三本の矢（技術・規則・教育）で守る情報基盤

西村　浩二

大学などにおける情報基盤を安全に保つためには高性能や高機能な「技術」を追求するだけでは不十分であり，情報基盤を適切な「規則」に基づいて運用・管理し，さらに情報基盤の管理者だけでなく利用者を適切に「教育」することが重要である．これらをバランスよく実施し機能させることで組織の情報基盤がより安全に保たれることを，毛利元就の三矢の教えに例えて表現している．本稿では，毛利輝元（毛利元就の孫）のお膝元であり，約20,000 名の構成員を擁する国立総合大学である広島大学における取り組みを紹介している．

キーワード：情報基盤構築，クラウドサ―ビス，ISMS，クラウドセキュリティ，情報セキュリティ教育，インシデント対応訓練

1. はじめに

大学などにおいては，高度かつ先進的な教育研究を円滑に推進するため，高性能かつ高機能な情報基盤の構築・運用が求められる．その際，昨今の情報セキュリティに対する脅威から組織を守るための情報セキュリティ対策と管理運用コストの削減という相反する要求が課せられる．これらをバランスよく実施し機能させるためには，組織全体を対象とした，全方位的かつ長期にわたる取り組みが必要となる．本稿では，12 学部・1 研究科，学生教職員 19,226 名（令和元 (2019) 年 5 月 1 日現在）を擁する国立総合大学である広島大学において，長年にわたり継続して行ってきた情報基盤とそのサービス，情報セキュリティに対する取り組みを紹介する．これらの取り組みとその成果を俯瞰することで，それぞれの組織が自らを守る情報基盤のあり方について議論を始めるきっかけとしたい．

以下では，広島大学において行っている情報セキュリティ対策を毛利元就の三矢の教えに例えて，「技術の矢」「規則の矢」「教育の矢」として紹介する．2 節「技術の矢」では情報基盤サービスにおける情報セキュリティ対策，3 節「規則の矢」では情報セキュリティ管理策に基づく情報セキュリティ対策，4 節「教育の矢」では情報セキュリティ教育に基づく情報セキュリティ対策についてそれぞれ述べる．最後に 5 節では，広島大学における全方位かつ長期にわたる情報セキュリティ対策の進め方および今後の方針について述べる．

にしむら　こうじ
広島大学情報メディア教育研究センター
〒 739–8511 広島県東広島市鏡山 1–4–2
kouji@hiroshima-u.ac.jp

2. 技術の矢（情報基盤サービス）で守る

2.1 広島大学情報ネットワークシステム (HINET2014)

広島大学のキャンパスネットワークは，その名称を，広島大学情報ネットワークシステム (Hiroshima university Information NETwork system) を表す “HINET” に整備された西暦を付したものとしている．平成 5 (1993) 年に整備された HINET93 から始まり，HINET95，HINET2001，HINET2007，HINET2014 とおおむね 6〜7 年ごとに整備・機能強化が行われてきた．現在稼働中の HINET2014 は，HINET2007 で新たに導入されたさまざまなセキュリティ機能を強化して運用されている（図 1）．HINET2007 で導入されたセキュリティ機能は次のとおりである [1].

1. 全学的な一元管理体制の構築
2. 個別ファイアウォール機能の提供
3. VLAN による柔軟な仮想配線の提供
4. すべての利用場所で利用者認証を要求

1 の「全学的な一元管理体制の構築」では，学内の建物の各フロアに設置されるフロアスイッチのポート（約 18,000 ポート）を一元的に管理する体制を整えた．これを実現するため，支線ネットワークの調査，再敷設などが行われた．2 の「個別ファイアウォール機能の提供」では，個別ファイアウォール（NAPT 機能と DHCP サーバ機能）を教員に一つずつ（計 2,000 個）提供し，これまでそれぞれがブロードバンドルータなどで行っていた研究室ネットワークの管理・維持コストの削減を図った．そして 3 の「VLAN による柔軟な仮想配線の提供」により，建物間やキャンパス間などの物理的な制約を超えて，個別ファイアウォールで保

 Copyright ⓒ by ORSJ. Unauthorized reproduction of this article is prohibited.

