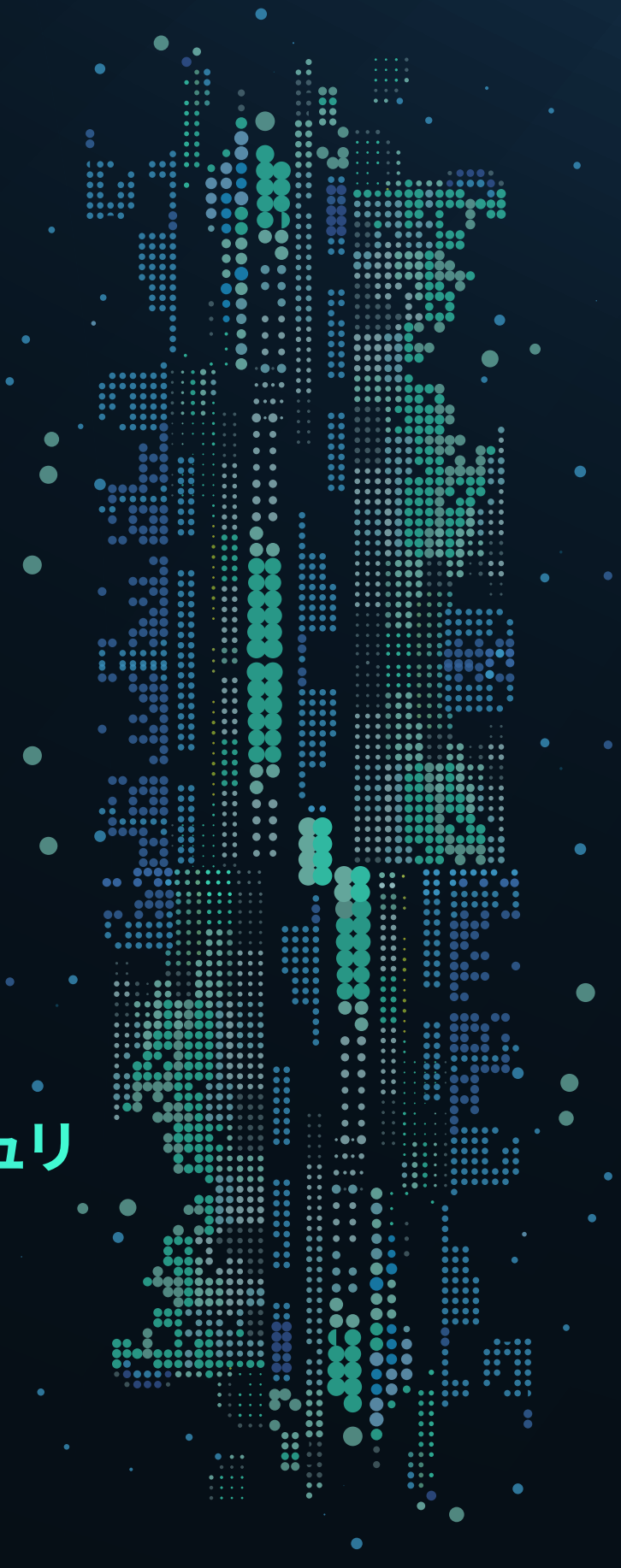
ANOMALI



2022

Anomali サイバーセキュリティインサイトレポート

企業におけるサイバーレジリエンスの状況

目次

はじめに

Anomali サイバーセキュリティインサイトレポート 2022 へようこそ。最初の調査では、現在と今後の高度なサイバー脅威に対する保護や対応に必要なレジリエンスのあるサイバーセキュリティ体制を確立したり維持したりする上で、企業が直面する問題を特定して調査します。

Anomali 脅威調査チームでは、レポートの基礎データを収集して構築するために、Harris Poll に委託して、5,000 人以上の従業員を抱える 11ヵ国の企業のセキュリティ意思決定者 800 人を対象に調査を実施しました。COVID-19 はビジネスやサイバーセキュリティに非常に大きな影響を与えました。したがって、意思決定者への質問を通じて、2019 年までのサイバーセキュリティ体制や問題を把握することで、世界的なパンデミックによるビジネスへの影響をより深く理解できるようになっています。さらに、Anomali 脅威調査チームの脅威インテリジェンスアナリストによる脅威の傾向分析で調査結果が補強されているので、これを読むことで、実用的な情報を活用して、侵害や攻撃者を検出したり対応したりする能力を向上させることができるようになります。

中でも重要なポイントは、サイバーセキュリティにどれほど投資しても、**攻撃者に対する防御、検出、対応に必要なレベルのサイバーレジリエンスを実現する上で多くの組織が問題に直面してしまうということです。**世界中で起こっている侵害やサイバー攻撃がこの数年間で増加していることを考えると、これを読んでいる方にとってこのような見解は驚きの内容ではないことでしょう。

サイバーレジリエンスの定義

脅威や攻撃者から組織を事前および事後対応的に保護したり、攻撃時における状況の変化にも適応したり、サイバー攻撃後に回復したりできる能力。

エグゼクティブサマリー

Anomali の調査によると、サイバーレジリエンスの実現が困難な理由が数多く存在することが明らかになりました。最も大きな要因として、現在および将来の攻撃やセキュリティ侵害に対する検知、対応、復旧に必要なパフォーマンスや能力を組織が十分身に付けていないことがあります。

今回の調査では、サイバー攻撃が増加していることが判明しました（パンデミック発生前の 2019 年から **15 %** 増加）。したがって、約 4 分の 3（**74 %**）の組織がサイバーセキュリティ予算を増額し、サイバーセキュリティ戦略の見直しを進めている（**78 %**）のも当然と言えます。

予算を増やしたにもかかわらず、大部分（**87 %**）の組織が過去 3 年間にサイバー攻撃による被害にあっており、損害、ビジネスの中断、侵害などの実害が生じています。セキュリティ対策の強化にもかかわらず、約 3 分の 2（**67 %**）が、パンデミック発生後ますます巧妙になるサイバー攻撃によって影響が生じていると回答しています。2020 年だけでも、平均で 7 件に 1 件（**14 %**）のサイバー攻撃が成功し、侵害、損害、ビジネスの中断が生じています。これまでにない規模で進行するデジタル変革プロジェクトとともに、組織の攻撃対象領域が拡大しており、セキュリティ意思決定者は今後もサイバー攻撃の被害が増加すると予想しています。このように脅威による危険性が高まっている状況にもかかわらず、攻撃を受けた際に利用できるインシデント対応のベストプラクティスを明確に定めている組織は 44 % にすぎません。

サイバーインシデントはほとんどすべての組織に経済的な損害を与えています。標的型のサイバー攻撃、マルウェアキャンペーン、フィッシング、インサイダー脅威、関連するデータ侵害などにより、1 つの組織だけで数十万ドルにもおよぶ損害が生じています。全世界の 3 割近く（**28 %**）の企業が 2020 年に 50 万ドル以上の損害を受けたと報告していますが、この数字は 2019 年と比較して 2 倍近く（**193 %**）となっています。10 万ドル以上の損害を受けたと報告した企業は半数近く（**47 %**）にのぼります。 被害金額の大きさに加えて、攻撃件数自体も急増しています。

デジタル変革の急速な進展や攻撃の急増といった要因に加え、企業のセキュリティ意思決定者の多くが、サイバー攻撃やデータ侵害に対する検知、対応、復旧を行う防御壁としての統合サイバーセキュリティソリューションが導入されていないと回答しています。

多くの組織は、直面している困難な状況への対抗策として、XDR（Extended Detection and Response）や高度な脅威インテリジェンスなどを利用した画期的な最新テクノロジーをすでに使用しているか、またはそのようなテクノロジーへの投資を予定していると答えています。

この調査では、サポートがしっかりしており（**48 %**）、使いやすく（**46 %**）、既存のフレームワークやアーキテクチャとの統合に優れた（**44 %**）サイバーセキュリティソリューションが求められていることも明らかになりました。4 割以上の意思決定者が、このような特性がサイバーセキュリティソリューションには不可欠であると考えています。

