セキュリティーマネジメントのための組織

只木(佐賀大)*　吉田(富士通)
*リーダー

SS研セキュリティーマネジメントWG
組織グループ

情報セキュリティ対策の必要性

- 情報システムと情報資産は大学業務の基盤
  - 情報システムの無い教育、研究、医療、大学運営は考えられない。
- 情報システムへの不正侵入や情報漏えいは大きなダメージ
  - 「ウィルス感染」のように問題を矮小化してはいけない
- 組織的対応が必要
  - 組織としての信用

組織整備の必要性

- 日常的なセキュリティマネジメント
  - セキュリティポリシーの策定
  - セキュアな情報システムの構築
  - ルールの遵守状況の監査
- インシデント時の対応
  - 現場が迅速に動けるように
  - 責任体制の明確化
  - 渉外の一本化

セキュリティポリシー (平常時)

- 日常的セキュリティ維持・向上体制
  - CISO(最高情報セキュリティ責任者)の設置、セキュリティ委員会、セキュリティ責任者、連絡網
- 情報の格付け
  - 機密性、完全性、可用性
- セキュアな情報システムの構築指針
  - 認証、証跡、権限管理、アクセス制限、セキュリティホール対策、ログ管理

セキュリティポリシー (平常時)(2)

- 利用者教育と利用者の義務
- ルールの遵守状況の監査

セキュリティポリシー (非常時)

- 通報義務
  - 職員の通報義務
- 連絡網
- 緊急待避対策
  - 情報関連部署の権限明確化
  - 技術者に責任を負わせない
- 対応体制
  - 常駐が必要
- 改善に向けた対策

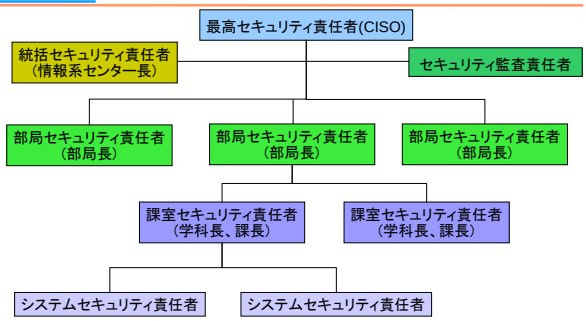
セキュリティポリシーを作る

- 無理のないポリシー
- 実情にあわせた手順
- 改善点を発見し、改善する
- セキュリティーに完全は無い
  - PDCAサイクルを回すことで徐々に改善
- ポリシー策定支援ソリューションの活用
  - 雛形があればあまり高価にならない

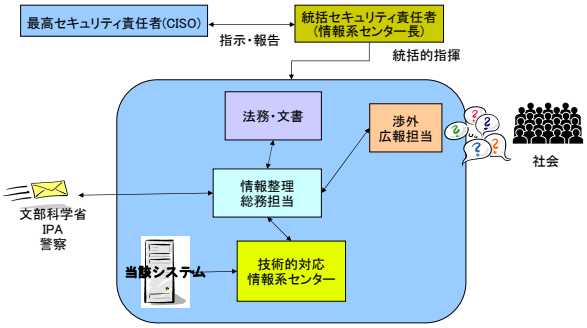
セキュリティポリシーを作るために

情報セキュリティガバナンス	http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html
政府機関の情報セキュリティ対策のための統一基準	http://www.nisc.go.jp/active/general/kijun01.html
高等教育機関の情報セキュリティ対策のためのサンプル規程集	http://www.nii.ac.jp/syskan/sp/
法律・ガイドライン	http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
脆弱性関連情報取扱体制	http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
ISMS [情報セキュリティマネジメントシステム]	http://www.isms.jipdec.jp/
プライバシーマーク(R)制度	http://privacymark.jp/
組織ポリシー策定/監査ソリューション	http://segroup.fujitsu.com/secure/solution/sol1.html http://segroup.fujitsu.com/secure/service/audit.html
セキュリティ認証取得ソリューション	http://segroup.fujitsu.com/secure/service/consulting/infosecure3.html

セキュリティーマネジメント組織 (平常時)



セキュリティーマネジメント組織 (非常時)



インシデント発生時

- 迅速な対応
  - 技術的対応：システム切断
    - 電源断は要注意：証拠を残す
  - 被害拡大を防ぐ
  - 必要に応じて通報：隠さない
    - 文部科学省、IPA、警察
  - 必要に応じて記者会見

インシデント発生時(2)

- 組織内部署の役割分担
  - 平常時から組織整備
  - 技術的対応、渉外、法務、総務を分離
- 対応マニュアル
  - コンティジェンシプラン
  - データ提供手順

インシデント対応マニュアル

- 情報漏えい発生時の対応ポイント集
  - http://www.ipa.go.jp/security/awareness/johorouei/
- 組織内CSIRT構築支援マテリアル
  - 組織内のインシデント対応組織
  - http://www.jpcert.or.jp/csirt_material/

セキュリティ関連団体

- セキュリティ関連情報の取得
- インシデント発生時の対応
- セキュリティ向上・維持の方針

IPA［情報処理推進機構］	http://www.ipa.go.jp/security/
JPCERT/CC [JPCERTコーディネーションセンター]	http://www.jpcert.or.jp/
JIPDEC [財団法人 日本情報処理開発教会]	http://www.jipdec.jp/

教育

- 情報セキュリティーは技術だけでは守れない
- 利用者教育
  - 日々の情報を扱う作業
  - 情報システムの利用
- 管理者教育
  - 情報システムの管理・管理運用
- 発注者教育
  - 情報システム構築時の注意

教育(2)

情報セキュリティ読本 改訂版	http://www.ipa.go.jp/security/publications/dokuhon/2006/
情報セキュリティ教本	http://www.ipa.go.jp/security/publications/kyohon/
セキュアなWebサーバーの構築と運用	http://www.ipa.go.jp/security/awareness/administrator/secure-web/
情報システムの信頼性向上に関するガイドライン	http://www.meti.go.jp/press/20060615002/guideline.pdf
最新IT解説：セキュリティ	http://sme.fujitsu.com/tips/itnew/

CIO/CISOの役割

- CIO(最高情報統括責任者)
- CISO(最高情報セキュリティ責任者)
- 誰が行うべきか
  - CIOとCISOを必ずしも分けなくても良い
- どういう役割かを整理する

用語	http://e-words.jp/w/CISO.html
SS研講演：岐阜大 篠田先生	http://www.ssken.gr.jp/MAINSITE/download/newsletter/2006/edu/stg_edu-1/doc6.html
SS研講演：京大 上原先生	http://www.ssken.gr.jp/MAINSITE/download/newsletter/2004/stg/2/1_uehara.html

大学法人役員の役割

- セキュリティの重要性を認識する。
  - セキュリティインシデントによるダメージを知る。
- セキュリティ改善の先頭に立つ。
  - セキュリティ改善は継続的活動
  - 組織トップの姿勢は極めて重要

ユビキタスとセキュリティ

- データ持ち出し、モバイルPCへの対応
  - 便利さとセキュリティーの調整が必要
- 重要データは持ち出させない
- 持ち出し時の手順を定める
- 特に教員の場合
  - 校務と研究・教育を区分する
  - 校務は職場で行う

セキュリティが過剰な負担にならないために

- 情報・情報システムの棚卸し
  - システムの数を減らす
  - 学内のサーバをセンターに集約する
  - 仮想化
- アウトソーシング
  - SaaS、ASP
- 業務端末のあり方の検討
  - シンクライアント
- 免責の明示

セキュリティが過剰な負担にならないために(2)

- 守備範囲を定める
  - 全て、100%は不可能
- 情報・情報システムに関わるリスクを洗い出す
  - リスクの分類
    - 必ず解消、解消を努力、リスクの存在を認識
- 守るべき情報・情報システムの範囲を定める
  - セキュリティレベルの異なる情報システムを同じネットワークに混在させない