情報セキュリティインシデントの発生状況と対策について

情報セキュリティインシデントの発生状況と対策について

情報システム室　片上伸夫

１．はじめに

情報セキュリティインシデントとは、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のことをいう。

JNSA（日本ネットワークセキュリティ協会）セキュリティ被害調査ワーキンググループが公開している、平成 27 年の 1 年間にインターネット上に公開された個人情報漏洩インシデント情報を対象とした調査（速報版）結果によれば、約 800 件のインシデントが発生している。これらの発生原因については、外部からの不正アクセス、管理ミス、不正な情報持ち出し、盗難など様々である。

表 1：平成 27 年個人情報漏洩インシデント概要データ（速報）

漏洩人数	4,960,063 人
インシデント件数	799 件
想定損害賠償総額	2541 億 3663 万円

（※JNSA より公開されている内容より抜粋）

表 2：平成 27 年個人情報漏洩インシデント　トップ 10

No	個人情報漏洩人数	業種	原因
1	101 万 4653 人	公務	不正アクセス
2	69 万 4217 人	金融業、保険業	管理ミス
3	68 万人	公務	不正持ち出し
4	26 万 7000 人	情報通信業	不正アクセス
5	20 万 9999 人	卸売業、小売業	不正アクセス
6	18 万人	公務	不正な情報持ち出し
7	14 万 2000 人	公務	内部犯罪・内部不正行為
8	13 万 1096 人	卸売業、小売業	不正アクセス
9	11 万 4400 人	医療、福祉	盗難
10	10 万 7368 人	製造業	不正アクセス

（※JNSA より公開されている内容より抜粋）

幸いなことに、本学では深刻な情報セキュリティインシデントは発生していないが、本学も上記のようなことが起こりうる環境にあることを認識し、本学が有する個人情報をはじめとした重要な情報の漏洩の防止や、無意識のうちに情報漏洩やデータの不正アクセスを行なわないための対策が必要であり、外部からの不正アクセスの防止の仕組みの導入と運用、学生・教員・職員への情報セキュリティに関する継続的啓発が重要であ

る。

２．平成 27 年度に本学で発生した情報セキュリティ事案

個人情報の入った USB メモリの紛失事案 1 件と軽微な事案 4 件が発生し、前者については報道提供することとなった。これらについては、情報システム委員会にて情報を共有し対策を検討し、再発防止策を実施している。

報道提供した事案とその後の対策については以下の通りである。

(1) 概要

・羽曳野キャンパス事務所内において、学生等の個人情報（過去の入学試験についての志願者、合格者等）が記録されている USB メモリ 1 個が所在不明となった。
・職員が、自分の机上にあるパソコンに USB メモリを接続した状態で業務を行い、業務終了後、USB メモリを自分の机の施錠ができない引き出しにしまったが、2 日後、引き出しを確認したところ、USB メモリがなくなっていることに気づいた。引き出しの中や机の周辺等を捜し、事務所内だけでなく、当該職員が出入りした学内の関係場所を全職員で捜したが、見つからなかった。
・本件による情報漏洩、及び漏洩による被害は報告されていない。

(2) 対応

・大学ホームページに、理事長・学長名で事実関係の説明とお詫びの文書を掲載した。
・在学生向けの掲示板（羽曳野キャンパス構内）に、理事長・学長名で事実関係の説明とお詫びの文書を掲示した。
・当該名簿に記載されていた入試志願者、合格者、大学院資格審査申請者に対して、理事長・学長名で事実関係の説明とお詫びの文書を送った。

(3) 再発防止策

・羽曳野キャンパス事務所において職員を臨時に招集し、所長から情報セキュリティに関する業務実施手順書の厳守について改めて徹底を命じた。また、羽曳野キャンパス事務所保有の USB メモリの使用状況について速やかに調査し、集約・データ移行の後、原則、USB メモリは使用しないよう命じた。
・本学全教職員に対しても同様に、理事長・学長より情報セキュリティに関する業務実施手順書の厳守について徹底を命じた。
・各事務課での USB メモリの利用実態を調査し、その結果もふまえ、すべての事務課において、情報共有サイト等サーバへのファイル保管を用いることにより原則として USB メモリを使用しないこととし、やむを得ず利用せざるを得ない場合は所属長の承認を得た上で、必ず暗号化機能つき USB を使用すること、さらに、USB の所在の管理を行うことをルール化した。

