

活動報告

香川大学の情報戦略 ～平成 30 年度活動報告～

林 敏浩¹ 近藤まゆみ² 小野滋己² 末廣紀史²
T.Hayashi¹ M.Kondo² S.Ono² 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 教育部などの学内の他組織と連携した業務にも対応する。本稿では、平成 30 年度の情報戦略部門の活動を、第 3 期中期目標・中期計画に基づく平成 30 年度実績の総括などを中心に概説する。

2. 情報化推進計画の策定

総合情報センター(当時は総合情報基盤センター)では、2005 年 9 月に「香川大学情報化推進基本構想 2005-情報化推進組織の整備について」

として、以下の項目について策定した。

- ① 情報化推進の目的
- ② 香川大学における情報化の現状と課題
- ③ 情報化推進体制の構造
- ④ 情報化推進の組織
- ⑤ 情報化推進の展望

上記の情報化推進基本構想総括を踏まえて 2020 年を目途に「香川大学 ICT ビジョン」の策定するため、以下の項目について検討を行った。

- ① 各大学の個別戦略
- ② 香川大学の個別課題
- ③ 中期目標に対する措置

3. 全学のシステム導入に係る助言・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

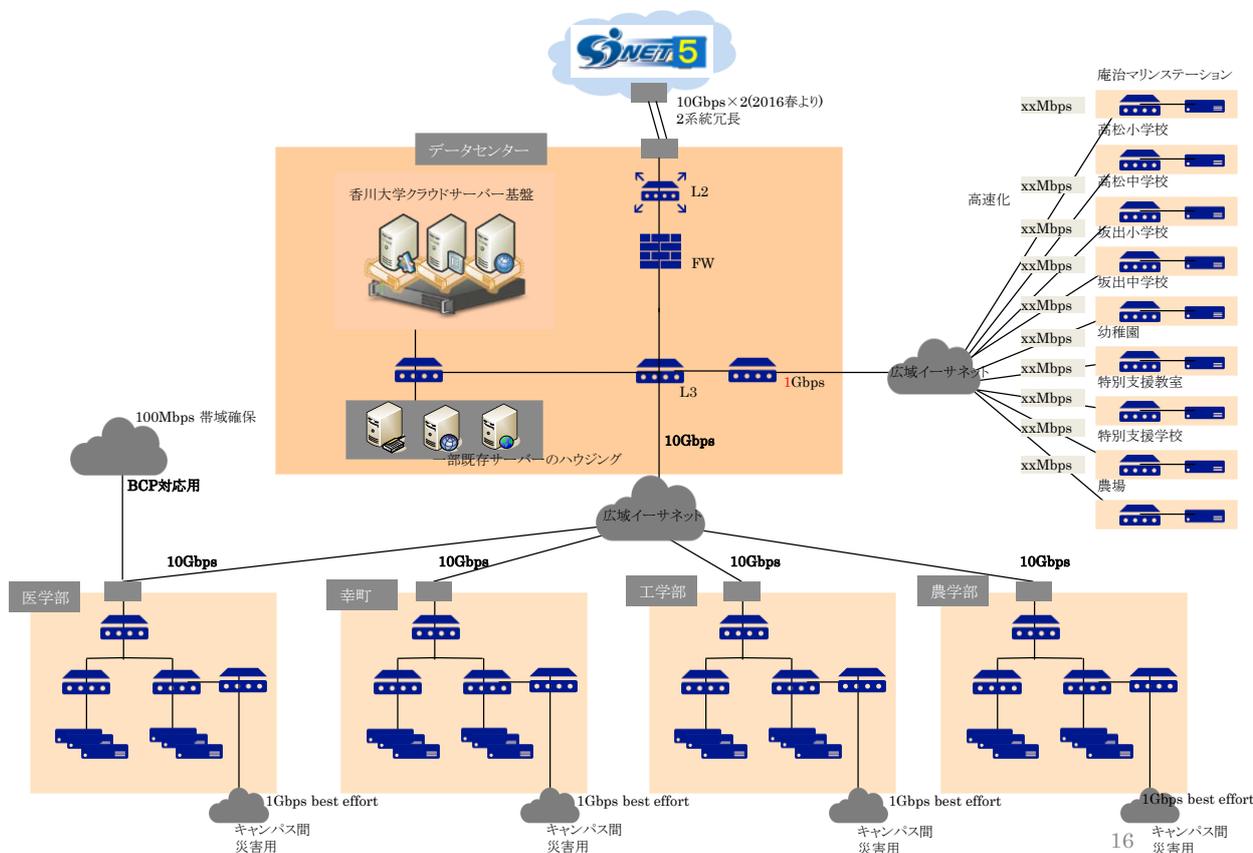


図 1 外部ネットワークの冗長化

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 30 年度は、学務系・総務系併せて 10 件のシステム新規案件の支援・調整を実施した。

4. 第 3 期中期目標・中期計画に基づく平成 30 年度実績の総括

- ① e ラーニングを利用した情報セキュリティ教育の実施として、セキュリティ教育前後のアンケートで、情報セキュリティ理解向上度の割合を 8 割以上にするようにした。
- ② 外部からの攻撃によるネットワーク停止を防ぐため、高度かつ詳細な設定可能な FW 機能を整備した。具体的には、標的型メール攻撃のリンク先ブロック、外部からの通知に基づく通信遮断を行うため、URL ブロック機能で、危険なサイトのブロック・カテゴリー別サイトのブロックの対応・対策を実施した。
- ③ セキュリティ装置の高度化のため、FW 装置にサンドボックス機能を付加し、未知のウイルスにも対応可能とした。
- ④ セキュリティ装置の冗長性を確保するため、FW 装置・DNS 装置を二重化した。
- ⑤ 外部ネットワーク回線の冗長化するため、外部接続ネットワーク回線を二重化した。図 1 は香川大学の外部ネットワーク回線の冗長化の現状を示している。
- ⑥ クラウドサービス利用時の情報管理の実施：クラウド利用ガイドラインにより、情報重要度に応じた、データ管理方法・クラウドサービス業者選定を実施した。
- ⑦ クラウドコンピューティング利用時の情報セキュリティ対策の確保として以下を実施した。
 - I. プライベートクラウド・データの暗号化とパスワード保護・災害対策・信頼性
 - II. ネットワーク・ストレージ・データ管理・ログ・バックアップ・準拠法の考慮
- ⑧ サイバー攻撃の早期発見態勢の強化及び学内セキュリティ連絡体制の徹底のため、以下のことを実施した。
 - I. ファイアウォールのログ監視体制を強化し、サイバー攻撃を早期発見

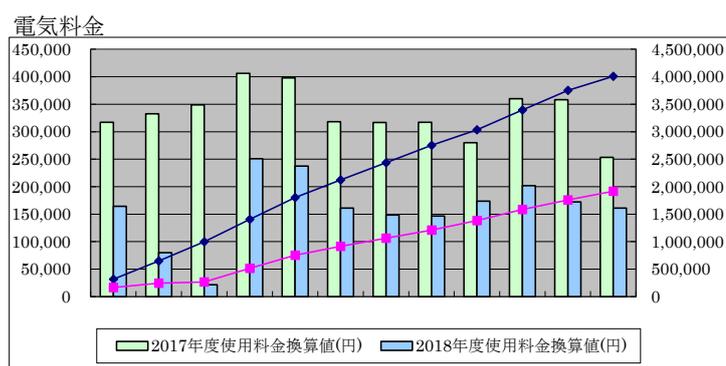
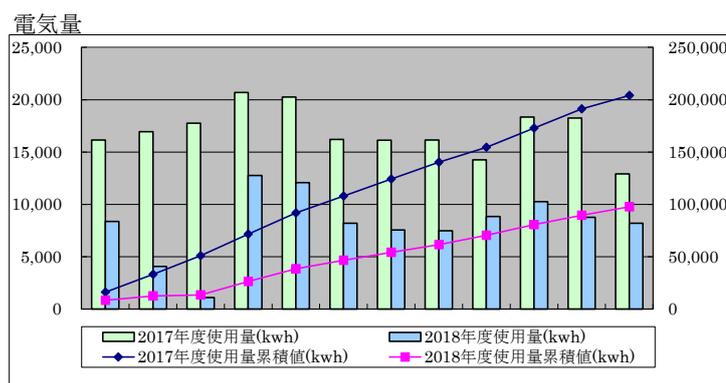


