

# 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





## 目次

- 02 ゼロデイ悪用への危険なシフト
- 04 ランサムウェア脅威の中心となる LockBit
- 13 ランサムウェア技術の大きな変化が更なる被害を生む
- 20 ランサムウェアの標的は引き続き重要な業界
- 26 収益別の分析：収益規模の小さな組織はランサムウェアのリスクが高くなる
- 28 ランサムウェア：APJ スナップショット
- 32 ランサムウェア：EMEA スナップショット
- 36 ソリューションと推奨される対策
- 42 結論
- 43 調査手法



## ゼロデイ悪用への危険なシフト

ランサムウェアをめぐる状況は進化を続け、攻撃者は被害組織が防御を強化するよりも速いスピードでその手口を巧妙化させています。現在、ランサムウェアグループは、フィッシングから脆弱性を悪用した攻撃へと、その軸足を移しつつあります。脆弱性を悪用した攻撃はその範囲を拡大するとともに、ますます巧妙さを増しています。これについて Akamai では「[セキュリティギャップのすり抜け](#)」で詳しく調査を行いました。さらに、ランサムウェアグループは、ゼロデイ攻撃を組織内で開発したり、バグ・バウンティ・プログラムを活用するなどして、ますます攻撃的な手口で脅迫や脆弱性の悪用を行うようになっています。ランサムウェアグループは、金銭的なコストをかけてでも積極的に経済的利益の獲得を目指しています。たとえば、他のハッカーに依頼してソフトウェアの脆弱性を発見してもらったり、イニシャル・アクセス・ブローカー（IAB）を通して標的へのアクセス権を獲得したりするために、対価を支払っています。

データをさらに詳しく検証すると、危険な傾向が明らかになり、2022 年の大規模攻撃の多発が再現される兆候があります。この傾向は、さまざまな業界で被害件数が増加していることから読み取れます。モノのインターネット（IoT）デバイスが増加している業界、特に製造業でランサムウェアの被害件数が増加しています。一方で、ヘルスケアなど、被害件数が比較的少ない業界でも大きな影響が出ており、ランサムウェア攻撃が成功すると、その被害は深刻になります。攻撃者は、収益性の高い経路を生み出す戦術についても方向性を変化させています。これまでは暗号化を通して脅迫を行う戦術でしたが、データを窃取し、バックアップを行っている組織に対しても優位に立つ戦術に移行することで、大きな成功を収めるようになっています。さらに、攻撃者は、被害組織の顧客やパートナーに電子メールを送り付けたり、電話をかけたりするなど、複数の脅迫の手口を用いるようになっています。事実、ランサムウェアは、ファイルやシステムを人質に取るだけに留まらない、サイバー犯罪を請け負う企業にまで発展しました。

私たちは、この「インターネットの現状」（SOTI）レポートでランサムウェアの現状をまとめ、ランサムウェアグループが初期アクセスからデータ流出までを達成するために利用している最新の攻撃テクニックやツールを明らかにしています。さらに、防御テクニックや推奨される対策をまとめた広範なリストも掲載しています。業界も個人も、ランサムウェア攻撃の新たな波から自身を守ることが重要です。このレポートでは、拡大するこの懸念の効果的な防御とリスク管理に役立つ知見を紹介します。

ランサムウェアグループは、ますます攻撃的な手口で脅迫や脆弱性の悪用を行うようになっています。

## 本レポートの主な知見

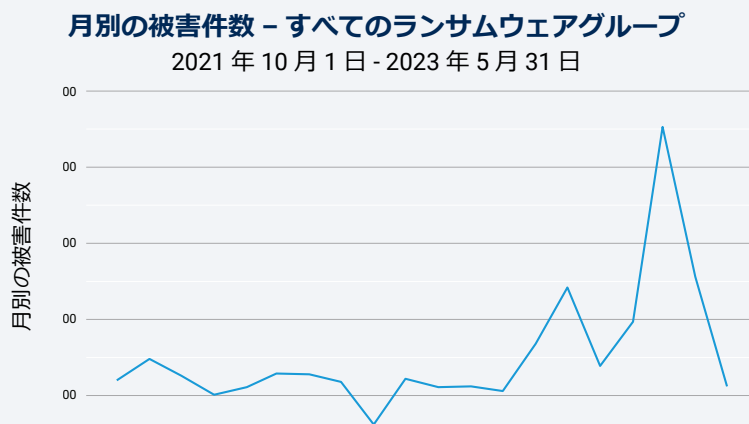
- ・ランサムウェアの脅威に用いられる戦術に、懸念すべき変化が見られます。過去 6 か月間でゼロデイおよびワンデイの脆弱性を狙った攻撃が猛威を振るっており、2022 年第 1 四半期から 2023 年第 1 四半期までの間に被害件数が 143% 増加しています。
- ・ランサムウェアグループは、ファイルの流出を目的とし、流出したファイルを主な脅迫材料として使用しています。最近の GoAnywhere や MOVEit の悪用ケースでも見られる傾向です。これは、ファイルの暗号化には有効なファイル・バックアップ・ソリューションが戦略としてはもはや不十分という事実を裏付けるものです。
- ・同じ被害組織が異なるランサムウェアグループから 2 度目の攻撃を受けるケースが見られます。Akamai の調査によると、複数のランサムウェアグループの被害を受けた組織では、最初の攻撃から 3 か月以内に後続の攻撃を受ける確率が 6 倍近くに上がることが判明しています。別のグループに攻撃される可能性があるため、組織は速やかに環境のギャップを埋めようと試みます。
- ・CL0P などのランサムウェアグループは、組織内でゼロデイ脆弱性を見つけ出し、その脆弱性を悪用するプログラムを開発すべく積極的に取り組んでいます。この戦略は実際に成功を収めており、CL0P による被害件数は 2022 年第 1 四半期から 2023 年第 1 四半期にかけて 9 倍増加しました。
- ・LockBit は、ランサムウェアによる被害件数全体の 39% (1,091 件) という多数を占めており、その件数は 2 位のランサムウェアグループの 4 倍以上に相当します。これまで主流だったランサムウェア Conti の活動が停止した隙を狙って、2022 年第 4 四半期から 2023 年第 1 四半期まで 92% 増と被害件数を伸ばしています。
- ・特定の業界への攻撃も同様に増加しています。製造業の被害件数は 2021 年第 4 四半期から 2022 年第 4 四半期の間に 42% 増加し、ヘルスケア業界の被害件数は同期間で 39% 増加しました。
- ・分析から 2 つの傾向が明らかになっています。1 つ目は、グループの規模やリソースなどの可変要素によりますが、ランサムウェアグループが継続的に活動していること。2 つ目は、CL0P による非常に的を絞ったセキュリティ欠陥の積極的な悪用のような、重大なゼロデイ脆弱性を悪用する活動が大幅に増加していることです。
- ・米国財務省の外国資産管理局 (OFAC) による規制により、特定の団体または



個人に対する身代金の支払いが違法となる可能性があります。ランサムウェア攻撃やデータ窃取のさまざまな影響を軽く捉えている組織は、身代金の要求に応じざるを得ないが、しかし身代金の支払いは OFAC の規則に違反してしまうという難しい判断を迫られる危険性があります。そのため、自社ネットワークに対する攻撃の試みを阻止するためのセキュリティコントロールやプレイブックのニーズがさらに高まっています。

## ランサムウェア脅威の中心となる LockBit

ランサムウェアなどの金銭目当ての脅威は、こうした脅威をもたらすリスクが広く認知されているにもかかわらず、組織に大きな損害を与え続けています。それを裏付けるように、被害件数は 2021 年第 4 四半期から 2022 年第 4 四半期の間に確実に増加しています (36% 増、図 1)。また、2022 年第 1 四半期と 2023 年第 1 四半期を比較した場合、被害件数は前年比 143% と大幅に増加しています。これはここ数か月、ゼロデイ脆弱性を狙った攻撃が猛威を振るっているからです。ランサムウェアの被害が急増している背景には、ビジネス運営の裏事情、ダーク Web における aaS (as-a-service) の提供 (例えば、IAB を介して売り出される企業ネットワークへの容易なアクセス)、Log4Shell や ProxyLogon、さらに最近の MOVEit のような Web アプリケーションの脆弱性に起因する [Web 攻撃が 2.5 倍増加したこと](#)など、さまざまな要因が重なり合っています。攻撃者が使用するテクニックも進化しています。ランサムウェア攻撃は構造が複雑で、複数の攻撃ベクトルが使用されるため、被害組織にとって防御しにくい手口と言えます。このセクションでは、2021 年 10 月から 2023 年 5 月までの 20 か月間のランサムウェアの世界的な傾向と影響を明らかにします。





また、公開済みのリークサイトのデータを詳しく検証し、主流となっているランサムウェア攻撃者を解明します（図 2）。Conti の消滅後は、LockBit が首位の座を占め、最も攻撃件数の多いアクティブなグループの 1 つになっており、攻撃者が公開しているリークサイトの情報によると、最多の被害件数を記録しています。データを分析した結果、[LockBit](#) は被害組織の 39%（被害件数 1,091 件）を占め、2 位につける ALPHV ランサムウェアの 4 倍以上の件数となっています。LockBit の拡大する活動と増加する被害を受けて、法執行機関やセキュリティ担当者は LockBit に対する警戒を強めています。あらゆる監視の目が LockBit に向けられていますが、LockBit が Conti と同じ道をたどることになるかは現時点では不明です。Conti は活動を停止しましたが、名称を変えて小規模なランサムウェアグループへと分化しています。

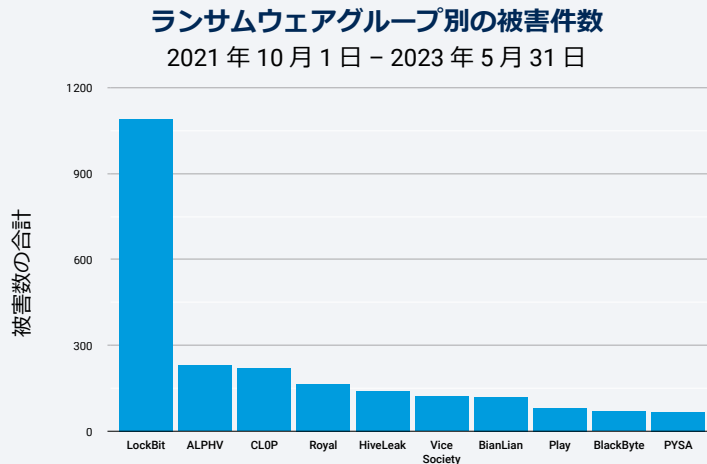


図 2：ランサムウェア攻撃の被害組織の大部分は LockBit による攻撃を受けており、ALPHV と CL0P がそれに続いている

LockBit が継続的に成功している理由は、その強化にあります。最新の 3.0 バージョンでは[新たなテクニック](#)を導入し、バグ・バウンティ・プログラム（あらゆるセキュリティ研究者、倫理的なハッカー、非倫理的なハッカーに自社ソフトウェアのバグレポートの提出を求め、その見返りとして 1,000 ドル～ 100 万ドルの報奨金を設定する、図 3）の実施や Zcash 暗号資産（仮想通貨）を支払いモードとして使用するなど、その脅威をさらに拡大しています。バグ・バウンティ・プログラムの使用目的は主に防御ですが、LockBit が利用できる脆弱性や新たな道筋を開拓することも狙いなのかどうかは定かではありません。





図 3 : LockBit のバグ・バウンティ・プログラムはハッカーにソフトウェアの欠陥を自ら開示するように促す仕組みである (出典 : Bleeping Computer)

さらに、標的となる組織に攻撃を展開するハッカーのアフィリエイトは、[身代金の支払い額の最大 75%](#) を獲得できます。被害組織をさらに追い詰めるために、LockBit に属する攻撃者は、被害組織の顧客にも影響を及ぼし始めました。顧客にインシデントについて開示し、[分散型サービス妨害 \(DDoS\) 攻撃](#)を含む、3 重の脅迫戦術を用いています。LockBit の全世界へのまん延を阻止するために、Cybersecurity and Infrastructure Security Agency (CISA) と国際的なパートナー／同等組織は、組織を防御するセキュリティ担当者のために LockBit のテクニックを解説した[サイバーセキュリティアドバイザリー](#)を公開しました。

