エンタープライズ・リスク・マネジメントとして情報セキュリティー対策を位置付け、グローバル・ガバナンスに基づいて全社的な取り組みを推進

日本アイ・ビー・エム株式会社
執行役員
お客様プログラム・
経営品質・社長室担当

江口 昌幸

高機能になったスマートフォンやソーシャル・ネットワーキング・サービス（Social Networking Service：以下、SNS）の台頭を背景としてIT環境が劇的に変化し、標的型攻撃に代表される巧妙なサイバー攻撃が深刻化している今日、情報セキュリティーが、事業継続、ひいては企業の存続にまでかかわる企業リスクの1つと認識されるべき時代を迎えています。情報セキュリティーは、コストや体制、利便性とのバランス、社会的責任などを総合的に考えなければならない難度の高いテーマであり、リスクの想定、ビジネスへの影響分析、ビジョンや戦略の策定まで、経営層が主体的に関与して意思決定を下すことが求められます。

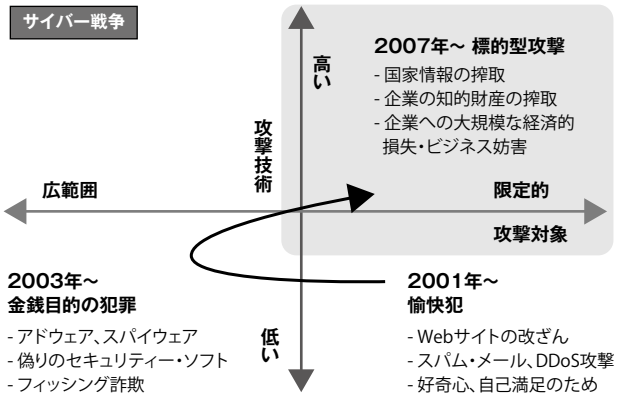
本記事では、日本IBMのCISO（Chief Information Security Officer: 最高情報セキュリティー責任者）として、IBMの取り組みを踏まえながら、企業の情報セキュリティーやリスク・マネジメントに対する考え方をご紹介します。

巧妙化するサイバー攻撃と拡大する被害

近年、大企業や官公庁、研究機関を狙ったサイバー攻撃が増加し、世界的な脅威となっています。従来のサイバー攻撃は、企業のWebサイトを無差別に改ざんする、また、サーバーに大量のトランザクションを送り付けてシステムをまひさせる（DDoS攻撃：Distributed Denial of Service attack）など、好奇心や自己満足のための愉快犯的な性格を帯びたものが主流でした。しかし、なりすましによるフィッシング詐欺行為など金銭を目的としたものが徐々に増加し、最近では特定の企業や団体にターゲットを絞って、知的財産に関する機密情報や顧客・社員などの個人情報を盗み取るという標的型攻撃が問題となってきています（**図1**）。

また、攻撃手法も高度化しています。最近の標的型攻撃では、まず企業や団体の特定の属性を持つ個人に対して、巧妙に作成された電子メールを送信して内部ネットワークに攻撃基盤を確立し、そこからウイルスを広める、あるいは外部サイトにアクセスさせて認証情報などを取得するという手法で攻撃を行います。その上、攻撃は、長期にわたり執拗（しつよう）に継続される場合もあります。

さらに、その企業や団体が損害を被るだけではなく、その企業や団体のサーバーを経由して第三者に被害を及ぼす攻撃が多発し、法的責任の所在が問題になっています。攻撃を受けた企業や団体が意図せずに踏み台となり他社を攻撃していた場合でも、被害者はその企業や団体に損害賠償を請求することができるという判例も出てき



サイバー攻撃は、国家・企業に大きな損失を与えるものに変わってきている。

図1. サイバー攻撃の変化

ています。つまり、そもそもの攻撃の被害者である企業や団体が、犯罪に加担したかのように位置付けられてしまうのです。また 2011 年には、ある海外金融機関がサイバー攻撃を受け、その影響で預金システムが 3 日間停止し、預金の引き出しや送金、クレジットカードやローンの利用ができなかったとして、信用格付けが下げられてしまうという事例も発生しています。

