平成 24 年 10 月 4 日
経営企画課 IT 推進担当

教職員各位

【重要】 情報セキュリティ対策の徹底について （通知）

「国際的なハッカー集団「ゴーストシェル」が、東京大や京都大など国内の５大学を含む世界の有力100 大学のサーバーに侵入し、学生や教職員などの個人情報約 12 万件を抜き取ったとする声明をインターネット上で発表した」という記事が、本日、新聞等で報道されました。東大から盗んだとされる情報には、教職員や学生などとみられる 4700 人分のメールアドレスが含まれ、このうち約 800 人分は名前と所属先、住所、電話番号がセットになっていたとされています。東大の広報担当者は「大学から流出した情報かどうか確認を急いでいる」とし、一部サイトを休止して調査しているとのことです。
【記事】 東大など５大学情報流出か…ハッカー集団が声明(読売新聞)
http://www.yomiuri.co.jp/national/news/20121003-OYT1T01663.htm?from=ylist

また、「ゴーストシェルによれば、大学のサーバの多くは、マルウェアに感染しており、クレジット情報が保存されているものも見つかった（Yahoo!ブログより）」という記事もあり、本学においても同様のサイバー攻撃を受ける危険性は十分にあります。そのため、パソコンやサーバを学内で使用している教職員は、情報セキュリティ対策の実施に細心の注意を払うよう心がけてください。具体的には、以下のことを実施してください。

① パソコンやサーバにインストールされているウイルス対策ソフトで、ウィルス定義ファイルが最新になっていることを確認し、ハードディスク全体のウィルスチェックを実施してください。
② さらに、サーバについては、アクセスログにより不正アクセスがないかどうかを確認してください。

日常の業務におけるパソコンやネットワーク利用にあたっての留意事項を情報セキュリティ対策ガイドラインとして通知しておりますので、再度徹底をお願いします。

以下は「情報セキュリティ対策ガイドライン」より抜粋

１．パソコンの管理

（１）ウイルス対策、および、アップデートの実施

- ウイルス対策ソフトのインストールを実施すること。また、定義ファイルは常に最新版が適用されるよう設定すること。
- WindowsUpdate などの、アップデートを随時実施すること。

詳細は添付ファイルをご確認ください。
＜添付ファイル＞
情報セキュリティ対策ガイドライン_20110726 改定.pdf

【担当】経営企画課 IT 推進担当
電話 ： 787-2340
E-mail: center@yokohama-cu.ac.jp

平成 23 年 7 月 26 日改定
経営企画課　IT 推進担当
総務・財務課　庶務・渉外担当

情報セキュリティ対策ガイドライン

１．パソコンの管理

（１） ウイルス対策、および、アップデートの実施

- ウイルス対策ソフトのインストールを実施すること。また、定義ファイルは常に最新版が適用されるよう設定すること。
- WindowsUpdate などの、アップデートを随時実施すること。

（２） 本体の管理

- 起動時の ID・パスワードの設定をすること。
- スクリーンセーバーのパスワードによる保護などの設定により、離席時に不正に操作されることを防止すること。
- 機器の保管場所や居室の施錠管理を徹底し、機器本体にセキュリティワイヤーに接続するなどの盗難防止措置を施すこと。
- パソコン本体表面へパソコン利用時に必要な情報を表示等しないこと。

補足説明）パソコン利用時に必要な情報：ID、Password、IP アドレス、Proxy など

２．データの扱い

（１） データの持ち出し

- 個人情報データの持ち出しをしないこと。
- やむを得ず、他キャンパスなど出張先で個人情報データを閲覧する際は、インターネット接続できない等の理由がある場合を除いて、リモートファイルサービスを利用すること。なお、個人情報を含まないデータに関しても、できるだけリモートファイルサービスを利用すること。
  - ➢ データを必要最小限にすること。
  - ➢ 使用後はすぐにシステム上から削除すること。
  - ➢ 離席する際は、必ずログアウトをすること。
- インターネット接続できない等の理由によりリモートファイルサービスが利用できない場合に、やむを得ず、個人情報データを持ち運ぶ際は、以下の対策を講じること。
  - ➢ 個人情報持出し返却管理簿に記載し、所属長（個人情報保護責任者）の承認を得ること。
  - ➢ 個人情報データを必要最小限にすること。
  - ➢ 持出し用の記憶媒体は自動暗号化機能付きのもの(暗号化 USB メモリなど)を利用すること。
  - ➢ 持出し用の記憶媒体もしくはファイルにパスワードを設定すること。
  - ➢ 私有のパソコン・モバイル端末・記憶媒体で個人情報データのコピー・保持をしないこと。
  - ➢ 使用後は速やかに持出し用の記憶媒体より削除すること。
  - ➢ 持出し用の記憶媒体は施錠できるところで保管すること。

補足説明） パソコン：タブレット PC（例：iPad）を含む

モバイル端末：携帯電話、スマートフォン（例：iPhone)、PDA（例：iPod touch)、超小型 PC など

記憶媒体：USB メモリ、USB ハードディスク、DVD、CD、フロッピーディスクなど

（２） e-メールでのデータ送信

・ e-メールでのデータ送信時は、本文や添付ファイルの情報内容の確認、宛先等の確認、ファイルのパスワード設定を徹底すること。

３．ネットワークの管理

（１） IP アドレス

・ あらかじめ付与された IP アドレスを使用すること。付与されたもの以外の IP アドレスは絶対に設定しないこと。

（２） ネットワーク利用

・ 大学のネットワーク環境を私的に利用しないこと。不正利用のないよう徹底すること。
・ Winny などの不特定多数の相互接続によるファイル交換・共有ソフトを利用しないこと。

４．ID・パスワードの管理

・ パスワードは「言わない」「見せない」「書かない」を守り、第三者に知られることのないようにすること。
・ ID・パスワードの共有や、他人の ID でパソコンを利用しないこと。

５．持ち込み機器

上記事項を守り、安全な機器であることを確認したうえで、ネットワークに接続すること。

６．学外からのアクセス

・ 学内サービスへインターネットを経由してアクセスしている際、離席する場合は必ずログオフをすること。
・ ログイン情報をそのパソコンに保存せずにログインすること。

７．その他

その他、ネットワークの正常な運用を妨げる行為や、他の利用者の正常な利用を妨げる行為、ネットワーク管理者が不適切と認めることを行わないこと。