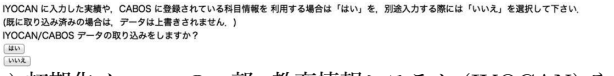
と定義され，平成 20 年度に実施された．実施手順の一部を実施要項等から抜粋すると次のようになる:

- 評価対象者を，授業改善システムの違いから，(1) 医学部医学科の教員で山口大学医学教育総合電子システム (eYUME) に入力を行う者と，(2) 本学の (1) 以外の教員で山口大学教育情報システム (IYOCAN) に入力を行う者とに区別する;
- (1) の者については，eYUME による教員の自己点検を医学部の長がさらに点検評価を実施する;
- (2) の者については，教員自身かが IYOCAN 及び YUSE の関連入力項目を点検し，担当各授業の「学生の学力向上への貢献状況」を記述した後，各組織の長が所属教員の教育活動状況及び自組織の教育上の課題等についてさらに点検評価を行う．

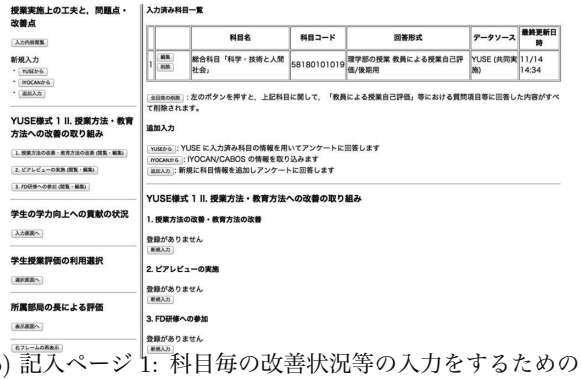
記述がやや複雑になっているのは，医学部医学科が独自の学習支援システム (eYUME) を先行して運用しており，全学共通の教育情報システム (IYOCAN) とは独立していたためである．より詳しくみると，医学部医学科以外の教員については，次の 5 つのデータソースがあることになる:

- 教育情報システム (IYOCAN) に登録された教員自身による評価と工夫や改善などの記述;
- 同 IYOCAN システムに登録された学生による授業評価;
- YUSE の様式 1 (教員の教育活動調査票) の 「1-II 授業方法・教育方法改善への取組み」に入力されたデータ;
- 電子シラバスシステム (CABOS)[8] に登録された科目情報;
- 教員が独自に調査した学生授業評価.

YUSE には自己点検評価以外には用いないという利用制限があるのだが，IYOCAN も YUSE と同様にデータの利用目的が制限されており，利用規則で「当該部局の大学教育職員本人の同意を得ているときには」という条件を付けて目的外利用を認めている．そのため，教育貢献度評価のサポートシステムでは，IYOCAN データの自動的なデータ取込みが出来ず，後述の通り教員自身による選択的取り込みの仕組みを提供せざるを得なかった．



(a) 初期化メニューの一部: 教育情報システム (IYOCAN) や電子シラバスシステム (CABOS) からのデータ取込み選択画面



(b) 記入ページ 1: 科目毎の改善状況等の入力をするためのエントリページ

(c) 記入ページ 2: 自己評価と部局長による評価

図 4: **YUSE** (オリジナルバージョン) での教育貢献度評価システムの記入画面 (平成 **19** 年度データを対象とした平成 **20** 年実施のもの)

図 4 は教育貢献度評価の教育職員の入力画面の一部である．(a) は初期化メニューの一部で，IYOCAN / CABOS からのデータの一括取り込みを選択することができる．予め取込んでおくことも技術的には可能であるが，上述の通り，利用規則により本人の同意を得る事が必要であるため，このような選択肢を与えることになった．図の (b), (c) は入力内容の編集画面である．(b) は科目情報の一覧ページで，個別科目に関するアンケートの編集／削除や，他のデータソースからの選択的取込みが可能である．図 (b) の画面では，本人の自己点検評価記入，学生授業評価利用の可否の指定，独自調査結果提出の有無の指定，及び部局長評価の閲覧が行える．部局長による評価画面では，図 3(b) と同様に，左フレームに教員一覧，右フレームに教員の記入内容の閲覧と評価入力ページが表示される．

このシステムでは CSV 形式等による静的なデータのやり取りではなく，IYOCAN 及び CABOS のバックエンドで稼働する PostgreSQL サーバへの直接接続によっ

てデータをやり取りしている．従って，システムの稼働時には，CABOS 2007 年度データ, IYOCAN 2007 年度前期データ，同 後期データ，YUSE ローカルデータ，の 4 種類のデータベースを利用している．

教育貢献度評価の入力率は 77.8%，学長による概要の学内公開は 平成 21 年 3 月 31 日付けである．

複数のデータソースに予め入力された内容をもとに評価を行うので，評価のための追加の利用者負担は，電子シラバスや授業評価システムの入力がすべて行われているという前提であればそれほど大きくはない．(入力済みデータを確認の上，自己評価のために数行の入力を行うのみである．) 一方，システム開発は，データの利用規則の関係でデータ取り込みを選択的にせざるを得ないことに加え，(授業評価の入力をしていないケースや授業を分担しているケースなどのように) 取り込むデータが存在しない場合でも適宜修正・追加入力できるようにしたために，ロジックが複雑になってしまった．開発のコストがかかる上に，似たような情報を何度も入力させられているというネガティブな印象を生む原因にもなっているようである．学内データ流通のための制度の整備に加え，データソースから集計されたデータについては確認以外の処理を認めない方針にするなど，エンドユーザの自由度を減らすことでトータルコスト低下が可能な一例と考える．

2.4 研究水準評価

研究水準評価は，平成 19 年度に平成 13 年度〜平成 18 年度の 6 年間の研究業績データを対象として実施された．上述の全般的活動評価及び教育貢献度評価は教員の自己点検評価結果に基づいて部局長がさらに評価を行うという仕組みであったが，研究水準評価は，教員自身による相互評価 (ピア・レビュー方式) の形態を取り，対象教員 866 名の教育職員を 36 の分野別のグループに分けて分科とし，分科毎に評価がなされた．分科は科学研究費補助金申請の際の分科に基づいており，人数の少ない分科を適宜統合することで作成されている．評価実施の前年度から分科の決定，分科の世話係による判定者 (判定責任者と判定補助者) の選出，研究水準判定基準 (卓越，優秀，標準，要努力) の定義作成がなされた．

YUSE によるサポートは概ね次のように分類される:

- 判定基準作成のための予備的なデータ提供
  各分科には水準判定基準に作成に先立ち，分科の構成メンバーに関する 3 年分の YUSE データ (匿名化処理済み) が渡された．匿名化データでは，職員 ID が研究水準評価用 ID に置き換えられ，さらに，論文等の著者情報は，(1) 著者人数，(2) 被評価者の順位，(3) 責任著者か否か，という情報に置き換えられている．

「山口大学教員研究水準評価」の評価結果について

1．このたび実施しました「山口大学教員研究水準評価」におけるあなたの研究水準評価結果は，次のとおりでしたのでお知らせします。

分科名： 情報学
判定責任者： 刈谷 丈治
判定補助者： 中田 充, 葛 崎偉, 市川 哲彦, 松野 浩嗣, 伊藤 暁

氏名	評価結果				判定根拠	
	卓越	優秀	標準	要努力	該当した判定基準	成果還元効果を加算
[redacted]	□	■	□	□	優秀基準3 優秀基準4 標準基準1	□
備考	＊「成果還元効果を加算」にチェックがある場合は，各分科の判定基準に応じて，1）成果還元効果を加算した結果，判定結果が，あるランクから上のランクに上昇した場合(例，「標準」における基準に成果還元効果を加算した結果「優秀」へランクアップした)を，または，2）当該ランクの基準（数が不足）に成果還元効果を加算した結果当該ランクにあると認められた場合を示す。					

2．あなたが所属する分科の評価結果の状況は，次のとおりです。

分科所属者数	卓越	優秀	標準	要努力	その他(判定不能等)
[redacted]					1

(a) 判定結果確認画面 (教員個人用)

分科毎一覧

注意
1．評価欄が空白の場合は，判定不能（評価結果に対し，本人から不服申し立てがなされたが，協議によっても決着が付かなかった等）を示します。
2．評価基準は分科毎に異なります。

「山口大学教員研究水準評価」の評価結果について

1．このたび実施しました「山口大学教員研究水準評価」における分科「情報学」の研究水準評価結果は，次の通りでしたのでお知らせします。

分科名： 情報学
判定責任者： 刈谷 丈治
判定補助者： 中田 充, 葛 崎偉, 市川 哲彦, 松野 浩嗣, 伊藤 暁

	氏名	所属	職名	評価結果				判定根拠	
				卓越	優秀	標準	要努力	該当した判定基準	成果還元効果を加算
1	[redacted]	大学院理工学研究科（理学）	准教授	□	□	■	□	優秀基準4 標準基準1 標準基準2 標準基準3	□
2	[redacted]	大学院理工学研究科（理学）	准教授	□	■	□	□	優秀基準1 優秀基準3 優秀基準4 標準基準1 標準基準2 標準基準3	□
3	[redacted]	大学院医学系研究科（工学）	准教授	□	□	■	□	標準基準1 標準基準2 標準基準3	□
4	[redacted]	大学情報機構	准教授	□	■	□	□	優秀基準3 優秀基準4 標準基準1	□
5	[redacted]	大学院理工学研究科（工学）	教授	□	□	■	□	標準基準1 標準基準2 標準基準3	□

(b) 判定結果確認画面 (分科毎用)

図 5: **YUSE** (オリジナルバージョン) での研究水準評価結果確認画面

- 水準判定のためのデータ提供，判定結果記入スプレッドシートの作成
  各分科の判定担当者には，YUSE から抽出された匿名化済みの 6 年分のデータと，判定結果記入用の Excel ブックの提供を行った．匿名化データは，Excel マクロによって，CSV 形式データを読み込んだ上で，適宜見出しの追加や罫線の追加などのフォーマット処理を加えて作成されたものである．

- 判定結果の収集と公開
  教員個人が判定結果と根拠資料を確認するための Web システムと，部局長が判定結果を確認するための Web システムの提供を行った．

図 5 に判定結果確認画面のスナップショットを示す．(a) は個人用，(b) は全学の分科一覧とそれぞれの判定結果の内訳を確認するための画面である．その他に，教員の所属部局毎に判定結果を確認するための機能も提供されている．

前述の教育貢献度評価が，複数データソースの統合利用処理を含むやや複雑なロジックで作られているのに対し，研究水準評価支援では，データ抽出とフォーマット処理が中心で，比較的単純な機能のみを提供している．これは，水準判定処理の部分をすべて判定担当者自身が行っているためである．実際，評価実施のスケジュールは次の通りであり，かなり長期間にわたることが判る:

- 5 月下旬 各分科毎に大学評価室より世話役を依頼.
- 〜6 月 29 日 世話役から分科所属の教員への呼びかけにより，研究水準を判定するための責任者及び補助者（若干名）の選出を行う.
- 6 月 18 日〜7 月 13 日 教員による誤記入箇所の修正.
- 〜7 月 31 日 大学評価室から各責任者・補助者宛に教員の研究活動実績データを送付.
- 〜9 月 28 日 分科の判定基準に基づき責任者・補助者が研究水準を判定し，所定の書式で判定結果を大学評価室に報告する.
- 〜10 月 19 日 大学評価室が結果を取りまとめ、判定結果（水準と判定根拠) を各教員に通知.
- 10 月 22 日〜11 月 20 日 不服申し立て
- 11 月 26 日〜12 月 21 日 不服協議
- 1 月 31 日 研究水準評価概要の公開

さらに，基準案作成作業はこの前年度に行われ，平成 19 年 1 月 18 日に開催された「教員の研究水準評価に係る意見交換会」においていくつかの分科会の基準案の提示と意見交換がなされている．こうした下準備も含めて，非常に人的なコストの高い評価であったと言え，IT を含めた技術面のサポートが期待されるが，一方で，精度の高い評価の自動化には，(1) 論文の引用回数の評価を含めた書誌学的な評価情報処理機能の整備，(2) 学会運営など書誌学的な指標には含まれにくい尺度の指標化，(3) 誤記入による誤った評価を避けるための記入精度の向上支援，のような技術的な課題に加え，こうした労力を人・システム間でうまく分担して，システム開発コスト，非評価者や評価者の人的コスト，及び評価で得られるゲインのバランスをどう取るのか，という現実的な課題もあり，評価の難しさを表す一例であると言える．

2.5 人事評価サポートシステム

YUSE のデータは全学的自己点検評価に使う事を原則としており，人事評価には使わないことになっている[9]．そこで教員の人事評価の試行 (平成 20 年度実施) では，YUSE に蓄積されたデータのうち，人事評価の基礎資料となる項目を参照するためのシステムを別途作成し，各教員の判断で利用することとした．なお，現在は次節で説明する「教員データベース」に基礎データの入力機能は移行し，YUSE は新システムに置き換えられているので，教員データベース情報を用いた人事評価支援が行われている．

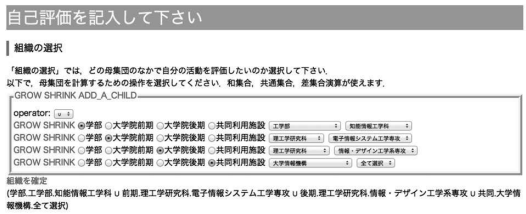
2.6 新 YUSE システム (YUSE/TNG) を用いた教員の自己点検評価

平成 22 年度より「教員データベース」が導入され 平成 23 年 3 月稼働を開始した．これは，自己点検評価システム (YUSE)，教育情報システム (IYOCAN)，電子シラバスシステム (CABOS)，教職員広報システム (人・知・技)，学術情報レポジトリ (YUNOCA)，などの複数のデータソースから共通する項目を抜き出し，別の情報ソースとして独立させたものである．従ってそれまで YUSE の収集項目に含まれていた担当授業科目[10]，研究業績，学内委員会，及び外部資金獲得状況，などの基礎データの収集が教員データベースに移行した．これに伴い YUSE (旧バージョン) の基礎データ入力部 (様式 1〜様式 6) の機能を停止し，統計データの閲覧と評価部 (様式 A) に相当する機能を新たに開発した．平成 23 年度に前年度データに基づく教員の自己点検評価に利用され，また，平成 24 年度でも同様に利用される予定である．

YUSE 旧バージョンではデータ入力とその継続的な蓄積が重要な機能であったが，YUSE/TNG では統計値の入力と指標の計算，及びそうした指標を用いた各種評価の支援が主要機能になっている．統計値のデータソースは電子シラバスシステムや教員データベースになるのだが，初年度の評価実施では，密なシステム間連携を敢えてせず，その代わりに他システムのデータ閲覧画面へのリンクのみを提示して統計値は各自が入力するという，上述の人事評価システムと人事評価サポートシステム間の関係に似た疎な連携を行っていた．これは，統計値の算出自体も自己点検評価の一部として考えていたためであるが，初回評価実施時の説明会・アンケート等で不評であったため，一部統計値については教員データベースの項目を CSV 形式でダンプした生データから計算するように，処理手順の変更を検討している．

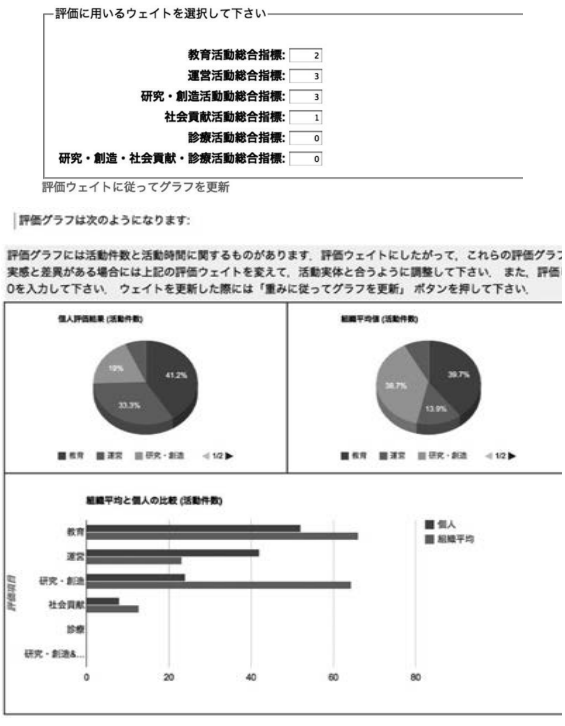
図 6 に自己点検評価画面の一部を示す．単に，指標データを表示するだけではなく，組織の指標値との比較や，前年度の自身の指標データとの比較も可能にしている．比較のための組織定義は (a) で行う．学部，学科等を基本単位として，和集合，共通集合，差集合を任意に組み合わせて定義可能である．他にも，評価室や部局長宛の意見を記入するためのアンケート画面も用意されている．

現在のところ，学内にある様々なシステムの役割分担は次のようになっている:



(a) 自己点検評価のための比較組織の定義

(b) 自身の評価指標値と，組織平均や過年度との比較



(c) 自身の評価指標値と，組織平均や過年度との比較．重み付け入力部，グラフ表示部

図 6: **YUSE/TNG** (新バージョン) での自己点検評価システム画面

(1) シラバスや授業評価などは教学支援システムに入力;

(2) 研究・大学運営の活動実績の記入は継続的に教員データベースに入力;

(3) 情報公開は研究者総覧または人・知・技で行う;

(4) 定期的な自己点検評価及び部局等への意見の入力は YUSE で行う;

(5) 業績査定は人事評価システムで行う.

以前に比して，システム連携も含めてより明確になっているのであるが，こうしたシステム間の相互関係が把握しにくいという意見があるのも事実である．そこで，各種システムへの入り口を一カ所にまとめた「教員ポータル」の作成が検討されており，現在公開に向けて準備中である.

2.7 組織活動情報集約システム

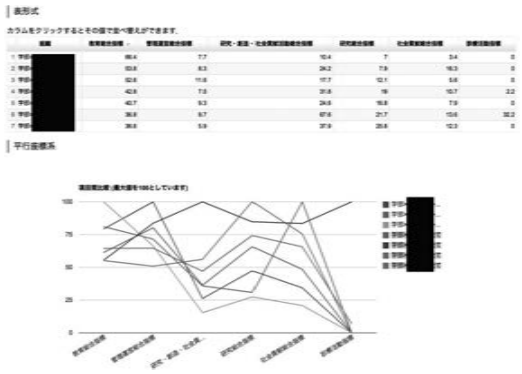


図 7: 組織活動情報集約システムでの比較画面

上記の個人別自己点検評価では，特定集合における指標値と自身の指標値を比較できるようにしているが，組織活動情報集約システムでは，組織別の項目別集計の機能と，様々な項目での組織間比較をすることができるようにしている．例えば学部の基本的な指標の平均値を，図 7 のように，ソーティング可能なテーブル形式と平行座標系を用いて表示することができる.

2.8 組織別自己点検評価

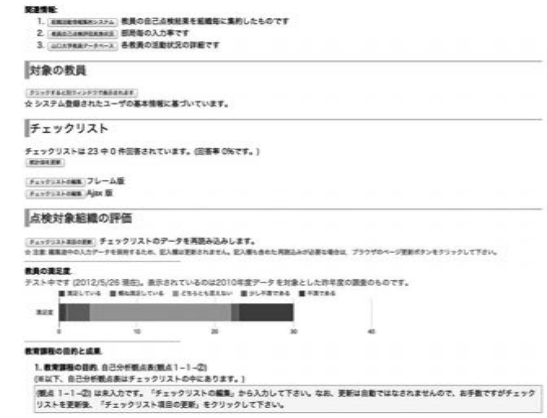
平成 13 年に定められた「全学的自己点検評価実施要領」(図 1) では組織別の評価の実施が定められたが，平成 19 年に定められた基本方針では

> 本学を構成する諸組織並びに大学全体を対象とする点検・評価は、主に、3）に示す第三者評価に対応するための全学的自己点検評価活動として行う。

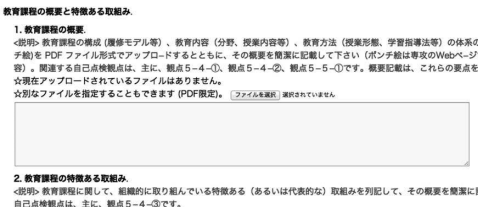
と定められ，組織評価は第三者認証評価と国立大学法人評価のための全学的自己点検評価活動と位置づけられた[11]．基本方針変更後のこうした評価は法人評価における学部・研究科に関する現況調査表の評価の観点 [22] に則って平成 19 年度〜平成 20 年度にわたって実施され，資料 [23] として平成 21 年 2 月に公表されている．この評価は Excel スプレッドシート等を用いた情報収集に

よって実施されており，YUSE 等のオンラインシステムによるサポートは行われなかった．

平成 24 年度に実施予定の組織別自己点検評価では，その位置づけに変化はなく，評価項目も大学評価・学位授与機構が実施する機関別認証評価，選択的評価，専門職大学院認証評価自己分析観点表の項目と，自己点検評価のための項目から構成されているものの，前回の評価と異なり，YUSE/TNG による入力支援が利用されている．



(a) 基本情報部．基本的な観点は別画面で入力する．



(b) 評価の記述部．組織別の集約情報や基本的な観点についての入力内容に基づいて行われる．

図 8: 組織別自己点検評価システムの入力画面．専攻に関する自己点検評価入力画面の一部．

図 8 に組織別自己点検評価のためのページの例を示す．(a) では部局に関する基本情報として，外部情報源へのリンク，部局に含まれる教員の一覧確認画面，自己分析観点表から構成されるチェックリストの記入画面などへのリンクが表示されている．(b) は教育課程の目的等を記入する部分であり，適宜チェックリストの内容が引用される．他にも，書き込み権限の管理機能，タイムスタンプを用いた編集衝突の検出機能，過去データ編集のためのタイムワープ機能など，複数担当者による分担記入の支援機能もサポートしている．

3 議論: ISMS との比較

本稿の第一著者と第二著者は，山口大学メディア基盤センターの情報セキュリティマネジメントシステム (ISMS)[21] の構築に関わっているが [24, 25, 26]，そうした立場から大学評価の現状を見ると，ISMS の構築当初に遭遇したものと同様な問題に直面しているように見える．

一つは，法令で定められた外部評価対応のための評価書作成という面が前面に出てしまい，PDCA サイクルが見えづらい，という点である．勿論，ISMS と大学評価では，テーマがそれぞれ情報セキュリティと大学経営という異質なものではあるが，(1)「何をしなくてはならないのか」ということに気を取られると全体的な PDCA サイクルが見えにくくなること，(2) そのためプロセスが形骸化しやすいこと，(3) 結果として PDCA サイクルの意義が理解しづらくスタッフから負担感に基づく不要論が出やすいこと，という点が共通しているように思われる．

ISMS の構築当初を振り返ると，規格書の要求事項を理解し，対応する文書等の準備をするだけで手一杯で，PDCA サイクルによる段階的な改善について組織内で十分な議論する余裕は全くなかったし，組織内でも ISMS に反対する声も存在した．しかしながら，ISMS の構築運用が進むにつれ，リスクアセスメントをはじめとする各種イベントが年間計画に組み込まれるようになり，その結果，徐々に個別アクティビティの全体中での位置づけが目に見えるようになってきた．現在では，ISMS の PDCA サイクルを回すことは通常業務の一つになりつつある．

一方，現在の大学評価の PDCA サイクルは，評価室を始めとする関係者の努力にも関わらず，ISMS の構築当初と同様，意識的にイベントを追いかけていかないと様々な活動がどのように連携しているのか見えづらいように感ずる．一つの要因はスピード感の欠如ではないかと考えられる．実際，ISMS の C(heck)-A(ct) フェーズを構成する内部監査やマネジメントレビューが，約二ヶ月の短い期間に現状を対象として集中的に実施されるのに対し，例えば平成 18 年度実積の教員自己点検評価は翌年度の 11 月から 3 月にかけて行われており，その最終的なフィードバックが教員に戻ったのは平成 19 年度末である．つまり，新年度の PDCA サイクルの開始段階になって初めてその前々年度のチェック結果が出されていて，定例的なチェックが次の活動へのインプットなっているという点が見えづらくなっている．

また，ISMS では PDCA サイクルや個別プロセスが，ISO や JIS 規格によって明確に定義されているので，それらを順次実践することで徐々に組織内に浸透させることができたのだが，大学評価や IR には相当する明確な定義があるわけでは無く，また，大学毎の多様性があり単純に他大学や他国の事例を輸入すればすむというものでもない．PDCA サイクルの “見える化” や “実質化” は，ISMS に比して更に難しい課題と言える．

自身にとってのメリットが見えないとネガティブな印

象を持ちやすいという点も共通の課題である．文献 [27] が「評価疲れ」と呼んでいるが，評価活動が始まって 10 年以上になるものの，依然として評価についてのネガティブな感情が残っているのではないかと推測している．大学評価には当初から人事評価に結びつくのではないかという反対意見が強かったと聞いているし，それが，平成 19 年版基本方針の「ただし，この結果を人事評価の参考にはしない」という但し書きにも残っていた．評価に関するアンケートの結果を見ても，評価自体に対する否定的な意見は依然として存在している．これはちょうど，ISMS の構築において，現場の運用に近いスタッフほどリスクの識別自体にあまり良い印象を持たず，リスクアセスメントや内部監査の意義を理解してもらうのに非常に苦労したことを想起させる．メディア基盤センターのような組織にとっては，リスクの識別や外部からの改善要求は，予算獲得に結びつく “ビジネスチャンス” であるし，何よりリスクを取ることを経営陣が表明すれば余計な責任をスタッフが負わなくて済むのであるが，実際のところ，欠点を指摘されているというようなネガティブな印象を払拭するのは容易ではなかった．大学評価やそれを含む IR が，外部のステークホルダーの要求に応えるだけではなく，内部に居る個々の教員や組織にも利益をもたらすものである，ということを少しでも目に見える形で示すということが，今後更に重要になると考えられる．

4 まとめ

これまで本学において開発された新旧の YUSE による各種評価の支援機能について概要を説明した．いずれも評価室 (評価室設置以前は評価データベース専門委員会) とメディア基盤センターの協力により学内で設計・開発されたシステムである．文献 [28] と比較すると，大学毎の多様性があるにも関わらず，IT システムの視点から見た評価プロセスの支援体制が，大枠では類似している点が興味深い．大学評価に関する法制面に由来する外部的な要求が同じであることと，複数データソースの統合利用やデータウェアハウスなど，利用されるデータ管理のための基盤技術が同様であることに由来していると考えられる．「大学改革」の実施により大学の多様性は今後さらに拡がると予測されるが，引き続き適宜総括と比較をすることによって，技術的な基盤での共通点と，多様性に由来する部分とを切り分け，結果として開発・運用コストの最適化につなげられることを期待している．

ただ，ISMS との比較で述べた通り，IT システムからのサポートが必要不可欠ではあるものの，PDCA サイクルを回す意義を明確にし組織内に浸透させることも，有効な大学評価のためには重要であると考える．その意味では，各種システムへの入り口を一カ所にまとめた「教員ポータル」が，技術的には非常に単純であるにもかかわらず，今後重要な役割を果たす可能性がある．そのため技術的な観点からのコストだけではなく，大学評価の有効性という観点からみたコスト・パフォーマンスについても議論する必要があると考えている．

ISMS との比較は第一著者の経験に基づく主観的な部分も含んではいるが，本稿で述べた大学評価サポートの事例が，少しでも評価文化の普及に寄与すればと期待している．

謝辞

YUSE オリジナルバージョンの入力・公開機能は山口大学教育学部北本卓也教授によって開発されたものです．教育貢献度評価においては，IYOCAN, CABOS との連携では大学教育センター岡田耕一講師，教育学部野村厚志准教授及び教育学部北本卓也教授に，また，保健学科授業評価システムとの連携では大学院医学系研究科市原清志教授にご協力いただきました．本学におけるこれまでの大学評価活動は，評価委員会委員長／評価室室長をされた山口大学理学部藤島政博教授，人文学部湯川洋司教授，及び経済学部塚田広人教授，並びに評価室初代専任教員であった山口大学理学部笠野裕修准教授の多大なる尽力により進められてきました．

参考文献

[1] 山口大学総務部企画・評価課：“中期目標・中期計画等”, http://ds.cc.yamaguchi-u.ac.jp/~kikakuka/mokuhyo/mokuhyo.html.

[2] 山口大学:“人・知・技”, http://kyouin02.atm-y.jimu.yamaguchi-u.ac.jp/search_hcw/IST.

[3] 山口大学：“研究者総覧”, http://kyouin02.atm-y.jimu.yamaguchi-u.ac.jp/search/IST.

[4] W. E. Knight Ed.: “The Primer for Institutional Research”, Assocation for Institutional Research (2003).

[5] IDE 大学協会:“特集「大学教育と IR」”, No. 528 (2011).

[6] 文部科学省：“「大学改革実行プラン」について”, http://www.mext.go.jp/b_menu/houdou/24/06/1321798.htm.

[7] 文部省：“大学設置基準の一部を改正する省令の施行等について”, 文部事務次官通知文高大第一八四号, http://www.mext.go.jp/b_menu/hakusho/nc/t19910624001/t19910624001.html (1991).

[8] 大学審議会：“21 世紀の大学像と今後の改革方策について　—競争的環境の中で個性が輝く大学—（答申）”, http://www.mext.go.jp/b_menu/shingi/old_chukyo/old_daigaku_index/toushin/1315932.htm (1998).

[9] 大学審議会：“大学院設置基準等の改正について（答申）　（（平成 11 年 9 月 6 日　大学審議会））”, http://www.mext.go.jp/b_menu/shingi/old_chukyo/old_daigaku_index/toushin/1315954.htm (1999).

[10] 大学評価・学位授与機構：“試行的評価に関する検証について”, http://www.niad.ac.jp/n_hyouka/jouhou/kenshou/index.html, 大学評価学位授与機構 (2008).

[11] 試行的評価に関する検証委員会：“大学評価・学位授与機構が平成１２年度から平成１５年度までに実施した試行的評価に関する検証について―試行的評価に関する検証結果報告書―”, http://www.niad.ac.jp/n_hyouka/jouhou/kenshou/1174681_959.html, 大学評価学位授与機構 (2008).

[12] 総務省：“学校教育法”, e-Gov [イーガブ], http://law.e-gov.go.jp/htmldata/S22/S22H0026.html.

[13] 総務省：“学校教育法施行令”, e-Gov [イーガブ], http://law.e-gov.go.jp/htmldata/S28/S28SE340.html.

[14] 平野敏彦：“国立大学法人法・独立行政法人通則法・準用組込み条文表”, 文献 [29] の補足資料, http://www.law.hiroshima-u.ac.jp/lawschool/hirano/nyumon/hojinho.htm (2003).

[15] 山口大学：“山口大学学則”, http://web.cc.yamaguchi-u.ac.jp/~hoki/kisoku/d1w_reiki/41690210000100000000/41690210000100000000/41690210000100000000_j.html.

[16] 湯川洋司：“山口大学における大学評価の取組み”, 大学評価シンポジウム: これからの大学評価と自己点検・評価のあり方 (実施報告書), (シンポジウムは 2008 年 10 月 6 日に開催), 山口大学評価委員会, pp. 7–16 (2007).

[17] 文部科学省：“学校教育法施行規則等の一部を改正する省令の施行について（通知）”, 22 文科高第 236 号, http://www.mext.go.jp/b_menu/hakusho/nc/1294750.htm (2010).

[18] 山口大学総務部企画・評価課：“認証評価について”, http://ds.cc.yamaguchi-u.ac.jp/~kikakuka/ninsyo/ninsyo.html.

[19] 大学評価・学位授与機構：“国立大学法人等の第 1 期中期目標期間における教育研究の状況の評価結果について”, http://www.niad.ac.jp/n_hyouka/kokuritsu/kekka_h22/.

[20] 大学評価・学位授与機構：“大学機関別認証評価”, http://www.niad.ac.jp/n_hyouka/jouhou/kenshou/index.html.

[21] JIS Q 27001: 2006 (ISO/IEC 27001:2005): “情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム要求事項”, 日本規格協会 (2006).

[22] 大学評価・学位授与機構：“国立大学法人等の教育研究評価”, http://www.niad.ac.jp/n_hyouka/kokuritsu/index.html.

[23] 山口大学大学評価室:“「組織を単位とする全学的自己点検評価実施概要」に基づく「研究活動」及び「教育活動」の評価について”, http://committee.ue.yamaguchi-u.ac.jp/sosiki/sosiki_hyoukasho.pdf (2009).

[24] 市川, 永井, 長谷川, 伊藤, 三池：“情報セキュリティマネジメントシステム (ISMS) における効率的な詳細リスクアセスメント実施手法の提案と情報処理センターへの適用”, 学術情報処理研究, 12, pp. 52–58 (2008).

[25] 市川, 永井, 長谷川, 三池：“山口大学における情報セキュリティマネジメントシステム構築の実例”, 情報処理学会インターネットと運用技術研究会報告, **2009-IOT-6**, 6 (2009).

[26] 市川, 小柏, 永井, 小河原：“山口大学における情報セキュリティマネジメントシステム (ISMS) 構築テンプレート作成及び適用範囲拡張について”, 情報処理学会インターネットと運用技術研究会報告, **2011-IOT-14**, 6 (2011).

[27] 関口：“IR から見た大学評価の課題”, [5], pp. 25–30 (2011).

[28] 高田:“大学評価を基礎とする IR: 九州大学大学評価情報室における試行的取組みについて”, [5], pp. 35–39 (2011).

[29] 平野敏彦：“国立大学法人法の基礎知識”, 広大フォーラム, http://home.hiroshima-u.ac.jp/forum/2003-10/t1.html, 広島大学公報委員会 (2003).

注意

URL はすべて執筆時のものである.

注釈

1 山口大学第２期中期目標[1]
V 自己点検・評価及び当該状況に係る情報の提供に関する目標
1 評価の充実に関する目標
・ 大学活動の自己点検及び改善を効率的に実施するシステムを確立し大学活動の質の向上を継続的に図るとともに, その自己点検・改善活動の状況を適切に社会へ公開する。
2 情報公開や情報発信等の推進に関する目標
・ 多様な広報の手段・機会を効果的に活用し, 社会への説明責任を果たすとともに大学ブランド力を高めるための情報提供・広報活動を推進する。

2 文部事務次官通知文高大第一八四号[7]
第一　大学設置基準 (昭和三一年文部省令第二八号) の一部改正
一　自己評価等について
(一)　今回の大学設置基準の大綱化による制度の弾力化の趣旨を生かし、大学自らがその教育研究の改善への努力を行っていくために、当該大学における教育研究活動等の状況について自ら点検及び評価を行うことに努めなければならないこととしたこと。(改正後の第二条第一項関係)
(二)　この点検及び評価を行うに当たっては、前記の趣旨に即し適切な点検・評価項目を設定するとともに、適当な実施体制を整えて行うものとしたこと。(改正後の第二条第二項関係)

3 大学審議会答申[8]
第２章　大学の個性化を目指す改革方策
4. 多元的な評価システムの確立　－大学の個性化と教育研究の不断の改善－
(1) 自己点検・評価の充実
(2) 第三者評価システムの導入
(3) 資源の効果的配分と評価

4 大学院設置基準等の改正について (答申) [9]
1. 大学設置基準改正要綱
第一　自己評価等に関する事項
大学は、その教育研究水準の向上を図り、その目的及び社会的使命を達成するため、教育研究活動等の状況について自ら点検及び評価を行い、その結果を公表するものとすること。
大学は、1 の点検及び評価の結果について、当該大学の教職員以外の者による検証を受けるように努めなければならないものとすること。

5 学校教育法[12]
第百九条　大学は、その教育研究水準の向上に資するため、文部科学大臣の定めるところにより、当該大学の教育及び研究、組織及び運営並びに施設及び設備（次項において「教育研究等」という。）の状況について自ら点検及び評価を行い、その結果を公表するものとする。
２　大学は、前項の措置に加え、当該大学の教育研究等の総合的な状況について、政令で定める期間ごとに、文部科学大臣の認証を受けた者（以下「認証評価機関」という。）による評価（以下「認証評価」という。）を受けるものとする。ただし、認証評価機関が存在しない場合その他特別の事由がある場合であつて、文部科学大臣の定める措置を講じているときは、この限りでない。
３　専門職大学院を置く大学にあつては、前項に規定するもののほか、当該専門職大学院の設置の目的に照らし、当該専門職大学院の教育課程、教員組織その他教育研究活動の状況について、政令で定める期間ごとに、認証評価を受けるものとする。ただし、当該専門職大学院の課程に係る分野について認証評価を行う認証評価機関が存在しない場合その他特別の事由がある場合であつて、文

部科学大臣の定める措置を講じているときは、この限りでない。
4　前二項の認証評価は、大学からの求めにより、大学評価基準（前二項の認証評価を行うために認証評価機関が定める基準をいう。次条において同じ。）に従つて行うものとする。

6 学校教育法施行令[13]
第五章　認証評価
（認証評価の期間）
第四十条　法第百九条第二項（法第百二十三条 において準用する場合を含む。）の政令で定める期間は七年以内、法第百九条第三項 の政令で定める期間は五年以内とする。

7 国立大学法人法【第 35 条による準用】[14]
通則法第 32 条（各事業年度に係る業務の実績に関する評価）
国立大学法人は，文部科学省令で定めるところにより，各事業年度における業務の実績について，国立大学法人評価委員会の評価を受けなければならない。
2　前項の評価は，当該事業年度における中期計画の実施状況の調査をし，及び分析をし，並びにこれらの調査及び分析の結果を考慮して当該事業年度における業務の実績の全体について総合的な評定をして，行わなければならない。
3 国立大学法人評価委員会は，第 1 項の評価を行ったときは，遅滞なく，当該国立大学法人及び政令で定める審議会（以下「審議会」という。）に対して，その評価の結果を通知しなければならない。この場合において，国立大学法人評価委員会は，必要があると認めるときは，当該国立大学法人に対し，業務運営の改善その他の勧告をすることができる。
4 国立大学法人評価委員会は，前項の規定による通知を行ったときは，遅滞なく，その通知に係る事項（同項後段の規定による勧告をした場合にあっては，その通知に係る事項及びその勧告の内容）を公表しなければならない。
5 審議会は，第 3 項の規定により通知された評価の結果について，必要があると認めるときは，当該国立大学法人評価委員会に対し，意見を述べることができる。
通則法第 34 条（中期目標に係る業務の実績に関する評価）
国立大学法人は，文部科学省令で定めるところにより，中期目標の期間における業務の実績について，国立大学法人価委員会の評価を受けなければならない。
2 前項の評価は，当該中期目標の期間における中期目標の達成状況の調査をし，及び分析をし，並びにこれらの調査及び分析の結果を考慮するとともに，独立行政法人大学評価・学位授与機構に対し独立行政法人大学評価・学位授与機構法（平成 15 年法律第 114 号）第 16 条第 2 項に規定する国立大学及び大学共同利用機関の教育研究の状況についての評価の実施を要請し，当該評価の結果を尊重して当該中期目標の期間における業務の実績の全体について総合的な評定をして，行わなければならない。
3　通則法第 32 条第 3 項から第 5 項までの規定は，第 1 項の評価について準用する。

8 教育貢献度評価実施当時は電子シラバスシステム (CABOS) は IYOCAN と同様学内で作成されたものであったが，現在は新たに導入された修学支援システムの一部として運用されており，CABOS という名称も用いられていない．

9 正確には「山口大学における全学的自己点検評価に関する基本方針」の平成 23 年 3 月 18 日改正において,「人事評価には利用しない」という文言は削除され,「本学における全学的自己点検評価活動に限り、 原則として使用するものとする」という表現に変更されている．

10 電子シラバスの情報を自動入力していたので，実際には教員は追加・修正のみを行う．

11 後半の但し書きは，平成 23 年 3 月改訂版の基本方針では削除されているが,「組織を単位とする全学的自己点検評価実施概要」等の関連文書は改訂されていないので，位置づけには変化はない．

全学ポータルを用いた学生・教職員間多機能連絡システムの開発

Development of a multi-functional message system among students and faculty members using a university portal

二木 恵†，東 昭孝†，笠原 禎也†，高田 良宏†，松平 拓也†
Megumi Futatsugi†, Akitaka Higashi†, Yoshiya Kasahara†,
Yoshihiro Takata†, Takuya Matsuhira†

futamegu@staff.kanazawa-u.ac.jp, higashi@staff.kanazawa-u.ac.jp, kasahara@is.t.kanazawa-u.ac.jp,
yosihiro@kenroku.kanazawa-u.ac.jp, takusng@kenroku.kanazawa-u.ac.jp

†金沢大学総合メディア基盤センター

†Information Media Center, Kanazawa University

概要

金沢大学では平成 19 年度より学内ポータルサイトとして「アカンサスポータル」を運用している．この「アカンサスポータル」は，当初学生向けのポータルサイトとして始まったものだが，現在はスケジューラなどの教職員向け機能を追加し，また，給与明細，施設システムなどの学内システムとも認証連携することで，再度のログインが不要なシングルサインオンによるワンストップサービスを実現し，全学的なポータルとして利用されている．

本稿では，アカンサスポータルのなかでも，学生と教職員間の連絡手段として便利さの威力を発揮している学生・教職員間多機能連絡システムの概要および，連絡手段システムとしての工夫点を述べるとともに，運用で起きた問題点を報告し，今後の改良点を提示する．

キーワード

ポータル，メッセージ，メール送信，多機能，スパム

1. はじめに

金沢大学では, 平成 19 年度より学内の各種情報サービスを一括して Web から利用できる「アカンサスポータル」と呼ばれるポータルサイトを運用している[1,2,3]．アカンサスポータルは，平成 18 年度入学生からの携帯パソコン必携化に合わせて導入された学習管理システムを出発点に，当初教育用ポータルサイトとして運用されてきた[4]．平成 22 年度には，教職員向けの情報サービスも提供する全学ポータルシステムに拡張され, 現在では , 教育・研究・業務に不可欠な様々な情報サービスを提供するに至っている．

金沢大学のユーザ数は，学生約 10,500 人，教職員約 3,800 人になる．アカンサスポータルは，在学，在職者

のみが対象ではなく，卒業後や退職後も利用できるポータルサービスであり，アカンサスポータルにログインするための ID（金沢大学 ID）は，「生涯 ID」としての位置づけを持つ. この金沢大学 ID 発行数は約 45,000 になる．日々のログイン数は，平日約 3,000 ユーザ，休日は約 1,000 ユーザであり，履修登録期間などは最大で 1 日に約 4,000 ユーザがログインする[5,6,7].

近年，大学でも情報システムの構築が進み，業務の効率化が図られてきたが, 頻繁に行われる大学(教員，職員）と学生間の連絡手法は，依然として掲示板による呼び出しや，電子メールを用いてきた．これらの方法は非常に効率が悪く, 業務遂行の妨げとなっていた. 例えば，掲示板は，学生が掲示を見るまでに数日間かかることを覚悟せねばならず，また，電子メールを利用するには，相手のメールアドレスを知っていなければならないので，メールアドレスを収集した上，最新のメールアドレスの状態を保つように管理するなど，非常に手間のかかる作業が伴った.

このような状況を解決するために，我々は，アカンサスポータルに，大学と学生の連絡を容易かつ確実に行うための機能「メッセージ」を導入した．導入当初は，大学と学生間の連絡が主であったが，現在ではユーザ間の連絡および各種情報システムからの通知機能も加わり，スムーズな連絡環境の提供と業務の効率化に貢献し，学内の連絡手段として大きな役割を果たしている.

本稿では,まずアカンサスポータルにおける「メッセージ」機能の重要性,多機能性を示し，次に運用で起きた問題とその解決方法,ならびに改善策を述べ，「メッセージ」が連絡システムとしての確実性，速報性を増した経緯を説明する.

2. 機能概要

2.1. メッセージの役割

アカンサスポータルには，表 1 に示す機能がある. この中で，ユーザ間の連絡手段として利用されているのが「メッセージ」という機能である．この「メッセージ」とは，アカンサスポータル内でやりとりするメールのようなものである．この機能により，教職員から学生への連絡事項の伝達，学生から教員への講義に関する質問，その他各種のユーザ間の個人的なやり取り，システム通知としての図書返却督促や，求人情報の配信など，様々な用途に利用されている.

表 1 に示すように，アカンサスポータル内の機能のうち,「メッセージ」を利用している機能が，全体の半数に及ぶことから,「メッセージ」がアカンサスポータルにおける機能の中枢を担っていることがわかる.

それぞれの機能の中で,「メッセージ」がどのような連絡内容として利用されているかを表 2 に示す．アカンサスポータルではユーザに通知を行う際に，メールではなく，「メッセージ」で行うことを徹底している.

表 1　アカンサスポータル内の機能

●アカンサスポータル内部の機能

お知らせ ＊	メッセージ	リンクメニュー
スケジューラ＊	施設予約＊	物品予約＊
ボランティア＊	在籍管理	機能ガイダンス
時間割＊	電子掲示板	学生呼び出し＊
成績照会	サークル情報	学生住所確認
求人情報＊	就職支援＊	IC カード一時停止＊
授業アンケート＊	図書サービス＊	パスワード再発行＊

●各種システムへのシングルサインオン先

教務システム	Web シラバス	LMS システム＊
サイボウズ	給与明細	施設システム
教員情報 DB	留学生ネット	学内 Web メール
図書館システム＊	SNS ＊	包括ライセンス

＊:メッセージを利用している機能

2.2. メッセージ配信のしくみ

次にメッセージ配信のしくみについて簡単に述べる.

アカンサスポータルの「メッセージ」内容は，基本的にはログインしてから Web ブラウザ上で確認するが，ユーザに対する利便性を高めるために「メッセージ」をユーザが指定するメールアドレスに転送するサービスも行なっている．メール転送の有無は，ユーザの個人設定で「メッセージをメールで受け取る」の on/off の切替えにて変更が可能である.

2.3. メールアドレスの交換が不要

ユーザへの連絡は「メッセージ」で行われ,「メッセージ」はユーザが各自登録したメールアドレスにメール転送されることから，結果としてユーザ同士はお互いのメールアドレスを知る必要がなくなる．これは，学生，教職員間でありがちな，メールアドレスの交換の必要がないことを意味し，変更の際の再連絡などの煩わしさから開放する効果がある.

また，メールアドレスがユーザ間で非公開であるため，自分のメールアドレスが外部に漏れるという心配もない．このことは，個人情報の観点からもセキュリティ的にユーザへ安心感を与えることができる.

表 2 機能ごとのメッセージ内容

お知らせ メッセージへの転送
メッセージ 通常メッセージ：個々人単位での連絡やりとり 回答付きメッセージ：簡易アンケート形式 緊急お知らせメッセージ：緊急時発信するメッセージ
スケジューラ スケジュールの登録・変更通知 スケジュール通知（リマインダー）
施設予約・物品予約 施設／物品予約申請の管理者宛の通知
ボランティア ボランティア申請時の管理者宛の通知 キャンセル待ちから昇格した際のユーザへの通知
時間割 休講，補講，時間割変更の通知 連携先 LMS での学生・教員間のメッセージ 連携先 LMS でのレポート提出通知
学生呼び出し 学生の呼び出し通知
サークル情報 大会申請の登録通知
学生住所確認 学生への住所登録の督促
求人情報 求人情報登録の通知
就職支援 進路決定・未決定の通知
身分証（IC カード）一時停止申請 身分証である IC カードを紛失した時の一時停止申請
授業アンケート 授業アンケートの学生からの回答登録通知
図書サービス 図書貸出の返却督促
SNS フレンド同士のメッセージ コミュニティイベント通知メッセージ
パスワード再発行 パスワード再発行の手続き案内

2.4. メッセージへの自動登録

アカンサスポータルの「お知らせ」は，掲示板的な役割をもつ．掲載者が「お知らせ」を知らせたい対象者を指定して登録すれば，該当するユーザはそのお知らせをログイン後のトップ画面で確認できる．

「おしらせ」は必ずしもログインして見てもらえる保証はないため，重要なお知らせは，「お知らせ」を掲載時に，そのままの内容で「メッセージ」としても発信できる「メッセージへの自動登録」機能を提供している（図 1 参照）．

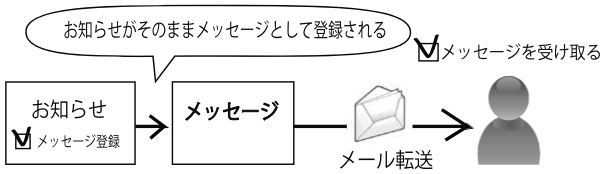


図 1 メッセージからメールへの転送

例えば，在学，在職者全員（15,000 人あまり）に対してお知らせを掲載し，メッセージ登録も指定した場合は，一度に15,000件のメッセージが登録され，また，同時に15,000通のメール送信も可能ということになる．

通常，メールをこの規模で発信することは，一般操作では不可能であるが，アカンサスポータルを通じてならば，容易に数万レベルでメール送信が可能となることを意味する．

3. メッセージの多機能性

教育上の配慮や利便性の向上，業務の効率化に対応した結果，アカンサスポータルの「メッセージ」は非常に多機能になった．本節では，具体的な「メッセージ」がもつ機能について述べる．

3.1. 通常メッセージ

通常のメッセージの作成画面は，「件名，本文，多言語入力指定，事務連絡メモ，配信日時，添付ファイル，宛先，所属指定による宛先，同報宛先，重要度レベル設定，学生による返信を許可設定」の入力項目を持つ．

アカンサスポータルで作成する「メッセージ」には，以下の工夫がある．

- 教職員が学生複数にメッセージを送った場合は，学生同士は BCC 扱いとなり同時に送られた他の学生がいるかどうかも分からない状態とする．
- 学生は，連携する LMS からは担当教員や職員のみにメッセージを送ることができる．基本的に学生同士の検索を許可しないが， SNS のフレンド同士ならばお互いの検索は可能とする．
- 多言語入力（現在は英語・中国語・韓国語に対応）が可能
- 添付ファイルは３つまで可能
- 学生には見えない，教職員専用の事務連絡メモ欄がある
- 所属単位に一括でユーザ指定が可能
- 学生からの返信を拒否することができる

3.2. 回答付きメッセージ

複数のユーザに，同じ質問による調査をしたい場合がある．このような簡易アンケート形式として利用できるのが，「回答付きメッセージ」である．

この「回答付きメッセージ」の特徴は以下となる．

- 回答方法は，回答番号のメールアドレスへの返信にて行う（返信内容は，空でも可）
- 回答を受け付ける有効期限がある
- URL リンクによる，Web からの回答も可能
- 回答結果の統計が出せる
- 回答返信の督促ができる

「回答付きメッセージ」の作成画面を図 2 に示す．本文の他に，回答項目を 9 個まで設定可能でき，複数回答もオプションで可能としている．回答付きメッセージを受信したユーザへは，図 3 のメッセージおよびメールが送られてくる．回答方法は，質問項目に応じたメールアドレスへ空メールによる返信を行うか，指定URL クリックよるWebブラウザからの回答になる．

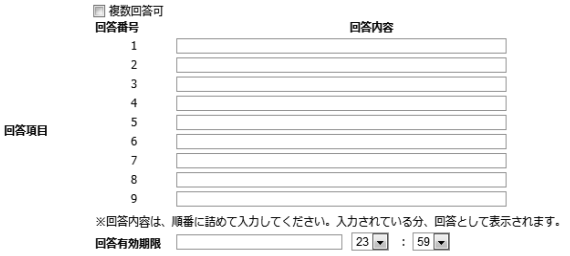


図 2　回答付きメッセージ作成画面

〈送信者〉
総合メディア基盤センター
二木　恵

〈本文〉
今日は何を食べましたか?

１．ごはん
ma1_rarptrpKIFTerPo.ans@cis.kanazawa-u.ac.jp
２．パン
ma2_rarptrpKIFTerPo.ans@cis.kanazawa-u.ac.jp
３．その他
ma3_rarptrpKIFTerPo.ans@cis.kanazawa-u.ac.jp
４．たべていない
ma4_rarptrpKIFTerPo.ans@cis.kanazawa-u.ac.jp

[回答受付期限]2012/06/28 23:59 まで

――回答方法――
１. 各回答のメールアドレスあてに空メールにて返信して下さい.
または，Web から回答もできます.
URL:https://acanthus.cis.kanazawa-u.ac.jp/Portal/u002/messageAnswerAccept.php?ID=rarptrpKIFTerPo
２．メールからの回答は単一回答のみ可能です.
複数の回答をしたい場合は Web から回答を行ってください.
３．連絡事項がある場合，本文に記入して下さい.

※システムからのメールの為, このメールには返信できません.

図 3　回答付きメッセージのメール内容

URL リンクによる Web からの回答する場合は, 図 4 の画面となる.

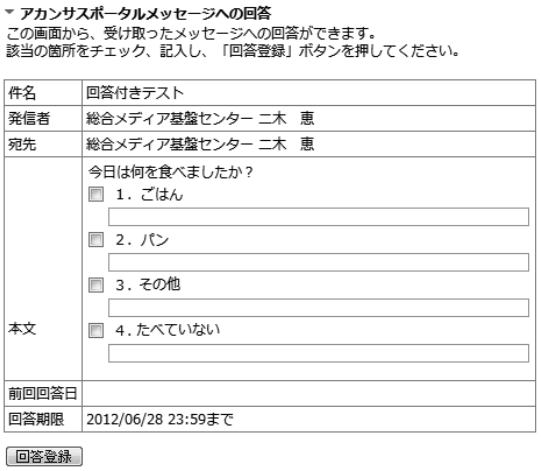


図 4　回答付きメッセージ Web 入力画面

回答結果は，簡易グラフ表示と詳細の閲覧が可能である．回答結果の詳細表示例を図 5 に，簡易グラフ表示の表示例を図 6 に示す.

図 5　回答結果の詳細表示

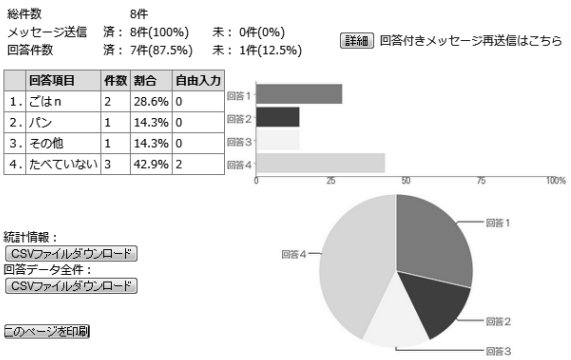


図 6　回答結果の簡易グラフ表示

3.3. 宛先のグループ化

メッセージの宛先をグループ化し，一括での宛先設定が可能である.

メッセージ作成時の宛先を設定する手順は，まずユーザを検索し，次にその検索した結果の中からユーザを特定する.

「宛先グループ化」機能は，よく利用するような宛先を事前にグループとして登録しておき，宛先にグル

ープとして設定することで，一括で宛先追加を可能とするものである．通常の手順と比べ，「ユーザ検索」，「宛先として追加」の２段階の手間を省くことができる．

グループには「My グループ」と「公式グループ」の二種類がある．「My グループ」は個人専用で使用するグループであり，「公式グループ」は名の通り，全学的に使用可能な公的なグループである．

「公式グループ」は，公的なグループであるが，全ユーザに公開されているわけではない．ユーザは，使用を許可されている公式グループのみ使用ができる．許可されていない公式グループは，候補として表示自体されないようになっている．

どちらのグループも，メンバ設定には，個人を特定して追加する方法と，身分や所属など範囲を指定して追加する方法の，両方の指定方法がある．図 7 の画面は，公式グループのメンバ編集画面になる．上段が個人を特定した追加エリアで，下段が範囲指定による追加エリアである．

図 7　宛先グループ 設定

3.4. CSV 差し込み型メッセージ対応

メッセージの本文に差し込みたいフィールドを指定し，それぞれフィールドに応じたデータ列を持つ CSV ファイルを読みこませることで，大量にメッセージを送信できる，差し込み型メッセージ作成機能を用意した．MS WORD の差し込み印刷のイメージである．

例えば，学生に授業料免除のメッセージを送る場合，A さんには半額免除で金額は XX 円，B さんは全学免除で金額は YY 円などの場合便利である．

図 8 に，サンプルを提示する．本文は同じ体裁で，宛先名と，免除区分，金額がそれぞれ異なる．本文には，差し込みフィールドとして「%x%」という（x は半角数字）の変換指定文字列を用いる．図 9 のサンプル CSV の列には，フィールド列に応じたデータをセットしておく．

学籍番号 : %1%%2%様
願い出のありました，授業料免除申請につきまして以下とおり決定しました．
＜%3%＞
所定の授業料（%4%円）を当該銀行の預金口座に・・

図 8　差し込みメッセージサンプル

%1% 学籍番号	%2% 氏名	%3% 免除区分	%4% 金額
0100520004	金沢　一郎	半額	133,950
0100520005	金沢　ニ郎	全額	267,900
0100520006	金沢　三郎	全額	267,900
0100520007	金沢　四郎	半額	133,950

図 9　差し込みデータ用 CSV

これにより作成されたメッセージ内容は，図 10 のとおりとなる．

学籍番号 : 0100520004　金沢　一郎様
　願い出のありました，授業料免除申請につきまして以下とおり決定しました．
　＜半額＞
所定の授業料（133,950 円）を当該銀行の預金口座に・・

学籍番号 : 0100520005　金沢　二郎様
　願い出のありました，授業料免除申請につきまして以下とおり決定しました．
　＜全額＞
所定の授業料（267,900 円）を当該銀行の預金口座に・・

：以下続く

図 10　差し込み後の各メッセージ

3.5. メール返信からのメッセージ登録

メールに転送されてきた「メッセージ」に対し，ユーザが個々に使用するメーラから直接メールを返信した際も，その返信をアカンサスポータル上の「メッセージ」として登録する機能である．

メールに転送されてきたメッセージに対し「メーラから直接メールとして返信したい」という要望により，本機能を追加した．この場合，アカンサスポータル側は「誰から誰に対する返信か」を識別し，送信者・受信者の両方のアカウントに「メッセージ」を登録する必要がある．以下に同機能の仕組みについて詳細を記す．

アカンサスポータルでは，データベース上，メッセージの構造を「メッセージ本体」と「メッセージ宛先」にテーブルを分けて考える．「メッセージは，一人の人が複数の人に向けて発信するものである」という前提から，このような「メッセージ本体：メッセージ宛先が 1：n」の構造となっている．

図 11 は，アカンサスポータルのメッセージのデータ構造図である．両テーブルを紐付けているのは，メッセージを識別するユニークな識別子（メッセージ識別 ID）である．メールから返信があった場合に，その返信をメッセージとして登録するためには，「どのメッセージ識別 ID に対する返信か」と，「誰への返信か（発信者情報）」及び「誰からの返信か（受信者情報）」が判別できればよいことがわかる．

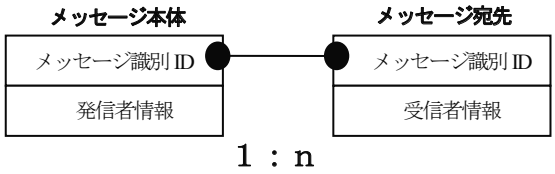
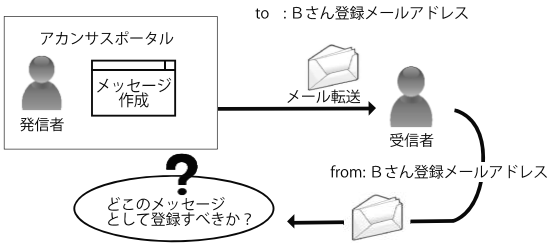


図 11　メッセージテーブル構成

図 12 に，アカンサスポータルが返信メールを受信した際における，前述の 3 つの情報を取得する方法を示す．メッセージ識別 ID が返信メールから識別できれば，返信メールをメッセージとして登録できることがわかる．そこで，メッセージ識別 ID を返信時に必ず残される情報である，アカンサスポータルへの返信メールアドレスに埋め込むこととした．

同機能を実現するため，従来アカンサスポータルからのメッセージをメールへ転送する際に用いていた，固定の送信元メールアドレスを，図 13 のように，メッセージ識別 ID を暗号化した値に変更した．

メッセージ識別 ID をそのまま利用せずに暗号化した値を採用した理由は，メッセージ識別 ID が数値型の連番で作成されており，ユーザが意図的に返信先メールアドレスのアカウント部分を編集することで，別人が発信したメッセージへの返信として登録されてしまう危険性を防ぐためである（図 14 参照）．



必要な情報への疑問	答え
どのメッセージに対する返信か？	メッセージ識別 ID が必要
誰への返信か（発信者は誰か？）	メッセージ識別 ID から判別可能
誰からの返信か（受信者は誰か？）	from のメールアドレスから特定

図 12 「メッセージ」登録に必要な情報

今までの from（固定アカウント）
acanthus@cis.kanazawa-u.ac.jp
↓
変更後（メッセージ識別 ID を変換（例））
p3vbsxczi5ao.msg@cis.kanazawa-u.ac.jp

図 13　メッセージ識別 ID を埋め込んだアドレス

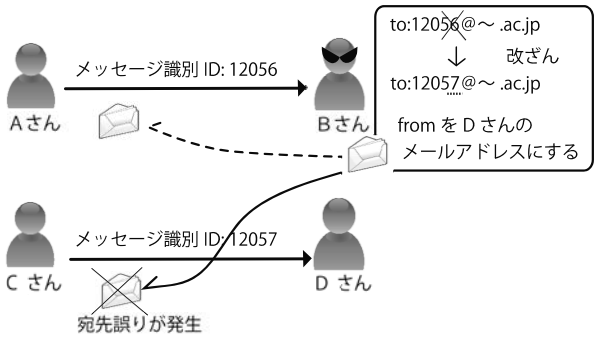


図 14 メッセージすり替わりの危険

次に，メッセージ登録するまでのシステムの流れを図 15 で説明する．

①メッセージ識別 ID が埋め込まれたメールアドレスに対して返信が行われると，②SMTP サーバでまずメールをキャッチする．③SMTP サーバでは，postfix の Alias 設定により，正規表現で一致した場合，④の PHP プログラムを呼び出す．PHP プログラムは，⑤アカンサスポータル Web サーバのメッセージ登録用の SOAP サービスを呼び出す．⑤のアカンサスポータルの SOAP サービスでは，パラメータチェックを行ない，正常ならばデータベースにメッセージを登録する．この後，⑥A さんがアカンサスポータルを見ると，B さんからの返信をメッセージとして確認できる．

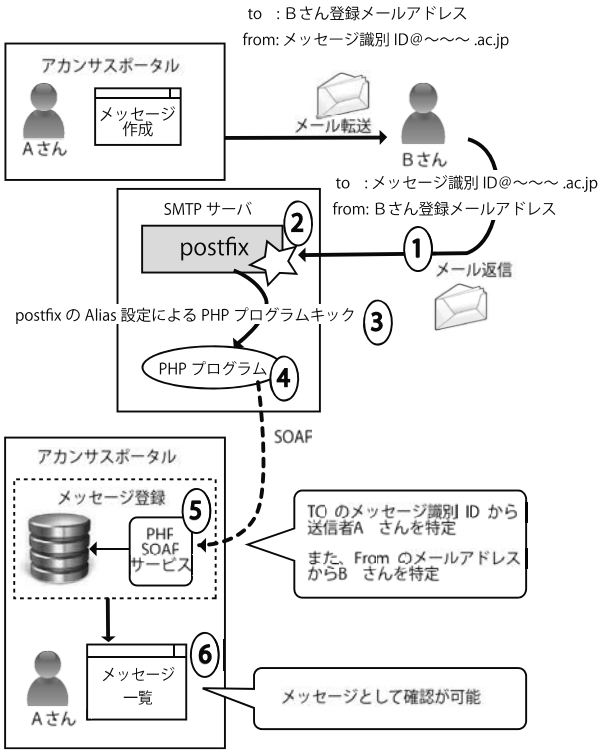


図 15　メール返信によるメッセージ自動登録

4. 問題への改善策

4.1. 携帯電話向けメールのスパム回避策

アカンサスポータルから配信するメールは，たやすく 1 万，2 万単位で送信することが可能だと述べた．しかし，短時間に大量のメールを送信することは，携帯電話キャリアが実施する迷惑メールフィルタによる受信ブロック対象(スパム扱い)となる危険性が高い．一度スパム扱いされてしまうと，携帯向けにメール送信ができなくなり，連絡システムとして致命的となる．このため，本システムは大量のメール配信が行われた場合も，絶対にスパム扱いされないよう，1 キャリアあたり 1 時間 1,000 通の送信制限を設け，小出しにメール送信するしくみをとっていた．

しかし，緊急事態の発生を知らせる「緊急連絡メッセージ」など，至急連絡する必要のあるメールも，1 万人の場合 4，5 時間かかることとなり，緊急連絡用途として十分に機能を満たせないという問題があった．

この問題の改善のため，平成 24 年度新たに，携帯向け大量送信可能なソフトウェア「アクセルメール[8]」を導入した．

「アクセルメール」は，KLab 社製の携帯・スマートフォン向けメール配信を高速化する，導入型のソフトウェア(MTA)である．このソフトウェアをメール配信時に経由することで，スパムの心配なく携帯やスマートフォン向けに，大量メール配信をすることが可能となる．また，オプション機能により，キャリアではじかれたメールをエラーレポートという形で確認することもできる．キャリアが返すエラー形式は，各社バラバラであるが，このアクセルメールが差分を吸収して報告するものである．

図 16 にシステム構成を示す. システム構成の変更点は，アカンサスポータル内部の MTA である Postfix から，今までは基幹系 MTA のメールサーバにリレーしていたのを，アクセルメール MTA にリレー先を変更するだけである（正確には，基幹系メールサーバを通さなくなったことでウイルスチェックができなくなったため，アカンサスポータルで別途ウイルスチェックサーバを通し，その後アクセルメールへ送信している)．

本来，アクセルメールは携帯向けの大量メール送信ソフトであるが，アカンサスポータルでは携帯に限らず，すべてのメールをアクセルメール経由で送信することとした。その結果，アカンサスポータルから送るメールすべてについて，送信エラーを検知することが可能となった．

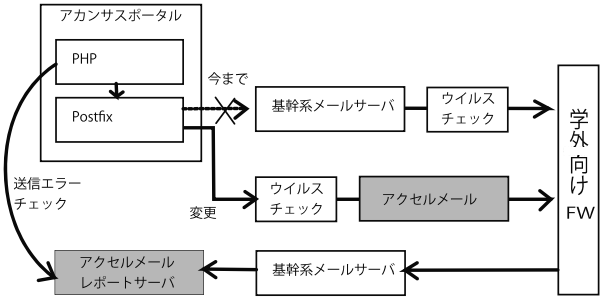


図 16　アクセルメール導入のシステム構成

アクセルメール導入により，携帯向けにメール送信を小出しにする必要がなくなり，メール送信時間が格段に短くなった．2012 年 5 月 9 日に行われた，本学の緊急連絡訓練での動作実績を図 17 に示す. この訓練では，本学の全学生・教職員に対し，緊急事態の発生を知らせるメッセージが，1 万 4 千件弱のメールとして対象ユーザ全員に送信されたが，送信に要した時間は 20 分あまりであった. また, アカンサスポータルでは，全ユーザに初回に転送用メールアドレスの登録を義務付け，その後も定期的にメールアドレスの変更などがないかをポータルログイン時に確認する運用を行っているため，送信エラー件数は，全ユーザの 9%弱にとどまっていることがわかる．

メール送信件数	: 13,695 件
メール送信時間	: 20 分 21 秒
	(2012/05/09 16:19:02 ～ 2012/05/09 16:39:23)
メール送信エラー件数	: 1,224 件

図 17　緊急お知らせ訓練時のメール送信結果

このように従来，全ユーザへのメール転送に 4，5 時間かかっていた送信処理が，20 分に短縮されたことは，連絡システムとしての速報性を大いに高めることとなった．また，アカンサスポータルから大量送出されるメールが，携帯電話キャリア側でスパム扱いされる危険性もほぼ解消し，ユーザへの情報到達性と信頼性が大幅に向上した．

さらに，送信エラーを検知できるようになったことは，アカンサスポータルの連絡システムとしての確実性を高めるのに大いに貢献することができる．これらアクセルメール導入後の違いを，表 3 に示す．

表 3　アクセルメール導入による違い

	今まで	アクセルメール導入後
メール送信時間（1 万 3,000 通）	4～5 時間	20 分
スパム扱いの危険性	あり	なし
送信エラー検知	なし	あり

4.2. 添付ファイル付きメールへの対応

3.1 節で述べたように，アカンサスポータルのメッセージ機能は，ファイルを最大 3 つまで添付することが可能である．しかし，メッセージをメール転送する機能において，大容量ファイルを添付したメールが，大人数のユーザに容易に送れることは，メールサーバに対する負荷や，メールを受信するユーザにとって大きな負担となり得る．

特に，2.4 節で述べた「お知らせ」を掲示するときに，確実に配信先ユーザに内容を見てもらうために，お知らせを掲載したユーザが，「メッセージ」に同時登録することは容易に想像できる．

このとき，掲載者が，お知らせ内容を Web ブラウザで閲覧することしか考慮せず，数メガサイズの PDF ファイルを添付掲載し，メッセージ自動登録（メッセージでも配信するよう設定）すると，1 万人を超えるユーザに数メガバイトの添付ファイル付メールが一度に配信されてしまう．現にそのような掲載者のオペレーションにより，基幹系メールサーバに多大な負荷をかけて，ダウンさせる事例も発生した．改善策として，お知らせ登録時にメッセージへの同時登録が行われた場合には，その宛先人数や添付ファイルサイズをチェックし，一定サイズ以上のメッセージは，メールに添付ファイルを付けないように機能変更した．

メール本文には，添付されるはずであったファイル名と，ポータルの Web ブラウザで添付ファイル内容の確認を促すコメントを付け加えた．

5. 考察

5.1. メッセージの利用度

ユーザニーズに応えるべく，創意工夫を行なってきた結果として，ユーザのメッセージ利用頻度が増大した。図 18 は，送信された「メッセージ」の全体件数を，年度別に示したものである．1 年毎に約 50 万件ずつ増加しているのが分かる．平成 24 年度は，6 月 20 日現在ですでに 72 万件となっており，残り月数を計算すると，平成 24 年度末には 300 万件近くに達することが予想できる．このことから，「メッセージ」は利用度からみても，本学の連絡システムとして，重要な位置づけとなっていることが言える．

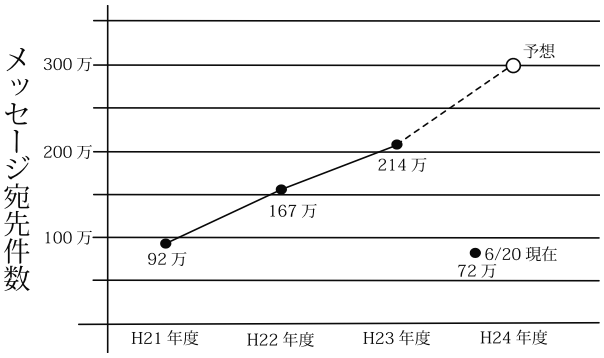


図 18　メッセージ件数の年度推移

5.2. 今後の改善点

これまでの運用により明らかになった問題点と改善策について述べる．

5.2.1. 転送メール対応

アカンサスポータルに登録されているメールアドレスが，メーラでの転送設定や，forward，MTA 側の機能等から，さらに別のメールアドレスに転送設定されている場合も少なくない．この場合，転送された先の別のメールアドレスから，アカンサスポータルに返信メールを送っても，メッセージとして登録されないという問題が起きる．原因は，from（送信元アドレス）のメールアドレスが，アカンサスポータルに登録された転送先メールアドレスと異なるために，ポータル側で返信を送ってきたユーザが特定できず，メッセージ登録処理が行えないためである．

システム側としては，アカンサスポータルに登録されていないメールアドレスから送られてきたメールは，セキュリティ上，送信者不明としてメッセージ登録しないのが望ましいが，複数のメールアドレスを学内外で使い分けているユーザは少なからず存在することか

ら，今後，このような場合の対応を検討する必要がある．対応策としては，from から送信者を特定するのではなく，返信者から送られてくるメールの To にメッセージ識別 ID と送信者 ID などの情報を暗号化した文字列を使用する予定である。

5.2.2. 送信エラー検知による今後の展開

これまでに，ユーザから「アカンサスポータルでメッセージを送っても，メールに転送されたことは分かるが，実際にメールとして相手が受け取っているかどうかわからないので不安だ」という意見が数多く寄せられている．

メールを相手が読んだかどうかは，メールシステム上わからないことはやむを得ないとしても，アカンサスポータルからメールを送信した時に，送信エラーとなったものは，少なくともメッセージを送ったユーザに連絡をすることが，有効と考えられる．

平成 23 年度までは，本学基幹系のメールサーバにリレーしていたため，携帯キャリアや外部メールサーバからのエラーなどはアカンサスポータル側で分からない状況であった．しかし，平成 24 年度のアクセルメールの導入により，送信エラーを検知することが可能となった．

4.1 節で，平成 24 年 5 月に行った緊急お知らせ訓練時でのメール送信エラー検知では，メール発信件数 13,695 件のうち，送信エラーとして検知できた数は 1,224 件になったと述べた．表 4 に送信エラーとなった原因の内訳を示す．

表 4 緊急お知らせ訓練時の送信エラー件数一覧

エラー理由	件数
メールアドレス不在	645 件
MailBox 一杯	1 件
携帯利用停止中	6 件
受信拒否	437 件
送信先ドメイン不正	6 件
その他不明エラー	29 件

現状では，アカンサスポータルでメッセージを送信すると，送信者は受信者のメッセージ開封状況が見え，相手がメッセージを開封したかどうかと，相手のメールに転送されたかが確認できる．

今後は，送信エラーの検知により，図 19 のように具体的に送信エラーとなっているユーザとエラー理由を示すことが可能となる．メール送信エラーとなっているユーザが把握できることで，送信者は相手が未読の場合，別な連絡手段を考慮するなどの対応が可能となる．

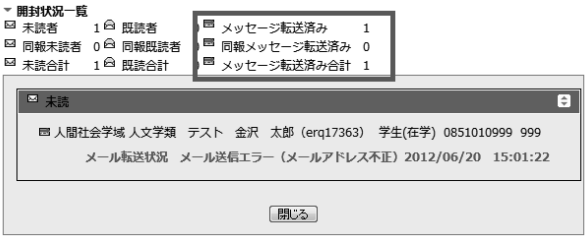


図 19 今後の転送済みメッセージの詳細画面

また，メール送信エラーとなったメールアドレスのユーザには，ログイン後に「あなたのメールアドレスへは○○により，送信できませんでした」という旨の連絡と，メールアドレス修正の依頼を画面から行うことが可能である．

これにより，連絡システムとしての情報到達性がより高まることが期待できる．

6. まとめ

大学での連絡システムとして備えなければならない性能は何かを考えると，まずシステム的な観点からは，「情報到達性（指定したユーザに確実に届く）」，「速報性（速く届く）」，「安全性（セキュリティ上問題がない，個人情報の漏洩がない）」が必要と言える．本システムでは，メール配信のしくみよりセキュリティの安全性を保ち，アクセルメールの導入によって速報性を満たし，送信エラー検知により情報到達性をより強固にしようとしている．

また，ユーザの利便性の観点からは，本システムは「多様な連絡方法」および「発信対象者の選択のし易さ」について有益な機能を持ち合わせている．

年々増加するメッセージの送信件数に表されているように，本システムは本学の連絡システムとして大きく貢献できていると言える．

今後は，きめ細かくユーザニーズに応えた，より安全で確実なシステムとして，さらなる開発を続けていきたいと考える．

参考文献

[1] 笠原 禎也, 高田 良宏, 森 祥寛, 松平 拓也, 二木 恵, 東 昭孝, 金沢大学統合認証システムと全学ポータルの構築 ～学内情報サービスの融合化をめざした統合認証とポータル環境の整備事業～, 金沢大学総合メディア基盤センターCOM.CLUB, pp.4-7, 2010.

[2] 東 昭孝, 笠原 禎也, 高田 良宏, 二木 恵, 松平 拓也, 森 祥寛, 金沢大学におけるポータルシステムの開発手法と現状の運用について, 大学 ICT 推進協議会 2011 年度年次大会論文集, pp.417-419, 2011.

[3] 東 昭孝, 笠原 禎也, 高田 良宏, 二木 恵, 松平 拓也, 森 祥寛, 金沢大学におけるポータルシステムの現状と課題～アカンサスポータルについて～, 第 36 回教育システム情報学会全国大会（JSiSE2011）, 第 3 全国大会講演論文集, pp324-325, 2011.

[4] 森 祥寛, 堀井 祐介, 東 昭孝, 二木 恵, 金沢大学における教育用ポータルサイト「アカンサスポータル」の開発 第 34 回 教育システム情報学会（JSiSE2009）, 2009.

[5] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 森 祥寛, Shibboleth によるポータルシステムを中心とした教育用情報システムの連携, 平成 22 年度情報教育研究集会, 講演論文集, pp141-144, 2010.

[6] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 森 祥寛, 大学における Shibboleth を利用した統合認証基盤の構築, 情報処理学会論文誌, Vol.52(2), pp.703-713, 2011.

[7] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 学認との融合化を視野に入れた金沢大学統合認証基盤の構築と運用, 学術情報処理研究, (当該号), 2012.

[8] アクセルメール, http://www.klab.jp/am/ , (参照日 2012.6.27),

分散キャンパスを利用したファイルバックアップシステム

File backup system taking advantage of remotely distributed campuses

野口 宏 †, 大瀧 保広 †, 鎌田 賢 †‡

Hiroshi NOGUCHI†, Yasuhiro OHTAKI†, Masaru KAMADA†‡

noguchi@mx.ibaraki.ac.jp, y.ohtaki@mx.ibaraki.ac.jp, m.kamada@mx.ibaraki.ac.jp

茨城大学 IT 基盤センター †
茨城大学 工学部 ‡
Center for Information Technology, Ibaraki University†
Faculty of Engineering, Ibaraki University‡

概要

東日本大震災において，茨城大学では人的な被害や ICT 機器自体には大きな被害が無かったものの，停電と建物内立ち入り禁止が長時間に渡り続いた．同規模の地震への対策を考える時、今回の震災でも懸念された建物倒壊という事態を想定しておく必要がある．本学では分散キャンパス構成になっているため，一つのキャンパスにおいて建物倒壊が起こったとしても，他のキャンパスの建物も同時に倒壊する可能性は低いと考えられる．そこで一般には通信・運営コストの面で不利な分散キャンパスという立地を逆手にとって，ファイルシステムのバックアップをほぼリアルタイムで他キャンパス相互に配置する分散バックアップシステムを設計・構築し，その評価を行った．

キーワード

災害対策, 分散バックアップ

1 はじめに

昨年 3 月 11 日に発生した東日本大地震では，茨城大学 (以下、「本学」と略) では人的な被害は少なかったものの，ICT 基盤は多くの被害を受けた．本学では日立, 水戸, 阿見の 3 地区に大きなキャンパスを有する (図 1)．各キャンパスにおける最大震度はそれぞれ 6 強, 6 弱, 6 弱であった．震源から最も遠い阿見キャンパスでは 5, 7 階に PC が設置してあったため，殆どの PC が転倒し中には机と共に転倒しているものもあった．幸いにも，サーバ類は収納したラックが床にボルトで固定されていたため転倒することはなかった．

停電期間は日立, 水戸, 阿見各キャンパスにおいてそれぞれ 3 日間, 2 日間, 2 日間であった．この長時間にわたる停電のため ICT 基盤は麻痺状態となっていた．

特に情報提供の要となる本来の大学の Web サーバ (以

図- 1: 茨城大学 3 大キャンパス

下,「本 Web」と略) が機能しなかった．地震発生が後期日程入試の前日であったこともあり，前期日程試験合格の入学手続き者や後期日程入試志願者に対して大学として早急な情報発信が必要であったが, それができない状況となった．震災前から学外組織に委託して開設してあった携帯電話向けの入試広報用 Web サイトはあったが，一般の方々には URL が知られておらず，検索エンジンでも上位には入っていなかったため，本学は Web での情報提供を全く行っていないように見えていた．

そこで初期対応として VIOPS(仮想化インフラストラクチャ・オペレーターズグループ) を通じて Web サーバを提供するボランティアに依頼し，クラウド上に本学の Web サーバ (以下,「仮 Web」と略) を構築し [4][5]，更に本 Web の URL で参照できるように仮の DNS サーバも構築した．本 Web 及び本学の DNS が復旧した後に JP DNS の設定を元に戻して頂いたが，DNS の『浸透問題』[6] が発生し，本 Web からの情報提供を充分に行うことができなかった．

サーバの停止期間が長引いた最大の要因は，サーバが設置された建物が甚大な被害を受けたことである．建物によっては 1 週間以上立ち入り禁止が続いた．特に震源地に近かった日立キャンパスでは，外壁が破壊された建物が多く，単独での立ち入りが更に 1ヶ月以上にわたり禁止されることとなった．サーバ室の通電チェックとサーバ類の再稼働作業は，建物倒壊の怖れがないことを確認できない状況のまま行われた．サーバ類は UPS に接続されていたため幸いデータの消失等は無かったが，データの保全が確認できるまで続いた恐怖は忘れられない．

同規模の地震への対策を考えるとき，今回の震災でも懸念された建物倒壊という事態を想定しておく必要がある．そこで我々は，建物倒壊時にも比較的短時間でサービスを再構成できるシステムを現行のネットワークトラフィックに影響が出ない形で実現できることを示すことを目的とし，震災時の対応の問題点を分析し，計算機システム及びネットワーク基盤の更新を機に対策を取り入れたシステムの設計・構築を行い，その評価を行った．

建物倒壊時には建物内に設置されたサーバの復旧は考えられないため，新サーバへの切り替え及びその前提となるデータ保全は必然となる．まず当該サーバに関連するデータは全て短い時間間隔で日頃から他のキャンパスでバックアップ保存するものとした．次にバックアップを所有しているキャンパスにおいて，システムの再稼働を実施する．この際，データを保存してあるネットワークドライブの IP アドレス等が変更になる．このため，セカンダリ DNS の外部委託を行いサーバ切り替えを確実に行えるようにする．このようにして，一般には通信・運営コストの面で不利と考えられる分散キャンパス環境を逆手に取り、分散バックアップシステムの構築を行った．

構成したバックアップシステムは，ほぼリアルタイムでファイルシステムのバックアップを他キャンパスに相互に配置するものである．同一学内であるためバックアップの際に暗号化等を行う必要もなく，ネットワークトラフィックを必要以上に増やすことがない．また，暗号化を行っていないため，すぐにシステムの再起動が可能となっている．

本論文は以下のように構成されている．2 章では震災時対応の問題点の分析について述べる。3 章では、幾つかの分散バックアップシステムの形態について比較・検討する．4 章で，本学が構築したバックアップシステムについて述べ、5 章で本システムが学内ネットワークに与える影響について分析・評価を行った．6 章はまとめである．

2　震災時対応と問題点の分析

2.1　対応の詳細

前述の通り，災害発生後に大学として早急に情報発信をすることが必要であったため，仮 Web を構築した．本 Web の URL でアクセスできるように DNS の設定を変更する必要があったが，本学の DNS サーバは停電のためまだ電源投入ができなかった．そこで仮 Web の A レコードを SINET の DNS に登録して頂くと同時に,「ibaraki.ac.jp」のネームサーバが SINET にあることを「jp」を管理している DNS サーバに登録して頂いた．これにより，仮 Web を本学の通常の URL で参照できるようになった．

震災の 3 日後，復電した日立キャンパスにおいて，倒壊の恐れがあるため立ち入り禁止となっていた IT 基盤センターのある建物の中で，火災の発生の怖れが無いことを確認の上サーバ室への通電が進められ，本 Web や DNS サーバの起動が行われた．まだ余震が続き，建物倒壊や再度停電が発生するかもしれない状況ではあったが，仮 Web から本 Web へ情報発信の拠点を戻すという決定がなされた．この決定を受け，SINET に向いていた DNS を本学の DNS に戻すとともに，VIOPS へ仮 Web の利用期限を申請した．これは DNS の TTL を考慮してものである．つまり，DNS のキャッシュサーバから仮 Web の登録が消失するまでは仮 Web のアドレスを答えてしまい，本 Web を閲覧できない可能性がある．

2.2 生じた問題

2.2.1 情報発信インタフェースの変更の問題

平常時以上に迅速できめ細かい情報発信が必要であったにもかかわらず，仮 Web における情報発信には困難を伴うこととなった．

本 Web 上のコンテンツは CMS 上に構築されていたため、コンテンツ管理者は平常時には CMS のインタフェースを利用してコンテンツの更新を行っていた．しかし仮 Web では本 Web と同じ環境を再現したわけではないため、同じ CMS は当然用意されておらず，情報を更新するには仮 Web 上のコンテンツを直接編集しなければならなかった．CMS によるコンテンツ管理に慣れていたコンテンツ管理者にとって，これは大変困難な状況であった．幸い、簡単な HTML を直に記述できる者を 2 名確保できたため，最低限の情報発信を行うことはできた．

2.2.2 DNS 切り替えに関する問題

前述の通り，仮 Web を実運用するにあたって SINET に DNS を依頼していた．本 Web を実運用に戻した段階で，本学 DNS の設定においてシリアル番号を新しいものと交換した．このことによりキャッシュサーバに蓄積されたデータは TTL に指定した 12 時間以内に順次置き換えられるはずであった．

しかし現実には，DNS の浸透問題により，遥かに長いほぼ 1 週間データが書き換えられなかった DNS があった．本学の Web サイトの参照のために同じ URL を指定しても，一方は本 Web をもう一方は仮 Web を見ているという状況が発生していた．スマートフォンの通信機能を利用し試したところ，高々40 分程度バスで移動しただけであるにもかかわらず接続するごとに仮 Web と本 Web が交互に表示されていた．

2.3 教訓

2.3.1 大規模なデータ消失を想定したバックアップ

被災前までは，小規模なデータの喪失に対する覚悟はあったものの，大規模なデータの喪失に関して切迫した危機感を皆持っていなかった．そのためバックアップも同一サーバ内あるいは同一サーバ室内の別のサーバにバックアップをとる程度であった．しかし建物倒壊が起こった場合は，これらのバックアップデータも同時に喪失してしまう．建物倒壊が現実味のある危険性として認識された今，喪失すると大学の運営が成り立たなくなるようなデータについても可用性を如何にして維持するかについて真剣に考えなければならない．

2.3.2 緊急時にも平常時と同じ環境が提供できること

震災時の大混乱の中，全く異なる環境で平常時以上の情報発信を行うことは非常な困難を伴う．平常時に利用する環境として，使い易い環境を提供し業務効率を高めておくことはもちろん重要である．しかしながら，日頃使い慣れた環境と同じ環境を，緊急時になってから改めてゼロから整えることは大変困難であるということを痛感した．特に緊急時の混乱の中では，同等の機能を持つがインタフェースは異なるツールでは意味がなく，ほとんど同じインタフェースを持つツールであることが重要である．すなわち，緊急時に平常時と同じ環境を如何に迅速に再構築するかよく検討しておく必要がある．

2.2.1 節で示した通り，Web コンテンツを構築するためのツールとしての CMS 等も，緊急時に異なる Web 上に異なる CMS しか用意できなかった場合は，コンテンツの作成作業も困難なものとなる．そのため，バックエンドの DBMS を含めた CMS が，緊急時にも提供できるような環境を提供できるようにする必要がある．

2.3.3 耐故障性のある DNS を構築すること

仮 Web のデータが TTL に指定したよりも遥かに長い時間残り続けた問題は，後日 DNS の浸透問題によって生じていたことが判明した．本 Web が本格稼働に入った際に，SINET における本学の DNS データを削除すれば，この問題を防ぐことができた可能性がある．

DNS に関しては，日頃より分散システムを意識し，耐故障性のあるシステムを目指すことが必要である．建物倒壊が起こった場合は，それまで運用していたサーバとは別の新サーバを稼働させるしかなく，その時に従来と連続性のあるサービスを提供するには DNS の速やかな切り替えが必須である．一つの方法として，当初から SINET のセカンダリ DNS サービスを受けていれば，本学の DNS サーバが復旧した時点で速やかに正しいデータに更新されたと思われる．

以上を総合すると，建物倒壊を想定した対策としては，緊急時に完全に新しいサーバの運用を開始することを想定し，平常時とまったく同じ環境を再構築するに必要十分なバックアップを，安全な場所に，かつ日常のシステム運用に大きな影響を及ぼすことなく取得する必要があることがわかる．

3 分散バックアップ

今回の震災のような大規模災害を考慮すると，バックアップの保管場所は，なるべく地理的に離れた場所に保管することが望ましいのは明らかである．選択肢としては以下の 3 つが考えられる．

1. 自組織内の別の場所に保管する,
2. 自組織外のデータセンタ等に保管する
3. 他組織と共同で互いに保管

以下では，それぞれのアプローチをとった場合の利点と欠点について検討する．

3.1 自組織内

自組織内でなるべく離れた建物にバックアップを保管する．キャンパスが一つであったり，複数でも余り離れていない場合には，今回のような広域災害に対しては無力であるが，地理的に大きく離れたキャンパスを有する場合には特に有効である．

自組織内でバックアップデータを保管することの利点としては，バックアップデータの取得, 移動, 保管において，自組織のネットワーク及びサーバで処理が完結することがあげられる．このことより，自組織の平常時の運用に影響を与えないようにバックアップや転送のスケジューリングを行うことが可能である．また，第三者がバックアップデータに触れる危険性がほとんどないため，第三者に対してデータの機密性を確保するための暗号化処理が必ずしも必要ではない．

ユーザデータよりはシステムの継続性に着目し OS イメージのバックアップを遠隔の自組織内に取り BCP 対策を行う場合 [3] も，自組織内であること及びバックアップ先でのシステムの起動を考慮し暗号化処理はされていない．

3.2 データセンタ

データセンタは通常耐震対策を行っているので，震災においてデータが喪失する危険性はほとんどない．

しかしデータセンタは通常自組織外にあるため，データセンタへのバックアップデータの保管のために，データセンタのネットワーク接続点にトラフィックが集中し，ボトルネックとなる恐れがある．またデータセンタの利用に当たっては，借用料等に加えて通信回線費が別途必要となる．

3.3 他組織と共同

東日本大震災以降，自組織のバックアップデータを他の組織と相互に保管しあうシステムを検討する大学が出てきている [1][2]．この方式では自組織全体が壊滅的な損害を受けたとしても，他組織に保管されたバックアップデータは損失を免れる可能性が高い．しかし同時に解決されなければならない問題点がいくつかある．

まず始めに，他組織が準備しなければならないストレージの容量が非常に大きくなることが予想される．重要なシステムのバックアップファイルは複数世代保管することが一般的であることを考えると，元データよりはるかに大きな容量が必要となるであろう．

次に，ネットワークトラフィックの観点からは，自組織とバックアップデータを保管する他組織の間のネットワークに，定期的にバックアップデータが流れることになる．システムのフルバックアップを送信する場合には大量のデータが瞬間的に送られることになるため，日常の他の通信に影響が出ないようにしなければならない．また，ファイルシステムのバックアップのように，前回のバックアップからの更新差分のみをバックアップするのが一般的である場合には，送信されるバックアップデータのサイズはフルバックアップに比べれば遥かに小さくなるものの，差分を求める頻度によっては日常業務の最中に定常的にバックアップデータの送信が行われることになる．いずれにしても複数の組織の間で，バックアップタイミングのスケジュール調整が必要となることは明らかである．

最後に，大学の運営にかかわるような重要なデータを他組織に保管する上で，暗号化は必須である．暗号化されていることにより，バックアップデータの差分を求める等の処理ができなくなるため，平文で保管する場合に比べると効率はどうしても悪くなる．暗号化されたデータのサイズは，基本的に元となるバックアップデータのサイズと同じである．複数拠点に分散してバックアップデータを配置する場合には，秘密分散法の利用等により，一拠点あたりのデータサーズを元データより小さくすることこは可能である．平文で保管する場合に比べて必要となる容量の点では大きな問題はないが，暗号化や復号の処理のための計算機資源を必要とすることには注意しなければならない．

4 茨城大学でのバックアップシステム

4.1 計算機システム及びネットワークの概要

まず始めに，分散バックアップシステムを導入する本学のキャンパスの地理的な関係及びキャンパスネットワークとサーバの構成を整理する．

本学は図 1 に示した通り大キャンパスが日立, 水戸, 阿見の 3 地区にある．キャンパス間の距離は日立-水戸間が約 30km, 水戸-阿見間が約 50km である．今回の震災では，冒頭にも述べたように各キャンパスでの震度の差があり，被害状況にも有意な差があった．同様の地震に見舞われても，万一にも 2 つ以上のキャンパスが同時に壊滅するとは考えにくい．そこで本学においては，

自組織内の他のキャンパスにバックアップを置くことは震災を考慮しても有効であると思われる．

本学の計算機システムやネットワークシステムを管理する IT 基盤センターは日立キャンパスにあるため，本学のネットワークとしての入り口は日立キャンパスとなっている (図 2)．このため，ファイアウォール等は日立キャンパスに設置されている．また，本学では SINET の共同調達に当初から参加している．各キャンパスの入り口に L3 スイッチを配置し広域イーサネットを利用して通信帯域 1Gbps で接続しているため，キャンパス間ネットワークはスター型となっている．附属学校 3 校や 3 研究センターは，通信帯域は 100Mbps ではあるが同じ広域イーサネット経由で接続している．

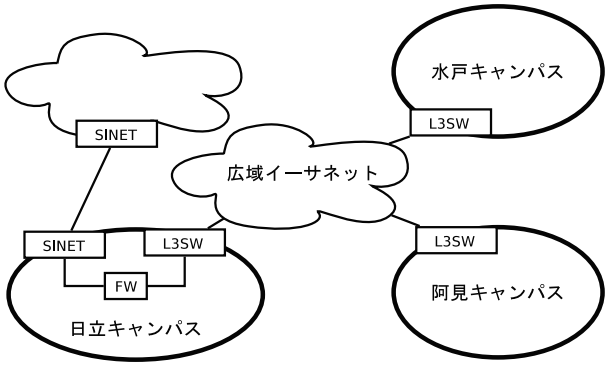


図- 2: キャンパス間ネットワーク

本学には 5 学部があり 1 年次生のほとんどは水戸キャンパスで修学しているが，工学部と農学部の 2 年次以降はそれぞれ日立, 阿見キャンパスにおいて修学している．

各キャンパスに学生用のサーバ (以下,「キャンパスサーバ」と略) を配置し，電子メールはもちろん演習用に学内に限った Web 頁の構築演習を行っている．1 年から 2 年に進級した際に，電子メールアドレスや作成した Web 頁の URL が変わってしまうのは，不要な混乱を招くだけと思われることから，アカウントは卒業までに一番長く修学するキャンパスのキャンパスサーバ上に入学と同時に発行している．つまり，工学部及び農学部学生用のキャンパスサーバはそれぞれ日立及び阿見キャンパスにあり，1 年次からそれを利用する．

次にバックアップの対象となるデータについて述べる．キャンパスサーバ上の各ユーザのデータは，ホームディレクトリに保管される．電子メールもホームディレクトリ配下に Maildir 形式で保存されるため，基本的にはユーザデータのバックアップはホームディレクトリのみを対象とすればよい．

茨城県は雷の発生等も多く，その影響で停電することも稀ではない．キャンパスが離れているため停電は基本的にキャンパス毎である．PC へのログインやネットワーク利用等における認証等が他キャンパスの停電によって影響されないよう，認証サーバ等は各キャンパスに設置してある．教職員が学内外へ情報提供するために Web を利用する基盤としての仮想サーバの提供も行っており，本学としての Web サーバも仮想サーバとして提供している．更に，仮想サーバのバックエンドとなる DBMS も複数用意している．

また，本学のネットワークとしての入り口が日立キャンパスであるため，上述の仮想サーバを含む主要サーバも日立キャンパスに設置されている．

平成 24 年 3 月に教育用計算機及びネットワークシステムのリプレースを行った．基本的にはこれまでのシステム構成は変更していないが，サーバのほとんどを VMware 上の仮想機械とした．更にディスクシステムも仮想化に対応するため，前システムでは各主要サーバ毎に用意していた NetAppp 社のディスクを，各キャンパスに 1 台ずつの EMC 社の VNX5300 に変更した．ディスクの大容量化により，各ユーザのホームディレクトリ以下の容量を表 1 に示した通りに増やすことが可能となった．

表- 1: ユーザのディスク容量

種別	容量 (前)	容量 (現)
教職員	250MB	3GB
学生	120MB	1GB

また，平成 24 年度末に全学的に無線 LAN 環境を整備し，アクセスポイント 320 台を各建屋の各階に 1 台以上配置した．無線 LAN システムは Aruba 社製のコントローラタイプのものであるため，他のシステムと同様に停電等を考慮し各キャンパスにコントローラを設置し，それぞれをキャンパス間接続用 L3 スイッチに直結している．

4.2 分散バックアップシステム

本学におけるバックアップの対象は，主に学生演習等による成果物や電子メールデータである．いわゆるネットショッピングにおけるトランザクションデータの様なクリティカルなデータではないが，大量のデータ量が対象となる．現時点での総データ量はリプレース直後ということもあり 2.5T バイト程度であるが，将来的にはその 10 倍程度になると見込まれる．

システムリプレースの際，各キャンパスに設置したディスクシステムを論理的に分割し，次の 4 つに分類した．

0. 実データ
1. 実データのバックアップ
2. 他キャンパスのバックアップ

3. 他システムのバックアップ

項番 1 はディスクシステムの耐故障性を通常の冗長化で向上させるためのもので，項番 2 は他キャンパスのデータのバックアップを保管するためのものである．項番 1 のバックアップは，EMC VNX5300 の機能を利用し，実データに変更があった際にはリアルタイムで反映される．

他のキャンパスへ保管する項番 2 のバックアップに関しても，EMC VNX5300 の機能を利用し 10 分間隔で変更が反映される．電子メールや受講学生の成果物という観点からは，本研究で実現したような短い間隔でのバックアップが必要と思われる．震災時に同時に 2 つのキャンパスで建物倒壊等の被害はないと考えているため，このバックアップは他の 1 つのキャンパスのみとした．

項番 3 は，別途購入した学内システムのバックアップデータを保管するための領域である．

工学部及び農学部の 1 年生のデータはそれぞれ日立及び阿見キャンパスにあるため，日常的に異なるキャンパス間の通信が発生している．例えば，水戸キャンパスにいる農学部 1 年生がホームディレクトリのファイルを更新すると，図 3 に示すようにデータを書き込む際に水戸-阿見間の通信が発生し，更にそのデータのバックアップを取るために阿見-日立間の通信が発生することになる．電子メールに関しても，同様の通信が発生することになる．

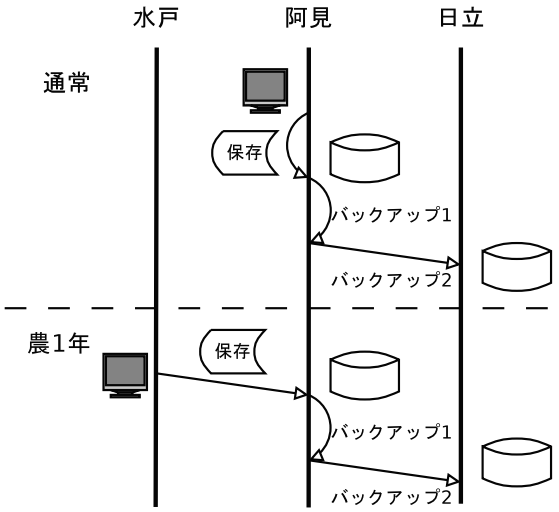


図- 3: 保存したファイルのバックアップ

なお，キャンパス間のバックアップについては暗号化処理を行っていない．これは次の理由からである．

1. バックアップを作成するシステムも保管するシステムも共に IT 基盤センターの管轄下にあるため
2. 平常時のバックアップ作成負荷を低く抑えるため
3. 緊急時の復旧作業を簡素にしておくため

また，圧縮も行っていないため，バックアップのデータはそのまま実データとして利用することができる．例えば，dump コマンドを用いた差分バックアップのような場合には，実データとしてそのまま利用できず，データの復元の際にマスタに差分を当てていく作業及びそのためのディスクが必要となってしまう．

また，将来的には総データ量は 25T バイト程度までを想定しているが，バックアップの際の送信対象は差分であるため，総データ量が現時点での 10 倍になったとしてもトラフィックはそれ程増加しないと考えられる．dump コマンドを用いた差分バックアップの場合のようにマスタとして全てを送る必要がある場合は，その都度総データを送信する必要が生じてしまう．

本学が採用した方式では，仮にいずれかのキャンパスにおいて建物倒壊等でシステムが利用できなくなった際も，そのシステムのイメージを VMware 上で動かした後にバックアップをマウントするだけで容易にシステムを再現することができる．

更に本学では，ユーザデータだけではなく，2.3.2 節にも示した通り，Web の CMS 及びバックエンドの DBMS も対象としている．これにより，建物倒壊が起こったとしても，Web サーバはもちろん CMS 環境の提供も可能となっている．

4.3 セカンダリ DNS

建物倒壊を免れた他キャンパスに新サーバを復旧させた場合，DNS の迅速な切り替えが必須である．これまでは DNS はプライマリ及びセカンダリともに本学内に設置していたが，前述のように DNS の浸透問題が発生した．

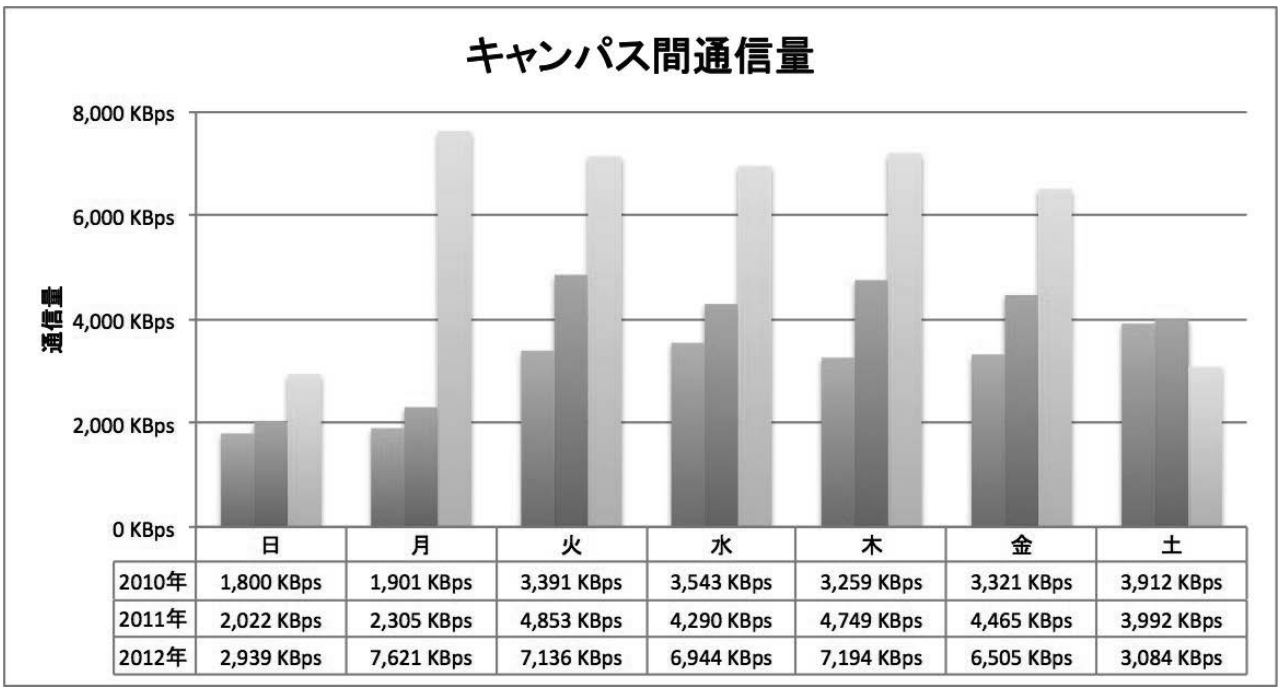
そこで被災時にも速やかに DNS のデータを更新できるように，SINET の提供するセカンダリ DNS サービスを利用することにした．災害時に本学の DNS サーバが被災しても，本学のデータを持つ DNS サーバをあわてて構築する必要がなくなっただけでなく，本学の DNS サーバが復旧した際にも DNS の浸透問題が発生しないことが保証されることになった．

5 分析及び評価

5.1 トラフィックへの影響

まず始めに，本分散バックアップシステムによってキャンパス間ネットワークのトラフィックにどの程度の影響を与えているかを調査した．

本システムでバックアップの対象となっているのは，全ユーザのホームディレクトリ以下のデータ, Web の仮想ホストのデータ及び DBMS のデータ等計算機システ



	日	月	火	水	木	金	土
2010年	1,800 KBps	1,901 KBps	3,391 KBps	3,543 KBps	3,259 KBps	3,321 KBps	3,912 KBps
2011年	2,022 KBps	2,305 KBps	4,853 KBps	4,290 KBps	4,749 KBps	4,465 KBps	3,992 KBps
2012年	2,939 KBps	7,621 KBps	7,136 KBps	6,944 KBps	7,194 KBps	6,505 KBps	3,084 KBps

図- 4: 3 年間のトラフィックの比較

ム上のユーザデータの全てである．システムリプレース直後のため，現時点での対象となるデータ量は 2.5T バイト程度である．比較を行ったのは，現在のシステムの運用が安定してきた 6 月の 2 週間分と過去 2 年間 MRTG で計測していたトラフィックデータである．曜日毎に平均を取ったものを，図 4 に示す．

一見してわかるように月曜日および土曜日が特異である．月曜日および土曜日の特異な傾向の変化は，本学のカリキュラム上の変化によるものであることがわかっている．

月曜日に関しては，本年度より PC を利用する講義が増えたという事情がありトラフィックが増大したものである．昨年度より工学部及び農学部学生に対する教養科目「情報処理概論」が，2 年次開講から 1 年次開講へと移行している．年次進行のために 1, 2 年生の両方に対して講義を開講する必要が生じたため，PC を利用する講義数が一時的に増加することとなったが，この増加分がこれまで PC を利用する講義の少なかった月曜日に集中して開講されるようになった．1 年生の PC 利用が増えると，キャンパス間の通信が増えることは 4 章でも述べた通りである．

一方，土曜日の通信が少なく見えるのは，むしろ 2010 年と 2011 年の通信が多かったことが原因である．2010 年は建物改修, 2011 年には震災の影響等で，一部の学部で土曜日に平日と同じ様に開講しており，その通信が発生していた．今年度は土曜日の開講がなくなったためトラフィックが減少した様に見える．

月曜日と土曜日を除くと，それ以外の平日は同様の傾向を示しており，2012 年は 2011 年の約 1.5 倍程度のトラフィックになっている．

トラフィック増加の要因としては，本バックアップシステム以外に，2012 年 3 月に整備した無線 LAN システムがある．昨年度までは研究室で設置された無線 LAN しかなかったため，学生は研究室に配属されるまで無線 LAN をほとんど利用することがなかった．今年度からは学内のほぼ至る所で無線 LAN が利用できるようになったことにより，現在では，毎日最大 500 デバイス程度が同時に接続されるようになっている．1 年生でも PC やスマートフォンを無線 LAN に接続する利用者は確実に増え続けている．

来年度以降「情報処理概論」の重複開講が解消されたとしても無線 LAN の利用等でトラフィックが増え続けて行くことは間違いない．しかし，現在の広域イーサネットへの契約帯域が 1Gbps であることから，本学としては現時点では余裕のある通信量であるということができる．これにより，キャンパス間ネットワークに支障を与えず，バックアップシステムが安定して運用できていると思われる．

5.2 バックアップデータの形式

次に，バックアップデータの形式について検討する．

前述のように，本システムではデータの圧縮や暗号化等をしておらず，実データと同じ状態で保存している．このため，停止したシステムを VMware 上で動かしバックアップをマウントするだけで容易にシステムを

再現することができる．災害からの復旧時に，複雑な処理をすること無しにシステムを容易に再現できるのはきわめて重要な条件と思われる．

バックアップデータを暗号化して保存する場合，共有鍵暗号方式であればデータ量は暗号化前のものと同じことも考えられる．しかし，本研究の方式と同じく差分データをバックアップした場合は，復元の際に各差分を復号し，基本となる全データへ差分を適用する必要がある．これには多大な手間が必要となる．更に，差分の適用回数を減らすためには，ある一定期間毎に基本となる全データをバックアップ先へ送る必要が生じる．仮に全データを 2.5T バイトとすると，1Gbps の通信帯域を専用に利用できたと仮定しても約 5.6 時間要する．これは本学にとっては現実的とは考えられず，ネットワークではなく別の手段を考える必要がある．もしくは，災害時に提供しなければならない Web コンテンツ及び CMS 関連のデータ等の必要最小限のデータに限ってバックアップを考えなければならない．

西村らの方法は，データの広域分散配置により東日本大震災よりもより甚大な災害にも堪えうる有用な方法であると筆者らも着目しているが，前段落で言及した通り本手法はキャンパスが地理的に分散している状況でのみ実現可能であるがゆえに，差分の適用の問題及び基本となる全データの送信問題を生じないものとなっている．更に，全データに関しては，分散した拠点数分の送信が必要となり，実現のためにはより広帯域が必要となる．もしくは，前段落で言及した通り，必要最小限のデータに限ってバックアップを考えなければならない．

6　まとめと今後の課題

東日本大震災で得られた教訓を基に，平常時には様々な面で不利と思われてきた分散キャンパスという立地を逆手に取って，分散バックアップシステムを構築することができた．本研究で実現したシステムでは，ユーザデータの全てに関して他キャンパスにバックアップを取っているが，そのための通信量は現時点での利用に影響の出るものではない．

バックアップデータは実データと同じ形式であるため，新しいサーバを稼働させた際にバックアップデータをそのままマウントすることができ，比較的容易にシステムの再構築が可能なシステムとなっている．

また，バックアップデータは学内に配置されるため，データのセキュリティを確保し易いという利点もある．

以上から，効率の良く安全で復旧が容易なバックアップシステムを構築することができた．これにより，建物倒壊の被害に遭遇しても，他のキャンパスで容易に再稼働することが可能となった．

分散キャンパスを有する大学は，基盤設備のキャンパス毎の調達やキャンパス間通信回線のコストが固定費となって常に苦しんできた．本報告では，固定費の範囲内でキャンパス間での分散バックアップが可能となった一例を報告した．また，単一キャンパスからなる大学では，データセンタとの間の通信回線コストが新規に必要となるが，遠隔地の信頼できるデータセンタを利用すれば同様のシステムを構築することが可能である．

今後の課題として，次の 2 つを考えている．第 1 の課題は，現在バックアップの間隔を 10 分としているが，その間隔を変えた際にどの様にネットワークへ影響が生じるかの調査である．第 2 の課題は，現在は，他キャンパスへのバックアップの対象を教育用計算機のデータのみに限っているが，他のシステムのバックアップを受け入れることで大学としての BCP に貢献していくことである．その際にも第 1 の課題に示したバックアップの間隔を変更して，システムの評価を行いたいと考えている．

参考文献

[1] 西村浩二: 電子情報の大学間相互保持に向けた遠隔バックアップ技術の研究, 学際大規模情報基盤共同利用・共同研究拠点 第 2 回シンポジウム 講演予稿 2011 年 1 月

[2] 熊谷悠平 他: 認証フェデレーションに基づく分散ファイル管理システムの提案, 情報処理学会 インターネットと運用技術研究会, Vol.2012-IOT-18 No.8, 2012 年 6 月

[3] 岩井真依 他: BCP 対策に向けたサービス無停止バックアップの実証実験, 情報処理学会 インターネットと運用技術研究会, Vol.2012-IOT-17 No.21, 2012 年 5 月

[4] 鈴木 宏康: cloudpack における AWS による DR, http://www.cloudpack.jp/topics/20110630.html, 技術評論社「G-CLOUD Magazine 2011 Summer」, 2011

[5] 茨城大学様からの御礼状のご紹介, http://www.viops.jp/2011/03/post-12.html, 2011 年 3 月

[6] 森下泰宏, 民田雅人: DNS 浸透の都市伝説を斬る ～ ランチのおともに DNS～, http://jprs.jp/tech/material/iw2011-lunch-L1-01.pdf, Internet Week 2011

ADFS による学術認証フェデレーション対応 SharePoint サービスの構築

Development of SharePoint Service for Gakunin by using ADFS

伊藤智博[†,††]，立花和宏[†]，奥山澄雄[†]，高野勝美[†,††]，田島靖久[‡,††]，吉田浩司[‡,††]
Tomohiro Ito[†,††], Kazuhiro Tachibana[†], Sumio Okuyama[†], Katsumi Takano[†,††],
Yasuhisa Tajima[‡,††]，Hiroshi Yoshida[‡,††]
tomohiro_ito@ieee.org, h9rbvq3x@yz.yamagata-u.ac.jp, sumio@ieee.org, ktakano@ieee.org,
tajima@sci.kj.yamagata-u.ac.jp, yoshida@ncsc.yamagata-u.ac.jp

† 山形大学大学院理工学研究科
‡ 山形大学基盤教育院
† ‡ 山形大学情報ネットワークセンター
992-8510 米沢市城南 4-3-16

† Graduate School of Science and Engineering, Yamagata University,
‡ Institute of Arts and Sciences, Yamagata University
† ‡ Networking and Computing Service Center, Yamagata University
4-3-16 Johnan, Yonezawa 992-8510 Japan

概要

山形大学で行われた SharePoint サービスを学術認証フェデレーションに提供するための様々な試みについて報告する．SharePoint の個人識別子について定め，mail 属性(OID: 0.9.2342.19200300.100.1.3)を採用した SharePoint サービスと学認で採用されているシボレスは直接認証連携が技術的にできないため，Active Directory Federation Service (ADFS)を経由して, SharePoint と ADFS を WS-Federation 連携することで解決した．また，ADFS は，学認のメタデータを直接読み込むことができないため，データベースサーバとメタデータ変換用ウェブサーバを組み合わることでメタデータの構造を自動変換することで解決した．これらの開発によって，学認に SharePoint Foundation サービスを提供することができた．

キーワード

SharePoint, Active Directory Federation Service，シボレス認証，WIF， XML，学認

1. はじめに

山形大学では，従来，各部局や部署が，システム毎に独自のアカウントを発行して，システムを構築・運用していた．2003 年の時点では，情報系センター（当時の情報処理センター；以下センター）のアカウントですら，UNIX 系と Windows 系で独立しており，パスワードの取り扱いが複雑になる問題が生じていた．また，山形大学は，4 つからなる分散キャンパスであるため，運用方針についても，キャンパス毎に異なる要望があり，その要望に応えるため，様々な運用形態が生まれ複雑化していた．2004 年度より，工学部が設置されている米沢キャンパスのセンターが中心になって，認証統合の技術的な解決策と試行運用が開始された．検証課題として，「デジタル証明書」，「UNIX 系と Windows 系のパスワード同期」，「ネットワーク装置からの Active Directory(AD)への認証」，「オブジェクト識別子(OID)の設計」，「複数認証基盤の連携」を掲げ，それぞれの課題の技術面及び運用面での解決が試みられた. 2005 年には, 全ての課題について, 問題解決がなされ，工学部の利用者は，センターが提供するリソースに対して，1 つのアカウントで全てのサービスが提供できるようになった．その後，80 番ポートを介在して増殖するワームの対策の 1 つとして，工学部では，外部接続時にネットワーク利用者認証を必須とする運用方針が適用され、アカウントの利用者数は，米沢キャンパスのネットワーク利用者数である約 4000 人へと増加した．また，2007 年に実施した教育用実習システムの更新では，全てのキャンパスに米沢キャンパスと同様の統合認証を導入した．これによって，センターが提供する全てのサービスがシングルサインオンで提供できるようになった．

教務システムや会計システムなどの業務系のシステムとの認証の統合については，様々な議論の結果，センターが中心となって運用している学術系の認証情報とは統合しないという結論に至った. 議論の内容を要約すると, 教育・研究現場では, 学問の自由が許されている. 一方, 業務システムでは，堅牢なセキュリティシステムが必要とされる. この 2 つのポリシーは、互いに相反するため, その両方を同一の認証基盤で円滑に運用することは，困難であると判断した．すなわち，山形大学では，センターが管理・提供する「教育研究用認証基盤」と事務が中心となって管理・提供する「業務系認証基盤」のセキュリティレベルが異なる 2 つのアカウントが存在する．

2006 年度から，国立情報学研究所(NII)及び全学共同利用情報基盤センターが中心となり，全国大学共同電子認証基盤構築事業（UPKI : University Public Key Infrastructure）を 3 年計画で実施した[1]．この事業では，各大学にある計算機資源や情報インフラなどを大学間で，シームレスかつ安全に活用すること目的して，「デジタル証明書」，「グリッドコンピューティング」，「証明局」，「シングルサインオン」，「無線 LAN ローミング」を中心に認証基盤のプロトタイプ試験を実施した．

2008 年度には，UPKI 認証連携基盤実現のために技術的及び制度的な検証を行うために，「UPKI 認証連携基盤によるシングルサインオン実証実験（SSO 実証実験）が実施された．山形大学では，分散キャンパスで円滑に認証連携を進めるための技術的なノウハウを蓄積することを 1 つの目的として，LDAP プロキシや Radius プロキシによる複数認証基盤を統合し，SSO 実証実験及び大学間無線 LAN ローミング eduroam (eduroam)に参加した[2,3]. 2009 年には，UPKI-学術認証フェデレーションの試行運用フェデレーション（現在の学術認証フェデレーション；以下学認）に参加し，本格的な利用者サービスを開始した[4]．Shibboleth (シボレス)認証は，東日本大震災が発生した際に，本学の安否確認システムを 6 時間程度で構築できることから，開発コストを軽減できるツールの１つであった[5]. 2011 年には, 東日本大震災を踏まえて, 複数 ISP と分散データベースによる高可用性認証連携システムを構築し，学認をはじめとする様々なフェデレーションとの認証連携機能の可用性を向上した[6,7].

