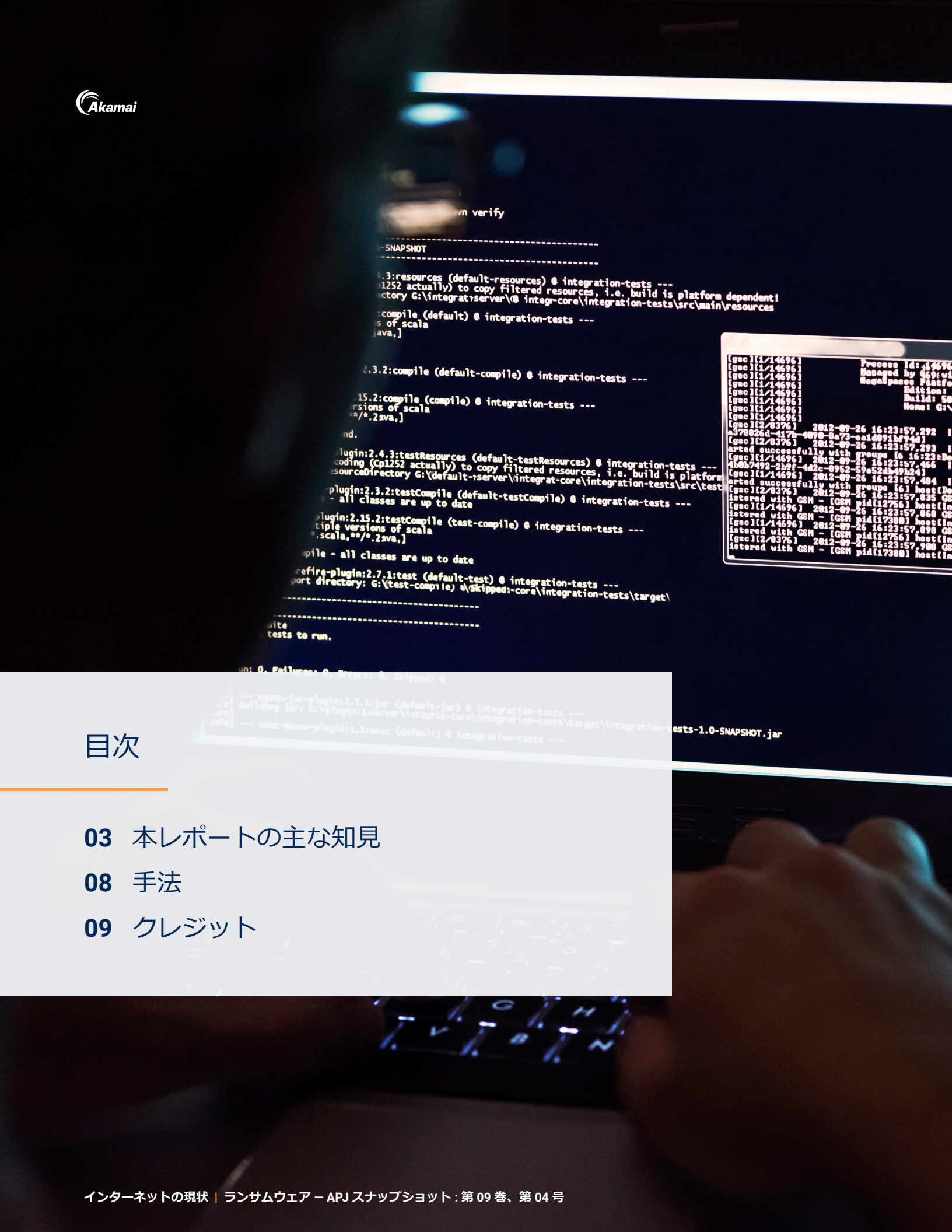
インターネットの現状
第 09 巻 | 第 04 号

猛威を振るうランサムウェア

APJ スナップショット



目次

本レポートの主な知見

このアジア太平洋・日本（APJ）地域版スナップショットは、ランサムウェアに関する包括的な SOTI レポート「猛威を振るうランサムウェア：進化する悪用手法と執拗なゼロデイの利用」（英語版のみ）に付随するレポートです。ランサムウェアグループの攻撃の傾向、手法、技法に関する詳細な分析、攻撃の段階に関する説明、組織を保護するための各段階に応じたソリューションと推奨事項、および調査手法については、SOTI レポート本体をご参照ください。

