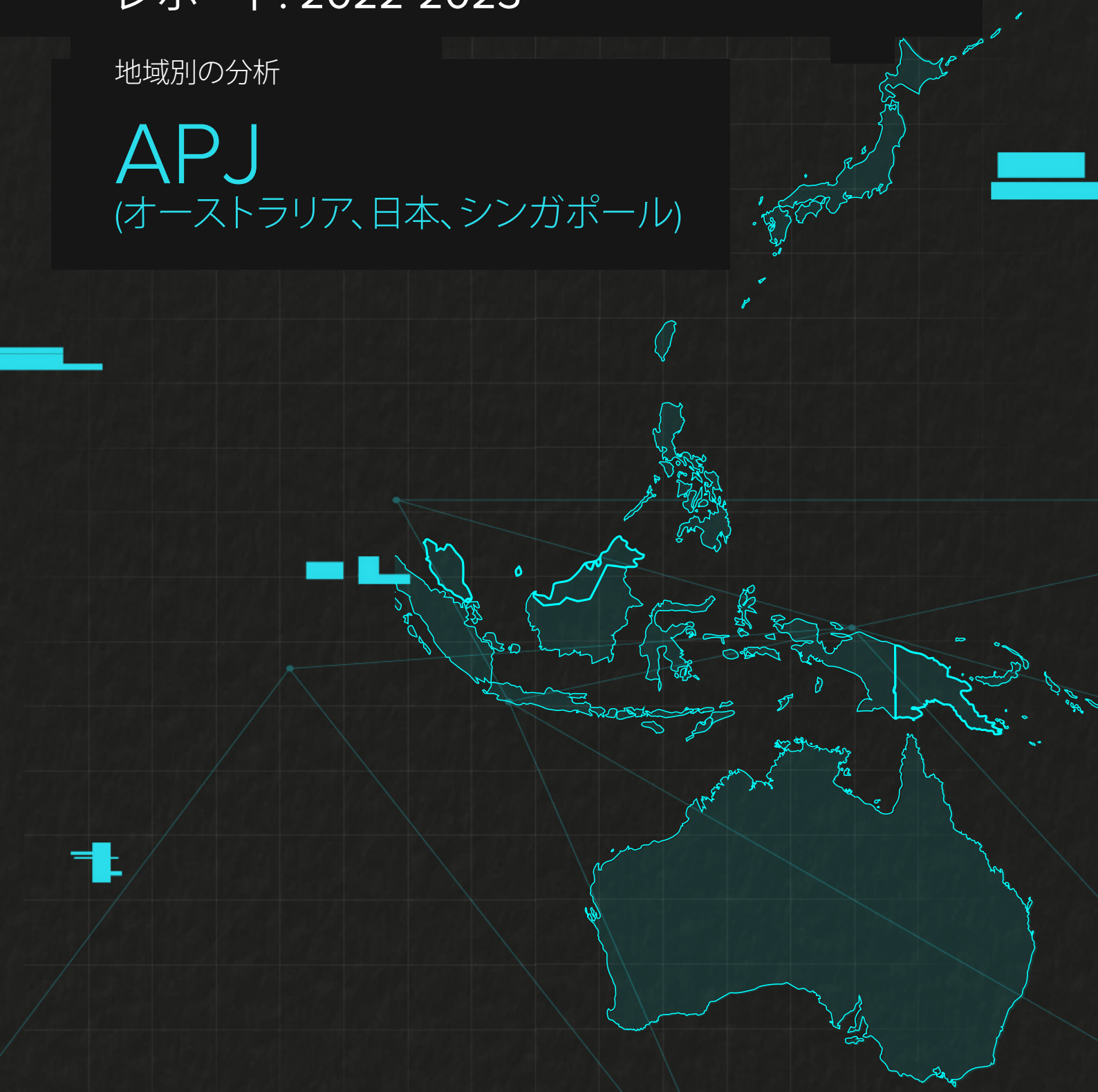
ARMIS®

サイバー
戦争の現状

ARMIS サイバー戦争の現状と傾向に関するレポート: 2022-2023

地域別の分析

APJ
(オーストラリア、日本、シンガポール)



目次

はじめに

グローバルな **Armis サイバー戦争の現状と傾向に関するレポート：2022-2023**をお読みになった方は、サイバー戦争を取り巻く脅威状況の進化を理解することが、ビジネスおよび IT のリーダーにとって非常に重要であることをご存知でしょう。そうすれば、こうした攻撃から防御するためのサイバーセキュリティ態勢を向上させることができます。本レポートを作成するにあたり、Armis は、全世界の IT およびセキュリティ専門家 6,021 人を対象に、サイバー戦争、攻撃パターン、サイバー支出などに対するセキュリティ専門家の意識に関連する世界的な傾向を調べるための調査を依頼しました。回答は、2022 年 9 月 22 日から 2022 年 10 月 5 日の間に集められました。

Armis は、受賞歴のある Asset Intelligence and Security Platform のデータを活用して、調査結果を現実のデータ傾向と照らし合わせて検証しました。2022 年 6 月 1 日から 2022 年 11 月 30 日までに収集された Armis プラットフォームの独自データでは、サイバー攻撃は減速していないどころか、悪化していることが確認されています。9 月から 11 月にかけて、全世界の Armis の顧客に対する脅威アクティビティは、その前の 3 か月と比較して 15% 増加しました。さらに、Armis は、重要インフラ組織に対する脅威アクティビティが最も多いことを確認し、さまざまな業界と比較して、ヘルスケア組織が 2 番目に多く標的とされていることを確認しました。

これらの世界的な調査結果に加え、Armis は地域別の調査結果や国別の分析を実施し、地域に限定した独自の洞察を提供しています。これは、個々の読者がどこに物理的な拠点を置き、どの国でビジネスを行っているかによって、より大きな影響を与える可能性があります。**今回の国別分析では、オーストラリア (511 名)、シンガポール (501 名)、日本 (501 名) の 3 か国から選ばれた、ヘルスケア、製造、小売、金融サービスなど、さまざまな業種で働く 1,513 名の回答者から得られた調査結果に焦点を当てています。**

