

活動報告

香川大学の情報戦略 ～平成 29 年度活動報告～

林 敏浩¹ 福家 隆² 近藤まゆみ² 末廣紀史²
T.Hayashi¹ T.Fuke² M.Kondo² N.Suehiro²
(総合情報センター¹, 情報グループ²)

1. まえがき

総合情報センター情報戦略部門は、香川大学の情報システム（コンピューターシステム、ネットワークシステム、事務系の業務システムなど）、大学情報及び情報基盤の戦略的整備計画の策定に関する基幹タスクを担っている。また、情報戦略部門では教育戦略室、大学教育基盤センターICT 教育部などの学内組織と連携した業務もある。本稿では、平成 29 年度の情報戦略部門の活動を概説する。

2. 基幹システムの更新・運用

平成 29 年度は、図 1 に示すネットワークシステム、キャンパス間回線、コンピューターシステムを更新した。これらの変更に合わせて、効率的なシステム構築と安定稼働の環境確保の検討などを継続的に実施した。従来、コンピューターシステムの更新の半年後に、ネットワークシステムの更新というサイクルであったが、データセンター移行には、ネットワーク基盤を固める必要があるため、コンピューターシステムのリースを 1 年間延長し、ネットワークシステムとコンピューターシステムの更新時期の順序を入れ替えた。また、図 2 に示す事務系の業務システムも、サーバ OS、クライアント OS

サポート終了時期を勘案し、継続的に担当部署と更新計画を策定し、導入業者との調整を行った。

3. 総合情報センター業務継続計画（BCP）

情報戦略部門では、災害発生時の具体的な復旧手順（復電の方法、サーバの起動方法など）のチェックリストを作成している。駆けつけたスタッフが誰でも復旧できるレベルまで詳細化したチェックリストを目指して内容をブラッシュアップした。

4. 他部署の支援・調整

従来、各部署でシステムを導入・更新する場合、総合情報センター・情報グループへ協力依頼範囲や内容が曖昧なまま、依頼されることが多かった。導入後の運用時、システム管理の役割分担が曖昧になることを防ぐため、「事務情報化に係るシステム導入・開発協力依頼書」により、担当部署の長から依頼いただくようにした。これにより、システム化の内容や運用における責任範囲を明確にできた。平成 29 年度は、学務系・総務系併せて 8 件のシステム新規案件の支援・調整を実施した。また、各部署の情報公開ページについて、学内のホームページ更新方法について調整・整理を実施した。

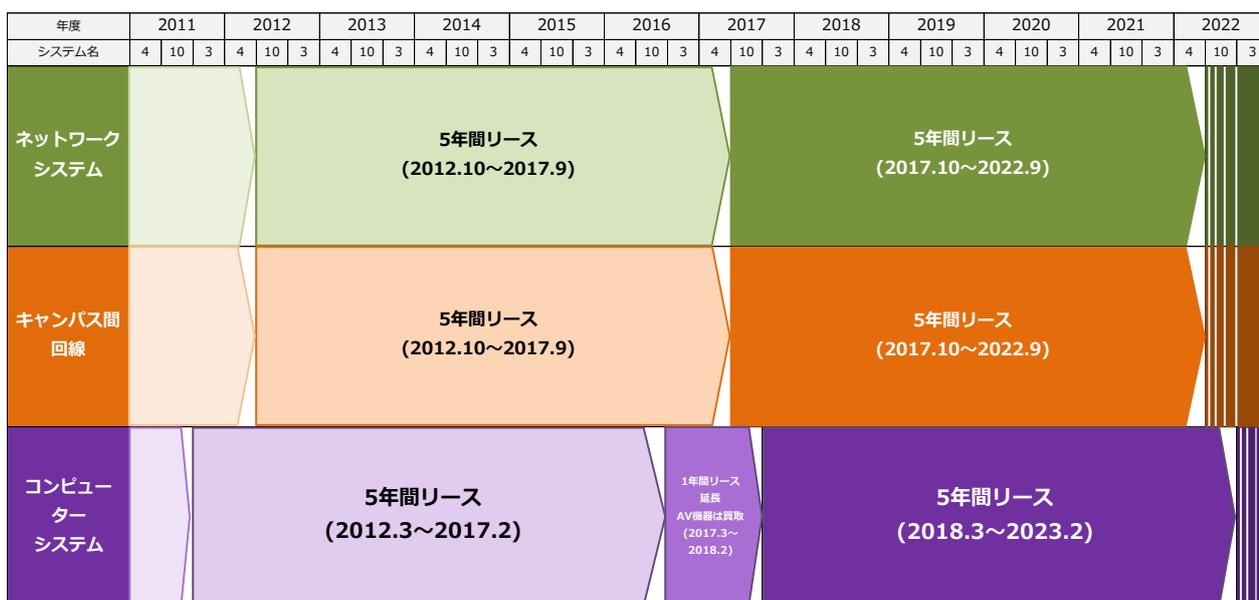


図 1. 総合情報センターの主なシステム更新の工程

区分	システム名	サーバOS	クライアントOS	平成27年度	平成28年度	平成29年度	平成30年度	平成31年度	平成32年度	平成33年度	平成34年度	平成35年度	
Server OS サポート終了予定	Windows Server 2003												
	Windows Server 2008, 2008 R2												
	Windows Server 2012, 2012 R2												
クライアントOS サポート終了予定	Windows Vista												
	Windows 7												
	Windows 8												
事務系システム	人事系	UPDS(人事給与システム)	2008R2	Win7					次期更新 予定				
		HR(人事評価システム)	2008R2	Win7					次期更新 予定				
	財務系	財務会計システム	2003→2012	Win7→ Win7,8,10		サーバ更新 システム更新 システム統合							次期更新 予定
		物品請求システム	2003→2012										
		科学研究費補助金システム	2008→2012										
		旅費システム	2008→2012										
	学務系	教務システム、免除システム	2008→2012	Win7		サーバ更新 システム統合				次期更新 予定			
		証明書発行システム	2003→2012	WinXP→Win7									
	GW	グループウェア (サイボウズガルーン)	RHEL5	web			SSharePoint を利用したス ステムに更新予 定						
	その他	大学基礎情報データベースシステム	2003→2012	web		サーバ更新 システム更新		後継システムに 移行準備中					

図 2. 事務系業務システムの更新計画

5. 第 3 期中期目標・中期計画に基づく平成 29 年度実績の総括

(1) クラウド化の推進，データセンター利用

ICT コスト削減，省エネルギー化，BCP 対策，コンプライアンス遵守等，これらを解決する方策として，多くの大学がクラウド化を進めている。香川大学でも同様に，平成 29 年度にハイブリッドクラウド環境（プライベートクラウド環境とパブリッククラウド環境の併用）を構築し，同環境に基幹システムを移設した。プライベートクラウド環境は，データセンター内に構築しており，従来よりセキュリティレベルが高いシステムとなっている。またネットワークも，データセンターを基幹とするスター型へ変更し，高耐障害性の構成となった。また，クラウド化は計算機資源の有効活用など教育研究の高度化や豊富化への貢献も期待される。

(2) 包括連携協定の締結

本学と株式会社 ST Net，リコージャパン株式会社は，相互の連携・協力を強化し地域の発展に寄与するため，地域活性化に資する研究交流，人材交流，人材育成，技術開発交流に関する連携・協力協定を締結した。既に共同研究や地域活性化イベント等の開催などで協力して取り組んできた実績があり，協定締結によりこれらをさらに発展させ，それぞれが有する人的・知的・物的資源を連携・協力して活用することにより，地域活性化に役立てる。

(3) 香川大学における LMS（学習管理システム）

基盤の安定した管理・運用について

e-Learning 利活用において複数 LMS 基盤の乱立が，教育の質保証等の観点から先行大学で問題（機器の管理・運用が不明確になる，ハードウェア・ソフトウェアの保守・更新計画が曖昧になる等）となっている。香川大学では大学教育基盤センター所掌の「香川大学 Moodle」（教員の講義支援），大学連携 e-Learning 教育支援センター四国所掌の「大学連携 Moodle」（四国国立 5 大学における共同授業実施）が同様な問題を発生する可能性があった。これに対して，香川大学総合情報センターコンピュータシステムに当該 LMS のハードウェアとソフトウェアを組み込み，さらに，LMS 基盤管理の一本化を図り，学習管理システム基盤として安定した管理・運用ができる環境を確立した。

6. まとめ

本稿では，平成 29 年度の総合情報センター情報戦略部門の活動を，基幹システムの更新・運用，総合情報センター業務継続計画，他部署の支援・調整，第 3 期中期目標・中期計画の観点から概説した。

第 3 期中期目標・中期計画について平成 29 年度は情報戦略として重要な案件が多かった。今後も，情報戦略部門として重要な判断が要求される場合が多々あると考える。このような可能性を踏まえ本学の情報戦略の要としての役割を認識して，今後とも迅速に質の高い業務遂行をこころがけたい。

