電子メールの情報漏洩対策の重要性
―電子メールのリスク管理高度化に向けて―

今日、電子メールは企業活動を支える必要不可欠な道具となっているが、電子メールに関わる内部および外部からの情報漏洩などの脅威にいかに備えていくかがきわめて重要な課題として認識されるようになってきている。本稿では、電子メールの情報漏洩対策の現状を概観するとともに、NRIセキュアテクノロジーズのサービスおよびツールについて紹介する。

電子メールを取り巻くリスク

近年、電子メールの利用が拡大するとともに、それにともなうリスクも飛躍的に増大している。電子メールの利用におけるリスクには、添付ファイルを通じたコンピュータウイルス、ワーム、スパイウェアの感染や、スパムメールによる業務効率の低下のほか、最近では金融機関のメールを装って暗証番号やクレジットカード番号などを詐取するフィッシングなどがある。これらは、電子メールにともなういわば外部からの脅威にあたるが、電子メールの中味に含まれる情報の漏洩、すなわち内部からの情報の漏洩も脅威として無視できない。「個人情報の保護に関する法律」（いわゆる個人情報保護法）の2005年４月からの全面施行を契機に情報漏洩対策が話題となったように、内部からの情報漏洩は企業のリスク管理上の重要な課題となっている。

自社の機密情報や技術情報の漏洩、顧客情報の漏洩は、企業の競争力の低下、企業イメージの悪化、損害賠償責任の発生など、企業経営にダメージを与えるものであり、従業員情報の漏洩は、その従業員の不利益につながる可能性がある。また、不適切な内容の電子メールによって企業イメージが損なわれることもあれば、業務以外の電子メール利用が生産性に悪影響を与えることもある。

電子メール管理に関するガイドライン

このような状況のなかで、企業のセキュリティ管理者は、どのように電子メールを管理すべきであろうか。

経済産業省が公表している「情報セキュリティ管理基準」では、「電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること」がうたわれている。そのなかでは、「電子メールに対する攻撃の対処」や「電子メッセージの機密性及び完全性を保護するための、暗号技術の利用」といった外部からのリスクへの対処とあわせて、「電子メールの添付ファイルの保護」「電子メールを使うべきでないときに関する指針」「会社の信用を傷つける恐れのある行為に対する従業員の責任」「訴訟の場合証拠として使える可能性があるメッセージの保存」「認証できなかったメッセージ交換を調査するための追加の管理策」など、内部リスクを念頭においた諸施策を、電子メールの使用に関する個別指針に含めることが求め

NRIセキュアテクノロジーズ
情報セキュリティ事業部
上級セキュリティエンジニア
小山秀樹（こやまひでき）
専門はセキュリティ製品の設計・開発

られている。

また、個人情報保護に関連して経済産業省が定める「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」では、個人データの送信時の対策として、盗聴される可能性のあるネットワークで個人データを送信する際に、個人データを暗号化することが望ましいとされている。たとえば、インターネットでメールに添付してファイルを送信するような場合には、外部からの脅威に備えるために暗号化が求められるということである。

金融業界に対しては、FISC（金融情報システムセンター）が示す「金融機関等コンピュータシステムの安全対策基準」のなかで、電子メール送受信、ホームページ閲覧などにおける不正使用防止機能を設けることが求められている。とくに、個人データを扱う場合には、業務目的以外の電子メールの送受信に対処するため、セキュリティポリシーと整合性のとれた不正使用防止対策を講じることが必要とされている。業務目的外の具体的な例として、業務に関係しない私的な情報の交換・連絡、業務上適切な範囲を逸脱した電子メールの利用（メーリングリストやメールマガジンの不適切な利用など）、公序良俗に反する情報の送信があげられている。

米国でも、SEC（証券取引委員会）規則17A-4や、HIPAA（医療保険の携行性と責任に関する法律）などの規制で、通信の保管とアクセス制御が要求されている。また、サーベンス・オクスリー法（いわゆる企業改革法）では、電子メッセージを含むデータの維持、保管、安全性の保持の必要性が強調されている。日本でもこの考え方を踏まえて内部統制の強化が議論されており、法制化に向けての検討が進められている。

高まる内部管理への意識

情報漏洩に対する各方面の厳しい姿勢と、内部管理強化の潮流の背景には、いわば性善説から性悪説への転換がある。

経済産業省の報告書『リスク新時代の内部統制―リスクマネジメントと一体として機能する内部統制―』では、日本の企業を取り巻く状況の変化を、「従来、わが国においては、終身雇用制の存在等を背景として、社内の関係者間の信頼関係や暗黙の了解をもとに業務が行われる傾向があり、社内における従業員間の相互牽制やモニター等の仕組みが必ずしも明確化されていなかった。しかし、現在では、雇用の流動化や企業再編の進展等により、従業員、当事者間の暗黙の了解や信頼関係のみに依存した経営管理のあり方に限界が生じてきている」と分析している。

NRIセキュアテクノロジーズでは、2005年3月に情報セキュリティに関するアンケート調査を実施した。そのなかで、セキュリティポリシーに基づいてすでに作成済みまたは作成予定の規定について尋ねたところ、78.4%

の企業が「個人情報管理に関する規定」をあげ、また75.1％の企業が「機密情報管理に関する規定」をあげている。いずれも「コンピュータウイルス対策に関する規定」をあげた71.8％を上回っており、内部管理への関心の高さをうかがわせる結果と言える。

