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」第２版の紹介～

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
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

あいおいニッセイ同和損害保険
新種保険部　サイバー保険室　室長

・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

ご存じでしょうか？

「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ときの、以下をまとめた資料

・どのような**対応**が必要か

・対応の**アウトソーシング先**は誰か

・**コスト**はいくらかかるか　など

◇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。

◇**ぜひご一読を！！！**

まとめ…。イイタイコト（レポートが訴えたいこと)

～シンプル、単純明快です！～

イイタイコト①（レポートで訴えたいこと）

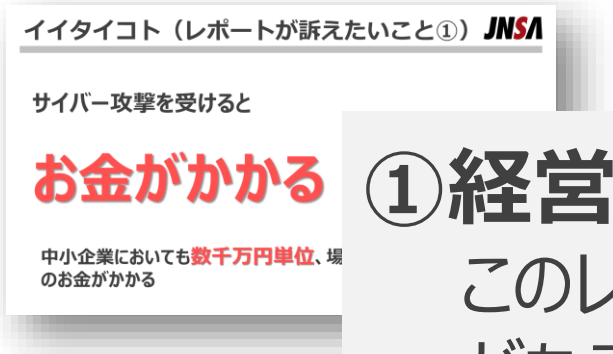
サイバー攻撃を受けると

お金がかかる

中小企業においても**数千万円**単位、場合によっては**億**単位のお金がかかる

「お金がかかる」って言いたいだけ？

イイタイコト②（レポートで訴えたいこと）



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**

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、情シスに説明してもらう**

イイタイコト③（レポートで訴えたいこと）

住所/氏名等の個人情報漏えいは、個人に対する慰謝料等で**損害賠償金が大変**なことになるんです！

サイバー攻撃を受けた場合、**被害（対応やそのコスト）はよくわからない**ですけどw、中小企業でも数千万の被害が発生するらしいですよ！

このレポートで（理解、引用等で）

具体的、リアル

なハナシを！

ということで
「レポート」を
みていただければ
幸いです…。

ここからは、
レポートの解説、
レポートをみるにあたってのポイント
をお伝えします

第２版の解説

～パワーアップしました…～

構成

前回（2021年8月）

今回（2024年2月）

本紙を見直しつつ、別紙作りました～

「別紙」が肝なんですけど、まずは、

「本紙」の説明します。

本紙の改定ポイント①　～概要～

◇**エグゼクティブサマリー**を追加

◇**既存コンテンツの見直し**

・金額などの数値データの最新化

・ヒアリング対象（対応のアウトソーシング先）の拡充

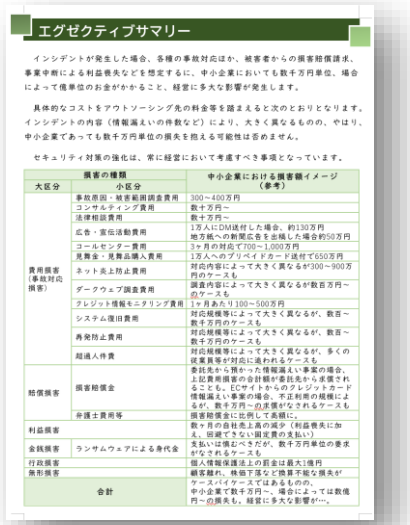
・その他直近動向を踏まえた内容

◇**以下のコンテンツ**を追加

・メンバーほか有志による**コラム**（６本）

・セキュリティ関係者による**座談会**（３本）

本紙の改定ポイント②　～エグゼクティブサマリー～


エグゼクティブサマリー

インシデントが発生した場合、各種の事故対応ほか、被害者からの損害賠償請求、事業中断による利益喪失などを想定するに、中小企業においても数千万円単位、場合によって億単位のお金がかかること、経営に多大な影響が発生します。

具体的なコストをアウトソーシング先の料金等を踏まえると次のとおりとなります。インシデントの内容（情報漏えいの件数など）により、大きく異なるものの、やはり、中小企業であっても数千万円単位の損失を抱える可能性は否めません。

セキュリティ対策の強化は、常に経営において考慮すべき事項となっています。

損害の種類		中小企業における損害額イメージ（参考）
大区分	小区分	
費用損害（事故対応損害）	事故原因・被害範囲調査費用	300～400万円
	コンサルティング費用	数十万円～
	法律相談費用	数十万円～
	広告・宣伝活動費用	1万人にDM送付した場合、約130万円 地方紙への新聞広告を出稿した場合約50万円
	コールセンター費用	3ヶ月の対応で700～1,000万円
	見舞金・見舞品購入費用	1万人へのプリペイドカード送付で650万円
	ネット炎上防止費用	対応内容によって大きく異なるが300～900万円のケースも
	ダークウェブ調査費用	調査内容によって大きく異なるが数百万円～のケースも
	クレジット情報モニタリング費用	1ヶ月あたり100～500万円
	システム復旧費用	対応規模等によって大きく異なるが、数百～数千万円のケースも
	再発防止費用	対応規模等によって大きく異なるが、数百～数千万円のケースも
	超過人件費	対応規模等によって大きく異なるが、多くの従業員等が対応に追われるケースも
賠償損害	損害賠償金	委託先から預かった情報漏えい事案の場合、上記費用損害の合計額が委託先から求償されることも。ECサイトからのクレジットカード情報漏えい事案の場合、不正利用の規模によるが、数千万円～の求償がなされるケースも
	弁護士費用等	損害賠償金に比例して高額に。
利益損害		数ヶ月の自社売上高の減少（利益喪失に加え、回避できない固定費の支払い）
金銭損害	ランサムウェアによる身代金	支払いは慎むべきだが、数千万円単位の要求がなされるケースも
行政損害		個人情報保護法上の罰金は最大1億円
無形損害		顧客離れ、株価下落など換算不能な損失がケースバイケースではあるものの、中小企業で数千万円～、場合によっては数億円～の損失も。経営に多大な影響が…。
合計		

