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～

日本ネットワークセキュリティ協会（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（あいおいニッセイ同和損害保険株式会社）

いきなりですが、

事務連絡です

このスライドについて

このスライド（pptx）、JNSAのサイトに本日公開しています！！！
是非、啓発活動等に活用してください！！！

では、本題

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

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

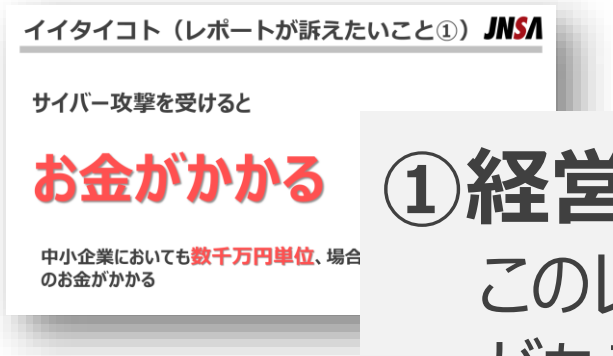
◇「本紙」「別紙」の**2部構成**

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

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**

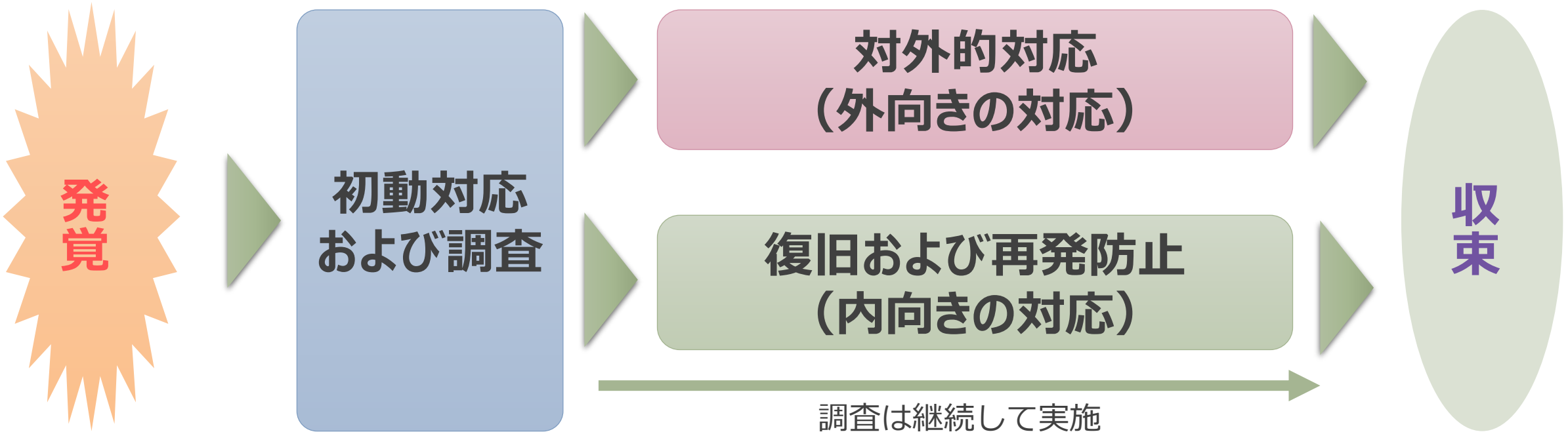
各種損害のコスト

～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～

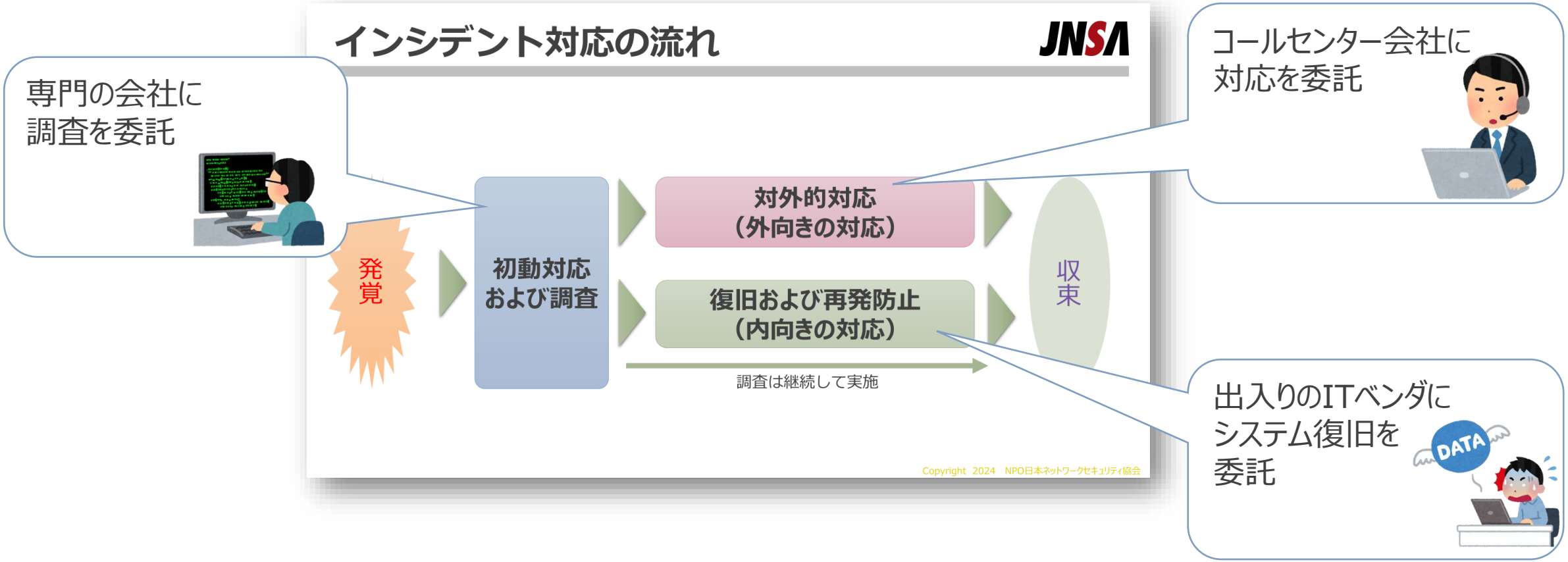
前提：対応と各種損害

～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、自組織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起こりうる

