「情報セキュリティ」

2009.7.13

講義内容：
1．ウイルスなどの感染防止と対策
2．ネット上の犯罪と倫理
3．医療関連の情報倫理

0．参考文献・資料

- 山口英『ブロードバンド時代のインターネットセキュリティ』，岩波科学ライブラリー，2002.
- 情報処理推進機構『情報セキュリティ読本』実教出版，2005.
- 宮田昇『学術論文のための著作権Q＆A』東海大学出版会，2003.
- http://www.ipa.go.jp/security/ （情報処理推進機構セキュリティセンター）
- http://www.npa.go.jp/cyber/ （警察庁サイバー犯罪対策；対策ビデオなど）
- http://www.cyberpolice.go.jp/ （@police）
- https://www.ccc.go.jp/index.html （サイバークリーンセンター）
- http://www.rcis.aist.go.jp/index-ja.html （独立行政法人産業総合研究所情報セキュリティ研究センター）
- http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html（個人情報保護法）
- http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/index.html（ガイドライン）

1．ウイルスなどの感染防止と対策

(1)「ウイルスなど」の主な種類

- ウイルス／ワーム：勝手に増殖して複製をばらまく
- トロイの木馬：他のファイルに潜伏し，そのファイルがアクセスされるときに作動
- スパイウェア:システムに常駐作動し，コンピュータ情報をサーバに勝手に送信
- ボット：ウイルスのうち，外部へ悪影響を与えるロボットのような動作をするものを呼ぶ。ネットワークを組んで一斉攻撃が起こるのが最大の脅威。

(2) 主な感染経路

- 電子メールの添付ファイル
- Webブラウズ時の自動実行(ActiveX, Javascriptなど)
- フロッピーディスク，CD-RやUSBメモリ等メディアを介して。最近はUSBメモリが狙われている
- Winny/Shareなどによる P2Pファイル共有
- システムの脆弱性を突いてネットワークから直接感染（主としてサーバまたは途上国でのダイヤルアップアクセス時）

(3) コンピュータウイルスが動作する仕組み

- コンピュータを「使う」＝人間がプログラムとデータをCPUに渡し，処理結果を得ること。図式化すると，

  [ヒト→プログラム・データ→CPU→結果→ヒト]

  ウイルス・ワーム・トロイの木馬は，このプロセスのどこかに紛れ込んで，CPUの処理を掠め取る
- もう少し詳しくみると，CPUは概ね連続的にプログラムを実行しつつ，割り込み（I/O，タイマ）を定期的にみている
- 主なI/O割り込みはキーボード，VSYNC（ディスプレイの同期），マウス，ストレージ（フロッピーI/O等），ネットワーク
- WindowsなどではOSが面倒をみる割り込みが多いので，書き換えてCPU時間を掠め取られる可能性のある部分が多岐にわたるため，昔のMS-DOSに比べるとウイルスなどが入り込みやすい

(4) 主なコンピュータウイルスの種類

- ブートセクタ感染型：コンピュータ起動デバイス（通常はフロッピーディスクやハードディスク）の，起動時にCPUが最初に参照する場所に入り込んで動作。最近はあまり流行っていない。
- ファイル感染型：感染ファイルあるいはそれへのリンク実行で動作。常駐プログラムやOSのシステムファイル（Windowsの初期設定ファイルなどを含む）に感染すると動作し続ける。割り込みで起動するようにシステムファイルを書き換えるものもある。多くのボットもこれに分類される。USBメモリを介して感染することもある。
- マクロウイルス：特定のアプリケーションソフト（よく狙われるのは，WordやExcelなど，ユーザが多いもの）のマクロになっていて，感染ファイルを開くと動作。
- メール添付ファイル型ウイルス：Windowsが特定の拡張子（pifとかicoとかjpgとか）のファイルのアイコン情報をプレビューする仕組みを使って，開かなくても感染。最近はたいていFromが詐称されている。

(5) 悪名高いコンピュータウイルス

- かつて大流行したもの
  - W32/Nimda: .emlメールでhtml形式をプレビューするとreadme.exeが実行されて感染，コピー配送。webでも。IEのセキュリティホール対策がされていれば自動実行されない

