

# 三菱情報セキュリティソリューション

勝山 光太郎\*  
小松田 敏二\*\*  
飯島 康雄\*\*\*

## 要 旨

インターネットを代表とするいわゆるIT化の進展により、企業はビジネスリスクの一つとして、ITリスクとりわけ情報セキュリティリスクを考慮した経営を迫られている。

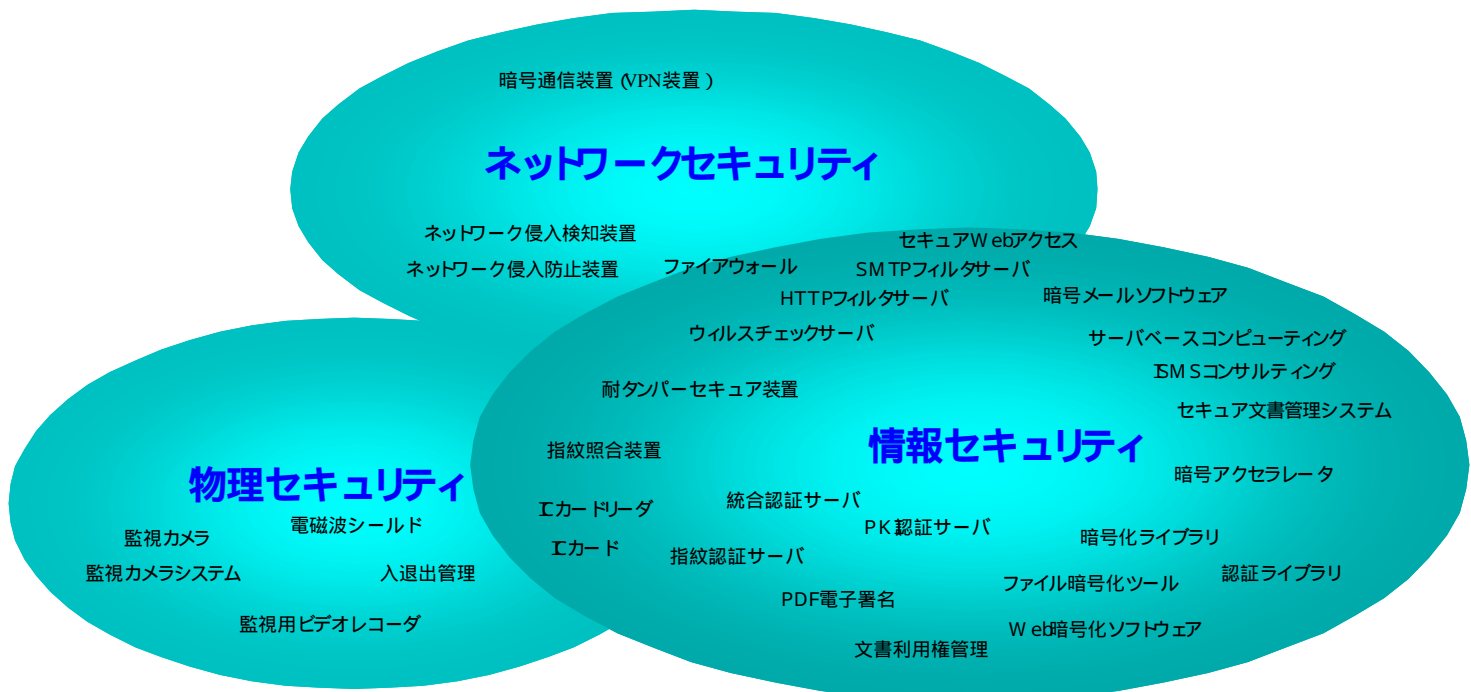
近年、マスコミで取り上げられることが多くなってきている個人情報の漏洩事件や、MS-Blaster などのウイルスにより情報システムがダウンするなどのリスクをどうコントロールしていくかが重要となる。さらに、法制度の面では、個人情報保護法や不正競争防止法において、情報の管理責任という意味で情報セキュリティ対策の実施がうたわれている。

