次世代のセキュアなテレワークに関するレポート

cisco SECURE

目次

エグゼクティブサマリー

コロナ禍により、世界中の企業がかつてないスピードと規模でテレワーク環境に移行しています。かつては従業員や企業にとって「できれば便利」だったものが、ほぼ一夜にして「必須」になり、世界中の組織が全従業員をテレワークに移行させました。テレワークに移行したことで、従業員がリモートから社内リソースに安全にアクセスして作業し、事業を継続できるように、サイバーセキュリティへのアプローチ、ソリューション、ポリシーを進化させる必要がありました。

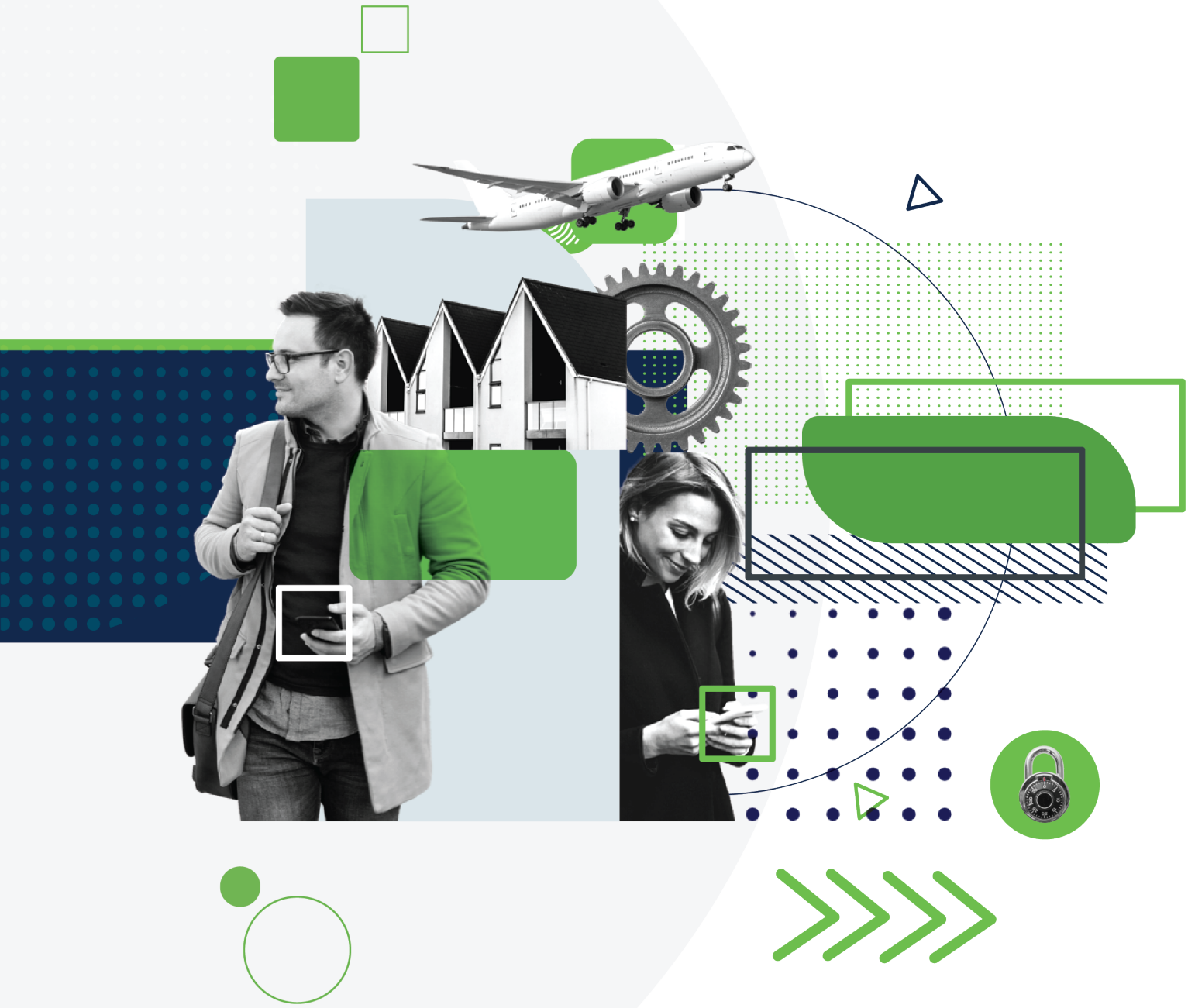
不確実性に満ちたこの 1 年の間に、ハイブリッド式の柔軟な次世代の働き方、という大きなトレンドが生まれました。長期間テレワークを続けてきた従業員は、コロナ後においても場所、時間、デバイスを問わずに働ける柔軟性と機能を確保し続けたいと考えています。それは、たとえオフィスに戻れたとしても変わりません。

そのため、サイバーセキュリティに対する方針を再評価する必要性が高まっています。ビジネスリーダーが企業のレジリエンスを高めようとしている現在では、その必要性が顕著です。ビジネスのレジリエンスはセキュリティによって高めることができます。現在の状況にも将来にも柔軟に適応できるセキュリティを確保していれば、事業を継続できます。そのためには、柔軟で使いやすく、効果的で安全なネットワークソリューションとコラボレーション ソリューションを導入することが重要です。また、オンプレミスのデータセンターで提供されるソリューションでもクラウドから提供されるソリューションでも、業務用、個人用を問わず、すべてのユーザデバイスが対象になっていなければなりません。

シスコは、コロナ禍によって世界中の組織が全従業員をテレワークに移行せざるを得なくなった際に、事業を保護するためにどのような準備ができていたかを把握しようと計画しました。さらに、より重要な、サイバー脅威やセキュリティに関するアラートが増え続ける中での企業の現状、突然の移行を迫られたことによる課題、定着化したハイブリッド式の柔軟な働き方に対するサイバーセキュリティへのアプローチの変化についても分析したいと考えました。そこで、アメリカ地域 (AMER)、アジア太平洋、日本、中国 (APJC)、ヨーロッパの 21 の市場において、小規模企業から大規模企業までの 3,000 人を超える IT に関する意思決定者を対象にグローバル調査を実施しました。

「次世代のセキュアなテレワークについて」というタイトルのこの調査は、組織がテレワークに移行する際に直面した課題を詳細に把握することが目的です。また、組織におけるサイバーセキュリティへの対応状況や、定着したと思われるハイブリッド式作業環境に対応する際の優先順位、ポリシー、投資状況の変化も明らかにしようとしています。

それでは調査結果について説明していきます。



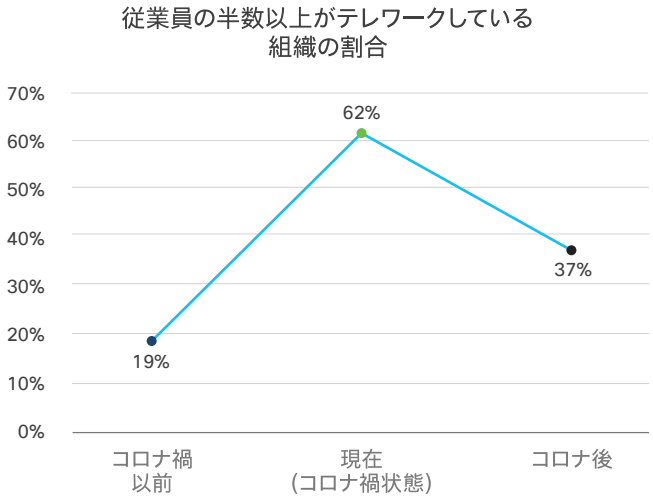
グローバルでの調査結果

グローバルでの調査結果

次世代のハイブリッドな働き方におけるサイバーセキュリティの重要性

組織はコロナ禍以前の状態には戻らない

組織がコロナ後の世界に向けた準備を始めるにあたり、1 つ明らかなことがあります。それは、コロナ禍以前の状態には戻らないことを前提に、今後仕事がどうなろうとも、従業員は、リモートから作業できる柔軟性と機能を確保したいと考えているということです。3 つの地域すべてで一貫して確認されたように、3 月の感染拡大時には、テレワークがかつてないレベルにまで急増し、回答者の 3 分の 2（62%）の組織で、**従業員の半数以上**が自宅から仕事をしていました。また、回答者の 37% が、**半数以上の従業員**がコロナ後も自宅で仕事を続けたいと考えていると回答しています。コロナ禍以前には、同様の状況だった組織はわずか 19% でした。



従業員の半数以上がテレワークしていると回答した人の割合

	グローバル	APJC	AMER	ヨーロッパ
コロナ禍以前	19%	19%	24%	16%
現在（コロナ禍状態）	62%	56%	75%	67%
コロナ後	37%	34%	46%	34%

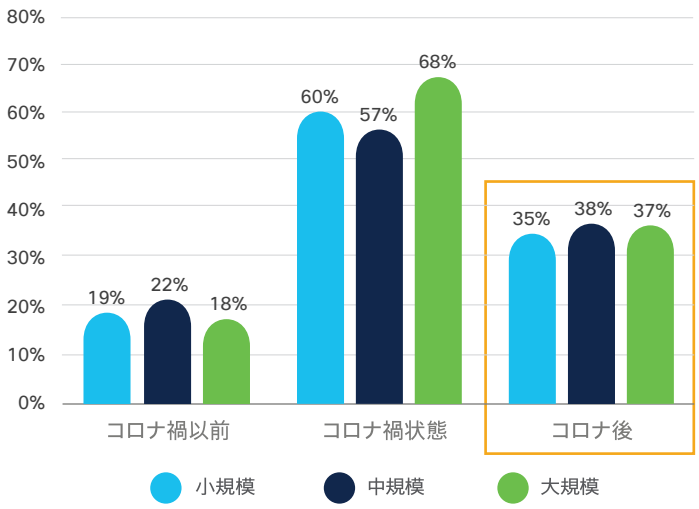
従業員の半数以上がテレワークしている組織は AMER で一番多く、回答者の 75% の組織に及んでいました。次いでヨーロッパが 67%、APJC が 56% となっています。