教育デザイン部門紹介

藤本 憲市, 岡本 裕之, 豊嶋 尚子, 安土 正枝, 川瀬 舞, 井戸元 彩夏, 中川 えんじゅ
K. Fujimoto, H. Okamoto, N. Toyoshima, M. Azuchi, M. Kawase, A. Idomoto, E. Nakagawa
(香川大学)

1. まえがき

教育デザイン部門は、情報通信技術 (ICT) を活用した e-Learning 環境の整備計画や、そこで用いられる電子教材制作の支援に関することを担当しており、四国における大学連携 e-Learning 教育事業 (通称、知プラ e 事業) を支える学内組織の一つである。本報告では、本部門の平成 29 年度活動内容と平成 30 年度の活動予定について述べる。

2. 平成 29 年度活動報告

平成 29 年度の人員体制は、教員 1 名 (併任)、事務職員 1 名、技術補佐員 6 名であり、大学連携 e-Learning 科目 (知プラ e 科目) のコンテンツ制作支援及びそれら授業の運用支援のほか、その他の e-Learning 科目についても学内外からのコンテンツ制作の支援を行った。

2.1. ICT 活用教育環境の整備

大学連携 Moodle のスナップショットを図 1 に示す。この Moodle 上に知プラ e 科目の各種コンテンツ (講義映像、講義資料、小テスト問題、課題など) を配置し、コンテンツの配信管理、授業改善アンケートの集計、Moodle へのアクセス数管理、受講者からのシステムトラブルに関する質問対応など、授業運用における支援体制 (ICT 活用教育環境) を整備した。また、年度末には教育用コンピュータリプレースが実施されたため、旧大学連携 Moodle 及び旧香川大学 Moodle 上にあるコンテンツの新サーバへの移行、並びに、講義映像ファイルを旧ストリーミングサーバからクラウド (Microsoft Azure) への移行について作業支援も行った。



図 1 香川大学における大学連携 Moodle

平成 29 年度は、クォータ制導入に伴う 2 単位科目の分割もあり計 19 科目の e-Learning コンテンツを配信したが、いずれの科目も大きなトラブルなく運用することができた。

2.2. コンテンツの制作支援

Moodle 上で配信する講義映像の収録は、主に、総合情報センター 2 階にある e-Learning スタジオで行っている。平成 29 年度は、クォータ制導入に伴う主題科目の分割に係る追加コンテンツ、平成 30 年度以降に新規開講予定の知プラ e 科目及び全学必修科目 (主題 C-基礎科目) のコンテンツ、及び他大学開講科目の香川大学教員担当分のコンテンツの制作支援を行った。

3. 平成 30 年度活動計画

平成 30 年度は、大学連携 Moodle 上で第 1 クォータに 4 科目、第 2 クォータに 5 科目、第 3 クォータに 6 科目、第 4 クォータに 5 科目、及び後期 1 科目 (計 21 科目) の知プラ e 科目を配信予定であり、それら授業の運用を支援する予定である。

コンテンツ制作については、知プラ e 科目だけでなく、香川大学のみで開講する全学共通科目 (主題 C-基礎科目) や、他大学開講科目のコンテンツ制作も支援の対象となったことで、コンテンツ制作に係る業務量は今後も増加することが予想される。

その他、連携大学を遠隔で接続して実施する知プラ e 事業に関する委員会の運用支援、大学連携 e-Learning 教育支援センター四国ウェブサイト更新支援、eK4 ウェブサイト管理支援、

e-Learning に関するニュースレター制作・発行支援、知プラ e 事業成果報告書作成支援、知プラ e 科目履修に係るリーフレット等の作成支援、及び大学連携 Moodle におけるアクセスログ調査を行う予定である。

4. あとがき

本原稿執筆時において技術補佐員 1 名減 (現在公募中) の体制で業務を行っているが、平成 30 年度も引き続き、知プラ e 科目や主題 C-基礎科目を大過なく開講・運用できるよう、総合情報センタースタッフ、大学連携 e-Learning 教育支援センター四国スタッフ、及び知プラ e 科目担当教員の各位のご協力をお願いする次第である。

教育システム部門活動報告

～2017年度頑張ったこと、将来のこと～

八重樫 理人¹, 末廣 紀史², 近藤 まゆみ², 川口 政秀²,
R.Yaegashi¹, N.Suehiro², M.Kondo², M.Kawaguchi²
末光 京子², 香西 理恵³, 高橋 岳水⁴, 土居 敬典⁵
K.Suemitsu², R.Kouzai³, T.Takahashi⁴, T.Do⁵

(総合情報センター/創造工学部¹, 学術・地域連携推進室 情報グループ²,
総合情報センター³, 医学部情報ネットワーク管理室⁴, 農学部会計係⁵)

1. 教育システム部門の概要

教育システム部門は、教育システムを中心とした全学基盤システムの運用・分析・企画をおこなう組織である。現在、教員1名(併任)、職員7名で構成されている。

2017年度は6年ぶりのシステムリプレースを実施したため、全体構成やサービスの中身に変更があった点が多々ある。それらの報告として学内FD「コンピュータシステムの更新について～2017年度 頑張ったこと、将来のこと～」を2018年6月22日に開催した。本稿ではそこで発表した内容を中心に端的に報告する。

2. リプレースの全体コンセプト

2.1 2011年度前回リプレースの振り返り

当時としては先進的な技術として、ID統合管理システム、仮想サーバ基盤、学生用クラウドメール、ICカードでの生協マネー課金プリントなどを取り入れた基盤構築をおこなった。

6年の運用の中でID連携するシステムは増え、業務系サーバも仮想基盤に追加され、学生のメール利用率は向上し、印刷サービスに対する運用コストも軽減された。これらの成果より、リプレースでは基本的なサービス方式は変更せず、より高機能化する方針とした。

2.2 外的要因

i)クラウド化、BCP対策の強化

東日本大震災を契機に、災害時のデータ等の保全を強化すること、高度な物理セキュリティの環境で管理すること、光熱費や設備の維持管理・省スペース化をすることなど、プライベートクラウド

化やパブリッククラウドサービスの導入など広義なクラウド化を国も推進している。

ii)サイバー攻撃の増加

本学も標的型メール攻撃の対象となるインシデントが発生したが、全国的にも未知の攻撃への防衛システムや攻撃の証跡を確認するシステム、セキュリティ対策専門チームの構築、組織への教育・啓蒙活動など、セキュリティ対策の高度化も求められている。

iii)上位ネットワークの高速化

国際的にも学術ネットワークが高速化し、本学も前回リプレース時の2.4Gbpsから20Gbpsへ上位回線も拡張している。

iv)職員数の減、業務の変化

従来の「システムの維持をする業務」に加えて、他部署案件の要件定義や設計、提案や分析など、より上流の業務が増えてきている。組織として運用を効率化して新しい業務のあり方を検討していく必要がある。

2.3 4つのコンセプト

これらの外的要因を組織の課題として設定し、本学の主たるIT基盤リプレース3案件(教育システム、ネットワークシステム、キャンパス間回線)共通のコンセプトを決定した。

それは、

「BCP対策の強化」、

「全学的なプライベートクラウド推進」、

「セキュリティの強化」、

「運用管理業務のアウトソーシング」である。

具体的には、基幹スイッチとサーバ群のデータセンター設置、従量課金型かつリソース拡張が可能な基盤サーバ、ネットワーク認証強化及び重点クライアントのゼロデイ攻撃対応、セキュリティ分析やサーバ運用のアウトソーシングなどがある。

その他の点にも、コンセプトに基づいて詳細設計を進め、その方針を反映させる内容とした。

3. リプレイス後の具体的な 16 の話

全体コンセプトに基づいて教育システムのリプレイスは行われたが、より具体的なポイントについて学内の構成員にも情報共有する必要がある。

特にユーザーに影響のある、リプレイスを契機に変化があったことや、実現に向けて取組中の事柄 16 を下記に記す。

16 の事柄は関係者の立場によって、それぞれ重要性は大小あるが、いずれも近年中に完了すべき具体的な課題といえる。

(1).堅牢なデータセンターへの集約

基幹のスイッチやサーバ群を外部のデータセンターに集約した(図 1)。

香川県は歴史的に見ても大地震の発生回数は少なく、津波や台風、液状化、火山活動などのリスクも少ないことで知られている。また四国を中心とした防災拠点として位置づけられている。

全キャンパスから 30 分程度で訪問も可能な立地で、2 系統の特別高圧電力系統、生体認証など Tier4 基準を満たした高機能なデータセンターがあり、本学としては地理的にも設備的にも好条件なデータセンターに集約することができた。

