Insights on
governance, risk
and compliance

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

EY
Building a better
working world

目 次

はじめに

ポール・バン・ケッセル
EYグローバル
リスクリーダー

ケン・アラン
EYグローバル
情報セキュリティリーダー

本書『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』をお読みいただきありがとうございます。

既に多くの組織が、中には苦い経験から身をもって学んでいるように、サイバー攻撃はもはや万が一発生した場合の問題ではなく、いつ起きるかの問題となっています。ハッカーはますます執拗に攻撃を仕掛けるようになっており、政治的な動機による場合も少なくありません。一つの作戦が失敗しても、ハッカーは組織の防御を突破するまで次々と別の作戦で攻撃をしかけてきます。同時に、オンライン状態の増加、ソーシャルメディアの幅広い活用、モバイル機器の浸透、クラウドサービスの利用拡大、ビッグデータの収集・分析を背景に、テクノロジーの利用が組織のサイバー攻撃に対する脆弱性を増加させています。

また、規制当局はこの脅威を認識しており、企業に規制を順守し、サイバー攻撃による侵害を公表し、詳細な調査を提供するよう迫っています。企業は規制当局の仕掛けた罠に陥らないように自社で対応しなければなりません。つまり、リーダーは残存リスクに対処するには何が必要かを見極め、自分たちが置かれている状況をしっかりと理解することが必要です。

組織は、いつ、いかなるところでも起こり得るサイバー攻撃と闘い、処理し、軽減するために対策を整えておかなければなりません。

16年目を迎えたこの調査では、多くのサイバー攻撃が絶え間なく起き、複雑性を増している中で、サイバーリスクに対処する3つのレベルを検証しています。

1. **Improve**—改善と挑戦：組織が現在直面しているサイバー脅威に対処するために行っている改善と、さらに一層の努力が求められている挑戦
2. **Expand**—リーディングプラクティス：新たな脅威により積極的に対処するべく現在の改善を拡大するために優れた組織がとっているステップ
3. **Innovate**—セキュリティのイノベーション：近く普及する技術あるいは将来登場する最先端技術に対応するために組織に求められているソリューション

今回の調査では、1,900社以上のクライアント企業の体験談と、これらの企業が今日のサイバー脅威にどのように対処しているかを検証しています。調査に加えて、EYの経験に基づき、サイバーリスクへの対応においてリーディングプラクティスを実践している企業を対象に、多くの経営層にインタビューしました。さらに、EYのセキュリティ専門家による分析や二次的なリサーチを用いて調査結果に深みを加え、充実させました。

調査にご協力いただいた回答者の皆様に心より感謝申し上げます。貴重なお時間を割いて体験談を述べていただき、誠にありがとうございます。

調査結果の内容についてさらなる議論を深めて参りたいと思いますので、ご意見をお待ちしております。

ポール・バン・ケッセル
EYグローバルリスクリーダー

ケン・アラン
EYグローバル情報セキュリティリーダー

今日のサイバー攻撃の現状

サイバー攻撃の脅威はすぐそこに!

サイバーセキュリティ攻撃はここ数年で急激に増加しました。日々急速に技術が進歩していく中で、より複雑な新しいサイバーリスクが出現し、組織のブランドと最終的な収益に大きな打撃を与える脅威となっています。すべての個人と組織が標的とされています。

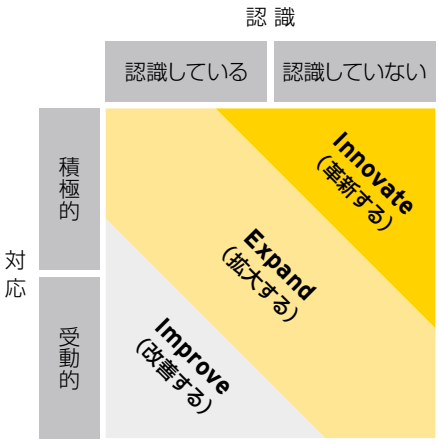
本書に目を通していく中で、多くの読者がサイバー攻撃によって自らの組織のセキュリティが既に侵されていることに気が付くことでしょう。数日、数週間、あるいは数カ月も前に侵害されていたおそれがあることに気が付かない場合さえあります。侵害された事実を認識し、その重大性が明るみに出た時点では、組織が負担する関連コストは膨大な額になるおそれがあります。世界中のマスコミで日々報道される有名企業や組織を標的とした注目度の高い攻撃について考察し、失われたデータの量、財務的損失、風評被害による損失を検証してその影響度を測る必要があります。

『ギャップを埋める闘い』と題した2012年グローバル情報セキュリティサーベイでは、組織の情報セキュリティプログラムの現状と、大多数の組織が直面しているより陰湿なサイバー攻撃から上手く身を守るためにあるべき姿との間でギャップが拡大しているという考えを示しました。今年のグローバル情報セキュリティサーベイでは、組織が正しい方向へ向かって前進しているものの、さらなる取組みが早急に求められていることを示しています。

本書は以下の3つの点を考察する形で構成されています。

1. **Improve（改善する）**
   多くの組織にとっては、これが現状の段階です。昨年1年間で組織はサイバー攻撃への備えを大幅に改善してきました。しかし、依然として受け身の対応であり、認識している脅威には対処しているものの、目前に迫りつつある脅威については積極的に理解しようとはしていません。

2. **Expand（拡大する）**
   先進的な組織はサイバー脅威と闘うためにさまざまな手段を講じています。これらの組織はセキュリティプログラムの中で、既知および未知のリスクの両方をより積極的に認識しています。しかしながら、セキュリティ対策を拡大する余地はまだあります。



3. **Innovate（革新する）**
   情報セキュリティの革新者を目指す組織は、新しい領域に目を向けなければなりません。これらの組織はより万全な備えをしておくために、情報セキュリティのフレームワーク全体を継続的に見直し、再検討し、将来的に再構築する必要があります。多くの場合、サイバーリスクが存在する環境の中で既知および未知のリスクの両方に対する防御を積極的に強化するために、イノベーションには情報セキュリティプログラムの抜本的な変革を伴うことがあります。

現在の脅威に対処するために組織が講じてきた対策、差し迫りつつあるサイバーリスクへの備えにおいて先進的な組織がどのように今後の脅威を見通しているか、また、最先端の強力な情報セキュリティプログラムや機能をもってしても確実に困難な状況となる将来に向けて組織が積極的に備える上で、新たな技術やアイデアがどのような役割を果たすかについて以降のページで考察していきます。

Improve（改善する）

サイバー脅威が認識され改善が加速

攻撃は避けて通れないと認識することが大きな改善を起こします。

70%

情報セキュリティポリシーは経営層が自身のものとして捉えている

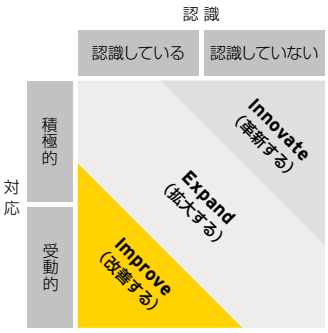
76%

データアクセス権を持つサードパーティーが構築した情報セキュリティ対策に対して自己評価を実施している、あるいは外部評価を委託している

サイバー脅威を認識することにより改善が加速

調査結果により、多くの組織が、経営トップから現場レベルに至るまで、直面している脅威の範囲と複雑性を認識していることが明らかになっています。回答者の4分の3近くの組織においては、現在、情報セキュリティポリシーは経営層が自身の責任として捉えています。

情報セキュリティ部門がCEOに直接報告する組織は10%でした。35%の回答者は、情報セキュリティの専門家が四半期毎に取締役会および最高意思決定機関の幹部に情報セキュリティについて報告していると答えており、毎月報告している回答者はわずか10分の1ほどでした。昨年の調査で、情報セキュリティの専門家が毎月経営幹部に報告していると回答した組織はゼロでした。



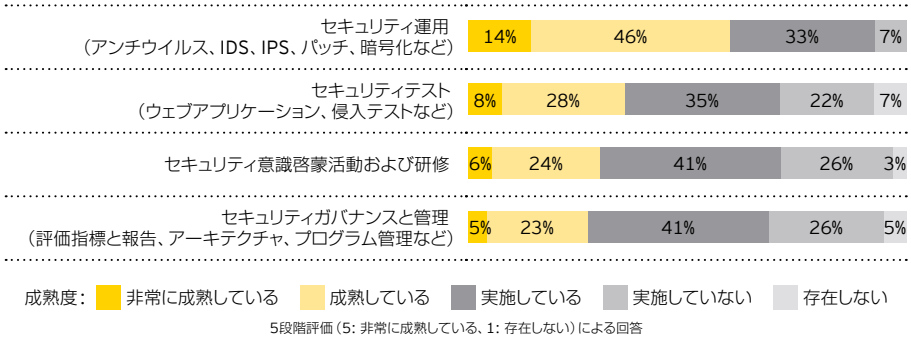
情報セキュリティは現在、組織が継続的に健全性を維持し、成功するためには不可欠であるとみられています。大部分の組織においては、正規のセキュリティ運用（アンチウイルス、IDS、IPS、パッチ、暗号化など）が十分に行われています。

