Insights on
governance, risk
and compliance

# デジタル社会に信頼を築く

## EY グローバル情報セキュリティ サーベイ 2015

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・
アドバイザリー
リスク・リーダー

ケン・アラン
EY グローバル・
アドバイザリー
サイバーセキュリティ・リーダー

**「デジタル社会に信頼を築く――EY グローバル情報セキュリティサーベイ（GISS）2015」へようこそ。18年目を迎える今回のサーベイでは、今日のビジネスで直面する最重要課題の一つであるサイバーセキュリティについて調査しました。**

今年のサーベイは1,755の組織にご参加いただきました。本報告書は、今回のサーベイの結果から得られた洞察と、世界中のクライアントへ品質の高いサイバー・セキュリティ・ソリューションを提供しているEYの幅広い経験に基づいて作成しています。

昨年の報告書では、Activate（始動する）、Adapt（適応する）、Anticipate（予想する）の3ステージをたどることで、サイバー犯罪に先手を打つ方法を解説しました。この概念が今後も有効であることに変わりはありません。しかし、サイバー攻撃は次々と戦術を変え、執拗（しつよう）さを増しており、サイバー空間における脅威はますます深刻化しています。急速に進むデジタル化による企業間の相互接続の拡大や、モバイル技術やインターネットとの結び付きが強くなっている個人の生活の変化を悪用して、攻撃者は常により新しく巧妙な手口を探究しています。

こうした状況に対して頭を悩ませているのは、貴社だけではありません。今回のサーベイ参加者の3分の1以上が、高度化していくサイバー攻撃を自社で発見できる自信がないと回答しています。長期的な攻撃の兆候である、わずかな異変に気付くことができるのは、とりわけ用心深い組織だけでしかないことを、我々は経験から知っています。

今や、サイバーセキュリティはテクノロジーを超えた問題として、IT領域だけにとどまらなくなっており、取締役会の誰かに一任できる問題ではありません。サイバーセキュリティの問題は、ビジネスのあらゆるレベルと、経営幹部が担当するすべての分野に、一見しただけでは気付かないようなさまざまな影響を及ぼします。本報告書では、今まさに、攻撃者が組織の重要な価値に打撃を及ぼしかねない情報を収集しているかもしれないこの状況の下で、組織横断的に各部門が協力し、攻撃の証拠を蓄積するための知見を共有する方法について考察します。

目標は、サイバー攻撃に対して先手を打ち続けることです。これは、今日では、「アクティブディフェンス」の体制を維持し続けることを意味します。本報告書では、アクティブディフェンスの維持とは何か、EYがどのようにお役に立てるかを説明します。

サーベイにご参加くださったクライアントの方々に深く感謝するとともに、本報告書が皆様にとって有意義であることを願っています。

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

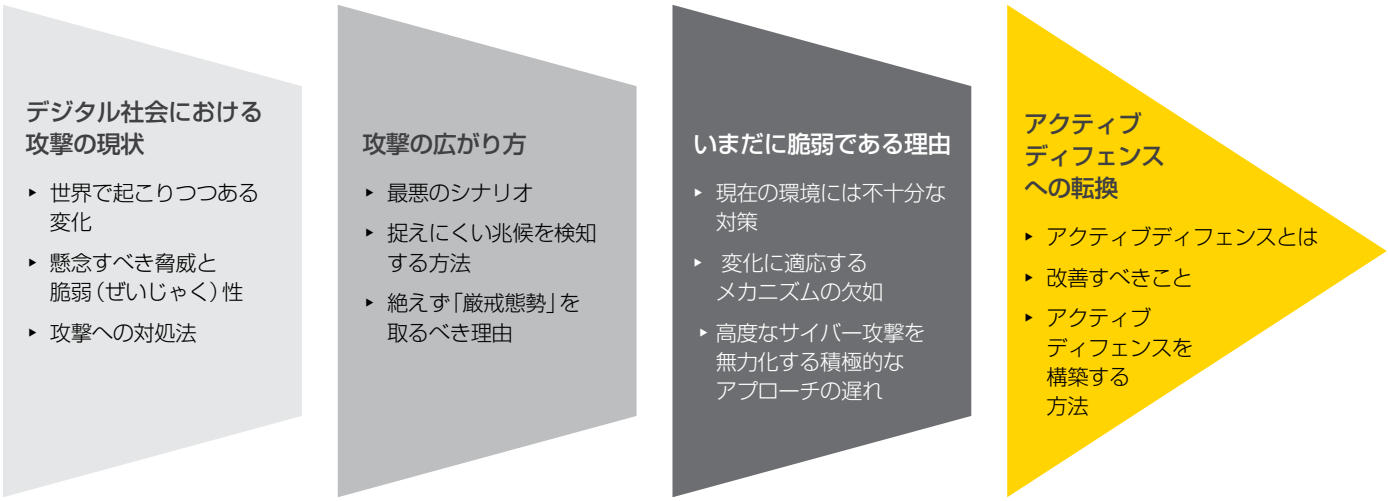
**ケン・アラン**
EY グローバル・アドバイザリー
サイバーセキュリティ・リーダー
kallan@uk.ey.com

## サイバーセキュリティの課題を理解する

デジタル社会には、急速に広がるイノベーションの可能性が満ちあふれ、その多大なメリットに企業、行政機関、個人からの注目が集まっています。今までにない市場や新製品に対して、消費者や市民が理解を深めることで、さまざまな形で人々がつながりを持つデジタル社会には、大きな可能性が秘められています。

一方で先を急ぐあまり、多くの予防措置が見落とされ、リスクを過小評価するといったことが起きてきました。また、デジタル社会の裏側では、営利目的の犯罪者や愉快犯が付け入る隙も非常に大きいという現実があるものの、まだ十分に認識されていません。人や組織、そして「モノ」が複雑に相互接続することで、予期せぬ事態が起こりつつあることに対して、危機感を抱く必要があります。

**現在の課題を認識し、課題に対して何をすべきかを組織が理解するには、以下の4つの分野全体を考慮することが重要です。**



# デジタル社会における攻撃の現状

88%

が、自社の情報セキュリティ機能は組織のニーズを十分に満たしていないと回答

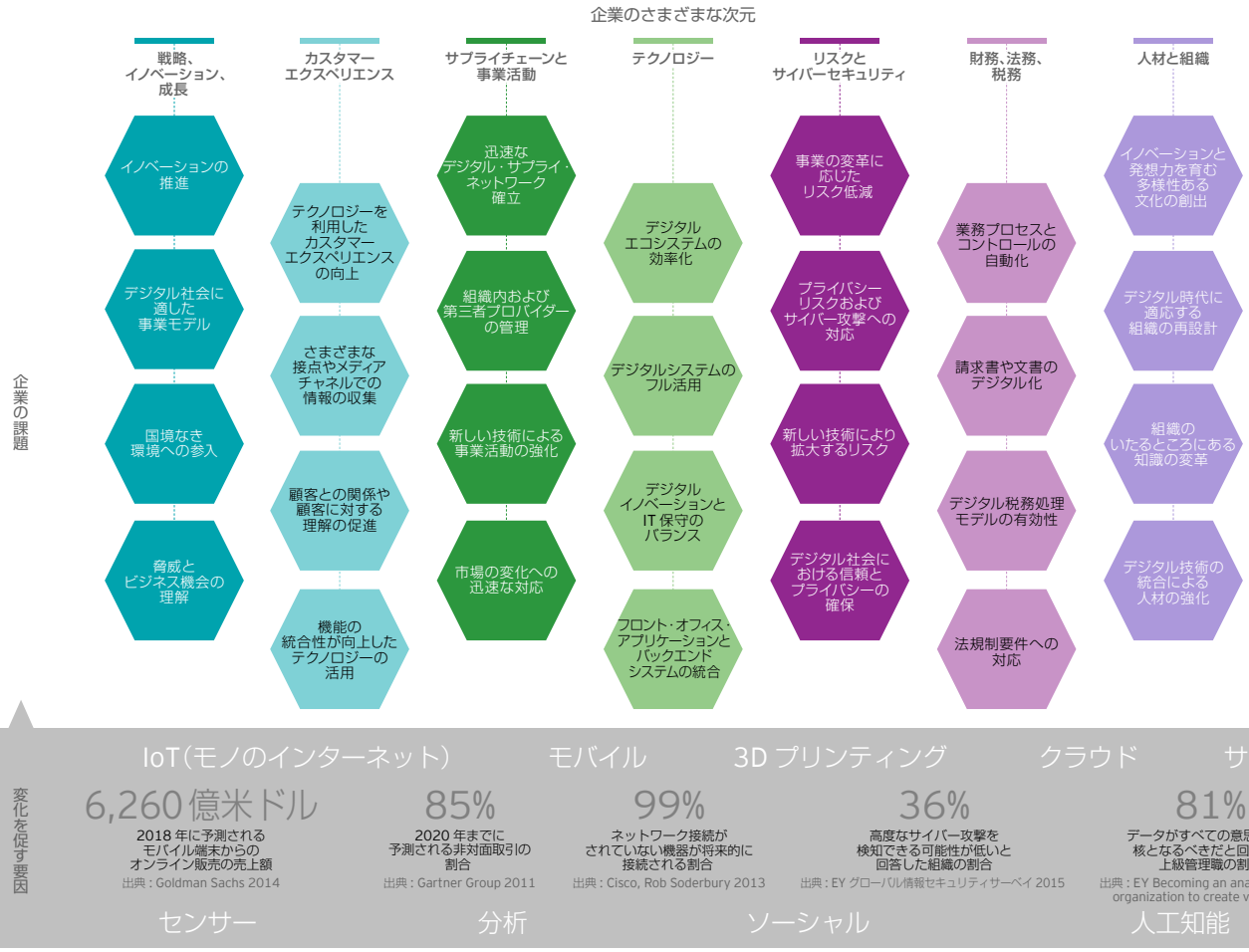
## 世界で起こりつつある変化

激変する環境の中でも、組織には事業活動を続けていく必要があり、サイバー空間と現実世界の間で起こるさまざまな出来事に、組織やメディアから注目が集まるのは必然といえます。顧客にとって、個人情報の流出や悪用は、到底容認できるものではありません。また、知的財産の窃盗は、利益損失や信頼回復のためのコスト負担へつながると同時に、組織発展を阻害します。さらには、メディア、通信、行政、防衛システムに対するハッキングや不正操作は、国家安全保障上の重大な脅威となります。

