大学における情報セキュリティインシデントの現状と対策、そして今後

西村 浩二
広島大学情報メディア教育研究センター　教授

概要：多くの大学では、在籍する構成員に対してコンピューティングサービスやネットワークサービスを提供することを主なミッションとする情報系センターを擁している。昨今の情報セキュリティインシデントの変化や増加により、これらのセンターが果たす役割は大きく変化してきている。広島大学における情報セキュリティインシデントの現状を概観し、これまでに行っている対策を紹介するとともに、今後検討すべき課題について述べる。

キーワード：情報セキュリティ、クラウド

1. 広島大学の情報セキュリティに対する取り組み

広島大学は、構成員数 18,936 名 [1] の比較的大きい国立大学である。東広島、霞、東千田の 3 つのキャンパスの他に、遠隔地区・施設、県外・海外オフィスがある。

大学は自由に研究ができて、制約を受けない場所という風潮があり、ファイアウォールを嫌う傾向があるが、広島大学では、2006 年に初めてファイアウォールを導入した。導入後に、ファイアウォールがブロックしたアクセス数をグラフにしたものが図 1 である。

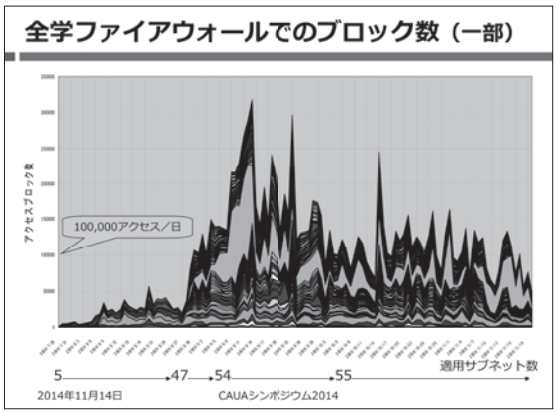

図 1　ファイアウォールでのブロック数

サブネット単位で管理をしており、少しずつファイアウォールの下に追加をしていったところ、適用サブネット数が 50 近くになったところで、ブロックされるアクセス数がぐんと上がった。大学は、自由な反面、非常に多くの攻撃を受けていることがわかる。この数値を大学の上層部に提示し、セキュリティ対策の必要性をアピールしていった。さらに、実際に使っている利用者に対してもこの結果を見せて、ファイアウォールの必要性をきちんと認識してもらうようにした。

その後、ウイルスチェックやアクセス制御、ウィルス対策ソフト、全学ファイアウォール、迷惑メールの振分の機能を加えていくことにより、2007 年ごろには、セキュリティインシデントの報告が急激に減った（図 2）。ネットワーク環境に対して、技術的に対策を取ることにより、一定の効果が出ることが証明された。

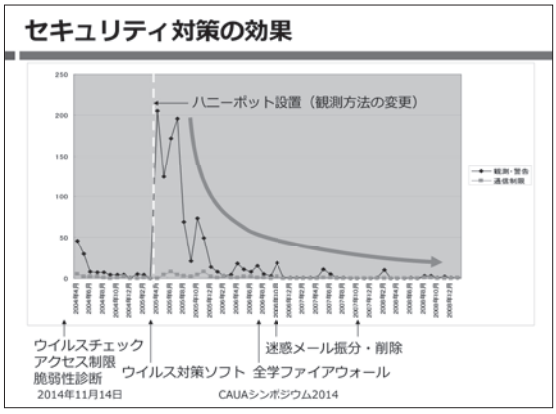

図 2　セキュリティ対策の効果

2. 大学のネットワークに求められるもの

大学には、高度で柔軟なキャンパスネットワークが求められる。これまでは、学部や学科、研究室単位でサブネットを運用し、好きなように使っていたが、ネットワークがライフライン化してくることにより、セキュリティインシデントが増えてきた。研究室は独立した企業と一緒であり、教授は社長や船頭に例えられることが多い。しかし、外部からは一

