特集 **経営リスクとしてのサイバー脅威**

企業価値を守るランサムウエア対策
侵入を前提とした備えと経営に求められる意思決定



篠原　隆

CONTENTS

Ⅰ　ランサムウエアは「経営を止める」脅威である
Ⅱ　実際の被害事例に見るランサムウエアの影響
Ⅲ　被害事例から得られる教訓
Ⅳ　技術面の最新動向：侵入を前提とした備え
Ⅴ　組織面の備え：経営として準備すべき対策事項
Ⅵ　まとめ：経営としてどう向き合うべきか

要　約

1　ランサムウエアは、企業経営に重大な影響を与えるサイバー脅威として深刻化している。近年は、システムやデータを暗号化して身代金を要求するだけでなく、窃取した情報を公開すると脅迫して金銭を要求する二重脅迫が一般化している。さらにRansomware as a Service（RaaS）の普及によって攻撃者の裾野が広がり、攻撃件数と影響範囲は急速に拡大している。

2　被害事例を見ると、VPN機器の脆弱性悪用に加え、委託先を起点としたサプライチェーン経由など侵入経路が多様化している。EDRで検知が困難な攻撃やバックアップまで暗号化される事例も確認されており、復旧までに長期間を要する傾向がある。2025年には国内大手企業でも被害が発生し、事業停止や信頼低下など経営への影響が顕在化した。

3　本稿では、こうしたランサムウエア攻撃の最新動向を解説するとともに、ランサムウエア被害に遭った企業の復旧・支援活動を通じて得られた知見を踏まえ、被害事例から得られる教訓を整理する。ランサムウエア対策を、事業継続と企業価値を守るリスク管理として位置づけ、マイクロセグメンテーション・NDR・サイバーリカバリー製品の活用といった技術的施策に加え、インシデント対応体制整備や取引先を含めた統制などの組織的対応など、経営として取り組むべき対策を提示する。そのうえで経営による強力なリーダーシップの下、セキュリティ対策に関する意思決定の重要性を提言する。

Ⅰ ランサムウエアは「経営を止める」脅威である

ランサムウエアは、単なる情報セキュリティ上の脅威を超え、企業の事業継続や企業価値に直接的な影響を及ぼす存在となっている。近年では、業務停止や情報漏洩にとどまらず、対外的な説明責任や資金的負担を含め、経営判断そのものが企業の将来を左右するケースが増えている。本章では、ランサムウエアがセキュリティ脅威の中でも特に経営のトップリスクとして捉えられている背景や理由を解説する。

1 ランサムウエアの攻撃手法とその変化

ランサムウエア攻撃とは、企業が保有するシステムやデータを暗号化し、情報システムの利用を停止させたうえで、復旧と引き換えに身代金を要求する攻撃手法である。現在ではこれに加え、事前に窃取した機密情報を公開すると脅迫して金銭を要求する二重脅迫が常態化しており、被害企業は暗号化による業務停止と情報漏洩という二重のリスクに同時に直面することとなる。

数年前までのランサムウエアは、ウイルスを添付したメールを機械的にばらまく無差別型の攻撃が主流であり、個別のPCやサーバのデータが暗号化される一時的な障害として処理されるケースが多かった。しかし現在の攻撃は、確実に金銭を獲得することを目的に、企業環境に侵入した後、内部での情報収集を経て攻撃を実行する形へと変化している。攻撃者は企業ネットワークに侵入し、認証情報や管理権限を奪取したうえで、ネットワーク内の端末やサーバを一斉に攻撃するという計画的な手法を採るようになった。

さらに、侵入後も長期間にわたって潜伏し、ネットワーク構成や重要資産を把握したうえで攻撃を実行するなど、手法自体も高度化している。加えて、正規の管理ツールを悪用した検知回避や、管理権限を利用した横展開といった手口により、従来の対策に加えてより高度なセキュリティ対策を講じなければ検知・防御が困難な攻撃が増加している。

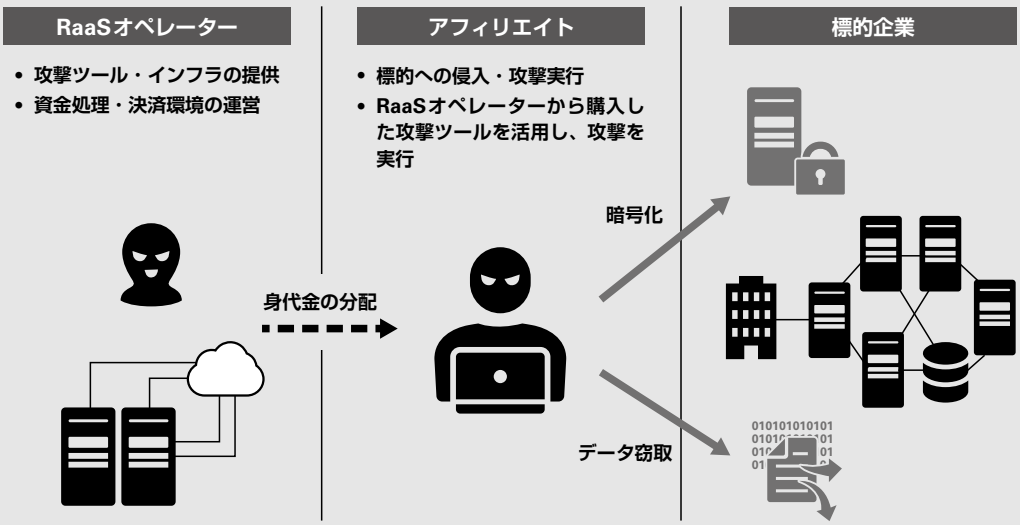
2 RaaSの普及と攻撃の裾野拡大

こうした攻撃の高度化と拡大を加速させている要因の一つが、Ransomware as a Service（RaaS）と呼ばれるビジネスモデルの普及である。RaaSとは、ランサムウエアの開発・運営を行う者（オペレーター）が、攻撃の実行者（アフィリエイト）にランサムウエアなどの攻撃ツールや決済環境などのインフラを提供し、被害者から回収した身代金のうち、手数料を差し引いた金額をアフィリエイトに報酬として分配するサービス形態である（図1）。

この分業体制により、高度な技術を持たない攻撃者でも大規模な被害を与えることが可能となった。また、侵入に必要な認証情報の入手や脆弱性情報の収集、身代金の交渉やロンダリングなどの資金処理・決済環境も組織化・ビジネス化され、攻撃者の裾野は急速に拡大した。

ランサムウエアによる攻撃は世界的に増加している。近年の調査では、ランサムウエアは全データ侵害の約44%に関与しており、サイバー攻撃の主要な類型となっている。また、被害件数自体も前年比で約58%の増加が

図1　RaaSの分業体制



報告されている。これらの結果は、ランサムウエアが特定の業界や地域に限定された脅威ではなく、あらゆる企業にとって現実的なリスクであることを示している。

さらに、被害を受けた企業の対応として、身代金支払いは依然一定数存在する。英国のサイバーセキュリティ企業ソフォスが世界17カ国3400組織を対象に実施した調査では、被害企業の約46％が身代金を支払っていると報告されている[注1]。