データ保護はもはや契約書の条項の一部であり、第三者に任せておけばよい項目とは考えられていません。回答者の4分の3は、データへのアクセス権を持つ外部のパートナー企業、ベンダー、請負業者が構築した情報セキュリティに対して自己評価、あるいは外部評価を社外に委託することを義務づけていると回答しています。

しかし、組織の取組みが正しい方向へと前進しているとはいえ、まだまだ改善の余地があります。多くの組織が情報セキュリティへの投資を拡大していますが、依然として、増大するサイバーリスクに対応するには予算が不十分だと感じている情報セキュリティの専門家は少なくありません。

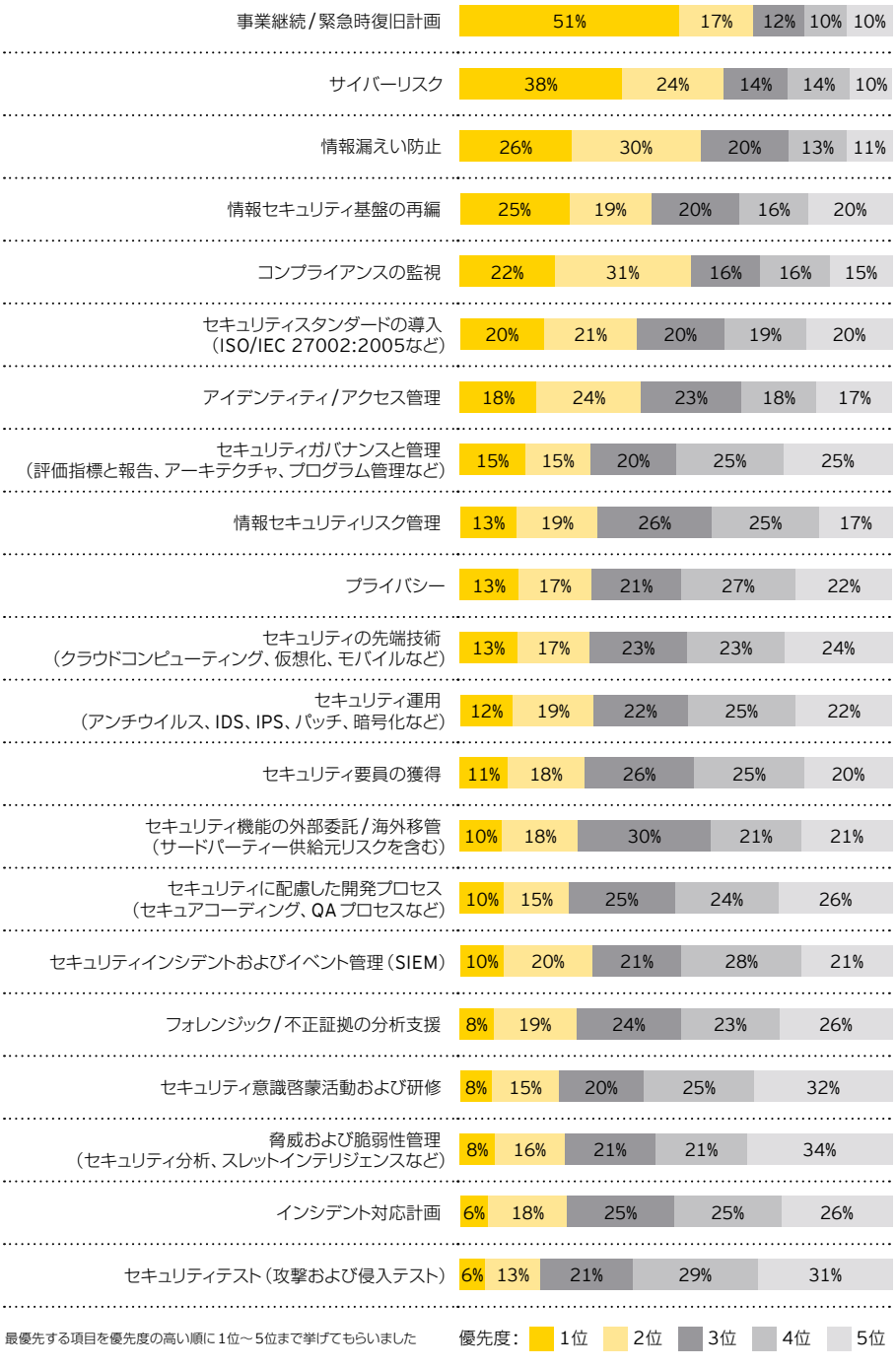
同様に、組織は適切な優先事項に対処していると感じているものの、ニーズをサポートするためのスキルを有する人材が不足していることを多くの回答者が示しています。現状維持から改善・革新へと重視する領域の傾向が変わってきているにもかかわらず、いまだに多くの組織がリスクにさらされたままになっています。さらに、技術（アンチウイルス、IDS、IPSなど）を導入、運用している組織の多くは、依然として、これらの技術に関連するコンフィギュレーションやプロセス（パッチマネジメントやスレットインテリジェンス（最新の脅威に関する情報収集と分析）など）が今日のニーズに対応していないと考えています。多くの組織がセキュリティ管理プロセスは一部の観点からまだ完全に成熟していないと感じているのは当然のことでしょう。

情報セキュリティ管理プロセスの成熟度



5段階評価（5: 非常に成熟している、1: 存在しない）による回答

今後12カ月間で最優先と考える情報セキュリティ項目を選択してください



35%

情報セキュリティ専門家が四半期毎に取締役会あるいは最高意思決定機関の幹部に情報セキュリティについて報告している

今年の調査結果に基づき、サイバー犯罪との闘いにおいて組織が大幅に前進した点を以降のページで示していきます。また、今日の環境において依然として組織に求められている取組みについても併せて明らかにしていきます。

組織が大幅に前進した点

68%

事業継続/災害復旧を最優先項目の上位2つに挙げている

組織は適切な優先事項をより重視する方向へ転換しています

概して、事業継続/災害復旧が今後12カ月間で最優先する情報セキュリティ項目として挙げられています。それに続き、サイバーリスク/サイバー脅威、情報漏えい防止、情報セキュリティ基盤の再編、コンプライアンスの監視が上位5位となっています。

金融機関はサイバーリスク/サイバー脅威をより重要視しており、これは売上高が10億米ドル以上の組織にとっても同様に懸念事項となっています。

43%

情報セキュリティ予算が増加しつつある

情報セキュリティへの投資は増加傾向にあります

全体で43%の組織が、予算が増加していると回答しています。

政府・公共部門では、一部の組織で予算が増加しているものの、大半は前年と同額と回答しています。

予算の増加額が最も高いのは、売上高が1,000万米ドル未満の中小企業や急成長市場における企業です。

46%

今後12カ月間に情報セキュリティの改善、拡大、革新に充てる費用の割合

組織は運用・保守から改善・革新へと目を向けています

セキュリティの運用・保守は引き続き重要ですが、前年と比較すると重要度は低くなっています。

回答者の注目はセキュリティの改善、拡大、革新へと移行しており、来年は支出の46%がこれらの取組みに充てられる予定です。

46%

情報セキュリティ戦略は組織のビジネス戦略に整合している

組織は全体戦略と個々の戦略を整合させています

インタビューした組織の約半数は、情報セキュリティ戦略と組織のビジネス戦略を整合させており、情報セキュリティ戦略とIT戦略を整合させている組織は過半数に上りました。

戦略の整合を最も推進しているのは金融サービス企業です。

このことから、組織の規模や業界に関係なく、また、情報セキュリティ戦略の義務について理解が高まってだけでなく、全体戦略と個々の戦略が合致している組織が増えていることがわかります。

68%

情報セキュリティ機能は組織のニーズを満たしていない

サイバーセキュリティプログラムを改善する取組みが増加しています

2012年の調査結果と比べると、情報セキュリティ機能が組織のニーズを満たしていないと回答した組織は8%から6%へと若干減少し、要件を満たしていると回答した組織はやや増加しています。

また、情報セキュリティ機能は組織のニーズに対して不十分で、改善を進めていると回答した組織は68%となり、金融サービス企業においては74%となりました。

全般的に、情報セキュリティ機能は企業のニーズをより効果的に満たし、価値を創出するために適切な改善を行っています。

依然として組織に求められている取組み

スキルを有する人材の不足と経営層の意識および支援の不足が、引き続き情報セキュリティ部門における課題です

情報セキュリティ部門は適切な優先事項に注力しているものの、多くの場合、それに対処するためのスキルを有する人材や、経営層の意識および支援が不足しています。特に、需要と供給におけるギャップが拡大しており、売り手市場になっています。半数の回答者が、価値を創出する上での障害として、スキルを有する人材の不足を挙げています。同様に、経営層の意識および支援の不足を課題として挙げた回答者は昨年の調査ではわずか20%だったのに対し、今年は31%に上りました。

調査結果では、情報セキュリティ部門自体は改善に向けて大きく前進しているものの、その他の部門が支援する上で後れを取っていることが明らかになっています。

50%

スキルを有する人材の不足が価値を創出する上での障害となっている

情報セキュリティ部門は依然として危機を感じています

予算は増加傾向にあるものの、情報セキュリティ部門は、予算の制約が企業に価値をもたらす上での最大の障害となっていると感じています。65%の回答者が、企業が期待する水準を達成する上での課題の第1位に予算不足を挙げており、売上高が1,000万米ドル以下の企業に至っては71%に上っています。