- W32/Ska (Happy99): happy99.exe という添付ファイルを実行すると花火が上がり，ウイルスが複製/送信される
- XM/Laroux: MS Excel のマクロウイルス
- W97M/Melissa: MS Word のマクロウイルス
- W32/MSBlaster：IIS サーバに感染し DoS 攻撃。再起動反復

- 現在流行中のもの（2009 年上半期被害届出数上位 6 種）
  - W32/Netsky：メールや P2P 経由。亜種が多い。services.exe
  - W32/Mydoom：メールや P2P 経由。破壊活動あり
  - W32/Mytob：メール添付か Messenger（ポート 445）経由。IRC バックドア設置。msnmsgr.exe
  - W32/Bagle：アイコン擬装，バックドア設置，アンチウイルスソフト停止
  - W32/Autorun: USB メモリを挿すだけで自動実行され感染。2008 年 11 月大流行
  - W32/Klez：メール添付経由。アドレス偽装。6 日に破壊活動。

(6) ボットの問題点と対策

- ボットの動作：迷惑メール送信，DoS 攻撃，ネットワーク感染，ネットスキャン，自律的動作，スパイウェア
- ボットの問題点
  - 侵入に気づきにくい
  - 多くの感染コンピュータが攻撃者の指示で一斉攻撃するボットネットワーク
- ボット対策
  - ファイアーウォールやルータを介してネットワーク接続する
  - 駆除には各社最新のアンチウイルスソフト，あるいはサイバークリーンセンターで配布している無料の「ボット(BOT)駆除ツール」を利用する(https://www.ccc.go.jp/flow/index.html)。サイト確認を慎重に。

(7) コンピュータ・ウイルス感染を防ぐために

- アンチウイルスソフトを導入し，常時パターンファイルを更新しながら作動させておく（学内では Symantec Antivirus が無料で使える）
  - OS に最新のセキュリティパッチを常にあて(Windows Update，Microsoft Update などを利用），毎日チェック。
- ブラウザからの侵入を防ぐ
  - ブラウザクラッシャーなどもあるので，怪しいサイトにはアクセスしない
  - Javascript や ActiveX などスクリプト実行機能を普段は停止しておき，必要なときだけ有効にする
  - Internet Explorer をデフォルト設定のまま使うのではなくて，セキュリティに気を遣ったブラウザ（Mozilla Firefox など）を使う
  - 検索で上位だからといって信用せず，必ず URL を確認（SEO ポイズニング対策）
- メールからの侵入を防ぐ
  - メールソフトの html や画像の自動表示機能をオフにする
  - Outlook Express をデフォルト設定で使うのではなく，セキュリティに気を遣ったメールソフト（Thunderbird など）を使う。gmail のアカウントを使い，Firefox から web メールとして使うのも有効らしい。
  - 怪しいメールに注意する
- P2P ファイル共有をしない（学内では禁止）

（事例）新型インフルエンザへの便乗

- SEO (Search Engine Optimization)ポイズニング：検索サイトから Swine（豚）と言う検索キーワードを入力して検索を行うと，その検索結果の上位に表示されるウェブサイトの一覧の中に，悪意あるウェブサイトが紛れていて，アクセスすると感染してしまう
- 2009 年 4 月末～5 月初にかけて，米国 CDC からのメールや日本では国立感染症研究所からのメールを装って，添付ファイル（pdf）内に Trojan.Pidief.C というウイルスを含んだメールが送られてきた。

(8) 主な市販アンチウイルスソフト会社

- トレンドマイクロ(http://www.trendmicro.co.jp)ウイルスバスターシリーズを販売
- シマンテック(http://www.symantec.co.jp)ノートン・アンチウイルスシリーズを販売
- マカフィー(http://www.mcafeesecurity.com/japan/)ウイルススキャンシリーズを販売
- キヤノンシステムソリューションズ(http://canon-sol.jp/product/nd/)NOD32 を販売
- Google で「アンチウイルス 比較」をキーワードで検索すると多くの情報が見つかる（ただし，SEO ポイズニングを警戒して，URL に注意すること）