概要

ランサムウェアは、組織に大きな損害を与え続けており、被害企業は増える一方です。攻撃者は絶えず進化し、攻撃手法を変化させ、新たな手口を導入し、拡大するアタックサーフェスを悪用し、セキュリティ予算の制約を逆手に取っている状況です。こうした危険な傾向の影響は、ランサムウェアグループが注目を集め、大きな成功を収めていることからも読み取れます。それを裏付けるように、APJ 地域では、被害を受けた企業の数が 2021 年第 4 四半期から 2022 年第 4 四半期の間に 50% 増加しています。また、2022 年第 1 四半期と 2023 年第 1 四半期を比較した場合、被害企業数は前年比 204% と大幅に増加しています。

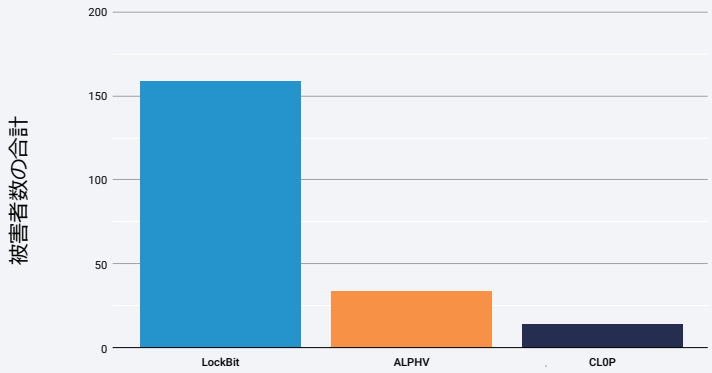
この APJ スナップショットでは、拡大するこの懸念に対する効果的な防御方法とリスク管理のために、以下のようにさらなる知見を共有します。

- 2021 年 10 月から 2023 年 5 月の期間は、LockBit がランサムウェアシーンを席巻し、CL0P が台頭して脆弱性を積極的に悪用しました。フィッシングからゼロデイ脆弱性やワンデイ脆弱性の悪用へと攻撃手法が変化した結果、被害企業数は大幅に増加しました。
- 全世界で一致している傾向として、被害を受けた組織が最も多い業種は製造業であり、ビジネスサービス業がそれに続いています。
- ランサムウェア被害者の大半は、収益が 5,000 万米ドル以下の小規模な組織でした。ただし、最大規模の組織も攻撃を受けています。

LockBit がランサムウェアグループの活動の多数を占める

ランサムウェアの認知度が高まり、この脅威に対処するためのツールやベストプラクティスが豊富に存在するにもかかわらず、APJ　で被害を受けた企業の数は 2021 年第 4 四半期から 2022 年第 4 四半期の間に 50% 増加しました。また、2022 年第 1 四半期と 2023 年第 1 四半期を比較した場合、被害企業数は前年比 204% と大幅に増加しています。弊社のグローバルレポートに記載されている調査結果データと同様に、2021 年 10 月 1 日から 2023 年 5 月 31 日までの期間に、LockBit　は　APJ　において被害企業に対する攻撃の大部分（51%）を占め、ALPHV と CL0P と共にトップ 3 に名を連ねています（APJ 図 1）。

