高知大学における情報システムの更新とセキュリティインシデント対応

石黒 克也 [1)], 佐々木 正人 [1)], 佐々 浩司 [1)], 山中 敏正 [2)]

1) 高知大学 学術情報基盤図書館
2) 高知大学 学術情報課

ishiguro@kochi-u.ac.jp

Update of The Information System and Response to Security Incidents at Kochi University

Katsuya Ishiguro [1)], Masato Sasaki [1)], Koji Sassa [1)], Toshimasa Yamanaka [2)]

1) Library and Information Technology, Kochi Univ.
2) Academic Information Division, Kochi Univ.

概要

高知大学では、2017 年度にネットワークシステムを含む全学情報システムの更新が行われた。これにより情報セキュリティインシデント発生時に、発生源となった機器やユーザの特定が容易になり、対応までの初動時間が短縮された。本稿では高知大学における情報システム更新の概要、およびセキュリティインシデント発生時の対応についての現状を報告する。

1 はじめに

高知大学（以下「本学」という）は、6 つの学部（人文社会科学部・教育学部・理工学部・医学部・農林海洋科学部・地域協働学部）および大学院から構成され、教職員数は約 1800 名、学生数は約 5000 名の規模の大学である。キャンパスは附属学校も含めると 5 つの地区（朝倉・物部・岡豊・小津・宇佐）に分かれて点在している。

本学では、2017 年度後半に全学で利用する情報システムおよびネットワークシステムの更新を実施した。更新されたものはメールシステムやグループウェア、認証システム、無線 LAN システムなど多岐に渡る。本稿では その中から情報セキュリティインシデント対応に関係するものをピックアップし、その概要を述べる。その後、それらを用いたインシデント発生時の対応について報告する。

2 情報システムの更新

システム更新の対象は各キャンパスで利用する情報システムおよびネットワークシステムである。更新されたもののうち、情報セキュリティインシデント発生時の対応に大きく関わってくるのがネットワークシステムである。そのため、まず今回のシステム更新において本学のネットワークがどのように変化したのか、その概要を示す。

2.1 更新前のネットワーク構成

図 1 はシステム更新前のネットワーク構成の概要である。

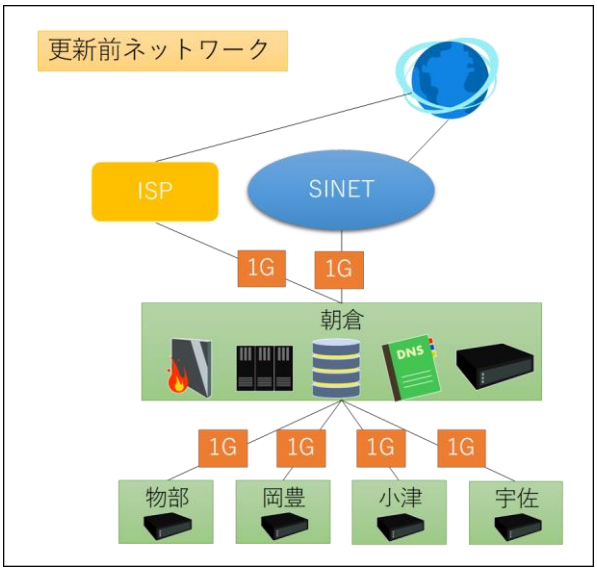

図 1 ネットワーク構成イメージ（システム更新前）

更新前のネットワークは、5 つのキャンパスのうち、本学本部のある朝倉キャンパスを中心に組み立てられているのが特徴で、メールシステムや DNS などサービス提供に必要となる主要なものが朝倉キャンパスに集まっている。そのため、他の 4 つのキャンパスのユーザがサービスを利用する際は学内ネットワークを通じて朝倉キャンパスに接続することになり、また学外のインターネットに接続する際にも朝倉キャンパスを経由して出ていく構成となっている。なお、メイン回線を SINET とし、バックアップ回線には ISP を利用していた。