損害の種類		中小企業における損害額イメージ（参考）
大区分	小区分	
費用損害	事故原因・被害範囲調査費用	300～400万円
	コンサルティング費用	数十万円～
	法律相談費用	数十万円～
	広告・宣伝活動費用	1万人にDM送付した場合、約130万円 地方紙への新聞広告を出稿した場合約50万円
	コールセンター費用	3ヶ月の対応で700～1,000万円
	見舞金・見舞品購入費用	1万人へのプリペイドカード送付で650万円
	ネット炎上防止費用	対応内容によって大きく異なるが300～900万
	省　略	
合計		ケースバイケースではあるものの、 中小企業で数千万円～、場合によっては数億円～の損失も。経営に多大な影響が…。

レポート上の各種損害を列挙し、具体的コスト、つまり、
お金がかかることを1ページでシンプルに表現

本紙の改定ポイント③　～既存コンテンツの見直し～

例えば、インシデントレスポンス業者・フォレンジックベンダへのヒアリング結果

前回（2021年8月）

会社	標準的なコスト		過去経験した高額事例のコスト
	初動対応	フォレンジック調査	
A社	150万円	PC：150万円/台 サーバー：200万円/台	—
B社	20万円	PC：120万円/台 サーバー：150万円/台	2,000万円超
C社	80万円	PC：100万円/台 サーバー：150万円/台	1,500万円超
D社	６万円/時間（実稼働時間でコストを計算）。数十時間程度は必要		—
E社	PC：220万円/台 報告会などは別料金		—
F社	最低300万円～		—

図表Ⅲ-１-１　事故原因・被害範囲調査費用

ぶっちゃけ、しょぼい･･･

今回（2024年2月）

会社	初動対応	フォレンジック費用（PC/サーバー）	ファスト・フォレンジック	過去経験した高額事例
A社	100万円	PC：180万円/台 サーバー：200万円/台	—	1,500万円
B社	個別見積にて対応	PC：150万円/台 サーバー：250万円/台	300万円 ～5,000台まで	4,000万円超
C社	90万円/台	PC：150～180万円/台 サーバー：200万円/台	350万円 ～50台まで	3,000万円
D社	別途契約	PC/サーバー： 600万円～/1週間	—	1,000万円
E社	200万円/1週間	PC/サーバー： 初動対応費用で対応	初動対応費用で対応	-
F社	10万円/台	PC/サーバー： 100万円/台	—	5,000万円
G社	300万円～	PC/サーバー： 200～300万円/台	60万円/台	約5億円
H社	300～500万円/5営業日	PC/サーバー： 初動対応費用で対応（1～2台）	初動対応費用で対応 10台まで	数千万円
I社	15,000円～/時間	PC/サーバー： 15,000円～/時間	15,000円～/時間	3,000万円超
J社	100万円	PC：150万円/台 サーバー：300万円/台	個別見積にて対応	1,000万円超
K社	100万円～	PC/サーバー： 300万円～/台	900万円～	8,000万円
L社	144万円	PC/サーバー： 120～180万円/台	2,125,000円 ～100台まで	2,000万円超
M社	-	PC：150万円/台 サーバー：200万円/台	個別見積にて対応	2,000万円超
N社	お客様でご対応	PC：100万円～ サーバー：200万円～	500万 ～50台まで	1,500万超
O社	100万円/5営業日	PC/サーバー： 300万円程度	3万円/台	1,700万円
P社	150万円	PC：72万円/台 サーバー：120万円/台	100台程度：6万円/台 1,000台以上：3万円/台	2,500万円超

図表Ⅲ-１-１　事故原因・被害範囲調査費用

◇たくさん聞けました！

◇標準的な価格は、特段変化なく
概ね300～400万円

◇**各社**が**経験**した**高額事例**は**注目**
調査費用だけで
数千万、億のケースも･･･

本紙の改定ポイント④　～コラム～

メンバーほか有志の方にコラムを書いてもらいました

コラム①CSIRT担当が思うこと
～CSIRTにおける迅速なインシデント対応のポイント～

コラム②ランサムウェア被害によって倒産してしまった中小企業のハナシ
～インシデント対応の現場から その1～

コラム③リスクコミュニケーションの重要性
～インシデント対応の現場から その2～

コラム④インシデント報告会について思うこと
～犯人捜しはやめましょう～

コラム⑤再発防止策の現場
～「推進サイド」と「現場サイド」の葛藤～

コラム⑥サイバー保険
～IT・セキュリティ業界の方に知っておいて欲しい、サイバー保険（というか損害保険）のハナシ～

サイバー攻撃による倒産事例！

今回、被害組織の調査（後述）でも、その後の存在が確認できない組織が複数アリ。

サイバー攻撃は倒産可能性も！

本紙の改定ポイント⑤　～座談会～

セキュリティ関係者で座談会（いずれも4名＋司会）を開きました

座談会①「インシデントレスポンス事業者編」

けっこう突っ込んだ内容…。今回のキラーコンテンツ笑
「ランサムウェアの復号可能！」を喧伝する業者のハナシなど…
インシデントレスポンス事業者の選択は十分精査が必要！