ALPHV (別名 [BlackCat](#)) は、LockBit に続く第 2 位の被害件数となっています。このランサムウェアの特徴は、Rust プログラミング言語を使用することで、Windows システムと Linux システムの両方に感染するという点です。[Microsoft Exchange サーバーの複数の脆弱性](#) (その中の [CVE-2021-34473](#) は CVSS スコア 10) が標的に侵入するために悪用されました。昨年のある ALPHV 攻撃では、攻撃者は[新たな脅迫手法](#)として、被害組織の Web サイトを複製し (タイポスクワッシングしたドメインを使用)、盗取したファイルを自分の Web サイトでリークするだけでなく、その複製サイトで公開して、標的に身代金の支払いを迫りました。アフィリエイトは利益の最大 90% を獲得し、他のグループや新たなアフィリエイトへのアピールに成功しました。



さらに、標的となる組織に攻撃を展開するハッカーのアフィリエイトは、身代金の支払い額の最大 75% を獲得できます。



CL0P は ALPHV に肉薄しており、被害件数は第 3 位となっています。CL0P は、マネージド型ファイル転送プラットフォームの複数のゼロデイ脆弱性を悪用する既知のランサムウェアファミリーです。被害例としては、2021 年に[サービスを終了した](#)レガシーファイル転送アプライアンス（[石油会社](#)の攻撃に使用）、2023 年 1 月の GoAnywhere MFT のセキュリティの欠陥（CVE-2023-0669）、2023 年 4 月の PaperCut 脆弱性（CVE-2023-27350 および CVE-2023-27351）、直近では [MOVEit Transfer のゼロデイ脆弱性](#)（CVE-2023-34362。多数の会社からのデータ盗難に発展）があります。MOVEit の脆弱なバージョンを使用している 2,500 以上のインターネット接続サーバーに、このセキュリティ欠陥のリスクがあります。CL0P は、被害件数は比較的小さいものの、新しいゼロデイ脆弱性を悪用した攻撃が発生すると、アクティビティが急増するのは注目すべき点です。LockBit とは異なり、CL0P の攻撃には一貫性やパターンがなく、次に発生する大規模ゼロデイ脆弱性によって攻撃が変わるため、予測が困難です。このグループは攻撃前に探知されないように努めていると推測できます。データを見ると、その効率の良さがわかります。CL0P は、より収益レベルの高いカテゴリーの組織に確実に被害を与えているランサムウェア攻撃の 1 つと言えます（詳しくは、[「収益別の分析」セクション](#)を参照）。他のランサムウェアグループが CL0P の戦略を模倣するかどうかは現時点ではわかりません。

Royal ランサムウェアが発生した時期は定かではありませんが、Royal の運営者は Conti ランサムウェアを展開していた Conti Team One のメンバーとのつながりや関連性があると言われています。Royal ランサムウェアは Zeon ランサムウェアをリブランドした可能性があります。他のランサムウェア運営者とは異なり、Royal には[アフィリエイトプログラムが存在せず](#)、IAB を介してネットワークへのアクセスを購入するのが通例です。身代金の要求額は 25 万ドル～200 万ドルであり、侵入ポイントとしてリモート・デスクトップ・プロトコル（RDP）マルウェアをコールバックフィッシング経由で拡散します。



CL0P の攻撃は、次に発生する大規模ゼロデイ脆弱性によって攻撃が変わるため、予測が困難です。





## 月別の傾向で明らかになるキャンペーンと被害件数のベースライン

Akamai Research がランサムウェア活動の増減状況を観測したところ、横ばいの状態と急増減を繰り返していることを確認しました（図 4）。既知の全ランサムウェアグループによる四半期ごとの合計被害件数のスナップショットを見ると、活発に活動していないグループや解散したグループが存在したり、一部は法執行機関による摘発で運営を停止しているにもかかわらず、被害件数の増加傾向を確認できます。

月別の被害件数 – LockBit、ALPHV、Royal、CL0P、HiveLeak  
2021 年 10 月 1 日 - 2023 年 5 月 31 日

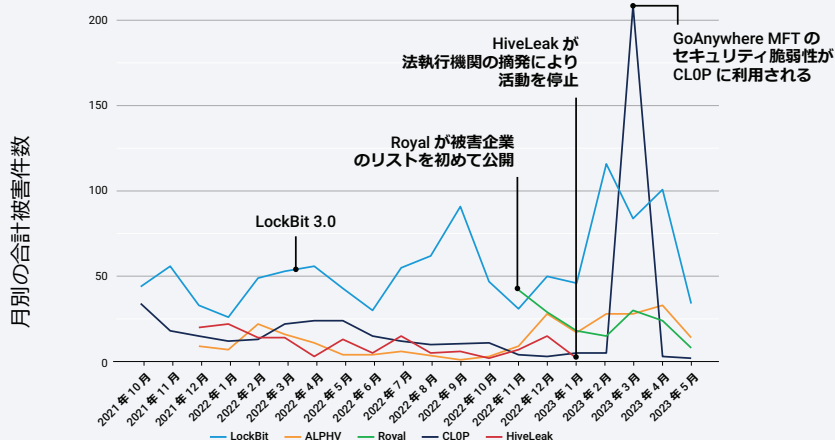


図 4：主なランサムウェアグループによる月別のランサムウェア被害件数の比較

ほとんどのランサムウェアの脅威には活動のベースラインがあります。使用するキャンペーン、新たな戦術の導入、アフィリエイトプログラムなど、さまざまな要素に基づいてその規模は変化しますが、グループ活動の分析から 2 つの傾向が見られます。1 つ目の傾向は、グループの規模（アフィリエイトの数）やリソースなどの可変要素によりますが、ランサムウェアグループが継続的に活動していることです。LockBit は月に約 50 件の被害件数を一貫して記録していますが、他のランサムウェアグループはそれより少ない件数にとどまります。ALPHV は、当初は控えめな活動でしたが、2021 年から 2022 年にかけて何度か急増しています。



Akamai Research は、ランサムウェア活動の増減状況を観測し、大幅な増加が見られることを確認しました。



2 つ目の傾向は、一部のグループが重大なゼロデイ脆弱性を悪用した場合に大幅な増加が見られるという点です。特に CL0P では、高度な標的型のセキュリティの欠陥を積極的に取り込む手口を観測しています。2021 年 10 月から 2023 年 2 月にかけて、CL0P の被害件数は月に 35 件未満でしたが、2023 年 3 月に突如として増加しています。これは複数の大手組織に影響を及ぼした、Fortra の GoAnywhere ソフトウェアに対するグループの[ゼロデイ攻撃](#)に関連している可能性があります。2023 年 5 月、[CL0P は SQL インジェクション \(SQLi\) の脆弱性 \(MOVEit Transfer 内\)](#) を悪用しました (CVE-2023-34362)。さらに、もう 1 つの活発な活動も確認しています。

一方、HiveLeak (米国の複数のヘルスケア組織を攻撃した結果、紙のカルテへの逆戻りが発生し、緊急手術がキャンセルになったことで知られる) は、2022 年第 4 四半期もランサムウェアグループの上位に入っています。2023 年 1 月には、[米国とドイツの法執行機関](#)などが連携して Hive のサーバーを差し押さえ、被害組織からの 1 億 3,000 万ドルもの脅迫金の支払いを未然に防いだことで、トップ 10 から陥落しました。

## 四半期ごとの分析によると、上位のランサムウェアグループに大きな変動が見られる

2022 年第 4 四半期と 2023 年第 1 四半期を詳しく比較してみると、起こりうるパターンだけでなく、ランサムウェアの傾向における異常値も明らかになりました。また、ほとんどのランサムウェアの脅威で今年初めに活動の増加が見られ、被害件数が著しく増加しています。一方 ALPHV や Royal は、上位 4 位以内を維持しています。2023 年第 1 四半期は、異常値を記録しました。このレポートで観測した他の四半期のベースラインより被害件数が多くなっています。

LockBit の被害件数は、この四半期分 (2022 年第 4 四半期から 2023 年第 1 四半期) だけで 92% 増加し、この脅威が一貫して上位を占めていることを物語ります。CL0P の 2023 年第 1 四半期における 10 位から 2 位への躍進 (図 5、1,642% の増加) は注目に値します。特定のプラットフォームで複数のゼロデイ脆弱性を利用した結果であり、標的を効果的に侵害するための新たな手口が加わったことを示唆しています。ランサムウェアのリスクが高まったことで、組織はセキュリティ対策を強化したり、セキュリティコントロールの有効性をチェックしたりして、ランサムウェア攻撃がもたらす危険を緩和することを余儀なくされています。さらに、タイムリーなパッチ適用も、境界のギャップを埋めるために非常に重要です。







### 被害件数別ランサムウェアグループ上位 10 2022 年 Q4 と 2023 年 Q1 の比較

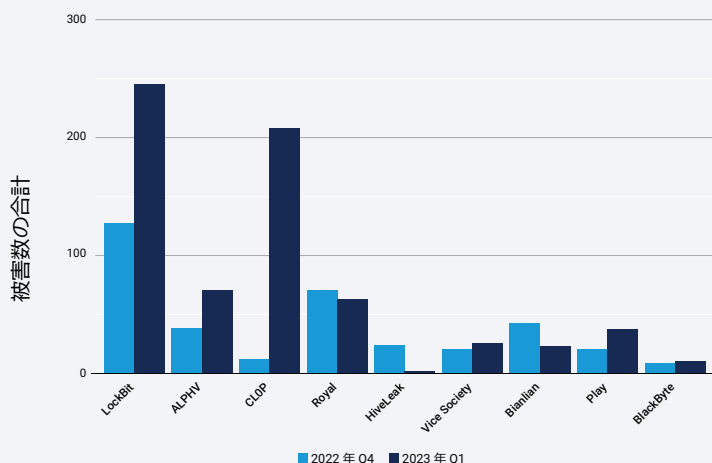


図 5 : CL0P の急増は、さまざまなゼロデイ脆弱性を侵入経路として悪用していることに起因すると考えられる

ランサムウェアごとの被害件数の分析は、リークサイトで公開された数字に基づく全体的な被害件数の内訳であり、身代金要求を支払わなかった被害組織しか把握できませんが、ランサムウェアのまん延度を垣間見る材料にはなります。ランサムウェア攻撃の影響は、金銭的な損失にとどまりません。国家の経済に欠かせない重要なインフラや他の業界への影響も生じます。高まるランサムウェア攻撃のリスクに対抗するために多くの国や地域が採用している対策の 1 つが、組織を監視するための規制です。

```
...chan); case status := <- workerCompleteChan: worl
...m()); count, err := strconv.ParseInt(r.FormValu
...log(r.FormValue("target")), count); }); http
... { fmt.Fprintf(w, "INACTIVE"); }; return; c
...); func main() { controlChannel := r
...workerActive; case msg := <-controlChan
...r *http.Request) { host
...fmt.Fprintf(w, "Control message
..."); select { case result := <
... "strings"; "time" ); typ
...}; for { select { cas
...chan chan chan
...ControlMessage(T
...when bool); statu
...);package
...chan boo
...wo
```



## 組織は 3 か月以内に 2 回目の攻撃を受けるリスクが高くなっている

「雷は同じ場所に二度と落ちない」ということわざは、ランサムウェア攻撃には必ずしも当てはまりません。Akamai の調査によると、複数のランサムウェアグループの攻撃を受けた組織では、最初の攻撃から 3 か月以内に後続の攻撃を受ける確率が、それ以降の期間よりも 6 倍近く高くなることが判明しています。つまり、組織にとって危険な最初のランサムウェア攻撃を防いで緩和することがあらためて重要になります。最初の攻撃を受けた組織は対応に追われ、混乱します。標的となる候補を探しつつ、競合グループの活動を監視している別のランサムウェアグループも、この混乱のタイミングを利用して同じ組織に攻撃を仕掛けようとします。たとえば、Royal は、Hive による最初の攻撃が発生し、[そのデータ漏えいが報じられた](#)約 4 か月後に同じ組織を攻撃しました。CL0P による最初の攻撃にも、RansomHouse と Abyss という 2 つの別のグループが追隨しています。このように、あるグループが最初に攻撃を仕掛けると、別の攻撃者がその混乱に乗じて同じ組織を攻撃するという構図が明らかになります。場合によっては、同じグループが最初の攻撃から 12 か月以内またはさらに長い間隔をおいて同じ組織を攻撃することもあります。こうしたケースでは、標的となる組織は、バックドアやツールなどの経路を問わず、ネットワークでのこうした脅威を完全に排除できていなかったと考えられます。たとえば、LockBit は、2021 年にある不動産会社を初めて攻撃し、2023 年に 2 回目の攻撃を仕掛けています。

