

# インターネット社会の安全対策

入門

## 何歳からの対策？

- 2009年まで
  - インターネットに繋がるPCが操作できる年齢 → キーボード入力のため
  - 9~10歳：小学校4年生…「ローマ字」を習う学年 → 新指導要領では小学校3年生
  - 無線LAN対応ゲーム機の発売まで → 2009年11月SONY PSPgo販売開始
  - ゲームカートリッジなし、オンラインソフトのみ
- 2010年以降
  - 2010年5月：iPad発売開始
  - ゲーム機を操作できる年齢
  - Wi-Fi等でインターネット接続
  - 3歳から！
  - 2013年：幼い向けタブレット発売開始
    - Meep (トイザラス2013~)
    - tapme (メガハウス2013~)
    - チャレンジ・タッチ (Benesse進研ゼミ2014~)
  - 14歳から刑事告訴から → 刑法としての著作権法
  - 2007年少年法改定：少年院送致年齢 → おおむね12歳以上 (小学5年生から)

## 安全対策：情報セキュリティ

- 定義：情報セキュリティ (Information Security) → 情報の機密性、完全性及び可用性を維持すること。更に、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい
- ISO/IEC 27001:2005 (JIS Q 27001)
- セキュリティの3要素
  - 機密性 (紙媒体と情報システム)：レベル1・2・3 → 情報の重要度
  - 完全性 (情報システム)：レベル1・2 → 性能の保証
  - 可用性 (情報システム)：レベル1・2 → バックアップと復旧
- 脅威 (インシデント) とリスク
  - 情報資産に対する脅威 (インシデント) → 危害を及ぼす、または発生する可能性のある事象
  - セキュリティ、コンテンツ、物理インシデント
  - 不正アクセス、不正書き込み、盗難、紛失、操作ミス、故障、天災等
  - リスク → 情報セキュリティの脆弱性により被害を及ぼす可能性
  - 脆弱性 → 脅威に対する攻撃に弱い状態のこと
  - なぜ脆弱性があるのか？ → PCは開発者向けに設計された情報機器 → システム内部の設定を自由に変更できる
  - マルウェア (Malware：悪意のあるソフトウェア) に侵される可能性大 → ウイルス、ワーム、スパイウェア、悪質なアドウェア、クラックツール等
- 脅威 (インシデント) の5W1H
  - What (なにを)？ → 通信インフラ攻撃から情報へ
  - Why (なぜ)？ → 功名心から金銭へ…グローバルな不正アクセスのビジネス化
  - When (いつ)？ → 週末・祝日… Patch Tue, Exploit Wed” → “0-day Attack”
  - Who (だれが)？ → 組織化、低年齢化、ドメイン内部の人的ミス
  - Where (どこで)？ → 米国 & 中国 & ブラジル & ナイジェリア経由…複数サーバ経由
  - How (どうやって)？ → 通信の脆弱性からブラウザの脆弱性狙い！

- 情報の防御
  - 情報システム内外の情報
  - 情報資産 → アナログ・デジタル媒体に記録された情報
  - アナログ媒体 (紙) 管理
    - 個人情報記録媒体 (紙) の管理は？ → 鍵付き引出、部屋
    - 個人情報記録の廃棄は？ → 燃やす or シュレッダー
  - デジタル媒体
    - PC内蔵ハードディスク・ドライブ：HDD、SSD
    - 外付け記録媒体 (HDD、USB、CD/DVD等)
    - オンラインストレージの活用 → SkyDrive, Dropbox, Evernote etc.
  - インターネット上の情報は記録されている！
  - PC・外部記録媒体の管理
    - パスワード保護、暗号化
    - バックアップ (定期的・周期的に！)

- コンピュータの防御
  - OS (Windows, MacOS, Linux) を最新の状態に保つ
  - OS以外のソフトウェアを最新の状態に保つ
    - JRE (Java Runtime Environment) は、SunからOracleへ
    - 脆弱性対策情報データベースサイトの活用 → myJVN
    - 無料オンラインウイルススキャン → Symantec etc.
  - ブラウザの使い分け…Internet Explorer だけは×
    - Internet Explorer, Firefox, chrome, Opera etc.
    - ブラウザのプラグインを最新の状態に保つ
    - Flash, QuickTime, Adobe Acrobat, Media Player etc.
    - SSL証明書のエラー → 即刻ブラウザ終了
    - 警告メッセージを読む

- ネットワークの防御
  - PCをネットワークに接続するということは → 双方向に情報のやり取りをしている → 有線・無線LAN共
  - 画面には表示されない → ネットワーク接続ポートのLEDで確認
  - PCのネットワーク接続 → ×プライベートネットワークでない
  - 〇パブリックネットワークである！ → スラム街ホテルの廊下をイメージ
  - PCのファイアウォール → ウイルス対策 (マルウェア対策) ソフトの限界
  - 有線ルータの設置を！ (バッファロー、コレガ等) = ファイアウォール機器