87 %

の企業のセキュリティ意思決定者が、過去 3 年間にサイバー攻撃を受けたことがあり、その結果、ビジネスにおいて損害、混乱、侵害を被ったと回答しています。

調査結果 1

多くの組織では、サイバー脅威に対する検知、対応、復旧への備えが十分ではない

セキュリティ意思決定者の 42 %は、レジリエンスが侵害や攻撃から組織を守るのに必要なレベルに達していないと考えています。なお、サイバーレジリエンスを実現していると自信を持って回答した意思決定者は 10 人中 6 人以下（58 %）でしたが、この結果は、87 % の組織が過去 3 年間に侵害を受けたことがあるという事実を反映していません。

調査結果 2

セキュリティ意思決定者の中で、自社のサイバーセキュリティチームは傾向、重大度、潜在的な影響に基づき、脅威に対して迅速に優先順位を付けることができると自信を持って回答したのは半分以下

3 分の 1 が、新たな攻撃に対処するためのセキュリティ制御の更新にチームが苦労していることを認めています（31 %）。企業セキュリティ意思決定者の中で、自社のサイバーセキュリティチームは傾向、重大度、潜在的な影響に基づき、脅威に対して迅速に優先順位を付けることができると自信を持って回答したのは半分以下（49 %）でした。サイバープロテクションテクノロジーが進化し、世界的に特定された新たな脅威を検出できると自信を持って回答した意思決定者はさらに減少しています（46 %）。3 分の 1（32 %）が、急速に変化するサイバーセキュリティ脅威の状況にチームがなかなかついていけないことを認めています。小規模な組織では、リスクがさらに高まります。従業員数が 10,000 人未満の組織では、サイバー攻撃に対応するときに参照できる一連のベストプラクティスがあまり用意されていない傾向があります（40 %）。

図 1.0.
組織のサイバーレジリエンス（「とてもそう思う」と答えた割合）

49 %
非常にそう思う

自分のチームは、トレンド、重大度、組織に与える影響をもとに、脅威の優先順位付けを迅速に行うことができる

46 %
非常にそう思う

サイバーセキュリティテクノロジーを進化させ、世界的に特定された新しい脅威を検出することができる

32 %
非常にそう思う

急速に変化するサイバーセキュリティ脅威の状況にチームがなかなかついていけない

調査結果 3

組織は、サイバー攻撃の検知と対応についての目標を達成できずにいる

滞留時間とは、攻撃者がネットワークへのアクセスに成功した後、検知され、その試みが阻止されるまでの期間を指します。滞留時間の長さは、攻撃者が引き起こす被害の大きさと直接的に比例します。ネットワーク内に長時間滞留するほど、攻撃者はより多くの情報を獲得し、より多くのデータや IP を盗み、より多くのシステムに侵入してランサムウェアなどの脅威への感染を引き起こします。攻撃者は、平均 140 日もの間検知を回避できると推定されています。ただし、この日数は、脅威が初めて検知され、公開される場合です。

滞留時間と同じような危険性をはらむ要素として、新たに公開された脅威が自組織の環境内にも存在するかを判断するまでにかかる時間があります。今回の調査では、すでに公開されている攻撃の検知と対応にかかった時間を尋ねました。結果は憂慮すべきものでした。おおむねすべてのセキュリティ意思決定者が、全体としての検知と対応の目標を達成できておらず、特定の種類の脅威において対応が遅れていると答えたのです。

図 1.1.
検知と対応の平均時間と目標
（日）

	データ侵害		ネットワーク侵害		サイバー攻撃	
	平均時間	平均の目標	平均時間	平均の目標	平均時間	平均の目標
検知	3.1	2.1	2.8	2.1	2.7	2.5
対応	2.5	2.2	2.5	2.1	2.4	2.1

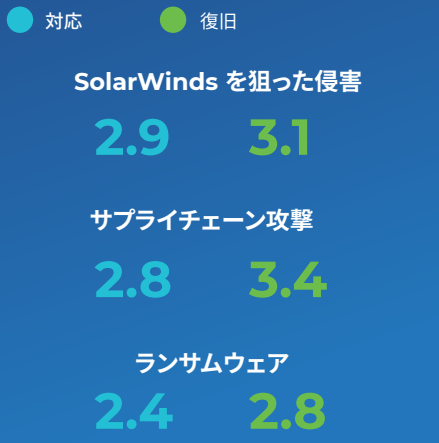
セキュリティチームが効果的に運用を行うためには、インシデント解決時の MTTR と MTTD の両方の指標に注意を払う必要があります。滞留時間を短くすると、損害やビジネスの中断といった全体的なリスクを低減することができるので、組織においては、これらの指標で示される時間の短縮に注力することが重要です。攻撃とその影響を理解することが、滞留時間（MTTD と MTTR）短縮の第一歩となります。効果的に検知と対応のプロセスを実施できるよう、組織に存在するサイロを解消し、部門間でのコラボレーションを推進する必要もあります。

MTTD 平均検知時間（MTTD）は、脅威の可能性がある事象を検知するのにかかる時間を表します。

MTTR 平均対応時間（MTTR）は、脅威の発見から、その脅威の制御、修復、除去を完了するまでにかかる時間を表します。

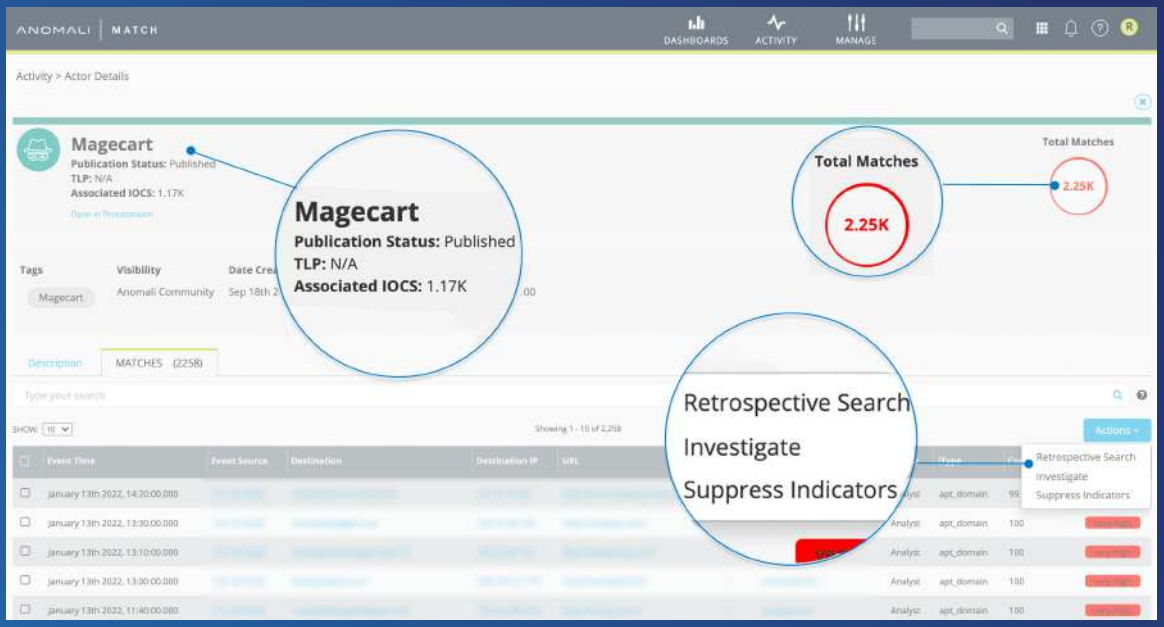
図 1.2.
既知のサイバー攻撃を検知するまでの平均日数

図 1.3.
サイバー攻撃への対応および復旧の平均日数



脅威の検知の仕組み

Magecart：悪意を持って e コマース Web サイトを狙い、支払いカード情報を盗み出して、犯罪者が集まる掲示板で販売するサイバー犯罪者グループ。



脅威にはさまざまな種類があります。脅威の検知は、脅威の緩和と対応を行うプロセス全体から見ると一部分にすぎません。脅威についてデータに基づく意思決定を行うためには、多くの情報を収集することが重要になります。

現在、サイバーセキュリティの専門家は、ビッグデータ（複数のソースから集められた膨大な情報）を分析することで、脅威による被害が生じる前に脅威を特定する取り組みを始めています。適切なテクノロジーを利用してビッグデータを分析することにより、人間の行動に関するインサイトを獲得し、将来のトレンドを予測して、セキュリティ侵害を防止することができます。