このように連続したランサムウェア攻撃が壊滅的な打撃を与え、システムの修復に[復旧時間](#)が必要になることは容易に想像できます。残念ながら、最初の攻撃を受けて身代金を支払ったとしても、組織の安全は保証されません。同じ組織から再び攻撃を受けるか、運が悪ければ複数のグループから攻撃を受ける可能性があります。被害組織が境界のギャップを埋められない場合、あるいは攻撃者が最初にネットワークに侵入する際に利用した脆弱性を修復できない場合は、そうした弱点が再び利用されます。さらに、組織が身代金要求に従ったとしても事態は改善しません。その後も同じグループや他のグループから攻撃対象と見なされる可能性があります。



「雷は同じ場所に二度と落ちない」ということわざは、ランサムウェア攻撃には必ずしも当てはまりません。



## 政府の政策はランサムウェアの状況を変えることができるか？

現在まん延している脅迫行為は、主に 3 つに分類できます。データの暗号化、窃取したデータを人質とした身代金要求、そして DDoS です。こうした攻撃への対策を検討する場合、重要なのは規制や法律の影響を考慮することです。考慮すべき点の 1 つ目は、身代金を支払うかどうかです。2022 年、フロリダ州はノースカロライナ州に続く 2 番目の州として、州および地方自治体が身代金の要求に従うことを禁止しました。さらに多くの州も同様の法律の導入を検討しています。連邦レベルでは、2023 年の国家サイバー戦略でランサムウェアに 28 回言及しており、オンライン犯罪インフラの撲滅とランサムウェアキャンペーンからの暗号通貨の差し押さえを CISA と FBI に指示しています。

米国財務省は、外国資産管理局（OFAC）と金融犯罪捜査網を通じて、特定の団体や個人に対する身代金の支払いを違法とする規制を適用しています。欧州連合（EU）も、基幹サービスに対して同様の立場をとっており、ネットワークおよび情報システム指令に従い、身代金の支払いに応じた EU 加盟諸国に対して罰金を課しています。さらに、[改正されたネットワークおよび情報システム指令](#)が正式に発効すると、ヘルスケア、エネルギー、デジタルサービス、電子通信サービス、郵便／宅配便サービスなど、多くの基幹セクターでサイバーセキュリティ基準が強化されます。

考慮すべき点の 2 つ目は、報告です。[2022 年の重要インフラ法によるサイバーインシデントの報告義務](#)では、ランサムウェアの攻撃（対象となるサイバーインシデント）を受けた対象組織は、そのサイバーインシデントを受けたと考えられる時点から 72 時間以内に担当当局に報告することを義務付けています。サイバーインシデントの報告を求める規制や契約の合意事項を確認し、その内容を危機管理計画に組み込むことが重要です。



米国財務省は、特定の団体や個人に対する身代金の支払いを違法とする規制を適用しています。





## ランサムウェア技術の大きな変化が更なる被害を生む

ランサムウェア攻撃を緩和するためには、ネットワークパーシステンスの施設への初期アクセスから、その後の暗号化とデータ盗取まで、攻撃チェーン全体で用いられているテクニックとツールを把握する必要があります。十分な試行を重ねた手口は信頼性が高いと言えますが、Akamai Research チームは戦術の変化と攻撃の複雑化を確認しています。増加する Web アプリケーションの脆弱性は攻撃に盛んに利用され、攻撃対象が広がっています。さらに、機微な情報が組み込まれているアプリケーションが新たな脅迫材料として利用されています。ゼロデイおよびワンデイ脆弱性も、特定のランサムウェアグループが多用する定番となっており、独自のプラットフォームやあまり一般的ではないソフトウェアのセキュリティの欠陥も悪用されています。

このセクションでは、現在上位を占めているランサムウェアグループの一部が使用している注目すべき戦術を紹介します。初期アクセスやコマンド & コントロール (C2)、ラテラルムーブメント (横方向の移動)、データ窃取など、さまざまな段階の攻撃で一般に使用されるテクニックを認識し、セキュリティコントロールでテストを実施するか、アドバイザリーシミュレーションを通じて対策を講じることで、セキュリティ担当者は攻撃者の 3 歩先を行くことができます。

攻撃者は攻撃を妨害する防御網を回避するためのテクニックを日々進化させています。これがランサムウェアの現状です。かつての攻撃チェーンは、攻撃ベクトルまたは侵入地点となるフィッシング攻撃が中心であり、ファイルの暗号化を目的としていました。



ランサムウェア攻撃を緩和するためには、攻撃チェーン全体で用いられているテクニックとツールを把握する必要があります。



システム侵害は、今や一連の攻撃段階のスタート地点にすぎません。そこから暗号化を経て、データ盗取に及び、場合によっては DDoS 攻撃まで発展します（図 6）。攻撃者は最大限の損害を与えながら、手順を最小限に抑え、最新化を図っています。そのために、多くの異なる脅迫戦術を駆使して、標的が身代金要求に従うように仕向けます。さらに、攻撃者は、標的組織のファイルを暗号化するだけでなく、データを盗取して脅迫することで、さらなる成功を収めています。

現在のほとんどのランサムウェア攻撃は、ネットワーク侵害からスタートします。脆弱なインターネット接続アセットを悪用するか、ソーシャルエンジニアリング戦術を使用して侵害したら、スキャナーを実行して追加のアセットを検出し、認証情報のダンプを通じてドメインでの権限昇格を果たします。最終的にその認証情報を使用して機微な情報を盗取し、ネットワーク全体にランサムウェアを拡散します。

Akamai の [2022 年上半期ランサムウェアレポート](#) では、攻撃テクニックのベースラインを詳しく解説しています。今年もこの進化が続いていますが、独自の傾向もいくつか確認しており、今後数か月あるいは数年間に起こりうる状況の手がかりを得ています。



攻撃者は、  
最大限の損害を与え  
ながら、手順の最小  
化・最新化を図って  
います。

## ランサムウェアの一般的なキルチェーン

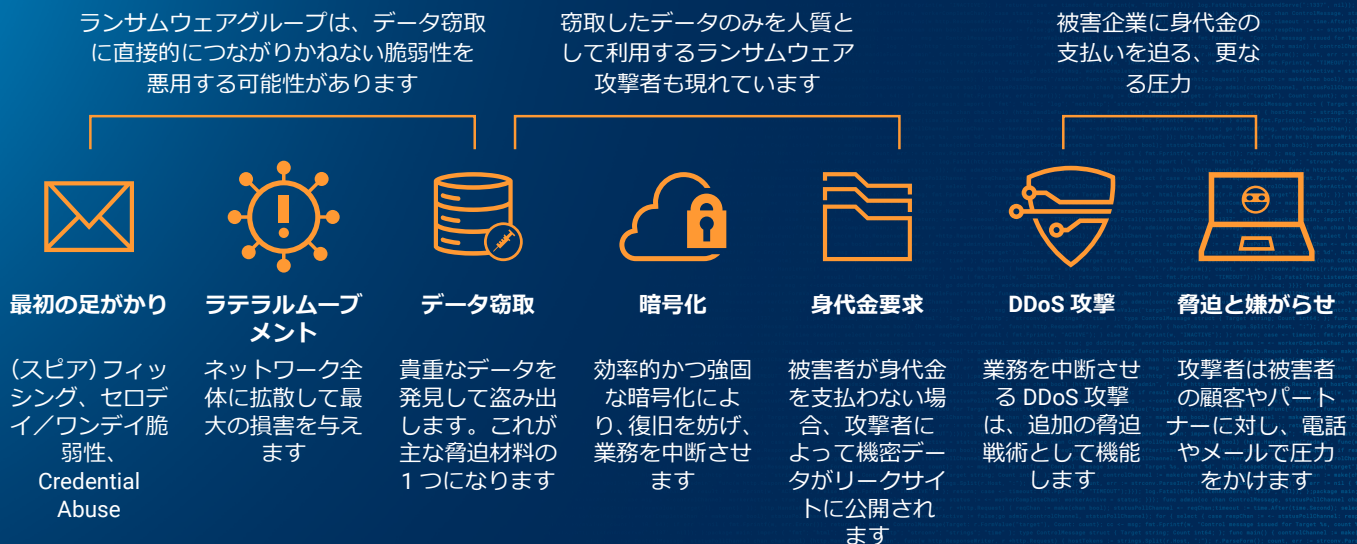


図 6：ランサムウェアのキルチェーンの概要（最新の脅迫戦術に関する情報を含む）



## 初期アクセス手法

### フィッシング

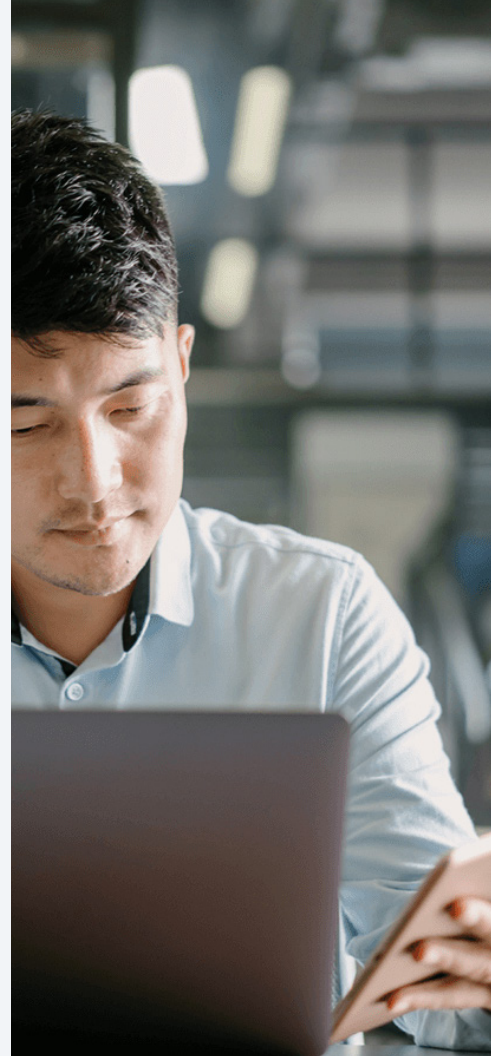
2023 年、攻撃者はフィッシングメールを送信する際の戦術を変更する必要がありました。ここ数年、攻撃者はマクロを含む Microsoft Office 添付ファイルを悪用し、ユーザーにダウンロードさせた悪性コードを実行していました。この手法があまりに多用されたため、Microsoft はポリシーを変更し、インターネットからダウンロードした [Office ファイルのすべてのマクロをブロック](#) するようになりました。

この変更により、攻撃者はマクロを見限り、標的を侵害する新たな手法を開拓することにしました。今年は、マルウェアを配信するためにさまざまな形式のファイルが多用されています。[ISO ファイル](#) は、一部のセキュリティ緩和対策を回避できるため、配信オプションとして多用されました。OneNote ドキュメントに悪性ファイルを埋め込む手法も、複数のマルウェアファミリーに広まっています。

さらに、LockBit アフィリエイトでフィッシングメールの使用が報告されました。このメールにより、[Amadey Bot](#) マルウェアをインストールし、デバイスを暗号化してコントロールを乗っ取ります。また、CL0P による攻撃者は、大量のスパイアフィッシングメールを従業員に送信し、組織への初期アクセスを獲得しています。コールバック型のソーシャル・エンジニアリング・フィッシング・キャンペーンも増加しています。さまざまな組織の従業員を標的とするキャンペーンであり、[BazarCall 攻撃](#)と呼ばれています。BazarCall 攻撃は、被害者を脅威グループのコールセンターへと導き、ソーシャルエンジニアリング戦術により、被害者にリモート画面共有セッションを開始するように仕向けます。そのセッション中に、攻撃者は被害者のマシンへの侵入ポイントを密かに確立します。検知機能が引き続き改善され、攻撃者が戦術を磨く中、このフィッシング手法の進化傾向は今後とも続くと考えられます。

### 脆弱性の開拓：ワンデイおよびゼロデイの悪用

ゼロデイおよび以前からある脆弱性は、次の大規模な攻撃ベクトルになります。同時に、ソフトウェアセキュリティの欠陥をネットワークへの初期アクセスポイントとして利用するランサムウェアグループの比率が高まっています。コード脆弱性がもたらす影響と、その脆弱性が標的を容易に攻略できる経路になることに気付いた攻撃者は、収益化のための戦術を見直しました。実際、攻撃者が初期アクセスを得るために使用する [最も一般的な手法](#) は、主にパッチ未適用システムのワンデイ脆弱性を介して、インターネット公開アプリを悪用することです。こうしたグループは、公開された脆弱性に速やかに適応し、ゼロデイを悪用します。そのため、時間との戦いとなります。組織は自社のソフトウェアやシステムに速やかにパッチを適用する必要があります。



