2025年8月

市場レポート

ランサムウェア・インサイト レポート 2025

世界各国の組織における ランサムウェア攻撃の被害実態と その影響について

Barracuda®
Your business, secured.

目次

はじめに

ランサムウェアは広く蔓延しており、今も進化を続けている脅威です。さらに、RaaS（Ransomware as a Service）キットが利用可能になったため、より多くのサイバー犯罪者が攻撃を実行できるようになっています。

ランサムウェアインシデントは、企業の評判を傷つけ、日々の業務を中断させ、混乱、データの損失、顧客の信頼低下などを引き起こす恐れがあります。あらゆる組織が標的になる可能性があります。

本レポートでは、過去12か月間に世界中の組織が実際に受けたランサムウェア攻撃の経験とその影響について調査しています。本レポートは、2,000人のITおよびセキュリティ意思決定者を対象にBarracudaとVanson Bourneが実施した国際的な調査の結果に基づいています。

調査結果は主に、以下の3つのテーマに分類できます。

- **ランサムウェアの被害を受けた組織は、セキュリティ対策が断片化している可能性が高く、**多くのセキュリティツールが連携せずに使用されており、重要なセキュリティ分野における対策が不十分となっています。
- **ランサムウェア攻撃は多面的**になっており、データの暗号化だけでなく、データが窃取されて公開されたり、悪意のある別のマルウェアがインストールされたりする場合もあります。
- **ランサムウェア攻撃を受けた場合の影響範囲は拡大**しており、新たなビジネス機会の喪失や、従業員、パートナー、顧客までもが支払いを要求されるケース、さらには規制当局への通報をちらつかせて身代金を支払うよう圧力をかけられる場合があります。

あらゆる規模や業界の組織が2025年のランサムウェアの脅威と影響を理解し、リスクとなる可能性のある分野を特定して適切に対応するために、本レポートが役立つことを願っています。

調査方法

Barracudaは、独立系市場調査会社Vanson Bourneに委託し、世界規模の調査を実施しました。この調査は、米国、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、スウェーデン）、オーストラリア、インド、日本の各国において、従業員数が50～2,000名の幅広い業種の企業に所属するITおよびビジネス部門のシニアレベルのセキュリティ意思決定者2,000名を対象に行われました。

調査は、2025年4月から5月にかけて実施されました。

主な調査結果

57%

の組織は、
過去12か月間に
ランサムウェア攻撃を受けている。

71%

の組織は、メール侵害とランサムウェア攻撃を経験。

32%

の組織がデータ復旧のために身代金を支払った。そのうちの41%は、すべてのデータを取り戻すことができなかった。

65%

の組織が、ランサムウェア攻撃を受けたのち、バックアップからのデータを復元。

24%

の組織が、ランサムウェアの被害を受けた上にデータを暗号化された。27%の組織が、データを窃取され、29%が攻撃者によって追加のマルウェアがインストールされたと回答。

25%

の組織が、ランサムウェアの被害を受けて、既存顧客を失った。同様に、25%が新たなビジネス機会を失っている。

ランサムウェアによる影響を受けた組織は半数以上

調査対象組織の57%が、過去12か月間にランサムウェア攻撃による影響を受けています。

ランサムウェアの被害を受けた組織のうち、3社に1社（31%）が2回以上被害を受けています。

ランサムウェア攻撃が繰り返し成功するケースがこれほど多いのは、各インシデント後に、セキュリティの弱点についての十分な調査や、適切な対処が行われていないことを示しています。本レポートでは、一度だけ影響を受けた組織と複数回影響を受けた組織の違いを分析し、データから得られる教訓と、その教訓をどのように活用して組織のセキュリティ体制を強化できるかを探ります。

今回の調査でランサムウェアの影響を最も多く受けた業界は、医療機関 （影響を受けた組織は67%）、地方自治体（65%）、小売業（61%）でした。調査データによると、製造業は最も影響を受けていない業界であり、ランサムウェア攻撃の影響を受けたと報告した組織は半数弱（46%）にとどまっています。

