情報セキュリティマネジメントシステム

Information Security Management System

椎木　孝斉　■ SHIIGI Takayoshi
石橋　雄一郎　■ ISHIBASHI Yuuichiro
井口　寛　■ IGUCHI Hiroshi

企業や組織の活動が，インターネットを含むネットワーク利用を前提としたものになっている現在，“情報セキュリティ”はますます重要なものになってきている。情報セキュリティへの取組みは，企業や組織全体として体系的かつ効果的に行う必要があり，“情報セキュリティマネジメントシステム（ISMS：Information Security Management System）”の確立が重要となってきている。

東芝は，情報セキュリティを企業の経営課題の一つとしてとらえ，ISMSの確立，導入，維持改善につながる各種サービスを展開している。

Information security has become much more important in today's networked society, where most organizational activities rely on information and communication technology (ICT)-based networks including the Internet. It is important for such organizations to deal with information security more systematically and effectively on the corporate level by establishing information security management systems (ISMS).

Toshiba regards information security as a key management concern, and is developing a wide range of services for the establishment, implementation, maintenance, and improvement of ISMS.

1 まえがき

Webページの改ざんや，ウィルス，個人情報漏えいなど，企業や組織は，“情報セキュリティ”に関する大きなリスクにさらされている。ネットワーク社会においては，これらのリスクが顕在化し，ひとたび事件や事故が発生すれば，たちまち企業や組織全体にわたってダメージを受けることになる。そのため，今や情報セキュリティは，ファイアウォールや侵入検知システムといった個別の対策だけで対応するのではなく，企業や組織全体のマネジメント（経営）の問題として取り組む必要がある。

企業や組織全体の課題として情報セキュリティをとらえるときに重要となるのが，“ISMS”という考え方である。

東芝は，このISMSに関連するサービスを積極的に進めており，ここではその概要と特長について述べる。

2 ISMS

ISMSを考える場合には，ISMSを情報セキュリティとマネジメントシステムに分けて考えるとわかりやすい。

まず情報セキュリティであるが，ISMSで対象としている“情報”とは，情報システムなどに電子的に保存される情報だけでなく，紙の文書や会話によるものなど広く企業や組織に存在する情報を対象としており，これらを企業や組織における資産，すなわち“情報資産”として考える。そして，これらの情報資産に対して，情報セキュリティ，すなわち“機密性”，“完全性”，“可用性”を確保することを目的としている。

次にマネジメントシステムであるが，これは情報セキュリティを企業や組織のマネジメントの課題としてとらえ，個別の対策ではなく，企業や組織として総合的かつ有効な対策を実施することを意味する。その際目標とするセキュリティレベルとしては，絶対的なレベルが存在するのではなく，企業や組織みずからがリスクを分析し，その企業や組織で独自の達成目標を定める。更に，情報セキュリティを継続的に改善が必要なプロセスとしてとらえ，ISMSの導入や維持・改善を図っていく。このプロセス改善アプローチは，いわゆるPDCAサイクル（Plan（計画）→Do（実施）→Check（点検）→Act（処置））を回していくことである。プロセス改善アプローチによるマネジメントシステムとしては，ほかにも品質マネジメントシステム（QMS）や環境マネジメントシステム（EMS）などが存在するが，ISMSはそれらの情報セキュリティ版ととらえることもできる。

情報セキュリティマネジメントは，2002年に改定された経済協力開発機構（OECD）のセキュリティガイドライン[(1)]においても原則の一つに位置づけられており，昨今の情報セキュリティにおける重要な取組みの一つとなっている。

QMSにはISO9000シリーズ，EMSにはISO14000シリーズといった国際規格が存在するように，ISMSに関する国際

規格としては“ ISO/IEC17799 ※注1)という規格が存在する。ISO/IEC17799は，英国規格であるBS7799を基に作られたものである。BS7799は，BS7799-1とBS7799-2から構成され，BS7799-1は情報セキュリティマネジメント実践規範として，ISMSを確立，維持していくために必要なベストプラクティスを集めたガイドラインとなっている。また，BS7799-2は情報セキュリティマネジメントシステム仕様で，この規格に基づくISMSの認証を行う際の基準となっている。

現在，ISO/IEC17799として規格化されているのはBS7799-1に相当する部分のみで，認証基準であるBS7799-2に関してはISOの規格とはなっていない。

ISO/IEC17799では，ISMSとして管理すべき領域を10の領域に分けている(**図1**)。図からわかるとおり，従来情報セキュリティとしてとらえられていた範囲と比較して非常に幅広い範囲が対象になっている。

