セキュリティの進化

ビジネスへの組み込み
(セキュリティ・バイ・デザイン)

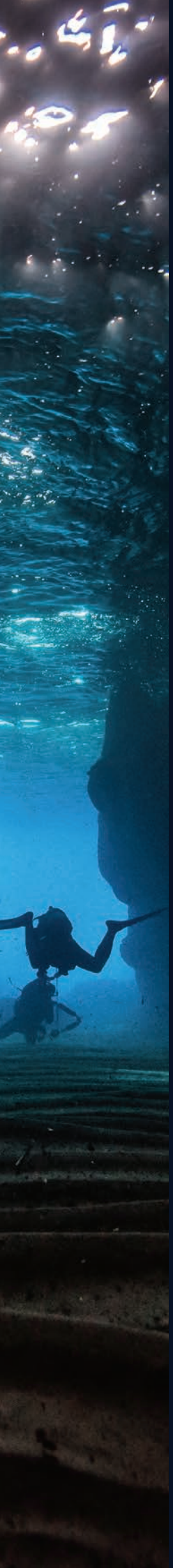
セキュリティ機能と事業部門の連携強化による
ビジネスと一体化したセキュリティ
プログラムの構築に向けて

EYグローバル情報セキュリティサーベイ
(GISS)2020

Building a better working world

EY GISSへようこそ

目次



Kris Lovejoy

EY Globalアドバイザリー・サイバーセキュリティ・リーダー

第22回EYグローバル情報セキュリティサーベイ（GISS）をご覧いただきありがとうございます。本書では、組織が現在直面しているサイバーセキュリティの重大な問題を掘り下げていきます。

組織におけるサイバーセキュリティ対策についてEYが調査を開始してから20年以上が経過しました。その間、サイバー攻撃の脅威は年々高まり、その形態もさまざまに変化し続け、私たちは今、かつてないほど多くの脅威に晒されています。悪意のある攻撃者の多様化、巧妙化も進み、攻撃の動機についてもインシデントごとに大きく異なる場合が少なくありません。

一方で、朗報もあります。取締役会と経営層はサイバーセキュリティやプライバシー保護に関する課題に以前にも増して積極的に取り組んでいます。変革の時代の到来を受け、経営層はサイバー攻撃に対する脆弱性や潜在的危険性を強く認識しています。

しかし、それだけでは十分ではありません。サイバーセキュリティは、進化するリスクだけにフォーカスして対策を講じればよいわけではなく、組織のイノベーションや変革プロセスにセキュリティを統合し組み込むことが不可欠です。つまり、「セキュリティ・バイ・デザイン」の実践こそが各組織が目指すべき姿でしょう。

今年度のGISSでは、このテーマを詳細に掘り下げています。本調査には1,300近い企業の皆さまがご参加くださいました。この場を借りまして、心よりお礼申し上げます。すべての組織のサイバーセキュリティがより良いものになるように、知識と経験を分かち合い、共に取り組んでまいりましょう。

「セキュリティ・バイ・デザイン」とは？

「セキュリティ・バイ・デザイン」は、サイバーセキュリティを後付けではなく、製品やサービスの企画・設計段階から組み込むという、セキュリティ対策の新しいアプローチです。このアプローチをとることにより、イノベーションの信頼性が担保されます。また、組織のあらゆる面に適用できる、戦略的かつ実用的なアプローチであるため、ビジネスプロジェクトの全ライフサイクルで「セキュリティ・バイ・デザイン」が有効的に働き、セキュリティリスクの持続的な管理と軽減が実現します。

エグゼクティブサマリー

破壊的変革の時代にある今、サイバー攻撃の脅威はますます高まっています。そのような環境だからこそ、最も先進的な考え方に基づくサイバーセキュリティ機能は、変革の重要な鍵になり得るでしょう。しかし、その役割を十分に発揮するためには、CISO（最高情報セキュリティ責任者）、取締役会、上級経営層、各事業部門の相互関係を新たに醸成することが組織に求められています。

EYの主な推奨事項

本年度のGISSの結果は、今こそ、サイバーセキュリティをビジネストランスフォーメーションやイノベーションの中核に位置づける時であるということを明確に示しています。これを実現するためには、取締役会、上級管理職層、CISO、全ての事業部門のリーダーが一丸となって取り組むことが不可欠です。以下、EYが推奨する取り組みポイントを5つご紹介します。

1. サイバーセキュリティをデジタルトランスフォーメーションの実現の鍵にする — 全ての新規ビジネスプロジェクトの企画・設計段階からサイバーセキュリティを組み込む。「セキュリティ・バイ・デザイン」のアプローチを活用して、ビジネストランスフォーメーションや、製品やサービス設計におけるセキュリティリスクを、後付けではなく企画構想段階からコントロールする。

2. 組織内のあらゆる部門と信頼関係を構築する — サイバーセキュリティチームと共に主要なビジネスプロセスを分析し、サイバーリスクがもたらすインパクトや、事業部門の取り組みを強化するためにサイバーセキュリティチームがどのようなサポートを提供できるのか理解する。

「セキュリティ・バイ・デザイン」の考え方の浸透および推進に取り組むサイバーセキュリティチームは、ビジネストランスフォーメーションの達成において重要な役割を果たすことができるでしょう。しかし、組織文化を変革していくことは組織全体の使命であると言えます。CISOが、他部門との連携強化を図ることは当然の任務ですが、取締役会や上級経営層もサイバーセキュリティチームとより密接な協働関係を構築することにコミットすることが求められます。組織内の他の事業部門についても同様です。

このように組織全体が一丸となって取り組むことにより、サイバーセキュリティやプライバシー保護が強化され、企業はそれらを戦略の中核に据えて競争力優位を維持し、独自の強みを引き出す絶好のチャンスを掴むことができるでしょう。CISOは、ディスラプション（創造的破壊）が進む市場で企業が直面しているビジネスの状況を認識する必要があるとともに、取締役会およびその下にある事業部門のリーダーは積極的にサイバーセキュリティについて話し合い、関わっていくことが不可欠です。

3. 成果を生み出すガバナンス体制を整える — 経営層および取締役会に対してリスクにフォーカスした報告をする際に引き合いに出すKPI（主要業績評価指標）およびKRI（重要リスク指標）を設定する。

4. 取締役会の関与・理解を高める — 取締役会が明確に状況を理解できるように説明する。サイバーリスクについて、より効果的に説明できるよう、サイバーリスク定量化プログラム研修を実施する。

5. CISOが新たに必要なコンピテンシーを分析するために、サイバーセキュリティ機能の有効性を評価する — CISOが戦略を練り直すべきエリアを特定するために、サイバーセキュリティ部門の強みと改善すべき点を洗い出す。

今年のGISSは、サイバーセキュリティ部門の役割の進化に焦点を当て、以下の3つの点を考察する形で構成されています。

1

コミュニケーションの構造的な問題

本調査結果により、重大な侵害を引き起こす攻撃者のうち2番目に多いのがサイバーアクティビストだということが明らかになっています。サイバーアクティビストによる攻撃が増加していることを受け、サイバーセキュリティ部門は、自社のビジネス状況をより深く理解することが強く求められています。CISOが十分に組織横断的に各部門と連携していないと、組織を新しい脅威に晒すおそれのある製品やサービスを立ち上げる事業部門やビジネスラインに気付くことができません。

まもなく発行される「EY Global Board Risk Survey」の早期集計結果によると、回答組織は、「テクノロジーディスラプション」を絶好の戦略的チャンスとして捉えています。多くの組織がテクノロジートランスフォーメーションによってこの戦略的チャンスを掴もうとしていますが、そのためにはCISOや取締役会、経営層、事業部門がこれまで以上に密接に連携を図ることが必要です。そうすることで、新規のビジネスプロジェクトの企画・設計段階からサイバーセキュリティを組み込むことができます。これがまさに「セキュリティ・バイ・デザイン」のアプローチです。

わずか

36%

新規のビジネスプロジェクトの企画段階からサイバーセキュリティチームが関与していると回答した組織の割合

- サイバー攻撃とプライバシー侵害の脅威は増加・拡大し続けています。10社中6社（59%）が過去12カ月以内に重大な侵害を経験しています。「EY Global Board Risk Survey」の調査結果によると、48%の取締役会メンバーが、今後12カ月間にサイバー攻撃やデータ侵害による一定以上の影響を受けるだろうと予測しています。このような攻撃の5件に1件（21%）は、ハクティビスト（テクノロジーを活用して政治的・社会的な主張をするためにサイバー攻撃を行うアクティビスト）によるもので、組織的なサイバー犯罪組織（23%）に続いて2番目に多い攻撃者タイプです。
- 新規のビジネスプロジェクトの企画段階からサイバーセキュリティ部門が関与していると回答した組織はわずか36%でした。
- サイバーセキュリティ予算は、イノベーションやビジネストランスフォーメーションではなく、大半が組織を守るための経費として使われています。新規のビジネスプロジェクトのサイバーセキュリティ予算の支出先は、77%の組織において、ビジネスチャンスに付随するものではなく、リスクやコンプライアンス面にフォーカスするものでした。
- 回答組織の5社中1社は、新規のビジネスプロジェクトにサイバーセキュリティ予算の5%以下しか費やしていません。

2

関係再構築による信頼の醸成

59%

サイバーセキュリティ部門とビジネスラインの関係について、「中立的」、「信頼していない」、あるいは「関わり合いがない」と回答した組織の割合

つまり、「セキュリティ・バイ・デザイン」の実践を目指して、CISOがマーケティング、R&D、販売などの他部門と組織横断的に連携を強化して、組織全体のサイバーセキュリティに対する理解を深め、「セキュリティ・バイ・デザイン」を実現させる環境を整えることが必要です。

事業部門との連携強化に注力することは非常に大切ですが、同時に、サイバーセキュリティ部門は、取締役会や経営層、管理職と生産的な関係を構築していくことも欠かせません。

わずか

20%

サイバーセキュリティリスクやその軽減に向けた現行の対策について、「大規模なサイバー攻撃から組織を守ることができる水準である」と非常に自信を持っている取締役の割合（「EY Global Board Risk Survey」の調査結果より）

3

変革の推進者としてのCISO

- 74%の組織が、サイバーセキュリティ部門とマーケティング部門の関係について、「中立的」、「信頼していない」、あるいは「関わり合いがない」と回答しました。R&D部門および各ビジネスラインとの関係性についても同様であると回答した組織はそれぞれ64%と59%でした。さらに、予算執行権限において深く関わり合いがある財務部門とも関係が薄く、十分な信頼関係が築けていないと57%の回答組織が感じています。
- 回答組織の半数近く（48%）が、サイバーセキュリティリスクに対する取締役会の理解不足を指摘しています。また、43%の組織が、取締役会はサイバーセキュリティチームの任務の重要性や必要性を十分に認識していないと回答しました。
- 「EY Global Board Risk Survey」の調査で、取締役は自社のサイバーセキュリティ対策に自信を持っていないことが明らかになりました。「自信がない」または「少し自信がある」と回答した取締役は50%にのぼりました。
- 取締役会の議題としてサイバーセキュリティを定期的に取り挙げている組織は54%にとどまりました。
- 10社中6社の組織が、サイバーセキュリティ関連の支出やその投資効果を定量化して取締役会に示すことができないと回答しました。

