2018 Trends in Cybersecurity – Building Effective Security Teams
サイバーセキュリティの動向：効果的なセキュリティチームの構築

サイバーセキュリティがその複雑さを増すにつれ、これまでの方法では、企業データの保護や個人情報の取り扱いといったような、広範な課題に対応しきれなくなっています。現在、セキュリティに関しては、新たなテクノロジー、プロセスの向上、広い意味での人材教育が求められているのです。新しいアプローチを取るにあたっては、組織内での文化を変える必要がありますが、それだけでなく、多様なスキルセットも求められます。企業が、このデジタル時代に求められるセキュリティに対応できる専門性を培うためには、セキュリティチームを立ち上げ、社内外の人材を活用することになります。このリサーチでは、そのための方策を検討していきます。

KEY POINTS: キーポイント

ほとんどの会社で、サイバーセキュリティ活動の主要部分は社内で行われています
通常の IT インフラチームの一部であれ、またはセキュリティ専門職であれ、セキュリティ人材を擁する会社の 72%が、企業オペレーションのためのセキュリティセンターを、社内でもつ機能だと考えています。サイバーセキュリティがオペレーションや評判に大きな影響力を持つようになっているため、企業は当然、いろいろなことに目を配ろうとしているわけです。

内部対応をしている企業でも、そのほとんどが外部の力を借りてサイバーセキュリティに取り組んでいる
社内にセキュリティ人材を抱える企業のうち、78%がセキュリティ対応のために外部組織を使っています。特定のセキュリティ活動に関して、外部企業と継続的な契約を結んで行っている場合もありますし、個々のプロジェクトごとに適宜、外部組織を使う場合もあります。実際、外部のパートナーを使用している企業の半数が、セキュリティ目的のために 2 社、3 社という異なる会社を使っています。このことからも、セキュリティがいかに複雑なものかがわかります。

サイバーセキュリティのスキル向上が必要
企業の中で、アクセスコントロールやネットワークセキュリティなどの特定スキルは、比較的強力に取り組まれていますが、脆弱性管理やセキュリティ分析などの他のスキルはまだまだです。しかし、強力なスキルの中にも、企業としてさらに向上を図ろうとしているものがあります。例えば、ネットワークセキュリティを大幅に向上することが必要だと感じている企業は 25%ですし、さらに、64%が中程度の改善が必要だと考えています。

必要なのは、サイバーセキュリティへの取り組みと成功度を定数管理する強力な測定基準
セキュリティへの取り組みに測定基準（メトリックス）を多く活用している企業は 21%しかありません。セキュリティが防御戦術から積極的な取り組みへと移行していく中、「公式なリスク評価を行ったシステム

の割合」や「異常フラッグが立ったネットワークトラフィックの割合」などといった測定基準が、成功度を計測するのに役立つだけではなく、今後どこにコストをかけていくのかという判断にも活用できます。

市場概況

この 10 年間、テクノロジー業界は大きく 2 つのドメインに分かれてきました。一方では、企業オペレーションを再定義するような新たなテクノロジーが生まれています。初期に出てきたクラウドコンピューティングやモバイルデバイスが、IT アーキテクチャの一部を構築してきました。最近出てきているのが、モノのインターネット(IoT)、人工知能、そしてブロックチェーンで、これらによって従来のテクノロジー活用・管理がさらに破壊されることが予見されます。その一方で、日々のオペレーションには欠かせないものの、新たな成長を牽引するわけではない従来型テクノロジーも存在しています。サーバー、ネットワーク、そしてストレージが大きく取り上げられることはないでしょうが、IT のプロはこれらが現代のニーズに対応すべく、進化している様子を注視しているのです。

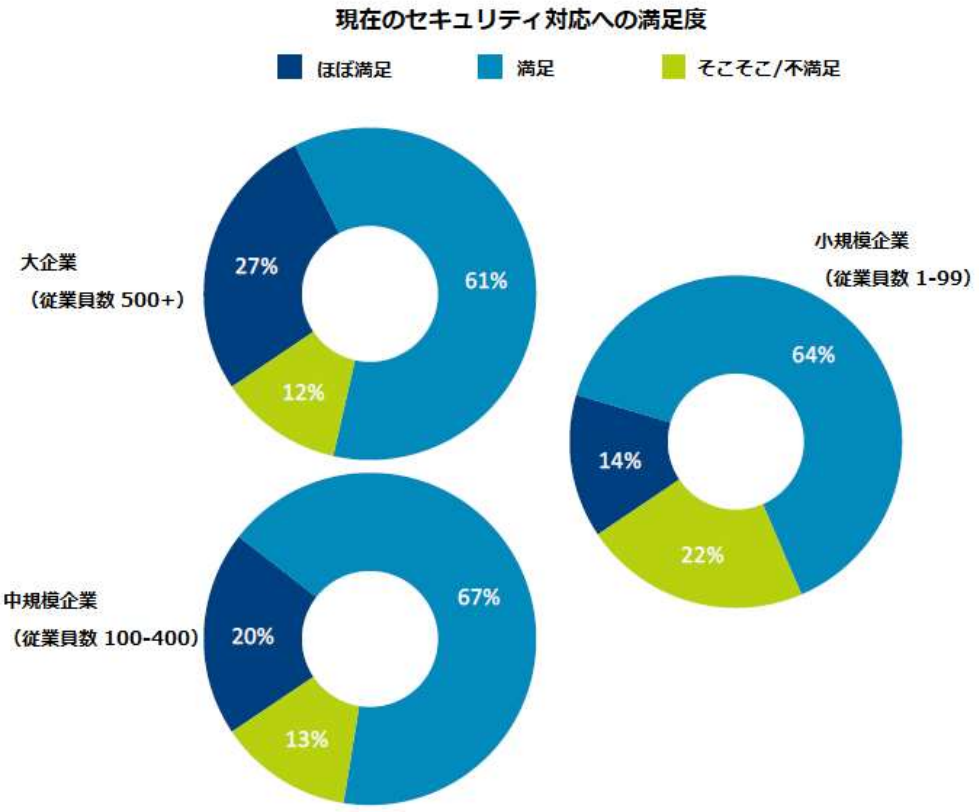
サイバーセキュリティはこの 2 つのエリアに関わっています。この新時代の初期、サイバーセキュリティはどちらかと言えば従来型のテクノロジーだと思われていました。現行モデルに大きな変更をすることなく、単に範囲を広げることによって新たなベンチャーに取り込まれていくものだ、と。昨今、新しいテクノロジーを使用するには、セキュリティに対する新たなアプローチが必要であることを、企業側は認識しています。従来型の部分をそのまま使うことはできますが、新たな構成要素とプロセスを追加する必要があるのです。

