2009．06．05
第13回サイバー犯罪に関する白浜シンポジウム

情報セキュリティってそもそも何だっけ？

総務省　総合通信基盤局
事業政策課　高村　信

はじめに（お断り）

- 本日の内容は、あくまで「個人」としてお話しするものであり、総務省の政策・施策とは関連性はありません。

- 私自身の業務とも乖離があるため、「個人的調査研究」に過ぎない部分もあります。
  現状に即したお話になっていない可能性がある旨、あらかじめご了承ください。

- 全くの新ネタ（＆多分二度とやらないネタ）なので、
  詰まった時はご

一見見えない所は、あくまで一見見えないようにしてあるだけです

まずはおさらい

おさらい（その１の１）

- OECD 情報セキュリティガイドライン（１９９２）
  - すべての基本
  - 情報セキュリティの目的を「情報システムセキュリティの目的は、情報システムに依存する者を、可用性、機密性、完全性の欠如に起因する危害から保護することである。」と定義

    - 可用性（Availability ：データ、情報、情報システムが、適時に、必要な様式に従い、アクセスでき、利用できること。
    - 機密性（Confidentiality）：データ及び情報が、権限ある者が、権限ある時に、権限ある方式に従った場合のみ開示されること。
    - 完全性（Integrity）：データ及び情報が正確(accurate)で完全(complete)であり、かつ正確さ(accuracy)、完全さ(completeness)が維持されること。

日本語訳は、（独）情報処理振興機構「 OECD 情報セキュリティガイドライン見直しに関する調査」(2003.5)による

おさらい（その１の２）

- OECD 情報セキュリティガイドライン（1992）つづき
  - ９つの原則
    a. **責任の原則（Accountability Principle ）**
    情報システムの所有者、提供者、利用者その他情報システムセキュリティに関わる者の任務および責任を明確にすべきである。
    b. **認識の原則(Awareness Principle)**
    情報システムへの信頼を高めるため、情報システムの所有者、提供者、利用者その他関係者は、セキュリティ維持と矛盾のないように、情報システムセキュリティのための手段、慣行および、手続の存在と、およその範囲について容易に適切な知識を得ることができるようにすべきであり、また、知らされるべきである。
    c. **倫理の原則(Ethics Principle)**
    情報システムおよび情報システムセキュリティは、他の者の権利と合法的な利益を尊重して提供され利用されるべきである。
    d. **多面的考慮の原則(Multidisciplinary Principle)**
    情報システムセキュリティのための手段、慣行および、手続は、技術、行政、組織、運営、営業、教育および、法律を含むその問題に関連するあらゆる考え、視点を考慮し、斟酌すべきである。
    e. **比例の原則(Proportionality Principle)**
    セキュリティへの要求は、個々の情報システムによって異なるのであって、セキュリティのレベル、コスト、手段、慣行および、手続は、適正であり、かつ情報システムの価値と要求される信頼度、セキュリティが破れた場合の被害の深刻度、発生の可能性、広がりに比例したものであるべきである。
    f. **統合の原則(Integration Principle)**
    情報システムセキュリティのための手段、慣行および、手続は、一貫したシステムセキュリティ創出のため、相互に、かつ、組織内の他の手段、慣行および、手続と調和的、統合的に行われるべきである。
    g. **適時性の原則(Timeliness Principle)**
    情報システムセキュリティへの侵害を防止し、かつ、それに対応するため、公共部門および民間部門は、国内・国際の両レベルにおいて、時宜に応じ協調的に行動すべきである。
    h. **再評価の原則(Reassessment Principle)**
    情報システムおよびそれに対するセキュリティの要求は時と共に変わるため、情報システムセキュリティは定期的に再評価されるべきである。
    i. **民主主義の原則(Democracy Principle)**
    情報システムセキュリティは、民主主義社会におけるデータと情報の合法的な利用および流通と整合のとれたものとすべきである。

