

国内主要企業における 情報セキュリティ対策の現状と今後の展望 ～「企業における情報セキュリティ実態調査2007」より～

NRIセキュアテクノロジーズ株式会社 富澤 亮太

はじめに

NRIセキュアテクノロジーズでは、2002年より毎年上場企業を中心に情報セキュリティに対する取り組み状況についてのアンケート調査※「企業における情報セキュリティ実態調査2007」を行っている。

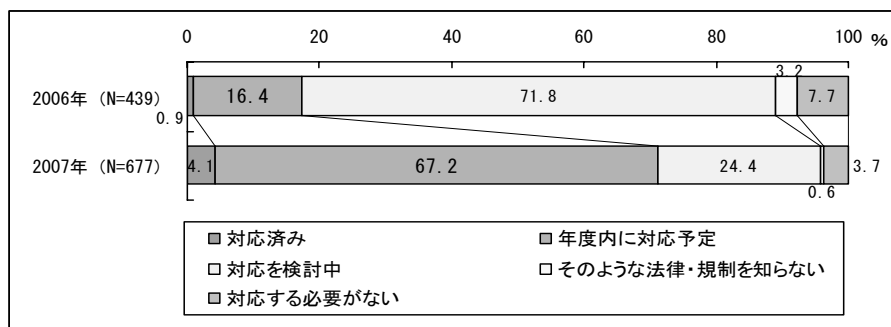
本稿では、688社から回答が寄せられた2007年10月実施の最新のアンケート調査の結果をもとに、企業における情報セキュリティの取り組み実態とともに今後の情報セキュリティのトレンドについて解説する。

1. 情報セキュリティに対する取り組みの現状

1) 日本版SOX法対応の現状

国内主要企業の情報セキュリティに対する取り組みの現状を把握する上で、まず初めに把握しておきたい動向として、上場企業が2008年4月の会計年度から適用される金融商品取引法(日本版SOX法)への対応状況について述べる。

2007年度内に日本版SOX法への対応を予定している企業の割合が全体の67.2%となっている。昨年の調査において、2006年度内に対応を予定していると答えた割合が16.4%だったことに比べると、約50ポイント上昇している。



【ご参考】「企業における情報セキュリティ実態調査2007」の概要

- (1)実施時期 : 2007年10月11日～10月31日
- (2)調査対象 : 東証1部・2部上場企業と従業員300人以上の非上場企業の計2,995社
- (3)調査方法 : 発送・回収とも郵送によるアンケート
- (4)回答企業数 : 688社 (回収率 23.0%)

