国立大学法人 長崎大学 NAGASAKI UNIVERSITY

個人情報保護研修会
（平成20年6月24日，中部講堂）

個人情報保護と日常からの情報セキュリティ

情報メディア基盤センター
データベース部門　上繁　義史

AGENDA

- 個人情報保護
  - 法律の概要
  - 情報漏洩の原因ベスト10！
  - ケーススタディ:Pマーク取得企業での情報漏えい事件とその対応
- 日常からのセキュリティに向けて
  - 個人情報漏えい事故からの教訓
  - セキュリティ対策の方針例
  - 【参考】パスワードについて
  - 情報セキュリティ対策に終わりはあるか？
- まとめ

個人情報保護法

- 趣旨：
  - *WHO?* 個人情報取扱事業者が
  - *WHEN?* データベース化されている個人情報を活用するにあたって，
  - *WHOM?* 個人情報の所有者やそれによってサービスを受ける者等に対して
  - *WHAT?* 果たさなければならない義務を定めたもの

個人情報の有用性と
個人の権利利益を保護の
バランスをとることが大事

個人情報保護法の概要 【1】

- 個人情報取扱事業者：
  - 5,000人以上の個人情報をデータベース化して事業に利用する者
    - 電子媒体，紙媒体の区別はありません
- 長崎大学は国立大学法人です：
  - **行政機関に準じる扱い．**

    ⇒「独立行政法人等の保有する個人情報の保護に関する法律」
  - 法律上，一般の個人情報取扱事業者とは区別されます．

個人情報保護法の概要 【2】

- 個人情報
  - 生存する個人に関する情報で特定の個人を識別可能なもの
  - ご注意ください！
    - **個人情報かどうかは，情報の受取り手によって変わります！「個人の識別」がカギです.**
  - 本学での例：現職教職員の場合
    - 氏名＋所属＋職位 ⇒ 立派な個人情報です
    - 職員番号＋氏名 ⇒ 情報の受取り手が業界人であれば十分個人情報になります
    - メールアドレスのみ ⇒ 個人情報になるケースがあります.

個人情報保護法の概要 【3】

- 独立行政法人等の義務と責任
  - 保有の制限
    - 利用目的の明示
    - 利用目的上の必要以上の個人情報保有の禁止
  - 利用目的の明示
  - 利用及び提供の制限
    - 正確性の確保
    - 安全確保の措置
    - 従事者の義務
      - 守秘義務と不正利用禁止
    - 保有個人情報の提供を受ける者に対する措置要求
  - 個人情報ファイル簿の作成及び公表

情報セキュリティの発想が必要ですね

情報セキュリティを考える

- 基本精神を共有するところから始めましょう.
  - 敵（セキュリティリスク）を知り，
  - 己（情報資産やセキュリティ対策の現状と方針）を知れば
  - 百戦危うからず（正しく対応できる）

※全学教育科目「コンピュータ入門」（上繁担当）より

では**敵**を知るところから始めましょう

情報関連の事故の原因ベスト10

- 個人情報漏洩他，情報関連のトラブルの原因
  - （独）情報処理推進機構（IPA）「情報セキュリティ白書2007」より
- 2006年の10大脅威「脅威の“見えない化”が加速する！」
  - 第1位　漏えい情報のWinnyによる止まらない流通
  - 第2位　表面化しづらい標的型（スピア型）攻撃
  - 第3位　悪質化・潜在化するボット
  - 第4位　深刻化するゼロデイ攻撃
  - 第5位　ますます多様化するフィッシング詐欺
  - 第6位　増え続けるスパムメール
  - 第7位　減らない情報漏えい
  - 第8位　狙われ続ける安易なパスワード
  - 第9位　攻撃が急増するSQLインジェクション
  - 第10位　不適切な設定のDNSサーバを狙う攻撃の発生

