CompTIA

RESEARCH REPORT

MARCH 2015

Trends in IT Security

IT セキュリティ動向調査　2015

調査について

CompTIA の「Trend in Information Security（情報セキュリティ動向）」調査は、企業が新しい技術を使用するにあたっての、IT セキュリティに伴う行動、テクニックそして機会についての知見を提供するものです。調査は 5 つのセクションからなっており、報告書全体において、章ごとにも、総括的にも見ることができます。

セクション１：市場概要
セクション２：課題
セクション３：使用パターン
セクション４：人員的観点
セクション５：チャネルダイナミクス

この調査は３つのパートで行われました。
パート１：一般的なセキュリティ問題に焦点を当てたオンライン調査。2015 年 1 月に、企業幹部（ビジネスエグゼクティブ）およびテクノロジープロフェッショナルを対象に行われました。アメリカ合衆国に拠点を置く全 400 社が参加しました。サンプリング誤差の全体的マージンは 95%、確実性は+/-5.0%ポイントです。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。

パート２：セキュリティトレーニング問題に焦点を当てたオンライン調査。2015 年 1 月に、企業幹部（ビジネスエグゼクティブ）およびテクノロジープロフェッショナルを対象に行われました。アメリカ合衆国に拠点を置く全 300 社が参加しました。サンプリング誤差の全体的マージンは 95%、確実性は+/-5.8%ポイントです。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。

パート３：セキュリティ提供に焦点を当てたオンライン調査。2014 年 10 月に、IT チャネルの幹部（エグゼクティブ）およびプロフェッショナルを対象に行われました。アメリカ合衆国に拠点を置く全 291 社が参加しました。サンプリング誤差の全体的マージンは 95%、確実性は+/-5.9%ポイントです。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。

どの調査でもそうですが、サンプリング誤差は唯一の誤差計測ソースです。非サンプリング誤差を正確に計測することはできませんが、調査設計、データの収集および処理のすべての段階において予防措置を取ることで、その影響を最小限に抑えました。CompTIA は全内容および分析に責任を負います。調査に関しての質問はどんなものでも、CompTIA Research and Market Intelligence のスタッフ reseach@comptia.org までご連絡ください。CompTIA は Marketing Research Association (MRA)の一員であり、MRA の市場調査倫理・基準規定を順守しています。

SECTION 1:

Market Overview

セクション１：市場概要

所見

- IT セキュリティは常に重要な分野でしたが、ビジネスがデジタル処理への依存度を強めるに従い、さらに重要度を増しています。この分野はまた、健全な成長を見せています。Gartner 社によると、全世界セキュリティの 2014 年末の推定歳入は 711 億ドルとなっています。
- 様々な脅威に関する懸念レベルは、伝統的な考え方と将来への新たな行動へのニーズの両方を反映しています。マルウェアとハッキングはいまだに懸念を起こさせる脅威のトップに位置づいており、企業の約半数がこれらを深刻な懸念であると言っています。ソーシャルエンジニアリングや人為的エラーをいった他のエリアも懸念事項として増えてはいますが、それらがもたらす真の影響や、抑制戦略を理解するための教育がまだ必要な段階にあるようです。
- セキュリティの重要性を強調するのは、セキュリティ議論における最良の方法とは言えません。ほとんどの企業において、セキュリティが重要だという点はすでに了承済みだからです。その代わりに、様々な組織でセキュリティを変えるきっかけとなった他の行動に焦点を当てるべきでしょう。例えば、

新たな IT 運用(47%)やトレーニングから得られた知識(34%)などです。

IT セキュリティ市場

IT を取り巻く状況はこの 5 年で劇的な変遷を遂げました。企業は、クラウドコンピューティングやモビリティといった新たなモデルを探索しているだけではなく、成長を直接加速させる戦略的試みにも目を向けているのです。これら 2 つの傾向は多少、相互に補完するものではありますが、企業がその IT 戦略を考える際、両方を同時に追求していくと、さらに複雑な様相を生み出すであろうことは明白です。

このような環境において、IT セキュリティは以前にも増して際立ったものとなってきました。テクノロジー追求における二つの点が、セキュリティに対する最悪の事態を生み出します。それは、新たなモデルには、悪用されかねない新たな抜け穴があるということ。そして、テクノロジー依存の高まりとともに、混乱の可能性が高まるという点です。プライバシーについての懸念や、重要な規制上の懸念の高まりも考慮すると、IT セキュリティが単なるファイアウォールやアンチウィルスソフトウェアを超えて、どれほど広大なものになっているかは容易に理解できます。

事実、セキュリティは IT に埋め込まれた機能としてではなく、それ自体、ひとつの領域になりつつあるというもっともな説もあります。これは、最高セキュリティ責任者(CSO)または最高情報セキュリティ責任者(CISO)という役職者を擁する大規模企業ですでに起きていることですし、このような役職者の 75%が 2018 年までには直接 CEO に報告を挙げることになる、という IDC の予測からも、領域として完成されつつある動きが見て取れます。この考え方は次第に、中規模、小規模ビジネスへと浸透していくでしょう。そこでは、セキュリティの専門家を導入するか、この分野に特化した第三者との協業を行うことになると考えられます。

セキュリティ「CIA」の変化

IT セキュリティは常に複雑な分野とされています。以下は、組織のアプローチとして、従来定義される 3 分野です。各分野の簡単な概要を見ると、どのように複雑化しているのかが分かります。

- Confidentiality（機密性）：過去においては、データの機密保持といった際、セキュアペリメーターによる制御・保護という措置が取られていました。しかしモバイルデバイスが普及した今日では、セキュアペリメーターそのものを不可能にしてしまいます。企業は、より詳細なレベルでデータ保護について検討しなければなりません。
- Integrity（完全性）：一貫したデータセットの保持は効率性および高度解析において重要とされます。企業がビッグデータの機会を模索していくなかで、多くのデータサイロが存在するということが分かりました。新しいデータは絶え間なく伝送されますが、それらは適切に整備管理される必要があります。
- Availability（可用性）：社内システムとともに、企業はリダンダンシー（冗長性）の確立および故障対応がさらに可能となりました。システムをクラウドプロバイダに移すには、リダンダンシーの全面的な再考が必要となり、それと同時に、要求されるシステムアップタイムという課題に取り組まなければなりません。

企業がスキルを導入して、自社チームを作り上げようとしていることは確かです。仕事の情報収集・提供をしている Burning Glass を見ると、情報セキュリティアナリストへの求人票数は、2013 年の第 4 四半期から 2014 年の第 4 四半期の間に 73%増加しています。仕事自体の母数は他の技術分野ほど多くはありませんが、Burning Glass の全カテゴリを通してみても、他を大きく引き離して一番の成長率です。さらに、労働統計局によると、情報セキュリティアナリストは最も成長の早い業務カテゴリになり、その全体成長率は 2012 年から 2022 年の間において、37%と予測されています。

世界的な支出推定は、想像する以上にセキュリティが成長エリアであることを示す、もう一つの指標です。Gartner 社の世界セキュリティ支出推定値は 2014 年には 711 億ドルに達しました。これは 2013 年から 7.9%の増加です。Gartner 社予測による IT 全体の支出が 2015 年に 2.4%の成長であることと比較すると、セキュリティが IT 諸要素の中の単なる共有項ではないということは明白です。セキュリティエコシステムの各パートについての予測が MarketsandMarkets によって出されていますが、そこでは、幅広いセキュリティの取り組みの中で、どれほど多くの活動が行われているかが示されています。

- アイデンティティアクセス管理（IAM）：2019 年までに 183 億ドル
- フィジカル（物理）アクセスコントロール：2020 年までに 104 億ドル
- エンタープライズ・ファイアウォール市場：2019 年までに 84 億ドル
- モバイルセキュリティ市場：2019 年までに 59 億ドル
- 暗号化ソフトウェア：2019 年までに 48 億ドル
- データセンター・ロジカル（論理）セキュリティ：2019 年までに 32 億ドル

企業が自社のセキュリティへの取り組みに関して考慮すべ事項の複雑性は、実際に起こっている攻撃の複雑性に直結しています。新たなテクノロジーモデル、新たなビヘイビア、そして新たなモチベーションによって、攻撃側は多くの新しい方法を活用してのデータを窃盗、あるいはオペレーションの混乱を引き起こしているのです。

セキュリティ脅威に対する懸念レベル

	懸念レベル		懸念の変化	
	中程度	深刻である	以前と変わらない/以前よりクリティカルではない	これまでにも増してクリティカルである
マルウェア	37%	50%	51%	49%
ハッキング	38%	49%	54%	46%
プライバシー	36%	45%	62%	38%
データロス/漏えい	42%	40%	66%	34%
ソーシャルエンジニアリング/フィッシング	41%	38%	58%	42%
新分野のリスクに対する理解	43%	36%	61%	39%
予算/サポートの不足	34%	34%	72%	28%
物理セキュリティ	42%	33%	71%	29%
企業コンプライアンス	37%	32%	75%	25%
内部者による権限乱用	35%	31%	75%	25%
一般スタッフ間の人為的エラー	52%	30%	74%	26%
ポリシー強制	38%	29%	74%	26%
正式なリスクアセスメント	46%	28%	73%	27%
ITスタッフ間の人為的エラー	41%	27%	80%	20%

Source: CompTIA's Trends in Information Security study | Base: 400 U.S. end users

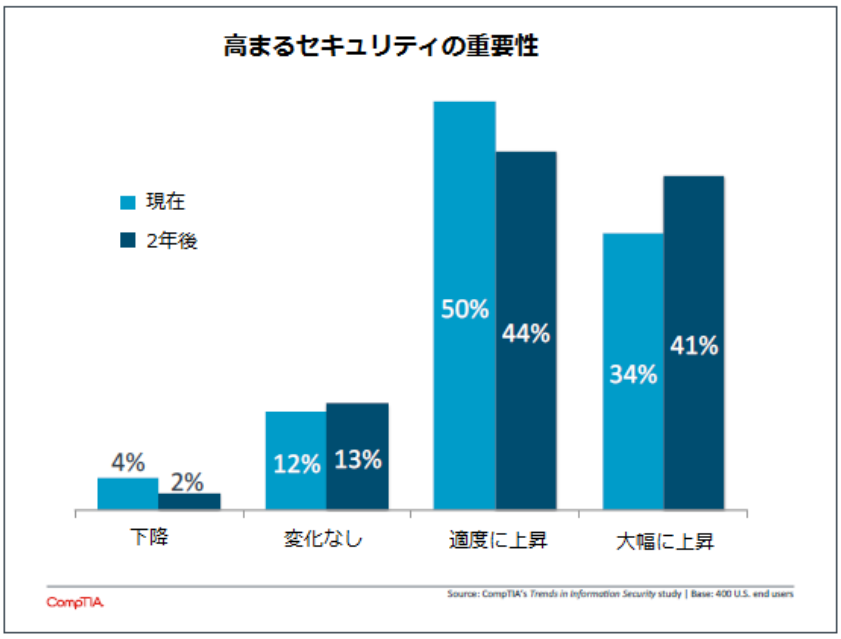
さまざまな脅威に対して示される懸念レベルは、これまでの考え方と将来の新たな行動へのニーズ、両方を反映しています。マルウェアとハッキングが懸念の中でトップのエリアです。これらは非常に伝統的な重点分野であり、確かに両方とも今日、大量に起こっているものです。セキュリティ企業 PandaLabs による直近の四半期概要報告書では、2014 年第 3 四半期だけで、2000 万もの新型マルウェアが作られたと推定されています。

しかしながら、この 2 つのエリア以外でもほぼ同レベルの懸念を喚起する、非常に多くの脅威が存在しています。フィジカルセキュリティは、モバイルデバイスが窃盗の対象となることが増えるに従い、より重要になってきています。インターネット経由で行われるビジネスの増加に伴って、コンプライアンスはさらに多くの企業で重要な役割を果たすようになっています。重要な懸念という意味では、人為的エラーのランクは低くなっていますが、企業からは、これがセキュリティ侵害の裏にある最も大きな要因であると報告が上がっています（さらなる詳細はセクション 4 を参照）。

すべての混沌のなかには肯定的な面もあります。2013 年のデータと比較したところ、マルウェア以外の全項目において、「深刻である」と評価した企業の割合が上昇していた点です。これは、企業が強固なセキュリティ体制を構築することの難しさを認識し始めているということを意味しています。ここで問われるのが、そうした状況を受け、彼らがどう行動に移すのか、です。

変化へのモチベーション

セキュリティがビジネスの最大懸念であると改めて言う必要はありません。IT セキュリティは IT 機能の誕生とともに存在し続けてきましたし、ほとんどの企業が、それが軽々に捉えるものではないことを理解しています。実際、CompTIA の調査において 74%の企業が、セキュリティは 2 年前よりも今日の方が高い優先度にあると言っており、85%が、今から 2 年後にはさらに高い優先度になるだろうと言っています。これらの結果は、企業の規模に関わらず、比較的一貫しています。実際、中規模企業においてはセキュリティの優先度がより高い傾向にありますが、これは企業活動が成長するにつれてセキュリティの改革が求められることに起因すると考えられます。