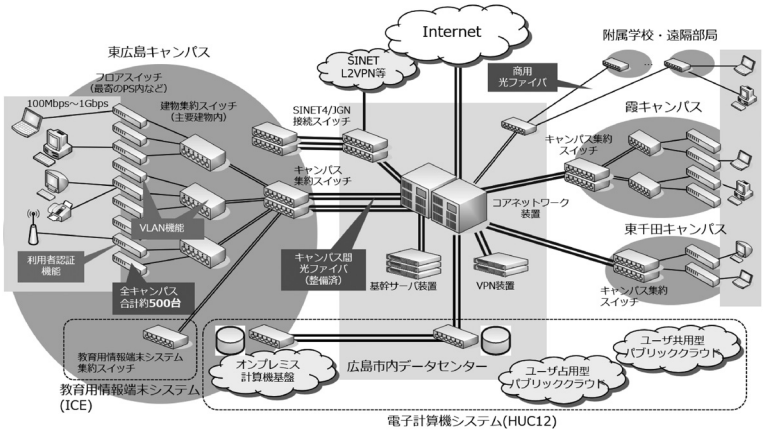


図 1　HINET2014

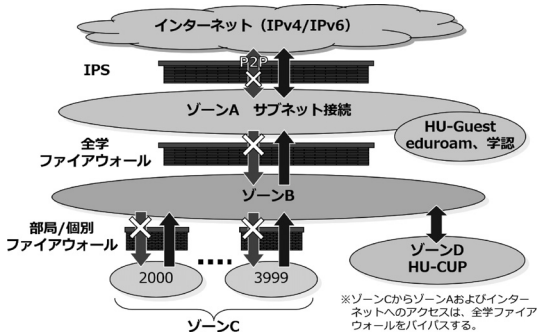


図 2　HINET2014 におけるゾーニング

護された研究室ネットワークを構築することを可能とした．さらに 4 の「すべての利用場所で利用者認証を要求」では，認証ポイントをフロアスイッチの各ポートとすることで，個別ファイアウォールの配下も含めて利用状況を把握できるようにした．

一方 HINET2014 では HINET2007 の機能を引き継ぎつつ，主に以下の機能強化が行われた [2]．

1. 個別ファイアウォールに接続可能な VPN サービス
2. SINET4/JGN-X における L2 接続の強化
3. ログ保存・検索のためのクラウドサービス利用
4. すべてのゾーンで IPv6 を標準サポート

この中で特筆すべきは，1 の「個別ファイアウォールに接続可能な VPN サービス」の提供であろう．2,000 個の個別ファイアウォールへの学外からのアクセス手段の提供は，利便性とセキュリティを両立するうえで重要なサービスとなっている．そのほかの機能の説明については紙面の都合上割愛するので，参考文献 [2] をご参照いただきたい．

HINET2007/2014 では，これらの機能に加えて学内外からのアクセス可否パターンや利用形態により区別される「ゾーン」の概念を導入している．図 2 にゾーンの概要を示す．構成員の多くは研究室などを単位とするゾーン C を申請し，その中で生活する．一方，学外公開を前提とするサーバなどはゾーン A に，複数のゾーン C やゾーン D からアクセスされる学内限定サーバはゾーン B に配置することが推奨されており，サーバ管理者は目的に応じたネットワーク環境を選択・申請し，利用する．このように広島大学では，多様な利用目的に適応可能なネットワーク環境を構築し，利便性とセキュリティの両立を図っている．

2.2　広島大学電子計算機システム (HUC12)

もう一つの広島大学の情報基盤サービスとして，広島大学電子計算機システムがある．こちらは (Hiroshima University Computer system) を表す “HUC” に整備された世代番号を付した名称となっている．つまり，平成 27 (2015) 年度から稼働中の HUC12 は第 12 世代目を意味している．これまでの電子計算機システムの構築は，サービスの設計から必要なハードウェアの調達，運用までを大学側で行うのが常であった．しかし，クラウドファーストの波は大学の情報基盤サービスの調達にも押し寄せつつあったことから，HUC12 では将来の HUC (HUC13) のクラウドサービス利用へのスムーズな移行を図る目的で，「トランジション」を合言葉として調達を行った．HUC12 の調達方針は，ハードウェア志向からサービス志向への調達方法の転換である．これまでのハードウェア中心の仕様策定から，クラウドサービスの活用や利用形態への適合性に重点を置いた，ハードウェアに依存しないサービス中心の仕様策定への転換に挑戦した．また同時に，クラウドサービスを活用する大学 ICT システムの将来像につ

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

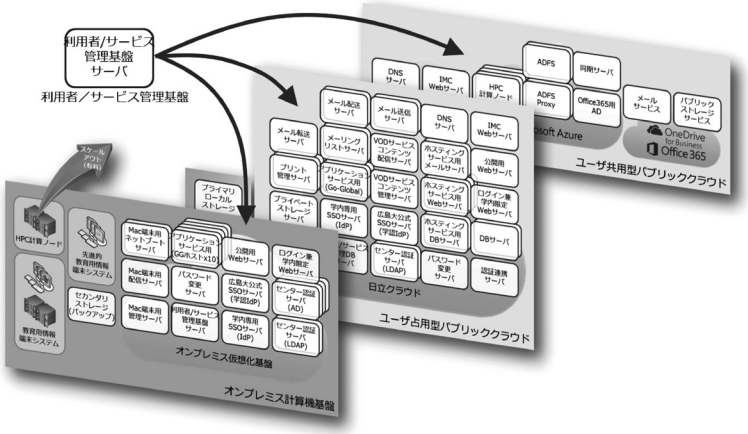


図 3　HUC12 の全体概要

図 4　広大 ID と IMC アカウントの関係（利用登録システム）

いての議論を重ね，利用者やサービスの管理を中心とし，目的に適した実装方法（複数のクラウドサービスなど）を選択して利用するシステムとして構築した [3]．HUC12 の全体概要を図 3 に示す．

