情報セキュリティの観点から見た内部統制の課題

姫野桂一

CONTENTS

要約

1　2006年は企業における内部統制が大いに注目を集め、IT（情報技術）業界は新会社法や金融商品取引法（いわゆる日本版SOX法）への対応ソリューション（問題解決システム）を活発に提案した。2006年11月には、日本版SOX法の内部統制構築のよりどころとなる「財務報告に係る内部統制の評価及び監査に関する実施基準（公開草案）」が発表された。これを受け、今後、各企業でも日本版SOX法対応の活動が本格化することになる。

2　情報セキュリティから見た内部統制の課題を抽出するために、NRIセキュアテクノロジーズでは独自の調査研究を行った。その結果、情報セキュリティ対策において、技術的対策は万全であっても、社員の情報セキュリティ教育などでは不安を抱えている企業が多いことが浮き彫りになった。また、社内にルールを設けていても、それを遵守していない社員が存在することも明らかになった。

3　IT全般統制を効率的に構築するためには、情報セキュリティの観点に着目することが重要である。社内のコンプライアンス（法令遵守）などの意識改革を浸透させていく活動に、経営層が積極的に関与していくことが、今後ますます重要になっていくものと考えられる。

Ⅰ 情報セキュリティが果たす役割と盲点

2006年は企業における内部統制が大いに注目を集め、IT（情報技術）業界は新会社法や金融商品取引法（以下、日本版SOX法）への対応ソリューション（問題解決システム）を活発に提案した。

2006年11月、金融庁は日本版SOX法の内部統制構築のよりどころとなる「財務報告に係る内部統制の評価及び監査に関する実施基準（公開草案）」（以下、公開草案）を発表した。国民から広くコメントを募集し（パブリックコメント）、それを受けて2007年に正式に実施基準となる。

内部統制とは何か。公開草案の「内部統制の定義（目的）」では、「内部統制とは、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の４つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいい、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）及びIT（情報技術）への対応の６つの基本的要素から構成される」と規定されている。

この定義のなかの「IT（情報技術）への対応」という文言は、日本版SOX法のもととなった米国のSOX法（企業改革法）には明示的でなく、今回の金融庁の実施基準（公開草案）で記載されたことから、ITベンダーの間に新たなビジネスの契機になるという思惑を生み、「内部統制ソリューションブーム」という一種の社会現象を生み出すまでに至っている。

しかし、一口に内部統制といっても、企業経営の観点によって遵守すべき対象が異なり、また、各種の内部統制のソリューションも必ずしも最適化されていない。そのため、現段階では汎用的な事例が少ないという問題がある。そればかりか、このような領域はそもそも費用対効果が見極めにくいことから、多大なシステム投資に見合うような内部統制が本当に効率的に構築できるのかという疑問もある。

こうしたことから、内部統制をいかに効率的かつ実効性のあるものに構築していくべきかという課題に関し、他企業の先進的な取り組みの事例を学びたいという欲求や悩みを抱えている経営層、IT担当者は非常に多いと考えられる。

本稿では、IT全般統制の構築に焦点を当て、その構築に当たって情報セキュリティが果たす役割や盲点について論じてみたい。

特に情報セキュリティに着目するのは、この分野がITの一つのセグメントに過ぎないという認識を持たれることが多く、これまで情報セキュリティの視点に立つ内部統制が、積極的に論じられてこなかったからである。

本稿の構成は、初めに公開草案における内部統制構築に向けての「ITの活用」に関する論点を整理する。そして、一般的に情報セキュリティ分野の範疇と考えられるビジネスソリューション全般について概観したうえで、情報セキュリティの観点から見た内部統制の現状と今後の展開方向について述べていきたい。さらに、企業経営の立場から、情報セキュリティを活用して内部統制を効率的に構築するアプローチや、経営層のコミットの

重要性についても論ずる。

Ⅱ 公開草案に見るIT全般統制のとらえ方

日本版SOX法への対応やIT全般統制に関する情報は、書籍やインターネットなどを通じてこのところ急増している。しかし、IT全般統制の目的や効率的な内部統制の構築法に対する最適解を示す情報は、まだあまり多くないようである。そこで、公開草案のポイントの一つとして、経営層（経営者）の関与がいかに重要であるかや、情報セキュリティと日本版SOX法の内部統制がどのように結びつくかについて論じてみたい。

