www.pwc.com/jp

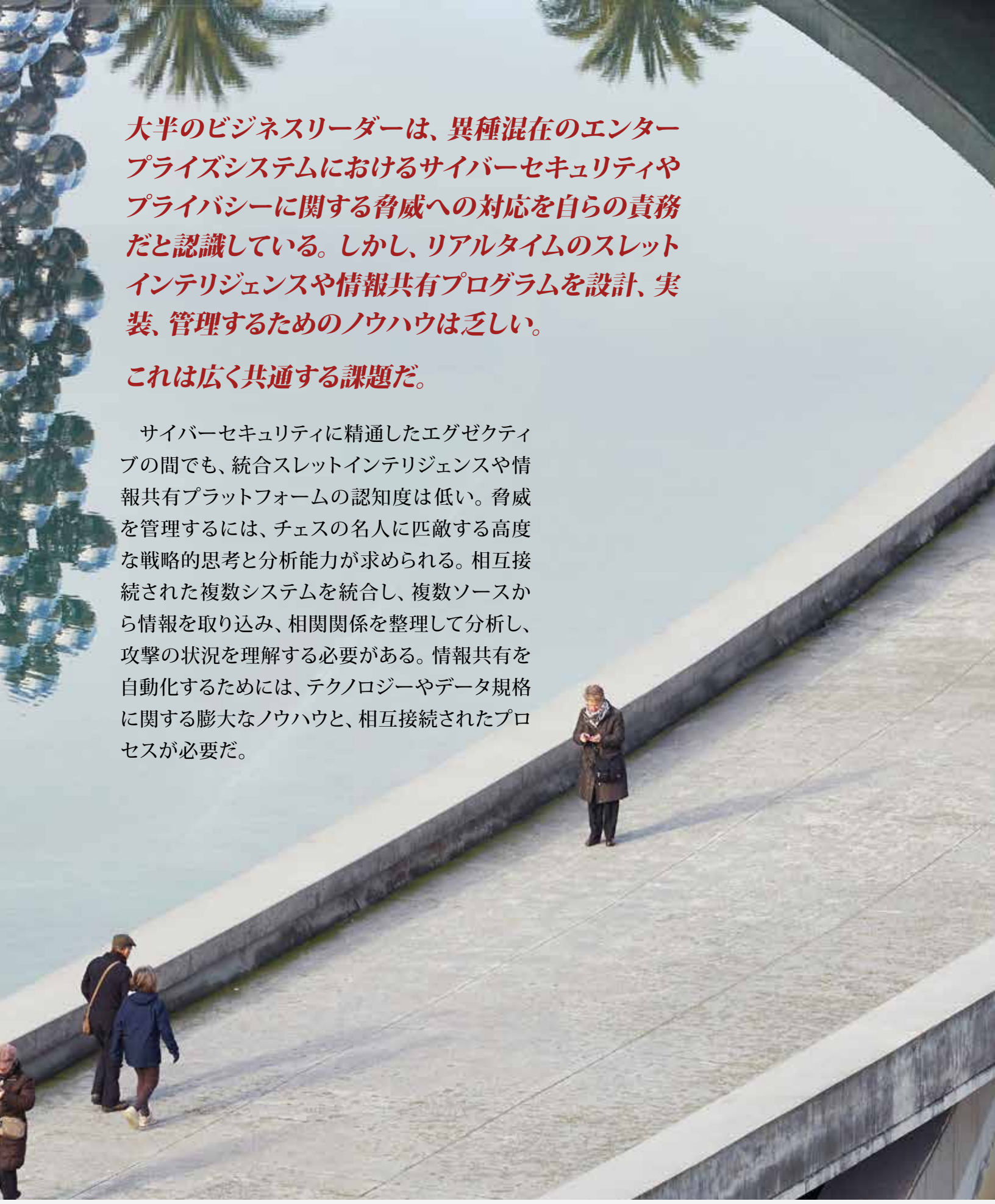
スレットマネジメントの新たな可能性に向けて

企業におけるスレットマネジメントと
情報共有に対する最新アプローチの活用

グローバル情報セキュリティ調査2017
The Global State of Information Security® Survey 2017
Vol.2

pwc

目次



大半のビジネスリーダーは、異種混在のエンタープライズシステムにおけるサイバーセキュリティやプライバシーに関する脅威への対応を自らの責務だと認識している。しかし、リアルタイムのスレットインテリジェンスや情報共有プログラムを設計、実装、管理するためのノウハウは乏しい。

これは広く共通する課題だ。

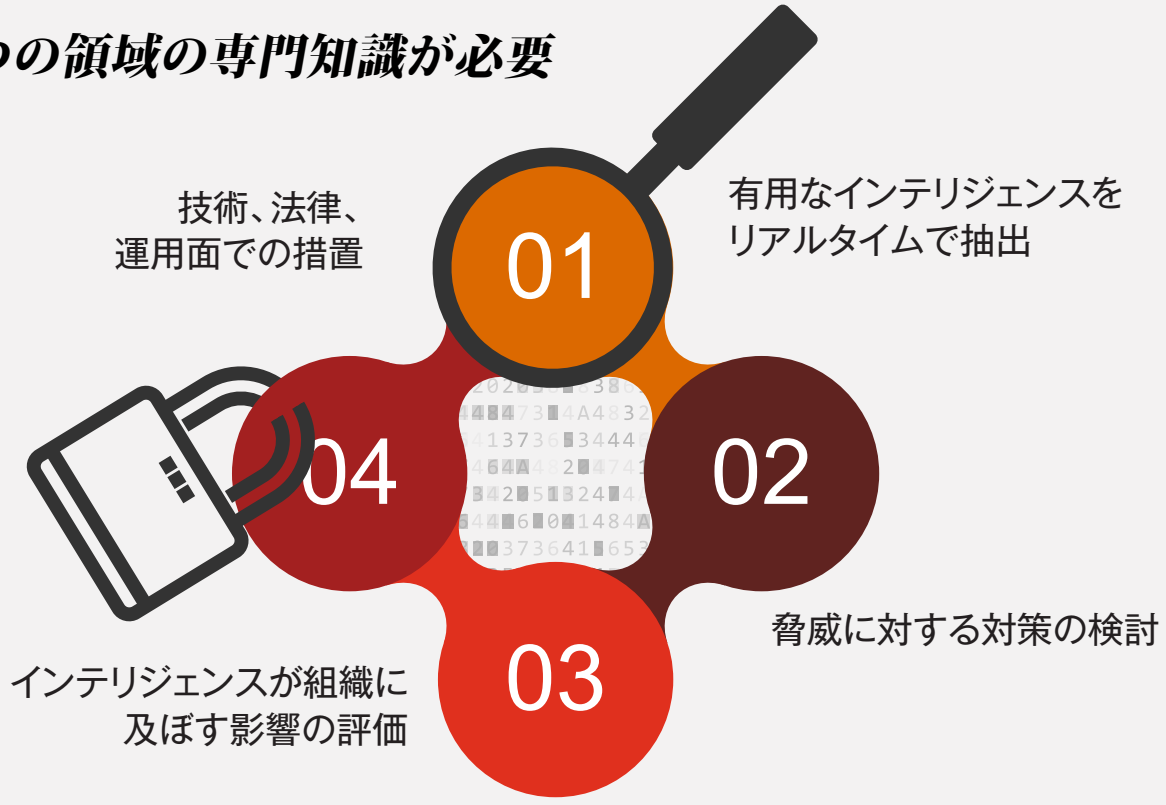
サイバーセキュリティに精通したエグゼクティブの間でも、統合スレットインテリジェンスや情報共有プラットフォームの認知度は低い。脅威を管理するには、チェスの名人に匹敵する高度な戦略的思考と分析能力が求められる。相互接続された複数システムを統合し、複数ソースから情報を取り込み、相関関係を整理して分析し、攻撃の状況を理解する必要がある。情報共有を自動化するためには、テクノロジーやデータ規格に関する膨大なノウハウと、相互接続されたプロセスが必要だ。

クラウドベースの監視および分析技術、相互運用可能な情報共有戦略やプラットフォーム、それに加えて考え抜かれたプロセス、これらのどれ一つとして欠かせない。これらを実現するために、次の四つの領域の専門知識を社内または社外から調達する必要がある。

- 情報を取り込み、有用なインテリジェンスをリアルタイムに抽出する。
- そのインテリジェンスが組織に及ぼす影響を評価する。
- 脅威を低減するための措置を検討する。
- 技術、法律、運用面での措置を速やかに取る。

この四つのスキルセットには、高い技術的専門知識とリソースを要する。そのため、サイバーセキュリティの深い専門知識の他、IT、法律、リスク、プライバシー、ビジネス部門からさまざまな人材を集めた多職種チームの構築が不可欠だ。このチームが、社内のシステム全体のアクティビティを統合するためのカスタムプロセスの開発を行う。

スレットマネジメントには四つの領域の専門知識が必要



スレットマネジメントプログラムの多くの変動要素を統合し、管理するには、クラウドコンピューティングサービスが不可欠であると考えられる。クラウドベースのモデルなら、あらゆるデジタルインタラクションを監視、分析し、リアルタイムで実用的なインテリジェンスを生み出すため、単一の情報リポジトリを作成することができる。

クラウド中心のソリューションが全ての企業に適しているわけではない。オンプレミスのスレットマネジメントソリューションを実装し、実行する選択肢もある。このアプローチには具体的な利点がいくつかある。例えば、オンプレミスのソリューションを所有していれば、システムを完全にカスタマイズして統合し、個々のビジネスニーズに対応することが可能だ。また、政府および各業界における法規制にも確実に準拠できる。データとアプリケーションが社内サーバーに保存されるため、サイバーセキュリティチームはデータの保存場所を常に把握できる。

