日本のサイバーセキュリティを「連携」「学び」「創造」

サイバー攻撃を受けるとお金がかかる

～インシデント損害額調査レポートから考えるサイバー攻撃の被害額～

JNSA 調査研究部会 インシデント被害調査WGリーダー　神山太朗

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

はじめに：要旨

サイバー攻撃を受けると

お金がかかる

中小企業においても**数千万**単位、
場合によっては**億**単位のお金がかかる

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

はじめに：レポートについて

「インシデント損害額調査レポート」

◇JNSA（日本ネットワークセキュリティ協会）という、セキュリティベンダの業界団体がまとめている、インシデントが発生した場合の**損害額**をまとめたレポート

◇「本紙」「別紙」の**2部構成**

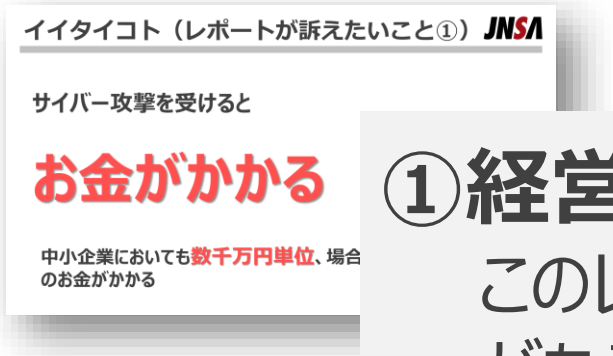
本紙	インシデント対応にかかる**アウトソーシング先へのヒアリング**を中心とした調査
別紙	公表・報道のあった被害組織をリストアップ これら**被害組織に対するアンケート**による調査 一部の組織には、直接ヒアリング（インタビュー）も実施

◇検索サイトにて「インシデント損害額」で検索をかけると出てきます

インシデント損害額 Search

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

レポートの活用シーン（立場別）



①経営者

このレポートで、経営に多大な影響（最悪の場合、倒産）があるがゆえ、**対策の必要性**を**自ら理解していただく**

②情シス（セキュリティ担当者）

このレポートで、**対策の必要性**を**経営者に訴えていただく**

③IT/セキュリティベンダ

このレポートで、**対策の必要性**を**経営者、情シスに訴えていただく**

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

各種損害のコスト

～アウトソーシング先のヒアリング等からみえてくるコスト～

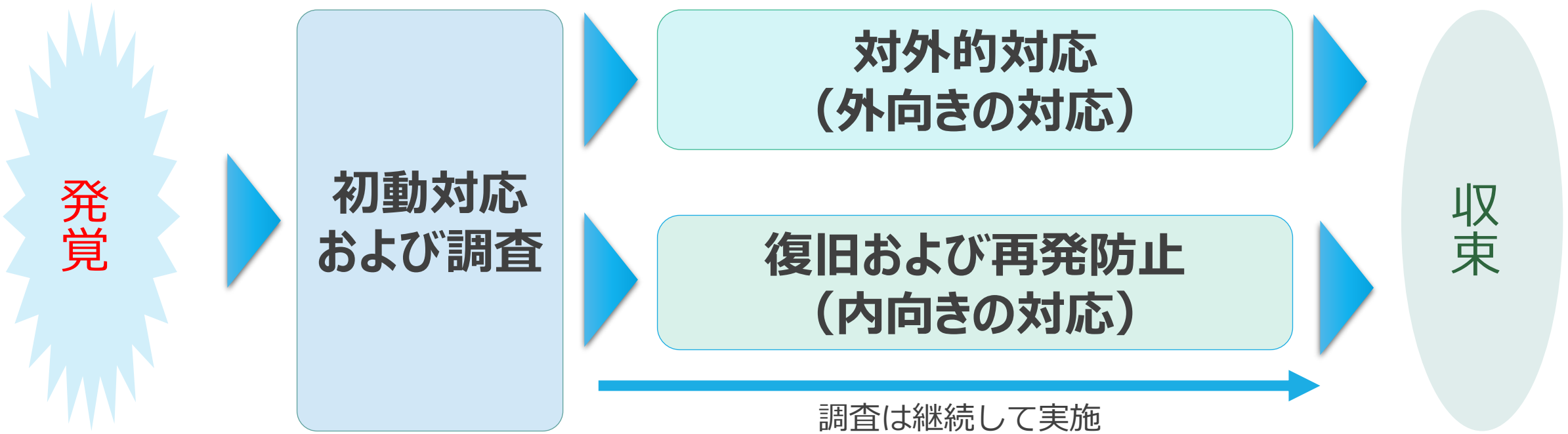
Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

前提：対応と各種損害

～インシデント対応の流れ、インシデントによって生じる各種損害～

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インシデント対応の流れ



Copyright 2024 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

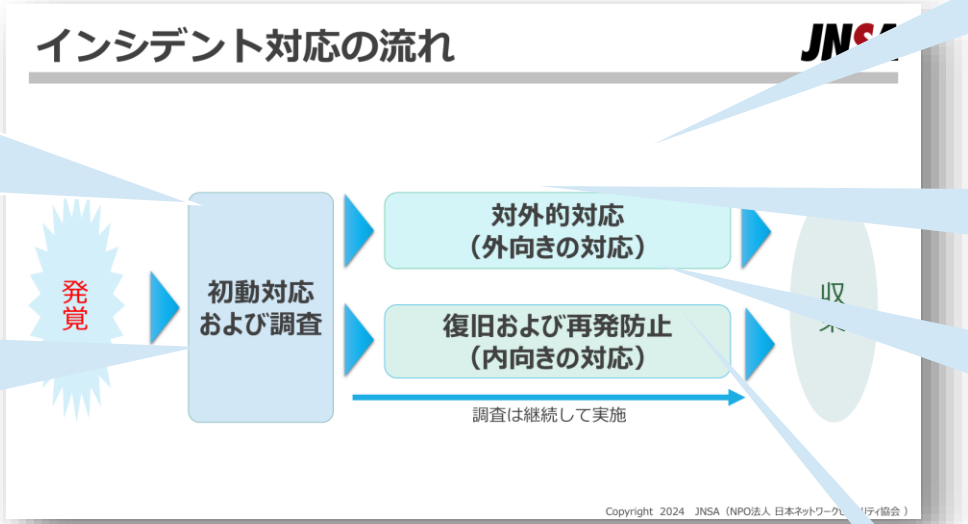
アウトソーシングの必要性

専門の会社に調査
（フォレンジック調査）を委託

300万円

法律事務所に
対応等を相談

100万円



被害者に詫び状を
送付 **130万円**

コールセンター会社に
クレーム対応を委託
600万円

出入りのITベンダに
システム復旧を依頼
500万円

セキュリティベンダに
再発防止策を依頼
200万円

自社だけでの対応は困難…。
専門の会社への**アウトソーシング**も必要

Copyright 2024 JNSA（NPO法人 日本ネットワークセキュリティ協会）

インシデント発生時において生じる損害

各種事故対応についてアウトソーシング先への支払が発生

1．費用損害（事故対応損害）	被害発生から収束に向けた**各種事故対応**に関してアウトソーシング先への支払を含め、自社で直接費用を負担することにより被る損害（下記２～６に該当しないもの）

さらに、次のような損害の発生も・・・

2．賠償損害	情報漏えいなどにより、第三者から損害賠償請求がなされた場合の**損害賠償金**や弁護士報酬等を負担することにより被る損害
3．利益損害	ネットワークの停止などにより、事業が中断した場合の**利益喪失**や、事業中断時における人件費などの固定費支出による損害
4．金銭損害	ランサムウェア、ビジネスメール詐欺等による**直接的な金銭（自組織の資金）の支払い**による損害
5．行政損害	個人情報保護法における**罰金**、GDPRにおいて課される**課徴金**などの損害
6．無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、**金銭の換算が困難な**損害

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

損害の例①　費用損害（事故対応損害）

被害発生から収束に向けた各種事故対応に関して、
アウトソーシング先への支払も含め、
自組織で直接、費用を負担することにより被る損害

Copyright　2025　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

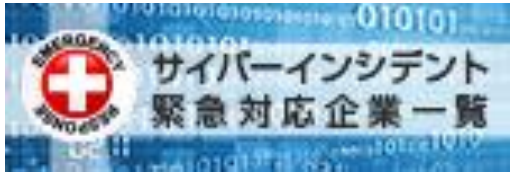
事故原因・被害範囲調査費用

◆対応
・その後の対応を進めるためにも原因や被害範囲等各種調査が必要
・サイバー攻撃等の場合、**フォレンジック調査**（注）が必要

（注）PC、サーバーにあるアクセスログ等を解析し、事故原因や影響・被害範囲の特定などを行う調査

◆アウトソーシング先
インシデントレスポンス事業者

◆コスト
300~400万円



※JNSAのHPに、インシデントレスポンスを行う会員企業の一覧あり

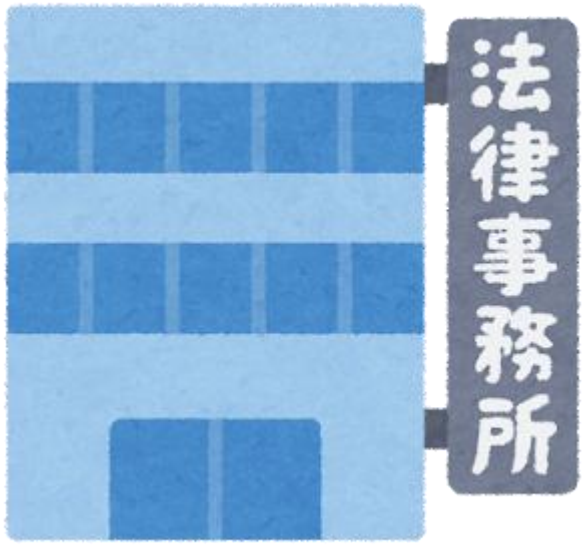
Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

法律相談費用

◆対応
・リーガル面（個人情報保護法等）を踏まえた対応が必要
・法律事務所へ依頼するのが通例

◆アウトソーシング先
法律事務所

◆コスト
数十万円～



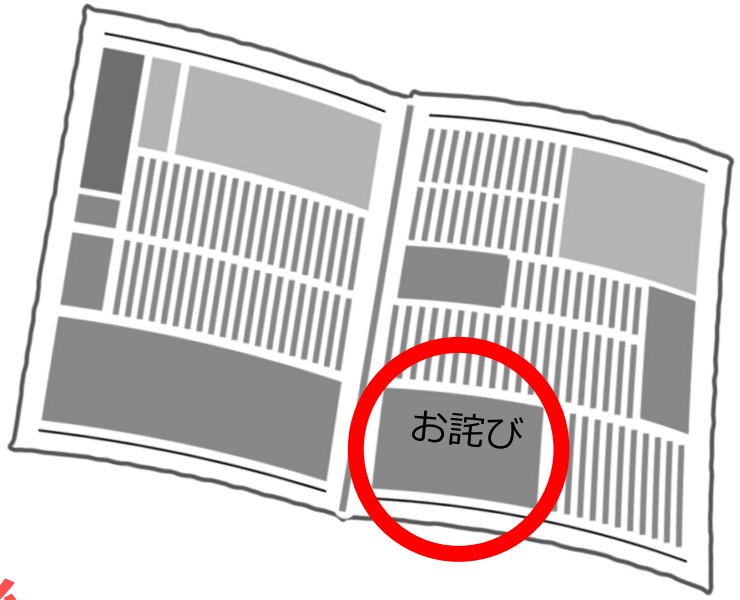
Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