図 2 2017 年度・2018 年度の電気量・電気料金の比較
(参考:香川大学環境管理室エネルギー使用量検針システム)

II. セキュリティ連絡体制に基づき速やかに学内に連絡・対策

- ⑨ セキュリティ監査の強化のため、セキュリティ監査の頻度を上げた
- ⑩ 情報セキュリティ内部対策ソフトの導入として、未知のウイルスに感染した場合、内部での振る舞から検知可能なシステムを導入した。

5. 総合情報センターの管理資源の効率的利用

図 2 に示すようにデータセンターへサーバ移設後、サーバ室を縮小し有効利用することにより、電気代の節減を実現した。

6. まとめ

本稿では、平成 30 年度の総合情報センター情報戦略部門の活動を、情報化推進計画の策定、全学のシステム導入に係る助言・支援・調整、第 3 期中期目標・中期計画に基づく平成 30 年度実績の総括、総合情報センターの管理資源の効率的利用の観点から概説した。今後も、情報戦略部門として多様かつ柔軟な業務遂行が要求される場合が多いと考える。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。

教育デザイン部門報告

藤本 憲市, 岡本 裕之, 豊嶋 尚子, 安土 正枝, 川瀬 舞, 中川 えんじゅ, 樽見 拓樹, 七條 強
K. Fujimoto, H. Okamoto, N. Toyoshima, M. Azuchi, M. Kawase, E. Nakagawa, H. Tarumi, T. Shichijo
(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) や学内の e-Learning 教育を支援する学内組織の一つである。本稿では、平成 30 年度活動実績等について概説する。

2. 平成 30 年度活動実績

平成 30 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 名である。技術補佐員のうち 2 名は、大学連携教育支援センター四国 (修学支援グループ所属) からの応援である。

平成 30 年度は、昨年度末に発生した授業配信システムにおける不具合の解消を図ったとともに、e-Learning 科目のコンテンツ制作支援、授業運用支援、及び Moodle 利用実績の分析支援等を行った。

2.1. 授業配信システムにおける問題解決

これまで、大学連携 Moodle、香川大学 Moodle、動画配信システム、及びユーザ認証システムは、本学がオンプレミスで構築していたが、e-Learning 科目運用に係る情報セキュリティ対策及び BCP 対策の一環として、両 Moodle と動画配信システム、学内者用のユーザ認証システムをクラウド化した。図 1, 2 に構築した大学連携 Moodle と香川大学 Moodle に関するそれぞれのシステムのアウトラインを示す。なお、このクラウド化は実際には平成 29 年度に実施していたが、知プラ e 科目の講義映像コンテンツを配置するパブリッククラウド (Microsoft Azure) からの配信不具合が平成 29 年度末に確認されたため、平成 30 年度にその解決を図った。

これらシステムの更新に伴い、Moodle のバージョンも 3.1 から 3.5 (導入当時の最新版) へアップグレードされたため、Moodle のインターフェースが大幅に変更されることを余儀無くされた。そのため、大学連携 Moodle、香川大学 Moodle とともに、マニュアルを刷新した。

平成 30 年度は、図 1 に示した大学連携 Moodle (ただし、動画ファイルは、図 2 に示すオンプレミスのストリーミングサーバ 2 台から配信) を用いて計 21 の知プラ e 科目のコンテンツを配信したが、大きなトラブルなく運用することができた。

一方、香川大学 Moodle については、教職員に自動的に付与されるはずのコース登録者権限が付与されないケースが続出するという不具合が発生したが、個別対応することにより事なきを得た。なお、この問題が生じた原因の特定しているところである。

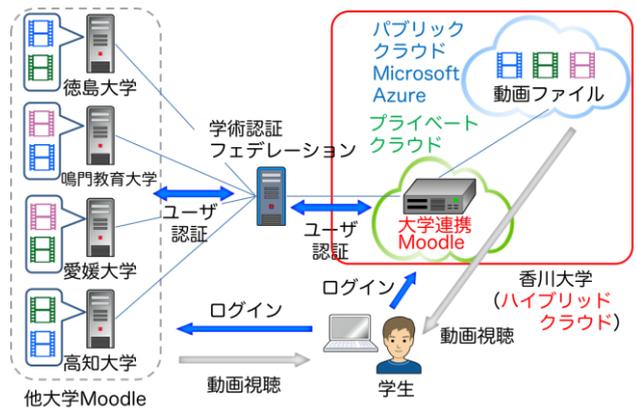


図 1 構築した大学連携 Moodle 関連システム

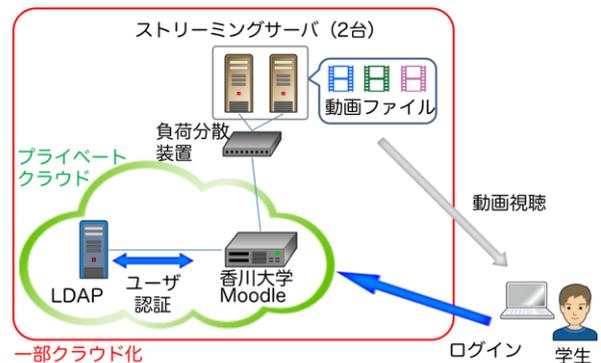


図 2 構築した香川大学 Moodle 関連システム

2.2. コンテンツの制作支援

平成 30 年度は、令和元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) の更新用コンテンツの制作支援を行った。これ

まで、講義映像の収録は講義室や e-Learning スタジオ等の屋内で行ってきたが、野外での空撮の需要もあったことから、大学連携 e-Learning 教育支援センター四国からドローンを借り受け、ドローン操縦士養成準備にも着手した。

現在開講している知プラ e 科目の主要コンテンツは動画であるが、他大学からの要請もあり、コンテンツのバリアフリー化を検討した。具体的には、映像を使用しないタイプの電子ブック型コンテンツを今後推進すること、字幕付き講義映像コンテンツを制作するために Microsoft Azure などの自動字幕生成機能を利用すること、などを検討した。検討の結果、前者については今後推進することになったが、後者の自動字幕生成機能については、音声から文字への変換精度が講義映像に使用できるレベルに達していないという結論に達し、今後の動向を注視していくこととなった。

その他、動画コンテンツ更新作業の省力化のため、音声合成ソフトウェアの利用を検討した。その音声合成ソフトウェアは、パワーポイント (PPT) とスピーチ原稿 (テキストデータ) さえあれば、そのスピーチ原稿を音声に変換しながら動画コンテンツを自動生成してくれるものである。平成 30 年度後期開講の知プラ e 科目に部分的に導入し、問題なく運用できることを確認した。



図 3 Microsoft Azure Media Indexer による字幕生成

2.3. Moodle アクセス数の分析

今後 e-Learning 科目が増加した場合に、サーバ負荷やネットワークトラフィック量の観点から必要となる対策を検討するため、大学連携 Moodle へのアクセス数を調査した。図 4 において、横軸が日付、縦軸がアクセス数、青色データが平成 30 年 1 月、オレンジ色が平成 31 年 1 月のデータをそれぞれ示している。両年度のデータともに、概ね 3~4 個のピークがみられ、これらピークの日付が課題

締切日とほぼ同期していたことが分かった。

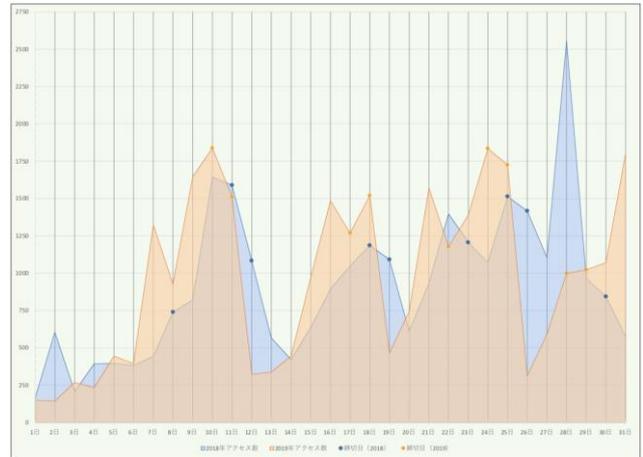


図 4 大学連携 Moodle へのアクセス数

3. 令和元年度における検討課題

システム面では、より利便性の高い e-Learning システムの構築を目指して、Moodle の機能強化のためのプラグインを調査したいと考えている。また、現在配信中の大学連携 Moodle マニュアル及び香川大学 Moodle マニュアルの動画バージョンを作成する予定である。

e-Learning 科目のコンテンツに関しては、動画コンテンツのバリアフリー化の推進及び動画コンテンツ制作作業の省力化について引き続き検討していく予定である。また、オンデマンド型 e-Learning 授業における第三者著作物の利便性向上が期待される改正著作権法第 35 条に関わる動向 (例えば、一般社団法人授業目的公衆送信補償金等管理協会 (SARTRAS) への補償金額の設定や本学の支払い可否など) についても注視していく必要がある。

