

「IT セキュリティに関するアンケート」 結果サマリー

このたびは「IT セキュリティに関するアンケート」にご協力いただきまして誠にありがとうございました。皆様のおかげを持ちまして調査は無事終了いたしました。

簡単ではございますが、結果のサマリーをご報告させていただきます。本調査結果が、貴社の IT セキュリティ対策を考える際のお役に立てば幸いです。

また、弊社ホームページ (<http://www.nikkei-r.co.jp>) にて、来月以降、他の調査も含めた結果をいくつかご紹介していく予定ですので、ご関心がございましたらご参照いただければ幸いです。

今後とも、調査実施の折にはご協力賜りますようお願い申し上げます。

2006 年 6 月

株式会社日経リサーチ

〒101-0048 東京都千代田区神田司町 2-2-7
パークサイド1ビル

TEL: 03-5296-5151 (担当: 渡辺(泰) 熊谷)
調査 No. 06-411-0040

【今回調査の実施概要】

- ・ 調査目的: 企業の IT セキュリティへの取り組み、課題等の現状と今後の動向を把握することを目的とする。
- ・ 調査対象: 企業の情報システムに関するセキュリティの管理・業務をされている方
- ・ 調査方法: 質問紙郵送法
- ・ サンプルング方法: 弊社企業データベースより企業規模ごとに層化し、各層内で無作為抽出
- ・ サンプル数: 回収 1,038 社
本結果サマリーでは、このうち社内ネットワークを構築し、サーバを導入されているとお答えの企業 701 社についての結果をご紹介します。
- ・ 調査実施時期: 2006 年 4 月 14 日 ~ 4 月 28 日
- ・ 調査地域: 全国
- ・ 調査実施: 株式会社日経リサーチ

企業・個人を問わず、従来にも増して、ITセキュリティに関する対策が重要性を増してきています。企業活動に関しても、昨年4月の個人情報保護法の完全施行にともなう様々な対応が要請される一方、相次ぐ個人情報の流出事件、機密情報漏洩事件など社会的な関心は高まるばかりです。

例えば、独立行政法人情報処理推進機構(IPA)発行の『情報セキュリティ白書 2006年版』では「2005年の10大脅威」として、

- 第1位 事件化するSQLインジェクション
- 第2位 Winny を通じたウイルス感染による情報漏えいの多発
- 第3位 音楽CDに格納された「ルートキットに類似した機能」の事件化
- 第4位 悪質化するフィッシング詐欺
- 第5位 巧妙化するスパイウェア
- 第6位 流行が続くボット
- 第7位 ウェブサイトを狙うCSRFの流行
- 第8位 情報家電、携帯機器などの組み込みソフトウェアにひそむ脆弱性
- 第9位 セキュリティ製品の持つ脆弱性
- 第10位 ゼロデイ攻撃

