SOPHOS

サイバーセキュリティの解けないパズル

3,100人の IT 管理者を対象とした、ソフォス委託の独立系調査会社による調査結果

ソフォスホワイトペーパー 2019 年 6 月

目次

サイバーセキュリティの解けないパズル

3,100人の IT 管理者を対象とした、ソフォス委託の独立系調査会社による調査結果

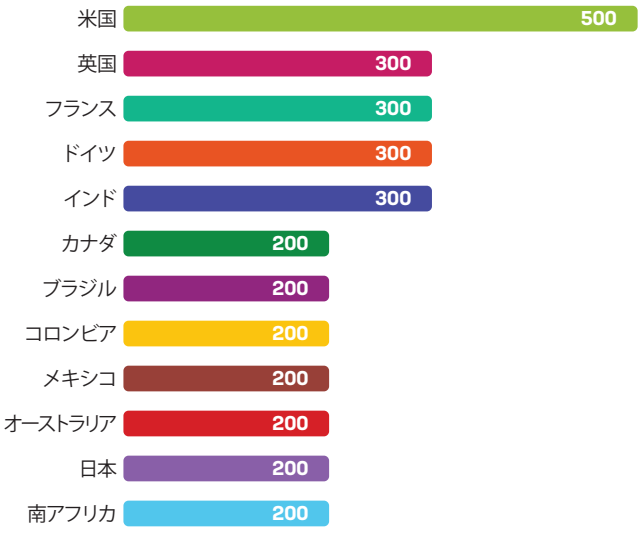
サイバーセキュリティ対策の負担が軽減される傾向は一切ありません。保護テクノロジーが急速に進化し続ける一方で、それを回避するためにサイバー犯罪者が使用する手法も進化し続けています。同時に、脅威の複雑化が進むなか、既に過剰な負担を背負っている IT 部門が対策を強化し続けるのは容易なことではありません。

このような課題を理解するために、ソフォスは、12カ国 3,100名の IT 管理者を対象にした独立アンケート調査を委託しました。リサーチ会社 Vanson Bourne が実施したこのアンケート調査によって、サイバー攻撃のレベルと種類、サイバーセキュリティ管理に伴う問題点の詳細など、興味深い結果が明らかになりました。

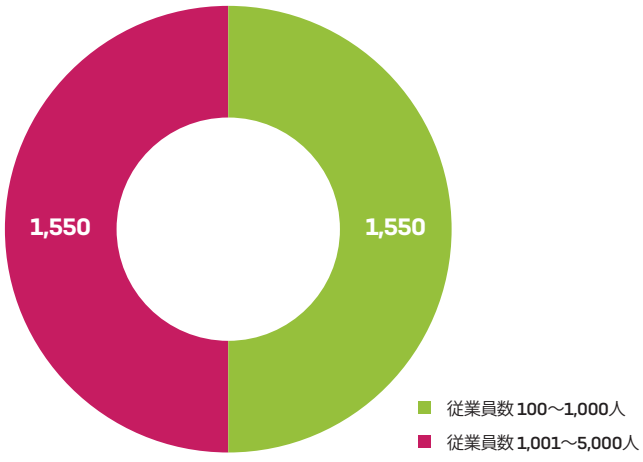
調査

英国のリサーチ会社 Vanson Bourne 社は、2018年 12月から 2019年 1月の間に、IT の意思決定者 3,100人にインタビューを行いました。企業規模による違いを均等に反映させるため、各国で、ユーザー数が 100～1,000人の企業と 1,001～5,000人の企業をそれぞれ同数、調査の対象にしました。

