IBM Institute for Business Value

デジタル時代における脅威の管理

経営幹部によるセキュリティー、リスク、およびコンプライアンスへの取り組み

IBM Institute for Business Value

IBM グローバル・ビジネス・サービスは、IBM Institute for Business Value (IBV) を介して、民間会社あるいは公共機関の重要な課題に関し、事実をベースにした戦略的な考察を経営者の皆さまに提供しています。このエグゼクティブ・レポートは、IBV のリサーチ・チームによる詳細な調査に基づいてまとめられました。これは、企業がビジネス価値を実現するために役立つ分析と視点をお届けするという IBM グローバル・ビジネス・サービスの継続的な取り組みの一環です。レポート作成者へのお問い合わせ、内容に関するご質問は、e-メール (*iibv@us.ibm.com*) でご連絡ください。IBM Institute for Business Value のその他の調査については、*ibm.com/iibv* に記載されています。

John Lainhart、Steve Robinson、Marc van Zadelhoff 共著

最近メディアで盛んに取り上げられるようになったことで、

さまざまな業界の企業に影響を及ぼすセキュリティー違反が急増しているという事実が浮き彫りになっています。こうしたセキュリティー障害により、その影響を受けた企業は莫大な出費を余儀なくされているだけでなく、消費者の信頼とブランドの良い評判を大きく損なっています。セキュリティーの問題は、もはや IT 部門の職責に委ねられるものではなく、今や間違いなく経営幹部の優先事項になっています。組織は、今日の情報主導経済におけるセキュリティーの脅威への取り組みとコンプライアンス要件の管理に向けて、より体系的でプロアクティブなアプローチへと移行する必要があります。

世界のデジタル化と相互接続が進むにつれて、新たな脅威や情報漏洩の危険性が高まってきています。今日では、商品、パスポート、建物、動物などのさまざまなものに対して、何十億という RFID タグが取り付けられています。2010 年末にはインターネット・ユーザーの数が 20 億人を超え、携帯電話の契約件数が 50 億件の水準を突破したことで、全世界のほぼ 3 人に 1 人がインターネットを利用するようになっています。[1] 2020 年までには、自動車、電気製品、カメラなどの 500 億を超えるデバイスが、デジタル形式で接続されるようになることが予想されています。[2] こうした複雑な組み合わせはさらに激化して、世界で生成および複製されるデジタル情報の量は 2020 年までに、およそ 35 兆ギガバイトという想像を絶する規模にまで膨れ上がるでしょう。[3]

データの量が増大しているだけでなく、それに伴うデジタル資産の価値も同様に高まっています。顧客の機密情報や知的財産、さらには主要な機器類の制御さえも、すべて電子形式へと次第に変わってきています。これらの資産に悪影響を及ぼす攻撃は、単に IT 部門だけでなく、組織全体に重大な影響を及ぼす可能性がはるかに高くなっています。例えば、Stuxnet (スタックスネット) ウィルスを見てみましょう。このウィルスは、ウランの精製を制御するプロセス・コントローラーの機能を狂わせて、この極めて危険な物質を安全に処理して制御する能力を低下させました。[4] この発生事象は、組織の技術インフラストラクチャーを狙った攻撃が、重要な業務工程に明らかに影響を及ぼすことを実証しています。

データ、デバイス、および接続の急増という紛れもない事実もさることながら、それよりもさらに切迫したその他の要因により、企業ではセキュリティーおよびコンプライアンスの管理方法の変更が不可欠となりつつあります。経済利益などの犯罪的理由、復讐や欲求不満といった個人的理由、あるいはテロ行為のような政治的理由のいずれにせよ、組織内に格納されている貴重なデータが、システムを攻撃する人々の標的となっています。情報や情報処理インフラストラクチャーを狙った攻撃は、その発生頻度が高まってきているとともに、高度な「専門的手口」で組織的に行われるようになってきています。

したがって、重要情報およびその関連資産を保護することが、これまで以上に重要でありながらも、より困難な課題となっています。セキュリティーはその注目度を急速に高めており、ブランドに対する潜在的リスクを評価している CMO、有害事象の財政的影響を理解している CFO、あるいは IT システムの障害が現行の業務運営に及ぼす影響を評価している COO のいずれを問わず、間違いなく経営幹部の新たな問題として浮上してきています。*セキュリティー・インテリジェンス*、すなわち潜在的脅威をプロアクティブに予測し、特定し、そしてそれに対処する能力が、デジタル時代における新たな優先事項となります。

セキュリティー面の課題がかつてないほどの規模に拡大

データ、デバイス、および接続の増加に伴い、セキュリティー面の課題の数が増加するとともにその範囲も拡大しつつあります。そうした課題は、「外的脅威」、「内的脅威」、および「コンプライアンス要件」という 3 つの大きなカテゴリーに分類されます。