ランサムウェア攻撃を受けた割合に関して、企業規模による大きな差は見られず、従業員数50人から2,000人まで、調査対象となったすべての規模で一貫した傾向が示されています。

メールが侵害され、ランサムウェア攻撃も受けた組織の割合は71%にのぼっており、これら2つの攻撃タイプの間に強い関連性があることが明らかになっています。

ランサムウェアの被害を受けた組織は、被害を受けなかった組織とは、セキュリティツールや優先している対策が異なる

セキュリティの乱立がもたらすランサムウェアへのリスク

この調査によると、「セキュリティ・スプロール」と呼ばれる過剰なセキュリティツールの導入は、統合性の欠如を伴うことでスクを高め、保護に抜け穴を生じさせる可能性があります。その結果、ランサムウェアを含む進行中の脅威を組織が検知・対処することを困難にしてしまいます。

データによれば、セキュリティの乱立やツール間の連携不足に直面している組織の割合は、ランサムウェアの被害を受けた割合に比例して増加しています。

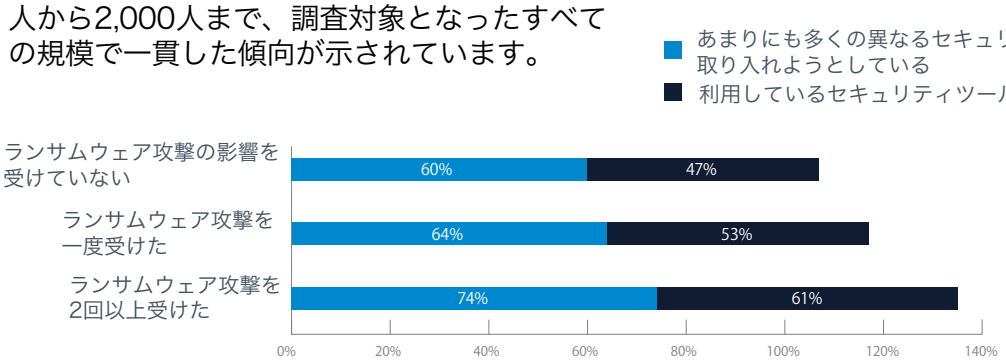


FIGURE 1

ランサムウェアインシデントとセキュリティツールの乱立

n=1,146

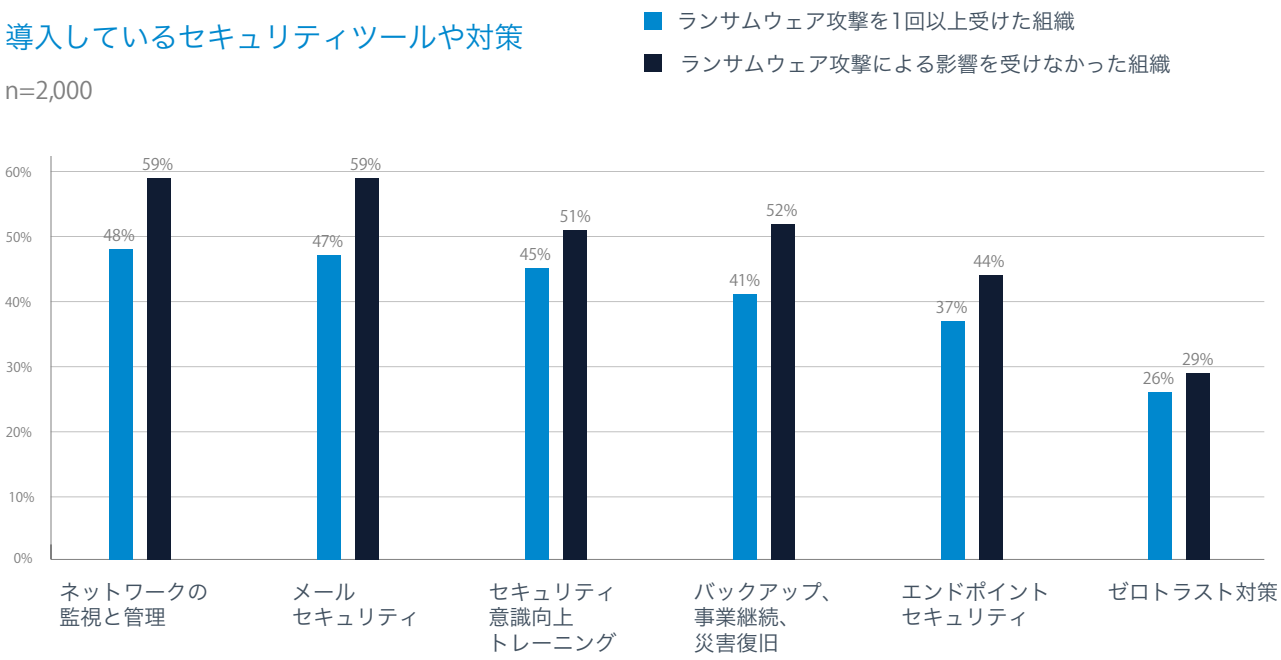
さまざまなセキュリティツールと対策

回答者によると、最も広く導入されているセキュリティ対策は、メールセキュリティ（52%が導入）、ネットワークセキュリティ（52%）、セキュリティ意識向上トレーニング（48%）でした。ランサムウェア攻撃の影響を受けたと報告した組織は、これらの対策を実施している割合が低い傾向にあります。

FIGURE 2

導入しているセキュリティツールや対策

n=2,000



回答者に

- メールセキュリティ：ランサムウェアの被害を受けた組織では47%、被害を受けていない組織では59%が導入。
- ネットワーク管理と監視ソリューション：ランサムウェアの被害を受けた組織では48%、被害を受けていない組織では59%が導入。
- セキュリティ意識向上トレーニング：ランサムウェアの被害を受けた組織では45%、被害を受けていない組織では51%が導入。
