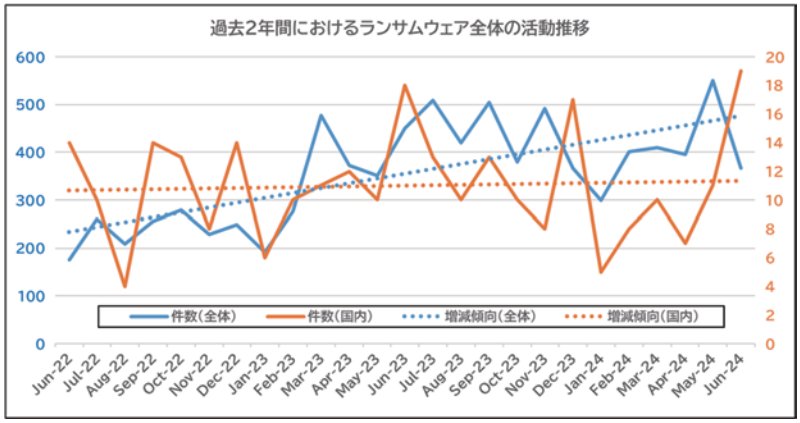
1. 拡大するランサム攻撃による被害：平時の対策と有事の対応方法

要約

- ランサム攻撃の被害が話題になっている。ランサム攻撃の被害に遭った場合、経済的な損失や評判の毀損など企業に多大な被害をもたらす。
- 攻撃者から要求される身代金については、法規制や復旧する保証がないことなどから、原則支払うべきではない。
- アップデートやバックアップなどの平時の対策に加えて、万が一発生した際にどのように対応するのか有事の対応方法について検討しておくことが重要。

ランサム攻撃による被害状況

ランサムウェアを代表とするサイバー攻撃を行い、身代金を要求するランサム攻撃による被害が大きな話題になっています。直近 2 年間のランサム攻撃の被害の件数としてダークウェブ上のリークサイトに掲載された企業数を調査したところ、右肩上がりで増加しているとするレポートもあります(*1)。また、情報処理推進機構(IPA)が公表している情報セキュリティの 10 大脅威(*2)においても、ランサム攻撃は 2021 年から 2024 年の 4 年間にわたり、組織に対する最大の脅威として位置付けられています。



出典：暴露型ランサムウェア攻撃統計 CIG マンスリーレポート 2024 年 7 月号（三井物産セキュアディレクション株式会社）(*1)を元に大和総研作成

ランサム攻撃を行う攻撃者の恐喝手法は、ランサムウェアによるデータの暗号化に加えて、窃取したデータをダークウェブ上のリークサイト上で公開すると脅す二重恐喝や、被害を受けた企業だけでなく、窃取した情報に含まれる個人や企業をさらに恐喝する三重恐喝など、多様化しています。

			
種別	(従来型)ランサムウェア	二重恐喝型ランサムウェア	三重恐喝型ランサムウェア
特徴	データの暗号化を行い、復号する代わりに身代金を支払うように要求する。	(従来型に加え、)身代金を支払わなければダウンロードしたデータを公開すると恐喝する。	(二重恐喝型に加え、)ダウンロードしたデータに含まれる個人・企業に対し、攻撃被害企業が身代金を支払わなければあなたのデータが公開されると間接的に恐喝する。

