IBM **Center for Applied Insights**

# セキュリティー・リーダーのための新基準

*2013 年 IBM 最高情報セキュリティー責任者アセスメントから得た洞察*

*十分に実行しているか。適切な点に着目しているか。どのように同業者と比較すればよいか。最高情報セキュリティー責任者 (CISO) およびその他のセキュリティー・リーダーはこうしたことを繰り返し自問する。我々の調査から、こういった質問に対処するのに役立つ一連の先進的なビジネス規範、テクノロジーの実態および指標の実態が明らかになった。また、課題の範囲も明確化された。ベテランのセキュリティー・リーダーでさえ、さまざまなビジネス上の問題、モバイル・セキュリティー・ポリシーの構築、そしてビジネスやリスク、セキュリティーに関する完全に統合された評価指標を管理する方法について奮闘している。適切なビジネス規範との組み合わせを持ち、この重要なチャレンジに取り組んでいるセキュリティー・リーダーは、さらに万能なセキュリティー・リーダーへと進化し、新たな基準を設定している。*

## 調査について

IBM Center for Applied Insights は、2012 年 IBM CISO 調査 (タイトル「***戦略的見解に関する調査***」) を継続し、進展させるために、 IBM Security Systems および IBM Security Services と共同で、組織の情報セキュリティー責任者である 41 名のシニア・リーダーを対象に詳細なインタビューを実施した。インタビューの目的は、他のセキュリティー・リーダーの役割と影響力の強化につながる、特定の組織的なプラクティスと行動を明らかにすることであった。

継続性を持たせるために、インタビュー対象者は、より成熟したセキュリティー・リーダーを中心に、2012 年の調査参加者の中から採用した (採用者の 80% は以前の参加者だった)。インタビュー対象者は 4 カ国の幅広い業界に渡った。80% 以上が大企業の関係者で、およそ 3 分の 1 が 100 万米ドルを超えるセキュリティー予算を持っていた。

2012 年 CISO 調査で説明されているとおり、セキュリティー環境全体で要求の厳しい状況が続いている。巧妙化の一途をたどる脅威や、ますます高まるモバイルへの期待は重要な課題である。その結果と思われるが、セキュリティー・リーダーはシニア・エグゼクティブから大きな注目を浴びている。同時に、セキュリティー・リーダーは組織における影響力を増大するための取り組みを強化している 1。また、セキュリティー・リーダーが、組織における情報リスク・スペシャリストへと進化することを求める声も多くあがっている 2。CISO への注目度が高まり、CISO の役割を企業の保護以上に広げるよう求める声があがる中、組織のリーダーは多くの重要な問題に直面する。適切なチームとスキルはあるか?同じ業種の他のセキュリティー・リーダーと比較する方法はあるか?今は採用していないが今後従うべき手法はあるか?

前回の CISO 調査「戦略的見解に関する調査」で、我々はこうした質問の答えを出し始めた 3。我々の分析によって、3 種類のセキュリティー・リーダーが描かれた。インフルエンサー、プロテクター、レスポンダーである。そして、それぞれの成熟度と特徴を調査した。その段階では、成熟したセキュリティー・リーダーほど、堅固な体制とマネージメントのアプローチを適所に導入し、組織の範囲を拡大し、パフォーマンスを厳格に測定するということを立証した。

今年の調査では同様のパターンが見られたが、さらに深く調査することで、成熟したセキュリティー・リーダーでさえ奮闘している先進的プラクティスや一連の問題点の重要な結果が明らかとなった。3 つの分野 (ビジネス規範、技術の成熟度、指標) を深く掘り下げてみると、新しいセキュリティー・リーダーおよび経験豊富なセキュリティー・リーダーの双方を導くことのできる道筋が現れる。