2.2 更新後のネットワーク構成

次に更新後のネットワーク構成概要を示したのが図 2 である。今回の更新の特徴としては、

① 災害等発生時のための BCP 対策
② 上位接続の経路変更
③ ネットワークの集中管理

などがあげられる。

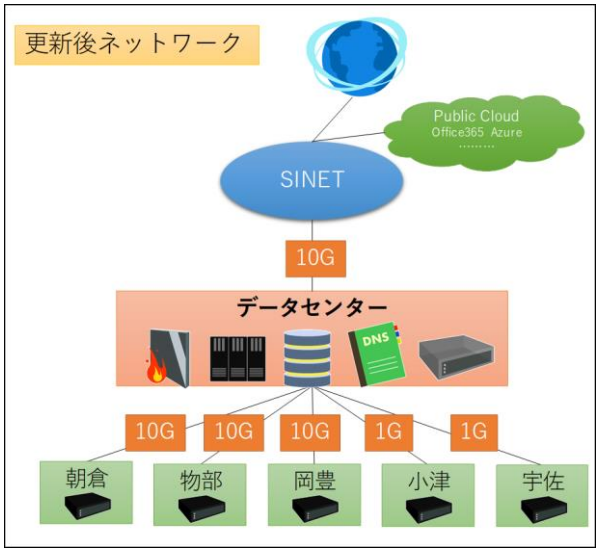

図 2 ネットワーク構成イメージ（システム更新後）

① BCP 対策

BCP 対策として、今回の更新によって主要な機器やサービスの学外への移行が実施された。これまで、主要サービスは朝倉キャンパスにある機器で提供されており、もし朝倉キャンパスが地震や水害などで被災すると大学のシステム全体が止まってしまう恐れのある状況であった。今回、メールシステムや DNS、認証システムなどを、データセンターやパブリッククラウドなどを利用して学外に移行したことにより、ユーザが ISP などのネットワークを利用すれば、朝倉キャンパスの状況に関係なくメール等のサービスを継続利用できるようになった。データセンターは災害に備えた堅牢な造りになっているため、更新前よりも被災時のサービスの復旧が迅速に可能となるはずである。また、本学には非常用自家発電装置がないため、これまで法定点検の停電時には大学のシステムが停止していたが、今後は学外から利用できるサービスは停電時にも継続して利用可能となった。

② 上位接続の経路変更

更新前の本学から上位のネットワークへの接続は、SINET をメイン回線とし、ISP をバックアップ回線として利用していた。しかしながら、SINET が非常に安定して運用されていることから、今回の更新により上位接続の経路を SINET のみとした。また利用者の多い朝倉・物部・岡豊の各キャンパスとデータセンター間をこれまでの 1G から 10G のネットワークに変更することにより、3 キャンパスのユーザは SINET まで 10G で直結されたネットワークを利用することが可能となった。

③ ネットワーク集中管理

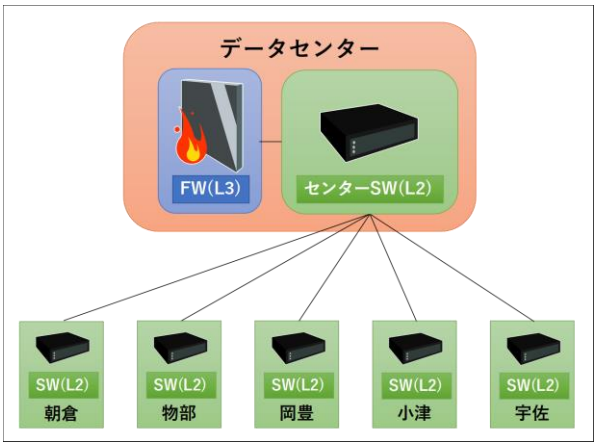

図 3 L2, L3 構成イメージ

本更新において、ネットワーク管理の中心的な役割を担っている機器が次世代ファイアウォール（L7 ファイアウォール）である。これをコア L3 スイッチとして利用し、その他のキャンパス内通信はすべて L2 ネットワークとすること

