独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

ランサムウェア被害から学ぶ教訓集

～ 経営者のためのランサムウェア対策ハンドブック ～

2026 年 9 月 8 日

独立行政法人情報処理推進機構

セキュリティセンター

目次

1 概要

本資料「ランサムウェア被害から学ぶ教訓集」（以下、「本教訓集」という。）は、国内で発生したランサムウェア攻撃による被害にあった複数の組織に対しヒアリング調査を実施し、被害組織の知見・経験をランサムウェア事案発生時における実践的な対処・対応に関する教訓として取りまとめたものである。調査に際しては、株式会社野村総合研究所の協力を得て実施した。さらに、本教訓集の作成に際しては、八雲法律事務所 山岡裕明弁護士に監修・加筆頂いた。

本教訓集の背景、想定読者層、構成、留意点を以下に示す。

1.1 背景

近年、ランサムウェア攻撃の被害が組織の規模を問わず多発している。ランサムウェア事案の発生により、業務停止や顧客情報を含む機密情報流出、また身代金支払等の被害が発生したとみられ、その対処は組織にとって深刻なリスクとなっている。

独立行政法人情報処理推進機構（以下「IPA」という。）では、「コンピュータウイルス対策基準」（通商産業省（現経済産業省）告示第 429 号、1990 年 4 月）、「コンピュータ不正アクセス対策基準」（同省告示第 362 号、1996 年 8 月）に基づき、国内のコンピュータウイルスの感染被害やコンピュータ不正アクセス被害の届出を受け付けており、届出状況や事例の情報を公表することで我が国組織の被害抑制に寄与してきた。

近年問題化しているランサムウェア事案もこうした被害届出の対象だが、他の事案に比べ、事案発覚時に経営者や現場に緊急性の高い判断・対処が求められることが多く、さらにどのような選択が正解だったのか事後的な検証が難しいケースもあると考えられる。

このような状況を踏まえ、国内の被害事例を分析して得られる教訓を、今後起こり得るランサムウェア事案への備えとして活かしていただくとともに、インシデント対応計画や事業継続計画（BCP（Business Continuity Plan））の更なる充実強化に役立てていただくために、本教訓集を作成した。作成の過程で、この脅威に立ち向かうには、経営者の明確な関与が不可欠であることを確信したため、サブタイトルに「経営者のためのランサムウェア対策ハンドブック」と名付けている。

1.2 想定読者層

本教訓集の想定読者は以下の通り。

- 経営者
- 経営・リスク管理に関わる部署の担当者

  （総務部門、経営企画部門、法務部門、広報部門、各事業部門等）

- インシデント対処に関わる部署の担当者

  （情報システム部門、セキュリティ部門等）

1.3 構成

各被害組織から得られた教訓は、経営・リスク管理に関わる部署向けの項目と、インシデント対処に関わる部署向けの項目に分類・整理した。

また、各項目は、以下の様式により取りまとめを行った。

① 教訓

各項目における教訓の要点を簡潔に記載した。

② ヒアリング調査に基づく分析

教訓の背景となった被害組織が得た気づきや直面した課題を掲載した。

③ 解説

②を踏まえ、教訓の趣旨、背景及び具体的な対応上の留意点を解説した。

1.4 本教訓集の留意点

本教訓集は、あくまでランサムウェア被害組織に対するヒアリング調査の結果をベースとしており、そこから得られた知見に基づいて作成した。そのため、近年のランサムウェア攻撃に即した事案対処の全体像やそれを推進するための包括的・体系的な方法論を示すものではない。

ランサムウェア事案対処において、被害組織が選択した対応・対策等は、事前の対策の内容・レベルやそれに伴うランサムウェア攻撃の被害状況、事案対処時に優先する対処方針等に伴い、被害組織毎に「必要」、「重要」、「有効」等の判断基準が大きく異なる。

加えて、IPA においても、被害組織が得た多くの知見の中から他社にも参考になると判断したものを選定して、その教訓の内容を教訓集として取りまとめている。従って、本教訓集に取りまとめた教訓の内容には、被害組織の認識・判断及び、IPA による事象の選定・分析に基づいている点にも留意する必要がある。

なお、本教訓集に含まれる法令・規制に関する記載は一般的な参考情報であり、個別事案に対する法的判断を示すものではない。法令の適用関係は事案毎に異なるため、最新の法令、所管官庁・個人情報保護委員会の公表資料等を確認し、必要に応じて専門家に相談されたい。

本教訓集が、組織の経営者や経営・リスク管理に関わる部署、インシデント対処に関わる部署の担当者にとって、ランサムウェア対策を検討するきっかけとなること、ランサムウェア事案発生時に求められる判断・対処をより一層的確かつ迅速に行うための一助となることを期待する。

2　ランサムウェア事案の特性

ランサムウェア事案では、通常の IT インシデントとは異なり、下記のような特性が存在する。円滑な対応の観点から、経営者に求められる判断事項は多く、ランサムウェア攻撃を念頭においた平時からの備えや、情報システム部門のみならず組織全体での対応体制の確保がとりわけ重要といえる。

✓　ランサムウェア事案は、何らかのデータが暗号化されてから被害に気付いた場合、事案発覚時において既に「インシデントフェーズの最終段階」となっており、対応の時間的猶予が限られる。すなわち、発覚時点で、一般的な IT インシデント発生に求められる種々の対処[1]について、「短期間」に実施することを余儀なくされる。

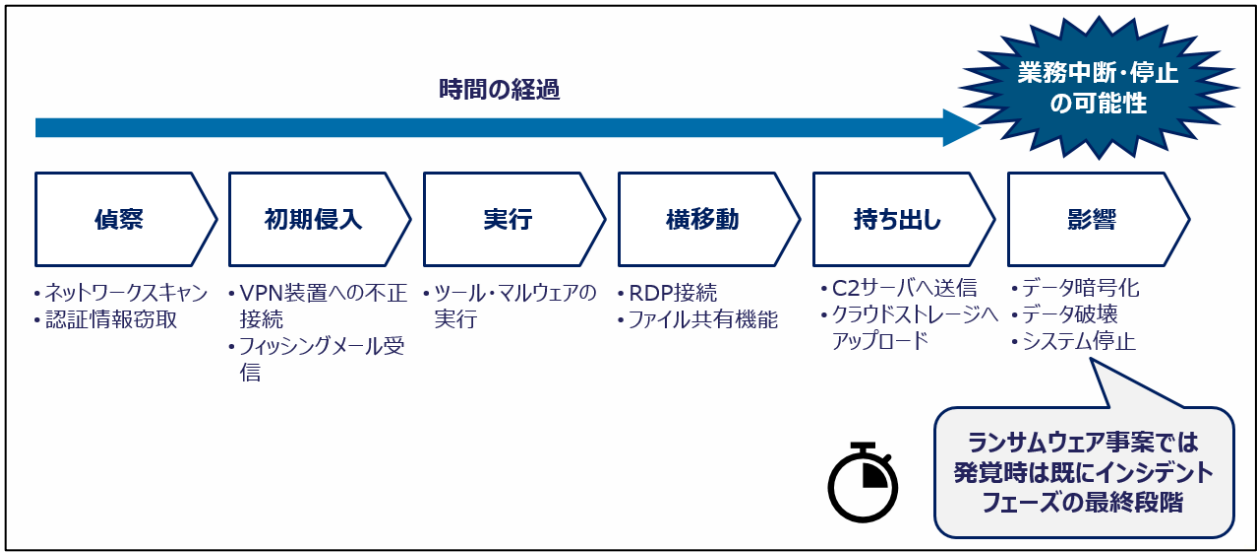

図 1　インシデントの主なフェーズ[2]

✓　加えて、二重脅迫[3]のように、脅迫者が身代金支払いのために後追い的で揺さぶり（窃取データの暴露脅迫）をかけてくるケースがあり、この場合、発覚直後から、技術的なインシデント対処やその他事業継続計画に即した対応に加え、場合によっては攻撃者との交渉対応（付随的な対応も含む）という、追加的な負荷を被ることになる。

---

[1] 侵害調査、システム復旧又は再構築の可否判断、実施可能な業務継続と取引先対応・公表対応、等。

[2] 主なフェーズは MITRE ATT&CK(https://attack.mitre.org/)の Tactics を参考に抽出・再構成して作成。

[3] ランサムウェアにより暗号化したデータを復旧するための身代金要求に加え、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暴露する等と二重に脅迫する攻撃方法。