情報セキュリティ対策を実施し、情報資産を守るためにはいくつかの側面があり、単に技術的側面だけでなく、設備や運用といった側面からもトータルにセキュリティ対策を実施することが求められている。経済産業省が2000年10月に発表した「情報セキュリティ総合戦略」においても、

こうした観点から、ISMS（情報セキュリティマネジメントシステム）やセキュリティ監査の重要性が述べられている。

三菱電機グループでは、情報セキュリティ、ネットワークセキュリティ、物理セキュリティを連携させたトータルな取り組みをしており、お客様のニーズにあったトータルセキュリティソリューションを提供している。本誌2002年4月号<sup>(1)</sup>では“情報セキュリティ技術”を中心に、2003年4月号<sup>(2)</sup>では“ユビキタス社会に向けたセキュリティへの対応”を紹介してきたが、本特集号では“情報セキュリティソリューション”に焦点を当てて紹介する。

“情報漏洩防止ソリューション”や“公開鍵基盤PKI（Public Key Infrastructure）による認証サービス”など、安全・安心を支える多彩なソリューションがあり、経営リスクに対応した体系的対策・運用を可能としている。



## 三菱電機のトータルセキュリティ

三菱電機(株)は、情報セキュリティ、物理セキュリティ、ネットワークセキュリティのいろいろなコンポーネントを組み合わせ、お客様のニーズにあったセキュリティソリューションをトータルに提供する。

\*三菱電機(株) 情報技術総合研究所 情報セキュリティ技術部長

\*\*三菱電機(株) インフォメーションシステム事業推進本部 情報セキュリティ推進センター長

\*\*\*三菱電機インフォメーションシステムズ(株) インターネットビジネスシステム部 インターネットセキュリティセンター長

## 1. まえがき

インターネットを代表とするいわゆるIT化の進展により、企業はビジネスリスクの一つとして、ITリスク、とりわけ情報セキュリティリスクを考慮した経営を迫られている。

個人情報の漏洩事件では、企業に対する損害賠償請求が起きたり、経営者の責任が問われることになる。また、MS-Blasterなどのウイルスにより情報システムがダウンするなどのリスクや、ネットワークからの不正侵入などのリスクは増大の傾向にある。

また、法制度はシステムの運用管理者や、データの利用者に責任を負わせる方向になってきている。

従って、体系的に情報セキュリティ対策を導入し運用するために、ISMS（情報セキュリティマネジメントシステム）を実施し、認定をとる企業も増えてきている。こうしたセキュリティ意識の高まりを背景に、本特集号では、安全・安心を支えるITソリューションと題し、三菱電機グループが取り組む、情報セキュリティや物理セキュリティに関していくつかの例を紹介している。採録されている論文の中には、直接セキュリティに関連するものもあれば、セキュリティや高信頼に配慮したソリ

ューションとして紹介しているものもある。

2章では、最近のセキュリティに関するトラブルの例をとりあげ、3章では世の中の動きとして、OECD（世界経済協力機構）の情報セキュリティガイドラインや法制度、特に個人情報保護法及び不正競争防止法に関して述べる。4章ではISMS（情報セキュリティマネジメントシステム）、5章では当社のトータルセキュリティについて述べ、6章では情報セキュリティソリューションの中のいくつかの事例を紹介する。

## 2. 情報セキュリティに関するトラブル

情報セキュリティに関するトラブルは、セキュリティの3要素（機密性、完全性、可用性）と関連づけると以下ようになる（表1）。

- (1) 機密性  
機密情報漏洩、個人情報漏洩、不正アクセス
- (2) 完全性  
ホームページ改ざん
- (3) 可用性  
DoS攻撃(サービス不能攻撃)、ウイルス・ワーム