しかし、身代金の支払いが復旧を保証するわけではない。米国のエンタープライズセキュリティ企業プルーフポイントが15カ国を対象に実施した調査では、１回目の身代金の支払いでデータやシステムを復旧できた企業はグローバル平均で約41％にとどまり、日本に至っては17％という結果が示されている[注2]。

このような攻撃手法の高度化とRaaSの普及を背景に、攻撃の目的も「事業の完全な停止」と「窃取データの公開を伴う二重脅迫による利益の最大化」へと変化している。影響範囲は個別端末にとどまらず、企業のネットワーク全体やサプライチェーンにまで及ぶ「事業停止」を狙う攻撃へと移行している。

3　ランサムウエアが経営課題である理由

ランサムウエア被害は、情報システムの問題にとどまらず、事業継続・顧客信頼・ブランド価値に直結する経営リスクである。2025年度の被害事例を見ると、Ａ社（大手飲料・食品メーカー）では基幹システムが暗号化され、国内グループ会社全般にわたり受注・出荷業務が停止した。同社の国内事業における１日当たりの利益は数億円規模とされ、復旧までの損失は甚大であった。

Ｂ社（大手EC・物流企業）においては倉庫管理システム（WMS）が暗号化され、物流センターの入出荷業務が不能となった結果、コア事業であるECサービスが全面停止し、１日当たり億円単位の営業利益を棄損したと報告されている。さらに同社の被害は、

表1　ランサムウエアによる被害事例一覧

企業・業種	侵入経路	攻撃手法	復旧期間	経営インパクト	教訓
A社 （大手飲料・ 食品メーカー）	発覚の約10日前に侵入。主に業務時間外に複数サーバへの侵入と偵察を繰り返す	週明けの朝という影響が大きいタイミングを狙い、ランサムウエアを一斉実行。基幹システムを暗号化	短期間（縮退運用により早期回復）	国内グループ会社全般で受注・出荷が停止。１日当たり数億円規模の利益喪失。店舗の棚から商品がなくなり、同業他社へも影響波及	EDRなどの導入だけでは進行プロセス全体を防げない。一方で、手作業による縮退運用へ速やかに移行する判断が功を奏し、主力事業への影響を売上１割減にとどめた
B社 （大手EC・物流企業）	例外的にMFA（多要素認証）を適用していなかった業務委託先アカウントを起点とし、発覚の約４カ月前に初期侵入	事前にEDRなどの対策ソフトを無効化。ランサムウエアの実行と同時にバックアップファイルも削除	既存環境を破棄し、ゼロから新環境を構築したため、主要サービスの復旧完了まで約3.5カ月を要した	WMS暗号化により物流・ECサービス全面停止。月間売上高が前年同月比95％減。被害総額100億円超過	ランサムウエア攻撃を想定したバックアップ環境が構築されていなかったことが復旧長期化の最大の原因。また、サプライチェーンを含めた委託先アカウントの統制徹底が不可欠
C社 （業務委託事業者）	委託先事業者経由の侵入	自社を直接狙うのではなく、委託先環境を踏み台にした侵入	暗号化データの復元は不可と判断し、新システムへ移行。事態収束までに数カ月以上を要した	最終的に数百万件規模の個人情報が漏洩。委託元である金融機関や自治体など、多数の組織へ被害が連鎖	委託先の被害が自社や顧客の重大インシデントに直結するため、委託先契約にセキュリティ要件を明記し、定期的な評価を実施するなどサプライチェーン全体の実効性ある統制が不可欠
D社 （大手コンテンツ企業）	フィッシング攻撃により、従業員のアカウント（認証情報）が窃取されたことが初期侵入の起点	ADを奪取し、仮想化基盤などを含む複数サーバを一斉暗号化。Windows標準ツールを悪用。バックアップの一部も破壊	データセンター内のバックアップも暗号化されたため、クリーン環境でのゼロからの再構築とテストが必要となり、復旧に４カ月半を要した	動画配信サービスをはじめグループ全体のサービスが停止。物流を担う委託先の被害が複数のEC事業者に波及し、サプライチェーン全体が停止	標準の管理ツールを悪用した攻撃はEDR単体では検知が難しい。バックアップの暗号化による既存環境の復元断念が、復旧の長期化を招く構造的な要因となる

取引先企業のEC配送にまで波及し、サプライチェーン全体が機能不全に陥るという構造的リスクを露呈させた（表１）。

これらの事例から分かるように、影響範囲が情報システムの枠を超え、企業活動全体に及んでいる。実際の被害においては、システム復旧の可否だけでなく、事業停止による売上への影響、顧客や取引先への対応方針、情報漏洩の有無を踏まえた対外公表の判断、さらには身代金支払いの是非など、企業の経営判断と直結する論点が同時に発生する。

これらは技術的な正否のみで判断できるものではなく、法務・広報・事業部門を含めた全社横断的な意思決定を伴う点に特徴があ

る。したがって、ランサムウエアは単なるIT課題ではなく、企業価値そのものに直結する経営課題として位置づけるべき脅威となっている。

Ⅱ 実際の被害事例に見るランサムウエアの影響

侵入経路の多様化や攻撃手法の高度化により、従来の対策を講じていても被害が発生し、復旧まで長期間を要する事例が相次いでいる。本章では、実際の被害事例を基に、ランサムウエア攻撃の実態と経営への影響を明らかにする。

1 侵入経路の多様化

近年の被害事例において最も顕著な傾向は、侵入経路の多様化である。警察庁の報告によれば、2025（令和７）年のランサムウエア被害における感染経路はVPN機器からの侵入が約66％、リモートデスクトップからの侵入が約21％を占めており、テレワークなどに利用される機器の脆弱性や、強度の弱い認証情報を悪用した侵入が大半を占める[注3]。

しかし、侵入経路はこれらに限らず、委託先環境から侵入されるケースも報告されている。Ｃ社（業務委託事業者）の事例では、委託先環境を踏み台にした侵入により、自社が直接狙われていなくとも甚大な被害が発生した。最終的に数百万件規模の個人情報が漏洩する事態に発展し、委託元である金融機関や自治体など多数の組織に被害が連鎖した。

Ｄ社（大手コンテンツ企業）の事例では、Active Directory（AD）[注4]を奪取され、仮想化基盤を含む複数のサーバが一斉に暗号化された。バックアップの一部も破壊され、動画配信サービスをはじめとしたグループ全体のサービスが停止した。さらに、同社の物流を担う委託先の被害は、複数のEC事業者に玉突き的に影響を与え、サプライチェーン全体が停止するまでに至った。

2 境界型防御の限界と課題

ランサムウエアの検知において重要な役割を担うEDR（Endpoint Detection and Response）[注5]などのエンドポイント対策を導入していても、正規ツールや管理権限を悪用した攻撃に対しては、検知や封じ込めが後手に回るケースが少なくない。

Ｄ社の事例では、攻撃者がWindows標準の管理ツール（PowerShellなど）を悪用する「Living off the Land（環境寄生型攻撃）」を行った。一般的なセキュリティ製品では怪しいツールは検知できるものの、標準の管理ツールを悪用した攻撃は検知が難しく、侵害範囲が拡大した。

前述したＢ社の事例においても、攻撃者はランサムウエアを起動する前にEDRをはじめとするセキュリティ対策ソフトウエアを無効化しており、さらに侵害が発生したデータセンターの一部サーバにはEDRが未導入であったことが発見の遅れや感染の拡大につながった。また、近年では攻撃者が検知回避のための工夫を行っていることから、EDR単体でランサムウエアを完全に防ぐことは難しい状況となっている。

