大阪大学のセキュリティに対する取組

笹尾　朋貴 1)

1)大阪大学　情報推進部

odins-room@odins.osaka-u.ac.jp

Security Approach at Osaka University

Tomoki Sasao1)

1) Department of Information and Communications Technology Services, Osaka Univ.

概要

大阪大学は、人文系、理工学系から医学・歯学に至るまで 11 学部・16 研究科を擁し、3,200 人を超える教員の下、23,000 人以上の学生が学業・研究に取り組む総合大学である。セキュリティ強化においては、情報セキュリティ対策基準や実施手順等を策定し、CSIRT 体制の整備や脆弱性診断の実施等に取り組んでいる。本稿では、こうした本学でのセキュリティに対する取り組みについて紹介する。

1　はじめに

大阪大学のキャンパスネットワークを運用する大阪大学総合情報通信システム（Osaka Daigaku Information Network System: ODINS）では、2019 年 5 月現在で教職員 10,407 人、学生 23,316 人を抱える大学の教育研究活動を支えている[1]。ODINS ではネットワークインフラに関する環境整備だけではなく、セキュリティ機器の運用や学内のサーバ管理者等を対象とした情報処理技術向上を目的とする講習会を開催し、ネットワークを安全に保つための取り組みを行っている[2]。

セキュリティ強化においては、情報セキュリティ対策基準等の規程や実施手順を策定し、セキュリティ対策の整備を進めてきた。しかし、各種サーバの不具合・脆弱性や管理者の設定間違いなどを悪用したウィルスやワーム、不正アクセス等の危険性は継続している。また、2019 年版情報セキュリティ 10 大脅威では、標的型攻撃やビジネスメール詐欺による脅威がランキングの上位を占めるなど、構成員一人一人のセキュリティリテラシーの向上がますます求められている。

このような情勢の中、2017 年に本学の情報システムが不正アクセスを受け、管理者 ID を含む最大 8 万 1107 件の個人情報が漏洩した可能性があるセキュリティインシデントが発生し、さらなるセキュリティ体制の強化に取り組むこととなった。本学のセキュリティインシデントの推移は図 1 のとおりであり、セキュリティインシデント発生件数は減少傾向にある。

本稿では、大阪大学が取り組んでいる脆弱性診断サービスをはじめとしたセキュリティ対策について、セキュリティインシデントを予防する事前対策とセキュリティインシデント発生時の事後対策のそれぞれに関する取り組みを紹介する。

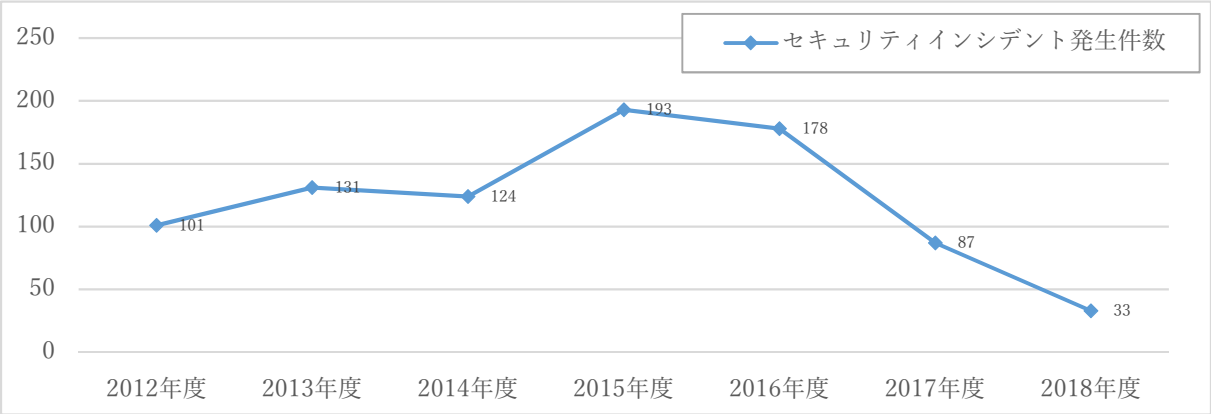

図1：セキュリティインシデントの推移

2　セキュリティ対策の変遷

前述した 2017 年の不正アクセスで表面化した課題は次のとおりである。

【事前対策における課題】
① 構成員のセキュリティリテラシーが十分でないこと
② 脆弱性を有する機器が適切に対処されていないこと
③ 悪意のある web サイトへのアクセス制限が十分にできていないこと
【事後対策における課題】
④ セキュリティ体制についてガバナンスが効かなかったこと