一方、AMER の回答者の 46% は、企業が通常の状態に戻った後も従業員の半数以上がテレワークを続けると想定していて、すぐにはコロナ禍以前のレベルには戻りそうにありません。APJC とヨーロッパのいずれでも、回答者の 34% が同じ回答をしています。

テレワークに対する方針は企業規模にかかわらず一貫していて、小規模企業の 35%、中規模企業の 38%、大規模企業の 37% が、コロナ後も従業員の半数以上がテレワークを続けると考えています。

多くの企業で今後仕事がどうなるか依然として不透明な状況にあると思われますが、現在の状況にも将来にも柔軟に適応できるセキュリティを確保していれば、ビジネスレジリエンスが向上し、より多くのテレワーカーをサポートできるようになります。

従業員の半数以上がテレワークしている組織の割合



一部の国では、他の国よりもテレワークをさらに推進することを計画

興味深いことに、ほとんどの組織はコロナ後に大半の従業員をオフィスに戻す計画を立てていますが、一部の国ではこの傾向に逆行し、従業員の半数以上が今後もテレワークを続けると回答した組織の割合が高くなっています。このような回答をした組織は、フィリピンで 48%、英国と米国で 50%、ブラジルとインドで 53% となっていて、すべて世界平均の 37% を上回っています。

48%
フィリピン

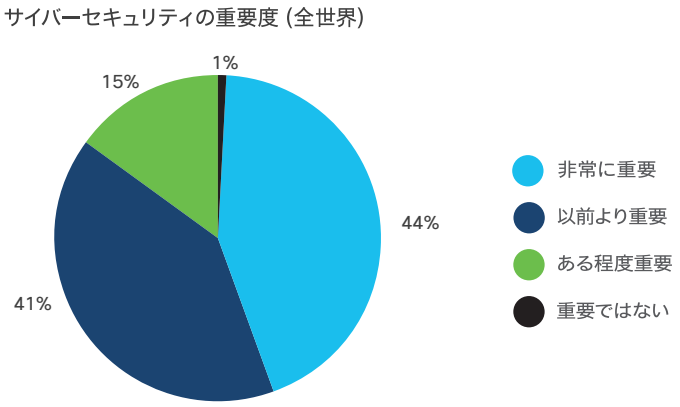
53%
ブラジル
インド

50%
英国
米国

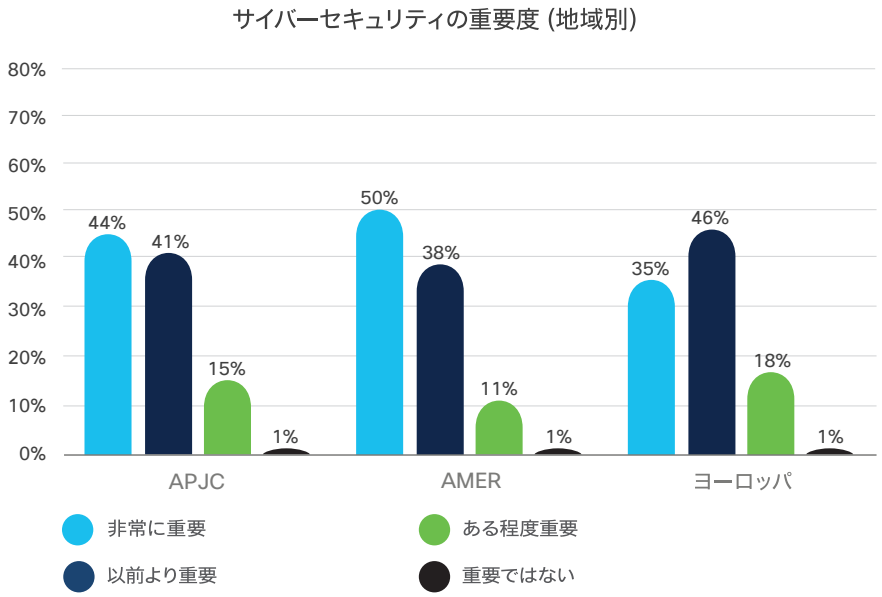
このようなハイブリッド式の柔軟な次世代の働き方を実現するために、企業はシームレスでセキュアなインフラ基盤を必要としています。

サイバーセキュリティが企業の最優先事項に

幸いなことに、サイバーセキュリティが企業の最優先事項となっています。世界の回答者の 85% が、サイバーセキュリティはコロナ禍「以前より重要」または「非常に重要」であると回答しています。



地域別に見ると、APJC (44%) と AMER (50%) では、サイバーセキュリティがビジネスにとって「非常に重要」であると回答した組織が最も多くなっています。一方、ヨーロッパでは、「以前より重要」と回答した組織の割合が多く、46% でした。



「以前より重要」または「非常に重要」と考える傾向は企業規模にかかわらず一貫していて、小規模 79%、中規模 87%、大規模 88% でした。

	小規模	中規模	大規模
非常に重要	36%	42%	53%
以前より重要	44%	45%	35%
ある程度重要	19%	13%	11%
重要ではない	1%	1%	0%

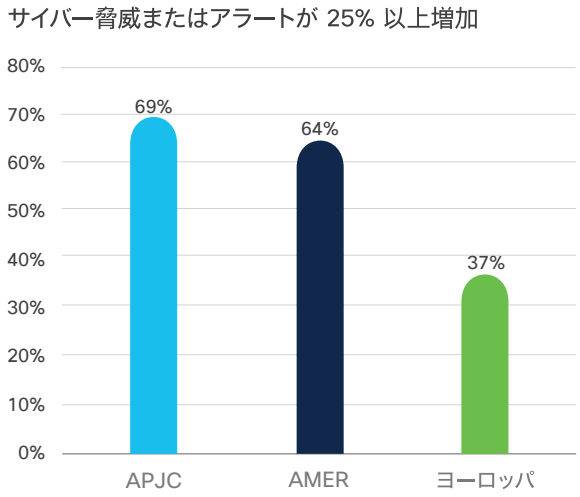
組織規模別のサイバーセキュリティの重要性

レジリエンスの回復：サイバーセキュリティ脅威への取り組みと課題

各レベルでサイバー脅威とアラートが増加

コロナ禍によってユーザが企業のネットワークやクラウドアプリケーションにリモートからアクセスする機会が増えるのに伴い、潜在的なセキュリティギャップにつけこんだ、サイバーセキュリティに対する脅威やアラートが世界的に急増しました。世界の回答者の 61% が、新型コロナウィルスの感染拡大後、**サイバー脅威やアラートが 25% 以上増加**したと回答しています。この傾向は、小規模企業の 55%、中規模企業の 70%、大規模企業の 60% で確認されました。

地域別に見ると、APJC で同様の回答をした組織が 69% と多く、次いで AMER が 64%、ヨーロッパが 37% でした。

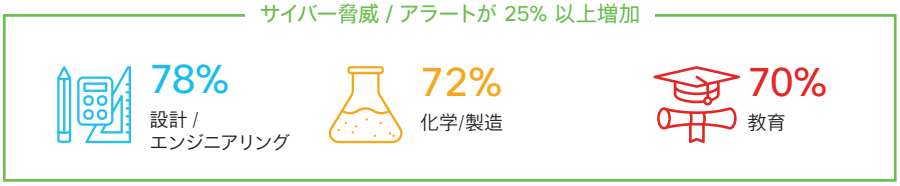


懸念されるのは、世界の企業の 8% が、サイバー脅威が増加したか減少したかを把握できていなかったことです。この傾向は、APJC の 6% と AMER の 5% に対して、ヨーロッパでは 17% と多くなっています。さらに詳細に分析すると、地域や業界によって脅威やアラートのレベルに大きな違いがあることもわかりました。

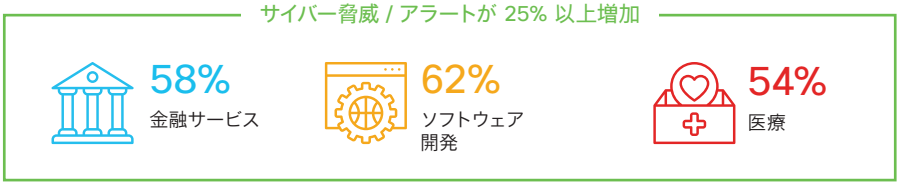
サイバー脅威 / アラートの増加率	グローバル	APJC	AMER	ヨーロッパ
0 ~ 24%	31%	25%	31%	47%
25 ~ 50%	33%	35%	36%	23%
51 ~ 75%	23%	27%	24%	11%
76 ~ 100%	5%	6%	3%	2%
不明	8%	6%	5%	17%

サイバー脅威 / アラートの増加率が *25% 以上*

たとえば、**設計 / エンジニアリング**業界の組織の 78% が、サイバー脅威 / アラートの増加率が 25% 以上と回答し、すべての業界で最も高くなっています。次いで、**化学 / 製造**業が 72%、**教育**が 70% でした。



興味深いことに、**金融サービス** (58%)、**ソフトウェア開発** (62%)、**医療** (54%) など、攻撃の対象となりやすいと見られていた業界では、予想に反してアラートが 25% 以上増加した組織の割合が比較的低い傾向にありました。



