インシデント損害額調査レポート

別紙「被害組織調査」

IDIR Incident Damage Investigation Report

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、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を対象とした「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2023年9月に実施しました。このレポートでは、同調査を行うにあたり集計した国内のサイバー攻撃被害組織の統計情報と、同調査の結果をまとめています。

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．調査の対象組織数、期間、収集方法

（１）対象組織数

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約1,300組織

（２）対象期間

2017年1月から2022年6月までの5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

本紙でも記載したとおり「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、今回の調査では、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、ブログなど情報も参考としています。

（２）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ているマルウェア。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。

（３）ウェブサイトからの情報漏えい

ECサイトを主とするウェブサイトを通じた情報漏えい被害です。発生する二次被害の規模を考慮し、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に分けて集計しています。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。

（４）その他

ランサムウェア、エモテット以外のマルウェア感染被害のほか、単なるいたずらなど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。

３．集計結果

調査対象とした国内の約1,300組織について、規模、業種、公表数の年別傾向、サイバー攻撃種別を集計、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。

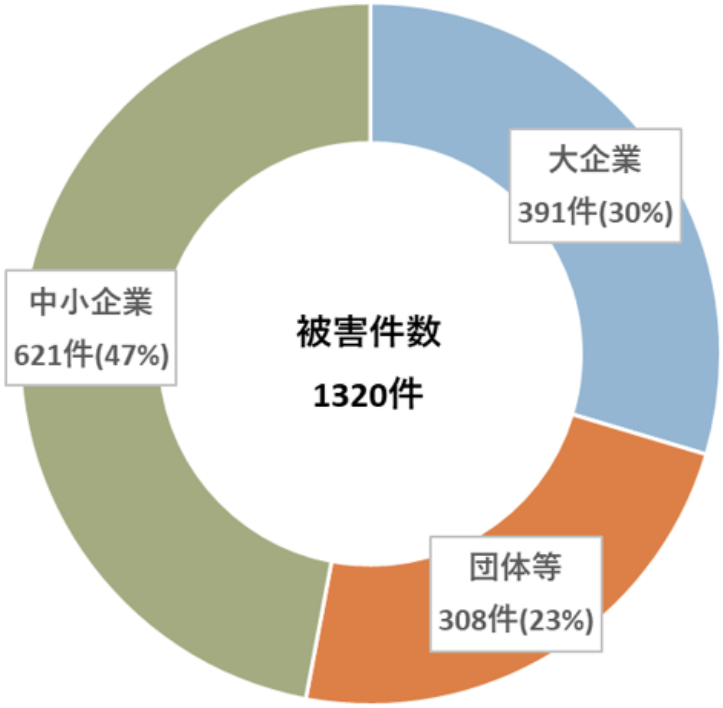
（１）全体（約1,300組織）のデータ

① 規模

被害組織の規模別件数・割合は図Ⅱ-1のとおりです。大企業以外（中小企業、団体等）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被害公表に積極的ではないと推定され、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（全体）の規模別割合