攻撃者が初期アクセスを得るために使用する最も一般的な手法は、インターネット公開アプリを悪用することです。

Log4Shell (CVE-2021-44228) や ProxyLogon (CVE-2021-26855) など、以前から出回っている脆弱性も、ネットワークを侵害してランサムウェアを拡散するためにいまだに利用されています。その証拠に、LockBit は Log4Shell を使用して VMware インスタンスを攻撃しています。さらに、一部の被害組織は、既知の Microsoft Exchange Server の脆弱性を介して BlackByte にアクセスされたと報告しています。

今年の傾向として、攻撃者は任意のサーバーとエンドポイントを標的とする従来のランサムウェア攻撃から脱却し、標的組織の脅迫に利用できる機微な情報を含んだアプリの悪用に移行しています。主な例を以下に示します。

- [ESXiArgs](#) ランサムウェアキャンペーンは、VMWare ESXi サーバーのワンデイ脆弱性を悪用し、サーバーでホストされている仮想マシンにアクセスして暗号化することで、利用不可の状態にします。
- 特に、CL0P および BI00dy ランサムウェアでは、[PaperCut MF/NG 不正アクセスコントロール](#)の脆弱性を悪用していることを確認しました。この場合、非認証のリモート攻撃者は、任意のコードをデバイスで実行することで認証を回避できます。
- CL0P は、複数のマネージド型ファイル転送 (MFT) サーバーで、大量のゼロデイ脆弱性を標的にしています。2023 年 3 月の攻撃のすぐ後に、2023 年 5 月の MOVEit に対する攻撃が発生しています。いずれのケースも、脆弱性を利用して機微なファイルを盗取し、被害組織を脅迫しています。

ゼロデイ脆弱性の利用自体は特に目新しい手法ではありませんが、重要なのは、CL0P などのランサムウェアグループが脆弱性を積極的に探索または調査し、大規模に悪用して数百または数千もの組織を侵害していることです。CL0P がゼロデイを悪用してから被害件数が急激な増加したという事実は、そうしたテクニックが多額の資金を生むことを意味しており、この傾向は今後しばらく続くと考えられます。同様に、LockBit のバグ・バウンティ・プログラムは、攻撃者が既存のランサムウェアソフトウェアを強化する道筋になります。



時間との戦いとなります。組織は自社のソフトウェアやシステムに速やかにパッチを適用する必要があります。



## 認証情報の窃取

窃取した有効な認証情報でも、インターネット接続アプリや攻撃を受けたサービスを介して初期アクセスが可能です。これは、Vice Society や ALPHV といったグループの攻撃ベクトルとして観測されています。有効な認証情報は、ダーク Web ベンダーや、フィッシング、総当たり攻撃、またはパスワード類推を通じて入手するケースもあります。有効な認証情報を得た攻撃者は、VPN や RDP などの外部リモートサービスを利用してネットワークに侵入します。2022 年 11 月に、攻撃者は Fortinet VPN サーバーの脆弱性を利用して初期アクセスを獲得し、ネットワーク全体にランサムウェアを拡散しました。LockBit アフィリエイトの ALPHV および Vice Society は、攻撃に Credential Abuse を利用していると報告されています。

## ドライブバイ侵害

ドライブバイ侵害を通じて初期アクセスを獲得する攻撃者も存在します。これは、悪性サイトまたは侵害された正規サイトである Web サイトを閲覧しているユーザーを介して攻撃者がシステムアクセスを得るケースです。この場合、攻撃者はユーザーの Web ブラウザーを悪用するか、攻撃者に付与されたアプリケーション・アクセス・トークンを介してアクセスを獲得します。LockBit や REvil などのランサムウェアグループは、このテクニックを使用して標的となるシステムへの初期アクセスを獲得してきました。

## 他のサイバー犯罪グループとの連携：イニシャル・アクセス・ブローカー

攻撃で最も難しいのは、標的となるネットワークへの初期アクセスを得ることです。IAB は、この作業に特化した犯罪グループです。さまざまな戦術を駆使してネットワークを侵害し、獲得したアクセス情報を最高額落札者に売却します。こうしたグループは、フィッシングやワンデイ脆弱性などの一般的な手法を用いてネットワークへの足がかりを確保します。その後、情報を収集してその組織ネットワークの規模と収益を明らかにし、それに応じてアクセス情報の価格を設定します。現代のランサムウェアグループは、ネットワークへの初期アクセスも含めて、攻撃に伴う多くの作業をアウトソースする傾向があります。

IAB は、引き続きランサムウェア侵入の主要ベンダーとして活動しています。Qbot や Black Basta など、特定のランサムウェアグループと深いつながりがある IAB もあれば、さまざまなグループにアクセス情報を売却している IAB もあります。LockBit、DarkSide、Conti、BlackByte などの背後にいるランサムウェアグループは、攻撃の一部に IAB を利用しているという報告があります。前回の DNS レポートの「[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](#)」によると、感染したデバイスの 26% が IAB と関連のあるドメインにアクセスしており（図 7）、Qakbot / Qbot（感染したデバイスの 4%）、Emotet（感染したデバイスの 22%）が含まれます。





脅威カテゴリごとのデバイスの割合  
2022 年 1 月 1 日～2022 年 12 月 31 日

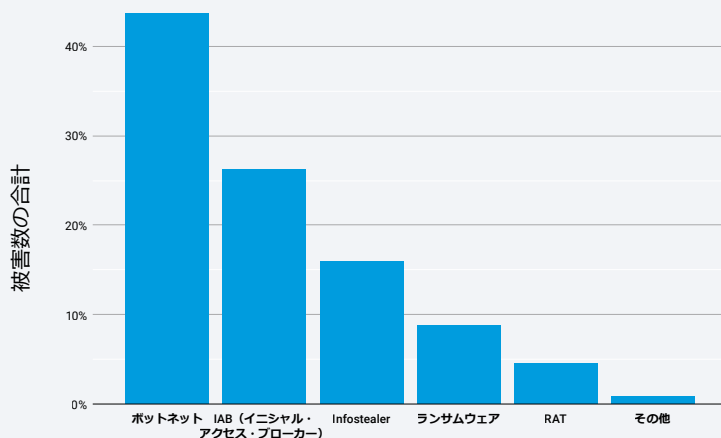


図 7：悪性 DNS トラフィックの分析に基づくエンタープライズ環境に存在する脅威のタイプ - 出典：Akamai による前回の SOTI レポート「攻撃の「高速道路」：悪性 DNS トラフィックの詳細な分析」

サービスとしてのランサムウェア（RaaS）ビジネスモデルとサイバー犯罪において、IAB はどのような役割を果たしているのでしょうか？ランサムウェア攻撃者がリモートアクセスと認証情報を必要とするのは、被害組織のネットワークに侵入するためだけでなく、ネットワークを横断して潜伏し、アクセス権限を取得するなどの活動のためでもあります。このランサムウェア攻撃者と IAB の共生的な関係は、ランサムウェア攻撃数の増加にさらに拍車をかけます。だからこそ、防御側で IAB が使用するマルウェアを検知できることが重要になります。初期感染からネットワーク全体へのランサムウェア拡散は衝撃的なほどすばやく完了します。



## データとともに駆け抜ける：脅迫手法はどのように進化してきたか

ランサムウェアの攻撃者は、主な脅迫手法である暗号化から脱却し、データ窃取に専念しています。そして、窃取した機微なデータを使用して被害組織を脅迫しています。機微な情報をオンラインで公開する、またはダーク Web で最高額落札者に売却すると主張し、被害組織を脅します。この攻撃手法を見ると、ランサムウェアを防御するためにはバックアップだけでは不十分なのは明白です。組織が暗号化から速やかに回復できたとしても、機微な情報の損失から回復することはできません。攻撃者は、ネットワーク全体を地道に侵害するよりも、情報を盗み取った方がメリットが高く、大きなインパクトを与えられると気付いた可能性があります。BianLian は、暗号化なしのデータ窃盗手法を採用した攻撃者の例です。暗号化を省略するため、元のランサムウェアのペイロードから復号業者が不要になります。組織は、キルチェーンのさまざまな段階で境界を保護し、ランサムウェアの損害を制限するために、DDoS 防御を備えたゼロトラスト・セキュリティ・モデルの導入が強く推奨されます。

近年、ランサムウェア攻撃者によるリスクは、複数脅迫スキームでさらに高まっており、被害組織は身代金要求に従わざるを得ない状況です。ほとんどのランサムウェア被害組織は、データの暗号化から始まり、身代金を支払うまでそのデータにアクセスさせないという複合的な脅迫テクニックに直面しています。データを窃盗し、人質として利用するというこの二層構造の脅迫手法は、今や主流になりつつあります。こうした脅迫を突き付けた後で、標的組織が攻撃者の要求に従わなかった場合、攻撃者は次の段階に進み、DDoS 攻撃を仕掛けてサイトトラフィックを飽和状態にしてビジネス運営を混乱させ、金銭的な損失をもたらします。ALPHV は、こうしたグループの一例であり、身代金要求が満たされないと DDoS 攻撃を仕掛けます。この複合的な攻撃に DDoS 攻撃が加わることで、データを盗取して暗号化するランサムウェア攻撃ですでに忙殺されているセキュリティチームは効果的な対処が難しくなります。さらに悪いことに、攻撃者は、被害組織の顧客、ビジネスパートナー、さらに報道機関にメールを送信することで、脅迫やハラスメントに利用する可能性もあります。組織がそうした攻撃の被害を受けたという情報をリークすることで、ブランドと名声を汚し、顧客の信頼を損なう結果を招きます。

組織が暗号化から速やかに回復できたとしても、機微な情報の損失から回復することはできません。

## ランサムウェアは重要な業界を引き続き標的にしている

現時点で最大規模のランサムウェア攻撃者の姿を把握し、こうした攻撃者が使用する戦術とテクニックを理解することで、防御側はランサムウェア攻撃に対する組織のセキュリティ体制を強化できます。しかし、重要なのは各業界がどのように標的にされているのか、どの脅威がどの業界や境界を標的にしているのか知ることです。そうすることで、侵入テストチーム、レッドチーム、セキュリティ担当者は、攻撃シナリオをシミュレートし、環境のギャップを埋める方法を把握できます。

ランサムウェア攻撃は、業界や規模を問わず、あらゆる組織にまん延しています。[Astra のレポート](#)によると、攻撃は約 19 秒に 1 件のペースで発生し、その合計数は 1 日に 170 万件に達しています。こうした攻撃の大半は私たちのデータ収集範囲の外部で発生していますが、同レポートでは、過去 5 年間の平均でインシデントごとに約 185 万ドルのコストがかかっていると指摘しています。さらに、[Cybersecurity Ventures の予測](#)によると、2031 年までには 2 秒に 1 件のペースでランサムウェア攻撃が発生することになります。

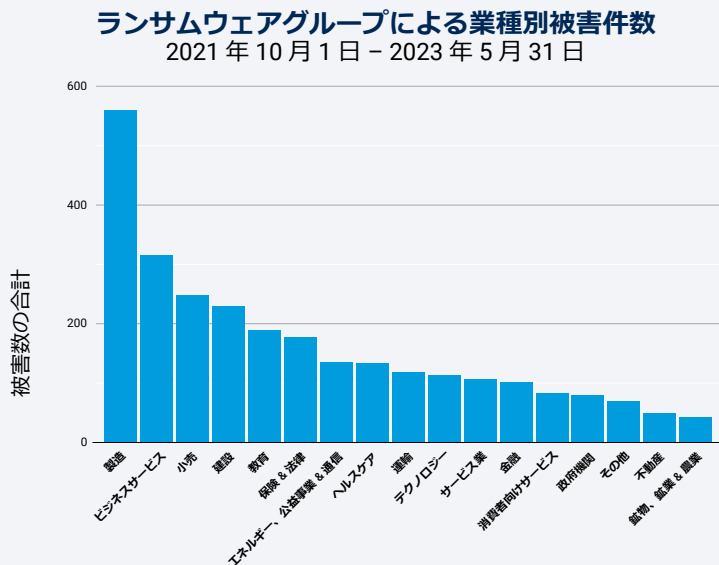


図 8 : 製造業は依然としてランサムウェア攻撃の被害件数が最も多い業界



製造業は依然として被害件数が最も多い業界であり（図 8）、ランサムウェア攻撃を受けた被害組織の 20% を占め、首位となっています。その製造業に、ビジネスサービスと小売がそれぞれ 11% と 9% で続いています。この結果は、昨年の[グローバル・ランサムウェア・レポート](#)でも同様であり、製造業とビジネスサービスは、Conti ランサムウェアの被害を受けた組織の上位を占めています。さらに、「[攻撃の「高速道路」：悪性 DNS トラフィックに関する詳細な調査](#)」レポートの結果とも一致しており、C2 トラフィックで分析された組織の 30% は製造業でした。製造業は他の業界より多くの攻撃を受けているというわけではありませんが、はっきりしているのは、攻撃者がこの業界を標的にすると攻撃が成功すると認識しているということです。さらに、ビジネスサービスがランサムウェアの被害件数の 2 位になっているという事実は、サプライチェーン攻撃の可能性をあらためて示唆しています。典型的な例として、ある[ガソリン小売会社](#)がサードパーティのサービスプロバイダー経由で CL0P ランサムウェア攻撃を受けました。主要業界ごとのランサムウェア被害件数の比較でも増加傾向を確認できます（図 9）。