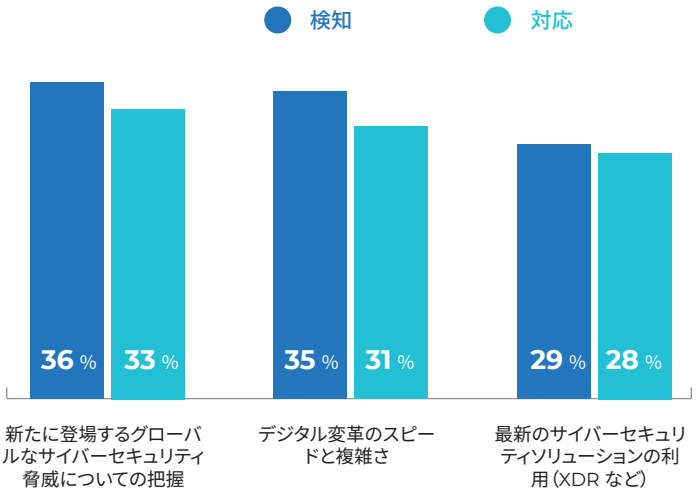
上記の例は、セキュリティ侵害インジケータ（IOC）、観察された行動、攻撃者についての知識、脅威モデルなどの膨大なビッグデータをまとめ上げるツールを使用することで、Magecart などの脅威が環境内に存在するかどうか、そしてどの程度滞留しているかをアナリストがただちに判断できる様子を示しています。このようなインテリジェンスによりただちに状況を把握できると、確実かつ迅速な対応につながります。サイバーレジリエンスを実現し、先手を打って脅威に対応できるセキュリティ体制を構築するには、このようなツールが欠かせません。

調査結果 4

新たに登場するグローバルなサイバーセキュリティ脅威について把握すること、そしてデジタル変革のスピードと複雑さが主な課題である

組織は、検知において多くの課題に直面しています。最も大きな課題は、新たに登場するグローバルなサイバーセキュリティ脅威についての把握（36 %）、デジタル変革のスピードと複雑さ（35 %）、そして XDR などの最新のサイバーセキュリティ関連技術の導入（29 %）となっています。脅威に対する対応と復旧においても、ほぼ同様の課題が挙げられています。

図 1.4.
サイバー攻撃、ネットワーク侵害、データ侵害に関する問題



調査結果 5

組織内リソース間で脅威インテリジェンスを共有できる仕組みが存在しないことが、緩和策の妨げとなっている

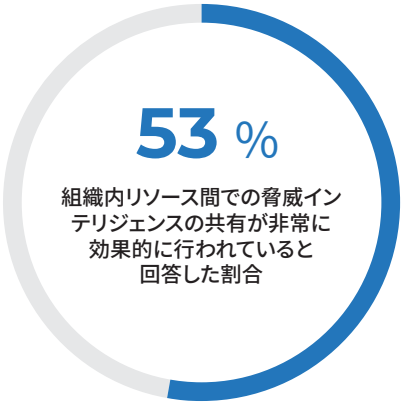
企業のセキュリティ意思決定者は、新たに登場するグローバルなサイバーセキュリティ脅威について把握すること、そしてデジタル変革のスピードと複雑さを課題として挙げています。しかし何よりも、統合ソリューションが導入されておらず、組織の各部門間で脅威インテリジェンスを共有できる仕組みが存在していないことが、サイバー攻撃に対する検知、対応、復旧を最も妨げている要因であると考えられます。組織内リソース間での脅威インテリジェンス情報の共有が非常に効果的に行われていると回答した意思決定者は、半数をやや上回る割合（53 %）にとどまっています。

サイバーレジリエンスを実現する上での主な問題

脅威インテリジェンスは複雑で、変数が非常に多く、表現方法もまちまちです。情報の共有を推進するため、MITRE、NIST、STIXX などの規格が策定され、プロセス改善に活用されています。

インテリジェンスの共有方法を理解するためには、共有しようとしているインテリジェンスがどのようなものであるかを把握する必要があります。脅威インテリジェンスを IOC と脅威アクターという 2 つのカテゴリに分けると理解しやすくなります。セキュリティおよびリスク担当者は、これらの違いを把握することで、インテリジェンス活用方法の理解を深めることができます。

図 1.5.
社内リソース間での脅威インテリジェンスの共有における有効性



IOC

- 適切にデータを取り込み、ラベル付けするプロセスが確立されていれば、OSINT（オープンソースインテリジェンス）フィードは簡単に活用できます。
- 脅威インテリジェンスプラットフォーム（TIP）が、無料のものや商用のものを含め、インテリジェンスソースから脅威インテリジェンスフィードを自動で集約してくれるため、面倒な作業は不要です。
- AlienVault（OTX）、Hybrid Analysis、MalwareBazaar、PolySwarm、VirusTotal、VirusBay、VirSCAN、URLhaus、URLScan などの IOC データベースおよびリポジトリは、コンテキストを収集し、データに基づく意思決定を行うための優れたツールです。
- AnyRun、Hatching、Hybrid Analysis、Inquest、Joe、Valkyrie Comodo などのサンドボックスは、全体的なトレンドや TTP を把握して、一般的な戦術を用いるマルウェアのシグネチャを作成するのに役立ちます。
- Yara、SIGMA、Snort など向けの OSINT 検知言語リポジトリを利用すると、一般的に見られる悪意のある行動を検知できます。

脅威攻撃者

- ThaiCERT、MITRE Groups、Malpedia、Maltego などの OSINT ソースは、優れた脅威データを提供します。
- TIP には、脅威アクターおよび関連する IOC についての豊富な情報をリアルタイムで提供することにより、活発に活動するさまざまなグループについての最新情報を常に把握できる機能が求められます。
- 各マルウェアファミリーについて、さまざまなグループにより実行されているもの、「サービスとして」販売されているもの、コモディティ型のマルウェアを改変したもの、正規のツールを利用したもの、あるいはカスタムのマルウェアを使用したものといった情報を把握することで、先手を打ってこれらの脅威への緩和策を打つことができます。

インテリジェンスタイプを分類することで、攻撃者や侵害の検出や対応がしやすくなります。組織ではイノベーションに目を向け、セキュリティインフラストラクチャで脅威インテリジェンスを自動化および運用し、その価値をさらに最適化することを目指しています。業界のトップアナリストが公表した最近のレポートによると、脅威管理プラットフォームなど、脅威インテリジェンス市場でのソリューション需要は、今後 3 年間で年間 16 % も増加すると言われています。

調査結果 6

サイバーインシデントが蔓延しており、パンデミック発生後に増加している

企業のセキュリティ意思決定者のほとんどは、パンデミックの発生以降、組織に対して試みられるサイバー攻撃の数が増加し（83 %）、フィッシング攻撃の試みも増えている（86 %）と回答しています。特に、パンデミックに便乗したテーマのフィッシングメールの数が増加しています（87 %）。5,000 名以上の従業員を擁する企業では、2020 年に平均 30 件のサイバー攻撃が報告されており、前年の 26 件から増加しています。これらのサイバー攻撃の 7 件に 1 件（14 %）が成功し、損害、ビジネスの中断、またはネットワーク、インフラストラクチャ、デバイスの侵害が生じています。