座談会②「マスコミ編」

マスコミ、セキュリティ業界、ユーザーそれぞれにおける
各種情報発信の在り方…。
セキュリティ業界としても発信の在り方は考えていくべき…

座談会③「弁護士編」

ここからは今回の肝・・・

「別紙」の説明します。

別紙の内容

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

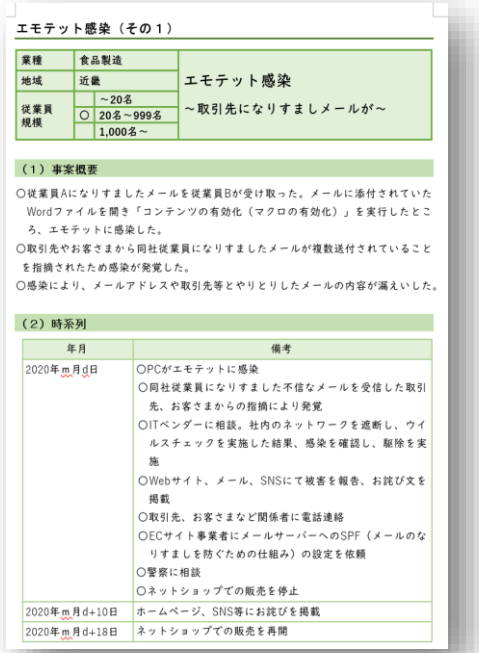
上記①の約1,300組織に対してアンケートを実施
回答を得られた組織について**被害額等を集計**