を挙げています。

このようにセキュリティに対する課題が山積する中、適切なセキュリティ対策を講じていることは、リスクを回避するのみならず、企業の信頼度を高めることにもつながります。

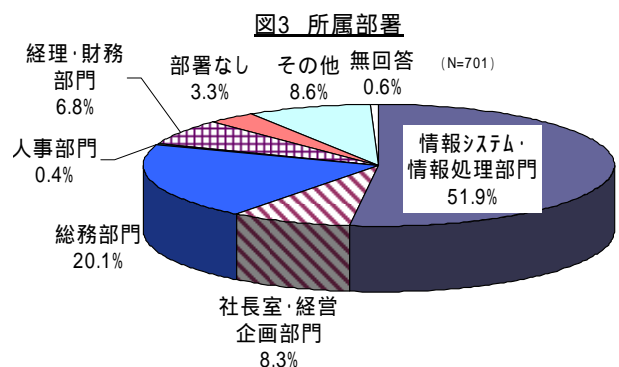
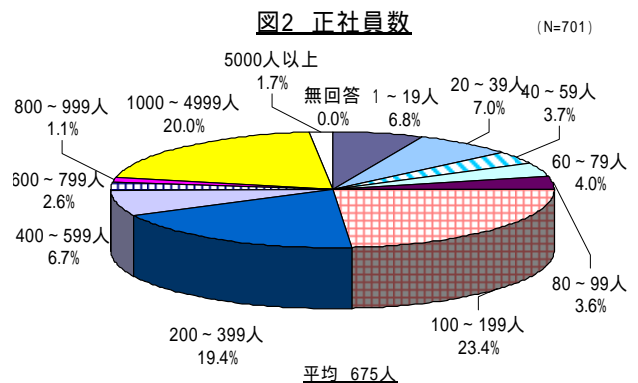
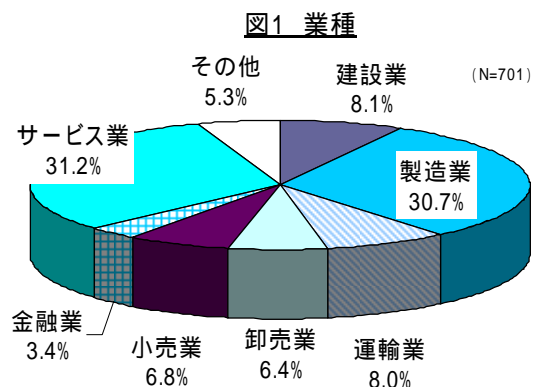
とはいえ、現実には様々な制約がある中で、思うとおりに対策を進めることは、なかなか困難なこともあります。実際に企業でのITセキュリティでの取り組みは現段階でどうなっているのか、簡単ではありますが調査結果のデータからご紹介したいと思います。

回答企業の属性

まず、調査にご協力いただきました企業の概要を確認しておきましょう。

今回調査では、多くの業種の企業のご担当者様よりご回答をいただきましたが、「サービス業」(31.2%)、「製造業」(30.7%)、「建設業」(8.1%)、「運輸業」(8.0%)の順で多い結果となりました。製造業が3割(215社)に対し、非製造業が7割(486社)でした。(図1参照)

正社員数は、99人以下の企業が25.1%、100~999人の中規模企業が今回の回答企業では最も多く53.2%、そして大規模の1000人以上が21.7%でした。(図2参照)

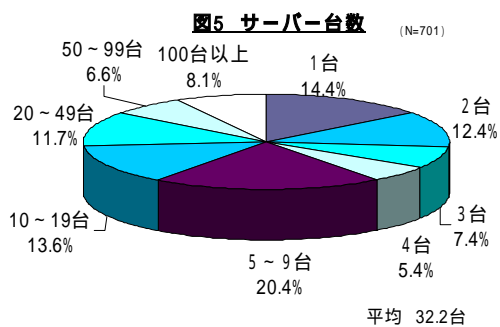
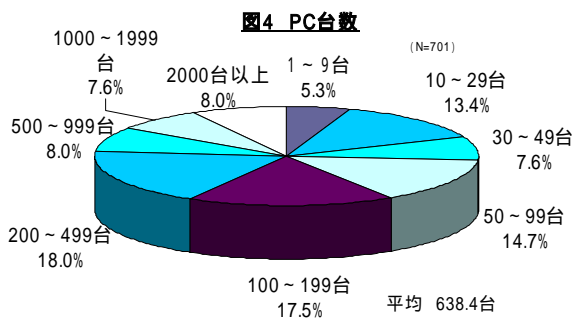


ご回答いただいた方のご所属部門を見ると、「情報システム・情報処理部門」の方が過半数、それ以外の部門の方が半数弱となっています。それ以外の部門の内訳は「総務部門」などをはじめ、社全体の管理部門が多くなっています。これは特に社員数の少ない企業を中心に、ITセキュリティ管理もこれらの部門にご所属の方が担当されていらっしゃるケースも多いためです。(前ページ図3参照)

つづいてIT環境について、PC導入台数とサーバ導入台数を見ておきましょう。

PC導入台数は、「200～499台」が最も多く18.0%、続いて「100～199台」が17.5%と続きますが、前ページで社員数の分布を見ましたように、今回の調査では多様な企業からお答えをいただくことができましたので、台数の分布も幅広くなっています。(図4参照)