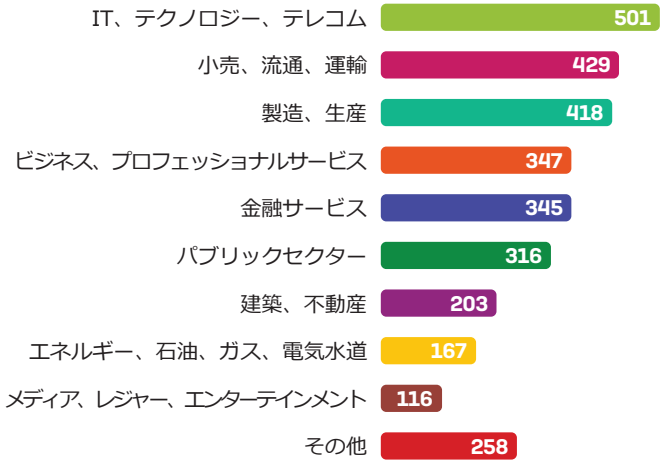
国別の回答者数



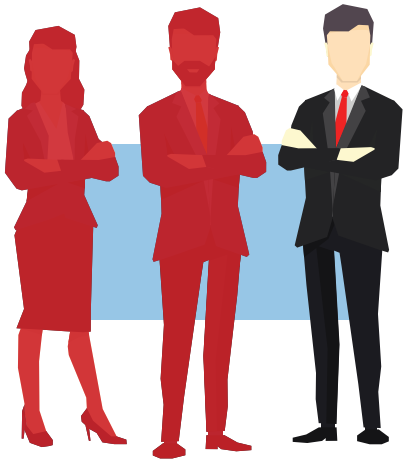
企業規模別の回答者数



業種別の回答者数



2018年では 3分の 2 の企業がサイバー攻撃の被害を受けた



各企業は、昨年、企業内のネットワークやエンドポイントへの侵入を阻止できなかったサイバー攻撃の被害を受けたかどうかという質問に回答しました。68% が「はい」と回答しました。被害を受けた企業に対する平均攻撃回数は 2回でしたが、企業の 10% は 4回以上の攻撃を受けたとしています。

回答した企業の 9割 (90.5%) が、攻撃時 (複数回の攻撃を受けた企業では最も大規模な攻撃を受けた際) に、最新のサイバーセキュリティ対策を実施していたと回答していることは特に懸念されます。調査した国別にみると、最新の保護を実行していた企業の割合が最も高いのはフランス (97.5%) で、一方、最も低いのはコロンビアで、7割 (70.9%) のみの企業が最新の対策を実行していました。

91%
攻撃時に最新のデータ保護対策を実施していた企業の割合

つまり、セキュリティに対する関心の高さや対策にも関わらず、脅威は企業の防御をすり抜けていることを意味します。これは、サイバーセキュリティ対策が十分でない、未対処のセキュリティホールがある、または保護にギャップがあるなどが原因であることが考えられます。また、最新のエンドポイント対策を実施していたからといって、それ以外のデバイスすべてが安全であるというわけではありません。

サイバー攻撃に伴う問題点

IT 管理者は、サイバー攻撃に伴う深刻な問題点として次のような事柄を挙げています。

データ流出：アンケート回答者が最も深刻な問題として挙げた事柄。回答者の 31% が最も重要な問題であるとしており、3分の 2 を超える回答者 (68%) が最も重要な 3つの問題の 1つに含めています。

コスト：回答者の 21% が、被害に対処するためにかかる金銭的および時間 / 労力のコストを最も深刻な問題として挙げています。

企業の信頼に与える影響：半数を超える IT 管理者 (56%) が最も重要な 3つの問題の 1つであるとしており、21% が最も重要な問題であるとしています。

さらに、IT 管理者が自分のキャリアよりも、IT 部門の持つイメージを重視していることは興味深いことで、IT 部門ではチームワークが大切にされているといえます。回答者の 13% は、サイバー攻撃を受けることによって、IT 部門の企業内におけるイメージの低下が最も深刻な問題であるとしており、この割合は、自分の職の安定を第一に挙げた回答者 (7%) のほぼ 2倍です。

相変わらず企業がサイバーリスクの軽減に苦戦している理由

ここで説明した結果が示すように、セキュリティテクノロジーへの投資に関わらず、サイバー攻撃の被害を受けることは今や当たり前になっています。この調査によって、企業がサイバーリスクの軽減に苦戦している主な理由として、次の 3つが明らかになりました。