情報セキュリティ部門の成功における最大の障害は、その価値に対する企業における認知を反映しています。17%の回答者が情報セキュリティ部門は組織のニーズを満たしていると回答している一方で、68%の回答者が依然として、組織のニーズに対して不十分であると感じており、改善を進めていると回答しています。

情報セキュリティ部門はセキュリティ投資の価値を明確に示し、実証していく上で今以上に努力しなければなりません。

65%

企業に価値をもたらす上での1番の障害は予算の制約である

セキュリティは改善しているものの、多くはいまだにリスクにさらされています

およそ3分の1の組織がスレットインテリジェンス（攻撃への理解を深め、対策を立てる）プログラムをいまだに整備しておらず、3分の1強の組織は非正規のプログラムを導入しています。脆弱性の特定に関しては、およそ4分の1の組織がプログラムを整備していません。

インタビューした業界のうち、金融サービス業が最も成熟度が高く、また売上高が10億米ドル以上の企業はサイバーセキュリティプログラムの成熟度が非常に高いという結果になっています。

しかしながら、組織は、業界や規模にかかわらず、多くのセキュリティ分野において全体的に成熟度が不十分で厳しい状況にあることを懸念しなければなりません。こうした重要課題は改善していく必要があります。今後、改善と革新に向けて早急に追加投資することが多くの組織に求められます。結局のところ、セキュリティが侵害された場合、費用がはるかに高くつく可能性があります。

35%

セキュリティプログラムにおけるリーダーまたは先駆者である

いまだに多くの組織において重要な領域との整合性が欠けています

組織は、ビジネス戦略とIT戦略の整合（あらゆるリスク領域を積極的に認識する脅威モデリング（脆弱性の洗い出し）のニーズや、技術主導からビジネス重視の活動への移行など）を進めているものの、リスク選好度あるいは今日のリスク環境との整合を推進している組織はほとんどありません。この点において、金融サービス企業は比較的先行している一方で、急成長市場における企業は後れを取っています。

こうした戦略の不整合から、予算を組む際やリソース要件を決定する際に備えている、あるいは必ず防御しなければならないサイバーリスクを考慮している組織があまりにも少なく、また、内部だけに目を向けて、サイバーリスクへの防御は十分だと自己満足している組織があまりにも多いことがわかります（こうした考えは攻撃を受けた場合に大きな損失を招くおそれがあります）。

62%

情報セキュリティ戦略が組織のリスク選好度/許容度と整合していない

セキュリティ対策の拡大と並行して脅威もそれを上回るペースで拡大しています

31%の回答者が、過去12カ月間でセキュリティインシデントの件数が5%以上増加したと回答しています。

情報セキュリティ機能の改善策を講じる際、組織は改善事項が現在および将来の脅威の予想される規模と頻度に対処できているか、また、脅威の拡大スピードに追いつく形で改善策を実施できるかを検討しなければなりません。より具体的には、改善策がいかに効果的に業務プロセスを保護する上で役立つか理解する必要があります。

59%

外部からの脅威が増加している

31%

過去12カ月間でセキュリティインシデントの件数が増加した

32%

フィッシングがリスクの影響度に最も大きい変化を与えた

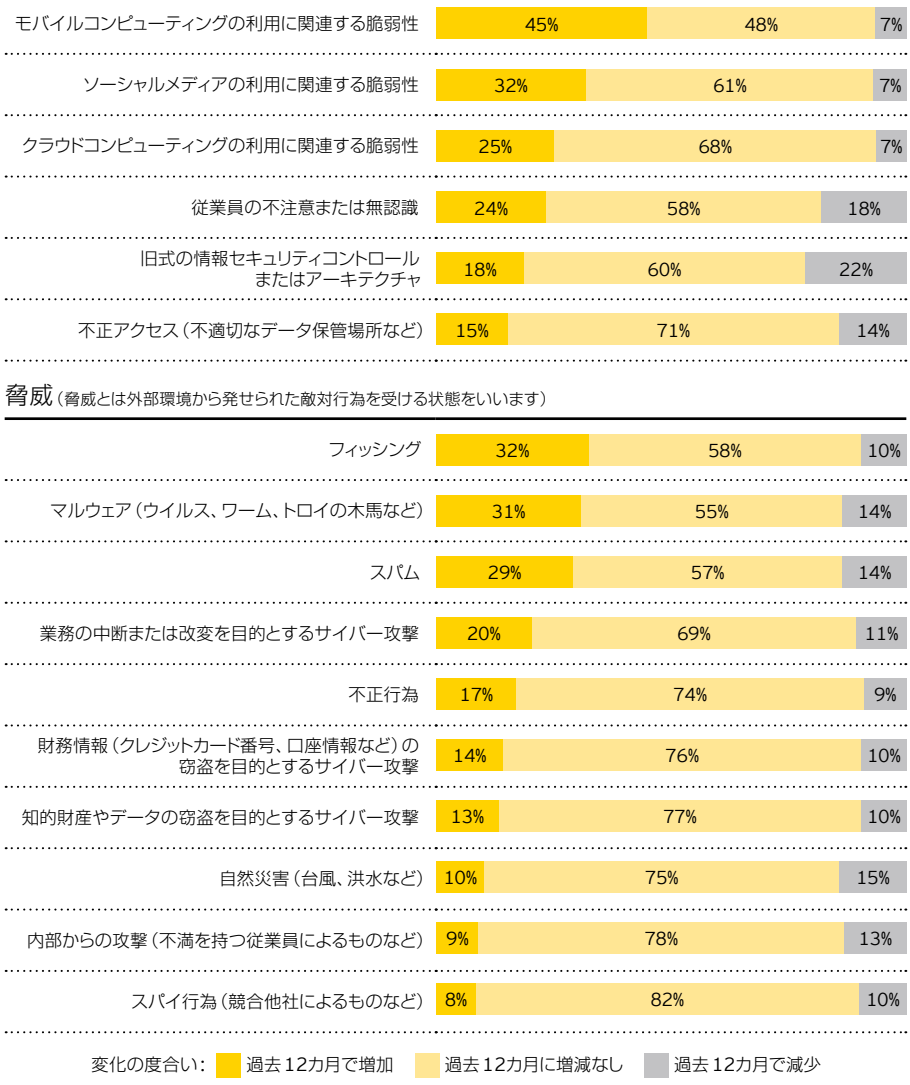
45%

モバイルコンピューティングがリスクの影響度に最も大きい変化を与えた

過去12カ月間で組織は情報セキュリティプログラムの改善を行ってきましたが、まだまだ多くの取組みが求められています。継続的な改善活動における重要な要素であるセキュリティ意識啓蒙活動および研修を最優先事項の第1位あるいは第2位に挙げた回答者はわずか23%で、最下位に挙げた回答者は32%でした。さらに多くの回答者がより優先度の低い項目として挙げた唯一のセキュリティ分野は、脅威および脆弱性管理でした。31%の回答者が脅威および脆弱性管理プログラムを整備していないという結果は驚くべきものです。というのも、脅威や脆弱性を管理することなくして、サイバー脅威が潜んでいる部分や、サイバー攻撃の原因となるおそれのある部分を見極めることはできないからです。

組織は大幅に前進してきたものの、多くの組織にとってはまだ長い道のりがあります。サイバー攻撃のペースが加速し、複雑性が増大し続けている中で、組織は、消費者や株主の信頼を揺るがすような大きな犠牲をもたらし、ブランドが損なわれるセキュリティインシデントが起こるリスクにさらされたままにならないよう早急に行動しなければなりません。

実際に発生したインシデントについて、過去12カ月間で回答者のリスクの影響度（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および脆弱性



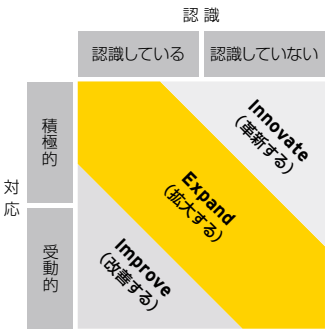
Expand（拡大する）

サイバー脅威と闘うためのリーディングプラクティス

経営層は積極的に未知の脅威に備えるために、支援する姿勢を示していかなければなりません。ただ単に受動的に対応しているだけで満足している組織は、次なる攻撃に打ち勝つことはできません。

サイバー脅威と闘うためのリーディングプラクティス

大部分において、組織は過去12カ月間で情報セキュリティプログラムを改善してきました。しかし、先進的な組織はさらにもう一歩先をゆく改善策を講じていることが調査結果から明らかになっています。特に、先進的な企業が改善の機会を拡大していると私たちが判断する10の分野を4つのカテゴリーに分類しました（12～13ページを参照）。



経営層のコミットメント

- **取締役会の支援**　情報セキュリティ部門に関する明確な規定および長期的な成長戦略を定めるためには、経営層からの支援が必要です。

組織内での整合性

- **戦略**　情報セキュリティ部門は、企業全体を取り巻くさまざまなステークホルダーと強力かつ確立した関係を築き、明確に定められた正式なガバナンスおよび運用モデルを確立しなければなりません。
- **投資**　組織はサイバーセキュリティへ積極的に投資する必要があります。