3 復旧が長期化する構造

近年のランサムウエア攻撃では、バックアップが暗号化・破壊され、復旧手段そのもの

が失われるケースが多い。警察庁のデータによれば、ランサムウエア事案におけるバックアップ復元成功率は20%程度にとどまり、失敗の過半数はバックアップ自体が侵害された事案であると報告されている[注3]。

B社では、ランサムウエアが暗号化と同時にバックアップファイルの削除まで実行した。「ランサムウエア攻撃を想定したバックアップ環境が構築されていなかった」ことが復旧長期化の最大の原因であり、同社は既存環境を完全に破棄し、ゼロから新環境を構築するという判断を下したため、主要サービスの復旧完了まで約3.5カ月を要した。

D社においては、複数の構造的要因が重なり、復旧に4カ月半を要した。データセンター内のバックアップも攻撃者によって暗号化されており、既存環境の復元を断念した。安全なクリーン環境で多くのシステムをゼロから再構築し、動作確認や連携テストを経て段階的に復旧する必要があったため、システムの復旧までに長期間を要することとなった。

4 国内企業の被害から見える経営インパクト

ランサムウエア被害は、直接的な業務停止に加え、顧客離反・取引先への影響・社会的評価の低下にもつながる。近年の国内被害事例では業務停止や売上減少といった影響が決算の数値として表れており、経営インパクトが定量的にも確認されている。

A社では、ライフサイクルの短い商品を取り扱う性質上、事件後すぐに「店舗の棚から商品がなくなる」という目に見える影響が生じ、出荷停止が同業他社にまで波及するという想定外の事業影響が発生した。

B社においては、物流システムの全面停止により11月の売上高が前年同月比95%減という壊滅的な水準まで落ち込んだ。特別損失として数十億円、逸失利益を含めた被害総額は100億円を超えた。通期業績予想は取り下げを余儀なくされ、中間配当は無配、役員報酬の減額措置も実施された。

さらに、ランサムウエア被害の影響は企業個別の範囲にとどまらず、社会インフラにまで波及するケースも発生している。たとえば、物流の要となる施設がランサムウエア攻撃を受けた事例では、貨物の搬出入作業が停止し、広範な物流に影響が及んだ。また、医療機関が被害を受けたケースでは、電子カルテシステムの停止により診療業務が継続できなくなるなど、市民生活に直接影響を及ぼす事態も確認されており、ランサムウエアは特定企業の問題にとどまらず、社会基盤そのものを停止させ得るリスクへと拡大している。

このように、被害は自社内にとどまらず、業界全体・社会インフラに拡大し得る点が、経営課題としての深刻さを示している。

Ⅲ 被害事例から得られる教訓

ランサムウエア被害の大小を分けるのは、必ずしも導入しているセキュリティ製品の数や機能だけではない。多くの事例を俯瞰すると、平時の備えや有事における判断などの組織としての統制のあり方が、被害の拡大や復旧の遅れに大きく影響していることが見えてくる。本章では、被害事例を踏まえた共通の失敗構造と、そこから得られる教訓を整理する。

1　従来型ランサムウエア対策の前提の崩壊

従来、多くの企業では、ランサムウエア対策を「マルウエア感染の防止」や「被害発生時のバックアップ復旧」といった枠組みで捉えてきた。しかし、近年の被害事例が示すとおり、こうした前提はすでに成立しなくなっている。

現在のランサムウエア攻撃は、単発的なマルウエア感染ではなく、長期潜伏を前提とした計画的な侵入活動である。B社の事例では、初期侵入は発覚の約4カ月前に行われており、攻撃者はその間、組織の構造やデータの配置を把握し続けていた。

攻撃者は侵入後、認証情報や管理権限を奪取し、ネットワーク全体やバックアップ環境、基盤システムを把握したうえで、最も事業への影響が大きくなるタイミングを狙って攻撃を実行する。A社の事例においても、攻撃者は発覚の約10日前から侵入し、主に業務時間外に複数のサーバへの侵入と偵察を繰り返したうえで、週明けの朝という最も混乱が大きくなるタイミングでランサムウエアを一斉実行している。このような攻撃に対して、侵入そのものを完全に防ぐことも難しくなっており、侵入後の横展開や被害拡大を前提とした対策を講じる必要がある。

2　ランサムウエア攻撃の流れと技術対策だけでは被害を防げない理由

ランサムウエア攻撃は単発的なマルウエア感染ではなく、侵入から内部偵察、権限奪取、横展開を経て最終的な暗号化に至るまでの一連のプロセスとして実行される。この攻撃の流れを踏まえると、特定の対策のみで被害を防ぐことの難しさが理解できる。

多くの被害企業では、EDRやアンチウイルス、ファイアウォールなど一定水準のセキュリティ対策を導入していた。実際にA社の事例では、NIST CSF[注6]に基づくリスクアセスメントやゼロトラスト[注7]を踏まえたEDR製品の導入、セキュリティ監査などを実施していたことが明らかにされている。しかし、それでも侵害を受けたという事実は、攻撃の進行プロセス全体を踏まえた対策が十分ではなかったことを示している。

近年の攻撃では、正規の管理ツールや管理者権限を悪用することで検知を回避しながら横展開が行われるケースが多い。Microsoftの分析によれば、人手によるサイバー攻撃の78%以上において攻撃者はドメインコントローラー[注8]の侵害に成功しており、ランサムウエアの大規模拡散において重要な役割を担っている[注9]。こうした事実は、エンドポイント単体の防御だけでは対応が難しいことを示している。

また、攻撃者は初期侵入後の潜伏期間中にネットワーク構造や重要資産を把握し、最も事業影響が大きくなるタイミングで攻撃を実行する。そのため、対策は侵入前の防御だけでなく、侵入後の挙動まで含めて設計する必要がある。

このように、ランサムウエア対策は単一の製品や技術で完結するものではなく、攻撃の進行プロセス全体を踏まえた多層的な対策として設計することが求められている。また、実際のインシデント発生時における初動対応や経営判断の重要性がより一層明確となる。

3 被害の差を生むのは「初動」と「判断」

実際の被害事例を比較すると、同様の侵入経路や攻撃手法であっても、被害規模や復旧期間には大きな差が生じている。両者を分けるのは、技術力ではなく初動対応の迅速さと意思決定の適切さである。

被害規模・復旧期間の差は、技術的要因のみに起因するものではない。判断基準や対応手順が事前に整備されていなかったことにより、検知後の意思決定が遅れ、結果として被害が拡大した事例は少なくない。たとえば、侵害の兆候を把握しながらネットワーク遮断の判断に時間を要した結果、横展開が進み、暗号化対象が拡大したケースや、業務停止と縮退運用[注10]の判断軸が定まっていなかったために事業停止が長期化したケースが報告されている。

一方、被害を限定できた企業では、侵害の兆候を早期に把握し、影響範囲の切り分けや業務停止の判断を迅速に行っていた。A社では、検知から約4時間後にネットワーク遮断を実施し、被害の拡大を防止した。さらに、システム停止後ただちに手作業による縮退運用へ移行する判断を下したことで、当該四半期の主力事業への影響を売上1割減にとどめることに成功している。同社の対応で特筆すべきは、検知から数時間以内に「遮断する」「縮退運用に移行する」という二段階の経営判断が下された点である。攻撃が業務時間外や週明けの混乱時を狙うことを踏まえれば、この時間軸での判断は、平時から判断基準が整理され、経営層への報告経路が機能していた結果として可能になったものといえる。