本学では，学内の利用者向けにグループボードワークスペースによるグループウェアサービスを展開している. 本学の研究者から，卒業生や学外の研究者との情報を共有できるグループウェアを提供してほしいとの要望があった．学外研究者とのコラボレーションツール提供の要望に応えるためには，グループウェアを学認に対応することが有効であると考えられる．本報告では，山形大学で構築した ADFS による学認対応 SharePoint サービスの構築について述べる．

2. 設計と使用した情報機器

2.1. ポリシー設計

SharePoint サービスを利用するためには，個人を識別するための個人識別子を使うことが必須になっている．すなわち，AD や学認から個人識別子がない場合は，利用することができない仕組みになっている．AD を認証基盤としてサービスを展開する場合は，ユーザログオン名(ドメイン¥ユーザ名)によって個人を特定し, SharePoint サービス内のメンバー登録に利用することができる．また，AD を利用する場合，AD の認証基盤を検索することも可能なため，サイトの管理者側の登録作業の負担も軽

減される．一方，学認で展開した場合，管理者が容易に利用者登録できる個人識別子を選択する必要がある．そこで，学認で定めている属性一覧から個人識別子を検討した結果，次に示す2つの属性名が適当であると考えられる [8].

・ePPN (OID:1.3.6.1.4.1.5923.1.1.1.6)
・mail (OID:0.9.2342.19200300.100.1.3)

これらの2つを比較したところ，ePPN 属性は学認内で一意性を保証しており，個人を識別することは容易である．しかし，各大学の諸事情などから，属性値から個人を直接推測できないように，ハッシュなどの不可逆暗号を行っている場合がある[9]．そのため，SharePoint サービスの管理者は，利用者から属性値を聞き出すなどの手順が必要になり，サイトを運用する上で，管理者への負担が大きい．一方，mail 属性は，一意性を保証するものではないが，個人を特定することが可能であるため，管理者の運用コストは軽減できる．特に，SharePoint Foundation サービスは，グループ内のワークスペースやスケジュール管理，ドキュメント共有を目的としているため，個人を特定して権限を付与することが必要不可欠である．このような背景のもと，SharePoint サービスで利用する個人識別子は, mail 属性を利用することにした.

SharePoint サービスは，グループに権限を付与することもできる．学認内で，グループ属性になり得る属性名としては，ePSA(OID: 1.3.6.1.4.1.5923.1.1.1.9)であった[8]. この属性を SharePoint のグループへの権限付与に使うことによって，特定の大学に所属する特定の職位の人に，権限を付与できる．例えば，山形大学の構成員に，SharePoint 内の特定サイトに読み込み権限を付与することができるようになる．もし，このようなグループ属性による管理機能がない場合，一人一人の mail アドレスをサイト利用者として登録するため，サイト管理者の負担が増大する．すなわち，グループ識別子による利用者登録が可能であることにより, 利便性の向上が期待される.

以上を踏まえて，SharePoint サービスの運用ポリシーをまとめると，

・個人識別子には，mail 属性
・グループ識別子には，ePSA 属性

を利用することにした.

2.2. 構築上の問題点とシステムの概要

SharePoint サービスを学認に対応するためには, 2つの大きな問題点を解決する必要がある．1つ目の問題点は，SharePoint サービスが提供する Security Assertion Markup Language (SAML)ベースの認証方式であるクレームベース認証は，学認が推奨するシボレスと直接連携が難しいことである．2 つ目の問題点は，Active Directory Federation Service (ADFS)は，学認が提供するような複数の認証プロバイダ(IdP)やサービスプロバイダ(SP)の信頼情報を1つのファイルに集約したメタデータを直接読み込めないことである. この2つの問題を解決するために，図 1 に示すようなシステムを構築した．1 つ目の問題点は，ADFS サーバがシボレス IdP からの SAML アサーションを WS-Federation 用の SAML アサーションに変換する認証ゲートウェイのような機能を利用することで解決した．2 つ目の問題点は，学認が提供するメタデータを読み込み解析するウェブクローラーモジュールを開発し，ADFS に対応したメタデータに変換し，読み込ませることで解決した.

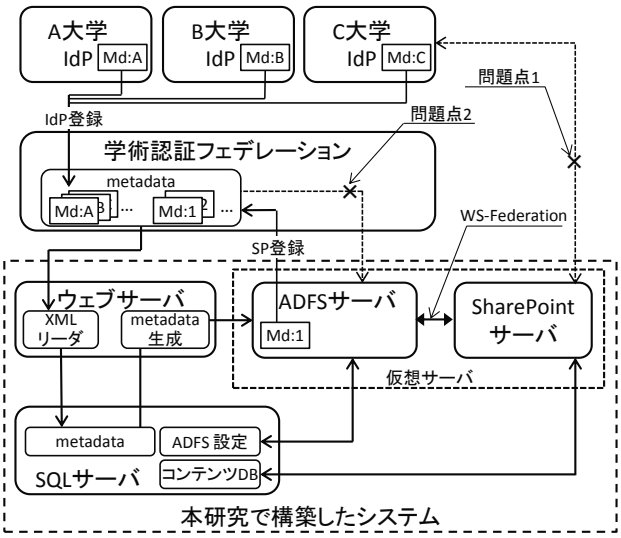


図 1. 学認対応 SharePoint サービスの概略

2.3. 各サーバのスペック

サービスの実運用において，ADFS サーバ，SharePoint サーバ，SQL サーバ，メタデータ変換用メタデータ変換用ウェブサーバを使用した. 学内の認証基盤は, Windows Server 2008 上の AD サービスによって提供されている．仮想サーバは，ADFS サーバ，SharePoint サーバをはじめとする 25 のゲストマシーンが動作している．今後，新しいサービスを展開することを想定し，40 程度のゲストマシーンを動作できるように設計した．SQL サーバは，研究やログの解析にも利用されおり，現在，約 1500 万件／日のトランザクションを処理している．導入時に，2 億件／日のトランザクションを処理できるように設計した．以下に，それぞれのサーバのスペックを示す.

[仮想サーバ]
CPU: AMD Opteron 6180SE 2.5GHz ×4
メモリ: 128 GB
ローカル HDD: 1.8 TB
共有 HDD: 10 TB
OS: VMware vSphere 5.0 Enterprise Plus
備考：冗長性を保つために，複数の物理サーバで構成

[ADFS サーバ]
CPU:2 (仮想サーバ上で動作)
メモリ：4GB
HDD: 90 GB
OS: Microsoft Windows Server 2008 R2 Enterprise Edition
アプリケーション：ADFS 2.0, Visual Studio 2008 Professional

[SharePoint サーバ]
CPU:2 (仮想サーバ上で動作)
メモリ: 4GB
HDD: 128 GB
OS: Microsoft Windows Server 2008 R2 Standard Edition
アプリケーション：SharePoint Foundation Server 2010

[SQL サーバ]
CPU: AMD Opteron 6282SE 2.6GHz ×2
メモリ：64GB
HDD: 3.6TB (900GB×8, RAID 6)
OS: Microsoft Windows Server 2008 R2 Enterprise Edition
アプリケーション： Microsoft SQL Server 2008 R2 Enterprise Edition

[メタデータ変換用ウェブサーバ]
CPU: Intel Pentium E2160 1.8GHz ×1
メモリ：4GB
HDD: 1.0TB (1TB×2, RAID 1)
OS: Microsoft Windows Server 2003 Standard Edition
アプリケーション： Visual Studio 2005 Professional

[クライアント PC]
CPU: Intel Core　i7 M620×1
メモリ：8GB
HDD: 128GB
OS: Microsoft Windows 7 Professional
アプリケーション： Internet Explorer 9, Firefox 13.0

3. 各機能モジュールの構築と総合評価

SharePoint サービスを学認に対応するためには，シボレス IdP は直接認証連携できない問題を解決することが必要不可欠である．本節では SharePoint サービスを学認に対応するために開発したモジュールと総合的な動作確認について述べる．

3.1. 学認メタデータ読み取りモジュール

ADFS に学認のメタデータを対応するためは，複数の IdP が一塊になっている XML ファイルをエンティティごとに分割し，ADFS に登録する必要がある．そこで，図 2 に示すような学認のメタデータを自動的に読み込み，エンティティごとに分割し，SQL サーバに登録するモジュールを開発した．

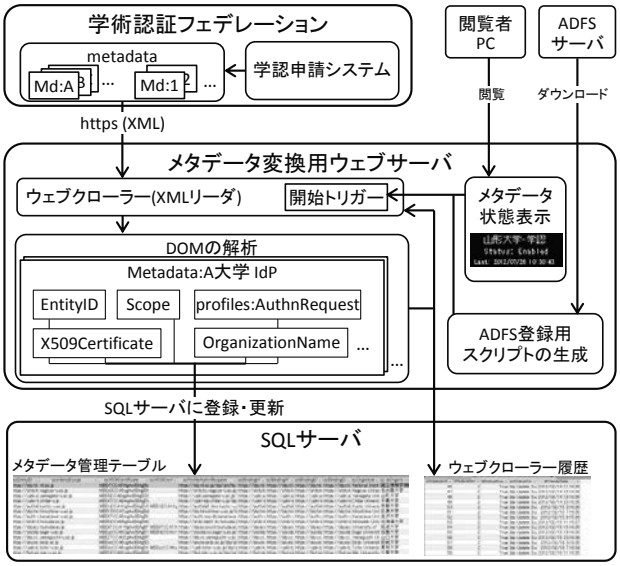


図 2. 学認メタデータ読み取りモジュールの概略

具体的には，メタデータ変換用ウェブサーバ内にウェブクローラーモジュールを開発した. このモジュールは，開始トリガーによって実行され，SQL サーバに記録されているウェブクローラー履歴を閲覧し，最後に，学認のメタデータの読み込みおよび SQL サーバへの登録・更新が成功した最終更新日時を得る．最終更新日時と現在の日時の差が 4 時間以上ある場合，学認のメタデータを https プロトコル経由で，読み込み，ドキュメントオブジェクトモジュール（DOM）の解析プログラムに学認のメタデータを受け渡す．DOM 解析プログラムは，受け取ったメタデータをエンティティごとに分割する. さらに，それぞれのエンティティの XML を解析し，要素や属性値に抽出する．それぞれの要素の属性値は，SQL サーバ内のメタデータ管理テーブルと照合され，登録または更

新の処理が行われる. すべてのエンティティを SQL サーバに登録・更新処理が完了した場合，ウェブクローラー履歴テーブルに，処理完了の履歴が記録される.

ウェブクローラーモジュールがクロールを開始するトリガーは，メタデータ変換用ウェブサーバ内の特定のアクティブサーバページに http 接続にしたときに有効になるようにした．具体的な特定ページとは，メタデータの更新状態をアイコン画像として表示するページと後述する ADFS サーバが IdP を登録するときに使用する ADFS 登録用スクリプト生成ページの 2 つである．ウェブページをトリガーにしたことによって，外部サーバとの連携が容易にできるようになっている.

3.2. ADFS の学認 IdP の自動管理

ADFS では，シボレスのようにメタデータを一括で読み込むことができない．通常は，GUI の管理ツールやコマンドラインから，手動で登録する．学認のメタデータには，2012 年 6 月の時点で 41 機関が IdP 登録されており，今後も増えることが予想される．サービス継続性を考慮すると，学認に登録された IdP を自動的に管理することによって，運用コストを軽減することが必要不可欠である．この問題を解決するために，図 3 に示すような SQL サーバと連携した ADFS への自動管理モジュールを構築した.

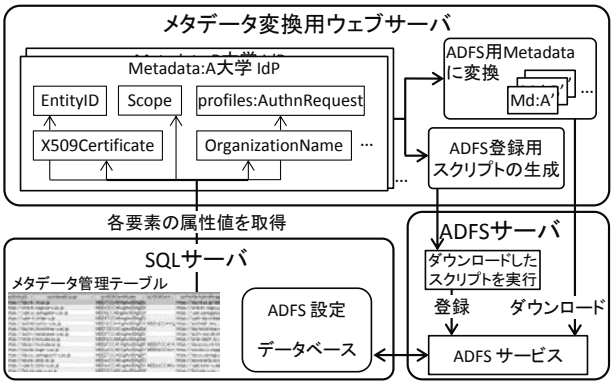


図 3. ADFS 用メタデータ自動管理システムの概略

具体的には，SQL サーバ内のメタデータ管理テーブルを参照し，表 1 の 1 に示すような ADFS に IdP 登録するためのスクリプトを自動生成する．スクリプトの 1 行目に記述されたコマンドによって，ADFS を管理するためのモジュールを読み込み初期化した．次に，2 行目に記述されたコマンドにより，ADFS の要求プロバイダ (Claims Provider Trust)に追加登録され，スクリプトに記述された Metadata URL から，ADFS 用に変換されたメタデータを読み込まれる．ADFS は，メタデータを解析し，種々の要素に関する属性値を取得し，登録する．シボレス IdP と ADFS とでは，セキュアハッシュアルゴリズムの既定値が異なるため，正常に SAML アサーションを送受信できない．この問題は，ADFS のセキュアハッシュアルゴリズムを SHA-1 に設定することで解決した. シボレス IdP から送信された SAML アサーションを ADFS が受け取るためには，要素 ID を表 2 示すように再定義する必要がある．3 行目のコマンドは，変換規則を記述した設定ファイルを読み込むことにより，ADFS に変換規則を定義した．また，2 行目と 3 行目のコマンドを繰り返すことによって，複数の IdP を登録・変換規則の定義を行うスクリプトを動的に生成するようにしている.

次に，スクリプトのダウンロードおよびスクリプトを起動するために，表 1 の 2 に示すようなコマンドを実行した．このコマンドは，前述したスクリプトをメタデータ変換用ウェブサーバからダウンロードし，パイプを経由して，PowerShell プログラムに渡し，スクリプトが実行されるようになっている. タスクなどの機能を使って，定期的に実行することで, 学認に IdP が追加されたとき，自動的に追加できるようにした．また，ADFS の設定情報は，SQL サーバに記録するように設定し，可用性や拡張性を高めている.

表 2　ADFS 内に設定した要素名の変換規則

シボレスの要素名	ADFS 側の要素名
mail[1)]	電子メールアドレス[2)]
ePSA[3)]	役割(Role)[4)]

それぞれの SAML の要素の ID は，'urn:oid:0.9.2342.19200300.100.1.3'(1) ; 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' (2) ; 'urn:oid:1.3.6.1.4.1.5923.1.1.1.9' (3) ; 'http://schemas.microsoft.com/ws/2008/06/identity/claims/role' (4) である.

表 1 ADFS の IdP 登録用スクリプトの例と登録スクリプトのダウンロードおよび実行コマンド

1.　ADFS 登録用スクリプトの例	1 行目: Add-PSSnapin Microsoft.Adfs.PowerShell 2 行目: Add-ADFSClaimsProviderTrust -Name '学認／National Institute of Informatics' -MetadataURL 'https://a.yamagata-u.ac.jp/amenity/network/AdfsIdPMetadataXml.aspx?IdPID=151' -AutoUpdateEnabled 1 -MonitoringEnabled 1　-SignatureAlgorithm 'http://www.w3.org/2000/09/xmldsig#rsa-sha1' 3:行目：Set-ADFSClaimsProviderTrust -TargetName '学認／National Institute of Informatics' -AcceptanceTransformRulesFile 'C:¥Gakunin-adfs¥Gakunin-IDP-to-ADFS.tpl' ・・・
2. ダウンロードおよび実行コマンド	wget http://a.yamagata-u.ac.jp/amenity/network/AdfsIdPAddPSCommand.aspx?FederationID=2 -O - | powershell -File -

3.3. SharePoint サーバのクレーム認証の設定

SharePoint サーバの認証に，シボレス認証を利用するためには，ADFS の認証ゲートウェイ利用することが必要である．そこで，SharePoint サーバのクレームベース認証の信頼 ID プロバイダに ADFS を設定した．
SharePoint サーバの Web アプリケーション（SharePoint の仮想サイトのこと）には，「クラシックモード認証」と「クレームベース認証」の 2 種類の認証モードがある．ADFS などをはじめとする SAML による認証連携を行うときは，「クレームベース認証」を選択することが必須になっている．そのため，学認用 Web アプリケーションの認証モードは，「クレームベース認証」を選択して，大学間連携グループ情報共有サイトを構築した．次に，大学間連携グループ情報共有サイトと ADFS 間に，WS-Federation の信頼関係を設定した．信頼関係を設定しただけでは，ADFS は，属性情報を送信しないので，表 3 に示すように大学間連携グループ情報共有サイトに属性情報を送信するように ADFS の要求規則を設定した．

表 3　SharePoint サービスへの属性情報の要求規則

ADFS の要素	SharePoint サービスの要素
電子メールアドレス [1)]	電子メールアドレス [1)]
役割(Role)[2)]	役割(Role)[2)]

それぞれの要素の ID は，"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"(1)；"http://schemas.microsoft.com/ws/2008/06/identity/claims/role"(2) である．

3.4. ADFS のカスタマイズ

ADFS は，学認に SharePoint サービスを提供した場合，所属機関の IdP を選択するディスカバリーサービス(DS)のような役割を果たす．利用者への利便性を向上するために，「アクティブディレクトリ(AD)による認証の無効化」と「利用者の IdP の候補を表示するための機能追加」の 2 つのカスタマイズを行った．

具体的には，AD の認証を無効化するために，web.config ファイルを次のように変更した．

（無効化前）

```
<localAuthenticationTypes>
        <add name="Integrated" page="auth/integrated/" />
        <add name="Forms" page="FormsSignIn.aspx" />
        <add name="TlsClient" page="auth/sslclient/" />
        <add name="Basic" page="auth/basic/" />
</localAuthenticationTypes>
```

（無効化後）

```
<localAuthenticationTypes>
<!–
        <add name="Integrated" page="auth/integrated/" />
        <add name="Forms" page="FormsSignIn.aspx" />
        <add name="TlsClient" page="auth/sslclient/" />
        <add name="Basic" page="auth/basic/" />
–>
</localAuthenticationTypes>
```

ADFS の DS 機能は，HomeRealmDiscoveryPage Class のライブラリーによって提供されている．このライブラリーと独自のコードを組み合わせ，利用者の IP アドレスから候補となる IdP を表示するプログラムを開発した．具体的な動作は，利用者が ADFS に接続すると，DS のモジュールは，ソース IP アドレスを元に，SQL サーバ内にある IdP 選択履歴テーブルを検索する．検索結果から，履歴があった場合，最後に選択された IdP を，候補 IdP として利用者の DS の画面の上部に表示する．履歴がなかった場合，候補 IdP としては，OpenIdP を表示する．DS の画面には，候補 IdP とは別に，学認に参加している全ての IdP の一覧が表示されているので，候補 IdP が誤っていた場合，所属機関の IdP を選択できるようになっている．利用者が IdP を選択すると SQL サーバの IdP 選択履歴テーブルが更新され，最後に利用したソース IP アドレスと IdP が記録されるようになっている．次回からの利用では IP アドレスが変わらない限り，利用者が前回に利用した IdP が候補として表示されるため，利用者の利便性を向上できる．

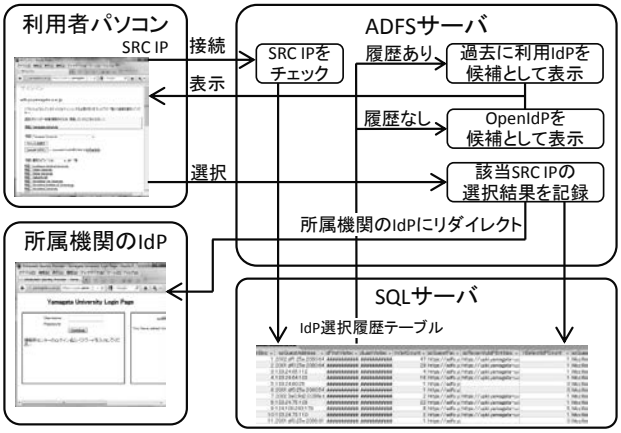


図 4. 利用者の IdP の候補検索モジュールの概略

3.5. 総合的な動作確認と IPv6 への対応

SharePoint サービスの動作確認を行った．利用開始ページに接続してから，SharePoint サービスが利用可能になるまでの一連の動作画面を図 5 に示す．まず，SharePoint サービスを利用するためには，利用開始ページ(https://adfs.yz.yamagata-u.ac.jp/)に接続する．利用開始ページの「利用開始」のリンクをクリックすると，SharePoint サービスのサインインページにリダイレクトされる．「学認ログイン」を選択すると，ディスカバリーサービスのページにリダイレクトされる．所属機関の IdP を選択すると，所属機関の IdP のページにリダイレクトされる．所属機関の認証方式に従って認証操作を行い，認証が成功すると，SharePoint サービスが利用開始される．

2011 年 4 月に JPNIC からの IPv4 アドレス割り当てが終了したことにより，IPv6 アドレスへの移行が進められ

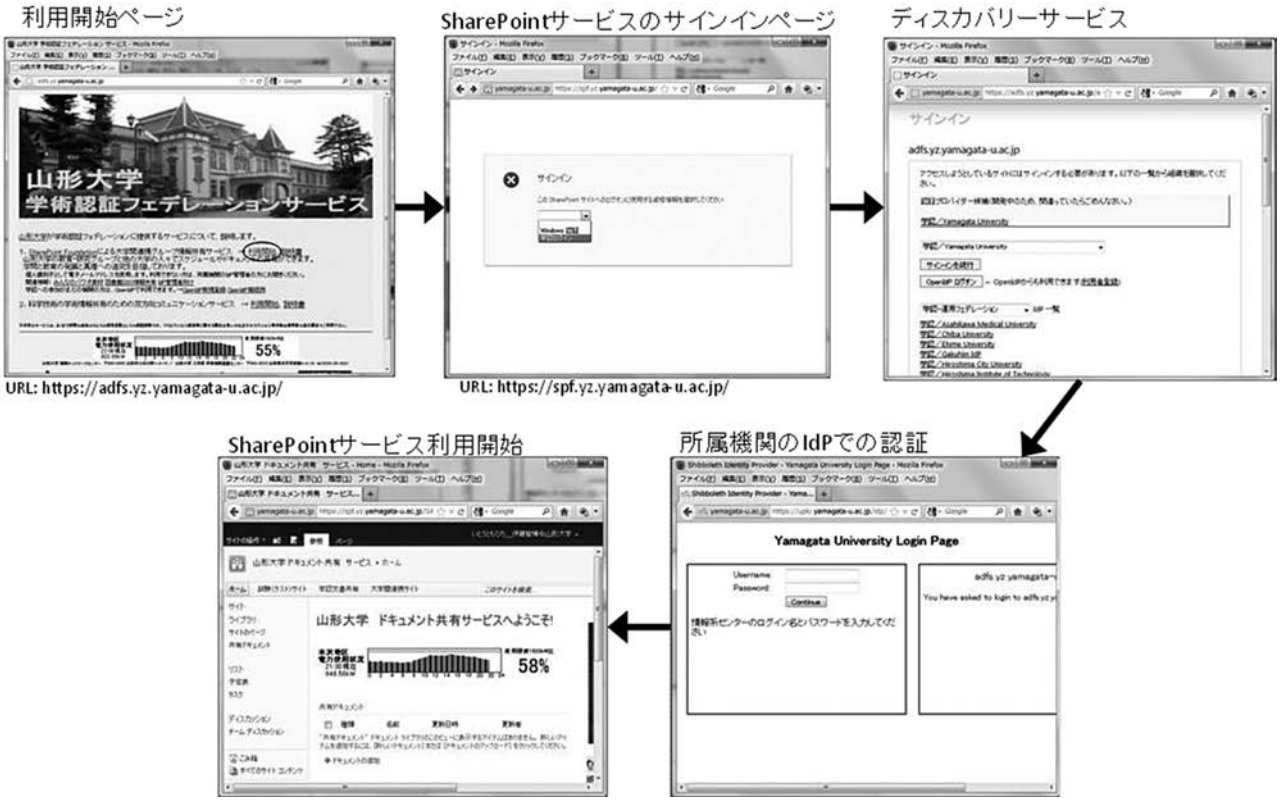


図 5. 学認に対応した SharePoint サービスの動作画面

ている[10]．本学の IPv6 ネットワークは，特殊用途用プロバイダ非依存アドレスを JPNIC より取得しており，BGP プロトコルによるマルチホーム構成によって上位 ISP に接続している．SharePoint サーバ，ADFS サーバ，SQL サーバ，IdP サーバに IPv6 アドレスを付加して，次世代 IP アドレスによるサービスの継続性を確認した．学内および学外から IPv4/IPv6 デュアルスタックのクライアント PC を使用して，SharePoint サービスの動作を確認したところ，全ての機能が問題なく動作した．

学認へのサービス提供を開始した 2012 年 3 月から約 200 人が利用している．1 日あたりの平均認証数は，15 件程度であり，2012 年 7 月までの間に，問題は発生していない．また，SharePoint サービスの共有ドキュメント機能を使用するときに，ウェブブラウザーから Office アプリケーションに遷移するときも認証情報がシームレスに接続できるように改良が加えられており，利便性の高いドキュメント共有サービスを提供できるであろう．

4. まとめ

学認にサービスを提供するために，個人識別子に関する運用ポリシーを定めた．個人識別子には，学認が定めている mail 属性(OID: 0.9.2342.19200300.100.1.3)を採用した．SharePoint サービスと学認で採用されているシボレスは直接認証連携が技術的にできないため，ADFS を経由して，SharePoint と ADFS を WS-Federation で認証連携することで解決した．ADFS は，学認のメタデータを直接読み込むことができないため，SQL サーバとメタデータ変換用ウェブサーバを組み合わることでメタデータの構造を変換することで解決した．これらの試みにより，学認対応 SharePoint Foundation サービスを提供することができた．現在，本学では卒業生用の認証基盤と認証連携用の IdP サーバの構築が計画されている．SharePoint サービスと卒業生用 IdP サーバが認証連携することで，卒業生へのサポートも充実できることが期待される．

先行事例として，Thia らは，FEMMA(Federation Metadata Manager for ADFS)によって，シボレス IdP のメタデータを管理すること述べている[11]．しかし，FEMMA による管理方法について，学認をはじめとする複数の IdP のメタデータを管理する具体例が述べておらず，大規模なフェデレーションへの展開は難しい．本報告では，メタデータの DOM を解析するプログラムを開発して，データベースに正規化した情報を蓄積することによって，SharePoint サービスの大規模展開を可能にした．フェデレーション毎に，メタデータのフォーマットが異なった場合，DOM 解析プログラムを改良することって様々なフェデレーションのフォーマットにも対応できるなどの利点がある．

技術的な利点として，これまで Windows サーバによる

ウェブサービスを学認に提供するときは，認証ミドルウェアとしてシボレスなどのサードパーティ製の認証ミドルウェアを導入し，ウェブアプリケーションは環境変数として認証情報を受け取るプログラムを開発してきた．サーバ内の環境変数を経由するということは，OS の言語設定が影響するため，日本語文字列などを含む SAML アサーションの文字列(UTF-8)が文字化けすることがあった[12]．SharePoint サービスのクレームベース認証機能は，Windows Identity Foundation (WIF)を基盤に開発されている．WIF は，ASP .NET アプリケーションの開発時に，Windows 認証やクライアント証明書，SAML をはじめとする複数セキュリティトークンを使用した統合的な認証機能を提供する API である．WIF による ASP .NET ウェブアプリケーションの開発においても SharePoint と同様に，ADFS を中継することによって，シボレス IdP とウェブアプリケーションが認証連携できるようになる．すなわち，ASP .NET ウェブアプリケーションと認証連携モジュールを同一のコード内で記述でき，属性値などの認証情報が OS の環境変数を経由しないため，文字化けの問題が改善されることが期待される．また，ウェブアプリケーションを複数の認証(AD,シボレス)に対応させるときに，アプリケーションコードをシンプルに開発できる可能性が高い．

今後，本学が提供しているウェブアプリケーションを WIF と ADFS を組わせて，学認と学内の AD 認証を統合した利便性の高いサービスプロバイダーを開発し，学問の発展に寄与したい．

謝辞

IPv6 ネットワーク接続を提供していただきました SINET4 および JGN-X の皆様に深く感謝申し上げます．シボレスおよび学認関連の質問にご回答いただきました国立情報学研究所および学認タスクフォースの皆様に深く感謝申し上げます．本学の認証情報の更新・管理にあたり，常に最新の情報に更新していただいた情報系センターのスタッフの皆様に深く感謝申し上げます．本サービスの一部の構築には，平成 22 年度国立大学法人設備整備費補助金事業の補助を受けて，実施した．

参考文献

[1] UPKI イニシアティブ，https://upki-portal.nii.ac.jp/，(参照 2009-07-20).

[2] 伊藤智博、吉田浩司、鈴木勝人、青木和恵 : “既存の複数認証基盤を統合した UPKI-SSO・eduroam 対応認証基盤の構築”，平成 20 年シングルサインオン実証実験報告書 (2009).

[3] “認証基盤も冗長構成化して可用性を向上”，学認活用事例集， https://www.gakunin.jp/docs/fed/info，(参照 2012-02-09).

[4] 学術認証フェデレーション，https://www.gakunin.jp/，(参照 2012-02-01).

[5] 伊藤智博，高野勝美，田島靖久，吉田浩司 : “ 災害時に備えた分散キャンパスによる情報基盤の整備”，学術情報処理研究誌，No. 15，pp. 5-11 (2011).

[6] 伊藤智博 : “分散キャンパスを活用した複数 ISP 接続による eduroam アクセス回線の冗長化について”，eduroam JP ケーススタディ，http://www.eduroam.jp/docs.html (参照 2011-06-10).

[7] 伊藤智博，高野勝美，田島靖久，吉田浩司 : “複数 ISP と分散データベースによる高可用性認証連携サービスの構築”，大学情報システム環境研究，Vol. 15，pp. 72-79 (2012).

[8] “属性リスト”，学術認証フェデレーション，https://www.gakunin.jp/docs/fed/technical/attribute ，(参照 2011-12-25).

[9] 松平拓也，笠原禎也，高田良宏，井町智彦，金沢大学UPKI SSO 実証実験WG: “金沢大学における IdP, SP 構築の現状と今後の展望”，平成 20 年シングルサインオン実証実験報告書 (2009).

[10] “APNIC における IPv4 アドレス在庫枯渇のお知らせおよび枯渇後の JPNIC におけるアドレス管理ポリシーのご案内”，JPNIC，http://www.nic.ad.jp/ja/topics/2011/20110415-01.html (参照 2011-05-01).

[11] Jean-Marie Thia , Philippe Beraud , Benjamin Guinebertière, Stéphane Goudeau : “ Step-by-Step Guide: Federated Collaboration with Shibboleth 2.0 and SharePoint 2010 technologies”，http://go.microsoft.com/fwlink/?LinkId=207916， (参照 2012-01-09).

[12] “IIS 上に Shibboleth SP を構築したときに属性情報の文字化けを修正する方法”，サイバーキャンパス「鷹山」，https://a.yamagata-u.ac.jp/amenity/Laboratory/LaboNoteWeb.aspx?nLaboNoteID=1173， (参照 2009-10-08).

学認との融合化を視野に入れた金沢大学統合認証基盤の構築と運用

Unified Authentication Infrastructure for Seamless Connection among Online Services inside Kanazawa University and Federation “GakuNin”

松平 拓也†，笠原 禎也†，高田 良宏†，東 昭孝†，二木 恵†，
Takuya MATSUHIRA†, Yoshiya KASAHARA†, Yoshihiro TAKATA†,
Akitaka HIGASHI†, Megumi FUTATSUGI†

takusng@kenroku.kanazawa-u.ac.jp, kasahara@is.t.kanazawa-u.ac.jp, yosihiro@kenroku.kanazawa-u.ac.jp,
higashi@staff.kanazawa-u.ac.jp, futamegu@staff.kanazawa-u.ac.jp

†金沢大学総合メディア基盤センター

†Information Media Center, Kanazawa University

概要

我々は，学認環境と金沢大学統合認証環境の間をシームレスに接続できる環境を実現することを目的として，これまでそれぞれ異なる ID を用いて運用していたものを，生涯 ID である金沢大学 ID に統一化した．さらに，平成 23 年度総合情報基盤システム更新に伴い，学認および金沢大学統合認証環境におけるサーバ群を仮想環境に移行し，システムの可用性を高めることを実現した．本稿では，金沢大学 ID へ統一したことによる学認への対応方法について述べ，構築した仮想環境について説明する．さらに，システムの運用実績を示すとともに，今後の課題についても考察する．

キーワード

学認，Shibboleth，シングルサインオン，認証，認可

Abstract

We unified the authentication ID to “Kanazawa University ID”, which is a lifelong ID, both for the online services in our university and those served by “GakuNin (the Academic Access Management Federation in Japan) in order to improve the convenience of the users by realizing the seamless environment between these services. Furthermore, we renewed the comprehensive information system in the university in FY2011 changing over the server group to a virtual environment aiming at the improvement of the availability. In the present paper, we describe the adaptation method of Kanazawa University ID to GakuNin environment. We also introduce the unified authentication service constructed on the virtual environment. Finally we show the operational results of the developed system and discuss our future works.

Keywords

GakuNin, Shibboleth, Single Sign On, Authentication, Authorization

1. はじめに

近年，“学認[1]”の認知度の高まりとともに，学認へ参加する機関が増加している．学認とは，学術認証フェデレーション（以降，GakuNin と記載）の略称で，国立情報学研究所（以降，NII と記載）が中心となって進められている，学術サービスを利用する機関，学術サービスを提供する機関・出版社等から構成された連合体を指す．各機関は GakuNin に参加することで，相互に認証連携を行うことが可能となる．具体的には，各機関で Identity Provider（以降，IdP と記載）と呼ぶ認証サーバを構築し，各機関でそれぞれ認証を行うことで，GakuNin 内でのシングルサインオンを実現する．また，フェデレーション内で提供される情報サービスを Service Provider（以降，SP と記載）と呼ぶ．金沢大学（以降，本学と記載）も，平成 20 年度に NII が中心となって実施された「UPKI 認証連携基盤によるシングルサインオン実証実験[2]」から GakuNin に積極的に関わっており，GakuNin が本格運用に入った平成 21 年からも，運用フェデレーションに参加し，IdP を運用するとともに，3 つの SP も提供している[3][4]．GakuNin では，認証基盤のミドルウェアとして Shibboleth[5]を採用している．Shibboleth は，オープンソースなため，安価にシングルサインオン環境を構築できることから，GakuNin 環境に限らず，学内の統合認証基盤においても採用している機関も増えてきている．本学は，金沢大学統合認証基盤（Kanazawa University Single Sign On（以降，KU-SSO と記載））を，Shibboleth をベースに構築し，平成 22 年 3 月から本格稼働を開始している[6]． KU-SSO への学内情報システムのつなぎこみ（Shibboleth SP 化）は，全学の情報化計画全体を統括する「情報戦略本部」の配下に位置する，「統合認証・ポータル整備 WG」が主導となり進めている．我々は，本 WG のメンバーとして，全学的なイニシアティブを確保したうえで，各部局が保持している情報システムの SP 化を実現してきた．平成 24 年 5 月末現在，本学の各情報システムへの入り口として機能する「アカンサスポータル」をはじめとし，約 30 の情報システムを SP 化し，KU-SSO によるシングルサインオンを実現している．そのため，KU-SSO 環境は，日々重要度が増してきており，365 日，24 時間運用が強く求められてきている．

一方で，本学の GakuNin 環境は，これまで，KU-SSO とは全く別に構築して運用を行ってきていた．同じ Shibboleth をベースとしていながら，同一の環境を利用することは困難であった．その理由として，KU-SSO と GakuNin の対象ユーザの相違が挙げられる．KU-SSO では，既卒者・退職者も含む，金沢大学に関わる全てのユーザを対象としているのに対し，GakuNin では原則として，在籍する教職員・学生を対象としている点である．これまで GakuNin では IdP で認証が成功すると，属性を必要としない SP へアクセスすることができる仕様であった．そのため，KU-SSO で利用する，「金沢大学 ID」と呼称される生涯 ID を利用することができず，GakuNin では，「ネットワーク ID」と呼称される，本学に在籍する教職員・学生のみが利用可能なネットワーク認証用の ID を使用していた．次に，KU-SSO と GakuNin の個人情報の扱いの相違も理由として挙げられる．KU-SSO 環境では，個人情報のやり取りは学内のみで完結される．そのため，学内の SP においては，個人を特定できる属性を IdP から流すことを前提に構築している．一方で，GakuNin 環境では，我々の管理が及ばない学外の SP が主な利用対象となるため，個人情報の送付を無条件に許可できず，個人情報の送付をユーザが承諾していることが原則となる．そのため，学内用に KU-SSO できめ細かく定義した個人情報属性は GakuNin で利用する属性では必ずしも必要ではなく，結果的に両者の属性定義が大きく異なっていた．さらに，KU-SSO と GakuNin の運用ポリシーの違いも大きな要因である．KU-SSO は，ユーザの利便性を第一に考えた結果，SP 間での情報共有やシングルログアウト[6]など，IdP と SP が密に連携した設計・運用が行われている．一方，GakuNin では個々の IdP や SP を運用する主体が一般に異なるため，独立して運用されることが望まれている．それは，ユーザが多種の SP を渡り歩いても，SP 間が結託することでユーザの嗜好性が特定されるべきではないという，ユーザの匿名性を第一に設計されていることが大きい．しかしながら，将来的には，同一の IdP によって，学内の SP はもちろん，GakuNin に参加している SP もシームレスに利用できる環境を構築することが，ユーザの利便性向上とシステム管理負荷低減の双方の観点から望ましい．

我々は，KU-SSO と GakuNin の環境の融合化を進めるべく，両環境で利用する ID 体系を「金沢大学 ID」に統一化を行い，ユーザの利便性を高めるとともに，LDAP サーバにかかる人的・金銭的コストを省力化した．さらに，KU-SSO および GakuNin 環境において，平成 24 年 3 月に総合メディア基盤センターの総合情報基盤システムを更新（以降，System12 と記載）し，その際に，KU-SSO 環境及び GakuNin 環境のサーバ群の仮想化を行い，システムの可用性向上を実現した．

本稿では，これらの課題に対する取り組みについて示し，Shibboleth を学内環境に適用することを検討している，あるいは運用中の他大学の一助となるとともに，GakuNin 普及を促進させることも目的としている．

2. KU-SSO および GakuNin 環境概要

本章では，本研究で我々が構築した，KU-SSO および GakuNin 環境の概要を示す．図 1 に本研究で構築した，KU-SSO および GakuNin 全体図を示す．本環境の説明に先立ち，Shibboleth の概要を以下に示す．

Shibboleth は SAML2.0[7]をベースとした，異なる情報システム間でのシングルサインオンおよび属性共有を実現するオープンソースソフトウェアである．

Shibboleth は 3 つのシステムから構成される．

- IdP
  - ユーザを認証する．
  - ユーザ属性情報を SP に送信する．
- SP
  - ユーザの認証を IdP に要求する．
  - ユーザの属性を IdP から受信し，アプリケーションに渡す．
- Discovery Service (DS)
  - 複数の IdP が存在する場合に，ユーザが適当な IdP を決定するための情報を提供する．

我々は，KU-SSO と GakuNin の環境の融合化に際し，KU-SSO および GakuNin で使用する ID を，金沢大学 ID に統一した．具体的には，GakuNin 用 IdP において，ネットワーク ID を管理する LDAP サーバから，金沢大学 ID を管理する LDAP サーバを参照するように変更した．このことで，本学のユーザは，KU-SSO 環境と GakuNin 環境ともに，金沢大学 ID で利用可能となった．

さらに，重要サービスを担うサーバ群の信頼性向上とともに強く求められていた，365 日，24 時間運用に近づけるべく，GakuNin および KU-SSO 環境の IdP サーバ，金沢大学 ID を管理する LDAP サーバにおいて，System12 の移行に伴い，仮想環境上に配置し，可用性の向上を行った．

3. KU-SSO と GakuNin の融合化

本章では，KU-SSO と GakuNin 環境の融合化を進めるために行った，利用 ID の統一に際し問題となる種々の対策について説明する．特に，GakuNin 環境で金沢大学 ID を利用できるようにするための課題とその解決策について，次節以降詳しく説明する．

3.1. 金沢大学 ID とロール

金沢大学 ID は，全学的な情報システムの一元化および統合認証に用いる生涯 ID として KU-SSO 環境で使用されている．金沢大学 ID は，常勤教職員・非常勤教職員，学生・研究生などを問わず，本学に関わる全構成員に対して 1 人に 1 つずつ付与する ID である．ユーザの重要な個人情報を含む情報サービスの利用に使われることを考慮し，金沢大学 ID の採番方法は，ランダムに与えたアルファベット 3 桁と数字 5 桁の 8 桁とし，他人の ID を容易に推測できないようにしている．また，転学類に伴う学籍番号変更や，卒業後に本学に就職した場合な

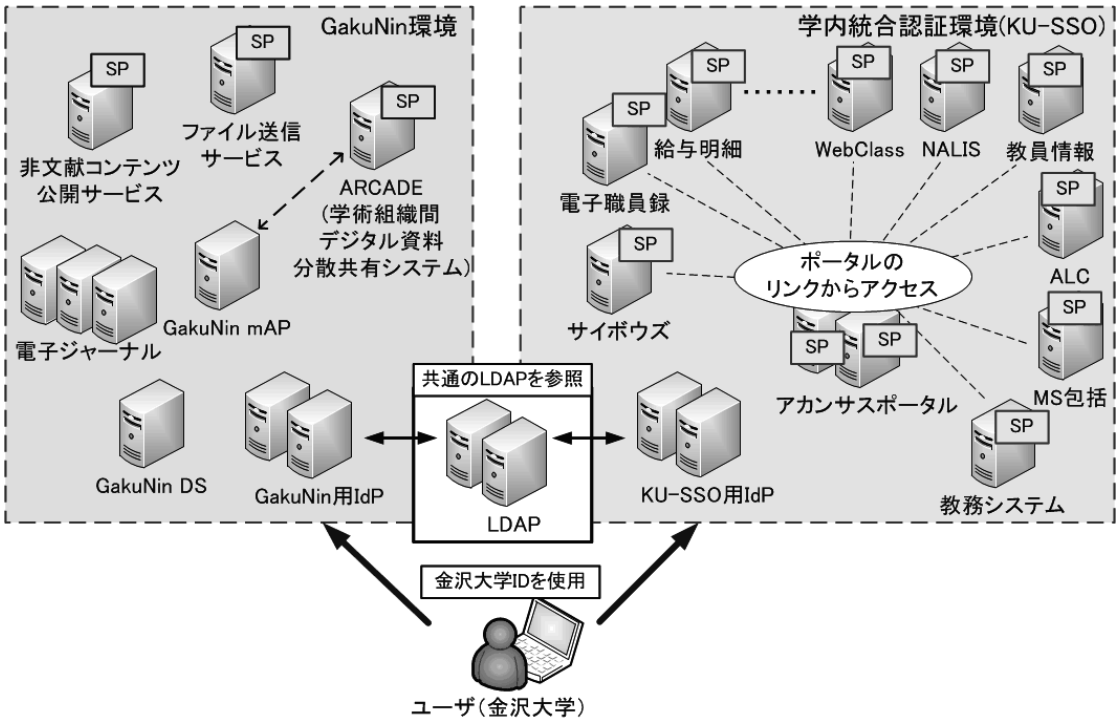


図 1 KU-SSO および GakuNin 全体図

どの場合においても，同一 ID を使用でき，卒業・退職後も ID を抹消されず，“1 ユーザ 1ID” を実現している．

一方，KU-SSO 環境の SP には，学生用の履修登録システムや，教職員用の給与明細システムなど，教育・研究・業務に関する様々な種類があるため，それらを使用できるユーザは，SP の利用目的によってそれぞれ異なる．そのため，各 SP が，ユーザの職分等の属性情報から，当該 SP を利用できる権限があるかどうかを判断できるように，ユーザの属性を“ロール” という名称で定義し，それぞれの SP で必要とされる区分分けを行っている．表 1 にロールの一覧を示す．学生は 4 パターン，教員は 10 パターン，職員は 8 パターン，その他 7 パターンを設定し，全部で 29 パターンに区分した．また，ユーザが複数のロールを持つことも想定している．たとえば，本学の学部を卒業し，博士前期課程を修了した後に本学の職員（学務系以外）になった場合は，学生（既卒），学生（既卒），職員（常勤学務系以外）という 3 つのロールが付与されることになる．なお，学部を卒業した場合と博士前期課程を修了した場合に分類されるロールは「学生（既卒）」で同一であるが，それぞれのロールに付随する学籍番号や所属等の情報が異なるため，SP から得られる情報はそれぞれ異なる．但し，複数ロールを持つユーザであっても，金沢大学 ID は 1 つである．

表 1 ロール一覧表

区分	ロール名	ロール番号
学生	入学前	0
	在学	1
	既卒	2
	退学	3
教員	常勤	4
	教諭	18
	研究員	20
	非常勤講師	38
	名誉教授	37
	医員	5
	TA	32
	RA	33
	退職・転出	6
	その他（学外教員等）	39
職員	常勤学務係	9
	常勤学務係以外	10
	非常勤学務係	11
	非常勤学務係以外	12
	非職員学務係・秘書含	22
	非職員学務係以外・秘書含	13
	教務補佐員	19
	退職	14
その他	管理者	15
	管理者（システム別）	23
	学外学生（公開講座）	16
	ゲスト	17
	学外学生修了（公開講座）	24
	研究協力員（共同研究）	26
	家族等	25

3.2. 金沢大学 ID の学認対応における課題

GakuNin 環境において金沢大学 ID を利用可能にするためにまず留意すべき事項は，前述の特徴を持つ ID による認証でも，「学術認証フェデレーション システム運用基準（以降，運用基準と記載） Ver1.2[8]」に適合する必要がある点である．運用基準の「3.2) 属性情報の信頼性」に「IdP は，自組織に所属する利用者の属性を保証すべきである．また，自組織に所属しない利用者の属性を保証すべきではない．例えば，A 大学の IdP が B 大学の学生の属性を保証すべきではない．ただし，自組織に所属しない利用者を自組織が管理する場合，SP に対する不正なアクセスが発生しないよう特に属性管理に注意することで，そのような利用者の属性を保証してもよい．」と記載されている．「自組織に所属する利用者」を，「在籍する教職員・学生」という解釈は最小構成として揺るぎないもので，そこを確実に保証することは，全ての大学に対して求められている．後半部分において，大学として責任がとれる範囲で、大学の裁量でそれ以外の範囲も含めることができる旨記載されているが，本学では認めていない．

上記を踏まえ，一つ目の課題として，利用者を在籍する教職員および学生のみに制限できるかいうことが挙げられる．前節で説明したロールで言うと，学生（在学），教員（常勤，教諭，研究員，医員），職員（常勤学務係，常勤学務係以外，非常勤学務係，非常勤学務係以外，教務補佐員）が該当する．選定の理由は職員証または学生証が交付されているかどうかである．これらのロールを持つ利用者のみ GakuNin 環境を利用できるように設計を行う必要がある．

二つ目の課題として，LDAP サーバを，金沢大学 ID を管理している LDAP サーバに変更する際に，「属性情報仕様一覧[9]」に記載されている，GakuNin を利用する際に必要となる属性値を賄えるかどうかということが挙げられる．

次節以降，これらの解決方法について説明する．

3.3. GakuNin 利用可能者の制限方法

GakuNin 環境においても金沢大学 ID を利用可能とするためには, GakuNin 用 IdP サーバが金沢大学 ID を管理している LDAP サーバを参照するように変更する必要がある．但し，変更を行った際，在籍する教職員または学生のみ利用可能という条件を維持するためには，uid の属性値（金沢大学 ID）だけではなく，在籍する教職員または学生のみが持つ属性情報を制限条件に用いる必要がある．本学の場合，ロール属性がそれに該当する．しかし，標準的な IdP の設定では，一旦 uid とパスワードによってユーザの認証が成功すると，IdP 側では属性情報による絞り込みができず，ユーザの属性情報を一切要求しない SP であった場合，たとえ在籍の教職員または学生以外のロールを付与されていても，金沢大学 ID さえ所有していれば, SP を利用できてしまう. 解決策として, IdP から SP に対してロール属性情報を送付し，SP 側で制御を行ってもらう方法がある．しかし，GakuNin 環境では，我々の管理が及ばない SP が大半であるため，現実には SP 側で利用制限を行うという対応は困難である．そのため，本学の IdP 側で SP の利用制限を行う必要があった.

そこで我々は，SampleFilterPerSP [10]という，IdP のプラグイン機能を利用して本課題の解決を行った．本プラグインを利用することにより，これまで困難であった IdP 側での SP へのアクセス制御を，ユーザの属性情報に基づいて実現することが可能となる. そこで, 本学の IdP での認証後に，SampleFilterPerSP を用いて，3.2 節で述べたロール属性をもつユーザのみ GakuNin 環境の SP へのアクセスを許可するように実装した．ロール属性を用いた SampleFilterPerSP の設定ファイルの記述例を図 2 に示す．この例では，NII が提供する，Fshare[11]という，大容量ファイル転送サービスを利用する場合に SampleFilterPerSP が動作する.「roleNumber」は金沢大学 ID を管理している LDAP サーバに持つロール属性で, 表 1 のロール番号が該当する．図 2 のように記載することで，学生（在学），教員（常勤，教諭，研究員，医員），職員（常勤学務係，常勤学務係以外，非常勤学務係，非常勤学務係以外，教務補佐員）のいずれかのロール属性を持つユーザだけが Fshare を利用することができる．そして，それ以外のロールのユーザについては，図 3 に示す画面を表示し, この SP を利用できないようにできる. このように，設定ファイルに記述されている SP 毎に，特定の属性値を持つユーザについてのみ SP の利用を許可することを IdP 側で制限でき, 金沢大学 ID を利用した場合でも GakuNin のポリシーに準拠することを実現した.

```
<EntityDescriptor entityID="https://fshare.sinet.ad.jp/shibboleth">
  <Attribute attributeID="roleNumber">1</Attribute>
  <Attribute attributeID="roleNumber">4</Attribute>
  <Attribute attributeID="roleNumber">5</Attribute>
  <Attribute attributeID="roleNumber">9</Attribute>
  <Attribute attributeID="roleNumber">10</Attribute>
  <Attribute attributeID="roleNumber">11</Attribute>
  <Attribute attributeID="roleNumber">12</Attribute>
  <Attribute attributeID="roleNumber">18</Attribute>
  <Attribute attributeID="roleNumber">19</Attribute>
  <Attribute attributeID="roleNumber">20</Attribute>
</EntityDescriptor>
```

図 2 SampleFilterPerSP 記述例

図 3 アクセス拒否画面

3.4. GakuNin 利用属性の扱い

二つ目の課題として，LDAP サーバを，金沢大学 ID 管理用に変更しても，GakuNin で必要な属性を利用できるようにする必要がある．LDAP を変更することで対応が必要であった GakuNin で必要な属性である，eduPersonPrincipalName（以降，ePPN と記載），eduPersonAffiliation（以降，ePA と記載），eduPersonScopedAffiliation（以降，ePSA と記載）についてそれぞれ説明する.

- ePPN

ePPN は，GakuNin 内で一意な，かつ，永続的な利用者識別子であり，GakuNin 内での一意性を保証する必要がある．金沢大学 ID は 1 ユーザ 1ID で，永続的に一意性が保証されているため，この条件についてはクリアしている．但し，金沢大学 ID は生涯 ID であり，変更できないため，そのままの値で送出すると，万一漏えいがあった場合に非常に問題となる．そこで，IdP の設定ファイルの一つである「attribute-resolver.xml」内で金沢大学 ID に変換処理をかけて，ePPN から金沢大学 ID を割り出せない形で送信するように設計した．attribute-resolver.xml の記述を図 4 に示す．このように，attribute-resolver.xml 内では Script タグ内において JavaScript が利用可能である. セキュリティ上，一部の変換部分は記載していないが, まず, uid 属性である金沢大学 ID を取得し，金沢大学 ID に対して特定の変換処理をかけた後に，ePPN として各 SP に対して送出している．例として,

123abc456def789hig@kanazawa-u.ac.jp

というような，金沢大学 ID を推測できない形で，かつ GakuNin 内で一意性を保証した上で送信を行っている.

```
<!-- Attribute Definition for eduPersonPrincipalName -->
  <resolver:AttributeDefinition id="principalName" xsi:type="Script"
xmlns="urn:mace:shibboleth:2.0:resolver:ad"

            sourceAttributeID="uid">
    <resolver:Dependency ref="myLDAP" />

    <resolver:AttributeEncoder xsi:type="SAML1String"
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:mace:dir:attribute-def:eduPersonPrincipalName" />

    <resolver:AttributeEncoder xsi:type="SAML2String"
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
friendlyName="eduPersonPrincipalName" />
    <Script>
      <![CDATA[

importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.
provider);
          importPackage(Packages.org.apache.commons.codec.digest);
          uniqueValue = uid.getValues().get(0);


          principalName.getValues().add(localpart + "@kanazawa-u.ac.jp");
      ]]>
    </Script>
  </resolver:AttributeDefinition>
```

図 4 ePPN 記述方法

なお，不正アクセスなどにより，SP 側からユーザの特定を要求された場合は，本学側で，発行済みの金沢大学 ID に対して，ePPN を生成している変換処理を順次かけていき，マッチングを行うことで，当該 ePPN を利用している金沢大学 ID を割り出し，ユーザの特定を行う．

- ePA および ePSA

ePA は，GakuNin 内における利用者の職種等を表す．GakuNin では，ePA には「faculty」，「staff」，「student」，「member」，「無し（空白）」の値が利用可能である．ePSA に設定する属性値は ePA と同値であるが，利用者が所属する機関を示すため，@以下にスコープを付加したものとなる（例：staff@kanazawa-u.ac.jp）． 我々は，現段階で ePA および ePSA を要求している SP の状況を鑑み，教職員を「staff」，学生を「student」としている．ただし，ここで考慮すべきこととして，一つの金沢大学 ID に二つ以上のロールを持つユーザの対応がある．例として，本学教員でありながら，大学院に社会人入学している場合は，教員かつ学生のロールを持つため，staff と student 両方の属性を SP に送出する必要がある．staff しか利用できない SP も存在するため，student しか送出されないことによる不利益が生じないように，両方の属性を送出する必要がある．

そこで，我々は，attribute-resolver.xml に図 5 のように記述することで対応した．まず，ユーザが持つロール数を取得し，「size」に格納する．そして，ロール数分 for 文を通す． ロール番号が 1 であれば「student」，4,5,9,10,12,18,19,20 のいずれかであれば，「staff」属性が ePA に付加される．それ以外のロール番号であれば何も属性が付加されない．先の例のように，教員かつ学生の場合は staff と student の両方が SP に送出されることになる．

```
<!-- Attribute Definition for eduPersonAffiliation -->
  <resolver:AttributeDefinition id="eduPersonAffiliation" xsi:type="Script"
xmlns="urn:mace:shibboleth:2.0:resolver:ad" sourceAttributeID="roleNumber">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="SAML1String"
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:mace:dir:attribute-def:eduPersonAffiliation" />
    <resolver:AttributeEncoder xsi:type="SAML2String"
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
friendlyName="eduPersonAffiliation" />
    <Script>
      <![CDATA[

importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.
provider);

    eduPersonAffiliation = new BasicAttribute("eduPersonAffiliation");

    size = roleNumber.getValues().size();

    for (i=0;i<size;i++){
      if (roleNumber.getValues().get(i) == "1" ) {
        eduPersonAffiliation.getValues().add("student");
      }
      if (roleNumber.getValues().get(i) == "4" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "5" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "9" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "10" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "11" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "12" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "18" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "19" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
      if (roleNumber.getValues().get(i) == "20" ) {
        eduPersonAffiliation.getValues().add("staff");
      }
    }
      ]]>
    </Script>
  </resolver:AttributeDefinition>
```

図 5 ePA 記述方法

図 6 EV-SSL 証明書

このように，GakuNin で必要とされる属性で，LDAP サーバに持たない属性の取り扱いにおいてもクリアすることができた．

3.5. EV-SSL 証明書

このように, GakuNin 環境においても金沢大学 ID を利用することにより，ユーザは，一つの ID のみを管理すればよく，利便性が向上する．しかし，金沢大学 ID を対学外のサービスにも適用することで，ユーザは，認証画面が表示されると，金沢大学 ID を条件的に入力してしまい，フィッシング詐欺の被害にあう危険性が想定される．KU-SSO と GakuNin で IdP を分けて構築しているのは，そのあたりをユーザに理解してもらうという側面がある．そこで，我々は，KU-SSO 用 IdP，GakuNin 用 IdP および多くの重要な情報を扱う，アカンサスポータルに対して，EV-SSL 証明書[12]の導入を行った．EV-SSL は Extended Validation-Secure Socket Layer の略で，証明書に記載される組織が法的かつ物理的に実在し，その組織が証明書に記載されるドメインの所有者であることを認証する．ドメインの所有者の確認は，WHOIS データベースに照会し，組織の法的実在性の確認は，公的書類や組織の実運用性を第三者データベース（帝国データバンク・DUNS・職員録）へ照会をかける．なお，公的書類には印鑑証明書だけでなく，登記事項証明書等も含まれる．さらに，EV-SSL 証明書は個人で取得することはできず，法人のみ取得可能となっている．世界標準の認証ガイドラインで，サーバ証明書の中で最も厳格な審査が行われている. 図 6 に EV-SSL 証明書を導入した KU-SSO 用 IdP の画面を示す．このように，EV-SSL 証明書を導入しているサイトにアクセスすると，アドレスバーが緑色に変化する．さらに，アドレスバーの右側に，サイトを運営している大学名が表示され, そこをクリックすると, 認証局の情報やサイト運営組織の所在地も確認できる．このように，EV-SSL 証明書を導入することで，ユーザに対して，アドレスバーの色とサイトの運営組織を確認したうえで，金沢大学 ID とパスワードを入力するように指導するようにした．

なお，今回，我々は EV-SSL 証明書を GMO グローバルサイン株式会社[13]（以降，グローバルサインと記載）から購入した. グローバルサインを選択した理由として, ライセンス体系が挙げられる．我々は，IdP サーバを冗長化して運用しており，他の認証局ではその場合 2 ライセンス必要であった．一方でグローバルサインは 1 コモンネームあたりの金額で，複製してインストール可能であり，冗長化したサーバにインストールするためのライセンスのコストを抑えることができた.

4. System12 への移行

4.1. システム構成

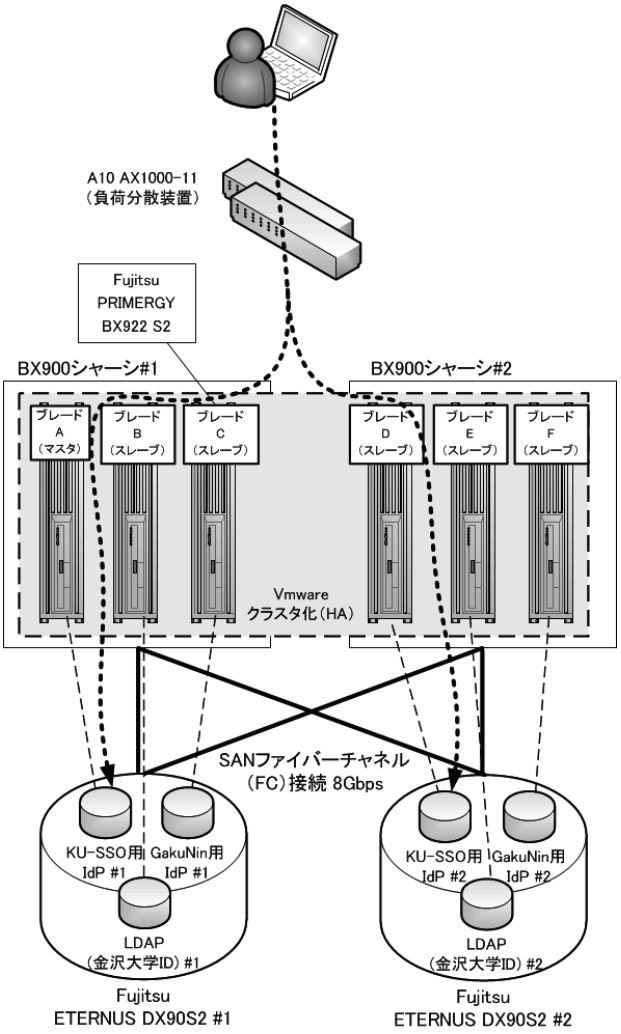


図 7 System12 システム構成図

我々は，System12 への移行に伴い，KU-SSO および GakuNin の IdP サーバ，金沢大学 ID を管理する LDAP サーバを仮想環境に移行して可用性の向上を目指した．System12 への移行前は，これらのサーバは，占有ハードウェアによる構成であった．そのため，ハードウェアに障害が発生した場合は，障害部分を修理するまで復旧は困難であった．なお，KU-SSO および GakuNin 両環境で金沢大学 ID を利用できるようにしたことで，今後はネットワーク ID を管理していた LDAP サーバ 4 台について意識する必要がなくなるとともに各種メンテナンスも不要となり, 金銭的･人的コストの削減に寄与している．System12 におけるシステム構成の概念図を図 7 に示す．System12 における仮想環境には，VMware vSphere 5 Standard[14]を採用している．なお，統合認証関係には，全部で 6 台のブレードサーバが割り当てられている．ブレードサーバのハードウェア諸元は以下のとおりである．

- Fujitsu PRIMERGY BX922 S2[15]
  - CPU：Xeon X5690 (3.46GHz/12MB/6 コア)
  - メモリ：48GB

ブレードサーバ自体はディスクを持たず，Fujitsu ETERNUS DX90S2[16]（以降，DX90S2 と記載）と SAN ファイバーチャネル（8Gbps）で接続されている．各ブレードサーバにおいて仮想サーバを立ち上げるためのハイパーバイザである ESXi ホストは, DX90S2 上にインストールする．なお，ブレード A～C の ESXi ホストは DX90S2 #1, ブレード D～F の ESXi ホストは DX90S2 #2 上で稼働する．そして，ブレード A～C の ESXi ホスト上で動作する仮想サーバは DX90S2 #1 に，ブレード D～F の ESXi ホスト上で動作する仮想サーバは DX90S2 #2 上にそれぞれインストールを行う．また，負荷分散装置として，A10 ネットワークス株式会社の AX1000-11 [17] を用いて，SSL アクセラレータによるクライアント単位での負荷分散を行う設計とする．SSL アクセラレータを用いて負荷分散を行うことで，プライベート配下のクライアントからアクセスが来た場合でも，均等に負荷分散を行うことが可能となる．なお，AX1000-11 自身もクラスタ化を行い，冗長性を高めるようにする．さらに，VMware の機能の一つである, vSphere High Availability（以降，HA と記載）を使用する．HA を構成すると，1 つの ESXi ホストがマスタとなり，その他の ESXi ホストがスレーブに設定される．マスタホストは，スレーブホストの状態を監視し，スレーブホストに障害が発生した場合に，当該ホスト上で稼働している仮想サーバをフェイルオーバーするホストを決定し，仮想マシンをすべて，ほかのホストでただちに再起動する．

4.2. IdP サーバの動作

本節では，KU-SSO および GakuNin 環境における IdP サーバの構成について説明する．それぞれの環境における IdP サーバの構成を以下に示す．

- ハードウェア割り当て（1 ゲスト OS あたり）
  - CPU：2vCPU（仮想ソケット数 1，コア数 2）
  - メモリ：8GB
  - HDD：120GB（シンプロビジョニング）
- OS
  - Red Hat Enterprise Linux 6.2 (x64)
- ミドルウェア
  - Shibboleth IdP 2.3.6
  - Apache 2.2.15
  - Jdk 1.6.0update31
  - Tomcat 6.0.35
  - Ant 1.8.3
  - Terracotta 3.6.1

図 7 に基づき，KU-SSO 用 IdP サーバの可用性について説明する．KU-SSO 用 IdP は，ブレード A の ESXi ホスト上に一台（IdP #1），ブレード D の ESXi ホスト上にもう一台（IdP #2）構築する．AX1000-11 を介して負荷分散を行う設計とするが，IdP はセッション情報を持つため，単純に負荷分散することはできない．そこで，Terracotta[18]を用いて IdP の冗長化を行うようにする．Terracotta は複数の JavaVM 上で同じ Java オブジェクトを共用できるオープンソースのミドルウェアである．Terracotta を用いることで，IdP 間でセッションを共有できるようになる．どちらかの DX90S2 に障害が発生した場合，AX1000-11 により，障害が発生している IdP には振り分けられなくなるようにし，IdP の動作を継続させるようにする. また, ブレードDに障害が発生した場合, HA 機能により，ブレード D 以外の ESXi ホスト上で，自動で IdP #2 が立ち上がるようにし，IdP #1 が一台で動作する時間を数分程度で済む設計とする．ただ，この間も，AX1000-11 で振り分けを行い，IdP の動作が継続するようにする．

このように，様々な部分で障害が発生した場合でも，極力管理者の手を介することなくサービスを継続できる設計とする．

5. 運用実績

本章では，これまで述べてきたシステムの運用実績を示す．System12 による運用は，平成 24 年 3 月 19 日から開始している（AX1000-11 のみ平成 24 年 7 月 8 日運用開始予定で，それまでは DNS ラウンドロビンで対応）．GakuNin と KU-SSO の IdP サーバは，ハードウェアおよびソフトウェアの構成が同じで，GakuNin よりも KU-SSO の認証処理が圧倒的に多いことから，KU-SSO の IdP で評価を行った．平成 24 年 3 月 19 日から平成 24 年 6 月 24 日までの IdP での認証数の推移を図 8 に示す．4 月は全入学生対象の情報処理基礎の講義や，学生の履修登録, さらにはアカンサスポータルを経由しての LMS の利用があるため，一年で一番 IdP での認証が行われる月である．多い時で，一日あたり 2 万件を超える IdP での認証処理が行われており, 平成 24 年 4 月 19 日に 21,477 回の認証処理が行われていることがわかる．そこで，平成 24 年 4 月 19 日の IdP #1 における IdP の認証数とそれに伴う CPU 負荷率およびメモリ使用率を図 9 に示す. 認証数が増加した場合でも，CPU 負荷率およびメモリ使用率に変化がほとんど見られず，どちらも十分に余力があることがわかり，IdP ではリソースに負荷を与えることなく運用できていることを確認することができた．

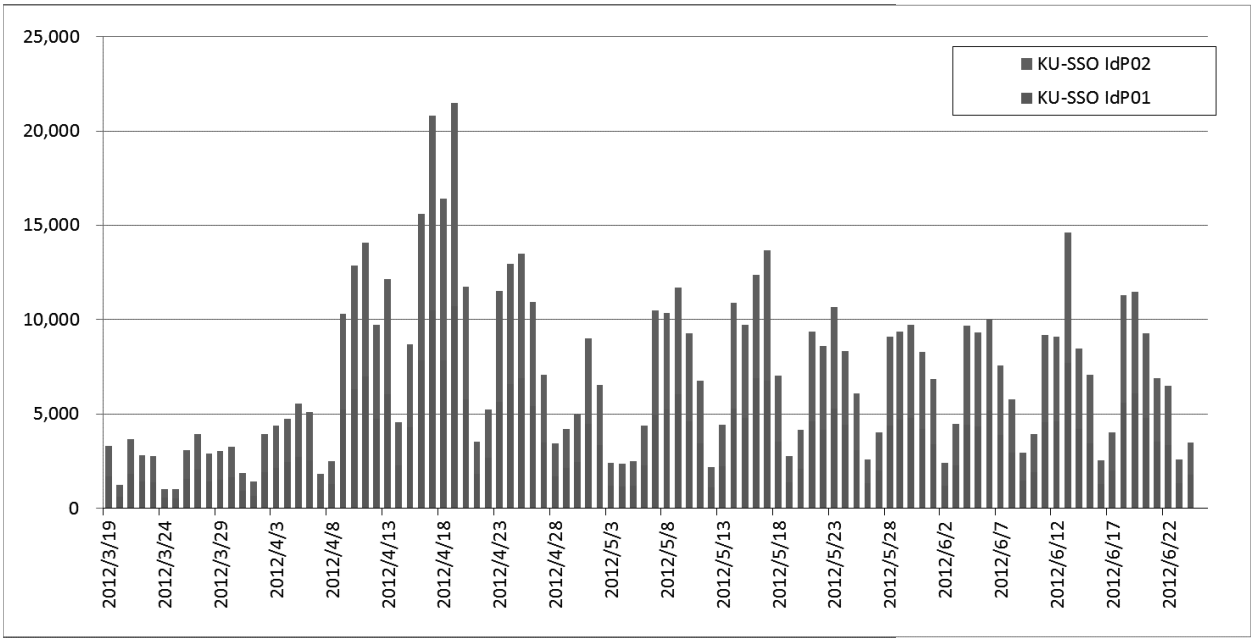


図 8 KU-SSO 用 IdP における認証数の推移（2012/3/19～2012/6/24）

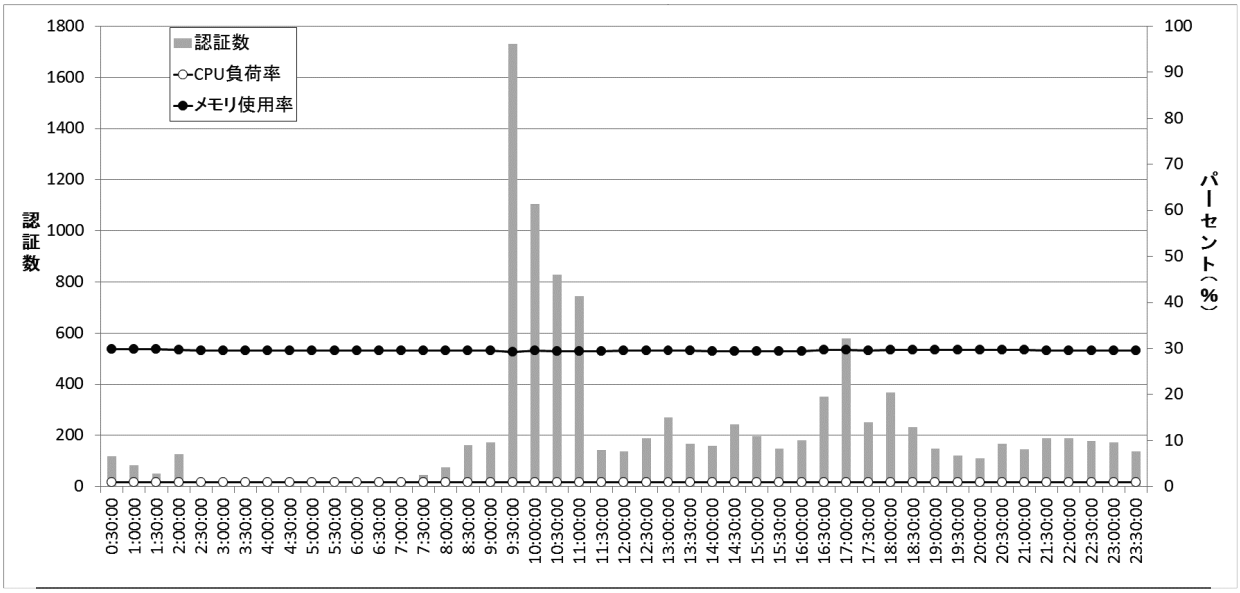


図 9 KU-SSO の IdP サーバにおける認証数と CPU 負荷率及びメモリ使用率（2012/4/19）

6. まとめ

今回，KU-SSO と GakuNin で使用する ID を金沢大学 ID に統一したことにより，ユーザは金沢大学 ID で GakuNin と KU-SSO のどちらもアクセスできるようになり，GakuNin と KU-SSO 環境の融合化を進めることができた．ID 統一化の際に発生した，GakuNin と KU-SSO の利用者範囲の相違の問題においては，SampleFilterPerSP を用いることで，本学 IdP 側で，特定のロールをもつユーザだけが個々の SP の利用を制御できるようにすることで解決した．また，GakuNin で参照する LDAP サーバを変更することにより生じた，GakuNin で必要ないくつかの属性の摺合せにおいては，LDAP 内でもつ属性を attribute-filter.xml 内で加工することで対応した．結果として，金沢大学 ID を管理する LDAP サーバのみを意識するだけでよくなり，人的負荷や運用コストの削減を実現できた．さらに，金沢大学 ID を対学外用サービスで用いることによるフィッシング対策として，EV-SSL 証明書を導入したことで，ユーザに対して視覚的に注意を促すことができた．また，本学において重要度が高い KU-SSO 環境および GakuNin 環境において，System12 への移行に伴い，KU-SSO 環境と GakuNin 環境で使用しているサーバ群を VMware で仮想化したことにより，システムの可用性を高めることができた．さらに，構築したシステムの評価を行ったことで，実運用においても十分耐えうるシステムであることを実証できた．

今後の課題として，KU-SSO および GakuNin の IdP サーバの完全統合による両サービスのシングルサインオン化が挙げられる．現在のところ，それぞれの環境をまたぐ際には，認証画面を表示することで，ユーザに注意喚起を促しているが，EV-SSL によるユーザリテラシーが向上したのち，進めていきたいと考えている．ただし，現在は KU-SSO 環境においてはシングルログアウトを実現しているが，GakuNin 環境では実現できていない．KU-SSO と GakuNin 環境をシームレスに利用できる環境を目指すために，両環境におけるシングルログアウトを実現できる機構を考案する必要があると考えている．海外では，各大学に統合認証システムを持っており，認証を行うと学内の情報サービスはもちろんのこと，国のフェデレーションにあるサービスもシームレスに利用可能なところも多い．我々も，将来的には KU-SSO に一本化し，KU-SSO と GakuNin でそれぞれ提供している SP の一元化及びシームレスに利用できる環境の構築に努めていきたい．

謝辞

本研究は科研費 若手研究 B （22700809）の助成を受けたものである．

参考文献

[1] GakuNin，http://www.gakunin.jp/docs/fed (accessed 2012.6)
[2] 平成 20 年シングルサインオン実証実験報告書，https://www.gakunin.jp/docs/open/fed/6 (accessed 2012.6)
[3] 松平 拓也, 笠原 禎也, 高田 良宏, 井町 智彦, “UPKI 認証連携基盤に基づく安全なデータ共有システム構築の試み”，学術情報処理研究，No13，pp.84-90，(2009)
[4] IdP, SP 一覧，https://www.gakunin.jp/docs/fed/participants (accessed 2012.6)
[5] Shibboleth，http://shibboleth.net/ (accessed 2012.6)
[6] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 森 祥寛，“大学における Shibboleth を利用した統合認証基盤の構築”，情報処理学会論文誌，Vol.52 No.2，pp.703-713，(2011)
[7] SAML2.0, http://www.oasis-open.org/specs/index.php (accessed 2012.6)
[8] 学術認証フェデレーション システム運用基準 (Ver. 1.2)，https://www.gakunin.jp/docs/files/GakuNin_System_SpecV1.2.pdf (accessed 2012.6)
[9] GakuNin 属性リスト，https://www.gakunin.jp/docs/fed/technical/attribute (accessed 2012.6)
[10] SampleFilterPerSP，https://www.gakunin.jp/docs/fed/technical/idp/customize/knowhow/authorization (accessed 2012.6)
[11] Fshare，https://fshare.sinet.ad.jp/ (accessed 2012.6)
[12] EV-SSL 証明書，http://jp.globalsign.com/service/ssl/ev.html (accessed 2012.6)
[13] GMO グローバルサイン株式会社，http://jp.globalsign.com/ (accessed 2012.6)
[14] VMware vSphere 5 Standard，http://www.vmware.com/jp/products/datacenter-virtualization/vsphere/mid-size-and-enterprise-business/overview.html (accessed 2012.6)
[15] PRIMERGY BX922 S2，http://jp.fujitsu.com/platform/server/primergy/product-navi/html/bx922s2-201011-pgx9s24ba.html (accessed 2012.6)
[16] ETERNUS DX90S2，http://storage-system.fujitsu.com/jp/products/diskarray/dx-entry/ (accessed 2012.6)
[17] A10 AX1000-11，http://www.a10networks.co.jp/press/pressrelease/12/2/2011.html (accessed 2012.6)
[18] Terracotta，http://terracotta.org/ (accessed 2012.6)

学認と学内統一認証の自動切替

Auto exchange of GakuNin and the unified authentication of a university

松澤英之，園田誠，黒木亘， 廿日出勇
Hideyuki Matsuzawa, Makoto Sonoda, Wataru Kuroki, Isamu Hatsukade

matuzawa@cc.miyazaki-u.ac.jp, sonoda@cc.miyazaki-u.ac.jp,
wata-k@cc.miyazaki-u.ac.jp,hatukade@cs.miyazaki-u.ac.jp

宮崎大学　情報基盤センター

University of Miyazaki, Information Technology Center

概要

学術認証フェデレーションに参加することで、大学の枠を超えて相互に認証連携を行う事が可能になり、大学や出版社等が提供する Web アプリケーションを利用できる。学認に参加している大学の多くは、学内統一認証 ID を学認 ID として利用しているが、宮崎大学では、セキュリティ及びシステム変更の際に掛かる経費及び労力を考慮して、学認 ID は、学内の統一認証 ID とは別の ID を利用することにした。そこで、現在学内統一認証で運用し、なおかつ学外者に簡単に提供できる学内 Web アプリケーションサービスである宮崎大学 Web ネットワーク認証を学認用のサービスプロバイダ(SP)化するシステムの開発を行った。宮崎大学では、学認と学内統一認証は独立して運用するので、現在運用している学内統一認証を用いた認証システムには極力影響を与えないように開発を行った。

キーワード

学認，学内統一認証，自動切替, Radius

1. はじめに

大学には研究用、教育用、事務用など多種多数なシステムがあり、各システムを利用する場合、利用者を特定する或は学外者の利用を制限するために認証が行われている。システム毎に別々の ID、パスワードを作って運用すると、利用者は、システム毎に ID、パスワードを覚えなければならないので、利便性を損なう。また、セキュリティ上、システム毎にパスワードを変えることが望ましいが、システムが多数存在する場合、利用者は非常に簡単な一つのパスワードを使いまわす傾向がある。一方、各システムの運用管理者は、各自で常にユーザデータベースを最新の状態に保つ必要があり、システムが増えるにつれ管理運用のための労力が増える。

そこで、まず一つの認証システムで学内ほぼすべてのシステムを認証できるように、統一認証システムを作ることが多い。それに加え、一回の認証ですべてのシステムの利用が可能になるように、シングルサインオン(SSO)を構築する場合もある。

いま大学内システムの認証について述べたが、これに

加え、別大学、或はクラウドのシステムを利用する場合でも、自組織が管理する一つの認証システムですべての大学或はクラウドのシステムが利用出来る様になれば、利用者と運用管理者の利便性とセキュリティの観点から非常に有益である。この大学の枠を超えた認証連携が学術認証フェデレーション(学認)である。学認に参加することで、大学や出版社等が提供するWebアプリケーションを利用できる。

本研究では、現在学内統一認証で運用し、なおかつ学外者に簡単に提供できる学内 Web アプリケーションサービスである宮崎大学 Web ネットワーク認証システムを学認用のサービスプロバイダ(SP)化するシステムの開発を行った。

2. 宮崎大学統一認証

宮崎大学では、学内統一認証ができる前は、2003 年 10 月に旧宮崎大学と宮崎医科大学が統合したことなど歴史的経緯から、学内に情報センター系、事務系、及び医学部系のシステムが存在していた。情報センター系システムを除いて、各システムはシステム毎に独自で認証を行っていた。年々全学で使うシステムが増えてきていたので、各認証システムを統合するよりも、新たに全学で利用できる認証システムを構築した方がよいという事となり、2009 年 4 月に LDAP システムを用いた宮崎大学統一認証が作られた。

統一認証を導入する当時、LDAP に簡単に対応できるシステムが多くなってきたこと。又、たまたま LDAP に対応できないシステムが近々に更新を迎えていたこともあり、2-3 年程度でほぼ全てのシステムが学内統一認証に移行することが出来た。これは、他大学の現状を見る限り非常に効率よく変更が出来た事例だと思われる。

この時の統一認証は学内にいる教職員、学生が学内システムを利用する場合を想定していた。

3. 学術認証フェデレーション(学認)

3.1. 概要

学認[1]は、大学の枠を超えて、学術e-リソースを利用する大学と学術e-リソースを提供する機関・出版社等がフェデレーションで定めた規程を信頼しあうことで相互に認証連携を実現している。この認証連携を利用して、SSOで学内だけでなく他大学や商用のサービスを利用出きる様になる。特に、学内電子ジャーナルを学外から閲覧する場合は、学認の認証を利用する事を求められることが多い。

3.2. システム

学認では、Shibboleth(SAML)を用いてSSOを実現している。学認システムは、Webアプリケーションリソースを提供するSP (Service Provider) 、認証を行うIdP(Id Provider)、及び多数のIdPから自分の所属する組織の認証を行うIdPを選択するためのDS (Discovery Service) からなる。IdPはバックグランドのデータベースとしてLDAPシステムを利用できる。そのため、学内統一認証によく用いられるLDAPサーバと比較的簡単に連携できる。

1. ユーザはブラウザを用いて利用したいSPにアクセスする
2. 最初に学認SPへアクセス時はIdPによって認証されていないので、認証を行う自組織のIdPを選択する為に、DSに転送される
3. DSの画面で自組織のIdPを選択すると、選択したIdPに転送される
4. 転送された自組織のIdPの画面で、IDとパスワードを入力する
5. IdPで認証を受けると、IdPとSP間で認証結果と認証された個人の属性情報のやり取りが行われる
6. ユーザはSPのサービスが利用出来る様になる。このときブラウザは、認証済みのcookieを受け取る

一度、認証を受けるとcookieによって認証情報が保存されるので、別のSPに接続した場合でも、ID、パスワードを入力せずにサービスを受けられるようになる。（図-1）

3.3. 利点

学認を利用する際に各大学が管理運用する必要最小限のシステムは、自組織に所属する人物を認証するためのIdPだけで、学内の統一認証システムを管理する場合と比べさほど大変ではない。

また、学内統一認証でよく利用されるLDAPサーバ(ShibbolethではIdPサーバに相当する)で認証を行う場合は、サービスを提供するWebアプリケーション(ShibbolethではSPサーバに相当する)にID、パスワードなどセキュアな情報を送り、Webアプリケーションサーバからサーバ(LDAPサーバにID、パスワードなどセキュアな情報を転送して認証を受ける。これに比べて、Shibbolethは自組織のIdPにID、パスワードなどセキュアな情報を送って認証を受けた後、各SPに対して氏名、所属など利用する際に必要な属性情報のみを提供するので、学外のSPに対してパスワード、及び個人情報が漏洩する危険性が低くなる。

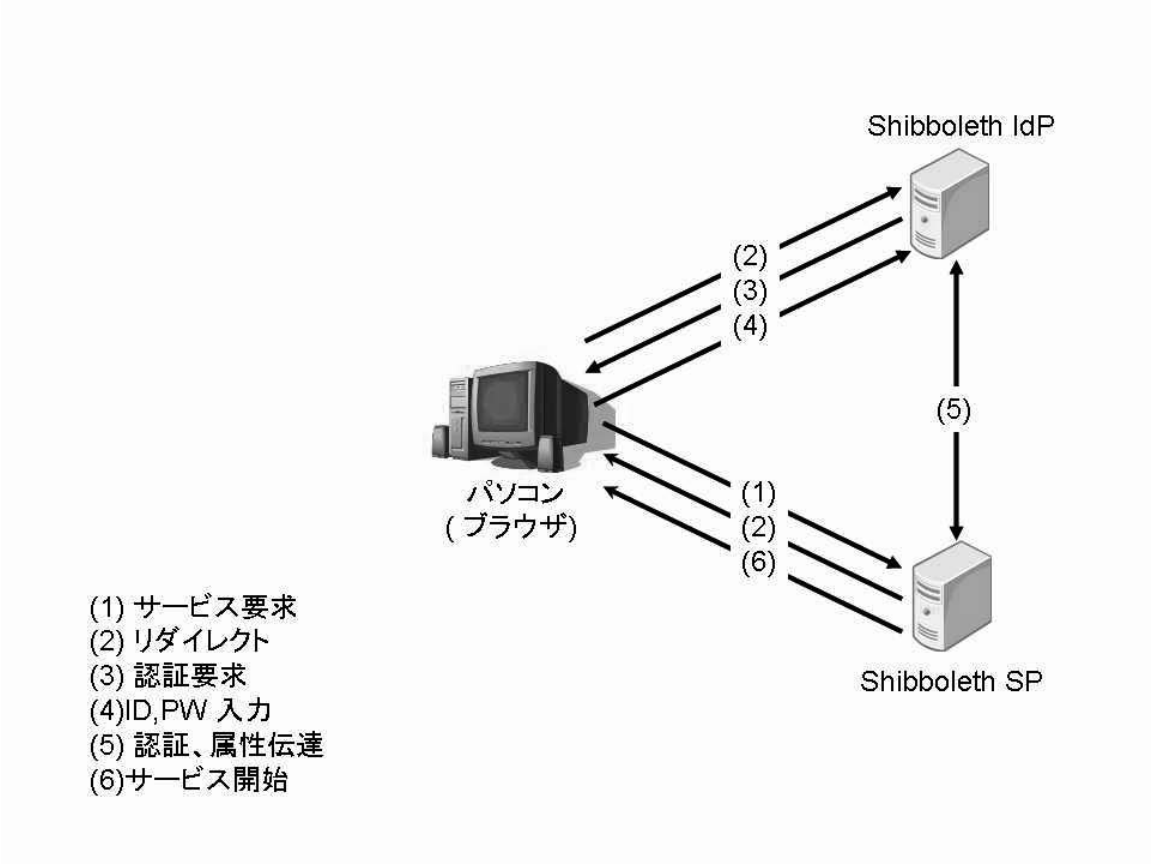


図-1 学術認証フェデレーション概念図(DS を除く)

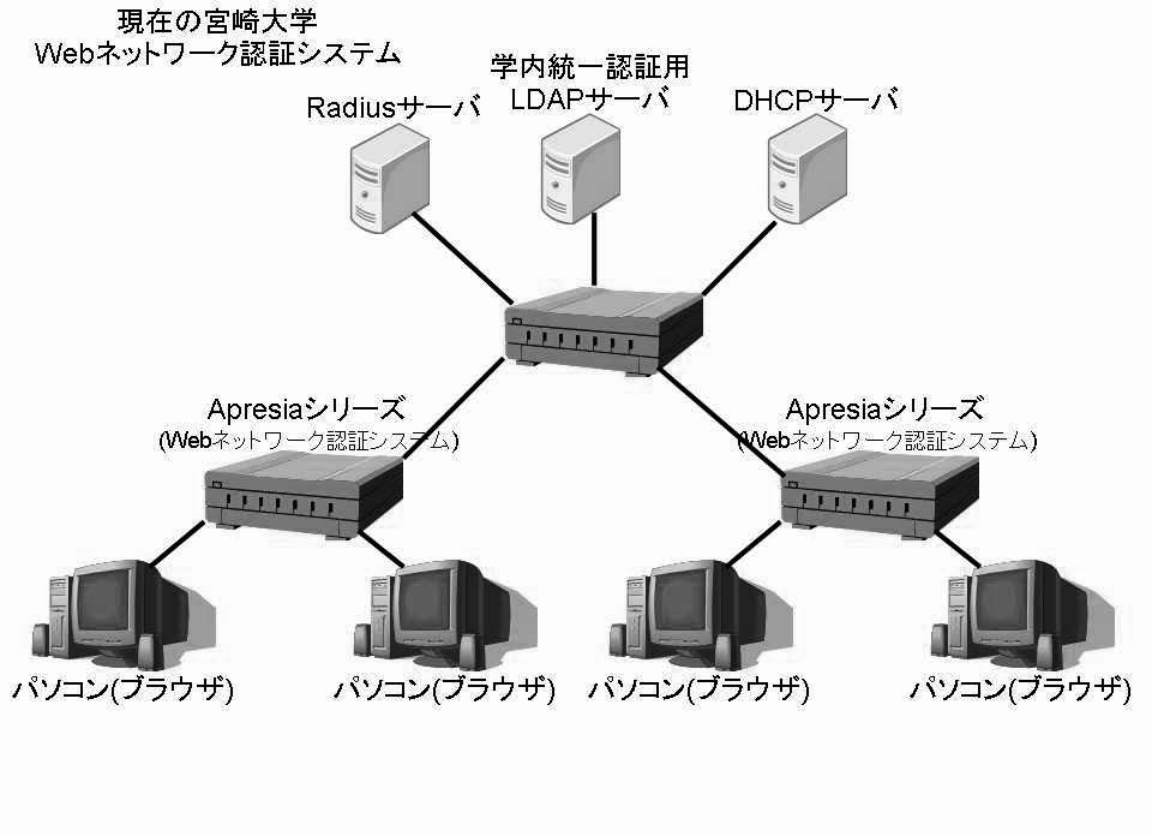


図-2 宮崎大学 Web ネットワーク認証システム

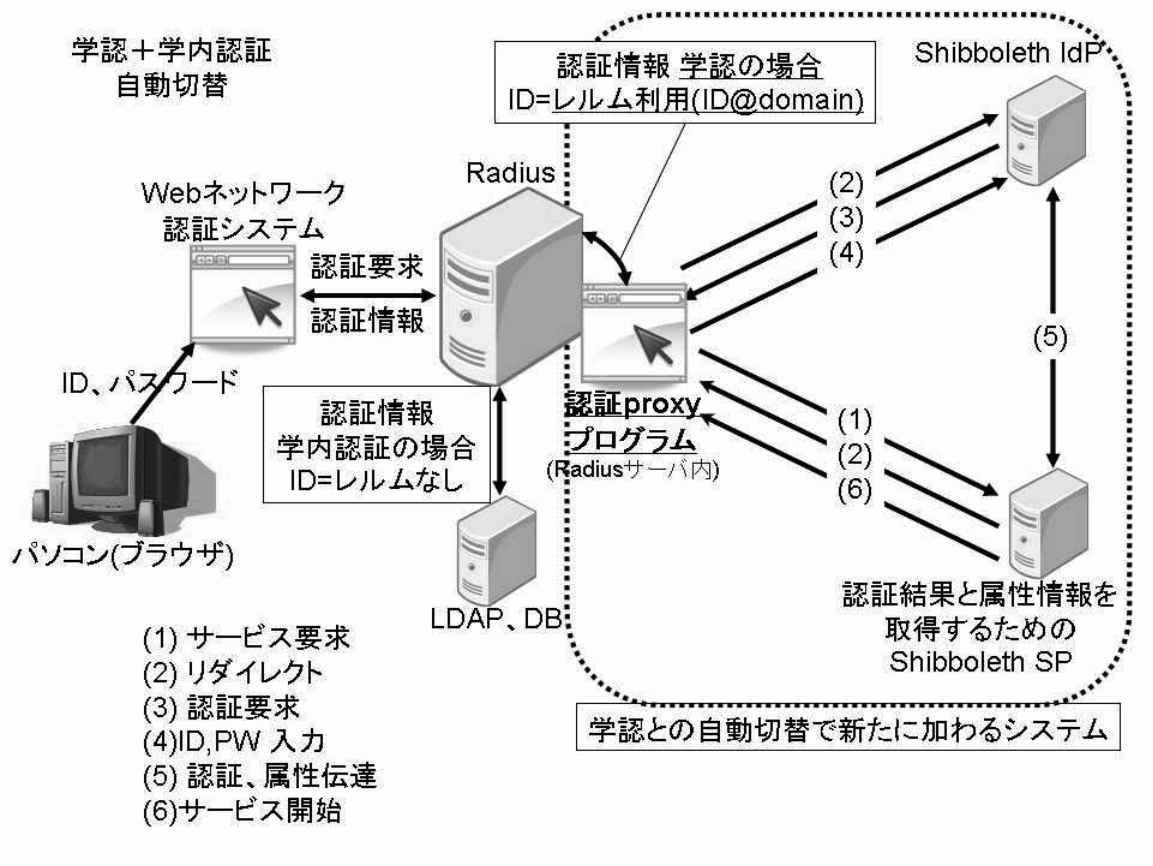


図-3 学認と宮崎大学統一認証の自動切替(DS を除く)

