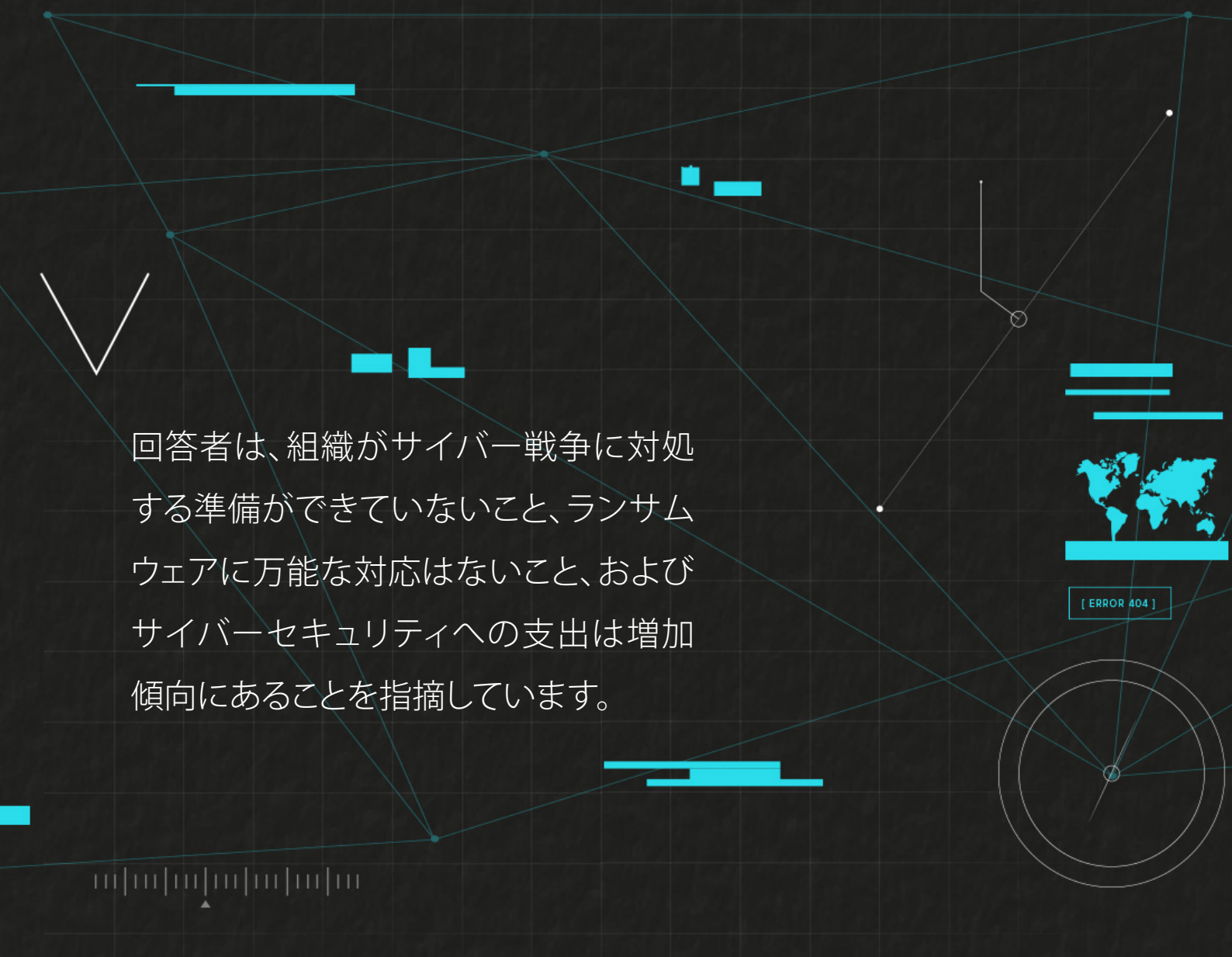
ARMIS®

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

世界の IT およびセキュリティ専門家のサイバー支出および対策に関する意識を確認する

回答者は、組織がサイバー戦争に対処する準備ができていないこと、ランサムウェアに万能な対応はないこと、およびサイバーセキュリティへの支出は増加傾向にあることを指摘しています。



NADIR IZRAEL による序文

ARMIS CTO 兼共同創立者

Armis は、世界のサイバー戦争に関する調査研究および市場分析の結果をお伝えできることを嬉しく思います。このグローバルレポートと姉妹版の地域レポートの内容が、皆様にとって貴重で価値あるものになることを願っています。

私たちが今置かれている状況を、もっとよく考えてみましょう。**主要なアナリストたち**[1]は、2025 年までには、サイバー攻撃者はオペレーショナルテクノロジー (OT) 環境を武器化し、人間に危害を加えたり殺したりすることに成功するだろうと予測しています。これは極端に思えるかもしれませんが、攻撃者が偵察やスパイの領域から、サイバー戦争ツールの物理的応用へと移行しているという、サイバー戦争の傾向を端的に表しています。このような物理的サイバー兵器はすでに発見されていますが、特に致命的な効果をもたらしたものはありません。たとえば、2017 年に発見されたマルウェア、Triton は、サウジアラビアの石油化学プラントの安全計装システム (SIS) のコントローラを**標的として無効化**[2]しました。もし問題が発見されなければ、プラント全体の災害につながったと考えられます。そして、**2021 年 2 月**[3]、米国フロリダ州にある小さな都市の給水設備に、ハッカーがリモートアクセスで毒を混入させようとしました。すでに医療分野に対するランサムウェア攻撃で**人命が失われた**[4]例もあり、意図的か否かにかかわらず、サイバー攻撃に潜在する影響の大きさは明らかです。

サイバー軍拡競争の未来は物理的サイバー脅威にあるのですが、サイバー兵器は特に新しい概念ではありません。2016 年、**Shadow Brokers が引き起こした流出**[5]により、**国家安全保障局**[6] (NSA) のサイバー兵器が世界中に公開されました。この出来事は、地球上で最も強力で目に見えないサイバー兵器のいくつかを暴露する結果になりました。これらの流出したサイバー兵器には、EternalBlue の脆弱性が含まれており、NotPetya や WannaCry など、史上最大規模の情報漏えいの基礎となりました。

このようなサイバー兵器の開発は、ゼロデイ市場として知られる業界全体の勢いを加速させました。ゼロデイ市場とは、ゼロデイエクスプロイトから利益を得ることを目的とした研究者、ブローカー、Web サイトの闇の集団のことです。業界全体の正確な金額は誰も知りませんが、公開されている価格表では、機能しているゼロクリックエクスプロイトの価格は、**Android で 250 万ドル、iOS で 200 万ドル**[7]であることが判明しています。

この状況は大きく進化し続けており、この 5 年間で、特に 2022 年 2 月のロシアのウクライナ侵攻後に途方もない変化を遂げました。そのため、ビジネスと IT のリーダーは、進化する脅威の状況を理解し、これらの攻撃から身を守るためにサイバーセキュリティ態勢を改善する必要があります。そこで、**Armis サイバー戦争の現状と傾向に関するレポート: 2022-2023**[8] が作成されました。このレポートを準備するにあたり、Armis は、米国、英国、スペイン、ポルトガル、フランス、イタリア、ドイツ、オーストリア、スイス、オーストラリア、シンガポール、日本、オランダ、デンマークの、従業員 100 人以上の企業で働く IT およびセキュリティ専門家 6,021 人を対象に、独自の調査を依頼しました。また、Armis は、受賞歴のあるアセットインテリジェンスプラットフォーム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。回答者には次のような質問をしました。

- あなたの組織は、サイバー戦争に対処する準備ができていると思いますか?
- あなたが拠点を置いている国の政府はサイバー戦争への対策ができている、とお思いなら、その自信はどれほどのものですか?
- ランサムウェア攻撃を受けた場合の身代金の支払いに関して、あなたの組織の方針はどのようなものですか?
- あなたの組織では、どのようなサイバーセキュリティ対策が実施されていますか?