わずか

7%

サイバーセキュリティを「イノベーション実現の鍵」だと捉えている組織の割合。「コンプライアンス主導」や「リスク回避」と捉えている組織が依然多数を占めている

CISOは、事業部門や取締役層との連携を強化して、組織が抱えるビジネス上の喫緊の課題に対する理解を深め、まだ気づいてすらいないサイバー脅威を予測することができれば、組織のビジネストランスフォーメーションにおいて重要な役割を担うことができるでしょう。

そのためには、新しい考え方や、コミュニケーション力、交渉力、連携力など、新たな能力が必要です。新しい取り組みに対して頭から否定・反論するのではなく、一旦納得・賛成してから自身の考えを述べる「そうですね、ただ…」といった形でコミュニケーションをとることができるCISOは、変革の推進者になることができるでしょう。

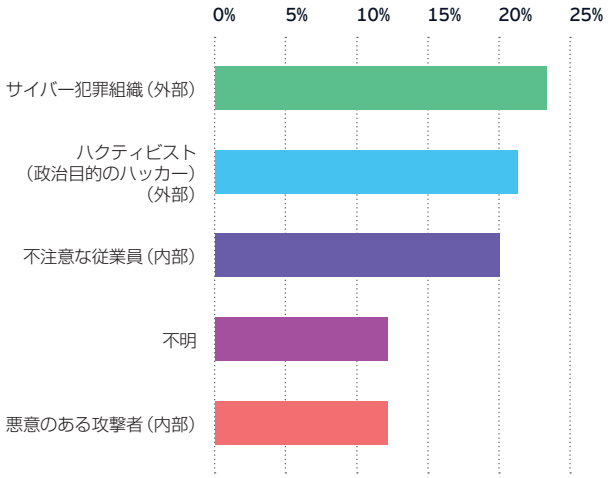
- サイバーセキュリティをイノベーション実現の鍵だと捉える組織は7%にとどまり、大部分の組織が「コンプライアンス主導」や「リスク回避」だと認識しています。
- 回答組織の半数近く（48%）が新規予算の支出先は「リスク軽減」だと答え、「コンプライアンス要件」と回答したのは29%でした。一方、「新規ビジネスの実現」と回答した組織は9%にとどまりました。
- 回答組織の10社中6社が、サイバーセキュリティの責任者は取締役会メンバーあるいは執行役員ではないと答えました。

60%

サイバーセキュリティの責任者は取締役会メンバーあるいは執行役員ではないと回答した組織の割合

1 コミュニケーションの構造的な問題

図表1：サイバー攻撃の実行者はハクティビストをはじめ複数存在
確認されたインシデントの攻撃実行者タイプ内訳



2019年4月にロンドン警視庁がインターネット活動家ジュリアン・アサンジ氏を逮捕した際、彼の支持者が過激な抗議活動を行いました。逮捕の数時間後、Police.UKのサイトにアクセスできない状態になり、関連する25の法執行機関のサイトが乗っ取られました[1]。このようなインシデントは決して特別なものではなく、ハクティビストは、敵対する企業や政府などへサイバー攻撃を世界中で仕掛けています。

本年度のGISSの調査結果は、このハクティビストによるサイバー攻撃が高まっていることを示しています。単に、破壊的な攻撃件数が大幅に増加しているだけではありません（とはいえ、59%の回答組織が過去12カ月間に攻撃頻度が増えたと答え、うち34%は攻撃頻度が10%以上増加したと回答するなど、状況はかなり深刻です）。攻撃実行者の種類にも変化が見られます。サイバー犯罪組織の次に多いサイバー攻撃実行者は、ハクティビストであることが本調査で明らかになりました。

ハクティビストがもたらす脅威は、CISOが直面するセキュリティ課題の一つを明示しています。長年にわたりサイバーセキュリティ対策の対象となってきた主な脅威は、データや知的財産の盗難、不正利用をはじめとする従来の犯罪者や、ランサムウェアやビジネスメール詐欺などを典型例とする攻撃者のテクノロジーへの対抗措置に重点が置かれてきました。しかし、現在のサイバーセキュリティは、多様化した攻撃動機により、脅威を与える攻撃者から組織を守る対策が求められています。例えば、炭鉱への投資や炭鉱での人権に関する記録、あるいはそれにかかわる執行役員のスキャンダル情報をハクティビストが入手できる環境にあるということにCISOが気づいていないとしたらどうなるでしょうか。CISOがサイバーセキュリティの役割を超えて組織の各部門と連携を図らなければ、これらの攻撃の動機となる情報を把握できないまま、組織はハクティビストの脅威に晒されることになります。

EY Globalアドバイザリー・サイバーセキュリティ・リーダーであるKris Lovejoyは、次のように述べています。

「サイバー攻撃の手口を予測し先回りをするサイバーセキュリティを組織内に構築することは必ずしも現実的であるとは言えません。これまでは金銭目的によるデータや知的財産などの盗難、不正アクセスに対する措置に焦点を当てたセキュリティ対策が主流でした。しかし、今は、主張を目的としたハッキング活動を行う攻撃者から身を守るために、サイバーセキュリティに対する考え方を大きく変える必要があります。それには、組織内の連携をこれまで以上に強化することが不可欠です」

EY Asia-Pacificサイバーセキュリティ・リーダーであるRichard Watsonは、次のように述べています。

「サイバーセキュリティチームは最悪の事態に直面しています。怨恨による攻撃や組織化された攻撃などによる破壊的な脅威が増加する中、事業

> 主張を目的としたハッキング活動を行う攻撃者から身を守るために、サイバーセキュリティに対する考え方を大きく変える必要があります。それには、組織内の連携をこれまで以上に強化することが不可欠です

Kris Lovejoy
EY Globalアドバイザリー・サイバーセキュリティ・リーダー

[1]「Hacktivits attack UK police sites to protest arrest of Julian Assange」（DataBreaches.net、2019年4月）[www.databreaches.net/hacktivists-attack-uk-police-sites-to-protest-arrest-of-julian-assange/]

わずか

36%

新規のビジネスプロジェクトの企画段階からサイバーセキュリティチームが関与していると回答した組織の割合

部門との連携が不十分であるばかりか、組織内であまり信頼されていないCISOが、組織に必要なセキュリティを提供できる可能性は極めて低いでしょう。だからこそ、セキュリティ部門とCISOは、消極的な技術者から脱却して積極的なビジネスパートナーにならなければなりません」

サイバーセキュリティは、依然として「後付け」が主流

多くの組織では、依然として、セキュリティ部門とCISOの「消極的な技術者から積極的なビジネスパートナーへ」の脱却が実現していないということが本年度のGISSで明らかになりました。サイバーセキュリティチームが新規のビジネスプロジェクトの立ち上げフェーズから関与している、つまり、新規プロジェクトに対して設計またはそれ以降の段階ではなく、企画段階から関与していると答えたのが、回答企業の36%にすぎなかったのは、注目すべき重要な調査結果の一つです。

この結果は、多くのサイバーセキュリティチームが、所属組織の一員であるけれども、その組織のビジネス要員ではないということを示しています。つまり、新規プロジェクトの企画段階からサイバーセキュリティを重要な要素として位置づける「セキュリティ・バイ・デザイン」ではなく、サイバーセキュリティチームは絶えず後付けでセキュリティ対策を講じているというのが現状であり、その結果、多くの場合、不十分なセキュリティと高額な費用が発生し、非現実的な回避策が講じられることになります。

デジタルトランスフォーメーションの時代では、どの組織も絶えず自社の製品、サービス、オペレーションプロセス、組織構造の改革などに取り組んでおり、このような後付けの対応では十分なサイバーセキュリティを確保することはできません。

EY Globalアドバイザリー・サイバーセキュリティ・リーダーであるKris Lovejoyは、次のように述べています。

「テクノロジーが急速に進化する環境にある中、組織は常に新しいテクノロジーを取り入れたビジネスプロジェクトを展開して競争力の維持を図っています。後付けによるセキュリティ対策が続けば、サイバーの脅威に常に翻弄されることとなるでしょう」

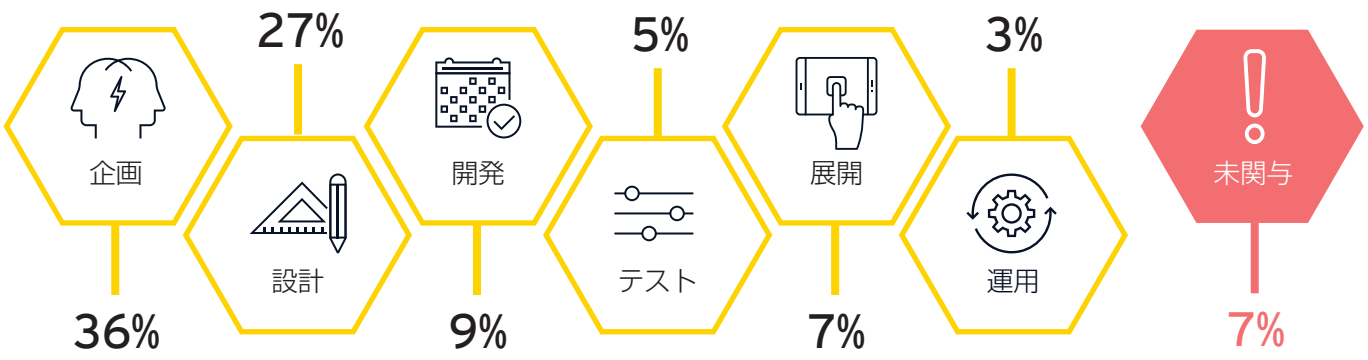
アクティビストがサイバー攻撃という手法を使い、企業はビジネストランスフォーメーションを加速させているという状況を踏まえると、サイバーセキュリティチームはこれまでのような防衛型、受け身型の対応から脱却することが必要です。サイバーセキュリティチームが組織の要員としてビジネスプロジェクトに関わることではじめて、デジタルトランスフォーメーション・プログラムの立ち上げフェーズからセキュリティを組み込み、組織にサイバー攻撃を仕掛ける全てのタイプの攻撃者による脅威を適切に想定した対策を講じることができます。

EY Americasサイバーセキュリティ・リーダーであるDave Burgは、次のように述べています。

「革新的成果を挙げている企業ほど、『連携、スピード、一貫性』を軸としたプログラムの展開に専心している傾向が見られる一方、成果の創出に苦心している企業では『連携、単純化、フォーカス』が欠如している傾向にあります」