情報関連の事故の原因ベスト10

- 個人情報漏洩他，情報関連のトラブルの原因
  - （独）情報処理推進機構（IPA）「情報セキュリティ白書2007」より
- 2006年の10大脅威「脅威の“見えない化”が加速する！」
  - 第1位　漏えい情報のWinnyによる止まらない流通
  - 第2位　表面化しづらい標的型（スピア型）攻撃
  - 第3位　悪質
  - 第4位　深刻
  - 第5位　ます
  - 第6位　増え
  - 第7位　減ら
  - 第8位　狙わ
  - 第9位　攻撃
  - 第10位　不

標的型（スピア型）攻撃

例：特定の個人（情報を持っていそうな人）に添付書類つきメールが送付されてくる

⇒添付書類のファイルを開いた途端，感染
（Word，Excel，PPT，PDF，一太郎ほか）

⇒自分のPCから情報が誰か（悪党）におくられる．

※特定の人しか感染していなため，発見も対策も困難です！

情報関連の事故の原因ベスト10

- 個人情報漏洩他，情報関連のトラブルの原因
  - （独）情報処理推進機構（IPA）「情報セキュリティ白書2007」より
- 2006年の10大脅威「脅威の“見えない化”が加速する！」
  - 第1位　漏えい情報のWinnyによる止まらない流通
  - 第2位　表面化しづらい標的型（スピア型）攻撃
  - 第3位　悪質化・潜在化するボット
  - 第4位　深刻化するゼロデイ
  - 第5位　ますます多様化する
  - 第6位　増え続けるスパムメ
  - 第7位　減らない情報漏えい
  - 第8位　狙われ続ける安易な
  - 第9位　攻撃が急増するSQL
  - 第10位　不適切な設定のDN

ボット

ボットのウィルスに感染したPC等が特定のサイトにリクエストを大量送信
⇒サイトを機能停止に追い込む.

※ボット感染者は被害者兼加害者

情報関連の事故の原因ベスト10

- 個人情報漏洩他，情報関連のトラブルの原因
  - （独）情報処理推進機構（IPA）「情報セキュリティ白書2007」より
- 2006年の10大脅威「脅威の“見えない化”が加速する！」
  - 第1位　漏えい情報のWinnyによる止まらない流通
  - 第2位　表面化しづらい標的型（スピア型）攻撃
  - 第3位　悪質化・潜在化するボット
  - 第4位　深刻化するゼロデイ攻撃
  - 第5位　ますます多様化
  - 第6位　増え続けるスパ
  - 第7位　減らない情報漏
  - 第8位　狙われ続ける
  - 第9位　攻撃が急増す
  - 第10位　不適切な設定

ゼロデイ攻撃

未公開の脆弱性をついたウィルスなどを用いた攻撃

※最近増加傾向にあるそうですが，決定的対策はありません．

情報関連の事故の原因ベスト10

- 個人情報漏洩
  - （独）情報処
- 2006年の10大
  - 第1位　洩
  - 第2位　紛
  - 第3位　紛
  - 第4位　洩
  - 第5位　ま
  - 第6位　増
  - 第7位　減らない情報漏えい
  - 第8位　狙われ続ける安易なパスワード
  - 第9位　攻撃が急増するSQLインジェクション
  - 第10位　不適切な設定のDNSサーバを狙う攻撃の発生

情報漏洩

- 記録媒体等の紛失・盗難
- 紙媒体の紛失・盗難
- ウィルス・ワーム
- メール等の誤配信
- 内部不正行為
- ファイル交換ソフト

※半分以上がヒューマンエラーが原因！

情報関連の事故の原因ベスト10

- 個人情報漏洩他，情報関連のトラブルの原因
  - （独）情報処理推進機構（IPA）「情報セキュリティ白書2007」より
- 2006年の10大脅威「脅威の“見えない化”が加速する！」
  - 第1位　漏えい情報のWinnyによる止まらない流通
  - 第2位　表面化しづらい標的型（スピア型）攻撃
  - 第3位　悪質化・潜在化するボット
  - 第4位　深刻化するゼロデイ攻撃
  - 第5位　ますます多様化するフィッシ
  - 第6位　増え続けるスパムメール
  - 第7位　減らない情報漏えい
  - 第8位　狙われ続ける安易なパスワード
  - 第9位　攻撃が急増するSQLインジェクション
  - 第10位　不適切な設定のDNSサーバを狙う攻撃の発生