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**

とりあえず、わかりやすいところで
順番は逆に、レポート掲載の
「③被害企業インタビュー」
の説明します。

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

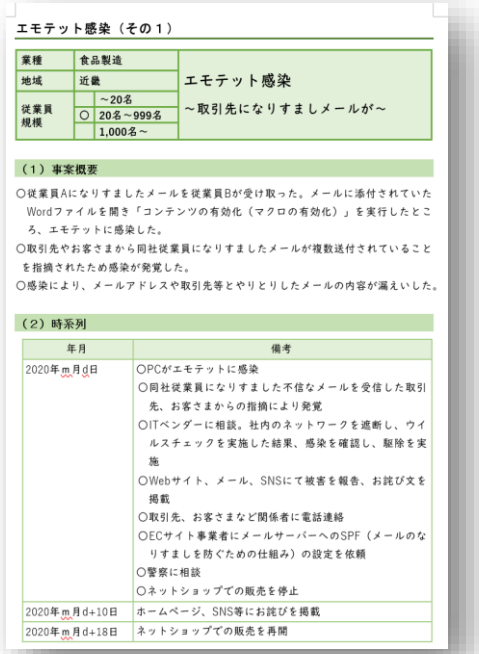
■事案概要

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

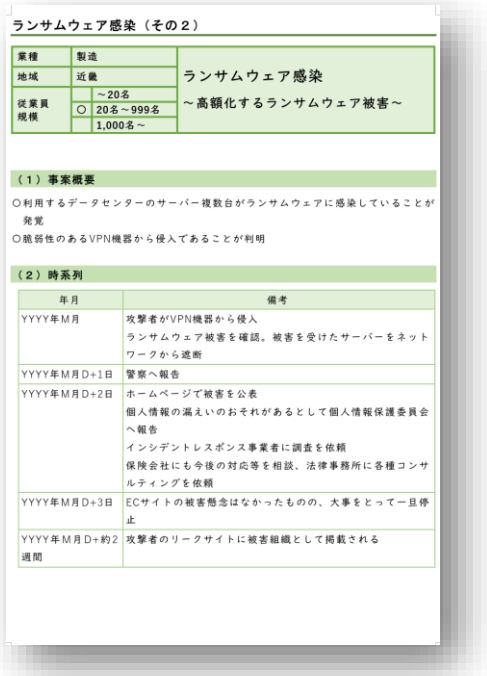