ただし、オンプレミスのスレットマネジメントには、複雑な課題を伴い、大量の内部リソースを要するという欠点もある。最大の課題は、脅威に関する膨大な量の非構造化情報やプロセスを管理して効果的に活用する専門スキルを持つ人材の採用と維持だ。また、オンプレミスのソリューションでは、データを検証し、情報に基づいて即時対応するために、高度なスキルを持つスレットインテリジェンスアナリストを採用し、定着化させなければならない。さらに、内外の膨大な量のスレットインテリジェンスに合わせて、拡張可能なアジャイル型のテクノロジーエコシステムも必要だ。

オンプレミスでもクラウドでも、スレットマネジメントシステムの実装は、豊富なリソースを持つ企業であってもたやすいことではない。しかし、この取り組みを推進する企業は、脅威の予防的な監視、侵害の特定、インシデントへの迅速な対応、スレットインテリジェンスの共有に向けた準備態勢がより良い形で整うだろう。このような能力が、顧客データや企業資産、ブランドの保護に役立ち、ひいては競争優位性の獲得に繋がる。

インタラクティブタイムラインをご覧ください。
http://pwc.com/gsiss
***Connecting the dots*：A timeline of technologies, threads and regulations that redefined cybersecurity and privacy**

クラウドでの大胆な組み合わせ

スレットインテリジェンスおよび情報共有のためには、クラウドプラットフォームが、最新の脅威プログラムの作成、統合、アクセスのための一元的な基盤となる。

一元的なクラウドプラットフォームの能力と相互運用性を活用すれば、さまざまな相乗効果のあるスレットマネジメントテクノロジーをまとめることができる。さらに、クラウドアーキテクチャの本質的なシンプルさを生かし、堅牢性と拡張性を備えた新しい脅威検知機能を開発することができる。また、クラウドにより、データセキュリティを脅かすことなく、複数のソースからのアナリティクスを結合し、より安全な情報共有を実現することも可能になる。

先進テクノロジーとクラウドアーキテクチャの融合によって、企業は脅威を素早く識別して対応し、顧客やビジネスエコシステムについての理解を深め、最終的にはコストを削減することもできる。このモデルでは、例えば機械学習や人工知能による膨大な量のデータ集約と分析に加え、グローバルなスレットインテリジェンスデータベースと相関付け、リアルタイムで脅威を識別し、資産への影響を分析して対応の優先順位を決定することが可能となる。

48%

クラウドを通じて提供されているITサービスの割合

PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

クラウドベースのスレットマネジメントは、急速な進化を遂げており、それによってオンプレミスベースのサイバーセキュリティやプライバシー対策のモデルに変化をもたらしつつある。*「クラウドモデルが急速に普及しているのは、コストの優位性や処理能力、拡張性、そして迅速かつ柔軟にコンピューターリソースを調整できる点が評価されたからだ」*と、Christopher O'Hara（PwC米国 Co-leade、Cybersecurity&Privacy）は述べている。*「クラウドベースのサイバーセキュリティはこれからも進化し、あらゆるタイプの脅威データを取り込んで処理、正規化し、ビジネスへの影響をリアルタイムで把握することが可能になると考えている。これは、現在のオンプレミスのソリューションでは不可能なことだ」*

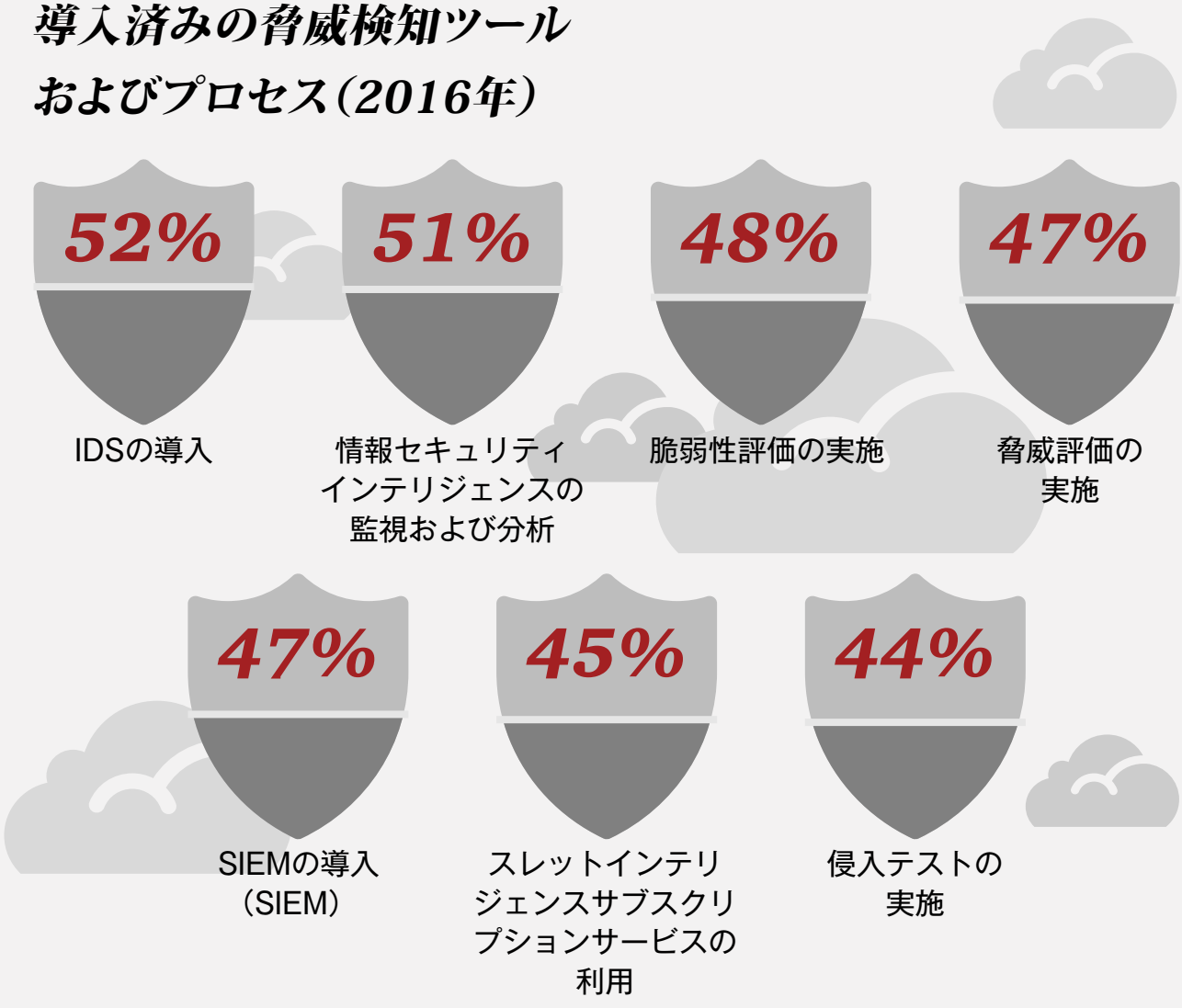
従来のオンプレミスシステムでは多くの場合、不十分なストレージ容量や処理能力、拡張性が制約となるからだ。そのため、サイバーセキュリティチームは、社内における調査やデータ分析ができず、調査作業に支障をきたし、誤検知が増加する。

クラウドにおけるスレットマネジメントツールの統合

多くの企業は、スレットインテリジェンスの収集や分析に不可欠なテクノロジーを積極的に導入し、また適宜更新している。従来のオンプレミスシステムよりもクラウドベースのマネージドセキュリティサービスを選ぶ傾向はますます強くなっている。

本調査の回答者の62％が、認証、IDおよびアクセス管理、リアルタイム監視、アナリティクス、スレットインテリジェンスの領域でマネージドセキュリティサービスを利用している。

導入済みの脅威検知ツールおよびプロセス（2016年）



出典：PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

予防的なスレットインテリジェンスにおいて、リアルタイムの監視およびアナリティクスよりも重要なものはない。本年の調査では、回答者の半分以上（51％）がリスクやインシデント検知のためにスレットインテリジェンスの積極的な監視および分析を行っていると答えた。

企業はこれまで、ログファイルやアクセス記録などの内部情報に重点を置いてきた。しかし近年、ベンダーが構築したシステムへの侵害が原因となった大規模な情報漏洩が続いたことから、外部ビジネスパートナーによるサイバーセキュリティとプライバシーに関する専門性が重要事項となった。

監視やアナリティクスの範囲の拡大に伴い、ソリューションにはリアルタイムの監視機能とアナリティクスプログラムには、生データを取り込んで解析を行う機能を備える必要が出てきた。脅威の状況を認識し、攻撃者の戦術、手法、手順を理解できるようにするためだ。アナリティクスとスレットインテリジェンスをクラウドで融合させれば、シームレスな相関付け、素早い検索、リアルタイムでの管理が可能となる社内全体で単一のデータソースを実現できる。

高度認証によるフィッシングの発見

近年、各業界のあらゆる規模の企業にとっての重要なリスクとして、フィッシングが現れた。フィッシングの手法は従来のソーシャルエンジニアリングに似ているが、近年ではさらに的を絞り、その有効性が高くなっている。サイバー犯罪者はフィッシングを巧妙に仕込み、ユーザーの認証情報を入手してから情報システムやデータへのアクセス権利を取得する。

本年はフィッシング被害を報告した回答者が38％に上り、サイバー攻撃の手法として最上位に挙がった。フィッシングによるインシデントの急増は、サイバー犯罪が高度なマルウェアによる攻撃から、既存の管理ツールや機能を悪用した「自力」型の攻撃へと変化していることを示している。

ユーザーの認証情報窃取に対抗するため、多くの企業がパスワードに代わって高度認証を導入している。生成・共有される消費者情報や企業情報が飛躍的に増加し、個人情報の保護が当然のこととして要求される中、この種の予防が重要なビジネス要件となった。

今日最も広く利用されている高度認証技術は、ハードウエアトークンおよびソフトウエアトークンだ。次いで多いのが指紋または虹彩スキャナーなどの生体認証である。ただし、来年の認証に関する最優先の支出項目として、スマートフォントークンが挙げられている。本年は回答者の28％がモバイルデバイスのセキュリティ侵害を報告しており、スマートフォンやタブレットの保護が念頭にあることは明らかだ。

