

インターネット社会の安全対策

入門

安全対策：情報セキュリティ

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
 - 3歳から！
 - 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
 - 2013年：幼児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)

定義：情報セキュリティ (Information Security) ISO/IEC 27001:2005 (JIS Q 27001)
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

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

- 情報資産 情報システム内外の情報
 - 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 だけでは×
 - 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はない！
 - 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
 - 順次、規程作成…？
 - 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を識別できる情報
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…???
- 組織資産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