(9) 無料で使えるアンチウイルスソフト

- Symantec Anti Virus: 群馬大学内のマシンなら無料。対応 OS: Windows
- BitDefender Free Edition: Windows と Linux 対応。要登録。
  http://www.bitdefender.com/bd/site/downloads.php?menu_id=21

- AVG Free Edition: 要登録。Windows 用。高機能。
  http://free.grisoft.com/freeweb.php
- Avira AntiVir: 個人・非営利なら無料。対応 OS は Windows，Linux，FreeBSD，Solaris
  http://www.free-av.com/
- avast! Home Edition: 家庭で非商用利用なら無料。要登録。
  http://www.avast.com/jpn/avast_4_home.html
- ClamWin Free Antivirus: ライセンスが GNU GPL なので，企業ユーザが営利目的で使うコンピュータでも無料で使える。Windows 用。検出力は高いが，リアルタイムスキャンがない。
  http://www.clamwin.net/

(10) もしも感染してしまったら

- 二次感染源（＝加害者！）とならないことが最重要
  - 感染が疑われたら，直ちに LAN ケーブルを抜く（電源ケーブルを抜くとコンピュータが壊れてしまうかもしれないので，電源ケーブルではなくて LAN ケーブルを抜く。無線 LAN の場合はスイッチがあれば切る）
- できるだけ早く駆除する
  - CD-R などで対策ツール（アンチウイルスソフト，専用駆除ソフト等）を用意し，コンピュータを CD 起動モードかセーフモードで再起動して，対策ツールを適用
  - または，コンピュータを完全に初期化（推奨）
- 感染を報告する義務
  - 群馬大学の規定は，昭和分室へ書面で提出となっている。
  - IPA/ISEC への届出は，http://www.ipa.go.jp/security/outline/todokede-j.html

2．ネット上の犯罪と倫理

(1) 不正アクセス行為の禁止等に関する法律

- 通称「不正アクセス禁止法」。平成 12 年施行(http://www.ipa.go.jp/security/ciadr/law199908.html)
- 骨子
  - 不正アクセス行為の禁止，罰則，再発防止援助
  - 不正アクセス行為の定義（以下 3 点は大意）
    - 他人の ID／パスワードを使ったアクセス
    - セキュリティホールからのアクセス
    - クラッキング
  - 管理者の防御義務
  - 都道府県公安委員会による援助規定
  - 罰則：懲役または罰金（例：ACCS 事件）

(2) 不正アクセスの原因と現状

- 原因
  - システム管理が杜撰（パスワードを紙に書いてコンピュータに貼ってある，パスワードが簡単すぎる，パスワードを設定していない，ログインしたまま長く席を離れている等）
  - システムにセキュリティホールがあって，パッチを当てていない
- 現状
  - 標的サーバだけでなくネットワークに被害
  - 検出率が低いし（高くても数%），検出されたうち報告される割合も低い（せいぜい 30%）
  - 主な攻撃は，盗聴，通信路改変，traffic 解析，DoS アタック，なりすまし，等
  - 主な防御手段はファイアウォール，システムスキャン，常に最新のセキュリティパッチを当てる，セキュリティが弱いソフトは使わない，分かりやすいパスワードは使わない，定期的にパスワードを変更する，など
    （最後 2 点の両立のためには，ID Manager などパスワード管理ソフトの導入は検討に値する）

(3) フィッシング(phishing)

- Phishing とは：銀行等の企業からのメールを装い，メールの受信者に偽りのホームページにアクセスするようにし向け，そのページにおいて個人の金融情報（クレジットカード番号，ID，パスワードなど）を入力させるなどして個人の金融情報を不正に入手するような行為
- 被害防止のために
  - 不自然な形で個人の金融情報を尋ねるメールが来たときは，当該企業に必ず確認
  - URL 擬装を見破れるブラウザを使う（バージョンが低い Internet Explorer は不可）
  - html メールを表示させない
- 事例：Visa ジャパン(2004 年 11 月)

