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被害額のハナシ～

JNSA（日本ネットワークセキュリティ協会）
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

発表者紹介

神山 太朗

JNSA（日本ネットワークセキュリティ協会）
幹事、調査研究部会　インシデント被害調査WGリーダー
⇒セキュリティベンダの業界団体！

あいおいニッセイ同和損害保険
新種保険部　サイバー・特殊リスクG　担当次長

・損保業界の商品開発部門に30年弱勤務
・入社以来、IT関連の保険（現サイバー保険）などの開発に携わる
・JNSAにて「**インシデント損害額調査レポート**」を公表。そのWGリーダーを務める

本日お話しする内容は「所属企業」の立場、見解等を代表するものではありません

はじめに

～中小企業におけるサイバー攻撃の話～

中小企業でよくあるサイバー攻撃

今回ご紹介するのは以下２つ

- **サポート詐欺**
- **ランサムウェア**

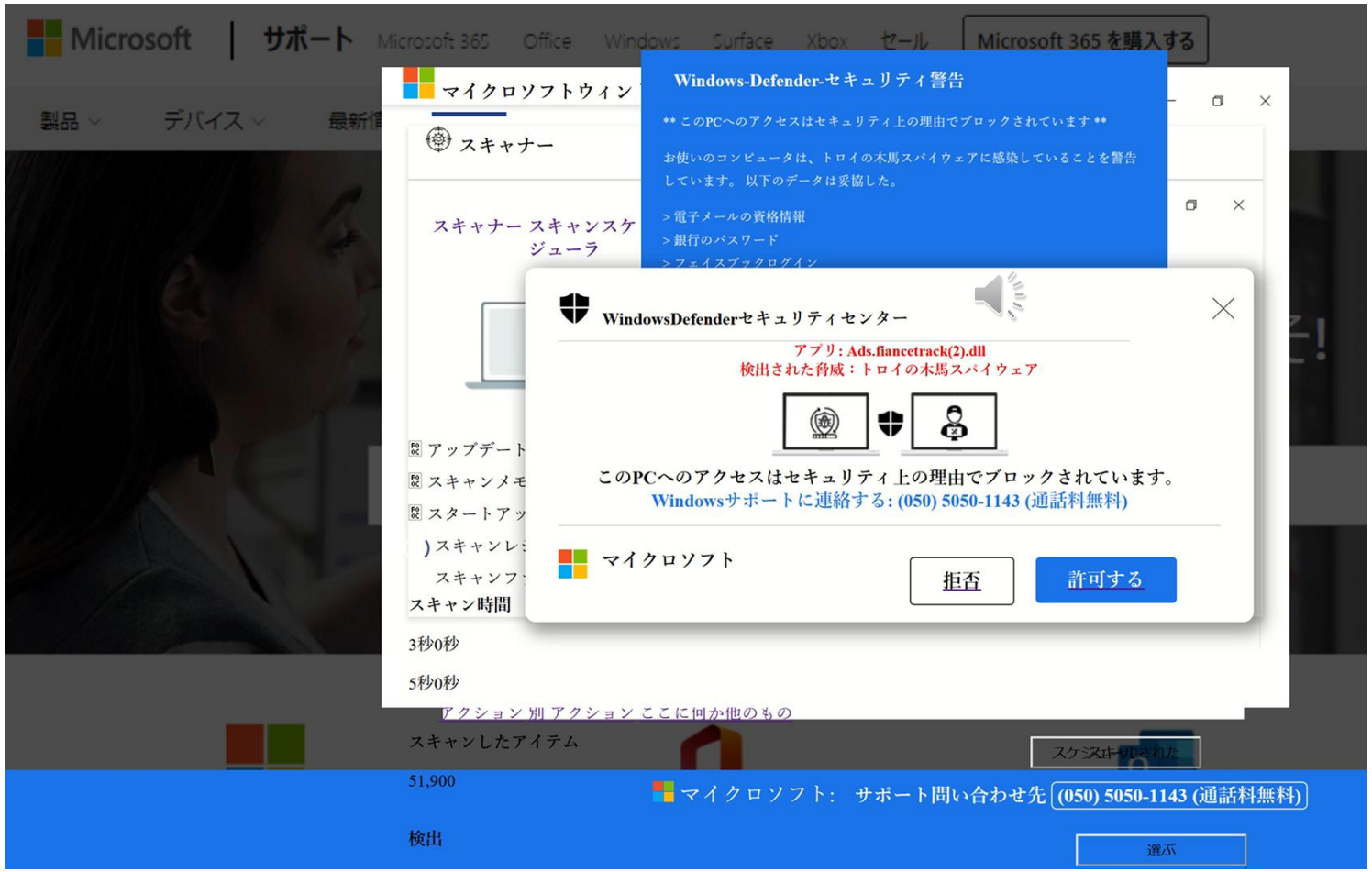
POINT	**ここ数年、中小企業でよくあるサイバー攻撃・・・。 が、他にもあるし、今後、新たな攻撃が発現する可能性もある**

サポート詐欺

～被害は個人だけではありません～

サポート詐欺　～こんなのみたことありませんか？～

◇ネットで探しものをしてたら、いきなり、こんな画面が・・・



サポート詐欺　～概要～

◇マイクロソフト等のサポートを装った**単純な詐欺**

◇個人だけではなく、**法人の従業員**がひっかかる事例が増加中

◇コンビニで「AmazonやGoogleの電子マネーを買ってこい！」と指示される（アヤシイ…ってか、ありえない…）

◇最悪、PCが乗っ取られる

対処方法	○**相手にしない**（ウイルスに感染していません） ○**ブラウザを閉じる**（ESCキーを長押しする、強制終了等） ○**電話しない**（画面に電話番号が表示していても無視） ○**電話しちゃってもすぐに切る**（いかにもアヤシイのでわかると思います…）