*「私たちは消費者の認証を容易にする非常に興味深いイノベーションを目にしている」*とDavid Burg（PwC米国 Global Co-leader, Cybersecurity&Privacy）は述べている。*「消費者はモバイルデバイス上でアプリケーション認証を行うことができるようになり、以前と比較して簡単で安全になった」*

パスワードレス認証やアプリケーション認証を利用するためには、ID管理のアプローチを再考し、アクセスのリスクに応じた認証レベルを設定する必要がある。何よりも重要なのは、エンドユーザーにとって容易で直感的に理解できることだ。簡易アクセスがビジネスの成長にどれほどの潜在的影響を持つかは、“シェアードエコノミー”で採用されるIDおよびアクセス管理（IAM）を考えれば明らかだ。

*「タクシーを呼ぶのがこれほど簡単になる、あるいはこれほど手頃な料金で民泊できるようになると誰が考えただろうか？ これらは全て新しい体験であり、その成功を支えているのは顧客からは見えないトランザクションだ」*とDavid Clarke（PwC、Digital Services and Experience Center Leader）は語る。*「新しい体験と新しいサイバーセキュリティの考え方は共存関係にある。速やかに進めるには、発案時点で多様な人材を集めることが極めて重要だ」*

認証技術は製品の展開ペースを加速させるだけではなく、データセキュリティ全体も強化する。本年の調査結果によると、高度認証を採用している企業の46％が、テクノロジーによってオンライントランザクションの安全性が高まったと回答している。また、認証技術の効果として、セキュリティおよびプライバシーへの消費者の信頼度の向上のほか、顧客体験の改善、ブランドの保護も挙げられている。

60%

マネージドセキュリティサービスを利用している企業のうち、IDおよびアクセス管理をサービスプロバイダーに依頼している回答者の割合

PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

セキュリティの境界が消え、IDが個人からインターネットに接続されたデバイスへと広がる現在、アクセス保護と侵入防止のためのIAMツールの重要性はかつてないほど高まっている。

*「この2年間、ほとんどのインシデントがIDに関連している」*とRichard Kneeley（PwC米国、Cybersecurity and Privacy Managind Director）は指摘する。*「これらのインシデントの多くは、不正侵入したIDを利用してアクセス権を取得し、ネットワーク内部に入り込んでIDを変更し、特権アカウントを乗っ取ってデータやシステムへのアクセス権を引き上げ、ネットワークやシステム、データへ制限のないアクセス権を取得するという手法を用いている」*

近年、IAMソリューションを導入した企業の数は50％前後にとどまっているが、クラウドベースのIDサービスを採用するトレンドが見られる。マネージドセキュリティサービスを利用している企業のうち60％が、IAMプログラムへの対応をサービスプロバイダーに依頼していると答えている。その理由としては、一般的にクライアントにとってIAMシステムの運用に必要なスキルの確保や維持が困難であることが大きい。クラウドを利用したIAMには、トレーニングを受けたオペレーターや、サービスを運用するエンジニアが含まれることが多い。

もう一つのトレンドは、アダプティブ（適応型）認証だ。ITシステムに取り込まれる情報の増加を受け、企業は不審な行動やパターンを識別するためのデータポイントを増やし始めている。アダプティブ認証では、ユーザーのログイン時刻や場所、アクセスパターン、デバイスタイプなどのデータに基づき、リスクベースでアクセスを判定する。アプリケーションがログイン試行中に異常なアクティビティを検知した場合、追加の認証ステップを設けたり、プロセスを停止したりすることができる。

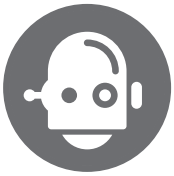
アダプティブ認証のための既存ソリューションはない。リスクプロファイルを作成するために、SIEMなどの既存ツールを組み合わせて使用する。*「優れたセキュリティツールを整備していなければ、アダプティブ認証を実装することはできない。アダプティブ認証は、セキュリティシステムや生成されるデータに依存するからだ。アダプティブ認証により、IDが新たなレベルに達するとともに、既存テクノロジーから付加価値を引き出すこともできる。CISOにとっては、『100万米ドルで一つの問題を解決しただけではなく、これまでの投資からより大きな価値を引き出した』と宣伝できる絶好の機会だ」*とKneeleyは述べている。

先進的な企業はアダプティブ認証の手法と人工知能（AI）、機械学習を組み合わせ、予測認証メカニズムの開発に取りかかっている。予測変数を使用することで、認証は特定のアクセス試行に伴うリスクに結び付けられた継続的イベントになる。そうなれば、顧客体験が大幅に向上するとともに、セキュリティレベルや信頼度も向上する。

回答者の23％が今後12カ月で人工知能や機械学習への投資を計画しているのも当然だろう。これらのテクノロジーが以前はSFと見なされていたことを考えれば、これは大胆な動きだ。

23％

本年、人工知能や機械学習への投資を計画している回答者の割合



PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

クラウドベースのスレットインテリジェンスの概要

スレットインテリジェンスと情報共有を併せ持つクラウドプラットフォームの導入に成功した企業はまだほとんど存在しない。その一因は、これらを構成するテクノロジーの歴史がまだ浅いことにある。しかし、オンプレミスで社内全体のスレットマネジメントを推進しようとすれば、複雑さを極め、テクノロジー面でもリソース面でもたちまち限界に達しかねない。

クラウドベースのテクノロジーは徐々に成熟し、新たなレベルのサービスを提供できるようになり、状況は変化し始めている。*「本年、私たちは、関連付けられていない膨大な量の情報を取り込み、それらを関連付けて意味を見いだすテクノロジーの活用方法を見つけ出した」*と*Burg*は述べている。

PwCは進化するテクノロジーを生かし、Secure Terrain™という新しいクラウドベースのサイバーセキュリティソリューションを設計、開発した。Secure Terrain™はGoogle Cloud Platformを利用して社内全体のアクティビティの精査を可能にし、戦略的なサイバーセキュリティリスクの管理と重要資産の保護を容易にする。

この一元的なソリューションでは、拡張可能な機械学習手法とエンタープライズクラスのクラウドテクノロジーを活用し、構造化データ、非構造化データ両方を含む、膨大な量のデータを集約、迅速な分析を行う。このデータをスレットインテリジェンスの大規模グローバルデータベースと相関付け、リアルタイムで脅威を識別し、ビジネスへの影響に基づいて対応の優先順位を決定する。Secure Terrain™ソリューションを支えるのは、PwCのグローバルなTerrain Operations Center（TOC）だ。TOCはアラートを出すにとどまらず、ハントチームによる分析、脅威の調査、復旧などを含むセキュリティ監視およびサポートも提供する。

また、PwCは別の面の課題にも対応している。Terrain Intelligenceは、スレットインテリジェンスのソースを1カ所にまとめて検索できる、統合スレットインテリジェンス共有プラットフォームだ。Googleのデータセンターと高速でグローバルなファイバーネットワークを利用することで、不正アクセスの兆候をほぼ瞬時に分析、相関付けすることができる。サイバーセキュリティインシデントの管理では、このスピードが極めて大きな優位性となる。

一元的なプラットフォームの威力

サービスプロバイダーは、クラウドモデルのアーキテクチャや運用面での優位性により、優れた一元的なスレットマネジメントと情報共有を提供できる。

統合クラウドソリューションは、オープンデータやクローズドデータ、脅威指標の商用ソースを取り込んで分析するために必要な処理能力とストレージを備えている。また、社内全体のネットワークとユーザーデータに不審なアクティビティがないかどうかを監視し、潜在的危険性を持つ未知の異常を検知する処理能力もある。

最大の価値を得るには、実用的なスレットインテリジェンスが不可欠だ。つまり、優先順位が適切に設定され、正確でビジネスに有用な情報をリアルタイムで入手できる必要がある。実用的なインテリジェンスの共有は、個々の企業の防御を強化、ひいては業界、同業者、地域といったエコシステム全体の防御の向上に繋がる。

脅威を検知すると、スレットマネジメントシステムはビジネスの状況に沿って対応の優先順位を設定し、最も影響を受ける部分への迅速な支援を図る。そのために必要なのは、資産台帳、機密データの形式とインフラストラクチャなどの関連情報のデータベースだ。このデータベースを使用して、脅威のフィルタリング、優先順位の設定、状況の分析を知的に行う。

リアルタイムのスレットマネジメントの複雑さとスコープに対応するには、TOCの専門技術が求められる。TOCはクラウドを活用した高度な分析手法でサイバーリスクを素早く察知できる。TOCチームはリアルタイムの監視を24時間365日実施するとともに、過去のセキュリティデータに対する的を絞った調査および分析も行う。

スレットインテリジェンスソリューションの設計と導入を終えた後は、多くの場合、システムの運用と継続的な改善が課題となる。デジタルエコシステムの監視、インシデント対応、スレットインテリジェンスの共有のため、マネージドセキュリティサービスを利用する企業はますます増えている。

マネージドセキュリティサービスは、さらに二つの継続的な課題への対応にも役立つ。熟練したサイバーセキュリティ人材の世界的な不足、そして慢性的な予算の制約だ。特にサイバーセキュリティの人材不足から、セキュリティプログラムの一部または全部をサードパーティーに委託する傾向に拍車がかかる可能性が高い。

また、マネージドセキュリティサービスの投資対効果の検討にも変化が生じそうだ。*「社内の人材と低コストの定型マネージドサービスの違いに注目したマーケットがあると考えている」とO'Haraは言う。「ビジネスに付加価値を提供し、企業においてフルタイムで雇うのが難しい高額な給与を必要とする人材を利用することに匹敵する新しいマネージドサービスのモデルが見込まれる」*

