情報セキュリティ管理の意義と内部リスク対策ソリューション

山越　俊也　　今泉　賢一

ネットワーク社会の発展に伴いインターネットの利用が急激に伸びている中，不正アクセス事件や情報漏洩事件が多発して問題となっている。近年，セキュリティに関する法や制度の整備が進んでおり，今後は企業における情報セキュリティ管理の徹底が必須条件となってくる。

当社では，高信頼性システム構築技術に基づくセキュリティネットワークの構築や，米国の著名コンサルティング会社との技術提供による情報セキュリティに関するコンサルティングなどのソリューションを開発し，官公庁を始めとして金融機関や企業に提供している。

本稿では，情報セキュリティを取り巻く環境を紹介するとともに，最近，大きな問題となっている情報漏洩などの内部リスク対策ソリューションについて述べる。

情報セキュリティを取り巻く環境

(1) セキュリティの脅威

情報セキュリティの対策として，まず外部からの不正アクセスを防ぐネットワークセキュリティがある。企業がインターネットに接続するときには，この対策を施し，外部リスクからの防御を行っている。不正アクセス対策やウィルス対策などの外部リスクマネジメントについては数年前から対策が普及しており，高度化を進める段階にある。しかし，内部リスクに関する情報セキュリティ対策を運営管理面において網羅的に行っている企業は2割程度に留まっている[1]のが現状である。

セキュリティの脅威は，①故意による意図的脅威（企業機密や顧客名簿の流出，顧客データの改竄・偽造，クレーム情報の隠蔽，情報システムに対する無差別攻撃），②事故や過失による偶発的脅威（ハードウェア故障やバグによるシステム停止，管理者の過失によるシステム停止，セキュリティの無知や無関心による情報漏洩），③災害等による環境的脅威（地震・火事・洪水・停電等によるシステム停止），に大別される。

最近では，意図的脅威や偶発的脅威に起因するセキュリティ・インシデントが増えており，特に内部からのセキュリティの脅威が増加している。

米国におけるCSI/FBIによる2002年度のセキュリティに関する攻撃や誤使用の発生状況の調査（図1）でも，コンピュータウィルスに次いで内部によるネットワークの乱用が約80%に上ると集計されている。

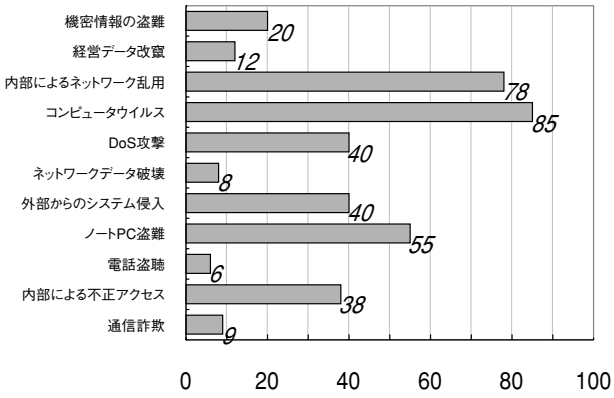

図1　2002年に発生した攻撃や誤使用の割合（%）[2]

また，機密情報の漏洩や経営データの改竄など企業の中核的な情報における被害額は相当な額（図2）となるので，十分なセキュリティ対策が必要となってくる。

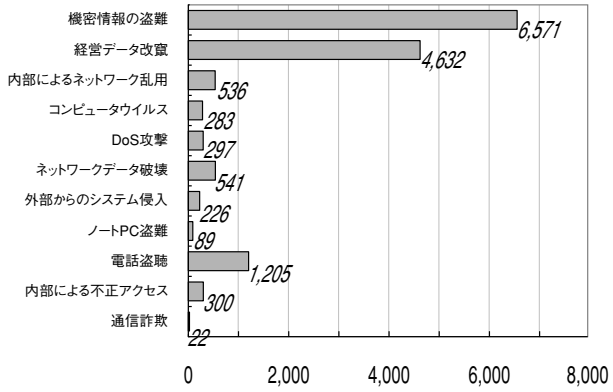

図2　2002年に発生した被害の各社平均額（千ドル）[2]

(2) セキュリティ対策の意義

セキュリティ対策としては情報セキュリティ管理の徹底が重要であり，その基本的な理念として，機密性，完

全性，可用性が挙げられる。

- 機密性（confidentiality）：アクセスを許可された者だけが情報にアクセスできることを確実にする。
- 完全性（integrity）：情報および処理方法の正確性・確実性を保持する。
- 可用性（availability）：許可された利用者が，必要なときに，情報および関連する資産にアクセスできることを確実にする。