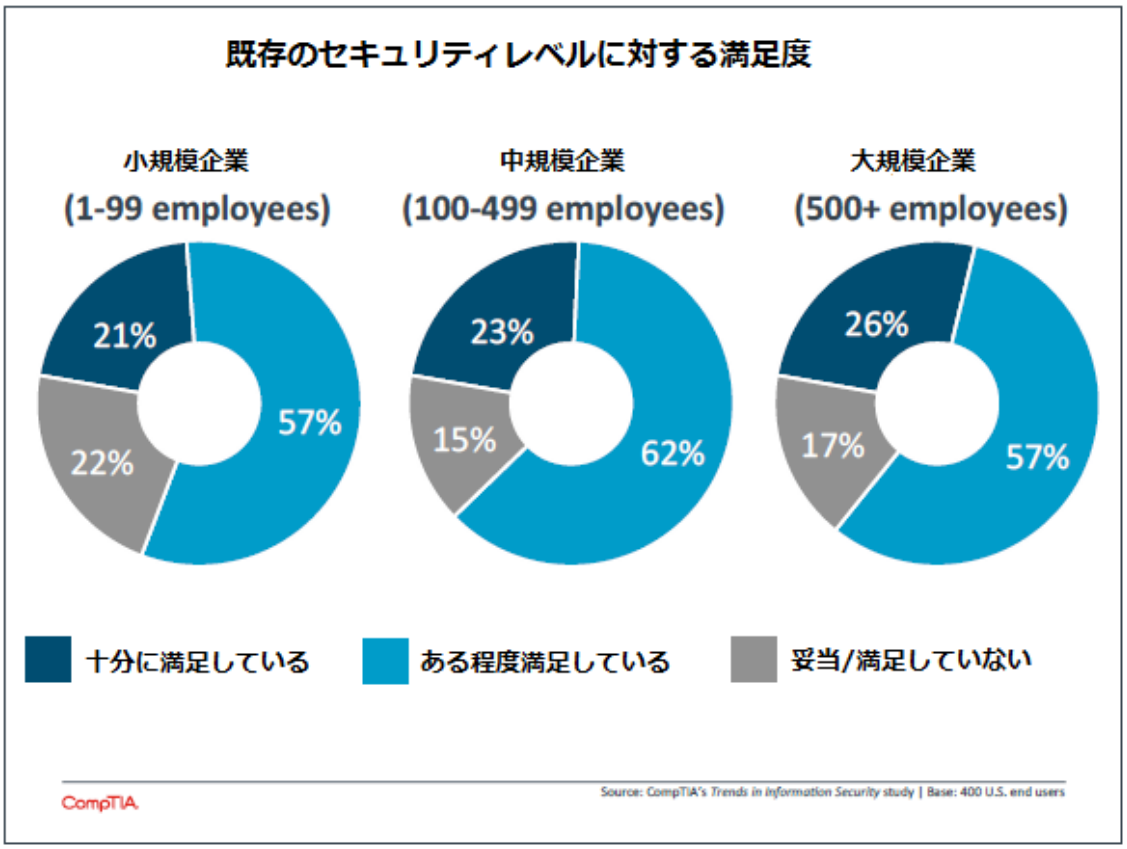


セキュリティを最高優先事項として討議する上での課題として、優先度をつけることと、どのような行動を取るべきかを知っていることは違う、という点があります。過去 2 年間に起こった大規模セキュリティ侵害を考えてみましょう。Target、Home Depot、eBay、JP モルガン・チェイス、そして Anthem はすべてセキュリティに高い優先度を置いていたと思われます。しかし、それでも各企業で 5000 万件以上の記録が盗難、という事態をもたらすような欠陥があったのです。さらに、これらの欠陥は新たなテクノロジーへの移行の結果ではありませんでした。むしろ大抵が、セキュリティ危険区域としてよく知られたエリアにおける習慣的なミスだったのです。

どのような行動をとるべきかを知るための最初のステップは、そのような行動の必要性を認識することです。企業はセキュリティを最高優先事項として強力に位置付けてはいますが、同時に、自社の現在のセキュリティが十分であるという感覚を強く持っています。企業の規模に関わらず、この所感は比較的一貫しており、何らかの形で自社の現在のセキュリティは単に適切なレベルである、あるいは不十分であると感じている企業は少数です。

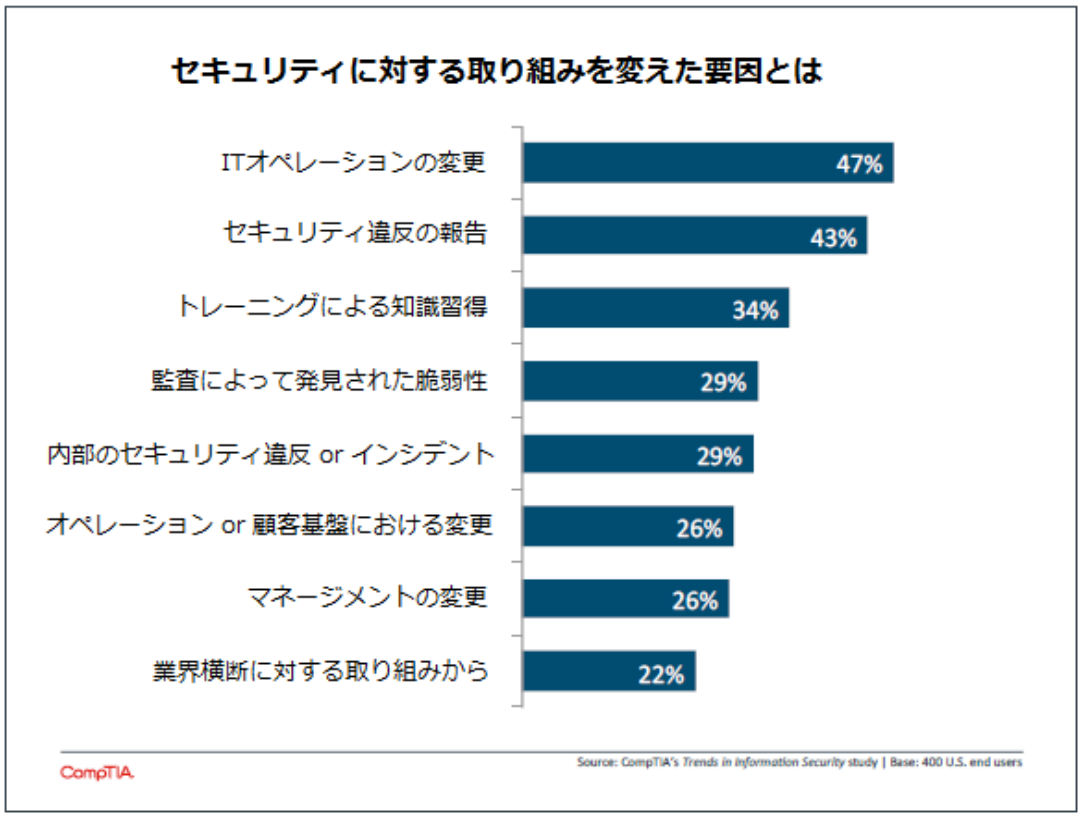
中規模企業は、自社の既存セキュリティレベルに最も自信を持っています。中規模企業が自社セキュリティ向上のために、必要な予防措置を取っている場合もあります。しかし多くの場合、中規模企業は、自社

データの重要性を大規模企業との相関で考えると脅威レベルは低いため、自社セキュリティは十分だと信じきっているようです。現実には、SMB スペースでの攻撃はエンタープライズスペースと同じ頻度で起こっています。この理由は、データの価値というよりは、むしろ防御の弱さからです。



そのため、企業がセキュリティの重要性を納得する必要がある、という状況にはありません。むしろ彼らに必要なのは、自社の現時点でのセキュリティへの取り組みが、自らを危険にさらしている可能性があることを納得することです。セキュリティ向上への最も一般的な契機は、組織内におけるセキュリティ違反の発生です。しかしながら、自社が適正な位置にいると信じている企業にとって、効果的なチェックリストとしての役割を果たすような、他の契機もあります。

クラウドとモビリティがプロセスと IT アーキテクチャにこれほど劇的な変化をもたらしていることを考えると、IT オペレーションの変更が最も一般的な契機であっても驚くには値しません。むしろ、調査対象である企業の中で、これを推進力だと報告しているのは半数に満たないということの方に驚きます。クラウドとモバイルソリューションの導入数値はこれよりもはるかに高いのです。そのため、新しい IT 戦略がどのような新たなセキュリティ問題を生み出すのかを考えている企業が、もっと多くあってしかるべきなのです。



セキュリティトレーニングは多くの企業にとって主要な取り組みとなってきていますが、その理由は 2 つあります。技術チームがダイナミック環境の速度に歩調を合わせていられるようにするため、そして一般職員が日々の業務で技術を使う際に、不要なリスクを生まないようにするためです。また、企業の 3 分の 1 が付加的な利点を見出しています。それは、実施しているトレーニングが、組織の意識改革をもたらす新たな知識につながっていくということです。

最後の契機として特筆すべきは、外部監査によって発見された何らかの脆弱性です。監査を外部に依頼するというのは、多くの企業が考えていない行為かもしれませんが、これが近い将来、多くのビジネスにとってのベストプラクティス（最優良事例）となると信じるに値する理由があるのです。委託された監査企業は、特化した専門性と偏りのない精密な調査を提供しますし、監査では、セキュリティ即応性を判断するベースライン（多くの監査企業がセキュリティインシデントの有無について基礎とする測定基準）を提供するでしょう。

IT 機能が、クラウドやモビリティの導入に続く新たな段階に入る際、IT セキュリティは重大な岐路に立つことになります。多くの IT オブザーバーとアナリスト(CompTIA を含みます)が、2015 年は IT セキュリティが変化を遂げる年になると予測しています。技術方式から内部プロセス、そして組織のトレーニングに至るまで、この変化が起こりうる道は何通りもありますし、IT 企業がその顧客にサービス提供する新しい方法を探すことのできるエリアも数多くあります。

SECTION 2:

Challenges

セクション２：課題

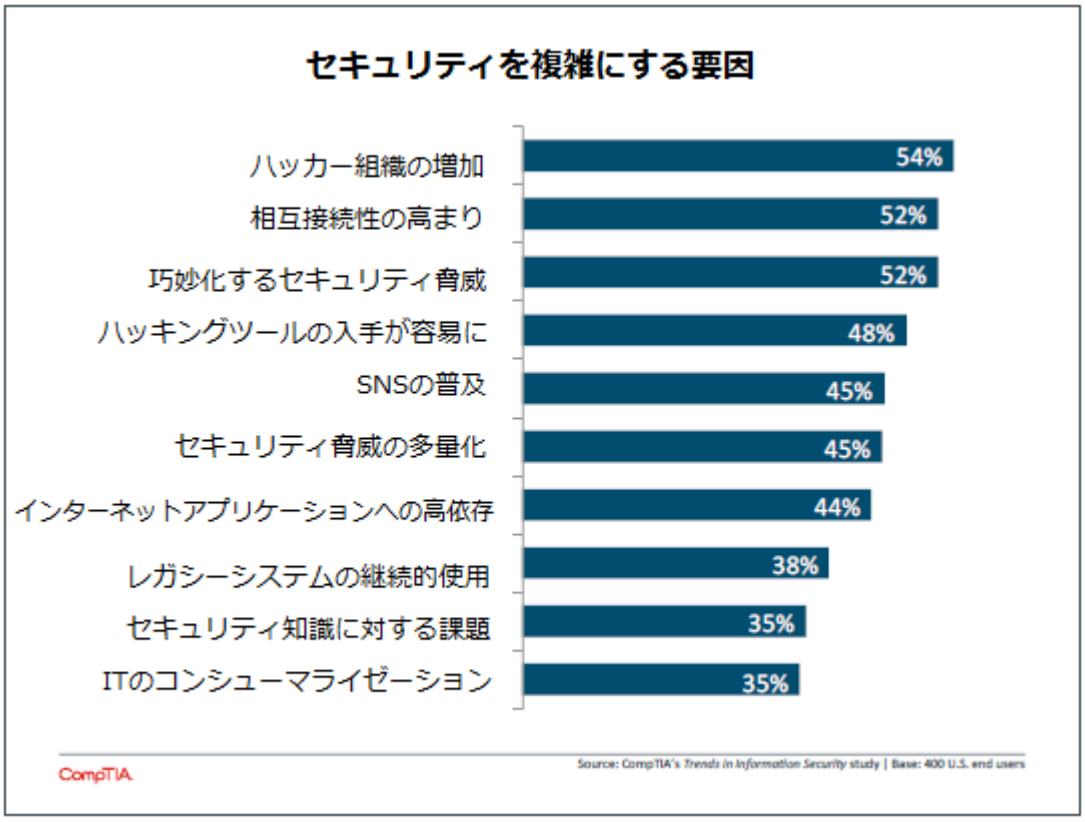
所見

- 複雑化するセキュリティには多くの要因が寄与しています。これらの要因には、外部的なもの（例：ハッカー組織の増加）と内部的なもの（例：システムやデバイスの相互接続性の向上)の両方があります。古いアプローチではこうした複雑性に対処できないことから、企業は新たな取り組みを考え始めなければなりません。
- データはおそらく、セキュリティの考え方を変えるべき主要エリアでしょう。データは、今や企業のセキュアペリメーター外に日常的に出ていくものだからです。29%の企業が、昨年にデータロスを経験したと報告しています。この数値は 2013 年の 19%からの上昇となります。
- クラウドコンピューティングに移行する企業が増える中、クラウドプロバイダに関するより綿密な検討が必要となります。多くの企業は、自社のセキュリティベースラインを十分に理解していないようですが、これは、クラウドプロバイダがセキュリティ面で何を提供しているかを理解する前にされるべきことです。

・ 企業が防ごうとしているモバイルセキュリティインシデントは、もはやデバイス紛失だけではありません。昨年、企業では、社員の「モバイルデバイス上のセキュリティ機能の無効化（31%）」や「モバイルマルウェア被害（30%）」といった事象が確認されています。