つまり、マネージドセキュリティサービスは、サイバーセキュリティおよびプライバシープログラムの運用方法を再定義するアウトソーシングモデルだと言える。

情報共有リソースのネットワーク

現時点で確かなことが一つある。サイバー犯罪者の間では、技術知識やツール、方法がうまく共有されているということだ。

ますます巧妙化するサイバー脅威に対抗しようと、多くの企業が敵を見習い始めている。同業者や業界団体、政府機関と重要なスレットインテリジェンスを共有し、協調してサイバーセキュリティの能力向上に取り組んでいる。

*「2016年に入ってから情報共有プログラムが本格的に広がり始めた」*とBurgは述べる。*「さまざまな企業や組織、州や地域組織、先進的な業界団体が集まってスレットインテリジェンスを共有し、ともに問題を解決しようと異例の取り組みを行っている」*

サイバー犯罪に対して統一戦線を張ることには、多くの利点がある。協力と情報共有により、最も関連性のあるリスクを具体的に把握した上で攻撃者の意図と戦術を理解し、最も効果的な対応方法を知ることができるのだ。

このような利点を得るには、情報共有プラットフォームでのアクティビティの分析、脅威の分類と検証、リアルタイムでのアラート発信が必要だ。前述のように、情報は実用的でなければならない。情報共有プラットフォームでは、脅威が企業固有の環境にどのような影響を及ぼすのか、正確かつ状況に沿った情報を提供する必要がある。

55%

セキュリティ強化とリスク低減のため、外部のパートナーと協力している回答者の割合

PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

複数の異なるシステム、データタイプ、企業との相互運用性を目指す新しいプラットフォームには、克服すべき課題も多い。最大の課題は、情報共有のために統一されたフレームワーク、プラットフォーム、データ規格がないことだ。先進のサイバーセキュリティ運用を行っている一部の企業では、情報共有プラットフォームが実装されているものの、ほとんどが政府機関や同業者との相互運用性の実現には至っていない。

データ量が膨大で扱いにくいため、二の足を踏んでいる可能性がある。*「ほとんどの企業は、流入するデータの量が膨大すぎて処理しきれないままだ」*と*Grant Waterfall*（*PwC米国、Cybersecurity and Privacy Global Co-Leader*）は言う。*「そのような企業では、データ集約と誤検知の除外のため、スレットフュージョンセンターとアドバンスドセキュリティオペレーションセンターが極めて重要だ」*

本年の調査では、回答者の55％がサイバーセキュリティの向上のために他社との協力や情報共有を行っていると答えた。このような回答者は、同業者や既存のセキュリティ情報共有組織（ISAC）から実用的な情報を入手したと述べている。

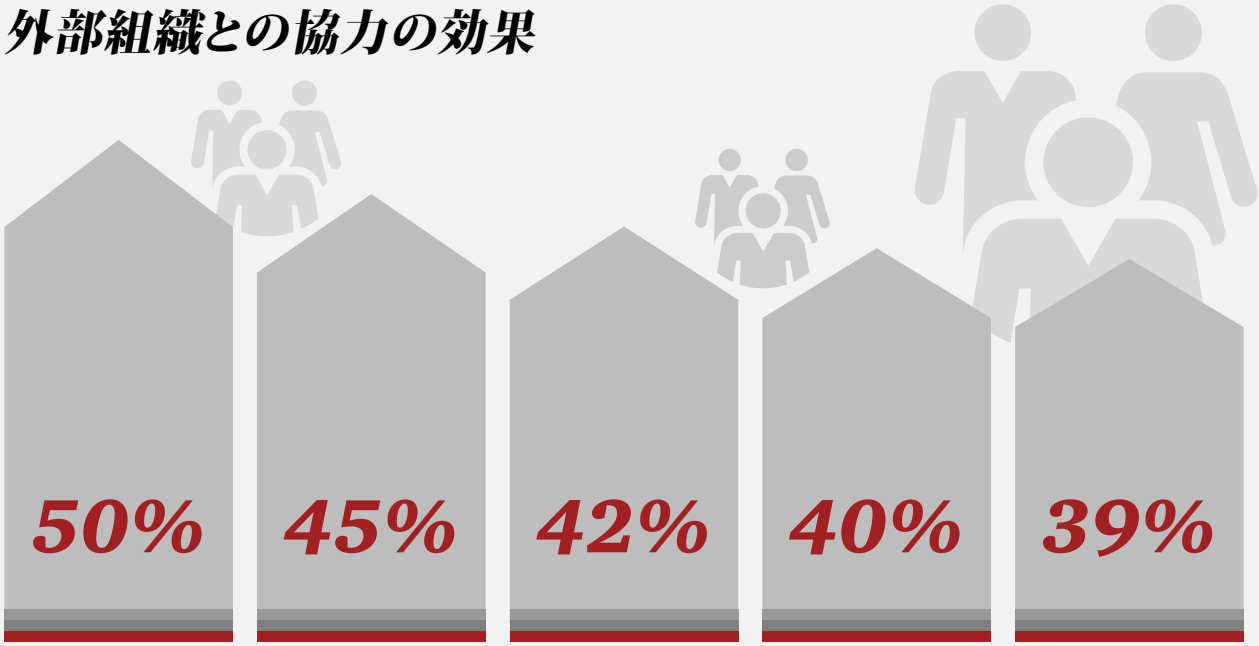
サイバーセキュリティのための新たな情報共有分析機関（ISAO）はこれまでとは違って企業間および公共機関とのスレットインテリジェンスの共有を目指しており、大いに期待できる。ISAOはバラク・オバマ元米大統領が組織の創

設を促すために発令した大統領令13691号（*官民のサイバーセキュリティ情報共有の推進*）により、2015年2月に発足した[1]。

発足以来、バージニア州ISAO（22ページを参照）、法律事務ISAO、小売業界ISAO、全国信用組合ISAO、海事および港湾保安情報共有分析組織など官民の多くの組織がISAOに参加（または参加を表明）している[2]。

1 Whitehouse.gov、大統領令13691号（官民のサイバーセキュリティ情報共有の推進）、2015年2月13日
2 The ISAO Standards Organization、Information Sharing Groups、2016年10月18日アクセス

外部組織との協力の効果



同業者と共有する（受け取る）実用的な情報の増加

ISACと共有する（受け取る）実用的な情報の増加

スレットインテリジェンスおよび認識の向上

ISAOと共有する（受け取る）実用的な情報の増加

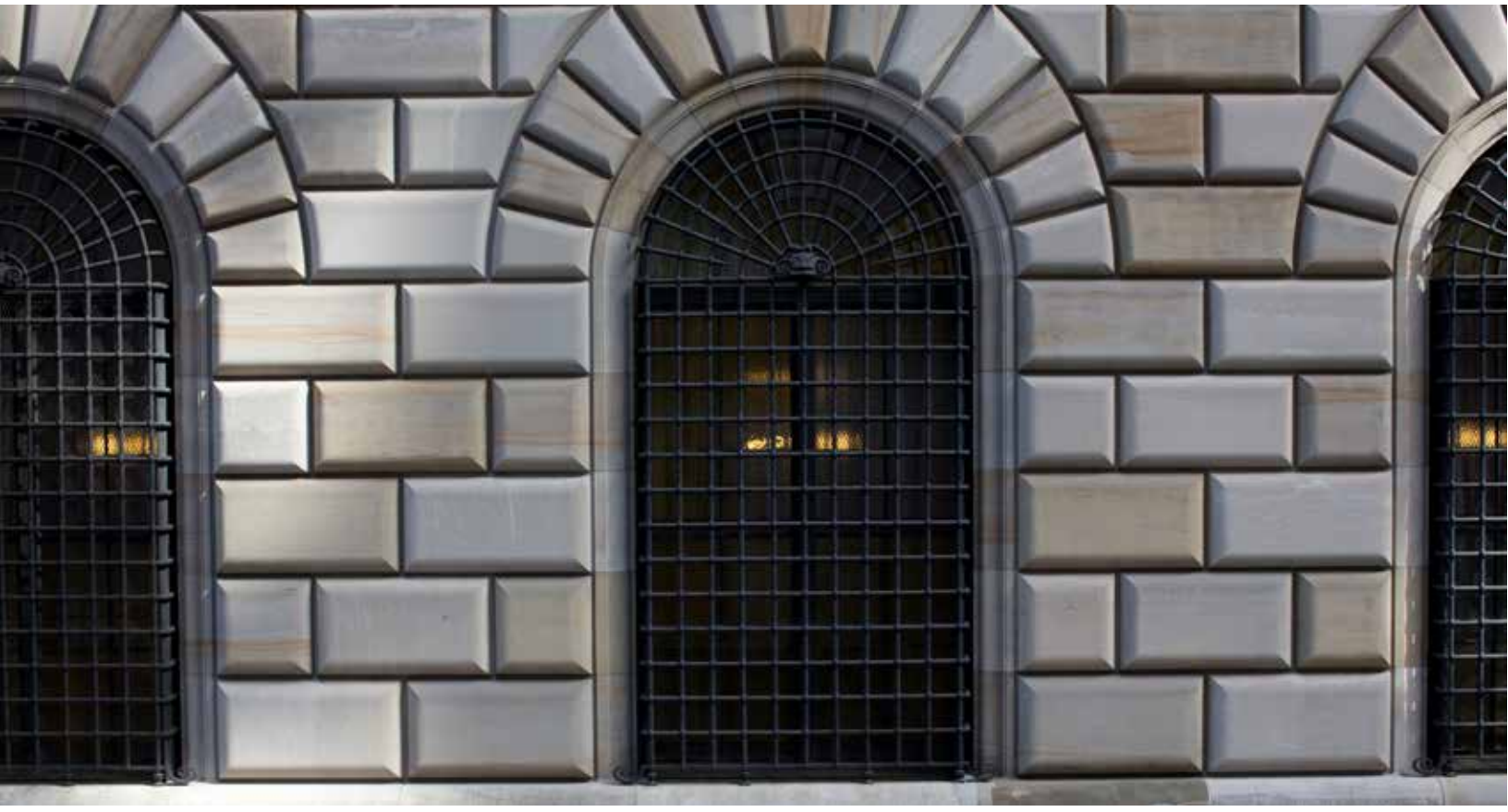
政府組織と共有する（受け取る）実用的な情報の増加

出典：PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

また、欧州連合は先頃、並行する目標を掲げた、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。この指令は、2016年7月に採択され、加盟国に対してコンピューター・セキュリティ・インシデント・レスポンス・チーム（CSIRT）の構築を義務付けた。また、重要インフラに携わる企業に対してはサイバーセキュリティインシデント発生時の国内当局への通知を義務付けた。さらに、企業にはリスク情報の共有を促すための協力団体の設立を求めている[3]。