これらの差は、技術製品の性能差ではなく、平時の備えの差に起因する。具体的には、以下の3点が初動の差を決定づける。

①判断基準の事前整備：「どのような兆候を検知したらネットワークを遮断するか」「どの業務を縮退運用で継続するか」といった判断基準が平時に整理されているか
②エスカレーション経路の明確化：現場の検知から経営への報告までの経路と時間軸が定義され、有事に機能するか
③経営層の即応体制：経営層が時間外・休日であっても迅速に意思決定できる体制が組まれているか

いずれも、有事に整備するものではなく、平時に整備しておくべき経営マターである。初動対応の成否は、技術力の差ではなく、平時にどこまで備え、どのレベルまで判断基準を整理していたかによって決まる。次節で論じる「侵入を前提とする」考え方への転換は、まさにこの平時の備えを設計するための前提となる。

4 「侵入を前提とする」考え方への転換

ランサムウエア対策においては、「侵入を防ぐこと」を唯一の目標とするのではなく、侵入を前提に被害を最小化し、事業を継続するための備えへと発想を転換する必要がある。すなわち、侵入後の横展開をどこまで抑えられるか、兆候をどれだけ早く把握できるか、そして確実に「復旧可能な状態」を維持できているかという観点で、対策全体を設計

することが求められる。

この侵入前提の考え方は、NIST SP800-160 Vol.2 Rev.1においても「サイバーレジリエンス」の概念として体系化されている[注11]。同文書では、「予測（Anticipate）・抵抗（Withstand）・回復（Recover）・適応（Adapt）」という4つの目的に沿って、技術的対策だけでなく、組織体制や経営判断のあり方にも直結するものとして位置づけられている。

次章以降では、この前提に立ったうえで、技術面および組織・経営面で求められる備えについて整理していく。

Ⅳ 技術面の最新動向：侵入を前提とした備え

ランサムウエア攻撃を完全に防ぐことが困難である以上、侵入を前提とした設計思想への転換が求められている。カギとなるのは、①封じ込め（被害範囲の限定）、②検知（兆候の早期把握）、③復旧（事業の立て直し）という3つの機能を担う技術（マイクロセグメンテーション・NDR（Network Detection and Response）・サイバーリカバリー）をどう組み合わせ、どこに優先投資するかという判断である。本章では、各技術の狙いと実装上の論点を整理しつつ、経営層に求められる視点を解説する。

1 「侵入前提」で考えるという発想の転換

従来のセキュリティ対策は、ネットワーク外部から内部への侵入を防ぐ「境界型防御」を中心に設計されてきた。しかし前章で見てきたように、VPNの脆弱性やサプライチェーン経由の侵入、正規ツールの悪用といった手法により、境界を突破される事例は後を絶たない。ここで求められるのは、完全防御から侵害前提のサイバーレジリエンスの考え方である。

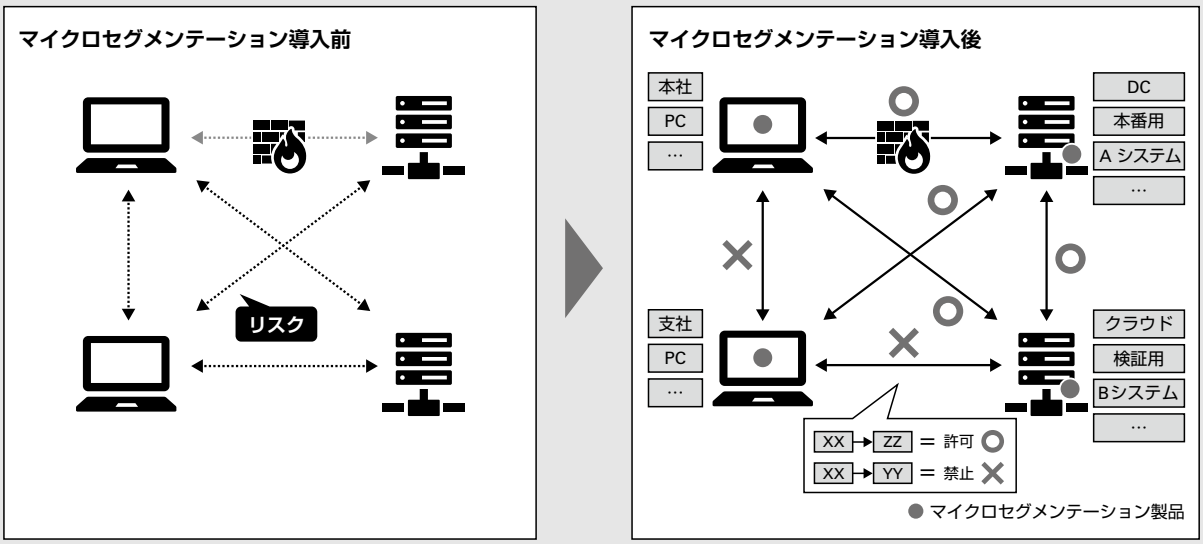
被害をゼロにすることを目指すのではなく、侵入されても被害を最小化し、事業を早期に復旧できる状態をいかに設計するかが、現代のセキュリティ対策にとって非常に重要なポイントである。

2 マイクロセグメンテーションによる封じ込めと実装のポイント

マイクロセグメンテーションは、ネットワークを細かく分割し、必要最小限の通信経路だけを許可することで、攻撃者の横展開を抑止する技術である。従来のネットワーク単位での分割に比べ、サーバやクライアントPCといったホスト単位で論理的に境界を設けることができるため、一部のシステムが侵害されてもほかのシステムへの影響を最小限に抑えることが可能となる（図2）。

その効果は実証データによっても裏づけられている。アカマイ・テクノロジーズが2025年に発表した調査レポートによれば、マイクロセグメンテーションを導入した企業の63%がランサムウエア攻撃の封じ込めを目的としており、導入済み企業ではランサムウエアの封じ込めにかかる時間が33%短縮されたと報告されている[注12]。金融庁が2024年に公表した「金融分野におけるサイバーセキュリティに関するガイドライン」においてもマイクロセグメンテーションの実装が推奨されるなど、重要インフラ業界を中心に導入が進んでいる[注13]。

図2　マイクロセグメンテーション導入の効果



なお、マイクロセグメンテーションはEDRが担う「検知」とはカテゴリが異なり、ネットワーク通信の「防御（遮断）」を担う技術である。両者は補完関係にあり、EDRで侵害端末を検知し、マイクロセグメンテーションで横展開経路を遮断するという、検知と防御の連携により実効性のある封じ込めが実現する。

マイクロセグメンテーションの導入に当たっては、いくつかの重要な検討ポイントが存在する。

（1） ラベル設計とポリシーの策定

マイクロセグメンテーションの導入において、最初に着手すべきはラベル設計とポリシーの策定である。マイクロセグメンテーションでは、IPアドレスに依存せず、「ロケーション」「環境」「アプリケーション」「ロール」といったラベル（属性タグ）をワークロードに付与し、ラベルの組み合わせで通信制御ルールを記述する。

