Insights on governance, risk and compliance

サイバー犯罪に先手を打つ

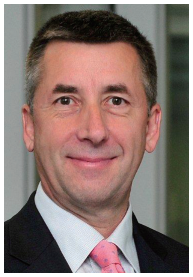
EYによる2014年 グローバル情報セキュリティサーベイ

EY
Building a better working world

目次

序文

ポール・ヴァン・ケッセル
EYグローバル・リスク・リーダー



ケン・アラン
グローバル情報セキュリティリーダー

「サイバー犯罪に先手を打つ」にようこそ

「サイバー犯罪を予想することが、それに先手を打つ唯一の方法である」。これは現在、第17回グローバル情報セキュリティサーベイ（Global Information Security Survey、以下「GISS」）に対する1,825社の回答に基づく、世界中の企業への私たちからのメッセージです。今回のGISSは、各企業がサイバー脅威をいかにうまく管理しているか、そして今日のサイバー犯罪に先手を打つためには何が求められるかという点に焦点を当てています。

メディアでは、サイバー脅威がますます高度化し、持続的、組織的になっており、サイバー攻撃によって生じる損害が企業に重大な影響を及ぼす可能性があることが頻繁に報道されています。2013年のGISS報告書で述べたように、たとえサイバー攻撃をまだ経験したことがないとしても、自社が今後攻撃の対象となる可能性がある、またはセキュリティがすでに侵害されていると考えるべきです。

2014年のサーベイでは、組織はサイバーセキュリティの基盤構築において進展を見せていること、そしてこの進展が重要であることが分かりましたが、大半の回答者は自社の基盤が成熟度の点で「中程度」の水準にしかないと回答しており、まだやるべきことが山積しています。

サーベイでは、サイバーセキュリティに対する取組みにおいて、基盤構築の先を見据えている組織が増加していることも示されています。これらの組織は、ビジネスの戦略と運営（例：合併・買収、新製品の導入、新市場への進出、新ソフトウエアの実装）の変化や外部の事業環境の変化に応じて、サイバーセキュリティ対策を適応させています。しかし、私たちは、こうした企業もまた、将来の脅威に対して受け身にならないために、考え方を変える必要があることを知りました。

これらを踏まえ、今回のサーベイ報告書をサイバーセキュリティの展開を踏まえた構成にしました。

- **Activate（始動する）**
  報告書の最初の部分では、サイバーセキュリティの基盤を取り上げています。2014年の状況はどのようなものであり、いっそうの注意を必要とする最も重要な要素とは何でしょうか？
- **Adapt（適応する）**
  次に、変化に焦点を当てます。組織は変化する要求にサイバーセキュリティ対策を適応させるために、何を実施しているのでしょうか？　サイバー脅威が変化し、より高度な技術を取り入れることによって、組織の防御を向上させることができるでしょうか？
- **Anticipate（予想する）**
  報告書の最後の部分では、先進的な組織がどのようにして準備態勢（自社に対するリスクと脅威の評価に自信を持ち、今後に備える）を整えるのか、言い換えれば、サイバー犯罪をいかに予測して先手を打つかという点について検討します。

組織はこうした展開を経て、格好の標的から侮り難い存在へと変身します。その結果、そこで初めて、攻撃に対する準備を本当に整えたことになるのです。

調査にご協力いただいた回答者の皆様に、感謝の意を表したいと思います。お時間を割いて自らの経験を私たちと共有していただいたことに感謝申し上げます。本報告書のご感想をお待ちしております。

あらゆる組織はサイバー攻撃を受けるリスクにさらされています。これからこの議論を一緒に続けていきましょう。

ポール・ヴァン・ケッセル
EYグローバル・リスク・リーダー
paul.van.kessel@nl.ey.com

ケン・アラン
グローバル情報セキュリティリーダー
kallan@uk.ey.com

サイバー脅威の状況

『サイバー攻撃の脅威：
EYによる2013年グローバル情報
セキュリティサーベイ』

『ギャップを埋める闘い：
EYによる2012年度グローバル情報
セキュリティサーベイ』

消える境界

サイバー脅威は今後も引き続き広がりを見せるでしょう。デジタル世界の到来、そして人、機器、組織に内在する相互接続性は、ITシステムの脆弱性においてまったく新たな分野を開きます。2012年グローバル情報セキュリティサーベイ（「情報セキュリティを確保するために〈*Fighting to close the gap*〉」）と2013年グローバル情報セキュリティサーベイ（「サイバー攻撃の脅威〈*Under Cyber Attack*〉」）では、このトレンドについて説明しました。

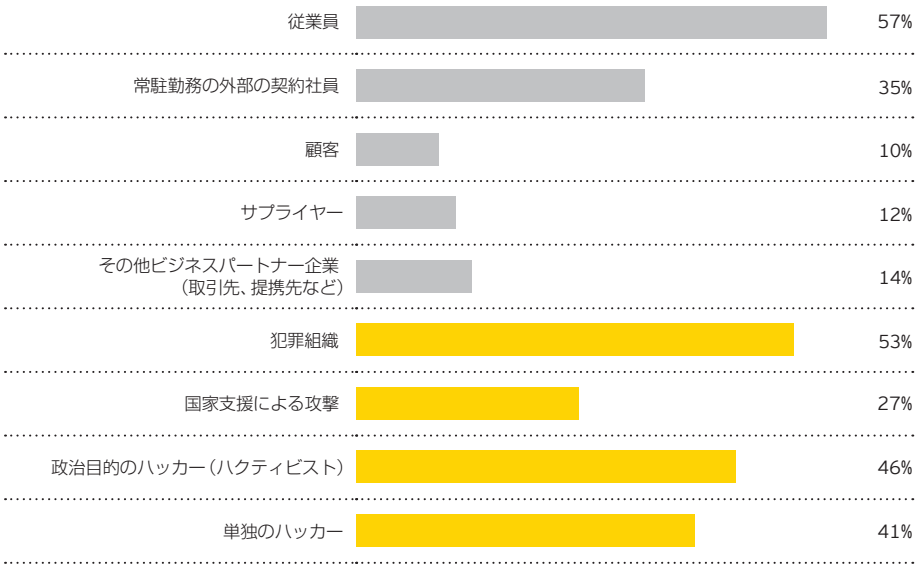
効果的なサイバーセキュリティを実現することが次第に複雑になっている5つの主な理由の概要を表したものが以下の表です。これらは、組織のセキュリティ防御に対して要求が高まり、従来の境界が損なわれ、それが脅威を与える犯罪者たち（脅威主体）のモチベーションを高める結果になっているということを示しています。

1	変化	経済危機後、企業には迅速な行動が求められています。新製品の発売、合併・買収、市場拡大、新技術の導入の動きはいずれも増加しています。こうした変化は組織のサイバーセキュリティの強度に複雑な影響を否応なく及ぼします。
2	モビリティとコンシューマライゼーション	モバイルコンピューティングの導入によって組織としての境界線が不明瞭になり、ITはユーザーに近い存在になる反面、組織から遠ざかっています。インターネット、スマートフォン、タブレットの使用（さらに、BYOD: bring-your-own-deviceとの組合わせにおいて）が、組織のデータにどこからでもアクセス可能とするのです。
3	エコシステム	私たちはデジタル接続された事業体、人々、データというエコシステムの中で生活を送り、ビジネスを行っていることから、職場と家庭の双方の環境においてサイバー犯罪にさらされる可能性が高まっています。
4	クラウド	クラウドをベースとするサービス、第三者によるデータ管理やストレージによって、以前には存在しなかった新たなリスクが出現しています。
5	インフラストラクチャ	制御技術システムは、これまで外部から遮断されていましたが、今ではIPアドレスが付与されているため、サイバー脅威がバックオフィスから、発電、交通システム、その他のオートメーションシステムなどの重要なインフラストラクチャへと拡大しています。

サイバー犯罪の攻撃力の高まり

サイバー犯罪者の攻撃力は驚くべきスピードで高まっています。攻撃者は膨大な資金源を持っています。彼らが身に付けている技術が執拗（しつよう）かつ高度になってきており、人々やプロセスを含む企業環境全体における脆弱性を見つけ出そうとしています。

サイバー攻撃を仕掛けてくる物（もしくは人）として貴社が最も可能性が高いと考えているものをすべて選択してください。



以前のサーベイでは、従業員が最も可能性の高い攻撃源とみなされていました。ところが、今回は、さまざまな外部攻撃者（犯罪組織、国家支援による攻撃、政治目的のハッカー〈ハクティビスト〉、単独のハッカー）が複合することにより、サイバー脅威がリスク源となる可能性がいっそう高まると考えられることが分かりました。また、回答者のほぼ全員が単一もしくは複数の外部攻撃者を評価の中に加えています。

今日の組織が直面している障害

次章から、どのような組織がこうした課題に対応しようとしているかを見ていきますが、まず、組織がサイバー犯罪にうまく先手を打つ前にどのような障害を取り除く必要があるかを検討する必要があります。

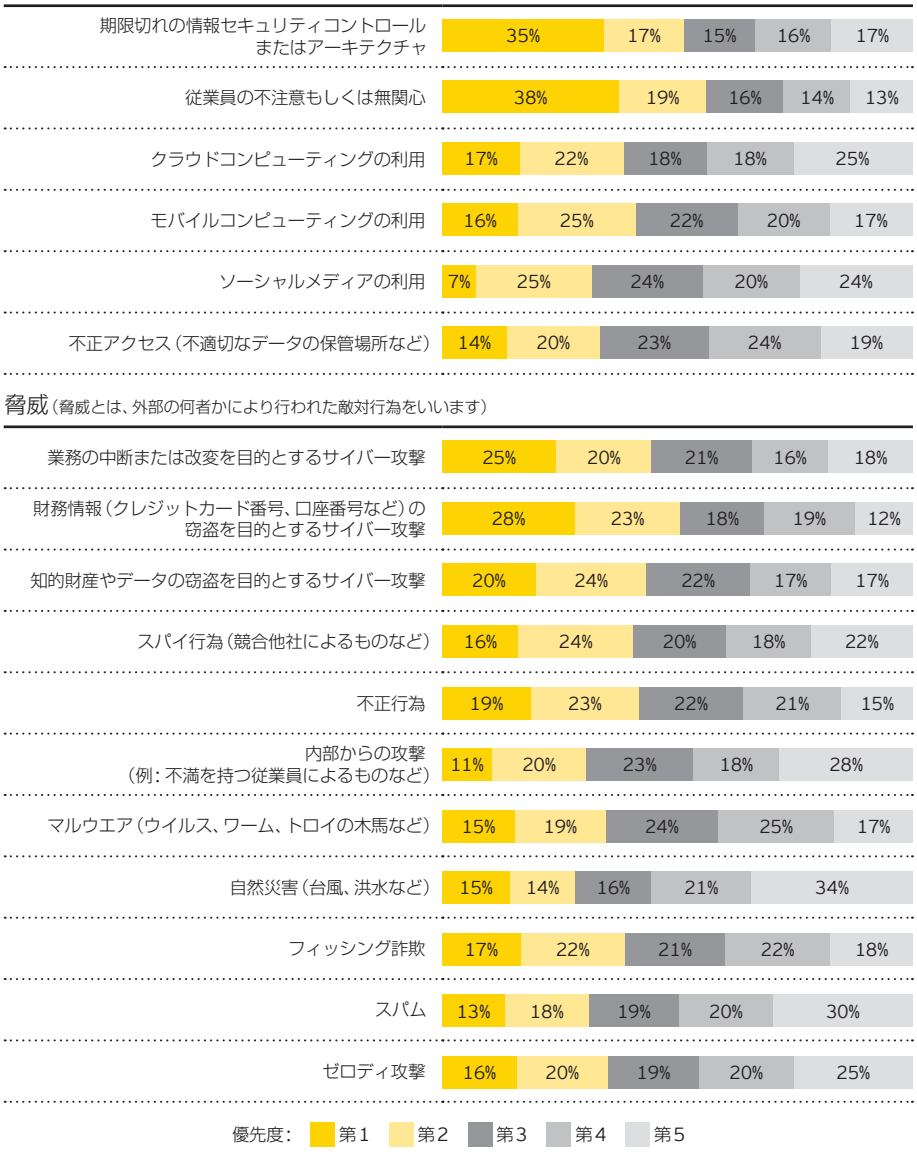
障害1――機敏さの欠如

サーベイの回答者は、サイバー脅威が増大しているだけでなく、自社のサイバー防御に既知の脆弱性が依然として存在すると述べています。言い換えれば、組織にはっきりとした危険性が存在していることを認識してはいるものの、既知の脆弱性を軽減するために十分迅速に行動していないのです。回答者の37%はサイバーリスクに関する知見をリアルタイムに入手しておらず、さらに27%は「時々」入手できるにすぎないと答えています。その結果、組織の基礎的なサイバーセキュリティの構築が後手に回っています。サーベイにおいて、注意を最も必要とする分野に関して詳細を知りたい方は、「Activate（始動する）」のセクションをご覧ください。