で、学内の通信がすべてファイアウォールに集約される構成となっている（図 3）。このような構成とした目的は、

- 学内通信の可視化
- 認証の連携
- セキュリティの強化

などである。

まず学内通信の可視化については、すべての通信をアプリケーション層の制御が可能なファイアウォールを通過させることにより、ネットワークを通して使用されているアプリケーションやコンテンツなどを把握することができるようになった。また、新情報システムではメールシステムを Office365 にするなどマイクロソフト社の製品を利用することが多くなり、それに伴い認証に AD(Active Directory)を利用する割合が増加した。さらに、更新と同時期に本学が NII(国立情報学研究所）の学術認証フェデレーションに加入したことにより、SAML(Security Assertion Markup Language)による認証も用いるようになった。これらの認証を次世代ファイアウォールと連携することにより、利用者の識別などが可能となっている。セキュリティの強化については、最新のセキュリティ機能を持った機器を利用していることのほかに、ファイアウォールや IDS(Intrusion Detection System)、IPS(Intrusion Prevention System)などの機能が一つに集約され、一元管理できるようになったことなども強化につながっている。

3 セキュリティインシデント対応

次に、本学において情報セキュリティインシデントが発生した場合に、新システムをどのように使って対応しているのかについて述べる。

3.1 CSIRT 体制

本学において情報セキュリティインシデントが発生した際に対応する部署は、情報セキュリティ委員会のもとに設置されている「高知大学 CSIRT(Computer Security Incident Response Team)」である。CSIRT のメンバーは

- CISO（Chief Information Security Officer 最高情報セキュリティ責任者）
- 学術情報基盤図書館教員
- 医学部附属医学情報センター教員
- 研究国際部学術情報課

から構成されており、業務内容は

- セキュリティインシデントへの対応
- 情報セキュリティに関する企画立案
- 情報セキュリティに関する啓発および指導

などが主なものである。

3.2 インシデント対応

本学で発生するセキュリティインシデントは、学内システムでの検知、ユーザからの通報のほかに、国立情報学研究所が提供する NII-SOCS（NII Security Operation Collaboration Services セキュリティ運用連携サービス）[1]に参加することにより送付されてくる警報メールなどを通じて CSIRT メンバーに知らされる。インシデントにより対応は異なるが、ここでは NII-SOCS から情報が提供された際の対応について記す。

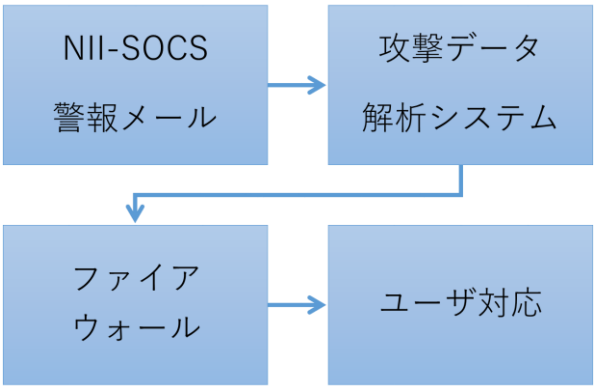

図 4 インシデント対応の流れ（NII-SOCS）

インシデント対応の大まかな流れは次のようなものである（図 4 参照）。

1). NII-SOCS からの警報メールを受信する。
2). NII-SOCS 攻撃データ解析システムのポータルサイトにログインし、警報の詳細を確認する。
3). 本学ファイアウォールにて NII-SOCS 警報の内容と一致するログを照合し、インシデント発生源の IP アドレスやユーザを特定する。また、必要に応じて通信を遮断する。
4). 該当 IP アドレス管理者、ユーザに連絡後、ヒアリング・機器調査などを実施し、状況に応じて対処する。

