NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

情報セキュリティ会計に関するガイドラインの策定に向けて

～2004年度活動報告～

2005 年 6 月 13日

セキュリティ会計ガイドライン検討WG
佐野　智己
(凸版印刷株式会社)

WGのご紹介

- 企業における情報セキュリティ確保への取り組みを適切に把握し、評価し、そして伝達する仕組みとして、「環境会計」に倣って、「セキュリティ会計」を提唱
- 「セキュリティ会計」とは、「環境会計」からとった造語
- セキュリティ会計の基本的な考え方を取りまとめ、ガイドラインとして発信することを命題にWGを設立
- 2004年度より、チャレンジ開始
- メンバー：14名 (2005年5月末日現在)

Copyright (c) 2005　NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

取り組み項目

JNSA

〈命題〉 セキュリティ会計のガイドラインの策定

その過程で、越えなければならないハードル（取り組み項目）がいくつかある。

1） セキュリティ会計モデルの基本設計
2） 環境会計などの既存モデルの調査と共通点・相違点の認識、適用の可否
3） コストの定義と算定方法
4） 効果の定義と測定方法
5） 情報セキュリティにおける資産の価値評価
6） モニタリング　など

Copyright (c) 2005　NPO日本ネットワークセキュリティ協会 Page 3

本日、お話したいこと

JNSA

1．セキュリティ会計の基本設計
- ⇢ セキュリティ会計とは
- ⇢ 「コスト」と「効果」、その間に「キューブ」

2．コスト
- ⇢ コストの算定

3．効果
- ⇢ 効果の考え方

4．今後の進め方
- ⇢ 次なるチャレンジは？

Copyright (c) 2005　NPO日本ネットワークセキュリティ協会 Page 4

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

1 セキュリティ会計の基本設計

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

セキュリティ会計とは

企業が自身の企業価値を維持し、さらに向上させていくことを目指して、情報セキュリティに関する取り組み（※）を効率的かつ効果的に推進していくことを目的として、事業活動における情報セキュリティのためのコストとその活動によって得られた効果を把握し、可能な限り定量的に評価し、伝達する仕組み

（※）「情報セキュリティに関する取り組み」とは、企業等が自身の情報資産を各種の脅威から保護し、その機密性、完全性、可用性を確保し、維持するための取り組みであり、加えて企業等が自身の事業活動を通じて、情報通信ネットワーク社会の秩序の維持と発展に資する取り組みを含むものである。

当WGが取り扱うセキュリティ会計は、企業を対象とする『情報セキュリティ会計』とする。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

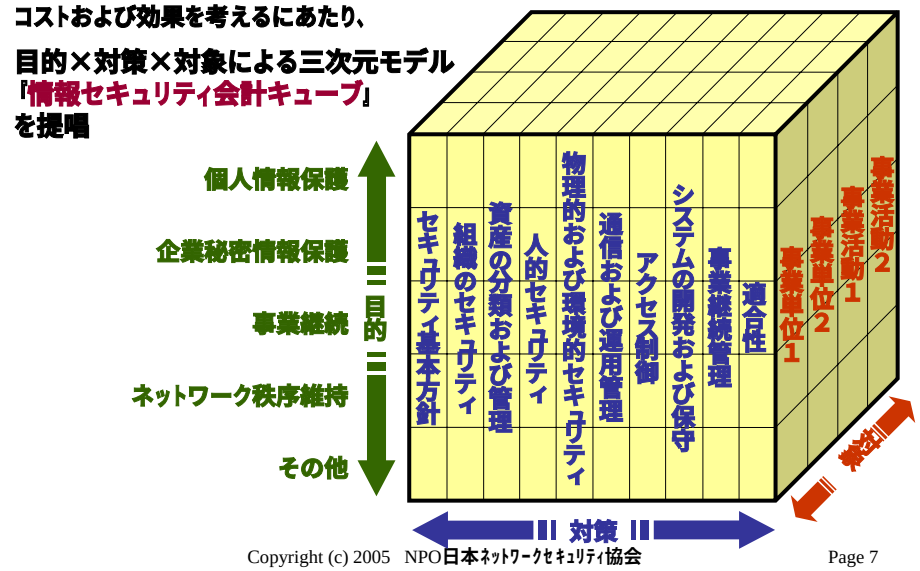
Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

