2023年3月

市場レポート

2023年 ランサムウェアに関する洞察

世界における ランサムウェア攻撃の広がりと 影響について

Barracuda
Your journey, secured.

目次

はじめに

ランサムウェア — 絶えず進化する脅威

ランサムウェアは、標的のネットワークに感染し、身代金が支払われるまでデータやシステムをロックするよう設計された悪意のあるソフトウェアです。ランサムウェアは、進化し多様化する脅威であり、機密情報の窃取や身代金を支払わない場合はデータを公に漏らすといった内容の脅迫を行うことがあります。犯罪ビジネスモデルは大きな利益を得るように設計され、多くの場合サービスとして利用可能になっています。そのため、攻撃者のリソースやスキルのレベルに関係なく、アクセスできるのです。

潜在的にすべての組織がターゲットとなります。ランサムウェア攻撃は、日常業務や顧客のサプライチェーンを麻痺させ、混乱と経済的損失を引き起こす可能性があります。さらに、会社の評判だけでなく、顧客との関係も破綻させる可能性があります。

当社は、過去12ヶ月間における組織を標的としたランサムウェア攻撃について国際調査を実施しました。その調査結果によると、回答者のほぼ4分の3（73%）が2022 年に少なくとも1回ランサムウェア攻撃の被害を受け、38%が2回以上被害を受けたと述べています。

ランサムウェアに何度も攻撃された組織は、暗号化されたデータを復元するために身代金を支払う傾向が高いことが回答から読み取れました。1回のみの被害者のうち31%が、暗号化されたデータを復元するために身代金を支払ったのに対し、2回攻撃を受けた被害者は34%、3回以上被害を受けた被害者では42% が身代金を支払ったと回答しました。攻撃が繰り返されている組織ほど、データ復元のためのデータバックアップシステムを使用している率も低くなっていました。

この調査結果によると、69%の組織において、ランサムウェア攻撃は、フィッシングメールのような悪意のあるメールを発端としていることがわかりました。フィッシングメールは、サイバー犯罪者が資産、サーバー、データベースを調査してランサムウェア攻撃を行うため、ネットワークアクセス取得用の認証情報を盗むように設計されていることがわかります。WebアプリケーションとWebトラフィックはメールに続く第2位の手法となっており、拡大し続ける脅威範囲の一部として、リスクが高まっている領域です。

サイバー保険に加入している組織は、ランサムウェアの攻撃を受ける可能性が高くなっていました。

サイバー保険に加入している組織の4 分の3 以上（77%）が、少なくとも1回はランサムウェア攻撃を受けていますが、サイバー保険に加入していない組織では65% でした。これは、保険会社が迅速なデータ復旧のために身代金を負担する可能性が高いと予測し、サイバー犯罪者が保険に加入している組織を標的として選ぶ傾向が高いことを意味していると思われます。

この調査では、調査対象の組織の4 分の1以上（27%）が、ランサムウェア攻撃に対処する準備が十分に整っていないと回答しました。

セキュリティ業界は、深くて多層的なセキュリティ技術、脅威のハンティングと拡張型検知応答（XDR）機能、侵入者を発見し攻撃者が簡単に侵入できないように隙間を埋める効果的なインシデント対応を通じて、組織がランサムウェアの脅威に対処するのを助ける重要な役割を、担っています。

調査方法

Barracuda は、独立した市場調査会社である Vanson Bourne に委託し、IT マネージャーと IT の専門家、ベテランの ITセキュリティマネージャー、ITおよび ITセキュリティについて意思決定権を有する人々を対象とした世界規模の調査を実施しました。農業、バイオテクノロジー、建設、エネルギー、政府関連機関、医療、製造、小売、電気通信、卸売など幅広い業界から1350人が調査に参加してくれました。調査参加企業の拠点国は、米国、オーストラリア、インド、ヨーロッパです。ヨーロッパの回答者は、英国、フランス、DACH（ドイツ、オーストリア、スイス）、ベネルクス諸国（ベルギー、オランダ、ルクセンブルク）、北欧諸国（デンマーク、フィンランド、ノルウェー、スエーデン）からでした。調査は 2022年12月に行われました。

このレポートでは、2019年に公開されたBarracudaの委託調査も参照しています。その市場調査には、南北アメリカ、EMEA（ヨーロッパ、中東、アフリカ地域）、および APAC（アジア太平洋地域）において IT セキュリティの職務を担う660 人の幹部、個人、チームマネージャーからの回答が含まれています。

調査結果 #1

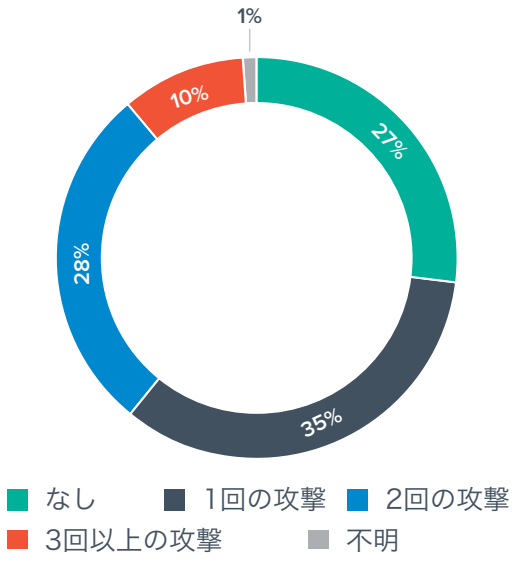
ほとんどの組織がランサムウェア攻撃を経験ーうち3分の1は2回以上攻撃を受けている

調査対象の組織の4分の3弱（73%）が、過去12ヶ月間に少なくとも1回はランサムウェア攻撃を受けたと報告しています。

全体的にランサムウェアの影響を受ける組織の割合が高くなっているのは想定外ではありません。ハッカーはますますサービス化されたランサムウェア攻撃モデル（Ransomware-as-a-Service、RaaS）に目を向けるようになっています。このモデルにより攻撃者はランサムウェア攻撃をより簡単かつ安価に実行できます。多くの場合技術的な知識はほとんど、またはまったく必要ありません。RaaSは、開発者がランサムウェアインフラストラクチャを、他のサイバー犯罪者にリースする有料のマルウェアです。