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、
自組織で直接、費用を負担することにより被る損害

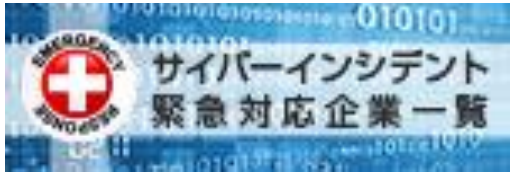
事故原因・被害範囲調査費用

◆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



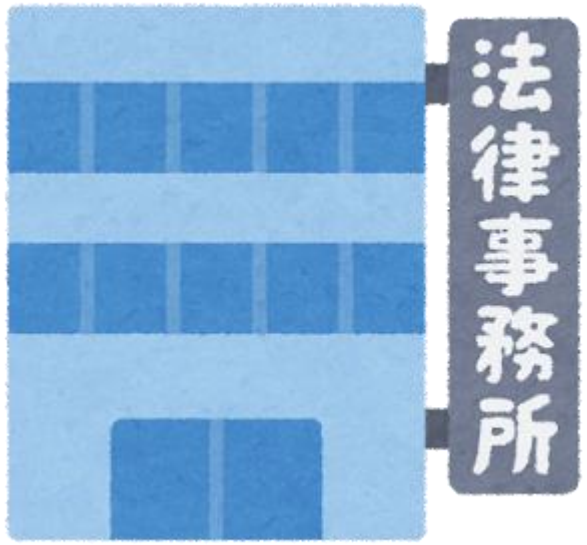
※JNSAのHPに、インシデントレスポンスを行う会員企業の一覧あり

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～

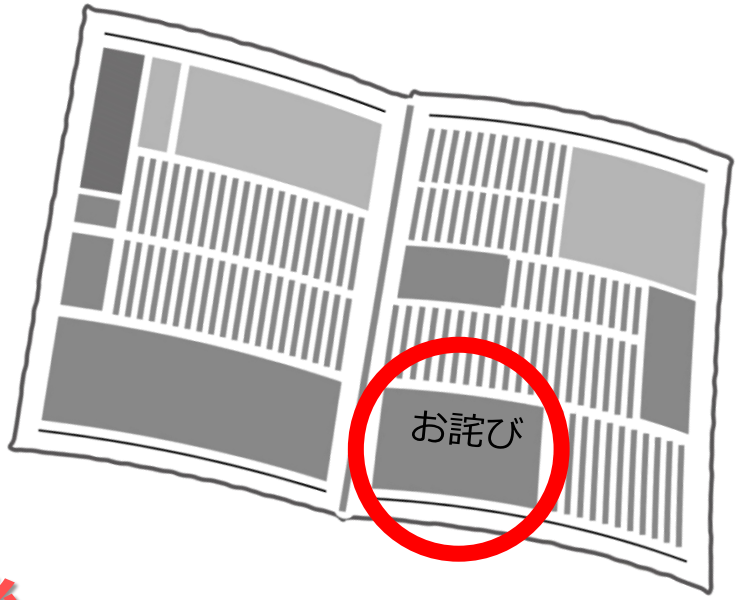


広告・宣伝活動費用

◆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**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

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	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

