2. 情報セキュリティアンケートから見た日常に潜むセキュリティリスク

情報メディア基盤センター　上繁　義史

1. はじめに

長崎大学には，ネットワーク，情報機器，電子ファイルの情報，紙媒体の情報など，多種多様な情報資産があり，その内容や量も日々変化している。この状況を念頭に，本学では，第二期中期目標において「情報マネジメント体制を整備し，情報セキュリティを向上させる」ことを掲げており，平成 23 年度の年度計画で「本学の情報資産に対するリスク分析を行う」ことを挙げていた。そこで，平成 23 年 12 月より平成 24 年 2 月まで，全教職員を対象に「情報セキュリティアンケート」を実施し，これらの情報資産の管理･運用に関する現状とそこに潜むセキュリティ上のリスクを調査した。以下，アンケートの方法及びその結果について報告する。

2. アンケートの方法

アンケートの内容は情報セキュリティ専門部会での検討を経て，平成 23 年 12 月 21 日に全教職員に対して「情報セキュリティアンケートの実施の協力について」と題して，アンケートへの回答をお願いするメールを送付した。アンケートへの回答は，同メールにて指定した URL にアクセスし，図 1 に示すような Web フォームへの入力により行った。設問は情報資産の保有状況や管理・運用状況など，全部で 9 分野 40 問であった。回答を平成 24 年 2 月 3 日に締め切った。

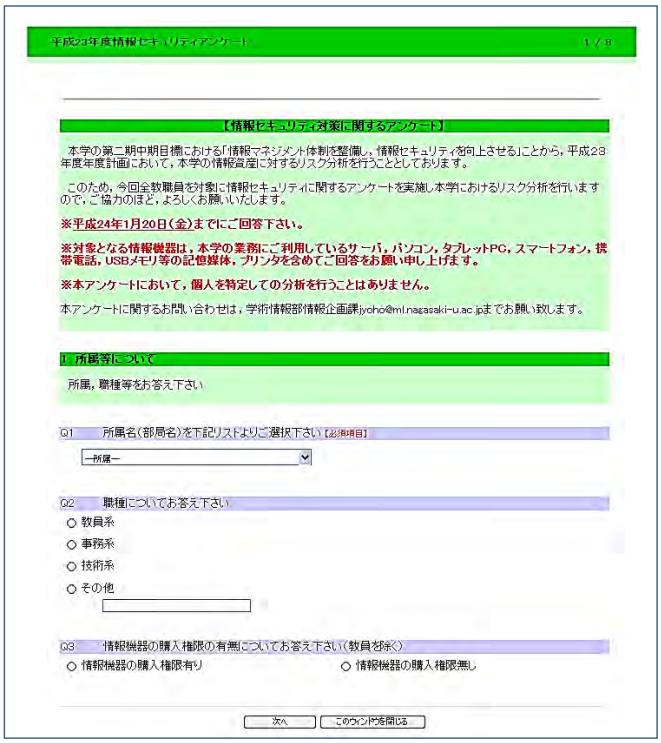


図 1　情報セキュリティアンケートの回答入力画面

アンケート対象の教職員の人数は常勤教員 1,158 名，常勤職員 1,609 名，非常勤教職員 1,207 名，合計 3,974 名（平成 23 年 12 月現在）に対して，アンケートの回答総数は 471（全教職員の 11.9%（母数を常勤教職員に限定すると 17.0%））であった。

アンケートの全回答について集計・リスク分析を行い，対策についての検討を加え，その結果を以下の会議等で報告した。その後「情報セキュリティリスク分析に関する報告書」として，学内に開示した。

- 情報セキュリティ専門部会（平成 24 年 3 月 6 日）
- 情報メディア基盤センター運営委員会（平成 24 年 3 月 13 日）

- 学長･副学長会議（平成 24 年 3 月 13 日）
- 情報政策委員会（平成 24 年 3 月 15 日）
- 連絡調整会議（平成 24 年 3 月 16 日）

3. アンケート結果から見えた日常のリスク

アンケートでは，多岐にわたる質問を行ったが，本誌が大学の内外に広く公開される性格に鑑み，一般的と思われる話題に絞って述べていく。詳細については，「情報セキュリティリスク分析に関する報告書」を参照されたい。

