情報セキュリティ基盤の考え方と東芝のソリューション

Information Security Infrastructure Provided by Toshiba

河井　宣之
■KAWAI Nobuyuki

個人情報の漏えいをはじめ，様々なセキュリティ事件や事故が発生し，企業や組織のセキュリティへの取組みは，社会的な責任として重要度を増している。企業・組織は，情報セキュリティに対してどのような対応をとるべきか。情報セキュリティ対応が，つぎはぎだらけの対策にならないためにはどうすればよいか。情報セキュリティ基盤の構築のための基本的な考え方に基づき，東芝ソリューション(株)は，情報セキュリティソリューションを提供している。

Security attacks such as unauthorized access of personal information occur daily.　It is vital for every company and organization to address such security issues due to their devastating impact on the company or organization concerned.　How should individual companies and organizations deal with these types of issues?　How can they be handled proactively?

Toshiba Solutions Corp. provides information security solutions based on the concept of building a basic architecture for system security.

1　まえがき

近年，企業の目覚ましいIT(情報技術)化とともに，業務の多様化，企業のグローバル展開，モバイル環境の拡大，そして企業間の複雑なコラボレーションが急速に拡大している。一方，情報に対するリスク意識は急激に高まりつつあり，それはテレビや新聞などでも取り扱われ，一般消費者にまで広まっている。つまり，セキュリティ事件・事故がひとたび起きると，企業・組織としての機密漏えいによる直接的な損害だけにとどまらず，損害賠償や企業・組織としての信用失墜という長期かつ深刻な問題に発展しかねない状況に陥ることが容易に予想できる。

ここでは，そのような重要な情報をいかに守るかについての基本的な考え方と，東芝ソリューション(株)が提供するセキュリティソリューションについて述べる。

2　情報のライフサイクル

企業・組織が扱う情報には，どのようなプロセスがあるのであろうか。それをあえて，情報のライフサイクルと呼ぶと，次のようになる。

⑴　情報の作成・生成
⑵　情報の保管
⑶　情報の持運び
⑷　情報の変更・加工
⑸　情報の配布・送付
⑹　情報の廃棄・削除

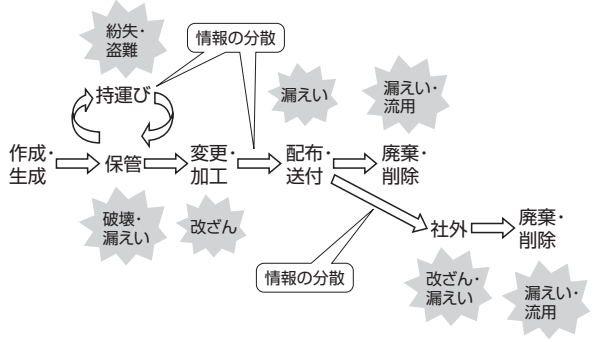

図1．情報のライフサイクルにおける脅威― 情報には，その置かれた状態により様々な脅威が存在する。

Life cycle of information

厳密には，各フェーズで閲覧や印刷，更に配布先での保管や変更・加工，再配布などが行われるが，それらも包含して前記のフェーズに集約してみた。

そのライフサイクルにセキュリティにおける脅威を当てはめると**図1**のようになる。図1を見てわかるとおり，“情報とは分散・拡散するもの”である。

一般に情報は，企業・組織活動のために共有され，更に改変して配布されるものである。つまり，情報の管理とは，いかに不用意に持ち出さないか(持ち出させないか)ということと同時に，持ち出された情報をいかにコントロールするかも重要となる。

同じレベルの権限を持った集団，あるいは同一部門，社内，許可した社外取引先など，様々なケースを想定し，

それに合った情報管理が必要となってくる。

情報とは，様々な状態で存在し，流動していく可能性がある。その“様々な状態”を把握することが，リスク管理の第一歩である。

3 情報資産について

企業・組織が守るべき“情報資産”といえば，すぐに思いつくのは電子的な情報や紙の文書，つまりデータベースや電子メール，契約書や図面などである。しかし，セキュリティの見地から情報資産という場合には，**表1**に示すものが含まれる。ここで注意すべきは，情報資産とは情報そのものだけではなく，情報を保管している物理的資産，あるいは情報を処理するソフトウェア，更にはそれらを取り巻く環境に関するものまで含まれることに注意したい。

表1．セキュリティにおける情報資産
Information assets of information security management system (ISMS)

