セキュリティマネージメントWG 活動報告

アカデミック機関での セキュリティマネージメントBCP

セキュリティマネージメントWG
湯浅富久子

背景

技術への追随が困難
守備範囲の拡大

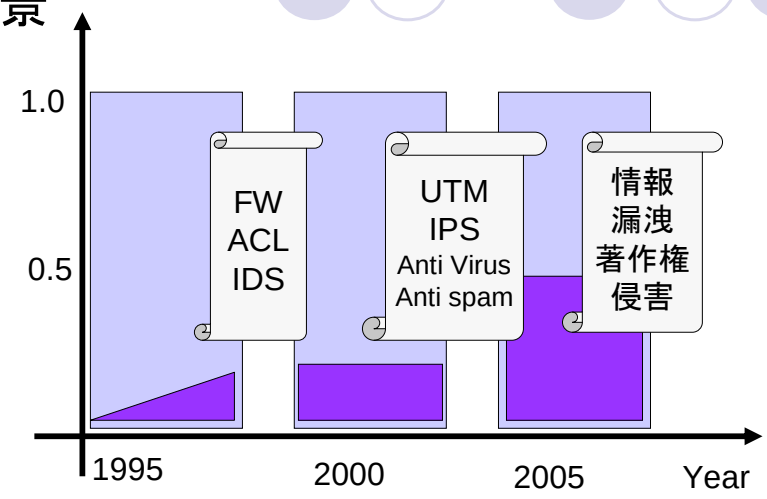
- 技術的なセキュリティ対策が一巡した
- 情報セキュリティポリシーを策定した

ずれ？

インシデントの性質が変化
- 金銭目的
- めだたなくなった
- 小規模化
- ノイズ化
- 影響は大

インシデントへの目が変化
- 必ず発生するものだが、、
- 不作為は許されない
- 社会的な責任
- 大学のブランドへの影響

背景



情報システム構築におけるセキュリティ対策の重要性
（イメージ図）

目標

セキュリティマネージメントに有益なノウハウを集める

- アカデミック機関が現時点でできる最善の実践策
  - 担当者が無限責任を負わないように
- 利便性とセキュリティの質のバランスをとる
  - 守ってもらえない規則は無意味
- 部局の自治を尊重しつつ統一的なセキュリティ対策
  - 一番弱いところが組織の脆弱度をきめる
- PDCAの設計ができること
  - 時代に追随できるように柔軟に

活動の特徴

- テーマの選択
  - 組織＝人間＋管理
  - 攻めのテーマと守りのテーマ
    - 先進性と実用性
  - 第一期に3つのテーマ、第二期に3つのテーマ
- チーム制
  - 6つのテーマごとにチームを作成、リーダを設定
- 会合、ML、SS研コミュニケーションサイト POESY

第一期のテーマ

- 2007年2月から2007年11月
  - セキュリティマネージメントのための組織
  - spam対策
  - デジタルフォレンジック
- 第一期成果レポートの作成
  - http://www.ssken.gr.jp/MAINSITE/activity/workinggroup/securitymng/index.html