1　平成 26 年 5 月 1 日現在

つの組織として見られてしまうので、一人の先生が問題を起こすと、広島大学としての問題となってしまう。そして、トップや大学の経営陣からは、効率的に運用することを求められた。そのため、2007 年のネットワーク更新（HINET2007）では、管理方針を根本的に見直した。

3. HINET2007

HINET2007 では、中央にスイッチを置き、そこから放射線状にネットワークを展開している（図 3）。エッジには、利用者認証機能を持つスイッチを配置した。ポート数としては、14,000 ポートあり、このすべてのポートをメディアセンターが管理し、一人一人に対して割り当てていった。

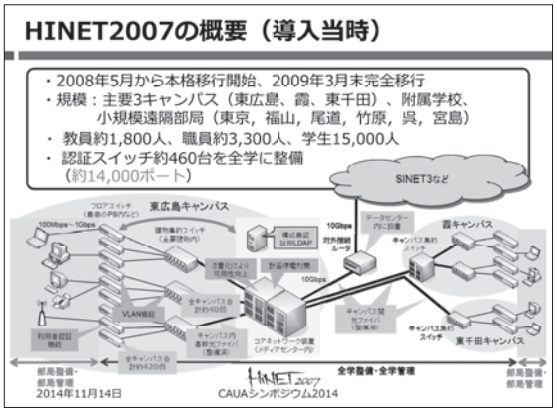

図 3　HINET2007 の概要

HINET2007 の特徴は大きく 4 つある。一つ目は、全学的な一元管理体制である。それまでは、ボランティアベースでそれぞれ管理を行っていたが、セキュリティインシデントへの対応がいい加減になったり、均一でなかったりしたため、各フロアに設置するスイッチまで全学で一元管理した。そして、そのための登録システムや申請システムを整備した。

二つ目は、すべての接続場所において利用者認証を要求したことである。多様な機器に対応するために Web/MAC アドレス認証を採用し、認証後はワイヤレートでの通信を必要とした。私は、1999 年から利用者認証を研究しており、NetSpring 社の FEREC[2] も製品化した。それを導入し、製品として運用、改善していくということも行った。

三つ目は、個別のファイアウォール機能を提供したことである。それぞれの研究室で完全に独立したネットワークを持てるように、約 2,000 人の教員それぞれにブロードバンドルータ相当のファイアウォールを提供した。その中は各自で管理してもらい、それ以外の見えない部分はセンターが中心になって管理した。これは当時注目されたが、最近でもよく導入されており、キャンパスネットワークの新しいカタチを提案できたのではないか。

最後は、VLAN による柔軟な仮想配線の提供である。当時、耐震改修が多く、研究室が変わることも多かった。そこで、異なる建物等に研究室が分散しても、一つの研究室として機能できるようにした。

ネットワーク上には、4 つのゾーンを作った。学外向けのサーバ接続用のグローバルゾーンと、学外と学内を仕切るファイアウォールゾーン、そして研究室とその外を仕切るローカルゾーン、無線 LAN 等をつなぐ公衆ゾーンである。

図 4 が構成である。大学のファイアウォールの下にファイアウォールゾーンがあり、さらにその下に約 2,000 の個別のファイアウォールがあり、研究室がある。そのため、同じネットワーク上でも、隣の研究室は見えない。学内で共有する情報は、学内で共通に見えるファイアウォールゾーンに置くように運用した。