この仕組みにより、ネットワーク構成の変更なく柔軟なセグメンテーションが実現でき、サーバの追加・移動時もラベルを付与するだけでポリシーが自動的に適用される。

ラベルは後続の可視化・制御すべての基盤となるため、必ず可視化工程よりも前に設計・付与を完了させる必要がある。ラベルがなければ、通信フローを「どのシステム間の通信か」という意味のある単位で把握することができず、可視化の目的を果たせないためである。また、システムやホストの増減は日常的に発生するため、将来的な拡張性を見据えたラベル体系の設計が求められる。

ラベル設計と並行して、制御の基本方針を事前に定めておくことも不可欠である。具体的には、以下の論点を設計段階で決定しておかなければ、後続の可視化・制御工程が進まなくなる。

- 制御の単位：システム系統で共通ルールとするのか、ホスト単位で個別に絞るのか
- 制御の方式：許可された通信以外をすべて遮断する「ホワイトリスト型」か、危険な通信のみを遮断する「ブラックリスト型」か
- 制御の粒度：L3（IPアドレス）、L4（ポート）、L7（アプリケーション）のどのレベルとするか

（2） 通信の可視化

ラベル設計とポリシーの策定が完了した後、次に行うのが通信の可視化である。可視化は制御を実施する前の必須工程であり、次の2つの目的をもって行われる。

第1の目的は、通信実態の確認である。対象システムにおいて、設計上把握していない未知の通信経路が存在しないかを確認し、制御ルールの定義に必要な情報を収集する。レガシーシステムや長期運用されてきた環境では、設計書に記載のない通信経路が存在することが珍しくなく、この工程を省略すると業務上必要な通信を誤って遮断するリスクが生じる。

第2の目的は、定義したルールの適正確認である。前項で策定したポリシーに基づいて作成した制御ルールを適用した場合に、業務上必要な通信が誤って遮断されないかを事前に検証する。具体的には、アラートモード（監視のみ・遮断なし）でポリシーを有効化し、一定期間のモニタリングを通じて既存業務への影響がないことを確認する。

（3） 段階的な制御の実施

可視化による検証が完了した後、実際の通信制御（ブロックモード）へと移行する。制御の実施に当たっては、ホスト単位や同系統のシステム単位といった細かい粒度で段階的に適用範囲を拡大していくことが有効である。万が一、想定外の業務影響が発生した場合でも、影響範囲を限定し、速やかに切り戻すことが可能となるためである。

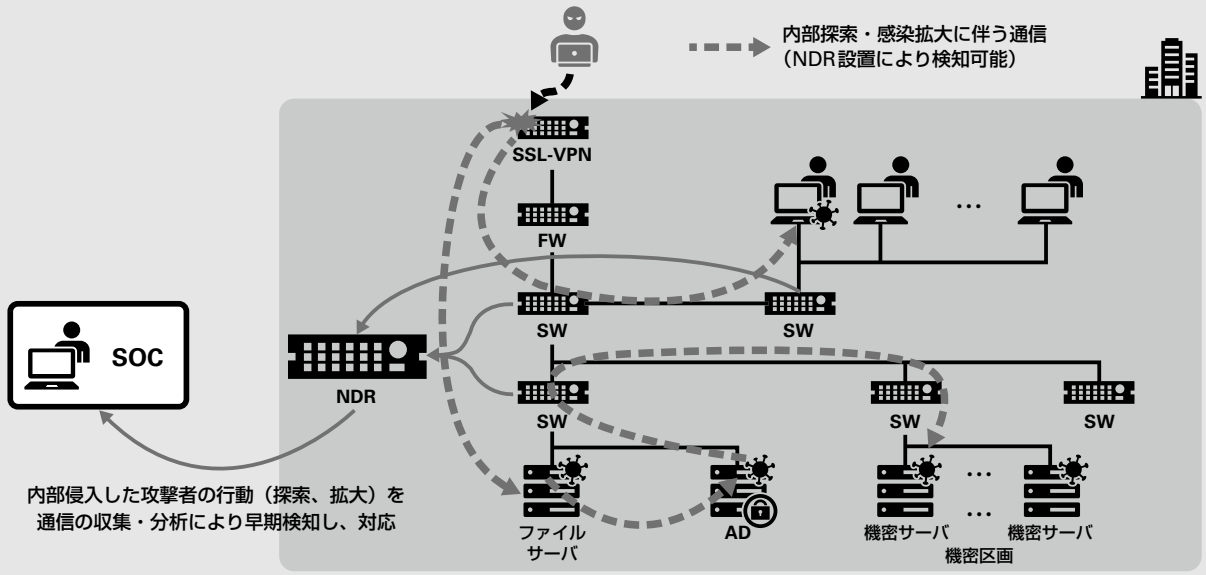
制御方式の選択については、最初からホワイトリスト型で進めることが理想ではあるが、すべての正規通信を事前に把握する必要があり、レガシーシステムや通信要件が動的に変化する環境では実現のハードルが高い。そのため、まずブラックリスト型でSSH（遠隔操作プロトコル）、RDP（リモートデスクトッププロトコル）、SMB（ファイル共有プロトコル）など攻撃者が悪用しやすい主要プロトコルの不要な通信をブロックし、早期にセキュリティベースラインを底上げしつつ、重要資産から順次ホワイトリスト型へ移行していくアプローチが現実的である。

3 NDRによる兆候把握と可視化

NDRは、ネットワーク通信のふるまい検知・分析を軸に、侵入や横展開の兆候をリアルタイムで検知・可視化し、影響範囲の迅速な特定と対処を可能にする技術である。EDRでは捉えにくいネットワーク内部の挙動を可視化し、特に潜伏期間中の兆候検知に寄与する点で、EDRを補完する重要な役割を果たす。

NDRの強みは、エージェントの導入を必要とせず、IoT/OT（Operational Technology：工場などの制御系システム）機器や

図3　NDRによるネットワーク監視と脅威検知



BYOD（Bring Your Own Device：従業員の私用端末）、EDR未導入の端末を含むネットワーク全体を横断的にモニタリングできる点にある。ログは専用アプライアンスに保全されるため、攻撃者による削除リスクも低い。金融業界を中心に、NDRを中核とした侵入前提設計への移行が進んでいる。

NDRの導入においても、いくつかの重要な検討ポイントが存在する（図3）。

（1） センサーの設置場所の選定

NDRはキャプチャした通信しか監視できないため、監視対象の通信を「インターネットやエクストラネットとの通信」と「サーバセグメント間や端末～AD間の内部通信」の2種類で捉え、それぞれどこまで監視したいかを明確にする必要がある。具体的には、まず基幹システムや重要情報が格納されているサーバやデータセンターなどの重要資産の所在を特定し、次にインターネットの出入口やEDRを導入できないホストが存在するネットワークなどリスクの高い出入口を列挙する。

そのうえで、現行のL3スイッチ機器におけるポートの利用状況や対応可能通信帯域、物理的な設置場所や配線・配電の制約を踏まえて実現性を検証し、センサーとブレインのモデル・台数やライセンス費用、光ケーブル配線や工事費用を含めたコスト最適化を図ることが求められる。