本アンケート調査の質問票と分析結果の概要は、以下のホームページでご覧いただけます。

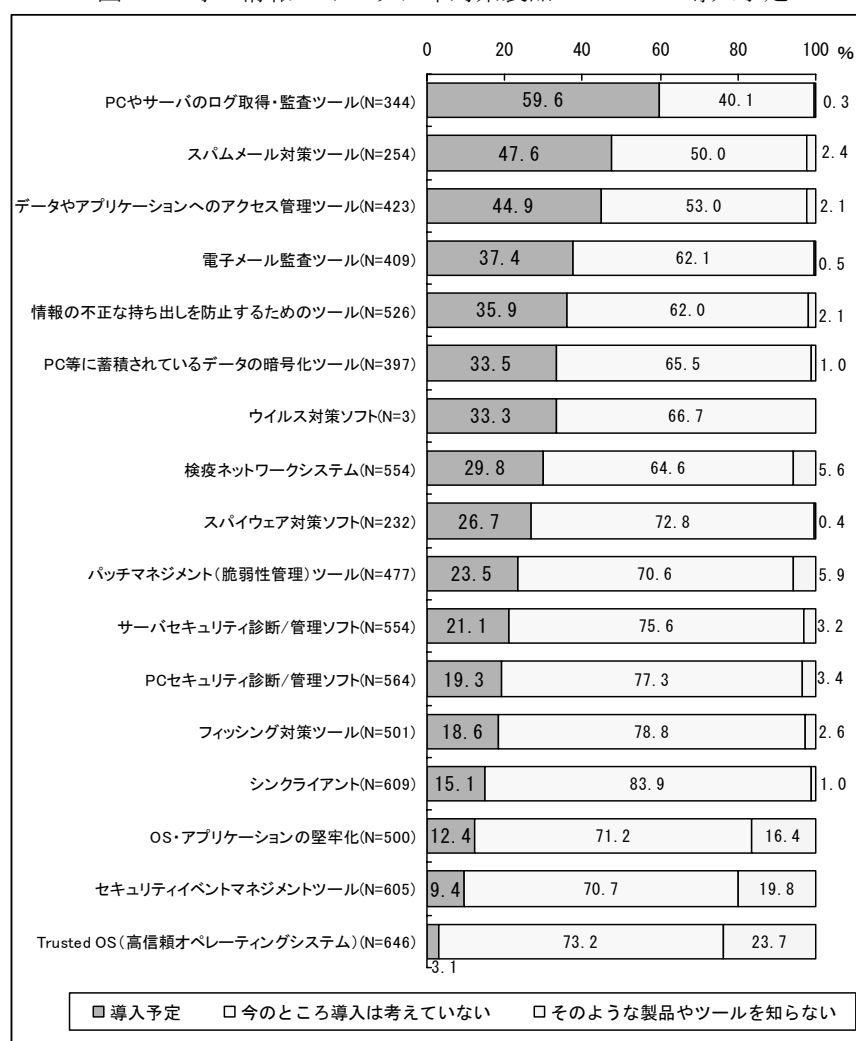
「企業における情報セキュリティ実態調査2007」公開ページ

http://www.nri-secure.co.jp/news/2007/1129_report.html

詳細な分析レポートをご覧になりたい場合は、上記の公開ページからお申し込みいただけます。NRIセキュアは、今後もこれらの調査結果の公表を通して、広く社会の情報セキュリティ意識の向上を支援してまいります。

また、今後導入を予定しているPC等のセキュリティ対策製品・ツール【図2】を尋ねたところ、「PCやサーバのログ取得・監査ツール」を選択する割合(59.6%)が最も高くなった。同法で求められる内部統制の運用面を視野に入れた動向と考えられる。

図2 PC等の情報セキュリティ対策製品・ツールの導入予定

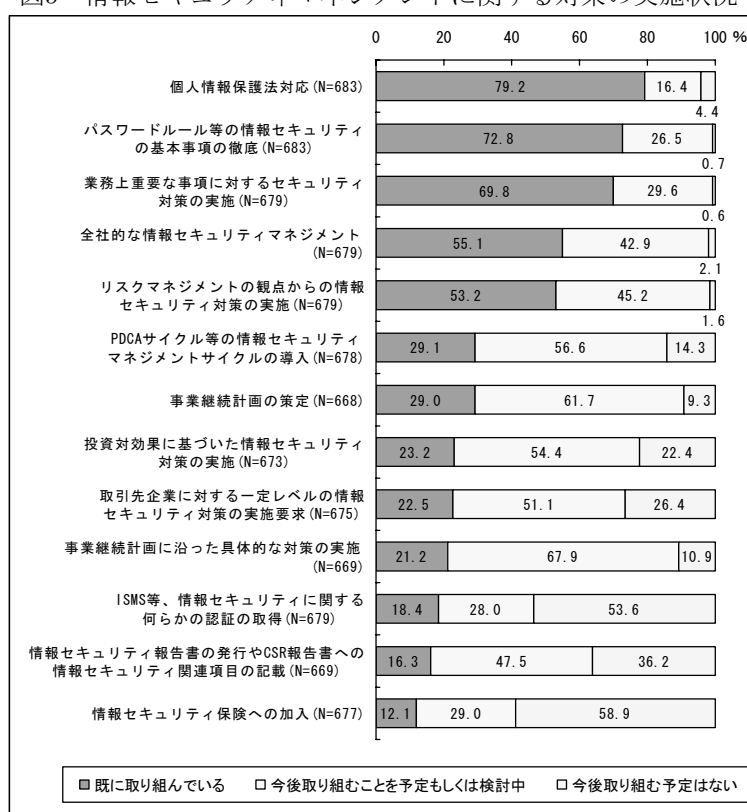


2) 情報セキュリティマネジメントに関する対策の実施状況

情報セキュリティマネジメントに関する対策については、「個人情報保護法対応」(79.2%)を実施している企業の割合が最も高く、「パスワードルール等の情報セキュリティの基本事項の徹底」(72.8%)の割合が次いで高くなっている。また、今後取り組むことを予定もしくは検討中の対策としては、「事業継続計画に沿った具体的な対策の実施」(67.9%)を選ぶ企業の割合が最も高く、「事業継続計画の策定」(61.7%)が次いで高くなっている。

る。法対応やパスワードルールの徹底といった基本的な対策が浸透し、事業継続計画に関わる対策に関心が動きつつある状況がうかがえる。「PDCAサイクル等の情報セキュリティマネジメントサイクルの導入」(29.1%)はあまり普及していない状況だが、情報セキュリティマネジメントに関わる対策の実施は、一過性ではなくマネジメントサイクルに沿って継続的に実施されることが望まれる。