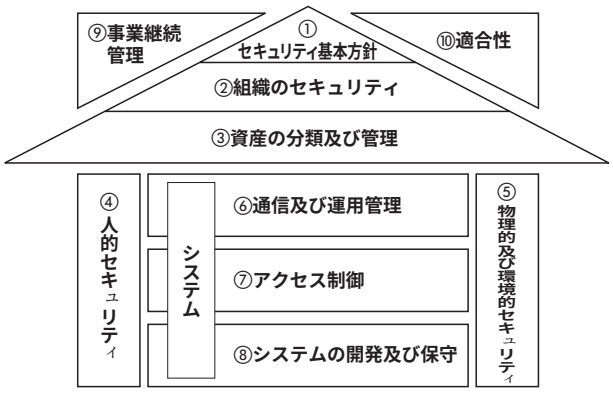

図1．ISMSにおける管理領域 ― 10の管理領域が設定されている。
Security domain of ISMS

ISO/IEC17799では，図1に示した10の管理領域に対して36の管理目的を定め，全体で127の管理策を設けており，企業がISMSを確立する際のガイドとして利用されることを想定している。

一方，特定の企業や組織が，適切なISMSを確立，導入，維持・改善を図っていることを認証するための基準は，前述のとおり現状では国際規格とはなっていない。現在のISMSに関する認証基準としては，英国規格であるBS7799-2と日本情報処理開発協会(JIPDEC)によるISMS適合性評価制度[(2)]のISMS認証基準があり，それぞれ企業や組織が確立したISMSの認証が行われている。既に多くの企業が認証を取得しており，東芝グループにおいても，東芝を含めたグループ企業の情報通信インフラサービスを提供している部門で，BS7799-2の認証を取得している。

(注1) ISO/IEC 17799は，JIS X 5080としてJIS化されている。(ISO：国際標準化機構，IEC：国際電気標準会議)

3 東芝のISMS関連サービス

3.1 東芝情報セキュリティサービスの概要

ISMS関連サービスをはじめとする，東芝の情報セキュリティサービスでは，“ 診断からのアプローチ ”と“ 企業経営サイクルと情報システムサイクルとの融合 ”をキーワードとして取り組んでいる。

診断からのアプローチとは，まず診断によりお客さま自身の現状を可視化し，そこを出発点とすることで，お客さまにもっともふさわしいサービスを提供するということである。

次に企業経営サイクルと情報システムサイクルの融合とは，情報セキュリティポリシーをトップとした企業や組織のマネジメントとしての情報セキュリティのサイクルと，個別具体的な情報システムのセキュリティ対策のサイクルとの整合性をとり，両者を融合した形で企業や組織のセキュリティを実現するということである(**図2**)。

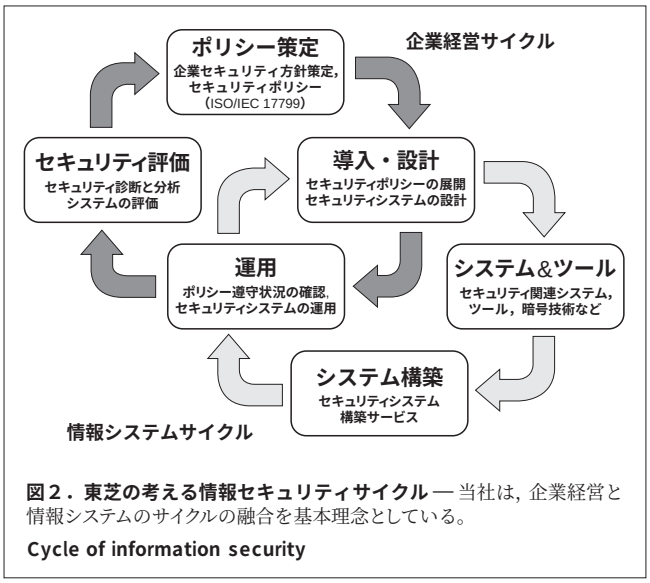

図2．東芝の考える情報セキュリティサイクル ― 当社は，企業経営と情報システムのサイクルの融合を基本理念としている。
Cycle of information security

ここでの企業経営サイクルとは，まさしくISMSにおけるPDCAサイクルにほかならず，個別のセキュリティ対策は情報セキュリティポリシーや各種基準など，マネジメントの観点から導き出されるものであることを示している。