外的脅威

最近では、主要な企業や政府組織に対する外部からの攻撃が急増しています。これまでこうした脅威は、単独で行動する個人によってもたらされていました。しかしこうした攻撃は、次第に組織的に行われるようになってきており、「ハクティビスト」と呼ばれる組織的ハッカー集団から、犯罪企業、さらには国が支援する組織に至るまでのさまざまなグループによって仕掛けられるようになっています。アタッカーの動機付け要因は、もはや利益の追求だけに限られたものではなく、時として自らの威信やスパイ行為までも含まれる場合があります。こうした攻撃は、顧客データベースや知的財産、さらには情報システムによって稼動する物的資産までも含めた、これまで以上に重要な組織の資産を標的にしています。

こうした外的攻撃は、財務面に重大な影響をもたらします。例えば、Epsilon からの顧客データの流出により、何百万人もの消費者の E メール・アドレスが危険にさらされて、多数の企業顧客に直接的に悪影響が及びました。初期対応とより長期的な訴訟リスクに伴うコストは、数億ドルに上ると見積もられています。[5] 最近では、そのほかにも金融サービス業界、メディア・エンターテイメント業界、小売業界、および通信業界の多くの企業から、顧客の個人情報や財務情報に対する同様のタイプの違反が報告されており、そのいずれにおいても膨大な IT コスト、訴訟費用、および調整コストが発生しています。

内的脅威

多くのケースでは、情報セキュリティーの違反がなくならない原因は、部外者ではなく、内部関係者の行為にあります。今日の内部関係者というのは、従業員の場合もあれば、請負業者、コンサルタント、さらにはパートナーやサービス・プロバイダーの場合もあります。こうした違反は、不注意な行動や管理上のミス (他者にパスワードを教える、バックアップ用のテープやラップトップを紛失する、不注意により機密情報が公開されるなど) から、不満を抱えた従業員による意図的行為にまで及びます。

これらの行為は、外部からの攻撃に引けを取らないほど危険な場合があります。その一例として、機密記録の無断公開を伴った Wikileaks の事件では、米国政府に数百万ドルに及ぶ損害がもたらされるとともに、世界各国の政府との関係も損なわれていると報道されています。[6]

コンプライアンス要件

企業は、着実にその数が増えてきている、それぞれ独自の基準と報告要件を持つセキュリティー関連の国、業界、および現地の命令への取り組みを求められています。そうした命令の例としては、米国 Sarbanes-Oxley (SOX) 法、J-SOX、COSO、COBIT、さまざまな ISO/IEC 国際標準、米国の HIPAA/HITECH、EU のプライバシー指令、インドのデータ・セキュリティーおよびプライバシー標準、PCI DSS、BASEL II など数多くのものが挙げられます。これらへの準拠には、問題の優先順位付け、適切なポリシーおよび規制条項の策定、ならびにコンプライアンスの監視を行うのに、膨大な時間と労力を要することがよくあります。

経営幹部の優先事項が影響を受ける

脅威やコンプライアンス要件は、個々の重役が各自の優先事項を完遂する能力に重大な影響を及ぼすことになります。次第にテクノロジーが果たす役割の重要性が増してくるにつれて、情報セキュリティーに関連する課題は CIO の職務領域を大きく越えるようになってきています。IBM が 2008 年から行っている 1 万 3,000 人を超える経営幹部のエグゼクティブとの協議では、エグゼクティブ・チームのどのメンバーも、セキュリティー問題の影響を受けていることが示されています (図 1 参照)。

経営幹部の各エグゼクティブによって、高い優先順位を付けるべきセキュリティー課題が異なっていますが、企業は今日のセキュリティー・リスクへの取り組みに向けて、まとまりのある形で行動する必要性を無視するわけにはいきません。これまでならもっと明確に描き出されていたかもしれないセキュリティー問題に対する責任が、物事がうまくいかない場合の潜在的ダメージと同様に、現在では組織の縦割り機構と重なり合っています。

例えば、ブランドの強化に徹底的に重点を置いている最高マーケティング責任者 (CMO) は、セキュリティー違反が原因で個人情報を紛失してしまった場合、顧客の信頼とブランドの良い評判を失うリスクにさらされる可能性があります。これは間違いなく、どの企業にとっても最大級のリスクであり、良い評判が損なわれることになれば経営幹部全体による取り組みが必要になります。

主に役員会の他のメンバーによって管理されているセキュリティー・リスクの例には、以下のようなものがあります。

- *最高経営責任者 (CEO)* は、自社の知的財産およびビジネス上の機密データが、内部関係者または部外者による不正利用の危険にさらされていないかどうかを気にかける必要があります。これらのタイプの侵入は、市場シェアおよび評判の潜在的喪失、規制による営業停止に関連する業務運営リスク、ならびに潜在的刑事責任という点において、重大な影響をもたらす可能性があります。