広告・宣伝活動費用

◆対応
・お詫び文を作成し、ホームページへの掲載、DM送付等が必要
・新聞出稿の検討も必要

◆アウトソーシング先
DM印刷・発送業者、新聞社

◆コスト
・DM印刷・発送　1通あたり**封書130円～**
・新聞（10cm2段）
全国紙240万円前後、地方紙50万円前後



Copyright　2025　JNSA（日本ネットワークセキュリティ協会 ）

コールセンター費用

◆対応
・問い合わせ対応のため、電話受付体制の整備が必要
・コールセンター事業者への委託が一般的

◆アウトソーシング先
コールセンター事業者

◆コスト
１オペレーター換算で１か月**140万円～**
⇒３か月対応、初月はオペレーター３席、
２か月目以降は１席とすると700～1,000万円

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

システム復旧費用

◆対応
・システムの消失、改ざん等があった場合、データ復旧等が必要
・データ復旧は主としてバックアップされたデータの復旧

◆アウトソーシング先
システムを構築したITベンダー等

◆コスト
対応規模によって大きく異なることから、
ケースバイケース

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

再発防止費用

◆対応
今後の再発を防ぐため、その防止策の策定・実施が必要

◆アウトソーシング先
セキュリティベンダー等

◆コスト
対応規模によって大きく異なることから、
ケースバイケース

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

損害の例②　利益損害

事業が中断した場合の利益喪失や、
事業中断時における人件費などの固定費支出による損害

Copyright 2025　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

利益損害

多くのシステムが生産・営業活動に直結している現状において、
システムの停止は事業中断につながり、売上高の減少をもたらす
当然、損失は売上規模、ITへの依存度等により**ケースバイケース**

利益損害のイメージ

項目	平時	事業中断時	差額
売上高	10億円	6億円	▲4億円
固定費 人件費、賃料等	2億円	2億円	—
変動費 材料費、電気代等	7億円	4.2億円	2.8億円
営業利益（損失）	**1億円**	**▲0.2億円**	**▲1.2億円**

◇事業中断による売上が4割減

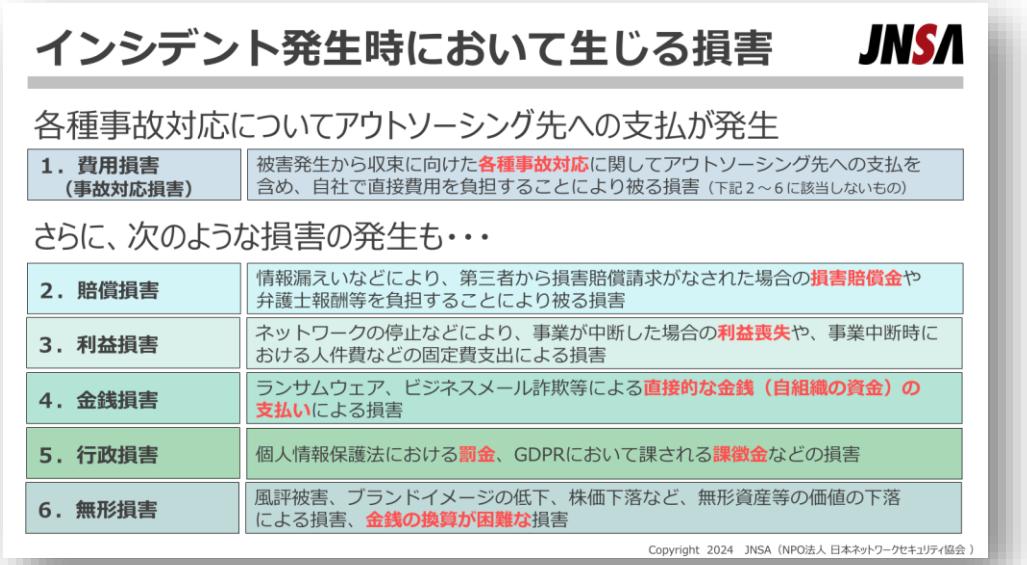
◇事業が中断していても
固定費は定額必要

◇通常1億円稼げるのに、
営業損益▲0.2億円

◇結果として、
▲0.2億円－1億円＝▲1.2億円
の損失が発生

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

前半のまとめ



インシデント発生時において生じる損害 JNSA

各種事故対応についてアウトソーシング先への支払が発生

1．費用損害（事故対応損害）	被害発生から収束に向けた**各種事故対応**に関してアウトソーシング先への支払を含め、自社で直接費用を負担することにより被る損害（下記２～６に該当しないもの）

さらに、次のような損害の発生も・・・

2．賠償損害	情報漏えいなどにより、第三者から損害賠償請求がなされた場合の**損害賠償金**や弁護士報酬等を負担することにより被る損害
3．利益損害	ネットワークの停止などにより、事業が中断した場合の**利益喪失**や、事業中断時における人件費などの固定費支出による損害
4．金銭損害	ランサムウェア、ビジネスメール詐欺等による**直接的な金銭（自組織の資金）の支払い**による損害
5．行政損害	個人情報保護法における**罰金**、GDPRにおいて課される**課徴金**などの損害
6．無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、**金銭の換算が困難な**損害

Copyright 2024 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

各種損害をアウトソーシング先のコスト等を踏まえてみると、
中小企業においても
数千万単位、場合によっては億単位の損害が発生する

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

実際の被害

～被害組織に対するアンケート等からみえてくるもの～

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

調査内容

2025年7月公表の調査内容

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

調査内容

①被害組織調査

2017年1月～2024年6月までの7年半に渡り、
サイバー攻撃による**国内**の被害組織を**約1,800**をピックアップ。
さらに、これらの組織の所在地、資本金、従業員数等の
各種情報を力業で調査

②アンケート調査

上記①の約1,800組織に対してアンケートを実施
回答を得られた組織について**被害額等を集計**

③被害組織インタビュー

上記②の回答を得られた組織のうち、同意を得られた
組織にインタビューを実施。**生の声を確認**

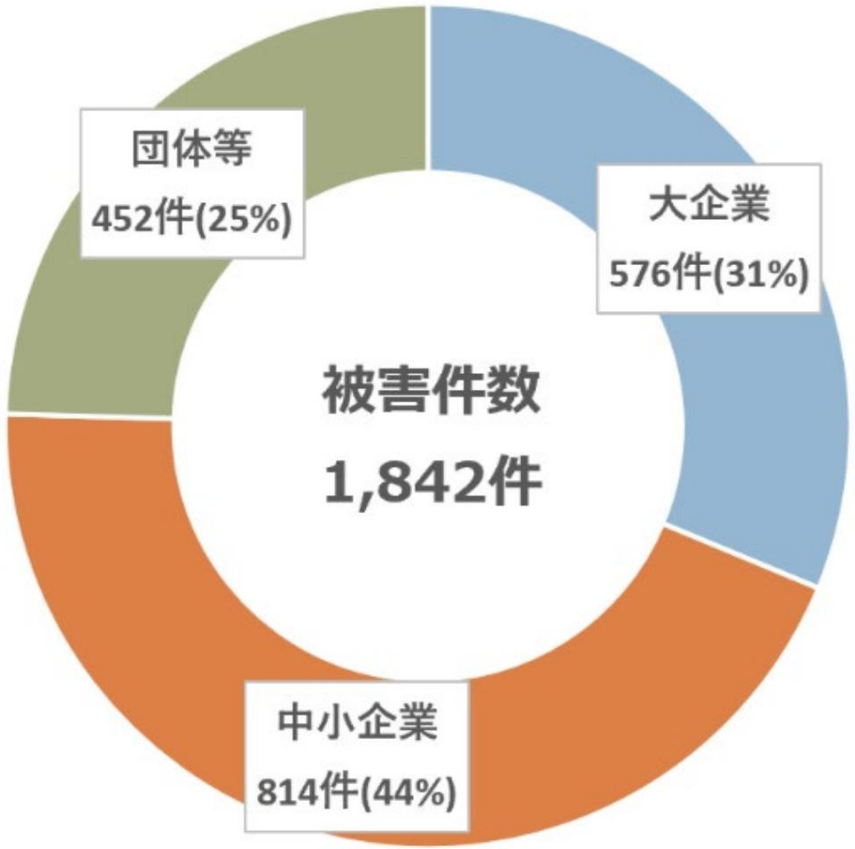
Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

