事業継続を揺るがすサイバー攻撃の脅威

～深刻化するマルウェア攻撃の手口と鉄壁の防衛戦略～

ライフデザイン研究部 主席研究員/テクノロジーリサーチャー 柏村 祐

1.あなたの企業が標的になる

企業のシステムが突如停止し、画面に身代金を要求するメッセージが表示されるような事態は、決して他人事ではない。

実際に、国内の大手飲料メーカーでは基幹システムが停止し出荷業務が滞る事態が発生した。また、大手物流企業では受発注システムが機能不全に陥り、取引先企業や一般市民にまで影響が波及した。医療機関では電子カルテシステムが暗号化され診療に支障をきたし、教育機関でも授業運営に混乱が生じるなど、その影響は社会インフラ全体に及んでいる。

これらの攻撃の正体が、ランサムウェアと呼ばれるマルウェアだ。マルウェア（malware）とは、「malicious（悪意のある）」と「software（ソフトウェア）」を組み合わせた造語で、悪意のあるソフトウェアの総称である。ランサムウェアはその一種で、コンピュータ内のファイルやシステムを暗号化して使用不可能にしたうえで、復旧と引き換えに身代金（ransom）を要求する。これは単なるITトラブルではない。事業継続を脅かし、顧客の信頼とブランドを一瞬で失墜する大きな経営リスクである。

事実、その脅威は年々深刻さを増している。警察庁の発表によると、2025年上半期におけるランサムウェアの被害報告件数は116件にのぼり、半期ごとの件数としては過去最多タイを記録している。さらに、被害を受けた企業のうち約3分の2を中小企業が占めており、大企業だけでなく、あらゆる規模の組織が標的となっている実態が浮き彫りになった。また、情報処理推進機構(IPA)が発表した「情報セキュリティ10大脅威 2025」においても、「ランサムウェアによる被害」は組織編で5年連続の第1位となっており、その脅威が社会全体にとって極めて深刻なレベルに達していることを示している。

本レポートは、その脅威の実態に迫り、我々が取るべき道筋を提示することを目的とする。

2.なぜ企業の防御網は突破されるのか？

堅牢なはずの企業システムが、なぜ容易に侵入されてしまうのか。その背景には、攻撃者の手口が巧妙化・多様化している現実と、防御する側に「想定外の穴」が存在

するという、二つの側面が複雑に絡み合っている。

攻撃の糸口は、単純なウイルス付きメールだけではない。VPN 機器の脆弱性、信頼している取引先、さらには何気なく閲覧したウェブサイトまで、あらゆる場所が侵入口となり得る。攻撃者は、企業の防御網の中で最も弱い一点を執拗に探し、そこから内部へと侵食してくるのである。