出典：大和総研作成 アイコンとして(*3)を使用

(*1) 暴露型ランサムウェア攻撃統計 CIG マンスリーレポート 2024 年 7 月号（三井物産セキュアディレクション株式会社）

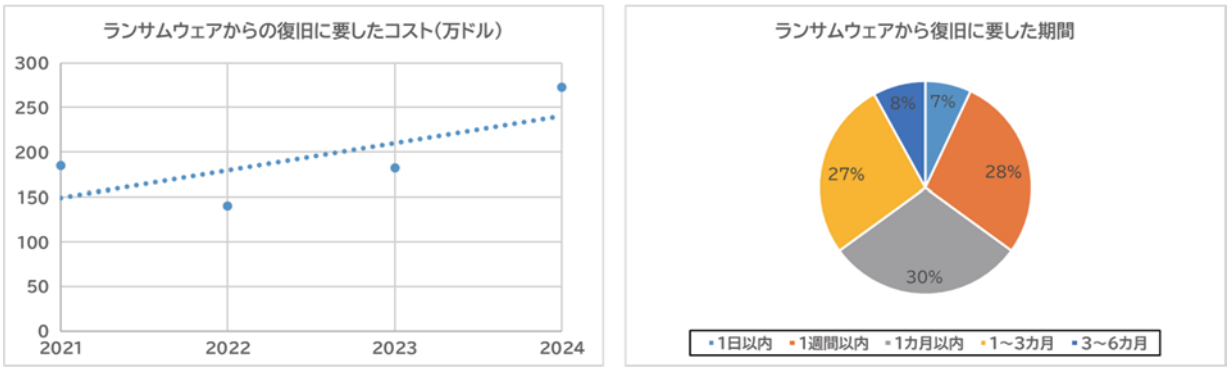
(*2) 情報セキュリティ 10 大脅威 2024（情報処理推進機構）

(*3) Dark web icons created by Freepik – Flaticon、https://www.flaticon.com/free-icons/speak

最近日本で発生したランサム攻撃による大きなインシデントとして、KADOKAWA とイセトーの事例があげられます。KADOKAWA は主に出版や動画サイトなどの B2C 事業を展開している企業で、ランサム攻撃による被害についてニュース記事や SNS で大きく報道されました。プレスリリース(*1)によれば、流出したデータには従業員情報だけでなく、KADOKAWA が運営する学校事業に関わる生徒の個人情報や、グループ会社の株式会社ドワンゴの取引先クリエイターの情報など、機微な情報も含まれていたとされています。一方、イセトーは B2B 事業を展開しており、情報処理業務を委託されている複数の自治体や銀行などの顧客の個人情報に関わるデータが流出したとされています(*2)。ランサム攻撃の被害発生当初は報道で多く取り上げられてはいませんでしたが、業務上の不備で個人情報が委託後も実際は削除されていなかったなど、被害状況が明らかになるにつれて、大きなニュースとして扱われるようになりました。

海外の大きなインシデント事例としては、米国の大手通信キャリアの AT&T の事例があげられます。AT&T は 2024 年の 4 月にランサム攻撃の被害を受け、同社のほぼ全ての顧客である約 1 億 1,000 万人ものアメリカ人の通信記録が窃取されました(*3)。攻撃者は当初、AT&T に対して流出したデータの削除のために 100 万ドル(約 1.5 億円)を要求しましたが、交渉の末、約 37 万ドル(約 5,600 万円)の支払いを行い、データの削除とデータを削除したことを示す動画を受け取ったとされています。なお、このインシデントの原因についてはセキュリティが不十分な SaaS サービスからのデータ流出とされています。企業の内部ネットワークには侵入されておらず、データの暗号化などランサムウェアは使用されていません。警察庁では今回のケースのようなランサムウェアを使用せずに、「窃取した情報を公開する」と恐喝するランサム攻撃をノーウェアランサム攻撃と呼んでおり、ランサム攻撃の多様化が進んでいる事例といえます。

これらの事例からも明らかなとおり、ランサム攻撃は経済的損害(ビジネス機会の喪失、復旧費用、身代金要求)、評判の毀損、時と場合によっては訴訟リスクをともなうこともあります。2024 年にランサム攻撃の被害を受けた企業の復旧には多くの場合、1 週間から 3 カ月の期間がかかり、平均の復旧費用は 273 万ドル(約 4.1 億円)にも及んでいるといったレポート(*4)もあります。身代金要求の観点については、次のセクションで詳しく取り上げます。



出典：ランサムウェアの現状 2024 年版 (Sophos)(*4)を元に大和総研作成

(*1) ランサムウェア攻撃による情報漏洩に関するお知らせ (株式会社 KADOKAWA)