調査結果の要約

全体として、Armis は、調査対象となった APJ 3 か国 (オーストラリア、日本、シンガポール) の IT およびセキュリティ専門家の回答を分析し、EMEA および米国の他のグローバル企業の回答者と比較して、いくつかの重要な相違点と傾向を特定しました。以下では、これらの調査結果とそれが示唆する傾向について詳しく説明します。

地域全体をおおまかに見ると、脅威のレベルは上昇しています。しかし、今回調査した APJ の企業における侵害件数は、世界の他の地域、特に EMEA に拠点を置く組織と比較すると、依然として低い水準にとどまっています。これに伴い、APJ の回答者の一部は、サイバー戦争が組織のさまざまな側面に与える影響について、無関心または無頓着であると回答しています。これらの組織が他の組織よりも攻撃を阻止することに成功していることは明らかですが、グループとして見ると、世界の他の回答者と比較して、平均レベルの準備態勢を示しているにすぎません。

国別分析では、オーストラリア、日本、シンガポールの回答者が、地域ごとに異なる傾向を示しています。

- オーストラリアでは、サイバー戦争の脅威を懸念し、その脅威に対応したビジネス上の意思決定を行っています。また、数百万ものオーストラリア人に広範な影響を与えた最近の一連のサイバー攻撃にもかかわらず、政府のサイバー戦争に対する防衛能力に高い信頼を示しています。
- 日本では、回答者全体がサイバー戦争に懸念を示していますが、これらの脅威に対して依然として無関心な回答者も非常に多くなっています。日本と他の国の回答者を比較した場合、際立つ調査結果があるのでしょうか？日本では、ランサムウェア攻撃時に身代金を支払う可能性が最も低くなっています。
- 革新的な技術先進国として知られるシンガポールの回答者は、サイバー戦争の脅威のためにデジタル変革プロジェクトを停滞または停止させていると答えています。このような脅威アクティビティの増加により、今後数か月間、サイバーセキュリティ態勢を向上させるための投資を継続する結果になるでしょう。

これらの調査結果やその他の詳細については、続きをご覧ください。

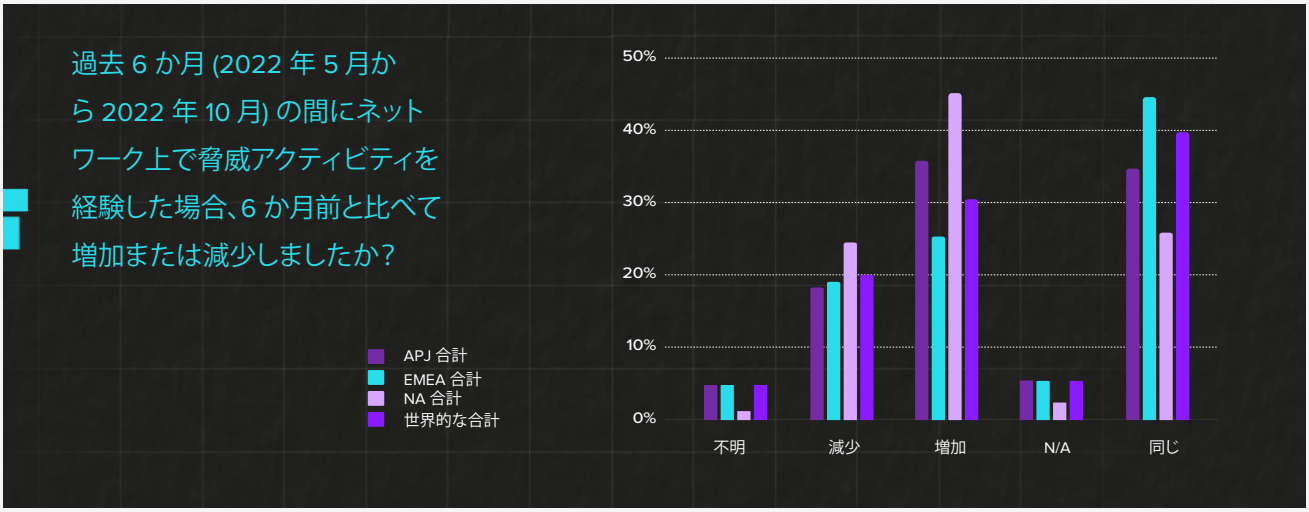
地域別の分析
APJ (オーストラリア、日本、シンガポール)

世界的に見ると侵害は比較的少ないが、地域的に見ると脅威が増加傾向にある

今回の調査によると、調査対象となったこれら APJ 3 か国 (オーストラリア、日本、シンガポール) の回答者は、世界中の回答者と比較してサイバーセキュリティ侵害の経験が最も少なく、オーストラリア、日本、シンガポールに拠点を置く IT・およびセキュリティ専門家の 53% が、自社が 1 件以上のサイバーセキュリティ侵害を経験したと答えています。さらに詳しく見ると、シンガポールは最も多くのサイバーセキュリティ侵害を経験しており、60% が 1 件以上侵害されたことがあると回答しています。オーストラリアの回答者の 57%、日本の回答者の 44% が 1 件以上の侵害を経験しています。一方、EMEA の回答者のほぼ 5 人に 3 人 (58%)、米国の回答者の 10 人に 7 人 (73%) が、自社が 1 件以上のサイバーセキュリティ侵害を経験したと答えています。

APJ 地域の調査対象の回答者は、EMEA 地域の回答者と比べて侵害の経験は少ないものの、オーストラリア、日本、シンガポールの IT およびセキュリティ専門家がネットワーク上での脅威アクティビティの増加を経験している割合は高くなっています。2022 年 5 月から 10 月の間に、これらの回答者はその 6 か月前と比較してネットワーク上で脅威アクティビティが 36% 増加したと答えています。EMEA で同じ質問をしたところ、同じように答えたのは回答者の 25% に過ぎませんでした。さらに、今回調査した APJ 各国の回答者の約 5 人に 3 人 (61%) が、サイバー戦争の行為を当局に報告しなければならなかったのに対し、EMEA では 33% にとどまっています。