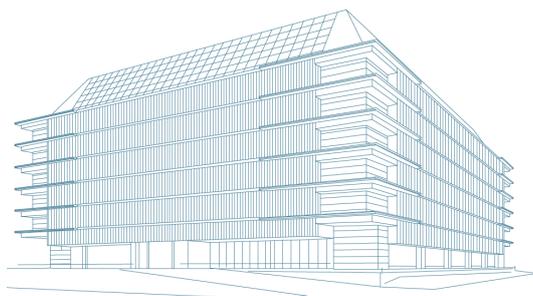


図 1 データセンター イメージ

(2).サーバ室の縮小、空調費削減(取組中)

データセンターに基幹機器が設置され、幸町地区のサーバ室の面積は半分程度まで縮小が可能であり、空調も大掛かりな床下空調設備から天吊空調などに変更が可能であることを試算した。

既に空調機は変更したが、引き続き余剰スペースの改修と有効活用を行なっていく。

(3).新しい学生ヘルプデスク体制(取組中)

余剰スペースの活用方法として、学生ヘルプデスクの職員が対応するスペースを拡張することを検討している。ユーザーサービス部門と協力し、ヘルプデスク職員間の共同作業や検証、授業準備などサービス内容を広範囲にしていく。



図 2 学生ヘルプデスク 変更イメージ

(4).学内の研究用、業務用サーバの集約(取組中)

データセンターに構築したプライベートサーバ基盤に、業務システムや研究用途のサーバ構築にも利用してもらい、基盤を拡張していくためのシステム・運用設計をすすめていく。

(5).学生用 PC スペックの向上

前システムではファットクライアントへのイメージ配信方式での PC 管理であったが、今回からはクライアントの SSD にキャッシュを蓄積するネットブート方式に変更した。

OS は windows10Enterprise(LTSB)とし、CPU・メモリの向上、HDD から SSD 化、ディスプレイサイズも 17 インチから 21.5 インチに向上した。

うち1教室はAdobe社製品を導入するため、メモリ・SSD容量を倍にし、CPU変更、ディスプレイも23インチに変更した教室を用意している。

(6).学生用PCの起動速度向上

前システムではPC起動時間の遅さが問題となっていた。今回のリプレースにおいては、不要なソフトウェアを棚卸しする運用をつくり、新規AD構築によるドメインポリシーの新規作成・チューニングを実施した。

電源ボタンをONにしてからログオンし、Office製品が起動するまでの時間を計測すると、前システムでは平均275秒ほどであったが、リプレース後は75秒まで改善した。

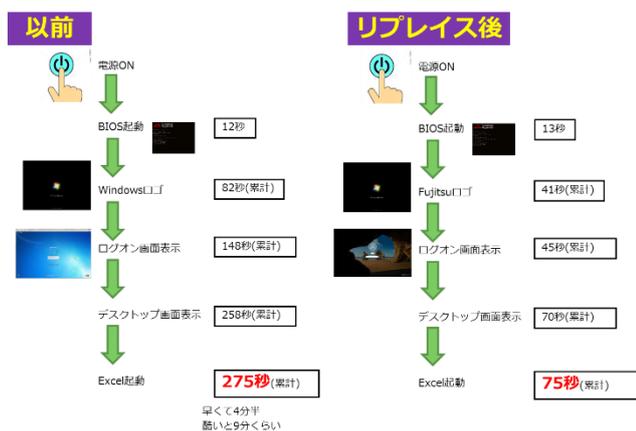


図3 起動速度の測定

(7).Adobe 導入教室の整備

前述のとおり、本学の創造工学部設置に合わせて、最新版のAdobe製品をデバイスライセンスで導入した教室を構築した。

創造工学部での授業用途以外にも、全学部学生の利用や一般の教職員の利用も想定している。一般利用者がアクセスのしやすい中央図書館内に構築したことで、全学的な利用が期待できる。

(8).授業用ソフトの追加に柔軟に対応(取組中)

ネットブート方式によって雛形の更新作業工数が減り、PCの中身の更新が比較的容易になった。

合わせてソフトウェア追加申請書とチェックの運用体制の整備を進めている。

(9).Hドライブに自動保存される対象を追加

本学のPC教室はHドライブをホームドライブとしてマッピングしているが、ドキュメントやピクチャ等のフォルダもリダイレクトするように設計変更をしている。学生が誤って作成したデータを削除するトラブルを軽減する。

デスクトップなどもリダイレクトすべきか、またHドライブのクォータ容量等を拡張するかは、運用を見ながら調整をしていく。

(10).PC操作統計データの取得(取組中)

以前は電源のON/OFF程度のログ集計を行っていたが、新システムではアプリケーションの起動や終了時間等も取得できる。

導入したソフトウェアが有効に使用されているか、学生がどのソフトを使用する傾向にあるか、クラッシュしたソフトは無いかなど、より利用実態の調査と分析が可能となった。

(11).PC教室環境の公開(取組中)

本学ではPC教室の環境を情報公開する整備が遅れている。各教室のPCスペックやAV機器、ソフトウェアの一覧などをホームページにて公開できるように準備をしている。

また、動画による利用マニュアルも作成し、授業者がどのような授業をできるか想像しやすいように整理を進めている。

(12).メールクラウド化による効率化(取組中)

本学は既に学生はクラウドメールに移行しているが、教職員はまだ学内メールサーバを使用している。システムの移行だけでなく、メールを中心とした現在業務のあり方を見直す検討もすすめている。

(13).メールセキュリティの見直し(取組中)

現在は部局ごとにメールサーバを管理しているため、アカウントの管理や有事の対応など脆弱な点が残ってしまっていた。

クラウドメールに統合する中で、アカウントの管理やセキュリティ対策システム構築、有事の対応など再度見直しを進めている。

(14).新メールアドレスの配布(取組中)

現在はメールアドレスについてもサブドメインが複数存在しているが、管理の集中化のためにワンドメインへ集約し、新たなメールアドレスへ統合を進める。既存のメールアドレスと整合性を取りながら、業務影響の少ない移行の段取りを現在調整している。

(15).メーリングリストの申請システム(取組中)

メーリングリストの管理についても、現在は曖昧な管理状況であるため、見直しを進めている。運用方式としては利用者が自らブラウザで利用申請をし、メンバーの登録を行い、承認を受ける形とする。管理者不在のメーリングリストが残らないよう、また、利便性を損なわないよう、設計を進めている。

(16).属人的でない運用体制(取組中)

最新の情報、過去の情報、ともに本学では情報共有が不十分であり、知識が属人的になりがちである。基盤システムの導入業者とともに、大学内および大学と企業間についても、効率的な情報共有の仕組みや運用を検討している。

システムに関するルーチンワークや、障害対応などにかかる工数を職員側も削減し、他の業務へ注力できることを目的としている。

システムを動かしながら、現在も改善に取り組んでいる最中である。

これら直近の取り組むべき課題とともに、AIやRPA, IoTなどの注目される技術を教育システムにも活用していけるかを評価すべく、外部からの情報収集も積極的に進めながら、取り組んでいく。

4. 2018年度活動目標

教育システムのリプレイスによって、前述のような課題を全て解決したわけではなく、新しいシ

香川大学ネットワークシステムの今昔

今井 慈郎¹ 山下 俊昭² 川口 政秀² 土居 敬典³ 高橋 岳水⁴
Y. Imai¹ T. Yamashita² M. Kawaguchi² Y. Doi³ T. Takahashi⁴

(総合情報センター¹, 情報グループ², 農学部会計係³, 医学部情報ネットワーク管理室⁴)

1. まえがき

現行「香川大学ネットワークシステム」(以下 NS)は平成最後(その次の世代への架け橋)でもあり、ここで少し回想することも許されると考え、現在から過去を振り返りつつ、「今昔」を述べる。すなわち、二世代前から現行 NS への流れをまとめておきたい(ページ数が2倍となった)。

この十有余年はセキュリティ対策と防災対策の世相を反映した時代であったことを再認識している。MS Blaster の出現から否応なしでセキュリティ対策を、兵庫県南部地震から東日本大震災大津波へと厳しい時代から防災対策を、意識したネットワーク構築の急務となった。高速性や高機能性が「計算環境」とほぼ同様に迫及されていた要求仕様が、徐々に、いやむしろ急激に上記の2つの必須項目重視へと舵をきることになった。

もちろん、分散キャンパスという特徴を持つ本学においては、ネットワーク環境は「ネットワークシステム」と「キャンパス間高速通信」との両輪が相補的に機能することが不可欠であり、今や遠隔会議や遠隔教育が常態化(必要インフラ)とみなされる状況となり、NSの要求仕様の中核であることも事実である。従って、本稿で扱う項目としては、「セキュリティ対策」「防災対策」「キャンパス間高速通信」の流れが現行 NS へとどのように受け継がれてきたか、という今昔物語とも言えるかもしれない。以下ではこれら3つの項目についてこれまでの変遷を俯瞰する。

2. セキュリティ対策とファイアウォール

三世代前になるがコンピュータウイルスという言葉が社会に衝撃を持って認識されたのは、その爆発的に拡大する影響力(悪影響)と他人事ではないという心理状態からであったかもしれない。事実、夏季休業を地元で過ごした学生が新学期でキャンパスに集うと授業より先にウイルス対策を強いられるような事態はまさに前代未聞の珍事となっていた。キャンパス間にもセキュリティ対策