サポート詐欺　～ネットバンキングを狙うパターンも～

◇電子マネーではなく、ネットバンキングの預金を狙うパターンも

◇笛吹市商工会の事案（右記）は、ネットバンキングを利用しているPCに遠隔操作ソフトをインストールさせ、知らない間に**1000万円**送金された事案

◇大津市の事案（右記）は、会社名義の口座に関連する情報を聞き出し、9回にわたって他の口座に**4250万円**送金された事案

ランサムウェア

～最近の一番の脅威～

ランサムウェア　～概要～

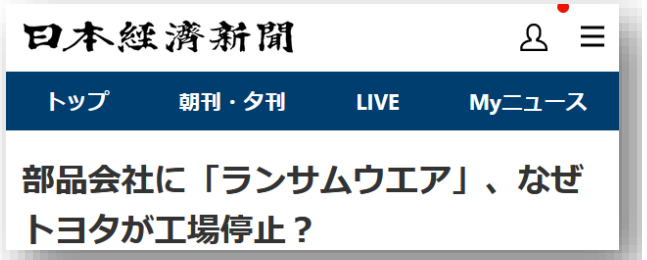
◇Ransom（ランサム）＝**身代金**

◇データを**暗号化**。復号（回復）と引換に身代金を要求するウイルス

◇システム停止等で業務が阻害。**取引先・顧客に迷惑をかける事態に**

◇次のような事例で誰もが知るところに

2021年10月　徳島のつるぎ町立**半田病院**
2022年　3月　**トヨタ**の工場停止（サプライヤーである小島プレス工業が感染）
2022年10月　**大阪急性期・総合医療センター**
2023年　7月　**名古屋港**（名古屋港運協会）
2024年　6月　**KADOKAWA**（ニコ動、ドワンゴ）



ランサムウェア　～一番の脅威～

◇**IPA**（注）が毎年発表している
「情報セキュリティ10大脅威」において
直近（2024/1/24公表）の**第１位！**

（注）アイピーエー。独立行政法人情報処理推進機構。経済産業省所管の独立行政法人。サイバー攻撃から企業・組織を守る取組み等を実施。「中小企業の情報セキュリティ対策ガイドライン」など多くのセキュリティ関連のコンテンツを公開

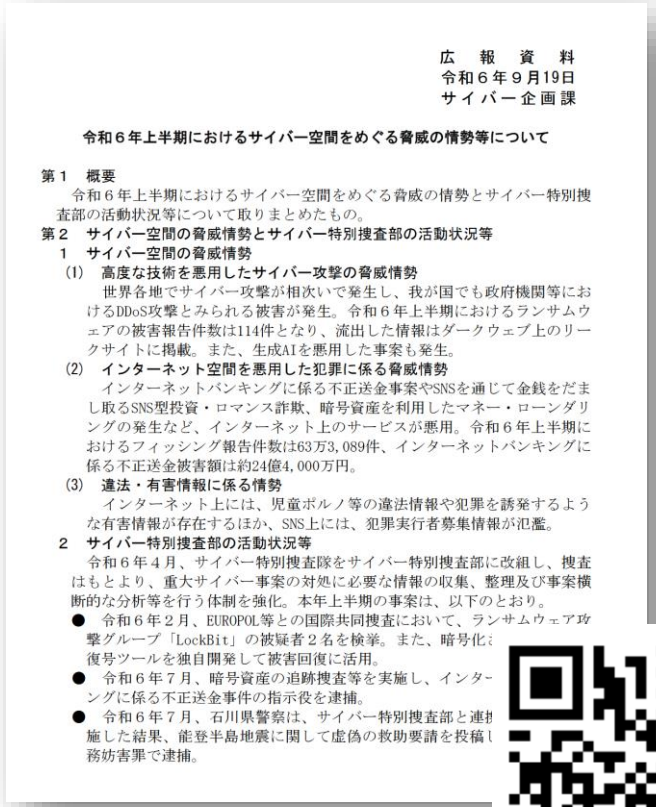
順位	内容
1位	**ランサムウェアによる被害**
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

