日本のサイバーセキュリティを「連携」「学び」「創造」

サイバー攻撃被害組織のアンケート調査（速報版）について

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

Version 1.01

はじめに

そもそものところで、ご紹介

「インシデント損害額調査レポート 2021」

◇インシデントが発生した際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**？
- **いくらくらいのコストがかかるか**？　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！！！**

予告およびこの資料

「インシデント損害額調査レポート 第2版」

◇前回に引き続き、インシデントが発生した際の以下をまとめた資料（**2023年内の公開予定**）

- **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**？
- **いくらくらいのコストがかかるか**？　など

◇前回は、アウトソーシング先へのヒアリングがベース
今回は**加えて、被害組織へのアンケートを実施**

◇その結果を**「サイバー攻撃被害組織のアンケート調査」**として「インシデント損害額調査レポート 第2版」の別紙にて公表予定（この資料はその速報版）

被害組織調査の結果

被害組織の調べ方①

次のようなソースからサイバー攻撃（注）の国内被害組織をピックアップ

（注）コンピュータ、ネットワーク等に対する不正アクセス、マルウェア送付等であって、従業員の持出し、誤送信・誤発送、PCや鞄などの盗難・紛失などは除く

①次のサイト（運営者の方、ありがとうございます）

Security NEXT　ScanNetSecurity　Cyber Security.com

②企業等の公表ページ

次のような語での検索

③セキュリティ関係のサイト、ブログ等

リークサイト（注）をウォッチしている国内外ブログ等の確認

（注）ランサムウェアの攻撃グループが設置した、窃取した情報を晒すサイト

被害組織の調べ方②

◇前頁のソースに基づき、法人名、ホームページのURL、所在地、代表者名等をメンバーが国内被害組織のホームページを確認

◇**2017年1月から2022年6月までの5年半**の被害組織（約1,300組織）をリスト化

NO	ソース		被害法人							
	公表日等	記事リンク	名称	法人NO	—	ホームページURL	郵便番号	都道府県	住所	代表者肩書	代表者名
1	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
2	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
3	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
4	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
5	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
6	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
7	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
9	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
11	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
12	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
13	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
14	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
15	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
16	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
17	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
18	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
19	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
20	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
21	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
22	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
23	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
24	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
25	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
26	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
27	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