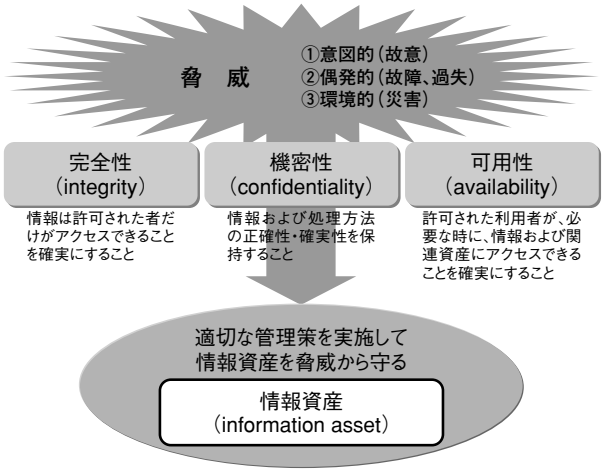

図3　セキュリティの要件

これらの理念を柱とした情報セキュリティ管理を導入することで，体系化された情報セキュリティの対策を策定でき，そのメリットも大きい。

- 責任権限の明確化，文書管理／記録管理の徹底等，経営全般のリスクマネジメントへの波及
- 従業員のモラルアップ
- コンプライアンス対応，損害賠償責任，対株主責任等，経営責任の公的担保
- 株主や行政，顧客等への信用度の向上
- 情報リスクマネジメントのステータスを確立し，企業イメージがアップ

(3) セキュリティ対策に関する世の中の動き

最近ではセキュリティに関する法規制や情報セキュリティの管理に関する標準化が進みつつある。

法規制では，不正アクセス禁止法（2000年2月）を始めとして，IT基本法（2001年1月），電子署名法（2001年4月），書面一括法（2001年4月），カード偽造犯罪刑法改正（2001年7月），プロバイダ責任法（2001年11月），電子契約法（2001年12月）が施行され，個人情報保護法が審議されている。

また，基準や標準化として，コンピュータウィルス対策基準（1995年7月），情報システム安全対策基準（1995年8月），コンピュータ不正アクセス対策基準（1996年8月），英国の情報セキュリティ対策の標準であるBS7799，そのPart1が国際標準化されたISO/IEC17799（情報セキュリティ管理実施基準），情報処理製品や情報処理システムのセキュリティ完備状況を評価するISO/IEC15408（セキュリティ評価基準），(財)日本情報処理開発協会によりBS7799に準拠した情報セキュリティ管理状況を評価する情報セキュリティマネジメントシステム（ISMS: Information Security Management System）適合性評価制度，経済産業省による情報セキュリティ監査制度など，情報セキュリティを体系的に管理する制度が整備されてきている。

沖電気の情報セキュリティへの取り組み

このように，外部リスクのみならず内部リスクによる情報漏洩等の対策を含めた制度の整備が進む中，当社では，標準化に対応したコンサルテーションなどの非技術的なソリューションとシステム構築などの技術的なソリューションとを提供できる体制を整え，情報セキュリティに関してトータルなソリューションを展開している。

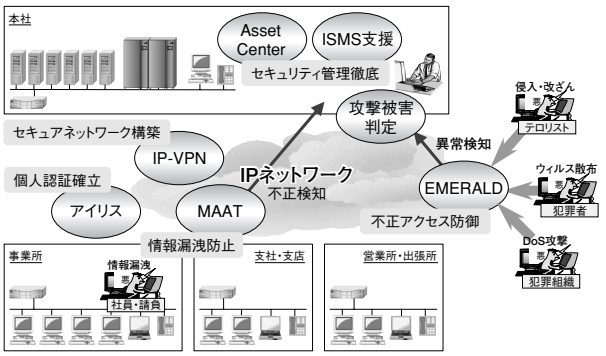

図4　当社のセキュリティソリューション概要

コンサルテーションとしてはセキュリティ評価・レビュー，ポリシー策定支援，情報セキュリティ教育支援などBS7799やISMS適合性評価制度の標準化に準拠したサービスを提供し，認定取得をゴールとしたコンサルテーションを行なう。システム構築などの技術分野では，外部リスク対策として，セキュアネットワーク構築（不正侵入検知システムEMERALD，IP-VPN），高可用性システム構築，セキュリティ診断，被害診断などのサービスを提供している。また，内部リスク対策として，ネットワーク監視システム（OpenView），情報漏洩監視システム（MAAT*1)），統合資産管理システム（AssetCenter*2)），アクセス分析システム，個人認証シ

