ニューノーマル処方箋（第16回）

予防&万が一の速やかなデータ復旧で業務を止めない！ ランサムウエアの被害を防ぐバックアップ6つのポイント

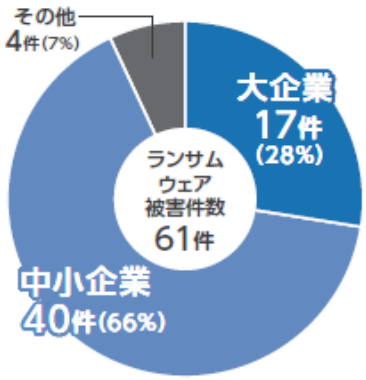
2022.03.29

企業内のネットワークに侵入してデータを暗号化し、その解除と引き換えに金銭を要求する「ランサムウエア」は企業にとっての大きな脅威になっています。その対策には大きく2つの方向性があります。1つは、感染リスクを最小化するセキュリティ対策を行うこと。もう1つは、万が一感染してしまってもデータを復旧できるようにバックアップを取ることです。しかし、近年のランサムウエアは大きく進化し、従来のシンプルなバックアップでは対処し切れなくなっています。ここでは「ランサムウエア対策」という観点から、バックアップを行うときに気を付けたい6つのポイントを解説します。

ランサムウエアはニューノーマル時代での重大なセキュリティ課題

ランサムウエアの脅威が増大しています。情報処理推進機構（IPA）が毎年発行する「情報セキュリティ10大脅威（組織）」では、2021年版で「ランサムウエアによる被害」が前年の5位から1位に上昇し、2022年版では引き続き1位を継続しています。

特に2021年後半は、日本の大手食品企業や地方の町立病院が被害に遭い、各メディアで大きく報じられました。これまでサイバー攻撃は国防機関や社会インフラ、大手企業などが標的になることが多かったのですが、警視庁の調査が示すように、現在では、中小規模の組織がターゲットとなっていることにも注意しなければなりません（図1）。



注　図中の割合は小数点第1以下を四捨五入しているため、総計が必ずしも100にならない

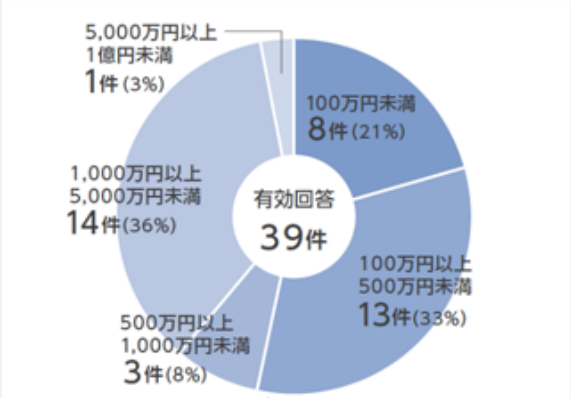
図1：2021年に警視庁に報告されたランサムウエア61件における企業規模の割合
出典：警視庁「令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について」

ランサムウエアはパソコンなどに保存されているデータを暗号化し使用できない状態にした上で、そのデータを復号する対

価として金銭を要求するものです。愉快犯的な犯行として古くからある攻撃手法でしたが、近年では組織化、ビジネス化がさらに進み、サイバー脅威の1つとして広く認識されるようになりました。

近年は在宅勤務が広がったことで、リモート環境で利用されるパソコンの脆弱性を突いて攻撃を仕掛けたり、リモートアクセスのためのVPN装置の脆弱性を突いて攻撃を仕掛けたりするケースが増加しています。

ランサムウエアは、被害件数、被害額も年々増加する傾向にあります。復旧のための費用はもちろんのこと、ファイルを扱えないことで事業が中断してしまえば、その分大きなビジネスの損失につながります。また取引先やパートナー企業にも損害を与えることになるため、経済的にも社会的信用の観点でもその影響は計り知れません。



注　図中の割合は小数点第1以下を四捨五入しているため、総計が必ずしも100にならない

図2:ランサムウエア被害に関連して要した調整・復旧費用
出典:警視庁「令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について」

「人手を介したネットワーク侵入」や「二重の脅迫」が顕著に

ランサムウエアは2016年頃に活発化してから日々進化を繰り返しています。そのため、ランサムウエアに対する考え方を見直していく必要があります。

典型的なケースは「ランサムウエア対策にはバックアップが有効であり、バックアップさえあればデータが暗号化されても問題ない」という考え方です。確かに以前はこうした考え方も有効でした。しかし現在は、はじめからバックアップを狙った攻撃が一般的になっており、「バックアップさえあれば安心」ではなくなってきています。

ランサムウエアはどのように進化を遂げてきたのでしょうか。IPAの「情報セキュリティ白書2021」や、警察庁サイバー犯罪対策プロジェクト、JPCERT/CCのランサムウエア対策特設サイトなどの情報を整理すると、大きく2つのポイントがあります。