「被害組織調査」

被害組織調査からみえてくるもの

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

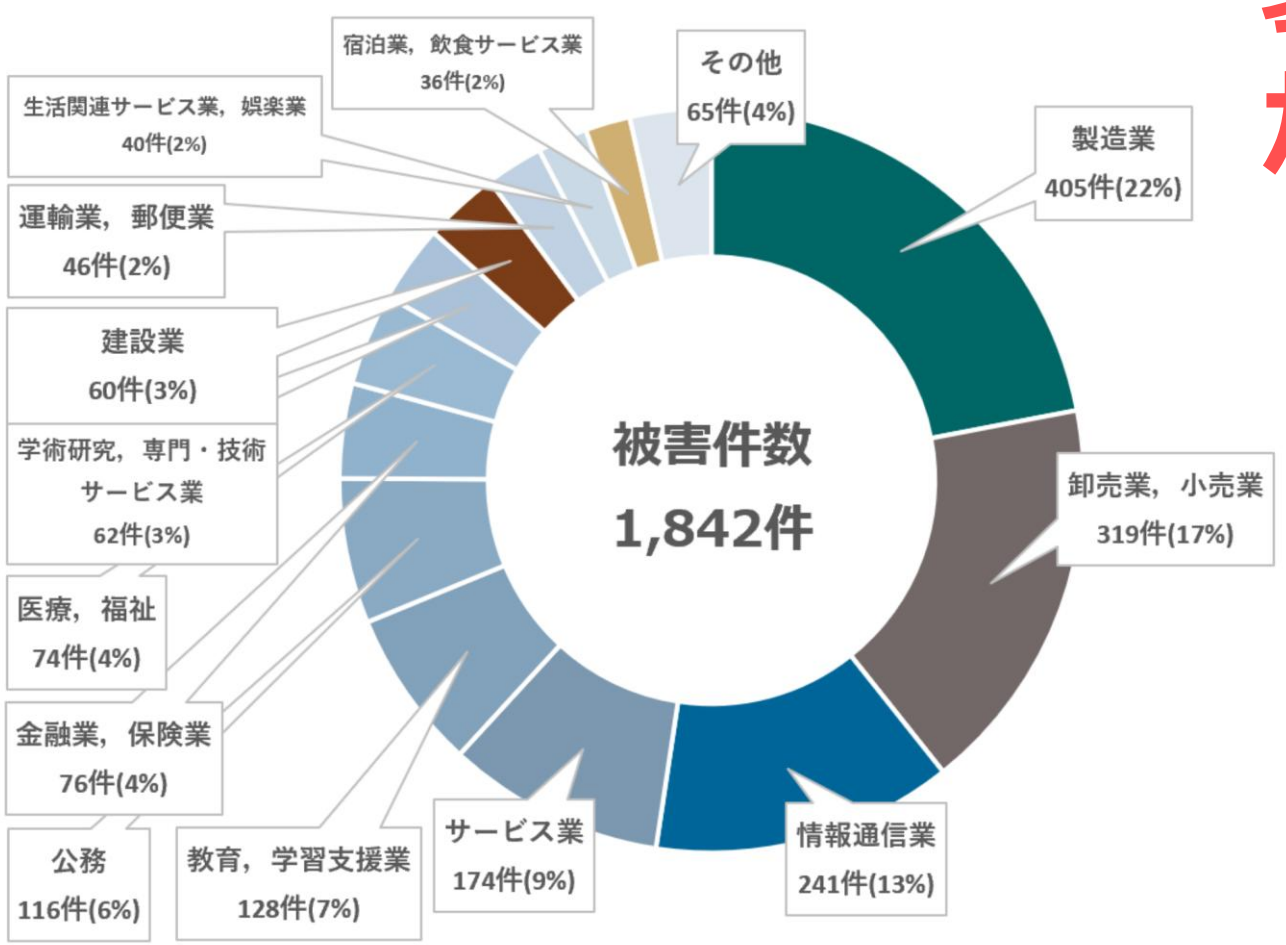
規模



大企業だけではない

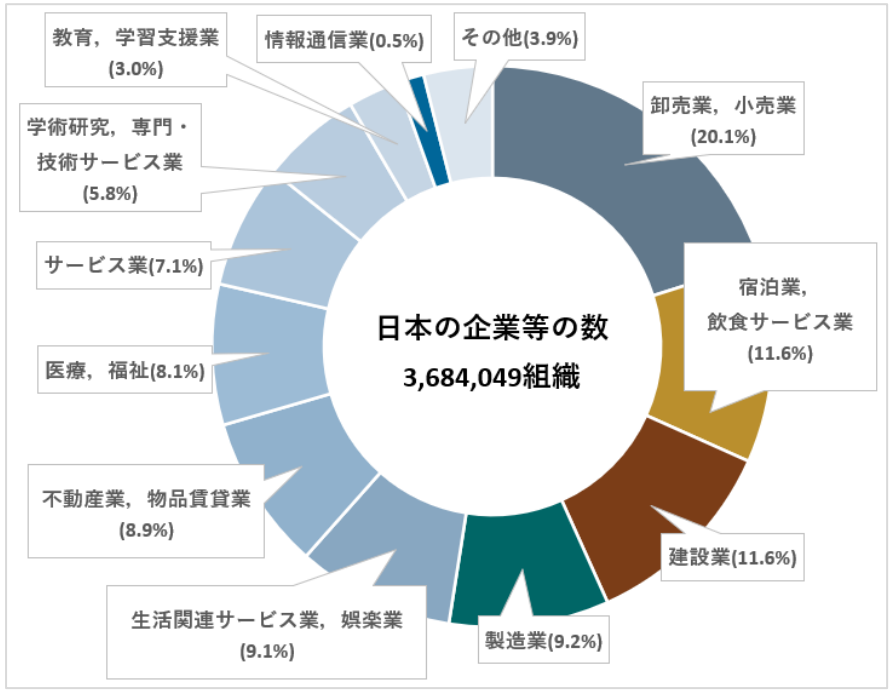
Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