これらや他の質問に対する回答をもとに、世界中、地域別、国別、状況別に、IT およびセキュリティ専門家の意識を判定し、このレポートにおいて傾向としてまとめました。では、この調査結果を詳しく見て、組織がサイバー戦争の攻撃に負けないサイバーセキュリティ態勢を整える方法を探っていきましょう。

サイバー戦争

/ˈsʌɪbəˌwɔːfɛː/

名詞:

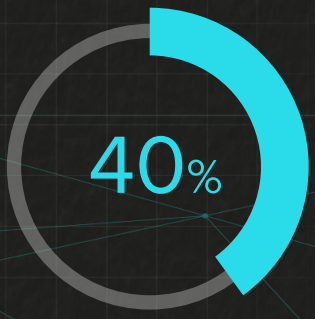
サイバー攻撃を使用して、実際の戦闘に匹敵する損害を与え、基幹的なシステムやサービスを混乱させること。意図する成果としては、スパイ活動、破壊工作、プロパガンダ、世論操作、脅迫、基幹サービスの妨害などが考えられる。

目次

組織は、サイバー戦争という嵐を切り抜ける準備ができていますか？

グローバルレポートから得られた重要な調査結果

ズームイン



C レベル (CTO、CIO、CISO) の 40% は、同じ期間に脅威アクティビティが増えたと回答しています。これらの C レベルの回答者のうち、食品・飲料 (44%)、電気通信 (44%)、自動車 (43%)、小売・卸売 (42%)、技術 (42%) などの業種の回答者は、平均よりも高い頻度で脅威アクティビティの増加を経験しています。

Armis の調査によると、グローバル企業の 3 分の 1 (33%) は、サイバー戦争の脅威を真剣に受け止めていません。これらの組織は、サイバー戦争が組織全体に及ぼす影響について無関心または無頓着であると見なされ、セキュリティギャップの余地を残しています。また、ウクライナでの戦争による地理的・政治的緊張の高まりから、サイバー攻撃の脅威がはるかに現実味を帯びてきています。Armis が調査した IT およびセキュリティ専門家の 64% 以上が、ウクライナでの戦争によってサイバー戦争の脅威が高まったことに同意しています。また、IT セキュリティの唯一の意思決定者である回答者の半数以上 (54%) 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たと答えています。このことを考えると、回答者の 45% が、サイバー戦争の活動を当局に報告する必要があったと答えているのも不思議ではありません。

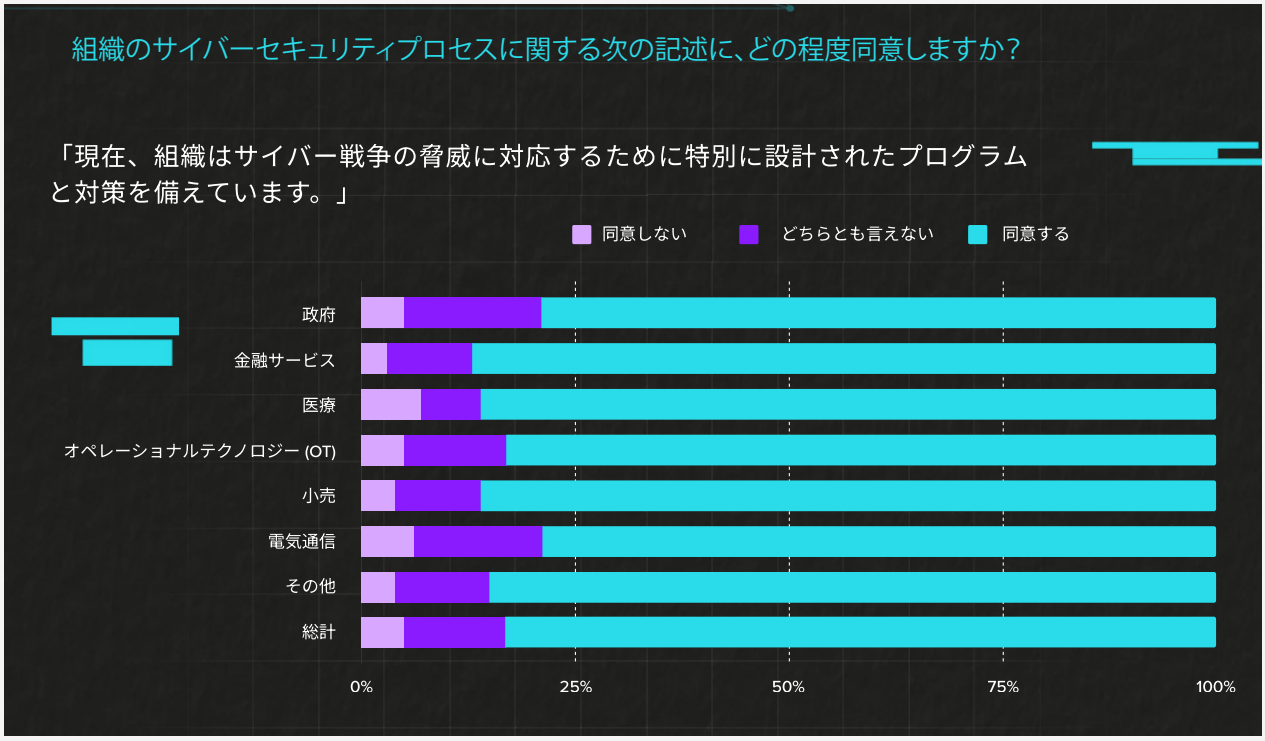
C レベルの回答者:

過去 6 か月の間にネットワーク上で脅威アクティビティを経験した場合、6 か月前と比べて増加または減少しましたか?

業種	産業部門	増加	同じ	減少	N/A	不明
政府	政府、地方自治体、公共機関	39%	44%	14%	3%	
金融サービス	金融サービスおよび保険	20%	70%	10%		
医療	医療、ヘルスケア、製薬	26%	52%	20%	2%	
オペレーショナルテクノロジー (OT)	自動車	43%	33%	24%		
	物流、ロジスティクス、輸送	30%	48%	19%	4%	
	食品・飲料	44%	44%	11%		
	製造、エンジニアリング	40%	30%	8%	22%	
	石油、ガス、鉱業、建設、農業	30%	50%	15%	5%	
	輸送	32%	36%	18%	14%	
	公益事業: エネルギー・水道	15%	62%	15%	8%	
OT 合計		37%	35%	12%	16%	
その他	慈善、非営利	29%	29%	14%	29%	
	その他 (指定してください)	33%	43%	5%	10%	10%
	技術	42%	25%	30%	2%	1%
その他の合計		42%	25%	29%	2%	1%
小売	小売・卸売サービス	42%	40%	15%	3%	
電気通信	電気通信、ケーブル、衛星	44%	38%	18%		
総計		40%	31%	22%	6%	0.5%

2022 年 6 月 1 日から 2022 年 11 月 30 日までに収集された Armis アセットインテリジェンスプラットフォームの独自データでは、前述の傾向が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。

脅威の悪化がデジタル変革プロジェクトに世界的な影響を与えていることは明らかで、世界中のイノベーションを減速させています。調査対象者の半数以上 (55%) が、こうした脅威のために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。この割合は、オーストラリア (79%)、米国 (67%)、シンガポール (63%)、英国 (57%)、デンマーク (56%) など、特定の国ではさらに高くなっています。



すべての業界がサイバー攻撃のリスクにさらされていますが、重要インフラ、ヘルスケア、政府機関は際立っており、国家を背景とする攻撃者にとって魅力的な標的となっています。ヘルスケアは、攻撃対象領域が広範囲に及び、攻撃が重要なプロセスや患者の健康と安全に影響を及ぼす可能性があるため、攻撃者にとって魅力的な分野と言えます。攻撃者は、政府機関が保存しているデータを狙っています。また、重要インフラは国家と経済の安全保障にとって重要であることから、引き続き高い順位を保っています。