特筆すべき点

複数のさまざまなタイプの外部攻撃者による複合体が、今や内部の脅威以上にリスク源となる可能性が大幅に高まっています。

過去12カ月間に貴社がリスクにさらされる確率に最も大きな変化を与えた脅威や脆弱性は何ですか？



43%

の回答者が今後12カ月の情報セキュリティ予算の総額が前年度予算並みにとどまると回答しています。また、5%は情報セキュリティ予算が減少するだろうと回答しています。

53%

の組織が熟練した人材の不足が情報セキュリティに取り組む上で支障をきたす主な障害の一つであると回答しています。

障害2――予算の不足

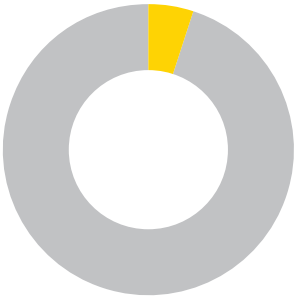
以前から予算の不足は最も困難な障害の一つです。過去には、サイバーセキュリティ予算が前年比で増加していたため、サイバーセキュリティに充てられる予算と必要な予算との格差について比較的前向きな見方をしていました。しかし、現在、予算が横ばいにとどまると答える企業が初めて増加しています。

世界中の取締役会や社外取締役の中では、サイバー犯罪に対する関心がかつてないほど高まっていますが、関心があるからといって予算が増額されるとは限らないようです。しかし、増大するサイバー脅威に効果的に立ち向かうためには、より多くの資金と人材が引き続き求められています。

障害3——サイバーセキュリティに関するスキルの不足

最も重大な障害は、サイバーセキュリティに関するスキルの不足です。専門家に対するニーズが高まる一方、毎年のサーベイでは専門家の不足が恒常的かつ深刻化する問題であることを示しています。また、サイバーセキュリティを中核事業に組み入れる非技術分野のスキルを構築することも必要です。

高度な組織ではサイバー攻撃から守るだけでなく、自社に起こり得ることを予想し、攻撃に備えたオペレーションが整っているという自信を得るために、分析力を駆使しています（詳細については、「Anticipate（予想する）」を参照）。しかし、サーベイは、脅威情報を分析し、適切かつ実施可能な結論を導き出し、決断を下し、対応を講じられるようにするために必要な専門家を採用するのは、極めて難しいことが示されています。



5%

の組織は、信頼性、関連性、脅威主体にどの程度さらされているかを評価する専任アナリストと外部のアドバイザーからなる脅威情報チームを擁しています。

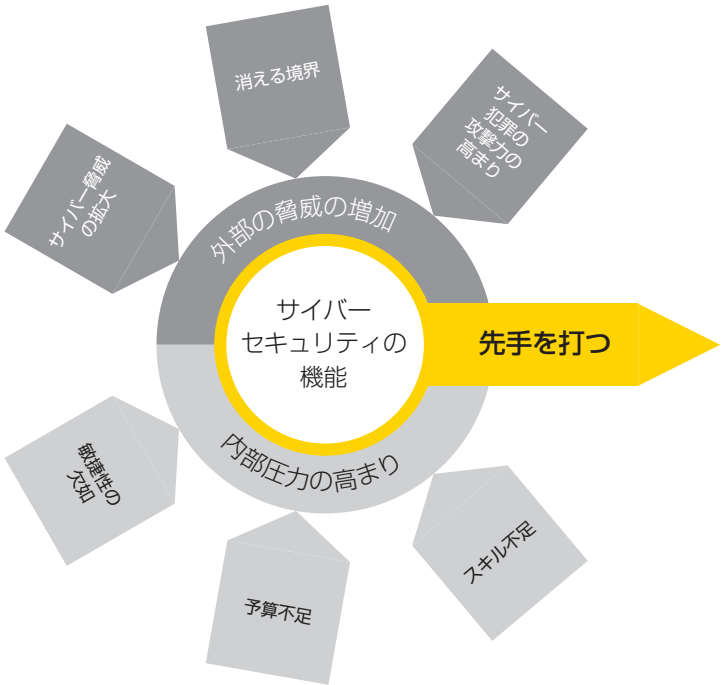
制御技術に対するサイバー脅威の増大

発電システム、交通システム、航空管制システム、ガス配給システムなどの制御技術システム（Operational Technology、以下「OT」）の対応力（resilience）が、ますます重要になると同時に、いっそうの努力も必要としています。新技術、規制面での圧力、変化するビジネス要件は、サイバーセキュリティをより必要としています。しかし、OT環境の複雑さ、レガシーシステム、異なるベンダーによるアーキテクチャ、OTチームとITチーム間の文化的違いにより、OTをセキュアにすることは容易ではありません。

IPアドレス経由のアクセスが比較的容易なため、OTシステムは往々にしてサイバー犯罪の標的となります。このため、サイバー成熟度の改善のためにOTシステムを組織の取組みの対象に含める必要があります。攻撃には次のものがあります。

- 鉄道網を管理するプロセス制御システムがワームやウイルスに感染して、運行の信頼性が低下する。
- 銀行の設備管理システムへのアクセスとビルの内部空調システムの不正操作が、オーバーヒートによるサーバーのシャットダウンを引き起こす。
- マルウエアが、原子力発電所の制御システムや石油・ガス会社の上流設備のプロセス制御を破壊する。

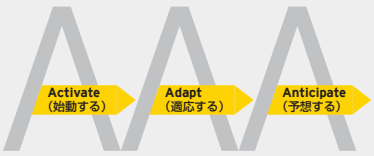
ここまで検討してきたこと（右図に要約）の中で、サイバー脅威が急速に増大していること、サイバー犯の能力が高まっていることなど、組織は依然として多くの障害に悪戦苦闘していることが分かりました。そして、サイバー犯罪に先手を打つことが容易ではないことを知りました。



サイバー犯罪に先手を打つ――

次章からサイバーセキュリティの成熟に向かう展開における三つのステージ――Activate（始動する）、Adapt（適応する）、Anticipate（予想する）（三つのA）――について検討します。これらを最先端のサイバーセキュリティを実現するために厳格な順序で（そして継続的に繰り返し）実行する必要があります。

サイバー犯罪に対する組織の対応は明確に区別された三つのステージに分類され、各段階でこれまで以上の高度なサイバーセキュリティ対策の実装を目的とする必要があることが分かりました。



Activate（始動する）

組織は盤石なサイバーセキュリティの基盤を持つ必要があります。この基盤はサイバー攻撃に対する基本的（基本的であって、優れているというほどではない）な防御となる包括的な情報セキュリティ対策から成り立っています。このステージでは、基盤を確立つまり、サイバーセキュリティを「始動」します。

基盤

サイバーセキュリティの**導入**

既存環境の保護対策に着目

静的アプローチ

現在の状況	以下から該当する項目をチェックすることで、貴社の特徴のうち「Activate（始動する）」のプロファイルに当てはまるものがいくつあるか、確認できます。
インシデント管理	☐ インシデントが起こったことはまったくない ☐ 第三者が情報を発表する、または貴社に通知する ☐ 誰が対応するのか決まってない ☐ 情報を公開する担当者がいない ☐ インシデント対応計画がない
リーダーの論点	☐ 取締役会の取扱事項ではない ☐ ツールとポリシーを重視したリーダーのコメント ☐ セキュリティ・リーダーシップ・チームとして関与していない
指標	☐ 社員数 ☐ 成熟度モデル ☐ 予算 ☐ コンプライアンス

三つのAに焦点を当てる

Adapt（適応する）

組織は変化します――その変化が生き残りのためか、成長のためかにかかわりませんが。また、脅威も変化します。それゆえ、情報セキュリティ対策の基盤は、ビジネス要件や動向の変化と歩調が合うよう適応しなければなりません。さもなければ、時間の経過とともに有効性が失われていきます。このステージでは、サイバーセキュリティを最新の状態に保つことに取り組みます。すなわち、変化する要件に「適応する」のです。

Anticipate（予想する）

組織は潜在的なサイバー攻撃を検知し減じるための対策を立てる必要があります。守る必要があるもの（組織にとっての「至宝」）を的確に知り、起こり得る攻撃／インシデントのシナリオ（事故を含めて）への適切な対応を繰り返し実践しなければなりません。これには、成熟したサイバー脅威情報収集能力、しっかりとしたリスク評価方法、熟練したインシデント対応の仕組み、情報に通じた組織が必要です。このステージでは、予見可能な脅威と予期しない攻撃に対し、自信を持って対応できる能力が備わります。つまり、サイバー攻撃を「予想して」いるのです。

動的	**先験的**
サイバーセキュリティの**組込み**	**先験的**なサイバーセキュリティの構築
変化する環境に着目	**将来**の環境に着目
動的アプローチ	**先を見越した**アプローチ
以下から該当する項目をチェックすることで、貴社の特徴のうち「Adapt（適応する）」のプロファイルに当てはまるか確認できます。	以下から該当する項目をチェックすることで、貴社の特徴のうち「Anticipate（予想する）」のプロファイルに当てはまるものがいくつあるか確認できます。
☐ 自社インシデントを特定し、それに対応している ☐ インシデント対応計画が参画する者に通知されている ☐ インシデント対応チームにはITのリーダーが含まれている ☐ 広報体制が確立されている ☐ 侵害が今後起こる、またはすでに起こっていることを受け入れられる	☐ 脅威シナリオに基づいて将来の侵害に備えている ☐ 上級幹部が対応チームの一翼を担っている ☐ 外部との通信が管理され、事実に基づき防御できる状態にある
☐ 災害復旧計画 ☐ 規制面の状況と影響 ☐ ITのリーダーとビジネスリーダーが侵害の発生と影響の実態について議論している	☐ 取締役会の定例の討議事項 ☐ ITのリーダーとビジネスリーダーは、セキュリティによってビジネスを強化する方法を議論している ☐ 同業他社との経営者レベルでの協力
☐ 攻撃／インシデント ☐ 侵害が売上高に及ぼす影響 ☐ 高度なリスク分析とスコアリング	☐ セキュリティによる売上高のサポート／拡大／保護 ☐ 事業目標との整合性

基盤を構築する

すべての組織は確固としたサイバーセキュリティ基盤を必要としています。この基盤を導入するのは容易なことではなく、やるべき事は業種や地域によって異なります。

これは目新しいことではありません。2012年グローバル情報セキュリティサーベイ報告書（「情報セキュリティを確保するために〈*Fighting to close the gap*〉」）では、実際に取り組まれているサイバーセキュリティ対策と導入されるべき基礎的なサイバーセキュリティの構成要素とのギャップについて調査しました。この基盤はサイバーセキュリティへの展開における最初のステップとなります。

Activate（始動する）

サイバーセキュリティのための基盤を始動したものの、その先に進めない組織は、一般に以下の三つの能力が不足しているといわれています。これらが、なぜサイバーセキュリティへの展開を続けなければならないかという理由となります。

1. サイバーセキュリティの導入

組織のサイバーセキュリティは、業務プロセスと事業活動に導入されています。しかし、サイバーセキュリティはまだ業務に組み込まれておらず、また価値を付加する活動ではなく、できるだけ削減すべきコスト要因とみなされています。もしアプリケーションを開発した後や主要な工程におけるチェックだけでセキュリティの保証が承認されるとすれば、組織はセキュリティ対策を導入したという段階で行き詰ってしまいます。

2. 既存環境の保護対策に着目

サイバーセキュリティの基礎レベルでは、まず組織が過去の経験に基づいてすでに認識しているリスクに目を向けることからスタートします。最終目標は、あらゆる脆弱性の解決策を確実に整備することです。単にリスク評価、統制の効率性、リスクの軽減のみが議論されるならば、組織は「Activate（始動する）」のレベルにとどまることになります。

3. 静的アプローチ

サイバーセキュリティ能力のこの段階では、組織がいつもの日常業務を安全に遂行できるようにすることを目指しています。規則に基づいたコンプライアンス主導の組織であり、指標に基づいた報告に重点を置きます。つまり、変化のない世界でのみ脅威に対応することができるのです。