以下では，当社の個々のISMS関連サービスについて述べる。

3.2 企業セキュリティ初期診断サービス

“ 企業セキュリティ初期診断サービス ”は，問診票に基づき企業や組織全体のセキュリティへの取組みを簡易的に診断するサービスであり，お客さま企業や組織がマネジメントの問題として情報セキュリティをとらえる第一歩としてもらうためのサービスとして位置づけている。

このサービスでは，お客さまにISMSをベースとした組織，

人，物理環境，システムに関連する約50項目の質問に答えてもらい，その回答結果を基に当社で診断，評価し報告する。問診票ベースのサービスは他社にも存在するが，当社では，以下の点を特長としてサービスを実施している（**図3**）。

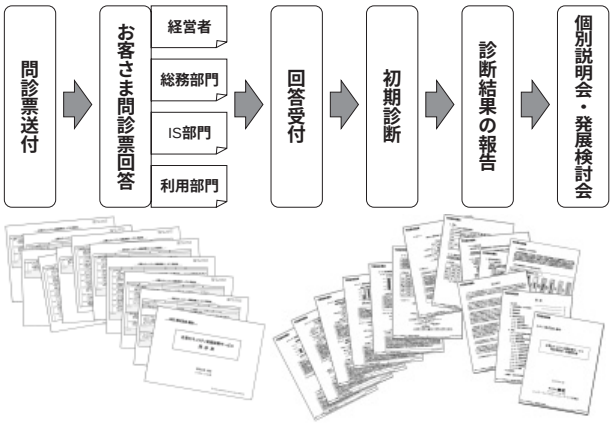

図3．企業セキュリティ初期診断サービスの流れとサンプル―お客さま4部門から問診票の回答を得て，診断結果をまとめて報告する。

Flow and sample of corporate security initial assessment service

⑴　お客さま企業や組織の経営層，総務部門，情報システム部門，利用部門の4部門から回答を得て，それぞれの部門のISMSに関する現状認識を明らかにし，その内容や部門間の認識ギャップに対して評価判断を行う。

⑵　いくつかの基準レベルを設定し，お客さま企業や組織のセキュリティ管理に対する意識レベルと，国際規格で求められる基準とのギャップを明らかにするとともに，他社との比較により，お客さまの意識レベルの相対的な位置を確認してもらうことができる。

⑶　お客さまの課題を可視化して診断結果報告書としてまとめ，お客さまに結果を説明する“個別説明会”を実施する。診断報告書及び個別説明会においては，診断後のセキュリティ対策におけるポイントなどのアドバイスも併せて行い，お客さまのそれぞれの事情に応じたほかのサービスに連携させることができる。

3.3　情報セキュリティポリシー策定サービス

ISMSのいちばんの基本であり，基礎となるのが情報セキュリティポリシーである。情報セキュリティポリシーは企業や組織のトップみずからが積極的に関与して作成する必要があり，また企業や組織がそれぞれの現状を把握し，みずからのリスクを分析したうえで策定することが重要である。このポイントが守られないと，実際に情報セキュリティポリシーを導入することが困難となったり，現実的ではない不適切な情報セキュリティポリシーを導入したりすることになる。

当社の“情報セキュリティポリシー策定サービス”は上記のポイントを大切にし，単にポリシー文書をつくるのではなく，現実的なセキュリティのレベルアップや具体的な対策実現につながる情報セキュリティポリシーを策定するためのサービスを行っている。

策定にあたっては，ISO/IEC17799などの国際規格に準拠するとともに，お客さまの要望に応じて，次節で述べるISMS認証取得にも対応できる形でのサービスを提供している。

また情報セキュリティポリシー策定は，企業や組織のISMSを確立するための出発点である。そこで，情報セキュリティポリシーの策定を行うことで，企業や組織のISMSにおけるリーダーを育成するコースも用意している。

3.4　ISMS認証取得支援サービス

BS7799-2やJIPDECのISMS認証基準に基づく認証取得を支援するサービスが“ISMS認証取得支援サービス”である。このサービスにおいては，情報セキュリティポリシー策定，リスク分析，リスク管理といったISMSの確立に最重要なポイントを支援することはもちろんのこと，審査ポイントのアドバイスや，認証取得で重要となる文書化されたISMSの実現へ向けて，必要なドキュメントの作成支援なども実施する。

BS7799-2は2002年9月に改訂され，JIPDECのISMS認証基準もそれに合わせて2003年4月にバージョン2.0が制定された。改訂にはいくつかの重要な変更点も存在しており，今後はこれら最新の認証基準に基づくサービスの提供を行っていく。