1 IT全般統制と第三者認証

表１は公開草案の参考資料から、「内部統制に関する評価項目の例」のITへの対応を抜粋したものである。

IT全般統制は、公開草案の他の項目と同様、抽象的な事項で記載されており、具体的な対応は個々の企業に任せるというスタンスをとっている。また、どのような方法で内部統制を構築していくかについても、方針が例示こそされているものの裁量の範囲は広い。そのため、どこから手をつけるべきかという点で戸惑う企業経営者、IT部門担当者もいるだろう。

さらに、IT全般統制をやみくもに実施すると、企業のIT投資負担が過大になることへの配慮もあって、公開草案には「金融商品取引法による内部統制報告制度においては、ITの統制についても、財務報告の信頼性を確保するためのITの統制を整備しようとするものであり、財務報告の信頼性以外の他の目的を達成するためのITの統制の整備及び運用を直接的に求めるものではない」という文言まで記載されている。この背景には、実際に米国の監査法人がSOX法に即した対応を実施した結果、監査対象企業の投資負担が過大になり、運用の見直しを迫られていることがあると推察される。

一方、今日の企業活動において、ITはあらゆる業務プロセスに必要不可欠なものとなっている。このため、内部統制のIT全般統制の対象範囲は広く、内部統制の構築といっても、つかみどころがない。

こうした点については、近代的サービスマネジメントの品質管理手法として、1990年代に注目を集めたISO9001（品質マネジメントシステム）、2001年からJIPDEC（日本情報処理開発協会）によって第三者認証が開始されたISO27001（情報セキュリティマネジメントシステム〈ISMS〉適合性評価制度）、さらに2007年４月から第三者認証が開始されるISO20001（ITサービスマネジメントシステム〈ITSMS〉適合性評価制度）などが、内部統制構築の際の参考となりうる。

その理由として、①ISMSやITSMSなどで

表1　公開草案の「内部統制に関する評価項目の例」（ITへの対応）

- 経営者は、ITに関する適切な戦略、計画等を定めているか。
- 経営者は、内部統制を整備する際に、IT環境を適切に理解し、これを踏まえた方針を明確に示しているか。
- 経営者は、信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及びITを用いた統制の利用領域について、適切に判断しているか。
- ITを用いて統制活動を整備する際には、ITを利用することにより生じる新たなリスクが考慮されているか。
- 経営者は、ITに係る全般統制及びITに係る業務処理統制についての方針及び手続きを適切に定めているか。

注）IT：情報技術
出所）金融庁「財務報告に係る内部統制の評価及び監査に関する実施基準（公開草案）――（参考１）財務報告に係る全社的な内部統制に関する評価項目の例」

実施される変更管理やアクセス管理などは、IT全般統制で必要な対応策と重なる部分があること、②いずれの国際規格もPDCA（計画・実行・評価・改善）サイクルを通じて、組織内部の内部統制が機能していることを第三者機関が認証するため客観性があること――などがあげられる。