HUC12 の中心となる利用者／サービス管理基盤は，システム全体の司令塔としての役割を果たす．具体的には，利用者の認証情報の管理と利用者が利用する各種情報サービスの制御（プロビジョニング）を行う．広島大学には大学の人事情報や学生情報に基づく「広大 ID」と情報メディア教育研究センター (IMC: Information Media Center)（以下，メディアセンターと言う）「IMC アカウント」の二つの ID 体系があり，それぞれ「人」の管理と「サービス」の管理に利用される．広島大学に在籍する（広島大学に資する活動をする）者には広大 ID が付与される．そしてこの広大 ID の所有者に，広島大学の情報基盤サービスを利用するための IMC アカウントが付与されるという関係にある（図 4）．したがって，在籍期間中は広大 ID が常に有効であり，IMC アカウントは広大 ID から停止や再開の制御を行うことができる．一方，IMC アカウントからは広大 ID を制御することはできない．後に述べるが，このような ID 体系を構築することが，利便性とセキュリティ維持の両立に役立つと考えている．

3.　規則の矢（情報セキュリティ管理）で守る

3.1　情報セキュリティポリシーとインシデント対応

広島大学では，多くの大学などが情報セキュリティポリシーを策定する際の参考としている「高等教育機関の情報セキュリティ対策のためのサンプル規程集」が策定された平成 19 (2007) 年 2 月よりも早い平成 17

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

(2005) 年 4 月に，基本方針，対策基準，実施手順からなる広島大学情報セキュリティポリシーを策定した（図 5）[4]．この策定にあたっては，理想としてどうあるべきかを考えるのと同時に，その実行可能性に重きを置いており，実施手順については，策定後ほぼ毎年見直しが行われている．情報セキュリティインシデントへの対応については，実施手順においてメディアセンターと情報化推進部（現：財務・総務室情報部）で組織する情報セキュリティ推進機構（以下，機構と言う）が情報セキュリティの維持および向上に関する業務を遂行することとなっている．また平成 27 (2015) 年度末の改訂によって，機構は広島大学の CSIRT (Computer Security Incident Response Team) 機能を担うことが明文化された．2 節で述べたとおり，広島大学では「技術の矢」によって情報セキュリティ対策を行っているが，昨今の情報セキュリティの脅威に対して必ずしも十分であるとは言えない．そのため，自組織の機器などから得られる情報のほかに，外部組織から提供される情報を参考に情報セキュリティ対応を行っている．ここでは，外部組織からの情報のうち国立情報学研究所 (NII) が平成 29 (2017) 年度から運用を開始した NII-SOCS（大学間連携に基づく情報セキュリティ体制の基盤構築）[5] の広島大学での活用方法について述べる．

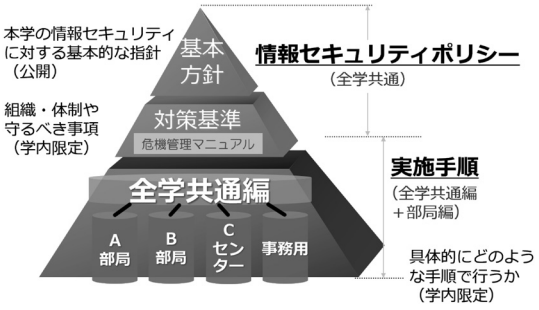


図 5　広島大学情報セキュリティポリシー

広島大学では，情報セキュリティインシデント発生時の対応手順において，メディアセンター長に通信制限の権限が与えられており，メディアセンター長が情報セキュリティインシデントと判断するに足る情報を確認し，緊急を要すると判断した場合は，該当者への事前通知なく通信制限を設定することを可能としている．機構では，平成 29 (2017) 年 3 月〜6 月末に行われた NII-SOCS の試験運用に参加し，その通知情報の正確性や即時性の検証を行った．そして同年 7 月からの正式運用に合わせて，メディアセンター長が NII-SOCS から提供される情報を「信頼できる情報」と指定し，全学委員会の了承を経て，メディアセンター長があらかじめ通信制限を指示しておくこととした．この指示により，NII-SOCS からの通知があった場合は即座に通信制限を行う体制が整ったが，CSIRT が 24 時間 365 日で対応することは現実的に不可能である．

広島大学の対外接続は，中国・四国地域の学術ネットワーク SuperCSI を利用している．SuperCSI では通信事業者による 24 時間 365 日の監視体制が敷かれており，夜間や休日の障害にも対応（運用担当者への電話連絡など）している．そこで，(1) あらかじめ通信事業者と通信制限を行う IP アドレス範囲を決定し，(2) NII-SOCS からの通知に通信制限対象の IP アドレスが含まれる場合は SuperCSI 監視部門がただちに通信制限を行って，(3) CSIRT に電子メールによる報告を行う（図 6）．加えて，(4) あらかじめ指名した CSIRT 担当者からの指示により通信制限の設定および解除を行うこととした．これを一次対応としたうえで，CSIRT 担当者は通信制限の対象となったホストの利用者を特定し，利用者が対応を行ったことを確認して通信制限を解除する．