すべての企業はサイバーセキュリティの構築でいかに進んでいようとも、サイバーセキュリティの基礎的な要件に精通していなければなりません。しかし、今回のサーベイから私たちが気付いたことは、非常に多くの組織がすべての基礎的な構成要素さえ導入していない状況です。

本報告書では、5つの重要な分野に焦点を当てています。今回のサーベイ、およびグローバルなクライアントと共に歩んできたEYの経験から、これらが最も大きな問題を引き起こす分野であることが明らかであるためです。

- 経営幹部の同意（buy-in）
- リソース
- パフォーマンス
- データへのアクセス
- コスト対価値

構成要素	問題となること
経営幹部の同意（buy-in）	▸ サイバーセキュリティの戦略、計画、実施に関して、ボトムアップ型のリーダーシップである、もしくはITの問題として見なされている。 ▸ 一貫性のあるサイバー脅威の管理体制が導入されておらず、取締役会ではサイバー脅威について定期的に議論されていない。
リソース	▸ サイバーセキュリティの職務に対し適切にリソースが割り当てられていない、もしくは熟練者によって実施されていない。 ▸ サイバーセキュリティチームが攻撃に関する見通しや知見を備えていない。
パフォーマンス	▸ 多くの組織が非常に薄く広い範囲を対象としている。つまり、非常に多くのサイバー能力を維持しており、結果としてその能力の有効性が限定的である。 ▸ サイバーセキュリティの有効性が計測されていない。
データへのアクセス	▸ 従業員がサイバーセキュリティのリスクであり、従業員のID／アクセス管理（Identity and Access Management、以下「IAM」）体制が脆弱である。 ▸ 過剰な手処理があったり、レビューや報告が定期的に行われなかったりするため、従業員による不正アクセスが非常に簡単にできる。 ▸ 従業員の異動、離職、入社が主要なサイバーリスク分野である。
コスト対価値	▸ 非常に多くの組織がサイバーセキュリティコストを多額であるとみなしている。 ▸ 導入済みの対策のメリットを評価していない。 ▸ サイバー攻撃の潜在的なコストを大幅に過小評価している。

サーベイの結果	左記の結果から導き出される結論
 最高情報責任者（CIO）またはIT部門の約80%は、情報セキュリティ部門から直接報告を受けているのに対して、CEOに直接報告しているのはわずか14%にとどまっています。	▸ サイバーセキュリティにおいて組織の上層部を関与させる必要がある。 ▸ 経営幹部の同意（buy-in）の欠如は誤りやサイバー犯罪の誘因となり、それによってサイバーセキュリティに必要な方向性と投資を失うことになる。
 サイバーリスクに関する知見をリアルタイムで容易に入手できる組織は20%未満です。  同業他社に関するサイバー攻撃に関して公表された情報を容易に入手できる組織は20%です。	▸ サイバー脅威の見落としや対応の遅れが起き得る。 ▸ フィッシングを巧みに利用したサイバー犯罪が成功する要因は、セキュリティに対する認識欠如の結果である。
 大半のサイバーセキュリティプロセスにおいて、回答者の35～45%が自社には「まだ改善するべき点が多くある」と評価しています。	▸ 基礎的なサイバーセキュリティプロセスが適切に機能していないため、高度で執拗な脅威（Advanced Persistent Threat、「APT」）の実行者が侵入する糸口が多数残されている。
 ほぼ3分の2の組織では、明確に定義され自動化されたIAM体制がありません。	▸ 従業員がサイバーセキュリティの巨大な脅威であるとみなされることがある。組織は外部からのハッカーを探しているが、不正行為はすでに内部で発生している。
 63%は予算の制限が情報セキュリティ運用における貢献や価値を創造する上での主な障害であると考えています。  ほぼ50%は今後12カ月間に予算の増額はないとみています。	▸ 組織は日常的に攻撃にさらされており、攻撃者は諦める兆候がないどころか、一段と巧妙で狙い澄ました攻撃を仕掛けてくることを理解する必要がある。また、次の侵害が致命的なものになる可能性がある。

すべての組織が「Activate（始動する）」必要のある場合の基礎的な活動

サイバーセキュリティの基礎的なレベルにまだ達していない組織は迅速に行動する必要があります。そのような組織をサポートする、見過ごされがちながらも早急に検討するべき極めて重要な事項を6つ挙げます。

1. **セキュリティの評価とロードマップ**
   サイバー脅威の評価、現在の成熟度の評価、目標とする状態の定義、ギャップ分析および実装に向けてのロードマップの策定、ISO 27001などのリーディングプラクティスとの整合を実行する。
2. **セキュリティの変革のため取締役会レベルの支援の獲得**
   IT部門以外のサイバーセキュリティの再編や、取締役会のプロセス理解の確保といった、サイバーセキュリティのガバナンスを再定義する。
3. **セキュリティの方針、手続き、支援基準の見直しおよびアップデート**
   情報セキュリティ・マネジメント・システム（Information Security Management System、「ISMS」）を実装する。
4. **セキュリティ・オペレーション・センター（Security Operations Center、以下「SOC」）の設立**
   周知の事例のモニタリングやインシデントの対応手続きを策定する。
5. **サイバーセキュリティ統制の設計および実装**
   データ紛失からの保護プロセスとID・アクセス管理の有効性を評価する。サーバー、ファイアウォール、ネットワークコンポーネント、データベースなどのIT資産のセキュリティの堅牢化を図る。
6. **事業継続性計画とインシデント対応手続きのテスト**
   ネットワークの境界、侵入ポイント、ソフトウエアアプリケーションに対する定期的な侵入テストを積極的に実施し、攻撃されやすい脆弱性を特定する。

セキュリティ・オペレーション・センター（SOC）

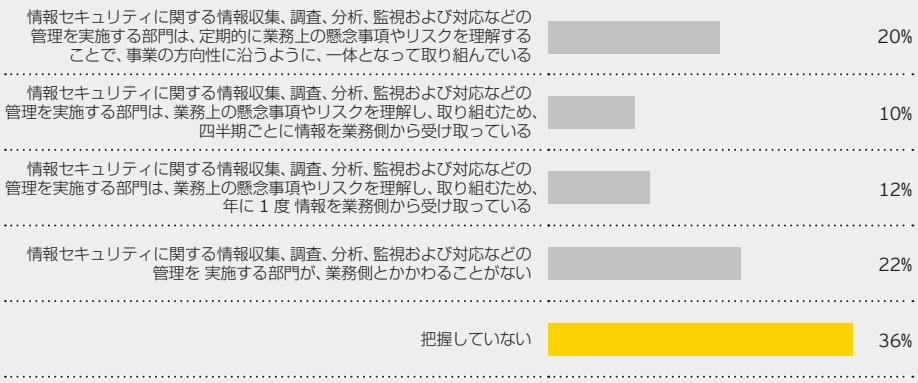
基礎的なサイバーセキュリティにとって決定的に重要なものは、情報セキュリティ機能をサポートするプロセスと技術です。これらが最も効果的なのは一元管理で組織化され、相互に連携されているときであり、SOCが重要な出発点であるのはそのためです。SOCは外部委託が可能ですが、自社の業務ニーズに確実に合致させることが重要であり、「万能サイズ」からカスタムメイドのSOCへ明らかにシフトしています。また、サイバーセキュリティの脅威と問題に関する最新の知見を持ち、ビジネス戦略に合致させることも重要です。

サーベイでは40%以上の組織がSOCを有しておらず、その点が懸念されます。SOCを設置している組織でも、一元管理によるメリットが実現できていない、または組織での周知や理解がされていません。回答者の半分以上はSOCが事業運営のニーズをどの程度満たしているかに関する質問に、回答できない、もしくは「不明である」または「SOCは業務側とかかわることがない」と回答しています。

42%

の組織はSOCを有していません。

貴社の情報セキュリティに関する情報収集、調査、分析、監視および対応などの管理を実施する部門（SOCなど）は、業務上のニーズを満たしているでしょうか、該当するものを選択してください。

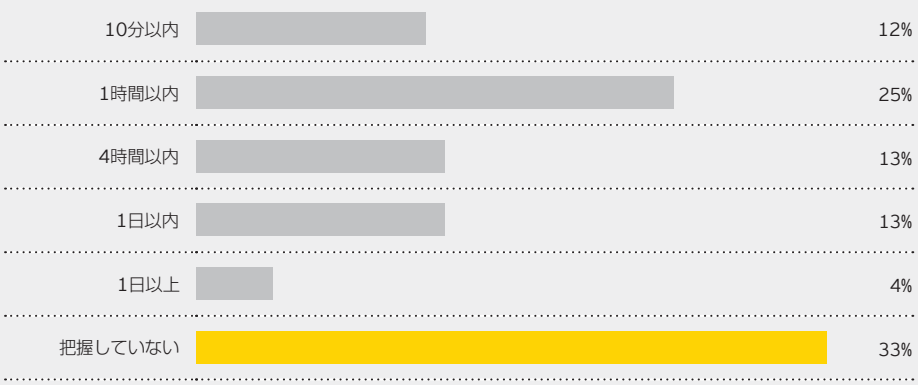


37%

はサイバーリスクに関する洞察をリアルタイムで入手できないと回答しています。

SOCが最新のサイバー脅威にいかに遅れないでついて行っているかという点においても、同様な認識不足がありました。回答者の50%以上は質問に答えられなかったか、発見または注意喚起されたインシデントに関してSOCが調査を開始するのにどれ位の時間がかかるか知りませんでした。改善を要請または命じる前に、組織はまず自社のSOCが何を行っているかについてもっと知る必要があります。

貴社の情報セキュリティに関する情報収集、調査、分析、監視および対応などの管理を実施する部門（SOCなど）が、発見・通報されたインシデントに対する調査開始までに要する平均時間について、該当するものを一つ選択してください。



全体として、SOCの技術基盤と業務側との接点（endpoints）は改善する必要があります。SOCのメリットがもっと理解されれば、組織の一般的な自衛能力は、最も基本的な職務にさえも、メリットをもたらすでしょう。

動的アプローチを取る

基礎を構築した組織は、サイバーセキュリティへの展開を始めていますが、競争力を維持するには、変化するビジネス環境と、その変化に伴い進化する脅威に対して常に変化、適応しなければなりません。その結果、組織のサイバーセキュリティの要件も、変化する必要に迫られます。具体的には、既知のリスク状況認識の改善をサポートすることを目的とした、制御基盤や技術力と技術の利用変更などです。組織が適応しなければ、そのサイバーセキュリティ基盤は急速に古びてしまうでしょう。

Adapt（適応する）

「Adapt（適応する）」の段階では、「Activate（始動する）」レベルに以下の特性が加わります。

1. セキュリティの組込み

サイバーセキュリティは、新たな業務プロセスの開発、新工場の開設、新製品の取得や導入など、組織が行うすべてのことにおいて考慮され、関与しています。 事業の変化はサイバーセキュリティの観点から、事後ではなく直ちに評価され、変化するサイバーセキュリティの要件がすべての業務プロセスに組み込まれます。その結果、サイバーセキュリティは常に最新の状態に保たれます。

2. 変化する環境に着目

より成熟度の高いサイバーセキュリティは、変化し続ける事業とその環境に常に適応します。例えば、デジタル化やクラウドサービスの利用は、以前には組織が直面しなかったリスクをもたらす可能性があります。状況の認識を深めることは、社内の変化を取り入れ、予想される脅威の変化に対応するリスク評価を可能にします。