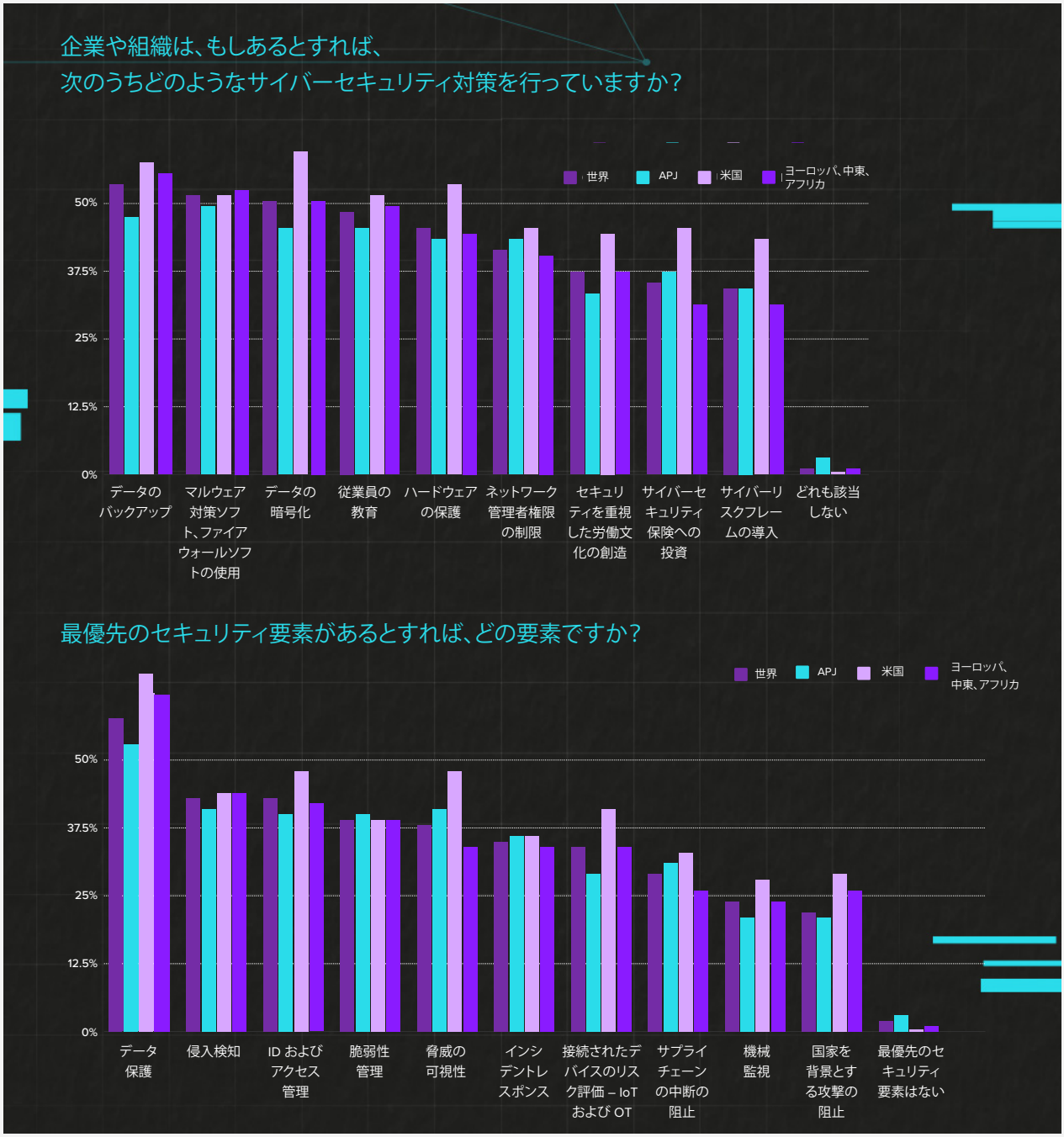
また、今回の調査では、オーストラリア、日本、シンガポールを拠点とする企業に対する脅威アクティビティが、これらの組織で行われる意思決定に影響を及ぼしていることがわかりました。調査対象の IT 専門家の 5 人に 3 人以上 (58%) が、サイバー戦



争の脅威により、組織がデジタル変革プロジェクトを停滞または停止させていると回答しています。さらに、ほぼ 5 人に 3 人 (59%) が、サイバー戦争の脅威がデジタル化を遅らせるであろうと回答しています。

調査対象の APJ 企業が実施し、優先しているサイバーセキュリティ対策は世界平均並み

このような脅威のレベルと企業への潜在的な影響にもかかわらず、調査対象となった IT 専門家の 4 分の 1 以上 (29%) が、サイバー戦争が組織全体に与える影響について無関心または無頓着で、10 人に 3 人 (30%) がサイバー戦争が自社の重要インフラや自社のサービスに与える影響について無関心または無頓着です。このような懸念の欠如は、EMEA や米国の回答者と比較して、回答者全体が世界平均並みのセキュリティ対策を実施し、特定のセキュリティ要素をより一貫して優先していることに起因していると考えられます。また、これまでサイバー攻撃を阻止することに成功していることも一因となっています。



