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

第5回 情報セキュリティ調査から見た情報セキュリティ状況の比較

情報セキュリティ大学院大学
情報セキュリティ研究科
内田研究室

目次

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
INSTITUTE of INFORMATION SECURITY

1. 本調査について

1.1 CSIについて

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

CSIとは

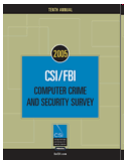
CSI
COMPUTER
SECURITY
INSTITUTE

- Computer Security Institute
- 1974年に設立された会員組織の情報セキュリティ団体
- 米国を中心に約2万人程度の会員
- CSIカンファレンスを毎年開催。今年で35回目

1.2　CSI調査について

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

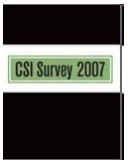
2006年まで



「CSI/FBI COMPUTER CRIME AND SECURITY SURVEY」

サンフランシスコの米国連邦捜査局の
コンピュータ侵入対策チームと共同で調査

2007年



「CSI COMPUTER CRIME AND SECURITY SURVEY」

CSIが単独で行っている

現在に至るまで，質問項目の多くをあまり変えずに行っている
米国における情報セキュリティ調査のベンチマーク的な役割を果たしている。

1.3　国内調査について

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

2002年から

文部科学省の「21世紀COEプログラム」において，中央大学が「電子社会の信頼性向上と情報セキュリティ」拠点として採択された際に開始

CSI調査との比較によって日米の情報セキュリティに対する
取り組みの相違を明らかにする

毎年継続的に実施

1.3　国内調査について

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

	CSI調査	情報セキュリティ調査
対象者	原則として自薦	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) から選択した約9,000の組織
回答数	2005年699名 2006年616名 2007年494名 ⇒回答率：約10%強	2006年1004件 2007年782件 2008年722件 ⇒回答率：約10%前後
特徴	全体的な傾向については的確であるものの，セキュリティのレベルについては米国の平均値より高い可能性がある	CSI調査との比較によって日米の情報セキュリティに対する取り組みの相違を明らかにするために，毎年継続的に実施

1.4　日米の比較と継続的調査の意義

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

米国では様々な情報セキュリティについての調査が行われている

日本では，継続的に日米の状況を比較できるような調査がほとんど存在しない

日本と米国の社会状況は異なる

調査方法や対象も完全に同一でない

比較・考察が意味を持たない

単純に数値の比較を行うことが有効でない調査項目も多い

懸念

情報ネットワークが世界規模のインフラとして重要な役割を担っている

複数の国の状況から全体としての傾向の把握及び分析を行うことは重要である

1.4　日米の比較と継続的調査の意義

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

米国では様々な情報セキュリティについての調査が行われている

日本では，継続的に日米の状況を比較できるような調査がほとんど存在しない

経年変化を発見

調査対象者に**意識の変容や啓発**を促す効果

継続的に調査

情報セキュリティの認識と必要性を高め，間接的にそれを引き上げる効果もある

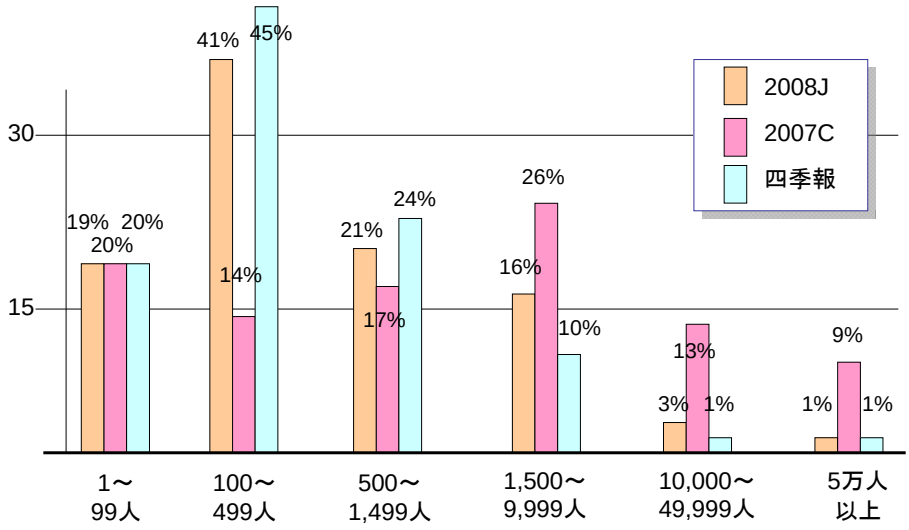
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2.調査結果について