日本語訳は、（独）情報処理振興機構「 OECD 情報セキュリティガイドライン見直しに関する調査」(2003.5)による

おさらい（その2）

- OECD 情報セキュリティガイドライン改訂版（2002）
  - a culture of security
  - 対象を公的部門・民間部門の「システム」関係者から、個人利用者を含む「参加者（participants）」に拡大
  - セキュリティマネジメントの概念を導入。
    - 「セキュリティマネジメントの原則」のほか、「リスクアセスメントの原則」「セキュリティの設計及び実装の原則」「再評価の原則」など、マネジメントプロセスを規定。
    - これに伴い、9原則は再マップ（内容はあまり変わっていない）
  - 困ったことに、「情報セキュリティとは何ぞや」という定義が消えた。
    ⇒　個人的には、これが自己目的化の原因と認識

日本語訳は、（独）情報処理振興機構「 OECD 情報セキュリティガイドライン見直しに関する調査」(2003.5)による

おさらい（その３）

- ISMSというか、ISO/IEC27000シリーズというか
  - 大雑把にいえば、セキュリティリスクを許容可能なレベルに低減させるべく、「努力する仕組みがあるか」を認定。
    - Plan：「資産の特定」⇒「脅威分析（含む脆弱性分析）」⇒「リスクアセスメント」⇒「対策検討」及び「残存リスク確定」
    - Do　　：対策実施
    - Check＆Action：監査及び見直し
  - ISMS自体は、セキュリティリスクを低減させる仕組みではない。
  - そして、「第三者認証」という「錦の御旗」（というか麻薬）が存在。

おさらい（その４：まとめ）

- そもそも「情報セキュリティ」とは、「情報システムの利用にまつわる被害を無くす」ことが目的であったはず。
- 「リスク」＝ $\sum$「驚異の発生確率」×「被害」
  というアセスメントを実施し、現実的な対応をすれば良いはず（「比例の原則」）。
- 情報セキュリティ対策は、組織内の手段・慣行・手続きと「調和的に」導入されるべきものであったはず（「統合の原則」）。