1,800万円（人件費込み）

■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」

ことがわかりますよね・・・

「お金がかかる」がわかったところで

「②アンケート調査」

を説明します。

10月の速報版を軽くまとめてみました

ランサムウェア感染組織の被害金額

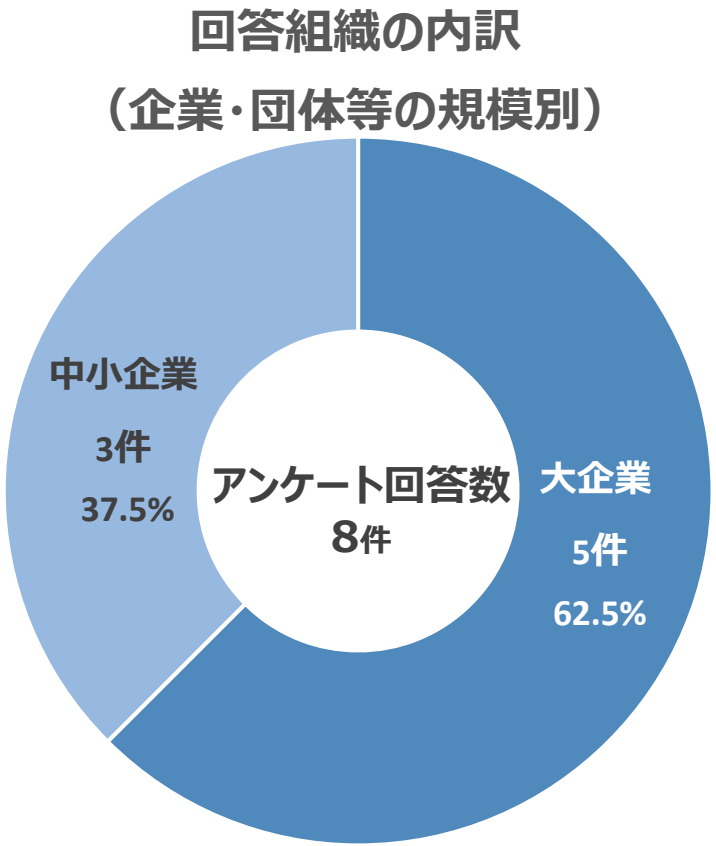
◇平均被害金額：**2,386万円**

◇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

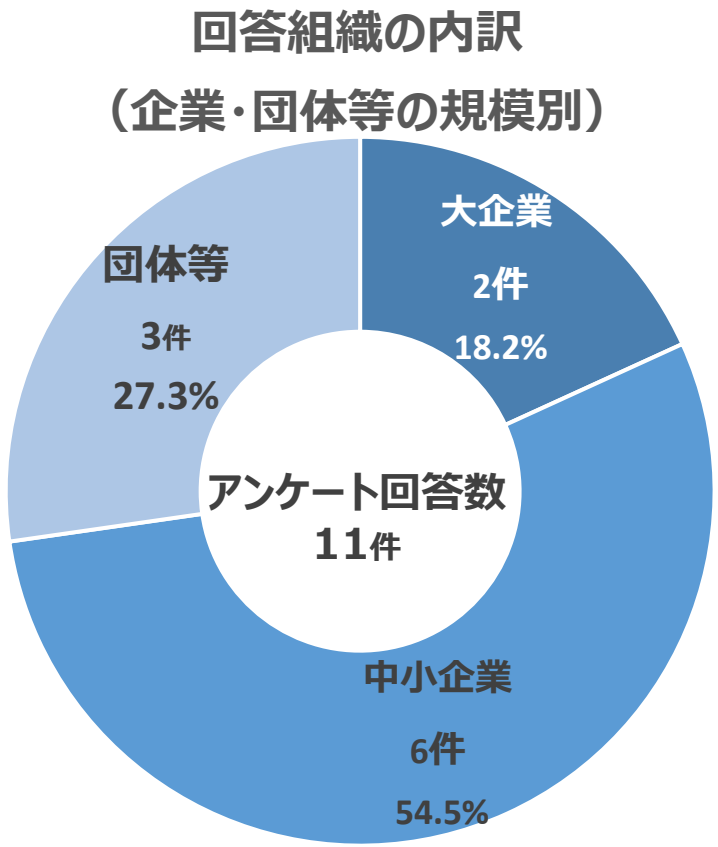


