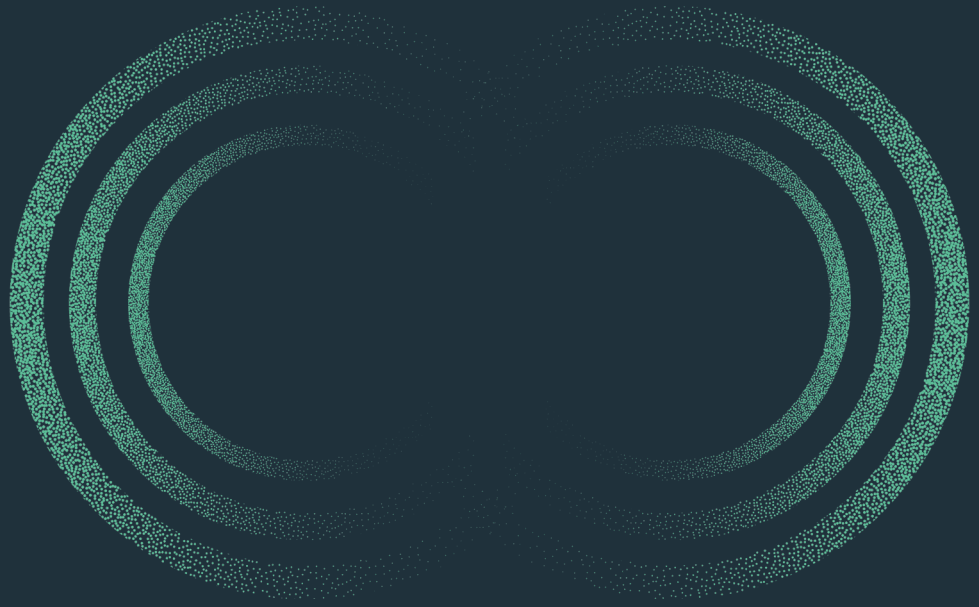
WithSecure™ Pulse 2023

知っておくべき ITサイバーセキュリティの 最新動向

WITH secure

目次



エグゼクティブサマリー

はじめに

WithSecure™では、グローバルで数千人のITプロフェッショナルを対象に、職務／組織／来年度における優先事項などに関するサーベイを実施しました。その結果得られたデータは、2023年以降のIT／セキュリティ戦略に活用することができます。

『Pulse 2023』は、日本／フィンランド／イギリス／フランス／ドイツ／ベルギー／オランダ／デンマーク／ノルウェー／スウェーデン／アメリカ／カナダの12ヶ国で合計3,072人を対象に実施されました。回答者は全員、IT／ネットワーク／クラウドの分野におけるセキュリティの意思決定者やインフルエンサーであり、自社のITセキュリティ製品およびサービスの導入における責任を担っています。

2023年におけるセキュリティの技術的優先事項

本サーベイの対象者は、今後12ヶ月間のビジネスおよびテクノロジーにおける最大の優先事項を回答しました。その結果判明した、サイバーセキュリティのリーダーにとっての技術的優先事項の上位5つは、以下の通りです。

セキュリティの技術的優先順位に関する詳細 (p.10以降) では、『Pulse 2023』サーベイによって明らかになったトレンドの概要を紹介しています。

「興味深い点は、誰も優先事項として選ばなかった選択肢が、実はセキュリティの態勢において最も大きな違いを生むということです。私の経験上、これらは多くの組織が失っているコンピテンシーであり、プラクティスなのです。」

Peter Page

ソリューションコンサルティング部門長

WithSecure

セキュリティの技術的重要課題 (トップ5)

34% データ侵害の防止

29% マルウェアやウイルスからの確実な防御

27% フィッシングやビジネスメール詐欺 (BEC) など、高度な電子メールベースの脅威の防止

27% Office 365やSalesforceなどのクラウドベースのコラボレーションアプリケーションのセキュリティ確保

26% 多様化するデバイス／サービス／ソフトウェアのセキュリティ確保

セキュリティへの支出

サイバーセキュリティが注目を集めている現在、企業にとって最も重要な問題は、おそらく損益でしょう。セキュリティにどれだけの予算をかけるべきなのか？いくら使えば十分なのか？従業員数／地理的条件／業種によって、必要となる予算は異なるのでしょうか？他社はどれだけセキュリティに注力しているのか、実際にどれだけの予算を割いているのか、従業員たちは理解しているのでしょうか？

当社のサーベイでは、企業がサイバーセキュリティに割く予算について、興味深いインサイトを得ることができました。このデータは、企業が戦略を進化させるにつれて、コストが重要な要素ではなくなりつつあることを示唆しています。

86%

86%の回答者が、今後12ヶ月の間のセキュリティ予算を増額する予定であると答えています。

「私は常々、最低でも5%から始めるべきだとお話ししています。お客様にとってセキュリティが重要であればあるほどその比率は高くなり、その逆も然りです。」

Teemu Mylykangas
B2Bプロダクトマネジメント担当ディレクター
WithSecure

「企業は、望んでいるセキュリティレベルを明確にする必要があります。どの程度のリスクを許容できるか、どの程度の事業中断を許容できるか、リスクを取るだけの意欲はどの程度あるかについて決定する必要があります。それに基づき、合理的なセキュリティ支出を決定することができるのです。」

Paul Brucciani
プロダクトマーケティング部門長
WithSecure

データレジデンシー (データの保存場所)

『2023 Pulse』サーベイによってでは、IT部門の人々は組織のデータがどこに保存され、処理されるかについて強い意見を持っていることが明らかになりました。当然といえば当然ですが、データに関する規則／規制、そしてデータの誤用や不正使用に関する多くの事例がこのテーマを深刻なものにし、多くの人々を感情的にしていることは驚くに値しません。

また、組織の規模やリージョン／業種によって意見が分かれる傾向がありました。

データの正しい扱い方について多くの意見があるとき、どのようにしてコンセンサスに達することができるでしょうか？組織のデータレジデンシーに関する方針は、顧客との関係に影響を与えるのでしょうか？多くの場合、規制当局とプライバシー保護活動家は強力な影響力を持っています。

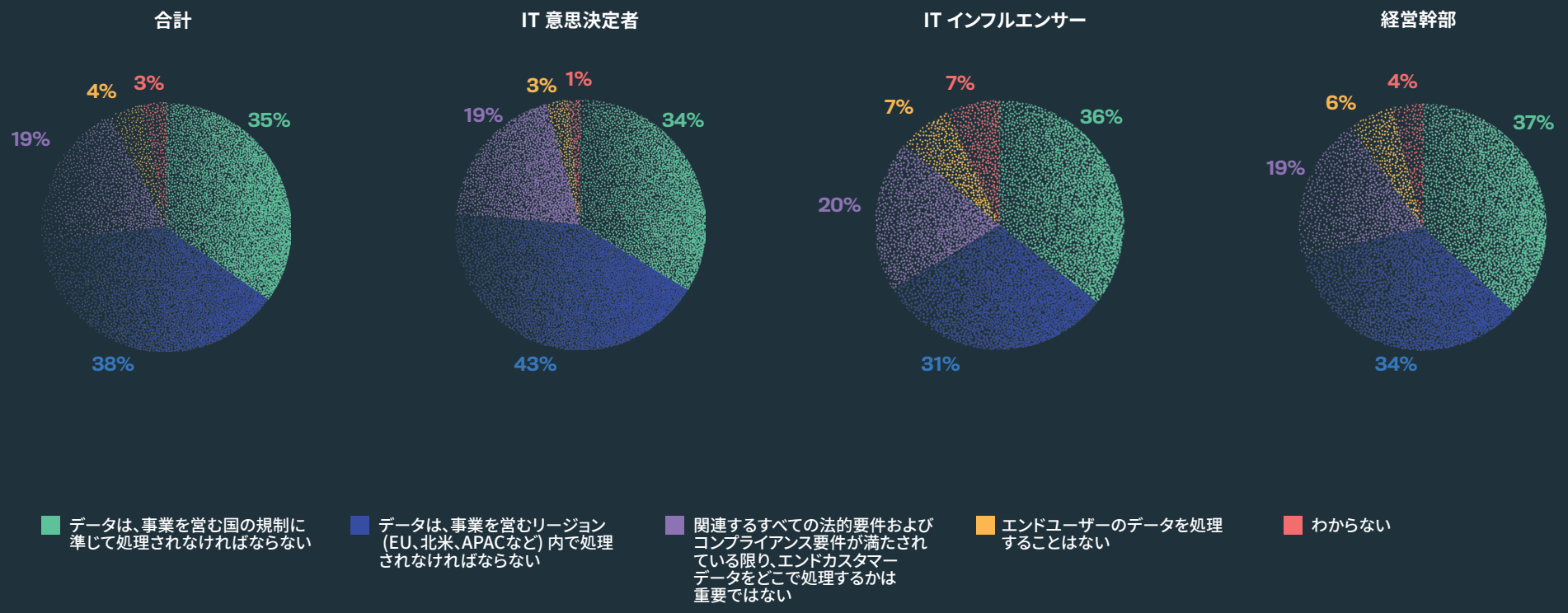
おそらく最も重要な疑問は、意見の相違がなぜ存在するのかということでしょう。意見の相違や誤解は、特に同じ組織内のITインフルエンサーや意思決定者との間で問題を引き起こす可能性があります。プライバシーと保護に関しては、ミスは許されないのです。

