IT部門が取り組むべき情報セキュリティー

アイ・ビー・エム ビジネスコンサルティング サービス株式会社
チーフ・セキュリティ・オフィサー
パートナー
IBMディスティングイッシュト・エンジニア
大木 栄二郎

Eijiro Ohki
Chief Security Officer
Partner
IBM Distinguished Engineer
IBM Business Consulting Services KK

2005年4月から施行される個人情報保護法により、今まではある意味で任意の努力目標であった情報セキュリティーの確保が、法定義務となります。個人情報を適正に管理しなければならないのはもちろん、適正に管理していることを証明できなければなりません。これまでの「安全が前提の社会」とは異なり、これからの「事故が前提の社会」では、企業のビジネス・プロセスやIT(Information Technology：情報技術)の中に適正なセキュリティー管理を実施していることを証明する仕組みを組み込んでいく必要があるのです。IT部門としては、限りある予算を有効に使って、合理的な仕組みを構築しなければなりません。OECD(Organization for Economic Cooperation and Development：経済協力開発機構)セキュリティー・ガイドラインをはじめとするセキュリティー・マネジメントの基準に照らしてセキュリティー対策を実施していく必要があります。特に、アクセス権限の与え方については明確なルールを設定し、すべてのシステムで信頼されるアクセス・コントロールを実現することが大切です。セキュリティーの重要性を再認識し、お客様や社員に信頼されるセキュリティー・アーキテクチャーをつくっていくことが、今後のIT部門の大きな仕事となるでしょう。

How IT Department Should Address Information Security

The protection of electronically stored information, which used to be covered by organization's voluntary efforts, becomes a kind of legal obligation when "Act for the Protection of Personal Information" come into effect in April 2005. Under the new laws, not only must personal information be properly managed, but an enterprise must also be able to prove it. The company needs to implement new mechanisms in its business processes and in its IT (information technology) systems that can perform the task of proving that security is being appropriately protected. IT departments are requested to design and implement effective and reasonable mechanisms fully utilising available resources within their budgets. The OECD (organization for economic cooperation and development) Security Guidelines and other security management standards are good basement and framework to design and implement your organization's comprehensive information security management system. It is especially important to define clear access authority policy and rules and decide how such authority should be granted so that we can ensure reliable access control in place in all systems. Reassessment of the significance of information security and practical design of oraganization's security architecture, which both customers and employees can trust on, therefore present a major challenge for IT departments.

高まる情報セキュリティーの重要性

個人情報保護法が2005年4月から施行されますが、この法律が企業に対して具体的に何を要求しているのかを理解すれば、いかに企業活動に大きな影響を与えるかがお分かりいただけると思います。

私は、アイ・ビー・エム ビジネスコンサルティング サービス（IBCS）のCSO（Chief Security Officer：最高セキュリティー責任者）として当社のセキュリティー全般を担当しているとともに、セキュリティー・コンサルタントとして、多くの企業のセキュリティー・マネジメントへの取り組みのお手伝いをさせていただいています。これらの経験から、企業におけるマネジメント・システムの一つとしてセキュリティー・マネジメントについて考察していきたいと思います。

最近になってセキュリティーの重要性が叫ばれるようになった理由として、次のような事象を挙げることができるでしょう。

- IT（Information Technology：情報技術）依存が急速に進んでいる
- 情報の価値が高まっている
- 脅威が増大している
- 企業が大きく変化している
- 社会の目が厳しくなっている

実際、北米のリサーチ会社の調査によりますと、「ITセキュリティー」や「災害対策」をIT部門にとっての最重要課題として挙げている企業が多くあります。日本アイ・ビー・エムも同様な調査を国内で行ったことがありますが、やはり同様の結果が出ています。

個人情報保護法の施行や不正競争防止法の改正など、法律により、企業の情報セキュリティーの確保が求められ、企業はそれに対応しなければならない時代を迎えつつあるのです。