✓ ランサムウェア事案では、IT セキュリティに起因し、かつ、高度な専門性を有するゆえに、とかく、情報システム部門に、経営者への報告、事業継続、取引先対応等、多くの対応が集中する傾向がみられ、短期間対応を求められる中で、更なるひっ迫状況を惹起するリスクがある。

✓ こうした状況下では、平時における備えの濃淡（暗号化・漏えいデータ特定のための台帳管理、有事の指揮命令・役割分担の有無、想定外対応体制等）が、一般的な IT インシデント以上に対応の成否を大きく左右する。

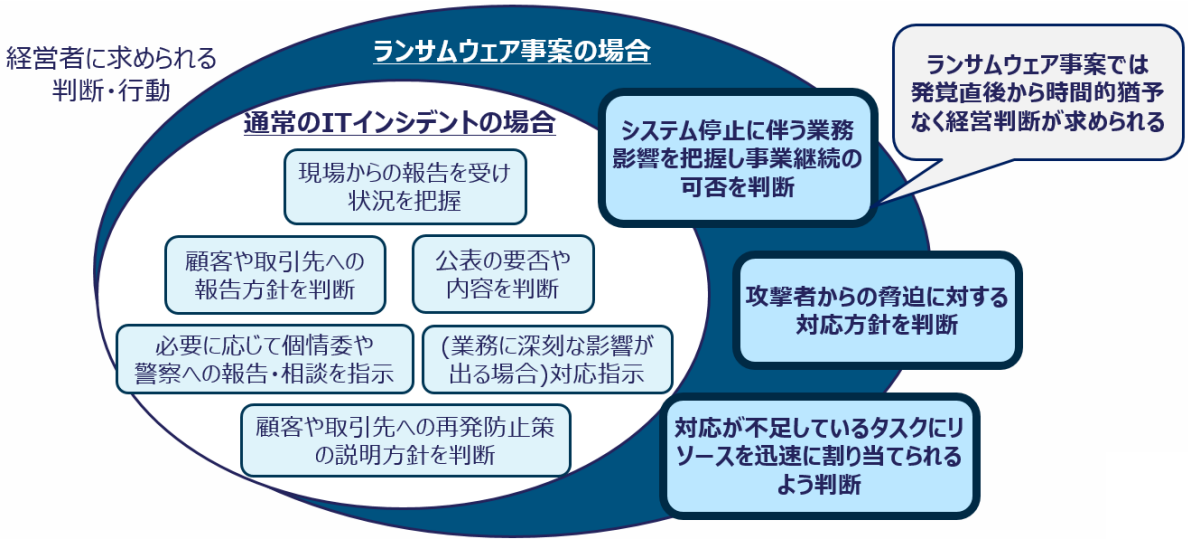

図 2 経営者に求められる判断・行動

3 経営・リスク管理編

経営者やリスク管理部門にとって重要な教訓は以下の通りである。

表 1 経営者やリスク管理部門が重視すべき教訓

担当者の分類	教訓
経営・リスク管理	(1) 経営者による迅速な経営判断と明確な関与
	(2) インシデント対応体制の整備
	(3) 事業継続計画（BCP）への反映
	(4) 個人情報を含むデータの現状把握
	(5) 経営者主導の意思統一
	(6) 窃取されたデータの暴露への備え

(1) 経営者による迅速な経営判断と明確な関与

ランサムウェア事案対応には時間の猶予がない。発覚直後から業務中断や脅迫への対応、メディア対応等における経営判断を迫られる。経営者は事前に発生し得るリスクを認識し、緊急時に迅速な意思決定を行えるよう、判断基準や意思決定プロセスをあらかじめ整備しておく。

(2) インシデント対応体制の整備

IT インシデントという特徴から情報システム部門に負荷が集中する傾向がある。しかし、ランサム事案は公表対応、法務対応、取引先対応、外部連携組織を含めた多方面の対応が必要となる。経営者は事前に情報システム部門、総務部門、広報部門、法務部門、営業部門を含めて全社的に役割分担を明確にしておく。

(3) 事業継続計画（BCP）への反映

ランサムウェア攻撃によるシステム停止は業務停止に直結し得る。システムの停止・復旧の判断には、事業部門の関与が必須。経営者は事前に情報システム部門と事業部門の協力のもとサイバー攻撃に対応した事業継続計画（BCP）の策定を指示しておく。

(4) 個人情報を含むデータの現状把握

流出・暗号化されたデータの内容を後から特定するのは、フォレンジック調査を行っても困難であることが多い。経営者は事前にデータを管理する部署に向けて個人情報を含むデータの台帳を整備するよう指示しておく。

(5) 経営者主導の意思統一

組織内の意識のずれが大きいと混乱を招き、円滑な事案対応を阻害する。経営者は情報発信や権限委譲等の工夫を凝らし、組織の意思統一やスピード感のある対応を実現する。

(6) 窃取されたデータの暴露への備え

身代金を支払ってもデータの回復や暴露中止は保証されない。経営者はこの前提で窃取されたデータがダークウェブ上で暴露されるリスクに備えつつ、データ及びシステムの復旧を図る。

3.1 経営者による迅速な経営判断と明確な関与

【教訓】

> ランサムウェア事案対応には時間の猶予がない。発覚直後から業務中断や脅迫への対応、メディア対応等における経営判断を迫られる。経営者は事前に発生し得るリスクを認識し、緊急時に迅速な意思決定を行えるよう、判断基準や意思決定プロセスをあらかじめ整備しておく。

【ヒアリング調査に基づく分析】

- ✓ ランサムウェアの攻撃者は時間をかけて探索し、バックアップ特定やデータ持出しを行った後、攻撃フェーズの最終段階として暗号化を開始する。組織は残された環境で実施可能な業務継続と侵害調査を行いつつ、システムの復旧方針を判断し、さらに関係機関への届出、公表、顧客や取引先等への説明、攻撃者からの脅迫への対応との交渉等の対処を短期間に取り組まなければならない。これらの多くは、経営者の関与が必要になる。
- ✓ 経営層と情報システム部門の間で、発生している事態やリスクについての認識共有と意思疎通が困難だったとする組織が多かった。
- ✓ 時間的猶予がない中で様々な判断を迫られるが、ランサムウェア被害に関する経営者の理解不足や、意思決定プロセスに不備がある、判断基準がない等の理由により、決定に時間がかかったとする組織が見られた。

【解説】

(1) 経営者の関与

ランサムウェア事案においては、システムの構成要素が破壊されるため、その影響は組織の事業継続の可否に直結する。この事態を乗り越えるためには、システムの主幹部門である情報システム部門と、事業継続の判断をする経営層との間で、発生している事態やその事業への影響についての認識が共有されている必要がある。しかし、今回ヒアリングした中では、この認識共有や意思疎通が困難だったとする組織が

多かった。また、システム停止時の事業継続においては、情報システム部門以外の従業員の活動にも大きな影響が及ぶため、経営者の判断と方針提示が重要であることが語られた。

(2) 組織の経営や業務に影響がある重要事項の決断

ランサムウェア事案対応の中では、組織内の重要システムの停止や対外的な公表といった、組織にとって重要な判断が必要になる。経営的、システム的な意思決定のためのプロセス、判断基準の整備が必要である。今回のヒアリングで多く挙げられたことのひとつが、これらの「重要事項の判断に苦慮した」点である。時間的猶予がない中で様々な判断を迫られるが、意思決定のプロセスに不備があったり、判断基準がなかったため決定に時間を要するなど、準備が不十分だったとする組織が多かった。また、意図的にシステム構成要素の一部、または全てを停止する、といった平時では行わないオペレーションについて、システム間の依存関係が把握できていないことにより判断に迷ったケースが見られた。

(3) ネットワーク遮断・封じ込め

ランサムウェア被害を認知した際に取るべき初動対応は、インターネット経路の切断、感染箇所の切り離しである。その後、状況に応じて重要資産の切り離しを行う。ランサムウェア事案の発覚は、暗号化が実行されたタイミングであることが多い。それを認知した場合は、初動対応として、①攻撃者のネットワーク経由の活動を阻止するために、インターネット経路の切断を行う、②どの端末・サーバが侵害されているか把握できている場合には、侵害拡大を防止するために、感染 PC やサーバのネットワークからの切り離し、またはセグメント単位の切り離しを行う。この２点は、おおよそどのヒアリングでも挙げられた対応であり、切り離した箇所は様々ではあったが、ネットワークからの切り離しは必須の対応だといえる。また、システムや業務の稼働状況、侵害の可能性を勘案して、重要な資産をネットワークから切り離したケースもあった。