3. 動的アプローチ

サイバーセキュリティは、柔軟性と機動性を備え、常に見直されて、ビジネス防衛の改善に絶えず適応しています。

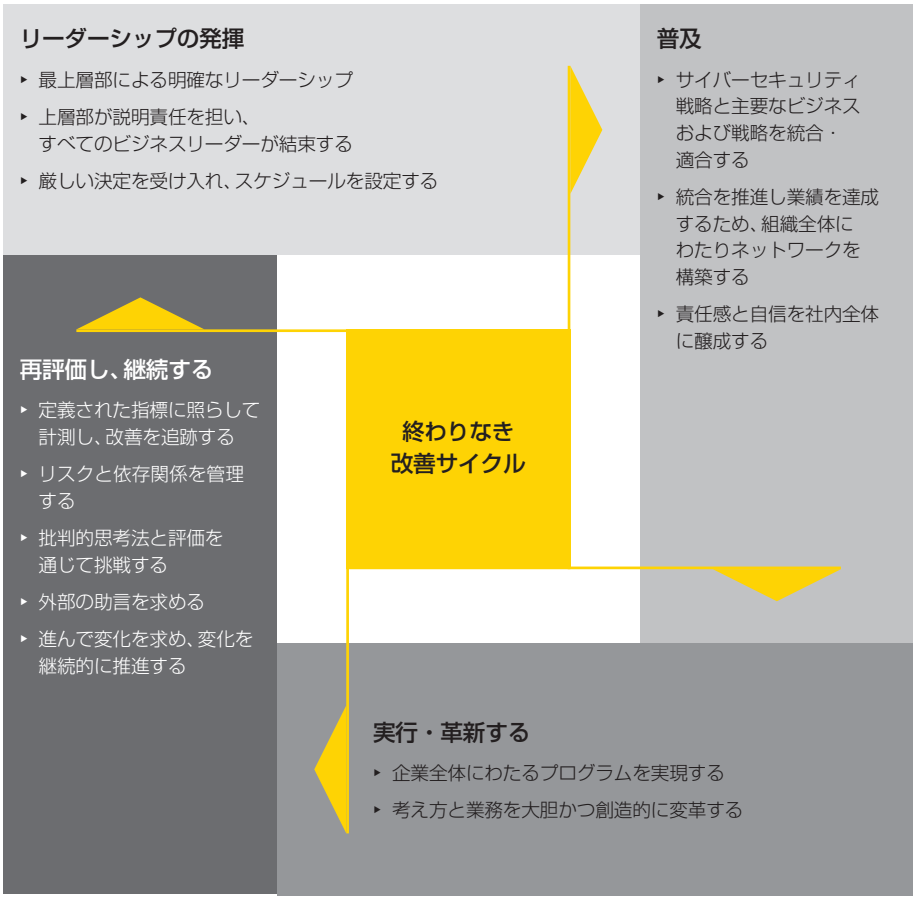
改善サイクル：適応性に対するアプローチ

組織は絶えず変化しています。以下はその例の一部です。

- 新技術（ソーシャルメディア、クラウド、デジタル、ビッグデータなど）を業務プロセスに統合する必要性
- ビジネスと個人の世界との境界をあいまいにする、モバイル機器（BYODなど）の急激な増加
- マネージドサービスやリモート・ホスティング・サービスの拡大、および複雑なアプリケーション（多くはリモートホスト上で稼働している）への依存度の高まり
- プロセス制御基盤と、バックオフィスおよび外部との統合
- 急速に変化する規制環境と要件

その結果、組織は変化するサイバーセキュリティ能力の改善とその評価という際限のないサイクルが求められる新たな脅威と、その課題解決という際限のないサイクルに対処しなければなりません。また、ビジネスを可能にし、コストを削減できるさまざまなセキュリティ機会を新たに捉え、そこからメリットを得なければなりません。そのためには、効果的、効率的な方法でこのサイクルを管理できるシステムを構築する必要があります。

改善サイクル



現実を把握するために過去を振り返る

サイバー犯罪に先手を打つためには、サイバーセキュリティ対策を自社のビジネス戦略に100%一致させることが極めて重要です。この課題は数年間にわたり優先議題となっており、年々改善が進んでいます。ところが今回のサーベイでは、過去5年間で初めて、組織のビジネス戦略と一致させるという課題への取組みが、実質的に後退していることが示されています。組織のサイバーセキュリティが継続的に改善されていますが、サイバー脅威の状況の変化（報告書の第1章を参照）はそれを上回る速度で進展しています。私たちはこのトレンドを2年前に予想していました*。これは、組織がニュースや個人的な体験によって、サイバー脅威の実態に対する認識を高めていることをも示唆しています。

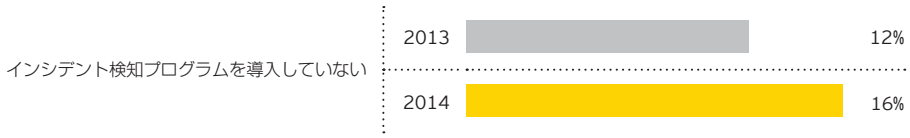
今回のGISSでは、以下のような結果が得られました。

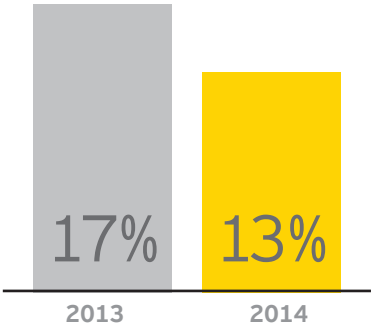
- 回答者の13%は自社の情報セキュリティ機能が自社のニーズを満たしていると答えています。これは2013年の17%から低下しています。
- 昨年は回答者の68%が、「情報セキュリティ機能が自社のニーズを部分的に満たしており、改善が進んでいる」と考えていましたが、今回は63%に低下しています。

これらの結果は、組織がサイバーセキュリティに関してより本格的に取り組む必要性が示されています。前ページの「改善サイクル」を利用すれば、軌道を戻す一助となるでしょう。

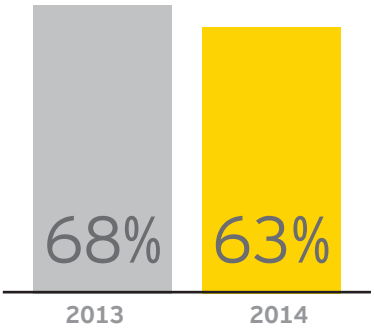
サーベイでは、サイバーセキュリティがなぜこれほど多くの組織のニーズ（例えば、インシデント検知）を満たしていないのかという点についても、検討しています。

貴社のインシデント検知プログラムの成熟度を最もよく表しているのはどれですか？





サーベイでは、情報セキュリティ機能が組織のニーズを完全に満たしているという回答が増加するとの予想に反して、減少していることが分かりました。



自社の情報セキュリティ機能が組織のニーズを部分的に満たしており、改善が進んでいると回答する組織の数が増加するとの予想に反して、5%の低下がみられました。

決定的に重要な改善をいかにして行うか

では、具体的により注意を払う必要があるのはどのような点なのでしょうか。どのような「手っ取り早く達成できる目標（容易に手が届く果実）」によって組織は前進しやすくなるのでしょうか。

大半の組織に当てはまる4つの改善点は以下の通りです。

1. SOCの改善

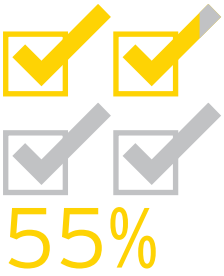
うまく機能しているSOCは、サイバー犯罪に先手を打つための重要な資産です。 組織の中で最新のサイバー脅威に気付くべきセキュリティ機能があるとすれば、それはSOCです。自社のSOCが最新のサイバー脅威に遅れをとっていないと感じているのは、回答者のほぼ3分の1にとどまっています。これは驚くべき結果です。

根本的な原因の一つは、多くの場合、SOCが技術を過度に重視している点にあります。技術の特性（何を計測・監視できるか）は重要ですが、出発点は業務側（何を計測・監視する必要があるか）にあるべきです。

鍵となるのは、業務側との意思の疎通です。GISSの回答者の22%はSOCと業務側との間に意思の疎通がないと答えています。そして、さらに36%は分からないと答えています。業務側がSOCと定期的にコミュニケーションを取り合っていなければ、どのようにしてSOCは適正なリスク（そして変化するリスク）に焦点を当てることができるのでしょうか。

* EYによる2012年度グローバル情報セキュリティサーベイ「情報セキュリティを確保するために（*Fighting to close the gap*）」を参照（www.ey.com/giss2012）。

** EYによる2013年グローバル情報セキュリティサーベイ「サイバー攻撃の脅威（*Under Cyber Attack*）」を参照（www.ey.com/giss2013）。



55%

の組織は、従業員の業績評価に情報セキュリティを含めていません。

2. サイバーセキュリティの中核チームの編成

サイバーセキュリティのアプローチと活動を、中核チームを中心に集約します。中核チームにおいてサイバーセキュリティの知見を確立することにより、組織は新たなサイバー脅威に対してより適応しやすくなります。この中核チームは集中型として組織することもできますが、組織の規模や要件に応じて部門や組織の境界を越えて分散させることも可能です。

中核チームは研修、スキル、意識向上についても焦点を当て、全従業員のために日常における情報セキュリティ面で実践すべき行為を策定する必要もあります。また、中核チームのメンバーはチームが推奨することを実践する大使のような役割を果たす必要があります。

3. 義務の規定

義務と業績測定の向上は、行動変化を達成する上で鍵となる方法です。組織のセキュリティがサイバー脅威にさらされれば従業員各自も同じ状態に陥ること、そしてサイバーセキュリティが業績指標であることを、従業員が理解することによって、意識や態度の変容につながる可能性があります。特に重要情報にアクセス可能な者を対象に、従業員として求められる行動を雇用契約に盛り込み、彼らの業績評価に組み入れます。たとえ重大な結果をもたらさないとしても、情報セキュリティ規約の侵害は極めて深刻に受け止める必要があります。

サイバー脅威について従業員に周知させることに加えて、従業員が組織の「目と耳」となり、何か疑わしいことに気付いた場合に誰もが従う明確なエスカレーションプロセスを確保します。本サーベイでは、フォレンジックによる支援とソーシャルメディアは情報セキュリティの優先順位の最下位の分野ですが、これらの技術とチャネルは組織が攻撃のリスクにさらされていることに最も早く察知できる方法になり得ます。

4. 境界を越える

変革サイクルが導入される中で、組織は境界の先に目を向け、サイバー攻撃がビジネスパートナー、サプライヤー、ベンダー、つまり自社の事業の「エコシステム」と呼ばれるコミュニティに及ぼす影響の評価に着手することができます（19ページを参照）。自社が変革に成功すれば、リーディングプラクティスが明らかになり、それをエコシステム内に周知することができます。それにより、サプライヤーとベンダーは契約によって、従わざるを得なくなります。

改善と変革のための措置を講じる

貴社が「Activate（始動する）」と「Adapt（適応する）」の中間の段階にある場合、早急に検討するべき5つのステップがあります。

1. 変革プログラムを設計・実行する

基本的レベルを上回る、サイバーセキュリティの成熟度の段階的な改善をサポートします。ここでは、セキュリティプロジェクトが段階的な形で個別に実現されます。変革プログラムの設計や運営の提供については外部からの協力も得ます。

2. 何を社内に残し、何を外部委託するかを決定する

例えば、自社のSOCの中核チームが完全な社内機能を維持するか、それともマネージド・セキュリティ・サービス・プロバイダー（Managed Security Services Provider、「MSSP」）に外部委託するか、それとも内製と外部委託の混合モデルに移行するかを決定します。

3. サイバーセキュリティのRACIマトリクスを定義する

4. 組織のエコシステムを定義する

セキュリティ侵害が第三者に及ぼす波及的な影響を考慮し、第三者との相互関係における潜在的なセキュリティギャップの排除または軽減に着手します。

5. サイバーセキュリティの従業員向け認知度向上研修を導入する

成熟度評価、目標レベルの定義、ギャップ分析を実施します。スタッフ（請負業者を含む）のための研修計画を策定・実施します。

境界の先に目を向ける：事業のエコシステム

私たちの調査では、サイバー犯罪との闘いにおいて大半の企業は社内組織（データ、システム、人材を含む）の周囲にフェンスを築くことに時間と資源の大半を費やしていることが示されています。これは出発点ですが、境界はもはや不変とはいえず、フェンスも有効とは言い切れません。