図3 情報セキュリティマネジメントに関する対策の実施状況



3) 具体的な情報セキュリティ対策の実施状況

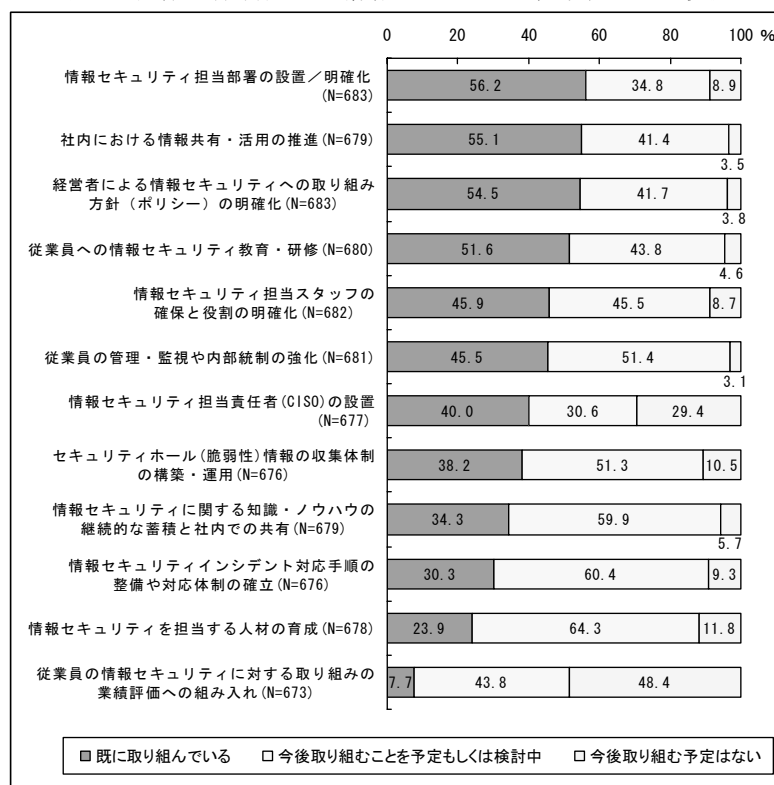
以下では具体的な情報セキュリティ対策の実施状況を、組織・体制面での対策と技術的な対策に分けて述べる。

(1) 組織・体制面での情報セキュリティ対策

「情報セキュリティ担当部署の設置／明確化」(56.2%)を実施している企業の割合が最も高く、「社内における情報共有・活用の推進」(55.1%)が次いで高くなっている。

今後取り組むことを予定、もしくは検討中の対策としては、「情報セキュリティを担当する人材の育成」(64.3%)を選ぶ企業の割合が最も高くなっている。担当部署の設置など対策を実施する仕組みは整いつつあるが、それを運用する人材の供給が追いついていない状況がわかる。

図4 組織・体制面での情報セキュリティ対策の実施状況

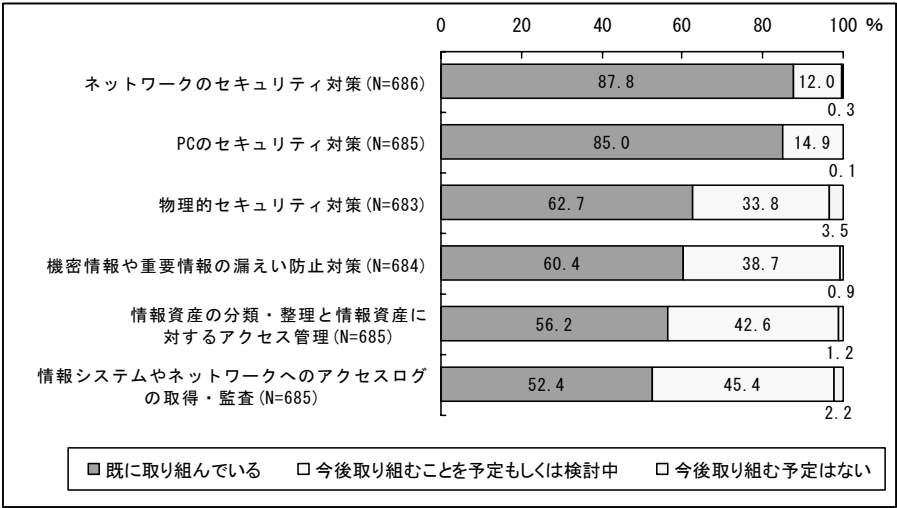


(2) 技術的な情報セキュリティ対策の実施状況

「ネットワークのセキュリティ対策」(87.8%)を実施している企業の割合が最も高く、「PCのセキュリティ対策」(85.0%)の割合が次いで高くなっている。また、今後取り組むことを予定もしくは検討中の対策としては、「情報システムやネットワークへのアクセスログの取得・監査」(45.4%)を選ぶ企業の割合が最も高く、「情報資産の分類・整理と情報資産に対するアクセス管理」(42.6%)が次いで高くなっている。金融商品取引法(日本版SOX法)で求められる内部監査の運用を見すえた傾向と考えられる。