が必要との認識をもたらした(それまで大学の内と外を開閉する番兵的な「ファイアウォール(以下 F/W)」はお飾りではないにしても「一応設置しておくもの」程度の認識であったと記憶している。しかし、コンピュータウイルスの衝撃は、それでは役に立たないことも明確になった。同時に“UTM(Unified Threat Management)”という聞き慣れないキーワードを耳にし始め、1台数百万円以上もする機器を各キャンパスの入り口に配置することでウイルスの不正侵入感知や抑制ができるとの触れ込みで、二世代前の NS 構築の1つの目玉になっていった。

少し話が前後するが20世紀最後の工学部と銘を打って創設された香川大学工学部では学生個人所有ノート PC を1つの特徴としていたので、IP 接続してネットワーク環境を利用するため DHCP サービスが不可避であった。しかし、残念ながらウイルス対策が完全表裏一体とはなっておらず、ある意味、平和な時代だったとも言えた。従って、本格的セキュリティ対策はやはり二世代前の NS から始まったとする認識を持っている。

しかし、今からすれば不思議なことながら、当時は「一度導入すればレンタル期間中は大丈夫」との安心感がセキュリティ対策機器に対しても例外なく適応されていたように思われる。もちろん実情がそれを徐々に許さなくなっていたのは周知の事実である。メールサービスは別、Web サービスは別・・・と次々に追加増資でセキュリティ機器の導入更新を迫られることで、導入時の検討事項をはるかに超える運用時の膨大なケアに忙殺されていったことで、「これがグローバル化の実態か」との感慨を新たにした。

運用規則を如何に効率的に設定し、適切に進捗させるか、は「セキュリティポリシー」が重要であるとの認識が学内外に起こり、しかも時代に即応して動的に変化できること(より正確には単なる「機能増減」ではなく、新規機能を渋滞なくリ

アルタイムに運用中のシステムへ導入できる体制作りを可能とすること)が再認識され、固定的な機能のF/Wの時代から戦略的なF/Wの時代に大きく進化したのが先代(一世代前)からである。その意味では現行NSのF/Wと同一メーカーの製品(Palo Alto Networks)であり、現在世界最高水準のF/W専用メーカーの製品を導入し、運用してきた。これは決して「最高水準なのだから仮に支障があっても我慢して欲しい」等と訴えようとしている訳ではないが、1台数千万円もする機器をDual System構成として採用するとコスト高を招来する象徴とも言える。しかし、NSにはこのような機能が不可欠となっている状況をご理解いただきたいと、心の底で祈念していることも事実である。NSに関する紹介を中心に行っているのでセキュリティ機能の詳細までには言及しないが、現行コンピュータシステムの一部として導入されている「spamメール対策機器」と相補って本学のセキュリティ対策の根幹をなしている事実と実績は大きい。先に述べた二世代前の状況を考えると安易に「未来永劫も」という訳にはいかないような「歴史的教訓」も頭をよぎる。現行NSではどうか持ち応えることを祈念するばかりだが、次世代となると・・・やはり不安も隠し切れない。今後学内外の衆知を結集しセキュリティ対策を講じる必要性・重大性を強く感じている。後にも述べるが、人材育成と適材適所化が今後も本学の課題であり続ける点も強調しておきたい。

3. 防災対策とデータセンター利用

日本が悲惨な震災(含む大津波)に襲われた記憶は色褪せない。多くの犠牲者と共に情報システムおよびそこに蓄積されていた情報そのものの喪失も大きな社会問題となった(なっていると現在形で述べるべきか)。本学における防災対策も前世代から本格的にスタートした。役員会のご理解・了承を取り付け、分散キャンパスの状況をむしろ奇貨居くべしとする対策を講じたのが一世代前である。結果としてキャンパス間通信(高速性)の必要性が増した。

クラウドサービスの普及も追い風となっている。世はまさに総クラウド化でGoogle、AMAZON等が幕開け役を演じたクラウド化の波は情報処

理・情報通信という限られたドメインに収まりきらず今や社会現象化している状況である。遠隔会議やe-Learningと言ったキーワードもその推進役となっている。これに防災対策も相乗りを決めていることは周知に事実である。すなわち、特定キャンパスが被災しても大学全体としては機能してキャンパスが他のキャンパスにおけるサービスを可能な限り代行できる構成とする。そのためには、基幹ネットワークの高速化が不可欠となる。大学が共同利用しているSINETインターネットバックボーンが10ギガ接続サービスを提供しており、本学の現行NSもこれを受けての環境整備という側面を持つ。

一方、二世代前よりも以前から幸町キャンパスは本学における「扇の要」を演じてきたが、高潮被害が懸念されることもあって、低いながら山頂にある医学部キャンパスをもう一方のインターネット窓口とする防災対策を講じてきた。そのような経験を踏まえ、現行NSでは(正確には現行NS導入後に)「扇の要」を近隣のデータセンターに移設することで、より適切な防災対策を実現できるネットワークを構成することとした。しかし、「扇の要」にはF/Wを含む各種サーバを含む本学の言わば「NSの中核」となる機器を移設(システム構築の動的修正)することになり、本学としても一大プロジェクトを組んで対応する必要があった。それでなくても、「ネットワークは正常に稼働して当然」という認識が一般的であり、一夜のうちに墨俣城を構築した木下藤吉郎の如き采配が強く望まれるものとなった。

ここでデータセンター利用のメリットをおさらい(要約)すると、

- ① データセンターの利用法：ハウジング VS ホスティング
- ② 堅牢な構造：地震や災害に強い建物構造
- ③ 情報セキュリティは当然で、物理的セキュリティも重要
- ④ 意外に重要な立地条件：あまり遠いとアクセスが不便!?
- ⑤ 電源設備に加えて回線・通信サービスの充実も必要条件
- ⑥ 決め手は管理体制とマネジメントの信頼性

⑦ (忘れてならない) コストメリット等が挙げられる。本学の場合、「NS 的中枢」機器の移設でも明らかなように①「ハウジング」型であり、②～⑤が最重要判断基準であったことも明確である。コストメリットは総てにかかる事案であるが、光熱水費低減でも実は導入効果があった様子だ。⑤ではインターネットバックボーン接続とキャンパス間接続の両方を兼ねている点でもデータセンター移行の効果(利用効果)があったと言える。

5. 現行 NS の特徴

ここまで複数世代を俯瞰し NS の今昔を述べてきたので、改めて現行 NS の特徴について紹介しておきたい。

(1) **高性能 F/W の継続的導入**：これまでも述べてきたように Palo Alto F/W の特徴は高いセキュリティ性能であるが、キャッチフレーズ等を要約すると、(a)低機能パケットフィルタ型 F/W ではなく高性能ゲートウェイ型 F/W の代表であり、(b)通過するアプリケーションの可視化(識別と個別制御、併せて本学ではサンドボックス機能を利用した高度セキュリティ対策も実施中)を高速実行する専用ハードウェアとして実装され、(c)ユーザ ID (Active Directory 等) と連携可能でセキュリティポリシーの柔軟な実現を可能とし、(d)トータルコストに優れた運用支援を「謳い文句」としている。実際、運用経験からも機器の導入が返って運用コストまで高騰させる事実を苦々しく感じてきたので、現行 NS ではセキュリティレポートを導入業者にも分担してもらい機動性を高めている。

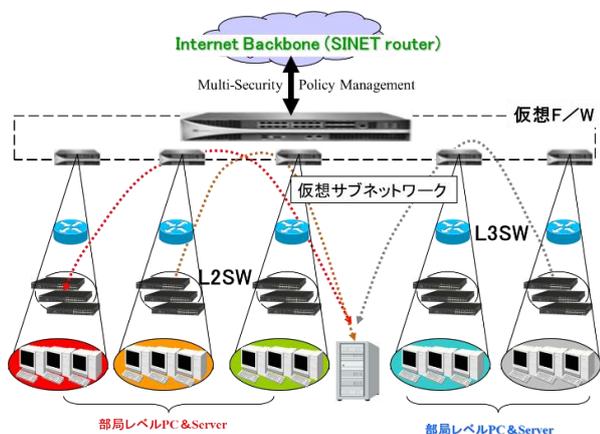


図1 仮想的サブネットワークの構築

図1のように、仮想的サブネットワークを構成することで、柔軟なセキュリティポリシーを容易に実現でき、かつ全体を統合できる。これは以降で述べるデータセンター移行時にも効果を発揮することになる。

