技術産業が成熟期に入ると、世界規模で動く新たなトレンドが意味するもの、その影響はますます不明瞭になります。社会的影響もさることながら、デジタルデータへの過剰な依存や、個人情報収集の拡大という事実によって、サイバーセキュリティやプライバシーの重要性がさらに際立っています。この報告書では、今日のビジネスにおいて、セキュリティがどのような状況にあるかを検証し、企業が理想的なセキュリティを構築するハードルとなっているものを探り、デジタル経済におけるよりよいセキュリティへのアプローチおよび取るべきステップについて提言します。

キーポイント

サイバーセキュリティはしっかりした実践へと進化しています
自社のセキュリティに完全に満足していると報告する企業数は増加していますが（2017 年の 21%から、2019 年の 45%）、大部分の企業で、まだ改善の余地が見られます。技術の劇的変化に伴い、新技術のチェックリストを確認するだけではすまない、新たなセキュリティへのアプローチが必要となっています。ビジネスにおいて、サイバーセキュリティに特化した業務が行われるようになってきています。実践へとシフトしているのです。この機能が社内スタッフによって果たされるのか、外部パートナーなのか、両方なのか、という点についてはさまざまです。

トレードオフ（折り合い）を理解することで、より良い優先順位づけができます
サイバーセキュリティと技術革新という、相対する事項に対し、企業はできる限り両方に対応しようとしています。特に幹部や事業部スタッフにこの傾向が見られます。IT スタッフはトレードオフ（折り合い）の必要性を理解していることが多いようです。ビジネスへの影響を含め、折り合いをつけるという発想について、技術社員が社内で教育する責任を負うケースが増えてきています。IT オペレーションにおける変化が、今も新たなセキュリティへの取り組みを牽引しています（企業の 57%が言及）。そして、新たなシステム導入に関するコストを考える際、セキュリティをまず念頭におくべきでしょう。

セキュリティ機能において、最も重要な要素がスキルです
企業がセキュリティのスキルを考える際、2 つの異なったエリアを考えなくてはなりません。1 つは一般職員です。企業のうち、自社の業務スタッフが理想的なセキュリティ専門性を持っていると考えているのは 44%にすぎません。スキルギャップがある企業の 77%でトレーニングが行われています。しかし、このトレーニングが非常に効果的だとされるケースは 45%しかありません。2 つ目のエリアとして考えるべきは、技術社員のスキルです。ここで必要とされるのはより深いスキルであることはもちろんです。そしてほとんどの企業は、最新のセキュリティスキル構築のために、トレーニング、パートナー契約、あるいは認定制度を用いています。

セキュリティの指標はいまだ初期段階にあります
サイバーセキュリティの進捗度を測るというコンセプトは、多くの企業にとって、いまだ目新しいものです。特に、戦術的活動から戦略的イニシアチブへと IT やセキュリティを転換させていく、という点については進捗度と言う認識はまだまだです。小規模企業では、セキュリティの指標を重用する傾向が最も高くなって言います。おそらくこれは、自社サービスに関して指標を提供してくれる第三者を使うケースが最も多いという理由からでしょう。ビジネスにおいて、オペレーションのセキュリティ専門センターへの投資が増加するにつれ、トラッキングを目的とした最適な指標を設定

することはもちろんですが、それに加えて、組織の適正なレベルで、その指標を見直す計画策定も必要になってきます。

市場概要

サイバーセキュリティの分野は、あらゆる技術の中でも、最もホットな話題となっています。新興のトレンドが紙面を賑わし、確立されたモデルがビジネスオペレーションに大量のサービスを提供しています。しかし、サイバーセキュリティにとっては、二面ともが常に必要で、常に技術の進化が求められるのです。

サイバーセキュリティについて、CompTIA が行った調査では、企業が求めるスキルや、セキュリティチーム構築のやり方に焦点を当てました。2019 年という 10 年の区切りを目前にした年に、企業のセキュリティについて一歩引いて、全体の状況を広い視野で見るのは有意義だと考えています。

まず手始めに、過去 10 年間で劇的変化を遂げたビジネスや技術の環境を考えてください。2010 年には、メガブリーチという概念はありませんでした。誰もが最初の近代的メガブリーチだと考えているターゲットハックが出現したのはその 3 年後の 2013 年でした。華々しくも急激なソーシャルプラットフォームは、まだ黎明期にありました。Facebook のユーザー数は、2008 年の 1 億 4500 万人から、2009 年の 3 億 6000 万人、そして 2010 年には 6 億 800 万に上りました。ツイッターに至っては、まだ成長のごく初期段階にありました。2010 年のユーザー数は 5000 万人にすぎなかったのです。ソーシャルエンジニアリングのプラットフォームは、サイバー犯罪の舞台となり始めたばかりでした。

一般的な脅威や個人の安全性は言うまでもなく、ビジネスオペレーションにおける脅威もこれまでにないほど高まっています。同時に、新たな技術を試したり、実装したりすることへの欲求も、これまでになく高まっています。2010 年には、企業が模索する技術トレンドは主に 2 つでした。クラウドコンピューティングとモビリティです。これらの技術（特にクラウドコンピューティング）については、いまや、ビジネスが取り組もうとする項目の数がさらに多くなっています。IoT、人工知能、ブロックチェーン、そして拡張現実といったものは、新たなビジネスの可能性を約束するものですが、同時に、新たなセキュリティの複雑性を生み出す要素になっています。

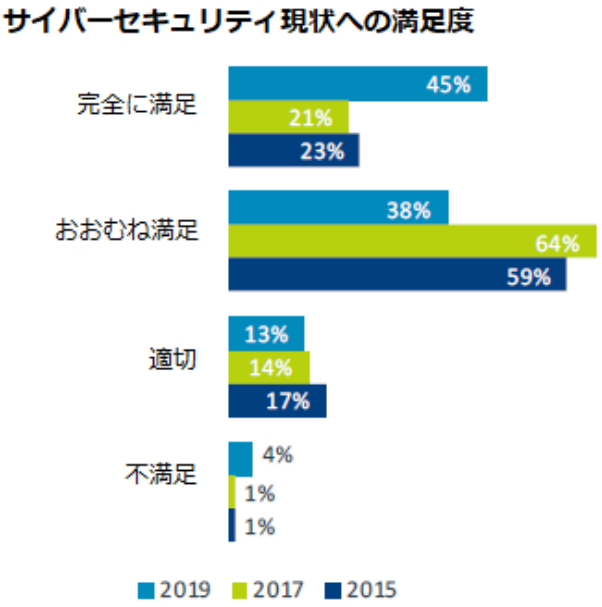
このような動向を考えると、セキュリティは今後数年間、確実に強力な成長を遂げると予想できます。IDC の予測では、セキュリティに対する全世界投資額は 2019 年には 1,031 億円に上るとされています。そして、2022 年まで複合年間成長率は 2022 年まで 92%を維持し、最終的には 1,338 億円で着地すると見込まれています。この成長は、サイバーセキュリティの役割が、既に構築された技術と新興技術の両方に及んでいることを示唆しています。構築済みの技術については、関連するセキュリティ技能と共に、かなり導入が進んでいるため、その成長は比較的ゆっくりであろうと考えられます。新興技術には、新たなセキュリティ方式が必要となるので、より爆発的な成長を見せることでしょう。

IDC はセキュリティへの支出をさらにいくつかのカテゴリに分けています。2019 年において最大のものは、マネージドセキュリティサービスへの支出です。CompTIA の最新データには、この支出を牽引するいくつかの要素が見えてきます。この報告書全体を通して、それらについて述べていきます。IDC によるセキュリティ支出の 2 つ目に大きなものは、ネットワークセキュリティのハードウェアです。これは比較的従来型のファイアウォールや脅威マネジメントといった範疇のものです。上位 4 つの残りは、インテグレーションサービス（新興技術導入とともに重要性が増しています）、そして、エンドポイントセキュリティ（これもモバイルデバイスや IoT とともに進化した従来型の範疇に入ります）です。

過去数年の経緯からの主な学び、そして今後数年間の予測を鑑みると、サイバーセキュリティの特性として、企業に役立つ新たなアプローチがしっかりと定義されて広がっていく、というものではありません。むしろ、サイバーセキュリティは動く標的のようなものです。企業が今、考えるべき新たな要素もあるかもしれませんが、計画は柔軟に、状況に応じて常に変更できるようなものにしなくてはなりません。

ここ数年、特に目立った動きはありませんでしたが、ここに来てセキュリティの現状を「完全に満足」とする企業の数は顕著に増えています。しかしまだ、全調査対象会社数の半分もありません。企業がサイバーセキュリティ構築を高い優先順位に置いていることを考えると、自社の取り組みに満足している企業数はもっと多くてもよいはずです。

さらに悪いことに、累積数だけを見てみると、あたかもうまくいっているかのように見えてしまいがちです。職位ごとに見ると、幹部社員の 55%が自社のセキュリティに完全に満足していると答えています。そして事業部社員の 61%も同じ評価をしています。しかし、IT スタッフ、つまりセキュリティアーキテクチャを最も理解している社員の回答を見ると、この数値は 35%と下がっています。



一般的に言って、近代的サイバーセキュリティが及ぶ範囲は、単なる技術的アプローチの枠を超え、プロセス面での取り組みや従業員教育にまで拡大してきています。セキュリティへの取り組みの現状に満足感が無いのは、更なる転換が必要だということです。セキュリティは複雑で変化が速いため、深いレベルでのしっかりした取り組みと継続的な管理が必要となります。それを実現するため、企業はこの重要なエリアへの投資レベルを前向きに検討しなくてはなりません。

サイバーセキュリティに対する企業の考え方

サイバーセキュリティへの取り組みがこれほど困難な理由として、いろいろな要素間での綱引き状況が挙げられます。強固なサイバーセキュリティ対エンドユーザーの利便性、あるいは、堅牢なサイバーセキュリティ対組織における積極的な技術導入といった綱引き状況があります。クラウドコンピューティングの黎明期には、後者の綱引き状況が注目され、その中でサイバーセキュリティへの近代的アプローチの必要性が強調されていました。多くの企業が、従来のセキュリティの考え方が、新たなモデルに適用できないことを十分に認識しないまま、クラウドのプロジェクトに飛び込んでいきました。時間がたつにつれ、企業が優良事例を目にするようになり、それとともにクラウドセキュリティの障壁はかなり低くなってきました。そしてセキュリティ問題への認識はその後の技術トレンドと相まって、かなり高くなってきたと言えます。

企業に対して、どのようにサイバーセキュリティと技術イノベーションに対応しているかを尋ねると、まだそこに綱引き関係があることがわかります。均衡を取ったアプローチが最も一般的で、企業の 48%がこの 2 つのトレンドの均衡を取ろうとしていると答えています。40%の企業が、技術イノベーションよりもサイバーセキュリティを優先していることから、サイバーセキュリティの重要性が見て取れます。最後に、最先端技術を求める姿勢が強いことも明確になっています。企業の 35%がサイバーセキュリティよりもイノベーションを優先しているのです。

技術イノベーションとセキュリティへの取り組み

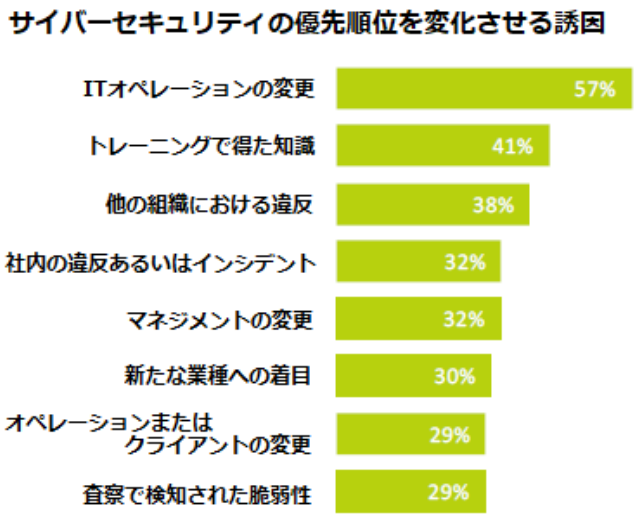
	幹部	事業部スタッフ	ITスタッフ
セキュリティよりイノベーションを優先	39%	46%	29%
イノベーションよりセキュリティを優先	47%	43%	35%
両方を均衡	50%	49%	45%
Total	136%	138%	109%

ただ、注意すべきは、回答した企業が明らかに、相いれないグループをまたがって複数回答の選択をしているということです。この調査は、技術追求とセキュリテ

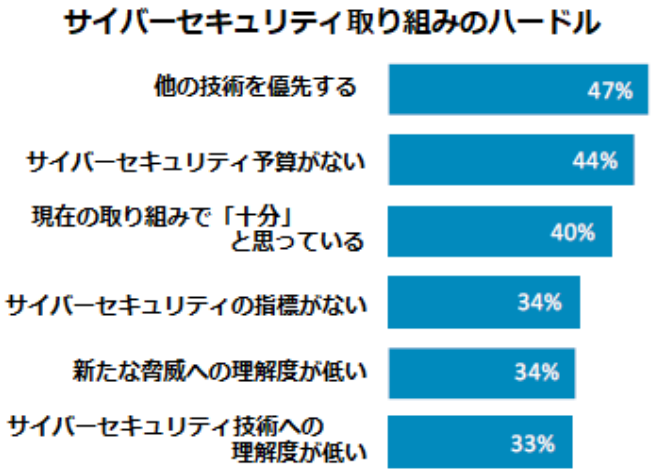
ィニーズに関してどれくらい混乱があるかを測れるよう、意図的に設計されています。そして回答状況をみると、ある程度の混乱が確実に存在していることがわかります。幹部社員や事業部スタッフが「上記すべて」的なアプローチをしがちであることは理解できます。IT スタッフは、新たな取り組みをすることイコール、ビジネスオペレーションを破壊することだ、という点をより認識しているようです。

ここ数年で、サイバーセキュリティの問題への理解は目覚ましく進みましたが、まだ改善の余地はあります。とくに、強力な技術的背景を持っていない社員に関して改善が必要です。幹部や事業部スタッフは、企業内でサイバーセキュリティはしっかり理解されていると考えがちです。彼らの 91%が、理解レベルを「非常に高い」あるいや「平均以上」としています。しかし、IT スタッフでこのような回答をしたのは 78%にすぎません。

デジタル組織になるための主要な要素の一つが、よりよい理解の構築です。これまでのセキュリティ調査の結果にも示されているように、セキュリティの重要性への認識を高めるきっかけとなるのは、IT オペレーションの変更です。これを裏付けるように、86%の企業が、過去 2 年間に技術アプローチに何等かの変更をしたと認めており（たとえば、導入加速、あるいは新興エリアの検討など）、87%の企業が同じ期間にセキュリティアプローチを変更したとしています（たとえば、新たな技術付加や、従業員教育の実施など）。

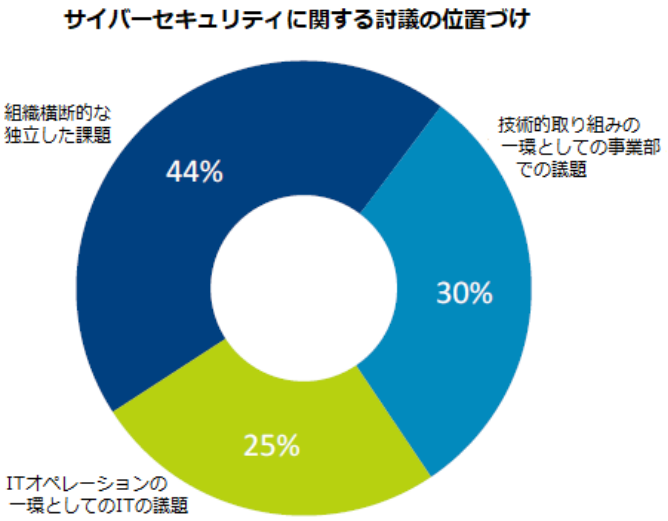


企業がサイバーセキュリティのアプローチを変更しようとするにあたり、理想的状況を実現するには常に課題がつきものです。「他の技術を優先する」が最大の課題に挙がっていることから、技術イノベーションとサイバーセキュリティを取り巻く混乱において、技術イノベーションがいまだに強力な引きであることがわかります。ほとんどの技術的取り組みにおいて、予算の問題がハードルとなるのは当然と言えますが、セキュリティが本当に優先事項となっているのであれば、予算も同時に上がってくるはずです。一般的に言って、IT がより戦略的な技術へと変化するにつれ、IT に対するコストセンター的アプローチも変わってきています。そしてこれはとりわけサイバーセキュリティに関して見られる傾向です。



サイバーセキュリティに関するさまざまな問題に対し、ビジネス界では、セキュリティを IT 戦略の要素の一つとしてではなく、独立したものとして対処しなければならないことを認識し始めています。2016 年、CompTIA の「A Functional IT Framework」白書において、セキュリティが多くの企業において、ごく近い将来、突出した取り組みになるであろうと予想されていました。こんにち、全企業の約半数が、セイバーセキュリティが独立した課題として全社横断的に検討されていると述べています（サイバーセキュリティが、技術面での決定がなされてからの後付け的存在であると答えた会社は 2%であることにも注意すべきでしょう）。

このような社内横断的な検討は、サイバーセキュリティがらみの問題を浮き彫りにするのには有用かもしれません。しかし、だからといって適切なソリューション構築の構造を生み出すわけではありません。サイバーセキュリティチームの構築は、2018 年の CompTIA セキュリティ調査の主要テーマでした。そして、そこで重視されたセキュリティチームの概念は、いまだ大半の企業にとって非常に新しい考え方である、ということです。この状態は 2019 年まで続いています。さらに、サイバーセキュリティ機能をどこで果たすか、という点におけるデータの劇的な変化から、多くの企業はサイバーセキュリティセンターの定義ですら迷っている状態が見て取れます。しかし、こういった動きの中、注目すべき主要事項もあるのです。



まず、企業においては、オペレーションの中心を社内に置こうとする傾向が見えます。概念として考えれば、これは納得できることです。リスク抵抗性の検証、データの分類、そしてセキュリティインシデントへの対応などは、企業の DNA を理解している社内従業員が最も適任です。ただし、専門チームを作ること自体が課題になる可能性があります。特に、一般邸に IT スタッフが揃っていないような小規模ビジネスにとっては大きな問題でしょう。

この状態から次のポイントが派生してきます。つまり、セキュリティチームの多様性です。社内にセキュリティオペレーションセンターを持とうとする企業のほとんどが、同時に、継続的またはその時々のプロジェクトで社外の第三者を活用すると述べています。一部の会社では、オペレーションの中心を社外の機能としていますが、そのほとんどが、この機能を社内人員で補助する形をとっていると述べています。その社内人員は通常、責務の一部にセキュリティが含まれている IT 担当社員です。

これらの傾向を考えあわせると、セキュリティが将来、ビジネス全体における懸念点になったときに、どのような位置づけで対処されるかが想像できます。想定される位置づけは、これまでの企業における自社の IT としての位置づけ、というよりは、IT 以外の重要な事業部門、たとえば法務や経理といった部門の扱いに最も近いイメージです。

非常に小規模なビジネスはこのような役割のために専門家を社内で雇う余裕はありません。しかし、専任担当者を必要とする状況は差し迫っています。第三者にこのエリアの管理をゆだねる場合、幅広いビジネスオペレーションを扱っている会社ではなく、クライアントの特定の業界またはその事業分野に深い専門知識を持った会社がその任に当たるべきなのです。

セキュリティがビジネスにおいて、その他の取り組みと同等の重要性を持っているとするならば、他の取り組みと同様の専門チームが必要となるわけです。チームの社内スタッフは、全体的な戦略や日々のオペレーションを牽引するセキュリティ専門家でなければなりません。セキュリティ-チームの報告体制は、セキュリティチームの成長に合わせて進化していかなければなりません。セキュリティ部門が CIO、COO、あるいは CEO にまで報告するようなケースもあります。

セキュリティを第三者が管理するという話になると、専門性については同じ要件が適用されます。きちんと機能するためには、セキュリティ会社は広く深く、セキュリティ関連を網羅する知識を持つ必要があります。一般的な IT 企業がセキュリティ責任窓口となり、専門的な部分を下請けに出す、という形もあり得ますが、このような形態はまだ世間一般では標準的ではありません。そして、自社と第三者との契約だけを考えている企業には、外部でさらに階層化されるような業態をカバーするような予算は無い、ということも想定されます。

マネージドセキュリティサービスがセキュリティ支出の主要な要素となる、と IDC が予測した際、かなりの専門性をもったサービス提供会社を想定していたと考えられます。IT 業界における他の多くの用語と同様、マネージドセキュリティサービスという名称が示唆するものは非常に幅広いので、実際に提供できるサービスの数がさほど多くないセキュリ

ティ会社でも、これを謳うことができてしまいます。予測される企業からの支出額増加の恩恵を全面的に享受するためには、IT 会社は自社のセキュリティポートフォリオとスキルを向上させておく必要があるのです。

セキュリティの置かれた状況は、すべての技術分野全体で起こっていることを象徴しています。企業はより戦略的になり、その要件はさらに意欲的かつ複雑になってきています。過去には、単に基本的な部分を提供する、ということだけでビジネスモデルとして十分だったかもしれませんが、現代の技術プロバイダには、強力な技術知識が必要とされます。セキュリティでいえば、使用される多くのツールや技能、安全なビジネスオペレーションを実現するためのプロセス、そして従業員間でのセキュリティリスクを確実に少なくする方策、といったことについての知識を意味します。

サイバーセキュリティのスキル構築

セキュリティ実務者にとって、最新の実践をすることは非常に重要です。しかし、各ビジネスプロセスに技術的機能が入り込んでいる状況においては、セキュリティ実践が全従業員の問題になっています。ビジネスはヒューマンエラーの発生を最低限に抑える最適な方法を決めなければなりません。ヒューマンエラーは常に、セキュリティインシデントの第一要因となっているからです。つまり、不快知識を必要とする職務について特に検討するだけでなく、基本的なサイバーセキュリティについての意識喚起について広い範囲で検討することが必要なのです。

通常、ほとんどの企業はセキュリティへの意識やスキルに関しては、目的とするレベルに至っていません。特に、セキュリティ専門家ではないスタッフについて、それが顕著です。従業員の専門性を考える際にまず対象となるのが事業部スタッフです。直接 IT の仕事をしていない従業員には、深いセキュリティ知識は必要ないにも関わらず、そうあるべきという発想であらゆる評価がなされています。事業部スタッフが企業の期待値に対して最も低いランクにあるという事実からも、新たなアプローチが必要であることがわかります。

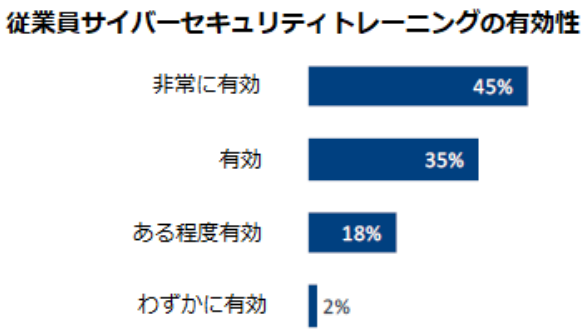
サイバーセキュリティの実践レベル

	事業部スタッフ	一般ITスタッフ	セキュリティ専門家
まさに目的とするレベルにある	44%	47%	54%
理想的なスキルセットにやや至っていない	32%	36%	32%
理想的なスキルセットにあまり至っていない	15%	9%	7%
目的とするレベルには全く至っていない	4%	5%	4%

この低いランキングに関して驚くのは、ほとんどの企業が問題に対処する明確な歩を進めているように見えることです。スタッフ間にサイバーセキュリティ格差がある 4 社のうち 3 社が、一般職員にサイバーセキュリティトレーニングを行っている、と述べています。会社規模にかかわらず、数値は一定しています。小規模企業（従業員数 100 名未満）の 74%、中規模企業（従業員数 100～499）の 75%、そして大企業（従業員数 500 以上）の 81%がトレーニングを実施しています。トレーニングとセキュリティ対策に対する満足度の間には比較的強い関連性があります。現在の自社セキュリティに全く満足している企業の 93%がトレーニングを行っているのに対し、現在の自社セキュリティは適切、あるいは不満と答えた企業の中では、トレーニングを実施しているのは 61%にすぎません。

セキュリティトレーニングが提供されているようには見えますが、従業員の意識についての理解が向上しているとは言えません。従業員へのトレーニングを行っている企業について、有効性のランクが事業部スタッフの専門知識のランクと関連しているのは興味深い点です。トレーニングの効果がない理由がわかれば、高いセキュリティ意識をもった社内構成を構築するために企業が取るべき次のステップが見えてきます。

効果の低いトレーニングとスキルのないスタッフという問題の背景となっているのは、成功を定義するためのしっかりしたデータが無いことです。現在のところ、CompTIA の調査では、スキルギャップや効果的なトレーニングについて、個々の認識の背景を深く探ったことはありません。しかし、調査では全体的なセキュリティ機能の指標使用についての評価は行っています。その結果はこの報告書で後ほど述べますが、簡単に言うと、ほとんどの企業では指標をしっかりと使用してはいません。そして、これはおそらく、従業員トレーニングにもあてはまると思われます。サイバーセキュリティにおいては比較的新しいコンセプトだからです。



トレーニングの効果と従業員の意識レベルに関する指標を構築しようとしてきた企業もあります。フィッシング攻撃のシミュレーションを使用すれば、企業は自社の従業員の何人が怪しいメールを適確に処理するかをトラッキングできます。そして、トレーニング前後のその人数を比較できるのです。セキュリティ知識の標準的評価では、弱点を指摘し、的を絞ったトレーニングについてのアイディアを提供します。ビジネスが取り組みを考える際に、推測にもとづくのではなく、このようなタイプの指標による具体的参照データを使うことができます。

指標を使用するためには、何を計測するかを理解しておくことが必要です。もしかしたら、これこそが企業にとって大きな課題かもしれません。従業員トレーニングは比較的新しコンセプトであることを考えると、ビジネス側では理想的なスキルセットの構成要素をきちんと把握していない可能性があります。さらにさまざまな職務を考えると、この問題はさらに複雑な話になります。たとえば、メールへのアクセスがない製造フロアにいる従業員は、フィッシングメールの識別力を緊急につける必要がありません。指標を適用し、進捗状況を把握するためには、適格なスキルレベルについての決定が必要になります。

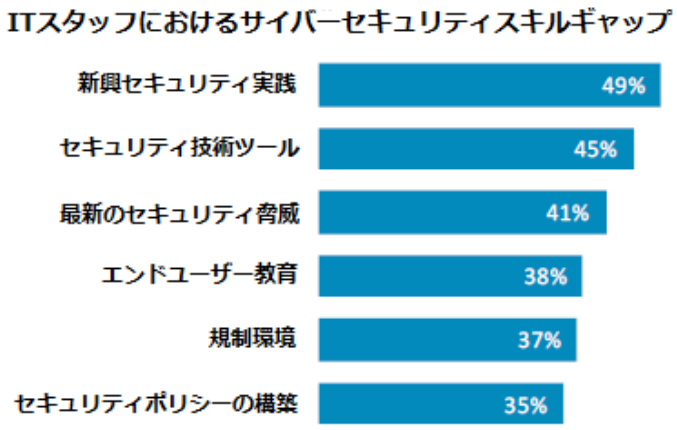
こう考えると、さらに複雑な事態になってきます。スキルのレベルを知ることで、ヒューマンエラーのリスクを真の意味で抑制することはできます。しかし、低減されたリスクをトレーニングの効果として完全に関連づけることは不可能かもしれません。トレーニングを効果的なものにするだけでも大変ですが、どんなに問題解決に向けての資金やエネルギーを注入したとしても、改善を促進できることが保証されているわけではなりません。企業は、サイバーセキュリティのトレーニングへのアプローチを決定すること以外に、ヒューマンエラーへの全社的アプローチも決定しなくてはなりません。この決定をするには、ビジネスの最上層部の各責任者間で、合意を取り付ける必要があります。その中には理事会や他の執行部門が入ることが多くなってきています。

一般従業員からさらに進んで、IT スタッフのスキルギャップを見てみると、さらに的を絞ったアプローチが必要になります。セキュリティスキルに関する需要を後押しした要素として、2 つの主要な変化があります。まず、サイバーセキュリティが IT 機能を超えた広範なものになってきたことです。かつて企業は、セキュリティは IT 担当に求められる多くのスキルの一部だとみなしていましたが、今や、デジタル資産のセキュリティ専属の従業員の必要性を考えるべき時に来ているのです。

この 1 つ目の変化から派生する形で 2 つ目の変化が起こっています。セキュリティが特筆すべき技能分野となるにつれ、最先端インフラやオペレーションのプロセスの安全を図るために必要とされるスキルセットが多様化しています。この 2 つの変化によって、セキュリティ業務の人材募集がめざましい成長を遂げました。Burning Glass Technologies の労働インサイトによると、サイバーセキュリティ業務の人材募集は 2017 年から 2018 年にかけて 34%増加しています。需要は驚異的に高まっていますが、供給はそれに全く追いついていない状況です。

需要の多いスキルは現代のセキュリティにおいて、3 つの主要カテゴリに大別されます。もっとも求められるスキルは、比較的従来型の技術カテゴリに属するものです。より先取的意識を反映する新たな実践（サイバーセキュリティ解析や浸透試験など）における、クラウド/モバイルインフラ（データ損失予防や識別、あるいはアクセス管理など）に対応するツールであれ、デジタル依存を逆手に取る新たな脅威（たとえばソーシャルエンジニアリングや DoS 攻撃）であれ、

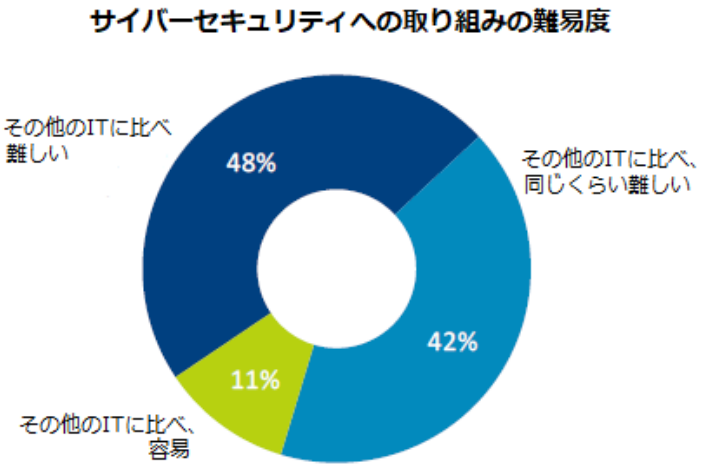
企業は自社の IT およびセキュリティ専門家が技術環境の変化速度に追いついていられるようにする必要があるのです。



前述の従業員教育に伴い、トレーニングやエンドユーザー行動の継続的モニタリングを誰が管理するのかという問題が出てきます。ほとんどの企業では自社の IT 部門、あるいはセキュリティソリューションプロバイダにそれを委ねようと考えていますが、これによって教育するというスキルも必要になってきます。多くの IT 実務者は特定のツールについてトレーニングを提供した経験があるかもしれませんが、セキュリティ教育はそれとは異なり、実際に行動を修正したり、セキュリティポリシーの裏にある根拠をしっかりと理解させたりするものなのです。

求められるセキュリティスキルの最後のグループは、安全なビジネスオペレーションに必要なプロセスに関するものです。この中には、法務や規制の知識も含まれますが、この状況は、特に規制が厳しい業界だけに留まらず、かなりの速度で範囲を拡大しています。また、組織全体で実践されるべきその他のポリシーもここに含まれてきます。たとえば外部の組織との関係や、システムあるいはデータの正式なリスク分析がそれにあたります。

サイバーセキュリティ専門家の人材不足は、企業が自社のセキュリティにおけるスキルギャップへの取り組みを難しくしている理由の 1 つにすぎません。実際、企業セキュリティアプローチ（企業の 58%が言及）への移行と現代のセキュリティが持つ複雑性（57%）によって、他の IT スキルに比べてサイバーセキュリティへの取り組みが難しくなっているのです。他の理由としては、しっかり定義されたトレーニングの選択肢がない、あるいは他の技術計画に比べて、サイバーセキュリティの優先度が低い、などが挙げられています。



おそらく、一般労働市場でスキル人材が不足していることから、サイバーセキュリティのスキルギャップを埋めるための新規採用というのは最後の選択肢になるでしょう。最近、追加の人材採用を考えたという企業は 33%しかありません。追加の助力を求めると言う点においては、外部会社とパートナー契約を結ぶというのがかなり一般的な選択肢となっており、セキュリティ面での不足を補うために外部パートナーを活用している企業は 49%に上ります。

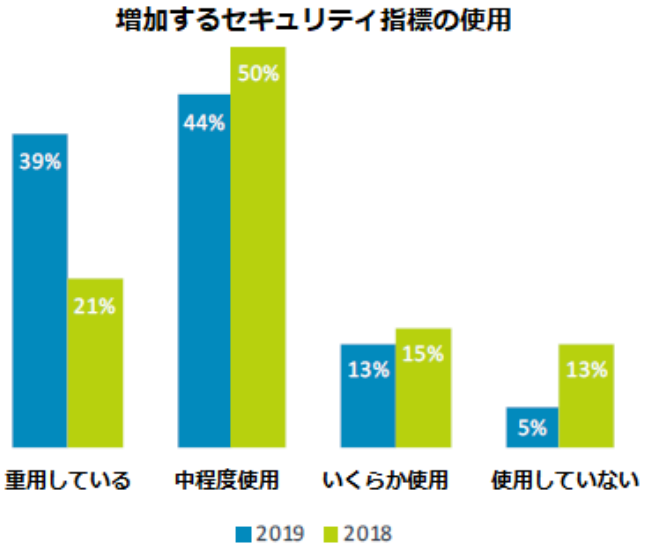
最も経済的、かつビジネスのセキュリティ戦略管理能力を強化する選択肢としては、既存の従業員に目を向ける、と言うものがあります。これはトレーニング（企業の 69%が活用）や認定制度（48%）によって行われています。認定制度は明らかにかなりの投資を要するので、トレーニングで十分だと考えたり、組織内に認定制度に対する理解が不十分だと感じたりする企業もあります。

認定制度は、セキュリティへの取り組みを調整するための知識を企業に提供することに加え、個々の従業員と組織全体にさまざまな利点を提供することができます。企業は自社のセキュリティ専門家が深い知識を持ち、最新の実践を行い、内外のチームとの協働を一貫して行っているという点について、自信を強めることができます。認定制度の価値についてのさらに詳しい記述は、CompTIA が協賛している IDC 白書、「キャリアマイルストーンにおける認定制度とトレーニングの影響（Impact of Certifications and Training on Career Milestones)を参照してください。

サイバーセキュリティ進捗のトラッキング

サイバーセキュリティが継続的な戦略的課題となるにつれ、進捗を計測し、データに基づく決定をする必要性が増してきました。セキュリティへの取り組みが単にファイアウォールやアンチウィルスのソフトをインストールすることに終始していた以前の環境では、指標はそれに対応するシンプルなモノでした。セキュリティ侵害ゼロ、で済んでいました。セキュリティへの取り組みがはるかに複雑になり、当然コストもかかるようになった環境では、取り組みや投資の計測も向上させる必要があるのです。

2018 年に比べて、自社セキュリティを進めるにあたって、指標を用いている企業数は明らかに増加しています。驚くことに、小規模企業がこのエリアで牽引役を務めています。大規模企業で指標を用いているのが、37%、中規模企業では 27%であるのに対し、小規模企業では 48%です。小規模企業におけるセキュリティ専門性が最も低いことを考えると、この数字には疑問の余地があるかもしれませんが、マネージドセキュリティに関して、小規模企業が最も第三者を使用する傾向を見せていることも確かです。この状況は、実際のセキュリティ活動の効果検証以外にも、提供されるサービスに関する指標構築が進む要因となっている可能性につながります。

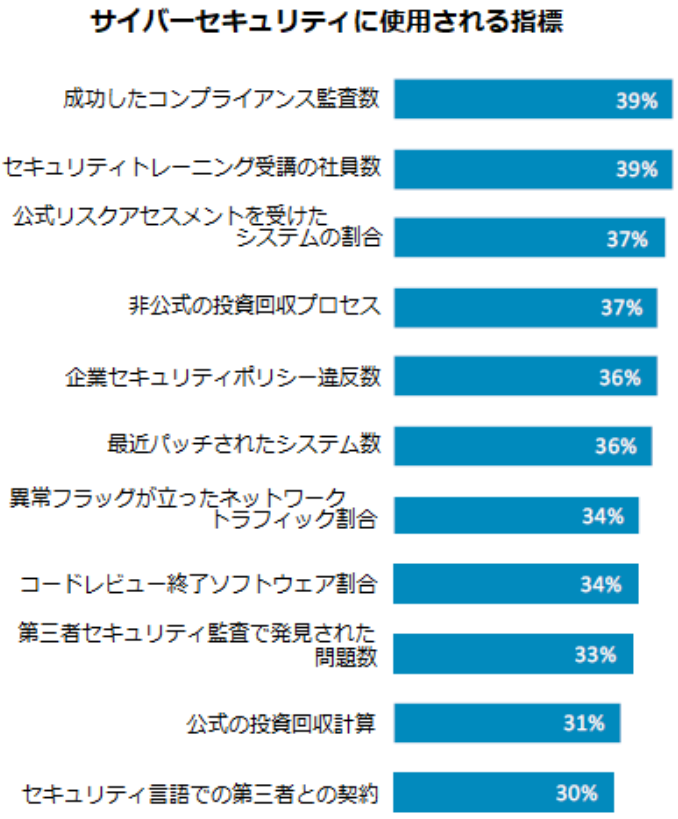


自社のセキュリティ現状に関する満足度という点で企業を評価してみると、さらに明確なコントラストが浮かび上がります。全く満足と答えた企業の過半数（64%）が、セキュリティ指標を重用していると述べています。それに比べ、おおむね満足と答えた企業で指標を重用していると述べたのはわずか 19%です。自社のセキュリティが適切なレベル、あるいは不満足と答えた企業では、この数値はさらに下がって 16%になっています。

明らかに、自社のセキュリティ状況に完全に満足している企業は、取り組みの結果を計測しているからこそ自信を持って明言することができるわけです。指標を構築するのは容易いことではありません。リソースが限られている分野では、定期的な指標トラッキングに割けるリソースがない、というのが指標を使用しない第一の理由となっています。しかし、セキュリティ機能がより公式になるにつれ、指標を盛り込む業務は、企業規律の形成という面で余剰効果を生むことになるでしょう。

セキュリティ指標の出発点としては、組織の中のどの部分が指標構築プロセスに関わるべきかを決定することです。セキュリティがビジネスオペレーションにおける重要性をいや増していく中、IT 機能を超えて、幅広く成功状況を検証するのは当然といえます。IT 従業員が、関連する指標を設定する傾向が最も高く、69%の企業がその動きを報告しています。しかし、指標の検討はもっと連携体制で行う活動です。組織内の各レベルでの考えがセキュリティ指標の検討にしっかりと反映されなければなりません。これは IT 部門（51%の企業で参加）から中間管理職（57%）、そして上級幹部（55%）に至るまでです。組織内での巻き込みという意味で、前年比で最も大きな進捗を遂げたのは、役員、あるいはその他の執行部に関してです。2018 年には、セキュリティ指標設定に役員が関わっているとした企業は 30%、検討に関わっているとした企業は 38%でした。2019 年にはこの数値がそれぞれ 42%と 53%になっています。

連携できる環境があれば、次に問うべきは、どのセキュリティ指標が使用するに最適なものか、ということです。この段階では明確な答えはありません。さまざまなセキュリティ指標を多種使っているということは、企業が最適な組み合わせを見つけようと実験しているということです。指標に関する最優良事例がまだ出てきていないのは、驚くことではありません。ビジネス界は、セキュリティは別箇に力を注ぐべき機能であることを認識する初期の段階にあります。この機能がしっかり構築され、技術、プロセス、そして教育のエリアでより率先されるようになれば、自社の取り組みを最もよい形で定数評価し、サイバーセキュリティを全社的成功と関連づけられるような指標は何か、が見えてくることでしょう。



本調査について

定数調査査は、2019 年 7 月に行ったワークフォースプロフェッショナルを対象としたオンライン調査で成り立っています。米国を拠点とする計 400 社が調査に参加し、全体のサンプリング誤差マージンについては+/-5.0%ポイントでの 95%信頼性を獲得しています。サンプリング誤差はデータのサブグループの方が大きくなっています。

どの調査でも同じですが、サンプリング誤差は起こり得る誤差理由の一つに過ぎません。非サンプリング誤差が正確に計算できないため、その影響を最低限に抑えるべく調査設計、集計、データ処理のあらゆる段階において予防的措置が取られました。

CompTIA は内容および解析すべてに責任を負います。調査に関する質問はすべて、Research / Market Intelligence のスタッフ research@comptia.org が対応いたします。CompTIA は Market Research Industry's Insights Association の会員であり、国際的に尊重されている調査基準と倫理を順守しています。

CompTIA について

CompTIA（the Computing Technology Industry Association）は、IT 業界の声として活動する非営利団体です。

約 2,000 の会員企業、3,000 の学校機関およびトレーニングパートナー、10 万を越える登録ユーザーおよび取得者数 200 万人以上の IT 認定資格を以て、CompTIA は教育プログラム、市場リサーチ、ネットワーキングイベント、プロフェッショナル認定資格、公的政策提言を通して業界の成長促進に取り組んでいます。

他のリソース

リサーチ

CompTIA は 100 以上のリサーチ報告書、要約、導入事例、エコシステムなどのアーカイブを持っていますが、それに加えて年間 20 を超える研究を実施しています。これらの多くが、ワークフォース分析の要素を含み、業務、スキル、採用実践、プロフェッショナル育成といった内容を含んでいます。

認定資格/学習

CompTIA は世界の IT 人材に対するベンダーニュートラルなスキル認定と教育を提供するリーディングプロバイダです。CompTIA は異なった知識基準を評価する 4 つの認定カテゴリを有しています。エントリーレベルから専門家レベルまで、クラウドコンピューティング、モビリティ、リナックス、ネットワーキング、セキュリティ、ヘルプデスクと技術サポート、サーバ、プロジェクト管理、その他のミッションクリティカルな技術といった内容を網羅しています。

コミュニティ/委員会

CompTIA メンバーコミュニティと委員会はベストプラクティス、協働的問題解決、そしてメンタリングを行うフォーラムです。当報告書で取り上げられている新興トレンドに関わる議論が頻繁に行われています。

政策提言

公的な政策提言の取り組みではありますが、CompTIA は一連の IT 企業に影響を与えるような、メンバー主導のビジネスおよび IT の重点実行項目を支援しています。小規模 IT サービスプロバイダやソフトウェア開発企業から、大規模機器製造会社や通信サービスプロバイダまで幅広く対象としています。CompTIA はテクノロジー企業の目、耳、そして声となっています。