- エンドポイントセキュリティ：ランサムウェアの被害を受けた組織では37%、被害を受けていない組織では44%が導入。

これらの調査結果は、ランサムウェアの被害を受けた組織が、リスクレベルの軽減に役立つセキュリティ分野への投資が不十分である可能性を示しています。

例えば、メールセキュリティ、ネットワークセキュリティ、エンドポイントセキュリティに加え、セキュリティ意識向上トレーニングを組み合わせることで、メールを媒体とするフィッシングやソーシャルエンジニアリング攻撃に対して強力な防御を提供できます。これらの攻撃は、認証情報を詐取し、攻撃者のネットワークへの侵入、デバイスを侵害し、横展開を行うといった、ランサムウェア攻撃において典型的に用いられる手法に対して強固な防御を構築できます。

ランサムウェアグループが身代金を受け取れる確率は3分の1

ランサムウェアの被害を受けた組織の32%が、データの復旧や復元のために身代金を支払っています。

調査結果は、組織が身代金を支払う傾向と、ランサムウェアの被害を受ける回数との間に相関関係があることを示しています。

ランサムウェアの被害を1回のみ受けた組織は、身代金を支払う傾向がやや低く、29%が支払いに応じていました。一方、2回以上被害を受けた組織では、データを取り戻すために身代金を支払った割合が37%に上りました。

この数値は、2年前に実施した前回調査からほとんど変わっていません。

2023年の調査結果では、被害を1回のみ受けた組織の31%、2度以上被害を受けた組織の38%が、データ復旧のために身代金を支払っていました。

複数回の被害と身代金の支払いとの関連については、組織が一度でも身代金の支払いに応じたことが知られると、他の攻撃者に狙われやすくなったり、同じ攻撃者が繰り返し標的にしたりする可能性がある、という説明が考えられます。

喜ぶべきは、ランサムウェアの被害を受けた組織の大多数（65%）がバックアップからデータを復旧できていたことです。

身代金を支払っても報われないという現実があります。身代金を支払った組織の41%（全体では13%）は、すべてのデータを、あるいは一部のデータさえも取り戻すことはできませんでした。