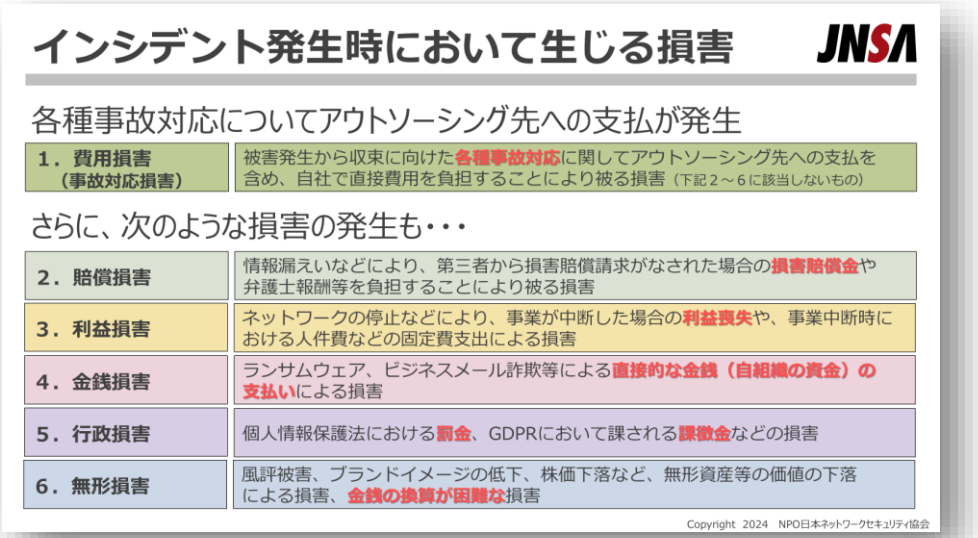
◇事業中断による売上が4割減

◇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

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

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

2017年1月～2022年6月までの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**

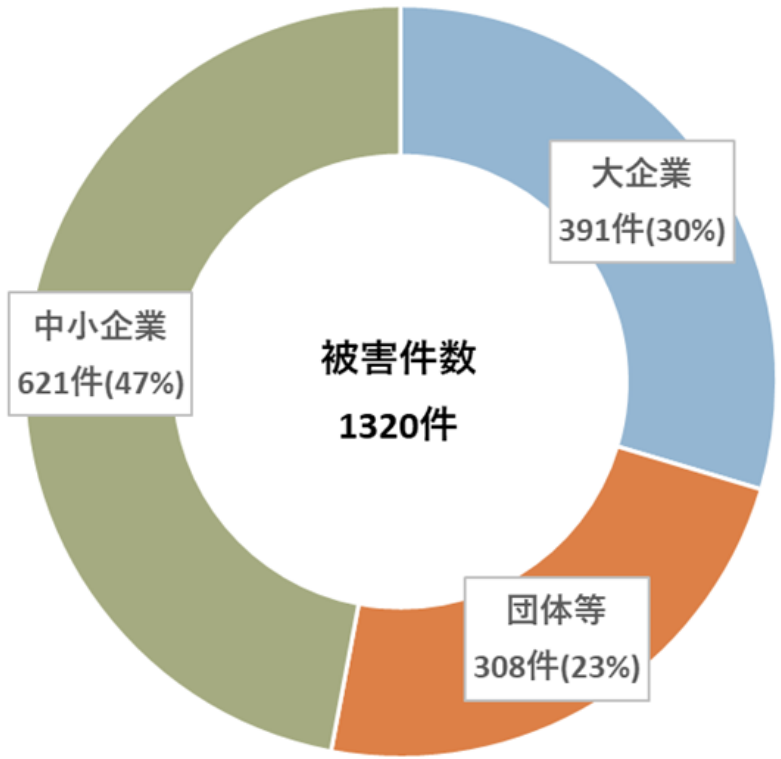
③被害組織インタビュー

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**

「被害組織調査」