エモテット感染組織の被害金額

◇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

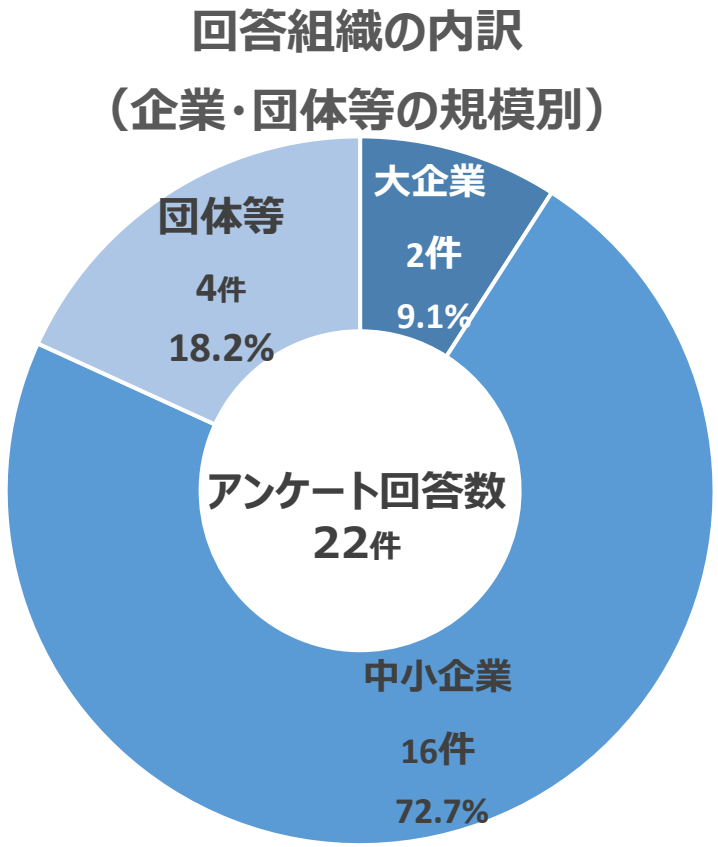
◇対応に要した組織の内部工数平均

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。。。

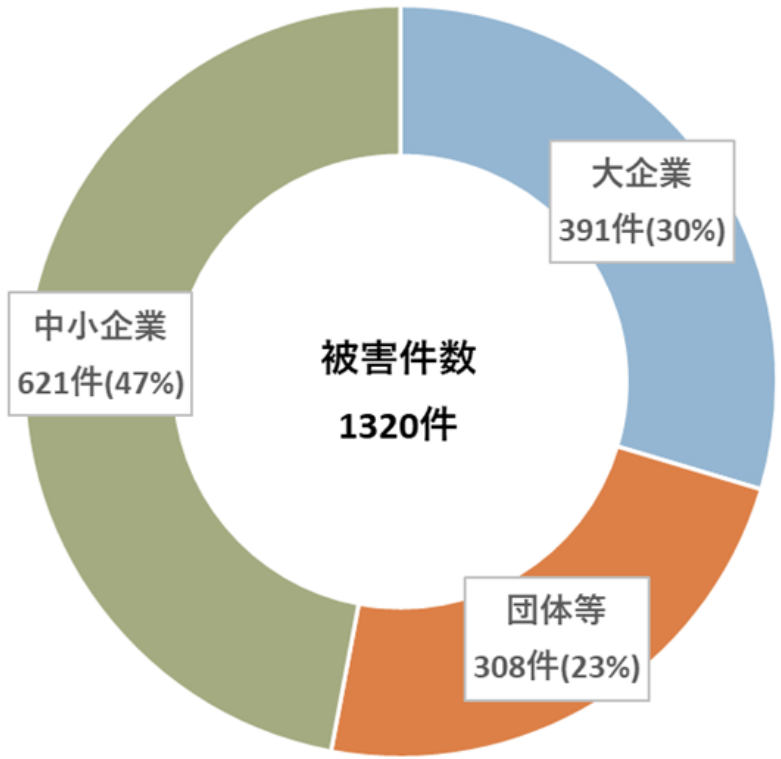
３つめ（おまけ）

「①被害組織調査」

の説明します。

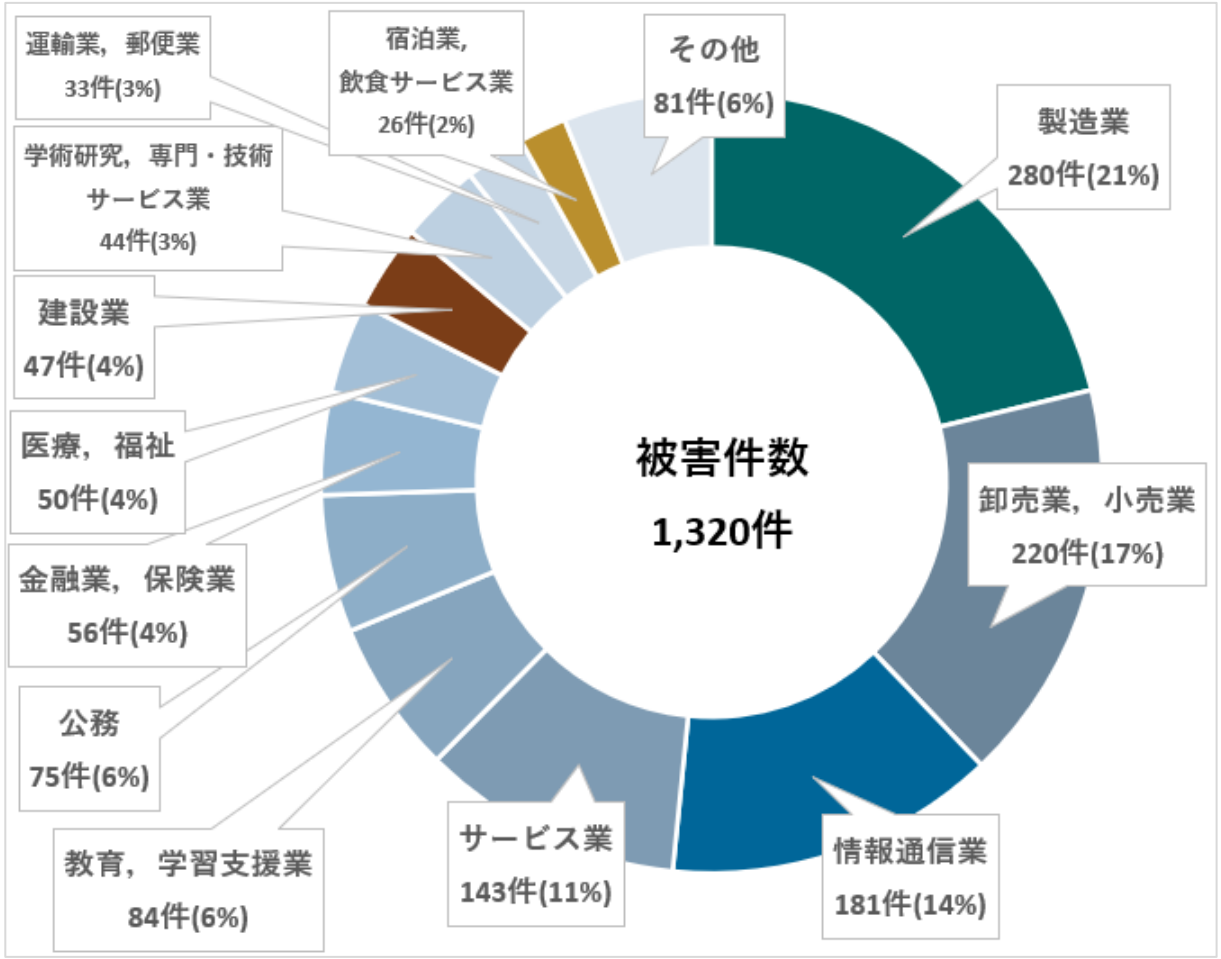