所属する組織は、過去12ヶ月間に何回のランサムウェア攻撃を経験しましたか？

(n=1,350)



調査対象の組織の3分の1以上（38%）が、過去12ヶ月間に2回以上のランサムウェア攻撃を受けたと報告しています。

複数回の攻撃成功が可能であるということは、最初の攻撃以降、セキュリティギャップへの対応が十分でないことを示唆しています。

これにはいくつかの理由が考えられます。例えば、セキュリティ管理、インシデント対応、調査能力の不足、攻撃者の高度化やステルス化の進行により、攻撃者が残したバックドアやその他の永続的なツールを特定・除去できていない可能性があります。アクセスポイントが開いたままになり、アカウントのパスワードがリセットされておらず、盗まれた認証情報が再び悪用されてしまったという事態が起きているかもしれません。

攻撃者はITチームが日常のビジネス目的で使用している正当なIT管理ツールを悪用することが多いため、攻撃を完全に抑制することは困難で、またネットワーク内に攻撃者が出現してもすぐに疑われることはありません。

業界ごとのばらつき

ランサムウェアの標的となる業種には、大きなばらつきがありました。例えば、消費者向けサービス企業では、ほぼすべて（98%）が、少なくとも 1 回のランサムウェア攻撃を経験しています。

多くの場合、消費者向けサービスは多数の個人顧客データを処理し、企業外から大量の通信を受信するため、ランサムウェアの格好の標的になります。同時に、ランサムウェア攻撃に対処する準備ができていないと自覚していたのは、この業界の回答者ではわずか22%でした。

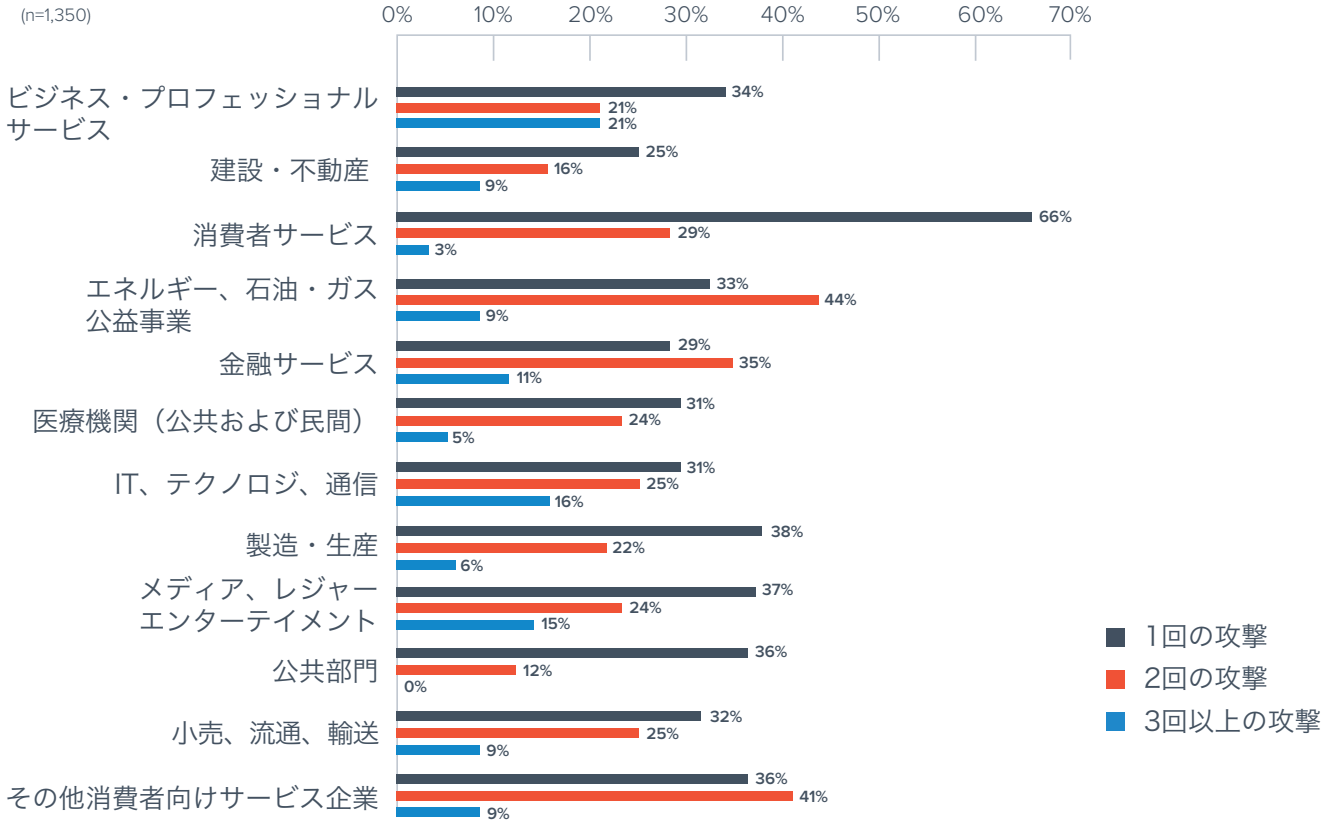
エネルギー、石油・ガス、公共事業の組織も、ランサムウェア攻撃の成功率が平均以上の85% であると報告しています。ランサムウェア攻撃が引き起こす混乱の大きさと潜在的な報酬の大きさを考慮すると、重要なインフラは人気の標的になりつつあります。

当社が昨年公表したランサムウェア攻撃に関する調査では、インフラ設備に関連するサイバー攻撃は4倍に増加しています。これは、サイバー犯罪者が直接的な被害者への影響を超えた、より大きな損害を与えようとしていることを示しています。

