インシデント損害額調査レポート

別紙「被害組織調査」第2版

IDIR Incident Damage Investigation Report

2025年7月

JNSA

インシデント被害調査WG

Version 1.00

目次

Ⅰ　はじめに

JNSA（NPO法人 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ワーキンググループは、2024年2月に別紙「被害組織調査」と題してサイバー攻撃によって生じた被害額等に関する実態調査を公開しましたが、今回、新たに、2022年7月から2024年6月までにサイバー攻撃に関する被害の公表または報道等がなされた国内の組織を対象に加えた調査を実施しました。

このレポートは、これらの調査によって、結果として、2017年1月から2024年6月までの7年半にわたる国内のサイバー攻撃の被害組織の統計情報と、調査結果をまとめたものとなります。

昨今、大企業、中小企業を問わず、サイバー攻撃による被害が後を絶ちません。これら被害を防ぐためには、セキュリティ対策の強化・向上が必要となりますが、自組織にとって適切なセキュリティレベルを検討するうえで必要な公知情報は十分ではありません。このことから、当ワーキンググループでは、その動機付けや検討のためにも、サイバー攻撃の具体的な被害情報（損失額等）を広く共有していくことが必要だと考えています。

本調査では、実際にサイバー攻撃被害に遭った組織について、組織の規模、業種、サイバー攻撃の種別ごとに集計した統計情報、アンケート調査によって判明したサイバー攻撃の被害組織が被った損害額、そしてアンケート調査に回答いただいた被害組織へのインタビューにより、被害の実態を明らかにしています。

Ⅱ　被害組織調査

１．調査の対象件数、期間、収集方法

（１）対象件数

サイバー攻撃に関する被害の公表または報道等約1,800件
下記「（３）収集方法」によって、当WGが手作業にて収集した件数であり、すべての公表事例等を網羅できているものではありません。

（２）対象期間

2017年1月から2024年6月までの7年半

（３）収集方法

情報の収集にあたっては次のような情報ソースを参照しています。

① セキュリティ情報サイト

定期的にインシデント情報を掲載している次の３つのセキュリティ情報サイト

Security NEXT（セキュリティネクスト）　https://www.security-next.com/

ScanNetSecurity（スキャンネットセキュリティ）　https://scan.netsecurity.ne.jp/

Cyber Security.com（サイバーセキュリティ.com）　https://cybersecurity-jp.com/

② 被害組織の公表ページ

サイバー攻撃による被害等を公表した組織のページ

③ セキュリティ関係のサイト、ブログ等

セキュリティベンダーやセキュリティ研究者が公開している国内外のサイト、ブログなど

２．調査対象としたサイバー攻撃種別

「インシデント（incident）」とはサイバー攻撃に限らず、システム、ネットワーク等の正常な運用・利用が阻害される事象・状態、不具合が生じる事象全般を指しますが、このレポートでは、調査対象を外部からのサイバー攻撃を受けた組織に限定しています。

具体的には、サイバー攻撃を次の4つに大別し集計しました。

（１）ランサムウェア感染

ランサムウェア（データを暗号化する等により身代金を要求するマルウェア）の感染被害です。集計に際しては、ランサムウェアによるデータの暗号化やそれにともなう業務停止に関する公表や報道のほか、ランサムウェアにおけるリークサイトを観測している、セキュリティベンダーやセキュリティ研究者の国内外のサイト、ブログなどの情報も参考としています。なお、データの暗号化はせずに窃取したデータ等に対して対価を要求する「ノーウェアランサム」と呼ばれる攻撃による被害も「ランサムウェア感染」として区分しています。

（２）ウェブサイトからの情報漏えい

ECサイトなどのウェブサイトを通じた情報漏えいの被害です。クレジットカード情報の漏えいを伴うケースと、個人情報のみが漏えいした等、クレジットカード情報の漏えいを伴わないケースでは、発生する二次被害の規模・影響等が大きく異なることも特長といえます。主に被害組織の公表情報（お詫び文）およびセキュリティ情報サイトが公開する情報を参照し、集計しています。

（３）エモテット（Emotet）感染

エモテット（2020年秋、2022年春に国内で多くの被害が発生したマルウェア。攻撃者からのなりすましメールに端を発し、添付ファイルを開封する等により感染、メールアドレス等を窃取します）の感染被害です。主に被害組織からの公表情報を参照し、集計しています。2023年以降は収束傾向にありますが、今後も第二のエモテットというべき新たなマルウェアの被害が懸念されるところです。

（４）その他

上記（１）～（３）に該当しない、情報漏えいを伴わないウェブサイトの改ざん、DDoS攻撃、メールアカウントやSNSアカウントの乗っ取りなどをその他とし

て集計しています。公表・報道等においては「不正アクセス」「サイバー攻撃」等の語を記載するに留め、実際はランサムウェア感染であるといった事例も推測されますが、これらは「その他」として区分しています。

３．集計結果

調査対象とした国内の約1,800事例について、規模、業種、本社所在地、公表件数の年別推移、サイバー攻撃種別等を集計、整理しました。また、サイバー攻撃種別ごとにも規模、業種等を集計、整理しました。

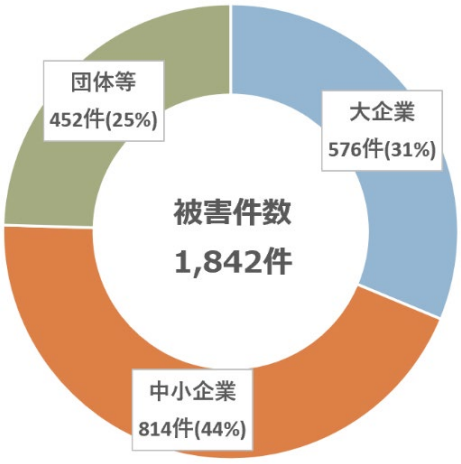
（１）全体のデータ

① 規模

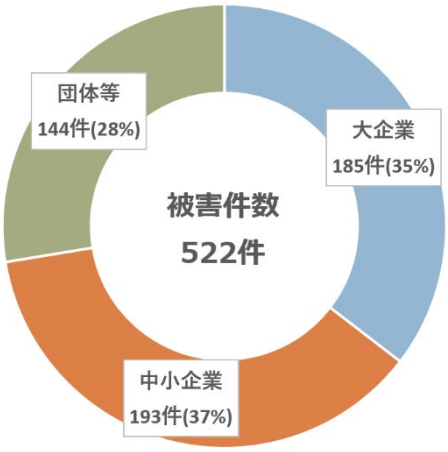
被害の規模別件数・割合は図Ⅱ-1、図Ⅱ-2のとおりです。中小企業、団体等（注）の被害が70%を占めています。

日本の企業のうち中小企業の割合は99%超であること[1]を鑑みた場合には大企業の被害割合が多いということになりますが、中小企業や小規模事業者では、手段、認識、必要性等の観点からホームページ等による不特定多数に対する被害公表に積極的ではないと推測され、必ずしも大企業の被害割合が多いとはいえないと考えられます。

いずれにせよ「大企業だけではなく多くの中小企業がサイバー攻撃による被害を受けている」ということはいえるでしょう。



図Ⅱ-1
被害組織の規模別割合
累計（2017年1月～2024年6月）



図Ⅱ-2
被害組織の規模別割合
直近2年（2022年7月～2024年6月）

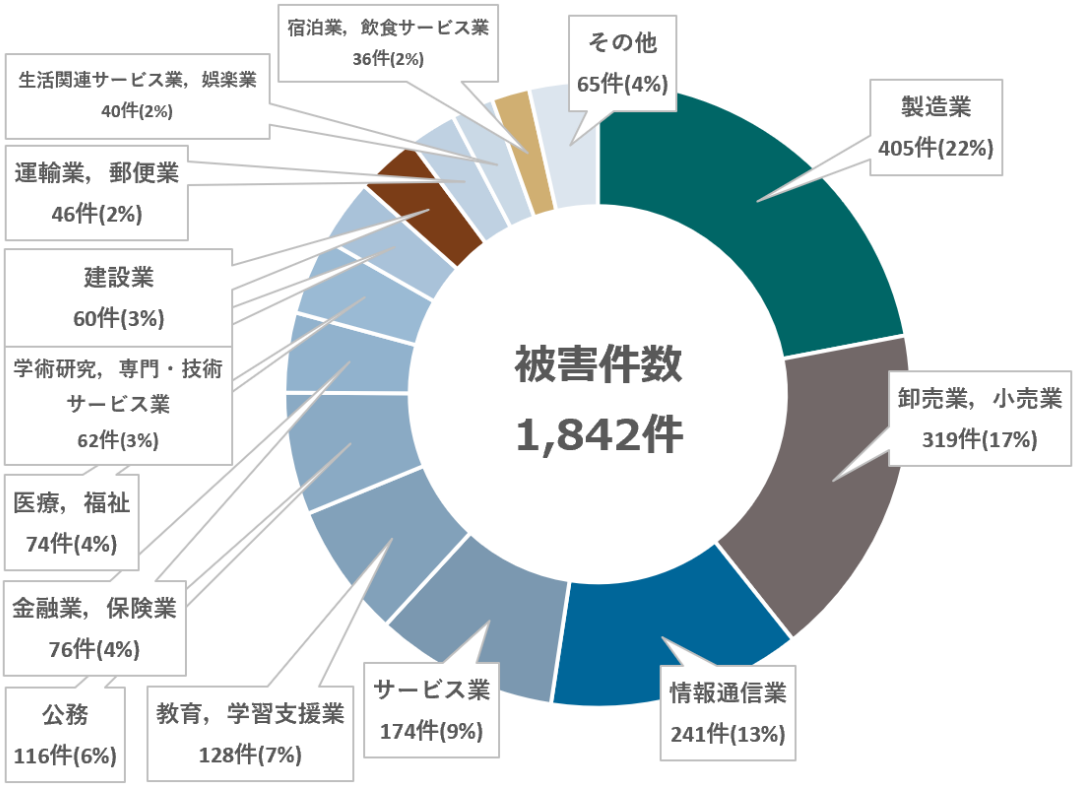
（注）「団体等」…企業以外の法人（医療法人、学校法人、社団法人、財団法人、協同組合、国、地方公共団体など）

② 業種

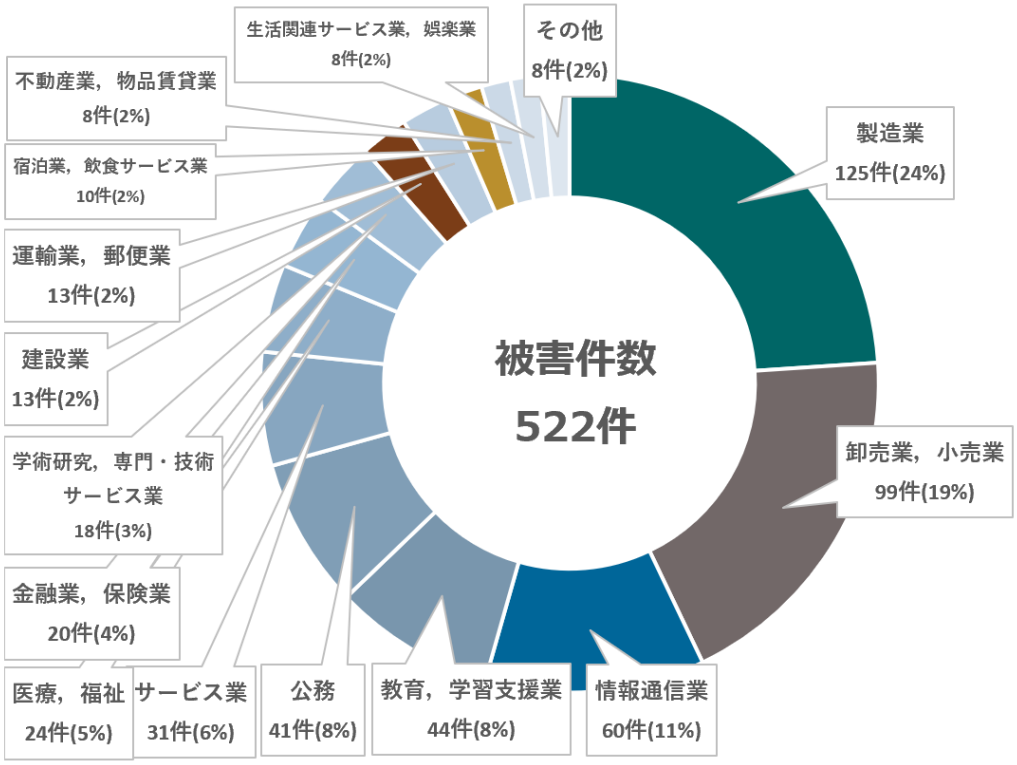
被害の業種別件数・割合は図Ⅱ-3、図Ⅱ-4のとおりです。製造業を筆頭に様々な業種において被害が発生していることが読み取れます。