*1）MAATはレイヤーセブン(株）の商標です。　*2）AssetCenterおよびINDはPeregrine Systems社の登録商標です。
その他，文中の製品名等は各社の商標または登録商標です。

ステム（虹彩認識アイリスパス）などを揃え，顧客のニーズに適した情報セキュリティシステムの提供を行っている。

当社社内においても，セキュリティポリシー策定，統合的な資産管理の徹底，BS7799およびISMS適合性評価制度の認証取得，顧客システムのセキュリティ設計強化などの実績を有し，そのノウハウを生かしてソリューションの強化に努めている。

情報セキュリティ管理の管理情報

(1) ISMS適合性評価基準の管理対象情報

内部からの情報漏洩を防止するためにも，体系だった情報セキュリティ管理手法を整備する必要がある。これを効率的に実施するために，ISMS適合性評価基準[3] が制定されており，この基準に基づいた管理の導入を検討している企業も多くなってきている。

ISMS適合性評価基準では規定面や管理面，運用面などのさまざまな基準が設けられているが，導入にあたっては当然各種データを管理する必要があり，その対象として，以下のようなものが挙げられる。

- 情報資産：内容，媒体，各種区分（システム区分，分類，区分），ロケーション，保管，台帳，更新履歴，原本，バックアップ）
- 人的情報：一般情報（所属，ロケーション，連絡先，職位，職務，職能），セキュリティ対象（区分，契約，教育）
- 装置情報：設置環境，電源対策，傍受対策，可用性，移動，保守，情報消去，保管，時刻同期
- システム情報：アクセス権，認証情報，ソフトウェア，バックアップ，作業履歴，ウィルス対策
- ソフトウェア情報：アクセス権，使用権，版数，パッチ履歴

また，システム運用に関わる情報としても，稼働状況，ネットワーク状況，利用状況，セキュリティ状況などに関する各種の情報（監視ログなど）が重要になる。

一般的に，これらの情報は人事管理システム，資産管理システム，ドキュメント管理システム，IT管理システムなどのシステムに分散して管理されていることが多い。今後，情報セキュリティ管理を推進するためには，これらの情報を連携して管理することが重要な要素となる。

(2) 管理対象情報の連携の重要性

たとえば，コンピュータウィルスが社内に侵入しPCが感染したケースを想定する。市販のアンチウィルスソフトでは，感染したPCのIPアドレスを知る事はできるが，その所有者や連絡先までは判らない。これらは通常，アンチウィルスソフトとは別次元の情報だからである。

このような状況において，PCの資産情報（IPアドレスを含む）と人事情報（所有者や連絡先）とを連携して管理されていると，感染したPCの所有者にいち早く連絡し，ネットワークから離脱させる処置や以降メールを使わせないといった早期対策を打つ事が可能となる。

内部リスク対策と情報管理

(1) 資産管理システムによる情報資産の管理

このように人事情報や資産情報，管理情報，監視情報などのさまざまな情報とそれを有するシステムを連携させて，情報セキュリティ管理の充実を図るため，当社では，統合資産管理システムAssetCenterを活用したセキュリティに関する内部リスク対策ソリューションを展開している。

AssetCenterは，企業内の資産情報を管理するシステムであり，以下の特徴を持つ。

第一に，AssetCenterは資産情報の統合データベースであること。資産情報およびその所有者の情報・場所の情報・契約の情報・コストの情報などをあわせて持つ事ができる。

第二に，高度なデータ検索機能を有すること。GUIではAND/OR等を含んだ複雑な条件検索機能を持ち，必要なデータを絞込んで取出す事が容易となる。

第三に，他システムとのデータ連携機能を持つこと。ERP（Enterprise Resource Planning）の人事情報・会計情報や，後述のIND[*2] およびインベントリ情報収集ツール等で収集した資産情報は，この仕組みを用いてAsset Centerに取り込み，統合的に管理できる。本機能によりデータベース構築が容易となり，またデータ自体の精度も向上する。

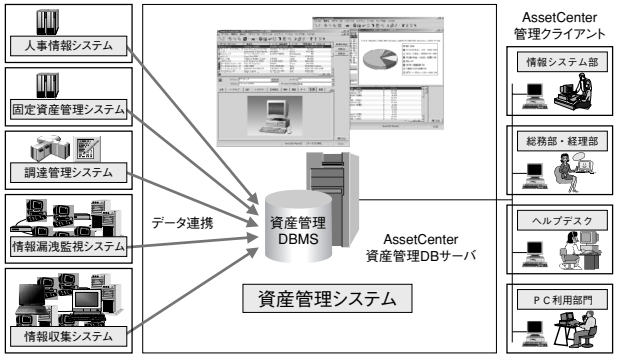

図5　AssetCenterによる統合資産管理

(2) ネットワーク管理機能との連携

IND（InfraTools Network Discovery）はネット

ワーク上に接続された装置の情報を管理・自動収集するシステムである。

INDを用いてネットワーク上に新たに出現したIPアドレスや，ネットワーク上に存在しなくなったIPアドレスの監視を行なう。もし条件に該当する機器を発見した場合，管理者にメール通知する事が可能である。これにより，機器の不正持出しやネットワークへの不正接続を監視する事ができる。

(3) インベントリ情報収集機能との連携

インベントリ情報収集システムとは，PCの情報（CPU・メモリ・DISK・OS・アプリケーション等）を取得するシステムである。たとえば，ウィルスのパターンファイルが最新版かどうかを確認したり，不正なソフトウェアがインストールされていないかをチェックしたりするのに有効である。更に，インベントリ情報収集システムの種類によっては，オペレーションログやアプリケーションの起動ログを見る事ができるものもある。これにより，内部からの情報漏洩等の不正行為を監査する事も可能である。

(4) 情報漏洩監視システムとの連携

情報漏洩監視システムとして，当社ではMAATを提供している。MAATは，ネットワーク上を流れるパケットを監視し，情報漏洩を検知して防止したり，監査用のログとして保存するソフトウェアである。「社外秘」や「機密」などのキーワードを指定し，ネットワーク上でこのキーワードを含んだパケットを発見した場合，送信者のIPアドレスをチェックしたり，該当パケットのセッションコネクションをリセットできる。

AssetCenterとの連携により，キーワードに抵触する行為を行った人物の名前や所属を特定する事ができる。また，MAATの設定情報をAssetCenterでチェックしたり，あるいは変更する運用も可能となる。

(5) システム事例

AssetCenterとその関連ツールを用いたセキュリティ対策の一例として，VISAインターナショナル殿の導入事例[4] を示す。

VISAインターナショナル殿が保有する社内データは，顧客リストなど重要な機密情報を含んでいる。外部からの侵入に対するセキュリティ対策は勿論，社内のPCにも不審なプログラムがインストールされる事のないよう，厳重に管理する必要があった。

また，ノートPCを中心としたモバイル端末の管理にも

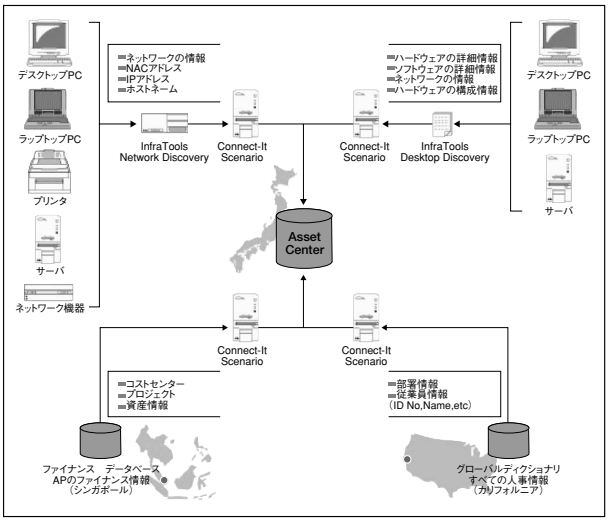

図6 ユーザシステム構成例

課題を抱えていた。一般的な割合が2%と言われている端末の紛失率が，年間4%にものぼっていたのである。資産の紛失による損失もさることながら，端末に格納された機密情報が漏洩する危険性もはらんでいた。

まずはINDの導入により，ネットワークへの不正接続や不正持出しを監視した。次にインベントリツールにより，PCにインストールされているソフトウェアの監視を行った。更にこれらで収集したデータや人事・会計情報をAssetCenterに連携し，統合資産情報として管理している。以上のシステム導入で資産を正確に把握する事が可能となり，最終的には端末の紛失率を0.5%に減少させるまでの大きな効果を上げている。 ◆◆

■参考文献

1）わが国における情報セキュリティの実態，(財)日本情報処理開発協会，2002年3月
2）2002 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, Apr, 2002
3）情報セキュリティマネジメントシステム適合性評価制度-ISMS認証基準Ver2.0案，(財)日本情報処理開発協会，2003年1月
4）AssetCenterユーザ事例カタログ，ペレグリンシステムズ株式会社

●筆者紹介

山越俊也：Toshiya Yamakoshi.エンタープライズソリューションカンパニー ソリューション企画部 シニアコンサルタント
今泉賢一：Kenichi Imaizumi.エンタープライズソリューションカンパニー インテグレーション部 チームリーダ