教員サポート 14・メディア・リテラシーワークショップ

情報セキュリティについて知ろう、考えよう

ワークショップを開催して

司会：日吉 ITC 所長・教養研究センター副所長・商学部教授
種村和史

本日は、教員サポート・メディアリテラシーワークショップ「情報セキュリティについて知ろう、考えよう」にご参加いただきありがとうございます。

このたび、「慶應義塾情報セキュリティポリシー」が制定され、慶應義塾の情報資産保護に対する基本方針がはじめて示されました。これは個々の教職員の行動を制約したり、責任を追及したりするものではありませんが、教育研究活動の中で得られた情報を慎重かつ適切に扱うという、慶應義塾の姿勢を内外に示したものであり、そこで働く我々も、重要な情報を扱う業務に携わる者としてのさらなる自覚が求められることには違いないと思います。

われわれは日々、セキュリティを要する情報に接し、作成し、保存管理しています。教員として、教育の場面で学生の個人情報を扱い、学務で人事情報などに接するだけではなく、研究者としての活動の場面でも、外部に漏らしたくない情報を扱うことも多いと思います。しかも、そのような情報は年々増えているというのが実感ではないでしょうか。

個人で管理するもののほかに、複数の人間が共同で管理する情報もあります。例えば、学生の出席情況・成績などを Excel などで管理なさっている先生は多いと思いますが、場合によっては、統一カリキュラム授業やオムニバス授業など、複数の教員が連携する授業を担当する場合もあるでしょう。そのような時、学生のデータを複数の教員で共有し、情報交換をしなければならず、より厳重な情報管理が求められることになります。このようなケースも年々多くなってきているのではないでしょうか。我々を取り巻くこのような状況の中にあって、みなさんの情報セキュリティはぜったい大丈夫と言い切れるでしょうか。

ここで、私が「セキュリティ」と言っているのには、2 種類の意味を込めています。一つは情報が外部に漏洩したりするのを防ぐという意味でのセキュリティです。例えば、安全性の高いパスワードとはどのようにしてつければよいか（そしてどうやったら忘れないか）、複数の人間の間でパスワードの受け渡しをするとき、どのような点に気をつけるべきなのか、ということなど知りたいと思います。

もう一つは、ファイルが壊れたりして大切な情報を失うことを防ぐという意味でのセキュリティです。もちろん、バックアップが必要ということはわかっているのですが、バックアップファイルが増えることによって、どれが拠るべきファイルなのかわからなくなってしまうということも日々経験することです。ファイル名の付け方などでよい方法があったら教えてほしいと思います。

我々ごく普通の教員は、情報セキュリティに関して素朴かつ切実な不安・疑問でいっぱいというのが実情なのではないでしょうか。本日の会は、日吉 ITC の職員を講師にお招きし、このような不安と疑問を解消していただきたいと思って企画されました。まず、「慶應義塾情報セキュリティポリシー」についてご説明いただいた後、プロの知識と経験から、情報を扱うに当たっての具体的なアドバイスをいただきたいと思います。

the liberal Arts

情報性キュリティについて知ろう、考えよう

講師：日吉 ITC　山根 健

情報セキュリティポリシー制定の背景

- 平成12年 内閣官房情報セキュリティセンター（NISC）による策定
  - 各省庁もこれに沿って策定
- 平成14年 大学における情報セキュリティポリシー制定要請（国立大学は義務）
- 平成19年国立情報学研究所が高等教育機関向け情報セキュリティ対策サンプル規程集を公開
  - 以後、私立大学でも規程の整備が広まる
  - 義塾もこれをベースにして策定
  - 外部資金獲得の条件や大学評価のポイントにも

「基本方針」の主旨

- 組織の情報資産をどのような脅威からどのようにして守るかについての基本的な考え方を宣言
- 対象となる情報資産ならびに対象者の範囲、義務、取り組むべき課題と目標を掲示
  - 3 対象範囲（2）対象者
  - 4 対象者の義務
- 用語を定義