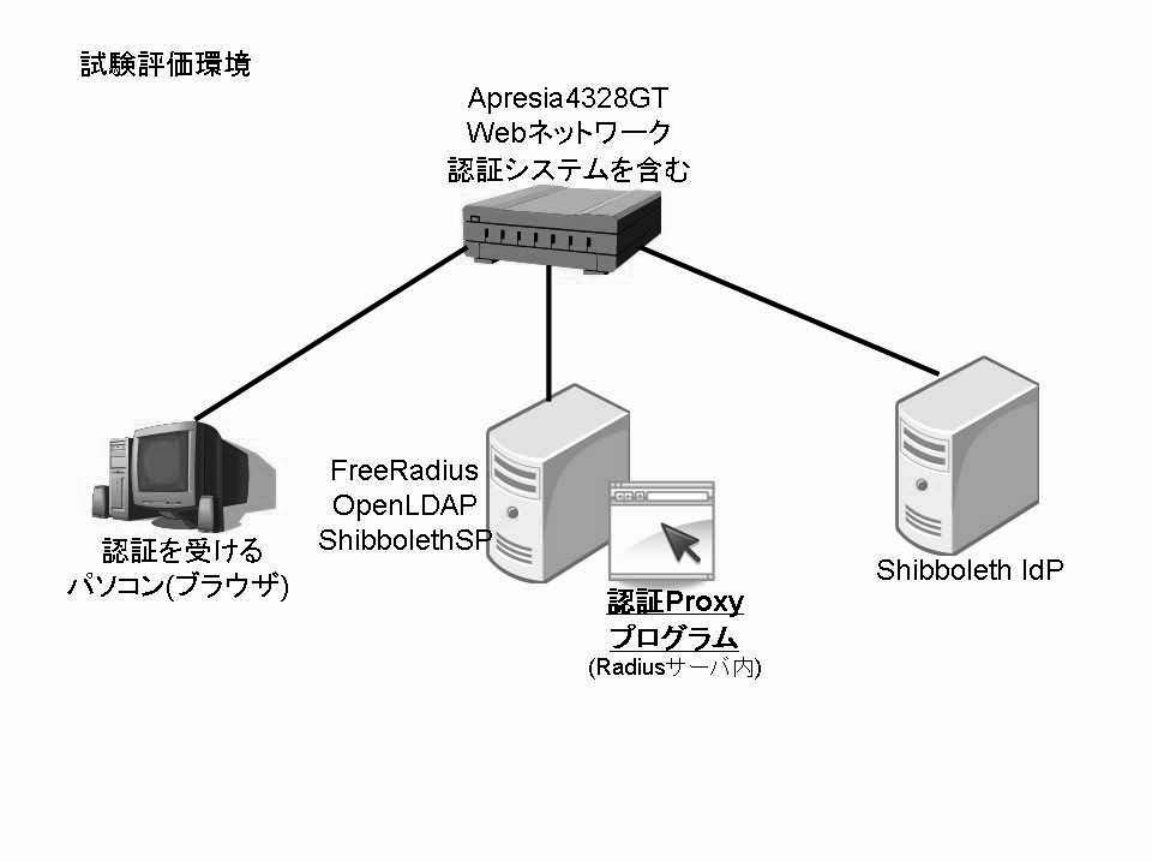


図-4 試験評価システム

学内統一認証システム(LDAPなど)単体では実現できないSSOを実現していることも利点として挙げられる。

3.4. 学認と宮崎大学統一認証

学認では、システム運用基準[2]で、認証を行う場合に自組織に所属している利用者のみを認証するように求めている。学認に参加している大学では、学内の統一認証IDを学認IDに使用している場合が多い[3][4]。また、統一認証によく利用されるLDAPシステム(Active Directoryサービスを含む)は学認認証用IdPシステムのバックグランドデータベースとして利用できるので、統一認証IDを学認IDとして利用することは自然である。しかし、宮崎大学では、以下の理由により学内統一認証IDとは別のIDを学認IDとして利用することにした。

1. 学内統一認証は主に学内からの利用を想定としている。電子ジャーナルの学外からの参照など、学認では、認証を行うIdPに学外から接続されることが予想される。学外から利用する場合、ホテルや空港など公共の場で提供されている安全でない可能性のある機器を利用したときにキーロガーによる情報流出等が想定されるため、現在の学内統一認証のセキュリティでは対応できない場合が想定される。学内統一認証を学外からの利用も想定したセキュリティレベルまで上げるためには、多大な経費がかかり現在では不可能である。
2. 学認では電子認証における保証レベル1を目指している[5]。今後もより高い安全基準を求められる可能性がある。学内統一認証IDを学認IDとして利用した場合、学認IDの保証レベルの上昇に伴い、学内統一認証のセキュリティレベルを上げることを求められる。しかし、学内事情から容易にセキュリティレベルを上げることが困難な場合も予想される。
3. 宮崎大学では、現在、SSOは実現されていない。将来、SSOを導入する時、学認IDに学内統一認証IDを利用していた場合、学認との連携を考慮してShibbolethで行うことが検討される。しかし、ShibbolethのSPに対応しているシステムは現在では少ないので、学内のSSOを実現するためには、多大な労力と経費が掛かる事が予想される。

4. 宮崎大学 Web ネットワーク認証システムにおける学認と学内統一認証の自動切替

4.1. 必要性

学内統一認証は一般に自組織に属する人物の認証を行う。しかし、ネットワーク利用時に学内統一認証で認証を行っている場合など、一時的に学外者にも提供できるIDを発行する必要に迫られる場合がある。

例えば、ネットワーク認証に学認を用いた場合、学外者の認証は学外者が所属する組織のIdPによって行われるので、臨時IDの発行等の管理業務が低減される。広島大学[6]や佐賀大学[7]は、学内の無線LANを学外者が利用する場合の認証に学認を利用している。しかし、学認で採用しているShibbolethのSAMLに対応しているシステムは少ないので、学内サービスを新たに学認SPとして公開する場合に、多大な経費と労力が発生する。また、宮崎大学の様に学内統一認証IDと学認IDが統一されていない場合、学内ユーザに対して学内統一認証以外の新しい学認IDの利用を呼び掛ける必要がある。学内ユーザは、新しいサービスが開始されたわけでもないのに、システムの認証が学認IDに変更になったことによって、新しいID、パスワードを覚える必要が出てくるなど利点は無い。

4.2. 宮崎大学 Web ネットワーク認証システム

宮崎大学のWebネットワーク認証は日立電線Apresiaシリーズのスイッチングハブによって行われている(図-2)。ネットワークに接続した際、パソコンからDHCPサーバへの接続要求が起きる。ネットワーク認証を行うスイッチングハブはDHCPサーバへの接続要求をリレーするので、パソコンはIPアドレス等の情報を得ることが出来る。しかし、まだ、認証は行われていないので、スイッチングハブから外のネットワークには接続できない。そこで、パソコン使用者は認証を行うためにWebブラウザを起動する。Webブラウザは起動時にブラウザに設定されているホームページへの接続を行う。認証スイッチングハブはこのhttp(https)要求をインターセプトして認証用ID、パスワードを入力する画面をブラウザに送信する。パソコン使用者はここで認証用のID、パスワードを入力すると、認証スイッチングハブはID、パスワードを外部のRadiusサーバに転送して認証を行う。認証スイッチングハブはRadiusサーバから送られた認証結果を基にネットワークへの接続の可否を決める。

4.3. Web ネットワーク認証システムの SP 化

既存のWebネットワーク認証システムを学認で認証する方法は、

１．Webアプリケーション自体をSP化する

２．SP化したリバースProxyを通してWebアプリケーションを認証する

方法が考えられる。佐賀大学では、１の方法すなわち既

存のSSOの入り口となる佐賀大学独自開発のWebネットワーク認証システムOpengateシステムをShibbolethに対応させた[7]。統一認証IDを学認IDとして利用した場合、どちらの方法でも利用可能である。

一方、統一認証IDと学認IDを分けた場合、WebアプリケーションをShibboleth SP化するとともに、統一認証用の認証システムと学認用の認証システムを自動的に判別して切り替える必要がある。宮崎大学のWebネットワーク認証システムはアプライアンスなので、ユーザがSP化することは困難である。一方、SP化したリバースProxyを利用する場合、統一認証で認証する場合はWebネットワーク認証システムに直接アクセスして認証を行い、学認で認証する場合はリバースProxy(SP)を通して認証を行うことが考えられる。しかし、Webネットワーク認証の場合、認証を受ける前はパソコンが認証システム以外には接続できないので、リバースProxy、DSや自組織の認証を行うIdPに接続して、認証を受けることが出来ない。そこで、３.Webアプリケーションが参照している外部の認証システムを利用して、統一認証と学認をシームレスに自動的に切り替える方法を提案する。

自動切替による認証は、Webネットワーク認証システムが参照する外部のRadiusサーバのレルムを利用して実現する。Webネットワーク認証システムは入力されたID、パスワードが統一認証用か学認用か判別する必要が無いので、アクセスするクライアントは、自動切替による認証の影響を受けない。

４．これ以外にも、eduroam仮名アカウント発行システム[8]の様に学認を用いてWebアプリケーションのアカウントを発行して利用することが出来る。しかし、この場合もWebネットワーク認証の前に、Webアプリケーションを利用するパソコン等がネットワークに接続出来ている必要があるので、宮崎大学のWebネットワーク認証システムには適さない。

4.4. システム概要

システム開発においては、Webネットワーク認証システムの変更を最小限に抑え、なおかつ学認SPとしてシステムを公開できることを目指した。

統一認証を行う場合、認証システムにLDAPを利用することが多いが、Radiusサーバを通して統一認証用LDAPサーバに接続、認証するシステムも多い。宮崎大学のWebネットワーク認証システムは外部のRadiusサーバを通して、学内統一認証LDAPサーバにアクセスし、認証を行っている。また、Radiusサーバは、レルム(例：ID@domain)を利用して認証を場合分けすることが出来る。本研究では、認証システムが参照するRadius のレルムを利用して、学認と学内統一認証の自動的な切替を行った。(図-3)

レルムを使わなかった場合は、従来通りにRadiusサーバを通して学内統一認証LDAPサーバにアクセスして認証を行う。

1. パソコンからブラウザを通してWebネットワーク認証システムにアクセスする
2. ブラウザ画面にID(レルムなし)、パスワードを入力する
3. ユーザが入力したID(レルムなし)、パスワードを受け取ったWebネットワーク認証システムは、認証を行うRadiusサーバにID、パスワードを転送する
4. Radiusサーバは受け取ったIDがレルムなしであることから、認証に学内統一認証を使うことを判断し、ID、パスワードをLDAPサーバに転送する。
5. LDAPサーバは、受け取ったID、パスワードから認証の可否を決定し、Radiusサーバに返答する
6. Radiusサーバは受け取った認証結果をWebネットワーク認証システムに返答する
7. Webネットワーク認証システムは認証結果を基にネットワークへの接続の可否を判断する。

一方、レルムが用いられた場合、RadiusサーバはWebネットワーク認証システムから渡されたID、パスワードをRadiusサーバにインストールされている外部プログラムに渡して認証を任せる。この外部プログラムが学認の各システムと通信して認証結果を得え、この認証結果をRadiusサーバに転送して認証を行う。つまり、この外部プログラムは、学認システムとRadiusサーバとの間で認証をProxyする機能を持つ。

先に学認での認証方法の方法で説明したように(図-1)、学認のサービスを利用する場合、Webブラウザを用いてSP、IdP、DSにアクセスする。この外部プログラム(認証Proxyプログラム)は、Radiusサーバにインストールされ、ID、パスワードをRadiusサーバから学認システムへ中継するプロキシとしての機能を持ち、認証情報をWebアプリケーションである学認システムとやり取りするため、http(https)クライアントとしての役割を持つ。

また、SPはIdPから認証結果と必要な個人の属性情報を取得する。本システムのSP(認証情報取得SP)は、認証Proxyプログラムと対話して、認証後必要な属性情報を認証Proxyプログラムに提供する。

認証Proxyプログラムは、http(https)クライアントソフトであり、一般のブラウザと同じように、

1. ヘッダー(cookie等)、html文を取得
2. リダイレクトの処理
3. html文の解析。接続先URL、入力フォームを取得
4. 1.に戻る。入力フォームがある場合は、入力データを渡す

を行う。実際のレルムを用いた場合の認証プロセスは、以下のとおりになる。

1. パソコンからWebネットワーク認証システムにアクセスする
2. ブラウザ画面にID(レルムあり)、パスワードを入力する
3. ユーザが入力したID(レルムあり)、パスワードを受け取ったWebネットワーク認証システムは、認証を行うRadiusサーバにID(レルムあり)、パスワードを転送する
4. Radiusサーバは受け取ったID(レルムあり)から認証に学認を使うことを判断し、ID、パスワードを認証Proxyプログラムに転送する
5. 認証Proxyプログラムがレルム(ID@Idpのdomain)からIDおよびIdPのドメインを取得する
6. 認証Proxyプログラムが認証情報取得SPにアクセスする
7. 認証を受けていないので、DSにリダイレクトされ、認証Proxyプログラムは、DSのhtml文からIdPのリストを取得する
8. 認証Proxyプログラムは、レルムから得られた大学ドメインを参考に7.で取得したIdPリストからIdPのURLを選択し、選択したIdPにアクセスする
9. 認証Proxyプログラムは、IdPからID、パスワードを入力するためのフォームを取得する
10. 認証Proxyプログラムは、Radiusサーバから送られたID、パスワードをIdPに送信し、認証を受ける
11. 認証結果がIdPから認証情報取得SPに送られ、認証Proxyプログラムは、認証結果と属性情報を認証情報取得SPから取得する
12. 認証Proxyプログラムは、受け取った認証結果及び属性情報をRadiusサーバに返答する
13. Radiusサーバは受け取った認証結果をWebネットワーク認証システムに返答する
14. Webネットワーク認証システムは、認証結果を基にネットワークへの接続の可否を判断する。

以上の様に、自動切替を行った場合でも、宮崎大学のWebネットワーク認証システムを利用するパソコンは、認証画面にID(レルムあり、レルムなし)とパスワードを入力するだけでネットワーク認証を受けられ、SP化の前後で利用形態に変化はない。

また、この認証自動切替は、IDにレルムを利用するときに特段の制限を設けていない。宮崎大学は学認の運用フェデレーションでIdPを立ち上げているので、学内者がIDとしてレルム(学認ID@miyazaki-u.ac.jp)を入力して学認の認証を受けることも可能である。

5. 試験評価

この認証Proxyプログラムを使って、実際の宮崎大学のWebネットワーク認証システムを模した独立した試験評価環境を構築して、非常に簡単な試験評価を行った(図-4)。Webネットワーク認証システムとして、現在宮崎大学で使われている日立電線Apresiaスイッチングハブを用いた。また、学認の代わりとして、Idpと認証情報取得SPからなるローカルフェデレーションを作った。比較のために、レルムを用いないOpenLDAPを使った認証システムも立ち上げている。試験評価で使用したシステムは、以下の通り。

- Webネットワーク認証システム Apresia4328GT
- サーバ1(認証Proxyプログラム及び認証情報取得SPを含む):CentOS 5.8
  FreeRadius 2.1.12
  OpenLDAP 2.3.43
  Shibboleth SP 2.4.3
- サーバ2:CentOS 5.7
  Shibboleth IdP 2.3.3

この評価環境で認証を行ったところ、OpenLDAPを使った認証と比べてほとんど遅延も無く学認を模したローカルShibbolethフェデレーションを使ったシステムでも認証できることが確認できた。

但し、この試験評価環境は単独のパソコンからのアクセスであるので、実際のネットワーク環境でネットワークによる遅延、Webネットワーク認証システムからの認証要求が集中するRadiusサーバの遅延、学認システムへの認証結果の遅延を考慮する必要がある。更に、現在の認証ProxyプログラムはRadiusサーバへ複数の認証要求が来ることを考慮していない。

6. まとめ

宮崎大学のWebネットワーク認証において、アプライアンス製品であるWebネットワーク認証システムが参照する外部のRadiusサーバのレルムを利用し、Radiusサーバの外部プログラムである認証Proxyプログラムと認証情報と属性を認証Proxyプログラムに渡すSPを作成することで、学認と学内統一認証を自動的に切り替えてシームレスに認証出来る様になった。これにより、Webネットワーク認証システムを利用するパソコンのアクセスが制限される状況であっても、安価に、アプライアンス製品であるWebネットワーク認証システムに影響を与えずに学認のSP化することができるようになった。

本研究では宮崎大学のWebネットワーク認証システム

をSP化するシステム開発を行った。しかし、本研究ではWebアプリケーションであるWeb認証システムに対しては一切変更を加えていないので、Webアプリケーションが外部認証システムとしてRadiusサーバを利用しているのであれば、同様にWebアプリケーションをSP化できると思われる。このSP化手法は学認と学内統一認証を自動的に切り替えて利用する場合だけでなく学内統一認証IDを学認IDとして利用している場合でも同様に利用でき、第４のSP化手法として有効である。

学認では、個人情報保護の観点から、個人が自分の属性情報をSPに送付するかどうかを選択できるuApprove.jpというプログラムを用意している。これは、IdPにアクセスした際、アクセスする本人がブラウザを使って送付する属性情報を選択する。Webアプリケーションの認証プロセスを利用して認証Proxyプログラムを走らせるので、ID、パスワード、ドメインとあらかじめ決められた情報しか取得、送信することが出来ない。よって、uApprove.jpには対応できない。今回の認証Proxyプログラムを利用したSPを運用する組織が必要最小限の個人情報の取得を心がける必要がある。

本研究では、宮崎大学のWebネットワーク認証をモデルとした試験環境での運用だけで、まだ実環境での負荷試験などは行っていない。今後は、様々な実環境でも十分に運用できるプログラムに仕上げていく必要がある。

参考文献

[1]学術認証フェデレーション　学認　GakuNin、
https://www.gakunin.jp/ja/
[2]学術認証フェデレーション運用基準(Ver.1.2)、
https://www.gakunin.jp/docs/files/GakuNin_System_SpecV1.2.pdf
[3]ゲスト利用者のネットワーク認証に活用／広島大学、
https://www.gakunin.jp/docs/files/12hiro.pdf
[4]江藤博文,大谷誠,渡辺健次,只木進一:Opengateとシングルサインオン,電子情報通信学会技術研究報告.SITE, 技術と社会・倫理, Vol.108, No.459, pp.259-264(2009)
[5]学認参加機関の各IdPの運用に関するアンケートの実施について：世界標準に適合したトラストサークルの確立に向けて、https://www.gakunin.jp/docs/fed/loa
[6]広島大学情報メディア教育センター:学内情報コンセント、
http://www.media.hiroshima-u.ac.jp/services/hinet/cup#anchor-3
[7]佐賀大学情報基盤センター：学認向け無線LANゲスト利用サービス(Opengate)、
http://www.cc.saga-u.ac.jp/gakunin/
[8]SAML連携によるeduroam仮名アカウント発行システムの実装、
https://upki-portal.nii.ac.jp/docs/files/SSO_report_2009kyoto.pdf

学内の様々な運用形態に対応したコンパクトなアカウント管理システムの実現

Realization of a Lightweight Account Management System Supporting Campus Member of Various Status

瀬川大勝 †，辻澤隆彦 †，石橋みゆき †

Hirokatsu SEGAWA†, Takahiko TSUJISAWA†, Miyuki ISHIBASHI†

{hiroka,t-taka,saji}@cc.tuat.ac.jp

東京農工大学総合情報メディアセンター †
Information Media Center, Tokyo University of Agriculture and Technology†

概要

東京農工大学総合情報メディアセンターは，提供する学内情報サービスに対応したアカウント管理システムを構築し，統一認証システムを通じて，アカウントの一元管理を進めている．大学には，周知のように，教職員や学生以外にも様々な身分の構成員が存在するが，東京農工大学では，これら多種多様な構成員の管理は，各部署で個別に行われている．アカウント管理システムは，アカウントの基礎データとなる各種個人情報を元にサービスやシステムごとに必要となるアカウントデータの生成を行う必要があるが，前述のように，各種個人情報の提供元は構成員の種別により異なり，また，管理形態が統一されておらず，時として非定形な例外処理を行う必要がある．筆者らは，各種個人情報を提供するデータベースを改修をすることなく，様々なサービスやシステムに対応することができるコンパクト（軽量）なアカウント管理システムの設計・構築を進めてきた．本稿は，東京農工大学におけるアカウント管理システムを中心とした統一認証システムの全体像を示すと共に，アカウント管理システムそのものについて詳述するものである．

キーワード

アカウント管理，統一認証システム，学内情報サービス

1 はじめに

近年，大学の情報化が進むに従って，学内には，様々な組織が提供する多種多様な情報サービスが存在するようになった．一般に情報サービスを利用するためには，適切な認証・認可のプロセスを経ることが不可欠であるので，その基礎となるアカウント管理の仕組みが重要であることは広く認識されており，今まで様々な工夫が行われてきた [1–10].

理想的には，一元的なアカウント管理に基づく統一された認証基盤があれば，利用者は自身に付与された唯一つのアカウントを用いて，一度の認証でその身分に応じた（その身分で許されている）複数の情報サービスが受けられることになる．また，情報サービスの提供者としても，システム個別のアカウントの維持・管理から開放され，サービスの追加や拡張などが容易となる．

しかし，大学は，一般的な企業などとは異なり，アカウントの基礎データとなる人事や学籍などの各種個人情報（以下，アカウント基礎データと呼ぶ）の管理・提供元は様々であり，それぞれが独自のポリシーで運用していることが多い．また，このことは，アカウント基礎データを利用する情報サービスの管理・提供元についても同じことが言え，これらが，学内での各種データのや

り取りを難しくしている．東京農工大学（以下，本学と呼ぶ）のアカウント基礎データの管理元とその身分で利用可能な主要学内情報サービスの関係を表 1 として示す．

本学では，以前からアカウント基礎データを保持する統合基盤データベースおよびこれに連携する統一認証システムの整備を進めてきたが，アカウント管理の一元化および認証システムの統一化は完全に達成されておらず，大きな問題として，次の二つがあった．

1. アカウント基礎データの構造や表現形式の変化に対する追従が困難
   大学には様々な身分の構成員（情報サービスの利用者）が存在し，近年，その職種などの身分を表す属性は，次々に変更される（追加・統廃合など）傾向がある．加えて，大学と直接の雇用関係を持たない職員や書類上の学籍が他大学となっている学生[1]などのいわゆる「例外」の存在も多種多様なものが次々に生まれ，それらは各部署が独自に管理している．結果として，アカウント基礎データの構造や表現形式が度々変更されており，欲しい情報を得るには，複数の部署からデータを受け取り，様々な加工（抽出，結合，変換など）をする必要があった．
2. 情報サービスの変化に対する追従が困難
   情報サービスは，ニーズに応じてその内容や形態が変化することが普通であり，たとえば，新しいサービスが追加されたり，既存のサービスの統廃合や拡張などが起こり得る．しかし，主にコストの問題で，互換性に十分配慮できない場合が多く，必要となるデータの種類や表現形式，プロトコルなどが変更されることがあり，その都度，対応作業が必要となっていた．

本学においては，各部署が独自に管理しているデータベースの改修やそれらの統合基盤データベースへの統合のような，これらの問題の抜本的な解決は，予算や組織内の歴史的な経緯（各部署でのシステム更新のタイミングの違いなど）といった様々な制約から，現状では非常に難しい状況である．そのため，システム間の連携処理とアカウント基礎データを元に各種情報サービス固有のデータ生成を行うための「各種システムの良き仲介役」となるようなアカウント管理システムが必要とされていた（図 1）．

このような背景から，本学の情報系センターである総合情報メディアセンター（以下，本センター）は，2010 年度末に教育研究用情報システムのリース期間終了に伴う大規模なシステム更新 [11] を契機に，本センターが運用するアカウント管理システムの改修を進めてきた．

改修の目標は，学内で様々な形態で運用されるアカウント基礎データベースや情報サービスに対応可能とすることであり，この時，将来のシステムの増加や更新などにも対応し易いように，アカウント基礎データのレプリケーションはあえて行わず，柔軟性のある簡潔なデータスキームを設計し，コンパクト（軽量）であることを重視した．結果として，その後の事務用 PC システムの更新などにおいて，その都度，使用データの追加や変更が必要となったが，アカウント管理システムとしては大きな改修をすることなく，対応することができた．

本稿は，事務用 PC システムの更新や例外的な一時アカウントの提供といった実例を通して，本センターが実現したコンパクト（軽量）なアカウント管理システムの詳細を記述するものである．最初にシステムの全体像を掴むために，本センターが運用する統一認証システムおよび周辺システムの全体を示し，その中でアカウント管理システムの位置付けや役割を述べる．次に，その後に起こった事務用 PC システム更新に対するアカウント管理システムの具体的な対応について述べる．さらに，例外的な一時アカウント提供のための特別処理を述べ，最後に，アカウント管理システムの負荷統計データに触れて，まとめとする．

2 統一認証システムの構成とアカウント管理システム

2.1 システムの概要

本節では，アカウント管理システムの機能や特徴，および統一認証システムとそれを利用する周辺システムの中でのアカウント管理システムの位置付けや役割について述べる．

1 章で述べたように，本センターでは，統合基盤データベースからアカウント基礎データを取得する機能と情報サービスごとに必要となるアカウントデータを発生する機能および非定型な（人手による）例外処理に対応する機能を持つ，アカウント管理システムの設計・構築を行い，統一認証システムの中で，アカウントの一元管理を進めてきた．

このアカウント管理システムは，電子メールや WWW サーバなどの各種情報サービスのためのアカウントの申請を WWW ブラウザから受付け，アカウント基礎データとパスワード情報に加え，情報サービスごとに必要となる付加データを認証システム（LDAP および Active Directory により構成される）に登録することで申請者

[1] 具体的には，本学が構成校の一つである岐阜大学連合獣医学研究科（本学以外の構成校は，帯広畜産大学と岩手大学）に進学した学生が該当し，書類上の学籍と実際の活動場所が異なる場合がある．

表- 1: アカウント基礎データの管理元と利用可能な情報サービスの関係

分類	大学と直接雇用関係がある教職員	大学と直接雇用関係のない教職員 (A)	大学と直接雇用関係のない教職員 (B)	名誉教授･特別栄誉教授	一般の学生	岐阜大学連合獣医研究科の学生
管理元	人事労務課	学術情報課	学術情報課	人事労務課	学生総合支援課	岐阜大学連合獣医研究科
主な利用サービス	教職員ポータル，財務・会計システム，共有フォルダ，学内ネットワーク，電子メール，学務情報システム，演習用 PC システム	教職員ポータル，財務・会計システム，共有フォルダ，学内ネットワーク，電子メール	学内ネットワーク，電子メール	学内ネットワーク，電子メール	学内ネットワーク，電子メール，学務情報システム，演習用 PC システム	学内ネットワーク，電子メール，学務情報システム，演習用 PC システム
人数（概算）	1700	40	140	260	6000	45

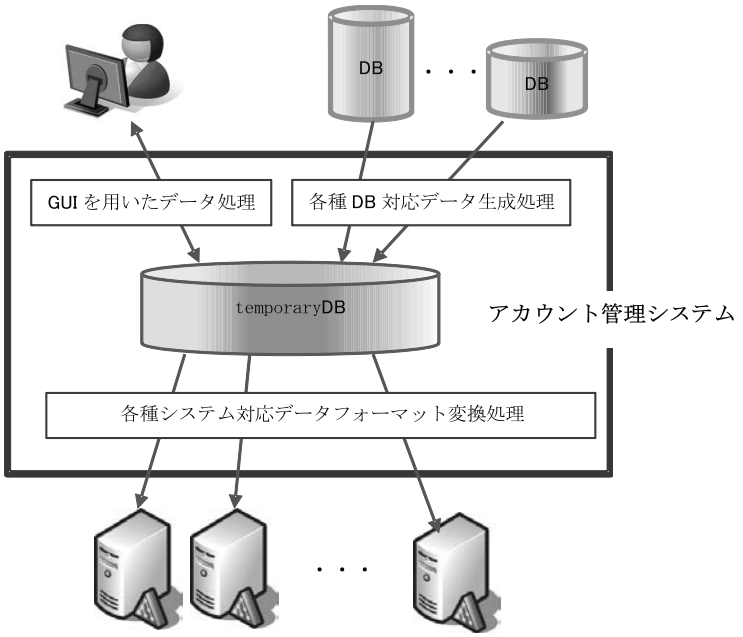


図- 1: アカウント管理システムの概念図

に対してアカウントを発行する機能を持っており，次の特徴がある．

1. アカウント基礎データを統合基盤データベースから入手し，LDAP，Active Directory，学術認証フェデレーションなどの各種認証システムに対応可能なデータの生成
2. 提供元のデータベースの構造や運用規則が変化しても対応し易いように，アカウント基礎データのレプリケーションは行わず，簡便な一時データベースの使用（図 1 の「temporary DB」に対応）
3. 統合基盤データベースのデータを活用できない，例外事例についての対応も可能としたデータ構造による LDAP データの生成
4. サービス対象となる学内情報システムの変更に対応できる柔軟性のあるデータ構造を持たせた登録用データフォーマットによる LDAP データの生成

図 2 および図 3 に統一認証システムとそれを利用する周辺システムを示す．アカウント管理システムでは，演習用 PC システム，認証 L2 スイッチ（学内認証ネットワーク），教職員ポータルなどの学内情報サービス利用 ID とパスワードが管理されていて，統一認証システムの枠組みの中で，同一 ID・パスワードでの利用が可能となっている．

本センターでは，この統一認証システムを次に示す処理により運用している．また，アカウント管理システムは，先に述べた特徴を実現するために，レプリケーションデータを持つことはせず，柔軟性のあるデータ構造を持たせた登録用データフォーマットを設計し，積極的に活用している．登録用データフォーマットは，CSV ファイルで表現され，用途に応じて二種類の形式を定義した（以下，その二種類の形式を Fromat-A, Format-B と呼ぶ）．

1. LDAP 系アカウント：
   (a) アカウント管理システムは，統合基盤データベースから入手したアカウント基礎データを基に CSV ファイル（Format-A： LDAP データ）を自動的に作成する（ただし，2.4 節で述べる「人手による例外データの処理」のために，作成のトリガは人間がかけている）．
   (b) この CSV ファイルを引数として，統一認証運用管理サーバ (LDAP Manager) の Java アプリケーション（ELM インターフェース）を自動的に実行する．この処理により，CSV ファイルに記載されたアカウント情報が統一認証運用管理サーバに自動的に提供される．
   (c) 提供されたアカウント情報は，メタディレクトリサーバに登録後，それぞれのシステムに自動的に登録される．登録先は図 3 に示したように LDAP 認証サーバ，ドメインコントローラ（Active Directory），図書館業務システムなどである．
2. 電子メールアカウント：
   (a) アカウント管理システムは，申請に応じて，統合基盤データベースから入手したアカウント基礎データを基に CSV ファイル（Format-B：メール・メーリングリスト）を自動的に作成する．
   (b) この CSV ファイルをメールアカウント制御サーバに自動的に渡す．
   (c) この CSV ファイルを引数として，メールアカウント制御サーバがメールサーバ（図 3 の A-cloud）に対して電子メールアカウント情報の追加・更新・削除を自動的に行う．なお，ここでの削除とはデータの無効化であり，通常は，データの物理的削除は行わないこととしている．

2.2 統合基盤データベースとアカウント管理システム

本節では，2.1 節で述べたアカウント管理システムが統合基盤データベースから入手するアカウント基礎データとアカウント管理システムが保持する一時データベースの内容について記述する．

統合基盤データベースから入手するアカウント基礎データは，次の三つのテーブルで表現されていて，これらのテーブルにより，たとえば，職員 A は，学術情報課に所属している非常勤職員である，といったアカウント基礎データが表現される．

1. 個人番号や氏名などの基礎的な情報が保持されているメインテーブル
   個人番号（学内でユニーク），氏名，連絡先（電子メールアドレスや電話番号など），統一認証システムパスワードなどの 47 種類の情報
2. 職種テーブル
   職種（教授，部長など）や職制（常勤，非常勤など）に関する最大 24 種類の情報（兼務などに対応するため，複数の職種や職制を許している．）
3. 所属テーブル
   所属（大学院，学部，部，課など）に関する最大

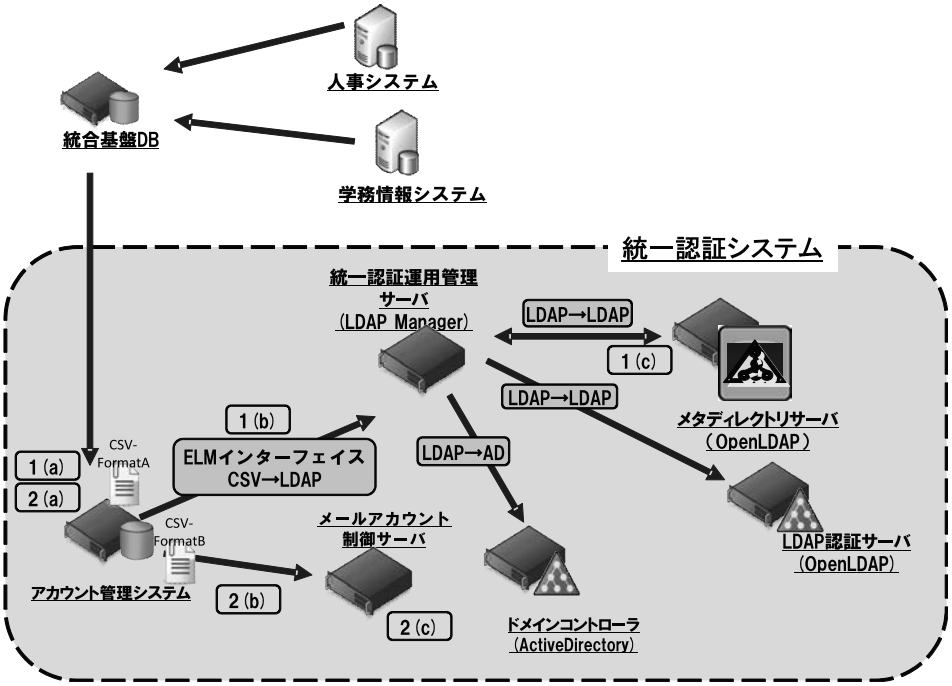


図- 2: 統一認証システム

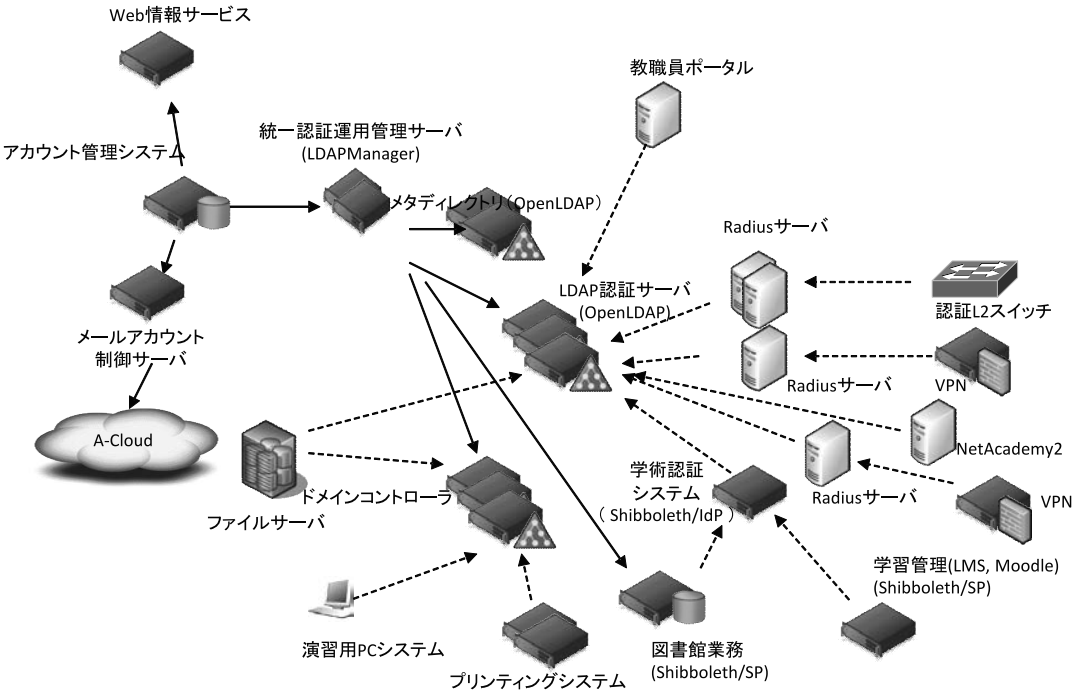


図- 3: 統一認証システムと周辺システム

90 種類の情報（兼務などに対応するため，複数の所属を許している.）

アカウント管理システムが保持する一時データベースは，統合基盤データベースから入手したアカウント基礎データを抽出・加工することにより自動的に生成され，メインテーブル関連では 26 種類，職種テーブル関連では 6 種類，所属テーブル関連では 50 種類の情報を保持している．これらのデータは，前述の CSV ファイルの作成などに用いられるが，ここで一度データを整形することで，提供元のデータ構造の変化に対する CSV ファイルの作成工程への影響を小さくしており，統合基盤データベースの構造の変化などに対応し易くしている.

さらに CSV ファイルも，主として職種データを基準として[2]，あらかじめ定められたルールに従って自動的に作成される[3].

2.3 登録用データフォーマット

2.1 節で述べたように，アカウント管理システムは，アカウント基礎データを統合基盤データベースから入手し，簡便な一時データベースと，各種システム間の登録用データフォーマットとして柔軟性のあるデータ構造を持つ CSV ファイルを積極的に活用することで，できるだけ例外に対応可能で，コンパクト（軽量）なシステムを実現した．これは，提供元のデータベースの構造や提供先のサービスが変化し，例外が発生した場合でも，一時データベースの構造に大幅な改修を加えることなく対応可能とするためである（CSV ファイルの構造の変更は比較的行い易いため）．また，結果として，一時データベースの構造を簡便に保つことも可能となった．本節ではこの登録用データフォーマットのデータ構造の詳細について述べる.

登録用データフォーマットは，用途に応じて Format-A と Format-B の二種類の形式を定義しているが，Format-A は LDAP データを扱い，統一認証運用管理サーバ (LDAP Manager) へ送付される．一名につき一ファイルであり，新規登録，更新および廃止時のそれぞれのタイミングで送付している．含まれるデータは次の 91 項目から成り，これを図 4 として示す.

- 「新規登録」,「更新」,「廃止」を示す文字列 (ADD, MOD, DEL)
- 個人識別番号とパスワードおよび名前やメールなどの 14 項目
- 職種関連情報の 6 項目

[2]職種により，利用できるサービスの種類などが定まるためである.
[3]2.1 節で述べたように，作成のトリガは人間がかけることとしている.

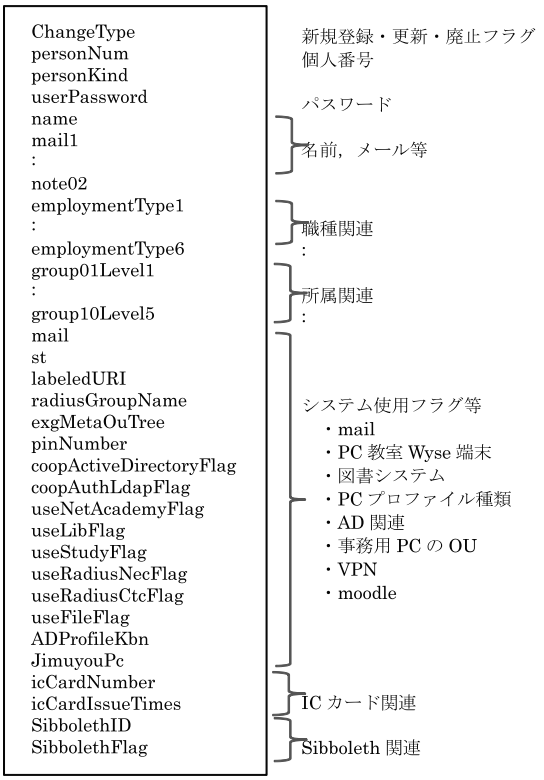


図- 4: 登録用データフォーマット：Format-A（LDAP データ）

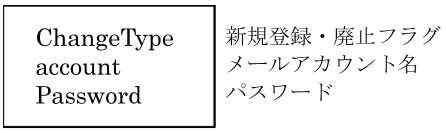


図- 5: 登録用データフォーマット：Format-B（電子メールの場合）

- 所属情報の 50 項目
- 各種システムの使用の可否等を示す 16 項目（職種関連情報と所属情報から生成）
- IC カード関連情報と Sibboleth 関連情報 4 項目

一方，Format-B は，電子メールまたはメーリングリストデータを扱い，メールアカウント制御サーバへ送付される．電子メールの場合は，新規登録や廃止時，およびパスワード変更時のそれぞれのタイミングで送付する．メーリングリストの場合は，新規登録や廃止時，およびリストに含まれるメンバの変更時のそれぞれのタイミングでデータを送付する．含まれるデータは，新規登録または廃止を示すフラグ，電子メールアカウント名，パスワード，管理メールアドレス，メーリングリストメンバであり，電子メールの場合を 図5，メーリングリストの場合を図 6 として示す.

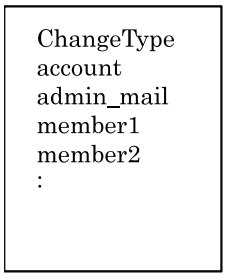


図- 6: 登録用データフォーマット：Format-B（メーリングリストの場合）

2.4 LDAP データに関する特別処理への配慮

2.3 節で述べたように，アカウント管理システムは，簡便な一時データベースと柔軟性のあるデータ構造を持たせた登録用データフォーマットを活用することで，できるだけ例外に対応可能なシステムとしたが，実際の運用上は，例外のさらに例外とも言うべき事例が発生することが避けられず，特別な処理が必要となる場合がある．具体的には，提供元に不正なデータが混入していて処理が中途で止まる，または，誤った情報が登録される，さらには，データ更新時に例外処理していた部分を誤って定形処理してしまうことなどが想定される．

これらのことに対応するために，本システムでは LDAP データの登録や更新時に各種データのチェックを行い，また，人間による処理の介入などの特別な処理をあらかじめ想定して実装した[4]．人手による処理は誤りを混入させるリスクがあるが，データ検索や変更のための WWW インターフェースを用意し（図 7），過去に行なわれた例外処理を強調表示するなどして（もちろん，この段階で行った処理も例外処理として保持される），ミスを起こしにくいように配慮している．また，この時，統一認証運用管理サーバ上の LDAP データを直接変更することはせず，あくまで，アカウント管理システム上の一時データベースに保持されている生成データに対して処理を行うことで，処理に誤りがあった場合の被害の拡大を防いでいる．具体的には，各段階において次のように対応している．

1. 登録・更新時のデータ確認
   生成した LDAP データと現在の LDAP データを比較し，変更および新規のデータを可読性のある形式で出力している．統合基盤データベースから得られた情報に不正や不具合などがあり処理が止まった場合は，この確認データを参照することで対応する．

2. 例外処理されたデータの上書き確認
   更新により差分を反映する場合，すでに例外処理されている部分を確認し，該当すれば変更を加えない（この例外処理部分をさらに例外処理する場合は，次の「人手による例外データの処理」で対処する）．

3. 人手による例外データの処理
   確認の結果，人手による例外処理する必要があれば，データ提供元の担当者がアカウント管理システム上に生成された LDAP データを編集する．

これまでに述べたアカウント管理システムの機能や特徴をまとめ，図 8 として示す．図中の二つのデータベースは，MySQL で実装されている．様々な処理を担当するプログラムや WWW インターフェースは，PHP で記述されており，WWW サーバは，Apache HTTP Server を採用した[5]．

3 事務用 PC システム更新への対応

3.1 事務用 PC システム更新の背景

2011 年度末から，本学の事務組織に所属する職員が使用する PC システムが段階的に更新されることになった．

これまで，事務用 PC システムは各部署で独自に調達・運用されてきたものが大半であったが，コンプライアンスやセキュリティ維持，メンテナンスなどの観点から，本学事務組織の情報システム担当部署が一括して管理できるようなシステムとなるように設計が進められた．初年度は，基礎となるサーバなどの管理システムの機能追加・改修および約 20 台のクライアント PC の導入から始めることとなった．最終的には，約 300 台のクライアント PC を更新する予定となっている．

このシステムは，本センターですでに運用が開始されていた電子計算機システム [11] で提供するサービスとの連携が重視され，認証の共通化や共有ファイルサーバの利用などの要件があり，既存の Active Directory を利用できることが必要とされた．本センターでは，これに対応するため，設計・構築支援を行うと共に，アカウント管理システムを中心として，LDAP や Active Directory 関連の改修も行うことになった．図 9 にシステム構成概念図を示す．

3.2 改修内容の概要

本センターがすでに管理・運用している Active Directory のドメインコントローラ内に新たに事務用 PC シス

[4] なお，電子メールデータについては，本学では運用が一律に行われているため，例外の発生頻度が極めて低く，特に配慮はしていない．

[5] なお，一時データベース（図中の「temporary DB」）を囲む太枠の中に含まれるものと申請アカウント管理データベース（図中の「申請アカウント管理 DB」）の一部は，本センターでの内製であり，それ以外は，仕様を元にした外製である．

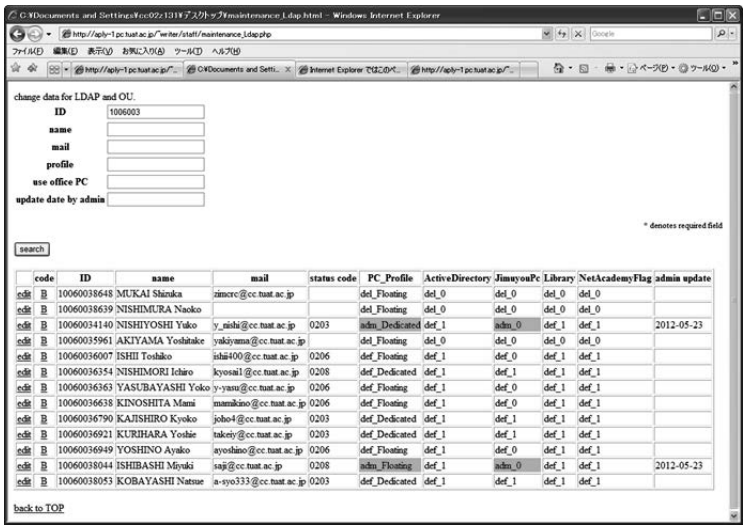


図- 7: 特別処理のための WWW インターフェース

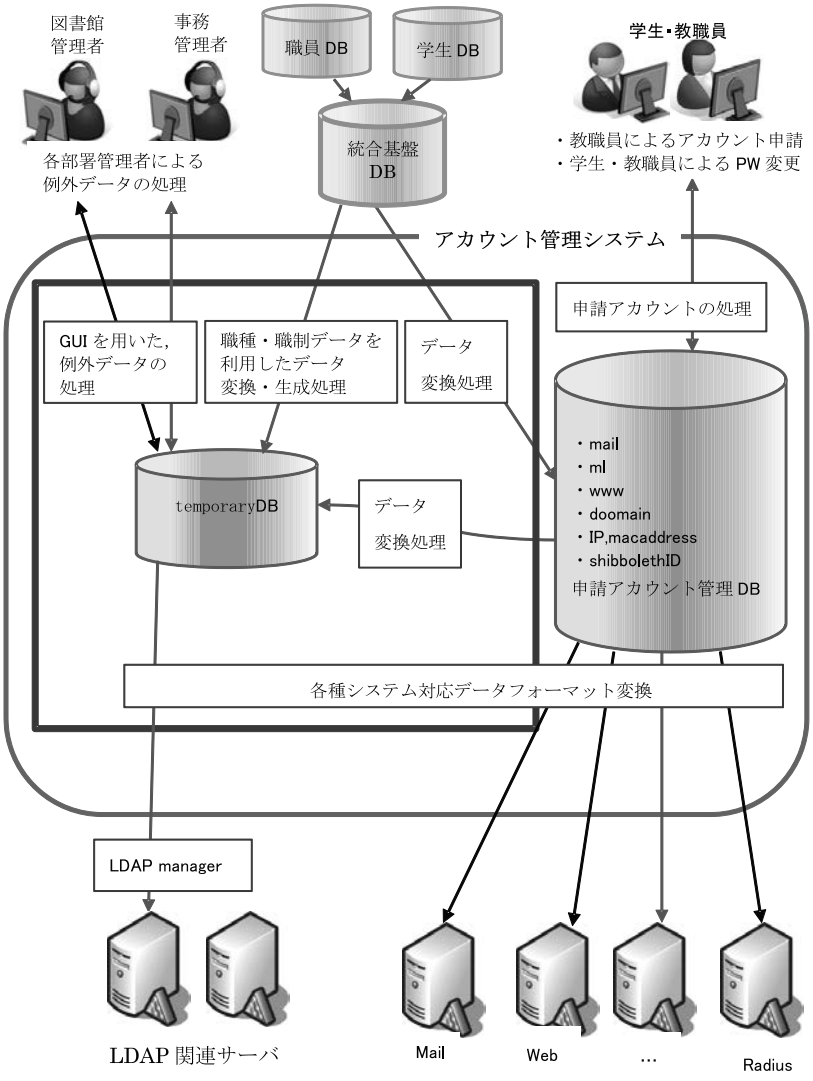


図- 8: 実現したアカウント管理システム

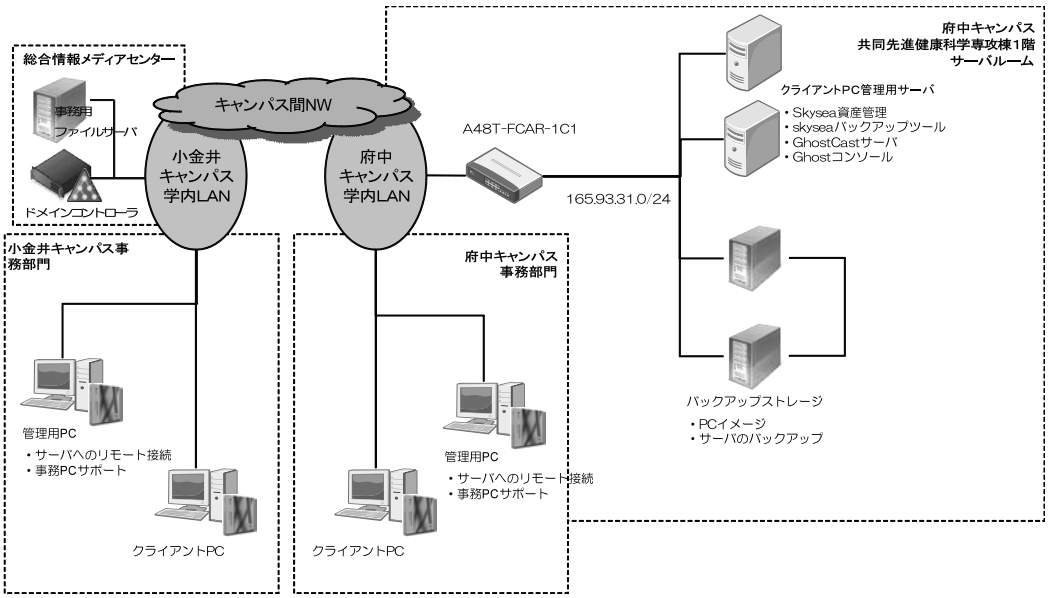


図- 9: 事務用 PC システム構成概念図

テム管理用の OU (Organization Unit) を作成することで，担当部署が既存のグループポリシーとは独立にポリシーを設定できることが必要となった．これは，既存のアカウント体系を流用しつつ，人事移動などの事務組織独自の都合に応じて，共有ファイルサーバへのアクセス権限の設定などを管理することができるようするためである．

しかし，人事情報上は事務組織に含まれる図書館職員が使用する PC システムは，2010 年度末のシステム更新で導入されたシンクライアントシステム [11] としてすでに運用を開始しており，これら図書館職員のアカウントは，例外として既存システムの枠組みの中で管理することが要求された．この結果，改修の影響範囲は，本センターが運用している統一認証運用管理サーバ (LDAP Manager)，ドメインコントローラ (Active Directory)，アカウント管理システムに及ぶことになった．

本センター側で必要となった改修の基本的要件をまとめると次のようになる．また，その概念図を図 10 として示す．

- 事務用 PC システムの利用対象となる事務職員のアカウントは，既存 Active Directory 内に新たに作成する事務用 PC システム管理用 OU に自動的に振り分けることとする．
- ただし，事務職員の中の例外として，図書館職員のアカウントは，アカウント管理システムを改修することで，事務用 PC システム管理用 OU には振り分けないこととする．
- 事務用 PC システム利用者アカウントの運用形態の変更に伴い，既存の Windows プロファイル割り当てルール[6]が変更となった．このため，例外処理として，職制データを基準として，アカウント管理システムが自動振り分けを行うこととする．

この例外処理をアカウント管理システムの改修により対応することになった．具体的には，すでに定義されている職種・所属情報から振り分けのための基礎データを生成する仕掛けを作り，2.4 節で述べた例外に対応するための特別処理を活用することで，事務組織の担当者が例外処理を実施可能とした．この例外処理は，人事異動のタイミングなどで散発的に年間およそ 30 件程度発生しているが，データベースの構造などに大きな改修を行うことなく，事務組織の担当者は，行うべき例外処理をすべてこの部分で集約して行うことができるようになった．

4 一時アカウント提供のための特別処理

本学では，原則として，正規雇用の教職員に関しては人事システム，学生については学務情報システムのデータベースで所属員の情報が管理がされていて，それらの情報は統合基盤データベースで管理されている（図 2）．

しかし，1 章で述べたように，本学の構成員には様々な身分があり，追加や統廃合などで次々に変更される傾向がある．つまり，表 1 で挙げた分類の内容は，常に変更される可能性があるが，時として（過渡期などに），どこにも分類されない例外的な身分が存在することが

[6]移動プロファイル利用者（Floating ユーザ）と固定プロファイル利用者（Dedicated ユーザ）の二種類が存在する．

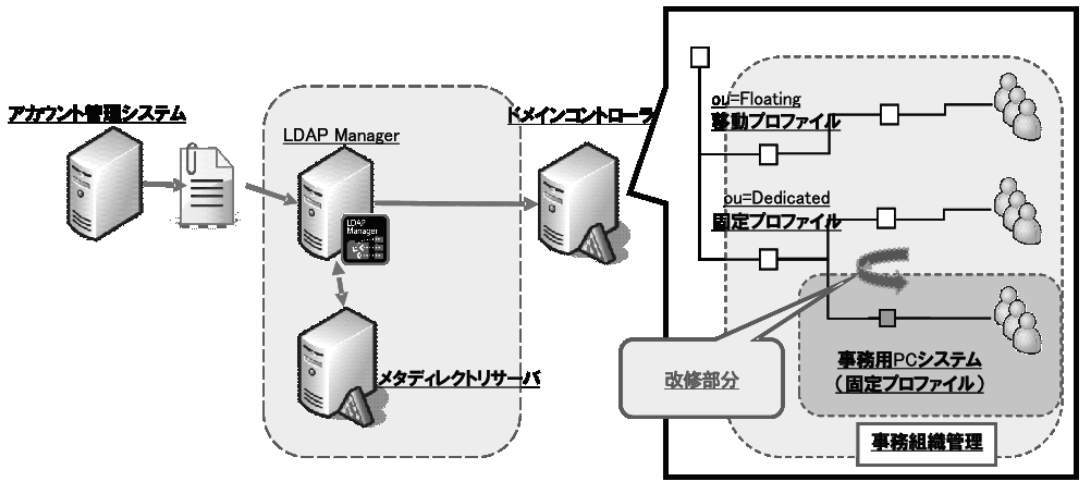


図- 10: 改修内容の概念図

ある．このような身分の者が職務などを遂行するにあたり情報サービスを利用したい場合，例外的に一時アカウントを提供しなければならない場合がある[7]．

また，表 1 で挙げた分類のどこかには属しているが，特別な理由ができて，本来は許されていない情報サービスを利用させなければならない，意図的な例外と言うべき場合も時としてあり得る．たとえば，非正規職員のための演習用 PC システムを用いた講習会などが過去にあった（表 1 の大学と直接雇用関係のない教職員 (A) または (B) に対応し，本来は利用権限がない）．

本センターから見ると，前者は，そもそも人物が統合基盤データベースに存在しない例外，後者は，(統合基盤データベースに人物は存在するが）ある人物に対する利用できるサービスの例外となるが，いずれにしても，従来，一時アカウントはほぼ手動で管理していて，発行・廃止に手間がかかっていた．このため，利用目的や雇用・修業期間に関わらず，すべての情報サービスを利用可能な年度限りの一時アカントを年度初めに多めに（200 アカウント程度）用意し，都度配布していたという問題があった．

この問題を解決するため，2.4 節で述べたアカウント管理システムの特別処理を活用して対応することとした．具体的には，次の通りである．

1. 人物が統合基盤データベースに存在しない場合，CSV ファイルを用いて，アカウント管理システムの一時データベースに人物情報を登録する．
2. 2.4 節で述べた特別処理を活用して，当該人物が利用する情報サービスを手動で有効にする．
3. アカウント管理システムが統一認証管理サーバに渡す CSV ファイルを自動生成し，それぞれのシステムにアカウント情報が登録される（図 2）．

結果として，従来は手作業で管理していたこれらの例外人物を，アカウント管理システムの一時データベースを用いることで，少なくとも本センター内部では統一して扱えるようになった．また，不要な一時アカウントの発行を抑制し（年間 100 アカウント程度まで減少し，従来の半分程度になった），当該人物に取って必要なサービスのみが有効になっている，適切な一時アカウントを随時発行することが可能となった．

5 アカウント管理システムの負荷統計データ

アカウント管理システムのハードウェア仕様を表 2 として示す．OS は，RedHat Enterprise Linux 5 であり，この上でデータベース (MySQL) や処理プログラム (PHP), WWW サーバ (Apache HTTP Server) などの必要なソフトウェアがすべて動作している．

アカウント管理システムは，原則として 24 時間動作しており，利用者はいつでもアカウント申請やパスワード変更などのサービスを利用できる．また，事務組織の運用都合で，アカウント基礎データの大規模更新が月に一，二度行われており，その都度，1700 件から 6000 件程度（表 1 の教職員と学生に対応する）の LDAP データを一斉に更新する必要がある．ある月の種類別処理件数を表 3 として示す．

アカウント管理システムの負荷状況として，表 3 に対応する月の Load Average と CPU の未使用率 (idle (%)) を図 11 として示す．どちらも，cron により，五分毎に

[7] コンプライアンスの観点からは，分類「後」が正しいかもしれないが，本稿では追求しない．

表- 2: ハードウェア仕様

プロセッサ	Xeon E5540 2.53GHz 1P/4C × 2
メモリ容量	8GB
ディスク容量	内蔵ディスクなし（SAN 領域にディスク容量確保）
NIC	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb

測定した結果である．前者の平均は，0.36，後者の平均は 99.08 % であり，十分に余裕を持って捌いていることが分かった．なお，Load Average に時折見られるスパイク（値が 2 以上）は，ウィルス対策ソフトなどの処理で，アカウント管理処理とは無関係なことが分かっている．

6 おわりに

学内において，様々な形態で運用されるアカウント基礎データベースや情報サービスに対応するためのアカウント管理システムを実現した．アカウント管理システムは，アカウント基礎データの取得に加え，情報サービスごとに必要となる，システム固有のデータを生成することや非定型の（人手による）例外処理を行う必要があった．さらに，将来のシステムの増加や更新にも対応できるように，コンパクト（軽量）なアカウント管理システムを目指して設計・構築を進めてきた．柔軟性を持たせた簡潔な登録用データフォーマットを定義し，例外処理を見越した設計を行ったことで，事務用 PC システムの更新や例外的な一時アカウントの提供にも対応することができ，アカウント管理システム実現方法の妥当性を実証することができた．これらのことから，将来，新たに運用方法やデータベースの構造が変更になった場合でも柔軟に対応可能であると予想している．

謝辞

本稿で触れたシステムの実現に協力頂いた，本学学術情報課情報係の諸氏に感謝する．特に，同所属の三好史恵氏にはデータ提供など，論文作成においても協力頂いた．ここに感謝の意を表する．

参考文献

[1] 内藤久資，梶田将司，小尻智子，平野靖，間瀬健二：大学における統一認証基盤としての CAS とその拡張，情報処理学会論文誌，情報処理学会，Vol. 74, No. 4, pp. 1127–1135 (2006.04).

[2] 平野靖，内藤久資，梶田将司，小尻智子，間瀬健二：名古屋大学のユーザ認証基盤の現状，平成 18 年度国立情報学研究所オープンハウスシンポジウム — 最先端学術情報基盤 (CSI) の構築に向けて — 講演予稿集，国立情報学研究所，pp. 41-45 (2006.06).

[3] 間瀬健二，平野靖，梶田将司：名古屋大学 ID の導入について — (I) 概要 —，名古屋大学情報連携基盤センターニュース，Vol. 5, No. 4, pp. 316–320 (2006.11).

[4] 平野靖，間瀬健二，梶田将司：名古屋大学 ID の導入について — (II) 全学 ID からの移行 —，名古屋大学情報連携基盤センターニュース，Vol. 6, No. 2, pp. 140–145 (2007.05).

[5] 内藤久資，梶田将司，平野靖，間瀬健二：名古屋大学における CAS^2 を核としたアイデンティティマネジメントの現状と課題，インターネットコンファレンス 2007 論文集，インターネットコンファレンス実行委員会，pp. 31–40 (2007.10).

[6] 梶田将司，平野靖，間瀬健二：名古屋大学 ID の導入について — (III) 将来構想 —，名古屋大学情報連携基盤センターニュース，Vol. 7, No. 1, pp. 11–17 (2008.02).

[7] 櫻田武嗣，石橋みゆき，萩原洋一：休眠アカウント調査のための Web を利用した情報サービス利用者確認システムの構築と運用，インターネットと運用技術シンポジウム 2008 論文集，情報処理学会，pp. 31- 38 (2008.12).

[8] 飯田勝吉，新里卓史，伊東利哉，渡辺治：キャンパス共通認証認可システムの構築と運用，電子情報通信学会論文誌 B，電子情報通信学会，Vol. J92-B, No. 10, pp. 1554-1565 (2009.10).

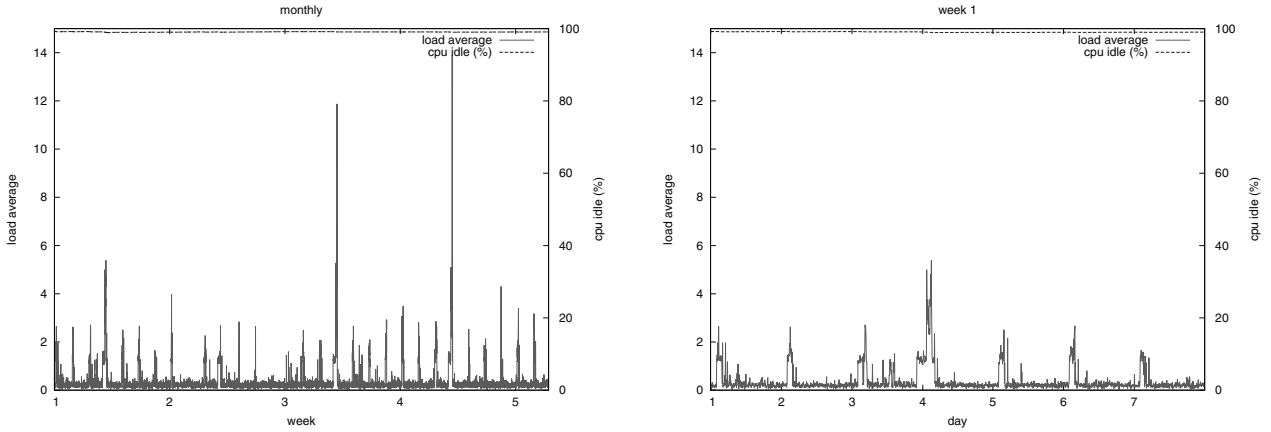
[9] 沖野浩二，布村紀男：富山大学における認証基盤の整備による業務軽減評価，第 14 回学術情報処理研究集会，学術情報処理研究集会，No. 14, pp. 31–39 (2010.09).

[10] 岩沢和男，宮原俊行，中川敦, 岩田則和，西村浩二，吉冨健一：センターサービス利用登録システムの再構築，第 15 回学術情報処理研究集会，学術情報処理研究集会，No. 15, pp. 89–97 (2011.09).

[11] 瀬川大勝，辻澤隆彦，辰己丈夫：仮想化技術を用いたサーバ集約と演習端末室の構築，第 15 回学術情報処理研究集会，学術情報処理研究集会，No. 15, pp. 134–141 (2011.09).

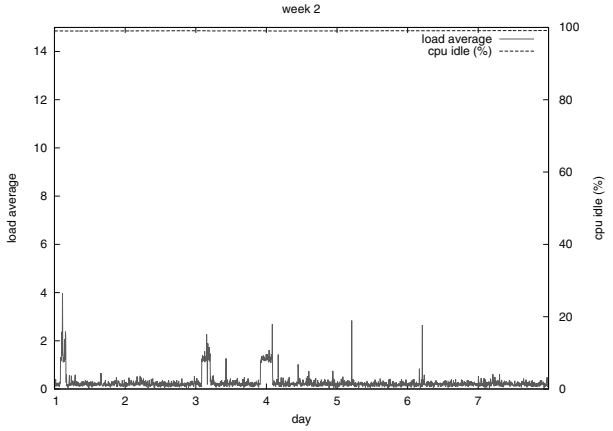
表- 3: 種類別処理件数

	ldap	mail	ML	WWW	IP	DNS	radius	合計
登録	18	18	3	2	13	0	7	61
再発行	47	4	0	5	0	0	0	56
変更	1672	5	43	1	5	0	0	1726
廃止	683	6	0	1	5	0	0	695
合計	2420	33	46	9	23	0	7	2558

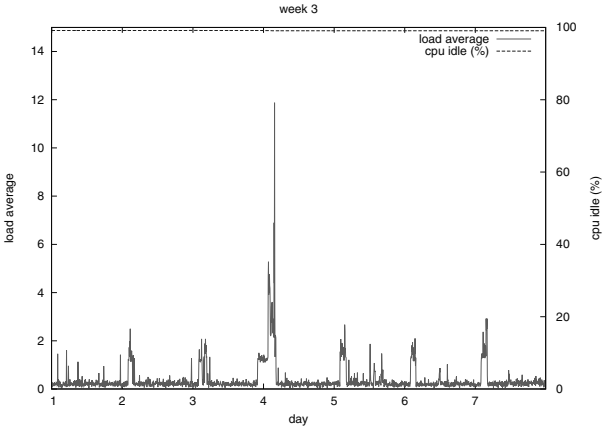


(a) 一ヶ月

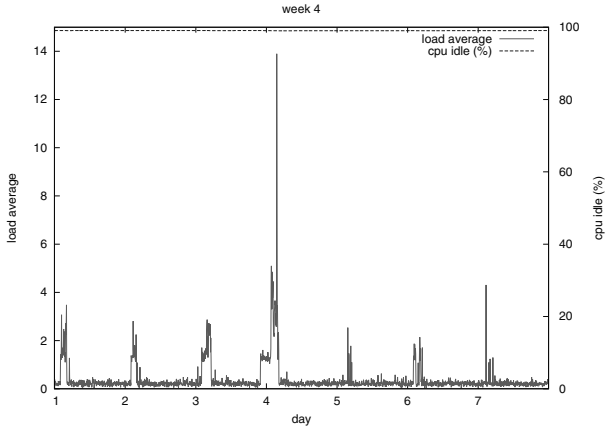
(b) 第一週



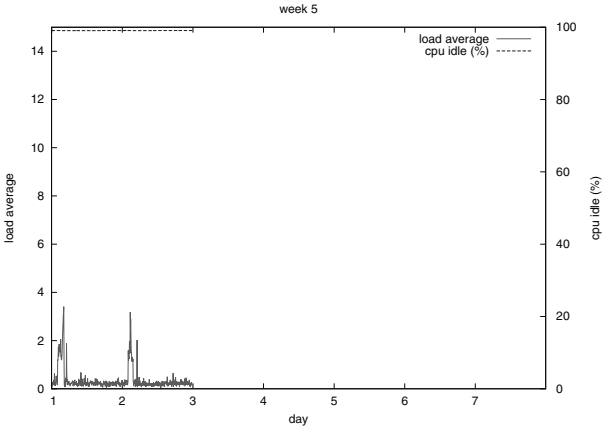
(c) 第二週



(d) 第三週



(e) 第四週



(f) 第五週

図- 11: ある月の Load Average と Cpu Idle (%) の推移

SaaS環境によるプログラミング初学者教育の試み
A Programming Class for Beginners with SaaS

田中克明†, 鈴木令子†, 山崎秀記‡

Katsuaki Tanaka†, Reiko Suzuki†, Hideki Yamasaki‡

katsuaki@cio.hit-u.ac.jp, suzuki@cio.hit-u.ac.jp, yamasaki.hideki@r.hit-u.ac.jp

一橋大学情報基盤センター†
一橋大学大学院商学研究科‡
Center for Information and Communication Technology, Hitotsubashi University†
Graduate School of Commerce and Management, Hitotsubashi University‡

概要

SaaS として提供される Google Apps を用い，Web サイトの作成，サイトへのアンケートフォームの設置，フォームを通して収集したデータの処理，およびそのための Web サービス呼び出しなどを含むプログラムの作成を，授業の一部として実施した．

本稿では，この授業に関連し，プログラミングを学習する環境として SaaS を利用するメリットの検討，授業で利用した Google Apps Script を含めた Google Apps の概要，授業の目的と実施内容を述べる．

キーワード

SaaS, オンラインプログラミング, Google Apps

1　はじめに

プログラミングなど計算機を操作する授業では，そのための環境を学習者が利用する端末上に用意する必要がある．また，学習者に自習をうながすためには，演習室などを提供するだけではなく，学習者所有の PC にもプログラミング環境一式をセットアップし自習環境を整えることが望ましい．しかし，学生が PC を保持している場合が多くなったとはいえ，プログラミング初学者にプログラミング環境のセットアップを要求することは難しく，結果として，あらかじめ用意された端末環境以外において学習を行うことは困難であった．

これに対して，Web を通したサーバサイドのサービス作成のためのプログラミングを対象とし，サーバサイドにプログラミング環境を用意する試みがなされている [1][2]．これらの手法は端末室を用意するよりは十分に負荷は低いが，授業目的に合うように環境を開発し整備を行う必要があるなど，直接の授業内容以外の部分の用意に相応の時間を要する．

環境の構築に時間を要しない方法としては，Microsoft Excel に組み込まれている Visual Basic for Application（VBA）を用いるなどの方法が考えられる．しかし，学習者の立場から見ると Microsoft Excel 固有の環境を学ぶという印象が強く，「プログラミング」を学習しているという意義が伝わりづらいことが，問題点として挙げられよう．

近年のクラウドの発展にともない X as a Service として，Software as a Service（SaaS），Platform as a Service（Paas），Infrastructure as a Service（IaaS）などの形でさまざまなサービスが提供されている．クラウドをプログラミングに関連して用いる場合，PaaS をあらかじめ記述したコードを実行するための環境として利用する，IaaS として提供された仮想マシン中に OS から環境を構築して実行環境を構成するといった，実行

環境としての利用が多くなされている．一方，プログラミング「環境」はSaaSに該当すると考えられ，例えばCloud9 IDE[1]のようなWebベースの統合環境がSaaSとして存在する．

一橋大学では，学生向けのメール環境として2008年よりGmailを導入しており，メール以外のいくつかのサービスを統合したGoogle Appsも利用可能となった．時間の経過とともにサービスも安定し，授業での利用が現実的になり，近年，Google Appsを教育に用いる検討がなされている[3]．そこで，2011年度より，Google Appsのうちいくつかのサービスを組み合わせつつ，JavaScriptに準じた言語体系を持ち開発環境がSaaSとして提供されているGoogle Apps Scriptを用いて，プログラミング初学者向けの授業を実施した．本稿ではその内容を報告する．

2 プログラミング学習における環境

2.1 一橋大学情報系科目におけるプログラミング授業の現状

一橋大学では，情報に関連した科目を共通教育科目の中で「情報基礎」「計算機概論」などとして開講している．「情報基礎」は，学部生を対象に開講しており，通年で24クラスが開講され，ほぼ全学生が学部1，2年次で履修を終える．「情報基礎」「計算機概論」とも，授業は学生1人ずつにWindows7がインストールされた端末が用意された演習室にて行い，実施内容は，ある程度まで担当する教員の裁量に任されている．

2.1.1 情報基礎におけるプログラミング導入

現状の情報基礎においては，半数以上の講義でシラバスに少なくとも一コマプログラミングを取り入れている．3章にて述べる以外に，取り入れ方は様々であるが，次のような目的に沿って行われている．

1. Excelにおける VBA
   Microsoft Excelのマクロ記述言語であるVBAを用い，操作手順を命令文の列で記述できること，分岐・繰返しといった基本的な制御構造の理解
2. Java+NetBeans
   統合開発環境におけるGUIをもつアプリケーション開発手順の理解
3. C言語によるプログラミング
   プログラミングを用いた「情報科学」という学問分野の基本概念理解

[1] http://c9.io/

2.1.2 計算機概論におけるプログラミング

計算機概論は，情報基礎を履修した後の基本的プログラミングを目的とし，年間16クラスを開講している．実施内容は，情報基礎同様ある程度まで担当教員の裁量に任されており，C，Javaなどいくつかの選択肢がある．ここではJavaを利用した授業例を示す．

- **使用環境:** Java，NetBeans
- **内容:** 基本的な値と型・変数，制御構造（分岐・繰返し），配列，アルゴリズムの巧拙：離散指数・整列における計算時間の比較，メソッド，ウィンドウズアプリケーションの作成（GUI部品，イベントの取得）
- **課題:** 簡易テキストエディタ，ファイル入出力

2.1.3 VBAとNetBeansの授業における利点と欠点

上述した情報科目におけるプログラミングの授業を通し，VBAとNetBeansの利用上のメリット，デメリットがいくつか浮かび上がった．

VBAのメリットとして，Excel内部からVBAを用いることによりスプレッドシートの操作やセル配列のイメージと結びつけてプログラムの動作を理解することが容易であることが挙げられる．命令とExcel上の具体的な操作を対応づけられプログラミングのイメージが掴みやすく，学生のプログラミングに対する敷居を下げられる．また，Excelさえあれば，プログラミング環境を構築する必要が無いことも利点である．

VBAのデメリットのひとつは，エラーメッセージなどが不十分でありデバッグが難しいことがある．また，Excelが「計算機」としての機能を補うため，データ型への意識，あるいは浮動小数点演算の誤差など，プリミティブな「プログラミング」を学ぶことが難しいこともデメリットとして挙げられる．

一方，NetBeansの利点は，Windowsアプリケーションの作成を目的にした上で，部品の配置，プロパティ設定が容易に行え，イベントハンドラの記述に専念することが可能であることが挙げられる．さらに豊富な入力補完機能があり，エラーメッセージも充実していることから，マニュアルを別途参照する手間が省ける．また，無償のオープンソースソフトウェアであり学習者のPCへのインストールが可能であることもメリットである．

NetBeans利用のデメリットとしては，開発環境そのものを習得するハードルが挙げられる．プログラミングに必要な開発環境の操作手順習得のために1回（90分）をあてている．誤操作を行った際の修復が困難であり，授業中，開発環境の操作に関する疑問への対応に相応の

時間を必要とすることも問題である．また，このような利用上の手間などにより，無償で配付されているとはいえ，自らのPCにインストールし活用する学生は少数である．

2.2 プログラミング実習における環境の割り当て方式

2.1.3でも検討を行ったように，授業にてプログラミングを取り上げる際，その環境をどのように用意するかということは，授業実施のために重要な事項の１つである．

プログラミングを計算機を用い実習を通して学習するためには，プログラムを作成する環境およびプログラムを実行する環境が計算機上に必要である．そのためには，学習者が利用できる物理的なインタフェイスを用意し，インタフェイスを通して計算機上のエディタなどの開発環境や実行環境を利用することが出来ればよい．これら割当て方には，例えば，以下のような方式が考えられる．

1. 学習者ひとりひとりに開発・実行環境としてPCを用意し，PCごとに必要なソフトウェアをインストールする
2. 学習者ひとりひとりに開発・実行環境として端末を用意し，端末はネットブートなどによるクライアントとして一括管理する
3. 実行環境をWebサーバなどに共通化し，学習者には開発環境が用意された端末を割り当てる
4. 実行・開発環境をWebサーバなどサーバ上に用意し，学習者にはサーバにアクセスする環境を割り当てる
5. 実行・開発環境にサービスとして提供されている環境（SaaS）を用い，学習者にはサービスにアクセスする環境を割り当てる

1.の１人１端末方式では端末の管理にある程度の費用が発生し，管理維持にも労力が必要である．そのため2.のようなシンクライアント方式が多数の端末を設置する多くの演習室で採り入れられている．本学でもこの形式で演習室を提供している．この場合，開発環境を新規に導入する際，原則としてオリジナルとなる１式分のディスクイメージ作成に注力すれば良いのだが，端末を利用する利用者IDごとに環境設定を必要とする事項が残ることもあり，授業進行中に受講者が設定作業を行う必要が生じる場合が多い．また，演習室以外で自習を行いたい場合には，演習室同様の環境を学習者ごとに設定する必要がある．

3.はWebサーバを用い，Webサーバ上で動作するプログラム，CGIなどを作成する場合などに用いられる形式である．エディタなどの開発環境を手元の端末に用意し，作成したプログラムをftpなどを利用してサーバに転送，サーバ上でプログラムを実行させる．手元の端末には最低限テキストエディタなどがあればよく，実行環境などをサーバ側で一元管理できる点では負担が低い．また，実行される環境への依存性が高いコンパイラ部分をサーバ上に設置する方式[4]もある．授業実施者による環境管理が容易であり，演習室の端末以外でもサーバにアクセスできれば手元にはエディタが用意できればよく環境設定の手間がかからないなどの利点がある一方，記述したコードをサーバに転送する手間や，デバッグの困難さが伴う．

4.は，主にWebを通したサーバサイドのサービス作成のためのプログラミングを対象とし，サーバサイドにプログラミング環境を用意する方式[1][2]である．その他，実行・開発環境は端末に持たせるが，プログラムソースコードの管理をサーバにて行い，学習の進捗状況などを把握する仕組みも提案されている[5]．これらは3.と同様に学習者に必要とされる環境設定が少ない上に，コード記述，デバッグなどの環境もWebを通して提供されることから，学習に集中することが可能である．一方，環境を構築するためには，Webベースのエディタやデバッグ環境，学習者を認証する仕組みなど，さまざまな仕組みの構築を行わなければならず，個別の授業ごとにサーバハードウェア，サーバ上で動作するソフトウェアなどを用意するとなると，それなりのコストを要する．

5.が本稿で報告するSaaS方式である．実施形態は4.と同じであるが，サーバのハードウェア，サーバ上で動作するソフトウェア，すべてサービスとしてあらかじめ提供されているものを用いる．学習者はWebブラウザさえ動作すればプログラミング環境を用いることができ，授業を行う側も，特別な環境の用意を行う必要がない．

2.3 Google Apps

今日，Webブラウザとネットワーク接続を用意すればソフトウェアによるサービスを利用できるSaaSとしてはさまざまなサービスが提供されている．その先駆けともなったサービスがメール（Gmail）に代表されるGoogle Appsである．Gmail以外にも，一般的なオフィススイートに準じた，スプレッドシート，ワードプロセッサ，プレゼンテーションツールなどがWebブラウ

図- 1: フォーム編集画面例

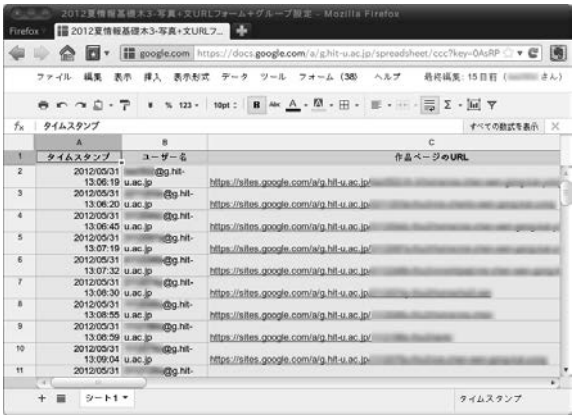


図- 2: フォーム入力データの記録例

ザを経由して利用可能なサービスとして提供されている．これらは，Google ドライブ（2012 年 6 月現在,「ドキュメント」からの移行が順次進んでいる）の各ファイルを編集する機能としてアクセスできる．

本稿では，この Google Apps に含まれるいくつかのサービスを組み合わせた上，Google Apps Script を用いて，情報基礎の授業においてプログラミング初学者向けのプログラミングの基礎の授業を行った．以下に，Google Apps に含まれるサービスのうち，本稿で述べる授業にて用いた機能の概要を説明する．

2.3.1 スプレッドシート・フォーム

複数のシートをもつスプレッドシートである．データは Goolge のサーバ上に保存され，複数のユーザが同時にシートの編集を行うことができる．編集，閲覧を行えるユーザは，後述する共有機能により制御が可能である．

また，スプレッドシートをデータの記録先として用いる Web 上のフォームを作成・編集，公開する機能が提供されている（図-1）．フォームから入力されたデータは，1 回の入力がシートの行，フォームの各項目がシートの列に対応付けて記録される．フォームから入力されたデータがスプレッドシートに記録された例を図-2 に示す．

図- 3: Google サイト編集画面例

スプレッドシートのセルへの変更は，編集履歴として記録される．編集履歴にはどのユーザが，いつ行ったものかという情報が全て記録され，また，この履歴により，スプレッドシートを任意の時点の状態に戻すことができる．

また，Microsoft Excel における VBA などに相当する機能として，Google Apps Script が用意されており，セルやシートの操作を行うことができる．Google Apps Script については 2.3.3 にて後述する．

2.3.2 サイト

Google ドライブとは別に，Web サイトを構築，公開する機能が「サイト」として提供されている.「サイト」は，Google が提供するサーバを用いて Web サイトを構築できるサービスであり，Web ページ管理機能，オンラインでの簡易な Web ページエディタなどを備える．ページ編集画面例を図- 3 に示す．本授業では用いなかったが，ページの HTML ソースコードを直接編集することもできる．なお，Google Apps 環境では，Web サイトの共有範囲として同一の Google Apps ドメインのアカウントを持つユーザを選択できることから，学生の間にのみ公開範囲を限定した Web サイトの作成が容易である．

サイトには，2.3.1 で述べたフォームに記入画面を埋め込むことができる．フォームから入力されたデータは，先に述べた通り，スプレッドシートを通して確認，編集することができる．

図- 4: Google Apps Script エディタ画面例

2.3.3 Google Apps Script

Google Apps Script（以下，AppsScript）は Google Apss 環境の一部として提供される，プログラミング，プログラム実行環境である[2]．図-4 に AppsScript エディタの画面例を示す．

以前より，Google はプログラム実行環境として PaaS である Google Apps Engine を提供していたが，プログラミングエディタなど統合環境を含む SaaS として，2009 年から Google Apps Script が利用可能となった．

AppsScript にて記述したプログラムの実行は Google のサーバにてなされ，手元の Web ブラウザを動作させている端末側にはスクリプト実行時の負荷はない．なお，1 つのスクリプトで利用可能な計算時間の総量は，特に明示されていないがある程度の制限がなされているようであり，計算時間が長時間に渡るような処理を行わせるには適さない．

AppsScipt の記述言語は JavaScript を基にしており，文法や基本的なメソッドは JavaScript に準じる．AppsScript には GoogleApps 環境で提供される各種サービスを操作する機能が与えられている．例えば，スプレッドシートではセルや複数のセルに渡る範囲の値の読み込みや書き込み，シートの追加，削除といった操作などを行える．サイトでも，各ページの記述内容の書き換え，ページの追加，削除などの操作が行える．その他，Google の翻訳機能を呼び出しテキスト翻訳を行うといったことも可能である．

AppsScript 環境を用いて記述したプログラムはエディタ画面から起動できる他，時刻を指定して実行する，スプレッドシートのメニューへ組み込みメニュー呼び出しにより実行する，サイトへガジェットとして組み込みサイト上のコンテンツとして実行することなどが可能である．

2.3.4 共有範囲の設定

以上に述べた各機能で作成したデータや Web サイトは，一般公開できる[3]ほか，他の Google アカウント保持者を選んで閲覧用に公開したり，共同編集者として指定したりすることができる．とくに Google Apps for Education 環境など法人向けの Google Apps 環境では，ドキュメントや設置したサイトの共有範囲として，同一の Google Apps ドメインのアカウントを持つユーザへの公開を選択できる．同一の Google Apps ドメインを利用するユーザを公開範囲として選択すれば，学生の間にのみ公開範囲を限定したドキュメントや Web サイトの作成を容易に行える．

[2] https://developers.google.com/apps-script/

[3] 本学では，学生用の Google Apps 環境において「一般公開」を選べないよう設定を行っている．

3 授業内容

3.1 概要

一橋大学における「情報基礎」授業のうち 1 クラス，商学部，経済学部，法学部，社会学部に属する学部生約 40 人を対象とし，Google Apps 環境を用いた学生各個人のサイトコンテンツの作成，アンケートフォームの設置，収集した回答の簡単な解析を 2011 年度より実施した．

本稿で述べる授業では，コンピュータおよびコンピュータネットワークに関する基礎的な学習を通し，情報の社会がどのような技術によって形作られているのかを理解することを大きな目的とし，Web に関連したインターネット技術の概観を中心とした学習を行った．

Information and Communication Technology（ICT）の Communication については，授業開始時のアンケートなどから，学生が常日頃から接している部分であることが分かっているため，その仕組みを説明し，機能を理解するためのいくつかの演習を中心に行った．一方，Communication ではない部分，コンピュータを計算機として用いることにより，人間に代わって情報を処理することができることについては，日常の生活では意識することがない部分であることから，その仕組みを構築する手法があることを実際に体験する学習に比重をおくこととした．

これを踏まえ，プログラミングに関する学習では，変数の概念や制御構造など基本的なプログラム記述に必要な概念を学びつつ,「Web を通して情報を集め，集めた情報に対し，人手では手間がかかると思われる処理を計算機を用いて行うこと」を作成するプログラムの目標として設定した．そのために，学生自身のサイトを作成しそこに入力フォームを設けて情報を集め，集めた情報を AppsScript により外部の Web サービスと連携して解析し，結果をスプレッドシートに保存する，という流れをとった．なお，単純な計算による解析であればスプレッドシート内で行うことが合理的であることから，スプレッドシートで行うには適さない，自由記述文章の形態素解析を Web サービスと連携した解析としてとり上げた．

3.2 フォームを用いたデータの収集

まず，Google Apps のサイト機能を用い，各自の Web サイトを作成した．自由にサイトを作ることでサイト機能の操作に慣れつつ，写真と短文の組み合わせを 1 つの作品単位とし，自分の作品の写真を他の授業参加者の写真と入れ替えた作品を複数作ることを通して，自分以外のサイトを見て回る機会を設けた．この際に，自身のサイトの URL を教員が設けたフォームに入力，入力した URL がスプレッドシートを通して一覧できるよう，フォーム入力内容が記録されるスプレッドシートを受講者全員で共有するよう設定した．共有したシートの例が図-2 である．

続いて，感想を記入するフォームを作成，サイト内の写真と短文の組み合わせを掲載したページ内に設置した．解析対象として数個の感想が集まるよう，相互に感想を書くためのグループ分けを，フォームを通してサイトの URL を集めたシートを学生が各自の端末上で表示している間に，各自のサイト URL の横に番号を記入することにより行った．フォームやスプレッドシートに他のユーザが記入した内容は，ほぼリアルタイムに各自が閲覧しているスプレッドシートに反映される．

3.3 AppsScript での処理目標

アンケートとしてフォームを用いて収集した自由記述文書を，外部の Web サービスと連携して形態素解析し，スプレッドシートに記録することを最終的な目標とした．例えば Yahoo!Japan が提供するサービス[4]など，一般の Web サービスとして用意されている形態素解析サービスでは，利用のために登録が必要である．学生に授業での 1 回の利用のために登録を要求することは現実的ではないと考え，文を渡すと形態素解析結果を返す Web インタフェイスを持つサービスを独自に用意した．サービスは REST 形式を模し，HTTP の GET メソッドで要求を受け取り，結果を CSV で返すものとした．XML を利用する方法に比べ，交換するデータの直感的な理解を容易にするためである．初学者向けではなく，より高度な利用を目指すのであれば，AppsScript に用意されている SOAP 関連のサービス[5]を用いることも可能であろう．

AppsScript を用いた Web サービスの利用に先立ち，Google マップ[6]など URL 中に引数を記すことで，その挙動の変化がわかりやすいサービスを用い，URL に GET メソッドで処理されるパラメータを付加し，パラメータにより Web サービスが応答として提示する情報を変化させられることを学習した．また，Web から情報を取得しスプレッドシートに格納する手法の学習を目的とし，AppsScript を用いて東京電力が提供する電力使用量 CSV[7]をスプレッドシートに取り込む方法，データを確認する演習を行った．

[4] http://developer.yahoo.co.jp/webapi/jlp/ma/v1/parse.html
[5] https://developers.google.com/apps-script/service_soap
[6] https://maps.google.co.jp/
[7] http://www.tepco.co.jp/forecast/html/images/juyo-2012.csv

図- 5: AppsScript エディタでの入力候補表示例

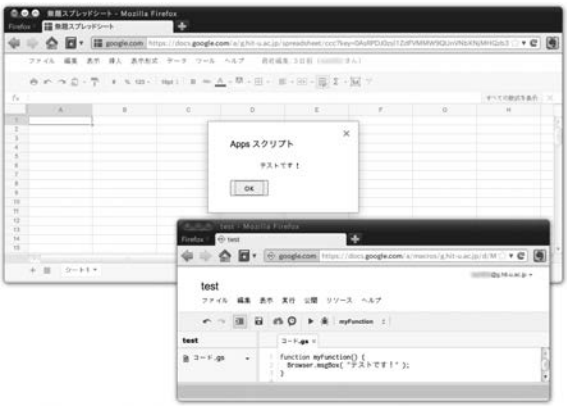


図- 6: AppsScript 実行例

3.4 AppsScript でのプログラミング

AppsScript は GoogleApps のスプレッドシートメニューから記述を行うことから，スプレッドシートと結びつけつつ，プログラミングの授業内容を行った．

3.4.1 メッセージボックスの表示

まず，人手によるスプレッドシート操作とは異なったことができることを学習するため，メッセージボックスを表示するコードの記述を行った．Web ブラウザ上で JavaScript を利用する際には window.alert() を用いるが，AppsScript では Browser.msgBox() を用いる．なお，AppsScript エディタでオブジェクト名，メソッド名などを入力する際には，入力途中でそれぞれの候補が表示される（図-5）．

エディタからは実行する関数を指定してコードを実行することができ，処理結果はエディタとは独立して AppsScript エディタを呼び出したスプレッドシート上に表示される（図-6）．

3.4.2 変数・配列の利用

AppsScript エディタをスプレッドシートのメニューから呼び出して実行することを踏まえ，変数，配列といったプログラミング上の概念を，スプレッドシートと結びつけて説明を行った．セルが言語上の変数に相当し，シートの範囲指定が配列に相当するものとして，AppsScript からセルや範囲の値の読み出し，値の設定を行いつつ，変数への値の設定と値の利用を並行して演習を行った．

3.4.3 制御構造

制御構造のうち，繰り返し処理については，変数などと同様にスプレッドシートと結びつけ，セルを連続して読み出す，連続して値を設定するなどの処理を記述することにより，視覚的に理解が行えるよう演習を行った．

分岐はスプレッドシート上で直接的な表現を行うことが難しいと考え，スプレッドシートとは結び付けず，先の Browser.msgBox() と入力を受ける Browser.inputBox() を組み合わせ，入力値に対して出力値を変化させるコードの記述をとりあげた．

3.4.4 外部サービスの呼び出しと結果の格納

先に述べたように，Web 上の単純な CSV ファイルの取得とスプレッドシートへの格納を行った後に，形態素解析を行う Web サービスの呼び出しと得られたデータの格納を行った．

Web サービスの呼び出しでは，フォームに入力された内容を記録したスプレッドシートから，解析対象としたいセルの内容を取得，形態素解析 Web サービス呼び出し用の URL を取得した内容を引数として生成し，URL が示す内容の取得を行った．AppsScript において URL を指定して URL の示す内容を取得するためには，UrlFetch Services[8] を用いた．

なお，取得したデータを一度配列に格納し配列をスプレッドシートに転記する方が効率的だが，スプレッドシートのセルを直接操作するイメージに近いほうが直感的に理解しやすいと考え，CSV から取得した値を 1 つずつセルに設定するサンプルコードを受講者に示した．

4 考察

4.1 本実践におけるプログラミング学習の位置づけ

3.1 にて述べたように，本稿で取り上げた授業におけるプログラミングの学習では，Web などをとおしたコミュニケーションの裏に隠れ日常の生活では意識する

[8] https://developers.google.com/apps-script/service_urlfetch

機会が少ない「計算機が（人間に代わって）情報を処理すること」について，実際に体験することに比重をおいた．

Google Apps のスプレッドシートを用いると，複数人が同時に同じシートを編集することができる．たとえば，授業中に 40 人で共同編集を行うと，眺めている間にセルに値が記入されていく．本稿で述べた形態素解析を行いシートに記録する AppsScript のコードにより，自ら書いたコードが，文書中にあらわれる単語の一覧を別の共同編集者に入力してもらっているかのように，動作することを体験することが可能であった．

このように，ここで取り上げたプログラミングでは，計算機上でプログラミングを行うことにより何ができるかを主たる目標とし，たとえば浮動小数点数の誤差など，計算機の内部に関する学習は取りあげなかった．

4.2 Web サイト構築に関する学習

Web 上で動作するプログラムの作成を行う学習には，Web サーバに HTML ファイルをおき，クライアントとなる PC からアクセスする，サーバ・クライアントモデルを体験する側面もある．つまり，サーバに ftp を用いてファイルを置き，アクセスすることでファイルの内容が表示されたり，プログラムが実行されることを学習の目的とすることも考えられる．

しかしながら，近年，多くの Web サイトは Web ベースのインタフェイスを持つ Contents Management System（CMS）を用いて管理されており，ftp などを利用して Web サイトを管理する必要性は多くはない．また，Web サーバを構築する時も，そもそも CMS が標準でインストールされていることが増えてきている．

これらのことから，本授業では，文科系学部における学部初年度で「ファイルを転送する」ことなどを実習する重要性は高くないと判断し，SaaS として提供される Web サイトやプログラミング環境を利用しつつ，Web サイトの仕組みについてはサーバ・クライアント方式として P2P 方式などと絡めながら，サービス提供におけるアーキテクチャとしてとりあげた．

なお，Google サイトでは，HTML の直接編集が行える他，画像は Web ブラウザ経由ではあるが「アップロード」を行う必要があり，これらを入り口に Web サイト構築の詳細を説明することも可能であろう．

4.3 AppsScript を用いたプログラミング授業の可能性

AppsScript は，コード記述を行うエディタ以外にも，デバッガ，プロファイラを備えるなど，開発環境が順次整備されている．また，Google Apps 以外の各種の Google API を利用するための拡張など，AppsScript で利用することが可能な機能も随時追加されている．

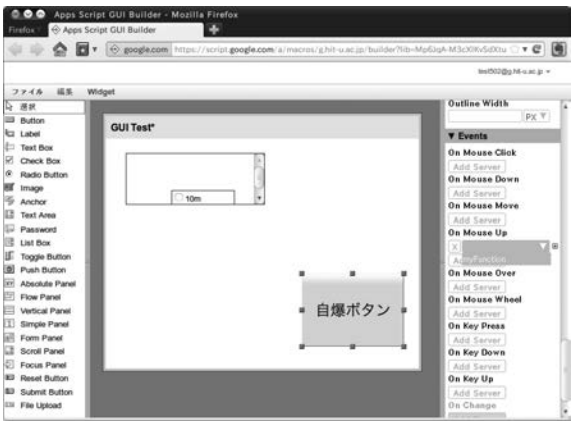


図- 7: AppsScript ユーザーインタフェース構築例

例えば，まだ正式な機能とはなっていないが，GUI 画面でダイアログボタンの配置，ボタン操作時などのイベントに対する実行コード記述を行える「ユーザーインタフェースを構築」機能も持つ（図-7）．これにより，2.1.2 にて述べたような GUI に基づくイベント駆動型のプログラミングについて授業を行うことも可能である．

Google Apps の機能を多用して授業を行うことにより，学習結果まで Google Apps に依存してしまはないかという懸念もある．この点，「サイト」機能は比較的低機能の CMS であり，むしろ現在の高機能な CMS を利用するための導入となるであろう．また，AppsScript は JavaScript をベースにしているため，汎用性が高いと考えられる．用いるオブジェクト名称などがブラウザベースで動作する JavaScript とは異なるが，同様の機能を異なるオブジェクト名称などで記述することになるのは，言語というより利用するフレームワークに依存する部分であり，AppsScript に限らずプログラミングの授業では問題となる事項である．このように，学習環境に過度に依存せず応用が利くよう，授業を組み立てることに留意することは，SaaS を用いるかによらず常に必要であろう．

4.4 プログラミング学習環境に SaaS を用いる利点と欠点

プログラミングの学習環境に SaaS を用いる利点として，まず，2.2 にも述べたが，授業ごとの環境構築，環境設定が不要であることが挙げられる．サーバサイドの環境構築も不要である．

端末環境も Web ブラウザが動作すればよく，例えば，若干の不便は伴うものの，タブレット型端末でもコード

の記述と記述したコードの実行が可能である．自習のための環境整備が不要となることから，授業時間外にプログラミングの実習を行うことも相対的に容易となる．

Google Apps 環境では，Web ブラウザへの依存性も十分に注意がなされているように見受けられた．本稿で述べた授業において挙動の違いが生じたのは，Internet Explorer を用いた際の iframe タグの扱い，同じく Internet Explorer を用いてテキスト入力を行う際のバックスラッシュの扱いのみであった．

その他にも，いくつか懸念事項が挙げられる．たとえば，サーバサイドで動作することから，授業でサービスへ同時アクセスを行った際などの安定性が挙げられる．現在までのところ，2011 年度前期には AppsScript エディタが不安定な状態になることがあったが，Web ブラウザにてリロードを行うことにより解決可能であった．2011 年後期以降同様のトラブルは発生していない．本授業を実施した学生がプログラミング初学者でありほかの環境との比較ができないであろうことから，プログラミング環境としての AppsScript の利用しやすさや安定性について調査を行っていないが，スプレッドシートについて Microsoft Excel と比較した利用しやすさや安定性について調査を行ったところ，動作が不安定であるという選択肢を選んだのは 40 名中 1 名であった．

また，これ以上に大きな事項としては，サービスの一貫性が挙げられる．SaaS として提供されている以上，SaaS の利点を活かすべく，サービスの内容は随時拡充，変更される．例えば，Google ドキュメント画面デザインは 2011 年 8 月にうちに水色を基調としたものからモノクロ基調のものに変更され，AppsScript にプロジェクトの概念が導入されるなどの変化があった．

とはいえ，Google Apps は，サービスの利用者が多数いることなどから，必要な機能が突然提供されなくなる可能性は低く，十分なアナウンスの後に実施されると期待できる．そのため，たとえば授業資料を用意してから授業を行うまでの間に大規模な見た目や機能の変更が行われるようなことはなく，大きな問題にはならないが，常に注意は必要であろう．また，本学では Google Apps for Education を利用する契約を行っており，大規模なインタフェイス変更などの導入タイミングは，Goolge Apps 管理者がコントロールすることができた．その他，利用規約の変更などにも，常に注意を払う必要がある．

5　おわりに

本稿では，SaaS として提供されている Google Apps の各サービスと，その一部として提供されており Google のサーバサイドでコードの実行もなされる Google Apps Script を組み合わせ，プログラミング初学者向けの授業を実践し，その報告を行った．

SaaS をプログラミング環境として用いることにより，授業時に環境の設定などを行う必要がなく，また，学習者も演習室以外を利用しての自習が容易となる．2011 年度より開始し，半期で 40 人，計約 120 人が受講したが，これまでのところ大きな問題はない．また，Google Apps のサービスであるスプレッドシートやサイト，サイトへ埋め込めるフォームなどを連携させ，Web 上でのデータ収集から解析までの一連の流れとして学習をすすめることができた．

現在，本学の「情報基礎」におけるプログラミング初学者向けの授業においてのみ Google Apps Script を利用しているが，今後，「情報基礎」に続けて開講する「計算機概論」においても，プログラミング環境として SaaS 環境を利用することが可能か，発展の検討を進める予定である．

参考文献

[1] 兼宗, 長：“文科系大学におけるサーバサイドプログラミング授業の試み”, 情報処理学会研究報告コンピュータと教育研究会, pp. 141–148 (2006).

[2] M. Đanić, D. Radošević and T. Orehovački: “Evaluation of student programming assignments in online environments”, Proc. of 22nd Central European Conference on Information and Intelligent Systems, pp. 111–116 (2011).

[3] Y. Wang and B. Jin: “The application of saas model in network education – take google apps for example”, Proc. of 2nd International Conference on Education Technology and Compute, Vol. 4, pp. 191–194 (2010).

[4] A. Malinowski and B. M. Wilamowski: “Web-based c++ compiler”, Proc. of the American Society for Engineering Education 2000 Annual Conference, pp. 1–7 (2000).

[5] 三浦, 國藤：“Subversion を用いた学習管理システムの構築とプログラミング初学者への適用”, 情報教育シンポジウム予稿集, pp. 155–162 (2006).

大規模 PC 実習室システムの更新及びその利用状況

Utilization Situation of the Updated Large-scaled PC Training Room System

右田 雅裕†，杉谷 賢一†，久保田 真一郎†，武藏 泰雄†，永井 孝幸†，
戸田 真志†，喜多 敏博†，松葉 龍一†，辻 一隆†，島本 勝†，木田 健†，
宇佐川 毅†，中野 裕司†
Masahiro Migita†, Kenichi Sugitani†, Shin-Ichiro Kubota†, Yasuo Musashi†,
Takayuki Nagai†, Masashi Toda†, Toshihiro Kita†, Ryuichi Matsuba†, Kazutaka Tsuji†,
Masaru Shimamoto†, Takeshi Kida†, Tsuyoshi Usagawa†, Hiroshi Nakano†
migita@cc.kumamoto-u.ac.jp

†熊本大学総合情報基盤センター
860‐8555 熊本市中央区黒髪 2 丁目 39‐1
† Center for Multimedia and Information Technologies, Kumamoto University,
2–39–1 Kurokami, Chuo-ku, Kumamoto 860–8555 Japan

概要

熊本大学では，2011 年 3 月に全学的規模の PC 実習室システム更新が実施された．本学の PC 実習室システムは情報教育とともに更新が重ねられ，約 4 年ぶりに更新された新システムでは約 1300 台の PC を有する．多数の PC を抱える新 PC 実習システムを安定運用するため，また，近い将来起こる可能性のある事業継続の問題に備えるべく調査を行った新システムの運用初年度利用状況について報告する．

キーワード

情報実習室，情報教育，ｅラーニング

1. はじめに

大学における PC 実習室は，情報コミュニケーション技術(ICT)を利活用した教育・研究活動を支える重要な情報基盤の一つである．熊本大学では，全 1 年生（約 1800 名）を対象にした情報リテラシー科目「情報基礎 A・B」（以降，情報基礎と表記）[1]や語学教育の一環である CALL(Computer Assisted Language Learning)等において，この PC 実習室を利用した教育体制が構築され，これまで実施されてきた．2011 年度からは，本学の多くの学部で必修科目とされるベーシック科目も 1 年生を対象にして開講されている[2]．情報基礎やベーシック科目は，ｅラーニングの利用を前提とした対面講義形態が採用されており，学生は決まった時間に決まった PC 実習室でその科目の受講を行う．これに対して，対面講義を伴わない完全ｅラーニング科目としては「情報処理概論」が開講されており，本学 2 年生のおよそ 2/3 に相当する約 1100 名が毎年受講している[3]．情報基礎は 2002 年度より，また，情報処理概論は 2003 年度より当センターが実施主体となり開講されており，これまで実施されてきた．本学における PC 実習室は情報演習だけでなく，LMS(Learning Management System)を中心としたｅラー

ニングを採用した科目の受講スペースとしても活用されている.

情報基礎の開講初年度である 2002 年度は, 当センター及び本学各学部に既設のPC実習室へ設置されたPCを利用して講義が実施された. ところが, 各実習室に設置されたPCには, 導入時期に伴う演算能力の差やインストールされたソフトウェアの種類及び設定に伴う演習環境の違いが生じており, 教員が作成するテキストの構成や実習を行う上で問題となっていた. そこで, その次の当センター計算機システム更新時期となる 2003 年のシステム導入の際に, これを改善すべく PC 実習室システムが一新された. この更新によって, 少なくとも情報基礎の演習を行う PC 実習室では, 全台同一ハードウェア構成の PC が整備され, なおかつ, どの実習室の PC を利用しても同一の利用環境を提供する PC 実習室システムが構築された. このとき全実習室に配備された PC は合計約 950 台であった. 続く更新時期である 2007 年に導入されたシステムでは, それまで対象に含まれなかった PC 実習室にまでその規模を拡張し, 本学のどのキャンパスの PC 実習室においてもこのPC実習室システムのPCが利用可能となった. その結果, この更新により PC の台数は合計約 1300 台に増加した. 2011 年 3 月, 当センター計算機システムはその時期を迎え, 更新が実施された. この更新では, 前回更新と同規模の PC 実習室システムが構築され, 翌月より運用が開始されている.