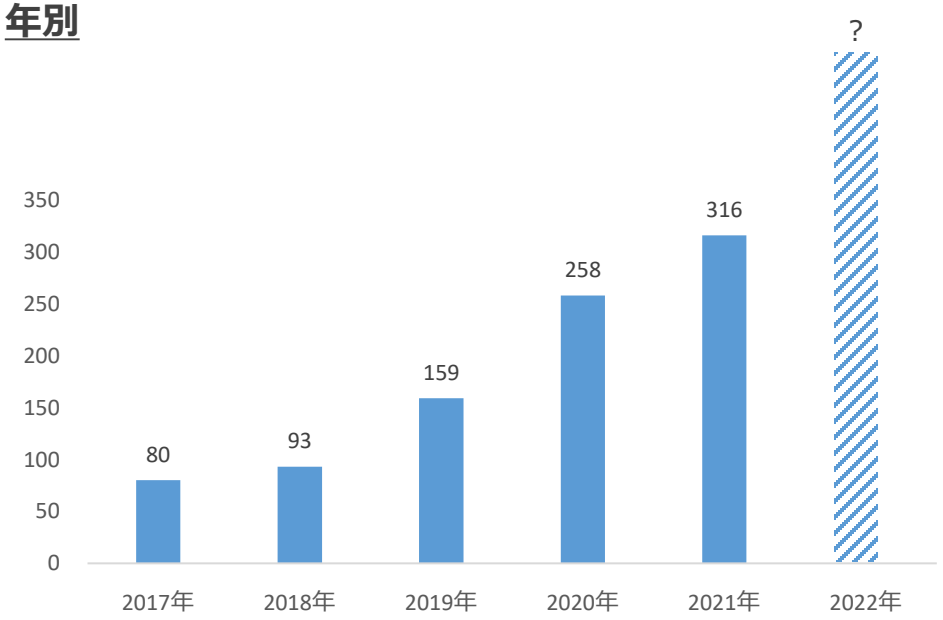
年別データ

◇リスト化した2017年1月から2022年6月までの5年半の国内被害組織（約1,300組織）の年別件数は次のとおり

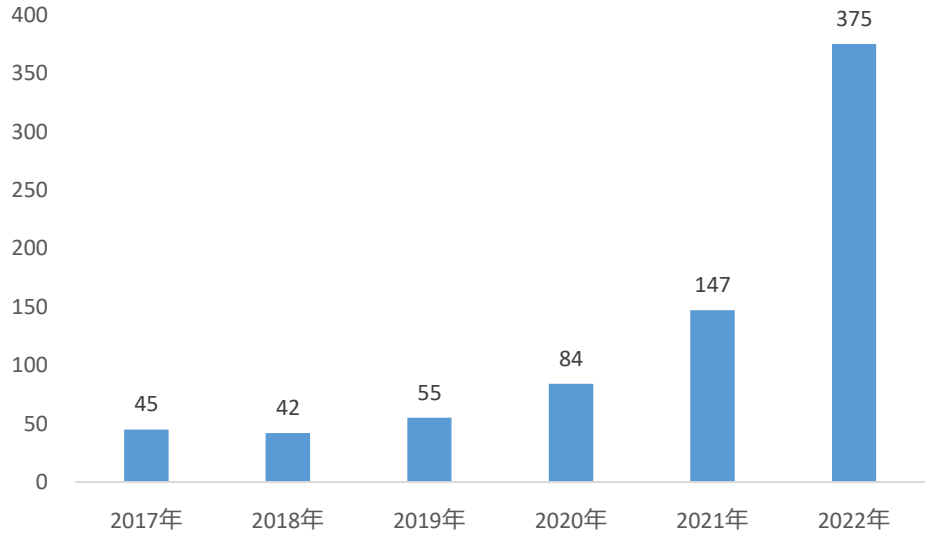
◇**報道・公表を実施する組織が年々増加していることは明白**

⇒サイバー攻撃の増加もさることながら、報道・公表等がなされるケースが増加していることが推測される

年別



上半期のみ



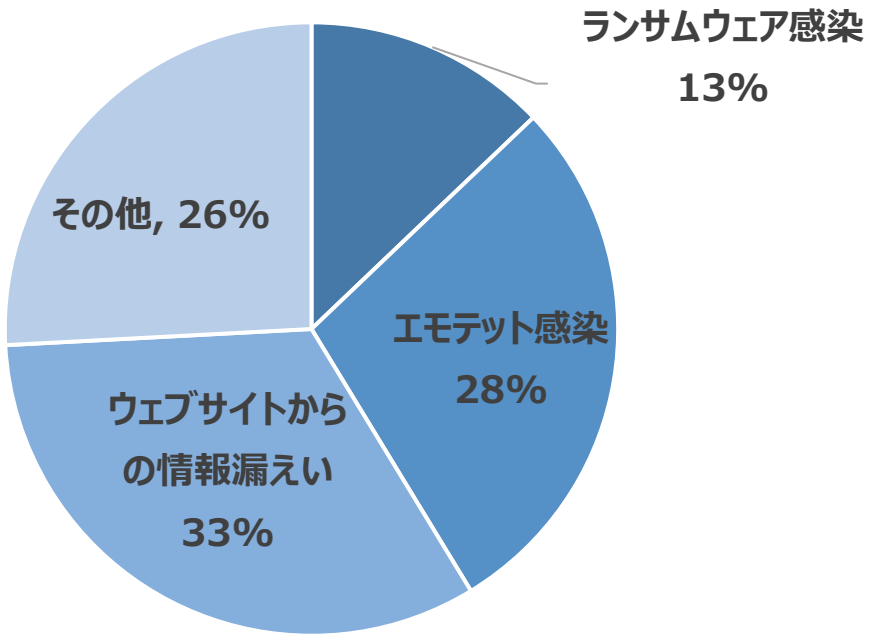
サイバー攻撃の種別構成①

◇リスト化した国内被害組織のサイバー攻撃の種別構成は次のとおり

◇「ランサムウェア感染」「エモテット感染」
「ウェブサイトからの情報漏えい」が**7割**を占める

⇒これら３つの事象が多いということではなく、取引先・顧客への影響の大きさ等から、報道・公表がなされることが多いということが推測される

その他の内容
- DDoS攻撃
- メールやSNS等のアカウントの乗っ取り
- 情報漏えいを伴わないウェブサイトの改ざん
- ランサムウェア、エモテット以外のマルウェア感染　など