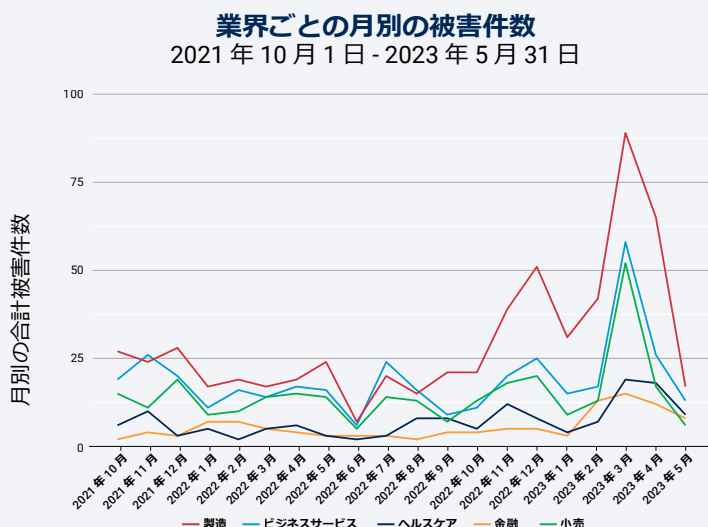


図 9：主要業界ごとのランサムウェア被害件数の比較でも増加傾向を確認できる

私たちは、金融サービス、ビジネスサービス、製造、コマース、ヘルスケアという 5 つの業界を分析して上位のランサムウェア脅威を明らかにし、攻撃傾向における収束と拡散を見極めました。LockBit はトップに君臨し、これらの業界全体で被害組織の大半を占めています。LockBit は、製造業では被害組織の 41%、金融サービスでは 50% に迫る比率となっています（ただし、被害件数は製造業より少なくなっています）。2019 年に ABCD ランサムウェアとして初めて確認された LockBit は、複数の改善が実施されており、2.0 バージョンでは、最速の暗号化メカニズムを導入したと運営者は主張しています。HiveLeak もこの 5 つの業界でまん延していたランサムウェアの 1 つでしたが、法執行機関が Hive のネットワークを摘発した昨年、活動を[停止](#)しています。ここからは、複数の業界をさらに詳しく見ていきましょう。各業界の課題とともに、ランサムウェア攻撃の標的とされる環境的な要因を明らかにします。



ビジネスサービスがランサムウェアの被害件数の 2 位になっているという事実は、サプライチェーン攻撃の可能性を示唆しています。



## 製造

製造会社は、一般にランサムウェアの脅威に対して脆弱性が比較的高いと言えます。これは、専門的なレガシー・オペレーティング・システムが多数存在すること、互いに接続されたデバイスや機器が多数あるため、アタックスurfaceが大きいことが理由です。製造会社の業務が中断すると、その影響が会社、会社の顧客、さらには社会にまで及ぶ可能性があるため、甚大なリスクとなります。業務が中断されると、高価な資本設備の停止または損傷、売上／市場シェア／安全性の損失、従業員や周囲のコミュニティへの環境的な損害につながります。さらに、製造会社に対する攻撃が成功すると、サプライチェーンが混乱し、必須の製品やサービスに遅延が発生します。

コネクテッドカーから化学プラントに至るまで、製造およびサプライチェーンのさまざまな拠点で運用されている機器、センサー、およびその他のコネクテッドエンドポイントにわたり、多数のレガシー商用ソフトウェアや古くなった商用ソフトウェアが展開されていることが、このようなリスクの増加の背景にあります。2021 年第 4 四半期から 2022 年第 4 四半期にかけて、被害を受けた製造会社の数が 42% 増加したという調査結果データからも、このようにリスクが高まっていることがわかります。長期的に見て、製造会社は、独自の設計、製法、企業秘密といった貴重な知的財産を保持しています。ランサムウェア攻撃は、この機微な情報を窃盗または公開し、競争力を損ない、法的な判断を仰ぐ状況を招く可能性があります。組織の評判に対するダメージは、長期的な影響も及ぼします。

```
...Chan); case status := <- workerCompleteChan: wor  
...m()); count, err := strconv.ParseInt(r.FormValu  
...log(r.FormValue("target")), count); }); http  
... { fmt.Fprintf(w, "INACTIVE"); }; return; c  
...); }; func main() { controlChannel := m  
...WorkerActive; case msg := <-controlChan  
... *http.Request) { host  
... fmt.Fprintf(w, "Control message  
... select { case result := <  
... "strings"; "time" ); typ  
...}; for { select { cas  
...Channel chan chan  
...ControlMessage(T  
... bool); statu  
...); packag  
...chan boe
```

# 42% ↑

2021 年第 4 四半期から  
2022 年第 4 四半期にか  
けて被害を受けた製造会  
社の増加率





製造会社の状況をさらに複雑にしているのは、複雑で長大になりがちなサプライチェーンです。ベンダーおよびサプライヤーとの関係を維持するためには、自動化されたデータインターフェースが必要となります。また、ベンダー担当者が製造会社のサイトを使用して、機器とやり取りし、システムを制御することになります。その結果、把握して防御すべきアタックサーフェスがさらに増加します。

## ヘルスケア

ヘルスケア組織には、病院、民間の診療所、製薬会社などが含まれます。特にヘルスケア情報テクノロジーは、大きな[一連のセキュリティ課題](#)に直面しています。たとえば、必須となるセキュリティ戦略がない中、絶えず拡大する「医療分野のIoT」環境でレガシーシステムを使用しなければならなかったり、あるいはMRI装置などの医療機器内の脆弱性がヘルスケアネットワークへの容易なアクセスポイントになるケースがあります。さらに、サイバー攻撃に対する境界セキュリティに取り組む上での新たな課題として、サイバーセキュリティスタッフの欠如（特に小規模な病院の場合）が挙げられます。

Health-ISAC が 2023 年 2 月に発行した「[Current and Emerging Healthcare Cyber Threat Landscape（現在と今後のヘルスケアサイバー脅威の現状）レポート](#)」によると、ランサムウェアは、ヘルスケア業界にとって最大のセキュリティ課題となっています。前述のセキュリティ課題のほかに、ヘルスケアデータもクレジットカード以上にダーク Web で非常に価値の高いアセットの 1 つです。そのため、この業界はサイバー犯罪者にとってさらに魅力的な標的になります。2021 年第 4 四半期から 2022 年第 4 四半期にかけて、この業界に対するランサムウェアの被害件数は 39% 増加しています BlackCat と LockBit はヘルスケア組織への攻撃を専門とし、特定の被害組織に合わせた[戦術のカスタマイズ](#)まで行っています。



小規模な病院でのサイバーセキュリティスタッフの不在が、新たな課題を突き付けています。

ランサムウェア攻撃が成功すると、ヘルスケア業界では特に悲惨な結果となる可能性があります。重要なサービスを提供するためには患者記録へのアクセスが不可欠であり、ときには生死を分ける要因にもなるためです。病院は攻撃の対象外だと公言するランサムウェアグループも存在しますが、データを見ると、LockBit や HiveLeak などのランサムウェアグループはヘルスケア組織を依然として標的としています。

## 金融サービス

ランサムウェアは、金融サービスにおけるサイバーセキュリティ攻撃の定番となっています。Financial Services Information Sharing and Analysis Center (FS-ISAC) による「[Navigating Cyber 2023](#)」レポートによると、ランサムウェアは金融機関にとって最大の懸念であり、急速にサイバーセキュリティ最悪の課題の1つになっています。被害件数は製造業や小売業より少ないですが、この業界の被害組織の合計数は 50% 増加しています。

不正な利益の一部を見返りとしてアフィリエイトにランサムウェアスイートへのアクセスを提供する RaaS プロバイダーは、この増加の主な要因でしょう。金融機関は、機微な情報を保持していることから、高価値の標的と見なされています。その結果、要求される身代金が他の標的より高くなります。金融サービスは経済システムを支える屋台骨です。そのため、金融機関が混乱すると、深刻な事態に陥りがちであり、その混乱が短期間でも、甚大な金銭的損失と評判の失墜を招く可能性があります。攻撃者は、金融機関のこうした立場を見越して膨大な額の身代金を要求します。さらに、データを暗号化して脅迫する前にデータ自体を盗み出す、リークサイトで被害組織を貶めて支払いを強要する、すでにランサムウェア攻撃への対応で手一杯の被害組織に DDoS 攻撃を仕掛けるなど、さまざまな戦術を使用します。インテリジェンスを駆使した脅威ハンティングは、事前対応型で効果的な防御メカニズムとなります。

ランサムウェアは、金融サービスにおけるサイバーセキュリティ攻撃の定番となっています。

50% ↑

金融サービス業界における合計被害件数の増加率



## コマース

小売会社とホテル・旅行会社で構成されるコマース業界は、業界別のランサムウェア被害件数で 2 位（小売業とホテル・旅行業の合計件数）となっています。これは、小売企業に対するランサムウェア攻撃が増加していると報告した [IDC の調査](#)とも一致します。私たちのデータ分析でも、小売業界の被害件数で 9% の増加を確認しています。この業界でランサムウェアのリスクが急激に高まっているのは、さまざまな要因の組み合わせが原因です。たとえば、コマース環境の複雑化が進んだことで防御が困難になっている、セキュリティの成熟レベルが低い、データを多用するアプリケーションを使用しているなどです。特に小売企業の場合、ランサムウェア攻撃が成功すると、重要なシステムやサーバーにアクセスできなくなるため、店舗とオンラインストアの両方の運営が突然停止します。機密扱いとなる顧客個人を特定できる情報（PII）やクレジットカードのデータが盗取されてダーク Web で売却されたとしても、あるいは攻撃者が脅迫に使用したとしても、ブランドや評判の失墜とともに、金銭的にもさらなる損害に発展します。年 1 回発行の「[RH-ISAC CISO Benchmark](#)」レポートによると、セキュリティリーダーは 2023 年に組織が直面する最大のリスクとしてランサムウェアを挙げています。ランサムウェア攻撃を受け、身代金の支払いに応じた小売企業は、平均 16 万ドルを支払ったと報告されています。さらに、同じ IDC 調査では、小売企業はランサムウェア攻撃を受けた場合、さまざまなビジネス上の混乱に陥る可能性が高いと指摘しています。

## 教育

大学や小中高などの教育機関は、ランサムウェアの標的になりつつあり（2021 年第 4 四半期から 2022 年第 4 四半期にかけて被害件数が 128% 増加）、データ盗取が発生した結果、数日間の[学校閉鎖](#)を余儀なくされるケースもあります。教育業界が保有する PII などの情報の性質から、こうした被害は特に懸念されます。教育業界を標的にしたグループの 1 つである [HiveLeak](#) は、心理アセスメントや社会保障番号など、非常に機密性の高い学生情報を公開すると脅迫しました。Vice Society も教育業界を標的としている主なランサムウェアの 1 つであり、この [Malwarebytes のレポート](#)によると、攻撃の 39% を占めています。私たちのデータでも、Vice Society（24%）は教育業界で LockBit に続く上位のランサムウェアとなっています。[ランサムウェア攻撃](#)は、大学だけでなく、小中高の学校でも広がっています。これは、予算の制約、セキュリティリソースの不足、スタッフのセキュリティに対する認識やトレーニングの欠如が原因と考えられます。