エネルギー、石油・ガス、公共事業も、複数の攻撃の影響を受ける可能性が最も高い業界の1つです。2回以上のランサムウェア攻撃の被害を報告している組織は、全体の合計38%と比較して、この業界では53% でした。

また、金融サービス機関では46% が、2回以上の攻撃を受けたと報告しています。医療機関など、ランサムウェアの標的として有名な企業は、複数の攻撃を受けることが少なく、2回以上の攻撃の被害を受けたと報告したのはわずか 29%でした。

12ヶ月間で成功したランサムウェア攻撃の回数（業種別）



調査結果 #2

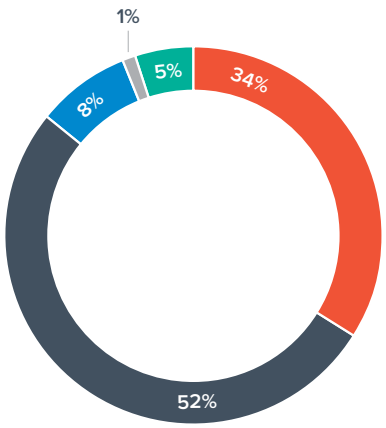
繰り返し被害にあう組織は暗号化されたデータの復旧のために身代金を支払う可能性が高い

通常、成功するランサムウェア攻撃では、組織内の貴重なデータが暗号化されます。過去12ヶ月間にランサムウェア攻撃の被害を受けた調査対象組織の95% が、データが暗号化され、ビジネスに大きな混乱を引き起こしたと報告しています。

全体として、暗号化されたデータを失ったのは1%だけで、34% が身代金を支払うことを選択し、52% はバックアップシステムを使用してデータを取り戻しています。

過去12ヶ月で最も重大なランサムウェア攻撃が発生した際、サイバー犯罪者は組織のデータを暗号化しましたか？

(n=982)

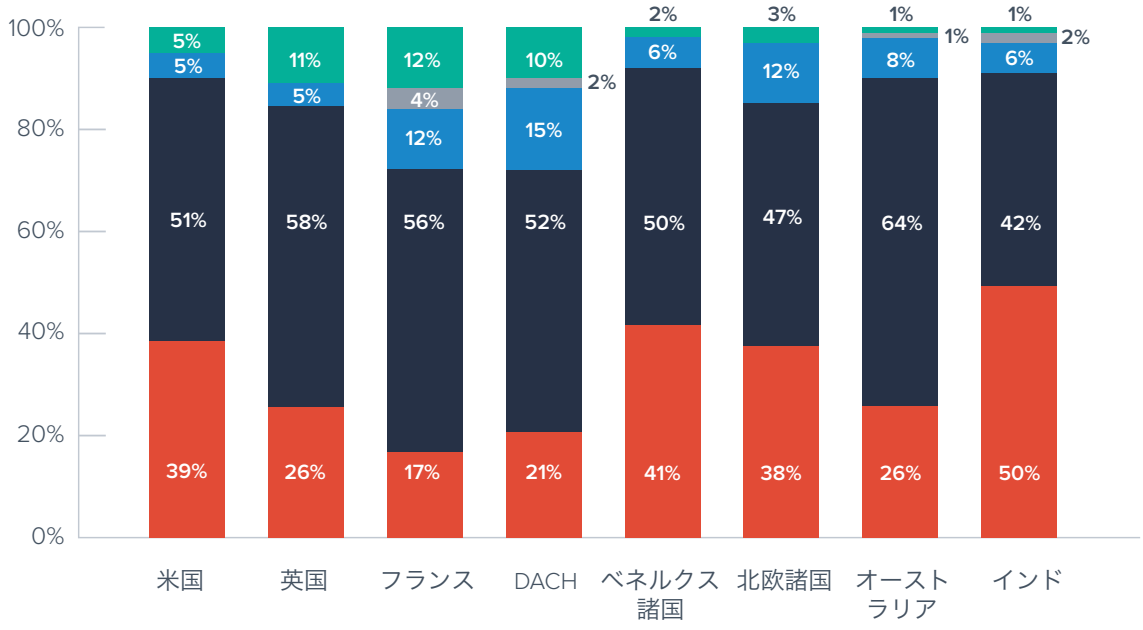


- はい、そしてデータを取り戻すために身代金を支払いました。
- はい、ただしバックアップシステムを使用してデータを取り戻しました。
- はい、ただし他の手段を使用してデータを取り戻しました。
- はい、暗号化されたデータを失いました。
- いいえ、データは暗号化されませんでした。

攻撃数に関係なく、身代金を支払う意思があるかどうかは、国や業界によって大きく異なります。

英国、フランス、DACH（ドイツ・オーストリア・スイス）、オーストラリアでは、組織がデータを取り戻すために身代金を支払った事例が少なく、インドでは被害の 50% で身代金が支払われたという結果が出ています。しかし、ほぼどの国、業界でも、データの復旧方法で最も多かったのはバックアップからの復旧でした。

過去12ヶ月で最も重大なランサムウェア攻撃が発生した際、サイバー犯罪者は組織のデータを暗号化しましたか？
(n=982)