IPA「情報セキュリティ10大脅威 2024」

◇政府組織、セキュリティの業界団体、多くの
セキュリティベンダ等を含めて、
業界の一番の関心事＆脅威はランサムウェア！

ランサムウェア　～大企業だけではない～

◇警察庁の広報資料からも被害拡大は明らか！！！

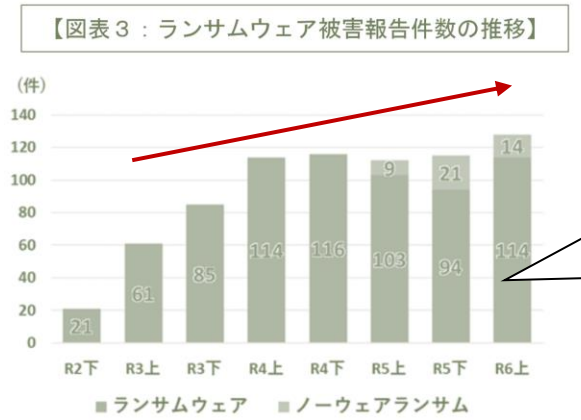


広　報　資　料
令和６年９月19日
サイバー企画課

令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について

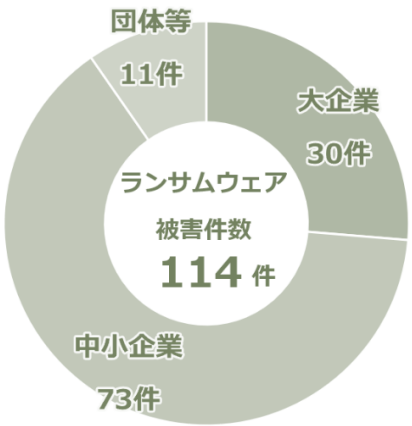
第１　概要
令和６年上半期におけるサイバー空間をめぐる脅威の情勢とサイバー特別捜査部の活動状況等について取りまとめたもの。

第２　サイバー空間の脅威情勢とサイバー特別捜査部の活動状況等
１　サイバー空間の脅威情勢
(1)　高度な技術を悪用したサイバー攻撃の脅威情勢
世界各地でサイバー攻撃が相次いで発生し、我が国でも政府機関等におけるDDoS攻撃とみられる被害が発生。令和６年上半期におけるランサムウェアの被害報告件数は114件となり、流出した情報はダークウェブ上のリークサイトに掲載。また、生成AIを悪用した事案も発生。
(2)　インターネット空間を悪用した犯罪に係る脅威情勢
インターネットバンキングに係る不正送金事案やSNSを通じて金銭をだまし取るSNS型投資・ロマンス詐欺、暗号資産を利用したマネー・ローンダリングの発生など、インターネット上のサービスが悪用。令和６年上半期におけるフィッシング報告件数は63万3,089件、インターネットバンキングに係る不正送金被害額は約24億4,000万円。
(3)　違法・有害情報に係る情勢
インターネット上には、児童ポルノ等の違法情報や犯罪を誘発するような有害情報が存在するほか、SNS上には、犯罪実行者募集情報が氾濫。
２　サイバー特別捜査部の活動状況等
令和６年４月、サイバー特別捜査隊をサイバー特別捜査部に改組し、捜査はもとより、重大サイバー事案の対処に必要な情報の収集、整理及び事案横断的な分析等を行う体制を強化。本年上半期の事案は、以下のとおり。
●　令和６年２月、EUROPOL等との国際共同捜査において、ランサムウェア攻撃グループ「LockBit」の被疑者２名を検挙。また、暗号化
復号ツールを独自開発して被害回復に活用。
●　令和６年７月、暗号資産の追跡捜査等を実施し、インター
ングに係る不正送金事件の指示役を逮捕。
●　令和６年７月、石川県警察は、サイバー特別捜査部と連
施した結果、能登半島地震に関して虚偽の救助要請を投稿
務妨害罪で逮捕。



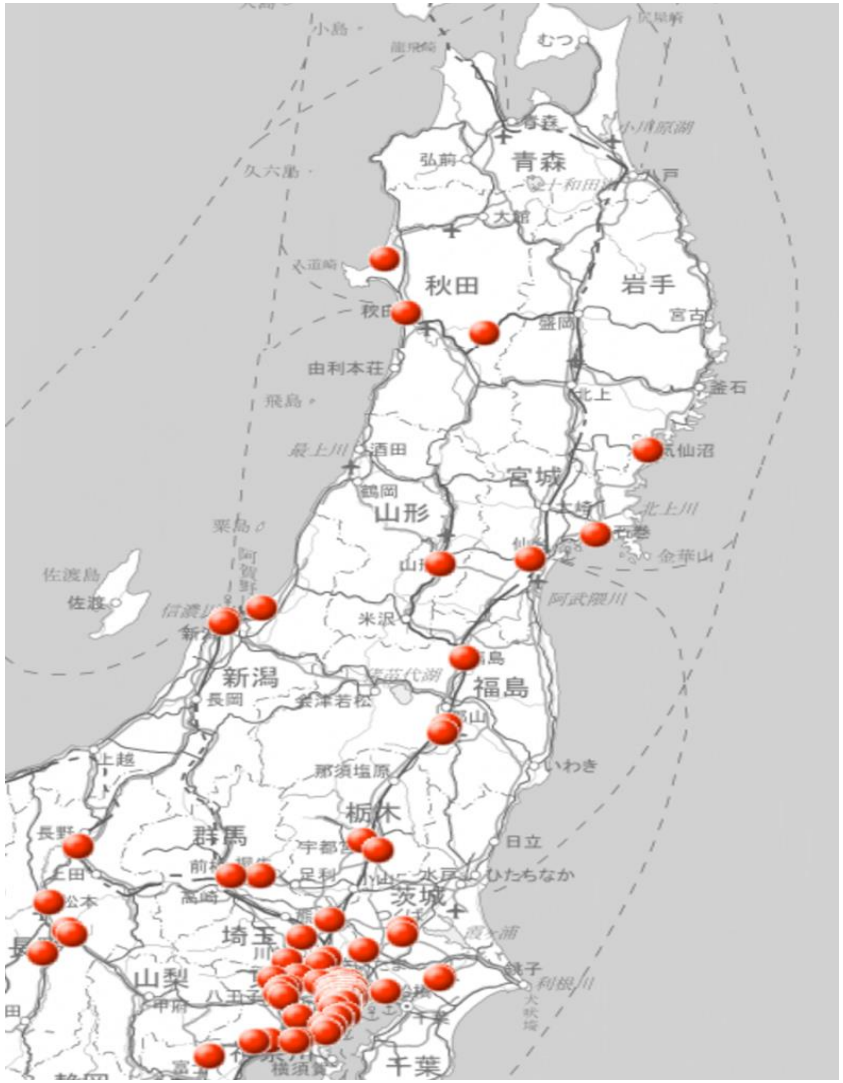
※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