No. 1 様々な手口を使って攻撃

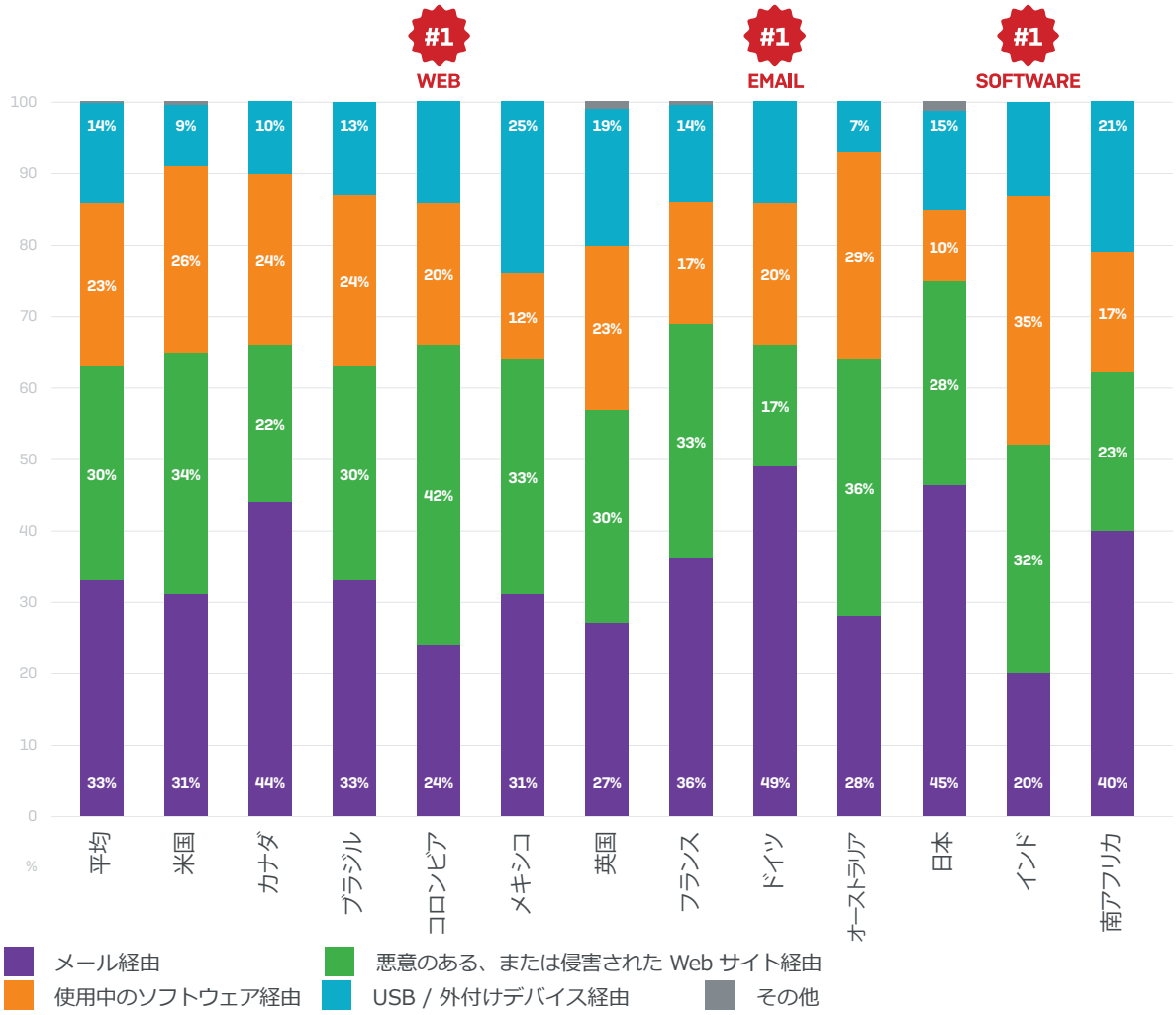
昨年サイバー攻撃の被害を受けた企業は、企業環境に最も被害を及ぼした攻撃の感染経路が何であったかについて回答しました。その結果、攻撃方法がわかっている状況で最も一般的な感染経路はメールで、33% の攻撃で使用されました。フィッシング攻撃が頻繁に行われているなか (詳細は後で説明します)、これは驚くべきことではありません。また Web も主な感染経路で、3割の攻撃で使用されています。両者を合わせると、メールと Web は、企業に侵入する攻撃の 3分の 2 を占めていることになります。