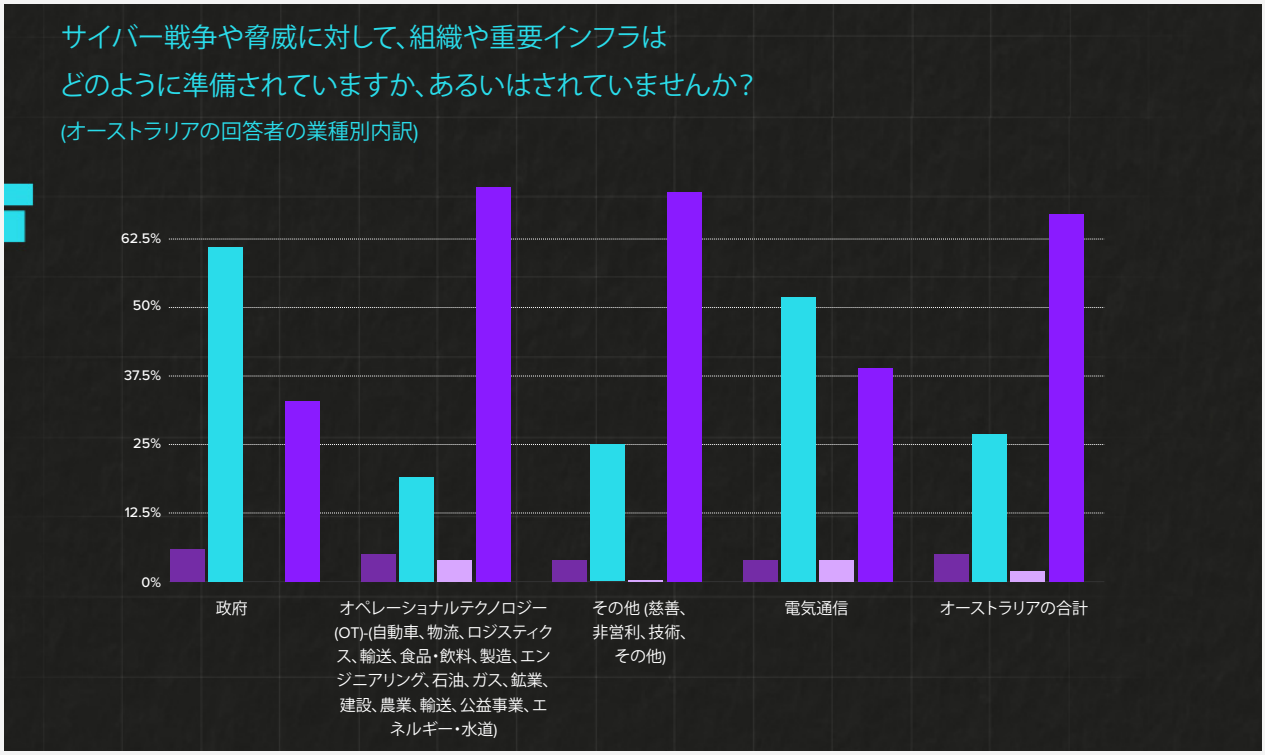
次に、国別の傾向分析について詳しく見てみましょう。

国別の分析
ARMIS サイバー戦争の現状と傾向に関するレポート: 2022-2023 から得られたオーストラリアの傾向

サイバー戦争の脅威に対する懸念が、オーストラリアでのビジネス上の意思決定に影響を与えている

オーストラリアの回答者は、世界平均 (31%) よりも多くの脅威アクティビティを経験しています。オーストラリアの回答者の 40% が、2022 年 5 月から 10 月の間に、その 6 か月前と比較して、ネットワーク上でより多くの脅威アクティビティを経験し、半数以上 (57%) が組織でサイバーセキュリティ侵害を経験したと答えています。

特にサイバー戦争に関しては、オーストラリアの回答者の 3 分の 2 以上 (68%) が、サイバー戦争の行為を当局に報告する必要があったと答えています。このことは、オーストラリアの IT およびセキュリティ専門家の 83% がサイバー戦争が企業全体に及ぼす影響を懸念し、84% が自社の重要インフラ、83% が自社のサービスについて懸念している理由を説明するのに役立つと思われます。こうした懸念にもかかわらず、調査対象となったオーストラリアの業界リーダーの大半 (93%) は、これらの脅威に対応するための制度的インフラおよび重要インフラの準備態勢に自信があると感じています。



サイバー戦争の脅威はこうした懸念を超えるものであるため、ビジネス上の意思決定を促しています。オーストラリアの回答者の大多数 (79%) は、サイバー戦争の脅威のためにデジタル変革プロジェクトを停滞または停止させていると答えています。また、66% がロシア・ウクライナ紛争の影響でサプライヤーを再検討していると回答しています。これは調査対象の APJ 各国の平均 (54%) よりも多く、また世界平均 (51%) よりも多い結果となっています。

オーストラリア人は、最近相次いで非常に影響の大きい侵害を受けたにもかかわらず、政府のサイバー戦争に対する防衛能力に非常に自信を持っている

この調査によると、オーストラリアの回答者の92%が、政府がサイバー戦争から防御することに自信を持っているのに対し、世界平均では 71% となっています。また、オーストラリアの回答者は、「Essential Eight」として知られる勧告など、政府からのガイダンスが必須であることに圧倒的多数で同意しています (95%)。

このような自信にもかかわらず、2022 年 9 月から 11 月中旬にかけて、Medibank Private や Optus など 8 社の現地企業が侵害されました。

Medibank の侵害だけで、現在と以前の顧客 1000 万人に影響を与えました。政府機関は現在、影響を最小限に抑えることを期待して、これらの攻撃に介入しています。司法長官の調査により、ロシア在住の犯罪組織が関与していることが明らかになり、オーストラリア政府は、オーストラリアで発生したデータ侵害に対して企業に課される罰金を増額しました。Medibank と Optus の両社が世間からの激しい非難を受けた結果として、プライバシー監視機関であるオーストラリア情報委員会の権限拡大など、オーストラリアのプライバシー法に関するより幅広い改革が進むと思われます。このため、サイバーセキュリティに対する需要はかつてないほどピークに達しています。自国がサイバー紛争に巻き込まれた場合にサイバー防衛連盟への協力を支持するかという質問では、世界平均 (63%)、APJ 平均 (59%) と比較して、オーストラリアの回答者が最も高いレベル (70%) を示しました。