今後は電子メールの管理に関しても、外部的なリスクに加え、内部的なリスク対策の必要が認識され、その対策が具体化されてくると思われる。

電子メールの情報漏洩対策ツール

その電子メールの情報漏洩に関する内部的なリスク対策として、NRIセキュアテクノロジーズでは、安全なファイル交換を可能にするサービス「クリプト便」と、電子メールの監査を支援するツール「SecureCube/Mail Check」を提供している。

(1) ファイル交換サービス「クリプト便」

2001年８月から提供されている「クリプト便」は、電子メールの盗聴、改ざん、情報漏洩などの脅威への対策として、インターネット上で安全にファイル交換ができるサービスであり、以下の機能を備えている。

①暗号化

インターネット上ではSSL（インターネット上でデータを暗号化送信するためのプロトコル）により、サーバー上ではDES（暗号化アルゴリズムのひとつ）により暗号化を行うことにより盗聴を防止する。

②誤配信への対応

電子メールの宛先としてあらかじめ登録された宛先だけをWeb画面から選択することにより誤配信を事前に防止する。また、Web画面から送付相手の受信確認を可能とすることにより、誤配信を早期に検知する。

③ユーザー承認による電子メールの監査

あらかじめ指定された承認者のチェックを受けた電子メールだけを送信することにより電子メールの内容の監査を可能とする。

④ウイルスチェック

電子メールデータが保管されるサーバー上でウイルスチェックを行う。

⑤アドレス指定送信

一定のセキュリティを確保した上で利便性を向上させることを目的に2005年４月から追加された機能で、事前登録していない相手にも、Web画面からアドレスを指定して安全に情報を送ることが可能である。

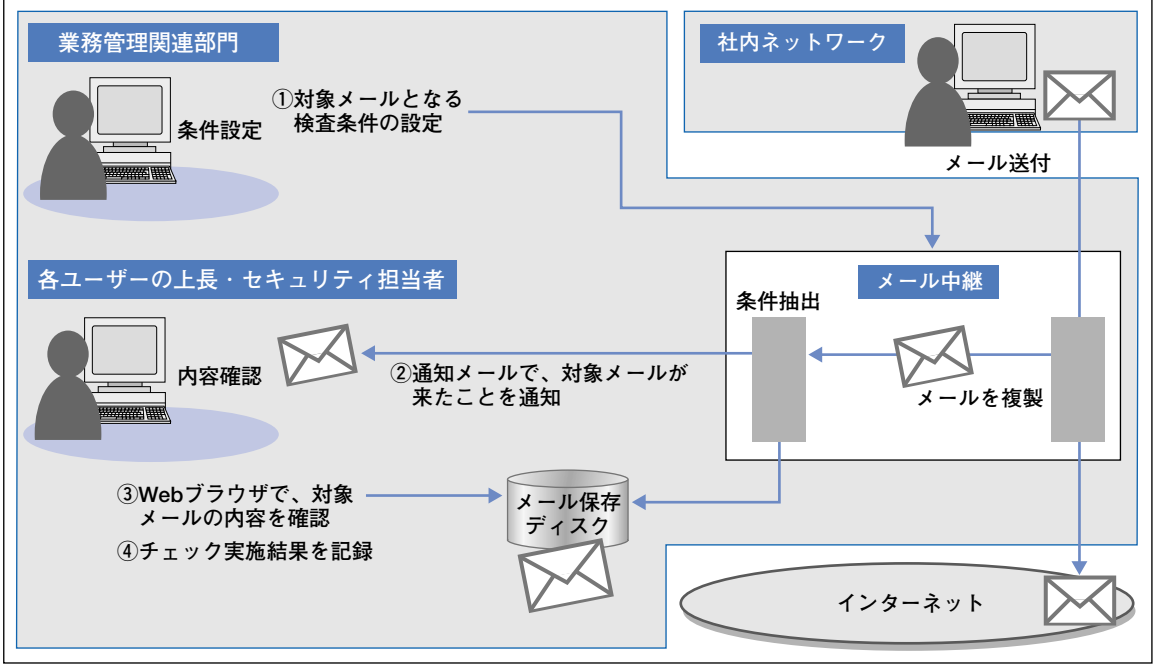
(2) 電子メール監査支援ツール「SecureCube/Mail Check」

「SecureCube/Mail Check」は2005年６月より販売を開始したパッケージで、おもな機能として以下のものがある（図１参照）。

①組織の実情に即した電子メールの監査

上司と部下の関係を設定することにより、職務権限として上司が部下の電子メールの監査を行う。組織の実情に即した効率的な監査

図1　SecureCube/Mail Checkの仕組み



が行え、情報漏洩や業務外目的の利用を抑止することができる。

②電子メール監査状況の可視化

電子メールの監査状況を可視化することにより、電子メール監査業務の実施状況の確認ができる。

③電子メールログの長期保存と高速検索

電子メールログ(証跡を記録したファイル)の長期保存が可能で、高速な検索もできる。

④アクセス管理

電子メールログを参照できる権限のあるユーザーを設定（制限）することや、電子メールの検索条件設定のログを管理することで、業務目的を逸脱したりプライバシーの侵害となるような電子メールの参照を牽制することが可能となる。

個人情報などを含む重要なファイルの交換には「クリプト便」を利用し、通常の電子メールは「SecureCube/Mail Check」を利用して電子メール監査を行うことで、利便性と高いセキュリティを両立させた、安全な電子メール利用環境を構築することが可能となる。

今後、セキュリティを維持しつつユーザーや管理者の利便性を向上させるため、「クリプト便」と「SecureCube/Mail Check」を連動させて、電子メールのログの一元管理や、特定の電子メールを自動的に「クリプト便」経由で送信することができるような改善を行う予定である。 ■