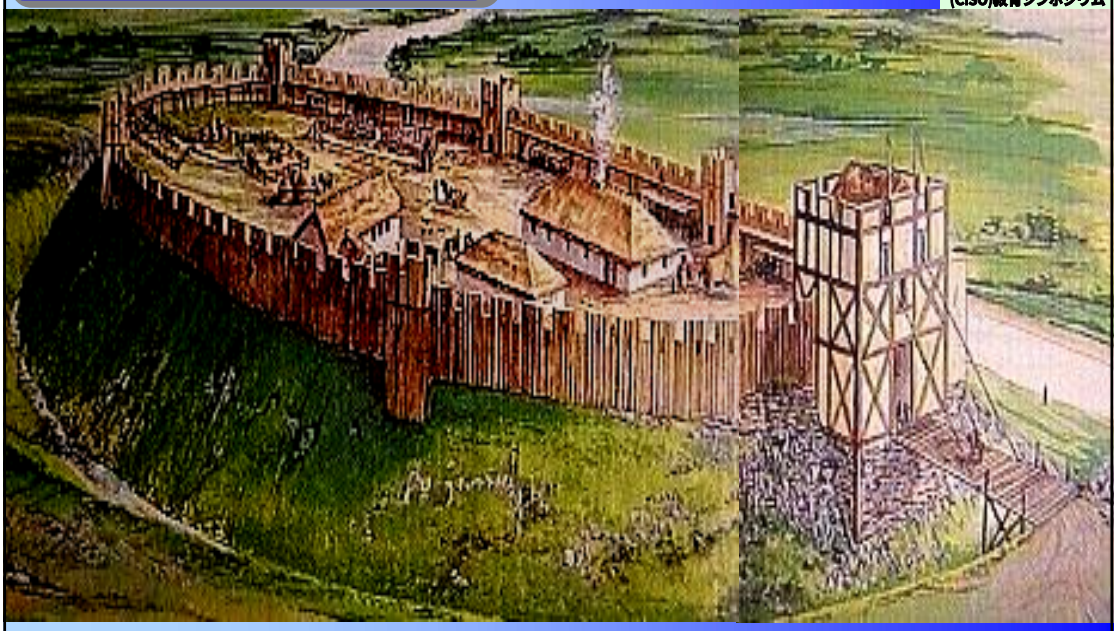
情報セキュリティ管理者（CISO）教育について

2006年7月12日
情報セキュリティ管理者（CISO）教育シンポジウム



情報セキュリティ大学院大学　　内田　勝也（uchidak@gol.com）

はじめに

「個人情報保護法」の完全施行（2005年4月）

「金融商品取引法（日本版SOX法）」の成立（2006年6月）

止まらない機密情報、個人情報の漏えい

情報リスク分野の広がり

個人情報、機密情報の漏洩
内部統制の強化

セキュリティ技術だけでは解決しない？

- インターネット接続サービスの加入者約450万人の個人情報が流出
- オンラインゲーム運営会社ハードディスクが紛失し、約6万4200人分の個人情報が流出
- 生命保険会社営業担当社員が顧客約3400人分の個人情報が入ったパソコンを電車内に置き忘れた
- 病院を退職した医師が自宅で空き巣にあい、267人分の患者情報が入ったノートパソコン2台を盗まれた
- メーカーの社員が車上荒らしで顧客のメールアドレス1，631件が保存されたパソコンが盗まれた
- 女性用下着メーカーのe-Commerceサーバーに不正アクセスがあり、顧客4,757人分の住所や電話番号、クレジットカード情報が流出
- 自衛隊が配備する地対艦誘導ミサイル（SSM－1）の運用システムなどに関する内部教育用資料が、ファイル交換ソフト「Share」を介してネット上に流出。 流出は、フロッピーディスク275枚分に相当
- 県警の事件関係者の氏名など延べ約4400人分の個人情報がファイル交換ソフト「Winny」を介してネット上に流出

はじめに

株主総会事項に

- 東京都内で株主総会を開き、インターネット接続サービスの加入者約450万人の個人情報が流出したことについて、社長が「多大なご迷惑をかけておわびします」と陳謝、原因究明と再発防止に全力を挙げる考えを示した。
- 株主からは、情報管理の甘さを指摘する厳しい質問が相次いだ。社長は、個人情報を扱う部署への指紋認証制度導入などセキュリティー対策を説明。「社員、委託会社に対するコンプライアンス（法令順守）研修をより一層強化する」と述べた。

ログの管理不十分？

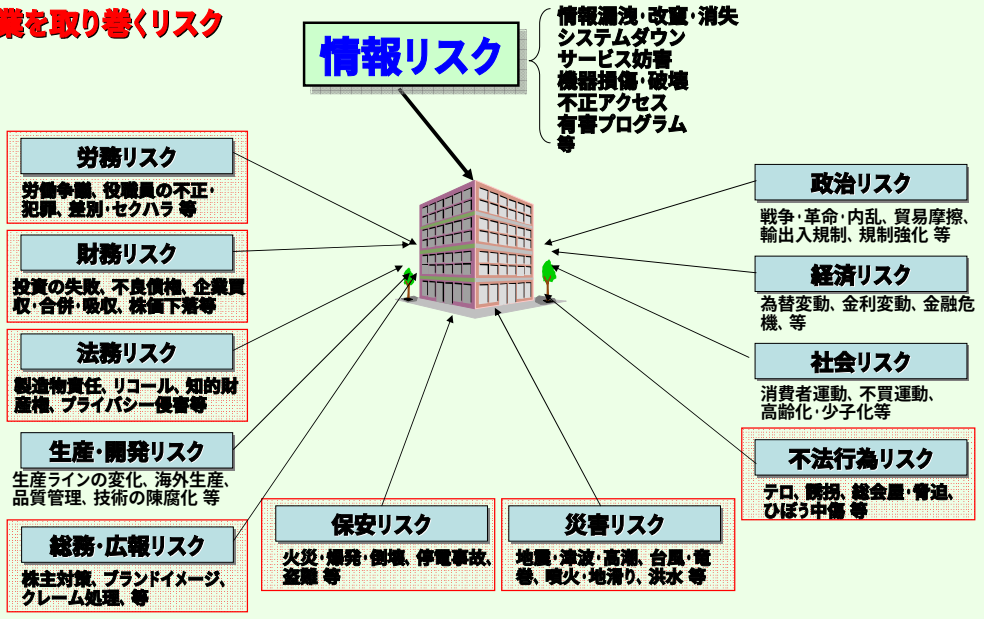
- 流出元と見られる保守用のパソコンはICカードで入退室が管理されたシステムルームにあり、社員48人、業務を委託していたシステム会社の社員177人が利用できる状態にあったという。外部から不正侵入することは不可能だったという。
- しかし、アクセスログの保存期間が1年間だったため、当時のログがなく、誰がデータベースにアクセスしたかは分かっていないという。

参考：ログ記録が役立たない（ない？）

- ある個人情報漏洩企業が、原因を追及した結果報告
  - 弁護士を含めた社内外の専門家で調査を行ったが、最後の1人に絞れなかった。
  - 当社及び子会社に設置してある数台のコンピュータを利用した約20名であることが判明したが、それ以上は強制力をもたない調査委員会の限界である。

情報リスクの広がり

企業を取り巻くリスク



実践「危機マネジメント」ぎょうせいより、筆者による追加・編集

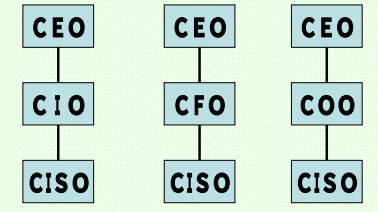
はじめに

「個人情報保護法」の完全施行（2005年4月）
「金融商品取引法（日本版SOX法）」の成立（2006年6月）
情報リスク分野の広がり

企業・組織における情報リスク対応

マネジメント支援者／プロジェクト推進者へ
情報セキュリティ管理者：
CISO (Chief Infromation Security Officer)

C レベルの役職者が全て役員とは考えていません

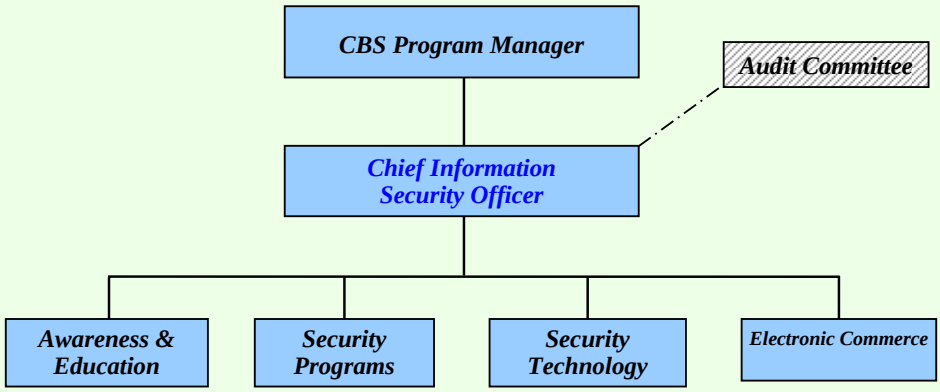


CISOの位置づけ

Katsuya Uchida uchidak@gol.com

はじめに 参考

Corporate Information Security Office



- Awareness
- Communication
- Education

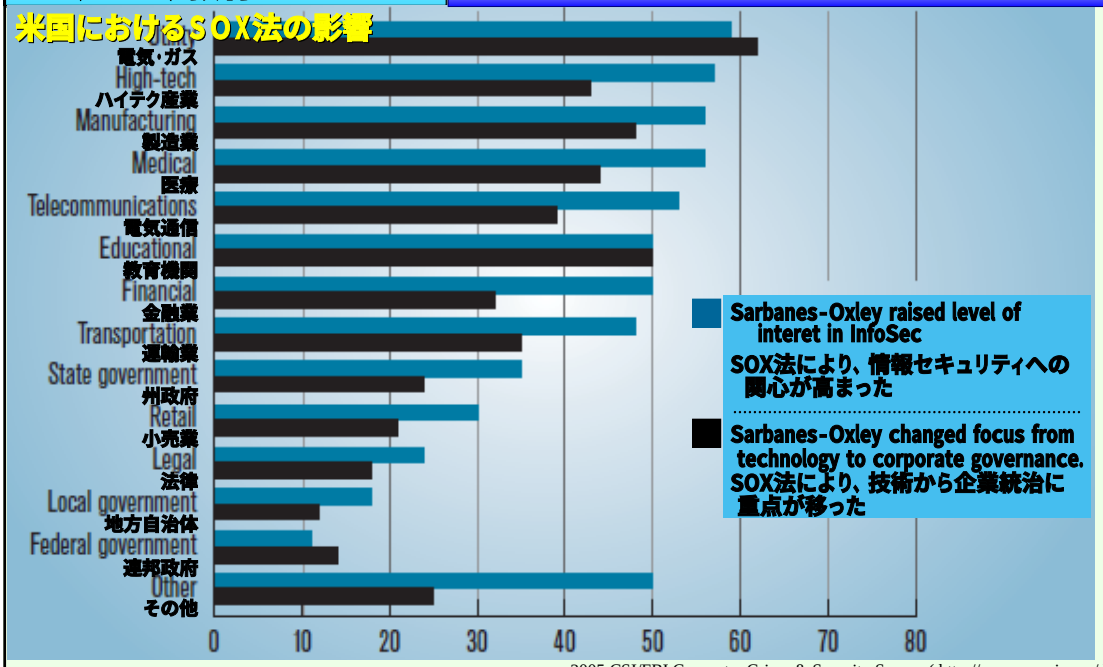
- Policy & Standards
- Business Support
- Security Officer Support

- Hacking
- Investigations
- Product Selection

From Citybank

Katsuya Uchida uchidak@gol.com

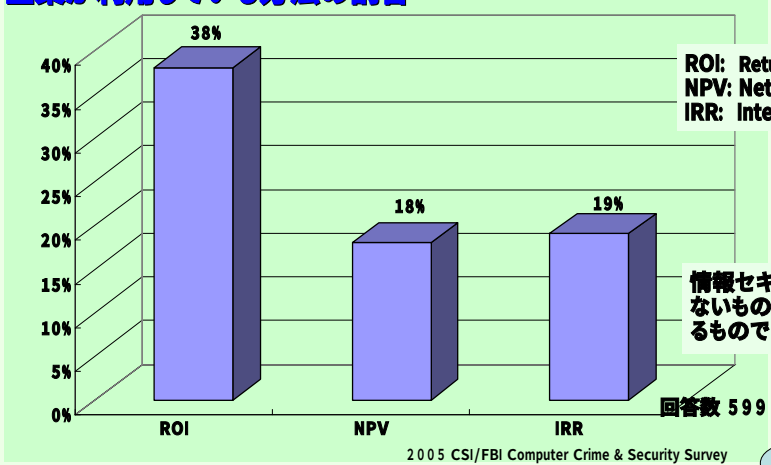
米国におけるSOX法の影響



2005 CSI/FBI Computer Crime & Security Survey (http://www.gocsi.com/)

Katsuya Uchida uchidak@gol.com

日米における投資対効果で企業が利用している方法の割合



ROI: Return on Investment 投資収益率
NPV: Net Present Value 正味現在価値
IRR: Internal Rate of Return 内部収益率

情報セキュリティ投資はやらなければならないものであり、「費用対効果」を計算するものではないとの考えもあるが・・・

2005 CSI/FBI Computer Crime & Security Survey

この差はどこにあるのだろうか？

国内調査 (2006年1月 筆者による実施) 中央大学21世紀COEによる調査研究

ROI	NPV	IRR	不明・その他	未実施
1%	0.3%	0.4%	9.6%	88.7%

合計 17 企業・組織　94 企業・組織　回答数 980

「第3回 情報セキュリティ調査」より
http://www2.gol.com/users/uchidak/

Katsuya Uchida uchidak@gol.com

海外のCISO教育事例

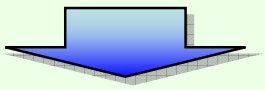
Chief Security Officer Executive Certificate

- カーネギーメロン大学CyLabが実施している管理者コース
- 下記8コースは 3日間の講座となっている
  - Strategic Planning & Leadership（戦略計画とリーダーシップ）
  - Organizational Management & Negotiation Strategies（組織管理と交渉戦略）
  - Smart Budgeting, Spending & Metrics（予算作成、支出、対比）
  - Physical Security（物理的セキュリティ）
  - Risk Management & Business Continuity Planning（リスクマネジメントと事業継続計画）
  - Law, Investigation, Ethics & Privacy（法制度、捜査、倫理、プライバシー）
  - Information Security（情報セキュリティ）
  - Key Technologies & Emerging Trends（重要技術と最新動向）
- コースの参加費： 2,400ドル（約28万円）／コース
  全コース参加費用合計： 約2万ドル（約 220万円）
- 修了後、CyLabから修了証が交付される

http://www.cylab.cmu.edu/default.aspx?id=760 より

情報セキュリティ管理者（CISO）

- 情報セキュリティ ＝ 技術 からの脱却を目指す
- 情報セキュリティを統括して考えることのできる管理職（役員補佐）の育成
- 経営トップに情報セキュリティ政策を具申できる知識・能力を持った者
- 個人としての知識・技術だけでなく、プロジェクトマネジメントができる情報セキュリティ管理者の育成を行う
- 大規模なセキュリティインシデント発生時に、経営者を補佐し、関連部門を統括して対応できる人材の育成
  リスクコミュニケーション（事後処理対応）の重要性の増大
  - 役員／社長室
  - 情報システム
  - 人事
  - 広報室
  - 法務部
  - 総務
  - 経理
- 情報セキュリティの理論（座学）だけでなく、実践に対する知識・経験を持つ者を目指す。



新しい情報セキュリティ管理者像の確立

教育方法について

- **講義形式**
  - 単純な集合方式だけでなく、ネットワークを利用したe－ラーニング方式（含 CD-ROM、動画）も含む。
  - 初期段階での教育には効果的であり、参加者間の切磋琢磨が可能。
- **実習形式**
  - 実際にシステムの設定やソフトウェアの導入等を通して、多くの問題を経験でき、またその解決方法を学ぶことが可能になる。
  - また、他人が構築したシステムの脆弱性調査を行い、その結果を基に、報告書作成を行う。
- **ケーススタディ・プレゼンテーション形式**
  - 過去に発生した事例を基に、複数の機器で作成されたログを調査し、原因調査、報告書作成、プレゼンテーション等を行う。
  - 稼働システムについて、脆弱性調査を実際の現場で行い、その結果について一連の処理（調査・報告書作成・プレゼンテーションなど）を行う。
  - 数人でのチーム作業、個人で対応、を体験させる。

■ **教育方法における基本的な考え方**（当然だが）
- 既知の知識を教えるのでなく、新しい問題が発生した場合、
  ①それらへの対応能力
  ②解決方法の発見能力
  をつける方法

全ての形式を単独でやるだけでなく、
1つの講座で色々な形式があってよい

CSO／CISO教育概観

以下のような講義を想定（環境の変化により講義内容は更新）

- 暗号・認証と社会制度
- インターネットテクノロジー
- セキュア社会制度論
- セキュリティの法律実務
- セキュア法制と情報倫理
- 個人識別と個人情報保護
- セキュリティ管理と経営
- 情報セキュリティマネジメントシステム
- リスクマネジメント
- セキュリティシステム監査
- プレゼンテーション技法
- セキュアシステム実習
- プロジェクト・マネジメント講座
- CISSP講座／SANS GIAC講座

上記講義を4科目以上履修

- セキュアシステム実習は必修
- CISSP or GIAC 資格の修得
- プロジェクトマネジメント履修

CSO／CISO教育概観

暗号・認証と社会制度 インターネットテクノロジー マネジメント プレゼンテーション 社会心理学／行動心理学 （英　語）	情報セキュリティマネジメント	プロジェクトマネジメント	法制度 ガイドライン 倫理（CSR）
	セキュアシステム実習		
	情報セキュリティ基礎知識		

広く深い知識・経験が求められるが・・・

Katsuya Uchida　uchidak@gol.com

情報セキュリティ管理者(CISO)教育について

CSO／CISO教育概観

情報セキュリティ基礎知識

- CSO／CISOとして、必要とされる基礎的な知識を体系的に修得する
- ピンポイント的な知識を求めるのではなく、関係する分野を俯瞰できる知識

A) 情報セキュリティマネジメント
B) セキュリティアーキテクチャー
C) アクセス制御
D) アプリケーションセキュリティ
E) 運用
F) 暗号
G) ネットワークセキュリティ
H) 物理的セキュリティ
I) 事業継続計画（BCP／BCM）
J) 法律・情報法科学（Information Forensics）・情報倫理
K) CISO倫理綱領

Katsuya Uchida　uchidak@gol.com

セキュアシステム実習

- ネットワークセキュリティの基礎的な経験の修得
- 不正侵入とその防御、検知について、実践的な実習を体系的に経験する
- 敵を知り、己を知らば、百戦危うからず

A) 情報収集方法
B) ネットワークレイヤへの攻撃
C) バッファーオーバーフロー攻撃
D) DNS (Domain Name System) への攻撃
E) ウェブサーバ (IIS、アパッチ) への攻撃
F) ウェブアプリケーションへの攻撃 (クロスサイトスクリプティング、SQLインジェクション)
G) スパイウェアとその検出方法
H) バックドアとrootkit
I) 総合演習

情報セキュリティマネジメントシステム

- 企業・組織におけるセキュリティマネジメント体制の構築

A) セキュリティ基本方針
B) 情報セキュリティのための組織
C) リスクマネジメント注
D) 監査の考え方注
E) 資産管理
F) 人的資源のセキュリティ
G) 物理的及び環境的セキュリティ
H) 通信及び運用管理
I) 情報システムの取得、開発及び保守
J) 情報セキュリティインシデント管理
K) 事業継続計画
L) 順守

(注) 講座として独立のものも想定

プロジェクトマネジメント

- 企業・組織の基盤として、情報セキュリティを考えると1人あるいは少数で対応できない
- 情報漏洩事件が発生すれば、「リスクコミュニケーション（事後対応）」等も必要になる

⇒ 事後対応のまずさは事件の大きさ以上に問題を拡大する

A) プロジェクトマネジメントとは
B) プロジェクトを立上げる
C) スコープを定義する
D) スケジュールを作成する
E) コストを見積る
F) 品質を管理する
G) プロジェクトチームを動かす
H) リスクを考える
I) 外部から調達する
J) プロジェクトを計画・実行し、実績を報告する
K) プロジェクトを監視し、変更を管理する
L) プロジェクトを終結する
M) プロおよび社会人としての責任

PMBOKやPM等の考え方を
実務との関連させて学ぶ
講義・チーム学習、プレゼンの組合せ

Katsuya Uchida uchidak@gol.com

その他

- 企業・組織を情報セキュリティ分野から対応できる管理者の育成
  - 情報セキュリティの推進： 教育・周知・・・
  - 事件・事故後の対応
- プレゼンテーションスキル
  - 経営者や利用者への情宣
- 行動心理学・社会心理学
  - ソーシャルエンジニアリング等、人間の心理的弱さを狙った攻撃への対応
  - ノートPCを車内に置き忘れる等への対応
  - 誤った情報セキュリティ製品（サービス）による過度なストレスへの対応
  - 安全・安心、信頼を与えるための方法
- ・・・・

Katsuya Uchida uchidak@gol.com

まとめ

- CSO／CISOの定義は？
- 米国：CISO修士コースでは、Javaプログラミングが前提知識もあるが
- 全能者には成れないが・・・
  情報セキュリティの広がりを考えると、コンピュータ技術者、ネットワーク技術者、法務担当、広報（リスクコミュニケーション）、人事（就業規則違反、SP違反）部門等との共同作業（プロジェクトリーダの役割）が必要？
- 情報セキュリティ戦略、予実算管理等の対応も

4割の企業で非常に重要な脆弱性が見つかっている
NHKスペシャル

- 3～4ヶ月程度での可能な限り育成を目指す
- 継続育成制度で、変化の激しい内容への対応
- 資格制度？　⇒ 産学協同？

真の専門家の育成を！

2007年問題
システム部門退職者の受け皿（？）にも

Katsuya Uchida　uchidak@gol.com

まとめ

以下のような講義を想定（環境の変化により講義内容は更新）

- 暗号・認証と社会制度
- インターネットテクノロジー
- セキュア社会制度論
- セキュリティの法律実務
- セキュア法制と情報倫理
- 個人識別と個人情報保護
- セキュリティ管理と経営
- 情報セキュリティマネジメントシステム
- リスクマネジメント
- セキュリティシステム監査
- プレゼンテーション技法

上記講義を4科目以上履修

- セキュアシステム実習
- プロジェクト・マネジメント講座
- CISSP講座／SANS GIAC講座

- セキュアシステム実習は必修
- CISSP or GIAC 資格の修得
- プロジェクトマネジメント履修

情報セキュリティ管理者（CISO）資格授与

Katsuya Uchida　uchidak@gol.com