サイバー攻撃の最新動向を踏まえた事前対策と体制整備について

～ランサムウェアの事例から学ぶインシデントレスポンスの重要性～

MS＆ADインターリスク総研株式会社
デジタルイノベーション本部スタッフ
スペシャリスト　遠藤 宣孝（えんどう のりたか）

要旨

- 近年、中小企業を狙ったサイバー攻撃が増加しており、特にランサムウェア攻撃による被害が多く発生している。
- 現在、ランサムウェア攻撃の大半がVPNやリモートデスクトップ経由の感染であり、これらの対策が必須である。
- サイバー攻撃の昨今の動向を解説し、特に中小企業に対するランサムウェア攻撃を想定した事前対策と対応方法、体制整備について解説する。

1 近年のサイバー攻撃の事例と動向

(1)サイバー攻撃の事例

近年サイバー攻撃に関するニュースが非常に多くなっている。特にランサムウェア攻撃と呼ばれる、データを暗号化し、さらには機密情報を窃取して、暗号化データの復旧や窃取した機密情報を公開しないことと引き換えに身代金を支払うことを強要する攻撃が被害を甚大化させている。表1は2024年の日本国内におけるランサムウェア攻撃の主な被害事例である。

ランサムウェア攻撃を受けた結果、顧客情報の漏えいや、数週間～数カ月にわたり業務が停止するようなケースが存在し被害が甚大化していることがわかる。

【表1】2024年の代表的なランサムウェア攻撃事例

時期	被害企業	被害内容
2024年2月	医療機関	ランサムウェア攻撃を受けた結果、救急と一般外来の受付を約2週間制限 30TBものデータが攻撃者によりアクセス可能であった可能性
2024年5月	情報処理	業務を委託していた地方自治体や金融機関などが影響を受け、全体で約150万件の個人情報が漏えい
2024年6月	出版社	グループ会社がランサムウェア攻撃を受けた結果、出版事業にも影響が及び約2カ月程度出版業務が停止 グループ会社においても同様にサービス停止に追い込まれ、約25万件の個人情報が漏えい
2024年6月	製造業	グループ会社がランサムウェアに感染、他グループ会社にも影響が拡大し、計7社がランサムウェアに感染 約32万件の個人情報が漏えい
2024年6月	コンサルティング	同グループ会社の顧客データを管理するサーバーでランサムウェア攻撃を受け、業務を委託していた会社の顧客情報が漏えい 約6万件の個人情報が漏えい
2024年7月	インフラ	グループ会社が不正アクセスを受け、業務を委託していた会社の顧客情報など約416万件の個人情報が漏えい

ランサムウェア攻撃の被害に遭った組織の経済的損失について公表されることは少ないが、平均2,386万円との調査結果をNPO日本ネットワークセキュリティ協会が公開している[1)]。同調査結果では被害組織の多くがデータ消失による利益の喪失、機会損失を正確に把握できていないとの報告もあり、実際の経済的損失は上記平均値を上回ると想定される。

なお、2024年6月にランサムウェア攻撃により甚大な被害を受けた出版社は、約36億円もの特別損失を計上している[2)]。

⑵狙われる中小企業とその理由

これらのランサムウェア攻撃の事例や、警察庁が発行した「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」[3)]で報告されているとおり、近年のサイバー攻撃の特徴の一つとして、グループ会社や業務委託先などの中小企業の被害が多い。

中小企業の被害が多くなっている理由の一つとして「セキュリティ対策にリソースをかけられない」ことがあげられる。中小企業は大企業と比較してセキュリティ対策にかける費用や人材などのリソースが不足しており、セキュリティ対策が遅れている傾向がある。例えば、製品を導入しても運用が追い付かずにプログラムの不具合や設定上のミスといったセキュリティの脆弱性を含んだバージョンを放置してしまい、結果として攻撃者に侵入されてしまったケースも多く存在する。