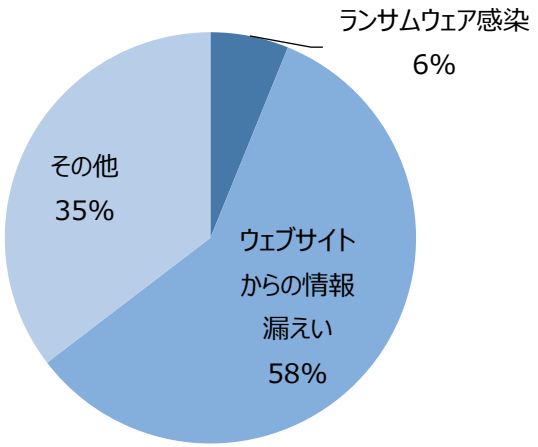


サイバー攻撃の種別構成②（年度別傾向）

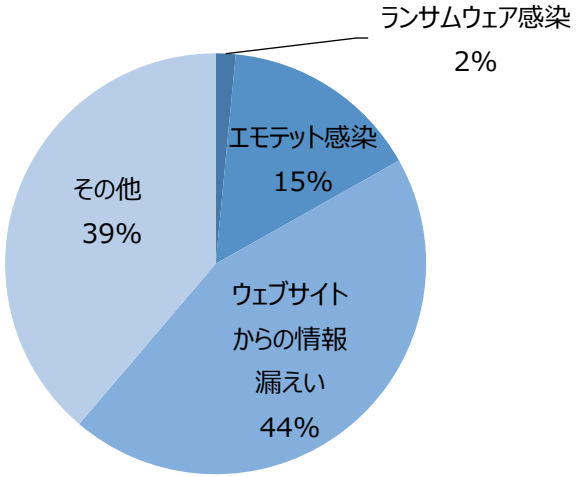
◇2017年度⇒2019年度⇒2021年度別の傾向は次のとおり

◇被害件数の増加ほか、その種別構成も変容している
　特に「**ランサムウェア感染**」「エモテット感染」が拡大している

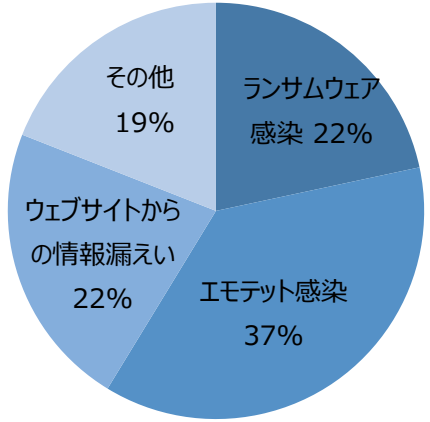
⇒ランサムウェアの被害の拡大は特筆すべきものがあり、警察庁のウェブサイトで公開されている「サイバー空間をめぐる脅威の情勢等」の結果と同様の傾向を示すところである



