マネジメント最前線 ①

ITセキュリティー・システム構築へのアプローチ

日本アイ・ビー・エム株式会社
e-セキュリティー・オフィサー
IBMディスティングイッシュト・エンジニア
石垣　良信

Yoshinobu Ishigaki
e-Security Officer of AP/Japan
IBM Distinguished Engineer
IBM Japan, Ltd.

企業におけるIT（Information Technology：情報技術）セキュリティー・システムは、機密情報の物理的な保護を行う「物理セキュリティー」、社内外間の機密情報へのアクセス・伝送・運搬にかかわる「運用セキュリティー」に始まり、社内外からのインターネットの利用が開始されたことにより、クラッカーやコンピューター・ウィルス対策のための「ネットワーク・セキュリティー」と進化してきました。しかしながらインターネット・アプリケーションの高度化、ブロードバンドやモバイル環境の整備などにより、単に社内のイントラネットや社内機密情報を外部からの不正なアクセスから守るという発想だけでは、企業のセキュリティーは保護できなくなってきました。今後はさらに上位のセキュリティー管理層「システム・インフラストラクチャー・セキュリティー」「アプリケーション・セキュリティー」が重要になってくると思われます。

また、セキュリティーに関連して、最近話題になっているのがプライバシー（個人情報）の保護であり、それに対応する実際的なITセキュリティー・システムの構築が緊急の課題になっています。プライバシー対策が急がれている理由の一つは、個人情報への不正アクセスや流出・漏えいに関する事件が頻発していることです。その対策のキー・ポイントには「個人情報の棚卸し作業」「アクセス・ログの取得」「社員PC（Personal Computer）などのアセット管理」「パートナー管理の見直し」があり、これらがITセキュリティー・システム構築への短期的アプローチになります。もう一つ注意すべき点は、「個人情報保護関連5法」が2005年4月には施行されることです。これにより、企業などが個人情報を取り扱う場合は、利用の目的を公表し、その範囲内でのみ使用することなどが定められます。

Management Forefront—①

SPECIAL ISSUE: **Information Security and Privacy**

A Practical Approach to Information Security

An enterprise's Information Security system started to evolve from 'Physical Security' that provided physical protection of confidential information, 'Operational Security' that dealt with accessing, transmitting and transporting confidential information internally and externally. The business use of Internet mandated 'Network Security' that provided countermeasures against crackers and computer viruses.

However, due to the rapid Extranet application development, the wide use of broadband and mobile tools, the concept of managing information security by simply protecting internal network and servers from illegal external accesses became obsolete.

Higher-level security management layers, such as 'System Infrastructure Security' and 'Application Security' are becoming essential, where end-to-end access control is enforced in any of the enterprise applications by a set of enterprise policies.

'Privacy Protection' has become another big issue for most companies because of the nearing enactment of "Act for the Protection of Personal Information" in April, 2005. Among the many management practices for Privacy Protection, the prevention of personal information exposure is the topmost issue to be addressed. 'Creating a Master of Personal Database', 'Access Log Management', 'Asset Management and Security Violation Monitoring of Employee PCs' and 'Security Management with Partners' are the key tactics for effective implementation of the management system.

ITセキュリティー・マネジメント・システムとは？

今、リスク対応がIT部門の最重要課題に位置付けられ(“2004 IT Outlook”Nov.2003「北米818社調査結果」)、セキュリティー投資がITマネジャーの最優先課題に挙げられています(IDC's IT Manager Surveys, July 2003「北米999社調査結果」)。

一般に、リスク・マネジメントとセキュリティー・マネジメントは混同して使われるきらいがありますが、企業が取り組むべき姿勢には少なからぬ違いがあります。

リスク・マネジメントは、経営に影響を与えるあらゆるリスクを対象として、包括的に対処できるマネジメントを指向するものです。具体的な施策には、危険分散、他責事項の徹底、損失の回避などがあり、財務的な発想も求められます。