これら各課題について、改善に向けて取り組んだ内容を本項では紹介する。

2.1 事前対策

2.1.1 セキュリティ研修

本学におけるセキュリティリスクとしては、メールの添付ファイルの不用意な解凍、メール送信時の宛先設定や添付ファイルの間違い、ソフトウェアの脆弱性未対応といった、構成員各個人の理解不足や不注意に起因するものが依然として多い。また、脅威の手口が巧妙化していく中で、インシデント発生時の被害を最小限にとどめるためには、情報セキュリティに関する教育や訓練をより効果的に、定期的に実施することが重要である。

そこで、従来からあった全教職員向け情報セキュリティ研修に加え、あらたに標的型メール攻撃への対処訓練を目的とした「標的型メール攻撃訓練」、部局情報セキュリティ責任者の責務を理解いただくことを目的とした「管理職向け情報セキュリティ研修」、学生のセキュリティ意識向上を目的とした「学生向け情報セキュリティ研修」を実施している。現在実施している研修を表 1 に示す。e-learning の受講率は図 2 のとおり。

また、各種研修の受講率向上に向けては、各部局のセキュリティ責任者に受講率を報告し未受講者に受講を促すよう通知しているほか、期間内に受講しなかった者は大阪大学個人 ID の利用を制限するなどした結果、教職員向け研修（e-learning）については 100%近い受講率を達成している。

表 1：セキュリティ研修一覧

研修名	対象者	内容
管理職向け集合研修	部局長等の管理職	部局情報セキュリティ責任者及び管理職が、セキュリティ上の脅威や管理体制上の責務について認識を深める。
新任教員研究員向け研修	新任教員 新任研究員	新任の教員や研究員に対し、本学の情報セキュリティポリシーについて解説し、必要な対策や手続きが実践できるようにする。
サーバ管理者向け集合研修	サーバ管理者	Web サーバや DNS サーバ等の安全な構築・運用について実機を用いた講習を実施している。近年は各種サーバのログ解析の方法について開催した。
標的型メール攻撃訓練	全教職員	標的型メール攻撃を理解し、正しい対応ができるよう、教育資料を配布するとともに、年に複数回疑似攻撃メールによる訓練を実施。
e-learning 及び自己点検	全教職員 及び学生	構成員一人ひとりの情報セキュリティ意識向上のため、また役割に応じて必要な対策の実践について自己点検を実施。

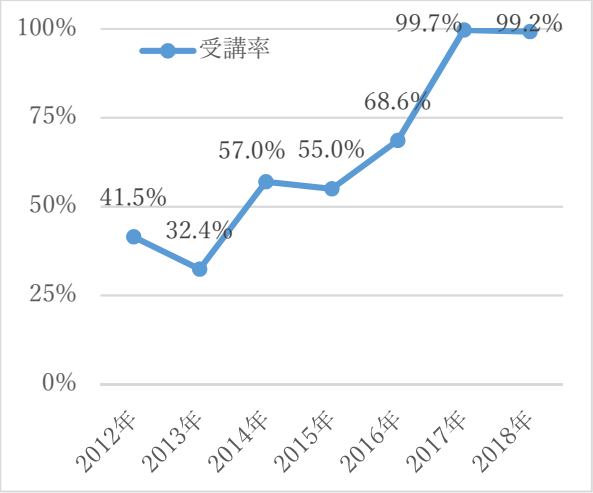

図 2：e-learning の受講率（教職員）
※小数点 1 位以下四捨五入

2.1.2 脆弱性診断

セキュリティ対策の一つとして、ネットワークに接続している情報システムの脆弱性を診断により発見し、それを改善することでセキュリティ水準を向上できることは広く知られている。脆弱