サイバー戦争の脅威が増大し、データ侵害の平均コストが米国で **944 万ドル**[9]、全世界で 435 万ドルに達するという不安がある中で、業界アナリストが 2023 年の世界のセキュリティおよびリスク管理に対する支出は 11.3%増加すると**予測している**[10]のも不思議ではありません。その要因として、リモートワークやハイブリッドワークのモデル、仮想プライベートネットワーク (VPN) からゼロトラストネットワークアクセス (ZTNA) への移行、クラウドベースの配信への移行などが挙げられますが、要するに、高度なサイ

バー兵器を開発できる国が圧倒的に多くなり、攻撃対象領域が拡大し続けていることが原因となっています。結局のところ、デジタル化され、真につながった組織は、サイバー支出を増やさないわけにはいかないのでしょうか？

サイバー戦争が組織に影響を与えるリスクにもかかわらず、そうした攻撃に対するサイバー防御と回復力は依然として低いままです。ますます多くの国家を背景とする攻撃者が、重要インフラから、あらゆる形態と規模の商業団体への攻撃へと焦点を移しています。皮肉なことに、この調査では、グローバル組織のほぼ 4 分の 1 (24%) がサイバー戦争の脅威に対処する準備ができていないと感じているにもかかわらず、IT およびセキュリティ専門家の中で最もランクの低いセキュリティ要素が国家を背景とする攻撃を防いでいることがわかりました。さらに、堅牢なサイバーセキュリティプログラムに資金を費やすことをいとわない組織であっても (支出の傾向については後で詳しく説明します)、関連する技術とソフトウェアを効果的に監視するために必要なスキルを備えた、サイバーセキュリティの役割を果たす人材を見つけることは、引き続き課題となっています。2013 年から 2021 年の間に、世界中のサイバーセキュリティの求人数は **350% 増加**[11]し、100 万人から 350 万人になりました。2025 年になっても、同じ数の人材が求められていると予測されています。

最も脆弱な業界は何ですか?

重要インフラに対する脅威

ウクライナでの長期化する紛争により、2022 年に、重要インフラを標的とした悪意のあるロシアのサイバー攻撃について、国際機関が複数の警告を発しています。注目すべきなのは、Industroyer2 と InController/PipeDream は、すべての業界のオペレーショナルテクノロジー (OT) を対象としたモジュラー型の攻撃ツールであり、Supervisory Control And Data Acquisition (SCADA) システム、分散制御システム (DCS)、リモートターミナルユニット (RTU)、およびプログラマブルロジックコントローラ (PLC) の動作環境も含まれています。

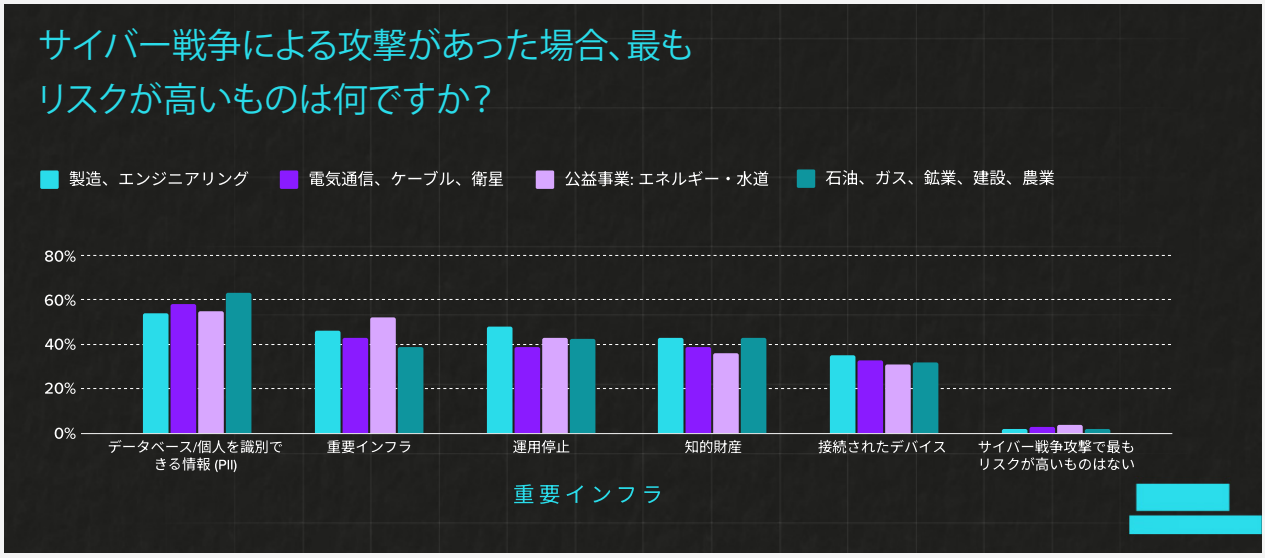
2021 年 5 月、米国東海岸で消費されるガソリン、ジェット燃料、ディーゼルのほぼ半分を制御する **Colonial Pipeline**[12] は、IT 内でランサムウェア攻撃の犠牲者となり、OT の運用が影響を受けました。Colonial Pipeline のハッキングは、米国の重要インフラに対するサイバー攻撃としては、これまでに公表されたものの中で最大規模のものです。Colonial Pipeline は、連邦捜査局 (FBI)、米国エネルギー省 (DOE)、国土安全保障省 (DHS)、サイバーセキュリティ・社会基盤安全保障庁 (CISA) と協議した結果、DarkSide ハッカーが要求した暗号通貨の身代金を支払うという苦渋の決断を下しました。

同社は、パイプラインを迅速かつ安全に復旧させるためには、お金を払ってでも復号化キーを入手することが最善の策であると考えました。それから約 1 か月後、FBI はハッカーが所有するビットコインを押収し、支払った身代金の大部分を回収することができました。

国家を背景とするサイバー戦争は、隣接する国や積極的な紛争参加国に限定されるわけではありません。攻撃者は、紛争に関連する (たとえば、武器の供給など)、または関連しない、いくつもの理由から他国を標的にする場合があります。2021 年、米国は、米国と EU の政府ネットワークに侵入するために SolarWinds のハッキングを実行したとして、ロシア対外情報庁の国家的攻撃者である Nobelium を正式に非難しました。Nobelium の攻撃は、事実上すべての業界の脅威の状況を様変わりさせました。2022 年 10 月、ロシアを支持するハッカー集団 Killnet が米国の航空業界に対して**数十回の DDoS 攻撃**[13]を仕掛け、米国のすべての重要インフラを持続的な攻撃下に置くであろうと宣言しました。

このように継続的かつエスカレートするサイバー戦争攻撃のニュースに加え、官民の組織による意識向上の取り組みは、ビジネスリーダーの間で無視できないものとなっています。Armis サイバー戦争の現状と傾向に関するレポート:2022-2023 では、重要な OT インフラを担当する世界の回答者の 74% が、サイバー戦争による脅威を受けて、取締役会がサイバーセキュリティに対する組織文化を変革しつつあることに同意していることがわかりました。

重要インフラと最も関連性の高い業界 (下表参照) を見ると、インダストリー 4.0 における IT とオペレーショナルテクノロジー (OT) の融合を回答から見て取ることができます。サイバー攻撃を受けた場合に、最もリスクが高いと思われる項目を 3 つまで選んでもらいました。各部門において、データベースと個人を特定できる情報 (PII) が最も懸念されるものとしてランクインしました。重要インフラ (物理的な機器や設備)、業務停止、知的財産がリスクのある分野の中間に位置し、重要インフラ部門で最も懸念が低かったのは接続されたデバイスでした。