一方、セキュリティー・マネジメントは、“安全”の概念でとらえるべきリスクを対象とし、安全対策、自責事項の徹底、信頼醸成などの保護策の有効性を指向するもので、具体的には脆弱性対策を中心に据えています。脆弱性とは、脅威(地震など自然の脅威、故障など技術の脅威、クラッカー、不誠実社員など人間の脅威)の発生を誘引する情報システム固有の弱点(人間系の弱み、セキュリティー・ホールなどの仕組みの弱点を含む)のことです。今日のセキュリティー・マネジメントでは、脅威が顕在化して情報資産にさまざまな影響が出る前に、脆弱性のある部分をきちんと識別・評価し、補強していくことが重要になっています。

包括的な情報セキュリティー・マネジメントの基準は1992年のOECD(Organization for Economic Cooperation and Development:経済協力開発機構)による9原則が最初といわれ、2002年には新しい9原則に改訂され、2003年にはISMS(Information Security Management System)適合性評価基準、情報セキュリティー監査基準なども発表されています。

OECD情報セキュリティー・ガイドライン改訂版では、(1)認識の原則 (2)責任の原則 (3)応答の原則 (4)倫理の原則 (5)民主主義の原則 (6)リスク評価の原則 (7)セキュリティーの設計および実装の原則 (8)セキュリティー・マネジメントの原則 (9)再評価の原則といった9原則が掲げられていますが、これらは単なる原則論にとどまるものではありません。基準がより明確になるとともに、現代のシステム環境に合わせた合理的かつ実践的な内容になっています。

いかなる基準や制度を用いる場合でも、IT(Information Technology:情報技術)セキュリティーを向上させるには、組織内に明確な方向性を示し、その目標に向け、さまざまな階層において漏れや考え方の相違がないように確実に遂行していくことが重要です。その意味で、この9原則の順守は一見遠回りのように思えますが、企業のセキュリティー・マネジメント・システム確立への近道の一つであり、コツといえましょう。

今後のITセキュリティー・システムに求められる機能

ここで、**図1**と**表1**をご覧ください。図1は企業におけるITセキュリティー・システムを概観したものであり、表1はその構成を層別に整理したものです。この層別は、下層から上層へと順番にセキュリティー・システムの上位管理層を示すと同時に、歴史的な経緯を示したものにもなっています。図1は企業におけるセンター・システムを中心に表示していますが、PC(Personal Computer)などのクライアントやネットワークでも同様なセキュリティー管理層が存在することに注意してください。

企業における情報セキュリティー対策は、バックアップ・センターを建設するといったように、まず盗難などから情報資産を防ぐ物理的な囲いを作ってしまうことから始まりました。次に盛んに取り組まれたのが入退室管理や社員のID／パスワード管理などの運用面でのセキュリティーですが、これは実用に際して人間の企業活動全般にかかわる難しい問題が多々あり、今日でも大きな課題であり続けています。そしてインターネット時代になって、マスコミなどの話題の中心となっているのがネットワーク・セキュリティーであり、悪意を持ってシステム内に侵入してくるクラッカーやコンピューター・ウィルスによるサイバー攻撃に対して、どの