サイバーセキュリティには、片足を従来型の方式に置きつつ、もう片方の足は新興テクノロジーに置いているという二面性があるため、この分野では平均以上の収入を得られるのでは、という期待感が高まります。CompTIA の IT Industry Outlook 2018 では、2018 年には IT セクター全体で 5.0%の成長を見込んでいます。サイバーセキュリティ分野に関して、IDC によると 2018 年には 10.2%の成長が見込まれ、これによって全世界収入額は 914 億ドルになるとされています。この数字には、セキュリティ関連ハードウェア、ソフトウェア、そしてサービスが含まれることは注目すべきでしょう。つまり、IT セキュリティへの従来型のアプローチではハードウェアとソフトウェアが中心的役割を担っている一方で、現在のアプローチにはコンプライアンス管理やエンドユーザー教育といったサービス的要素が含まれており、この両方が数値に表れているということなのです。

サービス的要素が付加されたことにテクノロジーのツールボックスの発展が相まって、IT セキュリティはさらにその複雑さを増しています。CompTIA の Functional IT Framework 白書では、セキュリティが広範なインフラの一部としてではなく、独自の機能となってきた様子を知ることができます。IT セキュリティには新たな方法が取り込まれており、現行ビジネスの成功への重要性が増していることから、特に注意して見ていく必要があります。

残念ながら、これらの複雑さをすべての企業が容易に吸収できるわけではありません。従業員数が 100 人未満の会社は大企業に比べて、自社の IT セキュリティはそこそこ/不満足と感じる傾向がかなり強く見られます。頼れるしっかりした人材プールがないため、小規模企業はサイバーセキュリティの新たな展開への対応に苦慮しています。攻撃の量が増加するにつれ、企業は資産を守り、顧客データを保護するための方策を真剣に考える必要に迫られています。

現在のセキュリティに必要なテクノロジー、プロセス、教育に対応するべく、企業はセキュリティチームを立ち上げることを考えています。堅牢なサイバーセキュリティ戦略構築に欠かせない専門スキルを担保するため、チームは内部と外部の人材の組み合わせで構成されることが多くなっています。

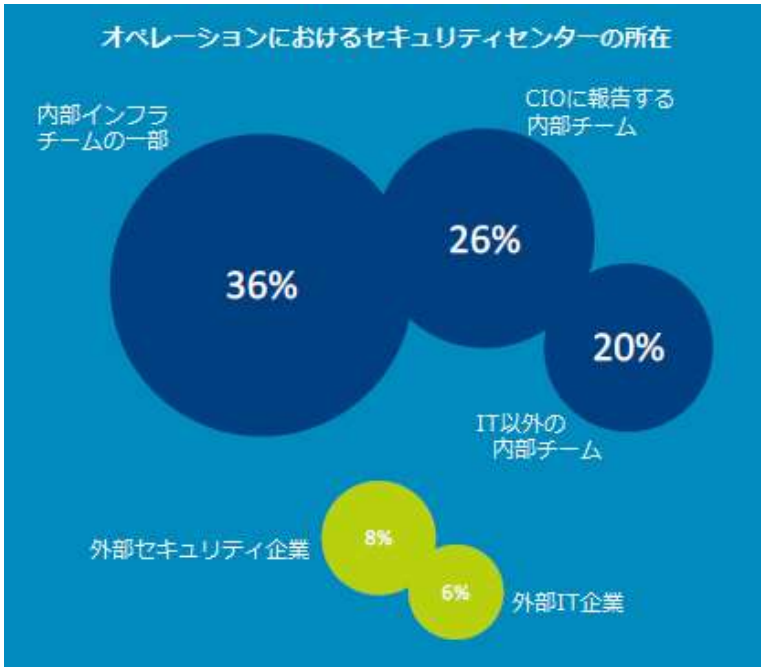


サイバーセキュリティにあまり力を入れていない企業にとっては、機能するチームを立ち上げる機運醸成は難しいかもしれません。自社のセキュリティが「まあ十分」と考えている企業は 46%にも上りますし、45%の会社がセキュリティに充てる予算が不足していると報告しています。しかし今後、セキュリティの重要性に対する認識が企業間で広がるにつれ、総合的なサイバーセキュリティ導入の必要性に対処できる適正レベルの専門性を確保するべき、という指示が企業の上層部から出てくることになるでしょう。

セキュリティチームの基本

サイバーセキュリティ専門チームが増えてきたとはいえ、まだ一般的ではありません。大企業が先鞭をつけています。人材をほぼ自社で潤沢に持っている企業もありますが、そういった企業は同時にサイバー攻撃のリスクも非常に大きいのです。大企業のほとんどが CISO を導入していますが、そこでも多様な報告系統が見られます（《例》CIO に報告、CEO に報告、CFO に報告、等）。どの企業においても、サイバーセキュリティに関する変更事項の中に、セキュリティ専門チーム創設は最低限の共通項として見られるものです。

しかし、セキュリティ活動の中心を明確化するために、特化したチームが必要だ、というわけではありません。セキュリティ機能が IT インフラチームの一部のままでも、サイバーセキュリティの中心的存在だとみなすまとまった人材を特定している企業がほとんどです。



第三者の関わりがこれほど低いのはある意味驚きではありますが、ほとんどの企業がセキュリティ戦略の実行に際して内部人材を使う意向を持っていることには納得できます。組織がデジタルトランスフォーメーションを進める中で、テクノロジーとビジネスの成功の関連性が強まっていきます（このトピックについて詳しくは CompTIA の白書 Using Strategic IT for Competitive Advantage を参照）。そのようなテクノロジーのセキュリティを確実にすることが、内部人材への投資を納得させる上での（企業にとっての）コアコンピテンシーとなります。