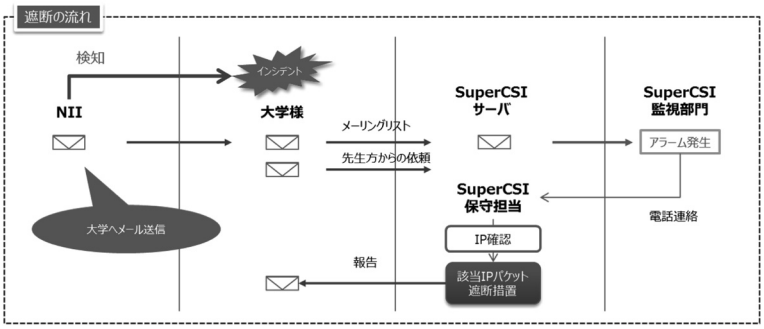


図 6　NII-SOCS 一次対応

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

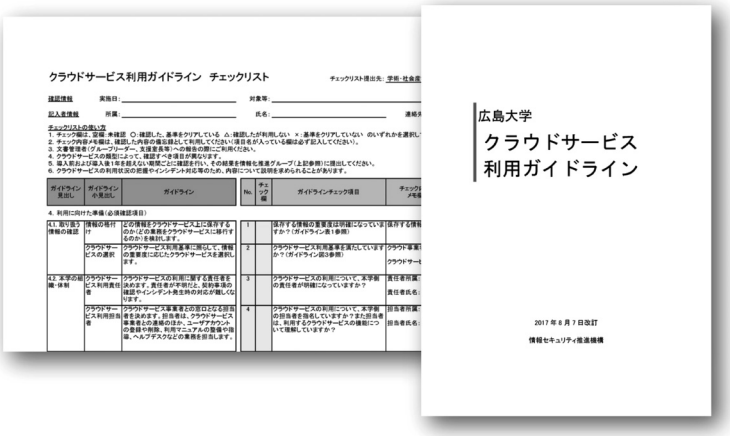


図 7　広島大学クラウドサービス利用ガイドライン・チェックリスト

3.2　クラウドサービス利用ガイドライン・チェックリスト

一般向けのクラウドサービスの提供が始まり個人利用へと浸透していく中で，広島大学においても，平成 23 (2011) 年頃から BCP/DR 対策を含めた大学での業務や教育研究活動におけるクラウドサービス利用に関する要望や問合せが急増するようになった．その多くは，個人向けのクラウドサービスにおいて大学の情報を取り扱ってよいか，クラウドサービスのよい使い方，悪い使い方を教えてほしいというものであった．しかし当時の情報セキュリティポリシーでは，重要な情報の組織外への持ち出しを禁止したり，制限を課したりすることのみが規定されており，クラウドサービス固有あるいはクラウドサービスごとに異なる表現に基づく具体的な条件や選定方法を示したものは存在していなかった．そこで広島大学では，国内外のガイドラインなどを参考に，平成 25 (2013) 年 3 月に広島大学クラウドサービス利用ガイドライン・チェックリスト（以下，ガイドラインと言う）を策定した（図 7）[6].

ガイドラインは 45（第一版当時，第三版では 46）のチェック項目からなり，大きくクラウドサービスの利用に向けた「準備」，契約条件や利用範囲，クラウド事業者の「検討」，「運用」の三つの部分から構成されている．「準備」においては，クラウドサービスで取り扱う情報の格付けや利用責任者・担当者などの運用体制，組織の情報セキュリティポリシーとの整合性などを確認する．「検討」においては，データの取り扱いなどに関する責任範囲や準拠法，管轄裁判所などの契約条件の確認，利用するクラウドサービスの品質や機能，コストの確認，クラウドサービスを提供するクラウド事業者の信頼性の確認などを行う．「運用」においては，クラウド事業者によるデータの管理状況やセキュリティ対策の実施状況，インシデント管理の方法などを確認する．

国立情報学研究所 (NII) 学認クラウド導入支援サービス [7] が提供するチェックリストや大学 ICT 推進協議会 (AXIES) クラウド部会が提供する大学向けクラウドソリューションカタログ [8] のように，クラウドサービスのガイドライン・チェックリストでは一般性を確保するため，主に「検討」に該当する項目を確認するものが多い．一方，本ガイドラインでは利用主体（利用者）のクラウドサービスに対する正しい理解や利用者としての対応の必要性を促すことに主眼を置いて作成されている点が異なっている．つまり本ガイドラインは広島大学用であり，それぞれの組織ごとにガイドラインを策定する必要があることを意味している．実際，本ガイドラインの内容は前述のチェックリストやカタログに記載されている項目のうち，広島大学が特に重要と考えている項目（サブセット）となっており，それに広島大学の情報セキュリティポリシーに基づく確認項目を追加したものとなっている．

