情報セキュリティ対策について

企画・情報部 情報基盤課 セキュリティ対策掛
戸田 庸介

１．　はじめに

文部科学省より令和元年 5 月 24 日付け元文科高第 59 号「大学等におけるサイバーセキュリティ対策等の強化について(通知)」が示され、国立大学法人にはサイバーセキュリティ対策等基本計画の策定が求められています。京都大学でもサイバーセキュリティ対策等基本計画を令和元年 9 月 25 日役員会決定しました。先端的な技術情報等を含む研究データをサイバー攻撃等の脅威から保護する項目が追加されており、研究データの管理においても情報セキュリティ対策の重要性が増していくものと思われる。

本講義では、京都大学のセキュリティポリシーと体制を説明する。次に、セキュリティ対策掛の業務であるネットワークログ監視からスパイウェア活動のログの紹介し、最後に本学で発生したインシデント事例とその対策について紹介する。

２．京都大学のセキュリティポリシーと体制について

情報セキュリティ関連規程等の体系はポリシー、スタンダード(規程、基準)、プロシージャ(手順、ガイドライン)の三階層のピラミッド構造となっている。

頂点のポリシー部分に位置付けられるのは、4 つの条項からなる「京都大学における情報セキュリティの基本方針」と 7 章 18 つの条項からなる「京都大学の情報セキュリティ対策に関する規程」(以下、「対策規程」とする)である。

対策規程第４条～第８条には、全学の組織体制について定義されている。(図１)

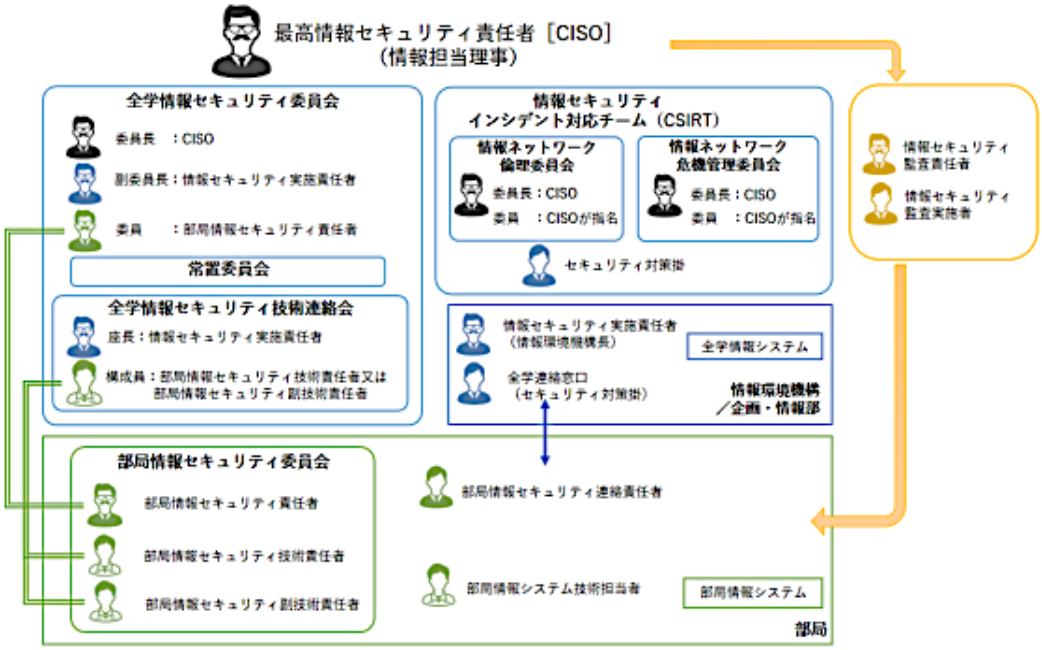

図 1　全学体制図

図中の CSIRT とは Computer Security Incident Response Team の略称であり、情報セキュリティでインシデント発生時に対処するチームのことを示す。インシデント発生時には情報環境機構サイト(http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/husei/)にコンピュータ不正アクセス対応連絡要領から情報セキュリティインシデント報告書まで掲載している。モバイル端末の普及により BYOD (Bring your

own device)化が進んでおり、コンピュータ不正アクセス対応連絡要領について情報資産の明確化を行う改訂を行ったことについても紹介する。

３．セキュリティ対策掛の日常業務について

セキュリティ対策掛の日常業務について下記に箇条書きで報告する。講義の中では実際の外部からの攻撃のログやマルウェア感染時のログを紹介する。

- インシデント対応
- セキュリティ監視装置より、学内と学外との通信を監視
- 情報セキュリティ関連の講習会等
- セキュリティ情報の掲載・周知
- 脆弱性情報やセキュリティアップデート情報を取得
- セキュリティ e-Learning の運用
- 脆弱性診断システムの運用
- 情報セキュリティ関連委員会（後述）の運営
- 本学情報セキュリティポリシー等関連規程の改訂
- 情報セキュリティ監査の実施（監査室が主体）
- 情報環境機構の情報セキュリティ対策の推進
- 情報セキュリティ関連の問い合わせ対応
- 不審メール問い合わせ(SandBox)

４．インシデント紹介とパスワードポリシーの遵守について

2019 年 3 月に発生した 2 件のインシデントの概要について紹介する。1 つはパスワード使い回しが原因となるインシデントであり、JPCERT/CC（Japan Computer Emergency Response Team/Coordination Center）のサイトで「STOP! パスワード使い回し!キャンペーン 2019」(http://www.jpcert.or.jp/pr/stop-password.html)について説明する。また、覚えやすいパスワードの作り方についても紹介する。

もう 1 つはフィッシングメールに関するインシデントであり、メールで注意すべき事について紹介する。