2024年上期は
2020年下期の約**6倍**



大企業だけの被害ではない。
中小企業や団体等の被害が約7割

ランサムウェア　～東北の被害組織～



◇左記は2017年1月～2024年6月までのランサムウェア被害組織（本社所在地）をマッピングしたもの

◇東北地方でも被害組織は散見される

ここまでのまとめ

サイバー攻撃は身近です
他人事ではありません

本題

～サイバー攻撃を受けるとお金がかかる～

レポート紹介

「インシデント損害額調査レポート」

◇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 生の声を聞くため、ウェブでの直接ヒアリングも実施

◇検索サイトで「インシデント損害額」の語で検索をかけると出てきます

ご一読を！！！

本日、イイタイコト

～シンプル、単純明快です！～

イイタイコト①

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

イイタイコト②

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**自ら理解してもらう**

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**経営者に説明してもらう**

③その他の方

このレポートで、**対策の必要性**を**経営者、情シスに説明してもらう**

前半

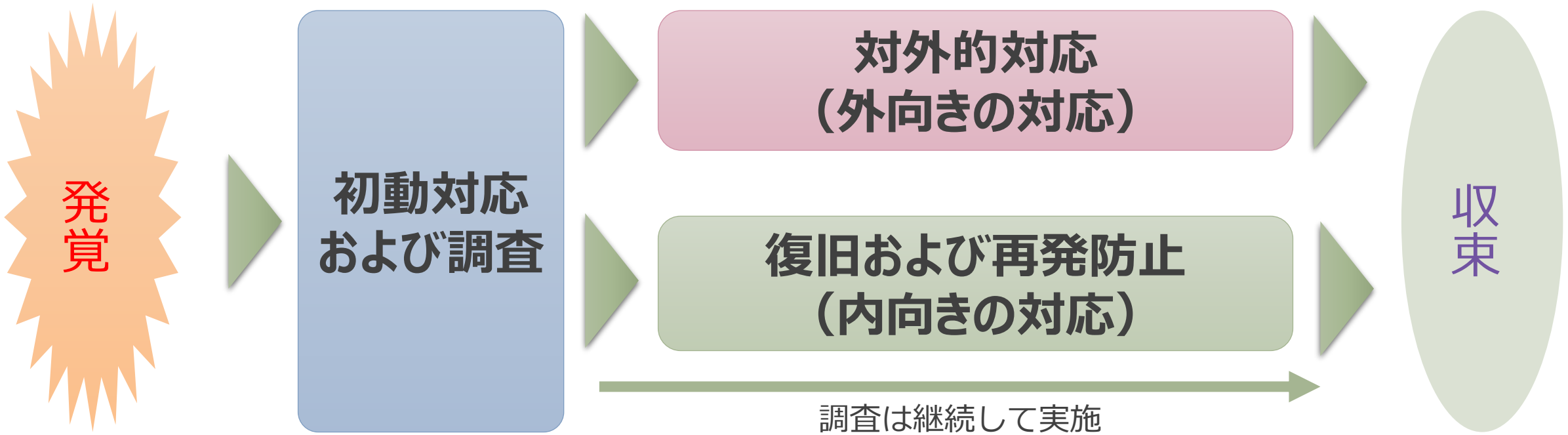
「各種損害のコスト」

～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～

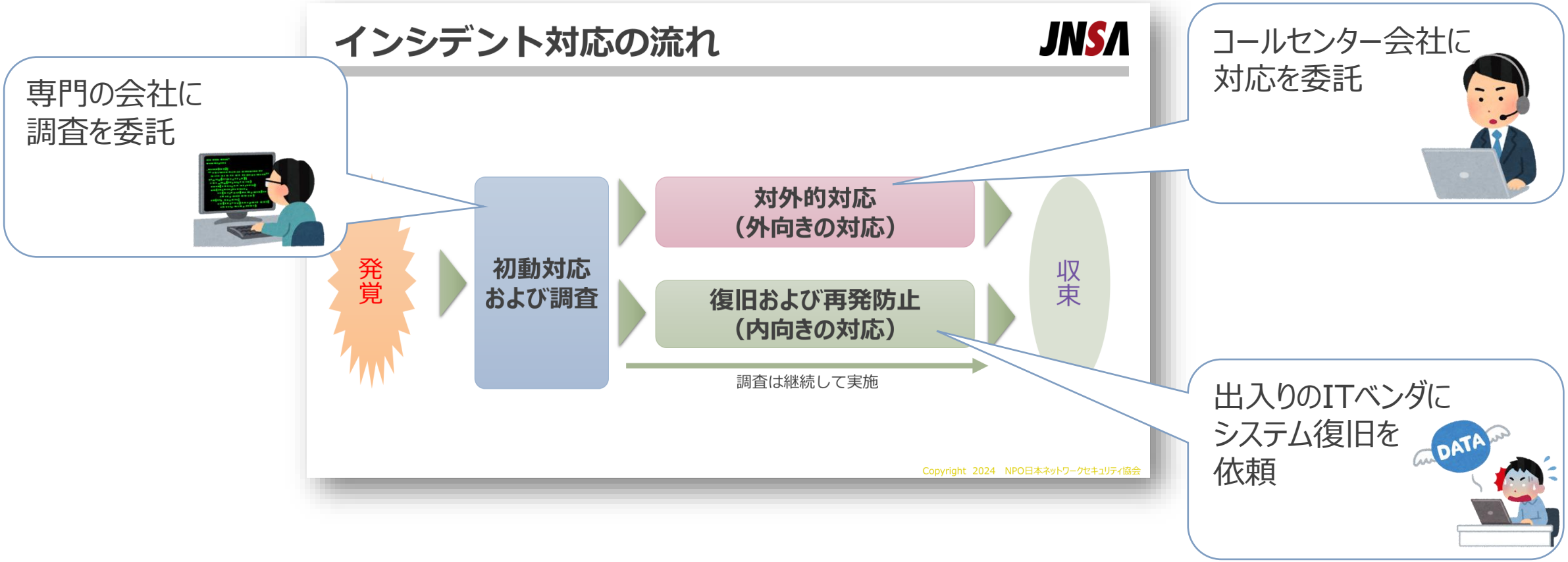