3.3　情報セキュリティマネジメントシステム (ISMS) 認証取得への取り組み

メディアセンターは，昭和 40 (1965) 年 4 月に学内共同利用施設として発足して以来，更新や機能拡張を繰り返しながら 2 節で述べたような情報基盤サービスを全学に提供する組織として活動を行ってきた．その方法は長年の経験や最新の研究から得られた知見に基づくものではあるが，同様な情報系センターの多くがそうであるように，第三者による外部評価を受けるこ

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

図 8　ISMS/ISMS-CLS 登録証

とがなかった．近年では，大学などのアカデミックの現場においても情報セキュリティインシデントあるいはその前兆とみられるトラブルが続いていたことから，第二期中期目標・計画（平成 23〜27 年度）における最終年度である平成 27 (2015) 年度末までに，情報基盤サービスの運用管理に対する情報セキュリティマネジメントシステム（ISMS, ISO/IEC 27001）認証を取得することを計画した．

メディアセンターにおける ISMS 認証取得は平成 24 (2012) 年度末から本格的な準備を開始し，平成 26 (2014) 年 12 月の文書レビュー，平成 27 (2015) 年 1 月の初動審査，同年 3 月の本審査を経て，初回の認証を取得した（有効期限：平成 30 (2018) 年 3 月）[9]．この時期の取得には，同年に予定されていた HUC12 の導入・運用に，ISMS に基づく情報セキュリティ管理を適用する目的もあった．新システムの導入・運用には，旧システムからのデータ移行をはじめ，新システムの導入説明会，ヘルプデスク対応など，導入業者だけでなく利用者（ISMS でいう利害関係者）への周知・教育が重要である．ISMS 維持管理活動は，メディアセンタースタッフの新システムへの理解を深め，情報セキュリティに対する意識を高めることに貢献したと考えられる．

2.2 節で述べたように，HUC12 ではオンプレミスでのシステム運用からクラウド活用へとシステム調達方法の転換を図った．その際，3.2 節で述べたガイドラインを活用して取り扱う情報や必要とされる機能などを確認した．ガイドラインの活用と ISMS におけるリスクアセスメントと管理策策定の経験が，オンプレミスとクラウド利用のリスクを冷静に比較・判断することを可能にしたと考えられる．その後 ISMS 認証規格においても，汎用的な情報セキュリティ管理策である ISMS にクラウドサービス視点の情報セキュリティ管理策を追加（アドオン）する ISMS クラウドセキュリティ (ISMS-CLS, ISO/IEC 27017) 認証が策定され，平成 28 (2016) 年度から利用できるようになった．そこでメディアセンターでは，本学のガイドラインのリスクアセスメント手法としての有効性と HUC12 の導入・運用の過程で行ったクラウドサービス選択と運用手順構築の妥当性の評価を目的として，ISMS-CLS 認証の取得を計画した．

ISMS-CLS 認証の取得に際しては，本学のガイドラインのチェック項目と ISMS-CLS 認証に関する要求事項 (JIP-ISMS517) との対応状況を確認し，クラウドサービスカスタマとしての要件への適合性を確認した．ISMS-CLS 認証の本審査は，ISMS 認証の 2 年次定期サーベイランス審査に合わせて受審し，平成 29 (2017) 年 3 月に認証を取得した [10]．前述したように ISMS-CLS 認証は ISMS 認証のアドオン認証であるため，その有効期限は ISMS 認証の有効期限である平成 30 (2018) 年 3 月までの 1 年間である．その後は ISMS および ISMS-CLS ともに PDCA に基づく管理策の改善を行いつつ，平成 30 (2018) 年 3 月には更新審査，平成 31 (2019) 年 3 月には 1 年次サーベイランス審査にそれぞれ合格し，現在に至っている（図 8）．