2017年4月～2018年3月
（約70件）



2019年4月～2020年3月
（約200件）



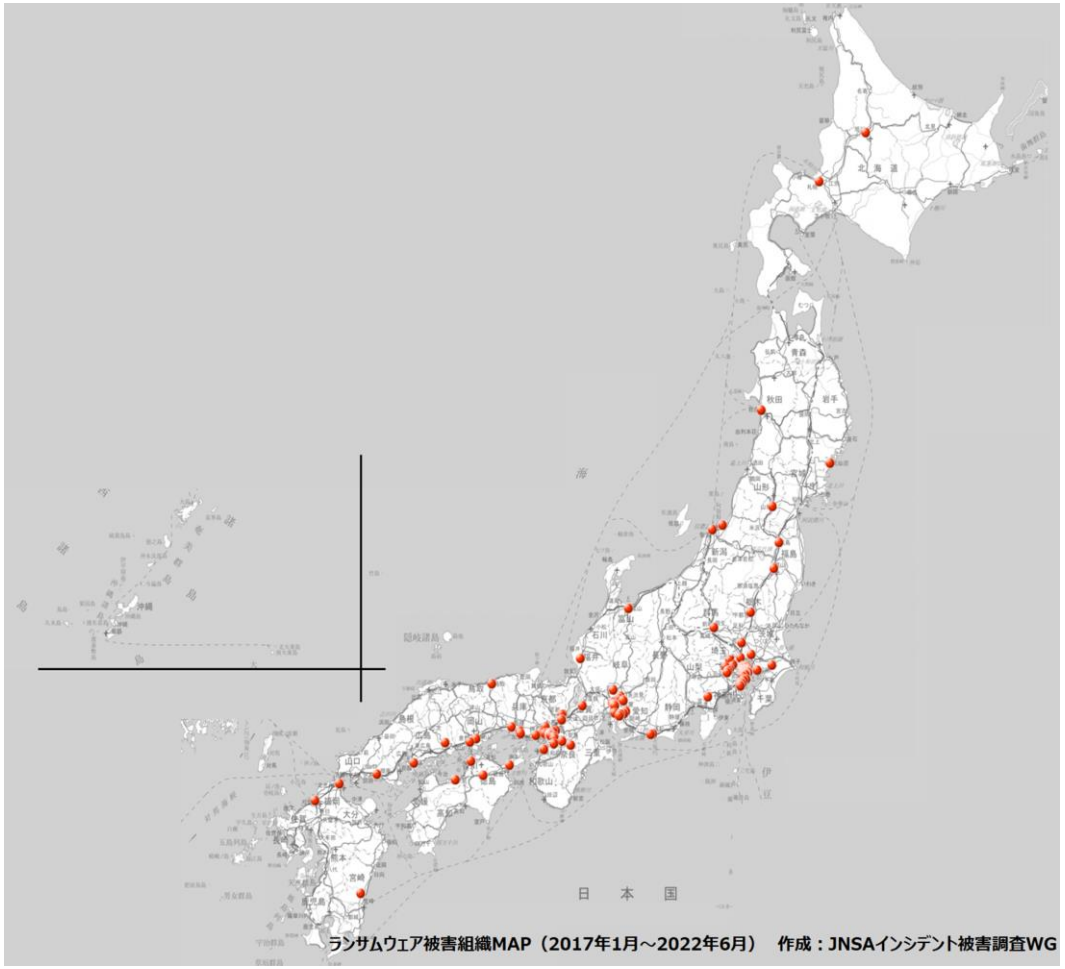
2021年4月～2022年3月
（約500件）

ランサムウェア感染被害

◇ランサムウェア感染による国内被害組織（約170組織）をマッピングした結果は次のとおり

◇**日本全国で被害が発生**していることがわかる

◇インターネットの世界において、海外の攻撃者が日本の特定の地域を狙うことは考えにくいことからも、今後も、日本全国で被害発生の可能性があるといえる



エモテット感染被害

◇エモテット感染による国内被害組織（約350組織）を
マッピングした結果は次のとおり

◇北は北海道、南は沖縄まで
日本全国で被害が発生している
ことがわかる

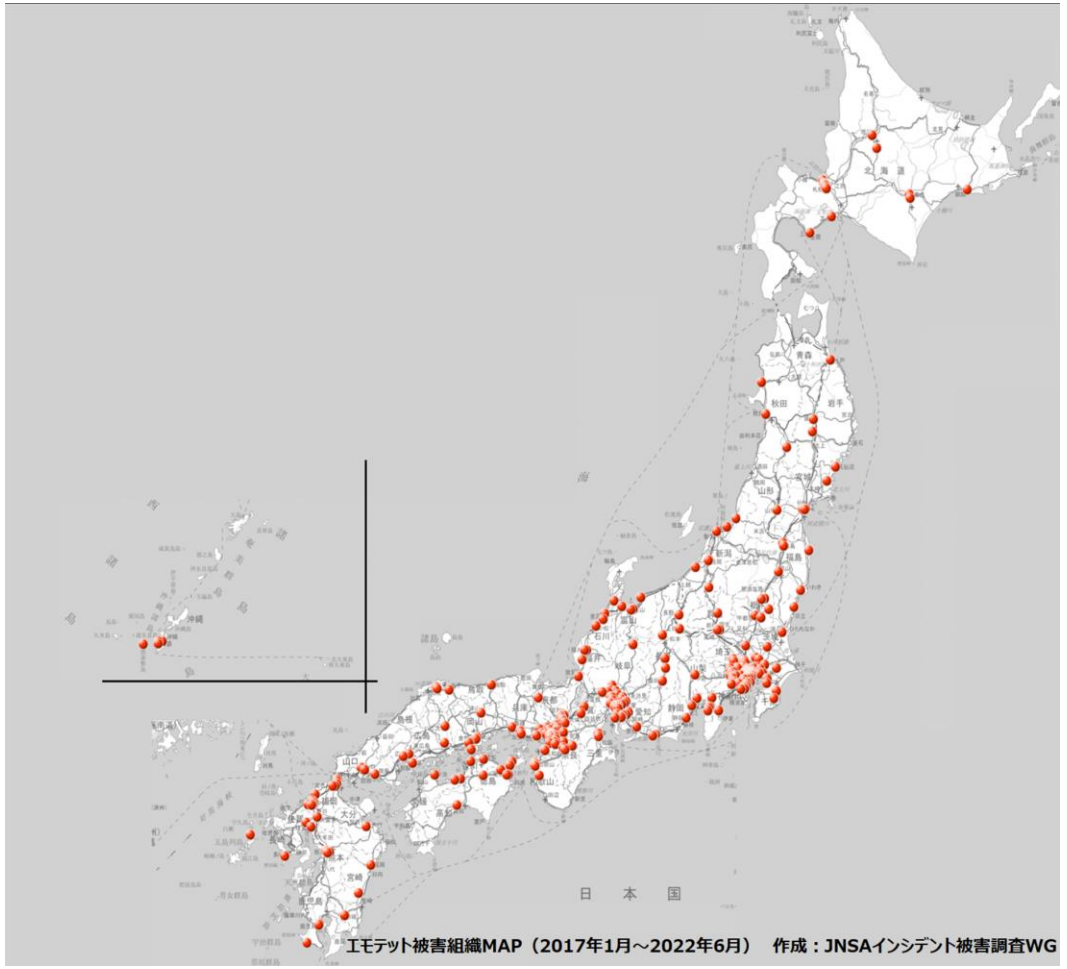
⇒マッピングの結果からは、企業数が多い都市部に集中しているようにみえるが、今回、本社所在地ベースでの集計であること、都道府県別の企業数（中小企業庁2016年統計）を分母とした被害組織の割合を鑑みるに、必ずしも都市部に集中しているものではないことを確認