1)巧妙化する侵入経路

マルウェアの主な侵入経路は以下の通りである（図表 1)。

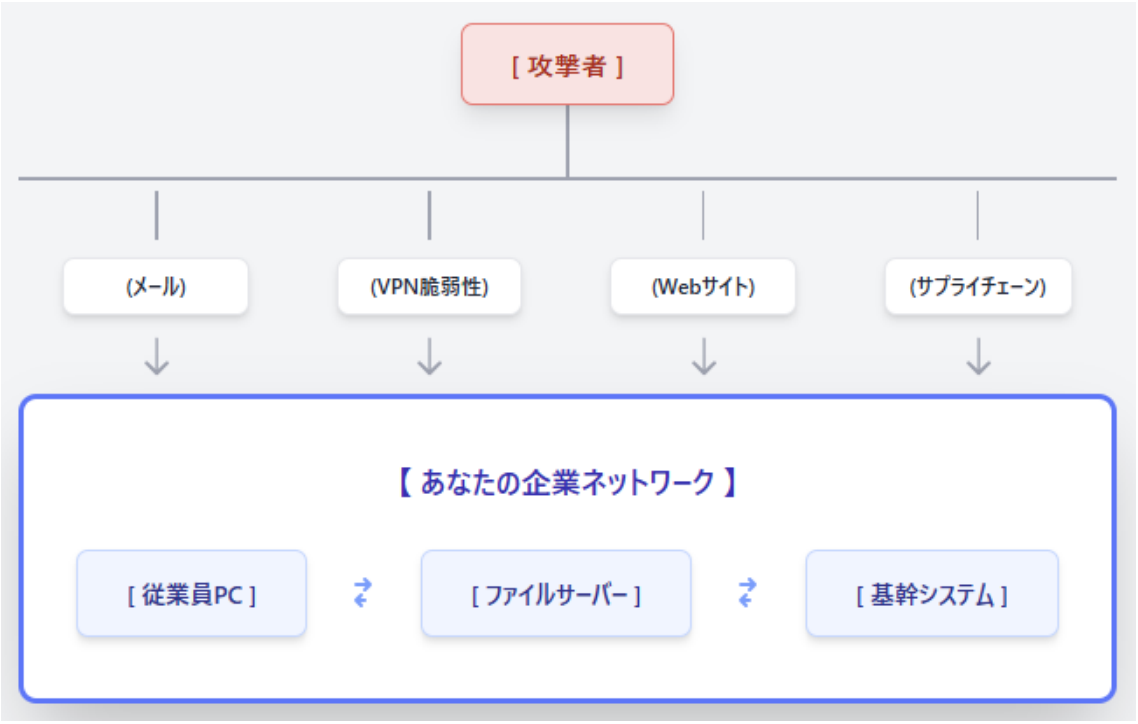
まず最も古典的かつ依然として最も多い感染経路が E メールである。業務連絡や取引先を装ったメールに添付されたファイル(請求書や見積書を偽装した Word/Excel ファイルなど)を開かせたり、本文中の URL をクリックさせたりしてマルウェアに感染させる。近年では、過去に実際にやり取りしたメールの文面を悪用する「Emotet」のような、極めて真偽を見分けがたい手口が猛威を振るった。

次に、リモートワークの普及に伴って主要な標的となっているのが VPN 機器等の脆弱性である。社外から社内ネットワークへ接続するための VPN(Virtual Private Network)機器において、公開されている機器のソフトウェアが古いまま放置されていると、その脆弱性を突かれて直接ネットワーク内部に侵入されてしまう。

さらに、自社のセキュリティ対策が強固であっても油断できないのがサプライチェーン攻撃である。取引先や子会社など、関連するセキュリティの甘い組織を踏み台にして侵入する手口で、信頼している相手からの連絡やデータ送信の機会を悪用し、相手の警戒が緩みがちな心理を巧みに利用する。

加えて、一般的なウェブサイトが改ざんされ、閲覧しただけでマルウェアに感染する「ドライブバイダウンロード」攻撃や、偽の警告画面を表示して偽のセキュリティソフトをインストールさせる手口などもある。

図表１　主なマルウェア感染経路



資料：筆者作成

2)企業の活動を蝕むマルウェアの正体

ひとたび内部への侵入を許すと、マルウェアはその種類に応じて様々な破壊活動を開始する。特に企業にとって脅威となるのは、以下のマルウェアである(図表 2)。

中でも企業の活動に最も致命的なダメージを与えるのがランサムウェア(身代金要求型ウイルス)である。サーバーや PC 内のファイルを勝手に暗号化し、使用不能な状態にしてしまう。そして、その解除(復元)と引き換えに、高額な身代金を要求する。

近年では、データを暗号化するだけでなく、事前に窃取した機密情報を「暴露する」と脅迫する「二重恐喝(ダブルエクストーション)」が主流となっており、たとえバックアップからシステムを復旧できたとしても、情報漏洩という深刻な事態に直面する。

また、PC に保存された ID・パスワード、メール情報、機密文書といった価値のある情報を盗み出す情報窃取型マルウェア(Emotet、スパイウェア等)も大きな脅威である。盗まれた認証情報は、さらなる不正アクセスや他のシステムへの侵入に悪用される。感染しても目立った症状が出ないことが多く、気づかないうちに長期間にわたって情報を盗まれ続けるケースも少なくない。

