IT投資の重要課題は情報セキュリティ対策だ

「W32/Nimda」や「Code Red」など，新たなコンピュータ・ウイルスがマスコミを賑わすたびに，情報セキュリティへの関心は高まる一方だ．ウイルス騒ぎが起きるとその対策ソフトが売れ，ホームページの改竄事件が起きると，ファイアウォールの必要性が叫ばれる．しかし，こうした短絡的な対応では情報セキュリティを守ることはできない．従来は性能向上，可用性向上がシステム開発の主眼だったが，これからは情報セキュリティ対策を優先すべきだとする声も出てきた．

OS開発を中断して情報セキュリティ対策

国内のコンピュータ・ウイルス被害をとりまとめている経済産業省の外郭団体，情報処理振興事業協会（IPA）によると，2001年に届け出のあったコンピュータ・ウイルスの件数は，前年の2.2倍の2万4,261件に達した．1999年までは最大で3千数百件のレベルだったが，2000年に一挙に1万件と桁が跳ね上がり，昨年はとうとう2万件の半ばにまで到達してしまった．

こうしたウイルス被害の増大とともに，情報システムへの不正接続も拡大している．米国では2001年にはホームページの書き換え事件が多発して社会問題化し，国内でも個人情報の漏洩事件がマスコミを賑わした．

これに伴い，ユーザ・サイドでは情報セキュリティに対する関心が高まっている．以前，特に「水と安全はタダ」という風潮のある日本においては，こうしたセキュリティに対しての関心は薄かったことは事実．しかし，単なるコスト要因に過ぎなかったセキュリティへ対する認識がここにきて変わってきた．

情報システムで最も関心のある項目について，従来のパフォーマンス，アベイラビリティ（可用性）と並び，情報セキュリティを挙げる人が増えている．

マイクロソフトのビル・ゲイツ会長も，最近の社員向けメッセージで，ソフト開発の最優先課題として，セキュリティ対策やプライバシー保護を挙げた．2002年2月には，次のOS開発を一次中断して，7,000人のエンジニアにセキュリティ対策技術の特別プログラムを受講させる計画だという（日経新聞，2002年1月18日）．

技術開発より人の買収？

それでは，セキュリティ対策はどのように進めればよいのか．

国際標準機構（ISO）が制定しているセキュリティの管理規格「ISO 17799」では，「情報セキュリティとは情報の機密性，一貫性および可用性を維持することである」と定めている．それぞれの内容は次のようなものだ．

①情報の機密性（Confidentiality）：情報へのアクセスを認可された者のみがアクセスできること
②情報の一貫性（Integrity）：情報が発生したときから，その後の処理，また廃棄に至るまでその意味が一貫しており，途中で改竄などがされていないこと
③情報の可用性（Availability）：情報や関連資産に対して（認可されたユーザが）必要なときにアクセスできること

このConfidentiality，Integrity，そしてAvailabilityがセキュリティ対策のポイントだといわれている．一般的には，この3つの言葉の頭文字をとって「情報のCIA」と呼んでいるが，この情報のCIAを守ることが情報セキュリティの最大のテーマというわけだ．

しかし，このようにテーマが明らかになったといっても，すぐにウイルス対策ソフトだ，ファイアウォールだというのは短絡的すぎる．その前に大きく立ちはだかるのが人の問題である．

情報のCIAはすべて人が管理するものであり，その人の管理やそれを支える組織や制度などの仕組み作りが求められる．

実際，ISO 17799の元になったイギリスの情報セキュリティにおけるベスト・プラクティス（最適慣行）をまとめた基本的な管理項目「BS7799」では，その主任監査員のトレーニング・コースでも次のような問題を出している．

「非常に堅牢なシステムから機密情報を盗み出すのに，手元に資金が1億円あったらどうするか」

実は，正解は「このシステムの担当者を買収する」というものだ．

技術的に現在のプロテクションをうち破る製品を開発するというのではなく，管理面での脆弱性をつくというのがポイント．この問題は，現在のセキュリティ対策の盲点をついたものともいえる．情報セキュリティの一番の弱点は人間であるというのがこのBS7799の基本にある．

情報セキュリティに対する脅威は，その80%以上が内部からのものであるという調査報告もある．厳重なパスワードでガードするなど，技術的な対策をいくら講じても，その担当の人間が機密情報を漏らしてしまえば元も子もない．これは，技術的な対策には限界があり，技術的な取組みとともに，管理的な対策が必須であるということを訴えたものだ．

リスクとコストのバランスが重要

企業は情報資産を守りたいと考えている．それに対して，さまざまな脅威が出現してきている．その情報資産と脅威の間に壁を作るというのが情報セキュリティの基本的な考えだが，その壁をどう作るのかという現実的な問題がある．ここでも，人の問題が介在する．

壁をいたずらに厚くしてしまえば，人にとってそのシステムは当然使いづらいものになる．安全につなぐためには脆弱な個所をいかに減らすかがポイントになるが，同時に，システムとしてきちんとした情報サービスが提供できなければならない．

コストの問題もある．セキュリティ・レベルを上げようとして，厚い，穴のまったくない壁を作ろうとすると無限のコストがかかる．それは，現実的には無理である．かつまた，そのシステムは使いづらいものになる．そこで，リスク分析をしながら，その許容点を見つけ，コストとリスクのバランスをとった対策が重要となる．

BS7799のPart.IIでは，こうしたマネジメントの仕組みに対する普遍的，包括的なガイド，基準を示している．このPart.IIには「ISMS（Information Security Management System）適合性評価制度」が盛り込まれており，127の対策項目が示されている．しかし，これをすべて実施するということではない．その主旨は，これに基づいてリスク分析を行い，リスクが高い場合に，どのようにしてそのリスクの許容範囲を下げるかということをこの適用宣言書で調べるということである．

ツールを単に導入するのではなく，その前提としてこうした適用宣言書を作成し，ここにすべての項目を記載し，リスク分析をして，実施するかどうかを決めるという作業を求めているわけである．

企業側は，これに基づいてまず情報資産を洗い出し，その脅威が起こったときにどうなるのか，その影響を考える．その情報資産に問題が起こったら，もし使えなくなったら，1日ににどの程度の影響が出るかを考えていく．

しかし，ここでリスクをゼロにしようとしてはいけない．現在のようなインターネットをベースにした情報システムから脅威をなくすことはできない．ここで必要なのが，バランスである．情報セキュリティも，重要なのはバランスなのである．

情報セキュリティ対策が企業のステータスを向上

かつては負の投資とまでいわれた情報セキュリティが，今なぜクローズアップされているのか．

情報の価値が増大する一方，インターネットなどの普及により情報システムに対する脅威が増大しているのが第1の理由．さらにここにきて，情報セキュリティへの取組みが企業のステータスを向上するという要素も出てきた．

マイクロソフトのビル・ゲイツ会長は，社員に対するメッセージの中で「信頼できるコンピュータ技術を開発することが，マイクロソフトにとって重要課題である」と言っている．企業の危機管理が問われるように，こうした情報セキュリティにきちんと取り組んでいるか否かが，企業の競争力を左右するようになってきた．

eコマースサイトを運営しているような場合は，情報セキュリティがしっかりしていない企業には注文はこない．顧客情報が漏れるような企業は，B to Bの関係でも取引停止になる可能性がある．情報セキュリティは完全に負の投資ではなくなった．

経済産業省も動き出している．日本には，2001年3月までは「情報処理サービス業情報システム安全対策実施事業所認定制度」（安対制度）という独自の基準があったが，これはすでに廃止され，BS7799 Part.IIと同様の認証制度に基づく「ISMS適合性評価制度」の取組みがスタート．これをJIS化し，近々正式運用がスタートする見込みだ．

こうした流れは，セキュリティ認証において国際的に相互認証を行おうという目的に基づいたものだが，それだけ情報セキュリティが重要になってきたことを示している．今の情報システムに求められるのはパフォーマンスや可用性だけではない．

（平成14年1月24日受付）

宍戸 周夫●（株）テラメディア
shishido@dance.plala.or.jp