(4) ワンギリ商法
- 悪徳業者はターゲットに電話をかけ，1回コールしただけで切る
- 謎の着信履歴をみて，ターゲットがコールバックする
- その電話は案内テープが自動受信するようになっており，案内にしたがって進むと有料番組に進んでしまって，利用料が請求される。ターゲットが自ら有料番組を選んだようにしか見えないため，これが不正料金請求である証拠が残らないのがミソ。
- ただし，ダイヤルQ2の利用料金はそれほど高額にはできないし（上限は3分300円），2002年からはパスワードも導入されたので，有料番組利用自体で高額料金請求になることはほとんどなく，むしろ，携帯番号が結びついた個人情報を入手した悪徳業者が，不当に高額な料金請求をする詐欺の被害につながる危険性の方が大きい。
- 対策としては知らない相手からの着信履歴にはコールバックしないこと

(5) ワンクリック料金請求
- 電子メールや電話、はがきなどを利用して、架空あるいは一度だけアクセスしたサイトから利用料金等を請求される
- 「自分が携帯電話からインターネットに接続し、いろいろなサイトを見ているうちに、突然アダルト（出会い系）サイトにつながり、料金請求の表示になる」ような事例が多い
- 携帯の識別情報や位置情報が正しくても，それだけで個人情報が漏れることはないし，電子契約法第3条により意思のない契約は無効になるので，慌てて代金請求に応じたりメール返信したりしないことが大事。あまりにも悪質な場合は最寄りの警察署に相談

(6) 架空料金請求
- アクセスしていない有料アダルトサイトなどの高額な利用料が請求される
  - 利用していないのであれば一切支払う義務はない。無視する
  - 「もしかしたら利用したかもしれない」など身に覚えのある場合でも、請求者が本当に権利者であるかどうか確認
- 最近は，「（支払いがない場合は）プロバイダ責任制限法に基づいて、お客様の氏名・住所等の情報の開示等の措置をとる」，個人情報保護法や債権管理回収業に関する特別措置法（サービサー法）など法律名を持ち出して正式通知書面であるかのような事例が多く，手口が巧妙化
- 総務省認可を騙った架空料金請求で，「退会手続き」をクリックさせることによって，個人情報を得るものも。無視すること。（電子契約法は経済産業省所管） [http://www.soumu.go.jp/joho_tsusin/d_syohi/futou.html]
- 裁判所からの「支払督促」「少額訴訟」は，放置するとまずい場合があるので，裁判所か弁護士，消費生活センター(http://www.kokusen.go.jp/map/index.html)に真偽を確認して対応

(7) 出会い系サイト
- 被害者の8割は18歳未満
- トラブル事例（http://www.joho110.com/thtt.htm より）
  - 「無料ポイント進呈」などで、無料と見せかけてポイントがなくなった時点から有料になり、罪悪感から親に隠れて支払ったり連絡先などの個人情報を教えて請求が繰り返されて何度も支払うことになった。
  - 援助交際の男性側が相手に恐喝されることが多くなり、男性側も恥ずかしくて告訴できない。
  - 実際に会った相手は風俗店のスカウトで親や学校にバラすと恐喝された。
  - 援助交際で会ったつもりでいかがわしい行為をしたがお金を支払ってもらえなかった。
  - 興味本位で会っただけなのに、交際を断わったところ、ストーカー行為を受けた。
  - 掲示板に「下着売ります」と掲示しただけで下着が購入価格10倍にて売ることができたのですが数日後、相手に「親に送り付けられたくなかったら10万円で買い取れ」と逆に脅迫された。