性診断には、自組織で診断可能な診断ツールを用意して実施する方法と、外部企業が提供する診断サービスの利用が選択できる。大阪大学では、2005年から外部企業が提供する診断サービスを利用しており、1 回/2 年の頻度で学内すべてのグローバルIPアドレスを対象とした脆弱性診断を実施していた。

しかしながら、各種サーバ等が抱える脆弱性は日々新たなものが発見され、その対応には即時性が求められる。そこで、従来の脆弱性診断に加えて、自組織で診断可能な診断ツール「Tenable.io」及び「wpscan」を導入した。

さらにこれまで学内のホストのみを対象としていた脆弱性診断を、学外のホスティングサーバも含めた対象に拡大することとした。これは、ホスティングサーバにおいて web 改ざんが発生したことに起因する。なお、対象となるサーバは各部局からの申請に加えて、検索エンジン「SHODAN」を用いて osaka-u.ac.jp ドメインを有するサーバを抽出し、診断漏れを防いでいる。

診断結果は各部局のセキュリティ担当者へメールにより通知し、検出されたリスク度に応じて対応期限を定め、期限内での対策を厳守している。定期的に脆弱性診断及びその対応を実施した結果、図 3 のとおり脆弱性件数が減少していることを確認している。

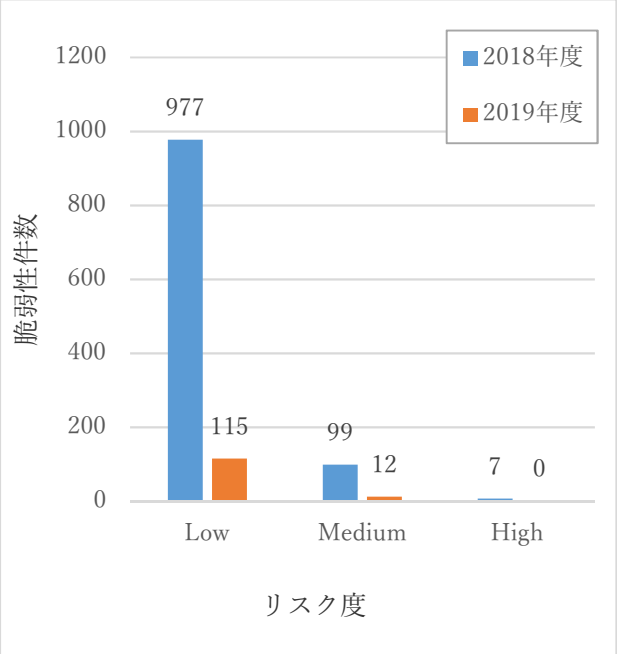

図 3：脆弱性件数の推移

2.1.3 アクセス制限

ODINS が有するセキュリティ機器として、迷惑メール対策装置、ネットワーク侵入防止装置（Intrusion Prevention System: IPS）、ネットワーク侵入検知装置（Intrusion Detection System: IDS）、及びDDoS攻撃対策システム[3]がある。図4にODINS のネットワーク論理構成を示す。

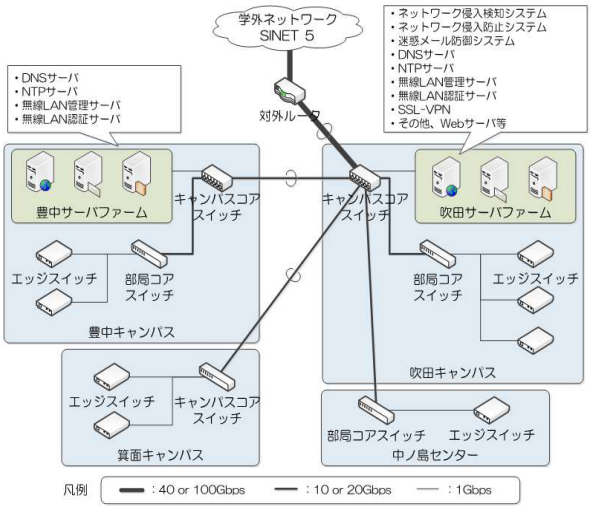

図4：ODINS ネットワーク論理構成図

IPS では、指定したIPアドレスを持つ機器に対するアクセス制限を行っていたが、IPアドレスの詐称や1つのURLに対して複数のIPアドレスを有する機器を用いた手口が増加するに伴い、期待する効果が見込めない状況であった。