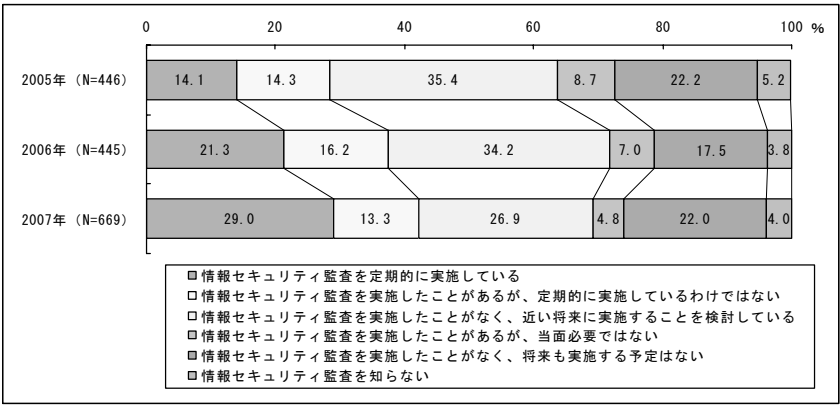
技術的な対策は、前出のマネジメントに関する対策や、組織・体制面での対策と比べて「今後取り組む予定はない」に回答する企業の割合が非常に低いという特徴も見られる。

図5 技術的な情報セキュリティ対策の実施状況



4) 情報セキュリティ監査の現状

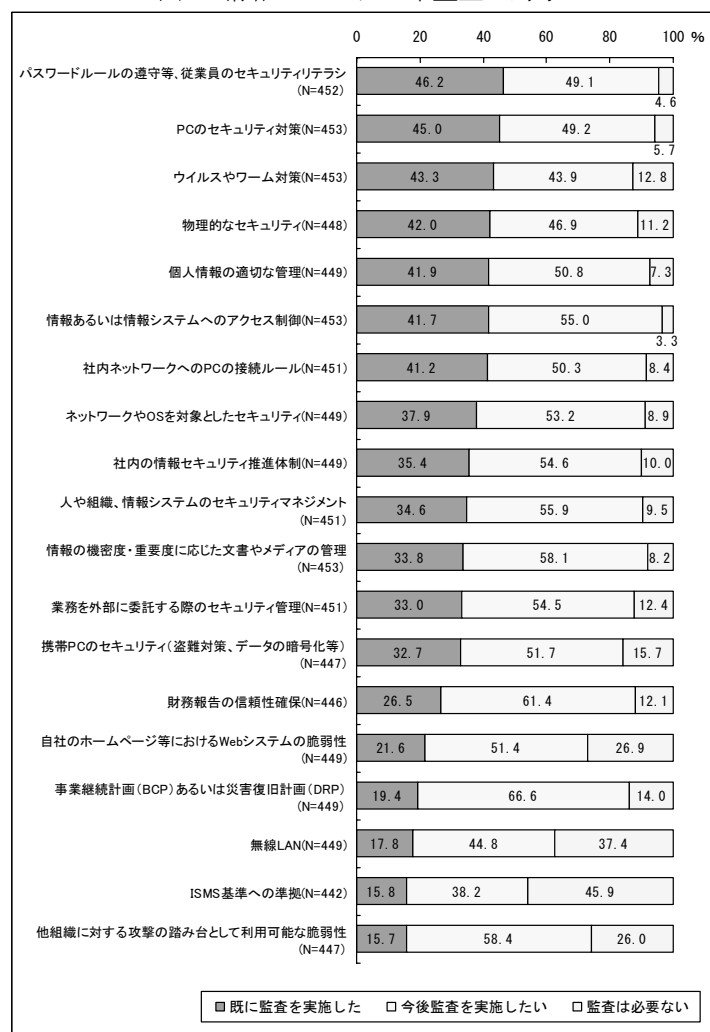
情報セキュリティ監査^{※1}を定期的の実施している企業は年々増加しており、2007年度は回答企業全体の29.0%であった。業種では銀行・証券・保険等(62.9%)、通信・情報処理・メディア等(61.6%)の回答率が高くなっている。



※1 情報セキュリティ監査：社内の独立した監査担当組織または社外の専門家によるチェック、評価を指す。自部門を自部門自らでチェック、評価する活動は含まない。

実施した監査の対象※²は、「パスワードルールの遵守等、従業員のセキュリティリテラシ」（46.2%）の割合が最も高い。また、今後監査を実施したい対象は「事業継続計画（BCP）あるいは災害復旧計画（DRP）」（66.6%）の割合が最も高くなっている。