前提：対応と各種損害

～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～

インシデント対応の流れ



アウトソーシングの必要性



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

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

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、自社で直接、費用を負担することにより被る損害

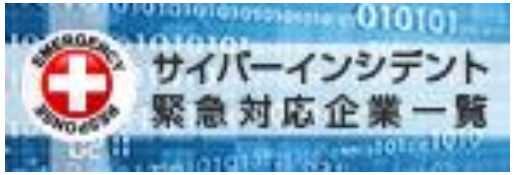
事故原因・被害範囲調査費用

◆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～



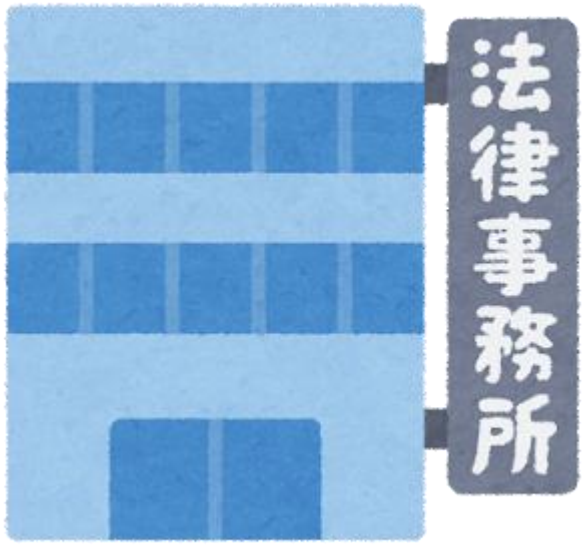
※JNSAのHPに、インシデントレスポンスを行う会員企業の一覧あり

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～

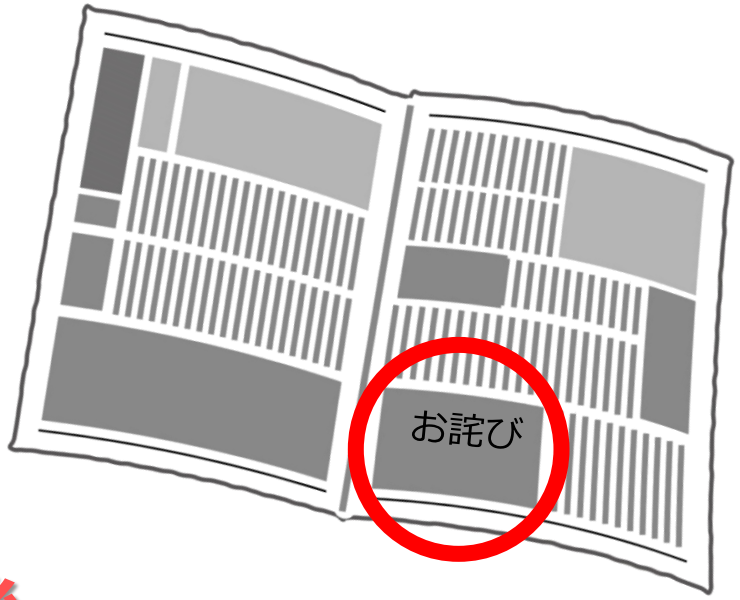


広告・宣伝活動費用

◆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



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**120万円～**
⇒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600万円～