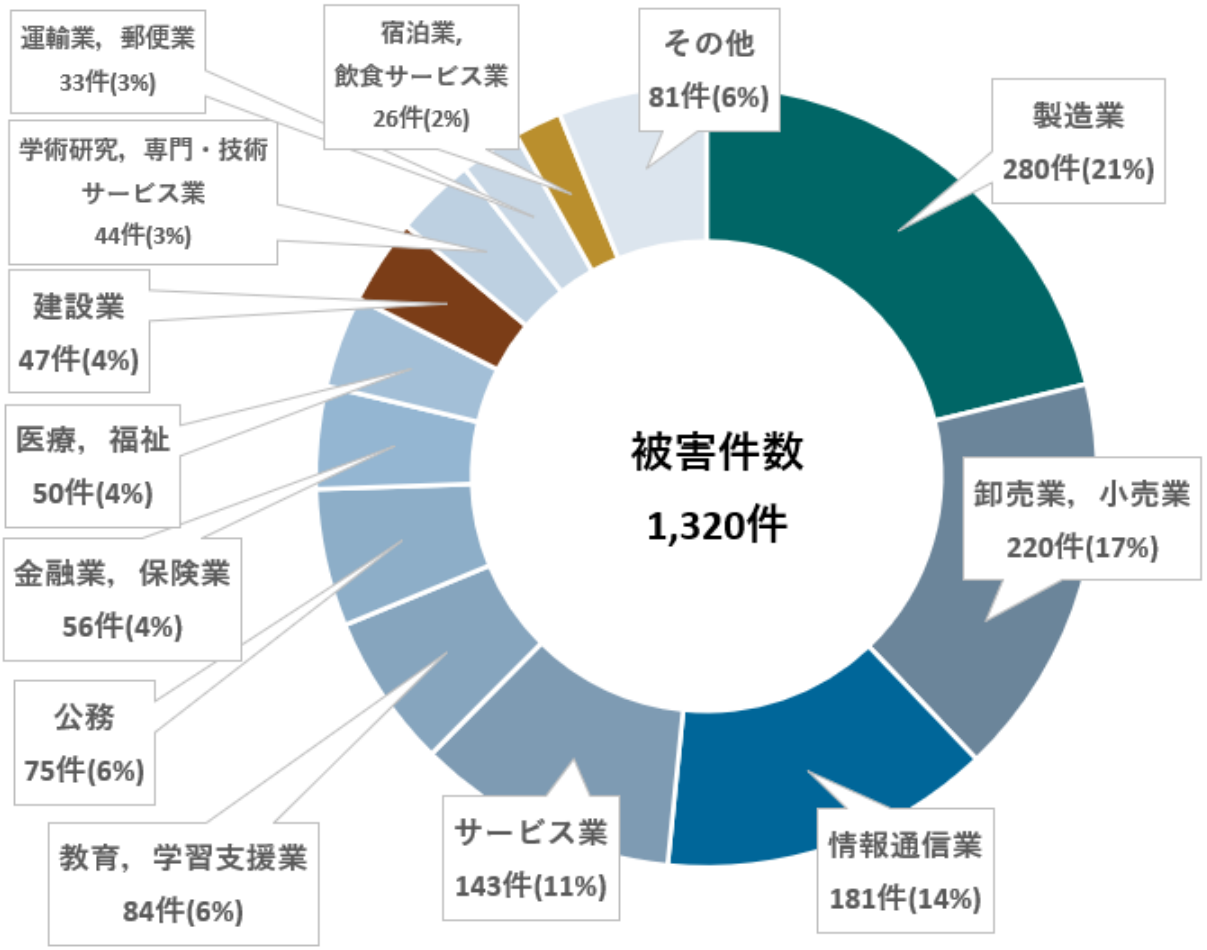
② 業種

被害組織の業種別件数、割合は図Ⅱ-2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。

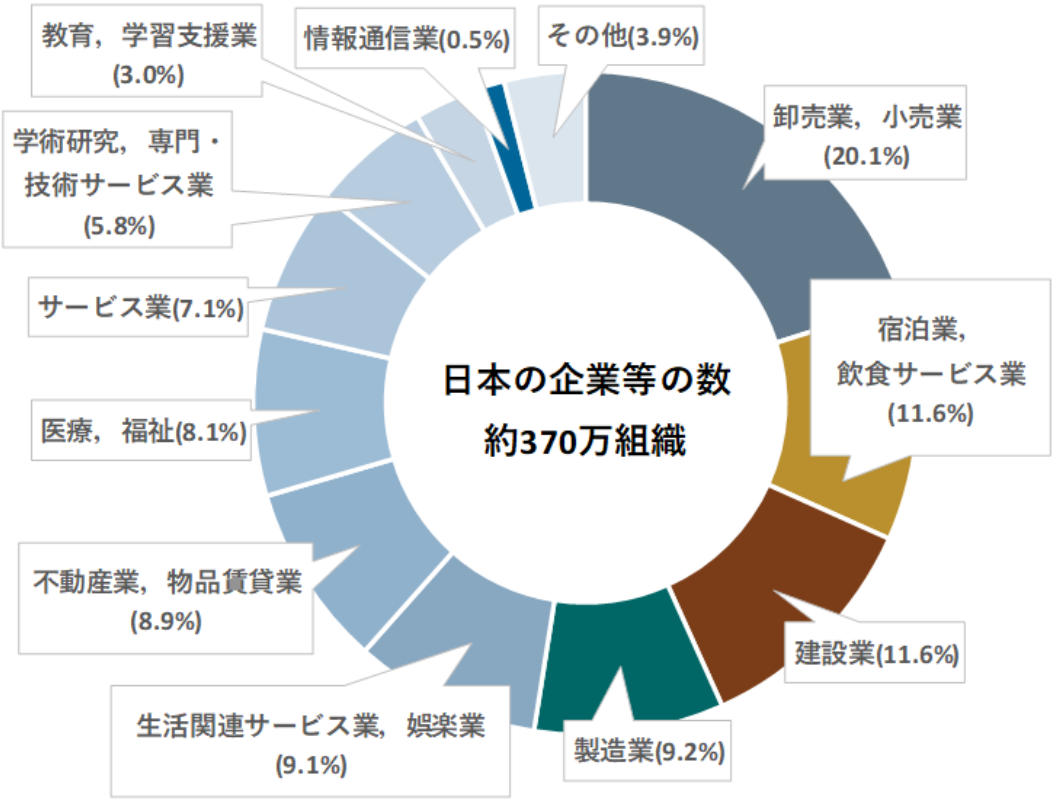
なお、このような業種別件数、割合をみる場合、国内企業全体の業種別割合も考慮する必要があります。次頁の図Ⅱ-3は「令和3年経済センサス-活動調査 調査の結果[2]」に基づき作成した、国内企業全体の業種別割合です。

２つの図を比較した場合、製造業や情報通信業では被害組織の割合が高いこと（例えば、製造業は、被害組織での割合が21%、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では被害組織の割合が低いことが見てとれます。

サイバー攻撃を受けやすい業種、受けにくい業種があることはさておき、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、小規模事業者の割合が多く被害公表のなされない業種があるということも理由として推測されます。