そこで、新たにWEBフィルタリングを導入し、表2の3パターンでアクセス制限を実施している。

表2：WEBフィルタリングによるアクセス制限

①	Palo Alto社のデータベースに「Command and Control」、「Malware」、「Phishing」のいずれかで登録されたURL
②	JPCERT/CC等の外部からの注意喚起に基づくURL
③	学内からの通報に基づくURL

WEBフィルタリングの導入により、毎月10万件以上のアクセスをブロックすることに成功している。図5にブロックの推移を示す。

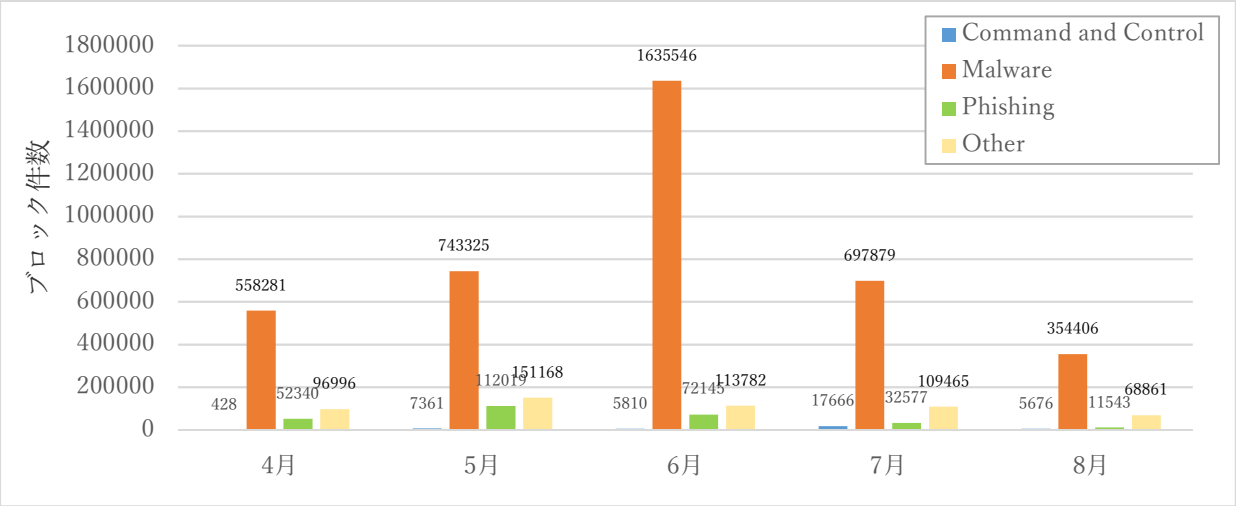

図5：アクセスブロックの推移

2.2 事後対策

2.2.1 組織体制

大阪大学では、情報セキュリティの維持及び向上に関し必要な事項について定められた大阪大学情報セキュリティ対策規程をはじめとする諸規定等に準じて組織体制を整えている。特に、情報セキュリティインシデントが発生した際に緊急対応としてネットワーク回線の遮断等が必要となる場合は、本規程に定められた大阪大学CERTによる判断を経た上で実施していた。

情報セキュリティインシデントについては、外部のSOCサービスを活用しており、本部がまずSOCサービスから通知を受け、対象となる機器を特定し、該当する部局のネットワーク担当者へ連絡、そしてネットワーク担当者から機器管理者へ対応を依頼するというフローでインシデント対応を行ってきた。

しかし、増加するセキュリティインシデントに対応するためにセキュリティ体制の一層の強化が必要となった。さらに、お盆や正月等の長期休暇、及び夜間帯におけるセキュリティインシデント発生件数が増加傾向にあり、これまでサーバ管理者不在時に放置されていたセキュリティインシデントへの即時対応が求められている状況にあった。

そこで、情報セキュリティ体制をより強固にするため、情報セキュリティ本部を設置し、本学の情報セキュリティインシデント対応を取りまとめる「本部CSIRT」、及び各部局内の情報セキュリティインシデント対応を担当する「部局CSIRT」を立ち上げることにより、セキュリティインシデントへの即時対応が可能な体制を整備した。また、各CSIRT担当者の負担軽減とセキュリティ強化を両立するため、土日祝日・平日夜間帯のセキュリティ業務を外部委託することとなった。新体制のセキュリティインシデントフローは図6のとおり。