「『データレジデンシー』は現在、企業として必ず考慮すべきことです。なぜなら、たとえば新興企業が米国のクラウドサービスプロバイダーを利用したSaaSを提供している場合、米国以外の顧客が国家安全保障に関する問題に懸念を抱いていることがあるからです。そうした場合、そうしたサービスを継続することができるのでしょうか？ 以前と同じペースでイノベーションを続けられるのでしょうか？ それとも代替ソリューションを見つける必要があるのでしょうか？ そういった問題を考慮すべきなのです。」

Albert Koubov Gonzalez
コンサルタント
WithSecure

データレジデンシー (データの保存場所)

あなたの業務上、データ処理において地理的な問題はどの程度重要ですか?

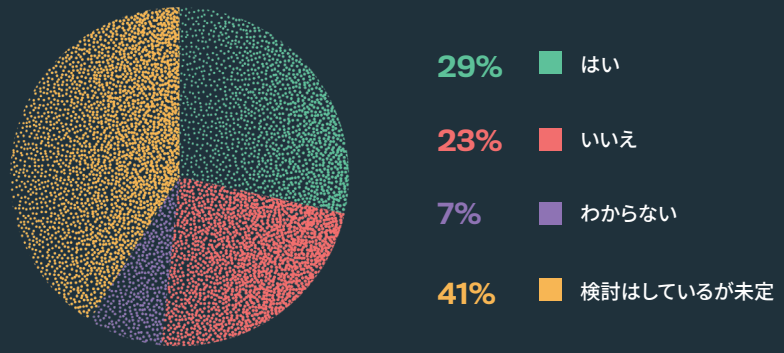


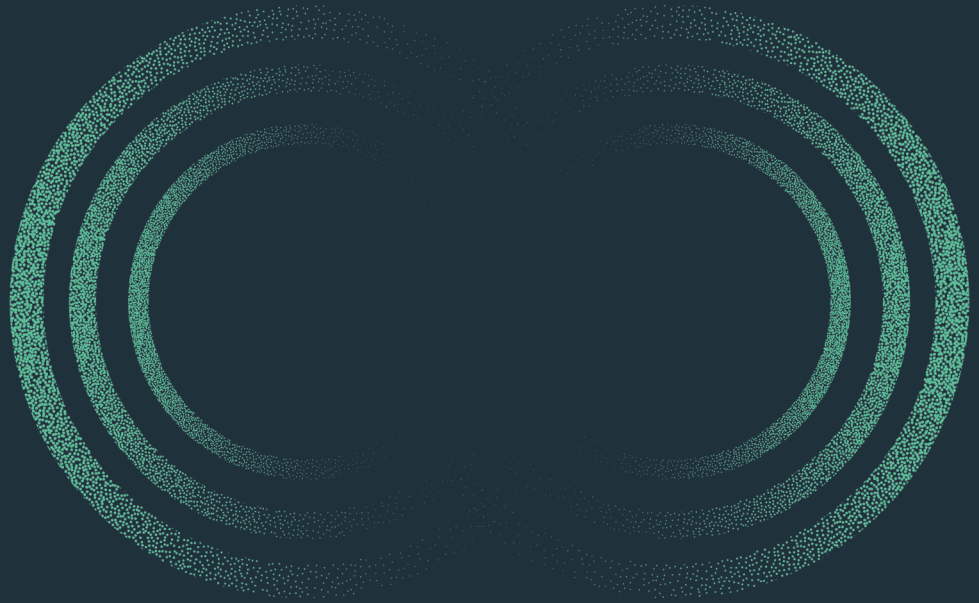
ベンダーの乗り換え

セキュリティベンダーの乗り換えは大変なことです。そのためには膨大な時間とリソースを費やすことになります。にもかかわらず、『Pulse 2023』サーベイでは、過去6ヶ月間にベンダーを変更したという回答は30%を超え、さらに約30%が「今後6ヶ月間にベンダーを変更する予定である」と回答しています。

これは、ベンダー乗り換えの大きな波が押し寄せていることを示しています。それは何故でしょうか？そして何が犠牲になるのでしょうか？

あなたの会社／組織は、今後6ヶ月以内にビジネスITセキュリティソリューション／ベンダーを変更する予定がありますか？



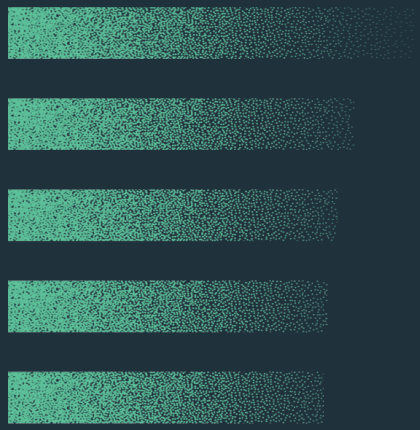


1.