しかし IT 管理者は、メールと Web 対策だけに専念すればよいというわけではありません。攻撃の感染経路の 23% はソフトウェアの脆弱性であり、14% は USB メモリまたは外付けデバイスです。さらに IT 管理者の 20% は、最も被害を与えた攻撃の感染経路を把握していません。感染経路がわからない場合、それを塞ぐことは困難です。

昨年、企業に最も被害を与えたサイバー攻撃の感染経路は何ですか？(整数に切り上げ)
全体数：攻撃の感染経路を把握している回答者 (1,685人)

データを詳細に解析すると、脅威の感染経路は、世界各地で著しく異なることがわかります。第 1位の感染経路はコロンビアでは Web ですが、ドイツではメールであり、インドではソフトウェアの脆弱性となっています。一方、メキシコでは USB メモリ / 外付けデバイスが攻撃の 25% を占めています。

このような違いが発生するのは、サイバー攻撃者が世界各地で異なる感染経路を使用しているからなのか、国によってセキュリティの脆弱性が異なるからなのか、という疑問も沸いてきます。



昨年、企業に最も被害を与えたサイバー攻撃の感染経路は何ですか？
全体数：攻撃の感染経路を把握している回答者 (1,685人)

IT 部門は、サイバーセキュリティ対策を実施するにあたり、さまざまなリスクを考慮する必要があります。各企業は、最も深刻なセキュリティリスクはなんであるかという質問に回答しました。先ほど説明した感染経路を考えると、フィッシング攻撃 (1位) とソフトウェアエクスプロイト (2位) が回答のトップを占めているのは納得がいきます。

しかし、ユーザー (従業員、契約社員、ゲストユーザーを含める) が 3位に位置付けられています。回答者の 44% が、ユーザーによるセキュリティリスクを最も重要な 3つの問題の 1つであるとしており、これは、他のサイバーセキュリティ問題とは異なる課題を IT 部門にもたらしています。

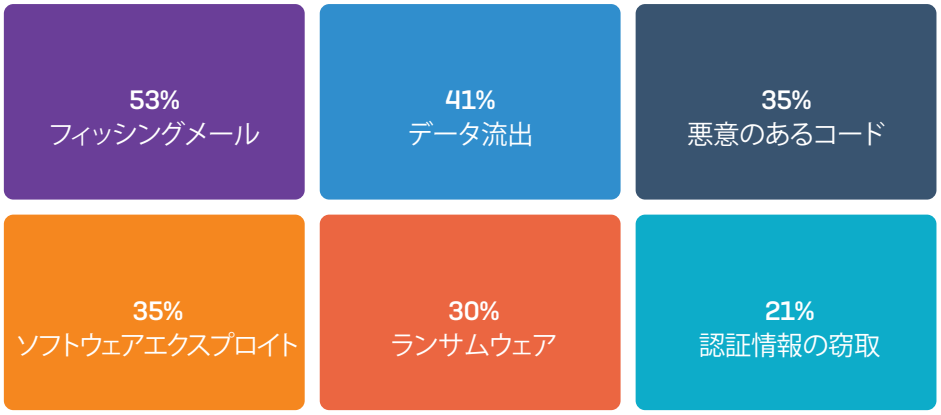
IT 管理者にとって Wi-Fi セキュリティに伴うリスクもまた深刻な問題であり、3分の 1 を超える回答者 (36%) が最も重要な問題の 1つに位置付けています。さらに、回答者の 3割 (31%) が、不明なデバイスを選択しています。

企業が直面する、最も重要なセキュリティリスクは何であると考えますか？
(1位、2位、3位に位置付けられた回答数を合計)：

1. フィッシングメール **50%**
2. ソフトウェアエクスプロイト **45%**
3. ユーザー (従業員、契約社員、ゲストユーザー) **44%**
4. 安全でないワイヤレスネットワーク **36%**
5. 不明なデバイス **31%**

No. 2 サイバー攻撃は多段的で、連係、複合されている

サイバー攻撃の被害を受けた企業の回答者は、昨年企業がさまざまな種類の攻撃を受けたとしています。



昨年、企業に対する、どのような種類のサイバー攻撃を受けましたか？
全体数： 昨年、サイバー攻撃の被害を受けたと回答した企業 (2,109社)