英国では、四つの銀行がUK National Cyber Crime Unitと協力する官民組織、Cyber Defense Allianceを設立した。銀行がスレットインテリジェンスや対応方法についての情報を適時に交換できるようにするためだ。そのうち1行は、シンガポールにあるインターポール（国際刑事警察機構）のサイバーセキュリティ調査ユニットにアナリストを派遣している[4]。

3 European Commission、The Directive on security of network and information systems (NIS Directive)、2016年10月17日アクセス
4 Bloomberg、Nothing Brings Banks Together Like a Good Hack、2016年10月18日



ISAOによる情報共有の強化

ISAOの設立を機に、企業各社は、連携して脅威環境をより的確に理解し、より豊富な情報に基づいて重要なサイバーリスクに対応するための投資を行い、セキュリティ管理策を素早く調整して新しい脅威に対応できるようになる。サイバーセキュリティの強化はハッカーの活動を阻み、経済全体に恩恵をもたらす。ISAO固有の強力なサイバーセキュリティ情報共有モデルには、次のような潜在的な利点がある。

- 信頼できるネットワークを構築し、個々の企業がサイバーリスクを識別し低減する能力を大幅に強化する
- 実用的なスレットインテリジェンスを迅速に提供し、測定可能なサイバーセキュリティの改善を支援する
- サイバーセキュリティの情報共有にかかるコストを削減し、参加障壁を低減する
- サイバーセキュリティに関する情報の管理、分析、インテリジェンスを強化、簡素化する
- 特定の賠償責任、独占禁止法違反訴訟、規制執行訴訟からの法的保護の条件を満たす
- セキュリティ侵害に関する経営幹部の説明責任の強化に伴い、規制当局から期待されるサイバーリスク低減策に十分に取り組めるようにする
- 情報共有のビジネスモデルを変革し、規模の経済を拡大する

最近、民間企業ではISAO自主ガイドラインが策定されている。これが産業界および政府機関におけるサイバーリスク管理の変革の契機となる可能性がある。PwCを含む業界関係者が立案した新ガイドラインでは、取締役会および経営幹部向けに、ISAOの構築を成功させるための具体的な助言を提供している。このガイドラインは4部で構成されている。

- ISAO 100-1:Introduction to ISAOs
- ISAO 100-2:Guidelines for Establishing an ISAO
- ISAO 300-1:Introduction to Information Sharing
- ISAO 600-2:US Government Relations, Programs and Services

最先端のサイバーセキュリティへの取り組み事例

2015年4月、バージニア州は米国でいち早く州レベルのISAO設立を発表した[5]。セキュリティ強化のためスレットインテリジェンスの共有を促進する米NISTサイバーセキュリティフレームワークの実装が最も早かったのも同州だ[6]。

最近では、コネクテッドカーへのサイバー攻撃の可能性に対応するために、バージニア州警察とともに官民のワーキンググループを設けた[7]。このワーキンググループは、連邦および州政府機関、学術機関、サイバーセキュリティ民間企業などの関係者で構成されている。自動車やその他の消費者向けデバイスへのサイバー攻撃をいかに検知し防止するかについて、当局者の理解を助けることを目的としている。

また、バージニア州は、サイバーセキュリティ・ソリューション・プロバイダーが提供するスレットインテリジェンスソリューションの実装も率先して行っている。同州は、住民の出生および死亡記録、確定申告、健康情報など、膨大な量の個人識別情報(PII)を保有している。同州当局者は昨年、フィッシング攻撃や従業員によるインシデントの増加に気付いた。これらのリスクを低減するために、バージニア州はインバウンドおよびアウトバウンドのトラフィックに不審なアクティビティやマルウェアがないかどうかを監視できるようにするスレットインテリジェンスソリューションを実装した。また、このソリューションにより、セキュリティアナリストは高度なマルウェア、ゼロデイ攻撃、標的型攻撃(ATP)を安全な方法で実行し、調査することができる。

悪意ある攻撃者に対する統一戦線は、同州の標語である「暴君は常にかくのごとし」[8]をこれまでにも増してふさわしいものとしている。

5 Virginia.gov、Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats、2015年4月20日
6 Virginia.gov、Commonwealth of Virginia Cyber Security Commission: Threats and Opportunities、2015年8月
7 Virginia.gov、Governor McAuliffe Announces Initiative to Protect Against Cybersecurity Threats、2015年5月15日
8 ブルトゥスがカエサル暗殺の際に語ったと言われる言葉。民主主義を象徴する言葉として用いられ、米国バージニア州のおける標語となっている

スレットインテリジェンスの未来へ

10年前、スレットインテリジェンスは後手後手の防止策と既知の脅威の分析に限られていた。ゆえに、未知の脅威があふれていたことになる。2008年のグローバル情報セキュリティ調査（GSISS）では、セキュリティインシデントを検知した回答者のうち、発生源を不明とした回答は42％を占めていた。近年、この数値は10％未満に低下している。

今日、動的なスレットインテリジェンスと情報共有を実現する企業が増加し、サイバーセキュリティおよびプライバシー対策は事後対応から予防へと移行した。個々の脅威をより的確に把握すること、そして官民でその情報を共有することがビジネス優位性と顧客の信頼の獲得に繋がるという理解が浸透している。

近い未来、スレットインテリジェンスをリアルタイムで取り込み、比較できるようにするテクノロジーが急速に進化するとO'Haraは見ている。*「これには、機械学習、人工知能、ビッグデータ分析などのテクノロジーが含まれる。将来は、スレットインテリジェンスやセキュリティインシデント管理にデータサイエンスを応用するようになるだろうと考えている」*

これは、スレットインテリジェンスの予防力が高まり、発生前にインシデントを阻止できるようになるということだ。IoTの普及とともに、消費者情報の保護も促進される。

情報共有について、新しいタイプの協力組織を通じ、スレットインテリジェンスの配信、個々の会員に合わせた情報提供に向けて、より包括的なアプローチが実現できるだろう。実用的な情報を入手できる環境の整備は、企業、政府、個人のセキュリティの継続的な向上に繋がっている。

日本企業への示唆

本セクションは、The Global State of Information Security® Survey 2017にご協力いただいた日本企業205社のデータを、PwC Japanグループが独自に分析し、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:スレットインテリジェンスの自動適用化の推進

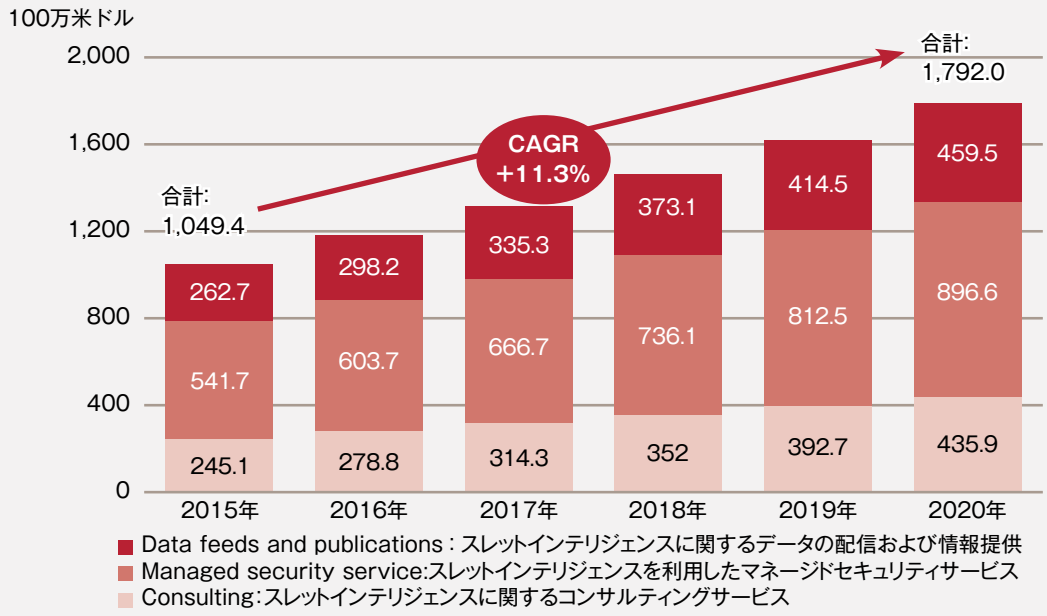
～スレットインテリジェンスとは～

スレットインテリジェンスとは、サイバー空間における攻撃や脅威などに関する情報を分析して得られる知識のことである。社内にSOC(セキュリティ・オペレーション・センター)の機能を有する企業であっても、仮に、その監視対象が社内で発生したログやイベントのみの場合、それらがどのような意味を持つのか、正確に分析することは難しい。

一方で、世界中のサイバー空間で発生した事象を取りまとめたスレットインテリジェンスを有効に活用すれば、世の中で起きているサイバー攻撃のトレンドや効果的な予防方法をほぼリアルタイムで知ることができる。そのため、自社に攻撃が来襲する前に「準備」が可能になるのだ。ゼロデイ攻撃のような未知の脆弱性を狙った攻撃を早急に検知することも可能になる。

今後、スレットインテリジェンスに関連する市場は、2020年までに年平均成長率(CAGR)11%で拡大する見込みであり、大きな注目を集めている(図1)。

図1:スレットインテリジェンスに関連する領域別収益予測(グローバル)



出典:IDC Dec 2016 "Worldwide Threat Intelligence Security Services Forecast, 2016-2020:Strength in Numbers" (US41053415)