安易なパスワード

パスワード管理は基本ですが，
案外抜け穴になってしまいます．

※あとで詳しくご紹介します．

情報関連の事故の原因ベスト10

- 個人情報漏洩他，情報関連のトラブルの原因
  - （独）情報処理推進機構（IPA）「情報セキュリティ白書2007」より
- 2006年の10大脅威「脅威の“見えない化”が加速する！」
  - 第1位　漏えい情報のWinnyによる止まらない流通
  - 第2位　表面化しづらい標的型（スピア型）攻撃
  - 第3位　悪質化
  - 第4位　深刻化
  - 第5位　ますま
  - 第6位　増え続
  - 第7位　減らな
  - 第8位　狙われ
  - 第9位　攻撃が急増するSQLインジェクション
  - 第10位　不適切な設定のDNSサーバを狙う攻撃の発生

SQLインジェクション

Webアプリケーションに不正なコードを含めて入力
⇒Webアプリがアクセスするデータベースから情報を盗み出される

※学内の業務関係のシステムでWebアプリが増えているので要注意です！

傾向と対策の変化

以前の傾向

目に見える影響

ウィルス感染で画面に影響など

個別に対策が可能

最近の傾向

影響が見えない

スピア型攻撃など人間心理の盲点をつく

利用者は

情報セキュリティ確保のための基本的な対策を講じる

管理者は、

総合的なセキュリティレベルを保つ、品質管理や保守作業と同様にセキュリティの体制を確保するなど、セキュリティを考慮した日々の運用を行う。

情報セキュリティを考える

- 基本精神
  - 敵（セキュリティリスク）を知り，
  - 己（情報資産やセキュリティ対策の現状と方針）を知れば
  - 百戦危うからず（正しく対応できる）

次に己を知るためのケーススタディを見ていきましょう

ケーススタディ～A社のばあい

- Pマーク取得企業A社での情報漏洩事件とその対応
  - 情報モラル向上を目的として以下の取り組みを実施：
  - セキュリティレベルを分けて，**入退室，アクセス管理，PC内情報の制御**
    - 最重要PCの使用は入退室管理室内で行う．
    - 同PCは社内ネットワークから分離
  - 意識改革として，カレンダーに標語入れるなど，**目に付くところからの啓発活動を実施．**
    - 情報保護の誓約書（全社員より収集）を『手書き』して提出
  - **社内試験の実施による知識，能力の確保**：情報管理資格試験の実施

ケーススタディ～事件発生！

- **2004年9月10日：役所発注の業務にて，プリントアウト帳票（住民情報入り）のゴミをそのまま破棄する事故を起こした**

⇒ゴミ集積所にて発見！元社員による事件．二次被害なし

- 上記事故発生からのA社の活動の概要は以下の通り：

【当日：9月10日】：廃棄書類発見（事故発生）

～役所から事業部門に連絡

～業務部門から本社に連絡

～社長へ連絡

【2日目：9月11日】：会社による元社員の身柄確保・事情聴取

～再発防止策の策定

～記者会見・TV報道～

ケーススタディ～事件発生！

- **2004年9月10日：役所発注の業務にて，プリントアウト帳票（住民情報入り）のゴミをそのまま破棄する事故を起こした**

⇒ゴミ集積所にて発見！元社員による事件．二次被害なし

- 上記事故発生からのA社の活動の概要は以下の通り：

【3日目：9月12日】：新聞報道

～A社緊急対策会議　～再発防止策実施準備完了

～HP上でお詫び掲載～

【4日目：9月13日】：再発防止策運用開始

～社長全社員メール送信

～お詫び・関係者処分　～顧客説明

～経産省，JISA（Pマーク審査機関）へ事故の報告

ケーススタディ～事件その後

- 事件対応のポイント：
  - **不測の事態が発生したときには，状況把握が危機管理の鉄則**
    - 報告・連絡の徹底が肝要！
  - **対応に当たって，企業の誠意を示すことが重要**
- 事件後のA社の対応：
  - A社：社員の啓発➡社員教育の緊急実施
  - 役所：委託業務先に対する緊急立ち入り検査を実施