なお、このような業種別件数・割合をみる場合、国内企業全体の業種別割合も考慮する必要があります。図Ⅱ-5は「令和3年経済センサス 活動調査 調査の結果[2]」に基づき作成した、国内企業全体の業種別割合です。図Ⅱ-5を踏まえれば、製造業や情報通信業の割合が高いこと（例えば、製造業の被害件数の割合は20%強に対し、企業全体での割合は9.2%）、逆に宿泊業、飲食サービス業や建設業の割合が低いことが分かります。

サイバー攻撃を受けやすい業種、受けにくい業種といった観点のほか、影響範囲が大きく取引先、顧客等から被害公表を求められる業種がある一方で、中小企業・小規模事業者の割合が多い業種、BtoBビジネスのため個人情報漏えいのおそれがない業種など、被害公表が積極的になされない業種があるということも念頭に置く必要があるでしょう。

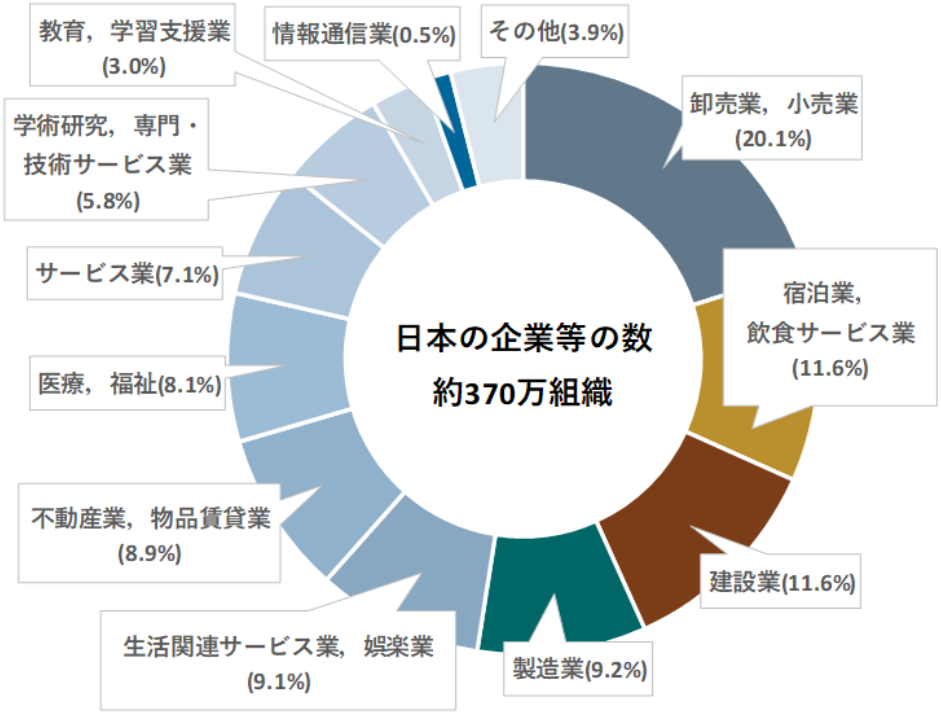


図Ⅱ-3 被害組織の業種別割合
累計（2017年1月～2024年6月）



図Ⅱ-4 被害組織の業種別割合

直近2年（2022年7月～2024年6月）

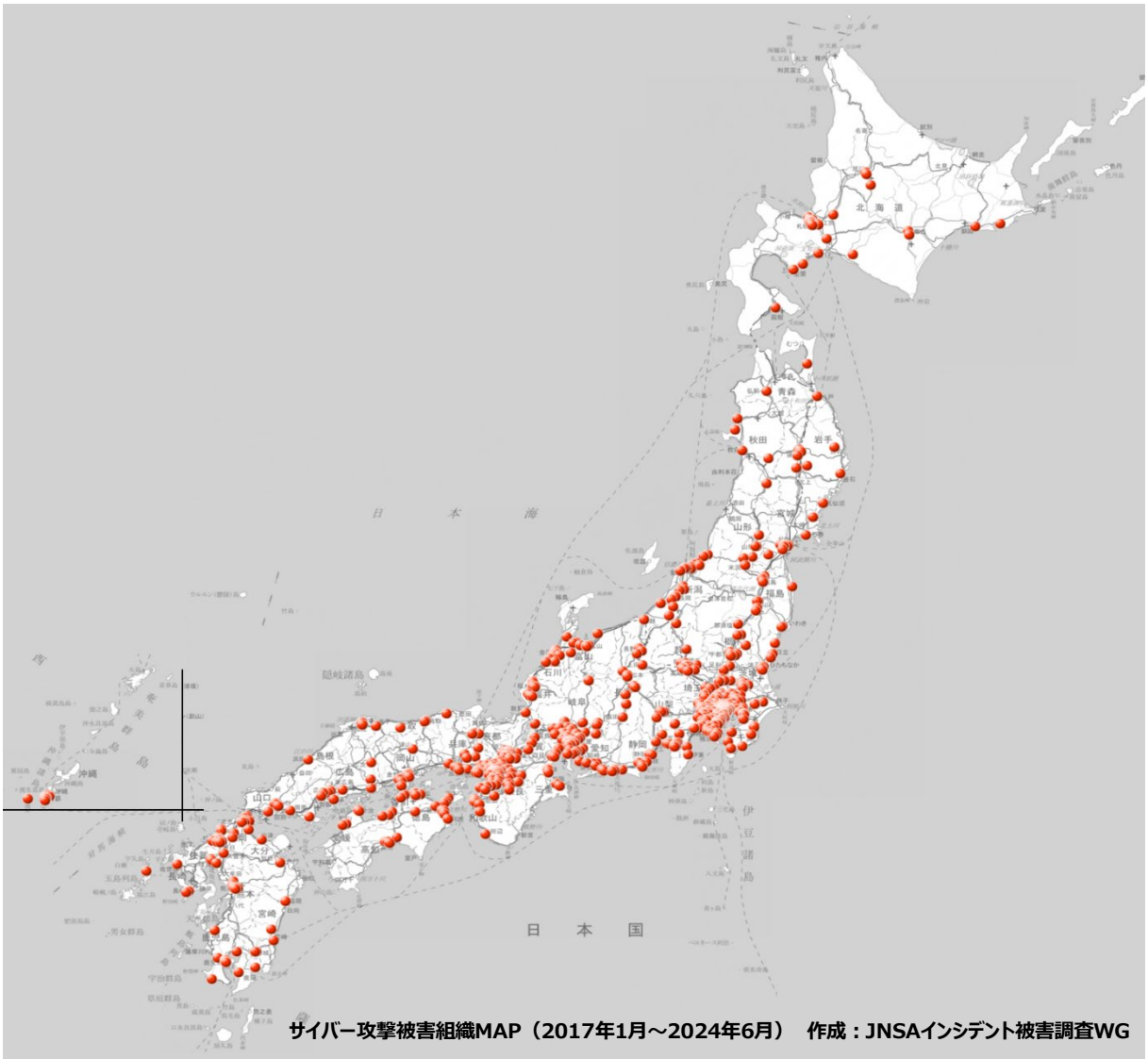


図Ⅱ-5 国内企業全体の業種別割合

③　所在地分布

被害組織の本社所在地をマッピングした結果は図Ⅱ-6のとおりです。

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ります。なお、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ますが、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を分母とした割合を鑑みても、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しています。

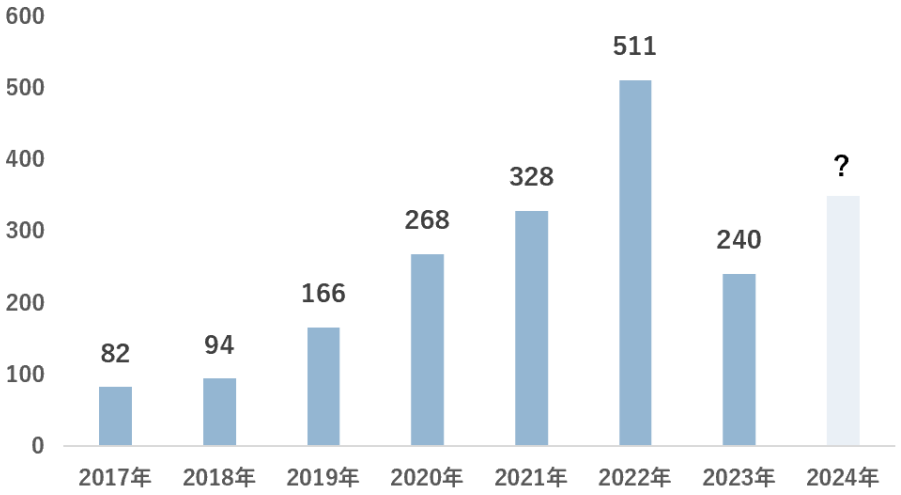


図Ⅱ-6　サイバー攻撃被害組織の所在地分布

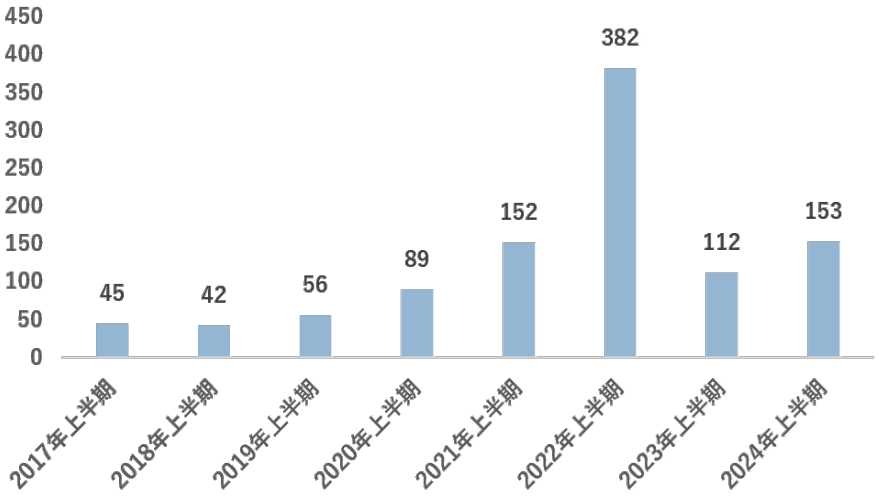
④　被害組織による公表件数の年別推移

調査対象とした約1,800事例における年別の公表・報道等の件数は次のとおりです。図Ⅱ-7は年別、図Ⅱ-8は上半期別（2024年は上半期のみの数字のため作成した図表）となります。

公表の実施や報道がなされる組織が年々増加している一方、2022年をピークとして、一旦は2023年に減少したことが読み取れます。これは、2022年上期まで猛威を振るっていたエモテット感染被害や、2021、2022年に集中した特定のメーカーの機器（VPN、NAS等）の被害が、2023年以降は一定収束していることが大きな要因として挙げられます。サイバー攻撃が減少しているということではなく、特定のマルウェア、特定の機器といったものが、瞬間風速的に多くの組織に影響を与えうることが公表件数を左右するともいえるでしょう。



