京都大学における情報セキュリティ監査の取り組み

斎藤 紀恵 [1)], 片桐 統 [1)], 石橋 由子 [1)]

1) 京都大学 企画・情報部

i-s-office@iimc.kyoto-u.ac.jp

Information Security Audit at Kyoto University

Norie Saito [1)], Osamu Katagiri [1)], Yoshiko Ishibashi [1)]

1) Planning and Information Management Department, Kyoto University.

概要

京都大学は約 60 の部局から構成され、約 34,000 名の構成員が在籍している。現在は毎年情報セキュリティ監査（内部監査）を実施しており、書面監査と実地監査を併用する方式をとっている。本稿では、2006 年より各部局に対して実施している情報セキュリティ監査の取り組みの変遷と現在の監査について述べる。

1 はじめに

京都大学（以下、「本学」という。）では、情報セキュリティ監査規程に基づき、各部局に対して情報セキュリティ監査（以下、「監査」という。）を実施している。監査の実施主体は本学監査室で、監査実施者は主に情報セキュリティ担当の教職員である。

現在の監査方式は、限られた予算で実施可能な内部監査で、また人員にも限りがあることから、全部局を対象に書面監査を実施した上で、実地監査の対象を選定する方式をとっている。また、実施が求められる幅広い情報セキュリティ対策について詳しくチェックが行えるよう、毎年重点監査テーマを定め確認を行っている。

2 監査の実施方法の変遷

2.1 監査の目的と規程の制定

本学では、各部局において情報セキュリティ関連規程に則って適切な情報セキュリティ対策の実施体制を構築できていることを確認し、問題点があった場合は改善されることを目的として、2006 年より監査を開始した。なお、2009 年には監査の実施に関する規程として「情報セキュリティ監査規程」を策定した。

2.2 網羅的な内容の監査

2006 年に開始した監査は、基本的な情報セキュリティ対策を網羅的にチェックする内容であった。実施にあたっては、毎年数部局を抽出し、書面および実地監査を実施した。2013 年度までの 8 年間に、概ね全部局に対して監査を実施することができた。

2.3 監査方法の変更

2014 年度には、全部局を対象に、2013 年度までと同様に基本的な情報セキュリティ対策を網羅的にチェックする書面監査を実施し、回答内容等をもとに抽出した数部局に対して実地監査を行った。

2014 年度までの監査により、基本的な情報セキュリティ対策については各部局とも実施が進んできたことから、2015 年度からは年度毎に定めた重点監査テーマに沿った監査を実施するよう変更した。実施は、全部局を対象に書面監査を実施し、回答内容をもとに数部局を抽出して実地監査を行う方式とした。

3 現在の監査

今年度の監査の年間スケジュールを図 1、監査実施の流れと体制を図 2 に示す。例年、年度当初に監査計画を策定し、年度末までに最高情報セキュリティ責任者（情報担当理事）への監査報告を行った上で、指摘内容に関する改善計画の策定まで完了するよう実施している。