“セキュ会キューブ”と言います！

JNSA

コストおよび効果を考えるにあたり、

目的×対策×対象による三次元モデル
『情報セキュリティ会計キューブ』
を提唱



Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 7

コストと効果をこう考えます！

JNSA

情報セキュリティ対策コスト

情報セキュリティインシデントの発生の防止、抑制または回避、影響の除去、発生した被害の回復またはこれらに資する取り組みのための投資額および費用額

対策 × 対象

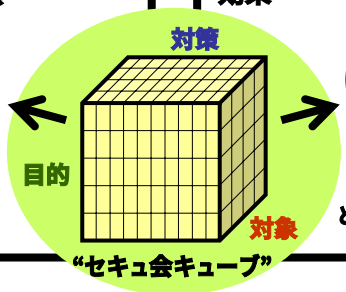
どの対象において、
どのような対策に、
どれだけ掛けたか？

情報セキュリティ対策効果

情報セキュリティインシデントの発生の防止、抑制または回避、影響の除去、発生した被害の回復またはこれらに資する取り組みによる効果

目的 × 対象

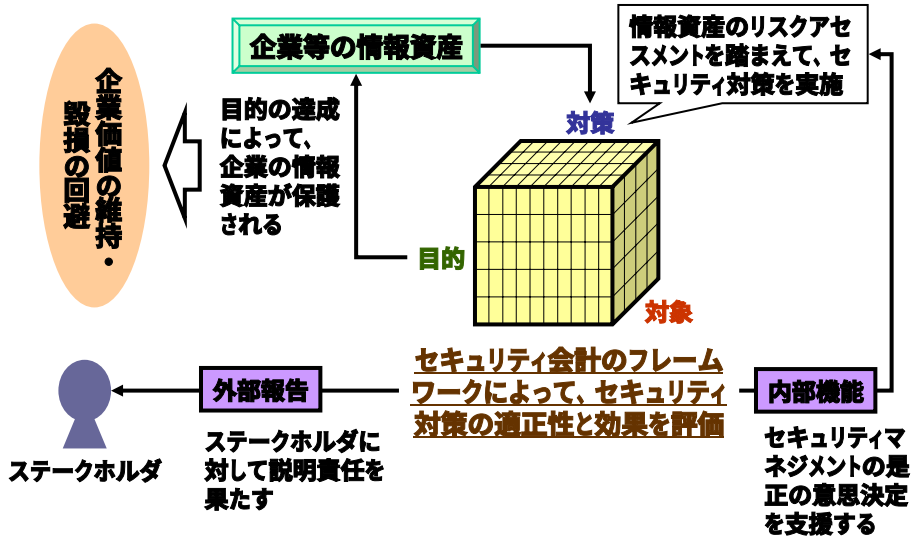
各対象ごとに、
設定された目的に対して、
どの程度の効果があったか？



Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 8

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

内部機能と外部機能があります！



Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 9

こんな使われ方ができるかも・・・

セキュリティ会計の導入イメージ、並びに波及効果

1) 内部管理への適用
   - 米国・連邦情報セキュリティ管理法に基づく内部管理、ISMS認証制度

2) セキュリティ監査とのセット利用

3) 情報セキュリティ報告書等との連携
   - コーポレートコミュニケーション活性化のツールとして期待

4) セキュリティ会計の特典
   - 情報セキュリティ融資に係る優遇金利の適用

5) 情報資産の価値評価
   - マーケティング活動における顧客情報の資産価値

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 10

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

2 コスト

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

コストを分類してみる

分類	内容
事業エリア内コスト	主たる事業活動により事業エリア内で生じる情報セキュリティ確保（情報ネットワークシステムを外部からの攻撃、内部からの不正使用、誤使用から保護するため）に係るコスト
取引先・委託先等に対する情報セキュリティ対策コスト	取引先・委託先等との情報のやり取りに伴って生じる情報セキュリティ確保に係るコスト、並びに取引先・委託先等の情報セキュリティのレベル向上に係るコスト
管理活動コスト	情報セキュリティ確保のための管理活動に伴うコスト
研究開発コスト	研究開発活動における情報セキュリティ対策のコスト
社会活動コスト	社会活動における情報セキュリティ対策のコスト
情報セキュリティ事故対応コスト	情報セキュリティ事故に対応するコスト
その他コスト	その他情報セキュリティ対策に関連するコスト