対　象	内　容
紙の文書	契約書，図面，見積書，マニュアルなど紙による情報
電子情報	データベース，ファイルサーバ内やPC内の情報など
ハードウェア	サーバ，ディスク装置，ネットワーク機器など
ソフトウェア	業務アプリケーション，開発用ソフトウェアなど
サービス	計算サービス，通信サービス，空調，電源など

セキュリティを考慮するには，単に情報そのものだけでなく，それが存在している領域全体及びその情報に直接的あるいは間接的に関与する物理的・論理的・人的なプロセス全体を視野に入れた対応が必要になってくる。

セキュリティを検討するにあたって，情報そのものだけに注目し対処することは危険である。その情報が存在する環境や状況に注目し，方策を考えなければならない。

4 セキュリティ対策で犠牲になるもの

セキュリティを向上させるということに対するトレードオフの関係として，“利便性”が挙げられる場合がある。つまり，セキュリティのためには，利便性を損なってもやむをえないという考え方である。しかし，セキュリティ対策の責任者や管理者としては，いかにその利便性を損なわないような対策を施すかが重要な要件となる。

まず，“本当にそのような対策でよいのか”，“一律，全員に同じ対策を講じるべきか”などの視点が必要だ。つまり，情報を持ち出さない対策として，完全一元管理（サーバでのみ情報を管理し，ほかには情報を存在させない）という有効な方法があるとしても，全情報，全員がそれに従うと，不便な局面が必ず生じる。その結果，なんとか抜け道を考える人が出てくる。それがまさに企業・組織の“セキュリティホール”となる。

どういった情報（What）のどこに（Where），誰に（Who），どのように（How）セキュリティ対策を施すかをしっかり考える必要がある。

5 セキュリティ対策の基本的な進め方

これまで述べてきた内容を踏まえて，いかにセキュリティ対策を講じていくべきか，次に示す。

ステップ1：セキュリティの基本方針を策定　まず，全社レベルでのセキュリティ基本方針を決める。“わが社にとって，重要な業務及びそれにかかわる重要な情報は何か”を明確に内外に宣言するのである。今後，このセキュリティ基本方針は，企業の姿勢・考え方を示すものとして，企業のホームページなどを通じて一般に公開する方向に向かうであろう。

ステップ2：情報資産とそのリスクの洗出し　一般に言うリスクアセスメントである。どこにどのような情報，特に重要な情報があり，どのように管理されているか，誰がアクセスしどのように扱われるか，を明確にする。そして，その情報についてどんな問題，つまりリスクがあるか，もしそのリスクが発生したらどんな影響があるか，を明確にする。それにより，おのずと対策を講ずべき対象の優先度が浮き彫りになってくる。なお，その際に，セキュリティ対策のレベル，すなわちどの程度のセキュリティを施すかの基本的な指針を決めておかなければならない。

ステップ3：対策案の策定　問題が明確になったら，それを解決する方策を検討する。ケースによっては，社内規程を見直すことかもしれない。あるいは，取引先など他社との契約内容を改定することかもしれない。そしてあるケースでは，ツールやシステムを導入する対策かもしれない。そのような，組織的な面や技術的な面，運用面，そして人的な面の対策を考えていく。

ステップ4：対策の周知徹底　具体的に対策が明確になったら，それを実現する。ツールやシステムの場合はそれらを購入し，評価し，構築・展開し，利用方法を周知し徹底させる。規程や契約の変更にあたっては，その内容を関係者（多くの場合，全社員）に対し，教育し周知徹底させる。

ステップ5：監査と見直し　セキュリティの状態が保たれているか，つまり決められたことを守っているかをチェックする。更に，セキュリティを強化すべき問題点

はないかを常に検討し，改善を図る。

このステップは，まさにISMS（情報セキュリティマネジメントシステム）の手順であるが，いかなるセキュリティ対策においても，前記のステップを踏まえた検討が重要である。それは，企業・組織内で統一のとれたセキュリティ対策，投資効果のあるセキュリティ対策，そしてなにより“守られる”セキュリティ対策を実現するための手順なのである。

6 東芝のセキュリティソリューション

セキュリティは，顧客の組織，業務，環境，システム，風土などにより，そのニーズは非常に多様である。当社は，いままで述べてきた情報の多様性と流動性に配慮し，以下のポイントに着目した。