3.1. 資産の管理不足による紛失･盗難のリスク

以下の設問に対する回答として図 2 のような結果を得た。

> Q 下記の機器を無くしそうになったことがありますか？（いわゆる“ヒヤリ・ハット”の経験も含む）
> (1) ノート PC・タブレット PC　選択肢（はい，いいえ，持っていない）
> (2) USB メモリ　選択肢（はい，いいえ，持っていない）

ノート PC・タブレット PC については，ヒヤリ・ハットを含めても，無くしそうになった経験は少ないことから，紛失のリスク自体は低いものとみられる。しかしながら，今後のリスクが 0 になったわけではない。

USB メモリについては，別の設問から教員系の回答者に持ち歩くケースが多い傾向が分かっており，その分だけ無くしそうになる経験が多いものと思われる。実施すべき対策と

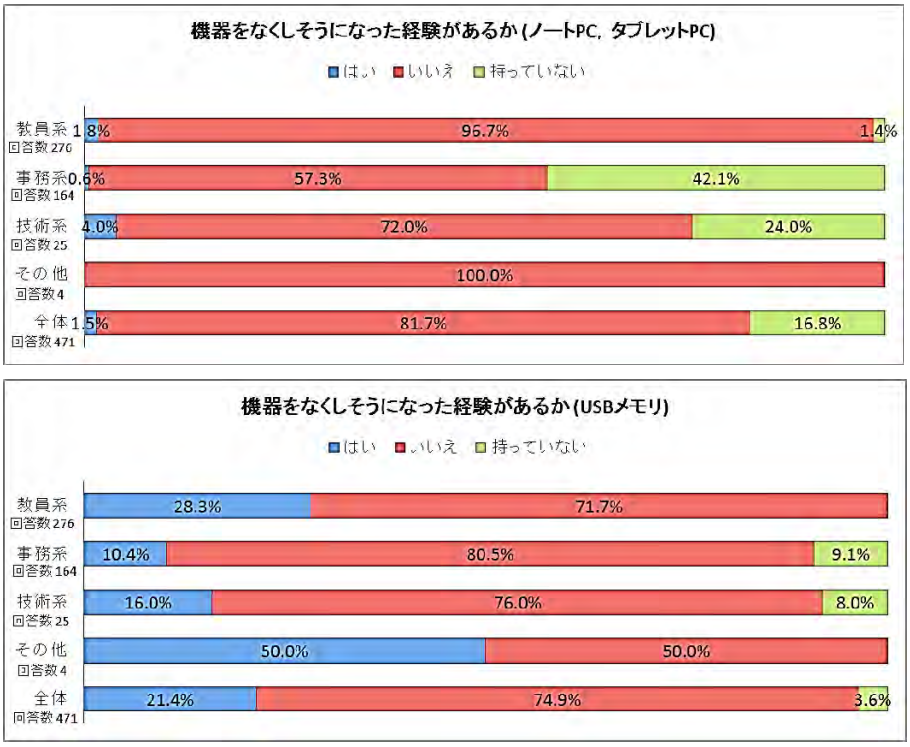


図 2　集計結果（機器を無くしそうになった経験）

して，以下の項目を考慮すべきである。

- 機器に重要な情報を格納しない
- ノート PC の HDD 全体を暗号化する
- 使わないときには鍵付きの場所にしまったり，部屋から出るときに施錠したりするなど，「保有者以外に扱えない」ように運用する
- USB メモリを外部に持ち出すときにストラップをつけて首にかけるなどして，紛失防止をはかる
- ハードウェア暗号化，ウイルス対策，指紋認証など，セキュリティ機能を持つ USB メモリを使い，紛失時の情報漏洩を防ぐ

