人間・管理・インシデントハンドリング

長谷川（中京大）* 湯浅（KEK）
吉田（大分大）　*リーダー

SS研セキュリティマネジメントWG
人間・管理グループ

目次

- セキュリティにおける人間の要因
  - 懲りない人々（繰り返し感染、繰り返し侵入被害）
  - セキュリティ教育の在り方と評価
- 人間要因の管理
  - セキュリティポリシーとPDCA
  - ポリシー雛型の導入体制
- インシデントハンドリング
  - CSIRTからSOCへ(Security Operations Center)

セキュリティにおける人間的要因

- 機械やソフトの役割は限定的
  - ソフトウェアや装置の導入による安心感
  - うっかり/好奇心/出来心による受動攻撃
  - スピア攻撃（上司からのメールに見せた添付書類）
- 繰り返される感染・侵入被害
  - 同じ人、グループが複数回
- 学生や留学生の意識
  - 意識/常識/認識の差
  - 知財権侵害（不正コピー利用/配布）への認識

セキュリティ教育

- 教育とその効果
  - 機会の提供
    - 講習会
    - E-Learning＋チェックテスト（テスト内容と評価の活用）
  - 受講の義務化
    - 例外なし
    - 役員、上級者（短期の効果的教育、予算確保に重要）
  - 教育効果の検証
    - インシデントが減少しないと意味がない

セキュリティ教育の問題点

- IT用語の問題
  - わかりにくい用語や概念
  - 上級職員の理解
  - 急激な環境変化
- 人の類型化
  - セキュリティ意識の調査（適切なアンケート等）
  - 分類・教育
- セキュリティポリシーの周知
  - E-learningとチェックテスト？

セキュリティ教育教材（有償）

- 情報倫理デジタルビデオ小品集　（制作：メディア教育開発センター）
  http://www.mitomo.co.jp/online/shop01/moral.html
  http://www.mitomo.co.jp/online/shop01/moral2.html
  http://www.mitomo.co.jp/online/shop01/moral3.html
  大学生協モデルでは一部映像をインストールして販売
  2009年度以降の活動予定不明（NIME組織改変）
- INFOSS情報倫理（日本データパシフィック）
  http://www.datapacific.co.jp/e_learning/e-ichiran.htm

セキュリティ教材（無償）

- 15分でわかるウィルスの脅威 （IPA）
  http://www.ipa.go.jp/security/y2k/virus/cdrom2/index.html
- 警察庁サイバー犯罪対策：情報セキュリティ対策ビデオ
  http://www.npa.go.jp/cyber/video/index.html
- 情報モラル啓発ビデオ （ハイパーネットワーク社会研究所）
  http://www.hyper.or.jp/staticpages/index.php/moral#moral_video
- インターネット社会を安全に暮らすために（人工知能研究振興財団）
  https://www.tokai-ic.or.jp/selfdefense/

セキュリティ教材（無償続き）

- 日本セキュリティ協会(JNSA)の無償セキュリティ教育
  http://www.jnsa.org/
- セキュリティ知識のチェック
  - セキュリティカランキング
    - 個人編と組織編があり、理解度チェックには有効

  http://www.jnsa.org/Seculiteracy/index.html

セキュリティ教材の鮮度

- 変更頻度少
  - セキュリティ基本教育用教材
- 変更頻度中
  - セキュリティポリシーとその周辺
- 変更頻度大
  - セキュリティ状況
  - IT基礎知識と応用知識

セキュリティチェックテスト

- セキュリティテキストとテスト
  - 実施基準書（部門別に作成）
  - だれが何を教え何をチェックするか
  - だれが何の権限で実施するか
  - 結果をどう日常のセキュリティに反映するか

階層別の対応

- 上級職員
- 教員
  - 事務と教育研究の境界
  - ベテラン教員のセキュリティ意識と現状把握
- 職員
  - 統一基準ベースでよい
  - ただし、機密扱いについて明確な基準必要
- 学生
  - 処分基準（ポリシーで切り分け）

階層別の対応

- 不安定短期雇用の増大
  - 産学連携、短期プロジェクト、派遣、外注
  - 組織への帰属意識の低下
  - 組織への忠誠度、信頼度の維持困難
  - セキュリティ意識の低下
- シングルサインオン等の導入
  - revokeリスト管理
  - DB管理の手間の増大