## ビジネス規範:
## 相手の言葉で話し、懸念事項を軽減する

新しい CISO にどうアドバイスするか、将来どのようなスキルが重要となるか、出資者の信頼をどのように得るかを尋ねると、成熟したセキュリティー・リーダーは共通して同様のアドバイスを行った。しっかりとしたビジョンの重視、戦略と方針、幅広いリスク・マネージメント、および効果的なビジネス上の関係性を推奨した。セキュリティー・リーダーたちは、わかりやすく、セキュリティー用語ではない言葉でコミュニケーションをとることにより、常に信頼を構築していると報告している。セキュリティー・リーダーたちは、テクノロジーに関する能力を基盤とし、ビジネス洞察力を磨くために、こうした活動が一層重要になってくると考えている。

*「セキュリティーは難しい、だからセキュリティー担当者は特別な存在だ。彼らは物事を異なった視点でとらえる。我々はビジネスにとって重要ではない『テクノロジーのゴミ』をなくそうとしている。ビジネスでは白黒をはっきりする要があり、机上の空論は必要ない」*

– 最高技術責任者、保険

**経験豊富なセキュリティー・リーダーから得られた、それぞれの役割で成功を収めることに関するコメント**

| | | |
|---|---|---|
| **強力な戦略およびポリシー** | 「セキュリティーに関する意思決定を行ううえで重要なことですか?戦略的なビジョン、リスク評価、セキュリティーにかかわる優先順位付け、新しいテクノロジーが及ぼす影響の把握、ソリューションの差別化を図って勝者を見極める能力です」(保険業界の IT ディレクター) | 「ポリシーに関して全体的な一貫性が必要です。つまり、1 つのフレームワークです。プロセスが鍵です。一貫性のあるセキュリティー・プロセスがない場合、人々はどうすべきか疑問に思います」(金融サービスの IT 担当上級副社長) |
| **包括的なリスク管理** | 「リスク評価情報を利用して自社のセキュリティー・ポリシーを決定しています。何を、どこで、いつ、どのように保護するのか、そしてそれを実践するためのコスト (ビジネスに対するコスト) を決めるのに役立ちます」(製造業の IT グループ担当ヘッド) | 「全体的なリスク管理には、ビジネスを理解する必要があります。つまり、モデル、外部団体との接点、規制の枠組み、ビジネス・リスクなどです。IT リスクだけではありません」(メディア/エンターテインメントの 最高情報責任者) |
| **効果的なビジネス関係** | 「ビジネス・サポートを得るということは、販売するということです。ビジネスに関して実用的な知識を備えているだけでなく、テクノロジーも理解している人、つまりビジネス価値について語り、リスクを理解できる人が必要です」(保険業界の最高技術責任者) | 「ビジネスとして機能するには、セキュリティー・リーダーはできる限り最大の透過性を実証し、ビジネス・ケースと代替手段を示し、そのビジネスのアプローチに合うソリューションについて語る必要があります」(医薬業界の IT 担当ヘッド) |
| **コミュニケーションに関する協力** | 「リスクを十分に伝えるためには、ほかの病院で実施している具体例を多数挙げる必要があります。記事の一部を提供したり、別の病院ではセキュリティー侵害をどのように定義しているかを示したり、罰金を示したりします」(ヘルスケア業界の最高技術責任者) | 「効果的な関係を築くには、たくさんコミュニケーションをとって、ビジネス・リーダーを支援したり、セキュリティーの重要性を伝える時間をそれぞれの会議で設けるよう要求したりしながら、成功について語ったり、リスクを伝えたりしています。そうした一定のやりとりがあれば、心を開いてくれます」(電力/ガス業界のインフラストラクチャー担当ディレクター) |