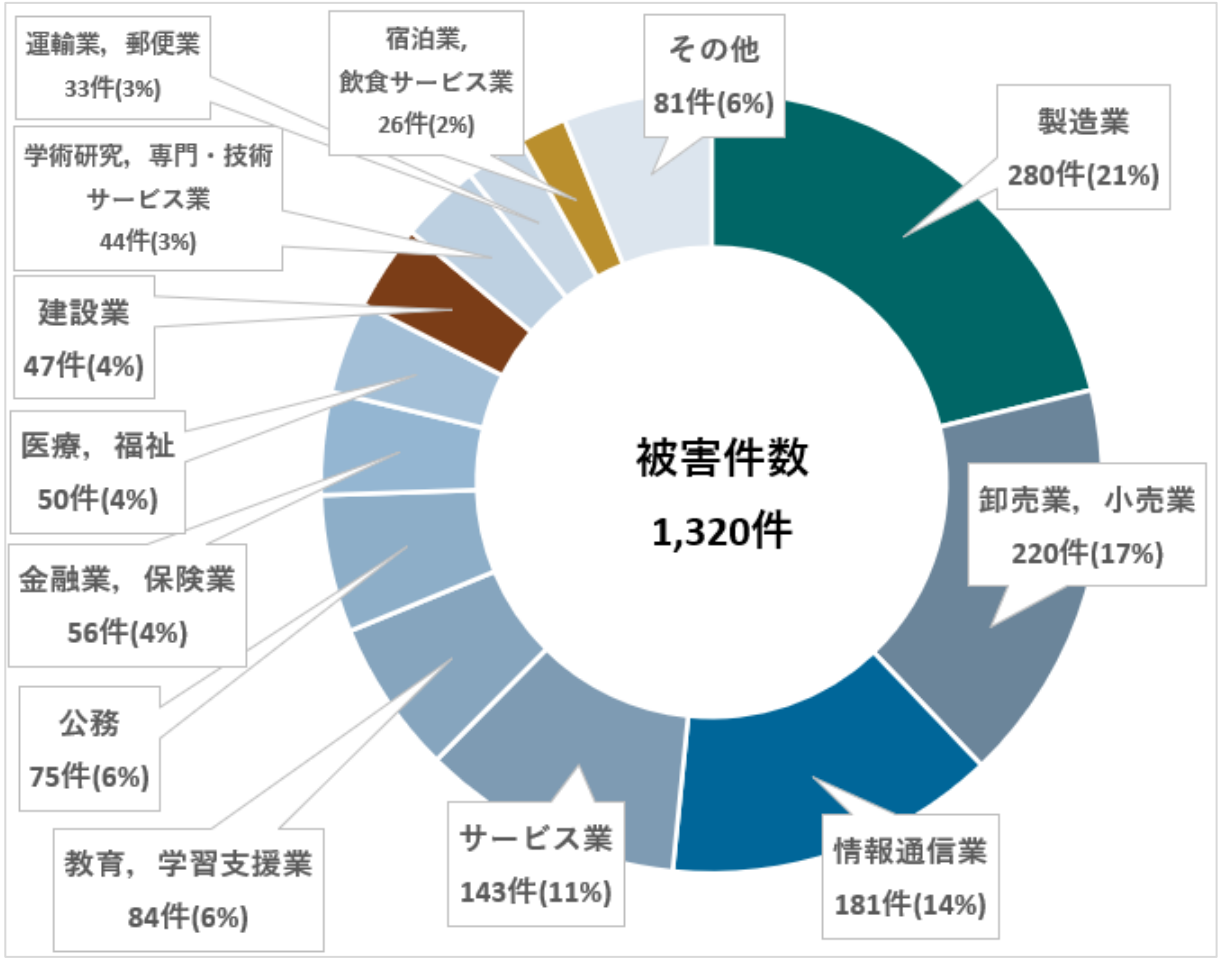
被害組織調査からみえてくるもの…

全体　～企業規模～



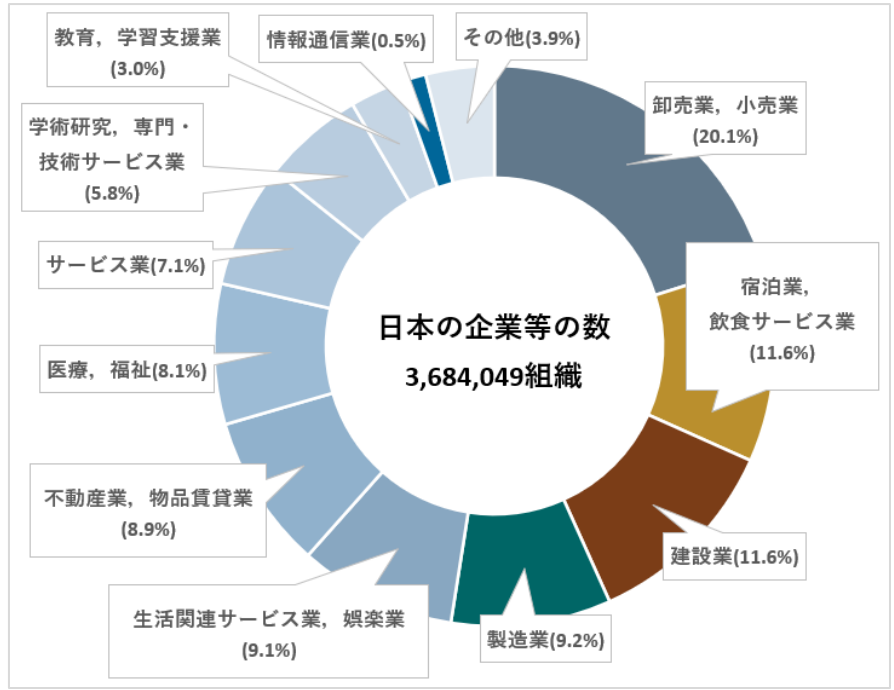
大企業だけではない

全体（1300組織）　～業種～

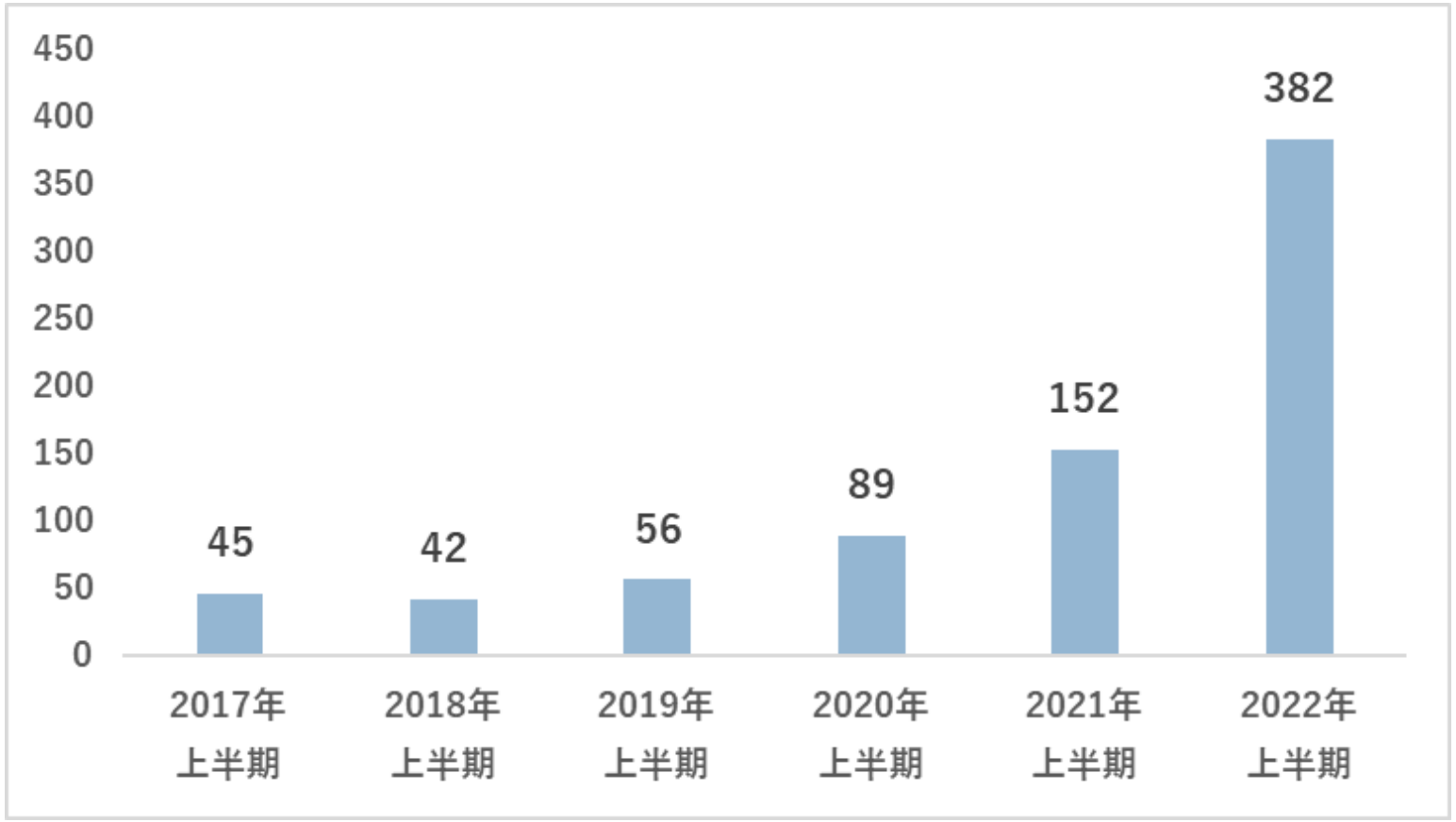


製造業、情報通信業が多い

参考（令和3年経済センサス）

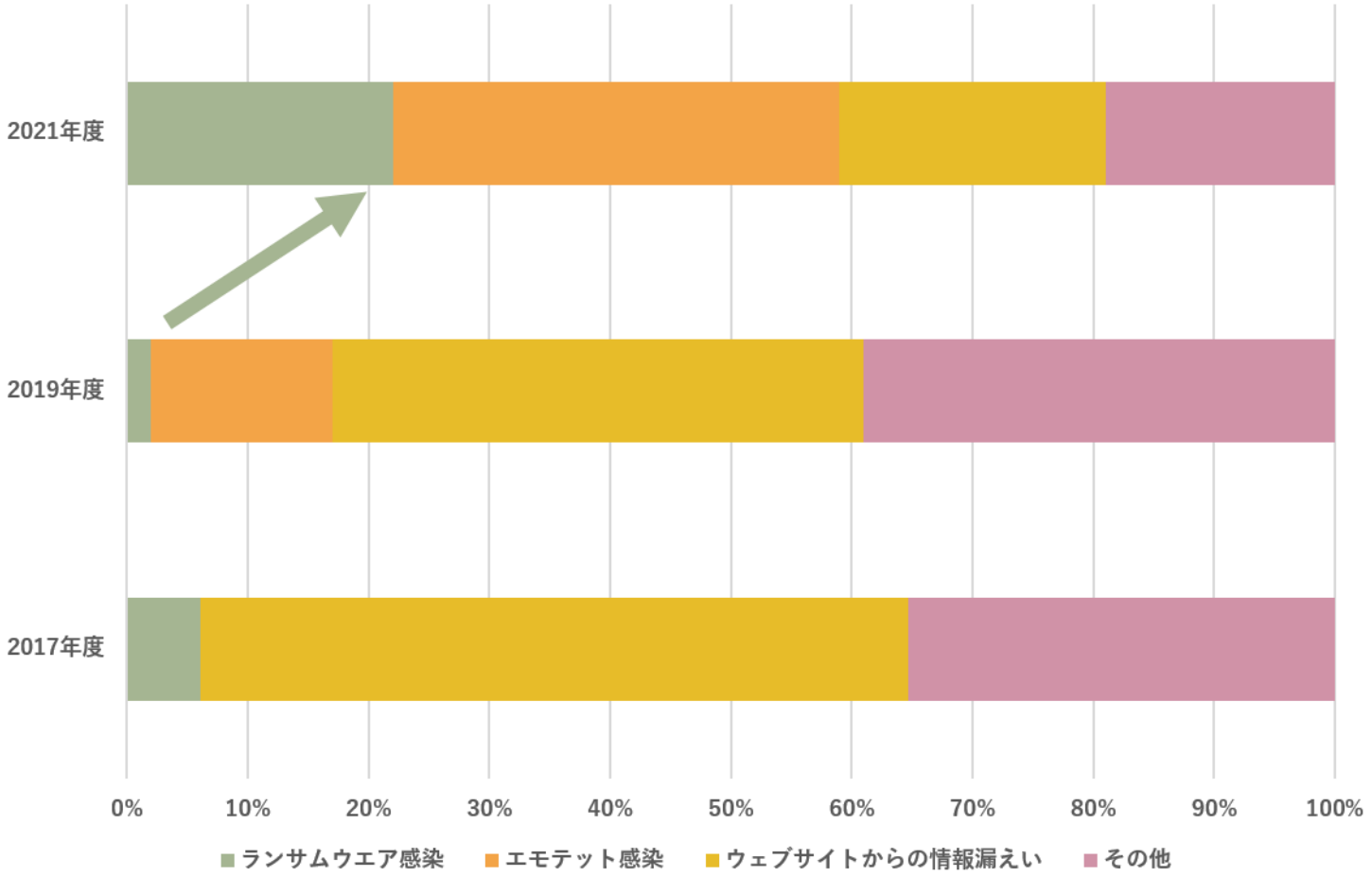


サイバー攻撃公表件数の推移



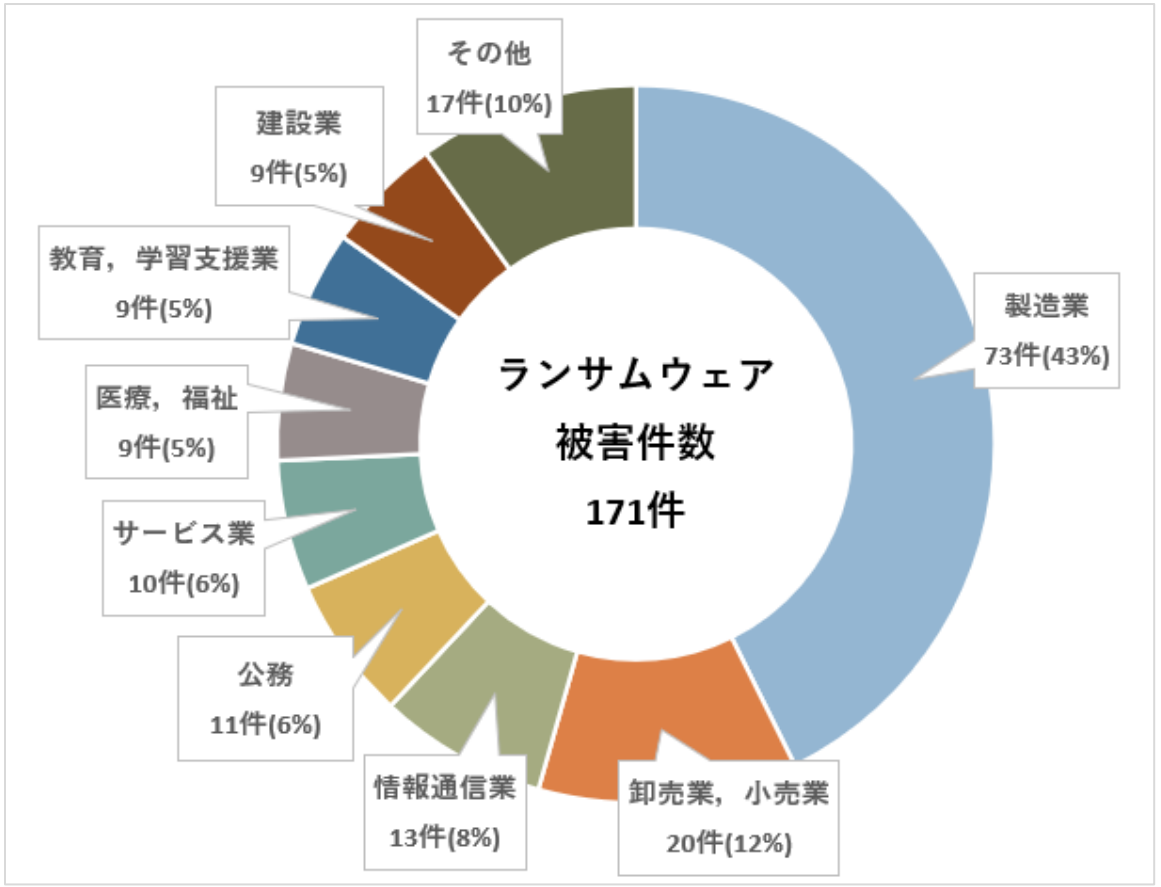
着実に年々、増えている

全体（1300組織）　～インシデント種別の年度別推移～



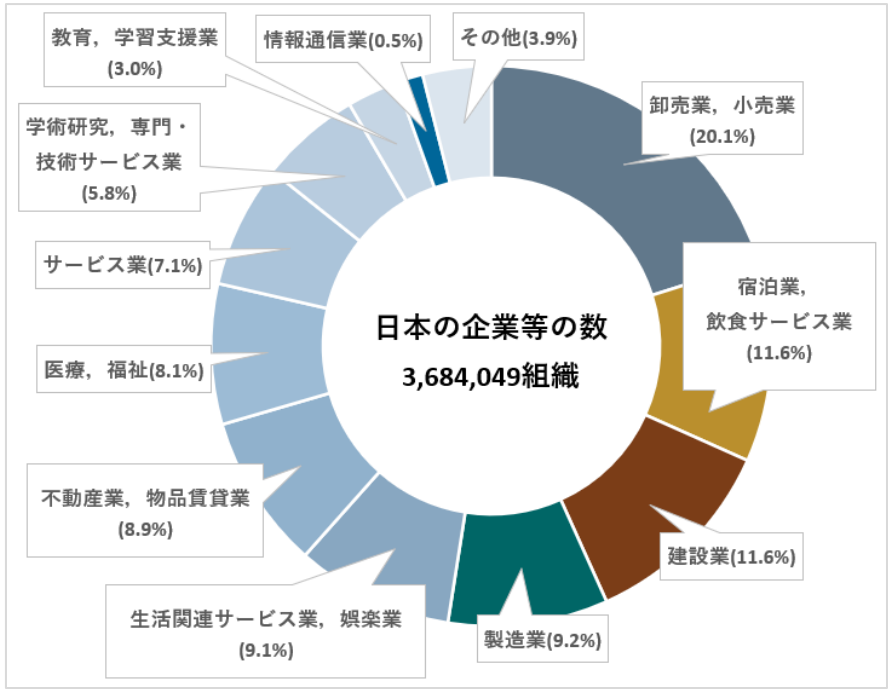
ランサムウェア被害の占める割合が増加

ランサムウェア　～業種～



間違いなく、