図 2.1.
パンデミック以降のさまざまなサイバー攻撃の増加

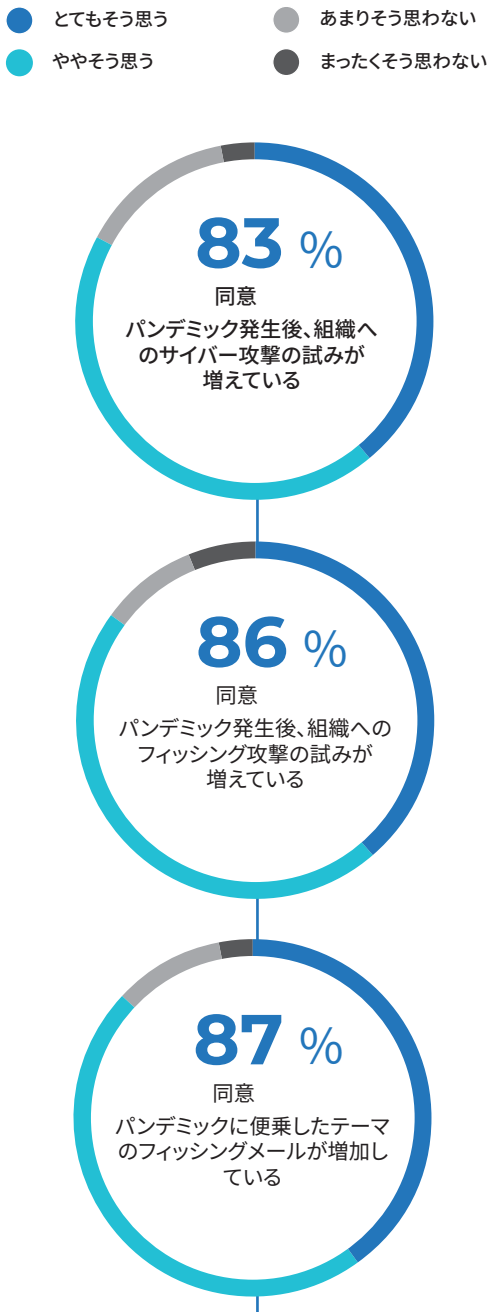


図 2.2.
組織に対するサイバー攻撃の平均数

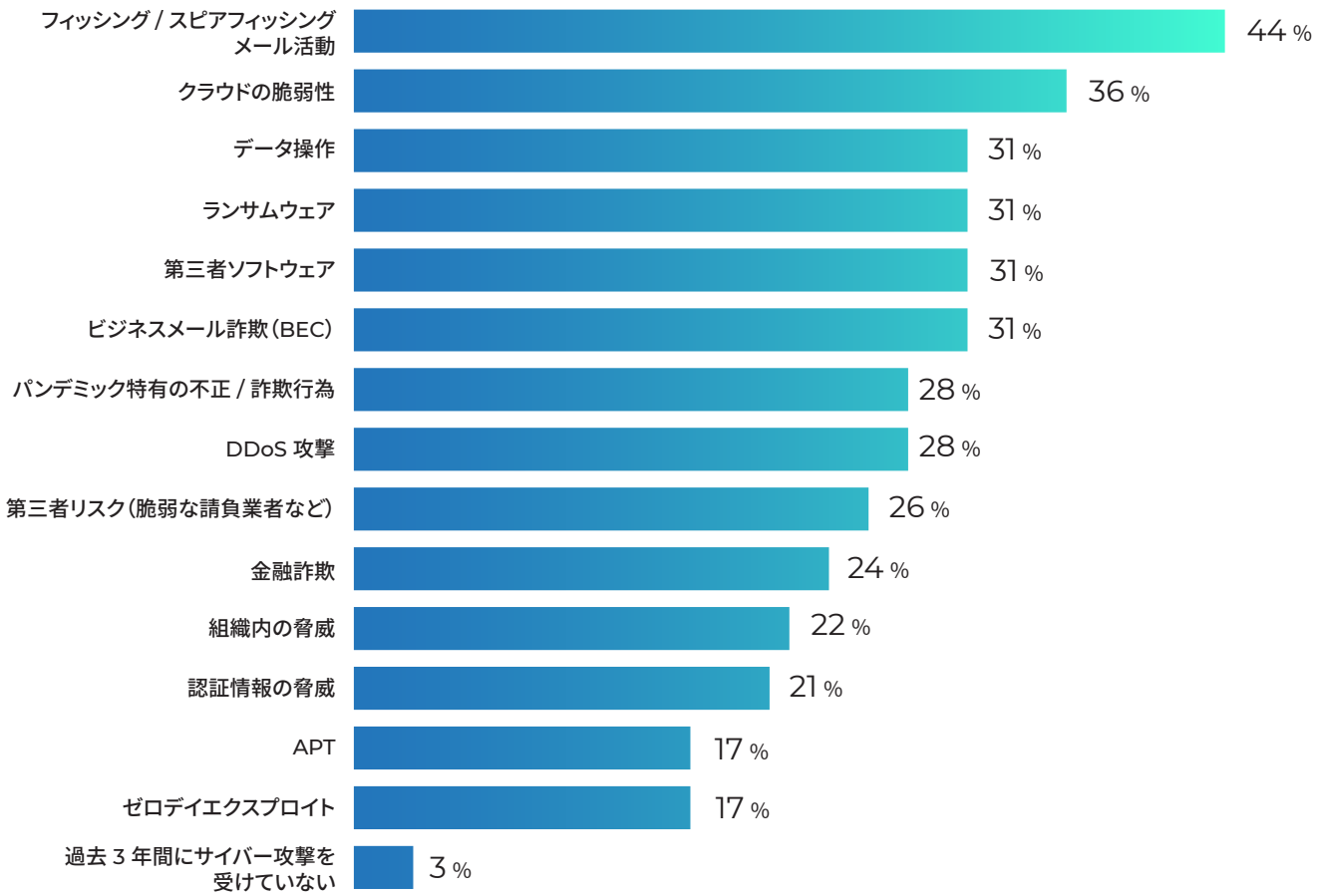
2019 年と 2020 年のいずれにおいても、従業員数 10,000 人以上の組織は、従業員数 5,000～9,999 人の組織に比べ、多くのサイバー攻撃の試みを経験しました（2019 年が 29.1 対 23.3、2020 年が 32.4 対 27.8）。

調査結果 7

最も多く発生する脅威はフィッシングメールによる攻撃

組織の 44 % が過去 3 年間にフィッシング攻撃を受けています。フィッシング攻撃は、最も一般的な種類の攻撃です。コモディティ型ツールが手に入ること、そして標的となる企業が増え続けていることにより、あらゆる熟練度の脅威アクターがフィッシングを利用するようになっています。コモディティ型のフィッシングキットを使用すると、熟練度の低い脅威アクターでも、コモディティ型のマルウェアを送り込むキャンペーンを実施し、被害をもたらすことができます。悪意のあるドキュメント（maldoc）自体も **EtterSilent** などのツールによりコモディティ化されています。脅威アクターやグループは、標的のメールアカウントを侵害することで、さらに悪意のある活動の範囲を広げます。フィッシング攻撃では、多くの場合、正当な活動に見せかけるために、正規のドキュメントが使用されます。Anomali の調査によると、**Gamaredon**（Primitive Bear）や **Mustang Panda** によるキャンペーンで正規のドキュメントが使用されたことが確認されており、前者では公開前の非公開ドキュメントが悪用された可能性があります。

図 2.3.
過去 3 年間に経験したサイバー脅威



調査結果 8

サイバーセキュリティの最大の脅威はサイバー犯罪組織（44 %）で、その次が個人のハッカー（21 %）とされている

公開後に企業がこれらのエンティティによる攻撃を検知するのに平均で3〜4 日かかる

企業のセキュリティ意思決定者の 44 % が、サイバー犯罪者グループが組織にとって最大の脅威であると回答しています。今日最も大きな被害をもたらしている攻撃やセキュリティ侵害はサイバー犯罪者グループによるものであることを考えると、この回答は当然と言えます。企業のセキュリティ意思決定者の 15 % が、組織のサイバーセキュリティに最大の脅威をもたらすのは国家が関与するアクターであると答えています。脅威に関与する国家として最も挙げられたのはロシア（39 %）で、次に中国（33 %）が多くなっています。イラン（10 %）や北朝鮮（8 %）が関与するアクターが脅威だと答えた割合は比較的少なくなっています。従業員 10,000 名未満の組織のセキュリティ意思決定者は、従業員 10,000 名以上の大きな組織と比べて、これらのアクターの目的をあまり把握できていない傾向があります。