ISMS 認証および ISMS-CLS 認証の取得を通して，メディアセンターが構築・運用する情報基盤サービスが第三者目線で一定の情報セキュリティレベルを有す

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

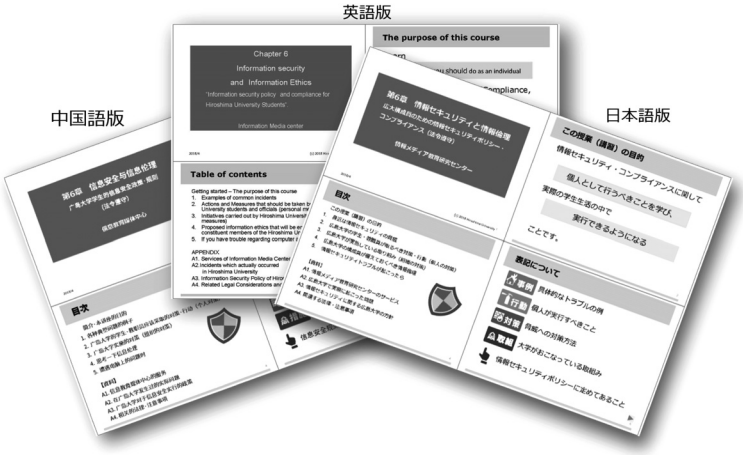


図 9　情報セキュリティ・コンプライアンス教育の教材

ること，本学のガイドラインがクラウドサービス利用のためのリスクアセスメント手法として有効であることが実証された．

4.　教育の矢（情報セキュリティ教育）で守る

4.1　情報セキュリティ・コンプライアンス教育

広島大学では，情報セキュリティの維持・違法行為の防止，広島大学の学生としてもつべき倫理観の醸成を目的として，平成 23 (2011) 年度より全学生に対する情報セキュリティ・コンプライアンス教育を実施している [11]．広島大学への在籍 1 年目となる学生（学部 1 年次生，大学院博士課程前期・後期 1 年次生，編入学生，研究生，科目等履修生など）は，在籍開始後 3 カ月以内に座学＋オンライン講座＋確認テストからなるフレッシュマン講習を受講する．一方，在籍 2 年目以降の学生は，毎年度 4 月から 3 カ月以内に自己点検＋オンライン講座＋確認テストからなるフォローアップ講習を受講する（平成 24 (2012) 年度から全教職員に対象を拡大した）．

フレッシュマン講習の座学では，広島大学で学生生活を送るうえでの基盤となる情報セキュリティやコンプライアンス，情報倫理の基礎そして広島大学の情報基盤サービスや規則について学ぶ．座学は，平成 30 (2018) 年度から学部 1 年次生の必修科目「大学教育入門」の一部に組込まれるようになった．フォローアップ講習の自己点検では，過去 1 年間の自らの行動を振り返り，改善すべき点を再認識する．両方の講習に含まれるオンライン講座では，1 年目に座学で学習した基礎知識をベースにその年度で新たに習得すべき事項や技術を学び，知識の更新を行う [12]．そして確認テストでは，座学で学習した基礎知識とオンライン講座で追加習得・更新された知識の定着を確認する．

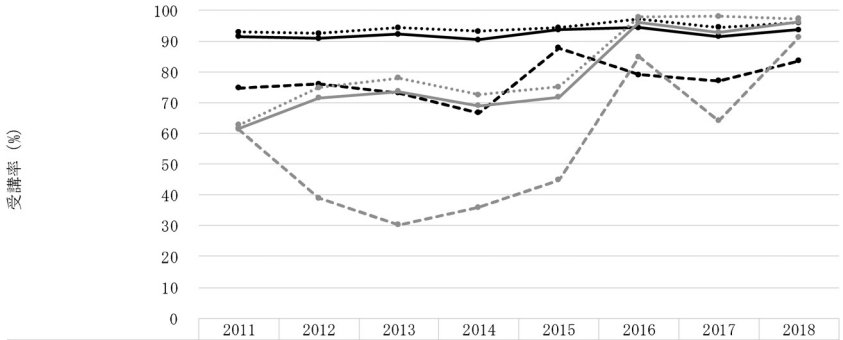
令和元 (2019) 年 5 月 1 日現在，広島大学には 72 カ国（地域）1,899 名の外国人留学生が在籍している．このうち 1,200 名 (63.2%) が中国語圏からの留学生である．そのため，情報セキュリティ・コンプライアンス教育の教材は日本語・中国語・英語の 3 カ国語で提供されており，座学は日本語と英語は講師が直接，中国語は逐次通訳を通して実施されている（図 9）．

平成 23 (2011) 年度から平成 30 (2018) 年度までの座学およびオンライン講座の受講状況を図 10 に示す．座学については開始以来 90%以上の受講率を達成・維持している．一方，オンライン講座の受講率は開始当初は 60%台だったのに対して，平成 28 (2016) 年度以降は 90%以上を達成・維持している．この理由については次節で述べる．

4.2　アカウントの年度更新・利用確認

メディアセンターが管理運用する情報基盤サービスにおいて，適切な管理が行われていないまま長期間放置されているアカウント（遊休アカウント）は情報セキュリティ上のリスクとなりうる．そこで平成 20 (2008) 年度から，在籍 2 年目以降となる学生・教職員および学外者を対象に「アカウント年度更新」を開始し，年度替わりの時期にアカウント継続利用の手続きを行わなかった場合はアカウントの停止（ロック）を行うこととした [13]．開始当初のアカウント継続利用の手続きは，利用登録システムへのログイン後に表示される利用規約に同意する（同意ボタンを押す）というものであった．しかしこの方法では形骸化を招くことが容

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.



	2011	2012	2013	2014	2015	2016	2017	2018
座学前期	92.9	92.5	94.4	93.2	94.4	97.1	94.5	96.0
座学後期	74.8	76.0	73.1	66.6	87.7	79.1	77.1	83.6
座学通年	91.5	90.9	92.3	90.4	93.6	94.3	91.4	93.7
オンライン講座前期	62.7	74.9	78.0	72.6	75.1	97.8	98.0	97.2
オンライン講座後期	61.3	39.0	30.3	35.9	44.9	84.8	64.1	91.2
オンライン講座通年	61.5	71.5	73.6	69.0	71.7	96.0	92.8	96.2

図 10　座学・オンライン講座の受講状況

易に想像できることから，情報セキュリティ・コンプライアンス教育を開始した平成 23 (2011) 年度からは，在籍 2 年目以降となる学生に対して確認テストへの合格をアカウント年度更新の前提条件とするよう変更した．また平成 24 (2012) 年度からの受講対象拡大に合わせて，教職員も確認テストへの合格が前提条件となった．