これらの回答は、IT[14]、OT[15]、および産業用制御システム (ICS)[16] 環境におけるさまざまな懸念を示しています。かつては異質であったこれらのシステムが近年急速に融合していることを考えると、これは驚くことではありません。重要インフラの ICS や OT システムの多くは数十年前に構築され、大部分は現在でもネットワーク設計や役割ベースのアクセスに基づくレガシー方式で保護されています。このような環境の相互接続と自動化が進むにつれて、既存のネットワークと、それらのネットワークに接続することがまったく意図されていなかった資産が交わる場所において、攻撃リスクが拡大しています。

Armis は、重要インフラに影響を与える脆弱性や攻撃に関する認識を広めるために、この接続された資産の交わる場所を対象としてセキュリティ脆弱性調査を実施することにしました。2022 年 3 月、Armis の研究チームは、データセンター、産業施設、病院などのミッションクリティカルな資産に緊急バックアップ電源を供給する 2000 万台以上の APC スマート無停電電源装置 (UPS) に影響を及ぼす可能性のある 3 つのゼロデイ脆弱性を公開しました。TLStorm[17] と総称されるこれらの脆弱性により、攻撃者は UPS 機器や接続された資産を無効化、妨害、破壊することができます。これらの脆弱性を悪用することで、攻撃者は、たとえば UPS デバイスが煙が出て燃えるところまで電圧を改ざんするなどして、UPS デバイスを武器化することができます。これらの脆弱性は、デジタル世界と物理世界をつなぐサイバーフィジカルシステムで発生します。このように、サイバー攻撃は、現実の世界に生命を脅かす結果をもたらす可能性があり、標的となるインフラの物理的破壊につながる可能性もあるため、それを特定することはさらに重要な課題となっています。

ヘルスケア業界に対する脅威

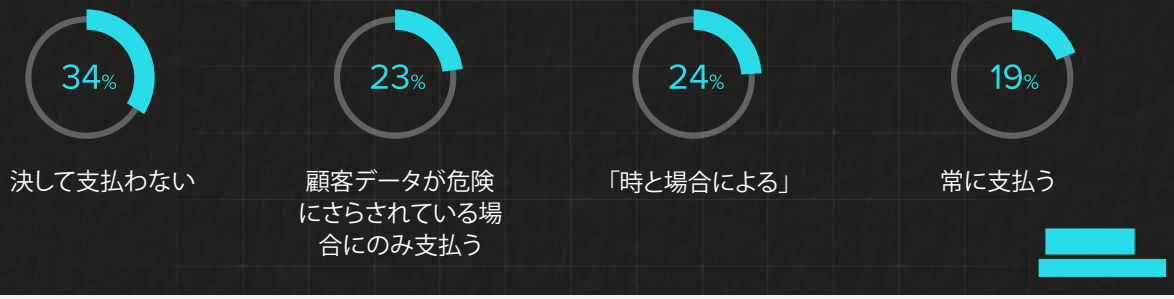
ヘルスケア部門は、どの国の国民にとっても極めて重要です。それは、社会の機能の仕組みに不可欠であり、近代国家の発展にも極めて重要な役割を担っています。患者の安全が危険にさらされた場合、生命を脅かす現実的な結果が生じるため、ヘルスケアは悪意のある攻撃者の最大の標的であり続けています。たとえば、2022 年 10 月、**CommonSpirit Health**[18] は、140 の病院と全米の 1,000 以上の介護施設を運営するシステムに大規模なランサムウェア攻撃を受けました。2022 年末の時点で、この攻撃は 21 州にわたる約 2000 万人のアメリカ人に影響を与え、その結果、医療従事者は患者のカルテがないまま医療を提供しました。これはもちろん、医療提供上、非常に危険な方法です。その結果、アイオワ州の 3 歳の子どもが鎮痛剤を大量投与され、幸運にも一命を取り留めたという事件がありました。2020 年の初め、**ドイツのデュッセルドルフの病院がより小規模なサイバー攻撃**[19]を受けて、ネットワークが停止し、患者を他の病院に搬送する必要が生じました。その結果、1 人の患者が死亡しました。

ヘルスケアへの攻撃は生命を脅かすだけでなく、すでに苦しい予算で作動し、まだ COVID-19 の大流行からの回復途上にある医療システムにとって、非常に大きな負担となります。**医療機関の CIO**[20] は、リモートワーカーが他の業界で得られるような高収入を求めていることから、重要な技術者やセキュリティ人材の維持に苦慮しています。医療機関は、引き続きサイバー戦争やサイバー犯罪の最も標的となる部門の 1 つであり、訓練されたスタッフの減少は、医療機関にとって危機的な状況となっています。(IBM は現在、ヘルスケア関連の情報漏えいの平均コストを **1010 万ドル**[21]と推定しており、全業界の 944 万ドルを上回っています。)2021 年にアイルランドの **Health Service Executive**[22] がランサムウェア Conti の攻撃を受けた際、公的資金による医療システムは紙ベースのプロセスに移行せざるを得ませんでした。このため、患者の予約の 80% がキャンセルされ、修復とシステムの交換にかかる費用は総額 6 億ドルと推定されました。

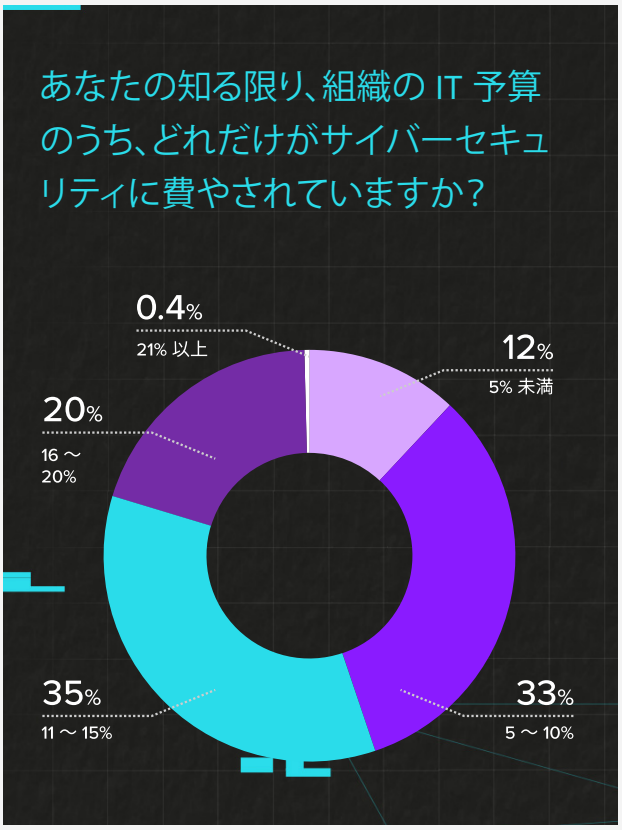
この調査によると、ヘルスケア、医療、製薬業界の IT 担当者の 72% が、サイバー戦争の脅威を受けて、取締役会が組織のサイバーセキュリティに対する文化を変革しつつあることに同意しています。この傾向は、ヘルスケア部門に対するサイバー攻撃の広がりと着実な進行に起因しています。業界の回答者の 45% は、2022 年 5 月から 10 月の間に、その 6 か月前と比較してネットワーク上で同じ量の脅威アクティビティが発生したと回答し、28% は、同じ期間で脅威アクティビティが増加したと答えています。そして、回答者は、サイバー戦争が組織全体に与える影響 (70%)、自社の重要インフラ (72%)、自社のサービス (68%) について、多少または非常に懸念していると答えています。