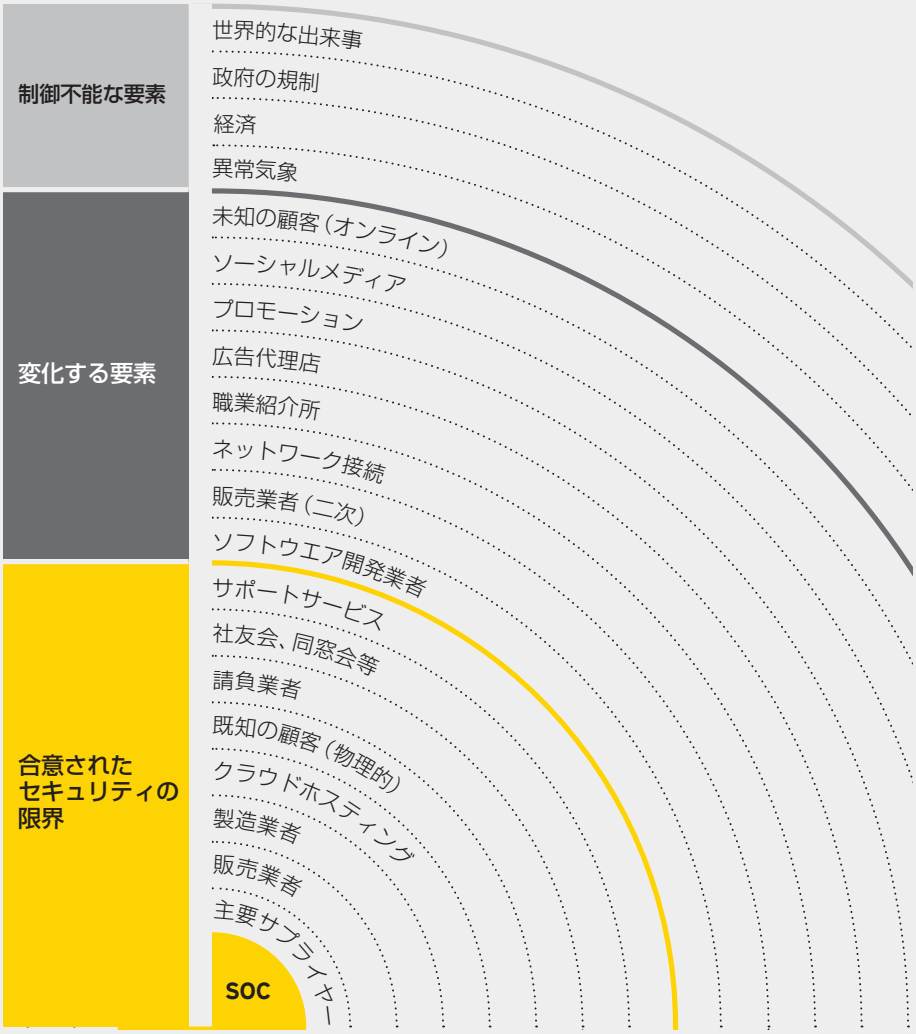
今日の事業の大半はフェンスの外側で行われています。組織がビジネスパートナーとのコミュニケーションを可能にするためには、フェンスに「穴」を空けなくてはなりません。結果として、サイバーセキュリティシステムはクライアント、顧客、サプライヤーやベンダー、ビジネスパートナー、そしてかつて組織に属していた人々などを含むより広範なネットワークを包含する必要があり、これらは「事業のエコシステム」と総称されています。

エコシステムにおいてリスクを効果的に管理するためには、エコシステムの範囲を明確に定義する必要があります。また、その範囲内で何を管理したいのか、それは組織自体から一歩離れたグループ（例：サプライヤー）が直面するリスクに限定するのか、エコシステムの中央から二歩離れたグループ（例：サプライヤーのサプライヤー）が直面するリスクの軽減に影響力を及ぼすべきなのか、などを決定する必要もあります。

組織は以下について検討する必要があります。

- 「セキュリティの範囲」とは何か。言い換えれば、サイバーセキュリティ全体を強化するため、いくつのパートナー企業と協力する必要があるか。
- 事業のエコシステムの中でリスクを管理するにはどれだけのことができるか。
- 事業のエコシステムから一定レベルのリスクを受け入れる用意があるか。

貴社の事業のエコシステム



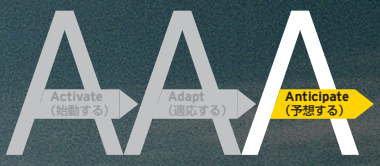
先を見越した準備態勢を整える

すでに発生した脅威に対応する上で組織にできることには限りがあります。しかし、新たな脅威がいったん活動を開始してから対応するのでは、遅すぎるかもしれません。

この複雑で動的な環境の中で先手を打つ唯一の方法は、課題を正面から把握することです。つまり、サイバーセキュリティを事業の中核として、そして生き残って成長するための総合的な能力として捉えることです。成功を収め、それを維持することは、終わりなき道のりです。そして、組織のサイバーセキュリティ能力を構築・維持することは、この終わりなき道のりの一部なのです。

準備が整った状態に移行すること、すなわち何が起こるかを予想し、それに従って行動・対応の準備を整えることに、意欲的に取り組むべきです。これを実行することは、不安定で心もとないオペレーションのせいでサイバー脅威による好ましくない不測の事態にさらされるのだという、「被害者」意識を捨て去ることを意味します。また、認識と高度な能力を構築し、説得力のある戦略を策定し、事業を通じてサイバーセキュリティの構成要素を設定することを意味します。また、サイバー犯罪に取り組むための組織の能力についての自信を高めることを意味します。

Anticipate（予想する）



「Anticipate（予想する）」の段階では、以下の特性を加える必要があります。

1. 先験的なセキュリティの構築

- **バランスの取れた方法で迅速に行動・対応するために注意を払い、準備を整える。**リーダーはサイバー脅威やリスクを中核事業の問題であり、サイバーセキュリティへの対応力は動的な意思決定プロセスの一部であることを認識しています。これにより、円滑で迅速な運営を行うための予防措置や対応の仕組みが可能になります。
- **自社の「至宝」を知る。**事業の中で最も大切な資産が何であるかを知らなければ、組織が攻撃に備えることができません。資産に優先順位を付け、何らかの形で、侵害、漏えい、または利用不可となることによる影響を理解した上で、脅威を評価するプロセスと関連付けできるようにしなければなりません。

2. 将来の環境に着目

- **自社の環境を徹底的に知る。**包括的でありながらも的を絞った状況認識は、より広範な脅威の状況とそれが組織とどのように関係するかを理解する上で、極めて重要です。サイバー脅威情報はこのための知見をもたらします。すなわち、社外と社内のリスク源の双方を取り込み、過去から学びつつも現在と将来の両方を取り扱うのです。
- **継続的に学習し進化する。**すべては流動的です。犯罪だけでなく、組織や業務環境のいかなる部分においてもそうです。だからこそ、継続的な改善サイクルがあり続けるのです。学習し続ける組織、つまり、フォレンジックを含めてデータを精査し、新たな協力関係を維持・検討し、戦略を定期的に刷新し、サイバーセキュリティ能力を進化させるような組織となる必要があります。

3. 先を見越したアプローチ

- **自社のインシデント対応と危機対応の仕組みに自信を持つ。**予想する段階にある組織は、インシデント対応能力の予行演習を定期的に行います。これには、シミュレーションや机上演習から、組織の能力を本格的にテストする複雑なインシデントに関するシナリオに基づいた訓練が含まれます。

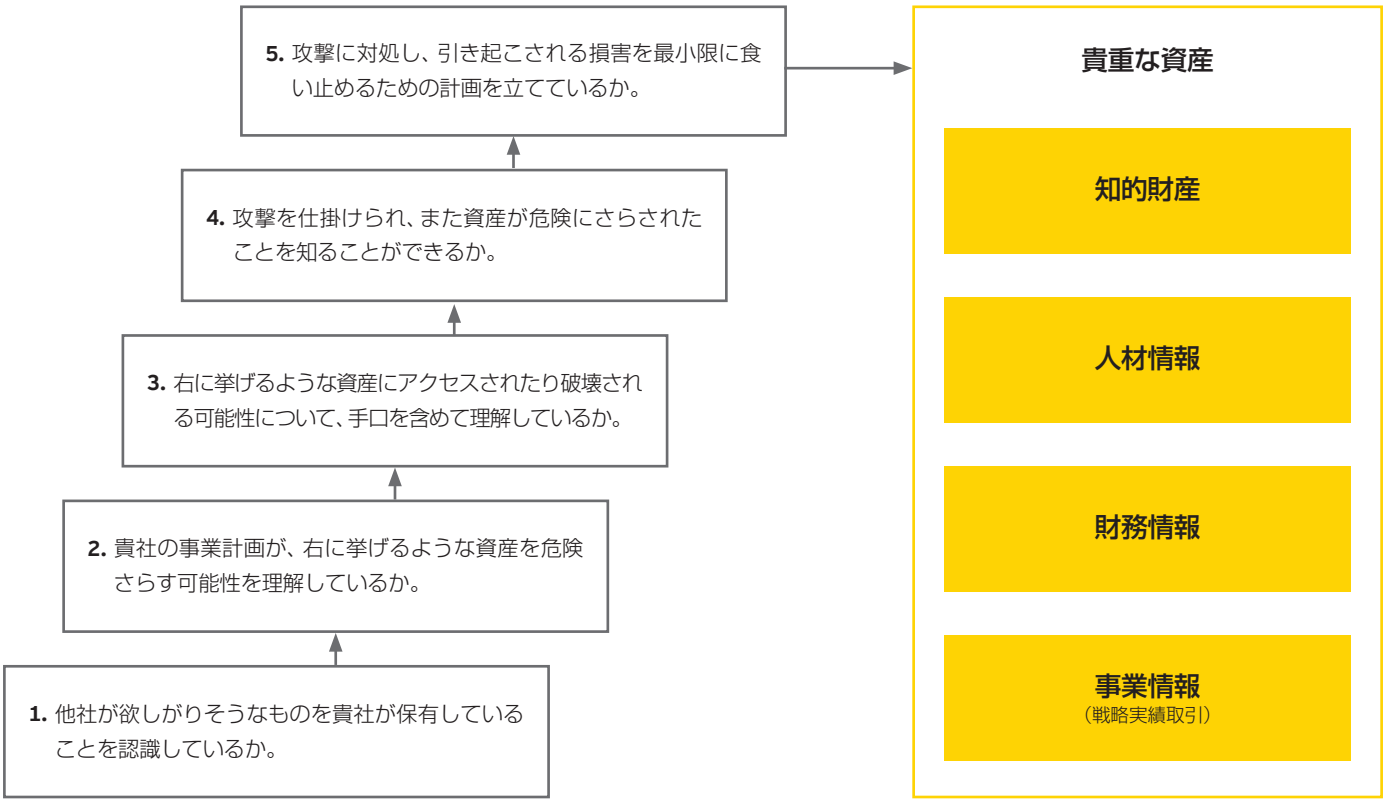
予想する準備を整える

準備が整った段階にある組織はまったく異なる考え方を持ち、世界を違った目で捉え、サイバー犯罪者が予想しないような方法で対応します。そのために、慎重に考え抜かれた、協力的な行動が求められます。そうした組織は学習し、準備し、予行演習します。いかなる組織や政府機関もすべての攻撃の予測や防御をすることはできないものの、標的としての魅力を減らし、攻撃に対する抵抗力を高め、想定される攻撃による損害を抑えることは可能です。

一歩先を維持する方法を学ぶことは、課題も多く時間がかかりますが、そうしたコストを費やすに足るメリットがあります。それによりデジタル世界によってもたらされる機会を活用しつつ、そのリスクの影響度とそれに対応するコストを最低限に抑えることが可能になります。

手始めに、組織とそのリーダーは以下の問いに対する答えを持っていなければなりません。回答の中に「いいえ」があれば、それがまさに焦点を当て、変更する必要がある分野なのです。

攻撃を受けることが避けられないとした場合、貴社はどのような準備を整えているでしょうか。5つの質問に対して「はい」と答えられるでしょうか。



以降では、組織が先手を打ち、上記の質問すべてに「はい」と答え、さらに先へ進むために今後何ができるかについて触れます。

自社の置かれた脅威環境を理解し、早期検知体制を確立する

脅威の存在を単に知るだけでは十分ではありません。組織は脅威の特質を理解し、どのように、かつどこで顕在化するか、また影響が及ぶものを評価し、理解する必要があります。侵害の早期警告や検知は、準備が整った状態に対する鍵となります。しかし、組織の大半は極めて単純な攻撃を探知できるにすぎません。これは、自社がより手のこんだ攻撃によってすでに侵害されていることを知らない可能性があること、そしてこうした特性を持つ将来の攻撃を検知できない可能性があることを意味しています。

サイバー脅威情報収集能力を統合または確立することは、組織がサイバー犯罪に先んじる助けとなり得ます。戦術的なレベルではSOCがこの能力を備えることになりますが、うまくいけばこの情報収集の役割は、戦略的レベル、経営幹部レベルにまで拡大します。