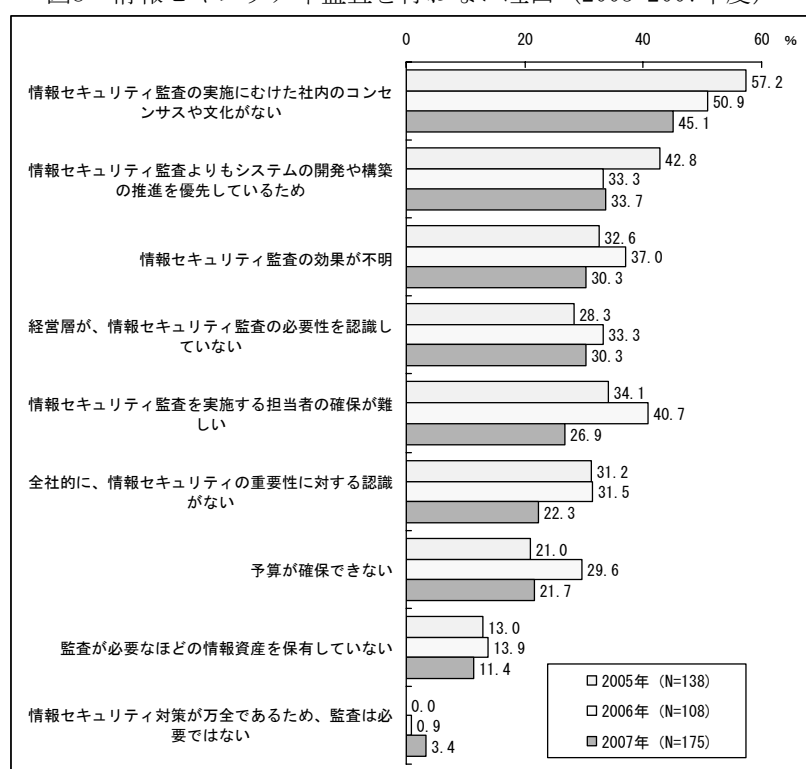
図7 情報セキュリティ監査の対象



※²「情報セキュリティ監査を定期的の実施している」「情報セキュリティ監査を実施したことがあるが、定期的の実施しているわけではない」「情報セキュリティ監査を実施したことがなく、近い将来に実施することを検討している」「今後監査を実施したい」「監査は必要ない」のどこかに回答）のいずれかに回答した企業からの回答

監査を行わない理由^{※3}については、「情報セキュリティ監査の実施にむけた社内のコンセンサスや文化がない」（45.1%、2006年度）の割合が最も高いが、その割合は年々低下しており、徐々に情報セキュリティ監査を行う文化が企業内に根付いてきていると受け取ることができる。

図8 情報セキュリティ監査を行わない理由（2005-2007年度）

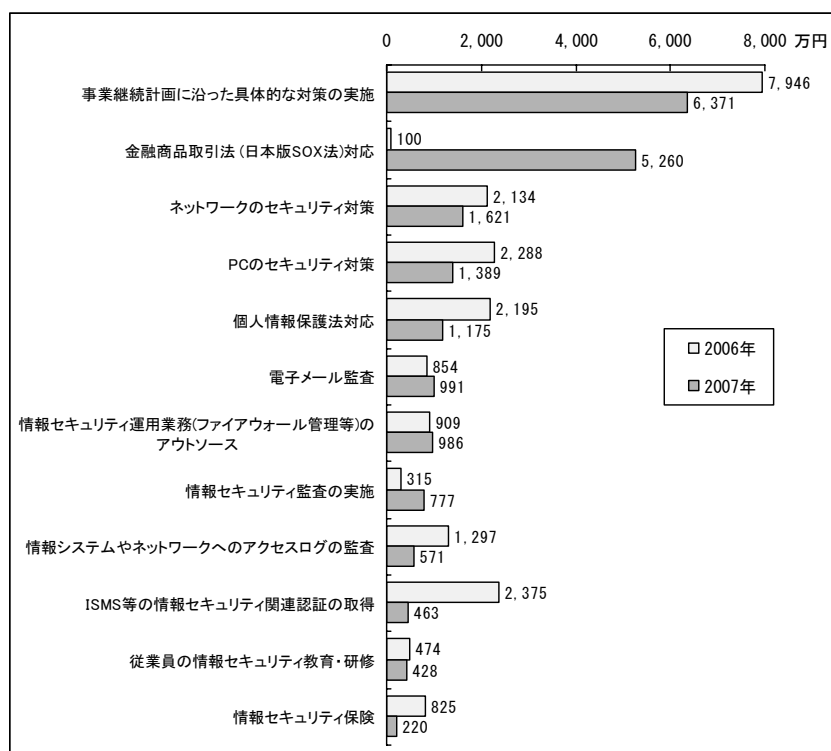


5) 情報セキュリティ関連投資の現状

2007年度の情報セキュリティ関連投資額（およその見込み額）を対象別に平均値で見ると、「事業継続計画に沿った具体的な対策の実施」（6,371万円）が最も高く、「金融商品取引法（日本版SOX法）対応」（5,260万円）が次いで高くなっている。

2006年度との比較では多くの対象で投資額の減少傾向が見られる中、「金融商品取引法（日本版SOX法）対応」への投資額は突出した伸び（前年度比52.6倍）を見せている。また、それに関連する「情報セキュリティ監査の実施」（同2.47倍）や「電子メール監査」（同1.16倍）などへの投資にも注力している様子がうかがえる。