その他、e-Learning 授業の改善に資するデータ提示を目的として、Moodle から得られる学習データを分析し、その分析データを有効活用するための方策についても検討したいと考えている。

4. あとがき

本稿では、平成 30 年度における教育デザイン部門の活動と今後の検討課題について概説した。令和元年度も引き続き、知プラ e 科目や香川大学 Moodle 上 e-Learning 科目が問題なく運用されるよう、可能な限り支援していきたいと考えている。

教育システム部門活動報告

～2020 クラウドメールへ～

八重樫 理人¹, 末廣 紀史², 近藤 まゆみ², 岸本 江未², 川口 政秀²,
R.Yaegashi¹, N.Suehiro², M.Kondo², E.Kishimoto², M.Kawaguchi²
南堀 公子², 香西 理恵³, 高橋 岳水⁴, 土居 敬典⁵
K.Minamihori², 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(兼任)、職員8名で構成されている。

本学では教育用途のメール・ファイル共有・印刷・ソフトウェア等のサービスや、535台のノートブック端末、基幹となる仮想サーバ約100台などを包括して教育システムと称している。

2017年度に6年ぶりのシステムリプレースを完了し、2018年3月より新基盤での稼働を開始している。それらのリプレースコンセプトの報告と、今後予定をしている業務メールのクラウド移行についての学内FDを2019年7月5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 外的要因

(1)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。

(2)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御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。

(3)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。

(4)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。

2.2 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. 教職員メールのクラウド化

3.1 対象とスケジュール

本学では学生メールについては2012年よりクラウド化が完了しているが、教職員については学内設置型のメールシステムを利用していた。

基盤のシステムを更新した際、ID連携システムの設計やセキュリティ機器の選定にもクラウドメール化を見越して構築を進めており、移行に向けた素地は完成していた。

約1年の新基盤運用を経て、安定稼働が確認できたことから、クラウドメール化を進めることとなった。

対象は医学部を除いた本学の教職員とし、2020年春からの新メールアドレス配布、2020年夏からは旧メールアドレスによる送信を停止し、2020年冬での旧メールサーバ切り離しを計画している。

3.2 メリット

一般利用者、メール管理者、全学運営それぞれの視点でメリット・デメリットが考えられる。本学では下記の要点にて情報共有を行い、同意形成を進めている。

(1).ユーザーの操作性向上

①WEBブラウザ、スマホ/タブレットアプリ等、新たなメール参照環境を提供でき、場所を問わず同一の環境でメール送受信ができる。一方、既に使用しているメーラーでも設定変更のみで引き続き使用することもできる。(図1)

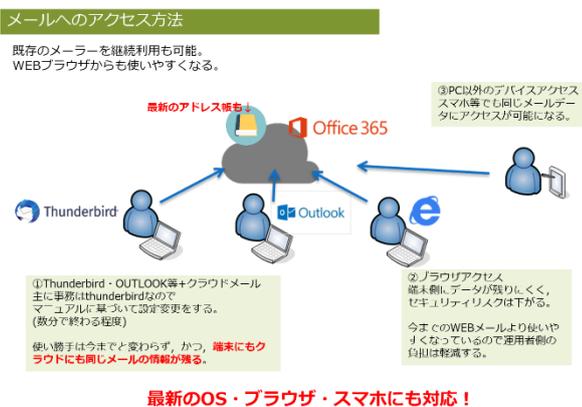


図1 複数デバイス 利用イメージ

②最新のブラウザ、OS,スマホ環境にも対応できる。

③従来に比べてメールボックス容量の心配がなく、IMAP 接続でメール参照が可能となる。

④従来は部局管理者がおこなっていたメーリングリスト作成申請、共有メールアカウント作成申請機能を一般ユーザーが利用できる(追加実装計画中)。

(2).管理者の負担軽減

本学では合計8部局それぞれでメールサーバの管理をしている。サブドメイン毎に仮想サーバが設置され、メールアカウント管理やユーザー対応も含めて部局管理者が行っている。(図2)部局管理者の担っている負荷も下記の点で改善することができる。

管理者の負担軽減

現在はメールアカウントの発行・停止や、パスワードを各部局ごと個別に作成している



- ・各部局の担当者がアカウント管理をする負担がある
- ・セキュリティインシデントが発生した際に、担当者に連絡がとれず緊急の対応ができないケースがある
- ・システムトラブルなどで対応を求められることがある。
- ・利用者も「メールと統合認証のパスワードは別」という分かりにくい状態。

図2 部局別管理 イメージ

①全学 ID 管理システムと自動連携をし、部局管理者が個別にメール用のアカウント・パスワード発行をする必要がなく、負担を削減することができる。

②緊急時の対応を情報センターにて実施することができる(セキュリティインシデント対応は、各部局においても遂行する必要はある)。

③仮想サーバ自体の維持管理工数を削減することができる。

④メンテナンス等で停止する業務影響がない(SLAで99.9%稼働等が保証されている)ため、利用者対応や動作確認などの負担も軽減される。

(3).セキュリティ強化

本学でもメールアカウントの乗っ取り、標的型攻撃、誤送信等々、メールサービスに関するセキュリティインシデントが発生しており、利用者の意識啓発と合わせてシステムの強化は急務である。

(図 3)



図 3 攻撃にさらされるサーバ

- ①全学の ID 管理システムと連携し、類推されやすい名前、脆弱なパスワードのアカウントを制限できる。アカウントを乗っ取られるリスクを軽減できる。
- ②全学の ID 管理システムと連携し、不要なメールアカウントが残留するリスクを軽減できる。
- ③学内にメールサーバを保持しないので、OS・ソフトウェアの脆弱性を突く攻撃リスクを回避できる。
- ④メール送受信に関する統一したポリシーを適用することができる。
- ⑤常に最新バージョンのサービスを利用することができる。
- ⑥多要素認証、誤送信防止など周辺の対策製品の選択肢が増え、導入が検討しやすい。

3.3 利用者への影響

メリットも多いが、ほぼ全ての構成員が利用するシステムなので変更の際しての影響範囲も非常に大きいものとなる。

(1).新メールアドレスへの移行

クラウドメール化に合わせて、ID システムとの連携を簡素化する目的や、将来的な組織変更・組織間の異動にも対応しやすいようワンドメイン化を検討している。そのため、新たなメールアドレスを発行し、その利用を促していく。

当然、ユーザーは従来のメールアドレスを他機

関に登録していることもある。そのため、旧メールアドレス宛を新メールアドレスへ転送することもユーザーに支障が無いように継続していく必要がある。

(2).メーラーの設定変更

Thunderbird, Outlook といったメーラーで送受信をするユーザーも多いことから、クラウドメールアカウントの追加を行う手順を共有する必要がある。

ただし本学では業務端末での SSO 環境は整備されていないので、メールアカウントの追加だけの手順となり、数分で完了する軽微なものを想定している。

(3).新たなメール活用へのリテラシー教育

WEB ブラウザやスマホ/タブレットでの利用、HTML 形式でのメール送受信、承認を経てのメール送信や、一斉送信時の制限ルールなど、従来のメールシステムに無い使い方や、機能を提供できるようになる。それらの周知のための検証や、マニュアル作成、研修会など、利用者への対応も継続していく必要がある。

4. おわりに

新しいシステムにリプレースし、従来のサービスを安定して提供していくことのみならず、新たなサービスを検討し、提供していく活動も重要である。2018 年度は基盤のリプレースが完了し、2019 年からはサービスの見直しを実施していく期間であると位置づけている。