(4) 被害情報の公表

被害の公表は、当該事案だけでなく組織に様々な影響を与える。セキュリティインシデントが発生した組織では、その経緯や被害、対策状況を、HP 等を通じて公表することが多くなっている。しかしながら、組織の属性や時流、公表内容その他の状況によっては、公表により、たとえば未確定情報が独り歩きする等、組織のレピュテーションに悪い影響を与えることがあり得る。取引先のような丁寧に状況を伝えるべ

きステークホルダーとそれ以外、それぞれにどの程度どのように伝えるべきかは悩んだ点だったと、今回のヒアリングでも多く聞かれた。

（5）収束宣言

収束宣言については様々な考え方がある。セキュリティベンダーの詳細調査を含む侵害調査の完了、調査結果に基づく対策が完了、復旧方針が定まり作業がある程度進捗したタイミングで検討するが、収束したことを明示的に外部に公表する場合には、宣言後の新事実判明による影響は考慮すべきである。

3.2 インシデント対応体制の整備

【教訓】

> IT インシデントという特徴から情報システム部門に負荷が集中する傾向がある。しかし、ランサム事案は公表対応、法務対応、取引先対応、外部連携組織を含めた多方面の対応が必要となる。経営者は事前に情報誌システム部門、総務部門、広報部門、法務部門、営業部門を含めて全社的に役割分担を明確にしておく。

【ヒアリング調査に基づく分析】

- ✓ 中小規模程度の組織では、「IT インシデントだから情報システム部門で対応」となるケースが見られ、経営層への報告、関係機関への届出、取引先対応についても情報システム部門中心になり、貴重な時間や人手が奪われることで、本来の事案対処に集中できなくなってしまう。
- ✓ ランサムウェア事案では、同時多発的な問題に対処しなければならないため、関係者による役割分担が極めて重要である。一方、事案発覚後は時間的猶予がなく、事前に体制を整備しない限り、実効的な役割分担は難しい。また、うまく対処できた組織では、過去のインシデント対応経験が活かされたことを要因としてあげていた。
- ✓ 事案発覚後、短期間で信頼できるセキュリティベンダーを確保するのは容易ではないため、平時の体制整備の一環として、予め候補となるセキュリティベンダーとの関係を構築しておくことが望ましい。（4.5 参照）

【解説】

(1) インシデント対応体制の整備と経験を踏まえた改善

インシデント対応体制の整備は、事前準備である。そして、対応経験を活かした再発防止策を講じ体制をより強固にする働きかけが必要である。ランサムウェア事案か否かにかかわらず、セキュリティインシデントへの対応が円滑に遂行されるかどうかは、インシデント対応体制を事前に整備できるかにかかっていると言っても過言ではない。ランサムウェア事案は、時間的猶予なく事業継続の判断を迫られるが、事前の準備なしに有事において万全の体制で対応に当たることは困難である。今回のヒアリングにおいては、CSIRT の設置や対応する委員会の設置など、いくつかの準備をしていた組織はあったが、そのよう

な事前準備を講じていた場合でさえ、その体制や対応内容には多くの課題があったことが語られた。また、「うまく体制整備が活かせた」と語った組織では、「２回目の攻撃時には」や「近い状況を経験していた」と、経験を活かせていたことを、その要因としてあげていた。

【コラム】 事案対処の最中に情報システム部門が業務を抱え込んだらどうなる？

ヒアリングでは、ランサムウェア事案が IT 案件であるということで、情報システム部門に対応が一任され、警察への対応相談や、個人情報保護委員会への報告、取引先への説明、攻撃経路の特定、被害分析、復旧方針の策定、復旧作業、必要となる対策の企画・導入に至るまですべての対応業務を担当したケースが見られた。このケースでは、復旧を支援していたセキュリティベンダーから「特に負荷の大きい外部組織への報告業務を関係部署に分担しなければ、復旧作業が進まなくなる」との指摘を受けたが、事前の取り決めがなかったため、情報システム部門は関係部署に業務を割り振ることができず、復旧作業に集中できなくなった。

3.3 事業継続計画への反映

【教訓】

> ランサムウェア攻撃によるシステム停止は業務停止に直結し得る。システムの停止・復旧の判断には、事業部門の関与が必須。経営者は事前に情報システム部門と事業部門の協力のもとサイバー攻撃に対応した事業継続計画（BCP）の策定を指示しておく。

【ヒアリング調査に基づく分析】

- ✓ ランサムウェア攻撃の被害は業務停止に直結する。システム停止により業務にどのような影響があるかは、事業部門でなければ正しく把握できない。情報システム部門と事業部門の相互協力がなければ組織の事業継続は困難。システム復旧と業務復旧についても同様である。たとえば製造業においては、生産管理システムが停止すると、在庫があっても納品できない事態となり、業務継続・復旧のためにはそれをシステム無しで解決しなければならなくなる。
- ✓ 事業継続計画を事前に策定していた組織において、サイバー攻撃は想定していなかった場合であっても、自然災害時のシステム停止に備えて手作業での業務継続手順を整備していた組織では、ランサムウェア事案にも実効的に対応できていた。

【解説】

(1) 事業継続計画（BCP）

ランサムウェア事案は、業務停止に直結する。したがって、ランサムウェア事案に対応できる事業継続計画を策定し、訓練を通じてその実効性を高めていくことが望ましい。自然災害やパンデミックに備えた事業継続計画は多くの組織で策定されていたようだが、IT インシデントを想定したケースは少なかった。もっとも、自然災害時のシステム停止に備えて手動による業務継続マニュアルを整備していた組織では、実際にランサムウェア事案においても対応できたようである。また、訓練の有効性について言及する組織も多かった。

(2) 業務の継続

システム停止状態で業務を継続するには、多くの場合、手作業による処理が必要となる。今回のヒアリングで聞かれた「厳しい状況」は、この手作業を中心にした業務継続に関するものが多かった。そしてこの手作業を可能にしたのは、システム化される以前の業務経験を有する従業員の活躍であった。一方でDX を推進している状況もあり、今後の業務のブラックボックス化を心配する声もあった。また、手作業による業務も、事案対応の時間経過とともに、一部に簡易的なシステムを稼働させる、クラウドサービスの活用で負荷を軽減するといった工夫をして乗り越えたという話もあった。

3.4 個人情報を含むデータの現状把握

【教訓】

> 流出・暗号化されたデータの内容を後から特定するのは、フォレンジック調査を行っても困難であることが多い。経営者は事前にデータを管理する部署に向けて個人情報を含むデータの台帳を整備するよう指示しておく。

【ヒアリング調査に基づく分析】

- ✓ 個人情報保護法上、個人データの漏えい等（滅失・毀損を含む）のおそれがある場合には、個人情報保護委員会あるいは所管省庁への報告や、データ主体に対する通知を行う必要があるため、個人データの漏えい等のおそれの有無を確認することが必須となる。漏えい等のおそれがある全てのデータについて、それを管轄する部署が調査しなければならない場合もあり、復旧活動と並行しての対応となることから、現場には大きな負担となる。
- ✓ 暗号化され復旧できないデータがあった場合、漏えいデータの特定が困難なケースが多い。いかなるデータが漏えいしたのかをどのように確認すべきか、事案発生時に混乱した現場で効率的な手順を見いだすことは容易ではない。

【解説】

(1) 情報漏えい事案としての対応

ランサムウェア事案においては、攻撃者によってファイルサーバやデータベースへの不正なアクセスがあったものとして、情報漏えい事案としても捉えるべきであり、事前に組織内で取り扱う情報を把握しておくことが望ましい。特に、法令上の対応が必要となる個人情報について、いかなる範囲のデータがどこにどのような管理のもと保管されているかといった状況の把握は喫緊の課題といえる。攻撃者から脅迫がなくとも、攻撃者がファイルサーバやデータベースに不正にアクセスした可能性がある以上、ダークウェブ上などに情報が公開される可能性は否定できない。今回のヒアリングでは、脅迫型のものが見られたが、その対応には大変な労力が割かれたことが語られた。業務継続のための対応と並行しての対応となることから、極めて厳しい状況であったことが推察される。

【コラム】 ランサムウェア事案ではどのような場合に個人情報保護法上の報告義務が発生する？

個人情報保護法では、下記の要件に該当する場合、漏えい等報告が義務付けられている。

(1) 要配慮個人情報が含まれる個人データの漏えい等(又はそのおそれ)※民間事業者等
要配慮個人情報が含まれる保有個人情報の漏えい等(又はそのおそれ)※行政機関等