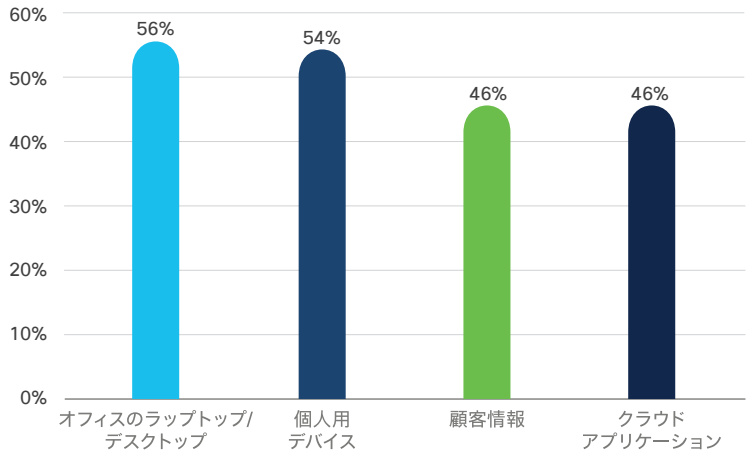
サイバーセキュリティに関して組織が直面している最も大きな課題はテレワークへの対応

セキュアアクセスとは、すべてのユーザが、任意のデバイスからいつでもエンタープライズ ネットワークとアプリケーションに安全にアクセスできることを意味します。そしてこれが、テレワーカーをサポートする際に最も多くの組織 (62%) が直面している**サイバーセキュリティの最大の課題**です。その他の懸念事項として世界中の組織が挙げているのは、データプライバシー (55%) です。この問題は、セキュリティ方針全体に関係します。また、アクセス制御の維持およびポリシーの適用も多く挙げられています (50%)。

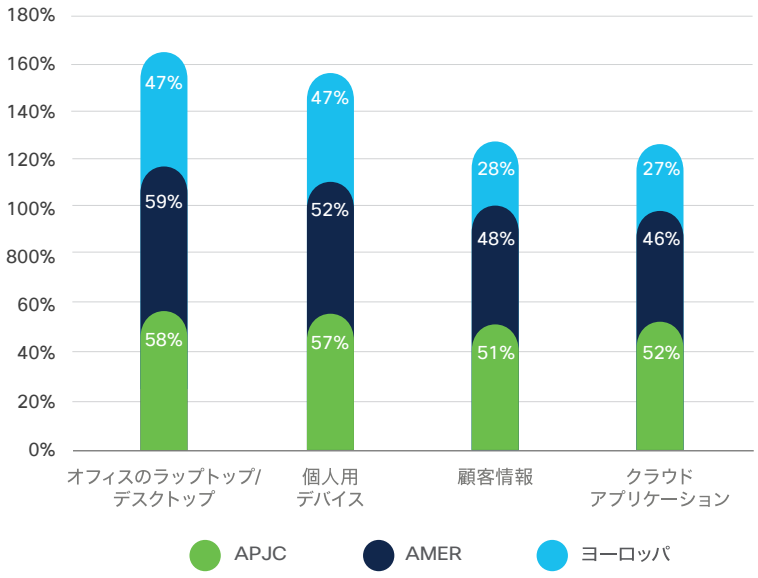
増加するエンドポイントの保護

デバイスの保護は、エンドポイントをキャンパスネットワークに接続して可視化し、更新プログラムを配信することができなくなった組織にとって、ますます大きな課題になっています。また、企業のリソースに接続する従業員の個人用デバイスが増加していますが、それらは管理対象になっておらず、セキュリティチームが確認できていません。回答者の 2 人に 1 人は、オフィスのラップトップ / デスクトップ（56%）と個人用デバイス（54%）が、リモート環境で保護する上で課題であると回答しています。続いて多かったのが顧客情報とクラウドアプリケーションで、いずれも 46% でした。

リモート環境での保護が課題となる対象



リモート環境での保護が課題となる対象
(地域比較)

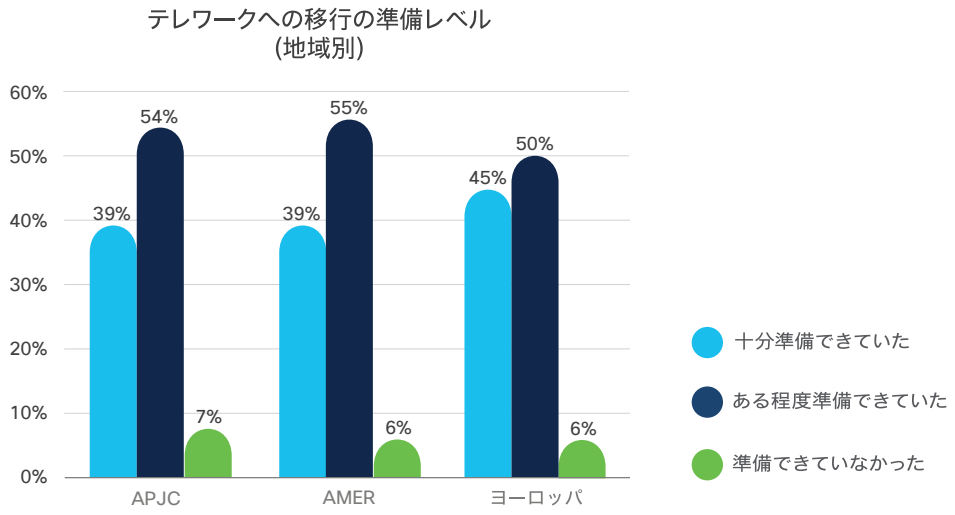


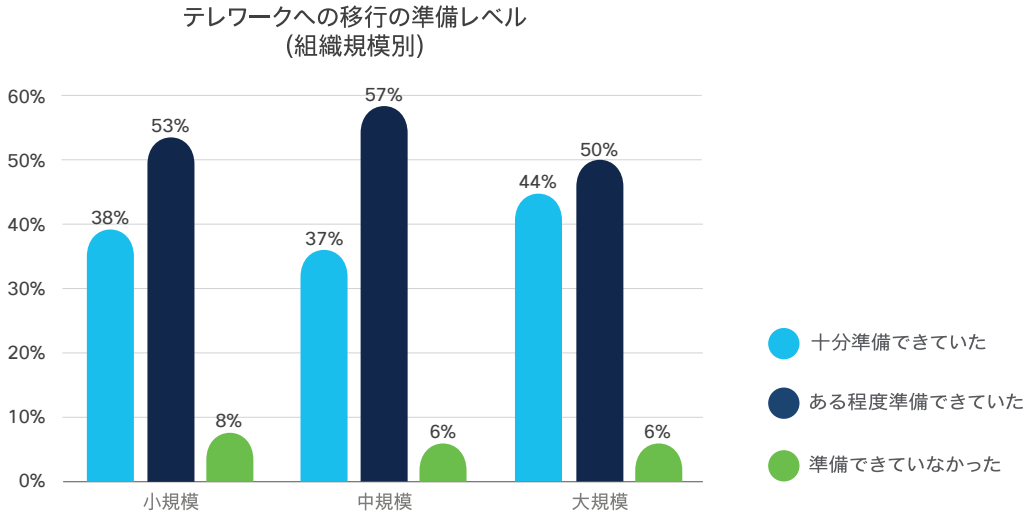
デジタル トランスフォーメーションの推進が求められる組織

多くの組織は、コロナ禍以前からクラウドファーストおよびリモートファーストへの移行を始めていましたが、それには多くの時間と投資が必要です。急速にテレワークに移行したことで、多くの組織がクラウドファースト / リモートファーストに移行するにはまだ時間がかかることが浮き彫りになりました。新型コロナウィルスの感染が始まった時点でのテレワーク環境への移行の準備状況を尋ねると、世界全体では、「ある程度準備できていた」（53%）または「準備できていなかった」（6%）のいずれかを回答した組織が多くなっています。

	グローバル	APJC	AMER	ヨーロッパ
十分準備できていた	40%	39%	39%	45%
ある程度準備できていた	53%	54%	55%	50%
準備できていなかった	6%	7%	6%	6%

テレワークへの移行の準備レベル





業界別に見ると、**設計 / エンジニアリング業界**（72%）において「ある程度準備できていた」と回答した組織の割合が最も高く、世界平均の 53% を上回っていました。一方、次の業界では突然の移行に対して「準備できていなかった」と回答した組織の割合が最も高くなっていて、世界平均の 6% を上回っていました。**卸売 / 流通**（15%）、**教育**（14%）、**化学 / 製造**、**非コンピュータ関連製造**、**非営利 / 慈善事業**（それぞれ 10%）。

IT チームやセキュリティチームがテレワークをサポートする準備ができていたかどうかは、事業の特性や、その業界の従業員が一部でもテレワークできていたかどうかによって異なる可能性があります。知識集約型作業の割合が高い企業は、製造業などの作業場所が限定されている業界よりも、テレワークをしている従業員の数が多い傾向にあります。元々テレワーカーが多かった企業は、さらに多くの従業員がテレワークすることにも無理なく対応できます。

67% の組織が「十分準備できていた」と回答しているベトナムが、すぐにテレワークに移行する準備が整っていた組織の割合が世界で最も高くなっていました。次に多かったのが英国（59%）、インド（54%）、インドネシア（49%）でした。

一方、感染拡大前にテレワーカーの割合が最も多かった米国（組織の 32% で半数以上がテレワーク）では、「十分準備できていた」（46%）組織よりも「ある程度準備できていた」（48%）組織の方が多くなっていました。