複雑なセキュリティ状況

セキュリティへの取り組みをいかに変えていくかを考えるにあたって、企業は非常に多くの要因を考慮に入れなければなりません。企業が新たなテクノロジー活用を考え、攻撃者が新たな手法を用いていることにより、新たな影響因子がセキュリティを形作っているのです。全体の中で、どれか一つが、主要要因として突出しているわけではないことから、新たな戦術を作る際には、全体の様子を幅広く考慮することがとても大切であることが分かります。



ハッカー組織とハッキングツールの増加は、企業の懸念となる二つの要素をもたらします。第一に、攻撃が、素早い変化と蓄えた資源による高い効率性を持ち、さらに動的になりうること。第二に、攻撃には新たなモチベーションが加わること。政治的集団や無作為なトラブルメーカーが、包括的な技術スキルを持つ必要もなく、大混乱を引き起こすことができるからです。これら２つの懸念はどちらも、SMB にとってより深刻となります。SMB は問題に対処する自社の資源が他より少なく、また、防御力が比較的低いため、標的となる可能性が高まっていることに気付くでしょう。

防御を進める上で、既存のインフラとスキルが障害となります。レガシーシステムは、ペリメーターセキュリティの観念に依存しており、クラウド環境に移行するには適切な候補とはいえません。セキュリティスキルも、企業の現在の設定に照準を合わせたものである可能性が高く、また、これらのスキルは、組織全体に広がっているというよりも、IT 機能に集中していることが多いのです。事業部門はこのような制約を最も強く感じています。新たなテクノロジーの探索に積極的に取り組みたいと思ってはいるものの、安全を担保するための適切なスキルを部門内でまだ持っていないのが現状です。

攻撃者の能力の変化と、既存構成の変化に伴う懸念以上に、セキュリティにおける複雑性は、企業が探索している新たなテクノロジーに拠るところが大きいといえます。デバイスやユーザーの相互接続性は、モビリティへの取り組みの結果です。ソーシャルネットワークの普及により、潜在的な違反のプラットフォームが生まれ、そして、意図せぬ漏えいにつながりかねない情報共有という新たな意識が生み出されました。インターネットアプリへの依存拡大は、より大きな機動性（アジリティ）を追求するクラウドプロバイダへと、システムが移行した結果に他なりません。これらの新たなテクノロジーには、確かに大きな可能性がありますが、活用する前に素早く解決しなければならない問題も生み出すのです。

企業は、導入している新しいビジネステクノロジーに合わせたセキュリティ技術を導入しているように思われるでしょう。しかし、Data Loss Prevention (DLP) は、いまだに最も一般的な新ツールの一つで、企業の 58%で現在使用されています。アイデンティティアクセス管理 (IAM)と、Security Information and Event Management (SIEM) は、どちらも 2013 年以来、かなりの飛躍を遂げました。IAM の採択は 47%から 57%へ、SIEM の採択は 37%から 49%へと増加しています。

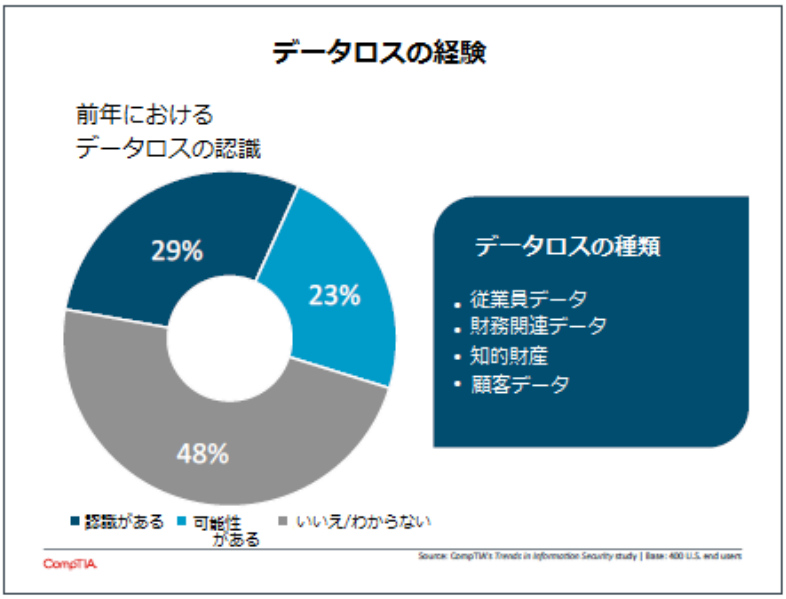
データへの着目

セキュリティ向上を実現するために必要とされるマインドセットには、データの「見方」と「扱い方」に対する変換が必要となります。単純な比較で言うと、自社システムとアプリのすべてを自社ファイアウォールの下で維持管理していた企業は、データをこれらシステムの単なる副産物と見なしていましたし、システムが強力なペリメーターで安全に保たれてさえいれば、データも安全だったのです。

今日のデータは、企業の物理的・仮想的境界線を簡単に超えて出ていきます。システムをクラウドプロバイダに移行することは、明らかにデータを外部管理のもとに移す、ということになります。そしてモバイルデバイスは、バックエンドシステムが社内にあったとしても、データを運び出す可能性を持っているものです。このことにより、データそのものを守る必要性が出てきます。データがいろいろな状況 (非使用中、移動中、使用中)に置かれることになるにつれ、タスクはさらに複雑になります。

企業がデータ中心の考え方に移行していく中、自社のデータ実務を向上させる必要性に気付くことがしば

しばあります。調査の結果、企業では、データのサイロ化が多発していることが分かりました。これは実際、企業が自社のデータがどのように保管され管理されているかに着目したことで明確になったのです。このようなサイロ型業務によって、包括的な分析が難しくなるだけでなく、どのようなデータがあるのかを把握したり、一元的な顧客状況を取り出したりすることが困難になります。



2013 年と比較すると、より多くの企業がデータロスのインシデントを確認しています。2 年前には、企業の 56%が、「データロスはなかった」あるいは「データロスの有無が分からない」と報告していました。さらに当時、前年におけるデータロスまたは漏えいを確実に認知していると言ったのは、企業のわずか19%に過ぎませんでした。データをより注視することで、データのサイロ化への認識が高まるのと同時に、どの時点でデータが危険にさらされたのかへの意識もより向上するのです。かなりの大差で、小規模企業はデータロスへの認知が低いことから注視レベルが比較的低いことを表しています。小規模企業がデータロスの危険にさらされる可能性を減少させるためには、データに基づくどのような取り組みにおいても、データ監査から始めるのがよいでしょう。

従業員データが最も喪失されがちな種類のデータであるという事実は、ハッカーのモチベーションの変化をさらに示唆するものです。大規模企業への攻撃対象は、財務データ、知的財産、あるいは顧客データという傾向がさらに進んでいますが、これらはすべて攻撃者の収益に直結するものです。しかし従業員データは、最終目的への手段という要素が強いものです。例えば、収集したデータを使って銀行あるいはより大きな対象にフィッシング攻撃をする、などです。あらゆる規模の企業が、高い割合で従業員データの喪失を経験しています。特に中規模企業が顕著な数値を示しています。

データのより良い保護のため、企業は多種多様の行動を考えています。最も取られ得る行動は、業務と個人用のデバイスをより厳しく分けることです。これは、ほとんどの企業が BYOD モデルに進まざるを得ないであろうという認識に真っ向から反するものです。これによって、業務目的で使用するデバイスを主に管理し続けるという発想の事業形態を、ビジネス界全般における他のデータポイントやアネクドートが、さらに支持することになる可能性があります。その他、デーロスに対して起こりうる動きとしては、ソー

シャルネットワークに関する企業ポリシーを作る、または強化する(49%)、デバイスセーフティ周辺の企業ポリシーを作る、または強化する(47%)、そしてモバイルデバイスおよびポータブルメディア上のファイル暗号化(47%)などがあります。

DLP の入手状況は？

企業の 58%が DLP ソリューションを配備していると言っていますが、堅牢なデータ保護を真に示すものではないでしょう。ESPO Systems はイリノイ州にあるセキュリティソリューションのプロバイダですが、これらのツールの需要の伸びを認めています。「私たちのベンダーは、一丸となって DLP ソリューションを支援しています。」と、ESPO Systems、Websense 事業部の副事業部長 Nick Stricker は言っています。「ファイアウォールやアンチウィルスのような分野は飽和状態ですが、データは未開拓の機会がある分野です。」しかし多くの企業は、DLP のラベルを自己裁量で使用しているツールで、求められるデータ保護がすべて完全にできていると、誤って思い込まされているのかもしれません。ESPO System の Proofpoint 事業部長の Brian Gardner は「DLP 能力を持つと謳っているツールの中には、クレジットカード番号や社会保障番号などといった基本的な情報しか見ていないものもあります。」と指摘しています。より堅牢な DLP ソリューションは、企業が識別用に選択するであろうどのようなデータでも追跡でき、段階的な導入が、企業のデータがどうあるべきか、そして企業ウォールからどれだけの量が実際に出て行っているかを企業が認識する助けとなります。典型的な DLP 設定では、まずモニタリングから始まりますが、ここではツールは単にネットワークのトラフィックを観察して、データの動きを理解するにとどまります。次の段階は検知です。ここでは、ユーザーが怪しいデータを送信したり、継続するか破棄するかを選択したりする際に、通知を受け取ることができます。最後に、電子メールで共有したり外部メモリにコピーしたりすべきではない、あらゆる慎重に扱うべきデータをブロックする構成をツールに組むことができます。これは、多くのツールが持っているいわゆる DLP 機能よりもはるかに堅牢なアプローチであり、企業の真の防御範囲を理解するために、データ保護戦略を深堀りするのは意味のあることです。もちろん、どのようなソリューションでもデータ喪失を完全に予防することはできません。「人が自分の携帯電話でいつ写真を撮っているかを知ることができるようなものは、まだ何もないのです」と Gardner は言っています。

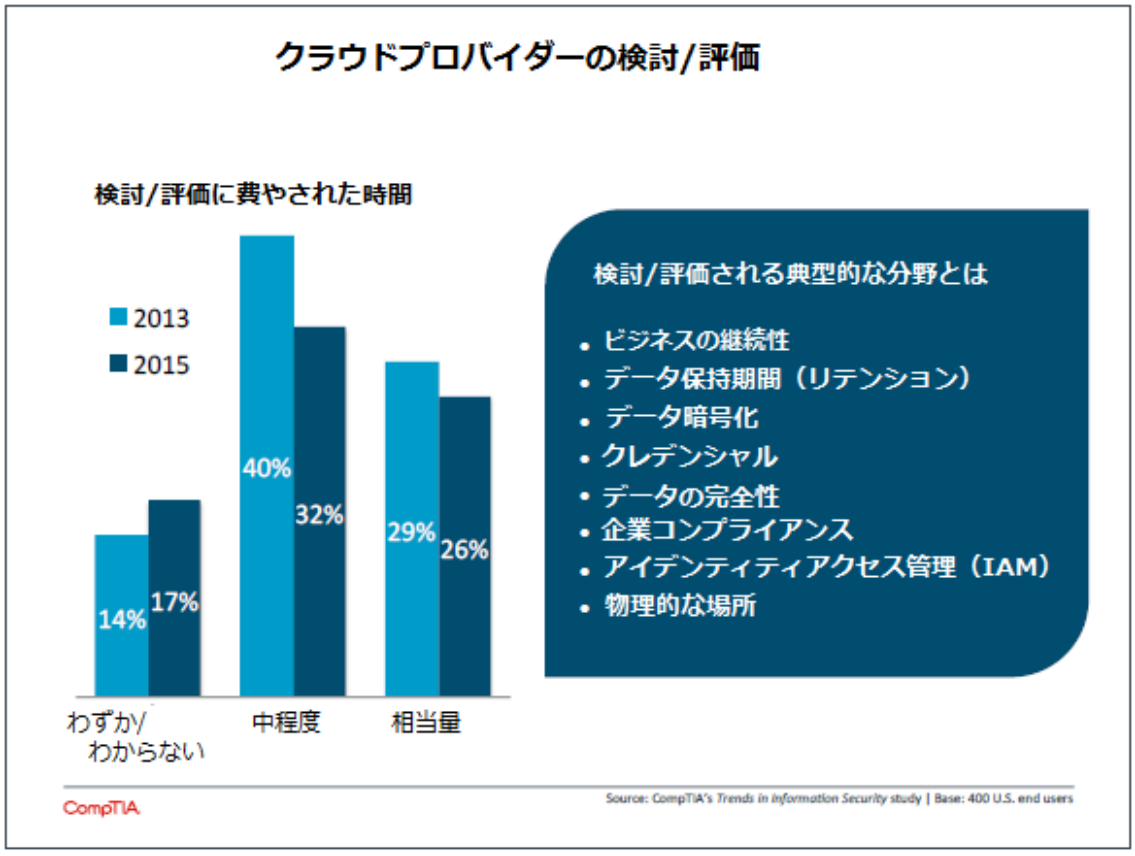
クラウド移行の影響について

データに関する懸念とは別に、システムのクラウドへの移行は、企業に対していくつかの問題を生み出します。特に、クラウドプロバイダと関わる前に、自社のセキュリティ要件を注意深く検討していなかった場合には顕著です。クラウド導入の初期には、企業がクラウドシステムを使用していない第一の理由として、セキュリティが挙げられることがしばしばありました。今日、企業の大多数が、クラウド環境のセキュリティを十分に検証することで、セキュリティという「ハードル」をクリアにしています。中には、クラウドシステム導入の現状から、適切なセキュリティが敷かれていると判断する企業もあるかもしれません。