APJ：被害者数別ランサムウェアグループ上位 3
2021 年 10 月 1 日 – 2023 年 5 月 31 日

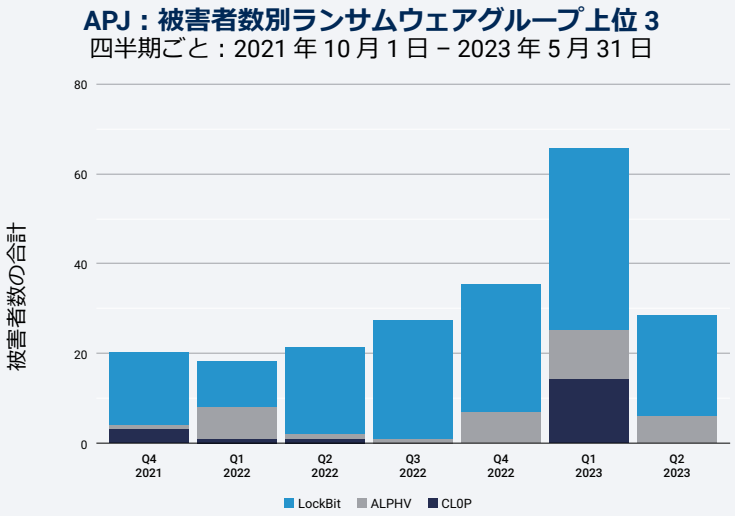


APJ 図 1：APJ で発生したランサムウェア攻撃の被害組織の大部分は、LockBit、ALPHV、CL0P による攻撃を受けている

四半期分析

LockBit が流行している一方で、CL0P ランサムウェアは 2021 年第 4 四半期から 2022 年第 2 四半期まで非常に活発で、2023 年第 1 四半期に急増しています。現在は APJ で最も活発なランサムウェアグループの第 3 位に上昇し、2 位の ALPHV に迫る勢いです（APJ 図 2）。CL0P の活動の急増は、さまざまなゼロデイ脆弱性を侵入経路として悪用していることに起因すると考えられます。過去 6 か月間で、フィッシングから脆弱性の悪用へと攻撃手法が変化した結果、被害企業数が大幅に増加しました。とはいえ、このレポートの時点では 2023 年第 2 四半期 * のデータは部分的にしか得られず、2023 年 5 月 31 日時点で CL0P の攻撃は記録されていませんでした。これは、2023 年第 1 四半期が異常であったことを示している可能性があります。しかし、2023 年 6 月に MOVEit の脆弱性が悪用された結果、CL0P の被害企業が増えており、APJ の多数の企業がその中に含まれていることに注意しなければなりません。

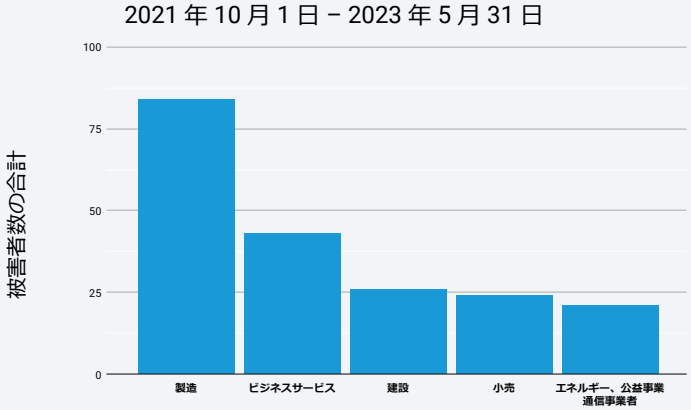
*** 2023 年第 2 四半期は 2023 年 5 月 31 日で中断されているため、完全な四半期データではありません。**



APJ 図 2：APJ におけるランサムウェアグループのトップ 3（LockBit、ALPHV、CL0P）の被害者数の四半期ごとの比較

リスクにさらされている重要な業界

APJ においてランサムウェアのリスクにさらされている重要な業界の上位 5 つは、製造、ビジネスサービス、建設、小売、エネルギーです（APJ 図 3）。世界的には教育業界が第 5 位に位置していることを除いて、これは全世界の一般的な傾向と合致しています。また、製造とビジネスサービスが上位 2 位に位置しているという点で、昨年のランサムウェアに関するグローバルレポートと概ね一致しています。当時、これらの業界は Conti ランサムウェアの被害を受けていました。Conti が消えると、LockBit がその後釜となりました。また、以前の DNS レポート「攻撃の「高速道路」：悪性 DNS トラフィックに関する詳細な分析」でも取り上げられている、多大な影響を受けた業界との重複が見られ、悪性のコマンド & コントロール（C2）トラフィックとランサムウェア攻撃との間につながりがあることがうかがえます。



APJ 図 3：APJ においてランサムウェア攻撃の被害組織数が最も多い業界は製造業

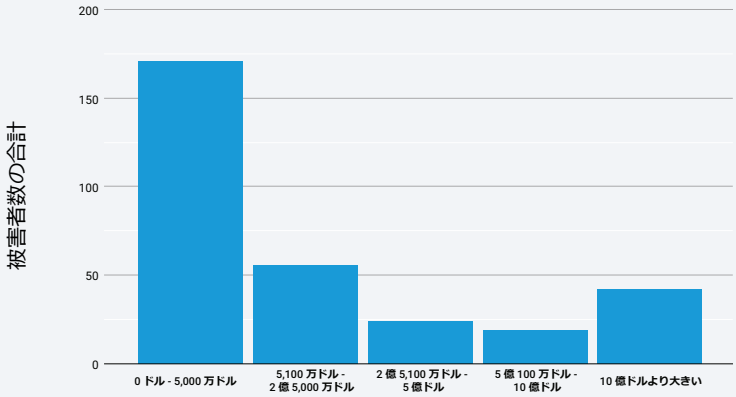
*** 2023 年第 2 四半期は 2023 年 5 月 31 日で中断されているため、完全な四半期データではありません。**

また、LockBit が業界の選り好みをしないことにも注意が必要です。APJ において LockBit は各業界で最も広く流行しているランサムウェアであり、製造業では攻撃の　60%、ビジネスサービスでは　55.8%、建設業では　57.7%、小売業では 45.8% を占めています。エネルギー業界では LockBit による攻撃の割合は 28.6% ですが、他の攻撃はいくつかの異なるランサムウェアグループに分散されており、14.3% を超えるグループは存在しません。