    ➡当時A社は赤字決算

    ➡**情報処理関係のアウトソーシング事業の難しさを露呈**

ケーススタディ～事件その後

- 事件後の対応（つづき）
  - A社が再発防止対策8項目策定
    - 監視カメラ（ほぼ100%カバー），メディアシュレッダー，セキュリティBOX
    - 情報セキュリティ設備の強化
    - 個人情報保護の日を設定（9月10日）：毎年手書きで誓約書
      - **情報セキュリティ技術でまかなえる部分は小さい**
      - **企業文化そのもの（人間の問題）と考えるべし**

ケーススタディ～事件その後

- 事件後の対応（つづき）
  - A社が再発防止対策8項目策定
    - 外部委員会設置：必ず市民活動家（オンブズマン等）を入れる（アメリカで顕著）
    - 個人情報保護資格認定制度：職務内容に応じた資格取得
      - 派遣社員，臨時職員も義務付ける
      - 資格取得していないと社内業務ができない規則になっている．
    - 情報セキュリティクォリティコントロール（QC）活動
      - セキュリティ実施状況を表すシールをPCに貼り付ける
        - ≫ 例：PCの暗号化，持ち出し許可，個人情報なし
      - カレンダーなど身近なものに標語をつけて啓発

ケーススタディ～事件その後

- 事件後の対応（つづき）
  - この事件をまとめた書物「65時間」を発行し，全社員に配布（実名入りにつき社外秘）

■首長の質問：個人情報保護の研修に参加したことは　あるのか？

⇒元社員の回答：参加していたが全部他人事と思っていた.

意識の問題だった！

日頃からのセキュリティ対策に向けて

・ 個人情報漏洩事故からの教訓:

委託先や自宅から漏洩

USBメモリからの漏洩

(元)従業員からの漏洩

・ 管理不行き届きで持ち出された情報が漏れている！

脆弱性対策に抜けがあった

攻撃を受けていたことに気づかなかった

・ 対策漏れ，不注意が命取り

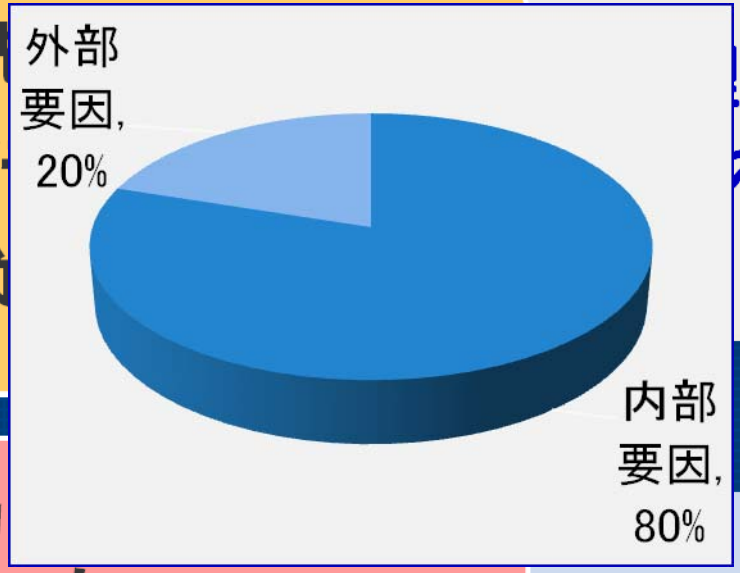
日頃からのセキュリティ対策に向けて

・ 個人情報漏洩事故からの教訓:

委託先

USBメ

(元)従



不行き届きで持ち
れた情報が漏れて
!