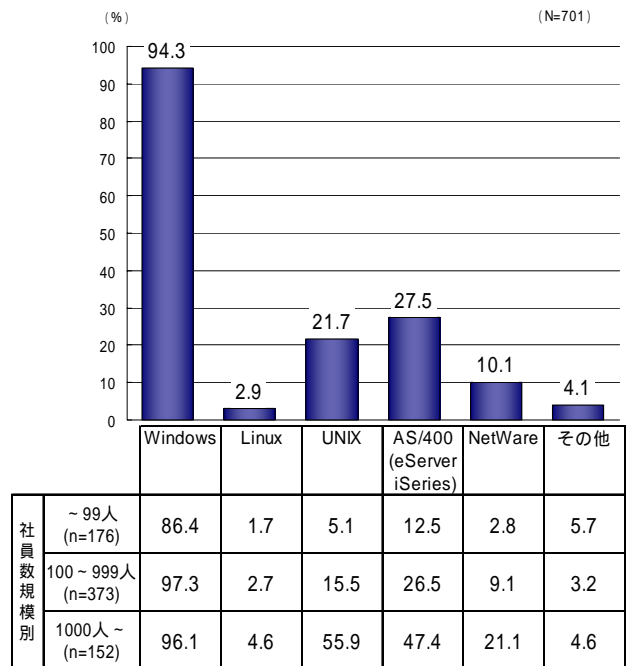
サーバ導入台数は、「5～9台」が最も多く20.4%、続いて「1台」で14.4%と続きます。10台未満の企業が6割を占めています。(図5参照)



Windowsサーバが利用のメイン、大企業はUNIX、eServer iSeriesの使用比率も高い

導入しているサーバOSの種類を聞いたところ、先頃Windows Server 2003 R2もリリースされたマイクロソフト社の「Windows」系のサーバOSが94.3%と圧倒的に高い導入率でした。次に、IBM社の「eServer iSeries (AS/400)」が27.5%、さらに「UNIX」系が21.7%と続きます。社員数規模が1000人以上の企業は、「UNIX」や「eServer iSeries (AS/400)」と「Windows」の併用率が高いことが顕著にあらわれています。(図6参照)

図6 導入しているサーバOSの種類

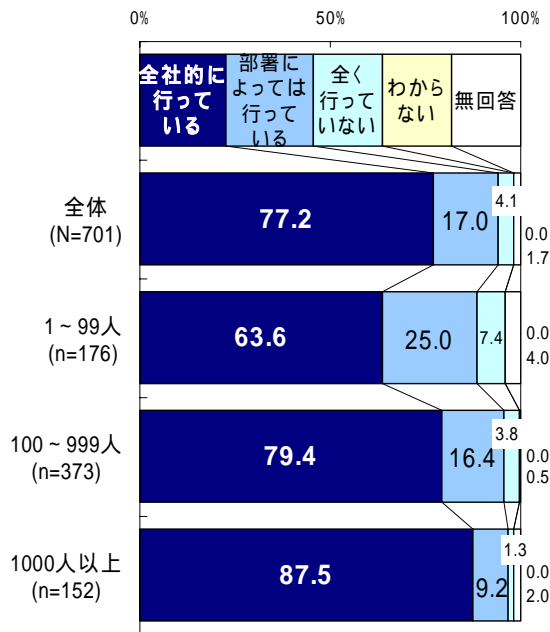


セキュリティ対策の強化は順調に進んでいかないという課題も

現状の情報セキュリティ対策の取り組み状況は、「全社的に行っている」が77.2%と大多数を占めます。「部署によっては行っている」(17.0%)も合わせると、94.2%の企業が何らかのセキュリティ対策を講じていることになります。(次ページ図7参照)

社員数規模別で見ると、規模が大きくなるほど全社的な取り組みを行っている割合が高くなり、1000人以上規模企業では、87.5%と大多数が取り組んでいることがわかります。

