IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報セキュリティエコノミクスの挑戦

Computer Security Symposium 2008(CSS2008)　発表資料

内容

- 位置づけ
- セキュリティ対策の考え方の現状
- セキュリティ事件・事故の実際
- **情報セキュリティエコノミクス**（Information Security Economics）の提案
- **情報セキュリティエコノミクス**の導入により得られる新たな視点
- まとめ

位置づけ

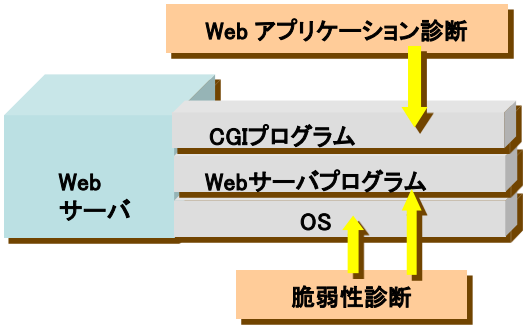
- セキュリティ事件・事故が減らない現状を打開し情報セキュリティ対策の新たな取り組みの方向性を見出すことを目的として「情報セキュリティエコノミクス」の適用を試みたポジションペーパー

セキュリティ対策の考え方の現状

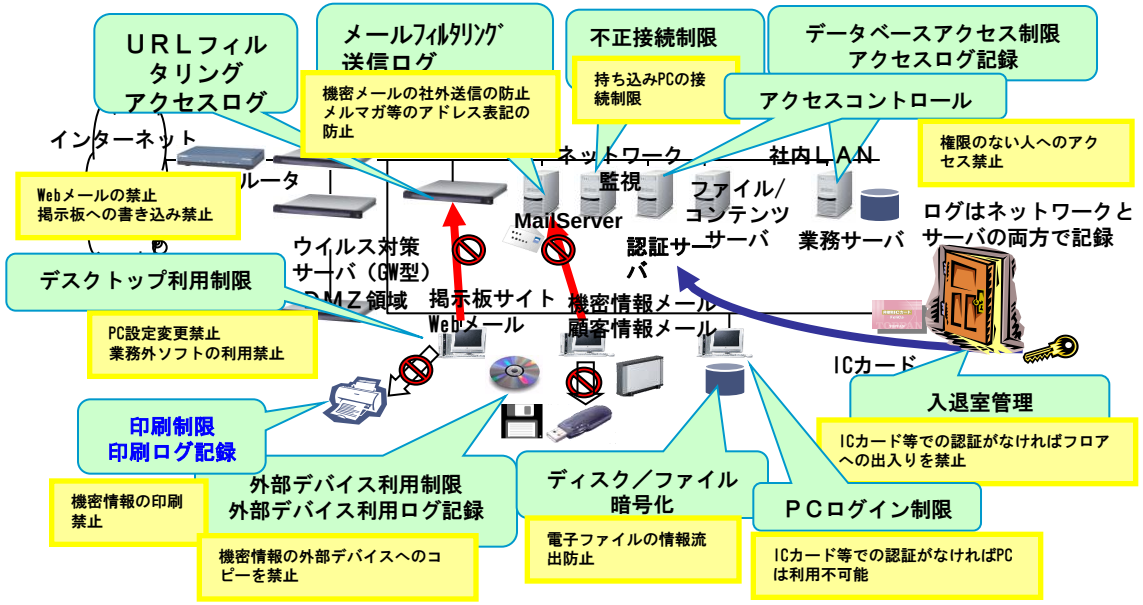
- 「ＩＴ技術」と「セキュリティマネジメント」の二つの視点
- 車輪の両輪になぞらえられている

