

# サイバーセキュリティの 転換と変革

グローバル情報セキュリティ調査2016

The Global State of Information Security® Survey 2016





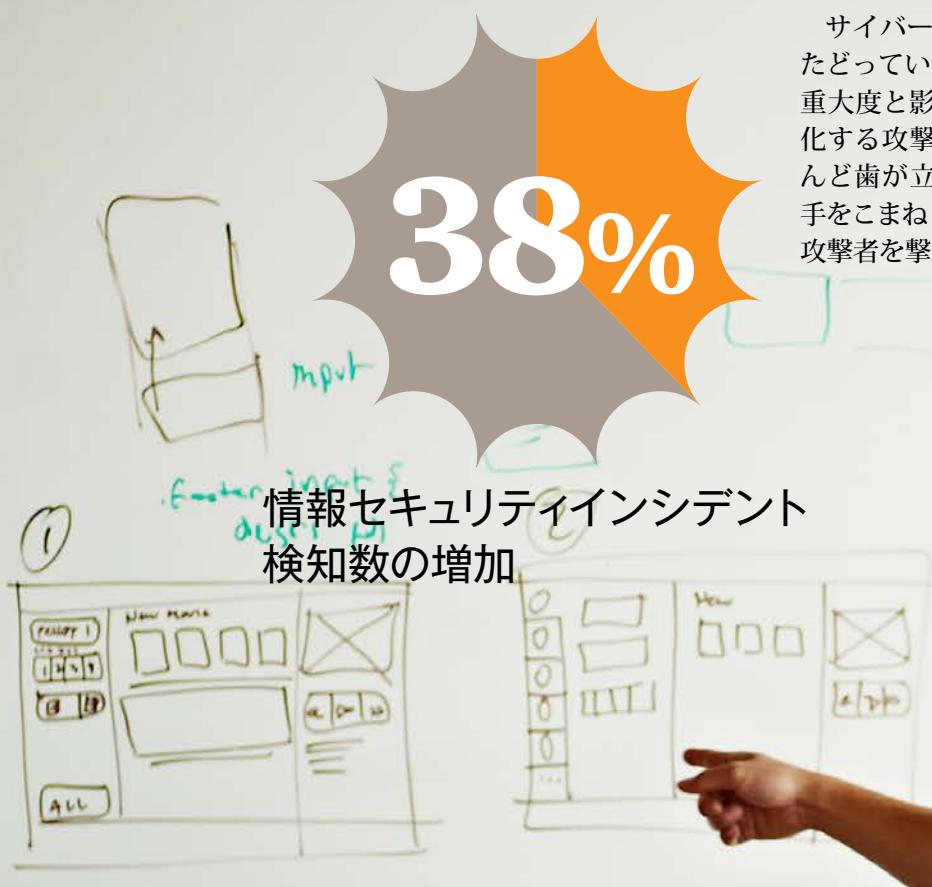
# 目次

---

増大するリスクへのグローバルな対応	2
イノベーションによるサイバーセキュリティの刷新	4
リスクベースのフレームワークの効果	4
クラウド化されたサイバーセキュリティの活用	5
ビッグデータが及ぼす大きな影響	6
パスワードから高度認証へ	8
IoTに備えてギアを上げる	9
モバイル決済の普及	12
協力体制によるセキュリティインテリジェンスの強化	13
保護できないものには保険をかける	15
経営陣の関与の高まり	18
経営陣はよりサイバーセキュリティに巻き込まれる	19
M&Aに伴うサイバーセキュリティのデューディリジェンス	21
サイバーセキュリティの未来に向けて	22
日本企業への示唆	24
付録A：増大するサイバーリスクへの対応	36
調査方法	39
サイバーセキュリティおよび プライバシーに関するPwCのお問い合わせ先（国別）	40

---

# 増大するリスクへのグローバルな対応



サイバー攻撃は年々、増加の一途をたどっている。発生頻度だけではなく、重大度と影響度も増すばかりだ。巧妙化する攻撃に対し、防止や検知はほとんど歯が立たなかった。多くの企業は手をこまねくばかりで、狡猾なサイバー攻撃者を撃退するリソースもない。

「多くの経営陣はサイバーリスクへの取り組みを、現代を特徴づけるものだと考えている」(PwCグローバルリスクコンサルティングリーダー、Dennis Chesley)

テクノロジーの進化は、時に経営モデルを様変わりさせるほど、企業の競争、価値創出の方法を革新的に変え続けている。データ分析の普及、ビジネス機能のデジタル化、業界の垣根を超えたサービスの提供など、近年の大きな波に乗ってテクノロジーとデータの使用が広がったことで、リスクはこれまでにないほど高まっている。

経営陣の間では、過剰な規制が長期的な阻害要因となるという見方も強い。また、国家によるサイバー攻撃などを含む政治的な衝突もサイバーセキュリティにますます大きな影響を及ぼしている。

このような現状から、サイバーリスクは官民のリーダーにとって大きな関心事となっている。PwCグローバルリスクコンサルティングリーダー、Dennis Chesleyは次のように解説している。「サイバーリスクへの取り組みは、現代を特徴づけるものだと言う経営陣は多い。その結果、企業はこの重要なリスク領域をビジネスの問題として捉えるようになった」。

先見の明のある経営者はサイバーセキュリティへの取り組みを見直すとともに、リスクを低減し成果を向上する革新的なテクノロジーに注目している。これらの全てのテクノロジーに共通するものがクラウドコンピューティングだ。クラウドは、個人、企業、政府が相互につながった現在のデジタルエコシステムの中心となる。規模を問わずあらゆる企業が活用でき、クラウドベースのサイバーセキュリティツール、ビッグデータ分析、高度認証をリンクできるプラットフォームでもある。さらに、IoT（モノのインターネット）、モバイル決済システムなどの新しいテクノロジー・プラットフォームの基盤にもなる。

クラウドコンピューティングはこの10年間でイノベーションに大きな影響を及ぼし、その影響はこれからも続くだろう。調査会社IDCの予測によると、本年のパブリッククラウドコンピューティングへの支出は700億米ドル近くまで増加し、新しいクラウドベースのソリューションの数は今後4、5年で3倍に増加する<sup>1</sup>。

ただし、テクノロジーだけではサイバーセキュリティの状況を好転させることはできない。賢明な企業は、セキュリティ対策として人的側面の重要性も理解している。スレットインテリジェンスや対応方法を官民の外部パートナーと共有し、協力体制を敷いてサイバーセキュリティに取り組もうとする動きがあるのはそのためだ。

企業内部では、経営陣の役割を拡大し、サイバーセキュリティ情報伝達の改善、準備態勢の強化、レジリエントの向上を目指している。サイバーセキュリティの基本教育を行い、蔓延する標的型攻撃などの心理的な脆弱性についても注意喚起する。

また、サイバーセキュリティへの意欲的な投資も大きな前進だ。本年実施したグローバル情報セキュリティ調査2016の回答では、情報セキュリティ支出が大きく増加しており、多くの企業がサイバーセキュリティの問題に正面から立ち向かう準備を整えている（インシデント、影響、コストの詳細については、付録Aを参照）。本書では、革新的な企業がこの課題にどのように取り組んでいるかを紹介するとともに、資産や評判、競争力を保護するためにはどのような総合的アプローチが効果的かを探る。

<sup>1</sup> IDC, Public Cloud Computing to Reach Nearly \$70 billion in 2015 Worldwide, According to IDC, July 21, 2015

# イノベーションによる サイバーセキュリティの刷新



リスクベースの  
サイバーセキュリティ  
フレームワークを  
採用した企業の割合

## リスクベースの フレームワークの効果

効果的なサイバーセキュリティプログラムでは、まずリスクに基づいた戦略策定を行う。今回の調査では、企業の大半がセキュリティフレームワークを（複数組み合わせて）採用し、大きな成果を得ていることがわかった。

実装されている主なガイドラインは、ISO 27001と米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワークの2つだ。これらのガイドラインは、リスクの識別と優先順位の設定、サイバーセキュリティへの取り組みの成熟度の測定、対内的、対外的なコミュニケーションの改善を可能にする。

リスクベースフレームワークは、サイバーセキュリティプログラムの改善に向けた目標の設計、測定、監視にも役立つ。例えば、トロントに本社を置くカナダ帝国商業銀行（CIBC）では、フレームワークに基づくスコアカードを開発し、自行のセキュリティプログラムの成熟度を評価している。「フレームワークによって構造化していなかったら、前年と比較して進行を把握することは困難だ」と、同行の情報セキュリティおよびリスク担当バイスプレジデント、Joe LoBianco氏は語っている。

## セキュリティフレームワークがもたらす利点

セキュリティリスクの識別と優先順位の設定を的確に行える **49%**

セキュリティインシデントをすばやく検知し、緩和できる **47%**

機密データの保護を強化できる **45%**

セキュリティのギャップを正確に把握し、対応できる **37%**

内外での協力やコミュニケーションを強化できる **32%**

## クラウド化された サイバーセキュリティの活用

近年のサイバーセキュリティ対策のための先進の手段としてクラウドコンピューティングが活用されている。クラウドプロバイダーらはデータ保護、プライバシー、ネットワークセキュリティ、IDおよびアクセス管理を行う最新鋭テクノロジーへの投資を絶えず行ってきた。さらに、情報収集、脅威のモデル化、攻撃への防御、協調的学習、インシデントレスポンスの迅速化の領域へも拡大させている。

機密データの保護とプライバシーの強化のためにクラウド型セキュリティサービスを利用しているという回答が大半を占めたのもうなづける。リアルタイムの監視や分析、高度認証、IDおよびアクセス管理など、クリティカルなサービスもクラウド化が広がっている。

例えば、アトランタに本社を置く世界的な決済テクノロジーサービスプロバイダーであるGlobal Paymentsでは、脅威監視とインシデントレスポンスにプライベートクラウド型管理サービスを活用している。「当社はあらゆるアラートと脅威情報の集約にクラウドソリューションを利用している。セキュリティ上の脅威とは見なされないもの、または誤検知のイベントやアラートは除外され、調査に必要なイベントがセキュリティオペレーションセンター（SOC）へ通知される」とエグゼクティブバイスプレジデント兼CIOであるGuido Sacchi氏は語る。クラウドはこの種のタスクに最適だ。クラウドプロバイダーは膨大な量の脅威およびイベントデータを高速処理す

ることに長けているからだ。それに加え、一般的な企業では開発、育成が困難な分析アルゴリズムの構築に必要とされる専門技術も保有する傾向がある。

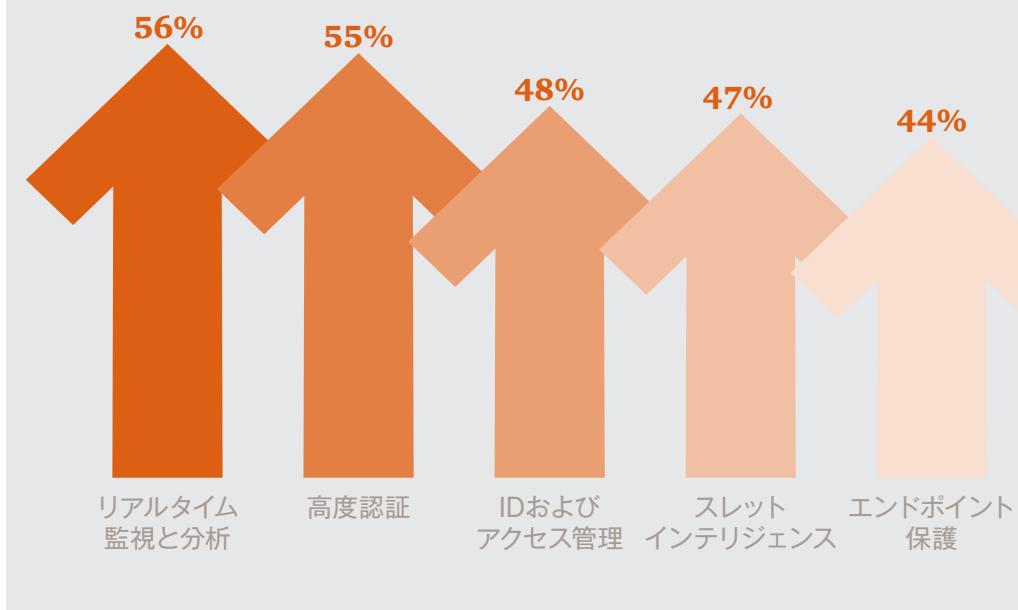
ミシガン州グランドラピッズを拠点とする家具会社、Steelcaseでもクラウド型サイバーセキュリティが採用されている。同社のITセキュリティアーキテクト兼イノベーションフェローであるStuart Berman氏によると、高度認証、ペネトレーションテストおよび脆弱性テスト、セキュリティアラート分析、ネットワーク動作分析など、さまざまなクラウド型管理サービスを利用している。

# 69%



クラウド型サイバーセキュリティサービスを使用している企業の割合

### クラウド型サイバーセキュリティサービスの採用



同社はこれらのクラウドサービスを利用して費用効率に優れたセキュリティプログラムを実施している。「クラウド型セキュリティサービスでは特定の領域における深い専門性を持ったサービスが提供される。このサービスを利用することにより当社のセキュリティ担当者は技術知識の獲得や維持に忙殺されることなく、セキュリティ問題の識別と管理に専念できる。これにより、リスクに基づいたコスト管理を適切に行えるようになった」(Berman氏)。

## ビッグデータが及ぼす大きな影響

サイバーセキュリティ上の脅威のモデル化と監視、インシデントレスポンス、データの使用者、使用方法、使用時期の監査や検証に、ビッグデータ分析を活用する企業はますます増加している。

「データ分析は現在、投資分野の1つである。セキュリティの中でも成長著しく、これからの仕事のしかたを大きく変えるだろう」とCIBCのLoBianco氏は語る。

データ駆動型アプローチにより、セキュリティは境界ベースの防御から、リアルタイム情報を用いたセキュリティインシデントの予測へと躍進する。企業はネットワークの異常値を的確に捉え、セキュリティインシデントをすばやく識別して対応できる。不審な行為を監視することで、従業員によるセキュリティインシデントの低減や迅速な検知にも役立てることが可能だ。

## クラウドとDevOpsのシナジー

Webサービス事業者はDevOpsの採用を通じてサイバーセキュリティの強化、自動化を進めている。DevOpsはアプリケーション開発者とIT運用者の間での緊密な協力を促すソフトウェア開発モデルである。このアジャイル開発アプローチは、アクティブなアプリケーションが数千あり、コード更新を頻繁に行う企業にとって特に有用だ。ストリーミングメディアプロバイダーのNetflixの事例では、DevOpsを使用し、多数のクラウドサービスアカウントの設定変更を識別するといったタスクを自動化している<sup>2</sup>。