(2) 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等(又はそのおそれ）※民間事業者等
不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等(又はそのおそれ)※行政機関等

(3) 不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）の漏えい等(又はそのおそれ）※民間事業者等

不正の目的をもって行われたおそれがある当該行政機関の長等の属する行政機関等に対する行為による保有個人情報（当該行政機関の長等の属する行政機関等が取得し、又は取得しようとしている個人情報であって、保有個人情報として取り扱われることが予定されているものを含む。）の漏えい等(又はそのおそれ)※行政機関等

※「不正の目的をもって」の主体は、従業者だけではなく、盗難等第三者も含まれます。

(4) 個人データに係る本人の数が 1,000 人を超える漏えい等(又はそのおそれ)※民間事業者等
保有個人情報に係る本人の数が 100 人を超える漏えい等(又はそのおそれ)※行政機関等

(5) 条例要配慮個人情報が含まれる保有個人情報の漏えい等（又はそのおそれ）※地方公共団体の機関、地方独立行政法人

このうち（3）については、ランサムウェア攻撃による被害に関連して、以下のような場合も含まれることに留意が必要である。

- 不正アクセスにより個人データが漏えいした場合
  - 個人データを格納しているサーバー等において、外部からの不正アクセスによりデータが窃取された場合

- マルウェアに感染したコンピュータに不正な指令を送り、IP アドレス等への通信が確認された場合
- 不正検知を行う専門家等の第三者から漏えいのおそれについて連絡を受けた場合

● ランサムウェア等により個人データが暗号化され、復元できなくなった場合

出所）個人情報保護委員会「漏えい等の対応とお役立ち資料」
https://www.ppc.go.jp/personalinfo/legal/leakAction/

3.5 経営者主導の意思統一

【教訓】

> 組織内の意識のずれが大きいと混乱を招き、円滑な事案対応を阻害する。経営者は情報発信や権限委譲等の工夫を凝らし、組織の意思統一やスピード感のある対応を実現する。

【ヒアリング調査に基づく分析】

- ✓ 事態を自分事として捉えられない社員も存在し、危機に対する意識は社員間で必ずしも揃わない。経営者が自ら情報発信を通じて、現場に理解と協力を訴える取り組みも見られた。
- ✓ 同じ取引先に対して営業部門、情報システム部門、経営層等、複数の窓口と異なる経路があり、説明が矛盾しないよう統制することも重要であると語る組織もあった。対外的な説明・報告は統一的に行う必要がある。
- ✓ 迅速な対応を実現するために、現場の責任者の判断で進められるよう経営層が権限委譲した組織があった。さらに混乱や反発を抑えるため、当該責任者の指示に従うよう社内に周知するといった対応も見られた。
- ✓ 各部門から情報システム部門に問合せや苦情が殺到すると、現場の復旧作業が滞ることを懸念して、経営層がそうした直接の問合せを控えるよう指示したケースが複数見られた。情報システム部門の社員が業務過重や責任追及により離職してしまうことを懸念した、と語る経営者もいた。

【解説】

(1) 事案対応での権限委譲

ランサムウェア事案対応では、初動を含めて迅速な対応・判断が求められる。こうした判断を行うには、組織の IT 資産に精通している必要があり、情報システム部門による中心的な関与は必須である。事案対応を円滑に行うため、情報システム部門を中心とした権限委譲をすることが有効である。今回のヒアリングにおいても、ほぼ全ての組織で、情報システム部門を中心にした権限委譲が行われていた。さらに、その活動が阻害されないよう、組織内の他部門からの、情報システム部門への直接問合せを禁止したり、課題管理表により問合せ・依頼を一元化し負荷を考慮するなど、情報システム部門のパフォーマンスを阻害しないような仕組みを導入した組織が見られた。

(2) 社内の混乱への対策

ランサムウェア事案対応中は、社内には様々な混乱が発生する。したがって、事案対応の中心である経営者、情報システム部門による配慮や工夫が必要となる。たとえば、事案対応中の従業員には、平時とは異なる業務の進め方以外にも様々な一時的対応（外部メールの送信に関するルールの遵守、新しいウイルス対策ソフトを各自インストール等）が要求されるため、適切な手順書の整備はもちろん、間違った手順では実施できないようにシステム上の制限をかけるといった配慮が求められる。

3.6 窃取されたデータの暴露への備え

【教訓】

> 身代金を支払ってもデータの回復や暴露中止は保証されない。経営者はこの前提で窃取されたデータがダークウェブ上で暴露されるリスクに備えつつ、データ及びシステムの復旧を図る。

【ヒアリング調査に基づく分析】

- ✓ 殆どすべてのヒアリング対象組織で、経営層が「身代金は払わない」という決断を早期に判断していた。
- ✓ 身代金を払ってもデータの回復や情報の暴露中止が保証されるわけではなく、情報暴露を恐れて身代金を払うと脅迫され続ける可能性もあるとの理由で決断した組織が複数見られた。
- ✓ 身代金を支払わないという結論を出した場合でも、攻撃者と接触する手段を残しておくことで、攻撃者の活動状況を把握できたケースもあった。

【解説】

(1) 攻撃者との交渉

身代金を支払わないという結論を出した場合でも、攻撃者と接触する手段は把握しておく必要はある。攻撃者が提示するランサムノートや送付されたメールの内容は、それらを手掛かりにして、攻撃者の特定やリークサイトを把握できることがあり、侵害調査に利するだけでなく事案対応が終了した後の情報漏えいの監視にも有効である。

(2) ダークウェブ調査

情報漏えいはダークウェブ領域で発覚することが多いとされている。事案が収束した後にも、情報漏えいが発生する可能性があるため、ダークウェブ領域を一定期間、監視・調査することが望ましい。その場合、ダークウェブ領域に知見のあるセキュリティベンダー等の専門組織に依頼する形が一般的である。

【コラム】 身代金の支払いについて公的機関・団体等が提唱する方針

ランサムウェアに対する国際連携の取り組みとして日本政府も参加している多国間会合「カウンターランサムウェア・イニシアティブ（CRI）」は、2024 年の会合で、ランサムウェア攻撃を受けた組織を支援するためのガイドライン「GUIDANCE FOR ORGANISATIONS DURING RANSOMWARE INCIDENTS」[a]を発表した。本文献では、組織の一般的な対応として、2023 年の第３回 CRI サミットで発出された共同声明に従い、金銭支払いを避けることを強く勧めている。また、多くのランサムウェア・インシデントにおいて、サイバー犯罪者はデータも盗むようになっており、身代金を支払えば盗まれたデータを削除するという約束を信用してはならないこと、身代金を支払ってもデバイスやデータへのアクセスが保証されるわけではないことに注意するよう促している。

警察庁では、「暗号化されたデータを復号するための対価と称して、ランサムウェア攻撃グループから要求される金銭等を支払うこと」に関し、「犯罪グループ等の活動資金となることが懸念される」「暗号化されたデータの復号が保証されるわけではない」旨を被害者に対して説明するとともに、要求された金銭等の支払いの有無も含む、ランサムウェア被害に係る情報の提供をはじめとした捜査への協力を求めている[b]。

経済産業省は、2020 年に発出した注意喚起[c]において「データ公開の圧力から、攻撃者からの支払い要求に屈しているケースは少なくないとの報告は存在するが、こうした金銭の支払いは犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである」としている。

出所 a) CRI「GUIDANCE FOR ORGANISATIONS DURING RANSOMWARE INCIDENTS」
https://www.cyber.go.jp/pdf/press/CRI_Insurance_Guidance.pdf

出所 b) 警察庁「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

出所 c) 経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」, 2020/12/18
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/001_07_00.pdf

4　インシデント対処編

インシデント対処にあたる部門にとっての重要な教訓は以下の通りである。

表 2 インシデント対処に当たる部門が重視すべき教訓

担当者の分類	教訓
インシデント対処	(1) バックアップとログの整合性確保
	(2) 基本的な対策の徹底
	(3) EDR 導入と定期ログ監査
	(4) 「漏えいなし」の証明は困難
	(5) セキュリティベンダーとの関係構築

(1) バックアップとログの整合性確保

バックアップは、汚染された可能性があるとシステム復旧に活用できない。少なくとも侵入開始時期よりも前の時点のバックアップは安全であることから、侵入開始時期を特定することの重要性は高い。そのため、必要なログを保存し、安全な復元時点を判断できるようにしておく。