製造業が多い

参考（令和3年経済センサス）



「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

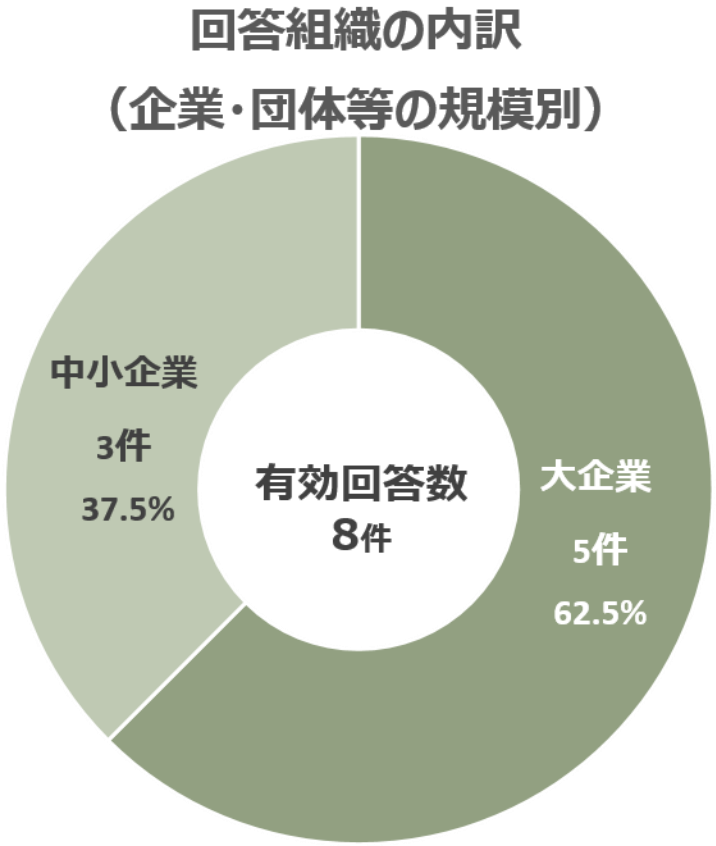
◇平均被害金額：**2,386万円**

◇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

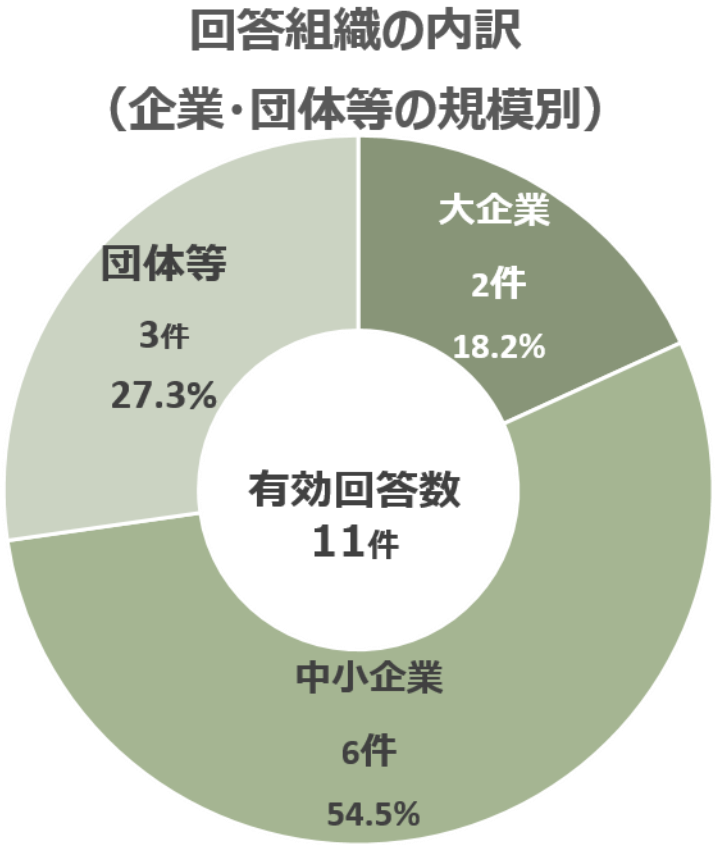


エモテット感染組織の被害金額

◇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

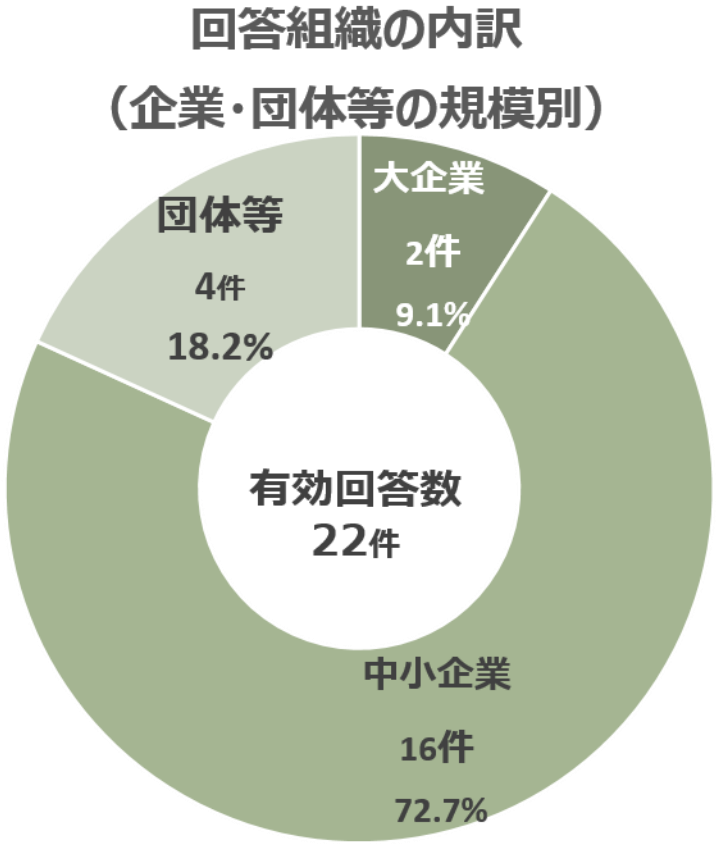
◇対応に要した組織の内部工数平均

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

