情報処理入門

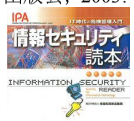
医学系研究科社会環境医療学講座生態情報学
准教授　中澤　港　<nminato@med.gunma-u.ac.jp>
2007 年 5 月 18 日

講義テーマ:
「情報倫理(1)」

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

文献・資料・参考サイト

- 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.
- 参考サイト(政府ドメインのもののみ)
  - 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)



ウイルスなどの感染防止と対策

- 「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。
- 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
  - フロッピーディスクや USB メモリ等メディアを介して
  - Winny 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

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, とは?
  - 人間がプログラムとデータを CPU に渡し, 処理結果を得る
  - 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→ウイルスなどが入り込みやすい

主なコンピュータウイルスの種類

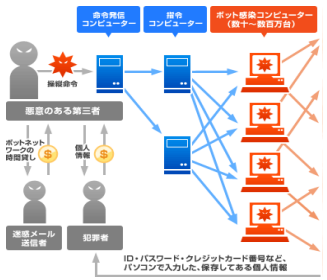
- ブートセクタ感染型:コンピュータ起動デバイス(通常はフロッピーディスクやハードディスク)の, 起動時に CPU が最初に参照する場所に入り込んで動作。最近はあまり流行っていない。
- ファイル感染型:感染ファイルあるいはそれへのリンク実行で動作。常駐プログラムや OS のシステムファイル(Windows の初期設定ファイルなどを含む)に感染すると動作し続ける。割り込みで起動するようにシステムファイルを書き換えるものもある。多くのボットもこれに分類される。例: Happy99, SQL Slammer, agobot, Randex
- マクロウイルス:特定のアプリケーションソフト(よく狙われるのは, 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。例: W97M/Melissa, XM/Laroux)
- メール添付ファイル型ウイルス: Windows が特定の拡張子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。例: W32/Netsky, W32/Mydoom

よく知られているコンピュータ・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って, ウイルスが複製され送信される
  - 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(Netsky は今年 4 月だけでも 666 件の届出)
  - W32/Netsky : メール, P2P 経由。亜種が多い。services.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/Mydoom : メールや P2P 経由。破壊活動あり
  - W32/Rinbot : リモート IRC チャネルに接続しコマンド待機するボット
  - W32/Antinny: Winny ネットワーク経由で拡大し情報漏洩
  - 山田ウイルス:感染するとマシンをウェブサーバ化して公開 ,youjo.exe
  - 山田オルタナティブ:ウェブサーバ化＋感染マシン同士をリンク

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。サイト確認を慎重に。
    (*) https://www.ccc.go.jp/flow/index.html



上図出典: https://www.ccc.go.jp/bot/index.html

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
- OS に最新のセキュリティパッチを常にあてておく(Windows Update, Microsoft Update などを利用)。毎日チェック。
- メールからの侵入を防ぐ
  - メールソフトの html 表示を停める
  - セキュリティに気を遣ったメールソフト(Thunderbird など)を使う
- 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停止する
  - セキュリティに気を遣ったブラウザ(Mozilla Firefox など)を使う
- P2P ファイル共有をしない(学内では禁止)

主な市販の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

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 95/98/SE/Me/NT4/2000/XP/Server 2003
- BitDefender: Windows98/Me/NT/2000/XP と Linux 対応
  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
- AntiVir PersonalEdition Classic: 個人・非営利なら無料。Windows98/Me/NT/2000/XP 。Linux 版，FreeBSD 版，Solaris 版もある。
  http://www.free-av.com/
- 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 98/Me/2000/XP/Server 2003 用。検出力は高いが，リアルタイムスキャンがないのが欠点
  http://www.clamwin.net/

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
  - 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
- 感染を報告する義務
  - 群馬大学の規定（昭和分室へ書面で）
  - IPA/ISEC への届出
    http://www.ipa.go.jp/security/outline/todokede-j.html

ネット上の犯罪と倫理

- 法規制
  - 不正アクセス行為の禁止等に関する法律
- 被害者にならないために
  - フィッシング (phishing)
  - ワンギリ商法
  - ワンクリック料金請求
  - 架空料金請求
  - 出会い系サイト
- 意図せず犯罪者にならないために
  - 著作権侵害をしない
  - 守秘義務と個人情報保護（コンピュータ盗難防止）

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）

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，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