すなわち、上記のような第三者認証には、企業のIT全般統制構築のための勘所をつかみやすいというメリットがある。

2　情報セキュリティ管理の重要性

図１は、日本版SOX法における内部統制のフレームワークと、情報セキリティ管理の強化が有効である理由を示したものである。

左側に、日本版SOX法が求めている内部統制構築のフレームワークを示した。

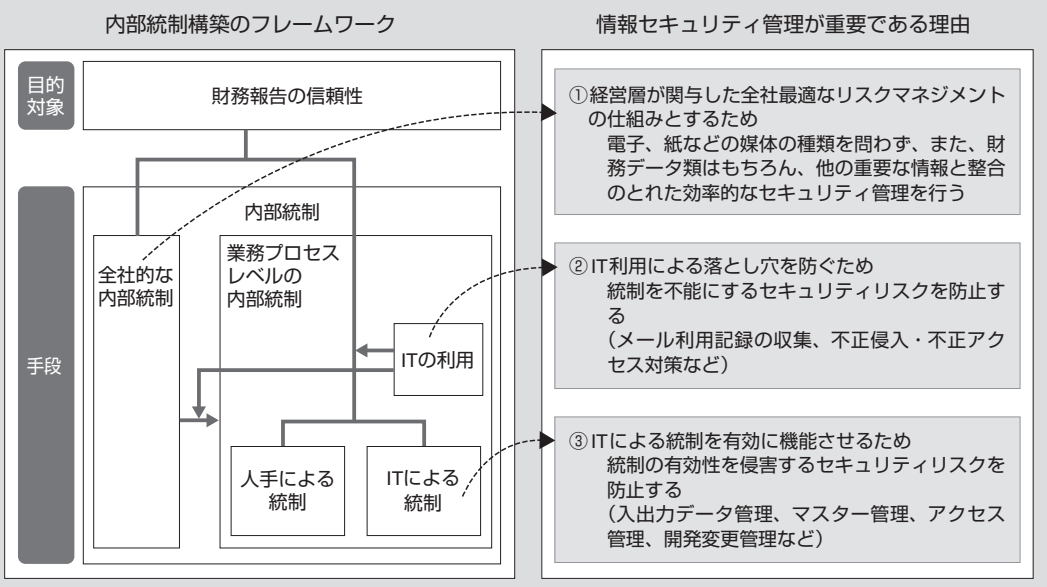
日本版SOX法の目的・対象は財務報告の信頼性の確保にある。そのための手段が内部統制であり、内部統制は、全社的な内部統制と業務プロセスレベルの内部統制とに大別できる。このうち、業務プロセスレベルの内部統制は、人手（マニュアル）による統制、ITの利用、ITによる統制という３つの統制手法が考えられる。

図１の右側では、情報セキュリティの対策が重要である理由を説明しているが、その説明の前に、情報セキュリティ対策の考え方についてあらかじめ述べておきたい。

情報セキュリティ対策は、よくCIAの３要素だといわれる。CIAとは、国際標準化機構（ISO）が定義した情報セキュリティ対策の要素で、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字を略記したものである。すなわち、機密性、完全性、可用性を担保することが情報セキュリティの目的であり、内部統制構築においてもCIAの観点は重要であるといえる。

内部統制構築において情報セキュリティ管理が重要だと考える理由は３つある。①経営層が関与した全社最適なリスクマネジメントの仕組みとするため、②IT利用による落とし穴を防ぐため、③ITによる統制を有効に機能させるため――である。