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

JIS X 5080 と対応づける
(情報セキュリティ管理基準)

JIS X 5080の分類(対策)	コスト分類
セキュリティ基本方針	管理活動コスト
組織のセキュリティ	管理活動コスト
	取引先・委託先等に対する情報セキュリティ対策コスト
資産の分類および管理	管理活動コスト
人的セキュリティ	管理活動コスト
物理的及び環境的セキュリティ	事業エリア内コスト
通信および運用管理	事業エリア内コスト
アクセス制御	事業エリア内コスト
システムの開発および保守	事業エリア内コスト
事業継続管理	管理活動コスト
適合性	管理活動コスト

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

「詳細コスト集計表」を例示する

※JIS X 5080に対応

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(物物件費)	内部人件費	その他		
9.5 オペレーティングシステムのアクセス制御										
9.5.1 自動の端末識別	無線LANを利用する場合の端末認証のための適切な設定、VPNの利用	無線LANサーバ等の費用、VPNのサーバ等の費用	無線LANサーバ等の費用、VPNのサーバ等の費用	導入対応のための内部の人件費	無形又は有形固定資産勘定の毎期の減価償却費	保守費用	導入対応のための内部の人件費		廃棄業者への機密削除費用	
9.5.2 端末のログオン手順	フィルタリングを実施してしている機器(ファイアウォール、ルータ、プロキシ・サーバなど)の導入、OSの設定	ファイアウォール、ルータ、プロキシ・サーバ費用	ファイアウォール、ルータ、プロキシ・サーバ費用	導入対応のための内部の人件費	無形又は有形固定資産勘定の毎期の減価償却費	保守費用	導入対応のための内部の人件費		廃棄業者への機密削除費用	
9.5.3 利用者の識別および認証	OSの設定	サーバ等の費用	サーバ等の費用	導入対応のための内部の人件費	無形又は有形固定資産勘定	保守費用	導入対応のための内部の人件費		廃棄業者への機密	
9.5.4 パスワード管理システム	OSの設定	サーバ等の費用	サーバ等の費用	導入対応のための内部の人件費	無形又は有形固定資産勘定	保守費用	導入対応のための内部の人件費		廃棄業者への機密	
9.5.5 システムユーティリティの使用	ユーティリティソフトの利用	ユーティリティソフトの費用	ユーティリティソフトの	導入対応のための内部の人件費	無形又は有形固定資産勘定	保守費用	導入対応のための内部の人件費		廃棄業者への機密	
9.5.6 利用者を保護するための脅迫に対する警報	警報のための仕組みの導入	仕組みの導入費用	仕組みの導入費用	導入対応のための内部の人件費	無形又は有形固定資産勘定	保守費用	導入対応のための内部の人件費		廃棄業者への機密	
9.5.7 端末のタイムアウト機能	OSの設定	サーバ等の費用	サーバ等の費用	導入対応のための内部の人件費	無形又は有形固定資産勘定	保守費用	導入対応のための内部の人件費		廃棄業者への機密	
9.5.8 接続時間の制限	OSの設定	サーバ等の費用	サーバ等の費用	導入対応のための内部の人件費	無形又は有形固定資産勘定	保守費用	導入対応のための内部の人件費		廃棄業者への機密	

情報セキュリティ対策として、ISMSを推進している企業にとっては、その延長線上に「情報セキュリティ会計」が位置づけられるのであれば、一貫性があり、メリットがあると考える。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

JNSA

3 効果

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

2つのアプローチが考えられるが、・・・

JNSA

1) 情報資産の価値や脆弱性、脅威の発生可能性を定量化し、年間損失予想額を積み上げてコスト対効果を算定するアプローチ方法

2) 情報セキュリティにおける評価指標を設定し、これらの達成度合いを数値化することにより効果を算定するアプローチ方法

ここでは、“セキュ会キューブ”に従い、2) を選択する。

事業単位や事業活動ごとの単位で把握可能な明確な指標に沿って効果を算定することが、経営者や顧客などの「報告を受ける者」にとっては理解し易いと考える。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