(2) **ネットワークの高性能化とデータセンターの活用**：キャンパス間を10G高速回線で、インターネットバックボーンとは10G×2の余裕かつ柔軟性のある回線で接続しており、ネットワーク性能は過去最高レベルとなっている。また、データセンター利用のメリットは前述の通りである。従来NSが幸町キャンパスを中心とするスター型(前述の「扇の要」)のトポロジーを採用していたため、幸町キャンパス被災時の影響が大きいという問題点を、新NSでは中心拠点をデータセンターへ変更し、耐災害性能とコストメリットに優れたデータセンターへComputing & Network機能をシフトし、被災リスク、管理・省エネコストの低減と機能性の向上を図っている点が大きな進化と言える。

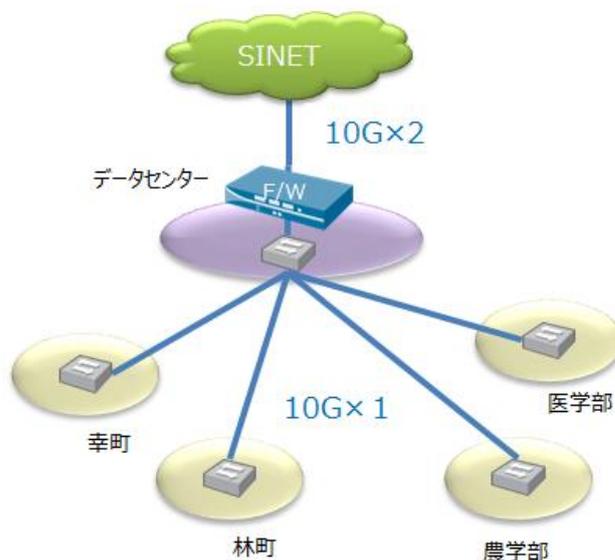


図2 データセンター移設後の現行NS

図2の構成からも見通しの良いネットワーク環境が実現できていることが明確である。

(3) **スマートフォンやPCに代表される持込機器への対応**：従来方式のDHCPではセキュリティ対策の面でも、ユーザ利便性の面でも限界となりつつあった。そこで、より柔軟なユーザ認証と

持込機器認証とを融合した認証システムの導入を図ってきた。情報化の影響から持込みノートPC数の増加、スマートフォン利用者数の急増、無線LAN経由の機器認証作業の煩雑化に対応することが現行NSのもう1つの特徴である。旧システムでは採用されたONGは導入コストと運用コストの問題で採用を見送り、同時に従来はスイッチ認証方式でなかったため、未登録端末でも手動でIPアドレスを設定すると通信可能となっていた。そこで、MAC認証機能を有するスイッチを採用すること未登録端末の接続を排除し、認証機能強化の方針が採用された。

採用されたスイッチ認証方式は図3の赤色機器Account Adapterと呼ばれるスイッチにより、「認証前アクセスリスト」と呼ばれる未認証の端末（図3の不正利用者のPC等）に対して認証前の端末の通信に適用されるアクセスリスト機能が使用できる。認証済みの端末（図3の左の利用者が使用するPC等）は許可する一方で「認証前アクセスリスト」の利用によりMACアドレス登録前の端末が学内ネットワークに接続することをブロックでき、また不正な利用者が未認証のネットワークを利用した不正な通信も抑制可能となっている。

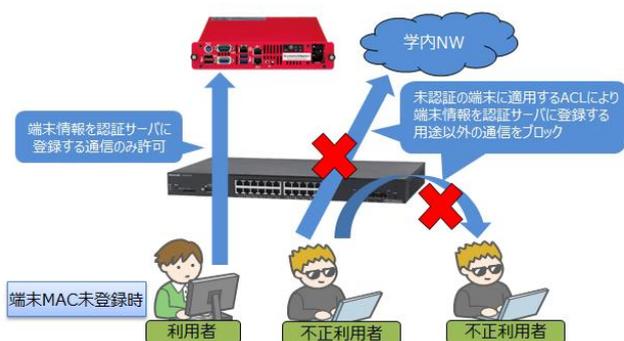


図3 スイッチ認証の有無（済み、未認証）によるネットワーク環境の動的な端末対応

6. ネットワーク利用の可視化

現行NSに切り替わる以前からネットワーク利用状況の可視化を図4のような形式で実施してきた。対象となるのは、①SINETルータ、幸町キャンパス、医学部キャンパス、工学部（林町）キャンパス）および農学部キャンパスに関する所定の1週間の幹線ネットワークの利用状況、と②各キ

ャンパスにおける無線LANの利用状況である。ちなみに、図4の上2つは幹線ネットワークの利用状況（2番目はピーク時1、2時間の詳細利用状況）となっている。一方、図4の下2つは無線LANの利用状況であり、医学部（4番目）のみ測定形式が他と異なっている。

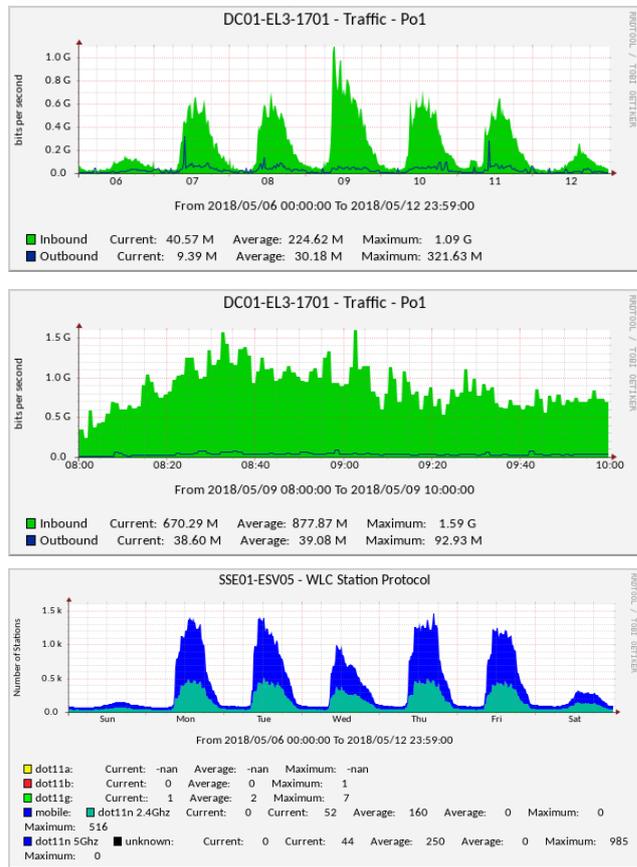


図4 ネットワーク利用の可視化の実例

5. あとがき

現行NSは分散キャンパス（含む附属施設）という本学の現状に即しつつ、可能な限り効率良く管理・運用されている。しかし、課題も少なくない。平成30年度当初、創造工学部1年生のPC認証時に生じた障害によって、機能設計は適正でも運用時の想定外の現象を予測することの難しさを突き付けられた。人材育成という課題もある。引続き、大学全体の理解と学内外の支援を祈念しつつ筆を置くことにする。

情報セキュリティ部門報告

後藤田 中¹ 米谷 雄介¹ 小野 滋己² 青木 有香² 福家 隆² 高橋 岳水³ 川口 政秀² 土居 敬典⁴
山下 俊昭² 末廣 紀史²

N.Gotoda¹ Y.Kometani¹ T.Fuke² T.Takahashi³ M.Kawaguchi² Y.Do⁴ S.Ono² T.Yamashita² N.Suehiro²
Y.Aoki²

(香川大学 総合情報センター/創造工学部¹, 香川大学 学術・地域連携推進室 情報グループ²,
香川大学 医学部情報ネットワーク管理室³, 香川大学 農学部会計係⁴)

1. まえがき

Emdiviによる標的型攻撃[1]は2015年6月にかけて「医療費通知のお知らせ」を中心として、関係者・組織を装い、全国の官公庁・高等教育機関・企業を含め、組織内の端末が感染し、組織内外への攻撃への踏台利用や情報漏洩のインシデントが多数発生した。端末におけるマルウェアによるウイルス感染の脅威について、標的型は特定の個人を攻撃対象としていながら、組織への被害(脅威)が極めて高くなっている[2]。このことから、インシデントに対して、個々の構成員におけるセキュリティ意識向上を含めた資質強化と、被害拡大を抑制するために、迅速かつ的確な初動対応がとれる組織・体制面強化の両面から取り組むことが必要な状況である。

後者の組織・体制面の強化として、2016年4月に情報セキュリティ部門を設置、従来よりも専任に近い形で、教職員スタッフを配置した。また、2017年3月には、部局ごとのセキュリティチームを再編し、横断的な組織対応を意識した香川大学情報セキュリティインシデント対策チーム“KADAI CSIRT”を発足させ、情報セキュリティのガバナンスを強化している。

一方で、本学の医学部附属病院における端末のウイルス感染によるインシデント発生後より、前者の対応として、IPAの教材[3]等に基づき「標的型攻撃メールの見分け方」に特化した講習会を全学の教職員を対象に実施した。一方で、その講習を活かした対応訓練を実施することにより、当事者意識の強化や講習で習得した知識の実践が可能と考え、2016年12月中旬および2017年12月中旬に全学教職員を対象とした標的型攻撃メール訓練も実施した。