クラウド型サービスと組み合わせると、DevOpsはサイバーセキュリティプログラムを大きく進化させることになる。DevOpsとクラウド型サイバーセキュリティの融合により、次のようなシナリオが現実のものとなる。『侵入者がアプリケーションコードを改変すると、自動分析および監視ソフトウェアがデータ漏えいを検知し捉え、接続を切断して、開発者にアラートを送信する。続いてサイバーセキュリティエンジニアが改変内容を特定し、コードを修正する。その後、システムが全てのユーザートラフィックを最新バージョンに切り替え、脆弱性のあるアプリケーション全てに対して、パッチを自動的に配布する。』

しかし、一般的に、ビッグデータ分析を行うには、多大なコンピューティングリソースとソフトウェアの専門知識が必要だ。そこでGlobal Paymentsのような企業は、クラウドソリューションを使用して、集約されたシステムログデータを分析している。クラウドはこのような膨大な量の情報分析に向いているからだ。

データ分析を既存のSIEM (Security information and event management) テクノロジーと組み合わせて、幅広いネットワークアクティビティを柔軟に把握することもできる。CIBCでは、従来のルールベースのSIEMを補完するものとして、新しい分析ベースの脅威検知および監視システムのテストを実施している。

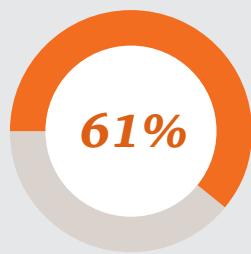


59%

ビッグデータ分析を  
セキュリティに活用  
している企業の割合

<sup>2</sup> Netflix, Announcing Security Monkey-AWS Security Configuration and Monitoring, June 30, 2014

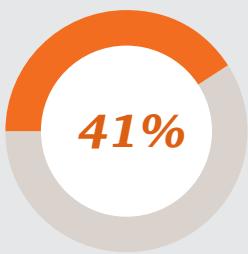
## データ駆動型サイバーセキュリティがもたらす利点



外部脅威を  
的確に把握



内部脅威を  
的確に把握



ユーザーの行動を  
的確に把握



異常なネットワーク  
アクティビティを  
より的確に把握



セキュリティ  
インシデントの  
迅速な識別と  
対応が改善

「SIEMのために収集したデータとその他のデータを組み合わせ、柔軟な調査機能を活用してSOCが脅威を検知および監視できるようにすることは必要不可欠である」(LoBianco氏)。

データ分析をIDおよびアクセス管理に利用し、従業員の使用パターンを監視し、異常値をフラグ付けようとしている企業もある。データ分析ソリューション

によって従業員のアクセス権限に関するパターンを探し、無用のアクセスを識別することができる。

このように広い視野を持つことが、予想外のシステム改善につながることもある。例えば、Steelcaseでは標的型攻撃や内部者リスクの監視のため分析を開始したが、ビッグデータから未知のネットワークパフォーマンスの問題が

見つかるともわかった。「データ分析により、干し草の山から“針”を見つけることが可能になる。セキュリティに関する問題だけではなく、パフォーマンスに関する問題が出てくることもある」とBerman氏は語る。「ビッグデータを分析することで、気付かなかったパターンを浮き上がらせ、先回りして問題に対する答えを導き出すことができる」。



「データ分析は現在、投資分野の1つである。セキュリティの中でも成長著しく、これからの仕事のやりかたを大きく変えるだろう」(CIBC、Joe LoBianco氏)

# 91%

高度認証を  
使用している  
企業の割合



## パスワードから高度認証へ

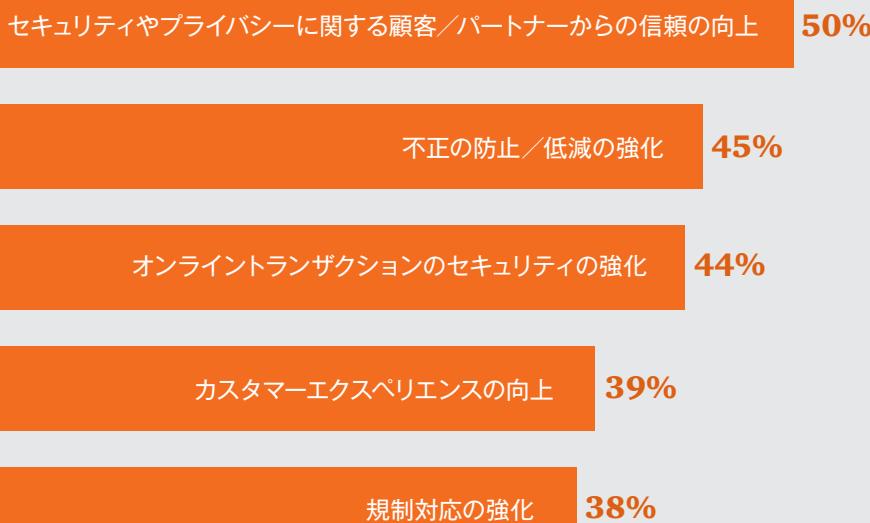
パスワードでは十分なセキュリティを確保できないという認識が一般的になつた現在、多くの企業はアクセス管理と顧客やビジネスパートナーからの信頼獲得のため、高度認証へと移行し始めている。

前述のとおり、高度認証はクラウドサービスとして導入されている。大きく報じられた攻撃の多くが認証情報の漏洩から始まったことを考えれば当然の流れだ。「パスワードがセキュリティ対策になると考へるのは間違いだ」とSteelcaseのBerman氏は語る。同社では、ワンタイムパスワードとハードウェアトークン、クラウド型認証プラットフォームを組み合わせて使用している。

顧客向けでも従業員向けでも、従来のパスワードを脱却する動きは特に銀行で顕著だ。CIBCのLoBianco氏の話では、顧客の携帯電話にワンタイムパスワードを送信する方式はユーザーに受け入れられ、データセキュリティの強化とともにヘルプデスクのコスト削減にもつながった。CIBCではネットワークやデータに特権的にアクセスできる従業員向けに二要素認証も使用している。多くの従業員は既にリモートアクセス用に強度の高い認証トークンを使用していたため、用途を特権アクセスに広げたかたちだ。

バイオメトリクス（生体認証）など、最先端のオンプレミス認証技術の開発と実装を進めている企業もある。テキサス州サンアントニオに本社を置き、退役軍人と現役軍人を顧客とする金融サービスや保険サービスを提供するUSAAでは、モバイルアプリケーションへのアクセスに顔認証および音声認証、指紋認証を導入した<sup>3</sup>。同社はバイオメトリクスによってセキュリティとカスタマーサービスを強化した他、ヘルプデスクへの問い合わせ件数を減らし、顧客にとっての利便性も高めた。

## 高度認証がもたらす利点



もう1つのアプローチはハードウェアベースの認証だ。巨大テクノロジー企業Googleは、Google for Workアプリケーションで安全性の高い二要素認証を行うための「セキュリティキー」というUSBデバイスを開発した<sup>4</sup>。セキュリティキーはFIDO AllianceのUniversal 2nd Factor (U2F) 標準に準拠し、検証コードではなく暗号化された署名を送信する。そのため、認証情報を盗聴することはできない。ユーザーはセキュリティキーをタップするだけでよい。認証コードを要求して入力するよりも簡単だ。

<sup>3</sup> SecureID News, *Biometrics secure next generation of mobile banking apps*, July 7, 2015

<sup>4</sup> Google, *The key for working smarter, faster, and more securely*, April 21, 2015

Starwood Hotels & Resortsでは、まったく異なるタイプのアクセスキーを開発した。同ホテルのSPGキーレスサービスでは、ホテル宿泊客があらかじめ登録すればチェックインデスクでの手続きが不要になり、スマートフォンやApple Watchで客室ドアのロックを解除できる<sup>5</sup>。常連向けプログラムStarwood's Preferred Guest (SPG)の会員向けアプリケーションを通じて、空港からの道案内、個々のホテルや常連アカウントに関する情報提供も行っている。

このようなパスワードレスの認証とアプリケーションを導入するには、ID管理の方法を見直し、ユーザー認証強化のためのソリューションを模索する必要がある、とPwCのマネージングディレクター、Suzanne Hallは考えている。「アクセスやトランザクションのリスクに応じて、適切なレベルの認証ソリューションを設計すべきだ。企業と個人の間の信頼関係では、検証すべき情報と保護の必要性のバランスが意識される」。

使いやすさも大きな要素だ。「パスワードを忘れないようにしたり、トークンを持ち運んだりする負担を和らげるソリューションが採用されるだろう。認証は気軽に使えなければならない」とHallは言う。

## IoTに備えてギアを上げる

IoT（モノのインターネット）については、もはや説明は不要だろう。インターネットで接続されたデバイス、運用ツール、設備のエコシステムは今後急拡大する見込みだ。調査会社IDCでは、インターネットに接続されるデバイスの数は、今年の推計130億台から2020年には300億台に達すると予測している<sup>6</sup>。

IoTは大きな利点をもたらすものの、データセキュリティやプライバシーのリスクも増大するということは、多くの企業に理解されている。事実、2015年に組み込みデバイス、運用システム、消費者向けテクノロジーなどのIoTコンポーネントの悪用があったという回答は2倍以上に增加了。

86%

運用システム、組み込みシステム、消費者向けシステムの悪用が発生したと答えた回答者の数は前年比で152%増加した。

34%

2014年

2015年

5 Starwood Hotels & Resorts, Starwood Hotels & Resorts Celebrates UK Launch of Keyless Check-In Through the SPG App for Apple Watch, April 24, 2015

6 IDC, Connecting the IoT: The Road to Success, June 2015



# 36%

IoTの  
セキュリティ戦略  
を策定している  
企業の割合



今後、センサーベースの接続デバイスやM2Mテクノロジーを展開する企業が増えるにつれ、ITおよび運用システムへの新しいアクセス方法が登場するだろう。この種の装置は一般的に、従来の基本的なITセキュリティ機能を備えておらず、攻撃者にシステムに侵入されれば、データ漏洩の他、運用への支障、製品やサービスの完全性損失といった事態に発展する恐れがある。

先進的な企業は、企業と顧客を守り、ユーザーから信頼を得るには、プライバシーやサイバーセキュリティの共通の標準が必要だということに気付き始めている。これらを整備するには、セキュリティ

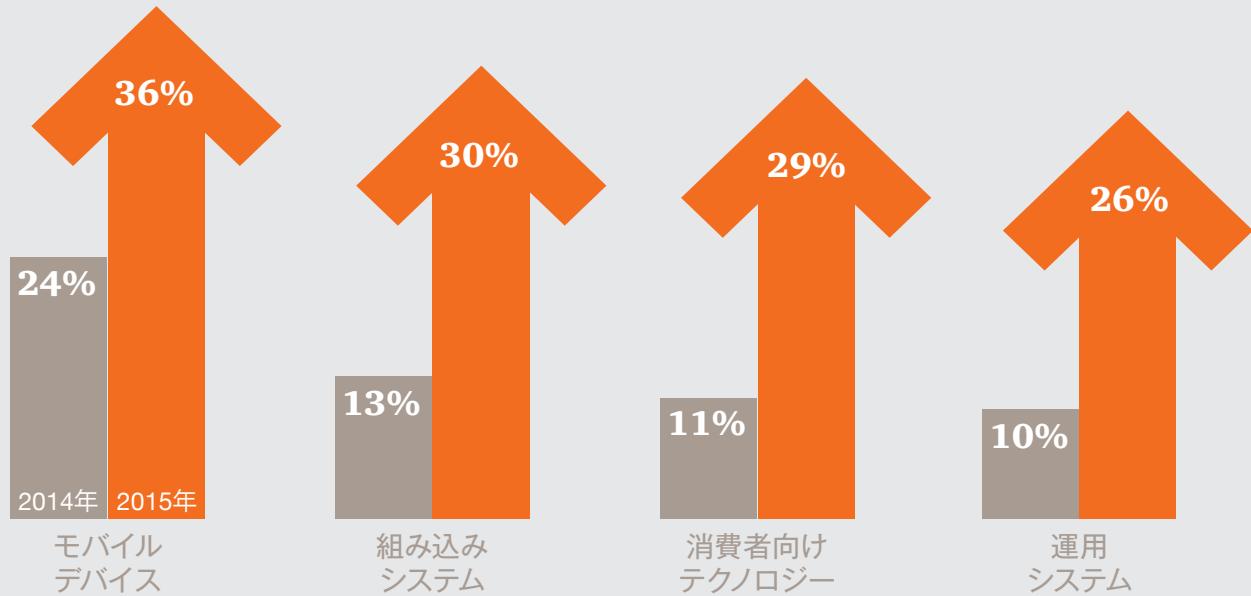
管理策のテスト、共通のデータフォーマット、顧客データの収集および使用に関するポリシー、適切な情報開示管理策などの課題に対応するプライバシーフレームワークをIoT関係者が開発し、遵守する必要がある。

IoTエコシステムにある他の組織と組み、サイバーセキュリティおよびプライバシー標準の構築に向けて合意形成をする企業も見られる。Steelcaseもその一例だ。SeamlessというIoT連合に参加することで地域のスタートアップ企業や大学と協力し、IoTに必要な部品と、それを組み合わせた際に必要となるプライバシー要件を策定している。同社はこ

の協力体制を通じて、産業用IoT製造プラットフォームを開発するとともに、顧客向けのスマートファシリティと相互接続のためのオフィス空間向けプラットフォームを開発している。いずれのプラットフォームの設計にも優れたセキュリティおよびプライバシーの原則と管理策を組み込んでいる、とBerman氏は意気込む。

IoTが工場や企業の施設から一般的な環境へと広がれば、プライバシーの問題が急速に広がるだろう。GEライティングと米国の2つの自治体が協力して取り組む「スマートシティ」プロジェクトを例にとって考えてみよう。

## IoTデバイスおよびシステムへの攻撃



このプロジェクトでは都市部の街灯をLEDに取り替える。LEDはセンサーとワイヤレストランスマッターを搭載し、データを中央集約し分析プラットフォームに連携される<sup>7</sup>。このようなスマートシティープロジェクトは、交通の流れの最適化、エネルギーコストの削減、歩行者にとっての安全な環境の構築などの利点をもたらす。自動車を空いている駐車場に誘導することも可能だ。

ただし、プライバシー擁護派からは、データ使用の監視と責任について危惧する声が挙がっている。例えば、街灯の動画撮影機能で歩行者や自動車運転者がリアルタイムでモニタリングされ、否応なく政府による監視、データ収集が行われるのではないかという懸念だ。このような懸念を拭い去るためには、プライバシーの保護を念頭に置いてシステムを設計する必要がある。

この例から、IoTの本格化に伴い、想定外のプライバシー問題が生じる可能性があることがわかる。「システムがもたらす価値と、企業と個人がプライバシーに関して抱いている懸念の間で板ばさみになっている」と、SteelcaseのBerman氏は述べている。「真の障壁は、プライバシー、法的な懸念、テクノロジーに対するこれまでの考え方とこれからの考え方との違いにある」。