企業が何を期待しているか、企業の規模によってアプローチは様々で、将来への方向性や機会についての思惑も鑑みられています。大企業の 3 分の 2 がサイバーセキュリティ専門チームを持っており、その中で IT 部門内にチームがある企業と報告先が別の部門である企業が半々です。専門チームが増えるにつれ、業種や企業文化によって報告系統はさらに分かれていく可能性があります。

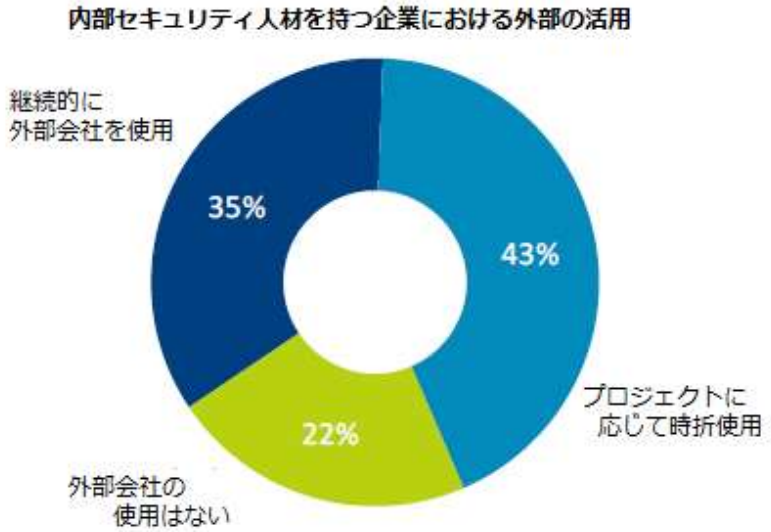
中規模企業は確かに多くの専門チームを持っています。しかし、今もなお、まず内部人材を優先する考えでいます。一般的インフラ職員をセキュリティ担当にするのは、中規模ビジネスの典型的なパターンです。ビジネスの範囲に見合う部門は設立するけれども、まだ高いレベルの専門科化と言う面では限界があります。

最も小規模の企業では、内部人材というバターンからは外れています。これらの企業はサイバーセキュリティの中心点として外部を使う傾向がはるかに高いだけでなく（中規模企業の 8%、大規模企業の 5 %に対し、26%）、社内におけるセキュリティへの注意が十分でなく、主担当を任命するほどには至っていないのです（中規模企業の 1%、大企業の 0%に対して、12%）。一見したところでは、セキュリティ問題に関して外部が主導権を取る機会に満ちているように見えます。しかしもちろん、これら小規模企業が使える予算額は最も低くなっています。

企業がサイバーセキュリティチームを構築するか否か、報告ルートを移行するか、チームを優先的に扱うかに関わらず、戦略決定を促すのは、IT オペレーションにおける変化です。過去、これらの IT 変化は新たなセキュリティの取り組みの機動力となってきましたが、それでもまだ、IT 戦術とセキュリティ転換の間にはギャップがあります。IT オペレーションの変化がセキュリティへの新たな取り組みを推進したと答えた企業は 48%しかありません。明らかに、より多数の企業がクラウドモデルやモバイルデバイスに移行しており、その両方が従来型のセキュリティへの取り組みに大幅な変化を必要とするにもかかわらず、この 48%という数値はここ何年も変わっていません。

外部人材の活用

多くの企業が、サイバーセキュリティに関連した活動に内部人材を充てることを考えていますが、外部人材は複雑性の高い分野で活躍を続けています。自社でセキュリティ人材を確保している企業のうち、78%が何らかの形で外部を使っています。外部を継続的な連携体制で使っていると企業と、プロジェクトごとに使っている企業の数は、ほぼ半々です。このことは、IT セキュリティ実装や管理に特化した企業に幅広い機会があることを示しています。



外部利用機会について企業規模による差異がほとんどないことには驚かされます。実際のところ、大規模企業ほど、セキュリティへの取り組みに際し外部の支援を使うことが多くなっています。時折のプロジェクトにおいて、外部の使用状況は一定しています。すべての企業種別において 43%です。しかし継続的事業については、中規模企業の 35%、小規模企業の 30%に対して、大企業の 39%が外部を使っています。

これらから読み取れることは明らかですが、さらに付け加えると：セキュリティ戦略の範囲は、アーキテクチャ上とオペレーション上の複雑性に直接結びつく形で広がっています。確かに、現在のテクノロジーに対するセキュリティの適正レベルを過小評価している中小/新規企業は少なくありません。その一方で、中小/新規企業の企業活動自体が小規模であることも事実です。しかしこのような企業も成長するにつれて、IT アーキテクチャの拡大や新たなオペレーション手順によって生み出されるセキュリティ脆弱性を認識する必要に迫られることになります。

セキュリティが IT 部門内で専門化されたと同様、セキュリティは IT サービスを提供する企業の間で、ひとつの小産業となっています。多くのソリューションプロバイダが、セキュリティをネットワーク管理やクラウドサービスに関連した他の業務の一要素としてではなく、一つの独立した提供業務として際立つようにしています。さらに先を行く会社もあります。IT セキュリティのみに特化するという道を選んでいるのです。こういった会社はマネージドセキュリティサービスプロバイダ（MSSP）として、知られています。このセグメントは既に十分堅牢になっているとして、Gartner 社からはこのエリアの最大企業 17 を評価する Magic Quadrant（マジッククアドランド）が出版されています。