～日本企業はスレットインテリジェンスの活用の余地が大きい～

スレットインテリジェンスの提供方法の一つとして、「サブスクリプションサービス」というものがある。メールマガジンなどで脅威情報などを配信するものである。今回の調査では、サブスクリプションサービスを利用する企業の比率は、グローバルよりも日本の方が高いことが分かった（図2）。しかし、受け取っているスレットインテリジェンスを有益と感じている企業の比率は、日本の方が圧倒的に低い（図3）。

その理由として、日本企業の多くは、単純にメール配信を受けるにとどまっていることが考えられる。本来であれば、受信したメールの内容を分析し、自社にどのような影響があり、どのように対処すべきかを判断し、具体策な対策を講じることまでが求められるのだが、そこまでは活用されていないのが実態のようだ。

図2：サブスクリプションサービスを利用している企業の割合

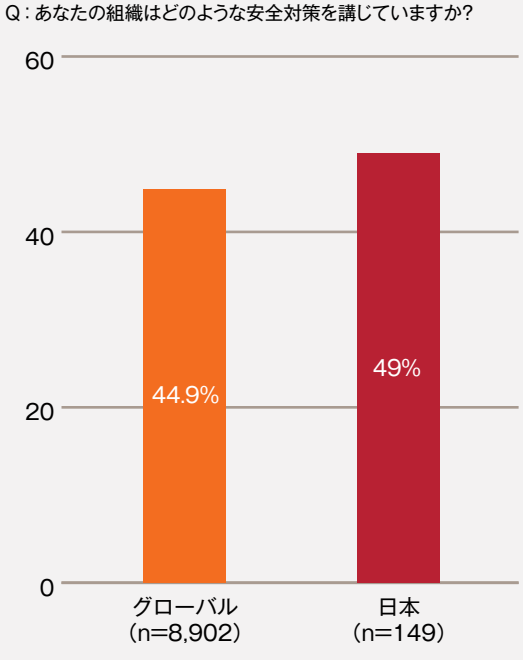
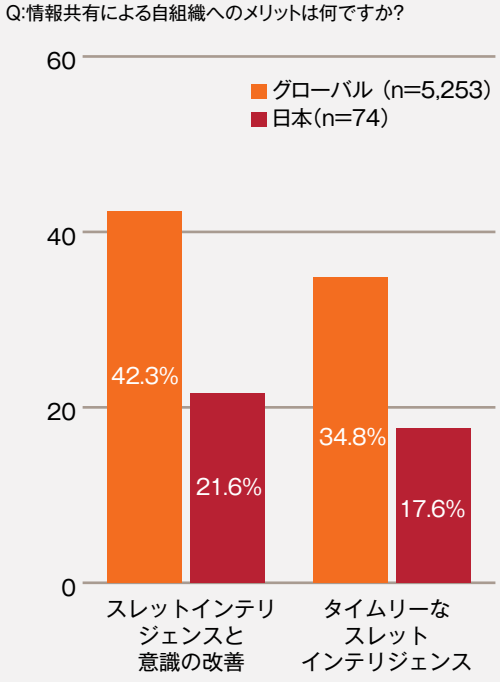


図3：スレットインテリジェンスをメリットと考えている企業の割合

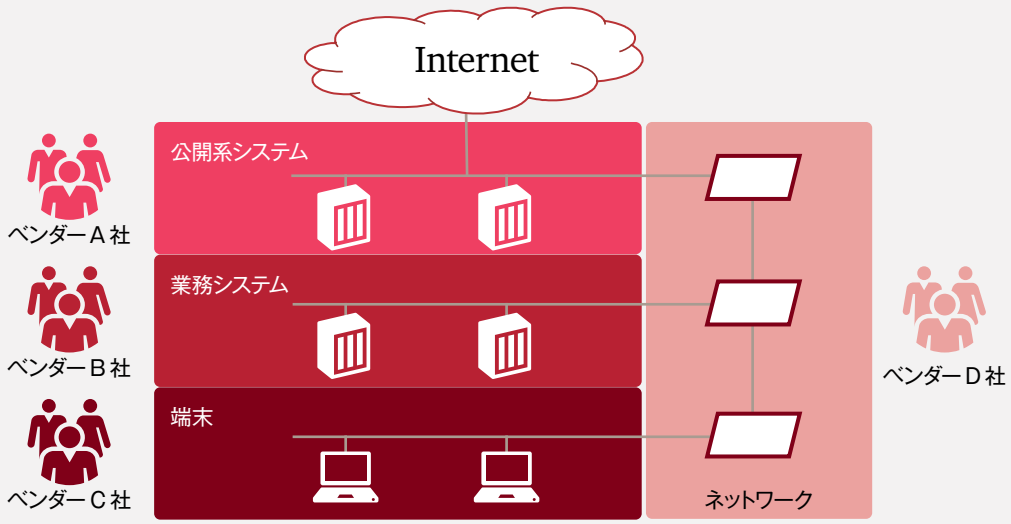


～スレットインテリジェンスの活用を妨げる独自の商習慣～

日本企業においてスレットインテリジェンスの活用が進まない背景には、日本特有の商習慣があると考えられる。日本企業の多くでは、セキュリティ管理を含むシステム運用をさまざまなベンダーに委託しており、極度に外部依存度が高い。

複数のベンダーが開発した複数のシステムを複数のベンダーが運用している状況は、言うまでもなく複雑性が高い。そのため、入手したスレットインテリジェンスを、どこにどのように適用すべきかを判断することが難しい。安易にシステム設定を変更してしまえば、複雑に相互依存するシステムのどこかで、予想もしなかった不具合が発生するかもしれない。システム資産管理やコンフィギュレーション管理、システム間データ連携などの相互依存性管理など、全システムを俯瞰した状況の把握が不可欠である。

図4：日本企業における情報システム構造の例



～スレットインテリジェンスの自動適用化を推進すべし～

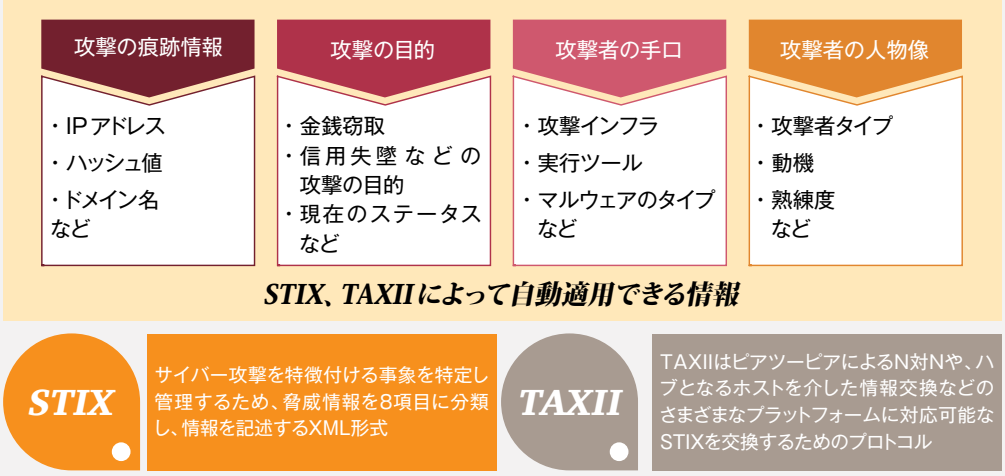
ますます巧妙化する昨今のサイバー攻撃に備えるためには、配信されたスレットインテリジェンスを担当者が読み取り手作業で対策を講じるのではなく、IPアドレスやファイルのハッシュ値など、攻撃の痕跡情報を「自動的に」セキュリティ機器に取り込む対策が効果的である。これまで、標的型攻撃の多くは、情報漏洩など、目に見える被害もしくはそれに準ずる自社システムの変化によって検知されてきた。つまり、それは攻撃や甚大な被害が発生した後である。ビジネス上の影響が出る前に手を打つには、スレットインテリジェンスの自動適用を推進することが有効である。

複数の外部ベンダーを利用している日本企業こそ、攻撃の痕跡情報などの新たなスレットインテリジェンスを入手した際に、その情報をできる限り早く、かつ、多くの関係者に共有する仕組みが必要である。それを実現する最適な手法が、統一的な情報の形式化および自動化である。

スレットインテリジェンスのセキュアな自動転送を実現する技術仕様として、「スティックス（STIX：Structured Threat Information Expression）」や「タクシー（TAXII：Trusted Automated Exchange of Indicator Information）」というものがある。これらは、オープンコミュニティによる無料で活用可能な技術仕様であり、攻撃の痕跡情報の他、攻撃者の目的、手口、人物像までデータに記載することが可能である。セキュリティアプライアンス製品やSIEM[1]などのセキュリティ機器にスレットインテリジェンスを自動的に取り込み（「データフィード」と呼ばれる）、ログ情報などと突合させることで、企業の担当者がマニュアルで判断せずとも迅速な対応が可能になる。

1 SIEM（Security Infomation and Event Management）
セキュリティに関するログ収集や分析を行うシステム

図5：STIXやTAXIIによって自動適用できる情報



示唆②：情報共有の推進

～情報共有は依然として進んでいない～

サイバー攻撃の手口は年々複雑化している。ここまでくると、もはや企業が一社単位で対抗できる限界を超えている。攻撃者に打ち勝つには、企業の垣根を越えた協力体制の構築が必要なのだ。

米国では、業界ごとに脅威や脆弱性に関する情報の共有・分析を行うISAC（Information Sharing and Analysis Center）が数多く設立されている。EUにおいては、金融機関同士の情報共有のためEuropean FI-ISAC（欧州金融業界情報共有分析センター）が設置されている。英国には官民が連携したCyber-security Information Sharing Partnership（CiSP）（サイバーセキュリティ情報共有パートナーシップ）があり、ドイツでは業種が異なる主要な企業から構成されるCyber Security Sharing and Analytics（CSSA）（サイバーセキュリティ情報共有分析）が設置されるなど、さまざまな形で情報共有が進んでいる。