「真の障壁は、プライバシー、法的な懸念、テクノロジーに対するこれまでの考え方とこれからの考え方との違いにある」(Steelcase、Stuart Berman氏)

<sup>7</sup> GE Lighting, GE Unveils LED-enabled Intelligent Environments, a Glimpse into The Connected Future, May 5, 2015

## モバイル決済の普及

本年の調査では、回答者の57%がモバイル決済システムを導入したと述べた。モバイル決済は既に主流となっているが、IT、金融、小売、通信の各社の新たな提携が相次ぎ、エコシステムの急速な進化が続いている。このような環境の変化とともに、予期せぬサイバーセキュリティの脅威が生じ、攻撃者の幅が広がる。

米国で注目を浴びたApple Payサービスの展開からもわかるように、新しいテクノロジーやプロセスはリスクももたらす。「(Apple Payの) 初期の課題は、必ずしも電話や認証情報の物理または論理セキュリティではなく、むしろ加入プロセスにあった」とCIBCのLoBianco

氏は指摘する。「新しい決済モデルを導入するときには、ユーザーの加入から、システムを経由するトランザクション、ユーザーの退会に至るまでのライフサイクル全体に目を配る必要がある。新しいプロセスがあれば、技術的な脆弱性だけでなく心理的な弱点を突こうとする者が現れる」。

トークンを加盟店システムに送信するモバイル決済テクノロジーは基本的に安全であると考えられている。クレジットカード情報をデバイスに保存したり、小売店のPoSシステムに送信したりすることがないからだ。しかし、スマートフォン決済は未来型トランザクションに向けての1ステップにすぎないという見方もある。

Global PaymentsのSacchi氏は、ユーザー経験から決済プロセスをなくして初めて真に革新的なモバイル決済であると言えると考えている。シームレスなプロセスで状況を一変させた企業として、タクシー配車サービスを提供するUberを挙げる。同社は登録されているペイメントカードを使用し、顧客のカードに自動的に請求する。「Uberはユーザー経験全体から決済ステップを消した。利用者は配車されたタクシーに乗って、降りるだけだ。同社の成功から学べることは、セキュリティとユーザー経験の両面に配慮する必要があるという点だ。この2つをうまく両立させた企業が市場を制するだろう」(Sacchi氏)。

## モバイル決済セキュリティを向上するために企業が取り組んでいる課題

マルウェア／悪意あるアプリケーションに関するリスク

57%

ハードウェア／デバイスプラットフォームに関するリスク

45%

不正を低減するための検証／プロビジョニングプロセス

45%

顧客の個人データの保護

43%

エンドユーザーのリスクおよび脆弱性

42%





## 協力体制によるセキュリティ インテリジェンスの強化

パートナーや顧客とデータを共有する企業が増加とともに、サイバーセキュリティ上の脅威や対応についての情報交換も進んでいる。この3年間で外部と協力する企業の数は着実に増加した。

利点ははっきりしている。ほとんどの企業は、外部と協力することで、同業者や情報共有機関（ISAC）とより多

くの実用的な情報を共有できるようになったと述べている。情報共有によって、脅威に対する認識が高まり、知識が増えたという声も多い。

一方、協力体制を構築していない企業は情報共有フレームワークや標準を持たず、データフォーマットやプラットフォームに官民におけるデータの互換性がない傾向が強い。また、現在の情報共有エコシステムには、サイバーセキュリティの最新情報が迅速に伝わっていないという問題もある。

データプライバシーに関する政策や規制は国によって大きく異なり、特定タイプのデータを共有することが顧客や従業員、その他の個人のプライバシーを侵害することになるのではないかと懸念する企業もある。収集した情報の合法性や有効性は、あらゆる組織の共通の関心事だ。

このようにさまざまな課題が山積する中、2015年になってバラク・オバマ米大統領が官民の協力を促す大統領命令を発令し、情報共有への関心が復活した。オバマ大統領が提唱するのは、新しい情報共有分析機関（ISAO）の創設である。業界固有のISACにはない柔軟性を特長とし、個々の業界や地域、課題、事象、脅威に関する情報を官民が共有できるようにする狙いだ。

ISAOを通じて、多くの企業が協力して情報を共有できるようになるだろう。PwCのグローバルおよび米国サイバーセキュリティリーダー、David Burgは、次のように述べている。「ISAOは従来の組織に欠けていた機能を補い、国家のサイバーセキュリティ体制の構築において大きな役割を果たすと考えている。PwCがホワイトハウスや産業界、学術機関の関係者とともに課題への対応に取り組んでいるのもそのためだ。議論を活性化し、ISAOの有効性を最大限に高めていく」

ISAOは企業にどのような利点をもたらすのだろうか。他業種の企業から多くを学べると考える企業もある。例えば、サイバーセキュリティの課題には業種による違いはあまりなく、企業の規模や顧客層による違いが大きい。大手銀行との共通点が多いのは、地方銀行よりも大手製薬会社だ。

業界の壁を越えた協力に慎重な企業もある。金融業界では、金融サービスのISACがあれば事足りるため、複数の情報共有組織が参加する機関は過剰で非生産的と見る向きもある。

このように、企業の見方は業界によってさまざまだ。ISAOは新しい概念であるがゆえに、今のところ各社とも様子見の姿勢をとっている。機関を通じて協力することに価値を見いだせないので。

---

「ISAOは現在の組織に欠けていた機能を補い、国家のサイバーセキュリティ体制の構築において大きな役割を果たすと考えている」（PwCグローバルおよび米国サイバーセキュリティリーダー、David Burg）

---

協力の利点を生かそうとしているのは米国に限らない。欧州議会は、加盟国および官民の間で、サイバーセキュリティイニシアチブに関する情報共有や協力を進めるためのネットワークおよび情報セキュリティに関する指令を承認した<sup>8</sup>。この指令により、特定の重要なインフラ業界の企業は、リスク管理を実施し、主なインシデントを各国当局に報告するよう義務付けられる。また、欧州ネットワーク・情報セキュリティ機関 (ENISA) では、標準化機構や関係者とともに、インシデント報告仕様の開発が行われている。

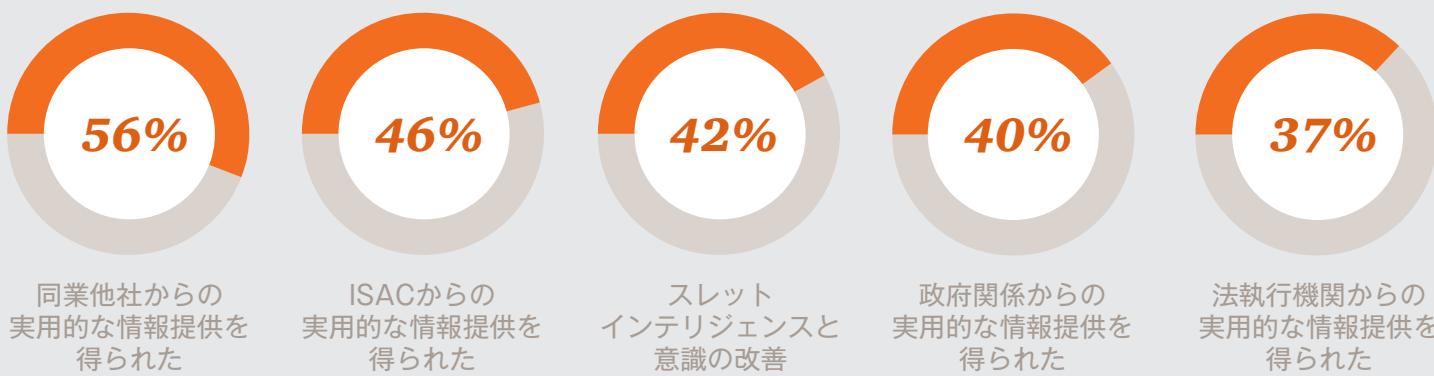
## 保護できないものには保険をかける

情報共有と先進のサイバーセキュリティテクノロジーをもってしても、サイバー攻撃を完全に阻止することは不可能だ。攻撃者は高い技術力を持ち、サイバーセキュリティ対策を迂回する方法を常に見つけ出す。そのため、多くの企業はサイバー犯罪による財務的損失を軽減しようと、サイバーセキュリティ保険に加入している。

サイバーセキュリティ保険は保険市場で著しい成長を遂げている。PwCの最新レポートでは、サイバー保険のグローバル市場の年間売上が2015年の25億米ドルから、10年以内には75億米ドルに達すると予測している<sup>9</sup>。

現在の保険商品では、データの破損、DoS攻撃、盗難、恐喝が補償対象となっている。インシデントレスポンス、復旧、調査、サイバーセキュリティ監査費用が含まれる場合もある。また、顧客への通知、危機管理、フォレンジック調査、データ復旧、業務中断などを補償する商品もある。保険業界ではさらに、知的財産の喪失、評判やブランドイメージの低下、サイバー関連のインフラ障害も補償対象に含めようとしている。

## 外部との協力がもたらす利点



8 European Commission, Network and Information Security (NIS) Directive, March 16, 2015

9 PwC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience, September 2015

保険に加入する企業は、サイバー犯罪に伴う財務リスクの低減に加え、自社の準備態勢を正確に把握しようともしている。加入条件として、現在の能力やリスクの徹底的な評価が保険会社から求められるからだ。この評価を通じて、サイバー犯罪が発生した場合の法的リスク、対応コスト、ブランドが受けけるダメージの予測が可能になる。

ただし、現在のサイバーセキュリティ保険では、価値に見合ったリスク管理が行えないこともある。CIBCは数年間かけて、サイバーセキュリティ保険を観察し評価した。「セキュリティチームと、リスク管理部門に所属する企業保険チームが銀行のリスクを毎年分析し、現在加入できる保険契約の内容と保険料と比較した。当行のリスク許容度に照らし合わせた結果、サイバー保険の準備はまだ整っていないと判断した。サイバー侵害において最も懸念されるのは、評判、信頼、ブランドだ。これらを保険で保護するのは至難の業だ」と、LoBianco氏は述べている。

また、どの程度の補償金額のサイバーセキュリティ保険に入るべきかという点も多くの企業にとって悩みの種だ。適切な金額はそれぞれの企業によって異なるため、一概には言えない。PwCのプリンシパル、Joseph Noceraは次のように述べている。「企業は、全ての損失リスクに保険をかけることはできないということを理解すべきだ。市場の供給体制がまだ整っていない。最近起こった大規模なセキュリティ侵害を参考に、大企業は8000万～1億米ドル、中小企業は1000万米ドル程度を補償金額とする保険に加入しようとしている。ただし、企業規模や業種、扱っているデータの種類、セキュリティ管理策の成熟度、個々のリスク許容度など、企業ごとにさまざまな要素があるため、1つの正解があるわけではない。企業の評判やブランドを守ってくれる保険商品はないことも肝に銘じておくことが重要だ」



サイバーセキュリティ保険に加入している企業の割合

「企業は、全ての損失リスクに保険をかけることはできないということを理解すべきだ。市場の供給体制がまだ整っていない」(PwCプリンシパル、Joseph Nocera)



## サイバー保険によって補償される インシデント関連の損失

47% 個人の識別が可能な情報

41% ペイメントカード情報

38% 知的財産／営業秘密

36% ブランドの評判の低下

31% インシデントレスポンス

「サイバー侵害において最も懸念されるのは、評判、信頼、ブランドだ。これらを保険で保護するのは至難の業だ」(CIBC、Joe LoBianco氏)

# 経営陣の関与の高まり

54%

セキュリティ  
プログラムを  
担当するCISOを  
任命している  
企業の割合



テクノロジーの発展が、手ごわいサイバー脅威への抵抗を可能にすることは間違いない。その反面、技術の進歩に注目するあまり、大きな防御力となる従業員の役割や能力、トレーニングが見落とされがちであるとも言える。しかし、企業の考え方には変化の兆しが現れている。

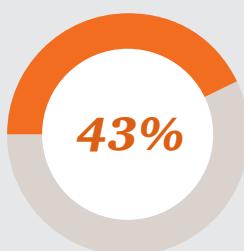
保険会社Marshのグローバル分析責任者、Claude Yoder氏は次のように語っている。「企業はテクノロジー中心の見方をする傾向があるが、サイバー情報が増えるほど、テクノロジーだけではなく、従業員やプロセスが着目されるようになるだろう」

サイバーセキュリティの取り組みをリードするのは、最高情報セキュリティ責任者（CISO）や最高セキュリティ責任者（CSO）などの幹部だ。これらの幹部の責任と能力が顕著になり、重要性が増している。

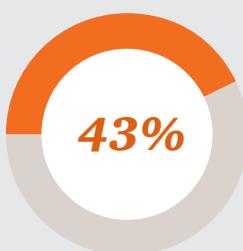
現在のCISOやCSOは、サイバーセキュリティのみならず、リスク管理、コーポレートガバナンス、ビジネス目標全体の専門知識を持つ上級幹部である必要がある。経営陣にビジネスリスクを解説し、リスクベースのセキュリティ課題を詳しく説明する能力を持っている必要がある。つまり、サイバーセキュリティリーダーには、他の上級幹部に匹敵するほどの変革力が必要なのだ。

PwCのグローバルCISOのJames Shiraは次のように指摘している。「今日のセキュリティリーダーには、COOのように、コミュニケーションやプレゼンテーション、ビジネスに精通した総合力が求められる。CISOやCSOに期待されるのは、リスクの説明責任を負い、企業全体で最低限の情報セキュリティ態勢を実現することだ。そのためには、これまでとは異なるレベルの経営能力が必要だ」

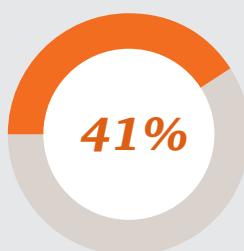
## セキュリティリーダーのスキルとコンピテンシー



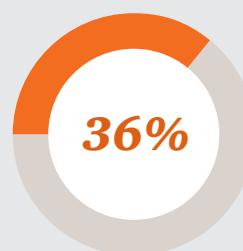
情報セキュリティに  
関するリスクおよび  
戦略を経営陣に  
直接報告している



情報セキュリティを  
企業全体の  
リスク管理の問題と  
捉えて取り組んでいる



自社の  
ビジネス課題や  
競合環境を  
理解している



内部の関係者と  
協力して  
ビジネス課題および  
ニーズの理解に  
努めている



1年に4回以上、  
最新の情報セキュリティ  
リスク情報を  
経営陣に  
提供している

セキュリティリーダーがこの大きな責任を果たすには、リスクと戦略の両方に権限を持つ最高責任者（CEOなど）の直属である必要がある。2015年の調査では、直属の上司として挙げられたのはCEO、CIO、取締役会、CTOだった（回答数順）。大企業では、情報セキュリティ機能がCIOの配下に設置されるケースもしばしば見られる。