図表2：

新規のビジネスプロジェクトでサイバーセキュリティチームが加わるのはどの段階か

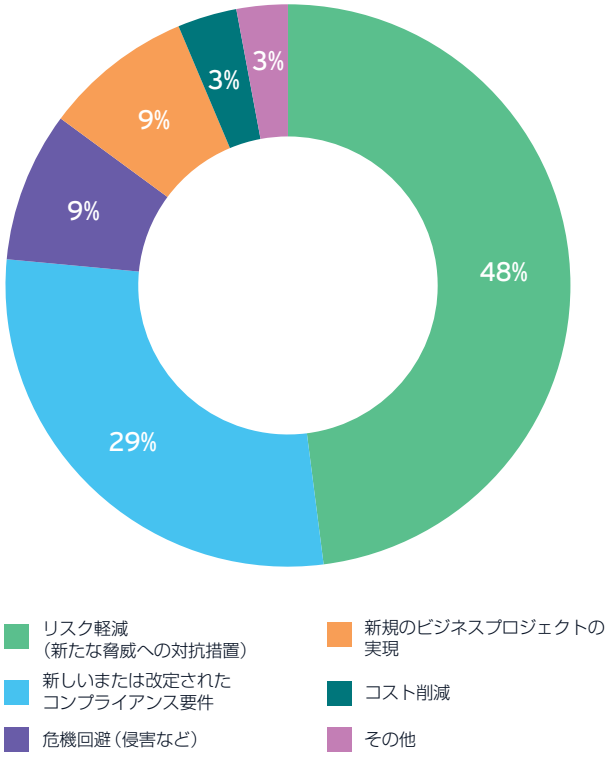


86%

危機回避とコンプライアンスが依然として新規あるいは追加のセキュリティ支出のトップを占めていると回答した組織の割合

図表3:追加予算は新規のビジネスプロジェクトのためではない

サイバーセキュリティの新規／追加予算の目的



サイバーセキュリティ予算の支出先は従来のまま～新規プロジェクトではない

サイバーセキュリティ予算の支出割合が大きい分野に関する回答結果を見れば、「セキュリティ・バイ・デザイン」の考え方を浸透させるためには乗り越えるべき課題がたくさんあることは明白です。過半数（60%）の組織が、「リスク」に対する懸念が高まっているために、この分野により力をいれ、サイバーセキュリティ予算を増やしていると回答しているのです。

新規予算を増加しているビジネスまたはテクノロジー関連の取り組み内容について尋ねたところ、「規制」と「リスク」への対応が最上位を占めました。デジタルトランスフォーメーションのセキュリティ強化について、14%の回答組織が重要視しているものの、先進的テクノロジーのセキュリティをフォーカスエリアとしている回答組織はごく少数でした。IoTデバイスに起因するサイバー脅威への懸念についてメディアなどで広く報道されているのにもかかわらず、IoT関連の取り組みにサイバーセキュリティ予算を新たに増やしていると回答した組織はわずか6%でした。また、人工知能（AI）が組織の意思決定やオペレーション、顧客とのコミュニケーションに影響を及ぼす可能性がますます高まる中、AI分野でセキュリティを強化していると回答した組織はわずか5%でした。

図表3が示すように、サイバーセキュリティ予算の主な支出先は新規のビジネスプロジェクトではなく、通常業務です。回答組織の17%が、新規のビジネスプロジェクトに予算の5%以下しか割り当てておらず、44%の組織において、予算の15%未満の割り当てでした。

CISOにとって、まだ発生していない脅威に備えて対策を講じることは必ずしも必要ではないということかもしれません。過半数（51%）の回答組織がサイバーセキュリティ予算の半分以上をオペレーションに充てており、3分の1以上（43%）の組織は重要プロジェクトや長期的投資に予算の4分の1未満しか使っていません。一方、プライベートエクイティ（PE）などの主要セクターの組織は、オペレーションの効率化や市場動向の把握、企業成長などの目的でテクノロジーの導入を注力的に行うことを検討しています。「EY Global Private Equity Survey」の調査結果によると、PEセクターのCFOの75%が、自社のスタッフに対してテクノロジー導入を検討するための時間をもっと割き、利用を高めていくよう強く要請しています。

59%

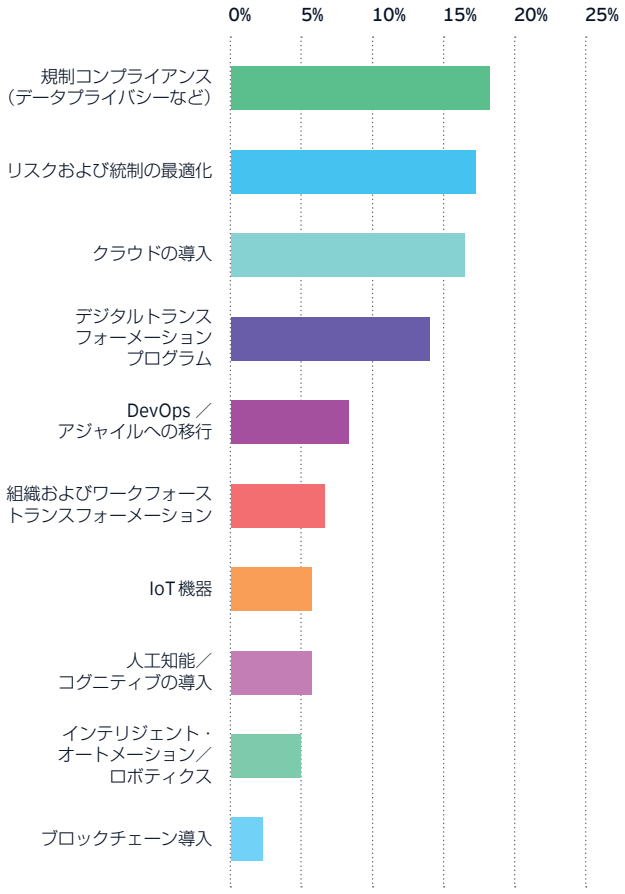
過去12カ月間に重大な侵害を経験したことがあると回答した組織の割合

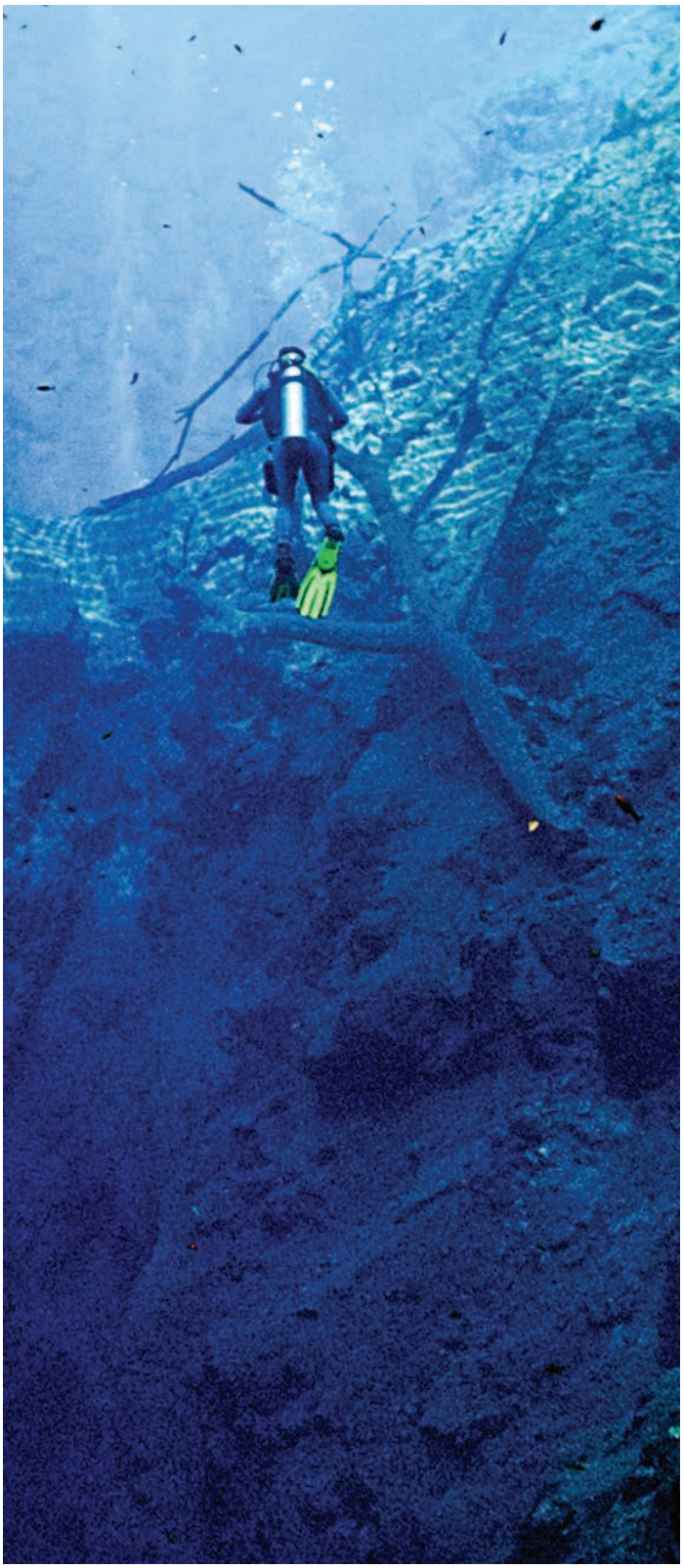
EY GDSサイバーセキュリティ・リーダーのVinod Jayaprakashは、次のように述べています。

「あらゆる新しい製品やサービスはどれも何かしらテクノロジーにより実現されている部分があるため、これらのテクノロジーはIT部門の管理の枠におさまらなくなっています。事業部門との連携が十分でない場合、組織の至るところでセキュリティを考慮することなくさまざまなテクノロジーが導入されてしまうでしょう」