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

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

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

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

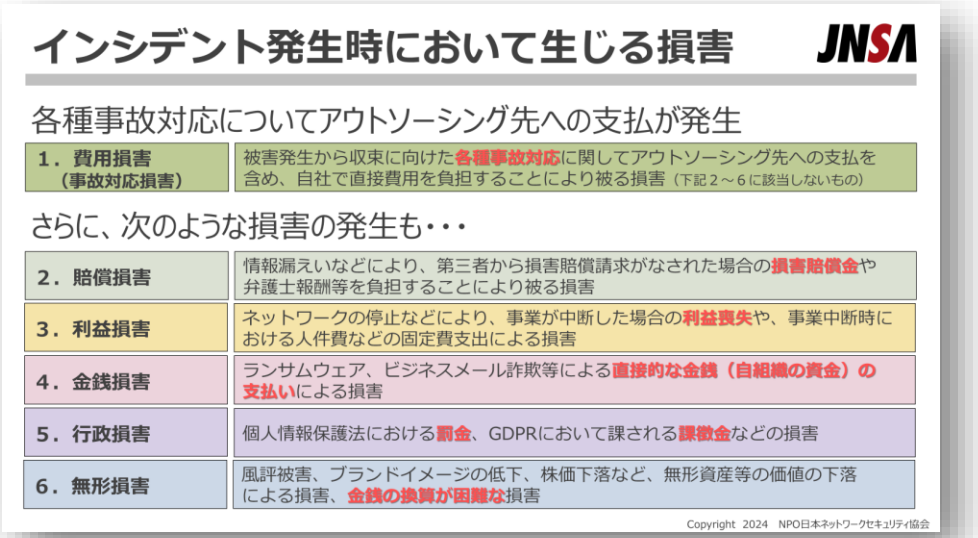
項目	平時	事業中断時	差額
売上高	10億円	8億円	▲2億円
固定費 人件費、賃料等	2億円	2億円	—
変動費 材料費、電気代等	7億円	5.6億円	▲1.4億円
営業利益（損失）	1億円	0.4億円	▲0.6億円

◇事業中断による売上が2割減

◇通常1億円稼げるのに、
固定費がかかるので0.4億円しか稼げなかった

◇**結果として、**
0.4億円－1億円＝▲0.6億円

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

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、

中小企業目線でも数千万単位、場合によっては億単位

の損害が発生する

後半

「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～

調査内容

「インシデント損害額調査レポート第2版」での調査内容

調査内容

①被害組織調査

過去5年半に渡り、**サイバー攻撃**による**国内**の被害組織を**約1,300**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1,300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**

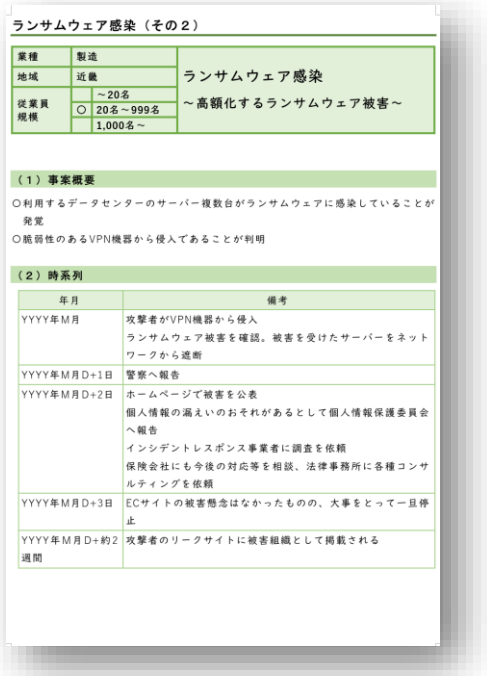
③被害組織インタビュー

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。**生々しい実態を確認**

まずは「被害企業インタビュー」

リアルな数字…をお伝えします

インタビュー　～ランサムウェア感染～



ランサムウェア感染（その２）

業種	製造	ランサムウェア感染 ～高額化するランサムウェア被害～
地域	近畿	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○利用するデータセンターのサーバー複数台がランサムウェアに感染していることが発覚
○脆弱性のあるVPN機器から侵入であることが判明

（２）時系列

年月	備考
YYYY年M月	攻撃者がVPN機器から侵入 ランサムウェア被害を確認。被害を受けたサーバーをネットワークから遮断
YYYY年M月D+1日	警察へ報告
YYYY年M月D+2日	ホームページで被害を公表 個人情報の漏えいのおそれがあるとして個人情報保護委員会へ報告 インシデントレスポンス事業者に調査を依頼 保険会社にも今後の対応等を相談、法律事務所に各種コンサルティングを依頼
YYYY年M月D+3日	ECサイトの被害懸念はなかったものの、大事をとって一旦停止
YYYY年M月D+約2週間	攻撃者のリークサイトに被害組織として掲載される

■事案概要

VPN機器からランサムウェアに感染

■時系列

年月	備考
YYYY年M月	攻撃者がVPN機器から侵入 ランサムウェア被害を確認。被害を受けたサーバーをネットワークから遮断
YYYY年M月D+1日	警察へ報告
YYYY年M月D+2日	ホームページで被害を公表 個人情報の漏えいのおそれがあるとして個人情報保護委員会へ報告 インシデントレスポンス事業者に調査を依頼 保険会社にも今後の対応等を相談、法律事務所に各種コンサルティングを依頼
YYYY年M月D+3日	ECサイトの被害懸念はなかったものの、大事をとって一旦停止
YYYY年M月D+約2週間	攻撃者のリークサイトに被害組織として掲載される

インタビュー　～ランサムウェア感染（続き）～

ランサムウェア感染（その２）

業種	製造	ランサムウェア感染 ～高額化するランサムウェア被害～
地域	近畿	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○利用するデータセンターのサーバー複数台がランサムウェアに感染していることが発覚
○脆弱性のあるVPN機器から侵入であることが判明

（２）時系列

年月	備考
YYYY年M月	攻撃者がVPN機器から侵入 ランサムウェア被害を確認。被害を受けたサーバーをネットワークから遮断
YYYY年M月D+1日	警察へ報告
YYYY年M月D+2日	ホームページで被害を公表 個人情報の漏えいのおそれがあるとして個人情報保護委員会へ報告 インシデントレスポンス事業者に調査を依頼 保険会社にも今後の対応等を相談、法律事務所に各種コンサルティングを依頼
YYYY年M月D+3日	ECサイトの被害懸念はなかったものの、大事をとって一旦停止
YYYY年M月D+約2週間	攻撃者のリークサイトに被害組織として掲載される