業種



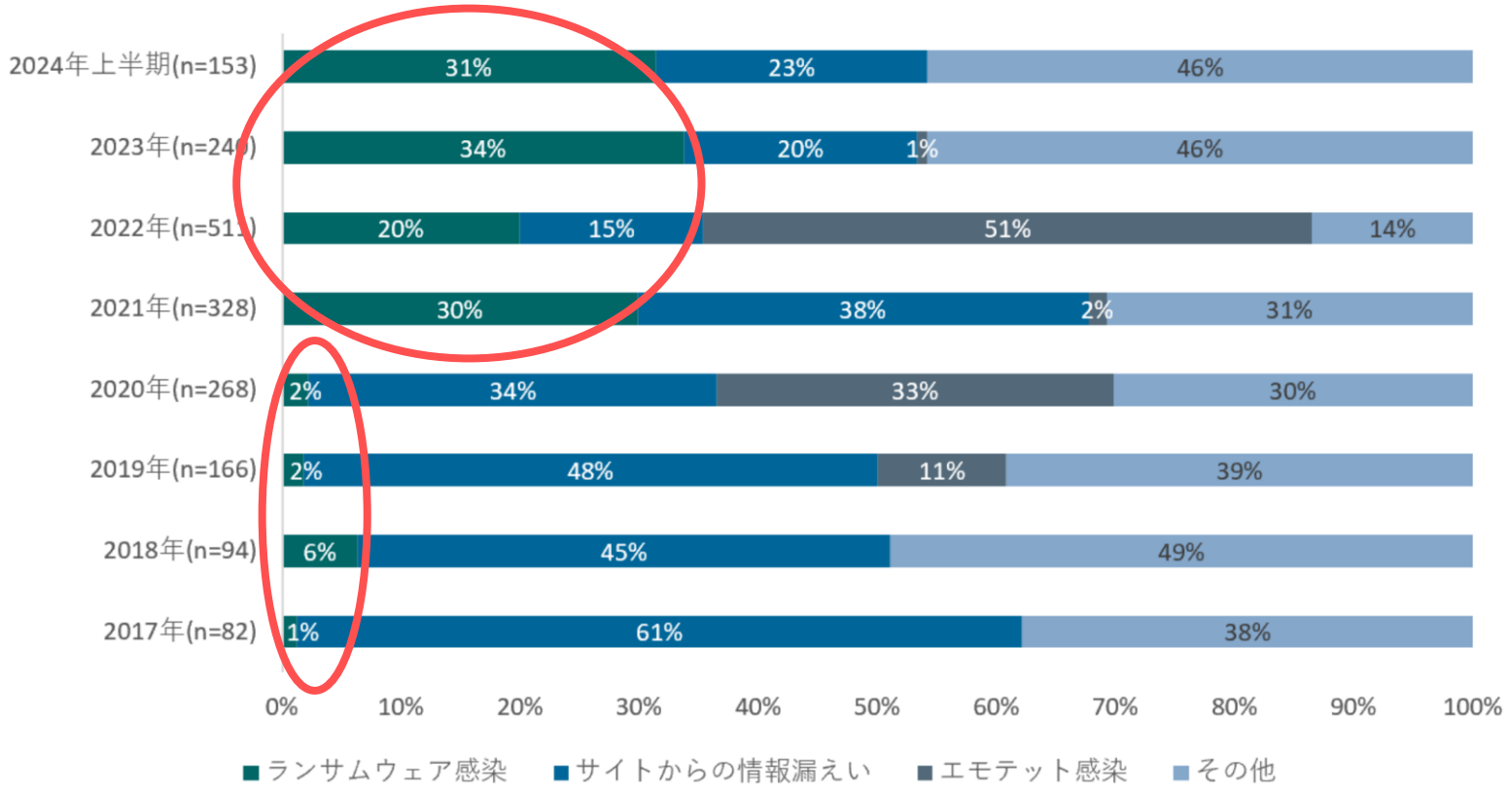
製造業、情報通信業が多い

参考（令和3年経済センサス）



Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

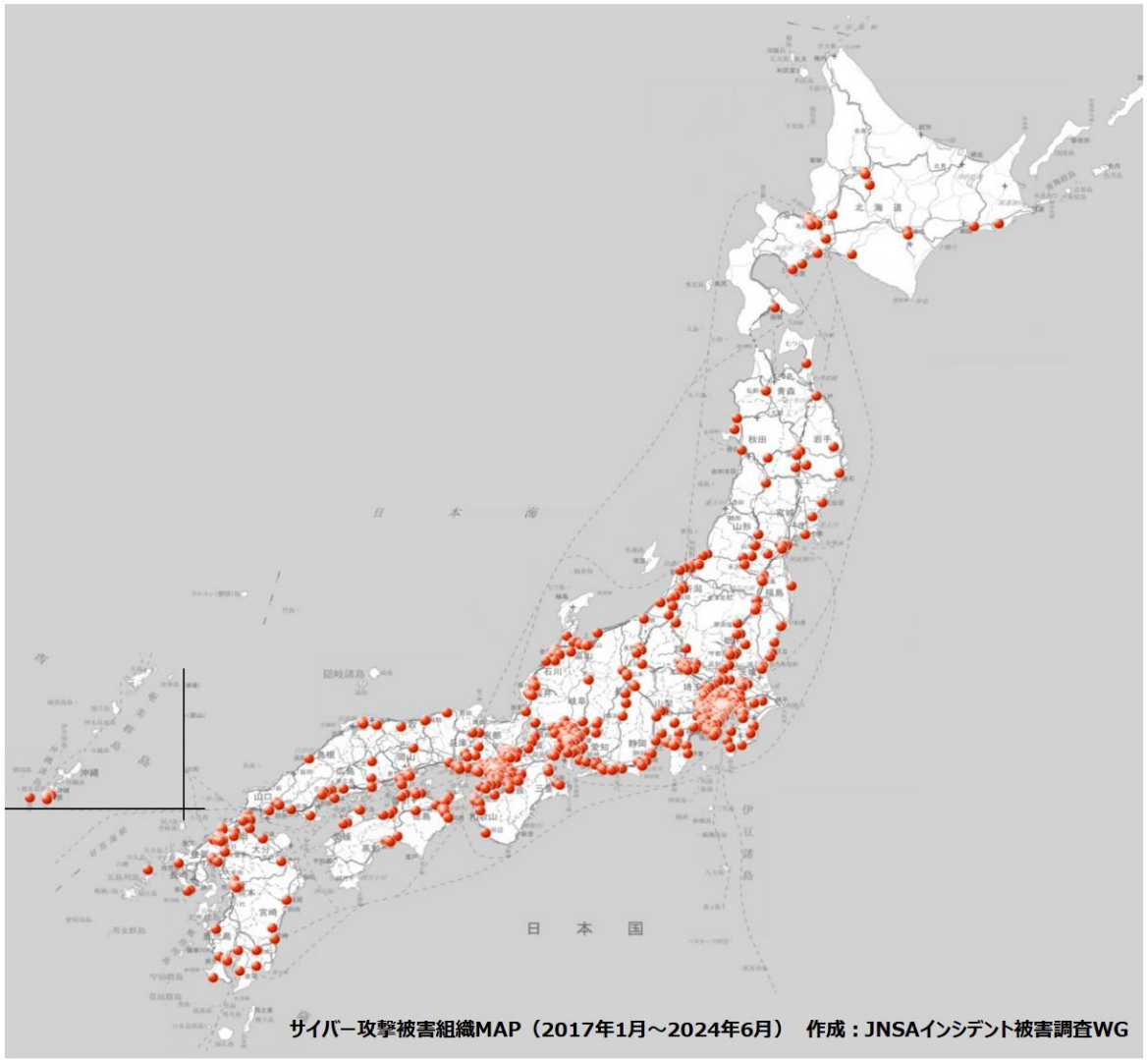
インシデント種別の年度別推移



2021年以降ランサムウェア被害が増加

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

所在地分布



北海道から沖縄まで
被害組織が存在

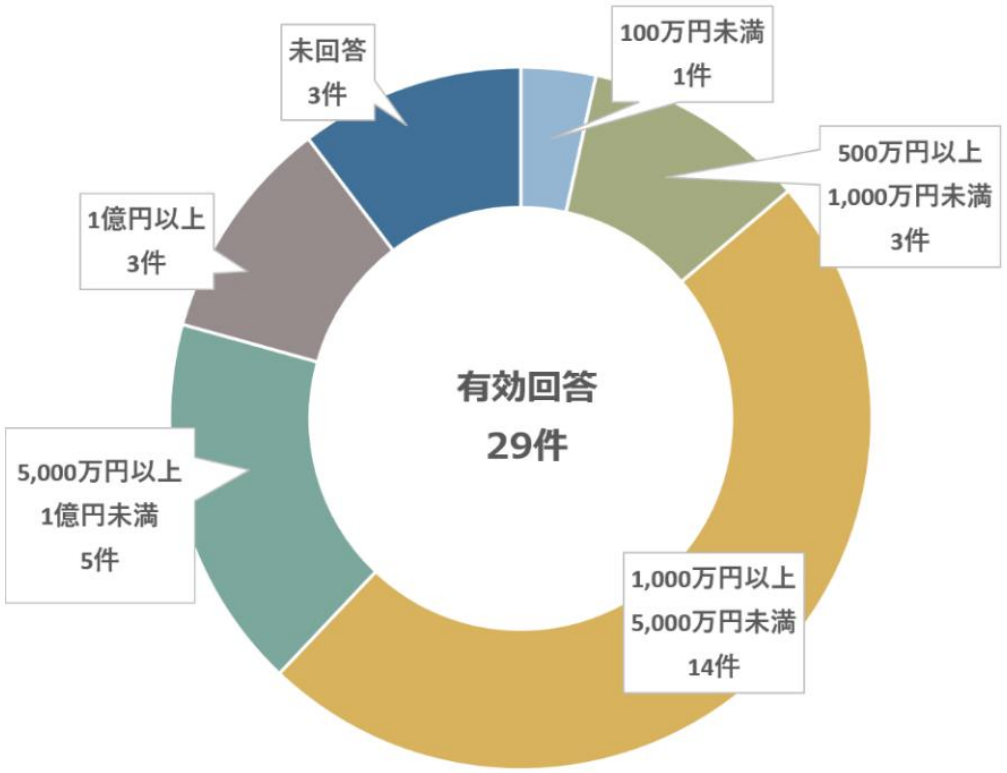
Copyright　2025　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

「アンケート調査」

アンケート調査からみえてくるもの

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

被害金額　～ランサムウェア～



平均値 4,959万円
中央値 3,260万円

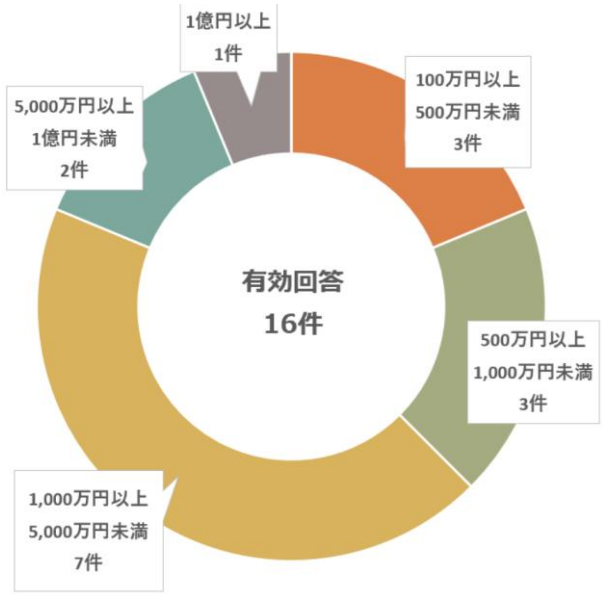
直近2年（2022年7月～2024年6月）は
平均値 6,019万円
中央値 3,800万円

多くの組織が、喪失利益や超過人件費等については未把握
実際の損害額は億単位となっている可能性も

Copyright　2025　JNSA（日本ネットワークセキュリティ協会 ）

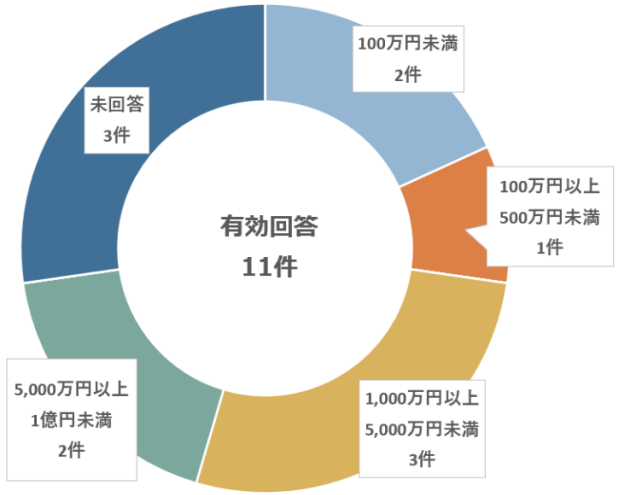
被害金額　～ウェブサイトからの情報漏えい～

①クレカ情報含む



平均値 3,608万円
中央値 1,690万円

②クレカ情報なし



平均値 2,407万円
中央値 1,165万円

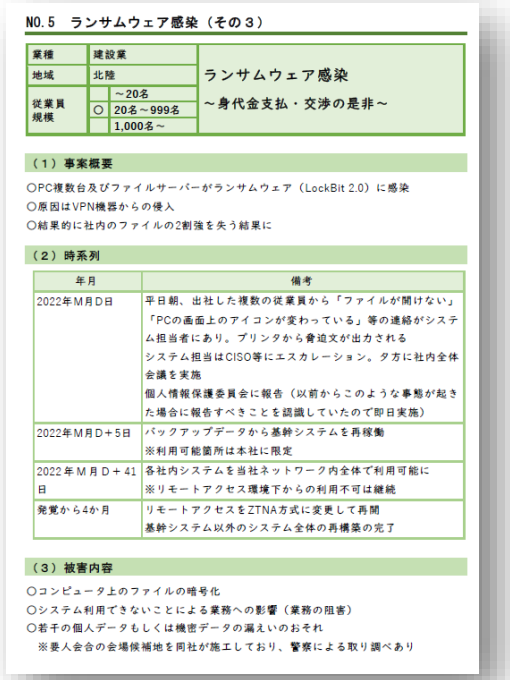
Copyright　2025　JNSA（日本ネットワークセキュリティ協会 ）

「被害企業インタビュー」

リアルな数字…をお伝えします

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー①建設業（北陸） 事案概要



NO.5　ランサムウェア感染（その３）

業種	建設業	ランサムウェア感染 ～身代金支払・交渉の是非～
地域	北陸	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○PC複数台及びファイルサーバーがランサムウェア（LockBit 2.0）に感染
○原因はVPN機器からの侵入
○結果的に社内のファイルの2割強を失う結果に

（２）時系列

年月	備考
2022年M月D日	平日朝、出社した複数の従業員から「ファイルが開けない」「PCの画面上のアイコンが変わっている」等の連絡がシステム担当者にあり。プリンタから脅迫文が出力されるシステム担当はCISO等にエスカレーション。夕方に社内全体会議を実施 個人情報保護委員会に報告（以前からこのような事態が起きた場合に報告すべきことを認識していたので即日実施）
2022年M月D＋5日	バックアップデータから基幹システムを再稼働 ※利用可能箇所は本社に限定
2022年M月D＋41日	各社内システムを当社ネットワーク内全体で利用可能に ※リモートアクセス環境下からの利用不可は継続
発覚から4か月	リモートアクセスをZTNA方式に変更して再開 基幹システム以外のシステム全体の再構築の完了

（３）被害内容

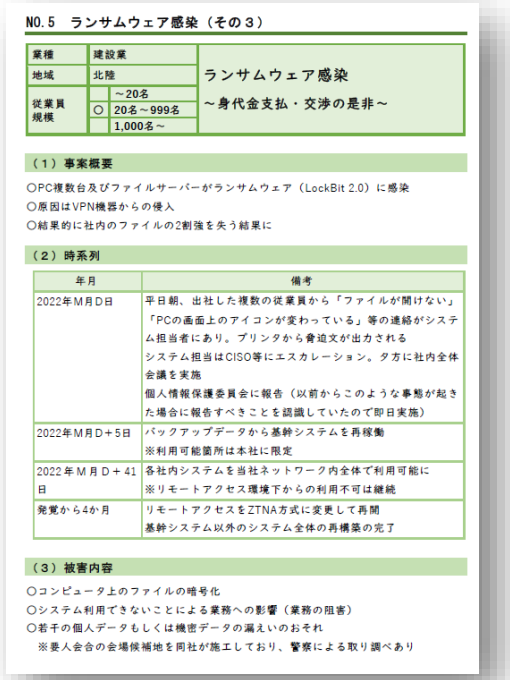
○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○若干の個人データもしくは機密データの漏えいのおそれ
※要人会合の会場候補地を同社が施工しており、警察による取り調べあり

VPN機器からの侵入によりランサムウェアに感染

年月	備考
2022年M月D日	平日朝、出社した複数の従業員から「ファイルが開けない」「PCの画面上のアイコンが変わっている」等の連絡がシステム担当者にあり。プリンタから脅迫文が出力されるシステム担当はCISO等にエスカレーション。夕方に社内全体会議を実施 個人情報保護委員会に報告（以前からこのような事態が起きた場合に報告すべきことを認識していたので即日実施）
2022年M月D＋5日	バックアップデータから基幹システムを再稼働 ※利用可能箇所は本社に限定
2022年M月D＋41日	各社内システムを当社ネットワーク内全体で利用可能に ※リモートアクセス環境下からの利用不可は継続
発覚から4か月	リモートアクセスをZTNA方式に変更して再開 基幹システム以外のシステム全体の再構築の完了

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー①建設業（北陸）被害額



NO.5　ランサムウェア感染（その３）

業種	建設業	ランサムウェア感染 ～身代金支払・交渉の是非～
地域	北陸	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○PC複数台及びファイルサーバーがランサムウェア（LockBit 2.0）に感染
○原因はVPN機器からの侵入
○結果的に社内のファイルの2割強を失う結果に