データの暗号化はランサムウェア攻撃の1つの手段に過ぎない

調査から、ランサムウェア攻撃を受けた場合は、身代金の支払いによる財務的な負担はもちろんのこと、ビジネス、業務、さらには従業員の感情面への影響も非常に大きいことが明らかになっています。

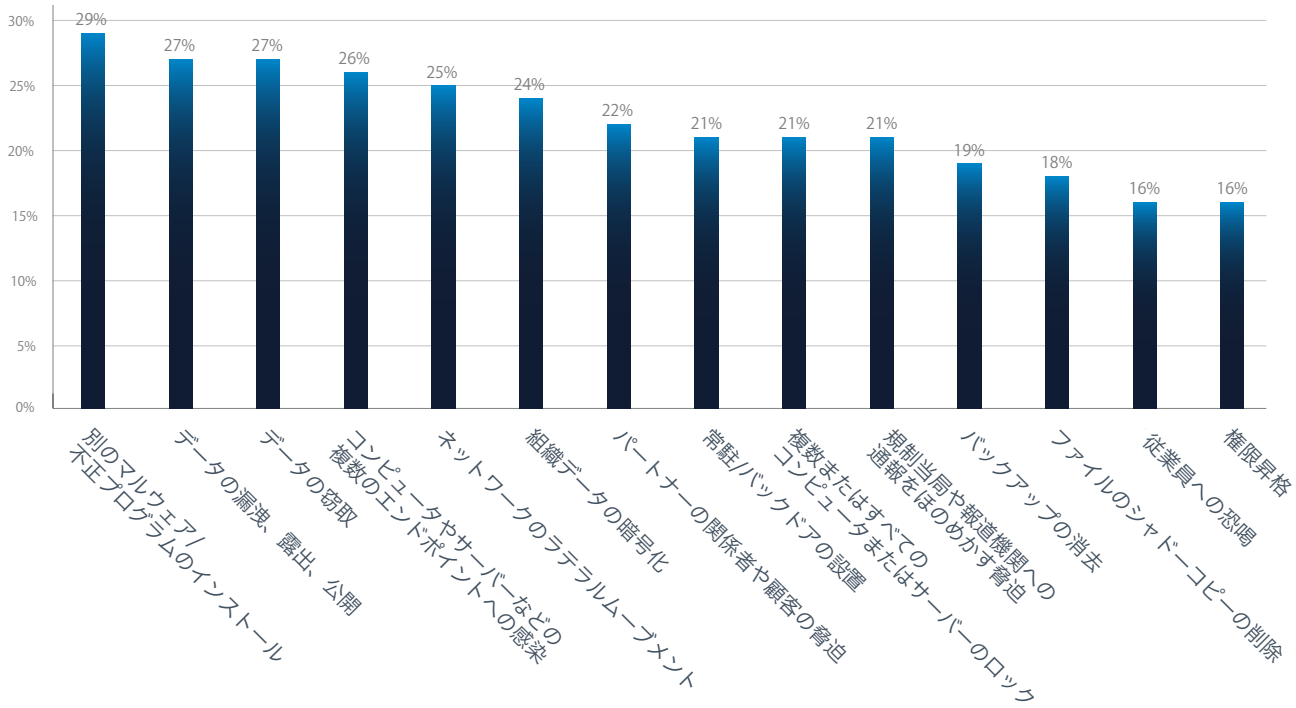
多くのランサムウェア攻撃では、データの暗号化やシステムやコンピュータのロックが最終的な目的とされています。これは攻撃において最も目に見える部分であるため、セキュリティチームに侵入者の存在を察知されやすく、その結果、脅威の封じ込めや排除につながる可能性が最も高くなります。

調査結果から、ランサムウェアが実行される前段階で、攻撃を成立させるため、あるいは別の活動の足がかりとするために、水面下で広範な活動が行われている実態が明らかになりました。

FIGURE 3

最も深刻だったインシデント発生時にランサムウェアグループが実行した活動

n=1,146



回答者が経験したランサムウェアインシデントの約4分の1では、データの暗号化（24%）、エンドポイントのロック（21%）、およびデータの窃取（27%）が発生していました。