2023年におけるセキュリティの技術的優先事項

セキュリティの技術的優先事項

最も重要なセキュリティの技術的優先事項



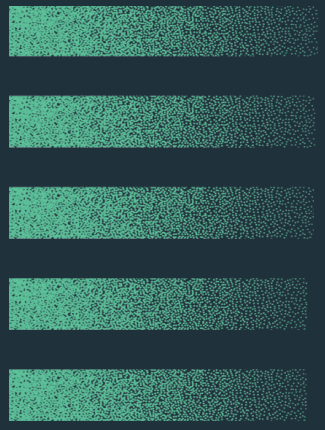
34% データ侵害の防止

29% マルウェアやウイルスからの確実な防御

27% フィッシングやビジネスメール詐欺 (BEC) など、高度な電子メールベースの脅威の防止

27% Office 365やSalesforceなどのクラウドベースのコラボレーションアプリケーションのセキュリティ確保

26% 多様化するデバイス／サービス／ソフトウェアのセキュリティ確保



26% 他のセキュリティ対策を回避した可能性のある攻撃の検出

26% 未知の脅威 (ゼロデイ) に対する継続的な防御

25% AzureやAWSなどのパブリッククラウドのセキュリティ確保

25% 悪意のある内部関係者による脅威への対策や制限

25% パッチなどのソフトウェア脆弱性への適切な対処の徹底

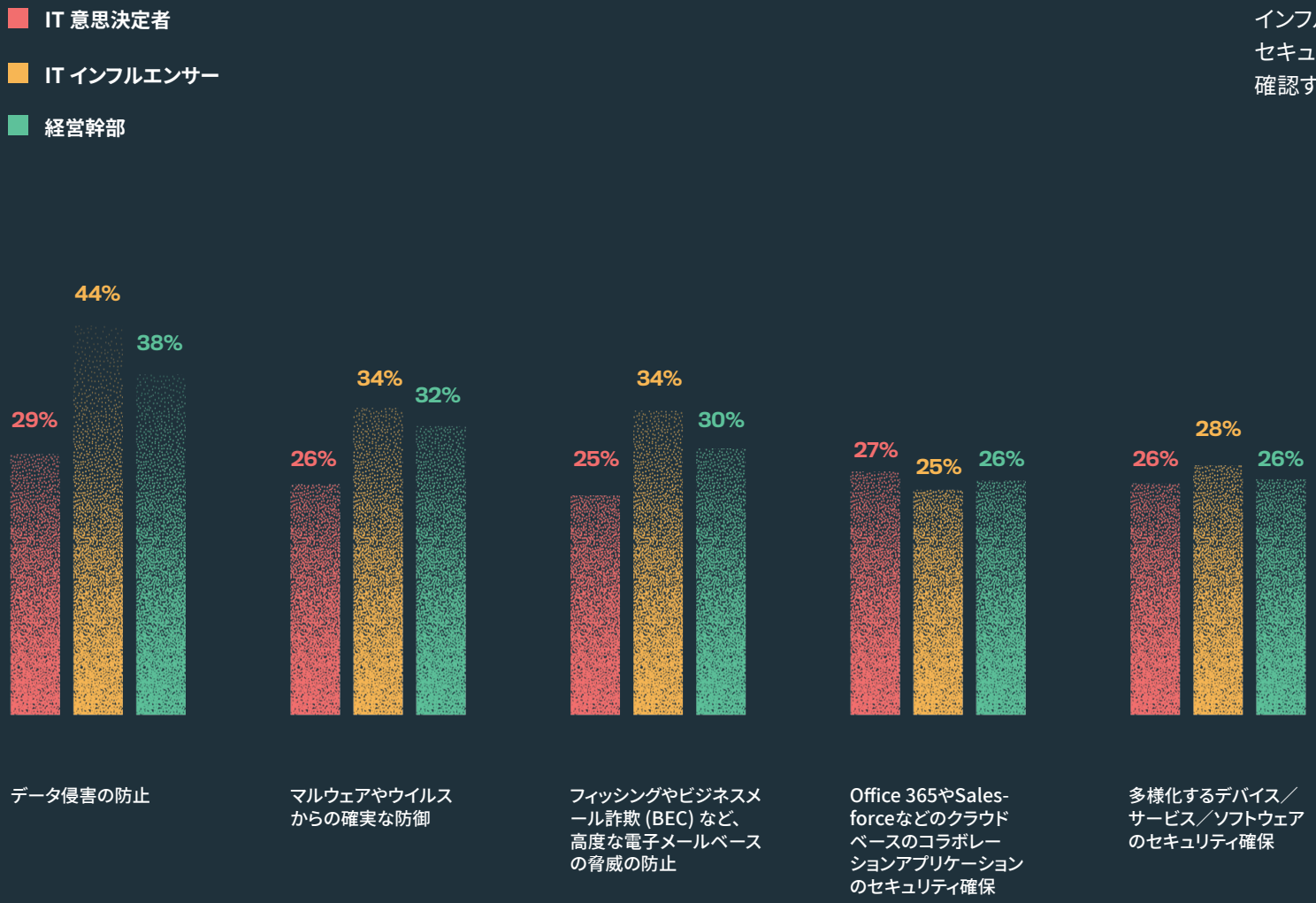
サーベイの結果、どの技術的な優先事項が最も懸念されるのかについて、幅広くコンセンサスが得られているという結果が得られていることがわかりました。1位は予想通り「データ侵害の防止」(33.7%) でした。電子メールベースの脅威の防止や、Office 365やSalesforceなどのクラウドベースのコラボレーションアプリケーションのセキュリティ確保も上位にランクインしています。その他は、概ね脅威の検知と対応というテーマに沿った課題が選ばれています。

「興味深い点は、誰も優先事項として選ばなかった選択肢が、実はセキュリティの態勢において最も大きな違いを生むということです。私の経験上、これらは多くの組織が失っているコンピテンシーであり、プラクティスなのです。誰もが、EDRやコンサルティングといったソリューションで攻撃を防ぐことに関心を寄せていますが、これはどちらも非常に重要なものです。EDRは、堅牢なソリューションを構築するために、EPPに加えて導入する必要があります。さらに、実際に持続的に影響を及ぼす通常業務における課題が見過ごされています。それは社内で推進する必要があり、多くの場合非常に困難な作業になります。セキュリティ文化の醸成をアウトソースすることはできないのです。」

— Peter Page　ソリューションコンサルティング部門長　WithSecure

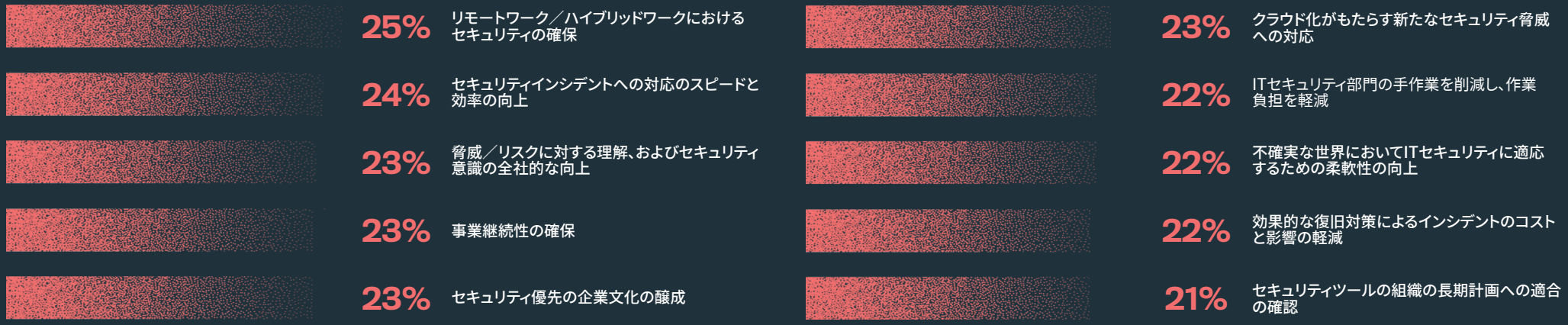
職務別の技術的優先事項　トップ5 (2022年3月)

このデータは、2023年における技術的優先事項のトップ5について、IT意思決定者／ITインフルエンサー／経営幹部ごとの割合を示しています。ここでも、回答者の間で、現在の最大の優先事項が何であるかについて、共通した見解が示されています。しかし、「データ侵害の防止」など、IT意思決定者とITインフルエンサーの間で食い違いがある事項については、セキュリティ部門の全員が同じ考え方に立っているかどうかを確認する価値があるかもしれません。



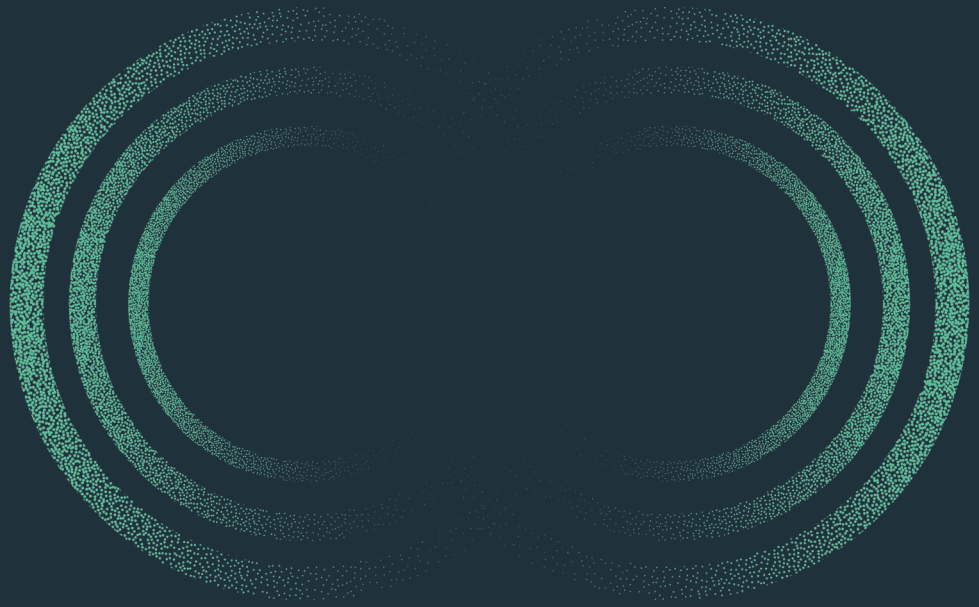
ビジネスにおける成果

ビジネス上の最大の成果 (アウトカム)



『リモートワーク／ハイブリッドワークにおけるセキュリティの確保』という課題が最も懸念されているのは当然といえば当然です。COVIDにより2020年に働き方が大きく変化し、組織がそれに適応できるように多くのガイダンスやアドバイスが提供されてきました。それは多くの人にとって、ITアーキテクチャの変更 (例えば、クラウドへの移行) や従業員の再教育を含む大規模なプロジェクトとなりました。現在はこれが最も懸念される項目となっていますが、2024年に再度このサーベイが実施される頃には、ほとんどの組織が適応し、誰もが新しい働き方に慣れ親しみ、安定した状態になっているであろうことを願うとともに、それに大きな期待を寄せています。」

— Peter Page　ソリューションコンサルティング部門長　WithSecure



2.
セキュリティへの支出

セキュリティには、どの程度の費用をかけるべきでしょうか？

これは世界中の何千もの企業から寄せられる質問ですが、IT予算のうちどれだけをサイバーセキュリティのために費やすべきなのでしょうか？

世界の情報セキュリティ市場は、2024年には1,747億USドル規模に達すると予想されています。これは、変化し続ける世界において、サイバーセキュリティの重要性が高まっていることを示す驚異的なデータであり、企業がセキュリティへの投資を増やすことで、高まり続ける脅威に対応していることを示唆していると言えます。