～約1,300組織の被害からみえてくること～

全体　～企業規模～



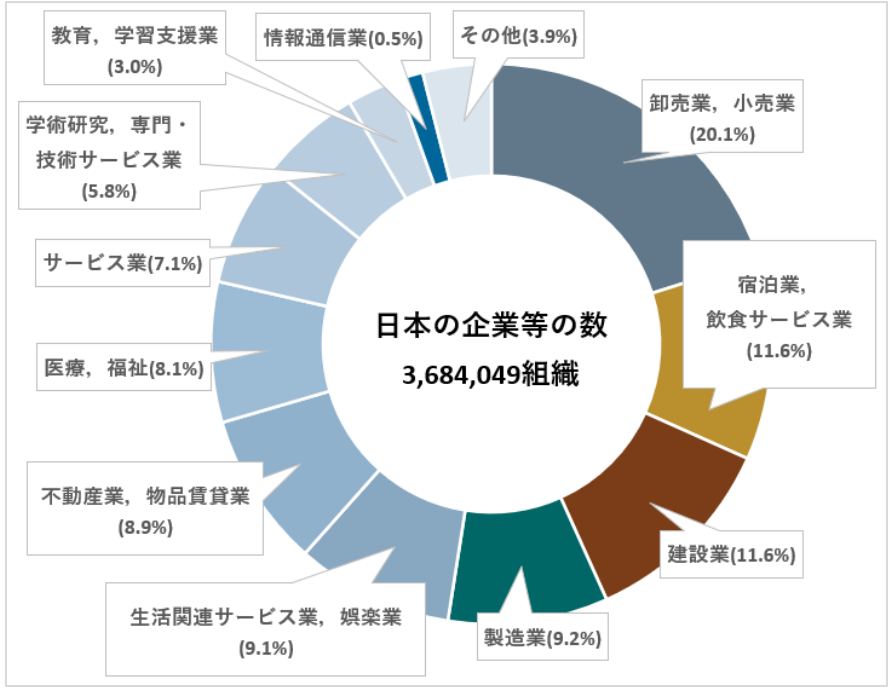
大企業だけではない

全体　～業種～

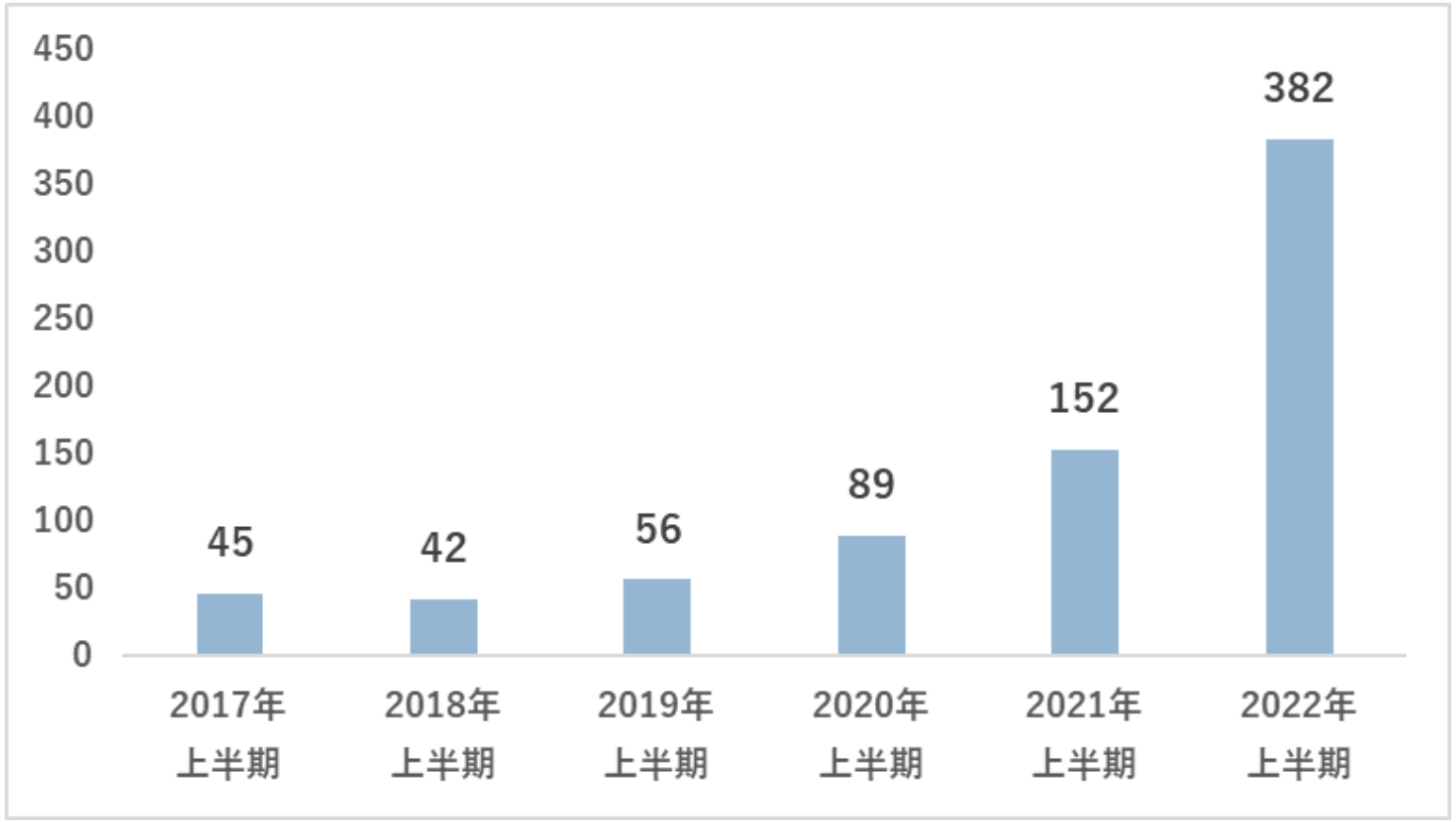


製造業、情報通信業が多い

参考（令和3年経済センサス）

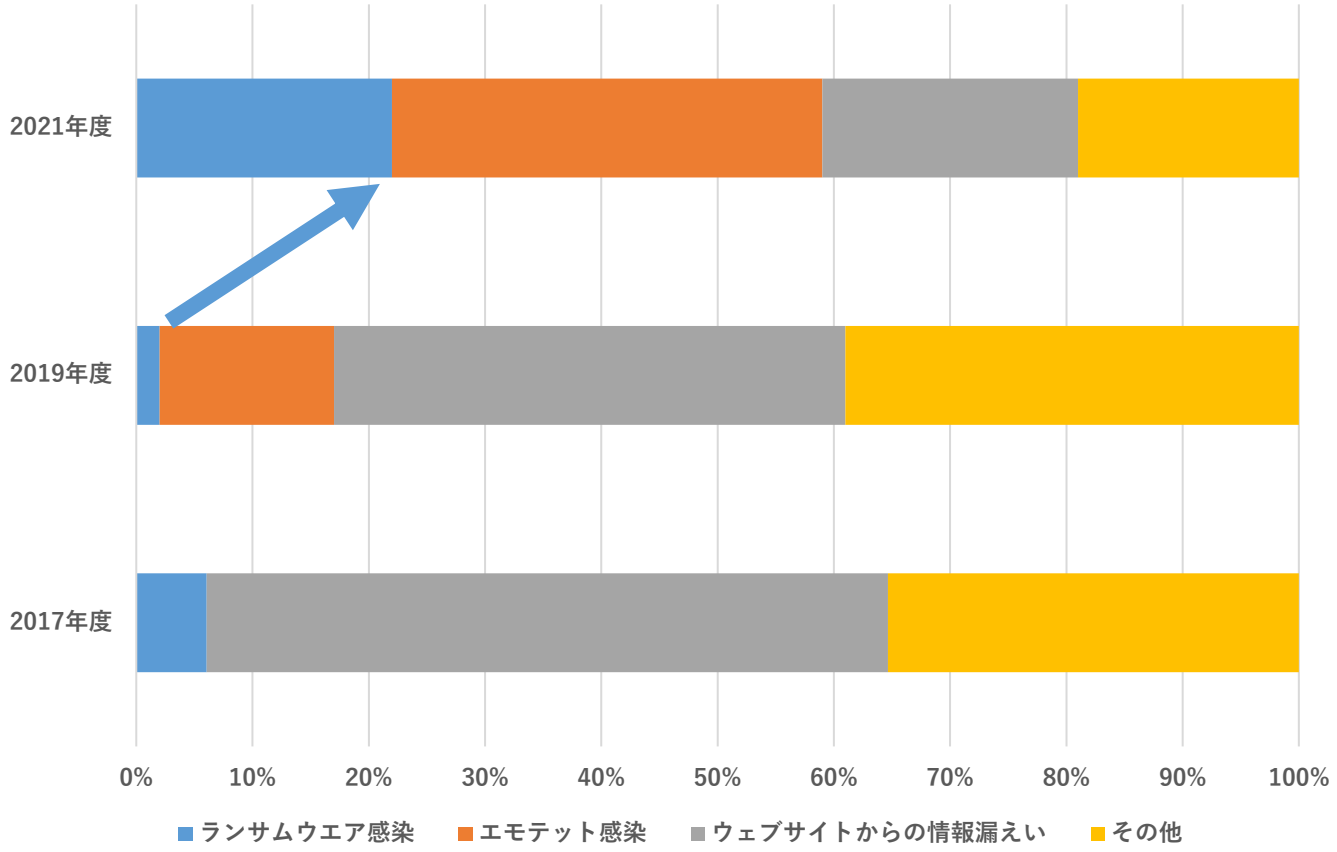


全体　～公表件数年別推移～



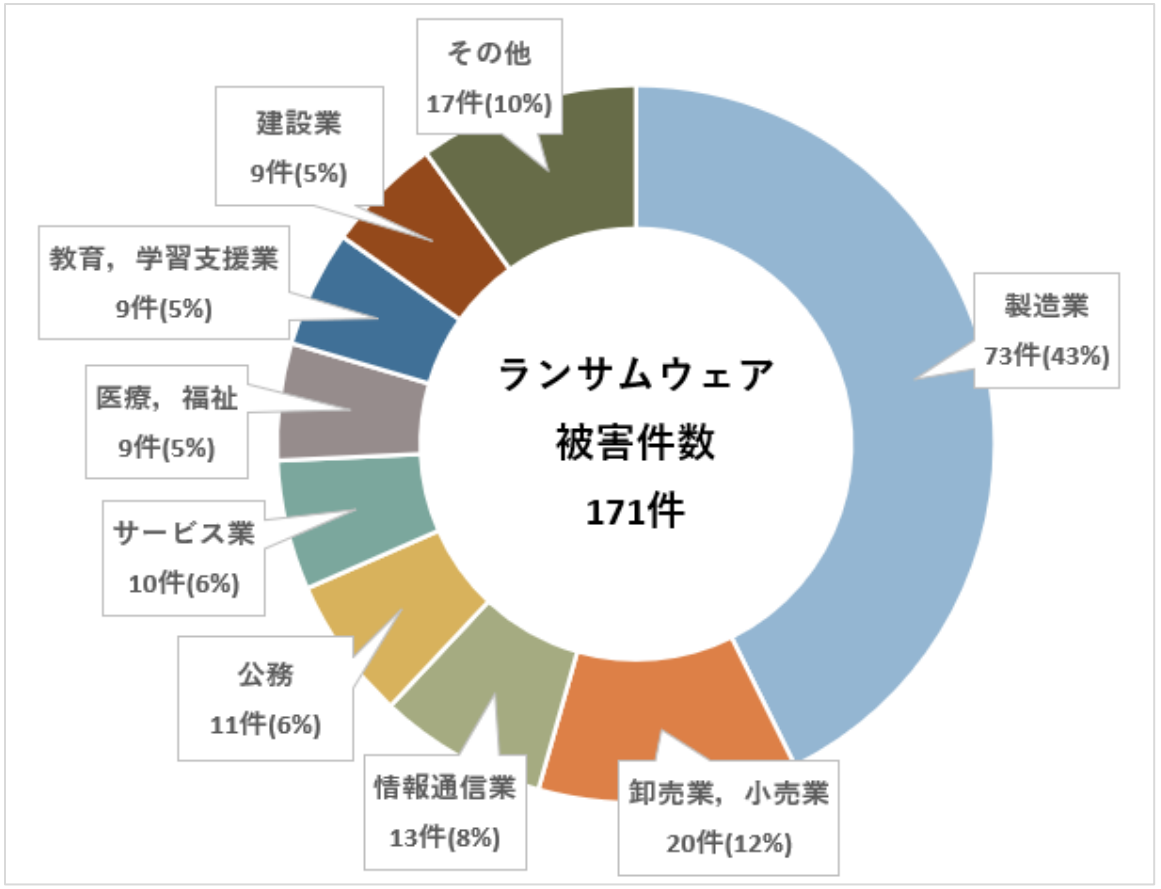
着実に年々、増えている