本学における PC 実習室システムはこれまでのところ情報基礎等の情報教育とともに進展しており, 先行研究[4]と通ずる部分が多々ある. また, 現在では同システムは情報教育だけでなく語学教育やベーシック科目等の教養教育科目もその利用を前提として教育体制が構成されており, 少なくとも本学では PC 実習室の需要は高いと考えられる. これとともに, PC 実習室をはじめとした情報基盤には安定した運用が強く望まれるため, その状況を把握することはこれに大きく貢献することが示されている[5]. PC 実習室は講義の際に利用されるだけでなく, 本学では講義が行われていない時間帯も学生及び教職員が自由に利用できるよう基本的に開放されている. そのため, PC 実習室の利用が多様に行われていることが予想される. さらに, 近年電力供給といった外的要因により事業の継続が困難になるような事態も現実的な問題となりつつあるため, PC 実習室の稼働状況を把握することは前述の安定稼働だけでなくそのような局面への有用な備えにもつながると考えられる. そこで, 当センターでは新システム運用初年度である 2011 年度の利用状況調査を行った.

本稿では, 2011 年に更新された本学の PC 実習室システムの概要を述べ, 更新された PC 実習室システムの 2011 年度（2011 年 4 月 1 日から 2012 年 3 月 31 日）1 年間の利用状況を報告する.

2. 更新された PC 実習室システムの概要

本稿におけるPC実習室システムとはPC実習室に配備された PC とその利用を支えるサーバから成る計算機システムを指し, その中でも本稿では利用者が操作を行う端末であるPCに着目する. 現行のPC実習室システムは, 2011 年 3 月の当センター計算機システム更新により導入されたものである. PC 及び各サーバは, 既設の学内 LAN を用いてネットワーク接続されている[6]. 各 PC 実習室内の PC は 1000BASE-T で, また, 総合情報基盤センター内に設置されたサーバは Gigabit Ethernet で学内 LAN と接続されており, 各建屋間のネットワーク基幹部は 10 Gigabit Ethernet で接続されている.

PC 実習室に配備されたPCは全台同一ハードウェアで構成され, 各 PC には Microsoft Windows 7 及び Ubuntu (Linux)の 2 種類の OS がインストールされている. 利用者は PC の起動時にどちらを起動 OS に用いるか選択することができる. 本システムにおける PC の構成及び仕様を表 1 に示す.

表 1. PC 実習室システムにおける PC 構成及び仕様

構成部品	名称または仕様
PC本体	富士通社製 ESPRIMO D750/A-K
CPU	Intel社製 Core i5-660
RAM	4GB
HDD 容量	160GB
外部ディスク装置	DVD-ROMドライブ
ネットワークインタフェース	1000BASE-T (1ポート)
OS	Windows 7 及び Ubuntu
ディスプレイ装置	対角19インチ 液晶ディスプレイ

表 2. PC 実習室の設置状況

実習室記号	PC台数	キャンパス	設置場所
A204	49	本荘	医学部
A302	61	黒髪	全学教育棟
A403	12	黒髪	全学教育棟
A404	31	黒髪	全学教育棟
A405	31	黒髪	全学教育棟
A406	77	黒髪	全学教育棟
A407	53	黒髪	全学教育棟
A408	53	黒髪	全学教育棟
B201	33	本荘	医学部
B301	61	黒髪	全学教育棟
B302	61	黒髪	全学教育棟
B401	105	黒髪	全学教育棟
CNT3	97	黒髪	総合情報基盤センター
CNT4	61	黒髪	総合情報基盤センター
CNTT	13	黒髪	総合情報基盤センター
LIBH	4	本荘	医学部図書室
LIBK	88	黒髪	附属図書館本館
LIBM	36	本荘	附属図書館医学部別館
LIBP	15	大江	附属図書館薬学部別館
MEDI	127	本荘	医学部
PHAR	101	大江	薬学部
SCIE	41	黒髪	理学部
TECH	109	黒髪	工学部

PC 実習室システム全体では合計約 1300 台の PC を有しており, 現システムでは 2007 年に導入された前システムと同規模の PC 台数が確保され, 更新により全 PC が新たに調達された．本学は大きく黒髪，本荘，大江の 3 つのキャンパスで構成されており, PC は各キャンパスにあるそれぞれの PC 実習室に設置されている．各実習室の設置場所とそこに配備された PC の台数を表 2 に示す．前システムと同様本システムにおいても，移動プロファイルにより利用者はどの PC 実習室の PC を利用してもその利用者の同一利用環境が提供される．

前システムでは PC へ 32bit OS（Microsoft Windows XP 及び Vine Linux）が導入されたが，拡大した搭載メモリを有効活用するために本システムの PC へインストールされた 2 種類の OS はどちらも 64bit 版が採用されている．このうち Windows 7 システム環境は，ウイルス対策ソフトウェア及び数式処理ソフトウェア等を除きほとんどがフリーウェア及びシェアウェアで構成されている．講義において利用される同システム環境のフリーウェア及びシェアウェアに関しては，前システム環境へ導入されていた多くのソフトウェアが利用可能であることが確認された. 本システムの PC は再起動によって PC の Windows 7 システム環境を自動的に起動前の状態へ復元する機能を有するが，教育の実施基盤としても利用される本学の PC 実習室システムにおいてこの機能の搭載は必須と考えられる．システム復元ソフトウェアにより実現される同機能は 64bit OS 環境においても有効に動作しており，前システムと同様，利用者により変更が行われた場合でも PC における同システム環境が維持されている．講義中の利用は少ないと考えられ，また，前システムでは保守を要する障害も多かったことから，各 PC 実習室へ設置されるプリンタに関しては当初本システムでの導入見送りが検討されていた．しかしながら，講義中のプリントアウトを実現するため本システムの構成にプリンタを求める強い要望があることが仕様策定段階で明らかになった．そこで，このような利用形態を維持できるよう本システムでも引き続き合計約 40 台のプリンタが導入されている．省資源のため各プリンタには両面印刷ユニットが実装されたが，保守を要する障害はこれに伴い増加している．

3. PC 実習室システムの利用状況

本節では，2011 年 4 月より運用開始された PC 実習室システムの運用初年度となる 2011 年 4 月 1 日から 2012 年 3 月 31 日までの 2011 年度利用状況を示し考察を行う．この利用状況は PC 実習室システムのログイン・ログアウト情報に基づくものである．本学では，2005 年度より利用者履歴記録システムを稼働しており[7]，この記録情報を採用した．なお，この利用者履歴記録システムでは各利用者の操作内容は記録されないため，ここでは単にログイン及びログアウトに関する情報のみを取り扱う．

3.1. 本学の概要

本学の概要を整理する．学習活動の主体となるキャンパスに関しては，主に黒髪キャンパスで教養教育が実施されているため，低学年次の学生はここで学習する機会が多い．専門課程については，医学部及び薬学部がそれぞれ本荘及び大江キャンパスで，これ以外の 5 学部（文学部，教育学部，法学部，理学部，工学部）はそれぞれ黒髪キャンパスで学習することになる．また，PC 実習室システムの主な利用者となる学部の学生に関してはおよそ 8000 名が在籍している．

3.2. 全 PC 実習室の利用状況

全体の状況を概観するため，全 PC 実習室の情報を統合した年間利用状況を図 1～3 に示す．図 1～3 はそれぞ

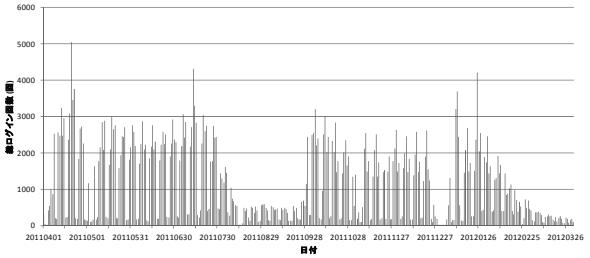


図 1. 全 PC 実習室における総ログイン回数

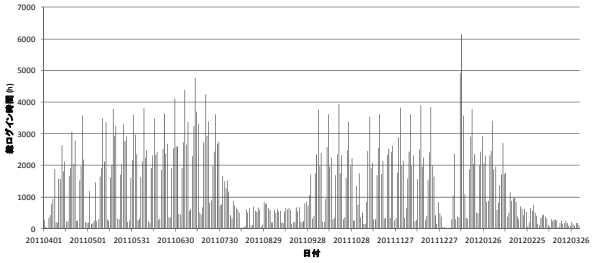


図 2. 全 PC 実習室における総ログイン時間

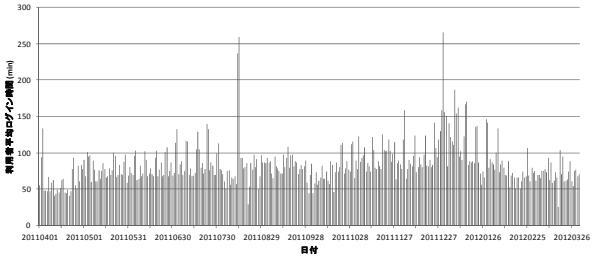


図 3. 全 PC 実習室における利用者平均ログイン時間

れ各日における全実習室分の総ログイン回数，総ログイン時間及び利用者平均ログイン時間を表す.

夏季，冬季及び春季の長期休暇期間を除くと，概ね年間を通して極端に大きな偏りなく PC 実習室が利用されている．週単位では，平日と週末で総ログイン回数及び総ログイン時間が大きく推移しており，主に大学へ通学する平日の利用が多い．一方で，週末の利用者がある程度存在するという状況でもある．図 1 の総ログイン回数に注目すると，2011 年 4 月 20 日，2011 年 7 月 13 日及び 2012 年 1 月 25 日に鋭いピークがみられる．また，図 2 の総ログイン時間では，2011 年 7 月 13 日，2012 年 1 月 10 日及び 11 日に同様の鋭いピークがみられる．以下，各ピークに関して考察を行う. 本学の 2011 年度前学期履修登録の締め切りは 2011 年 4 月 22 日であった．2011 年 4 月 20 日に関しては，この締め切りに伴う利用者の増加と考えられる．本学の全 1 年生を対象に開講される必修科目である情報基礎 A の課題締め切りは 2011 年 7 月 15 日であったが，2011 年 7 月 13 日に関してはこれに伴う利用増と考えられる. 前学期に開講される情報基礎 A に対して後学期に開講される情報基礎 B では 2012 年 1 月 12 日が課題締め切りとして設定された．2012 年 1 月 10 日及び 11 日に関しては, これに伴う利用増と考えられる. これらの課題は各学期末に実施され，それぞれプレゼンテーション資料及び Web ページの作成が課題として課せられた．これらの増加は情報基礎の受講者が各締め切り前に学内の PC 実習室で集中的に課題へ取り組んだ結果とみられる．なお，情報基礎 B の課題は学内 LAN からのみアップロード可能な制限が設けてあるが，情報基礎 A の課題アップロードには制限がなくインターネット経由で行うことが認められている．なお，情報基礎 A・B はともに約 1800 名の学生が受講している科目である. 2012 年 1 月 25 日に関しては，情報基礎 B の講義において PC の再起動を伴う演習が行われたためにログイン回数が急増したと考えられる. 情報基礎 B の講義では各 PC で特に障害が発生しない限り基本的に講義開始から講義終了まで各学生は PC で Windows 7 を起動してログインしているため，通常は 1 回の講義につき 1 回のログインとなる．ところが，この日に行われた講義では Linux (Ubuntu)で再起動して各 PC を Web サーバとして稼働するという演習が含まれるため，まず Windows 7 で PC へログインした後, 講義中に 1 回以上の PC 再起動を行う. したがって，受講者はその日 2 回以上の PC 起動を行うことになり，これがこの日（週）の総ログイン回数に影響したと考えられる．2012 年 1 月 25 日を除くと，いずれも締め切り前は PC 実習室の需要が極めて高いことがわかる．図 3 のグラフでは，利用者平均ログイン時間が 200 分以上となる日が数日あるが，これらはいずれも休祝日で利用者が極端に少ない日であった．このため，少数のログインの影響を受けて高い値を示している.

3.3. 各 PC 実習室の利用状況

PC 実習室ごとの年間利用状況を図 4～6 に示す．これらのグラフはそれぞれ 2011 年度 1 年間の統計を表す.

図 4 の総ログイン回数及び図 5 の総ログイン時間とも，黒髪キャンパスにある附属図書館本館(LIBK)の PC 実習室利用が極めて多い. 図書館に設けられた PC 実習室は，基本的に講義で利用されることがなく利用の際に（実習室での）講義の有無を気にしなくてよいこと，附属図書館が開館中であれば利用可能なこと，また，その利用可能な時間帯が他の実習室と比較して広いこと等がこの要因と考えられる．図 4 及び図 5 の各グラフでは，休祝日の総ログイン回数及び時間が通年のそれぞれと比較して少ないことが確認できるものの，休祝日の値が他の実習室における（平日も含めた）通年の各値に迫るかまたはそれを上回る PC 実習室も存在する．ところで，本学の

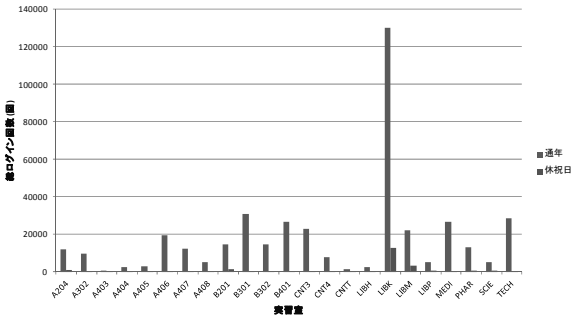


図 4. 実習室別年間総ログイン回数

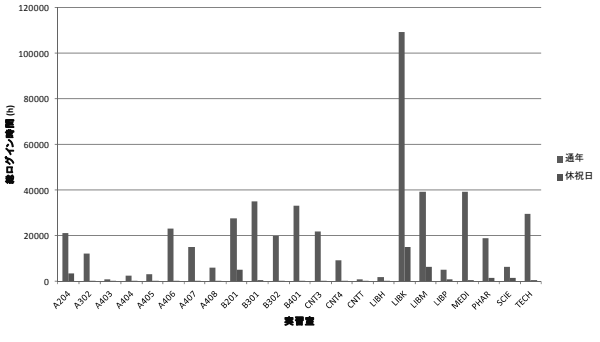


図 5. 実習室別年間総ログイン時間

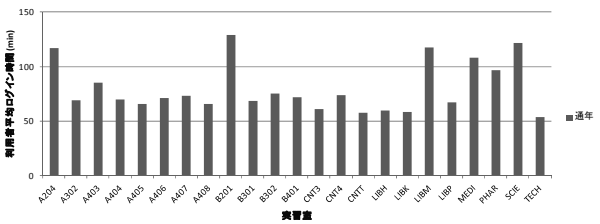


図 6. 実習室別年間利用者平均ログイン時間

講義時間は 1 コマ 90 分であるが，図 6 のグラフから 1 コマの講義時間より長時間 PC にログインして利用されている実習室があることもわかる．

3.4. 休祝日の利用状況

以上の結果から，平日と比較すれば少ないが週末も含めた休祝日の PC 実習室利用がある程度行われていること，休祝日のみの利用でも他実習室の通年並みの利用が行われている実習室が存在することが明らかになった．そこで, 図 1～3 から休祝日のみを新たに整理したグラフを図 7～9 に示す．

図9のグラフにおいて数日で200分以上の値を示すが，これは図 3 に関して 3.2 節で述べたように少数のログインによる影響を受けたものである．図 7 及び図 8 のグラフにおいてピークを示す 2011 年 10 月 10 日及び 2011 年 12 月 23 日は両日とも祝日であるが，本学では授業日に設定されていたことがわかった．この両日の各グラフにおける値が平日並みに高いのは，平日と同等の実習室利用が行われたためと考えられる．したがって，この両日は休祝日から除外することが妥当である．これを考慮して，この特定の 2 日を除いて全実習室合わせると，休祝日には 1 日あたり平均して約 200 回及び約 300 時間のそれぞれ総ログイン回数及び総ログイン時間の利用が行われた．また，附属図書館本館(LIBK)だけでも，約 120 回及び約 130 時間のそれぞれ総ログイン回数及び時間の利用があった．1 回あたりの平均ログイン時間は全室平均で約 100 分，附属図書館本館で約 65 分であった．

3.5. 附属図書館の利用状況

総ログイン回数及び時間ともに極めて多い附属図書館本館(LIBK)の PC 実習室利用状況について図 10～12 に示す．

図 10 のグラフでは, 前述の前学期履修登録締め切りに伴うピークがみられ，2011 年 9 月末から 10 月にかけても後学期履修登録に伴うピークが生じている（後学期履修登録期間は 2011 年 9 月 30 日～10 月 17 日）．図 11 のグラフにおいても，前述の情報基礎 A・B それぞれの課題締め切りに伴うピークがみられる．特に 2011 年 7 月

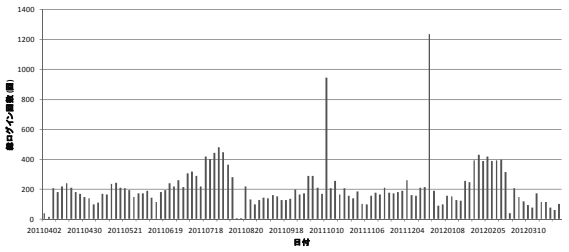


図 7. 全 PC 実習室における休祝日の総ログイン回数

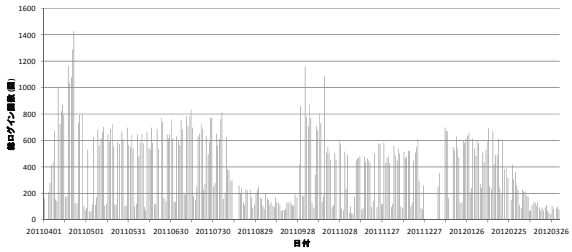


図 10. 附属図書館本館(LIBK)におけるログイン回数

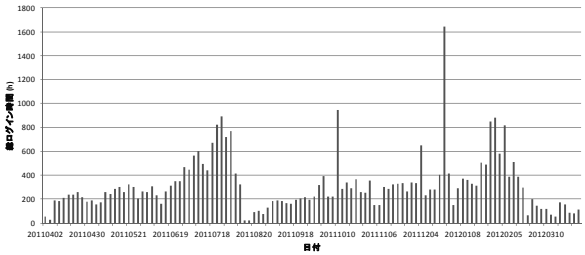


図 8. 全 PC 実習室における休祝日の総ログイン時間

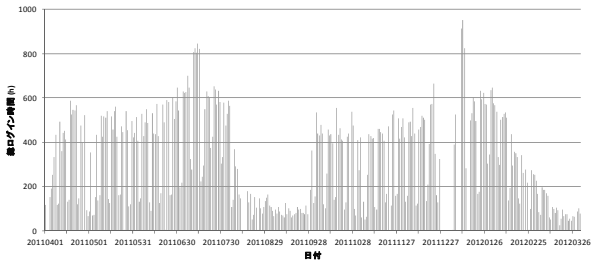


図 11. 附属図書館本館(LIBK)におけるログイン時間

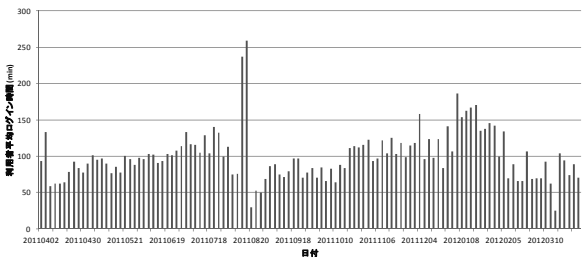


図 9. 全 PC 実習室における休祝日の利用者平均ログイン時間

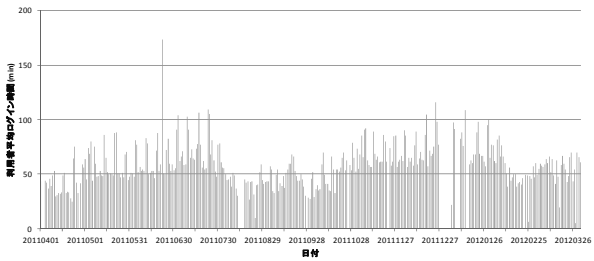


図 12. 附属図書館本館(LIBK)における利用者平均ログイン時間

11 日～15 日及び 2012 年 1 月 10 日～12 日にかけてはログイン時間が各日 800 時間以上を記録する．これらの値は，附属図書館本館の PC 全 88 台を用いて連日約 9～11 時間利用されていた状態に相当する．したがって，この期間中附属図書館本館ではほとんど空席なしの状態で PC が利用されていたと考えられる. 図 12 のグラフで 150 分以上の利用者平均ログイン時間を示す日（2011 年 6 月 22 日）があるが，この日のログインは 1 件のみで教職員による利用であったことから恐らくこの日は休館日だったと考えられる．

附属図書館本館における利用者平均ログイン時間は通年で約 60 分，休祝日のみで約 65 分であるので，平日及び休祝日を問わず 1 回のログインにつき同程度の時間の利用が行われていることがわかる．2011 年度の休祝日における時間帯別年間ログイン及びログアウト数を図 13 に示す. 図 13 のグラフから休祝日も開館時間中は広く利用されていることがわかる．以上のことから，附属図書館本館は本学内で平日だけでなく休祝日にも PC を利用できる場所として役割を果たしているといえる．しかしながら，その役割が高まるにつれ，黒髪キャンパスにおいて休祝日に唯一 PC を自由に利用できる場所となっている点が懸念事項として挙げられる．

4. まとめ

本稿では，2011 年度に運用が開始された PC 実習室システムの運用初年度利用状況について報告を行った．約 1800 名の受講者を抱える情報リテラシー科目やベーシック科目, 受講者数約 1100 名の完全ｅラーニング科目等が定常的に実施されている本学においても，特定の PC 実習室（附属図書館本館）に利用が集中していることが確認された．

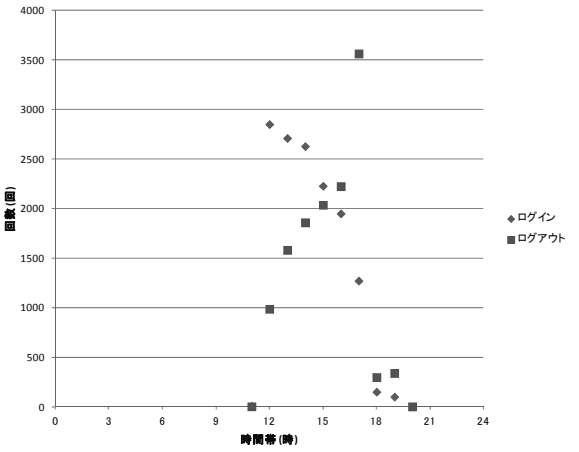


図 13. 附属図書館本館(LIBK)における休祝日の時間帯別年間ログイン及びログアウト数

参考文献

[1] 中野 裕司，杉谷 賢一，入口 紀男，喜多 敏博，松葉 龍一, 右田 雅裕, 武藏 泰雄, 太田 泰史, 合林 亨, 辻 一隆，島本 勝，木田 健，宇佐川 毅： 全学共通情報基礎教育におけるオンライン繰返しテストの学習効果, 第 3 回 WebCT 研究会予稿集, pp.71-76 (2005).

[2] 熊本大学： 1 年次生のためのキャリアガイダンス, http://www.kumamoto-u.ac.jp/careersupport/shiennaiyou/1_2kaisei.

[3] 右田 雅裕，杉谷 賢一，松葉 龍一，中野 裕司，喜多 敏博, 入口 紀男, 武藏 泰雄, 辻 一隆, 島本 勝, 木田 健，宇佐川 毅： LMS を用いた学期末試験としての一斉オンラインテスト，学術情報処理研究誌, No.11，pp.14-22 (2007).

[4] 宮下 健輔，水野 義之： 京都女子大学における全学情報教育とそれを支える情報システムの変遷に関する考察，情報処理学会論文誌，53，3，pp.997-1004 (2012).

[5] 佐々木 正人, 斎藤 卓也, 石黒 克也, 豊永 昌彦：高知大学総合情報システムの監視と利用者動向，学術情報処理研究誌，No.14，pp.64-71 (2010).

[6] 右田 雅裕, 杉谷 賢一, 久保田 真一郎, 武藏 泰雄, 永井 孝幸, 入口 紀男, 喜多 敏博, 松葉 龍一, 辻 一隆，島本 勝，木田 健，宇佐川 毅，中野 裕司： コストに配慮したキャンパス全域ギガビットネットワーク, 学術情報処理研究誌, No.14, pp.48-57 (2010).

[7] 久保田 真一郎, 杉谷 賢一, 武藏 泰雄, 中野 裕司, 永井 孝幸，入口 紀男，右田 雅裕，喜多 敏博，松葉 龍一，辻 一隆，島本 勝，木田 健，宇佐川 毅：パソコン実習室型講義におけるプレゼンスタイプ出席管理システムの構築とその評価，学術情報処理研究誌，No.13，pp.24-31 (2009).

ISMS 導入のための情報セキュリティインシデントコスト定量化について

For quantification information security incident cost in the introduction of ISMS

永井好和† 市川哲彦† 長谷川孝博※ 小河原加久治‡ 多田村克己‡

Yoshikazu NAGAI† Yoshihiko ICHIKAWA† Takahiro HASEGAWA※

Kakuji OGAWARA‡ Katsumi TADAMURA‡

ynagai@yamaguchi-u.ac.jp†, ichikay@yamaguchi-u.ac.jp†, cithase@ipc.shizuoka.ac.jp※,

ogawara@yamaguchi-u.ac.jp‡, tadamura@yamaguchi-u.ac.jp‡

†山口大学 大学情報機構メディア基盤センター ※静岡大学 情報基盤センター

‡山口大学大学院 理工学研究科

†Media and Information Technology Center, Organization for Academic Information, Yamaguchi Univ.

※Center for Information Infrastructure, Shizuoka Univ.

‡Graduate School of Science and Engineering, Yamaguchi Univ.

（要旨）

本論文では，情報セキュリティマネジメントシステム（ISMS;Information Security Management System）導入に際して，人件費を含めた情報セキュリティインシデントコストを定量的に把握する方法を提案する．情報セキュリティインシデントやそれに対する複数の是正・予防措置を，限られた予算枠内で実施するために，各施策の緊急度や重要度の比較に利用可能な指標が必要となる．インシデントにより発生する損失額は重要な指標の 1 つである．損失額としては，インシデントによる逸失利益や壊れた機器などの直接的に発生した損失と，原状回復費用などを合わせて算出すべきである．活動基準原価管理などの作業時間管理を含む個別原価管理を採用している組織では，人件費を含めてイベント毎のコストは原価として把握可能であるが，そうではない国立大学法人においては，個々のインシデントのコスト算出は極めて困難である．しかしながら，このような組織内でも一定の基準単価を定めて作業項目別の所要金額を算出する事は可能である．これらの所要金額の合計値をインシデントコストとみなす事により，インシデント間の大きさの比較が可能となる．ここで算出されるコストは，国立大学法人の会計基準に則った経費を算出するものではなく，インシデント相互の比較の為の定量的数値として意味をもつものである．山口大学では，提案方式を ISMS 構築において適用し，その効果を確認した．

キーワード:インシデントコスト，定量化，ISMS，情報セキュリティ

（Abstract）

We propose a method to quantitatively grasp the cost of the information security incident including the labor cost when the information security management system (ISMS) is introduced. In order to execute several corrective and preventive actions within a limited budget, we need some indicators to compare the level of urgency or importance on each action. The amount of a loss generated by the incident is one of the key indicators. The total amount of loss shall consist of not only the loss directly caused by the incident such as broken equipments and lost profits, but also the indirect cost to recover to the original state. In the organization that adopts the individual cost management including the working hours management like the activity-based management etc., the cost of each event can be understood as a cost including the labor cost. But if the organization does not adopt such accounting, calculating the cost of individual incidents is extremely difficult. However, to calculate the amount required, such values for certain criteria in the organization is possible. By calculating the total value of the amount required by these factors as a incident cost, we can compare the magnitude of the multiple incident in the organization. We applied the proposed method to constructing ISMS in Yamaguchi University, and confirmed the effectiveness.

Key words : incident cost, quantifying, ISMS, information security

1. はじめに

インターネットの普及が進み，情報システムが様々な脅威にさらされている中で，企業において情報セキュリティマネジメントシステム(ISMS；Information Security Management System)の導入が盛んである．国立大学においても，これを導入する動きがある．情報セキュリティマネジメントに関しては，国際規格（ISO/IEC27001）[4]が定められ，これに呼応して JIS 規格（JIS Q 27001）[8]が定められている．この規格への適合性を第 3 者機関が評価・認証する制度も，（財）日本情報経済社会推進協会（JIPDEC；Japan Institute for Promotion of Digital Economy and Community）により運用されている[12]．2012 年 5 月現在，全国で 4,000 を超える組織体がこの認証を獲得している[13]．国立大学法人情報系センター協議会の中に，先行して ISMS 適合性評価制度下での認証を受けた大学を中心として ISMS 研究会が立ち上げられたのも ISMS 導入機運の高まりを表している[5]．JIS Q 27001 の付属書 A.13.2.2 には「情報セキュリティインシデントの形態，規模及び費用を定量化し監視できるようにする仕組みを備えなければならない」という管理策が記載されており，情報セキュリティインシデントの費用を定量化して監視するように求められている．

製造業などの企業において個別原価計算[3]を採用している場合，個々のインシデントコストは原価として把握される．情報処理産業などにおいても，情報システムの開発原価を把握するため個別原価計算制度を採用する企業があり，そこでは，人件費も個別の案件ごとに把握して製造原価に組み入れている．また，活動基準原価計算（ABC;Activity-Based Costing）を採用して，業務毎の原価を把握している企業や自治体では，業務ごと(あるいは，作業項目ごと)の人件費についても把握されている[7]．以下，このような法人を「作業別人件費算出法人」と称する．作業別人件費算出法人においては，従業員の作業項目別の所要時間を集計し，人件費が原価計算に組み入れる仕組みが確立されている．このような法人の中でも，インシデント対策が作業の 1 つとして取り扱われる場合とそうでない場合とがある．後者においてはインシデントを発生させた業務のコストの中に含めて集計され，インシデントコストとして認識されないこともある．ISMS 適合性認証を受け ABC を採用している市川市などの自治体においては，業務別人

件費は把握しつつもインシデント対応に要したコストのみを抽出して把握することはなされていない[1]. 一方, 国立大学においては, 国立大学法人化の際に企業会計が導入されたとはいえ, 人件費を作業別に捉える仕組みにはなっていない[15]. 個別の業務ごとのコストを把握する仕組みはなく, インシデント対策作業毎に人件費などのインシデントコストを定量的に把握する習慣や仕組みもない. したがって, JIS 規格に適合した ISMS を構築するには, コスト定量化(算出)の仕組みを新たにつくる必要がある. すなわち, インシデントコストの要素を明確にして計算方法を確立する事が求められる. 本論文では, インシデントコスト算出の仕組みがないという ISMS 構築時の課題を解決する為に, 先行事例[9]などを踏まえて算出モデルを構成したうえで, インシデントコスト算出の仕組みを提案する. 提案に際して, モデル組織を想定して説明する. 提案する方式は, 個別インシデントに費やした人件費を含めてそのコストを算出し, 売上や利益という概念を必要としない国立大学における逸失利益を推計している点, さらには, インシデントの規模を 1 つの指標(金額)で比較可能としている点, 等の特徴がある.

2. 一般的なインシデントコスト算出方法と国立大学法人への適用上の課題

2.1 インシデント管理の範囲

ISO/IEC27001[4](JIS Q 27001)[8]の補助資料でもある ISO/IEC TR 18044:2004 (Information security incident management)によると「インシデントとは, 望まない又は予期しない単独又は一連の情報セキュリティ事象であって, 事業運営を危うくする確率, 及び情報セキュリティを脅かす確率が高いもの」と定義されている[11]. また, ITIL(Information Technology Infrastructure Library)[2]においては, インシデント管理と問題管理を別のプロセスとして捉えている. 前者の目的は, 可能な限り迅速に異常状態(あるいは非定常状態)を脱して平常状態(あるいは定常状態)に戻す点にある. 従って原因追求よりも早く平常状態に戻すことが優先される. これに対して後者の目的は, インシデントの原因を明確にしたうえで再発や類似事故発生を防止し, 業務への悪影響を最小限に抑える事にある. このため, 問題管理においては, 時間をかけてでも根本原因を追及して是正処置を講ずる事が大切になる. ITIL にいう問題管理の対象となる「問題」の中には, インシデント発生前のリスク対策としての改善要求対応なども含む. インシデントの内容によっては, その対応により平常状態(あるいは定常状態)に回復した後も根本原因追究やその解決策さらには再発予防策の検討・実施・検証の作業が残り, 長期間にわたる対応作業となる場合もある.

本論文では, ISMS 運用下の組織におけるインシデントのコストの算出を目的としており, インシデント発生による異常状態が解消されて管理者への報告が完了するまでの作業をインシデント管理の対象としている. 図 2 は対象範囲内の作業を示すものである. さらに, ISMS 適用範囲内の情報資産(JIS27001 附属書 A.7.1.1 の項で要求される資産目録に掲載される)に係るインシデントを対象とし, これにより発生する損害を算出するべきインシデントコストとする. 本論文では, 前述の図 2 に示されるインシデント管理範囲内の作業に必要なコストの算出方法を提案する.

2.2 一般的なコスト算出モデルにおけるインシデントコスト

ISMS に関する規格(ISO/IEC27001[4]もしくは JIS27001[8])においては, 情報セキュリティの 3 要素(機密性(Confidentiality), 完全性(Integrity), 可用性(Availability))を維持することを要求している. 管理対象の情報資産全てにおいて, 障害によってこれら情報セキュリティが阻害される可能性がある. 情報処理推進機構(IPA;Information-technology Promotion Agency, Japan:旧情報処理振興事業協会)の

「被害額算出モデル」報告書[9]によれば，組織体にとって被害額の把握が重要である．生じる損失額には，「情報セキュリティインシデントに関わる調査　調査報告書 Ver1.0」[10]によれば，表 1 のような項目があり，インシデントコストは各被害額の合計額である．同報告書に被害額項目の算出式が明記されているものについては，表 1 の備考欄に記載している．ここでいう「被害額」の合計が本論文の「インシデントコスト」にあたる．「被害額算出モデル」報告書[9]では，算出モデルと推計値として算出する範囲が提示されており，2 次的被害額は対象外としている．前記 2 つの報告書いずれにおいても，「インシデントコストの把握が重要であるにもかかわらず，我が国の企業や組織において充分把握できていない」と書いている．実際，著者らが調査した限り，インシデントの対応事例や対策技術等に関する文献はあるが，インシデントコストに関する他の文献の存在は確認されていない．前記文献[9,10]におけるコスト算出方式は，一般企業を想定しており，売上，原価，利益が明確な場合に適用可能な方法である．国立大学法人への適用にあたっては，幾つかの解決すべき課題（次節参照）があり，そのまま適用することは出来ない．本論文では，これらの課題を解決したうえで，国立大学法人におけるインシデントコストの算出方式を設定し提案する．なお，本論文では可用性を阻害するインシデントに限定してそのコスト算出について述べる．

2.3 国立大学法人への適用上の課題

前節で述べたコスト算出方法の国立大学法人への適用に際して表 2 の 3 つの課題がある．提案するコスト算出方式が必要とするデータを収集する仕組みが必要な事は言うまでもない．以下，表 2 記載の課題について順に説明する．

ここで，図 1 のサーバ側ネットワークスイッチ（以下，スイッチ）が故障し，これを予備の機器に交換して 1 時間後に回復した事例を考えてみる．この場合，消費したコストは取り替えたスイッチの費用だけではない．原因究明や障害部位の特定や機器入れ替え後の動作確認など，対応には人件費が必要である．国立大学法人においては，故障し交換した機器（スイッチ）の費用（価格）はコストとして扱うが，原因究明や障害部位の特定，あるいは機器の動作確認などに要した人件費は，従来インシデントコストには参入しない．結果として当該インシデントコストに含まれる人件費を 0 円と見なすこととなる．国立大学法人においては，個別イベント毎に要した人件費を捉える仕組みが制度化されておらず，これら個別案件対応の人件費を算出する習慣もない．表 1 の項番 2「復旧に要したコスト」の中の人件費など，インシデントコストに占める人件費を算出するために，個別のインシデント対応作業時間を記録し，人件費を算出する方法を確立する必要がある．これが第 1 の課題である．

もちろんコスト計算作業そのものにもコスト（人件費）が必要である．注意を要するのは，業務運営への影響の小さいインシデントに対してもコスト計算作業は必要であるということである．対策の為の作業量が小さいインシデントに対して過大な手間や時間をかけてコスト計算を実施することは本末転倒と言わざるを得ず，コスト算出の対象とすべきインシデントの範囲を適切に決定するべきである．これが第 2 の課題である．

さらに，表 1 の中の「売上」や「利益」は国立大学法人においては意味をなさないため，一般的なコスト算出法を国立大学法人に適用するに当たっては，逸失利益の定義及びその定量化が必要である．また，表 1 記載の多くの被害額の項目は，個別のインシデントに対して確定するのが困難な情報である．とりわけ表 1 の「潜在化被害額」（項番 7～項番 9）は，企業を含むほとんどの組織においても算出することが極めて困難である．前出の文献[9]においても「2 次的被害額」（表 1 の項番 3～6 及び項番 8～9）については推計することを断念している．これらの項目については，国立大学法人においての評価方法や定量化方法を決定する必要がある．これが第 3 の課題である．

3. インシデントコスト算出モデル

この章では，国立大学法人のモデル（本章では単にモデルという）として大学のキャンパスネットワークを例として，これを維持管理する情報系センター（以下，センター）におけるコスト算出対象範囲を設定し，インシデント別の人件費の考え方を説明する．

3.1 国立大学法人のモデル

キャンパスが複数(m)あるとし，各キャンパス A_i(i=1,2,…,m)では，n_i 棟の建物がキャンパスネットワークで結ばれていて，各建物（図 3 では A_{ij}(i=1,2,…,m；j=1,2,…,n_i)棟と表示）間はスイッチ同士で接続されており，センターは各建物の入り口であるスイッチ迄を管理していると設定する．当モデル（図 3）では，1 台の端末には，センターが管理する IP アドレスが 1 つ割り当てられている．各建物のスイッチの先には，スイッチが接続され，さらにその先にユーザの PC やサーバが q_{ij} 台接続されている．場所によってはサブネットが接続されるケースもある．本論文では議論を簡単にするため，各キャンパス A_i 内の建物の数（n_i）や各建物 A_{ij} 内の端末数（q_{ij}）が同数であるものとし，それぞれ n，q とする．さらに，ネットワークに接続される機器には IP アドレスが割り当てられ，全てセンターに届け出てセンターが管理する DNS (Domain Name System)に登録されているものと設定する（ここでは，IP アドレスの数は端末数と等しい）．大学内には，自らサブネットを構成し，サブネット内のローカルアドレスを各機器に IP アドレスとして割り当てて，中心となるサーバのアドレスのみをセンターに届けている場合がある．この場合はサブネット全体を 1 台の機器と扱う．

3.2 センターサービスとコスト計算対象インシデント

モデルにおいてセンターは，サーバを設置して学内に各種 IT サービスを提供している．図 4 は，モデルのキャンパスの1つ（A_i）においてセンターが提供するサービスの利用範囲とセンターの保守範囲を示している．サービスの利用範囲（図 4 の淡く網掛けしている点線内の範囲）とは，インシデント発生時に影響を受ける範囲であり，業務効率低下を伴う範囲でもある．各建物内のスイッチより先のネットワークについては，各部局のネットワーク管理者が設置されており，センターの管理外としている．センターはこの範囲内に影響を与えるインシデントについて対策を行い，国立大学法人としてのインシデントコストを算出する．ただし，後述のように軽微なインシデントについてはコストの算出を省略する．この範囲は，サービスの種類（たとえば，メールサービスやデータストレージ提供サービス，等）によって，学内全体の場合もあれば特定の範囲に限定される場合もある．保守範囲（図 4 の濃く網掛けしている範囲）とは，センターがその範囲内の機器を維持管理する範囲であり，センターが対策するべきインシデント発生時には，修復のための保守部品などをセンターの予算にて調達する．保守範囲以外のサービス利用範囲内で発生するインシデントに対しては，センターは対応作業を実施するが，修復のための保守部品などの調達にセンターの予算を使わない．保守範囲には，学内ネットワーク機器を含めて，サーバ室等のセンターが管理する施設に設置されている機器全てが保守範囲に含まれる．

4. 課題への対応

4.1 作業別人件費算出方法の確立（第 1 の課題）

4.1 1 人件費の考え方

人件費については，時間単価（円／人時）に所要時間を乗じた金額を算出すれば良いが，時間単価の設定が極めて困難である．厳密には，実際に対策に当たった要員毎の時間単価（教職員の給与等を元に個人別に算定される金額）を基に算出すべきであるが，プライバシーの問題と個人毎に単価を設定することによる計算の煩雑さを避けることも必要である．そのため本

論文では，公開されている情報[6,14]から，全学の常勤教職員の平均年間給与を所定年間勤務時間で除した金額を時間単価と設定し，インシデントコスト中人件費合計 C_0 は，4.1.2～4.1.4 に記載するような計算方法により算出される．本論文では年度内異動の少ない常勤職員に関する公開情報をもとに算定し，全学共通の数値を設定することとしている．これにより，インシデント毎の作業時間が判れば，対策に要した人件費が算出できる事となり，第 1 の課題に対応できたこととなる．最近では，常勤教職員以外にも非常勤教職員が障害対応するケースもある．しかし，時間単価設定方式については本提案の本質的な部分では無いことから，年間の就業期間や就業時間の把握が困難な非常勤職員を除外し，大学全体で一定の指標でインシデントの規模を比較することとしている．

4.1.2 作業工程と人件費

(1) 組織 A における教職員の時間単価は，全員共通かつ全工程で共通とし年度毎に算出して設定するものとする．一般的には，当該作業に従事する教職員の資格や年齢により時間単価は異なるが，ここでは説明と集計作業を単純にするため，組織 A 全体に亘って均一な時間単価を設定する．

(2) 国立大学法人（本章では以下，組織 A）は，N 人の教職員から構成される．それぞれの教職員を E_i (i=1,2,…,N)と表示する．

(3) 組織 A が各教職員 E_i のために負担する年間人件費は固定金額とし，C_i (i=1,2,…,N)と表示する．

(4) 組織 A のすべての業務がプロジェクト体制で推進され，各プロジェクトには番号が振られて，それぞれを P_j (j=1,2,…,M)と表示する．M は，本論文で対象とするインシデント発生年度（以下，当年度）の組織 A のプロジェクトの総数である．

(5) 組織 A では，組織内業務（各プロジェクト）を遂行する上での作業項目を分類しており，それぞれを工程と呼んで W_k (k=1,2,…,L)と表示する．

(6) 全ての教職員は，並行して複数のプロジェクトメンバーとなり，作業を進める．

(7) 教職員 E_i がプロジェクト P_j において工程 W_k のために $t_{(i,j,k)}$ の時間を費やしたと想定する．

4.1.3 時間単価の設定と人件費算出式

(1) 当年度の組織 A における総作業時間 T は，$T=\sum_k \sum_j \sum_i t_{(i,j,k)}$ となる．

(2) 組織 A の当年度の人件費合計は，$C=\Sigma C_i$

(3) 組織 A における当年度の作業時間単価は，$C_u=C／T$ と設定される．

4.1.4 インシデント対応作業と人件費

(1) あるインシデントへの対策を，n 人の教職員 E_h (h=1,2,…,n)[{E_h | h=1,2,…,n} ⊂ {E_i | i=1,2,…,N}]からなるプロジェクト P_0 として実施するものと設定する．

(2) 各教職員 E_h が，当該インシデント対策のため（現状復帰のため）それぞれ工程 W_k の作業を $t_{(h,0,k)}$ 時間実施するものと設定する．

(3) 当該インシデント対応のための作業時間の合計 t_0 と人件費 C_0 は，次式で計算される．

a. $t_0 = \sum_k \sum_h t_{(h,0,k)}$

…インシデント対応作業時間合計

b. $C_0 = C_u \times t_0$

…インシデントコスト中の人件費合計

4.2 インシデントコスト算出範囲の限定（第 2 の課題）

インシデントコスト算出作業のためのコストがインシデントコストの大半を占めるほど（逆に言えば，小さなインシデント）であれば，損失額を大きくしない意味でも，当該インシデントのコスト算出を省略すべきである．また，従来コストを定量的に把握する仕組みや習慣がない組織の場合，ISMS 導入当初においては，より重要なインシデントのコスト算出作業に限定するとともに，個々の計算精度を追求するよりも，個別インシデントのコスト評価を着実に実施していくことが大切で

あり，コスト算出作業による本来の業務時間の減少を極力抑えるべきである．ISMS におけるPDCA 実施過程（Plan，Do，Check，Actionをサイクリックに実施していくことをいう）の中で，順次仕組みを充実していくことを前提とし，本論文では，可用性喪失時間が一定時間以上の場合や，影響を受けた範囲が一定の範囲以上の場合等の重要なインシデントにコスト算出範囲を限定する．すなわち，定量化の範囲を現実的に可能な範囲 [1]に限定することにより第 2 の課題を解決する．閾値など具体的な条件は，ISMS に組織 A の経営陣に認められた ISMS 実施手順の中で規定する．

本論文では，教育用計算機を含む学内ネットワークの停止を重要視し，前述の ISMS 実施手順で規定された条件に該当する場合にインシデントコスト算出の対象とすることで議論を進める．

4.3 逸失利益の定義と算出方法の決定（第 3 の課題）

可用性に関わるインシデント（学内ネットワークや機器の停止）では，表面化する 1 次的被害の1つに逸失利益がある．本来稼働していれば実施された業務により生産されたはずの付加価値が得られないからである．企業の場合と異なって売上額等の評価指標がないため，本論文では，本来生み出されるべき付加価値を生み出すための費用を評価指標として設定する．表 3 は，表 1 を国立大学のインシデントに当てはめたものである．このインシデントにおけるコストを，

表 3 の項番 1 から項番 4 の各被害額の合計金額

と設定する．

ネットワークや機器の停止に関する逸失利益の算出では，全学の端末台数に応じた損失額を算出するが，複数キャンパスあるいは複数の建物の中にある端末台数（3.1 節の q_{ij}）を同数（3.1 節の q）とみなすことにより，コスト算出を簡便にする．影響を受けた機器の台数を正確に把握すれば，より正確なコスト算出が可能である．しかし，4.2 節で述べたように，正確さを追及するあまり作業を困難にすることを避けて着実にコスト算出を可能とするため，簡略化している．表 4 は学内ネットワーク停止に関する逸失利益算出方法を表している．機器の停止に関しても同様の考え方で逸失利益算出表を用意する．表 4 で算出される金額は端末が全く使えなくなった場合であり，業務効率低下による被害額算出式に記載のある「サービスへの業務依存度（重み）」は 1.0 である．端末は稼働しているものの一部のサービスのみが停止する場合，この数値は 1 以下になる．また，サービスを受ける個人によって，個々のサービスへの依存度は異なり，その値を決定する際にはその人の主観も入ると考えられる．この数値を客観的に決定する方式については，のちに述べるように今後の課題でもあるが，本論文では実用性を重視して，センター所属員へのアンケートにより，コスト計算上考慮するサービス項目とそれによる業務依存度（重み）を表 5 の通り設定する．もちろん，ISMS の PDCA 実行過程において定期的に見直されることにより，逐次精度を高める事を前提としているのは言うまでもない．一部のサービスが停止した場合，表 5 に示す各種サービスへの業務依存度（重み）を乗じた数値により業務効率低下による被害額を算出する．複数のサービスが停止する場合には，それらそれぞれの重みを加算する．ただし，合計が1を超える場合には，1.0 を合計値とする．大学によっては，表 5 に掲載されていないサービスを提供する場合もあるが，本論文では主要な（インシデントによる影響が比較的大きい）サービス項目を挙げている．

4.4 インシデントコスト計算に必要な情報

情報セキュリティ事象の処置が終了し平常状態に戻った時には，図 2 記載のとおり，コスト計算ワークシート（対応報告書）を作成し管理者に報告すると同時に，コスト計算のための情報を ISMS 事務局 [2]宛送付して当該インシデントについてのコスト計算を実施する．本論文では，コスト算出に必要なデータを説明するため，図 5 にコスト計算ワークシートの例を示し，コスト計算

に必要なデータ項目を明確にする. 図 5 の中で薄く網掛けした項目がコスト計算に必要なデータ項目である. 図 6 は, 図 5 の逸失利益に関する影響範囲(①～⑤)と障害の重み(①～⑥)の種類を凡例として示す図表である.

図 5 のワークシートにおいては, 原状復帰迄の時間(t 時間), 影響範囲(G ¥/時), 障害の重み(B), 対応者別作業時間(C1 人時～C4 人時), 旅費(D k¥), 物品購入費用(E k¥), その他(F k¥), 影響を受けた端末台数(r 台), 影響を受けてサービスが低下した時間(K 時間), 人件費単価(Uk¥/人時)の 10 項目である. ( )内は図 5 の中の対応するデータ項目につけた記号とその単位である. 影響範囲については, 図 6 凡例 A の①～⑤のいずれかに対応する算出式で計算される時間当たりの被害額(G)を決める. 障害の重みについても, 図 6 凡例 B の①～⑥のいずれかを選択して, 同凡例に従い重みを決定する. 決定の方法は 4.3 節の表 5 についての説明のとおりである. 図 5 の逸失利益欄の 5 定数のうち r 以外の数値は国立大学法人毎の定数であり, r はインシデント毎に決定される数値である. 可用性に関するインシデント(M k¥)は, これらのデータに基づき次式で計算される.

$$M = G \times t \times B/1000 + (C1+C2+C3+C4) \times U + D+E+F+ r \times B \times K \times U$$

ここで, 人件費単価 U は, 4.1 節で説明した考え方に基づき設定されており, 国立大学法人毎に異なる値が設定されるべきである. また,「影響を受けた端末台数」については, センターが管理するネットワークにおける DNS サーバ(Dmain Name Server)に登録される IP アドレスの数を使用する. センターが提供するネットワークサービス範囲と一致することがその理由である.

5. 提案方式の試行と検証

5.1 定量化方式(提案方式)適用事例

ここ迄の計算方法を, 2.3 節に記載した具体例に適用してみる. まず, 人件費の単価に関しては, 筆者所属大学の場合, 平成 20 年度一人当たり年間給与額が 6, 642 千円, 年間勤務時間数 1,944 時間であるため, 時間単価は約 3,417 円となる. そこで, 通常千円単位でインシデントコストの算出を行うことから, 百円単位迄で丸めて時間単価を 3,400 円と設定した.

2.3 節に記載した具体例では, 1 つの校舎(建物)全体において 1 時間のサービス停止に遭遇し, 6 名の教職員が延べ 5 時間をかけて対処している. アクセスできなくなったサーバは共用データベースを提供するものであるとともに, メールサーバを兼ねていたものである. 壊れたスイッチの簿価が1万円, 新たに購入して交換したスイッチの価格が 10 万円であった. また, この障害の間, 当該校舎(建物)内の全ての端末がネットワークに接続できなくなった. キャンパス内の建物の数が 4 棟, また, 当該キャンパスにおけるネットワーク維持コストは月額 480 万円, 端末台数は 500 台であった. (人件費の時間単価は前述の通り 3,400 円である.)この場合, コストは次のように計算され, a～c の合計で 98 万 2 千円となる. これを表 4 の各変数に代入すると, Y=4,800/240=20, m=1, q=4 である. (設定値は図 5 記載の値と異なる.)

a. 逸失利益 : Y/m/n = 20/1/4/＝5(k¥)
b. 復旧に要した費用 : 10(壊れた機器の価格)＋100(代替品購入価格)＋3.4×5(復旧作業人件費) ＝ 127(k¥)
c. 業務低下による被害額 : 3.4(人件費時間単価)×500(端末台数)×(0.2(ﾒｰﾙ機能の重み)＋0.3(共有ﾌｫﾙﾀﾞの重み))×1(停止時間)＝850(k¥)

従来このケースにおいては, 機器の価格(10 万円)のみをコストと捉えていた. 人件費を算入しない場合は 10 万円, 算入した場合は約 98 万円, この金額の差(88 万円)を見ても人件費が無視できない大きさであり, 算出することの必要性と提案方式の有用性が判る.

5.2 実務への適用(試行)

山口大学では, 平成 21 年度から実際の ISMS 構築において提案方式を適用し, 平成 22 年 9

月の ISMS マネジメントレビューにおける経営陣への報告に使用した. その報告によれば, その間のインシデントは全てが可用性に関するインシデントであった. その中でコスト計算を実施した 2 件と, 他大学のインシデントコスト計算事例 2 件ついて, その結果を一覧表にしたのが表 6 である [3]. いずれの事例においても, 入れ替えた機器の費用のみをコストとする従来の金額に比べて大きなコストがかかっている事が判る. 表 6 の事例番号 3 においてはサーバ(機器)の交換が必要であったが, 他の 3 件は機器の入替えを必要としない事例である. 表 6 の「差異(B-A)」の欄の様に, 機器の入替えの無い場合, 従来はコスト 0(ゼロ)と評価されていた事例が, 決してそうではないことが判る. 表 6 記載の各案件ごとに作成したインシデントコスト計算ワークシート [4] を見れば, 人件費がほとんどを占めている事が判り, インシデントコストに人件費を算入して, インシデントの大きさを比較することの重要性も浮かび上がってくる. 特に事例番号 1 及び 2 では, 学内ネットワークが全学的に停止したことによる影響として業務効率低下による損失が大きな金額となっている. マネジメントレビューでは, 人件費の一部が障害対応に使用されている事実を目に見える形で報告がなされた. 経営陣にもインシデント発生の状況とその対応にかなりの人件費が必要であることに対する理解を得て, 是正のための作業実施とそれによるコスト消費について承認を得ることができた.

6. おわりに

本論文では, インシデントごとの人件費の算出が可能な, 国立大学法人向けのインシデントコストの定量化方式を提案し, 筆者所属大学での適用事例を示した. 提案したコスト算出方式により, 従来インシデントを定量的に把握することなく是正・予防措置を実施してきた組織において, 個々のインシデントの大きさを定量的に把握し, 相互に比較することが可能になった.

さらに, 作業毎の所要時間を記録する習慣がない国立大学法人において, インシデント対応という一部の作業のみとはいえ, 本来(インシデントが発生しなければ)不要であるはずの作業時間の存在を数値で実感させる仕組といえる. これは、表 6 を見れば明らかであり, 少々のコストや要員を投入してでもインシデントを減らそうとするモチベーションに結びつく. 筆者が所属するセンターの ISMS のマネジメントレビューにおいて, CIO(最高情報責任者;Chief Information Officer)がインシデントの大きさを把握し, 対応方法の選択や状況判断するための情報として役立つことも確認できている.

さらに, 本論文でインシデントコストの計算や報告の流れや手順を示した. コスト計算自体にも人件費が必要となるが, コンピュータシステム化して, データ入力を含むコスト計算作業の省力化は可能である. 今後, 個別原価計算制度や活動基準原価計算の採用状況や, ISMS における PDCA 実践状況に応じてコスト計算要素の見直しを行い, さらにはインシデントコストの計算精度を向上させることは課題の1つである.

本論文では, インシデント対応に必要な人件費に着目しているが, 教職員の作業量を作業項目別に把握する仕組みを確立すれば, センターに必要な作業量が可視化され, 要員数と作業量の関係を説明する為の資料としても役立つと考えられる. 作業項目ごとの時間を記録する仕組みを, 教育・研究に従事する教職員の活動全般に広げるべきかどうかは, 今後の検討課題として残る. しかし, 一部とはいえ, インシデントコストを定量的に把握できる提案方式は, 優先順位をつけてリスク対応できる仕組みへの可能性を大きくし, 国立大学法人におけるリスクマネジメントに役立つ成果であり, 広く活用が期待される.

注)

1) ここで言う「現実的に可能な範囲」とは, ISMS を運用する組織体にとって, コスト算出作業その

ものによる作業量増が本来の業務に支障を与えない範囲で，構成員が極端な負担を感じることなく，無理なくコスト計算が実施出来る範囲を意味する．組織体としてその範囲について合意するべきである．

2) 図 2 中の「ISMS 事務局」は，ISMS 運営組織内にあって当該組織における情報セキュリティ責任者を補佐し，ISMS に係る管理事務を担うグループである．インシデント管理に関してはこれを記録しその対策の進捗などをフォローアップする役割を担うグループである．図 2 の中では，インシデントを記録し管理台帳を更新するタスクに関する部分を掲載している．

3) 本論文で提案するコスト算出方式の適用事例として，共著者の一人が所属する静岡大学情報基盤センターの協力を得て，静岡大学のインシデントについてコストを算出したものである．しかしながら表 6 に掲載している 4 件それぞれの大学名は伏せさせて頂いている．

4)「インシデントコスト計算ワークシート」は図 5 を参照されたい．図 5 における「人件費」の欄の金額とインシデントコスト（図 5 の「M」）における割合をみれば本文に記載した事を理解できる．また，表 6 掲載の個別事例の「インシデントコスト計算ワークシート」の掲載は控えさせていただいている．

参考文献

[1] 市川市「ABC(Activity-Based-Costing)について ～活動基準原価計算～」，http://www.city.ichikawa.lg.jp/pla02/1211000002.html （Jun.26.2012）

[2] 英国 OGC（Office of Government Commerce），サービスサポート(2003 年出版)，itSMF Japan,2003

[3] 岡本清，『原価計算六訂版』，国元書房，2000

[4] 国際標準化機構（International Organization for Standardization），*Information technology – Security techniques – Information security management systems - Requirements, International Standard ISO/IEC27001*, ISO/IEC ,2005.

[5] 国立大学法人情報系センター協議会 ISMS 研究会「ISMS 研究会」，http://sigisms-nipc.cc.yamaguchi-u.ac.jp/ （Jun.26.2012）

[6] 国立大学法人山口大学，役職員の給与水準の公表，http://ds.cc.yamaguchi-u.ac.jp/~jinjika/kyuuyo/housyu_kyuuyo.html （Jun.26.2012）

[7] 櫻井通晴ほか，『ABC の基礎とケーススタディ ABC からバランスト・スコアカードへの展開』，東洋経済新報社，2004

[8] 島弘志，『JIS Q 27001(ISO/IEC27001)情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項』，JIS 規格 ，2006.

[9] 情報処理振興事業協会（現，情報処理推進機構）セキュリティセンター，『「被害額算出モデル」報告書』，p1&pp7-10，情報処理振興事業協会，2003

[10] 情報処理振興事業協会セキュリティセンター：情報セキュリティインシデントに関わる調査調査報告書 Ver.1.0，pp.17-20，情報処理振興事業協会，2002

[11] 中野康二・中野初美・平野芳行・吉田健一郎，『ISO/IEC 17799:2005 詳解情報セキュリティマネジメントの実践のための規範』，pp292-304，日本規格協会，2007

[12] 日本情報経済社会推進協会（JIPDEC），ISMS 適合性評価制度，http://www.isms.jipdec.jp/isms.html （Jun.26.2012）

[13] 日本情報処理開発協会（JIPDEC），ISMS 認証取得組織数推移(2010 年 5 月)，http://www.isms.jipdec.jp/lst/ind/suii.html （Jun.26.2012）

[14] 文部科学省，国立大学法人等の役職員の給与等の水準（平成 20 年度），http://www.mext.go.jp/b_menu/houdou/21/07/attach/1282400.htm （Jun.26.2012）

[15] 文部科学省,「国立大学法人会計基準」及び「国立大学法人会計基準注解」に関する実務指針(平成 15 年 7 月 10 日, 平成 23 年 2 月 15 日改訂版), http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2012/04/09/1289344_06.pdf （August.1.2012）

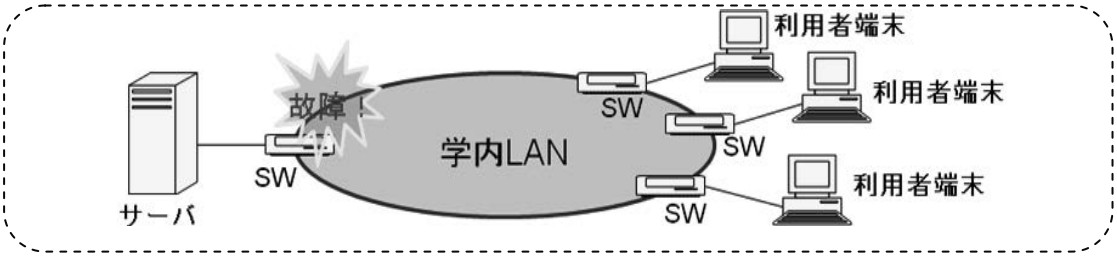


図 1　ネットワークスイッチ故障イメージ図

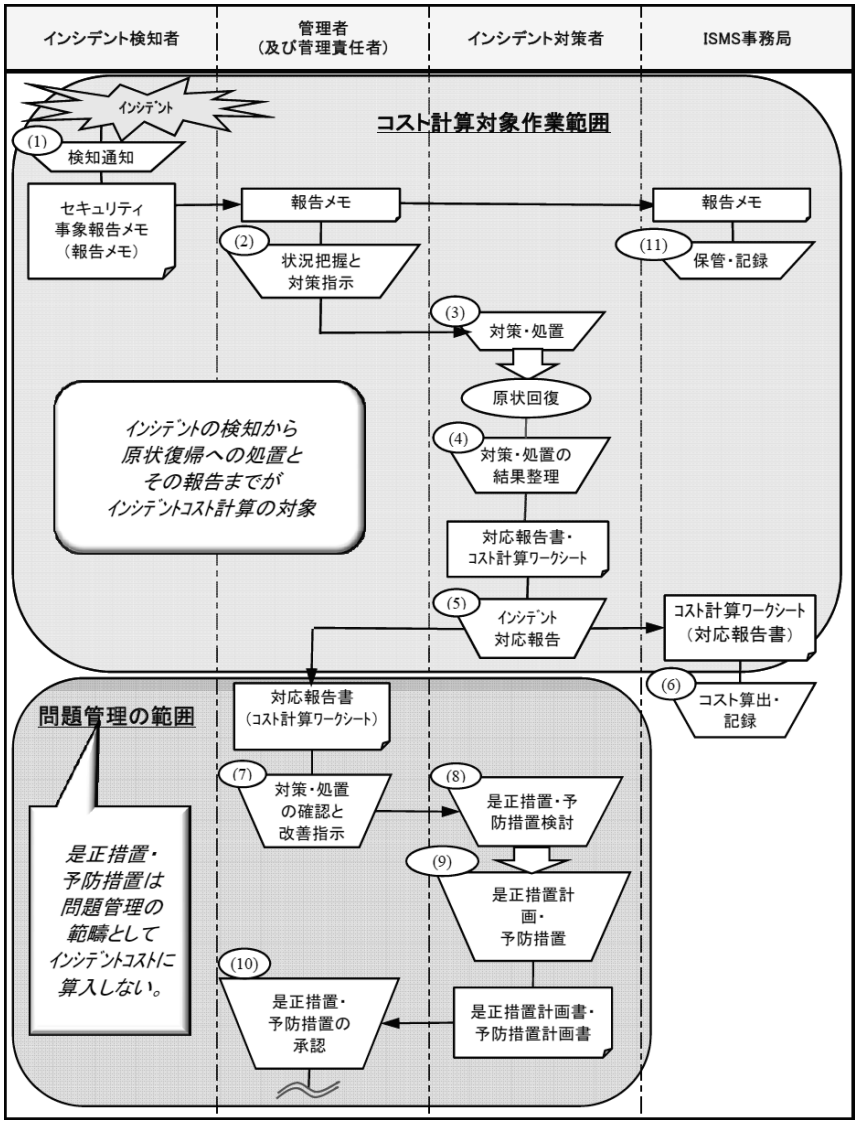


図 2 インシデント報告の流れ

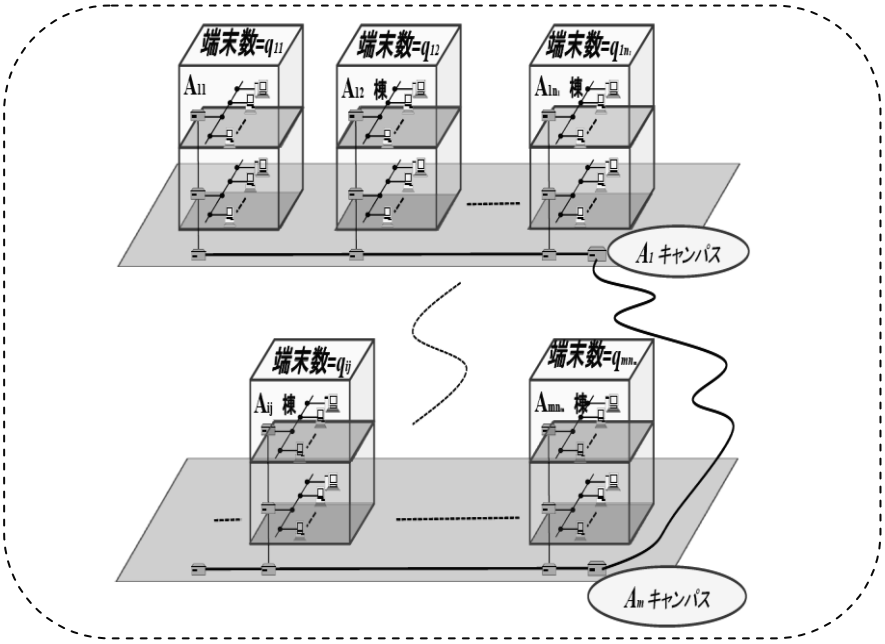


図 3　モデルキャンパスのネットワークイメージ

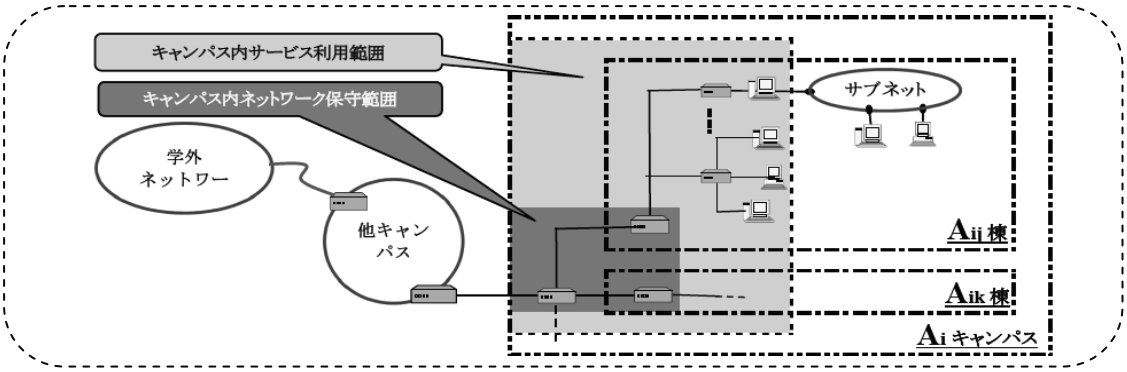


図 4　ネットワーク監視と保守の責任範囲イメージ図

障害NO.：

障害名称 ：		インシデントコスト ： (k¥)	M
発生日時			
原状(正常状態)復帰時刻			
対応完了日時			

(1)	逸失利益 (影響範囲)×(障害の重み)×(現状復帰迄の時間) ……			(補足)
	原状(正常状態)復帰までの時間(時間)		t	(補足)
	影響範囲 (凡例Aの①~⑤を選択)	① ② ③ ④ ⑤	G	(影響の状況)
	凡例A	図6　参照		
	定数 a	4,000,000	月次のネットワーク維持費用	
	定数 m	3	キャンパス数	
	定数 q	200	建物内の端末台数	
	定数 n	10	キャンパス内の建物数	
	定数 r	r	影響を受けた端末の台数	
	障害の重み (凡例Bの①~⑥を選択)	① ② ③ ④ ⑤ ⑥	B	(障害の重み設定根拠)
	凡例B	図6　参照		

(2)	復旧に要した費用(復旧費用)……			(補足)
	人件費	(作業概要)		
	単価: U 3.4 k¥/人時	対応者名	作業時間(人時)	対応作業内容
	①		C1	
	②		C2	
	③		C3	
	④		C4	
	旅費 (k¥)	D	(内訳)	
	物品購入費用 (k¥)	E	(内訳)	
	その他 (k¥)	F	(内訳)	
(3)	業務効率低下による被害額 (a×b×c×3400)……			(補足)
	a. 影響を受けた端末台数		r	
	b. サービスへの業務依存度 (凡例Bの「障害の重み」と同じ)		B	
	c. 影響を受けてサービスが低下した時間		K	

図 5　可用性に関するインシデントコスト計算ワークシート例

	項番	インシデント規模	算出式	説明
逸失利益凡例A	①	全学停止	Y=a/(30*8)　円/時	・月次のネットワーク維持費用をa円，1日8時間とする．月間の日数については，30日とみなす．
	②	キャンパス全体	Y/m　円/時	・キャンパス内の端末台数が各キャンパスで同数であるとみなし，キャンパス数をmとする．
	③	建物全体	Y/m/n　円/時	・建物内の端末台数(q)を建物間で同数であるとみなし，キャンパス内の建物数をnとする．
	④	建物の一部	(Y/m/n)×(r/q)　円/時	・停止により使用不能となった端末の台数をr台とする．
	⑤	計算機個別	Y/m/n/q　円/時	・評価しない
	項番	障害の種類・レベル	重み	説明
逸失利益凡例B	①	全サービスの停止（学内ネットワークの停止）	1.0	・学内ネットワークを利用する全てのサービス（機能）の利用ができない．
	②	認証機能の停止	0.7	・教育用端末・情報コンセント・メールが全て利用不可
	③	拠点間の分断	0.7	・認証機能が停止する．
	④	メール機能の停止	0.3	・学内外の業務上の情報交換機能が停止する．（WEBを参照することは可能な場合）
	⑤	WEBサービスの停止	0.3	・WEBサービスの依存度は限られているため．
	⑥	共有フォルダの停止	0.2	・多くの教職員・学生が利用しているが，共有フォルダを使用しない業務が続行できる．

図 6　可用性に関する逸失利益の凡例

表 1　企業等一般的組織におけるインシデントに係る被害額分類表

項番	大分類	中分類	小分類	備考
1	表面化被害額	1 次的な被害額	逸失利益	「時間当たりの売り上げに対する利益」×「システムないしサービスの停止していた時間」
2			復旧に要したコスト	
3		2 次的な被害額	各種の補償・補填	
4			損害賠償	
5			謝罪広告費用	
6			その他	
7	潜在化被害額	業務に関わる潜在化被害額	業務効率低下による被害額	「固定費（人件費）」×「インシデントによる影響を受けた人数」×「IT 感応度（業務依存度）」×「停止時間」
8		業務外の潜在化被害額	風評被害	
9			企業のイメージダウン	

表 2 国立大学法人への適用のための 4 つの課題

項番	課題	補足説明（必要となる取り組み）
1	作業別人件費算出方法の確立	インシデント毎の作業時間を記録し，インシデント別人件費を算出する仕組みを確立する．
2	インシデントコスト算出範囲の決定	インシデントコストよりもコスト計算作業そのもののコストが大きい場合，コスト計算作業を省略できるように，コスト計算対象範囲を限定する．
3	逸失利益の定義と算出方法の決定	売上や利益のない国立大学法人における逸失利益の金額算出方法を決める．また，一般的にも極めて困難な 2 次的被害額の，国立大学法人における取扱い方法を決める．

表 3　ネットワーク停止による被害額表

項番	大分類	中分類	小分類	備考
1	表面化被害額	1 次的な被害額	逸失利益	・全学停止，キャンパス全体停止，建物全体停止，建物の一部停止，計算機別停止，に分類して表 4 のとおり設定 ・ネットワーク上で，一部サービスのみの停止の場合，表 4 の「サービスへの業務依存度（重み）」を乗ずる．
2			復旧に要したコスト	・「壊れた機器の価格」＋「代替品購入価格」＋「工事費用」＋「復旧作業人件費」
3		2 次的な被害額	各種の補償・補填，賠償費用，謝罪広告費用	・発生しない（謝罪広告費用すなわち Web ページ作成作業費は項番 2 の「復旧作業人件費」に含む）
4	潜在化被害額	業務に関わる潜在化被害額	業務効率低下による被害額	「一人時あたり人件費）」×「影響を受けた端末台数」×「サービスへの業務依存度（重み）」(*1)×「停止時間」(*2)
5		業務外の潜在化被害額	風評被害，イメージダウン	・評価しない

*1:表 5 参照，*2:障害検知時刻から正常状態への復帰時刻迄の時間

表 4　ネットワーク停止による逸失利益算出表

項番	インシデント規模	算出式（円/時）	説明
1	全学停止	Y=a/(30*8)	・月次のネットワーク維持費用をa円，1 日 8 時間とする．月間の日数については，30 日とみなす．
2	キャンパス全体	Y/m	・キャンパス内の端末台数が各キャンパスで同数であるとみなし，キャンパス数をmとする．（3.1 節参照）
3	建物全体	Y/m/n	・建物内の端末台数(q)を建物間で同数であるとみなし，キャンパス内の建物数を n とする．（3.1 節参照）
4	建物の一部	(Y/m/n)×(r/q)	・停止により使用不能となった端末の台数を r 台とする．
5	計算機個別	Y/m/n/q	・評価しない

表 5　サービスへの業務依存度（重み）一覧表

項番	影響を受けるサービス	重み	説明
1	認証機能の停止	0.7	・教育用端末・情報コンセント・メールが全て利用不可
2	拠点間の分断	0.7	・認証機能が停止する．
3	メール機能の停止	0.3	・学内外の業務上の情報交換機能が停止する． （Web を参照することは可能な場合）
4	Web サービスの停止	0.3	・Web サービスの依存度は限られている．
5	共有フォルダの停止	0.2	・多くの教職員・学生が利用しているが，共有フォルダを使用しない業務が続行できる．

表 6 インシデントコスト算出事例 （単位;円）

事例番号	件名	差異(B-A)	A.従来方式によるコスト	B.提案方式によるコスト(C欄内訳の合計)	C. 提案方式によるコスト内訳		
					逸失利益	復旧費用	業務効率低下による被害額
1	ループ配線によるFW上流からストーム	41,945,070	0	41,945,070	36,670	20,400	41,888,000
2	GIP用L3スイッチハングアップ	18,352,243	0	18,352,243	16,043	10,200	18,326,000
3	Webサーバ故障	115,467	200,000	315,467	6,667	227,200	81,600
4	演習室PC接続不可	6,089	0	6,089	139	5,100	850
5	Aキャンパス停電	1,700	0	1,700	0	1,700	0
5 件合計		*60,420,569*	*200,000*	*60,620,569*	*59,519*	*264,600*	*60,296,450*

標的型攻撃メールの予防対策

Protective Measure for Targeted Cyber Attack Mail

伊藤　史人†，高見澤　秀幸†，佐藤　郁哉†
Fumihito ITO†, Hideyuki TAKAMIZAWA†, Ikuya SATO†

ito@cio.hit-u.ac.jp, h.takamizawa@cio.hit-u.ac.jp, ikuya.sato@cio.hit-u.ac.jp

†一橋大学情報基盤センター

† Center of Information and Communication Technology, Hitotsubashi University

概要

標的型攻撃メールは，ある特定の組織や個人を狙った機密情報等を窃取する手段に利用されている．攻撃に利用するメールにはファイルが添付されており，受信者がそのファイルを開くことでシステムの脆弱性等を突き任意のコードを実行する．メールの文面は，受信者が不審に感じ難いものとしていることが多く，完全な防御は極めて難しい．その一方で，効果的な対策としては，教育的効果を狙って模擬標的型攻撃メールを対象者に送り，同種の攻撃に対する意識を高めることが挙げられる．本論文では，標的型攻撃メールを病原体と仮定し，模擬標的攻撃メールを「予防接種」として作用させ，「人」に免疫反応を引き起こすことで攻撃への耐性を高める試みについて報告する．具体例として，一橋大学の学生 196 名と事務職員 200 名に対する模擬標的型攻撃メールを予防接種した結果と，解析結果から得られた今後の対策案について述べる．

キーワード

標的型攻撃メール, Web ビーコン, 脆弱性, 情報漏えい, 個人情報

1. はじめに

標的型攻撃メールは，セキュリティにおいて最も弱点となりやすい「人」をターゲットとしている点に特徴がある．「人」に対する情報セキュリティ対策は，統一的に実施するのは困難である．攻撃手法においては，未知のウイルスや脆弱性を悪用してシステムへの侵入を試みるため，確実な対策は極めて難しい．

そのため，標的型攻撃メールは認知されてから 7 年ほど経っており，もはや新しい手法ではないにも関わらず，未だ完全な対策が打てないのが現状である．今日も公官庁や大手電機メーカーからの機密情報漏えいが止むことはなく，情報セキュリティ対策は依然として対症療法的な対応とならざるを得ない状況が続いている．

セキュリティ対策としては，標的型攻撃メールが「人」に対する攻撃であることから，システムのみによる対策は実効性に乏しく，やはり「人」への対策が必須である．

本論文では，標的型攻撃メールそのものを病原体（抗原）と仮定し，模擬標的攻撃メールを「予防接種」として利用し，「人」に免疫反応を引き起こすことで攻撃への耐性を高める試みについて述べる．

2. セキュリティ対策と標的型攻撃メール

標的型攻撃メールは 2011 年の衆議院議員会館や原子力発電設備関連の情報漏えいで大いに話題になったため，新しい攻撃手法と思われがちであるが，インターネットの歴史の時間軸からみればけっして新しいものではない．ここでは，過去のウイルスメールについて振り返り，標的型攻撃メールの対策について考察する．

2.1. インターネット経由の攻撃活動の変遷

インターネットが一般家庭に普及した 2000 年以降, 大きく分けて 4 段階の攻撃手法に分類することができる[1].

2000 年初頭は,「均一的かつ広範囲にわたる単発被害」と表現することができる. 被害としては Web サイトのページ書き換え等が相当する．当時はセキュリティ対策が甘いサーバも多く，攻撃者は手動でも比較的容易に攻撃を成功させることができた．ユーザのセキュリティ意識も低かったことから，ウイルスが含まれた添付ファイルによって感染が広まった．Happy99 は愉快犯的なウイルスであるが，世間に多く広まったことから，コンピュータウイルスへの意識を高める契機となった．

また，当時の代表的なウイルスは，Nimda や Code Red が挙げられ，これらは無防備なシステムに感染し，ユーザの共有フォルダデータを消去するなど大きな被害をもたらした．さらには，サイバー攻撃を組織的に行うことで情報を窃取し, それをビジネスとする流れも生まれた.

2005 年にかけては,「均一的かつ広範囲にわたる連鎖的被害」となる．攻撃者は攻撃を多様な手段で自動化してマルウェアを流布するとともに, ワームを Web サイトに仕込むことでユーザのシステムを攻撃し，以前よりも広範囲かつ連鎖的に感染させることに成功した[3].

2005 年以降は「類似した局所的な被害」として，SQL インジェクションによる Web サイト攻撃や Winny, Share による情報流出が挙げられる．また，フィッシングやスパイウェア，さらにはボットなどが活発になった時期であった.

そして, 2006 年以降は「すべてが異なる局所的な被害」として標的型攻撃が認知されるようになった．攻撃者は不特定多数を対象にするのではなく，ある目的を持って特定の対象を決めてより確実な攻撃を仕掛けるようになったのである．このことは，以前よりもサーバの堅牢性が増したことと無関係ではなかったと考えられる．サーバのセキュリティ対策に比べ，クライアントについては脆弱性が放置されていることが多く，標的型攻撃はその穴を狙ったものであるといえる．そして，現在，標的型攻撃は完全防御できない攻撃手法として各所で大きな被害を出すに至っている.

2.2. 階層毎のセキュリティ対策

セキュリティ対策を実施するにあたって，一般的には階層毎に対策を行うこととなる.

表 1 にその例を示す.

ネットワーク階層においては，ファイアウォールやフィルタリングによる対策を実施することで，おおむねセキュリティは全体的に向上する．しかし，ネットワークの未知の脆弱性や，正常なプロコトル通信を悪用した被害からは免れることはできない．それらは，ゼロデイ脅威としてセキィリティ対策の大きなウィークポイントとなっている.

サーバおよびクライアントの階層ではウイルス対策ソフトやセキュリティアップデートにより，多くのセキュリティホールを塞ぐことが可能である．ただし，ネットワーク階層と同様に，ゼロデイ脅威となるソフトウェアの未知の脆弱性やウイルスによるセキュリティの低下は必至である．このことから，事前経験のない未知の脅威に対してはやはり完全に無防備であるといってよい.

パケットの振る舞いに着目して未知の亜種ウイルスに対応する手法も研究されているが，まったくの未知のウイルスに対してはやはり効果を発揮しない[2]．亜種ウイルスを予測するにはあらかじめベースとなる本体ウイルスを解析しておく必要があるためである.

最後に「人」の階層でのセキュリティ対策である.「人」は機械と異なり，推測する能力においては極めて高いとされる．その特性を活かすのと併せて，個人への教育や組織体制の見直しにより，ゼロデイ脅威に対して有効な作用を発揮する．機械が行う解析ベースのセキュリティ対策よりも柔軟に対応することが可能である．つまり，未知の脅威に対しても，教育等により完全に無防備になることなく，一定以上の効果を見込むことができるのである.

2.3. 「マスメール型」と「標的型」

ウイスルメールには，コンピュータウイルスに感染したパソコンから更にウイルスメールを送ることで感染を拡大する「マスメール型」と，特定の組織や個人からの情報窃取を目的とした「標的型」に大別することができる[1].

「マスメール型」は愉快犯的なウイルスも含まれており，その脅威は件数のみで判断できない．一方で,「標的型」はその目的から明らかに悪意のある場合が多いと考えられ，今日も重大なセキュリティインシデントを発生させている．そのため，ウイルス届出件数が減少してい

る現在においてもウイルスの脅威は決して減少していない.

なお，ウイルス感染の届出件数は，2005 年の 54,174 件から右肩下がりで減少し, 2010 年には 13,912 件まで減少している[4]．しかしながら，重大な情報漏えい事件はむしろ増加しており[5]，ウイルスの危険性や脅威は件数からはまったく判断できないことが分かる．あらゆる組織が情報化した今，少数の攻撃が過去に例を見ないほどの重大なインシデントを発生させており，脅威の総量はむしろ増大しているといってよい.

2.4. 標的型攻撃メールの攻撃方法とその防衛としての予防接種

標的型攻撃メールの特徴は，前述のように「マスメール型」とは異なり特定の組織や個人を狙っているということである．メールを攻撃対象者に信用させ，添付ファイルを開かせることができれば前段階の攻撃は成功である．次に，添付ファイルがシステムの脆弱性を突いてワーム等を送り込むことができれば攻撃はほぼ成功したことになる．攻撃者としては，まずは前段階の攻撃を成功させなくてはならず，それには対象者を考慮した事前の準備が必須となる．なお，メールヘッダやコードパターンの解析によりある程度の防衛は可能であるが完全に防ぐことはできない[6][7]．ウイルス対策ソフトウェアの定義ファイルに含まれないコードパターンは事前検知が不可能であるが，悪質なコードとの類似性によりある程度の対策は可能である．ただし，必要なメールが誤検知されることもあるため，検知に用いるしきい値設定は一般ユーザには難しい作業となる[8][9].

攻撃者はあらかじめ対象者についての何らかの情報を収集していると考えられる[10]．例えば，対象者の業務内容や人的ネットワーク等である．それらの情報から，攻撃者は信用に足るメール文面を生成する．通知文等の定型文を流用した，やや「マスメール型」的な標的型攻撃メールも存在しているが，対象者像を想定してメールを送り付ける点では，信用に足るメール文面となることには違いはない[11]．その点はフィッシングメールと同じ手法となるが[12]，より文面が巧妙である傾向があるとされる.

また，添付されるファイルは，PDF や Word など日常的に頻繁に利用するファイル形式であるため[13]，対象者が脅威に感じにくいのも対策の難しさのひとつとなっている[14]．メールクライアントのスパムフィルタは統計的な手法を用いる場合については，その効果も限定的なものとなる[15][16].

表 1　階層毎のセキュリティ対策

階層	対応策	効果／欠点
ネットワーク	● ネットワーク監視	○：既知の脆弱性や不審な通信の検知 ×：未知の脆弱性や正常な通信での悪用
	● ネットワーク構成の最適化	○：被害範囲の最小化
	● ファイアウォールの設定（IN/OUT 双方の通信制御） ● プロキシや URL/メールフィルタリング	○:正常でない通信先やプロトコルの悪用を阻止 ×：正常な通信先やプロトコルでの悪用は阻止できない
	● 各種ログのモニタリング	○：被害の早期発見
サーバ	● OS やサーバアプリケーションのセキュリティ修正プログラム適用	○：既知の脆弱性 ×：未知の脆弱性
	● 要塞化	○：未知の脆弱性の被害低減
クライアント PC	● OS のセキュリティ修正プログラム適用 ● クライアントソフトウェア（PDF，ZIP 等）のセキュリティアップデート ● セキュリティ設定による機能制限	○：既知の脆弱性 ×：未知の脆弱性
	● アンチウイルスソフトウェア	○：既知のウイルス ×：未知のウイルス
人	● セキュリティ教育	○：情報セキュリティリテラシーの向上 △：全員には行き届かない
	● インシデントレスポンス体制の確立	○：事故発生時の被害最小化 △：全員には行き届かない
	● セキュリティ事故を想定した訓練	○:体験型学習による免疫効果やエスカレーション体制が機能するか確認 △：全員には行き届かない

そこで，無防備に近い対象者を標的型攻撃メールから防衛するには，「予防接種」としてあらかじめ擬似的に攻撃を体験し，個人もしくは組織に「抗体」を生成するのが肝要である[17]．潜在的対象者が，添付ファイルをむやみに開かいないことや，OS やアプリケーションのアップデートを怠らないなどを習慣とすれば，脅威も自ずと減少すると考えられ，ユーザの意識向上が最も効果的であるとされる[18]．ただし，抗体の効果は長続きしないとも考えられ，定期的に予防接種を行い続ける必要がある．

3. 模擬攻撃の予備実験

本学職員への模擬標的型攻撃メールの送信を控え，著者の受け持つ学生への標的型攻撃メールの予備実験を行った例を報告する．単発のみの配信であるため，予防接種としての効果は算定できないが，一斉送信における解析方法および問題点を確認するために実施した．

3.1. 本学学生に対する標的型攻撃メールの予備実験の実施

一般教養科目および共通科目を履修している学生 196 名（文系学部・18～25 歳）に対して，標的型攻撃メールを模したメールを，大学が提供した学生メールアドレス宛てに一斉送信し，開封状況等を観察した．なお，講義中には，昨今のセキュリティ事情として標的型攻撃メールについて触れており，送信元ドメイン等の確認は怠らないよう注意をしてある．

メールの配信は，学外ドメインを持つホスティングサーバの SMTP とメール配信ソフトである Mail Distributer [19] を利用して一斉送信した．送信元のドメインは普段教員から送られるものとは異なるようにした．危険なメールを判別するためのヒントとするためである．

メールの文面は図 1 のように記載し，期末テストに関連する内容とした．文面冒頭には，メール配信ソフトの文字列差し込み機能を利用して，学生（攻撃対象者）の所属と氏名を入れた．テスト期間に近い時期だったため，学生にとっては極めて関心の高い内容である．添付ファイルを解凍すると，期末テストに関する情報が得られるとの指示を記載している．

添付ファイルは，Windows 実行ファイルをリネームして添付した．実行ファイルは，実行したことを記録するため既定のブラウザを起動して，プリセットされた URL の Web サーバにアクセスする．記録内容は，通常の Web アクセスログおよび実行時に利用している PC 名やログインユーザ名等とした．ここで，添付した実行ファイルをリネームした理由としては，本学学生が利用している Gmail が *.EXE を受け付けないための措置である．

実行ファイルを起動すると，図 2 のようにブラウザ画面が表示される．教育的効果を狙って，一見恐怖心を煽る画像を挿入している．文面としては，「送信元のドメインを確認せず，うかつに添付ファイルを開いてはいけません」という趣旨である．

メールの配信時間は平日午後 7 時とし，その後 24 時間を添付ファイル開封調査時間帯とした．

法学部　吉田さん

情報社会論を担当している伊藤です。
期末テストに関する重要なお知らせがあります。
添付ファイルを参照してください。

なお、添付ファイルは自己解凍ファイルとなっております。
解凍するにはファイル名を一部変更する必要があります。
デスクトップ等にダウンロードした後に以下のようにしてください。

（変更前）　期末試験のお知らせ.exe.bak
（変更後）　期末試験のお知らせ.exe

ファイル名を変更したら、ダブルクリックして実行してください。
※ Windows PCでのみ利用できます

一橋大学　伊藤史人
ito@cio.hit-u.ac.jp

図 1　模擬標的型攻撃メールの文面

図 2　模擬標的型攻撃メールの起動時に表示される Web 画面

3.2. 予備実験の結果と考察

予備実験の結果，開封者は196名中93名であり，開封率47%となった．当初80%を超えるものと想定していたが大きく下回ることとなった．

しかし，後日の聞き取り調査の結果，未開封者の中には，そもそも大学が提供しているメールを利用していない者がいることが判明した．また，開封調査時間帯の24時間では，アルバイト等でメールを確認できなかったケースがあったことも分かった．学生の生活リズムは，各人で時間的に大きな振れ幅があるため，それらを考慮した集計が必要だったと思われる．

ただし，開封調査時間帯を多く取ると二重開封をカウントしてしまう可能性が高まる．そのため，職員に対する予防接種においては，二重カウントを技術的に防ぐ仕組みが必要であることが分かった．さらに，実行ファイルをリネームできなかった学生もおり，潜在的な開封者も確認できたため，より簡単に開封者をカウントできる仕組みも必要であった．

なお，被験者の学生の感想としては，おおむね次のようなものであった．多数の同様の意見があったもののみ列挙する．

- 授業では標的型攻撃メールのことは聞いていたが，まさか自分に来るとは思わなかった．
- 焦って開いてしまった．
- 送信元ドメインなど気に留めなかった．
- 実際に攻撃を受けてみて，防衛がたいへん難しいことが分かった．

特に，最後に記載した感想は，標的型攻撃メールの予防接種を実施する前提として極めて有用だと考えられる．

以上の予備実験による反省点を踏まえ，職員に対する予防接種を実施した．

4. 標的型攻撃メールの予防接種

本学職員に対する標的型攻撃メールの予防接種は，株式会社ラック [20] の協力を仰ぎ，予備実験で得られた反省点を改善した上で実施した．また，事前に学内上位組織による承認を得た．

4.1. 予防接種の実施概要

予防接種の実施概要を表 2 に示す．定時出勤前の8:00を目途に，事前に決定したメールアカウントへ予防接種となる添付ファイル付きメールを配信する．その後，同日夕方には開封者データの集計を打ち切る．同じフローで1週間の時間を置いて実施する．2回行う理由としては，初回からの予防接種効果を確認するためである．

なお，対象は200名であるが，一部は共用アドレス化しているため，同一メールを複数人が閲覧する可能性がある．後述するWebビーコンの仕様により開封者数を二重カウントすることはない．しかし，共用する誰かが開封するとカウントされてしまう．

予防接種後は，全職員向けにセキュリティ講習を実施し標的型攻撃メールについてはもちろんのこと，近年のセキュリティ事故などについての知識を新たにしてもらうこととした．

表 2　予防接種の概要

項目	内容
対象	本学事務系職員200名（常勤・契約職員・パート職員） ただし，メールアカウントは複数職員で共用している場合がある．
目的	擬似的な標的型メール攻撃を実施して組織としての開封率などの指標を調べる．また，これを体験することで各個人に耐性をつけ，その結果として組織の耐性を向上させる
方法	添付ファイルには，マルウェアの代わりにWord 文書に Web ビーコンを仕込んだ擬似攻撃メールを配信し，Web ビーコンのログから添付ファイルの開封状況を計測する．
分析	Web ビーコンから得られた基礎データから以下の解析結果を得る． 開封者数／開封日時／開封率／非開封率／時系列の開封状況／対象者の属性 等
実施日時	・第1回メール配信 2012年3月7日 8:00 模擬訓練であることを通知 同日 19:16 ・第2回メール配信 2012年3月15日 8:00 模擬訓練であることを通知 同日 16:18

4.2. 模擬攻撃メールの文面

メールの文面は，対象者に攻撃であることを感じさせないことが重要である．今回は，表 3 および 表 4 に示すように，社会情勢や情報セキュリティ事情に合わせた内容とした．

送信元のドメインは，本学職員にとっては初見であり，これまでの情報セキュリティ講習の経験のある者であれば当然注意するはずの情報である．メールクライアントは職員で統一したものを利用しており，送信元ドメインの確認は容易なインターフェースとなっている．

標的型攻撃メールを判別するには，以下について意識しておく必要がある．

- 差出人の名前やアドレスが，見慣れないものである．
- 組織内の話題なのに，外部のメールアドレスから届いている．
- 添付ファイルを開くよう不自然に誘導している．
- 急がせて，メールの内容を吟味させまいとしている．
- 差出人の署名や名乗りが無いか曖昧である．
- 架空の差出人の名前や組織名を名乗っている．

表 3　第 1 回メール配信の文面

Subject	事業継続計画の定期見直し
From	危機管理・災害対策本部 <drc@jigyokeizoku. jp>
Message	一斉メール：危機管理・災害対策本部です． 2011 年 3 月 11 日に発生した東北地方太平洋沖地震では，計画停電や公共交通機関の大幅な乱れにより出勤が困難な状況となりました． つきましては，災害発生時の緊急対応方法について事業継続計画の見直しを行うこととしましたので，添付ファイルの指示に従って現状の調査にご協力をお願いします． 現状調査の項目には，各自の通勤経路(災害時の帰宅経路含む) の項目もありますので，全員の回答が必要です． よろしくお願いします． 一斉メール：危機管理・災害対策本部
Attach	事業継続計画現状確認シート 3. doc

表 4　第 2 回メール配信の文面

Subject	至急： PDF に関する注意喚起
From	情報化推進本部 <security@joshisu. jp>
Message	各位 最近，PDF ファイルを送りつけることで，ソフトの未発見のセキュリティホールを突いて侵入を試みる事例が激増しています． 多くの場合は適切な設定をしておくことで危険を回避できるものですので，添付の確認手順にしたがってお手元の PC の設定を至急点検し，より安全な設定にしていただきますようにお願いします． 情報化推進本部
Attach	点検手順. doc

4.3. Web ビーコンによるロガー

予備実験では，実行ファイルにより開封者データをロガーしたが，予防接種においては Web ビーコン [21] を Word ファイルに埋め込んだ．さらに，各添付ファイルには特定の ID を仕込むことで個人の特定を確実にした．Web ビーコンを仕込むことで Word ファイルの挙動が変わることはなく，職員（対象者）にとっては通常の文書を読むのと何ら変わることはない．

ところで，職員が利用する PC にはセキュリティ対策ソフトが導入されており，通信の常時監視により不正なトラフィックはブロックする仕様である．Web ビーコンの通信もブロック対象になる可能性もあったが，本学の使っているセキュリティ対策ソフトでは反応しなかった．

参考として図 3 に Web ビーコンを仕込んだ Word ファイルを DUMP したキャプチャを示す. 四角で囲った部分から分かるように，ファイルを開くと特定の URL にアクセスするようになっている．

図 3　Web ビーコンを含んだ Word ファイル

4.4. 訓練であることの周知

予防接種は業務中に実施するため，それによって業務を混乱させてはならない．すみやかに模擬訓練であることを知らせるために，添付ファイルには 図 4 のように「標的型偽装メールの実施ついて」として，模擬訓練であることを学内承認済みであることと共に明記した．この通知を行わないと，情報担当部署に大量の問い合わせが寄せられたり，苦情や思わぬトラブルが発生する可能性がある．

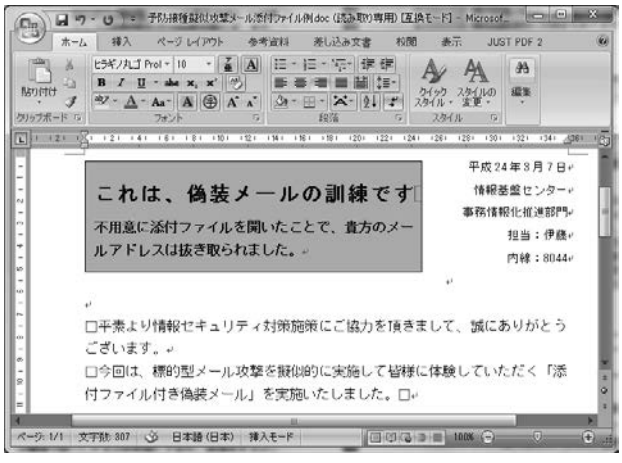


図 4　訓練であったことを明示

5. 結果と考察

予防接種当日，大きな混乱は無かったものの，職員の中には不審メールに気づき，開封の可否を情報担当部署

に問い合わせるケースが 5 件ほどあった．また，部署によっては先に開封してしまった者が他者に開封を留まらせるなどのケースもあった．

5.1. 時系列の開封率

図 5 に時系列の開封状況を示す. 本学の開封状況を比較するため，他組織平均のデータを[22]より引用した．他組織については，表 5 における他組織 A ～ E であり，いずれも同様の標的型攻撃メール予防接種を実施した日本国内の一般企業である．

図中において，本学の開封率は ◆ で示し，他組織平均は ○ で示している．開封者数比（縦軸）は，擬似攻撃メール配信時刻から 10 分刻みでその 10 分間の内に開封した被験者が全開封者に占める比率を示している．経過時間（横軸）は，擬似攻撃メール配信時刻から 1 時間刻みでの経過時間を示している．

他組織平均では全開封者のうちの半数が開封するまでに，擬似攻撃メール配信後およそ 30 分間しかかかっていないことがわかる. 今回の配信は 8:00 に行っており，平均累積開封者数比の傾向より緩やかな経過をたどるものの，1 時間経過した時点で今回の開封者のうちの 6 割程度がすでに開封している．一般的にも，メールを受信した直後に多くの開封者が開封しているという傾向があり，標的型メール攻撃への対策として人間が介在して情報集約するような仕組みでは間に合わない可能性が高いと考えられる．

やはり，スパム対策などの入口対策・ OS やソフトウェアのアップデートなどのデスクトップでの対策・DLP（Data Leak Prevention：情報漏えい防止策） などの出口対策を組み合わせて実施する必要があるといえる．

5.2. 各開封パターンによる開封率

開封率は各開封パターンで集計した. 各パターンとは，第 1 回および第 2 回の開封者，両方の回の開封者，第 1 回もしくは第 2 回のみの開封者，非開封者である．表 5 では全被験者を対象にこれら各パターンの開封率を他組織平均の情報と併せて示している．

表 6 は, 予防接種実施後に行ったアンケート（表 7 および 表 8 参照）の回答者のみを対象に集計した結果である．なお, アンケート回答者数は 200 名中 29 名であった．

今回の予防接種では 1 回目は 40.0%，2 回目は 28.5% の開封率であり，他組織平均と比較して高い傾向にあった．特に，1 回目 2 回目とも開封した被験者の割合が全体の 2 割近くであり，他組織平均と比較して高い値であるといえる．

今回の予防接種は初めてだったため，標的型攻撃メールへの耐性が低い被験者が多い可能性があり，継続した注意喚起や教育訓練の実施など対人間向けの教育を充実させることで組織の意識レベルのさらなる向上を図る必要がある．

また，攻撃が実際に行われた場合，それが届いたことを規程に従って報告させ，それを集約して警告を出すような対応策では時間的に間に合わない．

さらに，対象者からのアンケートでも業務関係のメールは違和感を覚えても開封する傾向が判明しており，被害を最小限にとどめるためには人的対策と組み合わせてスパム対策などの入口対策といった多層防御の考え方による防御態勢を整えることが求められる．

5.3. 被験者属性と開封率

表 7 に本学の被験者アンケート結果について, その選択肢毎に各回配信の開封者数・非開封者数を集計した結果を示す．どのグループの開封率が高いといった，有意な差や傾向は認められなかった．

他組織では，メール習熟度・平日 1 日当たりのメール数・1 時間当たりの処理メール通数・予防接種経験の有無・業務関連度 等で強い相関関係を示した例もある．しかしながら，本学ではこれらの属性については強い相関は認められなかった．

年齢層についてはやや有意な結果が出ており，全年齢層の中で 30 代の開封率が低いことが分かる. この年代は IT と業務に熟練した人材が多く，セキュリティに関する知識も十分であった可能性がある．20 代については，勤続期間の短いパートタイム職員が含まれるため，IT や業務に関して未熟である場合が考えられる．高齢の職員については，情報セキュリティについて知識はもとより，IT 全般に関するリテラシーの意識に乏しい可能性が極めて高い[23].

5.4. 被験者の感想

表 9 にアンケートの回答から得られた被験者の感想の一部を挙げる．職員に対しては，標的型攻撃メールの危険性について，日常的にポスターや講習等で周知していた．そのため，その存在自体は知っていたものの，実際の攻撃には無力であったとの感想が散見された．

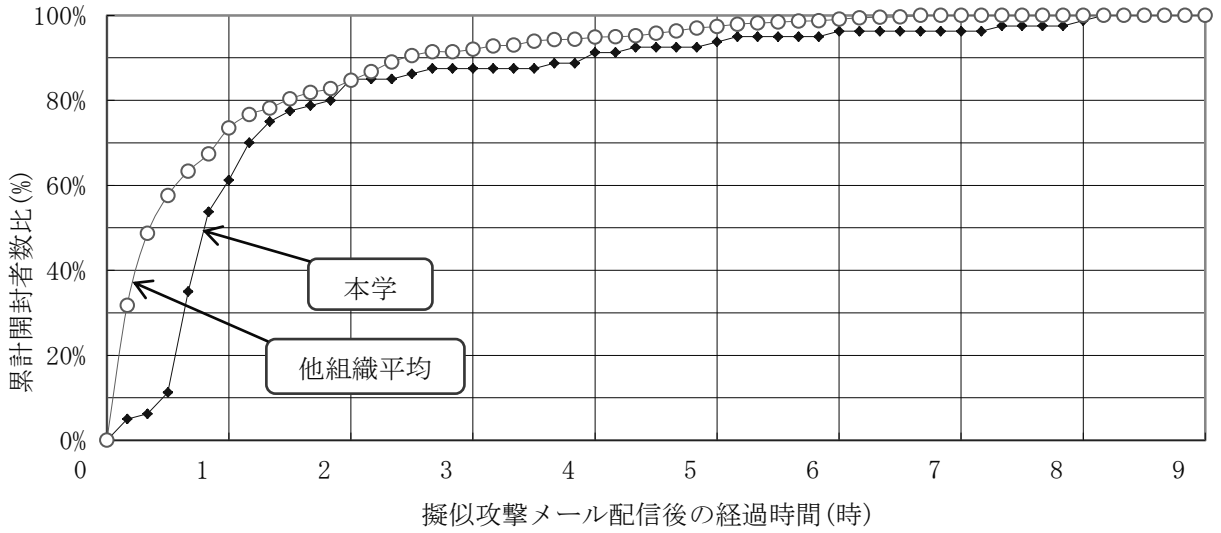


図 5　時系列開封状況

表 5　各開封パターンによる開封率（全被験者）

	被験者数	第 1 回 開封者	第 2 回 開封者	両回 開封者	第 1 回のみ 開封者	第 2 回のみ 開封者	非開封者	開封 減少率
本　学	200	80 40.0%	57 28.5%	34 17.0%	46 23.0%	23 11.5%	97 48.5%)	28.8%
他組織 A	2,927	623 21.3%	253 8.6%	80 2.7%	543 18.6%	173 5.9%	2,131 72.8%)	59.4%
他組織 B	500	102 20.4%	21 4.2%	8 1.6%	94 18.8%	13 2.6%	385 77.0%	79.4%
他組織 C	438	125 28.5%	19 4.3%	10 2.3%	115 26.3%	9 2.1%	304 69.4%	84.8%
他組織 D	200	66 33.0%	55 27.5%	22 11.0%	44 22.0%	33 16.5%	101 50.5%	16.7%
他組織 E	110	52 47.3%	25 22.7%	9 8.2%	43 39.1%	16 14.5%	42 38.2%	51.9%

表 6　各開封パターンによる開封率（アンケート回答者）

	アンケート 回答者数	第 1 回 開封者	第 2 回 開封者	両回 開封者	第 1 回のみ 開封者	第 2 回のみ 開封者	非開封者	開封 減少率
本　学	29	14 48.3%	11 37.9%	6 20.7%	8 27.6%	5 17.2%	10 34.5%	21.4%
他組織 A	1006	240 23.9%	86 8.5%	45 4.5%	195 19.4%	41 4.1%	725 72.1%	64.2%
他組織 B	182	40 22.0%	4 2.2%	2 1.1%	38 20.9%	2 1.1%	140 76.9%	90.0%
他組織 C	47	15 31.9%	4 8.5%	2 4.3%	13 27.7%	2 4.3%	30 63.8%	73.3%
他組織 D	32	11 34.4%	8 25.0%	6 18.8%	5 15.6%	2 6.3%	19 59.4%	27.3%
他組織 E	37	20 54.1%	5 13.5%	1 2.7%	19 51.4%	4 10.8%	13 35.1%	75.0%

表 7　被験者（職員）属性と開封率

設問[*1]	選択肢	第 1 回配信			第 2 回配信		
		開封	非開封	開封率	開封	非開封	開封率
性別 #1	男性	8	10	44%	8	10	44%
	女性	6	4	60%	3	7	30%
年齢層 #2	20 歳未満	0	0	0%	0	0	0%
	20 歳代	4	2	67%	4	2	67%
	30 歳代	2	6	25%	1	7	13%
	40 歳代	4	4	50%	4	4	50%
	50 歳代	3	2	60%	2	3	40%
	60 歳以上	1	0	100%	0	1	0%
職務 #3	役員	0	0	0%	0	0	0%
	管理職	2	1	67%	1	2	33%
	サービス・ CS	0	0	0%	0	0	0%
	事務職	11	12	48%	9	14	39%
	その他技術者	1	1	50%	1	1	50%
メール処理の習熟度 #4	非常に熟練	0	0	0%	0	0	0%
	熟練している方	1	1	50%	0	2	0%
	平均的	11	12	48%	9	14	39%
	あまり熟練していない	2	1	67%	2	1	67%
	ほとんどできない	0	0	0%	0	0	0%
メール数 #5	25 通/ 日未満	10	9	53%	8	11	42%
	25 以上 100 未満	4	4	50%	3	5	38%
	100 以上 250 未満	0	1	0%	0	1	0%
	250 以上	0	0	0%	0	0	0%
メールの処理時間 #6-1	2 時間/ 日未満	9	4	69%	7	6	54%
	2 以上 4 未満	3	9	25%	3	9	25%
	4 以上	2	1	67%	1	2	33%
1 時間当たりのメール処理数 #6-2	25 通/時未満	12	12	50%	9	15	38%
	25 以上 100 未満	2	2	50%	2	2	50%
	100 以上 250 未満	0	0	0%	0	0	0%
	250 以上	0	0	0%	0	0	0%
予防接種経験 #7	経験済	0	2	0%	0	2	0%
	未経験	14	12	54%	11	15	42%
業務関連度 #9	非常に強い関連	2	2	50%	3	2	60%
	どちらかと言えば関連	7	8	47%	5	8	38%
	わずかに関連	5	3	63%	3	6	33%
	無関係	0	1	0%	0	1	0%

*1 各設問の #(数字) は 表 8 の設問 No. に相当する

表 8　被験者アンケートの設問例

No.	感　想
1	あなたの性別を選択してください.
2	あなたの年齢層を教えてください.
3	あなたの職務は以下のどれに最も近いですか？
4	業務上の連絡を電子メールで送受する場合を想定すると，あなたは電子メールの取り扱いにどの程度熟練していますか？
5	あなたは業務上のメールを送受信合わせて何通程度取り扱いますか？
6	あなたは業務上のメールをどの程度の時間をかけて処理していますか？
7	あなたは過去に IT セキュリティ予防接種を経験しましたか？
8	あなたは今年度の第 1 回配信の擬似攻撃メールにどのように対応しましたか？
9	第 1 回配信の擬似攻撃メールの本文や表題は，あなたの担当業務とどの程度関連していましたか？
10	あなたは今年度の第２回配信の擬似攻撃メールにどのように対応しましたか？
11	第２回配信の擬似攻撃メールの本文や表題は，あなたの担当業務とどの程度関連していましたか？
12	予防接種について，ご感想・ご意見などを自由にご記述ください.