**組織とその中の人々にとって、デジタル社会を生き抜くということの意味がどこまで理解されているでしょうか？**

組織全体を「サイバー」という切り口から見つめ直し、以下の分野すべてについて考察する必要があります。

### デジタルによる機会と持続可能性のためのサイバーセキュリティの利用




変化を促す要因

| IoT（モノのインターネット） | モバイル | 3D プリンティング | クラウド | サイバー |
|---|---|---|---|---|
| 6,260億米ドル | 85% | 99% | 36% | 81% |
| 2018 年に予測されるモバイル端末からのオンライン販売の売上額 | 2020 年までに予測される非対面取引の割合 | ネットワーク接続がされていない機器が将来的に接続される割合 | 高度なサイバー攻撃を検知できる可能性が低いと回答した組織の割合 | データがすべての意思決定の核となるべきだと回答した上級管理職の割合 |
| 出典：Goldman Sachs 2014 | 出典：Gartner Group 2011 | 出典：Cisco, Rob Soderbury 2013 | 出典：EY グローバル情報セキュリティサーベイ 2015 | 出典：EY Becoming an analytics-driven organization to create value 2015 |
| センサー | 分析 | ソーシャル | | 人工知能 |

**デジタル社会における事業活動――新たな課題**

- 「スマート」デバイスや関連サービスの誕生による意図しない結果や大量のデータの発生、そして悪用につながる脆弱性の増大。多くの場合、意思決定プロセスに人が介在していない。
- ソーシャルメディアやBYODを利用する従業員、クライアント、一般の人々による「常時接続」状態や情報の共有。プライバシーや機密性への影響について十分に理解されていない可能性。
- クラウド上や外部委託先に保存されるデータの増加。便利な一方、危険を伴い、制御が困難。増加する脅威と予想もしないデバイスやシステムからの接続、すなわち、複雑なエコシステムの形成。
- 人々の行動の変化における、プラスとマイナスの両面。
- 多数の新しい法律や規制によって義務付けられる業務プロセスの変更が新たな脆弱性を誘発し、そのたびに脅威の展望や攻撃の対象となる範囲は更に変化する。

68%

が、「自社や他社との境界を含めたビジネスエコシステムの監視」を、IoT（モノのインターネット）における情報セキュリティの課題として認識していないと回答

## 懸念すべき脅威と脆弱性とは

デジタル社会の中で、組織がより安全で持続可能性のある環境へ移行していくためには、組織活動すべてにおけるサイバーリスクを踏まえることが重要です。

これまで以上に大きな脅威にさらされているにもかかわらず、あまりにもたくさんの組織がリスクや脆弱性に対して、場当たり的に対処しています。これは組織内の1人や2人に任せておけば済む問題ではありません。組織およびエコシステム全体にわたって、個々の責任を詳しく定め、それを誰でもアクセス可能な状態で一元的に管理する必要があります。取締役会や経営幹部と従業員とでは、閲覧できる情報は異なるでしょう。それは、パートナー、サプライヤー、ベンダーなどの外部関係者では閲覧できる情報が異なるのと同じことです。

ここで重要なのは、大量のデータに圧倒されるあまり、不要な仕事やリスクを作り出さないようにすることです。組織にとって、包括的で効果的なサイバー・セキュリティ・アプローチの優先度を明確化し、無駄を省き、緻密に策定することが重要です。組織のビジネス戦略、リスク、優先事項に見合ったサイバー・セキュリティ・アプローチを策定してこそ、真の価値が得られます。

その上で、さまざまなリスクと脅威の中で、効率的に組織を導いていくためには、リーダーがリスク選好度を適切に設定し、インシデントが発生したときは、断固たる措置をすばやく実行できるよう準備を整えておく必要があります。ここ数年の間に注目された話題として、サイバーインシデントに対する適切な対策と、組織内外への影響に対処するための効率的なコミュニケーションが確保されたリーダーシップによって、インシデントの影響が大幅に削減された事例がありました。

67%

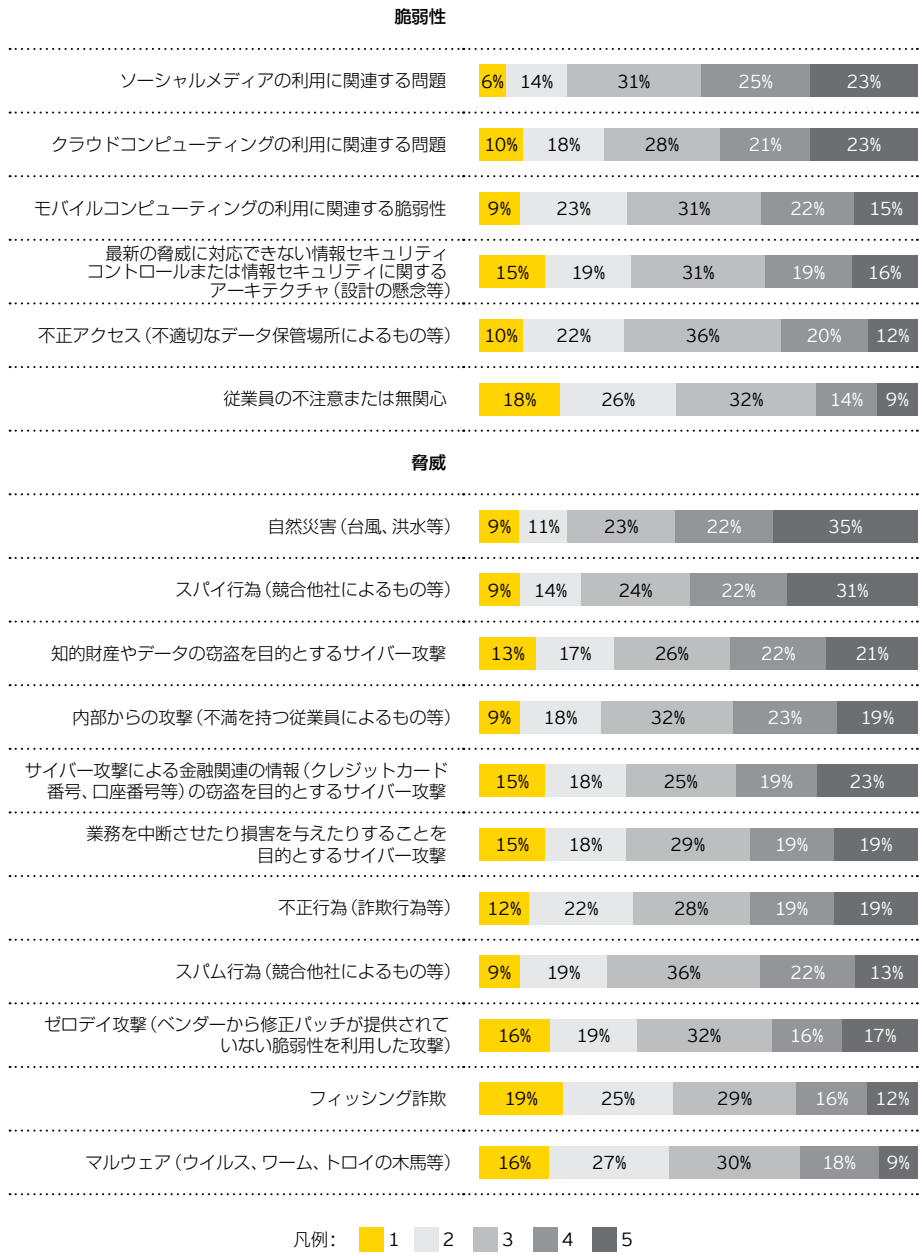
が、「組織へのアクセスポイントの増加への対応」を、IoT（モノのインターネット）における情報セキュリティの課題として認識していないと回答

**次の点について考察する必要があります。**

- デジタル社会に存在する脅威・脆弱性について、理解しているという確信を持っているか？
- デジタル社会における脅威の展望が、組織と戦略にどう結び付くかを判断し、その結果に基づいてサイバーセキュリティ対策を優先順位付けしているか？
- サイバーインシデント対応管理プログラムの策定に当たり、潜在的なインシデントによる損失や損害のうち、許容可能なものとそうでないものとを区別するためのリスク選好度を設定するノウハウがあるか？

取締役会が納得し、なおかつ組織が達成可能なリスク選好度を設定して、初めて持続可能なデジタル変革となります。

**過去12カ月間（または前年）に、貴社に大きな影響を与えた脆弱性*および脅威**は何ですか？**
（以下の項目すべてについて「最高の優先度」1から「最低の優先度」5までで評価）




* 「脆弱性」とは、攻撃や危害を加えられる可能性が存在することを表します。
** 「脅威」とは、外部環境の行為者による悪意の行動の可能性を表します。

## 2014年との比較から分かる2015年の状況

**脆弱性のトップ2は**

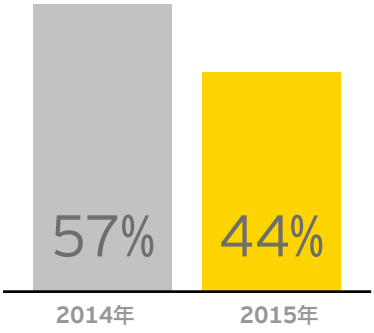
- 従業員の不注意または無関心
- 最新の脅威に対応できない情報セキュリティコントロールまたは情報セキュリティに関するアーキテクチャ（設計の懸念等）

2014年も本年と同様に、この二つの脆弱性への優先度が高い結果でした。しかし組織が実感する脆弱性の度合いは低くなっています。従業員の無関心に関連する脆弱性を挙げた回答は44%で、2014年の57%から低下しています。最新の脅威に対応できないシステムに起因する脆弱性については34%と、これも2014年の52%から低下しています。このことから、脆弱性に対し、より効率的に対処できるようになったと、組織が自己評価していることが分かります。

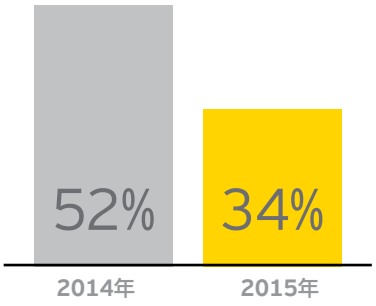
**対して、現状の脅威トップ2に目を向けたとき示唆するものは**

- フィッシング詐欺
- マルウェア（ウイルス、ワーム、トロイの木馬等）

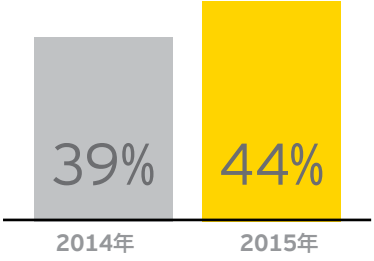
これらの脅威は、2014年のサーベイではそれぞれ5位と7位にランクされており、金融関連の情報や知的財産の窃盗、詐欺、スパイ行為、ゼロデイ攻撃の方が大きい脅威であると見なされていました。フィッシングとマルウェアに対する警戒感の急速な高まりは、脅威に対する認識が明らかに変化していることを物語っています。しかし、それは正しいのでしょうか、それとも間違った方向へ向かっていることを意味するのでしょうか？