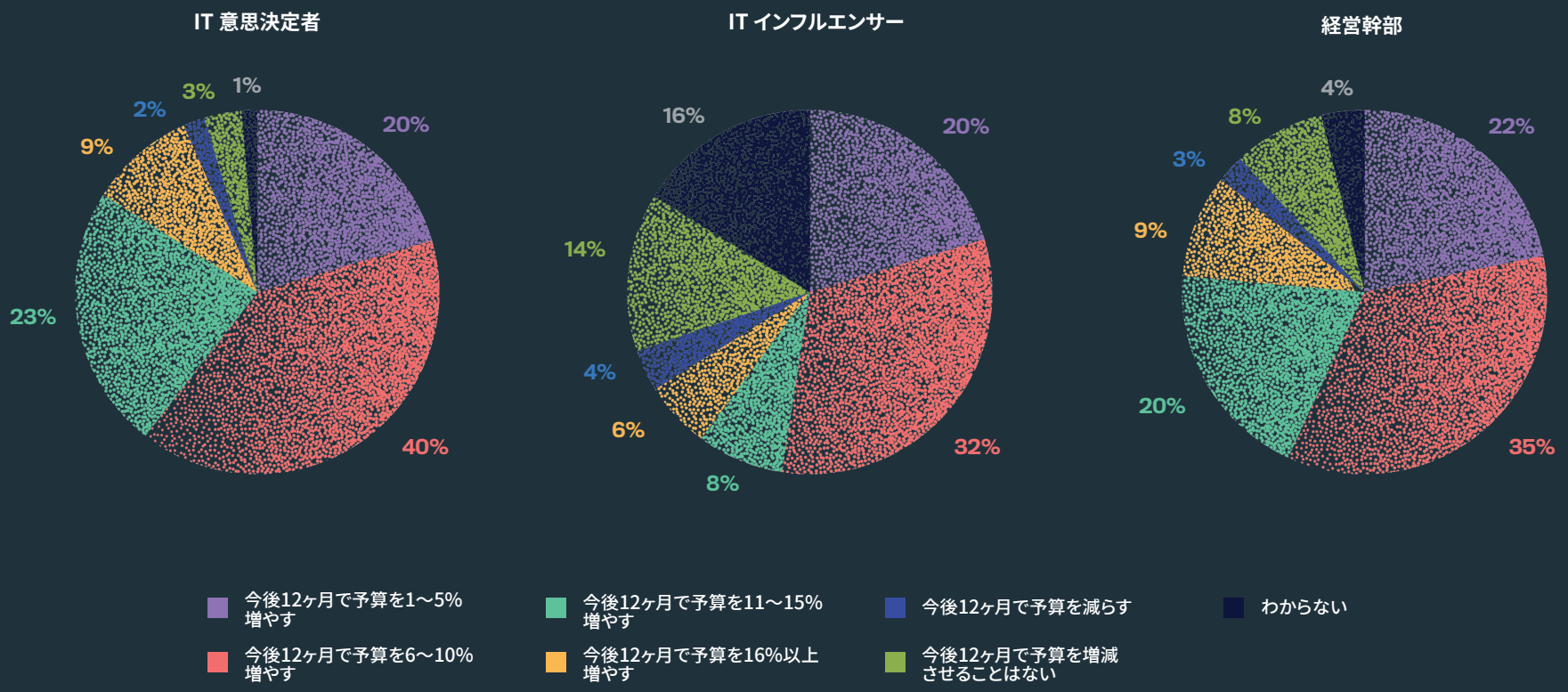
攻撃者の巧妙化、リモートワークの継続、世界的な地政学的状況など、さまざまな要因から、企業はどの程度のセキュリティがあれば十分で、それを得るためにどれくらいのコストを費やせばいいのでしょうか？

当社のサーベイでは、EUに拠点を置く企業の87.9%が、今後12ヶ月の間にセキュリティ予算を増額する予定であることが明らかになりました。それ以上に意外だったのは、8.3%がサイバーセキュリティにかけている費用で十分にカバーされていると感じているか、削減することを積極的に検討する意向を示していることです。

また、来年度の予算については職務によって大きな相違が見られます。IT意思決定者と経営幹部の回答者は大筋で一致しているようですが、ITインフルエンサーが予算に対して持つ期待とは大きく異なるケースがあるようです。混乱や土壇場での決定などの状況を避けるためには、セキュリティ関連の支出というテーマについてはステークホルダー間での早期の明確なコミュニケーションが重要となります。

こうしたケースに精通しているWithSecureB2Bプロダクトマネジメント担当ディレクターであるTeemu Myllykangasは、次のように語っています。
「企業に十分なセキュリティ投資をしているかどうかを尋ねると、企業は答えに窮します。もし、「はい」と答えたら、情報漏えいが発生した場合、人々は自分たちを守るために投資したにもかかわらず、どのように情報漏えいが発生したのかを知りたがり、自分たちに大きなダメージを与えることになります。もし「いいえ」と答えたら、その人たちは自分たちの仕事が正しく行われているか、ビジネスの安全性が確保されているかを疑うはずです。この質問に対する簡単な答えはありません。そうでないと言う人は、嘘をついているか、偽物を売ろうとしているかのどちらかです。IT業界では、一般的に企業は毎年予算の3%から15%をセキュリティ対策に費やしていると言われていまが、その幅のうちどの程度が適切なのかについては、私は常に、最低でも5%から始めるべきだと助言しています。セキュリティがお客様にとって重要であればあるほどその割合は高くなりますし、その逆も然りです。リスク評価と脅威のモデル化から始めてROIを定義し、広く知られた基本的なセキュリティのフレームワークを使ってその投資の適切な使い道を決定するのです。」

職務別のセキュリティ予算への見通し



リスク評価が重要

「セキュリティコストの充足度判断のための経験則を見出すことは非常に困難です。変数が多すぎるのです。企業のIT予算に占めるセキュリティ支出の割合は、状況によって10倍もの開きがあります。5年前には10%程度でしたが、その後上昇しました。セキュリティが極めて重要と考える企業では、IT予算の約12〜15%がセキュリティに費やされています」と、WithSecureのプロダクトマーケティング部門長であるPaul Bruccianiは述べています。

まず考えるべきは、自社にとっての脅威とは何か？ということです。最悪のシナリオが起こったと場合、どのような結果になるのか、年間損失予想額 (ALE) がどれくらいになるのか、そしてその確率を算出する必要があります。

通常、企業はその質問に対する適切な回答を持ち合わせていないため、当社のようなセキュリティのプロフェッショナルが必要とされます。インシデント対応における豊富な経験から、当社はリスク要因に対するALEをプロットし、企業がセキュリティに費やすべき金額を算出することができます。

リスクアセスメントについて、Bruccianiはこう語っています。「リスクを特定できれば、その後はそのリスクをどうするかということになりますが、選択肢は3つです。まず、リスクを転嫁する。例えば、サイバーセキュリティ保険に加入することです。次に、適切なセキュリティ管理／技術／サービスを利用してリスクを軽減すること。最後に、リスクを受け入れ、リスクと折り合いをつけながら物事に対処することです。基本的には、リスクをどの程度低減できるかを検討し、その結果、セキュリティのためにどの程度の予算を確保する必要があるかの判断をすることになります。どの程度のリスクを許容するか、リスク許容度のレベル、そして自社にそのリスクを吸収する能力があるかどうかを判断する必要があるのです。」

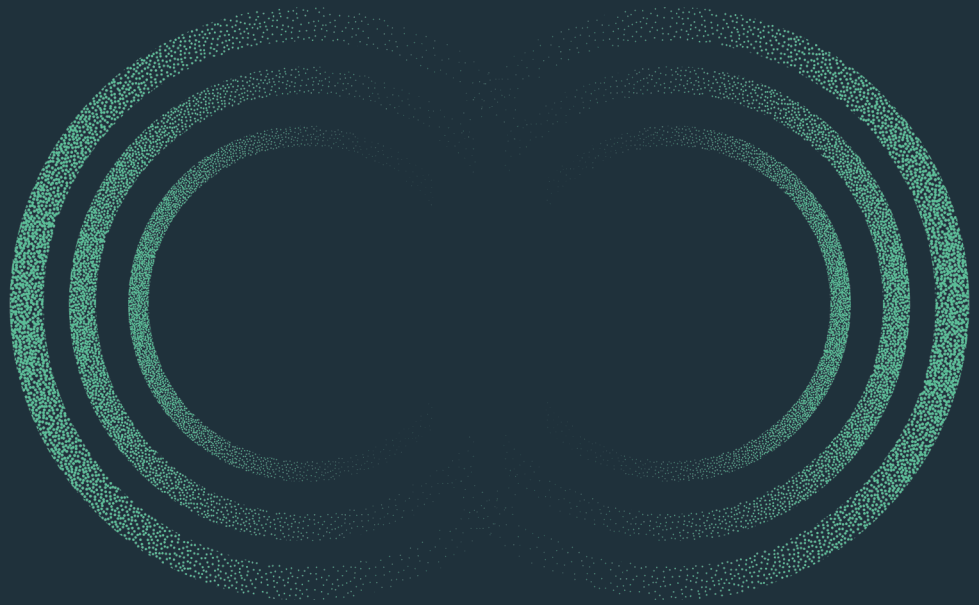
これらは、CFOが決定しなければならない問題です。そうして初めて、予算と不測の事態のための予備予算、リスクへの対処方法などを決定することができるのです。