図1　日本版SOX法で情報セキリティ管理の強化が重要である理由



①は、全社的な内部統制を構築するには経営層の関与が必要不可欠で、そのためには、全社最適なリスクマネジメントを構築することが必要だということである。

②は、メール利用記録の収集や、不正侵入・不正アクセス対策などを行うことにより、統制を不能にするセキュリティリスクを防止するという観点である。

③は、入出力データ管理、マスター管理、アクセス管理、開発変更管理などを講じることで、統制の有効性を侵害するセキュリティリスクを防止するという考え方である。

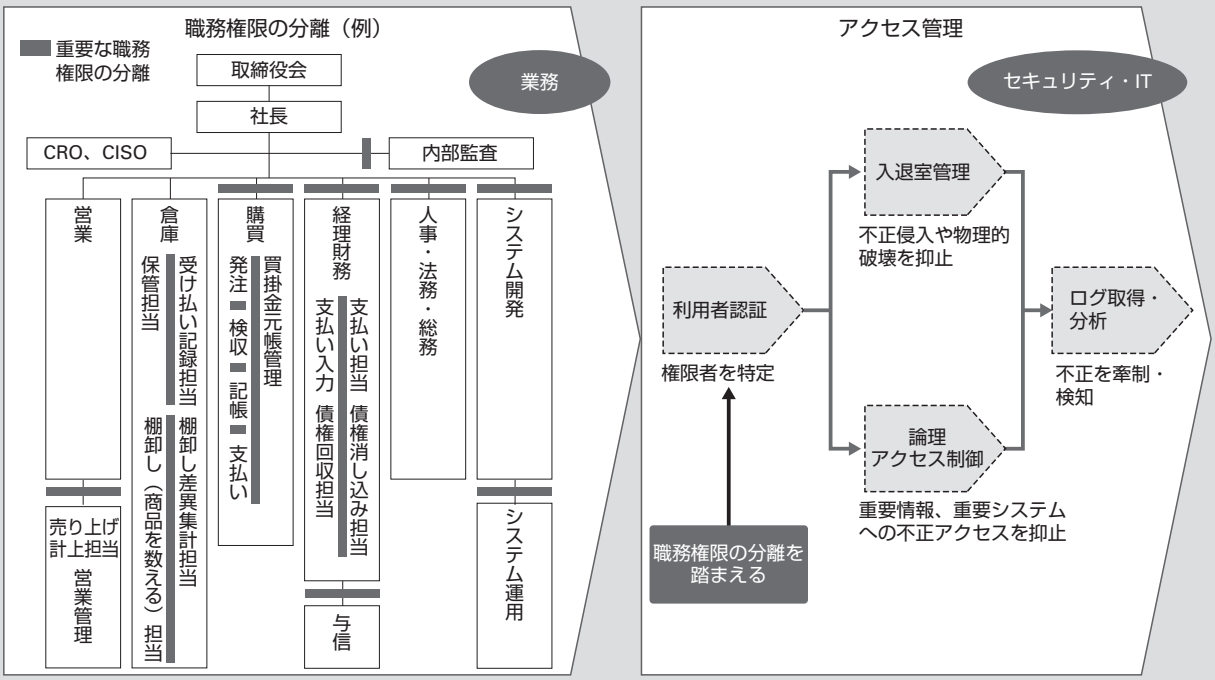
3　アクセス管理の重要性

前述したように、内部統制の構築に当たってはCIAの観点から特に完全性（日本版SOX法の場合は財務情報の完全性）の確保が重要になってくる。完全性を確保するためには、データの改ざんを防ぐことが重要であり、それには職務権限のある人しかデータにアクセスできない仕組みが求められる。この情報の完全性の確保を実現するためには、職務権限の分離とそれを支援するアクセス管理技術が必要となる。

その概念を示したのが図２である。ここではセキュリティ・ITの専門家と業務の専門家が連携して職務権限の分離を実現するアクセス管理構築の流れを示している。

アクセス管理技術は、「利用者認証」「入退室管理」「論理アクセス制御」「ログ取得・分析」などに分けることができる。特に、権限のない人による不正なアクセスやデータ改ざんを防ぐという観点からは、社内において、「Need to Know, Need to Doの原則」（情報を必要な人だけに開示する原則）を遵守することが必要である。すなわち、職務権限を明確に定義し、参照権限や人事異動などに伴う更新権限をシステム上で確実に反映して、情

図2　職務権限の分離を実現するアクセス管理の構築フロー



注）CISO：最高情報セキュリティ責任者、CRO：最高リスク管理責任者

報セキュリティ管理を適切に実施することが重要である。

Ⅲ アンケート調査に見る情報セキュリティ対策の現状と課題

企業が情報セキュリティ対策に本格的に注力するようになったのは、2005年４月に個人情報保護法や、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」の２法を総称したe-文書法が施行されて以降だと考えられる。

NRIセキュアテクノロジーズでは、企業や消費者の情報セキュリティに関する意識調査を経年的に実施している。その調査結果から読み取れるのは、情報セキュリティへの意識の高まりと内部統制構築の機運の高まり（日本版SOX法や2006年５月に施行された新会社法など）がほぼ重なっているということである。この流れは企業経営にとって大きな変化だと考えられる。

以下では、2006年７月に発表（調査は同年５月に実施）した「企業における情報セキュリティ実態調査2006報告書」と、同年11月にビジネスパーソンを対象として実施した「情報セキュリティに関する意識調査」のデータをもとに、IT全般統制についての現状と課題を概観する（表２）。