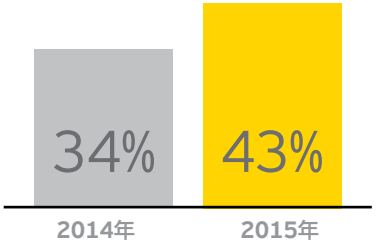

44%が、従業員の無関心に関連する脆弱性が懸念されると回答（2014年のサーベイでは57%）




34%が、最新の脅威に対応できないシステムに起因する脆弱性を指摘（2014年のサーベイでは52%）




44%が、フィッシング詐欺が現時点で最大の脅威と認識（2014年のサーベイでは39%）




43%が、マルウェアを現時点で最大の脅威と認識（2014年のサーベイでは34%）

42%

が、すべての資産について把握することが情報セキュリティの重要な課題だと回答

## 攻撃に対する準備はできているでしょうか？

今後、貴社はサイバーインシデントを経験することになるでしょう。これはデジタル化の進行による必然的な結果です。

組織としてサイバーインシデントに立ち向かうための出発点は、状況認識です。すなわち、サイバー攻撃者の立場から、貴社がどのように映っているかを理解するということです。

- 攻撃者が何を狙っているかが分からない場合、サイバーインシデントから組織を守れるでしょうか？
- 攻撃者はどのような手口で侵入するのでしょうか？また、それによりどのような損害が貴社とその重要資産に生じるでしょうか？
- 攻撃の検知、封じ込めから回復へ至るまでの具体的プロセスを理解していないのに、立ち向かう自信をもてるでしょうか？

多くの組織はリスクマネジメントの原則に慣れ親しんでいます。優れたリスクマネジメントの原則はサイバーセキュリティを考察する出発点として有益です。

| 主なリスクマネジメントの原則 | サイバーリスクへの適用 |
|---|---|
| 1 **最重要事項へのフォーカス**<br>固有のビジネスとリスクカルチャーの整合性 | **重要な情報資産の把握**<br>サイバー攻撃に対して最も脆弱な重要ビジネス資産の特定 |
| 2 **測定とレポート**<br>定性的な記述と定量的な測定値を使用 | **サイバーリスクのさらなる可視化**<br>サイバーリスクと基準となる指標の明確化 |
| 3 **網羅性**<br>現在と将来にわたるあらゆるリスクに対応 | **既存のリスクフレームワークとの整合性**<br>財務、業務、規制、クライアント、評判など |
| 4 **リスク選好度の割当て**<br>事業部門別、リスク種類別の選好度の割り当て | **ビジネスとサイバーリスクの関連付け**<br>組織レベルのリスクの、個々の事業部門と情報資産レベルへの落とし込み |
| 5 **事業計画とセキュリティ戦略の統合**<br>エビデンスを求める規制当局の動きが活発化 | **投資判断へのリスク選好度の組込み**<br>重要な分野への優先的な投資や、情報に基づく意思決定によるビジネス強化 |

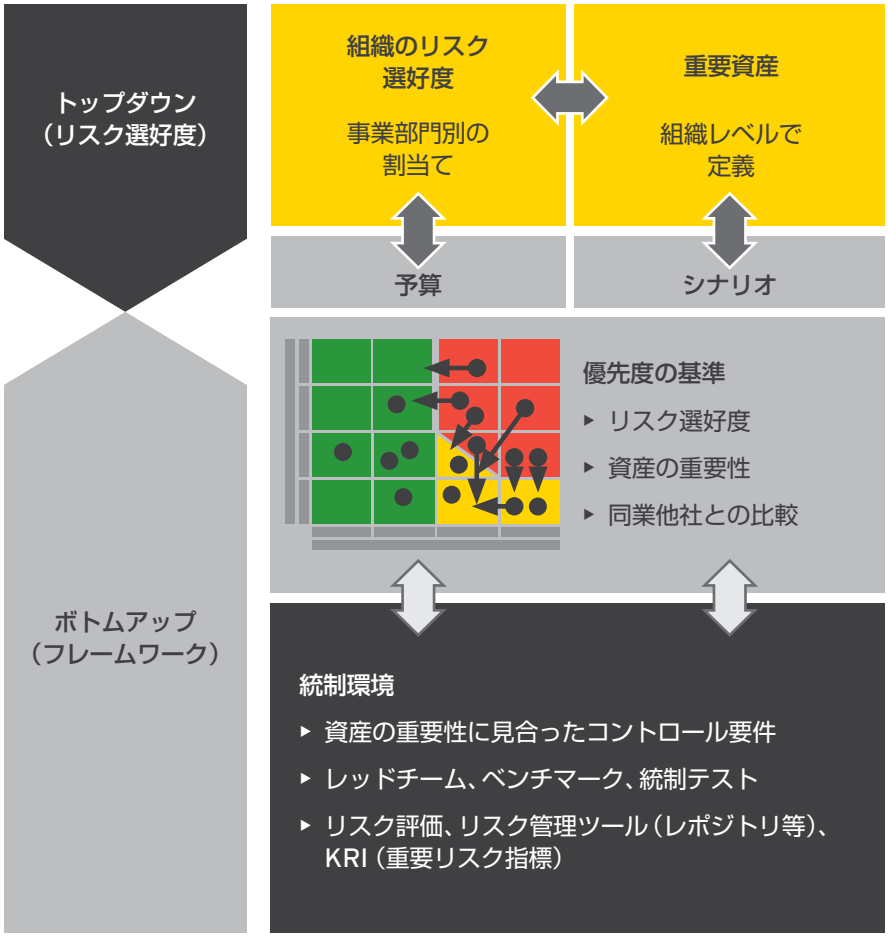
システムやサイトの機能停止を伴う大規模な侵害や、結果として消費者が被る損害や不都合など、サイバーインシデントは衝撃的な事件として報道されることがあります。何百万人分もの口座情報の盗難、膨大な量の機密情報のオンライン流出、知的財産の窃盗やシステム障害の発生などの大規模な事象が、トップ記事となり注目されます。

しかし、そうしたニュースは突然、降って湧いたわけではありません。攻撃の大部分は、何週間または何カ月も前から計画されています。サイバー犯罪者は、侵入の糸口を見つけ貴重な資産のありかを探り始めた時点から、その計画を密かに企てています。

さらにサイバーインシデントは、複雑なものか、単純なものか、あるいは特定のターゲットを狙ったものか、無差別かを問わず、1回で終わるものではありません。初期のわずかな兆候や、繰り返される攻撃による影響を理解し、計画やリスク選好度を決定する際に考慮に入れる必要があります。

20%

が、この12カ月で起きたサイバーインシデントに関する財政的な損失額は推計できないと回答




**レッドチームの編成：**レッドチームとは、侵入テストやソーシャルエンジニアリングなど、具体的な演習などを通じて、組織のセキュリティ強化を積極的に図るための活動を行うグループを指します。

**真のリスクを識別**

- リスク選好度と重要情報資産をトップダウンで定義
- システムと事業部門（および外部委託先）による重要資産のマッピング

**重要事項の優先順位付け**

- 侵害は起こり得るという仮定の下、攻撃の識別、防御、検知、対処、復旧を目的とする統制とプロセスの改善
- 新たな脅威や自社の能力に基づいた優先順位付け

**パフォーマンスの監視**

- パフォーマンスと残存リスクを定期的に評価
- 主要指標の測定により、深刻化する前に問題を発見

**投資の最適化**

- 予算を確保できない場合は管理可能なリスクを許容
- すべての投資について「費用」と「通常業務」への影響を考慮

**ビジネスパフォーマンスの実現**

- セキュリティを全員の責任として位置付け
- 新しいテクノロジーを制限せず、最大限利用

# 攻撃の広がり方

## 最悪の事態とは

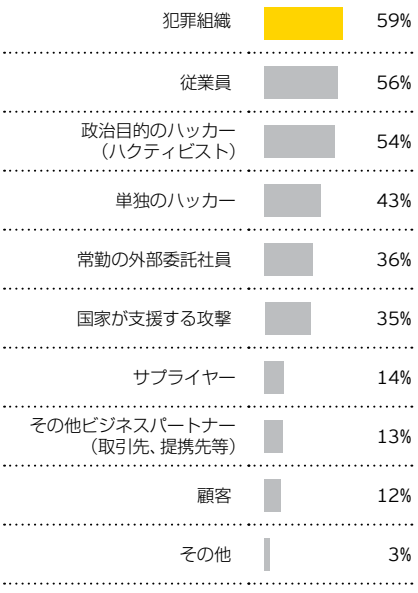
「何かがおかしい」と気付くためには、まず貴社がおかれている状況を徹底的に理解する必要があります。組織の発展のために何が重要なのかを明らかにし、重要なサイバー・ビジネス・リスクのシナリオを定め、リスクが顕在化した場合に、どの部分に最も損害が生じるかを具体化する必要があります。これにより、一連の予防措置に優先順位を付け、最も重要な分野、最も発生確率が高いと想定される攻撃に対策を講じることが可能になります。

**攻撃シナリオの例**


ビジネスとサイバーリスクに関連する重要なシナリオを複数策定することで、監視すべき範囲を明らかにすることが可能です。

- 盗み出された知的財産の使用を疑わせる売上げ
- 大規模な合併・買収を準備している間に企業価値が下落
- 多くの第三者が関与しているビジネスの重要な分野

**貴社へサイバー攻撃を行う人または組織のうち、攻撃元と想定されるものを、すべて選択してください。**




### すでに侵入されている？

サイバー犯罪者は、組織の内部に何カ月間も潜伏し、今後の攻撃に利用できる情報を探ったり、さまざまな情報をつなぎ合わせたりしています。そのため、彼らは検知から自身を守るための対策も講じています。また攻撃活動やその成果から注意をそらすための陽動工作を行うこともあります。犯罪者は盗み出した情報をしばらくは使わず、その後サイバー犯罪コミュニティの中で売買し、企業へ直接的な脅威を与えることもあります。