本稿では、総合情報センターにおけるCSIRTの構築という枠組みの中で、標的型攻撃メール訓練の設計と実施をその特徴的な取り組みとして報告する。

2. CSIRTの活動

CSIRTはインシデント対応だけでなく、情報セキュリティの啓蒙活動も行っているため、その一部を紹介する。

2.1. 情報漏洩・不審メールへの注意喚起

CSIRT発足は2017年3月であり、発足前の注意喚起メール送信数は月1件ほど、発足後の注意喚起メール送信数は月1.7件ほどで、CSIRT活動の効果が現れているといえる。

2.2. 不審メールの情報提供

CSIRTに情報提供のあった不審メール数について、2017年11月には、楽天やAppleなどの実在企業を騙った不審メールが急増した。2017年12月以降はいったん沈静化し、2018年3月末頃から再び報告数が増える傾向にある。本学構成員の不審メールに対する情報セキュリティ意識が浸透してきていると判断できることから、今後も啓蒙活動を続けていく。

2.3. 情報セキュリティ教育

2017年度も教育活動として情報セキュリティeラーニングを実施した。大学におけるFD(Faculty Development)の一環として行っており、実施期間は、システムリリースによるLMS(香川大学Moodle)の改修のため、年度跨りの2018年3月26日～5月11日であった。

eラーニングは香川大学Moodleを活用し、情報セキュリティ対策の自己点検シートと一般的な情報セキュリティの知識を問うクイズ形式とした。教材は、既存の教材[4-9]を基に大学教職員にとって有用と思われる内容を抽出し、大学組織の特徴に合わせ本学内部で修正したオリジナル教材である。Moodleの機能である多肢選択式問題と自動採点機能を利用し、回答に対して判断の正誤および詳細な解説が提示されるようにしたことにより、学習としても機能するようにし、正答率が80%を超えることを修了条件とした。なお、後述する標的型攻撃メール訓練の結果を受けて香川大学の正規WebサイトURLと不審なURLリンクを見分ける設問を必須問題とした。受講率は、全学で60%ほどと昨年度の45%ほどから、受講者が増えた。

3. 標的型攻撃メール訓練

3.1. 本訓練の目的

標的型攻撃メールの大学への潜在的脅威の認識及び、大学教職員の情報セキュリティ意識の向上、情報セキュリティインシデントが発生した場合に、報告・連絡、被害拡大防止等、迅速かつ的確な初動対応を取れるように訓練を実施した。標的型攻撃メール訓練に関する主な目的は以下の通りとした。

(1) 標的型攻撃メール訓練対象者(以下：訓練対象者)が、標的型攻撃メールを受信した際には、不審な URL の開封を行わなくなる。

(2) 対象者が標的型攻撃メールを開封し、ウイルス感染の可能性が疑われる場合には、本学で定められた手順に従い、部局のシステム管理者・責任者等に速やかに連絡・相談を行うようになる。

(3) 標的型攻撃メールは、特定の個人を対象とする事例も多いが、複数人への攻撃（特に対象アカウントがメーリングリストであった場合の複数人受信）の可能性もあり、標的型攻撃と疑われるメールを受信した場合には、部局内の関係者に情報共有を行い、また、必要に応じて(2)の手順と同様に対応関係者へ連絡・相談を行うようになる。

訓練を繰り返すことにより上記の効果を期待し、これらを見据えた情報セキュリティ意識調査項目を設計し、実践後、教職員に対してアンケートを実施した。

3.2. 本訓練の体制

本学の教育組織は6学部（教育，経済，法，工，医，農）7研究科（教育，経済，法，工，医，農，地域マネジメント）体制で構成されており、これらに加えて法人本部および各種の機構、センター、室により支えられている。学内部局によっては、独自に情報環境（メールサーバ等）を立ち上げている。こうした背景から本学では、情報セキュリティポリシー（対策基準）は大学全体での共通基準とし、各部局の状況を反映した部局ごとの実施手順を整備する体制を取っている。各部局にはシステム管理責任者が存在し、通常のインシデント対応手順は各構成員から CSIRT に集約することとなっているが、今回の訓練結果の調査に関しては情報システム管理責任者に依頼し、部局ごとに集約した内容を CSIRT に連絡する方法を採用している。

上記の本学の現状を考慮し、手順を以下の7つのステップで構成した。

(1) 各部局内の連絡体制の確認と部局内の実施手順書確認連絡を実施

セキュリティ対応関係者へ、部局内で整備されている連絡体制の確認と訓練を含むインシデント発生時に、迅

速な対応が可能なるようセキュリティ対応関係者間の連絡手順について確認するよう連絡を行った。

(2) 各部局の情報セキュリティ実施手順書の確認と周知の実施

訓練に先立ち、対象者へ、セキュリティ対応関係者への連絡先やインシデント発生時の対応手順の確認を行うよう通知した。

(3) 標的型攻撃メールの訓練実施予告メールの送信

対象者へ、訓練を予告に定める期間内（5日間）において実施することを周知した。

(4) 標的型攻撃メールの訓練実施

対象者に対して、訓練メールの配信を行った。メールは、学内に訓練用のサーバを設置しそこから配信した。

(5) 報告・連絡・被害拡大防止等実施の確認

(2)の手段により、対象者からの開封に関する連絡・相談、また情報共有について、報告を受け付けた。なお、その状況を訓練後に取りまとめられるよう、事前にセキュリティ関係者へ記録の依頼を行った。

(6) 標的型攻撃メールの訓練実施終了メールの送信

訓練の終了を通達すると同時に(4)におけるメールの内容を公開した。

(7) 訓練の解説及びアンケートの実施

訓練用メールの解説を学内専用サイトに掲載し、メールにて対象者に案内を行った。解説サイトのページ最下部にアンケートへのリンクを設け、対象者に回答してもらった。

3.3. 訓練メールの内容

2017年度では、題材として、「人事部局による年末調整」を利用した。より具体的には、2017年11月頃の実在企業等を騙ったメールの増加、および他大学のメールアドレス詐称事例を参考にした。「人事部局による年末調整のお知らせ」は実施時期(12月)に応じた内容であり、普段から高い情報セキュリティを持っているかどうかを評価することをねらいとした。主要な内容は以下のとおりである：

- ・メール題名：【重要】年末調整の確認について
- ・送信者：香川大学の人事関連部局
- ・アドレス：人事関連部局を騙った存在しない学内アドレス (kagawa-u.ac.jp)
- ・添付ファイル：なし
- ・外部リンク：詳細を確認できるようにした。本リンク先で本メールが訓練メールであることの種明かしを行った。リンク先が学外の不審なアドレス、マウスオーバーで確認することができるようにした。

3.4. 採用した訓練メールシステム

学内で別途メールサーバを立て、そこから送るようにした。2017年11月の実在する企業を騙ったメールの増加を鑑みて、攻撃メールの実態に沿った形で、メール本文に記述する形にした。メール本文表記と実URLが異なる偽装したURLリンクを用意し、この実URLは送信先に対してユニークに紐づいており、このURLをクリックすると、開封者が特定されるWebビーコン型で情報を収集した。

3.5. 訓練の実施結果

訓練対象者は、本学の教職員とし、教務職員、事務職員、技術職員、看護師等の附属病院等における医療系職員であった。対象者の総数は、2017年度は2,388名であった。

表1に標的型攻撃メール訓練の結果を示す。2016年度の結果では、低い値となっていたのは、総合情報センター一名で送信されることを含めて、添付されたPDFに記載のURLクリックを開封としたことから、世間一般のものと比較して標的型攻撃メールと気づかれやすいものだったと部門として判断した。そこで2017年度は真に訓練に繋がることを狙いに、より判別が難しいテーマを選択した。その結果として、表1に示すとおり、メール開封率は上昇したが、標的型攻撃メール訓練としては教職員へ有効な課題を提供できたと考えている。

表1 標的型攻撃メール訓練の結果

年度	受信者数	開封者数	受信報告数	開封報告数	開封率	受信報告率	開封報告率
2016	2179	241	452	65	11.1%	20.7%	27.0%
2017	2388	767	533	306	32.1%	22.3%	39.9%

表1の組織全体の開封報告率をみると、2016年度は実際に開封を行った対象者のうち、報告があったのは、27.0%にとどまったが、2017年度はこれが39.9%まで大幅に改善した。開封者の母数が増えたこともあるが、啓蒙活動の成果ととらえたい。

4. 事後のアンケート調査について

4.1. 調査の趣旨および各年度の目的

開封率や報告率については、訓練結果の集計によって定量的に観測可能である。一方で、明らかになった数値的指標の改善に向けた方略を検討するために、個人の意識、または、それに寄らない組織的な課題、訓練自体の課題等を調査するために、訓練対象者から訓練実施後に2016年度に続きアンケート調査を実施した。