	CEO	CFO/COO	CIO	CHRO	CMO
CxO の優先事項	• 競争力のある差別化の維持	• 規制順守	• モバイル・デバイスの使用拡大	• グローバルな労働力への柔軟性の実現	• ブランド強化
セキュリティー・リスク	• 知的財産の不正利用 • ビジネス上の機密データの不正利用	• 規制要件への取り組み不履行	• データの急増 • 安全が確保されていないエンドポイントと不適切なアクセス	• 機密データの流出 • 内部関係者の不注意な行動	• 顧客や従業員からの個人情報の窃盗
潜在的影響	• 市場シェアおよび評判の喪失 • 刑事責任	• 監査における不合格 • 罰金、損害賠償、および刑事責任	• データの機密性、保全性、および可用性の喪失、またはいずれかの喪失	• 従業員プライバシーの侵害	• 顧客信頼の喪失 • ブランド評判の喪失

出典: IBM Institute for Business Value の経営幹部調査の一環として実施された、1 万 3,000 人を超えるエグゼクティブとの対面インタビュー

図 1: **セキュリティーおよびコンプライアンスのニーズへの取り組みは経営幹部全体の優先事項**

- *最高財務責任者 (CFO)* は、特に規制上の指針に取り組む必要があります。そうした指針のセキュリティー条項の順守を怠ると、監査における不合格とその結果としての組織に対する処罰はもとより、自分自身や自らの組織に対する刑事責任の追求という事態に陥る可能性もあります。
- *組織の柔軟性および機動性を高めようとしている最高情報責任者 (CIO)* は、データの急増、および安全が確保されていないエンドポイントやデータへの不適切なアクセスの増加に関する課題に取り組まなければなりません。こうした問題は、いずれもデータの機密性、保全性、または可用性の喪失につながる可能性があります。
- *最高人事責任者 (CHRO)* は、労働力の柔軟性の向上を目指す際には、機密データの流出の可能性はもとより、従業員のプライバシーの侵害につながり得る内部関係者の潜在的に不注意な行動も認識しておく必要があります。

要するに、セキュリティー問題というのは、もはや CIO だけの責任下に置かれるものでもなければ、単純に最高情報セキュリティー責任者に委任できるものでもありません。こうした問題に対しては、経営幹部全体による注意と行動が必要とされます。

絶え間ない「セキュリティー・インテリジェンス」の構築

リスクの急増と重大さの双方に取り組むために、組織はセキュリティーに対する高度に自動化されたプロアクティブなアプローチを検討する必要があります。つまり、ビジネスの不可欠な要素として、*セキュリティー・インテリジェンス* を組み込む必要があるということです。これには、物理的セキュリティー、データ分類、従業員の認識や統制といった、幅広い問題をカバーする包括的アプローチが必要となります。

多くの組織では、セキュリティー・インテリジェンスは 3 つの段階にわたって進化します。こうした進化は、脅威の特定、追跡、およびそれらへの取り組みに対する、手動アプローチから次第に自動化されたプロセスの利用への移行を表しています。トレンドは、セキュリティー問題に対するリアクティブなアプローチではなく、プロアクティブな予測へと向かっています (図 2 参照)。

出典: IBM による分析

図 2: **セキュリティー・インテリジェンスの構築に向けた構造化された 3 段階アプローチ**

- *基礎的* – 組織は、物理アクセスと仮想アクセスの双方を規制する周辺防御の採用に重点を置きます。周辺防御は、発生事象や違反の手動報告に対する入力情報をもたらします。基礎的段階にある企業は、有益な第 1 ステップであるファイアウォール、アンチウィルス、アクセス制御、および手動による報告機能を配備しています。ただしそれらは、実際のセキュリティー態勢に対する洞察がほとんどない状態で、リアクティブな手動操作モードで運用されています。

- *熟達* – セキュリティーが、IT アプリケーションと業務運営の構造の中に層状に組み込まれています。この一連の流れの中には、主要なアプリケーション、データベース、およびビジネス・プロセスへのセキュリティーの組み込みが含まれます。熟達段階においては、セキュリティーがより包括的なものになっていきますが、その一方で組織のセキュリティーへの取り組みに複雑さが加わることにもなります。その結果、セキュリティーがより幅広く拡散した協調性の低いものになることから、企業は依然としてセキュリティー・インテリジェンスについては不十分な状態にとどまります。
- *最適化* – 組織は、予測的で自動化されたセキュリティー・アナリティクスを利用して、セキュリティー・インテリジェンスに向けて邁進します。この一連の流れには、潜在的な違反が生じ得る部分の予測とその発生の予防を目的とした、過去の侵入、従業員の活動、およびその他のデータ・ソースのプロファイル作成が含まれるため、セキュリティーが最適化されています。