セキュリティ対策の考え方の現状

- ＩＴ技術
  - ソフトウェア、通信プロトコルのセキュリティ
  - システム的なセキュリティ
  - 脆弱性対策、攻撃防御



Webサーバ脆弱性チェックの例

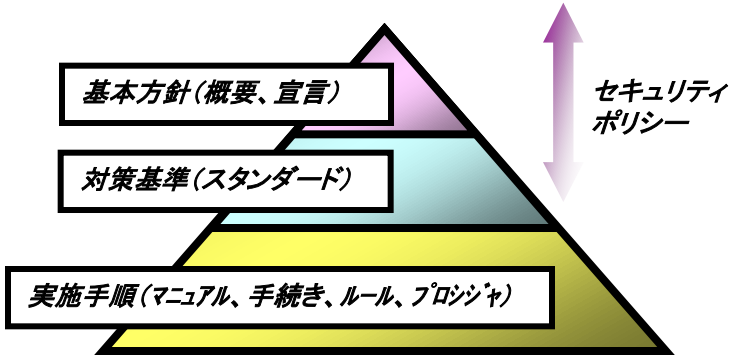


システム的なセキュリティ対策の例

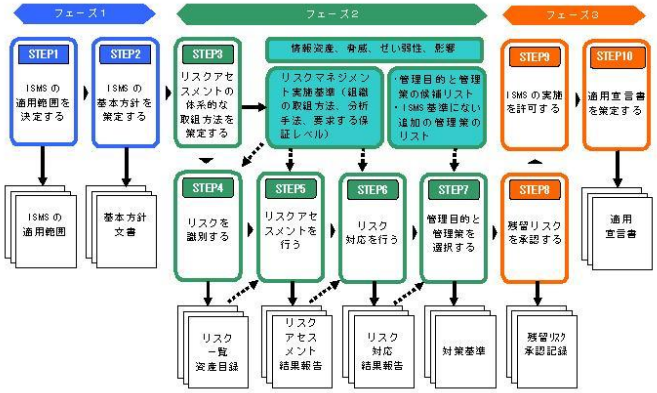
セキュリティ対策の考え方の現状

- セキュリティマネジメント
  - セキュリティポリシーの作成
  - セキュアな運用体制の構築と実施
  - セキュリティ監査
  - PDCAサイクルの確立と維持
  - ISMS（Information Security Management System）の構築

PDCAサイクル
（Demingサイクル）



ポリシー文書の構造例



「ISMS適合性評価制度」における
ISMSの構築例

セキュリティ事件・事故の実際

- セキュリティ事件・事故は発生し続けており、大きな社会問題となっている。
- 情報セキュリティ対策が重荷になってきており、「セキュリティへの過大投資」「セキュリティ対策疲れ」が発生しているとの意見もある。
  - セキュリティ対策に必要な金銭的・人的・時間的負担
  - セキュリティ対策による業務効率の低下
  - 従業員のモチベーションの低下、反発

- 2005年、経団連、環境問題と同様に市場メカニズムの中での企業の情報セキュリティに対する取り組みを評価する仕組みの必要性を提言。
- 産業構造審議会の情報経済分科会、ITと環境問題との関連性について議論。

情報セキュリティエコノミクスの提案

- 経済学的な視点を加えた情報セキュリティエコノミクス（Information Security Economics）
  - 経済学、社会心理学等を含む、幅広い行動科学の知見を導入
    - 経済学的知見
    - 心理学的知見
    - 社会学的知見
      - 判断の合理性と非合理性
      - 判断の正確性と不正確性
      - デシジョンのプロセス…

情報セキュリティエコノミクスの提案

- 海外では既に取り組みが進行中
  - WEIS（Workshop on the Economics of Information Security）
  - 情報セキュリティ経済とEU政策についての提言（ENISA）（European Network and Information Security Agency）
  - SHB2008（Interdisciplinary Workshop on Security and Human Behavior）
  - 国内では，情報セキュリティ投資の動機付けなどの研究（田中，松浦，2003）