現在および将来におけるサイバーセキュリティの優先順位

テクノロジーの導入と優先順位

幸いなことに、テレワークを実現するために採用されたすべてのテクノロジーソリューションのうち、サイバーセキュリティ対策の優先順位が最も高くなっています（世界全体の 52% が最優先と回答）。次いで多かったのが、コラボレーションツール（41% が最優先）、プロフェッショナルサービス（27% が最優先）でした。

導入割合が高い	vs	最優先
コラボレーションツール 73%	1	サイバーセキュリティ対策 52%
サイバーセキュリティ対策 68%	2	コラボレーションツール 41%
クラウドベースのドキュメント共有 63%	3	プロフェッショナルサービス 27%
分散データの保護 49%	4	クラウドベースのドキュメント共有 22%
プロフェッショナルサービス 33%	5	分散データの保護 19%

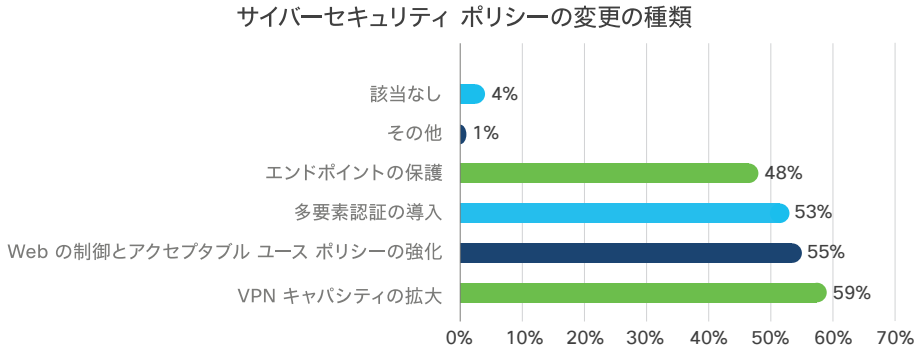
コラボレーションからファイル共有、ネットワーキングに至るまで、企業がさまざまなソリューションを導入しながら次世代の働き方を進める中で、すべての IT ツールにセキュリティを統合することが重要です。セキュリティを統合することで、安全なテレワークを実現できます。

適切なプロトコルとポリシーを適用したテレワークの促進

世界の組織の 96% が、テレワークをサポートするためにサイバーセキュリティ ポリシーを変更したと回答しています。企業規模別に見ると、小規模企業の 93%、中規模企業の 98%、大規模企業の 97% が該当していて、あらゆる規模の組織が、テレワークへの移行に対応するためにポリシーをただちに更新する必要があると考えたことを示しています。

たとえば、人事部門や財務部門が突然テレワークすることになった場合、企業ネットワーク内で日々の業務を遂行するために付与したセキュリティポリシーやアクセス権限を、リモート設定に複製して業務を継続できるようにする必要があることは明らかです。ポリシーの一貫性も、かつてないほど大きな問題になっています。

このような観点から、ポリシー関連の主な変更点は、VPN キャパシティの拡大（59%）、Web の制御とアクセプタブル ユース ポリシーの強化（55%）、多要素認証（MFA）の導入（53%）でした。



グローバル	APJC	AMER	ヨーロッパ
VPN キャパシティの拡大 (59%)	Web の制御とアクセプタブル ユース ポリシーの強化 (61%)	VPN キャパシティの拡大 (64%)	VPN キャパシティの拡大 (64%)
Web の制御とアクセプタブル ユース ポリシーの強化 (55%)	多要素認証の導入 (59%)	Web の制御とアクセプタブル ユース ポリシーの強化 (57%)	多要素認証の導入 (38%)
多要素認証の導入 (53%)	VPN キャパシティの拡大 (56%)	多要素認証の導入 (51%)	Web の制御とアクセプタブル ユース ポリシーの強化 (34%)

サイバーセキュリティ ポリシーに対する変更の上位 3 つ (地域別)

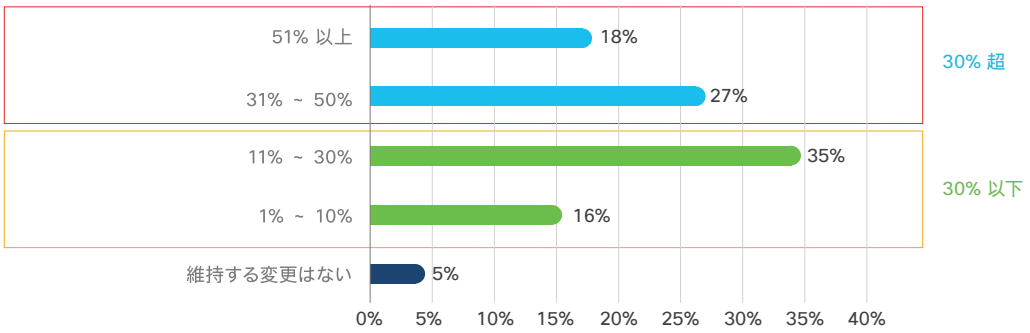
地域による違い

- **Web の制御とアクセプタブル ユース ポリシーの強化**
  - APJC で最高 (61%)
  - AMER で 2 番目 (57%)、グローバル (55%) と同様
  - ヨーロッパで 3 番目 (34%)
- **多要素認証の導入**
  - APJC (59%) とヨーロッパ (38%) で 2 番目
  - AMER で 3 番目 (51%)
- **VPN キャパシティの拡大**
  - AMER とヨーロッパで最も高く (いずれも 64%)、グローバル (59%) と同様
  - APJC で 3 番目 (56%)

企業のサイバーセキュリティ ポリシーに対する変更が今後も継続

この調査で最も注目すべき結果の 1 つは、テレワークに対応するために変更したサイバーセキュリティ ポリシーが今後も維持されるということです。この結果は、企業が現在のデジタルファーストの世界に本格的に対応するために、ビジネス戦略とセキュリティ戦略を変革するまたとない機会が得られたということを示しています。これにより、従業員がテレワークに求める柔軟性が実現します。

そのため、サイバーセキュリティ ポリシーを変更した組織の大多数 (95%) が、変更内容の一部は今後も維持すると回答しています。



サイバーセキュリティ ポリシーの変更を維持する割合

地域別に詳細を見ると、AMER（54%）とヨーロッパ（48%）では、サイバーセキュリティ ポリシーの変更の 30% 以上を今後も維持すると回答している割合が高く、次いで APJC の 41% の組織が同様の回答をしています。

ポリシーの変更を維持する割合	グローバル	APJC	AMER	ヨーロッパ
30% 以下	50%	54%	44%	45%
30% 超	45%	41%	54%	48%
合計	95%	96%	97%	93%

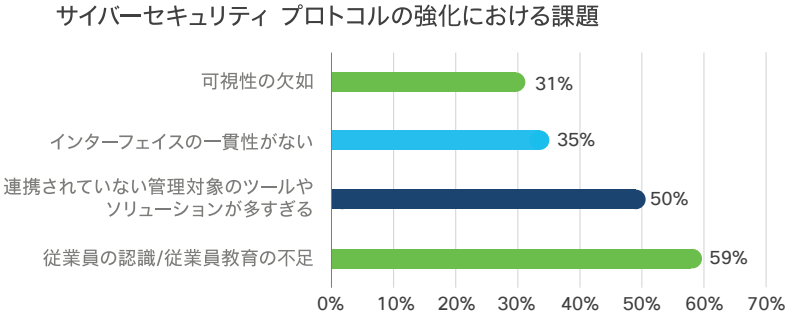
ポリシーの変更を維持する割合（地域別）

企業規模（小規模、中規模、大規模）による違い：

- 予想どおり、中小規模の企業よりも大規模企業（52%）の方が、変更したポリシーの 30% 以上を維持すると回答した割合が高くなっています。
- 一方、多くの小規模（55%）企業および中規模（54%）企業では、新しいサイバーセキュリティ ポリシーを維持する部分が 30% 以下になっています。

セキュリティに関する教育と文化：必須

さらなる教育と、シンプルで使いやすく、連携して機能する優れたセキュリティソリューションが必要です。全世界の組織の 59% が、テレワークのサイバーセキュリティ プロトコルを強化する上で、従業員の認識と教育の不足が最大の課題であると回答しています。次いで多いのが、連携されていない管理対象のツールやソリューションが多すぎるということです（50%）。APJC、AMER、ヨーロッパでも同様の傾向が見られました。



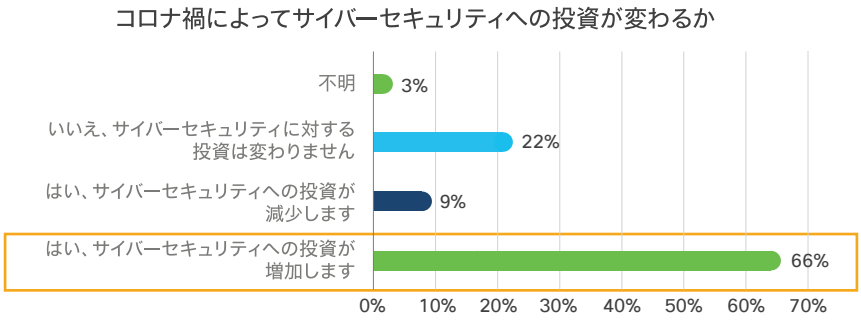
グローバル	APJC	AMER	ヨーロッパ
従業員の認識 / 従業員教育の不足 (59%)	従業員の認識 / 従業員教育の不足 (61%)	従業員の認識 / 従業員教育の不足 (58%)	従業員の認識 / 従業員教育の不足 (54%)
連携されていない管理対象のツールやソリューションが多すぎる (50%)	連携されていない管理対象のツールやソリューションが多すぎる (53%)	連携されていない管理対象のツールやソリューションが多すぎる (49%)	連携されていない管理対象のツールやソリューションが多すぎる (43%)
インターフェイスの一貫性がない (35%)	インターフェイスの一貫性がない (40%)	インターフェイスの一貫性がない (33%)	インターフェイスの一貫性がない (22%)