ズームイン

Armis が調査した世界の医療機関は、ランサムウェア攻撃時の身代金の支払いに関する方針を次のように示しています。



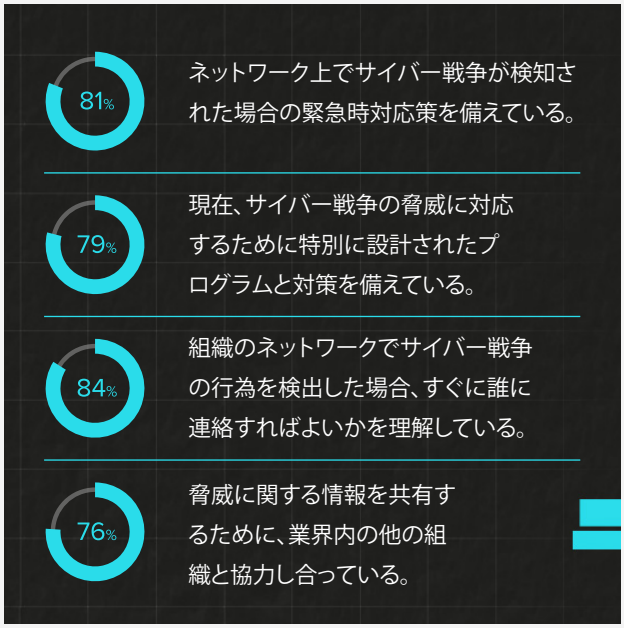
それでも、ヘルスケア組織におけるサイバーセキュリティへの支出は、世界の他の業界と比較すると低い水準です。ヘルスケア企業の約半数 (45%) は、サイバーセキュリティにかける IT 予算の割合が 10% 未満となっています。世界中のヘルスケア組織の回答者は、平均して自社の IT 予算の約 11% をサイバーセキュリティに費やしていると答えており、内訳は 11～15% (35% の組織)、16～20% (20% の組織)、20% 以上を費やしている組織はごくわずか (1% 未満) です。



ヘルスケア IT の進化と患者ケアのデジタル化が進む中で、イノベーションによって、人材不足、コストの上昇、コンプライアンスの問題など、ヘルスケア業界が直面する大きな課題に対処できる可能性があります。しかし、回答者の 55% は、サイバー戦争の脅威がこのデジタル化のプロセスを遅らせる可能性があると述べています。サイバー攻撃によってデジタル化が遅れると、デジタル化の恩恵を十分に受けられない可能性があるため、患者の生命に大きな影響を与える可能性があります。サイバーセキュリティを最優先に考えてデジタル化を完全に受け入れなければ、これらの新しいプロジェクトが悪用される可能性があります。空気圧管システム(PTS) を例にとってみましょう。これらのシステムは、**北米の 80% 以上の病院**[23]で使用され、世界中の 3,000 を超える病院に設置されており、気送管のネットワークを介して病院全体でロジスティクスと材料の輸送を自動化しています。これらのシステムは、患者ケアにおいて重要な役割を果たしており、ほぼ 100% 使用されています。Armis の研究者は、2021 年にこれらのデバイスに **PwnedPiper**[24] と呼ばれる 9 つの脆弱性を特定しました。これらがサイバー犯罪者の標的にされた場合、認証されていない攻撃者が標的の病院を完全に制御して、高度なランサムウェア攻撃を展開したり、病院の機密情報を漏洩したりする可能性があります。

政府機関に対する脅威

資産は、現代的かつグローバルで、常に断片化されたデジタル世界に共通する特徴です。そして、政府機関ほど、多くの資産 (人々、デバイス、ソフトウェア) を持つ事業体はありません。ここ数年に生じた出来事にもかかわらず、世界の公共部門の回答者は、サイバー戦争への対応に自信を持っているようです。



このような自信は、おそらく、世界的な提携関係を通して知識を共有する機会が増えたためだと思われます。**ファイブ・アイズ**[25]の構成国 (オーストラリア、カナダ、ニュージーランド、英国、米国) は現在、特に資産の保護に関して、セキュリティ態勢全体を強化するために積極的に情報資源を共有しています。さらに興味深いことに、これらの国のいずれかがサイバー戦争の紛争に巻き込まれた場合、世界の回答者の 63% がサイバー防衛連盟への協力を支持すると答えています。

この調査では、政府機関の回答者の 10 人に 9 人 (90%) が、自国がサイバー戦争から身を守ることに自信を持っていることが判明しており、相当な自信が改めて浮き彫りになっています。しかし、世界の回答者の 55% は、侵害が検出された後、政府機関がサイバー犯罪者の悪影響に対処し、最終的に修復することはできないと考えています。2022 年 4 月、ロシアのランサムウェアグループ Conti の攻撃者が**コスタリカ政府を攻撃した**[26]ときに、まったくその通りになりました。彼らの大胆な攻撃は、亜熱帯の国の税金システムを凍結させ、輸出に大損害を与え、現地の労働者への支払いを遅らせることになりました。攻撃を通じて、Conti は**盗んだデータ全体の 97%** [27]を流出させることに成功しました。2022 年 5 月までに、状況は悪化し、コスタリカ政府は非常事態宣言を出さざるを得なくなりました。

米国では、政府機関、団体、教育システムが、サイバー戦争集団の影響が徐々に浸透していることを実感しています。米国では 2020 年のパンデミックの真っ最中に、79 件のランサムウェア攻撃が政府機関に対して行われました。これらの機関は、復旧費用とダウンタイムで約 **188 億ドル**[28]の損失を被ったと推定されています。その結果、米国政府は 2021 年第 3 四半期に、**StopRansomware.gov**[29] でランサムウェアの総量を減らす積極的な作戦を開始しました。官民の連携により、米国のように、政府機関がランサムウェアの保護、検知、影響の修復をより良く開始できるようになることが期待されます。

ズームイン

政府機関は、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、43% の回答者が組織の方針として「決して支払わない」と回答しています (「決して支払わない」という方針を持つ回答者の割合は、世界平均 (26%) を大きく上回っています)。

世界ではどのようなサイバーセキュリティの傾向が生じていますか?

ランサムウェアに万能な対応はない

ランサムウェア攻撃は、単に重要なデータを盗むことが目的であると勘違いしている人が多いようです。しかし、実際には、ほとんどの組織が標的になりやすく、サイバー犯罪者は日和見主義者です。結局のところ、何十万もの個々のデータを流出させて闇市場で売るよりも、これらの企業に業務へのアクセスを回復するために数百万ドルの身代金を支払わせる方が、はるかに効率的で収益性が高いのです。

ランサムウェアを展開するのが国家を背景とする攻撃者であろうとサイバー犯罪者であろうと、ランサムウェア攻撃の構造は大体同じです。攻撃は侵入から始まり、多くの場合、侵害された Web サイト、フィッシング、標的型攻撃などの形で配信されます。侵入した攻撃者は、ネットワーク内を横断し、特権をエスカレートしてネットワーク内に潜り込みます。攻撃者は、トンネリングを使用して、コマンド&コントロール接続を確立します。そして最終的に、組織のデータを流出させ、ランサムウェアを起動して、ターゲットシステム上のデータを暗号化することになります。

DarkSide は、東ヨーロッパのサイバー犯罪者集団で、もともと GandCrab の亜種として広まったランサムウェアツール REvil を開発しました。これは先に述べた 2021 年の Colonial Pipeline 攻撃により最もよく知られるようになった Ransomware-as-a-Service (RaaS) プラットフォームの 1 つです。2019 年 4 月に初めて登場し、2021 年 10 月に REvil のサーバーが複数国の作戦でハッキングされ、オフラインに追い込まれるときまで、その活動は絶頂期を迎えていました。これまで、DarkSide は、「提携相手」にマルウェアを提供し、攻撃を行うクライアントと身代金を分配していました。DarkSide は、マルウェアそのものに加え、復号化機構 (現在でも、マルウェアファミリーの中で最も高度な復号化システムの 1 つであると考えられている)、ダークネットチャットのインフラストラクチャ、ダークネットリークサイト、マネーロンダリングサービスを提供していました。サイバー犯罪者の新種である初期アクセスブローカーは侵害されたネットワークのアクセスを販売しており、彼らの助けを借

ズームイン

誰が払い、誰が払わないのか?