PwCでは、一部の例外を除き、CISOやCSOは、CIOとは別に独立した役職であるべきだと考えている。相互牽制の他、セキュリティの課題を経営陣に上申できる体制を確保するためだ。また、サイバーセキュリティの予算も懸念される。CISOやCSOに必要なスキルと権限があっても、十分な資金がなければ職務を遂行することはできない。

「企業はテクノロジー中心の見方をする傾向があるが、サイバー情報が増えるほど、テクノロジーだけではなく、従業員やプロセスが着目されるようになるだろう」（Marsh, Claude Yoder氏）

## 経営陣はよりサイバー セキュリティに巻き込まれる

今日のサイバーセキュリティインシデントは、多くの場合、事業運営、評判、財務の面で損害を引き起す。そのため経営陣は、部門を越えた戦略や法務、財務に影響を及ぼす重大なリスク管理の問題としてサイバーセキュリティに取り組むようになった。

全米取締役協会（NACD）のガイドラインでは、サイバーリスクを企業全体の視点から捉え、潜在的な法的影響を把握するよう勧告している<sup>10</sup>。サイバーセキュリティリスクや準備状況について話し合い、企業全体のリスク許容度に照らしてサイバー脅威を考える必要がある。

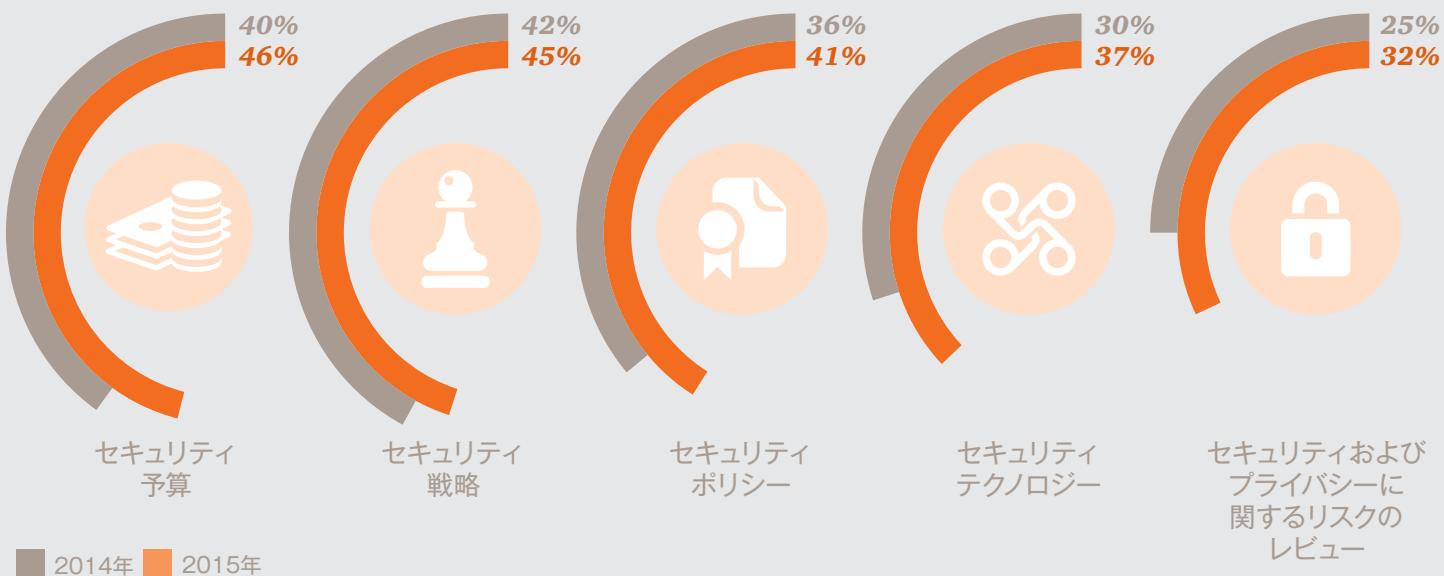
幹部はこの助言に耳を傾けているようだ。本年の調査では、情報セキュリティのほとんどの面で経営陣の参加率が二桁の増加を示した。参加率が増したことで、多くのサイバーセキュリティへの取り組みが向上したという声が寄せられている。サイバーセキュリティ予算会議への経営陣の参加率増加とともに、セキュリティ支出が24%増加したのは偶然ではないだろう。主なリスクの識別、セキュリティを重視する企業文化の醸成、全体のリスク管理やビジネス目標とサイバーセキュリティの連携の強化なども注目すべき成果だ。

# 45%

取締役会が  
セキュリティ  
戦略全体に  
関与している  
企業の割合



## 情報セキュリティへの経営陣の参加



何よりも、サイバーセキュリティ部門と経営陣が意見を交わせるようになったことが功を奏したのだろう。CIBCのLoBianco氏は次のように述べている。「サイバーセキュリティは経営に携わる者だけではなく、リスクやコンプライアンスにかかわる者も参加して取り組むべき企業全体の課題であることが理解されるようになった。その結果、経営陣と積極的に意見を交換する機会が増えた。プログラムの有効性など、さまざまな点について最新情報を定期的に報告することが期待されている」

LoBianco氏によると、CIBCでは、最高リスク責任者がリスク管理を統括し、セキュリティの脅威やインシデントに関する重大な進展について「リアルタイムに近い」報告を受けることになっている。

しかし、現在求められている報告は、不安分析ではない。SteelcaseのBerman氏は次のように語っている。「私は絶対に、恐れ、不安、疑念に話を持っていないようにしている。私は経営陣に対して、セキュリティ問題を暗闇に潜む怪物の話のように説明しない。経済的意志決定として管理可能なリスクであると説明する」

「私は経営陣に対して、セキュリティ問題を暗闇に潜む怪物の話のように説明しない。経済的意志決定として管理可能なリスクであると説明する」(Steelcase、Stuart Berman氏)

## M&Aに伴うサイバーセキュリティのデューディリジェンス

企業がM&Aを通じて成長するときは、買収先企業のサイバーセキュリティへの取り組みと法的責任が重大なリスクとなる。

買収先企業におけるサイバーセキュリティの取り組みを十分に評価しなければ、攻撃にさらされる恐れがある。サイバー攻撃者は狡猾にも、サイバーセキュリティ対応能力の低い小企業に潜入り、大企業に買収される機会を窺っているからだ。情報システムが統合されることで買収元企業のネットワークに足掛かりを得て攻撃を行う。

従って、財務状況だけではなく、買収先のサイバーセキュリティ能力とリスクを精査することが不可欠だ。しかし、買収先企業がどのようにデジタル資産を保護しているかを徹底的に調査する企業は少ない。Freshfieldsが214社のグローバル仲介企業を対象として行った調査では、回答者の78%が買収プロセスでサイバーセキュリティの詳しい分析や具体的な数値化を行っていなかつた<sup>11</sup>。

サイバーセキュリティリスクの評価では、検証すべき点が3つある。買収先企業が本社を置き事業を運営している国、業種、および個々のセキュリティへの取り組みとインシデント履歴だ。国によっては事業リスクがもともと高く、サイバーセキュリティおよびプライバシーに関する規制が厳しいこともある。リスクのタイプは業種によっても異なる。

買収先の情報資産台帳や保存場所(サードパーティサプライヤーのデータも含む)、データ収集プロセス、サイバーセキュリティに関するポリシーや管理策、プライバシーポリシー、サイバーセキュリティ保険の補償範囲などが脆弱性を図るために主要なポイントだ。また、インシデントレスポンス計画や危機管理計画の有無の他、過去にセキュリティ侵害が発生したことがあるかどうか、インシデントにどのように対応したかを考慮することも重要だ。

問題は、買収先のサイバーセキュリティの取り組みを評価する時間がごく限られていることだ。混乱なく迅速に買収先を評価するには、入念に練られた戦略をもってデューディリジェンスにあたる必要がある。

## 買収先企業のサイバーセキュリティ上のリスクを検証する際の3つの観点



11 Freshfields Bruckhaus Deringer, *Cyber Security in M&A*, July 2014

# サイバーセキュリティの未来に向けて

本書で取り上げた革新的なサイバーセキュリティ対策は、現時点で既知の脆弱性や脅威からの防御を強化するために役立つ。しかし、テクノロジーは進化し、攻撃者は腕を磨いている。将来のリスクを予期するにはどうすればよいのだろうか。



この問いに答えるのは簡単なことではない。いくら予測しようとしても、見えるのはせいぜい方向性くらいだ。現在の状況が不安定で常に移り変わっている以上、未来を予知することはほぼ不可能だ。とはいっても、今後5年間でサイバーセキュリティに備えるために、前提とすべきことはいくつかある。

まず、デジタル化は日常の生活の中でますます進むということだ。収集、分析されるデータが増加するほど、漏洩の可能性も高まる。人材やプロセスに関する情報の生成と共有も増える。IoTの普及とともに、マシン間での情報のやりとりも活発になるだろう。データの急増に伴って、個人や企業のIDおよびプライバシーは集約されていく。

今後の攻撃では、さらに巧妙なツールや手法が組み合わせられることを覚悟しておいたほうがよい。スパイと政治的ハッキングを織り交ぜた攻撃が官民ともに仕掛けられるようになり、狡猾さと攻撃性が増す。国家や政治的動機を持つハッカーによる攻撃が経済的制裁やサイバー戦争を引き起こす可能性もある。さらに、壊滅的なサイバーセキュリティインシデントが発生し、政府によるID管理が必要になる可能性もまったくないとは言い切れない。

認証およびID管理は、サイバーセキュリティにおける諸刃の剣だ。適切な防御を実現するには、ビッグデータ、クラウドコンピューティング、ヒューリスティックモデルに基づく新しいソリューションが必要だ。

先進的な企業は、従来の境界ベースの防衛から、データとユーザー行動パターンのリアルタイム分析に基づくクラウド型サイバーセキュリティへの移行に着手している。IoTの広がりとともに、M2Mのデータやアクティビティの分析はますます重要になってくる。このようなデータ中心の環境では、強度の高い暗号化の重要性を軽視することはできない。

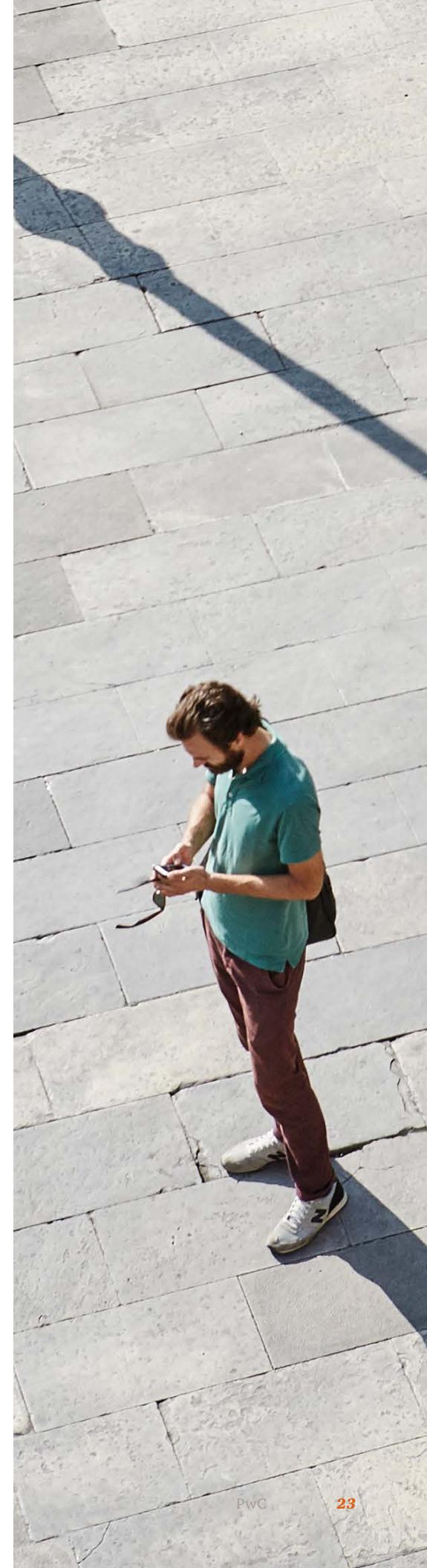
現在の地位に安穏としているソリューションベンダーが5年後もサイバーセキュリティの最先端を行っている可能性は低い。革新的なソリューションはむしろ、時代の流れに敏感な中小企業やスタートアップ企業から生まれるだろう。企業は多様なベンダーが提供する幅広いサービス、ソリューションを選択することになる。その結果、多種多様なテクノロジーと調和するセキュリティやITソリューションが求められるようになる。ベンダーによる囲い込みは境界ベースのセキュリティと同じ運命をたどることになる。今後は豊富な選択肢を取りそろえた者が圧勝するだろう。

事実、個人と企業のIDが融合すれば、現在私たちが知っているエンタープライズITは消えるだろう。各部門が独自のアプリケーションを構築してクラウドで運用するようになり、IT部門の支援はほとんど（あるいはまったく）不要になる。

政府は攻撃を追跡して侵入者の正体を突き止めようと、技術や能力の研鑽に励んでいる。個々のサイバー犯罪者や犯罪組織を告訴しても無駄だった。これからも効果は見込めないだろう。必要なのは、強制力のある国際条約だ。

現在の予測どおりに物事が進むかどうかはわからない。サイバーセキュリティの移り変わりを考えれば、5年後はあまりに遠い未来だ。

結局のところ、予想が役立つかどうかは疑問だが、用心のためさまざまな状況をあらかじめ想定しておくことは不可欠だ。先を見越して活発な議論を行うことで、起こり得るシナリオを探り、サイバー犯罪に対抗するレジリエンスを実現するための戦略を策定できる。将来を見据えたサイバーセキュリティプログラムを開発するには、テクノロジー、プロセス、人材のバランスをとることも必要だ。さらにさまざまなイノベーションが加わり、充実したセキュリティ対策を取ることが可能になる。今後の展開がどうなるにせよ、このような準備が整って初めて未来に備えることができるのだ。



# 日本企業への示唆

本セクションは、グローバル情報セキュリティ調査2016にご協力いただいた日本企業286社のデータを、プライスウォーターハウスケーパース株式会社が独自に分析し、グローバルとの比較を通じて、日本企業が今後取り組むべきサイバーセキュリティのポイントをまとめたものである。