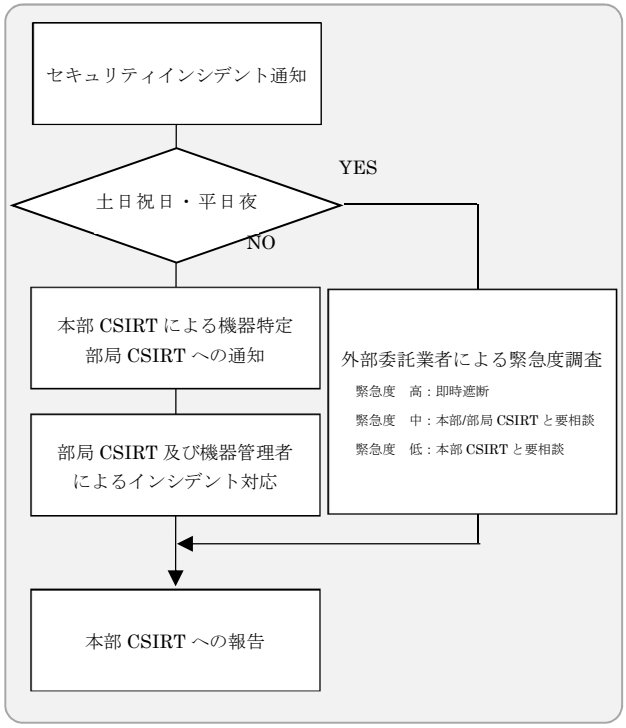

図 6：セキュリティインシデントフロー概略図

3　評価

3.1 セキュリティ研修

教職員向け研修（e-learning）は、未受講者に大阪大学個人IDの利用を制限する等を実施した結果、受講率は100%近くに達することができた。他方、2018年度から開始した学生向け研修（e-learning）の受講率は21%に留まったため、受講率向上に向けては、各部局のセキュリティ責任者へのより一層の受講を要請しており、今後、その状況を確認の上、必要に応じて施策を検討する。

3.2 脆弱性診断

自組織で診断可能な診断ツール「Tenable.io」及び「wpscan」による定期的な脆弱性診断結果を評価するにあたり、外部企業が提供する診断サービスによる脆弱性診断結果を図 7 に示す。なお、2016 年度までは 1 回/2 年の頻度で学内すべてのグローバル IP アドレスを対象に脆弱性診断を実施していたため、その合算値としている。

大きく変化したのはリスク度 Medium、Low と判断された脆弱性が減少したことである。これは診断ツールによる結果のうちリスク度 Low までのすべての改善を要請したことが大きく貢献している。

一方でリスク度 High については横ばいの結果となった。これは自動的に診断するツールでは発見できない脆弱性の存在が 1 つの要因であり、今後も外部企業が提供する診断サービスの継続利用を検討している。

3.3 アクセス制限

WEB フィルタリングの導入により、毎月 10 万件以上のアクセスをブロックすることに成功し、一定の効果が得られた。

一方、ブロックログを確認すると、1 つの端末から大量に、または定期的にブロック先の URL にアクセスしていることが確認できた。そのような挙動をする端末はマルウェア感染が疑われるため、必要に応じて所有者にウィルスチェック等の要請を行っていく。

3.4 組織体制

新たに立ち上げた情報セキュリティ本部により、セキュリティインシデント発生時には本部 CSIRT と部局 CSIRT が連携し、セキュリティインシデントへの即時対応を実現できている。

他方で、土日祝日・平日夜間帯のセキュリティ業務の外部委託については、セキュリティインシデントの種別や対象とする機器に応じた判断（通信遮断の可否や機器管理者への委任可否等）が必要となるため、状況に応じて外部委託業者と本部 CSIRT 間で意思疎通を図り対応している。今後は、本来の目的である CSIRT 担当者の負担軽減の推進