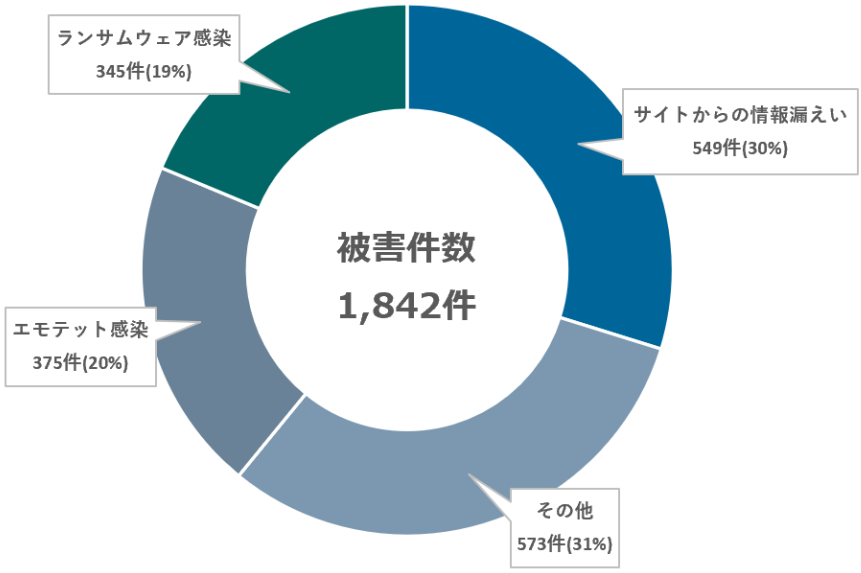
図Ⅱ-7 サイバー攻撃の公表件数の年別推移



図Ⅱ-8 サイバー攻撃の公表件数の上半期別推移

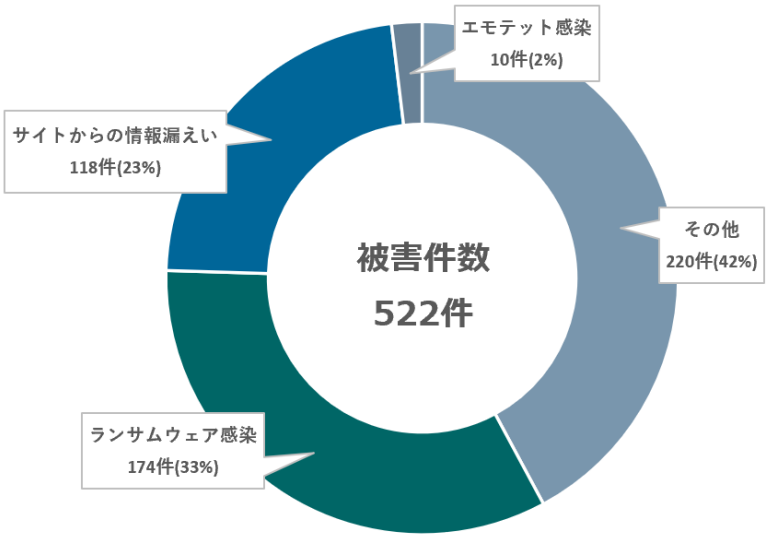
⑤ サイバー攻撃種別

サイバー攻撃の種別構成は図Ⅱ-9、図Ⅱ-10のとおりです。直近2年では「エモテット感染」が大幅に減少、その一方で「ランサムウェア感染」が拡大したことがみてとれます。



図Ⅱ-9 サイバー攻撃の種別構成

累計（2017年1月～2024年6月）



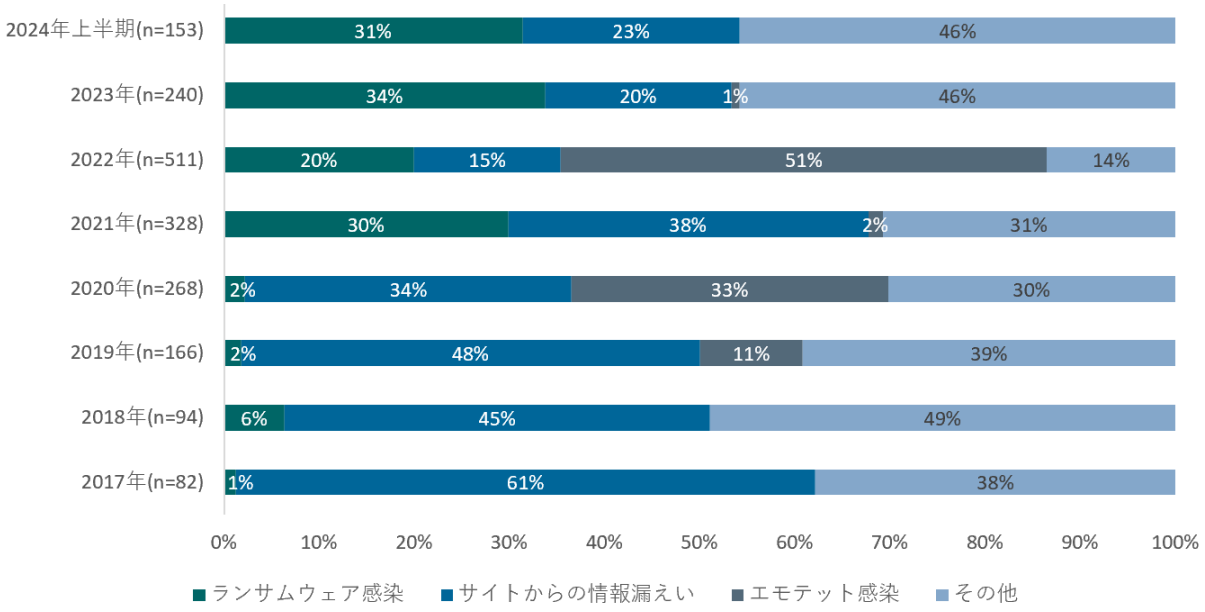
図Ⅱ-10 サイバー攻撃の種別構成

直近2年（2022年7月～2024年6月）

⑥ サイバー攻撃種別の年別推移

公表されたサイバー攻撃種別を、2017年から集計した結果は図Ⅱ-11のとおりです。

種別構成が大きく変容していることが分かります。特に2020年、2022年は「エモテット感染」の被害公表が占める割合が多いこと、2021年以降は「ランサムウェア感染」の被害拡大していることは特筆すべき点です。「ランサムウェア感染」の拡大については、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[3]」の結果と同様の傾向を示すところです。



図Ⅱ-11 サイバー攻撃種別の年度別推移

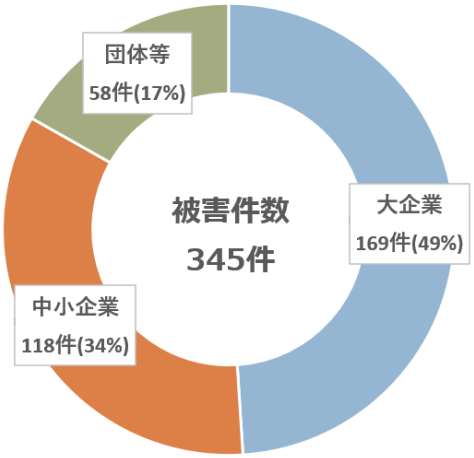
（２）サイバー攻撃種別ごとのデータ

① ランサムウェア感染

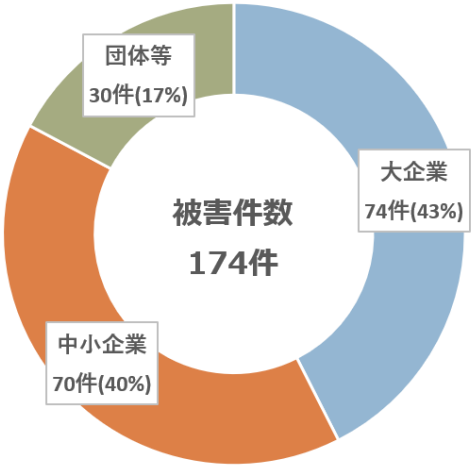
ア．規模

ランサムウェア感染被害組織の規模別件数・割合は図Ⅱ-12、図Ⅱ-13のとおりです。

前述の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」の結果では大企業は３割程度の割合であることから、同データとの相違が気になるところですが、この違いとして、中小企業においては、警察や個人情報保護委員会への報告等は実施しつつも、影響度の低さからホームページ等により不特定多数に対してランサムウェア被害の公表を実施しない企業が一定数存在することが理由として推測されます。



図Ⅱ-12
ランサムウェア被害組織
の規模別割合
累計（2017年1月～2024年6月）



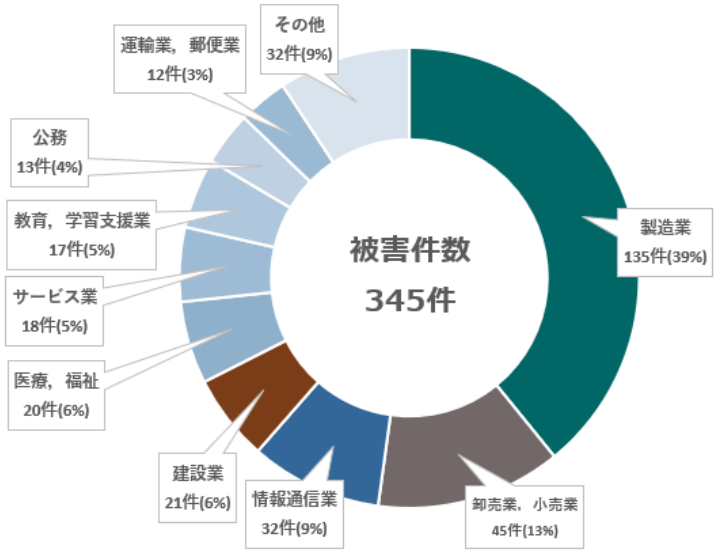
図Ⅱ-13
ランサムウェア被害組織
の規模別割合
直近2年（2022年7月～2024年6月）

イ．業種

ランサムウェア感染被害組織の業種別件数・割合は図Ⅱ-14、図Ⅱ-15のとおりです。

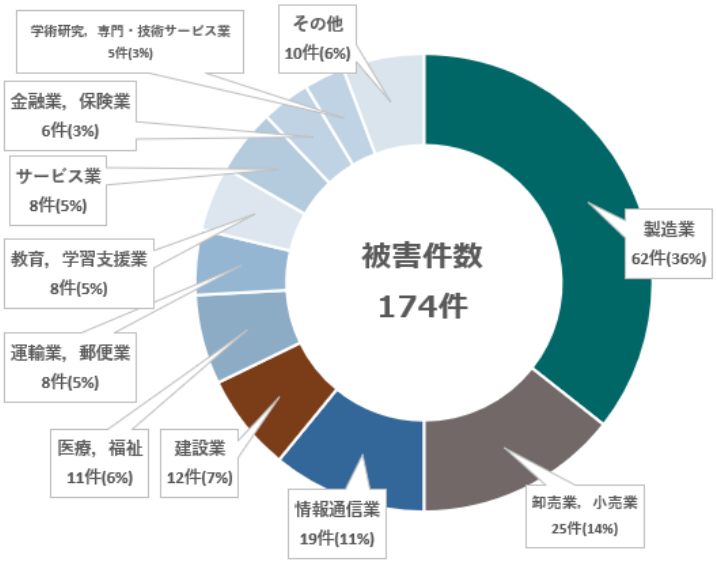
製造業の被害が全体の4割近くを占め、大きく目立った結果となっています。

攻撃者は身代金を得ることを目的としており、より脅しの利く相手をターゲットにすること、サプライチェーンのなかで大企業や多くの取引先に迷惑をかけてはいけないという心理が働く組織を狙うといったことが推測できますが、実際のところは攻撃者のみぞ知るということになります。