今回の調査から、日本企業における情報共有の取り組みは、グローバルに後れを取っていることが判明したが（図8）、日本でも同様の動きが見られる。金融ISACの正会員数は2017年6月時点で315組織に達しており、ワークショップやサイバー攻撃を想定した合同演習などが積極的に開催されている。情報通信業界では、2016年3月にTelecom-ISACが参加組織の範囲を拡大してICT ISACに生まれ変わった。今後のさらなる脅威に対抗するため、大手放送事業者やセキュリティベンダーも加えた格好である（図6）。電気事業分野においても、2016年に電力ISACが組織化された。大手電力会社に加え、電力小売自由化の機会に市場に参入したガス会社や鉄鋼関連会社もメンバーに加わっている。さらに、業界の枠を超えたCSIRT同士による緊密な連携も活発になってきている。日本CSIRT協議会の会員数は、年々増加し現在では200を超えるチームが参加するまでになった（図7）。

図6：近年の日本におけるISACの活動

金融ISAC	ICT ISAC
・正会員向けワークショップの開催（2016年）	・Telecom ISACからICT ISACに組織変更（2016年）
・金融ISACアニュアルカンファレンスの開催（2016年）	・The first International Workshop on ISAC Collaboration 2016 in Tokyoの開催（2016年）
・会員合同演習「Fire 2016」の実施（2016年）	

出典：一般社団法人金融ISAC　http://www.f-isac.jp/
一般社団法人ICT-ISAC　https://www.ict-isac.jp/

図7：日本CSIRT協議会の会員数の推移

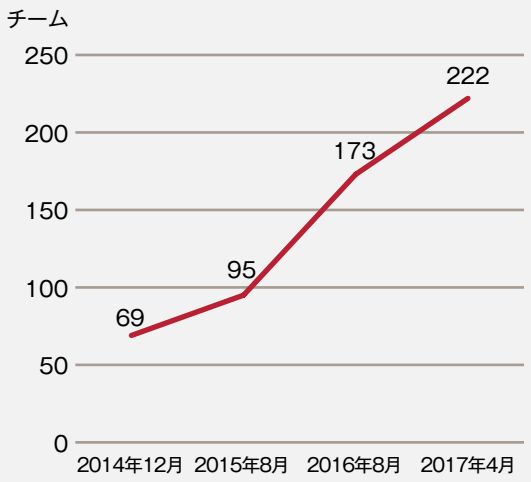
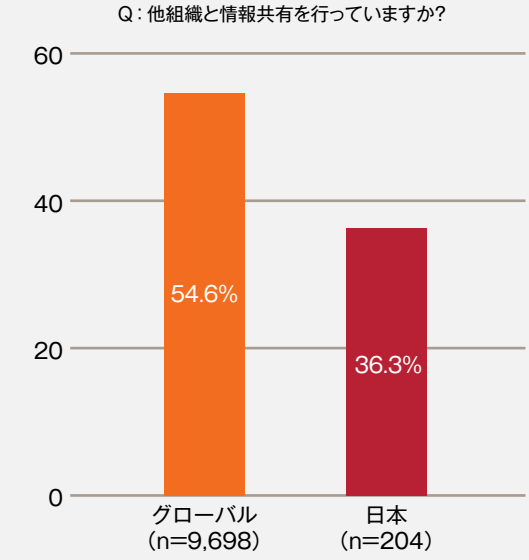


図8：情報共有を実施している企業の割合

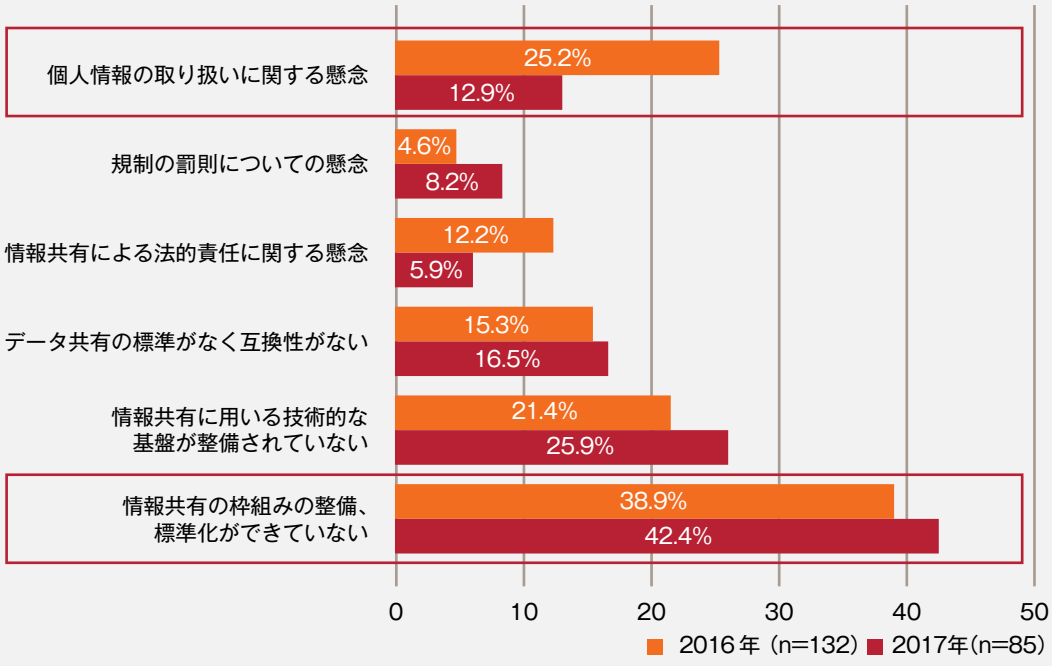


～枠組みが整備されない限り情報共有は進まない～

日本企業が他の企業と積極的に情報共有を行わないのはなぜか。本調査では「個人情報の取り扱いに対する懸念」を理由に挙げた日本企業の割合が、昨年の25.2%から今年は12.9%と大幅に減少した（図9）。

その一方で、昨年同様、「情報共有の枠組みの整備、標準化ができていない」と回答した企業が多数あった。逆説的な見方をすれば、情報共有組織が新設されたり、既存の業界団体を受け皿にした枠組みさえ整備されれば、情報共有が加速する可能性もある。

図9：他組織と情報共有を行わない理由



～情報共有組織設立の後れ～

日本の産業界では、米国と比較するとISACの設立が進んでいない。米国では、2003年にISAC間の相互連携を確立する目的で National Council of ISACs（NCI）が設立され、2016年6月時点では、21業種のISACが加盟している。米国に存在するISACと日本で設立されているISACを比較すると、対応業種数の違いがよく分かる（図10）。

なお、日本では、政府が官民の緊密な連携を目的として、重要インフラ分野[2]13業種における情報共有の枠組みを構築しているが、本調査における日本企業の回答から推測すると、十分に情報共有が行われていると言い切れない。

2 サイバーセキュリティ戦略本部重要インフラの情報セキュリティ対策に係る第3次行動計画を参照のこと

図10：日本と米国における重要インフラ分野におけるISACの比較（2016年6月時点）

米国におけるISAC※	分野	日本におけるISAC
FINANCIAL SERVICES ISAC	金融	金融ISAC
	クレジット	
COMMUNICATIONS ISAC	情報通信	ICT　ISAC
INFORMATION TECHNOLOGY ISAC		
NATIONAL HEALTH ISAC	医療	未設立
HEALTHCARE READY		
WATER ISAC	水道	
MARITIME　ISAC　※海運	物流	
SUPPLY CHAIN ISAC		
AVIATION ISAC	航空	
SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION AND OVER-THE-ROAD BUS ISAC	鉄道	
MULTI-STATE ISAC	政府・行政	
ELECTRICITY ISAC	電力	電力ISAC
CHEMICAL SECTOR ISAC（現在は活動実態なし）	化学	未設立
DOWNSTREAM NATURAL GAS ISAC	ガス	
OIL & NATURAL GAS ISAC	石油	
AUTOMOTIVE ISAC	自動車	日本自動車工業会内にワーキンググループあり
REAL ESTATE ISAC	不動産	未設立
RESEARCH AND EDUCATION NETWORK ISAC	教育	
RETAIL CYBER INTELLIGENCE SHARING CENTER	小売	
DEFENSE INDUSTRIAL BASE ISAC	防衛	
DEFENSE SECURITY INFORMATION EXCHANGE		
EMERGENCY MANAGEMENT AND RESPONSE ISAC	その他	
未設立		貿易会ISAC
		内閣サイバーセキュリティ戦略本部による重要インフラ分野

※National Council of ISACs 所属ISAC

～情報共有がビジネス要件になる前に～

米国には、ISACをさらに進化させた概念としてISAO（Information Sharing and Analysis Organization）と呼ばれる枠組みがある。ISAOとは、産官学の幅広い分野にわたりサイバーセキュリティの協力を促す組織として、政府と民間の情報共有の接点の役目を担っている。

米国では、ISAOに属することがビジネス要件になるほど、情報共有の重要性が広く認識されている。例えば、米国食品医薬品局（FDA）によるサイバーセキュリティに関するガイドラインでは、「製造者はISAOのメンバーであり、情報公開プロセスがあること」という要求事項が記載されている（図11）。

将来、日本でもISAOやISACなどに所属することがビジネス要件になる日がくるかもしれない。その時に備え、今から積極的に情報共有活動に参加し、業界内の体制やガイドラインの策定などに関与することが重要ではないだろうか。それにより、将来、自社のビジネスを有利に進められる可能性は高い。

ISAO SO（Standards Organization）が公開している「情報共有入門」には、「行動」と「情報のニーズ」を整合させ相互作用させるためのフレームワークが提示されている（図12）。情報共有に関する概念的フレームワークを基に、情報共有組織と参加組織の双方の役割を整理し、効果的な情報共有体制の整備を推進していくことが望まれる。