表1. 情報セキュリティにかかわるトラブルの事例

要素	時期	対象	トラブル内容
ホームページ改ざん	2001/1	日本政府	科学技術庁、総務庁、総合研究開発機構(NIRA)、運輸省のWebサイトが相次いで改ざんされた。
	2003/3	米企業等	イラク攻撃に従い、米国のWebサイトを中心に大量の改ざん。日本国内でも数例の事例。
不正アクセス	2002/2	宇宙関連	超高速インターネット衛星の受注にあたり、ライバル会社の機密情報を不正に入手。
	2002/8	宇宙関連	愛知県知立市の会社員所有のパソコンを踏み台にしたクラッキングを受けた。
ウイルス・ワーム	2001/7	全世界	'Code Red'ウイルス
	2001/9	全世界	'NIMDA'ウイルス
	2003/1	全世界	'SQL slammer'による被害。韓国では一時、インターネットに障害も。
	2003/8	全世界	'MS-Blaster'ウイルス
DoS攻撃	2002/10	Root DNS Server	DoS攻撃を受け、13台のRoot DNS Serverのうち、9台が機能低下。
機密情報漏洩	2002/8	防衛	防衛庁システムの開発資料の一部が流出。
個人情報漏洩	1999	個人	宇治市で住民基本台帳の記載事項が流出。
	2002/5	美容	約37,000人の個人情報が流出。
	2002/5	製造	約45,000人の個人情報が流出。
	2002/8	食品	約50,000人の個人情報が流出。
	2002/11	証券	約11,000人の個人情報が流出。
	2002/11	個人	ウイルスにより、茨城県つくば市が運営するメーリングリストから個人メールアドレスが流出。

DoS :Denial of Service , DNS :Domain Name System

### 3. 世の中の動き

#### 3.1 OECD情報セキュリティガイドライン

2002年にはOECDより情報セキュリティガイドラインが出され、その中では主に次のことが述べられている。

- (1) 情報システム及びネットワークを保護する手段として、すべての参加者の間にセキュリティの文化を普及させること。
- (2) 情報システム及びネットワークに対するリスク、それらのリスク対処のために有効な方針、実践、手段及び手続きならびにそれらの導入及び実施の必要性について、認識を高めること。
- (3) すべての参加者の間に情報システム及びネットワーク利用の形態における一層大きな信頼を醸成すること。

#### 3.2 個人情報保護法及び不正競争防止法

法律がシステム運用者やデータ利用者に責任を負わせる方向になってきている。

具体的には、個人情報保護法では、以下のような条項があり、何らかのセキュリティ対策実施を義務付けている。

##### 個人情報保護法 第20条（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏洩、滅失または棄損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

また、不正競争防止法でも以下のような条項があり、何らかのセキュリティ対策が必要となる。

##### 不正競争防止法 第14条（罰則）

（2003年の改正：営業秘密侵害に関する刑事罰の導入）

秘密漏洩に対する対策を講じている企業から、営業秘密を不正競争目的で取得・使用・開示する行為に対し、刑事罰（親告罪）を導入する（但し、秘密漏洩に対する対策を講じていない企業は、対象外）。

ここでいう営業秘密は、秘密管理性、有用性及び非公知性という3要件をすべて満たす必要がある。秘密管理性の判断基準として以下の点がある。

- (1) 当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること。
- (2) 当該情報にアクセスできる者が制限されていること。つまり、何らかの認証とアクセス制御が必要ということである。

#### 4. ISMS（情報セキュリティマネジメントシステム）

3章で触れた法律にもあるように、何らかのセキュリティ対策をすることが義務付けられているが、どこまでどのようにしたらよいか分からないという企業が多いのが現状であろう。

そこで、セキュリティ監査を実施し、ISMSを構築し

実践していくのが、大多数の企業がとる道と思われる。

情報セキュリティマネジメントの実施サイクルを図1に示す。基本方針や目標、実施規定、実施手順などを策定する。それを実際に導入する。そこでは教育や実際の対策（人的な面、設備的な面）を実施する。さらに運用では、実際に規定や基準通りに運用されているかを監視し、事故があった場合には決められた対策を実施する。そして内部監査等で実施状況を評価し、見直しを実行し、より高いセキュリティレベルへと向上して行くサイクルとなる。