情報セキュリティエコノミクスの導入により得られる新たな視点

事例[1] ボット感染者対策

事例[2] ウイルス対策ソフトの性能差

事例[3] セキュリ担当者の考える問題点

事例[4] ISMS適合性評価制度、Pマークの状況

事例[5] P2Pファイル交換ソフト利用者数の状況

事例[1] ボット感染者対策

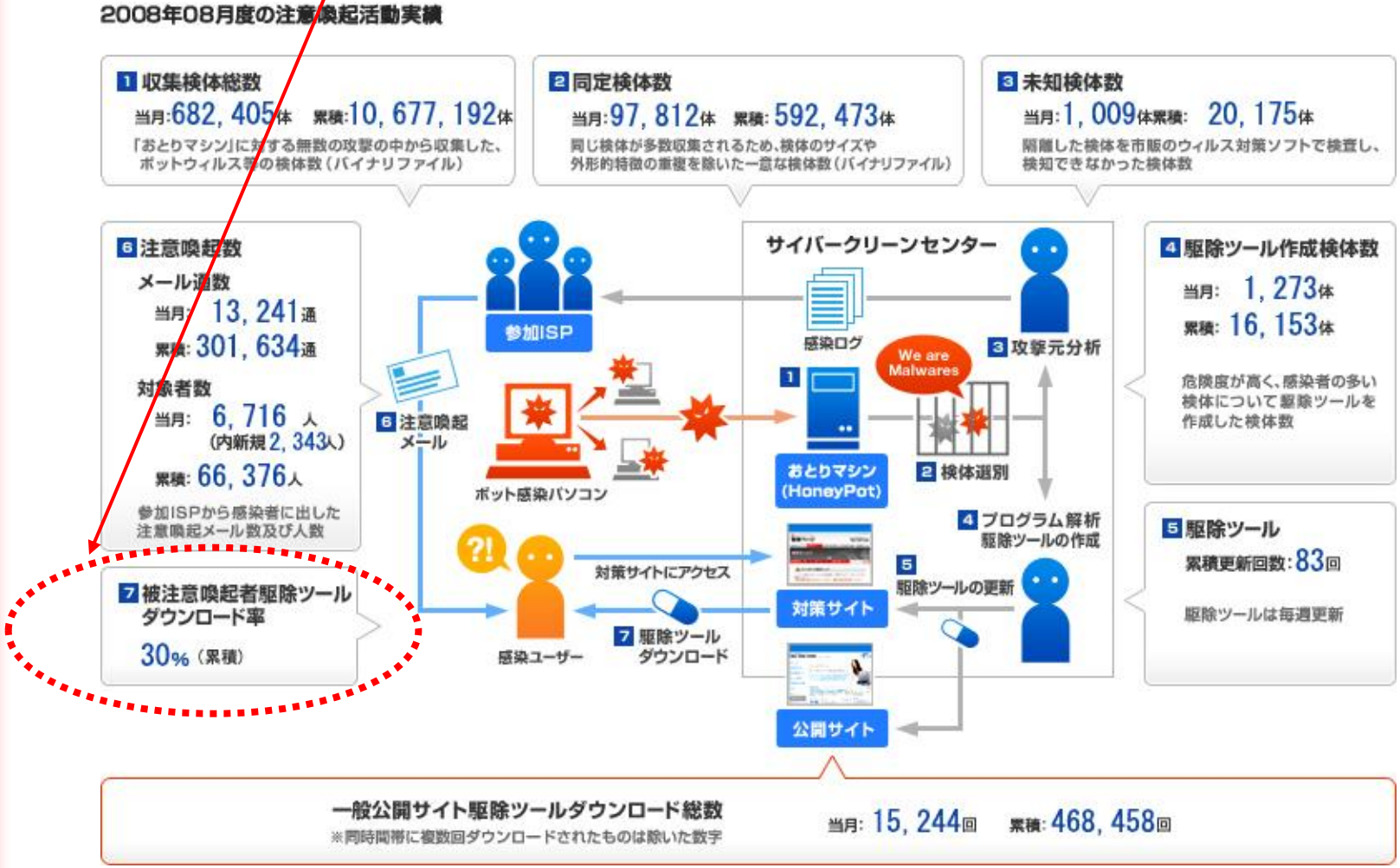
- ボット感染の状況
  - 現在、国内で40～50万人が感染と予測
- 総務省・経済産業省連携事業のボット対策プロジェクトとしてサイバークリーンセンター（CCC）を開設（平成18年12月）
- プロジェクト参加ISP、駆除ツール開発事業者、感染予防策ベンダ、セキュリティ専門組織と連携
  - おとりマシンを用意して感染者の発見やボットの収集を実施
  - ボットプログラムの解析、駆除ツールの提供、感染者への通知を実施