## 示唆①：変化するサイバー脅威に対応したセキュリティフレームワークを活用すべき

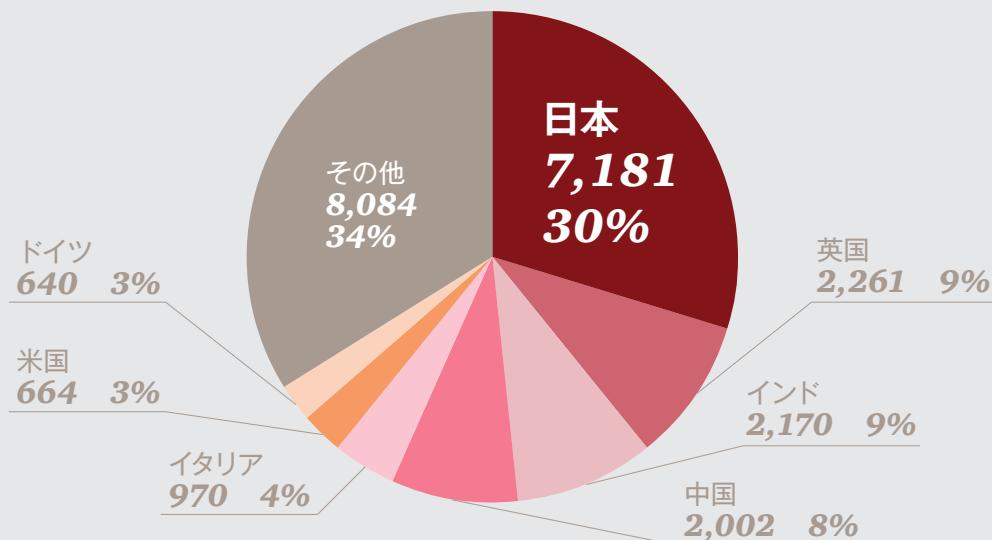
### 情報資産の保護からサイバーレジエンスの強化へ

サイバーセキュリティへの取り組みは、サイバー脅威に応じた個々のコントロールの導入から、マネジメント態勢の構築へと進化している。変化の大きいサイバー脅威に柔軟に対応するため、企業全体でのレジリエンス強化が求められている。

これまで、多くの日本企業は、「情報資産の保護」に重点を置いた情報セキュリティ対策を講じてきた。「機密性」「完全性」「可用性」の3つの軸で情報資産の重要性を定義し、その重要度に応じた対策を講じるというものだ。今日では、多くの日本企業がISO27000シリーズに則って情報セキュリティマネジメントシステム（ISMS）を構築している。

その一方で、昨今、企業価値や顧客サービスを脅かす「サイバー脅威」は、社員や委託先などの内部関係者の脅威に加え、外部からのサイバー攻撃が日常化し、手口が巧妙化している。また、組織が持つデジタルデータの増加により、情報漏洩リスクは飛躍的に拡大している。脅威の複雑性や企業に求められる対応のスピードはすっかり様変わりしてしまった。企業においては、時代にあったサイバーレジエンスの強化が急務であると言える。

図1：グローバルのISO27001認証組織比率（2014年）



出典：the ISO Survey on Management System Standards Certifications, [www.iso.org](http://www.iso.org)

## 日本企業は、ISO27001のセキュリティフレームワークに偏重

日本企業のセキュリティ対策の特徴を端的に示したデータがある。ISO 27001認証（情報セキュリティマネジメントシステム：ISMS）の国別取得企業（組織）数の割合である（図1）。日本企業でISMSを取得している企業数は、グローバル全体の3割を占め、ISMSの発祥国である英国の約3倍という高い認証取得数である。また、この数字には表れていない部分においても、認証こそ取得していないが内部管理の枠組み（フレームワーク）としてISMSを活用している日本企業が相当数あることも知られている。ISMSは、紛れもなく日本におけるセキュリティフレームワークのデファクトスタンダードなのである。

## グローバルで活用されているフレームワーク

では、海外の企業はどのようなフレームワークを活用しているのだろうか。PwCの最新のグローバル調査によれば、NIST（米国国立標準技術研究所）のCSF

（サイバーセキュリティフレームワーク）がISMSを追い抜くような勢いで採用されていることがわかる（図2）。

ここで注目すべきことは、NISTのCSFはわずか1年半前の2014年2月に発表されたばかりの新しいフレームワークであるという点である。そこで今回は、NISTのCSFとは何なのか、なぜ海外の企業で適用が進んでいるのか、NISTのCSFをはじめとするセキュリティフレームワークをどのように活用しているかについて見ていきたい。

## NIST CSF その成り立ちと特徴

2013年2月、米国で「重要インフラのサイバーセキュリティ強化に関する大統領令（第13636号）」が発表された。これは重要インフラサービスにおけるサイバーセキュリティの強化を目的とした包括的な指針と位置付けられ、この大統領令を受けて、2014年2月にNISTが発表したのが「重要インフラのサイバーセキュリティを強化するフレームワーク（NIST CSF）」である。

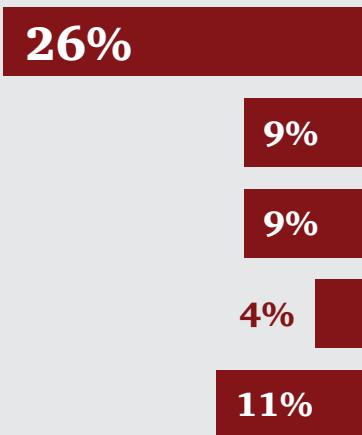
NISTのCSFはサイバーセキュリティ管理に必要な項目を「特定」、「防御」、「検知」、「対応」、「復旧」の5つのカテゴリーに分けて構成している。フレームワークとしての特徴の1つは、企業におけるリスク管理の一環としてサイバーセキュリティを扱う点である。このフレームワークはそもそも経営者によるサイバーセキュリティ管理のための枠組みとして設計されている。例えば、予防的統制（防御）、発見的統制（検知）などサイバーセキュリティへの対策状況を経営者が普段用いているマネジメントやリスク管理の言語で語れることである。

特徴の2つ目は、「サイバーセキュリティに関する対策は企業によって異なる」というリスクベースの論理に立脚していることである。従来型のセキュリティフレームワークの多くは、セキュリティに必要な「技術的対策」が詳細に記述され、企業はそのフレームワークに記載された対策を上から順に適用することで、他社と同じレベルのセキュリティ対策を実現するというコントロールベースの概念だった。

NISTのCSFには詳細な技術的対策は記載されていない。それは、事業内容や事業規模の違いにより、企業を取り巻くサイバーリスクやサイバーリスクの許容度が異

## 図2:Q. あなたの組織・企業では、どのようなセキュリティフレームワークを採用していますか？

日本企業（n=126）



ISO27001

9%

NIST Cyber Security Framework (CSF)

9%

SANS 20 Critical Controls

4%

ISF Standard of Good Practice

11%

その他のフレームワーク

40%

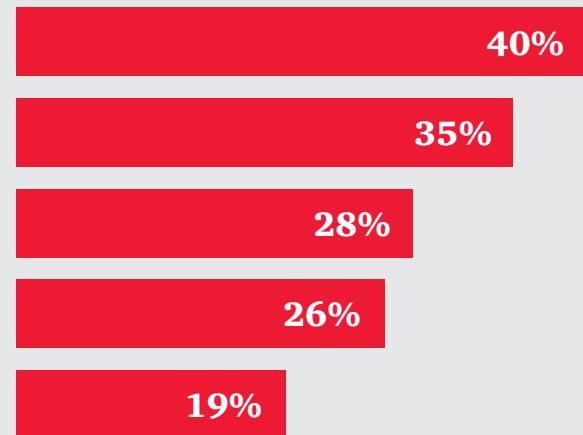
35%

28%

26%

19%

グローバル企業（n=8,140）



（複数回答、グローバル企業の回答の降順）

なるからである。NISTのCSFを活用することによって、例えば、「SOC」(セキュリティ・オペレーション・センター)を新規に構築する際、サイバーセキュリティのリスクや脆弱性の把握状況(特定)、防ぐことのできるサイバー攻撃の種類(防御)、インシデントレスポンスや危機管理態勢との連携(検知、対応、復旧)などが見えてくる。銀行における不正送金対策の見直しであれば、海外送金機能の有無によるサイバーリスクと影響(特定)、成りすましや金銭の窃取への対応状況(予防、検知)、顧客補償や追加施策の検討(対応、復旧)といった形でサイバー施策に必要な事項を可視化することができる。

なお、このフレームワークは、既存のセキュリティフレームワークを補完するものであり、技術的対策についてのガイドラインは従来のコントロールベースのものを参照することになっている。そして経営者向けのサイバーセキュリティガイドラインとしては現在、NISTのCSFが唯一無二の存在であることから、サイバーセキュリティという新たな分野への

チャンレンジにあたり、多くの企業がこのフレームワークを採用したのである。

## その他のセキュリティフレームワークの特徴と活用例

ISMSや今回紹介したNISTのCSF以外にも、セキュリティのためのフレームワークは多く存在する。そこで主要なセキュリティフレームワークを活用例とともにいくつか紹介したい。フレームワークの選択にあたっては、例えばグローバル企業とのベンチマークを実施したい場合にはISFを用いるなど、サイバーセキュリティ強化の目的にあった最適なフレームワークを選択し組み合わせることで、より効果的なインシアチブの設計が可能となる。

### ISO27001：情報セキュリティマネジメントシステム (ISMS)

情報資産をさまざまな脅威から守り、リスクを軽減させるための総合的なマネジメント規格。情報資産の保護をPDCAにより管理する。ただし、サイバー

セキュリティ固有の新たな脅威には必ずしも対応できないので注意が必要である。例えば、ISO27001の中にもインシデントレスポンスに関する記載はあるが、当該フレームワークが策定された当時は、今ほど外部からのサイバー攻撃が常態化していなかったため、インシデントの検知や動的な対応に関するガイダンスとしては十分ではない。

### NIST Cyber Security Framework (CSF)

米国の重要インフラ事業者向けに策定されたサイバーセキュリティマネジメントのスタンダード。サイバー攻撃への対応として「特定」「防御」「検知」「対応」「復旧」についての施策がまとめられている。

### ISF Standard of Good Practice

事業(ビジネス)に重点を置いて組織とサプライチェーンに関するリスクの識別と管理を行うための包括的なフレームワーク。Web上の専用ツールを用いてグローバルレベルでの同業他社とのベンチマーク比較をすることが可能である。業界水準に沿った態勢構築を目指す。

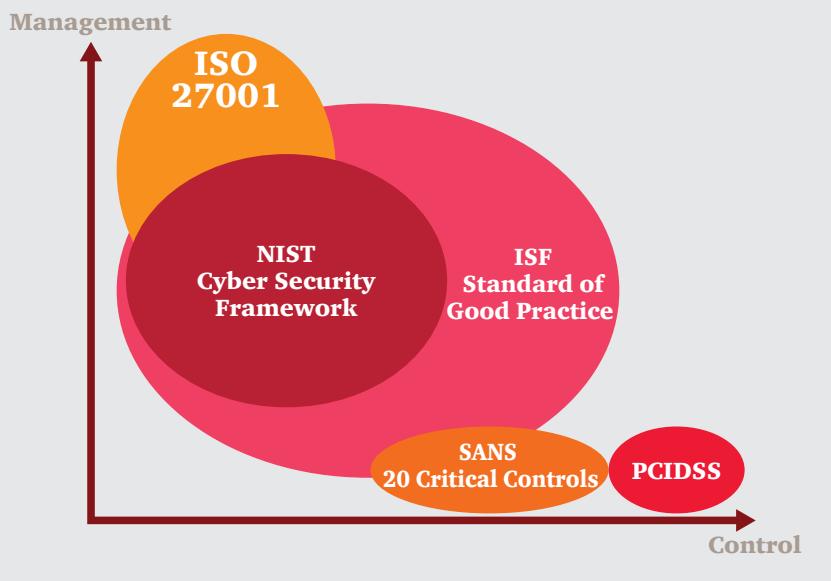
### SANS 20 Critical Controls

情報セキュリティ対策とコントロールについて優先付けされたベースラインを示したコンセンサスドキュメントであり、「最初に最低限行わなければならないセキュリティコントロール」に注力している。20項目のシンプルな構成の中で詳細な技術的コントロールが定義されているため、企業が優先的に行うセキュリティ施策を検討する際に用いられる。

### PCI DSS

カード会員データを保護するために規定された技術面および運用面における要件のベースライン。情報セキュリティの具体的な施策が定量的に示されているため、カード番号の保護に限らず、さまざまな種類の情報の保護施策として適用することが可能である。

図3：代表的なセキュリティフレームワークとその位置付け



## 示唆②：なぜ、日本ではサイバーリスクの情報共有が進まないのか？

### 日本企業ではサイバーリスクの情報共有が遅れている

昨今、サイバー犯罪の増加に対応するため、各国でさまざまな取り組みが進められている。その1つに、組織間ににおけるサイバーリスクの情報共有がある。日本では、2014年にサイバーセキュリティ基本法が成立し、脅威情報の共有／連携が求められている。一方、米国では、2015年2月にオバマ大統領が「新たな情報共有組織の設立」に関する

署名を行い、同様に情報共有の強化を求めている。情報共有を目的とした組織は、国内外に発足し、日本でも既に一部の企業・組織の間で活発な情報共有が行われている。

### 図4：産官学による情報共有にかかる日米の動向

#### 日本の動向

##### サイバーセキュリティ基本法の概要

- ・「国、地方公共団体、重要インフラ産業、サイバー関連事業者などによる積極的な相互連携」の必要性を明文化
- ・「重要インフラ事業者などにおけるサイバーセキュリティの確保の促進」、「民間事業者および教育研究機関などの自発的な取り組みの促進」をはじめ、犯罪の取り締まりや研究開発の推進、人材の確保や育成、国際協力などの必要性を明文化

##### 金融庁の監督指針などからの抜粋

- ・「情報共有機関などを活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策などを共有し、自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮し、必要な態勢の整備に努めているか」という要求事項

#### 情報共有組織の国内事例紹介

##### 金融ISAC

2014年8月発足。会員企業による積極的な連携が行われている。国外組織（FS-ISACなど）との連携も実施。

#### 米国の動向

米国では、2015年2月13日の大統領令13691号により情報共有をさらに強化

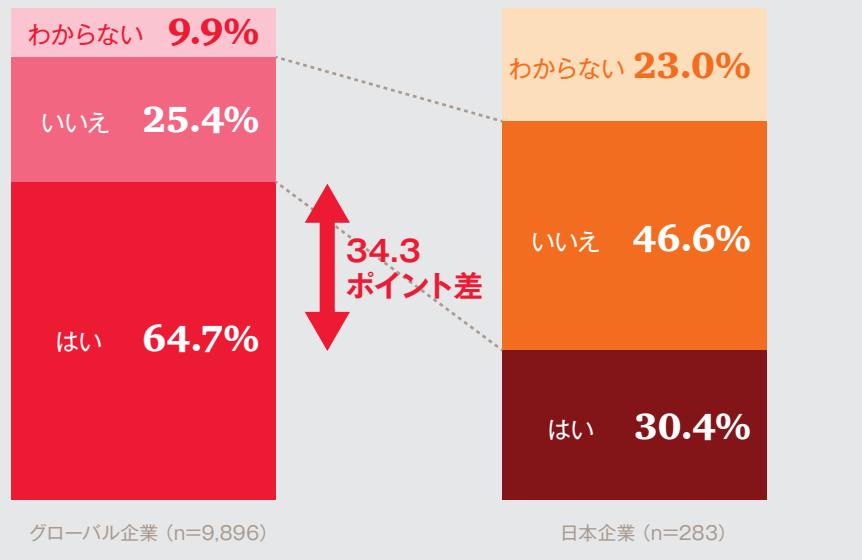
##### ISAOs (Information Sharing and Analysis Organizations)