1つ目は「人手を介したネットワークへの侵入」です。従来のランサムウエア攻撃は、不特定多数の利用者を狙ってメールを送信するという「ばらまき型」の手口が一般的でしたが、現在ではVPN機器から侵入し、特定の個人や企業・団体などを標的にする手口に変化しています。

標的型攻撃と同様の手口でネットワークに侵入し、侵害範囲を横に拡大(ラテラルムーブメント)して感染を広げていきます。その際に、バックアップファイルを探してバックアップデータごと暗号化したり、長期に潜伏して暗号化したことを悟られないようにしたりする手法も多く見られます。つまり、ただバックアップなどを取得しているだけでは対応できず、標的型攻撃と同様に多層的な対策を行う必要があります。

2つ目は「二重の脅迫」です。これは、ランサムウエアによって暗号化されたデータを復旧するための身代金の要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開・暴露するなどと脅迫するものです。攻撃者にとっては、身代金要求を二重に行うことで、金銭窃取の成功率を高める狙いがあります。

この場合、バックアップからデータを復元できたとしても、すでにデータは外部に流出しているため実害を被ることになります。また「データ暗号化」「データ暴露」に加え、企業のサービスサイトに「DDoS攻撃※1」を仕掛けて脅すといった「三重の

脅迫」も出現しています。
※1…攻撃対象のWebサーバー（Webサイト）などに対して複数のコンピュータから過剰なアクセス負荷をかけてサービス停止や妨害を図る攻撃

まずは「セキュリティ対策の基本」を徹底することが重要

ランサムウエア攻撃でバックアップが狙われると先述しましたが、もちろんバックアップに意味がないわけではありません。近年は、さまざまな業界団体の尽力により、暗号化されたデータを復号するための取り組みも進んでいます。ただし、それらで完全に復旧できるわけではないので、やはりバックアップや基本的なセキュリティ対策を含め、サイバー攻撃全体に対応していくアプローチを検討・構築することが重要です。そこではマルウエア対策、不正アクセス対策、脆弱性対策など、基本的な対策を確実かつ多層的に適用することが前提となります。例えば「情報セキュリティ白書2021」などでは、「新たなランサムウエア攻撃への対策」として、次の5つの対策をセキュリティ対策の基本として実行することを推奨しています。

1.「企業・組織のネットワークへの侵入対策（攻撃対象領域の最小化、アクセス制御と認証、脆弱性対策、拠点間ネットワークのセキュリティ強化、攻撃メール対策など）」

2.「ネットワーク内の侵害範囲拡大への対策（統合ログ管理、内部ネットワーク監視、エンドポイント監視など）」

3.「データの暗号化やシステム停止への対策（バックアップ、復旧計画の策定など）」

4.「データの窃取とリークへの対策（情報リスク管理：IRMの活用、ネットワーク分離など）」

5.「インシデント対応（CSIRT活動※2、ステークホルダーとのコミュニケーションなど）」

このように「ランサムウエア対策として何か特定のツールを導入する」という考え方ではなく、バックアップを含めたサイバーセキュリティ対策を事業継続や災害復旧の文脈から捉え直し、インシデントに素早く対応するための体制づくりを進めることが重要です。
※2…CSIRT（Computer Security Incident Response Team）とはセキュリティインシデントが発生した際に通知を受け取り、調査してその対応を行う組織体のこと

データの復旧にバックアップが機能しないことも

バックアップに関しても新しい考え方とアプローチが必要とされます。上述の5つの対策を「事前の予防策」と「事後の復旧策」という観点で分けた場合、バックアップは復旧策に該当し、いわば「最後の砦」としての役割を担います。予防策をすり抜けてくる脅威に対して確実に対処し、事業を継続できるようにすることが重要です。

しかし問題なのは、近年のランサムウエアは、こうした確実なデータ保護と復旧を妨害するところまで進化を遂げている点にあります。

例えば、長期間潜伏してバックアップデータを探し出し、ユーザーに適切にバックアップされていると誤認させながら、実際はバックアップデータ自体を暗号化し続けているケースがあります。ユーザーがランサムウエアに感染したと思ってバックアップをリストアすると、暗号化されたデータを戻してしまうことになります。

いつ感染したかに気付かないため、どのバックアップデータを使ってどの時点に戻せばよいかも分かりません。感染に気付いてから1日たっていても、2日前のデータを戻せばいいのか、1週間前のデータを戻せばいいのか、さらに1カ月前のデータが必要になるのか判断ができません。

また、確実にデータを復旧するためには、バックアップデータが感染していないことを証明する必要があります。もし感染した日時が特定できても、感染していないことが保証されなければ、復旧作業自体が大きなリスクをはらむことになります。

「ランサムウエア対策としてのバックアップ」に必要な6つのポイント… 続きを読む