図Ⅱ-14 ランサムウェア被害組織の業種別割合

累計（2017年1月～2024年6月）



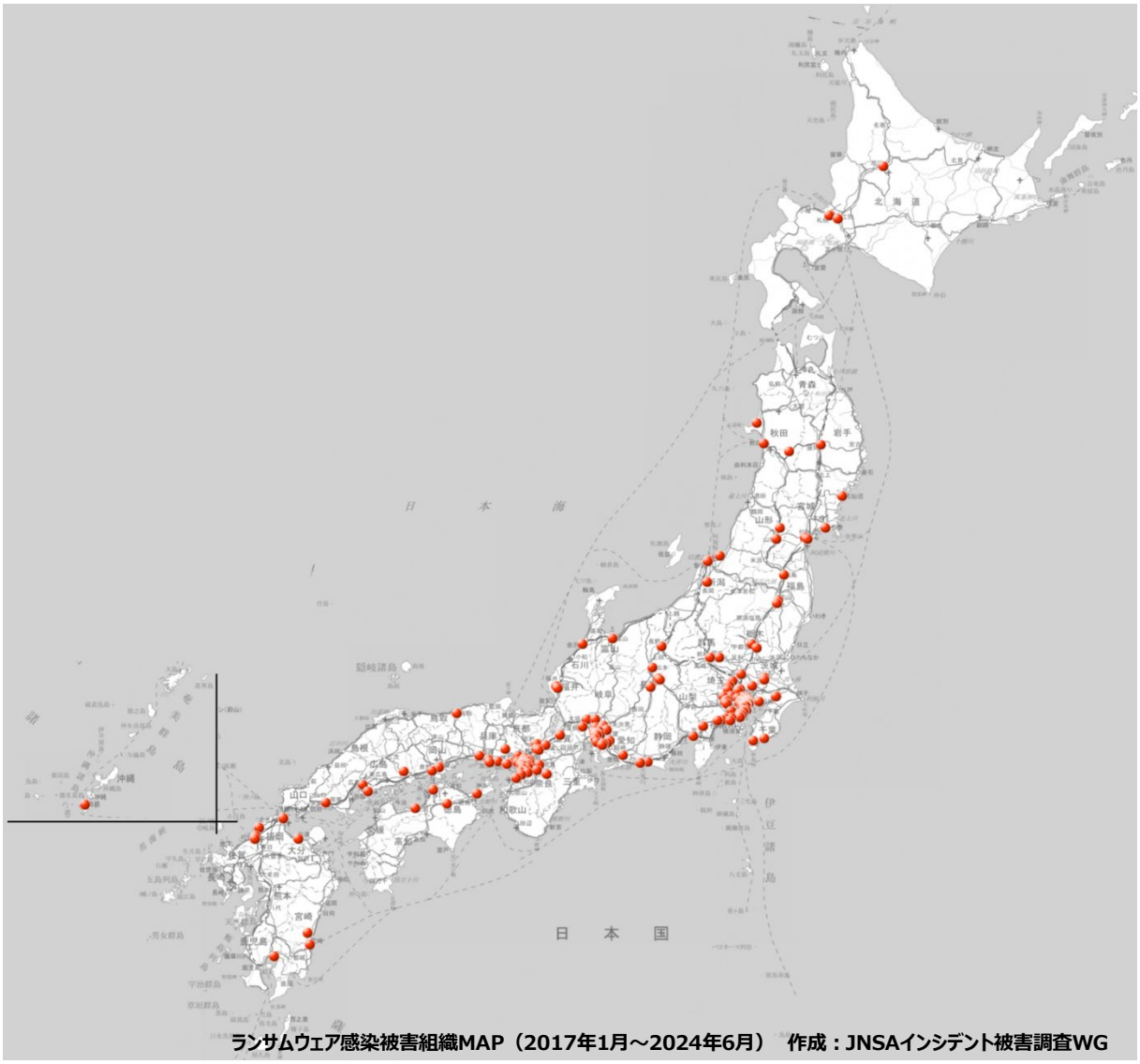
図Ⅱ-15 ランサムウェア被害組織の業種別割合

直近2年（2022年7月～2024年6月）

ウ．所在地分布

被害組織の本社所在地をマッピングした結果は図Ⅱ-16のとおりです。

ランサムウェア感染被害は日本全国で被害が発生していることがわかります。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ます。



図Ⅱ-16 ランサムウェア感染被害組織の所在地分布

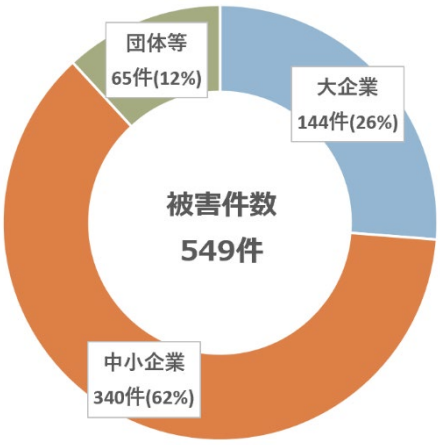
② ウェブサイトからの情報漏えい被害

ア．規模

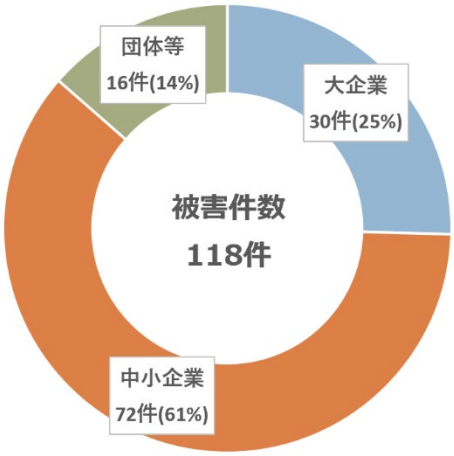
ウェブサイトからの情報漏えい被害組織の規模別件数・割合は図Ⅱ-17、図Ⅱ-18のとおりです。中小企業で発生した被害が全体の6割近くを占めています。

自社ホームページを設置することは当然ともいえる昨今ですが、セキュリティに対する意識が低かったり、コスト面の制約もあったり等で、CMS（コンテンツマネジメントシステム。ウェブサイトを運用・管理するシステム）など、ホームページを構成する各種のシステム、プログラムの脆弱性等を放置し、結果としてサイバー攻撃の被害を受ける中小企業が多いことが推測されます。

また、EC市場の規模が拡大するなか、中小企業においてもECサイトを設置することは一般的となっていますが、セキュリティ対策が不十分なまま、安易・安価で自社ECサイトを構築し、サイバー攻撃の被害を受ける中小企業が多いことも推測されます。



図Ⅱ-17
ウェブサイトの情報漏えい
被害組織の規模別割合
累計（2017年1月～2024年6月）



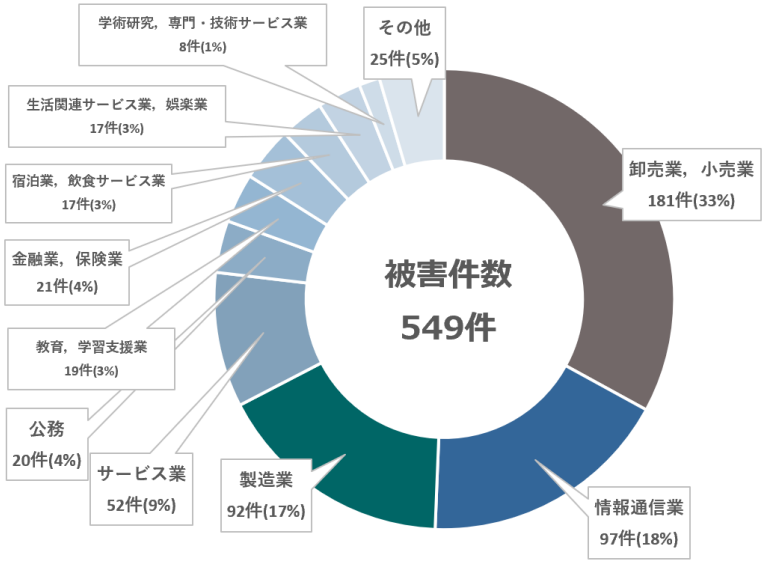
図Ⅱ-18
ウェブサイトの情報漏えい
被害組織の規模別割合
直近2年（2022年7月～2024年6月）

イ．業種

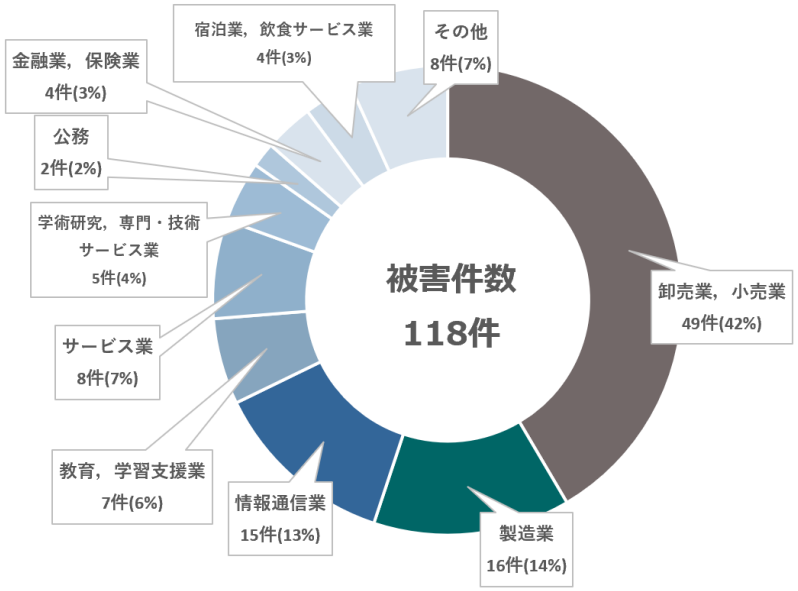
ウェブサイトからの情報漏えい被害組織の業種別件数・割合は、図Ⅱ-19、図Ⅱ-20のとおりです。