- ・重要インフラ産業のみならず、各分野や地域ごとに設立
- ・サイバー攻撃の情報を一元化
- ・フレームワーク／プラットフォーム／データ形式を標準化し、情報共有の自動化メカニズムを開発
- ・国土安全保障省傘下に、重要インフラ保護のために設立したNational Cybersecurity and Communications Integration Center(NCCIC)と連携

##### 日本CSIRT協議会

2007年3月発足。業界横断で国内企業のCSIRTが加盟している。脅威情報の共有、インシデント対応の共同演習など、活発な活動を展開。

## 図5:Q. 多組織とサイバーリスクに関する情報共有を行っているか?

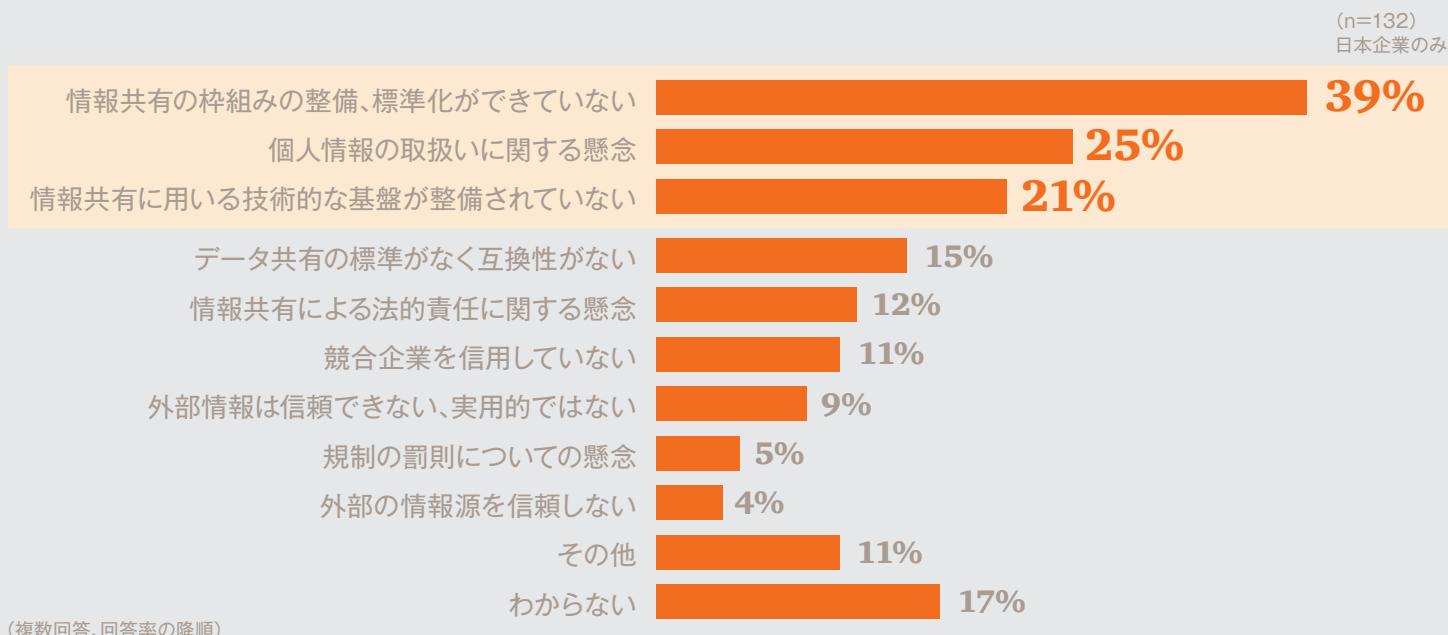


調査の結果、日本企業において、組織間でサイバーリスクの情報共有活動を行っている企業の割合は、約3割であることが判明した(図5)。この値は、グローバルの平均値と比較すると、半分未満にとどまっている。組織間の情報共有が求められる中、日本企業ではサイバーリスクの情報共有が遅れていると言える。

## 日本企業が情報共有に積極的でない理由

それでは、日本企業はなぜ情報共有に積極的でないのだろうか。情報共有を行わない企業は、その理由として、情報共有のプラットフォームや共有された情報の取り扱いに関する規則が未整備であるという問題を挙げている(図6)。情報共有を行う上で、どのように行うべきかわからない、情報を共有することによるリスクを測ることができない、といった課題が組織間の情報共有の足かせとなっている。

## 図6:他組織と情報共有を行わない理由



その一方で、情報共有により、企業はどのようなメリットを享受しているのだろうか。多くの企業は、同業他社、業界組織、政府関係機関から提供された情報に実用性を感じている（図7）。この点に関して、グローバル、日本ともに同じ傾向が見てとれる。

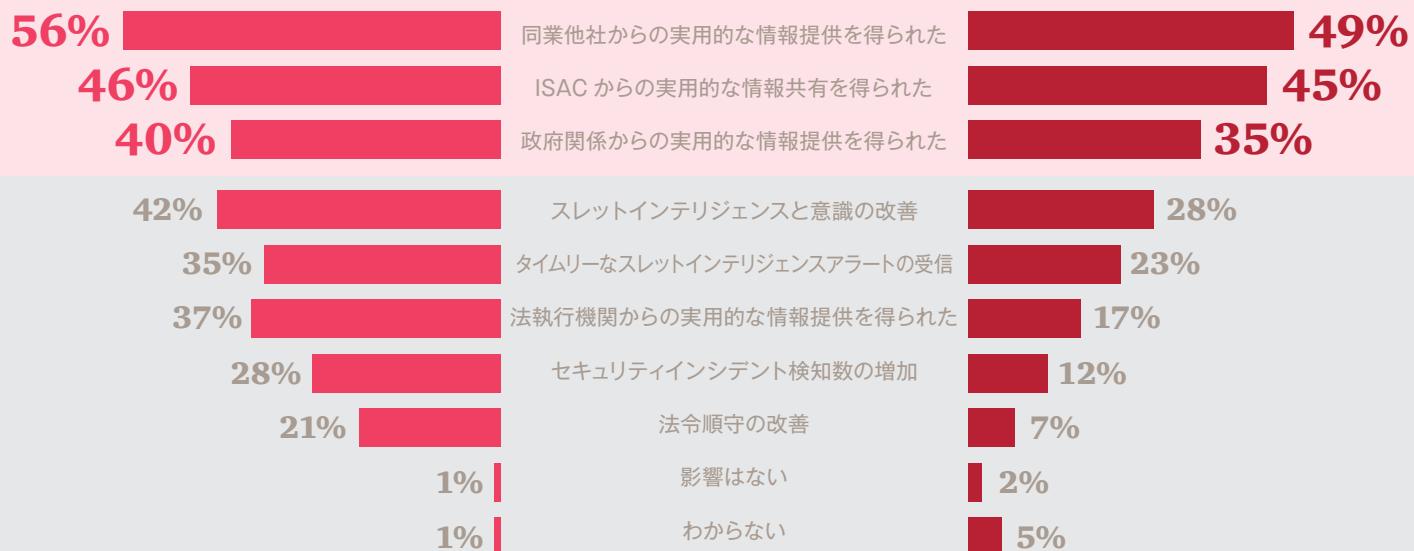
このことから、組織間の情報共有は、脅威情報の収集手段として有効に機能していると考えられる。そして、情報共有を行っていない日本企業は、このメリットを享受できていない。



## 図7:情報共有による自組織へのメリット

グローバル企業 (n=6,370)

日本企業 (n=86)



（複数回答、日本企業の回答の降順）

## 効果的な情報共有を実現するために

情報共有を活発化させるためには、業界としての対応が求められる。業界内で情報共有を行うためのプラットフォームや規則の整備を行い、展開・最適化していくことで、組織間の情報共有を後押しできる。このとき、企業には、展開される情報を受け取るばかりでなく、積極的に参画し、情報を提供していく姿勢が必要となる。これは、各組織だけでなく、業界全体のセキュリティ向上を実現していく上で必要な心構えとなる。

また、効果的な情報共有を実現するにあたり、企業内での課題が想定される。自社社員が業界組織に対して、積極的に参画する中で、その活動が他社を助ける活動であるというだけでなく、翻って自社のセキュリティ向上に対しても貢献するものであることをマネジメント層が理解し、社内で適切に評価する必要がある。また情報の提供を受けて、自社に対する影響、リスクの程度を判断し、適切な対応を行っていくために、情報を活用していくプロセスと仕組みの整備が重要となる。

図8:効果的な情報共有を実現する上での課題

### 業界としての課題



#### 枠組み／標準の不在

情報共有の枠組み／標準の整備、展開が必要



#### 共有情報の取り扱い規則

共有情報の取り扱いについて、組織間で統一された規則の策定が必要



#### 技術基盤の整備

共有情報が安全に保護されるためのインフラ整備が必要

### 企業内の課題



#### マネジメント層の理解不足

他社との情報共有活動に対し、自社のセキュリティ向上へ貢献するものとして、社内で適切に評価される制度が必要



#### 情報活用プロセスの不在

共有情報と自社環境の照合による影響・リスクの特定、脅威情報の社内通達、ナレッジDBへの登録など、情報を活用するプロセスの整備が必要

## 示唆③：スレットインテリジェンスを活用し、サイバー攻撃を予知せよ

### スレットインテリジェンスの活用：脅威情報サブスクリプションの効果

高度化するサイバー攻撃により、個人情報や機密情報の流出、金銭窃取などの深刻な被害が急増しており、事前対策だけでは、もはや防ぎきれない。従来の防御主体のセキュリティ対策から脱却し、攻撃を受けることを前提として迅速な対応を行うため、さまざまな脅威について適切に分析・評価した情報であるスレットインテリジェンスの活用に注目が集まっている。