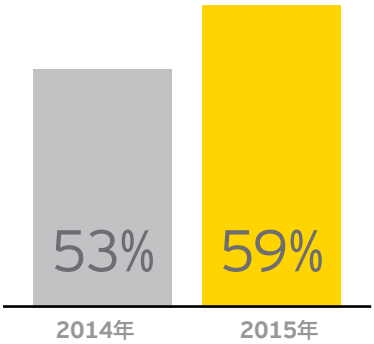
こうした潜入活動は、時として痕跡を残すこともありますが、ほとんど気付けないのが実情です。業務やシステム自体に小さな異常が見られても、通常は問題視されたり報告対象になったりしないため、攻撃の全体像を捉えることができません。サイバーセキュリティが役員の間で重要な議題となっている現在でも、各役員の担当部門で起きたいくつもの小さな原因不明の事象が、重大な損害を広範囲に与える高度なサイバー侵害の一部分であることは、なかなか明らかにはなりません。

## 捉えにくい兆候を検知するには

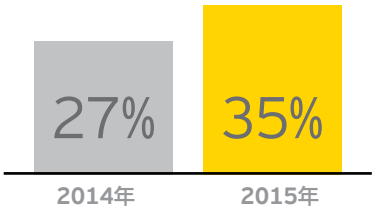
サイバーインシデントによる被害を最小化する鍵となる最初のステップは、最も価値が高く、最もリスクが高い分野に、特に注意を向けて、予防策や発生時の備えを講じることです。そして次の重要なステップは、サイバーインシデントを可能な限り早期に検知できるようにすることです。これを実現するためには、さまざまな指標を把握して、一定のしきい値を超えた時点でアラートを発する仕組みが必須です。組織にとって最も影響が大きいと想定されるインシデントの種類とリスク選好度を基に、しきい値を決定します。

攻撃は、突然に、はっきりと分かる形で発生することもあります。そのような攻撃を受けると、その対応だけに全体の注目を切り替えてしまいがちです。しかしながら、そのはっきりと分かる攻撃は陽動工作である可能性があることを認識すべきです。時間がたってから現れるパターンを把握するのに、各インシデントを分析できる能力が必要です。

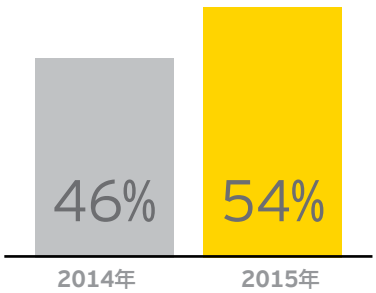
組織に侵入する方法はいくつもあり、サイバー攻撃者は最も脆弱な入り口を狙います。一部の入り口は目立つことから容易に補強ができ、その上で監視することになります。しかし、攻撃者が使う手口について想像力を働かせると、それほど目に付かない場所（たとえば一般向けWebサイト、社内のシステムに接続する第三者のシステム、産業システムやクラウドへの接続等）にも、防壁や監視機能を追加するのが得策ということになります。




59%が、攻撃を仕掛けてくる可能性が最も高いのは犯罪組織だと回答（2014年のサーベイでは53%）




35%が、攻撃の発信元として可能性が最も高いのは国家が支援する攻撃だと回答（2014年のサーベイでは27%）




54%が、攻撃を仕掛けてくる可能性が最も高いのは政治目的のハッカー（ハクティビスト）だと回答（2014年のサーベイでは46%）

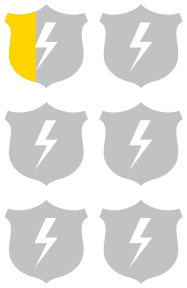
攻撃者は侵入に成功すると、「価値ある」情報のありかへ向かっていきます。それは貴社のビジネスにとって重要で、貴社に最も大きな損害を与える可能性があり、または貴社のビジネスパートナー（他社）のビジネスの根幹に関わるような重要な情報でもあります。

財務、マーケティング、研究開発、人事などの重要部門は、サイバー・ビジネス・リスクを認識する必要があります。そして何かがおかしいと感じた場合は、サイバーセキュリティの担当部署へ知らせる必要があります。

現実世界におけるテロ対策と同様で、不審に思ったことは積極的に通報することが重要です。サイバーセキュリティの担当部署への通報で、パズルのピースが組み合わさるように、全体が明らかになる可能性があるからです。

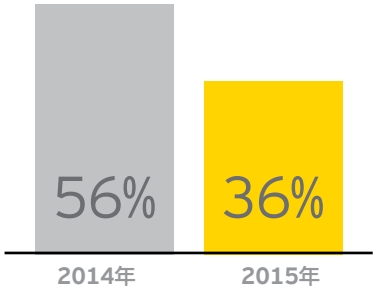
網を張り巡らせて検知すべき兆候の例は、次の通りです。

- DDoSなど明確な目的のない攻撃（明確な使用目的のない情報の窃盗）
- 予想を超えた株価の変動
- 研究開発中の製品に酷似している、または保有する知的財産を利用したと思われる新製品の発表（知的財産、戦略、新製品の市場投入時期等に関する情報が流出した可能性がある）
- 合併・買収（M&A）活動の妨害（ライバル企業の提案価格が非常に近かったり、社外秘の計画を知っているかのような動きを見せる場合は、M&Aの合併・買収先企業が知的財産の窃盗などのサイバーインシデントにさらされている可能性がある）
- 顧客やビジネスパートナーのいつもと異なる行動（サイバー犯罪者は、システムやデータにアクセスしやすくするために、顧客やビジネスパートナーを装って貴社に接近してくる場合がある）
- 従業員のいつもとは異なる行動（管理者は、特に機密性の高い業務を担当している従業員の行動変化に注意する必要がある）
- 原因不明のシステム停止
- 支払処理システムや注文処理システムの異常
- 顧客情報が格納されたデータベースの情報の不整合



7%

が、外部委託先や法執行機関を含むインシデント対応プログラムを整備しており、そのプログラムは、より広範な脅威や脆弱性管理機能に組み込まれていると回答




36%が、高度なサイバー攻撃を検知できる可能性は低いと回答。2014年の56%と比べて著しく改善されているが、日々巧妙になっている事実を忘れてはならない

56%

が、今後12カ月間、組織における情報漏えい・紛失防止の優先度は高いと回答

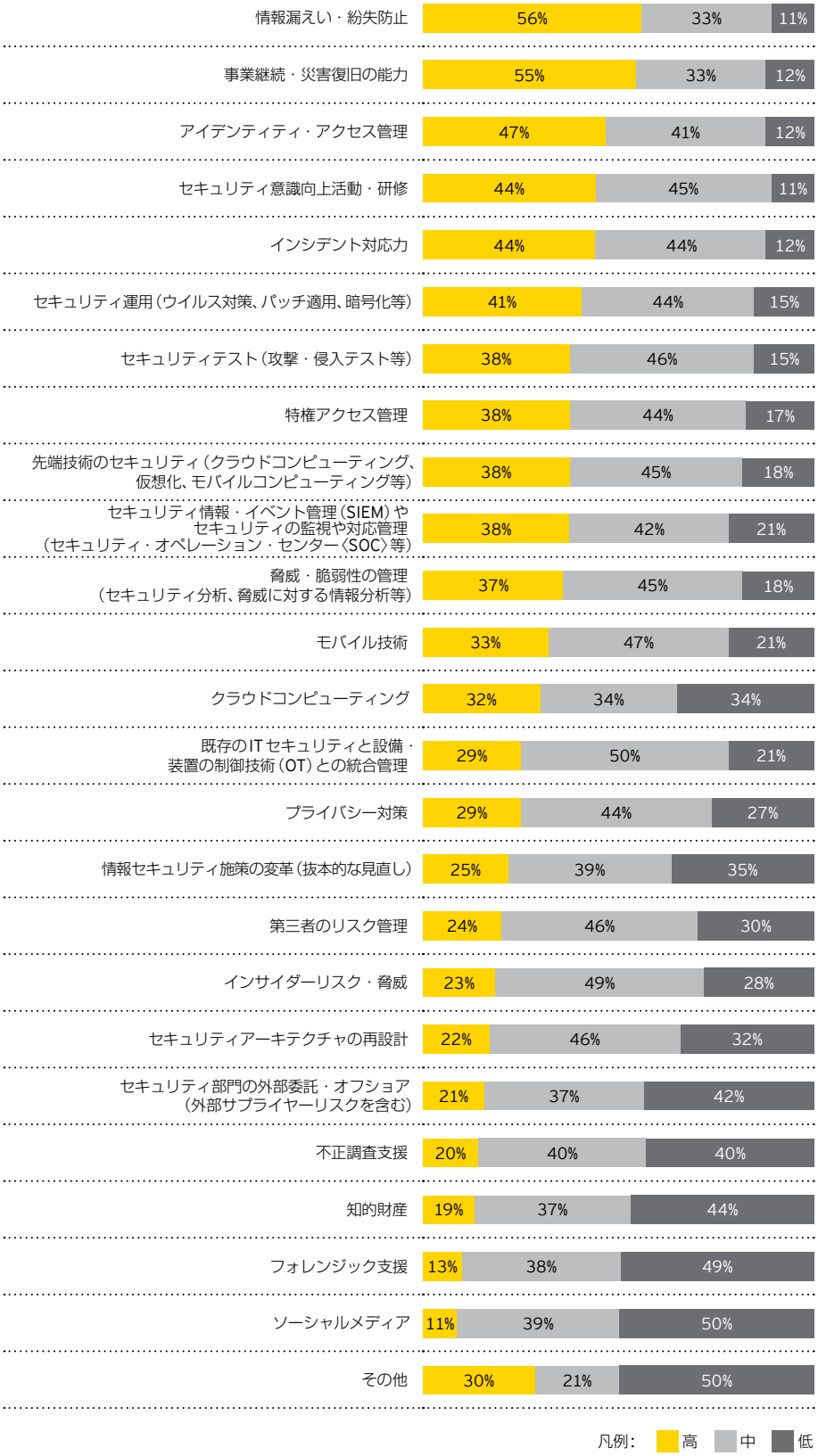
49%

が、インサイダーリスク・脅威の優先度は中程度だと回答。従業員による攻撃の可能性が高いとの回答は56%、常勤の外部委託社員による攻撃の可能性が高いとの回答は36%

50%

が、ソーシャルメディアの優先度は低いと回答

**以下の各項目について、今後12カ月間（または当年度）に想定される貴社の対応優先度を、「高」「中」「低」から一つ選択してください。**（項目ごとに一つ選択）



## 絶えず「厳戒態勢」を取るべき理由

デジタル社会では、どの組織もサイバーセキュリティの脅威や脆弱性に対して無関係ではありません。常に警戒を怠らず、環境の変化を敏感に捉え、迅速に対応できる態勢を整備することが重要です。予測される事態に対して、24時間365日の対応態勢の整備も不可欠です。