## ビジネス規範についての課題: さまざまなビジネス上の懸念事項の管理

多くのセキュリティー・リーダーは、役員クラスが何を懸念しているか理解している。これは、よいことである。組織全体に関心を持ち、コミュニケーションをとっている証拠だ。成熟したリーダーほど頻繁に取締役会や役員クラスに定期的に会い、関係を深める傾向がある。意外なことではないが、役員クラスのエグゼクティブごとにセキュリティーに関する最上位の懸念事項が異なる。インタビュー対象者の意見では、CEO はブランドの評判や顧客の信用に及ぶ悪影響を最も気にするという。CFO は、侵害やインシデントによる財務的損失に心を悩ます。COO は運用ダウン時間について眠れないほど心配する。最終的に、CIO は侵害、データ損失、テクノロジー投資の実行など、幅広い懸念事項を抱えている。

| | ブランドの評判/信頼の喪失 | 財務的損失 | 運用ダウン時間 | コンプライアンス違反 | その他 |
|---|---|---|---|---|---|
| CEO | 49% | 6% | 15% | 9% | 21% |
| CIO | 26% | 0% | 24% | 18% | 32% |
| CFO | 14% | 47% | 6% | 21% | 12% |
| COO | 38% | 4% | 42% | 8% | 8% |
| 平均 | 32% | 14% | 22% | 14% | 18% |

*図 1 - セキュリティー・リーダーによると、役員ごとにセキュリティーに関する最上位の懸念事項が異なる。*

この幅広い悩みが難問を突きつける。このようなさまざまな懸念事項を軽減するために、今回インタビューを行ったセキュリティー・リーダーは取締役会や役員クラスと頻繁に会議を開く (頻度について最も多かった回答は、4 半期に 1 回)。会議で議論される最重要議題には、リスクの識別と評価 (59%)、予算に関する問題と要求の解決 (49%)、新しい技術の導入 (44%) が含まれる。リスクに着目することは適切だ。セキュリティー・リーダーは、役員クラスのさまざまな懸念事項に対処する機会を与えられる。

セキュリティー・リーダーが概して、ブランドの評判を落とすことや顧客の信用を失うことは組織全体の最も重要なビジネス上の懸念であると考えていることで、興味深い問題が提起される。株価や世間の認識に影響を及ぼす可能性があるのにもかかわらず、セキュリティー侵害やその他のインシデントがブランドの評判に及ぼす影響を追跡することは、現在、ほとんど不可能である。我々が話したセキュリティー・リーダーのほとんどは、この分野の能力を備えていない。CEO の懸念は、最終的にブランドの評判と顧客の信用に集中する。しかし、役員クラスに対して、何が可能であるかをビジネス・スキルとコミュニケーション・スキルをもって現実的に描けるかどうかはセキュリティー・リーダー次第である。明らかに、業界全体で前進していかなければいけない分野である。

### CISO の見解ビジネス・リーダーとともにバランスを模索するには

Shamla Naidoo
情報リスク ＆ セキュリティー担当バイス・プレジデント
Starwood Hotels & Resor ts Worldwide, Inc.

Starwood は総合的なセキュリティー戦略を練り上げた。これは、会社の資産、および当社の関係者や顧客のデータを積極的に保護する目的でエグゼクティブのリーダーや取締役会がレビュー、承認したものである。業界の変化と進化する脅威についてリーダーに逐次報告するために、IT セキュリティー・チームは、戦略や潜在的セキュリティー・リスクに関して定期的な経過報告を行っている。サービス業はめまぐるしく変化するビジネス環境で運営されるが、そのサービス指向の性質のおかげで当社のセキュリティー・プロファイルが著しく向上している。その結果として、慎重かつ迅速な意思決定を伴った、健全な議論と率直な対話は、ビジネスの前進とセキュリティー・リスクの適切な管理を確保するのに役立っている。

新しいセキュリティー・リーダーに送る最高のアドバイス:

1. セキュリティー戦略を展開し、目標および計画に関してエグゼクティブの賛同を得る。
2. 訓練を受ける、または実務経験を積む。方法が分からなければセキュリティーを確保できない。
3. 絶え間なく変化するセキュリティー・リスクに後れを取らないようにし、セキュリティーに関する判断を下すときには法的問題を考慮する。
4. ビジネスが収益を生み出す方法を理解し、ビジネスの成長と改革に影響を及ぼす可能性のあるリスクを積極的にサポート、管理する生産的な手段を見つける。
5. ビジネス上の利害関係者とコミュニケーションをとって、潜在的なリスクおよびソリューションについて報告および教育を行い、セキュリティー陣営の一部になれるように支援する。

