情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2009年
情報セキュリティ調査から見た日米の比較

鈴木宏幸 宮本智 大和田竜児 村上靖 水沼彩子 澤近俊輔 新原功一 内田勝也

情報セキュリティ大学院大学

INDEX

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

1.セキュリティを取り巻く環境

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ大学院大学内田研究室では2003年より毎年継続して日本国内の情報セキュリティ調査を実施している。

米国の情報セキュリティのベンチマーク的な役割を果たすCSI(Computer Security Institute)の調査とほぼ同様の項目の調査項目を設定し、日米比較を行う。

ただし、セキュリティを取り巻く環境が異なり単純に比較できない部分がある。

均質な社会

- ほぼ単一民族国家
- 安全な社会(国別治安ランキング5位※1)
- 社会が安全を保障するという考え方

多様性を持った社会

- 典型的な多民族国家
- 高い犯罪率(日本の約5.1倍:2005年※2)
  (国別治安ランキング97位※1)
- 安全は自分で守るという考え方。

社会の変化やIT化の加速等により日本の均質性は崩れつつある。
⇒情報セキュリティ分野ではこれが顕著になりつつあることをふまえて
調査データを読み解いていきたい。

※1 Global Peace Index 2008年調査結果 http://www.visionofhumanity.org/gpi/results/rankings/2008/
※2 外務省 海外安全ホームページ 安全対策基礎データより http://www.anzen.mofa.go.jp/info/info4_S.asp?id=221

2. 調査概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

調査対象

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

下記から選択した約9,000の組織に調査資料を送付
会社四季報(上場企業, 未上場企業)
教育機関(4年制大学)
自治体(県, 政令指定都市, 中核市)

匿名での回答を得る形で実施

2009年回答数644件

※以降「国内調査」(年Jと表記)

CSI

約5,000人の情報セキュリティ専門家に対して調査資料を送付。
対象者は, 送付者側で抽出するのではなく, 原則として自薦による

匿名での回答を得る形で実施

2008年回答数522件

※以降「CSI調査」(年Cと表記)

2. 調査概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

国内調査設問の構成

1 貴組織・ご記入者について
2 情報セキュリティ予算について
3 情報セキュリティ監査について
4 情報セキュリティ教育について
5 情報セキュリティ対策について
6 情報セキュリティ事故(インシデント)の発生について
7 情報セキュリティ事故(インシデント)が発生した時の、組織の対応について

⇒全37問、設問は金額記入を除き全て**選択形式**とした。

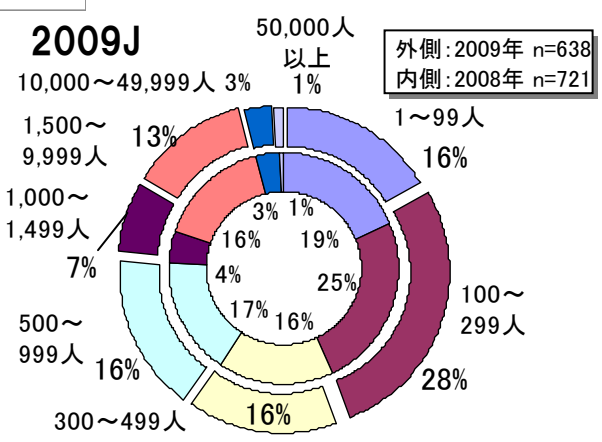
日米比較をおこなうために、質問項目をあわせ、さらに質問を追加した。

回答用紙は以下のURLからダウンロード可能
http://lab.iisec.ac.jp/~uchida_lab/enq/csi/2008/index.html

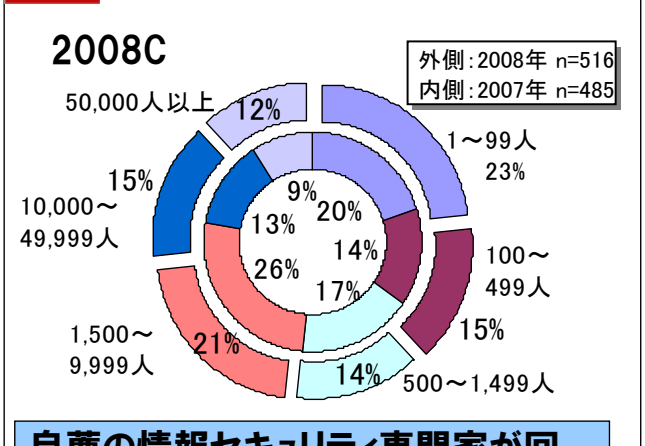
2. 調査概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