しかし、このレベルの警戒が要求されると、組織は疲弊し、「どこまで対応すれば十分なのだろう?」という疑問が湧き起こることも理解できます。

ここ3、4年の間に絶え間ない数々の攻撃が続いたことや、サイバー事象への対応を余儀なくされてきたことから、現状の対策で十分という考えに陥ってしまうかもしれません。「典型的な攻撃」(フィッシング等)への対処や、明らかな統制上のギャップへの対応(アイデンティティ・アクセス管理等)を行うことで、サイバーセキュリティの問題が「解決」したと考えてしまうかもしれません。しかし状況はさらに悪くなっているのが現状です。そして、限られた予算の中で、セキュリティ対策の投資対効果を明らかにすることが、さらに困難となっていることも事実です。

大部分の組織は適切なサイバーセキュリティの基盤を築いています。しかし、それがほんの始まりにすぎないということや、デジタル社会では投資による迅速で効果的なアプローチが必要であることは明確に理解されていません。リスクを適正な水準に抑制できるようになって初めて、組織は「十分な」サイバーセキュリティを確保したと見なすことができるのです。

組織のサイバーセキュリティの成熟度が上がるにつれて、セキュリティ投資の効果は実証しやすくなります。サイバー攻撃によって発生する損害コストの試算をより正確に行うことで、継続的投資や警戒の必要性の説明が容易になるでしょう。攻撃を発見できず、最悪の事態に至った場合に発生する損害額を推定することで、社内の体制づくりも含めたセキュリティ施策のビジネス的な価値を説明することができます。

正確な状況認識ができれば、投資の合理化や優先順位付けがしやすくなります。しかしながら現状は、必ずしもサイバーセキュリティ対策の成熟度を高めるとは限らない、本質的ではない統制や機器の導入に膨大な金額が浪費されています。

$$$$$$

**49%**

が、経営陣のリスク許容度に合う形で組織を保護するには、資金を最大で25%増額することが必要だと回答

$

**84%**

が、知的財産の情報セキュリティへの来年の支出額は、今年と同じかそれ以下になるだろうと回答

**70%**

が、セキュリティ運用(ウイルス対策、パッチ適用、暗号化等)への支出額は、今年と同じかそれ以下になるだろうと回答

**62%**

が、インシデント対応力向上に対する来年の支出額は、今年と同じかそれ以下になるだろうと回答

# いまだに脆弱である理由

2014年の報告書では、サイバーセキュリティの成熟度を表すActivate（始動する）、Adapt（適応する）、Anticipate（予想する）の三つのステージ（三つのA）を明確化しました。高度かつ総合的なサイバーセキュリティ対策を実施するために、これらのステージをより短い期間で実施していく必要があります。


三つのAは今でも有効です。2015年のサーベイからは、三つのステージすべてにおいていまだ導入途上であることが読み取れます。一方で、最新脅威に直面したことにより、従来は高度な対策と考えられてきたものの多くは、基本的な対策となってきています。

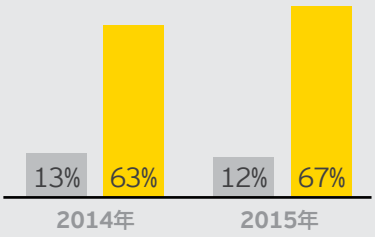
### 1. Activate（始動する）

このステージで、組織はサイバーセキュリティの確固たる基盤を確立します。**現在の**環境において基本的な防御に必要な一連のサイバーセキュリティ対策を含みます。この段階では以下のような取組みが求められます。

- セキュリティ評価の実施とロードマップの作成
- セキュリティ対策の変革に対する取締役会レベルの支援
- セキュリティ方針、手順、関連する基準の見直しと更新
- セキュリティ・オペレーション・センター（Security Operation Center、以下「SOC」）の設立
- 事業継続計画およびインシデント対応手順のテスト
- サイバーセキュリティ対策の企画と実施

サイバーリスクや脅威が高度化しつつある現在、二つの基本的な活動が新たに加わっています。

- 企業のエコシステムの定義
- 全従業員を対象とするサイバーセキュリティ意識向上トレーニングの導入

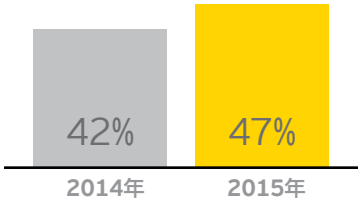



自社の情報セキュリティ機能がニーズを完全に満たしていると考える回答者の割合と、部分的に満たしているが、引き続き改善中であると答えた回答者の割合。

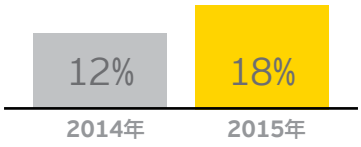
2015年のサーベイから分かる企業の成熟度

## 現在の環境には不十分な対策

- 自社の情報セキュリティ機能がニーズを完全に満たしていると考えている回答者は、わずか12%にとどまりました。67%の回答者が、引き続き改善中であると答えています。
  - ニーズに完全に対応できているという回答は1%減少に対し、改善中であるという回答は2014年からわずか4%しか増加していません。
- 69%の回答者が、経営陣のリスク許容度に合う形で企業を保護するには、情報セキュリティ予算を最大50%増やす必要があると回答しています。
- 47%の企業にSOCがありません。（2014のサーベイでは42%）
- 37%の企業にデータ保護プログラムがないか、あるいは場当たり的な施策やプロセスだけが実施されています。（2014年のサーベイでは34%）
- アイデンティティ・アクセス管理プログラムを実施していないという回答は18%でした。2014年のサーベイでは12%でしたので深刻な状況といえます。
- エコシステム（すべての第三者プロバイダー、ネットワーク接続、データ）の正確なインベントリを保持しているという回答は、わずか40%でした。
- 昨年、社内で最も重大なサイバー侵害を引き起こした主な統制、またはプロセスの問題として、エンドユーザーに対するフィッシング攻撃を挙げた回答は27%でした。




SOCを保有していない回答者の割合




アイデンティティ・アクセス管理プログラムを実施していない回答者の割合

54%

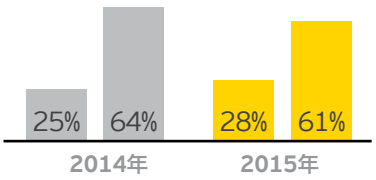
が、情報セキュリティに関して、先端技術が組織に与える影響を分析する担当者または部署がないと回答

### 2. Adapt（適応する）

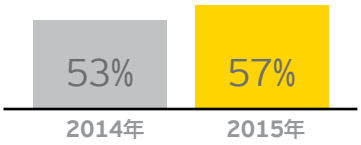
基本的な情報セキュリティ対策は、時間の経過とともに効力が低下していくため、このステージでは環境の**変化**に重点が置かれます。刻々と変化するビジネス要件に歩調を合わせ、適応していくために必要な措置が中心となります。

現在、このステージでは次のことが求められます。

- サイバーセキュリティ成熟度を一段階上げるための変革プログラムの計画・実施。このプログラムの計画・管理に当たっては、外部支援を得て先進的な取組みを迅速に採用
- 内製するもの、外部委託するものを決定
- サイバーセキュリティに関するResponsible Accountable Consulted Informed（以下「RACI」）マトリックスを定義




情報セキュリティの変革に対する支出額を増やす予定（または、昨年と同じ支出額）と回答




情報セキュリティが企業に貢献し価値を提供する上で妨げとなっているのは、スキルのある人材の不足と回答

2015年のサーベイから分かる企業の成熟度

## 変化への適応力の不足

- 54%の組織には、情報セキュリティ機能の中で、先端技術とそれが組織に与える影響を分析する担当者または部署が今のところありません。うち、そのような担当者または部署を設ける予定がないという回答が36%含まれています。
- 自社のセキュリティ監視は成熟している、または非常に成熟していると答えた回答者は34%にとどまり、2014年のサーベイと比べて4%増にすぎません。
- 自社のネットワークセキュリティは成熟している、または非常に成熟していると答えた回答者は53%にとどまり、2014年のサーベイと比べて1%増にすぎません。
- 57%の回答者が、情報セキュリティが企業価値向上に貢献する上で妨げとなっているのは、スキルのある人材の不足であると回答しています。（2014年のサーベイ結果では53%）
- 「昨年との比較」を問う設問で、28%の回答者が、情報セキュリティの変革（抜本的な見直し）への支出を増やす予定であると回答しました。2014年のサーベイと比べて3%増にすぎません。

### 3. Anticipate（予想する）

このステージでは、潜在的なサイバー攻撃を検知して無力化するための積極的な（proactively）戦術を策定する必要があります。この戦術では、**今後の**環境を焦点に、予測可能な脅威だけでなく、予期せぬ手口にも対処する必要があります。

このステージに到達している組織はごくわずかです。このステージでは次のことが求められます。

- 脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）における戦略の策定と実施
- 組織のより広い範囲をサイバー・セキュリティ・エコシステムに追加
- サイバー分野への経済的なアプローチの採用
- フォレンジックデータ分析と脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）の採用
- 全員が状況把握できる体制の確立
- 包括的なサイバー侵害対応戦略の策定による、最悪の事態への準備

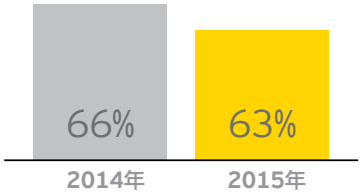
36%

が、脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）プログラムを実施していないと回答

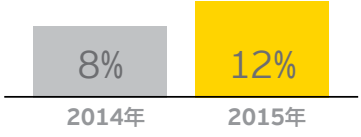
2015年のサーベイから分かる企業の成熟度

## 高度なサイバー攻撃を無力化する積極的なアプローチの遅れ

- 36%の組織が、自社では脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）プログラムを実施していないと回答しています。さらに、非公式なアプローチのみの実施であるという回答が30%に上りました。一方、5%の組織が、社内に高度な脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）機能があると回答しています。2014年と比べて、非公式な対応・アプローチを実施しているという回答が2%減少している点を除くと、これらの数字には変化が見られません。
- 63%の回答者が、脅威および脆弱性への対策は、優先度が中程度または低いと回答しています。この数字は、2014年のサーベイと比べてほとんど改善が見られません。
- サプライヤーだけでなくサプライヤーのサプライヤー（第四者）も視野に入れているという回答は、わずか12%にとどまりました。2014年と比べて、わずか4%の改善しかみられません。
- すべての外部委託先についてリスク評価を行い、適切なディリジェンスを実施しているという回答は31%にとどまりました。（2014年のサーベイでは27%）
- 79%の回答者が、モバイル端末について、ユーザーの意識・行動が主要なリスク原因であると回答しています。