表 9　被験者の感想

No.	感　想[*1]
1	添付ファイル以外にも偽装リンク先等を掲載し，部署ごとに違うリンク先が掲載されたメールを送り何回，アクセスがあったか集計するとより，客観的なデータが取れて良いのではないか．個人情報等を流失しないためにも定期的に IT セキュリティ予防接種があると職員の意識も高まり良いのではと感じました.
2	ドッキリみたいで面白かったです．二回目は予防接種だと気づきましたが，ついつい添付ファイルの内容を見てしまいました.
3	擬似攻撃メール配信から数時間後に，システム管理者から訓練を実施した旨がメールで報告されたが，当該メール・添付ファイルにも不審な要素があり，電話による確認作業を要するなど，混乱が続いた.
4	メールアドレスまで慎重に見るようになったので良かったと思う.
5	特にまだ入ったばかりで，上記の部分について把握しておりませんので今後，見解を深めていければと存じます.
6	今回の訓練の経験を踏まえ，少しは送信相手を確認するようになった.
7	送付されてきたメールアドレスをもう少し注意していれば，ひょっとしたら回避できていたかもしれません．2 回目は，その教訓が生きていたと思います．自分は，絶対大丈夫だと思っていましたから，少しショックでした．もう少し，メールそのものを疑って，注意深く確認するべきであると思い知らされました．どうもありがとうございました.
8	送信者を学外者の知られていない人物の名前にして試してみてはいかが？
9	1 回目の偽装メールの添付を開いて，失敗した！と思ったのですが，2 回目も同様にひっかかってしまいました．今後はメールを開くときに，注意深くしなければいけないと思いました.
10	メールに対する意識が変わりました．時々，訓練し意識しながらメールを使うようになる良い機会と思います.
11	不正メールへの対応について，各人の意識向上がはかれるので，重要なイベントだと思います．ですが，騙すことが目的ではないので，メールの内容が本務に限りなく近いと，狼少年のたとえのような状況となる場合もあるので，注意が必要とは思います.
12	擬似攻撃メールの訓練とのことだったので送信者名を確認してから添付も開いたが，通常は開かないと思われる．しかし，送信者名を騙られた場合はアウトだったと思うので反省すると当時に，その場合の見分け方等，予防策を教えてほしいと感じた.

*1 各感想は 表 8 の設問 No. 8, 10, 12 から採取した

6. おわりに

今後，大学においても標的型攻撃メールを懸念する事態になりかねない．大量の学生に関する個人情報を擁しているため情報漏えいのリスクは計り知れない．また，悪意のある者が自己の成績証明を書き換えることさえも考えられる．いずれのセキュリティインシデントも大学が長い時間を掛けて築き上げてきたブランドを貶める極めて深刻な事態である．われわれは，そのような事態を防がなければならい．

しかしながら，標的型攻撃メールは統一的に防衛することは不可能である．また，唯一の対策である予防接種の効果は，時間が経るにつれ限定的な効果しか発揮しない．大学組織は職員の出入りも少なくないため，年に複数回の実施は不可避であろう．

標的型攻撃メールは，情報部門と現場の職員との協働無くして防ぐことはできない．今後，すべて教職員に対して，情報セキュリティ全般の意識向上対策を行いつつ，絶対に漏えいしてはならない情報は LAN 経由でアクセスできないなどの対策を取る必要もある．さらには，学生に対する情報セキュリティ教育も必要であると考える．

参考文献

[1] 寺田真敏, “標的型メールがやってきた”, 情報処理, 51(3), pp.270-274, 2010

[2] 三森春佳, 阿部公輝, “ふるまいに着目した未知の亜種ウイルスの識別”, 電子情報通信学会技術研究報告（情報セキュリティ）,108(162), pp.1-7, 2008

[3] 高木浩光, “ソフトウェアのセキュリティ欠陥は誰が直すのか”, http://www.ipa.go.jp/security/fy14/events/ipa-winter2003-takagi-dist.pdf, 独立行政法人産業技術総合研究所, 2003

[4] IPA セキュリティセンター, “コンピュータウイルスの届出状況”, http://www.ipa.go.jp/security/txt/list.html, 独立行政法人情報処理推進機構, 2012

[5] 大谷尚道, “個人情報漏えいインシデントを減らすためには”, NTT データ, NTT セキュリティ被害調査 WG, Vol27, 2008

[6] 関根冬輝, 村井純, “メールヘッダ解析によるなりすましメールの検知手法の提案”, 慶応大学環境情報学部卒業論文, 2012

[7] 碓井利宣, 村井純, “コードの特徴に基づく悪性プログラムの分類”, 慶応大学環境情報学部卒業論文, 2012

[8] Georgios Sakkis, et at al., “Stacking classifiers for anti-spam filtering of e-mail”, Proceedings of the 6thConference on Empirical Methods in Natural Language Processing(EMNLP 2001), pp.40-50, 2001.

[9] Jose M.Gomez Hidalgo, “Combining Text and Heuristics for Cost-Sensitive Spam Filtering”, Proceedings of CoNLL-2000, pp.99-102, 2000

[10] 相馬基邦, “標的型攻撃への対処法 バックドア通信を遮断しウイルスの活動抑え込む”, 日経 systems (224), 40-45, 2011

[11] 山口健太郎, 小宮山功一朗, 内田勝也, “ユーザへの予防接種というアプローチによる標的型攻撃対策-2”, 情報処理学会第 71 回論文集, pp.349-350, 2009

[12] 猪俣敦夫, ラーマン・ミザヌール, 岡本健, 岡本栄司, “フィッシングメール防御のためのメールフィルタリング手法の提案”, SCIS2005, 2005

[13] 独立行政法人情報処理推進機構, “IPA テクニカルウォッチ　標的型攻撃メールの分析に関するレポート～だましのテクニック事例 4 件の紹介と標的型攻撃メールの分析・対策～”, 2011

[14] 八津川直伸, 石野貴子, “重大な脅威に対するセキュリティ設計手法の考察”, UNISYS TECHNOLOGY REVIEW 第 98 号, 2008

[15] 車古正樹, 松平拓也, 井町智彦, 中野三智子, 西川直樹, “Spam フイルタに関する統計”, 学術情報処理研究, No9, 2005

[16] 松平拓也, 車古正樹, 井町智彦, 西川直樹, “Spam メール及びウイルスメール対策システムの構築と運用”, 学術情報処理研究, No9, 2005

[17] 金野千里, “増大する脅威とそれに向けた取り組み”, 独立行政法人情報処理推進機構, IPA フォーラム 2011, 2011

[18] 田村佑輔, 甲斐俊文, 佐々木良一, “ユーザ標的型 Web サイト改ざんに対する検索エンジンを用いた検知手法の提案”, 情報処理学会論文誌, 51(1), 191-198, 2010

[19] Mail Distributor ver.6.4, http://www.woodensoldier.info/soft/md.htm

[20] 株式会社ラック, http://www.lac.co.jp/

[21] Web ビーコン, http://d.hatena.ne.jp/Kango/20111024/1319462526

[22] 株式会社ラック, “IT セキュリティ予防接種結果報告書（一橋大学）”, 株式会社ラック, 2012

[23] 宮本貴朗, “大学におけるセキュリティ対策”, 総合情報センター年報情報. 2002, 8, pp.4-11

大学1年生の情報活用能力とICT機器やメディアの利用状況調査

A Questionnaire Study of ICT Ability and Media Literacy of 2012 Freshmen

辰己 丈夫 ∗, 江木 啓訓 ∗, 瀬川 大勝 ∗

TATSUMI Takeo∗, EGI Hironori∗, SEGAWA Hirokatsu∗

tttt@cc.tuat.ac.jp, egichan@cc.tuat.ac.jp, hiroka@cc.tuat.ac.jp

東京農工大学総合情報メディアセンター ∗
Information Media Center, Tokyo University of Agriculture and Technology∗

概要

東京農工大学（以下、本学と記す）では、今年、ほぼすべての 1 年生を対象として、情報活用能力の身に付け方やその程度、および、日常の ICT 機器やメディアについてアンケート調査を行なった。その結果、高校の情報科の履修の実態は指導要領から離れている部分があり、大学生に必要と思われる情報活用能力とも異なることがわかった。特に、自分が持つ ICT 機器の設定や、メディアリテラシー、統計に関する能力に不足があることがわかった。今後、情報系センターがこのような方法で調査を行なう場合には、本アンケートのような項目を含むことで、今後の整備の資料にすることが望ましい。

Abstract

Information Media center of Tokyo University of Agriculture and Technology take place ”university information seminars for freshmen” in every April(the first month of fiscal year). In the seminar of this year, using a questionnaire to all freshmen, the authors evaluated the way of learning in their high school age, the degree of acquisition of the skills of ICT devices and the level of media literacy.

As a result, it was found that their ability did not cover the goals of the educational subject ”Information Studies” of Japanese National Curriculum guideline for high school. Their ability, also, was insufficient to the ability of utilization of ICT devices which is needed in university student daily life. They had a lack of the ability of setting up own PC, and they did not know the term of ”media literacy” and they did not learn the statistics.

キーワード

情報リテラシー、高校情報科、アンケート調査

Keywords

Information literacy, “Information Studies” in Japanese high schools, A Questionnaire Study

1 はじめに

1.1 情報環境の変化

インターネットを始めとする情報環境は新しい技術・インフラの発達により、日進月歩の勢いで変化を続けている。同様に、学校における情報環境も変化を続けている。近年は、一部の大学では端末室から PC を撤去してネットワークと電源のみを提供し、学生の PC 必携化を行なったり、いくつかの大学ではシンクライアント・ディスクレスクライアントを利用した PC 教室整備 [1]

や、メールシステムなどを中心にクラウドの利用 [2] も進んでいる。キャンパス内の情報環境についても、現在は、一般ユーザ（学生）向けには、無線 LAN 環境も整備されるようになった。

一方で、次節で述べるように、高校の学習指導要領では必履修教科「情報」の設置が行なわた。その結果、現在の我が国の大学に入学する学生のほとんどは、高校生のときに「情報科」を学んでいることになっている。

1.2 高校情報科の状況と実情

高校で 2003 年から実施された学習指導要領 [3, 4] では「情報」が必履修教科となり、

- 情報活用の実践力
- 情報の科学的な理解
- 情報社会へ参画する態度

の 3 つを学ぶこととなっている。2006 年以降は、これらの教科・科目（主に普通教科「情報」の科目「情報 A」）を履修した学生が大学に入学している。

だが、以下に見るように、現実に実施されている高校情報科の授業や一般情報教育の多くは、オフィスソフトの利用方法が中心のものが多い。

- 2006 年の大学 1 年生を対象とした望月ら [5] の調査や、CEC(一般財団法人 コンピュータ教育推進センター) が 2008 年度に高校教員に実施した調査 [6] では、現実の高校情報科の教育内容には偏りがみられていることが明らかとなった。具体的には、オフィスソフトの使用方法や、情報倫理（情報モラル）の学習に重点が置かれていた。
- 2006 年の大学 1 年生を対象とした青木ら [7] の調査では、情報科を履修して大学に入学した者の「情報に関する基礎学力」が、そうでない者よりも有意に差があることがわかった。
- 澤田 [8] は、高校の現場の状況と、大学の情報科の教員が持つ期待度の差が、大学の情報教育に与えた影響の問題点を指摘した。
- 辰己らが 2011 年に行なったインタビュー調査 [9] でも、大学 1 年生の学生が学んできたはずの高校「情報」は、履修状況に不足（未履修状態）があり、また、内容には「情報倫理」関連項目が多いのに対して、プログラミング関連はほとんど学ばれていないなどの偏りがみられた。
- 2011 年に実施された東京農工大学生協の調査 [10] では、大学生協パソコン講習会に参加した大学生の「自分のパソコンを使用する情報活用能力」は、講習受講前ではほとんど達成できてないことが示された。

1.3 大学の一般情報教育の状況

現在は、多くの大学で大学 1 年生の一般教育・教養教育として行なわれる情報教育（本稿ではこれを「一般情報教育」と呼ぶ）を実施しており、大学生に必要な情報活用能力を育成するために一般情報教育が行なわれており、次の状況が見られる。

- 大学全体で内容を統一して必修としている大学 [11, 12] もあれば、全学共通のセンターが実施している大学 [13] もあり、本学のように全学科が独自で実施する体制を構築している例もある。
- 情報倫理や情報セキュリティに関する能力については、例えば国立大学情報教育センター協議会タスクフォースで作成された「情報倫理ビデオ小品集」[14] などを利用して、「PC 教室や大学のネットワークの利用スキル」や「個人としての情報機器やサイト利用方法」を学ぶことができる。なお、このビデオ教材の対象となったすべての分野で、理解度の有意な向上が確認されている [15]。
- 「レポート作成能力」に必要な教育内容の多くはオフィスソフトの使用方法として教えられていることが多い。統計的な部分にも重点を置いている例 [16] もあるが、一部に留まっている。一方、情報科学や情報技術の基本となる理論や仕組み、情報社会の構成、情報倫理などの「情報学」を学ぶ例もある [17]。特に、情報フルーエンシー [18] などで提案されているように、学校卒業後、激しく変化をしていく情報技術に自学自習で追い付き、対応するために、在学時に情報科学を学ぶことが求められている。
- パソコンの設定などの「自分の機器」の設定は、大学生協などの活動に委ねられている例が多く見られる [19] [1]。

1.4 現在の大学生に求められる情報活用能力

一方で、現在、大学生が大学の PC 教室を利用する際には、さまざま能力が求められ、学習も必要となっている。

(1) レポート作成などにおいては、統計的データ処理や文献検索・文献データ管理などのさまざまな能力が必要とされる [16]。
(2) 適切な利用権限の設定や、適正な利用のために、アカウントやパスワードの管理、大学における著作権や個人情報の取り扱いなどを知る必要がある [20]。

[1] “無料セットアップ講習会” という言葉で Web 検索を行なうと、例えば、三重大学生協の「生協オリジナルパソコン＆講習会」(http://www.mucoop.jp/fresh/pc/pc.html) のように、多くの大学生協がパソコンセットアップ講習会を行なっていることがわかる。

(3) 大学のような不特定多数の利用者がネットワークに接続をする状況では、OS やアンチウイルスの設定・更新、セキュリティの観点から利用にさまざまな制約が課せられている。例えば、本学では OS とアンチウイルスの更新義務化、プロキシの設定などが、ネットワークを利用する際の必要な技能として位置付けられ、ソフトウェアのインストールとソフトウェアライセンス、その他の著作物の著作権や P2P についても知る必要がある [21]。
(4) 大学生個人としての生活においては、さまざまなサイトの閲覧や、デジタルカメラなどの機器操作、メディアリテラシーなどが求められている [22]。

1.5 2006 年〜2011 年の調査等からわかる問題点

本論では、これまでに 1.2 においては高校情報科の状況と実情、1.3 においては大学の一般情報教育の状況、そして、1.4 においては現在の大学生に求められる情報活用能力の内容について述べてきた。これらをまとめると、次の表 1 を作ることができる。

表- 1: 2006 年〜2011 年の調査等からわかる状況

項目	高校指導要領	高校の授業の実際	大学の授業の実際	大学生に必要
オフィスソフトの使用方法	×	◎	○	◎
PC 管理スキル	×	×	×	○
ネット接続	×	×	×	◎
情報科学	△	×	△	○
情報技術	△	△	△	○
情報倫理	○	◎	△	◎
情報セキュリティ	○	△	△	◎
文献処理	×	×	△	○
統計処理	×	×	×	○
メディアリテラシー	×	×	×	◎

この表からも、高校の情報科と大学の一般情報教育のそれぞれについて、指導要領、および、授業実施状況、獲得状況の実態などに問題やバラツキなどがあることがわかる。

だが、この表にまとめられた状況は、2006 年から 2011 年度の 6 年間の間に、いくつかの大学で調査されてきたことがらが中心であり、内容としてはやや古く、また、同じ母集団での状況などが明確にならない。さらに、1.1 で述べたように、現在の大学生を取り巻く情報環境は急速に変化をしてきている。そこで、2012 年の学生に必要な実際の情報活用能力はどのようなものか、それらはどのように学ばれているか、また、現在の情報環境における情報機器の活用などは、改めて、調査の必要があると思われる。

2 調査の方針と設計

2.1 調査の基本方針

本調査の目標は、各大学の情報系センターに求められる機器整備や教育内容の設計などの調査方法の資料とするために、「現在の大学 1 年生が、どのような情報活用をどこで学び、現在何ができるようになっているのかを調査し、大学生に必要な情報活用能力に含まれつつも十分でない項目を発見すること」である。本論文では、その結果について述べる。[2]

2.2 調査方法

本調査では、Web を利用した調査票調査を採用した。回答に当たっては、個人の成績とは無関係な研究目的であることを説明し、二重回答防止のために学籍番号や参加番号などを入力させるなどの工夫をした。

2.3 調査項目

調査項目を 7 つのカテゴリに分けた。

(1) **高校情報科の履修状況等:** 東京大学で 2006 年から実施している項目に準じた。
(2) **単元・項目毎の状況:** CEC が 2008 年度に高校教員に実施した調査項目 [6] に、高校情報科の学習指導要領に含まれない「統計処理」と「メディアリテラシー」の 2 項目を付け加え、高校情報科で身に付けたかどうか、役立っているかどうかを聞いた。
(3) **大学の情報関係の授業で学習したいこと: (2)** と同じ項目を採用した。
(4) **日常の情報機器の活用状況:** パソコン、携帯電話、スマートホンの保有・活用について質問した。
(5) **日常のネットワーク利用頻度:** メールや著名な Web サイトや SNS などの著名なサイトを列挙して調査項目に入れた。

[2] 他大学も含めた情報活用能力のデータの一部については、辰己が日本情報科教育学会で発表 [23] を行なった。また、大学生協と関連したデータの一部については、辰己が 2012PC カンファレンスで発表 [24] を行なった。

(6) 情報機器・ネットワークの活用: 機器設定ができるかなどについて、「情報フルーエンシー」[18] を参考にした。
(7) 本人属性: 性別。

アンケートの内容については、付録に示した。

3 回答の概要と分析・考察

3.1 調査時期・総数

本調査は、2012 年 4 月に実施した。実施対象は、本学の 1 年生（881 名中 865 名、回収率 98.2%）で、有効回答を行なった人数と性別は表 2 の通りである。

表- 2: 有効回答を行なった人数と性別

項目	人数	%
男	592	68
女	273	32
合計	865	100

3.2 高校情報科の履修状況

3.2.1 時間数と年度、進め方

高校情報科で配当された時間数と年度の回答を、表 3 に示す。

表- 3: 学習に費やした配当時間と年 (%)

項目	%
週 2 時間 1 年間 (*)	25
週 1 時間 2 年間 (*)	17
週 1 時間 1 年間	50
集中、不定期	6
授業がなかった	1
その他（旧課程など）	2

以上のデータからわかるように、一時期話題になった「未履修」はほぼ解消したものの、学習指導要領が定める 2 単位を履修しているのは、(*) の 42%に過ぎない。2 名に 1 名は学習指導要領が定める 2 単位の半分の 1 単位しか履修していない。

次に、授業の進め方の回答を表 4 に示す。62% の学生は、高校時代に副教材や教師が作成したプリントを主に利用した授業を受けている。このことから、内容に洩れがあり、高校情報科の教科目標が達成されていない可能性が考えられる。

表- 4: 情報の授業の進め方 (%)

状況	%
主に教科書を利用	26
主に副教材を利用	29
主に先生自作のプリント	33
「情報」の内容か不明	5
ある時期から他教科になった	2
完全に他教科の内容だった	1
その他（旧課程など、忘れた）	3

3.2.2 単元・項目毎の状況

CEC 調査 [6] で用いられた項目に、「メディアリテラシー」と「統計処理」の 2 項目を付け加えた質問項目について調査を行なった。（質問項目と選択肢は、付録 2. に示した。）情報の授業で学んで身に付けたと回答を多かった順に表 5 に示す。一方、情報の授業で学んでないし身に付けてもいないと回答を多かった順に表 6 に示す。

表- 5: 授業で学んで身に付けた (%)

項目	%
自分の個人情報の取り扱い	58
他人の個人情報の取り扱い	56
著作権	54
メールのマナー・モラル	44
検索サイトの使用方法	36
ワープロ（ワードなど）の操作	36
プレゼンソフト（パワーポイント）の操作	34
メディアリテラシー	30
表計算ソフト（エクセルなど）の操作	28
作文・文章作成（ワープロ操作以外の項目）	27
コンピュータやネットワークの仕組み	25
パソコンを使用したメールの基本操作	16
画像処理とマルチメディア	9
統計処理	6
Web ページ (ホームページ) を HTML で作成	6
データベースの作成	6
コンピュータプログラミング	5
モデル化とシミュレーション	3

「情報で学んだ ÷ 身に付いた」の値を求めたところ、次の通りとなった。

- 特に値が低いもの（身に付けた人のうち、情報で学んだ人が少ないもの）
  - パソコンを使ったメールの操作 (0.53)

表- 6: 授業で学んでないし身に付けてもいない (%)

項目	%
コンピュータプログラミング	52
統計処理	49
データベースの作成	46
Web ページ (ホームページ) を HTML で作成	42
画像処理とマルチメディア	38
モデル化とシミュレーション	34
パソコンを使用したメールの基本操作	25
コンピュータやネットワークの仕組み	24
メールのマナー・モラル	22
作文・文章作成（ワープロ操作以外の項目）	17
プレゼンソフト（パワーポイント）の操作	13
他人の個人情報の取り扱い	13
自分の個人情報の取り扱い	13
メディアリテラシー	11
著作権	9
表計算ソフト（エクセルなど）の操作	9
ワープロ（ワードなど）の操作	8
検索サイトの使用方法	5

表- 7: タッチタイピング (%)

項目	%
「情報」で学んだ。身に付いた	8
「情報」で学んだ。身に付いてない、 他の科目あるいは独学で身につけた。	5
「情報」で学んだ。 現在、身についてない。	18
「情報」で学ばなかった。 他の科目あるいは独学で身につけた。	18
「情報」で学ばなかった。 身につけてもいない。	48
言葉の意味がわからない	2

  - 検索サイトの使用方法 (0.57)

- 特に値が高いもの（情報で学んだ人が多いのに、身に付けた人が少ないもの）
  - モデル化とシミュレーション (2.39)
  - コンピュータプログラミング (2.11)

特徴的な回答があったものとして、「タッチタイピング」を表 7 に示す。情報科で学んだ者のうち、身に付いてない者の方が多い。また、高校で全く学んでおらず、身に付いていない者が約半数であった。

次に「メディアリテラシー」を表 8 に示す。「メディアリテラシー」という言葉は、大学の教員の多くはよく知っている言葉であるが、中学校や高校の学習指導要領には含まれていないため、28% もの 1 年生が言葉の意味がわからないと回答している。

表- 8: メディアリテラシー (%)

項目	%
「情報」で学んだ。身に付いた。	30
「情報」で学んだ。身に付いてない、 他の科目あるいは独学で身につけた。	10
「情報」で学んだ。 現在、身についてない。	13
「情報」で学ばなかった。 他の科目あるいは独学で身につけた。	9
「情報」で学ばなかった。 身につけてもいない。	11
言葉の意味がわからない。	28

表- 9: 統計処理 (%)

項目	%
「情報」で学んだ。身に付いた	6
「情報」で学んだ。身に付いてない、 他の科目あるいは独学で身につけた。	6
「情報」で学んだ。 現在、身についてない。	21
「情報」で学ばなかった。 他の科目あるいは独学で身につけた。	3
「情報」で学ばなかった。 身につけてもいない。	49
言葉の意味がわからない	14

最後に「統計処理」を表 9 に示す。統計処理に関する考察は 3.3 で述べる。

3.3 大学の情報関係の授業で学習したいこと

前節と同じ調査項目を利用して、大学の情報関係の授業で学習したいことを 3 つ回答させた結果を表 10 に示す。

コンピュータプログラミングは、表 6 の「情報の授業で学んでないし身に付けてもいない」でも高い値を示していたことから、高校での授業の量的な拡大や、大学 1 年生を対象とした情報教育における充実が適当であると思われる。

また、統計処理は、ほぼ半数が学んでなく身に付けてないと回答しつつも、15% が大学で学びたいことに挙げている。大学の PC 教室で統計を利用した学習を行な

表- 10: 大学の情報関係の授業で学習したいこと (%)

項目	%
表計算ソフト（エクセルなど）の操作	51
タッチタイピング (キーボードを見ない)	41
プレゼンソフト（パワーポイント）の操作	35
コンピュータプログラミング	35
モデル化とシミュレーション	24
ワープロ（ワードなど）の操作	23
統計処理	15
作文・文章作成（ワープロ操作以外の項目）	15
Web ページ (ホームページ) を HTML で作成	14
画像処理とマルチメディア	12
データベースの作成	12
コンピュータやネットワークの仕組み	6
なし	3
著作権	3
自分の個人情報の取り扱い	3
パソコンを使用したメールの基本操作	3
メディアリテラシー	2
メールのマナー・モラル	1
検索サイトの使用方法	1
他人の個人情報の取り扱い	1

うための環境整備（例えば、統計ツールのインストールを充実させる、など）が必要と思われる。

3.4 大学入学以前の日常の情報機器の活用状況

PC と Mac の入学前の所有状況を表 11 に示す。

表- 11: PC/Mac 入学前所有状況 (%)

項目	PC	Mac
ほぼ毎日利用していた	21	3
よく利用していた	13	2
時々利用していた	13	2
あまり利用していない	5	2
持っていない	48	92

スマートホンと iPad の入学前所有状況を表 12 に示す。

後述の調査（表 14）によればスマートホン所持率が、61% となっていることから、多くの大学 1 年生が、2012 年 3 月に高校を卒業して、2012 年 4 月に大学に入学する間にスマートホンを購入したことがわかる。

表- 12: iPhone/Android/iPad 入学前所有状況 (%)

項目	iPho	Andr	iPad
ほぼ毎日利用していた	9	12	4
よく利用していた	3	2	2
時々利用していた	2	3	2
あまり利用していない	1	1	1
持っていない	85	82	92

3.5 大学入学以前の日常のネットワーク利用頻度

3.5.1 質問の内容と単純集計結果

大学入学以前の日常のネットワーク利用頻度について、6 件法で質問を行なった。(質問項目と選択肢は、付録 2. に示した。)「かなり頻繁に（ほぼ毎日）利用していた」「よく利用していた」の合計を、表 13 に示す。

3.5.2 因子分析の結果

この設問の選択肢の値を元に、バリマックス回転を利用して因子分析を行なった。6 因子に分解できた。それぞれの因子に含まれる設問項目をもとに、適切な命名を行なった結果は次の通りである。

従来型ネット閲覧因子:
: 2 ちゃんねるまとめサイト、2 ちゃんねるなど BBS、ニコ動を見る、マスコミニュースサイト

ゲーム因子:
: モバゲー無料利用、GREE 無料利用、GREE 課金利用、モバゲー課金利用

twitter 因子:
: twitter で発言、twitter を見る

Ustream 因子:
: Ustream で発信、Ustream を見る

最近型ネット閲覧因子:
: 楽天、アマゾン、質問サイト、iTunesStore、Youtube を見る、facebook

図書館因子:
: 公営図書館、高校図書館

分けられないもの:
: おさいふケータイ、ニコ動へアップ、携帯メール、Youtube へアップ、ショートメール、mixi

表- 13: 日常のネットワーク利用頻度 (%)

項目	%
携帯メール	59
Youtube を見る	50
携帯同士の SMS	38
ニコニコ動画を見る	27
公営の図書館	25
twitter を見る	25
高校の図書室	21
大手ニュースサイト	19
mixi	16
twitter で発言	16
2 ちゃんねるまとめサイト	15
アマゾンで買いもの	14
2 ちゃんねる・したらばなど BBS	13
Yahoo 知恵袋など質問サイト	11
iTunesStore	11
モバゲー無料の範囲で遊ぶ	9
facebook	8
GREE 無料の範囲で遊ぶ	6
楽天で買いもの	3
Ustream を見る	3
おさいふケータイ	3
Youtube へアップロード	2
ニコニコ動画へアップロード	1
Ustream で番組発信	1
モバゲーで課金して遊ぶ	1
GREE で課金して遊ぶ	0

各因子負荷量をグラフにしたものを、図 1 に示す。(なお、図のラベルに使用した用語は、表示スペースの都合上略記されたものである。)

表 13 をみると、例えば Youtube は 50% の大学 1 年生がよく見ると回答しているが、図 1 によれば、Ustream 因子群や図書館因子群は Youtube 閲覧で 0 に近い負荷量を示している。高校生や大学 1 年生の各層に共通するサイト・場所がないことを示す。すなわち、高校生に大学情報を発信したり、大学 1 年生に情報教育を行なったりする場合には、それぞれに存在する各層に届くような方法・内容を考えることが必要であることを示している。例えば、大学が twitter を使った情報発信を行なっても、携帯ゲームや図書館の利用者には効果が高くないことを示唆している。また、2 ちゃんねるなどの従来型のネット利用者と、facebook などの最近型のネット利用者が分けられており、mixi の利用者は、そのどちらにも含まれていない。

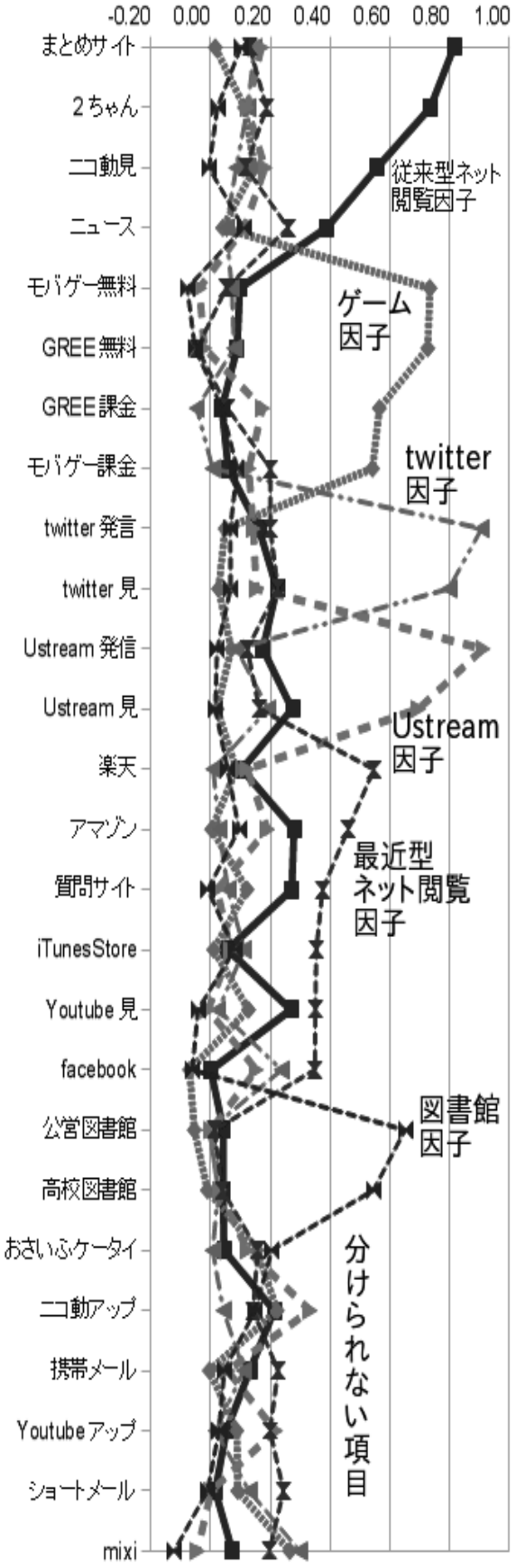


図- 1: バリマックス回転を行なった結果

3.6 情報機器・ネットワークの活用

情報機器・ネットワークの活用について得た回答を、表 14 に示す。(質問項目と選択肢は、付録 2. に示した。)

表- 14: 情報機器・ネットワークの活用 (%)

	選択肢				
項目	1	2	3	4	5
パソコン:セットアップ	9	19	42	26	3
パソコン:プロキシの設定	2	4	19	71	3
パソコン:無線 LAN 接続	12	20	30	35	3
パソコン:OS のアップデート	9	15	35	39	2
アンチウイルスアップデート	10	21	36	30	2
パソコンでインストール	17	25	31	25	2
ソフトウェアライセンス	6	10	22	48	14
データのバックアップ	7	15	33	42	3
スマートホンセットアップ	7	15	20	19	39
スマートホン無線 LAN 接続	10	13	18	20	39
携帯電 PHS セットアップ	11	22	33	26	9
ネット情報の根拠確認	8	20	30	39	3
匿名／複数アカウントを利用	12	18	25	40	5

選択肢:「1: よく理解している」から「4: 全く理解してない、独力ではできない」の順。および、「5: 該当なし (持っていない)」とした。

ほとんどの項目で、「あまり理解していない」「全く理解していない」の回答が多いが、特に、「全く理解していない」と回答したものが高いのは、プロキシの設定 (71%)、ソフトウェアライセンス (48%) であった。また、「ネット情報の根拠確認」も、69%が「理解していない」あるいは「全く理解していない」のどちらかを回答した。

4 今後の展望とまとめ

今回、我々は非常に大規模で詳細な調査を行ない、本学の 2012 年学部 1 年生の情報活用能力について、従来とは異なる視点からデータを得ることができた。その結果明らかになったことをまとめると次のようになる。

1. 高校情報科の履修状況は、改善はしているものの十分な状況にはなっていない。
2. 大学入学以前に「タッチタイピング」の指導と「コンピュータプログラミング」の学習があまり行なわれていないが、学生は学習を強く望んでいる。
3. 高校の学習指導要領に記載されていない「メディアリテラシー」「統計処理」は、いずれも非常に低い経験・理解度であった。
4. 学生の学習意欲は、オフィスソフトの中でも表計算ソフトに集中しているが、一方で、タッチタイピングとプログラミングへの学習意欲も高い。
5. 情報倫理やメール、ネット検索に関する項目を大学の授業で学習することは望まれていない。一方で、多くの学生が「情報の根拠（ソース)」の確認はできないと回答している。
6. PC の所有率は 50% 前後であったが、 Mac の所有率はかなり低い。
7. 自分のパソコンを安全に保つための OS アップデートや、プロキシの設定、ライセンスの概念を理解していないきない学生が多い。
8. Youtube, ニコニコ動画、2 ちゃんねるなどの掲示板、twitter の利用度は極めて高い。
9. 普段から利用しているデバイスやサイト、その他の情報源を、いくつかのパターンに分けることができる。

以上から、大学 1 年生に対して情報教育を提供する際や、大学が高校生に情報発信を行う場合は、以下の整備方針や、学内の教育設計、ネットワーク整備を設計し、大学としての、広報方針を立てることが望ましいと思われる。

1. 高校情報科の履修状況が十分であるという前提を置かずに、情報教育の内容を設計する。また、高校で「メディアリテラシー」「統計処理」が、ほとんど学ばれていないことを考慮する。
2. タッチタイピング，プログラミング，統計処理のソフトウェアの整備状況の確認。ほぼすべての情報系センターで用意していると思われるが，それが十分か不足か、また、適宜更新されているか。
3. 学生の個人所有のパソコンの管理状況の調査について、情報系センターで提供すべきか，また、本学など導入されている検疫ネットワークの利用方法の告知状況、その他、スマートホンなどを大学のネットワークにつなぐ際のスキルやリテラシ水準の確認。
4. 情報のソース（根拠）の確認ができないと回答している者が少なくなく、一方で、因子分析からも図書館を利用する人が限られていて、他の情報サービスの利用者とは異なるグループにいると考えられる。単に一般情報教育の中で図書館の利用を訴えるだけでなく、情報ソースの確認という視点から図書館などを利用する活動に促していくことも一つの案として考えられる。また、各大学で行なっているオンラインジャーナルや、電子ジャーナルの利用ライセンスについての教育などは、本来は図書館で行なう学術情報教育であるが、学外からの学認やプロキシを利用した利用の是非と可否など

については、情報系センターも教育に協力を行なうことが望ましいと思われる。

なお、本調査は、本学で 2012 年 4 月に実施したものであり、上記の方針は、その内容に基づいている。2013 年以降に同じ目的の調査を行なう場合は、本調査と同様の趣旨で最新の高校生・大学生の動向を調査するべきであるが、アンケート項目などは、年度・各大学の状況に応じて適切に更新することが望ましいといえる。

参考文献

[1] 瀬川大勝, 辻澤隆彦, 辰己丈夫. 仮想化技術を用いたサーバ集約と演習端末室の構築. 学術処理研究論文誌, No. 15, pp. 134–141, 2011.

[2] 辻澤隆彦. 学術基盤オープンフォーラム 2010. 国立情報学研究所, 2010.

[3] 文部省. 高等学校学習指導要領, 1999.

[4] 文部科学省. 高等学校学習指導要領, 2009.

[5] 望月俊男, 熊本悦子, 塚本康夫. 大学入学前の情報教育に関する学習機会の調査分析：関西地区の国立大学を対象とした事例研究 (特集 情報教育の成果と課題). 日本教育工学会論文誌, Vol. 30, No. 3, pp. 259–267, 2006-12-20.

[6] CEC 有識者委員会. 平成 20 年度「高等学校等における情報教育の実態に関する調査」, 2009.

[7] 青木謙二, 鍵山茂徳. 大学における教科「情報」の基礎学力確認テストの実施と結果の分析 (情報教育, ＜特集＞情報教育〜理念・理論・実践〜). 情報処理学会論文誌, Vol. 48, No. 8, pp. 2759–2766, 2007-08-15.

[8] 澤田大祐. 高等学校における情報科の現状と課題. 調査と情報, No. 604. 国立国会図書館調査及び立法考査局, 2008.

[9] 辰己丈夫, 久野靖, 加藤毅. 大学生を対象としたインタビューによる日本の情報教育の問題分析. 第 4 回全国大会予稿集, pp. 92–93. 日本情報科教育学会, 2011.

[10] 松葉哲史. 新入生対象のパソコン講習における大学生協のポジション. 2011 PC Conference 論文集, pp. 182–184. CIEC, 2011.

[11] 玉井哲雄. 東京大学における一般情報教育. 情報処理, Vol. 52, No. 10, pp. 1336–1340, 2011.

[12] 布施泉, 岡部成玄. 北海道大学における全学教育としての情報教育. 情報処理, Vol. 52, No. 10, pp. 1341–1345, 2011.

[13] 原田康也. 一般教育科目の情報化：情報検索リテラシーを重視した授業実践の試み. 情報処理学会研究報告. コンピュータと教育研究会報告, Vol. 2004, No. 100, pp. 17–24, 2004-10-02.

[14] 国立大学情報教育センター協議会 TF/メディア教育開発センター. 情報倫理デジタルビデオ小品集 3, 2007.

[15] 村田育也, 中村純, 山之上卓, 岡部成玄, 布施泉, 辰己丈夫, 中西通雄, 深田昭三, 多川孝央, 山田恒夫. 情報倫理ビデオ教材のプレポストテストによる評価. 電子情報通信学会技術研究報告. SITE, 技術と社会・倫理, Vol. 106, No. 401, pp. 31–36, 2006-12-01.

[16] 楠元範明, 前野譲二. アカデミックリテラシー 2009. 早稲田大学出版部, 2009.

[17] 川合慧 (監修). 東京大学教養学部テキスト 情報. 東京大学出版会, 2006.

[18] National Research Council. *Being Fluent with Infomation Technology*. National Academy Press, 1999.

[19] 中川徹也, 湯浅寛美, 吉野貴之, 虎岩雅明. 千葉大学及び東京理科大学における新入生パソコンライフ応援計画実施の報告. 2009 PC Conference 報告集, pp. 161–162, 愛媛大学, 8 2009.

[20] 教育用計算機システム利用の手引. 東京大学情報基盤センター情報メディア部門, 201.

[21] 東京農工大学総合情報メディアセンター利用の手引 2012 年度版. 東京農工大学総合情報メディアセンター, 2012.

[22] 和田正人. ソーシャルメディアを利用した東日本大震災ニュース映像についての大学生のメディア・リテラシー学習. 第 63 巻, pp. 255–262. 東京学芸大学紀要 総合教育科学系, 2012.

[23] 辰己丈夫, 久野靖, 加藤毅. 大学 1 年生を対象とした調査票調査にみる高校情報科の内容と実施状況の影響. 第 5 回全国大会予稿集, pp. 33–34. 日本情報科教育学会, 2012.

[24] 辰己丈夫, 松葉哲史. これからの大学生に必要な情報フルーエンシーを目指したパソコン講習会. 2012 PC Conference 論文集, pp. 359–362. CIEC, 2012.

付録：調査項目

1. 高校情報について

1. あなたは、教科「情報」を、いつ履修しましたか（いつ履修したことになっていますか？）
   (a) 履修したことになっているが、実際に「情報」のいずれかを履修した記憶がない
   (b) 中学段階で履修を始めた（中高一貫校、中等教育学校など）
   (c) 高校 1 年生で履修
   (d) 高校 2 年生で履修
   (e) 高校 3 年生で履修
   (f) 高校の複数学年で履修
   (g) 履修していない（インターナショナルスクール、高卒認定、その他の入学方法など）
   (h) わからない
2. 最初の教科「情報」の科目として、どの科目を履修しましたか（履修したことになっていますか）
   (a) 情報 A
   (b) 情報 B
   (c) 情報 C
   (d) 代替科目（「情報技術基礎」などの工業高校、商業高校設置科目）
   (e) わからない（授業はあったが、当時からわからなかった）
   (f) わからない（履修したことになっているが、実際には全く授業がなかった）
   (g) 忘れた（当時は覚えていた）
   (h) 該当しない（「情報」を全く履修していない）
3. 教科「情報」の時間設定はどうでしたか
   (a) 週 2 時間
   (b) 週 1 時間で、2 年間履修した
   (c) 週 1 時間で、1 年間履修した
   (d) その他 (1 学期のみ、不定期、夏季集中など)
   (e) 該当しない（「情報」を全く履修していない）
4. 2 つ目の教科「情報」の科目として、どの科目を履修しましたか
   (a) 情報 A
   (b) 情報 B
   (c) 情報 C
   (d) 代替科目（「情報技術基礎」などの工業高校、商業高校設置科目）
   (e) わからない（授業はあったが、当時からわからなかった）
   (f) わからない（履修したことになっているが、実際には全く授業がなかった）
   (g) 忘れた（当時は覚えていた）
   (h) 該当しない（「情報」の科目は 1 つだった、あるいは「情報」を全く履修していない）
5. 教科「情報」の授業内容はどのようなものでしたか
   (a) 主に教科書を利用して「情報」の内容を学んだ
   (b) 主に副教材（例えば、ワードの使用方法などの教材）を利用して「情報」の内容を学んだ
   (c) 主に先生自作のプリントで「情報」の内容を学んだ
   (d) ある時期は「情報」の内容だったが、別の時期は他教科の内容だった
   (e) 完全に他教科だった
   (f) 「情報」の内容かどうかがよくわからなかった
   (g) 該当なし（「情報」を全く履修していない）

2. 単元・項目毎の状況

- タッチタイピング (キーボードを見ないでタイプする)
- ワープロ（ワードなど）の基本的操作
- 作文・文章作成（ワープロ操作以外の項目）
- 表計算ソフト（エクセルなど）の基本的操作
- モデル化とシミュレーション
- プレゼンテーションソフト（パワーポイントなど）の基本的操作
- パソコンを使用したメールの基本操作
- 検索サイトの使用方法
- コンピュータプログラミング
- コンピュータやネットワークの仕組み
- データベースの作成画像処理とマルチメディア
- Web ページ (ホームページ) を HTML で作成
- メールのマナー・モラル
- 著作権
- 他人の個人情報の取り扱い
- 自分の個人情報の取り扱い
- メディアリテラシー
- 統計処理

選択肢

1. 高校の教科「情報」で学んだ。身に付いた。
2. 高校の教科「情報」で学んだ。身に付いてない、他の科目あるいは独学で身につけた。
3. 高校の教科「情報」で学んだ。
   現在、身についてない。
4. 高校の教科「情報」で学ばなかった。
   他の科目あるいは独学で身につけた。
5. 高校の教科「情報」で学ばなかった。
   現在、身についてない。
6. 言葉の意味がわからない。

3. 大学の情報関係の授業で学習したいこと

選択肢は、**2.** 単元・項目毎の状況と同じ。3 つを選択させた。

4. 日常の ICT 機器の活用について

選択肢は以下の通り。

1. かなり頻繁に（ほぼ毎日）利用していた
2. よく利用していた
3. 時々利用していた
4. あまり利用していないが見たことはある（あるいは会員登録したことはある）
5. 存在は知っていたが、全く利用していなかった
6. 存在を知らない、わからない

質問項目は以下の通り。

1. 自分専用のパソコン（Mac 以外）
2. 自分専用のパソコン（Mac）
3. iPhone
4. Android スマートホン
5. その他の携帯電話や PHS
6. iPad
7. デジタルカメラ
8. 携帯同士のショートメール（SMS）
9. 携帯を利用した電子メール（他社携帯やパソコンなどへ）
10. mixi
11. 2 ちゃんねる・したらば・まち BBS など
12. Yahoo 知恵袋や教えて goo など質問・回答サイト
13. モバゲーでアイテム購入などの課金をして遊ぶ
14. モバゲーで無料の範囲で遊ぶ
15. GREE でアイテム購入などの課金をして遊ぶ
16. GREE で無料の範囲で遊ぶ
17. facebook
18. twitter で自ら発言する
19. twitter を見る
20. Youtube への動画アップロード
21. Youtube を見る
22. Ustream で番組を発信する
23. Ustream を見る
24. ニコニコ動画への動画アップロード
25. ニコニコ動画を見る
26. ニュースサイト（大手マスコミが運営）
27. ニュースサイト（2 ちゃんねるまとめサイトなどのネットのニュース）
28. 楽天で買いもの
29. アマゾンで買いもの
30. iTunesStore(アプリ、音楽コンテンツ・ビデオコンテンツ)
31. おさいふケータイ機能（モバイル Suica を含む）
32. 公営の図書館（区立や市立の図書館）
33. 高校の図書室・図書館

5. 情報機器・ネットワークの活用

選択肢は以下の通り。

1. よく理解している／できる
2. ある程度理解している／できる
3. あまり理解していないが知っている程度／調べながらならできる
4. 理解してない／独力ではできない
5. 全く理解してない、該当なし（持ってない）

質問項目は以下の通り。

1. パソコンのセットアップ（Mac を含みます）
2. パソコンの OS のアップデート
3. パソコンのプロキシの設定
4. パソコンを無線 LAN に接続する
5. パソコンでのソフトウェアのインストール
6. ソフトウェアのライセンス
7. ウイルス対策ソフト（アンチウイルス）のアップデート
8. データのバックアップと復元
9. スマートホンのセットアップ
10. スマートホンを無線 LAN に接続する
11. その他の携帯電話・PHS のセットアップ
12. ネットに出ている情報のソース（根拠）の確認
13. 匿名アカウント／複数アカウント

6. 本人属性

1. 性別
   (a) 男
   (b) 女

IC カード全学導入に向けた認証基盤システム整備と評価

Development and evaluation of authentication infrastructure system in the aim of introducing an entire smart card system

清水　さや子†，戸田　勝善†，吉田次郎‡
Sayako SHIMIZU†, Masayoshi TODA†, Jiro YOSHIDA‡

smz@kaiyodai.ac.jp, toda@ kaiyodai.ac.jp, jiroy@ kaiyodai.ac.jp

†東京海洋大学情報処理センター
‡東京海洋大学大学院海洋科学技術研究科

†Information Processing Center, Tokyo University of Marine Science and Technology
‡The Graduate School of Marine Science and Technology, Tokyo University of Marine Science and Technology

概要

近年，大学において認証システムが重要視されるようになり，認証基盤システムの充実化や利用者アカウントの厳格な管理が求められている．東京海洋大学では 2006 年のシステム更新時に統合認証システムを導入することによりアカウントの一元化を図った．アカウントの一元化はユーザにとっては一組のアカウントとパスワードを覚えるだけで複数のシステムが利用できるため，利便性の向上につながったが，アカウントの管理や統合認証システムと連携するシステムにおける運用については，問題が山積みになっていた．そこで，2011 年のシステム更新では，IC カードの全学導入も考慮したシステムを検討する必要があり，アカウントやシステムの管理方法も含め認証基盤システムの見直しを検討し，新たに統合ディレクトリシステムの構築を行った．統合ディレクトリシステムの構築により，アカウントやシステムの一元管理が実現することができ，運用の効率化につながった．本稿では，旧システムでの問題点および新しく構築した統合ディレクトリシステムで解決できた問題について述べる．

キーワード

認証基盤システム，アカウント，統合ディレクトリシステム，IC カード

1. はじめに

近年，統合認証システムが導入されアカウントとパスワードの一元化が進みつつある[１]．アカウントとパスワードの組み合わせは一度破られると，後々に重大な問題に発展する恐れがあるため，さらなる認証セキュリティの強化として IC カードによる認証システムが使われることも多くなっている．

東京海洋大学は，2003 年 10 月 1 日に東京商船大学と東京水産大学が統合されて発足した大学である．統合に伴い両大学に存在していた情報処理センターも組織としては統合されたが，システムについてはレンタル契約上の問題等により，地区ごとに異なるシステムが稼働していた. そして, 統合から約 3 年が経過した 2006 年 8 月に，情報処理センターシステムの更新を行い，キャンパスごとに独立して稼働していたそれぞれのシステムを統合し，アカウントにおいても一元管理できるよう統合認証システムを導入し，実質的な統合を行った.

IC カードは，旧東京水産大学にあたる品川キャンパスで, 不正アクセス防止のため 2000 年から教育システムの認証用に導入されていた経緯より，2006 年 8 月のシステム更新時に, 全学的に IC カード学生証が導入されることになった[２][３]．これによって，全学的に教育システム利用時には IC カード認証が取り入れられた. この時より，統合認証システム導入によるアカウントの一元化，IC カード学生証導入による各種 IC カードを使った認証システムが利用可能になったが[４]，アカウント管理の問題，各システムのユーザ登録方法の問題，各システムに対する認可の問題等，様々な問題も発生していた.

2011 年の情報処理センターシステム更新では，これらの問題解決に向けて，ユーザおよびシステムの一元管理ができるシステムの構築を検討した．また，IC カードについては現時点では学生に対してのみ IC カード学生証を導入しているが, 教職員向けに IC カード身分証の導入も検討中であるため，IC カード全学導入を前提に認証基盤システムの設計を行い，新しく統合ディレクトリシステムの構築を行った.

2 章では，認証基盤システムの整備に至った様々な問題について述べ，3 章では，問題解決するための統合ディレクトリシステムの設計について，4 章では，構築したシステムとその評価，5 章でまとめと今後の展望について述べる.

2. 認証基盤システムの整備に至った旧システムの問題

アカウントの一元管理を実現した統合認証システムでは，アカウントの管理が重要となる．大学の構成員は学生と教職員だけでなく，短期間採用の職員や派遣社員，企業在席の研究者等などのさまざまな期間，さまざまな身分の人（以下，一時利用者とする）が存在する.

2.1 アカウント管理の問題

旧システムでのアカウントは，統合認証システムを管理している情報処理センター発行のアカウントとして，登録，管理は，情報処理センターで行っていた．登録方法は学生の場合と教職員や派遣社員，研究員等の場合で大きく異なっていた.

i. 学生情報の登録

学生情報を登録する場合, 学生は IC カード学生証が導入されていることより，入学者が決定し次第，学生担当係が IC カード学生証の発行用データ作成し, 学生証の発行手続きを行う．その後，情報処理センターではこの発行用データを受領し加工することにより，システムに反映させていた．学生情報を削除する場合は，同じく学生担当係から年度末に卒業者・退学者リストを受け取り，その情報に基づいて削除作業を行っていた．学生情報については，学生担当係からの情報を基に登録・削除作業を行っていたため，大きな間違いは発生しなかった.

ii. 教職員や研究員等情報の登録

教職員や研究員等の情報を登録する場合，学生以外は IC カード身分証が導入されていないため, IC カード発行用のデータを作成している部署がなかった．それで，新規採用の教職員は，着任時にアカウント登録申請書を情報処理センターに提出し，情報処理センターにて申請書情報の確認後，登録用データを作成し，登録作業を行っていた．アカウント削除は，離任時に本人が削除申請書を情報処理センターに提出し，情報処理センターにて削除作業を行っていた. これらは, 情報処理センターでは，個人情報を管理しておらず，本人の申請に基づき登録・削除作業を行っていたため，着任しても申請せずにアカウントを保持していない人や，離任しても削除申請がないため，退職者が削除されていない人がいることも多くあった. 特に常勤教職員以外については, 把握が困難で，離職後でもメールや図書館のサービスが利用可能な状況が生じていたため，ライセンス違反となる可能性があった.

各システムに対するアカウント管理の重要性は認識していたが，情報処理センターではユーザの正確な在職状況の有無を確認する術がなかった．また，身分属性に応じて，利用できるサービスが異なるが，身分属性を判断することが困難な場合があり，間違った情報が登録されることもあった．最近では，学認に参加する大学も増えており，東京海洋大学においても学認の参加に向けて準備を進めている所である．学認に参加することは，所属する大学のアカウントで学認加盟機関の様々なサービスを受けることができるようになるため[５][６]，さらなるアカウントの厳格な管理が求められるため，認証基盤シ

ステムの整備が必要であった.

2.2 各システムのユーザ情報の登録方法に関する問題

旧システムでは，以下のシステムが統合認証システムと連携していた.

- Gateway サーバ，研究支援サーバ
- ファイルサーバ
- Mail サーバ
- 研究室用 www サーバ
- 教育用 UNIX サーバ
- 教育用 Windows ドメインサーバ
- E-Learning サーバ（2 種類）
- SSL-VPN システム
- 無線 LAN 認証システム※1
- SSO ポータルシステム※1

統合認証システムと連携しているメールサーバやファイルサーバ，Windows ドメインサーバや E-Learning サーバ等ほとんどのシステムが，統合認証システムの LDAP サーバとは別に，身分属性に応じて個別にユーザ情報の登録をしなければならなかった．これらのユーザ情報の登録は，情報処理センターで行っていた．申請書に記されている情報を基に LDAP サーバ登録用データを作成し，LDAP サーバに登録後，LDAP サーバ登録用データをシステムごとに必要な形に加工し，システムごとに登録作業を行っていた．そのため，1 回のユーザ情報の登録作業に 1～2 時間要していた. あらかじめ登録日を決めていたが，ユーザにとっては，申請書を提出しても即時にアカウントが発行されず，システムが利用できない状態であることが多々あり，不便が生じていた.

2.3 システムに対する認可の問題

情報処理センターでは，認証基盤システムとしてアクセスしてきた情報の照合をすることはできても，各部局で個別にシステムを立ち上げ，管理されているシステムに対して，利用者に利用権を与えるという「認可」を行うことは非常に難しい．情報処理センターが管理するシステムであれば，認可は行えるが，情報処理センターシステムの中には，過去の経緯により，他部局管理のシステムを導入しユーザ管理をおこなわなければならないことがあった．具体的には，事務用 Windows ドメインサーバの管理であった．ユーザの正しい情報が管理できない中，また，日々，管理・運用業務に追われている少人数の組織で※2これらの作業を行うことは非常に負担となっていた.

2.4 IC カードの管理に対する問題

東京海洋大学では，2006 年度の情報処理センターシステム更新時より，学生に対しては IC カード学生証が発行されることになり，情報処理センター教育システムのログイン時の認証，証明書発行システムや図書館の図書貸出システム等で利用している．2010 年度の情報処理センターシステム更新時には，全学的に IC カード身分証の導入を検討しており，IC カード発行・管理システムは，学生向けではなく，全学のシステムとして管理運用できるようにする必要があった.

IC カード発行・管理システムは全学のシステムということより，システムの設計や構築，管理運用は情報処理センターで行うが，システム内の情報は各担当係（IC カード学生証であれば学生担当係，教職員向け IC カードであれば教職員担当係等）が必要に応じて作成し，登録することになっていた．これは，情報処理センターでは正しい在籍者情報を保持していないことと，組織の規模より個々の IC カード発行，失効，再発行等の管理運用が行うことが非常に困難であるためである.

現在，IC カード身分証の導入については停滞中であるが，導入された場合，教職員に対しては教職員担当係，派遣職員に対しては契約担当係等，身分属性によって担当部局が異なるが，各担当係が IC カード発行用のデータを作成することになる．そうなれば，情報処理センターでは，学生情報と同様，登録ユーザ情報の漏れがなくなり，適正なアカウント管理が行えるものと考えた.

3. 統合ディレクトリシステムの設計と構築

前章で紹介した旧システムの問題の解決に向けて，ユーザ情報および各システムの利用権および IC カード発行・管理システムの一元管理ができる統合ディレクトリシステムの設計・構築を行った．本章では問題解決において検討した内容について述べる．統合ディレクトリシステムでは，身分属性ごとの各担当係が IC カード身分証（学生証含む）用のデータを登録すれば，アカウント発行，身分属性ごとに異なる利用システムへのユーザ情報登録，登録したアカウントに対する IC カードの管理が行うことが可能になる．さらに，統合ディレクトリシステムでは，情報処理センターの管理外のシステムに対して，

※1 これらは 2006 年度のシステム更新時ではなく，2010 年度に新たに構築したシステムである.

※2 東京海洋大学情報処理センターは，専任職員（技術系職員）2 名，兼任のセンター長 1 名および兼任の副センター長 2 名，非常勤職員（事務系）数名で構成されている.

そのシステムの管理者がユーザごとに利用権の可否を設定することができる.

3.1 他大学の導入事例

一般的にアカウントの発行は，採用時・入学時に，担当部署からユーザ情報のデータを受け取り，センターが発行する場合や[５], 採用後・入学後にユーザが申請し，申請があったユーザのみ発行する場合がある．前者については，先進的に，全学レベルで事務方が全学 ID 管理をしている大学もあるが，全学 ID が発行されるだけでは，センター管理のシステムのシステムが利用できるわけではない[８]．大規模大学のように，学内にサーバが分散しており，部局ごとにメールサーバがあり，部局ごとにメールアカウントを発行しているため，採用時・入学時に全学アカウントがなくても問題ないような大学もあるが[９]，本学のような小規模大学では，メールサーバは情報処理センターで一元管理しており，利用には全学アカウントを利用するため，採用時・入学時にアカウント発行できるシステムであるのが望ましい．さらに，認証基盤システムやアカウントの管理が重要視され，専用の組織（センターやチーム）を立ち上げた大学もみられる[９][１０]が，本学においては，全学的にそのような動きがないため，専用の組織を立ち上げるのは困難であると思われる.

3.2 アカウント管理の問題回避に向けて

現在，東京海洋大学には，約 3000 人の学生と約 700 人の教職員，その他として派遣職員や企業研究者等の一時利用者で構成されている.

情報処理センターでは，統合認証システムのアカウント発行に必要な情報として，アカウント，氏名，ローマ字氏名，学籍番号（教職員番号），契約期間（ある場合），身分属性（所属グループ）等の比較的簡易な情報を管理していた．これらとは別に，事務局では詳細な個人情報を格納した DB を管理している．しかし，身分属性ごとに担当部署が異なるため，それぞれの部署に DB が存在する．本来は，この事務局の管理する DB と連携して必要情報を自動抽出し，統合ディレクトリシステムに反映させられることが望ましいが，事務専用ネットワーク内で稼働しているシステムであるため，セキュリティや個人情報等のポリシー問題もあることより，連携することが非常に難しかった．そこで，DB を管理している事務局で，必要情報を抽出し，採用・入学の度に，統合認証システム用のアカウントを登録・発行することができれば, アカウント情報は比較的正しい情報となる. しかし，事務局に登録業務を依頼することは，事務職員にとって技術的に困難であること，また業務が負担増になることなどから旧システム時においては難しかった.

3.2.1 IC カード発行用データとアカウント発行用データ

東京海洋大学では, 全学的に IC カード身分証の導入が検討されている．そうなると，事務局では，身分属性ごとの各担当部署を明らかにし，担当部署ではそれぞれの IC カードを発行することになる.

先に導入されている IC カード学生証を例に挙げると，IC カード発行用のデータに必要な情報は，漢字氏名，ローマ字氏名，学籍番号（教職員番号），所属，有効期限等である．これらの情報のほとんどが統合認証システムのアカウント発行に必要な情報と重複する. IC カード発行用データに発行するアカウント情報さえ追加すれば，アカウント発行用のデータとなる．これらより，IC カード発行システムと統合認証システムのアカウント情報の登録が一度で行えるようなシステムの設計を行った.

ここで問題となるのは，アカウント名である．従来は申請時に希望アカウント名を受け付けていたが，個別対応および重複確認の手間もあった．かねてから運用効率化における問題になっていた．これらを踏まえて，今回を期に，アカウント登録時に自動でローマ字氏名から指定の文字を抜き出し重複防止文字を追加する仕組みを作成した．これによって，従来の希望アカウント名の申請は廃止し，IC カード発行用データを登録するだけでアカウントが自動で発行することができるようになり，登録時の個別対応の手間が削減できた.

ただし，海洋大メールシステムでは，メールアドレスが*アカウント名*@kaiyodai.ac.jp としているため，発行されたアカウント名に対応したメールアドレスになる．現状では，本人の希望するメールアドレスが作成できないため，エイリアスを作成するなどして対応中であるが，今後は, メールアドレスにアカウント名を出さないよう，個人の希望メールアドレスが使用できるよう，検討中である.

3.2.2 登録担当係

IC カードを発行する場合，大学という組織においては身分属性ごとに担当部署が異なるため，どういった身分属性の人をどういった部署が担当すべきかが問題になる. 大学という組織は教員・職員の他，派遣契約職員や受託研究員・共同研究者等も在籍する．これらの人は在籍期間も業務もさまざまであるため，把握が非常に困難である．さらに，事務局を通さずに出入りしている企業在席の研究者等もいるが，非常に多くのパターンが予想されるため，今回は検討しないこととした.

まず，事務局で把握できる学生以外の人員に対して，

表 1　登録担当ロール

項	ロール分け	操作対象ユーザ
1	学生担当係	学生
2	教職員担当係	教職員
3	派遣契約等担当係	派遣契約などの職員
4	研究員等担当係	受託研究員等・共同研究者・訪問研究者等
5	ゲスト・テスト用アカウント担当係	ゲストカード・テストアカウント・システム管理者用アカウント
6	全管理者	全ユーザ

身分属性により 25 のグループに分けグループ ID を設定する．学生に対しては，便宜上，学科ごと入学年度ごとにグループ分けグループ ID を設定する．これらのグループ ID に対して，今回の統合ディレクトリシステムにおいては，学生は 1 グループ，学生以外は人員担当部署ごとに 5 つのグループの合計 6 つのグループ分ける．6 つに分けたグループには，それぞれ担当ロールとして事務局の担当部署を割り当て（表 1），それぞれの担当ロールは，割り当てられたグループに属する人員の IC カード発行手続きを行うと同時にアカウントの発行ができるようにする．

これらによって，項 2.4 の問題も解決し，アカウント登録漏れや削除漏れ問題も解消されると考える．

表 2　IC カード管理ロール

項	ロール分け	操作対象 IC カード
1	IC カード学生証管理係	学生証
2	IC カード職員証管理係	教職員証
3	IC カード簡易利用証管理係	派遣契約などの施設利用カード
4	IC カード簡易利用証管理係	受託研究員等・共同研究者・訪問研究者等用の施設利用カード
5	ゲスト・テスト・管理用カード担当係	ゲストカード・テスト用カード・
6	全管理者	システム管理者用のカード

本システム導入時においては，それぞれの登録担当ロールが IC カードを発行する設計であるが，大学当局の要望により，将来的に同じ部署の中でも登録担当係と IC カード管理係と分かれる可能性があるとのことより，さらに，表 2 のとおり，IC カード管理ロールも作成し，それぞれ担当する対象のカード情報に分ける（表 2）．操作対象 IC カードは，それぞれ操作対象ユーザと同じとする．

3.3　各システムにおけるユーザ登録方法

旧システムでは項 2.2 のとおり，システムごとに個別にユーザ登録を行っていたが，アカウントが発行されると，統合認証システムや，連携しているシステムに対しても自動でユーザ情報が登録されることが望ましい．そこで，統合ディレクトリシステムでは，グループ ID ごとに，以下のシステムに対して利用可否情報の DB を作成しておき，アカウントが発行されると，グループ ID を閲覧し，該当グループ ID に対して利用可能なシステムのユーザ登録や利用領域の割当てが自動でされるようにする．また，アカウント削除時には，統合ディレクトリシステム上からアカウントが削除されることにより，利用可能であったシステムからユーザ情報や利用領域の削除を自動で行う．

- LDAP サーバ
- Gateway サーバ，計算サーバ
- ファイルサーバ
- Mail サーバ
  - 転送メールシステム含む
  - Web ファイルシステム含む
- 研究室用 web サーバ
- DNS ツールシステム（IP アドレス管理用）
- 教育用 Windows ドメインサーバ
- 教育用プリンタ管理システム
- E-Learning サーバ
- 無線 LAN 認証システム※1
- SSO ポータルシステム※1

これらの実現により，アカウントを発行するだけで，利用できるシステムにユーザ情報の一括登録ができるようになるため，各システムに対する登録・削除作業の手間が削減され，非常に運用効率化につながる．

3.4　他部署管理システムの利用権発行方法

旧システムでは項 2.3 の通り，過去の経緯により，他部署管理のシステムを情報処理センターシステムとして導入し，ユーザ登録も情報処理センターで行うことがあった．情報処理センターでは，他部署管理のシステムに対して，個々のユーザに対する利用権の可否を知ることが非常に困難であり，非常に手間が発生していた．

2010 年度のシステム更新時には，旧システムで導入していた事務局用 Windows ドメインサーバは事務局に移転したが，新しく図書館システム用に SSL-VPN が導入されることになった．SSL-VPN は図書館に申請があった

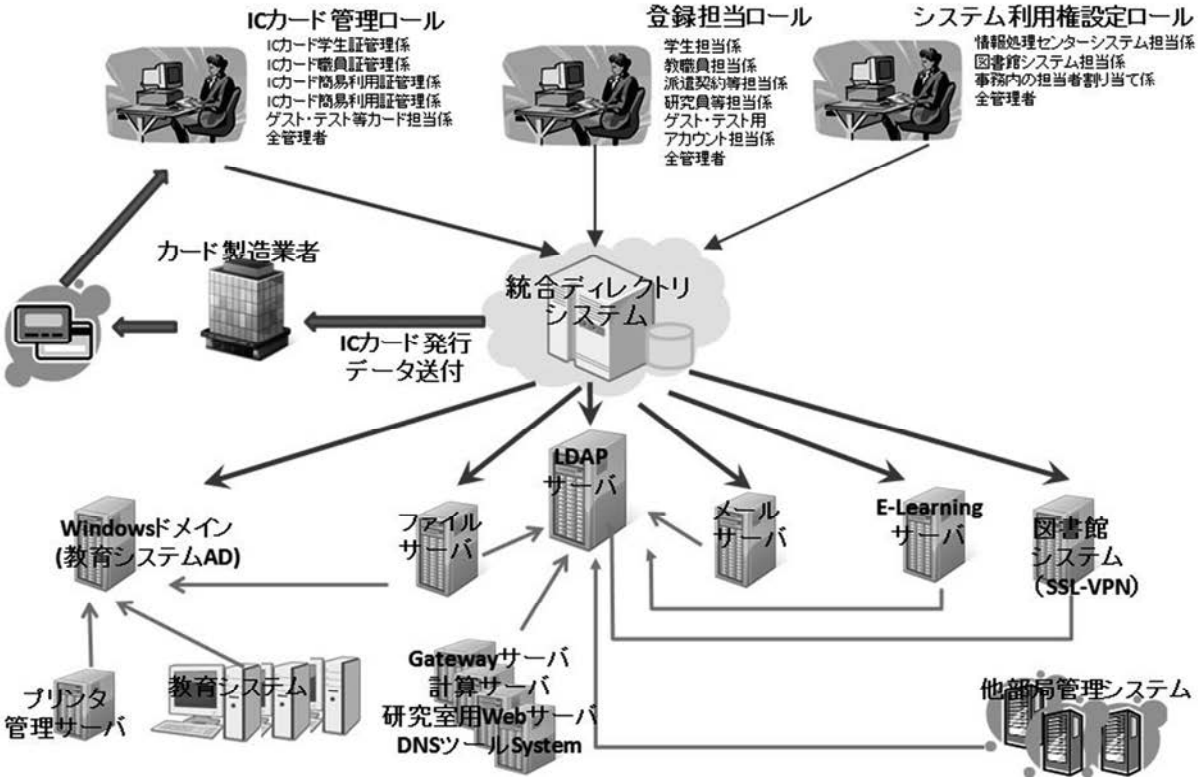


図 1　統合ディレクトリシステム

人だけ利用できるシステムであるため，情報処理センターでは，ユーザ登録を行うことはできない．そこで，事務職員でも比較的操作しやすいインターフェースを構築する必要があった．また，情報処理センターシステムにおいてもアカウント登録時にあらかじめ設定しているシステムに対して自動でユーザ登録されるが，個別に設定変更する場合もでてくる．さらに，登録担当ロールと IC カード管理ロールの各担当係の割り当てについては，事務局内で行われるため，事務局内で担当係の割り当てができたほうが効率がよい．

表 3　システム利用権設定ロール

ロール分け	操作するシステム
情報処理センターシステム担当係	情報処理センターシステムの各システムにおける認可
図書館システム担当係	図書館システムにおける認可
事務内の担当者割り当て係	登録担当ロール・IC カード管理ロールに関する認可
全管理者	システム利用権に関する属性の全て

これらより，表 3 のとおりロール分けし，統合ディレクトリシステムでロールごとに操作するシステム分けを行った．各ロールの担当係が担当範囲内について個別にユーザを設定できるようにする．ただし，操作対象者が事務局内の担当係となるため，Web 上から簡単に操作できるように簡素なインターフェースを構築した．

4. 構築した統合ディレクトリシステムの運用と評価

新しく構築した統合ディレクトリシステムでは，各登録担当者がユーザ情報を登録しアカウント発行を行うと，あらかじめ設定しているグループ ID ごとに，各システムの利用可否を確認し，利用可能なシステムに対して自動でユーザ登録が行える．また，将来的に身分属性ごとに IC カードの管理担当者も設定できるよう構築している．さらに，各システムの利用権を個別に登録や変更する際には，システム利用権担当者により，設定変更することができる（図 1）．本章では，本システムの運用方法について述べる．

4.1　ユーザ情報の登録

教職員であれば採用時，学生であれば入学時時に，それぞれ担当ロールの係が IC カード発行用のデータを作成し，統合ディレクトリシステムの管理画面よりユーザ情報の登録・アカウント発行業務を行う．

図 2　ユーザ登録用画面

ユーザ情報の登録作業は，1 部署で集中して行うのではなく，担当ロールごとに担当者が作業を行うため，Web インターフェース上で行う．さらに，作業は事務職員が行うため，図 2 のように比較的分かりやすくシンプルにする．登録作業における負担を軽減するため，登録情報は必要最低限の個人情報とする．登録時に Web インターフェース上のグループ ID を選択することで，あらかじめグループ ID ごとに設定されている利用可能なシステムに対して自動でユーザ登録される．グループ ID は登録時に選択するが，設定間違いを最低限にするため，担当ロールごとに複数のグループ ID が登録できるが，1 つのグループ ID に対して登録できるのは 1 つのロールとしている．また，IC カードの券面に表記される所属情報は，登録時に詳細に入力する必要はなく，あらかじめグループ ID 対して所属名の紐付けが行えるよう設定しているため，正しいグループ ID を選択するだけでよい．

IC カードの発行は，登録時に Web インターフェース上の「カード発行ステータス」箇所を「発行」とすることにより，ユーザ情報登録後，IC カード発行に必要なデータが抽出される．抽出されたデータをカード発行会社が指定する Web 入稿システムでアップロードすることにより，カードが発行される．

Web インターフェース上では必要な情報をテキストボックスに入力して登録するか，登録件数が多い場合は，あらかじめ csv ファイルを作成して一括登録も可能とする．Web インターフェース上から個別削除や一括削除もできる．

4.2　アカウントとカードの有効期限

登録時にアカウントとカードの有効期限の設定する．有効期限後は自動的に各システムのアカウントとグループ ID ごとに登録された利用可能なシステムの利用を停止する．通常は有効期限後，直ちにアカウント削除を行うのがよいが，例えば 3/31 に卒業した人が，4/1 にどうしても必要なデータを吸い上げるのを忘れていた事を思い出した時等に対応できるよう，有効期限後は一時的にアカウントをロック状態，カード使用不可状態にして，2 か月後に自動でアカウント削除を行う．登録時に有効期限を設定することにより，基本的には事務担当者が削除作業をする必要はない（表 4）．

IC カードの有効期限は，学生であればアカウント有効期限と同じであるが，教職員であれば，5 年間とする．非常勤職員の場合，アカウントの有効期限は長くても年度末までであるため，年度末までにアカウントの期限延長作業をする必要がある．ただし，カードには有効期限が記されるため，更新の可能性のある教職員に対しては，あらかじめ有効期限を 5 年とする．カードの有効期限前に退職した場合，先にアカウントの有効期限が切れるため，IC カードの停止処理を行わなくても，システムは利用できなくなる．ただし，認証基盤システムと連携して

表 4　アカウントの登録と有効期限に対するシステムとカードの利用可否

イベント	フロー	日付例	対応	アカウント利用可否	カード利用可否
新規登録	アカウント登録	2012/4/1	常勤教職員のアカウント有効期限は 2020 年と設定 非常勤はアカウントの有効期限を 1 年間に設定	○	×
	IC カード発行依頼	2012/4/2	IC カード発行依頼処理(業者に発行依頼) 学生証の IC カード有効期限はアカウントの有効期限と同じ (教職員の IC カード有効期限は 5 年間と設定)	○	×
	IC カード納品	2012/4/9	IC カード担当係宛に納品	○	×
	IC カード受け渡し	2012/4/10	IC カード個人に配布	○	○
期限延長	期限延長	2013/3/2	アカウントの有効期限が切れる前に再設定	○	○
期限切れ	IC カード返却	2013/3/21	IC カード返却	○	×
	期限切れ	2013/3/31	アカウントの自動的一時停止 IC カードの停止処理は行われないが、アカウントは停止 カードが返却されていなくても、ログイン不可	×	×
	アカウント削除	2013/5/31	2 ヶ月後にアカウント削除	×	×

おらず，カード内の読み取り可能な製造ID（IDm）等を認証情報とする簡易入退館システム等を個別に運用している場合にては，失効処理をしない限り，カードさえ持っていれば使えてしまうため，認証システムを管理する部局は運用ポリシー等を設定しておかなければならない．

4.3 IC カード運用上のイベント時の対応

IC カードを運用する際には，IC カード紛失，再発行，留年，休学，復学というイベントが発生する．これらのイベントについて，表 5 のように設定した．

I. IC カード紛失時

カードの使用停止処理を行い，数日間待ってカードが見当たらない場合は再発行手続きを行う．その間は，アカウントは停止処理しないため，カードを使ったシステムのみ利用できなくなる．再発行カードが納品された時点で，カード停止処理が解除され，新しいカード情報が上書きされ，カードを使ったシステムも利用できるようになる．

II. 留年の場合

アカウントは有効期限内に期限延長処理をしなければならない．カードについては券面に有効期限が記されているため，再発行することになる．カードがない間は，カードを使ったシステムのみ利用できない．

III. 休学の場合

アカウントも IC カードも停止処理を行うため，IC カードを使ったシステムも情報処理センターが管理する学内システムも利用できなくなる．復学した際にはアカウントと IC カードの復活処理を行い，両システムが利用できるようになる．

4.4 アカウントに対するパスワード変更および利用システム閲覧サービス

統合ディレクトリシステムではアカウントやシステムの登録等だけではなく，ユーザがパスワードを変更する際のインターフェースを提供している．ユーザがパスワード設定を行う際には，統合ディレクトリシステムの該当 URL にアクセスし，アカウントと現パスワードを入力してログインし，新パスワードの入力を行えば，LDAP サーバに反映される仕組みである．

また，ユーザごとに利用できるシステムが異なるため，ユーザごとに利用可能システムの一覧が表示できるインターフェースも備えている．ユーザが該当 URL にアクセスすることにより，各システムの一覧とそれぞれ利用の可否が表示される．

4.5 運用の評価

本システムの構築により，今まで情報処理センターで行っていた，個々のユーザに対する登録，変更，削除作業が事務局への移行を実現した．このため，今まで情報処理センターのアカウントとして，利用されてきたアカウントが，全学的なアカウントとなった．アカウントの管理が事務局に移行したことにより，ユーザ ID 通知書の発行・通知やパスワード再発行作業も事務の担当係が行うことになった．また，ユーザの情報を別の DB で保持している部署においてそれぞれ登録を行うため，ユーザ情報の登録漏れや誤入力がほとんどなくなった．ただし，非常勤職員用アカウントの有効期限については，一

表 5 イベント発生時のシステムとカードの利用可否

イベント	フロー	対応	アカウント利用可否	カード利用可否
IC カード紛失	紛失届	IC カードの一時停止処理	○	×
	紛失確定	一時停止している IC カードの執行処理(再発行)	○	×
IC カード再発行	IC カード発行依頼	IC カード発行依頼処理(業者に発行依頼)	○	×
	IC カード納品	IC カード担当係宛に納品	○	×
	IC カード受け渡し	IC カード個人に受け渡し	○	○
留年	留年決定	アカウントの有効期限延長	○	○
	IC カード返却	IC カード失効処理(再発行あり)	○	×
休学	休学・停学申請	アカウントの一時停止 IC カードの一時停止処理	×	×
復学	復学申請	アカウントの復活処理 IC カードの復活処理	○	○

部厳格な管理が行えていないケースもあるようである．本システム構築によって，情報処理センターとしては業務軽減の効率化が実現されたほか，かねてから問題であった正確なアカウント管理が行えるようになったといえる．

5. まとめ

本システムでは，IC カードの全学導入にむけて認証基盤システムを整備するため，旧システムでの問題を分析し，新しく統合ディレクトリシステムを構築した．

旧システムで問題となっていたアカウント管理，各システムのユーザ登録方法，各システムに対する認可についてさまざまな検討を行った結果，全てを一元管理できる統合ディレクトリシステムを構築した．アカウント発行・管理については，旧システムでは情報処理センターが行っていたが，本システム導入により，事務局の担当係が発行・管理を行うことになった．各システムに対するユーザ情報の登録は，旧システムでは個別に行っており，1 回の登録に約 1 ～2 時間かかっていた．しかし，統合ディレクトリシステムにアカウントを登録すると，グループ ID ごとにあらかじめ登録している利用可能なシステムに自動でユーザ登録されるため，1 回の登録にかかる時間は，数分程度となった．さらに各システムに対する認可については，旧システムでは，登録対象ユーザが不明であったり複雑であったが，簡易な Web インターフェースを用意することにより，各担当部局の担当者が容易に，認可を行えるようになった．

さらに，旧システムでは IC カード発行システムは単体のシステムとして稼働していたが，本システムでは統合ディレクトリシステムが包含し，IC カードの発行・失効等の管理も可能とした．

本システムが稼働して約 1 年になるが，Web インターフェースの一部改修は必要とするものの，大きな問題は発生していない．今後，IC カード身分証の全学導入が行われる予定であるが，本システムの構築により，比較的にスムーズに導入でき，システムも稼働できることを期待する．

参考文献

[1] 江原康生「大阪大学における新全学 IT 認証基盤システムの構築と運用」電子情報通信学会論文誌 D, Vol.J95-D, No.5, 1172-1182, 2012

[2] 清水さや子，横田賢史，戸田勝善，吉田次郎「東京海洋大学における IC カード学生証の運用・評価および今後の展開」学術情報処理研究 No.13, 64-73, 2009

[3] 清水さや子，横田賢史，戸田勝善，吉田次郎「東京海洋大学における全学 IC カード導入と多機能化に向けた取り組み」学術情報処理研究 No. 14, 149-152, 2010

[4] 清水さや子, 清水悦郎, 戸田勝善「IC カード認証・統合認証の連携システムの開発とその現状・評価」大学情報システム環境研究 VOL.11, 94-102, 2008

[5] 中村素典, 山地一禎, 片岡俊幸, 西村健, 庄司勇木, 古村隆明, 岡部寿男「学術認証フェデレーションを活用するサービスの展開」第 27 回インターネット技術第 163 委員会（ITRC）研究会 CIS 分科会,2010

[6] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 森 祥寛「大学における Shibboleth を利用した統合認証基盤の構築」情報処理学会論文誌 52(2), 703-713, 2011

[7] 沖野浩二, 布村紀男「富山大学における認証基盤の整備による業務軽減評価」学術情報処理研究 No. 14, 31-39, 2010

[8] 岩沢和男, 宮原俊行, 中川敦, 岩田則和, 西村浩二, 吉富健一「センターサービス利用登録システムの再構築」学術情報処理研究 No. 15, 149-152, 2011

[9] 京都大学情報環境機構” IC カード導入の効果” http://www.iimc.kyoto-u.ac.jp/ja/services/cert/iccard/merit.html

[10] 飯田勝吉, 新里卓史, 伊東利哉, 渡辺治「キャンパス共通認証認可システムの構築と運用」電子情報通信学会論文誌 B,Vol.J92-B No.10 pp.1554-1565,2009

学術情報光コアネットワークにおける
波長群スイッチングとリンク通過パス数均一化の効果

Impact of Waveband Switching and Equalizing of Paths in a Link on Photonic Core Networks in Japan

高野勝美†，軽部良‡，齋藤慶太‡，武田利浩‡，伊藤智博†
Katsumi Takano†, Ryo Karube‡, Keita Saito‡, Toshihiro Taketa‡, Tomohiro Ito†

ktakano@ieee.org

†山形大学　工学部学術情報基盤センター
‡山形大学　大学院理工学研究科

† Networking and Computing Service Center, Yamagata University
‡ Graduate School of Science and Engineering, Yamagata University

概要

次世代の学術情報ネットワークの高速化・低遅延・高信頼のため，その物理レイヤの構成を WDM 光パスネットワークとすることを念頭に，波長群パススイッチングの適用と波長資源の消費を抑えるためのリンク通過パス数の均一化が，ネットワークで必要となる波長数とノードスイッチ規模に与える影響を調査した．リンク通過パス数均一化は必要波長数を抑えるために有効である．波長群パススイッチングでは入力ポート数を低減できるが，リンク通過パス数均一化はその効果を劣化させることがないことがわかった．

キーワード

光クロスコネクト，波長群スイッチング，光パス，フォトニックネットワーク，波長資源

1. はじめに

一本の光ファイバ中に複数の異なる波長を多重する波長分割多重(WDM: Wavelength Division Multiplexing) 技術の進展により[1]，光ファイバ伝送の大容量化は著しく進歩した．その実用化により，学術情報ネットワーク SINET4 においても，アクセス回線として WDM 技術が用いられている[2].

光を用いた広帯域な情報伝送技術は，ポイント・トゥ・ポイントの伝送から，ROADM (Reconfigurable Optical Add/Drop Multiplexer)を用いるメトロ系の転送方式へと発展している．これは，光の波長を有効に利用し，電気処理を必要とせず，高速の伝送速度を保ったまま，柔軟なパス管理を可能としたものである．今後，複数のノードをメッシュ型に接続した形態にもこの考え方を適用する方向へ発展していくものと予想される[3]．すなわち，光方路の切替えに際し，電気処理によるルータの機能を光の波長を有効に利用してオフロードし，ノードにおけるボトルネックを解消するものである．

一方で, 日本の科学技術 10 ペタフロップス級の計算能

力を有する世界最高水準の京速コンピュータ「京」が開発され[4],「京」を中核として，計算機科学と計算科学分野の連携・融合を促す研究拠点の形成が求められている.「京」と全国の大学・研究所などに設置されている主要なスパコンをネットワークで結ぶ HPCI (High Performance Computing Infrastructure)の実現に向けた活動が進められており, そのネットワーク基盤としてSINET4が用いられている[5].

将来の計算機科学の進歩とネットワーク利用を考えれば，レイヤ２，３にとどまらず，物理レイヤも含めたボトルネック解消が必要となる. したがって, 次世代 HPCI のネットワーク基盤の設計では，光による転送技術まで踏み込んで考えることが有効である．このことは，学術情報ネットワーク利用上での，即時性の高いアップグレードやリンク・ノード障害もしくは災害時のセルフヒーリングのためのスペアリソース確保などにも有効であると考えられ，超高速・低遅延・高信頼な学術情報ネットワークの構築に役立つと思われる.

そこで本稿では，WDM を前提とした光パススイッチング技術を日本の学術情報コアネットワークに適用した場合を念頭に，波長数が増大した時に光方路切換え（光クロスコネクト）装置が大規模化する問題を解決するために，経路が一致する複数の波長パスをグループ化する波長群スイッチングを適用した効果について述べる．また，波長資源を節約するために，パスに対する経路の割当て方法として最短経路要請を緩和し，リンクを通過するパス数をネットワーク全体で均一化した経路割当てを行うことの効果について述べる.

波長群スイッチングについては，文献[6], [7]で報告があるが，扱っているネットワーク形態が東西南北に広がるメッシュ型である．本論文では，日本の学術情報ネットワークを前提に，ラダー型のネットワークについて検討を行っている．また，文献[6]ではリンク通過パス数均一化は行っていない．文献[7]では，リンク通過パス均一化は行っているが，その有無による違いについては検証されていない. 本論文では, この違いについても述べる.

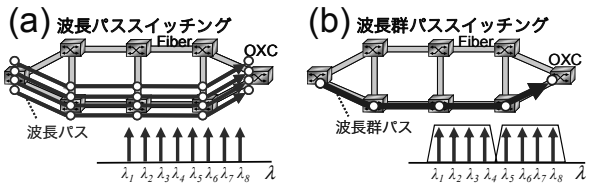


図 1. 波長および波長群スイッチング

第 2 章では，本論文で扱う前提となる技術について述べる．つまり，光クロスコネクト装置の構成およびその規模の評価方法について述べる．第 3 章では，パスに対する経路および波長割当て方法，およびリンク通過パス数の均一化方法について述べる．第 4 章では，本論文で評価した次世代学術情報ネットワークのネットワーク形態とリンク遅延について述べる．第 5 章では，ノード規模に対する評価結果と，ネットワークで必要となる波長数に関する結果を述べる．第 6 章はまとめである.

2. 波長，波長群パスと光クロスコネクト

2.1. 波長パスと光クロスコネクト

図 1(a)のように，光の波長をパスに割当て（以下，波長パスと呼ぶ), 光フィルタと光導波路による分合波器に基づいて方路を切り替える方法を波長スイッチングと言う．そのための光クロスコネクト(OXC : Optical Cross -Connect)装置の構成を図 2 に示す．光ファイバから出た光は波長分離器(DEMUX)により波長ごとに分離され, 波長単位で方路を切り替えられる．その後，波長合波器(MUX)により光ファイバ中に波長分割多重される．このように光の波長を利用して方路を切り替えることで，電気的な経路切り替えをなくすことができ，ノードにおける転送速度を向上することができる.

2.2. 波長群パスと階層型光クロスコネクト

光クロスコネクトでは，波長パスの数が増加すると OXC が大規模化し, 設備コストや消費電力の増加につながることが懸念される. OXC の規模を低減するため, 波長群スイッチングが検討されている．波長群スイッチングは，同一経路を通過する複数の波長パスを波長群パスにグループ化し，波長群単位で一括してスイッチングする．その概念図を図 1(b)に示す．図 1 における白丸がスイッチ素子を表しており，図 1(a)と(b)では，(b)の方がスイッチ素子の数を減らすことができることがわかる．これにより OXC を小規模化できる[6], [8], [9].

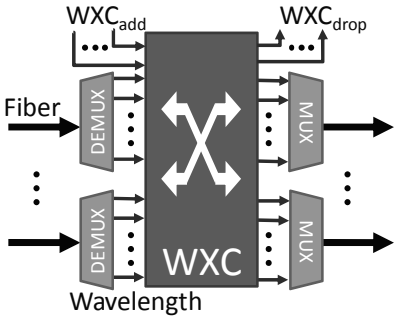


図 2. 光クロスコネクト(OXC)

波長群スイッチングでは，階層型光クロスコネクト(HOXC : Hierarchical OXC)を用いる．その構造を図 3 に示す[8]. 二つの階層からなり，ノード入出力光ファイバに近い階層は波長群スイッチングの機能を有し，BXC

（Waveband Cross-Connect）と呼ぶ．ここでは，波長群の合分波，波長群単位でのスイッチング，波長群 Add/Drop が行われる．波長パスの単位でスイッチングする機能は図 3 の上部であり，WXC（Wavelength Cross-Connect）と呼ぶ．ここでは，波長群から波長への分波とその逆の機能，波長単位でのスイッチング，波長 Add/Drop が行われる．より多くの波長パスを波長群として BXC でスイッチングできれば，OXC の規模を削減できる．

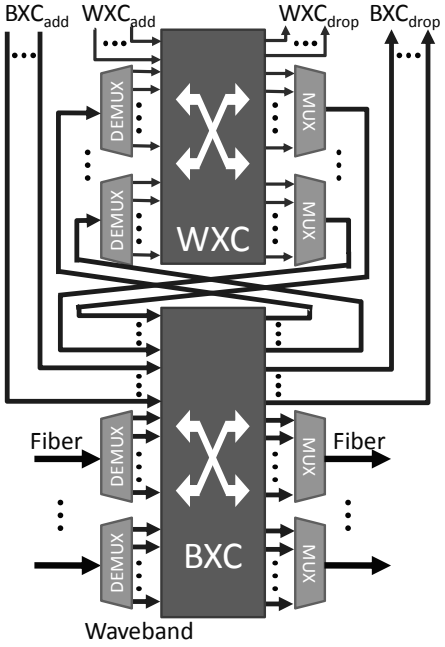


図 3．階層型光クロスコネクト（HOXC）

表 1．OXC 入力ポート数算出のためのパラメータ

記号	パラメータ
F	入力ファイバ数
B	ファイバ中の波長群数
N	波長群中の波長数
W	ファイバ中の波長数 (=BN)
y_{UP}	WXCからBXCへ送出される波長群数
y_{DOWN}	BXCからWXCへ送出される波長群数
x_{ADD}	WXCのAddポート数
x'_{ADD}	BXCのDropポート数

2.3. 光クロスコネクトの入力ポート数

OXC および HOXC の規模は, 重要な評価指標である．それらを定量的に評価するには，与えられたトラヒックパスに対して必要となる OXC および HOXC の入力ポート数を調べればよい．

BXC，WXC および HOXC の入力ポート数をそれぞれ P_{BXC}，P_{WXC}，P_{HOXC} と書くことにすると，スイッチとして分配選択型を仮定すれば，それらは以下の式で計算できる[10], [11]．すなわち，

$$P_{BXC} = FB + y_{UP} + x'_{ADD} \quad (1)$$

$$P_{WXC} = Ny_{DOWN} + x_{ADD} \quad (2)$$

$$P_{HOXC} = P_{BXC} + P_{WXC} \quad (3)$$

式中のパラメータの意味は，表 1 に記載した．

比較のために，波長群へのグループ化を行わない場合のクロスコネクト規模も以下のように計算する．想定するクロスコネクト（COXC: Conventional OXC）は図 2 のように WXC のみであり，方路光ファイバが直接 WXC に接続される．その入力ポート数 P_{COXC} は，

$$P_{COXC} = FW + x_{ADD} \quad (4)$$

で評価する．

3. 経路，グループ化，波長の設定方法

3.1. パスに対する経路および波長割り当て

光パス(波長パス・波長群パス)スイッチングネットワークでは，経路，波長，波長群グループ化について，その設定方法を決める必要がある．それらの方法は，パスの遅延時間，ネットワークで必要になる波長数，ノードの規模などにより評価される．

一般に経路設定に関しては，最短経路を割り当てるのが通例と思われる．それは，（1）通信における遅延を抑える，（2）経路のホップ数をできるだけ小さくしてスイッチポート数を減らす，という考え方に基づく[7]．波長群スイッチングでは，パスのグループ化によりスイッチポート数を削減できる．したがって，最短経路を選ぶ必要性の一つか緩和できると考えられる．

一方で，波長パスおよび波長群パススイッチングネットワークでは，波長数の増加はリンクのコストが上昇するために好ましくない．そのため，ネットワークで必要となる波長数が経路設定の目的関数になることがある．必要波長数を減らすには，特定のリンクに通過パスが集中するのを避けることが重要で，ある程度の遅延を犠牲にし，リンクの通過パス数を均一化する方法が有効である[12].

波長群へのグループ化は，経路が同一であるパス数が多いほどグループ化できるパス数が増え，スイッチポート数を低減する効果をもたらす．その一方で，リンクの通過パス数を均一化することは，ホップ数の増加をもたらし，スイッチ規模削減の妨げとなりうる．

このようなことから，本論文では，波長パススイッチングと波長群パススイッチングの両方の場合について，リンクの通過パス数を均一化する処理の有無が，ネットワークに必要となる波長数とノード規模(スイッチポート数)に及ぼす効果について数値計算により検証する．

経路，波長および波長群の設定のための全体のフローチャートを図 4 に示す. 大きく 3 つのステップからなる．

Step 1 では，与えられた要求トラヒックのパス（ソース・デスティネーションの対）に対して，Dijkstra アルゴリズム[13]により最短経路探索を行う(Step 1-1)．その結果に基づき，ネットワークの各リンクを通過するパス数が均一になるような経路変更処理を行う(Step 1-2)．この処理を施すことで，リンクで使用する波長数がほぼ同じになる[12]．本論文では，Step 1-2 の有無によるクロスコネクト規模削減効果の影響と，ネットワークに必要となる波長数への影響を調査する．この処理の詳細については，次の節で詳説する．

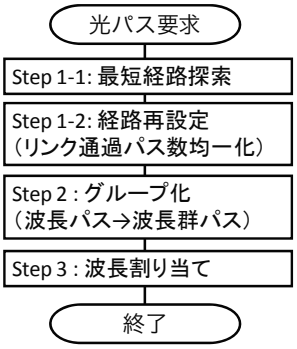


図 4．経路，波長，波長群グループ化のフローチャート

Step 2 は，波長パスを波長群パスにグループ化するために，全てのパスの経路を比較し，経路の一致する複数のパスをグループ化する．その際に，できるだけ長い経路が一致するパス同士をグループ化する．グループ化の方法として，経路の一部が一致しているパスをグループ化する Subpath grouping を用いた[14]．Subpath grouping はグループ化の対象となるパス数が比較的多くできる方法である．本報告中では波長群の大きさに関して，一つの波長群パスに含まれる波長パスを波長群容量 N とし，今回は 5 とした．同一経路の波長パスの数が N に満たないときにはグループせず，それらのパスは波長単位でスイッチングするものとした．

Step 3 で波長を割り当てる．波長割り当ては First-Fit により行った[15]．図 5 のように，まず波長群パスの波長割当てを行い，その後，波長パスの波長を割り当てる．波長群パスの波長配置は，できるだけ連続するように配置されることとした．また，なお，リンクの上りと下りで同一波長を使用できないものとした．1 つのパスデマンドに 1 つの波長を割り当てるものとし，ノードに波長変換を用いないことを仮定した．

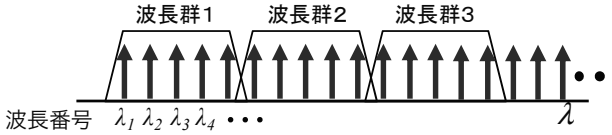


図 5．リンクの波長配置の一例

3.2. リンクの通過パス数均一化

本節では Step 1-2 について詳述する．まず，全てのリンクに対して，通過するパス数を調査する．その結果，通過するパス数が最も大きなリンクをマキシマムリンク(以下，ML と表記)とする．もし，ML が複数ある場合には，リンク番号が小さいリンクを ML とする．ML に対して，ML を通過するパスの中で遅延時間の長いパスを経路再設定パス（リルーティングパス）とする． リルーティングパスの経路を再設定するために，ML をないものとして考えてリルーティングパスについて Dijkstra アルゴリズムを適用し，ML を通過しない最短経路探索を行い，その経路に再設定する．この処理を，ML を通過するパス数が変化しなくなるまで繰り返す．以上の処理をフローチャートにしたものを図 6 に示す．

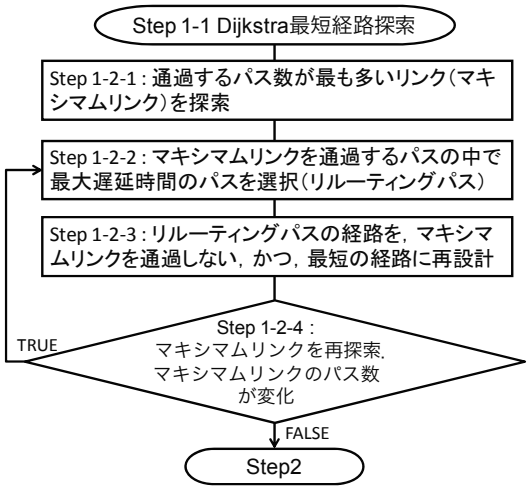


図 6．リンクの通過パス数均一化処理

4. ノード配置およびリンクの構成

図 7 は，本稿でのシミュレーションに用いたネットワークである．8 ノード，13 リンクからなる．リンクの接続形態は，SINET4 の接続形態を次世代光パスネットワークに拡張したと考えた．具体的には，SINET4 のコアノード配置都市に光クロスコネクトを配置し，SINET4 のリンクを WDM 光ファイバリンクとした．各リンクの遅延時間は，ノード間の地理的な距離と光の速度から見積もり，各リンクの遅延時間は付録に表 A1 として記した．リンク番号を i とし，リンクの遅延時間 t_i の具体的な計算方法は，以下の式に基づく．すなわち，

$$t_i = n L_i / c \qquad (5)$$

ここで，n は単一モード光ファイバの伝搬モード屈折率，c は真空中の光速，L_i はリンク i 両端ノード間を結ぶ地理的直線距離である．

図7. ノードとリンクの構成

5. 計算結果

本稿では，トラヒックとして複数のデマンドパスをランダムに与え, その量に対する HOXC 規模ならびにネットワークで必要となる波長数を評価する.

全パス数をネットワークのノードの組み合わせ数で除した値をトラヒック負荷と定義し，トラヒック量の指標とした．これは，1 つの送受信ノード対あたりのデマンドパス数の平均の意味を持つ．計算では，トラヒック負荷が 1 から 10 まで, トラヒック負荷 1 ずつ増加させて評価した.

HOXC 規模の評価は，ネットワークの各ノードに HOXC を配置したと仮定して，デマンドパスを実現するために必要となる HOXC 入力ポート総数を計算することよって行った．必要波長数は，デマンドパスを実現するためネットワーク全体で必要となる波長数で評価した.

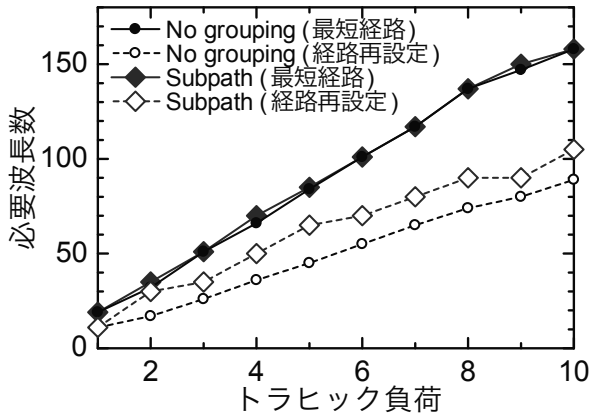


図8. トラヒック負荷に対する必要波長数

必要波長数のトラヒック負荷に対する結果を図 8 に示す．経路設定時に，Dijkstra アルゴリズムに基づく最短の経路設定した場合を「最短経路」と表記した．この場合，図 4 の Step 1-2 の処理は行わない．最短経路の状態に対し，リンクを通過するパス数を均一化するよう経路の再設定(Step 1-2)を施したケースを「経路再設定」と表記した．また，経路の一部が同一の波長パスを波長群へグループ化したものを「Subpath」と表記し，比較のため，グループ化を施さないケースを「No grouping」とした.

波長群パススイッチングを用いないとき(No grouping)では，最短経路の場合よりも経路再設定の場合の方が，必要波長数を少なくできる．波長パススイッチングを用いるとき(Subpath)も同様に，最短経路の場合よりも経路再設定の場合の方が，必要波長数を少なくできる．つまり，リンク通過パス数の均一化は，ネットワークで必要となる波長数を少なくできることがわかる．必要波長数低減の効果は，波長群パススイッチングリンクを用いるときの方が，そうでない時よりも弱いことがわかる．これは，波長群パスを用いるために，リンクによっては波長が連続的に配置されず，一部に使われない波長のあるリンクが存在することに起因する．この増加は，最短経路の場合を下回っていることから，リンク通過パス数均一化による必要波長数低減の効果を損なうほどのものではないことがわかる.