3.2. PC，USB メモリ，タブレット端末等を媒介したウイルス感染と拡大のリスク

セキュリティパッチ適用及びウイルス対策に関する意識について，以下のような質問を行った。

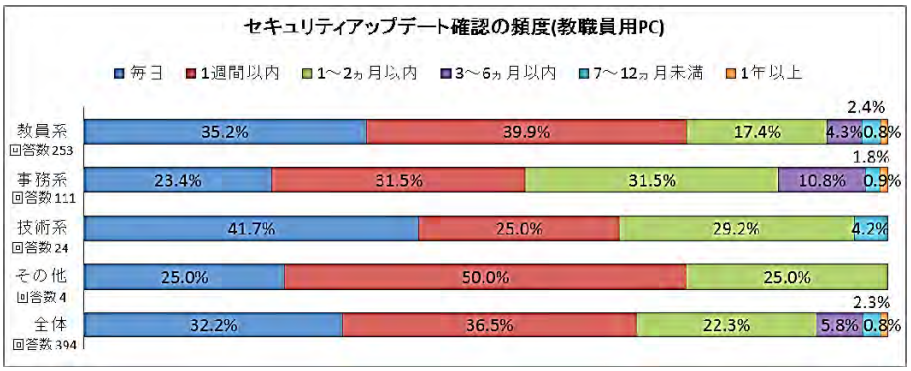
Q 教職員の PC や自ら管理している PC のセキュリティアップデートの確認頻度で，最も近いものを答え下さい。
選択肢（毎日，1 週間以内，1～2 ヶ月以内，3～6 ヶ月以内，7～12 ヶ月未満，1 年以上）
Q 教職員の PC や自ら管理している PC のウイルス対策ソフトの確認頻度で，最も近いものを答え下さい。
選択肢（毎日，1 週間以内，1～2 ヶ月以内，3～6 ヶ月以内，7～12 ヶ月未満，1 年以上）

セキュリティアップデート確認の頻度については，図 3 のとおり，全体では「毎日」(32.2%)と「1 週間以内」(36.5%)で 68.7%を占めており，頻繁に確認するとの回答が多かった。その一方で 0.8%「1 年以上」と回答しており，確認の頻度が少ない人もいることがわかった。ウイルス対策ソフトのアップデート確認の頻度についても，概ね同様の傾向が見られた。

自動更新をキャンセルするなど，セキュリティアップデートが適切に行われない場合には，標的型攻撃や PC 等端末の乗っ取りといったリスク，端末内のデータ窃取のリスクが高まる。他にも OS やソフトウェアの脆弱性を悪用した攻撃に晒されるリスク，ネットワーク内の他の PC 等に感染を拡大させるリスクなどが高まる。

Windows 系 OS や Microsoft Office 系ソフトウェアでは定期的（月 1 回以上）に自動更新が行われている。Adobe Reader，Adobe Flash Player や Java など，脆弱性を悪用されやすいソフトについても不定期ながら自動更新がなされる。その他注意すべきソフトウェア（ブラウザなど）については，JVN (Japan Vulnerability Notes)の Web サイトで公開されている MyJVN (http://jvndb.jvn.jp/apis/myjvn/index.html)を利用することで更新状況を確認することができるので，確実なアップデートを行う習慣が必要である。

多くのウイルス対策ソフトはアップデートをタイマー設定できるので，勤務時間かつ PC が起動している時間帯に設定することを推奨する。定期的なウイルスチェックの実施（例えば週 1 回以上）も併せて推奨したい。



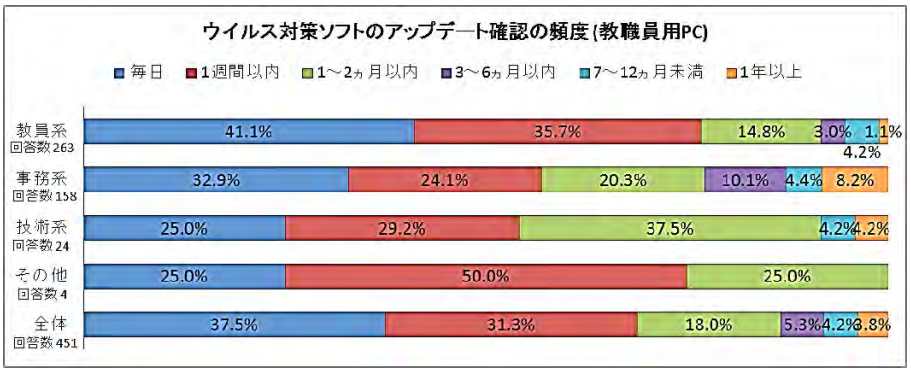


図 3　集計結果（アップデートの確認頻度）

3.3.　なりすまし等によるシステムの不正使用のリスク

Q　PC や業務システムのパスワードは，アルファベットと数字を混在させ文字数を長くする等，推測されにくいものを設定していますか？
　選択肢（はい，いいえ，該当なし（PC や業務システムを扱わない））