*「ビジネス・テクノロジーおよび消費者向けテクノロジーの最前線にいなければならない。BYOD (Bring Your Own Device) は、あらゆるものを取り囲もうとしている。デバイスは急増している。セキュリティー・リーダーはスマートで知識豊富でなければならない。ユーザーの立場で考えよう。ユーザーが何を実行しているかを考えよう」*

– 最高情報責任者、金融サービス

## テクノロジー:
## 基礎テクノロジーの先へ

セキュリティー・リーダーの関心がリスク管理、ビジネス関係の強化、およびコミュニケーションの促進に移っているとはいえ、セキュリティー・テクノロジーが総合的セキュリティー・リーダーにとって最も重要なツールであることに変わりはない。実際、インタビューを受けたリーダーたちはテクノロジーの評価に多大な時間を費やしている (24%、全体で最も大きい分野)。

セキュリティー・リーダーの多くは、基礎となる実用的セキュリティー・テクノロジーを組織における最も重要なコンポーネントと見ている。このテクノロジーには、企業の ID およびアクセス管理 (51%)、ネットワーク侵入防御および脆弱性スキャン(39%)、およびデータベース・セキュリティー (39%) が含まれる。高度なマルウェア検出 (20%)、セキュリティー・インテリジェンス分析 (15%)、代替認証メカニズム (12%) など、重要度において基本テクノロジーを超えるさらに高度で戦略的なテクノロジーは出てきていない。将来、どのように変化していくかは興味深い。

周知の懸念事項があるにもかかわらず、セキュリティー・リーダーは、モバイル・セキュリティーの実装とクラウド・ベースのセキュリティー・サービスを押し進めている。モバイル・セキュリティーは、「最近導入された」セキュリティー・テクノロジーのトップであり、セキュリティー・リーダーの 4 分の 1 はこの 12 カ月の間にモバイル・セキュリティーを展開している。クラウド環境のプライバシーとセキュリティーに懸念が残るにもかかわらず、4 分の 3 (76%) は何らかのタイプのセキュリティー・サービスを展開している。最も多かったのは、フェデレーテッド ID およびアクセス管理とともに、データの監視と監査であった (両方とも 39%)。

インタビュー対象者の多くはセキュリティー組織を強化しながら、より高度なテクノロジーを試し、クラウド機能とモバイル機能を確立している。セキュリティー・リーダーはあらゆるテクノロジーをすべて追いかける必要はない。むしろ、アプローチを変化させ、ビジネス目標を進化させるテクノロジーに集中するべきである。

## テクノロジーの課題: モバイル・セキュリティーのあらゆる側面を進める

最新の CISO 調査では、モバイル・セキュリティーはテクノロジー懸念事項の 1 位であった。半数以上のセキュリティー・リーダーが、今後 2 年間の重要なテクノロジー課題と位置づけた。モバイル・セキュリティーは大きな関心を集め続ける:14 種類のテクノロジー分野の中で、「最も重要」なものと、この 12 カ月間で「最も導入」されたものの両方に選ばれた。モバイルは、最大の関心事であり、投資によって裏付けられているにも関わらず、機能はいまだに成熟過程にある。

今日、モバイル・セキュリティーは発展の基礎段階にある。最も頻繁に展開されるのは、デバイスにモバイル・デバイス管理機能を搭載すること (78%)、そして、企業のネットワークやデータを使用するデバイスを記録すること (76%) である。企業で安全なモバイル環境を構築する際の代表的な最初の一歩である (図 2)。