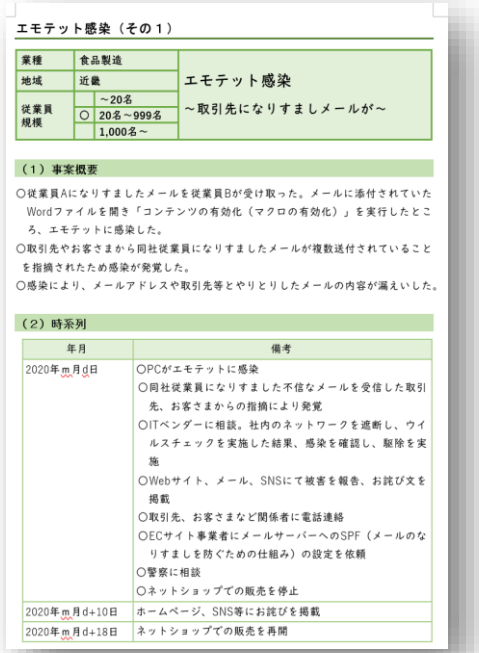
被害種別	平均被害金額
ランサムウェア感染被害	2,386万円
エモテット感染被害	1,030万円
ウェブサイトからの情報漏えい（クレジットカードおよび個人情報）	3,843万円

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と考えられる

「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　～エモテット感染～



エモテット感染（その１）

業種	食品製造	エモテット感染 ～取引先になりすましメールが～
地域	近畿	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○従業員Aになりすましたメールを従業員Bが受け取った。メールに添付されていたWordファイルを開き「コンテンツの有効化（マクロの有効化）」を実行したところ、エモテットに感染した。
○取引先やお客さまから同社従業員になりすましたメールが複数送付されていることを指摘されたため感染が発覚した。
○感染により、メールアドレスや取引先等とやりとりしたメールの内容が漏えいした。

（２）時系列

年月	備考
2020年m月d日	○PCがエモテットに感染 ○同社従業員になりすました不信なメールを受信した取引先、お客さまからの指摘により発覚 ○ITベンダーに相談。社内のネットワークを遮断し、ウイルスチェックを実施した結果、感染を確認し、駆除を実施 ○Webサイト、メール、SNSにて被害を報告、お詫び文を掲載 ○取引先、お客さまなど関係者に電話連絡 ○ECサイト事業者にメールサーバーへのSPF（メールのなりすましを防ぐための仕組み）の設定を依頼 ○警察に相談 ○ネットショップでの販売を停止
2020年m月d+10日	ホームページ、SNS等にお詫びを掲載
2020年m月d+18日	ネットショップでの販売を再開