実行するための人材、プロセス、テクノロジー

- **人材**　今日の情報セキュリティ部門には豊富な経験とさまざまな能力が求められており、技術的なITスキルだけではもはや不十分です。
- **プロセス**　プロセスは文書化し通知することが必要ですが、情報セキュリティ部門は改善の機会が訪れた際にプロセスを迅速に更新する変更管理の仕組みを整えておくことも必要です。
- **テクノロジー**　テクノロジーソリューションを最大限に活用するために、情報セキュリティ部門は、適切なガバナンス、プロセス、研修および意識啓蒙活動に対応した戦略的な取組みを技術展開に反映していかなければなりません。

効果的な運用

- **継続的な改善**　組織は、人材、プロセス、テクノロジーの分野において、継続的にパフォーマンスを監視し、情報セキュリティプログラムを改善するためのフレームワークを確立することが必要です。
- **物理的セキュリティ**　組織はすべての情報セキュリティ技術が物理的に安全であるよう、特にWi-Fiへのアクセスを考慮しておく必要があります。セキュリティオペレーションセンター（SOC）により、情報セキュリティ部門は迅速に対応し、協力的に機能し、効率的に知識を共有できるようになります。
- **分析および報告**　今日の環境において、シグネチャおよびルールベースのツールはもはや有効ではありません。代わりに、情報セキュリティ機能としては、IT環境におけるベースラインよりも行動ベースの分析技術の採用を検討したいと考えるでしょう。
- **環境**　情報セキュリティには、ビジネスの優先事項に関連するイベントを管理し、真のリスクや組織への影響を評価するために、十分に整備された企業資産管理システム（サポートされた業務プロセスの重要性を含む）などの環境が必要とされます。

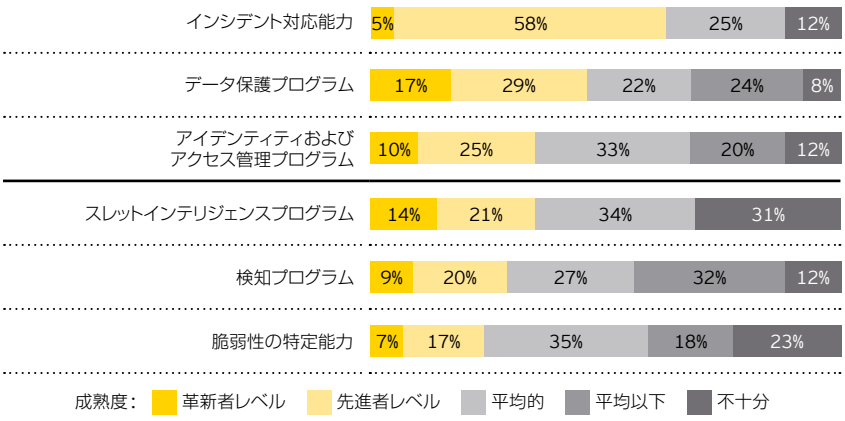
調査結果に加えて、今年は何名かの経営層を対象にインタビューしました。回答者の選定にあたっては、私たちの情報セキュリティにおける経験に基づき、積極的に対応し、未知なるものに注力することでサイバーリスクや脅威からより有効に保護されていると考える組織を対象としました。

インタビューの回答を調査結果の内容と照らし合わせて検討した後、EYの情報セキュリティ専門家による知識と多くのクライアント対応に基づく豊富な経験を活かして、これらの結果にさらなる意義を加えました。調査データ、クライアント対応に基づく経験、EYの知識を結集させ、識別された各改善領域が、4つの広範な改善分野に与える連鎖・累積する効果があるという明確な結論に至りました。最初のステップから着手しなければ（つまり、「経営層のコミットメント」の段階で改善に向けた努力を怠れば）、組織は、後に続くいずれのカテゴリーにおいても、変化を持続させ、これまでの成功を拡大することはできません。

情報セキュリティプログラムの成熟度

調査の中で、6つの主な領域における情報セキュリティプログラムの成熟度について回答者に順位付けをしてもらいました。

アイデンティティおよびアクセス管理プログラムなどの定着した情報セキュリティアプローチに対する回答は、必要とされる成熟度を満たしておらず、スレットインテリジェンスプログラムや脆弱性の特定能力などの比較的最近のアプローチについては、さらに成熟度が低く、さらなる注意が求められます。



回答を集計し、成熟度を「革新者レベル」から「不十分」まで順位付けしました。
高度なプログラムを整備している場合は「革新者レベル」、プログラムを整備していない場合は「不十分」としています。

組織の首脳陣は、情報セキュリティの成熟度を高めるように努め、その実現に対して説明責任を負うようコミットする必要があります。でなければ、情報セキュリティ部門が実施しようとしているその他のどの改善事項についても、意図された利益を実現することはできません。

クライアントとの一対一のインタビューの中で注目したリーディングプラクティスについて、以降のページで示していきます。これらのリーディングプラクティスのうち1つ以上を単独で実践すれば、貴社の情報セキュリティの現状改善に役立つでしょう。しかし、10個の重点領域それぞれにおけるリーディングプラクティスを同時に実践することにより、サイバー脅威対策を大幅に拡大し、貴社の情報セキュリティレベルを飛躍的に変革することができるでしょう。

改善を実現するリーディングプラクティス

「当社の情報セキュリティソリューションは、ビジネスそのものを保護する従来のアーキテクチャから、ビジネス全体を完成させるサービスを保護する方向へと移行しました。これにより、密接合モデルがより柔軟性のある疎結合モデルへと変わり、サービスによってセキュリティ機能を提供し、システムに投入するセキュリティサービスを包括しています」

金融サービス企業

「当社の考えでは、情報セキュリティにおいて最も成功する手法とは発想の転換でした。つまり、運用レベルで問題を検討していたこれまでのやり方から、リスクに基づく新たなアプローチに変更したのです。かつてはむしろ受け身的でしたが、現在は分析、報告、プレゼンテーションによって潜在的な問題を特定し、これらの問題をビジネス部門と共有することでより積極的に解決にあたっています」

テクノロジー企業

「当社は、社内監査や社内の情報セキュリティリスク評価およびセキュリティチェック、社外のIT監査およびコンプライアンスチェックといった社内外の監視を通して情報セキュリティマネジメントシステムの自己最適化プロセスを推進しています」

金融サービス企業

「ビジネスの視点を持った熟練した専門家を擁することは重要です。今日のセキュリティ市場における最大の課題は、イノベーションを起こし、求められるスピードで変化に対応できる専門家を見つけ出すことです」

鉱業・金属企業

経営層のコミットメント　→　組織内での整合性

経営層および取締役会の支援

- リスク選好度を明確に示して、はっきりとした明確な方向性を打ち出す
- 社内監査や情報セキュリティ機能などを通してセキュリティの問題を適時是正するように促す
- 情報セキュリティのパフォーマンスと成功の判断基準を測る
- 組織のすべてのレベルにおいて情報セキュリティ文化を育む
- セキュリティイベントが企業、サービス、製品に与える影響を理解する
- 情報セキュリティに対する洞察を直接経営層の意思決定プロセスに組み込む
- 情報セキュリティ脅威による影響を損益計算書および貸借対照表上に置き換える

戦 略

- すべての関連するステークホルダーを特定し、関与させる
- 全社的なSOCを設置し、包括的なスレットインテリジェンスおよび脆弱性の監視などを行う
- セキュリティ戦略を組織全体のビジネス戦略と整合させる
- どのセキュリティ機能を社内に整備するか、あるいは外部に委託するか、クラウド上で整備するか決定する
- 信頼できる基準（ISO、COSO、COBITなど）を利用して企業およびステークホルダーの信頼を高め、これらの基準と整合させる、あるいは正式な認証を取得することを検討する
- 独立したサードパーティーによる評価を実施した後、外部からセカンドオピニオンを得る
- 「安全な」組織とは何か定義づけし、成功を測るKRIおよびKPIを設定する
- パートナー企業やベンダーの専門性を活用する
- 受動的に反応するのではなく、率先して予測する情報セキュリティ組織、運用モデルを構築する

投 資

- サイバーセキュリティへの投資者を特定する
- 全体的なリスクフレームワークを定めて、広がりつつあるリスクの現状を把握する
- セキュリティへの新たな取組みを優先して、セキュリティ投資を促進する
- 期待される利益を分類する（ブランド保護、リスク低減、コンプライアンスの向上、コスト削減など）
- 保守およびインシデント対応への支出を減らし、改善および革新への支出を増やす

すべての企業がサイバー攻撃の標的となっています。攻撃の動機や手段、機会はさまざまですが、以下のライフサイクルにおいて企業がより一層リスクにさらされることがわかっています。