脅威・脆弱性への対策は、優先度が中程度または低いと回答




サプライヤーだけでなく第四者も視野に入れていると回答

# アクティブディフェンスへの転換

**「アクティブディフェンスは従来のセキュリティ運用を置き換えるものではありません。それを体系化し強化するものなのです」**

EY グローバル アドバイザリー
サイバーセキュリティリーダー、ケン・アラン

## アクティブディフェンスとは？

サイバーセキュリティは、組織にとって不可欠な防衛能力です。政府の国防機関（や軍隊）が攻撃力を配備し、サイバー兵器を開発し、破壊的な侵攻を企てているのに対して、民間の組織では、攻撃的な行動は必要とされておらず、多くの場合法律的に「グレーゾーン」になっています。

ただし、だからと言って組織が受け身の姿勢で被害者の立場に甘んじるべきだということにはなりません。

前述したように、重要なサイバー・ビジネス・リスクを理解し、攻撃者が貴社の何を狙っているかを知ることで、資産、人材、ビジネス分野に優先度を付け、脆弱性を補強する「的を絞った防御」が可能となります。さらに、運用環境、重要資産、ビジネス戦略に基づいて、企業にとって固有の脅威を評価することにより、脅威を及ぼす可能性が最も高い攻撃者と使われる可能性のある手法を予測し、それを組み込んだシナリオに基づいて、準備状況を評価することが可能になります。このシナリオはすべて貴社のSOCに知らされ、組織をサポートするための基盤とする必要があります。

より高度なSOCを保有し、脅威・脆弱性情報の分析（サイバー・スレット・インテリジェンス）と運用との効率的な連携を行うことで、アクティブディフェンスの実施が可能となります。インテリジェントなセンサーを張り巡らせることで、潜在的な攻撃者を発見し、脅威の分析・評価を行い、組織の重要資産に対する損害を未然に防ぐことが可能になります。同様に、同じような運営体制を持つ高度なSOCを利用することで、望まれない異常、「訪問者」あるいは既にシステム内に入り込んでいることが確認された攻撃者を、積極的に捕えることが可能となります。

24%

が、脆弱性識別プログラムを実施していないと回答

34%

が、脆弱性の識別については非公式なプログラムを実施し、自動テストを定期的に実行していると回答

27%

が、データ保護のポリシーや手順は非公式、または場当たり的な施策であると回答

## 改善を必要とするものは？

**高度な脅威・脆弱性情報分析：**基本的な問題設定にとどまらず、さまざまなレベルの脅威評価やプロファイリングが可能となります。より高度な脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）を採用すれば、さまざまな脅威や対抗措置を積極的に管理することができます。

**貴社の脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）機能を高度化する必要があるでしょうか？**

貴社の情報セキュリティ機能を知るための鍵となる重要な質問

- 貴社の組織・ビジネスに関して、どのような情報が、攻撃者の手に渡る可能性がありますか？その情報は、どのように利用される可能性がありますか？
- 貴社の敵となり得るのは、どのような種類の攻撃者ですか？（ハクティビスト〈政治目的のハッカー〉、販売品をターゲットとした犯罪者ネットワーク、詐欺師、国家が支援する攻撃者等）
- そうした攻撃者の能力は、どの程度ですか？（考えられるリソース、計画、技術力、内部協力者を勧誘する能力等）
- 攻撃者は、何に関心を持つと考えられますか？（貴社の組織・ビジネスにとって本当に重要なもの——貴社のクラウンジュエル＜最重要情報＞と照合）
- 狙われている標的・資産には、どのような脆弱性があり、どのように悪用される可能性がありますか？
- 敵対者は狙った標的に到達するため、どのような経路を利用する可能性がありますか？（空調システム経由、支払いシステム経由、内部協力者の勧誘、アクセス権のある重役または特定の従業員に対するスピアフィッシング等）
- 最も効果的な対抗措置は何ですか？
- 敵対者と遭遇した過去の経験から、どのような教訓が得られましたか？

このような質問への答えを用意することにより、経営幹部や上級管理職レベルの戦略的な経営判断に確かな情報を与え、SOCの活動の焦点を調整し、外部の脅威・脆弱性情報の提供サービスを使って、その時点で最も重要な分野を分析します。

59%

が、自社のSOCでは有料の脅威・脆弱性情報提供サービスに加入していないと回答

## アクティブディフェンスを構築するには

アクティブディフェンスとは、従来のセキュリティ運用能力を二つの点から改善したものであり、1点目は、専門的に分析された脅威・脆弱性情報が利用されることを意味します。アクティブディフェンスを行う場合、単に「情報」を受け取るだけではなく、実際に脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）を行うことによって、攻撃者と思われる者を突き止め、社内で最も狙われる確率の高いターゲットを推定し、攻撃がどのように展開されるかについて仮説を立てます。この分析の結果により、状況に合った対抗措置を実施することが可能になります。

2点目は、アクティブディフェンスの運用サイクルを実施することです。アクティブディフェンスでは、入手可能な情報を分析し、結論を導き出し対策を実行するための、統制されたプロセスを繰り返し実行することで、ダイナミックで予防的な要素を既存のセキュリティ運用に追加することができます。

アクティブディフェンスは、特定の機能分野の改善や、新しいテクノロジーの実装を目的とした、他のセキュリティサービスとは異なります。企業に以前から備わっているセキュリティ能力を統合し、強化することによって、執拗な攻撃者に対するより効果的な対抗を可能にするのが、アクティブディフェンスです。組織は継続的な学習と改善のための反復的なサイクルを実施することにより、説明責任を果たせるガバナンス能力を効率的に強化することができます。こうした能力の向上は、セキュリティの運用を効率化し、セキュリティプログラムの投資回収率の向上に直結することになり、企業を標的とした攻撃の影響を小さくします。アクティブディフェンスには、大規模なサイバー侵害が発生した場合のリスクの評価と、全社的なリスクマネジメント対策としての一元的な対応フレームワークの構築も含まれている必要があります。サイバー攻撃対応フレームワークには、明確に定義されたガバナンスモデルに加え、インシデントの調査、証拠の収集と分析、影響評価、訴訟対応も盛り込まれている必要があります。

**アクティブディフェンスは貴社に適しているでしょうか？**

次の問いに対する答えの中に「はい」が一つでもあれば、アクティブディフェンスのアプローチ導入を検討する必要があります。

- SOCを保有しているが、高度な攻撃の証拠を発見することは、まだできていない。
- SOCを保有しているが、それでも大規模な侵害が発生している。
- SOCを外部委託しているが、知的財産や業務システムが確実に安全だとは言い切れない。

## デジタル社会に信頼を築く、次の一手

「何が必要か」というシンプルな問いに対する答えは、下記のすべてということです。

- 組織に損害を与え、戦略の遂行を妨害する可能性があるものに関する知識
- 組織におけるクラウンジュエル（最重要情報）の明確な特定
- 攻撃の経過を正確に表現した、サイバー・ビジネス・リスクのシナリオ
- 組織のリスク選好度を正確に決定できる取締役会と上級管理職
- サイバーセキュリティ成熟度の現時点の評価と、リスク選好度に合わせるために必要な成熟レベルとの比較
- 改善へのロードマップ
- 状況に合った脅威プロファイリングと、高度な脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）
- さらに進化した社内、コソーシング、またはアウトソーシングによるSOC
- 予防的で多機能なサイバー攻撃への対応戦略

サイバーセキュリティのロードマップや実装計画に従って進めるためには、組織内の考え方を変える必要があり、これには取締役会が大きな役割を果たします。すなわち、包括的な解決策とフレームワークは、事業と完全に整合性を取る必要があります。そのためには、外部の専門家などの支援が必要不可欠です。どこまで対策を行うかを検討するに当たり、セキュリティに関する全社的な成熟度評価は、早い段階で取り組むべき実効的なアクションとなります。

以降では、成熟度の各段階を解説します。的を絞った防御アプローチの場合、貴社が現在どの段階にあり、どの段階に進む必要があるかによって、どの段階まで行うか、決定する必要があります。



66%

最近、重大なサイバーセキュリティインシデントを経験し、自社のSOCでそのインシデントを発見できなかった回答者の66%が、有料の脅威・脆弱性情報の提供サービスに未加入であると回答しています。

## 成熟度スペクトラム――現時点における組織のランク

| 成熟度に関する設問 | 1――存在しない | 2 |
|---|---|---|
| **貴社の脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）プログラムは、どのレベルですか？** | **36%**の回答者が、脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）プログラムを実施していないと回答 | **30%**の回答者が、信頼する第三者（JPCERT等）や特定のメーリングリストを利用した非公式の脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）プログラムを実施していると回答 |
| **貴社の脆弱性特定能力は、どのレベルですか？** | **24%**の回答者が、脆弱性を識別する体制を整備していないと回答 | **34%**の回答者が、脆弱性の識別について現場担当者レベルでの対応を実施しており、定期的に自動テストを実行していると回答 |
| **貴社の侵害検知プログラムの一連の対策は、どのレベルですか？** | **18%**の回答者が、侵害検知プログラムを実施していないと回答。さらに4%の回答者が、対応とエスカレーションのための公式なプロセスがないと回答 | **23%**の回答者が、境界ネットワークに対するセキュリティ機器（IDS等）を使用していると回答。さらに21%の回答者が、セキュリティ情報・イベント管理（SIEM）ソリューションを利用して、ネットワーク、IDS／IPS、システムログを積極的に監視していると回答 |
| **貴社のコンピューターインシデント対応能力は、どのレベルですか？** | **14%**の回答者が、インシデント対応について整備されていないと回答 | **21%**の回答者が、マルウェアや従業員の不正行為から復旧可能なインシデント対応計画を策定していると回答。ただし、根本原因に関する詳しい調査を実施したことはないと回答 |
| **貴社のデータ保護に関する管理・運営状況は、どのレベルですか？** | **10%**の回答者が、データ保護プログラムに関する管理・運営の仕組みは整備されていないと回答 | **27%**の回答者が、データ保護のポリシーや手順は現場担当者レベルの取組み、または場当たり的であると回答 |
| **貴社のアイデンティティおよびアクセス管理状況は、どのレベルですか？** | **18%**の回答者が、アイデンティティ・アクセス管理に関する管理・運営は実施していないと回答 | **25%**の回答者が、アクセス管理プロセスを監督するチームやアイデンティティ情報を集約するサーバが設置されていると回答。ただし、公式のレビューは実施されていない |