図表4: サイバーセキュリティの新規／追加予算はどのように使われているか

サイバーセキュリティ機能の新規予算支出先

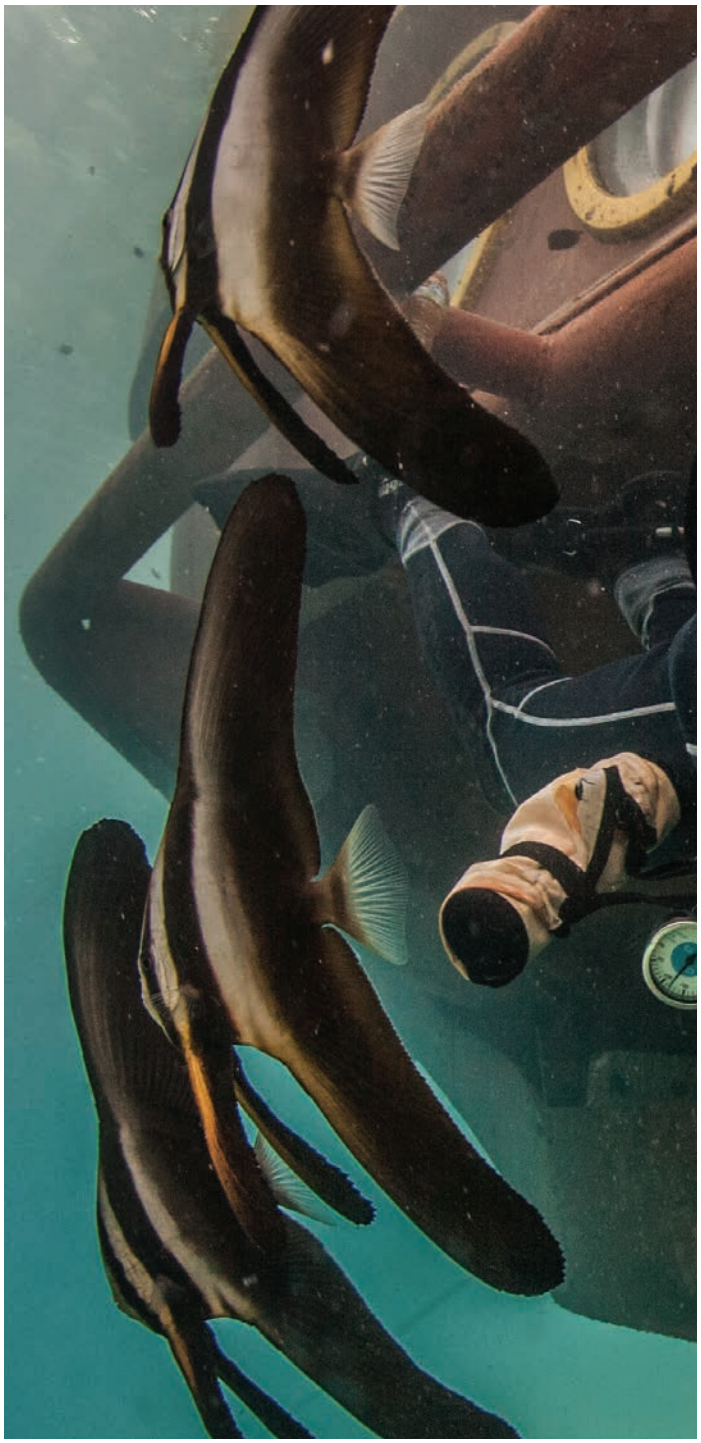




わずか

14%

デジタルトランスフォーメーション・プログラムに費やされた新規あるいは追加のサイバーセキュリティ予算の割合



CISOはプロアクティブな役割に備える必要がある

大きく役割を変えるというのは容易ではありません。そもそも、サイバーセキュリティ部門は、責任をもって対応しなくてはならない大量の業務を担い続けています。多様化するサイバー攻撃者への対抗措置をはじめ、イノベーションやビジネストランスフォーメーションなどのサポートなど、新たな役割を果たしていくことが求められると同時に、従来から対応してきた業務、例えば、組織のデータ侵害、特に、風評リスクや規制リスクをもたらす顧客データの侵害の対応措置などが今後も続いていきます。

多くの組織が、侵害の検知や防止対策に、依然として手を焼いています。過去12カ月間に経験した最も重大な侵害の検知に要した期間として、回答組織の72%が1カ月以内と回答している一方、28%の組織はそれ以上の期間と回答しました。攻撃の種類によってはさらに発見が難しくなり、39%の回答組織が、ファイルレスマルウェア攻撃は検知できそうにないと答えています。

それ故、CISOは、通常業務の保護を軽視してはならないということを強く意識しすぎるのでしょう。組織を守ることが依然として当然の優先事項とされるのです。

しかし、サイバーセキュリティを有効に機能させるためには、サイバーセキュリティ部門が組織のビジネス活動に適応することが必要です。組織がさまざまな変革に取り組み、外部ではサイバーの脅威が進化し続ける環境においては、CISOは、よりプロアクティブな役割を担う備えが必要です。

組織を守ることと組織を変革することは、相反することではありません。「セキュリティ・バイ・デザイン」の考え方を取り入れることで組織のレジリエンス力が高まり、その結果、侵害の検知、阻止、対応に要する時間を短縮できると実感できるでしょう。事業部門の取り組みを深く理解・把握しているサイバーセキュリティチームは、迫りくる脅威の予測能力や新たな潜在的侵略者に対する検知能力、事前対応能力が高まります。

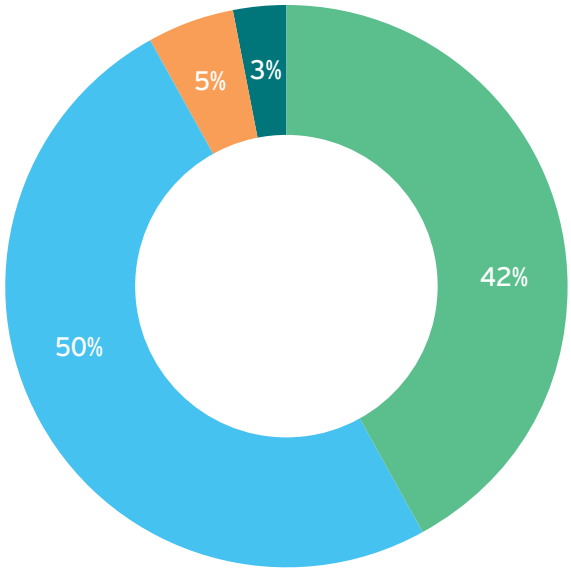
従って、CISOは、ビジネスパートナーや変革の推進者としてセキュリティ任務を遂行することにより、組織により高い価値を提供できるだけでなく、今まで取り組んできた業務をより効果的に行うことが可能になります。

92%

サイバーセキュリティの方向性や戦略策定に関与する取締役の割合。一方、サイバー攻撃の軽減に向けた自社の対策水準に非常に自信をもっていると回答した取締役はわずか20%

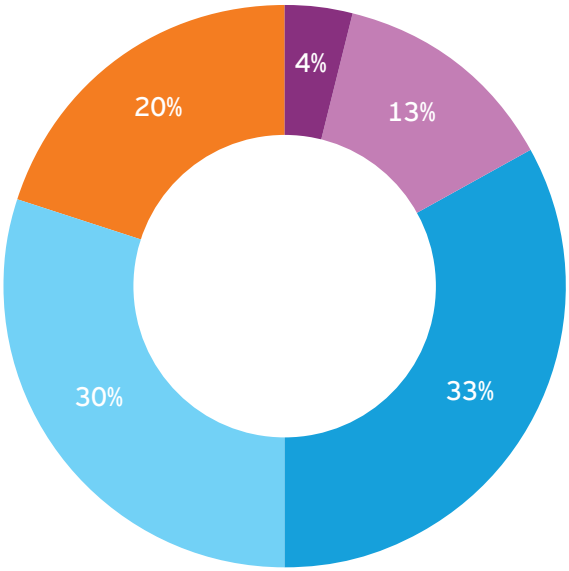
図表5: 取締役は、サイバーセキュリティ戦略の策定、方向性および予算の承認者としてサイバーセキュリティに深く関与している

サイバーセキュリティプログラムの戦略、方向性および予算の策定や承認における取締役会の関与レベルをCISOはどう見ているか



図表6：取締役は、サイバー攻撃の軽減に向けた自社のサイバーセキュリティ対策水準に自信をもっていない

大規模なサイバー攻撃に対する自社の防衛能力に取締役会はどれくらい自信をもっているか

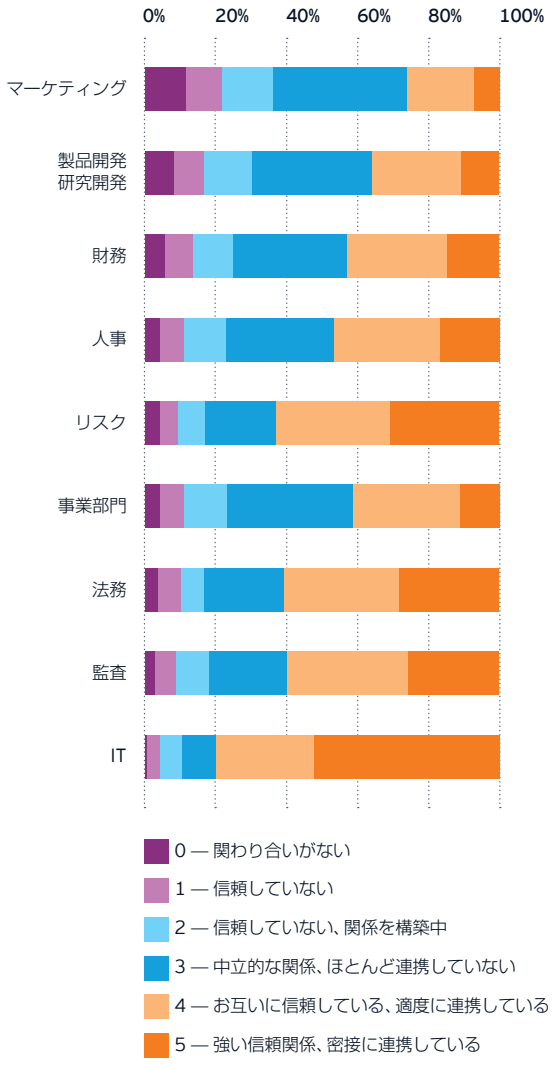


出典：Early findings from the forthcoming EY Global Board Risk Survey 2019.