一方，在籍 1 年目の学生・教職員は年度更新の対象とはならない．しかしながら初年度からアカウントは利用可能であるため，最長 1 年間は放置される恐れがあり，また在籍直後で広島大学の規則などへの早急な理解と実践が必要であることから，在籍 1 年目の学生・教職員に対する「アカウント利用確認」を平成 28 (2016) 年度から開始した．この名称はアカウント利用に関して初年度であるためであって，条件や内容は「アカウント年度更新」と同様である．4.1 節に示したようにオンライン講座の受講率が 90%以上に上昇・維持されているのは，この措置によるものである．

4.3　情報セキュリティインシデント対応訓練

広島大学の情報セキュリティポリシーでは，対策基準において CISO が全学共通の情報セキュリティに関する危機管理マニュアル（以下，危機管理マニュアルと言う）を策定することとなっている．危機管理マニュアルでは，情報セキュリティインシデント・トラブルの恐れがある場合，機構は該当するホストの通信制限を行ったうえで，当該ホストの利用者に一次報告を求める．一次報告の内容は以下に示すとおりである．

- 該当するコンピュータの利用目的
  共同利用や出張時使用など
- 該当するコンピュータの形状
  コンピュータの種類，メーカ，型番など
- 該当するコンピュータの使用状況
  OS の種類と bit 数，OS の最終更新日，ウイルス対策ソフト名，パターンファイルの最終更新日，最終スキャン日など
- ウイルススキャンの結果
  フルスキャン時の検知の有無，検知された場合のウイルス名や駆除状況など
- 暗号化されて開けないファイルの有無
- 該当するコンピュータに保存されている情報
  個人情報や法人文書などのデータの有無，データの内容，暗号化の有無など
- フリーソフトのインストール状況
- 指摘された原因
  思い当たる事象など
- 今後の対策
  初期化，ソフトウェア更新，フルスキャン実施など

しかし，突然の状況で適切な対応を行うことは一般には困難であると考えられる．このようなことから広島大学では，平成 30 (2017) 年度から情報セキュリティインシデント対応訓練（以下，対応訓練と言う）を行っている [14]．

一般に対応訓練と言えば，構成員宛にフィッシング

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

表 1　情報セキュリティインシデント対応訓練の受講・実施状況

実施年度	対象者	対象者数	事前教育		対応訓練	
			受講者数	受講率	実施者数	実施率
2017 年度	教員	1,749	1,116	63.8	1,153	65.9
	職員	1,747	870	49.8	766	43.8
	全体	3,496	1,986	56.8	1,919	54.9
2018 年度	学生	16,739	3,700	22.1	7,312	43.7
	教員	1,763	1,045	59.3	1,568	88.9
	職員	1,682	763	45.4	1,087	65.6
	全体	20,184	5,508	27.3	9,967	49.4
	（うち教職員）	(3,445)	(1,808)	(52.5)	(2,655)	(77.1)

メールを装った電子メールを送信し，その開封率や電子メールに記載された URL へのアクセス率を調べることで訓練の効果を測定することが多い．しかし広島大学の対応訓練では，情報セキュリティインシデントが発生した際の対応を全構成員がすばやく適切に行うことができることを目的としており，構成員が日常的に使用しているホストで情報セキュリティインシデントが発生した場合を想定し，機構に報告すべき内容と手順を学ぶ．

対応訓練の流れは以下のとおりである．(1) 対応訓練の 2 週間前に LMS (Learning Management System) を利用した事前教育が行われる．ここでは，標的型攻撃の脅威やインシデント発生時の対応手順などを学ぶ．(2) 対応訓練は対象者への訓練開始メールにより開始される．訓練開始メールは情報セキュリティインシデント発生の恐れがある場合に機構から通知される内容と同様である．利用者はこのメールの指示に従って，自身のホストの調査を行い，LMS で報告書を提出する．対応訓練の期間は 1 週間（その後 1 週間の延長期間を設ける）である．(3) 対応訓練期間が終了すると，機構は事前教育の受講状況および対応訓練の実施状況を所属部局別に集計・評価し，全学委員会において報告する．

平成 29 (2017) 年度は常勤教職員 (3,496 名)，平成 30 (2018) 年度は常勤教職員＋学生 (3,445 名＋ 16,739 名) を対象に対応訓練を実施した．実施状況を表 1 に示す．常勤教職員の事前教育の受講率は 56.8％から 52.5％に低下しているものの，対応訓練の実施率は 54.9％から 77.1％に上昇していることから，インシデント発生時の対応手順が浸透しつつあると考えられる．一方，学生の事前教育の受講率，対応訓練の実施率は，初年度ということもあり低い結果であった．今後，情報セキュリティインシデント対応訓練の必要性や意義に関する（事前教育のさらに前段の）教育が必要であると考えている．