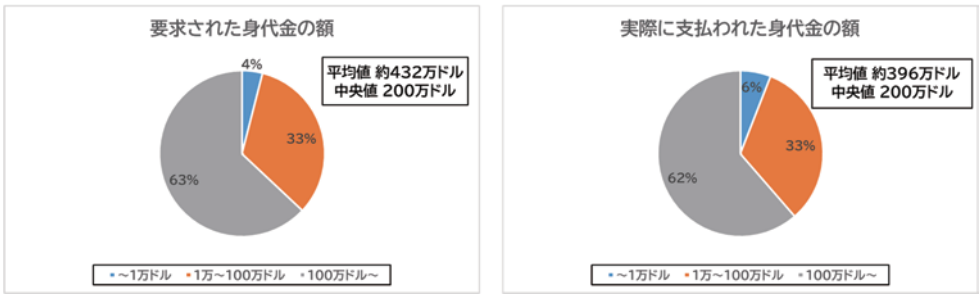
(*2) 「イセトー」にサイバー攻撃 委託元の約 150 万件の情報漏えいか (NHK)

(*3) AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records (WIRED)

(*4) ランサムウェアの現状 2024 年版 (Sophos)

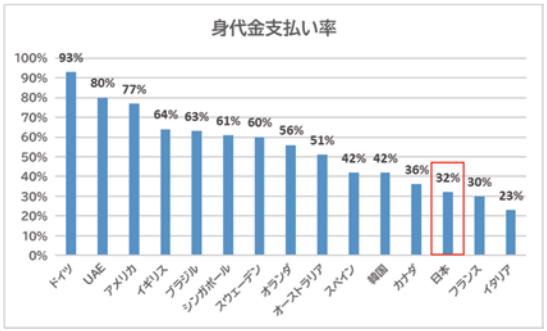
身代金要求の実態と対応

攻撃者からの身代金要求の実態は、世界的に見てかなり深刻です。前述のレポートでは、攻撃者から要求される金額の約 63%が 100 万ドル(約 1.5 億円)を超えており、その平均値は約 432 万ドル(約 6.5 億円)でした。実際に支払われた身代金の金額としては、中央値が 200 万ドル(約 3 億円)、平均値が約 396 万ドル(約 5.9 億円)となっています。企業が自社資産を用いて身代金を支払ったケースが最も多いものの、ランサム攻撃を含んだサイバー攻撃の被害を補償するサイバー保険も多く利用されていることが示されています。



出典：ランサムウェアの現状 2024 年版 (Sophos)を元に大和総研作成

一方で身代金支払い率の世界平均が 54%であるのに対し、日本の身代金支払率は 32%と低い水準となっているという調査(*1)もあります。これは、被害に備えたバックアップが取られていることや反社会的勢力に資金供与しない慣習もありますが、言語の壁で交渉が難しいことや、日本のサイバー保険の補償範囲に身代金支払いが含まれておらず資産調達ができないこと、また、身代金を支払ったとしても支払ったことを公表しない企業が多いことも理由として考えられます。



出典：ランサムウェア感染率/身代金支払率 15 カ国調査 2024(proofpoint)(*1)を元に大和総研作成

身代金の支払いに際しては、日本の外為法規制や米国の OFAC(Office of Foreign Assets Control)規制について把握しておく必要があります。外為法規制は、2001 年にアメリカで発生した同時多発テロを受けて、国際的にテロリストなどの犯罪者に資金供与を行わないようにするために強化されました。日本政府は、経済制裁を行っている対象者に対して政府の許可なく送金することを違法としています。現時点では、北朝鮮系のサイバー犯罪グループとして知られている“Lazarus Group”が経済制裁の対象として指定されています(*2)。米国の OFAC 規制は、特定の国や個人、団体に対する資金提供や取引を禁止する経済制裁を実施しており、経済制裁の対象には“Conti”や“TrickBot”と呼ばれるサイバー犯罪グループも含まれています(*3)。OFAC の規制は、米国内に居住する個人や企業だけでなく、米国の金融システムを利用する全ての取引にも適用され、これには、外国の金融機関が米ドルを使用する取引も含まれます。