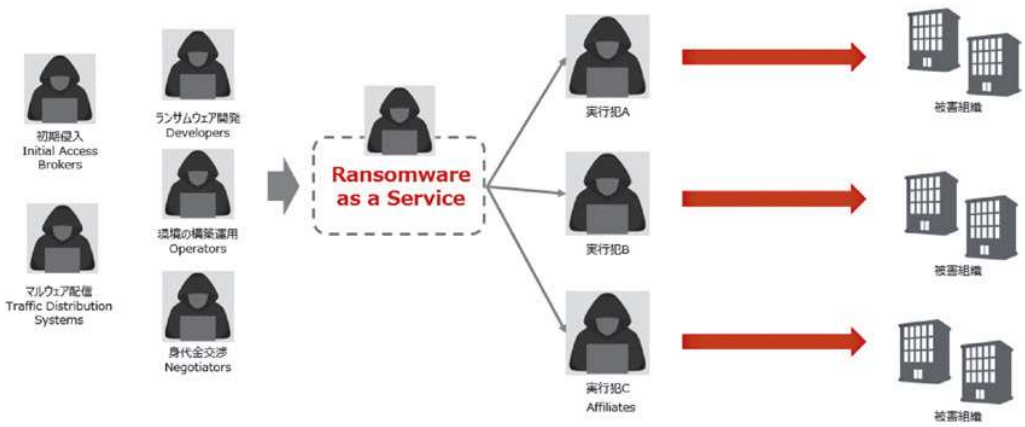
もう一つの理由として、サイバー攻撃のビジネス化により容易にサイバー攻撃を実行できる環境が整っていることがあげられる。これは攻撃側の役割や機能が細分化され、その個別の機能を攻撃者がさらに他の攻撃者に販売するというものである。具体的には、「被害企業への不正侵入の初期段階で必要となる情報や侵入経路を販売する者（Initial Access Brokers）」、「ランサムウェアの作成、実行環境を販売する者（Developers/Operators）」、「それらを利用して攻撃を行う実行犯（Affiliates）」など、様々な役割に応じて活動している。また、これらの機能をまとめて、より簡単に攻撃を実行できるようにサービス化し、販売している攻撃者も存在している。これはRansomware as a Service（以下、「RaaS」）と呼ばれ（図1）、数年前から報告されていたが、昨今はこのRaaSを利用した攻撃が多く報告されている。

攻撃の実行犯はRaaSの使用料を払うことで簡単に攻撃を行えるため、あえてセキュリティ対策がしっかりしている大企業を狙うより、セキュリティ対策が不十分で簡単に金銭を窃取できそうな中小企業を攻撃のターゲットとする傾向がある。活発な活動が報告されているLockBit、ALPHV（BlackCat）などのランサムウェアグループもRaaSの形態を取っており、世界全体で被害が発生している。

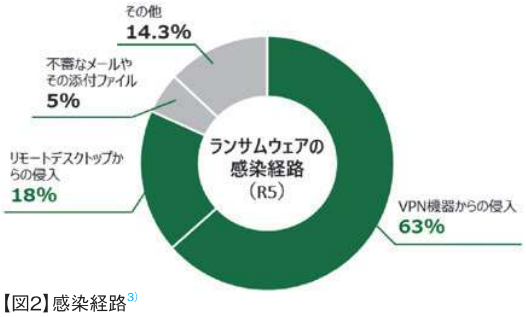
2 ランサムウェア攻撃の主な感染経路

現在、多くのランサムウェア攻撃の感染経路となっているものがVPN[注1)]やリモートデスクトップなどのリモートワークを想定したサービスである。前述の警察庁が発行した「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」の報告でもVPN機器とリモートデスクトップ経由の感染が全体の8割を占めており、多くの攻撃者がこれらのサービスを攻撃していることがわかる（次頁図2）。

コロナ禍以降、VPN機器を設置してリモートワークを採用する



【図1】Ransomware as a Serviceの概要



【図2】感染経路[3]

企業が増加した。当時は急いで導入した企業も多数存在しており、その結果適切に運用・設定できていない組織が多数あると考えられる。

【表2】問題となる運用・設定の例

問題となる運用・設定	内容
セキュリティを考慮していない設定	• IDとパスワードのみの認証 • 不要なアカウントの残存 • 不要なサービスの公開、アクセス制限の未設定
古いバージョンの使用	• 脆弱性を含んだバージョンを使用 • セキュリティ情報などの収集不足