(2) 基本的な対策の徹底

ランサムウェアの被害の多くは基本的な対策ができていないことに起因する。基本的な対策を徹底・継続する。加えて、境界防御に隙を作らず、内部ネットワークが安全ではないことを前提にした対策とその維持を徹底する。

(3) EDR 導入と定期ログ監査

従来型のウイルス対策ソフトのみでは、攻撃者の活動を十分に検知することができない場合がある。EDR 等を導入するとともに、アラートに迅速に対応できる監視体制を整備し、定期的にログを確認・分析する。

(4) 「漏えいなし」の証明は困難

顧客や取引先に対して「情報漏えいがなかったこと」を証明することは極めて困難。顧客や取引先には、フォレンジック調査等から判明した事実や経過観察の状況を、必要な範囲で丁寧に報告していくことになる。

(5) セキュリティベンダーとの関係構築

ランサムウェア事案への対応において、セキュリティベンダーが果たす役割は非常に大きい。一方、セキュリティベンダーに求められる役割は、組織の体制やインシデントの状況によって異なり、ベンダーごとに対応可能な範囲も異なるため、平時から必要な役割と対応範囲を把握し、適切なベンダーを選定し関係を構築しておく。

【コラム】 代替システムにはどんなものを使う？

ランサムウェアにバックアップを侵害された場合には、バックアップからシステムを復旧することができない。今回のヒアリングでも、そうした状況から復旧に取り組んだ組織が見られた。事案対応の中で、社外コミュニケーションツールとして、短期間でのリリースが可能なクラウドサービスによるメールやチャットを活用した例が多く、そのまま継続して本番運用にした組織も複数見られた。海外拠点とのネットワーク接続も含め SASE を活用する等、比較的新しいサービスの導入を進めたケースも見られた。

4.1 バックアップとログの整合性確保

【教訓】

> バックアップは、汚染された可能性があるとシステム復旧に活用できない。少なくとも侵入開始時期よりも前の時点のバックアップは安全であることから、侵入開始時期を特定することの重要性は高い。そのため、必要なログを保存し、安全な復元時点を判断できるようにしておく。

【ヒアリング調査に基づく分析】

- ✓ ランサムウェア事案の復旧は、バックアップからの復元が基本となるが、バックアップをもとに復旧する場合は、システムやデータをバックアップからリストアが可能かどうか、そのバックアップが安全かどうか、を見極める必要がある。
- ✓ 侵入の開始時点を特定できないと、バックアップの汚染の可能性を判断できない。バックアップをネットワークから切り離すなどして、バックアップの安全を確保すると同時に、侵害時期を調査できるよう必要なログを保存し、安全な復元時点を判断できるようにしておく必要がある。
- ✓ バックアップからリストアすることで発生するロールバックは、実際の業務に与える影響が大きい。ヒアリングでは、リストアで発生したロールバックのデータ補正のために、さらなる手作業が必要になり、大きな負担となって現場の疲弊につながった組織があった。システムの安全な復旧の要請が、業務負荷の増加を引き起こす場合があることを、「システム目線と業務目線の違い」と表現する組織もあった。

【解説】

(1) バックアップに関する考慮点

侵害されたシステムやデータを復旧するにあたっては、まず安全かつリストア可能なバックアップがあるかどうかと、次にリストアしたデータによって発生するロールバックがもたらす影響に業務運用が耐えうるかどうかを確認する必要がある。ランサムウェア事案では、侵害範囲の調査と並行して、バックアップの安全性、リストアの実現性を見極める必要がある。さらに、バックアップからリストアすることで発生するロールバックが業務に与える影響は少なくない。システム上は短時間のロールバックでも、業務上は大規模なデータ補正が必要となる場合もあり得る点を考慮しなければならない。

(2) ログに関する考慮点

侵害範囲の把握、侵入経路の特定、安全なデータの確保のいずれにおいても残存するログを調査することから始まる。侵害調査では、「調査に使えるもの」が調査対象となるため、Firewall やサーバのシステムログといったものから、ウイルス対策ログや操作ログ、ネットワーク機器の通信ログ等の様々な記録が使われる。セキュリティインシデントとは一見関係がないようなログも使われることがあるため、どこにどのようなシステムのログが存在するか、または存在する可能性があるかを組織または運用・保守事業者が把握していることが望ましい。今回のヒアリングでは、攻撃者の活動痕跡を発見できたものとして、PC の資産管理ソフトによる操作ログを挙げた例がいくつか見られた。

4.2 基本的な対策の徹底

【教訓】

> ランサムウェアの被害の多くは基本的な対策ができていないことに起因する。基本的な対策を徹底・継続する。加えて、境界防御に隙を作らず、内部ネットワークが安全ではないことを前提にした対策とその維持を徹底する。

【ヒアリング調査に基づく分析】

- ✓ ヒアリング対象の全ての組織で一般的なセキュリティ対策は実施されており、運用体制も整えられていたが、セキュリティ更新プログラムの適用の遅れや一時的な設定変更の放置等、わずかな隙をついて侵入され、さらに内部ネットワークの対策の弱さを突いて侵害が拡大された。
- ✓ 初期侵入においては既知の脆弱性を悪用され、初期侵入後の侵害拡大は「安易なパスワード」、「アップデートしていない NAS」、「管理者アカウントでの運用管理」等が主原因であった。このうち侵害拡大を許した要因は、従前の境界防御で足りるとして「内部ネットワークは安全である」ことを前提とした運用設計により生じた脆弱性といえる。
- ✓ Active Directory を侵害されたケースが多い。Windows OS には多くのセキュリティ機能があり、バージョンアップにより機能が追加されているが、十分に活用されていない可能性が窺える。
- ✓ 管理者アカウントやパスワードといったシステム上の重要管理情報が通常のファイルと同じ扱いをされていることがインシデント時の調査で発覚したとする組織もあった。

【解説】

(1) 基本的対策の徹底・継続

初期侵入や侵害拡大には、脆弱性の悪用や簡易な設定の悪用が多い。したがって、セキュリティ更新プログラムのタイムリーな適用、管理者権限の最小化、不要なアカウントの削除といった基本的対策を細部まで徹底し、継続することが重要となる。今回のヒアリングでは、全ての組織で一般的なセキュリティ対策は導入されており、運用体制も整えられていた。しかし、いずれのケースでも「セキュリティ更新プログラムの適用に少し時間を要した」「一時的な運用のために設定変更し、そのままにしていた」といった、日常の運用に生じたわずかな隙をついて初期侵入がなされ、さらに「ネットワーク内部なので簡易な設定

を許容していた」「システム管理の利便性を考慮した」といった内部ネットワークの弱点を突いて侵害が拡大していた。

(2) Active Directory サーバの保護

Active Directory 自体へのセキュリティ対策が必要であり、標準で利用可能なセキュリティ機能を実装することが望ましい。Active Directory への侵害は、ランサムウェア事案においても多く見られており、攻撃者の目標物の一つとなっていることが窺える。攻撃者は Active Directory の管理者権限を取得することで、組織の Windows OS のユーザー情報を取得したり、ドメイン参加しているコンピュータにランサムウェアを一斉に配布するなど効率的に侵害することが可能になる。Active Directory の設計の主題はシステム管理ツールとしての活用であり、データの保護や制限のためのセキュリティ対策はシステム管理の利便性と相反することがあるため、十分に実施されていないケースもある。一方で、Active Directory のセキュリティ対策機能は、各種、継続的にリリースされている。これらのセキュリティ対策機能を適時取り入れることは、セキュリティ対策として非常に効果的である。

(3) システム管理情報の保護

管理者アカウントやパスワードといったシステム上の管理情報は特別に保護する必要がある。ところが、これらの情報は、システム管理業務に必要なため、テキストファイルや Excel ファイルとして運用管理 PC やファイルサーバに置かれているなど、その保護が十分に意識されていない場合がある。ランサムウェア事案では、これらのファイルを窃取される可能性がある。今回のヒアリングでも、これらのファイルが侵害された範囲にあったとして、直接的な被害がなかった海外支社のシステムの設定変更を実施した組織があった。システム的な対策と合わせて、これらのデータそのものの保護対策が望ましい。

(4) ネットワークの分割・分離

ネットワークセグメントをベースにした対策は、取り入れるべきである。組織の防御において、ネットワークセグメントをベースにした対策は効率的に実施しやすい。今回のヒアリングでは、組織内部のセグメント分割とその制限内容によって、侵害の範囲が異なっていたとする組織が多かった。