攻撃者は通常、取引において身元を明かさないため、身代金を支払うことは外為法や OFAC の規制に抵触する可能性があります。また、身代金を支払ってもデータが復旧する保証がないことや、身代金を支払った企業だと知れ渡ることで別の攻撃者からも狙われる可能性もあるため、通常は身代金を支払うべきではありません。しかし、現実問題として、被害の状況によっては身代金の支払いが問題解決の手段の一つとなる場合があります。万が一、身代金を支払う必要があるかもしれないとなった場合でも、警察や弁護士などの専門家に相談を行うべきです。

(*1) ランサムウェア感染率/身代金支払率 15 カ国調査 2024 (proofpoint)

(*2) 経済制裁措置及び対象者リスト (財務省)

(*3) United States and United Kingdom Sanction Additional Members of the Russia-Based Trickbot Cybercrime Gang (Office of Terrorism and Financial Intelligence)

ランサム攻撃に対する平時の対策と有事の対応

これまで紹介したとおり、ランサム攻撃は多大な損害をもたらすため、平時からの予防策と有事の迅速な対応が求められます。本冊子でも取り上げている金融庁のガイドラインのように、各業界向けのガイドラインを確認することや、サイバーセキュリティに関する様々なフレームワークを取り入れるなど、網羅的な対策を継続的に行っていく必要があります。

ここでは、ランサム攻撃に対する平時における対策と有事の際の対応の観点としてそれぞれ記載しますので、ご参考にしていただければ幸いです。

平時の対策のポイント

対策箇所	対策観点
脆弱性対応	警察庁のレポート(*1)にあるとおり、ランサム攻撃の過半数が VPN 機器などの脆弱性が感染経路となっている。特にインターネットに接続している機器やサーバーの脆弱性については修正パッチ公開後、速やかに対応を行う必要がある。
有効なセキュリティ対策ソフトの導入	EDR や XDR などのランサムウェアの横展開を阻止するセキュリティ対策ソフトの導入が有効である。
有効なバックアップの実施	米国国土安全保障省配下の米国コンピュータ緊急事態対応チームが提唱するデータ保護の「3-2-1 ルール」など、定期的にバックアップを行いネットワークから切り離された形で保管するようにする。
適切なアクセス権限の設定と検知	最小権限の原則にのっとり、ユーザーに対して過剰な権限を設定しない。また、SaaS やクラウドのセキュリティ対策として、SSPM や CSPM を導入し、MFA の未設定や外部公開設定などのセキュリティ上のミスを検知する。
従業員への教育	ランサム攻撃の起点となるソーシャルエンジニアリングやフィッシングを防ぐために事例を交えた形で定期的にセキュリティ教育を行う。
ASM や脅威インテリジェンスの導入	インターネット上から不正にアクセスできる資産がないか確認するサービスを導入する。また、攻撃者がどういった手法でどのような企業をターゲットにしているか分析するサービスを導入する。 ※詳細は第3部で解説する。
インシデント対応計画の策定	有事に備え、従業員の対応や連絡フロー、感染後の復旧手順や身代金要求への対応方針などをまとめたインシデント対応計画の策定を行う。計画立案後はインシデント対応訓練などで有効性の検証を行うべきである。

有事の対応のポイント

対応箇所	対応観点
初動対応	横展開を防止するため、ランサムウェアが確認された端末・サーバーを隔離する。 ただし、フォレンジックのため、ランサムウェアを確認した端末のネットワーク抜線のみを行うか、電源自体を切るかについて事前に対応計画の中で検討しておくべきである。
被害状況の確認	ランサムウェアが確認された端末以外に被害がないか、ログなどから調査する。
関係者への報告	社内の関係者と社外の関係者(警察・IPA・JPCERT/CC・個人情報保護委員会・被害に遭った可能性がある企業など)に報告する。
復旧作業	隔離された端末・サーバー以外に被害がないことを確認した後に、バックアップから復旧を実施する。
フォレンジック	ランサムウェア攻撃についてどのように行われたのかログなどから調査を行う。
再発防止策の実施	フォレンジックの結果を元に、脆弱な箇所に対して対応を実施する。
情報の開示	自社ホームページやマスコミに対し、インシデントの内容について開示する。

（山崎　禎章）

(*1) 令和5年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）