2017年度は昨年度の結果を受けて訓練題材の改善を行った。

4.2. 調査方法

訓練が終了した後、アンケートを対象者全員に対して、通知を行い実施した。アンケートは、CSIRTのWebサイトで標的型攻撃メール訓練の解説を掲載し、その最後にGoogle Formを用いたアンケートへのリンクを掲載し、Webブラウザから回答を行ってもらった。

4.3. 調査項目

課題を探るために、調査項目を事前に検討した。代表的な項目としては、以下があげられる。

- ・標的型攻撃メールが届いたことを認識していたか
- ・標的型攻撃メールをどのように見抜いているか
- ・部局内で情報共有したか
- ・報告を行わなかった理由は何か

4.4. 調査結果

アンケートは、訓練対象となった教職員全員2388名に対して、回答数は384件で回答率は16.1%であった。先に示したとおり、本学メールアドレスを実施時期に即した内容のメールを題材としたことから開封率が上昇したとみられるが、一部回答者は、メール本文の内容で訓練メールであると判断されていた。2016年度の報告率と同程度の結果のため、報告していない理由を見ると、訓練であるためや、開封していないためなどを理由として報告をしていないケースが目立った。開封の有無に関わらず不審メールを受け取ったことを報告することが、訓練の目的の一つであることを周知してきたが、受信報告率が示すとおり、さらなる訓練の趣旨や報告体制の浸透が課題であると考えている。

情報共有をしなかった理由は、URLリンクをクリックしてページを開いたことに対して罪悪感をもち、周囲に話せなかったという意見が得られた。インシデントの予防としては、このような意識を払拭することが重要であり、根本的な組織文化をより開いたものへと変えていく施策が必要であると当部門としては考えている。そのための方策としてCSIRTがより構成員にとって相談しやすい存在になることが重要であると考えている。

5. おわりに

標的型攻撃メール訓練は、本学の情報セキュリティ対策基本計画の実施項目にも掲げており、2018年度以降も実施予定である。訓練実施後のアンケート結果から、連絡体制がわかりにくいといった意見は2年連続で多く、窓口を一本化することに対するニーズがあることがわかった。これを実現するためには、各学内部局の実施手順を変更する改定が必要であり、学内ヒアリングによってさらなる課題や改善に向けた対応の検討を行う予定である。

る。

以上、CSIRT 活動報告及び 2016 年度、2017 年度と継続して実施した標的型攻撃メール訓練の概略報告をもって当部門の年次報告とした。

6. 参考文献

[1] マクニカネットワークス株式会社, “標的型攻撃の実態と対策アプローチ,” https://www.macnica.net/file/security_report_20160613.pdf

[2] 独立行政法人情報処理推進機構 (IPA), “情報セキュリティ 10 大脅威 2016 ～個人と組織で異なる脅威, 立場ごとに適切な対応を～,” <https://www.ipa.go.jp/files/000051691.pdf>

[3] 独立行政法人情報処理推進機構 (IPA), “標的型攻撃メールの例と見分け方”, <https://www.ipa.go.jp/files/000043331.pdf>

[4] IPA, “ここからセキュリティ! :セキュリティチェック,” <http://www.ipa.go.jp/security/kokokara/quiz/>

[5] 内閣官房情報セキュリティセンター, “情報セキュリティ自己診断チェックリスト,” http://www.nisc.go.jp/security-site/files/checklist_20120417_02.pdf

[6] TREND MICRO, “is702 : クイズで判定あなたのセキュリティレベルは?,” https://www.is702.jp/special/1314/partner/12_t/

[7] MOTEX, “セキュリティ 7 つの習慣・20 の事例,” http://www.motex.co.jp/vision/enlightenment_activity/education_book/

[8] 日本ネットワークセキュリティ協会, “知っておきたい情報セキュリティ理解度セルフチェック,” <https://slb.jnsa.org/slbm/>

[9] JPCERT コーディネーションセンター, “新入社員等研修向け情報セキュリティマニュアル,” <https://www.jpccert.or.jp/magazine/security/newcomer.html>

ユーザーサービス部門活動報告

米谷 雄介¹, 最所 圭三¹, 後藤田 中¹, 近藤 まゆみ², 小野 滋己², 山下 俊昭²,
 Y.Kometani¹, K.Saisho¹, N.Gotoda³, M.Kondo², S.Ono², T.Yamashita²,
 豊嶋 尚子³, 末光 京子², 青木 有香², 香西 理恵³, 七條 強²
 N.Toyoshima³, K.Suemitsu², Y.Aoki², R.Kozai³, T.Shichijyo²

(香川大学総合情報センター/創造工学部¹, 香川大学 学術・地域連携推進室 情報グループ²,
 香川大学総合情報センター³)

1. まえがき

ユーザーサービス部門の業務は、図 1 に示すように、サービスの基盤の維持管理とユーザーへの対応である。サービス基盤の維持管理として、統合認証 ID や認証連携サービスの提供、それに付随するトラブル対応や PC ルームに関する業務があり、ユーザーへの対応として、ホームページ刊行物を通じての情報提供や FD 等のイベント企画、ヘルプデスクや問合せ内容の分析など、ユーザーに対するサービス提供状況の把握およびユーザー管理に関することを扱っている。現在の構成員は、教員 3 名、事務職員 8 名である。本報告では、PC ルーム運用、FD・SD 企画/イベント協力およびヘルプデスクに持ち込まれた相談の分析結果を紹介する。それらに加え、ヘルプデスクの分析に基づいた今後の運営方針を示す。

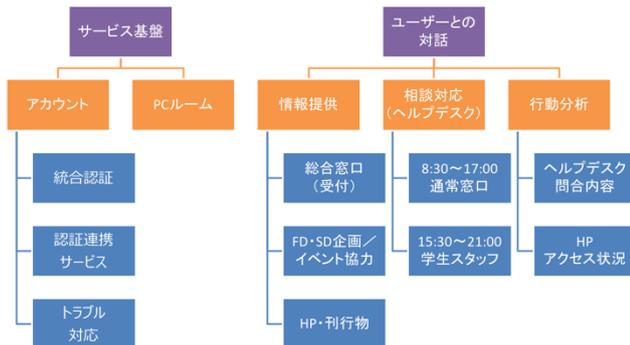


図1 ユーザーサービス部門の主な業務内容

2. PC ルームの効率的運用

授業改革や新学部の設定に伴い、少人数参加型授業への関心が高まる一方で、効率性、すなわち大規模一斉授業へのニーズもまた高くなっている。そこで

PC ルームも効率的な運用の実現のため、PC ルーム統合やスペースの活用について検討した。図2、図3に移設前の座席配置を示す。図4に移設後の座席配置を示す。移設の結果、59名の教室収容人員を確保し、情報リテラシー等のPC ルームを利用した一斉授業のニーズに対応した。また教室名については、「コンピュータルーム」と呼ばれていた箇所を「PC ルーム」に統一し、より実態に合った名称付けを行った。



図2 図書館コンピュータルームA(移設前)

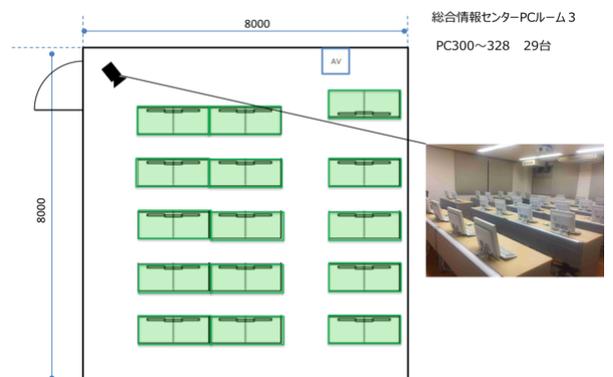


図3 総合情報センターPCルーム3(移設前)

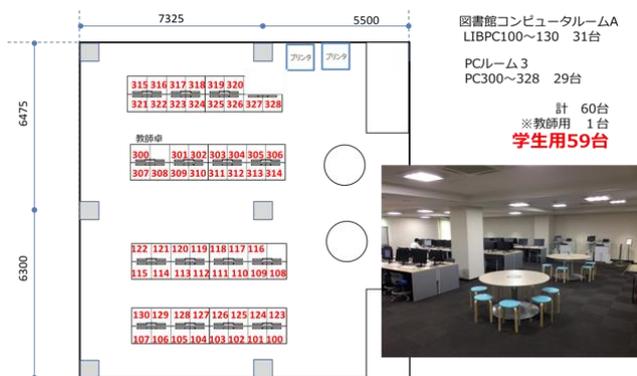


図4 図書館 PC ルーム L1 (移設後)

3. 国立大学法人等情報化連絡協議会への協力

FD・SD 企画／イベント協力の一環として総合情報センターユーザーサービス部門として協力した事例である。

国立大学法人等情報化連絡協議会は、大学の情報化に向けた取り組みに関する研究発表会(国立大学法人等情報化発表会)を毎年、全国の大学持ち回りで開催している。本発表会を通じて、情報共有・情報交換を図ることにより、より一層の情報化推進に資することをねらいとしている。図5に本発表会のポスターを示す。平成29年度は10月23日から10月24日まで、香川大学講堂で開催した。