2 関係再構築による信頼の醸成

図表7:信頼の欠如

サイバーセキュリティ部門の事業部門に対する関係



59%

サイバーセキュリティ部門と事業部門の関係について、「中立的」、「信頼していない」あるいは「関わり合いがない」と回答した組織の割合

ここまで見てきたように、多くの組織が自社のサイバーセキュリティ部門について、「防衛型の対応にとどまり、ビジネストランスフォーメーションをリードする役割を担う体制が整っていない」と感じています。何が、CISOの新しい挑戦を阻む障壁になっているのでしょうか。

その答えは、サイバーセキュリティチームと組織内の他のチームとの関係性にあります。つまり、サイバーセキュリティ部門が他部門、経営層、取締役との関係を再構築して信頼を醸成し、組織にサイバーセキュリティの価値を十分に提供することが、今、非常に求められているのです。

なぜ、連携することが極めて重要であるのか？

CISOに今、強く求められているのは、組織内のあらゆる部門とこれまで以上に密接に連携を図ることができるように、関係を強化することです。図表7が示すように、多くの組織では、サイバーセキュリティチームが、社内の主要な部門、特にイノベーションに取り組む部署や製品開発、顧客向けの活動をする部署との関係をほとんど、あるいは全く構築できていないのが現状です。

回答組織のほぼ4分の3（74%）が、サイバーセキュリティ部門とマーケティング部門の関係について、「中立的」あるいはそれより悪いとしていて、多くの場合、「信頼していない」、「関わり合いがない」と答えています。製品開発／R&Dチームとの関係についても同様に感じている回答組織が64%でした。一方、サイバーセキュリティ部門の従来からの役割である防衛や、コンプライアンスに深く関係するIT部門、リスク部門、法務部門との関係においては、「信頼している」、「協力的である」との回答が多数ありました（図表7参照）。多くの組織では、財務部門との関係構築も難しいようで、回答組織の4分の1以上が、「関わり合いがない」あるいは「信頼していない」と感じています。

信頼関係が十分に構築できていないCISOの場合、各事業部門の高い期待に沿う成果を出すことはほぼ無理でしょう。組織内の全ての部門との強い信頼関係の構築なくしては、サイバーセキュリティチームが新規のビジネスプロジェクトの早期段階から関与することは難しく、「セキュリティ・バイ・デザイン」の実現は程遠くなります。それだけにとどまらず、ハクティビストがもたらすサイバー攻撃などの脅威を予測するために必要なマーケット・インテリジェンスを収集することも難しくなります。

このように、より強固な関係を構築することは極めて重要です。EY Global金融サービス・サイバーセキュリティ・リーダーであるJeremy Pizzalaは、次のように述べています。

「成果を最大限に発揮するCISOは、時間をかけて事業部門との信頼関係を着実に深めています。そうすることで、自然と事業部門に溶け込み、ビジネスの戦略や企画、構想に加わることを狙いとしています。これは、CISOにとって非常に重要で新たな役割です」

> 成果を最大限に発揮するCISOは、時間をかけて事業部門との信頼関係を着実に深めています

Jeremy Pizzala
EY Global金融サービス・サイバーセキュリティ・リーダー

このようなアプローチは、社内で他部門との関係構築に時間と労力を費やす、ごく普通の例と言えるでしょう。しかし、CISOの場合、その関係性のあり方が重要になります。サイバーセキュリティ部門は「組織の安全性を確保する」という任務を遂行する部署として尊重されていますが、組織の変革プロセスの重要なパートナーとしてはみなされていないのが現状です。回答組織の29%が、サイバーセキュリティ部門は組織を守るアイデアを提供してくれる部署というイメージを持っていると答えており、サイバーセキュリティ部門があるため自信をもってイノベーションに取り組むことができると回答した組織はわずか7%でした。

そこで、サイバーセキュリティ部門に対する他部門の考え方を変えることが重要なポイントとなります。「サイバーセキュリティ部門はセキュリティを理由に新規のビジネスプロジェクトにストップをかける部署である」と見られ、イノベーションやビジネストランスフォーメーションの足枷になると思われている場合、他部門は、おのずとサイバーセキュリティ部門を避けるようになります。しかし、他部門が直面する課題に実行可能なソリューションを提供することができれば、サイバーセキュリティ部門は信頼できるパートナーになれる可能性は高いでしょう。

明確な説明で、取締役会の関与と理解を高める

サイバーセキュリティチームが構築すべき関係は部門間の関係だけではありません。多くの組織が、サイバーセキュリティ部門と取締役会メンバーの関係が希薄であると指摘していますが、これは懸念すべきことです。なぜなら、取締役会との関係が構築されていない場合、サイバーセキュリティ部門が他部門との関係を強化していくことが一層難しくなるからです。取締役会がサイバーセキュリティ部門を受け入れなければ、組織内の全部門が同様な姿勢をとることになり、さらにCISOがその役割を果たすために必要な予算を確保することも難しくなります。

EY EMEIAアドバイザリー・サイバーセキュリティ・リーダーであるMike Maddisonは、次のように述べています。

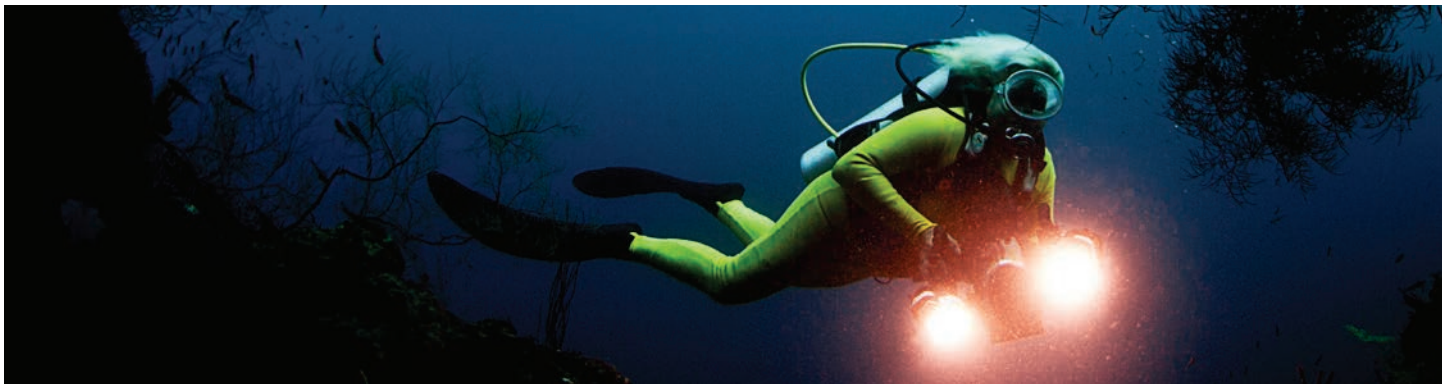
「サイバーセキュリティチームはよく、『取締役会が取り合ってくれない』ということを口にしますが、実際には、ほとんどの組織の経営層は、サイバー脅威について認識しています。彼らは、サイバーセキュリティ部門には課題を明確化する能力と実行力が欠如していると指摘しています」

> ほとんどの組織の経営層は、サイバー脅威について認識しています。彼らは、サイバーセキュリティ部門には課題を明確化する能力と実行力が欠如していると指摘しています

Mike Maddison
EY EMEIAアドバイザリー・サイバーセキュリティ・リーダー

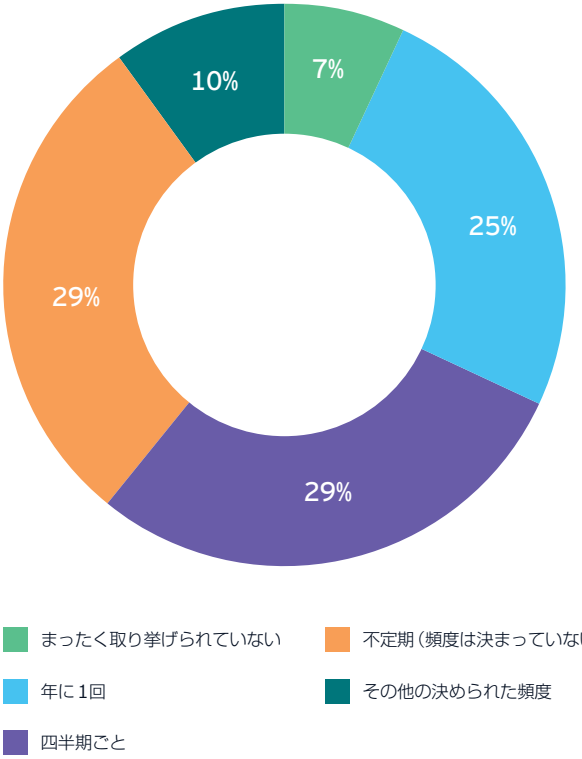
54%

取締役会の議題としてサイバーセキュリティを定期的に取り挙げていると回答した組織の割合



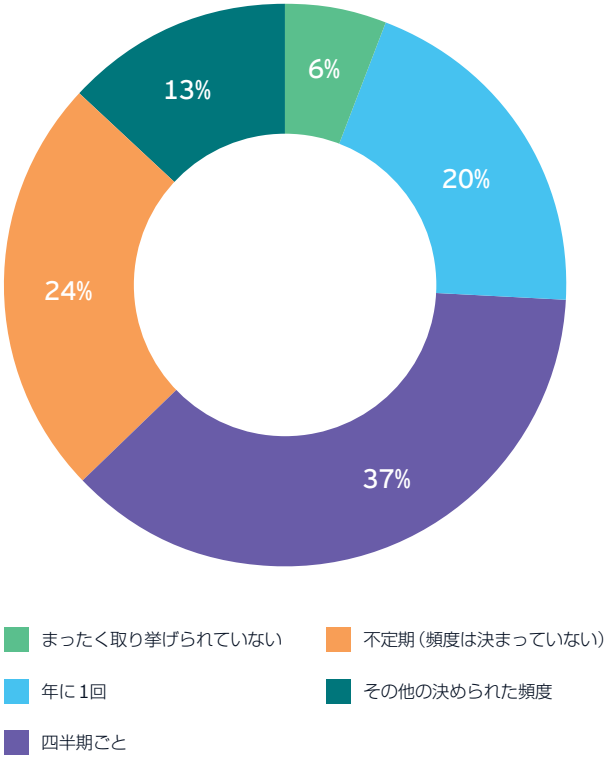
図表8: サイバーセキュリティは取締役会の定期的議題ではない

サイバーセキュリティは、どれくらいの頻度で取締役の全体会議の議題に取り挙げられているか



図表9: サイバーセキュリティに関する説明が小委員会で日常的に行われていない

サイバーセキュリティは、どれくらいの頻度で取締役会の小委員会（監査委員会など）の議題に取り挙げられているか



取締役会メンバーがサイバーセキュリティへ取り組むことの重要性を認識していない、というわけではありません。EYの調査[2]でも、CEOは、国や企業を狙うサイバー攻撃は、今後10年間で世界経済が直面する最も大きな脅威だと感じていることが明らかになっています。さらに本年度のGISSで、取締役会はサイバーリスクを「重大」な脅威と捉えていると72%の組織が回答しています。取締役会メンバー自身も、今後12カ月間でサイバーリスクが組織に非常に大きな影響を及ぼすであろうと予測しており、「EY Global Board Risk Survey」の調査の早期集計結果によると、50%の独立非業務執行取締役がそのように答えています。