(1)セキュリティを考慮していない設定

認証情報はダークウェブ上で売買されており、攻撃者は購入した認証情報を利用して、IDとパスワードのみで認証している正規ユーザーになりすまし、対象システムに不正アクセスしランサムウェアを感染させる。図3は日本企業の認証情報がダークウェブ上のマーケットに投稿されている例である[4]。なお、このような認証情報はユーザーが登録した外部サイトなどから漏えいした可能性もあり、パスワードの使いまわしなどにも注意が必要である。

【図3】ダークウェブ上のマーケットについて投稿[4]

このような売買されている認証情報以外にも、テスト用アカウントなどを悪用されたケースも多く存在する。

また、管理用サービスを無制限にインターネット上に公開しているケースも多く存在する。特にリモートデスクトップなどのリモートサービスは、メンテナンス目的で使用していると想定され、不特定のユーザーにアクセスさせる必要がないサービスである。

(2)古いバージョンの使用

認証方法が強固でも脆弱性を悪用されるケースが多く存在する。例えば、2024年1月16日にVPN製品であるIvanti Connect Secure(旧Pulse Connect Secure)の脆弱性が報告され、IPAやJPCERTなどからも注意喚起[5]が出された(表3)。攻撃者側は自動化された方法を通じて脆弱性が存在するVPN機器を無差別に探索し不正アクセスを試みたと考えられ、不正アクセスを試行した痕跡が多数報告されている[6]。このような脆弱性が報告された場合、「自社には盗まれるような情報がないから攻撃を受けることはないだろう」と考えて対応を後回しにすると、自社の脆弱なVPN機器を発見される可能性があるため早急な対応が必要である。

【表3】2024年1月以降のVPN製品関連の注意喚起(JPCERT)[7]

公開時期	注意喚起
2024年1月	Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性(CVE-2023-46805およびCVE-2024-21887)に関する注意喚起
2024年2月	Fortinet製FortiOSの境域外書き込みの脆弱性(CVE-2024-21762)に関する注意喚起
2024年4月	Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性(CVE-2024-3400)に関する注意喚起

3 サイバー攻撃に備えるために とるべき対策

このようなランサムウェア感染の原因を踏まえ、取るべき対策を次頁表4にまとめた。

(1)外部公開資産の洗い出しとセキュリティチェック

ランサムウェアの感染原因となる、不正侵入の足掛かりを特定するには外部に公開しているIT資産を総点検する。一つひとつ確認をするには時間と労力がかかる為、ASM(アタックサーフェスマネジメント)ツールと呼ばれる、攻撃にさらされる境界面にあるIT資産の脆弱性を診断するツールを活用することで、自社の弱点を効率的に特定することもできる。

【表4】サイバー攻撃の対策例一覧

対策	内容
外部公開資産の洗い出しとセキュリティチェック	ASMツールを利用した不正侵入の足掛かりとなる資産の洗い出しと脆弱性有無の確認
認証の強化	• 多要素認証（MFA）を使用 • 適切なパスワードポリシーの適用
アクセス権限の見直し	• テストユーザーなど不要なアカウントの削除・無効化 • 不要な管理者アカウントの削除・無効化
アクセス制限の実施	• リモートアクセスサービスのアクセス制限の実施 • 使用していないサービスの無効化
最新バージョンの継続的な使用	OS、アプリケーションなどのバージョンを最新の状態に保つ
不審メールの排除	• メールフィルタリングの導入 • 標的型メール訓練の定期的な実施 • 従業員への継続的な啓蒙
外部通信のフィルタリング	• 社内からインターネットへのアクセスの制限 • セキュリティ製品などによるフィルタリング
セキュリティソフトの導入	• ランサムウェアの動きを検知する製品の導入 • EDR／XDRの導入と監視
バックアップの取得	• 定期的なバックアップの取得 • 3-2-1ルールなどに基づいた適切なバックアップ • 復元テストの実施