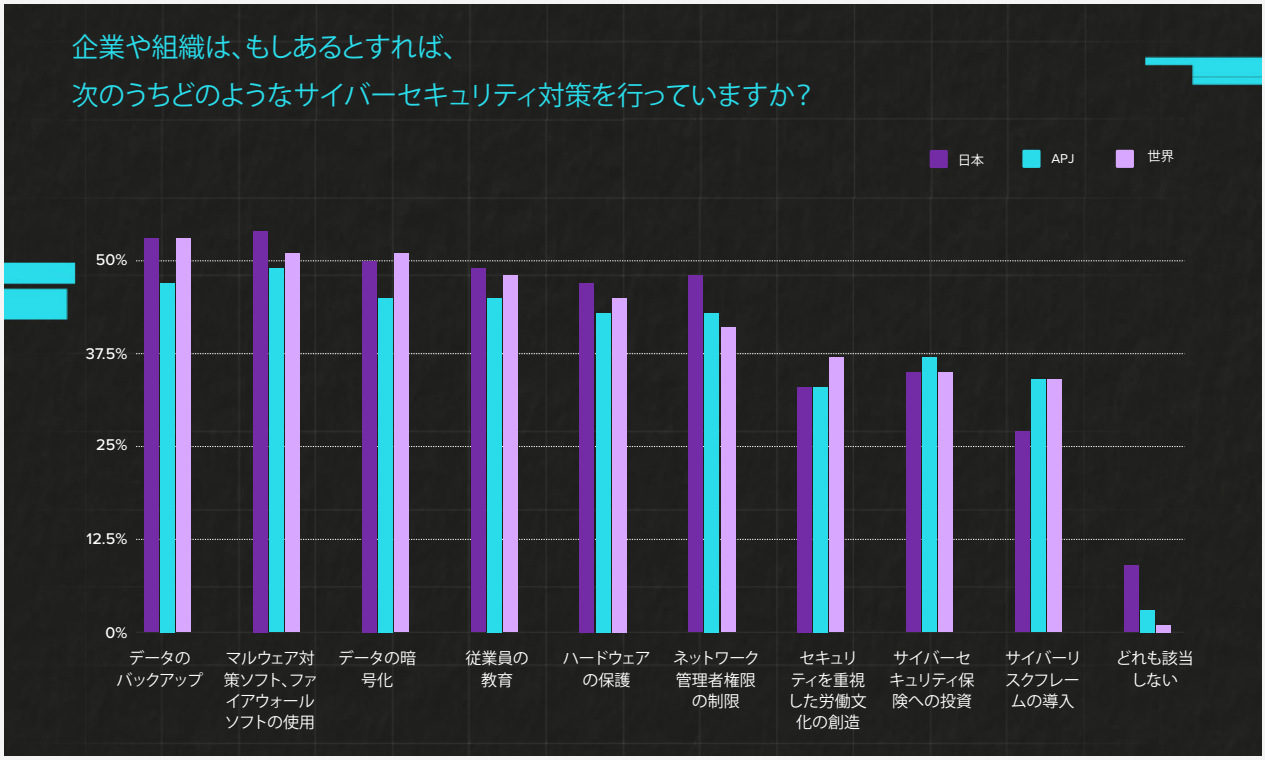
国別の分析
ARMIS サイバー戦争の現状と傾向に関するレポート: 2022-2023 から得られた日本の傾向

日本の IT およびセキュリティ専門家はサイバー戦争に懸念を抱いているが、多くの人は脅威に無関心のように見える

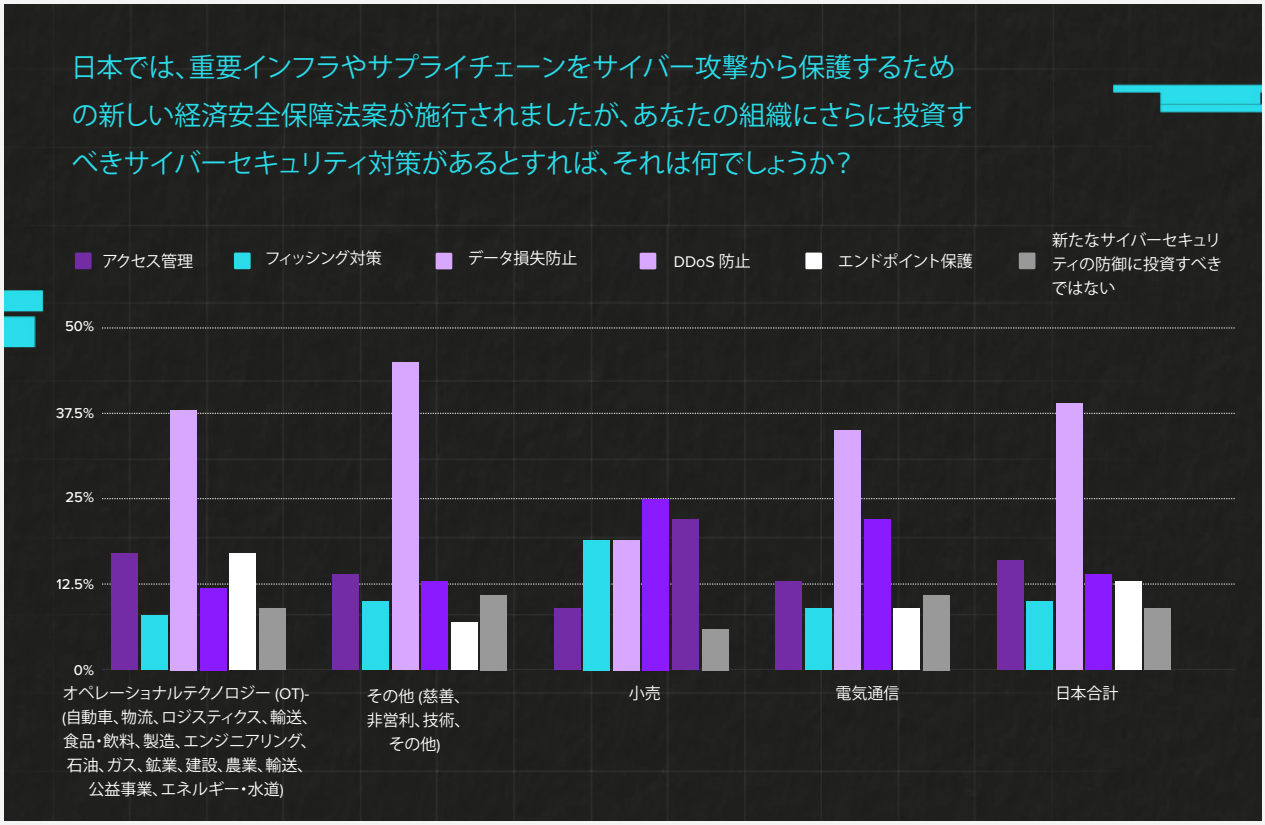
日本の回答者の 44% が、自社でサイバーセキュリティ侵害を経験したことがあると答えています。また、調査対象となった IT 専門家の 10 人に 7 人強 (71%) が、ウクライナや台湾の状況のような国際的な政治紛争や国家的な侵害が、自社のサイバーセキュリティに影響を及ぼすだろうと考えています。さらに、日本の回答者は、政府のサイバー戦争に対する防衛能力について、APJ および世界的に調査した他の回答者の平均信頼度レベルが 71% だったのに対し、著しく低い結果になっています (33%)。

サイバー戦争が仕事のさまざまな側面に与える影響について尋ねたところ、回答者の 59% が組織全体、58% が自社の重要インフラ、56% が自社のサービスについて懸念を示しました。日本の回答者の 60% が、組織は現在、サイバー戦争の脅威に対応するために特別に設計されたプログラムや対策を備えていると回答しており、APJ の回答者平均 (79%) や世界平均 (84%) を大幅に下回っています。

こうした状況にもかかわらず、日本の回答者は、自社のサイバーセキュリティプログラム、人材、プロセスに十分な予算があると感じており、62% の回答者が「ある程度同意する」または「強く同意する」と回答しています。しかし、組織で最優先するセキュリティ要素について尋ねたところ、9% が「最優先のセキュリティ要素はない」と答えています。また、日本の回答者の 9% が、データのバックアップ、データの暗号化、サイバーセキュリティを重視した労働文化の創造など、標準的なサイバーセキュリティ対策をまったく行っていないと回答しています。しかしながら、残りの回答者は、APJ や世界平均と比較して、平均以上の準備態勢を示しました。

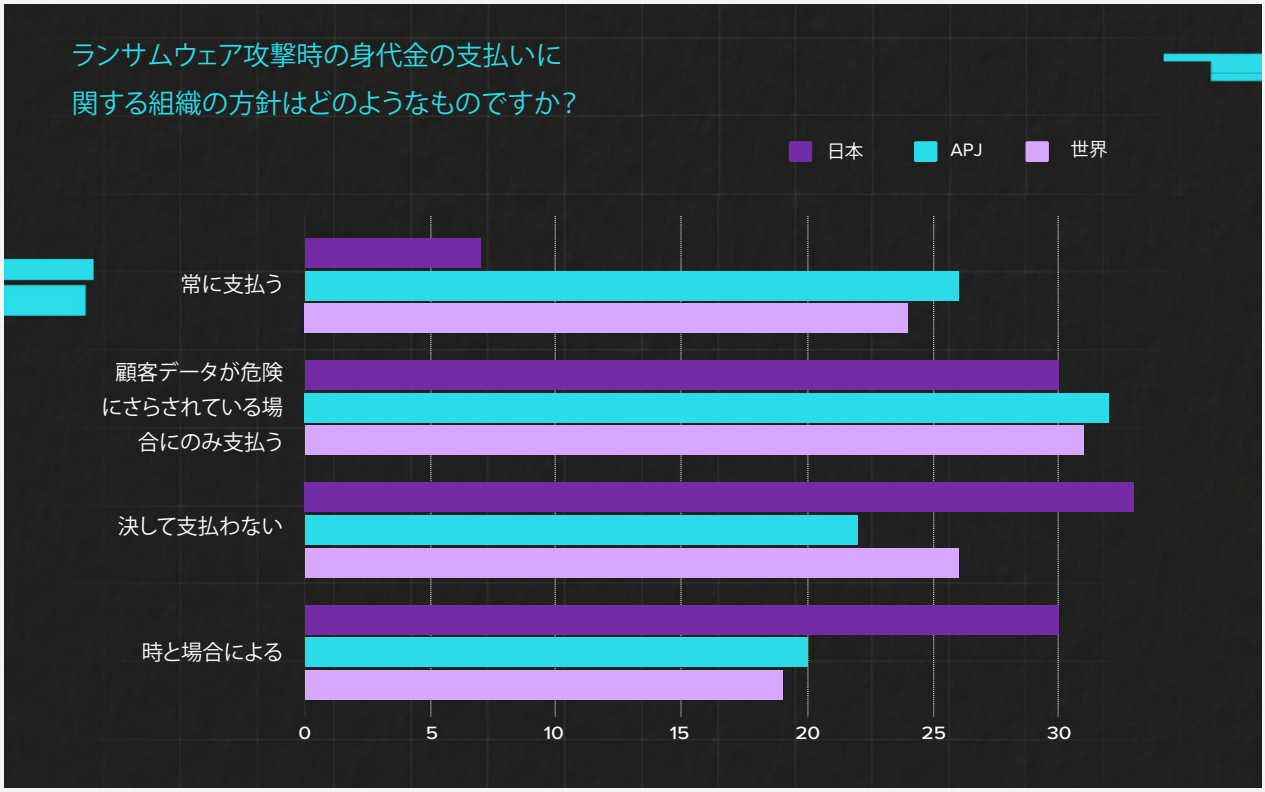


日本では、重要インフラとサプライチェーンをさらなる攻撃から保護することを目的とした新しい経済安全保障法案が施行されたため、回答者は組織の主要な優先事項として、データ損失防止 (39%)、アクセス管理 (16%)、DDoS 防止 (14%)、エンドポイント保護 (13%) にさらに投資すべきだという考えを示しています。また、回答者の 9% が、組織は新たなサイバーセキュリティ対策に投資すべきではないと考えていることを示しました。



日本の企業は、ランサムウェア攻撃時に身代金を支払う可能性が最も低い

ランサムウェア攻撃時の身代金の支払いに関する組織の方針について尋ねたところ、日本の回答者は、攻撃時に身代金を支払う可能性が世界で最も低いことを示しました。

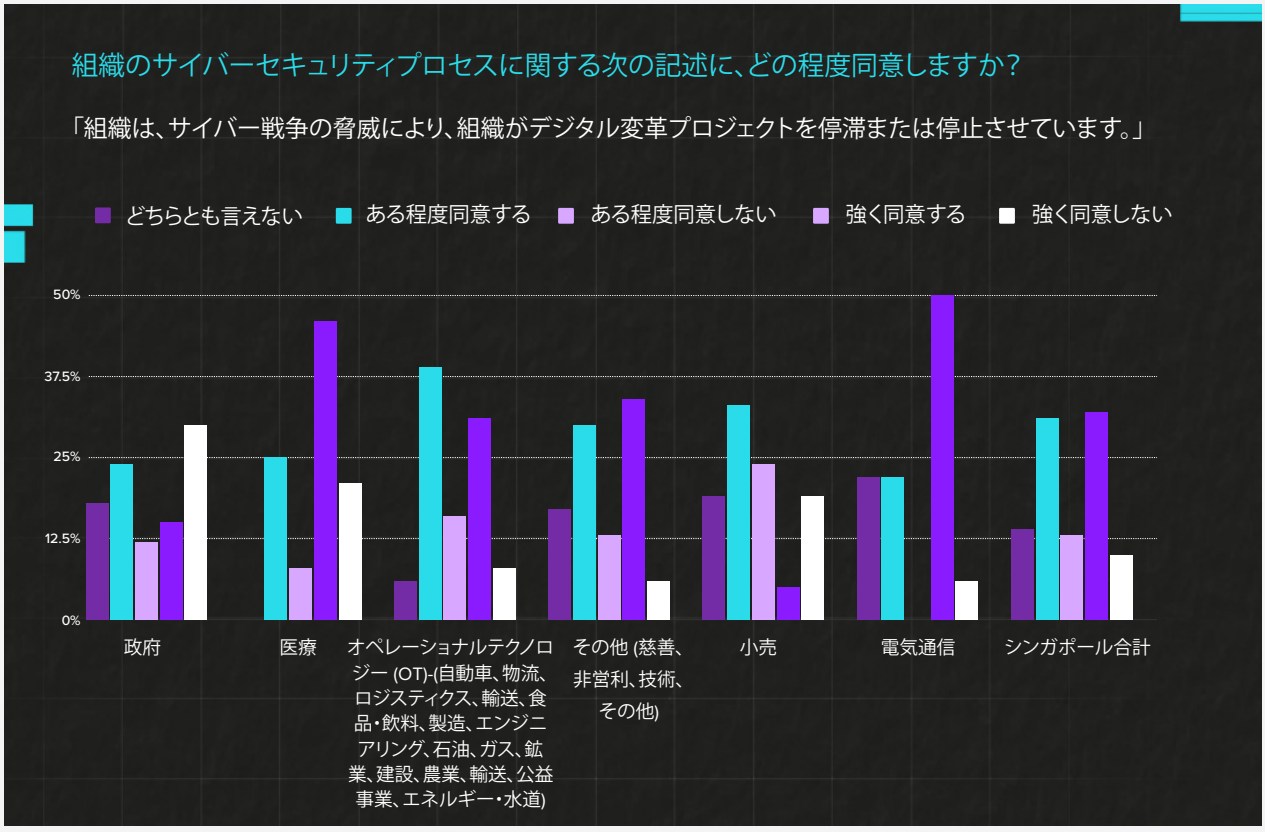


国別の分析
ARMIS サイバー戦争の現状と傾向に関するレポート: 2022-2023 から得られたシンガポールの傾向

回答者は、サイバー戦争の脅威のためにデジタル変革プロジェクトを停滞させている

シンガポールは、技術と革新のハブとして世界的に知られています。しかし、Armis の今回の調査結果は、サイバー攻撃の脅威が、都市国家の開発意欲に別の脅威を与えていることを強く示唆しています。サイバー戦争の脅威に対応するため、現地の回答者の 63% が、デジタル変革プロジェクトを停滞または停止させていると答えています。これは調査対象の APJ 平均 (58%) および世界的な平均 (55%) の両方を大きく上回っています。

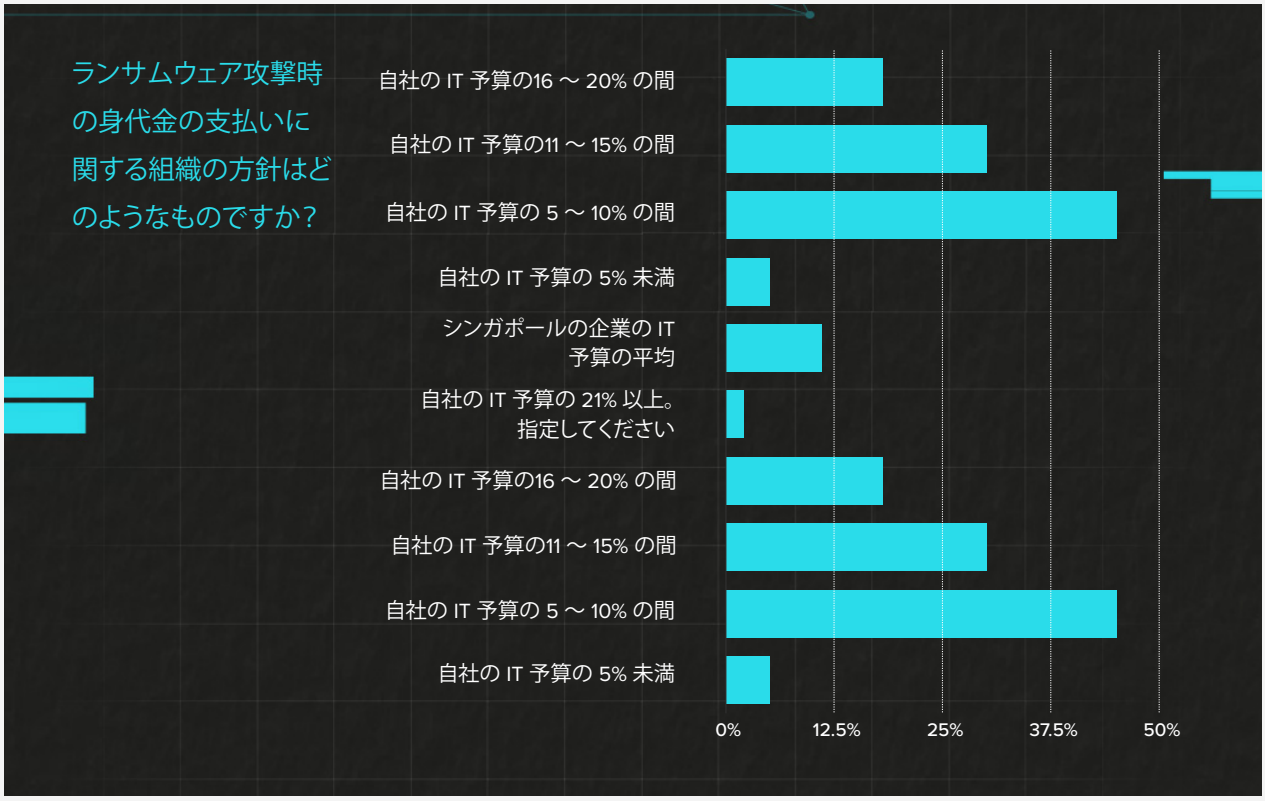
日本では、重要インフラとサプライチェーンをさらなる攻撃から保護することを目的とした新しい経済安全保障法案が施行されたため、回答者は組織の主要な優先事項として、データ損失防止 (39%)、アクセス管理 (16%)、DDoS 防止 (14%)、エンドポイント保護 (13%) にさらに投資すべきという考えを示しています。また、回答者の 9% が、組織は新たなサイバーセキュリティ対策に投資すべきではないと考えていることを示しました。