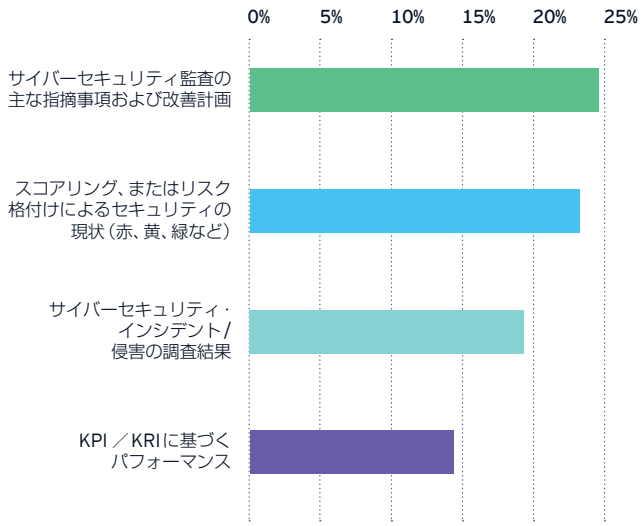
問題なのは、取締役会のサイバーセキュリティに関する課題の理解度です。本年度のGISSの調査結果によると、取締役会やエグゼクティブ・マネジメントチームが、サイバーリスクと組織を守るための現行のサイバーセキュリティ対策を十分に評価する必要性を理解していると回答した組織はわずか48%でした。同様に、42%の回答組織が、取締役会メンバーはサイバーセキュリティチームの価値とその必要性を十分に理解していないと不満に感じています。

組織は、どうすればこのような状況を改善できるのでしょうか。CISOがやるべき重要なことの一つは、取締役会メンバーへの説明方法について今一度深く考えてみることです。例えば、組織が直面するリスク対応に必要なサイバーセキュリティ支出の有効性を、財務的に定量化できると答えた回答組織はわずか25%でした。「EY Global Board Risk Survey」の調査結果によると、サイバーセキュリティチームが有効に機能していると高い自信を持っている取締役会メンバーはわずか20%でした。これでは、多くのCISOがサイバーセキュリティ人材の確保に苦心するのも当然です。

一方、多くのCISOが、取締役会はサイバーリスクを定期的にレビューする態勢をとっていないと懸念しています。サイバーセキュリティが取締役会の議題に定期的に組み込まれていると答えた回答組織はわずか54%でした。また、取締役会の小委員会で定期的な議題となっていると回答した組織は57%でした。これは、CISOが今まで取締役会とどのようにコミュニケーションをとってきたのかを反映しているのかもしれません。つまり、パフォーマンスやイノベーションではなく、セキュリティの現状や監査結果などを報告することに重点をおいてきたことがこのような状況を招いているのではないでしょうか（図表10参照）。

図表10: 今こそ、取締役会との対話内容を見直す時

CISOは取締役会に何を報告しているか



わずか

32%

今後想定される課題や変革の推進に関して取締役会で直接に意見交換を行っているセキュリティ責任者の割合

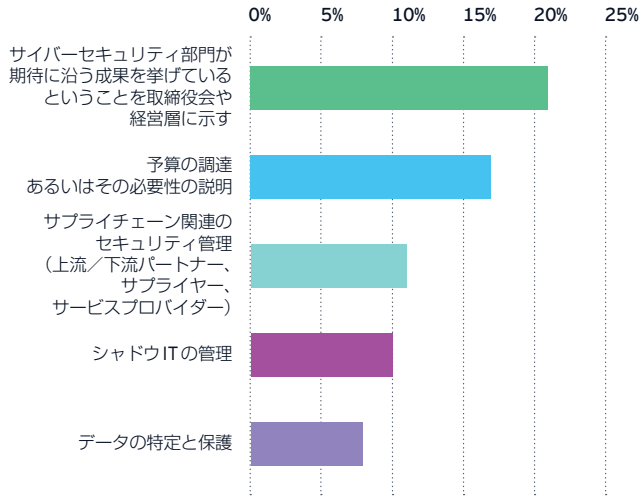
[2] 「How cybersecurity became the number one threat in the global economy for CEOs」（EY、2019年10月）[www.ey.com/en_gl/advisory/how-cybersecurity-became-the-number-one-threat-in-the-global-eco]

25%

サイバーセキュリティ支出の有効性を財務的に定量化できると回答した組織の割合

図表11:耳を傾けてもらう

サイバーセキュリティの喫緊の課題



> 投資を増やす場合、投資収益率を確保できるかどうかが非常に重要になります

Dave Burg
EY Americasサイバーセキュリティ・リーダー

サイバーセキュリティが組織にもたらす価値について取締役会メンバーやトップマネジメント層に説得力のある説明をしない限り、彼らの関与と理解を高めるのは難しいでしょう。

EY Asia-Pacificサイバーセキュリティ・リーダーであるRichard Watsonは、次のように述べています。

「リスク軽減状況を定量化するなど、脅威を定量化して取締役会のメンバーに説明できるようにしなければなりません。あまりに漠然とした説明をしてきたことが問題です」

多くのCISOが、サイバーセキュリティの取り組みがもたらす価値を理解してもらうことと、必要な予算を確保することが最も難しいと感じています（図表11参照）。多くのCISOにとって、このことは、セキュリティ管理はもとより、最新テクノロジーや新しい脅威への対応よりも難しいことなのです。

EY Globalアドバイザリー・サイバーセキュリティ・リーダーであるKris Lovejoyは次のように述べています。

「これが、サイバーセキュリティチームに対する次のような固定観念をリセットする必要があるもう一つの理由です。例えば、サイバーセキュリティチームが予算を費やすべきなのは、主としてリスクと統制の最適化だと思われています。サイバーセキュリティチームの報告先は、一般的に監査委員会です。さらに、その報告内容は、リスクと統制の最適化に関するステータスのベンチマーク結果なのです」

Kris Lovejoyは、さらに次のように述べています。

「サイバーセキュリティは、先を見越したアプローチで付加価値を提供できるにもかかわらず、今までは後付け対応型のアプローチを取ってきました。今後、サイバーセキュリティチームがビジネスプロジェクトに加わるとなると、まず重要となるのが、状況を『聞く』ことと、サイバーセキュリティを『理解してもらう』ことです。そのためにはまず、価値を示すことから始めます。そうすることで、サイバーセキュリティチームの取り組みが事業プロジェクトに有益であるということを事業部門に実感してもらうことができ、サイバーセキュリティ予算の使い道とその有効性を正当化できます。次第に、従来型のサービスを超えて、強固で前向きな関係が構築されていきます。対話も、『なぜできないのか』から『どうすればできるか』に変化し、協議内容もリスク軽減からイノベーションへと変わります」

セキュリティベンダーの役割とは？

セキュリティベンダーは、サイバーセキュリティのパフォーマンスの改善や事業部門との連携強化に向けたCISOの取り組みの一助となることができるでしょうか。現在、セキュリティベンダーが本当に価値を提供することができるのかどうか、懐疑的な見方も出ています。本調査結果では、サイバーセキュリティベンダーのマーケティングのための説明を信用していると回答した組織はわずか10%でした。一方、69%が、どのベンダーが説明するかによると回答しました。そして、4分の1近くの回答組織が、ベンダーが期待値に達していないと回答し、「成果にばらつきが見られる」（24%）、あるいは「製品やサービスがわかりづらい」（20%）と感じています。

しかし、4分の3の回答組織が最大で20ものサイバーセキュリティ製品またはツールを利用している状況（一部ではそれより多く利用している組織もありました）を踏まえると、最も信頼できるベンダーを慎重に選び、緊密に連携すれば、サイバーセキュリティ・パフォーマンスを改善できる余地はあります。CISOは、ベンダーに求める主要な品質として、業界経験と顧客サービスを重視しています。

EY EMEIAサイバーセキュリティ・リーダーであるMike Maddisonは、次のように述べています。

「CISOは、『最適化、簡素化するにはどうすればよいか?』とよく思案しています。その方法として、現在利用しているソリューションの数を減らす、または特定のソフトウェアプロバイダーと連携して管理負荷の削減を図るという選択肢があります。そして、企業が、一社のベンダーを最大限に活用できる幅広い契約を結ぶようになってきています」

図表12:
サイバーセキュリティプロバイダーとの信頼度を高める最も重要な要因は、業界経験と能力

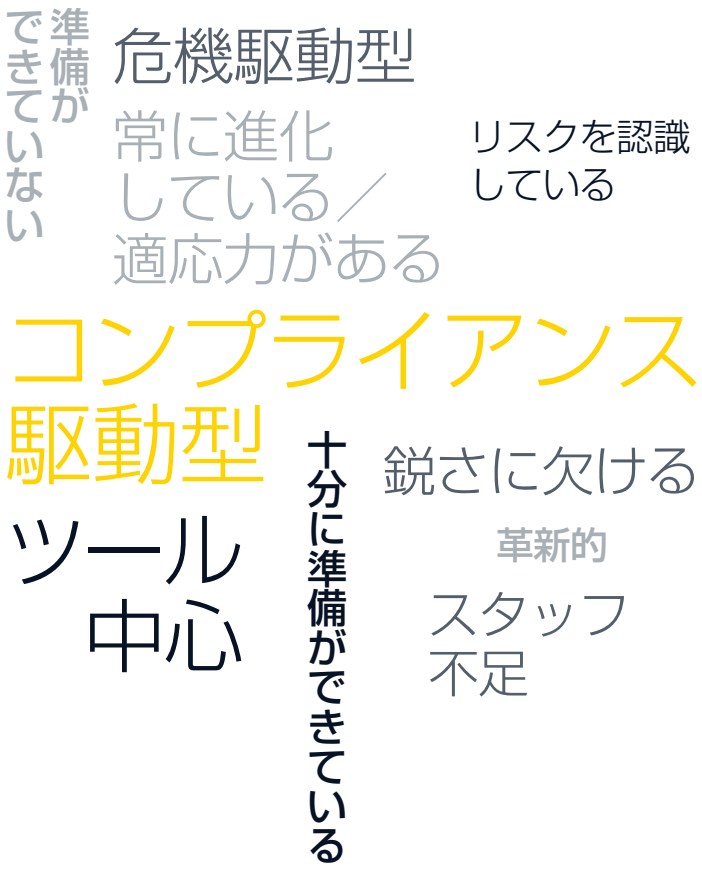
#1 業界経験と能力　素晴らしい評判

#2 優れたカスタマーエクスペリエンス　明確な契約条件

#3 製品やサービス情報の入手しやすさ　明確な価格設定

3 変革の推進者としてのCISO

図表13: 意識を変えるには、まだかなりの時間が必要
CISOは組織内でどのように思われているのか



「サイバーイネーブラーという概念は、かなり前から注目されています。この考え方は、サイバーセキュリティ機能の『最適化』と『成長』が重視されてはじめてその重要性が高まります」

Mike Maddison
EY EMEIAサイバーセキュリティ・リーダー

多くのCISOが今、重大な分岐点に立っていると感じています。これまでCISOがフォーカスしてきた任務は、防衛面の強化と、サイバー攻撃から組織を守ることです。その任務は今後も続いていきます。しかし、CISOには今、新たな一歩を踏み出すチャンスが訪れています。それは、組織が取り組むさまざまなビジネストランスフォーメーションの重要な要員である変革の推進者として新たな任務を果たしていくことです。

変革の推進者となったCISOは、サイバーセキュリティ機能をイノベーション実現の鍵へと進化させていくでしょう。そのために、各部門との連携をこれまで以上に強め、そこで築いた関係を生かし、さまざまな動機を持つ悪意のある攻撃者がもたらす新たな、または変化する破壊的脅威を予測します。