1 企業における情報セキュリティ対策

次ページの図３は、情報セキュリティに関連する法律や規制への対応状況を見たものである。

このうち「対応済み」という回答が多かったのは、個人情報保護法（81.0％）であり、他の法律や規制についての対応は、現状では必ずしも進展していないことがうかがえる。

この調査時点で、日本版SOX法に「対応済み」という回答はわずか0.9%、「2006年度に対応予定」という回答は16.4%にとどまっている。しかし、2007年度に実施基準が確定すれば、「対応を検討中」と回答した71.8％の企業も、急速に対応が進むと推察される。

次ページの図４は、自社で実施した情報セキュリティ対策への自己評価の結果である。

情報セキュリティ対策に関する自己評価は全般的に、「非常に自信がある」という回答が少ない。「非常に自信がある」「やや自信がある」という回答を合わせた「自信があると回答している層」が半数を超えている

表2　情報セキュリティに関するアンケート調査の概要

「企業における情報セキュリティ実態調査」

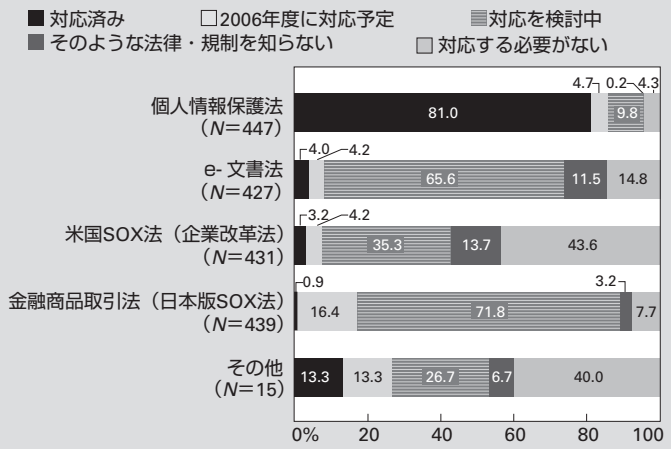
実施期間	2006年5月15日 ～ 5月31日
実施方法	郵送
調査対象	従業員300人以上の企業（東証一部・二部上場および非上場）と東証一部・二部上場の従業員300人未満の企業を中心とする3001社
回答数	449社
回収率	15.0%

「情報セキュリティに関する意識調査」

実施期間	2006年11月17日 ～ 11月21日
実施方法	Webアンケート調査
調査対象	ビジネスパーソン（消費者アンケートの回答から勤め人の属性を抽出した特別集計）
回答数	1266人
調査実施機関	Yahoo!リサーチ

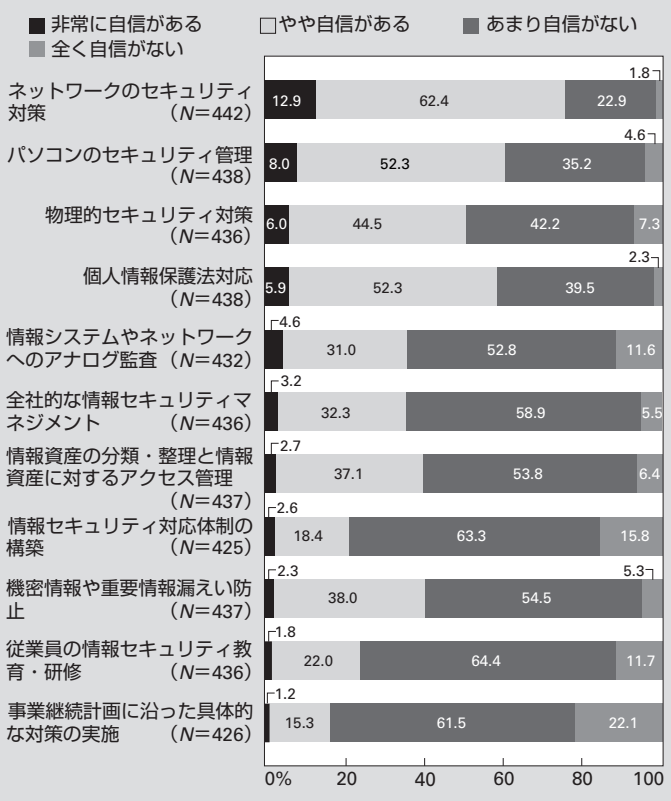
のは、「ネットワークのセキュリティ対策」（75.3％）、「パソコンのセキュリティ対策」（60.3％）、「個人情報保護法対応」（58.2％）、「物理的セキュリティ対策」（50.5％）の４項目に過ぎない。