成熟した議論への転換を

セキュリティー・コンサルタントとして、企業のトップの方にセキュリティーへの考え方をお聞きすると、驚くことにほとんどの方が「性善説」を採っておられます。「社内に悪い人間はいない。クラッカーや産業スパイ、テロリストは社外にいるのだから、社内情報を外部の脅威から守らねばならない」とおっしゃるのです。

また、住民基本台帳ネットワークシステム（住基ネット）については「100%安全でなければならない」という議論がありました。外部からの脅威に対しては厳しい目を向ける一方で、社内や足元については意外と危機感が少ないのです。

こうした内部からの脅威に対する意識の弱さが、結果的に昨今の個人情報漏えいの続発となって現れているのではないでしょうか。

経済産業省が2003年に発表した情報セキュリティー総合戦略では「従来のような100%安全といった原理主義的な議論から脱し、事故を前提にしたしなやかな社会を実現しましょう」という提言を行っています。事故を前提にするということは「事故は起きるかもしれない」という考えをさらに進めて「事故は必ず起こる」という立場で対策を考えていきましょうということです。

言い換えれば、これまでは、安全を前提にセキュリティー対策を考えていた、いわば「結果がよくて当たり前」の世界であり、裏を返せば「結果さえよければ、プロセスは問わない」ということです。セキュリティー対策に十分に取り組んでいなくても、幸いにも事故が起きなければ「よくやった」といわれ、たとえ一生懸命取り組んでいても不幸にして事故が発生すれば責任者の評価は落ちてしまったのです。

この段階に止まって議論している限り、セキュリティー

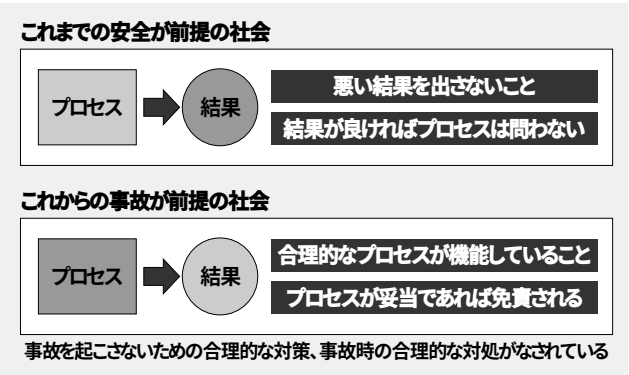

図1. 安全前提社会から事故前提社会へ

対策に新しい展開はないでしょう。今後は、企業においてセキュリティーに対する合理的なプロセスが機能しているのであれば、たとえ事故が起きたとしても「よくやっている」といわれるような仕組みをつくっていかねばなりません（**図1**）。最近就任されたCSOの方が、社長から「二度と問題を起こさないようにしてくれ」と指示されたと相談に来られますが、結果に固執するのではなく、事故を起きにくくし、起きても影響を少なくするプロセスにこそ注力すべきでしょう。今こそ、セキュリティーについて、成熟した議論への転換を図るべきときです。

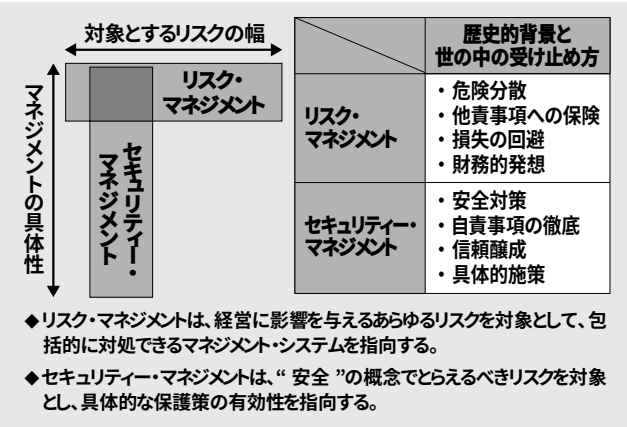

図2. リスク・マネジメントとセキュリティー・マネジメント

リスク・マネジメントとセキュリティー・マネジメントの違い

企業のマネジメント・プログラムの一つとしてセキュリティー対策をお手伝いする際に、よく質問を受けるのが「リスク・マネジメントとセキュリティー・マネジメントの取り組み方の違い」です。