図Ⅱ-2 被害組織業種別割合

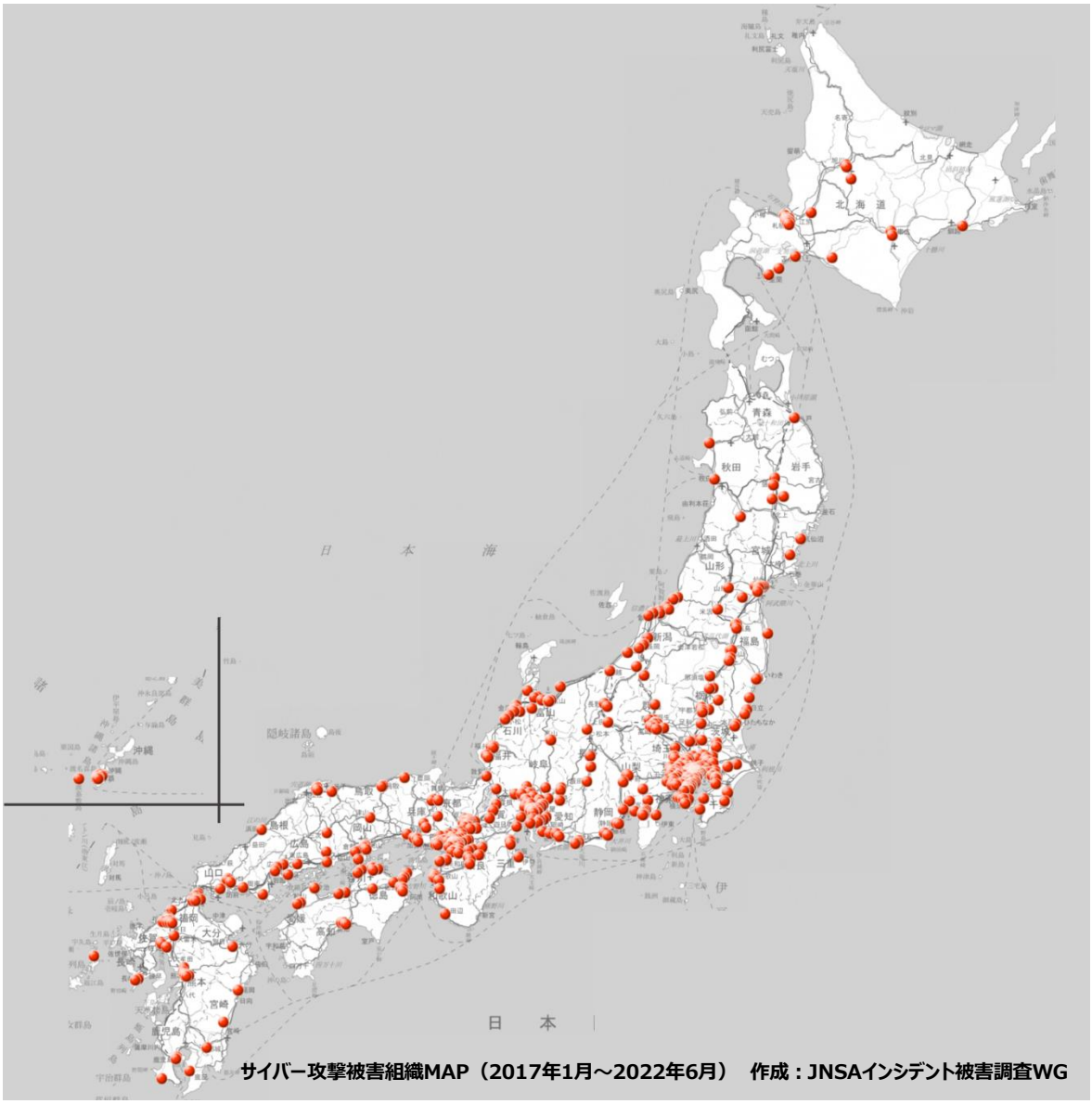


図Ⅱ-3 国内企業全体の業種別割合

③　所在地分布

被害組織をマッピングした結果は図Ⅱ-4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、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を分母とした被害組織の割合を鑑みても、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。