（２）時系列

年月	備考
2022年M月D日	平日朝、出社した複数の従業員から「ファイルが開けない」「PCの画面上のアイコンが変わっている」等の連絡がシステム担当者にあり。プリンタから脅迫文が出力される システム担当はCISO等にエスカレーション。夕方に社内全体会議を実施 個人情報保護委員会に報告（以前からこのような事態が起きた場合に報告すべきことを認識していたので即日実施）
2022年M月D＋5日	バックアップデータから基幹システムを再稼働 ※利用可能箇所は本社に限定
2022年M月D＋41日	各社内システムを当社ネットワーク内全体で利用可能に ※リモートアクセス環境下からの利用不可は継続
発覚から4か月	リモートアクセスをZTNA方式に変更して再開 基幹システム以外のシステム全体の再構築の完了

（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○若干の個人データもしくは機密データの漏えいのおそれ
※要人会合の会場候補地を同社が施工しており、警察による取り調べあり

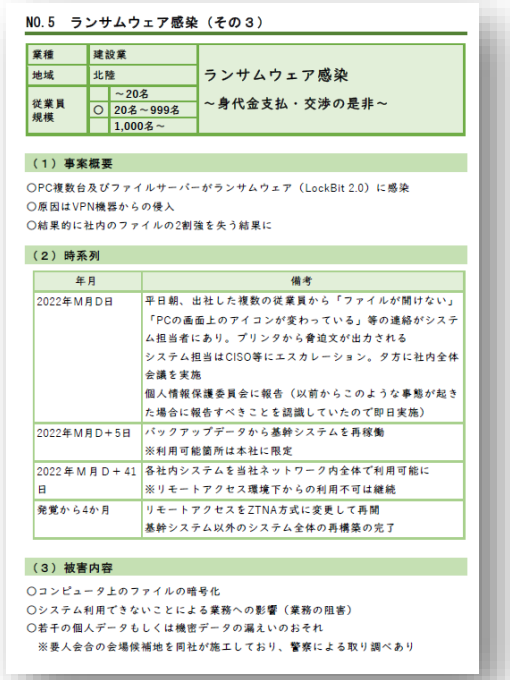
約2億5000万円

＋　対応に要した内部工数：45人月（システム対応について他部門にも応援要請）
＋　利益喪失：不明

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	1,000万円	サーバー4台、PC4、5台の調査
	システム復旧費用	400万円	ファイルサーバー等の更新費用およびネットワークベンダーの支援業務費用 基本的にはバックアップデータからの復旧は自社にて実施（アウトソーシングコストなし）
	再発防止費用	8,300万円	EDRおよびMDRで900万円、バックアップ製品で4,300万円、ZTNA（注）で3,000万円、その他としてドメインコントローラの監視サービス等。ZTNAおよび監視サービス以外は従前より導入予定であったもの
利益	固定費	1.5億	約1か月間、社員のパフォーマンスが50%程度に落ち込んだものとして試算

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー①建設業（北陸）被害者コメント



NO.5　ランサムウェア感染（その３）

業種	建設業	ランサムウェア感染 ～身代金支払・交渉の是非～
地域	北陸	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○PC複数台及びファイルサーバーがランサムウェア（LockBit 2.0）に感染
○原因はVPN機器からの侵入
○結果的に社内のファイルの2割強を失う結果に

（２）時系列

年月	備考
2022年M月D日	平日朝、出社した複数の従業員から「ファイルが開けない」「PCの画面上のアイコンが変わっている」等の連絡がシステム担当者にあり。プリンタから脅迫文が出力される システム担当はCISO等にエスカレーション。夕方に社内全体会議を実施 個人情報保護委員会に報告（以前からこのような事態が起きた場合に報告すべきことを認識していたので即日実施）
2022年M月D＋5日	バックアップデータから基幹システムを再稼働 ※利用可能箇所は本社に限定
2022年M月D＋41日	各社内システムを当社ネットワーク内全体で利用可能に ※リモートアクセス環境下からの利用不可は継続
発覚から4か月	リモートアクセスをZTNA方式に変更して再開 基幹システム以外のシステム全体の再構築の完了

（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○若干の個人データもしくは機密データの漏えいのおそれ
※要人会合の会場候補地を同社が施工しており、警察による取り調べあり

○感染1か月前にSSL-VPN機器の入替を予定。後継機種を約半年待つか（納期の関係）、別メーカーの機器をすぐに導入するかを議論したが、結論が前者となり結果的には反省点

○年2回という頻度でリストア訓練を実施していたため、基幹システムを比較的早期に復旧できた。システム担当としてリストア訓練の重要性を認識していたことが活きた。リストア訓練は100%動くところまでを目指すのではではなく、一定できる範囲での訓練を実施すべきと思う。（OSが起動するところまで確認できれば、その後はソフトウェアベンダーの保守で対応できる可能性が高い）

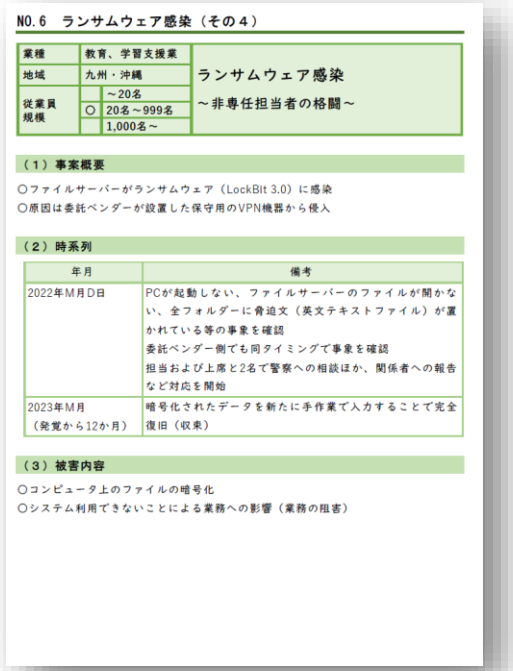
○バックアップ製品導入の必要性についても、今回の被害発生前に社内的に稟議を起案していた。経営層に被害発生による損失の大きさを示していた。

○総務部長が警察から「身代金を支払うべきではない」と聞いていたこと等の背景からのコンセンサスもあり、特段論議もなく身代金の交渉、支払はしないことを決定。

○個人的に身代金は支払うべきではないと思っている。最近「払うのはアリ」「交渉はアリ」という発信が気になる。払わずに涙を飲んだ会社が多くいるから諸外国と比べて日本は狙われていないといった話があると思う。払うことを是とするような発信をすることによってかえって狙われてしまうのでは。

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー②教育･学習支援業（九州沖縄）事案概要



NO.6　ランサムウェア感染（その４）

業種	教育、学習支援業	ランサムウェア感染 ～非専任担当者の格闘～
地域	九州・沖縄	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○ファイルサーバーがランサムウェア（LockBit 3.0）に感染
○原因は委託ベンダーが設置した保守用のVPN機器から侵入

（２）時系列

年月	備考
2022年M月D日	PCが起動しない、ファイルサーバーのファイルが開かない、全フォルダーに脅迫文（英文テキストファイル）が置かれている等の事象を確認 委託ベンダー側でも同タイミングで事象を確認 担当および上席と2名で警察への相談ほか、関係者への報告など対応を開始
2023年M月 （発覚から12か月）	暗号化されたデータを新たに手作業で入力することで完全復旧（収束）

（３）被害内容

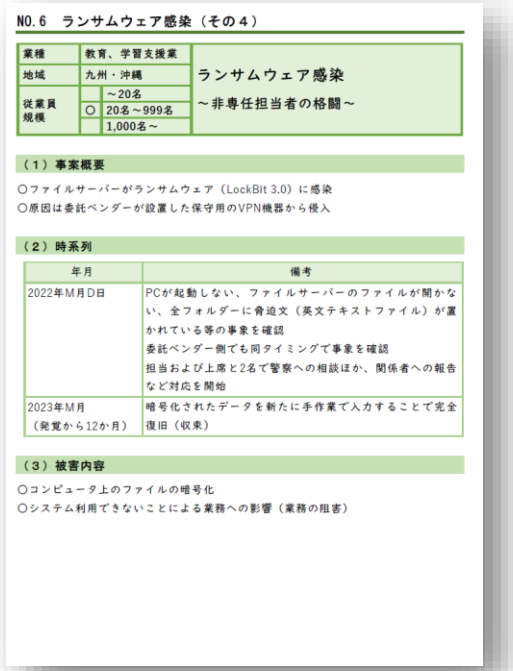
○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）

VPN機器からの侵入によりランサムウェアに感染

年月	備考
2022年M月D日	PCが起動しない、ファイルサーバーのファイルが開かない、全フォルダーに脅迫文（英文テキストファイル）が置かれている等の事象を確認 委託ベンダー側でも同タイミングで事象を確認 担当および上席と2名で警察への相談ほか、関係者への報告など対応を開始
2023年M月 （発覚から12か月）	暗号化されたデータを新たに手作業で入力することで完全復旧（収束）

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー②教育･学習支援業（九州沖縄）被害額



NO.6　ランサムウェア感染（その４）

業種	教育、学習支援業	ランサムウェア感染 ～非専任担当者の格闘～
地域	九州・沖縄	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○ファイルサーバーがランサムウェア（LockBit 3.0）に感染
○原因は委託ベンダーが設置した保守用のVPN機器から侵入

（２）時系列

年月	備考
2022年M月D日	PCが起動しない、ファイルサーバーのファイルが開かない、全フォルダーに脅迫文（英文テキストファイル）が置かれている等の事象を確認 委託ベンダー側でも同タイミングで事象を確認 担当および上席と2名で警察への相談ほか、関係者への報告など対応を開始
2023年M月（発覚から12か月）	暗号化されたデータを新たに手作業で入力することで完全復旧（収束）

（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）

500万円以上（多くの費用は委託ベンダーにて負担）

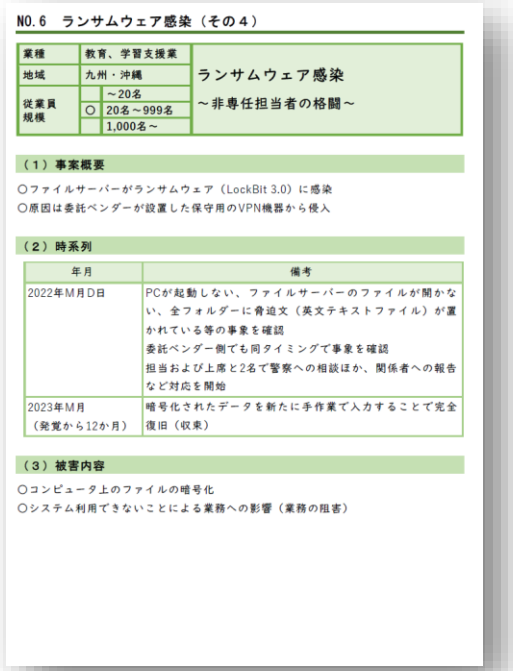
＋　対応に要した内部工数：42人月

＋　利益喪失：不明

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	不明	委託ベンダーとの責任分界点について弁護士を交えて交渉し委託ベンダーがコスト負担
	システム復旧費用 再発防止費用	500万円	バックアップも暗号化されたため、システムを再構築 復旧の中で再発防止を実施