(8) 著作権侵害をしない
- ソフトウェアの不正コピー使用は著作権侵害
  - 群馬大学ではないが，P2P (Winny や Share)で入手したりwarezと呼ばれるID情報を使って不正使用するとか，それをネットオークションで売りさばくなどして逮捕され，退学になった学生もいる
  - 群馬大学の学内のネットワークではP2Pファイル共有は禁止されていて，もし設定すると，ハードウェア的に，そのコンピュータのネットワークカードがブラックリストに載って，使用不能になる
  - 友達からコピーさせてもらうのもダメ。
  - できるだけフリーソフトを使う。プレゼンもOpenOffice.org（http://www.oooug.jp/参照）のImpressで十分。
- 個人のウェブサイトでも他人の著作物を無許可で公開するのは著作権法違反（「公衆送信権」という考え方）。出版物と同じなので，適切な引用ならOK。

(9) Winny/Share は絶対ダメ
- 相次ぐ情報流出
  - 平成19年4月も稚内署，江別署で警官の私物PCから捜査資料が流出，5月にも愛媛県愛南町，山口市，対馬市の個人情報流出（業務委託を受けた山口電子計算センターの1人の社員による。合計約5万人分）

- 平成 21 年 1 月，都立墨東病院で男性職員の私物パソコンから患者の氏名、年齢、性別、疾患名など 271 名分と、職員の氏名、住所、電話番号 64 名分、委託職員の氏名、会社名 291 名分、その他 14 名分の氏名とメールアドレスが流出。看護職員の破損した USB メモリ修理を請け負った際に私物パソコンを利用し，作業終了後もデータを消去しないままに Winny を使用し，ウイルスに感染

- 原因は2つ
  - 危険性を知らない
  - 自分が加害者になっていることを意識していない

(10) 安全な Web サイト利用の鉄則 [http://www.rcis.aist.go.jp/special/websafety2007/]

- フィッシング被害を防止する Web サイト利用手順の確認を目的として，RCIS から公開されている文書。必読!!
- 概要
  - 利用者の鉄則
    - 入力直前にアドレスバーでドメイン確認
    - 暗号化が必要なら https:// でサーバ証明書確認（https:// なら常に大丈夫というわけではない）
  - サイト運営者の鉄則
    - よくある質問と答え
- *多くのサイトで警告を無視して構わないと書かれているが，「オレオレ証明書」は信用するな，と明記されている。

＊メールアドレスは，個人情報保護法の対象になる場合とならない場合がある

> 個人の氏名等を含んだリストがあり、その1項目としてメールアドレスが含まれている場合、リストは全体として、また、メールアドレスはその一部として、個人情報に該当します。また、メールアドレスのみであって、ユーザー名及びドメイン名から特定の個人を識別することができる場合、そのメールアドレスは、それ自体が単独で、個人情報に該当します。一方、記号や文字がランダムに並べられているものなど、特定の個人を識別することができない場合には、別に取り扱う名簿などとのマッチングにより個人を特定することができない限り、個人情報には該当しません。(参照：http://www5.cao.go.jp/seikatsu/kojin/gimon-kaitou.html#2_3)

3．医療関連の情報倫理

(1) 守秘義務と個人情報保護

- 守秘義務をもつ者は，自分のコンピュータへの記録の保存も気をつけねばならない。私物でも。
- 保存の仕方が悪いと，犯罪被害にあったとき，同時に加害者となってしまう危険もある
- (例）ノートパソコンの盗難で患者情報が漏れてしまう危険。2005 年 1 月 5 日に新聞報道された，2004 年 12 月に三重大付属病院で 10 台のコンピュータが盗難にあったケースでは，「施錠を徹底し，患者名を匿名にするなど対策する」と病院長コメント
- フェイルセーフな対策の必要性（匿名化は当然）
  - 暗号化して保存
  - ハードディスクにパスワードロック
  - データはすべてサーバに保管
  - 群馬大学も病院で使われる USB メモリは暗号化されてパスワードロックがかかっている

(2) 個人情報保護法 [http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html]

- 正式名称は「個人情報の保護に関する法律」（平成一五年五月三十日法律第五十七号）
- 最終改正は平成十五年七月十六日法律第百十九号，平成 17 年 4 月 1 日施行。