脆弱
があった

攻撃を受けていたこ
とに気づかなかった

・ 対策漏れ，不注意が
命取り

日頃からのセキュリティ対策に向けて

・ 個人情報漏洩事故からの教訓：

委託先や自宅から漏洩

USBメモリからの漏洩

（三）従業員からの漏洩

・ 管理不行き届きで持ち出された情報が漏れている！

不正持ち出し，盗難，紛失のルート例

内部犯行

1）電子データ
- 電子メール
- USBメモリ，ディスク等の外部媒体
- パソコン

2）紙などの物理的要素
- 印刷等による紙媒体の直接持出
- 電子データの複写機，プリンタによる印刷
- ファクシミリからの流出

3）外部からのハッキング，クラッキング

セキュリティ対策の方針例

情報メディア基盤センターでもセキュリティポリシにそって対策はとっていますが，各ユーザの協力が欠かせません．

- **情報を持ち出させないことが基本**
- **最も脆弱なのは人間なので，技術対策でカバー**
- **不正アクセスの兆候を見逃さない**

セキュリティ対策の方針例

【方針例・1】情報を持ち出させない

- PCの外部持ち出し

  ⇒持出時に氏名，用務先，用務，使用時間を記帳

  - 持出用PCを別途準備しておくケースもあります.
- USBメモリは暗号化を施したものに限り，学内でのみ使用を許可する.
  - USBメモリむけの暗号化ソフトを利用
  - インストール不要の暗号化ソフト付きUSBメモリの利用

セキュリティ対策の方針例

【方針例・1】情報を持ち出させない

- 委託する場合，契約で工夫を
  - 委託者と受託者の義務と責任の分担を明確に
    - 受託者の地震，火事などにおける緊急時対応，委託者へのヘルプ作業，瑕疵担保責任期間，情報化保険の加入　・・・
  - 個人情報の取扱いについて，受託者だけでなく，再委託に関する措置を明記.
    - 委託者への連絡，受託者による再委託先の監査，
    - 再委託先の問題で損害が発生した時の責任の所在等
- 退職者の不適切な情報持ち出しを防止

セキュリティ対策の方針例

【方針例・2】最も脆弱なのは人間なので，技術対策でカバー

- 構成員への意識徹底が大事：教育で対応
  - 例：仕事の情報を家に持ち帰らせない
  - 例：ファイル交換ソフトは設定・操作ミスでも情報漏洩の原因になる
- ウィルス対策ソフトを常にアップデート
- OSのアップデートを欠かさずに
- パスワードの適切な設定を
- PCを廃棄するときは，HDDを磁気破壊装置に
- データの暗号化：CRYPTREC推奨の暗号の利用等

【参考】パスワードのばあい

- パスワードの重要性:「本人しか知らない」が原則！
- パスワード漏洩の原因:パスワードクラッキング

本人から入手	推測	解析	盗聴
・ソーシャルエンジニアリング（直接聞き出し，廃棄物から読み取り，なりすまして盗み見）	・ユーザの情報を元に推測	・パスワードファイル入手 ・不正なツールで解析	・LANを監視 ・ログインセッション等からパスワード抽出

【参考】パスワードのばあい

- パスワード解読技術の恐怖
  - パスワード解析は辞書攻撃＋総当たり攻撃
    - 解析ツールはフリーソフトも製品もあり
  - 表：PCでの総当たり攻撃による解析完了までの時間
    - 条件：PC（CPU: Pentium III 1.0 GHz，メモリ250MB）
    - 小室孝雄，水野聡美，中村英徳，佐々木良一，「パスワード型および画像選択型個人認証方式の評価」，電子情報通信学会SITE研究会，2003年10月発表

NUNetのIDで設定可能な範囲

種類＼文字数	4	5	6	7	8
数字のみ	0. 13 秒	1. 25 秒	12.5 秒	2.08 分	20. 8 分
大小英字のみ	1. 52 分	1. 32時間	2.86 日	148 日	21. 2 年
英数字のみ	3. 08 分	3. 18時間	8.22 日	1. 4 年	87 年
特殊文字を含む	17 分	26.9時間	106 日	27. 7 年	2630 年

【参考】パスワードのばあい

- パスワードを保護するための対策（IPA推奨）

1. 推測しにくいパスワードを使う
   - 大文字・小文字・数字・記号の組み合わせ
   - 長めのパスワード
     - NUNetでは現在6文字以上8文字以下
   - 自前の変換ルールでパスフレーズを変換
     - 例：JINSEI IROIRO⇒J!NS5R%R
2. 定期的にパスワードを変更
3. パスワードは絶対に人に教えない