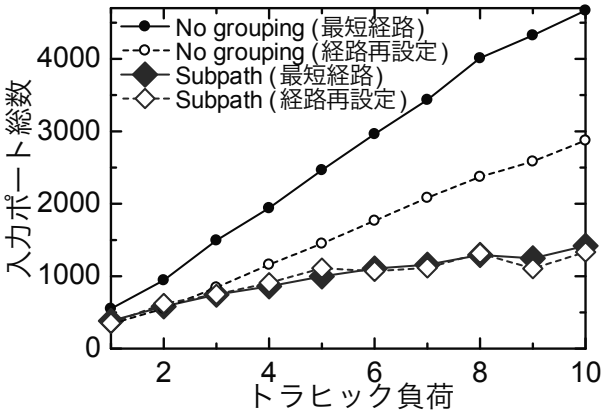


図9. トラヒック負荷に対する HOXC 入力ポート総数

HOXC 入力ポート総数のトラヒック負荷に対する変化を図 9 に示す．まず，波長群へのグループ化をしないとき(No grouping)では，経路再設定の場合は，最短経路選択の場合に比して入力ポート総数が小さくなる．この効果は，図 8 の結果で述べた波長数の低減に起因すると考えてよい．具体的には，式(4)の W が減少する．次に，No grouping と Subpath を比較する．最短経路の場合も，経路再設定の場合も，波長群パススイッチングを用いることにより, 入力ポート総数を低減できることがわかる．波長群へのグループ化した場合(Subpath)については，経路再設定の有無によらず，ほぼ同等の入力ポート数となっている．このようにほぼ同一の特性となることは，ネットワークのノード数を増やしたケースで計算した場合

にも得られた．つまり，必要波長数を減じるためのリンク通過パス数均一化が，波長群によるスイッチ規模の低減効果に悪い影響を及ぼさないことがわかる．最短経路の場合，ML を通過するパス数が低減されていないことから，波長群を用いることによりグループ化が進み，入力ポート数が減少する．他方，経路再設定の場合，グループ化は比較的少なくなるが，図 8 の波長数低減の効果により入力ポート数が減少する．それでも，経路再設定をする場合には，ホップ数が増加すれば入力ポート数が増加してしまうと考えられる．しかし，図 9 の結果を見ると，最短経路で波長群を用いる場合とほぼ同一の特性となる．このことは，リンク通過パス数の均一化によって, ほとんどホップ数が増加していないことを意味する．北米を模擬したネットワークトポロジーなど，東西南北に広がるメッシュ型の場合には，経路再設定によって，著しくホップ数が増加し，入力ポート数が増加する場合があろうと思われる．しかし，日本の学術情報ネットワークのコアノードを接続する形態で，最短経路をベースにした経路再設定では大きく迂回する経路とならず，著しくホップ数が増えることがないと考えられる. SINET4 の接続構造が，障害に対して堅牢となるような 5 ループ構造であることがこの効果をもたらしていると考えることができる．

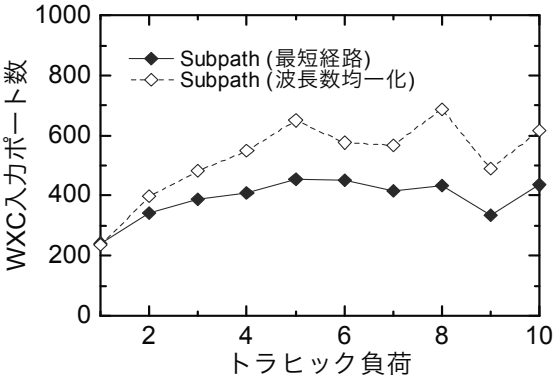


図 10．トラヒック負荷に対する WXC 入力ポート総数

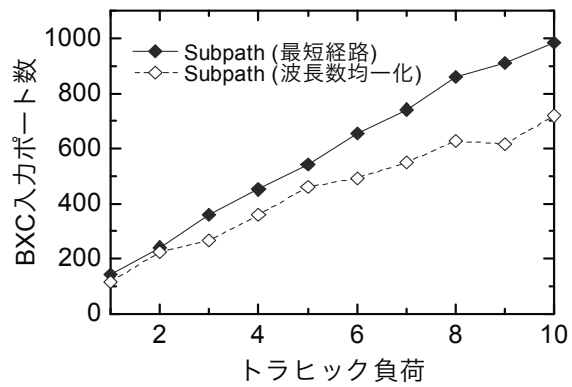


図 11．トラヒック負荷に対する BXC 入力ポート総数

HOXC 入力ポート数は，式(3)に示すように，WXC と BXC のポート数の和である．波長群パススイッチング (Subpath) の場合，図 9 に示したように，入力ポート総数は最短経路と経路再設定でほぼ同一であったが，その WXC と BXC の内訳を調査した．トラヒック負荷に対する WXC ポート総数および BXC ポート総数をそれぞれ図 10，図 11 に示す．

最短経路では，同じソース・デスティネーションとなる波長パスは全て同じ経路を通過するため，グループ化されやすく，トラヒック負荷に対して WXC ポート数の増加を抑制できる. 今回, 波長群容量 N が 5 であるため，トラヒック負荷が 5 以上でその傾向が顕著である．

経路再設定では，リンク通過波長数均一化により，最短経路設定で同一経路を通過していた光パスの経路が変更されるため，同一経路の光パス数は減少し，波長群パスにグループ化できる波長パス数が減少し，式(2)における BXC から WXC へ送出される波長群数 y_{DOWN} が増加し，トラヒック負荷に対して WXC 入力ポート数はさほど抑制されない．しかし，リンク通過波長数均一化より必要波長数が減少するため，式(1)におけるファイバ中の波長群数 B が減少し，BXC 入力ポート数が減少する．

6. まとめ

次世代の日本学術情報ネットワークの高速化・低遅延・高信頼のため，その物理レイヤの構成を WDM 光パスネットワークとすることを念頭に，波長群パススイッチングの適用と波長資源の消費を抑えるためのリンク通過パス数の均一化が，ネットワークで必要となる波長数とノードスイッチ規模に与える影響を調査した．リンク通過パス数均一化は必要波長数を抑えるために有効である．波長群パススイッチングでは入力ポート数を低減できるが，リンク通過パス数均一化はその効果を劣化させることがないことがわかった．これらの結果は，日本の大都市を結ぶネットワーク形態と，最短経路をベースにリンク通過パス数均一化の経路再設定を行うことに由来すると考えられる．

謝辞

本研究の一部は科研費（24246066）の支援を受けた．

参考文献

[1] C. A. Brackett: Dense wavelength division multi -plexing networks: principles and applications, IEEE Journal on Selected Areas in Communications, vol. 8,

no. 6, pp. 948-964 (1990).
[2] http://www.sinet.ad.jp/
[3] 佐藤健一，古賀正文: 広帯域光ネットワーキング技術，コロナ社 (2003).
[4] http://www.aics.riken.jp/
[5] http://www.hpci-office.jp/
[6] 山涌純，高田篤，今宿亙，長津尚英，盛岡敏夫: 波長群ルーチング NW の設備量評価と一括波長変換デバイスについての一検討，信学技報，CS，vol. 102，no. 102，pp. 11-16 (2002).
[7] 廣田悠介，本多弘明，戸出英樹，村上孝三: 光波長群ネットワークにおけるパスグループ化に適した経路設計手法の提案，信学技報，PN2004-36, pp. 13-18 (2004).
[8] 梯昌二，長谷川浩，佐藤健一: 多階層光パスネットワークノードの研究，信学技報，PN，vol. 106, no. 419，pp. 9-12 (2006).
[9] 高橋耐志，原井洋明，小関健: 波長変換を用いた階層型光パスネットワークの装置コスト最小構成，信学技報，OCS，vol. 103，no. 108，pp. 45-50 (2003).
[10] 吉田英二，高橋哲夫，河合武司，狩野文良: フォトニックMPLSルータを実現する波長ルーチング技術，NTT R&D，vol. 50，no. 10，pp. 750-757 (2001).
[11] 三木哲也，須藤昭一: 光通信技術ハンドブック，オプトロニクス社 (2002).
[12] Ardian Greca, Tatsuhiro Kato, Kiyoshi Nakagawa, and Mohd Fadzly: Provisioning Algorithm for Survivable WDM Optical Path Networks, Proc. of the Fifth Optoelectrnics and Communications Conference (OECC2000), 12P-25, pp.236-237 (2000).
[13] 片山直登: ネットワーク設計問題，朝倉書店，(2008).
[14] X. Cao, V. Anand, and C. Qiao: Waveband Switching in Optical Networks, IEEE Commun. Mag., vol. 41, no. 4, pp. 105-112 (2003).
[15] H. Zang, J. P. Jue, B. Mukherjee: A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks, Optical networks magazine, vol. 1, no. 1, pp. 47-60 (2000).

付録

表 A1．リンクの遅延時間

Link number	Node number		Delay time [ms]
1	1	2	2.7
2	1	3	4.2
3	2	3	1.5
4	2	4	2.1
5	3	4	1.4
6	3	5	1.3
7	3	6	2.0
8	4	6	1.2
9	4	7	2.3
10	5	6	0.7
11	6	7	1.4
12	6	8	2.4
13	7	8	1.0

複数認証基盤に対応する複合 SSO 環境でのユーザエクスペリエンス

Proposing User Experience based on WEB-SSO with Multiple Backends of Authentication/Authorization Engine

松浦健二†，上田哲史†，佐野雅彦†
Kenji Matsuura†, Tetsushi Ueta†, Masahiko Sano†

ma2@tokushima-u.ac.jp, ueta@tokushima-u.ac.jp, sano@tokushima-u.ac.jp

†徳島大学情報化推進センター

† Center for Administration of Information Technology, The University of Tokushima

概要

個人の ID が複数存在する場合の個人認証には，単一の認証源に登録されている場合だけでなく，複数の異なる内容での認証源に登録されている事もある．これをシングルサインオンのバックエンド情報源として利用する際には，その特性や扱う属性に注意しながら慎重に実装しなければならない．これらはセキュリティを考慮しつつ利便性および耐障害性を高めるための設計方針および運用方針を要し，本論文では本学での実装について述べる．さらに，異なるシングルサインオン技術を用いた異なるカテゴリでの統合的な操作環境について述べる．

キーワード

WEB-SSO, Shibboleth, Kerberos, ADFS

1. はじめに

組織内外で利用される個人の識別子（ID）は，その発行主体および運用方針に依存して，同一サービスに対する同一個人においてでさえ複数存在する事がある．大学等高等教育機関における本事象の要因として，例えば，下部組織が独立して臨時職員等を雇用するケースや，ID の発行主体となるシステムあるいは組織内下部組織の運用が独立しているケースなど幾つかのパターンがある．これらは，名寄せの問題やその応用となる生涯 ID 問題として研究される事がある．例えば，名古屋大学では，名古屋大学 ID として一貫性のある生涯 ID の設計がなされている[1]．生涯 ID の導入は，かなり長期間に渡る設計思想を必要とし，この長期間に外部組織による ID 発行・管理機関の登場など，多くの不確定要素もある．ただし，こうした長期間に渡り適用可能なスケーラビリティを要する設計思想自体は，組織のユーザ管理，中でも大学のような人の入れ替わりに特徴を有する組織での管理方針に，重要な示唆を与えうる．

ここで，一度整備・普及している ID の変更は大きな運用上のコストとリスクを伴うが，生涯 ID の導入に限らず，ID 運用方針の変更などを契機に，再整理されることもある．こうした場合には，重複期間なく新 ID に切り替える立場と，重複期間を設けた上でユーザへの説明

を重ねながら移行する立場もとれる．

ユーザ管理の方針が固まれば，その方針の下で ID 利用・運用する個人認証サービスが導入される事が一般的である．個人認証サービスの応用となるフロントエンドのアプリケーション個々の活用のされ方や，運用支援によって，ユーザの利用頻度やサービスの技術的な構成も変化する．大阪大学では，統合認証基盤を構築し，様々なアプリケーションに適用することでユーザの利便性向上が図られている[2]．さらには，統合認証基盤をバックエンドとする組織内外でのシングルサインオン環境も整えられている[3]．一旦シングルサインオン環境が整備されると，組織内のアプリケーション開発はこの基盤を用いて容易に実現できるようになる[4]．

国立情報学研究所を中心とする「学認」等の組織を跨ぐシングルサインオンでは，とりわけ個人情報の扱いに注意を要し，技術的あるいは運用上の様々な工夫を要する．一方で，単体組織内のシングルサインオンにおいても，パブリックなクラウドサービス[5]をシステムの系に採り入れることも多くなり，組織内の合意形成や運用的な対応は基より，技術的な対応も必要となる．さらには，統合認証基盤の利用とシングルサインオン環境の下では，認可制御方針を決めた上で，適切にそれを実装することが求められる．例えば，A 学部における教授会資料へのアクセスについてはその学部の教授に限定という要件もあれば，同じ大学内でも B 学部における教授会資料へのアクセスには，B 学部の教員(教授以外含む)全てに許可される要件もある．こうした様々な認可要件に対する柔軟性のある選択および実装が求められる．また，これらを実現するシングルサインオンの技術自体も，適用可能範囲や適性があるため，技術的に統一する方針にするか，適材適所で適応させるかは組織の意思決定に依存する．

こうした設計思想を背景に，ユーザ側の利便性をいかに高めて提供できるかは，近年ユーザエクスペリエンスとして議論されている[6]．ユーザエクスペリエンスという言葉自体は，近年のスマートフォンやタブレット等でのマルチタッチ操作などを含む様々な文脈で用いられるが，本論文ではシンプルに，従来よりも相対的に利便性の高い操作全般として捉えている．

徳島大学では，以上の議論の下，ユーザ ID を見直して構築し，これに伴う複数種のバックエンド認証基盤を運用することとなった．さらには，端末認証を活用した複数種のシングルサインオン技術を導入した操作環境も設計した．具体的には，ADFS と Shibboleth に加え，Kerberos を利用したシームレスな操作環境の構築である．これにより，教育環境を利用する学内構成員へのログインサービスとして高い利便性をもったサービス提供が可能となった．本稿では，この設計思想および，運用後の利用状況から得られる動向について述べる．

2. ID 運用の見直し

2.1. 体制上，技術上の従来の問題

組織内で全学的な認証基盤が構築される以前から開発・運用されてきた単独の学内全学向けアプリケーションサービスがある場合には，そのサービス側でユーザ情報をローカルに持つ方式で開発されることが多かった[7]．したがって，認証基盤への要望が後から高まった際には，このような利用頻度の高い全学アプリケーションサービスのユーザ情報を基にした認証基盤を構築する方が効率的であった．その場合には，ID 体系のスケーラビリティに依存して，ユーザ視点および管理者視点双方からの利便性の問題，あるいは ID ライフサイクルの問題が運用途中で出てくる事もある．

一方，現在多くの大学では，情報センター系組織等が主体となって，ID プロビジョニングの仕組みを検討し，基盤化してから外部サービスがそれを使うように設計するアプローチが多数見られる．認証基盤を大学全体で構築することは，利便性を高めるだけでなく，セキュリティ水準を全学的に一定以上に担保する上でも重要である．本学では，教職員については前者の経緯に基づく実装が人事課の業務フローと連動した形で確立されてきた．一方で，学生については後者のような認証基盤が学務課の業務フローを系に含む形で実装されてきた．すなわち，技術的な ID 発行・管理主体も異なるが，その業務フローに介在する人的な組織も独立していた．

これら異なる事務所掌組織に対して，ネットワークシステムで利用する ID の管理運用主体も統一化されずに運用されてきた．このため，二つの認証基盤を教職員向け，学生向けといった形でデータ分離し，一方で両者を扱う WEB サービスのためには，それらをプロクシする認証中継サービスを導入する形で，かろうじて認証基盤として統一的に見せていた．

この形で運用上生じる問題は，ID の発行主体が組織として複数存在し，運用方針もそれぞれに独立依存する形であるが故の煩雑さがある．パスワードや個人証明書等による認証基盤としてだけ考えれば，このような複数認証基盤であっても大きな問題とはならないが，ライフサイクルのずれを鑑みた場合には運用の手間が顕在化する．さらには，ユーザの属性情報を含めた認可制御を考慮すれば，異なる認証基盤で異なるスキーマによる属性運用では管理上の困難も生じる．

2.2. 統合化と並行期間の運用

徳島大学では，コンピュータシステム更新の契機に，

教職員も学生と同一の認証基盤に乗せることで，前節の問題を改めて解消することとした．両既存基盤とは独立して全く新しい認証基盤を構築するよりも，いずれかにまとめた方が既存のフロントエンドサービスへの影響が少なく，かつ設計上も容易になるためである．ここでは教職員の方が学生と比較して少数であり，かつ連絡が行き渡りやすい事から，教職員側を寄せる方針とした．

認証基盤の統合化に際し，ID 設計上の体系および運用が異なるため，サーバサイドでの ID を移行する事も検討したが，技術的および運用的に困難であった．そこで，一時的にユーザへの負担をかけることとはなるが，新しく ID を追加付与するという形をとることとした．他大学等でも ID 再構成の際には，追加という形が見られ，一定の実績も上がっている．なお，従来はユーザのマスタデータをそれぞれ異なる部署が所掌する形で，それに連動して独立した ID 管理体制であったが，本方式実現のためにオンラインでのプロビジョニング／デプロビジョニングを実現した．これは，他大学でのユーザ管理データベースと同様である[8].

この実現には，構成員に対して重ねてアナウンスを行い，周知広報活動を何度も展開した上で，当面の間並行利用することとした．すなわち，並行利用する間の利用動向を調査しながら，方針を柔軟に決めていけることになる．このような方針を採用する際には，重複 ID がこれら新旧の認証基盤には存在しない事が重要である．

3. シングルサインオン設計

3.1. SSO サービス

本節では，前述の認証基盤を利用したシングルサインオンについて述べる．これは，個人認証で最も利用されているパスワードなどの流通経路を隘路にすることで，セキュリティ上のリスク軽減を実現し，なおかつ認証操作の頻度を減少させる効果がある．

インターネット上には，OpenID 等の多用な技術が開発されているが，組織内で用いられるシングルサインオン技術として多用される主なものには，ADFS や Shibboleth といった SAML 対応のソリューションや，Kerberos など多種存在する．SAML や Kerberos はその特徴や，対応システムが異なる事が多い．そのため，いずれかを選択利用するという形では，対応できないアプリケーションも出てくる懸念がある．

徳島大学では，2007 年頃から分散 SNS を対象とした Shibboleth の拡張について研究を行っていた[9]．2010 年には，全学的な SSO 実現のための基盤技術として Shibboleth の採用が決まり，各種の SSO 対応 WEB サービスは Shibboleth へ，という流れが構成された．

2012 年 4 月の時点では，Shibboleth を用いた WEB-SSO として，下記のようなサービスが導入されている．また，内製の出席管理システムや WebDAV，ネットワーク監視などこの他にも同じ SSO に参加しようと幾つか計画段階のものもある．なお，下記に列挙しているサービスは元々 SAML 対応しているものもあるが，本学向けに Shibboleth 対応したものも含まれる．

- 全学統合ポータル（パブリックサービス）
- LMS（パッケージ）
- LMS（Moodle）
- ネットワーク利用申請（独自開発）
- ソフトウェアダウンローダ（独自開発）
- グループウェア（OSS カスタマイズ）
- 図書館システム（パッケージカスタマイズ）

3.2. WEB-SSO の認証連携拡張

前節で挙げた各種の WEB サービスは，アプリケーションサービスであり，個々に個人認証を経て，個人に依存したコンテンツを提供する．ここで，個人認証は，アクセスしているユーザが本人である事を確認するのが本質であり，その点からはアプリケーションサービスに限った要件ではない．例えば，個人認証を要する対象には，こうしたサービスの他，オペレーティングシステムやネットワークも含まれる．これらは適用場面の違いであり，個人認証そのものの本質は等しいと考える．このような適用場面を超えた SSO の枠組みも研究されており，例えばネットワーク認証を行うゲートウェイに Shibboleth を導入する研究がある[10].

個人認証の方式に関する運用方針は，それぞれの組織の実装に適した方式を検討すべきである．例えば，徳島大学では，ネットワークの一時利用（VPN や無線 LAN）を行うためのパスワード認証については，オンデマンドで必要に応じて発生するものとの判断があり，認証基盤を直接利用する対象とはしていない．一方で例えば，Windows ドメインへの参加については，学内のほとんどの構成員が教育場面や業務場面において，必須利用する．さらにはアプリケーションサービスも業務利用するものが多いことから，これらは透過的なサービスと考える．こうしたサービスには，Windows ドメインログインを以て，上位のアプリケーションサービスへも SSO できる環境の設計を行った．

ここで，Windows のドメインサーバは，ActiveDirectory で構成される．ドメイン参加によって Kerberos が利用できるようになる．Kerberos は各種の OS でサポートされ，ブラウザがそれを利用できるものもある．例えば，Windows 上の InternetExplorer や Firefox が対応している．

徳島大学の教育用コンピュータシステムは，2012 年度以降ネットブートを導入しており，これらブラウザの設定もイメージ更新時に簡単に設定できる．

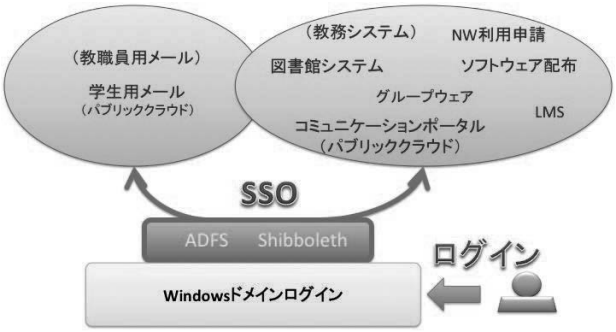


図 1　アプリケーションとドメインログイン

徳島大学において数年来運用している Shibboleth では，Kerberos ハンドラを導入することも可能である．そこで，上述の環境を実現すべく，Shibboleth と Kerberos を組み合わせて，ドメイン参加によるアプリケーションサービスへの SSO を実現する．なお，学生用の Exchange Online を利用したメールサービスは，同様にドメイン参加によるアプリケーションへの SSO が実現可能である．つまり，OS 認証によってアプリケーションログイン時には，ID やパスワードの入力は行わない．これには Shibboleth ではなく，SAML に対応した ADFS が利用されている．したがって，徳島大学では，Shibboleth，ADFS，Kerberos が混在しながらも，Windows ドメインへのログインを以て，上位の WEB アプリケーションサービスへの SSO が実現できることとなる（図１参照）．この場合，いずれを利用した場合にも，再度の認証は要求されず，透過的に各種のサービスを利用できることなる．すなわち，エンドユーザの視点からは ADFS グループや Shibboleth グループといった区分けのないシームレス環境となる．

3.3. アクセス元から見たサービス

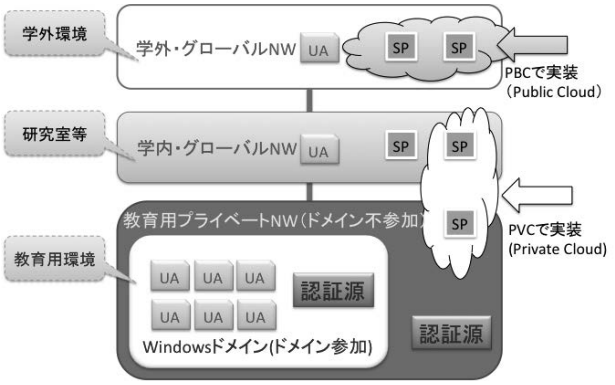


図 2 ネットワーク構造とサービス展開

前述の Kerberos を用いる場合には，図２におけるネットワーク構造のうち，左下部にある Windows ドメイン参加端末が対象となり，ドメイン参加していないコンピュータからは機能しない．図中の一般研究室や学外から本学のサービスを利用する際には，Kerberos を用いない Shibboleth 利用となるため，これら両要件に対応する設計・構築が必要である．補足として，図２中の UA は User Agent（＝ブラウザ）の略であり，SP は Service Provider（＝アプリケーションサービス）の略である．

4. システム構築

4.1. 複数種認証源への対応

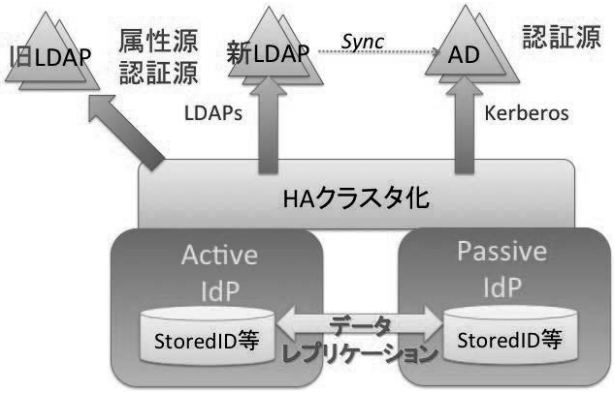


図 3　複数種バックエンドでの IdP 冗長化構成

前章までに述べた用件を実装するに際し，本章では特に Shibboleth の構成を具体的に述べる．図３は，Shibboleth における認証源へのユーザインタフェースを提供する部分（IdP，Identity Provider と呼ぶ）の構成である．徳島大学では，システムのクラスタ化による冗長性確保には，Active-Standby での構成をとって耐障害性を高めている．なお，サーバ自体は 64bit アーキテクチャで十分なメモリを割り当て，ディスクは RAID0+1 で構成している．認証源・属性源および IdP の各サーバは全て耐震固定のラック搭載で UPS が稼働し，これらを保管する部屋の入退室管理は電子錠で自動記録されている．なお，ネットワークアクセスに際しては，アクセス元や接続ポートの制限等だけでなく，運用上は，Nagios を利用した外部からの定期監視・自動通知とホスト内部のログの常時監視・自動通知の両方でセキュリティを高めている．

IdP には，StoredID（SP 毎に異なる ID 生成する機能）やその他の実装のために，内部にデータベース（RDB）を有している．この RDB は，上記のクラスタを実装するためにマルチマスタ構成をとり，Active 系が切り替わってもデータの保存としてはレプリケーションされる．

ここで，２章で述べた複数種バックエンド認証源・属性源への対応実装について述べる．前提として，IdP に

限らず，重要なサーバは物理・論理を問わず冗長化構成をしている．したがって，IdP から見たバックエンドとしては全てフェイルオーバ対応となる．認証源の選択としては，Windows ドメイン参加している場合には，再度のエンドユーザがパスワード入力して認証される必要はない．しかし，そうでない場合には，教職員，学生といった構成員全員のアカウントを有する新しい LDAP，またはそれとは重複のない旧来のアカウントを有する LDAP の二種類をそれぞれ認証源，属性源として登録する．この際，新しい統合 LDAP の方を優先するよう，順番は先に設定しておく．なお，これら新旧の LDAP には，主に下記の点で相違がある．

・バインド方式
・DIT 構造の違い（uid 生成則，DN 等）
・属性数，属性名（オプション含む）および属性値

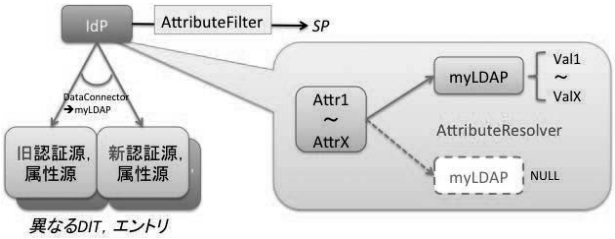


図 4　属性取得の仕組み

ShibbolethIdP では，認証を行った後，属性取得機能には新旧双方を設定する．この実装は AttributeResolver にて行われ，その中で属性定義する際に択一となるよう実装する（図 4 参照）．ここで，属性取得時は，前述のように属性名も異なる場合がある．そのような属性に対しては，単純に複数 LDAP への接続を設定するだけでは動作しない．そこで，徳島大学の実装においては，それぞれに保存される属性を Simple 型で一旦ダミー取得してからそれらを Script 型で属性選択する方式とする．属性取得が択一となるため，Script 中で例外処理を書いておかねばならない．具体的には，属性取得時はプロクシバインドしての検索となるが，これには設定ファイルに記載された順に試される．このため，最初のコネクタで検索失敗した場合には，例外が吐かれて以降の処理が停止するため，例外処理を書いて回避する．また，認証時に Kerberos ハンドラが選ばれているクライアントに対しては，属性検索時のフィルタにセットする値がパスワード認証とは異なる事になり，それぞれ適切に設定する．

4.2. 複数 SSO 技術のシームレス利用

Shibboleth における利用頻度の高いハンドラは，UsernamePassword ハンドラ，つまりバックエンドの認証源に対して，WEB を通じてクライアントから渡されるパスワード照合方法であろう．この時，ドメインログインを含めた処理概要を図 5 に示す．エンドユーザは，ドメインログインは OS 上のドメインログインであり，ブラウザ上での Shibboleth の世界はそれとは独立したものとして，機能的にもインタフェース的にも独立動作する．このため，図中の両領域間は，ユーザ視点においても SSO として機能しない．

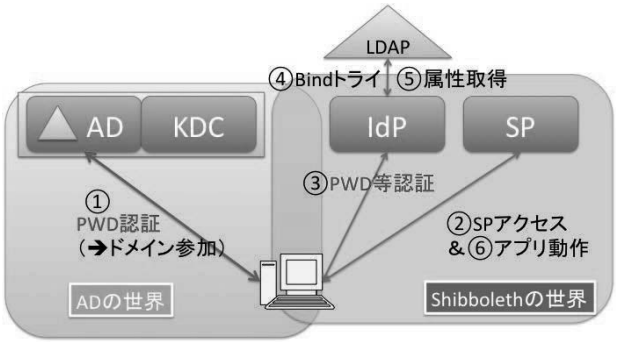


図 5　パスワード利用時の処理概要

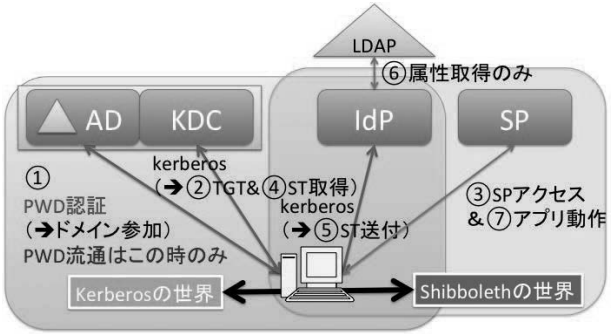


図 6　Kerberos 利用時の処理概要

徳島大学の実装においては，ドメイン参加時には，図 6 のような Kerberos ハンドラを選択できる．Kerberos ハンドラは，ShibbolethIdP を Kerberos の一つのアプリケーションサービスと位置づけることと見なせる．つまり，Kerberos ハンドラは，クライアントから渡されるサービスチケットの検証によって図中の KDC が認めたクライアントと見なす．図 5 と異なり，Windows ドメインの世界と Shibboleth の世界のオーバラップ領域が増え，エンドユーザが入力するパスワードの流通頻度は減少する．一旦 Kerberos のサービスとしての ShibbolethIdP で認証されれば，ShibbolethSP に SSO できることになる．

図 5 および図 6 は，それぞれ異なるハンドラでの実装となる．しかし，ユーザインタフェースとしては，同一の画面内で，エンドユーザのオペレーションによって使われるハンドラを変更するように実装している．具体的には，図 7 のインタフェース上の，画面下部のスニペッツが Kerberos ハンドラ用となり，パスワード入力を行わせる部分は UsernamePassword ハンドラとなる．これらにさらに，個人証明書による認証方式として RemoteUser ハンドラを加えたりすることも技術的には可能である．

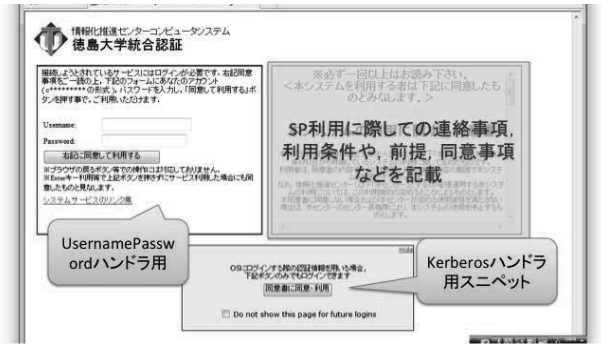


図 7　ログイン時の複数ハンドラの実装

Kerberos ハンドラの実装によっては，図 7 のようなユーザインタフェースを介さなくともよい．しかし，徳島大学での実装上は，隘路となる IdP の画面上で表示させたい同意事項やその他必要に応じて提示したい情報を一旦参照させるために，UsernamePassword ハンドラ用のログイン画面に Kerberos ハンドラへのアクセス用ボタンを含める形で実装している．従来のポータルサービスと異なり，任意方向 SSO となる Shibboleth においては，隘路としてはここが単一点であるため，簡単な伝達事項等はここに示しておくこととした．

5. 利用状況

5.1. ポータルサービス

一般的なキャンパス向けポータルサービスでは，大学の個人向け連絡機能を提供することも多い．徳島大学の全学統合ポータルは，コミュニケーションポータルとも呼び，構成員に対する SNS（Social Network Service）の機能を有する．すなわち，任意の構成員をフォローしたり，任意のグループを作ってフォーラムを開設したり，キャンパス内の情報交換がユーザ同士で双方向に行える．

一方で，従来的なポータルに見られた個人毎や所属毎のお知らせ機能も有する．これを利用して，所属や学年といった単位でのお知らせを掲示したり，就職活動に関する情報を流したりできる．これは主に教職員から学生への一方向のコミュニケーションである．

さらに，本ポータルサービスは，他の Shibboleth 対応サービスとの間でメッセージを受け取り，必要な構成員に秘匿メッセージとして投稿することもできる．例えば，LMS 上で，レポート課題が出されたり，受領されたり，あるいは図書館システムにおける図書の返却期限切れといったイベントを検知した際には，上流のサービスがメッセージを個人宛に投稿し，表示させることになる．この際，詳細な内容は上流のアプリケーションに SSO で遷移して確認するべく，Shibboleth 化されたロケーション URL をメッセージ内に埋め込んでおくことで，利便性の高いメッセージとなる．上流からのメッセージには添付ファイル等は伝播しない事で，一定のセキュリティ向上も図っている．このように，メッセージ集約を本サービスに行わせることで，従来的なポータルサービスの利用方法に近いサービスを提供している．

5.2. SSO 開始アプリケーション

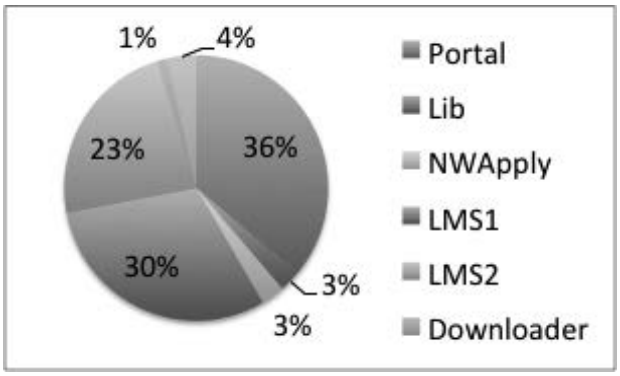


図 8　SSO の開始アプリケーション

徳島大学では，Shibboleth が導入されるまではポータルサービスからの片方向 SSO を実装していた．この場合，エンドユーザの WEB 遷移フローをある程度統制でき，各種の情報提示など片方向の情報発信側には利点が高い．一方で，エンドユーザは目的とするアプリケーションに直接到達できないという問題や，ユーザコミュニケーション向け機能を個別に用意するなども課題となる．

Shibboleth では，SSO の方向としては各種アプリケーションがフラットになるため，任意のアプリケーションから SSO を開始できることとなる．そこで，開始アプリケーションの割合を集計した．図 8 がその割合（2012 年 4 月 1 日から同 5 月 31 日）である．

導入初期には，ポータルが半分以上の割合を占め，そこから各種のサービスへ SSO 遷移する形が多く見られた．ところが，図 8 のように２ヶ月を経過した時点で集計してみると，各種サービスへのリンク集から直接ターゲットのサービスにログインする割合が増え，ポータル経由は 36%まで下がることとなった．一方で，LMS1 が 30%，LMS2 が 23%と増え，学生も教職員も，業務として日々利用する必要のあるサービスに直接アクセスするようになっている．

5.3. ログイン方法

（1）　新・旧の ID 選択状況

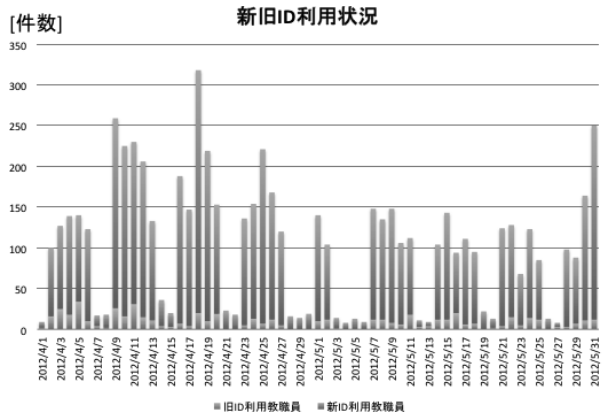


図 9　新旧 ID 利用状況

２章にて述べたように，新しいコンピュータサービスの一部には，旧 ID との並行利用期間を設けた．要求として，授業等で旧来的な ID を利用していたコンテンツが，当時の ID に紐付けられているものがあり，特に教職員からはそれらの再利用が強く求められ，要件定義に加えたものである．これらはほとんどが LMS，すなわち授業での再利用を意図している．

ここで，実運用開始初期の日々の ID 利用集計（教職員のみ）を見てみる（図 9）．このデータによれば，新 ID 利用（赤棒）は定常状態になった．一方で，旧 ID（青棒）はそれまでの切り替え周知を頻繁に実施した結果，当初時点から少なかったが，さらに減少している様子が分かる．新 ID の利用範囲（端末ログインやアプリケーションサービス）が多く，日常的に新しい ID で何らかを利用する機会が増えていると考えられる．

（2）　ログイン全体と Kerberos 利用

3 章以降で述べた Kerberos ハンドラの利用は，構築後間もない現状では，任意利用としている．このため，ドメインログインしない状況での Shibboleth 利用を除き，ドメインログイン状況では，ユーザの選択となる．そこで，総ログイン数の推移に対して，Kerberos 利用割合の推移を見てみることとする．

図 10 は，棒グラフ（主軸）は日々の Shibboleth でのログイン数，折れ線グラフ（第２軸）は Kerberos ハンドラを利用した 2012 年 4 月から 5 月にかけてのログイン数である．前者に注目すると，4 月は様々なシステムを年間で最も利用する時期であるため，5 月に入ってからは若干減数して定常状態となっている．一方で後者は，4 月は認知度が低かったためか，パスワード入力に慣れてしまっているためか，いずれにしても比較的少なかったが，5 月にかけては増加している様子が分かる．したがって，前者に対しては相対的に増加傾向が強いと言える．

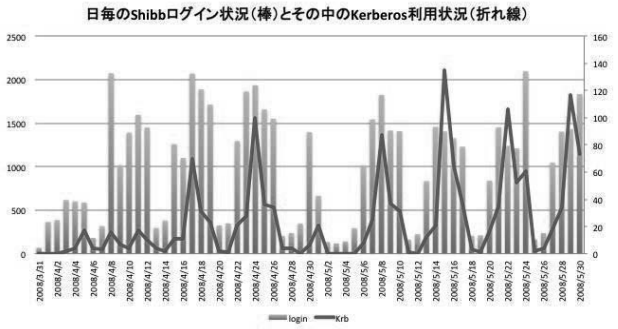


図 10　ログイン時の利用ハンドラの推移

6. おわりに

本論文では，徳島大学における複数種の認証源・属性源を利用した SSO 環境の実装について述べた．具体的に，複数のバックエンドを要する際の ShibbothIdP 設計上の方針を述べ，実装を行った．また，SSO については UsernamePassword ハンドラと Kerberos ハンドラの利用について述べ，かつ ADFS 対応アプリケーションも含めたシームレスな操作を提供できるユーザエクスペリエンス向上について述べた．5 章で見たように，利用開始間もないながらも，相対的に Kerberos 利用は増加傾向にある．しかし，システム利用開始初期のデータにつき，今後もこの動向については継続調査したいと考えている．

また，パスワード利用頻度および流通経路の軽減だけでなく，異なる認証方式や，セキュリティレベルに応じた複数要素認証方式なども今後検討していきたい．

謝　辞

本システムの IdP 設定に際しては，一部 NEC（株）の協力を得て実装している，また，既存の学内認証基盤実装から本論文のシステム検討に際し，徳島大学評価情報分析センター長の大家隆弘教授からは貴重なご意見・ご協力を頂戴した．謹んで感謝の意を表する．

参　考　文　献

[1] 太田芳博，梶田将司，田島嘉則，田島尚徳，平野靖，内藤久資，間瀬健二：大学における生涯 ID のための名寄せ手法，情報処理学会論文誌，Vol.51，No.3，pp. 965—973 (2010).

[2] 秋山豊和，寺西裕一，岡村真吾，坂根栄作，長谷川剛，馬場健一，中野博隆，下條真司，長岡亨：大阪大学における全学 IT 認証基盤の構築，情報処理学会論文誌，Vol.49，No.3，pp. 1249--1264 (2008).

[3] 松平拓也，笠原禎也，高田良宏，東昭孝，二木恵，森祥寛：大学における Shibboleth を利用した統合認証基

盤の構築，情報処理学会論文誌，Vol.~52，No.~2，pp. 703--713 (2011).
[4] 伊藤智博，高野勝美，田島靖久，吉田浩司，災害時に備えた分散キャンパスによる情報基盤の整備，学術情報処理研究, No.15, pp.5—11 (2011).
[5] The NIST Definition of Cloud Service http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (2012 年 6 月 29 日参照)
[6] Effle L-C. Law, Virpi Roto, Marc Hassenzahl, Arnold P.O.S. Vermeeren, Joke Kort: *Understanding, Scoping and Defininf User Experience: A Survey Approach*, Proceedings of CHI2009, pp. 719--728 (2009).
[7] 三好 康夫, 大家 隆弘, 上田 哲史, 廣友 雅徳, 矢野米雄, 川上 博：EDB を利用した学習経路探索を支援する e シラバスシステムの構築, 大学教育研究ジャーナル, No.3, pp.1--9, (2006).
[8] 岩沢和男，宮原俊行，中川敦, 岩田則和，西村浩二, 吉冨健一：センターサービス利用登録システムの再構築, 学術情報処理研究，No.15, pp.89—97 (2011).
[9] 金西計英, 松浦健二, 三好康夫, 高木知弘, 嵯峨山和美, 矢野米雄：大学間 WEB サービス連携のための Shibboleth を用いた許可管理機能の実現，日本教育工学会論文誌, Vol.32(Suppl), pp.93—96 (2008).
[10] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発, 情報処理学会論文誌, Vol.51 No.3, pp.1031-1039 (2010).

第 16 回学術情報処理研究集会

横浜国立大学におけるウェブホスティングサービス

A Web Hosting Service in Yokohama National University

志村俊也 †， 吉岡克成 ‡， 徐浩源 †， 牧田大佑 ‡， 星澤裕二 ‡ *， 松本勉 ‡
Toshiya SHIMURA †， Katsunari YOSHIOKA ‡， Haoyuan XU †，
Daisuke MAKITA ‡， Yuji HOSHIZAWA ‡ *， Tsutomu MATSUMOTO ‡

tshimura@ynu.ac.jp， yoshioka@ynu.ac.jp， haoyuan@ynu.ac.jp
makita-daisuke-jk@ynu.ac.jp ， yuji_hoshizawa@securebrain.co.jp， tsutomu@ynu.ac.jp

† 横浜国立大学　情報基盤センター
‡ 横浜国立大学　大学院環境情報研究院
* 株式会社セキュアブレイン

† Information Technology Service Center， Yokohama National University
‡ Graduate School of Environment and Information Science， Yokohama National University
* SecureBrain Corporation

概要

横浜国立大学情報基盤センターでは、利用者向けサービスとしてウェブホスティングサービスを提供している。また、同大学「情報・物理セキュリティ研究拠点」及びその共同研究者である(株)セキュアブレイン社の協力の下、ホスティングしているウェブサイトのコンテンツ検査を定期的に実施している。本稿では、ウェブホスティングサービスの概要と運用状況、およびウェブコンテンツ検査について紹介する。

キーワード

ウェブホスティング， クライアントハニーポットシステム， 法人向け gred セキュリティサービス

1. はじめに

横浜国立大学情報基盤センターでは、学内利用者向けにウェブホスティングサービスを提供している。ホスティングサイト総数は、2012 年 6 月 30 日時点で 171 サイトであり、その内訳は、表 1 に示す通りである。ここで、本学公式ウェブサイト www.ynu.ac.jp （以後、全学ウェブと呼ぶ） は、同じコンテンツを学内からのアクセス用と学外からのアクセス用の 2 つに負荷分散してホスティングしているので 2 サイトとしてカウントしている。負荷分散は、学外向け DNS サーバと学内向け DNS サーバに対して異なる A レコードの値を登録することで実現している。一方、利用者自身（研究室等）でウェブサーバを運用しているサイトは 43 サイトであるので、本学の

全ウェブサイトの約 80%が、当センターのウェブホスティングサービスを利用して公開していることになる。

	ウェブサイトの種類	サイト数
1	横浜国立大学公式ウェブサイト (www.ynu.ac.jp， 全学ウェブ)	2
2	部局・専攻・学科等の学内組織	71
3	委員会や部局横断的プロジェクト	12
4	GCOE、科研費等の政府の支援を受けているプロジェクト	6
5	研究室・学内研究グループ	76
6	本学主催の学会・研究会	4

表 1 ホスティングサイトの内訳

当センターでは、単にウェブホスティングサービスを提供しているだけでなく、本学環境情報研究院の研究者を中心とする本学の「情報・物理セキュリティ研究拠点」、及びその共同研究者である（株）セキュアブレイン社[1]の協力の下、ホスティングサイトのコンテンツ検査も行っている。本稿では、当センターのウェブホスティングサービスの概要と運用状況、及びホスティングサイトのコンテンツ検査について紹介する。

2. ホスティングサービス概要

2.1 システム構成

ウェブホスティングサーバは 3 台構成で運用している。サーバの 1 台あたりの仕様は、表 2 に示す通りである。

機種	富士通社製 PRIMERGY RX300 S5
CPU	Intel Xeon X5570 (クアッドコア/2.93GHz) × 2
RAM	12GB
HDD	1TB (RAID 5)
OS	RedHat Enterprise Linux 5.8
Httpd	Apache 2.2 系
PHP	PHP5.3 系
PHP 以外	RedHat 搭載版
データベース	MySQL (RedHat 搭載版)

表 2 ホスティングサーバの 1 台あたりの仕様

ホスティングサイトの 3 台のサーバへの振り分けは、目的・アクセス頻度・サーバへの負荷・管理面等を総合的に考慮して、下記のように振り分けている。

[1 台目 （以後、www1 と呼ぶ）]
全学ウェブ（学内からのアクセス用）と学内組織（表 1 の 2 番）の公式ウェブサイト 71 サイトを収容。これらのサイトは、SSL 証明書を利用した https での接続を提供する場合があるため、各サイトに固有の IP アドレスを割り当て、DNS 名 ←→ IP アドレスが 1 対 1 で対応する運用としている。

[2 台目 （以後、www2 と呼ぶ）]
表 1 の 3～6 番 のサイト（合計 98 サイト）を収容。これらのサイトは、SSL 証明書を利用しないため、1 つの IP アドレスに複数の DNS 名を対応させる仮想ホスト方式で運用している。

[3 台目 （以後、www3 と呼ぶ）]
全学ウェブ（学外からのアクセス用）のみを収容。学外向け本学公式ウェブサイトであるので、IPv6 Native でもアクセスできるようにしている。

1 サイトあたりの割り当て Disk 容量は、概ね 5GB 以内としている。また、コンテンツのアップロードに関しては、不正アップデートを防ぐため、ウェブサイト管理者が申請時に届け出た IP アドレス (学内端末 2 台まで指定可能。ただし、学外から指定端末へのリモートアクセスは禁止）からの SFTP（SCP, SSH）アクセスのみを許可するという対策を取っている。

2.2 CPU ロードアベレージとネットワークトラフィック

図 1, 2, 3 に示しているのが、それぞれ www1, www2, www3 の 1 分間及び 5 分間平均の CPU ロードアベレージである。縦軸の単位はパーセント（%）であり、緑色が 1 分間平均、青色が 5 分間平均を表している。図 4, 5, 6 に示しているのは、それぞれ www1, www2, www3 の 5 分間平均のネットワークトラフィックである。縦軸の単位は kB/s であり、緑色がサーバ ➔ クライアントへのダウンロードトラフィック、青色がその逆のアップロードトラフィックである。図の横軸は時系列を示しており、期間は、2012 年 7 月 19 日（木）01 時～7 月 20 日（金）09 時である。図 1, 2, 3 の CPU ロードアベレージについては、図の左側が 7 月 19 日 01 時に対応しているが、図 4, 5, 6 のネットワークトラフィック については、図の右側が 7 月 19 日 01 時に対応している。CPU ロードアベレージ、ネットワークトラフィックの双方とも、平日の振る舞いは、曜日によって大きな違いはない。

CPU ロードアベレージは、一時的に 100%を超える場合もあるが、平均的には、30%以下であり、余裕のある安定した運用となっていることがわかる。

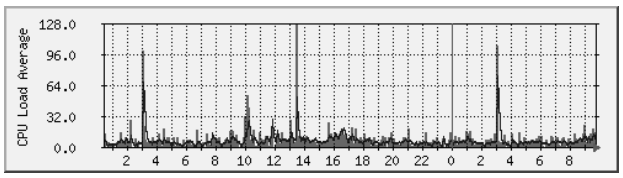


図 1　www1 の CPU ロードアベレージ

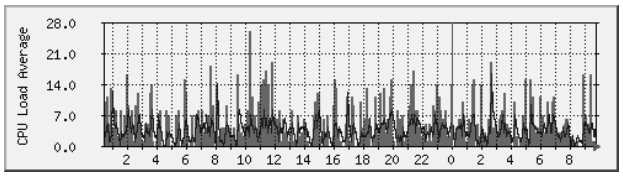


図 2　www2 の CPU ロードアベレージ

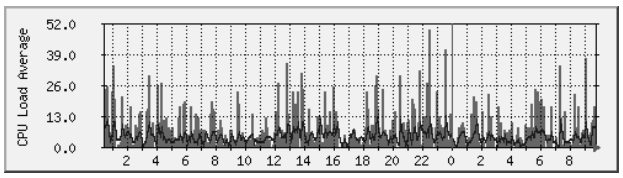


図 3　www3 の CPU ロードアベレージ

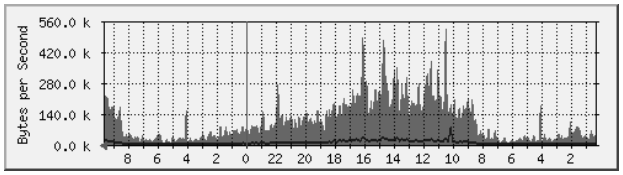


図 4　www1 のネットワークトラフィック

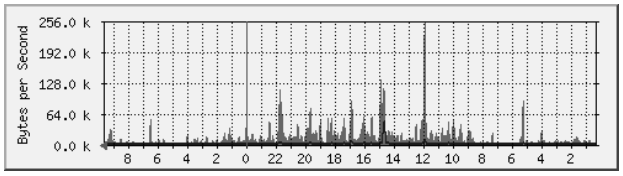


図 5　www2 のネットワークトラフィック

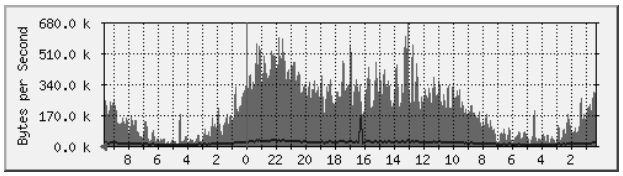


図 6　www3 のネットワークトラフィック

ネットワークトラフィックについては、平均的には、全学ウェブ（学外からのアクセス用）である www3 が最も多いが、それでも 700kB/s 以下である。紙面の都合上、図は記載していないが、休日のネットワークトラフィックは、www1, www2 が平日の半分以下に減少するのに対して、www3 は平日と大きくは変わらないという特徴がある。

2.2 アクセス状況

3 台のウェブサーバに対するアクセス状況を大まかに把握するため、各サーバにリクエストされた GET メソッド（クライアントからのファイルのダウンロード要求）の 1 日当たりの平均数を調べた結果を表 3 に示す。GET メソッドの集計期間は、2012 年 7 月 8 日（日） ～14 日（土）の 1 週間であり、平日平均は、7 月 9 日 ～13 日、休日平均は、7 月 8 日と 14 日 の平均数である。

	GET メソッド数（平日平均）	GET メソッド数（休日平均）
www1-www3 合計	1,417,723 (100%)	878,792 (100%)
www1-A 学内	155,030	21,274
www1-A 学外	229,379	174,451
www1-A 合計	384,409 (27.1%)	195,725 (22.3%)
www1-B 学内	263,833	21,176
www1-B 学外	896	934
www1-B 合計	264,729 (18.7%)	22,110 (2.5%)
www2 学内	17,090	1,095
www2 学外	36,463	22,083
www2 合計	53,553 (3.8%)	23,178 (2.6%)
www3 学内	700	213
www3 学外	714,332	637,566
www3 合計	715,032 (50.4%)	637,779 (72.6%)

表 3　各ウェブサーバに対する GET メソッドのリクエスト数の一日当たりの平均数。集計期間は、2012 年 7 月 8 日（日） ～ 7 月 14 日（土）の 1 週間。

表 3 の中で、www1-A は、www1 に対する GET メソッドの内、全学ウェブへのアクセスを除いた 71 サイトの分であり、www1-B は、www1 に対する GET メソッド

の内、全学ウェブに対する GET メソッドを示す。表中の「学内」は、学内からのアクセス、「学外」は学外からのアクセスを意味する。全学ウェブに対するアクセスは、学外からは www3 へ、学内からは www1 へ DNS ベースで振り分けているので、URL 名でアクセスする限り、www1 への学外からのアクセス、及び www3 への学内からのアクセスは発生しないはずであるが、IP アドレスベースで直接アクセスされる場合もあるためゼロにはならない。表 3 からわかることは以下の 5 つである。

① GET メソッドの一日当たりの平均数は、平日は約 142 万回、休日は約 88 万回（平日の約 60%）である。
② www1-A, www1-B, www2, www3 の平日平均数はそれぞれ、全体の 27.1 %, 18.7 %, 3.8 %, 50.4 %である。つまり、平日の GET メソッド全体の約半数は、学外からの全学ウェブに対するリクエストによるものである。
③ www1-B と www3 の平日平均の合計は、全体の 69.1%であり、全 GET メソッドの約 7 割が全学ウェブへのリクエストとなっている。
④ 学内からのアクセスにおける www1-A, www1-B, www2 の休日平均は、それぞれ、21,274、 21,176、1,095 であり、これは平日平均の 13.7%, 8.0%, 6.4% に相当し、大幅に減少する。
⑤ www1 全体、www2 の休日平均は、それぞれ、217,835、23,178 であり、平日平均と比べて半分以下の値となっているが、www3 の場合は、637,779 であり、平日平均と大きくは変わらない。これは、ネットワークトラフィックの振る舞いと一致している。

3. コンテンツ検査

3.1 クライアント型ハニーポットシステムによるコンテンツ検査

ウェブサイトが改竄されていないかどうかの確認は、ウェブサイト管理者の責務として利用規約に定めているので、本来であれば情報基盤センターが実施する必要はない。しかし、ウェブサイトのコンテンツをウェブデザイン会社に外注しているサイトが多数あり、JAVA, Perl, PHP, SQL 等のプログラミング言語で記載された SSI, CGI ファイルまでウェブサイト管理者自身で把握・検査をすることは事実上不可能である。また、コンテンツ管理システム（CMS）を利用してウェブブラウザ経由でコンテンツの更新を行う場合、CMS 用ユーザー ID/パスワード が盗まれてしまうと、正規のウェブサイト管理者としてアクセスされてしまうので、コンテンツ自体に脆弱性がなくても改竄されてしまう危険性がある。

そこで、当センターでは、本学の情報・物理セキュリティ研究拠点及びその共同研究者である（株）セキュアブレイン社の協力の下、ホスティングサイトのコンテンツがサイト閲覧者を攻撃する悪性サイトに改竄されていないかどうかの検査を定期的に実施している。コンテンツ検査は 2 種類の方法で実施しており、1 つは、クライアント型ハニーポットシステム（以後、CHP システムと呼ぶ）を利用した検査であり、もう一つは、セキュアブレイン社の「法人向け gred セキュリティサービス（3.2 章で説明）」を利用した検査である。

CHP システムとは、同システムを搭載した PC から検査対象ウェブサイトにアクセスし、「マルウェア等の意図しない不正なファイル」がクライアント PC 側に自動的に作成（ダウンロード）されないかどうかを検査する仕組みのことである。CHP システムのプログラムは、セキュアブレイン社が開発したものをベースにし、情報・物理セキュリティ研究拠点側で改良を加えたものである。CHP システムによるウェブアクセスの巡回方法は以下のとおりである。

① 検査対象ウェブサイトのトップページ（通常は、index.html ）にアクセスし、そこから再帰的にリンクを抽出し、アクセスしていく。
② リンクは、Anchor タグの HREF 属性で、相対パスで指定されているものを抽出する。絶対パスを抽出しないのは、検査対象サーバ以外の外部 URL まで 検査し、 検査が際限なく続く可能性を防ぐためである。
③ 各ページは、閲覧後 60 秒の待機時間を空けて、次のページの検査をする。60 秒間待機するには、クライアントからのアクセス後、時間をおいてマルウェアのダウンロードを開始させるコンテンツが存在するためである。

CHP システムは、ウェブブラウザやプラグインの脆弱性を利用した PC への攻撃を実行するような不正プログラムやマルウェアが検査対象ウェブサイトに仕掛けられているかどうかを検知するためのシステムなので、CHP システムを搭載した検査用クライアント PC は、脆弱性対策が適用されておらず、マルウェア対策ソフトウェアも搭載していない状態の PC を使用する必要がある。具体的には、Windows XP Professional SP2 で Microsoft Update が全く適用されていない状態の PC で行う。ウェブブラウザは IE6 を使用する 。このため、検査用 PC は、学内 LAN ではなく、商用の ISP に接続し、その上で学外からホスティングサイトの検査を実施することとしている。

このCHPシステムを用いた検査において、現時点では、ホスティングサイト上に不正なコンテンツは発見されていない。CHPシステムを使用して巡回調査中の検査PCの画面を参考のため図7に示しておく。

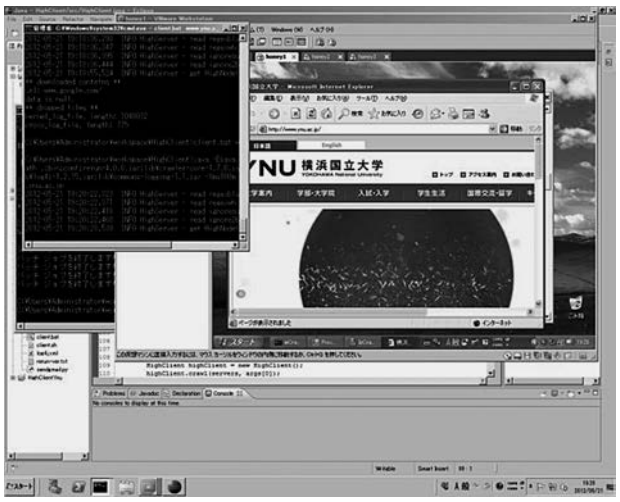


図 7　CHP システムを使用して巡回調査中の検査 PC の画面

3.2　セキュアブレイン社の法人向け gred セキュリティサービスによる検査

CHPシステムによるコンテンツ検査は、マルウェア等のクライアント攻撃型プログラムがウェブサイト上に仕掛けられているかどうかを検知する仕組みであるので、『フィッシングサイトの埋め込み』や『SQLインジェクション』といった改竄・危険性を検知することはできない。このため、当センターでは、CHPシステムに加えて、セキュアブレイン社の「法人向けgredセキュリティサービス（以後、gred サービスと呼ぶ）」を利用したコンテンツ検査を1ヶ月に一回の割合で実施している。gredサービスは、フィッシングサイトの埋め込みやSQLインジェクションといった不正コンテンツをも検知するシステムである。検査方法は、CHPシステムとは違い、シグネチャやルールベースでの検知となっている。このgredサービスは、同社が有償サービスで一般向けに提供しているものであるが、共同研究の関連もあり、セキュアブレイン社の御厚意により、同サービスを無償でご提供頂いている次第である。この検査においても、現時点ではホスティングサイト上に不正なコンテンツは発見されていない。

なお、セキュアブレイン社が提供しているgredサービスには、この法人向けgredセキュリティサービスとは別に、個人向けの「gredでチェック」という無料サービスも存在する。この無料版gredもフィッシングサイトやアクセスすると危険なサイトを判定する機能がある。従って、わざわざ有償版のgredサービスで検査する必要はないのではないかと考える方もいるかもしれないが、この無料版 gred はあくまで、有償版の gred サービスのデモという位置づけであるため、必ずしも、信頼できる結果が得られるとは限らないことに留意しておく必要がある。その理由は、無料版gredに限らず、このような「公開型動的解析サービス（任意の利用者から情報を受け付け、解析し、その結果を利用者に提供するシステム）」の多くは、検査プログラムが検査対象の URL にアクセスする際の IP アドレスが容易に露見してしまい、検査対象ウェブサイト側で検査を回避する設定を施すことが可能であるためである[2]。信頼できる検査結果を得たいのであれば、有償版のgredサービスを受けるべきであろう。

4.　おわりに

本稿では、当センターが学内利用者に提供しているウェブホスティングサービスの概要と運用状況、及びホスティングサイトのコンテンツ検査に関する紹介を行った。最後に、現在取り組んでいる課題について述べておく。上記で紹介したとおり、CHP システムは、「意図しないファイルの作成」を検知するシステムであるが、実は、その他に、クライアント PC 側の「レジストリの改変」や「プロセスの起動」も検知することができる。しかし、どのようなレジストリ改変やプロセス起動を悪性とみなすかという判定基準がまだ検討段階であるため、これらの検査は行っていない。この判定基準については、現在、情報・物理セキュリティ研究拠点が課題として取り組んでいるところである。

参考文献

[1]　http://www.securebrain.co.jp/

[2]　笠間貴弘、織井達憲、吉岡克成、松本勉、情報処理学会論文誌、「公開型マルウェア動的解析システムに対するデコイ挿入攻撃の脅威」vol. 52,　No.9, 2761 - 2774　(2011)

iSCSI 型ネットブートシステム起動性能評価システム

Development of a performance evaluation system for iSCSI-based thin client PCs system

本田　修啓

nhonda@gw.fukushima-u.ac.jp

福島大学総合情報処理センター

Fukushima University Information Network Center

概要

ネットブートシステムは,大学における実習教室の端末として多く採用されている.数百台の端末へのソフトウエアアップデートおよびセキュリティ更新を短時間で効率よく実施できる一方,起動時間に長い時間が必要となる問題が指摘されている.導入時の試験で実運用に近い環境でのテストは難しく,これらは運用後に表面化あるいは深刻化することが多い.本学総合情報処理センターでは,平成 23 年度導入した,iSCSI ネットブート型シンクライアントシステムの起動性能を MRTG グラフにより可視化し見やすく表示するシステムを構築し障害状況把握およびその解決に役立てているので紹介する.

キーワード

シンクライアント,ネットブート,可視化,性能評価,実運用

1. はじめに

福島大学総合情報処理センターでは,パーソナルコンピュータ端末約 300 台の Windows7 ネットブートシンクライアント端末（以下ネットブート端末）を平成 23 年 2 月に導入し運用している.セキュリティ維持や多数のクライアント端末の効率管理が得られる一方,以下のような障害報告がユーザから苦情として指摘された.

(1) 起動待ち時間増加
(2) 利用中の予期せぬ動作停止

アプリケーション利用中の予期せぬ動作停止は,Blue Screen Of Death (BSoD) と呼ばれる現象で,突然画面が青色になり,再起動以外に回復する手段はない.ファイル編集中に発生すると,利用者の被害は大きい.起動待ち時間の増加は,講義での実習開始時の影響が大きい.

特定の個人のみログオン後利用可能にならない状況は,ユーザプロファイル破損が原因であることが多く,個別にプロファイル初期化対応が必要で,管理者負担の増加の要因ともなっていた.

これらの不具合は突発的あるいは負荷集中時に発生し,導入時性能試験やユーザが少ない時間帯では障害が再現せず,被害を受けた利用者が障害報告を行わない場合も多く,障害の全体的な規模,起動遅延時間や発生時刻等ログやイベント確認に必要となるデータを把握することが難しい.このことが,迅速で適切な障害対策が行えない原因の一つとなっている.

報告するシステムは,ネットブートサーバ情報,クライアント接続スイッチ情報,iSCSI ストレージ情報を SNMP 等で収集し,日常の運用における,ネットブート端末の状況を収集し,管理者が状況を把握しやすいように可視化し,関連情報を並べて表示するシステムである.以下の情報をブラウザで簡便に確認可能としている.

(1) OS 起動後ログオン可能となるまでの時間
(2) クライアントと収容スイッチのリンク情報
(3) 起動されているクライアント数
(4) ネットワークトラヒック流量
(5) iSCSI 接続セッション数
(6) NAS 接続セッション数

2. 導入 iSCSI ネットブートシステム

評価対象システムは,NTT 情報流通プラットホーム研究所開発 STRAGEX を利用した iSCSI 型ネットブートシステムである.このシステムの起動時の動作を図 1 に示す.

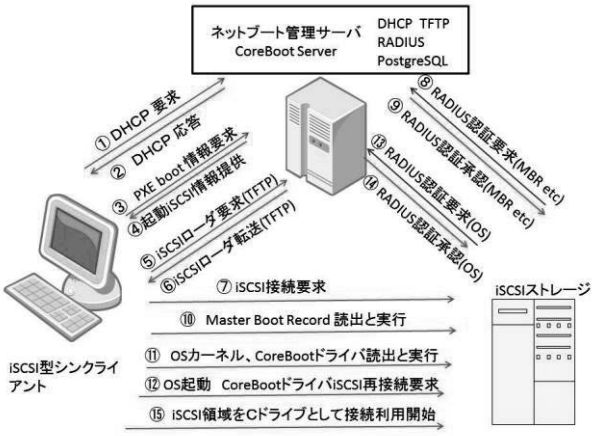


図 1 STRAGEX ネットブート起動時の動作

ネットブート管理サーバはクライアント起動時に起動のための情報を提供するのみで,クライアントは,iSCSI ストレージと直接通信し,OS およびアプリケーションを起動する.

起動後ネットブート管理サーバは,クライアントのログサーバとしてのみ動作し,負荷が原理的に少ないことから,クライアントシステム領域の配信サーバも兼ねるタイプのネットブート管理サーバと比して,より多数のクライアント管理を行うことができる特徴を持つ.

3 者のネットワーク構成を図 2 に示す.クライアントとネットブート管理サーバ,iSCSI ストレージは,同一 IP ネットワーク配置とし,2 個のレイヤスイッチを経由する.ジャンボフレームを使用しており,クライアントは⑪の OS 起動以降ジャンボフレーム(MTU 9000)で iSCSI ストレージと通信を行う.

ただしブート時は,0.5K あるいは 4K のブロック型転送が多く,ジャンボフレームの効果は限定的である.

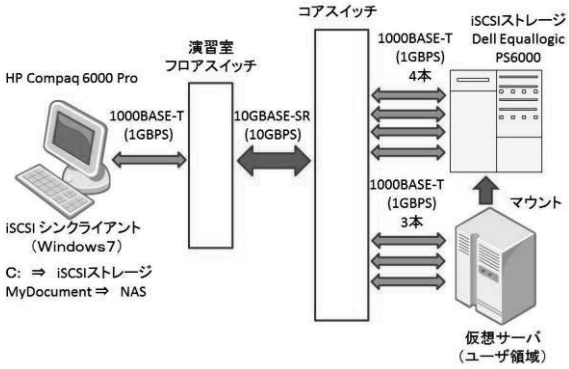


図 2 ネットワーク構成

2.1. 利用開始時トラヒックと起動時間

非混雑時クライアント起動時のトラヒックを図 3 に示す.電源ボタンを押し,ログオン可能になるまでの時間が約 110 秒あるが,うち 35 秒は OS 起動前の PXE 等の処理である.ログオン後利用可能状態まで約 1 分必要とする.ネットブートサーバは,OS 起動開始時およびログイン可能状態のタイミングを,内蔵データベースに記録する.起動時に流れるデータ量は約 1GB 弱である.

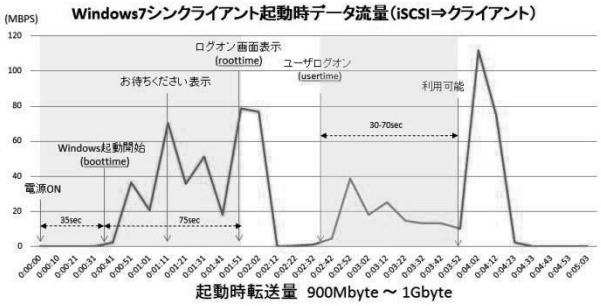


図 3 クライアント起動時データ流量(非混雑時)

文献[1]記載のように,ネットブート管理サーバは,起動時の処理のタイミングを内部データベースに保持する.この情報を利用することで,起動時刻,ログオン可能時刻,起動に要した時間をクライアント起動毎に把握することが可能である.

2.2. 混雑時トラヒックとクライアント起動

ネットブート端末 100 台同時利用時の演習室のフロアスイッチとコアスイッチ間トラヒックを図4に示す.帯域

は 10GBPS で余裕があるが,クライアント起動に要する時間が 5 分を超える遅延が多く発生する.

この状況は 100 人演習室 2 室で 200 人を超える利用者が一斉に利用開始するタイミングで発生する.

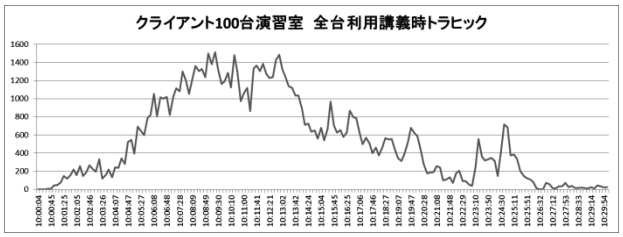


図 4 混雑時の演習室データ流量

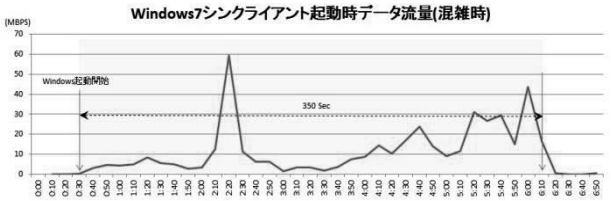


図 5 クライアント起動時データ流量(混雑時)

iSCSI ストレージ専用監視ソフトウェアで得られる情報を図 6 に示す.IOPS (Input/Output Per Second)が上限に達したことが確認できる.

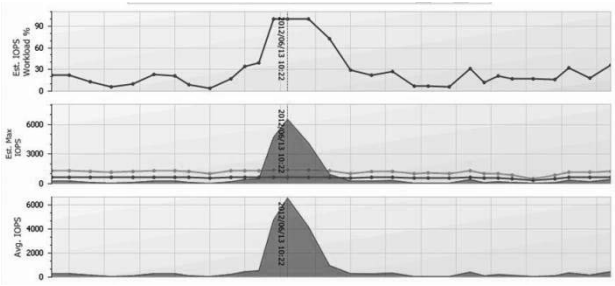


図 6 iSCSI ストレージ IOPS 状況

2.3. 100M リンク時のクライアント起動

BSoD の原因を調査する中で,クライアント起動時,フロアスイッチとの接続はオートネゴシエーションで 1GBPS 接続されるべきところ,まれに 100MBPS 接続になることが確認され,BSoD の原因の可能性を検討し,データ取得することにした. 非混雑時 100M 接続であると起動が遅くなる(図 7)ことでも検出は可能だが,フロアスイッチの SNMP 情報を確認することで混雑時でも確実に発生状況を把握することができる.(表 1)

表 1 リンク速度異常端末一覧

端末名	演習室名	boottime	roottime	usertime	stoptime	iscsi	linkspeed	起動時間
mul8022	MUL	2012-04-02 14:22:04	2012-04-02 14:25:04	2012-04-02 14:26:53	2012-04-02 15:12:17	str2_eth0	100	00:03:00
mul8016	MUL	2012-04-04 18:21:26	2012-04-04 18:24:35	2012-04-04 18:26:38	2012-04-04 19:01:03	str2_eth3	100	00:03:09
mul8016	MUL	2012-04-04 19:01:30	2012-04-04 19:04:22	2012-04-04 19:06:25	2012-04-04 19:07:29	str2_eth3	100	00:02:52
mul8013	MUL	2012-04-05 10:46:38	2012-04-05 10:49:45	2012-04-05 10:51:38	2012-04-05 11:49:11	str1_eth1	100	00:03:07
mul8016	MUL	2012-04-05 10:46:45	2012-04-05 10:49:56	2012-04-05 10:52:13	2012-04-05 11:09:10	str2_eth2	100	00:03:11

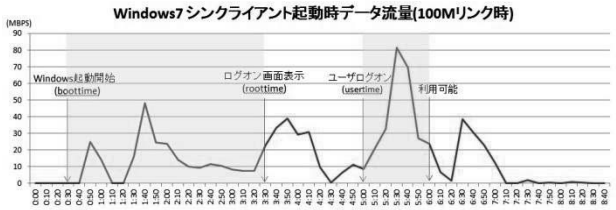


図 7 クライアント起動時データ流量(100M 接続)

3. 構築システム

3.1. 構成

構築した評価システムの構成を図 8 に示す.

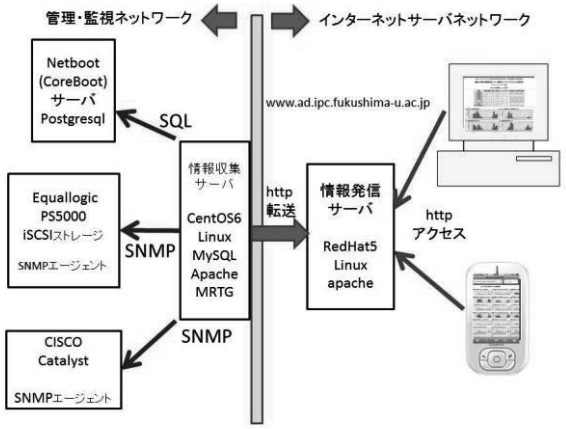


図 8 評価システムの構成

情報収集サーバは表2に示すように,ネットブートサーバ,iSCSI ストレージおよびフロアスイッチから,SQL,SNMP でデータ流量を除く,クライアント起動情報,クライアント接続情報,クライアントネットワークリンク情報を定期的に取得し,それを情報収集サーバデータベースに登録している.

表 2 収集情報一覧

収集情報	情報源	情報提供機器	プロトコル
OS起動開始時刻	iSCSIセッション情報MIB	iSCSIストレージ	SNMP
	ネットブート管理サーバ内部DB	ネットブート管理サーバ	SQL
利用可能時刻	ネットブート管理サーバ内部DB	ネットブート管理サーバ	SQL
接続リンク情報	演習室フロアスイッチMIB	演習室フロアスイッチ	SNMP
利用者ログオン時刻	ネットブート管理サーバ内部DB	ネットブート管理サーバ	SQL
利用終了時刻	ネットブート管理サーバ内部DB	ネットブート管理サーバ	SQL
	iSCSIセッション情報MIB	iSCSIストレージ	SNMP
iSCSIデータ流量	iSCSIセッション情報MIB	iSCSIストレージ	SNMP
演習室セータ流量	コアスイッチMIB	コアスイッチ	SNMP

収集データは,データベースから SQL,ネットワーク機器および iSCSI ストレージから SNMP で読み出し,MRTG でグラフを作成する.これらの処理に加え,関連するグラフ情報を並べて表示する html を定期的に自動作成するプログラム,情報発信サーバに転送するプログラムでシステムを構成している.プログラムは Perl で記述した.

情報発信サーバはインターネットに情報を発信する既存サーバ(www.ad.ipc.fukushima-u.ac.jp)を利用しており,アクセス制限は行っていない.学外運用支援スタッフの便宜,および学内スタッフが監視端末を離れても,スマートフォン等から閲覧できる便宜を優先させた.(図9)なお,発信情報はシステム性能情報のみであり,利用者アカウント名等,個人情報類は一切含ませていない.

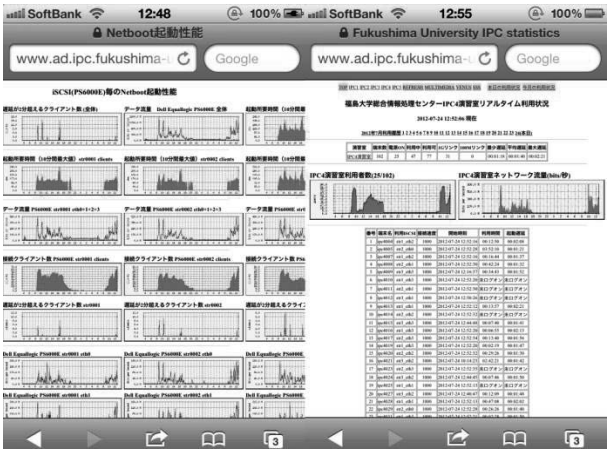


図 9 スマートフォンによる閲覧

3.2. 表示データと効果

3.2.1. 起動遅延情報

シンクライアント起動に要する時間情報は,ネットブートサーバ内部データベース情報の「OS 起動開始時刻」および「ログオン画面表示時刻」から計算して求めている.OS 起動前の時間は含まれない.したがって電源 ON 後ログオン画面表示されるのに要する時間は,この値に 30 秒程度加えた値になる.目視による実測およびパケットキャプチャログ確認を行った結果,ほぼ正確な値が得られることを確認した.

日常の利用で,どの時間帯に遅延がどの程度集中するか,どの iSCSI ストレージに集中するか確認が容易であることから,複数 iSCSI ストレージに起動クライアント割り当てを効果的に随時修正することが可能となっている.また修正の効果も確認しやすい.

3.2.2. 端末毎の起動に要した時間情報

起動し利用されているシンクライアント一覧を表示し,起動に要した時間情報も併せて表示する.加えて,最大値,最小値,平均値も表示する.

番号	端末名	利用ISCSI	接続速度	開始時刻	利用時間	起動遅延
1	ref6001	str1_eth3	1000	2012-07-06 16:22:09	00:19:57	00:01:35
2	ref6003	str1_eth0	1000	2012-07-06 16:12:05	00:57:06	00:01:28
3	ref6006	str1_eth2	1000	2012-07-06 16:36:07	00:08:23	00:01:32
4	ref6008	str1_eth0	1000	2012-07-06 16:34:04	00:10:01	00:01:27
5	ref6009	str3_eth0	1000	2012-07-06 14:12:26	08:40:13	00:01:06

演習室	端末数	電源ON	利用中	利用可	1Gリンク	100Mリンク	最少遅延	平均遅延	最大遅延
リフレッシュ	9	5	5	4	5	0	00:01:06	00:01:26	00:01:35

図 10 起動に要した時刻表示

3.2.3. 日統計情報

日毎の起動に要した時間情報をとりまとめる機能である.過去の日の情報も閲覧することができる.端末毎,利用毎の情報の他,最大値,最小値,平均値も表示する.

番号	端末名	利用ISCSI	接続速度	開始時刻	終了時刻	利用時間	起動遅延	備考
1	ref6001	str1_eth2	1000	2012-06-25 08:21:09	2012-06-25 08:29:58	00:06:30	00:01:22	
2	ref6001	str1_eth2	1000	2012-06-25 09:49:02	2012-06-25 10:00:42	00:09:21	00:01:25	
3	ref6001	str1_eth0	1000	2012-06-25 10:16:51	2012-06-25 10:40:02	00:20:36	00:01:38	
4	ref6001	str1_eth2	1000	2012-06-25 10:41:07	2012-06-25 11:38:32	00:55:05	00:01:28	
5	ref6001	str1_eth3	1000	2012-06-25 11:46:58	2012-06-25 11:56:53	00:05:40	00:01:25	
6	ref6001	str1_eth3	1000	2012-06-25 11:58:09	2012-06-25 12:17:03	00:16:04	00:01:35	
7	ref6001	str1_eth1	1000	2012-06-25 13:09:34	2012-06-25 14:36:40	01:24:33	00:01:35	
8	ref6001	str1_eth0	1000	2012-06-25 14:44:54	2012-06-25 15:43:38	00:55:58	00:01:50	
9	ref6001	str1_eth0	1000	2012-06-25 15:50:43	2012-06-25 16:07:39	00:14:32	00:01:27	
10	ref6001	str1_eth2	1000	2012-06-25 16:08:45	2012-06-25 17:04:45	00:53:07	00:01:59	
11	ref6001	str1_eth0	1000	2012-06-25 17:30:28	2012-06-25 17:42:38	00:09:40	00:01:25	
12	ref6002	str1_eth1	1000	2012-06-25 08:27:07	2012-06-25 08:42:10	00:12:31	00:01:26	

演習室名	利用回数	総利用時間	最小遅延	平均遅延	最大遅延	100MLink	異常終了	iSCSI-1	iSCSI-2	iSCSI-3
リフレッシュ	102	60時間49分	00:01:08	00:01:36	00:02:53	0	1	101	0	1

図 11 日統計情報

3.2.4. 月統計情報

演習室毎に,利用件数,月累積利用時間,起動に要した時間の最大値,最小値,平均値を表示する.

併せて,iSCSI ストレージ毎のクライアント接続数情報も表示させている.システムの利用統計データとしても活用可能な表示形式としている.

演習室名	利用回数	総利用時間	最小遅延	平均遅延	最大遅延	100MLink	異常終了	iSCSI-1	iSCSI-2	iSCSI-3
IPC1演習室	5599	6422時間52分	00:01:05	00:01:35	00:05:17	4	22	1722	1806	2071
IPC2演習室	725	796時間39分	00:01:14	00:01:56	00:05:47	0	5	0	0	725
IPC4演習室	2928	3939時間46分	00:01:06	00:01:44	00:04:31	0	14	923	987	1018
IPC5演習室	784	1017時間1分	00:01:06	00:01:35	00:04:00	0	5	302	465	17
IPCリフレッシュコーナー	1738	1206時間31分	00:01:04	00:01:35	00:04:23	0	5	1717	0	21
図書館マルチメディア室	1412	1895時間0分	00:01:05	00:01:28	00:03:36	0	14	625	782	5
IPC全体	13186	15280時間50分	00:01:04	00:01:37	00:05:47	4	65	5289	4040	3857

図 12 月統計情報

3.2.5. 接続速度情報

速度ネゴシエーションに失敗し 100MBPS 接続となったクライアント情報を記録し,各利用情報に合わせて表示させている.突発的な遅延原因の一つであり,クライアントNICあるいはネットワーク機器の交換により状況を改善している.ネットブートシステムのドライバに NIC リセットを追加することも若干の効果が見られた.

3.2.6. 起動端末数の可視化情報

MRTG を利用し,利用されているクライアント数の時間推移をグラフ化し表示させている.利用が多い時間帯,急激に利用が増加した時間帯を把握するのに有効である.

月,年グラフについてはピーク値も表示させ,平均化によってピーク値情報が失われないよう配慮している.

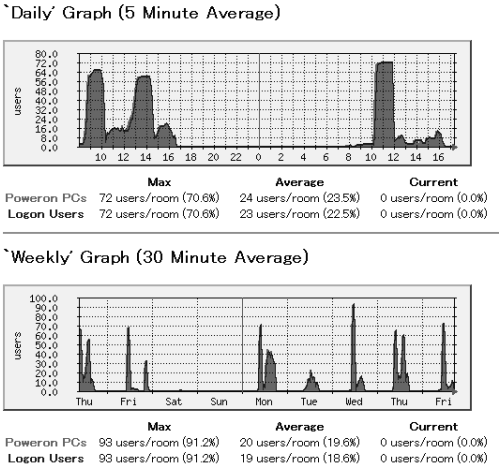


図 13　起動端末数情報

3.2.7. 起動に要した時間情報

ある5分間隔で,起動に最も長時間要したクライアントの起動時間を MRTG でグラフ可視化している.起動遅れが大きい時間帯の把握が容易である.

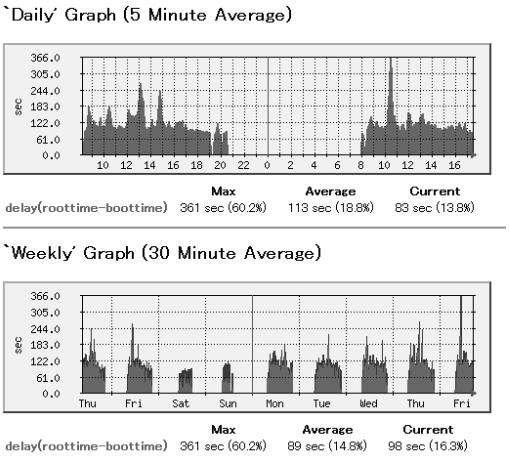


図 14　起動所要時間情報

3.2.8. 起動に長時間要した端末数情報

起動に 2 分および 3 分以上要したクライアント数を MRTG でグラフ化している.(5 分間のクライアント数)

起動遅れの発生時刻と規模が把握できる.

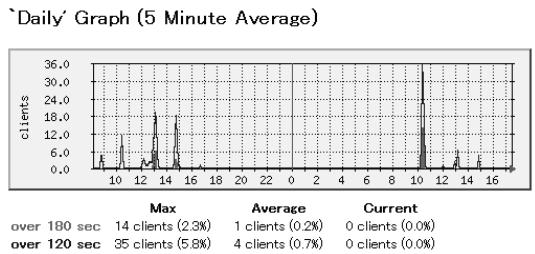


図 15　起動遅延クライアント数情報

3.3. ネットワーク流量情報

各演習室フロアスイッチとコアスイッチ間のネットワーク流量を MRTG 本来の機能でグラフ化している.

標準設定をそのまま利用しており,表示されるグラフは 5 分平均値であり,10 秒毎のサンプリンググラフよりピーク時流量は少なく表示されるが,起動端末数グラフ,遅延端末数グラフと併せて表示することで状況把握に便利である.

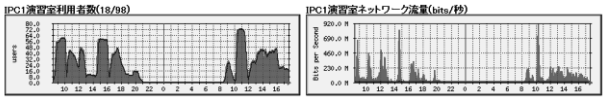


図 16　ネットワーク流量情報

3.4. iSCSI ストレージ情報

ストレージ状況は起動時間に大きな影響を与えると判断できるので,本システムでも SNMP を利用し,iSCSI ストレージインタフェース流量および,接続セッション情報から得られる起動端末数数情報,起動遅延情報等と同一画面に表示させている.

3.4.1. iSCSI 流量情報

iSCSI ストレージは3台あり,それぞれ4個の1000BASE-T インタフェースを有している.インタフェース毎の流量グラフの他,iSCSI 毎に各インタフェース流量を合算したグラフ,3 台の iSCSI の全流量を合算したグラフも作成させている. 図 17 は全合算流量である.

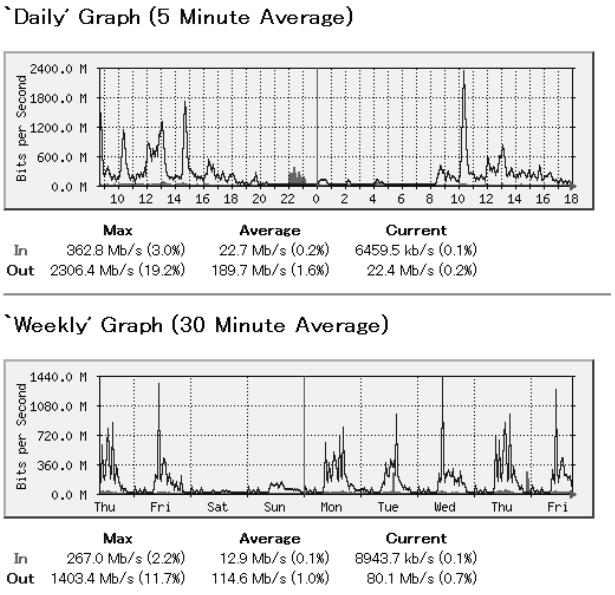


図 17　iSCSI データ流量情報

3.4.2. iSCSI 接続クライアント情報

iSCSI ストレージのクライアント接続 TCP セッション数を表として表示させている(図 18). クライアントが接続する iSCSI ストレージはネットブート管理システムで静的に指定するが,実運用の利用の偏り情報としての価値もあり,この情報を元にクライアントの iSCSI 割り当てを見直すことで,起動に要する時間を全体として低く抑えることが実現できた.

番号	端末名	利用ISCSI	接続速度
1	ipc1010	str1_eth2	1000
2	ipc1016	str1_eth2	1000
3	ipc1020	str2_eth3	1000
4	ipc1024	str3_eth3	1000
5	ipc1025	str1_eth3	1000
6	ipc1032	str2_eth1	1000

Equallogic	接続	Port	接続
STR0001	7	1	2
		2	1
		3	3
		4	1
STR0002	6	1	1
		2	2
		3	1
		4	2
STR0003	8	1	2
		2	1
		3	3
		4	2

図 18　iSCSI 接続クライアント数情報

3.4.3. iSCSI 接続クライアント数　可視化情報

iSCSI ストレージのクライアント接続 TCP セッション数を MRTG でグラフとして可視化した iSCSI ストレージ毎の接続クライアント数の変化と,同じ Web 画面に併せて表示される遅延可視化情報により,iSCSI クライアント数の変化とクライアント起動に要する時間の関係を直感的に把握することが可能となった(図 19).

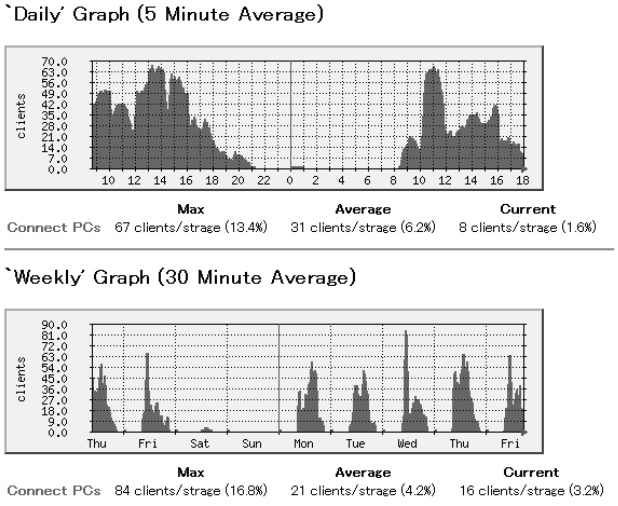


図 19　iSCSI 接続セッション数情報

4. まとめ

本システムは,導入当発生したプロファイル破損,BSoD の状況把握を目的に,順次機能を追加して行き,自動利用統計機能を加えて現在に至っている. 関係情報を MRTG, 発生した障害報告に対し,状況の把握を簡便に行うという目的は十分に果たしたと考える.関連する情報の同一画面表示は,状況把握効果が高く,自動統計機能は,遅延が大きい端末台数とその発生時刻,発生場所,発生規模(遅延が大きい台数) を記録し,行った障害解決の有効生を確認するのに有効であった.

プロファイル破損,BSoD については,iSCSI ストレージの予期せぬセッション断,ウィルス対策ソフトの予期せぬ動作,NAS 資源不足等が原因とわかり,改善され,障害報告および苦情は 0 に近い状態となっている.

今後は,負荷集中時の起動遅延問題の原因究明と解決に取り組みたい.

参考文献

[1] 市川俊一,岡純一,鷺坂光一：iSCSI を利用したシンクライアント PC システム STRAGEX,情報処理学会論文誌 : コンピュータシステム,Vol47 No.SIG12(ACS 15)

[2] 城所弘泰,村上登志男,磯上貞夫,坂本幸治郎 : シンクライアントの性能評価と大規模システムへの導入可能性の研究,学習院大学計算機センター紀要,Vol.29 2009

[3] 株式会社 NTT データ CoreBoot パンフレット http://www.coreboot.jp/wp-content/themes/coreboot/img/common/pamphlet.pdf

[4] 本田修啓：仮想サーバとクラウドサービスを活用した演習室クライアントシステム構築の一例,学術情報処理研究,No15 2011

大震災の経験から考案した BCP 非常用サーバ

The emergency server for BCP by the experience of the disaster

鵜川義弘†，福井恵子†，平井清巳†，安藤明伸†，小野元久†，本田茂広‡
Yoshihiro Ugawa†, Keiko Fukui†, Kiyomi Hirai†, Akinobu Ando†, Motohisa Ono†, Shigehiro Honda‡

sakura2012＠miyakyo-u.ac.jp†‡

†宮城教育大学情報処理センター
‡三菱スペース・ソフトウエア

†Miyagi University of Education
‡Mitsubishi Space Software CO., LTD.

概要

東日本大震災のとき，大学のサーバが２日間の停電で全機能が停止する中，携帯やインターネットが使えれば連絡ができたこと，その後１ヶ月日常生活ができなかったことを踏まえ，東北地方が全停電した状態であっても，Web で広報活動ができ，メールで安否確認が行えるよう大学宛メールから携帯等への“普段使い”の転送が維持され，復旧までの長期蓄積もできる非常用サーバを構築した.

キーワード

東日本大震災, BCP, 業務継続計画,事業継続計画, クラウドサーバ

1. 大震災の被害状況と BCP の策定

宮城教育大学は東北地方でも震央に近く沿岸寄りにある仙台市に立地し，地域は大きな被害を受けた.

情報処理センターのサーバ室は１階にあり，物理的な被害は軽微であった一方で，２日間の停電により情報処理センターの全機能が停止し，Web サーバやメールサーバが機能しなくなった. メールによる安否確認もできず，入学試験の中止の案内もできなかった[1]. 水道，ガス，自家用車にガソリンが自由に手に入るまでの１ヶ月以上の間は, 食料も満足に調達できない不自由な生活だった.

管理者が出張中で仙台に戻れない状況もあり，インフラだけでなく人命に不測の事態も想定する必要性もあった．非常時以前に，あらかじめ被害状況に応じた対応策を決めておく業務継続計画（Business Continuity Plan）を策定する必要性を痛感した[2].

大震災のとき SINET は電源喪失による停止はあったものの別ルートを回るバックアップにより途切れることはなかった．またネットワークインフラを支える複数の企業や組織の災害復旧，災害対応状況を見ると，今後のネットワークは災害時にも強いと考えられ，想定すべき最も重要な危機は電源であると思われる.

業務継続計画では東北地方全停電ですべての機能が停止する場合と，輪番停電などで一部機能が停止する場合が考えられ，後者は発電機や縮退運転モードを持つシステムの導入を計画しているが，本稿では前者について述べる．

2. 非常用サーバの構成

2.1. クラウドサーバ

今回構築した非常用サーバは，東北地方全停電により情報処理センターは機能を停止した状態．一方で携帯各社のネット機能は使える状態を想定し，東北地方と同時に停電する可能性がない離れた地域にクラウドサーバをレンタルし非常用 DNS，Web サーバとメールサーバを構築したものである．

非常用サーバは，まず，サーバ設置地域が東北地方ではないとわかるもの，またデータ転送量に制限がないものを検討した．その結果，仮想 4 コア CPU，主メモリー４G，ディスク容量 400GByte のものを年間 5 万円以下で契約することができた．

2.2. 非常用モードコントローラ

非常時には携帯から非常用サーバにアクセスし，通常サーバから非常用サーバに切り替えるコントローラ機能を持たせることにした．

非常用モードコントローラにより通常状態と非常状態を切り替える．災害直後など非常時の利用であることから携帯電話からのアクセスが可能なシンプルなインターフェースとした．

非常用モードコントローラは CakePHP[4]をフレームワークとして用いた Web アプリケーションとして開発した．

図-1　非常用モードコントローラーログイン画面

図-2　非常用モードコントローラー切替画面

2.3. 非常用 DNS

非常用 DNS により，Web サーバ，メールサーバが通常のものから非常用のサーバへと切り替わる（図-7　非常用 DNS 動作概念図を参照）．

非常用 DNS は通常状態ではセカンダリ DNS として動作する．

非常状態では，セカンダリとして収集している最新のゾーンファイルを元にすべての A レコードを非常用サーバの IP アドレスに切り替えたゾーンファイルを作成し，そのゾーンファイルを使用したプライマリ DNS サーバとして稼働する．

また，非常状態から通常状態に戻した際に DNS 情報の伝搬が高速になるように TTL を元のゾーンファイルより短く変更した．

ゾーンファイルの切り替えプログラムでは DNS::ZoneParse Perl モジュールを用いている．

2.4. 非常用 Web サーバ

非常用 Web サーバは非常用の連絡先，安否確認の方法など，非常時に必要な情報を提供するサーバである．

Web サーバについては一部コンテンツのミラーを持つ代替サーバも検討したが，震災後１ヶ月，生活もままならない状況で，通常のコンテンツを流していても，例えば停電時に着信できない内線電話の表記があったり，人が動けない状況では意味がなく，望ましくない状況が生まれる．そこでコンテンツは，被災状況，連絡先，安否確認の方法などの非常用情報を提供する最低限のものとした．コンテンツの更新も，携帯から更新ができるブログ形式のものとした．

他の Web サーバについても同様の状況と考えられ，非常用 DNS の設定により大学のトップページだけでなく

URL が .miyakyo-u.ac.jp で終わるすべての Web ページへのアクセスがこのブログへと導かれる.

非常用 Web サーバはパソコンでも携帯からでも見やすい Geeklog [5]を CMS として用いた. ブログ形式であり, 万が一の場合に, パソコンとネットの確保が難しい状態でも, 携帯電話から更新作業ができる.

図-3　本学の通常のホームページ

図-4　非常用 Web サーバでのブログホームページ
「非常時には非常時用コンテンツが表示される」

通常時に非常用コンテンツが見えると誤解を生むが, 管理者は通常時に非常用コンテンツの準備を行ないたい. そこで Geeklog のソースを変更し管理者としてアクセスした場合は通常時でも非常時用のコンテンツを閲覧/管理できるようにした.

非常用に切り替わっている状態のとき Google 等の検索サイトのロボットがクローリングし, 誤ったコンテンツを収集しないように robots.txt によりロボットからの収集を禁止した.

2.5. 非常用メールサーバ

非常用メールサーバは, 非常時のメールの蓄積と携帯メール等への転送を継続するためのメールサーバからなる（図-8　非常用メールサーバ動作概念図を参照）.

非常用メールサーバに, ユーザのメール領域を含め, 通常業務のすべての機能を代替しようとすると非常に大きなものとなり, ミラー方法, 提供方法も複雑になる. 今回の大震災では, 災害時にも携帯電話やプロバイダーのメールは動作しており大学のサーバ停止中であっても携帯電話や HotMail, YahooMail, Gmail に転送し, それで安否確認を含めて緊急の連絡を見ることができれば, 当面不自由はしない. そこで, 平常時, 大学から携帯や自宅プロバイダー等に転送している状況を自動で学習させ, 非常時にその転送ルールに従って転送する機能を持たせた.

一方で, 通常のメールサーバが停止中の間は, メールを非常用サーバに蓄積するようにし, 復旧後に改めて非常用サーバから再送するような機能を持たせた.

通常状態ではセカンダリメールサーバとして稼働し, 非常状態ではセカンダリメールサーバ機能に加え, メール転送機能を行う.

通常状態から非常状態となった時点で, DNS にて非常用サーバを MX レコードに追加した場合, その伝搬期間の間, メールが非常用サーバに届かないことになるため, 通常状態でセカンダリメールサーバとして稼働させている.

2.5.1. メール転送状況の学習

非常時に転送するアドレスをわざわざ登録させるページを作っておいたとして, そのことを覚えている人はどれだけいるかわからないし, 災害が起こってから転送先を入力してもらうことも考えられない. 学内には様々な方法で転送方法が提供されていて全てを網羅して調査することは難しい. そこで“普段”の転送状況を学習させることにした.

本学のメールシステムでは, どのホスト, サーバから送信しても必ずウィルス対策を行うメールサーバを中継してメールが外部または内部に配信される.

この中継用メールサーバのメールログのうち, メールの Message-ID ヘッダを用いて追跡をすることで, あるアドレスに対する転送先のメールアドレスが把握できる.

メーリングリストなどの同報メールの場合, 同一の Message-ID で複数の宛先に配信されるため, メールログの検査ではこれを除外した.

また最終転送先が同じ大学内のメールサーバである場合, 該当するメールサーバも非常時は停止していることが想定できるため, これも除外する.

非常時に確実に配送するため, 同一アドレスからの転送先が複数に変化した場合には, 変化分を追記する形にしている(図 5,図 6).

これは, 単に転送先を変更したのか, procmail, ActiveMail などを用い, 条件によって転送先を振り分けているのかがメールログだけでは分からないためである.

日付	転送元アドレス	転送先アドレス
2012/3/1	転送元アドレス A	転送先アドレス A
2012/3/10	転送元アドレス A	転送先アドレス B
2012/3/15	転送元アドレス A	転送先アドレス A
2012/3/20	転送元アドレス A	転送先アドレス C

図-5　収集した転送先アドレスが変化した様子

転送元アドレス	転送先アドレス
転送元アドレス A	転送先アドレス A, 転送先アドレス B, 転送先アドレス C,

図-6　変化した転送先アドレスを追加した様子

転送先の把握は毎日行うが，当日分のメールログ検査結果だけではその日にメールが届かなかったユーザの転送先が消えてしまうため過去 21 日分（メールログ三世代分）の検査結果をまとめ，転送先データベースを構築している．登録件数から見る限り，転送先を元々設定していない者を除きほぼ全てのユーザの転送先を把握していると考えている．

転送先データベースは 1 日 1 度非常用サーバに転送している．

2.5.2. セカンダリメールサーバとメール転送

セカンダリメールサーバでは，大学宛のメールを静的に大学の外部メールサーバに配送する．

ホスト名で配送先メールサーバを指定した場合，非常状態で配送先が自分自身となりループを発生させてしまうため，配送先のメールサーバは IP アドレスで指定する．

メールの転送は postfix の virtual_alias_maps 機能を用いて行う．通常状態では virtual_alias_maps 機能を無効にし，非常状態で virtual_alias_maps 機能を有効にすることで，メール転送機能の有効，無効を切り替える．

一日一度，転送された最新の転送先データベースを元に Alias ファイルを作成する．作成する際に転送元アドレスを転送先アドレスに加える．

転送元アドレスへの配送は，配送先サーバが停止しているため，非常用サーバの中のキューにたまり，配送先となる大学のメールサーバが復活した後に配送される．

この方法の欠点として，非常状態から通常状態に戻った後，本来のサーバで同一の転送が行われるため，転送メールが合計 2 通になることである．緊急性を重要視し，この欠点は無視した．

学内のメールサーバの内，独自に MX を持つサーバに関しては，指定した IP アドレスのメールサーバでは 3rd party relay とみなされ配送エラーが発生する．そこでセカンダリ DNS サーバとして収集しているゾーンファイルを検索し，独自に MX レコードを持つドメイン名を抽出し，静的配送マップに追加する処理を追加した．

3. その他

本学では通常時は広報・危機管理係が Web ページを管理しているが，震災時には，総務部に設置された災害対策本部が様々な情報を収集し発信を行なっていた．

非常用サーバは情報処理センターが設置したものであるが，災害対策本部や広報・危機管理係が内容を管理，普段から非常用連絡先，安否確認の方法などの情報を蓄積できるよう，情報処理センターと大学との役割分担に関して調整が必要であった[3].