5.　おわりに

本稿では，広島大学が長年にわたり行ってきた情報セキュリティ対策の概要について，その目的や位置づけなどを含めて解説した．個々の対策はいずれの大学などでも行われていると思われるが，それぞれの位置づけや連携については改めて検討する余地があると思われる．広島大学では，毛利元就の三矢の教えに例えた「技術」「制度」「教育」という三つの基本要素を連携させる形に落ち着いた．しかし広島大学においても，開始当初から現在の形を想定していたわけではなく，今必要とされることは何か？これまでに行ってきたこととの関連はどうか？今後どのように情勢が変化するか？を常に考えながら，無駄や矛盾がない情報基盤サービスの提供を心がけてきた．その結果として，サービスの利便性を保ちつつ，セキュリティを比較的高いレベルに向上・維持させることが可能となったと確信している．

本学では，令和 2 (2020) 年度に電子計算機システムの，令和 3 (2021) 年度にキャンパスネットワークの更新が控えている．次期システム／ネットワークの仕様検討では，HUC12 や HINET2014 の管理運用，ISMS 認証や ISMS-CLS 認証の維持から得られた知見を元に，システムとネットワークの連携をより強める必要があると考えており，クラウド時代における大学の情報基盤とそのサービスのあり方を再認識する機会としたいと考えている．

謝辞　日頃より広島大学の情報基盤サービスの構築および運用，利用者対応に尽力いただいている情報メディア教育研究センター各位，また情報セキュリティインシデント・トラブル対応や ISMS 推進活動などの進捗管理に尽力いただいている財務・総務室情報部各位に感謝いたします．

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

参考文献

[1] 近堂徹，田島浩一，岸場清悟，大東俊博，岩田則和，西村浩二，相原玲二，“利用者認証機能を備えた大規模キャンパスネットワークの性能評価，”インターネットと運用技術シンポジウム 2008 論文集，pp. 121–128, 2008.

[2] 近堂徹，田島浩一，岸場清悟，吉田朋彦，岩田則和，大東俊博，西村浩二，相原玲二，“クラウドコンピューティング活用のための大規模キャンパスネットワーク，”インターネットと運用技術シンポジウム 2014 論文集，pp. 101–108, 2014.

[3] 西村浩二，“広島大学電子計算機システム (HUC12) におけるクラウドサービス利用，”大学等におけるクラウドサービス利用シンポジウム 2015，https://www.media.hiroshima-u.ac.jp/st/news/cloudsympo/cloudsympo-20150320-5.pdf （2019 年 6 月 10 日閲覧）

[4] 広島大学，「情報セキュリティポリシー基本方針（全文），対策基準（あらまし）」，https://www.hiroshima-u.ac.jp/about/initiatives/jyoho_ka/security_policy （2019 年 6 月 10 日閲覧）

[5] 国立情報学研究所，「大学間連携に基づく情報セキュリティ体制の基盤構築 (NII-SOCS: NII Security Operation Collaboration Services)」，https://www.nii.ac.jp/service/nii-socs/ （2019 年 6 月 10 日閲覧）

[6] 広島大学情報メディア教育研究センター，「広島大学クラウドサービス利用ガイドライン」，https://www.media.hiroshima-u.ac.jp/news/cloudguide（2019 年 6 月 10 日閲覧）

[7] 学認クラウド，「学認クラウド導入支援サービス」，https://cloud.gakunin.jp/cas/ （2019 年 6 月 10 日閲覧）

[8] 大学 ICT 推進協議会，「クラウドソリューションカタログ」，https://axies.jp/ja/qruv9l/24gxa6 （2019 年 6 月 10 日閲覧）

[9] 広島大学情報メディア教育研究センター，「情報メディア教育研究センターにおける ISMS 認証取得の取り組み」，https://www.media.hiroshima-u.ac.jp/news/isms（2019 年 6 月 10 日閲覧）

[10] 西村浩二，“ISMS クラウドセキュリティ認証の受審報告，”大学等におけるクラウドサービス利用シンポジウム 2017，https://www.media.hiroshima-u.ac.jp/st/news/cloudsympo/cloudsympo-20170310-7.pdf （2019 年 6 月 10 日閲覧）

[11] 西村浩二，大東俊博，岩沢和男，隅谷孝洋，稲垣知宏，中村純，宮内祐輔，三戸里美，相原玲二，“広島大学における情報セキュリティ・コンプライアンス教育の取組み，”情報処理学会研究報告　インターネットと運用技術 (IOT)，2012-IOT-18, No.2, 2012.

[12] 渡邉英伸，岩沢和男，西村浩二，“全学構成員向け情報セキュリティ・コンプライアンス教育コンテンツの再開発，”学術情報処理研究，**21**, pp. 55–62, 2017.

[13] 岩沢和男，渡邉英伸，西村浩二，“情報セキュリティ教育を支援する情報サービス管理，”学術情報処理研究，**22**, pp. 83–91, 2018.

[14] 渡邉英伸，相原玲二，西村浩二，“広島大学における情報セキュリティインシデント対応訓練，” 大学 ICT 推進協議会 2017 年度年次大会，WF2-4, 2017.

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.