情報セキュリティ対策に終わりはあるか？

- 情報セキュリティ（対策）に終わりはありません
  - なぜなら，セキュリティリスクは常に変化するから
    - 新しい技術に伴うセキュリティホール，
    - 新たな攻撃技術の出現
    - 新しい脆弱性への対応不足，
    - ソーシャルエンジニアリングによる人からの情報聞き出し，
    - 廃棄物からの情報盗難など，
    - 「人」の脆弱性
    - ・・・・・・・

まとめ

- 個人情報保護
  - 法律の概要：独立行政法人等を対象とした法律
  - 情報漏洩の原因ベスト10：漏洩の「見えない化」が特徴
  - ケーススタディ：Pマーク取得企業での情報漏えい事件とその対応：迅速な対応と事件後の対策が重要！
- 日頃からのセキュリティ
  - 敵を知り，己を知れば，百戦危うからずや！
    - 敵：ウィルス・ワーム・脆弱性・人的エラー
    - 己：情報資産，セキュリティの技術・運用での対策
    - 百戦：情報資産の適正な管理・運用

参考文献及び情報源

- 辻井重男監修，萩原栄幸編集責任，デジタル・フォレンジック　研究会編，「デジタル・フォレンジック事典」，日科技連出版社，2006年12月
- 青柳武彦，「情報化時代のプライバシー研究　『個の尊厳』と『公共性』の調和に向けて」，NTT出版，2008年5月
- （独）情報処理推進機構編，「情報セキュリティ読本　IT時代の危機管理入門」，実教出版，2006年11月
- 菅野孝男，「実務者のための情報システム調達管理　第2版」，コンピュータ・エージ社，2006年2月
- 須藤修，小尾敏夫，工藤裕子，後藤玲子編，「CIO学　IT経営戦略の未来」，東京大学出版会，2007年11月

参考文献及び情報源

- 「平成19年度情報モラル啓発セミナー
  情報社会で企業に求められる情報モラル
  ー人権に配慮した個人情報の保護・情報セキュリティー」
  - （財）ハイパーネットワーク研究所主催，H19年7月13日京都市にて開催
- （独）情報処理推進機構（IPA）
  - ソフトウェアの脆弱性情報，ウィルスに関する情報をはじめ，人材育成，情報処理技術者試験等の情報が公開されている．
  - URL：http://www.ipa.go.jp/
- 総務省，「行政機関・独立行政法人の個人情報の保護」
  - 法令や基本文書，法制度に関する説明やFAQなどが公開されている．
  - URL：http://www.soumu.go.jp/gyoukan/kanri/kenkyu.htm

参考文献及び情報源

- 内閣府国民生活局，「【パンフレット】わかりやすい個人情報保護のしくみ」（平成20年4月発行）
  - 4部構成のパンフレットです：（1）個人情報保護法の概要，（2）いわゆる「過剰反応」の典型例，（3）個人情報保護に関する法体系，（4）よくある疑問と回答Q＆A集が公開されています．
  - URL： http://www5.cao.go.jp/seikatsu/kojin/kaisetsu/panfu08.html
- CRYPTREC
  - 電子政府推奨暗号の安全性を評価・監視し，暗号モジュール評価基準等の策定を検討するプロジェクト．電子政府推奨暗号リストを作成・公開している．
  - URL： http://www.cryptrec.go.jp/
- セコムトラストシステムズ（株），「情報漏洩対策サイト」
  - URL：http://www.secomtrust.net/infomeasure/rouei/column1.html

関連法令など

- 独立行政法人における個人情報保護関係の法令やガイドライン
  - 独立行政法人等の保有する個人情報の保護に関する**法律施行令**（平成15年政令第549号）
  - 独立行政法人等の保有する個人情報の保護に関する法律に係る行政手続等における情報通信の技術の利用に関する**法律施行規則**（平成16年総務省令第126号）
  - 独立行政法人等の保有する個人情報の保護に関する法律の施行に当たって**（施行通知）**
  - 独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（通知）**（安全確保指針）**

ご清聴ありがとうございました.