（2） 運用体制の設計

NDRは導入後、機械学習により正常な通信パターン（ベースライン）を学習し、そこから逸脱する挙動を自動検知する仕組みであるが、学習期間中に発生するアラートの精査や、運用開始後の誤検知への対応には専門的な知見が必要となる。そのため、SOC（Secu-

rity Operation Center：セキュリティ監視運用センター）やMSS（Managed Security Service：外部委託型のセキュリティ監視サービス）などのセキュリティ監視運用との連携体制を事前に設計し、NDRが検知した脅威をEDRやSIEM（Security Information and Event Management：各種ログを統合分析する基盤）、SOAR（Security Orchestration, Automation and Response：セキュリティ運用の自動化基盤）と連携してトリアージ・対処するフローを構築しておくことが重要である。

（3） 候補製品の選定と実証試験（PoC）

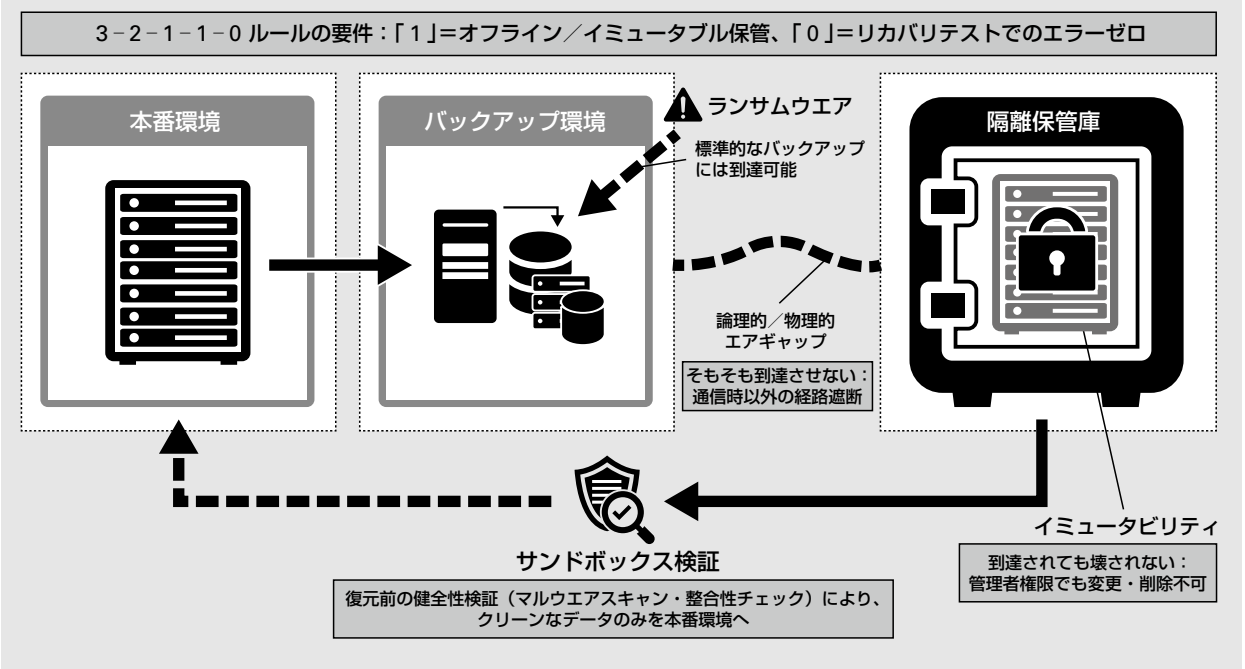
NDR製品は「教師あり学習」と「教師なし学習」のアプローチや、自動遮断機能の有無、対応プロトコルの範囲、クラウド環境への対応状況など、製品ごとに特性が異なる。導入前に机上評価で候補を絞り込んだうえで、自社環境におけるPoCを実施し、実際の検知精度や運用負荷を検証してから本番展開に移行することが望ましい。

4 サイバーリカバリーと復旧レジリエンス

バックアップの取得だけでは、ランサムウエア攻撃に対する復旧力は担保できない。前章で見たとおり、バックアップ自体が暗号化・削除される事例が多発しており、「バックアップがあるから安心」という前提はすでに成り立たなくなっている。

求められるのは、隔離（エアギャップ）・不変性（イミュータブル）・復元テストを含めた包括的なバックアップ設計、すなわち「サイバーリカバリー」の考え方である（図4）。

図4 サイバーリカバリーの考え方



サイバーリカバリーの設計に当たっては、以下の論点を体系的に整理する必要がある。

(1) バックアップデータ自体の安全確保

サイバー攻撃ではバックアップデータそのものが標的となるため、バックアップを攻撃者から「守る」設計が必要となる。バックアップのベストプラクティスとして広く知られる「3−2−1ルール」に対し、サイバーリカバリー製品のベンダーがさらに考え方を追加した「3−2−1−1−0ルール」がある。これは従来の3−2−1ルール（3つのコピーを2種類のメディアに保管し、1つはオフサイトに保管）を拡張したもので、「1つはオフラインまたはイミュータブル（改変不可）な状態で保管」し、「定期的なリカバリーテストでエラー0件を確認」するという2つの要件を追加している。

バックアップデータの堅牢性を高める技術は、その防御の性質に応じて「イミュータビリティ（不変性）」と「エアギャップ（隔離）」の2つの軸で整理できる。

イミュータビリティとは、一度保存されたデータを管理者権限であっても変更・削除できないようにする仕組みである。攻撃者がバックアップデータに到達したとしても、データの改ざんや暗号化を防ぐことが目的であり、「到達されても壊されない」ことを保証する技術である。

エアギャップとは、バックアップデータへの到達経路そのものを遮断する技術であり、攻撃者がバックアップの存在を認識しても「そもそもアクセスできない」状態をつくることを目的とする。

エアギャップには、テープ搬出やメディア取り外しによる物理的エアギャップと、バックアップ通信時以外のポート遮断や本番環境とは独立した認証基盤による管理など、ソフトウエア制御で仮想的な隔離を実現する論理的エアギャップの2種類がある。物理的エアギャップは最も強固な隔離を実現できるが復旧に時間を要し、論理的エアギャップはクラウド環境との親和性が高く自動化との両立が可能である。

イミュータビリティとエアギャップは代替関係ではなく、「到達されても壊されない」と「そもそも到達させない」という異なるリスクに対処する補完関係にあるため、両者を組み合わせることで多層的な防御が成立する。

(2) バックアップ取得の設計と世代管理

サイバーリカバリーを実効性のあるものにするためには、「何を取得するか（取得範囲）」「どの頻度で取得するか」「何世代保持するか」「どの方式で取得するか」を体系的に設計する必要がある。すべてのシステムを同一レベルで保護するのは現実的ではなく、最重要業務に関連するシステムから優先的にサイバーリカバリー対応のバックアップ体制を整備し、対策レベルの枠組みを明確化することが求められる。

とりわけ世代管理は、サイバーリカバリー特有の重要論点である。高度なランサムウエア攻撃では侵入から発覚まで数週間〜数カ月の潜伏期間が存在し、この間に取得されたバックアップにはマルウエアに感染したOSイメージやデータが蓄積されていく。暗号化が実行された時点で直近のバックアップがすべて汚染済みであれば、復旧は不可能となる。