サイバーセキュリティ プロトコルを強化する上での課題 (地域別に上位 3 つ)

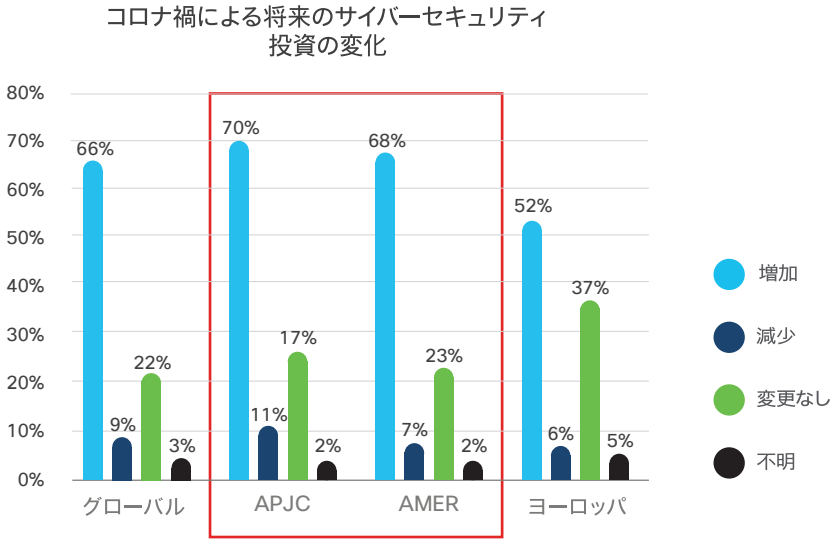
今回の調査結果から、セキュリティ業界は、現在の状況に対応するために根本的に変化する必要があることを示しています。そのためには、柔軟性を高めてテレワーカーをサポートし、セキュリティがコラボレーションを阻害するものではなく、促進するものであることを示すことが重要です。詳細については、以下で説明します。

増加するサイバーセキュリティへの投資

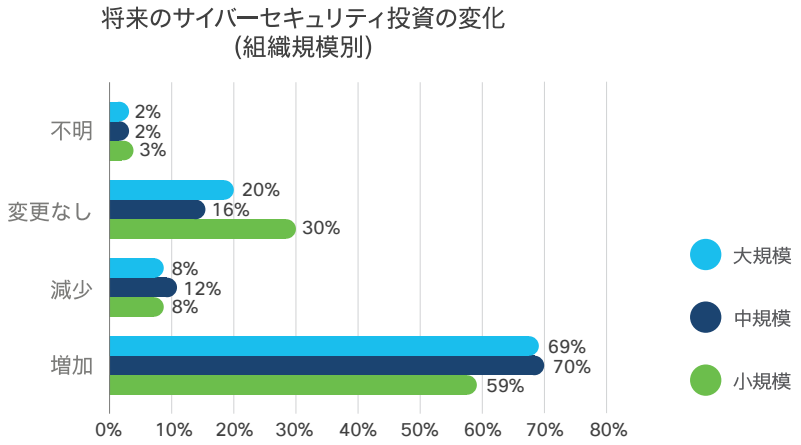
セキュリティの変更や改善とともに、コロナ禍によって、世界の組織の大部分 (66%) がサイバーセキュリティへの投資を増やす可能性があると回答しています。



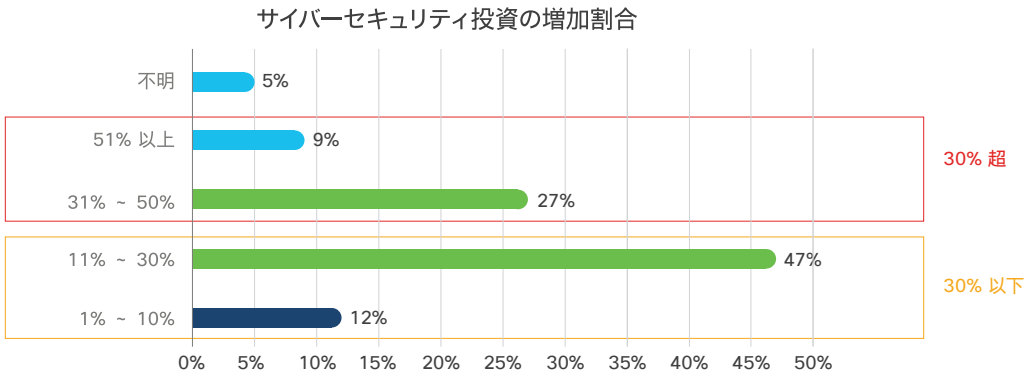
APJC (70%) と AMER (68%) では、世界の平均 66% と比較して、将来、サイバーセキュリティへの投資を増やすと回答した組織の割合が高くなっています。



サイバーセキュリティを積極的に推進するため、あらゆる規模の組織が、コロナ後も投資を増やすことを考えています。興味深いのは、中規模企業の方が大規模企業をわずかに上回っており、70% が投資の拡大を計画しているということです。小規模企業も遅れをとっておらず、59% が同様の計画をたてています。



各業界、地域、市場の組織が、サイバーセキュリティへの支出を増やす必要性について同意していますが、その割合はさまざまです。サイバーセキュリティへの投資を増やすことを計画している企業の 59% が、*1 ～ 30%* の拡大を見込んでいます。この傾向は、APJC (58%)、AMER (56%)、ヨーロッパ (65%) でも同様です。

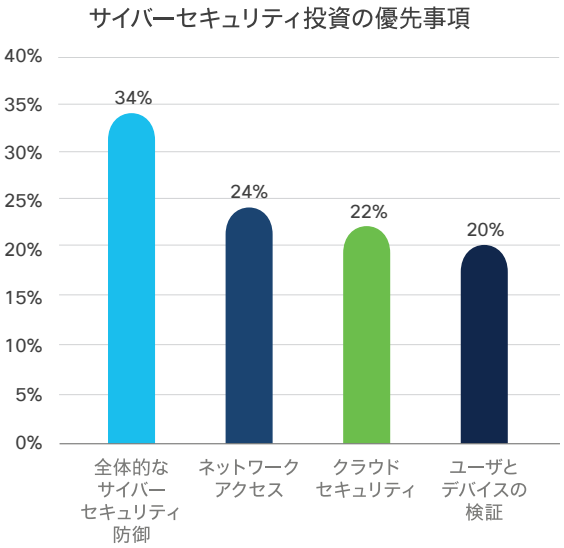


投資拡大の割合	グローバル	APJC	AMER	ヨーロッパ
30% 以下	59%	58%	56%	65%
30% 超	36%	39%	39%	23%

世界中の組織が全体的なセキュリティ戦略を再考している

コロナ後の世界に備えるためのサイバーセキュリティへの投資に関して、重要性の観点から優先順位を尋ねると、全体的なサイバーセキュリティ防御（脅威保護、リスク評価、監査、コンプライアンス、プライバシーなどを含む）への投資が最優先となりました（34% が最優先）。また、調査対象となった 21 の市場のうち 16 の市場で最優先になっています。このことは、テレワーク環境に移行することで、企業が対処する必要がある戦略的な課題が発生したことを示しています。この課題は、すでに普及したハイブリッド式の柔軟な職場環境を維持する最善の方法を再考する際に、合わせて対応する必要があります。

優先すべきその他の投資には、ネットワークアクセス（24% が最優先）、クラウドセキュリティ（22% が最優先）、ユーザとデバイスの検証（20% が最優先）などがあります。



最優先のサイバーセキュリティ投資

地域による違い

APJC	AMER	ヨーロッパ
全体的なサイバーセキュリティ防御（35%）	全体的なサイバーセキュリティ防御（31%）	全体的なサイバーセキュリティ防御（33%）
クラウドセキュリティ（23%）	クラウドセキュリティ（25%）	ネットワークアクセス（29%）
ネットワークアクセス（23%）	ネットワークアクセス（22%）	ユーザとデバイスの検証（21%）

重要なポイントと推奨事項

重要なポイントと推奨事項

#1 次世代の働き方はダイナミックになる：テレワーカーのニーズを満たすサイバーセキュリティが必要

世界は、従業員が長期間オフィスを離れて仕事をしている間もつながりを保ち、生産性を維持できることを認識するようになりました。多くの企業が、社内とリモートの両方の従業員に対応するハイブリッドな作業環境に移行する可能性があります。その結果、雇用者と従業員は、ビジネスと人材についてより多くの選択肢を得られるようになり、柔軟性や従業員の多様性が向上します。一方、急激に移行が進んだことで、さまざまなサイバーセキュリティ上の課題も発生しています。すなわち、これまでと一変した環境でいかにビジネスを継続するかや、かつてない規模のアクセスに対してセキュリティをいかに確保するかという課題です。

従業員は、オフィスのデバイスを自宅の Wi-Fi や外部ネットワークに接続したり、個人のデバイスを使用してクラウド内の企業アプリケーションに接続したりしています。その結果、セキュリティチームと IT チームは、いずれも突然の激務を強いられています。かつてない数のテレワーカーとそのデバイスを対象として、セキュリティを損なうことなく、迅速にサポートするという責務が課せられているのです。以前は本社に適用されていたポリシーと制御は、アクセスする場所や時間を問わず、すべての従業員に適用する必要があります。さらに、テレワークには負の側面もあります。現代のサイバー攻撃者はフィッシング攻撃を拡大し、ユーザをだまして情報を盗む、新たなテレワークシステムをマルウェアで侵害する、進化する企業のサイバーセキュリティのギャップにつけ込む、といった活動を増しています。