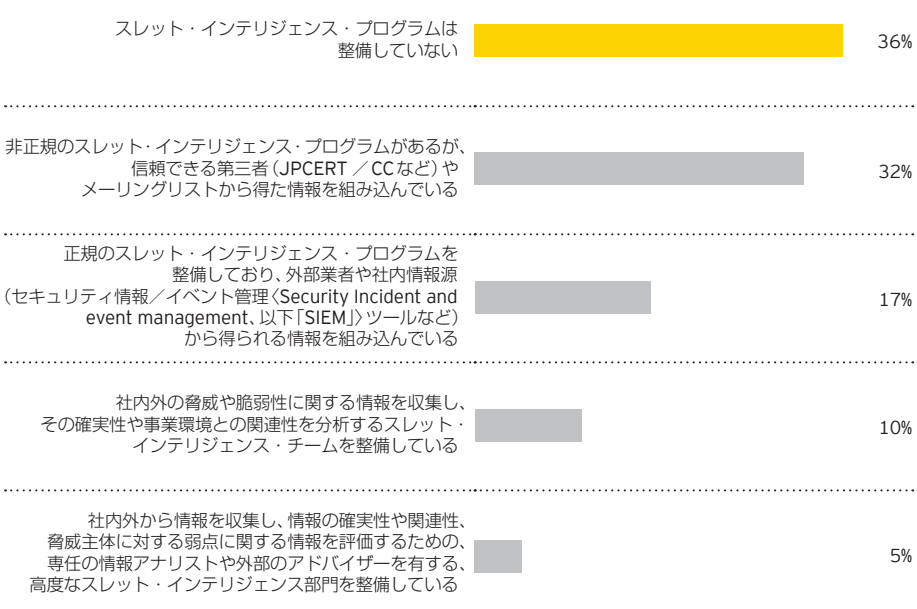
- 世の中で何が起きていて、そこから何を学ぶことができるか。
- いかにして「侮り難い標的」となることができるのか。また、「侮り難い標的」となることは必要か。
- 他の組織はどのようにして特定の脅威・攻撃に対処しているか。
- 他の組織が脅威や攻撃に対処することを助けることができるか。
- 標的として攻撃されているのか、「ランダムに」攻撃されているのかの違いを理解しているだろうか。
- どの脅威主体に関連付けられるだろうか。

このような質問は、サイバー脅威情報を通じてこうした回答を得ることができます。しかし、サーベイの結果からは、サイバー脅威情報がどのようなものであり、それが何をもたらすのかを把握している組織は少数にとどまっていることが示唆されています。

56%

の組織は、自社が高度な攻撃を検知できる可能性は低い、または極めて低いと回答しています。

貴社のスレット・インテリジェンス・プログラムの成熟度について、最もよく表しているものを一つ選択してください。



36%

の回答者が、スレット・インテリジェンス・プログラムを導入していない、と回答しています。

インテリジェンスは単に情報を収集するだけの活動ではありません。インテリジェンスのサイクルは一連の活動から成り立っています。

1. インテリジェンス要件の決定

何を認識する必要があるのか。知見の格差がどこにあるのか。

2. 情報収集

外部情報として利用可能なさまざまなオープンソースの情報提供元や内部のシステムからも多くのデータを得ることができます。

3. インテリジェンス・レポート作成を目的とした収集情報の分析および評価

分析や評価は外部委託することも、社内で実施することもできるでしょう。評価を有益なものにするためには、中核事業を理解することが極めて重要です。

4. 報告書を配布・伝達

5. 適切な措置を講じる

サイバー・スレット・インテリジェンスを有効なものにするためには、インテリジェンスのサイクルを迅速に実行する必要があります。一部の作業は自動化することができるため、技術やツール、サービスを利用することが可能です。自動化できない要素については、人の関与と介入が求められます。利用可能なサイバー・スレット・インテリジェンス・サービスはさまざま存在するため、組織の要件、選好度、成熟度に応じて個別に評価される必要があります。しかし、こうしたサービスの多くは、組織を無意味で実効性のない情報で溢れさせ、そのほとんどが無視される結果に終わるという欠陥があります。

サイバー・スレット・インテリジェンスでは、リスク管理で何らかの付加価値を生み出すには既存のネットワークやエコシステムに潜在する欠陥を指摘することが極めて有効であることも判明するかもしれません。それにより、より迅速な意思決定、データ保護の他、ギャップを明確化し、優先順位付けをしてそのギャップを埋めていくといった形で組織の機敏性を向上させるプロセスの変革につながることが見込まれます。確固としたスレット・インテリジェンス・プログラムは良質な指標プログラムと分析によりさらなる可能性を生み、多くの場合、企業のビッグデータプログラムとつながる可能性もあります。

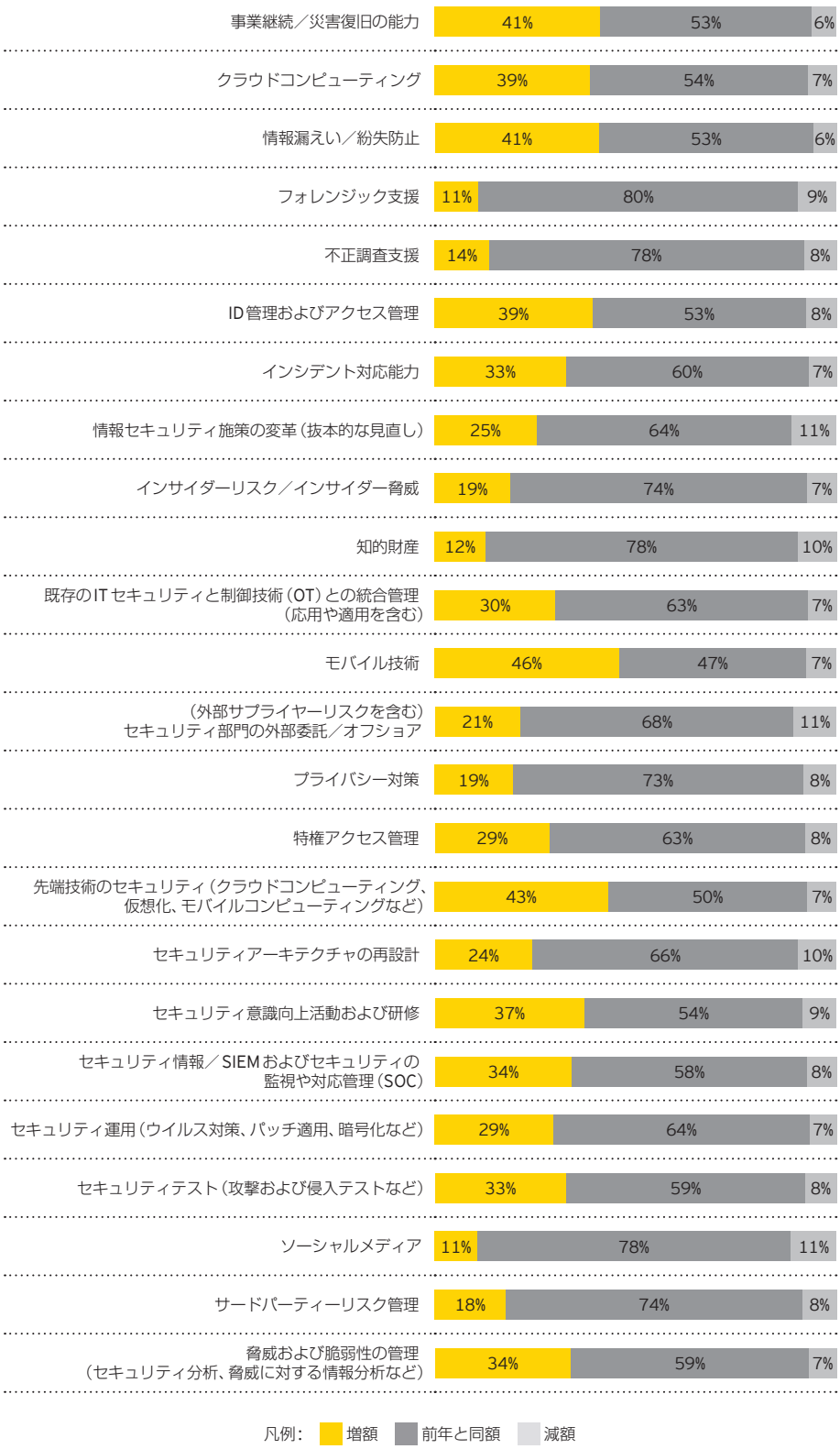
23%

の回答者が、自社の情報セキュリティ戦略の中で、今後3年から5年にわたる情報セキュリティの将来像に触れていると回答しています。

過去、現在、未来を見渡す

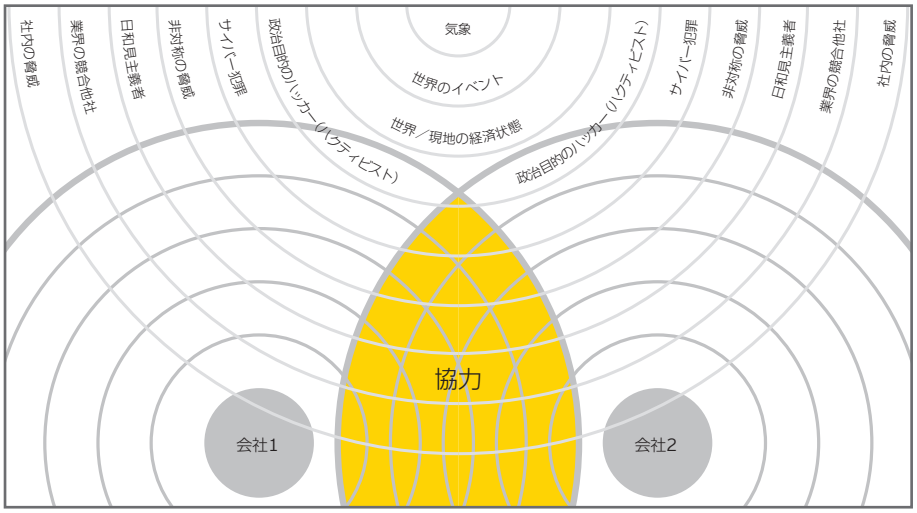
組織の大きな目標は、将来を見通すだけでなく、過去から学び、現在に備える取組みを網羅する必要があります。また、攻撃の種類、そして対処する方法やツール、技術における新たなトレンドやさまざまなトレンドに関する情報を常に収集している必要があります。入手した新しい技術に関する情報を事業で利用する機会を探索し続けると同時に、それによる新たなリスクの可能性と脆弱（ぜいじゃく）性に対して継続的に目を光らせることが極めて重要です。しかし、当法人の2014年の調査結果では、大半の組織が依然として現状に心を奪われ、将来に目を向けていないことが示されています。

当年度の予算を前年度と比較した場合、「増額」「減額」「前年と同額」から該当するものを一つ選択してください。



関与・協力する

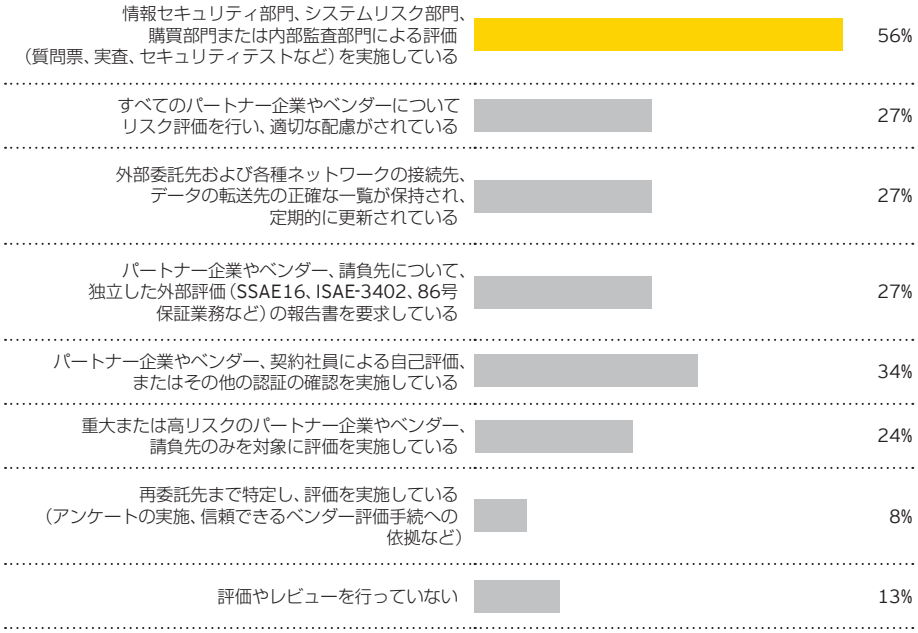
「Anticipate（予想する）」レベルでは、協力することが必要です。あらゆる組織（実際には個人）はこれらの問題に直面しています。また、能力が成熟するのに伴い、特に目標を定めた場合には、協力が成果を上げることを組織は学びつつあります。自社ネットワーク内の侵入を理解し、詳細な調査を行ってダメージの軽減に最も成功している組織の秘訣は、より大きなグループ（一時的、公式・非公式問わず）内で、都度、情報を事業のエコシステム全体にわたって共有していることです。