図3　情報セキュリティに関連する法律や規制への対応状況



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」2006年5月

図4　実施した情報セキュリティ対策に対する自己評価



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査」2006年5月

上記の対策は、入退室管理やネットワーク関連のアプリケーションなど技術的なコントロールによって、情報セキュリティ対策を実施できるものが多いので、一定の効果が期待できる。

一方、「あまり自信がない」「全く自信がない」という回答を合わせた「自信がないと回答している層」では、「事業継続計画に沿った具体的な対策の実施」（83.6％）、「情報セキュリティ対応体制の構築」（79.1％）、「従業員の情報セキュリティ教育・研修」（76.1％）などが上位にある。

以上、IT全般統制を構築していくうえで情報セキュリティ対策が果たす役割の大きさについて述べてきた。企業における情報セキュリティ対策の現状を見ると、技術的な管理は実施されているが、セキュリティ関連の障害や事故からの復旧対策といったインシデント対応、組織マネジメント、人的マネジメント（たとえば、情報セキュリティ対応体制の構築、情報セキュリティ教育）については、自信がないと回答する企業が多い。技術的対策に比べて、これらの対策は時間を要するものだと思われていることがうかがえる。

2　社員の行動から見た情報セキュリティ管理

それでは、内部統制を確立するために、各企業が情報セキュリティ管理規程や、セキュリティに関するルールなどの社内文書を整備していれば、それほど大きな問題が生じないのだろうか。

今回、ビジネスパーソンを対象にアンケート調査を実施したのは、この問題意識が背景にある。企業における情報セキュリティに関

するルールが明文化されているか、仮にルールが存在する場合でも社員がどの程度こうしたルールを遵守しているか、といった実態についてのデータはほとんどなかった。そこで、ビジネスパーソンを対象としたWebアンケート調査を実施して、上記の設問に関する回答を求めた。

その結果、単に社内のルールを整備し、文書化を進めるだけでは、内部統制がきちんと運用できていることの証明にはならないという実態が示された。ここに、内部統制構築の本質的な難しさがあると考えられる。

図５は、「自宅でパソコンを使った仕事の実施状況と企業ルールの遵守状況の関係」についての回答をまとめたものである。この設問では、「自宅でパソコンを使って仕事をすることを禁ずる」というルールがあるにもかかわらず、仕事をしたことがあるという回答が7.4％あった。また、禁止のルールがないため、自宅でパソコンを使って仕事をしたことがあるという回答は30.6％に上った。

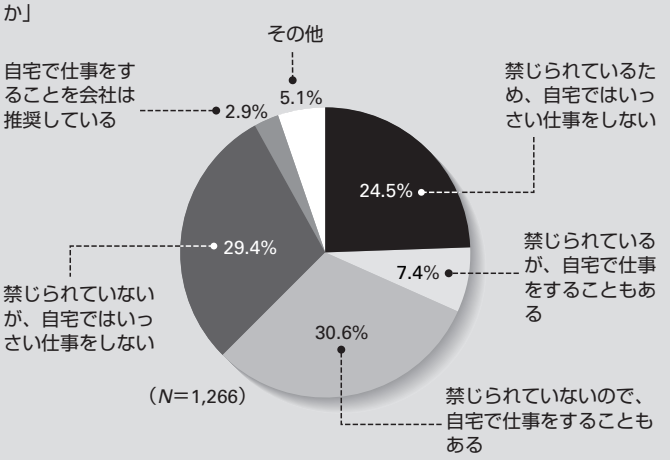
前者の回答は、企業の内部統制の確立という点では、自社の情報漏えいにつながるリスクをはらんでいるため、非常に興味深く、かつ由々しきデータである。