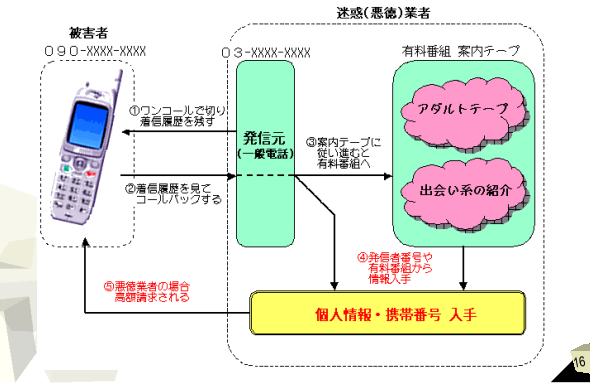
フィッシング (phishing)

- **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**
  - **htmlメールを表示させない**
- **事例**
  - **Visa ジャパン (2004 年 11 月)**

リンク先は，この URL とは全く違うサイトになっている

ワンギリ商法

- 下図出典
  http://www.pref.nagano.jp/police/keimu/hightech/deai_02.html



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」（下図は警視庁のサイトより）
- 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

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。
  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，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

「総務省認可」を騙ったメールの例

総務省認可

貴殿は今まで2サイトに退会処理をせず料金踏み倒しの経歴があります。このままで宜しいのですか？もしこのまま退会処理を行わなければ「電子契約法」に基づき、行政処分通達を総務省に通告致します。

経済産業省所管!!

退会入り口

裁判では、今後の給料差し押さえ並びに、不動産・動産物も強制執行致します。

※ 退会の仕方＝アドレス確認（メール送信）→ニックネームに「退会」と入力・貴方の電話番号を入力・パスワードには今日の日付を4文字の数字で入力し、送信→認証センターをクリックし、発信⇒番組入口をクリック⇒プロフィール更新⇒メニュー⇒退会

退会入り口

※ こちらと致しましては何も難しい事は言っておりません。退会処理もせず、そのまま放置はやめて下さいと言っているのです。退会処理を後回しにし、そのまま放置してしまったのは何故ですか？これは最後の警告です。早急に且つ料金が増幅しない内に退会処理を行って下さい。

退会入り口

【退会手順】アドレス確認（メール送信）→ニックネームに「退会」と入力・貴方の電話番号を入力・パスワードには今日の日付を4文字の数字で入力し、送信→認証センターをクリックし、発信⇒番組入口をクリック⇒プロフィール更新⇒メニュー⇒退会

19

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倍にで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。

20

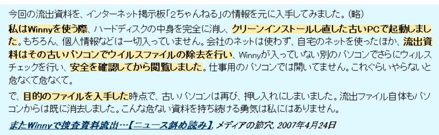
著作権侵害をしない

- 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 。

21

Winny 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）
- 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（北海道新聞記者の例）



今回の流出資料を、インターネット掲示板「2ちゃんねる」の情報を元に入手してみました。(略)

私はWinnyを使う際、ハードディスクの中身を完全に消し、クリーンインストールし直した古いPCで起動しました。もちろん、個人情報などは一切入っていません。会社のネットは使わず、自宅のネットを使ったほか、流出資料はその古いパソコンでウイルスファイルの除去を行い、Winnyが入っていない別のパソコンでさらにウィルスチェックを行い、安全を確認してから閲覧しました。仕事用のパソコンでは開いてません。これぐらいやらないと危なくて危なくて。

で、目的のファイルを入手した時点で、古いパソコンは再び、押し入れにしまいました。流出ファイル自体もパソコンからは既に消去しました。こんな危ない資料を持ち続ける勇気は私にはありません。

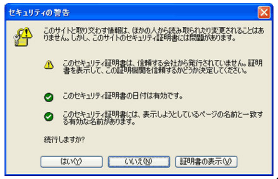
またWinnyで捜査資料流出…【ニュース斜め読み】, メディアの節穴, 2007年4月24日

出典：高木浩光＠自宅の日記2007.4.25（http://takagi-hiromitsu.jp/diary/20070425.html）

22

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
  - 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。



23

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

24

個人情報保護法

- **http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html** で全文を読むことができる。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：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。
- 第一章　総則（目的）
  - 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。

25

医療関連の情報倫理

- 医師の守秘義務
  - 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』
  - 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

26

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）
    - 6/30 三菱ウェルファーマ＠富山，7/1-2 久光製薬＠高松
  - 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）
  http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/index.html
  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）
  - 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

27