企業は、従業員がネットワークの内でも外でも同じ保護レベルで作業できるように、柔軟で安全なハイブリッド作業環境を構築する必要があります。ビジネスリーダーと IT リーダーによってテクノロジーとビジネスの優先順位が大きく変わるため、組織が最大限の能力を発揮できるように、サイバーセキュリティがビジネスとテクノロジーをつなぐ必要があります。

#2 ハイブリッド式の柔軟な作業環境を構築できるかは、準備、コラボレーション、従業員教育にかかっている

この 8 ヵ月で急激にテレワークに移行したことで発生した大きな問題の 1 つは、組織が正しく移行できたかどうかということです。クラウド セキュリティ ソリューションやゼロトラストフレームワークなど、コロナ禍以前のテクノロジーに段階的 / 継続的に投資してきた企業は、テレワークに対応する準備が十分整っています。同様に、そのような対応に対してサイバーセキュリティ対策を強化することで、サイバーセキュリティ攻撃の数や種類の増加にも十分対応できるようになっています。

しかし、ハイブリッド式の柔軟な職場環境のメリットを最大限に活用するためには、こうした投資を単独では実施できません。テレワークへの移行に伴い、ネットワークチームとセキュリティチームは、場所や時間を問わずにアプリケーションやサービスにシームレスかつ安全にアクセスできるようにする必要があります。セキュリティ、ネットワーク、コラボレーションは、もはや別々には語れません。すべて連携させることが必要です。また、これらの機能に加えて、新たなプロトコルを適用し、サイバーセキュリティ ポリシーを強化する必要があります。さらに、健全なセキュリティ文化への投資は絶対に欠かせないため、優れた従業員教育プログラムを実施する必要もあります。

#3 ビジネスレジリエンスを強化するには、さらにシンプルで効果的なサイバーセキュリティが不可欠

長期間のテレワークの経験により、企業の戦略におけるサイバーセキュリティの重要性が高まり、企業のサイバーセキュリティ ポリシーの変更が今後も維持される可能性があります。さらに、多くの組織が、サイバーセキュリティへの支出を将来的に増やすつもりであると回答しています。

IT リーダーにはその他にも多くの優先課題がありますが、セキュリティは後から考えることができません。セキュリティは、デジタル化を成功させるための基盤となる必要があります。そうすることで、セキュリティ、拡張性、適応力が確保されます。サイバーセキュリティが侵害される可能性と影響を軽減するために、組織は、サイバーセキュリティ対策をシンプルにする方法を見つける必要もあります。より効果的なセキュリティを確保するためにシンプルなアプローチを採用することで、現在必要なことや将来必要になることを妨げることなく、ビジネスを推進することができます。

推奨事項:

従業員が場所や時間、デバイスを問わず安全に作業できるようにするには、サイバーセキュリティがあらゆる IT 投資の基盤とならなければなりません。そのためには、プラットフォームアプローチを採用し、ネットワークからエンドポイント、クラウドに至るまで、非常に効果的なセキュリティを提供する必要があります。これは、ポイントごとに最適な製品を揃えるだけでは実現できません。セキュリティをシンプルにする必要がある場合、連携して使いやすいソリューションでなければなりません。

安全なテレワーク環境を構築し、今後の働き方にも柔軟に対応できるようにするには、次の条件を満たしている必要があります。

- ユーザのアイデンティティを検証して本人であることを確認し、信頼を確立できる
- デバイスや接続方式を問わず安全に作業できる
- 従業員が必要とする企業のアプリケーションやデータにアクセスできる
- ネットワークに接続したユーザを脅威から保護できる

次世代の働き方：10 のポイント

1. ゼロトラスト戦略を採用し、会社が承認したアプリケーションへのアクセスを許可する前に、すべてのユーザのアイデンティティを確認し、ワークフォース（あらゆるユーザとデバイス）、ワークロード（あらゆるアプリ）、ワークプレイス（あらゆる場所）を保護します。
2. 多要素認証 (MFA) は、テレワーカーを保護するための最初のステップであり、企業の資産にアクセスしようとする従業員のアイデンティティを確認するための手段です。
3. VPN は、ユーザとアプリケーションをつなぐ安全なトンネルとして、従業員が外出先や自宅で仕事する際に、安全に接続し、生産性を維持できるようにします。また、ユーザエクスペリエンスを損なうことなく適切なレベルのセキュリティを確保し、承認されたユーザにのみアクセスを許可します。
4. DNS を使用します。ほとんどのセキュリティ侵害はエンドポイントのユーザをターゲットとしているため、DNS レイヤでの最前線の防御が必要です。最初の重要なレイヤである DNS レイヤで、悪意のあるふるまいに関連するドメインが企業のネットワークに侵入する前にブロックするか、マルウェアがすでに内部に存在する場合は封じ込めます。
5. Office 365 の電子メールを高度な脅威から保護します。侵入経路として最も多いのは電子メールであるため、Microsoft 365 用の統合クラウドネイティブ セキュリティ ソリューションを利用して、内外から Office 365 に送信される脅威を阻止し、フィッシング、ランサムウェア、ビジネスメール侵害などの電子メールの脅威から保護する必要があります。
6. セキュアなエンドポイント ソリューションで防御の最終ラインを確保します。エンドポイントセキュリティは、サイバー攻撃を防御するだけでなく、脅威が防御をすり抜けてエンドポイントに侵入しても、悪意のあるファイルをすばやく検出して食い止め、修復することで、損害を未然に防ぎます。
7. クラウドベースのセキュリティソリューションを戦略的に導入し、あらゆる場所からあらゆる環境のアプリケーションにシームレスに接続できるようにすることで、従業員を保護します。セキュア アクセス サービスエッジ（SASE）は、SD-WAN 機能に、セキュア Web ゲートウェイ、クラウド アクセス セキュリティ ブローカー、ファイアウォールなどのクラウドネイティブのセキュリティ機能を組み合わせたネットワークアーキテクチャです。
8. プラットフォームアプローチにより、既存の製品を最大限活用することができます。プラットフォームアプローチでは、サードパーティのセキュリティソリューションを統合し、統合ダッシュボードで複数のセキュリティソリューションを確認することもできます。
9. セキュリティ オペレーション センター（SOC）のワークフローを自動化（脅威の調査、検出、修復など）することで、精度を上げながら効率を高め、運用コストを削減できます。自動化することで、セキュリティチームは、絶えず変化する脅威の状況に対応しながら、進化するビジネスニーズとテクノロジーニーズに適切に対応できます。
10. 重要:どのような防御でも最も重要なのは人です。サイバーセキュリティに関して従業員を教育し、認識を高めます。組織は、フィッシング攻撃を特定する、適切なパスワードポリシーを適用する、ソフトウェアを最新の状態に保つといった、セキュリティ中心の活動を実施することの重要性について、従業員の意識を高める必要もあります。サイバーセキュリティ トレーニングは、ほとんどの従業員が嫌がる、年 1 回のコンプライアンスベースのトレーニングであってはなりません。企業文化の一部にする必要があります。

Cisco SecureX ™ は、クラウドネイティブのプラットフォームとして、シスコのセキュリティ / ネットワークポートフォリオとお客様の既存のインフラを統合します。統合型のオープンでシンプルなソリューションのため、1 つのプラットフォームであらゆる情報を可視化でき、ワークフローを自動化することで運用効率を最大限に高められます。

アジア太平洋地域のポイント

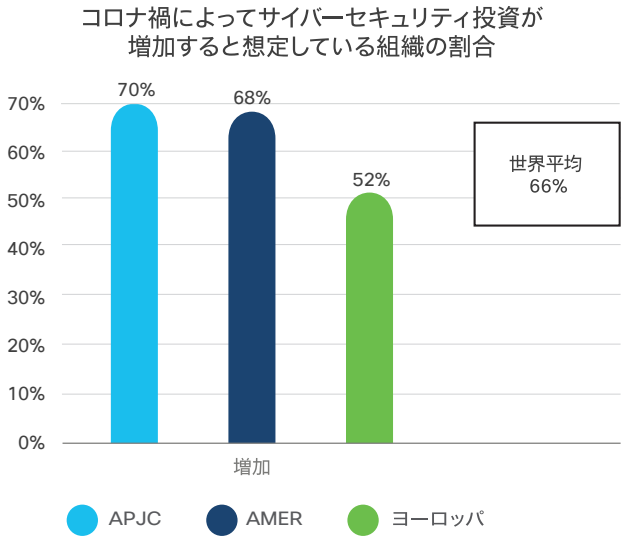
アジア太平洋地域のポイント

地域別サマリー

今回の調査では、APJC（アジア太平洋地域）の 13 の市場における 1900 を超える組織が対象になりました。その結果、シスコは、APJC 地域内の組織が、コロナ禍への対応においてグローバルな組織とどこが異なっていたかを把握できました。また、次世代のテレワークを実現するにあたり、テレワーカーと今後のサイバーセキュリティ計画をサポートするためにどのような対応をしたかも理解できました。