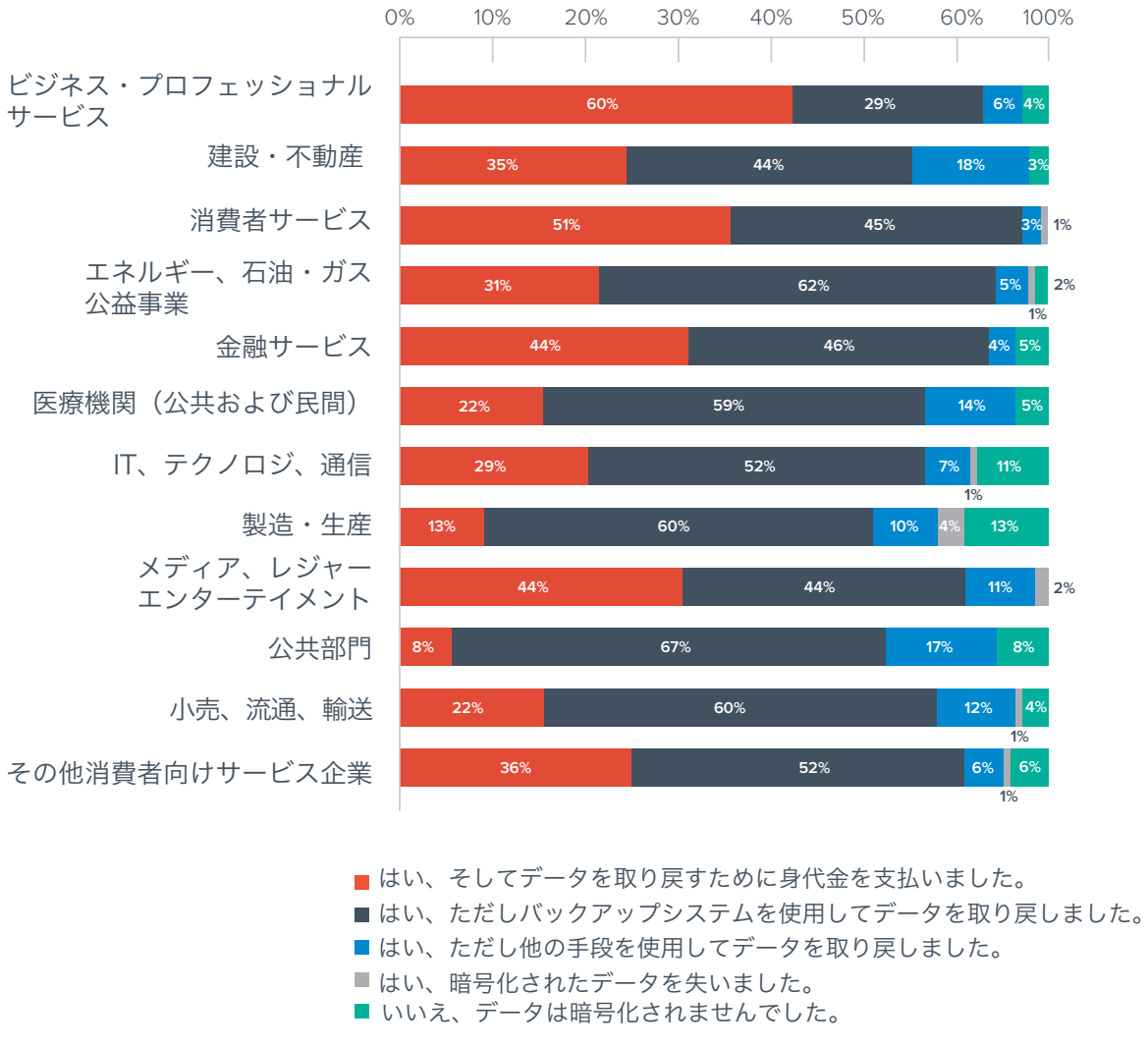
■はい、そしてデータを取り戻すために身代金を支払いました。
■はい、ただしバックアップシステムを使用してデータを取り戻しました。
■はい、ただし他の手段を使用してデータを取り戻しました。
■はい、暗号化されたデータを失いました。
■ いいえ、データは暗号化されませんでした。

ビジネス・プロフェッショナルサービス業界の組織は、データを取り戻すために身代金を支払う可能性が最も高く、60% の事例で支払いが行われています。消費者サービス業界の組織は 51%の事例で身代金を支払っており、金融サービス業界とメディア、レジャー、エンターテイメント業界ではそれぞれ被害の44%で支払いが行われました。

医療機関が身代金を支払う可能性は低く、実際に身代金を支払ったのは事例のうち22%のみでした。

過去12ヶ月で最も重大なランサムウェア攻撃が発生した際、サイバー犯罪者は組織のデータを暗号化しましたか？

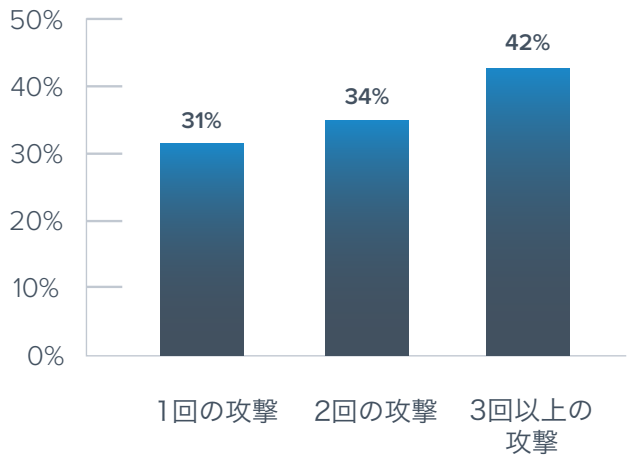
(n=982)



今回の調査では、ランサムウェアの被害を最も頻繁に受けた組織は、暗号化されたデータを復旧するために身代金を支払う傾向が高いことがわかりました。3 回以上の攻撃を受けた組織の 42%が身代金を支払っています。また、これらの組織は復旧に役立つデータのバックアップシステムを利用していない傾向も見られました。

暗号化されたデータを復旧するために身代金を支払った組織

(n=982)



2回以上のランサムウェア攻撃を受けていて身代金を支払った組織の割合は、他の研究の結果とも一致しています。例えば、2022年に行われた身代金の支払いに関する調査では、身代金を支払ったランサムウェア被害組織の 80%が 2 回目の攻撃を受け、多くの場合、再び身代金を支払っています。

複数回の攻撃とランサムウェアの支払いが関連している事象の説明として考えられるのは、ある組織が支払いに応じることがわかると、他の攻撃者もその組織を標的にするということです。

ブラックマーケットや初期アクセスブローカー（IAB）は、支払いに応じ、かつ脆弱な状態のままだとわかっている被害組織へのアクセス認証情報に特に注目している可能性があります。報告されている事例では、同じ攻撃者が再び攻撃してくることもあります。