他大学ではメールシステムの見直しとともに、「メールに依存している業務形態の見直し」を振り返っていることも聞く。メールに代わる新しいコミュニケーションツールの導入をすることも有益かもしれないし、もっと他者に理解されやすいように自分の業務内容を整理することも有益であるかもしれない。

利用者の理解を得ながら、大学全体として有益なサービスの提供を関係部署と共にこれからも検討していきたい。

香川大学ネットワークシステムの部門報告（平成30年度）

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.Do³ 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

「香川大学ネットワークシステム」(以下NS)は令和の年代へ移行した。そこで、平成最後の1年間を概観し、今後への備えとしたい。まず、NSの現状を簡単に図説し、現状のNSの特徴であるネットワークの形状や各部の通信速度について述べる。また、ネットワークの利用状況を可視化するため、基幹ネットワークおよびNSの支線部分を構成する無線LANの利用状況の可視化結果についても紹介する。

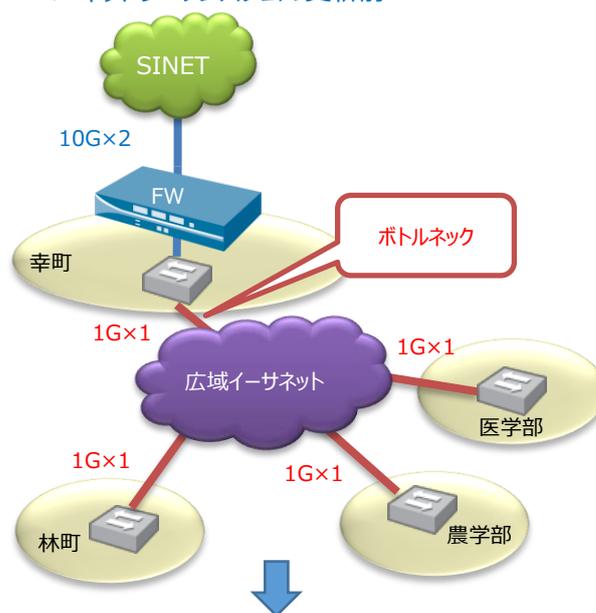
2. ネットワークシステムの改善

NSの大きな変化は図1のような「位相幾何学」的変更と通信速度的変更が実施されることで実現された。図でも明らかなように4カ所の分散キャンパス上でのインターネットへの出入口が、伝統的に幸町キャンパスに設置されてきた。しかし、医学部、工学部(創造工学部:林町キャンパス)および農学部ではこの状況は決してフェアでもなく、また大学全体の負荷分散という観点からも望まない状況でも無かった。また、SINET(インターネットバックボーン)の高速化に対し「ファイアウォール(以下F/W)までは10G×2の通信速度を準備しても幸町キャンパス以外にはそのメリットが及ばないという状況を打破する策も必要であった。そこで、NSとしては極めて大きな改善策となるものの、通信速度改善に見合う各キャンパスを均等に扱う方式を検討する=データセンターへのキャンパス間の扇の要の収納、という「位相幾何学」的変更(ネットワーク・トポロジーの改善)という言わば最後の手段を講じることになった。

これはコスト問題を事由にあげて逡巡してきた従来方式からすればまさに「コペルニクス的転回」と呼べる(禁断、しかし最強の)一手であった。これを可能にしたのは「データセンターへの移行」という全国的な情報センターの動向に加え、敢えて大ナタを振るおうと覚悟した総合情報

センター長、情報グループリーダーをはじめとするスタッフおよび関係各位の高い意識とその覚悟の賜物(業者の支援も)であったと喜んでいる。

▼ ネットワークシステムの更新前



▼ ネットワークシステムのデータセンターへの移行後

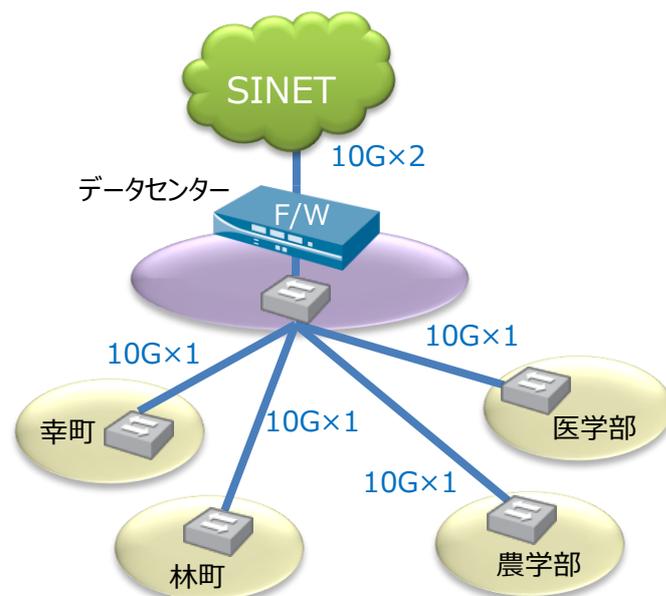


図1 ネットワークの改善(劇的 Before After)

3. ネットワーク利用の可視化

利用状況を可視化することで、いくつかのメリットが生じる。一番大きな側面は、比較の容易さであり、先月と今月の差異を容易に発見でき、問題点を比較的簡単に発見できる点であろう。図2を参照して欲しい。

基幹ネットワークを構成する5地点での利用状況の可視化を行っている。図1に示す新しいNSの特徴点（接続ポイント）と見比べてもらうと、

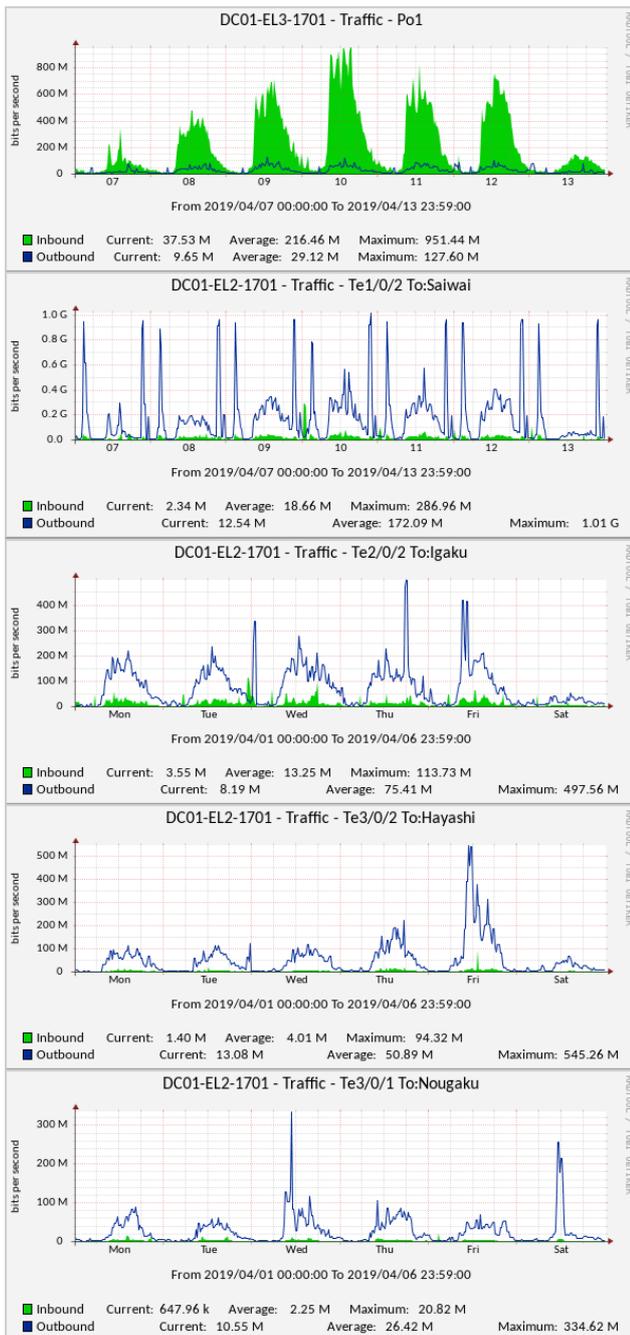
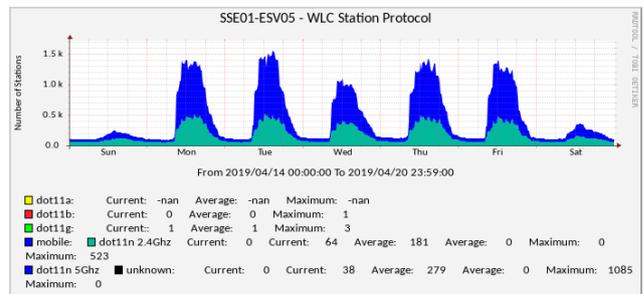