単にコストの問題だけではない

企業のセキュリティ管理は、コストをはるかに超越するものであると認識することが重要です。数多くの要因がありますが、当社のサーベイはまさにこの点を証明しています。サーベイでは、わずか13.2%の回答者が、セキュリティベンダーを選択する際に最も重要な点は最低価格であると回答しています。一方、5分の1以上 (21.8%) が24時間365日のサポートを最も重要視しており、さらに16.7%がベンダーの信頼性を重要視しています。

セキュリティにどれだけのコストをかけるべきかを決める確実な方程式はありませんが、WithSecureは、お客様を可能な限り保護するために取ることのできる、論理的で防衛的な方法を提供することができます。さらに、価格は常に重要な問題ですが、セキュリティは企業の損益をはるかに超えるものなのです。

WithSecure™ Elementsは、リスク／複雑性／非効率性を軽減するのに役立ちます。強力な予測／予防／対応のセキュリティ機能を組み合わせ、その全てを単一のセキュリティセンターで管理／監視します。



3.

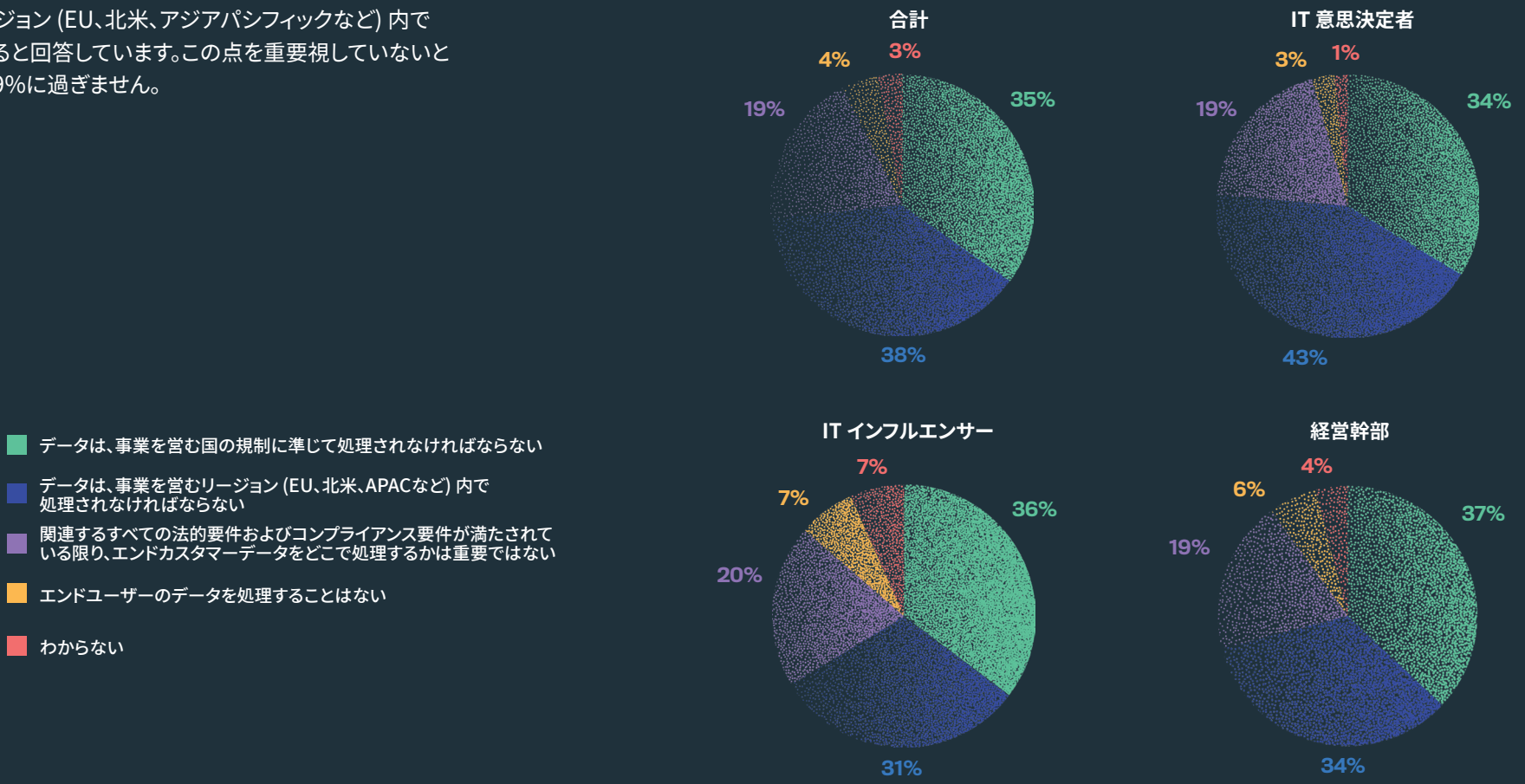
データレジデンシー (データの保存場所)

自分のデータがどこに保存されているかご存じですか？

人々は、自分のデータがどこに保存され、処理されるかについて懸念を抱いています。

『2023 Pulse』サーベイの結果から、データの保存／処理場所に対する強い関心が浮き彫りになりました。回答者の73%近くが、データは事業と同じ国、またはリージョン (EU、北米、アジアパシフィックなど) 内で処理される必要があると回答しています。この点を重要視していないと答えたのは、わずか19%に過ぎません。

あなたの職務上、データ処理の際に地理的な位置をどの程度重要視していますか？



データの保存場所

IT意思決定者の42.8%が、リージョン別でのデータ処理が必要と考えているのに対し、ITインフルエンサーではそれが30.9%にとどまっています。この回答は、リージョンごとの処理か国単位での処理かが明確でないこと、そして回答者のグループによって優先順位が異なることを示唆しています。ここに、職務別の回答のギャップが存在することがわかります。

特定の企業規模グループ (従業員数500〜999名および5,000名以上) では、リージョン別の処理が望ましいとする回答者が多く、また、顧客データがどこに送られるかはさほど重要ではないとの意見もありました。

こうした考え方は企業規模によって異なります。大企業の回答者は、「データは自社が存在するリージョン内で処理されなければならない」と考える人が、「どこで処理されるかはあまり重要ではない」と考える人よりも多くなっています。