2.1　調査対象（企業規模）

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

回答者の企業規模は，米国CSI調査と国内調査では分布に大きな違いがある。



2.1　調査対象（回答組織の従業員分布）

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

(単位：%)

	1～99人	100～499人	500～1,499人	1,500～9,999人	10,000～49,999人	5万人以上
2008J	24	40	21	16	3	1
2007C	20	14	17	26	13	9
四季報	20	45	23	10	1	1

2008J:2008年国内調査，2007C:2007年CSI調査

2008年の国内調査の結果

最も多いのは「100～499名の企業」全体の40%

国内調査の企業規模の分布については，
四季報の従業員分布とほぼ同様

2.1　調査対象（回答組織の従業員分布）

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

2008年の国内調査の結果

最も多いのは「100～499名の企業」全体の40%

国内調査の企業規模の分布については，
四季報の従業員分布とほぼ同様

2007年のCSI調査の結果

最も多いのは「10,000人以上の企業」全体の22%

大企業ほど，情報セキュリティ専門家を配置し，自薦の情報セキュリティ専門家が回答者になっている

2.1　調査対象（業種の内訳）

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

	国内調査2008		CSI調査2007	
	順位	割合(%)	順位	割合(%)
製造業	1	32	6	8
教育・学習支援業	2	15	4	11
卸売・小売業	3	12	10	2
情報通信業	4	7	5	10
建設業	5	7	―	―
公務(政府・自治体)	6	6	2	13
複合サービス業	7	4	―	―
金融・保険業	8	3	1	20
運輸業	9	3	13	1
不動産業	10	2	―	―
飲食店・宿泊業	11	1	―	―
ハイテク	12	1	―	―
コンサルティング	―	―	3	11
医療・福祉	―	―	7	7

（回答数：CSI調査 494件 国内調査 722件）※複数回答

2.1　調査対象（業種の内訳）

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

	国内調査2008		CSI調査2007	
	順位	割合(%)	順位	割合(%)
製造業	1	32	6	8
教育・学習支援業	2	15	4	11
卸売・小売業	3	12	10	2
情報通信業	4	7	5	10
建設業	5	7	―	―
公務(政府・自治体)	6	6	2	13
複合サービス業	7	4	―	―
金融・保険業	8	3	1	20
運輸業	9	3	13	1
不動産業	10	2	―	―
飲食店・宿泊業	11	1	―	―
ハイテク	12	1	―	―
コンサルティング	―	―	3	11
医療・福祉	―	―	7	7

（回答数：CSI調査 494件 国内調査 722件）※複数回答

2.1　調査対象（業種の内訳）

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

	国内調査2008		CSI調査2007	
	順位	割合(%)	順位	割合(%)
製造業	1	32	6	8
教育・学習支援業	2	15	4	11
卸売・小売業	3	12	10	2
情報通信業	4	7	5	10
建設業	5	7	―	―
公務(政府・自治体)	6	6	2	13
複合サービス業	7	4	―	―
金融・保険業	8	3	1	20
運輸業	9	3	13	1
不動産業	10	2	―	―
飲食店・宿泊業	11	1	―	―
ハイテク	12	1	―	―
コンサルティング	―	―	3	11
医療・福祉	―	―	7	7

（回答数：CSI調査 494件 国内調査 722件）※複数回答

2.1　調査対象（業種の内訳）

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

	国内調査2008		CSI調査2007	
	順位	割合(%)	順位	割合(%)
製造業	1	32	6	8
教育・学習支援業	2	15	4	11
卸売・小売業	3	12	10	2
情報通信業	4	7	5	10
建設業	5	7	―	―
公務(政府・自治体)	6	6	2	13
複合サービス業	7	4	―	―
金融・保険業	8	3	1	20
運輸業	9	3	13	1
不動産業	10	2	―	―
飲食店・宿泊業	11	1	―	―
ハイテク	12	1	―	―
コンサルティング	―	―	3	11
医療・福祉	―	―	7	7