回答組織の規模



母集団である会社四季報の分布とほぼ同等の分布



自薦の情報セキュリティ専門家が回答していることから，専門組織を置いている大組織の回答が多かった

国内調査の方が調査対象を網羅していると考えられる。

2. 調査概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

回答組織の規模

500人以上の組織の割合

40%

62%

1,500人以上の組織の割合

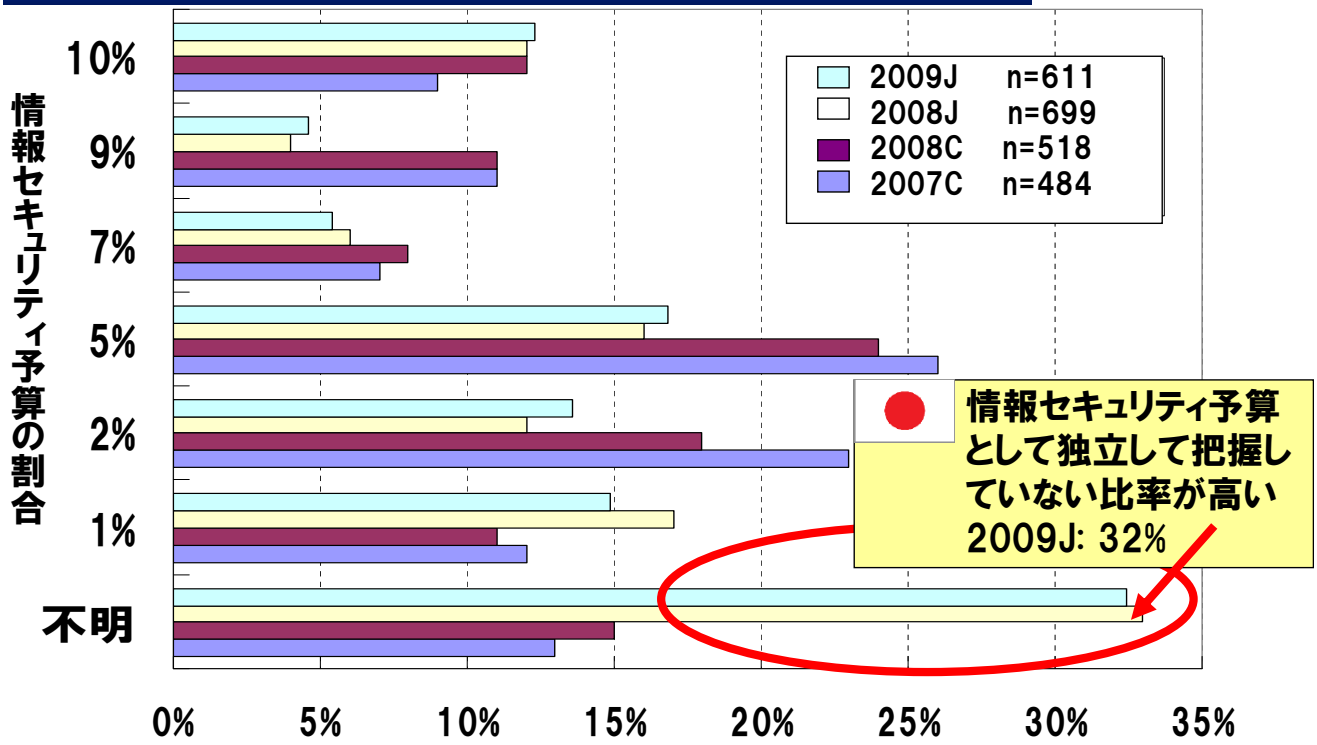
17%

48%

3.1情報セキュリティ予算について

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ予算が情報システム予算に占める割合



3.1情報セキュリティ予算について

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

まだセキュリティ予算として独立した予算として把握していない比率が高い。

前回調査より情報システム予算のうちセキュリティ予算割合1%以上の比率が約2%増加している。

情報セキュリティの重要性を組織が認識し、ある程度の予算確保をしたためと思われる。

日本と比較しセキュリティ予算の割合が多い。

⇒情報システムのうち3～5%を情報セキュリティ予算としている組織の割合24%

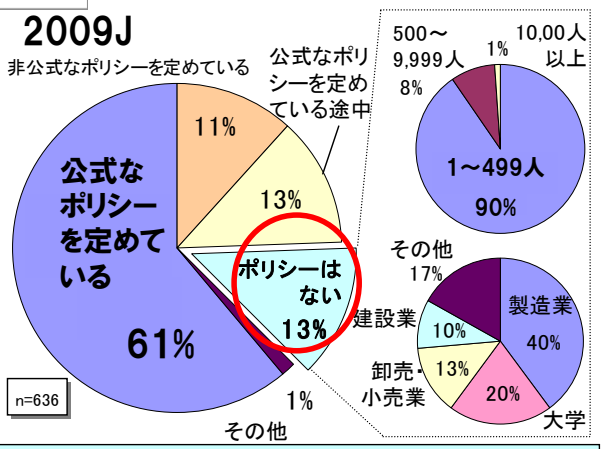
米国では情報セキュリティ予算がITだけではなく法務から監査業務までを含んでいることを考慮すべき。