https://www.chusho.meti.go.jp/koukai/chousa/chu_kigyocnt/index.htm

エモテット感染被害組織割合TOP10都道府県

東京都、和歌山県、京都府、鳥取県、徳島県、大阪府、愛知県、
岡山県、山口県、福井県

◇被害組織の大多数が中小企業



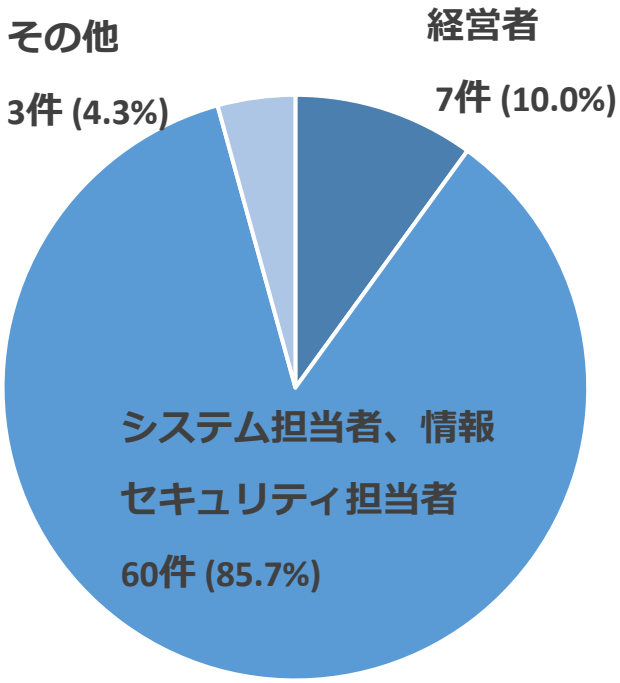
アンケート調査の結果

サイバー攻撃被害組織アンケート調査

リストアップした国内被害組織を対象に、
損害の実態に関するアンケートを実施

調査対象組織	2017年1月から2022年6月までの5年半の サイバー攻撃の国内被害組織 約1,300組織（※）
アンケート実施期間	2023 年7 月 24 日～ 9月30 日
アンケート形式	当WGからの依頼に基づくWebフォームでのご回答
アンケート結果	有効回答数：70件（回答率：約6%）

回答者の属性



（※）本調査データの収集は、作成メンバーによる手作業での実施。したがって、可能な限り多くの情報を収集するように努力しているものの、報道または公表内容等のすべてを収集できているものではありません

主なアンケート項目

- ■回答者の立場（職種）
- ■被害金額の合計
- ■被害金額の内訳
  - ・賠償損害
  - ・利益損害
  - ・金銭損害（詐欺・脅迫等による被害）
  - ・費用損害（各種事故対応の費用）
    - ・事故原因被害範囲調査費用
    - ・コンサルティング費用
    - ・法律相談費用
    - ・広告宣伝活動費用
    - ・コールセンター費用
    - ・見舞金見舞品購入費用
    - ・ダークウェブ調査費用
    - ・システム復旧費用
    - ・再発防止費用
  - ・行政損害（課徴金、罰金等）
- ■対応に要した組織の内部工数（人月ベース）
- ■ランサムウェア感染について
  - ・身代金を支払ったか
  - ・データ復旧できたか
  - ・誰にデータ復旧を依頼したか
- ■エモテット感染について
  - ・発覚経緯（自社発見、取引先指摘等）
- ■クレジットカード情報の漏えいについて
  - ・発覚経緯（自社発見、決済代行会社指摘等）
  - ・カード決済の停止期間
  - ・カード会社から不正利用の額について求償があったか
  - ・カード会社から公表時期に関して要請があったか