また、後者の回答は、こうしたルールの整備は個別企業の判断にゆだねられるとはいえ、そもそも社内ルールの整備ができていない企業が多く存在していることを物語っている。こうした企業においては、個人所有のパソコンが社内のネットワークに接続されるというリスクがあることを認識すべきである。

図６では、「自宅でパソコンを使って仕事をしたことがある」と回答した人に対して、どのような媒体、手段で仕事を行っているかを聞いている。その結果、自分（自宅）のパソコンが84.4％と最も多く、USB（ユニバーサル・シリアル・バス）メモリーが35.1％、会社のノート型パソコンが17.4％などとなった。特に、USBメモリーの利用が比較的多いことから、企業における情報セキュリティ対策上、こうした媒体に暗号化や指紋認証などのセキュリティ対策機能が実装されていないと、情報漏えいリスクが大きいことが確認さ

図5　自宅でパソコンを使った仕事の実施状況と企業ルールの遵守状況

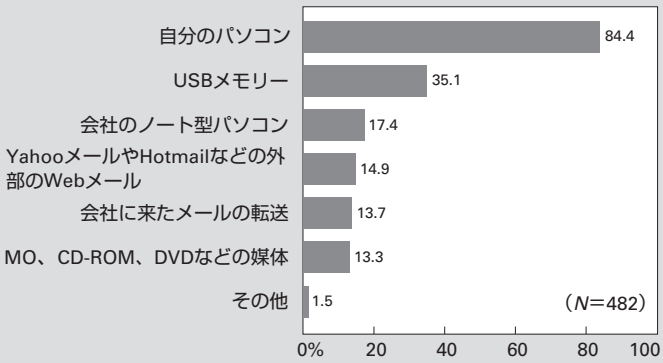
「あなたの会社では、自宅でパソコンを使って仕事をすることを禁じていますか」



出所）NRIセキュアテクノロジーズ「情報セキュリティに関する意識調査」2006年11月

図6　自宅で仕事をするときの利用媒体、手段

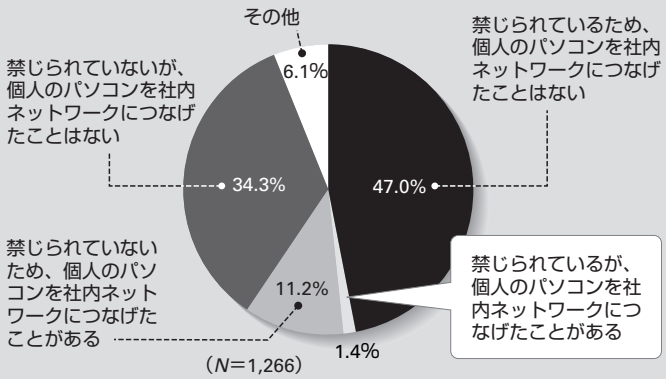
「自宅での仕事にはどのような媒体、手段を利用していますか」（複数回答）



注）CD-ROM：CDを使った読み出し専用外部記憶装置、DVD：デジタル多用途ディスク、MO：光磁気ディスク、USB：ユニバーサル・シリアル・バス
出所）NRIセキュアテクノロジーズ「情報セキュリティに関する意識調査」2006年11月

図7　会社のLANへの接続ルールとその遵守状況

「個人のパソコンを会社のLANにつなげることを禁じていますか」



注）LAN：構内情報通信網
出所）NRIセキュアテクノロジーズ「情報セキュリティに関する意識調査」2006年11月

図8　企業内の情報管理を徹底させる方策

「企業内における情報管理を徹底させるためには、どのような方策が望ましいと思いますか。考えに近いものを5つまで選んでください」（複数回答）

出所）NRIセキュアテクノロジーズ「情報セキュリティに関する意識調査」2006年11月

れた。

図7では、「自社のLAN（構内情報通信網）に自分のノート型パソコンをつなぐことを禁じているにもかかわらず、つないだことがあるか」という設問の結果をまとめたものである。