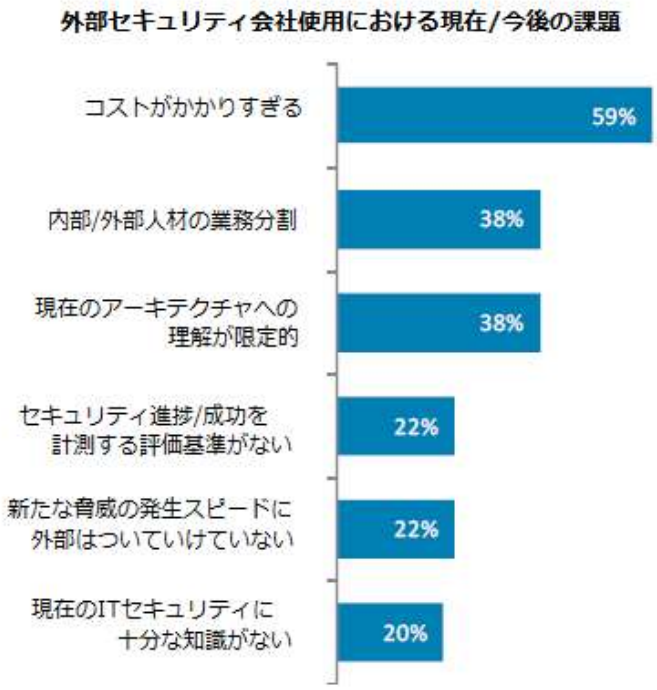
そうは言っても、MSSP はセキュリティのアウトソーシングにおいて支配的モデルではありません。セキュリティサービスに外部を使っている企業のうち、総合 IT ソリューションプロバイダを使用しているのは半数強（51%）にすぎません。さらに、38%が、IT セキュリティに関する物理的セキュリティを管理していると思われる総合セキュリティ会社を、35%が MSSP のように IT セキュリティに特化した IT セキュリ

ティ会社を、29%が、デジタルマーケティングやコンテンツ管理といった技術的ビジネスサービスを提供する会社を使っています。

これらの数字からは、企業が自社のセキュリティニーズを満たすために複数の外部会社を使用していることがわかります。加えて 50%が 2 社または 3 社のパートナーを使い、13%が 4 社以上を使っています。複数のパートナーを使用することで、高レベルの専門家が可能になりますが、同時にかなりの監視と調整が求められることになります。パートナーシップがきちんと構築されている場合もあれば、始めたばかり、という場合もあるからです。

企業が外部セキュリティ人材を使用しているか否かに関わらず、対処しなくてはならない課題がいくつかあります。第一に来るのは、外部を使うことに伴うコストです。IT オペレーションにとってコストは典型的なハードルですが、セキュリティがビジネスに投げかける問いには興味深いものがあります。セキュリティがビジネスオペレーションへの重要度を増すにつれて、セキュリティ環境がより複雑になるのであれば、セキュリティの現行のコストは以前のレベルよりも高くなって当然、という主張ができるわけです。

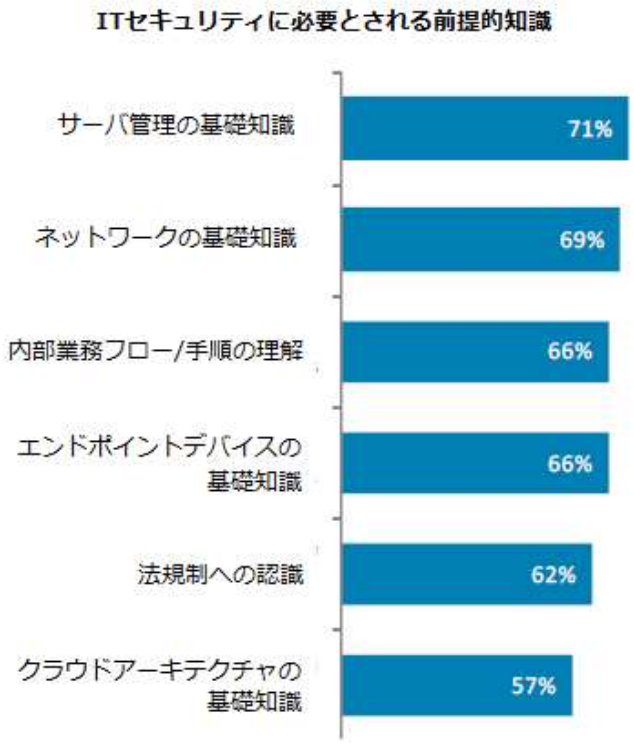
コスト以外にも、解決すべき技術的・手順的ハードルがあります。技術面では、ソリューションプロバイダはクライアントの現在のアーキテクチャへの理解を確実にする必要があります。特に、事業部が IT 部門の権限外からアプリケーションを導入しているような場合には注意が必要です。業務を分割し、異なるエリア間で調整を行う場合、その進捗と成功には継続的管理、明確な意思疎通、そして定義された評価基準が求められます。



チーム内のスキルに注目

サイバーセキュリティが IT インフラから独立したドメインになってきたために、キャリアパスとしてはどのような種別となっていくのか、という思惑も生まれています。例えば、セキュリティへの初級職務とはどのようなものなのか、と言う疑問です。従来、ほとんどのセキュリティ職務はインフラチームの延長線上と捉えられてきたからです。

今のところ、IT セキュリティの初級職務であっても、インフラにおける初級職務（ヘルプデスクのような）よりも高度なレベルとなっています。セキュリティ特有のスキルを学ぶ前に、志願者にはセキュリティ対象となる事物についての技能が必要となります。このような前提的スキル獲得はサーバーやネットワークから始めることになるでしょうが、現在の総合的セキュリティはそれ以外にも、内部の業務フローや手順、そして常に変化する規制環境といった要素も含んでいるのです。CompTIA A+のような認定で評価されたスキルをしっかりと身につけることが、サイバーセキュリティのキャリアにおける第一歩となります。



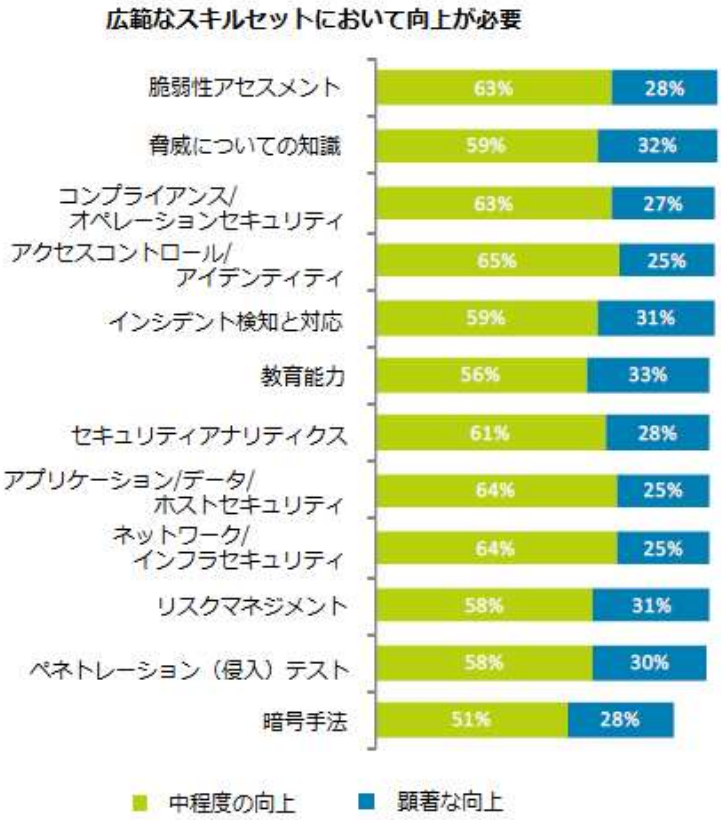
この基本的なスキルセットの上に乗るものとして、成功に寄与する広範な IT セキュリティスキルがあります。スキルの中には頻繁に使われるものも含まれています。ネットワークセキュリティ、エンドポイントセキュリティ、そして脅威への意識はセキュリティ戦略の一部となってきたスキルの一例です。それを反映するかのように、社内にセキュリティの中心チームを置いている企業は、こういった分野で強力な専門性をもつ内部人材を確保していますし、外部に中心を置いている企業はセキュリティのパートナー会社に比強力な専門性を確保しているケースが多く見られます。

スキルの積み上げということに関して言えば、クラウドやモビリティが IT オペレーションに根を下ろすにつれ、より重要になってきたスキルがあります。社内人材を活用している企業は、すでにこのようなスキルに対処し始めているかもしれませんし、一方で、既に構築されたサービス内容を売りにしている外部サービスプロバイダは新たな専門性獲得にやっきになっていることも考えられます。アクセスコントロールやアイデンティティ管理といった例を考えてみましょう。社内にセキュリティ中心担当を置いている企業 10 社のうち 8 社が、こういったスキルは社内に既にある、と感じているのに対し、外部に委託している企業では、パートナーがこういったスキルのスピードに追い付いていると感じている会社は全体の半数にも満たないのです。

最後に、セキュリティモニタリングと先手を打つ戦術の重要なスキルとして、新たに浮かび上がってきたものがあります。これらのスキルに対する理解レベルは全体としてまだ低めで、成長と機会が最も期待できるエリアとなっています。セキュリティ分析には、匿名的行動を検知するためのデータ使用も含まれており、システム内に何か脆弱性が潜んでいないかを検知する活動はペネトレーション（侵入）テストと呼

ばれています。CompTIA CySA+や CompTIA PenTest+といった新たな認定資格を活用することで、セキュリティ実施者がこれら現代のスキルにしっかり精通していることが確認できます。

企業が特定のスキルに比較的満足していたとしても、さらなる向上への意欲を持っているものです。必ずしも現在のスキルが実際に強靭だという訳ではありません。実際のスキルレベルというより、使い慣れているレベルにすぎないことが往々にしてあります。企業はネットワークセキュリティについてはかなり知識を持っているので、どのエリアを向上すべきか確実にわかっています。しかし、脆弱性評価についてはあまり知識がないため、まだまだ先は長い、ということしかわかっていないのです。

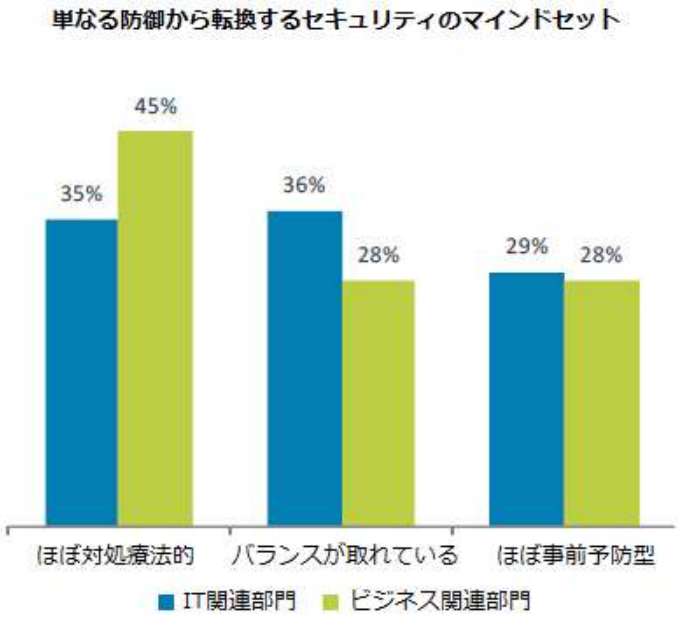


スキルギャップを埋めるため、企業はまず現在の取り組みを強化しようとします。現在の従業員を教育したり、外部の使用を拡大したりするのです。新たな人員配置や新たな外部との協力体制、といったことは次の考慮事項となり、この段階では適正なスキルが担保できているかを確認するための方法として、認定の必要性がにわかに認識されるようになります。

セキュリティチームをより効果的に

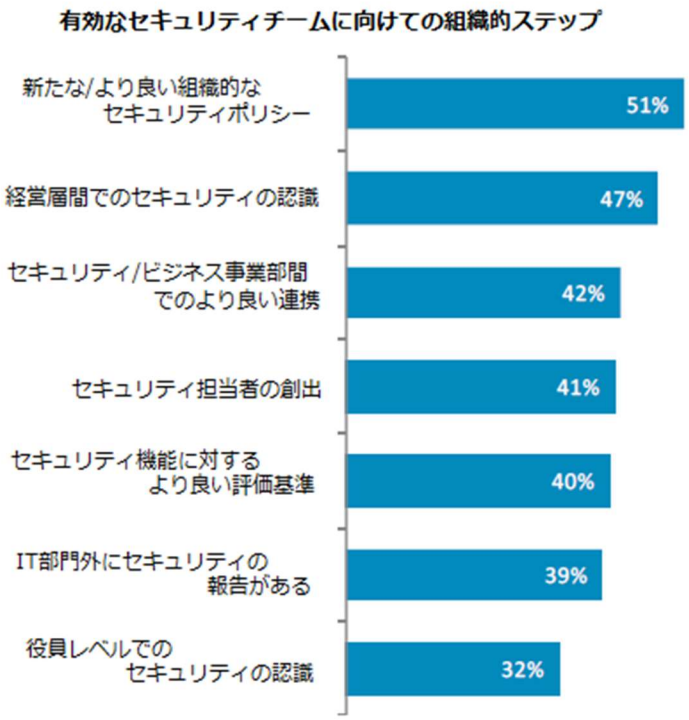
スキルを伸ばすことが、セキュリティチームの効果向上に最も直結する方法ではありますが、セキュリティチームの成功を確実にするために組織が取ることのできるステップは他にもたくさんあります。文化的視点から見ると、IT が今や、新たな考え方や行動を牽引する戦略的行動であるということへの理解もその一つです。同様に、セキュリティが独立したオペレーション機能となっているため、新たな対応や実践が必要になってきます。そして新たな考え方を組織全体に迅速に浸透させることが、セキュリティ業務の前進を後押しします。

現代のセキュリティに関して、組織としてはまず、目的はもはや理想的防御の構築ではないという理解を持つことが重要です。セキュアなパラメータの実装と維持管理は変わらず必要なタスクですが、それだけではもはや十分ではありません。クラウドコンピューティングとモバイルデバイスによって、新たなモデルを必要とする業務フローとデータストレージ技術が導入されることになります。そして攻撃が間断なく続くものであることを考えると、完全な予防は目的としてあまり意味をなさなくなってきます。このため、企業は強力なセキュリティ状況を確実にするため、より先手を打つ方法に目を向けています。



ビジネス関連部門の多くの従業員には区別できないかもしれません。彼らにとってセキュリティとは、未だに「便りがないのはいい便り」といったものなのです。IT 専門家の方が、現行のプロアクティブなステップ（先手を打つ事前予防型）を理解していますが、それでも実際にプロアクティブアプローチを重点的に行う形に移行しているケースはまだ少数派です。まだ初期段階にある、教育ニーズおよび侵害を監視する継続的ビジランス（警戒）を考慮すると、今後のセキュリティへの取り組みは、先手を打つ方策にかなり重点が置かれることになりそうです。

セキュリティが継続的活動であるという認識を持つことが重要です。なぜなら、この認識によって行動や投資への決定がなされるからです。セキュリティがどう機能するかを正しく理解することにより、組織としてセキュリティチームを強力で有能にするために必要な行動を取ることができるようになるからです。



多くの組織にとっての第一歩となるのは、セキュリティポリシーの創出もしくは変更です。新たなポリシーは新たな技術モデルの課題に対応するだけではなく、実施業務の定義づけをすることにもなり、これによってセキュリティ実践者に対して、他の従業員の行動を牽引する力を与えることになるのです。

もう一つの主要な取り組みとしては、経営層や役員、あるいはその他の経営主体でのセキュリティへの意識構築です。これは最近、IT の世界で頻繁に上がる話題ともなっています。つまり、ビジネスという観点でテクニカルな内容についての意思決定をしなければならない、ということです。テクニカルな指定事項は、ビジネス上の正当性に一致しないため、企業の成功に向けては、セキュリティ活動と投資を合わせて考慮に入れた上で、新たなセキュリティの役割を考える必要が出てきています。

合意をしっかり取る必要があるセキュリティ活動の例として、リスクアナリシスがあります。ほとんどの企業が、プロジェクト管理の枠組みにおけるリスクアナリシスのコンセプトは理解しています。しかし、セキュリティに関する厳密なりリスク管理はあまり一般的にはなっていません。ビジネスにおいて、リスクの評価はますます緻密になってきてはいますが、ソーシャルメディアやパートナー/サプライヤ関係といったエリアには、まだギャップが見られる可能性があります。

セキュリティに投資するというのは、決して新しいコンセプトではありません。投資を伸長・拡大する中で新たに加わる部分なのです。企業予算における標準的セキュリティ項目にはファイアウォールやアンチウィルスがあり、これらは今でもインフラのツールとして支配的な存在です。全組織のうち半分弱がデータ損失予防（DLP）あるいはアイデンティティとアクセス管理（IAM）を活用しています。この 2 つのツールはクラウド/モバイル環境にしっかりと根付いています。もちろん現在、技術に関する予算はセキュリティ全体予算の一部に過ぎなくなっています。特に、従業員教育はセキュリティ侵害の主要原因である人為エラーの低減に必要な要素です。

インシデント対応

多くの企業にとって現代セキュリティにおける最大の課題は、「侵害は確実に起こる」という考え方を持つ

ことです。長年にわたり、サイバーセキュリティにまつわる認識の基本となっていたのは、どのような侵害をも予防する、というものでした。侵害が起こりうるという考え方を受け入れるのは、企業がこれまで追求してきたセキュリティの目標と正反対の方向だからです。

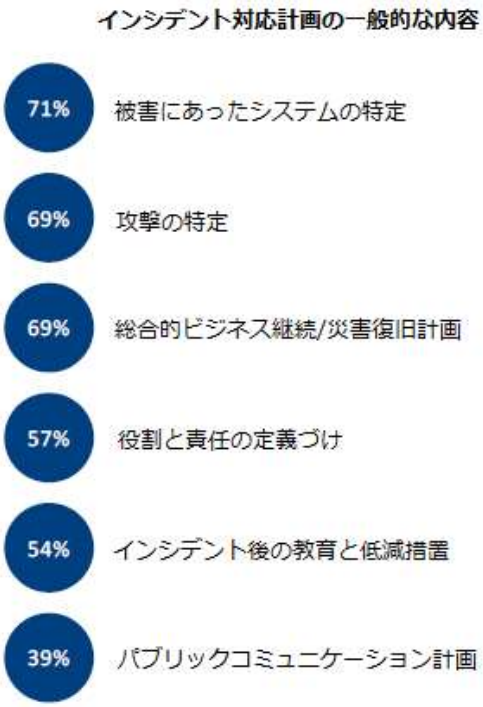
しかし前述のとおり、サイバー攻撃は大量で複雑であるため、すべてを予防するのは不可能です。セキュリティ専門家は理論上侵入不可能な防御を構築することはできるかもしれませんが、それは結果として天文学的な金額が必要になるか、現代の業務フロー上実行不可能なものになるのがオチです。率直に言って、これは常に起こってきた事象なのです。過去にセキュリティ侵害が起こっていないと考えていられたのは、防御が完全であったと言うより、全体の攻撃数が少なかったからにすぎません。正しい認識が必要なのは明らかです。セキュリティ侵害を検知する能力があってこそ、侵害について知ることができるのです。

調査の結果を見ての最大の驚きは、過去にセキュリティ侵害が全くなかったと答えた企業の数です。2015年には、34%の企業がセキュリティ侵害を近年経験したことがないとしています。今日、この数は相変わらず 33%です。サイバー攻撃の蔓延と新興技術使用による新たな脅威のリスク増加を考えると、デジタル資産に被害をもたらすフィッシング、データ漏えい、その他のインシデントに見舞われていない企業が、未だに 3 分の 1 もあるというのは、あり得ないでしょう。

この低い数値に関しては、自社で起こった侵害を深刻なものだと区分している企業の数にヒントがあるようです。2015 年、侵害があったとわかっている企業の 55%がその侵害を深刻だと区分しています。2018年にはこの数値は 46%です。調査において「深刻」の定義は回答者の解釈にゆだねられています。この点についても、企業がセキュリティ活動をどう見ているかを示唆するものとなっています。

セキュリティ侵害を認めながらもそれらを「深刻ではない」と区分している企業が増えているということは、侵害の中にはデジタルビジネスの一般的な項目として対処されているものがあることを示唆しています。しかし、それらを侵害だと認識しているということは、何らかの低減策が取られていることも示しています。セキュリティ侵害がなかったと考えている企業についても、データ損失やデバイスの紛失などは業務内で目にしているかもしれません。しかしそれらを一過性のインシデントとして扱うことで、根本原因への対処がされず、より根深い被害が起こっているかもしれないというリスクが高まってしまいます。

セキュリティ侵害がほぼ確実に起こるという認識を受け入れたら、次のステップは、侵害が検知された際にどのような対応をするかを決めることです。企業の 3 分の 2 がインシデント検知と対応について公式なポリシーと手順があり、これらのポリシーと手順は文書化されて組織内に徹底されていると述べています。これは健全な基盤のように思えますが、実情はこれより不安定であることを示す別のデータもあります。まず、IT 部門とビジネス部門の間に大きな相違があります。75%の IT 従業員が公式なインシデント対応がなされていると考えているのに対し、ビジネス関係の従業員では 45%となっています。さらに、公式/非公式な計画を持っている企業の中で、その計画が非常に有効だと考えている会社は 33%しかありません。

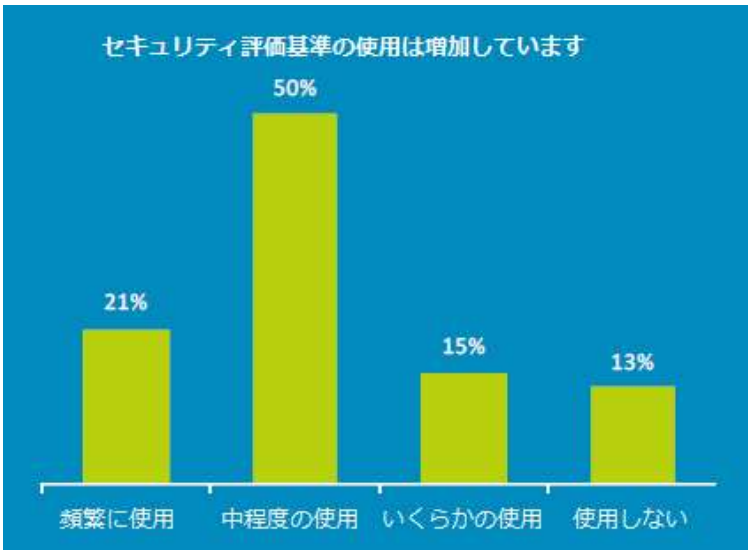


すでに何らかの正式なインシデント対応計画を実行している企業を見ると、その計画項目の違いが目につきます。最も一般的な項目は技術的なものです。被害にあったシステムの特定、攻撃種類の特定、そしてしっかりした BC/DR（ビジネス継続/災害復興）計画です。組織内の異なる部分に踏み込んだ計画要素は少し異なってきます。おそらくもっとも悩ましいのは、パブリックコミュニケーション計画を持っている企業が少ないことでしょう。セキュリティ侵害そのもの、あるいは侵害が起こったときに多くの企業しがちな、外部への誤った対応によってもたらされる風評被害を考えると、このエリアが全体のセキュリティへの取り組み姿勢の向上だけではなく、部門横断的なコミュニケーションを推進するものあることがわかります。

今日の状況における脅威の種類を理解する必要性も高まっています。多種多様なインシデントについての理解が十分でないと、インシデント対応の効果も限られたものになってしまいます。企業がもっと知りたいと思うような最も一般的な脅威というのは、過去から長いこと続いていたり、新聞の紙面を賑わしたりするようなものです。多くの企業が筆頭に上げるのは、スパイウェア、フィッシング、ランサムウェア、そしてウィルスです。確かに、これらの攻撃は常に進化しているので、無視することはできません。しかしながら、他にも異なった攻撃方法をする多くの脅威があり、もっと優先して対応をすべきなのです。ソーシャルエンジニアリング、IoT ベースの攻撃、SQL インジェクション、そして DDos 攻撃。これらはすべて、接続されたデジタル環境で起こりがちなもので、これらの脅威を十分理解していないと、悲惨な結末を迎えることになります。

