# リスク・マネジメントの視点からのセキュリティ対策が急務

## 第7回 情報セキュリティ

世界中で、悪質なウイルスによる攻撃や、ホームページへの侵害事件が相次ぎ、多くの企業にとって、情報セキュリティの重要性が高まりつつある。ところが日本の場合、被害にあってからセキュリティ・レベルを強化する、といった場当たり的な対策が先行しがちであり、リスク・マネジメントの視点から有効なセキュリティ対策を実施している企業は少ないのが現状である。そこで今回は、リスク・マネジメントという視点からのセキュリティのあり方、現在注目を集めている情報セキュリティ・ポリシー作成・運用のポイント、さらに、ビジネス・チャンスとのバランスを取るための考え方などについて話し合っていただいた。

**出席者**

**谷口博一氏　監査法人トーマツ　エンタープライズリスクサービス部　参与**
**佐藤慶浩　日本ヒューレット・パッカード（株）HPコンサルティング事業統括本部**
**セキュリティ&ITストラテジー・コンサルティング・グループ長**

# セキュリティはリスクの問題

**――リスク・マネジメントの視点から企業にとってのセキュリティはどう考えるべきか。**

**佐藤**：リスク・マネジメントで一番望ましいのはリスクが回避できることですが、回避の対極にあるのがリスクの受け入れ、その中間がリスクの軽減です。ここで、リスクを回避もしくは軽減するときに必要になるのがセキュリティ対策ということになります。ですから、セキュリティ製品にこんなものがあるから使ってみようというアプローチでは対策が先になり、リスク・マネジメントとはいえません。よく日本の経営者はセキュリティに関心がないといわれますが、それは間違っていると思います。情報システム部門の方は経営層に対し、セキュリティ対策を講じなければ、こういったリスクを受け入れることになると、リスクをキーワードに提言すればよいのです。経営者はリスクには関心があるのです。それを、この対策ならセキュリティがこれだけ強くなるという表現を使うと、では、それにはいくらかかるのか、という費用対効果の話になってしまいます。セキュリティを強化しても生産性が上がるわけではありませんから、そんなものがなぜ必要なのかということになり、対策が実施できなくなってしまいます。

**谷口**：すでに日本でも、有効なセキュリティ対策が実施できていないと、ビジネス展開に影響を与えるという場面が生じています。たとえば、自社のセキュリティ対策がしっかりしていなければ、コンペそのものに参加できないということもあります。いま、お話のあったように、マネジメントの視点からは、セキュリティ対策は生産性が下がってマイナスというネガティブな考え方もできますが、セキュリティ対策が自社の競争力を大きく左右するという状況は無視できません。

# 情報セキュリティ・ポリシーは自社で作る

**――なぜ情報セキュリティ・ポリシーが重要なのか。**

**佐藤**：情報セキュリティ・ポリシーで定めるのは、セキュリティをどういう状態にするかという目標です。目標がなければ、現状がいいのか悪いのかという判断もできません。また、セキュリティの目標というと、情報システム部門の目標のように考えがちですが、セキュリティはビジネス・チャンスとのバランスで考えるものですから、経営者の判断も必要であり、全社で足並みを揃える必要もあります。その意味で目標が必要であり、それはIT戦略ではなく、情報セキュリティ・ポリシーなのです。

**谷口**：経営戦略上、企業間のパートナシップが重要な課題となっていますが、そこでもセキュリティ・ポリシーは重要です。企業間でネットワークを接続する際に、セキュリティ・レベルをどうするかという問題が出てくるためです。この場合は、各社のセキュリティに対する考え方が違いますので、最低限の要求水準を情報セキュリティ・ポリシーとして定め、それ以上は各社で判断することになります。要求水準をどこまで想定するかは、リスク分析と投資費用、かける手間を考え、お互いに話し合って最低限のレベルを決めていくことになるでしょう。

**――情報セキュリティ・ポリシー作成のポイントは**

**谷口**：作成のプロセスが重要です。現実的にはシステム部門が作成することが多いと思いますが、本来情報セキュリティは紙ベースの文書管理も含めるべきで、当然、システム部門だけではすべてをカバーできません。トップの理解と全社のサポート体制が必要です。そのうえで、まず重要なのは、何のために情報セキュリティ・ポリシーを作るのかという目的を明確にすることです。また、他社の情報セキュリティ・ポリシーを真似すれば早く作成できると考えがちですが、他社の真似をすると、自社の現状がどうなっているかがわからない、つまり一番重要なリスク分析とい

