企業における情報セキュリティ特集によせて

執行役員常務
丸山　好一

平素よりNECのソリューション並びに製品をご利用いただき厚く御礼申し上げます。

企業のインターネット利用が本格的に活発化した90年代、電子メール、ウェブの利用が企業活動のすみずみまで浸透しました。電子メールによる情報交換、ウェブによる社内業務、ビジネスへと、近年例にない業務スタイル、ビジネスモデルの改革を実現しました。一方、電子化された情報は簡単に誰にでも渡せるため、個人情報漏えいなど重大な問題を起こしやすく、情報セキュリティ管理の強化が緊急の課題となっています。本誌でも2003年にセキュリティ特集を組み、課題に対する取り組み方を示しましたが、一方で新しい状況、新たな課題も明らかになっております。変化を続けるセキュリティの課題を解くためには、継続的かつ総合的な取り組みと対策の強化が必要です。

セキュリティというと、何に対しても必要なことと認識されている一方で、難解そうでどう取り組めばよいのかが分かりにくい、という印象を持つ人が多いようです。これはセキュリティ技術が難しいということではなく、セキュリティ対策が脅威に対して説明されるため、日常業務といった利用者目的とセキュリティとの関係が捉えにくいからです。

コンピューティング、ネットワーキングの方式や技術革新が互いを牽引し合って、高速、大容量、広域で使いやすいIT環境を実現してきました。セキュリティの脅威はこれら新しい技術や運用管理の狭間をついて現れます。しかも、IT技術が高速に向かって発展すると、ワームは速く拡散し情報がすぐ見つかるなど、脅威の強さも増します。脅威の影響は異なる場所に現れてすぐに変化していきます。その変化に合わせて対策も変えなければなりません(**表**)。このように変化のスピードが速い脅威は理解しにくいと言えます。

2000年代になると、外部からの攻撃に対する対策を中心にしていた90年代の状況から、コンプライアンスを背景として、人的なミスや故意によって内部から生じる情報漏えいの防止へと焦点が移りました。実は、セキュリティ問題の80%は内部で発生するというFBIの古典的報告があります。この事実に向き合って十分な対策を取るということは、単純に考えてもそれ

までの4倍の複雑さと労力を覚悟しなければなりません。

この性悪説に立った組織内の統一的なセキュリティ管理になると、実はまだどの企業でも十分できているわけではありません。PCを丸ごと暗号化するなどの対策を取ってはみたけれど、情報がどこかで漏れてしまうことを止められない、といったことをこの2〜3年で経験したという状況ではないかと思います。

個人情報保護法、e–文書法、金融商品取引法(J–SOX)などコンプライアンス準拠への真摯な企業姿勢が問われる時代を迎え、これまでのインシデント・ドリブンな対策から、抜け道を作りにくい本質的なセキュリティ対策の実現へと中長期的に取り組むべきタイミングに来ています。本質的、総合的なセキュリティ対策を企業戦略に組み込み、新しい脅威が発生しても最短時間、最小コストで対策を終えて、本業のビジネス遂行を続けられる企業が顧客の信頼を勝ち取ることができます。

NECでは、この新しいセキュリティ課題の本質的なところに深く入り込んで解を提供しなければ、問題はいつまでたってもなくならないと考えています。本質的なことというと、

1) 確実な認証とID管理

常にユーザ認証を行い企業内IT環境の匿名利用は行わせないことがセ

表　IT 技術、セキュリティの脅威と対策、その背景の歴史的推移と相関

年代	コンピューティング技術	ネットワーキング技術	代表的な脅威	主要な対策	牽引背景
70-	端末/ホスト	専用線、ダイヤルアップ	フレーカー		企業スパイ
80-	クライアント/サーバ	LAN、インターネット	不正ログイン、ウイルス	ユーザ認証、ワクチン	
90初	三層クラサバ	LANの広域化	ウイルスの進化		愉快犯
	Thinクライアント	オンラインネットワーク	攻撃ツールの一般化	ファイアウォール	
90中	ウェブ	商用インターネット	DOS、ページ改ざん	サーバ要塞化	
90後	ストリーミング	ブロードバンド	ワーム、ワームの進化	VPN、IDS	
00初	P2P		情報漏えい、	暗号化	コンプライアンス
	モバイルコード	無線LAN	フィッシング、	IPS、PC管理	
		モバイル	スパイウェア		
00中	空間共有		ボット、内部犯行	監視、フォレンジック	
今後	Web2.0	ユビキタス	スピア型ウイルス	対策の連携・統合化	企業責任
	グリッド	NGN	自己進化型ウイルス	安全なインフラ	企業戦略

キュリティ管理の出発点です。

2) 情報の格納先になるファイルの管理

暗号化による情報管理対象を、ユーザが日常アクセスする単位になっているファイルまで管理粒度を細かくすることが基本です。

3) 統合管理による統制

ユーザやファイルという粒度で、IT環境の利用を制御、監視し、証跡をとって分析まで行う統合的な管理が不可欠になります。

4) 抜け道をふさぐマルチレイヤー対策

1つの対策で十分とは考えず、対策を多重にレイヤー化して、1つの対策で抜け道が出ても別のところで防ぐことができる方式が必要です。

5) セキュリティを事前検証したシステム

セキュリティ製品を事前に組み込み、脆弱性がないことを事前検証したトータルシステムとして準備することが重要です。

6) 専門化の効果的活用

動きが落ち着いていない状態の脅威には、柔軟に対応できる専門家が一緒になって対策を考える体制が必要です。

といったことが挙げられます。

今回の特集では、このように今後不可欠な統合的、本質的なセキュリティ対策への取り組みを、具体的な製品、システム、SIなどの方向性と先行事例で紹介しています。NECでは、これら製品、システム、SIを自ら適用して有用性を向上させ、その経験をもとに高品質なセキュリティ対策手段を提供し、安心、安全な情報システムの利用と本業のビジネス遂行に注力できる環境を実現します。

今後とも、ご鞭撻を賜りますようお願い申し上げます。