他の業種に比べ、卸売業、小売業、情報通信業、製造業（小売を含む）が占める割合が多いことが特徴的です。

これは、ECサイトで商品・サービスの販売を行う卸売業、小売業、製造業、情報通信業や、ECサイトの運営を行う情報通信業からの被害公表が多いためと推測されます。



図Ⅱ-19 ウェブサイトからの情報漏えい被害組織の業種別割合
累計（2017年1月～2024年6月）

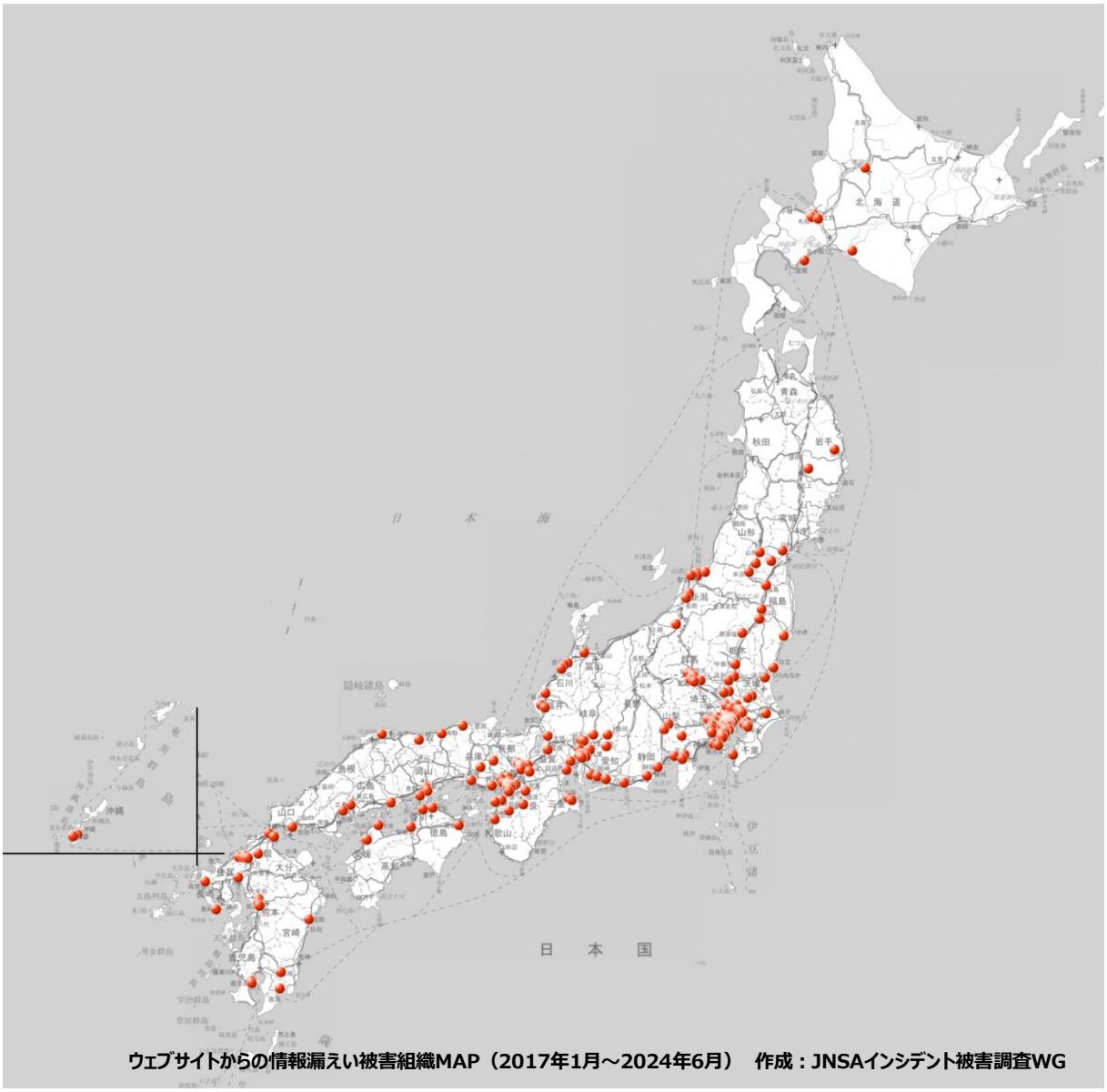


図Ⅱ-20 ウェブサイトからの情報漏えい被害組織の業種別割合
累計（2017年1月～2024年6月）

ウ．所在地分布

被害組織の本社所在地をマッピングした結果は図Ⅱ-21のとおりです。

ランサムウェア感染同様、ウェブサイトの情報漏えい被害は日本全国で被害が発生していることがわかります。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ます。



図Ⅱ-21 ウェブサイトからの情報漏えい被害組織の所在地分布

Ⅲ　アンケート調査

１．調査概要

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しました。

調査名	サイバー攻撃によって生じた被害額等に関する実態調査（アンケート調査）
調査対象	2017年1月から2024年6月までの7年半のサイバー攻撃の国内被害約1,800事例のうち、国・地方公共団体を除いた事例
アンケート形式	インターネット調査（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：118件（回答率：約6.6%）

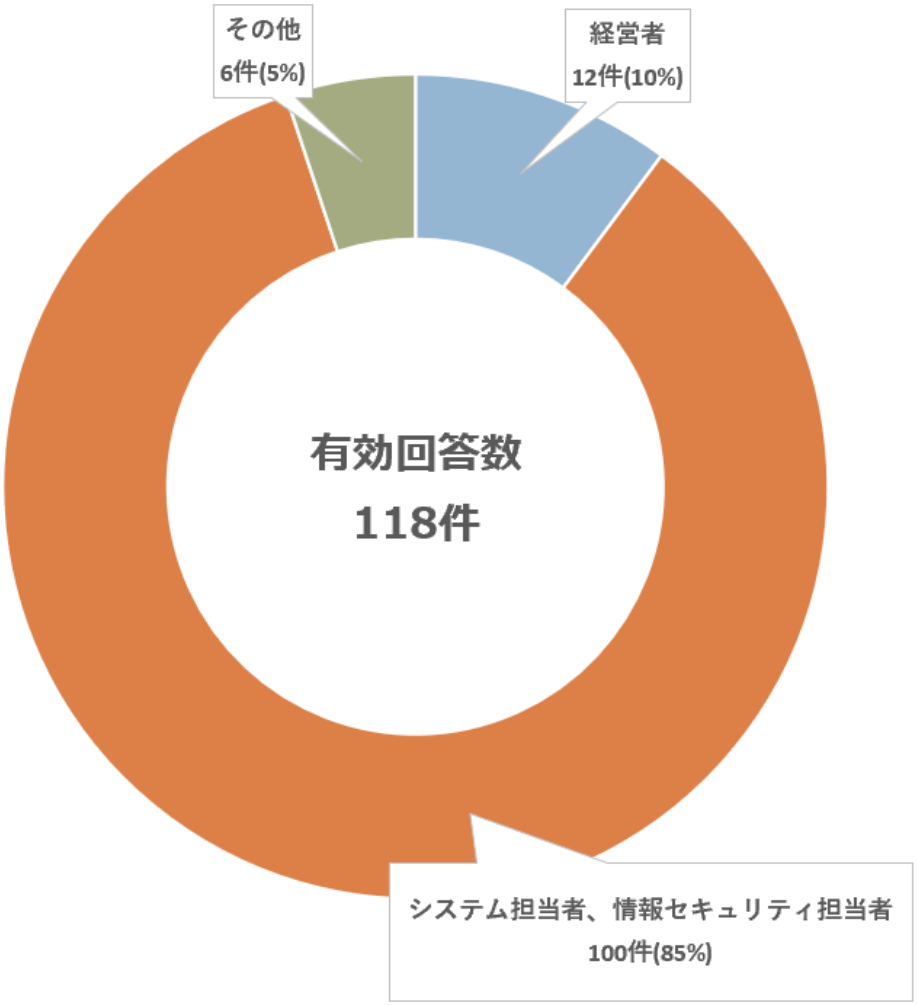
２．主なアンケート項目

主なアンケート項目は次のとおりです。

- 回答者の属性（立場や職種）
- 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・脅迫などによる被害）
  - 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（お詫び文掲載にまつわる費用など）
    - ✧ 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
    - ✧ 再発防止費用
  - 行政損害（課徴金、罰金など）
  - 対応に要した内部工数（人月ベース）
- ランサムウェア感染被害に関する追加質問
  - 身代金の支払い有無
  - データ復旧可否
  - データ復旧に関する依頼先
  - 攻撃の侵入経路
  - 攻撃を受けてから発覚までの期間
- エモテット感染被害に関する追加質問
  - 発覚経緯（自組織での発見、取引先やお客様からの指摘など）
- クレジットカード情報の漏えい被害に関する追加質問
  - 発覚経緯（自組織での発見、決済代行業者からの指摘など）
  - カード決済の停止期間
  - カード会社からの求償有無
  - カード会社からの被害公表時期に関する要請有無

３．回答者の属性

アンケート回答者の属性（立場や職種）の内訳は、図Ⅲ-Ⅰのとおりです。



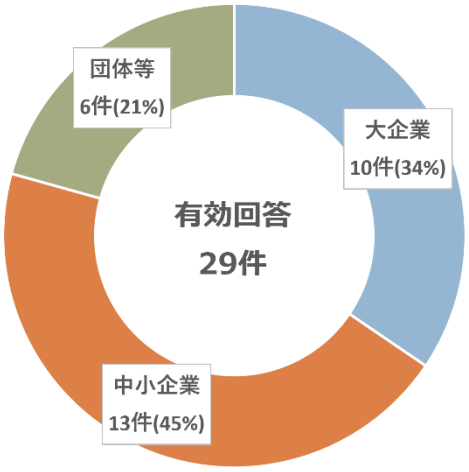
図Ⅲ-Ⅰ 回答者の属性

４．ランサムウェア感染

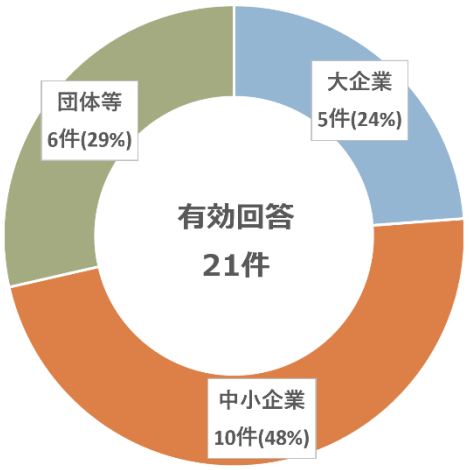
ランサムウェア感染被害組織からのアンケート回答数は29件でした。

① 規模

回答のあった被害組織の規模別内訳は、図Ⅲ-2、図Ⅲ-3のとおりです。



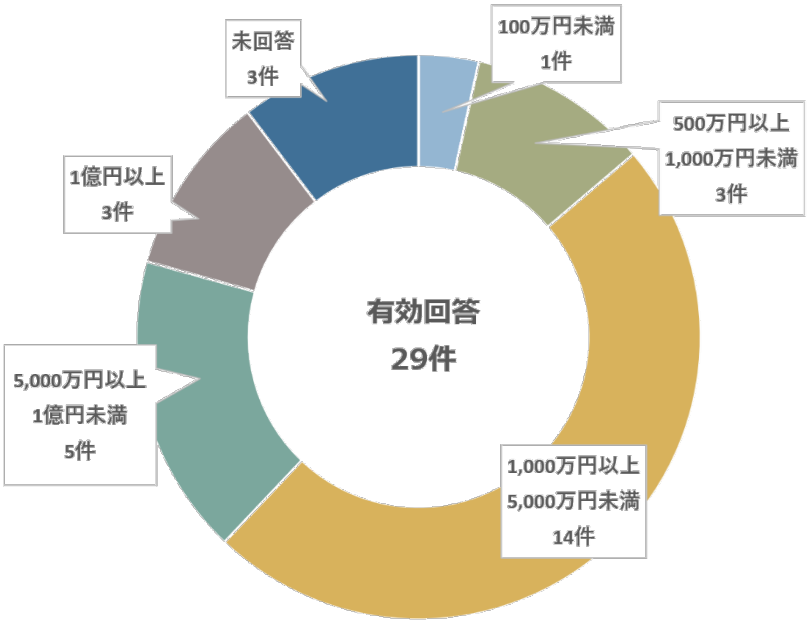
図Ⅲ-2
回答のあったランサムウェア感染被害組織の規模別割合
累計（2017年1月～2024年6月）



図Ⅲ-3
回答のあったランサムウェア感染被害組織の規模別割合
直近2年（2022年7月～2024年6月）

② 被害金額

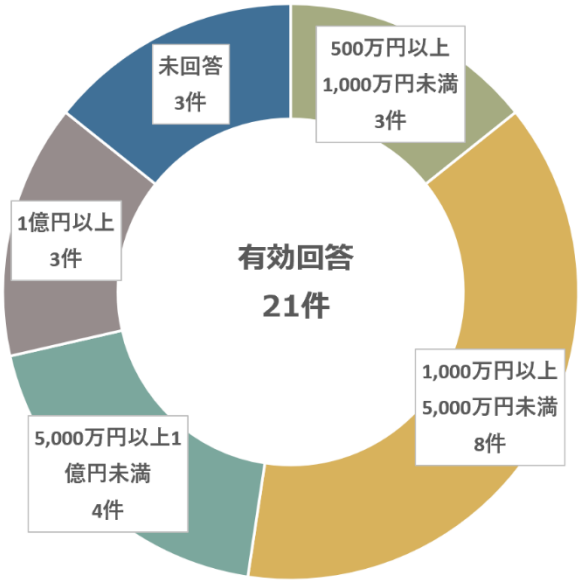
回答のあった被害組織の被害金額内訳は、図Ⅲ-4、図Ⅲ-5のとおりです。



（万円）

平均値	4,959
中央値	3,260

図Ⅲ-4
回答のあったランサムウェア感染被害組織の被害金額
累計（2017年1月～2024年6月）



（万円）

平均値	6,019
中央値	3,800

図Ⅲ-5
回答のあったランサムウェア感染被害組織の被害金額
直近2年（2022年7月～2024年6月）

ランサムウェア感染被害を受けた組織にて生じた被害金額はほとんどの被害組織が被害金額を1,000万円超と回答しており、回答の平均値は4,959万円、中央値は3,260万円でした。直近2年（2022年7月～2024年6月）についてみてみると、回答の平均値は6,019万円、中央値は3,800万円となり、ランサムウェア感染被害による損害額は増加傾向にあるといえます。

