# 大学が講じるべき情報セキュリティ対策
## -同志社大学の取り組み事例を踏まえて-

田村 祐司 [1)], 井部 力也 [1)], 土佐 卓司 [1)], 今西 覚 [1)], 原 真一 [1)]

1）同志社大学 情報化推進部

yujtamur@mail.doshisha.ac.jp

# Information Security Required of Universities
## -Based on the Case Study of Doshisha University-

Yuji Tamura [1)], Rikiya Ibe [1)], Takuji Tosa [1)], Satoru Imanishi [1)], Shinichi Hara [1)]

1) Division of ICT Promotion, Doshisha Univ.

概要

生成 AI やクラウド技術の普及により、サイバー攻撃は巧妙になり、その件数も増加している。こうした外部環境を前提に、大学においても情報セキュリティ対策の全体像を見直す必要がある。本稿では、同志社大学における取り組みと課題を例として、大学として講じるべき情報セキュリティ対策の具体的な施策について考察する。

## 1 はじめに

近年の生成 AI やクラウド技術の急速な普及により、組織、個人を問わず、多様かつ高度な IT サービスが自由に利用できるようになった。大学においても、教育・研究・事務を問わず、こうしたサービスを利用する機会が増えている。

一方で、こうした技術の進歩には負の側面も存在する。たとえば、RaaS（Ransomware as a Service）やMaaS（Malware as a Service）のようなサービスが登場し、サイバー攻撃者は、より容易かつ安価にサイバー攻撃を仕掛けられるようになっている。また、生成 AI の普及により、標的型攻撃やソーシャルエンジニアリング、偽情報といった脅威が拡大している[1]。2023年の調査によると、米国では 2022 年末の ChatGPT 公開以降、標的型攻撃メールは1年間で 1265％増加し、資格情報窃取攻撃は 967％増加したとされている[2]。

他方で、情報セキュリティ上の脅威の種別という観点で調べてみると、こちらには大きな変化がないことが分かる。独立行政法人情報処理推進機構（以下、IPA という）が公開している「情報セキュリティ 10 大脅威2025」[3]によると、最も影響が大きい脅威は、“ランサムウェア攻撃による被害”とされており、10 年間ランクインし続けている。2位以下の脅威を見ても同様の傾向があり、同資料で挙げられている 10 個の脅威のうち 9 個が、5年以上連続で選出されている脅威種別である。

また、「大学等におけるサイバーセキュリティ対策等の継続的な取組について（通知）」（6 文科高第 1551 号）では、大学等においては、情報セキュリティインシデントの半数近くが、基本的な情報セキュリティ対策の未実施や意識の欠如に起因していることが指摘されており、人為的なミス、抜け漏れのない組織体制をどのように構築・維持していくのかという点が課題となっている[4]。

これらの資料から、生成 AI やクラウド技術が普及した現在においても、情報セキュリティ対策として求められる施策に大きな変化は無い一方で、サイバー攻撃の巧妙化や増加傾向から、基本的な情報セキュリティ対策を抜け漏れなく、確実に実施することがより重要になってきていると考えられる。

本稿では、こうした情報セキュリティを取り巻く外部環境（以下、情報セキュリティ環境）の中で、同志社大学が実施している情報セキュリティ対策を事例に挙げながら、大学がどのような情報セキュリティ対策を講じるべきかについて検討する。また、本稿においては、技術的な対策やセキュリティツールについては可能な限り触れないこととし、大学の予算規模や専門知識の有無に関わらず、多くの大学で実施可能と考えられる取り組みに焦点を絞って考察する。

## 2 情報セキュリティ対策方針の可視化

### 2.1 情報セキュリティポリシーの整備

大学に限らず、組織における情報セキュリティ対策の根幹となるのが、情報セキュリティポリシー（以下、ポリシー）である。情報セキュリティ対策の基本方針を示す上位規程だけでなく、対策基準や各種対応手順、ガイドラインなどの下位規程についても、しっかりと規定しておくことが重要である。下位規程まで詳細に明文化しておくことで、情報セキュリティインシデント（以下、インシデント）発生時にも、迅速かつ適切に対応することが可能となる。

本学においても、2008年に『同志社大学情報セキュリティポリシー』を制定している。図 1 の通り、最上位の基本方針（Layer1）として『同志社大学情報セキュリティ基本規程』を置き、その下に7本の実施規程・対策基準（Layer2）、18本の手順書・ガイドライン（Layer3）を制定している。また、Layer1 から Layer3 までの規程類は、学生を含め、本学の全構成員に公開している。

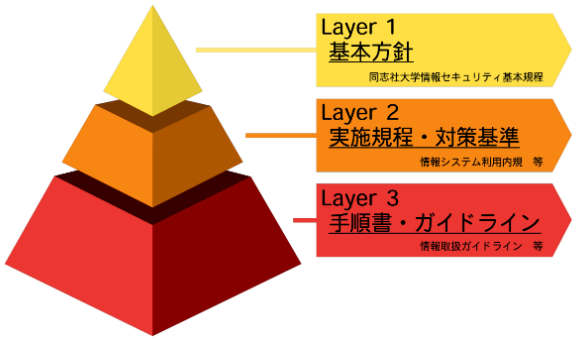


図 1：同志社大学情報セキュリティポリシー構造図

また、ポリシーの整備にあたって最も重要な点は、情報セキュリティ環境の変化に伴って内容が陳腐化しないよう、継続的なメンテナンスを行うことである。本学においては、『同志社大学情報セキュリティ基本規程』だけで、11回の改正を行っており、2008 年の制定から、絶えず情報セキュリティ環境の変化に対応し続けている。

### 2.2 情報セキュリティ環境の把握

組織の情報セキュリティ対策方針を検討するにあたっては、その前提となる情報セキュリティ環境を把握しておくことも必要である。情報セキュリティ環境を適切に把握することで、資金や人材を効率的に投下することが可能となり、より効果的な情報セキュリティ対策基本計画の策定にも繋がる。

本学では、前述したとおり情報セキュリティ環境を分析・把握しており、現時点では新たな脅威が生じているわけではなく、標的型攻撃メールや資格情報窃取攻撃を中心に、サイバー攻撃の件数が増加し、巧妙化している状況だと認識している。こうした環境下では、インシデントの発生を防ぎ切ることは難しく、事後対応も含めた情報セキュリティ対策がより重要になると考えている。

### 2.3 情報セキュリティ対策基本計画

情報セキュリティ対策に関して、新たな施策を実施するには多くのリソースが必要となるため、予め計画性をもって実行する必要がある。また、施策が場当たりにならぬよう、組織として体系的に情報

セキュリティ対策を実施するための計画が必要である。これらの施策を具体的に記載したものが、情報セキュリティ対策基本計画である。

本学における情報セキュリティ対策基本計画は、情報セキュリティ対策の中期的な活動方針を示すもので、情報セキュリティ環境を踏まえ、今後4年間で実施する取り組みについて、時系列で示した計画書となる。なお、本稿で取り上げている各施策についても、情報セキュリティ対策基本計画において明記されたものである。

## 3 情報セキュリティ対策体制の整備

### 3.1 内部統制体制の整備

情報セキュリティ対策においては、CISOや情報システム部門による内部統制が効く体制を構築する必要がある。特に事務職員については、業務の中で個人情報や情報システムを扱う場面が多く、より徹底した内部統制が求められる。

図2は、本学の情報セキュリティ対策にかかる内部統制体制図である。CISO、CISOO、学部等CISO、学部等 CISOO、情報セキュリティ監査責任者、セキュリティアドバイザーについては、それぞれの役割や責任範囲について、基本規程において規定している。

また、全ての部署は必ずシステム担当者を置くこととしており、システム担当者の役割も含めて、Layer3 において規定している。具体的には、各部署での情報資産の適切な管理や ICT 化の推進、システム担当者会への参加といった役割を求めている。システム担当者会とは、情報セキュリティに関する重要事項の通達、新しいシステム・サービスの利用説明など、広く ICT に関わる内容について周知を行う事務職員向け会議である。不定期ながら年間10 回程度、情報システム部門の主催で開催しており、事務職員への内部統制強化に繋がっている。

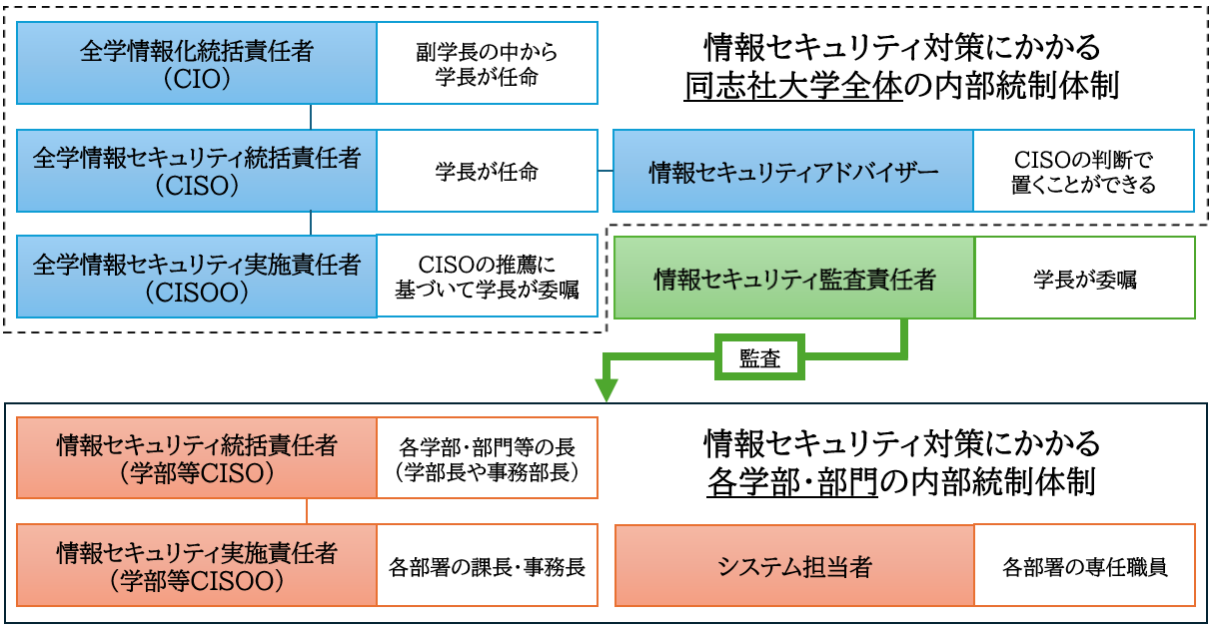


図 2：同志社大学の情報セキュリティ対策にかかる内部統制

### 3.2 CSIRT 体制の整備

インシデント発生時には、CSIRTの発足が必要となる。CSIRTについては、予めメンバーを定め、ポリシーに規定しておくことが望ましい。

本学における CSIRT のメンバー構成などについては、Layer2 で規定している。CSIRT については、インシデント発生時の迅速な対応が求められることから、本学では、業務用グループウェアを使って CSIRT の構成メンバーが全員含まれるグ

ループを常設しており、インシデントの恐れがあると判断した場合には、グループウェア上で第一報を CSIRT メンバー全員に通知するという運用をとっている。

また、インシデント発生時の一般的な対応手順については、Layer3で規定しており、手順に従って対応を進めることとなる。しかしながら、文字情報が多く、手順が分かりにくいという課題や、個人情報漏洩時などの個別対応手順については、整備が不十分であるという課題を認識している。

そのほかの課題として、CSIRT の特性上、広報部門をはじめとした他部署の事務職員もメンバーとして入るため、CSIRT メンバーを対象としたインシデント対応訓練などの教育についても必要性を感じている。

### 3.3 全体像の把握

自組織の情報セキュリティマネジメントを考える上では、情報セキュリティ対策に関する PDCA サイクルを適切に把握し、情報セキュリティ対策の総合的強化を図っていくことが有効となる。同様の取り組みは、政府機関等でも行われている[5]。また、インシデントの発生を前提とした情報セキュリティ対策体制の全体像を把握しておくことは、迅速かつ適切なインシデント対応に直結する。

図 3 は、本稿で取り上げる本学の施策について、情報セキュリティ対策の全体像として図示したものである。自組織の情報セキュリティ対策に関する全体像を把握する際には、一度現在の状態を可視化しておくと、現時点で出来ていることと不足していることが認識しやすくなり、適切な情報セキュリティ対策体制の整備に繋がる。

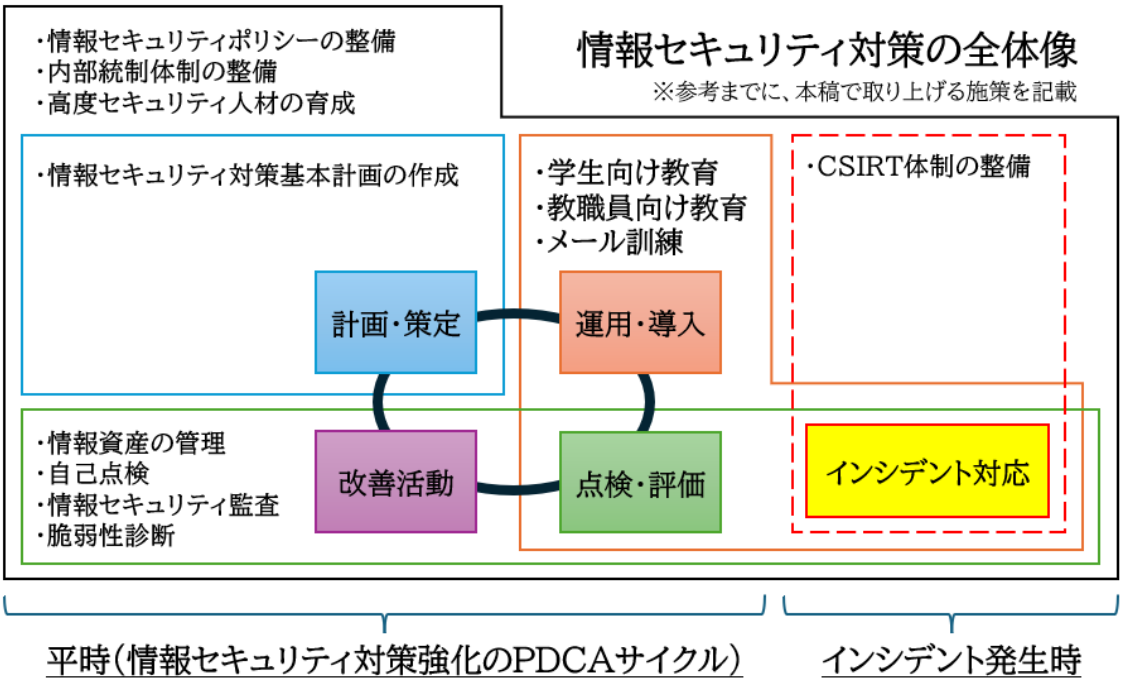


図 3：情報セキュリティ対策全体像の可視化

## 4 IT リテラシー教育と人材育成

### 4.1 学生向け教育

多くの大学において構成員として最も多いのは学生であり、学生の IT リテラシー向上についても大学として取り組むべき課題となる。

本学では、学生の IT リテラシー向上を目的として講習を行うことを Layer2 で規定しており、学生向けの IT リテラシー教育コンテンツとして、e-learning 形式で、テキストとテストを用意し、全

新入生を対象として受講を必須としている。テストは何度でも受験可能だが、入学後1か月以内に合格点を取れなかった学生については、IT リテラシーが不足していると判断し、合格点に達するまで電子メールを含めた一部の IT サービスの利用権限を停止している。

なお、テスト問題はパッケージを利用しているが、IPA が実施する IT パスポート試験で問われる程度の難易度に設定しており、制限時間 30 分で、4択問題を 20 問出題している。正答率 80%以上で合格となる。

当該テストの各年度における5月30日時点での受験状況を示しているのが表 1 である。サービスの利用制限もあってか、合格率が極めて高い水準で、ほとんど変動なく推移していることが分かる。他方で、平均受験回数とテキスト閲覧率が共に低下傾向にあり、わずかな受験回数で、テキストを読むことなくテストに合格する新入生が増えているようである。入学前から一定の IT リテラシーを備えた学生が増えてきているようにも見えるため、今後の教育内容を検討するうえでも、受験状況の推移を注視していきたいと考えている。

表 1:4月入学者の受験状況（各年度 5 月 30 日時点）

| | 2021年度 | 2022年度 | 2023年度 | 2024年度 | 2025年度 |
|---|---|---|---|---|---|
| 受験対象者数（人） | 7,080 | 7,311 | 7,397 | 7,263 | 7,463 |
| 合格者数（人） | 6,980 | 7,217 | 7,312 | 7,146 | 7,318 |
| 未合格者数（人） | 100 | 94 | 85 | 117 | 145 |
| 合格率（%） | 98.59 | 98.71 | 98.85 | 98.39 | 98.06 |
| 受験回数の平均（回/人） | 1.68 | 1.62 | 1.86 | 1.52 | 1.44 |
| テキスト閲覧率（%） | 72.47 | 67.31 | 66.34 | 66.27 | 65.68 |

4.2 教職員向け教育

教職員におけるITリテラシーの底上げは、インシデント発生の防止や、インシデント発生時の適切な対応に繋がる。昨今の情報セキュリティ環境からも、IT リテラシーの底上げは急務であり、重要度が増していると言える。

本学では、全教職員の IT リテラシー向上を目的として講習を行うことを、学生と同様、Layer2 で規定している。

定期的な講習として、学生と同じように e-learning 形式で、テキストとテストを用意しており、毎年の受講を促している。システムとしては学生と同じものを利用しているが、学生向け教材と比べ、より実践的な内容となっている。

また、定期的な講習だけでなく、新入職員向けの基礎講習や、システム管理者向けの講習会も実施している。定期的な講習以外に、立場に応じた教育を実施することで、それぞれの役割や責任に応じた知識の習得機会としている。

その他には、全教職員を対象とした迷惑メール対策訓練を4年に 1 回のペースで実施している。標的型攻撃メールの急増という環境変化もある中で、直近では2025年度に実施している。結果については集計中となるが、属性別に分析したレポートを作成し、全部署向けに報告する予定である。

### 4.3 高度情報セキュリティ人材の育成

サイバー攻撃が増加する中で、大学に関わらず、高度な情報セキュリティ知識を持つ高度情報セキュリティ人材の必要性は増すばかりである。こうした状況において、中途採用による高度情報セキュリティ人材の確保は難しくなってきており、現実的には、組織内で人材を育成するほかない。

しかしながら、多くの大学における事務職員は、3～6 年程度の間隔で異動することが多く、専門人材育成については大きな課題となる。

本学においても、事務職員の多くは4～6年程度の間隔で異動となるため、人材育成については、非常に大きな課題として認識している。そこで、本学の情報セキュリティ部門にあたる情報基盤課情報企画係では、2024 年度より研修体系を見直し、高度情報セキュリティ人材の養成に力を入れている。具体的には、インシデント訓練やログ分析を題材とした演習形式の研修など、より実践的な外部研修を受講することで、適切なインシデント対応が可能な人材の育成を行っている。