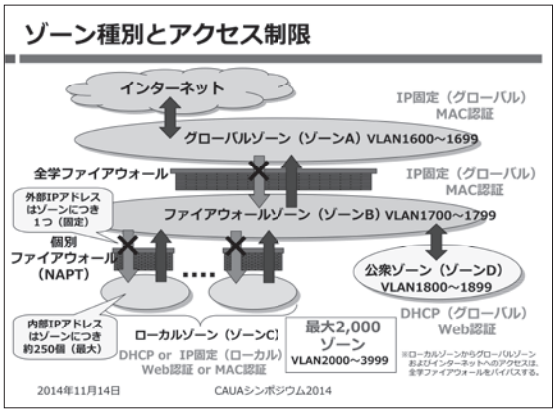

図 4　ゾーン種別とアクセス制限

利用者認証に関しては、それぞれのスイッチにサーバ証明書を入れ、そこに利用者は Web ブラウザでアクセスすることで認証を行った。ネットワーク機器やプリンターの場合は、事前に登録をした Mac アドレスで認証を行った（図 5）。

2　http://www.ferec.jp/

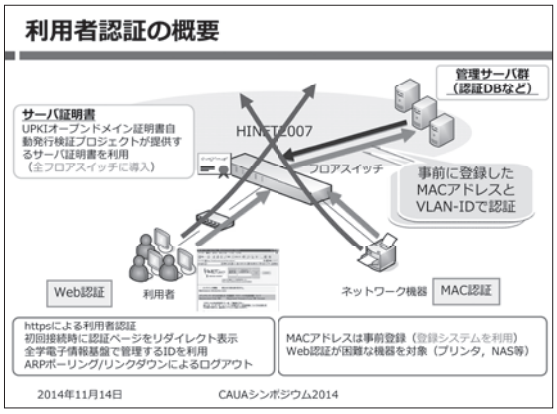

図５　利用者認証の概要

また、教育用端末へのログインには、二要素認証を取り入れた。電源を入れて OS を選択した後、学生証の IC カードをかざし、それに対応するユーザー ID とパスワードを入力しないと端末が使えないようにした。それまでは、ID とパスワードを人に貸すことが頻繁に行われていたが、学生証の ID カードに生協の電子マネーを入れたことにより、ID の貸し借りは無くなった。

広島大学では平成 26 年 8 月から、次期ネットワークシステムとなる HINET2014 の運用を開始している。HINET2014 では HINET2007 の特徴を継承しつつ、以下のような機能強化等を行っている。

- ゾーン A ホストに対するアクセス制御機能（ACL）の提供
- ゾーン C に接続可能な VPN（SSL）サービスの提供
- 不正侵入防止システム（IPS）の導入
- ゾーン C での IPv6 標準サポート

4.　情報セキュリティ教育の必須化

このような対策をしていく中で、セキュリティインシデントは少なくなったが、ゼロにはならなかった。文部科学省からの要請や、著作権等権利者団体等より著作権の侵害についての情報が寄せられたこともあり、大学として対策する必要があった。これまで、技術的、制度的な対策を行ってきたが、それだけではなく、構成員の意識や行動を根本的に変化させる必要があると考え、情報セキュリティ教育を必須化した。

まず、情報関係のガバナンスの再構築のため、情報メディア教育研究センターに情報セキュリティ研究部門が作られた。ここでは、情報セキュリティに関する研究開発や強化策の実施、そして、情報セキュリティとコンプライアンス教育の企画立案を行うことになった。

広島大学では、平成 23 年度から全学的に情報セキュリティコンプライアンス教育を始めた。フレッシュマン講習として、1 年生は大学のルールを知ってもらうためにも、座学の講義とオンラインテストを必須とした。

一方で問題なのは、2 年目以降の学生や教職員に対しての教育だった。そこで、フレッシュマン講習に対して、フォローアップ講習として、平成 24 年度から年に 1 回すべての構成員が受講することを義務付けた。翌年には、自分の 1 年間の活動や行動を振り返る意味での自己点検も行うようにした。

5.　フレッシュマン講習

フレッシュマン講習の対象者は、初めて広島大学にきた人である。例えば、過去に広島大学にいて座学を受けたことがある人が大学院生として再入学した場合には、座学は免除し、オンライン講座については毎年内容が変わるので、受けてもらうようにした。平成 25 年度の対象者は、座学が 3,350 名、オンラインは 4,559 名であった。