ランサムウェアグループは ROI を重視

企業規模や収益に関係なく、すべての組織がランサムウェア攻撃のリスクにさらされています。しかし、世界的な傾向と同様、APJ では攻撃者が小規模な組織に対して攻撃を成功させていることが、データで示されています（APJ 図 4）。シンガポール・サイバーセキュリティ庁のレポートよると、シンガポールで報告されたランサムウェア被害企業の大部分は製造業と小売業の中小企業でした。Akamai の推測では、小規模企業はランサムウェアの危険に対抗するためのセキュリティリソースが限られているため、攻撃に対して脆弱で侵入されやすい一方で、身代金を支払う余地があるのです。ただ、最大規模のエンタープライズも攻撃を受けており、被害組織の収益が多いほど身代金の支払額も多いことが、調査で明らかになっています。

APJ：ランサムウェアグループによる収益規模別の被害者数
2021 年 10 月 1 日 – 2023 年 5 月 31 日



APJ 図 4：APJ におけるランサムウェア被害組織の大半は、報告収益が 5,000 万米ドル以下の組織

> 企業規模や収益に関係なく、すべての組織がランサムウェア攻撃のリスクにさらされています。

APJ スナップショットの結論

ランサムウェアは、組織に大きな損害を与え続けています。世界的にも地域的にも、各国政府が共同戦線を形成して脅威に対処し、セキュリティ担当者による組織の保護を後押しする手法を明らかにしています。オーストラリア、インド、日本の外務大臣と米国の国務長官が発表した声明は、ランサムウェアが国家安全保障やすべての業界に与える影響を緩和することが急務であると示す良い例であり、組織のサイバーセキュリティ能力の強化と耐障害性の確保を支援するプログラムの構築に向けた取り組みを強化するものです。今年初めに、オーストラリアが代表を務める国際的な反ランサムウェア・タスク・フォース（International Counter Ransomware Task Force）が設立され、36 の加盟国と EU による連合の協力体制を強化し、サイバー脅威インテリジェンスの共有など、ランサムウェアの拡散と影響に対抗することとなりました。2022 年 10 月、シンガポールは、増え続けるランサムウェア攻撃から企業と重要インフラを守るために、複数の政府機関で構成される初の省庁間タスクフォースを創設しました。

規制当局が、サイバーセキュリティ基準を強化するためのイニシアチブとポリシーを打ち出す中、自社の領域における報告要件を把握して、プレイブックや危機管理計画にその要件を取り入れられるようにすることと、多層防御によってリスクを緩和できる可能性があることを認識することが重要です。

詳しくは、ランサムウェアに関するグローバルな SOTI レポート「猛威を振るうランサムウェア：進化する悪用手法と執拗なゼロデイの利用」をご覧ください。

手法

ランサムウェアデータ

このレポートで使用しているランサムウェアのデータは、約 90 のさまざまなランサムウェアグループのリークサイトから収集したものです。一般に、こうしたグループは、タイムスタンプ、被害者名、被害者のドメインなど、自らの攻撃の詳細を公表しています。注意が必要なのは、こうした公表は、ランサムウェアグループが自らの犯行を世に示したいという欲求の現れだということです。報告されているこうした攻撃の成否は、この調査の対象ではありません。

代わりに、この調査では、報告された被害者に焦点を当てています。それぞれの解析では、各グループ内で固有の被害者数を測定しました。この被害者データを ZoomInfo から取得したデータと照合することで、各被害者の所在地、収益規模、業種などの詳細を明らかにしています。

すべてのデータは、2021 年 10 月 1 日から 2023 年 5 月 31 日までの 20 か月間に収集されたものです。

クレジット

共同執筆者

Ori David
Badette Tribbey
Charlotte Pelliccia
Lance Rhodes

校閲およびテーマ別寄稿者

Moshe Cohen
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

データ分析

Chelsea Tuttle

マーケティング・出版

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

その他の「インターネットの現状／セキュリティ」レポート

高い評価を受けている Akamai の「インターネットの現状／セキュリティ」レポートのバックナンバーおよび今後のリリースについては、**akamai.com/soti をご覧ください。**

その他の Akamai の脅威リサーチ

以下のリンクから、最新の脅威インテリジェンス分析、セキュリティレポート、サイバーセキュリティリサーチをご確認いただけます。常に最新情報を把握するためにお役立てください：**akamai.com/security-research**

このレポートに掲載されている Akamai データ

このレポートに引用されているグラフや図のハイクオリティ版を以下のリンクからご覧いただけます。これらの画像は、出典元として Akamai を明記し、Akamai のロゴをそのまま残すことを条件に、利用および引用が可能です。**akamai.com/sotidata**

Akamai ソリューションの詳細

Akamai のランサムウェア向けソリューションの詳細については、**セキュリティソリューション**のページをご覧ください。

Akamai はオンラインライフの力となり、守っています。世界中の先進企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、世界中の人々の生活、仕事、娯楽をサポートしています。超分散型のエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 8 月。