JNSA

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

～2005年度活動報告～

2006 年 5 月 30 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)

ワーキンググループのご紹介

- 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」＝「環境会計」からとった造語
- 期待成果：　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
- 設立：　２００４年４月
- メンバー：１５名（２００６年４月１日現在）

ワーキンググループの活動概要

JNSA

２００４年度　・・・・・・＞概念設計

２００５年度　・・・・・・＞コストにフォーカス

- 当ワーキンググループの取り組みに賛同していただいた企業（ＩＳＭＳ認証取得済み）の協力を得て、情報セキュリティ対策コスト集計表（２００４年度成果物）のモニタリングを実施
- 上記を受け、「公開用フォーマット」および「詳細コスト集計表」の改善に向けて設計
- 研究者や企業のＣＳＲ担当者の方々と意見交換

JNSA

2005年度 活動報告 0

2004年度の活動を振り返るところから始めましょう！

《2004年度成果報告会資料（2005年6月13日）より転載》

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。

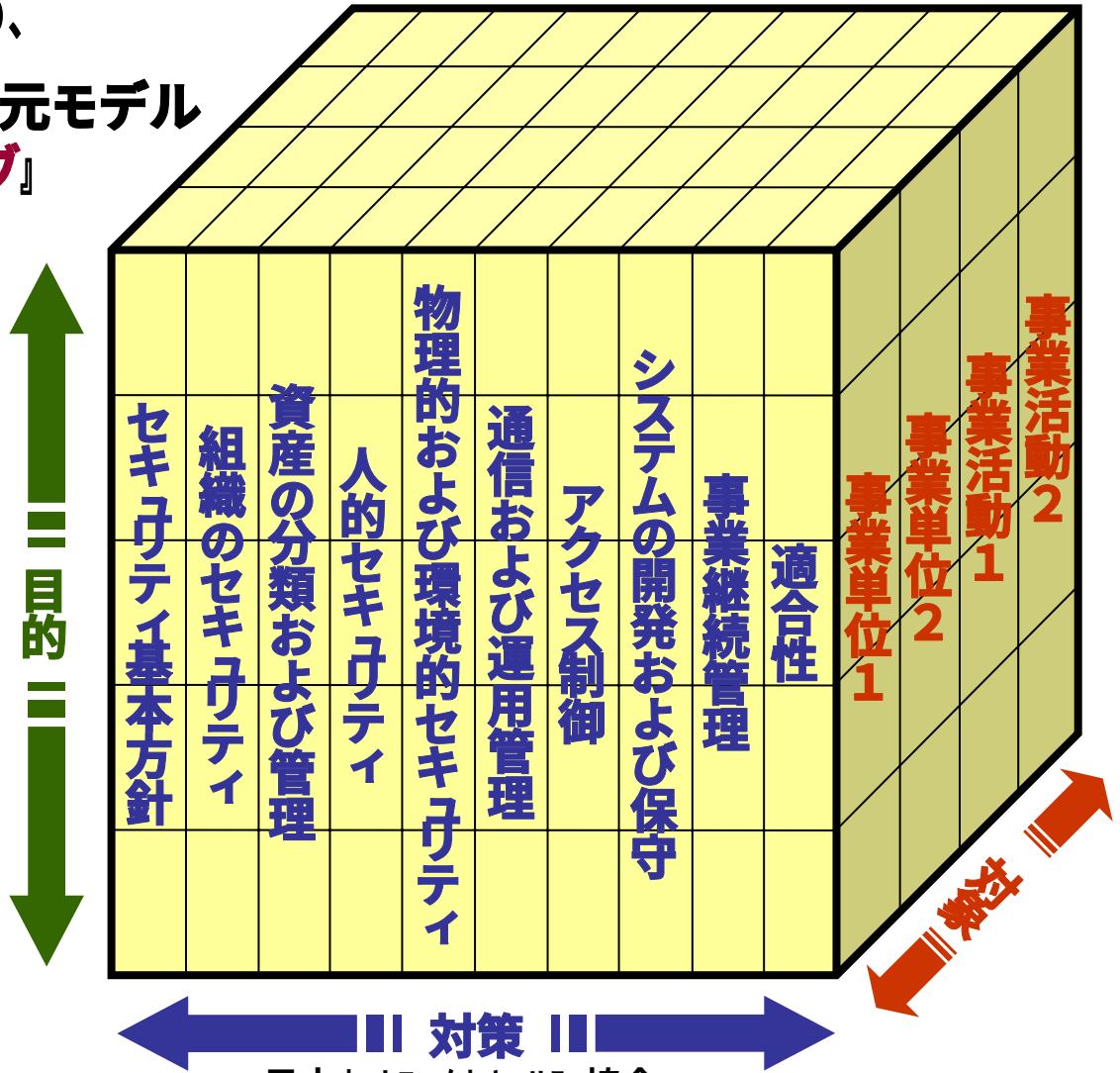
《2004年度成果報告会資料（2005年6月13日）より転載》

“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



《2004年度成果報告会資料（2005年6月13日）より転載》

コストと効果をこう考えます！

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

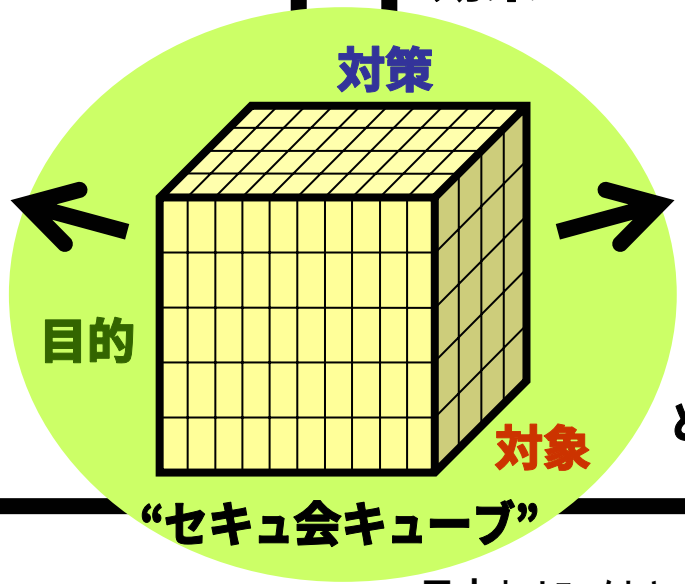
どの対象において、
どのような対策に、
どれだけ掛けたか？

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

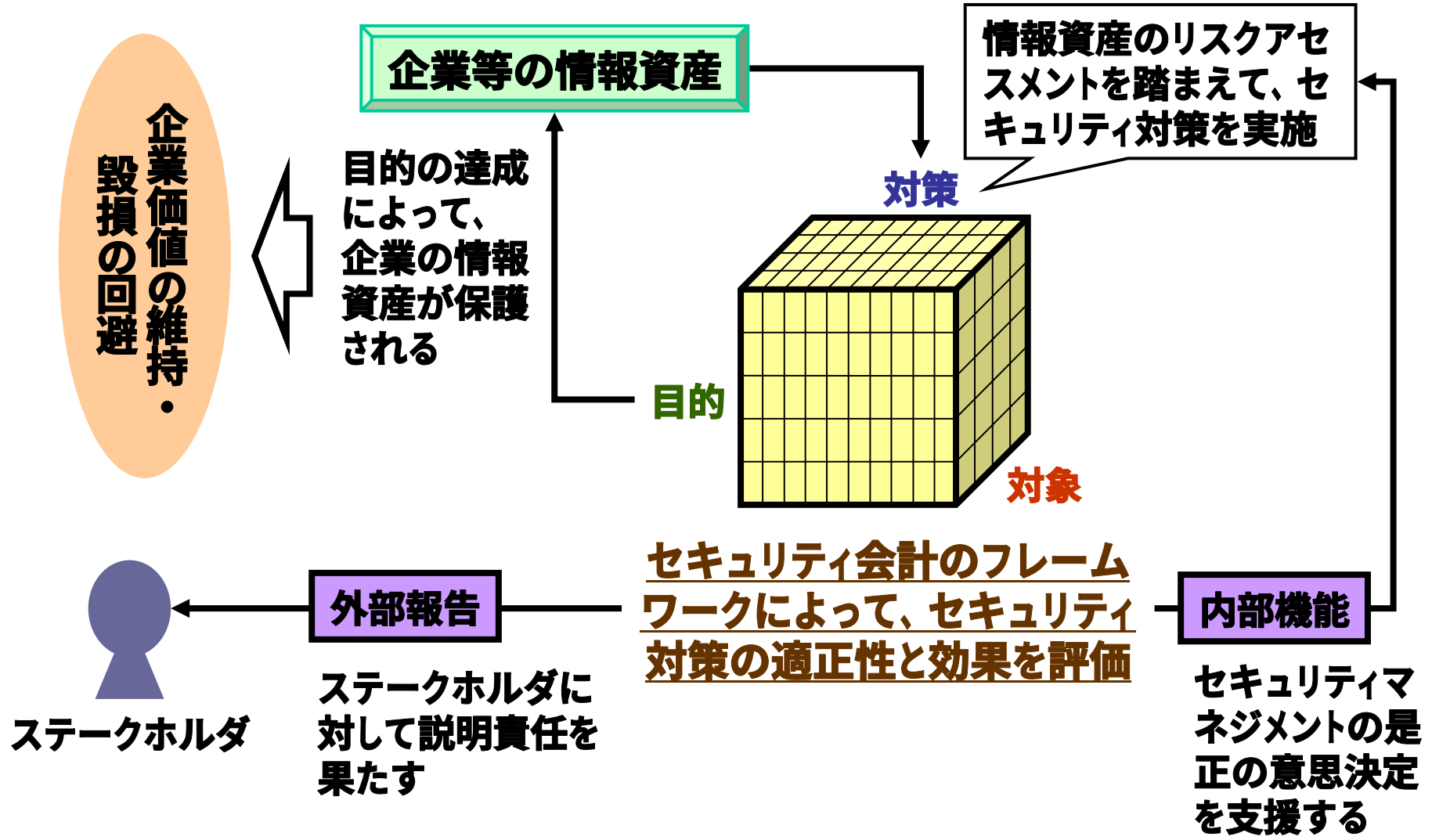
目的 × 対象

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？



《2004年度成果報告会資料（2005年6月13日）より転載》

内部機能と外部機能があります！



《2004年度成果報告会資料（2005年6月13日）より転載》

コストを分類してみる ⇒「公開用フォーマット」

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

《2004年度成果報告会資料（2005年6月13日）より転載》

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

《2004年度成果報告会資料（2005年6月13日）より転載》

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（他物件費）	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。

《2004年度成果報告会資料（2005年6月13日）より転載》

例えば、こんな評価指標でしょうか？

※当時、「未完成につき、今後の検討課題である」とした。

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 特定事業活動 全社レベル	機密情報漏洩事件発生件数
		機密情報への不正アクセス件数
事業継続	全社レベル	事業再開（暫定復旧）までに要した時間
		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

2005年度
活動報告 1

情報セキュリティ対策コスト集計表（2004年度成果物）のモニタリングをやりました！

モニタリングの概要

1．　当ワーキンググループの報告書を基に、Y社管理本部長およびISMS運営事務局担当者に作業を依頼

●対象期間：　平成○年○月○日～平成○年○月○日

●管理本部長による作業

対象期間における経費支出を全件視認し、Y社の情報セキュリティレベル向上を目的とする支出をピックアップ情報セキュリティ製品・サービスに対する支出を抽出
※機密性のみではなく、完全性・可用性向上のための支出も抽出