この違いは文字通り、実施すべき対策を「リスク」でとらえるのか、それとも「セキュリティー」でとらえるのかということであり、すなわち危険側から見るのか、安全側から見るのかということでしょう。その意味では本質的な違いはなく、コインの裏表の関係ではないかと、私自身は思っています。

ただし、企業のマネジメント・プログラムとして見た場合、おのずとその取り組み姿勢に違いが生じることも確かです。まず、リスク・マネジメントにおけるリスクは、本質的には企業が自身の力ではコントロールできないものへの対応です。本質的に制御できない不確実性への対処ですから、「他責事項への保険」がリスク・マネジメントの中心的なテーマとなります。一方、セキュリティー・マネジメントは、安全をどうすれば確保できるのかということであり、「自責事項の徹底」がその本質となります。

もう一つの違いは、セキュリティー・マネジメントは個人情報の保護や情報資産の安全確保を対象としているだけに、間口は狭く、内容がより具体的であるといえるでしょう（**図2**）。

セキュリティー・マネジメントの基準

企業が対策に取り組むに当たって依拠すべきセキュリティー・マネジメントの基準も、ここ数年で明確になってきています。具体的には次に挙げるような基準が整備されています。

- OECDセキュリティー・ガイドライン（1992、2002年）
- BS7799、ISO/IEC-17799（1995、2000年）
- JIS-X-5080（2002年）
- ISMS適合性評価制度（2002、2003年）
- 情報セキュリティー監査基準（2003年）

情報セキュリティーの原点とも呼べる基準が、1992年に発表されたOECD（Organization for Economic Cooperation and Development：経済協力開発機構）のセキュリティー・ガイドラインにおける九つの原則です（**図3**）。これはネットワーク環境の変化に合わせて2002年に改訂され、「認識の原則」がトップになり、「責任の原則」の英文タイトルがAccountabilityからResponsibilityに変更され、あるいは「リスク評価」や「セキュリティーのデザインと実装」「セキュリティー・マネジメント」などの言葉が原則に採用されるなど、今日の状況を反映したものとなっています。また、2002年版では"Culture of Security"が提唱され、情報セキュリティーについて皆が意識する土壌を育むという考え方につながっています。

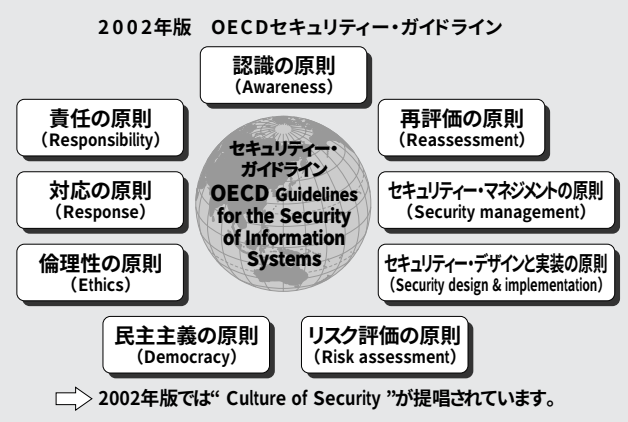

図3. OECDセキュリティー・ガイドラインの9原則

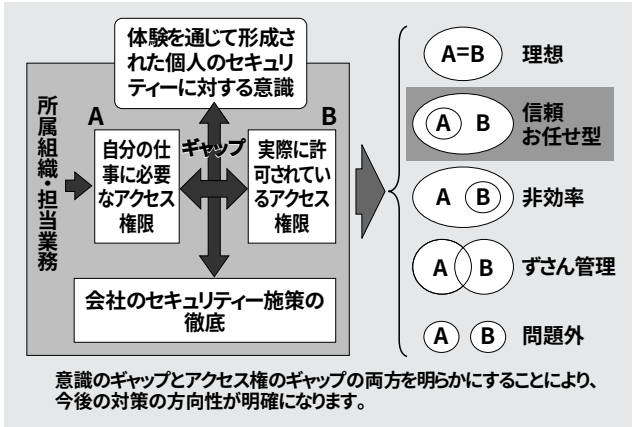

図4. アクセス権のギャップ

OECDセキュリティー・ガイドラインを受けて、英国規格協会（British Standard Institute）が定めた規格がBS7799です。この規格が国際的に受け入れられ、ISO（International Organization for Standardization：国際標準化機構）の規格であるISO/IEC-17799になりました。それをJIS規格としたものがJIS-X-5080です。

また、ISMS（Information Security Management System）適合性評価制度は、BS7799の認証制度を参考に国内の認証制度として確立したものです。また、情報セキュリティー監査制度も、情報セキュリティー管理基準として同じくJIS-X-5080を基礎としています。

企業において包括的な情報セキュリティーを確立するには、こうした基準に照らして対策を進めることが、合理的な対策を実施していることの論拠となります。

情報漏えいとアクセス・コントロール

IT部門が、セキュリティー対策を具体的に実施するに当たって、最重要課題の一つとなるのがアクセス・コントロールです。

これは一つの仮説として聞いてほしいのですが、最近になって個人情報の漏えいが頻繁に起こっている原因の一つに、アクセス・コントロールの不備が関係しているのではないかと疑っています。

つまり、個人情報を蓄積しているシステムにおいて、業務上必要なアクセス権限と、実際に社員に与えられているアクセス権限にギャップがあるのではないかということです（**図4**）。

多くの企業が、アクセス権限の与え方について必ずしも明確なルールを持っているとは思えません。アプリケーション・レベルで設定していることが少なくないようなのです。実際、「アクセス権限をオーソライズできるのはだれか？」「どんな原則に基づいているのか？」と突き詰めていくと、あいまいなまま運用されている事例が多いのです。

こうしたアクセス権限のギャップについては、図の右側に示したA=Bという理想型を維持している企業はほとんどなく、恐らく2番目の「信頼お任せ型」になっているのではないかと思われます。性善説から出発している「信頼お任せ型」を事故前提社会で通用する「理想型」に変革するには、やはりセキュリティー・ポリシーを作り、その中で情報へのアクセス権限の基本となる考え方を定め、会社としての今後の方向性を明らかにしていく必要があります。実は、有効なセキュリティー・ポリシーを持っている国内企業は3割程度にすぎないという報告があります。もちろんセキュリティー・ポリシーがあったとしても、それだけでは意味がありません。現場で個人情報を扱う社員のセキュリティーに対する意識は別問題だからです。社員一人ひとりが、個人の体験を通じてセキュリティーに対する確固たる意識を身に付けていることが肝要なのです。アクセス権限の付与について原則をきちんと作るだけでなく、現場で徹底させないと合理的な対策にはなり得ません。難しい点は多々あるでしょうが、不断の努力が必要なのです。

アクセス・コントロールの見直しについて

JIS-X-5080には、全部で127のコントロール（管理策）が示されています。章別に見ると9章の「アクセス制御」が最大で31項目、8章の「通信及び運用管理」が24項目、10章の「システムの開発及び保守」が18項目、7章の「物理的及び環境的セキュリティー」が13項目、11章の「事業継続管理」が5項目などです。

このように全体で127のうち80以上はIT部門が取り組むべきテーマということになります。アクセス・コントロールについては、新たに構築するシステムだけでなく、運用中の既存システムについてもさまざまな面から見直す必要があります（**図5**）。

例えば図の右下から2番目に「個人情報にはさらに新たな条件が加わる」となっていますが、これはお客様からお預かりした情報を利用する際に、お客様が同意された利用目的にかなっているかどうかということです。従来のシステムには、恐らくそれをチェックする仕組みが組み込まれていないはずです。

このように、お客様情報すなわち個人情報のアクセス・コントロールについては、すべてのシステムで大きく見直す必要があります。

信頼されるアクセス・コントロールの実現を

合理的なアクセス・コントロールを実現するには次の三つの要素が欠かせません。

- 明確な方針の設定
- 業務ニーズに基づく権限付与
- アドミニストレーションによる維持

これらの要素は、安全が前提の社会ではさほど重要視されませんでしたが、事故が前提の社会では大切です。セキュリティー・ポリシーに明確に示すなど、より基礎的なところからの取り組みが不可欠なのです。

ただし、その実現には不断の努力が求められるだけではなく、運用にかなりのコストが掛かります。欧米のセキュリティー対策と国内のセキュリティー対策の根本的な違いは、この部分にいかにコストを掛けてきたかということだと思います。欧米の企業はTivoli®製品などこの分野で的確な機能構造を持つ製品を積極的に導入して、セキュリティー対策のシステム化を図っていますが、国内企業ではあまり浸透していません。今後、国内でも対策を打っていくに当たり、この部分に莫大な人件費を掛けるのは難しいでしょうから、いかにコストを掛けずに合理的な対策を維持できるシステムを構築するかということを考えねばなりません。

IT部門にとっては、合理的な対策を作り上げ、維持

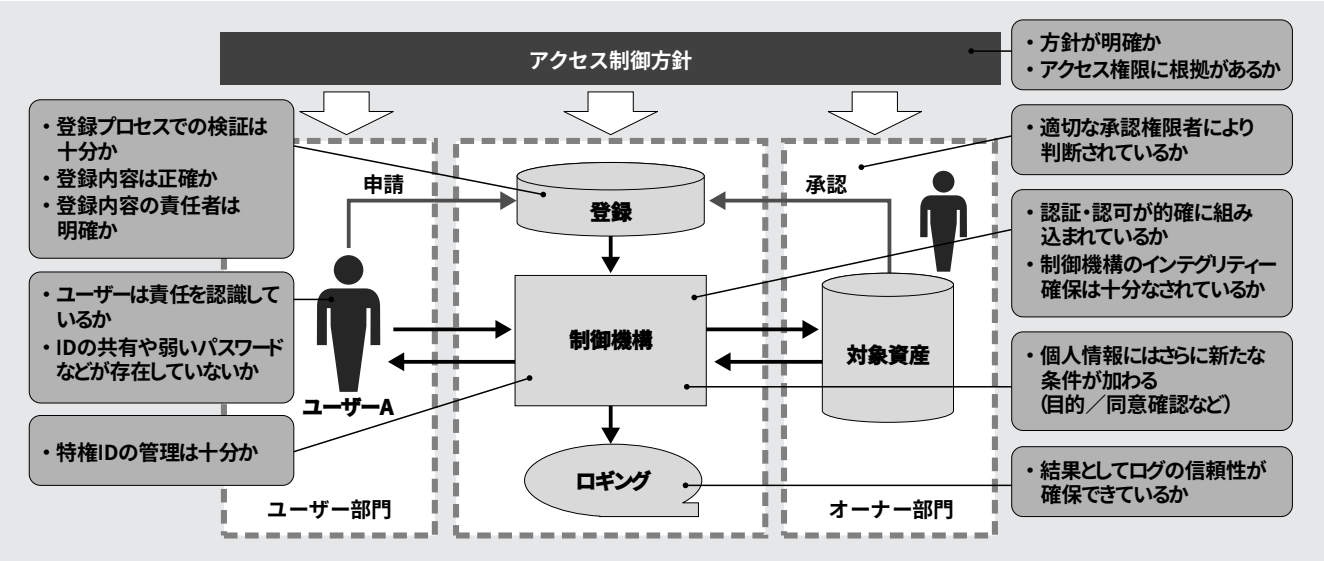

図5. アクセス・コントロールの見直し

していくことが今後の大きな命題の一つであり、知恵が問われるところです。今後のシステム構築では、経営方針や事業戦略から導き出されるシステムの要件に加え、情報セキュリティーの基本方針から導き出される要件も同時に満たされなければなりません。

問題はこの二つの条件を満たす最適な設計や実装がいかにして可能になるかにあります。IBMには、長年にわたって取り組んできたシステム・デザインの参照フレームワークや方法論があり、実際に構築してきた経験もありますから、そういう意味でも皆様のお役に立てるのではないかと思います。

セキュリティー・アーキテクチャーの構築

注意しなければならないのは、セキュリティー・ポリシーと、セキュリティー・コントロールを含む実際のシステム構築の間には非常に大きなギャップがあるということです。このギャップを埋めるのが情報セキュリティー・アーキテクチャーです。これは、情報セキュリティー技術標準と情報セキュリティー構築ガイドから成り立っていると考えると分かりやすいでしょう。

従来、企業がシステムの構築をSI（System Integrations：システム統合）ベンダーに発注する場合、その要求仕様の中にはセキュリティー要求仕様は必ずしも明確には示されていなかったと思われます。もちろんインターネットを利用するシステムであればセキュリティーを確保しなければなりませんが、具体的な対策はSIベンダーにお任せすることが多く、自分たちで検証できないということも少なくありませんでした。

そこでセキュリティー・アーキテクチャーを構築し、例えばネットワークのセグメントごとに、どの場所にどんな分類の情報を置いていいのか、あるいはセグメント間にどんなセキュリティー機能が必要かなどといった、それぞれに実装されるべきセキュリティー機能要素を示すことが重要です。

セキュリティー・アーキテクチャーの構築に当たっては、自分たちで一からつくっていって、それにのっとったセキュリティー関連製品を組み合わせていくという方法もありますが、もう一つの考え方として、的確なセキュリティー・アーキテクチャーを基に構築された製品をそのアーキテクチャーごと導入して運用するという方法もあります。実証されたアーキテクチャーに基づく製品群を導入することにより、短期間に効果を挙げることが期待できます。

その際の大きなポイントは、そこでデザインされているセキュリティー・アーキテクチャーが自分たちにとっても本当にいいものであり、頼れるものであるのかを検証することです。個々の製品の機能ももちろん大事ですが、その背景にあるアーキテクチャーを見極めるということが非常に重要になります。

IT部門が取り組むべきこと

結論として、IT部門が今取り組むべきことは、次の二つです。

- 新たな視点からのセキュリティー・マネジメントのデザイン・実装・運用。
- IT部門自身の改革。

ITをデザインする際の要件に、セキュリティーやプライバシーが占める割合はますます大きくなっています。従って、IT部門における企画・開発・運用・保守というプロセスの中に、まずはセキュリティーやプライバシーを埋め込んでいただくことが、今後取り組むべき重要なテーマになるかと思います。

とはいっても、システムのセキュリティーの機能を一から手づくりするということは手間やコストの点から考えられません。セキュリティー関連のソフトウェア／ハードウェアをいかに組み合わせて自社のセキュリティー・システムをつくり上げていくのかということになります。その組み合わせの基本的な考え方がセキュリティー・アーキテクチャーであり、それをきちんとつくっていくことがIT部門の大きな仕事になるでしょう。

セキュリティーに対するIT部門の取り組みに際して、私たちIBMがお役に立てることがあればぜひお声を掛けていただきたいと思います。