- **大規模な組織・構造改革**　新技術によりマーケティング、顧客重視の新たな取組みが推し進められていますが、それに伴う情報セキュリティ手段は必ずしもそのペースに追いついているわけではありません。マーケティングおよび開発部門が新技術に伴うリスクや脅威を認識し、それらの対応に備えているとは限りません。また、組織改革によって従業員のまとまりがなくなったり、注意力が散漫になったりしてテスト済みのセキュリティ手段や手順が忘れ去られる、あるいは破棄されてしまうおそれがあります。
- **M&A**　新たなシステムやポリシー、セーフガードの導入により、情報セキュリティシステム、手段、手順の間にギャップが生じる可能性があります。M&Aは人員削減を伴うことが多く、企業のシステムやプロセス、セキュリティ手段に精通している多くの意欲的な元従業員が不満を募らせて、セキュリティ侵害へと駆り立てられることがあります。
- **新市場への参入**　新市場への参入は、通常、新たなプロセス、ベンダー、バイヤー、システム、さらには新たな言語や文化を意味します。これらの要因はすべて、セキュリティリスクおよび脅威の認識のレベルがそれぞれ異なります。プライバシー、コミュニケーションおよびデータセキュリティに関する政府の規制にあまり精通していないため、セキュリティ環境はさらに複雑化します。
- **注目度の高い事象の発生時**　ハッカーやサイバー攻撃者は、他のことに気を取られている企業を標的にするために広報活動が混乱している機会を利用することがよくあります。こうした機会では、従業員や株主が不規則に予想外の行動を取る可能性があり、さまざまなプラットフォーム上に拡大する脅威を特定し、それらに対処する企業の能力が損なわれるおそれがあります。短期的な問題を解決するような「何か起こってからの緊急対策」は、現実的に侵入されるリスクを高め、長期的なリスクをもたらしうる課題があります。

実行するための人材、プロセス、テクノロジー

人 材

- セキュリティ責任および組織の資産、IP、データ、テクノロジーの適切な利用に対する従業員の意識を向上させる
- 適切なスキルと能力を有する人材（ハイリスクの役職を含む）を探して採用する
- 従業員の業績評価に情報セキュリティに関する項目を含める
- 管理者権限を持っている者を把握、管理する
- 社内で「セキュリティ知識に優れた人材」を育成する

プロセス

- 契約の中に検証済みの強制力のある条項を定め、情報セキュリティの責任と説明責任をパートナー企業やベンダーに負わせる
- 情報セキュリティプロセスを説明して、従業員に規則および手順を理解してもらい、社内での共通認識を図る
- 広く認められている基準（ISO 27001など）と整合させる
- 情報セキュリティを独立した機能としてではなく、組織におけるGRC（統合リスク管理）機能の重要な一部として組み込む
- 外部委託しているサービスの中に統制の継続的な保証モニタリングを設定する
- コンプライアンスおよび規制要件と、脅威の現状把握を区別する
- リスク管理プロセスにビジネス部門を関与させて、重要リスクの特定能力およびセキュリティ意識を向上させる
- サイバーガバナンスを業務および業務プロセスに組み入れる
- 潜在的なセキュリティ侵害を予測し、十分なインシデント対応とコミュニケーション方法を確立する

テクノロジー

- IT、運用技術、情報セキュリティ間で明確な関係を構築する
- テクノロジーの選択と、テクノロジーがもたらす脅威および脆弱性とのバランスをとる
- 情報セキュリティをITプロジェクトの重要な一部として組み込むことで、新たな情報システムを初めから安全な状態にしておく
- 信頼しているテクノロジーの一覧を理解し、具体的な基準を定める
- 機密データと重要なビジネスサービスを含むテクノロジー資産をリアルタイムに監視できる能力を開発する
- アプリケーションレベルおよびインフラレベルで定期的にセキュリティをテストする
- 情報セキュリティにおける取組みを製品の安全性、サービスの堅牢性、顧客満足と整合させる
- 情報セキュリティを製品/サービス提供の中に取り込む

効果的な運用

継続的な改善

- 業界団体、司法当局、同業他社、規制当局、専門アドバイザーの知識を利用する
- 新たな技術や脅威の現状を継続的に再評価し、適切な優先事項に注力できているか確認する
- セキュリティシミュレーションサンドボックス/機能を確立し、ハッカーの立場からセキュリティをテストする
- 常に注意を怠らず、市場で何が起きているか耳を傾け、情報セキュリティの新たな動向や新たな脅威を理解し、それに従ってリスク評価を調整する
- 情報セキュリティ部門にイノベーション機能を組み込み、新技術における情報セキュリティの課題に先手を打つ

物理的セキュリティ

- ワイヤレス機器を考慮して物理的セキュリティとネットワークセキュリティの関連を把握する
- 効果的な防御策には、情報セキュリティ、人事、IT、法務部門間における密接な協力が求められる
- 物理的なITセキュリティと情報セキュリティ間の連携を向上する
- 先端技術に対するリスク分析を体系的に実施する

分析および報告

- 社内外の複数の者に独立した評価を委託し、GRCおよび情報セキュリティ機能の有効性を評価する
- 分析的ツール/モデルを用いて、イベント間の隠れた関係を見つけ出し、異常なふるまいを検知する総体的な機能を構築する
- セキュリティ脆弱性とコンプライアンス改善度を測るために、専門のセキュリティ保証レポート機能を設置する
- 外部脅威の現在のレベルを調査、評価し、IT部門およびビジネス部門に早期に警告を発して、危機対応チームを編成する
- サイバーセキュリティ脅威が損益計算書、貸借対照表、評判、ブランドに及ぼす影響を取締役会に提示する
- サービスプロバイダーや認証団体と連携して情報やリーディングプラクティスの交換を行う

環 境

- 第一、第二、第三防衛ラインを整理して責任を再確認し、重複する職務を削減する
- 効果的な防御策には、情報セキュリティとIT部門間における密接な協力が求められる
- 重要資産およびその脆弱性を理解し、インフラレベルへの攻撃を慎重に監視する

「成功する手法で重要なことは、理解できること、適用できることです。一般的に、難解な学術的アプローチとは逆の現実的な実践が好まれるものです。明確な標準化された質問項目を通して業務プロセス全体における情報関連リスクを特定し、確認した結果から得られた情報を検証した上で、この情報を利用して自社の重要資産を見極め、関連するすべてのステークホルダーを検討する必要があります。こうすることで、企業はビジネスへの影響とリスク評価を、提案するリスク低減策と合わせて明確にすることができます」

石油・ガス企業

「サードパーティーとのパートナーシップにより、外部の市場知識や専門知識を利用して情報セキュリティプログラムや関連する改善プログラムを設計できるようになりました。また、セキュリティアーキテクチャ·設計、セキュリティテスト、セキュリティインシデント対応・調査に対する需要の急速な高まりに対応するように、リソース要件を変更することもできるようになりました。コソーシング/外部委託は、コスト削減という理由以上に、能力が向上するという利点の方が大きな役割を果たすと見られています」

金融サービス企業

「適切な機能である『コアコマンドセンター（情報セキュリティ、IT、事業部のリーダー、コミュニケーション、マーケティングおよび物理的セキュリティ担当者間における連携機能）』に適切な人材をそろえておくことが重要です。ビジネスのあらゆる局面について適切なコネクションをもっている人材の名前を予め把握しておくべきす。そして、適切な幹部レベルの人材、つまり意思決定の権限者が常時対応できることが必要です」

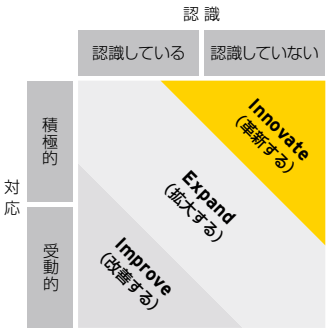
金融サービス企業

Innovate（革新する）

生き残るためにはイノベーションが変革を引き起こす

革新的な情報セキュリティソリューションによって既知のサイバーリスクを防御し、未知なる将来に備えることができます。

昨年1年間で、多くの組織が、既知のサイバーリスクから自らをより安全に守るために、現行の情報セキュリティプログラムを改善してきました。また、優れた組織は、さらに積極的に既知および未知のサイバーリスクに先手を打つための改善機会を拡大してきました。しかし、サイバー脅威との闘いで革新者になるためには、私たちが明確に示した4つの主なカテゴリーにおける10のリーディングプラクティスのはるか先を行く必要があります。革新者は、先端技術がもたらすそれぞれの機会における脆弱性を見つけ出すべく、常に水平線を見渡していなければなりません。

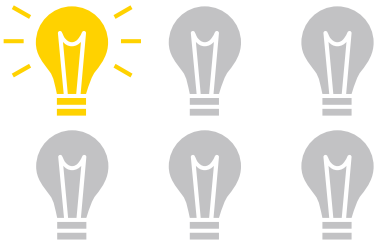


セキュリティイノベーションに向けた予算配分は年々増えており、組織は未知なる将来に備えるための革新的なソリューションにさらに多くのリソースや労力を投入できるようになってきました。

しかしながら、いまだに多くの組織が、イノベーションを起こす先駆者になるには予算が不十分だと感じています。このことから、新たな技術を評価する際にはその利点を理解するだけでなく、重要な知識のギャップや関連するサイバー脅威、つまり、組織のテクノロジー精通度やこれらのリスク対応能力についても理解するように多くの時間と労力を費やすことが重要です。未知なるリスクが既知のリスクとなれば、組織は重要性に従ってリスクの優先順位を付けて対処できます。

50%

今後12カ月間で予算が5%～25%以上増加する



14%

今後12カ月間でセキュリティイノベーション（先端技術）に向けられる費用の割合

先端技術とトレンド

調査の中で、私たちは回答者に以下の13の先端技術とトレンドについて、重要度を回答してもらいました。私たちはこれらの技術とトレンドを3つのカテゴリー（現行の技術、近く普及する技術、将来登場する最先端技術）に分類しました。