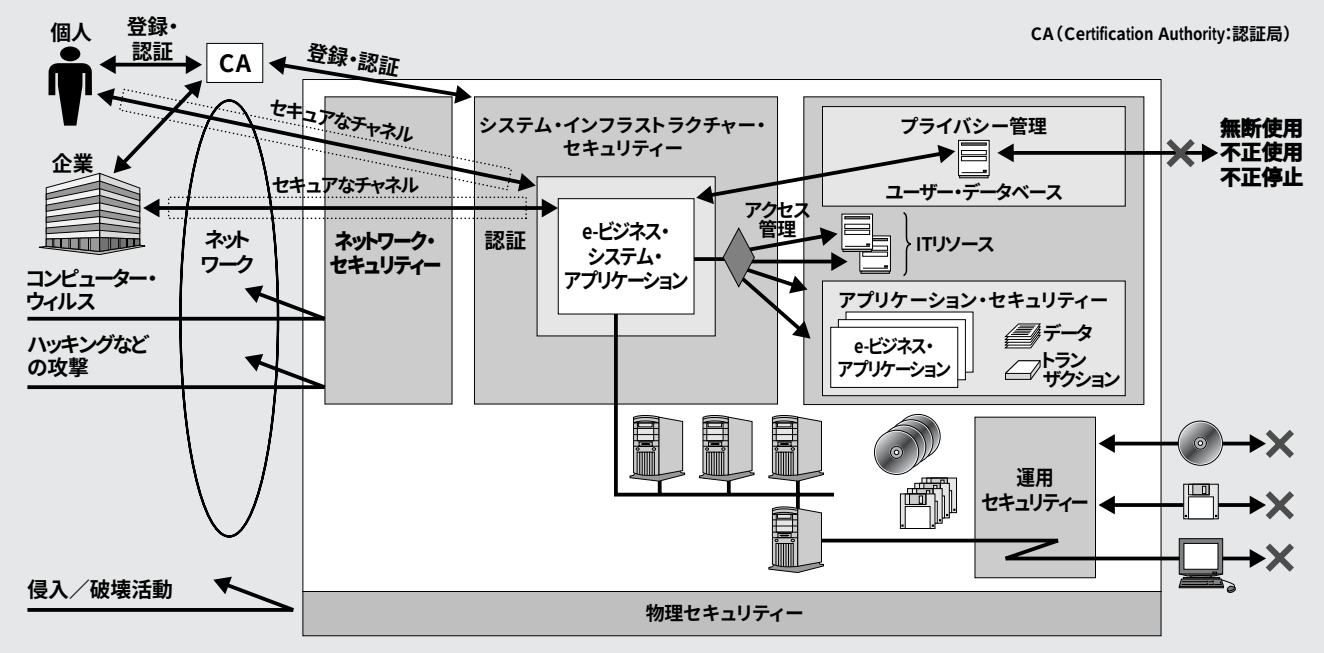

図1. ITセキュリティー・システム概観（センター・システム中心）

表1. ITセキュリティー・システム構成とその中期／短期アプローチ

e-ビジネス ITセキュリティー・システム層	セキュリティー・システムの目的	対象とする脅威や危険	どのような仕組みで守ろうとするか	サブシステムやコンポーネント名	
プライバシー管理	ユーザーのプライバシー情報を保護する	・プライバシー情報の漏れ ・プライバシー情報の不正使用や不正修正	・プライバシー情報のアクセスを監視・制御する	・プライバシー情報管理システム ・プライバシー監査システム	今後
アプリケーション・セキュリティー	ユーザーとデータ内容のアクセス・コントロールを正しく運用する	・データの不正使用 ・機密情報の漏れ	・アプリケーション・ロジックの作成／パッケージ使用 ・DBMS（Database Management System）のデータ機密保持管理	・アプリケーション・セキュリティー ・パッケージ・ソフトウェア・セキュリティー ・データ機密保持管理	
システム・インフラストラクチャー・セキュリティー	ユーザーとリソース間のアクセス・コントロールを正しく運用する	・ITリソースの不正アクセス ・不正取引 ・しらばくれ ・“ 成りすまし ”	・ユーザーを特定する ・ユーザーのリソースへのアクセスを制御する	・ディレクトリー管理システム ・認証システムとCA ・リソース・アクセス管理 ・システム・フロー制御	
ネットワーク・セキュリティー	ITシステムへのネットワークから（特にインターネットから）の不正アクセスを排除する	・ハッキング／クラッキング ・コンピューター・ウィルス ・DOS攻撃	・プロトコル／ポートの制限 ・侵入の検知 ・コンピューター・ウィルス検知とワクチン投与	・DMZ（Demilitarized Zone）／Secure Zones ・侵入検知システム ・コンピューター・ウィルス検知システムとワクチン	企業の現状
運用セキュリティー	ITシステムを運用するときにセキュリティー問題が発生しないこと	・媒体・ソフトウェアなどの不正交換やコピー、持ち出し ・電子メールによる情報漏れ	・運用体制や手順の確立と実施 ・入退館をコントロールし記録する	・媒体管理 ・入退館管理 ・開発／運用体制	
物理セキュリティー	ITシステムや媒体・端末などの物理的な保護や回復	・物理的な破壊 ・盗難	・セキュアな施設・装置を用意	・施設構築 ・バックアップ・センター	