※3 「情報セキュリティ監査を実施したことがあるが、当面必要ではない」「情報セキュリティ監査を実施したことがなく、将来も実施する予定はない」と回答した企業からの回答

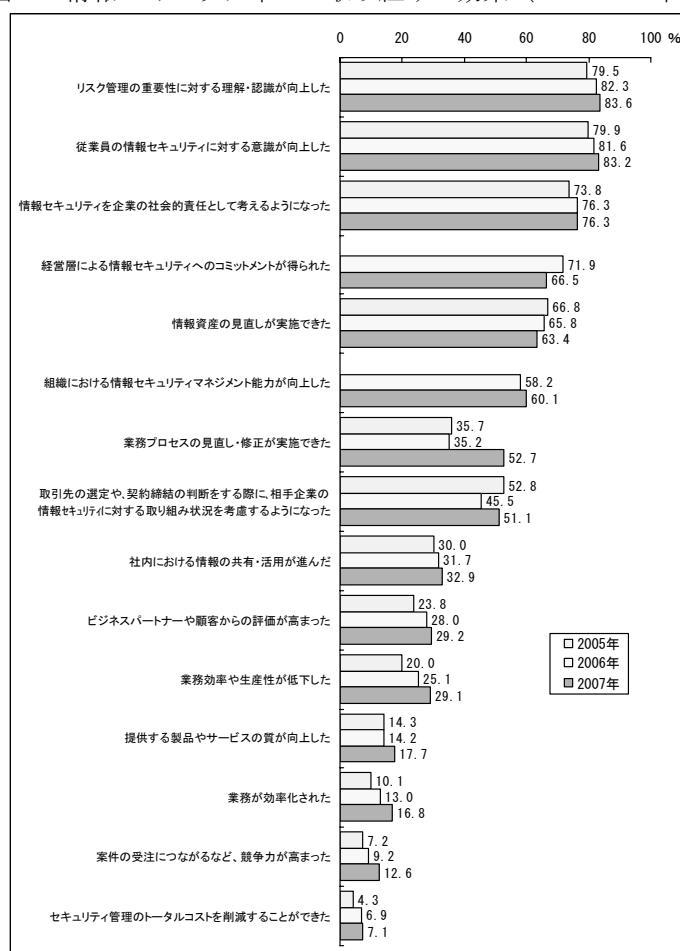


6) 情報セキュリティへの取り組みの効果

情報セキュリティへの取り組みを実施したことによる効果は「リスク管理の重要性に対する理解・認識が向上した」(83.6%)を選んだ企業の割合が最も高く、「従業員の情報セキュリティに対する意識が向上した」(83.2%)の割合が次いで高くなっている。どちらもわずかではあるが年々上昇傾向にある。

「業務プロセスの見直し・修正が実施できた」(52.7%)の割合は、2006年度(35.2%)から約1.5倍に増えている。日本版SOX法で求められる内部統制に連動した顕著な傾向と考えられる。

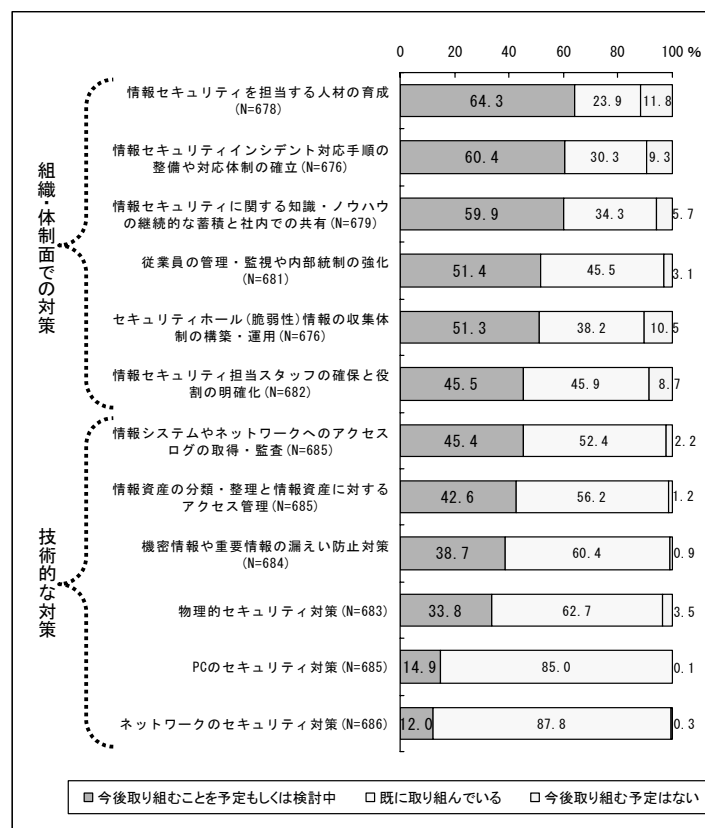
図10 情報セキュリティへの取り組みの効果（2005-2007年度）



2. 情報セキュリティに対する取り組みの展望

1) 今後取り組む予定の情報セキュリティ対策

今後取り組むことを予定もしくは検討している具体的な対策では、「情報セキュリティを担当する人材の育成」(64.3%)をはじめとする組織・体制面のいくつかの対策の回答率が、各種技術的な対策の回答率を上回っている。技術的な対策については、「既に取り組んでいる」という回答率が高く、技術的対策の一巡後に、人材育成等の組織・体制面の対策が後続していく今後の傾向が見える。