この一連の流れはインシデント発生時の一般的な対応と思われるが、システムが更新される前は上記 3)の作業に時間がかかることがあり、対

応が遅れてしまうこともあった。その理由は次のようなものである。

- ファイアウォール、IDS/IPS などが別々に分かれていたため、問題の通信がどこまで届いているのかわかりにくい場合がある。
- ログが上記のほかにプロキシーサーバや無線 LAN コントローラーなどにも存在し、幾つもの機器にまたがってログを調査する必要がある。

システムの更新後は学内ネットワークをファイアウォールで集中管理するようになったため、、IP アドレスやユーザ ID などの機器やユーザを特定するための情報の多くがファイアウォールに集約された。そのため、ほとんどの場合ファイアウォールのログのみから IP アドレスやユーザを特定することが可能となり、上記 3)にかかる時間が短縮された。その結果、より早く不正通信の遮断を行うことができるようになり、被害の拡大を防ぐことが可能となった。また、使用中のアプリケーションの情報もある程度得られるため、該当 IP アドレスを持つ機器がどのような通信を行っていたのかなどを把握しやすくなり、インシデントの詳細を掴むヒントとして役立っている。

3.3 課題

上記では NII-SOCS 警報メールへの対応を例としてあげたが、新システムへの移行後、本学で把握しているセキュリティインシデントの多くは NII-SOCS からの情報提供である。そのため、学内からの不正通信をいかに検知し、学外に出さずに処置できるかを考えることが今後の課題の一つとしてあげられる。このためには、本学のファイアウォールの機能をより活用できるよう、本学向けにカスタマイズするなどが必要になるものと思われる。

また、インシデントの発生時にどのように機器を調査し、どのように対応するのかについては、インシデントがケースバイケースであることがほとんどであるため担当者に依存してしまいがちである。そのため、調査方法および対応方法についてなるべく汎用的なマニュアルを作成し、担当者による違いを少なくする必要がある。本学の CSIRT は実動可能な人員が少なく、また人の入れ替わりも毎年のようにあるため、マニュアル作成は作業の効率化、および調査・対応漏れを防ぐセキュリティ強化の一環にもなり得ると考えられる。

インシデントの発生を防ぐことが困難な昨今では、大学所属員の情報リテラシーおよびセキュリティ意識を高めることがインシデントの発生件数を少なくする上で非常に重要である。現在、本学では CSIRT の活動として、学内構成員向けにセキュリティ講習やセキュリティ教育[2]などを毎年実施しており、参加者のセキュリティ意識は徐々に高くなっていると思われる。一方、大学間の国際交流などが盛んになるにつれて、大学には留学生や短期滞在研究員などの正規の所属員とは異なるものも増加している。このような短期滞在者にはネットワーク利用時の注意事項が十分には伝わってなく、利用している PC のマルウェア対策や脆弱性対応の不備があることも多い。そのため、本学でもしばしばインシデントの発生源となってしまっている。この例のような利用期間・時期がイレギュラーなユーザへの対応も今後の課題である。

4 おわりに

本稿では、まず 2017 年度に本学で実施された情報システムおよびネットワークシステムの更新について、特にセキュリティインシデント対応に関連する部分について概要を報告した。その後、NII-SOCS からの警報を例にしたインシデント対応の現状を報告し、そこから見えてきた課題についてまとめた。我々を取り巻く情報環境は日々変化しており、今後もセキュリティに関する脅威や要望はますます高まってくるものと予想される。それらに対応するため、今後はシステムの更新に加えて、ユーザのセキュリティ意識を高める活動にも注力していきたい。

参考文献

[1] NII-SOCS 、https://www.nii.ac.jp/service/nii-socs/、（2018 年 8 月 30 日閲覧）

[2] 佐々木正人、石黒克也、佐々浩司、「高知大学における情報セキュリティ教育の現状」、大学 ICT 推進協議会年次大会論文集 WF2-3、2017.