なお、回答のあった被害組織の多くは、費用損害（各種事故対応の費用）の金額は把握しているものの、ランサムウェア感染によって引き起こされたシステムの停止およびこれに伴う業務中断による利益喪失等の損害については十分に把握していませんでした。また、被害組織が事故対応に要した内部工数（人月）（注）の回答の平均値は19.7人月という結果が得られましたが、これらをコストとして把握していないケースも多くみられました。つまり、利益喪失や内部工数コスト等の額がアンケート回答として得られなかったことを鑑みると、企業全体の損害額は、平均値および中央値ともに、上記以上の額であることは間違いないでしょう。

ところで、ランサムウェア攻撃者に対しての身代金支払い有無について「支払った」とアンケート回答した組織は存在しなかったことはここで書き添えておきます。

（注）1人が1か月間働いた作業量を1とするもの。
例）10人が業務時間の半分を3か月費やした場合、10人×50%×3か月＝15人月

〇データを復旧できた組織は73%

「復旧できた」という回答の多くは、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1件のみでした。「復旧できなかった」という回答のなかには、そもそもバックアップを取得していなかったケースのほか、バックアップデータが暗号化されてしまったケースも見られました。

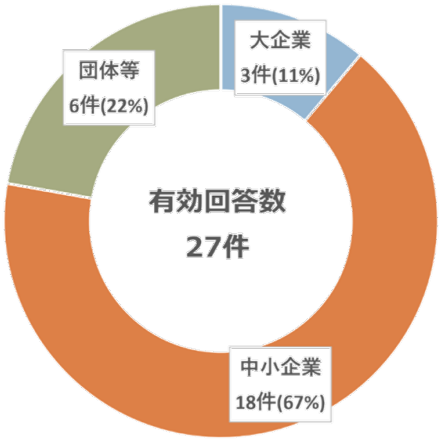
前回のアンケート調査（2017年1月～2022年6月の被害が対象）では「復旧できた」と回答した組織は50%でしたが、今回のアンケート調査では、データを復旧できた組織の割合は大幅に向上しています。これはバックアップそのものの普及のほか、オフラインでの保存やバックアップデータからの復旧体制の整備など、ランサムウェア対策を意識した備えが実施されていることがうかがえます。

５．ウェブサイトからの情報漏えい

ウェブサイトからの情報漏えい被害組織からのアンケート回答数は27件でした。なお、直近2年（2022年7月～2024年6月）については回答数が5件と少なかったことから、累計ベースでのとりまとめのみを記載しています。

① 規模

回答のあった被害組織の規模別内訳は、図Ⅲ-6のとおりです。

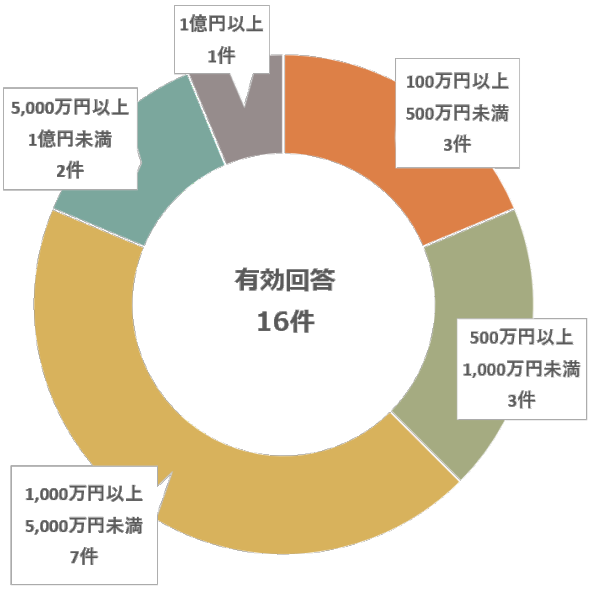


図Ⅲ-6 回答のあったウェブサイトからの情報漏えい被害組織の規模別割合
累計（2017年1月～2024年6月）

② 被害金額

回答のあった被害組織の被害金額内訳は、図Ⅲ-7、図Ⅲ-8のとおりです。

ア．クレジットカード情報を含む情報漏えい

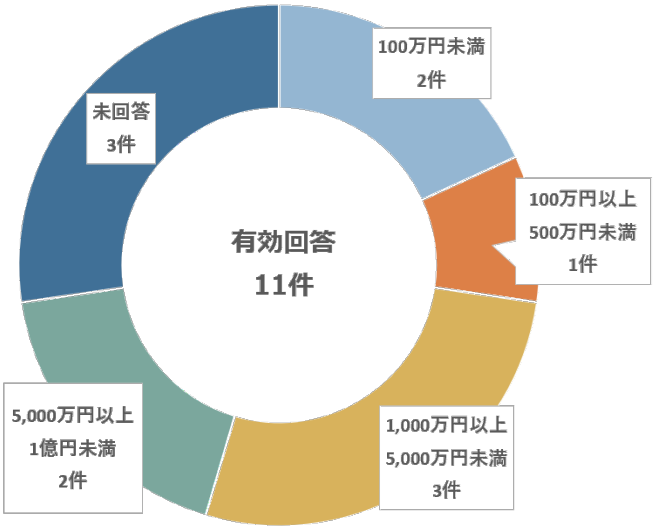


（万円）

平均値	3,608
中央値	1,690

図Ⅲ-7 回答のあったクレジットカード情報を含む情報漏えい被害組織の被害金額
累計（2017年1月～2024年6月）

イ．クレジットカード情報を含まない情報漏えい（個人情報のみ漏えい）



（万円）

平均値	2,407
中央値	1,165

図Ⅲ-8 回答のあったクレジットカード情報を含まない情報漏えい被害組織の被害金額
累計（2017年1月～2024年6月）

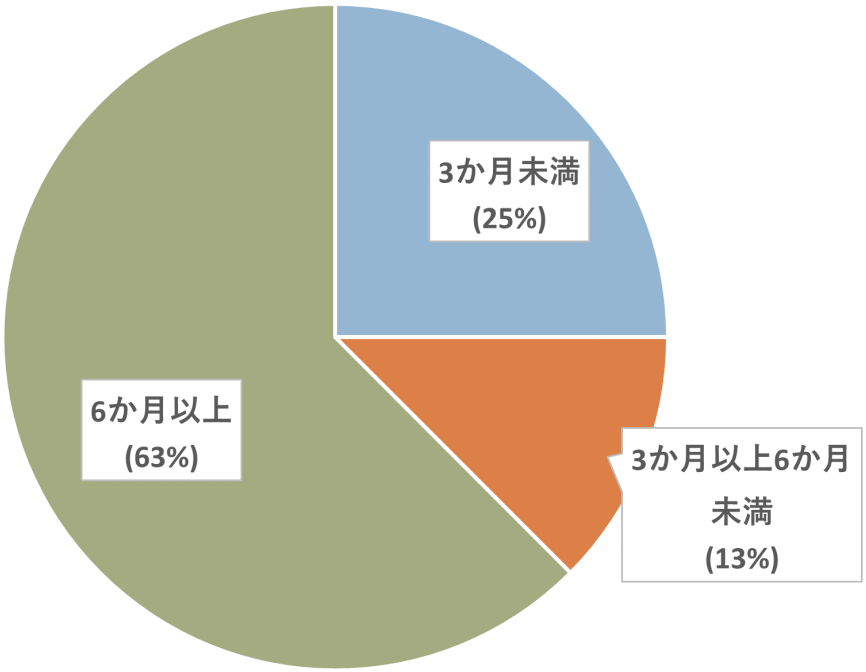
ウェブサイトからの情報漏えい被害を受けた組織にて生じた被害金額は漏えいした情報の内容により大きな開きがあります。

漏えいした情報にクレジットカード情報が含まれている場合の被害金額の回答の平均値は3,608万円、中央値は1,690万円でした。一方、個人情報のみが漏えいした場合の被害金額の回答の平均値は2,407万円、中央値は1,165万円でした。この差異は、賠償損害の有無です。クレジットカード情報が漏えいした場合、不正利用やカード再発行費用についてカード会社からの求償が生じ、損害賠償金等の損害が発生することが多く、これが差異として顕れているといえるでしょう。

なお、被害組織が事故対応に要した内部工数（人月）の回答平均値は、個人情報のみが漏えいした被害の場合は9.2人月、クレジットカード情報を含む情報漏えい被害の場合は15.4人月でした。ランサムウェア感染と同様に、これらはコストとして把握していないケースが多々見られました。

６．クレジットカード情報を含む情報漏えい被害について

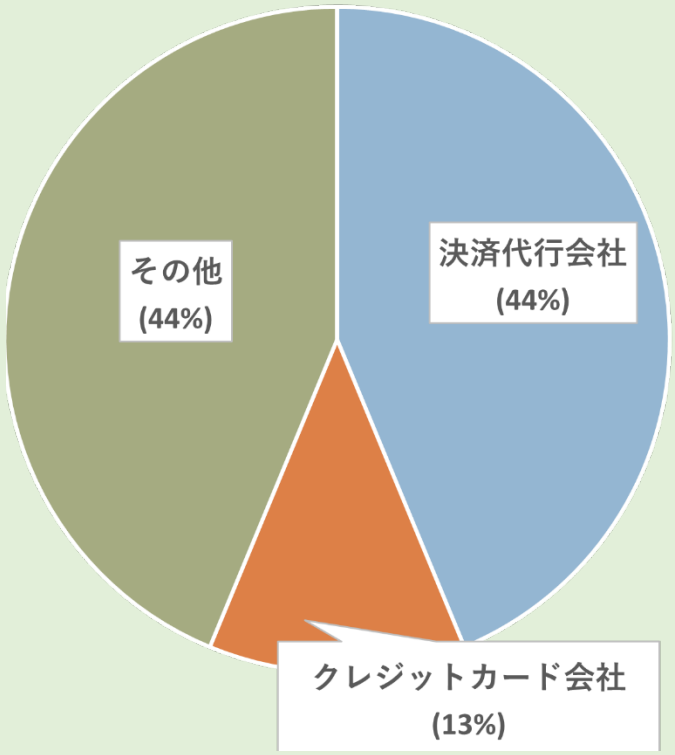
クレジットカード情報を含む情報漏えい被害の損害額が大きくなる要因の一つに、前述の賠償損害（クレジットカード会社に対する損害賠償金の支払い）のほか、被害発生から問題解決までの間に、クレジットカード決済を停止せざるを得ないことによる機会損失があります。クレジットカード情報を含む情報漏えいの被害組織の多くは、ECサイトを運用しており、クレジットカード決済の停止は売り上げの減少に直結するケースが多いためと推測されます。アンケートに回答したクレジットカード情報の漏えい被害組織のクレジットカード決済を停止した期間の平均は131.8日であり、内訳は図Ⅲ-9のとおりです。被害組織の60%以上が6か月以上、クレジットカード決済を停止したと回答しています。



図Ⅲ-9 クレジットカード決済の停止期間

○クレジットカード情報の漏えい発覚経緯

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発覚することが多いこともクレジットカード情報の漏えい被害の特徴です。アンケートに回答した組織が回答した被害発覚の経緯の内訳は図Ⅲ-10のとおりです。



図Ⅲ-10 クレジットカード情報漏えい発覚経緯の内訳

○クレジットカード情報の漏えい被害の発表時期

サイバー攻撃の被害が発覚した場合、一般的には速やかな公表が期待されますが、クレジットカード情報の漏えい被害においては、クレジットカード会社から即時公表の見送りを求められるケースも確認されました。2か月から6か月程度の期間が多く、影響範囲の調査、問い合わせへの準備等のための期間と推測されます。

Ⅳ　被害組織インタビュー

より生々しいサイバー攻撃の実情を知ってもらうべく、主にアンケート調査を実施した被害組織に対し、サイバー攻撃の内容、サイバー攻撃の対応、被害額の内訳等をインタビューしとりまとめました（次頁以降）。

NO.1～4は、前回（2024年2月）の公表資料でも掲載している4組織のインタビュー、NO.5～10は、今回の公表資料にあたって新たにインタビューを実施した6組織、合計10組織へのインタビューをとりまとめたものです。