ランサムウェア感染組織の被害金額

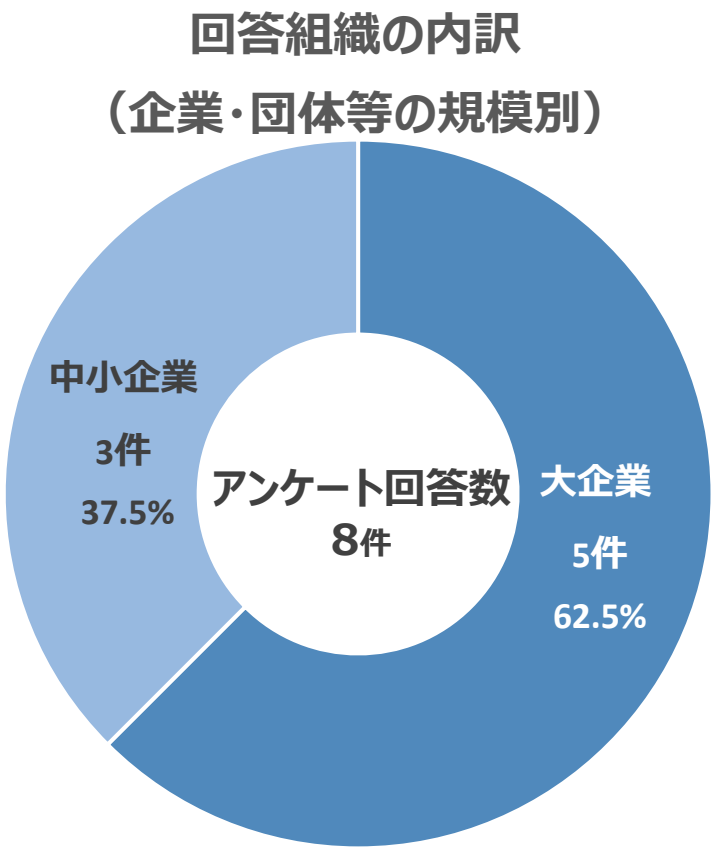
◇平均被害金額：**2,386万円**

◇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%**

⇒「復旧できた」という回答はすべて、バックアップデータからの復旧であり、バックアップデータを使わずに復旧（暗号データの復号）ができたという回答は見られなかった
⇒バックアップがされていなかった、またはバックアップデータも暗号化されたケースがあると推測される



◇システムの停止、データの消失による利益の喪失などによる損害額は非常に大きいと推測されるが、
被害組織の多くが機会損失の損害額は把握していない旨を回答

◇ほとんどの被害組織について、被害金額は1,000万円超となっており、
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**