■被害額

1.24億＋人件費（1,000万強）＋利益喪失

■コメント（レポートの一部抜粋）

○「**なるべくしてなった（経営層にイイタイ…。）**」
「他人事と捉えていた。まさか自社が被害に遭うとは」

○**情報セキュリティの指揮官がおらず**、インシデント発生時に
何から手を付ければいいかわからなかった。

○実は**VPN機器の保守サービスを途中解約**してしまったことに起因

○セキュリティ対策の強化を図っているが、
今後、**EDRだけでは防げないであろうことも認識**している。

リアルをみても

「お金がかかる」

ことがわかります・・・

ランサムウェアは特に高額に・・・

「アンケート調査」

アンケート調査からみえてくるもの…

ランサムウェア感染組織の被害金額

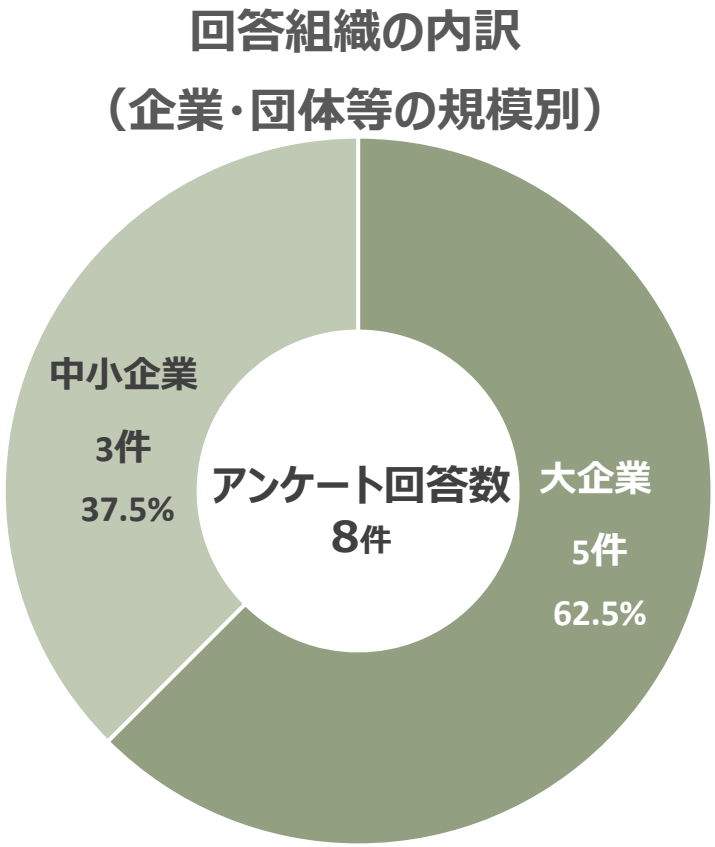
◇平均被害金額：**2,386万円**

◇対応に要した組織の内部工数平均：**27.7人月**

◇ランサムウェア被害のすべての回答組織が
身代金は支払っていないと回答

◇暗号化されたデータを復旧できた組織は**50%**

◇ほとんどの被害組織について、
被害金額は1,000万円超
被害に遭った場合の影響が大きいことを確認

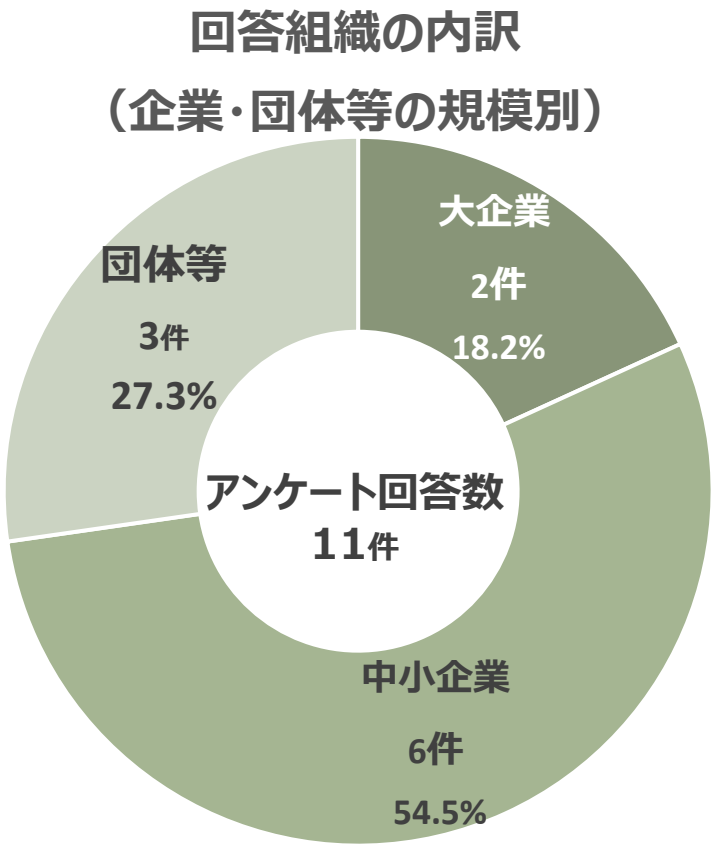


エモテット感染組織の被害金額

◇平均被害金額：**1,030万円**

◇対応に要した組織の内部工数平均：**2.9人月**

◇被害金額のばらつきが大きい



ウェブサイトからの情報漏えい被害組織の被害金額

◇平均被害金額

クレジットカード情報および個人情報の漏えい：