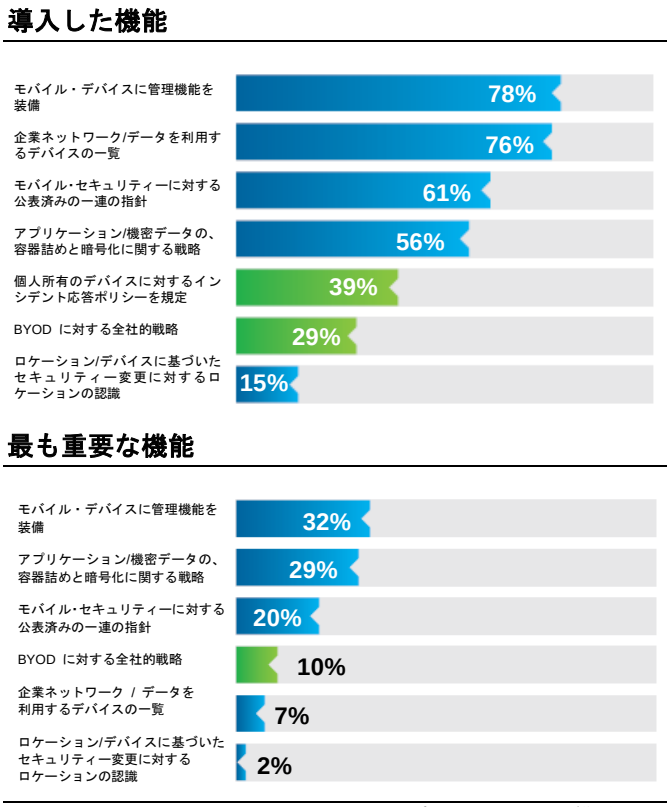


*図 2 - モバイル・セキュリティーのポリシーおよび戦略はまだ優先されていない。*

セキュリティー・リーダーにとってモバイルに関する主要な課題は、初期段階の先へ進み、テクノロジーについて考える時間を減らし、ポリシーと戦略について考える時間を増やすことである。インタビューを受けた大半のリーダーの場合、パーソナル・デバイスに対する総合的なモバイル・ポリシーや戦略は、まだ広く利用されていない、または重要とみなされていない。個人的に所有するデバイス特有に対応したポリシー、または BYOD （Bring Your Own Device）の企業戦略を展開している組織は 40% に満たない。また、こういったポリシーや戦略を「最も重要」と考えているセキュリティー・リーダーはほとんどいない。

ただし、セキュリティー・リーダーたちは、このずれを認識して対処している。今後 12 カ月で開発が計画されている分野の上位 2 つは、BYOD の企業戦略を立てている (39%)、個人所有のデバイスの状況に対応するポリシーを築いている (27%) のである。

**CISO の見解**
**懸念事項を取り除くための信頼の構築**
Ken Kilby、最高情報セキュリティー責任者
BB&T

当行は 141 年近く営業しており、少なくとも今後 141 年は存続すると思っています。これを実現するために、我々は一丸となってセキュリティーとリスクに取り組んでいる。これは全行員の責務である。最終的には、組織全体で責任を負う。クライアントと顧客に対して安全なアクセスを維持できない場合は、仕事を続ける資格がない。管理とポリシーは、結局は評判に焦点を合わせる必要がある。

この目標に到達するために、役員クラスおよび取締役会との信頼を構築することに多くの時間を費やしている。私は常に取締役会やエグゼクティブ・マネージメント・チームの各メンバーに連絡をとり、個人的な関係を築いてきた。役員クラスの別のメンバーは、私が取り組むべき懸念とは異なる懸念を抱いている。

BYOD も我々にとっては大きな関心事である。テクノロジーについていこうとしているが、最新かつ最高のテクノロジーに対して常に遅れを取り戻そうとしている気持ちになる。多種多様なモバイル・プラットフォームを管理し、安全を確保しなければならない。大量のマルウェアの出現により、これは非常に困難である。