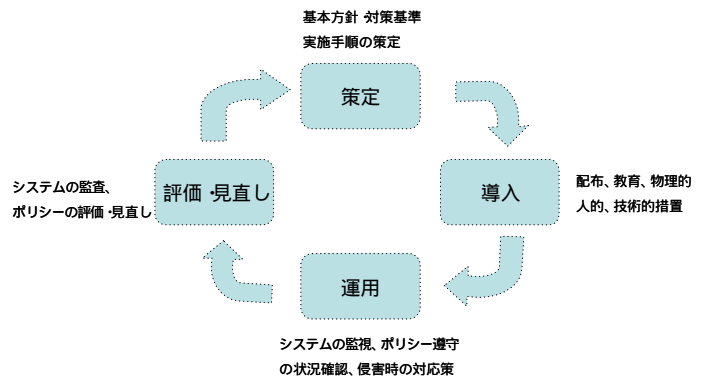


図1. 情報セキュリティマネジメント実施サイクル

### 5. 三菱電機のトータルセキュリティ

三菱電機(株)では、要旨イメージ図に示すように、単に情報セキュリティのソリューションのみならず、物理セキュリティ及びネットワークセキュリティを、総合電機メーカーである特色を活かし、トータルに提供している。本章では、物理セキュリティとネットワークセキュリティについて簡単に触れ、6章で情報セキュリティソリューションのいくつかを紹介する。

#### 5.1 物理セキュリティ

物理セキュリティのコンポーネントとしては、本来建物への侵入を監視するなどの防犯や、広域の状況監視などに利用される監視カメラや監視用ビデオレコーダなどの製品がある。盗聴防止といった観点から、電磁波の漏洩を防止するペルセウスシールドといった製品もある。

ビルやオフィスなどの入退出管理では、ICカードや指紋認証などを利用した製品がある。特にビル向けの製品であるMELSAFETYは、高いシェアを持っている。

#### 5.2 ネットワークセキュリティ

##### (1) 暗号通信装置（VPN装置）

VPN（Virtual Private Network）装置は、IPSECv2

（Internet Protocol Security Version2）準拠で、暗号アルゴリズムとして米国標準暗号/認証アルゴリズムに加え、MISTY<sup>(注1)</sup>、Camellia<sup>(注2)</sup>をサポートしており、さらに暗号アルゴリズムのカスタマイズの要求にも応

えられる。

## (2) IDS装置

IDS (Intrusion Detection System) 装置は、ファイアウォールなどと組み合わせ、ネットワークからの不正侵入を検知し、防御する。侵入パターンであるシグニチャを管理装置から一元的に更新できるなどの特長がある。

## (3) マネージドセキュリティサービス

セキュリティは構築して完了ではなく、むしろ、スタートである。日々のセキュリティ監視、新たな脆弱性への対応、システム変更時のセキュリティチェックなどによって、セキュリティは維持される。三菱電機情報ネットワーク(株)(MIND)は調査分析から、設計、導入、運用・監視及び評価というサイクルに対応したトータルなマネージドセキュリティサービスを提供している(図2)。米国 RedSiren Technologies 社(旧 SRI コンサルティング社)との提携等で常に最新情報をサービスに反映し、24 時間 365 日の統合管制センター ICC (Integrated Control Center) をベースに絶え間ないサービスを提供している。なお、MIND では BS7799-2 (情報セキュリティ管理システム仕様/認証規格) の認証を取得し、情報セキュリティマネジメントシステムの確立・維持によって、信頼されるサービスを提供している。以下に代表的なサービスを紹介する。