今後は国内組織も情報セキュリティをIT投資としてではなく、別投資として分け、組織構造も抜本的に改革していく必要があるものと思われる。

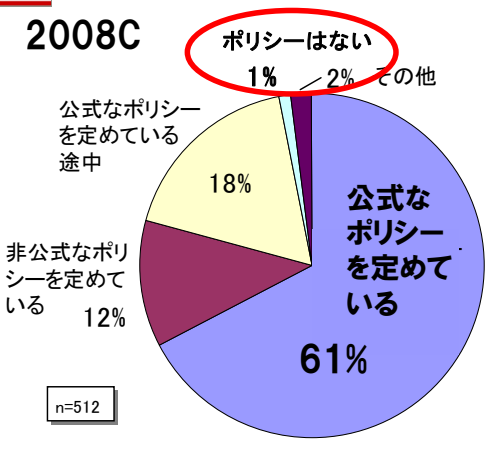
3.2ポリシーについて

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティポリシーを定めている割合



規模の小さい組織ほどポリシーが定められていない。



3.2ポリシーについて

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティポリシーを定めていない組織

ポリシーのない組織の割合

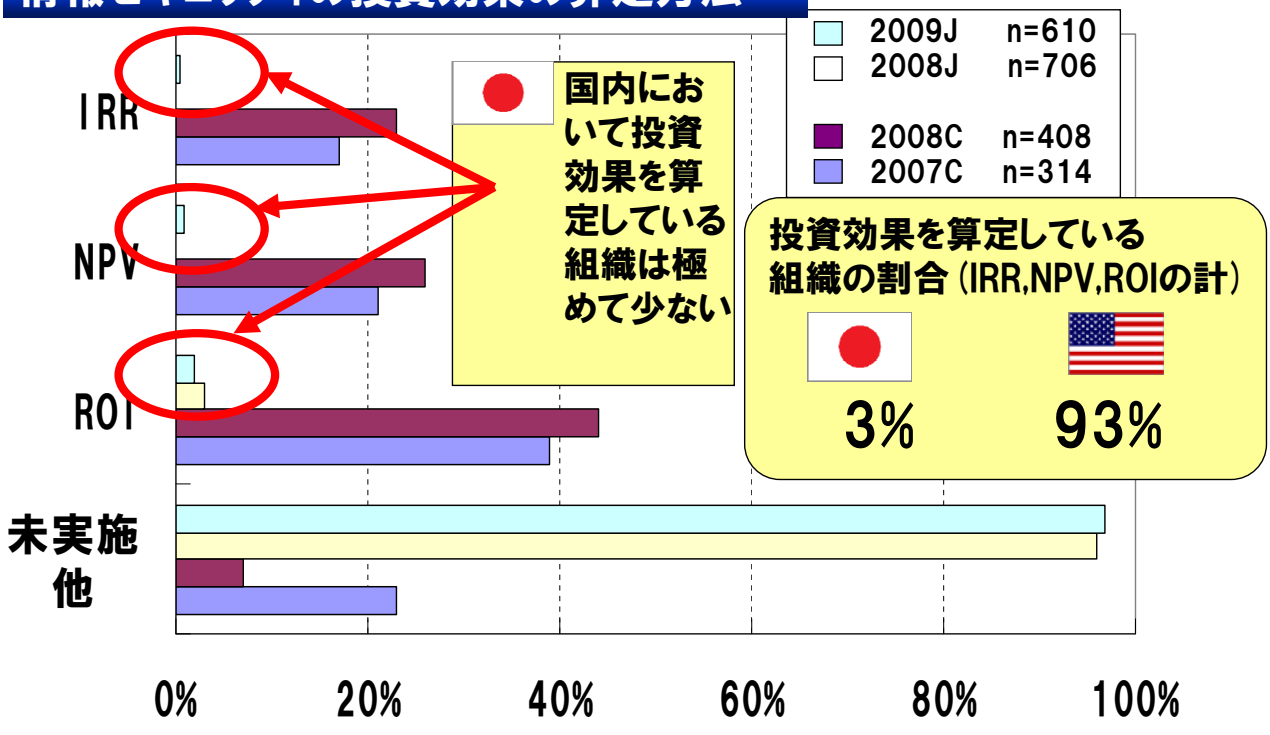
13%　　1%

ポリシーを定める事なくセキュリティ対策を行っても効果が保証されない。
中小組織はセキュリティポリシーテンプレートの適用を実施すべき。

3.3投資効果算定について

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティの投資効果の算定方法



3.3投資効果算定について

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

投資対効果を算定している組織は非常に少ないが、一部の組織が情報セキュリティ投資効果の算定を米国での事例を参考に模索しはじめた。

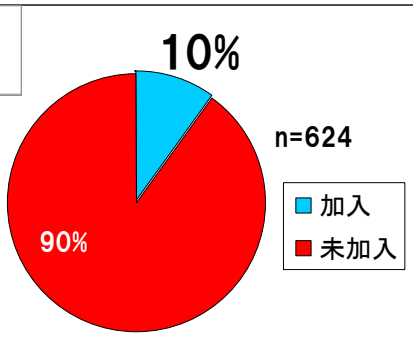
情報セキュリティ投資効果の算出がもはやスタンダードになっている。

情報セキュリティ投資効果を算出する様々な手法を取り入れ、情報セキュリティ予算を確保すべき。
さらに投資家へその効果をアピールすることにより、企業価値を高めていく必要がある。