3,843万円

個人情報のみの漏えい：

2,955万円

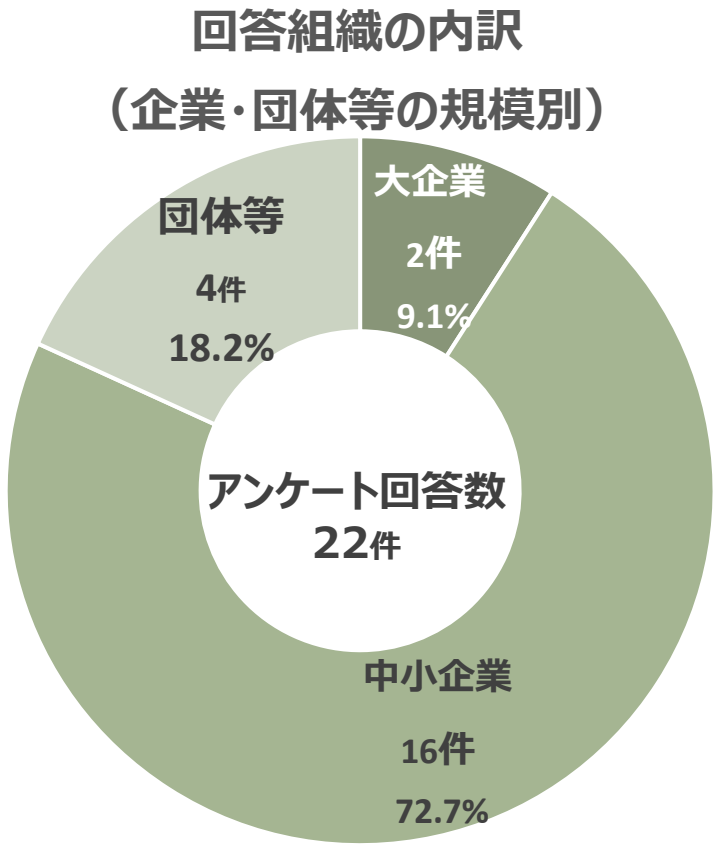
◇対応に要した組織の内部工数平均

クレジットカード情報および個人情報の漏えい：

13.3人月

個人情報のみの漏えい：

13.5人月

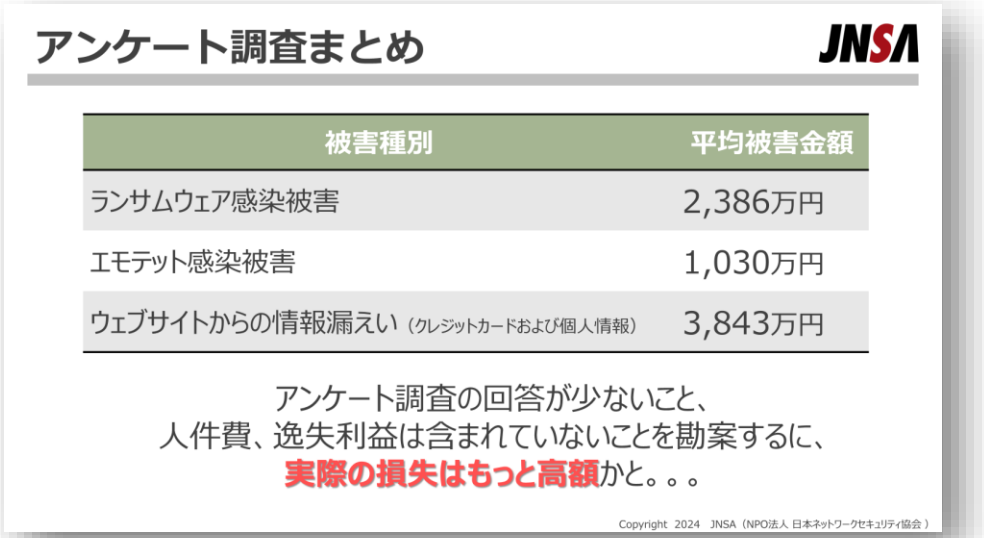


アンケート調査まとめ

被害種別	平均被害金額
ランサムウェア感染被害	2,386万円
エモテット感染被害	1,030万円
ウェブサイトからの情報漏えい（クレジットカードおよび個人情報）	3,843万円

アンケート調査の回答が少ないこと、
人件費、逸失利益は含まれていないことを勘案するに、
実際の損失はもっと高額かと。。。

後半のまとめ



アンケート調査まとめ

JNSA

被害種別	平均被害金額
ランサムウェア感染被害	2,386万円
エモテット感染被害	1,030万円
ウェブサイトからの情報漏えい（クレジットカードおよび個人情報）	3,843万円

アンケート調査の回答が少ないこと、
人件費、逸失利益は含まれていないことを勘案するに、
実際の損失はもっと高額かと。。。

実被害をみても、
中小企業目線でも数千万単位、場合によっては億単位
の損害が発生する

さいごに

対策における大きなポイント

経営者のリーダーシップで進める

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ありません

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講じていきましょう


JNSA