助言を求めているセキュリティー担当者にアドバイスが 2 つある。第 1 にセキュリティー・リーダーは良い結果を追い求め続けなければならない。取締役会が理解できる言葉で取締役会とコミュニケーションをとらなければならない。常に積極的に関わり、日々のつまらない業務に飲み込まれてはいけない。第 2 は私自身の仕事に不可欠なこと:法執行機関、業界のパートナー、議員との関係を築く。公私にわたって良いコミュニケーションを育むことで、最終的に攻撃対象になる数を減らすことができる。協力することで、多くのことを実現できる。

## 指標:
## 適切なフィードバック・ループの作成

今日、セキュリティー・リーダーは主に予算の指針と新しいテクノロジー資産を主張するために評価指標を利用する。場合によっては、セキュリティー組織の戦略的優先順位の構築を支援するために測定を利用する。しかし、一般的に技術評価指標とビジネス評価指標では、いまだに運用上の問題に重点が置かれている。たとえば、インタビューを受けたリーダーの 90% 以上が、セキュリティーにかかわるインシデント、レコード/データ/デバイスの紛失または盗難、および監査ステータスとコンプライアンス・ステータスを追跡している。いずれも、すべてのセキュリティー・リーダーが追跡するのが当然と思われている基本的な次元である。セキュリティー・リーダーたちが、企業リスク全体にセキュリティーが及ぼす影響は最も重要な成功要因であると述べているにもかかわらず、ビジネス対策やセキュリティー対策を企業のリスク・プロセスに入れようとしている回答者は非常に少ない (12%)。

*「我々はプロセスと意識を改善し続けるために評価指標を使用する。評価指標は有利な状態を継続するために、次に何が起こるかを判断する手助けとなる」*

– IT 担当上級バイス・プレジデント、金融サービス

## 指標に関する課題:
## セキュリティー評価指標のビジネス用語への変換

企業リスク・プロセスに評価指標を利用する認識の重要性と実際の業務との間のずれは、CISO とセキュリティー・リーダーが直面している課題を反映する。2012 年 CISO 調査では、成熟したセキュリティー・リーダーほど多くの事柄を評価し、より頻繁に評価していることが分かった (教育、トレーニング、リスク他)。しかし、情報を使って何を処理すべきか、行動に拍車をかけるためにどのように情報をビジネスに伝えるべきか。

セキュリティー・リーダーのほぼ 3 分の 2 は、評価指標を決算に反映させていない。反映させるための人材が不足している、またはビジネス要求がない、あるいは算出するには複雑過ぎるのいずれかである。その上、半数以上がセキュリティー評価指標をビジネス・リスク評価と完全に統合しない(図 3)。関連する成功の測定を組み合わせないと、他のビジネス・リーダーとコミュニケーションをとるためのセキュリティー・リーダーの能力が制限される可能性があり、社内の組織の状況を効果的かつ正確に示すことが困難になる。

**CISO の見解**
**ビジネス上の利益に対する評価**

Felix Mohan、シニア・バイス・プレジデント兼
グローバル最高情報セキュリティー責任者
Bharti Airtel Limited

当初、我々は現状よりも運用的/戦略的マネージメント・レベルでマトリックス測定プログラムを開始した。コスト・センターとして必要なリソースを正当化するためものだった。習得し、成熟度が増すにつれて、評価方法を戦略的な方向へシフトさせた。リスク、コンプライアンス、ビジネス継続性、意識とトレーニング、重要なアプリケーションの稼働時間を追加した。

今日、我々はマトリックス・プロセスを改善し続けている。自動化を進め、企業リスク・レベルに合わせ、セキュリティー測定をビジネスへの影響に変換している。ビジネスのリスク許容度とその測定方法について理解を深めるよう根気よく努めている。

最新版のマトリックスの一部として、我々の製品およびサービス (企業に収益をもたらすもの) の元にあるすべての重要プロセスを識別している。プロセスが依存する IT/テクノロジー・インフラストラクチャー全体を確認した (例: システムとアプリケーション、重要な資産)。プロセスと資産が使用できない場合、復旧時間はどれくらいになるか?という質問にも答えた。次に、プロセスを「最高」、「高」、「中」、「低」に分類した。この分類は、インフラストラクチャーの復旧に求められる速さ (数時間から数日の範囲) を定めるものである。