## 収益別の分析：収益規模の小さな組織はランサムウェアのリスクが高くなる

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。攻撃者は、中堅、中小、大手など、組織の規模にこだわりません。しかし、大手の方が収益が多く、攻撃でより多くの利益を得られるため、標的になりやすいと一般的には考えられています。収益別の被害件数の分析では、まったく異なる傾向が明らかになります。分析を行った被害組織の60%以上（図10）は、収益5,000万ドル以下の小規模組織であり、攻撃者は小規模組織にも攻撃を仕掛けて成功していることを示しています。収益の低い組織の場合、環境に侵入しやすく、ランサムウェアの危険に対抗するセキュリティリソースに限りがあるため、こうしたランサムウェア攻撃に対してより脆弱だと推測できます。同時に、ビジネスの混乱を回避し、収益損失の可能性を避けるために身代金を支払う余裕があることも、収益が比較的低い組織の特徴です。

ランサムウェアグループによる収益範囲別の被害件数  
2021年10月1日 - 2023年5月31日

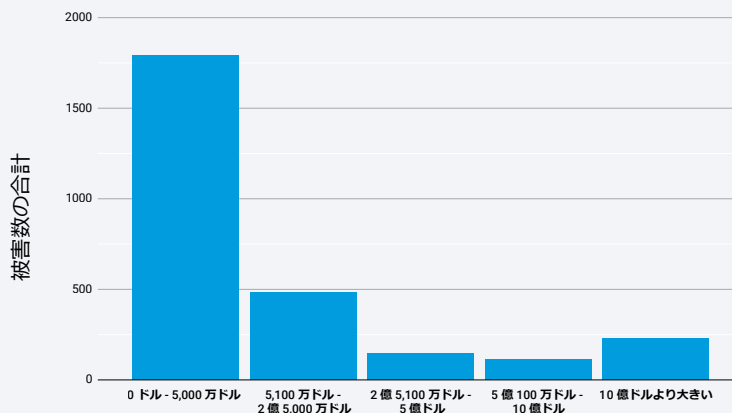


図10：ランサムウェア被害組織の大半は、報告収益が5,000万ドル以下の組織である

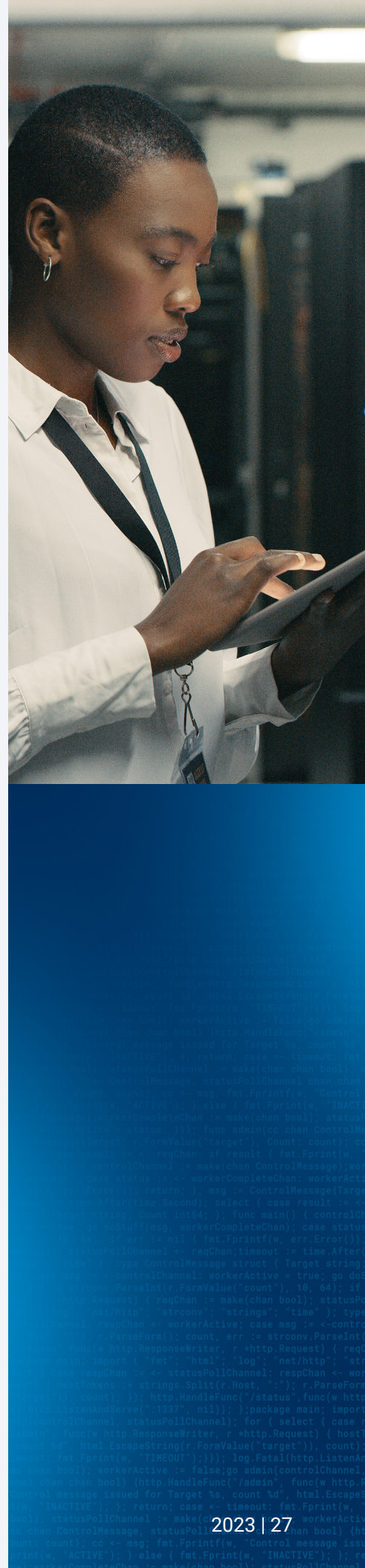


被害を受けた 17% 以上は、収益規模が 5,100 万ドルから 2 億 5,000 万ドルの組織です。さらに、報告収益が 5 億 100 万ドル以上の大手組織もランサムウェア攻撃を受けやすく、この収益範囲の被害件数の比率（12%）からも確認できます。大手組織がランサムウェア攻撃を受けた比率はそれほど多くありませんが、境界防御を怠ると、高価値の標的も攻撃の対象となり、ランサムウェアの危険をさらされるのは明らかです。[Sophos の調査](#)では、被害組織の収益と攻撃者への身代金の支払額との関係をまとめていますが、被害組織の収益が多いほど、身代金の支払額も高くなっています。たとえば、収益規模 10 億ドル以上の組織の平均支払額は 100 万ドルとなります。

私たちの分析でも、被害件数とそれに対する収益範囲に関して、ほとんどのランサムウェアグループに同様の傾向が見られます。平均すると、ランサムウェアグループによる被害組織の 67% は最も低い収益範囲であり、LockBit と PYSA については、この収益範囲により集中しています（約 75%）。しかし、いくつかのグループは、高い収益範囲の被害組織の比率が著しく高くなっています。HiveLeak の報告された被害組織の 21% は収益規模 5 億 100 万ドル以上であり、同様に CLOP は 29%、ALPHV は 15% となっています。

[Cybercrime Magazine の報告](#)によると、全世界のランサムウェアの被害コストは 2031 年までに年間 2,650 億ドルに達すると予想されます。来年には年間 420 億ドルとなる見通しですが、これは 2 年前の 2 倍以上の金額です。この年間コストの上昇傾向とともに、ランサムウェア攻撃の件数も引き続き増加するため、今後数年間に合計被害件数が劇的に変化することが予想されます。

**アジア太平洋・日本（APJ）地域とヨーロッパ・中東・アフリカ（EMEA）地域におけるランサムウェア動向の詳細については、各地域の以下のスナップショットをご覧ください。**



ランサムウェア：

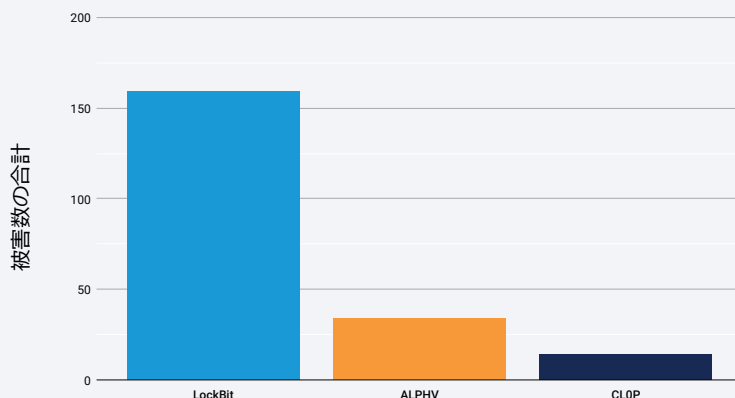
## APJ スナップショット

APJ 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。

## 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、アジア太平洋・日本地域（APJ）で被害を受けた企業数は 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：被害件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



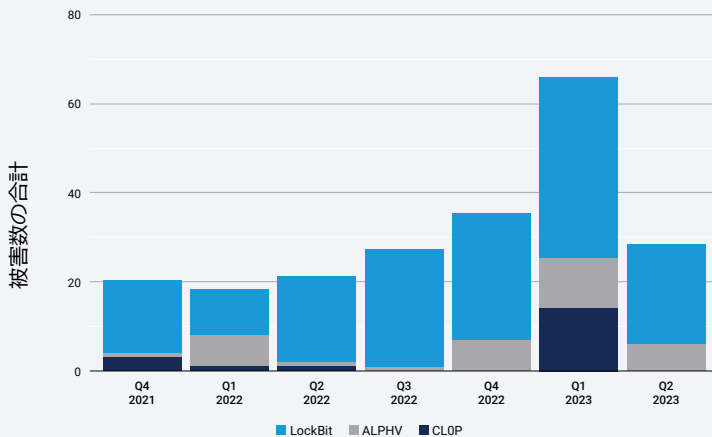
APJ 図 1：APJ で発生したランサムウェア攻撃の被害組織の大部分は、LockBit、ALPHV、CL0P による攻撃を受けている



## 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。

**APJ : 被害件数別ランサムウェアグループ上位 3**  
四半期ごと : 2021 年 10 月 1 日 - 2023 年 5 月 31 日



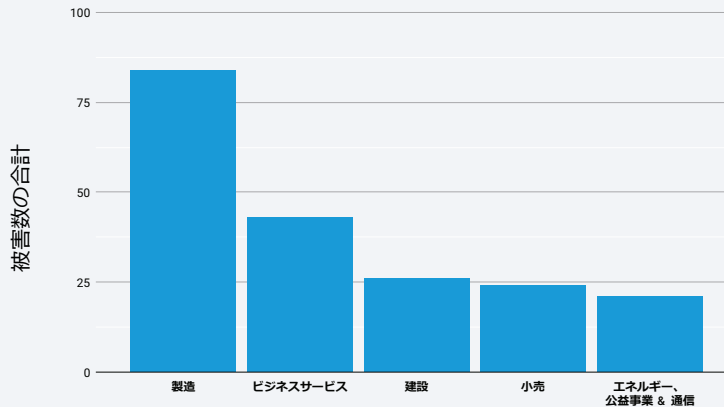
**APJ 図 2 : APJ におけるランサムウェアグループのトップ 3 (LockBit、ALPHV、CL0P) の被害企業数の四半期ごとの比較**

## 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、最も影響を受けている業界については、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](#)」とも一致しており、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。

\* 2023 年第 2 四半期については、2023 年 5 月 31 日までのデータのため、完全な四半期データではありません。

### APJ : ランサムウェアグループによる被害件数上位 5 業界 2021 年 10 月 1 日 – 2023 年 5 月 31 日



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

また、LockBit が業界の選り好みをしてい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

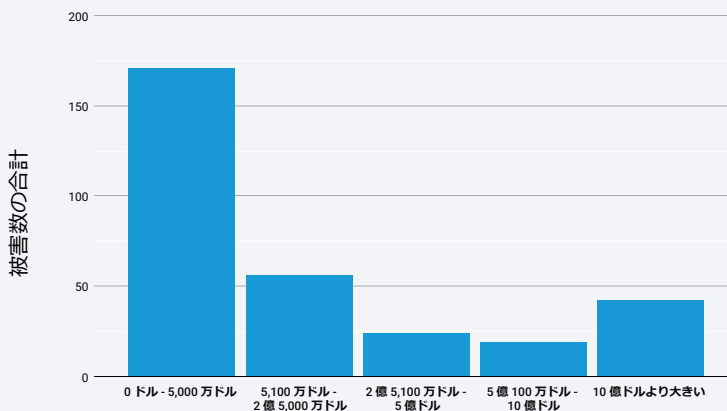
企業規模や収益に関係なく、すべての組織がランサムウェア攻撃のリスクにさらされています。しかし、世界的な傾向と同様、APJ では攻撃者が小規模な組織に対して攻撃を成功させていることが、データで示されています（APJ 図 4）。シンガポール・サイバーセキュリティ庁の[レポート](#)によると、シンガポールで報告されたランサムウェア被害企業の大部分は製造業と小売業の中小企業でした。Akamai の推測では、小規模企業はランサムウェアの危険に対抗するためのセキュリティリソースが限られているため、攻撃に対して脆弱で侵入されやすい一方で、身代金を支払う余地があるのです。ただ、最大規模のエンタープライズも攻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



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 : ランサムウェアグループによる収益範囲別の被害件数 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 万ドル以下の組織

### 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、自社の地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盛り込み、多層防御によってリスクを緩和する方法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。

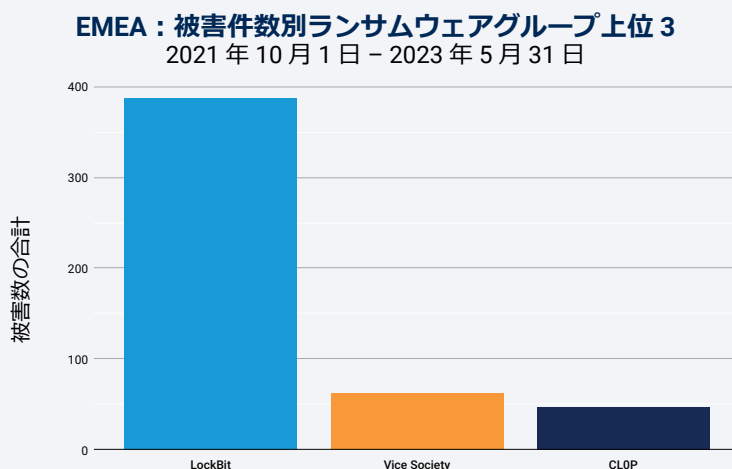
ランサムウェア：

## EMEA スナップショット

EMEA 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。

### 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、EMEA で被害を受けた企業数は 2021 年第 4 四半期から 2022 年第 4 四半期の間に 18% 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 77% と大幅に増加しています。当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 EMEA において被害企業に対する攻撃の大部分（45%）を占めています。しかし、EMEA では、Vice Society が ALPHV に代わって最もアクティブなグループの 2 位になり、CL0P が 3 位になっています（EMEA 図 1）。