図2 「5地点での基幹ネットワークの利用状況」

上から順に、インターネットバックボーン SINET との接続点、幸町キャンパスとの接続点、以下同様に、医学部、創造工学部、農学部のそれぞれの接続点の packets 流量、すなわち NS の利用状況を可視化して表示している。各キャンパスの特徴も出ているが、計測時刻の特徴も反映しており、一週間の周期性も明確に読み取れる。一年間を通じて利用状況を可視化したデータを解析すれば、月ごとの利用状況の違いも読み取れるので、繁忙期と閑散期も容易に把握できる。

次は、無線 LAN の利用状況について述べる。図3を参照いただくと、無線 LAN の利用状況を把握できるので、ここでも可視化の効果が読み取れる。



順位	無線AP名	設置場所	平均アソシエート数	最大アソシエート数
1	SSF02-EWL01	南6号館2F 第三講義室	34	111
2	NSL02-EWL04	図書館3F 閲覧室	28	74
3	NSL02-EWL07	図書館2F ラーニングcommons	26	79
4	NSK01-EWL03	大学会館1F 食堂	25	130
5	NSC02-EWL03	北3号館2F 323講義室	23	130
6	NSK01-EWL06	大学会館2F 廊下	22	101
7	NSF01-EWL02	北6号館1F 611講義室	20	98
8	NSC01-EWL04	北3号館1F 314講義室	18	104
9	NSD01-EWL06	北4号館1F 415講義室	18	70
10	NSK01-EWL05	大学会館2F カフェ	17	99

図3 無線 LAN の利用状況（グラフ化と実績表示）

図3の下部はアクセスポイントの利用実績を表示しているが、Top10 という形で各キャンパスのどの位置（無線 LAN のエリア）がより多くの利用者を得ているかも示せるため、機器の代替えなどの作業における優先順位などを検討して、よりユーザー側の利便性に配慮したりプレース計画なども運用できる。

4. あとがき

ネットワークシステムはまさに縁の下の力持ち的役割である。可視化の結果、少しでも利用者の理解が得られ、システム管理者の業務がより正當に認識されることを、平成から令和に移っても期待している。

情報セキュリティ部門報告

～ 情報セキュリティ対策基本計画における訓練の統括 ～

後藤田 中¹ 喜田 弘司¹ 米谷 雄介¹ 小野 滋己² 青木 有香² 福家 隆² 山下 俊昭² 高橋 岳水³

川口 政秀² 土居 敬典⁴ 末廣 紀史²

N.Gotoda¹ K.Kida¹ Y.Kometani¹ S.Ono² Y.Aoki² T.Fuke² T.Yamashita² T.Takahashi³

M.Kawaguchi² Y.Do⁴ N.Suehiro²

(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

政府のサイバーセキュリティ戦略を統括する内閣サイバーセキュリティセンター (NISC) は2018年7月25日に3ヵ年計画を公表し、日本の重要インフラ保護と並び、新たに、「大学等における安全・安心な教育・研究環境の確保」が追加された。国立大学2016年における、ある不正送金マルウェアの感染率は国立大が4割と突出している等、一般企業と比較し、国立大学が標的にされている事実が明らかになっている[1]。本学では、Emdiviによる標的型攻撃[2]以降、2016年度に策定した3ヵ年の情報セキュリティ対策基本計画（以下：基本計画）に基づき、情報セキュリティ対策を強化してきた。2018年度はその最終年度にあたる。これまで、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、迅速かつ確かな初動対応がとれる組織・体制面強化の両面から取り組んできた。

まず、後者の組織・体制面の強化として、基本計画1年度目は、2016年4月に当部門(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することからスタートした。2年度目の2017年には、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”の発足に基づき、情報セキュリティのガバナンスを強化した。また、3年度目を迎え、組織を越えた学外間で、各CSIRTの専門スタッフが、情報セキュリティに関する情報交換を行う「学術系CSIRT情報交流会」へ2018年10月に正式に加入し、同じ学術組織連携に基づくアンテナからの情報収集能力を強化した。

また、前者に対応する個人の情報セキュリティ対応の資質強化として、1年度目は、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。2年度目は、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、それぞ

れ、2016年12月中旬、2017年12月中旬に継続実施した。基本計画最終年度も2018年11月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、基本計画に基づき、総合情報センターにおけるCSIRTの構築・運用という枠組みの中で、3ヵ年にわたる標的型攻撃メール訓練の実施成果を報告する。

2. KDAI 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、また、収集した情報セキュリティのログ情報に基づき、セキュリティ製品の選定に関わる妥当性の検証も行っているため、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た。徐々にKADAI CSIRTの認識が高まり、2018年においては、インシデントの相談・通報窓口としてのメールアドレスだけでなく、個人に届く不審メールの通報窓口への通報件数が飛躍的に増加することとなった。

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、Amazon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加傾向に転じた。2018年度においては、報告のある不審メールを含み、本学のメールサーバに届く、半数以上がブロックされている状況となっている。構成員からの報告については、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と同時に、こうしたブロック割合の状況等の構成員が普段知ることのできない情報も理解促進のため、共有していく。

なお、昨年の訓練実施後のアンケート結果から、連絡

体制（CSIRT への一次通報先含む）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った。また、CSIRT としても、緊急性の高い一次対応と通報を切り分ける必要があった。

そこで、スパムを含む不審メールの学内通報窓口を設置し、学内の情報セキュリティ FD 等を通じて、その都度、窓口としてのメールアドレスの周知を行っている。なお、インシデント発生における、CSIRT への通報については、実施手順書に反映できていない部局もあり、順次改訂がすすめられた。その他、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。

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、システムプレイスによる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。2018年度は、2019年2月4日～3月4日に実施した。

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ている。受講率は、2016年度の45%ほどからスタートし、2017年度は、全学で約60%、2018年度で、約55%であった。なお、受講期間は、4月や10月などの入職者の教育機会に即時的に対応するため、2019年の4月以降は、Moodle で、ほぼ年間を通じて公開することを決定した。

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、創造工、医、農)7研究科(教育、経済、法、創造工、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、2017年度からは、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、2016年から2018年度を通じて、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、迅速な対応が可能と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

訓練の終了を通知すると同時に(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

2018年度では、題材として、「ストレスチェック」を利用した。昨年の続き、学内の部局の手続きを彷彿させる内容とした。主要な内容は以下のとおりである：

- ・メール題名：ストレスチェックの訂正について
- ・送信者：給与福利グループ
- ・アドレス：給与福利グループを騙った学内アドレス(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

2017年度に続き、2018年度においても、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。実在する組織を騙る攻撃メールの実態に沿った形で、メール本文に外部へのリンクを記述する形にした。大学のドメインと異なる偽装したURLリンクを用意し、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、2018年度は2,507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。2018年度は、2017年度に続き、学内の部局を装う形で実施したが、開封率は、低下した。

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%
2018	2507	345	713	170	13.8%	28.4%	49.3%

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。さらに2018年度は、49.3%と約半数から報告が得られる形となった。

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の検討が必要である。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2017年度、2018年度も同様のアンケート調査を実施した。

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

2018年度のアンケートは、訓練対象となった教職員全員2507名に対して、回答数は342件(2017年度:384件)で回答率は13.6%(2017年度:16.1%)であった。先に示したとおり、2017年度は、本学で実施している題材としたことから開封率が上昇したとみられるが、2018年度は低下に転じ、一定の割合で、組織を騙る点の可能性を考慮できていたものとみられる。なお、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、インシデントの報告先として「香川大学CSIRT」が加えられ点についても問い、その結果、8割弱が、CSIRTを聞いたことがあると回答していたことから、報告先の一元化が報告率を向上させた可能性もある。開封率は、ヒューマンエラーの抑止の限界から不可避の可能性もあり、今後は、報告に重点をおいた訓練への転換を検討している。