(5) 海外拠点でのセキュリティ対策・インシデント対応

ランサムウェア事案は日本国内のみならず、海外拠点でも起こり得る。今回のヒアリングでは、海外拠点と日本国内で取り得るセキュリティ対策やインシデント対応体制が異なることが指摘された。そのような場合、組織全体の侵害調査の範囲やその内容に不備や不足が出てしまうことがある。事後の対策として、海外拠点のセキュリティ対策の統合や、インシデント対応体制の整備を進めると語る組織もあった。

【コラム】 海外拠点対応について考慮すべき点

インシデント対応において、日本国内と海外拠点との間の差異として以下の点が挙げられる。

まずは IT インフラの差異である。M&A によってグループ企業化した海外拠点は、そもそもネットワークやセキュリティに関する IT インフラが本社と異なることがある。例えば、本社では各業務用のアカウントについて多要素認証を徹底できているのに海外拠点ではできていないことに起因して不正アクセスを受けたり、本社では EDR を導入しているので EDR によるログ監視や隔離がスムーズにできるのに対して海外拠点ではそれができないため被害が拡大しやすいといった差異が生じる。

また、法令や法慣習の違いもある。例えば、米国ではサイバーインシデントにより個人データが漏えいすると、漏えいした個人データの主体によってクラスアクション（集団訴訟）が比較的容易に提起される。そうなると、日本国内の対応と比べて、訴訟で不利にならないようにフォレンジック調査や対外公表を慎重に進める必要性が高くなる。

4.3 **EDR** 導入と定期ログ監査

【教訓】

> 従来型のウイルス対策ソフトのみでは、攻撃者の活動を十分に検知することができない場合がある。EDR 等を導入するとともに、アラートに迅速に対応できる監視体制を整備し、定期的にログを確認・分析する。

【ヒアリング調査に基づく分析】

- ✓ 現在のランサムウェア攻撃で使われる手法は、高度な標的型攻撃（APT（Advanced Persistent Theart）攻撃）で使われる隠密性の高い手法と共通点も多い。LOTL(Living Off The Land)攻撃、すなわち OS 標準ツール等の正規のツールを悪用する手法も使われており、マルウェアの検知を前提とするウイルス対策ソフトだけで全てを検知し防ぐことは難しい。
- ✓ サーバや PC の挙動を監視し、不審な動作を検知・停止する EDR(Endpoint Detection and Response)[4]は、ウイルス対策ソフトを補完する対策として検討すべき。
- ✓ 暗号化を検知した際、管理者宛てのアラートメールが発出されていたが、週末の深夜だったため、タイムリーに受け取れていなかった事例もあった。検知だけでなく、アラートに常時対応できる監視・運用体制が必要である。
- ✓ 取引先から、メールや EDI を再開するなら EDR や SOC(Security Operation Center)[5]を導入するよう強い要望があったとする組織も複数あった。
- ✓ 攻撃者の活動には、ウイルス対策ソフトや EDR を含むセキュリティ対策の無効化もあり得る。また LOTL 攻撃を使われた場合、検知をすり抜ける可能性がある。セキュリティ対策の状態変化や LOTL 攻撃の痕跡を発見するには、攻撃検知がないとしても、その可能性を考慮し、ログを確認することは有効である。定期的にログ監査を実施することで発見できる可能性が高まる。

---

[4] サーバおよび PC 内の処理や外部との通信等の不審な振る舞いを検知することで迅速な対応を可能にする。(出所：IPA「情報セキュリティ 10 大脅威 2025：セキュリティ対策の基本と共通対策」, 2025/2, https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kihontokyoutsuu_2025.pdf)

[5] セキュリティ・サービス及びセキュリティ監視を提供するセンター。(出所：NCO「サイバーセキュリティ 2025（2024 年度年次報告・2025 年度年次計画）別添 4 用語解説」, 2025/6, https://www.cyber.go.jp/pdf/policy/kihon-s/cs2025.pdf)

【解説】

(1) PC やサーバへの侵害の検知

現在のランサムウェア攻撃は、まず組織ネットワークや PC、サーバへの侵入が行われ、最終段階として暗号化が行われる、というのが実態である。これらをウイルス対策ソフトだけで検知し防ぐことは難しいため、ウイルス対策ソフトを補完する対策として、PC やサーバ（エンドポイント）の挙動を監視し、不審な動作を検知・停止する EDR を検討することが望ましい。ステークホルダーから事後対策としての EDR や SOC の導入を要望されたケースが複数あり、EDR や SOC の認知度が高まっていることが窺える。

【コラム】 EDR について考慮すべき点

EDR はかなり普及してきた印象であるが、ウイルス対策ソフトと異なり、EDR は導入するだけで十分ではない点に注意が必要である。

EDR は端末上の不審な動作を検知・停止することが機能として期待されるが、検知したら自動的に停止させるモードだけではなく、誤検知による業務への負担に配慮して検知したらアラートを発出させてユーザーに停止させるか否かを判断させるモードもある。後者の場合は、ユーザーが積極的に停止を選択するまで不審な挙動は継続するので被害が拡大することになる。

したがって、EDR や SOC の導入にあたっては、その機能や設定を細やかに確認する必要がある。

4.4 「漏えいなし」の証明は困難

【教訓】

> 顧客や取引先に対して「情報漏えいがなかったこと」を証明することは極めて困難。顧客や取引先には、フォレンジック調査等から判明した事実や経過観察の状況を、必要な範囲で丁寧に報告していくことになる。

【ヒアリング調査に基づく分析】

- ✓ フォレンジック調査は攻撃者の活動痕跡を詳細に把握するために必要な調査であり、ヒアリングでもほぼ全ての組織でフォレンジック調査を実施、その結果を基に取引先へ事実関係を説明していた。
- ✓ セキュリティベンダー等によるフォレンジック調査は、侵害の原因や被害の範囲の特定に有用だが、攻撃者の活動すべてを明らかにできるとは限らない。
- ✓ 複数のヒアリング先で、情報漏えいがなかったとの証明をセキュリティベンダーからもらうよう取引先から求められていたが、フォレンジック調査で攻撃者の活動が全て明らかにできるわけではないため、セキュリティベンダーもそうした保証は難しい。

【解説】

(1) フォレンジック調査

侵害された PC やサーバの詳細調査としてフォレンジック調査がある。攻撃者の活動痕跡を詳細に把握するために必要な調査であり、攻撃の起点となった可能性のあるものや重要資産である機器には実施するべきである。ただし、調査のコストが高額であり、調査時間もある程度必要なため、対象機器の全てに実施することが難しい場合は、攻撃の起点になったと思われる機器を優先することが考えられる。たとえば、侵入経路として利用される VPN のログや AD サーバのログが想定される。なお、フォレンジック調査によって、データ持ち出しを含めて全ての攻撃者の活動が明らかになるわけではない点に留意する必要がある。また、被害組織は、フォレンジック調査に基づくセキュリティベンダーの見解を、被害状況の対外説明に活用することができる。今回のヒアリングでも、ほぼ全ての組織でフォレンジック調査を実施し、その結果をもとにステークホルダーへの説明を行っていた。もっとも、調査で判明した事実をどの範囲まで

開示するかは、二次被害の防止や調査の進捗等を考慮した各組織の判断となるため、説明の相手方や時期に応じて、説明が必要な範囲を検討することが望ましい。

(2) 攻撃者の特定

使用されたランサムウェアの特定は、多くの場合、攻撃者グループの特定につながる。攻撃者グループを特定できれば、そのグループの TTPs の把握につながり、侵害範囲の特定に利用できる情報が得られることがある。また、暗号化を実行するランサムウェアを特定できた場合は、PC やサーバの感染有無の判定に有用な手掛かりとなる。しかし、攻撃者はランサムウェアだけを使って攻撃、侵害する訳ではなく、初期侵入、侵害拡大において、様々な経路やツールを用いる。事案対応において、攻撃者が使った経路、ツールについて仮説を立て、その検証のための調査を実施することは重要である。さらに、攻撃者グループの活動は、各国の法執行機関やセキュリティベンダー、リサーチャーが長期的に追跡しているため、事案発生時には判明しなかった事実についても、事後に何らかの情報を得られる可能性もある。このため、事案の収束後も攻撃者グループに関する情報収集を継続することが望ましい。

4.5 セキュリティベンダーとの関係構築

【教訓】

> ランサムウェア事案への対応において、セキュリティベンダーの果たす役割は非常に大きい。一方、セキュリティベンダーに求められる役割は、組織やインシデントの状況によって異なり、ベンダーごとに対応可能な範囲も異なるため、平時から必要な役割と対応範囲を把握し、適切なベンダーを選定し関係を構築しておく。