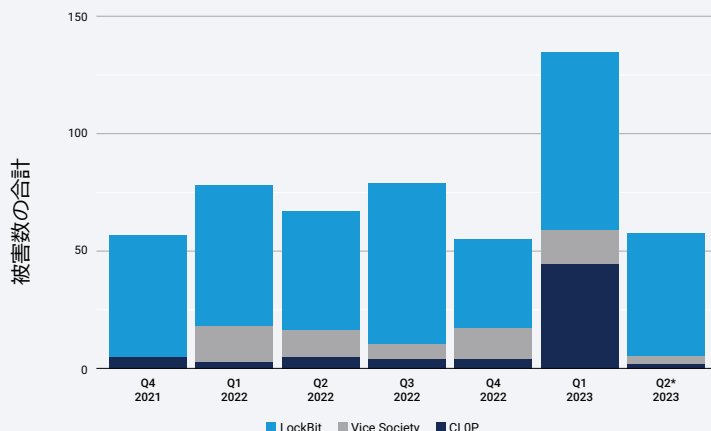
EMEA 図 1：EMEA で発生したランサムウェア攻撃の被害組織の大部分は、LockBit、Vice Society、CL0P による攻撃を受けている



## 四半期分析

ランサムウェアグループ別の被害件数を見ると（EMEA 図 2）、LockBit が首位を守る中、Vice Society が一貫した存在感を発揮しています。これは、EMEA では教育業界がランサムウェア攻撃の主な標的となっていることと密接に関連しています（以下の EMEA 図 3 を参照）。なぜなら、Vice Society は教育分野を**集中的に標的としている**サービスとしてのランサムウェアだからです。一方で、世界的なデータ傾向と同様、CL0P は EMEA ランサムウェア環境でも増加しており、2023 年第 1 四半期の急増は、さまざまなゼロデイ脆弱性を侵入経路として利用したことが原因と考えられます。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 の活動は 2022 年に観測したレベルまで回復しています。この四半期がどのようなデータになるのか断定はできませんが、2023 年 6 月に CL0P は MOVEit 脆弱性を利用して、EMEA において**さらに多くの被害組織**を攻撃したと発表しているため、被害件数はさらに増加すると考えられます。

EMEA：被害件数別ランサムウェアグループ上位 3  
四半期ごと：2021 年 10 月 1 日 - 2023 年 5 月 31 日



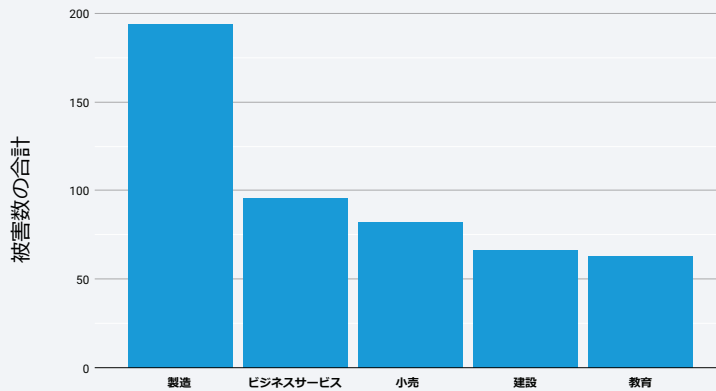
EMEA 図 2：EMEA におけるランサムウェアグループのトップ 3 による  
四半期別被害件数の比較 LockBit、Vice Society、CL0P

## リスクにさらされている重要な業界

EMEA においてランサムウェア攻撃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、小売、建設、教育です（EMEA 図 3）。これは全世界の上位 5 つの業界と同じであり、製造とビジネスサービスが上位 2 つの業界となった 2022 年の**グローバル・ランサムウェア・レポート**の結果とも一致します。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、最も影響を受けている業界については、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**」とも一致しており、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明確なつながりがあることがうかがえます。

\* 2023 年第 2 四半期については、2023 年 5 月 31 日までのデータのため、完全な四半期データではありません。

### EMEA : ランサムウェアグループ別の上位 5 業界 2021 年 10 月 1 日 - 2023 年 5 月 31 日



EMEA 図 3 : EMEA 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である

ここでも重要なのは、EMEA 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 45.9%、ビジネスサービスでは 45.4%、小売業では 45.1%、建設業では 53.6% を占めているという点です。教育分野は例外的です。ほとんどの攻撃は Vice Society によるものであり（36.5%）、LockBit による攻撃は 22.2% にとどまります。



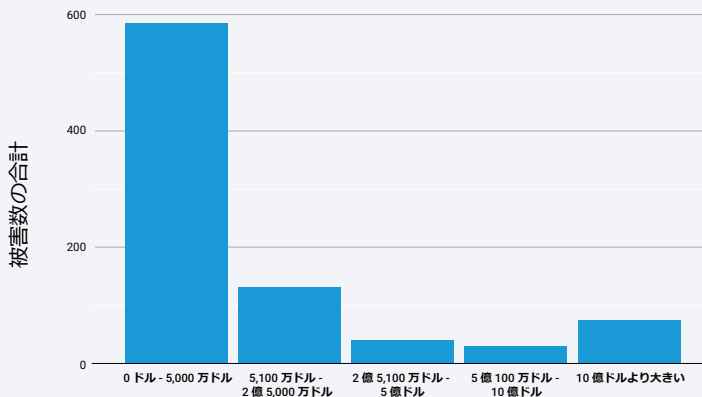
企業規模や収益に関係なく、すべての組織がランサムウェア攻撃のリスクにさらされています。



## 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、EMEA 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（EMEA 図 4）。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。

EMEA : ランサムウェアグループによる収益範囲別の被害件数  
2021 年 10 月 1 日 - 2023 年 5 月 31 日



EMEA 図 4 : EMEA 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 万ドル以下の組織

## EMEA 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と耐障害性の構築を後押しする手法を明らかにしています。ENISA（欧州ネットワーク・情報セキュリティ機関）が発行したアタックサーフェスネットワークおよび情報システム司令（NIS2）は、EU 全体のサイバーセキュリティを改善することを意図したものであり、脆弱性レジストリの構築など、新たなタスクを盛り込んでいます。EU 以外の国や地域では、サウジアラビアの国家サイバーセキュリティ庁（NCA）など、独自の管理体制を構築・実施しています。

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。



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、自社の地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盛り込み、多層防御によってリスクを緩和する方法を認識することが重要です。

## ソリューションと推奨される対策

このレポートでは、さまざまなランサムウェアの傾向とともに、攻撃の各段階でテクニックがどのように変化しているのか解説しました。ランサムウェア攻撃は多面的で、複数の段階と多くの戦術が存在します（図 11）。そのため、推奨される対策も攻撃の段階、さまざまな製品、および戦術に応じて異なる内容になります。

ランサムウェアの脅威を効果的に緩和するためには、以下の行動が重要となります。

- サイバーセキュリティに多層的なアプローチを導入し、すべての攻撃段階と脅威環境に対処します。攻撃の各段階に適したソリューションタイプの詳細については、次のセクションで確認できます。
- ネットワークマッピングとセグメンテーションで重要なシステムを特定して分離し、それらのシステムへの（からの）ネットワークアクセスを制限します。アクセスを制限することで、万が一セキュリティ侵害が発生しても、マルウェアのラテラルムーブメント（横方向の移動）を抑制できます。

```
...Chan); case status := <- workerCompleteChan: worl
...m()); count, err := strconv.ParseInt(r.FormValu
...log(r.FormValue("target")), count); }); http
... { fmt.Fprintf(w, "INACTIVE"); }; return; c
...); func main() { controlChannel := r
...WorkerActive; case msg := <-controlChan
... *http.Request) { host
... fmt.Fprintf(w, "Control message
..."; "time" ); typ
...}; for { select { ca
...llChannel chan chan
...ControlMessage(T
... bool); statu
...);package
...chan boe
...}
```



- すべてのソフトウェア、ファームウェア、オペレーティングシステムに最新のセキュリティパッチを適用し、常に最新の状態に保ちます。これにより、既知の脆弱性を緩和して、ランサムウェアによる悪用を防止できます。
- 重要なデータの定期的なオフラインバックアップを実施し、効果的な災害復旧計画を確立します。こうすることで、速やかに業務を回復できるようになり、ランサムウェアインシデントの影響を最小限に抑えることができます。
- ランサムウェア攻撃を受けたとき取るべき手順をまとめたインシデント対応計画を作成し、定期的にテストします。この計画では、明確な伝達経路、役割、責務とともに、法執行機関やサイバーセキュリティの専門家への連絡プロセスを明らかにします。
- サイバーセキュリティの意識向上トレーニングを定期的を実施し、フィッシング攻撃やソーシャルエンジニアリング、ランサムウェア攻撃者が一般に使用するその他のベクトルについて従業員を教育します。従業員は、疑わしい活動があれば直ちに報告するように徹底します。このトレーニングには、物理的にオンサイトで対応するベンダーと社内システムでリモートに対応するベンダーの両方に適用するポリシーと手順も盛り込むようにします。すべてのベンダーとサプライヤーも、サイトやシステムにアクセスする前に、このトレーニングを受けるように指示します。

## LIFECYCLE OF A RANSOMWARE INCIDENT

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

certnz

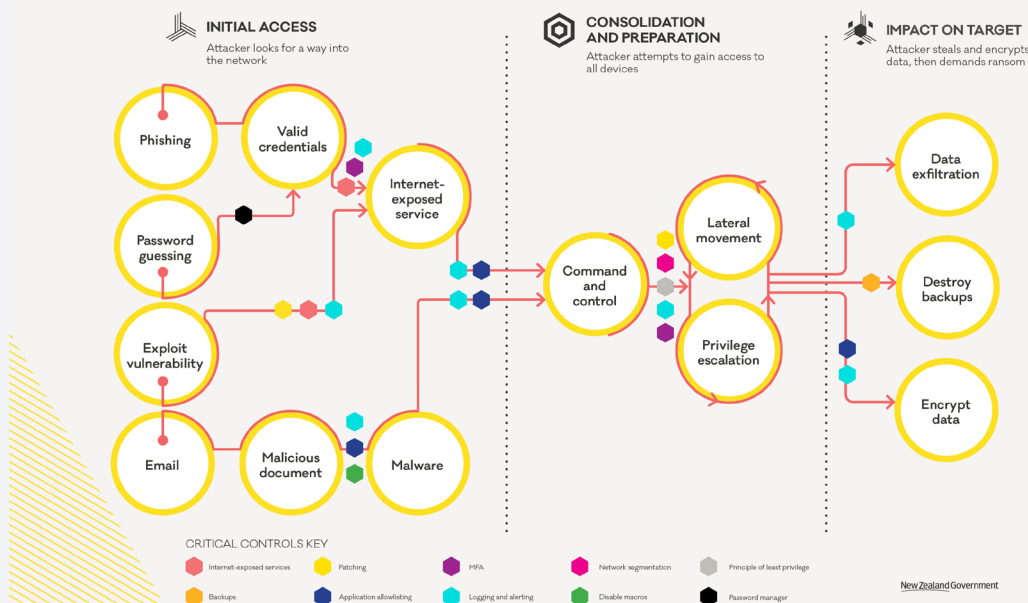


図 11：ランサムウェア攻撃の各段階

## 初期アクセスに対する防御

### インターネットに面しているサーバーの保護

インターネットに面したサーバーに対するワンデイおよびゼロデイ脆弱性の悪用は、感染ベクトルの主流になっています。こうした脅威に対する効果的な防御方法の1つが、Web アプリケーションと API の保護（WAAP）の導入です。たとえば、Web アプリケーションファイアウォール（WAF）は保護シールドとして機能し、受信側の Web トラフィックを分析して、Web アプリケーションの脆弱性を悪用する可能性がある悪性のリクエストをフィルタリングします。WAF は、HTTP および HTTPS トラフィックを検査することで、一般的な攻撃パターンや既知の悪用の試みを検知してブロックします。WAF は仮想パッチ適用などの機能を提供し、永続的な修正が適用される前に既知の脆弱性を即座に保護します。さらに、WAF は、MOVEit ゼロデイケースで発見されて CL0P グループに利用された未知の脆弱性に対する効果的な防御策としても実績があります。