３．情報システムにおける情報セキュリティ対策について

現在稼動中の共通基盤システム、キャンパスネットワークにおいては以下の対策を施している。

・Firewall、SPAM 対策装置の設置
・事務端末へのウィルス駆除ソフトのインストールと更新、パターンファイルの自動更新の仕組み
・ウィルス駆除ソフトのダウンロード可能な環境の整備
・外部情報発信コンテンツがある各部局サーバについて、「大学標準 Web サイト作成・集システム（標準 CMS)」への移行推進によるサーバの一元化
・持ち込み端末の検疫チェックの実施
・キャンパスネットワークシステム接続時の認証システムの導入
・ハードディスクの情報消去のための磁気破壊装置の学術情報センター内の設置と利用など

現在、平成 28 年度 10 月から利用開始すべく、共通基盤システム・キャンパスネットワークの更新の準備を進めつつあるが、上記の対策を継承すると共に、次世代ファイアーウォール（Palo Alto）の導入により、従来の Firewall よりも細かな制御を行い、Bit Torrent をはじめとした P2P ソフトウェアを原則使用不可とする予定である。

４．学内での情報共有

学外からの不審なメールを受信した場合などには、全学に注意喚起を行うための通知文を学内ポータルに掲載している。平成 27 年度は、9 回の掲載を行った。

表 3：情報セキュリティに関する通知の学内ポータル掲載状況

	月日	表題	内容
1	7/27	情報セキュリティの確保について（通知）【学内ポータル掲載】	USB 等外部記憶装置の取り扱い、暗号化などについて
2	7/29	不審なメール受信時の対応について【学内ポータル掲載】	スパムメール、フィッシングメール等不審メール受信時の対応について
3	7/30	学内メールアドレス詐称メールに関する注意喚起【受信者へのメール発信】	学内メール宛に、教職員・学生のメールを騙る不審メール受信時の注意事項について
4	8/12	（再通知）不審なメール受信時の対応について【学内ポータル掲載】	スパムメール、フィッシングメール等不審メール受信が散発しているため再通知

5	12/16	（注意喚起）不審な電子メールについて【学内ポータル掲載】	12/8 に発生した不審メールに関する注意喚起
6	1/14	不審なメール受信時の対応について【学内ポータル掲載】	日本郵便を騙った迷惑メール受信時などの対応について
7	1/28	映画の不正ダウンロード及びメール転送設定に関する注意喚起【学内ポータル掲載】	映画の不正ダウンロードに関する警告などの事案に伴う注意喚起
8	2/4	（お願い）不審なメール受信時の対応について【学内ポータルの掲載】	りそな銀行を騙った迷惑メール受信時などの対応について
9	3/17	情報の取り扱いに関する注意喚起【各学域長・研究科長へのメール】	学生に対し、映画の不正ダウンロードに関する警告などの事案に伴う注意喚起を要請

５．今後

情報セキュリティインシデントの発生を抑止するためには、情報システム上の技術的な仕組みによる防止策と共に、本学に所属する学生、教員、職員全員が情報セキュリティに関する関心と見識をもつことが重要である。このためには、情報セキュリティに関する研修の実施や、情報セキュリティ対策やインシデントに関する全学的な情報共有を引き続き行っていき、情報キュリティに関する風土つくりを、今後も地道に行っていくことが重要である。

また、今後の大阪市立大学との法人統合、新大学の設立に向けての情報基盤、ネットワークの検討においても、情報セキュリティポリシーの統合、それをふまえた情報システム上でのセキュリティ確保の仕組みの構築と、関係者全員の情報セキュリティに関する啓発を行っていくことが重要である。

以上