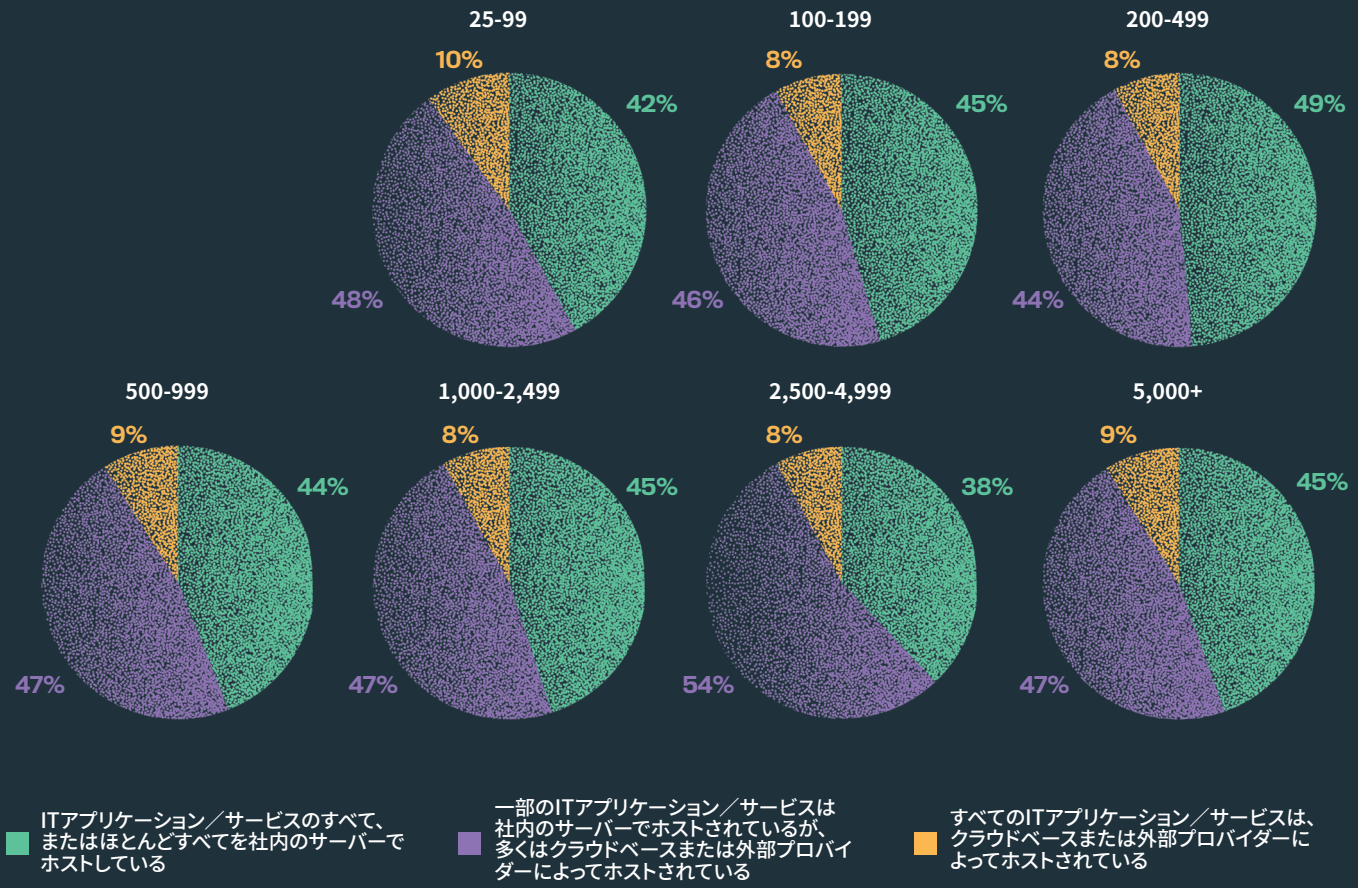
強力なデータレジデンシーが好まれるのは、ルールの面でも物理的な事象の面でも、大きな激動と変化の結果かもしれません。データ主権 (個々の国が国境内でデータを扱うためのルール) は、コンピューティングとデータ処理のグローバル化／地域規制／地政学／戦争／政変などの競合する力の間で引っ張り合い、結果としてリスクを減らしたいという欲求が生まれました。このような背景から、自分のデータがどこにあり、どこを経由してどこへ移動するのかに注目が集まっています。

データを処理する場所

ここで少々予想に反することがあります。私たちは常にいかにクラウドがすべてを変えるかについて聞かされていますが、それはどうやら本サーベイの回答には反映されていないようです。

アプリケーションを社内でホスティングするか、クラウドでホスティングするか、どちらが多いかによって、回答者の意見が異なることはありませんでした。従業員2,500人以上の組織および北米の企業では、社内でアプリケーションをホストする傾向がやや強く、デンマーク／スウェーデン／ドイツ／イギリスの回答者は、オンプレミスよりもクラウドを好む傾向が強いという結果となりました。すべてをクラウドで処理する先進的な組織は6.2%から12.1%となっています。

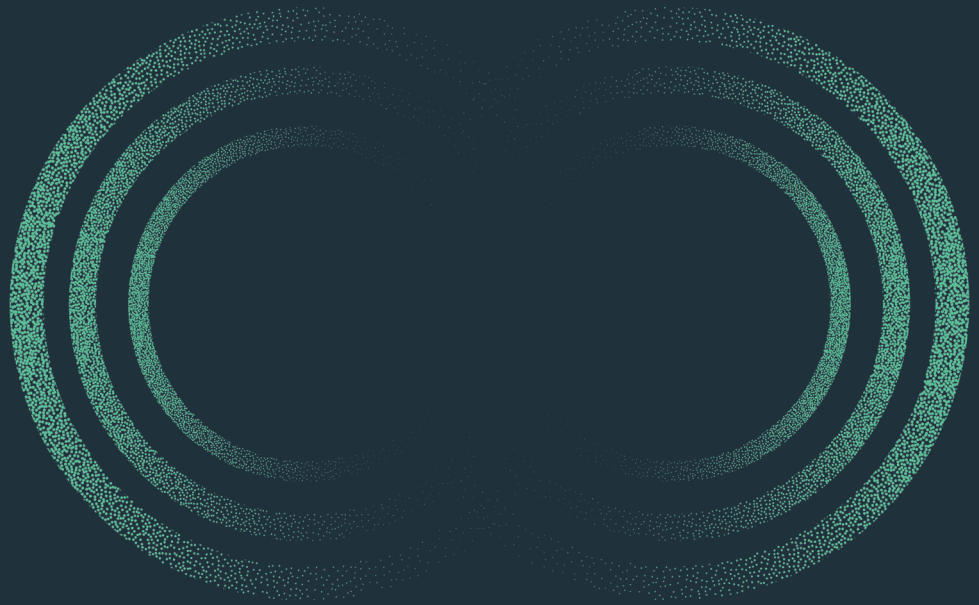
企業規模別IT環境



結論と提言

最終的に、規制要件を満たし、かつ自社の顧客に十分なサービスを提供できるようになるかどうかは、個々の企業次第です。これは非常に複雑な課題です。クラウドをやめて、オンプレミスのデータストレージとデータ処理に切り替えるには、コンプライアンス／セキュリティ／技術的な負担が伴います。当社のコンサルタントからのアドバイスとしては、まずは自社が拠点を構える国のデータ保護規制の要件に従った上で、顧客の懸念や要件を追加考慮していくことです。。

IT意思決定者と、より戦略的な影響力を持つマネジメントとの間で、リージョンごとのデータ処理に関して若干のギャップが見られます。国別とリージョン別の要件の違い、そしてなぜ企業内でこのような意見の違いが生じるのかを理解することが、このレポートを読んでいるみなさんが直ちに着手すべき課題だと考えます。



4.

サイバーセキュリティベンダーの乗り換え

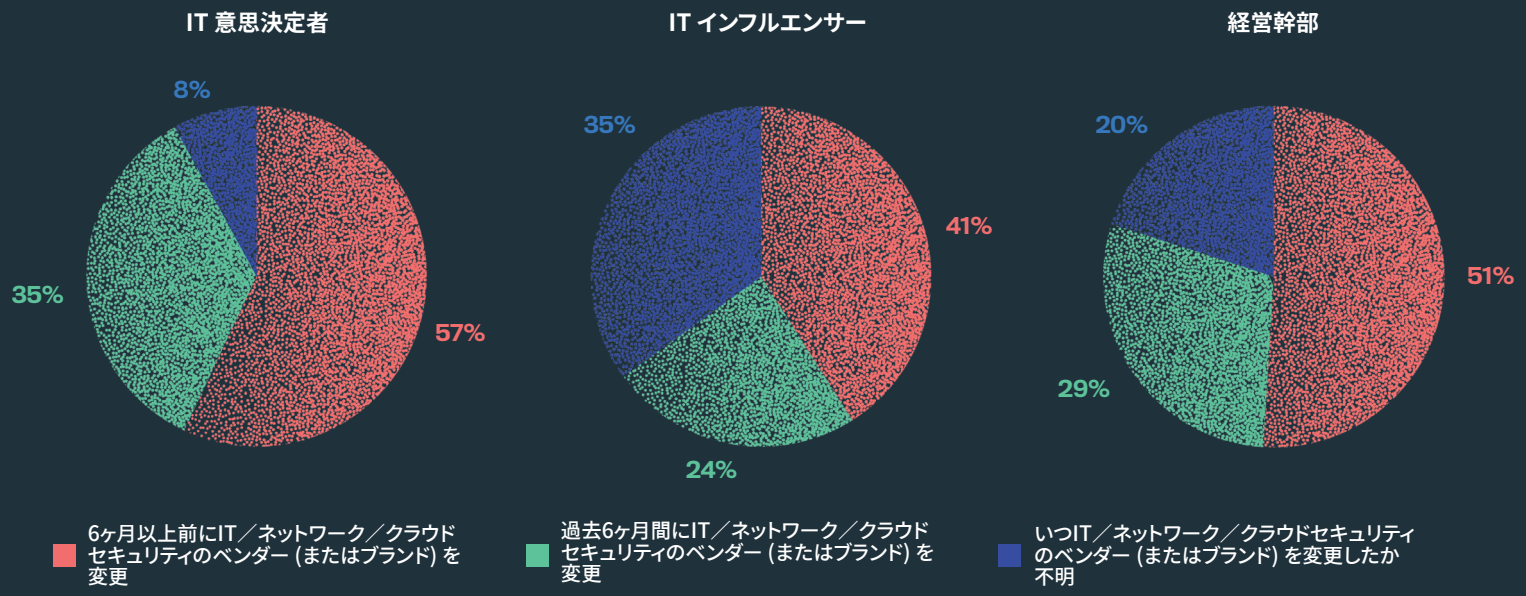
ベンダーの変更は頻繁に起こっている

セキュリティベンダーもサプライヤーも、すべては変化するものです。

今回のサーベイでは、約3分の1にあたる31.9%が6ヶ月以上前にセキュリティベンダーを変更したことがあり、32%が今後6ヶ月間にITセキュリティソリューションまたはベンダーを変更する予定であると回答しています。