データのバックアップと復元に役立つデータ保護ソリューションに投資することで、サイバー犯罪者の再攻撃を助長する可能性のある身代金の支払いを回避できます。

調査結果 #3

ランサムウェア攻撃の最も一般的な手法はメール

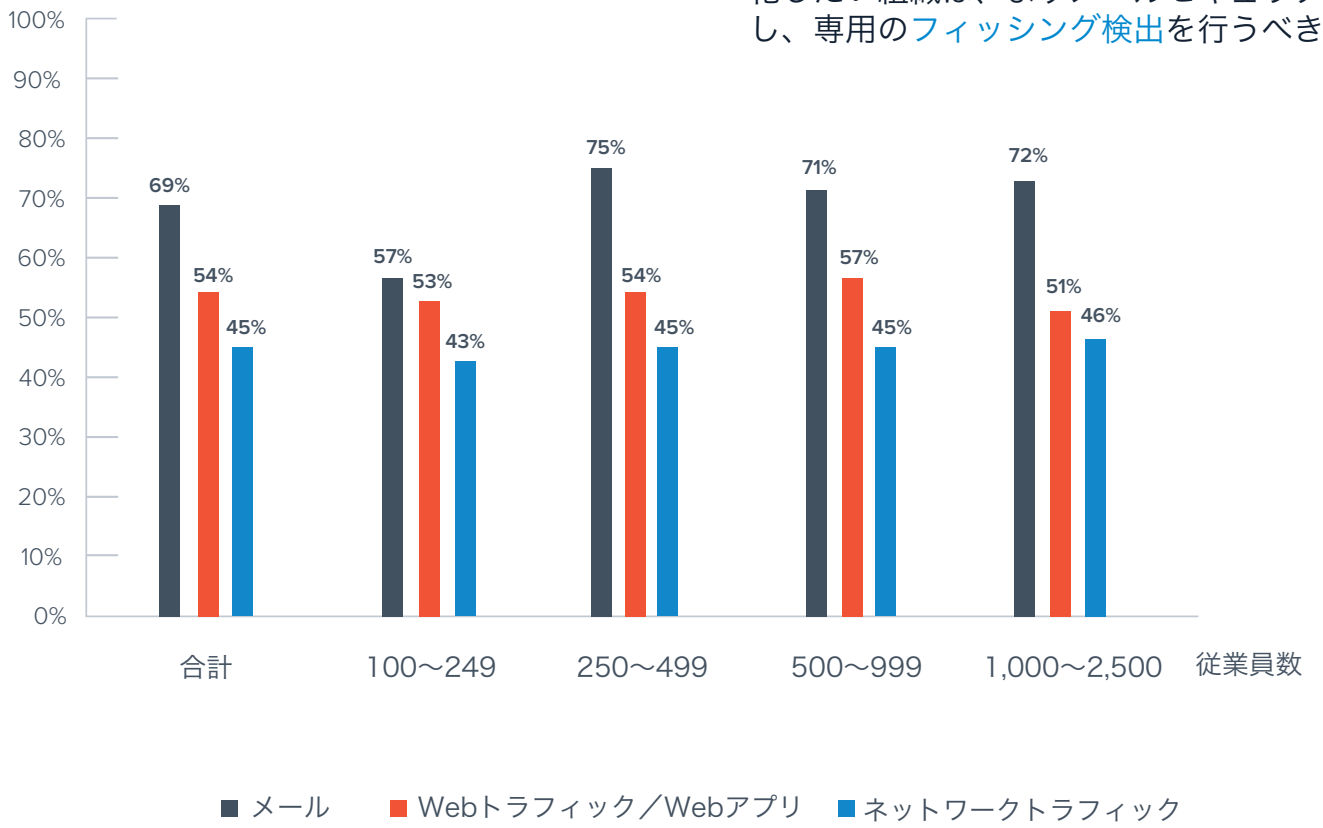
組織の69%で、ランサムウェア攻撃の手法は、悪意のあるメールが使われていました。

従業員が250人を超える中規模の組織では、この割合は平均（75%）よりも高くなります。メールの送信は、組織のネットワークに侵入するよりもはるかに簡単です。

従来、ハッカーは、悪意のあるペイロードを含む文書や、マルウェアを配布する偽のウェブサイトにつながる URLをメールに添付していました。組織がサンドボックスやタイムオブクリックURL保護などの高度な脅威保護を導入するにつれ、サイバー犯罪は、ユーザのログイン認証情報をフィッシングするソーシャルエンジニアリングという手口に変わっていきました。侵害されたアカウントはランサムウェア攻撃の起点となり、サイバー犯罪者は組織内を横方向に移動することで発見を回避できます。ランサムウェアに対する防御を強化したい組織は、まずメールセキュリティに投資し、専用のフィッシング検出を行うべきです。