- マネジメント & コンプライアンス
  - 琉球大学情報セキュリティポリシー
    - 琉球大学情報システム運用・管理規程
    - 情報システム非常時行動計画に関する規程 → インシデント対応手順
    - インシデント発生・再発防止策に関する報告・申請書
  - 日本の情報政策の基本法「IT基本法」
    - サイバー犯罪、通信の秘密と情報開示
    - 電子商取引の推進とインターネット利用規制
    - 知的財産、個人情報保護、内部統制
  - 緩やかな保護規制により順次整備…現実とのギャップ

## インターネット社会の情報防御

- 個人情報の漏洩防止策が最も重要
  - 個人情報とは？ → 特定の個人を識別できるあらゆる情報…ユーザID・学籍番号も！ → 人格権 → プライバシー権
  - 個人情報保護法 (2005年施行) の個人情報とは？ → 生存する個人の情報
  - 個人情報 (5000件以上) データベースなどを事業用に持つ事業者対象
- 現状の企業内PC管理の矛盾 → PC管理であり、データ管理ではない
  - 個人携帯 (スマホ) はOK…???
  - 外部記録媒体の制限可能…???
- 琉大資産PC → 個人情報管理 → パスワードロック、施錠、外部媒体 (暗号化)
- 個人資産PCの活用 → 個人情報を分割し、個人情報がない情報活用等

## 「情報セキュリティ白書2013」10大脅威

- 1位「クライアントソフトの脆弱性を突いた攻撃」
  - 更新忘れのクライアントソフトが狙われている → Adobe Reader, Adobe Flash Player, Oracle Java (JRE)
  - ユーザの対策意識を高めることが重要 → Mac OSを狙うFlashbackマルウェア (Adobe Flash Playerのアップデートを装う)
  - 脆弱性対策に加え、被害の出にくいシステム設計を行う → 個々のPCにファイアウォール (ハード) を設置
- 2位「標的型諜報活動の脅威」
  - 知らない間にスパイがあなたの情報を盗んでいる → 金銭目的のサイバー空間上での諜報活動
  - 攻撃者によるウイルスを使ったリモートハッキング → 標的型メール攻撃…URLへ誘導 → PCハッキング
  - 外部からだけでなく、内部からの攻撃を想定した対策を → インターネットはパブリック・ネットワーク
- 3位「スマートデバイスを狙った悪意あるアプリの横行」
  - あなたの個人情報が狙われている → 金銭目的
  - 悪意あるアプリが情報を根こそぎ持って行く → 個人情報が多く保存されているスマートデバイス
  - 信頼できるアプリやサービスの利用を心がける → スマートデバイス用のウイルス対策ソフト
- 4位「ウイルスを使った遠隔操作」
  - 知らない間に濡れ衣を着せられることに！ → 被害者ではなく加害者へ
  - 知らない間にウイルスによって遠隔操作される → 自分のPCがDDoS攻撃への加担 (ポット化)
  - 日頃からPCを安全な状態に → 脆弱性対策 (アップデート)、ウイルス対策
- 5位「金銭窃取を目的としたウイルスの横行」
  - 日本でもインターネットバンキングが狙われている → 海外の猛威が日本のユーザを標的に
  - 認証情報を取られると他人の口座に送金される → SpyEyeウイルス対策
  - PCを健全にし、自衛に努める → 脆弱性対策 (アップデート)、ウイルス対策
- 6位「予期せぬ業務停止」
  - 自然災害やハードウェア障害、人的ミスが思わぬ事態を引き起こす → 日頃の堅実な運用・監視
  - 自然災害や障害は突然やってくる → 可用性対策！
  - 自然災害や障害を想定したシステムと運用を → システム設計・監視、アカウント/権限管理
- 7位「ウェブサイトを狙った攻撃」
  - 断続的に続くウェブサイトを狙った攻撃 → 脆弱性大：ウェブサイトはさまざまなアプリケーションで構成
  - さまざまな意図により狙われるウェブサイト → 情報の窃取、ウイルス配布、改ざん (主義・主張)
  - 開発から運用・監視まで幅広い対策を → システム設計・監視、アカウント/権限管理、脆弱性対策
- 8位「パスワード流出の脅威」
  - 知らぬ間にパスワードが盗まれていませんか？ → パスワードからパスフレーズへ、3か月 (四季) 毎の更新
  - オンラインサービス増加に伴うパスワード使い回しの現状 → サービス毎に別のパスワード・パスフレーズ
  - 安全なパスワードの運用・管理が重要 → アカウント/権限管理、パスワード更新設定
- 9位「内部犯行」
  - あなたの職場は大丈夫？内部に潜む犯行者 → 元雇用員、非正規雇用員
  - 金銭目的での内部犯行が多発 → 2012年度統計：内部犯行の動機の32%が金銭目的 → 組織への不満、転職目的が26%
  - 不正を起こしづらい状況を創出 → アカウント/権限管理、ポリシー/ルール
- 10位「フィッシング詐欺」
  - あなたの口座から預金が無くなっていませんか？ → インターネットユーザをターゲットにしたフィッシング詐欺が横行
  - メールとウェブサイトを使った詐欺行為 → 大手銀行を装ったフィッシング詐欺
  - 注意深い対応・対処を心がけること → 教育/啓蒙、アカウント/権限管理

Source → <https://www.ipa.go.jp/security/vuln/10threats2013.html>