図9:スレットインテリジェンス

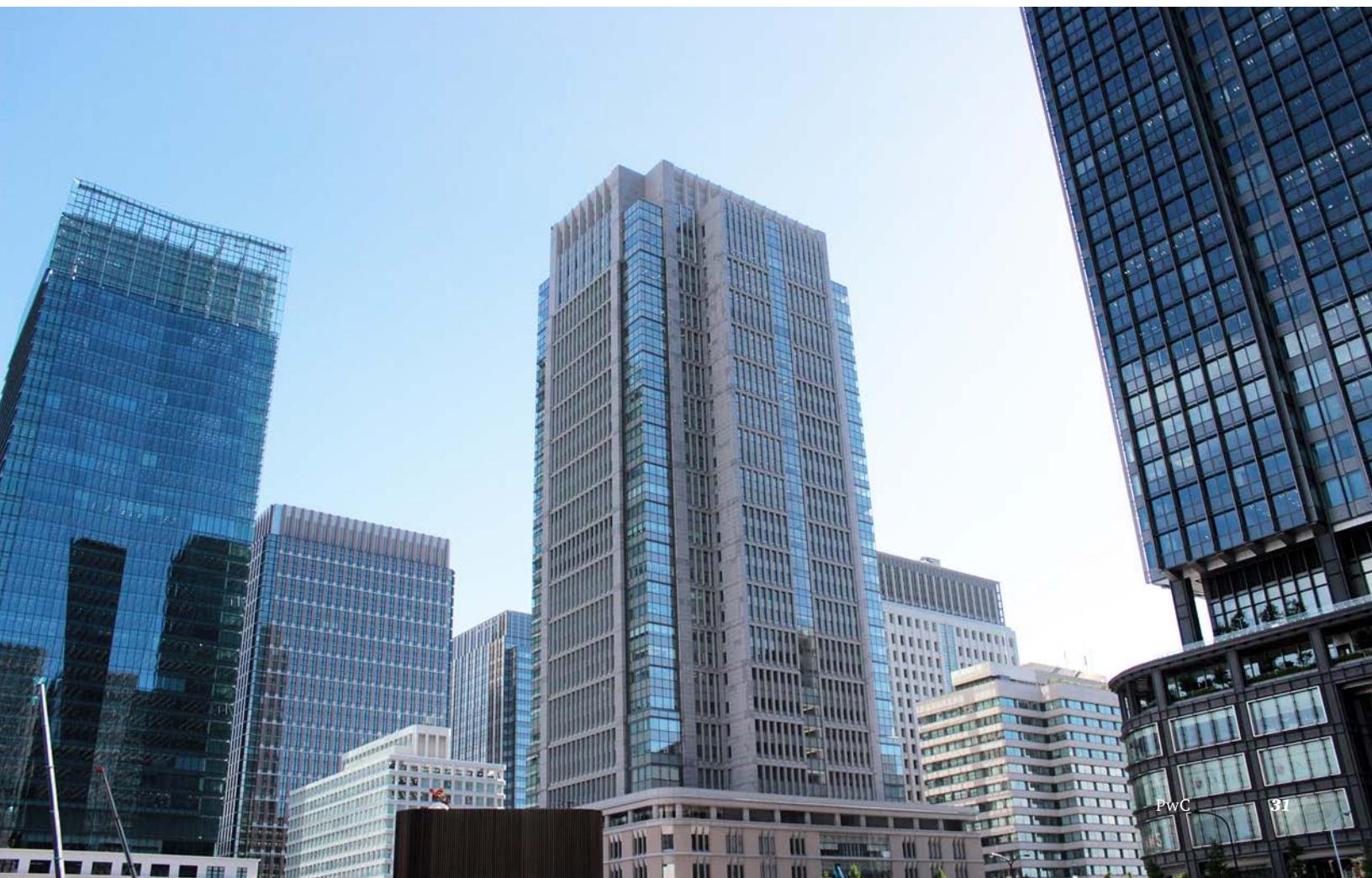


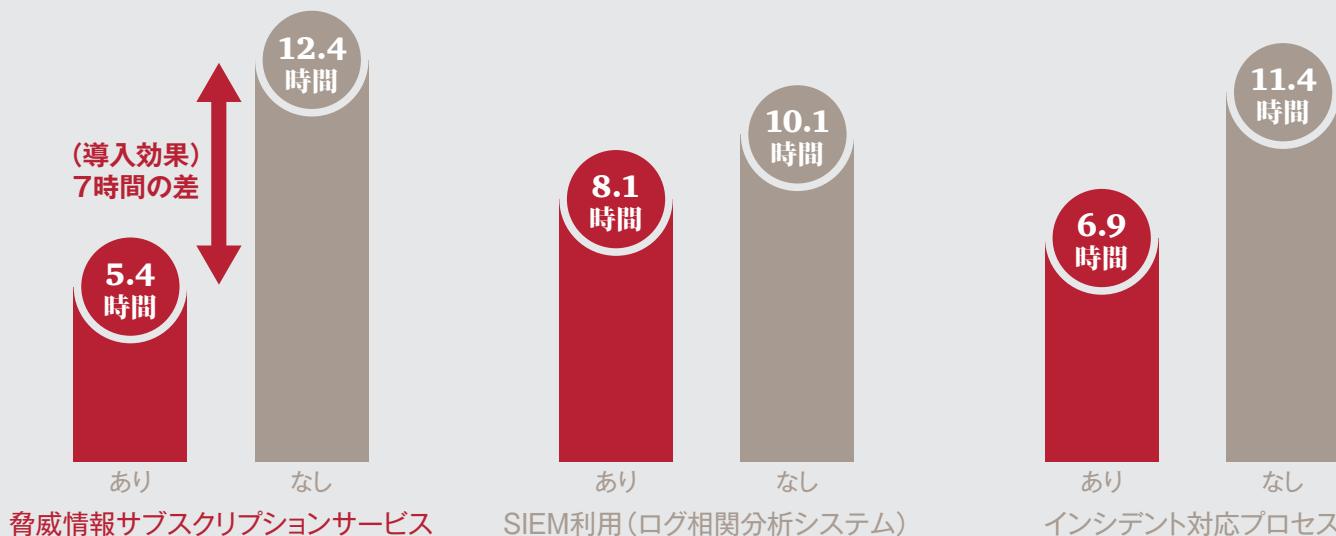
図10はセキュリティ関連インシデントにより発生したダウンタイム（サービス／アプリケーション／ネットワークが利用できなくなる状態）と、実施しているセキュリティ対策の関係を示している。さまざまなセキュリティ対策の内、セキュリティインシデントによる業務停止時間を短くすることに最も効果的だったのは、スレットインテリジェンスの1つである、「脅威情報サブスクリプションサービス（セキュリティ脅威と解析情報の定期購読サービス）」であった。SIEM（ログの相関分析）ツールの導入や、CSIRTにおけるインシデント対応プロセスを整備することもダウンタイムを短くすることに寄与しているが、その効果は比較的小さかった。

## スレットインテリジェンスの活用：脅威情報の業界別採用率

図11は脅威情報サブスクリプションサービスの業界別採用率を表している。金融業界では3分の2の企業（66%）が脅威情報サブスクリプションサービスを利用している。金融ISACに加盟することで、会員企業に配信される脅威情報を入手することができるため、それが本調査の結果にも表れたと考えられる。金融機関によっては、それ以外にも複数のルートから脅威情報を購入している企業が少なくない。

図10: Q. 過去一年間で、セキュリティ関連インシデントのために合計何時間のダウンタイムが発生しましたか？

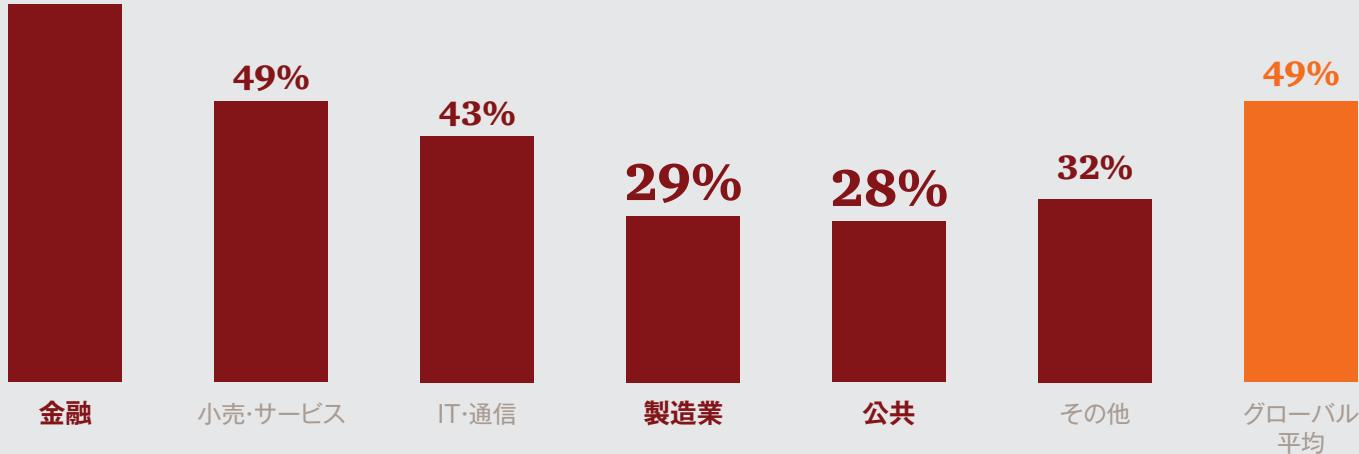
(n=235)  
日本企業のみ



## 図11:Q. あなたの組織において、現在「脅威情報サブスクリプションサービス」を導入していますか？

(n=286)  
日本企業のみ

**66%**



ある国内の銀行では、脅威情報をログ解析ツールに取り込み、分析することでサイバー攻撃を検知している。また、ある保険会社では、脅威情報をもとに攻撃の時期を予測し体制を整備するなど、金融業界においては、脅威情報サブスクリプションサービスを活用している事例がいくつかあり、効果が出ている。

一方、製造業や公共の2業種は、製造業29%、公共28%と、脅威情報サブスクリプションサービスの導入があまり進んでいないことがわかった。

## 図12:金融業界における脅威情報サブスクリプションサービスの活用事例



ある国内銀行では、複数の情報元から入手した脅威情報をログ解析ツールに取り込み、分析することで、サイバー攻撃の検知、被害状況の把握の迅速化をはかっている



ある国内保険会社では、脅威情報をもとに攻撃の時期を予測し、責任者の夜間連絡体制構築などを整備している

## スレットインテリジェンスの活用：脅威情報サブスクリプションサービスから得られる有益な情報

スレットインテリジェンスを活用すると、公開情報からでは得られない最新の脅威情報を世界中からリアルタイムに入手でき、その中には、セキュリティ機器に配信されて自動的に設定に反映されるものもあるなど、サイバー攻撃の防御や検知をより迅速かつ正確にできる効果が期待できる（図13）。

## スレットインテリジェンスの活用：脅威情報の活用ステップ

脅威情報は、とにかく大量に収集すればいいというものではない。むしろ、さまざまな情報ソースから自社に有益な情報を取捨選択すべきである。脅威情報サブスクリプションサービスを契約したが、膨大な情報量に圧倒されて、有効な情報を見落としてしまったという事例を耳にすることがあることから、スレットインテリジェンスの運用方法で悩んでいる企業は多いのではないか。

図13：脅威情報サブスクリプションサービスから得られる有益な情報

得られる情報例	効果
<p>公開情報では得られない情報を入手</p> 	<p>サイバー攻撃のトレンド、攻撃手法に関する解説、個社別のカスタマイズ情報</p> <p>公開されていない情報から、サイバー攻撃の動向を把握し、未知の脅威へのセキュリティ対策をいち早く検討することが可能</p>
<p>最新の脅威情報をリアルタイムにセキュリティ機器へ配信</p> 	<p>マルウェアのファイル名、ハッシュ値の情報、ブラックIPアドレス、ドメイン情報、標的型攻撃メールの送信元アドレス、件名、本文、インシデント詳細情報、脆弱性情報</p> <p>最新の脅威情報（危険なURL、ファイルハッシュ値など）をリアルタイムにセキュリティ機器に配信し、自動的に設定に反映することで、サイバー攻撃の防御や検知をより迅速かつ正確に実施することが可能</p>

重要なことは、自社に適した脅威情報を選び、不要なもの捨てる事である。そのために、まずは自社のインベントリ情報（OS、アプリケーション、デバイスなど）を正しく把握する必要がある。自社に有益な脅威情報を厳選して収集することが、プロアクティブなインシデント対応態勢の第一歩である。

脅威情報を選別した後は、最新の脅威情報（危険なURL、ファイルハッシュ値など）を自動的にセキュリティ機器へ配信するよう設計する。自動化できない脅威情報に関しては、セキュリティアナリストのリソースを集中させ、自社内で情報の把握や分析を行い、脅威情報の内容に合わせた適切な対策（モニタリング強化、社員への周知啓蒙など）を実施する必要がある。そして、過去や現在のサイバー攻撃の状況を定期的に分析し、将来のサイバー攻撃をフォーキャスティング（予測）することが重要である。

#### 図14：脅威情報を活用したプロアクティブな対応態勢構築のステップ

##### 脅威情報の取捨選択

###### 【脅威情報提供元の例】

- ・サイバーセキュリティ調査機関
- ・政府・公共機関
- ・セキュリティベンダー
- ・業界団体・ISACなど

###### 【情報選定基準の例】

- ・自社利用OS
- ・自社利用アプリケーション
- ・自社利用デバイス

1



##### 情報取得時の対応整備

- ・社員への周知啓蒙
- ・SIEM、Proxy、IDS、エンドポイントなどによるモニタリング強化
- ・Firewall、Proxy、IPS、WAF、エンドポイントなどにブラックリストとして反映
- ・セキュリティパッチの適用