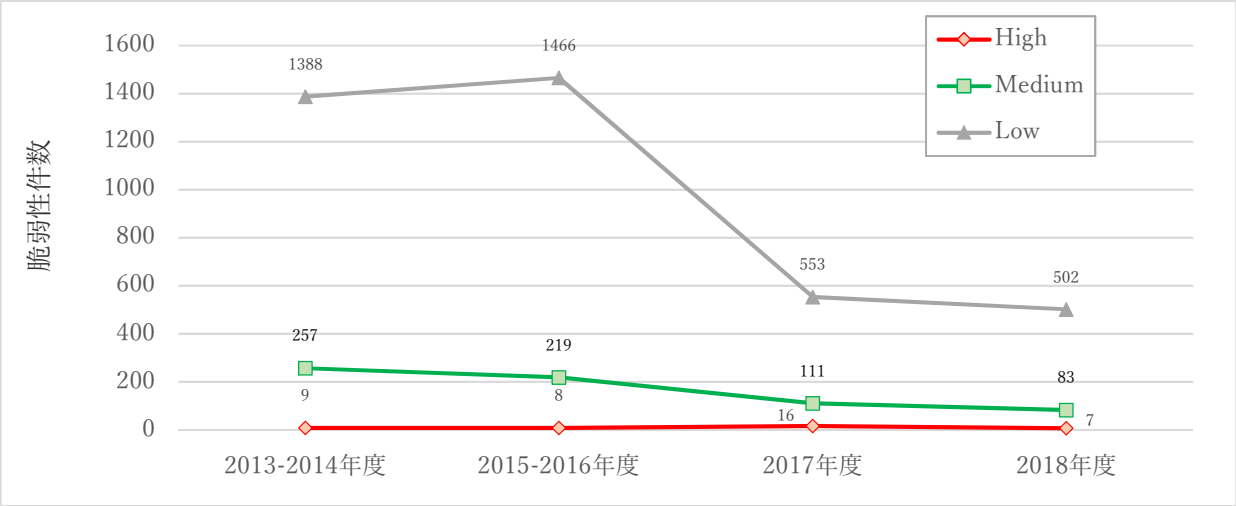

図 7：外部企業が提供する診断サービスによる脆弱性診断結果

に向けて、外部委託業者のみの判断でセキュリティインシデント対応を可能とするような基準策定を進める。

4　今後の取組

本項ではこれまで紹介した取り組みのほか、新たに取り組んでいることについて簡単に紹介する。

4.1 プライベート空間の集約

情報資産の管理はセキュリティの基本であるが、各部局にプライベート空間が構築されている環境ではシステム的に把握することが困難であった。そのため、Excelベースの情報資産管理を行っているが、人的負担が大きく、また記入漏れ・更新漏れが散見される状況にある。そこで、新たにイントラネットワークを構築し、各部局のプライベート空間からの移行を進めている。

4.2 エンドポイントセキュリティの導入

教育・研究上の機微情報や個人情報等、真に保護すべき情報を保有する機器において、既知のマルウェアの侵入や実行を防止するウィルス対策ソフトだけでは、ゼロデイ攻撃に対応できない状況にある。

そこで、機微情報を扱う機器に次世代型エンドポイントセキュリティシステムを導入し、ゼロデイ攻撃をはじめとしたサイバー攻撃の阻止に努めている。また、マルウェア情報やログ情報を一括管理することにより、侵入された後の感染経路特定や、影響範囲の分析に活用している。

5　まとめ

本稿では、大阪大学におけるセキュリティへの取り組みと課題について紹介した。セキュリティに対する予算が限られている中、年々高度な対応を求められることが増加しており、対応にはさらなる工夫が必要である。現実的な対応を導き出すために、関係各位の広い見識を頂ければ幸いである。

参考文献

[1] 大阪大学プロフィール（https://www.osaka-.ac.jp/ja/guide/about/profile/profile2019），pp.4-4，2019.

[2] 原口直大，南吉英，大阪大学におけるネットワーク環境の構築とその運用，大学 ICT 推進協議会 2013 年度年次大会論文集 W1E-5，pp.1-1，2013.

[3] 原口直大，キャンパスネットワークに対する SMTP Flood による DDoS 攻撃への対策と効果，大学 ICT 推進協議会 2016 度年次大会論文集 WE24，pp.2-6，2016.