| 3 | 4 | 5——非常に成熟している |
|---|---|---|
| **20%**の回答者が、外部業者による有料の脅威・脆弱性情報提供サービスや社内情報（セキュリティインシデント、イベント管理ツール等）を利用した、公式の脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）プログラムを実施していると回答 | **10%**の回答者が、社内外の脅威や脆弱性に関する情報が収集され、その信頼性や事業環境への関連性を分析する脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）チームがあると回答 | **5%**の回答者が、社内外の情報を利用し、情報の信頼性、関連性、脅威主体に対する弱点を評価する、専任の脅威・脆弱性情報分析アナリストや外部のアドバイザーを擁した、高度な脅威・脆弱性情報分析（サイバー・スレット・インテリジェンス）機能があると回答 |
| **20%**の回答者が、ソーシャルエンジニアリングや手動でのテストを含む、さまざまな検査アプローチを採用していると回答 | **18%**の回答者が、外部業者による脆弱性・侵入テスト、業務プロセスの定期的なテストやプロジェクトベースのテスト（新規のシステム等）に基づく評価プログラムを含む、脆弱性情報の分析機能が手続きとして整備されていると回答 | **5%**の回答者が、高度な脆弱性情報の分析機能があり、リスク管理部門の合意を得た結果を基に年間を通じてリスクベースの評価を実施していると回答 |
| **6%**の回答者が、現場担当者レベルのエスカレーションプロセスを実施していると回答。さらに5%の回答者が、脅威の収集、統合、対応、エスカレーションに場当たり的なプロセスで対応していると回答 | **13%**の回答者が、社内外の通信を監視する最新の技術（ホストベース・ネットワークベースのマルウェア検知、行動の変則性の検知等）を備えた、社内規程等で定められている検知プログラムを実施していると回答 | **11%**の回答者が、各分野の最新の技術（ホストベースのマルウェア検知、ウイルス対策、ネットワークベースのマルウェア検知、DLP、IDS、次世代ファイアウォール、ログ集約）を一つにまとめた検知機能の実行を規定している。高度なデータ分析を利用して、変則性、トレンド、相関関係を識別していると回答。ただし、脅威の収集、拡散、対応、エスカレーション、攻撃の予測のための社内規程等が整備されていると回答したのは、わずか2% |
| **43%**の回答者が、社内の正式なインシデント対応プログラムが整備されており、インシデント発生時の調査を行っていると回答 | **16%**の回答者が、社内の正式なインシデント対応プログラムが整備され、より網羅的なアイデンティティ応答サービスや調査のため、外部業者と契約している回答 | **7%**の回答者が、第三者機関や法執行機関を含む強固なインシデント対応プログラムを実施しており、より広範囲な脅威・脆弱性の管理を実施する部門と統合されていると回答。さらに、これらの企業では、潜在的なインシデントに対応する対応手順を作成し、定期的な机上訓練を行って検証していると回答 |
| **19%**の回答者が、事業部門レベルでデータ保護の施策と手順が定められていると回答 | **26%**の回答者が、（企業グループ等の）事業体レベルでデータ保護の施策と手順が定められていると回答 | **17%**の回答者が、データ保護の施策や手順は、経営陣による監督体制も含め、（企業グループ等の）事業体レベルで定められ、全社に周知されていると回答。個々の事業部門の例外事項は文書化・追跡され、年1回のレビューを実施していると回答 |
| **34%**の回答者が、社内で正式に任命されたチームが、アクセス管理プロセスを監視していると回答。ただし、その作業は大半が手動で行われている。各種のリソースを集中管理するサーバが設けられているが、限られた数のアプリケーションのみが対象であり、定期的なレビューは実施されていない。 | | **23%**の回答者が、社内で正式に任命されたチームが各事業部門とやり取りし、アイデンティティ・アクセス管理を監督していると回答。このチームは整備されたプロセスに従い、自動ワークフローを限定的に使用し、大部分のアプリケーションに対するシングルサインオンを提供し、定期的なレビューを実施している |

32%

が、同業他社の成熟度に関するベンチマーク情報が最も有益であり、最優先事項だと回答

## 組織を改善の軌道に乗せる

業績を最適化すると同時に、情報資産を効果的に保護するようなスキルやリソースを社内に保有している組織は、現時点でごくわずかです。自社の情報セキュリティ関連のプログラムや構造を客観的に評価することは、どの業界の組織にとっても有益です。

実効性のある評価には、以下のような効果が期待できます。

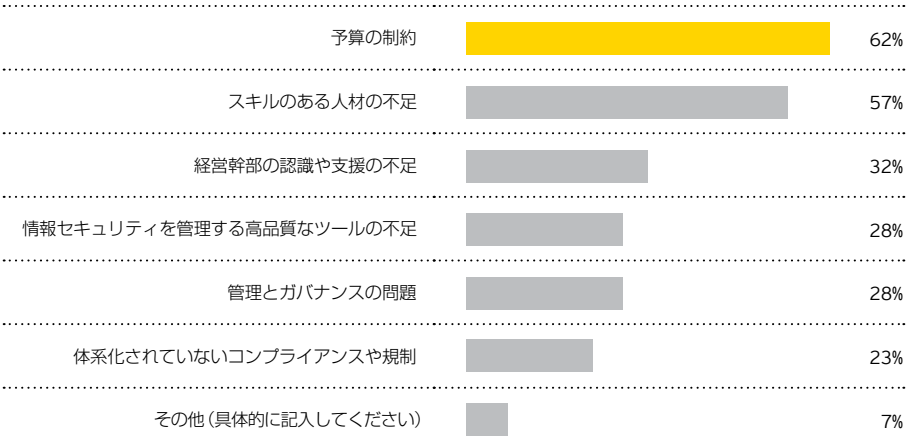
- 組織に起こる可能性のあるリスクについての理解
- 現在のサイバーセキュリティプログラムの成熟度評価と、改善が必要な分野の識別
- プロジェクトへの投資や組織変革にむけてのイニシアティブについて優先度に従ったロードマップの策定
- 他社と照合できるベンチマーク作成のための情報収集
- セキュリティ投資に対する改善状況の検証

この評価は、個々の分野や構成要素にまで、広範囲に、しかも深く掘り下げて行う必要があり、EYはその支援を行うことが可能です。ダッシュボード形式で示される指標により、情報セキュリティ戦略の継続的な評価、変革、持続可能性をサポートするため、何が必要か示されます。

また、成熟度評価を行うことで、現時点での到達レベルや競合他社との比較、将来的な到達目標が示されます。

**情報セキュリティの有効性**

情報セキュリティが企業に貢献し価値を提供する上で、主な障害となっているものは何ですか？（該当するものをすべて選択）



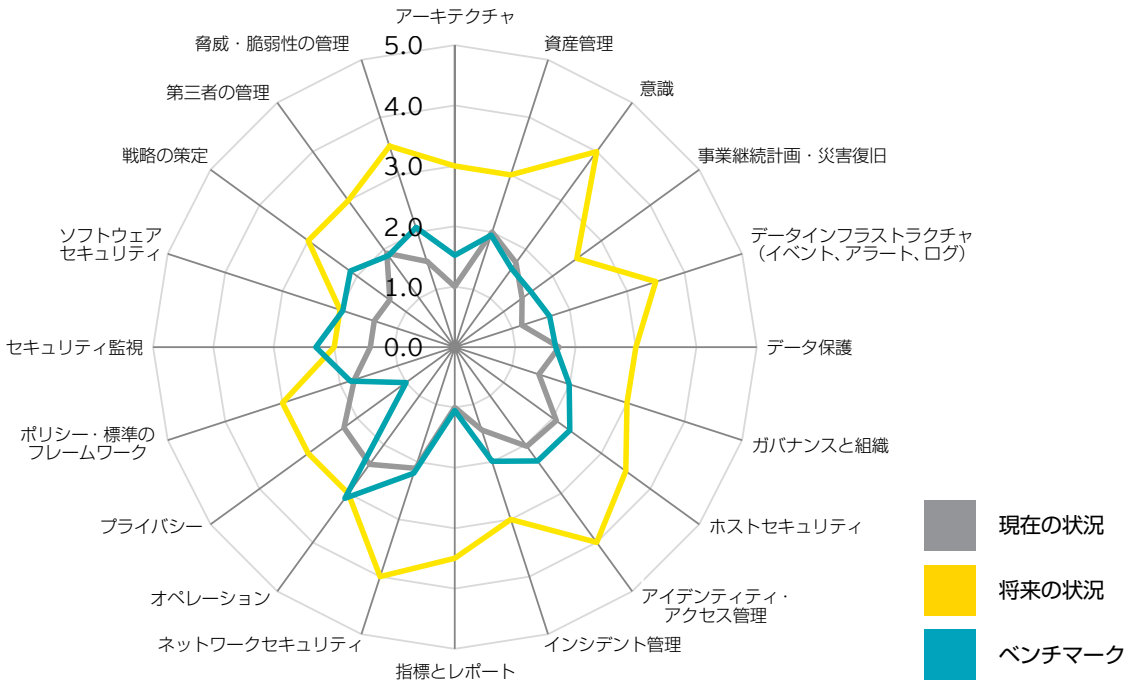

### RACIマトリックスを整備していますか？

取組みに対する姿勢を示し、要求水準を設定する取締役会では、全社的な協力体制が重要です。同時に、「サイバーリスクやサイバー攻撃が一人一人に及ぼす影響」に対する警戒心も重要です。効果的なセキュリティ管理は、組織のすべての担当者、すべての部門に影響するため、RACIマトリックス、優れたガバナンス、協力的な従業員のすべてが不可欠となります。EYの「三つのA」アプローチでは、サイバーセキュリティにおけるAdapt（適応する）レベルに当たる重要な要素です。RACIマトリックスで映し出される貴社の姿を検討し、サイバーセキュリティはもはや単なるITの問題ではないことを明確に理解することが重要です。