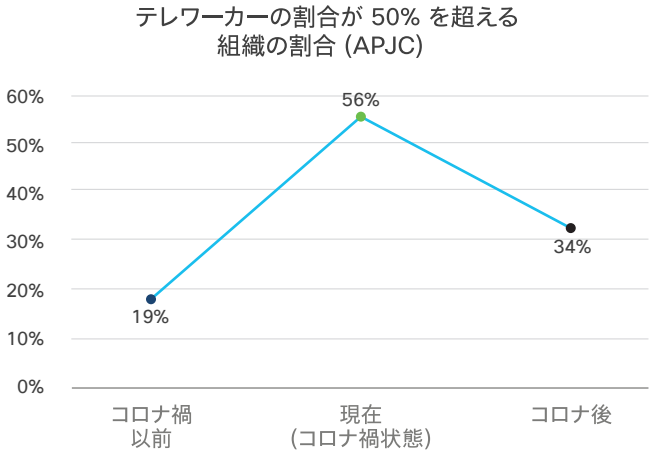
APJC の組織の 54% は、全世界の平均と同様に、テレワークへの突然の移行に際し「ある程度準備できていた」と回答しています。一方「準備できていなかった」と回答した組織は 7% で、全世界、AMER、ヨーロッパの平均よりも 1% 低くなっていました。

APJC の組織の大半は、新しい職場環境におけるニーズと制約に依然として翻弄されていますが、良い面としては、70% の組織がコロナ禍によってサイバーセキュリティへの投資を拡大すると回答していることが挙げられます。その結果、APJC では、世界の 3 つの地域の中で、サイバーセキュリティへの投資を増やそうとしている組織の数が最も多くなっています。



主な調査結果

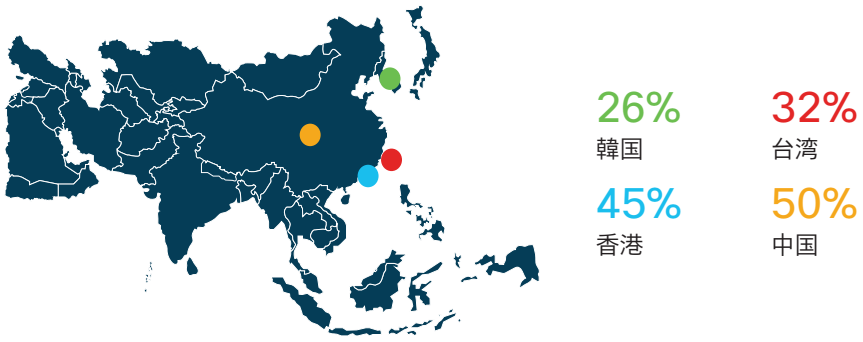
テレワーカーの推移は世界の平均と一致していますが、一部の市場ではトレンドに逆行しています。



	グローバル	APJC
コロナ禍以前	19%	19%
現在 (コロナ禍状態)	62%	56%
コロナ後	37%	34%

APJC は、ハイブリッド式の作業環境への移行において世界的なトレンドに沿っていますが、いくつか違う点があります。

- 感染が最も拡大している時期に、**韓国、香港、台湾**では、他の地域に比べてテレワーカー数が少なく、従業員の半数以上がテレワークしていると回答した組織の割合は、それぞれわずか 26%、45%、32% にとどまっています。
- 一方、**中国**の組織では、テレワーカーとオフィスワーカーが 50% ずつで均等に別れています。



これらの調査結果は、台湾では感染拡大期間を通じて大規模な全国的ロックダウン措置が取られなかったという事実に合致しています。一方、早い段階で感染が拡大した中国、韓国、香港は、感染を早期に抑え込むことができたため、多くの従業員をテレワークに移行させる必要が少なかったと思われます。

先進国でも発展途上国でも、テレワークの準備状況やサイバーセキュリティの優先順位が予想と異なる国がある

ベトナム、インド、インドネシアなどの発展途上国では、テレワークへの移行に向けた準備が進んでいますが、日本（17%）や韓国（12%）など、世界で最も技術が発展している国の一部では、テレワークへの移行の**準備ができていない**組織の割合が平均よりも高くなっています。フィリピン（12%）でも同様の傾向が見られます。

APJC の組織におけるサイバーセキュリティの優先順位は、世界の平均と一致しています。APJC の組織の 85% が、サイバーセキュリティはコロナ禍「以前より重要」または「非常に重要」であると回答しています。同地域内では、フィリピン（93%）、シンガポール（89%）、タイ（87%）、ベトナム（93%）が、サイバーセキュリティを最優先事項とする組織の割合が同地域および世界の平均よりも多くなっていました。

APJC におけるサイバーセキュリティ脅威への取り組みと課題

APJC では、新型コロナウィルスの感染拡大後、サイバー脅威やアラートが **25%** 以上急増した組織が多く、世界平均の 61% を超えています。インド（73%）、インドネシア（78%）、韓国（74%）、台湾（73%）、ベトナム（91%）で、サイバー脅威 / アラートが **25%** 以上急増し、同地域の平均 69% より多くなっています。

マレーシアの組織の 10% および日本の組織の 15% が、サイバー脅威 / アラートが増加しているか減少しているかを把握できておらず、世界平均の 8% を上回っています。組織のサイバーセキュリティ防御においては可視性が重要であるため、この傾向は懸念されます。見えないものを保護することはできません。

APJC の組織の半数以上が、オフィスのラップトップ / デスクトップ（58%）と個人のデバイス（57%）がリモート環境で保護する上で課題であると回答していて、テレワークに関しては、デバイスの保護が広く普及しています。

一方、AMER の組織の 46%、ヨーロッパの 27% に比べて、APJC の多くの企業（52%）がクラウドアプリケーションを保護すべき 3 番目の課題として挙げています。

グローバル	APJC	AMER	ヨーロッパ
オフィスのラップトップ / デスクトップ（56%）	オフィスのラップトップ / デスクトップ（58%）	オフィスのラップトップ / デスクトップ（59%）	個人用デバイス（47%）
個人用デバイス（54%）	個人用デバイス（57%）	個人用デバイス（52%）	オフィスのラップトップ / デスクトップ（47%）
顧客情報（46%）	クラウドアプリケーション（52%）	顧客情報（48%）	顧客情報（28%）

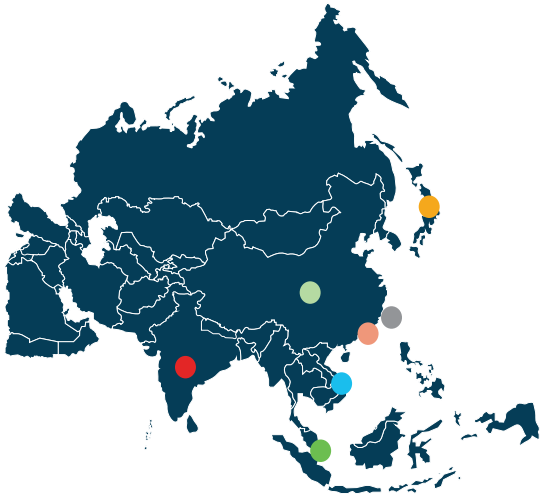
現在および将来におけるサイバーセキュリティの優先順位

APJC の組織の 97% がサイバーセキュリティ ポリシーを変更しました。これは、世界の平均 96% と一致しています。次のような変更がなされています。

- Web の制御とアクセプタブル ユース ポリシーの強化（61%）、多要素認証の導入（59%）、VPN キャパシティの拡大（56%）

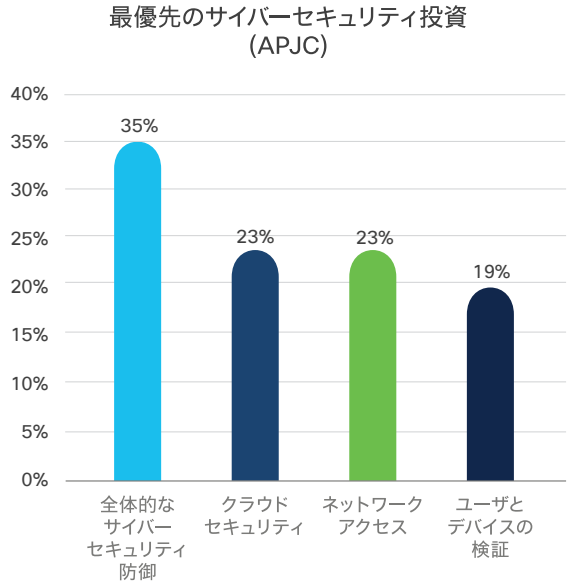
APJC の組織は、将来のサイバーセキュリティへの投資を増やし、ハイブリッド式の柔軟な作業環境を新たな標準としてとらえ、対応することに関して最も積極的です。APJC の組織の 70% が、コロナ禍の影響でサイバーセキュリティへの投資が増加すると回答しています（AMER 68%、ヨーロッパ 52%）。

- APJC で調査対象となった国の半数以上（シンガポール、ベトナム、インド、日本、中国、香港、台湾）で、70% 以上の組織がサイバーセキュリティへの投資を拡大すると回答し、同地域の平均を上回っています。
- 香港ではサイバーセキュリティへの投資を増やすと回答した組織が 80% を超え、世界で最も多くなっています。



76% シンガポール
72% 中国
78% ベトナム
80% 香港
77% インド
72% 台湾
71% 日本

テレワークに関するサイバーセキュリティへの投資は、最も重要な投資として、全体的なサイバーセキュリティ防御（35% が最優先）に組み込まれる可能性があります。組織が回答したその他の優先的な投資には、クラウドセキュリティとネットワークアクセス（それぞれ 23% が最優先）、ユーザデバイスと検証（19% が最優先）などがあります。これは、世界の傾向と一致しています。世界中の組織が、ハイブリッド式の柔軟な次世代の働き方をサポートする最善の方法を再検討し、対応しようとしています。