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー②教育･学習支援業（九州沖縄）被害者コメント



NO.6　ランサムウェア感染（その４）

業種	教育、学習支援業		ランサムウェア感染 ～非専任担当者の格闘～
地域	九州・沖縄		
従業員規模		～20名	
	○	20名～999名	
		1,000名～	

（１）事案概要

○ファイルサーバーがランサムウェア（LockBit 3.0）に感染
○原因は委託ベンダーが設置した保守用のVPN機器から侵入

（２）時系列

年月	備考
2022年M月D日	PCが起動しない、ファイルサーバーのファイルが開かない、全フォルダーに脅迫文（英文テキストファイル）が置かれている等の事象を確認 委託ベンダー側でも同タイミングで事象を確認 担当および上席と2名で警察への相談ほか、関係者への報告など対応を開始
2023年M月 （発覚から12か月）	暗号化されたデータを新たに手作業で入力することで完全復旧（収束）

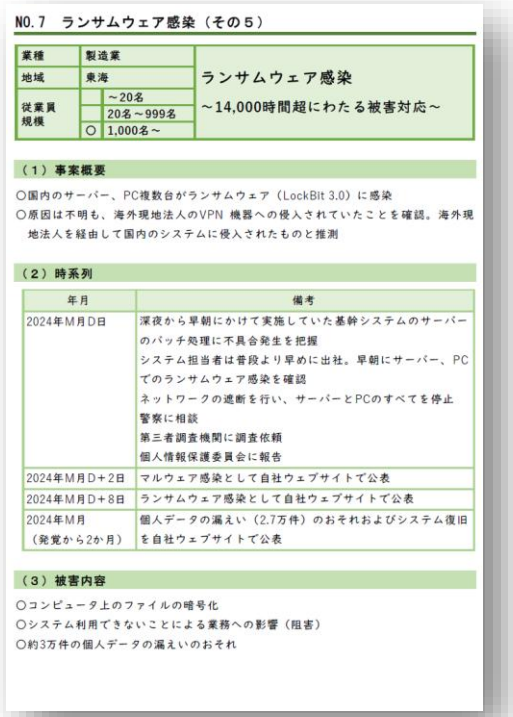
（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）

○復旧することを最優先に、少ない人員（上席とあわせて2人）でできる限りの対応をした。例えば、事業が一部停止したことによる問合せ・苦情は多々あったが、コールセンターへの委託等はせずに2人で対応した。事前に体制の整備、訓練等を実施していれば違ったかもしれないが、外部に応援を求める余裕・発想がなかった。
○事業規模が小さく、窃取された可能性のある情報は有益なものは少ないため、なぜ狙われたのかわからない。練習台にされたのかもしれない。
○身代金の支払いは、業種的な観点からも念頭になかった。
○委託ベンダーが設置した保守用のVPNのID/PasswordがSNSの公式アカウントに投稿された。また、攻撃者と思われる人物からメールで連絡もあった。脆弱性対応していたとしても、侵入された可能性は高いと認識。
○委託ベンダー側の問題（脆弱性対応の不備）はあったかと思うが、原因追及調査や復旧スケジュール等は上層部を交えながら情報共有を図り、スピーディーに対応してもらえた。
○データ復旧は人海戦術で対応した。完全復旧まで1年かかった。
○問題発生後、各部門からさまざまな意見が出て取り纏めに苦労した。インシデント対応は各部門が連携した取り組み、ワンチームでの取り組みが必要。

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー③製造業（東海）事案概要



NO.7　ランサムウェア感染（その５）

業種	製造業	ランサムウェア感染 ～14,000時間超にわたる被害対応～
地域	東海	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○国内のサーバー、PC複数台がランサムウェア（LockBit 3.0）に感染
○原因は不明も、海外現地法人のVPN 機器への侵入されていたことを確認。海外現地法人を経由して国内のシステムに侵入されたものと推測

（２）時系列

年月	備考
2024年M月D日	深夜から早朝にかけて実施していた基幹システムのサーバーのバッチ処理に不具合発生を把握 システム担当者は普段より早めに出社。早朝にサーバー、PCでのランサムウェア感染を確認 ネットワークの遮断を行い、サーバーとPCのすべてを停止 警察に相談 第三者調査機関に調査依頼 個人情報保護委員会に報告
2024年M月D+2日	マルウェア感染として自社ウェブサイトで公表
2024年M月D+8日	ランサムウェア感染として自社ウェブサイトで公表
2024年M月（発覚から2か月）	個人データの漏えい（2.7万件）のおそれおよびシステム復旧を自社ウェブサイトで公表

（３）被害内容

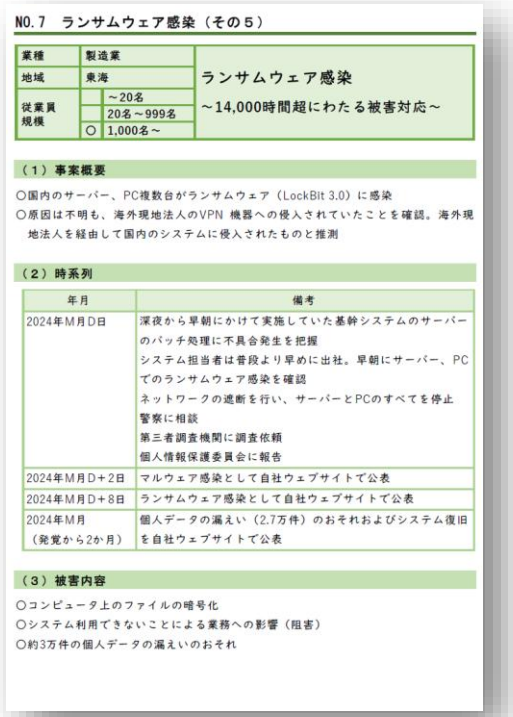
○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（阻害）
○約3万件の個人データの漏えいのおそれ

海外現地法人のVPN機器からの侵入により国内本社がランサムウェアに感染

年月	備考
2024年M月D日	深夜から早朝にかけて実施していた基幹システムのサーバーのバッチ処理に不具合発生を把握 システム担当者は普段より早めに出社。早朝にサーバー、PCでのランサムウェア感染を確認 ネットワークの遮断を行い、サーバーとPCのすべてを停止 警察に相談 第三者調査機関に調査依頼 個人情報保護委員会に報告
2024年M月D＋2日	マルウェア感染として自社ウェブサイトで公表
2024年M月D＋8日	ランサムウェア感染として自社ウェブサイトで公表
2024年M月（発覚から2か月）	個人データの漏えい（2.7万件）のおそれおよびシステム復旧を自社ウェブサイトで公表

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー③製造業（東海） 被害額



NO.7　ランサムウェア感染（その５）

業種	製造業	ランサムウェア感染 ～14,000時間超にわたる被害対応～
地域	東海	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○国内のサーバー、PC複数台がランサムウェア（LockBit 3.0）に感染
○原因は不明も、海外現地法人のVPN 機器への侵入されていたことを確認。海外現地法人を経由して国内のシステムに侵入されたものと推測

（２）時系列

年月	備考
2024年M月D日	深夜から早朝にかけて実施していた基幹システムのサーバーのバッチ処理に不具合発生を把握 システム担当者は普段より早めに出社。早朝にサーバー、PCでのランサムウェア感染を確認 ネットワークの遮断を行い、サーバーとPCのすべてを停止 警察に相談 第三者調査機関に調査依頼 個人情報保護委員会に報告
2024年M月D+2日	マルウェア感染として自社ウェブサイトで公表
2024年M月D+8日	ランサムウェア感染として自社ウェブサイトで公表
2024年M月（発覚から2か月）	個人データの漏えい（2.7万件）のおそれおよびシステム復旧を自社ウェブサイトで公表

（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（阻害）
○約3万件の個人データの漏えいのおそれ

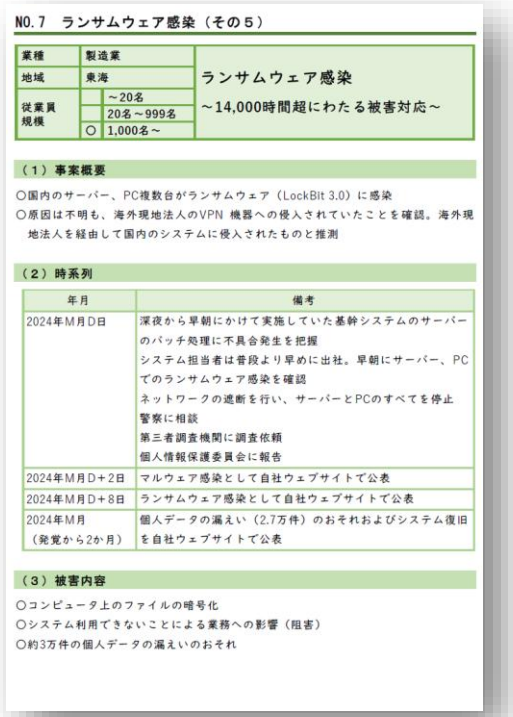
9,740万円

＋　対応に要した内部工数：約95.4人月（IT部門のみ。14,309時間）
＋　利益喪失：不明
※国内の対応費用のみ

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	850万円	調査費用は時間単価での計算によるコスト
	システム復旧費用	1,570万円	バックアップからの復旧。バックアップがなかった機器は再構築（費用としては主に再構築額）
	法律相談費用	120万円	紹介に基づきサイバー事案に長けた弁護士に相談
	広告・宣伝活動費用	400万円	お詫び状の郵送にかかった費用
	再発防止費用	4,200万円	EDRを導入
	超過人件費	1,700万円	システム停止に伴い増加した業務費用。（被害に伴い増加した人件費（残業代および休日出勤手当）1200万円を含む）
賠償	損害賠償金	900万円	通常とは異なるチャネルで商品を流通させたことにより、販売店が負担した追加コストを補填

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー③製造業（東海） 被害者コメント



NO.7　ランサムウェア感染（その５）

業種	製造業	ランサムウェア感染 ～14,000時間超にわたる被害対応～
地域	東海	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○国内のサーバー、PC複数台がランサムウェア（LockBit 3.0）に感染
○原因は不明も、海外現地法人のVPN 機器への侵入されていたことを確認。海外現地法人を経由して国内のシステムに侵入されたものと推測

（２）時系列

年月	備考
2024年M月D日	深夜から早朝にかけて実施していた基幹システムのサーバーのバッチ処理に不具合発生を把握 システム担当者は普段より早めに出社。早朝にサーバー、PCでのランサムウェア感染を確認 ネットワークの遮断を行い、サーバーとPCのすべてを停止 警察に相談 第三者調査機関に調査依頼 個人情報保護委員会に報告
2024年M月D+2日	マルウェア感染として自社ウェブサイトで公表
2024年M月D+8日	ランサムウェア感染として自社ウェブサイトで公表
2024年M月 （発覚から2か月）	個人データの漏えい（2.7万件）のおそれおよびシステム復旧を自社ウェブサイトで公表