一方、このチャンスを生かすことができない場合、サイバーセキュリティ機能は次第にビジネス活動の隅に追いやられていくでしょう。

EY EMEIAアドバイザリー・サイバーセキュリティ・リーダーであるMike Maddisonは、次のように述べています。

「サイバーイネーブラーという概念は、かなり前から注目されています。この考え方は、サイバーセキュリティ機能の『最適化』と『成長』が重視されてはじめてその重要性が高まります。しかし、多くの組織では、セキュリティの責任者がなかなか新しい一歩を踏み出せずにいます」

一方、この新しいチャンスを掴むと、従来とは大きく異なるCISO像が創出され、サイバーセキュリティチームも総じて新しいアプローチに適応していくことが必要になるでしょう。この大変革には価値があります。これは、サイバーセキュリティ機能が、変革を推進し、その価値を提供しながら、組織のバリューチェーンの中心で信頼されるビジネスパートナーになるチャンスなのです。

現在のサイバーセキュリティ業界に対して、「コンプライアンス駆動型」、「危機対応への備え」、「既存のツールが中心」という見方が浸透しています（図表13参照）。この業界が「常に進化している」または「適応力がある」と回答した組織はわずか13%で、「革新的」という表現を使った組織は、それよりもさらに少ない割合でした。

新しい時代のCISO：新しいスキル、体制、ステータス

CISOにとってここで重要な問題は、彼らが新しいアプローチで取り組み、よりプロアクティブで未来志向のサイバーセキュリティ機能をリードするにふさわしいスキルと経験を備えているかどうかということです。さまざまなサイバーセキュリティ対応を通してキャリアを積み、培ってきた高いテクニカルスキルだけでは十分でありません。CISOの新しい役割には、ビジネス関連の知識や高いコミュニケーション力、連携力が求められます。

わずか

7%

侵害による影響を財務的に定量化できる能力を備えているセキュリティ責任者の割合

EY Asia-Pacific サイバーセキュリティ・リーダーである Richard Watson は、次のように述べています。

「いくつかの組織では、CISO に求められる新しい能力を念頭に、サイバーセキュリティ分野の経験に関係なく CISO を採用しています。このような組織が採用しているのは、サイバーセキュリティ以外の分野、特に、ビジネス分野で経験のある幹部職の人材です。CISO は技術者である必要はないと思います。つまるところ、リスクを管理することが CISO の任務ですから、リスク管理の意味や定義、概念を理解している人が CISO に最もふさわしいと思います」

一方で、どちらかというと従来同様の資質・経歴を持つ CISO を好み、同時に、サイバーセキュリティチーム、取締役会／経営層、組織内の他の部門間の関係を強化する組織体制を整えようと試みる組織もあるでしょう。

EY Global アドバイザリー・サイバーセキュリティ・リーダーである Kris Lovejoy は、次のように述べています。

「サイバーセキュリティチーム自体を変革するだけでなく、サイバーセキュリティチームがビジネス上のコミュニケーションをとることができるような管理体制とガバナンス構造を構築することが必要です。基本的には、サイバーセキュリティチームと、取締役会／経営層、その他の部門が相互に理解し合うための話し合いの機会とメカニズムが必要です」

Kris Lovejoy は、また、次のようにも述べています。

「端的に言えば、頭から否定・反論する CISO ではなく、一旦納得・賛成してから自身の考えを述べる「そうですね、ただ…」といった形でコミュニケーションをとることができる CISO が求められています。つまり、CISO はイノベーションの妨げになるなどと思われてはなりません。CISO は、課題解決役として『セキュリティ・バイ・デザイン』を促進し、組織のビジネスプロジェクトの安全面とセキュリティ面を担保する推進者であるべきです」

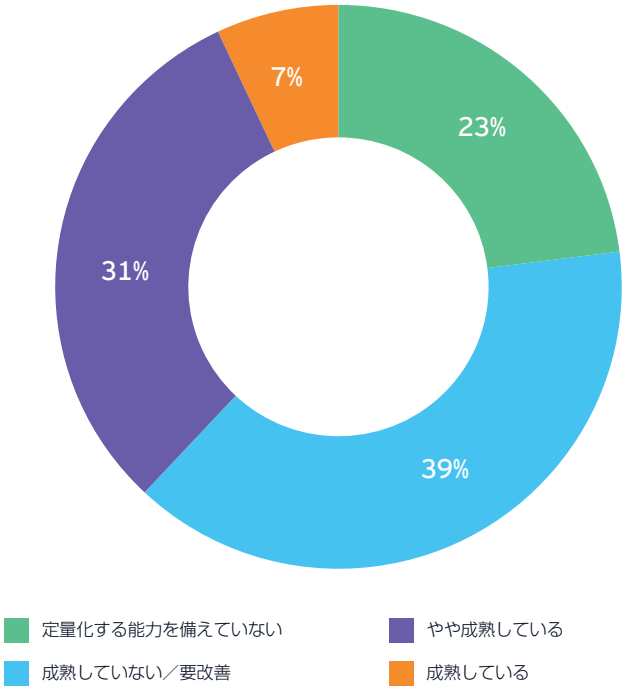
しかし、ここで、新しい CISO の役割が従来とは異なるタイプであるということを踏まえると、現行の CISO のレポートラインが CISO の新しい役割に沿うものであるか、という懸念があります。現在、CISO が取締役会メンバーまたは執行役員である組織は、36% に過ぎません。CISO の役割として経営層や事業部門との関係拡大や緊密な連携が以前にも増して重要になる場合、組織はその役割のステータスを引き上げることが必要かもしれません。

レポートラインについて回答組織に尋ねたところ、CISO は CIO の直属である場合が多いようです。このようなレポートラインは、サイバーセキュリティを事業部門から一歩遠ざけてしまい、CIO が、CISO と事業部門をつなぐパイプにならざるを得ません。

現時点で CEO の直属になっている CISO は 18% に過ぎませんが、サイバーセキュリティがビジネストランスフォーメーションの実現の鍵としての役割を担う組織では、このような方向に進むでしょう。CISO のレポートラインがリスク、財務、法務部門などである組織は少なくなってきますが、この構造はもはや機能しないでしょう。

図表 14: 侵害の財務的影響を定量化する能力が欠如

サイバーセキュリティ侵害の財務的影響を定量化するセキュリティ責任者の能力の成熟度



> CISO はイノベーションの妨げになるなどと思われてはなりません。CISO は、課題解決役として『セキュリティ・バイ・デザイン』を促進し、組織のビジネスプロジェクトの安全面とセキュリティ面を担保する変革の推進者であるべきです

Kris Lovejoy
EY Global アドバイザリー・サイバーセキュリティ・リーダー

事例紹介

AXA

Arnaud Tanguy氏

AXAグループ・チーフ・セキュリティ・オフィサー

Arnaud Tanguy氏は、2018年にフランスの保険会社AXAのグループ・チーフ・セキュリティ・オフィサーに就任しました。このTanguy氏の採用は、サイバーセキュリティ、フィジカルセキュリティ、オペレーション・レジリエンスをそれぞれ担当していたAXA社の各チームをセキュリティ部門として1つに統合する組織再編の一環で行われたものでした。これについてTanguy氏は、「この一体的なアプローチは、サイバーの脅威もグローバルで集約的になってきているからです」と述べています。

組織の再編により、企業と顧客を守るセキュリティ機能が強化されただけでなく、戦略的なセキュリティ対応も可能になりました。

Tanguy氏はまた、次のようにも述べています。

「我々は、組織のビジネス活動を常に把握し、事業部門とも緊密に連携を図っています。しかし、それだけでは十分ではありません。我々セキュリティ部門は、カスタマーエクスペリエンスの変革に取り組んでいる企業の一員として、我々の会社が安全で脅威に対する回復力があるということを、競争の激しいこのビジネス環境で対外的に伝えることができるようサポートしています。セキュリティ機能の統合によって、セキュリティを一体的な視点で捉え、我々の会社が行うすべての活動に『セキュリティ・バイ・デザイン』を取り入れることができるようになりました」

AXAのセキュリティ部門がこのように変革の推進者としての役割を果たせるのは、同社のマネジメント・コミッティ・メンバーであるグループ・チーフ・オペレーティング・オフィサーがグループ・チーフ・セキュリティ・オフィサーの直属であることにより、AXAのセキュリティ部門と経営層が良好な関係を保っているからです。

これについて、Tanguy氏は次のようにも述べています。

「つまり、セキュリティ機能がAXAの戦略的意思決定の一部になっているということです。我々セキュリティ部門は、AXAのグループ戦略の実行をサポートすることを使命とし、我々テクノロジー主導企業の顧客にフォーカスしながら、組織を守ることに専心しています」

明るい兆しはあるものの、課題はまだ残っている

サイバーセキュリティに対する組織内の意識が低い場合、その潜在的付加価値を十分に提供することは難しいでしょう。

EY Americasサイバーセキュリティ・リーダーであるDave Burgは、次のように述べています。

「セキュリティ部門の積極的な関与に力を入れている組織は、短期的にも長期的にも、ビジネス上で非常に大きなベネフィットを実感できるでしょう」

明るい兆しも幾分見えてきています。例えば、回答組織の50%が、ビジネスリスクあるいはオペレーショナルリスクの観点から、サイバーリスクとそのリスク許容度を明確に示していると答えています。また、3分の2（67%）の組織が、新しく創出する知的財産のガバナンス整備においてセキュリティ部門のサポートを期待しており、それより少し下回る（61%）組織がオペレーショナル・テクノロジーについても同様のサポートを期待すると答えています。

このような調査結果には期待も膨らみます。しかし、組織は、サイバーセキュリティ部門と事業部門の連携を模索する際に乗り越えなければならない課題に直面するでしょう。

中でもとりわけ困難を要するのは予算の配分かもしれません。多くの組織では、ビジネスラインや事業部門など、すでに複数の予算源からサイバーセキュリティ予算を獲得できる状況にあります。本調査でも、3分の1（32%）近くの回答組織が、サイバーセキュリティへの予算源が複数あると答えており、連携が拡大すれば、予算源も増加していきます。この予算管理をどの部署が主管するべきかという質問に対して、4分の3近く（68%）の回答組織が、予算の拠出と配分を一元管理する主管部署があると回答しました。しかし、これはまだ議論の余地があります。

これらは、セキュリティの新しいアプローチを阻む大きな障害というよりも、重くのしかかる構造上、運営上の課題です。事業部門とサイバーセキュリティ部門の連携強化によって受ける恩恵はこの障害に勝るものであり、これら課題の解決に向けて組織が全力で取り組むべき理由はここにあります。