これら 3 つの段階のそれぞれに、さらに不注意と故意の双方によるセキュリティー事象に対する準備のための層が付加されます。企業のエコシステム全体を通してセキュリティー・ギャップを特定して埋めるために、組織は自らの最も切迫したニーズを満たすための分析能力を探究して利用する必要があります。以下に挙げる 4 つのセキュリティー・ドメインの徹底的な評価を行うことで、ガバナンス、リスク管理、およびコンプライアンスが体系的に改善されて、組織をセキュリティー・インテリジェンスへと導くことができます (図 3 参照)。

- *ひと* – パスワードを介したアプリケーションごとのアクセス制御から、ダッシュボードおよび特権ユーザー制御を通じてユーザー・アクセスを制御する、役割ベースのアプローチへと切り替えます。
- *データ* – 基本的なアクセス制御および暗号化方式の枠を超え、データ・ガバナンスを向上させてデータの使用法とフローを管理することでデータを保護します。
- *アプリケーション* – 既存のアプリケーションにおける脆弱性のスキャンへの依存から、不正行為の検出と新規アプリケーションへのセキュリティーの組み込みへと進化させます。
- *インフラストラクチャー* – 無許可アクセスやウィルスのブロッキングのようなリアクティブな方法を、高度なネットワーク・モニタリングや科学捜査を可能にすることでシステムの安全を確保する、プロアクティブな方法に置き換えます。

セキュリティー・ドメイン	現在	セキュリティー・ギャップ	将来: セキュリティー・インテリジェンス	
ひと	アプリケーションごとに ID 管理		役割ベースのダッシュボードと特権ユーザー管理を採用	高度な相互関連付けおよびディープ・アナリティクスを応用
データ	アクセス制御および暗号化実施		使用状況監視による情報漏洩を抑制	
アプリケーション	脆弱性スキャン		開発初期からセキュリティーを実装	
インフラストラクチャー	望ましくないネットワーク・アクセスおよびウィルス・ブロック		リアルタイムでの高度な脅威検出および科学捜査を実施	

リアクティブ → *プロアクティブ*

出典: IBM による分析

図 3: **物理的、技術的、および人的資産を管理するためにはバランスの取れたアプローチが必要**

経営幹部のための 3 段階の計画

経営幹部のエグゼクティブは、セキュリティー・インテリジェンスの構築に向けて以下の 3 つの重要なステップを踏む必要があります。

- **情報を得る。**ビジネスおよび IT のリスクの評価に対する体系化されたアプローチに取り組みます。
- **整合させる。**拡張された企業全体にわたって高度なセキュリティーを導入、実施します。
- **スマートになる。**アナリティクスを利用してプロアクティブにリスクを浮き彫りにし、脅威の特定および監視とそれに対する取り組みを行います。

1. 情報を得る。

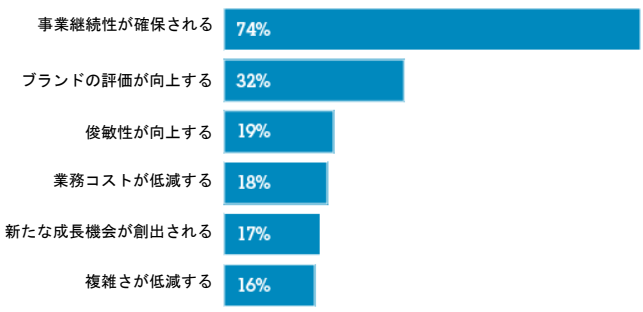
「情報を得る」には、より広範なエンタープライズ・リスク管理フレームワークの一部としての、IT セキュリティー・リスクへの取り組みが伴います (図 4 参照)。

出典: IBM Institute for Business Value「2010 IBM Global IT Risk Study2010 IBM Global IT Risk Study」(2010 年 9 月)

図 4: **オペレーショナル・リスク管理に取り組むための主要ステップ**

このビジネスおよび IT のリスクの評価に対する体系化されたアプローチには、主要な脅威およびコンプライアンス命令の特定、セキュリティーに関する既存のリスクおよび課題のレビュー、リスク管理プロセスおよび共通抑制フレームワークの導入および実施、ならびに危機が生じた場合のインシデント管理プロセスの実施が含まれます。もう 1 つの重要な対策は、セキュリティー関連の問題について取締役会および同僚と定期的に連携し、ビジネスの中で IT リスクに関する会話がなされるように推進する、経営幹部のリスク担当エグゼクティブに権限を付与することです。

IBM Global IT Risk Study の回答者は、IT リスク管理に投資することにより、特に事業継続性 (74%) と会社の評判の保護 (32%) という分野において、著しいビジネス上のメリットがもたらされ得ると考えています (図 5 参照)。回答者によれば、IT リスクの管理は防御的戦術以上のものとみなされるべきであるということです。またそれらの回答者は、IT リスクの管理の向上によって実現したメリットとして、俊敏性の向上、コストの削減、新たな成長機会、および複雑さの低減も挙げました。[7]



出典: IBM Institute for Business Value「2010 IBM Global IT Risk Study2010 IBM Global IT Risk Study」(2010 年 9 月)

図 5: **IT リスク管理の向上によるメリット**

事例:

IT セキュリティー管理のリスクに関連する監査上の課題が IT ガバナンスの刷新を活性化

米国の大規模金融機関は、社内外の双方における IT ガバナンスおよびビジネス管理の重大な課題に直面していました。同社の外部監査員からは、サーベンス・オクスリー (SOX) 法上の欠点をはじめとする数々の重大な欠陥が挙げられ、一方で内部監査では、IT セキュリティーに関するいくつもの望ましくない報告書が作成されました。

同社は、業界のベスト・プラクティスに基づく包括的で強力なガバナンス・プログラムと併せて、新たな制御手段が確実に定期的に更新され改善されるようにするのに役立つシステムを導入する準備を整えました。そのプロセスでは、はじめに、IT の汎用制御、アプリケーション制御、IT ガバナンスなどを含めた、同社のセキュリティーおよび制御システム全体の評価が行われました。セキュリティー・プロセスのレビューや、ポリシー、標準、および手順の作成または更新などを含め、組織の情報セキュリティー・ガバナンスが評価されました。

特定されたギャップは、明確なポリシー、標準、および手順を持った 4 つの IT ガバナンス委員会の設置を通じて埋められました。さらに同社は、セキュリティー、データ保全性、変更管理、および業務運営の分野における財務報告に関連する問題点や欠点を効果的に是正する、IT ガバナンス・フレームワークおよび補助ツールセットも導入しました。

こうした取り組みの結果、この金融機関は外部監査員から、財務諸表に対する健全な監査結果と SOX 法に関する肯定的所見を得ることに成功しました。これは、それ以前の 3 年間にわたり同社が成し遂げることができなかったことでした。このことにより、同社は証券取引委員会 (SEC) に新たに普通株を登録することができ、それによって投資家の信頼が高まって株価が上昇しました。さらに同社は、IT ガバナンスとセキュリティー・プロセスおよび慣行の継続的改善を可能にするための、IT ガバナンス・ライフサイクル・プログラムを制度化することもできました。

2. 整合させる。

セキュリティーは、組織の境界線で止まるものではありません。企業が成功するためには、拡張された企業全体にわたって高度なセキュリティーを導入して実施する必要があります。これには、以下に挙げる主要な利害関係者を関与させることが含まれます。

- *顧客* – 個人情報に関するポリシーを策定して伝達します。透明性を維持し、プライバシーの侵害に迅速に対処します。
- *従業員* – セキュリティーおよびプライバシーに関する明確な期待事項を設定します。セキュリティー・リスクを特定してそれに対処するための教育を施します。システムとデータの双方へのアクセスとそれらの使用法を管理します。
- *パートナー* – サプライチェーン全体の組織と協力し、セキュリティー基準を設定して実施します。通常の業務運営の一環として、セキュリティー事象も含めたリスクに関する報告とその管理を行います。
- *監査員* – 企業と IT のリスクを整合させます。制御フレームワークに貢献します。規制および企業ポリシーを定期的にレビューします。
- *規制官* – 規制に関するリスクを管理するとともに、既存の規制に対するコンプライアンスを実証します。要件の変化に基づいて、既存の制御対策をレビューして修正します。

事例:

効果的なガバナンスが業界のコンプライアンスを促進して監査の即応性を改善

例年、何度も監査に入られるという状況に直面していた米国の医療保険会社は、各々の監査報告書に対応しなければならない状況から脱却し、リスクを管理して賢明な抑制対策を導入し維持していきたいと考えていました。さらに同社は、そうした監査がビジネスに及ぼす影響を軽減することも望んでいました。それと同時に、同社では、医療保険の相互運用性と説明責任に関する法律 (HIPAA) や全米保険監督官協会 (NAIC) のモデル監査規則に関連するものなどといった、保険業界の新たな規制要件に対するコンプライアンスを確立する必要もありました。

この問題を解決するには、同社の IT プロセス・ガバナンス構造を見直す必要がありました。その取り組みの一環として、同社は 15 の不可欠な IT プロセスに対するガバナンスを含め、すべての業務および事業部門全体に及ぶ業界標準の IT ガバナンス制御を導入しました。そして、そのそれぞれに対して、循環的プロセスが用いられました。それらは、ガバナンス手順の確立、導入、および運用、それらの手順のテスト、そして最後に結果のモニタリングおよび報告が行われることで、リスクが特定されてその抑制のためのフレームワークが定義されます。

この新たな抑制対策は、同社が業界の規制および標準に対するコンプライアンスを監視するのに役立つだけでなく、ビジネスと IT の整合性の向上、リスクの管理、およびセキュリティーの向上にも役立ちます。現在同社では、監査に対してより効率的で一貫した対応がなされており、監査への対応に要する労力がほぼ半減しています。

3. スマートになる。

アナリティクスを利用してプロアクティブにリスクを浮き彫りにし、脅威の特定および監視とそれらに対する取り組みを行います。企業におけるセキュリティー防御の強化の必要性が高まるにつれて、予測的分析の利用が次第に重要な役割を果たすようになります (図 6 参照)。予測的分析を行うことで、複雑な相互関連付けを行って高度な持続的標的型攻撃を検出し、ガバナンスの意識を定着させ、また自動化された全社的リスク・プロセスを整備することができます。

これには、以下のことを行う能力が含まれます。

- 過去の違反パターンおよび外部の脅威を特定して、潜在的な攻撃対象領域を予測する。
- システムに対する従業員の行動を調査して、潜在的な悪用パターンを特定する。
- 潜在的なセキュリティーの脅威に注目して外部環境を監視する。

セキュリティー・インテリジェンス

	ひと	データ	アプリケーション	インフラストラクチャー
最適化	• ガバナンス、リスク、およびコンプライアンス • 高度な相互関連付けおよびディープ・アナリティクス			
	• 役割ベースのアナリティクス • 特権ユーザー制御	• データ・フロー・アナリティクス • データ・ガバナンス	• 安全なアプリケーション開発 • 不正行為の検出	• 高度なネットワーク・モニタリング / 科学捜査 • 安全なシステム
熟達	• ID 管理 • 強力な認証	• アクティビティー・モニタリング • データ損失の防止	• アプリケーション・ファイアウォール • ソース・コード・スキャン	• 資産管理 • エンドポイント / ネットワークのセキュリティー管理
基礎的	• パスワードおよびユーザー ID	• 暗号化 • アクセス制御：	• 脆弱性のスキャン	• 周辺部のセキュリティー • アンチウィルス

出典: IBM による分析

図 6: **アナリティクスを利用してプロアクティブにリスクを浮き彫りにし、脅威の特定および監視とそれに対する取り組みを実施**

事例:

アナリティクスがセキュリティー・リスク機能の向上に貢献

グローバル規模の製薬会社は、脅威に対処するための「よりスマートな」方法を模索しながら、マルチベンダー型のセキュリティー環境に伴うコストの削減と複雑さの軽減を望んでいました。同社の旧式のセキュリティー・インフラストラクチャーでは、報告されている脅威と脆弱性データとの相互関連付けが不十分であったため、本当に重大な発生事象を特定することが困難となっていました。さらに、複数のセキュリティー・デバイスからのアラートをリアルタイムでプロアクティブに監視して、違反が発生する前に対策を講じるようにするためには、熟練したリソースが必要とされていました。

セキュリティー・ソフトウェア・ソリューション、コンサルティングの専門知識、およびマネージド・サービスを利用して、同社は保護を拡大すると同時にコストと複雑さを軽減させることもできました。現在では、同社のコンピューティング環境全体にわたって何百万ものマルチベンダー型セキュリティー・イベントの分析が行われていて、また高度なアナリティクスによって、リアルタイムにセキュリティー・イベント・データが処理されています。問題を迅速に是正して脆弱性へのアクセス機会を削減するために、エキスパート改善ガイダンスが用いられています。さらに、報告書のおかげで、同組織は時間の経過とともに脆弱性および脅威となるデータを追跡してその傾向を見極め、自らのセキュリティー態勢に対するより幅広い見方を得ることもできます。

このセキュリティー改革の一環として、同社は 5 つのベンダー環境を 1 つに集約することができました。さらに重要なこととして、プロアクティブ・アプローチを取ることにより、同社ではセキュリティー管理コストを 57% 削減するとともに、重大なセキュリティー・イベントも 1 日あたり 1 万件からわずか 15 件にまで減少しました。

セキュリティー・インテリジェンスを構築しているか

脅威の可能性と、より高度なセキュリティー・インテリジェンスを利用してそれらのリスクを軽減する機会に基づいて、組織は以下の質問に対する回答について考察する必要があります。

セキュリティー・ドメイン全体

- セキュリティー・リスクの評価に向けてどのような計画を立てているか。
- どのようにすれば、ドメイン全体にわたる脅威の検出とコンプライアンスの報告を行うことができるか。
- 自社にはログの保存および監査の機能があるか。
- 発生事象対応および災害復旧への取り組みにどのプロセスを使用するか。
- 社内外の主要な利害関係者をどのようにしてセキュリティーの問題に関与させるか。

ひと

- ID プログラムをどの程度まで展開しているか。
- 認証済みユーザーの行動をどのようにして把握するか。
- ID および役割ベースの管理の自動化に向けてどのような計画を立てているか。

データ

- どのような方法で機密データの分類および暗号化を行っているか。
- 認証済みユーザーの行動をどのようにして把握するか。
- 特権アクセスを含め、データへのアクセスをどのようにして監視するか。

アプリケーション

- セキュリティーが、どのようにして最初からアプリケーション開発プロセスに組み込まれているか。
- 自社の Web サイトの脆弱性について、どのようにして定期的にテストしているか。
- レガシー・アプリケーションからの潜在的な機密漏れの検査に対して、どのようなアプローチを取っているか。

インフラストラクチャー

- 接続されたデバイスに対して、どのようにして迅速にパッチの適用を行っているか。
- どのような方法で、インバウンドやアウトバウンドのネットワーク・トラフィックを監視しているか。
- 新たなイニシアチブ (クラウドやモバイルなど) に、どのようにしてセキュリティーを組み込んでいるか。

結論: 本当のリスクには経営幹部全体による統合的対処が必要

複雑さが徐々に増し、相互接続が進む今日の世界では、リスクは現実のものであり急増しています。セキュリティーの問題を CIO だけに委任している企業では、リスク要因が複合的に絡み合って状況がさらに悪化しています。ますます、企業では、指導部の各メンバーが、組織全体を流れるデータおよび知的資本の安全性の確保において重大なかかわり合いと強力な役割を持つようになっています (図 7 参照)。そこには 1 つの共通する特徴があります。「今日のセキュリティーは、単なる技術的問題にとどまるものではない」というものです。むしろそこでは、リスク、投資、およびセキュリティー問題に対する予防的アプローチの採用に関する率直な議論が必要とされます。

言うまでもなく、潜在的リスクや偶発的事象のすべてに対して、費用対効果の高い方法で取り組むことができるわけではありません。したがって組織は、考えられるすべての脅威から身を守ろうとするのではなく、潜在的リスクのビジネスへの影響に優先順位を付けなければなりません。

しかしながら、そうした優先順位付けは、各自の特定の責任分野に関する独自の見方を提示する、経営幹部の複数のエグゼクティブからの意見や情報によって左右されることになります。

IBM Institute for Business Value が今回実施した調査の詳細については、*iibv@us.ibm.com* までお問い合わせください。その他の調査の一覧は、以下の Web サイトでご覧いただけます。

ibm.com/iibv

IBM Institute for Business Value の最新の洞察をいち早く入手することができます。IBV の調査をもとに、戦略的洞察の提供と提案を行うエグゼクティブ・レポートを中心とした毎月発行の弊社電子ニュースレター、IdeaWatch をご購読ください。

ibm.com/gbs/ideawatch/subscribe

CEO	CFO	COO	CIO	CHRO	CMO
セキュリティー・リスクが株主の価値や信頼に影響を及ぼすのを防ぎます。	不都合なセキュリティー・イベントの財務的影響を認識します。	IT システムの障害が現行の業務運営に及ぼす影響を評価します。	情報セキュリティーの低下がビジネス全体に及ぼす副次的影響を理解します。	従業員データの不当な流出に伴うリスクを見極めます。	セキュリティー違反に伴うブランドの問題に取り組みます。

出典: IBM による分析

図 7: **セキュリティーは経営幹部の責任**

変化する世界に対応するための最適なパートナー

IBM はお客様と協力して、業界知識と洞察力、高度な研究成果とテクノロジーの専門知識を組み合わせることにより、急速な変化を遂げる今日の環境における、卓越した優位性の確立を可能にします。私たちは、ビジネスの設計と実行に対する統合的なアプローチを通じて、戦略を行動に転換するためのサポートを提供いたします。また、17 業種を網羅する業界専門知識と世界 170 の国と地域に及ぶグローバルな能力を駆使し、お客様がグローバルに変化を予測し、新たな機会から利益を創出する支援をいたします。

著者について

John Lainhart は、IBM グローバル・ビジネス・サービスの、Global Security & Privacy Service と U.S. Public Sector Cybersecurity & Privacy Service のそれぞれのエリア・リーダーを務めています。また、米国公認会計士協会 (AICPA) の Assurance Services Executive Committee の Data Integrity Task Force と、Center for Internet Security の Strategic Advisory Council に、IBM の代表として参加しています。これまで情報システム・コントロール協会および IT ガバナンス協会において、国際会長をはじめとする数々の職位に就いてきており、現在は枠組み委員会のメンバーを務めるとともに、CobiT® 5 Task Force の共同議長、ならびに CobiT®、ValIT®、および RiskIT® 関連のイニシアチブの IT ガバナンス担当ボランティア主任アドバイザーも務めています。連絡先: *john.w.lainhart@us.ibm.com*.