【ヒアリング調査に基づく分析】

- ✓ インシデント対応においてセキュリティベンダーの果たす役割は大きい。もっとも、ひとことでセキュリティベンダーといっても、いわゆる専門技術の提供となるログ調査やマルウェア解析、フォレンジック調査以外にも、調査結果に基づく対策の立案やインシデントのハンドリング業務、被害公表のやり方、取引先への説明の仕方といったコンサルティング業務等、その活動範囲は非常に幅広い。ヒアリングしていても、セキュリティベンダーの活動をプロジェクトマネジメントと評した組織もあるなど、組織の体制や事案の状況によって、セキュリティベンダーに求める役割は異なることが窺えた。
- ✓ 複数のヒアリングで「セキュリティベンダーが途中で交代」していた事からも、インシデント対応中の短期間に信頼関係の構築は難しいと考えられるため、できることなら事前に関係構築ができていることが望ましい。

【解説】

(1) インシデントハンドリング業務

インシデント対応の全体をハンドリングするインシデントハンドリング業務は重要である。豊富な知見を持つセキュリティベンダーに支援を依頼するという方法もある。セキュリティ管理部門や情報システム部門がハンドリングしていくことが望ましいが、組織の IT 資産や業務体制の把握以外にも、インシデント対応そのものの経験値による知見も必要とされる。今回のヒアリングでも、「うまくいった部分」として、組織の事業継続や復旧方針を踏まえた助言をしたセキュリティベンダーの例があった。セキュリティ

ベンダーへの依頼は、フォレンジック調査といった個別の専門的調査だけでなく、インシデントハンドリングへの支援を選択することも可能である点は理解しておきたい。

（2）調査スコープ

セキュリティベンダーに期待したい支援として「調査のスコープ」がある。時間的猶予がない中で、迅速に侵害調査を進めるには、この何を調査対象とするのか、という調査スコープの範囲の検討が重要である。どの範囲を対象に調査するべきかは事案ごとによって異なり、たとえば VPN 経由での侵入が典型的なランサムウェア事案では VPN 経路が存在するなら VPN を調査対象とすべきであるが、組織側ではこのような判断ができないことが多い。豊富なインシデント対応経験のあるセキュリティベンダーによる調査スコープの立案は必須といってよく、できれば事前に信頼できるベンダーを複数候補選定しておきたい。さらにいえば、セカンドオピニオンの取得を検討しておくことが望ましい。

5 まとめ

ランサムウェア事案は、インシデント発覚直後から、時間的猶予のない状況で、事業継続/中断の判断、メディア対応、さらに攻撃者からの脅迫への対処等の経営判断を迫られる点で、一般的な IT インシデントとは大きく異なる。したがって、経営者はそうした特性を正しく理解した上で、ランサムウェア事案に対する組織の耐性を高めるべく、社内外の体制・枠組みを整備し直し、事前対策の着実な遂行と事案発生時の円滑・柔軟な対処の実現に向けた準備を進める必要がある。

具体的には、経営者や経営・リスク管理部門は、事案発生時に迅速に判断できるよう、何が起こり得るかを正しく理解し、事前に対応業務の分担を明確にしておくことが必要である。事業継続のために、ランサムウェア事案に対応できるよう事業継続計画を見直すとともに、インシデント対処部門だけでなく事業部門も含めた全社的な対応を実現すべく、必要に応じて関係者が互いに協力し合える体制を構築すること、どこでどんな情報を保有しているか把握しておくことが必要である。また、インシデント対処部門は、平時においては基本的なセキュリティ対策を行った上で、ランサムウェア事案発生時に効率的・効果的に対応できるように、復旧を想定したバックアップ、攻撃活動を捕捉するための EDR 導入等、事前に十分な準備・対策を実施しておくことが必要である。繰り返しになるが、これらを組織内に実装するためには、経営者からの明示的な働きかけが極めて重要である。

参考として、本教訓集の内容から、事前の備えに重点を置いたランサムウェア対策を以下に示す。

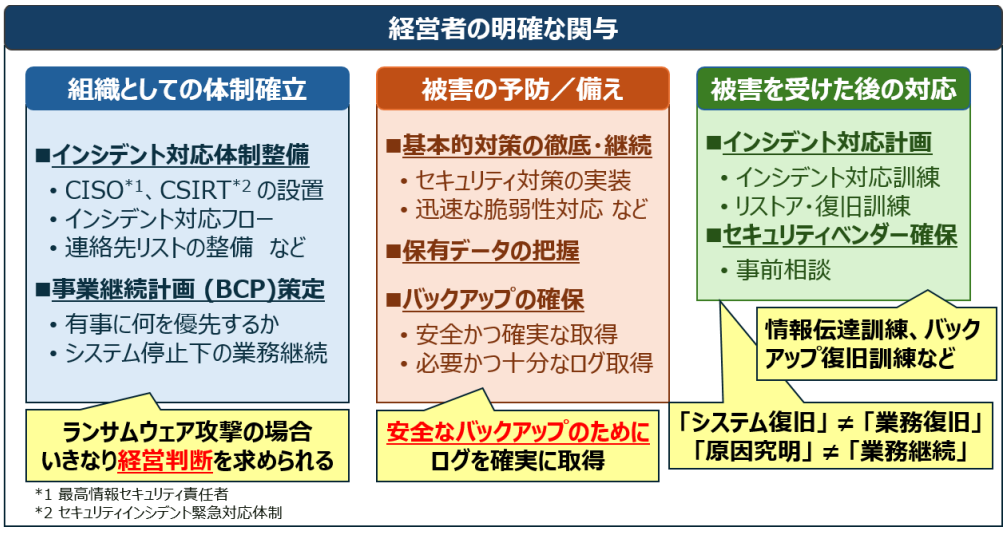

図 3 事前の備えに重点を置いたランサムウェア対策

参考　公開ドキュメントにおけるランサムウェア対策の例

参考として、公的機関の文献で採り上げられたランサムウェア対策の例について、以下に紹介する。詳細については、各文献を参照頂きたい。

(1) IPA 「情報セキュリティ10大脅威2026 解説書（組織編）」

(https://www.ipa.go.jp/security/10threats/omgdg50000008fi8-att/kaisetsu_2026_soshiki.pdf)

IPA では、情報セキュリティの専門家等の協力を得て、主に前年に発生した社会的影響が大きかったセキュリティの事故や攻撃の状況等から脅威候補を選出し、「情報セキュリティ 10 大脅威」を投票により決定している。「情報セキュリティ 10 大脅威」は組織編と個人編で構成されているが、ここでは組織編の解説書を紹介する。2026 年 3 月に公開された本書は、「ランサム攻撃による被害」の対策・対応として、以下を挙げている。

【経営者層】

A) 被害の予防および被害に備えた対策
- インシデント対応体制の整備
- サイバー保険の検討
- セキュリティ対策のための予算確保
- 身代金要求に対する姿勢を決めておく

【システム管理者、従業員、職員】

A) 被害の予防および被害に備えた対策
- インシデント対応体制を整備し対応する
- 「情報セキュリティ対策の基本」を実施（

・　表 3 参照）
・　安易に添付ファイルの開封やリンク・URL のクリックをしない
・　多要素認証（MFA）や FIDO／FIDO2（パスキー11 など）を利用する
・　提供元が不明なソフトウェアを実行しない
・　PC やサーバー、ネットワーク機器、Web サイト等に適切なセキュリティ対策を行う
・　ディレクトリーサービスや共有サーバー等へのアクセス権の最小化と管理の強化

表 3 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
マルウェアの利用	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取による情報漏えい等のリスクを低減する
設定不備	設定の見直し	誤った設定が悪用され、攻撃を受けないようにする
データの暗号化	バックアップの取得	PC やサーバーのデータ削除や暗号化に備える
ソーシャルエンジニアリング（罠にはめる）	脅威・手口を知る	手口から重視すべき対策を理解

- 不要なポートは閉じ、必要なサービスのみに絞る
- 公開サーバーへの不正アクセス対策
- 適切な取得日時、頻度を検討し、バックアップ運用を行う
  - WORM（Write Once Read Many）機能等バックアップ自体の改ざん耐性強化策やバックアップからの復旧訓練の実施も有効。
- 暗号化された場合を想定したクリーンビルドの手順確立
- 定期的な復旧訓練の実施
- 例外措置の定期的な見直し、例外適用範囲の最小化