図5 国立大学法人等情報化発表会のポスター

情報セキュリティに関する取り組み、業務・システムの最適化に関する事例、管理運営の業務改善、および事業継続計画・危機管理体制の整備事例など多岐に渡る事例について、2日間で計14の研究が発表され、熱心な質疑応答が行われた。全国から127の機関(国立大学法人、研究所、高専)から2日間を通じて約140名の参加があった。

4. ヘルプデスク相談分析

図6に、過去4年間の相談内容ごとの相談件数の推移を示す。図6から分かるように、教育用PCに関する問い合わせは、年々減少傾向にある。持ち込みPCについては増加する傾向にあったが、本カテゴリに対してスマートフォンに関連する質問が増えてきていたため、2018年度からは記録カテゴリの見直しを行うこととしている。

2017年度は、無線LAN／プリンタの質問が多くあった。メールについての質問は2016年度から増えているが、これは情報リテラシーの授業でGmailの利用者教育を行っていることと関係していると思われる。

本学の Learning Management System として利用されている Moodle や、統合認証 ID に関する問合せが増えているのは、Moodle での授業が増えていることが関係していると思われる。Moodle については本センターだけでなく、本学の学務グループや修学支援グループも関係が強いため、学生に対して正確にアナウンスを行うためには、部局間連携が大切であると考えられる。

少数例ではあるが、学外の講師等から、授業のためPCルームの使い方に関する質問が例年発生していることもわかった。そこで教員の事前の授業計画がスムーズになるようにハードウェアの使い方等をわかりやすく伝えるビデオマニュアル等の整備を検討することとした。

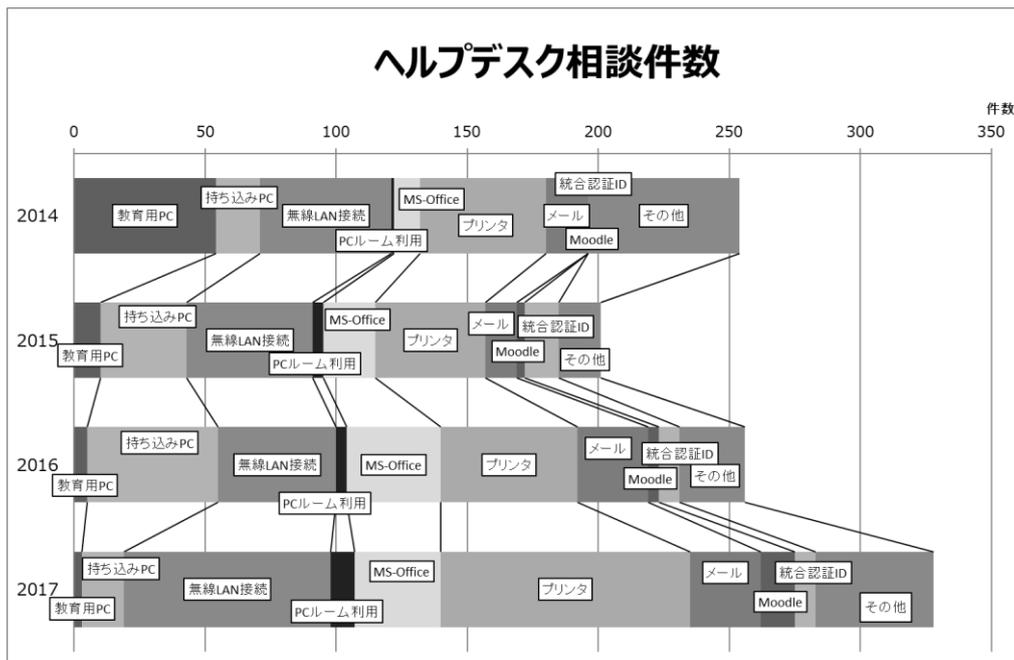


図6 ヘルプデスクに対する内容別相談件数の年次推移

コンピュータシステムリプレイス前は、無線 LAN のアクセススポットに繋いだ後の操作がわからない、携帯を買い換えたので無線 LAN に繋がらなくなったという無線の接続方法や、プリンタの紙詰まり、持込 PC からの印刷方法、印刷場所などの相談が多く寄せられた。コンピュータシステムリプレイス後は、システムリプレイス後の Mac アドレス登録システムのログイン後の登録方法や手順通りに登録を行っても登録できない事例や、OSによって必要手順が増えるなどの事例も発生し、本センターの教育システム部門やネットワーク部門等と連携して解決にあたった。

Moodle に関する問合せの増加と同時に、統合認証ログインによらない部局独自の e-learning システムに関する問い合わせの増加も観測されている。Moodle とその他の e-learning システムとを区別していない学生も少なくなく、トラブル対応の際に学生がたらい回しに遭うことを避けるため、管理が部局間にまたがるものは対応フローを整備するなど、トラブル解決のための情報整理を行う予定である。また、来年度は、ナレッジ化を進め、チャットボットによる対応の一部自動化を検討している。

5. あとがき

平成 30 年度から米谷教員が部門長として就任する。部門員として、総合情報センター長の最所教員、情報セキュリティ部門部門長の後藤田教員に加え、事務職員の新メンバーも加わる。部門員一致協力して、上記の業務に加え、ホームページのユーザビリティ向上やユーザーへの情報セキュリティサポートの強化を推進していく。

医学部キャンパス報告

高橋 岳水¹ 川田 延枝¹ 多田 志乃舞¹
T. Takahashi¹ N. Kawada¹ S. Tada¹
(香川大学医学部 情報ネットワーク管理室)

1. はじめに

情報ネットワーク管理室では医学部キャンパスに於ける情報セキュリティ対応と医学部キャンパスネットワークの整備などを担当している。

平成 29 年度の活動について報告する。

2. 総合情報センターネットワークシステム更新

平成 29 年度の総合情報センターネットワークシステム更新において、医学部キャンパスでは機器の更新と共に下記の改善を実施した。

2. 1 附属病院の災害時優先通信の設定

香川大学はBCP対策としてマルチホームネットワークを従来から構築しており、通常回線のSINETが何らかで利用できなくなると医学部からのバックアップ回線に切り替わる構成が取られている。しかし、バックアップ回線は通常回線より帯域の制約があるため、災害時に附属病院で必要な通信が確保できるか課題となっていた。

今回の更新ではバックアップ回線のファイアウォールが通常回線と同一機能となり帯域優先設定が可能となったため、附属病院の以下の通信について設定した。

1) 防災機関との通信、2) 国立大学病院医療情報遠隔バックアップシステムへのアクセス、3) 附属病院内の災害時優先端末からの通信

本改善により附属病院の災害時における優先通信を準備することができた。

2. 2 医学部事務ネットワークの構成変更

医学部設備部門が入る中央機械室はネットワークが基礎臨床研究棟から管理棟を経由していたため、建屋ごとに行われる電気設備点検の計画停電ではネットワークが停止する問題があった。

今回のシステム更新では中央機械室が各建屋の計画停電の影響を受けないよう経路の変更を実施した。また、中央機械室やBCP対策のバックア

ップ回線などの重要回線の一部についてはUPS+自家発電源とし停電時でもネットワークが継続利用できるように改善を図った。

3. 附属病院再開対応のネットワーク整備

医学部附属病院は、再開事業に平成 23 年度から着手しており、事業の進捗に合わせて附属病院内の学内ネットワーク整備を進めている。

3. 1 附属病院内のアクセススイッチ更新

附属病院で現在稼働しているアクセススイッチは平成 19 年度の導入で老朽化によるトラブルが課題となっている。このため、再開工事に合わせ、平成 27 年度から 4 年計画で更新を順次進めている。

平成 29 年度は東西病棟、外来診療棟、放射線関連棟で更新を進め、台数ベースで全体計画の約 84% の進捗率となった。最終年度となる平成 30 年度は外来診療棟、放射線関連棟などの更新を引き続き進める予定である。(表 1)

表 1 附属病院内のアクセススイッチ更新計画

	平成27年度	平成28年度	平成29年度	平成30年度
東西病棟				
中央診療棟				
外来診療棟				
管理棟				
放射線関連棟				

3. 2 学生自習室移転対応の無線LAN整備

再開対応で学生自習室の一部が移転したため無線LAN環境の整備を実施した。移転先は学部ネットワークが未整備のため、既設光ケーブルを中継し合わせて計 5 か所にアクセスポイントを配備した。

4. おわりに

本報告では、総合情報センターネットワークシステム更新と医学部附属病院再開対応のネットワーク整備について述べた。附属病院再開対応は計画の最終年度に入っており、今後の運用に備えドキュメント類の整備も進める計画である。