⑵認証の強化

サイバー攻撃の手法が多様化している中、従来のIDとパスワードのみでは十分な安全性を確保することが難しい状況であり、近年では多要素認証の実装が推奨されている。特にVPNなど社内システムにアクセス可能なサービスについては多要素認証の実装が強く推奨される。

多要素認証とは、ID／パスワードの認証以外に一つまたは複数の要素を使用した認証である。例えば、IDとパスワードでログイン後、さらにメールやスマートフォンのアプリケーションに表示された認証コード（ワンタイムパスワードなど）を入力させる認証方法である。

多要素認証の実装が難しい場合は、「パスワードポリシーの強化」、「アカウントロックの設定」などを行う。

⑶アクセス権限の見直し

テスト用に作成したアカウントは、頻繁にログインしてテストを実施するため、簡易なパスワードが設定されていることが多い。このようなアカウントは本番運用時に削除する。その他にも退職者や異動した従業員のアカウントの削除もしくは無効化が必要である。

また、管理権限が付与されているアカウントを確認し、不要な管理者アカウントがあれば管理権限の付与を見直す。特にActive Directoryを利用したドメイン環境[注2)]では、ドメイン管理者権限が付与されているアカウントはドメイン管理下にあるすべての端末・サーバーに実質的にアクセス可能であり、攻撃者にこのアカウントを奪取されると組織内の全システムを掌握されてしまう。過去にはドメイン管理者のアカウントを奪取され、その後Active Directoryのグループポリシーを利用して、ドメイン管理下にあるすべての端末を暗号化した事例も存在する。したがって、管理者権限の付与は最低限のアカウントのみに限定することが必要である。

⑷アクセス制限の実施

リモートデスクトップなど管理者や関係者のみアクセスする必要があるサービスをインターネット上に制限なしで公開しているケースが存在する。具体的に以下のようなケースでは、アクセス元を確認しアクセス制限を実施する必要がある。

- リモートデスクトップやSSH（Secure Shell）などのリモート管理サービス
- FirewallやVPN機器などのネットワーク／セキュリティデバイスやWebサービスの管理画面
- 開発環境や検証環境などのテスト環境

など

リモートデスクトップは前述のとおりランサムウェアの感染経路として狙われている。各種デバイスやWebサービスの管理画面においても脆弱性が報告されることがあるため注意が必要である。なお、これらについては、本来管理者のみにアクセスさせるべきものであり、アクセス元を絞って制限する必要がある。

開発環境や検証環境は通常アクセス制限をしていると考えられるが、昨今のリモートワークの普及により自宅からアクセスする場合もあり、アクセス制限なしで公開しているケースも見受けられる。開発環境や検証環境は適切な認証方法で実装された踏

み台サーバーやVPN経由でアクセスできるように設定することが推奨される。

⑸最新バージョンの継続的な使用

日々様々な脆弱性が報告されており、インターネット上に公開されているサーバーの脆弱性を無作為に探索している攻撃者も存在するため、「自社には盗まれるような情報がないから攻撃を受けることはないだろう」と考えて対応を怠ることは危険である。使用しているソフトウェアや製品を洗い出し、危険度の高い脆弱性が存在する場合は迅速なバージョンアップやセキュリティパッチの適用を推奨する。

なお、IPA[8]やJPCERT[7]では危険度の高い脆弱性が報告された場合には注意喚起として情報をリリースしている。脆弱性のチェックにはこのようなサイトも活用する。

⑹不審メールの排除

現在、VPNなどのリモートアクセスサービス経由のランサムウェア感染が大半を占めているが、不審メール経由での感染も報告されている。このような不審メールについてはメールのフィルタリング製品が有効である。また、標的型メール訓練も一定の効果がある。定期的に標的型メール訓練を実施したとしても、不審メールのクリックをゼロにすることは難しいが、クリックした従業員による迅速な報告や感染時の対応方法などを理解させることは有用である。このような標的型メール訓練などを含めた従業員への啓蒙活動を継続的に実施する。