◆ 現行の技術

現行の技術はここ数年多くの組織が認識しているもので、その多くは既に導入されています。以下に例を挙げます。

- **電子デバイス**　以下に関連するセキュリティおよびリスク対策を含む
  - スマートフォンおよびタブレット
  - ソフトウェアアプリケーション
  - オンラインアプリケーション（HTML5）およびモバイル画面に合わせたウェブデザイン
- **ソーシャルメディア**　電子ビジネス事業者やネットワーク仲介業者の台頭を背景として

● 近く普及する技術

近く普及する技術はここ最近注目されており、近いうちに導入や採用が拡大してくる可能性があります。以下に例を挙げます。

- **ビッグデータ**　管理下にある指数関数的なボリュームかつ複雑なデータを意味する
- **企業用アプリケーションストア**　従業員が要望するアプリケーションを購入した場合の生産性の向上と比較した関連コストを含む
- **サプライチェーンマネジメント**　外部資産（顧客、サプライヤー、ベンダー、請負業者、パートナー企業）がセキュリティに与える影響度について
- **クラウドサービス仲介事業**　仲介業者がどのようにクラウドセキュリティやプライバシーおよびコンプライアンス問題に対応しているか
- **個人使用のクラウドの活用**　企業、サードパーティー、あるいはその両者によって保有、管理、運用され、社内あるいは社外に設置されている個人のクラウドインフラや、クラウドオーナーのみが管理している関連データおよびアプリケーションへのアクセスを含む

■ 将来登場する最先端技術

将来登場する最先端技術はコンセプトや発想の段階から前進しており、いずれ実用化する可能性があります。以下に例を挙げます。

- **インメモリコンピューティング**　複雑なデータベースの代わりにメインとなるランダムアクセスメモリの中にデータを保存し、膨大なデータのリアルタイムな分析を可能にする
- **モノのインターネット**（内蔵センサー、画像認識技術など）　セキュリティプログラムの中で用いられているが、今後は日常生活の中にさらに取り入れられていく
- **電子マネー**　モバイルマネーサービスに関連する不正やマネーロンダリング問題に対処するために関連法令を整備する必要がある
- **サイバーヘイブン**　面倒な規制なしに、データホスティングサービスを提供する国

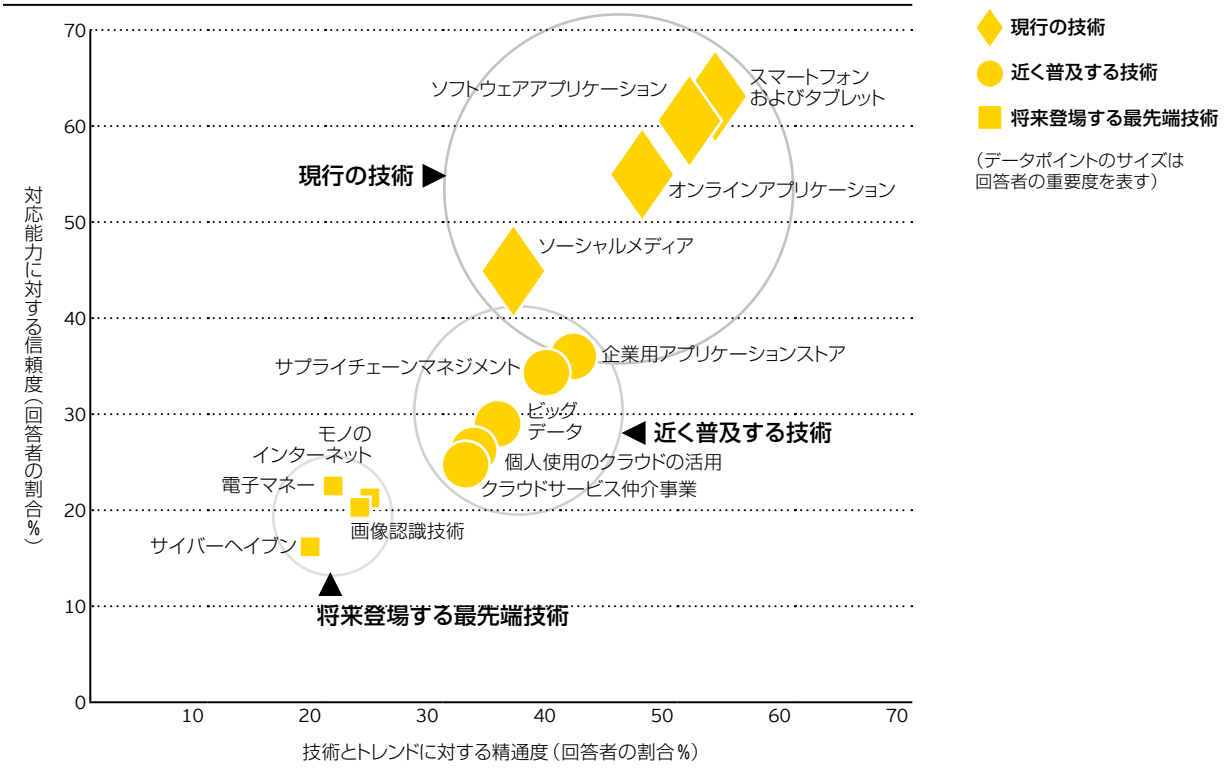
私たちは回答者に先端技術とトレンドについて、重要度の他に精通度を評価してもらった上で、これらの先端技術がもたらす影響に対する対応能力に関して信頼度を評価してもらいました。

- **精通度**　先端技術について理解しているか？
- **対応能力**　先端技術がセキュリティに与える影響に対処できるか？
- **重要度**　先端技術による脅威をどの程度重視しているか？

また、インタビューの中で、先端技術および個人使用のクラウドの活用といったトレンドに対する考えを答えてもらいました。これらの結果とEYのセキュリティ専門家による分析から、私たちは精通度と対応能力に対する重要度を位置付ける相関図を作成しました。

横軸は精通度を表し、円の大きさは重要度を示しています。予想通り、組織の精通度と先端技術に対する重要度の間に相関関係が見られます。縦軸は、サイバー脅威を防御し、脆弱性を低減する能力に対して組織が現在どの程度信頼しているかを示しています。

先端技術とトレンド

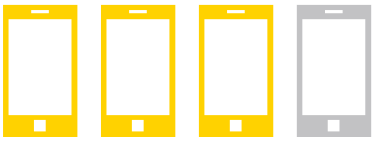


26%

個人使用のクラウドの活用は重要である

19%

インメモリコンピューティングは重要である



70%

スマートフォンおよびタブレットの
セキュリティは重要である

71%

ソフトウェアアプリケーションの
セキュリティは重要である

多くの組織は現行の技術を重視

「先端技術とトレンド」の相関図（17ページ）で示されているように、重要度、精通度、対応能力に対する信頼度の観点から現行の技術とトレンドが最も重視されています。多くの場合、組織はこれらの技術について理解しており、既に導入済みの場合がほとんどです。

しかしながら、電子デバイスの重要度は高いと予想していたものの、スマートフォンおよびタブレットが重要であるとした回答者は70%に留まり、これらの機器のユビキタス性を考えると低い結果となりました。数年前まで、組織は従業員が仕事のために個人のスマートフォンやタブレットを社内に持ち込むことなど想像もできなかったことでしょう。実際、個人所有機器の持込み（BYOD）は2009年に市場に登場したばかりで、BYODが幅広く採用されはじめたのはつい最近のことです。

しかし、スマートフォンやタブレットを利用している従業員が機密セキュリティを侵害したというニュースを頻繁に耳にする中で、誰がスマートフォンのデータに対して責任を負うのか（雇用者か従業員か）、という疑問が生じてきます。また、どの程度の頻度でスマートフォンはアップデートされ、セキュリティ通知が行われているのでしょうか。

現行の技術が組織のネットワークや文化においてさらに定着すると、組織は従業員が職場とプライベートな場でどのように機器を使用するのか考慮しておく必要があります。これは、特にソーシャルメディアについていえることです。これは引き続き、リスクへの対応能力において組織がいまだに信頼できないと感じている分野であることが調査結果からわかりました。

職場でモバイル機器が使用されるようになって4年が経つというのに、組織における信頼度がいまだに低いのであれば、パーソナル/ホステッドクラウドを管理し、防御するという課題にどのように対処していけばよいのでしょうか。さらに、現行の技術対応にすべての労力を費やしているのだとしたら、近く普及する技術や将来登場する最先端技術に対してどのように備えていけるでしょうか。

組織はもっと将来に目を向けていかなければなりません。今や現行の技術となった電子デバイスやソーシャルメディアについて見てみると、組織はそれらが将来の先端技術として登場し始めていた時に備えておくべきでした。いまだに現在使用している技術への対応能力を改善しているようなら、近く普及する技術から組織を積極的に守るための備えに時間を割く余裕はないでしょう。