●ISMS運営事務局担当者による作業

JIS X 5080ベースでの項目設定に沿って、対象期間におけるISMS活動に係る投入工数実績を関係者ごとに概算で報告させ、集計

2．　上記の分担により得られたデータを「詳細コスト集計表」に転記

3．　「詳細コスト集計表」を基に、それぞれの分類ごとに集計し、「公開用フォーマット」を作成

「詳細コスト集計表」はこうなりました！（1）

項目	取り組み内容（代表例）	投資額	費用額	廃棄費用	計	「公開用」との対応
セキュリティ基本方針	書式作成、手順書改訂	28,000	90,000	ー	118,000	管理活動
組織のセキュリティ	委員会開催	ー	632,000	ー	632,000	管理活動
資産の分類および管理	情報資産の洗い出し	ー	113,000	ー	113,000	管理活動
人的セキュリティ	ISMS教育の実施	9,000	928,000	ー	937,000	管理活動
物理的および環境的セキュリティ	サーバルームの整備	328,243	1,632,481	ー	1,960,724	事業エリア内
通信および運用管理	サーバ容量拡張、文書処分	247,000	2,548,100	250,700	3,045,800	事業エリア内
アクセス制御	外部接続システム導入	503,000	1,374,700	ー	1,877,700	事業エリア内

「詳細コスト集計表」はこうなりました！（2）

項目	取り組み内容（代表例）	投資額	費用額	廃棄費用	計	「公開用」との対応
システムの開発と保守		ー	ー	ー	ー	事業エリア内
事業継続管理	試験、計画書の改訂、教育	ー	334,000	ー	334,000	管理活動
適合性	ISMS内部監査	ー	696,000	ー	696,000	管理活動
研究開発	（研究開発）	ー	100,000	ー	100,000	研究開発
社会活動	（社会活動）	ー	4,050,000	ー	4,050,000	社会活動
事故対応	（事故対応）	ー	340,000	ー	340,000	事故対応
その他		ー	ー	ー	ー	その他
合計		1,115,243	12,838,281	250,700	13,953,524	

「公開用フォーマット」はこうなりました！

「詳細コスト集計表」との整合性をとるため、「廃棄費用」を追加

項目	取り組み内容 (代表例)	投資額	費用額	廃棄費用	計
事業エリア内コスト	サーバルームの整備 外部接続システム導入 文書処分	1,078,243	5,555,281	250,700	6,633,524
取引先・委託先等に対する情報セキュリティ対策コスト	－	－	－	－	－
管理活動コスト	委員会の開催 ISMS教育の実施 ISMS内部監査 事業継続試験・改訂	37,000	2,793,000	－	2,830,000
研究開発コスト	(研究開発)	－	100,000	－	100,000
社会活動コスト	(社会活動)	－	4,050,000	－	4,050,000
情報セキュリティ事故対応コスト	(事故対応)	－	340,000	－	340,000
その他コスト		－	－	－	－
合計		1,115,243	12,838,281	250,700	13,953,524

モニタリングをやってみたら、・・・

【ご協力いただいた企業さまからのコメント（要約）】

- JIS X 5080の内容に精通している担当者でなければ、実際に「詳細コスト集計表」を使いこなすことは難しい
- ある費目が「詳細コスト集計表」のどこに該当するのかを一義的に決めることが困難な場合があった
- どこまでを情報セキュリティ対策というか？
- 維持コストが圧倒的であった
- “何が読み取れるか？”、“何を伝えたいか？”が弱い
- 「効果」が無いと、やはり片手落ちの感がある
- 集計作業に係る負荷が結構大きい

モニタリングを受けて

1．《内部機能の強化》　「詳細コスト集計表」の改善やこれを効果的に使いこなすための『手引書』の策定

情報セキュリティ対策コストとは何か？
それぞれの施策がどこに分類されるのか？
その計算方法は？
・・・・・・

2005年度報告

2．《外部機能の強化》　別視点からの「公開用フォーマット」の提案など、情報セキュリティ対策コストの開示のあり方の追究

何を伝えるのか？
効果が無いと、本当に片手落ちなのか？
コストだけでも、努力している姿を伝えることができるのではないか？
・・・・・・

2005年度
活動報告 2

情報セキュリティ対策コストの開示のあり方について考えてみました！
～別視点からの「公開用フォーマット」の提案

今度は、「対策の段階」で分類します

対策の段階	
リスク回避の施策	リスク回避
事故の発生を未然に防止するための施策	リスク予防
事故が発生した際の損失を軽減するための施策	リスク軽減
情報セキュリティ確保に向けた管理活動	リスク回避・予防・軽減共通
事故対応	リスク移転
その他	ー