非常モードでは，学内の Web サーバの全てが非常用 Web サーバに切り替わる．各組織で，非常時に必要な情報を広報・危機管理係に集め準備することが必要である．

未曾有の災害と言えども時がたてば記憶も薄れ対策が疎かになる．１年に１度は必ずある電源設備点検時等のタイミングで切替訓練を行なう計画である．訓練に伴うアナウンスでは，学内の Web サーバの全てが非常用 Web サーバに切り替わること．非常モードで転送した先ではメールが重複すること等の注意の他，非常用サーバでは訓練であることを示すことが必要である．

4. 参考文献

[1] 宮城教育大学情報処理センター被災状況
http://edb.miyakyo-u.ac.jp/ugawa/20110926/MUE-IPC-311/

[2] 宮城教育大学情報処理センター大震災被災状況と業務継続性計画
http://www.ipc.miyakyo-u.ac.jp/nenpo/no.19pdf/06.pdf

[3] 宮城教育大学非常用サーバ案内
http://staff.miyakyo-u.ac.jp/~ugawa/Center/BCPserver.pdf

[4] CakePHP
http://cakephp.jp/

[5] Geeklog オープンソース CMS
http://www.geeklog.jp/

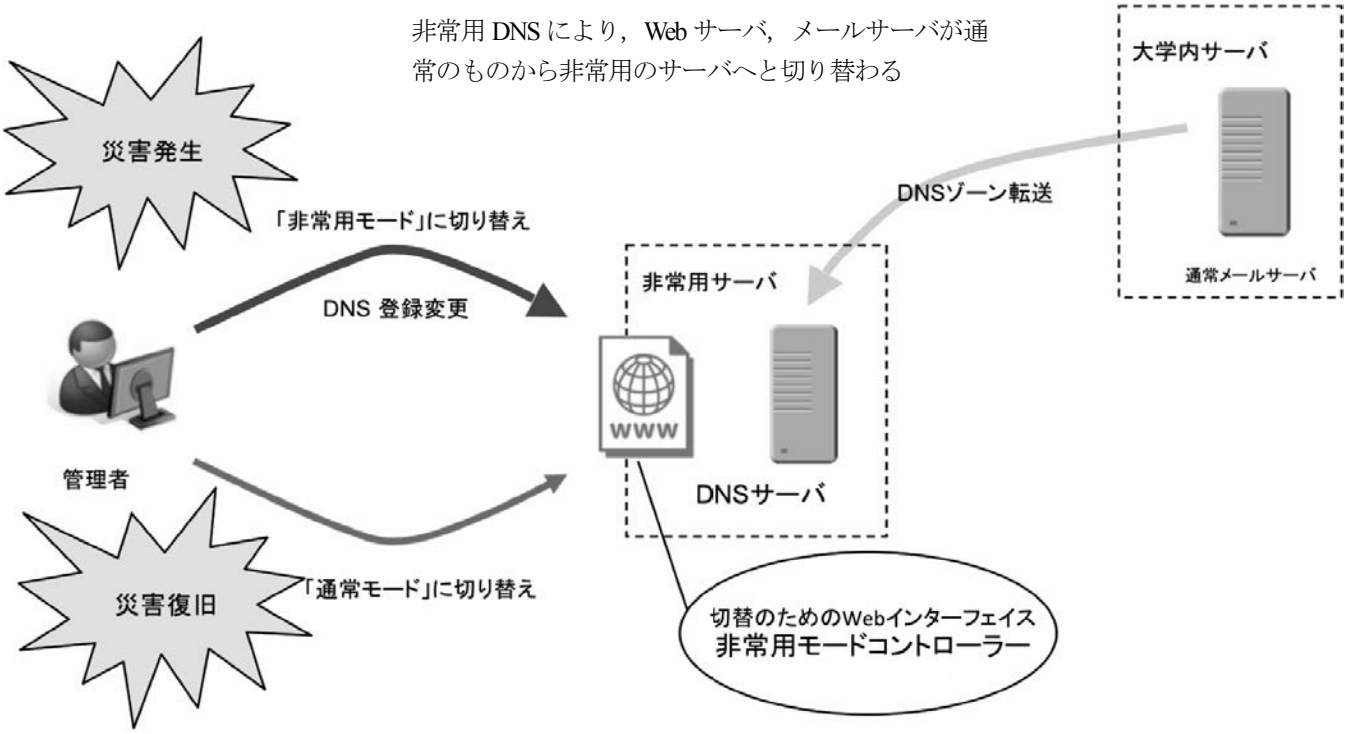


図-7　非常用 DNS 動作概念図

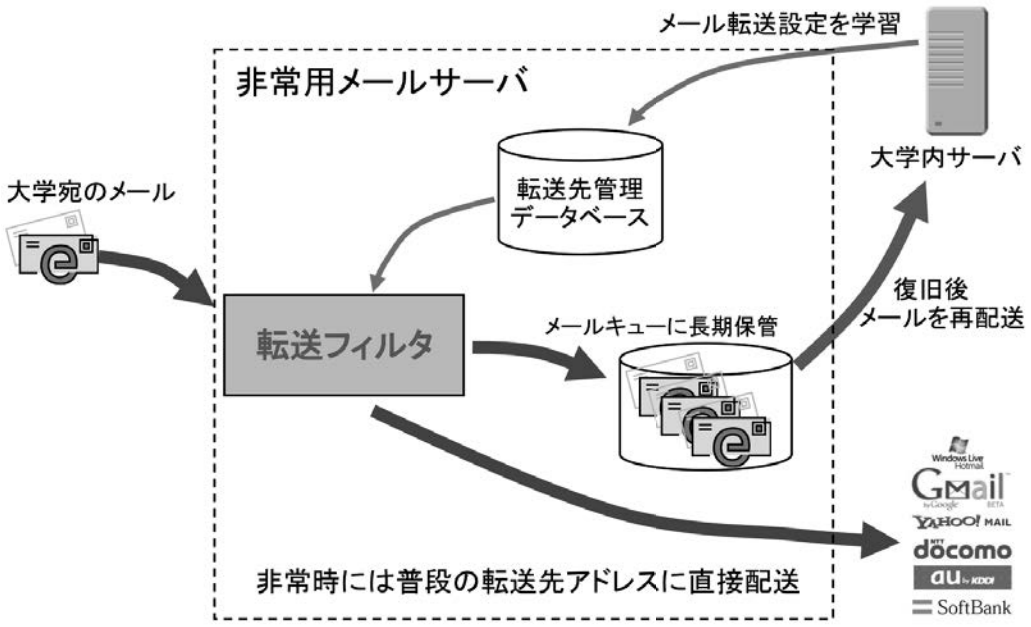


図-8　非常用メールサーバ動作概念図

無線 LAN 接続状況の可視化と無線 LAN アクセスポイントの動作解析

Visualization of Wireless LAN access and Behavior Analysis of Wireless LAN access points

内藤郁之†，望月源†‡，佐野洋†‡
Takashi Naito†, Hajime Mochizuki†‡, Hiroshi Sano†‡

naito_takashi@tufs.ac.jp, motizuki@tufs.ac.jp, sano@tufs.ac.jp

†東京外国語大学総合情報コラボレーションセンター
‡東京外国語大学総合国際学研究院

†Information Collaboration Center, Tokyo University of Foreign Studies
‡Institute of Global Studies, Tokyo University of Foreign Studies

概要

本学では，無線 LAN アクセスポイントを学内に設置し，ユーザ向けにネットワーク接続を提供している．現行システムの導入後から無線 LAN アクセスポイントの障害が多発したことにより，原因究明および対策のため，アクセスポイントの動作状況の把握および動作解析を行った．さらに，無線 LAN アクセスポイント経由でアクセスしているユーザの一覧を取得するスクリプトの作成により監視精度の向上を図った．

キーワード

ネットワーク管理，無線 LAN，SNMP

1. はじめに

本学の無線 LAN アクセスポイントは，エッジスイッチを経由してコアスイッチに接続されている．特に無線 LAN を経由したアクセスは，個人持ち込みの PC およびスマートフォン，タブレットでの学内ネットワークへの接続に利用され，その安定性は日増しに高まっている．

本学において，当初，無線 LAN アクセスポイントの不具合が多発し，アクセスポイントがダウンしたため，状態の把握が必要となり，ネットワーク監視ソフトウエア以外に無線 LAN チェッカーの導入およびアクセスポイントのシステム情報を任意のタイミングで取得する監視用のスクリプトの作成，および取得した情報の可視化を行った．

2. ネットワーク構成

無線 LAN アクセスポイントとコアスイッチまでの物理接続は，PoE インジェクター，エッジスイッチを経由してコアスイッチ，認証スイッチと接続されている（図 1）．PoE インジェクター以外の機器は，SNMP の情報の

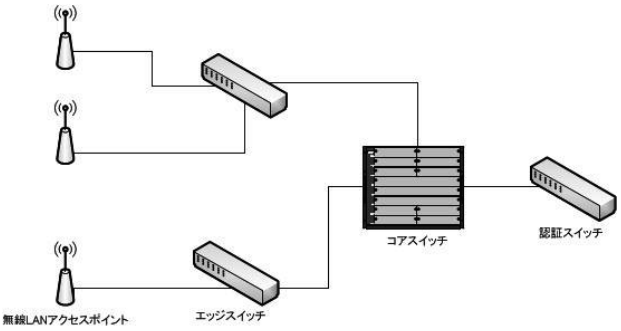


図 1 ネットワーク構成

取得，syslog へのログ転送機能があり，状態を把握することが可能である．これらの機器では，監視ソフトウエアによる死活監視および統計情報の取得をおこなっている. PoE インジェクターが, リモートから管理が行えず, 設置場所で動作 LED を確認する必要があり, 障害発生時の切り分けに手間がかかることが問題である.

ネットワーク機器の監視には，死活および流量監視に Nagios を利用し，流量の取得に Cacti を利用している．さらに，各機器で取得したログを syslog サーバに集約している．これらの構成を図 2 に示す.

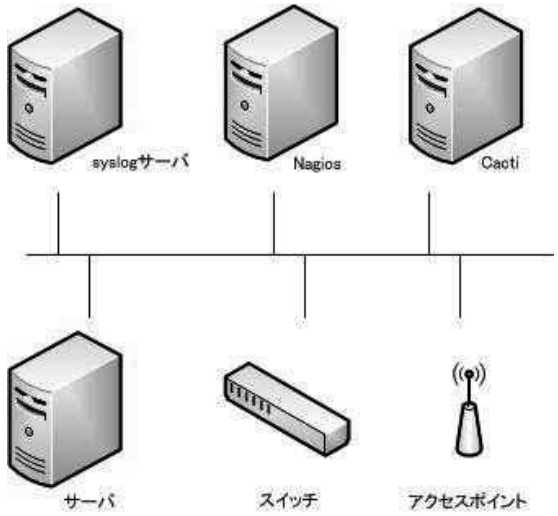


図 2 監視の構成

3. 無線 LAN 接続の障害の概要

無線 LAN 接続環境の障害は，無線 LAN アクセスポイントの機器の不良によるものと，その後の認証クライアント数の増加にともなうものがあり，それぞれ，以下に詳細を説明する.

3.1. 無線 LAN アクセスポイント

本学の無線 LAN アクセスポイントは, 2011 年 11 月まで，ダウンする機器が発生するという障害が頻繁に起こっていた．図 3～図 5 に 9 月から交換前までの 1 日あたりの障害発生件数を示す．この障害は，発生条件，発生頻度等には偏りが無く，原因究明は困難であり，対策の方を重視する運用を行っていた．対策は，ダウンしたアクセスポイントの電源を入れ直すというものであった．アクセスポイントのログは，syslog により syslog サーバに集約されていたが，syslog サーバでは，特にエラーに関する情報は確認できなかった．アクセスポイントのコンソールでログを表示させることが可能であり，これと syslog サーバに転送されたログの比較を行ったところ，一部のログだけが転送されていることが判明した．これに対し，スクリプトにより，任意のタイミングでログを取得することを試みた．最終的に，この障害は，機器の不良により発生したことが判明し，交換となったので，交換後は，発生していない.

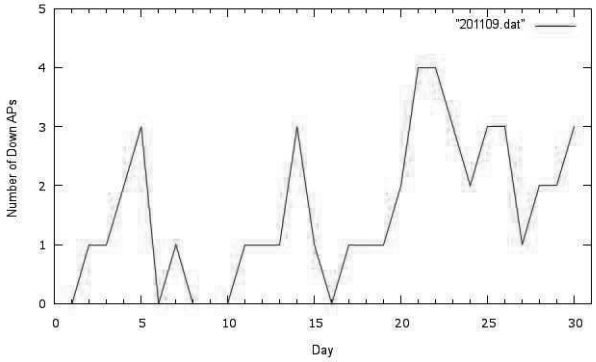


図 3　ダウンしたアクセスポイント数(9 月)

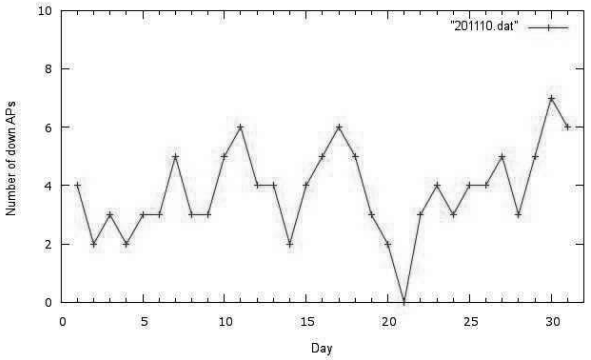


図 4 ダウンしたアクセスポイント数(10 月)

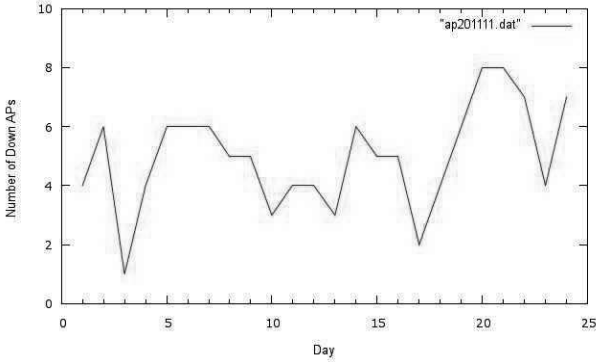


図 5 ダウンしたアクセスポイント数(11 月)

無線 LAN アクセスポイントの syslog 取得により，無線 LAN アクセスポイントとクライアントとのネゴシエーションの発生に関する動作が判明した．本学の無線 LAN 接続では，認証を行わなければ，ネットワークの利用はできないが，無線 LAN アクセスポイントは，クライアントとの通信を行い，クライアントに対して，アクセスポイントの存在を通知する．このとき，認証を行わなくても，アクセスポイントでは，検知されたクライアントとして扱われるので，人の集まる場所では，多数のクライアントが検出され，そのため，アクセスポイントの負荷の上昇につながっている．また，このアクセスポイントの仕様として ARP テーブルのリフレッシュが行われず，情報を蓄積していくため，適切なタイミングで電源を再起動する必要がある．

3.2. 認証スイッチの障害

認証スイッチの CPU 負荷の上昇(図 6)および新たな無線 LAN 接続のクライアントの認証不能という事態が発生した．これは，認証スイッチに認証の要求が届く件数が増加したためである．直接的な原因は，クライアントが増加したためであり，主に，無線 LAN 接続をサポートしているスマートフォンおよびタブレットの増加にともなうものである．また，これは，クライアントから DHCP での IP アドレス割り当て要求が発生し，その後，認証にリダイレクトされるようになっているが, ここで，認証の操作を行わない場合でも，認証の処理が行われるためである．この障害に対しては，スイッチの処理能力が限界に達したと判断し，より高性能の機器に入れ替えた．その結果，CPU 負荷の上昇は，発生はするものの 5 分以内に解消し，多くのユーザの認証を行える状況に好転した．

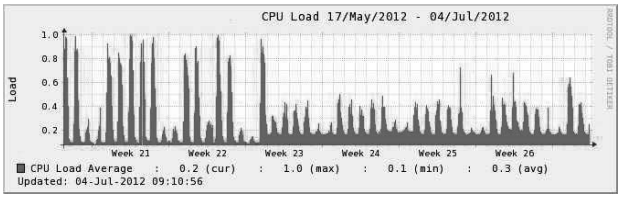


図 6　認証スイッチの負荷

4. 監視状況

監視は，リアルタイムに SNMP を利用した監視ソフトウエアによるものと syslog 転送機能を利用し，ログサーバでのログ確認の 2 本立てで行っている．

リアルタイムの監視では，Nagios による死活監視および流量監視と Cacti による流量監視を行っている. また，Nagios のアラートに対して，適宜，snmpwalk および ping 応答の確認を行っている．Nagios の監視条件は，以下のようになっている．

表 1 監視項目の設定

監視項目	間隔(分)
ping	5
ネットワーク流量	30
サービス	10

Nagios では，フラッピングの回避を行っているので，状態の変化から 30 分後に通知が発生するようになっている. Cacti では, 5 分間隔でネットワークの流量を取得し，流量グラフの出力に加えて，閾値監視として，一定の流量を継続して超えた場合に，メール通知を行う設定となっている．Nagios では，SNMP での流量監視は，変化率で評価するため，閾値監視を行う上では，扱いにくいので, 現在, ネットワーク監視に関しては, Nagios から Cacti へ移行を図っている．

4.1. 無線 LAN アクセスポイント

無線 LAN アクセスポイントの監視は，共通的な前述の設定に加え，任意に snmpwalk および ping の応答の確認を行っている．さらに，第 2 節で触れたように，syslog 転送を行っており，syslog サーバでログを集約している．現在，syslog で収集できるログは，無線 LAN アクセスポイントに関しては，アクセスポイント内に蓄積されているログの一部しか転送されない仕様であることが判明しているので，スクリプトにより，適宜，ログを取得するように変更している．

4.2. 認証スイッチ

無線 LAN アクセスポイントのセグメントに関しては，認証が一つのスイッチで行われるため，認証されたクライアント情報がスイッチに格納されている. この情報は，MIB で定義されているものの外部からアクセス不能に設定されており，同じ情報は，スイッチのコンソールからコマンドを入力することで閲覧することが可能となっている．この認証情報は，無線 LAN アクセスポイント経由のアクセスのほぼ現在の利用状況に一致する情報が取得できる．認証は，ユーザが切断しない場合，接続が確認できなくなってから解除されるまで 30 分の設定となっているので，一部，接続していないユーザも含まれていることになる．

4.3. 監視状況の可視化

Nagios および Cacti では，ウエブインタフェースにより結果が可視化されている．Nagios では，アクセスポイントの状態，また，Cacti では，パケット情報が可視化されている．一方，認証情報に関しては，前節で述べたようにスイッチのコンソールからコマンドを入力し確認する方法しかない．これに対し，認証情報を取得し，html ファイルとして出力し，管理用のウエブページに表示するようなプログラムを実装した．これは，Python およびシェルスクリプトにより実装し，認証が維持される最大時間 30 分の半分の 15 分間隔で cron により自動的に情報を更新する設定である．その結果，最大で，750 ユーザの認証が通っている状況になっている．スイッチで取得できる情報は，クライアントのユーザ ID，MAC アドレス，IP アドレス，接続先ポートである．これらの情報に加えて，コアスイッチの情報も取得して，マッチングを行い利用状況の可視化が行えればよいと考えている．

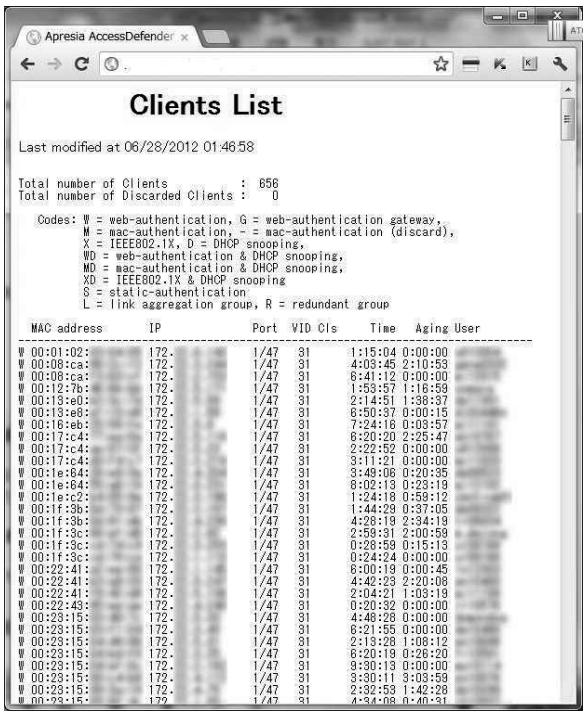


図 7　無線 LAN 認証クライアント一覧

現状では，無線 LAN アクセスポイント経由で認証を行うスイッチのみの情報を取得し，管理ウエブサイトで表示するようになっているが，全体の利用状況を取得することが，ネットワークの利用状況の把握に欠かせないので，無線 LAN セグメント以外のスイッチに対しても認証状況の可視化を行っていく予定である．さらに，コアスイッチの情報とのマッチングをはかり，正確な利用者分布を把握することを目指している．

4.4. 無線 LAN アクセスポイントの syslog 取得

無線 LAN アクセスポイントの syslog に関しては，アクセスポイント本体で保存されているログの取得を試み，アクセスポイントのコンソールでのコマンドの実行結果をローカルにダウンロードするためのスクリプトを開発した．これは，Python のネットワーク関係のライブラリを利用して syslog の取得を行うものである．これを利用して，アクセスポイントでのクライアントの動きが分かるようになる．

また，無線 LAN 認証スイッチ，エッジスイッチ，およびコアスイッチについても取得情報の絞り込みをはかり

5. まとめ

本報告では，無線 LAN アクセスポイントの障害の解析および監視状況について述べた．ネットワークは，状況に把握には，統計データの取得，ログの解析が欠かせない．また，機器単独での情報では，全体がわかりにくいので，統合的に，複数の機器からの情報をまとめて，監視の効率を上げる仕組みを構築していく予定である．また，syslog によるログ収集に関しては，本報告では，触れなかったが，ログ収集だけでなく，ログ解析の部分の強化を図り，障害への対応力の強化を図っていく予定である．

参考文献

[1]内藤郁之，望月源，佐野洋，「オンデマンドおよびスケジュール監視を併用した無線 LAN アクセスポイント監視システムの構築」，第 74 回情報処理学会全国大会，2012 年 3 月

[2]内藤郁之，「無線 LAN 接続環境の安定化」，東京外国語大学総合情報コラボレーションセンター年報　第 6 号, 2012 年

CMS 小テスト問題分析による授業改善の試み

The attempt for the improvement of the teaching approaches based on Moodle quizzes analysis

和田　武 †
Takeshi Wada †

wada@cite.ehime-u.ac.jp

† 愛媛大学総合情報メディアセンター

† Center Information Technology, Ehime University

概要

近年，Moodle（Course Management System）の多肢選択方式等を用いた小テストによる成績評価が数多く実施されているが，作成した設問の内容によっては，正解率に大きな差が生じて正当な評価ができない場合がある．Moodleでは，小テストの結果に対する分析としてアイテム分析機能が備わっており，テストの信頼性の指標を表す識別指数や判別指数を求めることができる．さらにより詳細な分析を行うためにTDAP [1]を用いた項目反応理論に基づく分析[2]など数多くの研究が行われている．

本稿では，今後の設問作成の参考とするために，講義で利用したMoodleの小テストに対して，これらの手法を用い，平均点や標準偏差などの基本統計量を求めて分析する古典的テスト理論および現代テスト理論である項目反応理論やS-P表理論[3]を用いた分析を行い，試験問題の妥当性を検証したので報告する．

キーワード

テスト理論，小テスト，Moodle

1. はじめに

情報系センターは, ネットワーク管理, 学術研究支援, 地域貢献などの情報基盤の統括に加え，情報教育の中核としての役割がある．最近では，センターシステムの教育用システムに Moodle（CMS: Course Management System）を組み込み，情報系センターの教員等が情報基礎教育を担当している大学が少なくない. CMS を用いた授業では, 教材の提示以外に各回ごとの確認問題や期末試験を Moodle の多肢選択方式等を用いた小テストによる成績評価が実施されているが，作成した設問の内容によっては，正解率に大きな差が生じて正当な評価ができない場合がある．そこで，受験者の学習評価や指導内容と学習達成度の整合性などを分析し，試験問題の難易度や受験者の能力値といった特性を定量化する従来からの古典的テスト理論を用いた研究や，項目反応理論やラッシュ測定理論などを用いた現代テスト理論による研究が行われている．

本稿では，今後の設問作成の参考とするために，講義で利用した Moodle の小テストに対して，Moodle のアイテム分析や TDAP による分析および S-P 表理論を用いた分析を試み，試験問題の妥当性を検証したのでここに報

告する.

2. 方法と結果

Moodle の小テスト問題を検証するために，Moodle のアイテム分析を用いる方法，TDAP を用いる方法，および S-P 表による分析を行った.

2.1 Moodle のアイテム分析

Moodle の小テストにはアイテム分析機能が備わっており，(1)ファシリティ指標，(2)識別指数，(3)判別係数などの統計データが古典的テスト理論によって算出される.

(1)ファシリティ指標は，項目容易度とも言い，小テストの受験者にとって設問がどれだけ難しいか簡単かを示す指標であり，今回使用したデータに対しては，全て多肢選択方式の設問で構成されていたので，正しく答えた受験者の割合を示す．(2)識別指数は，弁別力ともいい，受験者間の特性の違いをどの程度正確に捉えられるかを示す指標で，優秀な受験者ほど正答しやすく，そうでない受験者ほど誤答しやすい傾向が顕著な場合にこの項目の指数が高くなる．(3)判別係数は，小テスト全体と設問の点数との相関係数で，この係数が負の設問は，優秀な受験者が間違って回答したことを意味し，優秀な受験生に対してペナルティになってしまうので，このような設問は避けるべきである．判別係数は受験者全体の情報を利用するので，上位中位下位グループ分けの情報を利用する識別指数に比べてより詳細に分析できる.

開始日時	受験完了	所要時間	評点/10	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
2012年02月2日13:05	2012年02月2日13:19	13分44秒	8	1/1	1/1	1/1	1/1	0/1	1/1	1/1	1/1	0/1	1/1
2012年02月2日12:57	2012年02月2日13:02	5分25秒	8	1/1	1/1	1/1	1/1	0/1	1/1	1/1	1/1	0/1	1/1
2012年02月2日12:59	2012年02月2日13:04	5分10秒	9	1/1	1/1	1/1	1/1	1/1	1/1	1/1	1/1	0/1	1/1
2012年02月2日13:00	2012年02月2日13:42	41分54秒	7	0/1	1/1	1/1	0/1	1/1	0/1	1/1	1/1	1/1	1/1
2012年02月2日12:55	2012年02月2日13:01	6分4秒	7	1/1	1/1	1/1	0/1	0/1	1/1	1/1	1/1	0/1	1/1
2012年02月2日13:02	2012年02月2日13:12	10分	6	0/1	1/1	1/1	1/1	0/1	0/1	1/1	0/1	1/1	0/1
2012年02月2日12:56	2012年02月2日13:02	5分48秒	8	1/1	1/1	1/1	0/1	1/1	1/1	1/1	0/1	1/1	1/1

図１．Moodel のアイテム分析

2.1.1 使用データ

今回，Moodle のアイテム分析で使用したデータは，2012 年 2 月に実施した文系学科の担当科目 24 名の期末試験結果の一部である．（図１参照）

表１に今回使用した小テストの出題項目を示す．50 個の設問がブロック(1)から(5)に分かれて出題されている.

表１．　小テストの出題項目

2011年度 法文 試験項目

	ブロック(1)	ブロック(2)	ブロック(3)	ブロック(4)	ブロック(5)
問1	区間推定(2)	ばらつき	クロス集計(1)	クロス集計(4)	ヒストグラム(3)
問2	基本統計量(1)	回帰直線(1)	区間推定(1)	クロス集計(2)	ソーダーチャート
問3	基本統計量(2)	回帰直線(2)	仮説の検定(1)	差がある	回帰直線(3)
問4	外れ値	データの種類	仮説の検定(2)	分散分析(3)	基本統計量(3)
問5	分散分析(1)	正規分布(1)	分散分析(2)	危険率	時系列分析(2)
問6	度数分布とヒストグラム(1)	相関係数(1)	指数平滑化法	中心極限定理	正規分布(3)
問7	度数分布とヒストグラム(2)	相関係数(2)	正規分布(2)	帰無仮説	相関係数(3)
問8	時系列データ(1)	確率分布(1)	分布(3)	母集団と標本	相関係数の有意性検定(4)
問9	棒グラフ	確率分布(2)	t-検定(1)	t-検定(3)	相対参照と絶対参照
問10	Paird t検定	移動平均	クロス集計(3)	スマホのセキュリティ	乱数

(136308) 正答	確率分布(2): 確率分布の記述の中で、誤っているものを選んでください。	確率変数がどのような値になるかを示す分布である。	(0.00)	6/24	(25%)	58%	0.504	-0.20	-0.00
		正規分布、カイ2乗分布、t分布、F分布などが該当する。	(0.00)	2/24	(8%)				
		標準正規分布は、平均が1、標準偏差が0の理論的に設定された正規分布である。	(1.00)	14/24	(58%)				
		正規分布は、連続分布の中で最もよく現れる代表的な分布である。	(0.00)	2/24	(8%)				

図２．　Moodle の設問とアイテム分析結果

2.1.2 アイテム分析結果

図２は，表１のブロック(2)-9（確率分布(2)）の設問とアイテム分析結果を示す. 右欄の７個の係数はそれぞれ，部分点（ここでは選択肢の３番目が部分点１となっているので正解を表す），解答数（24 名中 14 名が正解），解答%，ファシリティ指標（58%），標準偏差（0.504），識別指数（-0.20），そして判別係数（-0.00）を示す．識別指数が負値となった設問は 50 問中図２以外にブロック(2)-問１（バラつきに関する問題）があった．残りの 48 問は識別係数が正の値となり問題は見受けられなかった.

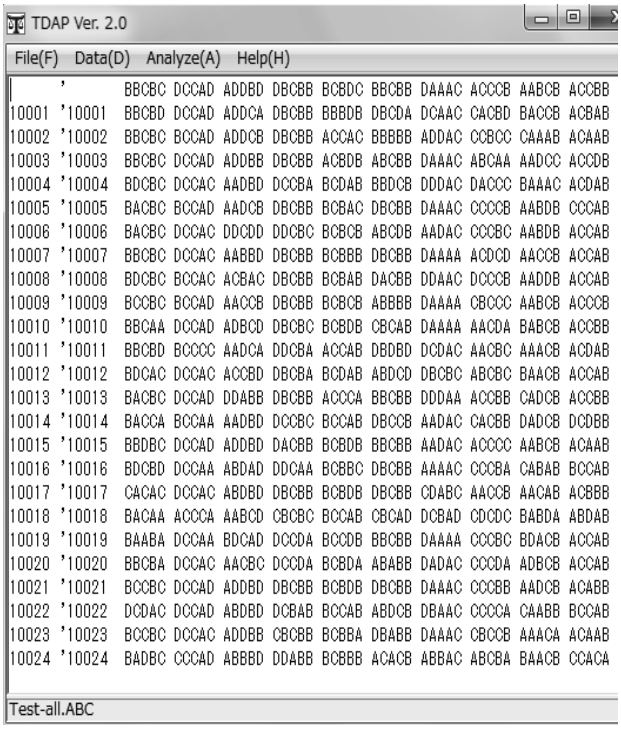
判別係数が負の値をとるのは，成績が良くない学生が良い学生よりも正解数が多いことを示し，このような設問は小テスト問題全体の精度を下げるといわれているので，今後除外すべきである．判別係数が負の値となるのは，図２以外にはブロック(3)-問４（仮説の検定に関する設問②　-0.09），ブロック(5)-問１（ヒストグラムに関する設問（-0.07））の２つの設問であったが，わずかにゼロを下回っていた. 残り 47 問の設問については問題は見受けられなかった.

2.2 TDAP による分析

TDAP(Test Data Analysis Program）は，選択肢問題で構成される小テストの結果データを分析するためのフリーソフト[1]で，基本統計量などの古典テスト理論のみならず現代テスト理論の項目分析や項目応答理論の指標なども求めることができる．

表２に TDAP で使用したデータを示す．これは「2.1 Moodle のアイテム分析」で利用したデータを TDAP で扱えるようにしたものである．A～D は各設問の選択肢を表す．1 行目は正答，2 行目以降は個々の解答データで，左から行番号，受験者番号，そして 50 問の解答データで構成される．

表２． 使用データ



2.2.1 古典的テスト理論

古典的テスト理論によるテストデータの分析には，(1)基本統計量から受験者グループを分析する方法，(2)項目分析により分析する方法などがある．

(1) 基本統計量

従来の基本統計量（グループの平均値，分散，偏差値など）から受験者グループの特性を分析する手法で，受験者グループの大まかな特性を把握するのに便利な分析手法である．これは一般的にも説得力がある方法と言われている．図３は，TDAP より基本統計量を求めた結果の一部である．24 名の受験者の平均点は 50 点満点の 33 点で，最高点が 43 点，最低点が 20 点であり，尖度(Kurtosis)が負の値を示しているので正規分布よりも平坦で分布の裾野が広く，歪度(Skewness)も負の値となっているので左に裾野が広く（右に偏った分布）であることがわかり，比較的今回の試験問題はよくできたといえる．

図３の後半には，標準得点(Standard Scores)が示されている．Z-s(Z Score)は，受験者各自の得点と平均点の差を標準偏差で割った値で，偏差値とも言われており，各受験者の得点が平均点からどのくらい離れているかを示すもので，負の値は平均点よりも低く，正の値は平均点よりも高い度合いを示しているので受験者ごとに成績がわかる．ここで 5s は 5 段階，9s は 9 段階の評定を表している．

```
*** BASIC STATISTICS ***

Name of *.CUT file = Test-all.CUT

Number of examinees ------------    24
Sum of the raw scores ----------   793
Minimum score ------------------    20
Maximum score ------------------    43
Median -------------------------    33
Range --------------------------    23
Mean ---------------------------    33.042
Variance -----------------------    30.623
Standard deviation -------------     5.534
Skewness -----------------------    -0.235
Kurtosis -----------------------    -0.357


*** STANDARD SCORES ***

   * NOTES *
     ID = Identification Number of examinee
     R-s = Raw score,  Z-s = Z-score,  T-s = T-score
     5s = Five point scale,  9s = Stanine scale

     ID    R-s     Z-s      T-s     5s   9s
=========================================
    10001    33   -0.008    49.925    3    5
    10002    32   -0.188    48.118    3    5
    10003    40    1.257    62.574    4    7
    10004    29   -0.730    42.696    2    4
    10005    39    1.077    60.767    4    7
    10006    32   -0.188    48.118    3    5
    10007    39    1.077    60.767    4    7
    10008    34    0.173    51.732    3    5
    10009    35    0.354    53.539    3    6
    10010    37    0.715    57.153    4    6
    10011    26   -1.272    37.275    2    3
    10012    28   -0.911    40.889    2    3
    10013    36    0.535    55.346    4    6
    10014    28   -0.911    40.889    2    3
    10015    42    1.619    66.188    5    8
```

図３．古典的テスト理論（基本統計量）

(2) 項目分析

図４は，項目分析により求めた，①項目困難度(DIFF)，②項目弁別力指数(DISC)，③実質選択肢数(AENO)等の結果の一部である．

① 項目困難度（DIFF）

項目困難度は，テスト項目がどのくらい難しかったかを検討する指標で，正答率とも呼ばれている．0.000 から +1.000 の値をとり，1.000 に近いほど易しい設問で，0.000 に近いほど難しい設問だったと解釈できる．図４では，設問 7,8 が全問正解，0.5 以下が設問 2,10,12 をはじめ 11 問で全体的に易しかった設問といえる．

〈NOTES〉
DIFF = Item difficulty index (p)
DISC = Discrimination power index (r pbi)
AENO = Actual equivalent number of options (k)
ADIF = Appropriateness of difficulty
ADIS = Appropriateness of discrimination power index
AAEN = Appropriateness of actual equivalent number of options
SADIF = Standard appropriateness of difficulty
SADIS = Standard appropriateness of discrimination power index
SAAEN = Standard appropriateness of actual equivalent number of options
SATOT = Standard appropriateness total
RANK = Rank in SATOT order

*** ITEM ANALYSIS SUMMARY TABLE ***

NO.	DIFF	DISC	AENO	ADIF	ADIS	AAEN	SADIF	SADIS	SAAEN	SATOT
1	0.917	0.057	1.411	0.417	0.003	0.895	0.430	0.416	0.557	1.403
2	0.333	0.282	3.780	0.417	0.087	0.948	0.430	0.467	0.584	1.481
3	0.833	0.145	1.723	0.583	0.021	0.818	0.495	0.427	0.519	1.441
4	0.750	0.370	1.964	0.750	0.158	0.736	0.561	0.511	0.478	1.550
5	0.667	0.405	2.356	0.917	0.196	0.786	0.627	0.535	0.503	1.664
6	0.667	0.405	2.415	0.917	0.196	0.820	0.627	0.535	0.520	1.681
7	1.000	0.000	1.000	0.250	0.000	0.000	0.364	0.414	0.110	0.888
8	1.000	0.000	1.000	0.250	0.000	0.000	0.364	0.414	0.110	0.888
9	0.917	0.547	1.332	0.417	0.427	0.722	0.430	0.677	0.471	1.578
10	0.458	0.401	2.784	0.667	0.192	0.683	0.528	0.532	0.451	1.511
11	0.875	0.026	1.578	0.500	0.001	0.860	0.463	0.414	0.540	1.417
12	0.417	0.467	3.444	0.583	0.279	0.891	0.495	0.586	0.555	1.636
13	0.542	0.218	3.059	0.833	0.050	0.896	0.594	0.445	0.558	1.597
14	0.542	0.203	2.956	0.833	0.043	0.851	0.594	0.440	0.535	1.570
15	0.583	-0.207	2.930	0.917	0.045	0.912	0.627	0.442	0.566	1.634
16	0.917	0.275	1.332	0.417	0.082	0.722	0.430	0.464	0.471	1.365
17	0.583	0.388	2.922	0.917	0.177	0.908	0.627	0.523	0.564	1.714
18	0.917	0.356	1.411	0.417	0.146	0.895	0.430	0.504	0.557	1.490
19	0.833	0.185	1.761	0.583	0.036	0.861	0.495	0.436	0.540	1.471
20	0.583	0.541	2.611	0.917	0.414	0.761	0.627	0.669	0.490	1.786

図４．項目困難度，項目弁別力指数，実質選択肢数

② 項目弁別力指数（DISC）

優秀な受験者とそうでない受験者を弁別（識別）できたかどうか検討する指数で, -1.000 から+1.000 の値をとり, +1.000 に近くなるほど弁別力が高いと判断され, 能力の高い受験者よりも低い受験者のほうが多く正答した場合には負の値が算出される．図４では設問 15 が負の値を示しており，その他，設問 21, 設問 39 が負の値を示した.

③ 実質選択肢数（AENO）

多肢選択形式の設問で，用意した選択肢が偏りなく選択されているかどうかを検討する指標で, 0.000 から選択肢の数までの値（今回は４）の値をとる．図４では，実質選択肢数は，設問１から 50 までで，22 問が 2.0 以下となっており，４つの選択肢を用意したにもかかわらず，２つ分の働きしかしていなかった．今後，問題作成の際にはこの点に特に注意が必要である.

2.2.2 項目反応理論

項目反応理論は，項目応答理論とも言われ，テスト問題の特性（例えば，難しさや易しさなど）と受験者の能力との間にある確率的な関係を仮定すれば学力の絶対値が測れるという理論である．ここで項目反応理論について説明する．項目反応理論のモデルには、計算に使用するパラメータ数によって、主に３つのモデルがある。(1) 項目困難度パラメータ（item difficulty parameter=b）のみを想定する１パラメータモデル、(2) 項目困難度パラメータ(b)と項目弁別力パラメータ（item discrimination parameter=a）を含む２パラメータモデル、そして、(3) 当て推量パラネータ（guessing parameter）を含む３パラメータモデルである。TDAP では、以下のモデル式で表される(1)の １パラメータラッシュモデル（ロジスティックモデル）を使用している。このモデルは、パラメータの解釈が比較的簡単で、少ないサンプル（100～200）でも安定した推定が可能である。

$$P_j(\theta) = \frac{1}{1+e^{-(\theta - b_j)}}$$

$P_j(\theta)$ ：θ で表される能力を持つ受験者が、項目j に正答する確率

θ ：受験者能力パラメータ

b_j ：項目 j の項目困難度パラメータ

ここで$-(\theta - b_j)$は、問題の難しさが学力をどれだけ上回っているかを表し、一般的にb_j、θは、それぞれ-3～+3 の値をとり、$b_j = 3$であれば大変難しい設問で、例えば, $\theta = -1.4$であればあまり成績が良いとは言えない学生である。上のモデル式から、学力の値と難しさの値が一致している場合、$-(\theta - b_j)$=0 となり、$P_j = 0.5$ となるので、解ける確率は 50%となる。また、設問の難しさが学力を上回れば上回るほど、ギャップ x が大きくなると分母が大きくなるので、正解率P_jは小さくなるから、正解の確率は低くなる。

この項目反応理論は，教育分野で登場した理論で，試験問題に依存しなくて受験者の能力を適切に測定でき，留学のための語学試験や企業の入社試験などでも利用されている．また，試験問題が適切に出題されたかなど適正レベルを把握することも可能である.

図５は，１パラメータラッシュモデル（PROX 法)を用いた項目反応理論によるテストデータ分析結果の最初の画面である．全設問の初期項目困難度を示している．実際のデータ解析には, 図６の最終項目困難度パラメータ, 図７のモデルとの適合度の検討に焦点をあてる.

図６-１は, 項目反応理論により求められた最終項目困難度（最終能力パラメータ）を表したものである．Item No（設問）7,8 は「All Correct Responses」となっており，この設問は全受験者が正解だったので，この設問では受験者の能力を推定することができないので除外されている．設問が易しすぎたようである．ここで，負の値は平均的な困難度より易しく，正の値は平均的な困難度よりも難しい度合いを示すもので，-3.000 から+3.000 の値を示す.

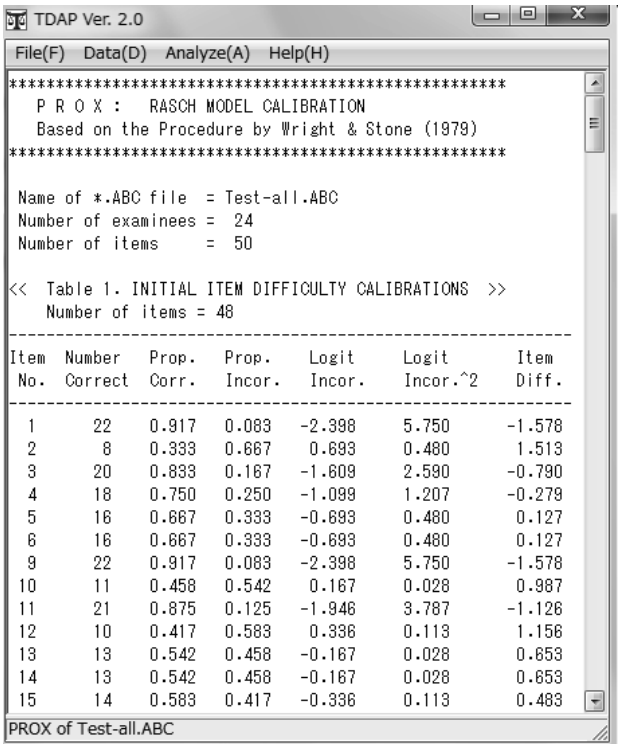


図５．項目反応理論

Expansion factor; Y = 1.083

Item No.	Final Calib.	Standard Error
7	All Correct Responses	
8	All Correct Responses	
1	-1.710	0.769
2	1.639	0.451
3	-0.856	0.570
4	-0.302	0.491
5	0.137	0.451
6	0.137	0.451
9	-1.710	0.769
10	1.069	0.426
11	-1.220	0.642
12	1.252	0.431
13	0.707	0.426
14	0.707	0.426
15	0.523	0.431
16	-1.710	0.769
17	0.523	0.431
18	-1.710	0.769
19	-0.856	0.570
20	0.523	0.431
21	-0.856	0.570
22	-2.509	1.063
23	0.335	0.439
24	1.639	0.451

図６-１．最終項目困難度（１）

図６-１の設問 1, 3, 4, 9, 11, 16, 18, 19, 21, 22 をはじめ計 21 問が負の値を示し，難しい設問だったことを示すが，残りの 29 問は正の値を示したので，設問としてはほぼ妥当だと判断できよう．

図６-２は，最終項目困難度の出力結果（受験者能力値）を示す．「0」は平均的な能力をもつ受験者，負の値は平均より低く，正の値は平均より高い能力を持つ受験者を示す．受験者 10011 は平均的な受験者で，受験者 10018, 10024 は平均より低く，受験者 10021, 10015 は平均より高い能力を有する受験者である．

Expansion factor; X = 1.292

Person No.	Person Measure	Standard Error
10001	0.776	0.343
10002	0.660	0.339
10003	1.725	0.404
10004	0.325	0.331
10005	1.568	0.390
10006	0.660	0.339
10007	1.568	0.390
10008	0.896	0.348
10009	1.019	0.354
10010	1.280	0.369
10011	0.000	0.328
10012	0.216	0.329
10013	1.147	0.361
10014	0.216	0.329
10015	2.080	0.440
10016	0.660	0.339
10017	1.147	0.361
10018	-0.660	0.339
10019	0.435	0.333
10020	0.776	0.343
10021	2.284	0.465
10022	0.216	0.329
10023	1.147	0.361
10024	-0.108	0.328

図６-２．最終項目困難度（２）

<< Table 4. ANALYSIS OF FIT >>

Item No.	Sigma(Z^2)	t
1	26.429	0.488
2	24.618	0.235
3	31.932	1.215
4	20.906	-0.316
5	20.423	-0.391
6	21.382	-0.243
9	10.228	-2.316
10	22.111	-0.132
11	25.888	0.413
12	20.560	-0.370
13	24.684	0.244
14	24.892	0.274
15	32.327	1.265
16	22.222	-0.116
17	23.480	0.070
18	13.850	-1.535
19	20.768	-0.338
20	18.999	-0.619
21	32.243	1.254
22	27.743	0.668
23	17.269	-0.908
24	19.911	-0.472
25	27.938	0.694
26	29.321	0.878
27	20.600	-0.364
28	21.117	-0.284
29	18.125	-0.763
30	15.397	-1.241
31	29.112	0.850
32	19.018	-0.616
33	21.330	-0.251
34	26.429	0.488
35	29.081	0.846
36	27.604	0.649

図７-１．　モデルとの適合度の検討（１）

図７は，PROX 処理を行った全項目と全受験者について，モデルとの適合度の度合いを求めたものである．ｔはモデルとの適合度の度合いを示す値である。t >2 の場合,その項目または受験者はミスフィットと判断される．ミスフィットは，例えば，能力の高い受験者の誤答が多く，逆に低い受験者の正答が多い場合などがミスフィット項目となり，受験者のミスフィットの場合には，例えば，当て推量だけで解答したために，能力パラメータから判断すれば，当然正答してもよいような易しい設問に誤答したり，反対にとても正答できないような難しい設問に正答するなどの場合にミスフィット受験者となる．従って，より正確な受験者能力パラメータなどを算出するためには，このようなミスフィットは除外することが望ましい．図７-１の場合，設問 38 がミスフィット項目に該当した．図７-２では，10017 の受験者がミスフィット受験者に該当した．

一方，ｔ< -2 の場合，オーバフィットと判断されて，例えば，能力の高い受験者が全て正答し，能力の低い受験者が全て誤答する場合など，オーバフィット項目となる．受験者の場合には，ある受験者の解答が，易しい設問には全て正答し,難しい設問には全て誤答するように，モデルが想定しているパターンとのずれが極端に小さい場合などがオーバフィット受験者となる．ただし，オーバフィットの場合には，除外して再計算することはしないが，原因を明らかにして改善していくことが必要となる．図７-１では設問 9, 47 がオーバフィット項目に，図７-２では，10021 の受験者がオーバフィット受験者となった．

Person No.	Sigma(Z^2)	t
10001	60.591	1.317
10002	62.321	1.474
10003	46.083	-0.095
10004	35.081	-1.324
10005	40.285	-0.720
10006	35.376	-1.288
10007	51.535	0.457
10008	40.688	-0.675
10009	29.979	-1.968
10010	41.998	-0.531
10011	41.963	-0.535
10012	37.070	-1.087
10013	54.225	0.719
10014	41.034	-0.637
10015	50.989	0.403
10016	45.538	-0.152
10017	70.128	2.163
10018	48.472	0.151
10019	57.572	1.037
10020	47.543	0.056
10021	21.465	-3.216
10022	52.595	0.561
10023	48.980	0.202
10024	55.731	0.863

図７-２．モデルとの適合度の検討（２）

2.3 S-P 表分析

S-P 表分析（Student-Problem score table analysis）とは，試験問題の結果から，受験者の学習内容や教員の指導法の診断など評価情報を得るために作られた分析方法で，成績順位や得点結果からは見ることが出来ない受験者個々の育成ポイント，指導の改善ポイントなどを教員が判断することができる．

表３．　S-P 表分析

macro	D* = 0.446										
		1	2	5	3	4	6	%	Blank	9	c.s
3	10003	1	1	1	1	1	5	100	0		0
5	10005	1	1	1	1	1	5	100	0		0
7	10007	1	1	1	1	1	5	100	0		0
15	10015	1	1	1	1	1	5	100	0		0
21	10021	1	1	1	1	1	5	100	0		0
10	10010	1	1	1	1	0	4	80	0		0
13	10013	1	1	1	0	0	3	60	0		0
17	10017	0	1	1	1	0	3	60	0		0.67
20	10020	1	0	1	1	0	3	60	0		0.67
23	10023	1	1	0	0	1	3	60	0		1
1	10001	1	1	0	0	0	2	40	0		0
2	10002	1	1	0	0	0	2	40	0		0
4	10004	1	1	0	0	0	2	40	0		0
6	10006	1	0	1	0	0	2	40	0		0
8	10008	0	0	1	0	1	2	40	0		1.5
9	10009	1	0	1	0	0	2	40	0		0
12	10012	0	1	1	0	0	2	40	0		0
11	10011	0	0	1	0	0	1	20	0		0
14	10014	0	1	0	0	0	1	20	0		0
16	10016	0	0	0	1	0	1	20	0		2
19	10019	0	0	0	1	0	1	20	0		2
22	10022	0	0	0	0	1	1	20	0		3
18	10018	0	0	0	0	0	0	0	0		0
24	10024	0	0	0	0	0	0	0	0		0
		14	14	14	10	8	60				
%		41.2	41.2	41.2	29.4	23.5	35.3				
cp		0.04	0.08	0.08	0.17	0.19					

S-P 表作成には，高知県庁ホームページで公開されている S-P 表作成ワークシートを用いた．表３は，50 の設問を 5 ブロックに分け，10 点満点のデータを基に平均点以上を「1」, 平均点以下を「0」として S-P 表を作成した．

Ｓ曲線（実線・青色）は，得点の度数分布を表し，曲線の左側に「1」，右側に「0」が並ぶのが理想型で，受験者の達成状況や学習状況が把握される．このＳ曲線左上の「0」(誤答)は，成績の良い受験者が簡単な設問を間違えているので単なる間違いであり，右下の「0」は内容が理解されていないことに原因があると思われる．また，受験者 10008 は左側に正答がなく，右側に正答があるので，易しい設問ができず，難しい設問しかできていないので，欠席など学習上での問題の可能性が考えられる．

Ｐ曲線（点線・赤色）は，正答数の度数分布を表し，曲線の上側に「1」, 下側に「0」となるのが理想型で，個々

の設問の適切さ，指導の効果などを読み取ることができる．ブロック(1)～(5)の設問は上側の正答数が下側の正答数を上まわっているので，得点が高い受験者は正答し，低い受験者は誤答しているので，設問としては適切と考えられる．

Ｓ曲線とＰ曲線は一般に接近しているが，若干離れているのは，受験者の学習が不十分で学力のばらつきが大きいか，出題問題としての不適切さが考えられる．さらに，曲線と S-P 曲線の乖離は 0.446 と大きくなく，標準的な試験問題といえよう．

なお，表中の CP は問題注意係数を示し，全て 0.2 以下となり，試験問題として適切だと判断された．CS は受験者注意係数を示し，0.5 以上の受験者 7 名が要注意の受験生と判断された．

３．　まとめ

今回，受験者の正当な評価を行うために，Moodle の小テスト問題に対して，古典的テスト理論および現在テスト理論によるテスト問題の分析を行った．その結果，いくつかの課題がみつかった．

まず，Moodle のアイテム分析による分析では，判別係数が負の値となった３つの設問が，また，識別指数が負の値となった２つの設問が見直しの対象となったが，他のほとんどの設問においては，Moodle のアイテム分析では問題は認められなかった．

TDAP による項目分析では，設問 7, 8 が全員正答となり，また，項目困難度が 0.5 以下となった設問 11 個以外の 39 問は易しい設問と判定され，全体的にはほぼ妥当な結果が得られた．項目弁別力指数では，設問 15, 21, 39 が負の値を示し，能力の低い受験者が高い受験者よりも多く正答したと判断され，今後検討が必要である．今回の項目分析で最も課題が明らかになったのは，実質選択肢数が 2 以下の設問が 50 問中 22 問もあり，４つの選択肢を用意したにも関わらず，２つ分の働きしかしていなかったことがわかった．今後，選択肢の問題作成の際には大いに注意を払わなければならない．

現代テスト理論の項目反応理論による分析では，最終項目困難度は 50 問中難しい設問と判断されたのは 21 問だったので，全体としてはバランスがとれた 50 問だったといえよう．一方，モデルの適合度の検討では，ミスフィット項目として設問 38 が該当したので，今後検討を要する．

S-P 表分析では，得点が高い受験者は正答し，低い受験者は誤答しているので，設問としては適切と判断される．

今後は，表１の小テストの出題項目から明らかなように，出題項目とブロックが対応していないので，分野別にまとめる必要がある．また，より多い受験生の小テスト結果について，試験問題の妥当性の検証を行いたい。

参考文献

[1] 中村洋一著，テストで言語能力は測れるか，桐原書店，2004
[2] 竹内俊彦，項目反応理論入門，青山学院大学総合研究所，2006.
[3] S-P 表の入門，佐藤隆博，明治書店.

大学導入教育としての情報教育の実践

Practice of Information Education in "Basic Style Study"

佐々木正人，石黒克也，斎藤卓也，豊永昌彦
Masato Sasaki, Katsuya Ishiguro, Takuya Saito, Masahiko　Toyonaga

高知大学総合情報センター

Integrated Information Center, Kochi University

概要

高知大学では，平成９年度よりノートＰＣ必携による情報教育を実施している．高校での情報教育の実施，インターネット利用環境の普及に伴い，学生は入学時既にパソコンやインターネット利用技術を一定身に付けている．１５年を経過した本学のノートＰＣ必携による情報教育のあるべき姿について担当者間で議論され，それぞれの担当者の裁量で新しい取り組みも始まっている．本発表では，「自分で考える」ことに重点を置いた「情報処理」授業での新しい教育方法の取り組みについて報告する．

キーワード

ノートパソコン必携，情報教育，導入教育

1. はじめに

高知大学では，平成９年度から新入生全員に入学時にノートＰＣを購入してもらい情報教育を行ってきた．主にノートＰＣを使った演習を行う「情報処理Ⅱ (15 回)」とコンピュータやインターネットの仕組み，情報倫理・モラル，セキュリティ対策などを解説する講義「情報処理Ⅰ(7 回)」を必須科目として実施してきた

この取り組みを始めた当初は，多くの学生がパソコンやインターネットの利用経験がなく,「情報処理Ⅱ」では，電源の On/Off の説明から始まり，OS やアプリケーションソフトの操作演習が中心であった．また教える側の負担を最小限にするために，独自テキストを作成し，それに沿った授業展開を行ってきた．さらに，学内に多数の情報コンセントを設置し，授業外での自習を促し，ノートＰＣを利用する機会を増やす努力を行ってきた．

高校での情報教育の実施やインターネットの普及に伴い，大学入学までにパソコンやインターネットの基本操作を習得した学生が増え，平成２０年度からは講義と実習を行う「情報処理 (15 回)」とした．現在では，この取り組みを始めて１５年以上を経過し，本学における情報教育(「情報処理」)の見直しが授業担当者間で議論され，学部・学科に応じた新しい取り組みも始まっている．

総合情報センターでは，「情報処理」の内容に応じた計算機環境やネットワーク環境の整備・充実，各種情報システムの運用支援はもちろん，技術情報の提供，セキュリティ教育，パソコン活用の実践の場の提供，文科系学科の「情報処理」の担当など，当初から情報教育の支援を行ってきた．特に，授業中に解決しなかったトラブル等の対応や利用支援を学生スタッフを中心に行ってきた．

以下では，トラブルや相談で学生と直接関わってきた総合情報センターとして，「情報教育」の今後のあるべき姿を模索し，これまでの全学共通の「情報処理」の内容を踏襲しつつ，「自ら問題に気づき，自ら考え，問題解決のための行動できる」ことを目指した「情報処理」授業での新しい教育方法の取り組みについて報告する．

2. 自分で考えさせるためのポイント

単に知識獲得や操作パターンの習得だけではなく,「自分で考える」ことを実践するため,以下の点を重視した.

2.1. 学生の「情報処理」に対するイメージを変える

第１回目の「情報処理」の授業アンケートで,『「情報処理」の授業内容はどのようなものと考えているか?』に対する回答（図 1）から，78%がパソコン実習を行う授業と考えている．また,『パソコン利用について（自信の有無)』に対する回答（図 2）から，92%が「少し不安」「とても不安」と回答しており，大学ではさらに高度なパソコン操作技術が求められると考えていることがうかがえる．情報処理の授業を通じて「自分で考える」ことを実習するためには，受講学生の授業に対するイメージを変えることが必要である.

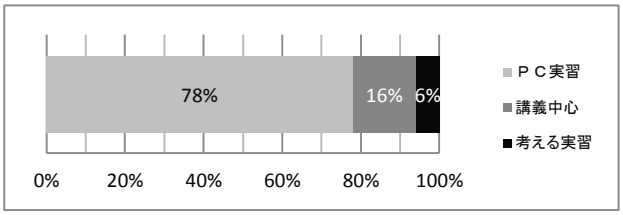


図 1　授業内容

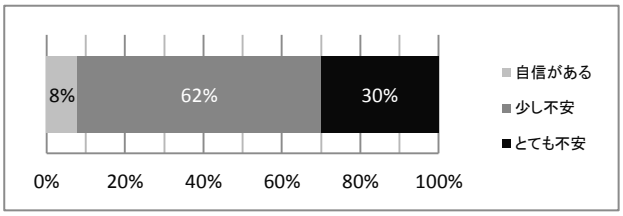


図 2　パソコン利用

このため，検索サイトで検索してもヒットしないような，すぐに正解と判断できないことを考えさせることから始める．同時に，自分なりに分かったという感覚を思い出させ，考えた結果「分かった！」の瞬間を体験させる（Aha!体験）.

また，パソコンの操作を教える際も，いきなり操作方法をプロジェクタに投影し学生に同じ操作をさせるといった講習会方式ではなく，まず「何をやろうとしているか(目的)」,「そのために必要な処理の概要（処理概要)」,「具体的な操作方法（方法)」の順に徐々に具体化しながら，全体像を説明した上でパソコン操作をさせるように心がけた．この際は，全体のどの部分を実施しているのかを常に意識させ，目の前の操作のみに集中しないよう配慮した．さらに，処理が終了したら，目的が達成できているかのチェックを徹底させる.

このように，常に操作の全体像を意識させ，操作方法のみ覚えることが無いよう配慮し,「操作を覚える」から「考えて操作（行動）する」という練習（実習）を繰り返し行う.

2.2. 常に問題意識を持たせる

『生協の食堂のメニューはあまり変わらない』といった文章をいくつか示し，全員に『あなたにとって情報はいくつあったか?』に回答させ，個人により異なることを実感させる.『あなたにとって「情報」とは何か?』に対して言葉で回答できる学生はほとんどいない．この問いに対する回答を最終回の授業の際に提出してもらうこととし，それまでの間,「何が」,「どのような状況」で情報になるかを常に考えさせる課題を出す．もちろん広辞苑や国語辞書で調べたり，紹介した参考書での「情報」の定義を調べさせた上で最後に自分の言葉で表現させる.

2.3. やりっぱなしは厳禁

授業中のパソコン操作でのフィードバックはもちろん,前回提出の課題の評価，授業終了時にその日のまとめを毎回実施させる．特に課題については，他学生の提出物を見せながら（もちろん提示の際には誰のものか分からないよう配慮）自分自身で評価・修正させる．高校時代では他学生のアウトプットを見る機会が少ないため，自分と他学生との違いから何かに気づくことを体感させる.

2.4. 息抜きのブレイク

常に問題意識を持ち，考えながらパソコンを操作すると９０分間集中できない．そこで，中間で「ブレイク」（表１）を入れる．視覚の話題や注意を向ける能力の限界などできるだけ五感を通じて体感できる話題を選んでいる．また，コンピュータやインターネットの仕組みを学習する前にゲーム・クイズ感覚で参加できるよう配慮する.

①Aha!体験
②注意を向ける能力の限界
③視覚の不思議
④内緒話は難しい
⑤仲間外れはどれ？
⑥キーボードからの入力・表示を人間がやってみる
⑦紙に高速で交わらないようにたくさん線を引く
⑧錯視・RGB

⑨魔方陣
⑩伝言ゲーム
⑪PDCA を考える
⑫コンビニで昼食を購入する（最適化を考える）

表 **1** ブレイク一覧

3. 主な授業内容

本学のノートＰＣ必携による情報教育（「情報処理」）では，以下の内容を必ず教えることとなっている．

1．**情報活用の実践力**
道具としての情報機器やシステムの利用技術の習得

2．**情報の科学的理解**
情報機器やシステムの原理及び情報科学の基本概念の学習

3．**情報化社会に参画する態度**
情報技術が我々の生活や社会に与える影響及び情報を扱う際のモラルや倫理の学習

本授業では，日々の知的な活動をまず考え，さらにどの場面でパソコンやインターネットが利用できるかを考え，実際にやってみる授業構成とした．その後どのように利用するかは各自で考えさせる．

3.1. まずは準備から

本学では，2011 年度から新入生も各自のノートＰＣを利用して Web 履修登録を行っている．情報処理の授業開始前に履修登録するため，別途準備会を行い事前に必要な設定やウイルス対策ソフトの導入を行っている．本授業では，授業開始前に各自に資料を渡しこれらの作業が確実にできているかどうかを確認させている．自分のＰＣは自分で管理することを強く意識させる．

3.2. 自分にとって情報とは？

「情報とは何か？」を考えることから始める(2.2 参照)．また，個別の具体的事象から全体像をイメージさせ（モデル化），現実との違いからモデルを修正・強化することなど，違うが分かるにつながることを実感させる．さらに，パソコン操作における心得（①何をするために[目的]，②どのような手順で[概要・シナリオ]，③具体的にどうする[方法]，④目的が達成できたか[フィードバック]）に沿ってパスワードの変更処理や TeraPad のインストール，Thunderbird のインストールと利用等を実習する．また，生まれてからこれまでの出来事を，Terapad を使って入力させる（課題名：「私史」）．もちろん行の移動や文字編集，ファイル操作，タイピング練習を兼ねている．各自で眺めて，自分のキーワード（少し抽象的な表現．「古風」「大和撫子」など）と，キーワードを繋げたり，さらに抽象的な表現を加えたりしてキャッチフレーズも考えさせる．最後に，キーワードやキャッチフレーズを取り入れながら自己紹介文を作成する（300 字程度）．

3.3. 相手に自分の考えを正確に伝えるには？

文書を読んでどのように全体を把握しているのかについて考える課題を行う．あらかじめ準備した４種類のシナリオを見て，もっとも具体的イメージが湧いたものを選択しタイトルを付ける．イメージをより具体化し箇条書きで付け加える．このタイトル，シナリオ，箇条書きからなる文書（アウトライン）で，自分の考えが正確に伝わるかどうかをチェックし，不明瞭なところを修正する．ここでは，このアウトラインをどのように構成・表現するかが重要（皆違う・自分ならでは）であり，完成すればパワーポイントやワードでは操作（皆同じ）に専念できることを実感させる．

3.4. 複数人で共通のミッションを遂行するには？

目的，内容，最終提出物および提出期限を説明した資料のみをほぼ初対面の３名のグループに渡し，それぞれのグループでグループワークをさせる課題を行った．これまでグループワークの経験は一定あるが，その具体的な内容が指示される場合がほとんどである．

課題の内容は，『米国の中・高校生（指導者も対象）向けに作成された人間の知覚等に関する実験・解説文（英文）を訳し，実際に実験機器の製作・実験実施・自分なりの見解も含めたまとめを行って発表する．』というもので，最終提出物は，Ａ３用紙１枚にまとめた文書（後日ポスター発表し受講者，先輩，教員等が評価）と実験風景等を撮影したビデオである．必要な材料は，グループ連絡係から連絡してもらい提供するが，実験機器の製作から実験まですべて自分たちが手作業で行う．

パネル発表会で，他グループの優れいている点を見つけさせ，最も優れたグループの番号とコメントを投票させる．さらにその結果を参考にして，授業 SA に協力してもらって評価（評価項目別に点数化）し，最優秀賞，優秀賞，チームワーク賞，特別賞（計１１グループ）を決定する．受賞したグループの報告書との違いをグループメンバ間で議論させ，次回への改善点を考えさせ報告させた．

3.5. 最適な問題解決を行うには？

与えられた条件・制約により，問題解決のための解が異なることを実感（ブレイク）させた後，２つの課題を実施する．

１つ目は，無作為に選んだ職業をインターネットで調べ，3.2 の「私史」課題で作成したキーワード，キャッチフレーズ，自己紹介文を参照してエントリ文章を作成する．求められる能力・人材等を考えさせ，それに沿って自分をアピールする文章を作成させる（300 字程度）．就職活動の経験のある先輩に出来のいい作品を選んでもらい，自分のものとの違いを考えさせる．

２つ目は，１つ目の課題をさらに進め，自分が将来やりたいと思う職業について調べ，必要な資格や準備，その業界の将来性，自分のウリなどを盛り込んで５年後の自分を想像させながら文書にまとめる最終課題を行う．この課題は以前から行っており，１年生当時のことを振り返る際に参考になると好評である．

4. アンケート結果

最終授業においてはアンケート調査を実施（ほぼ同じ内容のアンケートを初回にも実施）した．以下，そのいくつかについて報告する．

『「正解の無い問題」に自分なりの考えが持てるか』の問いに対して，「持てる」の回答が，授業当初の 18%から 60%に増加しており（図 3），「正解を探す」から「考えて自分なりの答えを考える」意識が出てきたと期待できる．

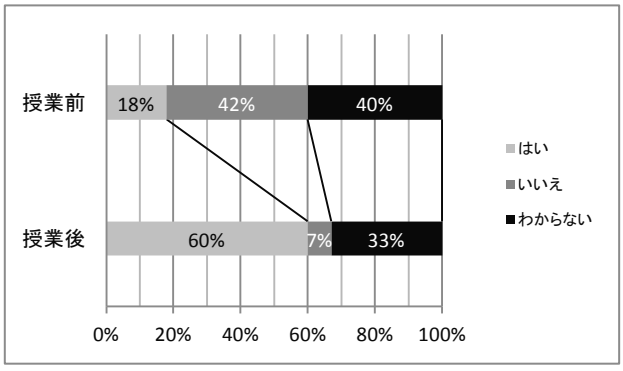


図 3　正解の無い問題に対する考え

『自分の行動を後から評価・改善できるようになったか』の問いに対して，74%ができるようになったと回答しており（図 4），授業で繰り返し実施させた効果があったと思われる．このことは，課題の評価を行った授業後の授業コメントでも，反省点やその改善点を書く学生が多いことからも分かる．

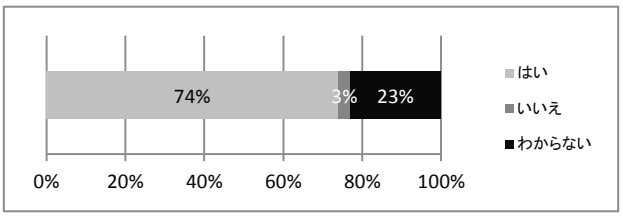


図 4　自分の行動に対する評価・改善

『アウトプットしようという意識が持てるようになったか』の問いに 72%が持てるようになったと回答しており（図 5），その積極性が今後が期待される．

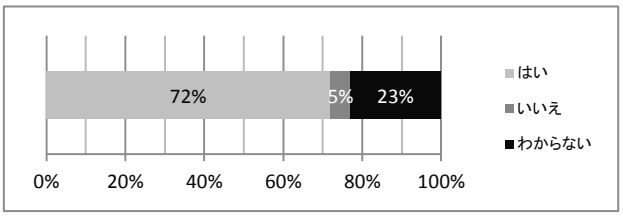


図 5　アウトプットの意識

『他人との違いから自分自身について何か発見があったか』では，「発見があった」が授業当初の 23%から 77%に増加している（図 6）．課題終了の度に他学生の作成したものを見せ，評価させることで「違うが分かるにつながる」が体感できたものと考える．

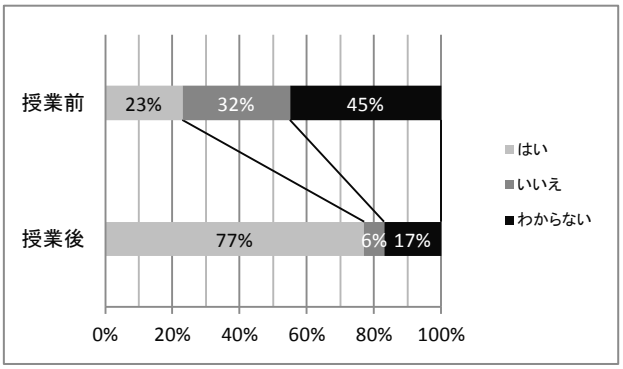


図 6　他人との違いからの発見

5. まとめ

全学共通の内容を踏襲し，自分で考えることを重視した新しい教育方法で「情報処理」を実施した．アンケート結果によれば，単なる知識獲得学習だけでなく，正解が無い問題も考え自分なりの考えをアウトプットすることの重要性は理解できたと思われる．今後は，授業教材や指導方法をさらに改善すると同時に，授業後の追跡調査，効果の検証方法についても検討する予定である．

大分大学医学部キャンパスのネットワーク運用ポリシーとシステム構成について

Network policy of Oita university medical school, and their implementation

島岡章，板倉紀子
Akira SHIMAOKA, Noriko ITAKURA

shimaoka@oita-u.ac.jp, itakura@oita-u.ac.jp

大分大学学術情報拠点（医学情報センター）

Oita University Medical Information Center

概要

医学部は附属病院を持っており，ユーザのパソコンに患者情報を保有していることが多く，また職員の異動が多いため，より厳格なセキュリティ対策が必要である．ここでは，大分大学医学部キャンパスのネットワーク運用ポリシーと，それを制定した背景，それを実現するに至る経緯，技術的に実現することができるようになったシステム構成について検討する．

キーワード

ネットワークポリシー, マルチステップ認証，パソコンのセキュリティ

1. はじめに

かつての大学のネットワークは，インターネットに開かれたネットワークであったが，近年の情報セキュリティや情報漏えい防止の高まりの中で，キャンパスネットワークでも，ファイアウォールを設けてインターネットの脅威から防御し，キャンパス内部でも，Web 認証や MAC アドレス認証などの制限をかけるようになってきている．大分大学医学部（旧大分医科大学）では，以前から厳格なセキュリティポリシーを設けてキャンパスネットワークの保護に努めている．その背景とそれを実現するために行ってきたシステム的な仕組みについてご紹介する．

また，ポリシーを厳格にすれば，必然的に，ユーザにもセンター業務への負担も大きくなる．その負担を軽減するための対応についてもご紹介する．

2. ネットワーク運用ポリシー

(1) ネットワークやシステムを利用するものは申請を出して許可を受けること．

(2) ネットワークに機器を接続する場合は，申請を出して許可を受けること.
(3) ネットワークに接続するパソコンは，セキュリティ対応をすること.
(4) キャンパスネットワークをインターネットの脅威から防御すること.

3. ポリシーの背景

3.1. 医学部の特性

大分大学は，教育福祉学部，経済学部，工学部と本部事務局が位置する旦野原キャンパスと附属小中学校，特殊支援学校が位置する王子キャンパス，病床数 604 床の附属病院を有する医学部の挟間キャンパスからなる，学部学生数が 5,035 人の地方大学である.

医学部は,他学部と比べると,次のような特性がある.

- 学生数に比して職員数が多い（図１）
- 非常勤職員が多い.（図１）
- 職員の異動が多い.（図２）
- 人事異動（退職，採用）があっても，大学とのつながりが継続している人が多い.
- 病院情報システム，医療情報部門が存在している. 24 時間オンコールサポートが通例となっている.
- 患者の情報をパソコンに保存しているユーザが多い.
- 情報センターのスタッフが少ない，あるいは医療情報部門が兼任している.
- ウイルス感染事例が多い.

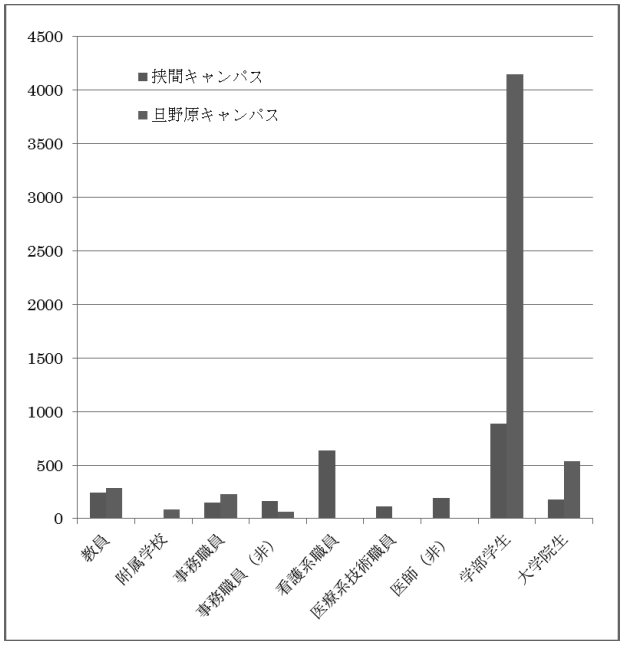


図１．職員数と学生数

3.2. ポリシーの運用の経緯

1995 年の学内 LAN 開設当初から，キャンパス内部はプライベートアドレスを使用している．そのため，インターネットとの間にはファイアウォールを設置して，プロキシサーバを経由してアクセスを確保している.

当初からグループウエアを導入し，ほぼ全職員と全学生にメールアドレスを交付しており，また，組織名や職名アカウントも交付し，古くから，事務連絡はメール（メーリングリスト）で行われている. ユーザアカウントは，このグループウエアにアクセスするためのものであった.

2001 年からユーザ登録申請，端末設置申請をオンライン化し，ユーザに利便性を提供している．申請情報は，センター管理者宛に，サーバに登録するバッチコマンドとともにメールで送信され，管理者の業務軽減，操作ミスの防止につなげていた.

2007 年からは，統合認証システム（コムネット社アカウントマスター） を導入した. アカウントマスターは，ユーザから紙で申請を受けて，管理者が Web 画面に手入力をする仕組みであるため，オンライン申請からメールでバッチ登録用の CSV ファイルを送る方法を取った.

2009 年には，アラクサラスイッチの機能を使って，マルチステップ認証を開始した．この時は，アカウントマスターが MAC アドレスを扱えなかったので，アラクサラに直接 MAC アドレスを登録した．また無線 LAN(Meru)はアラクサラをスルーするため，無線接続する機器の MAC アドレス認証のために，別途 Radius サーバを立てて，この Radius サーバにも MAC アドレスを登録した．登録用のコマンドを，管理者宛の申請メールに記載したので，入力ミスは防げたが，センター業務は著しく増えた.

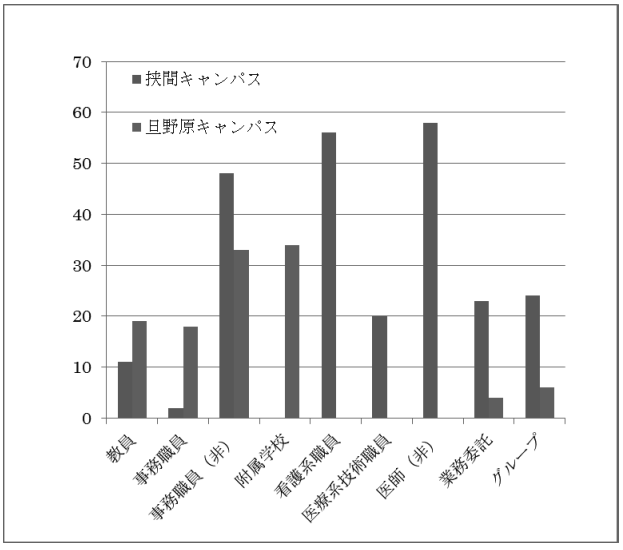


図２．新規ユーザ登録数(2011 年度)

4. セキュリティポリシーの実現に向けて

4.1. ファイアウォール

基本的には, 学内 → 学外は, http, https, ftp のみ通し, 学外 → 学内には, 公開する Web サーバあてにリバースプロキシを経由する http, https のみしか通さない．キャンパス間の業務用通信やサーバ間通信など，必要な場合には，ファイアウォールの穴あけをしている．

4.2. プロキシサーバ

キャンパス内部からは, http, https のみ通すプロキシ(squid)を経由しないと，外部へのアクセスはできない．後に述べるように，ネットワークアクセス時に，Web 認証と MAC アドレス認証を導入したので，学内サーバにアクセスできないゲスト用のプロキシを準備している．

4.3. 統合認証システム

統合認証システムは，新規登録時に，所属に応じて，デフォルトのアクセス権限を設定し，メールサーバ，ファイルサーバ，グループウエア，LDAP サーバへの登録処理が自動的に行われる．AlcNetacademy，WebClass，教務情報システムは，統合認証が行われるが，ユーザ登録は手動で行われている．給与システム，業務可視化システム，物品請求システム，教員業績データ登録システムは，統合認証に参加していない．サーバ，システムのアクセス権限は，変更申請により追加削除する．

職員の新規登録は，本人からのオンライン申請を受けて対応している．これは，人事からの採用情報では，すでに登録済みの人が多数存在するからである．

学生は入学時に全員登録し，オリエンテーションで配布している．学生用パソコンへのログインは，統合認証により行われ，ファイルサーバに保存された個人プロファイルとＺドライブの割り当てが行われる．学生用プリンタの印刷管理，一部の部屋の入退室は，統合認証と連携した Felica カードで認証している．

ユーザ認証を開始したことにより，学外からのお客さんや短期滞在者がネットワーク接続ができなくなったため，ワンディアカウントと短期滞在者用ゲストＩＤの２種類のゲスト用アカウントを準備している．ワンディアカウントは，大学職員が，オンラインで認証後に，リアルタイムに発行を受けることができ，その職員の責任で学外者に利用してもらう仕組みにしている．

4.4. MAC アドレス認証

2012 年 6 月から，MAC アドレス認証方式を変更し，アラクサラから，Radius サーバ経由で，統合認証システムで管理する LDAP サーバに問い合わせを行う方式とした． MAC アドレスの登録は，統合認証システムの新規機能として追加した．

ノートパソコンやスマートフォンのように移動する端末であっても，認証後にユーザごとに設定された VLAN に入り，Meru のシングルチャンネルの仕組みとともに，キャンパス内のどこに移動しても，パソコンの接続性は保持される．

プリンタやＮＡＳなど，ユーザ認証ができない機器には，固定 IP アドレスを付与し，統合認証サーバに認証除外機器として登録している．

学外からのお客さんが持ち込んだパソコンでインターネットにアクセスできるように，学内のサーバやパソコンには接続できない，ゲスト用 VLAN を準備している．また，職員学生が新規にパソコンを購入した際に，MAC アドレスの登録がないためネットワークに接続できず，初期設定やセキュリティ更新ができない状態になるが，その際にも，ゲスト用 VLAN を使うようにしている．毎日認証をするように，MAC 認証の有効時間を 16 時間としている．

4.5. マルチステップ認証

図３に示すように，アラクサラのマルチステップ認証を利用し，Web 認証と MAC アドレス認証の両方を通過したパソコンだけがネットワークに接続できる仕組みとしている．認証情報は，統合認証システムの LDAP サーバに問い合わせするようにしている．

ゲスト用の接続ルートを準備していることは既に述べたとおりである．

4.6. ユーザ登録，MAC アドレス登録の省力化に向けて

統合認証システムとオンライン申請を結合して，センター業務が削減できるようにした．これについては，本研究集会で，板倉が発表する[4].

4.7. ネットワークに接続するパソコンのセキュリティ要件

2011 年 8 月から，セキュリティ対応が行われていないパソコンは，キャンパスネットワークへの接続を許可しないこととしている．

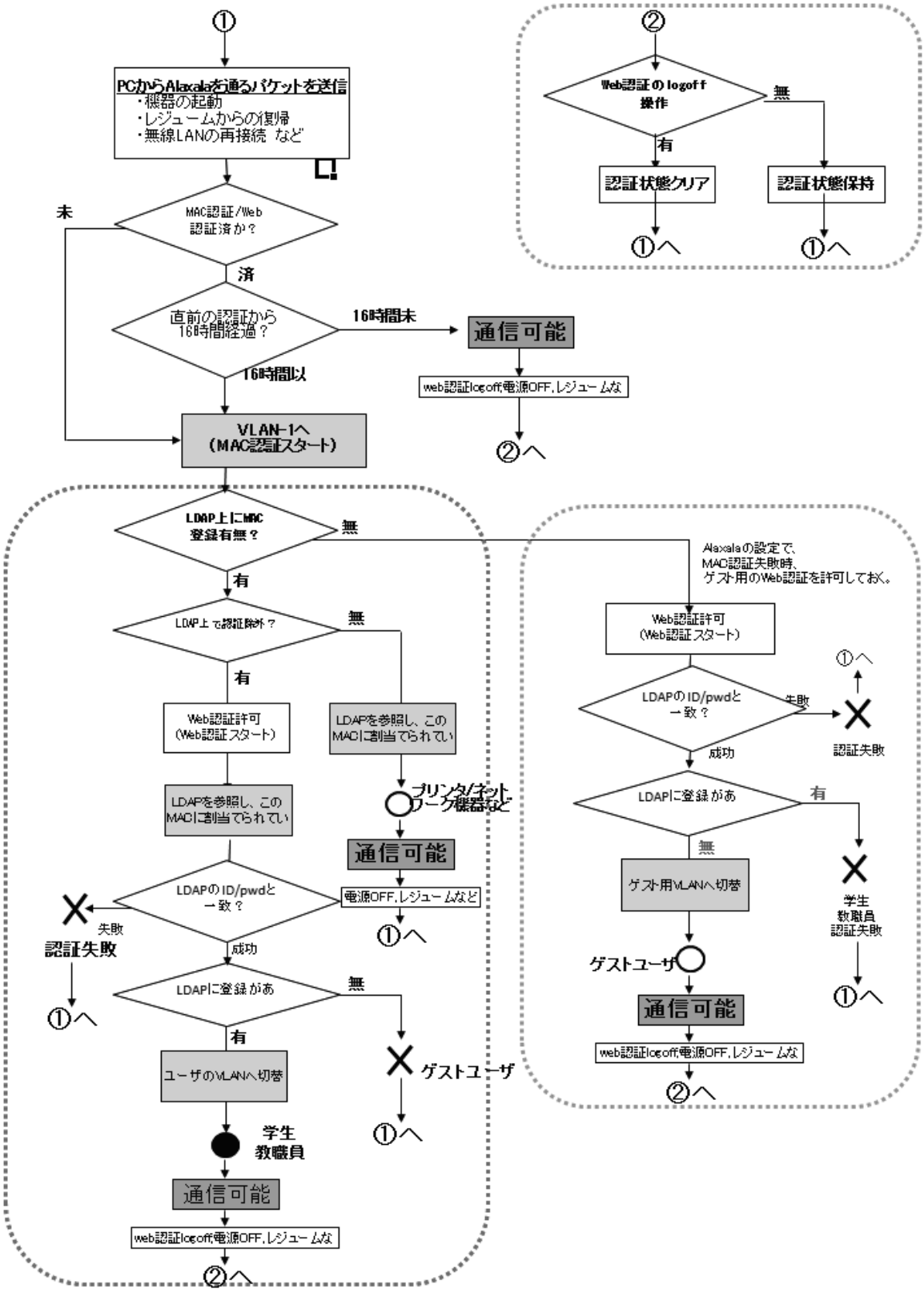


図３．マルチステップ認証の処理フロー

その条件は，ＯＳ，Office, Adobe Reader, Flash Player などのアプリケーションのセキュリティ更新を(自動的に)行うことと，ワクチンソフトのインストールを必須としたことである.

セキュリティ更新のしかたの周知とパソコンのそれらの更新日付の調査を行い，メーカーからセキュリティパッチが提供されなくなった古いＯＳのパソコンは，接続許可を取消した.

ワクチンソフトは，職員学生の私物のパソコンも含め

て無償提供している．登録された MAC アドレスに対して，１回だけダウンロード可能としている．

5. 現在のシステムの問題点と今後の課題

MAC アドレス認証と Web 認証を併用している大学[1][2]や，認証 VLAN を導入している大学[2][3]からの報告があり，これらを参考にしながら，ネットワーク運用ポリシーの実現に努めてきた．

現在利用しているアラクサラのマルチステップ認証は少し無理があるので，次の更新までには，よりスマートな認証方式がとれるように検討したい．

本学では，申請はオンラインで受けているが，他大学では，計算機利用負担金の支払いの名残りがあるせいか，印鑑のついた書類を提出させることが多いようである．本学ではオンライン申請の際に，所属長の承諾を得たかというチェックボックスを設けて，「はい」と答えないと申請を受け付けない仕組みにしている．また許可メールは，所属する講座等にも送付している．情報センターでの事務手続きに，情報システムを使わないのは，どうも理解できないところである．

パソコンのセキュリティ対応状況については，自己申告に頼っているので，今後は，パソコンのＯＳやアプリケーションのバージョンを自動的に収集する仕掛けを導入したいと考えている．

病院情報システムは，ウイルス侵入防止，情報漏えい防止の観点と，電子カルテの普及に伴う病院情報システムの重要性の増大から，インターネットやキャンパスネットワークから切り離される傾向にある．病院情報システムの利用者が要求する，不具合が発生した機器やシステムの短時間での復旧（24 時間 365 日サポート）は，基盤情報システムでも理想的ではあるが，情報センターの少ないスタッフ＋業務委託では現実的に対応できるものではない．

他学部と異なり，医学部ユーザは，医療情報部門のオンコールサービスに慣れているので，対応する情報センターのスタッフには心労をかけている．

ユーザにも使いやすく，センタースタッフの負担も少なく，しかもセキュリティの向上につながる仕組みを検討していきたい．

参考文献

[1] 谷内田昌寿，白清学，”MAC アドレス認証と Web 認証併用キャンパスネットワークの導入”, 学術情報処理研究，No.14，pp. 140-143，2010.

[2] 岡山聖彦, 山井成良, 大隅淑弘, 河野圭太, 藤原崇起, 稗田隆，”岡山大学における認証・ロケーションフリーネットワークの構築”, 学術情報処理研究, No.15, pp.161-165, 2011.

[3] 内田奈津子，因幡哲男，”フェリス女学院大学におけるネットワーク認証システムの構築”, VIEW POINT, No.10, pp.86-90, 2010.

[4] 板倉紀子，島岡章，小谷明義，吉田和幸，”ユーザと機器のオンライン申請、登録、認証システムの開発とその運用について-- センター管理業務の削減の観点から –“，（本年の学術情報処理研究集会にて発表予定）

ユーザと機器のオンライン申請，登録，認証システムの開発と その運用について -- センター管理業務の削減の観点から --

Development and operation of consecutive online system, from user/PC application, LDAP registration to user/PC authentication. -- To reduce administrative costs --

板倉紀子*[1]，島岡章*[1]，小谷明義*[2]，吉田和幸*[3]

Noriko Itakura*1, Akira Shimaoka*1, Akiyoshi Kotani*2, Kazuyuki Yoshida*[3]

*[1] 大分大学医学情報センター
*[2] 株式会社コムネット
*[3] 大分大学情報基盤センター

*[1] Oita University Medical Information Center
*[2] Comnet co., LTD.
*[3] Oita University Information Technology Center

概要

大分大学挾間（医学部）キャンパスでは，学内 LAN を利用する際に Web 認証と，MAC アドレス認証を併用したマルチステップ認証を行っている．本稿では，ユーザの利便性を高め，センターの管理業務を軽減するために，ユーザとパソコンの両方の申請について，ユーザはオンラインで申請を行い，メールでセンターに通知され，センターでは，Web 管理者画面で操作すると LDAP サーバや各種サーバに自動的に登録が行われ，申請者あての許可書の印刷や許可メールの発送までの一連の作業を行うことができるシステムを開発したので，その概要と運用経過について報告する．

キーワード

センター運営業務の軽減，オンライン申請，Web 管理画面，Mac アドレス認証, Web 認証

1. はじめに

近年，キャンパスネットワークのセキュリティを高めるために，MAC アドレス認証，Web 認証を合わせたマルチステップ認証を導入している大学があり[1][2]，大分大学挾間（医学部）キャンパスでも，許可されたユーザ・許可された機器のみが学内 LAN を利用することができるというポリシーを実現するために，マルチステップ認証を導入している[3]．それぞれの認証を行うためには，ユーザアカウントと，接続する機器の MAC アドレスに

ついて，ユーザからの申請を受けて，認証サーバに登録する必要がある．従来のセンターの申請処理は，オンラインの申請画面で入力されたデータをセンターがメールで受け取り，それぞれのシステムへの登録処理をバッチ登録で作業をしていた．登録作業を行うにはそれぞれのシステムのサーバや通信機器にログインしコマンドを実行する必要があるため，作業するセンター職員が固定化してしまい，ユーザへ利用許可を発行するまでの時間を要するという課題があった．

ユーザからの申請をオンラインで受けている大学もあるが[4]，センター業務を一元管理するシステムに関する報告は見当たらない．

そこで，このような課題を解消するために，申請から登録までの一連の処理をオンラインシステム化し，Web管理画面から操作できるようにして，センター職員の業務改善を図ることとした．システムを改善するにあたっては，センター職員の誰もがどの処理作業でもできること，作業量が軽減し，尚且つ確実な処理が求められた．

2. システムの概要

2.1. システム構成

本システムで使用しているサーバは，すでに稼動中であるコムネット社のアカウント管理システム（アカウントマスター）の DB サーバ，LDAP サーバと，申請画面を搭載している Web サーバがある．Web サーバには Apache2.2.3 , PHP5.1.6, Mysql5.5.1 がインストールされている．

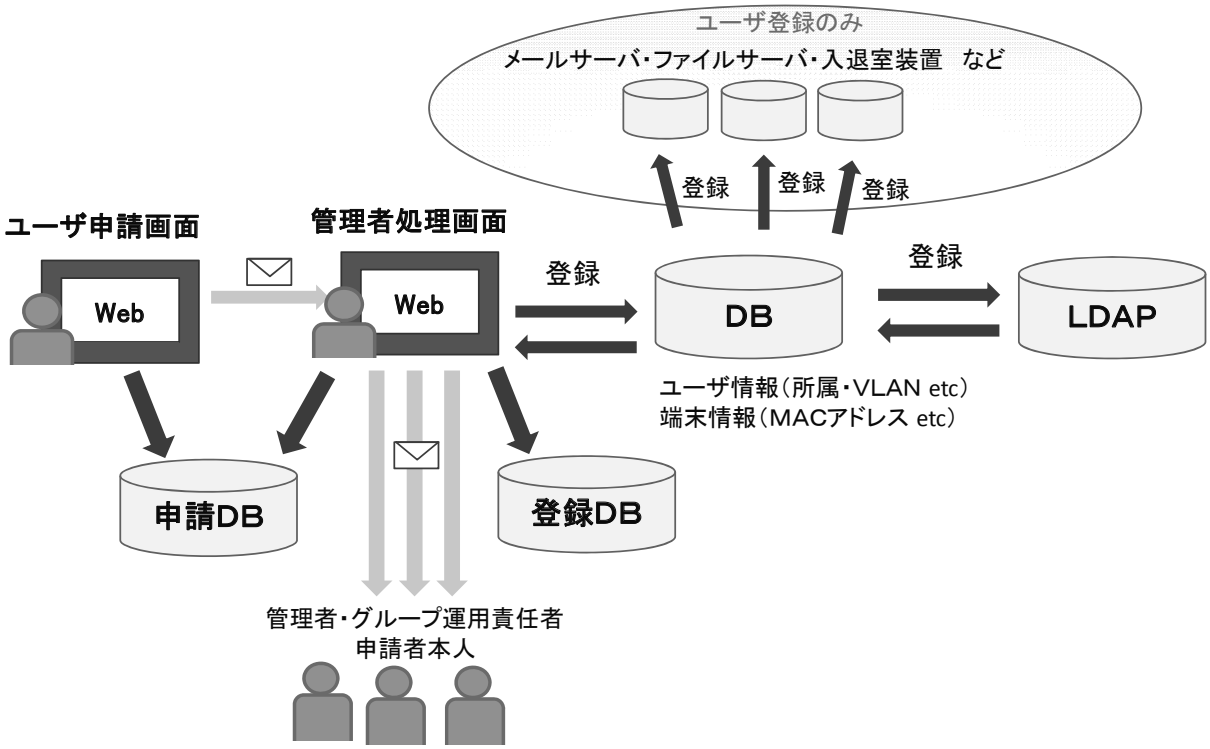


図１．ユーザ・機器登録の流れ

図２．管理者Ｗｅｂ画面

2.2. ユーザアカウント申請処理の構成

ユーザアカウント申請には「新規」「変更」「廃止」の３種類がある．ユーザが申請して処理が完了するまでの流れは共通している（図1）.

ユーザが申請をすると申請 DB に申請内容が保存され，通知メールがセンター管理者に届く．管理者は通知メールにある URL から管理者画面にログインする．管理者画面に表示された申請データを確認し，在籍確認・職員番号入力・重複登録確認を行い，登録ボタンをクリックする. 登録ボタンをクリックすると，認証サーバへの DB, LDAP サーバに登録され，各種サーバ・システムへの登録処理を自動的に行い，申請 DB にあるデータは登録済み DB に保存される．登録後に申請者本人・所属グループ･センター管理者に完了通知メールが自動送信される．登録したデータは申請 DB から削除され，登録日時，作業者, コメントの履歴を記録して登録 DB へ移行される．データの動きは管理者画面で確認することができる.

新規登録時には，ユーザアカウントの所属に応じて，VLAN と複数のシステムへのアクセス権限が自動的に与えられる．変更申請時には登録内容の変更と同時にアクセス権限の追加・削除の申請を行うことができる.

2.3. 端末申請処理の構成

端末申請には「パソコン用」「固定機器用」「LAN アダプタ用」，これに共通の「変更」「廃止」の５種類ある．端末申請には大きく分けてパソコン等の認証機器とプリンタ等の認証除外機器があり，それによって入力項目も変わってくるため，申請画面を分けている．申請の流れはユーザアカウント申請とほぼ同じで，申請が届くとセンター職員が管理者画面にログインし，申請内容を確認する．内容に問題なければ登録ボタンをクリックする．同時に DB と LDAP に登録処理が行われ，自動的に申請者・所属グループ・センター管理者に通知メールが自動送信される.

基本的な登録の流れの他に管理者画面にある機能を紹介する.

(1) 申請却下

申請者が誤った申請をした場合や内容に不備がある場合は却下理由を入力し，却下ボタンをクリックすると申請者本人とセンター宛に却下通知が送信され，申請

DB から削除される.

(2) 保留

申請内容を確認するために問い合わせ対応中の申請の場合は誤って他の職員が処理を進めてしまわないように対応中の状況を入力し，保留ボタンをクリックすると，申請未処理一覧に赤く表示される.（図２）

(3) 検索・変更・削除機能

登録中の機器を検索・変更・削除することができる.

(4) 登録中データの抽出

登録 DB にあるデータを CSV で抽出できる.

管理者画面以外にもユーザ向けに，登録内容を確認することができるように，登録内容検索画面が公開されているおり，ユーザアカウント・MAC アドレスから登録中の機器をいつでも確認することができる.

3. 運用状況

3.1. ユーザアカウント申請処理の業務の変化

システム導入前のユーザアカウント登録は，主に以下の作業が発生していた.

(1) メールで申請内容を受け取る
(2) 各種システム用バッチファイル実行用 CSV データ作成
(3) 定期的（10 分間隔）に登録用バッチファイルが実行される
(4) LDAP にユーザ VLAN を設定する
(5) 申請翌日に許可書を印刷

システム導入後は，申請をメールで受け取り，管理者画面にログインして申請内容を確認し，登録ボタンをクリックする．新規登録の場合は登録完了画面に印刷用ファイルが表示され許可書を印刷する．変更・廃止申請の場合は登録ボタンをクリックすると自動的に完了通知メールが送信される.

3.2. 端末申請処理の業務の変化

システム導入前のパソコン等のマルチステップ認証対象機器の登録は，主に以下の作業が発生していた.

(1) １日に一度登録・削除件数をまとめ，登録コマンド用テキストを作成
(2) Alaxala にログインして，登録内容確認
(3) 登録・削除コマンド実行
(4) 登録内容確認
(5) Radius にログインして，登録内容確認
(6) 登録・削除コマンド実行
(7) 登録内容確認
(8) 管理者画面にあるボタンで許可メール送信

認証除外機器の場合も，作業の流れは同じだが固定 IP アドレス・VLAN を設定する作業が発生する．この項目を割り振るには，場所・所属が関係してくるために自動的に連番を与えることができないため，オンラインシステムとは別に IP アドレスのデータを持っている．この点に関してはオンラインシステムで完了していない.

機器申請に関してもシステム導入後には，通知メールを受け取り，管理者画面にログインして申請内容を確認し登録ボタンをクリックするのみになった.

3.3.システム導入後の利点

・登録するシステム別に異なるコマンドを実行する必要がないため，処理ミスがなくなり，主担当者が不在でも処理が行えるようになった.

・管理者画面の未処理一覧で処理されていない申請が確認できるため，処理漏れ（遅れ）が少なくなった.

・以前は，処理ミス防止のため１日分の申請をまとめて処理していたため，処理完了は申請日翌日としていたが，随時処理を行えるようになった.

・機器申請で間違った MAC アドレスを申請してしまった場合に，一度申請をして許可を受けて認証を試すとエラーが出てしまう．そこで初めて申請内容が間違っていたことに気が付くユーザが多く，正しい MAC アドレスを申請するとまた翌日になってしまうこともあった．オンライン後には随時処理を行えるので，ユーザを待たせることが少なくなった.

システム導入前後の申請処理の所要時間を調査したところ，システム更新後の所要時間は，システム更新前に比べるとユーザアカウント申請は 30 分程度、端末申請は 4 分の 1 程度に減少していることがわかる（表１）.

表１．システム導入前後の申請時刻から許可メール発行までの所要時間

	システム更新前	システム更新後
ユーザ申請	10:46:43	10:10:04
端末申請	5:57:23	1:28:27

※のべ勤務時間の中央値（時間：分：秒）
※照会が必要であった事例を除く
※認証機器のみ

ユーザアカウント申請についての所要時間は機器に比べるとそれほど減少していないようにみえるが，これは

登録処理前の人事情報確認作業と登録処理後の動作確認作業に時間がかかる件数がこのシステムを導入した時期（年度末・年度初め）に多かったこと，新しいシステムを導入するにあたって職員番号との連携を取るようにしたことが原因である．

4. 今後の課題

基本的な申請の流れは Web 画面上で完結するようになったが，いくつか改善すべき課題がある．

まずは認証除外機器の登録に必要な固定 IP アドレスの割り振りが自動化されていない．これも自動化できるようにしたい．

もう 1 点は機器申請について，MAC アドレスは各自で調べて入力しているので番号の入力ミスがある．MAC アドレスを自動取得できる仕組みを取り入れ，それと同時にパソコンのセキュリティ情報（OS のバージョン，更新日付，ワクチンソフトの利用状況など）も自己申告して入力しているので確実な情報を得るために自動取得できるような仕組みが必要である．

これらの課題についても引き続き実現できるように検討していきたいと考えている．

参考文献

[1] 谷内田昌寿，白清学，”MAC アドレス認証と Web 認証併用キャンパスネットワークの導入”, 学術情報処理研究，No.14，pp. 140-143，2010.

[2] 久長穣，杉井学，為末隆弘，金山知余，小河原加久治，”山口大学におけるネットワーク運用支援システム”，学術情報処理研究，No.15，pp. 31-39，2011.

[3] 島岡章，板倉紀子，”大分大学医学部キャンパスのネットワーク運用ポリシーとシステム構成について”，（本年の学術情報処理研究集会にて発表予定）

[4] 岩沢和男，宮原俊行，中川敦，岩田則和，西村浩二，吉冨健一，”センターサービス利用登録システムの再構築”，学術情報処理研究，No.15，pp. 89-97，2011.