ですが、この判断はクラウドへ移行する最適な方法でないことは明らかです。企業は、たとえ解決可能で

はあっても、セキュリティに関する懸念はまだ存在することに気付くことになるでしょう。初期クラウド移行に続いて、多くの企業がセキュリティに関する理由で、二次的な動きを見せています。この中には、パブリッククラウドからプライベートクラウドへの移行(36%)、パブリッククラウドからオンプレミスシステムへの移行(31%)、あるいは、一つのパブリッククラウドプロバイダから別のプロバイダへの移行(30%)などがあると考えられます。

二次的移行は、クラウドプロバイダのポリシーを適切に検討していれば避けられたであろう教訓が、移行後に残されていたことを表します。前述同様、このような検討を行うには、自社のセキュリティ要件を事前に理解することが必要ですが、理解ができた後は、プロバイダを詳細に評価することで、混乱や付加的業務を回避することができるようになるでしょう。



企業がクラウドプロバイダと関わる前に、自社のセキュリティ要件を理解しておくことがこれほど重要な理由は、安全性と信頼性の担保には非常に多くの分野が含まれているからです。全体にわたり、上図のリストにある各項目を常に評価していると言っている企業の割合は、過去 2 年間で増えています。分布もかなり堅調です。40%から 60%の企業が常に各分野を評価していると言っています。企業は、評価を行う重要性と見直しの対象となる課題の広さを認識しつつあるのです。

セキュリティ要件を理解し、クラウドプロバイダを評価するプロセスを通し、内部的な変化も推進されます。48%の企業が、クラウドセキュリティへの見方が変わった結果として、企業ポリシーを変更したと言っています。そして 41%がクラウドホストのアプリケーションに追加的セキュリティ機能を構築しています。クラウドへの移行は、クラウドプロバイダに存在するギャップを埋めるための追加的なセキュリティ手段を必要とするだけでなく、アプリケーションのアーキテクチャとビジネスの業務フローの変化も求めるのです。そして多くの場合、これらの変化はシステム移行以上に難しい、ということが明らかになります。

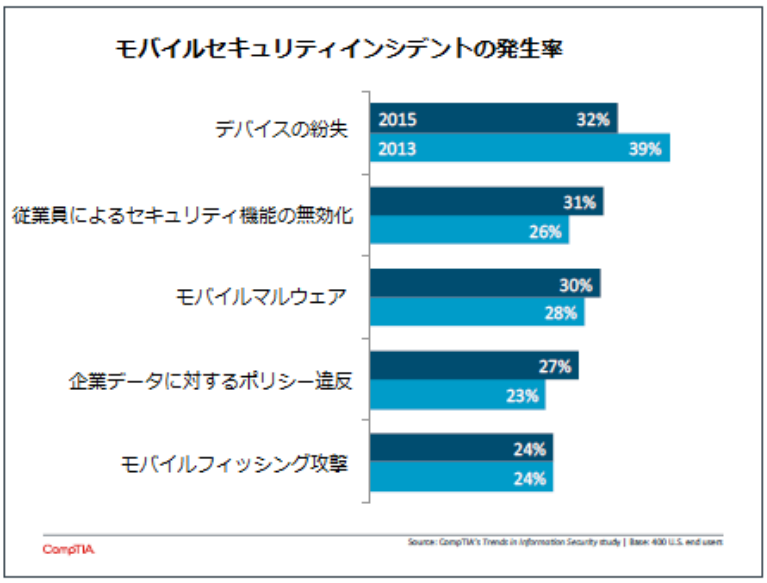
デバイスを超えたレベルでモビリティセキュリティをとらえる

わずか 3 年前、企業が心配するモバイルセキュリティに関する主要インシデントは、デバイスの紛失でした。スマートフォンやタブレットがより携帯しやすく便利であると同時に、デバイス紛失はやっかいといえます。最悪の事態では、デバイス内に企業秘密データが保存されていた場合、深刻なセキュリティ侵害となる可能性もあったのです。

BYOD によって事態はさらに複雑になりました。従業員が自分の個人デバイスを業務に使用できるよう IT を推進したり、単に使用できる方法を見つけたりしたことで、あらゆる種類の企業追跡ソフトやアンチウィルスによる保護の配備が、宙に浮いた状態になりました。また、企業は、モバイルデバイスを提供することで生産性を追求し、コンシューマーテクノロジーでは、広域な利用など、もっと高い技術レベルを求めていました。

今や、モバイルセキュリティの実態は、典型的なエンタープライズセキュリティの考え方に似たものとなっています。直近のデータでは、モバイルのマルウェアは増大を続け、エンドユーザーの問題もより頻繁に起こるようになっています。

モバイルセキュリティに関するインシデントの報告は、中規模企業からより多い傾向にあり、これは直近の BYOD スペースへの移行に関係しています。企業は、自らを BYOD から生じる危険に目を向けることなく、モビリティ戦略を追求しつつあります。モバイルデバイスとモバイルオペレーティングシステムは、よりエンタープライズが使いやすいものと



なり、企業は、管理を維持したままで、望ましいデバイスを提供できるようになっています。これは大規模企業で頻繁に起きていることであり、大規模企業からのモバイルセキュリティインシデント報告数が低いことに結びつきます。

小規模企業では、モバイルセキュリティ脅威によって、自社が持つ能力を超える複雑性がもたらされます。様々な領域の脅威を認識していても、自社には無い処理能力が要求されることもあります。モバイル脅威の状況を十分理解する妨げとなる資源的な制限が、デバイス管理についての強力なポリシーをも妨げるのです。ですから BYOD は中規模企業で最も急増しています。リスクは高いことから、これらの企業への教育、製品そしてサービス提供という機会が実際に存在します。

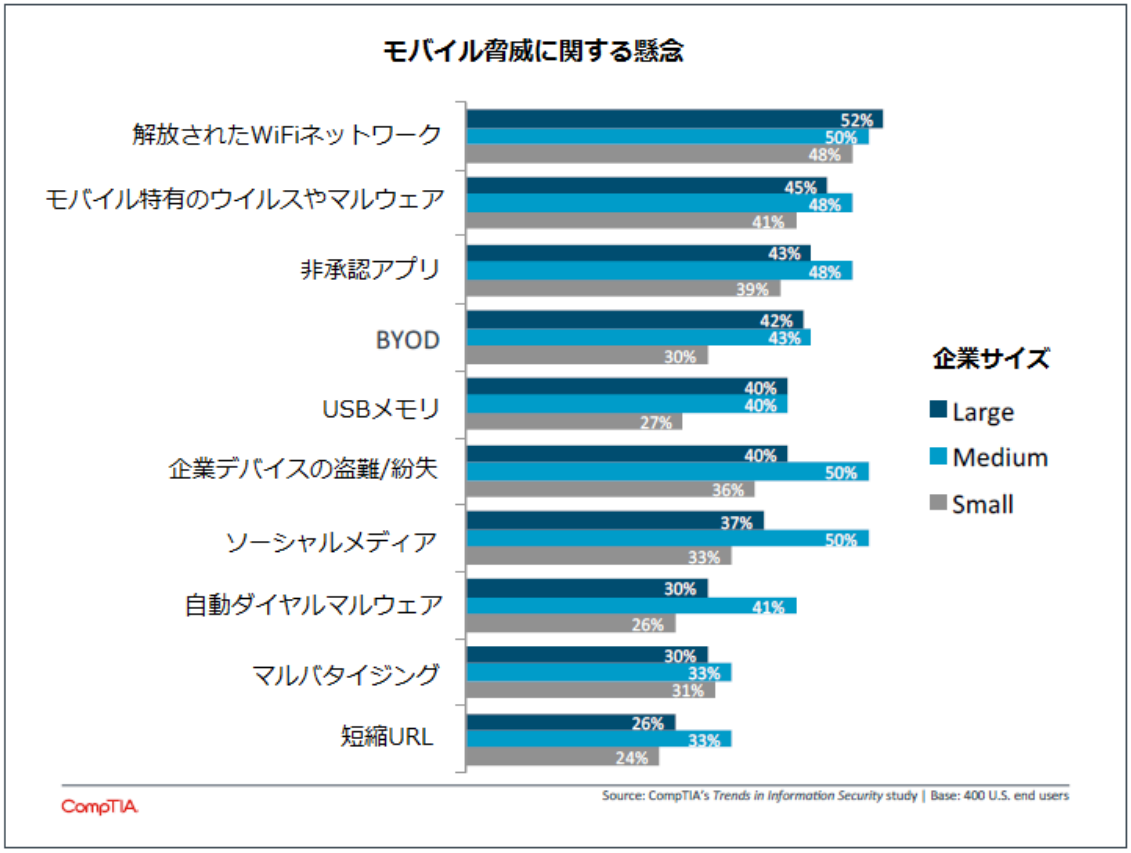
モバイルセキュリティを始めるのは、決してコストのかかる試みではありません。モバイルセキュリティインシデントの結果として、企業が一般的に行う取り組みのほとんどは、モバイルデバイスのための追跡もしくは完全消去ソフトウェアをインストールすることです。次にあげる取り組みにはコストはかからず、単にベストプラクティスに対する理解が必要なものもあります。

このデータからは、モバイルセキュリティが行く道はまだ遠いことも分かります。クラウド移行の際と同様、先陣を切っている企業はモバイルデバイスを含む安全な環境を完全に実現するためには、さらなる変化が必要であることに気付いています。例えば、企業データへのアクセスのためのバーチャルデスクトップのような、新たな方策を使用することなどがあります。しかしながら、この種の選択肢を検討している企業はわずか 33%です。企業は、収益と成長を推進するためにクラウド、またはモバイルベースの技術への追求を継続していく中で、適切なセキュリティというものが、既存の戦略をつぎ合わせるだけにとどまらず、セキュリティ実践を完全に計画し直すところまで広がって行くものだと認識するでしょう。

モバイルセキュリティ向上のための取り組み

45%	追跡/完全消去ソフトのインストール
44%	モバイルデバイスにパスコード要求
41%	デバイス紛失についての手続き確立
39%	モバイルデバイスに暗号化要求
35%	正式なモバイルポリシー構築開始
33%	企業データにアクセスする新たな方策
32%	モバイルセキュリティに関する追加的トレーニング
30%	モバイルセキュリティへの第三者の参加
26%	アプリについての承認プロセス構築

CompTIA


モバイル脅威に関する懸念
解放されたWiFiネットワーク
52%
50%
48%
モバイル特有のウイルスやマルウェア
45%
48%
41%
非承認アプリ
43%
48%
39%
BYOD
42%
43%
30%
USBメモリ
40%
40%
27%
企業デバイスの盗難/紛失
40%
50%
36%
ソーシャルメディア
37%
50%
33%
自動ダイヤルマルウェア
30%
41%
26%
マルバタイジング
30%
33%
31%
短縮URL
26%
33%
24%
企業サイズ
Large
Medium
Small
CompTIA
Source: CompTIA's Trends in Information Security study | Base: 400 U.S. end users

SECTION 3:

Usage Patterns

セクション 3：使用パターン

所見

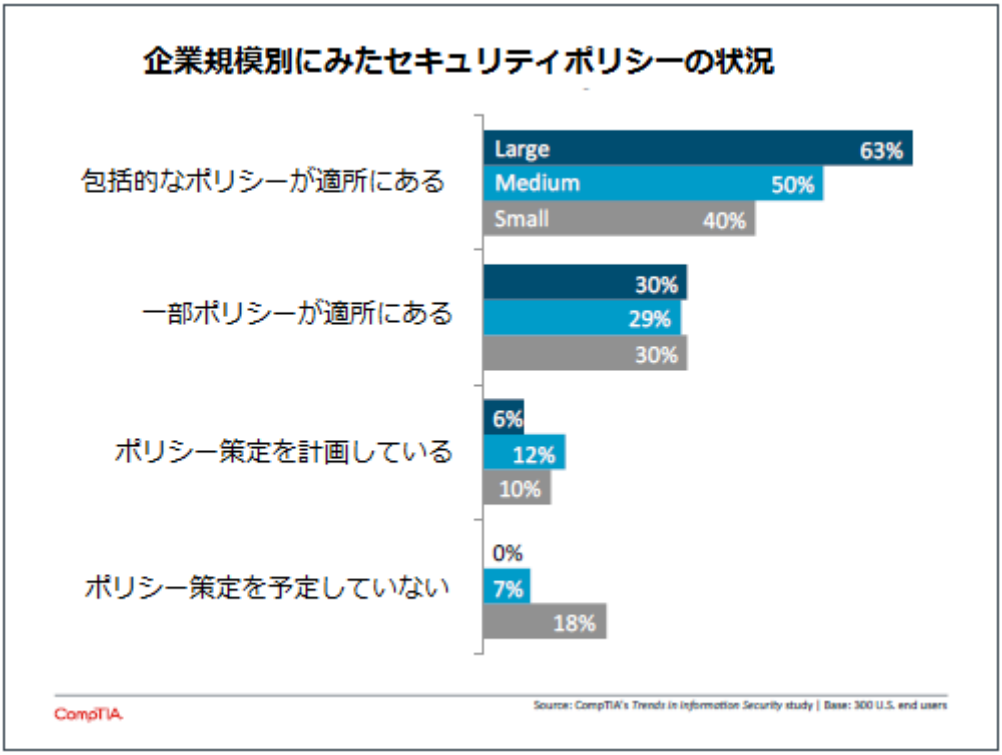
- テクノロジーは新たなセキュリティ取り組みの一片に過ぎません。プロセスも考慮しなければなりませんが、プロセス決定を記述する最適な場所はセキュリティポリシーです。全企業の中で、包括的なセキュリティポリシーを持っていると報告しているのは半数に過ぎません。小規模企業の 18%に関しては、来年にポリシーを作成する予定すらない状況です。
- 正式なリスク分析は、もっと多くの企業が焦点を当てるべきプロセスです。2013 年と比較すると、セキュリティとリスクのバランスが自社において適切であると感じている企業数は少なくなっています。このことは、企業がこのエリアをより注視し始めていることを示しています。企業の 34%が現在、自社のリスクはあまりに大きく、より厳しいセキュリティを検討すべきだと感じています。
- 企業に、広範な規制がかけられることがさらに増える中、急速に重要度を増しているもう一つのプロセスはコンプライアンスです。企業の 54%が、コンプライアンスの維持には、高レベルの努力が要求されると言います。これは、コンプライアンスは、コアコンピテンスではないことから、この業務を

外部委託したいという意思の表れかもしれません。

プロセスとポリシー

テクノロジーの特徴には、単に既存モデルの置き換えだけではなく、企業のプロセスと業務フローのより深いレベルでの変換をもたらすという点があります。これは、企業がクラウドやモビリティについて目にしている事象です。これら 2 つの基本的な傾向により、企業は自社の IT アーキテクチャ、ビジネスオペレーション、そしてポリシーを調査せざるを得なくなっています。

企業が、さらなる進化を進めようとする際、セキュリティは特別な検討を必要とするエリアです。セクション 1 で述べた通り、ビジネスの急激なデジタル化によって、サイバー犯罪によってもたらされ得る影響は増大しました。セキュリティ違反は企業活動に甚大な影響を与えかねませんし、復旧コストはかなりの額になるでしょう。特に、ほとんどの顧客にとってプライバシーが重要と考えられるようになっている時代に、データ違反が起きた場合、これらのコストには、企業の評判を回復するコストも含まれます。攻撃者はこれらの可能性を熟知しており、その攻撃パターンの幅を広げています。企業規模に関係なく、自分たちの目的達成を可能にするような弱い防御がないか探しているのです。



企業が IT セキュリティに対する考え方と取り組みを変化させていく中、自社のセキュリティポリシーに注意を向けることが必要になってきます。これまでのセキュリティに対する捉え方が、単にオンプレミスデ

バイスと情報のためのセキュアペリメーターであった場合、ポリシーはあまり堅牢なものではないことが多いのです。ポリシーそのものが全くない場合もるでしょう。理由はどうであれ、全企業の半分が、ポリシーがない、あるいはポリシーに手を加える必要があると述べていることが調査では分かっています。

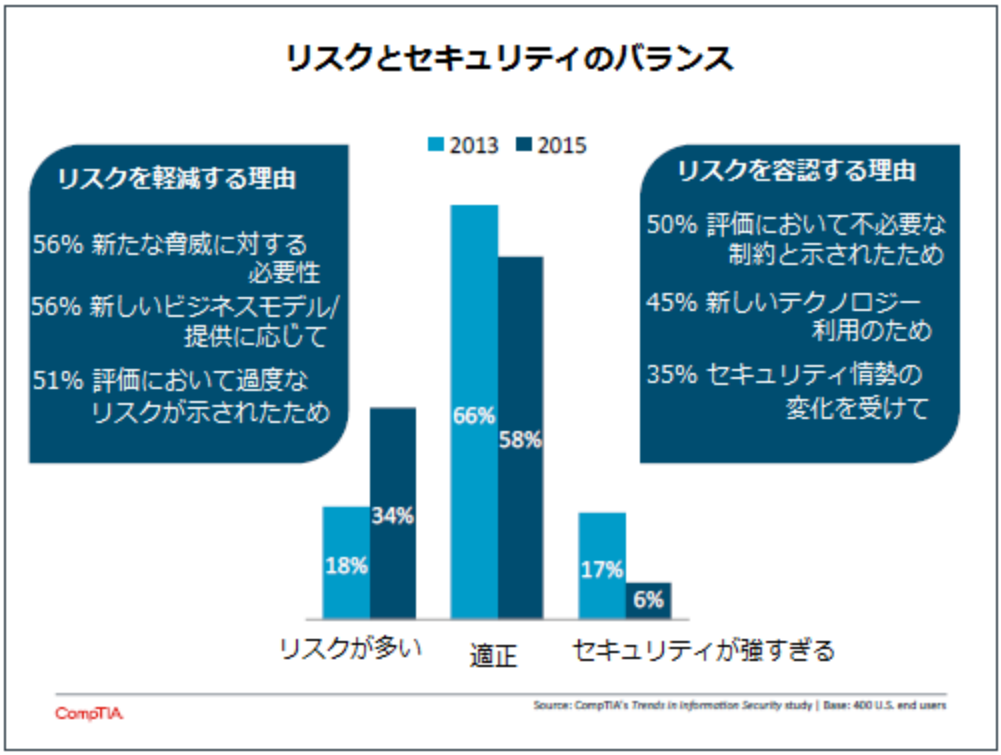
企業の規模別にみたポリシーの有無は、予想通りでした。大規模企業の 63%が、自社のポリシーは包括的であると感じていますが、この割合は中規模企業では 50%、小規模企業では 40%になります。今後 12 か月で、ポリシー調整あるいはポリシー構築の計画が必要だと考えている割合はかなり均等です。小規模企業は、ポリシーがない、あるいは構築する計画がない、というセグメントで大半を占めています。これらの企業は、正式なセキュリティポリシーはやり過ぎだと感じているのかもしれませんが、ポリシーはセキュリティ事項における合意機会を提供しますし、発生コストは、討議に必要な時間だけです。

包括的なセキュリティポリシーは、セキュリティについての満足度に直接関係しています。企業は、十分に時間をかけ、セキュリティ全てのエリアにおける徹底的な見直しを行うことで、自社はベストな状態にあると感じることができるのです。「自社のセキュリティに完全に満足している」と回答した 10 社のうち 7 社が、包括的なセキュリティポリシーを社内に持っています。

はじめはリスク分析から

セキュリティポリシー改定においては、規定や、全面的な見直しがされるべき内部プロセスに直面することがあります。これらのプロセスは、セクション 2 にあった、日々のモニタリングや管理を行うセキュリティとは異なるものです。先のテクニカルオペレーションが IT チームの業務範囲なのに対し、これら内部プロセスには、組織内の全部門が関わることになります。

まずこれらのプロセスとして、正式なリスク分析があります。プロジェクトマネジメントにおけるリスク分析の実施は、十分に確立されています。様々なリスクに確率と影響がアサインされ、その設定に基づいて、軽減戦略が導入されます。しかしながらこの方法は、全般的なセキュリティのエリアにおいて、広く実践されているわけではありません。



正式なリスクアセスメントは、企業がセキュリティ脅威とする項目において、ほぼ最下位にランクされていました。わずか 28%が、深刻な懸念だとしている状況でした。これは CompTIA の企業調査全体に見られる傾向で、企業は、あまり理解していない分野にはそれほど重点を置かないことが分かっています。概して、懸念と導入レベルは、新しいトレンドが定着するに従い、増加してくると思われます。

リスク分析がより注目されるようになっていることを示す兆候がすでにいくつか見受けられます。2013 年のデータと比較すると、自社のリスクとセキュリティのバランスが適切であると感じている企業の数は少なくなっています。この観点は、すべての規模の企業において均一に広がっています。リスク/セキュリティ領域の両端にわずかな差異が見られるだけです。大規模企業は、現在の自社のセキュリティが過剰に厳しい、と言う傾向が比較的強く、中規模企業は、受容しているリスクが多過ぎると言う傾向が強くなっています。

職務毎に見てみると、差異はより大きいことが分かります。適正なバランスであるとする傾向は、企業幹部（エグゼクティブ）たちに多く見られ、64%が自社についてこのような状態だとしています。IT 従業員の数値もさほど低くなく、59%が適正なバランスであると考えています。

最大の差異は、最大の驚きでもありますが、事業部門の従業員の結果です。現在のバランスが理想的だと感じているのは 43%に過ぎません。驚くべきは、この数字自体ではなく、事業部門の従業員が、制限を減らす方に強く働きかけているわけではないということです。それどころか、彼らの 45%が、現在の環境に

はリスクが多すぎ、さらなる投資、ポリシー、あるいはトレーニングが状況を改善できるだろうと感じています。

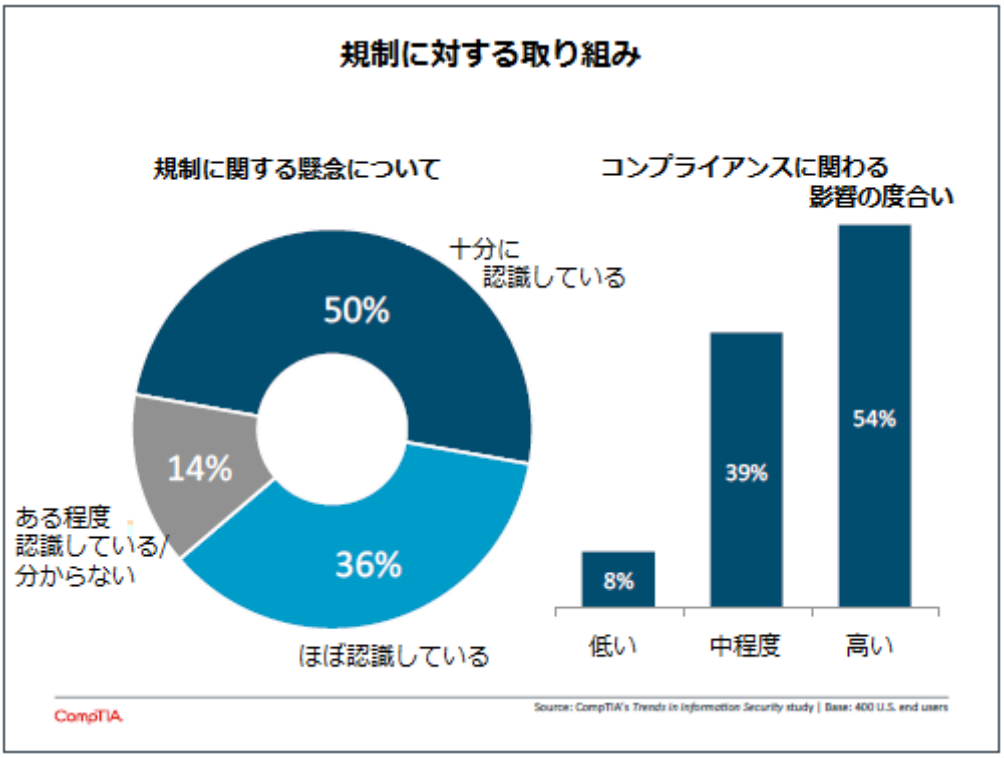
この見解は、ローグ IT に関する一般的な考えとは、大幅に反するものです。ローグ IT は、自分たちで調達やテクノロジー使用を行うため、IT 部門を避けている事業部という図式で描かれるものです。クラウドコンピューティングやモビリティが、テクノロジーのアクセスや設定を容易にしたことから、ローグ IT は封じ込めの難しい脅威のように捉えられてきました。しかし、最近のデータを見ると、事業部は自分たちだけで突き進む中で、困難に遭遇していることが分かります。インテグレーションは、多くの部門が正しいスキルを持つことが難しい、課題の一つであることは間違いありません。そして、リスクに関するデータからは、彼らが直接セキュリティ事象を経験しているか、あるいは、ローグ IT がセキュリティを弱くする状況を生み出したことを理解していることが分かります。

企業が正式なリスク分析に向かい、社内全体の従業員を教育するよりよい方法を模索していくと、日々の行動がどれほどセキュリティ体制につながっているかが、明らかになってくるでしょう。セキュリティ自己評価を行う基本的枠組みについては、本セッション末の別添をご参照ください。さらに詳しい情報は、CompTIA の Buying Guide for IT Security（IT セキュリティ用購入ガイド）に掲載しています。

コンプライアンス分野の成長

今日、企業が直面している最大の懸念は、規制環境の変化と様々な法規を順守する必要性です。理念としては新しいものではありません。近代のコンプライアンスプラクティスは、その起源を 1934 年の証券取引所法に遡ります。新たな点は、高スピードで成立を続ける異なる法律です。州または国境を越えたデジタル環境でビジネスが行われているために、多くの企業は以前には存在すらしなかった部分に懸念の種があることに気付き始めています。

Sarbanes-Oxley（企業改革法）、PCI DSS（クレジットカードセキュリティ基準）そして HIPAA（米国における医療保険の相互運用性と説明責任に関する法令）は、コンプライアンス意識と検証活動の新たなレベルを推進する最近の規制の中で、代表格となる例です。法規の中には、特定の対象に向けられたものもありますが（HIPAA がヘルスケア産業向けであるように）、それでも、企業が相互に影響を与え合い、コンプライアンスを保つべき物品やサービスを受け取れば、波及効果が生じることになるでしょう。データプライバシーは、さらに広大な影響を持つ新たな法規を推進するような、次の主要テーマになる恐れがあります。

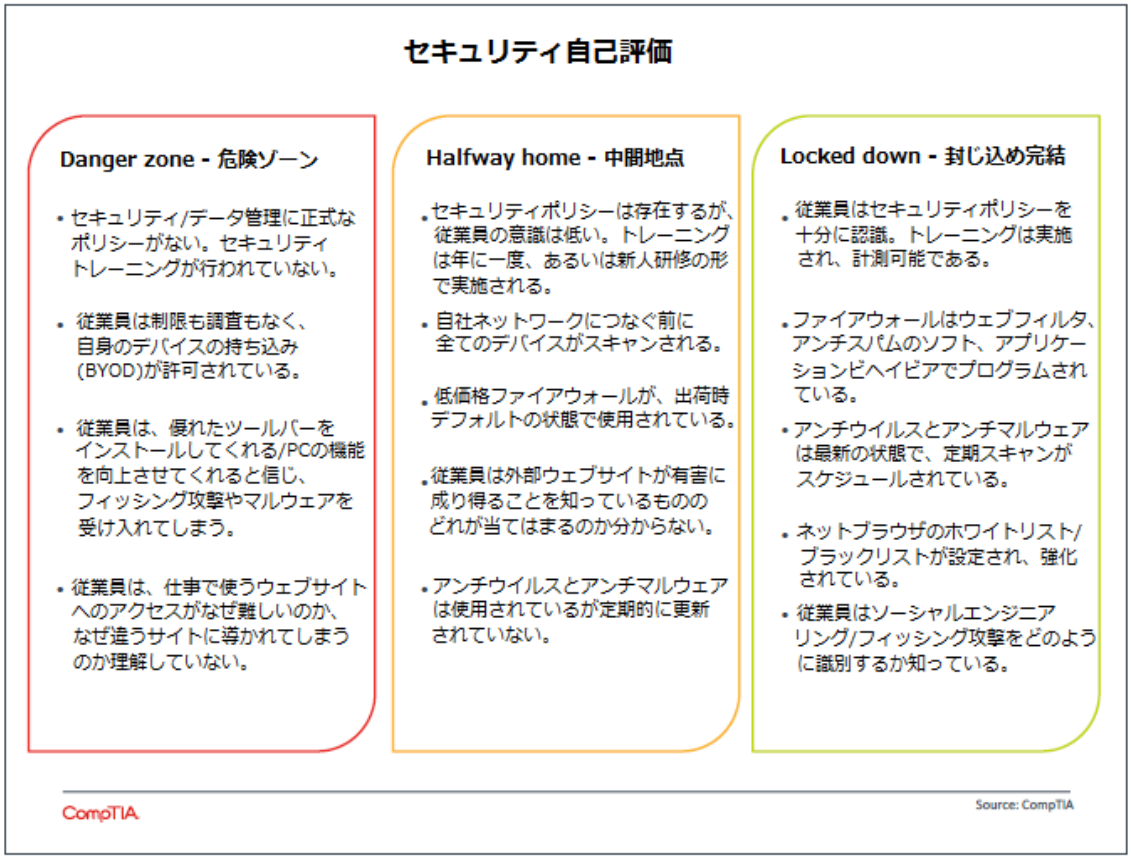


コンプライアンス問題を扱う際、最初にすべき仕事は、個々のビジネスにどの規制が適用されるのかを認識することだけです。法規順守しなかった場合に起こりうる結果を考えると、自社に影響しうる規制面での懸念をすべて認識していると答えたのが全企業の半数に過ぎないという結果には、驚くものがあります。予想通り、小規模企業は認識が最も低い(41%)のですが、大規模企業も、その自信のレベルは想定ほど高い数値を示してはいません(54%)。

さまざまな規制を認識し、監査の適正記録を維持するためには、多くの労力を要します。この点では大規模企業は大きなリードを見せ、その 61%が高いレベルで労力を費やしていると述べています(対して、中規模企業では 56%、小規模企業では 46 %です)。労力レベルの捉え方に関して、職務間の差異はあまり見られません。ですから、コンプライアンスは、企業において、代表的な部門横断的取り組みのテーマとしてふさわしいと考えられるのです。

コンプライアンスの維持・管理は、単に政府と問題を起こさないようにするという考えだけではありません。優良ビジネスプラクティスでもあるのです。10 社のうち 4 社が(44%)、規制コンプライアンスを維持した結果、顧客満足度が向上したと言っていますが、これはおそらく、より効率的な内部プロセスと企業データの体系化向上によるものでしょう。36%が、コンプライアンスの維持管理が新たな顧客を引き寄せたと言っており、27%がコンプライアンスは差別化を生むと言っています。コンプライアンスには付加的メリットは何もなく、単に業務を行うコストに過ぎないといっているのは、21%に過ぎません。

別添


セキュリティ自己評価
Danger zone - 危険ゾーン
• セキュリティ/データ管理に正式なポリシーがない。セキュリティトレーニングが行われていない。
• 従業員は制限も調査もなく、自身のデバイスの持ち込み(BYOD)が許可されている。
• 従業員は、侵れたツールバーをインストールしてくれる/PCの機能を向上させてくれると信じ、フィッシング攻撃やマルウェアを受け入れてしまう。
• 従業員は、仕事で使うウェブサイトへのアクセスがなぜ難しいのか、なぜ違うサイトに導かれてしまうのか理解していない。
Halfway home - 中間地点
• セキュリティポリシーは存在するが、従業員の意識は低い。トレーニングは年に一度、あるいは新人研修の形で実施される。
• 自社ネットワークにつなぐ前に全てのデバイスがスキャンされる。
• 低価格ファイアウォールが、出荷時デフォルトの状態で使用されている。
• 従業員は外部ウェブサイトが有害に成り得ることを知っているもののどれが当てはまるのか分からない。
• アンチウイルスとアンチマルウェアは使用されているが定期的に更新されていない。
Locked down - 封じ込め完結
• 従業員はセキュリティポリシーを十分に認識。トレーニングは実施され、計測可能である。
• ファイアウォールはウェブフィルタ、アンチスパムのソフト、アプリケーションビヘイビアでプログラムされている。
• アンチウイルスとアンチマルウェアは最新の状態で、定期スキャンがスケジュールされている。
• ネットブラウザのホワイトリスト/ブラックリストが設定され、強化されている。
• 従業員はソーシャルエンジニアリング/フィッシング攻撃をどのように識別するか知っている。
CompTIA
Source: CompTIA

SECTION 4:

Workforce Perspectives

セクション４：人員的観点

所見

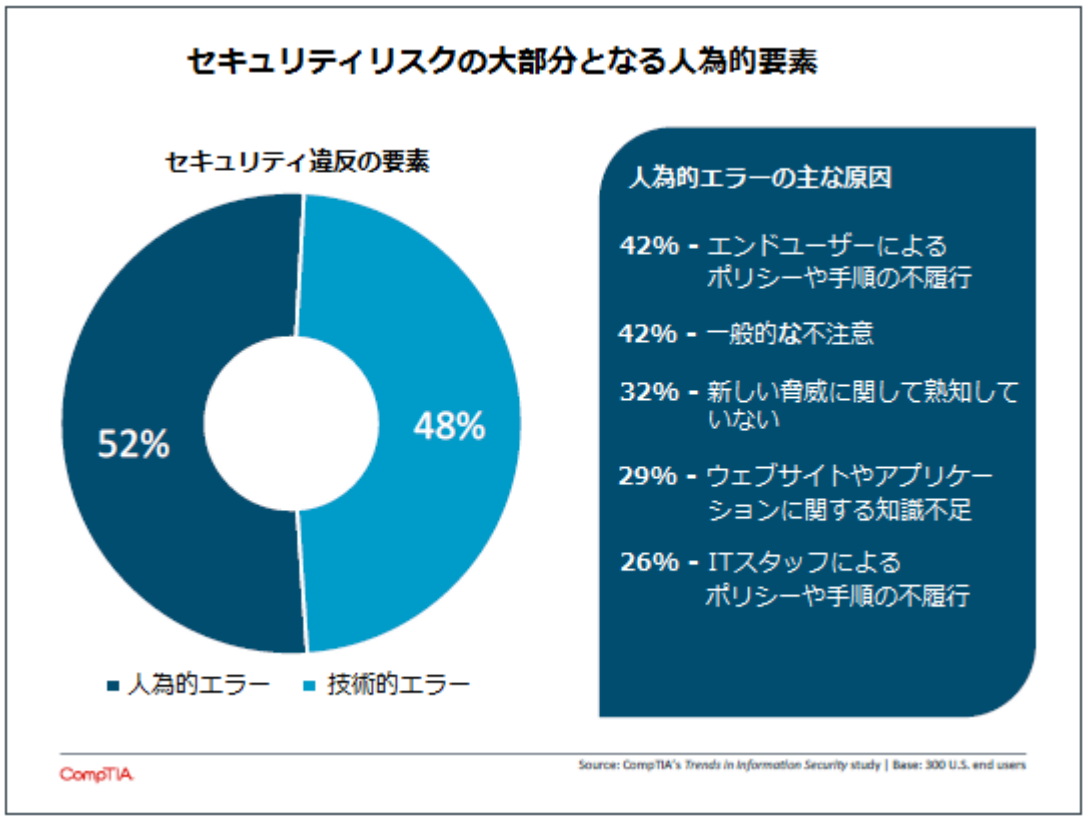
- 新たなセキュリティの取り組みにおける最後の要素は、人的要素を考慮することです。これを深刻な懸念だと位置づけている企業はわずか 30%です。これらの企業は、人為的要素はセキュリティ違反の根本原因の 52%を占めるとも報告しています。ここ数年にも増して、企業は人為的エラーがセキュリティインシデントに影響を与えている、特定のエリアに言及しています。
- トレーニングは、人為的エラーを低減する答えとしては明確なものですが、企業はトレーニングへの投資をどのようにすればよいか理解するのに苦慮しています。サイバーセキュリティのトレーニングを何らかの形で行っている企業はわずか 54%で、大抵は、新入社員の導入教育、あるいは年に一度の再教育コースのような形で実施されています。
- セキュリティのトレーニングを行っている企業の 86%が、トレーニングは効果的だと感じていますが、これは、自社の現在のセキュリティは十分だと感じている企業が多い状況と似ています。このエリアについての測定基準は無いに等しく、企業は、自社のセキュリティトレーニング内容をもっとよくし

たいと思っていることを認めています。

最弱のリンク

本調査のセクション 1 では、存在する多種のセキュリティ脅威と、企業が各脅威に対して持っている懸念レベルを記しました。最も低いレベルの懸念をもたらすものの一つが人為的エラーで、それが、一般職員が起こすエラーであれ (深刻な懸念だと評価した企業はわずか 30%です)、IT スタッフが起こるものであれ (深刻な懸念だとした企業は 27%) 状況は同じです。

このような懸念レベルの状況が、ショッキングである理由は、企業が常々、人為的エラーがセキュリティ違反の主な原因だと評価しているからです。もちろん、人為的エラーを技術的エラーと区別するのが難しいこともあります；例えば、不備のあるファイアウォール構成は、技術的エラーなのでしょうか、それとも適切な設定をするための知識不足による人為的エラーなのでしょうか。解釈が入る余地はありますが、様々な CompTIA 調査において、一貫している事例から、どのような行為が「人為的エラー」区分に入るのかを示すベースラインがあります。



2015 年のデータによると、企業が日々の業務における人為的エラー事例を目にする機会は、増加し始めています。2013 年には、人為的エラーの最も大きな原因は「エンドユーザーによるポリシーと手順の不履

行」と「IT スタッフによるポリシーと手順の不履行」でした。それから 2 年後、企業はこれら 2 つの一般化された理由に、さらに具体的な事例を加えて示しています。

一般的な不注意は、今や人為的エラーの 2 番目の理由と評されています。この行為は、セキュリティと利便性が衝突した結果の最たるものです。エンドユーザーは、セキュリティにおけるベストプラクティスが何なのかを知ってはいても、効率性を追求する中で、より利便性の高いソリューションを選ぶことがよくあります。パスワードはこれを顕著に表す例です；ほとんどの人々はどうしたら強力なパスワードになるか、十分認識していますが、SplashData における最悪のパスワードは今もって「123456」や「password」です(このリストは、漏えいしたパスワードリストから最も一般的な文字列を集めて作られています)。

新たな脅威のスピードに後れを取ることも、人為エラーの原因となります。企業では、自社の従業員がテクノロジーソリューションを推し進めながらもセキュリティが何を意味するのかを十分に理解していないという状況下、このような事態が非常に多く起こるようになっています。ローグ IT はやや低迷してきてはいますが(セクション 3 を参照)、このような種類の行為に結びつく可能性はまだ残っているのです。

人為的エラー対、技術的エラーが混ざった状況全体は、年々変化するものではありませんが、人為的エラーがさらに大きな懸念原因をなりうることを示すものが他にもあります。人為的エラーがセキュリティインシデントに何らかの要因となっていると述べた企業のうち、39%が、「人為的エラーは過去 2 年間において、さらに大きな要因となっている」と報告しています。この回答は、セキュリティ違反の根本原因特定のため詳細な調査がされている大規模企業において多く見られます。小規模、中規模企業においても、セキュリティ問題により敏感になるにつれ、従業員の経験不足や不注意から起こる問題を目にすることになるでしょう。

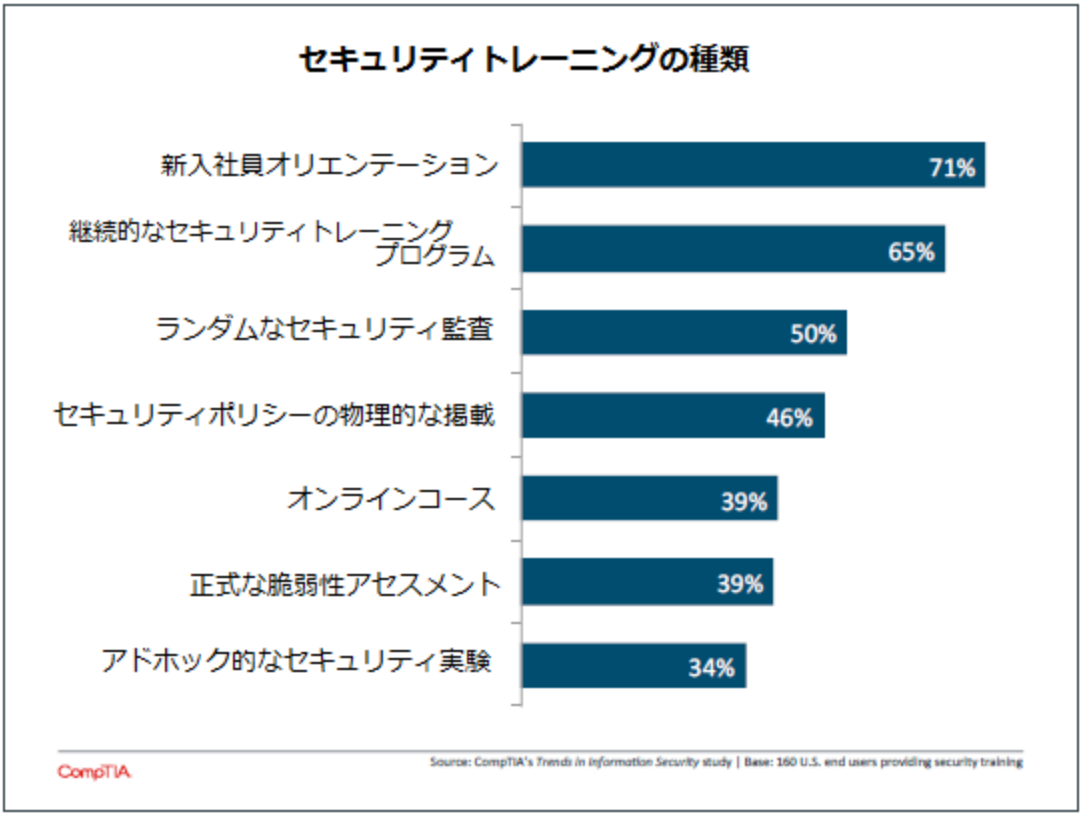
トレーニングの選択肢を探る

企業が「人為的エラー」に対して低レベルの懸念を示す理由は、それが明確なソリューションを持たない問題だからといえます。マルウェアやハッキングに対する高レベルの懸念は、技術的な投資によって対処できます。従業員のエラーに関する高いレベルの懸念は、トレーニングに投資することで、対処できる可能性はありますが、そこには複雑な要素が絡んできます。

多くの企業が、教育提供に関して苦戦しているといえるでしょう。彼らの得意分野ではなく、効果測定が非常に困難だからです。ビジネスの結果に直接結びつくトレーニングプログラムは無いに等しいのです。そして、インシデントが起こらないことが望ましい効果とされる、セキュリティのような分野においては、特に複雑な状況になるのです。

それでも、ほとんどの企業は、業務関連であれ、コンプライアンス志向であれ、あるいは人事上の義務で

あれ、基本的なトレーニングの提供を考えているのです。セキュリティトレーニングは最も一般的なものの一つですが、だからといって、広く行われているということではありません。何らかのサイバーセキュリティのトレーニングを行っている企業は 54%に過ぎません。企業が人為的エラーの問題と戦う中で、この数字は伸びていくと考えられます。



この図は、企業がよりセキュアな人材の育成を考えるにあたって、その手段のベースラインとなるでしょう。現状のトレーニングと、理想的とされる状況のギャップを把握するには、最も実施の高いトレーニングを見ると良いでしょう。セキュリティは、新人社員オリエンテーションにおいてのみ議論となるのであれば、従業員が業務に就いてしまった後に提供されるという仕組みがないことになるのです。

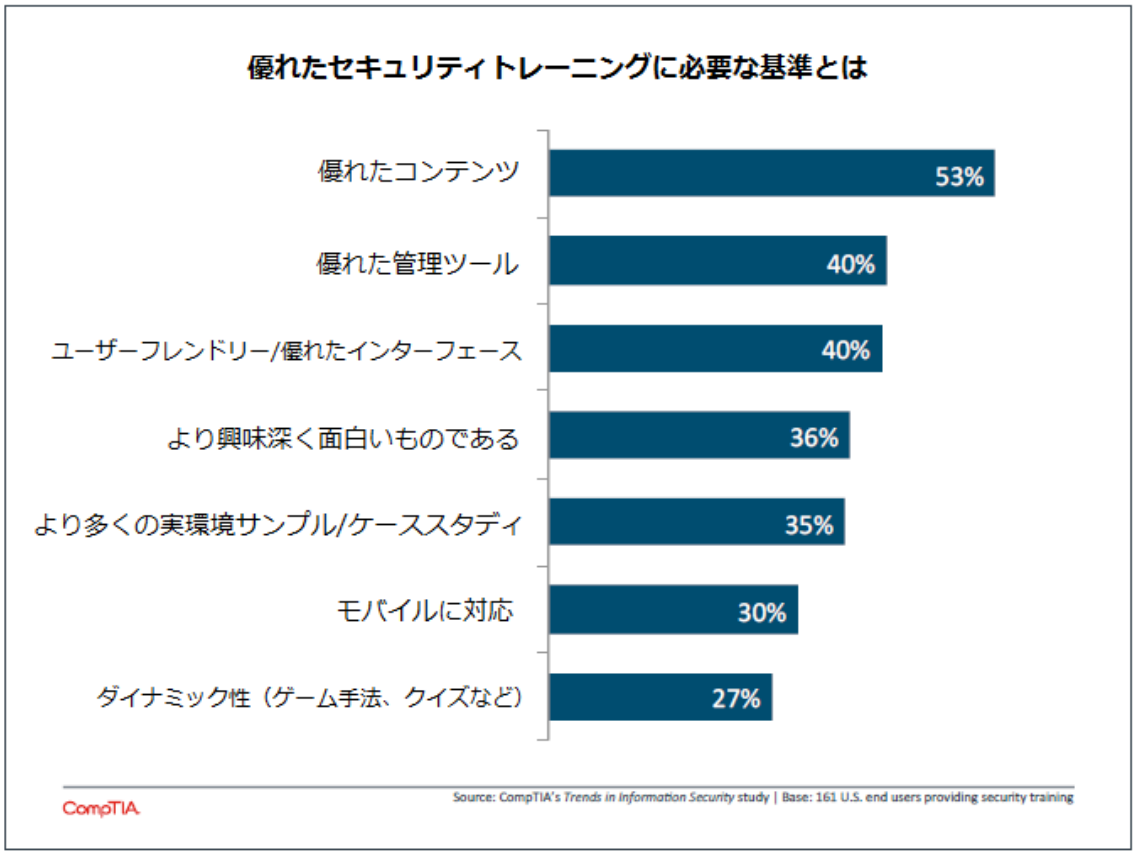
セキュリティトレーニングを行っていると述べている企業は、従業員に義務付けている年に一度の再教育のような形態を指していることが多いのです。また、比較的少数の企業は、年間を通して複数の関連プログラムを実施しています。これらのプログラムには、フィッシング攻撃のシミュレーションや、コンピュータにプラグインされるとセキュリティチームに警告を送るようになっている USB スティックを「落とした」場合、といった特別な検証目的のためのセキュリティ体験が含まれている場合もあります。

方法はどうであれ、企業は自社の現在のセキュリティトレーニングが機能していると思っています。セキ

ュリティトレーニングを行っている中で、10 社のうち 8 社を超える企業(86%)が、「非常に有効」または「ほぼ有効」だと考えています。一見、ここには改善の余地はあまりないように思われます。しかしながら、「非常に有効」という評価をつけているのは企業の 36%に過ぎないことから、少なくとも何らかの向上可能性があることが分かります。

さらに、これらの企業を深堀りして、どれくらい正確に有効性を計測しているかを聞いてみる価値はあるでしょう。きちんと構築された計測法がなければ、一般的な感覚によるところが大きいかもしれません。異なった役割を持つ回答者が、どのように自社のセキュリティトレーニングを評価しているかを調べてみると、このことがよく分かります。幹部 - 大きな違反を除いて起こりうるセキュリティ問題から一番遠い存在- の半数以上が、自社のトレーニングを「非常に有効」と評しています。同じように感じているのは、IT 担当者ではわずか 32 %、事業担当者では 26%です。

企業が、自社セキュリティトレーニングを過大評価している可能性が考えられる最後の理由は、より良い取り組みのための改善点を簡単に挙げられることがあります。特に、最も多く示される案が、セキュリティトレーニングの内容改善であるという事実を考えると、企業は自分たちが適切にカバーできていないエリアを認識しているように思われます。



他に改善可能な点としては、トレーニングの確実な効果があります。トレーニングをより参加型や活動型のものにすることで、定着度が上がり、結果としてセキュリティ意識が向上するでしょう。もし企業がこのような意識を計測する方法を構築することができれば、様々なトレーニングにおける明確な差別化要因を得ることとなります。

現在セキュリティトレーニングを行っていないセグメントを見てみましょう。予想通り、これらの企業がトレーニングを行わない主な理由の一つは、予算が不十分（26%）でした。あるいは、適切なセキュリティトレーニングが分からない（20%）、最も効果の高いセキュリティトレーニングが定かではない(19%)というものでした。

しかしながら、セキュリティトレーニングを行わない最大の理由として挙げられたのは「行う理由がないから」というものでした。3 分の 1 近い(29%)企業が、セキュリティトレーニングに対して特に障壁があるわけではないが、単に行っていないだけだと言っています。この分野には IT 企業にとって大きな機会が溢れています。IT 企業は、ベストトレーニングや、ベストセキュリティパッケージを提供し、人為的エラーの低減、企業のセキュリティ態勢の改善を提案・提供することができるでしょう。

SECTION 5:

Channel Dynamics

セクション 5：チャネルダイナミクス

所見

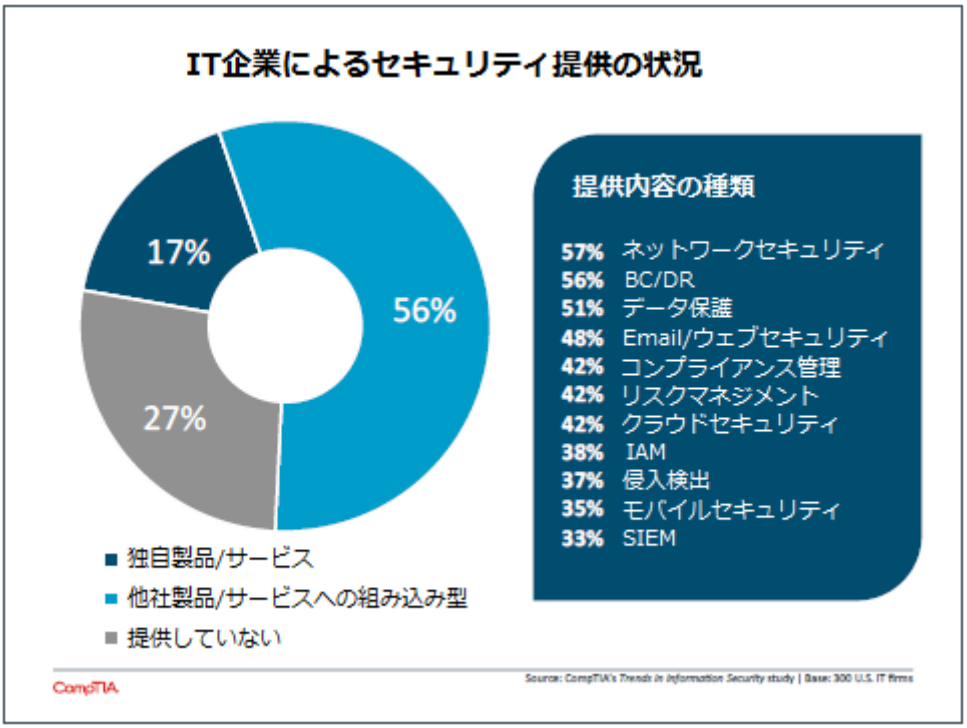
- セキュリティを提供しているチャネル企業のほとんどは、セキュリティと独立した製品やサービスとするのではなく、他の提供物の一部として提供しています。セキュリティがより重要で専門的になる中、セキュリティを新たな方法で提供する、あるいは顧客のためにより堅牢なセキュリティ態勢を創造するために協力する、といった可能性が出てきています。
- チャネル企業のうち、少なくとも 3 社に 1 社は、セキュリティをサービスとして、もしくはマネージドセキュリティサービスとして提供していると述べています。その率は、ソリューションプロバイダーや MSP のようなリーフチャネル企業において、より高くなっています。これは広い解釈であって、実際は包括的なセキュリティ提供でない場合もあります。ですが、さらにケイパビリティを向上させていく上では、良いスタートを切っていると言えるでしょう。
- 全チャネル企業のほぼ半数(48%)が、主なセキュリティ違反の結果として、何の調査も受けず、何の行動も取らなかったと言っています。これは、セキュリティについての討議を積極的に行ったり、顧

客が危険にさらされる可能性のあるエリアを明らかにする機会があることを示しています。

チャネルのセキュリティへの関わり

最低ラインとして、チャネル会社はセキュリティを取り巻く状況について、確実に理解する必要があります。規制分野が拡大するにつれ、パートナーやサプライヤーがセキュリティ侵害について責任を取るというハロー効果のような状況が発生しています。2013 年に起きた Target への大規模な侵害は、まさに第三者が情報暴露を生み出したのです。ハッカーは、Target の HVAC 請負業者の一つを攻撃した際、盗んだ認証情報を使って、Target のネットワークにアクセスすることができたのです。

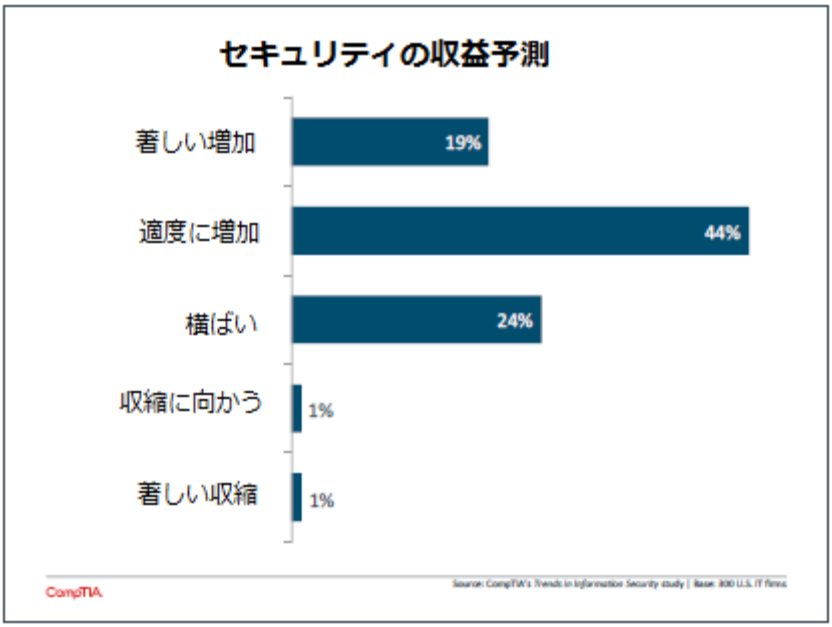
セキュリティは、長期に渡る重要なテーマであるため、ほとんどの IT 企業がある程度セキュリティに対処しているのも当然のことです。チャネル企業のほぼ 4 社に 3 社が、何らかの形で自社の製品ラインの一部にセキュリティを持っています。ソリューションプロバイダー、VAR、あるいはマネージドサービスプロバイダーと特定されるような企業で、この率はやや高くなっています(81%)。



チャネル企業が提供する製品やサービスは、顧客がセキュリティに対して取り組んできた方法にかなり沿った形になっています。ネットワークセキュリティ、ビジネス継続性、そして E メールセキュリティは全てセキュリティ戦略の基盤部分であり、企業はこれらを何年にもわたって行ってきました。データ保護も幅広く提供されていますが、セクション 3 で述べているように、データ保護には多くの特徴があります。

現在提供されているサービス全てが、包括的なものであるとも限りません。

拡大の可能性のあるデータ保護サービスに加えて、他のエリアでも強力なポテンシャルを見せるものがあります。ネットワークセキュリティと E メールセキュリティが無くなることはないでしょうが、コンプライアンス管理、リスクマネジメント、クラウドセキュリティ、IAM、モバイルセキュリティ、そして SIEM は全て、新たなセキュリティベースラインに容易に成り得るものなのです。



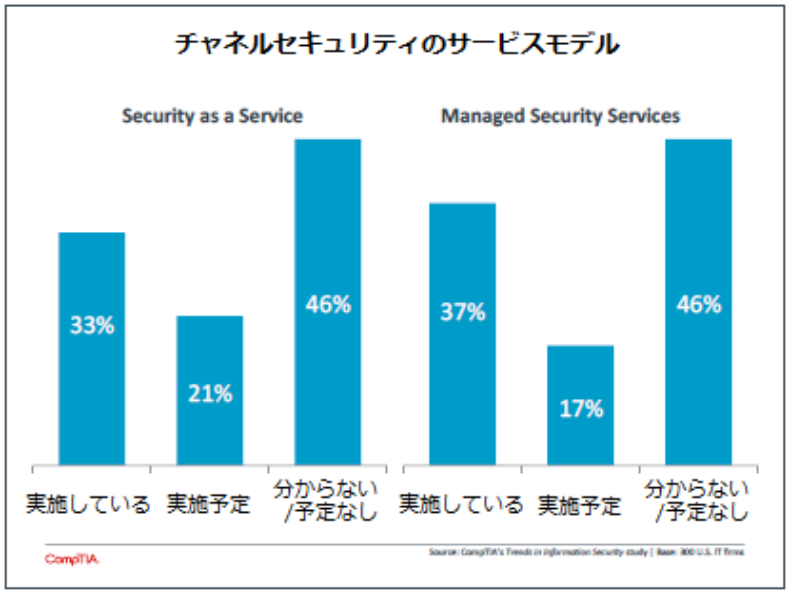
このような状況は、エンドユーザーにとって新たなレベルの複雑性を生み出すと同時に、これらのソリューションを扱う企業にも複雑性をもたらしています。再販売会社にとって新製品は、新たなエリアについてのトレーニングであれ、販売担当者の増員であれ、販売構成への変化を意味します。サービスプロバイダにとっては、より広い範囲での選択肢に関して、すべてをどう組み合わせて可能な限りベストサービスを提供したらよいのか、理解することが求められます。セキュリティが複雑性を増す中、エンドユーザーは自身でインテグレーションを提供するケイパビリティや労力を失い、人生をシンプルにしてくれる共生的ソリューションをますます求めるようになってくるでしょう。

こういったタイプのソリューションを調達する方法の一つは外部委託です。そしてこれは、チャネル企業がセキュリティ収益の成長が前進して伸びていくと見込む、理由の一つとなっています。収益見込みは、企業規模に関わらずかなり一貫していますが、ソリューションプロバイダー/VAR/MSP においてよりポジティブな展望が見られます。これらの企業は大抵、顧客が求めている包括的ソリューション各種を提供する傾向にあるので、特定製品のベンダーよりも大きな可能性を見ていることが分かります。

セキュリティプロバイダーになる

比較的大規模な企業は、セキュリティがさらに独立した重要エリアになっていると考え始めています。そして、チャネル企業にとっても、セキュリティを自社の領域として考え始める、同様の機会があるのです。

個々の製品についてのインストールやサポートは提供され続けますが、その一方で、製品、プロセス、そして人を包括する「一から十まで」のアプローチがますます求められるようになるでしょう。



この種のセキュリティアプローチに該当する 2 つの展開モデルを考察すると、チャネルは上記のアプローチを起こすに相応しい位置づけにあるように思えます。チャネル企業の少なくとも 3 社に 1 社は、サービスとしてのセキュリティ、あるいはマネージドセキュリティサービスを提供していると述べています。この率はソリューションプロバイダーや MSP のようなリーフチャネル企業でより高くなっています。

上記以外でも、今後 12 か月の間に顧客に対して、どちらかのセキュリティサービスを実施計画しているグループがあります。つまり、全チャネル企業の半数以上が、近い将来、何らかの形でのセキュリティ収益を得ることになるのです。

しかしながら、こういったタイプのビジネスモデルを持っている企業数と、セキュリティをスタンドアロンのサービスとして提供している企業数には相違があります。この相違は「サービスとしてのセキュリティ」と「マネージドセキュリティサービス」の解釈が、広義にわたっていることから生じている部分が大きいのです。クラウドベースの、もしくはより広範なマネージドサービス契約の一部にセキュリティがあるような、セキュリティ製品を一つ提供していればよいのだ、と捉えるチャネル企業もあります。セキュリティサービスを提供する傾向が最も強いリーフチャネル企業の中でさえ、セキュリティをスタンドアロン提供品として持っているのはわずか 23%に過ぎません。これは、議論の中心が、他の製品やサービスに置かれ、セキュリティはそれに伴う話題という位置づけで取り上げられている状況を示唆しています。

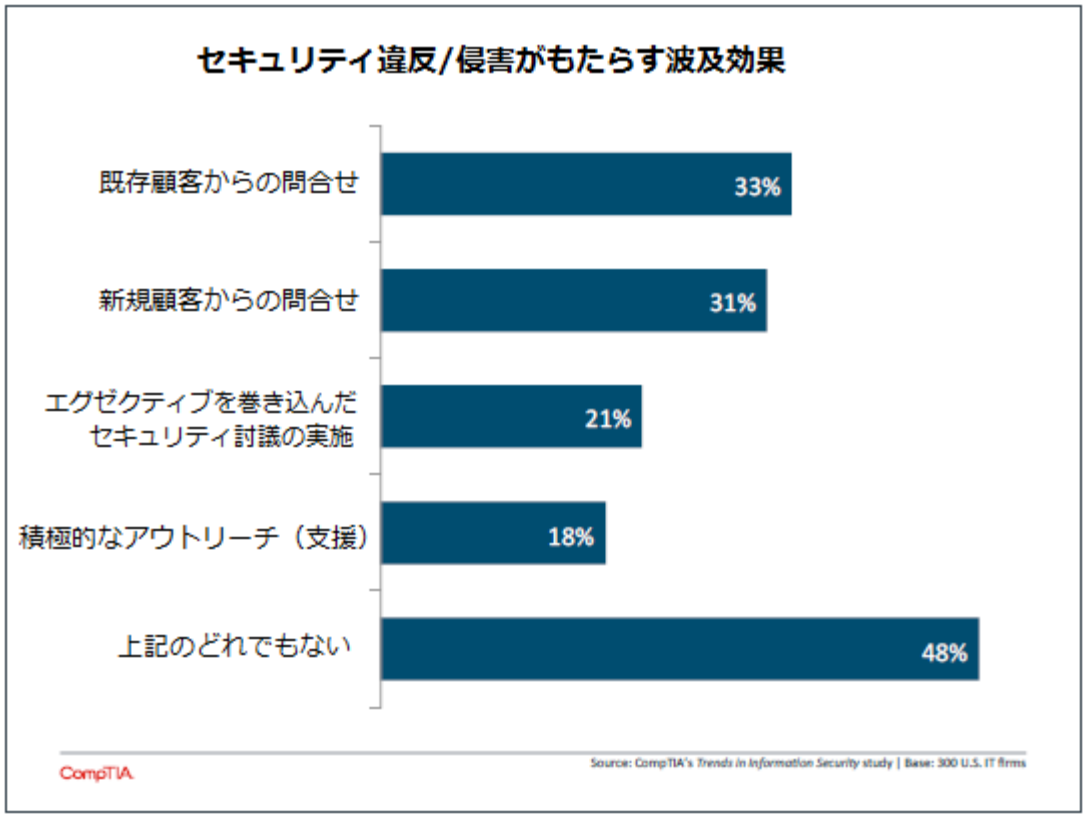
セキュリティにもっと焦点が当たり、明確なテーマとして扱われるようにするための第一歩は、正しい方法でセキュリティの会話をすることです。セクション 1 で述べたように、セキュリティの重要性を強調することは、会話を始めるには最良の方法ではありません。ほとんどの会社がセキュリティの重要性をすでに理解しているからです。IT への内部的変更やビジネス運営の変化を使うことが、特定の取るべきセキュリティ行動を際立たせる、より有効な方法と考えられます。

頻繁にトップニュースとなっているセキュリティインシデントも、チャネル企業にとってのもう一つのエントリポイントになるでしょう。Target や Sony Pictures、そして Heartbleed に至るまで、セキュリティ侵害とループホールは、ますます報道の主流になり、攻撃者の多様な攻撃方法や動機に注目が集まっています。

多くのチャネル企業では、インシデントの結果として、既存/新規顧客からの「問い合わせ」を受けています。ある企業では、積極的なリーチアウトを行い、事業幹部（エグゼクティブ）間におけるセキュリティ討議実施の必要性を感じています。しかし、多くは新たな活動に注視していませんし、どのような行動も取っていないのです。セキュリティに関する包括的プラクティスを構築するには、まず、全体の状況をもっと認識し、よくあるミスに注目した上で、これらのミスを低減し、顧客が自社のセキュリティに真に自信をもてるような計画を提示することです。

すべての人のための場所

LogicNow のパートナーコミュニティのディレクターとして、Dave Sobel はチャネル界に起きた変化を最前列で見てきました。Sobel と彼のチームは、LogicNow の MAXfocus MSP プラットフォームに加入している企業-100 か国、12,000 社以上-と仕事をしています。一般的な IT、そして特にセキュリティに関する物事が複雑性を増す中、チャネル企業が増大する需要に応えるために変化を遂げる多くの方法があります。「チャネル界は、多様な新興モデルをいまだ理解できていない状況です。」と Sobel は言っています。「業容は、単一のセキュリティ製品の再販売会社、あるいは単一製品から経常収益を得ている MSP かもしれません。それ以上に、マネージドサービスプロバイダー(MSSP)で、より包括的なソリューションを作り上げるために複数のセキュリティ部分を食い合わせようとしている、マネージドセキュリティサービスプロバイダー(MSSP)であるかもしれません。そして、バーチャル CIO として機能している企業もあります。ビジネス関連事項を深く理解した上で、技術的ソリューションに取り組む前に、開始地点として適切なプロセスを構築しているのです。」興味深いのは、これらすべてのモデルが、予見できる将来に実現しそうであることです。各エンドユーザーのニーズ、予算、そしてテクノロジーへのニーズはそれぞれ異なっています。ですから、モデルの数や組み合わせは、状況によって違ってくるのです。「すべての体系を理解できていないのと同様、すべての相互関係も理解できていないのです」と Sobel は述べています。「多くの異なる種のビジネスが協働して、未来がどのようになるか解明するという大きなチャンスが広がっています。」


セキュリティ違反/侵害がもたらす波及効果
既存顧客からの問合せ
33%
新規顧客からの問合せ
31%
エグゼクティブを巻き込んだ
セキュリティ討議の実施
21%
積極的なアウトリーチ（支援）
18%
上記のどれでもない
48%
CompTIA
Source: CompTIA's Trends in Information Security study | Base: 300 U.S. IT firms