> 「セキュリティ部門の積極的な関与に力を入れている組織は、短期的にも長期的にも、ビジネス上で非常に大きなベネフィットを実感できるでしょう」

Dave Burg
EY Americasサイバーセキュリティ・リーダー

#1 サイバーセキュリティ予算の支出先で最も大きい割合を占めるのは、セキュリティオペレーション・センター（SOC）

セキュリティオペレーション・センター（SOC）は、期待通りの成果を出しているか？

本年度のGISSで、多くの組織がSOCに失望感を抱いていることが明らかになりました。本調査報告によると、回答組織は、サイバーセキュリティ予算の28%、担当者の工数の27%をSOCの運営に充てていました。しかし、過去12カ月間で組織にとって最も重大な侵害をSOCが検知した、と回答した組織はわずか26%でした。

このような調査結果の背景には、多くの組織で、手作業による解析に相当の労力を要する第一世代のSOCを今もなお運用していて、新たな機能に十分な投資がされていない、という事情があるのかもしれません。SOCのアーキテクチャや機能にかけられている予算はわずか19%に過ぎません。SOCがサイバーセキュリティの足枷になっているということはないでしょうか？

EY Asia-Pacificサイバーセキュリティ・リーダーであるRichard Watsonは、次のように述べています。

「標準的な技術のみを活用したSOCは事後対応型で、異常検知を人間の目で見分ける必要があり、手作業に大きく依存しています。次世代のSOCは、フィッシングメール攻撃への自動対応などのユースケースをもち、自動化されています。その性質上、事前対応型であり、アナリティクスを活用して異常を検知します。また、クラウドを活用し、利用者の環境に適した設計がなされています」

これは、SOCを次世代に進化させることによって大きなメリットを享受できる、ということを意味します。脅威や侵害に対する検知力が高まるだけでなく、多くの作業が自動化されることにより人材を他のエリアで有効活用できるのです。SOCの運用に必要な工数を削減できた組織では、サイバーセキュリティ人材を事業活動に直接関与する任務にアサインすることもできます。

わずか
26% 過去12カ月間に発生した侵害のうち、SOCが検知した侵害件数の割合

まとめと次のステップ

本年度のEYグローバル情報セキュリティサーベイ（GISS）では、「セキュリティ・バイ・デザイン」の概念に基づいてサイバーセキュリティ機能をビジネストランスフォーメーションの中核に据えようと試みる組織の取り組みを調査し、その進捗状況を考察しました。

CISO、取締役会、経営層、各部門が連携してサイバーセキュリティ機能の新しい価値を引き出す大きなチャンスが今、到来しています。努力と挑戦を重ね、このチャンスをつかんだ先には、組織の競争力を維持するために各事業部門が取り組まなければならないビジネストランスフォーメーションを、サイバーセキュリティが変革の鍵となり、実現へと導くことができる組織の姿があるでしょう。さらに、「組織を守る」という従来の防衛面においても、サイバーセキュリティ機能の有効性の向上を実感するでしょう。例えば、ハクティビストがもたらす潜在的なリスク状況をより的確に捉えて、新たに迫りくる脅威を予測できるようになります。取締役会に対する報告やコミュニケーション方法においても新たなアプローチをとることで、取締役会メンバーとCISOの関係強化を図ることができるため、人材確保やサイバーセキュリティ機能が提供する価値をめぐる闘いは、もはや過去のことになるでしょう。

1

サイバーセキュリティをデジタルトランスフォーメーションの実現の鍵にする

「セキュリティ・バイ・デザイン」を実践して、サイバーセキュリティ機能をビジネスプロセスに組み込みます。全ての新規ビジネスプロジェクトの企画段階からサイバーセキュリティ機能を組み込むアプローチは、後付け対応で優先順位付けに要する労力とコストを削減するだけではなく、プロジェクトのスタート段階から製品やサービスの信頼性を担保することができる、最適なビジネスモデルです。サイバーセキュリティ機能とビジネス活動の一体化および相互協力がこれまで以上に必要になっています。

2

組織内のあらゆる部門と信頼関係を構築する

サイバーセキュリティ機能がビジネス活動に組み込まれると、CISOは、イノベーションを牽引する重要な変革の推進者となるとともに、組織が直面する脅威関連情報を入手しやすくなります。そこで重要になるのが、既存のデータをもとにビジネスプロセスおよびその統制をモデル化することと、CISOとの連携によりビジネスプロセスにサイバーセキュリティ機能がもたらす重要なメリットを理解することです。そのメリットの根拠が明確になれば、各事業部門は、ビジネスプロセスに必要なセキュリティに関する有用な情報をリアルタイムで得ることができます。このようにして信頼関係を構築することができれば、CISOも更なる潜在的なリスクや脅威に関する状況を把握できるだけでなく、ビジネス統制やイノベーションに必要なセキュリティ対応を見極めることが可能になります。

3

成果を生み出すガバナンス体制を整える

取締役メンバーや経営層は、イノベーションの中核をなす新たなサイバーセキュリティ機能の役割を踏まえ、レポートラインや、予算管理、説明責任について見直す必要があります。それに続いて、直ちに取り組むべきことは、経営層および取締役会への報告においてリスクの観点から説明する際に引き合いに出すKPI（主要業績評価指標）とKRI（重要リスク指標）を設定することです。

この移行期を乗り切ることは単純なことではありません。しかも、誰もが同じようにやればよいというものでもありません。組織が今後取り組むべきこと、そして、CISO、取締役メンバー、経営層、各部門がそれぞれにフォーカスするべき次のステップは、各組織のサイバーセキュリティ機能の現状や組織文化、組織の目指す姿によって異なります。しかし、全ての組織がこの変革のチャンスを最大限に生かすために優先的に取り組むべきアクションが5つあります。

4

取締役会の関与・理解を高める

サイバーセキュリティ機能の重要性に関して、取締役会の賛同を得られるような定量化の方法とレポートラインを確立することが不可欠です。ビジネスの観点からサイバーリスクをより効果的に説明し、取締役会とのコミュニケーションに弾みをつけるために、サイバーリスクの定量化に関する計画を策定、実行することが重要なステップになります。

5

CISOが新たに必要なコンピテンシーを分析するために、サイバーセキュリティ機能の有効性を評価する

サイバーセキュリティの責任者に求められる資質は、ビジネスセンス、事業部門が理解できるように説明する能力、そして一方的に否定・反論せずセキュリティに関する問題解決に向けてソリューションを積極的に見つけようとする姿勢です。まず、サイバーセキュリティ機能の強みと改善すべき点を理解し、それに基づいて、CISOが戦略を練り直すべきエリアを特定することから始めます。次に、マネージドサービスの利用範囲、価格の妥当性、成果の有効性を確認し、マネージドサービスが適切に利用されているかどうか判断します。そして、マネージドサービスに関連する手作業でのプロセスの削減と、それにより解放されたサイバーセキュリティ人材を事業部門のサポートに回して付加価値のある人材配置を実現するために、自動化やオーケストレーションの状況を評価します。

サイバーセキュリティの責任者に求められる資質は、ビジネスセンス、事業部門が理解できるように説明する能力、そして頭から否定・反論せずセキュリティに関する問題解決に向けてソリューションを積極的に見つけようとする姿勢です。

松下 直
EY Japan
サイバーセキュリティ
リーダー

新型コロナウイルス感染症（COVID-19）の拡大により、日本の社会は大きな変化を余儀なくされています。

数年前から叫ばれだした働き方改革により、日本の組織のシステムアーキテクチャは変革の時期に差し掛かろうとしていました。クラウドファーストの考え方が浸透し、ゼロトラストアーキテクチャへの転換が緩やかに進んでいるまさにそのとき、新型コロナウイルス感染症への対応で、多くの組織が十分な準備もできないまま、急激に在宅勤務へとシフトすることとなったのです。これは新型コロナウイルス感染症が終息したアフターコロナでも揺り戻すことなく、基幹システムなどのクラウドへの移行をはじめとして、ゼロトラストアーキテクチャへの全体的な転換がさらに加速していくこととなるでしょう。

EY Japan サイバーセキュリティ・リーダーである松下直は、本調査の結果とアフターコロナの日本の姿を重ね合わせ、次のように述べています。

「緩やかに進んでいたゼロトラストアーキテクチャへの転換は、新型コロナウイルス感染症により急激に進むこととなるでしょう。一般的にアーキテクチャの転換期はセキュリティを最初から組み込むチャンスですが、今回のように転換が急激な場合には、むしろ最初から組み込むことが安全に進めるために必要不可欠になります。本調査報告で述べている5つのアクションに積極的に取り組み、セキュリティ・バイ・デザインを実践していかねばなりません」

急激なアーキテクチャの転換においてセキュリティを組み込むには、高度なセキュリティ人材の確保が重要となります。しかし、既存のセキュリティ対策がゼロトラストアーキテクチャへの緩やかな転換に十分に対応できていないがために、これらの人材はその状況の補完に忙殺されているようです。例えば、本調査において、日本の企業で過去一年間に発生した最も重大なセキュリティ侵害のうち、SOCが検知した割合は14%と低い水準にとどまっている一方、そのようなセキュリティ侵害の調査を完了するまでに1カ月以上を要した割合は38%となっています。組織内のセキュリティ人材は、巧妙化する攻撃を検知しようと努力をし、さらにそれをすり抜けて発生したインシデントを終息させるために奔走しているのです。

松下直は、さらに次のように述べています。

「クラウドとオンプレミスが複雑に絡み合う今日のシステムでは、インシデントの発生検知や対応にも相当の労力を要し、高度な技能を有するセキュリティ担当者が疲弊することとなります。高度な自動化やオーケストレーションを提供するSOCに切り替え、これらの人材を本来のセキュリティ業務に転換することが、セキュリティ・バイ・デザインを成功させる鍵となるでしょう」

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。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYについて詳しくは、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。EY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・アンド・コンサルティング株式会社などから構成されています。なお、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。

EY アドバイザリー・アンド・コンサルティング株式会社について

EYアドバイザリー・アンド・コンサルティング株式会社は、EYの日本におけるメンバーファームです。さまざまな分野の専門性を有するプロフェッショナルがグローバルに連携し、企業が抱える経営課題に対し、最先端かつグローバルな視点と実行力で、最適なアドバイザリーサービスを総合的に提供いたします。詳しくは、eyjapan.jp/advisory をご覧ください。

©2020 EY Advisory & Consulting Co., Ltd.
All Rights Reserved.
本書はEYG no. 000676-20Gblの翻訳版です
ED None

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスを行うものではありません。EYアドバイザリー・アンド・コンサルティング株式会社および他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。

eyjapan.jp/giss

本調査レポートについて

第22回EYグローバル情報セキュリティサーベイ（GISS）は、2019年8月から9月にかけてEYが実施し、1,300近い企業のトップマネジメントの皆さまから回答を得ました。

本調査は世界規模で実施され、回答組織の地域別内訳は、EMEIA（欧州、中東、インド、アフリカ）が47%、Americas（北・中・南米）が29%、Asia-Pacific（アジア・パシフィック）が24%です。回答者の職務・職位は、さまざまなセクターのCISOあるいは同等の職務・職位です。