図 2.4.
組織にとっての最大の脅威

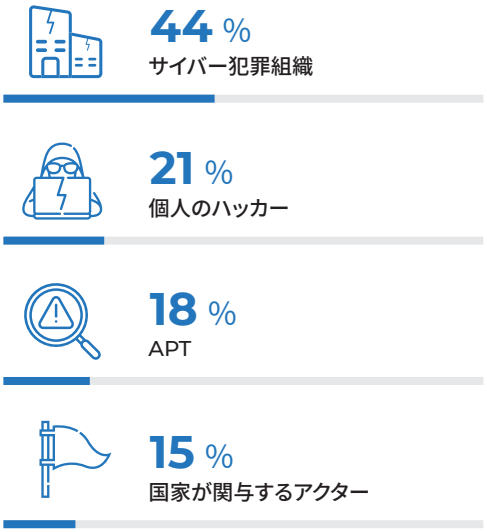


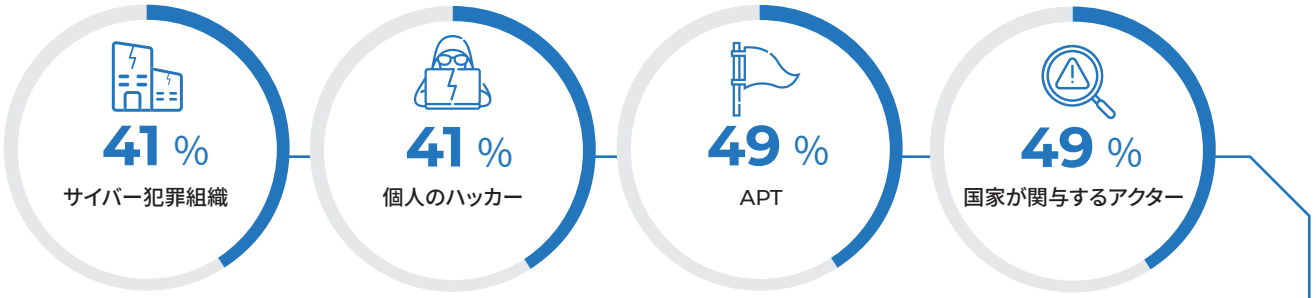
図 2.5.
最もサイバーセキュリティの脅威となる国

調査結果 9

企業のセキュリティ意思決定者の半数近くが、攻撃者の目的を十分把握していないと答えている

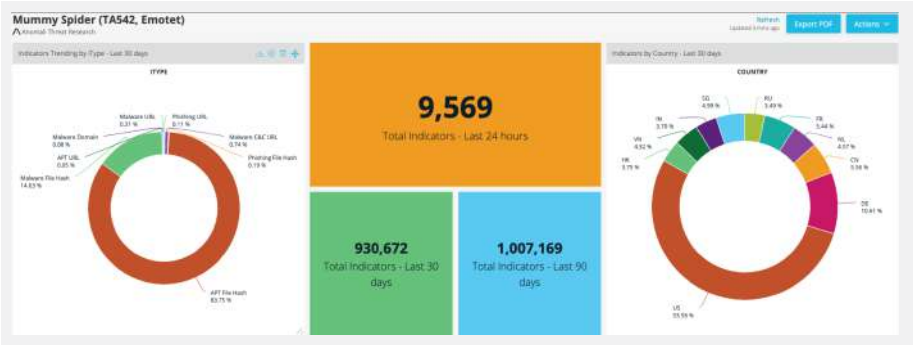
低レベルから中レベルの巧妙さを持つ攻撃者からのノイズは絶え間なく、セキュリティ侵害インジケータ（IOC）はもはや海原に落とされる一滴同然と言えます。そのような中で、さらに高度な攻撃集団がこうしたノイズに隠れて、カスタムツールやマルウェアを作成したり正規のソフトウェアを悪用したりして、標的型攻撃を実行するのです。そのため、攻撃者の目的を把握して、攻撃者の動きや組織への攻撃方法を知ることが重要になります。

図 2.6.
攻撃者の目的、戦術、手法、手順をあまり理解していないセキュリティ意思決定者の割合



金融サービスやプロフェッショナルサービスの企業では、サイバー犯罪者の目的を把握していると考える傾向が最も高く（それぞれ 64 %と 65 %）、一方で、医療機関ではその傾向が最も低くなっています（45 %）。

脅威アクター：状況を正確に把握



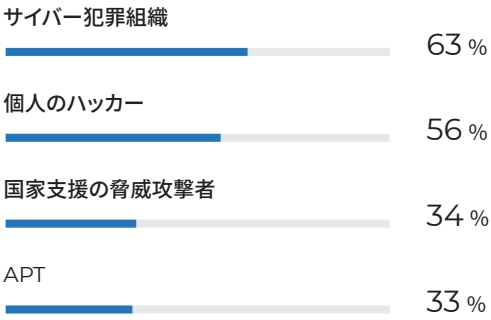
Anomali 脅威調査では、脅威インテリジェンスの管理方法を確認できるダッシュボードを開発し、これにより、広範な初期ネットワークを形成したりデータを集約したりすることができるようになりました。精度がこれほどのレベルであれば、攻撃者の目的や対象を把握しやすくなります。この例では、ダッシュボードを Mummy Spider に適用しています。Mummy Spider は、一般的に Emotet または Geodo と呼ばれるマルウェアの開発に関わっているサイバー犯罪集団です。

調査結果 10

過去 3 年間で、10 社のうち約 9 社（87 %）が何らかのサイバー攻撃の被害を経験

このうちの半数以上が、サイバー犯罪者組織および個人のハッカーによる被害を受けています。3 分の 1 が国家が関与するアクターおよび高度標的型攻撃（ATP）の標的となっています。

図 2.7.
組織へのサイバー攻撃に成功

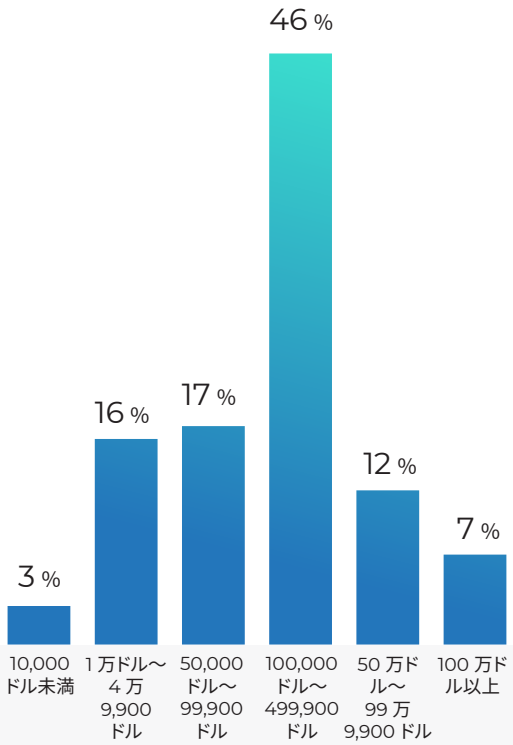


調査結果 11

組織のおよそ半数（52 %）が、過去 3 年間にランサムウェア攻撃を受けている

約 40 %の企業が身代金の支払に応じ（39 %）、5 社のうち 1 社（19 %）が 500,000 ドル以上支払っています。ランサムウェアは最も広く普及している既知の脅威の 1 つであるにもかかわらず、あらゆる組織に大きな損害をもたらし続けています。企業としては、こうした脅威から保護するために、脆弱性の場所を把握し、ネットワークを適切にセグメント化し、ユーザー権限を制限したり監視したりし、バックアップを維持し、ネットワークに侵入される前にランサムウェアを検出して対応できるようになる必要があります。