### (a) セキュリティ診断サービス

システムのセキュリティ状態を擬似攻撃によって診断する。三菱統合セキュリティ診断ツール (ISAT) を使用したクロスサイト・スクリプティングによる脆弱性チェックなど、Web アプリケーションまで踏み込んだ診断も行う。診断結果は検出した脆弱性の対策も提示している。

### (b) セキュリティ教育・情報サービス

初心者から専門家までに対応した総合的な情報セキュリティの e ラーニングサービスを用意している。また、日々公開されるセキュリティ情報を複数の情報ソースからシステム管理者に代わって対象システム要件を踏まえて収集、分析し、その対処と合わせて提示している。

### (c) 不正アクセス監視/インシデントレスポンスサービス

もはや、ファイアウォールだけではセキュリティを維持できなくなっているため、セキュリティホールへの攻撃を不正アクセス監視装置によって、24 時間監視を行う。万一の緊急事態発生時には、原因究明から対処までのインシデントレスポンスにも対応している。

## 6 . 情報セキュリティソリューション

情報セキュリティソリューションも各種存在するが、ここでは、個人情報保護法の関連で注目を集めている“情

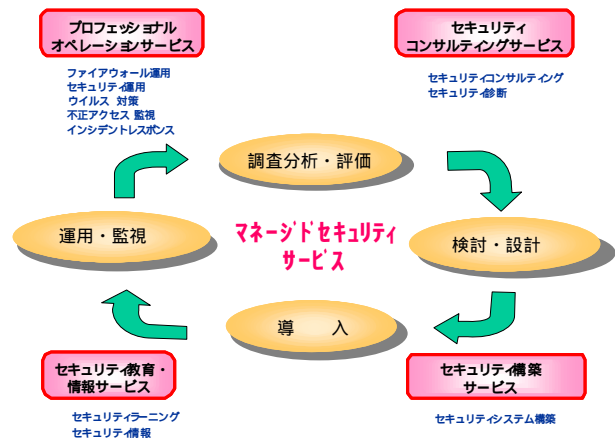


図2 . MIND マネージドセキュリティサービス

報漏洩防止ソリューション”、そして、公開鍵基盤 PKI についてヘルスケア分野を例として述べ、さらに、“セキュア Web ソリューション”を紹介する。

### 6 . 1 情報漏洩防止ソリューション

情報漏洩防止ソリューションの一構成例を図3に示し、その特長を以下に述べる。

#### (1) 利用者の統合的な認証

- 1 枚の IC カードですべてのシーンでの認証をカバー
- ・部屋に入るときは指紋認証
- ・PC を使うときはログイン認証
- ・ファイルにアクセスするときはデジタル認証

#### (2) 情報の保護

- 世界最高水準の暗号技術 MISTY でファイルを暗号化
- ・利用クライアントの情報保護 (ファイルの暗号化)
- ・共有サーバの情報保護 (サーバの暗号化、アクセス制御)
- ・コンテンツの情報保護
- ・ダウンロード後ファイルのコピー (カプセル化、外部出力防止)