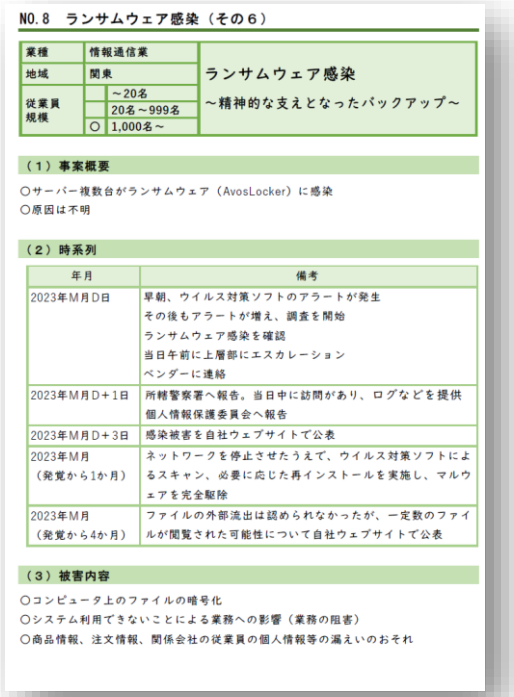
（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（阻害）
○約3万件の個人データの漏えいのおそれ

○海外現地法人のVPN装置からの侵入と推定されるが、現地法人が初動対応で機器のアップデートなどの作業を行ってしまったため、証跡が残っておらず、侵入経路に関する詳細な調査ができなかった。
○監査法人から再発可能性がないことの強い確認もあって、再発防止策としてEDRを導入した。その当時はランサムウェア事案の再発防止策としてEDRの導入が必須ともいえる状況だった。
○脅迫文で指示された連絡先にはアクセスしていない。身代金を支払うという選択肢はその当時の世間の雰囲気としてもなかったように思う。社内的な議論もなかった。
○被害当時、サイバー保険には未加入。加入していた場合、どの程度の金額が補償されたのかを確認するため、サイバー保険で補償される項目を中心として、対応に要した工数や人件費（残業代）などを算出した。現在はサイバー保険に加入。
○自分の身に降りかかるとは思っていなかった。狙って価値のある企業を狙うものでないことを認識。「流れ弾」に当たるようなもの。誰でも被害にあうおそれがある。

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー④情報通信業（関東）事案概要



NO.8　ランサムウェア感染（その６）

業種	情報通信業	ランサムウェア感染 ～精神的な支えとなったバックアップ～
地域	関東	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○サーバー複数台がランサムウェア（AvosLocker）に感染
○原因は不明

（２）時系列

年月	備考
2023年M月D日	早朝、ウイルス対策ソフトのアラートが発生 その後もアラートが増え、調査を開始 ランサムウェア感染を確認 当日午前に上層部にエスカレーション ベンダーに連絡
2023年M月D＋1日	所轄警察署へ報告。当日中に訪問があり、ログなどを提供 個人情報保護委員会へ報告
2023年M月D＋3日	感染被害を自社ウェブサイトで公表
2023年M月 （発覚から1か月）	ネットワークを停止させたうえで、ウイルス対策ソフトによるスキャン、必要に応じた再インストールを実施し、マルウェアを完全駆除
2023年M月 （発覚から4か月）	ファイルの外部流出は認められなかったが、一定数のファイルが閲覧された可能性について自社ウェブサイトで公表

（３）被害内容

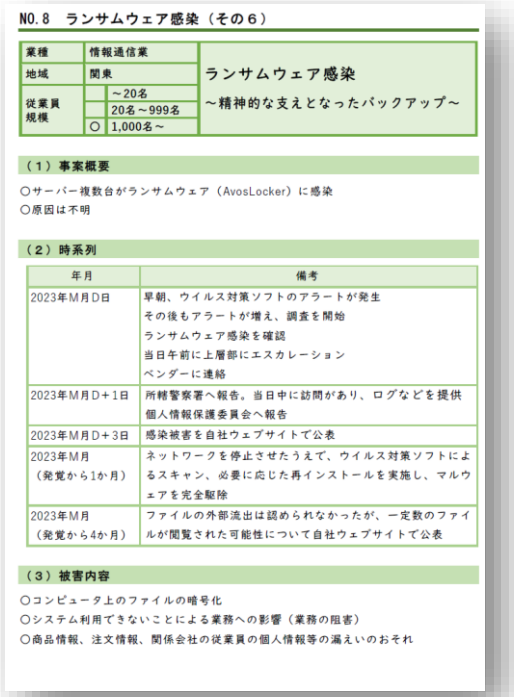
○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○商品情報、注文情報、関係会社の従業員の個人情報等の漏えいのおそれ

ランサムウェアに感染（侵入原因不明）

年月	備考
2023年M月D日	早朝、ウイルス対策ソフトのアラートが発生 その後もアラートが増え、調査を開始 ランサムウェア感染を確認 当日午前に上層部にエスカレーション ベンダーに連絡
2023年M月D＋1日	所轄警察署へ報告。当日中に訪問があり、ログなどを提供 個人情報保護委員会へ報告
2023年M月D＋3日	感染被害を自社ウェブサイトで公表
2023年M月 （発覚から1か月）	ネットワークを停止させたうえで、ウイルス対策ソフトによるスキャン、必要に応じた再インストールを実施し、マルウェアを完全駆除
2023年M月 （発覚から4か月）	ファイルの外部流出は認められなかったが、一定数のファイルが閲覧された可能性について自社ウェブサイトで公表

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー④情報通信業（関東）被害額



NO.8　ランサムウェア感染（その６）

業種	情報通信業	ランサムウェア感染 ～精神的な支えとなったバックアップ～
地域	関東	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○サーバー複数台がランサムウェア（AvosLocker）に感染
○原因は不明

（２）時系列

年月	備考
2023年M月D日	早朝、ウイルス対策ソフトのアラートが発生 その後もアラートが増え、調査を開始 ランサムウェア感染を確認 当日午前に上層部にエスカレーション ベンダーに連絡
2023年M月D＋1日	所轄警察署へ報告。当日中に訪問があり、ログなどを提供 個人情報保護委員会へ報告
2023年M月D＋3日	感染被害を自社ウェブサイトで公表
2023年M月 （発覚から1か月）	ネットワークを停止させたうえで、ウイルス対策ソフトによるスキャン、必要に応じた再インストールを実施し、マルウェアを完全駆除
2023年M月 （発覚から4か月）	ファイルの外部流出は認められなかったが、一定数のファイルが閲覧された可能性について自社ウェブサイトで公表

（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○商品情報、注文情報、関係会社の従業員の個人情報等の漏えいのおそれ

1億6,100万円

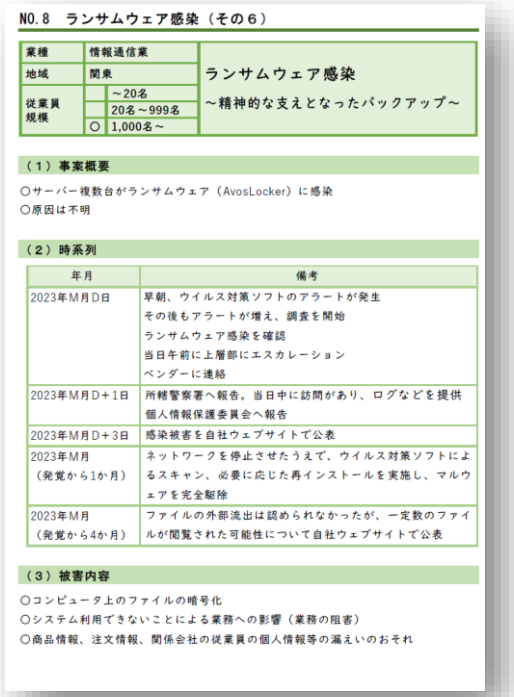
＋　対応に要した内部工数：60人月

＋　利益喪失：不明

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	1,600万円	
	法律相談費用	―	顧問弁護士に相談できたため、個別の費用発生はなし
	システム復旧費用	8,000万円	
	再発防止費用	6,500万円	複数年にわたる計画で実施中。記載の費用はインタビュー実施日時点で要した金額

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー④情報通信業（関東）被害者コメント



NO.8　ランサムウェア感染（その６）

業種	情報通信業	ランサムウェア感染 ～精神的な支えとなったバックアップ～
地域	関東	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○サーバー複数台がランサムウェア（AvosLocker）に感染
○原因は不明

（２）時系列

年月	備考
2023年M月D日	早朝、ウイルス対策ソフトのアラートが発生 その後もアラートが増え、調査を開始 ランサムウェア感染を確認 当日午前に上層部にエスカレーション ベンダーに連絡
2023年M月D＋1日	所轄警察署へ報告。当日中に訪問があり、ログなどを提供 個人情報保護委員会へ報告
2023年M月D＋3日	感染被害を自社ウェブサイトで公表
2023年M月 （発覚から1か月）	ネットワークを停止させたうえで、ウイルス対策ソフトによるスキャン、必要に応じた再インストールを実施し、マルウェアを完全駆除
2023年M月 （発覚から4か月）	ファイルの外部流出は認められなかったが、一定数のファイルが閲覧された可能性について自社ウェブサイトで公表

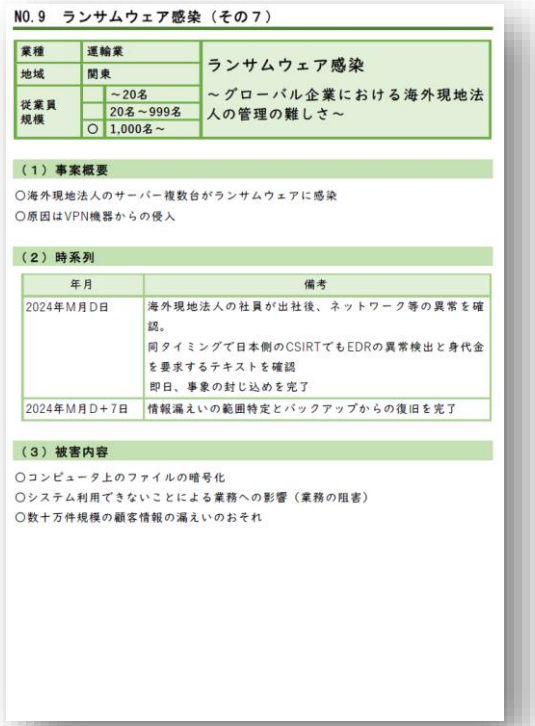
（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○商品情報、注文情報、関係会社の従業員の個人情報等の漏えいのおそれ