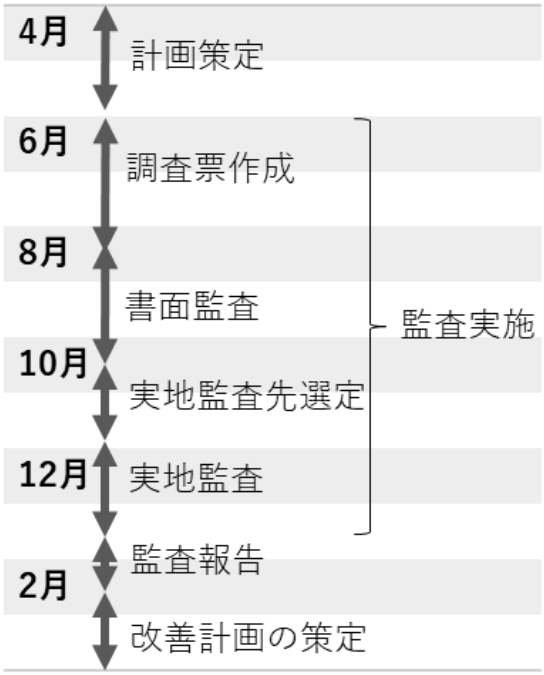

図 1 監査の年間スケジュール

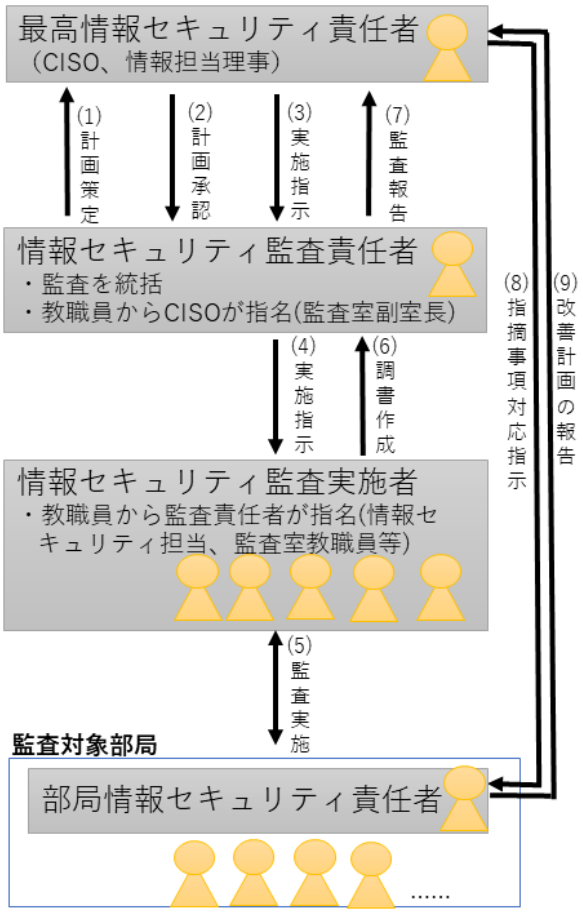

図 2 監査実施の流れと体制

3.1 監査計画の策定

年度毎に定めた重点監査テーマに沿った監査を行うため、監査計画の策定時に重点監査テーマを選定する。テーマは、当該年度に重点的に取り組みを推進したい項目や最近発生したインシデント（未遂含む）に関連する項目を中心に選定している。　　また、新しいルールが浸透されるよう、最近制定や改正を行った情報セキュリティ関連の規程等に関する内容も設定している。2015 年度以降の重点監査テーマを表 1 に示す。なお、重点監査テーマとは別に、前年度の監査で確認された課題についてはフォローアップとして毎年テーマに加えている。

表 1　2015 年度以降の重点監査テーマ

年度	重点テーマ
2015	・ 外部委託の状況 ・ 約款による外部サービスの利用 ・ 無線 LAN 構築時の措置
2016	・ 学内ネットワーク接続機器の把握 ・ パスワードガイドライン ・ 情報セキュリティポリシー実施手順書 ・ インシデント連絡網
2017	・ 情報システムログガイドライン ・ バックアップ ・ 情報セキュリティに関する情報伝達 ・ 部局公式 Web サイト ・ 部局公式メール ・ サポート終了後の OS 使用状況
2018	・ 情報セキュリティ連絡体制、周知 ・ 不正プログラム対策ガイドライン ・ 脆弱性診断の実施 ・ 情報格付け基準

3.2 調査票の作成

監査計画で定めた重点監査テーマに基づき、調査票を作成する。調査項目は、毎年確認を行っている情報セキュリティに関する連絡体制に関する 1 項目を除き新規に作成している。項目数はテーマによりばらつきがあるが、例年 30 項目前後となっている。表 2 に設問と回答選択肢の例を示す。

回答は、原則として選択式にしており、回答と合わせて回答の根拠となる資料の名称の回答を求めている。また、項目によっては、具体的な取り組み状況や問題がある場合の改善目途等も記入する欄を設けている。また、回答の選択肢については「できている」、「できていない」に相当する項目に加えて、比較的短期間で改善できる項目については「できていなかったため見直した」、最近制定されたルールに関する項目については

「年度末までに実施する」等の項目を設けて書面監査を改善のきっかけとなるよう工夫している。

表 2 設問と回答選択肢の例

<設問> 部局公式 Web サイトについて、担当する教職員は必要なバックアップを行っていますか。
<回答選択肢> 1. はい。行っています。 2. 行っていなかったため、この機会にバックアップを行うように見直しました。 3. 行っていません。(補足欄に理由、改善の目途を記入してください)

3.3 書面監査の依頼

監査責任者より調査票を各部局に配布し、回答を依頼する。回答にあたっては、大規模部局でも確認等の時間が確保できるよう、1 か月以上の十分な期間を設けるようにしている。

3.4 実地監査先部局の選定

各部局からの回答内容をとりまとめた上で、実地監査先の部局を選定する。対象の部局数は、3～4 部局程度である。選定にあたっては、特徴ある取り組みを行っている部局や、回答内容に問題がある部局に限らず、様々な傾向の部局からバランスよく抽出するようにしている。

3.5 実地監査

実地監査は、監査担当者（4～5 名程度）が各部局に直接赴いて行っている。監査にあたっては書面監査の調査票に記入された内容を確認し、詳しい状況を確認するとともに、回答の根拠とされた資料の確認を行う。さらに、実際の機器やサーバルーム等の現地確認を行う場合もある。

3.6 監査報告と改善計画

実地監査の完了後、書面監査の内容と合わせて監査報告書を作成し最高情報セキュリティ責任者（情報担当理事）に報告を行う。報告書では、「課題および問題点」のほか「助言的意見」についても記載し、各部局が情報セキュリティ対策の向上に活用できるようにしている。

実地監査の対象部局に対しては、当該部局の監査に関する報告書を送付した上で、「課題および問題点」について改善計画の策定を求め、期日までに報告するよう依頼している。

書面監査については、全部局の部局長（部局情報セキュリティ責任者）から構成される全学情報セキュリティ委員会で結果を報告しセキュリティ対策をさらに進めるよう依頼するとともに、「課題および問題点」については、次年度の監査でチェックを行っている。

4 おわりに

本稿では、本学における情報セキュリティ監査の状況について述べた。書面監査は全部局に対して毎年実施しているが、監査を担当できる教職員は限られており実地監査を行える部局は数部局に留まっている。また、監査の単位となっている部局の規模や体制（情報担当の教職員の有無や一元的な管理を行っているか等）についても様々である。

本学全体として情報セキュリティ対策のレベルアップを図り、重大インシデントの発生を未然に防ぐことができるよう、限られた予算、人員でどのような監査を行うのが最適か、継続的に見直しを行う必要がある。さらに、状況によっては予算を確保した上で、外部監査の併用も検討していきたい。

本稿で紹介した本学の監査の状況が、各大学で実施する監査の取り組みの参考となれば幸いである。