これらの数値の合計は明らかに 100% を超え、多段的な攻撃が今や当たり前になっていることを意味します。たとえば、フィッシングメールが悪意のあるコードをインストールし、それがソフトウェアエクスプロイトを悪用し、それによってランサムウェアがインストールされる場合などが考えられます。また、合計が 100% を超えることは、IT 部門が大規模な問題に直面していることも裏付けています。

フィッシング：最も頻繁に実行されるサイバー攻撃

2018年にサイバー攻撃の被害受けた 2,109社の企業のうち、半数を超える企業 (53%) は、フィッシング攻撃の被害を受けました。事実、フィッシングは、アンケート調査した、コロンビア以外のすべての国で最も頻繁に発生した種類の攻撃でした。コロンビアでは2番目に頻繁な攻撃でした。3,100人の全回答者のうち、3分の 1 を超える企業 (36%) が、フィッシングメールの被害を受けました。

ソフトウェアエクスプロイト：国ごとに異なる被害の規模

サイバー攻撃の被害を受けた企業のうち 3割を超える企業 (35%) は、使用中のソフトウェアにある脆弱性がエクスプロイトによって悪用された結果、被害を受けました。エクスプロイトの被害を受ける可能性の高い企業の割合には、著しい地域差があります。メキシコでは、サイバー攻撃の被害を受けたと企業の半数以上 (51%) が、ソフトウェアエクスプロイト攻撃を受けています。これは、ブラジル (22%) や、南アフリカと日本 (共に 23%) の攻撃の 2倍を上回っています。

ランサムウェア：依然として際立った存在

衰退が噂されているにも関わらず、ランサムウェアは依然として際立った存在になっています。サイバー攻撃を受けた企業の 3割 (30%) は、ランサムウェアの攻撃を受けました。しかしこの数値は世界平均値であり、その影には著しい地域差が潜んでいます：

- 日本の回答者の約半数 (49%) はランサムウェア攻撃を受けており、英国 (43%) がこれに続いています。
- メキシコでは回答者のわずか 5% がランサムウェア攻撃を受けており、コロンビアでも 13% のみです。

No. 3 技術や人材、時間の不足

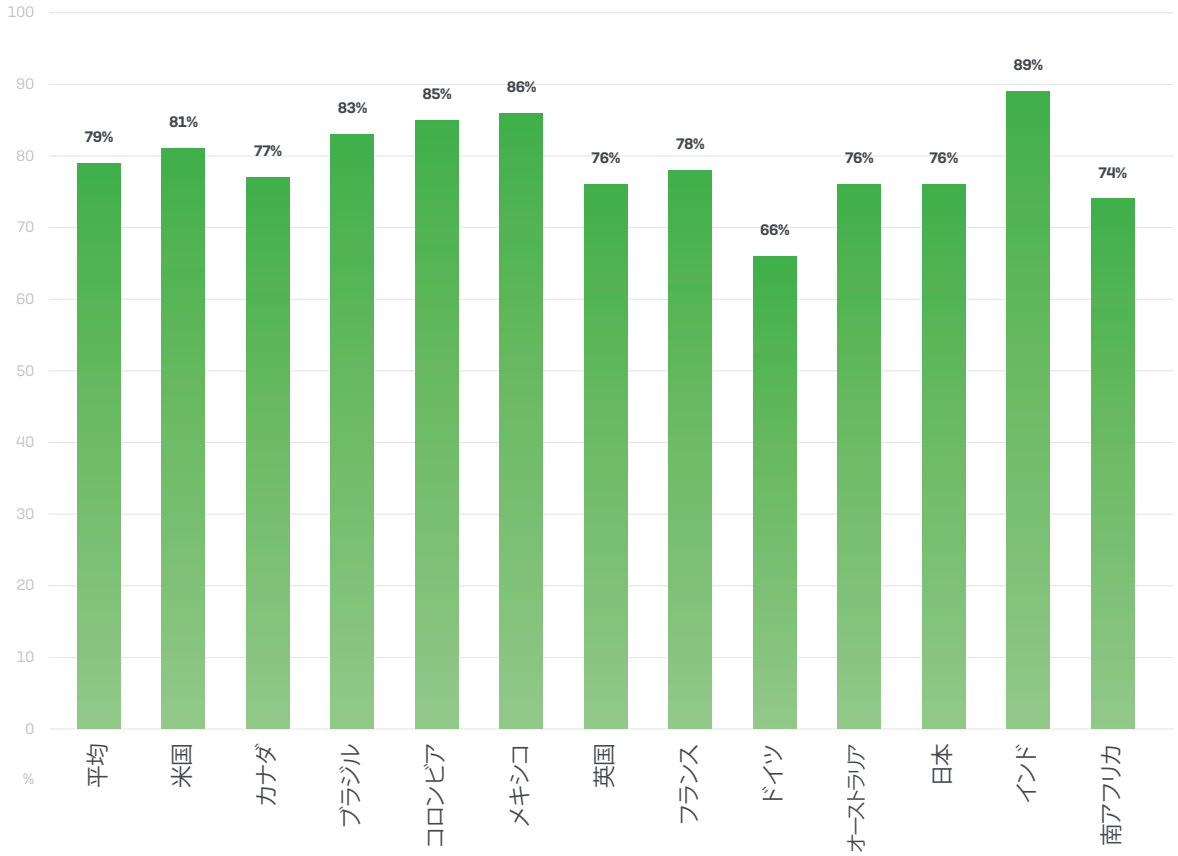
先ほど説明したように、企業は多様な攻撃に直面しており、多種の脅威の感染経路を塞ぐ必要があります。このアンケート調査では、IT 部門が平均で 26% の時間をサイバーセキュリティ対策に費やしていることがわかりました。回答した企業の大半にとって、これは望ましい状況ではありません。