> 第一条 この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

- プライバシー権を保護するための法律であり，背景としてはプライバシー概念の変化（憲法 18 条の身体の自由，憲法 19 条の内心の自由，刑法，著作権法などの規定とは別に，相対的に「社会から切り取られたプライベート」の重要性が生まれ，『自己情報がどう扱われるかを知り，コントロールする権利』が認知された）がある。

(3) 医療関連の情報倫理

- 医師の守秘義務
  - 一般には，刑法 134 条『医師，薬剤師，医薬品販売業者，助産師，弁護士，弁護人，公証人又はこれらの職にあった者が，正当な理由がないのに，その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは，6 月以下の懲役又は 10 万円以下の罰金に処する』が根拠法
  - 精神保健福祉法第 53 条『精神科病院の管理者、指定医、地方精神保健福祉審議会の委員、精神医療審査会の委員、第 22 条の4第4項、第 33 条第4項若しくは第 33 条の4第2項の規定により診察を行つた特定医師若しくは第 47 条第1項の規定により都道府県知事等が指定した医師又はこれらの職にあつた者が、この法律の規定に基づく職務の執行に関して知り得た人の秘密を正当な理由がなく漏らしたときは、1年以下の懲役又

は 100 万円以下の罰金に処する』
    - 感染症予防法第 67 条『医師が、感染症の患者（疑似症患者及び無症状病原体保有者並びに新感染症の所見がある者を含む。次条において同じ。）であるかどうかに関する健康診断又は当該感染症の治療に際して知り得た人の秘密を正当な理由がなく漏らしたときは、1年以下の懲役又は 50 万円以下の罰金に処する』
- 注意が必要な例
    - 大学病院から退職した医師が患者に独立開業の案内状を送付→個人情報保護法違反
    - 横浜市衛生局港湾病院を退職した医師が元患者に年賀状を送付→横浜市個人情報保護条例違反
    - 覚せい剤中毒者を本人に無断で警察に通報→従来，麻薬は都道府県知事に届出義務があり，覚せい剤は届出規定はないが，平成 17 年 7 月 19 日の最高裁判所第一小法廷（あ）第 202 号　覚せい剤取締法違反被告事件の判決で『必要な治療や検査の過程で採取した尿から違法な薬物を検出した場合，捜査機関に通報するのは正当な行為であり，守秘義務に違反しない』とされた。
- 診療記録電子化（電子カルテ）に伴う問題
    - 紙カルテに比べ，紛失，持ち出し，改ざん，誤読はされにくい反面，大量漏洩の危険は大きい
    - 診療記録電子化の条件：3原則（厚生省3局長通知，1999 年 4 月）→(1)真正性，(2)見読性，(3)保存性

(4) 医療関係機関・組織の情報漏洩と対策
- 医療関係機関の個人情報漏洩事例
    - 製薬企業プロパーのノートパソコンを狙った車上荒し多発(2005 年夏）
    - ウイルス感染と盗難が多い。紛失もある
    - 2006 年は，4/24 東芝メディカル電車内紛失，4/20 福井県立病院研修医の PC ウイルス感染，4/1 関西医科大学附属滝井病院看護師の PC 盗難，4/7 虎ノ門病院退職医師の PC 盗難
- 対策『医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン』（2004 年 12 月 24 日，厚生労働省，2006 年 4 月 21 日最終改正）
    - http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf
    - 特徴
        - 取扱い情報 5000 件以下の医療機関に対しても患者情報保護を求める（個人情報保護法では対象外だが，医療情報が有する高い機密性を理由として要請）
        - 死亡患者の個人情報も保護対象として明記
        - 保護と利用のバランスを具体的に明示（個人情報保護法第1条の趣旨の例外として，本人の同意にかかわらず高い公益性から医療の特殊性を考慮した利用が可能な場面を明記）
        - 遺伝情報には特別な留意を(http://www.mext.go.jp/unesco/009/005/004.pdf)
    - 2006 年 4 月 21 日改正のポイント
        - 警察・検察への情報提供原則 OK，災害時対策

*今回の講義について，何か質問，意見，感想などありましたら，公衆衛生学の中澤准教授(nminato@med.gunma-u.ac.jp)までメールをください。