第一期の活動から

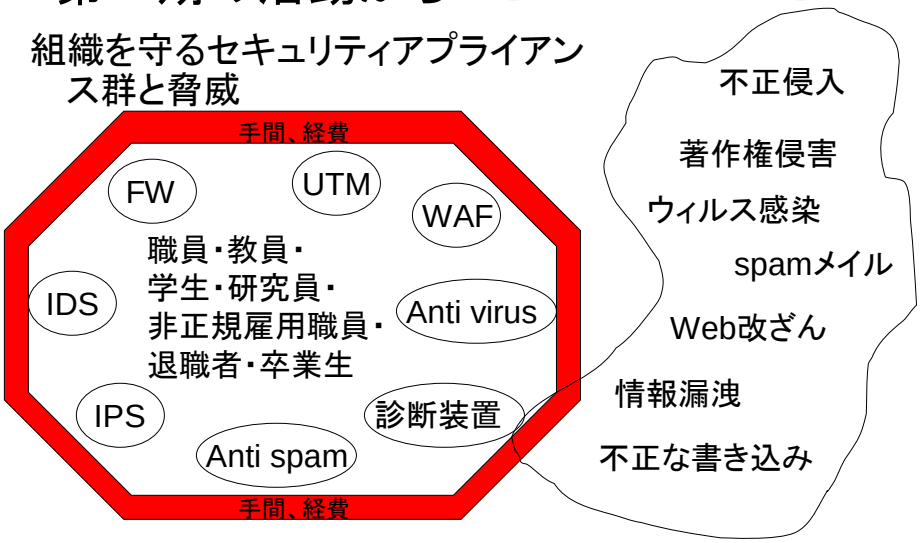
- デジタルフォレンジック
  - 過去におこったインシデントを科学的に立証するための証拠を保全・収集・分析すること
  - サーバ等の情報機器のログやシステムの状態が記録された媒体について調査解析を行う技術と手法
  - アカデミック機関での対応
    - 通信内容を一定期間（判例では3年など）保存する
    - 保全（暗号化、分散バックアップなど）とデータベース化
    - アウトソーシング
      - 機関内のサーバ類を減らす
      - ログ解析のアウトソーシング
  - 上原哲太郎、IPSJ Magazine Vol.48, No.9 pp.889.

第二期のテーマ

- 2008年3月から現在まで
  - 人間・管理・インシデントハンドリング
  - 状況確認のためのセキュリティアプライアンス
  - エンドポイントのためのセキュリティ対策
- WG成果報告書の作成
  - 冊子
  - http://www.ssken.gr.jp/MAINSITE/download/wg_report/securitymng/index.html

第二期の活動から

組織を守るセキュリティアプライアンス群と脅威



10機関へのアンケート

- 二つの大問
- FW、IPS/IDS、WAFなどの導入とそのポリシーについて
  - 機器の傾向、導入の動機、運用点・管理の実情
  - 9つの質問
- 「P2P」関連ソフトウェアに関する対策とそのポリシーについて
  - 10つの質問