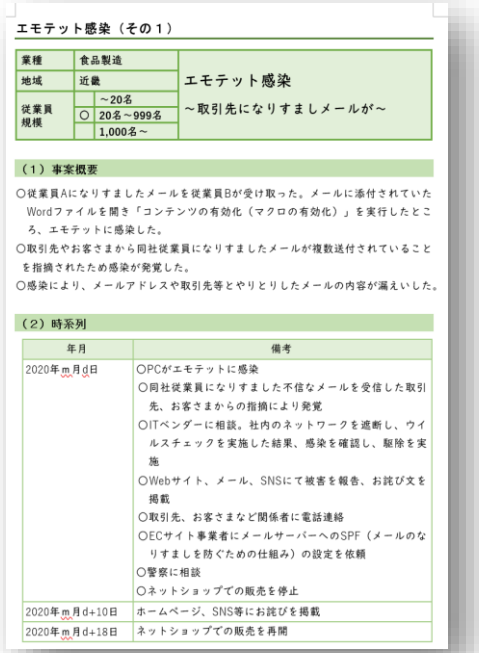
■事案概要

エモテットに感染（WORDファイルからの感染）

■時系列

年月	備考
2020年m月d日	○PCがエモテットに感染 ○同社従業員になりすました不信なメールを受信した取引先、お客さまからの指摘により発覚 ○ITベンダーに相談。社内のネットワークを遮断、ウイルスチェックを実施した結果、感染を確認し、駆除を実施 ○Webサイト、メール、SNSにて被害を報告、お詫び文を掲載 ○取引先、お客さまなど関係者に電話連絡 ○ECサイト事業者にメールサーバーへのSPF（メールのなりすましを防ぐための仕組み）の設定を依頼 ○警察に相談 ○ネットショップでの販売を停止
2020年m月d+10日	ホームページ、SNS等にお詫びを掲載
2020年m月d+18日	ネットショップでの販売を再開

インタビュー　～エモテット感染（続き）～



エモテット感染（その１）

業種	食品製造	エモテット感染 ～取引先になりすましメールが～
地域	近畿	
従業員規模	～20名	
	○ 20名～999名	
	1,000名～	

（１）事案概要

○従業員Aになりすましたメールを従業員Bが受け取った。メールに添付されていたWordファイルを開き「コンテンツの有効化（マクロの有効化）」を実行したところ、エモテットに感染した。
○取引先やお客さまから同社従業員になりすましたメールが複数送付されていることを指摘されたため感染が発覚した。
○感染により、メールアドレスや取引先等とやりとりしたメールの内容が漏えいした。

（２）時系列

年月	備考
2020年m月d日	○PCがエモテットに感染 ○同社従業員になりすました不信なメールを受信した取引先、お客さまからの指摘により発覚 ○ITベンダーに相談。社内のネットワークを遮断し、ウイルスチェックを実施した結果、感染を確認し、駆除を実施 ○Webサイト、メール、SNSにて被害を報告、お詫び文を掲載 ○取引先、お客さまなど関係者に電話連絡 ○ECサイト事業者にメールサーバーへのSPF（メールのなりすましを防ぐための仕組み）の設定を依頼 ○警察に相談 ○ネットショップでの販売を停止
2020年m月d+10日	ホームページ、SNS等にお詫びを掲載
2020年m月d+18日	ネットショップでの販売を再開

■被害額

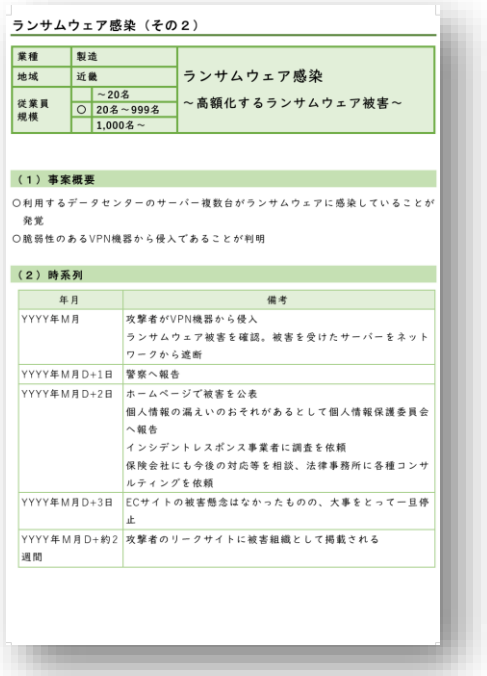
1,800万円（人件費込み）

■コメント（レポートの一部抜粋）

○QUOカードの配布について、顧問弁護士からは配布不要のコメントもあったが、若手社員を中心に「**今の若者は個人情報漏えいに敏感**」との意見もあり、配布に踏みきった。

○**うちは大丈夫という思いが少なからずあった**。しかし、被害に遭うと対応も大変で精神的な苦痛も大きいので、今後はセキュリティ対策のしっかりしたサービスへの変更ほか、サイバー保険も検討したい。

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。

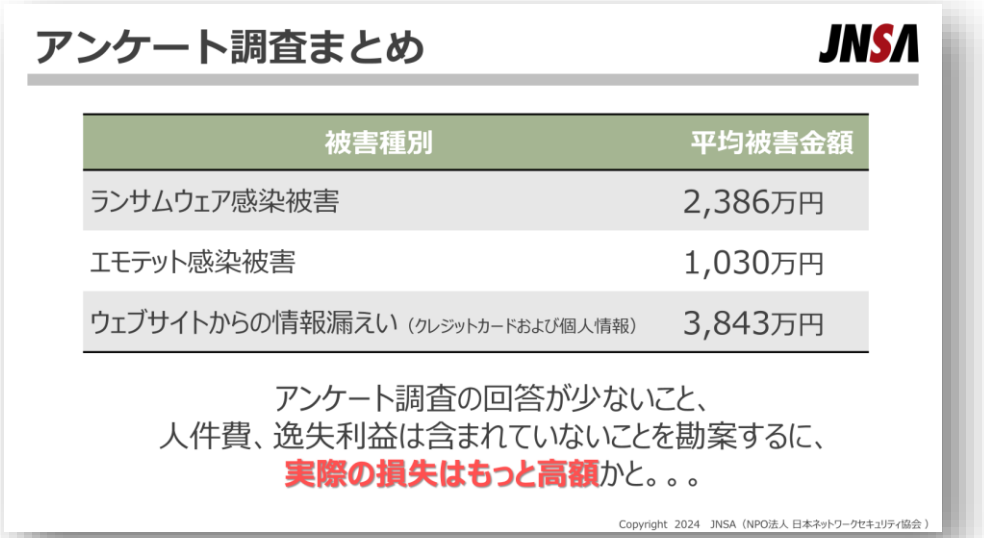
リアルをみても

「お金がかかる」

ことがわかります・・・

特にランサムウェア被害は高額になる傾向があります

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

さいごに

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講じていただくことを
切にお願いします


JNSA