## 財務的影響を測定する


「財務的影響の測定は、テクノロジーを実装したい場合には重要です。ROI、インシデントのコスト回避はどうですか?当社はそれを利用して、価値があることを証明しています」(保険業界の最高技術責任者)

## IT とビジネスのリスク指標を統合する


「継続性とビジネスへの影響に関する広範囲の分析の一部として、セキュリティー指標にお客様の満足度を組み合わせています。ほかの問題とともに、サイバーセキュリティーをリスク分析に統合しています」(電力/ガス業界の IT 担当ディレクター)

*図 3 - 財務的影響、セキュリティーの統合、およびリスクを判断する上で不十分な点は明らかである。*

## 万能なセキュリティー・リーダーへ向けて

これらの洞察と課題から、情報セキュリティー・リーダーの関心とアプローチについて何が分かるであろうか。評価プロセスのモデルの構築を支援できるだろうか。または、道筋を示せるか。

初心者の場合、セキュリティー・リーダーは強力なセキュリティー戦略を、IT セキュリティーの経済的影響を考慮したリスク・マネージメント全体と組み合わせる必要があり、かつ効果的なビジネス上の関係を構築してシニア・リーダーの信頼を得る必要があると示唆する。基本的なセキュリティー・テクノロジーを維持する必要はあるが、高度な戦略的機能の実装を犠牲にしてではない。リーダーはモバイル・セキュリティーに対して、総合的にアプローチする必要がある (ポリシーを重要視し、個人所有のデバイスの使用を可能にするなど)。

適切なフィードバック・ループを作成することも必要である。セキュリティー・テクノロジーとビジネスの評価指標は両方ともリスク・マネージメント・プロセスに取り入れる必要がある。項目の一部としてではなく、深い統合を通してだ。それらの評価指標を組織の言葉に変換する必要がある。これを行わなければ、セキュリティーがビジネス・イニシアチブを有効化することはできない。また、組織全体のセキュリティー・プロジェクトに費やすことの必要性を正当化することが難しくなる。

## 高度な CISO のプラクティスに対する方針を打ち出す

インタビューを受けたセキュリティー・リーダーの中には、この多才なモデルに近いリーダーもいたが、このモデルに求められるすべてを実行しているリーダーはほとんどいなかった。ビジネス・プラクティス、テクノロジー、および測定機能を正しく組み合わせ、かつ重要な課題に対処している者は、セキュリティー・リーダーシップにおける成熟度の基準を設けている。彼らは、情報セキュリティーが組織内で果たす役割を変えつつある。 テクノロジーやビジネスに関連した多数の作業分野に精通していることを証明し、セキュリティー・リーダーシップのルネッサンスに急速になりつつあるものを促進している。

## 詳細な情報

セキュリティー・リーダーシップの役割の変化については、**ibm.com**/ibmcai/ciso をご覧ください。

### ビジネス規範

**必須のステップ**

**CISO としての役割を形式化して**、組織と予算に関連した権限を有する唯一の上級セキュリティー・リーダーと確実に認識してもらいます。

**セキュリティー戦略を構築します。**この戦略は、定期的に更新され、広範囲にわたって伝えられ、組織内のその他の戦略 (製品開発、リスクと成長など) と連動して開発されます。

**効果的なビジネス関係を構築し**、経営幹部や取締役会と頻繁に会議を開き、さまざまな懸案事項を管理するための手法を開発します。測定対象を決める際、こうした懸案事項を考慮します。

透明性のある信頼できる方法でビジネスの利害関係者と頻繁にコミュニケーションを取ることにより、**信頼を構築します**。

### テクノロジー

**必須のステップ**

ビジネス目標に一致する場合には、**先進テクノロジーに投資します**。基本的なセキュリティー・テクノロジーだけにすべてのリソースを費やさないでください。手法の転換につながる先進テクノロジーと方法を探してください。