例えば、こんな評価指標でしょうか？

目的	対象	評価指標（例）
個人情報保護	特定部署 特定事業活動 全社レベル	個人情報漏洩事件発生件数
		個人情報への不正アクセス件数
		個人情報に関する苦情・問い合わせ件数
企業機密情報保護	特定部署	機密情報漏洩事件発生件数
事業継続	全社レベル	時間
		事態の収束までに要した時間
ネットワーク秩序維持	特定部署 特定事業活動	外部に発信した不正パケットの量
		Webページの改ざん被害件数
その他	特定部署 特定事業活動 全社レベル	コンピュータウイルスの感染件数
		ユーザによる情報セキュリティポリシ違反件数

未完成につき、今後の検討課題である。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

4 今後の進め方

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

次は、ガイドラインの策定へ

初年度にあたる２００４年度は、セキュリティサイドから、『セキュリティ会計』という領域にチャレンジし、その素材を調製した。

今年度は、“ガイドラインの策定”に着手したい。

- 素材の精緻化、評価指標の設定
- 外部機関等との意見交換
- ガイドライン策定でジョイント
- モニタリング　など

Copyright (c) 2005　NPO日本ネットワークセキュリティ協会

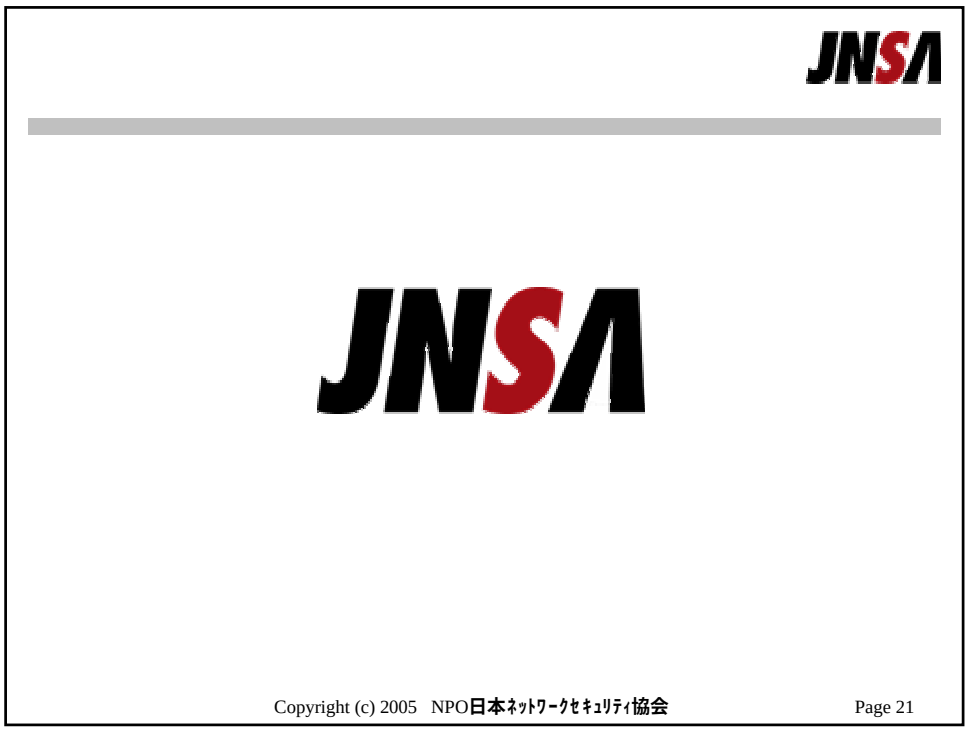
さいごに

ここまでの検討内容を取りまとめ、現在、報告書を作成中、近日公開予定

このテーマは、未だ完成された研究ではなく、みなさまと広く意見交換を重ねながら、さらなるチャレンジをしていきたいと考えている。

Copyright (c) 2005　NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会



Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会