集計結果は図 4 のようになった。「はい」との回答が全体の 84.9%にのぼり，ある程度パスワードに関する考え方が浸透していると考えられる。その一方，「いいえ」との回答が 14.2%見られた。パスワード変更の頻度が低い場合，パスワード解析が成功するリスクを抱えていることになる。

対策として,「推定されにくいパスワードの設定」と同時に「パスワードの定期的な変更」を行うことが必要不可欠である。パスワードに関する対策は基本的に教職員個々人にお願いするしかないのが実情である。最近は ID とパスワードを管理するためのフリーソフトもあり，従前に比べて管理が容易になってきている。このような仕組みを利用するなどし

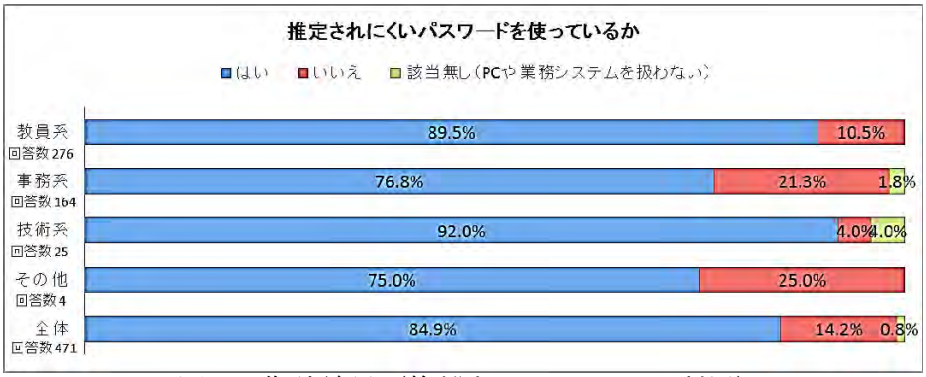


図 4　集計結果（複雑なパスワードの利用）

て，適切に管理することが必須である。

組織的な対策としては，定期的なパスワード変更の啓発を行うとともに，一定期間パスワードの変更がない場合に，強制的にパスワード変更を行う仕組みを運用するなどの対策が考えられる。

パスワードの管理状況について，以下の設問で尋ねた。

Q　ID やパスワードの管理状況についてお答え下さい（複数選択可）
選択肢（
すぐ見られるところに付箋紙を貼ったり，メモを置く等している
手帳に書いている
PC 等の電子ファイルにメモしている
PC やシステム，ブラウザ等に覚えさせている
頭に記憶している
他人に管理してもらっている等，自分の ID やパスワードはよくわからない　）

図 5 に示すように，基本的に「頭に記憶している」との回答が最も多く，全体で 38.4%となっている。「手帳に書いている」(23.5%)，「PC 等の電子ファイルにメモしている」(19.9%)との回答がこれに続いているが，誰の目にも触れる性質のものでない限り，脆弱性は必ずしも高くない。一方，「すぐ見られるところに付箋紙を貼ったり，メモを置く等している」(9.9%)については，端末の設置環境によっては，誰でも見られる可能性があるため，脆弱性の程度が高くなると考えられる。また，「PC やシステム，ブラウザ等に覚えさせている」(8.2%)については，パスワードの入力を省略することになるため，当該 PC にアクセスできれば，同時に各種システムにアクセスすることが可能となる。したがって，左記の例よりも脆弱性の程度がさらに高いと言える。ごくわずかの回答数であるが，「他人に管理してもらっている等，自分の ID やパスワードはよく分からない」が 0.2%あった。基本的に ID は個人にひも付いているので，管理責任の主体が ID 所有者個人である点を十分認識する必要がある。