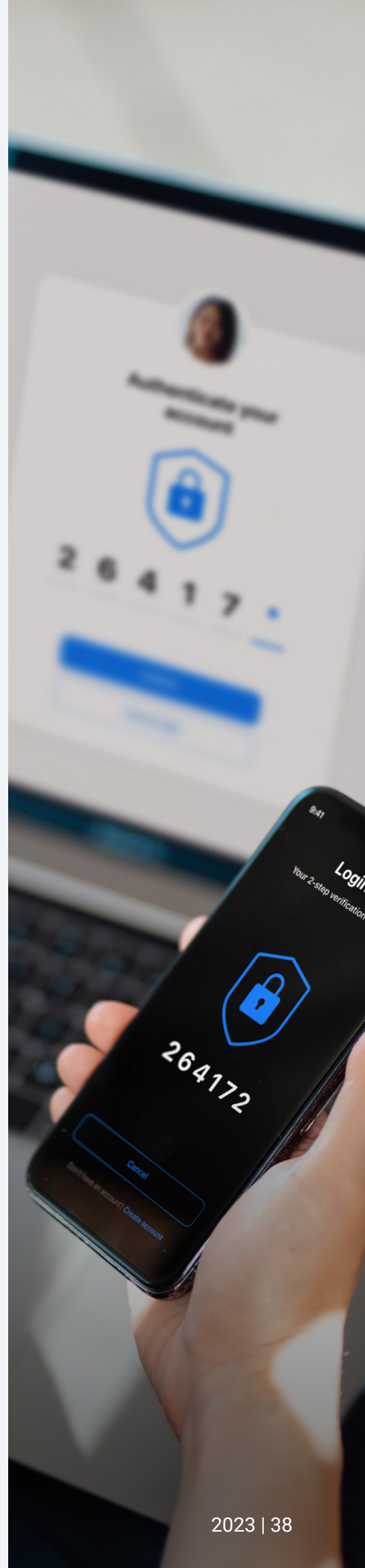
### エンドポイントをフィッシングから保護

URL 検査機能を使用し、フィッシングの試みを検知してブロックします。この機能を使用してエンドポイントを保護することで、ユーザーがクリックする URL をそのつどリアルタイムでスキャンし、悪性または異常なリンクを特定してブロックできます。

さらに、エンドポイント検知および応答ツールにより、悪性のペイロードを実行するフィッシングメールによる潜在的な侵害や悪性の活動を特定してアラートを受信できます。

### VPN のアタックサーフェスを縮小

ゼロトラスト・ネットワーク・アクセス（ZTNA）を使用して、アプリケーション固有の安全な VPN アクセスを実現し、外部のアタックサーフェスを縮小します。ZTNA によって、ネットワークに対してアプリケーション固有のロールベースのアクセスが可能になり、リスクが大幅に減少します。ZTNA は、従来の VPN のようにネットワーク全体へのフルアクセスを許可するのではなく、特定のアプリケーションに対する限定アクセスのみを許可します。こうすることで、攻撃者がユーザーの認証情報を侵害して多要素認証保護を回避したとしても、ネットワーク全体にはアクセスできず、一部のアプリケーションセットに封じ込めることができます。





## 重要なサービスでは多要素認証を使用

パスワードは、さまざまな方法で攻撃者に攻略されます。強力なパスワードはもはや鉄壁の防御策とは言えません。攻撃者は、総当たり攻撃や Credential Stuffing などの攻撃を使用して、パスワードを侵害し、ネットワークに侵入します。このリスクは、多要素認証ソリューションを使用してサービスを保護することで軽減できます。

## C2 に対する防御

### C2 サーバーをブロック

セキュア Web ゲートウェイなど、アウトバウンドのインターネットトラフィックを検査するソリューションを使用して、既知のマルウェア C2 サーバーをブロックします。このソリューションは、すべての通信をリアルタイムで監視し、悪性ドメインへの通信をブロックすることで、マルウェアが正常に稼働して目的を果たすのを阻止する必要があります。

## 発見に対する防御

### ネットワークスキャンを特定

侵入検知システムソリューションを使用し、疑わしいネットワークスキャンを特定します（図 12）。攻撃者はさまざまなツールを使用してネットワーク内の次の標的を特定します。この活動を検知できれば、攻撃の拡散を事前に阻止できます。

| <b>DESCRIPTION</b><br>A network scan has been detected | <b>Destinations</b>                                                                                                                                                                                                 |            |               |             |                                                                                                         |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------|-------------|---------------------------------------------------------------------------------------------------------|
| <b>SEVERITY</b><br>Medium                              | <table> <tr> <th>IP Address</th><th>Scanned Ports</th></tr> <tr> <td>172.17.0.62</td><td>334, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 443, 445, 446, 474</td></tr> </table> | IP Address | Scanned Ports | 172.17.0.62 | 334, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 443, 445, 446, 474 |
| IP Address                                             | Scanned Ports                                                                                                                                                                                                       |            |               |             |                                                                                                         |
| 172.17.0.62                                            | 334, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 443, 445, 446, 474                                                                                                             |            |               |             |                                                                                                         |
| <b>ASSETS</b><br>WindowsAgent                          |                                                                                                                                                                                                                     |            |               |             |                                                                                                         |
| <b>TIME</b><br>2023-07-12 16:14                        |                                                                                                                                                                                                                     |            |               |             |                                                                                                         |
| <b>TAGS</b><br>Host Port Scan Internal                 |                                                                                                                                                                                                                     |            |               |             |                                                                                                         |

図 12 : Akamai Guardicore Segmentation でのネットワークスキャンインシデント



ソリューションは、すべての DNS 通信をリアルタイムで監視し、悪性ドメインへの通信をブロックする必要があります。

## 発見を阻止する手法

ソリューションが作成または提供するハニーポットにより、攻撃者の「暗闇での手探り」を利用できます。攻撃者をハニーポットサーバーに誘導し、活動を監視して、異常を検知した場合にアラートすることで、攻撃者の活動を検知して阻止できます（図 13）。

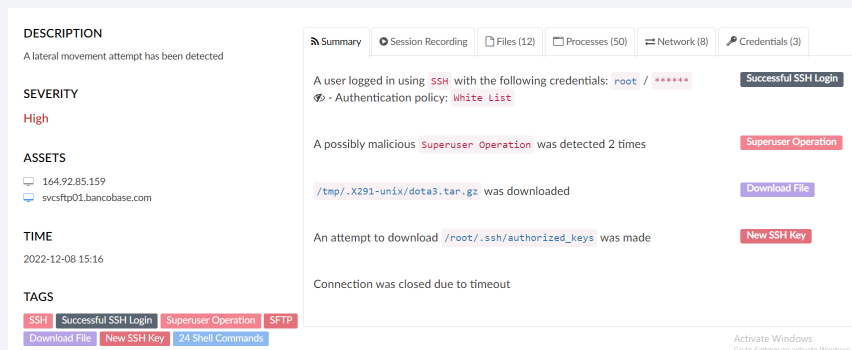


図 13 : Akamai Guardicore Segmentation での不正インシデント

## ラテラルムーブメントに対する防御

### 管理ポートを制限

ソフトウェアベースのセグメンテーションを使用してプロセスレベルのポリシーを作成し、機微なポートにおけるアタックサーフェスを縮小します。可能であれば、ポリシーをプロセスレベルで適用できるソリューションを使用し、機微な管理ポートを介して通信すべきプロセスを指定できるようにします（図 14）。こうすることで、そうしたポートが悪性の活動に使用される可能性を抑制できます。

| Section | Source  | Destination | Ports/Protocols | Action |
|---------|---------|-------------|-----------------|--------|
| Allow   | Ansible | Windows     | 5985 TCP   UDP  | Allow  |
|         | Any     | Any         |                 |        |
| Block   | * Any   | Windows     | 5985 TCP   UDP  | Block  |

図 14 : WinRM 通信を制限する Akamai Guardicore Segmentation ポリシーの例





## 盗取に対する防御

### 盗取ドメインをブロックする

既知の悪性 URL や DNS トラフィックをブロックするソリューションを使用するか、特定のドメインへのアクセスをブロックできるソリューションやコントロールを使用して、データ盗取に悪用される可能性のあるサービスへのアクセスを制限します（図 15）。そのドメインへのアクセスを必要としないすべてのエンドポイントからのアクセスをブロックして、ブラウザなどの承認済みアプリケーションを介したアクセスのみを許可することで、盗取ツールを使用した攻撃のリスクを最小限に抑えることができます。

| <div>▼</div> |              | <div>✓ Publish</div> <div>🗑 Discard</div>    |                 | <div>👤 CSV</div> |  |
|--------------|--------------|----------------------------------------------|-----------------|------------------|--|
| Section      | Source       | Dest                                         | Ports/Protocols | Action           |  |
| Allow        | 🔧 chrome.exe | <div>🌐 *.mega.nz +2 🛠</div> <div>🔧 Any</div> | Any TCP   UDP   | 🟢 Allow          |  |
|              |              |                                              |                 |                  |  |
| Block        | * Any        | * Any                                        | Any TCP         | 🔴 Block          |  |

図 15 : 悪用ドメインをブロックする Akamai Guardicore Segmentation ポリシーの例

```
...Chan); case status := <- workerCompleteChan: wor
...(); count, err := strconv.ParseInt(r.FormValu
...log(r.FormValue("target")), count); }); http
... { fmt.Fprintf(w, "INACTIVE"); }; return; c
...; }); func main() { controlChannel := r
...WorkerActive; case msg := <-controlChan
... *http.Request) { host
... fmt.Fprintf(w, "Control message
..."; select { case result := <
... "strings"; "time" ); typ
...}; for { select { cas
...ControlChannel chan chan
...ControlMessage(T
...when bool)); stat
...chan boo
...ni wo
```

## 結論

この Akamai ランサムウェアレポートでは、多くのランサムウェアグループがソフトウェアの脆弱性を悪用して企業を脅迫する戦略へと移行していることを取り上げました。今年は、他の MFT システムが CL0P などのランサムウェアグループの高価値の標的になる可能性があるかと予想されます。

この変化は、攻撃者が用いる戦術の大幅な進化とともに、攻撃の効果を最大限まで高めるという適応力と決断を示すものです。組織はサイバーセキュリティの防御策を引き続き強化していますが、ファイル・バックアップ・ソリューションはランサムウェアグループに対抗するための包括的なソリューションとしてはもはや機能しない、という事実は明白です。現在の課題を克服するためには、ネットワークセグメンテーション、脆弱性管理、タイムリーな「仮想」パッチ適用、ファイル転送システムの積極的な監視など、未然防止型の対策を優先し、ランサムウェアグループの攻撃の被害者となるリスクを緩和する必要があります。

さらに、今こそプレイブックを更新すべきです。昨今はソーシャルエンジニアリングよりもマルウェアが重視されるようになり、テクニカルコントロールが防御の最前線になります。ゼロデイ脆弱性と IAB では、暗号化の拡散とデータの窃盗を防ぐために状況認識と緩和戦略が必要になります。侵入テストチームとレッドチームは、LockBit などのグループを使用して検証演習をモデル化することが重要です。組織は、法務チームとともに規制を検証し、計画に漏れがなく、コンプライアンスが確保されていることを確認し、ベストプラクティスとして CISA と ISAC を利用する必要があります。

それでも攻撃を受けた場合は、復旧のための時間的余裕がないことを自覚し、1 つ目のインシデントの対応中に第 2 波の攻撃を受ける可能性があることを認識する必要があります。チーム全体で次の攻撃に備えましょう。

最新の Akamai リサーチを[セキュリティ・リサーチ・ハブ](#)でご確認いただけます。



組織はサイバーセキュリティの防御策を引き続き強化していますが、ファイル・バックアップ・ソリューションはランサムウェアグループに対抗するための包括的なソリューションとしてはもはや機能しない、という事実は明白です。



## 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、収益範囲、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  
Eliad Kimhy  
Lance Rhodes

Charlotte Pelliccia  
Badette Tribbey

### 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](https://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](https://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バージョン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](https://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](https://akamai.com/ransomware)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、各ソリューションの詳細については、[akamai.com](https://akamai.com) および [akamai.com/blog](https://akamai.com/blog) をご覧いただくか、[Twitter](https://twitter.com/Akamai) と [LinkedIn](https://www.linkedin.com/company/akamai-technologies) で Akamai Technologies をフォローしてください。公開日：2023 年 8 月。