⑴ 外部からのアクセスの管理　　不正な人を監視し，管理する。

⑵ ネットワーク経由のセキュリティ　　不正なアクセス，侵入，ウィルスを防ぎ，情報流出を管理する。

⑶ 正当なアクセス　　正しい人，正しい機器だけにアクセスを認める。

⑷ 情報漏えいの対策　　情報の持出しを管理する。

当社のセキュリティソリューションでは，前記を踏まえ，業種・業務システムに共通なセキュリティ基盤を提供できるようなソリューション体系とした（**図2**）。

⑴ セキュリティコンサルテーション　　セキュリティ全般に関して，顧客の課題とニーズを明確化し，組織面や人的な面などトータルにセキュリティ構築を実現する。“何から手をつけてよいのかわからない”あるいは“わが社に合ったセキュリティ対策とは”などの悩みに対し基本から考え，最適な解決策を提供する。更に，ISMSやプライバシーマークなどの認証取得，製品のセキュリティ品質を確保するISO（国際標準化機構）15408取得なども効果的，効率的に行えるコンサルティングを提供する。

⑵ IT資産管理システムソリューション　　当社は，重要な情報を“情報資産”の定義どおりその範囲を情報だけに限らず，関連するハードウェアやソフトウェアなどにまで拡大し，“IT資産管理”と呼んで，重要な情報を守るためのシステムを提案する。情報の持出し管理やメール・ウェブを介した情報管理，更にはセキュリティ監視やIT資産（ハードウェア，ソフトウェア，ライセンス）管理まで統合的に提供する。

⑶ ID管理／認証システムソリューション　　情報セキュリティの基本は，許可された正しい人，正しい機器のみがアクセスできること。そのための仕組みとして，PKI（Public Key Infrastructure）認証システム，ICカードシステム，シングルサインオンシステムなどのほか，最近注目されているアイデンティティ（ID）管理やバイオメトリクスなどの仕組みも提供している。

⑷ ネットワークセキュリティソリューション　　ファイアウォールや不正侵入検知・防御などのほか，検疫ネットワークなどを強化した。ネットワークに接続を許可されたパソコン（PC）であっても，接続してもよい状態（基本ソフトウェア（OS）パッチやウィルス対策ソフトウェアの状態など）かどうかにより接続を拒否したり，PCを最新の許可された状態に自動的に更新する。更に，今後重要性を増す責任追及性の手段の一つとして，フォレンジックシステムも提供していく。

⑸ 物理セキュリティソリューション　　不正な第三者の侵入を防ぐことは，セキュリティの基本である。入退出管理システムや監視カメラシステムにより，組織・人の管理の基盤を作る。更に，顔認証とゲートシステムを組み合わせたソリューションなど，ニーズに合わせた多彩なシステムを提供する。

⑹ セキュリティSI　　セキュリティSI（System Integration）とは，セキュリティシステムを構築するにあたり，業務システムとの連携，システムとしてのセキュリティ基本方針策定（基本設計），運用方法も含めたシステム設計，セキュリティシステムの構築・展開などをトータルにサポートし，確実なセキュリティシステムの構築を支援する。

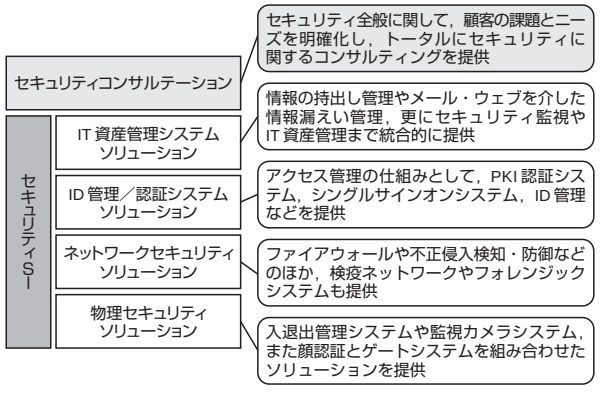

図2．東芝のセキュリティソリューション体系 ― 業種・業務システムに共通的なセキュリティ基盤を提供できるソリューション体系としている。

Toshiba information security solutions

これまでに述べた当社のセキュリティソリューションは，現実の場面においてどのような分野をカバーするかを，概略セキュリティマップに当てはめると**図3**のようになる。

当社は，上流のコンサルティングにより，企業・組織ごとに持つ課題を洗い出し，更に，その企業が持つ組織風土などを踏まえたうえで，いかに“定着するセキュリティ”を構築する