⑺外部通信のフィルタリング

ランサムウェアは感染後、暗号化キーのやり取りや窃取した情報を持ち出すために外部サーバーと通信を行う。そのため、内部ネットワークからインターネットへの通信を可能な限り制限することで、万が一ランサムウェアに感染した場合でも影響を最小限にとどめることができる。業務内容によってはこのような制限は難しい場合もあるが、インターネットの接続を限定できる業務内容の場合、必要なインターネット通信のみを許可する(ホワイトリスト形式によるフィルタリング)。

なお、平時の通信制限が難しい場合でも、ランサムウェア感染時には一時的に制限するなどして、影響拡大を防ぐことが推奨される。

⑻セキュリティソフトの導入

ウイルス対策製品によっては、プログラムの不審なふるまいを検知してブロックする機能がある(ふるまい検知機能など)。例えば、ランサムウェアのように複数ファイルを連続して暗号化するような特徴的な挙動を見て検知・ブロックする機能である。このような機能は、導入済みのウイルス対策製品に存在しているものの、初期設定では無効になっていることが多い。使用しているウイルス対策製品を確認し、このような機能も有効に活用する。なお、ふるまい検知機能は正規プログラムも誤って検知する場合があるため、十分な検証が必要である。

また、万が一感染した場合に早期に検知できるEDR(Endpoint Detection and Response)の導入も効果的である。EDRは実行プログラム/プロセス、ネットワーク通信、システムログ、ユーザアクティビティなど様々なデータを収集し脅威を検知する。ランサムウェア感染の早期検知のみでなく、その後のインシデント調査でもこれらのデータは有効である。

⑼バックアップの取得

万が一、ランサムウェア攻撃を受けファイルが暗号化されると、業務が停止し復旧までに時間がかかる可能性がある。定期的、かつ適切にバックアップを取得することが重要である。例えば、「3-2-1ルール」といわれるバックアップ方法は、「バックアップデータを3つ作成」し、「2つの異なる媒体で保存」して、「1つはオフライン環境で保管」する方法である。すべてのシステムでこのルールを適用することはコストの面で難しいと考えられるが、基幹システムの重要データではこのような方法でのバックアップも検討する。

また、バックアップの復元を事前にテストしておくことも重要である。例えば、バックアップは取得していたものの、「バックアップデータが壊れていて復元できなかった」、「復元方法がわからず復旧までに時間がかかってしまった」などのケースも存在した。このような事態にならないよう、復元テストの実施も必要である。

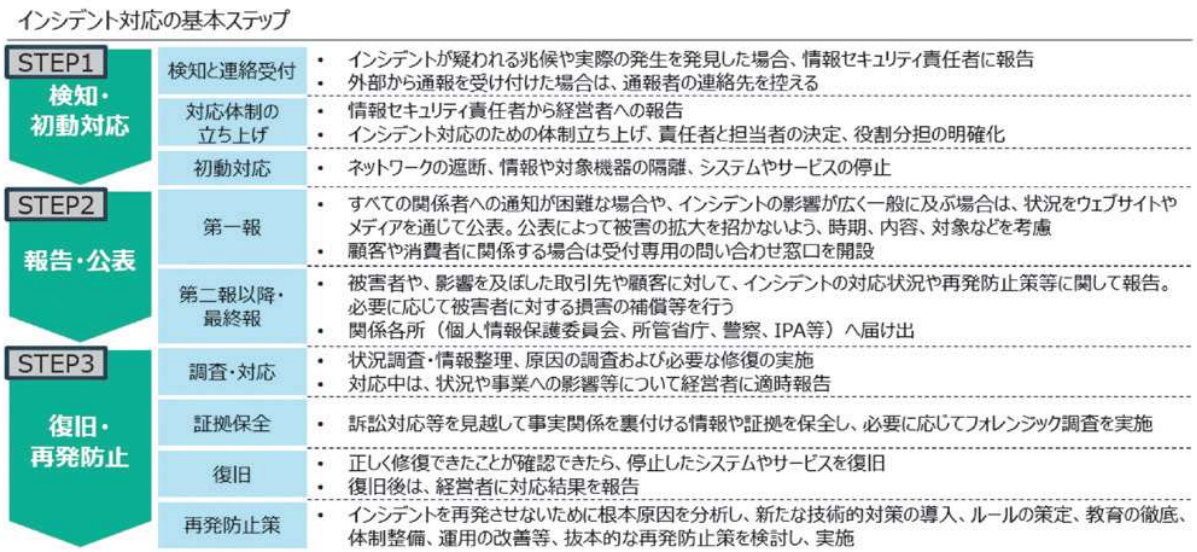
4 サイバー攻撃を受けた場合の体制

このような対策を実施していたとしても、セキュリティインシデントが発生する可能性をゼロにすることは難しい。インシデント発生時にどのように対応する必要があるのか、IPAの「中小企業のためのセキュリティインシデント対応の手引き[9]」を参考にしながら、ランサムウェアに感染した場合を例に対応方法について解説する(次頁図4)。

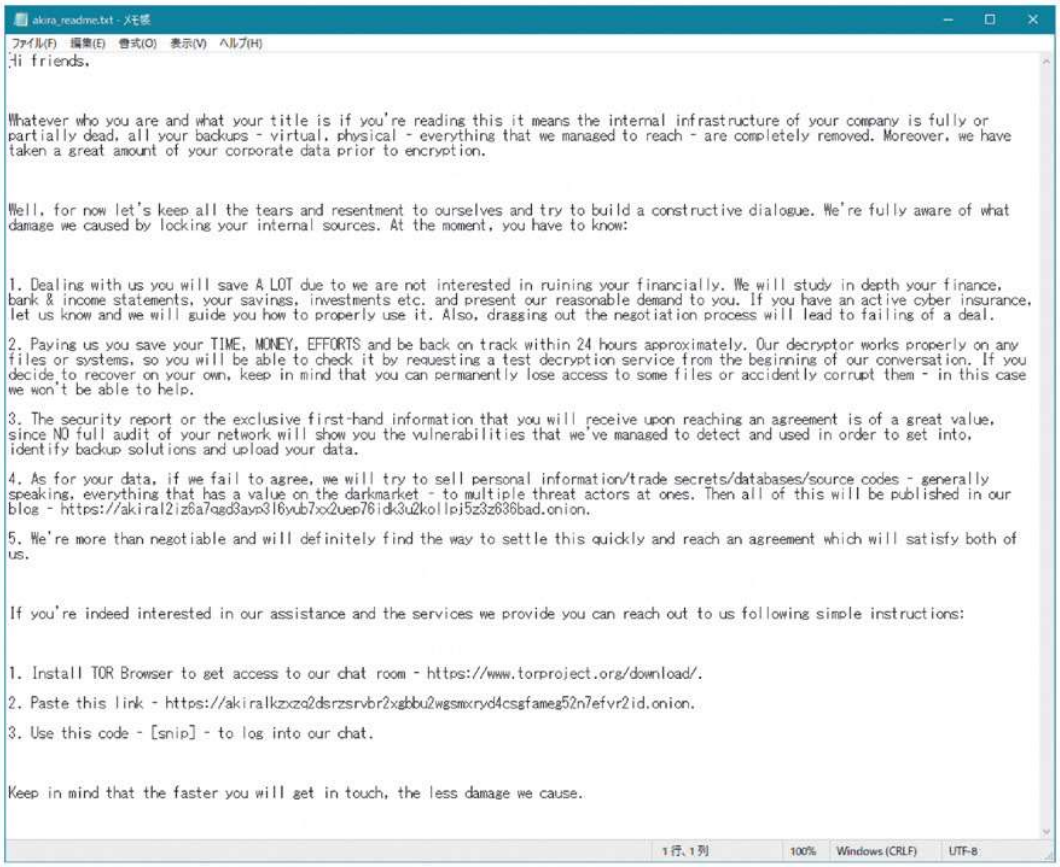
⑴STEP1 検知・初動対応

ランサムウェア攻撃を受けた場合は、ファイルが暗号化され、身代金を要求するようなテキストファイルやメッセージが表示される(次頁図5)。このような状況が発生した場合は、まず被害を最小限にするため、感染した端末をネットワークから切り離し、セキュリティ担当者および上司に早急に報告を行う。

セキュリティ担当者は、速やかに経営者に報告を行い、経営者



【図4】インシデント対応の基本ステップ[9]