この設問でも、「禁じられているが、自分のパソコンをつないだことがある」という回答が1.4％あった。ウイルスに感染したパソコンを外部から持ち込み社内ネットワークに接続すると、ネットワーク上の他のパソコンがウイルスに感染したり、情報が漏えいしたりしてしまうリスクが非常に高くなる。社内ネットワークへの不正アクセスを禁じている企業では、ルールを厳格に遵守させるための社員教育を実施することが必要である。

さらに、人為的なミスを極小化するために、技術的対応（たとえば、不正なパソコンをネットワーク上で利用できないようにする、検疫ネットを導入するなど）を図ることが、情報セキュリティ管理から見た内部統制の構築においては重要だといえる。

社内の情報セキュリティのルールが定められているにもかかわらず、社員が社内ルールで禁止されている会社のノート型パソコンを無断で社外へ持ち出して盗難にあったり、企業情報を漏えいしてしまったりする事例は後を絶たない。その点では、社員に対する情報セキュリティ意識の醸成はどの企業にとっても緊急の課題である。

以上、今回のアンケート調査結果から、情報セキュリティから見たIT分野の内部統制の盲点、たとえば、社員を通じての情報漏えいの潜在的なリスクなどが現実に存在することが確認された。

Ⅳ 情報セキュリティを活用した効率的な内部統制の構築に向けて

内部統制の構築は、企業経営の立場からは、法令の遵守や社会的信頼の確保などを目的として実施することが多いが、現場部門の負荷が非常に大きいという問題がある。

日本版SOX法のように、正確な財務情報の遵守が要請される場合は、データの完全性が求められるため、不正な手続きをした場合、いかにその発生を検知し、状況を確認できるかが重要である。

情報セキュリティの観点から内部統制を見た場合、重要なポイントは、前述したように職務権限の分離を支援する機能（たとえばアクセス管理）など、特に完全性の確保に収斂するのではないかと考えられる。

本稿の最後に当たり、「企業内の情報管理を徹底させる方策について」のビジネスパーソンの意識調査のデータを紹介したい（図８）。

「企業内の情報管理を徹底させる方策」としては、「社員の情報セキュリティ教育の実施」（66.3％）、「社内の情報管理ルールの明確化」（58.1％）、「ウイルス対策ソフトやパッチ対策などのネットワークセキュリティの強化」（53.1％）などが上位にある。また、「社内情報のアクセス権限の厳格化」（40.1％）や「会社の経営層の情報セキュリティ管理への参画」（35.4％）などがその後に続く。いずれも、自社の内部統制を適切に構築するためには必要不可欠な項目である。

2007年度は、日本版SOX法への対策が一気に加速すると考えられる。先にも述べたように、公開草案の指針は、自社の実情に合わせてITの利用を図るというスタンスをとっている。日本版SOX法の狙いとする内部統制には、実施した後の評価がある。この評価において、全社的な内部統制の評価が良好であれば、評価対象の事業拠点を絞ったり、評価の負担が軽減されたりすることについても触れている。

全社的なルールの見直し、全社員・関係者の意識改革、全業務への組み込みと仕組み化ができる立場にあるのは経営層だけであるという点からも、自社社員の情報セキュリティ教育や、個人情報や機密情報の漏えいの防止などについて、経営層はしっかりと関与していくことが求められている。

特に、社内ルールを決めてもそれを守らない社員が存在することに関しては、こういった事象を所与の条件として、その対策を盛り込んでいくという発想の転換も必要である。

この意味において、社内の法令遵守などの意識改革を浸透させていく活動や、社員が不正やミスを犯すリスクを低減させるツールの導入（たとえば、検疫ネットや、パソコン本体に記憶・保存装置を持たないシンクライアントなどの導入）についても、経営層が積極的に関与し、自社における内部統制構築への責任を果たすことが、一層求められるようになるだろう。

著者

姫野桂一（ひめのけいいち）
NRIセキュアテクノロジーズ(株)コンサルティング事業部上級セキュリティコンサルタント、 技術士(建設部門、総合技術監理部門)
専門は情報セキュリティ分野の技術評価マネジメント、リスクマネジメント