CCC公表資料より引用

事例[1] ボット感染者対策

- 対策率30%程度

CCC公表資料より引用



事例[1] ボット感染者対策

- ボット駆除ツールダウンロード率30%（＝70%未対策）
  - ボットは他のPCに悪影響を及ぼし、ネットワーク全体の安全性を低下させる　（＝自分が駆除すると全体の利益となる）
  - しかし、目に見える形では感染PCへは悪影響を及ぼさない（＝自分にとっては、駆除しても得にならない）
- 経済学でいう「外部不経済」が生じている
  - 外部不経済：経済主体の行動が市場を通さずに他の経済主体に負の影響を与えること
- 解決には「内部化」が必要
  - 外部不経済の原因分析
  - 内部化の方策の例：感染者に対するペナルティやネットワーク全体の対策費用の負担　等

事例[2] ウイルス対策ソフトの性能差

- 製品により、検知能力、新たなウイルスへの更新タイミング、処理速度などに差がある
  - ５種類のソフトで検査した結果、検出率は　97.8%～60%
    （ネットエージェント（株）　プレスリリース　2007.8.1）
  - ウイルスの種別に地域性が存在

- 利用者の製品選択の基準の調査
  （(株)アイシェア　コンピュータウイルスに対する意識調査 2008.8.8）
  - 性能以外の項目が主
  - ウイルス対策ソフトの「性能品質」は評価されていない？

１位	52.7%	価格
２位	49.0%	コンピュータへの負荷
３位	45.7%	更新料
４位	44.6%	スパム対応，ファイアウォール等の機能
５位	27.1%	検出率

（複数回答可）

事例[2] ウイルス対策ソフトの性能差

- 「レモン市場」が発生している
  - レモン市場（Akerlof, G. 1970）
    - ◆サービスや財などの商品の品質に関して買い手の情報が乏しいために適正な価格がわからず、市場に品質の低い商品が選択的に出回る現象のこと
    - ◆中古車市場において品質の悪い製品が出回る現象を説明
- 「情報の非対称性」（Asymmetric Information）によって起こる

情報の非対称性を
解消することにより解決する

事例[3] 情報セキュリティリスクの評価と対策

- セキュリティ対策実施上の問題点

１位	39.3%	どこまで行えばよいかわからない
２位	37.0%	費用対効果が見えない
３位	36.7%	対策を構築するノウハウが不足している
４位	36.2%	コストがかかりすぎる
５位	26.9%	教育訓練がいきとどかない

（警察庁「不正アクセス行為対策等の実態調査　調査報告書」平成20年2月　より）

  - 技術的な問題は３位のみ
  - それ以外はリスクの考え方やセキュリティ対策の投資と効果に関する内容

- セキュリティ対策の投資と効果についての構造解明が求められる
- Gordon and Loab(2002)による情報セキュリティの最適投資を分析する経済学的なモデル化などの先行研究あり

事例[4] ISMS適合性評価制度、Pマークの状況

- セキュリティ関係の制度としてはそれなりに機能している
- しかし、一部には課題も指摘
  - 品質保証の責任の所在が明確であり、そのメカニズムが正しく働いているか？
  - セキュリティレベルの向上につながっているか？
  - 取得が、セキュリティレベルに関する評価の指標に成り得ているか？
  - 認証を取得した組織でセキュリティ事件・事故が発生した場合に、それがセキュリティ向上に正しくフィードバックされる仕組みになっているか？