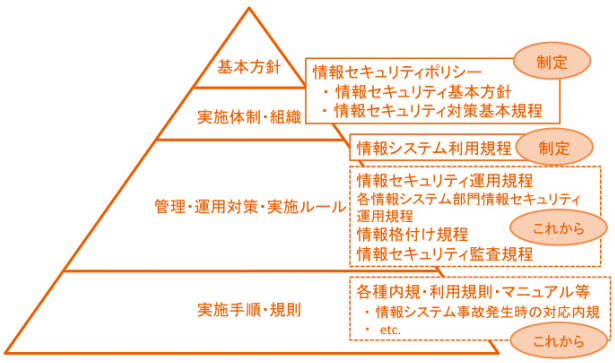
義塾情報セキュリティポリシーの目的

- 「慶應義塾の研究・教育・医療活動および経営管理における電子情報の取り扱いにあたり、責任ある情報資産の活用を図り、自由かつ安全な利用環境を実現すること」（基本方針第1条）
- 義塾の情報資産を守るために行われる業務について、その管理運営の方針、および具体的基準・手順をとりまとめる
- “リスク管理”

「基本方針」による用語の定義

- 情報
  - 義塾の活動によって発生もしくは収集され、情報システムに記録された情報及び情報システムに関係がある書面に記載された情報であり、電磁的媒体に記録された情報すべてを含む
- 情報資産
  - 情報および情報を管理するための仕組みの総称
    - ア 情報
    - イ 情報を電磁的手段で記録している媒体
    - ウ 情報を一時的に送受信、もしくは表示している装置
    - エ 義塾内で使用される各種情報機器・設備
- 情報セキュリティ
  - 情報資産の機密性、完全性、可用性を維持すること

情報セキュリティポリシーの体系



「基本規程」の主旨

- 「基本方針」を実現するための運用と組織の体制を規定
  - 最高情報責任者＝IT担当常任理事（第4条）
  - 情報システム部門管理責任者（第5条）
  - 情報セキュリティ委員会（第7条）
- 遵守すべき行為および判断などの基準を明示
- 対象範囲（人と物）、組織体制、情報資産の軽重（格付け）と管理、セキュリティ侵害への対処、ネットワークの監視および利用情報の取得などを規定

教員サポート14「情報セキュリティについて知ろう、考えよう」

情報セキュリティの組織体制

- 個人情報保護規程に定められている各部門の個人情報管理責任者が情報セキュリティについても当該部門の管理責任者を兼務する
- ITCは各部門の管理責任者を補佐する

「情報システム利用規程」の主旨

- 「基本方針」が記す「教育・啓蒙」および「罰則」を具体化
  - 利用者の遵守事項（第4条）
  - 違反行為等に対する措置（第5条）
- 利用者の行動規範の指針、ならびに塾内各部門の情報システム管理者が事故発生時にとることのできる措置を明確化

利用者の遵守事項

1. 利用規程、個人情報保護規程の遵守
2. 義塾建学精神に則り、品位を保ち、社会の一員としての自覚に基づいてシステムを利用
3. 利用者としての管理責任を怠らない
4. アカウント・パスワードを第三者に開示しない
5. 情報資産の利用に関する虚偽の申請をしない
6. 情報資産を営利目的に使用しない
7. 情報資産を利用して法令や公序良俗に反する行為をしない
8. 情報資産を利用して他人のプライバシーや著作権、商標権等の知的財産権を侵害する行為をしない
9. 情報資産を利用して他人に対する迷惑や不利益を与える行為及び誹謗・中傷など人権を侵害する等の行為をしない
10. 他のネットワークシステムへの不正な侵入や運用の妨害、及び禁止されている操作をしない
11. 一般にネットワーク上で各個人が守るべきであると理解されているルールに違反しない
12. 利用規程のほか、各学校・学部・部門で定めた規則等に従う

教職員が扱う情報・情報資産

- 授業で発生・収集されるものの例
  - 履修者名簿、出欠状況、教材、レポート、試験問題・解答、成績
  - 履修学生とのメールのやりとり
  - 共同担当教員とのメールのやりとり
- 研究で発生・収集されるものの例
  - 実験の材料・成果、論文
- 学務で発生・収集されるものの例
  - 会議資料
  - 入試に関する情報