攻撃には、ネットワークにわたるラテラルムーブメント（25%）、複数のエンドポイント（コンピュータやサーバーなど）への感染（26%）、追加の悪意あるペイロードのインストール（29%）、権限昇格（16%）、およびバックドアやその他の常駐メカニズムの埋め込み（21%）も含まれています。

さらに、被害組織が身代金を支払わずにデータを復旧するのを困難にするために、攻撃者の約5人に1人がバックアップにアクセスして消去したり、ファイルのシャドーコピーを削除したりしていました（いずれの攻撃も被害者の19%で発生）。

また、調査結果からランサムウェアが実行され身代金が要求された後、攻撃者は心理的な手法によって被害者に圧力をかけ始めることも判明しました。これらの手法には、パートナーや株主、顧客への脅迫（22%が経験）、マスコミや規制当局への通報をほのめかす脅迫（21%）、さらには従業員への脅迫（16%）などが含まれます。

実際に被害を受けたランサムウェアインシデントの27%において、攻撃者は窃取したデータの漏洩、露出、あるいは公開に及んでいます。

ランサムウェア攻撃の被害により、顧客や新たなビジネス機会を喪失

実際の攻撃が一段落した後、被害を受けた組織は業務やビジネスへの影響に直面することになります。

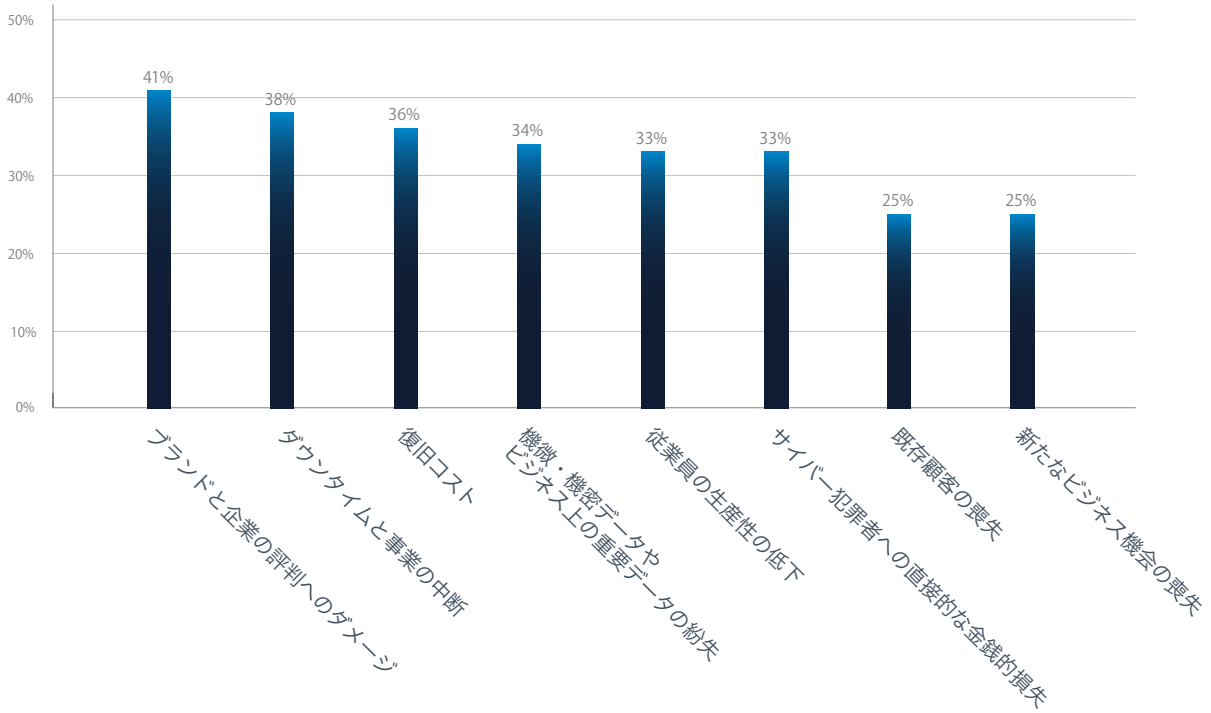
ランサムウェア攻撃の被害組織が最も多く挙げた影響は、ブランドや評判へのダメージでした（41%に影響）。そして、ダウンタイム（38%）、復旧コスト（36%）が続きます。3分の1（34%）が機密データを失ったことを認めています。