3.5　情報セキュリティ教育サービス

情報セキュリティの問題の大部分は，最終的には人の問題に帰着される。すなわち，情報セキュリティを考えるうえでもっとも重要な問題が人の問題であると言える。たとえ企業や組織に情報セキュリティポリシーがあったとしても，それが確実に導入され，関係者の間に周知徹底されなければ，それは企業や組織にとって意味のないものとなってしまう。そこで重要となるのが，情報セキュリティ教育である。

当社では，情報セキュリティ教育として以下のコースを用意している。

⑴　一般基礎・基本教育コース　　情報セキュリティポリシーの有無にかかわらず，セキュリティにかかわる基礎知識，基本ルール，マナーについて，事例を含めて学ぶコース

⑵　ポリシー前提の基本心得コース　　策定済み又は策定中のポリシーを前提にして，最低限周知徹底すべき基本精神や基本心得をわかりやすく学ぶコース

⑶　ポリシーの周知徹底コース　　策定済み又は策定中のポリシーの全文公開を含め，ポリシー規定事項，関連規定・ルールを関係者全員がわかりやすく学ぶコース

情報セキュリティポリシーに関する教育では，特に全社員

及び関係者に行うことが重要となるため，教育の実施形態としては，運用管理面やコスト面から，e-Leaningによる方法が最適であると考えている。

3.6　システムセキュリティ診断サービス

情報システムに存在するセキュリティホールなどの脆弱（ぜいじゃく）性を検査するサービスが“システムセキュリティ診断サービス”である。システムセキュリティ診断サービスは，ISMSにおいて様々な観点で利用することができる。例えば，以下のような観点で用いることができる。

⑴　セキュリティポリシー策定時の現状分析
⑵　新規システム構築時の検証
⑶　ISMSのCheck段階における確認

当社のシステムセキュリティ診断サービスは，当社の自社実践に裏打ちされており，以下のような特長のあるサービスを実施している。

⑴　ツールに業界最大手のISS社（Internet Security Systems Inc.）のInternet Scanner(注2)を採用し，その上に当社の独自ノウハウを付加
⑵　お客さまの実際の課題を解決するための手段として，診断目的の事前確認，現地での診断，及びお客さまの目的に合わせた診断レポート作成を実施

上記により，お客さまの課題の詳細を明らかにし，その後のお客さまのセキュリティレベルアップ実現につながるサービスを実施している。

4　あとがき

企業や組織の情報セキュリティへの取組みを包括的にとらえたアプローチであるISMSは，今後ますます重要性が高まってくると考えられる。

ISMSに関連して，2003年4月からは“情報セキュリティ監査制度”(3)といった新しい制度の運用も始まり，またISO/IEC15408(注3)に基づくIT（情報技術）セキュリティ評価・認証プログラム(4)の運用も本格化しつつあるなど，様々な動きも出てきている。

当社としては，今後も企業経営の視点を重要なポイントとして位置づけ，企業や組織全体の実質的なセキュリティの向上を図るために，お客さまのISMSの確立，導入，維持・改善を支援する各種サービスを提供していく。

文　献

⑴　OECD. Guidelines for the Security Information Systems and Networks – TOWARDS A CURTURE OF SECURITY. ＜http://www.oecd.org/pdf/M00034000/M00034292.pdf＞, (accessed 2003-05-06).
⑵　日本情報処理開発協会. 情報セキュリティマネジメントシステム（ISMS）適合性評価制度. ＜http://www.isms.jipdec.or.jp/＞,（参照 2003-05-06）.
⑶　経済産業省. 情報セキュリティ監査制度の運用開始について. ＜http://www.meti.go.jp/policy/netsecurity/information_audit.html＞, (参照 2003-05-06).
⑷　製品評価技術基盤機構. ITセキュリティ評価・認証プログラム. ＜http://www.nite.go.jp/asse/its/jisec-index.htm＞,（参照 2003-05-06）.

（注2）Internet Scannerは，Internet Security Systems Inc.の米国における登録商標。
（注3）IT製品やシステムの評価に関する国際基準。

椎木　孝斉　SHIIGI Takayoshi
e-ソリューション社　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担当主務。情報セキュリティサービスの開発に従事。情報処理学会会員。
Platform Solutions Div.

石橋　雄一郎　ISHIBASHI Yuuichiro
社会ネットワークインフラ社　システムコンポーネンツ事業部　ターミナル機器営業部主務。セキュリティシステム・サービスの開発に従事。
System Components Div.

井口　　寛　IGUCHI Hiroshi
e-ソリューション社　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担当主務。情報セキュリティサービスの開発に従事。電子情報通信学会会員。
Platform Solutions Div.