対策の段階に基づく「公開用フォーマット」

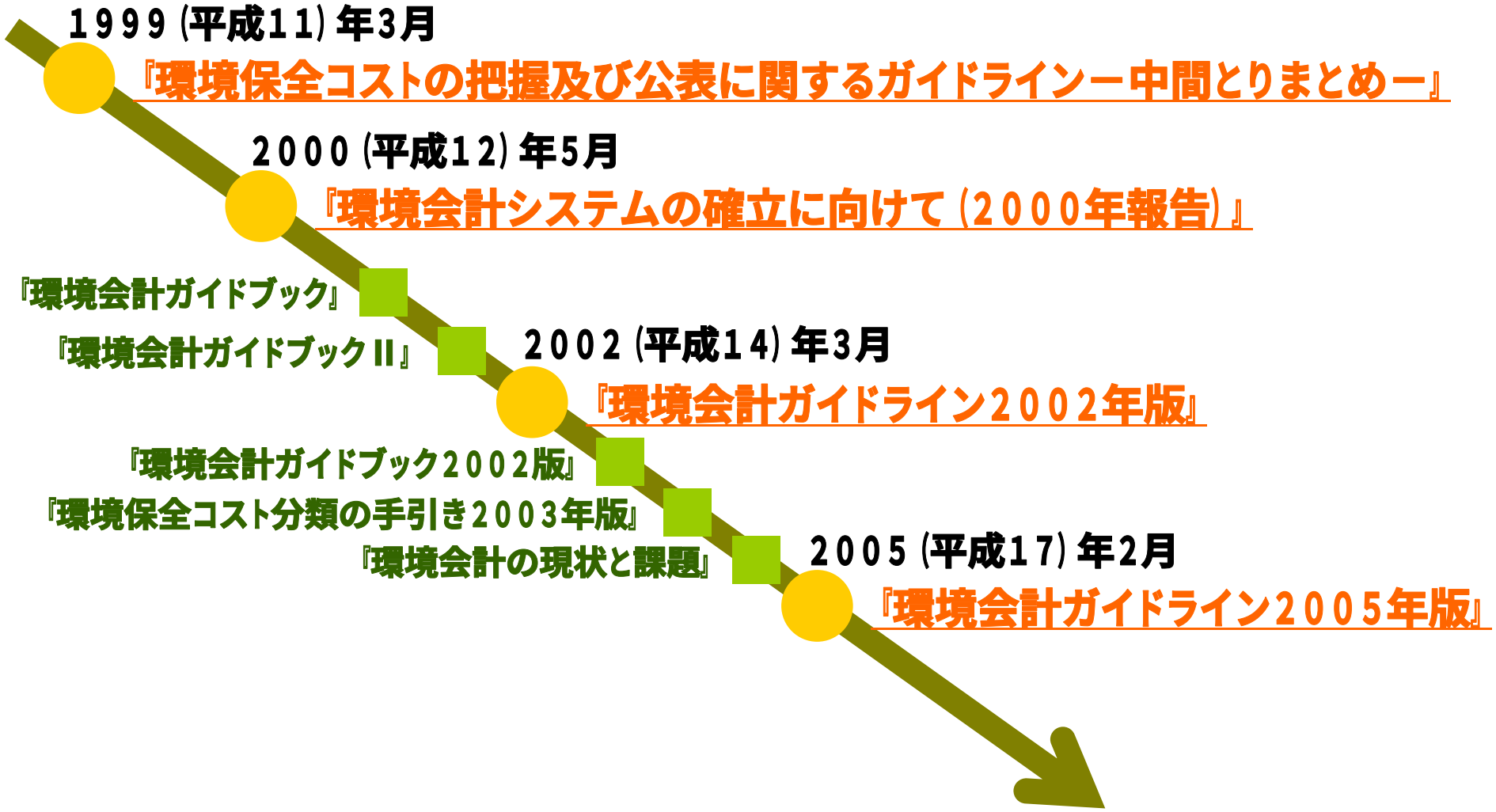
対策の段階	項目	細目	費用	投資	今年度の実施概要
リスク回避の施策	データ廃棄	データ廃棄	0	0	終了したサービスで収集した個人情報の廃棄（外部委託）
事故の発生を未然に防止するための施策（リスク予防）	良好な職場環境の整備	職場における文書管理	0	0	シュレッダーの設置、機密文書回収委託
		委員会・小集団活動等	0	0	
	従業員啓発（派遣等を含む）	情報セキュリティのための教育訓練	0	0	内部監査員教育
		e-ラーニング	0	0	システム開発・運用、コンテンツ制作
		啓発ツール制作	0	0	ポスター・ハンドブック等の制作
		各種資格の受験推奨	0	0	情報セキュリティアドミニストレーター他
	技術面での情報セキュリティ強化	ウイルス対策強化	0	0	
		不正アクセス防止対策	0	0	
	設備面での情報セキュリティ強化	入退室管理の強化	0	0	ICカード導入
		情報金庫の設置	0	0	
	情報セキュリティ確保のための活動	規程類の改訂	0	0	モバイルパソコンの社外持ち出し禁止など
		外部委託先の査察・監査	0	0	
		業界標準の策定	0	0	
事故が発生した際の損失を軽減するための施策（リスク軽減）	良好な職場環境の整備	連絡体制の整備	0	0	
	従業員啓発（派遣等を含む）	情報セキュリティ管理責任者の教育訓練	0	0	
		事故を想定した対応訓練	0	0	
	技術面での情報セキュリティ強化	データセンタの移設費用	0	0	
	設備面での情報セキュリティ強化	自然災害対策	0	0	
	情報セキュリティ確保のための活動	危機管理マニュアルの改訂	0	0	
		BCPの策定	0	0	
情報セキュリティ確保に向けた管理活動（リスク回避・予防～軽減共通）	ISO認証取得		0	0	
	Pマーク維持・運用		0	0	
	内部監査		0	0	
事故対応（リスク移転）	事前負担	個人情報漏洩保険	0	0	
	事後負担	復旧費用	0	0	
		被害者へのお詫び	0	0	
		訴訟費用	0	0	
		広報関連	0	0	
その他	社内表彰		0	0	
	社会貢献		0	0	小学生向けセミナー開催（100校）
	広告		0	0	CM制作