全体　～インシデント種別の年別推移～



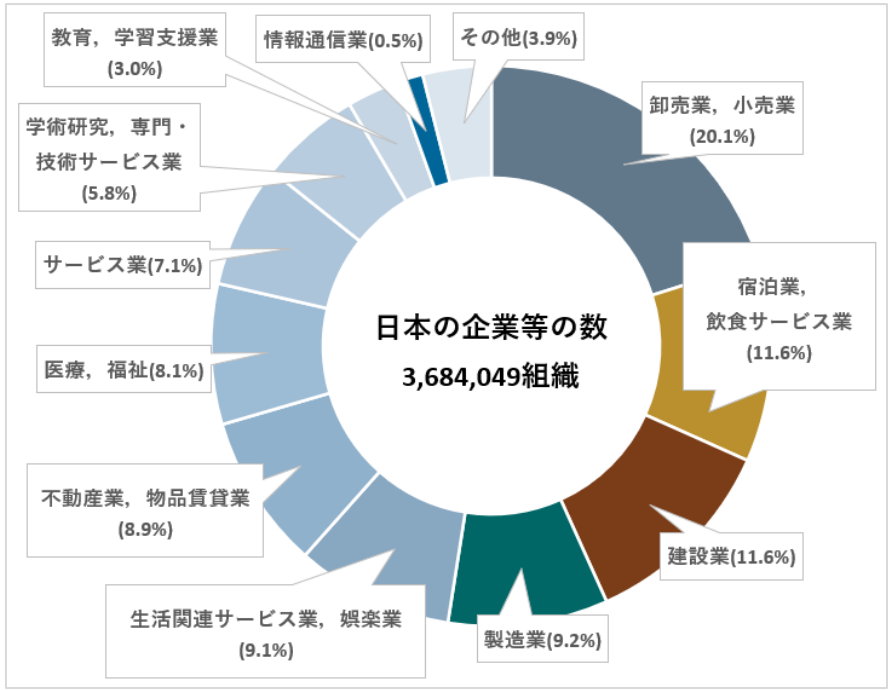
やっぱ、
ランサム・・

ランサムウェア　～業種～

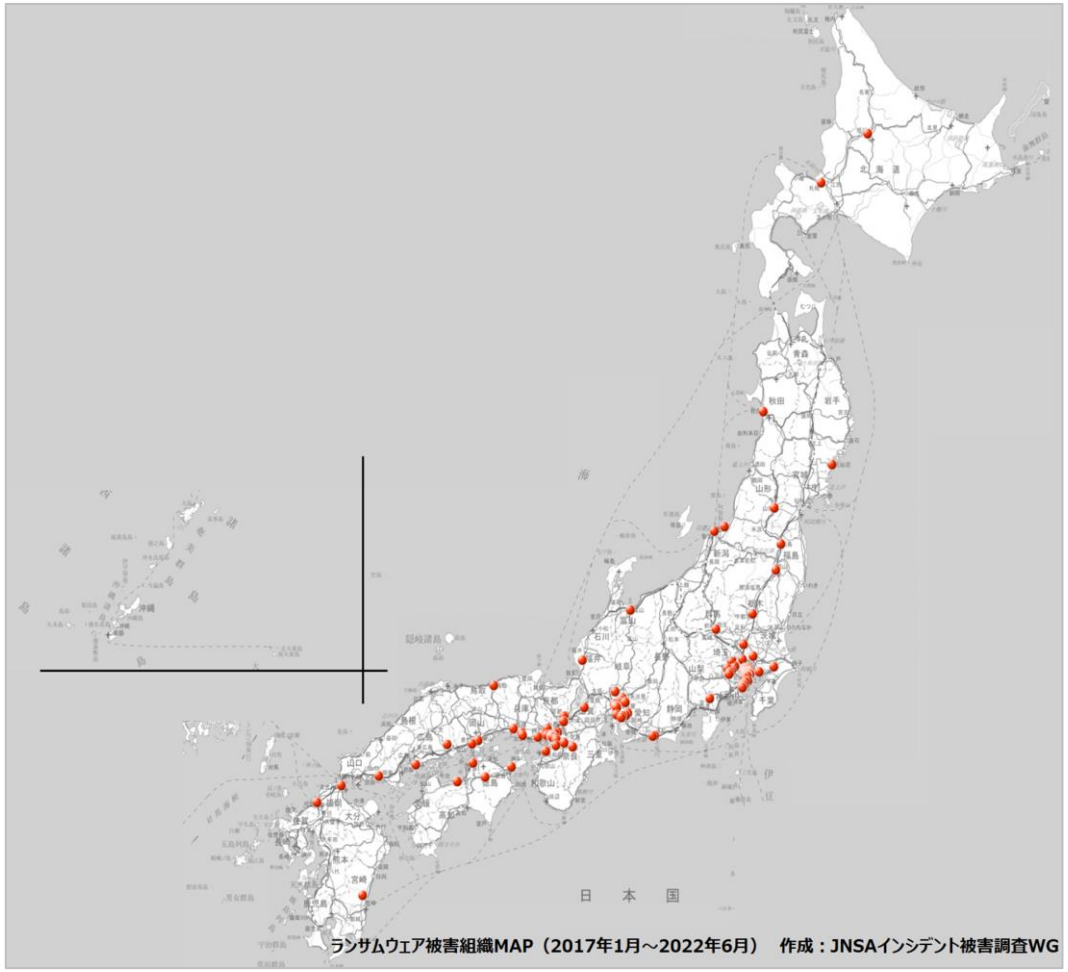


間違いなく、
製造業が多い

参考（令和3年経済センサス）



ランサムウェア　～所在地分布～



地域は関係ない
（当然…）

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く必要がある

「ぜひ、レポートもご一読いただき、
ご活用いただけましたら幸いです」
（と、セキュリティ業界の方にイイタイです）