26%
IT 管理者がサイバーセキュリティ対策に費やしている時間の割合

最も多くの時間を割いているのはインド (32%) で、最短の時間を費やしているのは日本 (19%) です。サイバー攻撃を受けた企業 (28%) は、そうでない企業 (23%) と比較して、いくらか多くの時間を IT セキュリティに費やします。

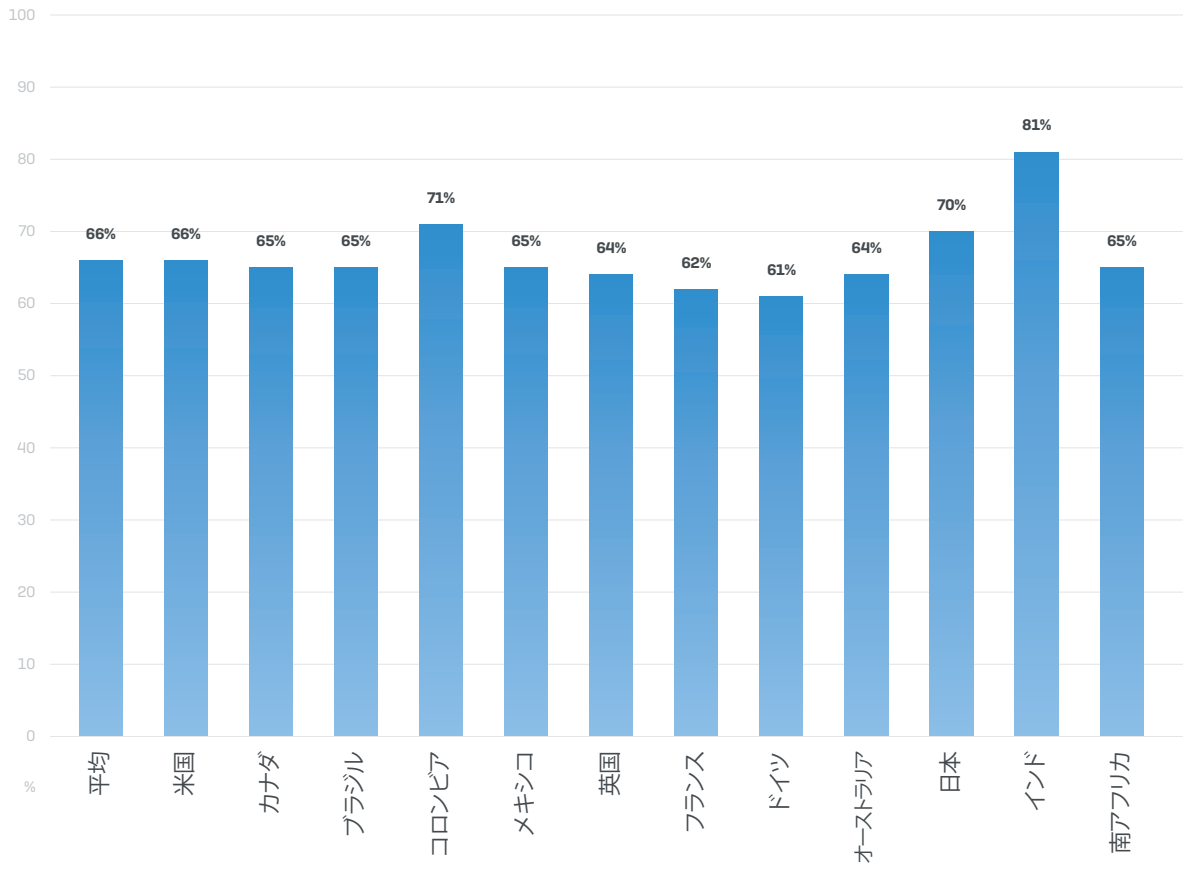
脅威は複雑でさまざまな種類があることを考えると、回答した企業の 86% が、サイバーセキュリティのより高度なスキルが必要であるとしているのも驚きではありません。攻撃を受けたことのある企業で、サイバーセキュリティの専門知識が必要であるとする企業 (89%) の割合は、そうでない企業 (79%) を上回ります。これは、対処が必要なセキュリティ問題がより多くある、または複雑な今日の攻撃ついて、認識が深いことが原因の可能性もあります。