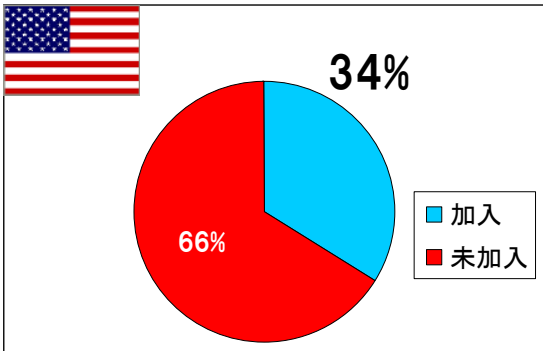
3.4保険

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ保険の加入割合



保険が個別セキュリティ事故に対応するものではなく、包括的な内容になっていて保険料が高い傾向がある。
この事からも、大規模法人が加入しているに留まっている。



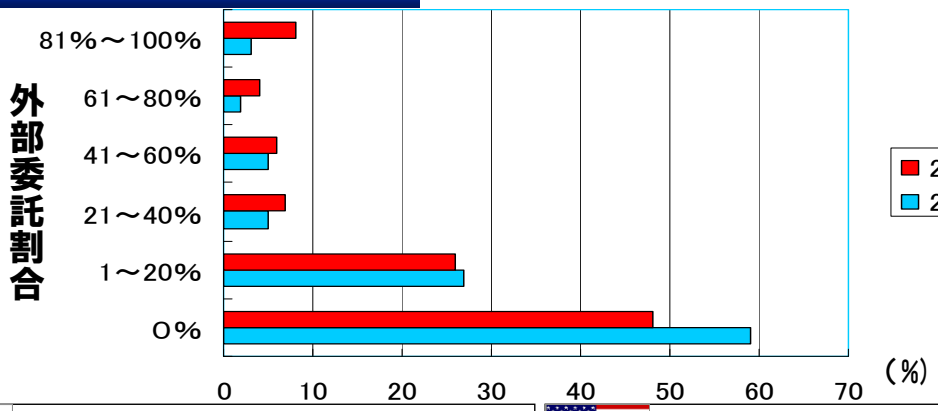
情報セキュリティ保険が一般的になってきており、企業において情報セキュリティを検討する中で、保険が選択肢としてある。

保険は今後は個別セキュリティ事故に対応した製品も増えてくることが想定されることから、今後は国内組織においても加入を検討していくべきである。

3.5外部委託

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ外部委託割合



情報セキュリティ業務の専門性の必要性が増加し、外部に委託する企業が増えている可能性がある。

専門性を考慮し、外部委託を開始した企業がある反面、情報セキュリティ業務を自社に戻す動きがあることも示している。

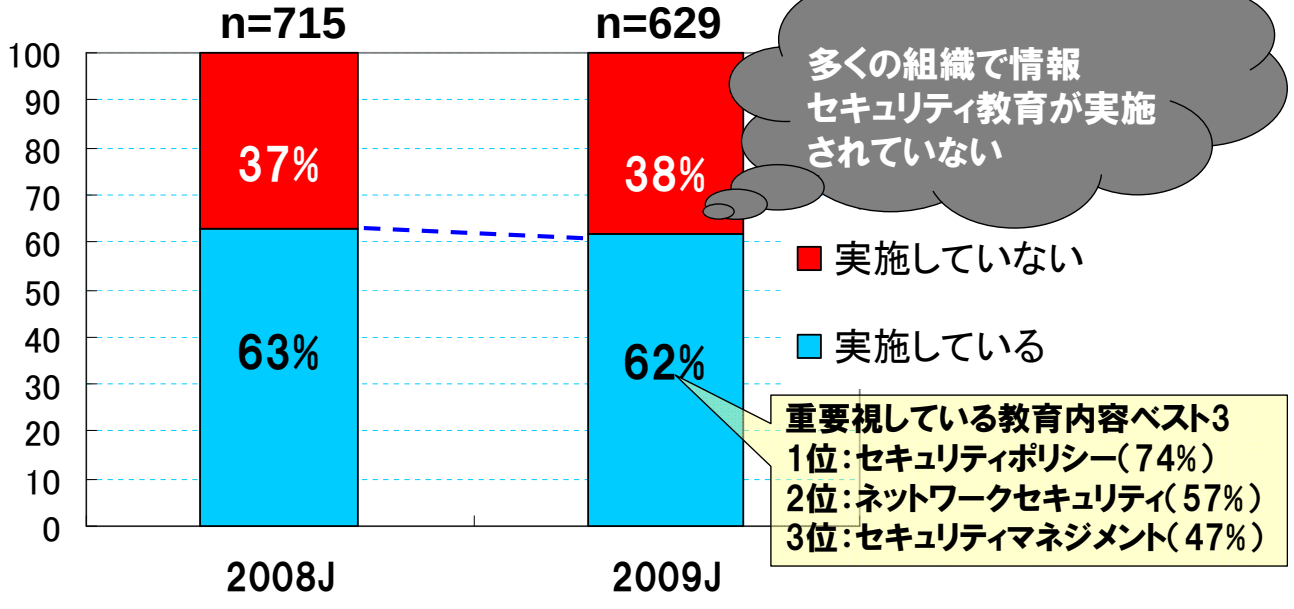
情報セキュリティ業務の外部委託については安全性の検証が不可欠であり、各組織が今後どのように確認していくのか考察が必要である。
⇒外部委託を行う事によってリスクが無くなる訳ではない、あくまでも業務の委託と考え、委託に伴うリスクも考慮し委託を行う事。

3.6教育

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ教育の実施割合

該当する調査項目なし



多くの組織で情報セキュリティ教育が実施されていない

重要視している教育内容ベスト3
1位：セキュリティポリシー（74%）
2位：ネットワークセキュリティ（57%）
3位：セキュリティマネジメント（47%）

3.6教育

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

該当する調査項目なし

・約4割の組織において情報セキュリティ教育が実施されていない。
・情報セキュリティ教育の実施割合は2008年とほとんど変化していない。

セキュリティを取り巻く環境は1年で大きく変化するが、変わらない（変えられない）組織の姿を見る事ができる。

情報セキュリティ教育なしに各種の施策を行っても効果は限定的となり、組織全体の情報セキュリティリスクの削減にはならない。

情報セキュリティ教育は、セキュリティ施策を行う上で組織が共通のベースを作り出す上で必須である。

3.7導入技術

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

導入技術上位5位の経年変化（2009Jを基準に上位5位）

%

	2009J		2008J		2008C		2007C	
	順位	割合	順位	割合	順位	割合	順位	割合
ウィルス対策ソフト	1	98	1	99	1	97	1	98
ファイアーウォール	2	91	2	92	2	94	2	97
一般的なパスワード認証	3	81	3	78	14	46	9	51
アクセス制御	4	73	4	74	13	50	8	56
スパイウェア対策ソフト	5	60	6	54	4	80	4	80
VPN	6	54	5	55	3	85	3	84
IDS	11	30	11	23	5	69	5	69

前年と比較して国内での大きな変化なし。
日本では未だ一般的なパスワード認証に依存する比率が高い。

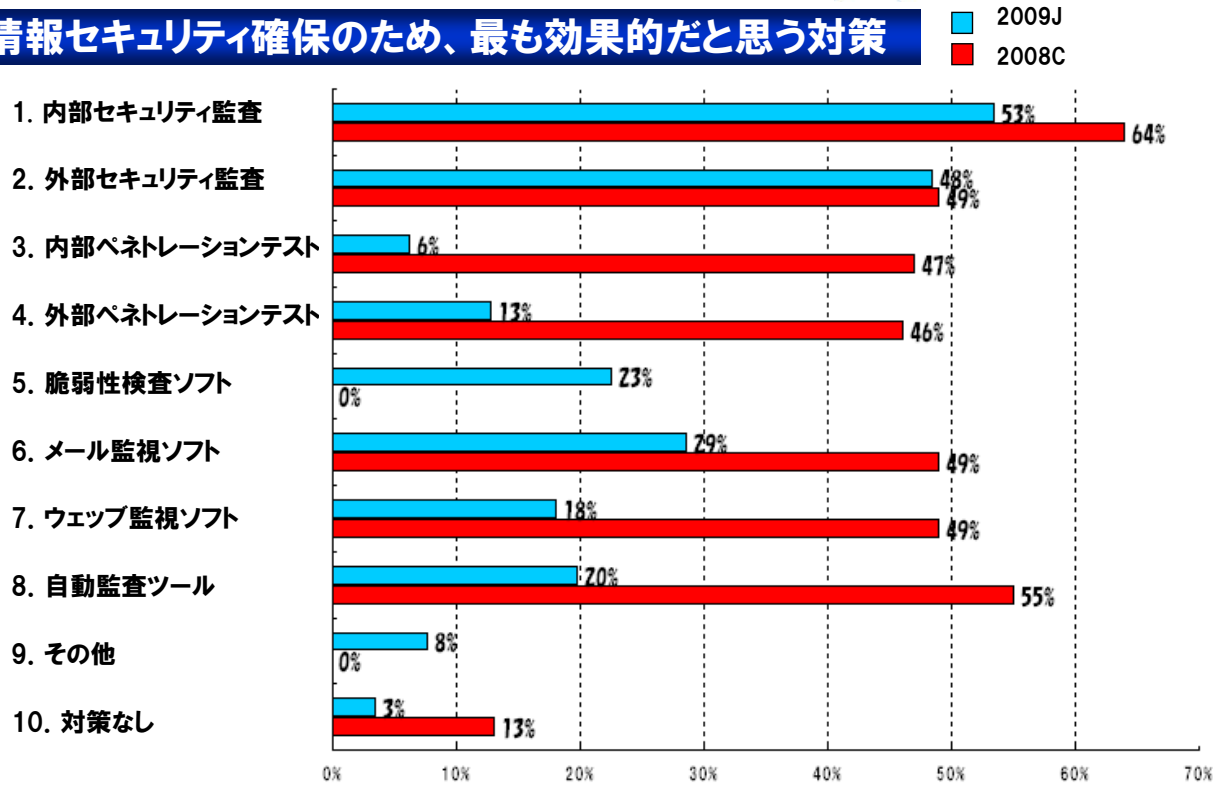
2008CではVPNが3位、IDSが5位に入る。
比較的コストがかかるセキュリティ製品であっても効果が見込めれば導入が進む。
一般的なパスワード認証に代わる認証技術の導入が進んでいる。
（Smartcard 36% Biometrics23%）

米国の技術をウオッチし、効果が見込めるものを日本にも積極的に導入すべき。

3.8セキュリティ確保のための対策

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ確保のため、最も効果的だと思う対策



※5.脆弱性検査ソフトと9.その他はCSI調査では項目なし

3.8セキュリティ確保のための対策

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

セキュリティ確保の対策として監査が上位に挙がっている。
↓