図11：米国食品医薬品局によるサイバーセキュリティに関するガイドラインの要求事項

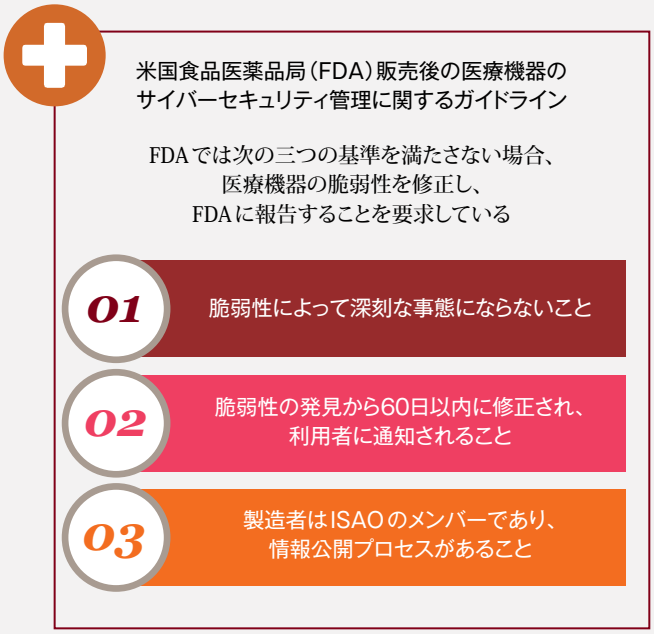


図12：情報共有に関する概念的フレームワーク

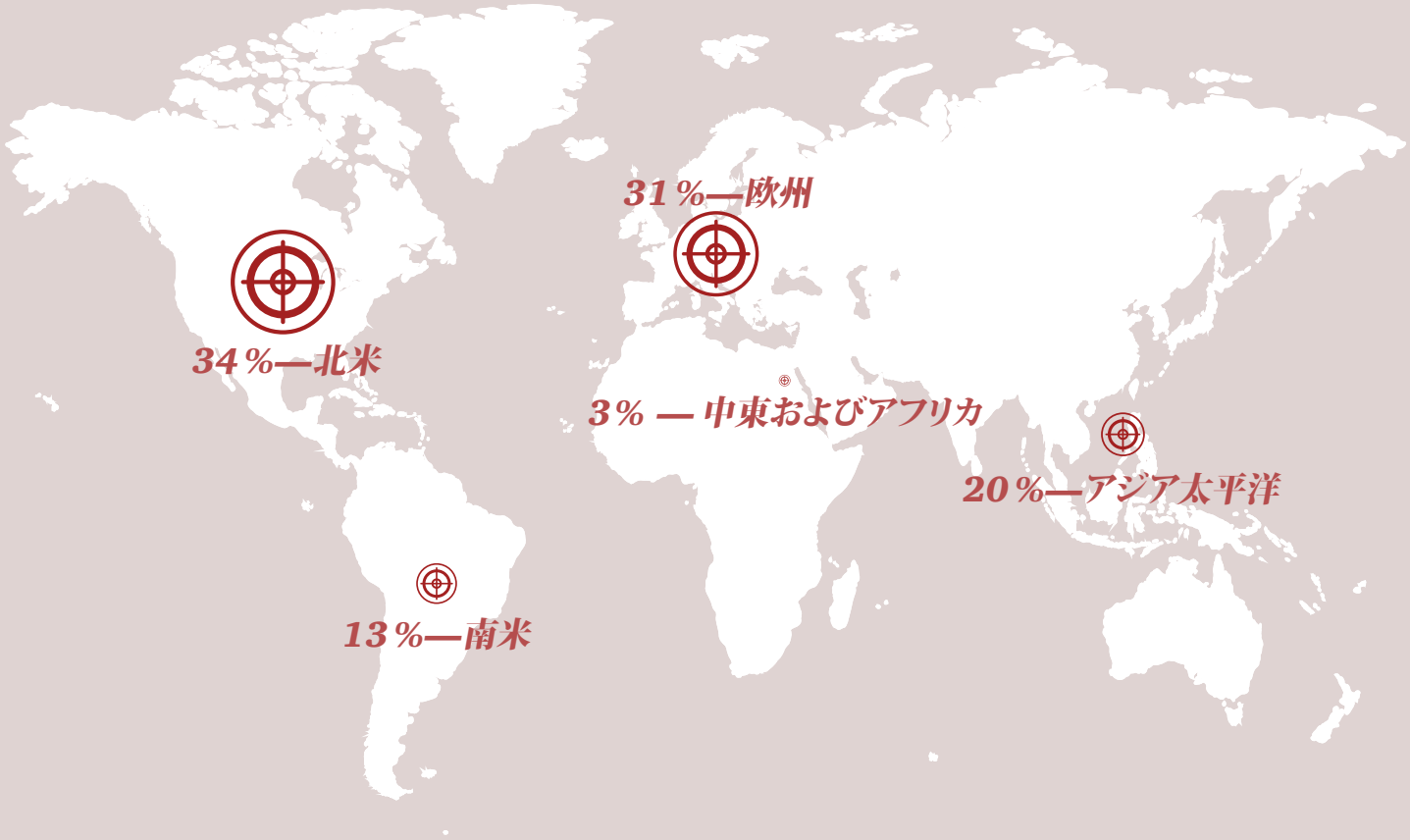
出典:IPA 独立行政法人　情報処理機構, ISAO 300-1: 情報共有入門,https://www.ipa.go.jp/files/000059103.pdf,
本資料は、米国 ISAO Standards Organizationが発行した文書を当該機構にて日本語訳し作成した資料である

調査方法

The Global State of Information Security® Survey 2017（以下、「本調査」という）は、PwC、CIO、およびCSOが実施した情報セキュリティに関する世界的な調査です。2016年4月4日から6月3日までの期間において、CIOおよびCSOの読者、および全世界のPwCクライアントに対して、電子メールによって調査への協力を依頼し、オンライン調査を実施しました。

本報告書で解説する調査結果は、10,000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ます。

回答者の地域別では、北米が34％、欧州が31％、アジア太平洋が20％、南米が13％、中東およびアフリカが3％です。



誤差は1％未満です。ここでは四捨五入した数値を使用しているため、数値の合計が100％にならない場合があります。本報告書の全ての図表は、調査結果に基づき作成したものです。

PwCサイバーセキュリティおよびプライバシーについての各国のお問い合わせ先

オーストラリア

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

オーストリア

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

ベルギー

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

ブラジル

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

フランス

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

ドイツ

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

イタリア

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

カナダ

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

中国

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

デンマーク

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

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

インド

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

イスラエル

Rafael Maman
Partner
rafael.maman@il.pwc.com

メキシコ

Fernando Román Sandoval
Partner
fernando.roman@mx.pwc.com

Yonathan Parada
Partner
yonathan.parada@mx.pwc.com

Juan Carlos Carrillo
Director
Carlos Carrillo@mx.pwc.com

南アフリカ

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

ニュージーランド

Adrian van Hest
Partner
adrian.p.van.hest@nz.pwc.com

ノルウェー

Lars Erik Fjørtoft
Partner
lars.fjortoft@pwc.com

ポーランド

Rafal Jaczynski
Director
rafal.jaczynski@pl.pwc.com

Jacek Sygutowski
Director
jacek.sygutowski@pl.pwc.com

Piotr Urban
Partner
piotr.urban@pl.pwc.com

日本

Yuji Hoshizawa
Partner
yuji.hoshizawa@pwc.com

Sean King
Partner
sean.c.king@pwc.com

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

Kei Tonomura
Partner
kei.tonomura@pwc.com

韓国

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

ルクセンブルグ

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

中東

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

オランダ

Gerwin Naber
Partner
gerwin.naber@nl.pwc.com

Otto Vermeulen
Partner
otto.vermeulen@nl.pwc.com

Bram van Tiel
Director
bram.van.tiel@nl.pwc.com

ロシア

Tim Clough
Partner
tim.clough@ru.pwc.com

シンガポール

Vincent Loy
Partner
vincent.j.loy@sg.pwc.com

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

東南アジア

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

スペイン

Javier Urtiaga Baonza
Partner
javier.urtiaga@es.pwc.com

Elena Maestre
Partner
elena.maestre@es.pwc.com

スウェーデン

Martin Allen
Director
martin.allen@se.pwc.com

Rolf Rosenvinge
Director
rolf.rosenvinge@se.pwc.com

スイス

Reto Haeni
Partner
reto.haeni@ch.pwc.com

トルコ

Burak Sadic
Director
burak.sadic@tr.pwc.com

英国

Neil Hampson
Partner
neil.r.hampson@uk.pwc.com

Richard Horne
Partner
richard.horne@uk.pwc.com

Alex Petsopoulos
Partner
alex.petsopoulos@uk.pwc.com

米国

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

Grant Waterfall
Partner
grant.waterfall@us.pwc.com

お問い合わせ先

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
03-6250-1200（代表）

山本 直樹
パートナー
naoki.n.yamamoto@pwc.com

ショーン キング
パートナー
sean.c.king@pwc.com

外村 慶
パートナー
kei.tonomura@pwc.com

PwCサイバーサービス合同会社
〒104-0061 東京都中央区銀座8-21-1
住友不動産汐留浜離宮ビル
03-3546-8480（代表）

星澤 裕二
パートナー
yuji.hoshizawa@pwc.com

グローバル情報セキュリティ調査2017
日本版レポート執筆委員

PwCコンサルティング合同会社
上杉 謙二
道輪 和也

PwCサイバーサービス合同会社
太田尾 亘

www.pwc.com/jp

PwC Japanグループは、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あらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、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、コンサルティング、ディールアドバイザリー、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223,000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 をご覧ください。

本報告書は、PwCメンバーファームが2017年2月に発行した『Toward new possibilities in threat management』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
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.com/gx/en/issues/cyber-security/information-security-survey/new-possibilities-threat-management.html
日本語版発刊年月： 2017年8月　　管理番号： I201703-2

©2017 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 for further details.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.