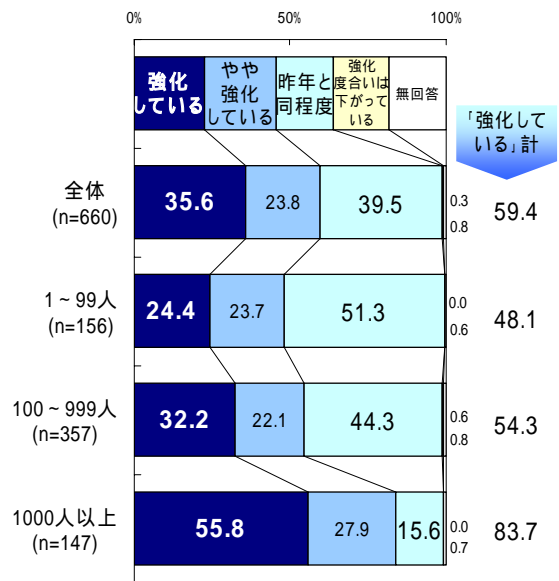
図7 情報セキュリティ対策状況



さて、セキュリティ対策を講じている企業は、昨年と比較して強化度合いは高まったのでしょうか。全体では「強化している」(35.6%)、「やや強化している」(23.8%)を合わせると 59.4%の企業が強化をしたと回答しています。一方、強化度合いが下がっている企業はほとんど見られませんが、「昨年と同程度」という企業も全体の4割ほどとなっており、特段の強化はしていないという企業も一定の割合になっています。(図8参照)

社員数規模別に見てみると、1000人以上規模の企業では、「強化している」割合が 55.8%と特に高いスコアを示し、「やや強化している」を合わせると 83.7%もの企業が強化していることがわかります。特に大企業にとっては、セキュリティ対策の整備は重要な課題と位置づけられているようです。

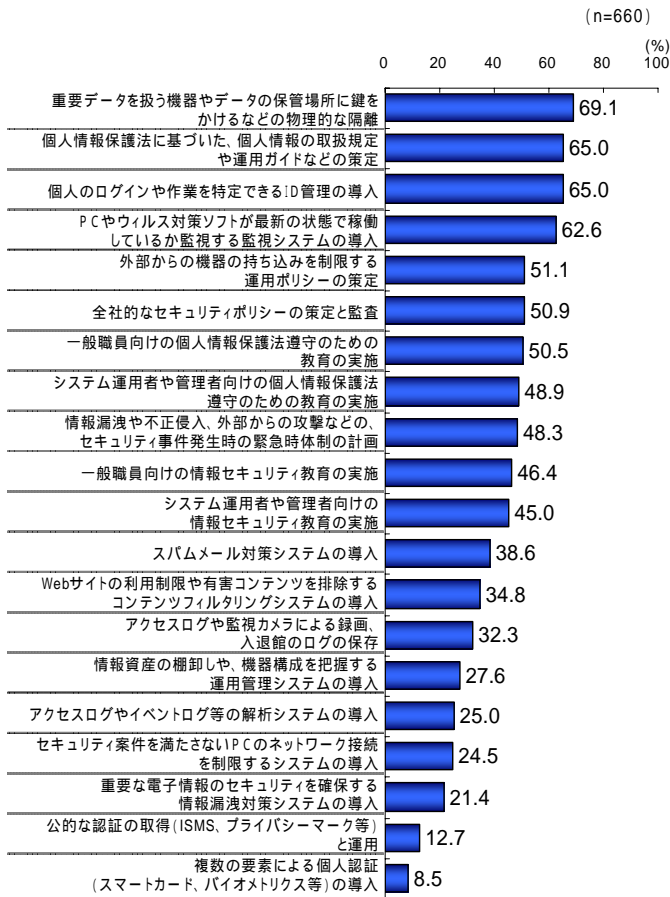
図8 セキュリティ対策の強化度合い



現状の項目別対策状況～セキュリティポリシー面は順次対策が進められているが、技術面の取り組みはまだ多くの課題を残している

それでは、セキュリティ対策を講じている企業は、具体的にどのような対策を導入・実施しているのでしょうか。「重要データを扱う機器やデータの保管場所に鍵をかけるなどの物理的な隔離」(69.1%)、「個人情報保護法に基づいた、個人情報の取り扱い規定や運用ガイドなどの策定」(65.0%)、「個人のログインや作業を特定できる ID 管理の導入」(65.0%)、「PC やウイルス対策ソフトが最新の状態で稼働しているか監視する監視システムの導入」(62.6%)といった項目については、既に取り組みが進んでおり、6割を超える企業が実施しています。その他にも、「外部からの機器の持ち込みを制限する運用ポリシーの策定」(51.1%)や「全社的なセキュリティポリシーの策定と監査」(50.9%)が半数以上の企業が実施しているなど、各種ポリシー策定については導入が進んでいます。(次ページ図9参照)