◎パソコンに保存したデータも印刷した紙も含む

教職員が扱う情報のセキュリティ

- 機密性の維持
  - 紙の場合：鍵のかかるところに保管する、放置しない
  - データの場合：パスワード付与、暗号化、他人がアクセスできるところに保存しない
    - 勿論、パスワードの機密性維持も重要
- 完全性の維持
  - 紙の場合：散逸しないようにまとめてファイルする
  - データの場合：フォルダに系統立てて保存する、最終版なら不意に改変されないよう読み取り専用にする
- 可用性の維持
  - availability、稼動性、壊れにくさ
  - 重要な情報はバックアップを取り、別の場所に保管

機密性維持の実例

- セキュリティ対策ソフトウェアをインストールする
  - ウィルスによる漏洩を防止
  - サイトライセンス契約のESETの活用
- ファイルにパスワードを付ける
  - Acrobat, Office等アプリケーションの機能で付ける
  - パスワードを付けてzipファイルに圧縮する
  - 他人へのパスワード伝達は、機密性が高いなら事前に別途行うべき
- メールの送受信は接続を保護する
  - POPS, IMAPS, SMTPS
  - その上で、機密性の維持が必要なファイルはパスワード付与して送受信する
  - （本当に機密性が高ければそもそもメールを用いない）

良いパスワード、悪いパスワード

- 悪いパスワードの例
  - 自分や身近な人の氏名、アカウント名そのまま
  - 辞書に載っている単語
  - 生年月日、住所、電話番号
  - 同じ文字の繰り返し
- 良いパスワードの例
  - できるだけ長く
    - 文字数制限がなければ文章にするとか
  - 大文字小文字、数字、記号を組み合わせる
    - 英字を似た数字や記号に置き換えるとか
  - 但し「絶対大丈夫」はないので注意

可用性維持の実例

- バックアップは別の媒体に取る
  - USBメモリ、外付けハードディスク、等々
- 複数世代のバックアップを保管する
  - 1世代だとバックアップ中に事故が起きると対応できない
- 一定の頻度でバックアップを取る
  - 間隔が長いと復元できない確率が増す
- バックアップをスケジュール化する
- バックアップソフトウェアを活用する
  - Mac付属のTime Machine
  - 高い機密性が必要なら有償製品の検討も
  - 一定規模の情報量や高い機密性が必要ならバックアップ専用ストレージも選択肢

機密性を維持する保管場所

- データを保管するPCは自動ログインしない（パスワード認証付与）
- データを保管する媒体は持ち歩かない
  - ノートPC、USBメモリ、CD/DVD-Rなど普段持ち歩くものに機密性のあるファイルを保管しない
- 学内サーバに保管する場合も安全であること
  - ソフトウェアシステム、アカウント・パスワード管理
- 学外サーバに保管すること自体が悪いわけではないが、安全が保証されること

※維持すべき機密性の度合い（格付け）によって適した保管場所を判断する

まとめ

- 義塾の情報セキュリティポリシーは策定されたが、規程はこれが全てではなく、これからが重要
- 情報に格付けをして、適切なセキュリティ対策を選択する
- “リスク管理”の意識

完全性維持の実例

- ファイル/フォルダ名に日付・時間を付け、いつの時点の情報か明確にする
  - 例：教員サポートスライド20130703.ppt
- ファイル/フォルダのアクセス許可を読み取り専用にする
  - 例：[プロパティ] > [セキュリティ] で Everyone に対して「読み取り」だけを許可する

ワークショップ概要

日　時：2013 年 7 月 3 日（水）18：30 ～ 20：00

場　所：来往舎 2 F 大会議室

対　象：慶應義塾の教員・教諭・職員

主　催：教養研究センター・日吉 ITC

慶應義塾大学教養研究センター Report No.20
教員サポート（担当：種村和史）

2013 年 10 月 31 日発行
代表者　不破有理
〒 223-8521　横浜市港北区日吉 4-1-1

TEL：045-563-1111（代表）
lib-arts@adst.keio.ac.jp
http://lib-arts.hc.keio.ac.jp/