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(2016~2018年度)の実施項目の一つではあるが、本計画の実施を統括する上で、構成員の資質の変化を捉える上で、重要な指標が示されている。特に報告率の大幅な向上は、インシデントの未然の抑止、インシデント発生時の迅速な初期消火につながる可能性がある。本報告で述べている標的型訓練の詳細については、2017年度までに実施された内容を、2018年度の学術誌に投稿・採録されており、別途参照いただきたい[10]。以上、情報セキュリティ対策基本計画(3カ年)における標的型訓練の統括について、当部門の年次報告とした。

6. 参考文献

[1] 日経BP社，“世界から脅威が迫る「間接攻撃」に備えよ”，日経コンピュータ，2018年9月27日。

[2] 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(参照日：2017年10月01日)

[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>(参照日：2017年10月01日)

[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/>，(閲覧日：2017年7月4日)

[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 (閲覧日：2017年7月4日)

[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/ (閲覧日：2017年7月4日)

[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/ (閲覧日：2017年7月4日)

[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/>，(閲覧日：2017年7月4日)

[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.jpCERT.or.jp/magazine/security/newcomer.html> (閲覧日：2017年7月4日)

[10] 米谷 雄介，後藤田 中，小野 滋己，青木 有香，宮崎 凌大，八重樫 理人，藤本 憲市，林 敏浩，今井 慈郎，最所 圭三，“香川大学での標的型攻撃メール訓練の導入と改善点の検討”，学術情報処理研究，No.22，pp.54-63，2018年

ユーザーサービス部門活動報告

米谷 雄介^{1,2}, 最所 圭三^{1,2}, 後藤田 中^{1,2}, 近藤 まゆみ³, 小野 滋己³, 山下 俊昭³,
Y.Kometani¹, K.Saisho¹, N.Gotoda³, M.Kondo², S.Ono², T.Yamashita²,
豊嶋 尚子¹, 岸本 江未³, 青木 有香³, 香西 理恵¹, 南堀 公子³
N.Toyoshima³, E.Kishimoto², Y.Aoki², R.Kozai³, K.Minamihori²

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

1. ユーザーサービス部門について

香川大学総合情報センターのサービスは、(1)香川大学の情報基盤（「コンピュータ&ネットワーク」）、(2)情報基盤において動作するソフトウェア、システム（「ソフトウェア&システム」）、(3)ユーザーが香川大学の情報基盤、ソフトウェア、システムを効果的に活用できるよう支援する「利用者支援」の3つに大別される。ユーザーサービス部門は「利用者支援」の提供を主な仕事としている。

図1に業務範囲を示す。サービス利用環境の整備、ユーザーに向けた情報メディアの整備、ユーザーに対するトラブル解決支援、教職員のICT活用支援、行動分析に基づくサービス評価・改善などの「利用者支援」が中心となっている。これらに加えて、統合認証アカウントの管理や認証連携の管理を行っている。2019年7月5日現在、教員3名、事務職員8名が本業務範囲を担当している。

図1の業務範囲、周辺(他部局、地域、他部門)からの要請、ユーザーサービス部門のもつ業務遂行能力の制約等に基づき、ユーザーサービス部門の活動内容を規定している。表1に活動内容を示す。活動の種類は以下の2種類に大別される：

- (1) 定型的な活動: 総合情報センターガイダンス開催、総合情報センター活動報告会開催、年報作成、パンフレット作成、統合認証アカウント管理等
- (2) 非定型的活動: ユーザーニーズ、バンダーサポートの変化、「コンピュータ&ネットワーク」「ソフトウェア&システム」の更新等に応じたサービス利用環境整備、情報メディア整備、トラブル解決支援、教職員ICT活用支援

本報告では、ユーザーサービス部門の2018年度の活動を概観するとともに2019年度の活動計画を示す。

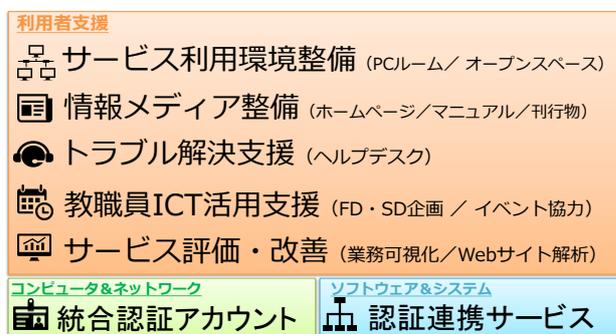


図1 ユーザーサービス部門の業務範囲

表1 ユーザーサービス部門の活動内容

内容	期日※
入学式（学部・大学院・夜間主）において総合情報センターガイダンスを実施する。	1 Q
総合情報センター活動報告会を実施する。	2 Q
FD・SDを企画・実施する。	年間
総合情報センターマニュアルを作成する。	年間
ヘルプデスクによる対応を実施する。	年間
総合情報センターホームページにより、広報活動を行う。	年間
年報を作成し、広報活動を行う。	2 Q
統合認証システムで、採用教職員・入学生のアカウント追加、退職教職員・卒業生・退学生のアカウント削除を実施する。	年間
新入生用パンフレットを作成する。	4 Q
外部組織主催のイベントへの協力	年間

1 Q: 4~6月、2 Q: 7~9月、3 Q: 10~12月、4 Q: 1~3月

2. 2018年度活動報告

定型的な活動は、表1の計画どおりに実施されたので割愛する。本章では、2018年度の非定型的活動のうち、特筆すべき活動を紹介する。また業務可視化／Webサイト解析の結果に基づき、サービスの利用状況を示す。

2.1. 2018 年度の特筆すべき活動

2018 年度の特筆すべき活動を以下に示す。

2.1.1. 学生オープンスペース 1 の改修計画

サービス利用環境の整備として、ヘルプデスクが配置されている学生オープンスペース 1 の改修案を検討した。図 2 に 2017 年度の部屋配置図を示す。2017 年度の総合情報センターシステムリプレイスによって、コンピュータ室に配置されていたサーバ・ネットワーク機器がデータセンターに移行した。空いたスペースを活用するため、セミナー室 1 を移動させ、学生オープンスペース 1 を広げる計画を議論した。

図 3 に議論のたたき台となった改修案の一つを示す。ユーザーの作業スペースを拡張するとともに、ユーザーとの距離が縮まることでよりトラブル解決相談のしやすい環境を提供できると期待される。本計画は 2019 年度末の実行を予定しており、2019 年度も継続審議され、什器の種類や壁の撤去等、より利用しやすさを高める案を策定していく。

2.1.2. Windows10 アップグレードマニュアル

2020 年 1 月 14 日における Windows7 のサポート切れに備えて、本学の事務端末を中心として Windows10 へのアップグレードが急務となった。情報メディア整備の一環として、Windows10 へのスムーズな移行をサポートするため Windows10 のアップグレードマニュアルを整備し、2018 年度の末にマニュアルを公開した。

2.1.3. Excel 講習会の実施

教職員 ICT 活用支援の一環として、Excel の有効な使い方を大学の構成員が学べる講習会を企画・運用した。日時は、2018 年 9 月 4 日 13:00～16:00、場所は総合情報センター 1 階 PC ルーム C1 に行われた。本センターの加入している富士通ファミリー会（富士通株式会社提供）の講師派遣を利用し、Excel の関数、表、グラフ、データベース、ピボットテーブルの利用方法について講習を行った。受講者は 17 名、総合情報センター側からサポート 6 名が参加した。