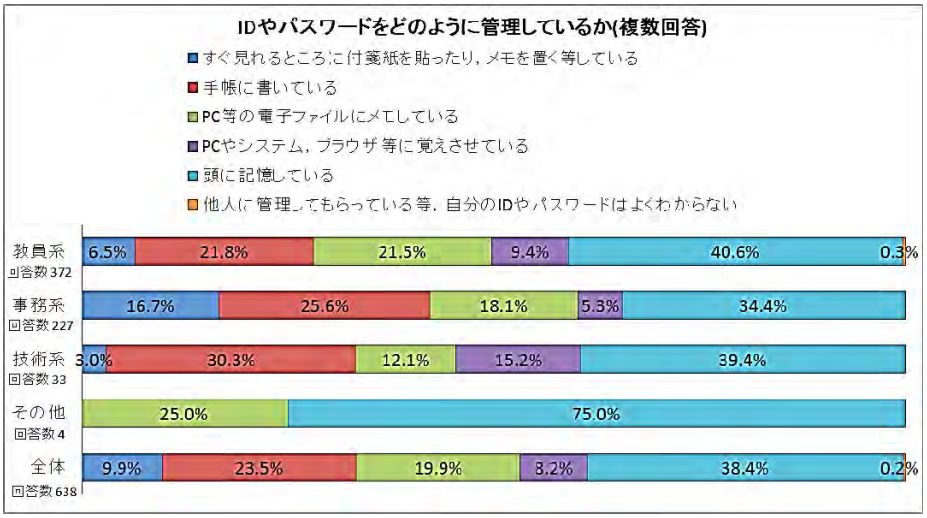


図 5　集計結果(ID・パスワードの管理状況)

基本的な対策としては，

- モニタにメモを貼り付けるなど，他人の目に直接触れるような所に放置しない
- PC やブラウザ等にパスワードを記憶させない
- 暗記することが望ましい
- ID・パスワードの管理ツールを利用して，安全に保管する

などを行うべきである。

3.4　ファイル共有サービスによる情報漏洩・改ざん・消失のリスク

学外のファイル共有サービスの利用状況について以下の質問を行い，図 6 のような集計結果となった。

> Q　利用している共有フォルダ又は共有サービスの存在場所についてお答え下さい（複数選択可）
>
> 選択肢（学内（部局内），学内（部局外），学外）

回答者全体の 78.3%が「学内（部局内）」，6.4%が「学内（部局外）」と回答しており，各部局や研究室にてネットワークアクセスが可能なストレージが設置されているためとみられる。一方，15.3%が「学外」と回答している。学外サービスを利用する傾向は教員系において顕著であった。

共有フォルダ又は共有サービスにおけるリスクとしては，ウイルス対策が不十分な場合，ウイルス等に感染したファイルの共有による感染拡大が挙げられる。回答者の過半数が利用している状況があることから，このリスクは十分に考慮すべきである。また，アクセス制御が十分活用されていない場合，なりすましなどの不正アクセスのリスクが考えられる。

特に学外サービスについては，以下のリスクを考慮する必要がある。

- 保存したファイルのセキュリティ維持を利用者が直接行えない（アクセス権の設定ができても，システム維持については利用者にはできない）
- サービス停止時のファイルの取り扱いが不透明（特に企業買収など，事業が継続されるかがサービス提供者側の状況に依存する）
- サービス提供者側の従業者のセキュリティが不透明

管理者の対策としては，サービス開始時に

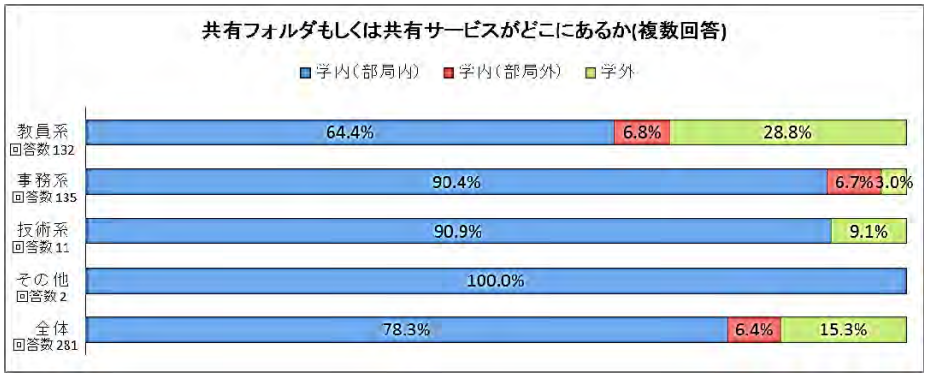


図 6　集計結果（共有フォルダ・共有ファイルの利用）

- ウイルス対策ソフトの利用やセキュリティアップデートといったソフトウェア対策
- ユーザ管理やフォルダ･ファイルへのアクセス設定といったアクセス制御
- 装置の一部もしくは全部の故障に備えた冗長化

などの対策を取ることが考えられる。

利用者の対策としては,

- 適切なパスワードを利用し，定期的にパスワードを変更する
- 機密性の高い情報を部局内等で共有する場合には，パスワードを設定するなど，ファイルを暗号化する。
- ファイルにアクセス権（閲覧，更新の許可･不許可）を設定し，情報の更新状況を管理する。