監査が有効であるという認識が高まっていると推測される。

日本以上に監査を有効と考えている割合が高い。
（内部監査の割合が高いのは、組織内に専門家を有しているためと推測される。⇒内部監査は状況にフレキシブルに対応でき、またそれが出来る実力を組織が有している）
また、監査だけではなく、テスト、ツールを組み合わせてセキュリティを確保している事が推測される。

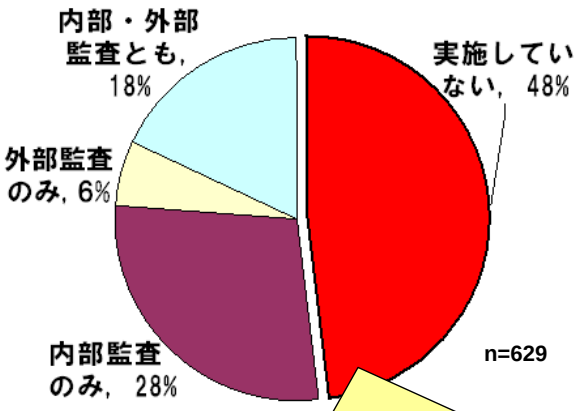
セキュリティ確保の対策としては、監査等の運用技術とテスト、およびセキュリティツールを組み合わせる事が望ましい

3.9監査

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

監査を実施している組織の割合

国内における監査実施の割合



48%の組織において情報セキュリティ監査を実施していない

CSI調査では、内部監査・外部監査の実施状況のみを設問化していないため単純な比較はできないが、セキュリティ技術の評価を行うツールとして、49%が外部監査を、64%が内部監査を利用している