世界に 9 カ所設置された IBM セキュリティー・オペレーション・センター（SOC）の 1 つである東京 SOC の調査によると、2011 年に標的型メール攻撃を受けた日本企業の業種別の割合は、政府機関 35%、報道機関 29% をはじめとして、以下運輸、金融、製造などの民間企業が続きます。標的型攻撃が依然として増加傾向にある中、先端技術を扱う企業はもとより、あらゆる企業、団体がすべてそのターゲットになり得ます。

こうした攻撃をひとたび受けてしまうと、損害賠償などの金銭的逸失被害だけでなく、社会的責任を問われて会社の信用やブランド・イメージを損なうことになりかねません。つまり、セキュリティー対策は、単に情報を守るというだけでなく、企業のリスク・マネジメントそのものとしてとらえるべき時代になっています。そして、自然災害などと同様に、サイバー攻撃は事業継続を阻むものであるという前提でリスク・マネジメントに取り組まなければなりません。

IBMが実践する全社的リスク・マネジメントの一環としてのセキュリティー対策

ここで、リスク・マネジメントの一環であるセキュリティー対策の一例として IBM における取り組みをご紹介します。IBM は米国本社が主導し、グローバルにビジネスを行う視点から、業務遂行などにおけるリスクを定義し、包括的かつ戦略的に対応策を講じるエンタープライズ・リスク・マネジメント（Enterprise Risk Management：

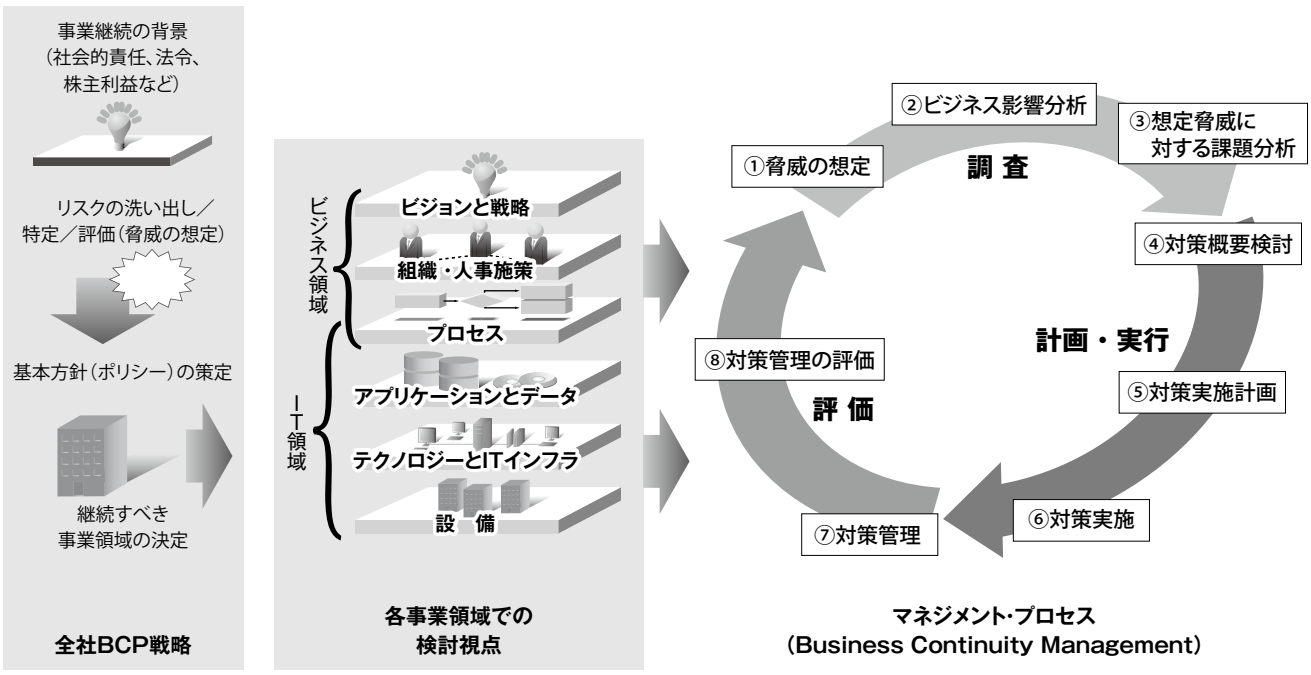


図2. IBMが考える事業継続計画(BCP)策定の流れ

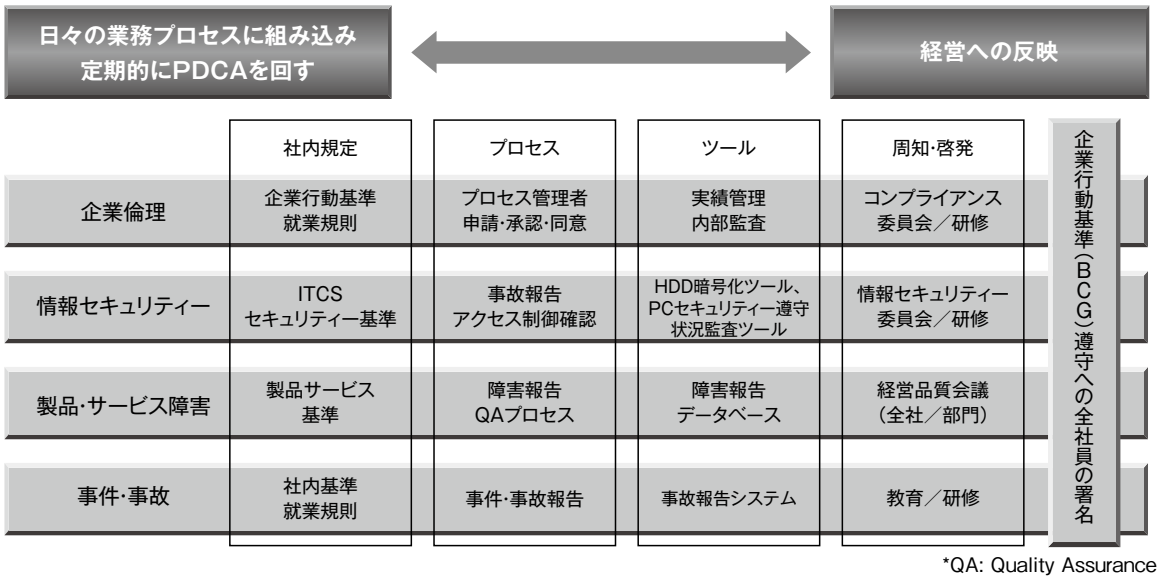


図3. オペレーショナル・リスクにおけるプロセス・マネジメント

以下、ERM）を遂行しています。対象となるリスクは、地震や洪水などの自然災害、疫病や新型インフルエンザなどのパンデミック（世界的大流行）、円高などの為替リスクや著作権侵害などさまざまですが、現時点では、サイバー攻撃や情報セキュリティー管理もERMの最重要課題として位置付けられています。リスク・マネジメントでは、事業リスクを特定し、業務への影響を分析してリスクの優先順位を決めるなど一定の評価を行った後、事業や社会に与えるインパクトが大きいインシデント・リスクと、日々の業務で発生し得るオペレーショナル・リスクによって、異なる対応を取ります。

まず、インシデント・リスクについては、事業継続計画（Business Continuity Plan：以下、BCP）を策定します。この策定に当たっては、「ビジョンと戦略」「組織・人事施策」「プロセス」のビジネス領域と共に、「アプリケーションとデータ」「テクノロジーとITインフラ」「設備」のIT領域を連携して検討することが重要です。そして、この6つの領域に対して、①脅威の想定②ビジネス影響分析③想定脅威に対する課題分析④対策概要検討⑤対策実施計画⑥対策実施⑦対策管理⑧対策管理の評価という8つのプロセスを繰り返し行います（**図2**）。

例えば、2011年の東日本大震災では、日本IBMは、震災発生からわずか1時間ほどで被災地の拠点の状況をほぼ把握するなど、その迅速な初動とその後の対応を高く評価いただきました。それを可能にしたのは、「脅威は必ず訪れるものであり、業務は中断する」という前提で、BCPの策定に取り組んでいたからでもあります。1995年の阪神・淡路大震災の後に震災を対象とした災害対策規定を策定しているほか、2007年には新型インフルエンザのパンデミックに備えたBCPも策定していました。ただ、東日本大震災においては、BCPで想定していなかった事態も発生し、改善すべき多数の項目が挙げられました。改善項目については、現在取り組んでいる

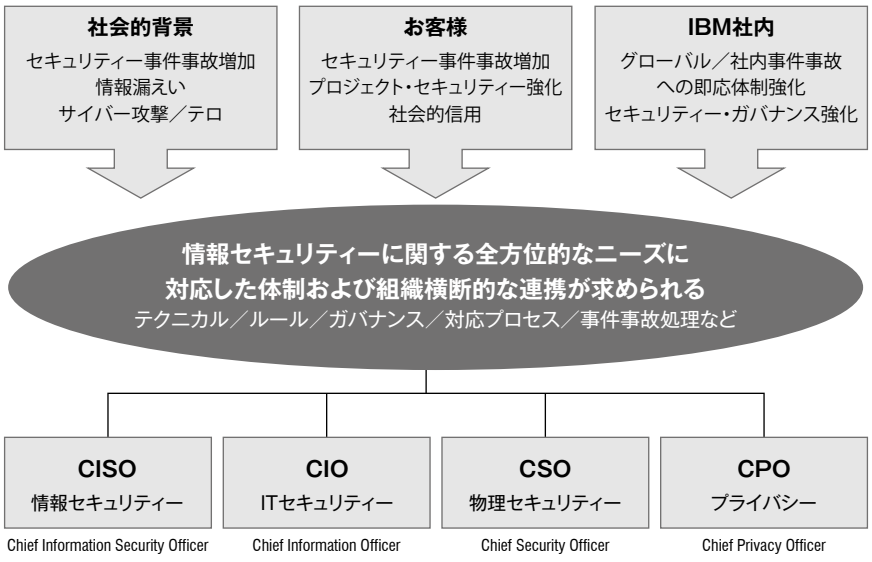


図4. 情報セキュリティーに対するIBM社内体制

首都圏直下型地震に対するBCPに反映するなど、常に見直しを行って対策の向上を図っています。

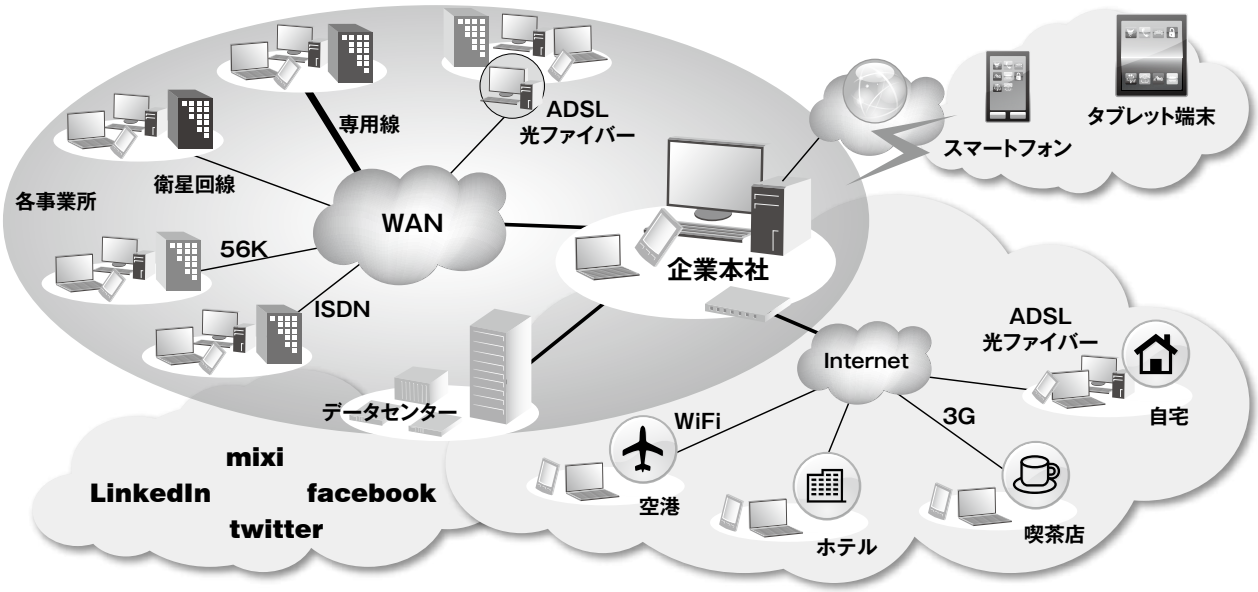
とはいえ、地震、台風、津波などの自然災害やパンデミックは、想定される被害内容が時代の経過と共に大きく変化することはありません。首都圏直下型地震も、中央防災会議の発表を見れば地震発生による被害の内容をある程度想定することができます。これに対して、情報セキュリティー事件は、特にサイバー攻撃など日々手口が巧妙化する上、地域やビジネス形態の違いなども相まって、被害の想定が非常に困難であり、その対策も常に見直しが必要になります。

つまり、情報セキュリティー対策では、サイバー攻撃に代表されるインシデント・リスクへの対応を行う一方、市場や企業、ビジネス・モデルの変化に伴い日常に発生し得るオペレーショナル・リスクへの対応も重要といえます。オペレーショナル・リスクは、セキュリティーだけでなく企業倫理なども含みますが、プロセス・マネジメントにより発生を最小限に防ぐ仕組みを確立し、定期的にPDCA（Plan/Do/Check/Action）サイクルを回すことで対応しています（**図3**）。次々と新しい脅威が登場し対応が必要となる情報セキュリティー対策においては、特にこうしたPDCAサイクルによる継続的な見直しが必要不可欠であると考えます。

また、リスク・マネジメントには社内体制の明確化も欠かせません。リスクごとに担当責任者を決定して最適な危機管理体制を組織します。情報セキュリティーに関しては、情報セキュリティーの責任者であるCISO、社内情報システムの責任者であるChief Information Officer（以下、CIO）などが連携し、テクニカル、ルール、ガバナンス、対応プロセス、事件事故処理など全方位的なニーズに対応可能な体制を築いています（**図4**）。さらに、お客様や社員などへの影響を精査する中で、法律的な賠償問題なども配慮しなければならないケースも増えていることから、法務や物理セキュリティー、プライバシーなど、それぞれの部門責任者との連携も強化しています。

急速に変化するIT環境に応じた情報セキュリティー対策の視点

情報セキュリティー対策を検討するとき、昨今大きく変化している企業のIT環境（**図5**）も視野に入れる必要があります。まず、高機能なスマートフォンやタブレット端末をはじめとする新しいモバイル端末の普及が著しく、PCに取って代わる勢いです。また、これまでは私的な利用が多かったSNSも、生産性や創造性の向上、情報収集、マーケティング効果の把握などを目的に、新しいビジネス・プラットフォームとして業務への活用を推進する企業も増えています。このようなネットワーク、クライアント端



・イントラネットへの新たな脅威　・ワークプレースの多様化　・スマートフォンなどのPCに代わるユーザー・インターフェースの普及
・SNSなどビジネス・プラットフォームの変化

図5. 企業を取り巻くIT環境の変化

末などの進化によるIT環境の変化は、セキュリティーの観点では新しい深刻な脅威になり得ます。例えば、SNSの普及により、情報を受発信する機会や頻度が増えることで、SNSを通じた情報漏えいやそのほかのセキュリティー事件も増加しています。

さらに、社員のワークプレースは会社外の場所へと広がり、多様化しています。IBMでは、ワークプレースに柔軟性を認める「オンデマンド・ワークスタイル」や「テレワーク制度（在宅勤務制度：ホーム・オフィス／ e-ワーク）」（PROVISION70号34ページ以下：スポットライト参照）を推進し、社員が個々の能力を最大限に発揮し、より豊かな生活を実現するために、仕事と生活のワーク・ライフ・インテグレーションを考慮しています。このテレワーク制度は、実際、東日本大震災発生時には、事業への影響を最小限にとどめることに貢献しました。首都圏の震災時における通勤困難を想定し、ワークプレースの多様化を検討する企業はますます増えていくでしょう。しかしながら、これは、システム・インフラが完備されているだけでなく、発生し得るセキュリティー・リスクへの対策があって初めて実現する制度です。例えば、ワークプレースが会社外に広がったことで、クライアント端末（PC、携帯、スマートフォンなど）を紛失したことに起因する情報漏えいリスクも高まるからです。IBMでは、PCの持ち出し禁止やシンクライアント採用という対策を実施しない代わりに、①個人の責務と意識を明確にするためのルールの定義②プロセスとルールを明確にするためのITセキュリティーに関するコーポレート・スタンダードの策定③ITテクノロジーによる予防策の実施という3つの対策で情報セキュリティーへのリスクの発生防止を強化しています。

具体的には、個人の責務と意識を明確にするために、社員一人一人が遵守すべき行動規範と情報セキュリティーの遵守について「ビジネス・コンダクト・ガイドライン（以下、BCG）」としてまとめており、世界中の全社員がこれに従って行動するように求めています。BCGは毎年内容が更新され、すべての社員は、毎年必ず研修を受けた上で同意の署名を行います。BCG違反者に対しては解雇を含む厳正な処分が課されることも明記されています。また、全社員は、毎年セキュリティー研修を受講し、最新のセキュリティー脅威とその対策について理解を深め、日ごろのセキュリティー遵守の意識を高めます。

ITセキュリティーに関するコーポレート・スタンダードとしては、Information Technology Corporate Standard（以下、ITCS）という規定を策定し、プロセス・オーナーの下で継続的にオペレーショナル・リスク対策の見直しを実施します。ITCSには、サーバー、ネットワーク、アプリケーションなどのセキュリティー基準を定めたサーバー基準と、クライアントPCや業務上の情報取り扱い・管理、セキュリティー事故予防・対策などの基準を定めたクライアント基準を規定しています。

そして、IBM社員が業務で使用するすべてのPCには、ITCSの遵守状況を自動的にチェックするツールや、社内基準として必要とされている各種パッチ・アプリケーションの導入・適用を行うソフトウェア更新管理ツール、ハード・ディスク・ドライブ（HDD）全体を暗号化するツール、USBメモリーや外付けHDDなどのポータブル記憶媒体への情報の書き出し時にデータを暗号化するツールなどを導入しています。これらのツールを活用することにより、万が一IBM社員がPCを紛失しても情報が外部に流出するなどの事態を防止するための管理を日常的に行なっています。

グローバル・ビジネスに不可欠なグローバル・ガバナンス・モデル

グローバルにビジネスを展開する企業が、世界中のビジネス機会に合わせて迅速に経営資源を再配置し、各地域の市場に効率的に適合していくためには、情報セキュリティーについても、グローバル・ガバナンスを強化し、全社レベルでリスクを管理することが重要となります。

前述の通り、IBMでは情報セキュリティーをERMの1つと位置付け、米国本社が強い統制力をもって情報セキュリティーの取り組みをけん引しています。本社は、情報セキュリティーの統一されたプロセスや仕組みを通じてガバナンスを維持し、またグローバル戦略や投資方針と連動して、セキュリティーに関する投資を最適化しています。ただし、実際のセキュリティー管理活動は地域ごとに行い、地域で起きた事象に即時に対応できる体制を構築し、柔軟性と迅速性を確保しています。

今後は、さらに多くの日本の企業が海外に進出していくでしょう。先進国では情報そのものが利益の源泉であることが十分認識されているのに対して、まだ多くの国では情報の取り扱いに関する意識が浅く、情報セキュ

リティーに関するリスクも高いといえます。情報セキュリティーに関するグローバル・ガバナンスを強化するためには、事業展開するすべての国・地域の法律や制度、慣習、マーケット・ニーズ、国民性などを分析した上で、情報セキュリティーのリスクが高い国に合わせてグローバル・スタンダードを策定し、遵守していく必要があるでしょう。IBM では、セキュリティーのあらゆる取り組みはある一国の独自の施策ではなく、世界中で一貫した共通方針をもって展開されています。さらに特長的なのは、そこに経営層の強力なリーダーシップがあることです。

経営トップがけん引する攻めのセキュリティー対策

情報セキュリティーに対する課題は企業リスクであるという認識に基づき、経営層が主体的に関与して、意思決定を下す必要があります。自社にとって保護すべき情報を特定し、それに対するリスクやそのインパクトを経営層自ら認識しなければなりません。

対策の内容は、ビジネスの環境や投資できるコストによって変わる上、セキュリティーの強化と情報システムやネットワークの利便性とがトレードオフになる場合もあります。そのバランスをどこで取るのか、予算に応じて何を重点的に守るのか、組織・体制をどうするのか。こうした意思決定は、情報システム部門だけではなく、企業の経営層が果たすべき役割です。

昨今の厳しい経済環境にあっても、CISO が情報セキュリティーを経営戦略の一環として経営層に助言し、経営層自らがセキュリティー対策について意思決定を下す体制が求められる時代にきていると言っても過言ではありません。IBM では、1 人の CIO がグローバル全体の情報システムを統括しており、各国にはグローバルの全社方針に基づき施策を展開する責任者がいます。情報セキュリティーに関しては各国に CISO が置かれ、前述の通り、物理セキュリティーやプライバシーなどを担当する役員と組織横断的な連携する体制を確立しています。

現在、企業が取り組むセキュリティー対策は、予防対策に重点を置く守りのアプローチが主流ですが、これからは、情報セキュリティー・リスクは必ず起こるものとして想定し、ERM の観点から、人、データ、アプリケーション、IT 基盤のあらゆるレイヤーでプロセスと組織体制を整備する、攻めのアプローチへと変わっていかなければならないと考えます。

日々変化するセキュリティーの脅威への対応をさらに強化

IBM は、サイバー攻撃に代表される情報セキュリティー事件に関して、現時点で想定されるリスクへの対策を取る一方で、日々変化する脅威に向けて対応を一層強化する必要があると認識しています。

そのため、IBM Tivoli Endpoint Manager を全社的に導入し、社員の PC の管理を強化し、セキュリティー・パッチの強制導入を実施しています。これは、起こり得るサイバー攻撃に備えた取り組みで、全 PC を把握し、問題があると判断した PC について遠隔から解析し、強制的に切り離すなど即時の対応を取れるようにしています。また、新たにセキュリティー専門の緊急対応チーム（Computer Security Incident Response Team：以下、CSIRT）を設立し、マルウェアの解析や、セキュリティー事件の原因究明に必要な解析や証拠収集を行うフォレンジックなどのインシデント対応を通じて、機密情報を守るために必要な活動を 24 時間体制で実践しています。CSIRT については、日本の企業各社でも設立が検討され、セキュリティー専門チームによるインシデント対応の有効性の認識が高まっています。すでに設立された各企業の CSIRT 同士の連携もあり、国内外のセキュリティー・インシデント情報の共有を図り、企業間で連携して、サイバー攻撃への対策を強化する体制が始まっています。

情報セキュリティーのリスク・マネジメントは、業種やビジネス形態によりリスクの特定や評価が異なるため、IBM が実施しているセキュリティー対策や BCP のプロセスがすべての企業で最適であるとは限りませんが、重視すべき視点や体制は共通です。そのような共通の視点や体制を踏まえながら、IBM は企業リスクとしての情報セキュリティー対策を推進されるお客様をサポートする活動を展開しています。今後もその活動をより拡充させていくために、これまで IBM が講じてきた情報セキュリティー対策の経験を生かし、お客様に向けたソリューションをさらに充実させていきたいと考えます。