テクノロジーだけでなく、ビジネス・プラクティスやビジネス・ポリシーも用いて、個人のデバイスとビジネス所有のデバイスの両方に対して**モバイル・セキュリティーを強化してください**。

同業者を含め、その他のグループと**情報を共有してください**。これは、[テクノロジー投資を行う際の]自信を高め、セキュリティーの優先事項や主なプラクティスに関する質問に回答するのに役立ちます。

### 指標

**必須のステップ**

監査やコンプライアンスだけではなく、組織に及ぼす**経済的なリスクの影響全体に重点的に取り組んでください**。ビジネスを保護する方法を決定し、ブランドの価値や評判に及ぼすセキュリティーの影響について理解してください。

取締役会や経営幹部とともに、風評リスクやお客様の満足度にかかわる**懸案事項に対処してください**。何が可能かを現実的に説明してください。

測定基準を財務的影響に変換し、IT とビジネスのリスク測定基準を完全に統合してください。

*図 4 – より強いセキュリティー・リーダーになるための必須のステップ*

## 著者について

*Marc van Zadelhof は、IBM Security Systems の戦略および製品担当バイス・プレジデントである。*
IBM のグローバル・セキュリティー・ソフトウェアおよびサービス・ポートフォリオの管理、予算および位置付け全体に責任を負っている。連絡先: marc.vanzadelhoff@us.ibm.com.

*Kris Lovejoy は、IBM Security Services のゼネラル・マネージャーである。*
ワールドワイドで IBM の顧客に対する管理されたプロフェッショナルのセキュリティー・サービスの開発および展開に責任を負っている。Services における役割以前、Kris は IBM の情報テクノロジー・リスク担当バイス・プレジデント兼グローバル CISO として、グローバルで IBM のセキュリティーおよび回復機能の管理、監視、およびテストに責任と負っていた。連絡先: klovejoy@us.ibm.com.

*David Jarvis は、IBM Center for Applied Insights のマネージャーである。*David は、新興のビジネスとテクノロジーの課題に関する実態調査を専門にしている。また、2012 年 IBM CISO 調査および *Cybersecurity Education for the Next Generation* を含む IBM の数多くのセキュリティー調査に関する共著者である。David の連絡先: djarvis@us.ibm.com.

## 謝辞

Caleb Barlow、*ディレクター、モバイル・セキュリティー、アプリケーション・セキュリティー、データ・セキュリティー、クリティカル・インフラストラクチャー・セキュリティー*

David Puzas、*グローバル・マーケティング・エグゼクティブ、IBM Security Services*

Adam Trunkey、*グローバル・マーケティング・マネージャー、IBM Security Services*

### IBM Center for Applied Insights について

**ibm.com**/ibmcai

IBM Center for Applied Insights はこれまでにない新しい考え方、働き方および指導の方法を紹介している。同センターは実証的な調査を通じて、リーダーに対し実践的な助言と変革の事例を提供する。

## 注記および出典

[1] Gottlieb, Joe.“Being great:Five critical CISO traits.”*SC Magazine*.2013 年 6 月 13 日
http://www.scmagazine.com/being-great-five-critical-ciso-traits/article/298686/

[2] Ashford, Warwick. “CISOs must shape up or ship out, says Forrester.”*ComputerWeekly.com*. 2013 年 6 月 11 日
http://www.computerweekly.com/blogs/david_lacey/2013/07/where_next_for_the_enterprisin.html

[3] *戦略的見解に関する調査:2012 年 IBM 最高情報セキュリティー責任者の評価から得た洞察。* IBM. 2012 年 5 月。
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=CIE03117USEN

## IBM セキュリティー製品の Web サイト
**http://ibm.com/security/jp**

## IBM セキュリティー製品の Web サイト
http://www.ibm.com/services/jp/ja/it-services/jp-sc-igs-security-privacy.html



日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町 19-21

Produced in Japan
October 2013