## 佐藤 慶浩

**1986年日本アポロコンピュータ(株)入社。1990年日本ヒューレット・パッカード(株)入社。1993年からの2年間はカリフォルニア州クパチノ市にてセキュリティ製品の仕様開発に従事。現在は主としてセキュリティ・ソリューションのコンサルティングに従事。1997年以後は、通常のコンサルティング活動のほかに、JPCERT／CCのHP対応窓口を担当。各種社外セミナにて情報セキュリティ関係の講演をしている。**
**情報処理学会(www.ipsj.or.jp/) 正会員**
**日本ネットワークセキュリティ協会(www.jnsa.org/) 理事**
**情報処理振興事業協会(www.ipa.go.jp/) セキュリティセンター研究員**
**金融情報システムセンター(www.fisc.or.jp/) セキュリティポリシー研究会 委員**

セキュリティの今後の動向は
「社内や社外といった領域の違いによって安全かどうか決まるのではなく、これからは情報と情報との間やシステムとシステムとの間のセキュリティが保たれている必要があります。そのためには個人の認証が問題で、PKIは解決の一つの要素になると思います。システムや情報のレベルでセキュリティが保たれ、信用のある第三者の認証が、空間や領域ではなくて、情報のレベルで行われるための技術なりソリューションがこれから出てくると思います」

## 谷口 博一 氏

**通信機器メーカ、外資系コンサルティング会社を経て1989年監査法人トーマツ東京事務所入所。医療機器や情報サービスのマーケティング戦略の策定、エンタプライズモデリング法を活用した情報システム戦略構築方法論に基づくシステム化構想策定、情報システムの有効性評価、システム評価制度の導入等を実施。現在、情報セキュリティ・ポリシーや基準の策定、個人情報保護やセキュリティ関連コンサルティング、リスク指向のセキュリティ監査等を担当。**
**公認情報システム監査人（Certified Information Systems Auditor）。**

---

セキュリティの今後の動向は
「今後は、トラストがキーワードになると思います。認証局とか信頼できる第三者が保証するという信用のできる仕組みが社会インフラとして必要です。その意味で、今後PKIを使ったインフラが出てくると思います。また、システム日付が世界標準の時刻と正確に合っていることを証明できる機能も必要になります。さらに、社会のシステムが全部つながっていくと、どこかに欠陥が出ると、影響も大きくなりますので、より信頼度の高いソフトやハードが必要とされるのではないでしょうか」--

うプロセスが抜け落ちてしまいます。現状を知り、リスク分析を行って、経営者の判断を仰ぐためにも、一連のプロセスを経て、自社で情報セキュリティ・ポリシーを作ることが重要です。

**佐藤**：情報セキュリティ・ポリシーは社員に守ってもらわなければ意味がありません。そのためには、いかに現場の要求を吸収できるかがポイントになります。そこでＨＰコンサルティングの情報セキュリティ・ポリシー作成支援サービスでは、例外を前提にするという考え方を採り入れています。セキュリティ・ポリシーは絶対不変ではない。その時々のビジネスの状況に応じて、ビジネスに例外が生じたのであれば、セキュリティにも例外が起こりうる、という考え方です。といって、ポリシーに違反してもいいですよ、というのでは、ポリシーの意味がありません。作業者だけの判断で違反するのではなくて、逸脱するための手続きを踏んで、例外を記録するなり、承認する仕組みを作っておくことが重要だということです。

**谷口**：情報セキュリティ・ポリシーの作成には、自社の現状に対するリスク分析が必要になります。そこでセキュリティの教科書をみると、リスク分析には、情報資産の洗い出しなどが必要だと書いてありますが、そのとおりに実施するには膨大な時間がかかります。リスク分析やセキュリティ・ポリシーの作成に1年もかかるのであれば、それは現実的ではありません。しかも、目的がはっきりしていなければ、膨大な調査書が完成しても使い道がわからない、という状況になってしまう。セキュリティ・ポリシーは一度にできるものではなく、少しずつ作っていくものだという割り切りも必要です。たとえば、ある程度わかる人たちが話し合って、簡単に作れる場合もある。精緻なものはできなくても、わかっている人たちが作るのだから、ポイントもそんなにずれることはないでしょう。eコマースに参入しようというのであれば、そのリスクにフォーカスして、情報セキュリティ・ポリシーを0.5くらい作っておけば、そんなに日数をかけなくても作成できると思います。

**佐藤**：現状のリスク分析の結果に基づいてセキュリティ・ポリシーを作成するのが理想的ですが、いまのお話にあったように、いまのビジネス・スピードではそれが難しい状況です。そこで仮の目標を置いて、現状分析を進めていく中で、仮の目標に合わない部分が出てくれば手直しする。つまり現状分析を少し進めて、それでわかる範囲の目標、ポリシーを作る。ポリシーが決まることで、そこに関連する現状を分析する。この結果ポリシーがまた細かく定められる、といったスパイラル型の進め方が現実的だと思います。

# リスクとビジネス・チャンスのバランス

**――利便性あるいはビジネス・チャンスとのバランスはどう考えればよいか。**

**佐藤**：そういった問題はお客さまとの話によく出てきます。たとえば、メールを暗号化しているが利便性が悪いため、ポリシーを守らせることができない、といった話です。ここで重要なのは、そもそも何でメールを暗号化すると決めたのか。メールを暗号化しないとどんなリスクがあり、そのリスクはどんな根拠で受け入れられないのかを考えることです。その結果、そのリスクを取ることでビジネスが成功するのなら、例外として、きちんと手続きをしたうえで、逸脱する、という判断があってもいい。人・物・金・情報が経営資源といわれますが、人・物・金については、リスク判断についても権限委譲が行われています。しかし、情報はそうなっていません。情報についても、何らかの権限委譲があって、たとえば、課長が承認すればいいと決めておけば、ビジネスの状況判断でメールを暗号化しないリスクを受け入れることがあってもいいと思います。

**谷口**：利便性については、面倒だから守らないというケースもあります。たとえば、パスワードを3ヵ月に1回変更しようと決めても、いまは一人がいくつものパスワードを持っていますから、変更のサイクルが違っていれば覚えるのも大変だし、それこそ面倒です。これを技術的に解決できる場合もあります。たとえば、指紋認証などを導入するといった方法です。ところがこの場合、今度はコストが問題になります。導入するかどうかは、ビジネス面でのメリットとコストの費用対効果で決まるということです。また、面倒だからといって守られないのであればリスクを受け入れることになりますが、このリスクに指紋認証などのコストが見合うかという判断も必要です。さらに、面倒だからということに対しては、教育が有効な方法かもしれません。単にルールだけを教えて、それを守れというのではなくて、ルールを守らなかった場合、どんな不利益があるのかを理解してもらうことが大切です。日本のセキュリティ・ポリシーや規定類には、なぜそれが必要かという背景、理由が書かれていません。その書かれていない部分をカバーする意味でも教育は重要です。

**佐藤**：セキュリティ対策を実施しないということは、結果的に何らかのリスクを受け入れることですから、そのリスクを受け入れるかどうかを判断し、コストに見合うかどうかで決めることになります。極端に言えば、世界中の企業が対策をしているからといっても、その企業に必要かどうかはわかりません。逆もまた真で、世界中の企業が対策をしていないとしても、その企業に必要な場合もあります。あくまでも判断基準は、どんなリスクを受け入れて、どんなリスクは受け入れないかにあります。たとえば銀行は、従来のビジネス・モデルでは自行のネットワークをインターネットに接続することは想定していませんでした。ところがある銀行が、インターネットに接続することで生じるリスクを受け入れたことで、インターネット・バンキングという新たなビジネス・チャンスが生まれたということなのです。

セキュリティを考える場合、その強弱を論ずるのではなく、リスクを受け入れるかどうか、といったリスク・マネジメントに基づいた経営判断によって行うべきで、さらに、情報システム部門だけの問題ではなく、経営トップの理解のもと、全社で取り組むべき課題であるとのお話であった。非常に示唆に富んだお話で、参考にしていただければ幸いである。