脅威アクティビティの増加に伴い、セキュリティ支出が増加する

シンガポールで調査対象となった IT およびセキュリティ専門家の 5 人に 3 人 (60%) が、自社でサイバーセキュリティ侵害を経験したことがあると答えています。また、現地の回答者の 36% が、2022 年 5 月から 10 月の間に、その 6 か月前と比較して、ネットワーク上で脅威アクティビティが増加したと答えています。同じ時期で調べると、脅威アクティビティの増加が最も大きかったのは、ヘルスケア業界の回答者 (63%) で、次いで電気通信業界の回答者 (53%) となっています。

シンガポールの回答者の大多数 (83%) は、自社がサイバーセキュリティプログラム、人材、プロセスに十分な予算を割り当てていると考えており、89% は自社が包括的なサイバー防御プログラムを備えていると感じています。2022 年 5 月から 10 月の間に、シンガポールの回答者は多くのサイバーセキュリティツールやサービスに投資していました。投資対象では、エンドポイント保護 (46%)、セキュリティ情報イベント管理 (SIEM)(44%)、アクセス管理 (43%)、脆弱性管理 (43%)、マネージドセキュリティサービスプロバイダー (MSSP)(40%) などが上位に挙がっています。IT およびセキュリティ専門家の 83% は、最近および現在進行している突発的な世界的な出来事(パンデミック、ウクライナ戦争など) に対応して、自社がサイバーセキュリティに多くの予算を投じる可能性が高いと考えています。



これらの調査結果が重要なのはなぜですか?

脅威の状況が変化する中、企業がサイバー戦争の脅威に十分な備えができるようになるのは、まだまだ先のことです。防御が強化されればされるほど、攻撃者も強化されます。そこで、企業は今、適切な対応策を実行する必要があるのです。サイバー戦争の脅威は、デジタル変革プロジェクトの実施から技術的な進歩を立ち止まらせています。セキュリティに対する積極的なアプローチとして、資産を完全に可視化する適切な計画を策定し、定期的にテストすることが、増大する脅威から企業を保護するための正しい方向への一歩です。

組織を守るために何ができますか?

では、組織は何をすればよいのでしょうか?早期発見と継続的な監視は、セキュリティ態勢を改善し、迅速に是正するための最良の方法です。結局のところ、問題があることに気づかなければ、それを修正することはできません。同様に、資産が見えなければ、それを保護することはできません。そこで、Armis が役に立ちます。

ARMIS アセットインテリジェンスプラットフォーム

Armis アセットインテリジェンスプラットフォーム は、すべての資産タイプにおいて、統一された資産の可視化とセキュリティを提供します。これは、マネージド、アンマネージドを問わず、情報技術 (IT)、Internet of Things (IoMT)、オペレーショナルテクノロジー (OT)、Internet of Medical Things (IoMT)、クラウド、セルラー IoT などが対象となります。エージェントレス Software-as-a-Service (SaaS) プラットフォームとして提供される Armis は、既存の IT およびセキュリティスタックとシームレスに統合し、現在の運用やワークフローを中断することなく、組織のセキュリティ態勢の改善に必要なコンテキストに基づく情報を迅速に提供します。Armis は、脅威やサイバー戦争などを問わず、目に見えない運用リスクやサイバーリスクからの保護、効率性の向上、リソースの使用の最適化、ビジネスの成長のために新技術による安全な革新を実現します。

今すぐ登録して**セキュリティリスク評価**を実行し、どのアセットが最も攻撃されやすいかを調べてください。これらの情報を利用して、リスク軽減戦略に優先順位を付け、すべての脆弱性の特定と優先順位付けが必要な規制に完全に準拠してください。

Armis のカスタムデモをご希望の方は、こちらをご覧ください。armis.com/demo.

Armis サイバー戦争の現状と傾向に関するレポート:2022-2023 の世界規模での調査結果をより掘り下げて理解したい方は、こちらをご覧ください。**armis.com/cyberwarfare.**

サイバー
戦争の現状

ARMIS について

資産可視化とセキュリティにおけるリーディングカンパニーである Armis は、コネクテッドデバイスから生じる新たな脅威の状況に対応するために設計された、業界初の統一アセットインテリジェンスプラットフォームを提供しています。Fortune 100 企業は、IT、クラウド、IoT デバイス、医療機器 (IoMT)、オペレーショナルテクノロジー (OT)、産業用制御システム (ICS)、5G に渡るすべての管理・非管理資産を完全に把握できる、当社のリアルタイムかつ継続的な保護ソリューションを導入しています。Armis は、サイバーセキュリティにおいて、パッシブなサイバーアセット管理、リスク管理、ポリシー自動施行を提供します。Armis は、カリフォルニア州に本社を置く、非上場企業です。

armis.com

info@armis.com

20230110-1

ARMIS®