

インターネット社会の安全対策

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 27001:2013 (JIS Q 27001)
情報の機密性、完全性及び可用性を維持すること。
+ (真正性、責任追跡性、否認防止、信頼性) 等特性

情報セキュリティのCIA (3要素)

- Confidentiality-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
- Integrity-完全性 (情報システム) : レベル1・2 → 情報の完全性、性能の保証
- Availability-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PC
 - 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 → 情報
- Why (なぜ)? → 功名心 → 金銭…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 → ブラウザの脆弱性狙い!

安全対策：情報セキュリティ

情報の防御

- 情報資産 → 情報システム内外の情報
- 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 → リスク大
 - 外付け記録媒体 (HDD, USB, CD/DVD等) → リスク小
 - オンラインストレージの活用 → OneDrive, Dropbox, Evernote etc. → 暗号化必須!
- インターネット上の情報は全て記録されている! → 画像ファイルの脅威: Exif (Exchangeable image file format) 情報
- PC・外部記録媒体の管理
 - パスワード保護、暗号化が必須!
 - WinOS用: アタッチケース → <http://hibara.org/software/attachecase/>
 - オンラインストレージ用: Cloudfogger → <https://www.cloudfogger.com/en/>
 - 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×
 - Firefox, Chrome, Opera, Sleipnir 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
- ネットワーク・ファイアウォールの限界
- 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
 - 順次、規程作成…?
- 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…ユーザーID・学籍番号も!
- ! 人格権 → プライバシー権とは異なる個人情報保護法
- 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

プライバシーに関する個人情報の管理 → 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

- BYOD (Bring your own device) の積極的活用
- 個人情報を分割し、個人情報がない情報活用等

個人情報漏えい状況2014年度 (経済産業省2014年12月)

- 業種：金融業と電気業で60%以上の報告
- 漏えいした人数：10人以下が80%以上、1%程度の大規模な漏えい事案は増加
- 原因：人的ミスによる漏えいが80%以上、不正アクセスはわずか2%
- 事例：2014年7月教育関係事業会社委託先業者が顧客情報持ち出し販売 (約2.895万件) 個人情報保護法 (6月30万) で起訴ではなく、不正競争防止法 (5年500万) で起訴!

情報セキュリティ 10大脅威2015

- 1位「インターネットバンキングやクレジットカード情報の不正利用」
 - 2位「内部不正による情報漏えい」
 - 動機：不満、機会：誰の操作も特定不能、正当化：情報価値の軽視
 - 2014年7月ベネッセによる個人情報流出 (3504万件)：委託先業者の社員の犯行、顧客補償費約200億円
 - 東芝の研究データ韓国SKハイニックスに流出：業務提携サンディスク社員の犯行、損害賠償約330億円
 - 3位「標的型攻撃による諜報活動」
 - 4位「ウェブサービスへの不正ログイン」
 - 5位「ウェブサービスからの顧客情報の窃取」
 - 6位「ハッカー集団によるサイバーテロ」
 - 7位「ウェブサイトの改ざん」
 - 8位「インターネット基盤技術を悪用した攻撃」
 - 9位「脆弱性公表に伴う攻撃」
 - 10位「悪意あるスマートフォンアプリ」
- Source → <https://www.ipa.go.jp/security/vuln/10threats2015.html>