- 制度が機能する中で、インセンティブメカニズムがどのように働いているかを明確にする必要がある。

事例[5] P2Pファイル交換ソフト利用者数の状況

- 2004年春頃から情報流出が頻発し社会問題となったにもかかわらず、P2Pファイル交換ソフト※の利用者は減少していない

2002	2003	2004	2005	2006
3.0%	3.4%	2.6%	2.7%	3.5%

コンピュータソフトウェア著作権協会
「2006年ファイル交換ソフト利用実態調査の概要」2006年7月25日　より

(※ WinMX、Winny、Limewire、Share(仮称)、Cabos　等）

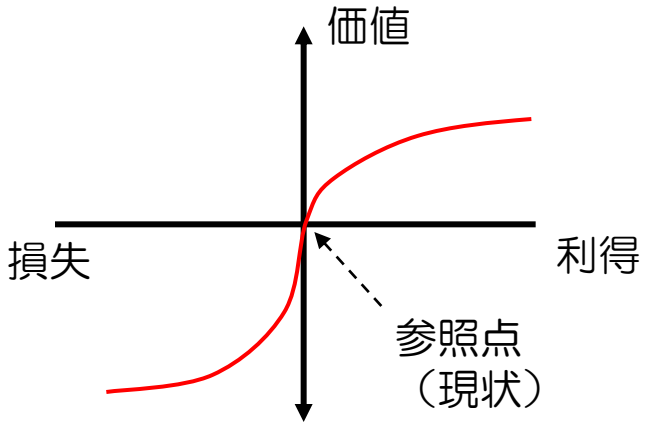
- 危険性が指摘されているにもかかわらず利用し続ける理由は？

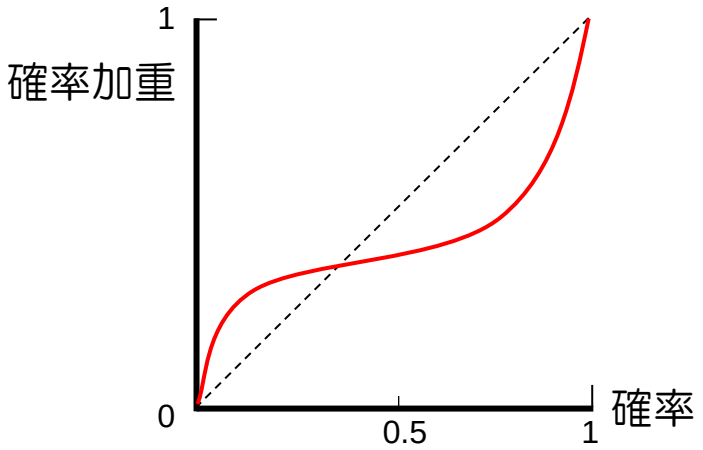
事例[5] P2Pファイル交換ソフト利用者数の状況

- 利用者のWinny利用に対するリスク認知の問題があるのではないか
- リスク：
  ある事象生起の確からしさと、それによる負の結果の組合せ
  （ JIS Z8115: 2000 ）
- 利用者は危険性（被害の大きさ）をどのように認識しているのか？
- 利用者は事件・事故が発生する確率をどのように認識しているのか？
- 利用者は利用と非利用の判断をどのように行っているのか？

事例[5] P2Pファイル交換ソフト利用者数の状況

- リスク認知の知見の例
  - プロスペクト理論（Tversky，Kahneman）
    - 価値関数
      - 人が感じる損と得
        - 感応度逓減性
        - 参照点依存性
        - 損失回避性
    - 確率加重関数
      - 人が感じる発生確率
    - これらの知見を適用することにより、新たな分析結果が得られる可能性がある





結論

セキュリティのアプローチ

- IT技術、マネジメントに加え、「セキュリティエコノミクス」の導入が必要と考える。

セキュリティエコノミクスを支える分野

- 経済学
- 行動科学
- 社会心理学
- 安全工学
- 経営学
- ：

セキュリティエコノミクスのさまざまな知見

- 脆弱性の定量化
- 最適投資の経済学的なモデル化
- インセンティブメカニズムの解明
- 制度設計
- ゲーム理論
- マルチエージェントシミュレーション
- リスク認知
- リスク選好
- プロスペクト理論
- 感情ヒューリスティックモデル
- リスク感情仮説
- ：