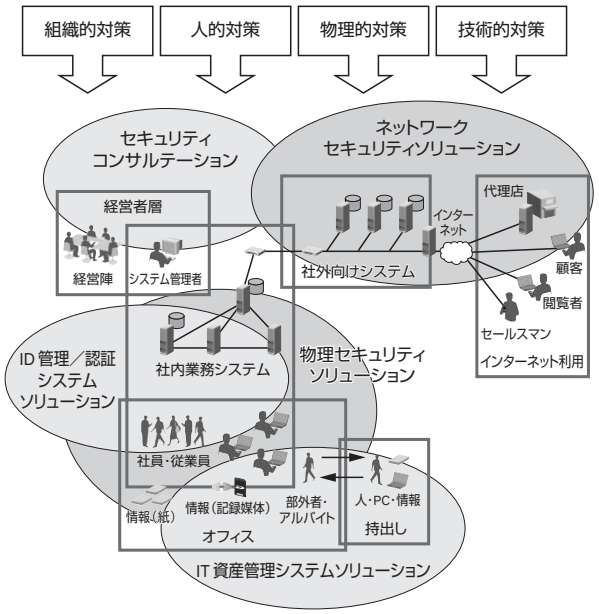

図3．セキュリティソリューションマップ― 企業活動の様々な場面でのリスクを網羅している。

Toshiba solutions on security map

かを考え，そのうえで，必要なセキュリティシステムを提案していく。

7 情報セキュリティ強化のプラスアルファ

情報セキュリティを向上させることは，なにかとめんどうである。ポリシーを考え，体制を整え，具体的な規程を定め，全員に周知徹底し，システム的なものも含め対策を実施し，なによりも維持継続し，更に，改善しなければならない。

目的は，“セキュアな組織作り”であり，“顧客をはじめとした関係者に迷惑をかけない”，そしてひいては“企業・組織としての信用の向上”である。しかし，実際に，ISMSなどに取り組む企業・組織の多くは，それだけにとどまらない目標を持ち，成果を出している。

例えば，ISMS構築やセキュリティシステムを通じて，**表2**のような効果が考えられる。

実際，個人情報保護法を契機に社内の個人情報を洗い出した際，個人情報の管理方法や受渡しの方法などがあいまいであることに気づいたという人も少なくないと思われる。

つまり，これは，TCO（Total Cost of Ownership）の削減であり，事業戦略にも関与する。

表2．セキュリティ強化による副次的効果

Effects of security controls

項　目	副次的効果
通常業務の改善	不要又は冗長な書類や電子データを削減したり，対外的な契約の見直しでスリム化
業務プロセスの改善	社内業務フローの見直し，文書管理などの業務遂行上の手続きや規程などの根本的見直しと改善
業務システムの見直し	システムやネットワーク，マシン室の見直しによる効率化や簡素化の実現など
事業継続管理の改善	セキュリティ事件・事故防止策の一環としての対リスク強化と情報伝達のスピードアップ
事業そのものの見直し	セキュリティ上問題となる業務のあり方の見直しなど

企業のセキュリティに対する世間の目が厳しい現在，信用を失った企業・組織は，その存続すら危うくなる。コンプライアンスの一つとして，また，会社・組織の社会に対する責任＝CSR（Corporate Social Responsibility）の一つとして，情報セキュリティは，経営上のリスク管理対象の重要な要件なのである。

8 あとがき

情報セキュリティ対策についての基本的な考え方と，それに沿った解決策として，当社のセキュリティソリューションについて述べた。今後，セキュリティに対する脅威はますます高度・強大化し，顧客のセキュリティに対する要望（ニーズ）は，それに伴い多様化していくものと思われる。

当社は，今後も，より安心できる企業・組織作りに役だつソリューションを提供していく。

文　献

⑴ （財）日本情報処理開発協会（JIPDEC）．ISMS認証基準（Ver.2.0）．
⑵ 日本規格協会．JISハンドブックマネジメントシステム．
⑶ （財）日本規格協会．情報技術－情報セキュリティマネジメントの実践のための規範 JIS X 5080.

河井　宣之　KAWAI Nobuyuki

東芝ソリューション（株）プラットフォームソリューション事業部プラットフォームソリューション第三部参事。情報セキュリティ関連コンサルティング及び情報セキュリティシステムの構築に従事。

Toshiba Solutions Corp.