図 2.8.
身代金で支払われる金額（米ドル換算額）

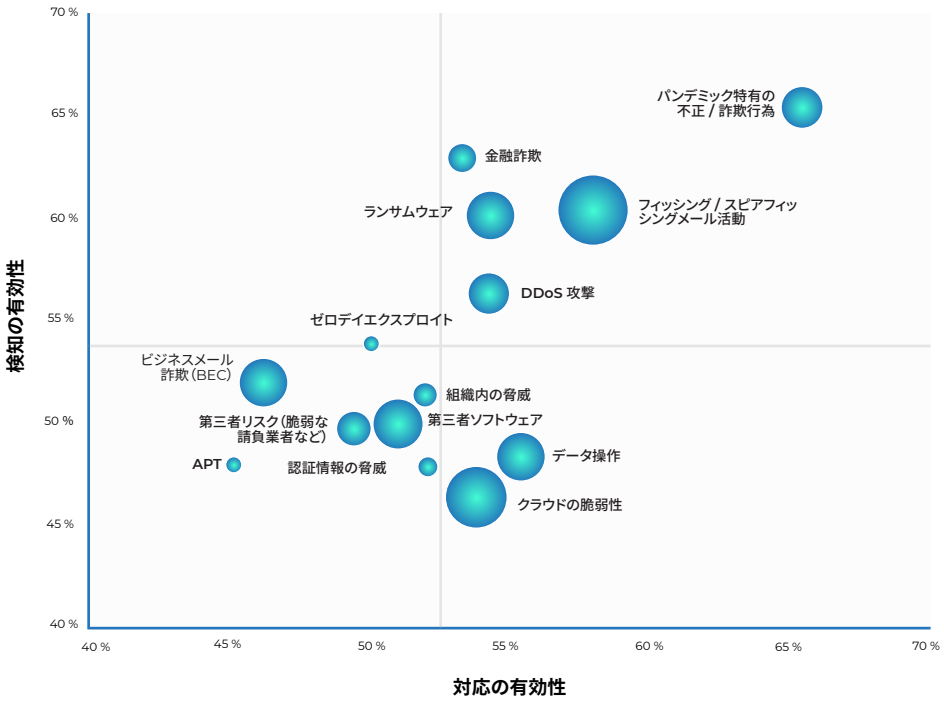


39 %

が、過去 3 年間にランサムウェア攻撃に対して身代金を支払ったことがあると回答

最新の脅威状況

図 2.9.
潜在的な脆弱性領域



注：バブルのサイズは、過去 3 年間に発生した脅威の頻度を表します。

過去 3 年間に APT 攻撃を経験した組織の割合は 17 % になります。この割合は、組織のサイバーセキュリティにおいて APT 攻撃が最大の脅威と考える組織の割合 (18 %) とほぼ同じです。企業セキュリティ意思決定者は、他のタイプのサイバー攻撃に比べ、これらの脅威に対処する能力が低いと感じています。また、組織が APT に対して非常に効果的に検出している (45 %)、あるいは対応している (48 %) と回答している人は比較的少ない傾向があります。

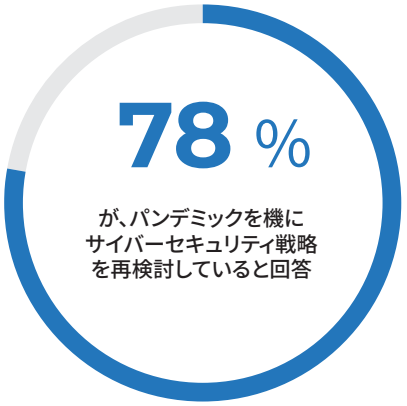
パンデミック発生後、Anomali の脅威インテリジェンスアナリストは、**6,200 件のセキュリティ侵害インジケータ (IOC) と少なくとも 15 の異なるキャンペーンを検知しました。**これらは、80 種類におよぶ MITRE ATT&CK の手法を使用して 39 の異なるマルウェアファミリーを配信する、11 の脅威アクターまたはグループと関連していました。Anomali では早い段階から、公的な組織や民間企業を狙った COVID-19 関連のフィッシングキャンペーンによる脅威が増加し続けると予想していましたが、調査結果 6 および 7 はそのような攻撃が激しさを増していることを示しています。

調査結果 12

パンデミックを機に組織ではサイバーセキュリティ戦略を再評価

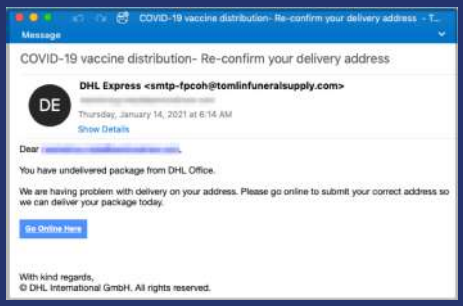
企業セキュリティ意思決定者の 4 人中 3 人 (78 %) が、パンデミックをきっかけにサイバーセキュリティ戦略を再検討するようになったと回答しています。当社では、これにはいくつかの理由があると考えています。デジタル変革プロジェクト、リモートワーカーの増加、対応するクラウドインフラストラクチャの拡張により、パンデミック以前に比べ、攻撃対象領域の拡大が早くなっています。こうした結果、組織ではシステムの可視性を高める必要に迫られています。XDR、MITRE ATT&CK、脅威インテリジェンスなどへの投資計画とそれらの既存の使用状況をわかりやすくするためです (調査結果 13)。さらに、COVID-19 は、フィッシング活動や他の悪意のある活動を実行する上でわかりやすいテーマを脅威攻撃者にもたらしてしまいました。つまり、パンデミックは、混乱、恐怖、好奇心などの感情を植え付けて、悪意のあるリンクをクリックするよう人々を誘導できる強力な武器になることが判明してしまったのです。新しい COVID 亜種が常に出現するため、組織では、特にフィッシングメール活動など、一般的な攻撃に対応する能力を高める必要があります。

図 3.1.
パンデミックがもたらすサイバーセキュリティ戦略への影響



世界的なパンデミックで攻撃者が有利に

COVID-19 以来、Anomali 脅威調査では、世界的なパンデミックを利用した悪意のある活動を数多く見つけ検出してきました。右側の画像は、2020 年 6 月初旬に出回り始めた偽の COVID-19 モバイルデバイスアプリケーションの例です。こうした詐欺的なマルウェアの拡散からセキュリティーコミュニティーや消費者を保護するために、Anomali 脅威インテリジェンスのアナリストは、次のトピックのブログを公開して詳細を解説しています：**「デバイスを監視して個人データを盗み取るマルウェアをダウンロードさせる偽の COVID-19 コンタクトトレースアプリケーションを Anomali 脅威調査が確認」**



Anomali 脅威インテリジェンスのアナリストは、偽の COVID-19 コンタクトトレーシングアプリに加えて、パンデミックをテーマにしたメールフィッシング活動も検出しました。このメールは 2021 年 2 月に検出されたものです。

クレジット：「悪意のある **PDF** をホストする **AWS** を悪用した活動を実施するために、脅威攻撃者は **COVID-19** ワクチンに関するニュースを利用」Anomali 脅威調査より

調査結果 13

サイバー脅威の金銭的影響は、サイバーセキュリティ予算の増加と、サイバーインシデントやランサムウェア攻撃による直接損失の両面で評価可能

組織は、フィッシングメール活動、クラウドの脆弱性、ランサムウェア、APT など、さまざまなサイバー脅威から保護するために、堅牢な防衛を維持する必要があります。企業は現在、IT 予算の約 40 %をサイバーセキュリティに充てています（38 %）。また、企業セキュリティ意思決定者の 4 分の 3（74 %）は、予算が前年から増加していると回答しています。

しかし、このような支出レベルにもかかわらず、サイバーインシデントによる直接的な損失は増え続けています。2019 年の報告によると、100,000 ドル以上（米ドル換算）の損失となった企業は世界規模で約 3 分の 1（36 %）程度でした。2020 年になると、それがほぼ半分（47 %）のレベルにまで上昇しました。また、報告によると、同年において 500,000 ドル以上の損失と 100 万ドル以上の損失が倍になっています（2019 年～2020 年にかけ、500,000 ドル以上の損失が 15 % から 28 %まで上昇、100 万ドル以上の損失が 5 % から 11 % まで上昇）なお、調査実施当時、2021 年の数値はありませんでした。

図 3.2.
サイバーセキュリティの予算

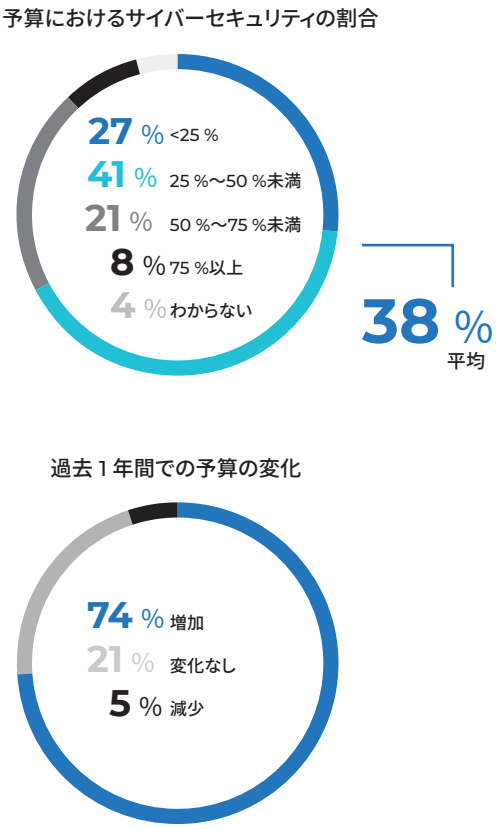
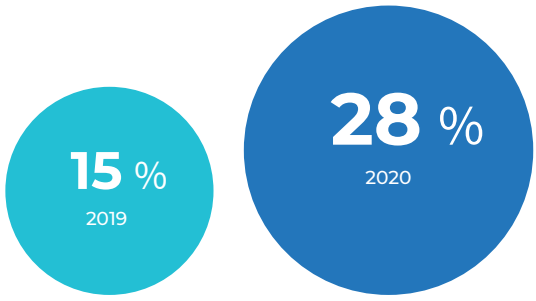