我々が重視したのは、外国からの留学生に対しての講習だった。平成 26 年 5 月現在、約 1,000 人の留学生が広島大学で学んでいる。50% 超が中国からの留学生である。残りの大部分は英語圏の国の留学生である。そのため、中国語と英語に対して、何らかの策を講じないと、1,000 人の留学生をカバーできない。

英語に関しては担当教員が資料を翻訳し、講習会も英語で実施しているが、中国語に関しては中国人留学生に学生アルバイトとして資料の翻訳と講習会での逐次通訳を担当してもらっている。講義資料の中には、講義の際に話すべきことをノートに全て書いている。それらもすべて翻訳することにより、研究室の中でセキュリティ教育が必要となった場合に、教員がその資料をダウンロードして内容の説明ができる。講習会でも、中国語での説明は、学生アルバイトに通訳をしてもらうが、その際にも、翻訳されたノートが役立っている。

座学の資料は約 50 ページで、代表的なトラブルの例としてウィルス感染の様子や情報

漏えいの様子をビデオで見せたり、ニュースで話題になった一般的なトラブルも例として掲載したりしている。また、広島大学で実際に起こったトラブルも例として紹介することにより、身の回りでも起こり得ることを認識してもらう。そして、なぜ広島大学は「ファイル共有ソフトウェア」の使用を禁止するのかなど説明して、個人がどのようなことに気をつけ、実践していくべきか、そして大学が実施している取組みを説明し、最後に、トラブルにあった場合は相談に来るようにと教えている。

講習会にどうしても参加できない人のためには、講義をビデオ撮影したものを提供し、受講率を上げた。話している先生を撮影し、音声は日本語のみであるが、講義の資料は3か国語を用意した。講習会ビデオで受講した学生にも、オンライン講座と試験を必須とした。

6. アカウントの年度更新

アカウントは、メディアセンターで発行しているが、それを使わずに部局のアドレスを使っている人もいるので、発行されているが使われていない遊休アカウントが多く存在していた。そのアカウントが脆弱性の元になる可能性があった。そのため、平成20年度からは毎年、アカウントの年度更新を行い、更新する意思表示を明確にさせている。それをしない場合は、アカウントをロックして、大部分のサービスを利用不可にした。

セキュリティ教育が始まるまでは、利用者が毎年春に利用規則へ同意するというボタンを押すだけだった。しかし、平成23年度からは、アカウント年度更新をするためには、フォローアップ講習を受けることを必須とした。平成25年度からは、さらに自己点検として、過去1年間の自らの行動を振り返る約20問のチェック項目を確認し、オンライン資料で知識の更新をして、確認テストに合格することで、アカウントの更新ができるようにした。2014年度は、対象の90%の約15,000人がオンライン講座と確認テストを受けて、アカウントを更新した。ここで更新されないアカウントについては、ロックしている。

7. 情報セキュリティインシデントの現状

2011年度からセキュリティ教育を始め、この4年間で、著作権侵害等のセキュリティインシデントは減少しているが、ゼロにはなっていない。逆に、最近増加傾向にあるのが、不正アクセスである。特に多いのが、アクティブメールを対象にしたフィッシングメールである。メールのログイン画面の大学ロゴと画面がそっくりに作られている。

広島大学の1日のファイアウォールのログは、約8GBにもなる。

ある脆弱性に対しての注意喚起がくると、4,500万行あるログの中から、該当のものを検索し、ターゲットになるアドレスを見つけて通信制限をかけることを都度行っている。サイバーセキュリティ基本法[3]が成立したので、通信のログを取得して、調査できることが組織としての責任となっている。一方で、ログは肥大化し、プライバシーの問題で組織間の連携は難しくなっている。そして、クラウドサービスを利用している場合はどうなるかが重要な問題となっている。