この図の中心にある協力の構成要素は、サイバー・スレット・インテリジェンスについても当てはまります。情報やインテリジェンスを共有するプラットフォームが、業種別、業種横断、国営、国家的なコンピュータ緊急対応チーム（Computer Emergency Response Team、「CERT」）と関連がある形態、政府の関与を伴う独立系事業体など、多くの形態で存在しています。政府や主要組織は（米国CERTのサイバー・レジリエンス・レビュー〈Cyber Resilience Review、「CRR」〉など）や、世界経済フォーラムの「サイバーレジリエンスのためのパートナーシップ（Partnering for Cyber Resilience、「PCR」）」といった抵抗力のあるサイバーエコシステム開発を支援する政策・実践の枠組みの中で主要な役割を果たし始めています。これらのフォーラムでは、緊急を要する情報を組織に配信するとともに、脅威主体と将来のシナリオ、軽減の技術、業界の背景および政府の行動に関する戦略的な洞察も提供しています。

また、協力関係は、パートナー企業とサプライチェーンに対する組織の認識を高め、エコシステム全体に影響を与えてそこから学ぶ力を、組織にもたらします。より大規模な組織では、自社のセキュリティ能力が一部のサプライヤーよりもはるかに成熟していることが多いため、サイバーセキュリティに関する知見の共有やサイバーセキュリティ活動のサプライヤーとの連携が、単独で行うよりもはるかに効果的であることを理解する必要があります。解決策の共有はエコシステム内部と周囲での防御を強化します。しかし、組織には認証、保証契約などに基づいた「信頼モデル」を構築することが求められます。いかなるインシデント対応の訓練も、より広いエコシステムにおける第三者と他の重要な組織を含める必要があります。

パートナー企業、ベンダー、請負先が貴社の情報を適切に取り扱い、管理するために実施している対策について、該当するものをすべて選択してください。



サイバーエコノミクス

以下の4つの質問は、サイバー攻撃の実際的な影響を評価し、最終的な収益や組織のブランド、評判に及ぼす影響を理解するものです。

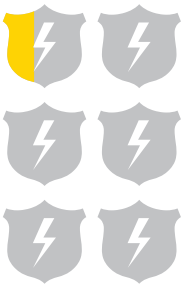
- 株価にどのような影響を与えるか。
- 顧客が影響を受ける可能性があるか。
- 売上高の減少につながるか。
- 攻撃に対して備えていないことが原因による社内システムすべてが受ける被害の修理やハードウエアの交換に掛かる費用はいくらになるか。

サイバーエコノミクスの手法は、サイバー攻撃の影響を数値化するために役立つよう開発されています。

サイバーインシデント訓練の実施

組織は攻撃された場合に何をすべきかを全員が分かっていると確信しているでしょうか。確信できない組織では、想定をはるかに超えた被害が予想されます。

サイバーインシデントへの不十分な対応が、多くの企業に深刻な影響を与えてきました。侵害が検知された場合でも、自社の重要な資産とそれに関連する悪影響に対して十分な知見を有していれば、適切に取り扱うメカニズムが動き始めるでしょう。株主、顧客、従業員、広報、規制当局などの当事者すべてが、攻撃をいかにうまく乗り越えるかを決定する上で何らかの役割を果たすのです。



6%

の組織が、第三者機関や法執行機関を含めた、より広範囲な脅威や脆弱性を管理する部門に統合された、強固なインシデント対応体制を整備していると述べています。

58%

の組織は新しい技術と情報セキュリティに対する新技術の影響に焦点を当てた部門や役割を有していません。

常に準備を整えておくためには、組織がすでにさまざまな攻撃シナリオの訓練を行っている必要があります。少なくとも年に1回は、複雑なサイバー攻撃シナリオ全体を通した危機対応メカニズムの訓練をする必要があります。この種の訓練を安全に、一方で現実的に実施するためのさまざまなサービスが利用可能です。困難である一方、学んだ教訓は有益なものだということが分かるでしょう。現在、サイバーシナリオの実施や結果報告を規制当局が求めている分野もあります。

EYのクライアント・サービス・チームは、サイバーセキュリティのシミュレーションとウォーゲームに着手している多くのリーディングカンパニーの取締役会と協力しています。組織の経営幹部がより広く真剣に考慮できるように、また、「Anticipate（予想する）」という正しい方向を目指せるように支援するためです。

行動を起こす――そして先んじる

すでに「Anticipate（予想する）」レベルに至っている場合、5つの重要な取組みにふれます。

1. サイバー脅威に対するインテリジェンス戦略の設計と実装

情報セキュリティ部門は取締役会との連携を通じて、戦略的な事業に対する決定を支援し、サイバーセキュリティの価値を活用するために、取締役会が脅威情報の利用方法を理解できるように支援しなければなりません。

2. 組織のサイバーセキュリティにおけるエコシステムの範囲とカバレッジの決定

組織の広範なエコシステムにおいて他者と連携し、RACIおよび信頼モデルを定義し、能力を共有した方が有利だと考えられるときは協力を取り付けます。

3. サイバーエコノミクスのアプローチ選択

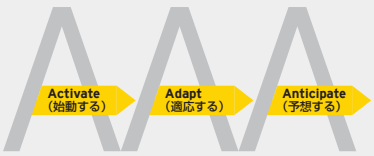
組織の中で最も重要なサイバー資産と、その資産が持つサイバー犯罪者にとっての価値を理解した上で、セキュリティへの投資計画を再評価します。

4. フォレンジックと分析の利用

最新の技術ツールを活用することによって、起こり得る脅威がいつ、どこから来ているかを分析し、それに対抗する能力を高めます。

5. 発生事象に対する全員の理解

強力なガバナンス、ユーザー管理、定期的なコミュニケーションによって、従業員は最新情報を受け取り、組織全体の「目と耳」の役割を継続的に果たします。



一つの企業、三つのストーリー

以下は三つの異なる方法で語られる、馴染みのあるストーリーです。これは架空の例ですが、対応、影響、出来事は私たちの顧客との実体験とその際に展開した出来事に基づいています。Activate（始動する）、Adapt（適応する）、Anticipate（予想する）のさまざまな局面にあるさまざまな企業は、極めて多様な方法でこれらのインシデントを特定し、反応・対応し、そこから回復するでしょう。当法人はそうした企業に対する影響を評価します。

1. 財務面 | 2. 運営面 | 3. 人事面

ケーススタディには、大規模な個人向け業務（400超の個人向け／顧客サービスセンター）を擁する大手通信事業者（売上高120億米ドル超）の三つのバージョン（Activate、Adapt、Anticipate）と対面およびオンラインでの顧客との直接的なやり取りが盛り込まれています。これらの企業は顧客データの侵害に見舞われますが、各社が非常に似通ったイベントに対して非常にさまざまな対応を行うことを目にすることになります。

Activate（始動する）

シナリオ： この企業は顧客データの重大な侵害に見舞われました。まず外部の情報筋によって発表され、最終的に同社が追認する形となりました。同社は、非常に迅速に対応し、侵害が発生したことを確認し、問題を特定し、解決し、影響は最小限にとどまったと公表しました。

ところが、1週間後、初めに発表した外部情報筋は、損害は同企業の確認した数字を大幅に上回り、何百万件ものクレジットカードの詳細情報が盗まれたと発表し、同企業はこれが事実であると認めました。情報筋はさらに新たな事実を見つけ出し、メディアではこのニュースが何度も取り上げられました。その後、最終的に失われた記録の数は当初言及された数字の10倍以上に上り、侵害がまだ継続し、しかも解決されていないことが判明しました。

財務面： メディアでは、最繁忙期直前までの2カ月間にわたって報道されました。同社は多数の顧客を失いました。最終的な損失は株価と売上高共に数十パーセント減少しました。1年以上たっても、侵害以前の数値に回復するに至っていません。侵害による最終的な費用総額は年間売上高の5%を上回ると予想されています。

運営面： 同社は、この問題（情報漏えい）の解決ではなく、問題そのものに（メディアの）焦点が当たってしまったことに対する対処に何カ月も追われ、発生したメディアリスクと危機管理への対応に労力を集中しました。同社はクレジット・モニタリング・サービスを指定・提供し、銀行や顧客と連携することで彼らの懸念を解消し、最終的に顧客の信頼回復を図る必要がありました。

人事面： この出来事は最高経営責任者（CEO）や最高情報責任者（CIO）を含め、組織全体にわたり多数の経営幹部や主だった責任者の解雇や辞任につながりました。

Adapt（適応する）

シナリオ： この企業は顧客データの重大な侵害に見舞われました。まず外部の情報筋によって発表され、最終的に同社が追認する形となりましたが、ほぼ1週間にわたりコメントを発表しませんでした。同社は極めて慎重な対応を行い、侵害を認め、侵害が起こった場所を特定していることを確認し、問題に対応したと確信しており、問題の程度を確認するため調査の完了を待っていると述べました。2週間後、公の場に姿を現し、損失総額を確認し、侵害の発生源を特定したことを確信し、軽減策が導入され、恒久的な解決に取り組んでいると発表しました。以降、矛盾する報告は行われていません。

財務面： このインシデントは三つの大きなニュース記事となりましたが、メディアに取り上げられていたのはごく短期間でした。侵害は重大なものでしたが、顧客離れには見舞われませんでした。同社はクレジット・モニタリング・サービスを提供し、顧客を店舗に呼び戻すため、コストを掛けて特別なキャンペーンを案内しました。3カ月以内に売上高、株価、業務は侵害前の水準に回復しました。

運営面： メディアは1カ月もたたないうちに関心を失いました。同社はメディアの圧力に対応するよりも、この問題の是正に対してより多くの時間と労力を費やしました。同社は銀行、ブランド、顧客と連携する必要があり、また、その労力は徐々に増加するサービスと事業のサポートに重点を置いたものとなりました。

人事面： この厳しい時期を通じて、同社は危機発生時に確固としたリーダーシップを示し、顧客、株主、取締役会の信頼を維持しました。

Anticipate（予測する）

シナリオ： この企業は顧客データに対する重大な侵害に見舞われました。攻撃の数カ月前、同社は同業他社、法執行機関および社内の脅威情報チームと協力してこの侵害に関連する攻撃者活動情報を収集し、同社に対するリスクを特定していました。また、業界内で生じた他の侵害についても学習していました。それにより、追加的な隔離・防御策を構築し、攻撃・対応訓練のシナリオを作成することができました。同社は最終的に攻撃の発生を食い止めることはできませんでしたが、支払明細やセンシティブな個人情報はすでに別に保管され、またさまざまな管理策によって保護されていたため、その損失を免れました。また、追加のモニタリングによって、攻撃はまず社内で発見されました。インシデント発生直後、何か発生し、それにどのように対応したかに関して同社の公式声明を発表しました。

財務面： 侵害からの回復費用は膨大なものでしたが、株価、顧客離れ、メディア報道に対する影響はごくわずか、もしくは皆無でした。費用は調査と是正対策に限定されました。同社は顧客データ侵害に対する通常の対応であるクレジット・モニタリング・サービスを提供する必要がないことに十分な自信を示すことで、メディアの過熱報道を抑えることができました。これだけで、少なくとも3億5,000万米ドルの潜在的な対応費用が節減されるとみられ、これが顧客と規制当局の信頼を高めたことは間違いありません。

運営面： 同社が発表した声明以外には、メディア報道は実質的にありませんでした。このため、同社は平常業務の回復に力を注ぐことができました。調査や是正のための費用は追加運営費となりました。また、侵害の調査は通常業務のプロセスに悪影響を及ぼすことなく、また侵害の結果生じる心理的な余波が生み出す頻繁なエラーから、その後も侵害を引き起こし得るといった、防御力の弱体化にはつながりませんでした。

人事面： 解雇または辞任は討議されず、経営幹部の間では新たな自信が現れています。

サマリー

組織は今

サイバーリスクは増大し、かつ急速に変化しています。サイバー犯罪者は、貴社を含め組織のセキュリティに侵入するため新たな技術の開発に日々取り組んでいます。彼らの目的は損害を与え、機密データにアクセスし、知的財産を盗むことです。彼らの攻撃は日増しに高度になり、防御するのが難しくなっています。

こうした進展が続いているため、来年、あるいは今後5年間、10年間にどのような種類の脅威が現れるかを正確に言うことはできません。ただ言えるのは、これらの脅威が現在よりもさらに危険になるということです。また、旧来のサイバー脅威源が消えて行くのに伴い、それに代わる新たな脅威源が現れることは確実です。