学外サービスについては，上述のリスクにより，業務や研究に関する情報共有の手段としては利用しないことが望ましい。利用者が学内に限られるのであれば，グループウェアやネットワークストレージなどの仕組みを適切に活用することにより，情報漏洩のリスクを低減することも可能となる。

学外との情報共有など，学外サービスを利用せざるを得ない場合には，サービス提供者の SLA（サービスレベルアグリーメント）を確認の上で，ユーザ管理やアクセス権限の設定を厳格に行うとともに，共有する情報を暗号化したり，必要最低限の利用にとどめたりするなど，細心の注意が必要である。

3.5　メール転送による情報漏洩のリスク

本学ドメインのメールアドレスに届いたメールの転送について以下のような質問を行ったところ，図 7 のような結果となった。

Q　学内のメールアドレス（例：@nagasaki-u.ac.jp）に届いたメールを，学外（個人所有のアドレス）に転送していますか？
選択肢（はい，いいえ，該当無し（学内のメールアドレスを持っていない））

Q　転送したメールを読む主な機器についてお答え下さい
選択肢（PC，タブレット PC（iPad, Android, Windows 等），携帯電話（スマートフォン含む））

※　上の設問で「はい」と回答した人が対象

図 7 より，転送の利用は教員系に多い傾向（39.1%）が分かった。転送したメールを読む機器としては， PC が 72.7%と最も多く，スマートフォンを含む携帯電話が 22.7%，タブレット PC が 4.5%となった。学内のメールシステムでは Web メールが推奨されているが，従前からのメール環境を使い続けるケースが多いためと考えられる。

メールの転送によるリスクとしては，情報漏洩・ウイルス等感染拡大が挙げられる。更に，メール送信者（転送メールの送信）側，メール受信者（転送メールの受信）側，転送したメールを受信するメールサービス提供者について，以下のようなリスクも考えられる。

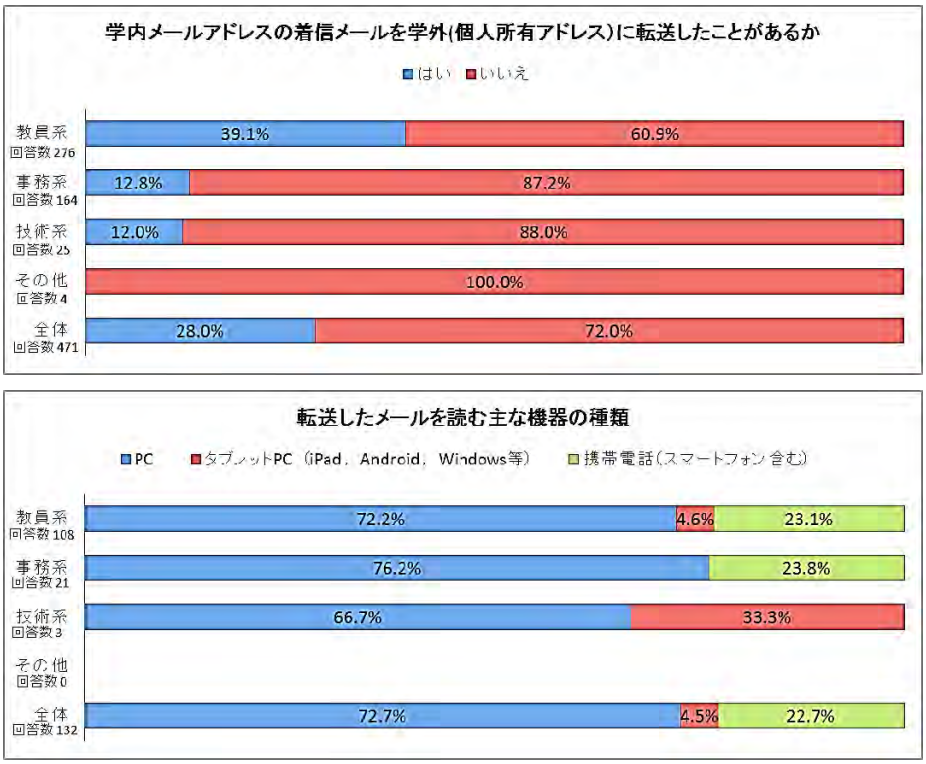


図 7　集計結果（メール転送の状況）

(1) メール送信側（転送メールを送信する側）

- 転送するメールがウイルス等を含む場合に転送先にウイルス等の感染を拡大させるリスクがある。多くの場合には，何らかのメールセキュリティの仕組みで防止できるが，未知の脆弱性をついた攻撃（ゼロデイ攻撃）などを抑止できないことがある。
- メール転送を PC のメールクライアントソフトから行っている場合に，PC がウイルス等に感染して，転送メールに不正なコードを埋め込んで送信することが考えられる。