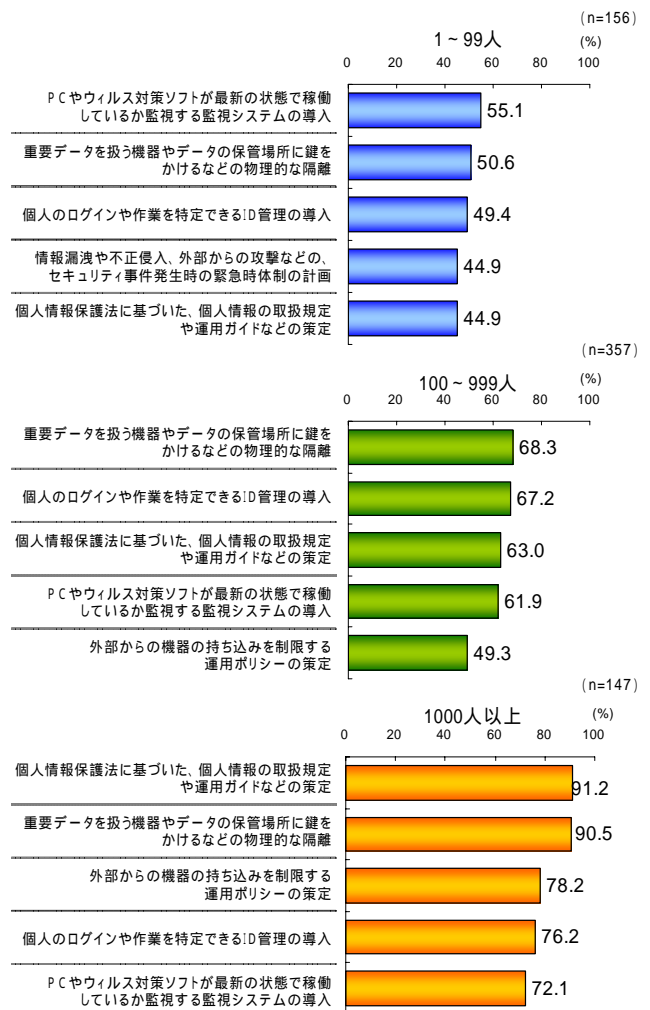
図9 セキュリティ対策の具体的導入・実施内容



続いて、社員数規模別に、導入・実施率が高いものから上位5つまでを示したのが図10です。社員数規模が大きい企業ほど、各項目の導入率が全体的に高いことがわかります。

社員数1000人以上規模の企業は、「個人情報保護法に基づいた、個人情報の取り扱い規定や運用ガイドなどの策定」(91.2%)、「重要データを扱う機器やデータの保管場所に鍵をかけるなどの物理的な隔離」(90.5%)は9割を超える企業が実施済みです。また、実施率こそ大規模企業と比べて下がりますが、100~999人規模や1~99人規模の企業でも、上記2項目は上位の導入対策として挙げられています。また、「個人のログインや作業を特定できるID管理の導入」、「PCやウイルス対策ソフトが最新の状態で稼働しているか監視する監視システムの導入」についても、1000人以上規模企業で7割以上の導入率、100~999人規模企業では6割以上、1~99人規模では5割前後の導入率であり、社員数規模に関係なく広く

図10 セキュリティ対策の具体的導入・実施内容(社員数規模別)



採られている技術的な対策であることがわかります。

このように見てきますと、多くの企業でセキュリティの対策を進めていこうというスタンスははっきりしていますし、対策の強化も行われている企業が多くなっています。ただし、社員個人や部署・部門という単位を超え、全社的にポリシーを策定したり、社員へ教育を行ったり、必要なシステムを導入していく部分にはまだまだ道のりが残されているようです。あるいはベーシックな対策には着手していても、さらに高次の対策へは踏み出していないケースもあるようです。

自社にとって採るべき対策は何であるか、その導入・運用のためにはどのような課題をクリアすればいいのか、など、日頃からの情報収集や社内での働きかけなどもますます重要性が高まっていると言えるでしょう。