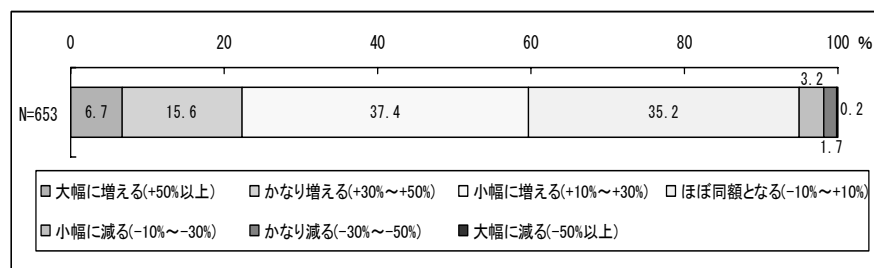


(注) 組織・体制面での対策には上記以外にも対策があるが、技術的な各種対策との関係を簡便に示すため割愛している。

2) 情報セキュリティ関連投資の見通し

情報セキュリティ関連投資の2006年度と比較した2007年度の見通しは、2006年度よりも同額以上に増えると回答する企業の割合^{※4}が全体の9割以上を占めており、旺盛な投資意欲が伺える。

図12 情報セキュリティ関連投資の見通し (2006年度との比較)



※4 上記グラフの凡例「大幅に増える」「かなり増える」「小幅に増える」「ほぼ同額となる」の4つを合算した割合。

3. 情報セキュリティ関連の新たな仕組みへの関心

以下では情報セキュリティ関連の新たな仕組みとして注目される「情報セキュリティ格付け制度」と「CSIRT」について、それぞれ国内主要企業がどのように受け止めているかについて述べる。

1) 情報セキュリティ格付け制度^{※5}

「情報セキュリティ格付け制度」を名称程度まで知っている企業の割合は44.4%と、まだ実施されていない制度にも関わらず高い割合であり、この制度への関心の高さがうかがえる。

また、格付けの取得については、3割以上の企業が検討する意向を示した。理由としては「自社内の各組織のセキュリティレベルを知りたい」（意向を示した企業の58.3%）、「対外的（委託元や取引先等）に自社のセキュリティレベルをアピールしたい」（同45.6%）を選ぶ企業の回答率が高かった。

図13 情報セキュリティ格付け制度の認知度

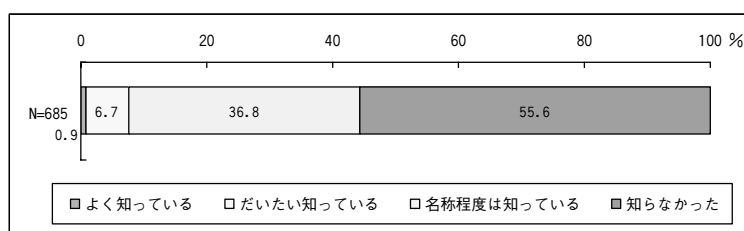
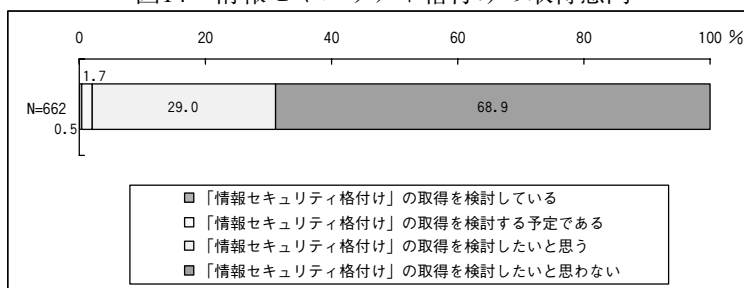
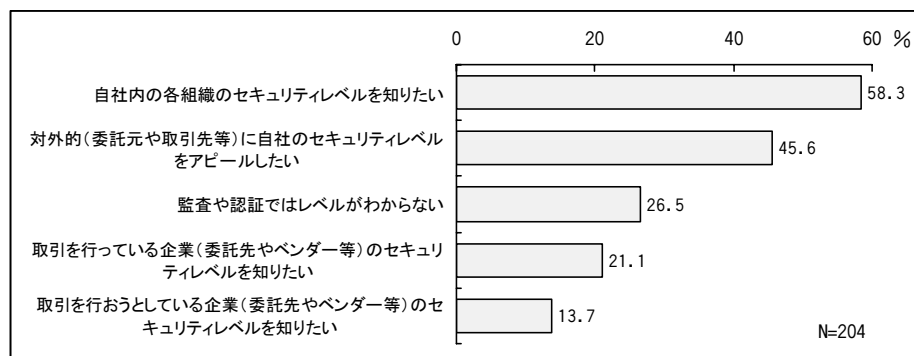