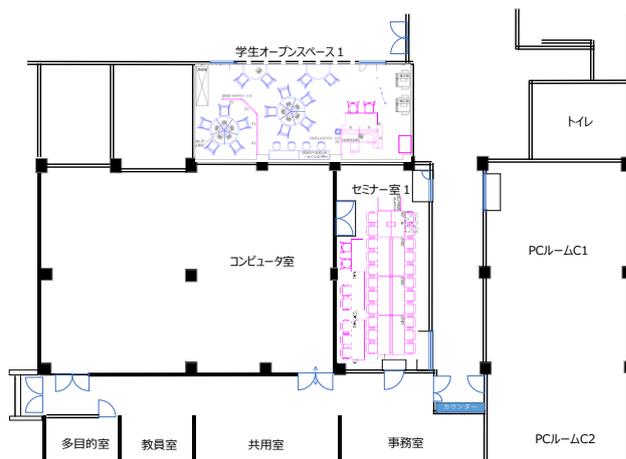


図 2 2017 年度時点の部屋配置

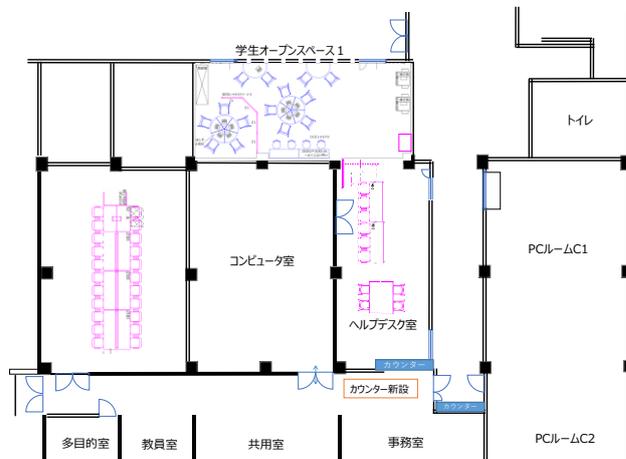


図 3 オープンスペース改修案の一つ

2.2. 2018 年度のサービス利用状況

業務可視化／Web サイト解析の結果に基づき、サービスの利用状況を示す。図 4 に 2018 年度のヘルプデスクの問合せ状況を示す。ヘルプデスクに対する問合せはその内容に応じて、「無線 LAN」「MS-Office」「ウイルス対策ソフト」「プリンタ」「メール」「Moodle」「統合認証 ID」「その他」に分類して記録している。図 4 によると、新入生が増える 4 月に問合せが多いことがわかる。問合せの上位を占めるのは「無線 LAN」「プリンタ」「メール」である。

図 5 に、2018 年度のユーザーからの問合せ件数と 2019 年度の問合せ件数の比較を示す。本報告執筆時点で得られている、問合せ件数の多い、4・5 月分（2 ヶ月分の累計）を比較している。問合せ件数の多かった「無線 LAN」「プリンタ」「メール」に関して減少が

見られた。これは、本部門による情報メディア整備や、教育システム部門、ネットワークシステム部門などの他部門におけるシステム改修の効果によるものであると推察される。特に無線 LAN については、当センターで導入している認証サービスのユーザインタフェースの改修があり、iOS 機器 (iPhone, iPad 等) を介したサービスの利便性が向上したことが、問い合わせ減少につながった。

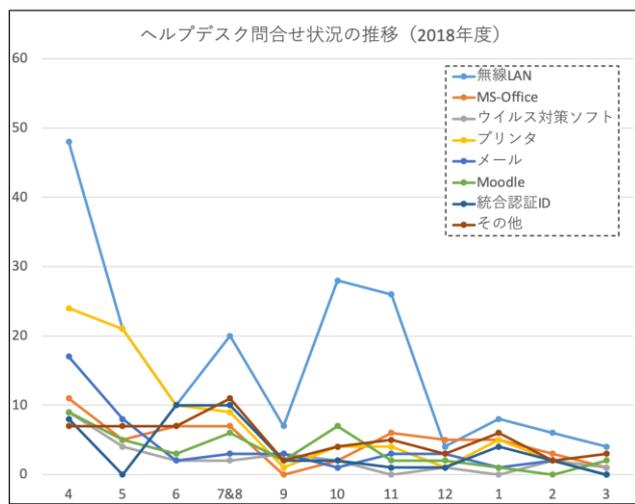


図 4 2018 年度のヘルプデスク問合せ状況

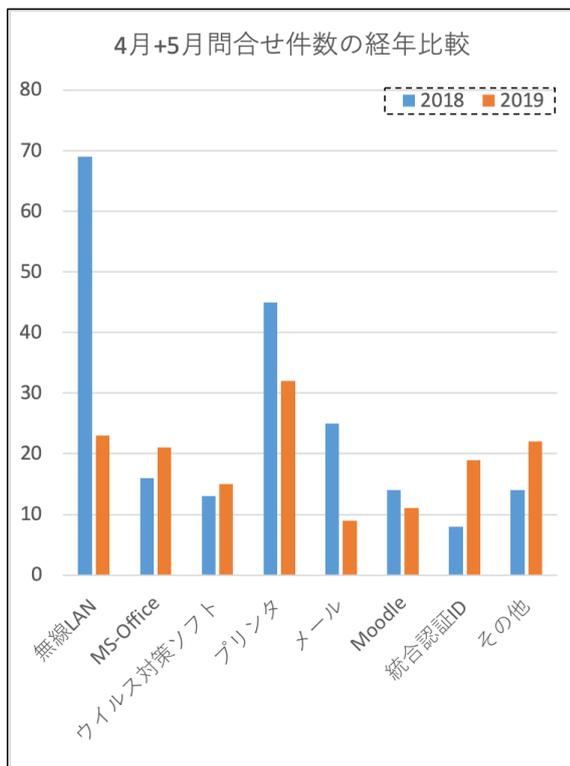


図 5 4 月・5 月の問合せ件数の比較

表 2 に Google Analytics を用いた Web サイト解析の結果を示す。2017 年度と 2018 年度との間でアクセスランキングを比較した。上位 10 位以内に含まれる Web ページの組み合わせにはほとんど違いが見られないが、各 Web ページにおけるアクセス数は 2018 年度においては大きく伸びていることがわかる。情報サービスの利用者数増加が主な要因であると推察される。

本学の Learning Management System (LMS) の一つである香川大学 Moodle は、大学教育基盤センターの所管するシステムであり、総合情報センターはシステムを稼働させるための情報基盤を提供するという形で連携している。ただし、ユーザーの目から見ると、情報サービスの所管は総合情報センターであるというイメージが強いことから、総合情報センターのホームページに香川大学 Moodle に関する紹介 (大学教育基盤センターの提供するホームページへの誘導) を行っている (/service/kagawaumoodle/)。本ページについては、アクセス数だけでなく順位も向上しており、香川大学 Moodle の利用者数の増加に伴い、ユーザーの導線確保に役立っていると考えられる。

表 2 Web ページアクセスランキングの経年比較

#	2017年度アクセスランキング		2018年度アクセスランキング	
	Webページ	回数	Webページ	回数
1	/service/gmail/loginlink/	46462	/	175140
2	/	33086	/service/gmail/loginlink/	104429
3	/service/gmail/	8218	/service/gmail/	33234
4	/service/gmail/	5581	/service/	23850
5	/contact/network	3098	/service/wifi/	17094
6	/service/wifi/	1498	/service/ninsyo/	9902
7	/service/	1296	/service/kagawaumoodle/	7621
8	/new_ts/	983	/service/gmail	7554
9	/service/office365/	944	/contact/network	6169
10	/service/kagawaumoodle/	736	/service/gmail/login/	5919

3. 2019 年度活動計画

2019 年度も引き続き、図 1 の業務範囲、表 1 の活動内容に沿って業務を遂行する。特筆すべき活動および業務改善として次の事項を考えている：

- ・サービス利用環境の整備として、本報告において述べた学生オープンスペース 1 の改修工事を実行する
- ・情報メディアの強化としてビデオコンテンツの

利活用を検討する

- ・トラブル解決支援の強化として、チャットボットの導入を検討する

- ・教職員 ICT 活用支援の強化として、オンライントレーニングコースの展開（業務に役立つ Excel スキルを題材として、香川大学 Moodle におけるビデオコンテンツ配信を計画している）

4. おわりに

2018 年度から米谷教員が部門長として就任した。2019 年度からは、部門員として、事務職員の新メンバーも加わる。部門員一致協力して、より良い「利用者支援」を目指して仕事に取り組んでいきたい。

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
(医学部情報ネットワーク管理室¹)

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。

本稿では平成 30 年度で完了した医学部附属病院の再開発に於ける学内ネットワークの対応について報告する。(学内ネットワークは Web やメールが使用可能なネットワークで電子カルテや PACS など医療業務ネットワークとは完全に分離されている)