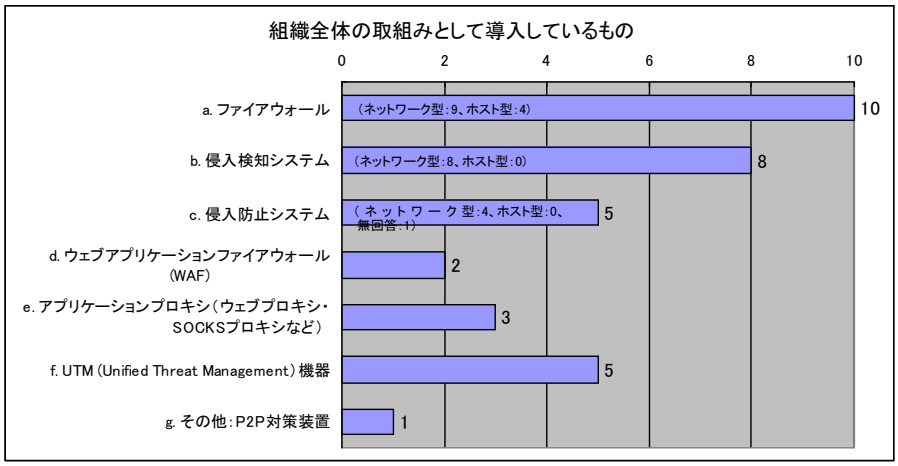
「FW、IDS・IPS、WAFなど」の導入とそのポリシーについての設問

Ⅰ	設問
1.	組織全体の取り組みとして導入しているものは何ですか
2.	UTMを導入している組織は、その機器の有する機能と利用している機能は何ですか
3.	1.や2.で回答した機器を導入することになった経緯を、差し支えない範囲で教えてください。
4.	導入して良かったことは何ですか（セキュリティ的な観点と、運用の観点から）
5.	導入して大変だったことは何ですか（セキュティ的な観点と、運用の観点から）
6.	ファイアウォール、IDS/IPSなどのさまざまなログをどのように扱っていますか（長期保存や閲覧規制など）
7.	トラフィックの監視や流量制限を実施する際の根拠はどのようなものですか
8.	ログやIDSで収集された通信内容には、通信の秘密やプライバシー等のセンシティブな情報が含まれている可能性がありますが、これら情報の扱いはどのような権限で行われていますか
9.	1.であげた機器のうち、以前導入していたが運用をやめた機器があれば、その種類と理由を教えてください

「P2P」関連ソフトウェアに関する対策とそのポリシーについての設問

Ⅱ	設問
1.	P2P方式を利用したソフトウェアの制限等を実施していますか
2.	どのような種類のソフトウェアを制限していますか
3.	制限する手段はどのようなものですか
4.	制限している理由を、差し支えない範囲で教えてください
5.	制限の根拠はどのようなものですか
6.	P2P関連ソフトウェアへの制限等を実施していない理由は何ですか
7.	P2Pによるファイル交換で、外部組織から通知を受けたことがありますか
8.	どこからの通知だったか、差し支えなければ教えてください
9.	通知に、どのように対処しましたか
10.	その他P2Pに関するコメント等ありましたら、ぜひご記入ください

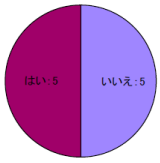
アンケート結果

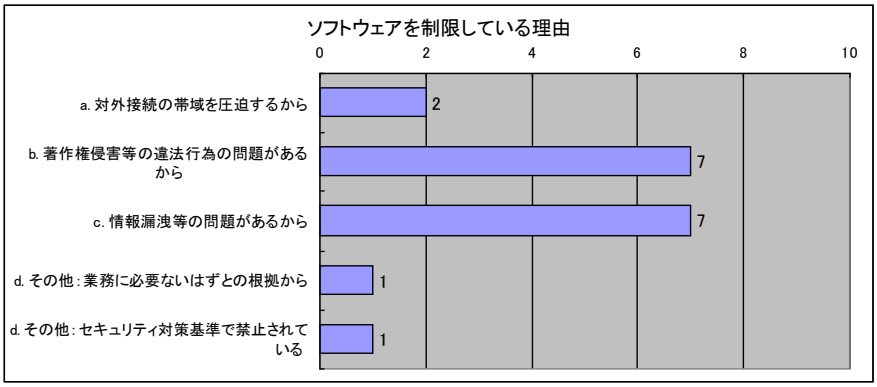


アンケート結果スナップショット

P2Pによるファイル交換で、外部組織から通知を受けましたか？

50%YES





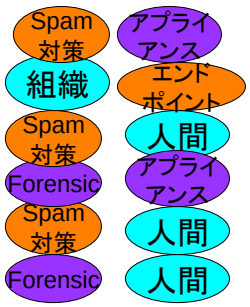
まとめ

- セキュリティマネージメントの鉄則
  - 無限責任を負わないよう体制作りに時間をかける
  - セキュリティレベルごとに対策を定義しておく
  - 組織を超えてセキュリティマネージャ間で情報共有しよう
  - 情報セキュリティ教育に力をいれる
  - 隙間の時間で最新技術を会得
  - アプライアンスなどの道具は磨きが必要
  - 現時点での最善策を選択できるように！

メンバーと担当テーマ

- 担当幹事
  - 長谷川明生
- 推進委員
  - 笠原義晃
  - 只木進一
  - 長谷川明生
  - 武蔵泰雄
  - 吉田和幸
  - 湯浅富久子

（五十音順）



  - 須永知之
  - 三谷修
  - 山田久仁
  - 吉田真和