従業員数が 500 人以上の企業では、調査対象の IT 専門家の 10 人に 3 人強(31%)が、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「決して支払わない」と回答したのに対し、従業員数が 100〜249 人の企業では、調査対象の IT 専門家の 5 分の 1 強 (23%) が同様に回答しています。米国では調査対象の IT 専門家の約半数 (47%) が、ランサムウェア攻撃時の身代金の支払いについて「常に支払う」と回答したのに対し、日本では 14 人に 1 人 (7%) が同様に回答しています。

りて、提携相手はターゲットネットワークへのアクセスを獲得します。そして、REvil ペイロードを起動し、影響を受けた組織と、暗号化されたデータを復元するための身代金の交渉を行います。

インターポール事務局長の Jurgen Stock 氏は、2022 年 5 月に、ランサムウェアやゼロデイ市場だけでは不十分な場合、国家が開発したサイバー兵器が今後数年のうちにダークネット上で入手可能になることを懸念していると述べています。スイスのダボスで開催された世界経済フォーラムでの **CNBC がモデレータを務める**[30]パネルディスカッションで、Stock 氏は「これは物理的な世界における大きな懸念だ。戦場で使われる武器が、明日には組織犯罪集団に使われることになる」と述べました。

今回の調査で、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を尋ねたところ、世界の IT 担当者の間で回答が分かれました。回答者の 24% が「常に支払う」、31% が「顧客データが危険にさらされている場合にのみ支払う」、26% が「決して支払わない」、19% が「時と場合による」という結果になりました。

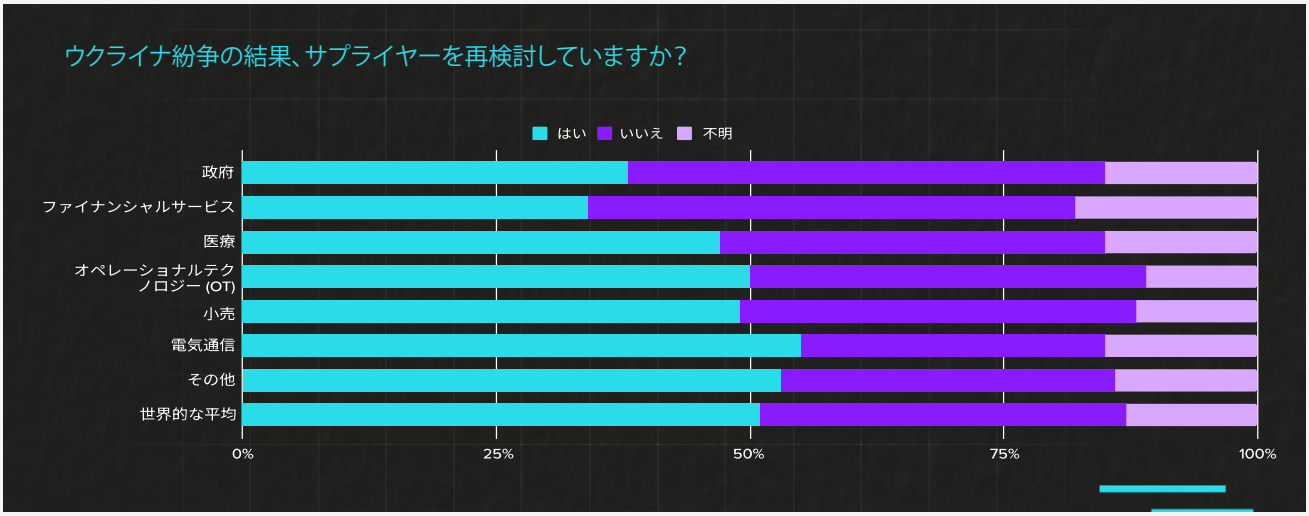
サイバーセキュリティへの支出は増加の一途をたどっている

企業が今後どのような IT 投資をしていくかについて、関連するサイバー防衛、回復力、保護サービスへの支出を増やそうとしていることを知っても驚くことはないでしょう。

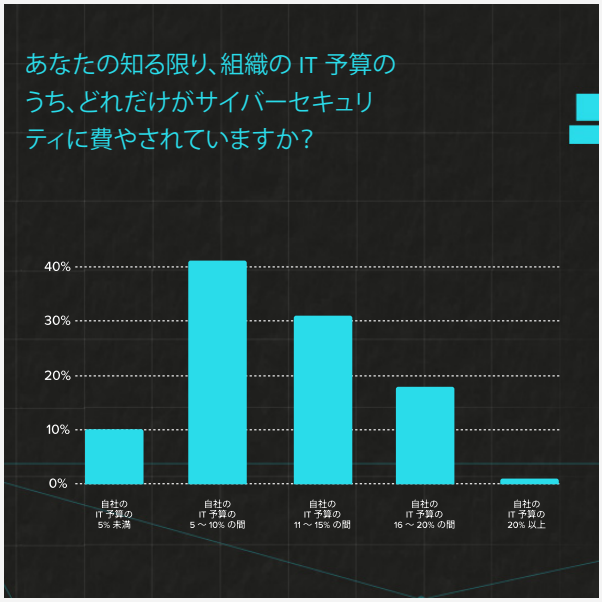
調査対象の IT 専門家の 4 分の 3 強 (76%) が、サイバー戦争の脅威を受けて、取締役会が組織のサイバーセキュリティに対する文化を変革しつつあることに同意しています。取締役会からのこのような監視はこれまでほとんど例がなく、これらの個人が組織のサイバーセキュリティ態勢を向上させる責任を共有するようになったのは重要なことです。

そして、世界の回答者の半数強 (51%) が、ウクライナ紛争の影響でサプライヤーを再検討しており、自社が新しいサイバーセキュリティプロバイダーやマネージドセキュリティサービスプロバイダー (MSSP) をすぐに (31%) または今後 6 か月間に導入する予定であると回答しています (29%)。ベンダーは、適切なソリューションを確実に提供できるように、支出の傾向や組織が最もサービスを必要としている分野を理解することが重要です。

> 「サイバーセキュリティのスキル不足は依然として大きな問題です。というのも、人員不足によってサービスやソリューションをまとめて提供する需要が高まり、パートナーの価値ある能力に大きく依存するようになるからです。MSSP や、より良い収益を得るために社内サービスを開発することでビジネスへの影響リスクを軽減しようとしているパートナーにとって、スキル不足はサイバーセキュリティ市場を活性化します。」
>
> **TIM MACKIE**
> ARMIS の ワールドワイドチャネルVP