Steve Robinson は、IBM Security Solutions のジェネラル・マネージャーで、セキュリティー関連の製品およびサービス部門全体にわたる IBM セキュリティー・イニシアチブに対して、世界的責任を負っています。戦略リーダーとして、ソフトウェア、ハードウェア、およびサービス部門の開発チームはもとより、マーケティングおよびセキュリティー営業チームにもガイダンスを提供しています。現職に就く前は、2005 年から Rational ブランドの販売戦略および実施に対して責任を負う IBM Rational Software の Worldwide Sales 担当バイス・プレジデントを務め、1,000 人を超える営業プロフェッショナル、チャネル・チーム、およびビジネス・パートナー、システム・インテグレーター、ISV などを含む戦略的リレーションシップの拡張コミュニティーという、世界規模の部隊を率いていました。1984 年に IBM に入社して以来、営業、技術サービス、および製品管理部門において、数々の役員職および管理職を歴任してきました。連絡先: *steve_robinson@us.ibm.com*.

Marc van Zadelhoff は、IBM Security Solutions の世界戦略担当ディレクターで、IBM のソフトウェアおよびサービス・ポートフォリオのオファリング管理、予算、および位置付け全体に対して、グローバルに責任を負っています。この職務において、彼は IBM のお客様に対する諮問委員会を運営しており、世界中でお客様と会合を開いて、IBM の方向性を作り出しています。過去には IBM において、Tivoli のセキュリティー関連の M&A、買収した Internet Security Systems (ISS) 部門のマーケティング・チーム、そして直近ではグローバル・テクノロジー・サービス部門の Strategy, Portfolio & Business Development for IBM Security Services を指揮しています。Marc は戦略コンサルタントとしてそのキャリアをスタートさせました。連絡先: *marc.vanzadelhoff@us.ibm.com*.

協力者

Linda Ban: IBM グローバル・ビジネス・サービスの IBM Institute for Business Value の AIS Studies の Global CIO Study ディレクター

Hans A.T. Dekkers: IBM グローバル・ビジネス・サービスのアソシエート・パートナー

Peter Korsten: IBM グローバル・ビジネス・サービスの IBM Institute for Business Value のパートナーおよびバイス・プレジデント、グローバル・リーダー

Eric Lesser: IBM グローバル・ビジネス・サービスの IBM Institute for Business Value のリサーチ・ディレクター兼北米担当リーダー

Kristin Lovejoy: IBM BT/CIO 組織の IT リスク担当バイス・プレジデント

Wolfram Stein: IBM グローバル・ビジネス・サービスのコンサルティング・サービスのパートナーおよびバイス・プレジデント、Global Strategy & Transformation Service ライン・リーダー・エグゼクティブ

Nichola Tiesenga: IBM グローバル・ビジネス・サービスの Cybersecurity and Privacy の公共部門担当パートナー

Marisa Viveros: IBM グローバル・テクノロジー・サービスの IBM Security Services のバイス・プレジデント

参考文献

1 International Telecommunications Union. “Global Number of Internet Users, total and per 100 Inhabitants, 2000-2010.” United Nations. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/Internet_users_00-10_2.xls

2 Ericsson. “More than 50 billion connected devices – taking connected devices to mass market and profitability.” February 14, 2011. http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c

3 IDC “Digital Universe Study,” sponsored by EMC.May 2010.

4 McMillan, Robert. “Siemens:Stuxnet worm hit industrial systems.” ComputerWorld.September 14, 2010. http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

5 Greene, Tim. “Worst-case projected cost of Epsilon breach:$4B.” NetworkWorld.May 1, 2011. http://www.network-world.com/news/2011/050111-epsilon-breach-costs.html

6 Fildes, Jonathan. “What is Wikileaks?” BBC.December 7, 2010. http://www.bbc.co.uk/news/technology-10757263

7 Ban, Linda B., Richard Cocchiara, Kristin Lovejoy, Ric Telford and Mark Ernest. “The evolving role of IT managers and CIOs.” IBM Institute for Business Value.September 2010. http://www-935.ibm.com/services/us/gbs/thoughtleadership/ibv-global-it-risk-study.html

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
August 2011

GBE03423-JPJA-00