#### (3) 簡単な導入・運用

- ・ユーザ認証情報の一括登録と IC カード発行
- ・ログ管理サーバでの一元管理
- ・ISMS 等認定取得のためのテンプレート

(注1) MISTY は、三菱電機(株)の登録商標である。

(注2) Camellia は、日本電信電話(株)と三菱電機(株)の登録商標である。

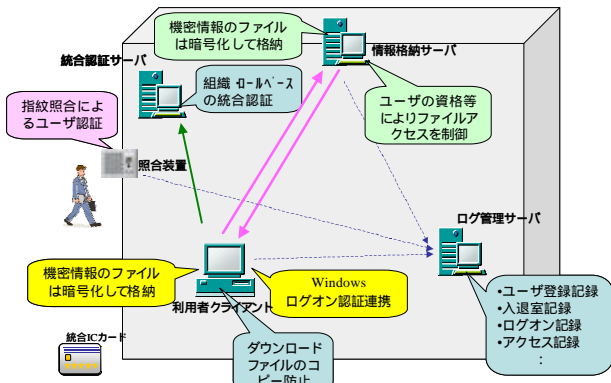


図3 情報漏洩防止ソリューションの構成例

### 6.2 公開鍵基盤 PKI

これまで、電子政府や電子自治体などで、GPKI (Government PKI)、あるいは LGPKI (Local Government PKI) として PKI 基盤が整備されてきている。一般にはブラウザを利用したアプリケーションでの SSL (Secure Socket Layer) の利用が進んできている。今後 PKI 基盤の整備が進む分野の一つにヘルスケア分野がある。ここではヘルスケアセキュリティにおける PKI 利用について述べる。

図4に示すように、今後ヘルスケア分野での電子化の促進に伴い、電子カルテ、処方箋、紹介状、レセプトなどに電子署名が必要となる。医療分野での PKI については、ISO17090 で標準化が進んでいる。

電子署名を実現するために、証明書の発行が必要となる。ジャパンネット(株) (Japan Net) は、PKI に基づく証明書の発行サービスをはじめ電子認証システムの運営管理サービス(ハウジング、ホスティング)等を提供している。証明書発行サービスについては、特定認証業務の公的認定を取得し、府省・自治体などが実施する電子調達参加者向けの証明書発行も行っている。

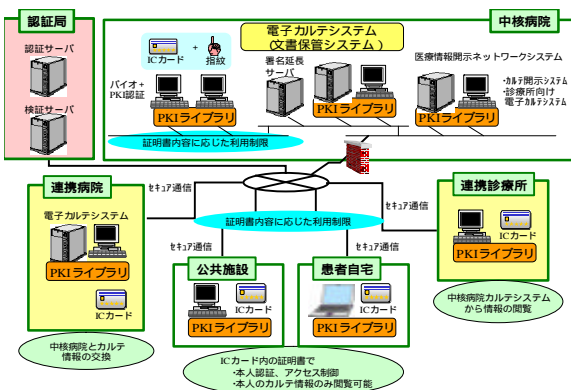


図4 ヘルスケアセキュリティ

### 6.3 セキュアWebソリューション

三菱電機インフォメーションシステムズ(株) (MDIS) では Web ベースシステムのセキュリティ上の課題を解決したり、情報システムにセキュリティ機能を即応するためのフレームワークとして、“セキュア Web ソリューション”を提供している。セキュア Web ソリューションは、人的・物理的な側面も含めた情報セキュリティシステムを構築支援する“セキュリティコンサルティング”、PKI 関連ライブラリを始めとする“セキュリティ基盤コンポーネント”、情報漏洩防止やセキュアな B2B 環境及びこれらの活用ノウハウを集積した“セキュリティ応用ソリューション”から構成される(図5)。



ISMS : Information Security Management System, CP : Certificate Policy, DWH : Data Ware House  
 CPS : Certification Practice Statement, PDF : Portable Document Format, PKI : Public Key Infrastructure  
 EDI : Electronic Data Interchange, ISO : International Organization for Standardization

図5 セキュアWebソリューション

### 7. むすび

三菱電機(株)のトータルセキュリティについて簡単に紹介するとともに、今回特集テーマである“安全・安心を支えるITソリューション”の情報セキュリティに関するいくつかの例を述べた。企業のIT化が進む中、ITリスクとりわけ情報セキュリティリスクを経営の中でどう取り組んでいくか、経営者の意識が問われる時代となっている。今後、ISMSを導入する企業が増えると予想されるが、そのセキュリティ対策のためのツールやサービスに、当社の情報セキュリティソリューションを積極的に提供して行きたい。さらに、技術の方向や標準化の流れ、法制度をにらみつつ、今後とも最適なセキュリティソリューションを提供していく所存である。

#### 参考文献

- (1) 三菱電機技報:特集“情報セキュリティ”,76, No.4, (2002)
- (2) 勝山光太郎,ほか:ユビキタスセキュアソリューション,三菱電機技報,77, No.4, 239~242(2003)