（回答数：CSI調査 494件 国内調査 722件）※複数回答

2.1　調査対象（業種の内訳）

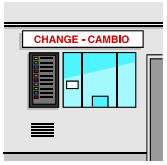
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2008年の国内調査の結果

「卸売・小売業」及び「教育・学習支援業」が上位

当該業種が個人情報を扱っており，個人情報保護の観点からセキュリティへの関心が高いといった傾向を反映しているものと考えられる

2007年のCSI調査の結果



「金融・保険業」及び「コンサルティング」の多さ

米国ではSOX法等への対応のため，相当に専門性を持つ担当者がいることが考えられる

2.1　調査対象（回答者のプロフィール）

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

2008年の国内調査の結果

「情報システム管理部門」と「情報システム開発部門」が64%

情報セキュリティに特別な役職を設けるのではなく，情報システム部門で担当している可能性

情報システム管理の一部であり，情報セキュリティ管理を専任で遂行する部門を有する組織が少ないと推測

2007年のCSI調査の結果

「security officer」が27%

「CEO」，「CIO」，「CSO」及び「CISO」の回答が29%

2.2　情報セキュリティのコスト（予算割合）

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

情報システム予算全体に対する情報セキュリティ予算の割合を調査・比較した結果を示す。

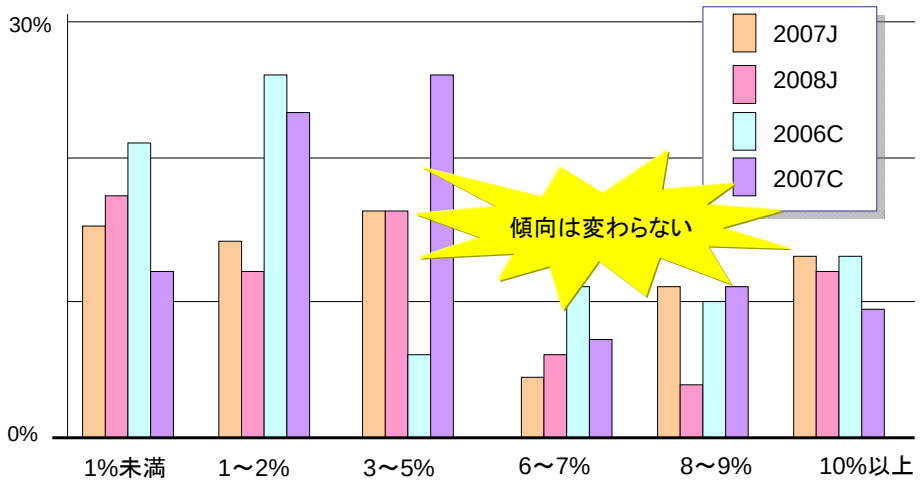
（単位：%）

	国内調査		CSI調査	
	2007J	2008J	2006C	2007C
1%未満	15	17	21	12
1～2%	14	12	26	23
3～5%	16	16	6	26
6～7%	4	6	11	7
8～9%	11	4	10	11
10%以上	13	12	13	9
不明	27	33	12	13

2.2　情報セキュリティのコスト（予算割合）

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

情報システム予算全体に対する情報セキュリティ予算の割合を調査・比較した結果を示す。



2.2　情報セキュリティのコスト（予算割合）

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

2008年の国内調査の結果

- 6%未満の累計が45%
  6%以上10%未満が22%
- 「不明」と答えた割合がCSI調査のほぼ倍近くの割合
- 情報セキュリティに投じたコストの把握が進んでいない傾向

2007年のCSI調査の結果

- 6%未満が12%
  6%以上10%未満の割合が48%

※情報システム予算に占める割合を比較

2.2　情報セキュリティのコスト（投資効果）

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

情報セキュリティ投資効果算出の有無及びその方法について調査・比較した結果を示す。

（単位：%）

	ROI	NPV	IRR	未実施 他
2008J	3	0	0	96
2007J	2	1	0	97
2007C	39	21	17	23
2006C	42	19	21	18