しかし、必要な専門知識を獲得することは、大きな課題です。10社のうち 8社の企業は適切な人材を見つけるのに苦労していると回答しています。人材の採用において、最も問題が深刻なのはインド (89%) で、最も好ましい状況の国はドイツです。しかし、それでも 3人に 2人のドイツの IT 管理者は、適切なスキルを持った人材を採用するのは困難であるとしています。



次の文章に同意する回答者の割合：必要なサイバーセキュリティスキルを持つ人材を採用することは難しい課題である。**全体数：** 全回答者 (3,100人)

同時に、サイバーセキュリティに十分な予算が割り当てられているわけではなく、3人に 2人の回答者 (66%) は、人材と技術に対する予算は低すぎるとしています。2018年にサイバー攻撃を受けた企業による回答では、この値は 70% と多少増加します。



サイバーセキュリティの予算（人材/技術を含む）が必要な予算を下回っていることに同意する回答者の割合。**全体数：** 全回答者 (3,100人)

予算の不足とサイバーセキュリティの人材の採用状況は、明らかに関連しています。人材の採用に苦労する率が最も低い国であるドイツは、予算不足に悩む率も最も低くなっています。反対に、予算の不足が最も深刻なインドでは、人材の採用にも最も苦労しています。

これは、サイバーセキュリティ人材の需要が高く、その数に限りがあるため、サイバーセキュリティ専門家はより有利な給与や福利厚生を要求できることを反映しています。

サイバーセキュリティの難解な課題

セキュリティベンダーは、サイバーセキュリティ製品を何十年にも渡って開発してきています。一方企業は、引き続きサイバーセキュリティに時間、労力、お金を費やしています。しかし、何年にも渡る技術革新や投資にも関わらず、サイバーセキュリティ対策の強化は容易なことではなく、企業はいまだかって必要なリソースを持ち合わせていないことが、この調査で明らかになりました。

今までとは違う取り組みが必要なのではないでしょうか？

今までとは違う取り組み：システムとしてのサイバーセキュリティ

ここで説明したように、サイバー脅威は、互いに連係した複数の手法や技術を使って攻撃を行い、1つのシステムとして機能します。同時に IT インフラも 1つのシステムです。これは、PC、Mac、サーバー、プリンタ、モバイルデバイス、アプリ、クラウドワークロード、スイッチ、ファイアウォール、ワイヤレスシステム、および同環境で実行されるソフトウェアなどが互いに連係して稼働する複雑なシステムです。IT インフラとサイバー脅威が、それぞれシステムとして稼働していることを考えると、サイバーセキュリティ対策も、互いに独立したポイント製品ではなく、システムとして稼働するように構築することは納得のいくことです。