8. クラウドサービス利用ガイドラインの整備

クラウドサービスが出てくるまでは、メディアセンターが大学内の利用者に対してサービスを提供してきたので、「こういうサービスがほしい」と言われても、検討しますと答えていた。しかし、平成23年頃からクラウドサービスが増えてくると、「このサービスを使ってもいいか」と、学生や教職員から言われることが多くなった。「Dropboxに学生の情報を置いていいか？」、「サービスの良い使い方、悪い使い方を教えてほしい」という問い合わせもあった。そして、平成17年に作った、広島大学セキュリティポリシーとの整合性が取れなくなってきていた。

クラウドサービスの利用については、クラウド事業者に外部委託契約をすることになるが、クラウドサービスと一言でいっても、さまざまな定義がある。現時点ではクラウド事業者および使用するサービス内容に対する基準等が定められていない。

そこで、平成24年度の一年をかけて、クラウドサービス利用ガイドライン[4]を整備した。45項目のチェックリストを設け、利用

3 http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm

4 http://www.media.hiroshima-u.ac.jp/news/cloudguide/toppage

開始前に確認をするように推奨した。そして、インシデント発生時には、確認結果の提出を求められる場合があるとした。

2013 年に改訂・発行された、ISO/IEC 27001、ISO/IEC 27002 を受け、クラウドサービス利用のためのセキュリティマネジメントガイドライン [5] も修正されている。そして、クラウドコンピューティングにおける情報セキュリティの国際標準である ISO/IEC 27017 が 2015 年に発効する（図 6）。広島大学のクラウドサービス利用ガイドラインも、これらを盛り込んでいるので、クラウドサービスの提供者に確認すればそれに見合ったサービスを提供してもらえ、利用者側もこのガイドラインに沿って利用すれば、ISMS の基準を満たして、安心して使うことができる。

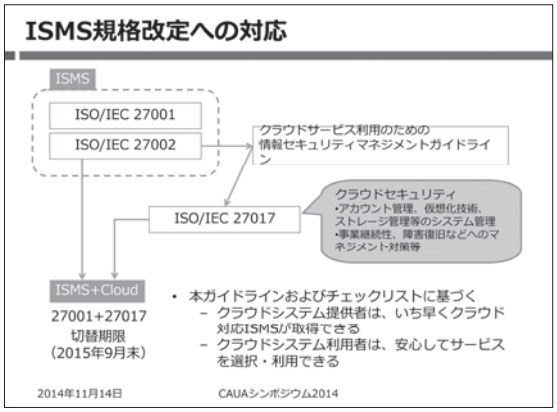

図 6　ISMS 規格改定への対応

9.　広島大学のクラウド化手順

クラウドサービスのガイドラインを整備した目的は、大学システムのクラウド化を進めることでもあった。このチェックリストがあることにより、運用上注意すべき点が明確になる。そして、オンプレミスでシステムを作った場合でも、同じように考えなければならず、担当者レベルで確認や判断ができるようになった。

これを受け、財務会計や人事システムといった、大学の中ではかなり機微な情報を持っていると思われるシステムが、真っ先にクラウド化された。国立大学法人で初めての財務会計システムのクラウド化である [6]。

5　http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf

6　http://www.benic.co.jp/release/20140203.html

さらに、人事労務システムや公式 Web サイト、事務用のメールシステムをパブリッククラウド化し、研究者総覧・研究力分析システムや学生・教職員用のメールも準備を進めている。このように、広島大学内の事務系システムが次々と外に出ていっている。

10.　ガイドライン策定の功罪

クラウドサービス利用ガイドライン策定の功罪を考えたい。一つは、確認すべきポイントが明確になったことである。それまでは、オンプレミスのシステムは安全で、外に出すことは不安だと漠然と思っていたが、実はそれは安全神話で、PDCA サイクルでチェックし、改善していくというサイクルが重要であることを再認識させられた。また、ポイントが明確になったことで、担当者レベルで確認できるようにもなった。しかし、危惧しているのは、定期的に再チェックするようにはなっていないため、安易なクラウド化を冗長するのではないかということである。今後見直すことも検討している。