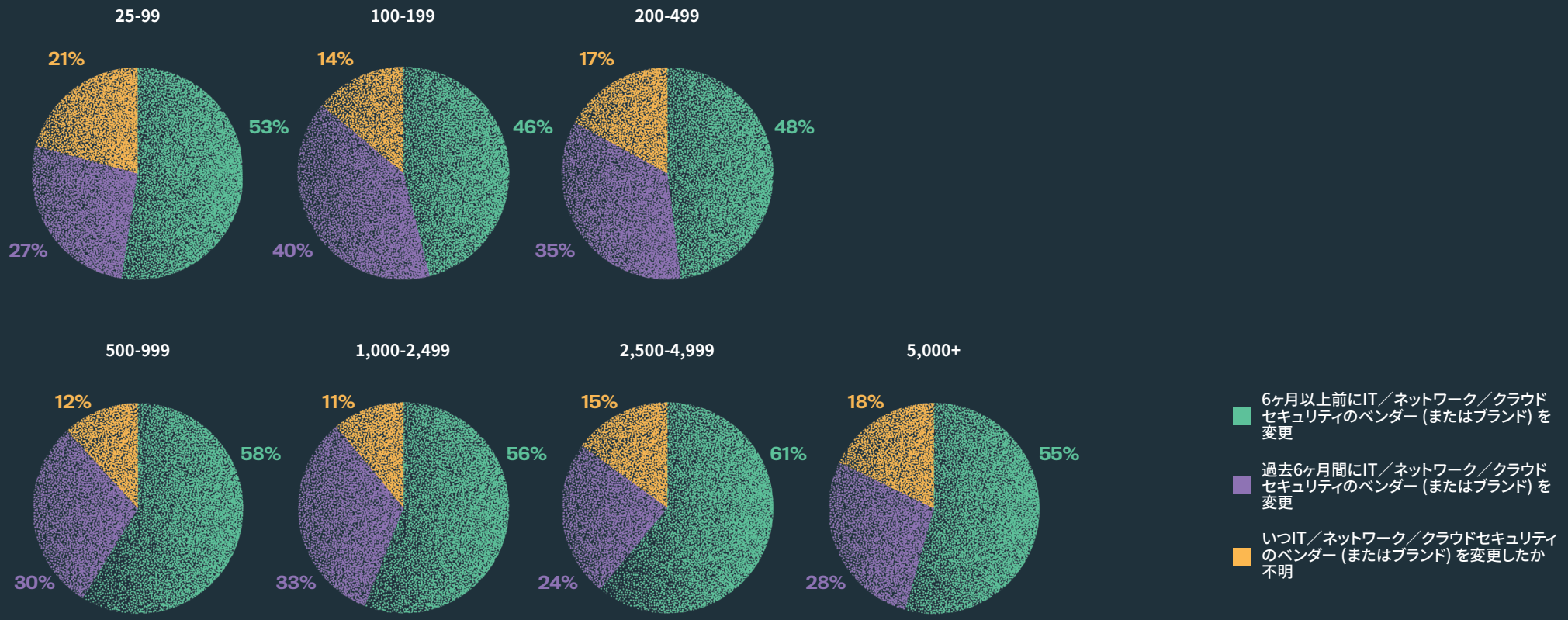
ベンダーを6ヶ月以上前に変更した回答者は金融・保険業では59.4%、ITサービス・テクノロジー業では58.4%。そして今後6ヶ月以内に変更する予定の回答者が金融・保険業では45%、ITサービス・テクノロジー業では41.1%となっており、これらの業界では高い乗り換え率を示しています。

職務別のベンダー／ブランド変更の意向と基準



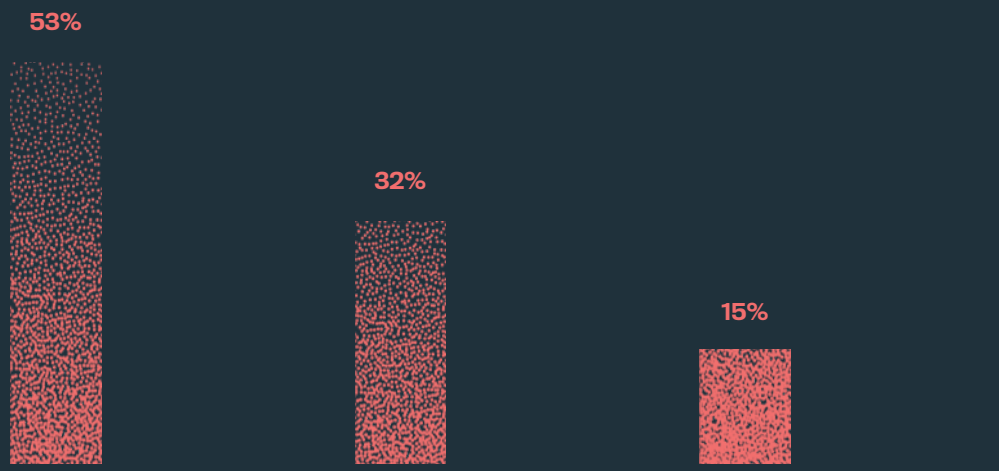
これを企業規模 (n=1,800) で見てみると、大企業よりも
中堅・中小企業で多くの動きがあることがわかります。

企業規模別のベンダー／ブランド変更の意向と基準

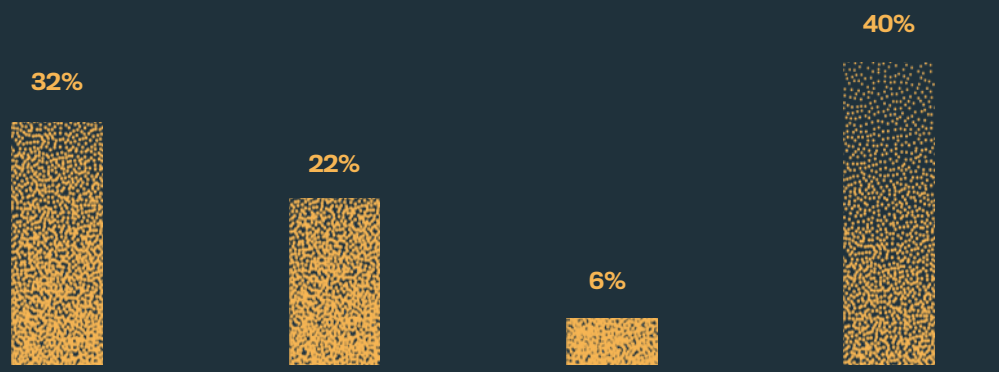


多くの企業にとって、プロバイダーを次々と乗り換える「オールチェンジ」は当たり前のことかもしれませんが、このプロセスは複雑で時間がかかるものです。そこで、当社のソリューションコンサルティング部門長であるPeter Pageに、企業がサプライヤーの乗り換えにどのように取り組むかについて考えを聞きました。また、ベンダーと顧客との間の信頼関係を構築し、維持するためのポイントについても探ってみました。

IT／ネットワーク／クラウドセキュリティのベンダー（またはブランド）の変更について



御社では、今後6ヶ月以内にビジネスITセキュリティベンダーを変更する予定がありますか？



移行プロジェクトでクライアントが最も恐れていることは何か?

リソースが有限であることや制約が存在することは、多くの企業にとって身近な問題であり、あるベンダーから別のベンダーに乗り換えるためには大きな労力が必要となります。簡単に言えば、パフォーマンスの悪いベンダーを切り捨てようとしても、そのために労力がかかりすぎるケースも多く見受けられる、いうことです。しかし、サーベイの回答者たちの話を聞くと、どうやらそうとも限らないようです。

その点について、Pageはこう説明しています。「セキュリティチームは、多くの場合、新しいサービスを導入する担当者ではありません。ソフトウェアを導入するためには、プロジェクトマネジメントやITチームのサポートが必要となりますし、自分たちが行おうとしている変更が、自分たちの責任範囲を超えてビジネスの多くの部分に影響を与えている場合には、ネットワークチームに頼らなくてはなりません。そして、さまざまなステークホルダー全員から賛同を得なければならないのです。」

クラウドサービスの出現で切り替えは簡単になったか?