また、従来は語学試験のみに利用可能だった受験費用の補助制度について、IT 系資格試験への適用範囲拡充を人事部に要望し、2023年度よりIT系の資格試験についても補助対象となった。この補助制度拡充により、情報基盤課では、IPA が実施する資格試験（以下、IPA 資格）について、取得を目指す若手職員が増えている。参考までに情報基盤課（現員 11 名）における2021年度以降のIPA資格取得状況の推移を表 2 に示す。

表 2：情報基盤課における IPA 資格の取得状況

| | 2020年度以前 | 2021年度 | 2022年度 | 2023年度 | 2024年度 | 資格取得者数（資格別） |
|---|---|---|---|---|---|---|
| **基本情報技術者**<br>※第二種情報処理技術者を含む | 2 | 0 | 0 | 3 | 1 | 6 |
| **情報セキュリティマネジメント**<br>※情報セキュリティアドミニストレータを含む | 2 | 0 | 0 | 1 | 1 | 4 |
| **応用情報技術者** | 0 | 0 | 0 | 0 | 1 | 1 |
| **情報処理安全確保支援士** | 0 | 0 | 0 | 1 | 1 | 2 |
| **ネットワークスペシャリスト**<br>※テクニカルエンジニア（ネットワーク）を含む | 1 | 0 | 0 | 0 | 0 | 1 |
| **資格取得者数（年度別）** | 5 | 0 | 0 | 5 | 4 | |

## 5 情報資産の管理

### 5.1 継続的な情報資産管理

多様な利用者、システム、機器等が利用される大学においては、大学が所有する情報資産を正確に把握し、リスクを特定・評価しておくことが重要である。保管場所・管理方法に問題のある情報資産を事前に特定することができれば、これを継続的に改善していくことで、インシデントの予防効果が期待できる。また、情報資産を適切に管理しておくことで、情報漏洩が懸念されるインシデントが発生した場合においても、漏洩した情報の特定や関係者の把握、漏洩経路の分析をスムーズに進めることができる。

本学では、すべての部署は、所管する情報資産について、保管場所・管理方法だけでなく、データ保存期間や第三者提供状況などを継続的に管理し、機密性・完全性・可用性の3要素に基づいて格付けしたうえで、リスクの評価と特定を行うこととし

ている。情報資産の管理やリスク評価・特定の手順については、Layer3 において規定している。

具体的には、Layer3 で規定しているリスク算定式を用いて、各情報資産のリスク値を算出し、算出したリスク値が基準以上となる情報資産については、各部署においてリスク対応計画の策定することとしている。

5.2 情報資産管理状況の一斉点検

先述の通り、情報資産の管理については、各部署が常日頃から継続的に実施することが重要である。しかしながら、各部署における担当者の異動や組織改編によって、管理が疎かになるケースが想定される。こうした懸念に対しては、定期的な一斉点検が有効である。

本学においても、同様の懸念があり、2024年度に全部署を対象として情報資産管理状況について一斉点検を実施している。具体的には、事前説明会を実施したうえで、現時点での情報資産管理台帳の提出を求めている。また、これに併せて、情報資産管理台帳のフォーマットについても見直しを行っている。

一斉点検の際に、各部署から提出された情報資産管理台帳を点検したところ、情報資産の管理状況が不十分な部署を複数確認できたため、後日、全体報告会を実施し、複数の部署で共通していた管理上の問題点を中心に情報を共有することで、組織全体としての対策強化につとめている。

5.3 新規サービス導入前の審査

新規で導入・契約を検討しているシステムやサービスなどについては、導入前の段階でセキュリティ上の懸念点や、個人情報等の取り扱い方法について確認しておく必要がある。

本学においては、SaaS を含む新規システム・サービス導入時には、CISO への申請を必須としている。申請にあたっては、当該サービスに保存・投入する情報の取り扱い方法について、契約書や約款に記載された内容が、『同志社大学情報セキュリティポリシー』が求めるセキュリティ水準以上であることを承認の条件としている。

また、独自環境の構築が必要となるシステムなど、より厳格な審査については、CISO が座長を務める情報化推進委員会での説明と承認を求めており、を行っている。

6 各システムの点検と改善

6.1 自己点検の定期実施

大学では、教員が研究室独自のサーバを運用していることが少なくない。また、各部署において個別に運用しているシステムのサーバが存在する場合もある。こうしたサーバに対しても定期的な点検と改善活動を義務付けることで、セキュリティ強度の継続的な維持・向上を図る必要がある。

本学では、各部署や教員が構築しているサーバを含め、すべてのサーバ管理者に対して、チェックシートによる自己点検を毎年実施している。各サーバの管理者にはチェックシートに回答の上、情報基盤課に提出するよう求めているため、教員が管理しているサーバの状態についても漏れなく把握することが可能となっている。

また、昨今では、クラウドサービスも増えていることから、クラウド環境に特有のチェック項目も追加するなど、チェックシートについても毎年見直しを図り、情報セキュリティ環境の変化にも適宜対応している。

6.2 情報セキュリティ監査

自己点検だけでは客観性が確保できないことから、監査部門や第三者を交えた情報セキュリティ

監査の実施も必要である。

本学においては、情報セキュリティ監査の手順について Layer3 で規定しており、毎年、3つ程度のシステムに対して監査を実施している。監査対象となるシステムについては、リスクアセスメントや過去の監査実績に基づいて、情報基盤課と監査部門で選定している。また、監査実施にあたっては、外部の情報セキュリティ企業に委託を行い、第三者による助言型監査の形をとっている。

具体的な監査手法としては、事前ヒアリングを実施の上、文書レビューのほか、インタビューとウォークスルーによる実地調査も実施している。また、監査報告書で指摘された事項については、改善計画の立案と実施を求めており、監査対象システムの責任者は、改善計画書を提出する必要がある。なお、改善計画書の作成にあたっては、改善方法や実施期日を具体的に明記するよう求めており、確実な改善策の実施を重視している。

### 6.3 脆弱性診断

各システムの脆弱性診断やペネトレーションテストについても、情報セキュリティ監査と同様に、定期的に実施することが望まれる。

本学では、情報セキュリティ監査の対象システムとなったシステムに対して、脆弱性診断も併せて実施している。具体的な診断内容としては、対象サーバのポートスキャンや各種ソフトウェアの脆弱性確認が主な内容であり、現時点では、ペネトレーションテストのような、より実践的な診断手法については実施できていない。

## 7 まとめ

本稿では、昨今の情報セキュリティ環境を確認したうえで、大学が講じるべき情報セキュリティ対策について、本学における具体的な取り組み事例や課題を取り上げながら、方針、組織体制、全体像を概観できる形でまとめた。

本稿で取り上げた事例については、いずれも多額の投資や専門知識を必要とするものではなく、大学の規模に関わらず実施しやすいものとなっている。また、文部科学省が言及している取り組み[6]も多いため、基本的な情報セキュリティ対策の具体的なモデルケースとして、大学業界全体の情報セキュリティ強化に資する内容だと考えている。

今後は、本稿でも触れてきた本学の抱える課題について対応することで、本学の情報セキュリティを強化していくとともに、最新の情報セキュリティ環境に関する情報収集に努め、さらなる知見を深めていきたい。

## 参考文献


[1] 独立行政法人情報処理推進機構、情報セキュリティ白書 2024、pp.208-240、2024.

[2] SLASHNEXT、The State of Phishing 2023、pp.1-4、2023.

[3] 独立行政法人情報処理推進機構、情報セキュリティ 10 大脅威 2025、2025. https://www.ipa.go.jp/security/10threats/10threats2025.html

[4] 文部科学省 大学等におけるサイバーセキュリティ対策等の継続的な取組について(通知)、6文科高第 1551 号、pp1-2、2024.

[5] 内閣官房 国家サイバー統括室、政府機関等のサイバーセキュリティ対策のための統一基準群の概要、pp.1、2025.

[6] 文部科学省 前掲通知、pp.3-5、2024.