もう一つは、システム構築手法を見直す契機になったことである。例えば、ハードウェアについては、4 ～ 5 年で新しいものと入れ替えていたが、クラウドサービスでは、必要な時に必要なものを使うことができる。大型システムの調達の際に、その性能をどう評価していくかも課題である。そして、ソフトウェアライセンスのクラウド上での利用について、制限がでてくるという問題もある。

11.　大学における情報セキュリティ対応の課題

これまでは、大学の計算機やネットワークインフラの整備や運用は、情報系のセンターが担っていた。大学側が情報環境を提供する立場であったが、PC の必携化や BYOD が進む中で、大学側が情報環境を提供する範囲が狭まっている。それは、ガバナンスを喪失する恐れがあるということだ。

そして、クラウドサービスが出てきたことにより、財政的なメリットを求める経営陣と便利さや手軽さを求める利用者からの圧力がかかってくる。計算機のリソースの調達方法も変わり、セキュリティポリシーとの折り合いをどうつけていくかという問題もあり、ここでもガバナンス喪失につながる恐れがある。

一方で、サイバーセキュリティ基本法にあるように、セキュリティに対する責任は増大傾向にある。そして、情報センターがクラウドサービス利用の可否判断を迫られるため、迅速かつ適切なインシデント対応が求められるが、果たして、ガバナンスを失いつつある状況で、本当にできるのだろうか。

2014年10月のサイエンティフィック・システム研究会[7]で、“溶け込んでいく情報”いわゆるビックデータをどう活用していくかをテーマにしたセミナーがあった。これまでは、とにかくデータを集めることに注力していたが、これからはまず何がしたいかがあり、その次に必要な技術を考えるべきだという。まさに、Seeds oriented から Needs oriented へ変わっていかなければならない。

そして、ビックデータは、気づきを見つけるためのものである。非日常的なところから気付きは出てくる。ロングテールデータとも言われる。メディアセンターに当てはめると、ログの活用が重要だということである。

クラウドサービスは、アップロードすること、つまり、データを集めるところは無料である。処理やデータを蓄積することも安価にできる。しかし、ダウンロードには課金がされる。クラウドサービスの事業者は、単にサービスをしているのではなく、データを集めて何かに使おうと考えているのだろう。我々も、それぞれの組織にあるさまざまなデータをきちんと処理し、うまく使う方法を考えるべきである。

12. 発生源処理の必要性

組織の中で集めた情報ソースを、他大学と一緒に連携して使うことになった時には、匿名化をし、暗号化する必要がある。現在は、すべてのデータを暗号化しないと外に出せないという風潮になっているように思える。発生源ですべてのデータを匿名化・暗号化するのは大きな負担であり、データの取りこぼしがあったり、大部分の不要なデータにコストをかけて非効率になったりしていることがあった。今後は、データをまず貯めて、その蓄積場所で必要な価値あるデータのみを処理して、匿名化・暗号化して、他大学と共有、連携していくことを考えたい（図7）。これには、組織横断的に実行できる仕組みが必要である。

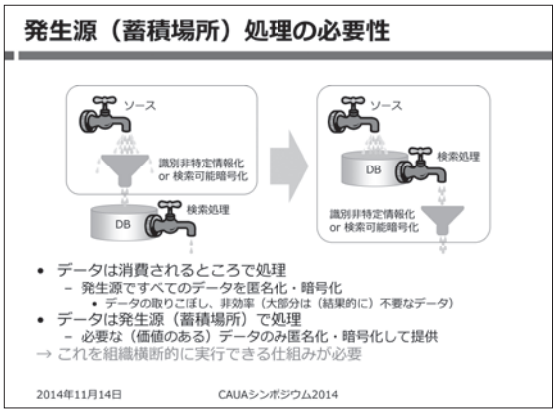

図7　発生源処理の必要性

7　http://www.ssken.gr.jp/MAINSITE/index.html