図14 情報セキュリティ格付けの取得意向



※5 「情報セキュリティ格付け制度」とは：わが国の情報セキュリティ・ガバナンス向上を目指し、情報セキュリティ対策の成熟度合いによって企業を格付けする制度。情報セキュリティ対策の進捗度合いやコンプライアンスへの取り組み状況等によって、企業に財やサービスなどの商取引指標となる格付けを行う。2007年7月、NTTコミュニケーションズ、松下電器産業、富士ゼロックス、格付投資情報センターの4社が、情報セキュリティ格付けの共同事業化に向けて「情報セキュリティ格付け制度研究会」を設置。2008年4月にも第三者機関を立ち上げ、事業が開始される予定。（弊社は、野村総合研究所と共に、同研究会に参画しています。）

図15 情報セキュリティ格付けの取得を検討したいと思う理由

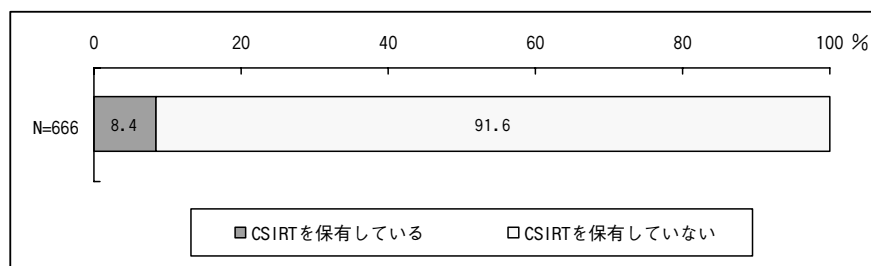


2) CSIRT ※6

CSIRTを現在保有している企業は全体で8.4%となっている。業種では「通信・情報処理・メディア等」(22.1%)の割合が最も高く、「銀行・証券・保険等」(14.3%)が続いている。コンピュータを多用する業種での保有率が高い傾向を示している。

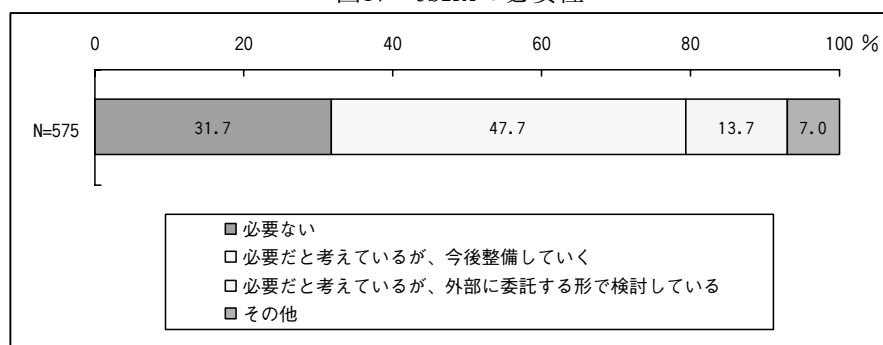
また、CSIRTを保有していない企業におけるCSIRTに対する考え方は、「必要だと考えるが、今後整備していく」が保有していない企業の47.7%、「必要だと考えるが、外部に委託する形で検討している」が同じく13.7%となっている。CSIRTの必要性は認識され、今後整備が進む方向にある。内製化する傾向ではあるが外部委託を検討している比率も低くはない。

図16 CSIRTの保有状況



※6 CSIRT (Computer Security Incident Response Team)：コンピュータセキュリティに関するインシデントが発生した場合に対策する専門チーム

図17 CSIRTの必要性



まとめ

国内主要企業における情報セキュリティ対策の現状としては、全体の約7割が日本版SOX法に対応中であることが特筆できる。2006年度との比較では、実施率で約50ポイント、投資額では52.6倍の上昇という際立った傾向が見られた。また、今後については、技術的対策が一巡した後に情報セキュリティ担当者の育成など組織・体制面の対策が後続していくと考えられる潜在的なトレンドが明らかとなった。旺盛な情報セキュリティ関連投資への意欲も確認され、「情報セキュリティ格付け制度」など新たな仕組みへの関心も高かった。国内企業全体が日本版SOX法対応を原動力として、情報セキュリティ対策をより一層強固にしていくことを期待したい。

最後になってしまったが、今回の調査にご協力頂いた多くの企業の方々に深く感謝するとともに、本稿が主要企業のみならず、情報セキュリティの次の一手を模索している多くの企業や団体の一助となることを願っている。