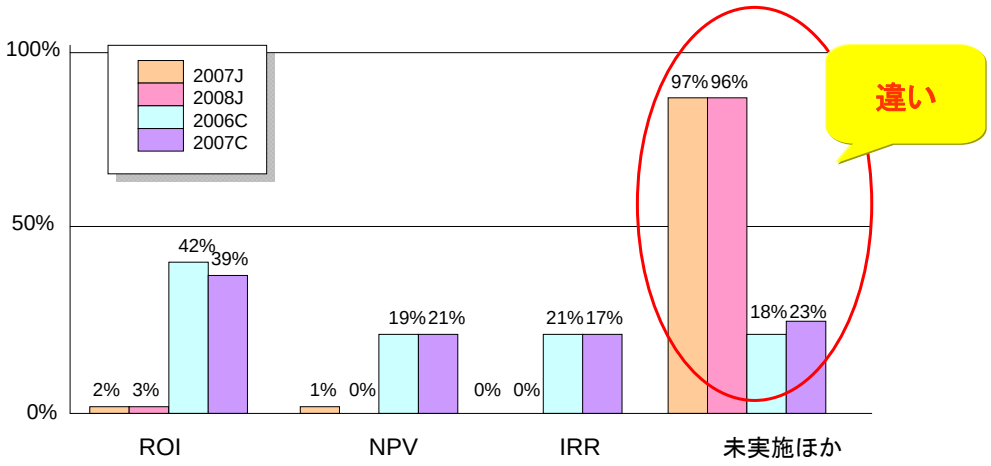
ROI：Return On Investment（投資収益率）
NPV：Net Present Value（純現在価値）
IRR：Internal Rate of Return（内部収益率）

計算していない：82%
不明：10%
その他：4%

2.2　情報セキュリティのコスト（投資効果）

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

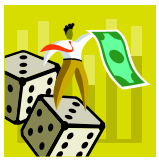
情報セキュリティ投資効果算出の有無及びその方法について調査・比較した結果を示す。



2.2　情報セキュリティのコスト（投資効果）

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

2008年の国内調査の結果



情報セキュリティ投資効果を算出しているとの回答が3%
「未実施 他」の回答が96%

ほとんどの組織において情報セキュリティの投資効果を算出していない

2007年のCSI調査の結果

ROIが39%，NPVが21%，IRRが17%

情報セキュリティ投資効果を算出しているとの回答が合計77%

2.3　情報セキュリティ導入技術

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

	2008J		2007C	
	順位	割合	順位	割合
ウイルス対策ソフト	1	99	1	98
ファイアウォール	2	92	2	97
VPN	5	55	3	84
スパイウェア対策ソフト	6	54	4	80
侵入検知システム（IDS）	11	23	5	69
通信の暗号化	13	22	6	66
パッチマネジメント	16	14	7	63
アクセス制御（サーバ用）	4	74	8	56
一般的なパスワード認証	3	78	9	51
保存ファイルの暗号化	14	20	10	47
	＜中略＞			
ICカード／ワンタイムパスワード	9	30	15	35
PKI	19	8	16	32
無線LANセキュリティ ソフトウェア	―	―	17	28
クライアント用セキュリティ ソフトウェア	―	―	18	27
生体認証システム	17	13	19	18

2.3 情報セキュリティ導入技術

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

	2008J		2007C	
	順位	割合	順位	割合
ウイルス対策ソフト	1	99	1	98
ファイアウォール	2	92	2	97
VPN	5	55	3	84
スパイウェア対策ソフト	6	54	4	80
侵入検知システム（IDS）	11	23	5	69
通信の暗号化	13	22	6	66
パッチマネジメント	16	14	7	63
アクセス制御（サーバ用）	4	74	8	56
一般的なパスワード認証	3	78	9	51
保存ファイルの暗号化	14	20	10	47
	＜中略＞			
ICカード／ワンタイムパスワード	9	30	15	35
PKI	19	8	16	32
無線LANセキュリティ ソフトウェア	―	―	17	28
クライアント用セキュリティ ソフトウェア	―	―	18	27
生体認証システム	17	13	19	18