セキュリティ評価基準の設定

セキュリティチームが取るべき最も重要な行動は、効果を計測し、オペレーションの指針となる評価基準の設定です。多くのサイバーセキュリティコンセプトに見られるように、評価基準は劇的な変化をとげつつあるエリアです。ファイアウォールやアンチウィルスソフトのインストールだけでセキュリティ対応をしている環境では、評価基準はそれに対応して単純なものになります。つまり、セキュリティ侵害はゼロ、ということになってしまうのです。セキュリティ対応がもっと複雑な環境では ― もちろんコストが上がるのは不可避ですが ― 対応の効果や投資についてもっときちんとした測定ができるはずです。



自社のセキュリティ活動において評価基準を頻繁に使用していると報告しているのは 5 社に 1 社しかありません。予想にたがわず、頻繁な使用は大規模企業に多く見られます。頻繁に使用していると回答した率は、中規模企業で 20%、小規模企業で 17%だったのに対し、大規模企業では 26%となっています。大企業には人材が豊富にあり、セキュリティ実施を最先端の方法で行おうとしている実情を考えると、評価基準にもっと力を入れていると思いそうなものですが、結果として企業規模間でさほど大きな数値の差が見られないのは、ある意味驚きです。

実際、中規模企業はこの分野に関して、より詳細に検討しているようです。中程度の使用率は大規模企業で 43%、小規模企業では 43%だったのに比べて、中規模企業では 61%にのぼっています。中規模企業はこの新興分野でスイートスポットにいるのかもしれません。大規模企業ほどの人材プールはありませんが、中規模企業の人材はフットワークが軽く、新たなニーズに対して新たな活動を設定する機会に恵まれています。中規模企業における IT 専門家とその企業と協働しているソリューションプロバイダにとって、セキュリティ評価基準を導入しやすい環境であると言えます。

評価基準の検討は、IT 界で発生している多くの検討課題を反映していると言えます。ビジネスのあらゆる部分を統合する素晴らしい機会を与えてくれるものなのです。実現すれば、役員レベルから様々な管理職レベル、そして日々のセキュリティ業務を実施している従業員に至るまで、設定された目標に対する適正な評価基準や進捗確認をする権利を持つことになります。セキュリティ専門家としては、ビジネス目標に鑑みたセキュリティ活動に対応して評価基準になっていることを確実にすべく、さまざまなレベルの人たちとうまくコミュニケーションをとる力を身につけることが必要となるでしょう。

評価基準に関与している組織内部門

	基準の設定	基準の見直し
IT部門	73%	57%
いくつかの事業部	43%	50%
中級管理層	48%	54%
上級管理者	47%	52%
役員会	30%	38%

どの評価基準を使用するかについては、企業が自社のセキュリティ対応に使用を検討している評価基準は多岐にわたっています。セキュリティのすべての側面をカバーする評価基準を確実に選ぶことが、最も重要な指針となります。テクニカルな評価基準（異常フラッグが立ったネットワークトラフィックの割合など）もあれば、コンプライアンス評価基準（成功した監査数など）もあります。従業員の評価基準（セキュリティトレーニング修了者の割合など）やパートナー評価基準（セキュリティ言語についての外部契約数など）もあります。どの組織にも当てはまるような完璧なリストはありませんが、堅牢な一連の評価基準によって、包括的取り組みが可能になるのです。

セキュリティ評価基準とセキュリティチーム設立は相互補完的な活動と言えるでしょう。企業が評価基準をあまり使用しない理由は、特定業務にフォーカスしたチーム立ち上げる理由にもなるのです。何よりも、企業としては単純に評価基準をトラッキングする人材の不足を挙げています。セキュリティ部門が他のインフラ活動も含む複数任務を担当している場合、さらに複雑かつ繊細な業務を追加することは難しいのでしょう。それ以上に、企業は自社の評価基準を検証する適正レベルのスキルを決めかねていますし、そもそも適切な評価基準選びに自信がないという現状があります。改めてまとめると、特定業務にフォーカスした人材、もしくは外部が適切なスキルセットを導入もしくは構築し、社内あるいは特定の会社に合うよう調整した評価基準セットにも力を注ぐことができる、ということです。

サイバーセキュリティは今日、企業における優先度がさらに高くなっているだけではありません。独特の扱いをしなくてはならない重要な機能でもあります。セキュリティチーム創設は、短期的に見ればどの企業にとっても正しい決定でしょう。しかし、あらゆる点から見て、セキュリティは最終的には内部と外部の人材を活用して戦略を立て、戦略を実行し、評価基準を管理するという総合力での取り組みになってくと考えられます。セキュリティチームの形状は、ビジネス規模やセキュリティ要件によってさまざまでしょう。しかし、どのような形状であれ、その核となる要素は変わりません。スキルのさらなる専門化、より広範な方法によるアプローチ、そしてサーバーセキュリティとビジネスの成功をさらに結びつけるということなのです。

本リサーチについて

定量的調査は 2 度のオンラインサーベイから成ります。初回は、2018 年 7 月/8 月にワークフォースに関連するプロフェッショナルが対象で、米国にベースを置く総計 402 の企業が参加し、全体のサンプリング誤差プロキシが 95%、信頼度数+/-5.0 パーセントポイントとなりました。2 度目は、2018 年 5 月に実施。米国にベースを置く総数 478 の企業が参加し、全体のサンプリング誤差プロキシが 95%、信頼度数+/-4.6%でした。サンプリング誤差は、データの亜郡の方が大きくなっています。

どの調査においてもそうであるように、サンプリング誤差は起こり得る誤差原因の一つに過ぎません。非サンプリング誤差を正確に計算するこができないため、その影響を最低限に抑えるべく調査設計、データ収集および処理のあらゆる段階において注意深い手順が踏まれています。

すべての内容と分析に関して CompTIA がその責を負います。この調査に関する質問はすべて CompTIA リサーチ&マーケティングインテリジェンスのスタッフ research@comptia.org が受け付けます。CompTIA は、市場リサーチ業界の Insights Association の会員であり、国際的に認められた標準規範を厳守しています。

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 の学校機関あたは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。