回答者からのリーディングプラクティスに関する提案

- 「後れを取っているならば、行く手を阻んだり、所有したり管理したりするためではなく、物事を前進させ、実現するためにビジネス部門とIT部門で双方向のディスカッションを行うべきです」— 小売・卸企業
- 「プライバシー、セキュリティ、不正に関する機能は統合するべきです。顧客や従業員が個人情報とみなすものは変化していかなければなりません」— 金融サービス企業
- 「情報セキュリティにおける最大の弱点は人材に関する点です。ですから、私たちは常に意識啓蒙プログラムを改善し、新たなセキュリティ手段を導入しています」— 金融サービス企業
- 「私たちはアプリケーションの中に脅威やリスクを見出しています。以前はネットワークや無防備なシステムを保護していましたが、今はネットワーク全体を通してすべてのシステムをアプリケーションレベル（Eメールや添付ファイルなどのアプリケーション内の情報を含む）で保護する必要があります」— 小売・卸企業

近く普及する技術とトレンドに対する重要度は中程度

「近く普及する技術」に分類された技術（ここ数年、認識はされているものの、まだ導入されていない、あるいは広く採用されていない技術）については、重要度、精通度、関連するサイバーリスクへの対応能力に対する信頼度の観点から中程度の評価となりました。

一般的に、組織はこれらの技術を業績改善や競争優位性を生み出す機会として捉えています。近い将来、これらの技術の重要性が大幅に増してくる可能性が高いことから、これは精通度および対応能力に対する信頼度を今のうちに高めておく必要がある分野です。

ビッグデータ、サプライチェーンマネジメント、企業用アプリケーションストア（シャドーITとして知られている場合もあります）という用語は既に企業で使われています。BYODがちょうど1年前に採用されたのと同じように、個人使用のクラウドの活用やクラウドサービス仲介事業も組織内に採用されつつあります。組織は、これらの技術に関連するサイバーリスクやこれらのリスクに対する組織の脆弱性および低減策について、今、理解しておく必要があります。技術を採用する時点でサイバー脅威を確認するのではあまりにも遅すぎます。

近く普及する技術を考慮する上で回答者に共通する見方

「提携あるいはコソーシングを通してギャップを埋める計画を立てます。現行のツールや技術を十分に利用して監視能力を強化します。サービスプロバイダーのデューディリジェンスを高め、より強固なインシデント管理プロセスを作り出し、スレットインテリジェンスを確立しています」
— 金融サービス企業

「セキュリティインテリジェンスが将来を左右する鍵となります。・・・（中略）攻撃者を見つけ出すにはビッグデータによる手段が必要です」
— 金融サービス企業

将来登場する最先端技術とトレンドにはさらなる注目が必要

組織は目の前にある技術にかなりの労力を費やしているため、今のところ、「将来登場する最先端技術」に分類された技術とトレンドには十分に配慮していません。技術が出現し、採用されるスピードが加速している中で、私たちが考えるよりも未来は間近に迫っています。

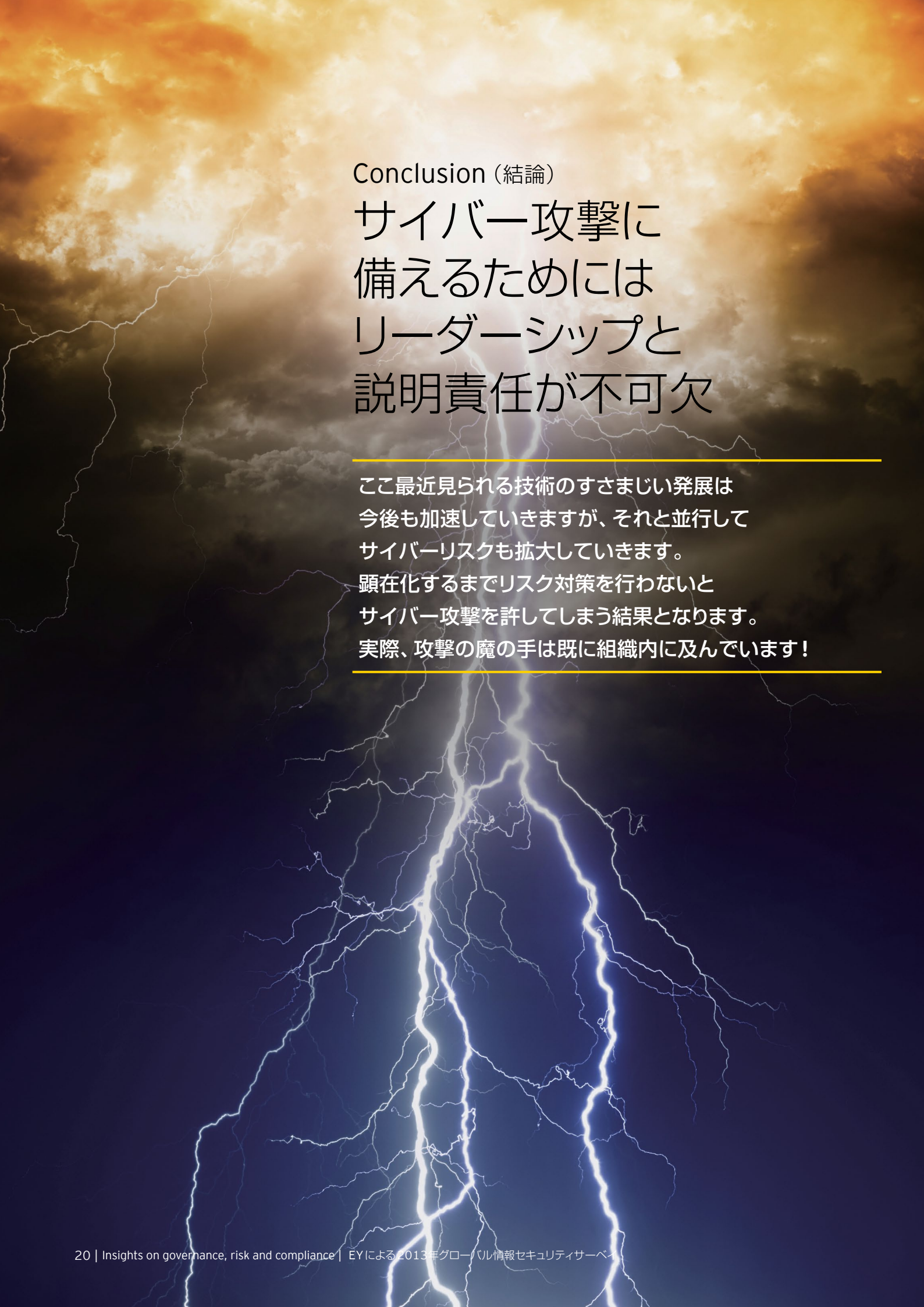
成熟した組織は既にこれらの技術について検討を始めています。これらの組織は、情報セキュリティプログラムを見直し、再考し、場合によっては再設計して将来の技術に備え、イノベーションにより得られる利益を測定しています。

サイバー脅威に先手を打ちたい（あるいは、少なくとも追いつきたい）と考えているならば、近く普及する技術に関連する既知および未知のリスクのみならず、将来登場する最先端技術に関連するリスクについても積極的に対応していかなければなりません。機会および脅威の把握に向けて人材を投入し、その結果に基づいて行動する必要があります。また、必要に応じて、情報セキュリティプログラムを抜本的に変革する準備をしておく必要があります。こうした備えを怠ると、情報セキュリティプログラムと組織が直面しているサイバー脅威とのギャップが拡大し続けることになるでしょう。

将来登場する最先端技術とトレンドを考慮する上で回答者に共通する見方

「情報セキュリティを完璧に整備したということは決してできません。もしそういえるのだとしたら、それは単なる自己満足に過ぎません。脅威とセキュリティ手段の間にある潜在的なギャップを埋めることは終わりなき闘いなのです。このギャップを埋めるためには、既成の枠を超えなければなりません。当社は市場に耳を傾け、情報セキュリティにおける新たなトレンドを理解し、新たな脅威やその対応策を明確にするよう努めています。常に慎重でなければなりません。最も大切なことは、全体的な視点で捉え、柔軟な姿勢を持ち、議論や協力を受け入れることです。組織内だけでなく、さまざまな組織の枠組みを超えて、こうした姿勢を持つことが必要です」
— 金融サービス企業

「新技術によって、事前に考えておかなければならない新たな課題が生じてくるでしょう」
— 専門サービス企業



Conclusion（結論）

サイバー攻撃に備えるためにはリーダーシップと説明責任が不可欠

ここ最近見られる技術のすさまじい発展は今後も加速していきますが、それと並行してサイバーリスクも拡大していきます。顕在化するまでリスク対策を行わないとサイバー攻撃を許してしまう結果となります。実際、攻撃の魔の手は既に組織内に及んでいます！

組織は既に認識しているリスクへの対応策を大幅に改善してきました。しかし、情報セキュリティ部門が企業のニーズを十分に満たしていると答えた回答者はわずか17%に留まっており、組織にとってはまだ長い道のりがあります。

しかも、残された時間はあとわずかです。中でも近く普及する技術や将来登場する最先端技術に関連する未知のサイバーリスクが急激に増加しており、組織はそのスピードに追いつけずにいます。

現在、新技術によってマーケティング、顧客重視の新たな取組みが推し進められている一方で、情報セキュリティは関連するサイバー脅威を後から追う形になっています。M&A、組織の構造改革、新市場への参入といった要因すべてが、十分な保護機能を提供する情報セキュリティ部門にさらなるストレスとなってのしかかっています。