2



##### フォーキャスティング (予測)

- ・定期的な対策効果レビュー
- ・フォーキャスティングの実施

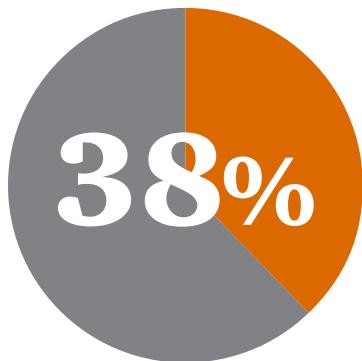
3



# 付録A：増大するサイバーリスクへの対応

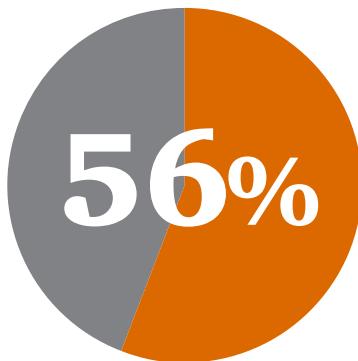
## グローバル情報セキュリティ調査2016

### セキュリティインシデントの平均数



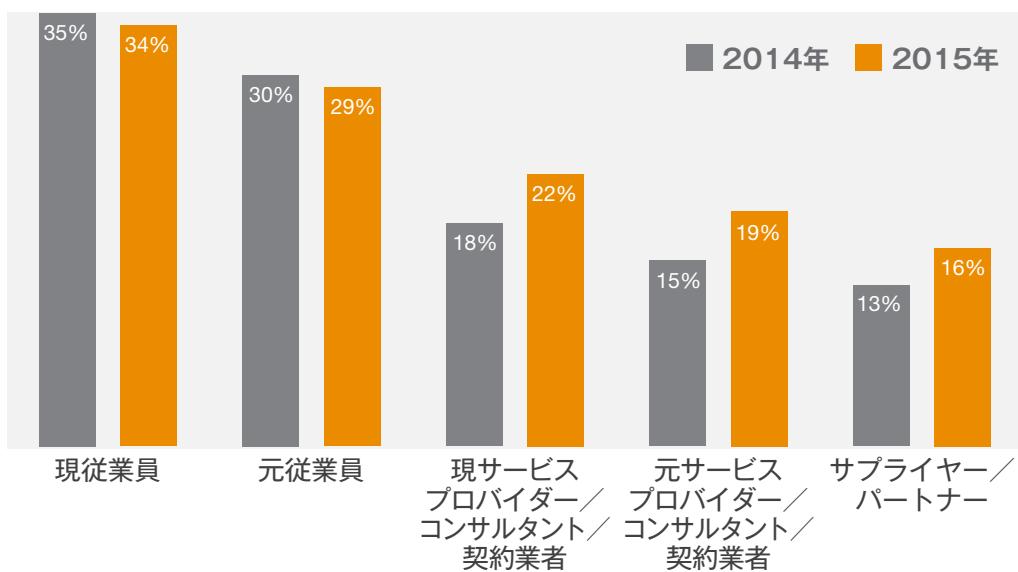
2015年のセキュリティインシデント検知数は2014年より38%増加

### セキュリティインシデントの影響



2015年の知的財産の窃取は56%増加

### セキュリティインシデントの発生源



**22%**

セキュリティ侵害の原因として挙げられたのは今回も「従業員」が最多だったが、「ビジネスパートナー」に起因するインシデントが22%を占めるようになった

## 情報セキュリティの平均予算



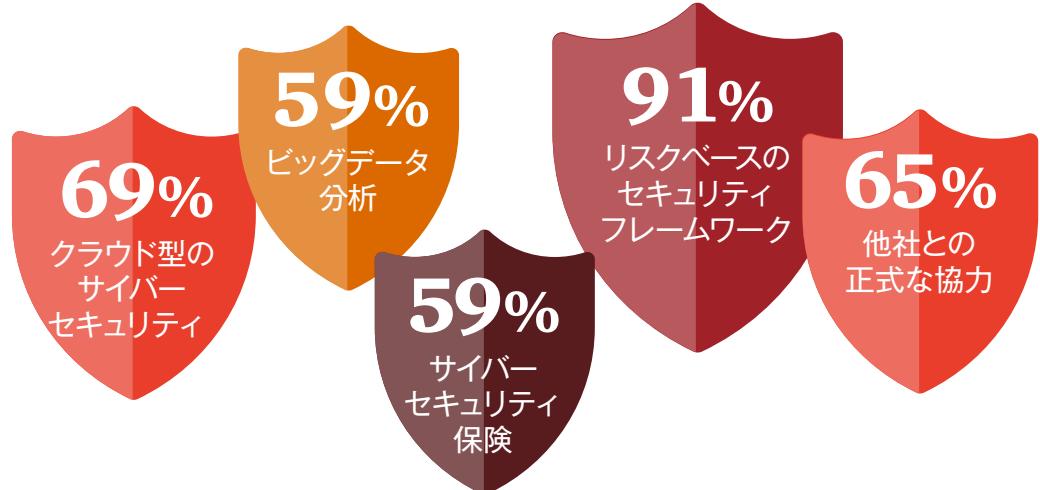
2015年の情報セキュリティ予算は24%  
増加

## セキュリティインシデントによる 平均的な財務的損失額

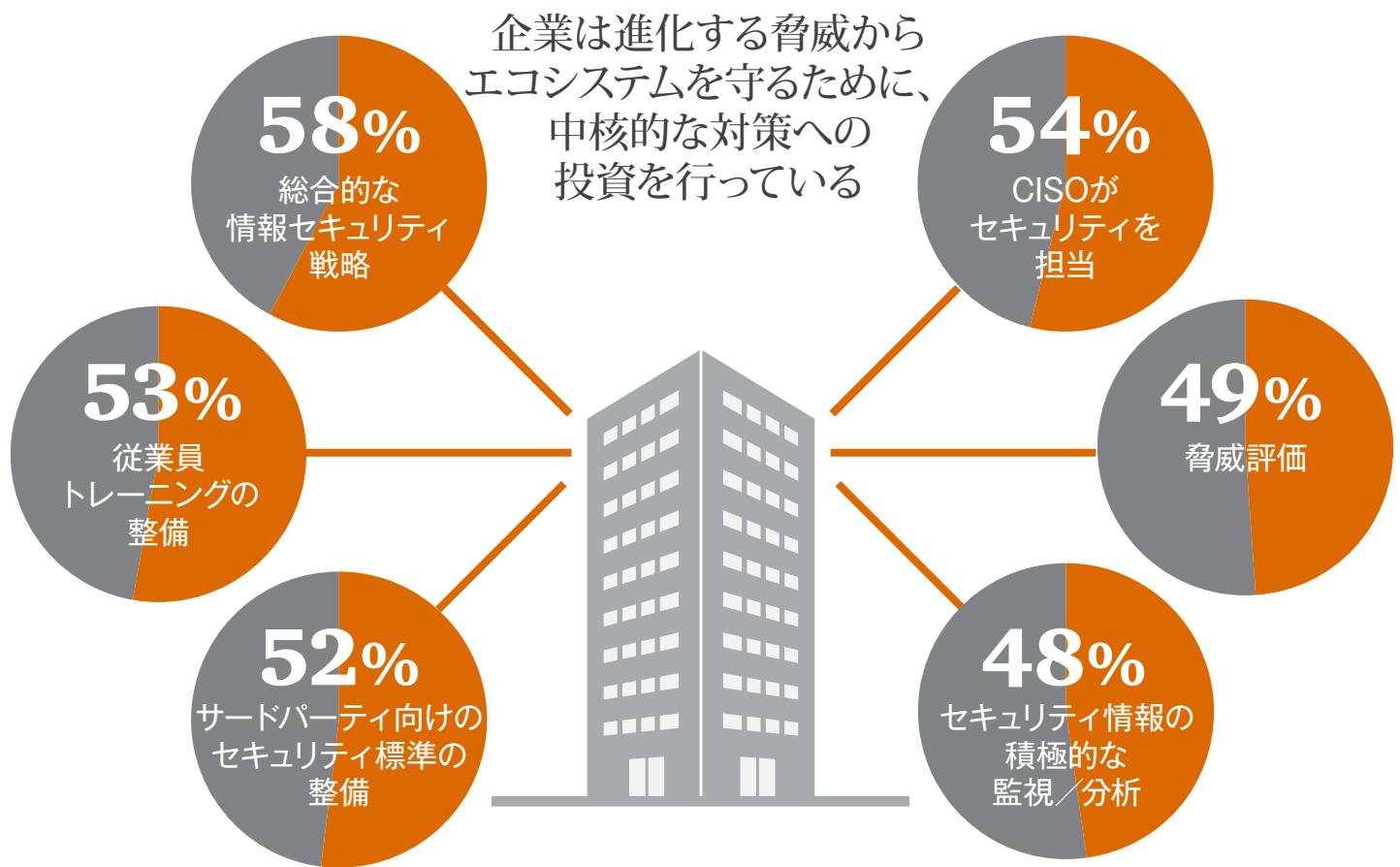


## 戦略的セキュリティイニシアチブの採用

多くの企業は戦略的  
イニシアチブにより、  
セキュリティの向上と  
リスクの低減に  
取り組んでいる



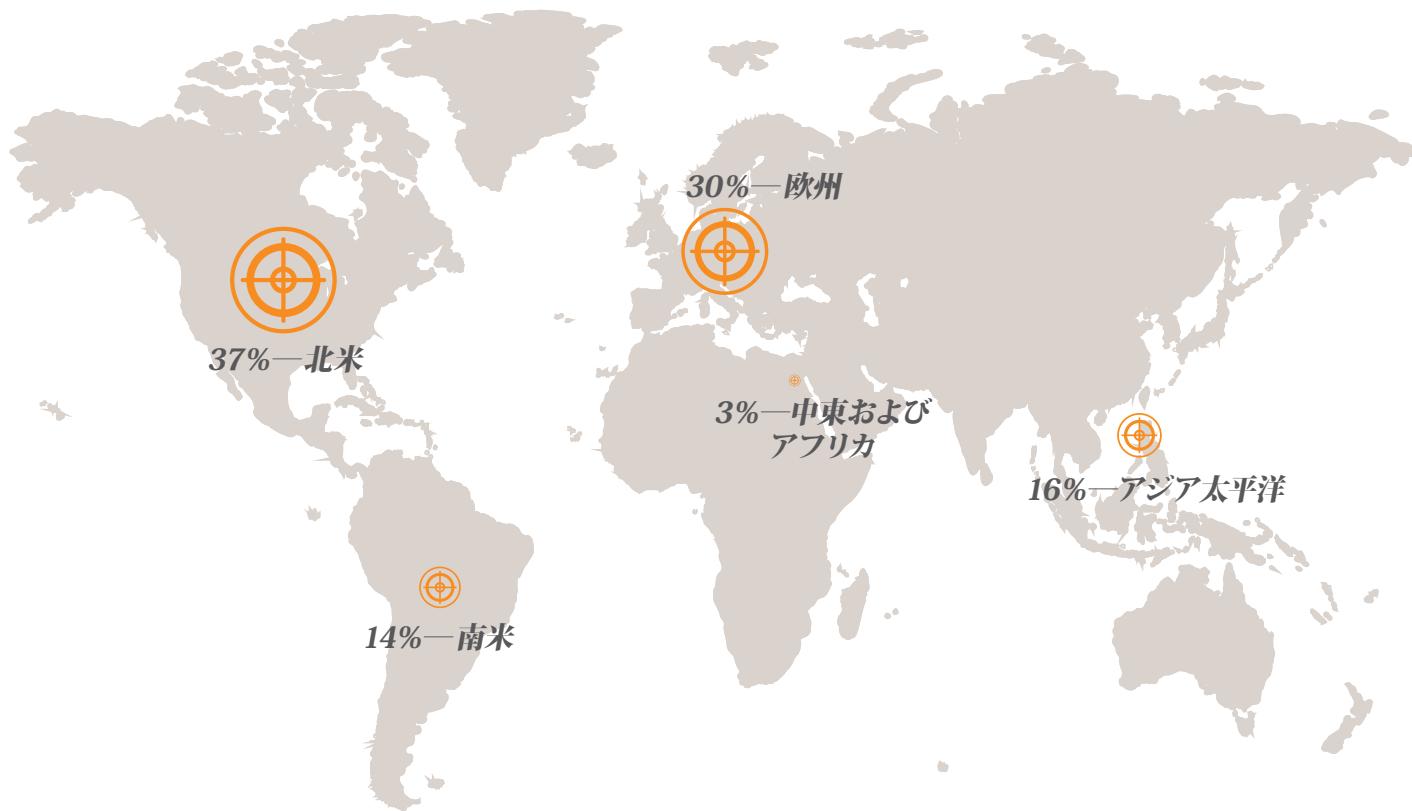
## 主なセキュリティ対策の実装



# 調査方法

グローバル情報セキュリティ調査 (The Global State of Information Security® Survey) 2016は、PwC、『CIO magazine』、『CSO magazine』が実施した世界的な調査である。2015年5月7日から2015年6月12日までを調査期間とし、オンライン調査を実施した。調査対象者は『CIO magazine』および『CSO magazine』の読者、世界各地のPwCのクライアントとし、電子メールで回答を依頼した。

本書で解説する調査結果は、127カ国、1万人以上の最高経営責任者 (CEO)、最高財務責任者 (CFO)、最高情報責任者 (CIO)、最高情報セキュリティ責任者 (CISO)、最高セキュリティ責任者 (CSO)、副社長、ITおよび情報セキュリティ役員からの回答に基づいている。



誤差は1%未満である。

このレポートの全ての図表は、調査結果に基づき作成されたものである。

# サイバーセキュリティおよびプライバシーに関する PwCのお問い合わせ先 (国別)

## Australia

**Richard Bergman**  
Partner  
richard.bergman@au.pwc.com

**Andrew Gordon**  
Partner  
andrew.n.gordon@au.pwc.com

**Steve Ingram**  
Partner  
steve.ingram@au.pwc.com

## Austria

**Christian Kurz**  
Senior Manager  
christian.kurz@at.pwc.com

## Belgium

**Filip De Wolf**  
Partner  
filip.de.wolf@be.pwc.com

## Brazil

**Edgar D'Andrea**  
Partner  
edgar.dandrea@br.pwc.com

## Canada

**David Craig**  
Partner  
david.craig@ca.pwc.com

**Sajith (Saj) Nair**  
Partner  
s.nair@ca.pwc.com

**Richard Wilson**  
Partner  
richard.m.wilson@ca.pwc.com

## China

**Megan Haas**  
Partner  
megan.l.haas@hk.pwc.com

**Ramesh Moosa**  
Partner  
ramesh.moosa@cn.pwc.com

**Kenneth Wong**  
Partner  
kenneth.ks.wong@hk.pwc.com

## Denmark

**Christian Kjær**  
Director  
christian.x.kjaer@dk.pwc.com

**Mads Nørgaard Madsen**  
Partner  
mads.norgaard.madsen@dk.pwc.com

## France

**Philippe Trouchaud**  
Partner  
philippe.trouchaud@fr.pwc.com

## Germany

**Derk Fischer**  
Partner  
derk.fischer@de.pwc.com

**Wilfried Meyer**  
Partner  
wilfried.meyer@de.pwc.com

## India

**Sivarama Krishnan**  
Partner  
sivarama.krishnan@in.pwc.com

## Israel

**Yaron Blachman**  
Partner  
yaron.blachman@il.pwc.com

## Italy

**Fabio Merello**  
Partner  
fabio.merello@it.pwc.com

## Japan

**Yuji Hoshizawa**  
Partner  
yuji.hoshizawa@jp.pwc.com

**Maki Matsuzaki**  
Partner  
maki.matsuzaki@jp.pwc.com

**Naoki Yamamoto**  
Partner  
naoki.n.yamamoto@jp.pwc.com

## Korea

**Soyoung Park**  
Partner  
s.park@kr.pwc.com

## Luxembourg

**Vincent Villers**  
Partner  
vincent.villers@lu.pwc.com

## Middle East

**Mike Maddison**  
Partner  
mike.maddison@ae.pwc.com

**Patrick MacGloin**  
Director  
patrick.macgloin@ae.pwc.com

## **Netherlands**

### **Otto Vermeulen**

Partner

otto.vermeulen@nl.pwc.com

### **Bram van Tiel**

Director

bram.van.tiel@nl.pwc.com

## **New Zealand**

### **Adrian van Hest**

Partner

adrian.p.van.hest@nz.pwc.com

## **Norway**

### **Tom Remberg**

Director

tom.remberg@no.pwc.com

## **Poland**

### **Rafal Jaczynski**

Director

rafal.jaczynski@pl.pwc.com

### **Jacek Sygutowski**

Director

jacek.sygutowski@pl.pwc.com

### **Piotr Urban**

Partner

piotr.urban@pl.pwc.com

## **Russia**

### **Tim Clough**

Partner

tim.clough@ru.pwc.com

## **Singapore**

### **Vincent Loy**

Partner

vincent.j.loy@sg.pwc.com

### **Kok Weng Sam**

Partner

kok.weng.sam@sg.pwc.com

## **South Africa**

### **Sidriaan de Villiers**

Partner

sidriaan.de.villiers@za.pwc.com

### **Elmo Hildebrand**

Director/Partner

elmo.hildebrand@za.pwc.com

### **Busisiwe Mathe**

Partner/Director

busisiwe.mathe@za.pwc.com

## **Spain**

### **Jordi Juan Guillem**

Director

jordi.juan.guillem@es.pwc.com

### **Elena Maestre**

Partner

elena.maestre@es.pwc.com

## **Sweden**

### **Martin Allen**

Director

martin.allen@se.pwc.com

### **Rolf Rosenvinge**

Director

rolf.rosenvinge@se.pwc.com

## **Switzerland**

### **Rodney Fortune**

Manager

rodney.fortune@ch.pwc.com

### **Chris Hemmi**

Manager

christoph.hemmi@ch.pwc.com

### **Jan Schreuder**

Partner

jan.schreuder@ch.pwc.com

## **Turkey**

### **Burak Sadic**

Director

burak.sadic@tr.pwc.com

## **United Kingdom**

### **Neil Hampson**

Partner

neil.r.hampson@uk.pwc.com

### **Richard Horne**

Partner

richard.horne@uk.pwc.com

## **United States**

### **David Burg**

Principal

david.b.burg@pwc.com

### **Scott Dillman**

Principal

scott.dillman@us.pwc.com

### **Chris O'Hara**

Principal

christopher.ohara@us.pwc.com

### **Shawn Panson**

Partner

shawn.panson@us.pwc.com

### **Grant Waterfall**

Partner

grant.waterfall@us.pwc.com

# お問い合わせ先

## プライスウォーターハウスクリーパース株式会社

03-6250-1200(代表)

**松崎 真樹**

パートナー

[maki.matsuzaki@jp.pwc.com](mailto:maki.matsuzaki@jp.pwc.com)

**山本 直樹**

パートナー

[naoki.n.yamamoto@jp.pwc.com](mailto:naoki.n.yamamoto@jp.pwc.com)

## PwCサイバーサービス合同会社

**星澤 裕二**

パートナー

[yuji.hoshizawa@jp.pwc.com](mailto:yuji.hoshizawa@jp.pwc.com)

[www.pwc.com/jp](http://www.pwc.com/jp)

PwC Japanは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた監査法人、京都監査法人、プライスウォーターハウスクリーパース株式会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、ディールアドバイザリー、コンサルティング、税務、法務のサービスをクライアントに提供しています。

PwCは、社会における信頼を築き、重要な課題を解決することをPurpose(存在意義)としています。私たちは、世界157カ国に及ぶグローバルネットワークに208,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は[www.pwc.com](http://www.pwc.com)をご覧ください。

本報告書は、PwCメンバーファームが2015年10月に発行した『Turnaround and transformation in cybersecurity Key findings from The Global State of Information Security® Survey 2016』を翻訳し日本企業への示唆を追加したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

電子版はこちらからダウンロードできます。 [www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html](http://www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html)

オリジナル（英語版）はこちらからダウンロードできます。 <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>

日本語発刊月：2016年2月 管理番号：I201508-9

©2016 PwC. All rights reserved.

PwC refers to the PwC Network and/or one or more of its member firms, each of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.