所属している組織が経験したランサムウェア攻撃は、どこから発生しましたか？

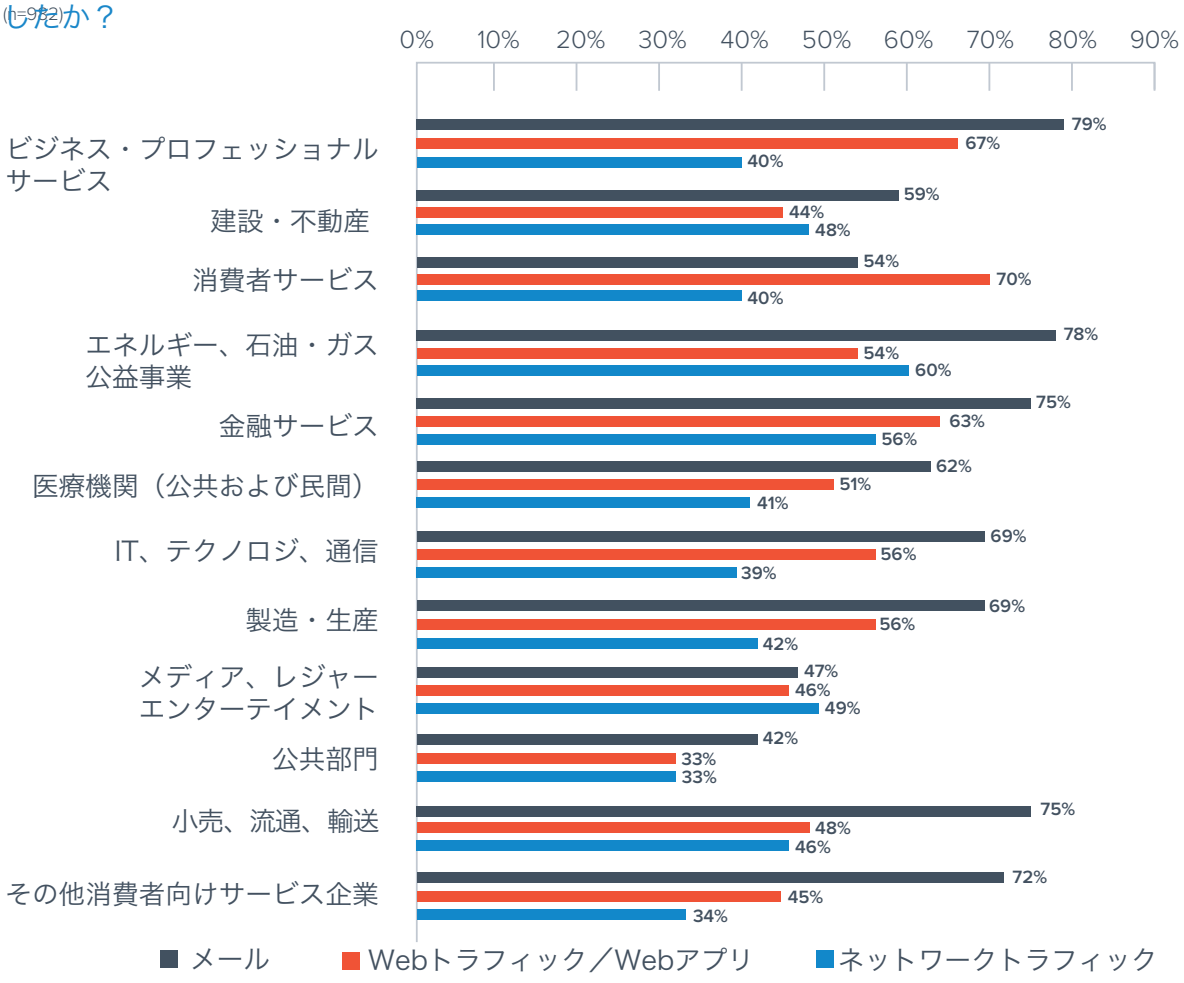
(n=982)



ただし、メールがすべての業界において最大のランサムウェアの媒体というわけではありません。例えば、消費者向けサービス業界では、ほとんどのランサムウェア攻撃は、Webトラフィックと Webアプリケーションから発生しています。

ファイル共有サービス、Web フォーム、eコマースサイトなどのオンラインアプリケーションは、攻撃者によって侵害される可能性があります。Webアプリケーションは、ユーザインタフェイスまたはAPIインタフェイスを介して攻撃されます。多くの場合、こうした攻撃には、クレデンシャルスタッフィング攻撃、ブルートフォース攻撃、またはOWASPの脆弱性が含まれています。アプリケーションが侵害されると、攻撃者はランサムウェアやその他のマルウェアをシステムに導入できます。これは、ネットワークだけでなく、アプリケーションのユーザにも感染する可能性があります。

所属している組織が経験したランサムウェア攻撃は、どこから発生しましたか？ (n=992)



調査結果 #4

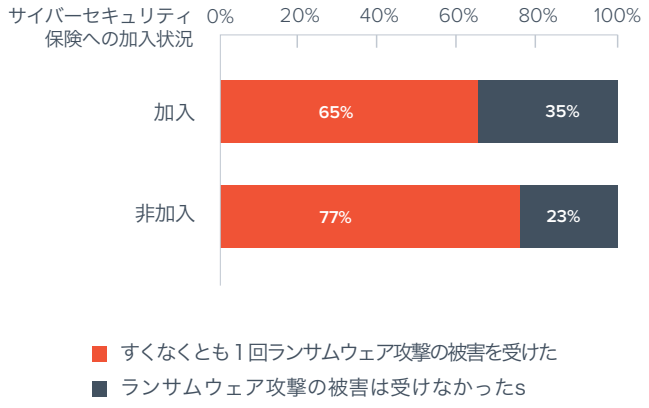
サイバー保険加入組織はランサムウェア攻撃を受ける可能性が高い

調査対象組織の 63%が、あらゆる種類のデータ侵害に関連するコストを最小限に抑えるために、サイバーセキュリティ保険に投資しています。サイバーセキュリティ保険会社は、身代金の支払いの交渉を支援したり、支払いのための資金を提供したりできますが、保険証書には複数の例外事項が含まれていることが多く、組織は依然として非常に多額の請求に直面することになります。

サイバー保険に加入している組織は、昨年ランサムウェア攻撃の被害を受けた割合が高く、**77%がランサムウェア攻撃に見舞われているのに対しサイバー保険に加入していない組織は65% でした。**この結果からは、サイバー犯罪者が、保険会社がデータ復旧をスピードアップするために身代金のコストをカバーする可能性が高いと予測して、保険に加入している組織を積極的に標的にしている可能性が読み取れます。