監査自体が情報セキュリティを確保する有効なツールであると認識されている。

監査を行なう事により組織の現在の状況、情報セキュリティに対する数々の施策及び効果を客観的に示す事ができる。

3.10インシデント

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

インシデント発生率（2009Jを基準に上位5位）

%

	2009J 順位	2009J 割合	2008J 順位	2008J 割合	2008C 順位	2008C 割合
ウィルス感染	1	50	1	60	1	60
発生していない	2	42	2	30	－	－
ノートPCの盗難	3	15	3	25	3	42
内部者のネット・アクセス乱用	4	10	4	16	2	44
Ｄｏｓ攻撃	5	7	5	9	6	21
		n=714		n=633		n=433

・国内ではインシデントの発生傾向は前回調査から変化していない。しかし、2位に「発生していない」が入っている事は、事象を把握しエスカレーションする仕組みがうまく機能していないため、発生を知らないという懸念がある。

的確に事象・インシデントを捉える仕組みの充実が必要。

3.10インシデント

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

発生したインシデント(事故)金額

回答のあったインシデントの総件数は732件(1組織複数回答あり)。

インシデント1件当たりの平均被害額は約43万円。

最大の金融詐欺で2億円の損害。

情報資産の損失額(総計)が顕著に増加している。
- 2008計　8千400万円
- 2009計　1億3千800万円

2008年CSI報告書ではサマリのみ記載あり。

インシデント1件当たりの平均被害額は3万5千ドル。(日本円で約350万円※)

最大の金融詐欺で50万ドルの損害。(日本円で約5千万円※)

※ 1$=¥100換算

国内においても高額の被害が発生している。被害のパターンを知り最適な対策を取る必要に迫られている。

3.10インシデント

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

内部的な対応(2009Jを基準に上位5位)

%

	2009J 順位	2009J 割合	2008J 順位	2008J 割合	2008C 順位	2008C 割合
加害者を特定しようとした	1	31	1	33	1	60
セキュリティホールを塞ぐ為の暫定処置	2	29	4	28	2	54
セキュリティソフトをインストールした	3	29	3	30	4	37
セキュリティパッチをインストールした	4	28	2	31	3	46
その他	5	23	–	22	–	–

米国の方がインシデントレスポンスの体制が確立されている。国内においても早急に体制を整える必要がある。

外部組織への届出(2009Jを基準に上位5位)

%

該当する調査項目なし

	2009J 順位	2009J 割合	2008J 順位	2008J 割合
届出を行わなかった	1	69	1	66
警察	2	22	2	22
IPA	3	8	4	7
その他	3	8	4	7
監督官庁	5	7	3	9
JPCERT/CC	6	3	6	2

国内の傾向は変わらない。届出の割合を高めるために、インシデント情報を共有する仕組みの強化が必要。

4. 調査結果からの考察

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

日米比較から見た国内の状況の考察

①金融・保険業、教育機関の回答の減少

セキュリティの主体がアンケートを送付した企業本体では無く，関連企業にアウトソースされているため回答されないケースがあったと考えられる。

②回答の6割を占める中小組織では、セキュリティの専門役職者がいない。また、セキュリティ対応体制の整備も遅れている。

国内調査では，中小組織では情報セキュリティの専門役職であるCSO，CISO不在の割合が高い。また、セキュリティ全般を専門とする組織を設ける予算、人材が不足している事が読み取れる。

③セキュリティポリシーのない組織が13%あり、小規模組織での割合が高い。

セキュリティポリシーは流用できる。ポリシーテンプレート等の活用を行いポリシーを定める事を提言したい。

4. 調査結果からの考察

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

④投資効果を計っている組織は僅かしかない。

セキュリティだけに無限に投資できる組織はない。今後ステークホルダーは、組織に対して情報セキュリティ投資効果の算定を求めるようになる。

⑤約4割の組織が情報セキュリティ教育を実施していない。

情報セキュリティ教育は組織にセキュリティに対する共通の認識を生む。セキュリティ施策の遂行には情報セキュリティ教育は必須である。

⑥日本国内のセキュリティ状況は米国並みに悪化している。

セキュリティ状況の悪化に対して、対策・体制が追いついて行かない状況が読み取れる。セキュリティ状況をタイムリーに捉え、リスクに対応した対策を取る必要がある。

以上