また、上記10組織のインタビューに加え、NO.11～13として、昨今、委託先企業においてランサムウェア感染が発生し、委託元企業にも影響が拡大する事例が増加していることを踏まえ、2024年に発生したランサムウェア感染事案につき委託元3社へのインタビューをとりまとめたものです。

NO.1　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、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 ○ウェブサイト、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

（３）被害内容

顧客等の個人情報（メールアドレス、住所、氏名、電話番号等）が約2万件の漏えいのおそれ

（４）被害額

合計：1,800万円（人件費込み）

損害	費目	金額（万円）	備考
費用	システム復旧	100	PCの初期化・入れ替え
	事故原因・被害範囲調査費用	—	サーバーとPCのフォレンジック調査（出入りのITベンダーによる無償対応）
	法律相談費用	—	顧問弁護士への相談（無償対応）
	見舞金・見舞品購入費用	1,200	券面額500円のQUOカード×18,000人 送料、事務手数料などの諸経費
利益	固定費	200	
	営業利益	200	

（５）被害者コメント

〇所轄の警察に相談したが、海外にいるであろう攻撃者に対しては捜査権がないのでどうしようもないと回答があった。

〇食品を取り扱う会社として、問題の兆候があった場合には少しでも早くお客さまや取引先などの関係者にお知らせしなければという思いがあり、発覚当日にできるだけの対応を実施した。

〇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では」との意見もあり、配布に踏みきった。

〇うちは大丈夫という思いが少なからずあった。しかし、被害に遭ってしま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。（対応完了後、セキュリティ対策の強化を実施し、サイバー保険にも加入）

（６）WG所感

〇多くの企業が感染の発覚から発表まで、数日の期間を要していることを考えると、感染が発覚した当日に、ウェブサイト、メール、SNSを通じた報告・注意喚起を発信し、警察への相談、ネットショップでの販売の停止を判断し実行するなど、多くの対応を実施されたというのは非常に早いと感じられる。

〇インシデント対応に関しては、危機管理コンサルなどに相談した結果ではなく、普段から食品を取り扱う会社として出荷した商品に問題があった際に速やかに対処してきた経験や、そうした事態を想定した対策を積み重ねてきた経験を踏まえたものであったことは特筆すべき点といえる。

NO.2　エモテット感染（その２）

業種	各種団体		エモテット感染 ～ステークホルダー信頼回復のための代償～
地域	東京		
従業員規模		～20名	
	○	20名～999名	
		1,000名～	

（１）事案概要

○顧客からのメールを装ったなりすましメールを職員が受け取った。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。

○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等について、漏えいしたおそれ

（２）時系列

年月	備考
YYYY年M月D日	なりすましメールを受信した職員のPCがエモテットに感染
YYYY年M月D日＋1日	ウェブサイトにて迷惑メールに関する注意喚起を公表
YYYY年M月D日＋7日	アンチウイルスソフトがマルウェアを検出
YYYY年M月D日＋31日	ウェブサイトにてエモテット感染被害と業務正常化を公表

（３）被害内容

顧客などとの送受信メールおよびメールアドレス数万件の漏えいしたおそれ

（４）被害額

合計：2,000万円以上（全端末の徹底調査、証拠保全、防止策導入）

＋　対応に要した内部工数：2人月

損害	費目	備考
費用	事故原因 被害範囲調査費用	・ステークホルダーからの要請も受け、組織内の全端末を徹底調査 ・ダークウェブ調査
	コンサルティング費用	対応に関するコンサルティングサービス
	法律相談費用	
	システム復旧費用	証拠保全のためリース機を買取った費用を含む
	再発防止費用	・ウイルス対策ソフトの入れ替え ・EDR、資産管理ソフトの導入など

※　ご協力くださった組織の希望により、費目ごとの損害額は非公開

※　業務の正常化までに発生したコストで算出

※　業務正常化以降も、組織内に情報セキュリティ委員会やセキュリティに関するアドバイザーを設置するなど、セキュリティ対策や体制を強化しているが、それらのコストは算出外

（５）被害者コメント

〇被害前はセキュリティ対策が不十分でログなどの記録も存在しなかったため、被害規模や影響の調査範囲が膨大となり、相当の対応費用を要した。

〇信頼回復を図るため、関係者の多くが相当な精神的重圧を抱えながらの日夜必死の対応を迫られた。

〇ITの世界はインターネットを通じて世界中とつながっている。欧米においてはサイバー攻撃者との“戦争”といった考えをもって、セキュリティ対策を十分に行っていると思われるが、日本においては、安全な生活が当たり前の安穏な意識があり、セキュリティ対策が疎かになっていたのではと感じている。

（６）WG所感

〇取引先等ステークホルダーからの要請により、事故原因・被害範囲調査などを徹底的な対応を実施した事例であること（多額のコストを要した事例であること）は特筆すべき点

〇本件インシデント発生以降、専門組織が設置されるなど、セキュリティ対策の重要性を鑑みた対応が継続されているが、インシデント発生を契機とするものではなく、平常時においても経営者等が関心を持ったうえで各種対応が図られるような啓発活動の必要性を実感

NO.3　ランサムウェア感染（その１）

業種	商社		ランサムウェア感染 ～狙われる海外拠点～
地域	関東		
従業員規模		～20名	
		20名～999名	
	○	1,000名～	

（１）事案概要

○海外拠点のVPN機器から侵入。海外拠点を経由して日本本社のシステムにも侵入された。

○国内のサーバー複数台がランサムウェアに感染。データが暗号化された。

（２）時系列

年月	備考
YYYY年M月（注）	攻撃者が海外拠点のVPN機器から侵入
YYYY年M月D日	社内ユーザーから「システムが動かない」と問い合わせがあり、被害が発覚
YYYY年M月D＋3日	感染被害を自社ウェブサイトで公表

（注）被害発覚から大きな期間の開き無し

（３）被害内容

○国内のサーバー複数台がランサムウェアに感染。データを暗号化された。

○ネットワークハードディスク（NAS）に保存していたバックアップデータも暗号化されてしまい、復号不可

○情報の窃取によるいわゆる二重脅迫（暗号化したデータの復旧にかかる脅迫、および窃取した情報を公開する旨の脅迫）はなかった。

○被害を受けた社内システムの復旧には1.5か月から2か月、業務の正常化には約半年を要した。

（４）被害額

合計：4,000万円

＋　対応に要した内部工数：40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	400万円	
	ダークウェブ調査費用	200万円	ダークウェブ上に自社の情報が流れていないかの調査をベンダーに依頼
	システム復旧費用	2,000万円	サーバーの再セットアップなど
	再発防止費用	1,000万円	・新規セキュリティ対策（EDR、IDS/IPSなど）の導入 ・脆弱性への対応
利益	営業利益	算出不可	日々の運用を手作業で行ったが、業務が十分に遂行できなかったことによる機会損失
	固定費	算出不可	

（５）被害者コメント

○「明日は我が身」

○いくら多層防御を重ねてもすべての攻撃を100%止めることは不可能。被害を受けることも想定した対策も必要。

○今後は導入機器に危険な脆弱性が公表された場合は、情報を提供するようベンダーに依頼した。

（６）WG所感

〇海外に展開している企業において、その海外拠点が狙われ、ランサムウェア被害に遭う事案は非常に多いが、本件もその一つ。日本本社でのセキュリティ対策は進んでいたとしても、海外拠点でのセキュリティ対策が不十分な企業も多く、海外拠点のセキュリティ対策は大きな課題

〇「明日は我が身」の言葉にもあるように、サイバー攻撃は100%防ぐことは困難であり、攻撃を受けることを想定した対策も必要

NO.4　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

（３）被害内容

〇国内のサーバー複数台がランサムウェアに感染。データが暗号化

〇情報の窃取によるいわゆる二重脅迫（暗号化したデータの復旧にかかる脅迫、および窃取した情報を公開する旨の脅迫）も発生。法律事務所への相談等を踏まえ、身代金は支払わず。

〇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。被害がないことを後日確認

〇被害を受けた社内システムの復旧には２か月を要した。また、カード情報の漏えいの確認に期間を要したため、会社全体の業務の正常化には約７か月を要した。

（４）被害額

合計：1億2,400万円

＋　対応に要した内部工数：不明（残業代等超過人件費として1,000万円強を計上）

＋　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	800万円	
	法律相談費用、コンサルティング費用、ダークウェブ調査費用	1,600万円	
	詫び状送付、見舞品等購入費用	4,500万円	クオカードなどの送付
	コールセンター費用	600万円	
	システム復旧費用	4,000万円	新規システム構築のコスト
	再発防止費用	900万円	・新規セキュリティ対策（EDR/MDR）の導入 ・VPN機器の保守の見直し、AD（アクティブディレクトリ）管理の見直し
利益	営業利益	算出不可	
	固定費	算出不可	

（５）被害者コメント

○「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している。目先の利益に捉われ、セキュリティ対策にかけるコストを削った場合のリスクについて想定が十分でなかった。指揮官がいないのもそういうジャッジになった。

○同業他社で同様の事案が起きていることの把握もできていなかった。

○損失について大部分は保険で補てんされた。日頃から保険会社とのコミュニケーションを取ることが大事だと思う。
サイバーリスクに限らず、鳥の目、マクロの視点でものをみることが大事。

○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。

（６）WG所感

○ランサムウェア被害が高額化した実例。本件企業はBtoBほか、BtoC事業も展開しており、個人情報漏えいのおそれもあったことから、詫び状・見舞品の送付、コールセンター設置などの対応も実施したため、被害額も高額なものとった模様

○原因となったVPN機器は、国内でも多くの被害組織が発生しているが、その保守サービスを途中解約してしまったのは特筆すべき事案。コスト削減によって得られる目先の効果ではなく、十分なリスク想定が必要

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

（４）被害額

合計：約2億5,000万円以上

＋　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

（注）ゼロトラストネットワークアクセスの略。あらゆるアクセスを常に検証するゼロトラストの考え方のもと社内・社外を問わず厳密なアクセス制御を行う。

（５）被害者コメント（システム担当者）

○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）

〇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。

〇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。

〇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。

（６）WG所感

〇システム早期復旧という結果からも、リストア訓練の実施の重要性がわかる事例

〇ランサムウェア被害組織の当事者として、身代金交渉・支払の是非についての考え方も参考としたい事例

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）

（４）被害額

合計：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

（５）被害者コメント（システム担当者）

○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。

（６）WG所感

○システム担当は専任ではなかった事例

〇事業規模から委託ベンダーや他部門の協力が不可欠であり、他部門の人員は通常業務に加え復旧作業にも参加。勤務時間等の制約から完全復旧に1年を要した。事業規模にもかかわらず、バックアップ・リストアなど、事故想定など事前にできることを実施しておくことの重要性をあらためて認識させられる。
〇ユーザー側と委託ベンダー側との作業分担、責任分界点等の観点から、脆弱性対応の難しさを想起させる。ユーザー側でもサービス内容・費用に加え、サービスにおけるセキュリティ、運用体制などのチェックも必要

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

（４）被害額

合計：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

（５）被害者コメント（システム担当者）

〇海外現地法人の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。

〇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。

〇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。
〇被害当時、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。
〇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。

（６）WG所感

〇海外に展開している企業において、その海外現地法人が攻撃を受け、国内にも波及する事案が存在するが、本件もその一つと考えられる。
〇海外現地法人のセキュリティ対策状況の確認はもちろん、初動対応を海外現地法人が先に進めてしまい、調査のための証跡が残っていない場合があるため、有事の際の対応についても確認しておくことが重要
〇被害によって生じた内部工数、人件費等を把握していない被害組織が多い中で、IT部門が主体的に被害への対応に費やした内部工数や、被害に伴い増加した人件費を詳細に記録した事例

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

（４）被害額

合計：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

（５）被害者コメント（システム担当者）

○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。

（６）WG所感

〇多くの組織の情報を扱う情報通信業は、ランサムウェア被害の公表事例が多いが、本件もその一つ

〇被害発覚後、警察への届出や個人情報保護委員会への報告が実施されるなど、速やかに対処されており、日頃から準備がなされていたことがうかがえる。

〇被害にあった際の従業員の精神的負担は大きい。「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。」の言葉にあるとおり、バックアップは被害発生時の心の拠り所としても重要