. . . ちょっと寄り道。

ところで、環境会計って、どうだったの？

環境会計を巡る動き

(環境省による公開情報を基に整理)



環境会計を巡る動きから見えて来たこと

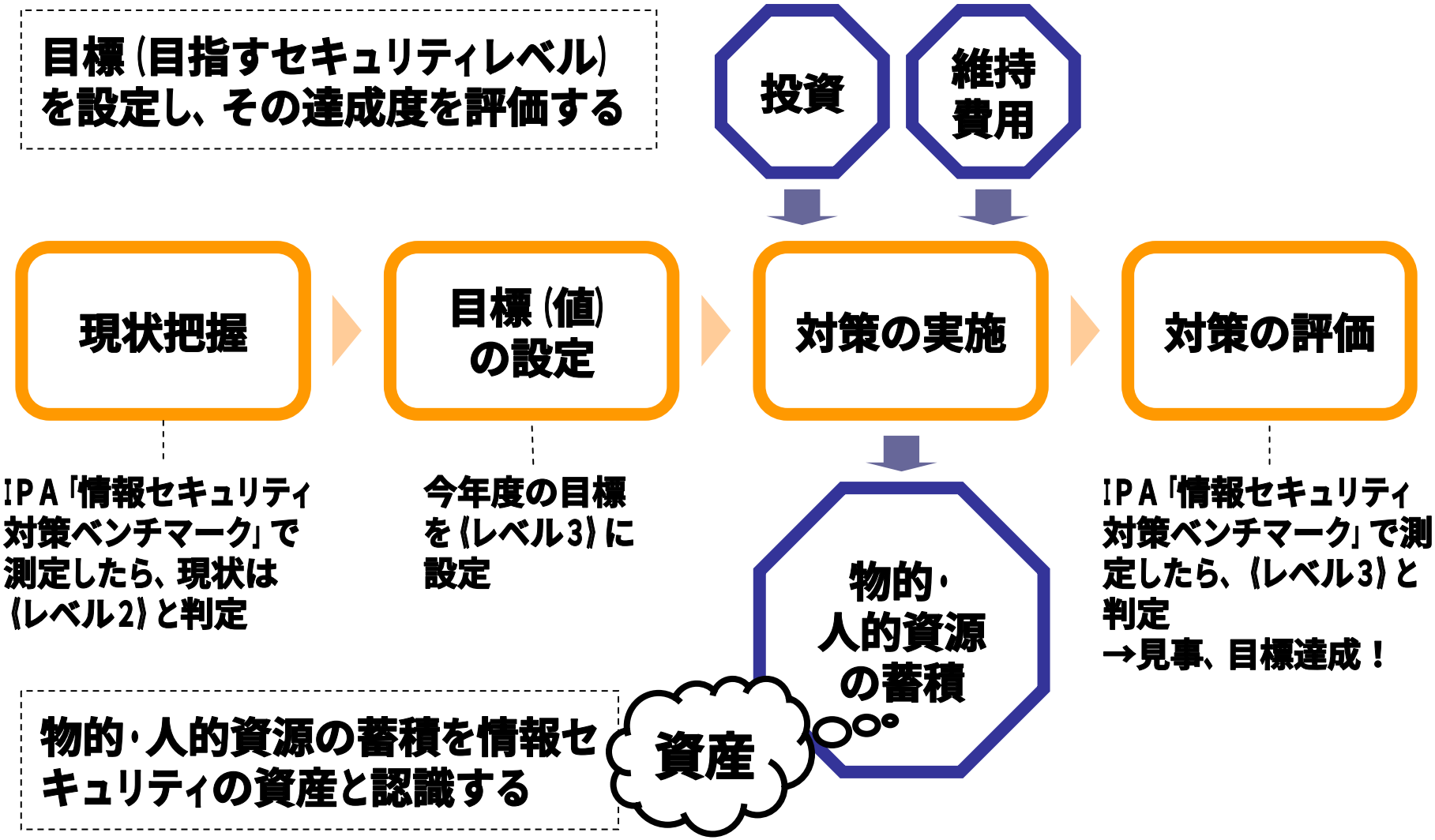
- 環境会計も最初の一歩は「コスト把握」からだった。
- ガイドラインの発行に続いてガイドブックが制作され、環境会計導入に係る解説、Q＆A、導入事例などが記載され、環境会計の普及拡大に貢献している。
- 実際に環境保全コストの集計をしてみると、どの分類に該当するか迷うという声が多く寄せられたため、コスト分類の「手引き」が作成されている。
- 利用者が理解しやすいという観点から、ガイドラインのコスト分類の他に、類似事例を提供している。
- 維持的コストの効果対応、ストック情報（環境資産・環境負債）の反映などが課題として認識されている。

2005年度
活動報告 3

それでは、「効果」について、どう考えるか？

「効果」についてどう考えるか？

目標（目指すセキュリティレベル）を設定し、その達成度を評価する



効果を考える際の論点

- IPA「情報セキュリティ対策ベンチマーク」との連動により、レベルアップを情報セキュリティ投資に対する効果と考える。
- 情報セキュリティコストを「投資」と「(維持) 費用」に分けて考える
- 情報セキュリティ対策の推進・レベル向上は「物的・人的資源の蓄積」を生む。これを「情報セキュリティ資産」と認識する。
- 教育投資については、物的投資の投資効果を高めることに留意し、その両面をあわせた投資を測る。

2005年度
活動報告 4

まとめ

２００６年度の活動

「２００５年度は、“ガイドラインの策定”に着手したい」と昨年の成果報告会で発信したが、実現できなかった。
ガイドライン策定に向けて、情報セキュリティの領域に止まらず、他分野の方々とも広く意見交換を重ね、引き続き検討していく。

【次なるチャレンジ】

- ＡＢＣ会計の導入（会計としての追究）
- 今回提示した「公開用フォーマット」を含めたモニタリングの実施
- 情報セキュリティ投資に対する“ご利益”の追究
- 『セキュ会』の使い方の追究
- シンポジウムの開催　など

さいごに

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。