あなたの組織は、過去12ヶ月間にランサムウェア攻撃の被害を少なくとも1回経験しましたか？

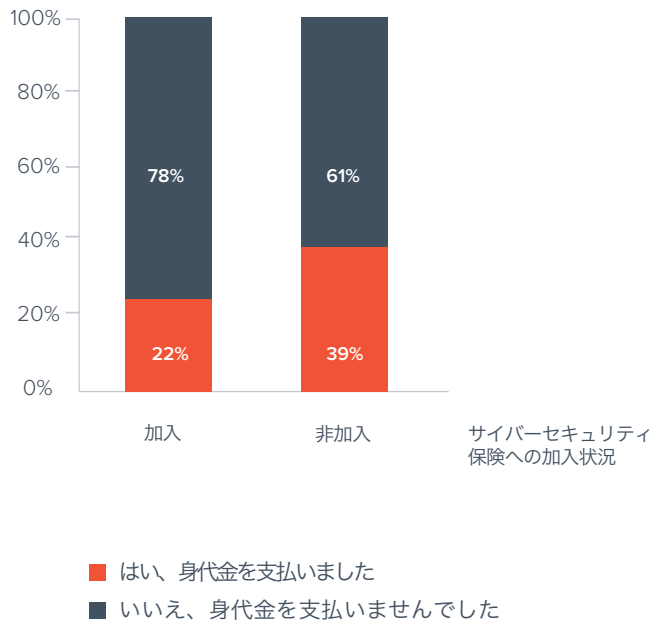
(n=1,350)



例えば、調査結果によると、**サイバーセキュリティ保険に加入している企業は、データを取り戻すために身代金を支払う可能性が高くなっています（保険加入組織は39%、非加入組織は22%）。**また、関連性は認められていませんが、**2回以上のランサムウェア攻撃の影響を受けた組織は、サイバー保険を導入している可能性も高い（70%）ことも注目すべき点です。**

データを取り戻すために身代金を支払いましたか？

(n=982)



調査結果 #5

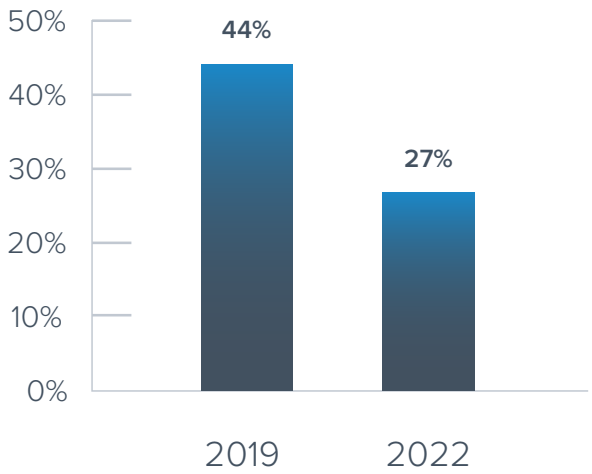
多くの組織は ランサムウェアへの備えが 十分ではないと感じている

調査対象の組織の4分の1以上(27%)が、ランサムウェア攻撃に対処する準備が十分に整っていないと述べています。

これは、ほぼ半数(44%)が「ランサムウェア攻撃に対する準備ができていない」と答えた、2019年の調査と比較すると改善されています。2019年以降、多大な経済的損失をもたらし、非常に注目を集めたランサムウェア攻撃がいくつか起こりました。それらの事件に関する多くの報道があったことで、多くの組織がセキュリティに投資し、潜在的なランサムウェア攻撃に備えるようになった可能性があります。

ランサムウェアに対処するための準備が十分整っていない

(n=660 2019; n=1,350 2022)

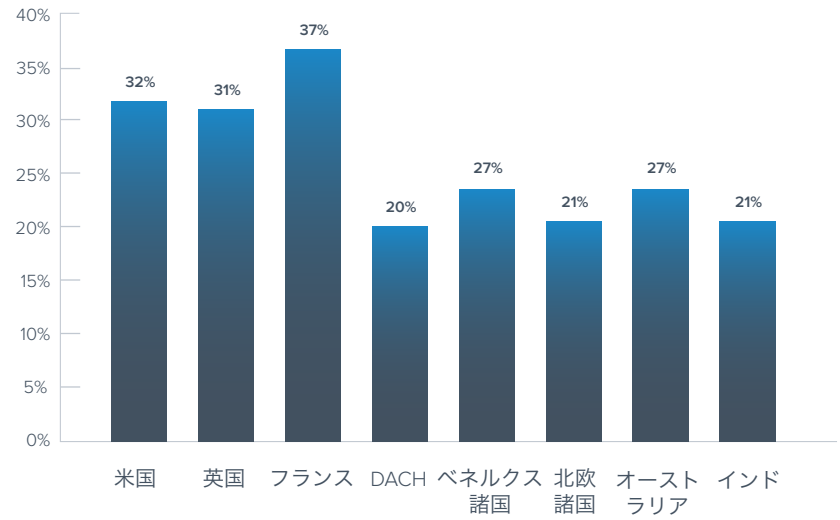


以前のNordLockerの調査によると、米国、英国、カナダ、フランスでは、ランサムウェア攻撃の数が世界で最も多いことがわかりました。当社の調査では、米国、英国、フランスの回答者も、ランサムウェアに対処する準備ができていないと感じていることがわかりました。

その最も多い理由は、組織はサイバー攻撃の数が圧倒的に多いと感じていることで、多数の攻撃により攻撃の成功率が高まることを懸念しています。また、大規模な組織は、保護する必要のあるデータが大量にあり、攻撃対象領域もはるかに大きいという背景から、準備が整っていないと感じています。

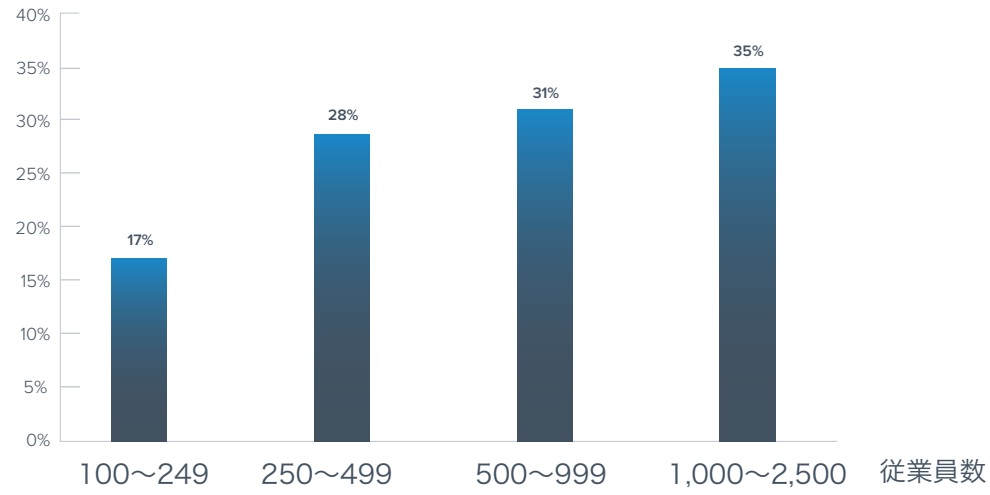
ランサムウェアに対処するための準備が十分整っていない

(n=1,350)