したがって、感染前のクリーンな世代が確実に残存するよう、潜伏期間を上回る保持期間の設定が不可欠である。

この要件は、「いつの時点に戻れればよいか（RPO）」を定義するBIA（事業影響度分析）だけではなく、「いつの時点であれば感染していないか」という攻撃者視点の時間軸を加えて決定する。また、想定される潜伏期間を考慮した世代保持ポリシーを別途策定する必要がある。

（3） バックアップデータの健全性検証

バックアップデータが保護されていても、そのデータ自体がマルウエアに感染していない保証は自動的には得られない。そのため、復元前にバックアップデータの健全性を検証するプロセスが不可欠である。具体的には、隔離されたサンドボックス[注14]環境でバックアップイメージを展開し、マルウエアスキャンや整合性チェックを実施したうえで、クリーンであることが確認されたデータのみを本番環境への復元に使用する。近年のサイバーリカバリー製品では、取得後に自動でスキャンを実行し、各世代の健全性をスコアリングする機能を備えるものもある。

加えて、復元が成功しても、侵入に使われた脆弱性まで復元してしまい、再侵入を受けた事例も報告されている。復元前のマルウエアスキャンだけでなく、復元後の脆弱性対処（パッチ適用・侵入経路の遮断）を含めた一連の手順を事前に整備しておくことが重要である。

（4） 運用体制

サイバーリカバリー製品を導入した後も、バックアップデータの正常性確認、侵害監視、定期的な復元訓練といった運用項目が日常的に発生する。これらの運用を遂行するための体制整備と役割分担の検討が不可欠である。

また、サイバーインシデントからの復旧においては、システム復旧だけでなく、業務プロセスの再開までを含めた「オペレーショナルレジリエンス」の観点で設計を行い、BCP（事業継続計画）と連動させた復旧訓練を定期的に実施することが求められる。ダウンタイムを最小限に抑えるために「復旧可能な状態」を確実につくることは、事業継続の観点から経営的にも非常に重要である。

5 侵入を前提とした多層防御の実装

マイクロセグメンテーションは侵入後の横展開を封じ込める「抑止」の役割を果たし、NDRはネットワーク内の異常を「検知」する機能を担い、サイバーリカバリーは事業を「復旧」するための基盤となる。だが、万能な対策は存在しないため、これら3つをはじめとした、複数の技術を組み合わせ、多層的な防御体制を構築することが、侵入を前提とした昨今の対策検討における重要な点である。

経営に求められるのは、これら技術の細部を自ら設計することではなく、事業継続上の優先資産やRTO（Recovery Time Objective：サービス停止から復旧までの許容時間）／RPO（Recovery Point Objective：復旧時に許容できる最大データ損失時間）といった判断軸を示し、技術部門が適切な設計判断を下せる前提を整えることである。停止が

顧客被害に即直結する事業では封じ込めと復旧を、機密情報を多く扱う事業では検知の早期化を優先するなど、自社のリスク特性に応じた投資の優先順位づけは、経営判断そのものである。

Ⅴ 組織面の備え：経営として準備すべき対策事項

前章で述べた技術的対策は、導入するだけで自動的に効果を発揮するものではない。実際のインシデント対応では、技術の有無以上に、初動対応のスピードや判断のあり方が被害規模を左右している。本章では、技術的対策の実効性を高めるために、経営として平時から準備すべき組織面の論点について整理する。

1 インシデント対応体制の整備

ランサムウエア被害が発生した際、対応が遅れる最大の要因の一つは、「誰が何をすべきか」が事前に定まっていないことである。平時と有事の役割分担を明確にし、エスカレーション経路を整備し、経営層が速やかに意思決定できる体制を平時から構築しておく必要がある。

A社は攻撃発覚後ただちに緊急事態対策本部を設置し、外部専門家と連携して調査・復旧作業を進めた。こうした体制が迅速に機能するためには、平時からの訓練と手順の整備が不可欠である。

2 経営判断が求められる主な論点

ランサムウエア被害に直面した際、経営層が判断を迫られる論点は多岐にわたる。身代金を支払うか否かの判断は、その最たるものである。JIPDEC（日本情報経済社会推進協会）の調査によると、身代金を支払ったとしても約6割が復旧に失敗しており、支払いは犯罪組織の資金源となり再攻撃の対象となるリスクも伴う。

加えて、事業停止・再開の判断、対外的な説明方針の決定、個人情報保護委員会や捜査機関への報告対応など、いずれも現場やIT部門に委ねるのではなく、経営が責任をもって行うべき事項である。これらの判断は企業の短期的な損失だけでなく、中長期的な企業価値や社会的評価を左右する重大な意思決定である。

3 「IT部門任せ」にしないために

ランサムウエア対策を経営リスク管理として位置づけ、対策の基本方針と判断軸を事前に示すことが重要である。ランサムウエア被害は、情報システム部門のみで影響を完結させることができず、営業、製造、物流、広報、法務など、企業活動のあらゆる領域に連鎖して影響を及ぼす。

そのため、経営として全社横断のリスク管理として捉える視座が不可欠であり、平時から「何を守るのか」「どこまで復旧できれば事業継続と見なすのか」「最悪の場合にどの判断を行うのか」といった点を整理しておく必要がある。

4 サプライチェーンを含めた統制設計

委託先の被害が自社の重大インシデントに直結する時代において、サプライチェーン全体を視野に入れた統制設計が求められる。

C社の事例では委託先が攻撃を受け、委託元である金融機関や自治体を含む多数の組織に被害が波及した。B社の事例では、例外的にMFA（Multi-Factor Authentication）[注15]を適用していなかった業務委託先アカウントが攻撃の起点となった。

委託先契約にセキュリティ要件を明記し、認証管理の徹底や定期的な評価を実施するなど、実効性ある統制設計が不可欠である。

5　演習と見直しによる実効性確保

計画や体制は、演習を通じて初めて課題が顕在化する。インシデント対応訓練では、ランサムウエア攻撃を題材に、データ暗号化被害や情報暴露に関する脅迫といった実践的なシナリオを設定し、チーム間での情報連携や意思決定の訓練を行うことが有効である。訓練は一度実施すれば終わりではなく、定期的に繰り返し、インシデント対応フローの見直しも含めて、有事に確実に動ける状態を維持し続けることが重要である。

Ⅵ　まとめ：経営としてどう向き合うべきか

ランサムウエア対策の成否は、最終的には経営層の関与と意思決定にかかっている。被害に遭うかどうかではなく、被害をどこまで抑え、どれだけ早く事業を立て直せるかが企業価値を左右する。本章では、本稿全体を踏まえ、経営層に求められる姿勢とリーダーシップのあり方を整理する。

1　ランサムウエア対策を経営リスク管理として捉える

ランサムウエアは、数あるサイバー攻撃の一つにとどまらず、企業の事業継続や社会的信頼に直接影響を及ぼす経営リスクである。自然災害や重大事故と同様に、「発生を前提として、いかに被害を抑え、早期に立て直すか」を考える必要がある。つまり、ランサムウエア対策は単なるIT投資やセキュリティ対策ではなく、BCPや危機管理の一環として、経営が主体的に関与すべきテーマである。

実際に、その影響は企業価値と事業継続の双方に及んでいる。日本サイバーセキュリティ・イノベーション委員会（JCIC）の分析によれば、インシデントに関する適時開示を行った国内企業では株価が平均10％下落し、純利益は平均21％減少しており、サイバー攻撃が市場からの信頼と収益基盤を直接毀損する実態が明らかになっている[注16]。