B) 被害を受けた後の対応

- 適切な報告／連絡／相談を行う
- 適切に運用されているバックアップデータからのリカバリーを行う
- 整備した対応体制に基づき対応する

(2) NIST IR8374 Rev.1 Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile

(https://csrc.nist.gov/pubs/ir/8374/r1/final)

同資料は、米国国立標準技術研究所（National Institute of Standards and Technology）（以下「NIST」という。）の「Cybersecurity Framework 2.0」（以下「CSF 2.0」という。）におけるセキュリティ上の成果のうち、ランサムウェア事案における統治・管理、特定、防御、検知、対応、および復旧を支援するものを示した文書で、NIST が 2022 年 2 月に発行したものを 2026 年 6 月に改訂している。ランサムウェア事案のリスクを管理するための指針としての利用やランサムウェア事案対応のプレイブックにも利用できるものとしている。

「基本的なランサムウェア対策（Basic Ransomware Tips）」として挙げられている６項目を紹介する。

表 4 基本的なランサムウェア対策（Basic Ransomware Tips）

1. ランサムウェア事案に備えて計画を立てる
組織としての優先事項を定め、許容できるリスクの水準を明確にして、事業上のニーズとリスクに合致したランサムウェア対策を選定する指針とする。（GV.OC-01, GV.RM-02, GV.RM-03）
誰が意思決定者であるかを把握する。サイバーセキュリティ上の説明責任と明確な意思決定を促進するために、役割と責任を定める。（GV.RR-02）
法的要件を洗い出す。サイバーセキュリティリスクおよび対応に影響する法的、規制上、契約上の要件を理解し、管理する。（GV.OC-03）
2. ランサムウェア感染を回避する方法について従業員を教育する
定期的にフィッシング訓練やソーシャルメディア上の模擬訓練を実施し、不明な送信元からのファイルを開いたりリンクをクリックしたりしないよう従業員を訓練する。（PR.AT-01）
年次研修および定期的なセキュリティ注意喚起を通じて、私物デバイスを業務ネットワークに接続することのリスクを従業員に教育する。（PR.AT-01）
サイバーリスクを引き起こした行為について従業員を非難するのではなく、疑わしいサイバー事案を直ちにセキュリティ担当へ報告するよう促すことで従業員の主体的対応を支援する、インシデント報告の文化を醸成する。（PR.AT-01）

3. ランサムウェアが悪用できる脆弱性をシステムに残さない

関連するシステムに最新のパッチを確実に適用する。利用可能なパッチを特定するための定期確認を実施し、実行可能になり次第できるだけ早く適用する。(ID.AM-02, PR.PS-01)

すべてのネットワーク接続システムでゼロトラスト原則を採用する。すべてのネットワーク機能へのアクセスを管理し、実行可能な場合は内部ネットワークを分割して、マルウェアが標的となり得るシステム間に拡散するのを防ぐ。(PR.AA-01, PR.AA-03, PR.AA-05, PR.IR-01)

許可されたアプリのみインストールおよび実行できるようにする。OS やサードパーティ製ソフトウェアを設定し、承認済みアプリケーションのみ実行されるようにする。これは、許可リストに登録するアプリケーションの追加・削除を審査する方針を採用することでも支援できる。(PR.PS-05)

技術ベンダーに対し、ランサムウェア攻撃を軽減するため、リスクに見合ったサイバーセキュリティ対策を講じることを期待している旨を伝える（例：契約条項に明記する)。(GV.SC-02)

4. ランサムウェア攻撃や感染を迅速に検知し、阻止する

常時、マルウェア検知ソフトウェア（エンドポイントセキュリティ製品など）を使用する。メールや USB メモリを自動的にスキャンするよう設定する。(DE.CM-09, DE.AE-02)

ディレクトリーサービス（およびその他の主要なユーザー情報ストア）を継続的に監視し、侵害の兆候や進行中の攻撃を検出する。(DE.CM-03, DE.AE-02)

信頼できない Web リソースへのアクセスを遮断する。悪意があることが判明している、または悪意あるシステム活動の兆候と疑われるサーバ名、IP アドレス、ポート、プロトコルへのアクセスを遮断する製品やサービスを利用する。これには、アドレスのドメイン部分（例：hacker@poser.com）の完全性保護を提供する製品やサービスの利用も含まれる。(ID.AM-03, DE.CM-01)

5. ランサムウェアが拡散しにくいようにする

可能な限り、管理者権限を持つアカウントではなく、多要素認証を備えた標準ユーザーアカウントを使用する。(PR.AA-01, PR.AA-05)

パスワードの推測を自動で試みる攻撃への防御として、認証時の遅延を導入する、または自動アカウントロックアウトを設定する。（PR.AA-01, PR.AA-05）
すべての企業資産およびソフトウェアについて認証情報の権限付与を割り当て・管理し、最小権限の原則に従って、各アカウントが必要最小限のアクセス権のみを持っていることを定期的に確認する。（PR.AA-05, PR.AA-06, PR.IR-01）
データを不変形式で保存する（新しいデータが利用可能になった際に、データベースが古いデータを自動的に上書きしないようにする）。（PR.DS-11）
内部ネットワーク資源への外部アクセスは、安全な VPN 接続経由のみに限定する。（PR.AA-03）
6. 将来のランサムウェア事案から復旧しやすくする
インシデント対応・復旧計画を策定する。役割分担と意思決定戦略を明確にしたうえで、インシデント対応・復旧計画を策定、実施し、定期的に演習する。これは事業継続計画の一部として組み込むこともできる。計画には、復旧の優先順位付けを可能にするために、任務遂行上重要なサービスやその他の事業継続に不可欠なサービス、およびそれら重要サービスの事業継続計画を特定しておく必要がある。また、ランサムウェア事案によって通常の業務連絡手段が妨害された場合に備え、帯域外通信の戦略も含めるべきである。（RS.MA-01, RS.CO-02, RC.RP-01, RC.CO-03）
データをバックアップし、バックアップを保護し、復元をテストする。データのバックアップおよび復元戦略を慎重に計画、実装、検証するとともに、重要データのバックアップを保護し、隔離する。（PR.DS-11, RC.RP-03）
連絡先を整備しておく。法執行機関、法務顧問、インシデント対応支援先を含む、ランサムウェア攻撃時の社内外の連絡先一覧を常に最新の状態に保つ。（RS.CO-02, RS.CO-03, RC.CO-03, RC.CO-04）
ランサムウェア保険を検討する。サイバー保険は、特に中小企業にとって、ランサムウェア事案による財務的圧力を軽減し、対応および復旧の間も組織が事業を継続できるよう支援する可能性がある。（GV.RM-03）

（出所：NIST IR8374 Rev.1「Basic Ransomware Tips」を IPA が翻訳・編集。この表は NIST の公式訳ではありません。）

（補足）

表 4 の各項の文末にある（英文字-数字）の文字列は、CSF 2.0 におけるコアの機能及びカテゴリー（表 5 参照）と、そのカテゴリーに含まれる個別の成果項目（Outcome）の参照番号を表している。

表 5 CSF 2.0 コア機能及びカテゴリーの名称と識別子

機能	カテゴリー	カテゴリー識別子
統治（GV）	組織の状況	GV.OC
	リスクマネジメント戦略	GV.RM
	役割、責任、権限	GV.RR
	ポリシー	GV.PO
	監督	GV.OV
	サイバーセキュリティサプライチェーンリスクマネジメント	GV.SC
識別（ID）	資産管理	ID.AM
	リスクアセスメント	ID.RA
	改善	ID.IM
防御（PR）	アイデンティティ管理、認証、アクセス制御	PR.AA
	意識向上とトレーニング	PR.AT
	データセキュリティ	PR.DS
	プラットフォームセキュリティ	PR.PS
	技術インフラのレジリエンス	PR.IR
検知（DE）	継続的監視	DE.CM
	有害事象の分析	DE.AE
対応（RS）	インシデント管理	RS.MA
	インシデント分析	RS.AN
	インシデント対応の報告とコミュニケーション	RS.CO
	インシデントの軽減	RS.MI
復旧（RC）	インシデント復旧計画の実行	RC.RP
	インシデント復旧のコミュニケーション	RC.CO

（出所：NIST「Cybersecurity Framework 2.0」（IPA 翻訳版）より表を抜粋。同資料は NIST の公式訳ではありません。）

https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf

本レポートに関する問い合わせ先

IPA：コンピュータウイルス・不正アクセス届出窓口

https://www.ipa.go.jp/security/todokede/crack-virus/about.html

Beyond Digital

独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan