学術研究機関における サイバーセキュリティ・ ガバナンス WG 報告書

Version. 20181017

1. はじめに

全国の国立大学法人、大学共同利用機関法人、国立高等専門学校（国立高等専門学校機構）、放送大学学園では情報セキュリティ強化が実施されている。各組織において、情報セキュリティ対策基本計画の策定、情報セキュリティインシデント対応体制及び手順書等の整備、情報セキュリティポリシーや関連規定の組織への浸透、情報セキュリティ教育・訓練や啓発活動の実施、情報セキュリティ対策に係る自己点検・監査の実施、情報機器の管理状況の把握及び必要な措置の実施を行なっているところである。さらに、法人評価においても組織の情報セキュリティへの取り組みが課題として指摘されている。

本報告書は、このような日本各地で策定、実施されている情報セキュリティ対策基本計画の参考になるよう、情報セキュリティに関する環境、ICT システムの変化の速さを考慮して、平成28年度からの3年間を対象にしてその例を示すものである。対象者は、各組織の教職員を想定している。情報セキュリティ対策基本計画は、まず、各組織の個別事情に基づいた組織の方針を「全体方針」として記載し、次に、具体的な個別方針を記載し、最後に工程表を作成する。具体的なことが記載される個別方針の項目は、対象となる全ての機関で共通であるが、機関の規模や、教員、職員の構成によって、その内容が左右されることが予想される。しかし、いずれにしても共通的な事項は多く、また、どこまで詳細に記載すべきか判断に迷う組織もありそうである。このような状況で、本報告書は、いくつかの典型的な大学の内容を例にして、情報セキュリティ対策基本計画の個別方針に記載すべき内容を示すものである。

個別方針は、以下の6項目で構成される。

1) 情報セキュリティインシデント対応体制及び手順書等の整備
2) 情報セキュリティポリシーや関連規程の組織への浸透
3) 情報セキュリティ教育・訓練及び啓発活動
4) 情報セキュリティ対策に係る自己点検・監査の実施
5) 情報機器の管理状況の把握及び必要な措置
6) その他、法人の特性や法人を取り巻く脅威等に応じた対策等

各項目の概要は下記の通りである。

1) 情報セキュリティインシデント対応体制及び手順書等の整備
(1)情報セキュリティシンシデントに対応する体制および手順書、(2)緊急時に停止可能な機器や事業継続のために停止機関が最小限であることが臨まれる機器の把握、(3)最新の脅威・脆弱性情報の入手、(4)インシデント対応を行なう職員に対する訓練、などを決め記載することが求められている。

2) 情報セキュリティポリシーや関連規程の組織への浸透
(1)情報セキュリティポリシー・情報倫理規定などの規定のタイムリーな更新、(2)学務・診療・財務を含めた情報の格付けを決め記載することが求められている。

3) 情報セキュリティ教育・訓練及び啓発活動
(1)役職員・情報システム管理者・担当者に対する情報セキュリティに関する教育・訓練の定期的な実施・継続方法、(2)実践的かつ関係部門横断的な訓練、非常勤職員や派遣職員、(3) 客員教員等、随時採用される職員だけでなく、新・編入生や留学生へも洩れなく対応するための手段を決め記載することが求められている。

4) 情報セキュリティ対策に係る自己点検・監査の実施
(1) 構成員が自ら情報セキュリティ対策を実施できることを確認するための自己点検、(2)自己点検結果の評価、(3)第三者による監査を実施するための手段を決め記載することが求められている。

5) 情報機器の管理状況の把握及び必要な措置
(1) グローバル IP アドレスの管理・把握の徹底、(2)グローバル IP アドレスの適切な通信制限の実施、(3) 重要情報を取り扱う機器の通信制限、(4)利用予定のない IP アドレスの返還計画、(5)基本・応用ソフトウェアのタイムリーな更新の実施の徹底、(6)強度の高いパスワードの使用の励行を決め記載することが求められている。

6) その他、法人の特性や法人を取り巻く脅威等に応じた対策等
国立大学法人の組織の特性 (総合大学、単科大学、附属病院の有無、附属学校の有無等) に応じて体制・脅威が異なるため、それぞれの特性に応じて対策を記載することが求められている。

なお、情報セキュリティ対策は大学における法令遵守や危機管理の一部であるが、本報告書では法令遵守や危機管理まで扱わない。また、受託研究等の契約書に記載される情報漏洩対策の記述や、教育コンテンツにおける著作権対策など、契約担当や知財担当が主として対応するべき部分である。加えて、附属病院内ネットワーク (医療情報) や附属学校内ネットワークは大学ネットワークとは別管理となっている場合があるため、ここでは扱わない。

2. 高等教育機関における情報セキュリティインシデント対応体制

2.1. 任務

情報セキュリティインシデント (以下、インシデントと呼ぶ) が発生した際に、最初に対応する CSIRT (Computer Security Incident Response Team) と呼ばれる組織を設置する動きが広まっている。この組織は、理想的には、セキュリティに対応する技術者だけでなく、対応を判断し、必要に応じて外部との連絡や組織上層部への連絡を行う管理者から構成されるべきである。また、インシデントの発見、分析、防御などの記述及び装置の保有とともに、インシデント発生時に迅速に対応するための権限も必要となる[1][2][3]。しかし、大学等の高等教育機関では人員や予算などの様々な制約があり、理想的な CSIRT を構成することは困難である。そこで、本稿では、国立大学法人を想定して、現実的な CSIRT のあり方を考える。

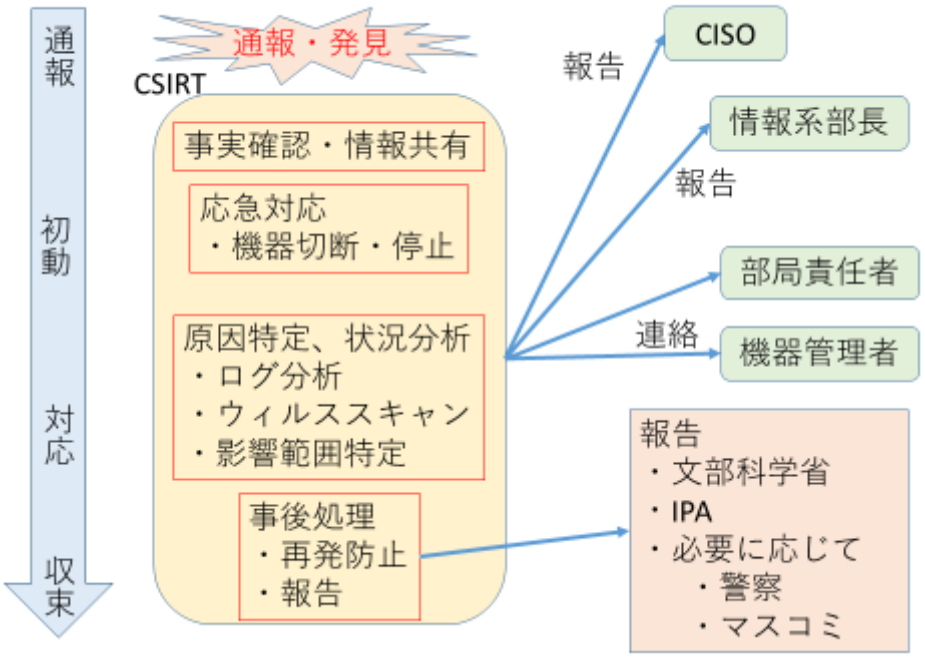

図 2.1-1 処理手順の例

図 2.1-1 に対応手順の例を示す。国立大学法人の CSIRT の役割の第一は、インシデント発生時の通報を受ける窓口である。国立情報学研究所や文部科学省をはじめとした外部組織からのインシデント発生時の通報だけではなく、大学内で発生した場合にも第一報が届く場所としておきたい。そうすることで、その後の対応を組織的に行うことが可能となる。また、CSIRT が十分に機能するためには、組織内外にその存在を周知しておく必要がある。例えば、電話やメールなどの連絡口を公表しておくべきである。

CSIRT への通報があった場合、あるいは CSIRT 自身がインシデント発生を検知した場合、その内容を把握し重大性を定めるとともに、発生源を特定し、ネットワークからの切り離しやシステム停止、FW 等を用いた防御、あるいはアカウントの停止を迅速に行う。この場合の重要な点は、被害の拡大を防ぐことである。

対応を迅速に行うためには、組織内部のネットワーク構成及び業務関連システムの概要、そして各システムや部署の対応者を把握しておかなければならない。業務システムの中には、ネットワークからの切り離しや停止が業務に大きな影響を与えるものがある。そのため、重要業務システムについては事前に情報を集め、セキュリティポリシーなどに基づいてネットワークからの切り離しや停止の可否を迅速に判断できる準備が必要となる。

被害拡大を防いだ後、インシデントのより詳しい分析とともに、原因の特定を行う。大学が保有する技術だけでは困難な場合が十分に想定される。重大な事案の場合には、システムの導入業者や保守業者だけでなく、外部のセキュリティ会社や警察などの支援を受ける必要がある。

インシデントの重大性に応じて、大学本部や外部への報告、さらに広報が必要となる。軽微なものは、件数を半期毎、年度毎に適切な委員会に報告すれば十分であろう。しかし、重要な事案の場合には、各大学が定める危機対応の手順に従って、大学本部へと報告することになる。状況を適宜、CISO、必要ならば学長に非公式であっても報告するチャンネルがあると心強い。案件によっては、文部科学省、IPA、あるいは警察へと通報することになる。報告する判断基準を定めるとともに、報告のひな形を持つことが、迅速で適切な報告を行う上で重要である。さらに、重要情報漏えいや、外部が関係する事案の場合には、記者会見が必要となる場合がある。広報の手順についても事前に確かめておく必要がある。なお、個人情報漏えい案件は、総務部などの組織が対応する場合が多いことに注意する。

停止あるいはネットワークから切断したシステムの再接続許可は、CSIRT が行うべきか情報系センターが行うかは、運用上の問題である。ウィルススキャン、脆弱性監査、管理運用体制確認などが必要であることは当然である。ただし、再接続したシステムのセキュリティ対策が十分であることの責任を負うのは CSIRT の役割ではないことを確認しておく必要がある。

CSIRT は、インシデントが起こるまで、何もしなくても良いということではないが、個々のシステムのセキュリティ対策を実施或いは確認する責任を負う部署でもない。しかし、CSIRT が起動しなくて済むための予防的活動も CSIRT の役割としておくほうが良い。インシデントの予兆に関する情報、例えば、脆弱性情報、攻撃情報を収集し、事前の広報や対策を情報系センターと協力して行うことが CSIRT の役割として含まれるであろう。

2.2. 体制

前述の CSIRT の役割を担うための装置や人員を、大学が新たに設けることは実際的に不可能である。従って、情報系センターが CSIRT の基礎的な設備と人員を担うほかにはない。単科大学など、単独で基本的体制が取れない場合については、別に議論する。

しかし、情報系センターだけで CSIRT を構成するのも得策ではない。学内に情報セキュリティの専門家が居れば、協力を得ることはもちろんである。さらに、全学の情報システムが対象であるため、事務情報システム、附属病院や附属学校、あるいは遠隔キャンパスにおけるインシデントに対応できるよう、現場担当者を加えておくことも検討しておくべきである。インシデントの大学本部への報告、外部への通報、記者会見などへの対応のため、担当事務への窓口の整備も必要となる。

CSIRT の母体は情報系センターのメンバーが中心となるであろうが、CSIRT を情報系センター内に設置するのは検討の必要な点である。大学全体の情報セキュリティインシデントに迅速に対応するには、ある程度の強い権限と、結果責任の明確化が必要である。そのため、学長や担当理事の直下などに設置することが望ましい。

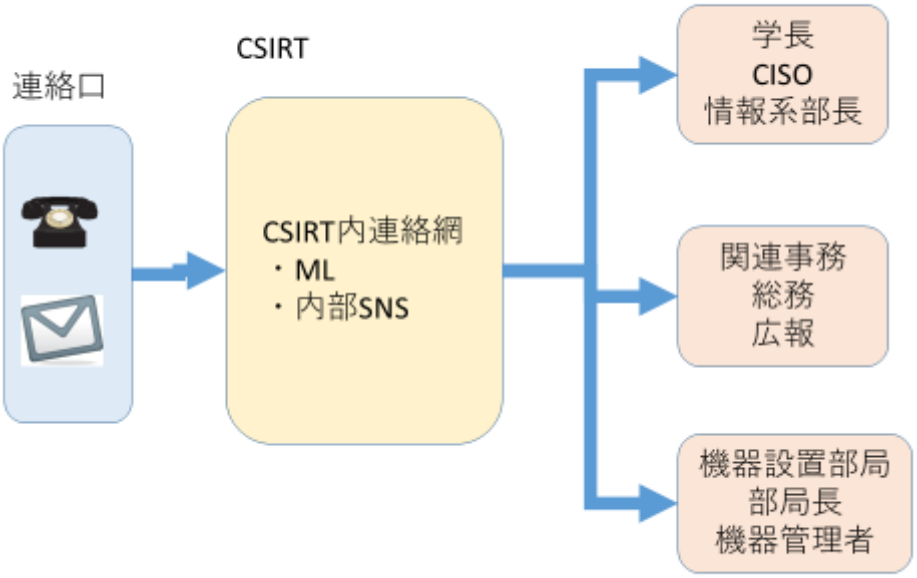

図 2.2-1　連絡体制イメージ

これらの体制が機能するためには、情報共有や連絡体制を事前に確認しておく必要がある(図 2.2-1)。CSIRT 内の連絡は、閉じた SNS やグループウェアなどを用いて、事象への対応の記録を残すことができるものを選ぶのが望ましい。情報システムを設置している責任者や担当者については、メールアドレスや電話番号の収集を行っておく。

2.3. 制約と対策

大学の情報担当部署は、その役割の増大にも係わらず少人数で構成されているのが実際である。さらに、国立大学法人を取り巻く状況は厳しく、運営費交付金が毎年度減額され、人件費の割合が増大している。大学の情報担当部署の人員や予算が増えることはほとんど期待できないだけでなく、一部の大学では情報担当部署の予算と人員の削減が行われている。

インシデントはいつ発生するか分からない。しかし、上記の情報担当部門の制約のため、対応できることには大きな制約が発生する。教員と職員で CSIRT を構成する場合、交代制などをとって 24 時間 365 日対応することは事実上不可能である。勤務時間外や休日にインシデントが発生した場合に、少人数での拙速な対応は慎むべきである。拙速な対応は、事態を悪化させる恐れがあるとともに、学内への説明に問題を生じさせる恐れがある。そのため、勤務時間外や休日の対応手順とその発動要件を定めておく必要がある。

インシデントの分析を行うための十分な道具と技術を揃えておくことも困難である。重大事案の場合に、外部専門家の応援をえるための、予備費などを確保しておくと良い。

CSIRT のメンバーは、専任ではなく他の業務を兼務することになるであろう。特に、教員は講義や出張で迅速に対応できない場合がある。事務職員や技術職員で初動対応ができる準備が必要である。

2.4. 手順整備

インシデントが発生した場合、そのインシデントへの対応レベルの設定が必要である。

毎日着信している迷惑メールやウィルス付メール、あるいは FW に記録された遮断された不正な通信は、被害の恐れがなければ、軽微な動作として特別な対応を行わない。後に、毎月や半年毎に総数を取りまとめ、適切な委員会に報告する。

不正な通信などの報告が受けたが、被害が発生しないものも多数存在する。例えば、PC のウィルス感染、攻撃を受けているとの外部からの通報を受けて対応したが被害のなかったもの等である。こちらは、ウィルス駆除やパスワードロックなどの対応を行う。簡単な報告を、後日まとめて行う。

機微情報の漏えいや外部への攻撃が疑われるものは、迅速に対応し、被害拡大を防ぐ必要がある。状況は適宜、担当理事や学長へ報告する必要がある。また、関連事務と連携し、対応策を講じる。一応の対応の後、外部への報告の必要性を検討する。

2.5. 大学間の連携

大学の情報担当部署の人員や予算には厳しい制約がある。特に、理工系学部を有しない小規模大学では、情報系部署に専任教員を置くことも困難である。そういう大学が CSIRT のような体制を構築するにはどうすればよいであろうか。

一つの方法として、近隣大学の支援を得るという方法を検討してみる価値はある。もちろん、連絡窓口業務と事務作業は自大学で担う必要はある。連携する大学側は、初動対応や分析などの技術的な支援を行う。

しかし、実際に行うためには、相互の情報共有が十分に行われている必要がある。支援を受ける大学側の情報を連携相手に伝えるだけでなく、支援大学が他大学を支援することの位置づけを明確にする必要もある。

3. 情報セキュリティ教育・訓練及び啓発活動

3.1. はじめに

情報学内システムのセキュリティ向上のためには全学内構成員のセキュリティに対する意識を向上させることが不可欠である。セキュリティ教育としては学生や一般教職員のみならず、学内部局において管理を担当する者、全学的なセキュリティ対策を講じる CSIRT スタッフ、さらに大学のセキュリティ対策の方向性を決定する CISO や大学執行部のそれぞれに合わせた内容の教育が求められる。第一に、全構成員が自らの役割に応じたセキュリティ問題の意識を持つことを目指し、セキュリティ対策を実践できるように教育を実施する。

主な教育方法としては、学生には一般講義でのセキュリティ科目の開講や、コンピュータシステム利用時の事前講習がある。また、講義方法は、講義形式や e-Learning が考えられる。受講を学内システム利用の条件とすることで、受講率の向上を行う方法もある。また、教職員（役職者、CISO、CISRT スタッフを含む）については、学生同様の一般的知識に加えて、学内情報資産や運用規則の理解について講演や e-Learning の受講を進める。さらにはセキュリティ対策訓練の実施がある。これらの受講を徹底するためには、評価と連携した仕組みを検討してもよい。運用管理スタッフには、一般教職員と同様の内容に加えてインシデント発生時に素早く対応するための教育が必要となる。CSIRT スタッフには、十分なコンピュータとネットワーク、セキュリティの知識はもちろんのこと、学内情報資産や運用規則に対する十分な理解が求められる。もちろん、インシデント発生時に対する対応策の理解と訓練が必要である。最後に、CISO や役職者には、学内情報資産やリスクマネジメントに対する理解と、セキュリティ対策へのコストとインシデント発生時の影響に対する十分な理解を求める。

3.2. 学生

学生へのセキュリティ教育は、学生がマルウェアなどの被害者にならないためと、意に反して加害者にならないために、基礎的な情報倫理とともに実施する必要がある。さらに、大学の計算機端末とネットワークの利用を許可するために必要な場でもある。また、各大学のシステムに合わせた利用上の注意点があると考えられることから、各大学のシステム（ライセンスソフトウェアの有無やパスワードポリシーなど）に応じた内容が必要である。

学生に対するセキュリティ教育を実施するために、時期、方法について検討する必要がある。まずは、入学時点における教育として、大学における計算機とネットワーク利用に関する説明とセキュリティポリシーのガイダンスを実施し、理解した旨の署名の提出を求める。実施時期は、アカウント発行前に行い、この署名の提出をアカウント発行条件とする。また、毎年度、e-Learning を用いてセキュリティポリシーなどを理解しているかを確認（試験）する。この試験に合格することをアカウントの継続利用の条件とする。さらには、各学年での e-Learning に合格していることを卒業条

件とすることを検討しても良い。なお、アカウント停止は、必要な演習・講義の単位が得られない可能性があるため、学内規則の制定と周知徹底に留意する必要がある。

内容は、実施方法や回数によって異なるが、情報セキュリティに各個人で取り組むことの必要性、ソフトウェア更新、ウイルス対策（アンチウィルスソフト導入やメール添付ファイルの取り扱い）、各種詐欺（フィッシング詐欺や架空請求）対策、SNS 利用上の注意、著作権、公衆無線 LAN の利用の注意、パスワード設定について等、セキュリティ対策の基本となる項目を重点的に行う。また、りんりん姫**エラー! 参照元が見つかりません。**や INFOSS 情報倫理[5]などの e-Learning 教材の活用も有効である。加えて、各大学のシステムに合わせた利用ガイダンスを組み合わせる必要がある。さらに、講義科目を設置し、各内容を詳しく指導することも重要である。

3.3. 一般教職員

一般教職員へのセキュリティ教育は、大学が有する情報および情報システムを安全かつ安定的に利用するために不可欠である。このため、法令順守を徹底するとともに、各大学が定めるセキュリティポリシーや運用規則（インシデント対応を含む）への理解を深める必要がある。また、大学が扱う情報には多くの個人情報が含まれることを理解してもらう必要がある。対象は、常勤の教職員に限らず、非常勤の教職員も含む必要がある。

3.3.1. セキュリティ教育

内容は、基本事項として一般学生と同様の項目が必要である。加えて、個人情報の取り扱い方法、ファイル持ち出し、クラウドサービス（職務上の情報のクラウドへの保管、サービスの利用）の利用、学外へのメール転送など各大学が定める情報取り扱い規定の理解が重点内容となる。

実施方法としては、採用時には大学の基本セキュリティポリシーを理解させるとともに、各大学における情報システム利用規定を理解させ、セキュリティポリシーに対する誓約書の提出を求める。その後、年 1 回程度、重要事項とその時々の問題に対する理解を確認する機会を設ける。実施形式として、セミナー形式でも e-Learning 形式でも良いが、受講後に試験を実施することでより深い理解を得るようにする。教職員に特化した e-Learning コンテンツ[6]もあるため、活用することも有効である。

セキュリティ教育実施に関する問題として、受講率の低迷がある。どの大学も、受講率が低迷していると思われるため、受講率を挙げる工夫が必要となる。セキュリティポリシーとして、学内計算機・ネットワークの利用にはセキュリティ教育受講を必須条件とすることが考えられる。未受講の場合、アカウントの停止を含めた規定を検討する必要がある。さらに、学内で開催される他のセミナーなどと合わせて、受講数を昇進基準の一部に組み入れる方法もある。また、部局単位での受講率向上として、受講数の部局長への報告や部局単位での受講率の比較・競争、受講率による部局予算の変動といった策を検討する。また、大学アカウントがなくても困らない教職員（NAT 配下でネットワーク利用、学内サービスを全く使わない等）がいる場合、アカウント停止策は有効ではない。根本的には対策が難しいが、学内ポータルや重要サービス（出張申請や物品購入など）

を学内アカウントでのみ実施できるようにするなど、学内アカウントの必要性を上げることでの解決を検討する必要がある。

3.3.2. セキュリティ訓練

インシデント発生時の対応として、定期的な訓練を実施する必要がある。訓練のポイントとしては、問題に気が付いた時点で学内インシデント対応手順に従って、上司や CSIRT 等に連絡することの周知徹底である。特に、問題発生によるペナルティを恐れて連絡が遅れることがないように不必要にペナルティを与えることなく対応手順を作成し、その旨の学内周知を行う必要がある。

特に、近年増加している、標的型メール攻撃への対応として、不審メールに対する通報や、メール添付ファイルを開いた後での不審な動作の通報について、対応方法の周知徹底とその訓練の実施が必要である。訓練により、教職員にインシデント対応手順の理解を深めてもらう。

3.4. 部局管理スタッフ

部局管理スタッフは、問題発生時に CSIRT や大学システム管理部局と共同でインシデント対応に当たる必要がある。そのために、「大学として守るべき情報資産の理解」および「インシデント発生時の対応手順の理解とその実施能力」が必要となる。また、インシデント対応に必要となる「部局が利用する大学システム・ネットワークの構成の理解」、「部局内システムの構成の理解」が求められる。当然ながら、一般教職員と同様のセキュリティ基礎および学内規則を十分に理解する必要がある。

3.4.1. インシデント対応

インシデント対応については、初期対応手順を CSIRT などでまとめ、その実施について教育し、訓練を定期的に実施する。特に、インシデント対応初期手順について、「インシデントが発生した計算機の停止の可否の判断」が素早くできることが必要である。このため、インシデントの影響範囲を判断できるように準備する必要がある。訓練においては、インシデント発生時の対応手順の確認、計算機停止の迅速な判断、上位管理組織（CSIRT 等）への連絡が滞りなく行えるかの確認を重点的に行う。

3.4.2. 管理・運用技術

部局管理スタッフは、システム管理者としてのシステム管理研修、通常時のセキュリティ啓蒙活動、インシデント発生時のための対応訓練が必要となる。システム管理としては、部局システムの規模や構成によって異なるが、基本的な OS、アプリケーションの管理（更新作業を含む）とネットワークの設定等から、ID 発行や認証システムや Web システムの運用など多岐にわたる。担当者

の交代などでのシステム情報や設定の引継ぎ不足を認識できるように、インシデント対応訓練において各システムの設定状況を確認する項目を含めることが望ましい。

通常時のセキュリティ啓蒙活動については、Windows Update 等の適用のアナウンスや、部局内システムの利用状況確認、異常な活動の検知など、部局が管理するシステムの稼働状況の把握と上位組織への報告に関する教育と連携の訓練を行う。

3.5. CSIRT スタッフ

大学の情報資産とリスクマネジメント、関連法令に対する教育が必要となる。さらに、インシデント発生時における対応方法について十分な理解と実践能力を維持できるように継続した教育および訓練が必要である。特に、部局管理スタッフからのインシデント発生報告への対応、インシデント発生機器の停止の判断、CISO 等への報告等が滞りなく実施できるように訓練を実施する。また、最新のマルウェアの発生状況や、学内でのインシデント発生状況の共有などを行い、インシデント発生時の対応を円滑にできるようにする。

過去の事例などを用いて、対応手順を確認する机上訓練は、比較的容易に実施することができる。過去の事例の見直しを通じて、CSIRT のレベルアップの効果が期待できる。CSIRT 訓練のツール[7]やサービス[8]もある。

3.6. CISO・役職者

情報セキュリティの学内での統括責任者として、情報セキュリティの必要性（人、コスト）と問題発生時の学内外への影響の理解を深める。また、他大学の事例などによるケーススタディを行い、情報セキュリティの必要性と影響を具体的に理解する。

学内情報セキュリティ対策の方針と学内システムおよびセキュリティ対策（組織、委員会など）の現状について理解を求める。必要に応じて、組織体制の点検を行い、適切な人材や外部組織との連携を検討する。特に、部局単位での対策ではコスト効率が悪い場合があるので、全学的な対策導入についての理解を求める。また、インシデント発生に備えて、法務部門や広報部門と連携したセキュリティ対策体制の構築を理解する。また、全構成員に対するセキュリティ教育・訓練についての理解を求める。

インシデント発生時には、CSIRT や部局からの情報に基づいて優先事項の決定や対外広報に対する方針決定を行うこととなるため、学内情報資源とリスクマネジメントを理解し、インシデント発生時の大学への影響に対する十分な理解を求める。

4. 自己点検および監査

4.1. 自己点検および監査の目的

情報セキュリティの確保のためには、それぞれの組織において、セキュリティ確保のための基準や計画が策定され、それらに基づく各種規程が適切に運用されていることが重要である。そのため各種規程の準拠性、実効性、および妥当性の有無を定期的に確認しなければならない。この確認のため、自己点検や、独立性を持つ者による情報セキュリティ監査を行う。また、監査結果を分析し、対応の指示、計画や各種規程の見直しを行う必要がある。

各大学の実際の監査の規程等は、「経済産業省 情報セキュリティ監査実施手順」[10]や政府統一基準[9]をベースに大学向けに国立情報学研究所が作成した「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」[11]の監査に関する項目を参照していただきたい。本節ではこれらを元に実際に監査を行っている大学の状況を調査し、監査の規程や実施方法のポイントを述べる。

4.2. 監査責任者

監査を行うにあたって、CISO は監査責任者を任命する。監査責任者は以下の役割を担う。

- 実際に監査を行う監査実施者および監査チームの編成
- 監査計画の策定
- 監査結果報告書を作成し、CISO への報告

なお、監査責任者を CISO とは独立させ、学長が任命するよう定める考え方もある。また、既設置の法人監査担当部署の長が監査責任者となる事例もある。監査責任者の任命に関しては、情報システム運用基本規程等の基本規程で定める。

4.3. 監査実施者および監査チーム

監査責任者は監査実施者および監査チームを任命する。監査実施者および監査チームは、被監査者と同一人物であってはならない。監査実施者および監査チームには情報システムや情報セキュリティに関する知識・技術だけでなく、倫理観、監査についての知識や技術も求められる。また、監査チームに外部の専門業者を含むような体制も考えられる。

4.4. 監査計画

監査は年 1 回以上行わないと、その実効性が疑われる。そのため、年度当初に監査計画の承認を受け被監査側へ周知を行う必要がある。また、監査結果を受け次年度の情報セキュリティ全体の計画等を見直す必要があるため、それらの検討時には、監査結果を報告しなければならない。これらを勘案し監査計画を策定する。監査項目および監査対象は、大学等においては、膨大となるため、1 年で全ての監査を行うことはできない。中・長期的な監査計画も必要となる。また、以下に該当する場合は、監査対象に取り入れる。

- 前回の監査で指摘(不備・違反)があった箇所
- 組織等の改変があった箇所
- 規程が改訂または追加された箇所

監査計画策定にあたっては、以下を明確にする

- 監査方針
- 監査の目的
- 監査対象(業務、システム等)および、対象となる組織/人(一部の学内組織等)
- 監査のスケジュール
- 監査基準
- 監査業務の管理体制(誰が実施するか等)

4.5. 監査における指摘の基準の策定

監査における指摘の基準は、基本的に各種規程を逸脱(違反)しているか、していないかのどちらかであるが、政府の統一基準においては違反を

- 重大な違反: その違反単独で、又は他の違反と複合することにより、重大なリスクの発生を引き起こす可能性のあるものをいう。
- 軽微な違反: 重大な違反以外のものをいう。

の 2 つに分類し報告することとなっている。その他、ISO 監査では

- 改善の機会: 違反ではないが、改善のために何らかの対応が望ましい。

という事項を設ける場合もある。

4.6. 監査の実施

監査にあたっては、何の監査を行ったかを記録する監査調書を必ず作成し、一定期間保存する。監査調書では、判断を行った監査証拠を明確にしなければならない。違反等、指摘する項目がある場合は、監査調書とは別に「指摘事項等報告書」を指摘事項ごとに作成する運用もあり得る。指摘事項に関しては、内容に関して被監査側と必ず同意を得ねばならない。

また、大学等の大きな組織では、全数調査は難しい。基本的には、サンプリング調査になる。機器の実態調査(サーバ等のポート制限状態等)においては、ツールを用いた調査で、全数調査を行っている事例もある。

4.7. 監査結果の報告

監査責任者は監査報告書を作成し、CISO(または学長等)に報告を行う。監査報告書では、読み手が CISO(または学長等)であることを考慮し、指摘事項の重要性や緊急性により区分けを行い、指示すべき内容が明確になるように記述する。

4.8. 監査結果への対応

CISO は監査報告を受けて指摘事項に対し期限を設け改善を指示する。この際、対応計画書を作成する運用もあり得る。該当指摘事項の情報セキュリティ責任者は改善が困難な場合はリスク軽減策を示し対応目標を提示する。教育や訓練により解決すべき事項の場合は、教育訓練の計画を提示する。

4.9. 自組織内の相互監査

規模の大きい大学では部局毎に CISO を設置し、部局毎に情報セキュリティ監査を行うよう定めている場合もあり得る。このような場合、他の部局から監査人を選出し相互監査を行うことも考えられる。組織全体としては、各監査が適切に行われているか管理する必要がある。

4.10. 現在の情報セキュリティ監査の状況および対策

国立情報学研究所が公表している「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」では、基本規程(C1001 情報システム運用基本規程)にて、監査責任者を置くことと監査規程に従って監査を行うことが規定されている。しかしながら具体的監査規程が未整備なため、実際には監査を行っていない組織も見受けられる。サンプル規程集(C2401 情報セキュリティ監査規程)を参考にし、早急に監査を行う体制を整備し、実効性のある監査を行う必要がある。また、大学等においては、主に事務職員または教員がセキュリティ監査を行うことが想定される。その場合、情報システムや情報セキュリティに関する知識だけでなく、監査に関する知識・技術も必要となる。監査に関する知識をもつ者が少数の場合、どうしてもそれらの者だけに監査を頼ってしまうことになる。そのため、多くの者が監査側になれるよう監査に関する知識・技術の教育も必要となる。これら監査に関する教育は、外部委託も考えられる。また、一部大学では、互いに監査を行うような取り組みを始めているところもある。

4.11. 自己点検

自己点検では、構成員が自らの役割に応じて実施すべき対策事項を実際に実施しているかどうかを確認する必要がある。また、自己点検の結果を踏まえ、それぞれの責任範囲において、必要な改善策を実施しなければならない。

そのため、自己点検を行う際は、構成員それぞれの役割に応じた複数の自己点検票が必要となる。「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」での自己点検の基本的な流れは、全学実施責任者(統括情報セキュリティ責任者)が年度自己点検計画を策定し、部局総括責任者が構成員ごとの自己点検票及び自己点検の実施手順を整備することとなっている。また、同規定集では年に 2 度以上の頻度で実施することが望ましいとしている。自己点検結果は、部局総括責任者が分析、評価し、さらに全学実施責任者はこれらを総括した分析、評価を行い、CISO に報告する。CISO は自己点検報告を受けて全学実施責任者および部局総括責任者に改善を指示する。

5. 機器・IP アドレスの管理

5.1. 情報機器と IP アドレス管理の目的

インシデント発生時には、多くの場合において発信源の IP アドレスを元に通信機器を特定することが求められ、同時に、当該機器の管理者との連絡が必要となる。したがって、情報機器に対する管理者と付与されている IP アドレスの情報を一元管理することが情報セキュリティ対策上、非常に重要なものとなっている。

本節では、情報機器の管理における押さえておくべきポイントについてまとめ、技術的な手法に踏み込んで整理する。

5.2. 情報機器と IP アドレスの管理

5.2.1. IP アドレスの管理

インターネット黎明期においては、IP アドレスは台帳管理で静的に割り当てることが一般的であった。機器が少ないうちはこのような手法でも管理が可能であったが、更新作業の滞りにより、データを最新の状態に維持することが困難となってきている。また、静的な台帳管理では、割り当てたグローバル IP アドレスの利用状況が把握できないため、調査対象となる通信時刻における通信状況を正しく判断できない点も問題となっている。そのため、IPAM（IP Address Management）に代表されるネットワークシステムを活用した管理が求められる。

また、多くの高等教育機関においては、アドレス変換機構（NAT/NAPT: Network Address Port Translation）を有するルータ（以下、NAT ルータ）を利用したプライベート IP アドレスを利用している場合がある。この場合、インターネット上での通信としては NAT ルータのグローバル IP アドレスでの通信となるため、対象となる通信を実施した機器を特定することができなくなる。そのため、プライベート IP アドレスに関してもグローバル IP アドレスと同様に、利用状況を管理することが求められ、その管理は NAT ルータ管理者に求められることになる。特に通信状況を把握するためには、NAT ルータにおけるアドレス変換ログを保持することが必要となる。

5.2.2. 機器情報の管理

ネットワーク接続機器を管理する際には、対象機器の管理者および利用者を合わせて管理することが重要である。特に、ネットワーク接続を行う機器の場合、機器のネットワークインターフェースに設定されている固有のアドレスである MAC（Media Access Control）アドレスを機器の ID として管理することが一般的である。ただし、MAC アドレスは、機器のインターフェースを交換すると変化してしまい、また、ソフトウェアで変更することも可能である。さらに、複数のネットワークインター

フェース（有線 LAN と無線 LAN など）を有する機器も想定されることから、別途機器 ID を設定することも検討されたい。

5.2.3. システムによる IP アドレス管理手法

前述のように、IP アドレスの採番を静的に行い台帳で管理することは、情報セキュリティを維持する上で好ましくない。以下に、IP アドレスの管理手法について技術的な側面でまとめる。

- DHCP（Dynamic Host Configuration Protocol）
  DHCP は、ネットワークに接続された端末に IP アドレスをはじめとした、ネットワーク接続に必要な情報を自動的に割り当てるプロトコルであり、多くの環境で利用されている。DHCP ではリース情報を管理しているため、割り当てた IP アドレスと MAC アドレスの対応を時系列に把握することが可能となる。
- ARP テーブルの監視
  IP アドレスと MAC アドレスの対応を把握する手法としてルータが保持している ARP（Address Resolution Protocol）テーブルを収集する方法がある。定期的に収集することで、時系列で対応関係を把握することができる。
- IPAM システムの利用
  IPAM は IP アドレスと利用者を管理するシステムで、DHCP サーバと DNS サーバを統合的に管理することを実現する。利用者情報の管理機能により、IP アドレスの利用者を容易に特定することが可能になる[12]。

5.2.4. システムによる機器情報の管理手法

機器情報となる MAC アドレスと利用者および管理者情報を管理するための技術的手法について以下にまとめる。

- IEEE802.1X 認証
  ネットワーク接続の際に、利用者の認証情報を元に接続の可否を決定する技術で、無線 LAN 利用においては一般的に利用されつつある。この技術を利用することで、利用者が利用した端末情報（MAC アドレス）と利用時刻をシステムにて把握することが可能になる。ただし、有線ネットワークでは機器側にて別途対応が必要な場合がある。
- MAC アドレス認証
  登録した MAC アドレスを元に接続の可否を決定する技術である。利用者および管理者と機器情報（MAC アドレス）の関係は、別途データベースを構築する必要がある。

どちらの認証技術においても、独自に認証サーバを構築する必要があり、組織の認証情報との連携が重要となる。また、IoT（Internet of Things）の一般的な利用に伴い、ネットワークに接続される機器が急増することが予測されているため、ネットワーク機器情報管理におけるシステム化は急務であると言える。

5.2.5. IPv6 利用における考察

本稿執筆時点においては、多くの高等教育機関における IPv6 利用は進んでおらず、現行の IPv4 における対策で十分ではあるが、IPv6 を導入する際に押さえておくべき観点を整理する。

- IPv6 ではインターフェースに複数の IP アドレス設定が可能である
  IPv6 ではインターフェースに IP アドレスが複数設定されるため、IPv4 のように MAC アドレス対 IP アドレスの関係が 1 対 1 にはならない。1 対 1 を前提とする仕組みのままでは IPv6 に対応できない点を考慮する必要がある。
- リンクローカルアドレスでセグメント内通信が行われる
  IPv6 では、グローバル IP アドレスが割り当てられなくとも、セグメント内（ルータを超えない範囲）での通信が可能となる。したがってセグメント内通信の監視を行う場合には、グローバル IP アドレスだけではなく、リンクローカルアドレスの管理も併せて必要となる。
- DHCP では MAC アドレスを管理できない場合がある
  IPv6 用の DHCP（DHCPv6）では、IP アドレスを割り当てる端末管理に用いる ID として DUID（DHCP Unique ID）が用いられ、IPv4 の場合の MAC アドレスと異なる。DUID には四種類のフォーマットがあり、IPv4 と同じ MAC アドレスの形式もあるが、すべてが MAC アドレスとはならない[13][14]。そのため、IP アドレスと MAC アドレスの組を管理するためには、NDP（Neighbor Discovery Protocol）近隣キャッシュを確認するなどの別手法を実施しなければならない。

表 5.2.5-1 機器情報・IP アドレス管理手法

	できること	課題など
台帳管理	管理者により静的に管理できる	定期的に利用状況を更新しないと現状にあっていない情報となる IP アドレスの利用状況を把握できない
DHCP/DHCPv6	割り当てた IP アドレスと MAC アドレスの対応関係を動的に管理できる	MAC アドレスと管理者/利用者情報の対応関係は別途管理が必要である IPv6 の場合は MAC アドレスとの関係を自動管理できない場合がある
ARP Table/NDP Cache 管理	利用している IP アドレスと MAC アドレスの対応関係を動的に管理できる	定期的に情報収集する仕組みを用意する必要がある
IEEE802.1X 認証	利用者情報（ユーザ ID）と MAC アドレスの対応関係を動的に管理できる	有線ネットワークでの利用にて機器側での別途対応が必要なため敷居が高い
MAC アドレス認証	利用する認証システムに依存するが、利用者情報（ユーザ ID）と MAC アドレスの対応関係を動的に管理できる	MAC アドレスを登録管理する仕組みを用意する必要がある

5.3. グローバル IP アドレスの適切な通信制御の実施

グローバル IP アドレスは、そのままの状態で運用すると、インターネット上のすべての端末からの到達性を提供することになる。そのため、適切な通信制御（パケットフィルタリングなど）を実施する必要がある。基本的に、クライアント端末として利用する場合には、インターネットからの通信をすべて遮断し、インターネット側への通信を基に動的にパケットフィルタを開放する SPI（Statefull Packet Inspection）を利用することを推奨する。

より厳しく制限する場合には、インターネット接続において利用するプロトコルを制限する運用も可能である。この場合にはパケットフィルタリングで実施するのではなく、プロキシサーバ等を利用した直接通信を制限する手法が有効である。

IPv6 の場合でも、IPv4 と同様にパケットフィルタリングや SPI が可能であるため、IPv4 と同様の通信制御が可能である。IPv4 と IPv6 を同時に利用するデュアルスタック環境においては、通信制御を実施する際のポリシを IPv4 と IPv6 で同じとなる運用を行うことが肝要である。

パケットフィルタリングはルータやファイアウォール機器が標準的に有している機能であるため、インターネットに組織のネットワークを接続する際には必ず有効的に利用する必要がある。ここで気をつける必要があるものとして、カプセル化された通信がある。カプセル化通信は、別のプロトコルで実際の通信を隠蔽して通信するもので、トンネリング通信や VPN で利用される通信手段である。カプセル化された通信の中身までチェックして制御するには、DPI（Deep Packet Inspection）機能が必要となり、廉価な通信制御機器では対応が難しい場合がある。その場合にはカプセル化通信を遮断する対応が必要である。

5.4. 重要情報を取り扱う機器の通信制限

個人情報や医療情報などに代表される重要情報を取り扱う機器においては、外部からの不正侵入を回避するためにより重要な通信制限が求められる。このような機器は、基本的にはインターネットに直接接続しない環境を構築することが望ましい。外部との通信が必要な場合には、プロキシサーバ等を利用した間接通信を利用することが重要となる。プロキシサーバでは、接続先サーバを限定する機能やダウンロードファイルのアンチウィルス機能を活用することで、重要情報を取り扱う機器がマルウェアに感染することを抑制することができる。

また、重要情報を扱う機器を、一般作業を行う機器が接続されたネットワークと完全に分離し、専用ネットワークセグメント内で運用することは、情報漏えいや不正侵入から重要情報を守るために有効な手段である。この場合、専用セグメントへの接続に際し、IEEE802.1X 認証や MAC アドレス認証などの接続認証を併用することが肝要で、不正な端末の接続を排除することが重要である。

IPv6 を利用する場合には、プライベート IP アドレスに相当する ULA（Unique Local Address）を利用することで、IPv4 と同様の運用が可能となる。

5.5. 基本・応用ソフトウェアのタイムリーな更新の実施の徹底

情報機器で扱うソフトウェアには、多くの場合プログラム上の誤りに起因する BUG や想定外の利用による脆弱性が存在している。そのため、問題が発生した際の迅速なソフトウェア更新が求められる。一般的に継続的な利用をサポートしているソフトウェアの場合、定期的なセキュリティアップデートが提供されているため、ソフトウェアを最新の状態に保つためにも自動更新設定とすることが肝要である。

オペレーションシステムなどの基本ソフトウェアの更新においては、その上で動作するアプリケーションへの影響を考慮する必要がある。基本ソフトウェアに脆弱性が発見された場合には、その上で動作するアプリケーションの動作検証も含めた更新作業が必要となるため、基本ソフトウェアの更新に耐えうるアプリケーションの設計が必要となる。

ネットワーク運用管理部門では、サービス提供しているアプリケーションのバージョン調査が重要である。例えば、ウェブサーバにおけるコンテンツ管理システム（CMS）の代表格である WordPress は多くの脆弱性指摘がなされており、最新版に適宜更新することが求められている。利用中のバージョン情報を調査した上で利用者に更新を促すなどの取り組みが考えられる。

5.6. 強度の高いパスワードの使用の施行

ユーザ認証を実施する際においてパスワード認証が現在の主流である。これまではパスワードを紙などに記載し情報端末に添付する行為の禁止や、定期的なパスワード更新が推奨されてきた。このため、ユーザは記憶することを最優先し、単純なパスワードを利用する傾向となっていた[15]。また、利用するシステム/サービス毎にパスワード認証が求められる場合があり、ユーザは多くのパスワードを管理する必要があったが、こちらも記憶することを優先するために同じパスワードの使い回しが横行していた。

上記のような状態を放置しておくと、管理対象のシステムにおいて ID 管理を徹底したとしても、別システムの ID 情報の流出などにより不正アクセスを許すことになってしまうため、現状では以下の対応が推奨されている。

- パスワードには複数の文字種を用い、文字長も最低限 8 文字以上とする
  - 文字種類 × 文字長で総当たり解析時間が決まる
- 記憶するために辞書に載っているような単語を用いない
  - 単語を利用し、o を 0、i を 1 に置き換えるような単純な対策だけでは不十分
  - パスワード管理ツールを利用し記憶できるパスワードを用いない
- 同じパスワードを複数のシステム/サービスで利用しない
  - 別システム/サービスからのパスワード流出による影響を低減する
- パスワードの定期的な更新を強制しない

なお、セキュリティレベルを高めるためには二段階認証や二要素認証の導入が有効である。

6. 事例紹介

6.1. 情報セキュリティインシデントに対する 1 次対応サービス（広島大学）

2 章において述べられているように、CSIRT には情報セキュリティインシデント発生時の POC（Point of Contact）としての役割が求められるが、教員と職員で 24 時間 365 日の受付体制を維持することは現実的に困難である。この問題に対する解決事例として、広島大学がその対外接続を提供する通信事業者の協力を得て開発している、情報セキュリティインシデントに対する 1 次対応サービス（案）を紹介する。

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である SuperCSI ネットワークサービスを利用している。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等）している。この監視部門に、POC の機能の一部を担わせようというものである。

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、情報メディア教育研究センター長（以下、センター長）に通信制限の権限が与えられており、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ができる。

一方広島大学は、国立情報学研究所が「大学間連携に基づく情報セキュリティ体制の基盤構築」に基づき平成 29 年 7 月に正式運用を開始したセキュリティ運用連携サービス（NII-SOCS）に試行運用開始時（平成 29 年 3 月）から参加し、NII-SOCS から提供される要確認情報への対応を通して、その通知頻度や正確性、即時性等の検証を行ってきた。そして正式運用への移行に合わせて、センター長が NII-SOCS から提供される要確認情報を「信頼できる情報」と指定し、全学委員会での承認を経て、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。

具体的には、(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 からの要確認情報に通信制限対象の 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) 広島大学の担当者に電子メールによる報告を行う。このほか、(4) あらかじめ指名する広島大学の担当者からの電子メールによる指示があれば、SuperCSI 監視部門が通信制限の設定および解除を行うこと、としている。

広島大学の担当者は NII-SOCS からの要確認情報を受信すると、SuperCSI 監視部門の 1 次対応と並行して通信制限の対象となったホストやその利用者を特定し、該当者に緊急措置を行った旨の通知と緊急対応（ネットワークからの切り離し等）を依頼する。該当者との連絡が取れ、応急対応が完了したことの確認をもって、センター長が通信制限の解除を指示する。

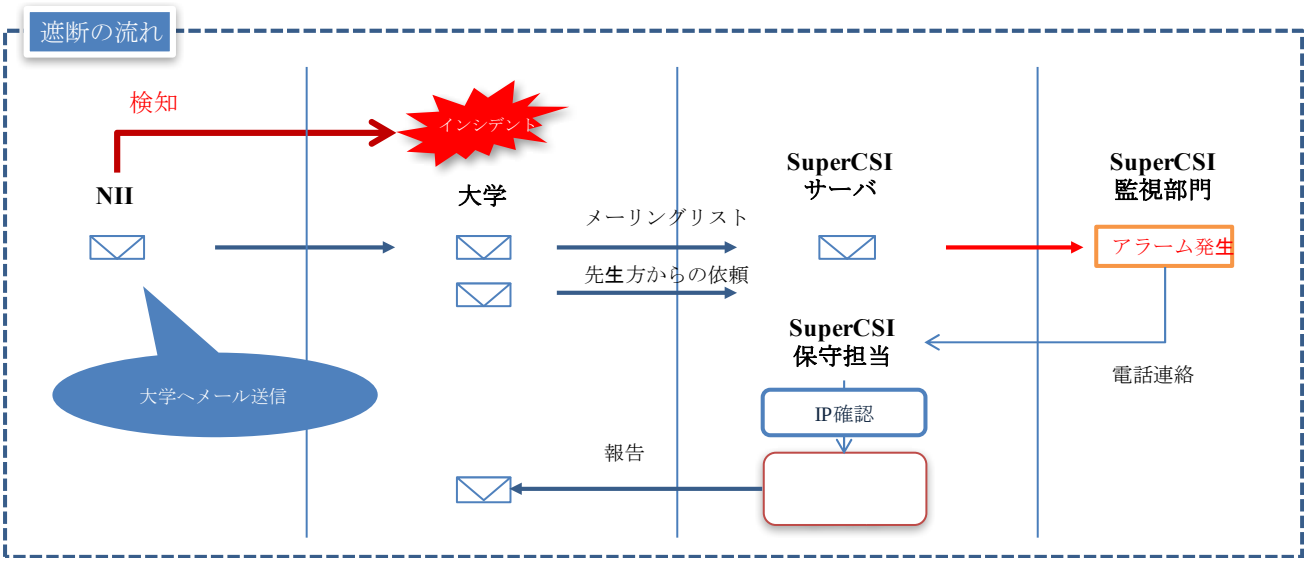

図 6.1-1　広島大学による運用体制図

この方式を機能させるためには、2 つの条件（ポイント）がある。

1つは、通信制限を行う主体と対象である。SuperCSI ネットワークサービスは接続組織にスイッチを設置し、そのスイッチを責任分界点としている。そのため、スイッチの設定は 24 時間 365 日の監視体制を持つ通信事業者である SuperCSI の責任で行うことができる。組織が所有するスイッチの設定を運用保守業者に行わせる場合は、あらたに 24 時間 365 日の監視体制を構築する必要がある。また組織が所有するスイッチの設定を通信事業者に行わせる場合は、当該スイッチの管理や運用手順について詳細な打合せと契約が必要となる。

もう1つは、役割の適切な分離と分担である。ここで紹介する 1 次対応サービスは、大学から指定された情報に基づいて通信制限を行うだけである。与えられる情報の信頼性や具体的な内容には一切関知しない。そのため、インシデントの原因調査や関係するセキュリティ対策などは含まれない。これらはすべて大学の CSIRT で実施すべき役割である。通信事業者には契約に基づいて通信を許可し制限させることを徹底すべきである。本来負うべきでない役割を負わせようとすると、新たな契約やコストが発生することに注意して体制を構築することが重要である。

6.2. 総合大学における情報セキュリティ管理体制（富山大学）

総合大学における CSIRT 構築を実現するための取り組み事例として、富山大学の事例を紹介する。富山大学は、平成 17 年 10 月に 3 つの大学（旧富山大学、旧富山医科薬科大学、旧高岡短期大学）が合併して開学した大学で、3 キャンパス 8 学部を擁する総合大学である。セキュリティや運用ポリシの異なる大学の合併から始まり、現在の CSIRT 体制を構築するに至った経緯を以下にまとめる。

富山大学におけるセキュリティ体制の整備における経緯については、以下の 3 つの段階に分けて考えることができる。

・第一時代　　平成 17 年～平成 22 年
　第一時代では、全学統一認証基盤の整備を実施している。このシステムにより「だれが利用しているかを記録」することを実現している。また、総合情報基盤センターにおける利用規則において、情報機器におけるマルウェア対策や不正コピーの防止、P2P ファイル共有による著作権侵害へ対応するための利用細則を追加している。教育面では情報処理教科において情報倫理教育を開始したが、徹底には至っていない。

・第二時代　　平成 23 年～平成 27 年
　第二時代では、フィッシングメールによるマルウェアへの感染やポートスキャンによる攻撃が急増していたことを受け、本格的なセキュリティ対策を展開している。この時期、文部科学省からの通達もあったことから、情報セキュリティポリシの作成と CIO/CISO の任命を実施している。CIO と CISO には情報担当理事を兼任で任命し、セキュリティインシデントが発生した際のフローを明確にすることで迅速な初動対応を実現した（図 6.1-2）。これに合わせて、ネットワーク機器における通信ログの長期保存やフォレンジック機材の準備、脆弱性診断のための疑似攻撃の実施を総合情報基盤センターで実施し、「だれが何をしたかを記録する」体制に移行している。

　通信ログの収取に関しては、大学の法人としての法的な責任関係を説明する資料として保存することを目的として実施している。富山大学では、3 大学が合併した経緯から対外節部分の大学 FW と 3 つのキャンパスの入り口にキャンパス FW を設置して通信制御を実施している。通信ログの収集においては、一つの通信に対してキャンパス FW と大学 FW の二箇所で記録し、一つの記録に対して専用のログシステム（3～6 ヶ月保持）と syslog サーバ（1 年間保持）の二箇所で記録している。

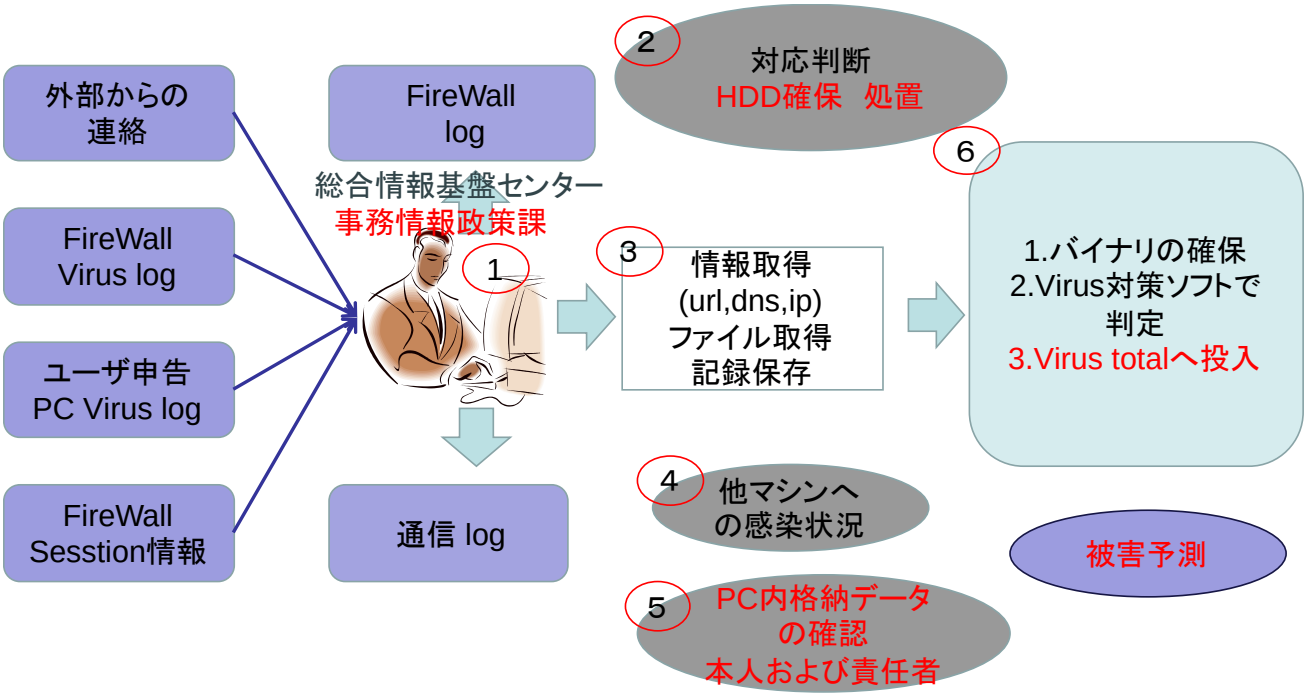

図 6.1-2　富山大学におけるセキュリティインシデント発見と判断フロー

　以上のように、本格的なセキュリティ体制の運用を開始したが、いくつかの課題が残った。一つは役員および構成員の情報セキュリティポリシに対する理解や遵守するためのインセンティブの

整理ができておらず、セキュリティ対策に対するコストの優先順位付けが不足していた点であり、もう一つは、監査体制や法的な責任体制が明確となっていない点であった。

・第三時代　　平成 28 年～

第二時代に残された課題を解決するべく、情報セキュリティに関する教育に力を入れている。役職員向けの情報管理・セキュリティハンドブックの発行や全構成員向けに e-Learning によるセキュリティ教育の導入を開始した。セキュリティ教育に関しては受講を義務付けており、未受講の場合にはペナルティが発生する。また、規則の整備を進め、大学規則集内に「情報」の項目を設け、情報セキュリティ対策の規則を明確に定義した。合わせて、CSIRT を組織し、情報セキュリティ体制を刷新している（図 6.1-3）。このように「組織的なセキュリティ体制の構築」を第三時代では目指して取り組んでいる。

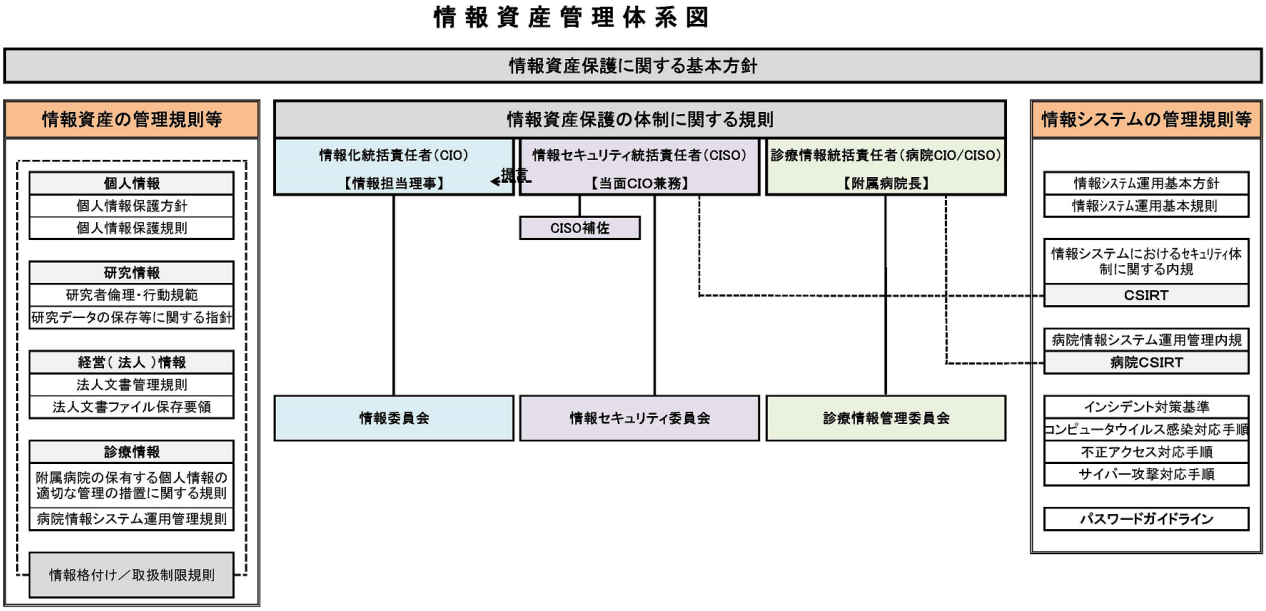

図 6.1-3 富山大学における情報セキュリティ体制図

ただし、情報セキュリティへの教育効果はまだまだ上がっておらず、どのようにルールの徹底を図るかが今後の課題となっている。また、インシデントは完全になくすことは不可能であり、設置した CSIRT による活動が必須となっているが、現在の構成員は1名と十分な人員を配備できておらず、体制改善に向けた努力を継続している。

6.3. 小規模大学における情報セキュリティ体制（鹿屋体育大学）

小規模な単科大学における情報セキュリティ対策事例として、鹿屋体育大学の取り組み事例を紹介する。鹿屋体育大学は、体育学部のみの単科大学で、学生数が約 800 名、教職員が約 180 名と全体で 1000 人に満たない小規模校である。大学内の情報システムについては、教育研究系のシステムを情報系センターであるスポーツ情報センターが、附属図書館を含む事務系のシステムを学術図書情報課情報システム係がそれぞれ集約的に管理・運営している。

鹿屋体育大学では、情報セキュリティに関する事項の最高責任者として最高情報セキュリティ責任者（CISO）を定めている。情報セキュリティに関する事項については常任委員会である学術情報・産学連携委員会の審議を経て CISO が定めることとしている。従って CISO もこの委員会から選出されている。CISO の下には、3 名の部局システム管理責任者（体育学部システム、事務局システム、対外接続および基幹システム）が定められ、各部局の情報システムおよびネットワークの管理責任を有している。各教員および各課室長はシステム管理者という位置づけで、それぞれの管理する情報機器の管理責任を有している。

情報セキュリティ対策の推進に関しては、情報セキュリティポリシーに則り、大学の中期目標・中期計画にも記載され、これらが年度計画に落とし込まれ実施されている。平成 29 年度実績では、情報セキュリティ運用計画、評価実施計画、監査実施計画、研修・教育実施計画の 4 つが実施された。

鹿屋体育大学では、平成 16 年に情報セキュリティポリシー基本方針が制定されて以降、情報セキュリティポリシーに関する業務は実質的に情報システム係 1～2 名とスポーツ情報センターの専任教員 1 名が担ってきた。しかし、情報系システムに関する通常業務が増大する一方で、情報セキュリティに関する業務も年々増加し、特にインシデントが発生した場合の対応や体制構築、教育や訓練、規則や手順書の整備などに苦慮していた。このような状況から、学長の意向により平成 29 年度に情報セキュリティ専任としてスポーツ情報センターに特任助教を配置し、情報セキュリティに関する取り組みを促進していくこととなった。

1 名の増員があったとは言え、増大する脅威への対策や遅れがちであった規則の整備など、課題は山積しており、余裕が生まれたわけではない。可能な限り制度や手続きの簡素化を目指し、例えば本学では CSIRT について新たに組織を設置するといったことはせず、それまでに定めていた連絡・対応体制をもってそれに変わるものと位置づけた。内部監査は、過去に情報システム係に在籍した職員を中心に監査業務を依頼し、外部監査としては県内の NPO 法人と連携するなど、他部署への協力体制も模索している。平成 30 年度の教職員向け情報セキュリティ教育については市販の e-Learning 教材の利用を試みているところである。

また、国立情報学研究所が提供する情報セキュリティに関わるサービスについては、NII-SOCS や UPKI 電子証明書発行サービスなどを利用している。文部科学省などが開催するセミナー等にも可能な限り職員を派遣し、情報や技術の収集を心掛けているところである。近年では国立大学情報系センター協議会や SS 研などの研究会などでも情報セキュリティをテーマに情報交換が行われることも多いが、そのような機会は普段、情報が入手しづらい我々にとって貴重な機会となっている。今後も関係各所と情報交換を図りながら、先進的ではなくても着実な情報セキュリティ対策を推進していきたいと考えている。

7. 著者情報

● 担当幹事	西村　浩二（広島大学）
● まとめ役	北口　善明（東京工業大学）
	武蔵　泰雄（熊本大学）
● WG メンバー	井上　俊治（富士通株式会社）
	岡村　耕二（九州大学）
	齋藤　彰一（名古屋工業大学）
	下園　幸一（鹿児島大学）
	園田　哲平（富士通株式会社）
	只木　進一（佐賀大学）
	長谷川　明生（中京大学）
	山下　眞一郎（富士通株式会社）
● オブザーバー	高倉　弘喜（国立情報学研究所）
● 事務局	甲斐　友一朗（富士通株式会社）
	松本　孝之（富士通株式会社）

（五十音順）

8. 謝辞

本ガイドライン執筆にあたり、富山大学の沖野浩二先生および鹿屋体育大学の和田智仁先生、石田元気先生から、所属大学における事例紹介を提供いただき、合わせてガイドラインに対するコメントをいただきました。ここに感謝の意を表します。

9. 参考資料

[1] 日本コンピュータセキュリティインシデント対応チーム協議会: CSIRT スタータキット. (オンライン) http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf.
[2] 勝村幸博: セキュリティ組織 CSIRT. 東京 : 日経 BP 社, 2015.
[3] 満永拓邦: 企業における情報セキュリティ緊急対応体制. (オンライン) https://www.ipa.go.jp/files/000039115.pdf.
[4] 国立情報学研究所: 学認連携 Moodle 講習サイト, りんりん姫. (オンライン) https://security-learning.nii.ac.jp/
[5] 日本データパシフィック株式会社: U-Assist コンテンツ　INFOSS 情報倫理 2018 版. (オンライン) https://www.datapacific.co.jp/u-assist/contents/mrl008.html
[6] 日本データパシフィック株式会社: U-Assist コンテンツ　教職員のための情報倫理とセキュリティ 2018 年度. (オンライン) https://www.datapacific.co.jp/u-assist/contents/fd002.html
[7] TrendMicro: インシデント対応ボードゲーム. (オンライン) https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=205.
[8] 富士通: 富士通セキュリティソリューションインシデント対応訓練サービス. (オンライン) http://www.fujitsu.com/jp/solutions/business-technology/security/secure/global-managed-security/incident-exercise/index.html
[9] 政府機関統一基準適用個別マニュアル群 https://www.nisc.go.jp/active/general/kijun_man_index.htm 本マニュアル群のうち「DM2-06 自己点検の考え方と実務への準備 解説書」および「DM2-07 情報セキュリティ監査実施手順 策定手引書」が 4 章に最も関連する文書である
[10] 経済産業省: 情報セキュリティ監査制度について http://www.meti.go.jp/policy/netsecurity/isaudit.html 一般企業や省庁等、汎用的に参考にできる情報セキュリティ監査全体について、詳細が記述されている
[11] 国立情報学研究所: 高等教育機関における情報セキュリティポリシー策定について http://www.nii.ac.jp/service/sp/ サンプル規定集（2015 年版補訂）の「C2401 情報セキュリティ監査規程」および「C3401 情報セキュリティ監査実施手順」が 4 章に関連する部分である
[12] Timothy Rooney: IP Address Management Principles and Practice, IEEE Press series on network management, Wiley-IEEE Press, 2011.
[13] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315 (2003).
[14] T. Narten and J. Johnson: Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID), RFC 6355 (2011).
[15] NICT: Digital Identity Guidelines -Authentication and Lifecycle Managemant-, NIST Special Publication 800-63B, 2017. (オンライン) https://pages.nist.gov/800-63-3/sp800-63b.html