○セキュリティベンダーの調査の結果から、リモートデスクトップサービス（AnyDesk）からドメインコントローラに侵入されたことを確認
○データが暗号化されたほか、保存データの一部が攻撃者に参照されたおそれ。ただし、ファイル転送などの痕跡はなく、社外に流出した事実は確認されなかった。
○システムの復旧には約1か月を要した。感染端末・サーバーからランサムウェアを駆除。EDRを導入し、監視を一定期間行ったうえで、復旧完了
○身代金に関しては、早い段階から支払わない方針を上層部で決定
○バックアップから復元できるようにしておくことが重要。バックアップの世代管理、リストア手順のシミュレーションも実施しておく必要がある。
○「バックアップから復元するための数日間、我慢すれば戻ると思えるだけで、現場は頑張ることができる。」
○EDR導入を予定していたが導入前に被害にあってしまった。必要なセキュリティ対策は早めに取り入れておく必要性を感じている。

Copyright　2024　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー⑤運輸業（関東）事案概要



NO.9　ランサムウェア感染（その７）

業種	運輸業	ランサムウェア感染 ～グローバル企業における海外現地法人の管理の難しさ～
地域	関東	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○海外現地法人のサーバー複数台がランサムウェアに感染
○原因はVPN機器からの侵入

（２）時系列

年月	備考
2024年M月D日	海外現地法人の社員が出社後、ネットワーク等の異常を確認。 同タイミングで日本側のCSIRTでもEDRの異常検出と身代金を要求するテキストを確認 即日、事象の封じ込めを完了
2024年M月D＋7日	情報漏えいの範囲特定とバックアップからの復旧を完了

（３）被害内容

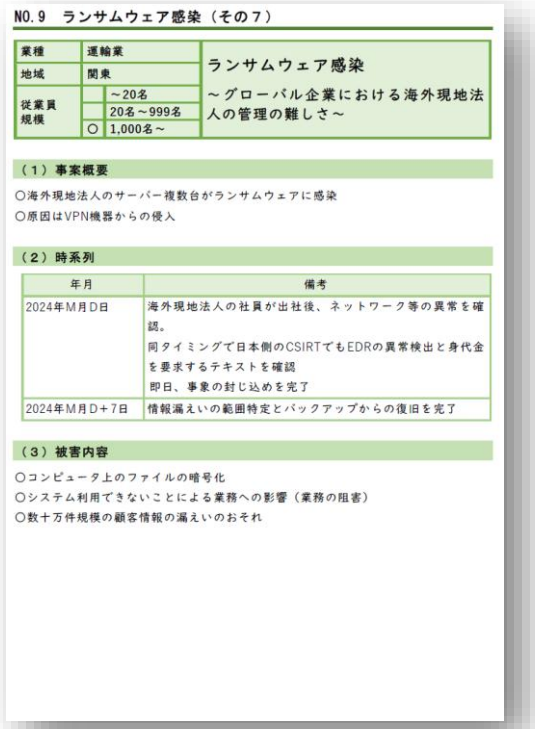
○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○数十万件規模の顧客情報の漏えいのおそれ

VPN機器からの侵入によりランサムウェアに感染

年月	備考
2024年M月D日	海外現地法人の社員が出社後、ネットワーク等の異常を確認。 同タイミングで日本側のCSIRTでもEDRの異常検出と身代金を要求するテキストを確認 即日、事象の封じ込めを完了
2024年M月D＋7日	情報漏えいの範囲特定とバックアップからの復旧を完了

Copyright　2025　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー⑤運輸業（関東）事案概要



NO.9　ランサムウェア感染（その７）

業種	運輸業	ランサムウェア感染 ～グローバル企業における海外現地法人の管理の難しさ～
地域	関東	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○海外現地法人のサーバー複数台がランサムウェアに感染
○原因はVPN機器からの侵入

（２）時系列

年月	備考
2024年M月D日	海外現地法人の社員が出社後、ネットワーク等の異常を確認。 同タイミングで日本側のCSIRTでもEDRの異常検出と身代金を要求するテキストを確認 即日、事象の封じ込めを完了
2024年M月D＋7日	情報漏えいの範囲特定とバックアップからの復旧を完了

（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○数十万件規模の顧客情報の漏えいのおそれ

5,000万円

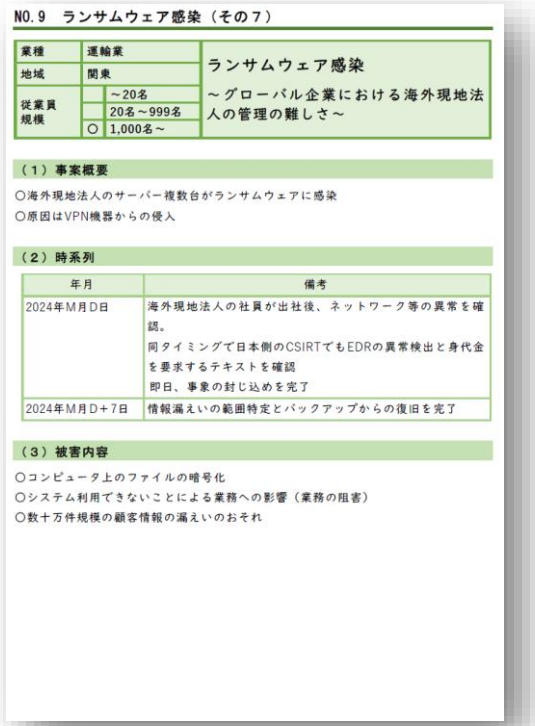
＋　対応に要した内部工数：30人月

＋　利益喪失：不明

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	1,000万円	EDRベンダーのリテーナー契約に基づきフォレンジック調査を実施。調査費用と日本のCSIRTメンバーの海外現地法人への渡航費用
	再発防止費用	1,500万円	ADサーバーの再構築などの海外現地法人での支払い
	法律相談費用	2,000万円	海外のローファームへの法律相談（対応策に関するコンサルティング費用を含む）
	コールセンター費用	500万円	国内顧客への対応のためのグループ内コールセンターへの委託費用

Copyright　2025　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

インタビュー⑤運輸業（関東）被害者コメント



NO.9　ランサムウェア感染（その７）

業種	運輸業	ランサムウェア感染 ～グローバル企業における海外現地法人の管理の難しさ～
地域	関東	
従業員規模	～20名	
	20名～999名	
	○ 1,000名～	

（１）事案概要

○海外現地法人のサーバー複数台がランサムウェアに感染
○原因はVPN機器からの侵入

（２）時系列

年月	備考
2024年M月D日	海外現地法人の社員が出社後、ネットワーク等の異常を確認。 同タイミングで日本側のCSIRTでもEDRの異常検出と身代金を要求するテキストを確認 即日、事象の封じ込めを完了
2024年M月D＋7日	情報漏えいの範囲特定とバックアップからの復旧を完了

（３）被害内容

○コンピュータ上のファイルの暗号化
○システム利用できないことによる業務への影響（業務の阻害）
○数十万件規模の顧客情報の漏えいのおそれ

○VPN機器のメンテナンス用ID/Passwordに多要素認証が入っていなかったため侵入を許したと認識
○従前に身代金要求には応じない方針をグループ内の最上位の機関として決定済のため身代金支払はしていない。
○海外現地法人の事業は、日本法人と比較して薄利であることは珍しくない。この場合、日本からセキュリティを目的とした大規模な投資は税制上難しい。そのため、ある程度は海外現地法人の裁量に対応を委ねる必要がある。
○日本側で構築したガバナンスを海外現地法人に共有したことなどが有効に作用。本件インシデントでも日本側で各機器のログを確認するなどした。この対応が海外現地法人との信頼関係の構築につながったと感じている。
○以前にも、別の海外現地法人で不正アクセスが発生。1億円弱の被害が生じた。従来の海外現地法人への対応はリモートでのヒアリングやチェックシートの活用に留まっていたが、同案件以降、体制を変更したことが功を奏した。

Copyright　2025　JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

リアルをみても

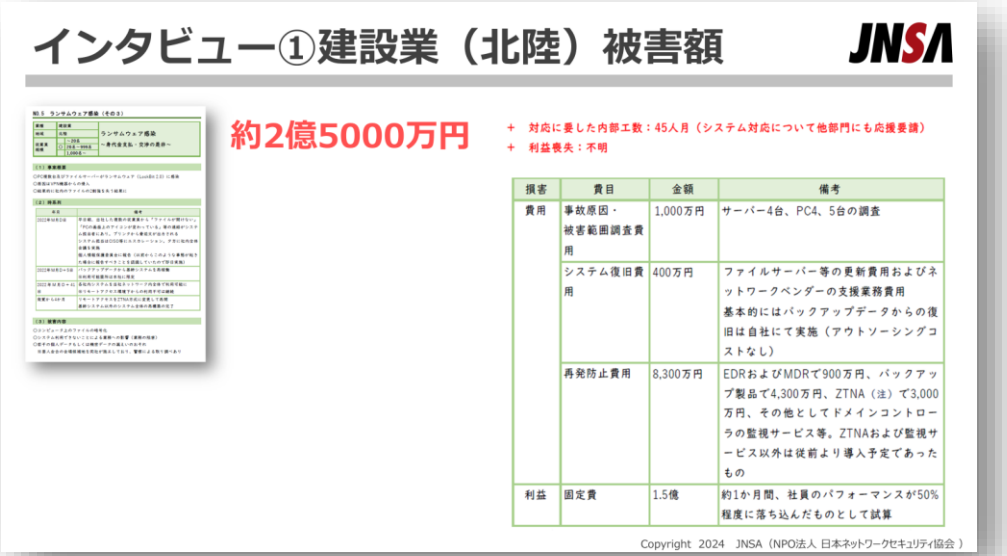
「お金がかかる」

ことがわかります・・・

特にランサムウェア被害は高額になる傾向があります

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

後半のまとめ



インタビュー①建設業（北陸）被害額

JNSA

約2億5000万円

＋ 対応に要した内部工数：45人月（システム対応について他部門にも応援要請）
＋ 利益喪失：不明

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	1,000万円	サーバー4台、PC4、5台の調査
	システム復旧費用	400万円	ファイルサーバー等の更新費用およびネットワークベンダーの支援業務費用 基本的にはバックアップデータからの復旧は自社にて実施（アウトソーシングコストなし）
	再発防止費用	8,300万円	EDRおよびMDRで900万円、バックアップ製品で4,300万円、ZTNA（注）で3,000万円、その他としてドメインコントローラの監視サービス等。ZTNAおよび監視サービス以外は従前より導入予定であったもの
利益	固定費	1.5億	約1か月間、社員のパフォーマンスが50%程度に落ち込んだものとして試算

Copyright 2024 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

実被害をみても、

中小企業においても数千万単位、場合によっては億単位

の損害が発生する

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

さいごに

Copyright 2025 JNSA（NPO法人 日本ネットワークセキュリティ協会 ）

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

さいごに

サイバー攻撃を受けると**お金がかかる**

ケースによって、数千万～億の損失がでてもおかしくない

このような被害を発生させないためにも
セキュリティ対策を見直し、強化しましょう

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）

Copyright 2025 JNSA（日本ネットワークセキュリティ協会 ）