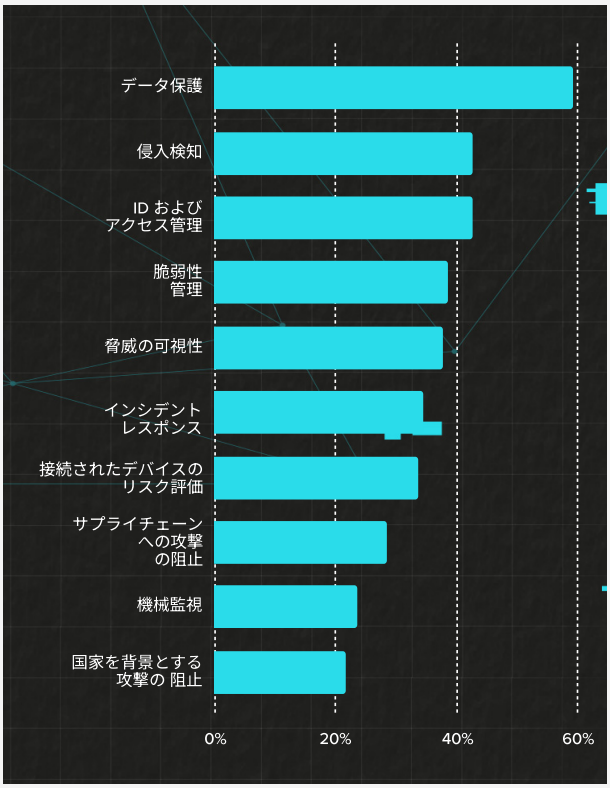


データを見ると、調査対象の IT 専門家のほぼ 5 人に 4 人 (78%) が、最近および現在進行している突発的な世界的な出来事 (パンデミック、ウクライナ紛争など) について考えた場合、自社がサイバーセキュリティに多くの予算を投じる可能性が高いと答えており、ほぼ 5 人に 2 人 (37%) がその可能性が非常に高いと見ていることがわかります。では、組織はどれだけの費用を、何に使っているのでしょうか？今回の調査では、世界的に見ると、IT 予算のうちサイバーセキュリティに割り当てられる割合は平均 11% であり、その内訳は以下のとおりです。



投資が最も多い企業では、37% が「近々投資を増やす可能性が非常に高い」、41% が「やや可能性が高い」と回答しています。しかし、投資が少ない企業は、すぐに投資を増やす可能性は低くなっています。

セキュリティ要素に優先順位を付けて選択するよう求めたところ、世界中で次のような回答が得られました。



調査対象の IT 専門家の 5 人に 2 人以上 (42%) が自社の**脆弱性管理**[31]への投資をすぐに行うと予測し、ほぼ 10 人に 3 人 (28%) が 6 か月以内に行うと回答しています。**アセット管理**[32]への投資については、37% がすぐに投資を行うと回答し、30% が 6 か月以内に投資を行うと回答しています。

企業はサイバーセキュリティソリューションに投資するだけでなく、組織全体でサイバーセキュリティを最優先する原則を採用し、サイバーセキュリティのトレーニングに投資しています。調査対象の IT 専門家の 3 分の 1 (33%) は、自社が「**ゼロトラスト**[33]」をすぐに採用すると予測しており、28% は 6 か月以内と回答しています。サイバーセキュリティのトレーニングに関しては、世界の回答者の 41% が、組織がサイバーセキュリティのトレーニングの強化にすぐに投資すると回答し、46% が今後 1 年間で投資すると回答しています。サイバーセキュリティのトレーニングを増やすために何も行動を起こさないと答えた組織は、わずか 4% でした。

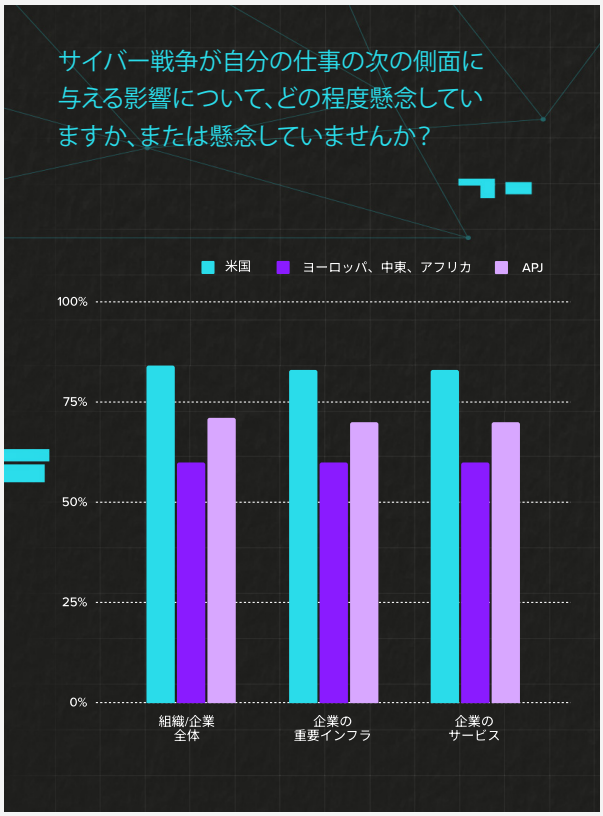
> 「セキュリティチームが効果的に活動するために、運用環境全体に対して、状況に基づく高度な可視性が必要であることは明らかです。最新技術を使用した高度な可視性は、CISO とそのチームが、ビジネスコンテキストとデータに基づいた現状を判断し、古い競合するソリューションとすべての関連費用を環境から排除するのに役立っています。」
>
> **CURTIS SIMPSON**
> ARMIS の最高情報セキュリティ責任者
> (CISO)

地域別 (米国、EMEA、APJ) では、どのような違いがありますか?

上記の世界的な傾向に加えて、米国、EMEA、APJ (オーストラリア、日本、シンガポール) の回答をグループ化したところ、地域ごとの違いも顕著になりました。いくつかの例を紹介します。

サイバー戦争の影響に関する懸念

米国、EMEA、APJ の回答者に、サイバー戦争が自分の仕事のさまざまな側面に与える影響について、どの程度懸念しているか、または懸念していないかを尋ねました。EMEA の回答者は懸念は小さく、対して APJ の回答者は懸念を抱いています。さらに懸念が最も大きい米国の IT 専門家と比較すると、懸念は著しく小さくなっています。



脅威アクティビティと経験した侵害の数

- 今回の調査によると、APJ の回答者はサイバーセキュリティ侵害の経験が少なく、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た APJ の回答者の割合は 53% でした。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。
- また、米国では、ここ数か月で最も多くの脅威アクティビティが発生しており (45%)、APJ (36%) や EMEA (25%) と比較すると、その割合は高くなっています。

組織の準備に対する自信

米国の回答者は、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ことに最も自信を持っており、米国ではほぼ 10 人に 9 人 (88%) が自信を示しています。それに対し、APJ では 78%、EMEA では 76% にとどまっています。さらに、米国の回答者の 90% が、組織の従業員は不審なサイバー活動に気づいた場合に誰に相談すればよいかを知っていると答えたのに対し、EMEA または APJ の回答者は 5 人に 4 人 (82%) でした。

すでに実施されているサイバーセキュリティの取り組み

- サイバーセキュリティ保険への投資については、米国企業が最も多く (45%)、次いで APJ (37%)、EMEA (31%) となっています。
- 従業員教育の重要性については、3 つの地域とも同じような回答でした。米国 (51%)、EMEA (49%)、APJ (45%)。
- セキュリティを重視する労働文化の創造については、米国の回答者の 44% がセキュリティを最優先する文化があると答えたのに対し、EMEA では 37%、APJ では 33% にとどまりました。
- サイバーリスクフレームワークを導入しているのは、米国が最も多い 43% で、APJ では 34%、EMEA では 31% となっています。

機密データの保護とスマートワークの実現

回答者は、一連の記述に同意するか否かを尋ねられました。

- 「私の組織は機密データを保有しており、従うべき規制があります。そして、セキュリティイベントによる悪影響を最小限に抑えたいと考えています。」
  - » 同意した回答者の割合：91% (米国)、84% (APJ)、83% (EMEA)。
- 「スマートワークの導入により、IT セキュリティの問題は、従業員にとってより重要なものとなっています。」
  - » 同意した回答者の割合：91% (米国)、85% (APJ)、81% (EMEA)。

国別の分析

上記のような地域差をより深く理解したい方のために、Armis チームは本レポートの一環として、調査対象国および地域に最も関連する国別の分析を独自に作成しました。

これらの国別報告書 (英語版および翻訳版) は、**https://www.armis.com/cyberwarfare** でご覧になることができます。

1. **米国**
2. **英国**
3. **フランス**
4. **DACH** (オーストリア、スイス、ドイツ)
5. **イベリア**
6. **イタリア**
7. **デンマーク**
8. **オランダ**
9. **APJ** (オーストラリア、日本、シンガポール)

まとめ

これらの調査結果が重要なのはなぜですか。そして、組織を守るために何ができますか?