教育レベル設定

- 教育対象のレベル設定
  - 初級教育
    - 学生・教員
    - 中途半端な上級者が不満
  - 来て欲しい人がこない
    - 事務は人事記録のしばりによる効果
    - 役員、経営層
  - 教育は組織としてのアリバイ？
  - 小中学校向け教材は初級教育に有用

ポリシー遵守を助けるIT環境
ミスの発生を防ぐ環境

- ローカルに情報を残さないシステム
  - SaaS＋Web
  - Thin Client
- お仕着せ端末（余計な自由度なし）
- ICカード認証と物理的セキュリティ
- 身をまもるためのログ保全
- Cloud、SaaS,アウトソース
  - コスト削減とセキュリティリスクの移転

Cloud,SaaS,アウトソースの問題

- メール等のアウトソーシング
  - 認証データの外部提供は大丈夫？
  - データの外部保管
- データの取り扱い
  - 統計処理されてはいても大丈夫？
  - メールの紛失等
- サービスの継続性
  - サービスが消えたら（M&A等）
  - 無償から有償へ

セキュリティの管理

- セキュリティポリシーとPDCAサイクル
  - セキュリティポリシーは誰のためのものか
  - あるだけでは意味がない
  - 役に立つポリシーや手順
  - セキュリティポリシー遵守を助ける環境
    - セキュリティ機器、ソフトウェア
    - 教育、指導、援助
  - セキュリティ監査

セキュリティ監査

- 第3者監査
  - 機密保持契約（監査仕様書例は付録）
  - 監査人の資格（CISSP,JASA主任監査人）
- 内部相互監査
  - 近隣大学間や地域での情報共有
一方で地域ネット組織のあいつぐ解散
  - 近隣大学や地域でのセキュリティ相互監査
    - セキュリティ意識の向上

セキュリティ監査手順

- 監査立案
  - 実施体制
    - アウトソース/内部監査
    - 日程等
  - 実施手順書
    - 監査対象項目、監査対象者等選択
- 監査実施
- 監査レビュー

各種セキュリティ基準等

- 各種認証や証明
  - ISMS/ISO27000
    - セキュリティシステム基準への適合証明
  - プライバシーマーク
    - 名刺一枚の管理も大変（大学にとってのメリット？）
    - とりあえず学籍情報は重要だけれど
  - 事業継続/ISO25999（BCP/BCM）
  - セキュリティ格付け会社（格付けトライアル）
    - アイ・エス・レーティング（www.israting.com）
  - SOX法、JSOX法
    - 会計基準
    - 法人化した大学への適合必要？

セキュリティ体制

- CSIRT機能構築
  - セキュリティ計画
    - ポリシー策定、セキュリティシステム導入計画、インシデントハンドリング計画
  - 分析とレポート/記録
    - ぜい弱性スキャナ、ペネトレーションテスト、ログ監視
  - インシデント対応
    - インシデント拡大防止、エスカレーション、レビュー
  - トレーニング、教育
    - サイバードリル

インシデントの定義

- インシデントとは何かを明確にする
  - 部局単位？
  - ウィルスやtrojan
  - 侵入
- 外へのコンテンツ侵害はCSIRTの範囲？
  - 掲示板荒らし、内容の話への対応
    - たぶん範囲外、しかし連絡は来る！
  - ただし連絡窓口は一本化（Point of Contacts）
    - 窓口は統一しても全部はやらない

インシデントハンドリング

- 一定割合でのインシデント発生
  - ボランタリーな対応では無駄が多い
  - 担当者の無限責任にしない
  - インシデントの切り分けとエスカレーション
    - 情報トリアージ
    - インシデントの局在化
    - 事後報告

インシデントハンドリング手順

- 手順の類型化
  - インシデントハンドリングポリシー
  - 守備範囲（無限責任にならない）
- CSIRTマップ（付録PDF）
  - 早期での全組織対応か局所対応かを見極める

まとめ

- セキュリティマネージメント体制の整備
  - ポリシーとポリシーの周知徹底（教育）
  - 監査（内部、外部）と日々のセキュリティ改善
    - セキュリティ戦略→BCP/BMP
    - セキュリティ啓発活動
  - でも、完全なセキュリティはありえない
    - インシデント対応体制
    - インシデントにも学ぶ