さらに、感染した PC を攻撃者の意のままに操れる「ゾンビ PC」に変えてしまうボット(遠隔操作ウイルス)にも注意が必要である。これは、他の企業へのサイバー攻撃の踏み台にされたり、迷惑メールの大量送信に悪用されたりすることで、自社が「加害者」になってしまうリスクをはらんでいる。

図表 2　マルウェアの種類と企業への影響

マルウェアの種類	主な目的	企業への影響(被害)
ランサムウェア	データの暗号化と身代金の要求、データの暴露	事業停止、復旧コスト、身代金支払い、情報漏洩による信用の失墜
情報窃取型マルウェア	ID/パスワード、機密情報、個人情報の窃取	機密情報の漏洩、顧客情報の流出、不正アクセスによる二次被害
ボット	PCの乗っ取りと遠隔操作	サイバー攻撃への加担、迷惑メールの送信元となることによる信用失墜

資料：筆者作成

そして、これらの技術的な脅威に加え、最も根本的な原因となっているのが、「人の脆弱性」である。OS やソフトウェアの更新を怠るといったシステム管理の不備はもちろん、「自分は大丈夫」「うちのような中小企業は狙われない」といった過信や、不審なメールに対する警戒心の欠如、単純なパスワードの使い回しといった従業員一人ひとりのセキュリティ意識の隙間こそが、攻撃者に絶好の侵入機会を与えている。

これら一つ一つの穴が、堅牢なはずの企業の壁を崩壊させる要因となる。攻撃者は、もはや特定の企業を狙うのではなく、インターネット上で無差別に脆弱な「穴」を探し、見つけ次第攻撃を仕掛けてくる。つまり、対策を怠っていること自体が、最大のリスクとなっている。

3.アナリストが示す鉄壁の防御網

第 2 章で明らかにした巧妙かつ複合的な脅威に対抗するには、単に高性能なセキュリティ製品を導入するだけでは不十分である。必要なのは「多層防御」というアプローチである。これは、複数の防御壁を重ね合わせることで、仮に一つの対策が破られても次の対策が脅威を食い止めるという考え方だ。本章では、図表 3 に示すように、技術的対策、組織・人的対策、サプライチェーンでの連携、そして社会レベルでの取り組みという 4 つの防御層を組み合わせた総力戦の体制を提示する。この重層的なアプローチこそが、進化し続けるマルウェア攻撃に対する唯一の有効な処方箋である。

図表 3　企業が構築すべき「多層防御」の概念図

資料：筆者作成

1)技術的対策:システムの要塞化

まず、基本となるのがサイバー攻撃の侵入を防ぎ、万が一侵入されても被害を最小化するための技術的な防御壁である。

第一に、最新の脅威情報を反映したファイアウォールや、不審なメール・Web サイトからのアクセスをブロックするフィルタリングシステムの導入は基本中の基本である。同時に、マルウェアが外部と行う不正な通信を検知・遮断する「出口対策」も強化し、情報を外部に持ち出させない仕組みを構築する必要がある。

しかしながら、100%の防御は不可能である。そこで「侵入はされうるもの」という前提に立ち、侵入後の検知と対応を迅速化することが極めて重要になる。従来のウイルス対策ソフトに加え、PC やサーバーの不審な挙動を検知・分析する EDR(Endpoint Detection and Response)の導入は、もはや現代のビジネスにおける必須装備といえるであろう。

また、攻撃者は OS やソフトウェアの「脆弱性」という名の綻びを狙ってくる。使用

している PC やサーバー、ネットワーク機器のソフトウェアを常に最新の状態に保つ「パッチ管理」を徹底することが、最も基本的かつ効果的な防御策の一つである。

そして特にランサムウェア対策において、事業継続の生命線となるのがデータのバックアップである。ただし、単にバックアップを取るだけでは不十分である。攻撃者がアクセスできないよう、ネットワークから隔離された場所(オフライン)に保管し、いざという時に本当に元に戻せるかを確認する「復旧訓練」を定期的に実施することが不可欠である。

2)組織・人的対策:防衛文化の醸成

最新のシステムを導入しても、それを使う「人」や「組織」に隙があれば意味がない。セキュリティは IT 部門だけの仕事ではなく、全社で取り組むべき文化として根付かせる必要がある。

何よりも重要なのは、全社員に対するセキュリティ教育の徹底である。セキュリティ対策はコストではなく、事業継続のための「必要コスト」である。具体的な教育プログラムを構築し、継続的に運用する仕組みを整備することが、全ての対策の出発点となる。新入社員研修での基礎教育の必須化、部門別・役職別のカスタマイズ研修、e ラーニングによる最新情報の定期配信など、対象者や内容に応じた多層的な教育体制を確立する。さらに、理解度テストによる習熟度測定や、インシデント事例の社内共有により、実効性を高めることが求められる。次に、被害が発生した際に誰が何をどのように行うのか、この手順を定めた「インシデント対応計画」を事前に策定し、CSIRT(シーサート)(注 1)のような専門チームを組織することが重要である。これによりパニックを防ぎ、被害を最小限に食い止めることができる。攻撃者にとって最も狙いやすいのは、システムの脆弱性よりも「人の心の隙」である。実際に偽の攻撃メールを送って対応を訓練する「標的型攻撃メール訓練」などを定期的に実施し、組織全体の「デジタル免疫力」を高めることも効果的である。

3)サプライチェーンでの連携

自社だけを守っても、ビジネスは成り立たない。取引先との連携により、ビジネスエコシステム全体で防御網を築くことが重要である。

セキュリティの強度は「最も弱い部分」に依存する。これは「チェーンの強度は最も弱い環=リンクで決まる」という原則と同じで、たとえ自社が万全の対策を講じていても、セキュリティ対策が脆弱な取引先を経由して攻撃者が侵入してくる可能性があるということだ。実際に、取引先の中小企業を踏み台にして大手企業が攻撃を受ける事例が相次いでいる。したがって、自社だけでなく、重要な取引先や業務委託先にも一定のセキュリティレベルを求め、サプライチェーン全体で脅威に立ち向かう視点が不可欠である。また、万全の対策を講じても被害に遭う可能性をゼロにすることはで

きない。万が一の際の事業停止損失や賠償責任に備え、その経済的ダメージを補填するサイバー保険への加入を検討することも、有効な経営判断の一つである。

4)社会レベルでの取り組み

企業による個別の対策に加えて、社会全体でセキュリティ水準を底上げする仕組みも重要である。

政府や公共機関は、サイバーセキュリティ基本法をはじめとする法整備を進め、企業に一定のセキュリティ対策を義務付けるとともに、違反に対する罰則を設けることで、社会全体の防御レベルの向上を図っている。また、重要インフラの防護体制の強化や、中小企業向けの支援制度の拡充など、公的な支援体制も整備されつつある。

さらに、業界団体や JPCERT/CC、警察などが発信する最新の脅威情報や脆弱性情報を常に収集し、自社の対策に活かすプロアクティブな姿勢が重要である。単独で行うのではなく、専門家の知見も積極的に活用すべきである。一般市民に対しても、学校教育やメディアを通じた啓蒙活動により、基礎的なセキュリティリテラシーの向上が図られるようになってきた。サイバー攻撃は企業だけの問題ではなく、社会全体で取り組むべき課題であるという認識が広がりつつある。

これらの対策は単独では不完全であり、相互に連携させることでより強い効果を発揮する。技術的な要塞を築き、全従業員が門番としての意識を持ち、サプライチェーン全体で連携し、社会的な支援体制も活用する。この「多層防御」の考え方こそが、本章で示す防御網の核心である。

なお、セキュリティ対策は、一度行えば終わりというものではない。攻撃者の手口が日々進化するように、この多層防御の仕組みもまた、継続的な見直しと改善を続けていかなければならない。脅威の進化に応じて各層の防御を強化し、新たな防御層を追加していく。この終わりなき改善と進化の姿勢こそが、見えざる敵から企業の貴重な資産と信頼を守り抜くための唯一の道となる。

【注釈】

1) CSIRT(シーサート): Computer Security Incident Response Team の略。
セキュリティインシデントが発生した際に、迅速かつ適切に対応するための専門組織。インシデントの検知、分析、対応、復旧、再発防止までを一元的に担う。