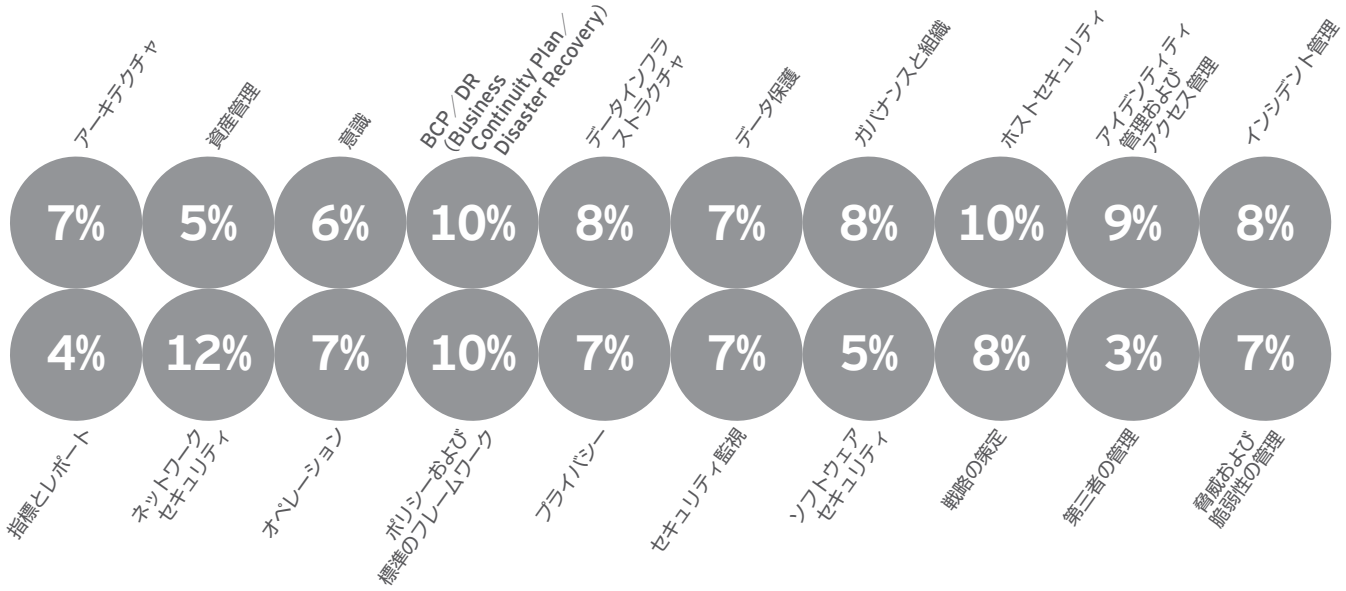
### X社の現状におけるサイバーセキュリティ成熟度の同業他社との比較

X社の現状における成熟度は、比較可能な同業他社とほぼ同じレベルですが、目標として将来の成熟度をかなり高く設定しています。

**X社と同業他社の比較**




### 今回のサーベイで自社の成熟度を「非常に成熟している」と回答した企業の割合



# サイバーセキュリティは
# デジタルイネーブラー

デジタル社会では、サイバーセキュリティは足かせではありません。むしろデジタル社会を完全に機能させ持続可能なものとします。

サイバーセキュリティは、イノベーションと成長を促進する重要な鍵となります。各組織の状況とリスクに見合ったアプローチを採用することで、組織はビジネス機会に集中することができます。IoT（モノのインターネット）では、個人と機器（携帯電話からヘルスケア機器、スマート家電からスマートカーまで）を完全にサポートし、保護する必要があります。こうしたビジネスで成功を収め、信頼を築くことは貴社の競争優位性を生み出すことにつながります。

今行動を起こし、デジタル社会のバランスを持続可能で安全なものへと調整していくことで、貴社ブランドの信頼を築き、より強力に組織を守ることが可能となります。

# サーベイの方法について

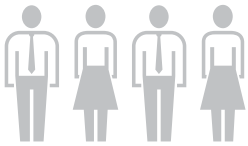
EYグローバル情報セキュリティサーベイは、2015年6月から2015年9月にかけて実施されました。67カ国における主要な業種にわたる1,755人が回答しています。

このサーベイでは、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）、その他情報セキュリティの幹部に参加を募りました。各国で使命された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を基に作成された質問票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にアクセスしてリクエスト用紙にご記入ください。

## 回答者のプロファイル



1,755
人の回答者

世界67カ国

25
の業種

## エリア別の回答者内訳（回答者数：1,755人）

凡例

| | |
|---|---|
| 欧州、中東、インド、アフリカ | 51% |
| 北・中・南米 | 29% |
| アジア・パシフィック | 15% |
| 日本 | 5% |

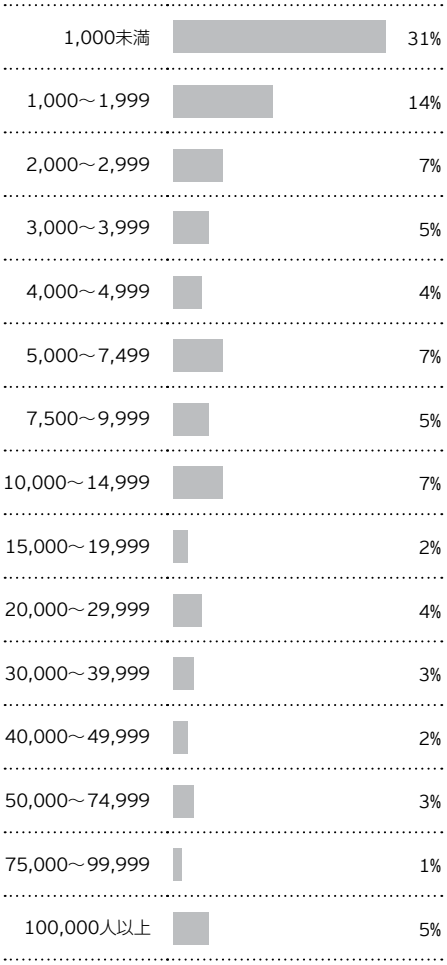
## 回答企業の年間総売上高別内訳

金額はすべて米ドル

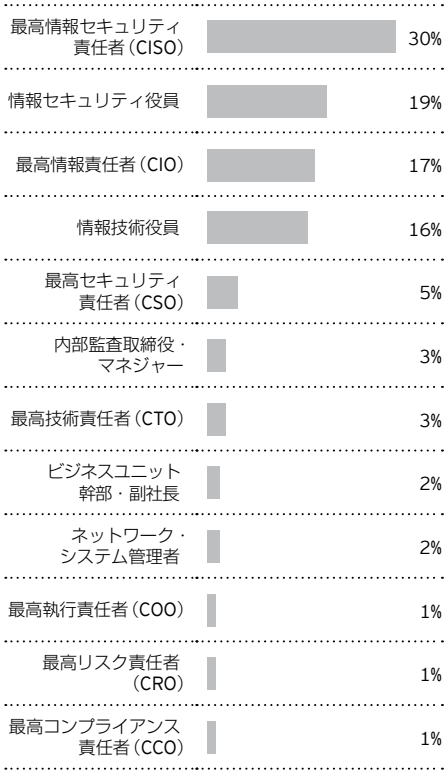
| | |
|---|---|
| 1,000万ドル未満 | 5% |
| 1,000万～2,500万ドル未満 | 5% |
| 2,500万～5,000万ドル未満 | 4% |
| 5,000万～1億ドル未満 | 6% |
| 1億～2億5,000万ドル未満 | 9% |
| 2億5,000万～5億ドル未満 | 9% |
| 5億～10億ドル未満 | 11% |
| 10億～20億ドル未満 | 10% |
| 20億～30億ドル未満 | 7% |
| 30億～40億ドル未満 | 4% |
| 40億～50億ドル未満 | 3% |
| 50億～75億ドル未満 | 4% |
| 75億～100億ドル未満 | 3% |
| 100億～150億ドル未満 | 3% |
| 150億～200億ドル未満 | 2% |
| 200億～500億ドル未満 | 4% |
| 500億ドル以上 | 3% |
| 政府機関、非営利団体 | 6% |
| 該当なし | 4% |

## 回答企業の業種別内訳


## 回答企業の従業員数別内訳




## 回答者の職務・役職別内訳



# より深く知るには？

**“Insights on governance, risk and compliance”**は、ITとビジネスリスクに関連した課題や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、知見を提供いたします。
“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

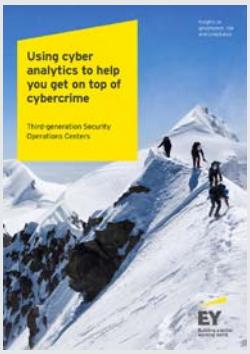

*“Managed SOC – EY's Advanced Security Center:world-class cybersecurity working for you”*
（英語版のみ）
http://www.ey.com/managedSOC


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


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


『サイバー犯罪に先手を打つ
EY2014 グローバル情報セキュリティ
サーベイ――日本企業の現状と課題』


*“Cybersecurity and the Internet of Things”*
（英語版のみ）
www.ey.com/IoT




*“Using cyber analytics to help you get on top of cybercrime: Third-generation Security Operations Centers”*
（英語版のみ）
www.ey.com/3SOC


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


*“Cyber breach response management – Breaches do happen. Are you ready?”*
（英語版のみ）
www.ey.com/cyberBRM

## サイバー攻撃に気付けますか？

EY のアドバイザリー部門にとって、より良い社会とは、大規模で複雑な業界の問題の解決、そしてクライアントのビジネスを成長させ最適化し保護するといった成果をもたらす、さまざまな機会の活用を意味します。EYはコンサルタント、業界プロフェッショナル、提携パートナーからなる世界規模のエコシステムを形成しています。その中心にあるのは、常にクライアントです。

サイバー攻撃に先んじて、アクティブディフェンスを実践すること。それが、サイバー犯罪に先手を打つための唯一の方法であるとEYは考えます。クライアントを中心に思考するEYは、貴社の事業、優先事項、脆弱性について、より優れた問題提起をします。その上で、必要とされるソリューションの実現に役立つ革新的な答えを導き出せるよう貴社と共働します。戦略から実行まで長期にわたって有効な、優れた成果の実現をご支援します。

組織がサイバーセキュリティに対してより適切に対処することで、世界はより良いものとなると、EYは確信しています。

サイバー攻撃に気付けますか？ EYにお問い合わせください。

**The better the question. The better the answer. The better the world works.**

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。

## EY Japanについて

EY Japanは、EYの日本におけるメンバーファームの総称です。新日本有限責任監査法人、EY税理士法人、EYトランザクション・アドバイザリー・サービス株式会社、EYアドバイザリー株式会社などの13法人から構成されており、各メンバーファームは法的に独立した法人です。詳しくはeyjapan.jpをご覧ください。





本書は EYG no. AU3588の翻訳版です。
ED None

## 連絡先


| | | |
|---|---|---|
| **Japan** | | |
| **髙橋可祝** | +81 3 3503 3500 | takahashi-kshk@shinnihon.or.jp |
| **Global Cybersecurity Leader** | | |
| **Ken Allan** | +44 20 795 15769 | kallan@uk.ey.com |
| **Area Cybersecurity Leaders** | | |
| Americas | | |
| **Bob Sydow** | +1 513 612 1591 | bob.sydow@ey.com |
| EMEIA | | |
| **Scott Gelber** | +44 207 951 6930 | sgelber@uk.ey.com |
| Asia-Pacific | | |
| **Paul O'Rourke** | +65 6309 8890 | paul.orourke@sg.ey.com |