私たちの調査結果が示しているように、組織は従業員の意識啓蒙、予算の増額、革新的なセキュリティソリューションへのリソースの投入を今以上に重視しなければなりません。組織のトップにいる経営層はソリューションの8割が非技術的なものであることを認識し、これらの取組みを支援していく必要があり、これをもって優れたガバナンスといえるでしょう。

留まるところを知らないサイバー攻撃

過去12カ月間で攻撃の頻度が増したと答えた回答者数は、減少したと答えた回答者と比べて倍以上にも上りました。攻撃者が組織のセキュリティ境界に上手く侵入した場合、少なくとも組織の気を散らし、最悪の場合はセキュリティが麻痺してしまうことになります。セキュリティ侵害は組織の重要な目的を阻むおそれがあります。株主・アナリスト・消費者からの信頼を損ない、ブランドの評判を傷つけ、甚大な財政的損害をもたらしかねません。

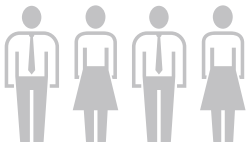
多くの場合、情報セキュリティはコンプライアンス上必要なもので、企業にとってコスト負担になると考えられています。経営層は情報セキュリティを企業と顧客に真に利益をもたらす機会と捉えるべきです。そして、本書に示されているリーディングプラクティスに目を通し、どのようにして自社に当てはめることができるか検討していく必要があります。しかし、今後12カ月間で新たなセキュリティソリューションのイノベーションに充てる予算支出が14%に過ぎないという回答結果からすると、ハッカーが組織に打撃を与える可能性は高いどころか必然的と言わざるを得ません。

「サイバー犯罪は今日における企業の生き残りを掛けたサバイバル競争にとって最大の脅威です」

ケン・アラン
EYグローバル情報セキュリティリーダー

調査の方法

回答者のデータ



1,909
回答者数

64
国数

25
業界数

EYは2013年6月から7月にかけて、グローバル情報セキュリティサーベイを実施しました。主要な業界に従事する64カ国の1,900社以上の方から回答をいただきました。

サーベイにあたり、CIO、CISO、CFO、CEOその他情報セキュリティに関与している担当役員に参加を依頼しました。EYの国別プラクティス担当プロフェッショナルにサーベイのプロセスを統一するための説明書とともに質問表を配布しました。

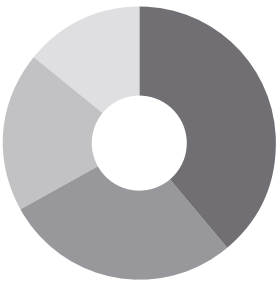
サーベイの回答の大半は対面インタビューによって集めたものですが、インタビューができない場合は、オンラインで調査を実施しました。

来年以降、EYのグローバル情報セキュリティサーベイへの参加をご希望の方は、弊社の担当者あるいは最寄りのオフィスまでお問い合わせいただくか、www.ey.com/gissにアクセスしてリクエストフォームをご記入ください。

回答者の業界分布

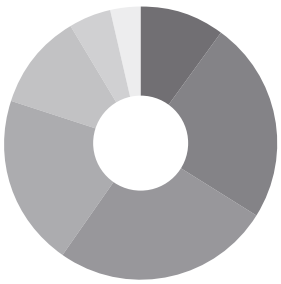
航空宇宙・防衛	47
航空会社	12
資産運用・管理	42
自動車	66
銀行・証券	361
化学	35
クリーンテクノロジー（環境保全技術）	5
消費者製品	116
各種産業用製品	128
政府・公共部門	128
ヘルスケア	37
保険	125
ライフサイエンス	47
メディア・娯楽	57
鉱業・金属	39
石油・ガス	43
電力・公益事業	61
プライベート・エクイティ	3
専門サービス	73
ケアプロバイダー	12
不動産	69
小売・卸	98
テクノロジー	179
電気通信	72
輸送	54

回答者の地域分布（1,909名）



地域：	
EMEIA（欧州、中東、インド、およびアフリカ）	39%
南北アメリカ	28%
アジア太平洋	19%
日本	14%

回答企業の年間総収益



収益：	
100億米ドル～500億米ドル未満	196
10億米ドル～100億米ドル未満	455
1億米ドル～10億米ドル未満	492
1,000万米ドル～1億米ドル未満	388
1,000万米ドル未満	217
政府、非営利団体	96
該当しない	65

ソートリーダーシップ関連出版物のご紹介

EYは情報セキュリティに関するソートリーダーシップを含め、**「Insights on governance, risk, and compliance」**シリーズを定期的に発行しています。本シリーズは、経営幹部レベルの役員にとって重要な問題に関して価値ある洞察をタイムリーに提供することにより、クライアント企業の一助となるよう構成されています。www.ey.com/GRCinsightsをご覧ください。

"Beating cybercrime. Security Program Management from the Board's perspective."
※日本語版作成中

多くの組織は目まぐるしく変化するテクノロジーや脅威の拡大スピードについていくのに苦戦しており、組織の存続能力を脅かす真のリスクと、これらのリスクに効果的に対応し、低減する組織の能力との間に危険なギャップが生じています。EYのセキュリティプログラム管理アプローチを活用すれば、組織は情報セキュリティプログラムおよびその構造を客観的に評価できます。

"Cybersecurity: considerations for the audit committee" ※英語版のみ

サイバーセキュリティは単なるテクノロジーの問題ではなく、企業全体で対応しなければならないビジネスリスクです。取締役会はこの問題に注意を払い始めています。特に監査委員会の委員は現在、重要課題の中にサイバーセキュリティを挙げるようになっています。

"Security Operations Centers against cyber crime. Top 10 considerations for success."
※英語版のみ

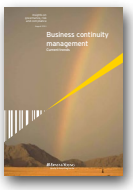
企業は、機密情報への攻撃を完全に防御することは決してできないことを認識し、適切に対処できるよう検知能力を高めておかなければなりません。こうした取組みの中で中心的役割を果たすのは、十分に機能したセキュリティオペレーションセンター（SOC）です。本書では、SOCの成功にとって鍵となる上位10項目を考察しています。

"Identity and access management (IAM): beyond compliance"
『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』

アイデンティティ・アクセス管理は、コンプライアンス中心のプログラムから真のビジネス基盤へと変革するための新技術を活用しながら、権限管理やロジカルアクセス制御ができるリスクベースのプログラムへと進化しています。

"Business continuity management" ※英語版のみ

およそ半数の企業が、企業の存続を脅かすおそれがある災害時において事業を継続させるための対策を講じていません。災害の影響でリソースが確保できなくなってしまうと多大な損害を招くことになりかねません。優れた企業は効果的な事業継続性管理プログラムを策定、維持、継続する必要性を一層認識するようになっています。

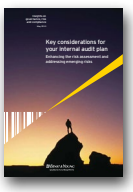


"Privacy trends: the uphill climb continues"
『プライバシートレンド：前途多難な状況が続く』

プライバシーに関する展望が進化し、成熟していく中で、いかにして市況が企業のプライバシー判断に影響を及ぼしているかという点を中心にトレンドが形成されています。本書では、プライバシー保護における新たな時代へと突入する中で、ますます大きな役割を果たしている三つの大きな潮流（ガバナンス、テクノロジー、規制）を取り上げ、考察しています。

"Key considerations for your internal audit plan: enhancing the risk assessment and addressing emerging risks" ※日本語版作成中

内部監査におけるリスク評価と継続的な見直しプロセスは、企業に大きな利益をもたらすために内部監査業務で実施する項目を特定、精査する上で重要となります。このプロセスでは、新たなリスクと重点分野を特定し、それらに対応する実務的な、価値に基づく監査を判断していくことから始めます。



EYと情報システムコントロール協会（ISACA）が発行したサイバーセキュリティに関するレポートもご参照ください。

EYのリスクサービスについて

私たちは企業リスクのあらゆる側面を総合的な視点で捉えています。EYは内部監査、財務リスクおよび管理におけるマーケットリーダーです。また、ガバナンス、リスク、コンプライアンスを含むその他の分野、ならびに全社的リスクマネジメントにおける能力を常に高めています。

私たちは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において他社をリードすべく革新し続けています。業界屈指の技術的なIT関連のリスクマネジメントに関する深い知識を生かして、IT統制の設計、実行、合理化に焦点をあてたIT統制サービスを提供しており、これによりクライアントのアプリケーション、インフラ、データに潜むリスクの低減を実現していきます。情報セキュリティは、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の現在の展望の中でEYがリーダーとして広く認められている注目分野です。

連絡先

Japan		
東　義弘	03 3503 3500	azuma-yshhr@shinnihon.or.jp
横川　晴良	03 3503 1704	yokokawa-hrysh@shinnihon.or.jp
Global		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Americas		
Jay Layman	+1 312 879 5071	jay.layman@ey.com
Europe, Middle East, India and Africa (EMEIA)		
Jonathan Blackmore	+44 20 795 11616	jblackmore@uk.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.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。

本書はSCORE no. AU1885の翻訳版です。
ED 0115

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 2846
E-mail: AS-Markets@shinnihon.or.jp