ランサムウェアに対処するための準備が十分整っていない

(n=1,350)



結論

組織は、拡大し続ける攻撃対象領域をランサムウェアなどの進化する脅威から保護するために、統合された多層セキュリティを必要としています。リスクを最小限に抑え、ランサムウェアやその他のサイバー脅威にさらされることを最小限に抑えるために、重点的に取り組むべきサイバーセキュリティ分野を以下に示します。

- 認証情報の保護：認証情報の保護には、二方面からのアプローチが必要です。まず、検出および対応ツールに投資し、次にユーザのトレーニングに重点を置きます。
- メール保護技術は、リンクや添付ファイルを通じて配信された悪意のあるペイロードを検出できるものでなくてはいけません。また、フィルタリング技術を回避してユーザを騙して行動を起こさせるように設計された、高度なソーシャル エンジニアリング戦術を使っている場合でも検出できる技術である必要があります。ソーシャルエンジニアリング攻撃をより高い精度で検出し、通常の通信パターンからわずかなズレを探し出すことができる機械学習技術を統合したメールセキュリティを特に推奨します。
- 従業員が疑わしいメールを認識し、それを報告する方法を学ぶことも重要です。フィッシングシミュレーションなどのツールを使用し、トレーニングの効果を検証するとよいでしょう。
- アカウント、アプリケーション、ネットワークへの安全なアクセス：多要素認証（MFA）は、依然としてベストプラクティスであり、すべての組織で採用されるべきものです。しかし、攻撃者は MFAを回避する方法を見つけるようになってきています。より高度なゼロトラストアクセス戦略の導入を検討してください。この戦略ではユーザとデバイスを継続的に検証し、正しいユーザにのみ正しいリソースへのアクセスを許可するというものです。
- データのバックアップ：ランサムウェア攻撃の影響から組織を守るには、データを適切かつ安全にバックアップし、クラウドにある場合であっても隔離する必要があります。また、データのバックアップによって、合理的な時間枠でデータを復元できるようにする必要があります。そのためには、バックアップの復元プロセスを定期的にテストし、その機能を確認してください。
- 脅威インテリジェンス、インシデント対応、XDRにより、徹底した防御を構築します。ランサムウェアのリリースは攻撃の最終段階であることが多く、それ以前に、横移動、データ流出、追加ツールのインストールなどの作業が発生します。これらの初期段階で攻撃を検知し阻止できれば、ランサムウェアの影響を完全に防ぐことができるかもしれません。
- そこで、XDRのようなサービスの出番となります。XDR（Extended Detection and Response）は、継続的に更新される脅威インテリジェンスに裏打ちされた IT環境全体の可視性を提供します。XDR およびその他の自動インシデント対応ソリューションは、インシデントが拡大する前に特定、抑制、無効化するのに役立ちます。
- 最新の攻撃者の行動やツールなど、進化する脅威の状況を常に把握し、何に注意し、どう対応すべきかを理解することが重要です。違和感がある場合は、すべて調査を行うようにすべきです。調査を行うためのリソースが不足していることが懸念される場合、例えば XDRプラットフォームの一部であるアウトソーシングのセキュリティオペレーションセンターのサービスを利用することを検討してください。このサービスでは、24 時間年中無休でネットワークを監視し、異常な行動や疑わしい動作を調査してくれます。
- Webアプリケーションの保護：ファイル共有サービス、オンラインフォーム、eコマースサイトなどのオンラインアプリケーションは、攻撃者によって侵害される可能性があります。アプリケーションは多くの場合ユーザや APIのインタフェイスを介して狙われます。APIベースのアプリケーションセキュリティと次世代型Webアプリケーションファイアウォールを検討してください。これらのサービスは、ゼロデイ攻撃を含む高度な脅威をブロックする多層セキュリティ、マルウェアの侵入防止とサンドボックス化、ネットワーク内の横移動を防止する強力なネットワークセグメンテーションを提供します。

ランサムウェア対策に関する詳細情報と実用的なガイダンスについては、「身代金を支払わないために～ランサムウェア対策のための3つのステップ～」を参照してください。ガイドに付属しているランサムウェア対策のチェックリストもダウンロードできます。

バラクーダについて

バラクーダは世界をより安全な場所にするために尽力しています。

バラクーダは、すべてのお客様が購入、導入、使用しやすい、クラウド対応かつエンタープライズレベルのセキュリティソリューションを使用できることが当然であると考えています。また、お客様のビジネスとともに成長および変化する革新的なソリューションによってメール、ネットワーク、データ、アプリケーションなどを保護しています。

世界中の20万を超えるお客様がバラクーダを信頼しています。お客様がリスクにさらされていることを知らない場合でも、バラクーダはお客様を保護できます。このため、お客様はビジネスを次の段階に移行することに注力できます。

詳細については、barracuda.co.jpをご参照ください。

バンソン・ボーンについて

バンソン・ボーン（Vanson Bourne）社は、テクノロジ分野の市場調査における独立系スペシャリストです。同社の堅牢で信頼性の高いリサーチベースの分析は高く評価されています。その土台となっているのは厳格なリサーチ原則、そしてさまざまなビジネスセクターおよび主要市場における技術・経営部門の上級意思決定者の意見に耳を傾ける能力です。

詳細については、vansonbourne.comをご参照ください。

Barracuda®
Your journey, secured.