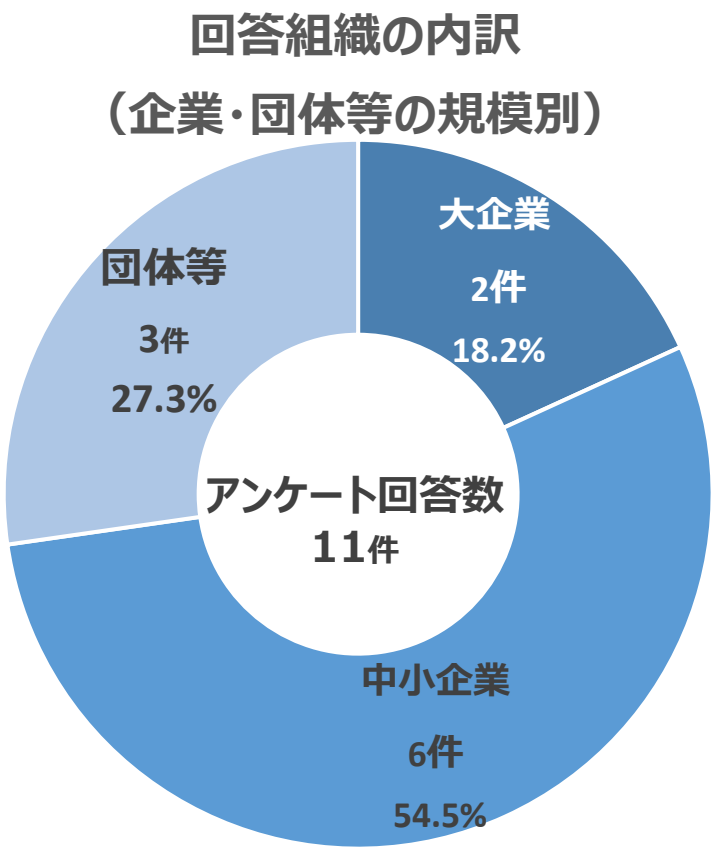
◇取引先・顧客からの連絡で感染が発覚した組織は約半数

自社で気づいた：6件　取引先・顧客からの連絡：5件

◇他のサイバー攻撃種別と比べ、中小企業からの回答が占める割合が大きい

◇被害金額のばらつきが大きい

⇒被害金額として2,000万円以上と回答した組織がある一方で、
被害金額が極端に低い組織（数10万円以下や対応工数のみなど）がある



◇事故原因調査や対外発表、再発防止策をしっかりと行った組織と、感染端末の再インストールのみを行った組織に分かれた結果と推測される

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

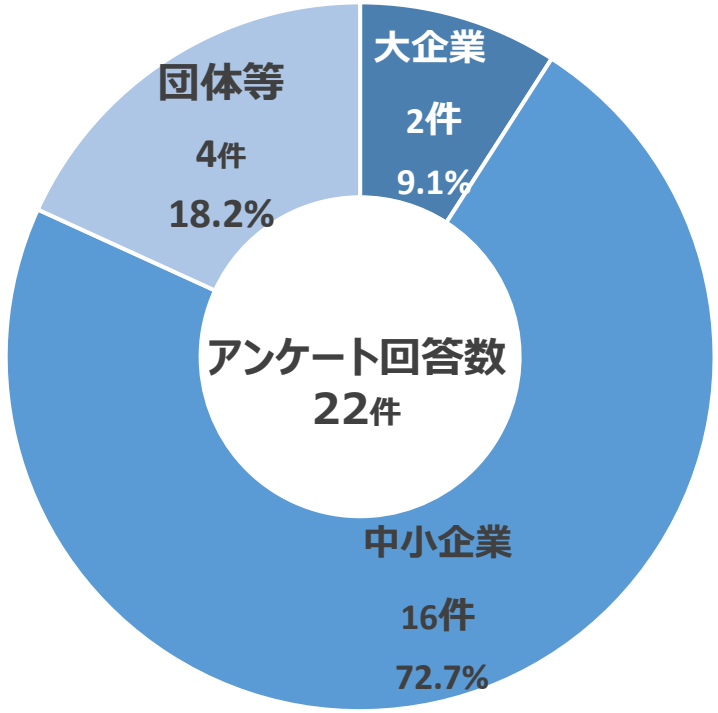
クレジットカード情報および個人情報の漏えい：**13.3人月**

個人情報のみの漏えい　　：**13.5人月**

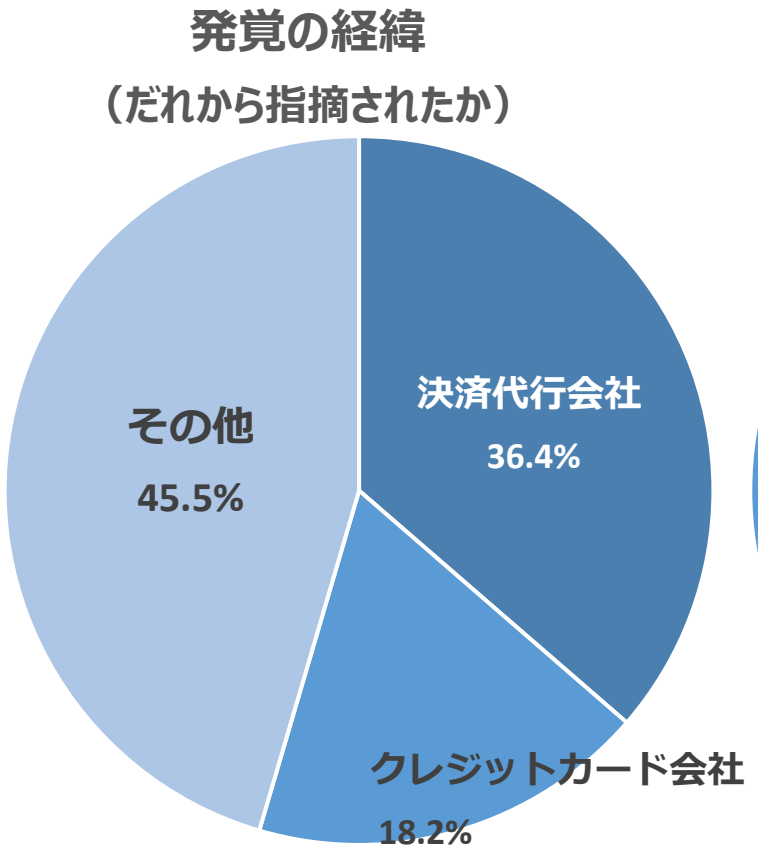
◇対応に要した内部工数は、クレジットカード情報の
漏えい有無にかかわらず、回答に大きな差異は見られなかったが
平均被害金額には大きな違いがみられた