ように企業情報資産を守るかが問題となっています。

しかし、ネットワーク・セキュリティーに注力し、ユーザー認証などの新しい仕組みを導入しても、ITリソースへの不正アクセスが減少する兆しはありません。むしろ最近の機密情報漏えいにかかわる事件の大半は社員やパートナー企業など社内に原因があると報告されています。アクセス権限を持っている人がひとたびシステム内に侵入すれば、悪意のあるなしにかかわらず何でもできてしまうところに現在のセキュリティー上の根本的な脆弱性があるのです。

そこで、今後のITセキュリティー・システムにおいて最も注目されているのがシステム・インフラストラクチャー・セキュリティーです。ユーザーとリソース（プログラムやデータ）間のアクセス関係をアプリケーション・プログラムに任せず、ITシステムのインフラストラクチャーとして実現することを目指します。人事情報管理を含めたユーザー管理システムに連携させた認証システムとアプリケーションやデータへのアクセス管理システムとして機能します（**図2**）。今後の主流はアプリケーション数のさらなる増大への対処、さらには企業全体として一貫性を持ったセキュリティー・プラクティスの実現から、セキュリティー・ポリシー・ステートメントの定義・管理を自動的にアクセス管理に反映するITシステムになってくると思われます。

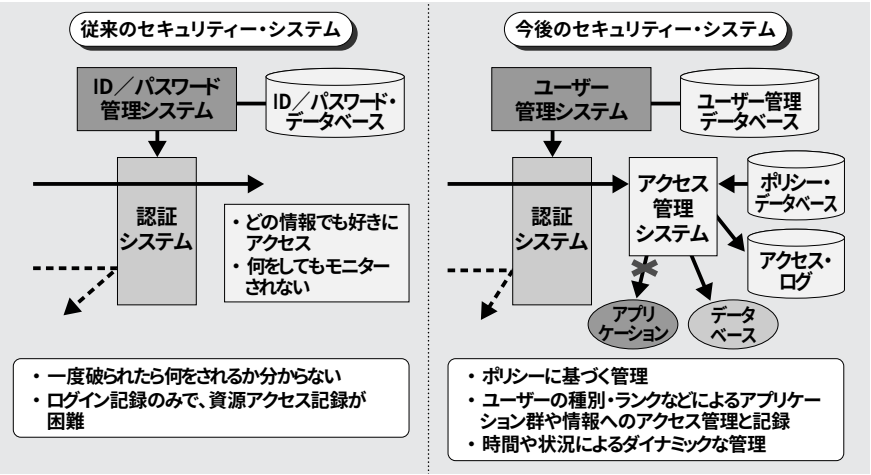

図2. 今後のITセキュリティー・システムに求められる機能

アプリケーション・セキュリティーはユーザーとリソースのアクセス管理において、アプリケーション・コンテキストに従って変化するダイナミックなアクセス管理の実現、さらに業界標準や法律、規則などによって規定されるセキュリティー・テンプレートやガイダンスの実現を目指すものです。プログラムやデータへのアクセスについては、その不正アクセスを防ぐためにも業界のセキュリティーのレギュレーション（標準）を確立させようという動きが高まっています。既に米国ではHIPPA（Health Insurance Portability and Accountability Act）と呼ばれる医療関連の法律が法制化され、患者に関するデータとプライバシーについて厳しいセキュリティーが医療関係機関に求められています。このほか、データの改ざんなどが起きた場合の罰則規定を設けた金融系の法律もセキュリティーの標準化として制定されています。これに対して、残念ながらセキュリティーの業界標準化の推進について日本では目立った動きがなく、その対応が遅れているのが気になるところです。

中期的なアプローチ

表1の「ITセキュリティー・システム構成と、その中期／短期アプローチ」に示されたITセキュリティー・システムの各層を漏れなくカバーし、ITセキュリティーが管理されている状態を確立し保持すること、それがITセキュリティー・システム・マネジメントの中期的な目標になります。