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

（４）被害額

合計：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

（５）被害者コメント（システム担当者）

〇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

〇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。

〇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。

〇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。

〇以前にも、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。

（６）WG所感

〇海外現地法人事案ならではの費用発生や対応の難しさは特筆すべき点

〇過去の事案を糧に構築された本社CSIRTによるグループ横断体制と、日本側の積極的な関与が現地との連携を促進した、日本のガバナンスの有効性を示す好事例

NO.10　ランサムウェア感染（その８）

業種	―		ランサムウェア感染 ～大規模システムの被害は高額に～
地域	―		
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に感染

○原因はVPN機器からの侵入

（２）時系列

年月	備考
2022年M月	ランサムウェア感染発覚
2023年M月 （発覚から3か月）	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）

（４）被害額

合計：数億円以上

＋　対応に要した内部工数：21人月（システム担当のみ）

＋　利益喪失：不明も億単位

損害	費目	金額	備考
費用	事故原因・被害範囲調査費用	数千万円	サーバー等20台強の端末の調査で数千万
	ダークウェブ調査費用	一定額	数か月間ダークウェブの調査（モニタリング）を実施
	システム復旧費用 再発防止費用	数億円	バックアップデータからの復旧、数千台の端末について再インストールの実施、各種システムの再構築等により全体で数億円
	弁護士費用	一定額	ステークホルダー対応の相談

（５）被害者コメント（システム担当者）

〇ランサムウェアの感染原因として、特定のメーカーのVPN機器が原因であるとの誤った発信、誤解があるように思う。

〇複数のメーカーのVPN機器が原因となってランサムウェア感染が発生している現状をみるに、結局のところ、他人事と捉えている組織が多いように思う。

〇ユーザー、そしてベンダーも基本的なことを押さえたうえで対応していく必要があると思う。ユーザーだけではなく、未だベンダーの中にも対岸の火事、他人事として捉えているところもいると思う。

（６）WG所感

〇規模の大きさ等から組織を特定される可能性もあり多くの情報が非公開であったが、影響を受けたシステムが多岐に渡り、事故原因・被害範囲調査費用が数千万円、システム復旧費用が数億円と非常に高額になった事案であることは特筆すべき点

〇日本各地において、依然としてランサムウェア被害が後を絶たないなかで、被害組織関係者として「他人事にしない」旨の警鐘的発言が複数回あったことも印象的

NO.11　委託先のランサムウェア感染（その１）

業種	卸売業		委託先のランサムウェア感染 ～事前の想定の重要性～
地域	関東		
従業員規模		～20名	
		20名～999名	
	○	1,000名～	

（１）事案概要

○業務の再委託先がランサムウェア感染

○再委託先が管理していた、自社の顧客情報について、情報漏えいのおそれ

（２）発覚経緯

○委託先からの連絡

（３）時系列

年月	備考
2024年M月D日	再委託先がランサムウェア感染
2024年M月D日＋1日	再委託先の公式サイトにて公表
2024年M月D日＋6日	委託先から、再委託先のランサムウェア感染により、顧客情報が漏えいした可能性がある旨の連絡
2024年M月D日＋7日	個人情報保護委員会への報告
2024年M月D日＋13日	公式サイトにて第1報。（顧客情報漏えいの可能性あり）
2024年M月D日＋42日	公式サイトにて第2報。（顧客情報漏えいの可能性なし）

（４）被害内容

顧客情報の漏えいのおそれ

（５）被害額

合計：0円

＋　対応に要した内部工数：1.3人月

＋　利益喪失：不明

・金銭的被害はなし。

・対応方針決定のため、セキュリティ部門、コールセンター部門、広報部門、マーケティング部門の責任者を含めて約1時間の協議を実施。ほかにも被害者と想定される顧客情報の抽出や通知作業を実施。関係者全20名を動員したが、主な対応はほぼ1日で実行。

―20名が平均2時間を費やしたと仮定。20×2＝40時間。

・当時、被害者と想定される顧客には本事案についてホームページおよび個別にメールにて連絡した（700件以上）。顧客のほとんどが法人。

－メール1件当たり15分と仮定し、10500分＝175時間。

・上記対応により40時間＋175時間＝215時間。これを労働時間1日8時間、一か月20営業日と仮定すると内部工数は1.3人月。

（６）委託先への損害賠償請求の実施有無等

委託先への損害賠償請求は実施せず

（７）被害者コメント

○本件に関する顧客等からの問合せは一件もなかった。また、損害賠償の請求のような話も出ず、正確な事実確認・状況報告が求められた。委託先に対しては個人情報保護委員会への報告事項について詳細を確認した。

○ここ数年、年1，2度委託先でこのようなセキュリティ事故が発生している。また、過去にインシデント対応訓練をしたことがある。

○インシデント発生時は、当日中に対応方針を決めることとしており、今回もその方針で動いた。

（８）WG所感

○情報漏えいの可能性があった顧客が法人顧客であったため、関係者間で正確な状況認識をして対応していたと思われる。結果として費用負担はなかったが、内部工数対応という「見えないコスト」が発生

○事故発覚後にすぐ関係部門の責任者を招集して対応方針を決定していたのは素晴らしい。毎年のようにインシデント対応をした結果として対応能力が向上しているとすると、やはりインシデント対応訓練は有用と考えられる。

○一方で、毎年のように各委託先（再委託先を含む）でインシデントが発生しているのは、憂慮すべき状況といえる。委託元から最終委託先までサプライチェーン全体でのセキュリティ確保の取組みが求められる。

NO.12　委託先のランサムウェア感染（その２）

業種	小売業		委託先のランサムウェア感染 ～委託元でも発生する損失～
地域	近畿		
従業員規模		～20名	
		20名～999名	
	○	1,000名～	

（１）事案概要

○業務の委託先がランサムウェア感染

○委託先が管理していた、自社（委託元）の顧客情報について、情報漏えいのおそれ

（２）発覚経緯

○委託先からの連絡

（３）時系列

年月	備考
2024年M月	委託先から、不正アクセスおよび、業務停止の連絡 委託業務を継続するため、担当者が現地訪問。作業、指図対応 自社および委託先の公式サイトにて公表
2024年M＋1月	個人情報保護委員会へ委託先より確報を連名にて連絡、監視は継続 新システムにて再稼働開始、現地での自社作業も終了 自社公式サイトにて委託先での復旧を公表
2024年M＋2月	自社公式サイトにて情報漏えいがないことを公表
2025年M＋3月	情報漏えいはないことを確認するも「おそれ」はあるため、本人通知実施 コールセンターを外部業者へ委託し開設（１か月） 委託先から本人通知完了を個人情報保護委員会に連絡
2025年M＋4月	コールセンター終了、委託先より対応に要した費用相当額を受領

（４）被害内容

顧客情報20,000件以上が漏えいしたおそれ

（５）被害額

合計：630万円

損害	費目	金額	備考
費用	広告・宣伝活動費用	170万円	詫び状送付（印刷、封入、郵送代金）90万円、公式サイトへの告知文、個人情報保護委員会への報告内容の支援
	コールセンター費用	310万円	外注代金
	交通費等	150万円	遠征作業工数、レンタカー代金等

（６）委託先への損害賠償請求の実施有無等

委託先への損害賠償請求は実施せず

（７）被害者コメント

〇委託している業務の停止は免れた。緊急的な代替手続きとして当社の旧システムの再立ち上げや自社社員が委託先まで遠征し作業を実施したことにより、顧客に迷惑が掛からず。意思決定も迅速で現場も臨機応変に対応ができた。

〇このようなインシデントに対し、委託先と顔を合わせて話をしたことでスムーズに対応をすることができたと思っている。

〇個人情報の内容は住所、氏名、電話番号のみのため本人通知に対するコールセンターへの問い合わせも当初見込みよりかなり下回ったが内容は様々であった。本人通知は、メールアドレスが分かる方は、メールで、それ以外は文書を郵送した。

〇この件をきっかけとして情報セキュリティ対応規程を策定、併せてCSIRTを立ち上げ緊急時の演習を実施予定。これより以降セキュリティ対策を強化する事になっている。

（８）WG所感

〇委託先からの情報漏えい事案に関して、契約（損害賠償等）、インシデント発生時に委託元と委託先が真摯に話し合い、最善の対応をし、業務自体に影響が出なかった参考になる事例

〇インシデント対応は「初動対応および調査」「対外的対応」「復旧および再発防止」があるが「対外的対応」としての費用が明確になったといえる事例。自社でのインシデントを想定すると、さらに「初動対応および調査」「復旧及び再発防止」が加わるため、実際に何をしなければならないか、委託先の対応と参考として自社のセキュリティ対策の見直しにつながる理想的な事例

NO.13　委託先のランサムウェア感染（その３）

業種	小売業		委託先のランサムウェア感染 ～委託先被害を契機とした対策向上～
地域	近畿		
従業員規模		～20名	
		20名～999名	
	○	1,000名～	

（１）事案概要

○業務の委託先がランサムウェア感染

○委託先が管理していた、自社（委託元）の顧客情報について、情報漏えいのおそれ

（２）発覚経緯

○委託先からの連絡

（３）時系列

年月	備考
2024年M月D日	委託先から、ランサムウェアによるサイバー攻撃を受けて個人情報漏えい等の可能性があるとの報告
2024年M月D＋6日	公式HPにおいて、委託先へのサイバー攻撃の結果、個人情報が漏えいした可能性がある旨を公表
2024年M月D＋11日	委託先から「調査が難航しており、事態報告のスケジュール見込みが立っていない」との報告
2024年M月D＋14日	公式HPにおいて、委託先からの報告内容を転記する形で、状況の追加報告を実施。
2024年M＋1月	委託先から「これまでの調査結果において、ヒアリング対象会社に関する個人情報漏えいの事実は確認されていない」旨の報告
2024年M＋1月	公式HPにおいて個人情報漏えいの事実は確認されていない」ことを報告

（４）被害内容

〇結果として「個人情報漏えいの事実」は確認されておらず、その観点での被害無し。
〇但し委託先からの報告を受け、個人情報漏えいの可能性がある旨を公表したため、同公表内容に関する対応・コストが発生した。また報告から1か月程度、委託先のシステムが利用できなくなり、その分の代替策対応のコストも発生した。

（５）被害額

合計：79万円

＋　利益喪失：不明

※委託先のシステムが1か月ほど利用できなくなったため、その代替作業をヒアリング対象会社社内で実施した際にかかった人件費を基に算出

（６）委託先への損害賠償請求の実施有無等

委託先への損害賠償請求は実施せず

（７）被害者コメント

〇委託先からの貰い事故であったこともあって、自社で個人情報漏えいおそれの件数把握をすることができなかった。このようなインシデント発生時には、改めて自社で把握することができるようにする必要がある。
〇インシデント収束後、委託先から今回のインシデント発覚時の対応方針や対応内容について、詳細を説明してもらう場を作ってもらえたが、非常に参考になる内容であった。委託先でのインシデント対応について、しっかり考えていきたい。
〇インシデントがVPN絡みであったことを踏まえ、社内VPNの刷新を検討開始

（８）WG所感

〇二次被害であったため、再発防止策はあまり検討されていない印象
〇一方、他人事という意識はなく、委託先のランサムウェア感染事案がVPN起因であったということを知って自社でもVPN刷新の検討を開始するなど「当事者意識」をもって、何らかの取り組みをしていこうとされている姿勢が感じられた。

Ⅴ　参考文献・資料

[1] 中小機構：日本を支える中小企業
https://www.smrj.go.jp/recruit/environment.html

[2] 経済産業省統計局：令和3年経済センサス-活動調査 調査の結果
https://www.stat.go.jp/data/e-census/2021/kekka/index.html

[3] 警察庁：サイバー空間をめぐる脅威の情勢等
https://www.npa.go.jp/publications/statistics/cybersecurity/

変更履歴

Version	日付	修正内容
1.00	2025/7/23	Ver1.00公開