(2) メール受信側（転送メールを受信する側）

- PC やタブレット端末（スマートフォン含む）のソフトウェア等の脆弱性対策が不十分な場合に情報漏洩のリスクが高まる。特に Android 系端末については，ウイルス発見の件数が増大しており，十分な注意が必要である。

(3) メールサービス提供者（転送したメールを受信するメールサーバ側）

- ID・パスワードの情報漏洩によるアカウントの乗っ取り（放置されたメールアドレスを持っている場合に特に注意）
- 脆弱性を突いた第三者の攻撃による不正なメールデータの取得（一部の学外サービスで過去実際に発生）

最も有効な対策は，転送自体を行わないことである。しかしながら，業務上不可避と考えられる状況もあるので，最低限の対策として，以下のようなことを行うべきである。

- PC，タブレット端末，スマートフォンにおいて，ウイルス対策ソフトをインストールし，確実にアップデートを行う

- PC，タブレット端末，スマートフォンにおいて，OS やアプリのアップデート確認を定期的に行う
- 自動転送を行う場合，転送のルールを設定するなどして，機密性の高い内容が転送されないようにする

3.6　セキュリティ教育の不徹底によるリスク

本学では平成 21 年 2 月に情報セキュリティポリシーの第 3 版を発行している。これに関連して，以下のような質問を行い図 8 のような結果を得た。

Q　長崎大学の情報セキュリティポリシー（第 3 版）を知っていますか？
選択肢（はい，いいえ）

現行の情報セキュリティポリシーがアンケート実施の時点で改訂から約 3 年経過していたにもかかわらず，認知度が極めて低いことが明らかとなった。この状況から考えられるリスクとしては

- 組織的なセキュリティ対策基準の共通理解が進まない
- 対策の必要な箇所に対策がなされない
- 必要以上に対策を取ろうとして過剰投資を生じる

といったことが考えられる。対策としては，全学的に再読を促すと共に，適宜セキュリティポリシーに関する講習会や FD を開催して啓発することが挙げられる。

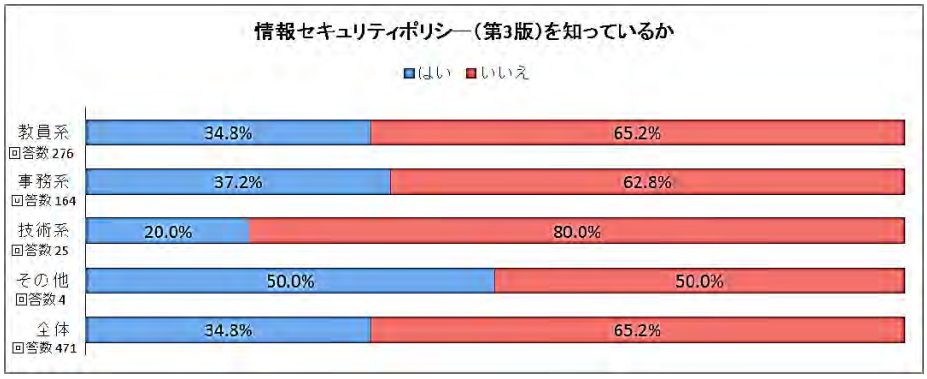


図 8　集計結果（セキュリティポリシーの周知状況）

4.　まとめ

本報告では，情報セキュリティアンケートの集計結果に基づいて，長崎大学におけるセキュリティ上のリスクの現状及び実施すべき対策について考察を行った。今後のアンケートについて回答しやすい手法を検討すると共に，広くセキュリティ意識向上と実効性担保をはかっていく方法について検討する予定である。

謝辞

情報セキュリティアンケートに回答いただいた教職員の皆様方に厚く御礼申し上げます。