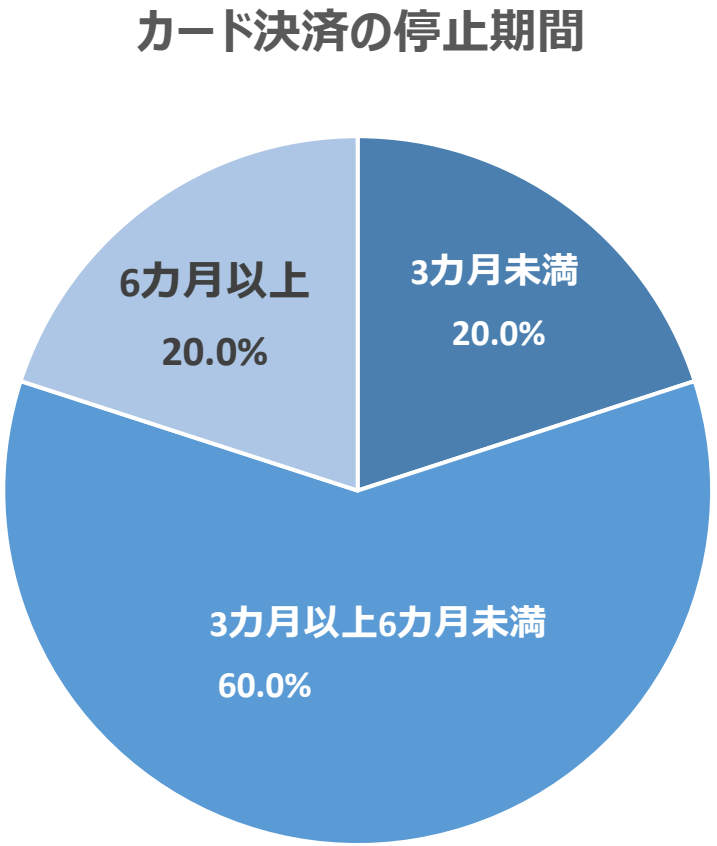
◇クレジットカード情報が漏えいした場合、
損害賠償額が大きくなる傾向があること、不正利用に対する
カード会社からの求償などが発生することが要因と推測される

回答組織の内訳
（企業・団体等の規模別）



参考：クレジットカード情報漏えいの影響





◇決済代行会社やクレジットカード会社からの指摘により情報漏えいが発覚したケースが多くみられた

◇ECサイトからクレジットカード情報の漏えいが発覚した場合、カード決済を停止せざるを得ない場合があり、機会損失による損害が大きくなる可能性がある

◇回答の中には、カード会社から即時公表の見送りを求められたという回答もみられた

⇒1ヵ月～2ヶ月程度の期間が多く問い合わせへの準備や、影響範囲の調査期間と推測される

総括

◇回答された平均被害額は「ウェブサイトからの情報漏えい」と「ランサムウェア感染被害」が他を引き離した結果となった

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
ウェブサイトからの情報漏えい（個人情報のみ）	2,955万円
その他のサイバー攻撃被害	473万円

◇ただし「ランサムウェア感染被害」による損害額はより大きなものになる可能性がある

- 被害組織の多くが、被害の影響による機会損失の損害額を算出できていない
- 対応に要する内部工数が高い傾向にある

◇今回の調査から、**中小企業であっても被害額が数千万円~に及ぶケースを考慮すべきといえる**

さいごに

さいごに

◇2023年内に「インシデント損害額調査レポート 第2版」を公表予定

◇前回レポートを踏襲しつつインシデントレスポンス事業者等アウトソーシング先へのヒアリングを拡充

◇アンケート回答企業のうち、いくつかの組織に対してインシデントの概要（侵入経路、被害内容等）を追加でヒアリング予定

インシデント被害調査WGメンバー

■リーダー

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
サブリーダー	西浦　真一	キヤノンITソリューションズ株式会社

■メンバー（五十音順）

大谷　尚通	株式会社エヌ・ティ・ティ・データ
竹内　智子	株式会社クレスコ・デジタルテクノロジーズ
戸田　勝之	NTTデータ先端技術株式会社
西原　真仁	日本アイ・ビー・エム株式会社
本多　規克	アルプス システム インテグレーション株式会社
三国　貴正	株式会社YONA
山田　道洋	日本電気株式会社

■サポート

前田　典彦	株式会社FFRIセキュリティ　（JNSA調査研究部会 部会長）

サイバー攻撃被害組織のアンケート調査（速報版）

更新履歴

Version	日付	修正内容
1.00	2023/10/24	
1.01	2023/10/30	P7,8,14誤植修正、更新履歴を追加