既に述べたように、クラウドによってセキュリティのニーズや課題が変化してきています。プロバイダーの乗り換えは容易になってきていますが、それはクラウドの性質によるものではなく、ユーザーはオンプレミスのサービス間を切り替えるのと同じように、クラウドサービス間の切り替えをより快適に行うことができるようになってきているということです。

「結局は人次第なのです。クラウドの開発／実装／セキュリティのスキルを持つ人材は、現在、非常に豊富です。セキュリティプロバイダーもそのような能力を持つ必要があります。しかし、境界が変われば、セキュリティサービスも変わります。そのリスクを顧客が理解できるようにする際に、クラウドセキュリティポスチャーマネジメントといったものが求められるのです。」と、Pageは解説しています。

なぜ契約期間が短くなってきているのか?

契約期間の短縮は、サイバーセキュリティ市場の製品やサービスの状況と、CISO (最高情報セキュリティ責任者) の任期が短くなる傾向の2つの要因によるものと思われます。CISOたちの多くは2年未満で他社に転職していくことが多くなっています。

CISOの交代に伴い、要件や決定事項が常に変化するため、市場が不安定になり、そうしたことがベンダーが定期的に入れ替わる一因にもなっているようです。

「また、常に『新しいもの』や『次善の策』を求める傾向があり、それが市場の行動様式となっています。最新／最高のものを買うために使うリソースは、基本的なこと、つまり既に自分たちが持っているものをチューニングすることに使ったほうがいい場合もあるのです。市場には多くのノイズが存在するため、どのようなアプローチが最適なのか理解することは困難です。CISOが複数年にわたる高額なサービスを利用するには、自分たちが必要とする成果、そして経営陣が求めている成果を得られると確信する必要があるのです。」と、Pageは語っています。

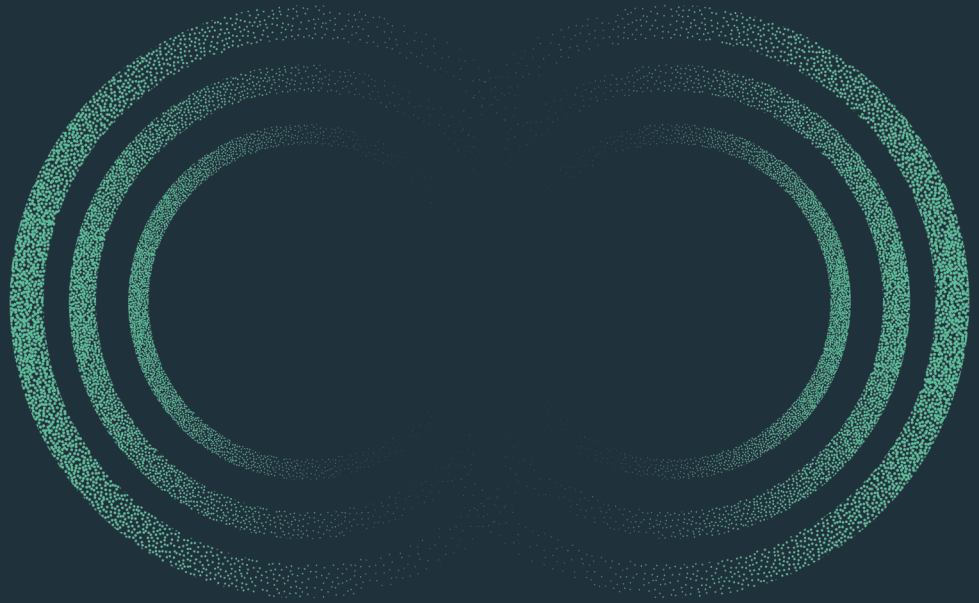
CISOがベンダー乗り換えを決断するのは難しくなっているのか、それとも簡単になっているのか？

「以前は、CISO がサイバーセキュリティに多額の費用を投じることについて、経営陣の理解を得ることは困難でした。経営陣／CFO／CEOは、企業における侵入やランサムウェアの感染を目の当たりにし、財務や企業成果に与える影響を理解することができるようになりました。

しかし、市場の状況により、CISOがこの問題に取り組む方法は実にさまざまです：どこにお金をかけるのか？どこにお金をかけるのか、インソースするのか、アウトソースするのか。MDRとEDR、SIEMとそれ以外ではどうでしょうか。つまり、ほとんど「分析しすぎて麻痺状態になる」ようなものです。選択肢が多すぎるため、RFIを実施し、ベンダーと話すことに多くの時間を費やすことになり、それだけでフルタイムの仕事になってしまいます。」

結局は時間

現在のサイバーセキュリティ市場は議論で騒がしいものの、Pageはセキュリティのためには、どんな決断でも何もしないよりはましだと考えています。
「何もないところから何かを始めるのであれば、資産の可視化や補償ができないので、とにかく決断することが重要になります。しかし、マネージドサービスの場合は、契約の終了日が期限となります。そこで問題となるのが、切り替える予定のベンダーとの交渉開始時期です。CISOは、契約終了日の12ヶ月前から選択肢の検討を始めれば、最良の結果を得られることでしょう。」



5.
まとめ

まとめ

今回のサーベイは、分析にかなりの時間を要しました。サイバーセキュリティの意思決定者は、さまざまな意見や期待を持っていることは明らかです。データを分類して、単に興味深いものではなく、実用的な情報を見つけるのは難しいことです。とはいえ、ここでは私たちが最も適切と考えるインサイトを紹介します。このレポートを読んでいる方の中には、既にご存知の事柄もあり繰り返しになるかもしれませんが、当社のデータもそれらの推測を裏付けるものです。

1) 認識している優先事項が、セキュリティ対策に最も大きな違いをもたらすとは限りません。自分たちの組織に欠けているプラクティスやコンピテンシーを確認し、認識されている優先事項と比較し、そのうえでギャップを見出してください。

2) セキュリティ支出は考え方の問題です。当社のサーベイでは、来年度のセキュリティ予算に関する認識に大きな違いがあることが明らかになりました。期待値のギャップは、混乱／対立／性急な決断をもたらしてしまう原因となります。予算がまだ確定していない、あるいは示されていない場合でも、すべてのステークホルダーが、どの程度の予算であれば変更／購入／達成できるかがわかっていることが、沈着冷静かつ余裕を持った意思決定をする秘訣です。

3) データレジデンシーは極めて重要な問題であり、回答者の70%以上にとって不可欠なものです。しかし、データレジデンシーが保証されないクラウドベースのアプリケーションを放棄して、代替のアプリケーションを使うことの意味を考えることも同様に重要です。

4) ベンダーを変更する場合は、早めに決断してください。移行を成功させるには、契約満了または更新の少なくとも12ヶ月前にキックオフすることを肝に銘じ、また、分析ばかりおこなって麻痺状態に陥らないようにしましょう。

最後に、今回のサーベイのデータでは、対象の職務の間でしっかりと合意やコンセンサスが取られていることが示されました。これは、組織の調和がとれていることを示すものです。ただし、意志決定者／インフルエンサー／経営幹部の間で意見が大きく割れた点もありました。そのような点については全てのステークホルダーが関心を持つべきであり、明確でオープンなコミュニケーションこそが今後1年間において最も効果的なツールになることでしょう。

調査方法

WithSecureが2022年5月にオンラインで実施したB2B市場調査では、フィンランド／イギリス／フランス／ドイツ／ベルギー／オランダ／デンマーク／ノルウェー／スウェーデンのヨーロッパ9ヶ国と、日本／アメリカ／カナダの計12ヶ国の3,072人 (内訳はヨーロッパ: 2,098人、それ以外: 974人) から回答が寄せられました。回答者は全員IT／ネットワーク／クラウドセキュリティの意思決定者／インフルエンサー／経営幹部であり、組織におけるIT／ネットワーク／クラウドセキュリティ製品とサービスの導入に影響力を持つ人々です。

WithSecure™について

WithSecureは™、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を検出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたWithSecureは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。

詳細は www.withsecure.com をご覧ください。
また、Twitter @WithSecure_JP でも情報の発信をおこなっています。

ウィズセキュア株式会社
〒105-0004　東京都港区新橋2丁目2番9号　KDX新橋ビル 2階
Tel: 03-4578-7710 / E-mail: japan@f-secure.co.jp
https://www.withsecure.com/ja_JP/

2022.10 JP

WITH secure