「ITセキュリティーが管理されている状態」とは、次のようなものです。以下、その事項に沿ってコメントを付しておきます。

1. **管理する対象が明確であること、それらの望ましい状態が明確であること。**
2. **管理者がいること。**
3. **管理プロセスが文書化されていること。**
4. **業務プロセスの実施記録と報告が確実になされていること。**
5. **監査が確実に行われていること。**
6. **PDCAが確実に実施されていること。**
7. **何らかの事故のときに追跡が可能であり、原因究明、対策立案といったアクションがすぐに決定できること、アクションを取る体制がいつでも発動可能であること。**

ISMSでは、組織内におけるセキュリティー・プロセスを明確にし、その相互関係を把握して運営管理することに合わせて、一連のプロセスをシステムとして適用する“ プロセス・アプローチ ”が奨励され、それ

を実現する考え方としてPDCA（Plan,Do,Check,Action）モデルを提示しています。すなわち、マネジメントにおけるPlan（計画＝ISMSの確立）、Do（実施＝ISMSの導入および運用）、Check（点検＝ISMSの監視および見直し）、Action（処置＝ISMSの維持および改善）です。このPDCAサイクルがきちんと実施され、セキュリティー体制がスパイラルに向上しているかどうかを審査するのがセキュリティー監査で、これには社内で行う内部監査と、コンサルタント会社などに依頼する外部監査とがあります。内部監査は一般的に行われていますが、どうしても評価が甘くなりがちであり、より客観的な評価を得るためにも外部監査を定期／不定期に実施することをお勧めします。

特に見直しを必要とするのが、システムのアクセス制御です。信頼される確実なアクセス制御の実現には、明確な方針の策定、業務ニーズに基づく権限付与、業務管理による維持など、これまで安全が前提の社会ではあまり重要視してこなかった部分に対する基礎的な取り組みが重要になります。また、このことは後でも触れますが、アクセス・ログを必ず取っておくことも大切になります。

以上のような「ITセキュリティーが管理されている状態」の実現が、企業におけるITセキュリティー・マネジメント・システム構築への中期的なアプローチになるでしょう。

プライバシー保護という新たな問題

セキュリティーに関連して、最近にわかに注目を浴びているのがプライバシー（個人情報）の保護であり、それに対応する実際的なITセキュリティー・システムの構築が企業でも緊急の課題になっています。ここでいう個人情報とは、特定の個人を識別できる情報（その情報だけでは識別できないが、ほかの情報と照合することで個人を識別できる情報を含む）です。

プライバシー対策が急がれている背景は、大きく二つあります。

一つは、顧客／社員情報など、個人情報への不正アクセスや個人情報の流出・漏えいに関する事件が頻発していること。その防止に特化したソリューションが切望されています。

もう一つは、個人のプライバシーを保護するための法律「個人情報保護関連5法」が2003年5月に成立し、既に施行された基本法部分を除き、2005年4月には施行されることです。以前は個人情報についてそれを取得した企業にその取り扱いなどすべての権限がありました。しかし今後、条文に明確には記載されていないものの、個人情報の制御権は情報主体である本人に属すると考えたほうがよいでしょう。すなわち、企業などが個人情報を取り扱う場合は、利用の目的を公表し、その範囲内でのみ使用すること、個人情報を勝手に取得したり、漏えいや不正流出させたりしてはならないし、また、本人の申し出があれば訂正や削除をすることが定められました。

この個人情報保護関連5法には「表現の自由」を理由にマスコミが除外されているために、それが企業に与える影響があまり報道されていませんが、CRM（Customer Relationship Management）などを展開している企業にとっては、コンピューターが日付をうまくカウントできずにエラーが起こる可能性のあった「2000年問題」に匹敵するほどのインパクトを持っているといえましょう。

これだけはやっておきたい個人情報漏えい対策

次に、短期的ITセキュリティー・システム・アプローチとして、個人情報漏えい対策のキー・ポイントを幾つかご紹介します。

(1) 個人情報の棚卸し作業

最初に、自社（各部門）にどれだけの個人情報（名簿）があるかを把握し、整理して新しい台帳（ディレクトリー）を作成します。プライバシー対策の原点にもかかわらず、この基礎的な作業をおろそかにしている企業がほとんどです。顧客・社員・契約社員などの個人情報データ、内容、適用業務、保管場所、利用目的、収集経路、アクセス可能な人間…などを記録します。