⇒　そんなに難しい話ではないはず？

サブタイトル
（当日発表）

個人的に思うところの発端

- OECDプライバシ8原則（1980年）の実装化であるはずの、個人情報保護法にまつわる議論
- 住民基本台帳ネットワークにまつわる議論

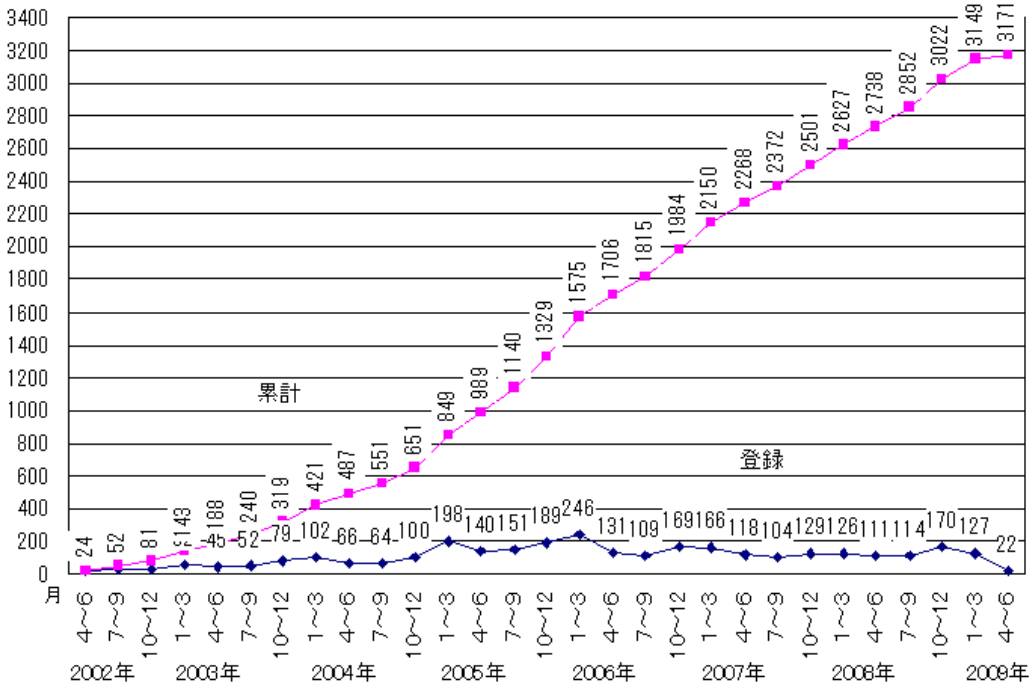
輪をかける国民性（その1）

- 「最大限の努力をしています」と言わないと許してもらえない雰囲気
  - プライバシーマーク、ISMS取得企業数はウナギ登り

プライバシーマーク所得数

http://privacymark.jp/ より（5／20現在）

ISMS認証取得組織数推移（国内）



日本情報処理開発協会Webサイトより（5／15現在）

輪をかける国民性（その2）

- ISMSをちゃんと運用できているんでしょうか？

ISMS認証取得組織数

World results	Dec. 2006	Dec. 2007
World total	5 797	7 732
World growth	–	1 935
Number of countries/ economies	64	70

The ISO Survey – 2007
http://www.iso.org/iso/iso9000-14000/pdf/survey2007.pdf

さらなる問題の発生

- 「リスク」＝$\sum$「警異の発生確率」×「被害」

結果巻き起こること

- 何でもかんでも、
  - 機密性2情報
  - xxxx co. confidential
- 何はともあれ、
  - 個人情報漏えいのお詫び
  - 添付ファイルは暗号化。でも、その直後のメールでパスワード送付。

本質的な対策

CyberとRealに差は無い

- 大は小を兼ねない。
- ニコイチは所詮ニコイチ。
- 大事なものは、大事にとっておく。
  - なぜ、「外部接続用」と「内部業務用」を分けられないのか？
    - 「外部接続用」は、webとメールのブラウジング専用（Knoppixで十分）
    - 内部業務用は、全部closed network化。
    - 内部と外部を繋ぎたい時は、全部関門局経由。そもそもISMSやってれば、外部送信や外部からの受け入れは、第三者の許可を取るプロシージャになってるはず。
    - 実はサボり防止に、きわめて効果的

セキュリティ対策と責任追及は相反

- 意外と忘れられているが、フォレンジクスのためのデータは、大本のデータよりも余程危険である。
- 「情報漏えいがあったときのために」フォレンジクスデータを取っているなら、今すぐ捨てたほうがよい。フォレンジクスデータを安全に管理できるのであれば、大本のデータも当然安全に管理できる。
- 「どうせワークフローがシステムに乗っている」からアクセスを監視すれば業務統制ができる、という発想と、「システム利用を統制しよう」という発想の間には、大きな違いがある。

業務継続と異常対応

- 多分、永遠に交わることの無いテーマ
- 民間企業（特にインフラ企業）にとって、「役務を止めない」ことは、何よりも優先される事項
- 一方で、その場しのぎの対応は、原因究明の証拠を破壊する行為でもある

本当に守る価値があるのか？

- 身もふたも無い言い方ですが、

非常に簡単なテスト

- ぜひ一度やって（やらせて）みましょう。

最後に

- 情報セキュリティ政策の言いだしっぺの一人ではありますが、最近の情報セキュリティ対策の自己目的化の激しさには閉口しています。
- 情報セキュリティは、本質的には、participantsの端くれである木っ端役人にも理解できるレベルの話のはずです

- どこかで「風評対策」をまじめにやらないと、無駄なコストばかり掛かる事を懸念しています。どうしたらいいんでしょう？