図 3.3.
サイバー攻撃による組織の損失は 50 万ドル以上（米ドル換算額）



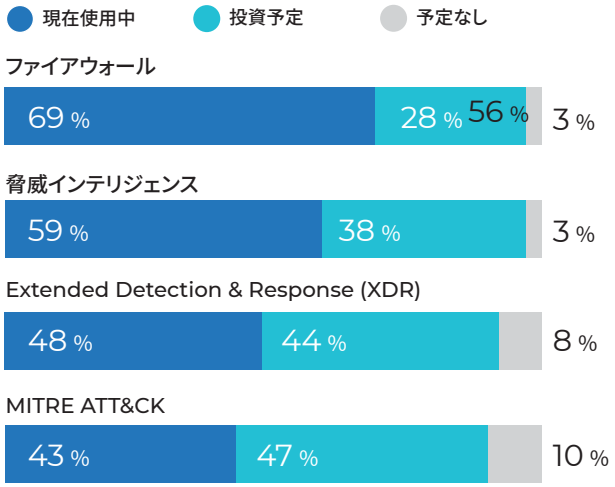
ランサムウェア攻撃も非常にコストがかかるようになってきました。ランサムウェア攻撃を受けて身代金を支払った組織は約 5 分の 2（39 %）でしたが、さらにその約 3 分の 2（65 %）の組織が、米ドル換算で 10 万ドル以上支払っていました。

調査結果 14

組織は従来のテクノロジーを使い続けているが、新たなイノベーションも取り込み始めている

7 割（69 %）の組織は、今でもファイアウォールを使用してネットワーク内の脅威を検知しています。しかし、脅威インテリジェンスを使用している組織は 59 %（投資予定の組織は 38 %）、XDR を使用している組織は 48 %（投資予定の組織は 44 %）、MITRE ATT&CK フレームワークを使用している組織は 43 %（投資予定の組織は 47 %）となっています。このような新しいツールに投資し、使用する姿勢への変化は、従来のソリューションもセキュリティ防衛戦略において引き続き一定の役割を果たすものの、これらのみに依存して進化する脅威を検知し、対応することはできないと企業が認識していることの表れだと考えています。

図 4.1.
現在使用されているイノベーション



調査結果 15

新しいサイバーセキュリティソリューションを既存のフレームワークやアーキテクチャに統合することが必要

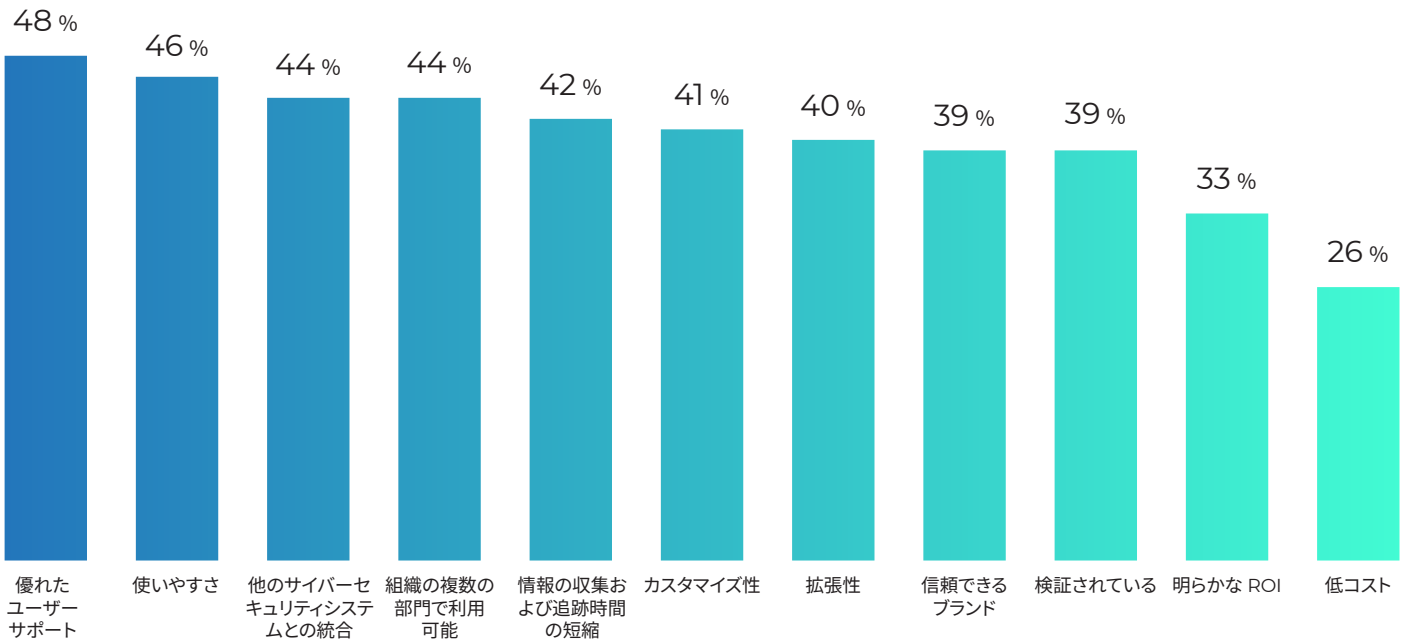
企業セキュリティ意思決定者は、日々直面するサイバー脅威に対処するために、サポートが充実し、使いやすく、他のサイバーセキュリティシステムや組織のさまざまな部分と統合された新しいソリューションを求めています。

また、新たなサイバーセキュリティツールを評価する際、少なくとも 10 人中 4人（41 %）の意思決定者がカスタマイズや拡張性を重要な要素と考えています。意思決定者の多く（39 %）は、十分にテストされている信頼できるブランドのソリューションを求めています。

興味深いことに、新しいサイバーセキュリティソリューションにおいて ROI を実証することが不可欠と感じている意思決定者は、3 分の 1 程度となっています（33 %）。低コストは関心事として最も低く、これを必須要件として挙げている意思決定者は 4 分の 1（26 %）程度になっています。

サイバー攻撃への対応

図 4.2.
サイバーセキュリティソリューションの評価に不可欠な要素



従来のテクノロジーに対し過度に依存し続けていることが判明しているにもかかわらず、今もなお組織が、MITRE ATT&CK フレームワーク、XDR、脅威インテリジェンスなどの、問題に対処できるイノベーションを使用したりイノベーションへの投資を計画したりしていることがわかったのは、心強いことでした。

調査結果 16

脅威状況に対応するために、ほとんどの組織が世界的な脅威を監視できるツールやテクノロジーを使用

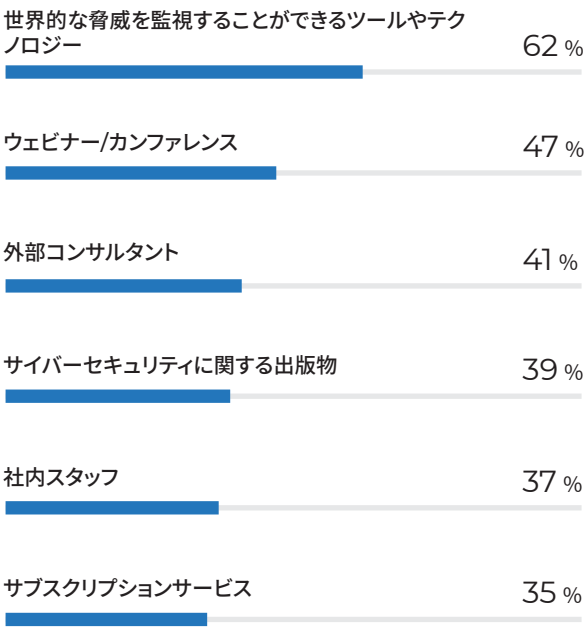
企業がサイバーリスクを管理してサイバーレジリエンスを構築することができるようになるには、脅威インテリジェンスの運用は一層不可欠となります。多くの場合、セキュリティチームは収集したデータや受信したアラートの量で手に負えなくなります。特定のデジタルフットプリント関連の脅威に対応できるようになれば、効果的かつ効率的になります。