また、アイ・ティ・アールの調査では、2024年以降にランサムウエア被害を受けた国内企業のうち完全復旧できなかった企業が70％に達し、復旧に１週間以上を要した企業も70％に上る。こうした数字は、ランサムウエア被害が企業の信頼と事業基盤そのものを揺るがす経営リスクであることを裏付けている[注17]。

2　成否を分けるのは「判断と備え」

ランサムウエア対策の成否は、「侵入を完全に防げるかどうか」ではなく、「被害をどこまで抑え、どれだけ早く事業を立て直せるか」によって決まる。JIPDECの調査では、身代金を支払わずに自力で復旧できた企業が

141社存在し、そのうち6割以上が1カ月以内にシステムを復旧させている。これらの企業に共通するのは、日頃からオフラインバックアップ体制を構築し、実効性のある事業継続計画を整備していたことである。

平時において、「何を守るのか」「どこまで復旧できれば事業継続と見なすのか」「最悪の場合にどの判断を行うのか」といった点が整理されていない場合、有事における意思決定は遅れがちになり、被害拡大や復旧長期化を招くリスクが高まる。だからこそ、ランサムウエア対策は技術論に終始するのではなく、経営判断を支えるための準備として設計される必要がある。

3　経営に求められる役割と姿勢

平時からランサムウエアを経営リスクとして捉え、対策の基本方針と判断軸を示すこと。これにより、有事における現場の迷いや判断のばらつきを最小限に抑えることができる。

有事においては、情報が不完全な状況下であっても、覚悟をもって迅速に判断する姿勢が求められる。身代金支払いの是非、事業停止や再開の判断、対外的な説明方針などは、現場やIT部門に委ねるのではなく、経営の責任において決断すべき事項である。

4　本稿のまとめ

ここまで見てきたように、ランサムウエア対策は、技術・組織・経営判断のいずれか一つで完結するものではない。侵入を前提とした技術的備え、迅速な初動対応を可能とする組織体制、そして最終的な意思決定を担う経営の関与が、相互に連動して初めて実効性を持つ。

経営が実際に下すべき判断は、時点ごとに整理することができる。平時には「守るべき

表2　経営層が押さえるべきポイント

時点	経営が下すべき判断	判断の主な論点（例）	本稿参照
平時	• 守るべき優先資産の特定 • 復旧目標（RTO・RPO）の設定 • 投資の優先順位づけ	• 事業停止が許容できないシステムはどれか • どこまで復旧できれば事業継続と見なすか • 封じ込め・検知・復旧のどこに優先投資するか • サプライチェーン上のリスク把握	Ⅳ Ⅴ―3 Ⅴ―4
有事	• 事業停止・再開のタイミング • 身代金支払いの是非 • 対外公表方針 • 規制当局・捜査機関への報告	• 縮退運用へ即移行するか、全停止か • 支払いの可否と社会的影響 • 情報漏洩の有無を踏まえた公表範囲・タイミング • 顧客・取引先への対応方針	Ⅴ―1 Ⅴ―2 Ⅵ―3
事後	• 再発防止に向けた追加投資 • インシデント対応フローの見直し • ガバナンス強化の方針	• 侵入経路の遮断と脆弱性対処 • 委託先含むサプライチェーン再評価 • 演習・訓練の継続的な実施 • 経営報告・取締役会への定期的なリスク報告	Ⅴ―4 Ⅴ―5

優先資産の特定」「復旧目標の設定」といった備えの判断を、有事には「事業停止・再開のタイミング」「身代金支払いの是非」「対外公表方針」といった即応の判断を、事後には「再発防止に向けた追加投資」「ガバナンス強化の方針」といった学びの判断を、いずれも経営の責任として下す必要がある（表２）。

ランサムウエアが経営リスクとなった現在、企業価値を守るために問われているのは、「どれだけ高度な対策を導入しているか」ではなく、有事において経営としてどう向き合い、どう立て直すのかという姿勢である。その覚悟と準備こそが、ランサムウエア時代における企業価値防衛の本質である。

そして、この考え方はランサムウエアに限らず、あらゆるサイバーリスクへの対応においても共通するものである。デジタル化の進展により企業活動とITが密接に結びついた現在、セキュリティは単なる技術対策にとどまらず、経営として主体的に取り組むべき重要な責務である。

注

1 ソフォス「The State of Ransomware 2025」（2025/６）
https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2025.pdf

2 プルーフポイント「身代金を支払わない結果、日本のランサムウエア感染率は減少？ ランサムウエア感染率／身代金支払率15か国調査 2024」（2024/４/25）
https://www.proofpoint.com/jp/blog/threat-insight/japan-ransomware-payment-result-2024

3 警察庁サイバー警察局「令和７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」（2026/３）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

4 Windowsドメインの認証・認可基盤。攻撃者に乗っ取られると組織内の権限昇格や大規模横展開の足がかりとなるため喫緊の防護対象

5 PC・サーバなどの端末（エンドポイント）上の不審な挙動を検知し、対処を行うセキュリティ製品

6 米国国立標準技術研究所（NIST）が策定したサイバーセキュリティ対策のフレームワーク

7 社内ネットワークも含めてすべての通信を信頼せず、アクセスごとに認証・認可を行う設計思想。「侵入されることを前提とした防御」の代表的な考え方

8 Active Directory環境の中核となるサーバ。ユーザー認証や権限管理を一元的に処理する

9 Microsoft Security Blog “How cyberattackers exploit domain controllers using ransomware”（2025/４/９）
https://www.microsoft.com/en-us/security/blog/2025/04/09/how-cyberattackers-exploit-domain-controllers-using-ransomware/

10 システムの一部機能を制限してでも業務の核心を維持する運用

11 NIST Special Publication 800-160, Volume 2, Revision 1 “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach”（2021/12）
https://doi.org/10.6028/NIST.SP.800-160v2r1

12 アカマイ・テクノロジーズ “Segmentation Impact Study: Why microsegmentation now defines enterprise cybersecurity, risk, and resilience”（2025/10/８）
https://www.akamai.com/site/en/documents/research-paper/segmentation-impact-study-2025.pdf

13 金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」（2024/10/４）
https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf

14 隔離環境でファイルやシステムイメージを展開・実行してマルウエアの有無を検査する仕組み。バックアップの健全性検証などで用いられる

15 多要素認証。パスワードに加えて、SMSコード・生体認証などの追加要素を組み合わせる認証方式。アカウント乗っ取りリスクを大幅に低減する

16 日本サイバーセキュリティ・イノベーション委員会（JCIC）「取締役会で議論するためのサイバーリスクの数値化モデル」（2018/9/19）
https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf

17 アイ・ティ・アール「ランサムウェア感染から完全復旧できない企業が7割に上る／サイバー攻撃を前提としたバックアップデータ保護と迅速な復旧の仕組みが重要に／ITRが『企業のサイバーリカバリ実態調査』の結果を発表」（2025/6/4）
https://www.itr.co.jp/topics/pr-20250604-1

著者

篠原 隆（しのはらたかし）
NRIセキュアテクノロジーズ アーキテクチャコンサルティング事業本部 インテグレーションコンサルティング部 シニアセキュリティコンサルタント
専門はセキュリティ施策の企画実行、セキュリティソリューション導入や運用設計など