世界中の IT およびセキュリティのリーダーは、サイバー戦争の脅威を真剣に受け止めていないこと、サイバー戦争に対処する準備が十分でないと感じていること、そして彼らの目には、国家を背景とする攻撃を防ぐというセキュリティ要素が最下位に映っていることを認めています。さらに、ウクライナでの戦争の結果、サイバー戦争の脅威が増加していることを理解しています。それは、2022 年 5 月から 2022 年 10 月にかけて、その 6 か月前と比較して、自社のネットワーク上で発生した脅威アクティビティが増加していることからも明らかです。彼らはより多くの活動を目にし、それを真剣に受け止めていないだけでなく、サイバー戦争の脅威がイノベーションに影響を与えることを許し、その結果、デジタル変革プロジェクトを停滞させたり、停止させたりしていることを認めています。このような脅威から逃れることはできないことは明らかです。これらの脅威から身を守るためには、正面から取り組む必要があるのです。

レポートの前半で、すでにサイバーセキュリティへの投資が最も多い回答者は、37% が近々投資を増やす可能性が非常に高く、41% がやや高いことを示しています。調査対象の IT およびセキュリティ専門家の 5 人に 2 人以上 (42%) が自社の**脆弱性管理**[34]への投資をすぐに行うと予測し、ほぼ 10 人に 3 人 (28%) が 6 か月以内に行うと回答しています。**アセット管理**[35]への投資については、37% がすぐに投資を行うと回答し、30% が 6 か月以内に投資を行うと回答しています。

ネットワーク攻撃が国家を背景とする攻撃者によるものであれ、サイバー犯罪者によるものであれ、組織の業務と評判に与える影響は同じです。さらに、リモートデスクトッププロトコル、BYOD (持ち込みPC) ネットワーク、仮想プライベートネットワークの脆弱性、プロトコルの設定ミスなどが、攻撃者の最も一般的な入口となりつつあります。こうした状況はパンデミックによって悪化しており、2021 年にランサムウェア攻撃は、世界的に**倍増**[36]しました。

インシデントレスポンス (IR) 計画に加え、適切なツールを導入することは、最初のステップに過ぎません。この計画を定期的にテストすることで、サイバーセキュリティの弱点を事前に特定し、防御を強化することができ、企業や消費者の重要なデータを保護するのに役立ちます。もちろん、情報漏えいのコストを何百万ドルも削減できることは言うまでもありません。

Armis は、すべての組織に以下の対策を推奨しています。

- 導入するツールや手法にかかわらず、多くの組織では、インシデントレスポンスの実行で攻撃の影響を軽減する支援が必要となります。多くの場合、従業員の中にインシデントレスポンスの専門家チームを配置することは、コストを削減し、インシデントレスポンスのスピードを向上させるのに良い方法です。
- 攻撃を検知したら、その影響を最小限に抑えることが重要です。ほとんどの組織では、戦略として依然として孤立化または分離が支配的です。分離手法にはさまざまなものがあり、ほとんどのエンドポイント検知および対応ツールは、デバイス上での分離機能を備えています。これにより、インシデントレスポンス担当者は、個々のマシンをネットワークの他の部分から分離することができます。

- さらに、優れたバックアップ戦略とプロセスは、国家を背景とする攻撃とサイバー犯罪者の両方に対する主要な防御線でもあります。組織は、選択したソリューションが攻撃に対して耐性があることを確認するとともに、継続的な監視と整合性チェックを含める必要があります。
- また、サイバーレジリエンスのある組織は、従業員のためのセキュリティ意識向上トレーニングに投資します。悪意のあるメールトラフィックを特定する方法を従業員に定期的に教育し、使いやすいレポート方法を提供します。

組織は、国家を背景とする攻撃者やサイバー犯罪者がその取り組みを成功させるであろうという原則のもとに活動する必要があります。結局のところ、悪意のある攻撃者は、組織のネットワークにアクセスするために、すべての試みのうち 1 回だけ成功すればよいのです。一方、セキュリティと IT のチームは、これらの攻撃を防ぐために、防御を 100% 成功させる必要があります。

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、情報テクノロジー (IT)、モノのインターネット (IoT)、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。

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.

レポートの人口統計

本レポートを作成するにあたり、Armis は Censuswide に調査を依頼し、米国、英国、スペイン、ポルトガル、フランス、イタリア、ドイツ、オーストリア、スイス、オーストラリア、シンガポール、日本、オランダ、デンマークの従業員 100 人以上の企業で働く IT およびセキュリティ専門家 6021 名を対象に調査を実施しました。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。

国別の回答者	
オーストラリア	511
オーストリア	100
デンマーク	50
フランス	501
ドイツ	501
イタリア	500
日本	501
オランダ	52
ポルトガル	251
シンガポール	501
スペイン	500
スイス	50
英国	1003
米国	1000

役職/役割別の回答者	
最高情報責任者 (CIO)	432
最高情報セキュリティ責任者 (CISO)	241
最高技術責任者 (CTO)	530
コンピュータサポートスペシャリスト	229
データベース管理者	457
情報セキュリティアナリスト	392
情報テクノロジー (IT) プロジェクトマネージャー	1831
ネットワーク管理者	394
ネットワークアーキテクト	260
その他	346
システムアナリスト	493
Web 開発者	416

業種別の回答者	
政府、地方自治体、公共機関	369
金融サービスおよび保険	120
ヘルスケア、医療、製薬	255
OT (自動車、流通、ロジスティクス・輸送、食品・飲料、製造、石油、ガス、建設、鉱業、農業、輸送)	1415
テクノロジー他	3133
小売・卸売	295
電気通信	434

文末脚注

1. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we
2. https://www.csoonline.com/article/3654833/u-s-charges-russian-government-agents-for-cyber-attacks-on-critical-infrastructure.html
3. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
4. https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
5. https://www.nsa.gov/
6. https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html
7. https://arstechnica.com/information-technology/2019/09/for-the-first-time-ever-android-0days-cost-more-than-ios-exploits/
8. https://www.armis.com/cyberwarfare/
9. https://www.ibm.com/reports/data-breach
10. https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i
11. https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025
12. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
13. https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet
14. https://www.armis.com/cybersecurity-asset-management/
15. https://www.armis.com/ot-device-security/
16. https://www.armis.com/ics-risk-assessment/
17. https://www.armis.com/research/tlstorm/
18. https://www.healthcaredive.com/news/commonspirit-health-ransomware-cyberattack/634011/
19. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
20. https://www.beckershospitalreview.com/healthcare-information-technology/a-war-for-talent-cios-detail-the-challenges-of-retaining-health-it-professionals.html
21. https://www.ibm.com/reports/data-breach
22. https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
23. https://www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/products-and-services/transport/translogic-pts/pts-513-swisslog-healthcare-delivers-unmatched-innovation.
24. https://www.armis.com/research/pwnedpiper/
25. https://www.zdnet.com/article/five-eyes-advisory-warns-more-malicious-russian-cyber-activity-incoming/
26. https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/
27. https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
28. https://www.americancityandcounty.com/2021/03/22/report-ransomware-attacks-cost-local-and-state-governments-over-18-billion-in-2020/
29. http://stopransomware.gov

30. https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html
31. https://www.armis.com/avm/
32. https://www.armis.com/armis-asset-management/
33. https://www.armis.com/zero-trust/
34. https://www.armis.com/avm/
35. https://www.armis.com/armis-asset-management/
36. https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021#:~:text=Ransomware%20attacks%20rose%20by%2092.7,nation%2Dstate%20cyberattacks%20and%20more.

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®