調査によると、組織の 62 %がツールやテクノロジーを使用して世界的な脅威に注視したり、脅威インテリジェンスのパフォーマンスを向上させたりしています。また、業界指標では、脅威を検出するグローバルなインテリジェンスを使用する脅威管理プラットフォームに対する需要や、データの収集や相関を自動化してセキュリティチームがデータ運用できるようにするテクノロジーに対する需要が高まっていることが示されていますが、今回の調査結果はこの指標とも一致しています。

また、これらのツールにより、利害関係者の要件を管理したり、攻撃者の意図や目的を把握の上でデータ分析を最大限に活用したり、意思決定の予測や改善を行ったりするプロセスがインテリジェンスの専門家にもたらされます。

サイバーセキュリティは今や重要なビジネス戦略です。サイバーセキュリティ脅威を把握してこれを軽減していくには、適切なツール、情報、専門知識が必要です。効果的な脅威インテリジェンスプログラムにより、組織は脅威を早期に検出し、迅速に対処することができるようになります。

図 4.3.
急速に変化する脅威の状況に組織が対応する方法



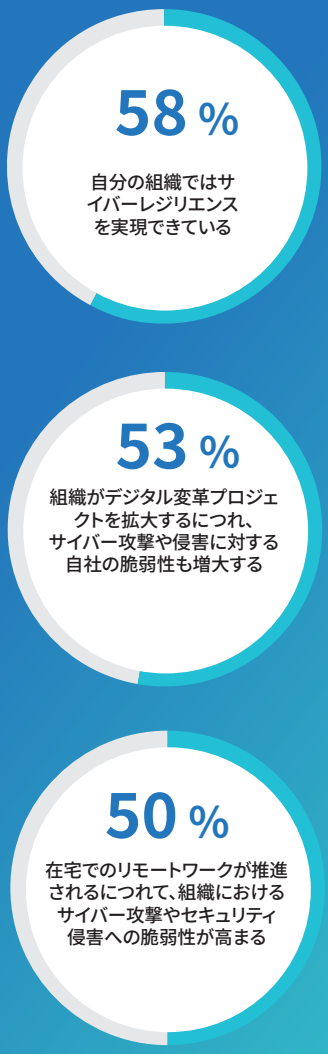
まとめ

組織が達成したサイバーレジリエンスレベル

この調査では、サイバーレジリエンスについて、脅威や攻撃者から組織を事前および事後対応的に保護したり、攻撃時における状況の変化にも適応したり、サイバー攻撃後に回復したりできる能力と定義しました。組織ではサイバーセキュリティ予算を増加したり、革新的なセキュリティレイヤーを追加したり、コストに対する有効性に注力したりしていますが、将来的な成長を望むのであれば、すべきことがまだ多くあることがわかりました。

ほぼ 2 年にわたり、私たちは仕事や個人の生活で前例のない問題や混乱に見舞われました。企業のセキュリティ意思決定者の中にはあれから進歩していると考える人もいますが、当社としてはそのような判断はできません。10 人中 6 人 (58 %) の意思決定者は、サイバーレジリエンスを実現していると自信を持って回答していますが、過去 3 年間にサイバー攻撃によりビジネスの損害、混乱、侵害を被った組織は 87 %にのぼっています。レジリエンスが必要なレベルに達していないと感じている組織は 42 %で、セキュリティ体制に対する評価をより正確に行える余地があります。レジリエンスの実現を自負するセキュリティ意思決定者も含め、意思決定者の約半数は、デジタル変革プロジェクトの拡大やリモートワークの継続により攻撃の被害者になる可能性が高まると考えています。

図 5.1.
組織のサイバーレジリエンスの状況
(とてもそう思う)



Anomali について

Anomali は、インテリジェンスに基づく XDR (Extended Detection and Response) サイバーセキュリティソリューションのリーダーです。ビッグデータの管理を基盤とし、人工知能と機械学習により磨きをかけた Anomali プラットフォームは、業界最大規模のグローバルインテリジェンスリポジトリと、お客様が導入しているセキュリティソリューションから得た膨大なテレメトリを相関付ける独自の機能を備えているため、セキュリティ運用チームが正確に脅威を検知し、最適な対応を行い、レジリエンスを実現し、攻撃者やセキュリティ侵害を阻止できるように支援します。Anomali の SaaS を基盤としたクラウドファーストソリューションは、既存のセキュリティ技術スタックと簡単に統合できるため、ハイブリッド型の導入にも対応します。Anomali は、2013 年の設立以降、公的な組織や民間企業、ISAC、MSSP、そして全世界の Global 1000 企業のお客様にサイバーセキュリティソリューションを提供してきました。さまざまな業種のお客様にご利用いただいており、主要業種を網羅しています。Anomali は、Google Ventures、General Catalyst、IVP などの大手ベンチャーキャピタルから出資を受けています。詳しくは、www.anomali.com をご覧ください。

Anomali ができること

サイバー犯罪、国家規模の攻撃者、ハクティビストは、組織を標的とした敵対行為を試み続けています。組織は、脅威インテリジェンスデータやインサイトを使用して、脆弱性を完全に把握し、脅威に先んじて迅速に対応していく必要があります。

Anomali のインテリジェンス駆動型の拡張検出および応答 (XDR) により、脅威に対する迅速かつ効果的な防御や対処に必要なコンテキストが、セキュリティチームにもたらされます。セキュリティチームは、社内外の脅威データ、情報、インテリジェンスを収集したり分析したりするプロセスを自動化することで、脅威を迅速に把握し、影響を判断し、最適化された応答を通知できるようになります。

Anomali 製品

Anomali ThreatStream
脅威インテリジェンス管理です。生データの収集や処理を自動化し、それをすぐに使える脅威インテリジェンスに変換して、検出の迅速化、調査の合理化、アナリストの生産性向上を実現します。

Anomali Match
インテリジェンス駆動型の Extended Detection and Response (XDR) により、脅威の検出や対応がリアルタイムで迅速にできるようになります。Match では、あらゆるセキュリティテレメトリをアクティブな脅威インテリジェンスと自動的に関連付けて、1 秒間に 190 兆件以上の脅威イベントを配信して既知および未知の脅威を明らかにし、侵害や攻撃を阻止します。

Anomali Lens
自然言語処理 (NLP) 拡張機能。Web ベースのコンテンツを自動的にスキャンして関連する脅威を特定したり、問題を調査してレポートを作成するライフサイクルを合理化したりすることで、脅威インテリジェンスを運用できるようになります。

Anomali が組織のサイバーレジリエンス向上にどう役立つかについては、**anomali.com** をご覧ください。

SS

Anomali は Harris Poll に委託して、従業員数が 5,000 人以上の組織の企業セキュリティ意思決定者に対してオンライン調査を実施しました。この調査は、2021 年 9 月 9 日～10 月 13 日に、下記の国で実施されました。

調査対象者

- **18** 才以上
- **フルタイムで雇用されていること**
- **金融サービス、製薬、医療、電気通信、製造業、専門サービス業界**
- IT **担当**
- **技術的な立場：**マネージャ以上で、データセキュリティソリューションに影響力を持つ
- **ビジネス的な立場：**ディレクタ以上で、データセキュリティ戦略に影響力を持つ

製造業、電気通信、金融サービス、医療、医薬品、専門家、科学技術サービスなどの選定産業における従業員数 5000 人以上の企業の生データに関しては、各国ごとに必要に応じて、従業員数群の企業数でウェイトが置かれ、母集団中の実際の比率と一致するようになっています。その後、ポストウェイトで各国を統合して、合計にて等しく釣り合うようにされています。