会議時貸し出し用 iPad における Apple Configurator を用いたセキュリティ対策

Security measure using Apple Configurator for lending iPad at a meeting

川戸聡也 †, 本村真一 †

Toshiya Kawato†, Shin-ichi Motomura†

t.kawato@tottori-u.ac.jp, motomura@tottori-u.ac.jp

鳥取大学 総合メディア基盤センター †
Center for Information Infrastructure and Multimedia, Tottori University†

概要

近年，スマートフォンに代表される携帯情報端末が急速に普及しており，娯楽用途だけではなく教育やビジネス用途での利用が注目されている．鳥取大学においても，Apple 社のタブレット型携帯情報端末である iPad を導入し，会議時に配布して，ペーパーレス会議を試行中である．配布した iPad は回収して，再度会議時に配布するのだが，考慮しなければならないのがセキュリティ面での対応である．本稿では，iOS デバイス設定管理ツールである「Apple Configurator」を用いた効率的なセキュリティ対策，及び会議時貸し出し用 iPad の運用方法を紹介する．

キーワード

セキュリティ, iPad, Apple Configurator

1 はじめに

近年における情報通信機器の発展は著しく，スマートフォンに代表される携帯情報端末の普及には目覚ましいものがある．その利便性の高さから，個人向けの娯楽用途だけに留まらず，教育やビジネス用途として導入する大学や企業が増加している。鳥取大学（以下,「本学」という）においても，Apple 社によって開発されているタブレット型携帯情報端末である iPad を 50 台程導入している．導入した iPad は，会議時に紙資料を減らすことを目的としたペーパーレス会議に試用している．紙の使用量が減ったことに加え，開催者側では資料の印刷や差し替えといった準備の手間が減り，利用者側でも資料が煩雑にならないなど，一定の成果を挙げている．

この際，iPad は会議開始時に配布し，会議終了時に回収するという形を取っている．現在は試行中であるため特定の会議でのみ用いているが，将来的には多くの会議で利用することを想定しているため，必要数が増える個人貸与は考えていない．iPad が安価で大量に導入できれば問題はないが，現時点で揃えようとするとある程度の出費が必要となるため，最低限必要な数以上の導入は控えた方が経済的であると判断した．

iPad の配布及び回収を行うにあたって考慮しなければならないのがセキュリティ面での対応である．会議終了時に回収して，特定の管理者が特定の場所で保管するため，一般的に考えられる紛失や盗難による情報漏えいの可能性は低い．しかし，一台の iPad を複数の人が使用することになるため，前のユーザが入力した情報やパスワード，ダウンロードしたファイルは削除しなければならない．また，iOS のアップデートといった端末の更新作業も必要となる．それらの作業は数台であれば，一台ずつ行えば問題ないだろうが，数十台ともなると管理者の割かれる時間が増えて労力が増してしまう．資

料配布などのペーパーレス会議のための設定も必要となるため，配布する iPad を一台一台設定するのではなく，一括して設定できる方法が望ましい．

一括での設定を実現する方法として，Apple 社により公開された，iOS 搭載デバイスの設定管理ツールである「Apple Configurator」の利用が挙げられる [1]．Apple Configurator は，複数のデバイスにおける iOS のアップデートやバックアップの一括適用に対応している．バックアップの適用を利用すれば，資料の一括しての配布や，ユーザデータの削除も行うことができる．

本稿では，Apple Configurator の機能や実現できるセキュリティ対策，本学での Apple Configurator の利用を組み込んだ会議時貸し出し用 iPad の運用方法を紹介する．

2 Apple Configurator

Apple Configurator は，USB 経由で一度に 30 台までのデバイスを一括して設定及び監視することが可能な，iOS 搭載デバイスの設定管理ツールである [2]．Apple 社が開発した公式のソフトウェアであり，App Store にて無償で提供されている．

Ver.1.1 時点で次のような機能を備えている．

- iOS アップデートの一括適用
- iOS デバイスの監視
- バックアップの作成及び一括適用
- プロファイルの作成及び一括適用
- アプリケーションの一括インストール

動作条件は以下の通りである．

- Mac OS X Lion 10.7.2 以上（Windows 不可）
- iTunes 10.6 以上
- 対象デバイスは iOS 搭載機器のみ
- USB 経由（遠隔不可）
- 一度に一括して設定できるデバイスは 30 台まで

Apple Configurator には大きく分けて「準備」,「監視」,「割り当て」という 3 つの項目がある．順番に設定することで iOS 搭載デバイスをセットアップでき，デバイスの効率的な設定管理を行うことができる．ここでは，主として利用している「準備」と「監視」について説明する．

2.1 準備

デバイスの初期設定を行う．以下のような項目を設定する．

- デバイスの名前（連番も可能）
- 監視対象とするか否か
- iOS のバージョン選択（基本はアップデート）
- 復元（バックアップ適用）の有無
- プロファイルの作成及び適用
- アプリケーションのインストール

ここでの構成は Apple Configurator に接続した複数のデバイスに一括して適用することができる．その際，一度デバイスは初期化される．

図- 1: 準備

2.2 監視

監視対象としたデバイスを Apple Configurator に接続して，設定した構成を一括して適用することができる．2.1 節での構成はここで再設定が可能であり，iPad をグループ分けしてグループごとに構成を変えるといった利用もできる．

図- 2: 監視

3 Apple Configurator を用いたセキュリティ対策

Apple Configurator を用いて iPad を設定管理することで実現できる，効率的なセキュリティ対策について説明する．

3.1 デバイスの監視

監視対象とされたデバイスは，監視設定をした PC 以外では操作及び同期ができなくなる．これにより，管理 PC 以外での内部のデータの持ち出しといった想定していない利用は大きく制限される．

3.2 ユーザデータの消去

ユーザ利用前のバックアップを取っておき，ユーザ利用後の iPad にそのバックアップを適用することで，ユーザデータは消去される．従って，初期状態に戻す作業を怠らず，配布した iPad を使い回さなければ，入力された情報やダウンロードしたファイルが残ることによる情報漏えいは無くなる．

3.3 プロファイルの適用

ユーザ側では削除できないプロファイルを作成して適用することができる．プロファイルでは，機能やアプリケーションの制限，Wi-Fi や資格情報（証明書）などの多岐に渡る項目を設定できる．そのため，プロファイルをセキュリティポリシーとして扱い，強制することで，ユーザの不必要な操作を事前に防ぐことができる．

3.4 一括適用

バックアップやプロファイルの適用を，30 台までであれば一括して行うことができる．一括して設定するため，設定忘れといった人為的なミスが減り，一台一台するよりも時間的に効率が良くなる．

4 会議時貸し出し用 iPad の運用

本学ではペーパーレス会議において，主に会議資料を閲覧するために iPad を配布及び回収して試用している．その際，Apple Configurator を利用してセキュリティ対策を講じている．実際に行っている運用方法について紹介する．

4.1 運用の流れ

運用には大きく分けて二種類の方法がある．書類を事前に iPad 入れておく場合と，書類を無線 LAN 経由でネットワークからダウンロードする場合である．手順としては配布作業が若干異なるのみで，事前準備や回収作業は共通の作業となる．

基本的な運用の流れを図 3 に示す．破線で示されているのが，Apple Configurator を用いて行う作業である．

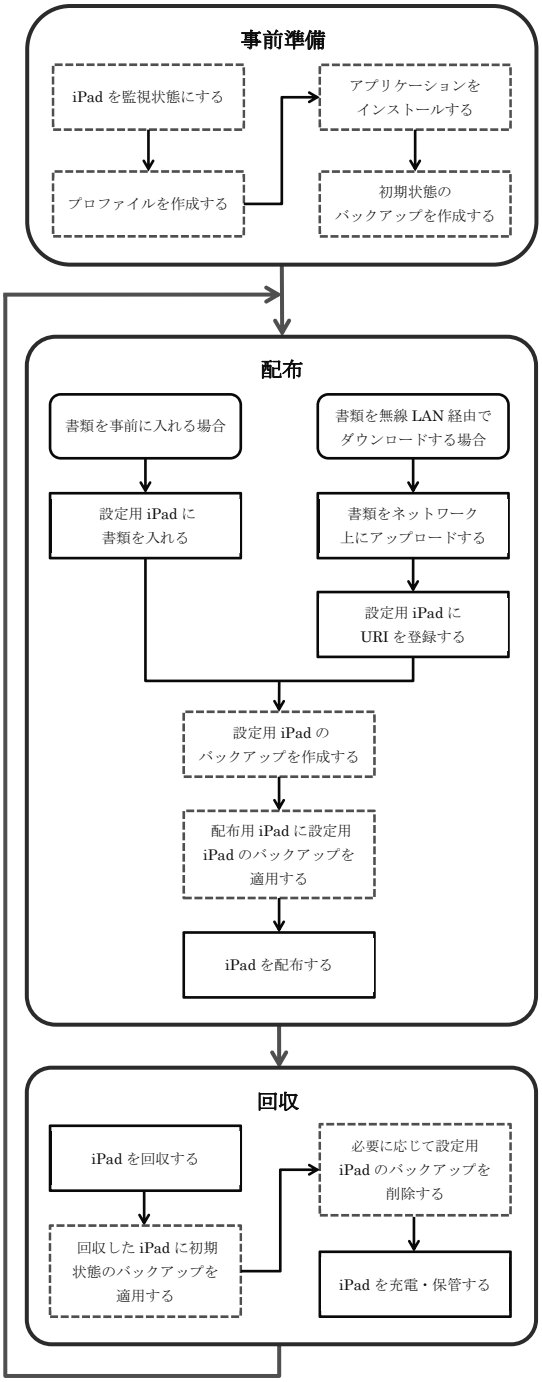


図- 3: 運用の流れ

4.2 事前準備

事前準備の作業について説明する．

まず，iPad を Apple Configurator を用いて監視状態とする．これにより，バックアップやプロファイルの一括適用が可能となる．

次に，配布した iPad の使用方法を制限するためにプロファイルを作成し，バックアップの適用の際にこちらも適用されるように設定する．併せて，必要なアプリケーションを一括してインストールする設定も行う．

また，ユーザデータを削除する（初期の状態に戻す）ために，貸し出しにおける共通の設定のみが反映された初期状態のバックアップを作成しておく．

4.3 配布

iPad の配布作業について説明する．

まず，書類の準備と設定用 iPad の設定をする．書類を事前に iPad 入れておく場合は，iTunes などを用いて設定用 iPad に書類を入れる．書類を無線 LAN 経由でネットワークからダウンロードする場合は，ネットワーク上の文書管理システムなどのファイル置き場に書類をアップロードする．この場合，アップロードした URI を設定用 iPad の Safari のブックマークに登録，または WEB クリップを作成することで，使用者が書類を閲覧し易くしておく．

次に Apple Configurator を用いて，設定用 iPad のバックアップを作成する．その後，設定用 iPad のバックアップを配布用 iPad に一括適用する．この際，PC と iPad の接続には，図 4 に示す Griffin 社製の「MultiDock」を使用している．MultiDock は 1 台につき iPad を 10 台接続及び格納でき，一括しての PC との接続や充電が可能な製品である．この MultiDock を 3 台連結することで，30 台の iPad を一括して PC に接続し，バックアップの一括適用を可能とした．

一括適用を終えた iPad は会議開始時に配布し，主に書類の閲覧に利用している．

4.4 回収

iPad の回収作業について説明する．

会議終了後に，配布していた iPad を回収し，MultiDock に格納する．この際，iPad に割り振られている管理番号の順番で並べることで，トラブル時に対応し易くしている．

MultiDock を PC に接続し，Apple Configurator を用いて，事前準備において作成しておいた初期状態のバックアップを一括して適用する．これにより，ユーザの入力した情報やダウンロードしたファイル，配布した書類は削除され，初期状態に戻される．

図- 4: MultiDock（iPad 格納状態）

書類が含まれている，登録した URI が一度きりの利用，などで配布時に作成した設定用 iPad のバックアップを使い回さない場合，そのバックアップを削除する．書類を無線 LAN 経由でダウンロードする場合に，汎用性のある URI を登録しておけば，バックアップを使い回すことができ，配布時の作業を省くことができる．

初期状態に戻した iPad は MultiDock 経由で一括して充電し，次の利用まで保管する．

5 おわりに

会議時貸し出し用 iPad における Apple Configurator を用いたセキュリティ対策，及び本学での運用方法について紹介した．Apple Configurator の利用により，効率的なセキュリティ対策を実現でき，作業量を抑えられた．

将来的にはその都度貸し出しではなく，個人貸与も検討しなければならないであろう．且つ iPad に限らず，個人に与えられた携帯情報端末を大学での業務に利用することも十分に考えられる．この場合，それらの機器は主に使用者の手にあり，貸し出し利用のように管理することは難しくなる．今後の課題として，携帯情報端末の利用用途に合わせたセキュリティ対策を考え，実行していかなければならない．

参考文献

[1] Mac App Store - Apple Configurator（http://itunes.apple.com/jp/app/apple-configurator/id434433123）

[2] 企業向け iOS 運用のベストプラクティス（http://news.mynavi.jp/series/appleconfigurator/menu.html）

SINET4 への移行に伴う対外接続回線の冗長化構成の構築と評価

Construction of Redundancy of External Network with the shift to SINET4 and it's Evaluation.

柳沼匠†，清水さや子†，吉岡諭†，吉田次郎‡
Takumi YAGINUMA†, Sayako SHIMIZU†, Satoshi YOSHIOKA†, Jiro YOSHIDA‡

yaginuma@m.kaiyodai.ac.jp, smz@kaiyodai.ac.jp, yoshioka@kaiyodai.ac.jp, jiroy@kaiyodai.ac.jp

†東京海洋大学情報処理センター
‡東京海洋大学大学院海洋科学技術研究科
†Information Processing Center, Tokyo University of Marine Science and Technology
‡Graduate School of Marine Sciences and Technology, Tokyo University of Marine Science and Technology

概要

東京海洋大学では，学外への通信に利用する対外接続回線に関して，2012 年 SINET4 アクセス回線の共同調達（以降，共同調達）への参加に伴って，これに対応する規格へと回線を変更した．その際，これまでの冗長化による対障害性の向上を目的として運用してきたネットワーク構成を用いることができなくなり，接続トポロジーとルーティング方式の変更を行うことにした．これに並行して，キャンパス間接続回線の見直しも行い，ネットワークの強化とコスト削減を実現した．本稿では，この変更におけるネットワーク構成の構築と移行の過程や，それらの評価について述べる．

キーワード

冗長化, SINET4

１．はじめに

東京海洋大学は 2003 年 10 月に旧東京商船大学（越中島キャンパス）と旧東京水産大学（品川キャンパス）が統合して設立された新しい大学である．大学の越中島・品川，両キャンパスとも東京湾に面し，四方を河川や運河に囲まれた島状の埋立地に立地しているため，地震等の災害により，橋脚が損傷すると孤立する危険性がある．また，そのような緊急災害時において大学は，災害対応の拠点（越中島：江東区指定広域避難所，品川：東日本大震災時，帰宅困難者受け入れの実績）となるため，情報通信手段の確保はより重要な案件となる．このような大学の立地条件，災害対策を含む対障害性の向上，回線の有効活用を考え，対外接続回線およびキャンパス間接続回線には，冗長化による対障害性の向上を目的とした図 1 のような三角形の接続方式を用いてきた．この方式は良好であったため，2011 年 2 月の情報処理センターシステムのリプレイスの際にもそのまま継続して用いた（参考文献[１]）．しかし，これまで対外接続回線用に使用していた機器が，既にメーカーサポートが終了しており，保守契約なしで運用していたため，早急に更新しな

ければならなかった．さらに，対外接続回線用に利用しているSINET3のSINET4への移行とその仕様変更への対応，コスト削減・ネットワーク充実の求めなどがあり，これらに対応するため, 2012年3月に共同調達に参加し，対外接続回線を SINET4 に対応する仕様へ変更した．それに伴い，回線高速化とキャンパス同士の接続トポロジーとルーティング方式の変更を行うことにした．また，これに並行して，回線機能の向上とコスト削減を兼ね，キャンパス間接続回線の更新も行った．本稿では，対外接続回線とキャンパス間接続回線の切替に伴う，ネットワークトポロジーやルーティング方式の変更のために行ったネットワーク構成の構築・移行過程などについて述べ，機能面・コスト面・試験結果などから，その評価を行う．

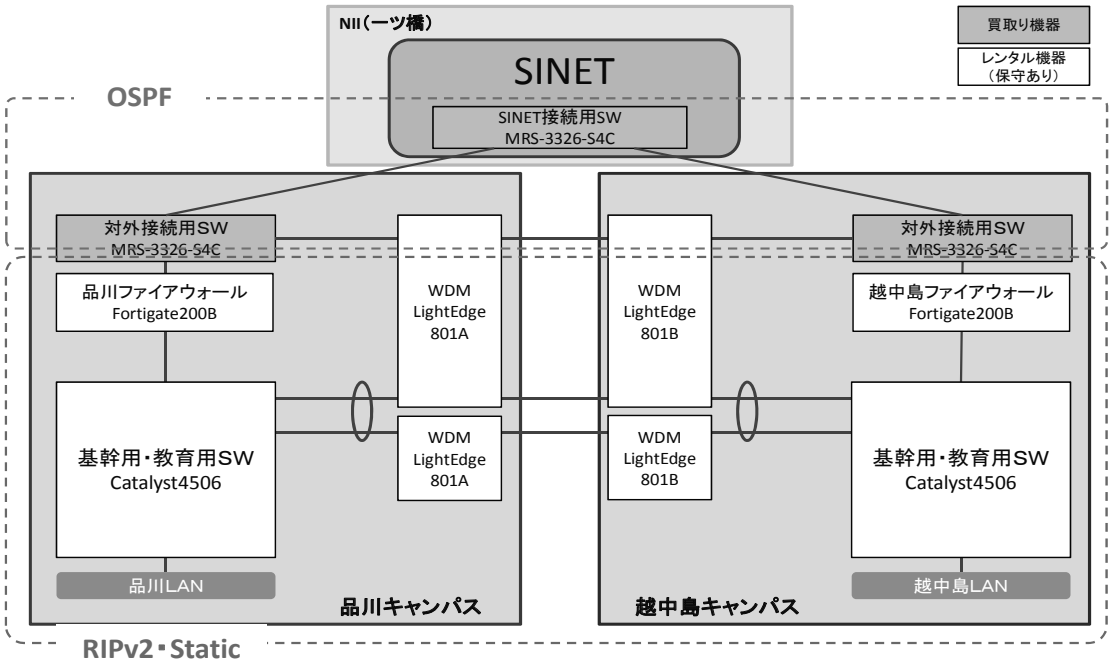


図 1：ネットワーク構成概略図（2011年2月～2012年3月）

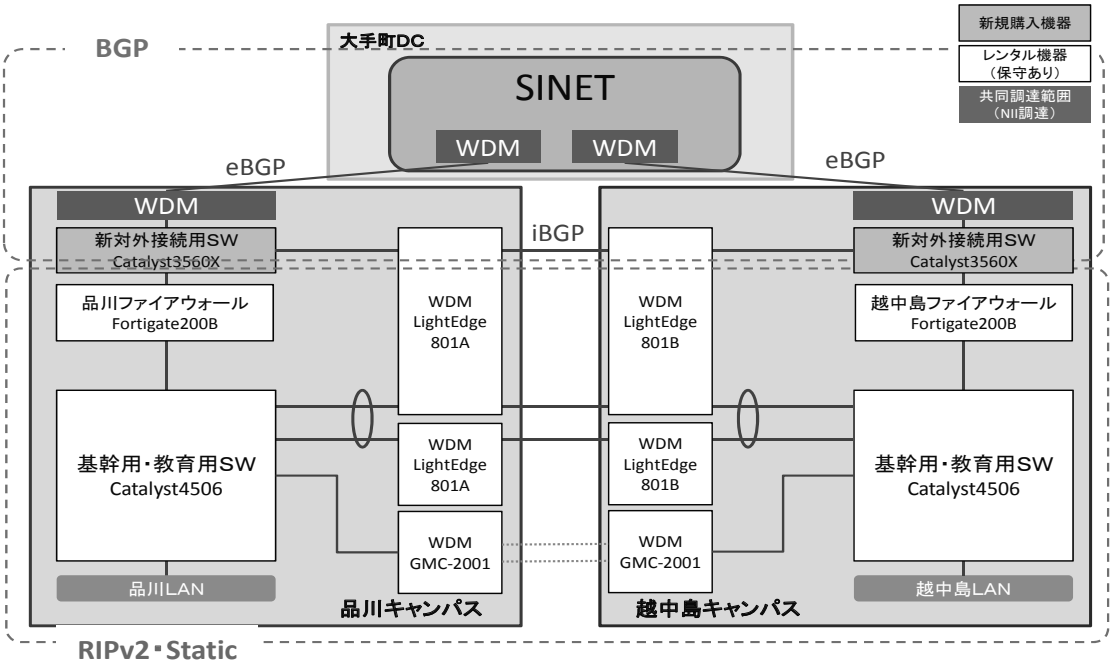


図 2：ネットワーク構成概略図（～現在）

２．従来の対外接続回線とキャンパス間接続回線の構成

2-1．これまでの対外接続回線とキャンパス間接続回線

ここでは，2012 年 3 月までの東京海洋大学の回線構造について述べる．

図 1 のように，SINET（NII 一ツ橋）と品川・越中島両キャンパスに対外接続用 L3 スイッチ（以降，SW）を設置していた．対外接続回線の概形は，これらの SW をそれぞれ接続した三角形構造で構成していた. SW 間の回線速度は SINET と各キャンパス間が 100Mbps，両キャンパス間が 1Gbps であった．本大学の対外接続回線は，このような構造のネットワークを構成して, OSPF によるルーティングを行っていた.

東京海洋大学のファイアーウオール（以降 FW）は，歴史的な経緯より，各キャンパス別に異なった設定である（参考資料[1]）．各キャンパスでは，対外接続用 SW から各々の FW を経由して各々のコアスイッチに接続している．両キャンパスは，WDM を用いた 8Gbps 専用回線で接続している．この回線は２回線で冗長化を行い，片系の回線または WDM で障害が発生しても，他方の回線でキャンパス間通信を維持する．この回線の内，1Gbps 分を前述した対外接続回線用に，残りは，両地区のコアスイッチ間を接続して，キャンパス間通信に用いている．このキャンパス間接続回線は, コアスイッチおよびWDM を介して．RIPv2・Static ルーティングで接続を行っていた.

通常時，学外との通信には SINET と各キャンパスを相互に結ぶ回線を，キャンパス間の通信には両キャンパスを結ぶ専用線であるキャンパス間接続回線を用いる．また，一方のキャンパスと SINET 間でのネットワーク障害時には，OSPF によるルーティングによって，この障害の影響下のキャンパス内からそのキャンパスの FW を通過後，キャンパス間接続回線を経由し，他方のキャンパスの対外接続回線用 SW を経由して SINET（学外）との通信を行う．これによって，他方のキャンパスを経由する場合でも，個々のキャンパスの FW の設定を維持しながら対外接続回線を確保することができる．このような冗長性を持つことで対障害性を実現してきた．この三角形の接続方式の回線構造は，運用中に東日本大震災などあったが, これまで安定して稼働を続け, 接続を維持した.

2-2．SINET4 仕様への対応と回線共同調達の仕様による問題点

昨今の通信高速化への対応や大学を取り巻く経済状況等の諸事情から，本大学もコストを抑えることができる共同調達を利用して SINET４への対応を行うことにした. コスト面を考慮したネットワーク構成は，「SINET～一方のキャンパス～もう一方のキャンパス」の１ラインの線形トポロジーとなるが，この構成はこれまでのような冗長性を持たないため，対障害性，災害対策等の面で問題点があった．また，冗長性を持つ従来の接続方式では SINET 側のラックに大学の機器を設置することが必須である（図１参照）．しかし，共同調達の場合では，SINET 側のラックを利用するオプションを選択できないため，これまでの冗長化方式を用いられないなどの，いくつかの問題点が浮かび上がった．これらの問題に対応するため，新たな方式を検討することにした.

３．SINET4 への移行にむけての対外接続回線とキャンパス間接続回線の再構築

3-1．SINET4 への移行に伴う対外接続回線の構成の計画案

3-1-1　品川ベースの 1 ライン（線形トポロジー）案（SINET～品川～越中島）

当初は，コストの面等から SINET への接続（対外接続回線）をすべて品川キャンパス経由の 1 ラインとした線形のトポロジーとして設計を行うこととした.

SINET 側を上流とすると，SINET と下流の品川キャンパスに設置した対外接続用 SW 間の回線は，WDM を用いて接続する．この対外接続用 SW で品川側と越中島側に回線を分岐する．品川キャンパスでは，品川の FW を経由して，対外接続用 SW と品川キャンパスのコアスイッチを接続する．対外接続用 SW とさらに下流の越中島キャンパスのコアスイッチ間の回線は，WDM を用いたキャンパス間接続回線と越中島の FW を経由して接続する．これらのような回線構成によって，各地区別の FW の設定を維持する．このように，SINET - 品川キャンパス - 越中島キャンパスを線形に接続をして，対外接続回線を構成する.

しかし，このような線形のトポロジーを用いた案では，SINET と品川キャンパスとの間の回線・キャンパス間接続回線の切断や，回線上流での通信機器の故障や停電などによる障害が発生した場合，障害箇所の下流のネットワークが外部との通信ができなくなる問題があった．さらに，東日本大震災以降，災害や停電への対応を想定した冗長性の高いネットワーク構成を求められたことなどの事情により，この案の採用を見送った.

3-1-2　冗長化（マルチトポロジー）案（SINET—品川，SIENT—越中島）

前述のように冗長性の高いネットワーク構成を求められたことにより，これまで用いてきた冗長性を持つネットワーク構成を継続して用いることにした．SINET 側に機器を設置せずに，冗長性を持たせるためのネットワーク構成の概要は以下のように検討した．

対外接続構成として，SINET 側および各キャンパスの対外接続用 SW を撤去し，新たに各キャンパスに対外接続用 SW を設置し，これらと SINET 間は WDM を用いて接続する．また，東京海洋大学としてプライベート AS（Autonomous System）番号を一つ取得し，SINET と各キャンパス間は BGP によるルーティングを行う．この方式により，SINET と個別キャンパス間でのネットワーク障害時においては，これまでと同様に，障害がおこったキャンパスの対外通信を，そのキャンパスの FW を通過後，対外接続 SW 間を渡り他方のキャンパスを経由して SINET へ接続して行う．

キャンパス間構成として，キャンパス間接続回線は RIPv2・Static によるルーティングの変更はせずに，これまでと同様に障害等に対応する．また，この回線において，2 系統ともに障害が発生した場合，Firewall で許可されている通信については，障害側の対外接続用 SW から SINET（学外）を経由して他方の対外接続用 SW と接続をすることでキャンパス間通信を行う．

コスト面としては，対外接続回線を従来と同じ 2 ラインとしたため，1 ラインの場合と比較してコストは高くなる．しかし，回線自体のコストが下がったことと，そのコストがデータセンターからの距離に比例することから，両キャンパスとデータセンター（大手町）が非常に近い距離（直線距離で，品川：7km，越中島：3km 程）にある本大学では，これまでよりコストを抑えることができる．東京海洋大学の立地条件が，ネットワークコスト削減にとっては有利となった．

3-2. キャンパス間接続回線の構成案

本大学では，キャンパス間接続回線にダークファイバーを用いている．キャンパス間接続回線は，大学合併時に敷設されたものであるが，当初から回線の見直しが行われていなかったため-，対外接続回線の切替を機に見直すことになり，図2のようなネットワーク構成の変更を，2012 年 6 月に行うことにした．従来の契約は回線のみの契約であり，WDM 機器などはレンタル機器を利用していた．新しい契約でも，従来と同様に回線のみの契約を行う予定であったが，現在，WDM 回線のみの契約はほとんどなく，あってもコストが高くなるため，これまでの契約よりコストが抑えられる指定の WDM 付契約に変更した．回線自体のコストも以前より下がっていたことも相まって，コストは半減した．

また，現状の構成の変更を最小限に止めることを前提にレンタルの WDM を使用すると，障害時に問題切り分けがとても困難となることから，キャンパス間接続回線のトラブル時に指定の WDM に切替られるように図２のように指定の WDM（WDN-GMC-2001）も設置した．但し，普段は使わずに，レンタルの WDM のバックアップ用として，レンタルの WDM の障害時に自動で指定の WDM に切替できるように設定した．これにより，現状の構成の変更を最小限に止め，冗長性も向上させながらコストを大幅に抑えることに成功した．

４．SINET4 への移行に伴う対外接続回線の冗長化構成およびキャンパス間接続回線の切替によるネットワークの構築および評価

本大学では図 1 のように SINET，品川キャンパス，越中島キャンパスのそれぞれに，対外接続用 Ｌ３スイッチを設置し，それらを接続することによって三角形のネットワーク構成し，動的な経路制御を行うことによって冗長性を持たせ，有効な耐障害性を実現してきた．しかし，前述したように，SINET4 の仕様により SINET 側のスイッチの撤去が必要になったため，これまでの OSPF を用いた動的な経路制御を行なうことができなくなった．そこで，新たな動的な経路制御を行うため，(3-1-2）のように動的経路制御方式として BGP を利用することとした．

4-1. 対外接続回線の構成について

SINET4 への対応に伴い，対外回線速度を従来の 100Mbps より 1Gbps に高速化した．また各キャンパスからそれぞれ SINET に接続する構造には変更はないが，OSPF の代わりに動的経路制御方式として用いる BGP では，組織内部（学内）と外部（学外）の AS が通信を行うため，別途 AS 番号を手配することにした．組織内部用に大学として AS 番号を取得し，外部のものは SINET の AS 番号を利用することにした．

4-2. キャンパス間接続回線切替に伴う問題と対応

キャンパス間接続回線に関しては，WDM の切替も行うことにしたが，レンタル WDM から指定の WDM への切替後，品川基幹スイッチ上で ipv6 default route が消失する現象が発生した．そのため ipv6 による通信ができないなど，いくつかの問題が発生した．そこで，改善策として次の 2 つの方法が考えられた．一つは両キャンパスの対外接続用 SW を MBGP(ipv6 の BGP)対応機器に変更し，ipv6 についてもマルチホーミング化すること，もう一つは，ipv6 default route がキャンパス間を通過する様に設定変更することである．しかし，ipv4 と ipv6 ではネットワ

ーク設計思想が異なるため，非推奨とされたことと，改善策のコストが高く，一方，指定の WDM を利用する可能性は低いため，現状の設定での運用とした．これらより，最終的に図 2 のようなネットワーク構成とした．

５．対障害性の試験および評価

SINET4 対応と WDM の切替を 2012 年に行い，その切替の際，回線試験を行った．試験は，外部にサーバーを設置して，そのサーバー（学外サーバー）と各キャンパス間の通信性能を，通常状態と障害状態（SINET と品川間，SINET と越中島間，キャンパス間）について，切替の前後で計測した．以下の表は，その回線試験の結果である．

表 1 : FTP パフォーマンス（Download/Upload）計測結果[KB/s]

回線状態	正常状態時			
通信方向	Down		Up	
切替	前	後	前	後
品川端末 ⇔越中島端末 ・学外サーバー	2124.59	9591.51	3338.74	5593.20
越中島端末 ⇔品川端末 ・学外サーバー	5449.32	9730.51	4535.43	5174.15
回線状態	障害状態時			
	品川−SINET間			
通信方向	Down		Up	
切替	前	後	前	後
品川端末 ⇔越中島端末 ・学外サーバー	7608.67	1413.74	6374.13	3474.35
越中島端末 ⇔品川端末 ・学外サーバー	7404.41	8376.43	4996.95	3313.47
回線状態	障害状態時			
	越中島−SINET間			
通信方向	Down		Up	
切替	前	後	前	後
品川端末 ⇔越中島端末 ・学外サーバー	5604.06	8376.43	4105.78	3313.47
越中島端末 ⇔品川端末 ・学外サーバー	5249.70	8065.97	4134.84	5242.18

表 2 : RTT 計測結果（経路別平均）[ms]

回線状態	正常状態時				障害状態時					
					越中島−SINET間				キャンパス間	
通信方向	越→学外		学外→越		越→学外		学外→越		越→品	
切替	前	後	前	後	前	後	前	後	前	後
品川端末 ⇔越中島端末 ・学外サーバー	3.8	1	5	4	4.6	2.2	7	5.4	3.4	1
越中島端末 ⇔品川端末 ・学外サーバー	5	1	5	4	4.8	1	6.6	5	4	1

表 3 : 障害切替りダウンタイム計測結果 [s]

通信区間	品川−SINET間		越中島−SINET間		品川−越中島	
切替	前	後	前	後	前	後
品川端末 ⇔越中島端末 ・学外サーバー	24	82	0	0	0	0
越中島端末 ⇔品川端末 ・学外サーバー	0	0	24	93	0	0

計測結果より，回線の高速化については良好であった．特に学内から外部に対しての遅延時間（RTT）が大幅に短縮された．一方，障害時のルーティングの切替時間は，以前より時間が掛かるようになった．これは動的経路制御方式を OSPF から BGP と変更したためで，計測結果は想定の範囲内に収まっている．これらの結果より，冗長性の保持と，通信速度の向上のという目的を達したと評価できる．

６．まとめ

今回の SINET4 対応のための対外接続回線とキャンパス間接続回線の変更に伴う，ネットワークトポロジーやルーティング方式の変更において，これまでの対障害性等を実現してきた冗長性の保持とコストの大幅削減を，実現することができた．

東京海洋大学では 2 つのアドレスブロックをまとめて AS とし，SINET 側の AS と 2 ヶ所のエッジルーターで接続している．SINET には海洋大 AS の接続情報とエッジルーター2 台の IP アドレスを通知し，海洋大内部ではエッジルーター同士の経路交換により，片側が切断された場合でも外部との接続を維持するようになっている．今回，BGP を利用することで，学外への接続について外部に依存しない自律構成を得ることができたことは，現在 2 ヶ所のキャンパスのみではあるが，対象が広がった場合でもこれを応用することで，最適なネットワーク構成を取ることが可能となるといえる．このことは，他の関連施設への拡張のみならず，他の組織への拡張など今後の発展の可能性を持つといえる．

参考文献

[1]平沼賢次,柳沼匠,清水悦郎 : 対外接続の冗長化による対損害性の向上，学術情報処理研究 No.15,pp.145-149,2011
[2]伊藤智博,高野勝美,田島靖久,吉田浩司 : 災害時に備えた分散キャンパスによる情報基盤の整備，学術情報処理研究 No.15,pp.005-011,2011
[3]八代一浩,大西康雄,二戸麻砂彦,中俣賢司,笹本正樹,岡裕人,林英輔 : ＢＧＰ情報を用いたアプリケーションレベルのマルチホームを実現するシステムの構築，インターネット運用技術研究会シンポジウム 2002,pp.123-128,2003

ISMS 研究会

ISO 審査機関からみた国立大学法人の ISMS

The progress and problem of The ISMS of National University Corporations through the position of ISMS certification body

山本富夫†
Yamamoto Tomio†
Yamamoto.tm@jaco.co.jp
†株式会社日本環境認証機構
† Japan Audit and Certification Organization (JACO)

概要

大学での ISMS は情報基盤センターなどの IT 運営分野では ISMS と ITSMS の統合導入など新しい動きが進んできているが、大学全体では内部統制分野など企業ほどには進んでいない．本当に重要な情報（産学連携における営業機密、ナーバスな個人情報）を保護するための厳格なセキュリティ文化、体制、手続きなどが不十分な状況にある．本稿ではこのような現状の課題と解決のための方向性（ISMS の深堀と横展開，安心安全社会実現の基礎としての ISMS，システムアシュアランス）を提示する．最後に弊社が提供する大学向けカスタムテイラード監査パッケージサービスについて紹介する．

キーワード

ISMS, 内部統制，営業機密，ナーバスな個人情報，安心安全社会，システムアシュアランス，カスタムテイラード監査サービス，統合マネジメント

1. 大学での ISMS の整備進展状況と課題

大学での ISMS は情報基盤センターなどの IT 運営分野では ISMS と ITSMS の統合導入など進んできているが、大学全体では内部統制分野など企業ほどには進んでいない分野もある．全学規模で e ラーニング受講などにより一般的な情報セキュリティ意識は高まってきている．しかし，情報公開を伝統としてきた大学自治の伝統、歴史の浅い産学連携の状況などの理由により、産学連携における営業機密、医療情報などナーバスな個人情報を保護するための厳格な文化、体制、手続きなどがまだ先鋭的な企業に比べると不十分である．

2. 大学での ISMS の課題解決の方向性

ISMS の対象は全ての業務の土台である情報である。ISMS は、この情報を機密性，完全性，可用性というトータルな視点でリスクアセスメントを行い，対策，点検，アクションするマネジメントシステムである。このため、ISMS は組織の内部統制の土台として活用できる．

また，ISMS は ISO のマネジメントシステムの中では唯一人間の悪意（意図的な不正）を想定している規格である．このため，ISMS を運用するには人間性に対する深い認識，組織文化に対する省察などが必要である．

本稿はこの ISMS の本質に立脚し，大学での課題を具体的に取り上げ，その解決の方向性を示す．一つは ISMS の深堀であり，情報の機密性，完全性，可用性の 3 つの側面を取り扱うマネジメントシステムであることを最大限に生かすことである．二つは ISMS の横展開であり, ISMS を土台にして品質管理，IT サービス管理，事業継続管理など ISMS に隣接するマネジメント分野との統合を目指すことである．

① ISMS の深堀

- 機密性：産学連携での営業機密（共同研究成果など）、大学病院での患者情報、カルテ情報などの重要な情報の戦略的

な保護と安全文化の確立

- 完全性：研究費の不正使用、論文の盗用、データの改ざんなどを防止するための研究業務自体とその管理業務への情報セキュリティの組込み
- 可用性：大学内情報インフラの機密性、サービスのトータルパフォーマンスの向上

② ISMS の横展開

- ISMS を大学情報インフラの品質管理の土台とする．
- ISMS を土台に品質管理 QMS（ISO9001），IT サービス管理 ITSMS，事業継続管理 BCMS（ISO22301）を統合的に構築する．
- ISMS の土台の上に乗せる各分野のマネジメントシステム要求事項を出来る限り ISMS に統合して軽くする．
- 統合マネジメントシステムの整備を行い，カスタムテイラード監査サービスを活用する

3. 安心安全社会の実現の土台としての ISMS

ISMS は単なる情報漏えい対策として見られることが多いが，機密性，完全性，可用性という情報の本質に根ざしたマネジメントシステムであるため，全てのマネジメント分野にとって必須のものであり，土台である．

例えば，IT によって高度にシステム制御された半導体製造プロセスは半導体製造機器へインプットされる情報が誤っていると良品はできない．

また，私たちの社会インフラの電子化（情報化，ソフト化）が進んでいる．このため，その安全性を情報セキュリティが担うようになってきている．このため，社会インフラも情報セキュリティリスクへの対策が必要である．

これから発展するスマートグリッド，スマートシティも広域で複雑な巨大システムであるが，原子力発電所のような専門オペレータに依存できない宿命にある．このような巨大システムの安心・安全を確保するためには情報セキュリティが大きな要素となる．社会の安心・安全は情報セキュリティによって維持されている．

福島原発は国民の安全・安心にとって大きな脅威を与え続けている．私たちは ISMS を安全・安心社会の土台として活用してゆく必要がある．

ISMS の延長線上に上記課題を解決するためのシステムの安全性アシュアランスサービス（システムアシュアランスサービス）がある．

4. ISMS を軸とした JACO が提供する大学向けサービス

最後に ISMS を軸とした JACO が提供するサービスを紹介する．

従来は ISO 審査認証機関である JACO は ISO 認証基準に基づく審査認証サービスに絞ってきたが，お客様の状況として事業環境が厳しくなり，より具体的に経営に貢献するサービスが望まれるようになってきた．

このため，ISO27001 に基づく審査だけではなく，例えば，医療関係組織向けに，ISMS に加え，医療個人情報のためのガイドである「ISO 27799 - 健康情報の情報セキュリティ管理」の要求事項を追加した審査サービスも行っている．これが ISMS に医療分野での要求事項を追加した「ISMS 医療オプション審査サービス」である．

また，ISMS 認証（登録証と認証の外部公開）に価値を求めるのではなく，自らのために内部統制と経営改善を狙うお客様にはカスタムテイラード監査サービスがある．例えば，「ISO 27799 - 健康情報の情報セキュリティ管理」にさらに独自の厳格な要求を付加した独自基準にもとづく組織診断サービスがカスタムテイラード監査サービスの一つである．

カスタムテイラード監査は，監査基準を JACO とお客様が共同作業でテイラリングを行い，その基準をお客様の組織員に教育，トレーニングすることと，その基準がどこまで組織に浸透しているかを監査により確かめる総合的なサービスである．

大学向けサービスとしては次のカスタムテイラード監査サービスが用意されている．ISMS にオプシ

ョンとして組み合わせることも，単独で自己改善のためのカスタムテイラード監査として行うこともできる．また，教育，トレーニング，監査の総合的なパッケージサービスとして利用することもお勧めである．

- 経産省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」によるカスタムテイラード監査サービス
- JISQ150001「個人情報保護マネジメントシステム-要求事項」によるカスタムテイラード監査サービス
- ISO22301（BS25999）「事業継続マネジメントシステム要求事項」によるカスタムテイラード監査サービス
- 経産省「IT サービス継続性ガイドライン」によるカスタムテイラード監査サービス

参考文献

1. JIS Q 27001: 2006「情報セキュリティマネジメントシステム-要求事項」.
2. JISQ150001「個人情報保護マネジメントシステム-要求事項」.
3. ISO22301（BS25999）「事業継続マネジメントシステム要求事項」
4. 経産省「IT サービス継続性ガイドライン」（平成 20 年）.

参考資料

ISMS で扱う情報の 3 つの側面

（1） ＩＳＭＳで価値を保護する 3 つの分野と対象

価値ある情報を創造すると、機密性、完全性、可用性と言う 3 つの視点で情報を保護する必要があります。逆に言うと 3 つの方面から情報に対する脅威があり、そこに脆弱性が存在すると、リスク（被害）が現実化するということです。ISMS はこの 3 つの視点でリスクアセスメントを行い、リスクが現実化することを防ぐマネジメントシステムです。機密性、完全性、可用性は英語の頭文字をとり、略して CIA と呼ぶことがあります。

情報セキュリティと言うと情報漏えいと理解されている場合がありますが、ISMS の対象は、機密性の保護に相当する情報漏えいだけではなく、完全性、可用性も含む広い範囲に及んでいます。

完全性は情報の品質であり、ISMS は情報の品質管理です。また、可用性は情報が必要な時に取り出せることであり、情報サービスの品質管理です。このため、ISMS は企業活動全般を対象として、情報の価値と情報によるサービスを創造し、保護する活動と言えます。

分野	特性	英語	想定リスク	例
C	機密性	confidentiality	情報が漏えいした	個人情報漏洩
I	完全性	integrity	情報が改ざんされた	財務諸表の改ざん
A	可用性	availability	情報が利用できない	情報システムダウン

（2） 3つの側面ごとのリスクの具体的な事例

事故を起こした企業名、具体的な記述は出せませんので、少し抽象的ですが機密性、完全性、可用性ごとにご説明します。ISMS が取り扱うリスクが、どのような性質であるのか、その被害、影響の程度などをイメージできると思います。

C：confidentiality 機密性

- ■ リスク：情報漏えい
- ■ 事例：従業員による情報漏えい
  - 証券会社の顧客になりすまして、オンライントレードのシステムを利用して株の売買を行った情報処理サービス会社の社員 A が、不正アクセス禁止法違反、電磁的記録不正作出及び供用罪で逮捕されました。
  - 情報処理サービス会社の社員であった A は、派遣先の証券会社でオンライントレードのシステムに関わる作業を行った際に、ユーザー名やパスワードなど、約 3 万 8000 人分の顧客情報を自分のノートパソコンにコピーして不正に入手していました。社内の自分の評価に不満があり、トラブルを起こすことそのものが目的であったそうです。

Ｉ：integrity 完全性１ （原本性）

- ■ リスク： 成りすまし
- ■ 事例：メールの成りすましによる詐欺
  - ご入会ありがとうございます。あなたの個体識別番号は以下の通りです。
    2468XXXXX
  - サービスのご利用料金は 1 ヶ月間で 8,000 円です。1 週間以内にお振り込み頂けなかった場合には、ご自宅にまで回収にお伺いすることになります。なお、お支払い頂けない場合には、裁判所からご連絡がいくことになります。

Ｉ：integrity 完全性２ （正確性）

- ■ リスク：改ざん
- ■ 事例：財務諸表の信頼性、品質

- 営業責任者が顧客と共謀して売上金額をピンハネするために稟議決裁なしで、現物の出入りの必要のない役務サービスを、高額で偽装販売しました。
- ノルマ圧力から、小売店に商品を納入した時点で売り上げ計上してしまう「押し込み販売」といった“見せかけの売り上げ作り”がありました。

Ａ：availability　可用性

■ リスク：情報システムダウン

■ 事例：ATM の停止

- ３連休にすべてのＡＴＭが停止する事態に至った銀行のシステム障害。発端は＊日未明に起きた「バッチ処理」のトラブルでした。
  - 銀行は＊日未明、バッチ処理が予定時間までに終了しなかった。原因について同行は「東京都内の特定支店の特定口座への振り込みが想定以上の件数に上った」と説明しており、その段階でシステムが動かなくなった可能性があります。会見で頭取は「一部の口座では、データ容量の上限設定が適切な数値になっていなかった」と人為ミスの可能性に言及しています。

大学情報系センターにおける SLA の構築

Development of Service Level Agreement for an Information Infrastructure Center in University

長谷川孝博 †
Takahiro HASEGAWA †
cithase@ipc.shizuoka.ac.jp
† 静岡大学情報基盤センター
† Center for Information Infrastructure, Shizuoka University

概要

大学情報系センターにおける ISMS と ITSMS との統合マネジメントシステムの確立を目指す取り組みに関する中間報告である．ITSMS の規格における，利用者との合意要件をまとめ，センタースタッフの年間就業時間，サービスの理想的な稼働時間に対して，想定される年間障害時間を各サービスに対して設定することで, 27 の全サービス項目に関する SLA 案を策定した. おおむね 98%以上の SLA を設定可能と結論している．

キーワード

ITSMS, ISO20000, SLA, ISMS, ISO27001，マネジメント

1. はじめに

本学情報基盤センターの ISMS[1−2]初期構築活動期である 2003 年頃, 相応の資源を先行投資する必要のあるマネジメント体制の構築活動に対して，学内には否定的な意見も多かった．情報系センターにおける ISMS の構築活動そのものが暗中模索の状態にあったことや，情報セキュリティの活動が機密性の保護活動に偏狭しているように誤解されたことが原因であったと考えられる．実際のところ ISMS は，情報の機密，完全，可用の価値を，組織の要求に合わせて効率良く維持向上しながら，利用者（顧客）が創出した情報資産の価値を安全に保護するものである．当センターでは，情報の可用性の価値に重きを置いた ISMS 活動を約 10 年間継続して来た. クラウド情報基盤[3]や事務系組織との連携強化などの成果を上げてきた．同時に学内組織や利用者からの一定の理解も得られたものと考えている．少なくとも ISMS 不要論の声は聞こえて来ない.

ISMS が一つの役割を終えたように感じはじめたころ, 当センターでは ITSMS[4−5]との統合マネジメントシステムの構築に着手し始めた[6]. ISMS と ITSMS は，最終的に利用者と共有できる価値を創出するという目的は同じである. しかし, それぞれのアプローチは少し異なる. ISMS が防衛型とするなら，ITSMS は協調型の印象を与えるため，導入の理解は得られ易い．例えば「情報セキュリティを守るために」よりも「IT サービスをより良くするために」の方が利用者には分かり易い.

本報では，2012 年 9 月に迫る ISMS+ITSMS 統合認証の最終段階にあって，利用者との合意項目を整理した上で，ITSMS の中核にある SLA の策定手法の一案について報告する.

2. 利用者との合意

ISMS の規格書本体には「合意（Agreement)」の文字は 1 カ所しかなく，代わりに「契約（Contract)」の出現頻度が高い．一方，ITSMS では「合意」の出現頻度は 10 カ所以上にも及ぶ．合意の相手は，サービスコンポーネントの提供や保守を行うサービス供給者も一部に含まれるが，主たる合意相手は利用者である．具体的には，その代表委員の集まりであるセンター運営委員会を考えている．以下に合意すべき規格要件を示す.

1. 新規を含むサービス変更の計画立案
2. 新規を含むサービス変更
3. 提供するサービスとその目録
4. 各サービスに関する一つ以上の SLA
5. サービス報告書の記載内容
6. サービス継続および可用性の要求事項
7. 容量・能力およびパフォーマンスの要求事項
8. 苦情の定義
9. 重大なインシデントの定義
10. 緊急変更の定義

11. 変更失敗の際に取るべき処置
12. 頻度および種類を記述したリリース方針
13. 緊急のリリースの定義
14. リリースの受け入れ基準
15. リリースの失敗の際に取るべき処置

項目数が多いようにも感じられるが，国際調達で行われる全学情報基盤整備などの大型の調達は，これらの多くを網羅して遂行されていると考えられる．ITSMS の運用においては，より小規模の変更やリリースにおいてもこれらの要件を踏まえて当該プロセスを遂行して行く必要がある．例えば，システム変更における事前の通知や Web サイトによる予告や進捗の通知を徹底することも利用者との合意形成活動の一環と考えられる．センターの活動の透明性を高めることが，すなわち ITSMS 活動そのものに直結するものであり，これは従来のセンターの運営方針に反するものではない．

情報系センターの活動が ITSMS の規格要件に合致する点を楽観的に述べた．その一方で，全てを網羅するものでないことも明らかである．「苦情の定義」は，ISMS 上にも規定されておらず，ITSMS マニュアルの中で新規に定義づけする必要がある．定義として次を策定した．

> 苦情とは，センターが提供するサービスが SLA やサービスの提供内容に対する不履行の指摘を含む相談，申し出，連絡を言う．
>
> これ以外の利用者からの強い申し出の多くは，全学合意した上で提供されている現行サービスそのものへの改善を求める申し出である場合が多い．これを「改善の要望」と定義し，「苦情」とは分けて適切に処理する．「改善の要望」は「サービスレベル管理プロセス」で取り扱う．

このような定義のひとつひとつが利用者との合意に至れば幸いであるが，仮に利用者から不合意の意見が出されたとしても，それは双方の意識合わせをしていくためのよい機会として捉える．

3. SLA

先に示したように，ITSMS では「提供するサービスとその目録」および「各サービスに関する一つ以上の SLA」を利用者の合意の下に定める必要がある．

論理性のある SLA を策定するために，まず，センタースタッフの稼働時間と障害発生時間の想定を起案し，表-1 のようにまとめた．これらの値に基づき，表-2 の SLA 案を作成した．

センタースタッフの勤務態勢は大学の労働規定に準じるもので，昼間 8 時間の就業が原則である．シフト制などによる夜間勤務や深夜勤務などはない．表-1 によれば，年間の総時間に対する勤務時間率は，わずか 21.5%であり，残りの 78.5%の時間帯に起こる障害に対して，厳密には障害対応ができない状態にある．それにも関わらず，基幹ネットワークやメールサービスなど実質的には年間稼働率 100%の実効運用がなければ，利用者の苦情が殺到するサービスを多く抱えている．恒常的に感じるセンターの運用体制の厳しさを，はじめて数量的に理解することができた．

表-2 では，サービス目録を列挙し，各サービスの提供時間を明確にした．表-1 で想定した年間の許容停止時間（想定される障害発生時間と頻度）を前提に，各サービスに対する論理的稼働率を SLA として定めた．ほとんどの SLA は 98%以上となり，妥当な稼働率目標を得ることができた．20 番の「遠隔講義システム」だけが「保守や運用に恒常的な不安を抱えているサービス」であり，95.8%の稼働率としている．SLA と同時に，これまでの実績値に基づくセンターの稼働率目標値のほとんどを 99%以上の値で示している．2012 年 8 月から翌年までの ITSMS のサービス稼働率を目標値の横に添えて，毎年報告することを計画している．

4. まとめ

大学情報系センターにおける ISMS と ITSMS の統合構築を例に，各マネジメントシステムの特徴と役割を整理した．ITSMS の構築で重要となる利用者との合意について，規格書に基づく合意項目を整理し，いくつかの対応方針を示した．また，センタースタッフの年間勤務時間と障害想定頻度に基づき，SLA の理論値を算出する方法を示した．多くは未合意の案であるが，情報系センターにおける SLA 構築の一案として，有効であると考えている．その結論は，2012 年 9 月中に行われる ISMS+ITSMS 総合審査とその後の本格運用において明らかになっていくと思われる．今後の活動にご注目頂きたい．

参考文献

1. JIS Q 27001: 2006 （ISO/IEC 27001:2005），財団法人日本規格協会（2006）．
2. ISMS ユーザーズガイド，財団法人日本情報処理開発協会（2006）．
3. 「BCP を支えるクラウド情報基盤 静岡大学情報基盤センター2011 年度の活動記録」，井上春樹・長谷川孝博ら，静岡学術出版（2012）
4. JIS Q 20000-1（ISO/IEC 20000-1:2011），財団法人日本規格協会（2011）．
5. ITSMS ユーザーズガイド，財団法人日本情報処理開発協会（2007）．
6. 「ISMS から ITSMS への取り組みについて」，長谷川孝博・中野光義，研究報告インターネットと運用技術（IOT），2012-IOT-16，**39**，pp.1-5（2012）．

表-1：センタースタッフの稼働時間と障害発生時間の仮定（未合意案）

項 目	値	単位	備 考
年間の休み日	129.3	日	土日数(104.3 日)＋祝日(15 日)＋正月と盆(10 日)
年間の勤務日	235.7	日	
年間勤務時間	1886	時間	欠勤がない場合の一人当たりの最大勤務時間
年間時間	8760	時間	＝24 時間×365 日
年間総時間に対する勤務時間率	21.5%	[－]	＝(保守契約の障害対応可能時間率)
年間の許容停止時間(想定される障害発生時間と頻度)			
24 時間×(365 日)の供給を要するサービス	134.0	時間	金曜夕方から月曜の正午までの障害が年に 2 回発生
8 時間×(稼働日合計)の供給要を要するサービス	12.0	時間	4 時間のサービス停止が年に 3 回発生する想定
障害時の応急対応に困難が予想されるサービス	－	個別	保守や運用に恒常的な不安を抱えているサービス

表-2：各サービスに対する SLA（未合意案）

No.	サービス名称	理想時間(100%)			障害	SLA		目標値	サービス時間に関する備考
		サービス時間／日	稼働日／年	完全稼働時間／年	許容停止時間／年	稼働率	完了工程業務日数		
0	基幹ネットワーク	24	365	8760	134.0	98.5%		99.0%	契約上の保守対応は平日 9-17 時まで(※)
1	アカウント(登録／削除)						5	99.0%	スタッフ会議承認後からの完了日数
2	パスワード再発行	12	236.7	2841	12.0	99.6%		99.6%	ただし，棟の入館可能時間に左右される
3	パスワード変更	24	365.0	8760	134.0	98.5%		99.0%	
4	メール	24	365.0	8760	134.0	98.5%		99.0%	
5	WEB メール	24	365.0	8760	134.0	98.5%		99.0%	
6	WEB サイト	24	365.0	8760	134.0	98.5%		99.0%	
7	情報コンセント	24	365.0	8760	134.0	98.5%		99.0%	
8	無線 LAN	24	365.0	8760	134.0	98.5%		99.0%	
9	無線 LAN ゲスト	24	365.0	8760	134.0	98.5%		99.0%	
10	情報教育用端末	12	236.7	2841	12.0	99.6%		99.6%	平日 8:30～21:00
11	シンクライアント	24	365.0	8760	134.0	98.5%		99.0%	
12	パソコン接続(PIP)	24	365.0	8760	134.0	98.5%		99.0%	
13	サーバ接続(GIP)	24	365.0	8760	134.0	98.5%		99.0%	
14	サーバ証明書						2	99.0%	平成 27 年度までの提供(国立情報学研究所)
15	DNS サーバ	24	365.0	8760	134.0	98.5%		99.0%	
16	DNS 登録						2	99.0%	
17	クラウドサーバ	24	365.0	8760	134.0	98.5%		99.0%	クラウド供給元との SLA は 99.99%
18	クラウドストレージ	24	365.0	8760	134.0	98.5%		99.0%	
19	ソフトウェア貸出	8	236.7	1894	12.0	99.4%		99.4%	
20	遠隔講義システム	8	236.7	1894	80.0	95.8%		96.0%	
21	京都大学スパコン	24	365.0	8760	134.0	98.5%		99.0%	
22	研究支援サーバ	24	365.0	8760	134.0	98.5%		99.0%	
23	全学電子掲示板	12	236.7	2841	12.0	99.6%		99.6%	
24	メディアサイト	8	236.7	1894	12.0	99.4%		99.4%	
25	入退室管理	24	365.0	8760	134.0	98.5%		99.0%	
26	サービス窓口	7.7	236.7	1823	12.0	99.3%		99.3%	昼休み 12:30～13:30 と週1会議(90 分)を除く

※システム構成上，No.0 が大規模に停止した場合，配下にある全サービス SLA の不履行のカウントを停止する．

ISMS 認証取得後の活動について

Our activities after the ISMS certificated

佐野雅彦†，上田哲史†
Masahiko SANO†, Tetsushi Ueta†

sano@tokushima-u.ac.jp, ueta@tokushima-u.ac.jp

†徳島大学情報化推進センター

†The Center for Administration of Information Technology, The University of Tokushima

概要

情報化推進センターは，平成 24 年 3 月に情報セキュリティマネジメントシステム（ISMS）を取得した．これは，我々が管理・運用する情報システムを，適切に運用するための活動及び体制を国際標準規格の下で確立するプロジェクトであった．ISMS を取得した時点では，その物理的な適用範囲は情報化推進センター棟に限定しており，本来含めるべき情報化推進センター蔵本分室を適用外としていた．今回，適用外としていた蔵本分室を適用範囲に含めるため, ISMS の変更審査を受審（変更審査は 9 月）するため活動を行ったので，その事例を紹介する．

キーワード：

ISMS，変更審査，事例紹介

1. はじめに

徳島大学情報化推進センターは，平成 22 年 7 月に，学内の情報化推進をより強力に支援するため，高度情報化基盤センターから改組された．改組後の大きなミッションとして，コンピュータシステムの更新（平成 24 年 3 月稼働）と，センターか管理する情報システムを適切に運用するための仕組みの再構築があった．とくに後者のミッションは ISMS の仕組みに類似する部分が多く，このミッションのアウトプットとして ISMS の取得を行うこととなった [1].

平成 23 年 5 月に ISMS 取得活動を開始した際には, 常三島地区の情報化推進センター棟および蔵本地区の情報化推進センター蔵本分室（附属図書館蔵本分館内）を ISMS の物理的な適用範囲として準備を進めてきたが, 附属図書館蔵本分館が改修工事中（平成 23 年 9 月～平成 24 年 5 月）であったため, 議論の末, ISMS 取得時点（登録日は 2012 年 3 月 9 日）ではこれを適用範囲外とし, 改修工事後にその適用範囲を変更することより，本来の対象範囲に含めることとした．平成 24 年 3 月には ISMS（ISO/IEC 27001:2005・JIS Q 27001:2006）を取得した．

本稿では, ISMS 取得後半年余りで ISMS の適用範囲変更（拡大）を行った，我々の活動事例を紹介する．

2. ISMS 取得後

平成 24 年 1 月の ISMS 本審査受審後，平成 23 年度末までは，マネジメントレビュー結果による是正項目への対応と本審査結果への対応が主であった．とくに，マネジメントレビュー結果からの是正項目「マニュアル等の整備不足」は，これまでの属人的なセンター運用体制から業務マニュアルによる組織的運用体制への移行を図るうえで重要な課題であった．しかし，同時進行していた「情報化推進センターコンピュータシステム」更新プロジェクトが導入段階に入っており，新システム用の業務マニュアルが次々と必要になり，業者作成分 170 を含む 250 超のマニュアル（7 月末時点）を整備する結果となった．加えて平成 24 年 4 月には，ISMS 構築チームの主要メンバー5 名中 3 名が移動となり，大幅なリソース減となった．これらのため，従来システムに対するマニュアル整備は進まず，新システム稼働の喧騒が一段落（6 月以降）してからの取組となり，本来予定していた 4 月末

から遅れる結果となった.

ISMS 取得までは，ある意味，「ISMS とるぞー，おぉー」的な勢いにまかせた面があり，短期間で ISMS を取得できたはいいが，本当の苦労はこれからという事態がまさに具現された状態である．この状況下で，以降に述べる適用範囲変更を行った（本稿執筆時点では変更審査受審前）.

3. 適用範囲変更のための活動

冒頭部で述べたように, 本センター蔵本分室は ISMS 取得後に変更審査により適用範囲に含める方針のため，平成24年5月に審査機関と連絡をとり変更手続きのための前準備に入った（定期審査の時に行う選択肢もあった）. 本学の場合，ISMS の認定範囲の変更には審査機関側に変更届を提出し，変更届から 3 か月以内に変更審査を受審する手順であることから，前述の是正事項の対応も含め，9 月上旬の受審とし，6 月上旬に変更届を提出した.

適用範囲変更のための作業は, ISMS の PDCA サイクルを P（計画）から開始することと言える．これは，JISQ27001:2006, 4.2.1 ISMS の確立 a)で規定される，「ISMS の適用範囲及び境界を定義する」[2] に該当するためである．この P（計画）においては，図-1 に示すように，適用範囲及び境界の変更により洗い出される新たな情報資産のリスクアセスメント，リスク対応のための管理目的及び管理策の選択という流れを経て，D（実行）サイクルへ移行する.

今回の適用範囲変更では, 図-1 に示す ISMS 基本方針やリスクアセスメントに対する組織の取組み方には変更を加えなかった（必要性がないと判断した）ため，実質的には新たな適用範囲及び境界の策定，情報資産の洗い出し，脅威の洗い出し，リスク評価といった P の残る部分についての作業を行った．また，蔵本分室で提供されるサービスも認定済みの範囲で提供しているものと同じであるため，サービス上の変化はない．よって，適用宣言書自体には変更は生じなかったが，各種規定類，下位手順書・マニュアル等は該当部分を変更している.

3.1. リスクアセスメント

情報化推進センター蔵本分室は，図-2 に示す 2 部屋構造であり，入口手前から，受付・執務室，NW 室として運用されてきた．予備的なリスクアセスメント行ったところ，受付領域，執務領域の分離が必要と判断したが，しかし予算と住環境悪化の問題から，境界の明示と簡易パーテーションによる分離とした．その際，受付領域は一般人が立ち入る領域であるが，執務領域，NW 室は職員あるいは特別に許可された場合のみの立ち入りを許可するリスク対応策とした．そのほかいくつかの対策を事前に行い，ある程度対応済みとなった時点で，ISMS 手順に従ったリスクアセスメントを実施し，問題点が小さくなるように配慮した．なお，確認された問題点は是正あるいは予防措置として対処する計画としている．余談であるが, 蔵本地区は電源事情が常三島地区より悪く（これもリスク), 時間帯による電圧変動幅が大きく±10%程度の変動は普通である．このため，蔵本分室には以前から AVR（交流定電圧電源装置）を介して UPS を接続している（リスク対応）.

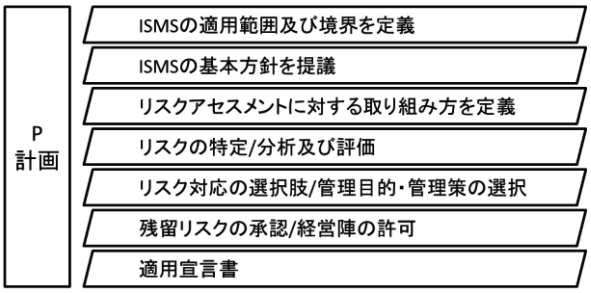


図-1　ISMS の Plan（計画）のフェイズ

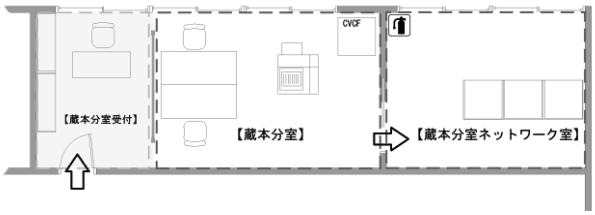


図-2　蔵本分室概略図

3.2. 内部監査ほか

内部監査は 7 月 9 日から 13 日の間で実施された. これはヒアリングと実施確認を主体とするもので，今回は適用宣言書の管理策実施状況の確認を中心に行われた．蔵本分室に関する内部監査からの指摘事項は，入退出管理の記録不備や業務記録の不備が主であった．今後，マネジメントレビューを経て，改善プロセスに取り組む.

4. おわりに

本稿では，ISMS 取得後の活動のうち，ISMS の適用範囲変更の例を取り上げた．これは ISMS の PDCA の P からサイクルを回すことに他ならない．幸い認定取得時の経験から，人的リソースが大幅に削減された現在の状態でも，短期間で PDCA サイクルを一巡することが可能になったと思われる．あとは 9 月の変更審査待ちである.

参考文献

1) “組織評価と ISMS,” 情報処理学会研究会報告, Vol. 2012-IOT-16 No.41.
2) “JIS Q 27001:2006,” 日本規格協会.

センター紹介

福岡教育大学「学術情報センター」の発足

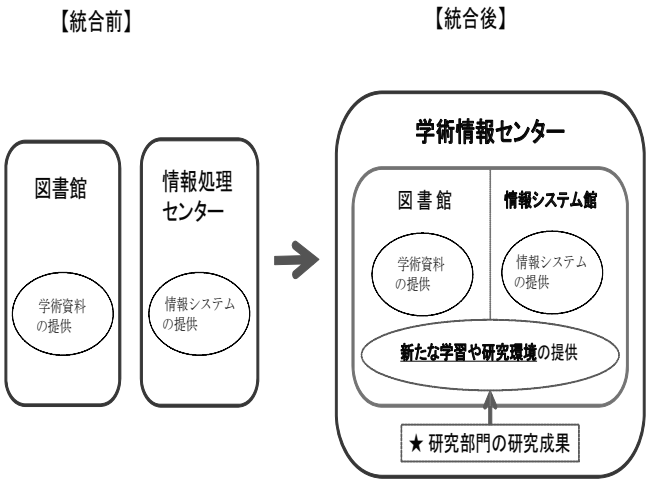
副学長(学術情報担当)・学術情報センター長　大坪　靖直
副理事(評価担当)・学術情報副センター長　清水　紀宏

平成 24 年 7 月 1 日，福岡教育大学学術情報センターが発足した。これは，附属図書館と情報処理センターの統合によるものである。

１.「附属図書館」と「情報処理センター」の組織統合

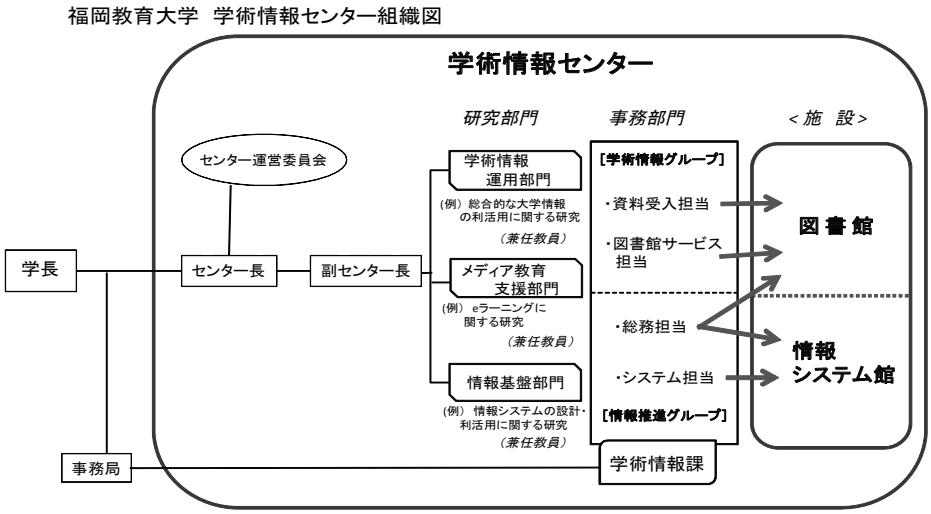
福岡教育大学は九州唯一の教員養成系大学として，長年にわたって，教員の養成，教育者の育成を行っており，教育を通して生涯学習社会への対応に必要な能力を持った人財の育成を支援してきた。

附属図書館と情報処理センター，また，これらを支える事務組織の学術情報課と情報推進課は，本学の情報関連組織として，情報基盤や大学(事務）情報の運用管理にあたり，本学の教育研究及び社会貢献を支援してきた。この四組織を統合することによって情報の収集・管理・運用が一元化され，情報システム・ネットワーク関係業務と,学術資料の提供の業務について,マクロな視点から見直すことが可能となり，本学での情報活用促進が一層高まると期待できる。このことは本学の教育研究や社会貢献の支援向上につながり，生涯学習社会への一層の貢献が可能となる。



２.「学術情報センター」の組織

学術情報センターには，「学術情報運用部門」「メディア教育支援部門」「情報基盤部門」等の研究部門を置くことができ，プロジェクト型の研究を推進していくことになる。このことは，センターの情報収集・管理・提供に係る業務の高度化を図ることにつながる。これら研究部門と事務部門(学術情報課）の連携により，学生や教職員による情報活用が促進される。



３．展望と課題

統合前は，情報関連組織がそれぞれの役割を遂行するべく機能してきた。統合後は，組織が一体となって機能し，情報基盤を確立するともに，他の学内組織と連携することによって，学習・教育・研究支援の強化ならびに情報化の推進にあたっていく。このことで以下のことが期待できる。

① 教育研究の高度化
情報基盤を活用した，新たな授業や研究を展開できるようになる。

② 教員養成・教育者育成支援の高度化
課題を発見し解決する能力や，生涯にわたって知識を活用する能力をもった教員の養成を支援し，また教育者の育成を支援することができる。

③ 社会貢献の進展
上記①②による本学教員の学術文化発展への寄与，本学卒業生の学校(園）教育への貢献，及び地域連携の増進による社会貢献が進展していく。

④ 情報関連の人財育成の機会創出
教職員へ情報関連のスキル獲得機会を提供することによって，上記の効果を強化する。

⑤ 大学情報の活用促進
大学情報を迅速に収集・管理・運用・発信できるようになり，本学の運営及び社会貢献に寄与することができる。

⑥ 学習機会の多様化
ラーニングコモンズのような，情報設備と図書館資料を活用した学習の場が提供されることにより，学習機会が多様化する。

⑦ 図書館機能の向上
情報ネットワークを介した情報収集や情報活用を行う環境がさらに整備され，図書館の教育研究支援機能が活性化する。

⑧ 大学ブランド「福教大ブランド」の確立
大学が優れた教員，教育者を養成(育成)することを通じて，大学の価値を高め，ひいては地域社会での存在価値を高めていく。

組織統合の意義を具現化するためには，解決すべき課題もある。他組織との連携のあり方，施設(建物）の一体化，ニーズの把握，業務内容の精査などが課題となる。これらに対応し，期待に応えるべく，一歩ずつ前進していくこととしている。

情報教育及びｅラーニング開発支援体制を拡充

長崎大学情報メディア基盤センター
野崎　剛一，藤井　美知子，丹羽　量久，上繁　義史，古賀　掲維，柳生　大輔

1.　情報メディア基盤センターの専任教員の増員

長崎大学においては，情報メディア基盤センターは主に学術系情報基盤の企画，管理，運用並びにその利用に係る技術支援及び研究開発を行ってきた。これまで，当センターの専任教員 4 名（教授 1，准教授 1，助教 2）がこれらの業務を担っていたが，平成 23 年 5 月 1 日より，大学教育機能開発センターの教員 3 名（教授 2，准教授 1）が当センターに異動し，当センターは長崎大学における情報基礎教育の中核組織としての機能が加わるに至った。（平成 24 年 4 月，助教 1 名が工学部に異動，現在 6 名）

2.　新しい教養教育新体制へのセンターの取り組み

長崎大学では，平成 24 年 4 月より教養系科目体系の大幅な刷新を行っている。その特徴は（1）教養必修科目の再編と（2）モジュール教育の導入である。これらのいずれについても，当センターの全教員が直接関係科目を担当し，教養教育における情報技術の基礎知識や活用技法を教授している。

2.1.　必修科目「情報基礎」の教材開発と授業実施

上記の教養必修科目の再編の中で，情報系科目についても刷新され，従前の科目「情報処理入門」を後継する形で新科目「情報基礎」（1 年対象，前期開講）が開講された。平成 24 年度は，当センターの全教員で，本科目の授業設計や教材開発を行うとともに，全 30 クラスの授業を担当した。表 1 に情報基礎の授業概要を示す。

表 1　情報基礎の授業概要

サブタイトル	授業の概要
ガイダンス	情報基礎の授業の概要と，学習にあたって必要な準備を行う
ICT 基礎知識編	
情報セキュリティ	情報セキュリティの定義と情報社会での身の守る基礎を学ぶ
情報の検索・活用と情報倫理	検索サイトの種類と情報検索法の基礎，情報倫理の考え方を学ぶ
情報のデジタル化	情報のデジタル化とコンピュータでの記憶の仕方について学ぶ
ネットワークの仕組み	コンピュータネットワーク等での情報通信の基礎を学ぶ
PC 操作スキル編（授業の順序，回数はクラスによって異なる場合がある）	
プレゼンテーション作成術	PowerPoint を使った効果的なプレゼン資料作成法を学習する
文書作成技法	学会原稿の作成を目標に，Word の様々な機能を活用した文書作成の方法を学ぶ
表計算技法	Excel の様々な機能や関数を活用した，表の作成や集計，グラフの作成方法を学ぶ
Web ページの基礎	プレゼン資料の HTML 化を目標に，HTML エディタによる Web ページ作成の基礎を学ぶ
総合演習	

2.2. モジュール教育における情報系教養科目群の開講

長崎大学で導入するモジュール教育は，これまでの選択科目（複数）の代替として，学部ごとに必修となる「学部モジュール」に加え学生は自分の関心があるテーマの科目群（モジュール）を全 23 モジュールの中から一つ選択し，その中から 1 年生後期～2 年生後期の期間でそれぞれの学部が定めた単位数を必ず履修するものである。当センターも表 2 のモジュール科目群「情報社会とコンピューティング」を提供し，平成 24 年 10 月より，情報の技術や社会での利活用，セキュリティに関する知識を深め，実践的な情報処理技法を習得させる教育を展開する予定である。

表 2　モジュール科目群「情報社会とコンピューティング」の概要

	科目名	概要
モジュールⅠ	情報の活用	デジタル文書作成技法と表計算技法の中級レベルを学ぶ
	情報社会の安全と安心	情報社会におけるセキュリティ維持に関する考え方を学ぶ
	計算機の科学	コンピュータの動作原理，データ表現などのしくみを学ぶ
モジュールⅡ	問題解決のアルゴリズム	アルゴリズム設計やプログラミング言語の機能などを学ぶ
	情報と社会	実社会（経済，技術，医療など）と情報の結びつきを学ぶ
	情報化の役割と課題	実社会で運用されている情報システムからその役割を学ぶ
	情報通信とコンピュータネットワークのしくみ	ネットワークの要素技術などから情報通信の仕組みを学ぶ
	情報化時代の仕事術	ライフハックの事例から，現代の情報社会での仕事術を学ぶ
	ソフトウェアの利用技術	解決すべき問題に応じたアプリケーションの活用術を学ぶ

3. e ラーニングコンテンツ開発支援室設置

当センターでは，これまでも e ラーニング普及の為の活動を行ってきた。その推進体制をさらに拡充し，LMS（Learning Management System）利活用や映像・音声の素材収録などを支援する「e ラーニングコンテンツ開発支援室」を平成 24 年 7 月 1 日に設置した。主に以下のような支援活動を展開する。

(1) e ラーニングの導入支援
(2) e ラーニングコースの設計・作成に関するコンサルティング
(3) e ラーニングシステムの活用支援
(4) オフィス系・デザイン系ソフトウェアの活用支援
(5) 映像・音声コンテンツ素材の収録
(6) コンテンツ素材の変換・加工
(7) オープンコースウェア(OCW)の作成・公開支援
(8) e ラーニング、e ポートフォリオに関するセミナー・ワークショップ等の開催

4. 今後の展開

長崎大学情報メディア基盤センターは情報インフラに関する機能に，情報基礎教育の機能が大幅に強化されたことで，大学における ICT を活用した教養教育などの研究・実践・支援の効果が期待されている。また，CIO を中心とした情報ガバナンスを構築・強化するために，従前以上に情報政策の中核としての活動が求められている。

報告

第６回国立大学法人情報系センター長会議議事要旨

○開催日時：平成２３年１０月２１日（金）　１４：００ ～ １７：００
○開催場所：ホテルメリージュ　鳳凰の間（３階）

○出席者（敬称略）：
文部科学省研究振興局情報課学術基盤整備室長　鈴木　達也
文部科学省研究振興局情報課学術基盤整備室学術情報第二係長　政田 眞弥
国立情報学研究所 学術基盤推進部長　安達　淳
国立情報学研究所 学術基盤推進部　学術基盤課　特任専門員　平原　孝明
静岡大学情報基盤センター（副センター長）　長谷川　孝博

北海道教育、室蘭工業、帯広畜産、旭川医科、北見工業、弘前、岩手、宮城教育、秋田、山形、福島、茨城、筑波、筑波技術、宇都宮、埼玉、千葉、東京外国語、東京学芸、東京農工、東京海洋、お茶の水女子、電気通信、一橋、横浜国立、新潟、富山、金沢、福井、信州、北陸先端科学技術院、山梨、岐阜、静岡、愛知教育、豊橋技術科学、三重、滋賀医科、京都工芸繊維、大阪教育、神戸、奈良教育、奈良女子、和歌山、奈良先端科学技術院、鳥取、岡山、広島、山口、徳島、鳴門教育、香川、愛媛、高知、佐賀、長崎、熊本、大分、宮崎、鹿児島、琉球
以上６１大学のセンター長（代理者を含む）

○会議内容：

１　配布資料の確認
当会議の司会である、宮崎大学の青木副情報基盤センター長から、配付資料の確認があった。

２　日程等説明
青木副センター長から、本日の日程等の説明があった。

３　開会
青木副センター長から、開会宣言があった。

４　来賓紹介
青木副センター長から、来賓である文部科学省研究振興局情報課の鈴木学術基盤整備

室長、国立情報学研究所 学術基盤推進部の安達部長及び静岡大学情報基盤センター（副センター長）の長谷川准教授の紹介があった。

5　当番校挨拶

当番校である宮崎大学の菅沼学長及び廿日出情報基盤センター長から挨拶があった。

6　文部科学省説明

鈴木学術基盤整備室長から、挨拶の後、学術情報基盤等に関する最近の動向等について、資料２－１、資料２－２に基づき以下の説明があった。

１）　平成２４年度概算要求について

平成２４年度概算要求は、例年の８月３１日ではなく、東日本大震災の関係で１ヶ月遅れの９月３０日に文部科学省から財務省へ要求を行い、現在、要求内容について財務省への説明を行っている。

概算要求の内容については、裁量的経費を一割削減し、削減した予算に応じて、日本再生重点化措置への要求を行い、また別枠として、東日本大震災の復興・復旧にかかる経費の要求を行えることになっている。

特別経費における学術基盤整備室関係の予算については、基盤的設備等整備分として学内 LAN 等、図書館設備、文化的・学術的な資料等の保存等の事項で予算要求している。

全国共同利用共同実施分の関係では、学際大規模情報基盤共同利用・共同研究拠点における共同研究推進に関する要求を行っている。

文部科学省全体の予算構成としては、対前年度１，６０９億円、２．９％の増額要求となっており、日本再生重点化措置、東日本大震災の復興・復旧にかかる特別枠分以外では、減額となっている。

また、情報課関係では、革新的ハイパフォーマンス・コンピューティング・インフラ(HPCI)構築の予算を、日本再生重点化措置も含めて要求を行っている。

HPCI については、現在、利用課題選定の在り方に関する検討や、計算資源提供機関に対し詳細設計の中間報告及び意見集約の場を設け、テスト運用への準備を進めているところ。来年１１月に供用開始を予定しており、各情報系センター関係者に引き続き協力をお願いしたい。

日本再生重点化措置の予算枠は７，０００億円であるが、２兆円を大きく上回る要求が出ているため、国立大学法人運営費交付金、HPCI システム関係予算を含めて、１２月の予算編成の段階でどのような形になるかは全く分からない状況である。

特に、日本再生重点化措置についてはかなり厳しい状況である。

学術基盤整備室では、各大学の要望を踏まえて学内 LAN 等の基盤的な整備等の要求を行っている。

学術基盤整備室では、大学の基盤を支える情報関係と図書館の予算を担当しており、

大学の基盤を支える経費について予算措置を行いたいという希望はあるが、各大学の基盤的整備については、省内、財務省への説明においても、各大学が本来行うことであるため、基本的には運営費交付金での措置を行うように言われている。

一方、大学の規模や現状において、学内 LAN の整備など大学では整備が厳しい内容については、ぎりぎりの形で要求を行っているが、各センター長には、大学を支える情報基盤の重要性を、日頃から学内外に訴えていただきたい。

２）　第４期科学技術基本計画について

昨年１２月に「科学技術に関する基本政策について」として、それまでの検討の結果が取りまとめられ、平成２２年度中に策定予定だったが、東日本大震災を受け、総合科学技術会議において内容を再検討することになり、平成２３年８月１９日に閣議決定された。

基本的な考え方としては、第一に国として目指すべき社会の姿を明らかにし、その実現のためにとるべき科学技術イノベーション政策の在り方を提示している。

第二に、今回の大震災、特に福島第一原子力発電所の事故によって、国民が原子力技術に対し不安を持っていることから、これまでの科学技術政策を真摯に再検討し、科学技術イノベーション政策について国民の理解と信頼を得る取り組みを進める必要があること、などが述べられている。研究者、技術者等の説明不足に基づく混乱や、一方で、科学技術基本計画を推進していくためにはもちろん予算が必要であり、そのためには国民の理解が必要になることから、各大学における活動について、日頃から国民への説明等を通して理解を得る努力が必要である。特に、科学技術関係の政策の中で目に見えやすい技術、例えばはやぶさなどの宇宙関係や、医療関係については国民へ説明を行いやすいが、情報関係など基盤部分については見えにくい部分であり、このような部分への予算措置は、見えやすい研究を説明する以上に困難なことである。このため、各センター長には十分な説明を行うよう協力をお願いするとともに、学術基盤整備室としても、基盤の重要性を引き続き各方面に地道に説明をしていきたい第４期科学技術基本計画においても､研究情報基盤の整備という項目において､学協会が刊行する論文誌の電子化、国立国会図書館や大学図書館が保有する人文社会科学も含めた文献、資料の電子化及びオープンアクセスの推進、電子ジャーナルの効率的、安定的な購読が可能となるよう有効な方策を検討することが期待されている。

３）　科学技術・学術審議会　学術分科会　研究環境基盤部会　学術情報基盤作業部会における審議状況について

学術情報基盤作業部会においては､「コンピュータ及びネットワーク」､「大学図書館」､「学術情報発信」の三つの柱の在り方について検討を進めており､平成１８年３月に「学術基盤の今後の在り方について」として総合的な取りまとめが行われた。コンピュータ及びネットワークに関しては、平成２０年１２月に「学術情報基盤整備に関する対応方

策について」が取りまとめられた。また、平成２１年７月には「大学図書館の整備及び学術情報流通の在り方について」が取りまとめられた。平成２２年１２月には、大学図書館の機能・役割や、大学図書館職員の育成・確保の必要性などについて指摘した「大学図書館の整備について」が取りまとめられた。

本年４月からの第６期の作業部会においては、学術情報流通発信に関する強化、拡充などについての検討が進められている。

４）　平成２２年度「学術情報基盤実態調査」結果について

各情報系センターからも協力を得て取りまとめており、コンピュータ及びネットワーク編と図書館編と、二つに分かれている。

コンピュータ及びネットワーク編については、例年と比較して大きな変化はない。ただ、課題面については、セキュリティポリシーの策定やセキュリティ対策の充実を挙げている大学が多く、セキュリティに関連する対策について各大学が腐心しておられる状況がうかがえる。

平成２３年度の調査は、情報系センター協議会からも助言を得て、現在、総務省との協議を進めており、協議が終了した段階で各大学へ依頼を行う。その節はご協力のほど、よろしくお願い申し上げる。

５）　平成２３年度　国立大学情報系センター協議会　要望事項について

例年は、情報系センター協議会総会において説明を行っているが、今年については、センター協議会総会が延期されたため、資料２－２に基づき本センター長会議にて説明を行わせていただく。

セキュリティを含めたコンピュータネットワークの維持・更新の経費に関する要望が多数あるが、概算要求に関する説明でも申し上げたとおり、基盤的部分については、国立大学法人の運営費交付金の中にその整備を行う経費は措置済みであるということが、財政当局の見解であり、基盤関係の整備に関しては、各大学の中で大学執行部の理解を得て、措置を行う努力をお願いしたい。

セキュリティ関係などについては、情報系センターの様々な課題などについて、本情報系センター協議会等の各大学のネットワークの活用をお願いしたい。

また、法人化後、国として対応できる部分は非常に狭くなってきている部分もあるため、各国立大学法人については、ご協力をお願いしたい。

次に、著作権関係の要望に関して、e ラーニング関係のコンテンツを作成する際の著作権の取り扱いについては、一昨年１月の「著作権分科会報告書」においても、関係者からの具体の提案や関係者間の協議状況を踏まえて検討することになっている。学術基盤整備室としても、各大学からの具体的な情報を元に、必要があれば文化庁著作権課への橋渡しが可能である。

最後に、本協議会のような場を利用して、各情報系センター間の連携を密にしていくとともに、文部科学省情報課にも様々な情報を提供していただき、必要に応じて一緒に検討させていただきたいとのあいさつがあった。

7　国立情報学研究所説明

安達学術基盤推進部長から、学術情報基盤整備の現況について、資料３に基づき以下の説明があった。

1）SINET4 のネットワーク構成と増強計画について

平成２３年４月から、向こう５年間の運用予定で、SINET4 の運用を開始した。SINET4 では、民間のデータセンターをエッジノードとした。また、平成２３年度中に全国すべての都道府県にエッジノードを整備する。

現在、ノード校と呼ばれている、大学に設置された接続環境経由で SINET に繋がっている大学が多いが、この環境は SINET4 終了時にはなくなるので、SINET4 で採用した最寄りの民間のデータセンターへの接続移行を、平成２７年度末までに実施するようにお願いしたい。

なお、移行するにあたり、接続に関わる問題が通信会社等と生じた場合には、国立情報学研究所　学術基盤課にお問合せくだされば、調整を行う。また平成２３年度中に、東京－大阪間の４０G の帯域を８０G に、東京－札幌間の帯域を１０G から４０G に増速する予定である。

2）SINET の利用例について

神戸で運用を開始する「京」も関係している HPCI は、SINET を通じて、大学関係者、および企業から利用を行うことができるようになる。

また HPCI において、国立情報学研究所はネットワークの他、認証も担当している。

3）商用クラウドサービスを活用した大学等のプライベートクラウド構築へのサポート

SINET を通じて、商用のクラウドサービスを用いたセキュアなプライベートクラウドを構築できる。

商業クラウド提供業者のサービスを、SINET のネットワークと直接接続し、VPN を用いてセキュアに利用することが可能である。すでに、東京農工大学等で実績がある。

4）東日本大震災時の影響について

東日本大震災の時に、SINET の回線が一部の地域で切れる障害が発生したが、エッジ回線、コア回線は、全て二重化し、ネットワークとして冗長経路を確保していたため、バックボーンのサービス断は発生しなかった。

また、弘前では１７時間、山形では２８時間、仙台では９６時間の停電が発生したが、

SINET が利用しているデータセンターでは、自前の電源供給施設があるため、SINET の機能停止にはいたらず、信頼を失うことなく運用を続けられた。

5）学術認証フェデレーションについて

学術認証フェデレーション（「学認」）とは、各大学内で構築されている認証基盤を、統一的な認証技術を用いて連携させることで、シングルサインオンで、各大学で利用されている様々なサービスが組織を超えて活用できるようにするものである。

現在、学認への参加は、３０機関ほどある。また、この認証により利用できるサービスは３０ほどあり、主なサービスは、電子ジャーナルの利用である。

学認に参加するメリットについては、学認のホームページ上で参加機関のケーススタディを掲載しているので、参考にしてほしい。

また、認証環境の構築に関する研修会も、国立情報学研究所で開催しているので、参加の検討をお願いしたい。

なお、今後、e-Rad とも連携する可能性もあるため、学認が一層の広がりをもつと予想している。

6）サーバ証明書発行プロジェクトの継続について

サーバ証明書発行プロジェクトの現行体制を維持し、平成２７年３月までサーバ証明書発行サービスも無償で継続する。

7）共用リポジトリサービスについて

独自で機関リポジトリの構築・運用が難しい機関に対して、ハードウェア及びソフトウェアを国立情報学研究所が管理・運用を行う、共用リポジトリサービスを平成２４年４月から提供していく予定であり、サービス利用の検討をお願いしたい。

8）国立情報学研究所への要望に対する回答について

国立情報学研究所への要望について、資料３に基づき回答するが、今後とも、要望等がある場合は、学術基盤推進部　学術基盤課へ連絡をお願いしたい。

8　基調講演

静岡大学の長谷川副センター長から、「ISMS からクラウド情報基盤への展開」について資料４に基づき基調講演が行われた。その概要は次のとおりである。

1）静岡大学の紹介

静岡大学は、浜松キャンパスと静岡キャンパスの二つに分かれており、それぞれに教職員及び学生が６，０００名ずつ合わせて１２，０００名である。

２）情報基盤センターについて

情報基盤センターは、教職員１４名と情報企画課６名の計２０名で構成されており、浜松キャンパス、静岡キャンパスに在籍する１２，０００名の教職員・学生が利用する情報インフラ整備とサービスを行っている。また、静岡大学の情報基盤の構築に協力いただいた企業から１３名を客員教員として招き、基盤構築のノウハウについて助言いただいている。

３）ＩＳＭＳについて

ISMS とは、ISO/IEC27001 によって定められた規格である。ISMS を確立するためには、いくつかの要求事項があり、その中で情報資産を識別しリスクアセスメントを実施していくことが手間のかかる部分である。それらの要求事項全体をＰＤＣＡサイクルで循環させていき、年１回外部審査機関による審査を受けることになっている。ISMS 認証事業者数については、２００２年から規格化がはじまり、静岡大学が認証を取得した２００３年当時の事業者数は２００程度であったが、現在は３８９６まで増加している。国立大学では５大学が認証されている。ISMS の規格書はＰＤＣＡの構造がそのまま書かれており、ISMS の特徴としては、１３３の詳細な管理策が存在し選択した管理策それぞれについて手順書が存在していることが規格で求められている。規格要求事項の第４章が規格の中心構造になっており、規格全体と管理策について文書化することが求められている。情報資産を保有するとリスクが発生するが、そのリスク対応として管理策による低減、サービスの廃止等によるリスク回避、クラウドサーバ等によるリスク移転などが挙げられる。静岡大学の２０１１年の ISMS 審査は不適合０件、改善の機会６件、グッドポイント３件という結果であった。受動的なセキュリティ対策から、能動的なセキュリティ活動へ変更するきっかけとなった ISMS 認証であるが、クラウドコンピューティングとのバランスを取りながら認証継続していくことを目標としている。

４）クラウドコンピューティングについて

ネットワーク上にサーバ資源を保管することが一つのクラウドの流れである。クラウドの特徴としては、拡張性や可用性、経済性等を含む５つの特徴があり、クラウド化の種類としては、アプリケーションのクラウド化、サーバやストレージのクラウド化、データベース等のミドルウェアのクラウド化等がある。クラウド化推進においては、財源の枯渇や、震災の危機等の様々な問題を計測し数量化することが合意形成のポイントとなった。クラウド化によって、ＩＴ投資コストの低減や、大規模災害時における事業継続(BCP)危機への対策、ＩＴ機器の消費電力料金の削減などの効果が期待される。

情報基盤としては、PRCC と PBCC の二階層のクラウドレイヤによって確立し、商用 iDC を活用したアウトソースを実現しており、また、学認への参加も進めている。廉価な商用パブリッククラウドサーバサービスを開始し、教職員に対して無償提供を行っており

現在２００台以上が利用されている。

5）全学安否情報システムについて

平成２３年3月１１日の東日本大震災時には､約 12,000 名の登録者の内 7,650 名の安否情報を収集することができた。GPS 対応携帯により、自分の位置情報を登録し表示する機能を付けている。安否確認の訓練では、３日間で登録者の 70%の安否情報をシステムで回収することができ、訓練開始１３日後には 91.4%の安否情報を確認することができた。学生・教職員からも好評であった。

6）節電システムについて

節電システムを｢パンドラシステム｣と呼んでおり､各キャンパスの契約電力量の 90%に達した時点で登録されているメールアドレスへ警報メールが通知される。学内では、１分間隔で各建物の各部屋単位で消費電力量が見えるようになっている。消費電力がピークカットレベルに達した場合は、１５分間隔で各棟の空調出力レベルを調整するなど不快感を与えないように遠隔で調整を行っている。基本電力量を 10%以上削減できている。

7）パブリッククラウドの利用満足度アンケートについて

パブリッククラウドサービス開始日から３ヶ月後に利用満足度アンケートを実施した。セキュリティについては 90%が「学内同等」以上と評価し、総合評価では 90%以上が「学内同等」以上と評価した。

9　議長選出

宮崎大学の廿日出情報基盤センター長が議長として選出された。

１０　議　事

議長の議事進行のもと、次の議題等について協議を行った。

（1）　報告事項

ア　第２３回情報処理センター等担当者技術研究会について

技術研究会当番校である室蘭工業大学の刀川情報メディア教育センター長から、資料５に基づき次の報告があった。

第２３回情報処理センター等担当者技術研究会が、平成２３年８月２５日（木）及び２６日（金）に開催され７７名が参加した。今回の特徴として、情報メディアセンターの演習室を会場とし、教育システムのパソコンを実際に使用することで施

設見学の一環とした。また、特別講演としてさくらインターネット(株)の田中邦弘社長を招き石狩データセンターの紹介として講演していただいた。「世話人会」の名称変更を行い、「運用連絡会議」とした。
次回は佐賀大学で開催される予定である。

イ　第６回国立大学法人系センター研究交流・連絡会議及び第１５回学術情報処理研究集会について

研究交流・連絡会議当番校である三重大学の松岡総合情報処理センター長から、資料６に基づき次の報告があった。

第６回国立大学法人系センター研究交流・連絡会議及び第１５回学術情報処理研究集会を、９月１５日（木)、１６日（金）に総合研究棟Ⅱ１F メディアホールを会場として開催した。参加大学は５９大学１１１名が参加した。平成２２年度に設置した検討 WG の結果、センター長会議について平成２３年の宮崎大学を最後とし、次年度以降は総会時にセンター長懇談会を併設することとしたため、「学術情報処理研究」の査読体制が問題となった。検討の結果以下のような体制で査読を行う事となった。

・当該年度及び前年度の学術情報処理研究集会開催校が中心となって実施する。
・主査は前年度の学術情報処理研究集会開催校のセンター長が務める。
・一つの論文に所属の異なる２名の査読者を充てる。
・開催校以外からも査読者を依頼する。
・編集委員（査読者を含む）一覧を「学術情報処理研究」の最後に記載し、同一者に査読負担が集中しないように配慮する。

学術情報処理研究投稿規程の査読者について規程の改定を行う提案があり、研究集会の運営委員について、現行の４校体制からいずれ２校体制にするという結論に至ったことが報告された。

ウ　「PI アドレスへの課金への対応」に関する WG 報告

佐賀大学の只木総合情報基盤センター長から、資料７に基づき次の報告があった。

歴史的 PI アドレス課金対策検討のためのアンケートについて回答校は５７校であった。この５７校について課金が行われた場合に総額が 22,229 千円となり、５７校分のPIアドレスを１つの組織に集約した場合は1,889千円となることが報告された。PI アドレス維持費を各大学が単独で負担する場合と１つの組織で集約した場合では各大学の負担額が大幅に削減できるため、国立情報学研究所に取り纏めをお願いし、管理組織として「歴史的 PI アドレス管理部会（仮称)」を設置することが提案された。

国立情報学研究所の安達学術基盤推進部長から、国立情報学研究所へ PI アドレスを移転し集約した場合に、各大学の管理権が消滅する可能性があること、提案さ

れた内容で集約を行った場合に、維持費が安くなるか定かではないとの意見があり、PI アドレスへの課金への対応については、国立情報学研究所と対策 WG で今後、検討していくこととなった。

（2）議　　題

ア　情報系センター協議会の３会議の在り方

佐賀大学の只木総合情報基盤センター長から、平成２２年度に設置された検討 WG において、情報系センター協議会の３会議の在り方について議論を行い、３会議には機能の重複がみられることや、意志決定に曖昧さがある等の問題点があることから、WG ではセンター長会議を今年度までとし総会と研究集会の２会議に整理して、総会時にセンター長懇談会を同時開催することで結論を得たとの報告があった。

また、情報系センター協議会の性格付けの整理や、幹事会の機能強化、事務局の設置等については、今後も検討が必要との報告も併せてあった。センター長会議の単独の開催については、今年度で最後とし、総会と同時開催するセンター長懇談会とすることで決定したいと提案があり、拍手により承認され、次回の総会の議題とすることとなった。また、関連して、報告事項イの「学術情報処理研究」の査読体制について、査読者を２名とする提案についても、拍手により承認された。

イ　大学 ICT 推進協議会について

熊本大学の宇佐川情報化担当学長特別補佐から、大学 ICT 推進協議会設置の経緯や目的、総会や年次大会等の予定等について、次のとおり説明があった。

アメリカの EDUCAUSE では２，０００もの大学が参加しており、ICT を利用した教育・研究の高度化だけでなく、各大学の CIO が参加して経営的な視点から ICT をどのように活用するかという議論が行われている。日本でも高等教育・学術研究機関の経営効率化が大きな問題となっていることから、「ICT を利用した教育・研究・経営の高度化」を目的として大学 ICT 推進協議会を設立した。2010 年 12 月 11 日に設立総会を行い、2011 年 5 月 28 日には第 1 回通常総会を一橋記念講堂で開催した。2011 年 12 月 7 日（水）から 9 日（金）には、2011 年度年次大会の開催を予定している。会員数については 2011 年 10 月 7 日時点で４４大学、２２社が参加している。年次大会では、CIO 向けセッション（クローズド）、ソフトウェアライセンスや認証連携等の専門性の高い企画セッションを提供している。

ウ　大規模災害に備えたクラウド化やアウトソーシング化の現状と課題について

島根大学から、各大学のアウトソーシング化の現状と課題について意見交換を行い大規模災害に備えたクラウドサービスやアウトソーシングの利用、また、各大学が検討を進めている事例等について情報交換を行うことを目的として事前に提案されていたが、本日、提案者の野田総合情報処理センター長が欠席であることと、議

題エの内容と共通する部分が多いことから、議題エの中で議論することとした。

エ　クラウド環境の活用に向けたセキュリティポリシーのあり方について

信州大学の不破総合情報センター長から、業務の効率化及び大規模災害発生時の業務の継続という観点からクラウドの活用を検討しているが、学内の様々なシステムについてクラウド活用を進めていく場合にセキュリティが重要となるため、クラウドの契約を行う際の注意点やクラウド環境の活用に向けた大学のセキュリティポリシーの整備について、多くの大学と情報共有を行いたいとの説明があった。

これに対し、一橋大学の高見澤情報基盤副センター長から、３年程前から学生系メールとしてGoogleのGmailを活用している。また、平成２３年４月から教員系メールもGmailに移行している。メールシステムについてのユーザーの要望としては、可用性と機密性が保証されていることが重要とされ、学内でメールサーバを運用している場合に、計画停電やネットワークトラブルが発生した場合には、メールが利用できなくなった事例もある。このような場合にも、クラウドを活用する事で可用性を確保することができる。Googleとの契約についての内容を公開することはできないが、通常の利用契約に加え、大学独自の内容を含ませたオプション契約を行うことも可能であるため、セキュリティポリシーに沿った契約も可能であるとの説明がされた。

次に、国立情報学研究所の安達学術基盤推進部長から、SINET 関連の説明会の開催を予定しており、その中で、「セキュリティポリシーのクラウド対応にについて」というセッションを設けていること、また、１２月にオープンフォーラムを開催するが、その中で、セキュリティポリシーとクラウドとの対応について事例紹介することが報告された。

次に、千葉大学の井宮総合メディア基盤センター長から、大学附属病院においては、ホームページや安否確認システムについてアウトソーシングしており、緊急時にも最低限の情報発信等ができるよう整備していることが報告された。

オ　国立大学法人の情報サービス資源の最適配分、及びユーザーに提供する枠組みを考える

東京外国語大学の佐野総合情報コラボレーションセンター長から、先ほど千葉大学や一橋大学から報告が行われたが、各大学とも事情も規模も異なるため、取り組めない事項等も多々あり中堅大学や単科大では厳しい状況である。また、交流会等で情報交換を行い、各大学が取り組まれているような先進的な取り組みを推進していきたいと思案するものの、人的面、予算面等の問題があり中堅以上の大学と、中堅大学や単科大で毎年差が広がっているため、先程、佐賀大から提案があったセンター協議会再編の中で事務局を作り、有用な意見や経験等がより効率的に各大学で利用できるよう進めてほしいとの提案がされた。

これに対し佐賀大学の只木総合情報基盤センター長から、検討 WG では総会等の様々な会議について、開催の案内や過去の履歴等の整理を東京農工大学がボランティアで行っているが、今後、継続して会議や WG 等で議論を行っていくためには、ボランティアではない事務局が必要となるのではないかということで提案を行ったとの報告がされた。しかし、事務局を設置する場合には、センター協議会で会費を徴収するのかなどの課題もあることが説明され、これについては、センター長会議の議題ではないので、次回の総会での継続審議事項とすることで、承認された。

カ　その他

電気通信大学の小池情報基盤センター長から、今年度の総会が震災の影響で中止となったため、来年度の総会の開催校については、電気通信大学と東京学芸大学の２校で協議して決定したいとの提案があり、２校に一任されることとで承認された。

１１　閉会

青木副センター長から、会議の閉会宣言が行われ本会議を終了した。

１２　その他

情報交換会の冒頭、宮崎大学の廿日出情報基盤センター長から、来年の研究交流・連絡会議の当番校は、香川大学にお願いしたいとの提案があり承認された。

（以上）

○配付資料：

資料１　第６回国立大学法人情報系センター長会議
資料２－１　学術情報基盤等に関する最近の動向等について（文部科学省説明資料）
資料２－２　平成２３年度　国立大学情報系センター協議会　要望事項について
＜要望・質問事項件数：　１９件＞
資料３　学術情報基盤整備の現況について（国立情報学研究所説明資料）
資料４　基調講演「ＩＳＭＳからクラウド情報基盤への展開」
資料５　第２３回情報処理センター等担当者技術研究会実施報告
資料６　第６回国立大学法人情報系センター研究交流・連絡会議及び第１５回学術情報処理研究集会について
資料７　歴史的ＰＩアドレス課金対策検討のためのアンケート結果報告
資料８　国立大学法人情報系センター協議会の３会議の在り方
資料９　AXIES　大学 ICT 推進協議会について

第６回国立大学法人情報系センター研究交流・連絡会議　報告

三重大学総合情報処理センター長　松岡　守

開催日時：平成 23 年 9 月 15 日(木) 13:30 ～ 17:00
開催場所：三重大学総合研究棟Ⅱ1F　メディアホール

参加者：計 58 **大学** 107 名

配布資料：

1. 第６回国立大学法人情報系センター研究交流・連絡会議及び第 １５回学術情報処理研究集会出席者名簿
2. 第６回国立大学法人情報系センター研究交流・連絡会議議事次第
3. 第 6 回情報系センター研究交流・連絡会議資料
4. 学術及び総合情報処理センター　センター長会議，研究交流・連絡会議　開催校一覧
5. 第 15 回学術情報処理研究集会プログラム
6. 学術情報処理研究　№15　2011
7. 三重大学総合情報処理センター・パンフレット，三重大学概要，他

会議次第：

1. 開会の挨拶 三重大学 総合情報処理センター長 松岡 守
2. 開催校挨拶 三重大学 評価・情報担当理事 滝 和郎
3. 議長選出
4. 【議事１】ＢＣＰ・災害対策～東日本大震災に学ぶ～
   ◇セッション概要紹介
   ・震災事例紹介（福島大学・本田 修啓）
   ・震災事例紹介（岩手大学・吉田 等明）
   ・震災事例紹介（弘前大学・佐藤 友暁）
   ・災害対策事例紹介（信州大学・鈴木 彦文）
   ◇討論
5. 【議事２】クラウドと災害対策
   ◇セッション概要紹介
   ・パブリッククラウド事例紹介（岡山大学・岡山 聖彦）
   ・クラウド共同調達提案（埼玉大学・吉田 紀彦）
   ◇災害対策：「バックアップ」について
   ・データバックアップ事例紹介（岐阜大学・佐藤 俊介）

・大学間バックアップ事例紹介（お茶の水女子大学・佐藤 祐子）
・大学間データバックアップ提案（三重大学・杉浦 徳宏）

◇討論

6.【議事３】募集議題より
・e-learning システムの利用促進について（島根大学・小林 聡）
・歴史的 PI アドレスの課金等に対する意見・検討（佐賀大学・只木 進一）
・その他

7.【議事４】情報系センター協議会の３会議のあり方について
検討WG主査 佐賀大学 総合情報基盤センター長 只木進一

8. 閉会

議事内容：

議事１では，東日本大震災の影響を強く受けた大学より，大学の情報ネットワークを中心とした震災の状況，その後の対応についての報告がされた。これに続き議事 2 では，採択対策を意識したクラウド，データバックアップの事例報告がなされた。議事 3 では，e-learning システムの利用促進，及び歴史的 PI アドレスの課金問題についての報告，意見交換がされた。議事 4 では情報系センター協議会の 3 会議の在り方について只木佐賀大学総合情報基盤センター長より問題提起がなされ，今後の「学術情報処理研究」の査読体制について国立大学法人情報系センター長会議に提案することとした。

第 15 回学術情報処理研究集会　報告

三重大学総合情報処理センター長　松岡　守

開催日時：平成 23 年 9 月 16 日(木) 9:30 ～ 17:00

開催場所：三重大学総合研究棟Ⅱ1F　メディアホール

研究発表：以下計 21 件（発表 12 分，質疑応答 5 分）の報告があった。

ネットワーク・システムの構築	5 件
ネットワーク・システムの運用	4 件
認証システム	4 件
情報処理教育	4 件
センター運営	4 件

参加者：計 58 大学 106 名

学術情報処理研究投稿規定（暫定）

平成 24年　　月　　日　改定

（平成11 年5 月13 日改定）

（平成10 年4 月16 日制定）

1．本誌に掲載する記事は未発表のもので、その分野と種類は以下のとおりとする。

分野

（1） 学術情報処理の研究・開発、教育に関するもの

（2） 情報系センターシステムの設計・管理・運用に関するもの

種類

（1） 査読付き論文

（2） 学術情報処理研究集会予稿

（3） 解説・記事

（4） 報告（※研究報告は対象外）

（5） その他

2．投稿者は、原則として大学の情報系センター関係者・利用者とするが、必ずしもこれに限るものではない。

3．査読者は、編集委員会の議を経て、編集委員長がその該当分野の専門知識を有するものに依頼する。1つの論文の査読は2名により行う。1名の査読者が掲載不可と判断した場合、更に1名の査読者の判断を追加し、合計3名の多数決により掲載の可否を決定するものとする。尚、査読者は非公開とする。

4．原稿の分量は以下とする。

査読付き論文	標準10,000字（6～8ページ），最大12ページ程度まで
学術情報処理研究集会予稿	6ページ程度まで
上記以外	6ページ程度まで

（ページ数は刷り上がり時を示す）

5．校正の際に原文を大きく改変することは許されない。

6．本誌は冊子体で配布するほか、同じ内容がWWWにより公開される。

7． 査読付き論文の場合、有料で別刷り50 部を最低とし、それ以上は50 部単位で受け付ける。

8．本誌に掲載された著作物の著作権は、すべて編集委員会に属することとする。

9．その他の詳細は、別途「原稿の作成の手引き」によるものとする。

編集後記

この「学術情報処理研究」は今回で第 16 号となります。この冊子に掲載される論文は第 15 号までは 1 名の査読によるものでしたが，本号より 2 名による査読体制となり，より権威ある学術誌へと歩みを進めることとなりました。編集サイドとしては従来とは異なる対応が必要となり，投稿者，編集委員，査読をお願いした方々にご迷惑をおかけした部分もあったかと思いますが，最終的にはこのように刊行にこぎつけることができました。関係の方々のご理解ご協力にまずは感謝申し上げます。

投稿論文を見ますとネットワーク・システム関係，情報処理教育関係，セキュリティ管理関係，センター運営関係，学内情報サービス関係，災害対策関係と多岐に亘っています。情報ネットワークの進化は指数関数的であり，その利用方法も広がると同時に脅威の程度も広がり，深刻さを増しています。また大きな災害時における情報ネットワークの重要さがあらためて確認されてきています。投稿論文はちょうどこうした情報ネットワークを取り巻く状況を反映したものとなっていると感じます。

情報ネットワークを取り巻く状況，重要さはそのまま大学の情報系センター業務にあてはまるものです。この学術情報処理研究には他の学術誌には見られない，センター業務に深くかかわる事項について詳細な記述がされている論文が多々あり，情報系センター相互に有用な情報と思います。このように本誌が情報系センターの皆さまにはもちろん，ひろく情報ネットワークの発展につながることを期待します。

「学術情報処理研究」
編集委員会主査　松岡　守

「学術情報処理研究」編集委員会

委員長	松岡　守　（三重大学）	廿日出　勇（宮崎大学）
	本田　道夫（香川大学）	杉浦　徳宏（三重大学）
	松澤　英之（宮崎大学）	林　敏浩　（香川大学）

学術情報処理研究 No.16　2012
Journal for Academic Computing Networking
2012 年 8 月編集
2012 年 9 月 13 日発行

編集　　「学術情報処理研究」編集委員会
委員長　松岡　守

発行　　香川大学総合情報センター
〒760-8523　香川県高松市幸町 2-1
TEL 087-832-1292
MAIL nipc@cc.kagawa-u.ac.jp

URL　　http://www.kagawa-u.ac.jp/itc/ipc2012/

ISSN　　1343-2915

Journal for Academic Computing and Networking

学術情報処理研究

No.16　2012

学術情報処理研究編集委員会