地域別分析 : アジア太平洋

日本

調査パラメータ	国の割合	地域平均	世界平均
次世代のハイブリッドな働き方におけるサイバーセキュリティの重要性			
従業員の半数以上がテレワークする組織の割合	・コロナ禍以前 : 13% ・コロナ禍状態 : 65% ・コロナ後 : 32%	・コロナ禍以前 : 19% ・コロナ禍状態 : 56% ・コロナ後 : 34%	・コロナ禍以前 : 19% ・コロナ禍状態 : 62% ・コロナ後 : 37%
組織にとってのサイバーセキュリティの重要性	・非常に重要 : 34% ・以前より重要 : 44% ・ある程度重要 : 19%	・非常に重要 : 44% ・以前より重要 : 41% ・ある程度重要 : 15%	・非常に重要 : 44% ・以前より重要 : 41% ・ある程度重要 : 15%
ビジネスレジリエンスの回復 : サイバーセキュリティ脅威への取り組みと課題			
サイバー脅威 / アラートの増加レベル	・25% 以上増加 : 55% ・不明 : 15%	・25% 以上増加 : 69% ・不明 : 6%	・25% 以上増加 : 61% ・不明 : 8%
直面しているサイバーセキュリティの課題 (上位 3 つ)	・セキュアアクセス : 68% ・データプライバシー : 62% ・アクセス制御の維持およびポリシーの適用 : 46%	・セキュアアクセス : 63% ・データプライバシー : 59% ・アクセス制御の維持およびポリシーの適用 : 53%	・セキュアアクセス : 62% ・データプライバシー : 55% ・アクセス制御の維持およびポリシーの適用 : 50%
リモート環境での保護における課題	・オフィスのラップトップ / デスクトップ : 58% ・個人用デバイス : 48% ・クラウドアプリケーション : 46% ・顧客情報 : 42%	・オフィスのラップトップ / デスクトップ : 58% ・個人用デバイス : 57% ・クラウドアプリケーション : 52% ・顧客情報 : 51%	・オフィスのラップトップ / デスクトップ : 56% ・個人用デバイス : 54% ・顧客情報とクラウドアプリケーション : 46%
新型コロナウィルス感染拡大時におけるテレワーク環境への移行準備状況	・十分準備できていた : 19% ・ある程度準備できていた : 63% ・準備できていなかった : 17%	・十分準備できていた : 39% ・ある程度準備できていた : 54% ・準備できていなかった : 7%	・十分準備できていた : 40% ・ある程度準備できていた : 53% ・準備できていなかった : 6%

調査パラメータ	国の割合	地域平均	世界平均
現在および将来におけるサイバーセキュリティの優先順位			
テレワークを実現するために導入した IT ソリューション(上位 3 つ)	・コラボレーションツール : 68% ・サイバーセキュリティ対策 : 58% ・クラウドベースのドキュメント共有 : 56%	・コラボレーションツール : 73% ・サイバーセキュリティ対策 : 68% ・クラウドベースのドキュメント共有 : 65%	・コラボレーションツール : 73% ・サイバーセキュリティ対策 : 68% ・クラウドベースのドキュメント共有 : 63%
導入した IT ソリューション (重要度の高い順に回答。最優先に位置づけた組織の割合)	・サイバーセキュリティ対策 : 57% ・コラボレーションツール : 56% ・クラウドベースのドキュメント共有 : 29%	・サイバーセキュリティ対策 : 50% ・コラボレーションツール : 41% ・プロフェッショナルサービス : 29%	・サイバーセキュリティ対策 : 52% ・コラボレーションツール : 41% ・プロフェッショナルサービス : 27%
テレワークをサポートするために行ったサイバーセキュリティ ポリシーの変更 (上位 3 つ)	・VPN キャパシティの拡大 : 49% ・エンドポイントの保護 : 36% ・Web の制御とアクセプタブル ユース ポリシーの強化および多要素認証の導入 : 35%	・Web の制御とアクセプタブル ユース ポリシーの強化 : 61% ・多要素認証の導入 : 59% ・VPN キャパシティの拡大 : 56%	・VPN キャパシティの拡大 : 59% ・Web の制御とアクセプタブル ユース ポリシーの強化 : 55% ・多要素認証の導入 : 53%
サイバーセキュリティ ポリシーの変更を維持する割合	・30% 以下 : 54% ・30% 超 : 33%	・30% 以下 : 54% ・30% 超 : 41%	・30% 以下 : 50% ・30% 超 : 45%
サイバーセキュリティ プロトコルの適用における課題 (上位 3 つ)	・従業員の認識 / 従業員教育の不足 : 56% ・連携されていない管理対象のツールやソリューションが多すぎる : 47% ・インターフェイスの一貫性がない : 29%	・従業員の認識 / 従業員教育の不足 : 61% ・連携されていない管理対象のツールやソリューションが多すぎる : 53% ・インターフェイスの一貫性がない : 40%	・従業員の認識 / 従業員教育の不足 : 59% ・連携されていない管理対象のツールやソリューションが多すぎる : 50% ・インターフェイスの一貫性がない : 35%

調査パラメータ	国の割合	地域平均	世界平均
増加するサイバーセキュリティへの投資			
コロナ禍による今後のサイバーセキュリティへの投資の変化	・増加：71% ・減少：3% ・変更なし：25%	・増加：70% ・減少：11% ・変更なし：17%	・増加：66% ・減少：9% ・変更なし：22%
将来サイバーセキュリティへの投資が増加する割合	・30% 以下：62% ・30% 超：29%	・30% 以下：58% ・30% 超：39%	・30% 以下：59% ・30% 超：36%
サイバーセキュリティへの投資（重要度の高い順に回答。最優先に位置づけた組織の割合）	・全体的なサイバーセキュリティ防御：39% ・ネットワークアクセス：28% ・ユーザとデバイスの検証：17% ・クラウドセキュリティ：16%	・全体的なサイバーセキュリティ防御：35% ・ネットワークアクセスおよびクラウドセキュリティ：23% ・ユーザとデバイスの検証：19%	・全体的なサイバーセキュリティ防御：34% ・ネットワークアクセス：24% ・クラウドセキュリティ：22% ・ユーザとデバイスの検証：20%

次世代のセキュアなテレワークに関するレポートについて

2020 年 2 月から 3 月にかけて、組織は従業員に在宅勤務を義務付けることで従業員を保護しようとしました。この措置は、地域や従業員を保護するために必要なものでしたが、セキュリティ担当者が、自分のチームやセキュリティ担当者に頼る従業員、および担当している重要なシステムから物理的に切り離されることになりました。また、テレワークに移行することにより、すでに厳しい状況にあった中で、既存のデジタル化ポリシーと事業の継続性計画に大きな変更が発生しました。

だからといって、この新しい働き方に適応する方法が見つからなかったということではありません。シスコは、2020 年 6 月 16 日から 9 月 4 日にかけて、金融サービス、医療、設計、運輸などを含む幅広い 30 の業界において、小規模から大規模まですべての規模の企業を対象に、3,000 人を超える IT 意思決定者に対して調査を行いました。調査の目的は、サイバーセキュリティの観点から、コロナ禍による影響を把握することです。

3196 人の回答者

対象：21 の市場

AMER：
- ブラジル
- カナダ
- メキシコ
- 米国

ヨーロッパ：
- フランス
- ドイツ
- イタリア
- 英国

APJC：
- オーストラリア
- 中国
- 香港
- インド
- インドネシア
- 日本
- 韓国
- マレーシア
- フィリピン
- シンガポール
- 台湾
- タイ
- ベトナム

業種：
- 会計
- 設計
- ビジネスコンサルティング
- 化学 / 製造
- 建築
- 教育
- 金融サービス
- 政府 / 自治体
- 医療
- 製造：
- 非コンピュータ関連
- 小売
- ソフトウェア開発
- 電気通信
- 運輸
- 卸売 / 流通
- 非営利 / 慈善事業

対象読者：
自社の IT を担当するプロフェッショナル

対象企業規模：
- 小規模（従業員 1 ～ 249 人）、
- 中規模（従業員 250 ～ 999 人）、
- 大規模（従業員 1000 人以上）

目的：

- 組織の従業員の一部またはすべてをほぼ一夜にして**テレワーク環境**に移行した際の**課題**と、世界中の組織がテレワーク環境で自社のビジネスを保護することに対する**準備状況**を調査する。

- サイバーセキュリティに関する優先事項、ポリシー、投資の変化など、企業がこの突然の移行にどのように適応したかを理解する。

- 企業がハイブリッド作業環境を理解し、現在の状況にも将来にも安全に適応できるようにする。

調査パラメータ

#1 コロナ禍におけるテレワーカーの増加と、テレワーカーをサポートするためのサイバーセキュリティの重要性

1) 新型コロナウィルスの感染拡大前、拡大中、収束後のテレワーカーの人数
2) コロナ禍の現在におけるサイバーセキュリティの重要性およびテレワークの状況

#2 サイバーセキュリティに関する準備状況、脅威、課題

1) テレワークに（突然）移行した際に、サイバーセキュリティの機能 / ソリューションにどの程度対応できていたか
2) 大規模なテレワーク中に発生したサイバーセキュリティの課題の種類およびその重要度
3) テレワーク環境を保護する上で最も困難だった課題

#3 テクノロジーの優先事項およびテレワークをサポートするために採用したテクノロジー

1) 採用したテクノロジーの種類
2) 採用したテクノロジーの重要度とその順位

#4 テレワーカーをサポートするために変更したサイバーセキュリティ ポリシーとプロトコル

1) 変更のタイプ
2) サイバーセキュリティ ポリシーを変更した割合
3) サイバーセキュリティ プロトコルを適用する際の課題

#5 現在および将来におけるサイバーセキュリティへの投資

1) コロナ禍が組織の将来のサイバーセキュリティ投資に影響を与えるか
2) 投資の増加、減少、現状維持の割合
3) 将来のサイバーセキュリティ投資における重要度

次世代のセキュアなテレワークに関するレポート

cisco SECURE