(2) アクセス・ログの記録

すべてのアクセス内容をモニターするのは不可能ですが、個人情報アクセスのログは必ず取るようにします。できるだけ、個人情報へのアクセスに関する5W1Hの詳細記録を取るようにしてください。このことはセキュリティー対策上にも非常に重要かつ有効であり、会社が常時アクセス状況をモニターしていることを明確にすれば社内外の犯罪予備軍に対して大きな抑止力になります。また、ひとたび漏えい事件が発生したときにもその被害の範囲を正確に把握し、素早い事後策・対処策の実施を可能にします。アクセス・ログはITシステムによる個人情報へのアクセスだけでなく、人間系の業務においても同じように記録されることが大切です。

しかし大量の個人情報漏えいは、大抵の場合ITシステムやそのデータ媒体を使用して発生します。5W1Hのアクセス記録をログとして残すにはそのための前提ITシステムの整備が絶対に必要です。まずWhoを確実に記録するためにはID管理システムとその認証システムが前提です。一つのIDとパスワードを複数のユーザーが使い回すなどの便宜策を取ってはいけません。WhatとWhereさらにWhenについて詳細に記録するためには対象となるプログラムやデータなどのリソース管理にその機能があり、常時実施していることが必要です。WhyとHowを記録するためにはアプリケーションごと、およびユーザーごとの役割と、業務ネットワーク全体の場所とアプリケーション・フローが正確に記録されなければなりません。

(3) 社員PCなどのアセット管理とセキュリティー・モニタリング

最近は、社員が使っているノートブックPCなどから社内Webシステムや基幹システムが汚染・破壊されたりするケースが増えています。これら社員が所有するPCなどについても、ハードウェア／ソフトウェアのバージョン管理、コンピューター・ウィルス・パッチ管理、セキュリティー・バイオレンスのモニターを行うようにします。必要であればファイルの内容やメール内容などのモニタリングも行います。

(4) パートナー管理の見直し

外部委託で消費者や社員などの個人情報を取り扱う場合、あるいは個人情報入力／更新を再委託でほかの業者などに発注している場合には、必ず個人情報の受け渡しに関する記録を取り、作業後には複写・削除管理をしっかり行い記録するようにします。

変換点にあるセキュリティー・システム

米国企業がITセキュリティー・システムにかける平均的な費用は、IT投資の約15%といわれます。それに対し、日本企業についての統計的な資料はないのですが、数%と思われます。昨今こそITセキュリティー・システムへの関心が急速に高まっていますが、欧米企業に比べて日本企業はまだまだセキュリティーに対してお金も人間も費やしていないのが現実です。

その理由の一つは、法解釈の違いにあります。欧米では不正アクセスや情報流出に対する法律が懲罰主義なのに対して、日本では実害証明主義なのです。例えば、人口20万人の市で情報流出の事件があると、米国では1人3万円として200,000（人）×30,000（円）＝6,000,000,000（円）となり、60億円の賠償金が課せられます。これに対して日本では情報流出を訴え出た原告だけが実害者とみなされ、原告が3人のみの場合、企業に課せられる賠償金は、米国と同じく1人3万円として3（人）×30,000（円）＝90,000（円）、9万円で済んでしまうのです。このように、米国ではITセキュリティー・システムの不備により倒産の危機さえあることを考えると、日本の法律は企業に甘いと言わざるを得ないでしょう。

さらに、事件が起こっても「のど元すぎれば熱さ忘れる」式の日本特有の文化が日本企業におけるセキュリティー意識を低くしています。

しかし、ビジネスや情報システムがますますグローバル化する中で、ITセキュリティー・システムも国際的な標準に準拠しないわけにはいきません。プライバシーという日本人にとって不慣れな概念も登場してきました。今、日本企業のセキュリティーへの考え方と取り組みは、大きな変換点を迎えているといえましょう。