ランサムウェアの被害を受けた4社に1社は、既存顧客と新規ビジネス機会の喪失という長期的なビジネスへの影響にも直面しています（いずれも25%）。

FIGURE 4

過去12か月で最も深刻だったランサムウェア攻撃による影響

n=1,146



結論

ランサムウェアに対して強靭であるためには、拡大し続ける攻撃対象領域をサイバー脅威から守るための統合的で多層的なセキュリティ対策が必要です。

以下の実践的な対策によってセキュリティを強化できます。

- **データを定期的かつ安全にバックアップ**し、オフラインで保管されていることを**確認します**。効果的にデータを復旧できるようにテストを実行します。
- **多要素認証を導入し、最小権限の原則を適用**して、企業資産やアプリケーションへの**アクセスを制限**します。これより、認証情報が窃取されても、攻撃者が価値の高いデータやシステムを標的にすることから防御できます。
- 最新のセキュリティパッチを適用して**ソフトウェアを更新**し、セキュリティの弱点を解消します。
- 最新のフィッシングやランサムウェアの手法を中心に学ぶことができる、従業員向けのサイバーセキュリティ意識向上トレーニングを定期的に実施します。
- **ネットワークをセグメント化**し、重要なシステムを隔離して、攻撃者によるラテラルムーブメントを防ぎます。
- クラウドを含め、すべての**設定に誤りがないか確認します**。設定ミスはセキュリティ侵害の主な原因になっています。
- **堅牢なメールセキュリティソリューションを導入します**。メールは依然としてランサムウェアの主要な侵入経路であり、高度なAIを活用したセキュリティ対策は、悪意あるペイロードの検出や、セキュリティ対策を回避する巧妙なソーシャルエンジニアリング手法の識別に効果を発揮します。
- 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**Webアプリケーションを保護します**。アプリケーションは、ユーザーインターフェイスやAPIインターフェイスを通じて標的にされることが多くあります。
- **インシデント対応計画を策定し、定期的に訓練します**。
- さらに、マネージドサービスプロバイダーやセキュリティベンダーなど、**外部の専門家と連携して、支援を受けることも検討してください**。これらのパートナーは、先進的な統合型セキュリティプラットフォームやソリューションの導入を支援し、24時間365日体制で進行中の脅威を検知、ブロック、対応することで、深刻な被害が発生する前にインシデントを封じ込め、無力化することが可能です。

バラクーダについて

バラクーダネットワークスは、米国カリフォルニア州に本社を置き、あらゆる規模の企業に対し、複雑化する脅威から包括的に保護する最先端のサイバーセキュリティソリューションを提供しています。AIを搭載したサイバーセキュリティプラットフォーム「BarracudaONE」を中核に、一元管理型ダッシュボードなど革新的なソリューションを展開し、メール、データ、アプリケーション、ネットワークを強固に保護。最高水準のセキュリティとサイバー・レジリエンスを実現します。世界中の数十万にのぼるITプロフェッショナルやマネージドサービスプロバイダーから厚い信頼を獲得し、強力なセキュリティ機能を容易に導入・活用いただけるよう支援しています。

バラクーダネットワークスジャパンは、米国 Barracuda Networks Inc. の日本法人です。詳細については、barracuda.co.jpをご覧ください。

Vanson Bourneについて

Vanson Bourneは、テクノロジー分野の市場調査を専門とする独立系の市場調査専門会社です。Vanson Bourneの確かな評価と信頼性の高い調査分析は、厳格な調査手法に基づいており、あらゆる業界および主要な市場における技術部門およびビジネス部門の上級意思決定者の意見を的確に収集する能力に裏付けられています。詳細については、vansonbourne.comをご覧ください。