2.3 情報セキュリティ導入技術

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

2008年の国内調査の結果

「ICカード／ワンタイムパスワード」と「生体認証」の合計が43%
「一般的なパスワード認証」が78%

2007年のCSI調査の結果

「ICカード／ワンタイムパスワード」と「生体認証」の合計が53%
「一般的なパスワード認証」が51%

国内の経年変化は？

2.3　情報セキュリティ導入技術（国内経年変化）

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

	2008J		2007J	
	順位	割合	順位	割合
ウイルス対策ソフト	1	99	1	95
ファイアウォール	2	92	2	92
一般的なパスワード認証	3	78	3	82
アクセス制御（サーバ用）	4	74	4	69
VPN	5	55	―	―
スパイウェア対策ソフト	6	54	5	47
メールフィルタリング	7	38	―	―
ログ管理ソフトウェアICカード／ワンタイム	8	37	6	37
パスワード	9	30	8	26
URLフィルタリング	10	29	―	―
侵入検知システム（IDS）	11	23	9	24
送信中のデータ暗号化	12	23	7	35

2.3　情報セキュリティ導入技術（国内経年変化）

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

	2008J		2007J	
	順位	割合	順位	割合
通信の暗号化	13	22	―	―
保存ファイルの暗号化	14	20	10	19
侵入防止システム（IPS）	15	15	12	15
パッチマネジメント	16	14	―	―
生体認証システムアプリケーション	17	13	14	9
ファイアウォール	18	11	11	17
PKI	19	8	15	9
シンクライアント	20	7	―	―
検疫ネットワークシステム	21	6	―	―
フォレンジックスソフト無線LANセキュリティ	22	2	16	2
ソフトウェア	―	―	13	12
その他	―	3	―	4

（回答数：CSI 調査 436 件，国内調査 716 件）

2.3　情報セキュリティ導入技術

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

2008年の国内調査の結果

「ICカード／ワンタイムパスワード」と「生体認証」の合計が43%
「一般的なパスワード認証」が78%

順位が7位以下になると，導入率の割合が50%以下となっている

国内における情報セキュリティ対策技術の導入の傾向は，
大きく変化していない

2007年のCS

「ICカード／ワンタイムパスワード」と「生体認証」の合計が53%
「一般的なパスワード認証」が51%

2.4　情報セキュリティインシデント

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

実際に発生した情報セキュリティインシデントについて調査・比較した結果を示す。

	2008J		2007C	
	順位	割合	順位	割合
ウイルス感染	1	60	2	52
ノートPCなどの盗難	2	25	3	50
内部者のネット・アクセス乱用	3	16	1	59
DoS攻撃	4	9	6	25
情報への不正アクセス	5	7	7	25
情報資産の盗難	6	4	16	8
システム侵入	7	3	11	13
無線LANの無許可利用	8	3	10	17
ウェブの改ざん	9	2	14	10

割合に違いがあるものの、上位3つのインシデントは同じ

2.4 情報セキュリティインシデント（内部的な対応）

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

	2008J		2007C	
	順位	割合	順位	割合
加害者を特定しようとした	1	33	1	61
セキュリティパッチをインストールした	2	31	3	38
セキュリティソフトをインストールした	3	30	4	36
セキュリティホールをふさぐための暫定措置を施した	4	28	2	54
担当部門だけで処理した	5	21	–	–
組織のセキュリティポリシーを変更した	6	13	5	34
追加のセキュリティハードウエアを導入した	7	11	7	28
何もしなかった	8	2	–	–
弁護士に相談した	9	2	8	24
外部の法執行機関等に報告した	–	–	6	29
外部組織に報告しなかった	–	–	9	30
その他	–	22	–	–

「セキュリティパッチをインストールする」,「セキュリティソフトをインストールする」など，**技術的対策については両調査とも同程度**の割合で行っているとの結果になった。

（回答数：CSI 調査 274 件，国内調査 467 件）

2.4 情報セキュリティインシデント（内部的な対応）

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

「セキュリティパッチをインストールする」,「セキュリティソフトをインストールする」など，**技術的対策については両調査とも同程度**の割合で行っているとの結果になった。

加害者を特定しようとした	1	33	1	61
セキュリティパッチをインストールした	2	31	3	38
セキュリティソフトをインストールした	3	30	4	36
セキュリティホールをふさぐための暫定措置を施した	4	28	2	54
担当部門だけで処理した	5	21	–	–
組織のセキュリティポリシーを変更した	6	13	5	34
追加のセキュリティハードウエアを導入した	7	11	7	28
何もしなかった	8	2	–	–
弁護士に相談した	9	2	8	24
外部の法執行機関等に報告した	–	–	6	29
外部組織に報告しなかった	–	–	9	30
その他	–	22	–	–

（回答数：CSI 調査 274 件，国内調査 467 件）

2.4 情報セキュリティインシデント（内部的な対応）

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

	2008J		2007C	
	順位	割合	順位	割合
加害者を特定しようとした	1	33	1	61
セキュリティパッチをインストールした	2	31	3	38
セキュリティソフトをインストールした	3	30	4	36
セキュリティホールをふさぐための暫定措置を施した	4	28	2	54
担当部門だけで処理した	5	21	―	―
組織のセキュリティポリシーを変更した	6	13	5	34
追加のセキュリティハードウエアを導入した	7	11	7	28
何もしなかった	8	2	―	―
弁護士に相談した	9	2	8	24
外部の法執行機関等に報告した	―	―		29
外部組織に報告しなかった	―	―		
その他	―	22		

お国柄？

（回答数：CSI 調査 274 件，国内調査 467 件）

2.5 情報セキュリティインシデント後の対応

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

情報セキュリティインシデントが発生した場合に，外部組織に報告を行ったかどうか

	2008J
	割合（%）
届出を行わなかった	66
警察	22
監督官庁	8
IPA	7
JPCERT/CC	2
その他	7

（回答数：449 件）

届け出ない理由は？

2.5　情報セキュリティインシデント後の対応

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

外部組織に届出を行わなかった理由について調査した結果を示す。

	2008J		2007C	
	順位	割合	順位	割合
社内対応で十分だと判断したため	1	97	4	7
報告をしようという考えに至らなかったため	2	11	5	5
外部からマイナスイメージを持たれるおそれがあったため	3	2	1	26
警察／監督官庁は頼りにならないと思っているため	4	1	2	22
競合他社に利用されるおそれがあったため	5	0	3	14
その他	―	18	―	2

（回答数：CSI 調査 196 件，国内調査 114 件）

2.5　情報セキュリティインシデント後の対応

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

外部組織に届出を行わなかった理由について調査した結果を示す。

	2008J		2007C	
	順位	割合	順位	割合
社内対応で十分だと判断したため	1	97	4	7
報告をしようという考えに至らなかったため	2	11	5	5
外部からマイナスイメージを持たれるおそれがあったため	3	2	1	26
警察／監督官庁は頼りにならないと思っているため	4	1	2	22
競合他社に利用されるおそれがあったため	5	0	3	14
その他	―	18	―	2

（回答数：CSI 調査 196 件，国内調査 114 件）

2.5　情報セキュリティインシデント後の対応

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

外部組織に届出を行わなかった理由について調査した結果を示す。

	2008J		2007C	
	順位	割合	順位	割合
社内対応で十分だと判断したため	1	97	4	7
報告をしようという考えに至らなかったため	2	11	5	5
外部からマイナスイメージを持たれるおそれがあったため	3	2	1	26
警察／監督官庁は頼りにならないと思っているため	4	1	2	22
競合他社に利用されるおそれがあったため	5	0	3	14
その他	―	18	―	2

（回答数：CSI 調査 196 件，国内調査 114 件）

2.5　情報セキュリティインシデント後の対応

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

2008年の国内調査の結果

「社内対応で十分だと判断したため」が97%

2007年のCSI調査の結果

「外部からマイナスイメージを持たれるおそれがあったため」が26%

「警察／監督官庁は頼りにならないと思っているため」が22%

「競合他社に利用されるおそれがあったため」が14%

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

3.まとめ

3. まとめ

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

まとめ

- 今後も調査を継続して実施し，データの集積を続ける
- 国内の情報セキュリティの対策について，経年変化の傾向を把握できるようなデータを提供する

今後の課題

- 調査方法の改善
- モデルや判断基準の提示

謝辞

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

アンケートに回答していただいた
多くの方々のご協力に
感謝します。

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

ありがとうございました。