Synchronized Security は、数々の受賞歴を誇るソフォスのサイバー セキュリティ システムです。エンドポイント、ネットワーク、モバイル、Wi-Fi、メール、暗号化製品はすべてリアルタイムで情報を共有し、インシデントに自動対応します。単一の Web ベースのコンソールからすべての機能を制御しているので、スムーズに管理できます。

Synchronized Security：難解な問題を解決

Synchronized Security を使用して、企業は、この調査で明らかになった
複雑な問題に対処することができます。

複数の攻撃方法：

- 保護機能の包括的なポートフォリオを活用して、メール、Web、ソフトウェアの脆弱性、USB デバイスなど、あらゆる感染経路からの脅威をブロックすることができます。
- 各製品は連係して動作するように設計されており、セキュリティギャップを排除するだけでなく、互換性に関する問題も回避します。
- ネットワークトラフィックに潜む悪意のあるアプリなど、これまで隠れていたリスクを検出し、かつてないレベルでセキュリティ状態を把握することができます。

複雑、多段的で、連係されている攻撃：

- 統合された最高レベルの多層防御を提供。複数の段階と複数の手法を活用して、高度な脅威をブロックします。
- インシデントレスポンスの自動化で、脅威による被害を大幅に削減。数秒で攻撃をブロック・隔離します。
- 保護領域全体を可視化することで、問題の根本的な原因を特定して対処できます。

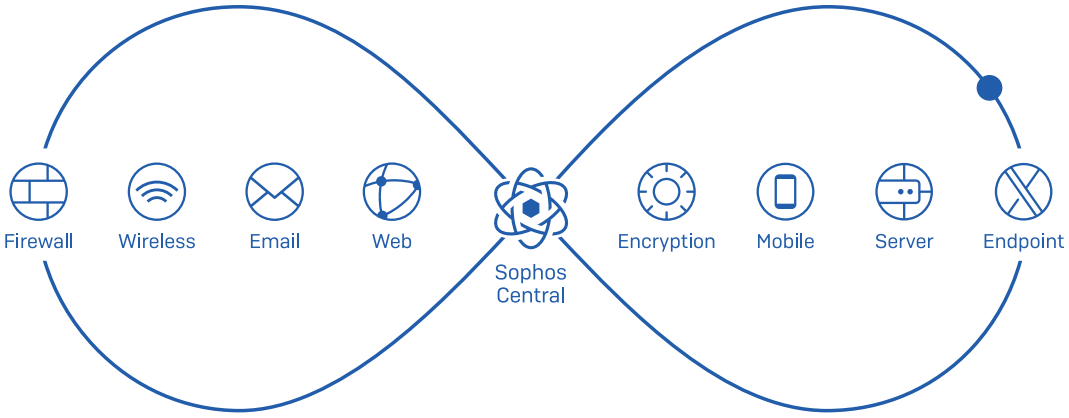
時間や人材、技術の不足：

- 単一の Web ベースのコンソールからすべての製品を管理することで、日々の作業負荷を大幅に削減しつつ、IT 管理者の負担を軽減します。
- インシデントレスポンスの自動化によって、IT 管理者が手動で感染マシンを検出、修復する必要がなくなるので管理負荷も削減されます。
- 一貫した見慣れたインターフェースですべての製品を管理できるので、新しい製品であっても、より迅速・簡単に使用を開始することができます。

まとめ

サイバーセキュリティのテクノロジーに、途絶えることなく多額の予算が注ぎ込まれているなかで、世界各地の IT 部門の負担が軽減される傾向は一切ありません。サイバーセキュリティに対する従来のアプローチを継続するのではなく、サイバーセキュリティをシステムとして扱うときがきました。各種のセキュリティ製品がリアルタイムで情報を共有し、連係することで、脅威の一歩先を行く対策を提供するだけでなく、貴重な IT リソースへの負担を軽減することができます。

Sophos Synchronized Security は、世界各地の何千という企業が活用している、数々の受賞歴を誇るサイバー セキュリティ システムです。詳しい情報やオンラインデモをご覧になる場合は、次のサイトを参照してください。www.sophos.com/ja-jp/synchronized



詳細情報と
無償評価版はこちら
www.sophos.com/ja-jp/synchronized

ソフォス株式会社
営業部
Email: sales@sophos.co.jp

19-06-21 WP-JA (RP)

SOPHOS