2. 医学部附属病院再開発の概要

医学部附属病院は旧香川医科大学附属病院として昭和 58 年 (1983 年) に開院し病院機能充実と医療の高度先進化・専門化等を推進し地域医療の中核的役割を担っている。しかし経年による施設の老朽化や狭隘化はサービス面や特定機能病院として十分な状態ではなくなってきていた。このため平成 24 年度 (2012 年度) に開院以来の大規模な再開発に着手し南病棟と手術棟の新営、既存施設の改修を推進、平成 30 年度 (2018 年度) に完了した。

3. 再開発に於ける学内ネットワークの対応

3. 1 再開発前の学内ネットワーク

旧香川医科大学に学内ネットワークが最初に整備されたのは平成 6 年 (1994 年) である。以後ネットワーク機器の変革や更新で整備、拡充が図られて来た。ただ建屋に後付けで整備を重ねて来たため機器の多くは壁掛けか天吊りで、外来の待合や入室時に更衣が必要な手術機材準備室などすぐにアクセスができない箇所も多かった。また情報コンセントは増設時に空きポートのあるスイッチに繋ぐ対応がされたため情報コンセントとは別フロアや隣接する建屋のスイッチにも収納されており、結果行先不明の配線も多数存在する状況になっていた。

3. 2 設備の改善

再開発ではネットワーク機器や情報コンセントの配置がゼロベースで見直しされ改修工事と共に一体で整備された。アクセススイッチは各フロアの EPS 内 1 箇所 (中央診療棟、外来診療棟は各フロア 2 箇所) に 19 インチラックを設置し廊下から平服ですぐにアクセスが可能となった。情報コンセントは各部屋のレイアウトに合わせ数量と配置の最適化が図られた。これにより部屋内で LAN ケーブルが床や頭上を配線されることが無くなり安全面や見た目でも改善された。(図 1)



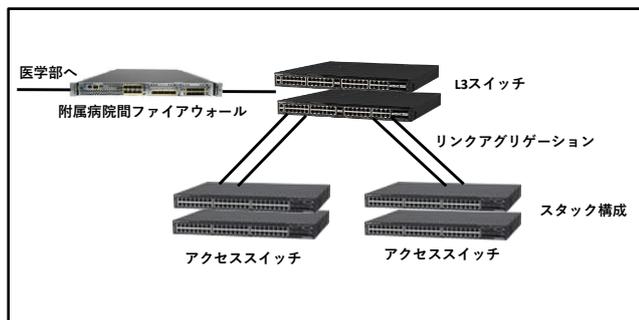
図 1 EPS 内の通信ラック

3. 3 基幹ネットワークの整備

医学部の基幹ネットワークは既に 10Gbps 化していたが、附属病院内の学内ネットワークは 1Gbps の構成であった。再開発では基幹ネットワークを 10Gbps 化で整備し、また L3 とアクセススイッチ間はリンクアグリゲーションによる冗長化と帯域拡張を図っている。また、アクセススイッチと各部屋の情報コンセント間は LAN ケーブルを Cat6A で整備しており将来は末端の機器まで 10Gbps 通信が行える環境としている。

附属病院と医学部間はファイアウォールによりセキュリティを確保しているが、ファイアウォールについても 10Gbps 化とパフォーマンスの向上を実施した。(図 2)

図2 附属病院の学内LAN基幹ネットワーク



3. 4 アクセススイッチ更新と情報コンセント

附属病院のアクセススイッチは平成19年度(2007年度)の導入で老朽化によるトラブルが課題となっていた。このため、工事の工程に合わせ、平成27年度(2015年)から4年計画で順次更新を実施した。(表1)

表1 附属病院内のアクセススイッチ更新

	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				

アクセススイッチの台数は新営の南病棟と手術棟で10台を整備したが、既設の建屋で設置場所の最適化やスイッチのポート数変更で4台削減し計6台の増加に抑制することができた。(表2)

表2 附属病院内のアクセススイッチ台数

	再開発前	再開発後
東西病棟	9	8
中央診療棟	9	9
外来診療棟	8	5
管理棟	1	1
放射線関連棟	4	4
(新営)南病棟	-	8
(新営)手術棟	-	2
合計	31	37

情報コンセントについては部屋のレイアウトに合わせる対応により再開発前に比べ約3倍と大幅に増加している。(表3)

表3 附属病院の情報コンセント数

	再開発前	再開発後
東西病棟	129	283
中央診療棟	164	475
外来診療棟	100	401
管理棟	11	11
放射線関連棟	46	46
(新営)南病棟	-	120
(新営)手術棟	-	45
合計	450	1381

3. 5 その他の整備

附属病院のヘリポートは平成26年(2014年)に新営され香川県防災航空隊などにより特に島嶼部や山間部などの患者輸送で大きな役割を果たしている。ヘリポートの気象情報などはヘリの安全運航に欠かせないため関係機関に常時提供できるよう整備されている。

3. 6 再開発工事中の対応について

再開発工事でも附属病院の診療や業務は通常通りでこの間に病院内で部屋の移動対応やネットワーク構成の変更が発生した。このため業務に支障がないよう仮設のフロアスイッチを延べ11箇所に設置、また移動に合わせVLAN変更やIPアドレスの割り当てを実施した。仮設のフロアスイッチは工事個所での設置が多く、主に撤去した機器を充当したが工事による粉塵は相当なもので機器内部に大量に入り込んだ。これによる故障やトラブルの発生はなかったが機器は工事後に全て廃棄となった。

4. おわりに

本報告では医学部附属病院の再開発対応に於ける学内ネットワークの対応について述べた。医学部では経年による施設の老朽化が進んでいる。今後の施設の改修時に今回の実績を踏まえて関係部門と連携しながら対応していきたい。

平成30年度の総合情報センター R & D : 対外発表

平成30年度サマリー

原著論文：1 招待論文：1 招待講演：1 講演論文：4

原著論文

[1] 米谷 雄介, 後藤田 中, 小野 滋己, 青木 有香, 宮崎 凌大, 八重樫 理人, 藤本 憲市, 林 敏浩, 今井 慈郎, 最所 圭三, "香川大学での標的型攻撃メール訓練の導入と改善点の検討", 学術情報処理研究, Vol.22, No.1, pp.54-63, 2018年9月19日(水)

招待論文

[2] 米谷 雄介, "香川大学における情報基盤のデザイン～技術的・物理的・人的・組織的観点からの総合的アプローチ～", 信学技報, ICTSSL2018-26, IN2018-43, pp.1-6, 2018年10月18日(土), 電子情報通信学会 情報ネットワーク研究会(於 高松商工会議所)

招待講演

[3] 米谷雄介, "香川大学での標的型攻撃メール訓練の導入と改善点の検討", 第15回総合情報メディアセンターシンポジウム2018, 2018年11月30日(金), (於 東京農工大学)

講演論文

[4] 宮崎 凌大, 後藤田 中, 米谷 雄介, 小野 滋己, 青木 有香, 八重樫 理人, 林 敏浩, 今井 慈郎, 喜田 弘司, 最所 圭三, "判断基準学習のための模擬インシデントによるリスクアセスメント訓練システム", 平成30年度電気関係学会四国支部大会論文集, 愛媛, p.193, 2018年9月22日(土)

[5] 宮崎 凌大, 後藤田 中, 米谷 雄介, 小野 滋己, 青木 有香, 八重樫 理人, 藤本 憲市, 林 敏浩, 今井 慈郎, 喜田 弘司, 最所 圭三, “振り返り強化のための模擬インシデント訓練によるリスクアセスメント情報共有システム”, 大学 ICT 推進協議会 2018 年度年次大会論文集, TC1-4, 2018 年 11 月 21 日 (於 札幌)

[6] 小野 滋己, 後藤田 中, 米谷 雄介, 青木 有香, 八重樫 理人, 藤本 憲市, 林 敏浩, 今井 慈郎, 最所 圭三, “パターン定義に要する対応期間の調査に基づくセキュリティ製品の妥当性点検”, WA1-3, 2018 年 11 月 21 日 (於 札幌)

[7] 宮崎 凌大, 後藤田 中, 米谷 雄介, 小野 滋己, 青木 有香, 八重樫 理人, 藤本 憲市, 喜田 弘司, 林 敏浩, 今井 慈郎, 最所 圭三, “リスクアセスメント情報を活用した判断基準共有のための模擬インシデント訓練システム”, 教育システム情報学会 2018 年度第 5 回研究会論文集, pp.67-74, 2019 年 1 月 12 日 (土) (於 福島)