こうした不確実性にもかかわらず、つまりこうした不確実性ゆえに、必要とするサイバーセキュリティの種類について明確にしておく必要があります。

組織が必要とするもの

サイバーセキュリティを適正な状態にするための最初のステップは、適正な基盤を築くことです。最近のサイバー攻撃がいかに注目されているかを踏まえると、その危険を知らないなどと言うことは誰にもできません。ですから、組織が基本的なサイバーセキュリティシステムおよびプロセスをまだ導入していないということは言い訳にはならないでしょう。

基礎をいったんマスターすると、次の段階は自社のサイバーセキュリティをよりダイナミックにするとともに、主要な業務プロセスとの適合性と統合性を高めることです。この極めて重要な段階を踏まない場合、組織は依然として脆弱な状態にあります。組織とその環境、そして組織が直面するサイバー脅威がすべて変化しているときには、特に顕著になります。

この段階を経て、初めて真の機会、つまり、サイバー犯罪に先手を打つ機会が現れます。未知のもの、すなわち未来および広範なエコシステムに関するサイバーセキュリティに焦点を当てることにより、準備が整わないうちに脅威が発現することを避け、脅威を抑える能力の構築に着手できるのです。

構成要素	サイバーセキュリティシステムの構成要素	状態
「Anticipate（予想する）」は未知のものについて調査をすることです。サイバー・スレット・インテリジェンスに基づき、潜在的なハッカーを特定し、損害を与えられる前に措置を講じます。	**Anticipate（予想する）**	**「Anticipate（予想する）」**は新たに出現したレベルです。サイバー犯罪に先手を打つため、サイバー・スレット・インテリジェンスを利用する組織がますます増加する中、以下のステージを革新的に強化します。
「Adapt（適応する）」は変化に関することです。サイバーセキュリティシステムは、環境の変化に伴い変化し、企業の明日を保護することに焦点を当てています。	**Adapt（適応する）**	**「Adapt（適応する）」**は広範囲にはまだ実行されていません。組織の事業が変更するたびに、サイバーセキュリティの意義が評価されることは、まだほとんどありません。
「Activate（始動する）」はサイバーセキュリティの各ステージを設定します。つまり、企業を今日と同様に保護することに焦点を当てた複雑な一連のサイバーセキュリティ対策です。	**Activate（始動する）**	**「Activate（始動する）」**はすべての組織におけるサイバーセキュリティシステムの一部ではあるものの、必要なすべての措置が講じられているわけではなく、まだやるべきことがたくさんあります。

組織が向かう先は

組織は将来を見越し、事業の先に目を向けなければなりません。すなわち、今日も作られている新しい脅威に対し、先手を打つ必要があります。今回のサーベイからは、その状態にすぐに達するとは考え難いものの、私たちはすべての組織にとって先見的でインテリジェントなサイバーセキュリティが標準となることを望んでいます。

私たちは企業に対する壊滅的な攻撃、あるいは広報を襲う災難ではなく、組織を強化することに焦点を当てたいと考えています。なぜなら、企業には、革新的で新しいアプローチを導入し、強力な新ツールを利用してこれまで以上に強力で安全な組織にする基盤がすでにあるからです。私たちは企業がイニシアティブを取ることで、サイバー犯罪がもうからず時間と労力の無駄になるようにしたいと考えています。言い換えれば、ハッカーの勢力を排除し、サイバー犯罪に先手を打ちたいと考えているのです。

EYがお手伝いできること

EYでは、組織のリスクすべてに関して統合的な視点を持っており、サイバーセキュリティは鍵となる重点分野です。モバイル技術、ソーシャルメディア、クラウドコンピューティングが普及しつつある現在、EYは、これらの分野ではリーダーとして認められています。

私たちのサイバーセキュリティの専門家は業務運営に対する情報およびサイバーセキュリティ・リスクを管理するという課題に取り組んでいます。私たちのグローバルな組織から得られる業界最高レベルの詳細な技術やIT関連のリスク管理の知見を活用することによって、統制の設計、実装、合理化に焦点を当てたIT統制サービスを提供しています。これにより、皆様のアプリケーション、基盤、データにおけるリスクを低減できる可能性があります。

サイバーセキュリティについては、取締役会で定期的に議論されていますが、私たちは事業への影響と技術的な詳細、そしてこのような課題を経営幹部にどのように提起するかを知っています。事業への影響や技術的な詳細は、リスクに対するより深い洞察と経営幹部によるより詳細な議論につながります。また、資産を保護・確保するという課題に直面しているクライアントに対し、私たちは信頼の置けるアドバイザーになることを目指しています。
当法人は以下の点で顧客を支援します。

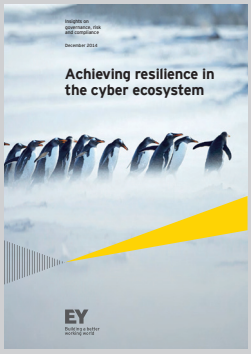
- 情報セキュリティ戦略をビジネスニーズと整合させる
- 複雑なサイバー侵害を封じ込め、かつ調査し、検知・対応アプローチを是正する
- 情報セキュリティコストを最適化し、サイバー・プログラム管理（Cyber Program Management、「CPM」）の費用効率性と持続可能性を高める
- SOCの能力を改善する
- モニタリング、保守、アクセス管理方針の遵守、ならびに法律および規制遵守の達成を支援する
- 技術とプロセスの実装に要するリソースとスキルの適性を評価する

私たちのサイバーセキュリティ・サービスには、サイバー犯罪に先手を打つため、当報告書で論じた「**Activate（始動する）**」、「**Adapt（適応する）**」、「**Anticipate（予想する）**」といった重要なファクターを盛り込んでいます

より深く知るには？

『**Insights on governance, risk and compliance**』は、IT・ビジネスリスクに関連した課題・機会に焦点を当てたシリーズです。これらは最新の論点に基づいてタイムリーに解説されています。GRC理解の一助として、価値ある考察を提供いたします。
『Insights on governance, risk and compliance』シリーズについての詳細は、EYのホームページhttp://www.shinnihon.or.jp/services/advisory/risk-advisory/global-contents/index.htmlをご覧ください。

"Cyber Threat Intelligence – how to get ahead of cybercrime"
（英語版のみ）
www.ey.com/CTI



"Achieving resilience in the cyber ecosystem"
（英語版のみ）
www.ey.com/cyberecosystem

"Cyber Program Management: identifying ways to get ahead of cybercrime"
（英語版のみ）
www.ey.com/CPM

"Security Operations Centers – helping you get ahead of cybercrime"
（英語版のみ）
www.ey.com/SOC

『プライバシートレンド2014:
テクノロジーの時代における
プライバシー保護』
www.shinnihon.or.jp/tl/privacytrend2014

"Maximizing the value of a data protection program"
（英語版のみ）
www.ey.com/dataprotect

"Building trust in the cloud"
（英語版のみ）
www.ey.com/cloudtrust

『アイデンティティ・アクセス管理:
コンプライアンスのその先へ』
www.shinnhion.or.jp/tl/iam

『ビッグデータ:
企業の競争と業務に変革を起こす』
www.shinnhion.or.jp/tl/bigdata

サーベイの方法について

EYグローバル情報セキュリティサーベイは2014年6月から2014年8月にかけて実施されました。60カ国における主要な業種すべてにわたる1,800人以上が回答しています。

サーベイで、当法人は最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、最高財務責任者（CFO）、最高経営責任者（CEO）、その他の情報セキュリティの幹部の参加を呼びかけました。各国で指名されたEYの専門家に対し、グローバルで一貫した調査を行うための指示とともに質問内容が配布されています。

回答の大半は対面インタビューで行われました。インタビューができなかった場合には、オンラインで回答を得ました。

今後、EYグローバル情報セキュリティサーベイへの参加を希望される場合には、EYの担当者または現地のオフィスにご連絡いただくか、www.ey.com/gissにアクセスして、簡単なリクエスト用紙にご記入ください。

エリア別の回答者内訳
（回答者数：1,825人）

エリア：

EMEA（欧州、中東、インド、アフリカ）	39%
Americas（北・中・南米）	26%
Asia-Pacific（アジア・太平洋）	22%
Japan（日本）	13%

企業の年間総売上高別の回答者内訳

年間総売上高：

100億～500億米ドル	167
10億～100億米ドル	441
1億～10億米ドル	479
1,000万～1億米ドル	314
1,000万米ドル未満	209
政府機関・非営利団体	119
該当なし	215

回答企業の業種別内訳

航空宇宙・防衛	63
資産運用	60
自動車	62
銀行・資本市場	308
環境保全技術	2
消費財	132
各種工業製品・化学品	146
政府機関・公的セクター	119
ヘルスケア・介護	70
保険	138
生命科学	40
メディア・娯楽	44
鉱業・金属	43
石油・ガス	55
電力・公益	68
プライベートエクイティ	1
プロフェショナルファーム・サービス	68
不動産	56
小売・卸売	100
テクノロジー	117
通信	62
輸送	71

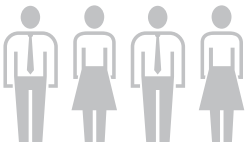
回答企業の従業員数別内訳

1,000人未満	664
1,000～5,000人	557
5,000～1万5,000人	283
1万5,000～5万人	194
5万人以上	127

回答者の職務・役職別内訳

最高情報責任者（CIO）	208
最高情報セキュリティ責任者（CISO）	283
最高セキュリティ責任者（CSO）	54
最高技術責任者（CTO）	41
情報セキュリティ役員	233
情報技術役員	346
内部監査取締役／マネジャー	72
ネットワーク／システム管理者	38
他の経営幹部／役員／バイスプレジデント	60
その他	490

参加者のプロフィール



1,825
人の回答者

世界
60
カ国

25
の業種

連絡先

当法人は組織のリスクのすべての面に関して統合的な視点を持っています。内部監査、財務リスクおよび統制のマーケットリーダーであり、ガバナンス、リスク、コンプライアンス、ならびに企業リスク管理などの他の分野においても引き続き能力の向上を図っています。

当法人は競争優位を維持するためにリスクコンサルティング、リスク分析、リスク技術などの分野で革新を進めています。業界最高レベルの詳細な技術・IT関連のリスク管理の知見を活用し、制御の設計、実装、合理化に焦点を当てたIT制御サービスを提供しています。これにより、顧客のアプリケーション、インフラ、データにおけるリスクを低減できる可能性があります。情報セキュリティは鍵となる重点分野であり、モバイル技術、ソーシャルメディア、クラウドコンピューティングが普及しつつある現在、当法人はこの分野におけるリーダーリーダーとして認められています。

当法人のリスク・リーダーは以下の通りです。

Japan		
東 義弘	+81 3 3503 3500	azuma-yshhr@shinnihon.or.jp
Global		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
Europe, Middle East, India and Africa (EMEIA)		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com

当法人のサイバーセキュリティ・リーダーは以下の通りです。

Japan		
遊馬 正美	+81 3 3503 3500	asuma-msm@shinnihon.or.jp
Global		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
Europe, Middle East, India and Africa (EMEIA)		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 6309 8890	paul.o'rourke@sg.ey.com

EY | Assurance | Tax | Transactions | Advisory

EYについて
EYは、アシュアランス、税務、トランザクションおよびアドバイザリーなどの分野における世界的なリーダーです。私たちの深い洞察と高品質なサービスは、世界中の資本市場や経済活動に信頼をもたらします。私たちはさまざまなステークホルダーの期待に応えるチームを率いるリーダーを生み出していきます。そうすることで、構成員、クライアント、そして地域社会のために、より良い社会の構築に貢献します。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。詳しくは、ey.com をご覧ください。

新日本有限責任監査法人について
新日本有限責任監査法人は、EYメンバーファームです。全国に拠点を持つ日本最大級の監査法人業界のリーダーです。監査および保証業務をはじめ、各種財務アドバイザリーの分野で高品質なサービスを提供しています。EYグローバルネットワークを通じ、日本を取り巻く経済活動の基盤に信頼をもたらし、より良い社会の構築に貢献します。詳しくは、www.shinnihon.or.jpをご覧ください。

ED None

本書は SCORE no. AU2698の翻訳版です。

新日本有限責任監査法人
アドバイザリー事業部
〒100-6028
東京都千代田区霞が関三丁目2番5号
霞が関ビルディング28F
Tel: 03 3503 3500
E-mail: As-Markets@shinnihon.or.jp