【図5】Akiraランサムウェアの脅迫文の例[10]

は事業や顧客に与える影響を踏まえながら、インシデント対応体制（危機管理員会など）を立ち上げ、対応方針に従い、責任者と担当者を定め、役割分担を明確にする。

なお、どのようなインシデントを経営者に報告するべきか、深刻度の基準をあらかじめ定義しておくことで緊急時においても迷うことなく経営者に報告することができる（表5）。

【表5】深刻度の定義の例

深刻度	説明	例	一次報告先
高	非常に重大なインシデント	• 顧客情報の漏えい • 業務全体が停止	経営者 ※危機管理委員会の設置
中	重大なインシデント	• 自社情報の漏えい • 業務の一部が停止	事業部長
低	軽度なインシデント	• 情報漏えいを伴わない端末単体の感染 • 不審なファイルをクリックした結果、不審な通信が発生したがブロックした	セキュリティ部門長

⑵STEP2 報告・公表

影響を及ぼした取引先や顧客に対して発生したインシデントについて速やかに報告し、その後の調査で判明した事項を第二報、第三報として報告する。なお、二次被害が発生しないよう対応方法を伝えることも重要である。

また、個人情報の漏えいもしくはその可能性がある場合は、個人情報保護委員会に3～5日以内に速報として報告が必要である[11]。

インシデントの影響が広く一般に及ぶ場合はウェブサイトやメディアを通じて公表する。

⑶STEP3 復旧・再発防止

ランサムウェアに感染した場合、原因・影響範囲を特定する必要があるが、通常は自社でフォレンジック調査などの専門的な調査を実施することは難しい。そのため、事前に依頼する専門事業者を決めておくことで、インシデント発生時の調査依頼までの時間を短縮することができる。

また、No More Ransom[12]というサイトには、暗号化されたファイルの復号ツールが公開されている可能性もあるため、専門事業者と相談のうえ活用する方法もある（図6）。しかし、すべてのランサムウェアに対応しているものではなく復元できない場合も多い。なお、データの復旧にはバックアップが必須であるとの認識は必要である。

また、特定できた原因から再発防止策を立案し実施する。再発防止策には、設定変更などすぐに対応できる対策と、ソリューションの導入など中長期的な対策があるため、適切な再発防止策を立案し関係者に説明することも重要である。

【図6】No More Ransomで公開されている警察庁が作成したLockbit 3.0の復号ツール[12]

5 事前の体制整備の重要性

ランサムウェア感染に限定した対応だけでも表6に記載のように事前準備が必要な事項が多く存在する。

特に現場担当者と経営者とのコミュニケーションは重要である。現場担当者は、平常時から経営者を巻き込み、体制整備や机上訓練など行い、緊急時にどのような役割で対応するのか、どのような報告が必要となるのか、双方の理解を深めることが重要である。また、経営者としては、総務省の「サイバーセキュリティ経営ガイドライン[13]」を参考にしつつ、セキュリティ対策は経営課題であるとの認識を持ち、積極的な関与が必要である。

【表6】インシデント対応の事前準備の例

事前準備事項	内容例
インシデント発生時の連絡体制	インシデント発生時、誰がどこに連絡するか事前に連絡表を作成
深刻度の定義	インシデントの深刻度を定義し、深刻度に応じたエスカレーションを行う
危機管理委員会の設置	• 危機管理委員会を設置する基準の策定 • 責任者と担当者、役割分担の明確化
インシデント対応方針	• 発生したインシデントに対して、どのような初動対応を行うかなどのマニュアルの整備 • ランサムウェア感染では、攻撃者の要求に応じないなどの方針決定
インシデントの外部向け報告・公表	• 外部向け報告・公表の基準作成、報告・公表方法の整備 • 関係各所（個人情報保護委員会、所管省庁など）への届け出方法の確認
外部専門事業者の確保	フォレンジック調査などを実施する専門事業者との事前契約や依頼
復旧方法・インシデント終息の基準	• インシデントに応じた復旧方法の策定 • インシデントの終息宣言を出す基準の策定

以上

（出典の記載のない図表はすべてMS&ADインターリスク総研作成）