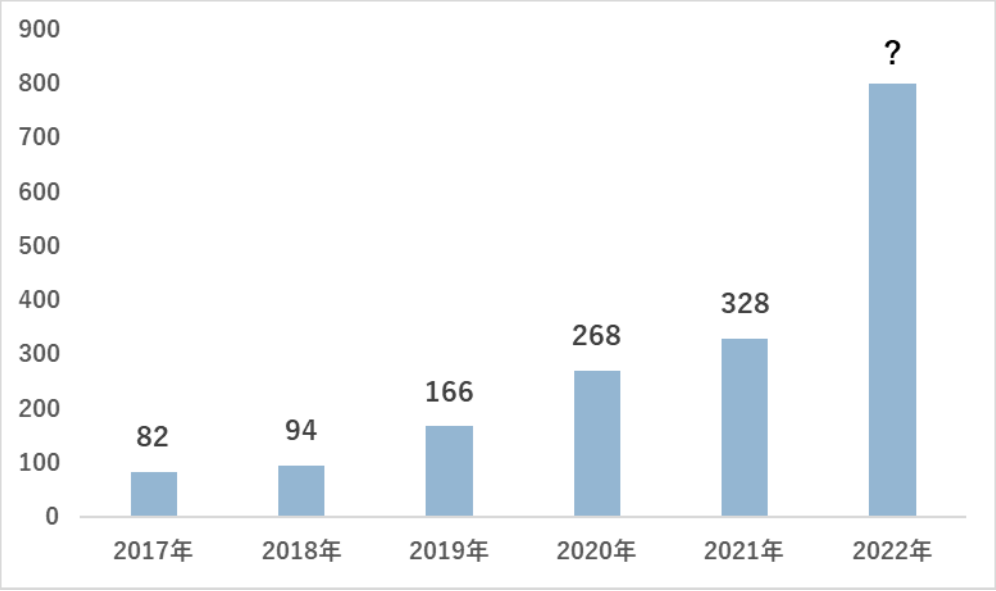


図Ⅱ-4　サイバー攻撃被害組織の所在地分布

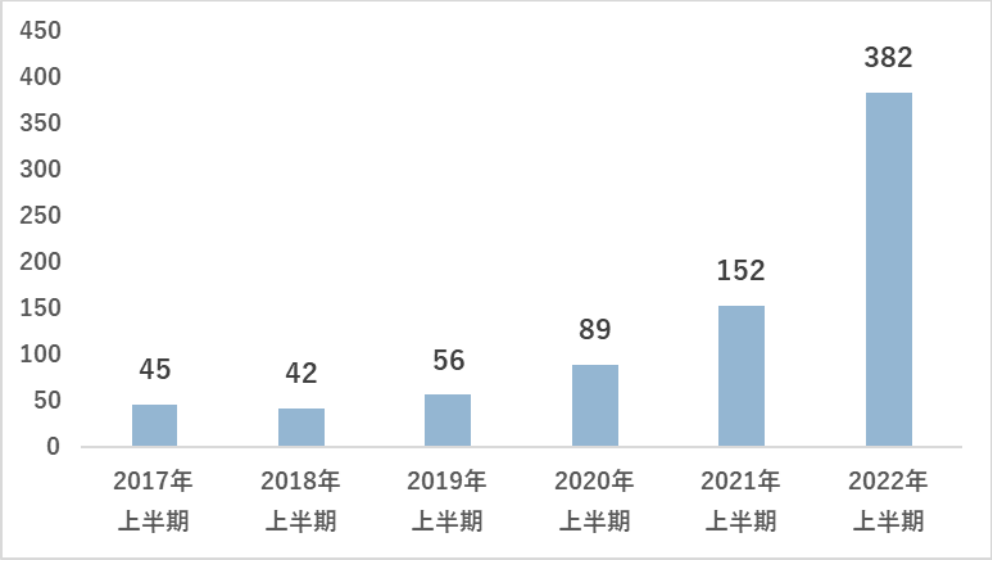
④　被害組織による公表件数の年別推移

今回調査対象とした約1,300組織における年別の公表件数は次のとおりで、図Ⅱ-5は年別、図Ⅱ-6は上半期別（2022年は上半期のみの数字のため作成）となります。

報道・公表を実施する組織が年々増加していることが読み取れます。サイバー攻撃の増加もさることながら、2022年4月に施行された改正個人情報保護法の影響（被害者本人への通知が必要となったためホームページ等で公開する組織が増加したと推定）などにより、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ます。



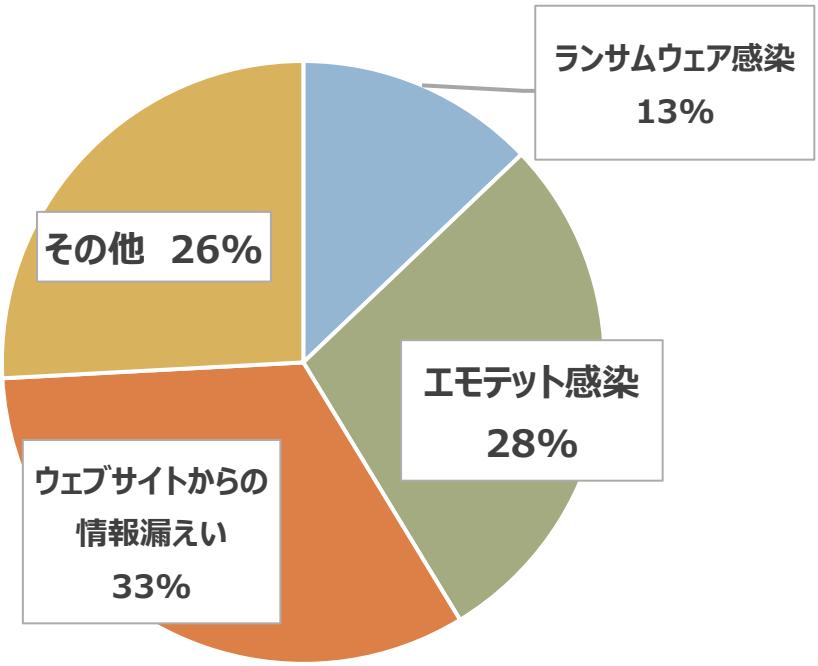
図Ⅱ-5 サイバー攻撃の公表件数の年別推移



図Ⅱ-6 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

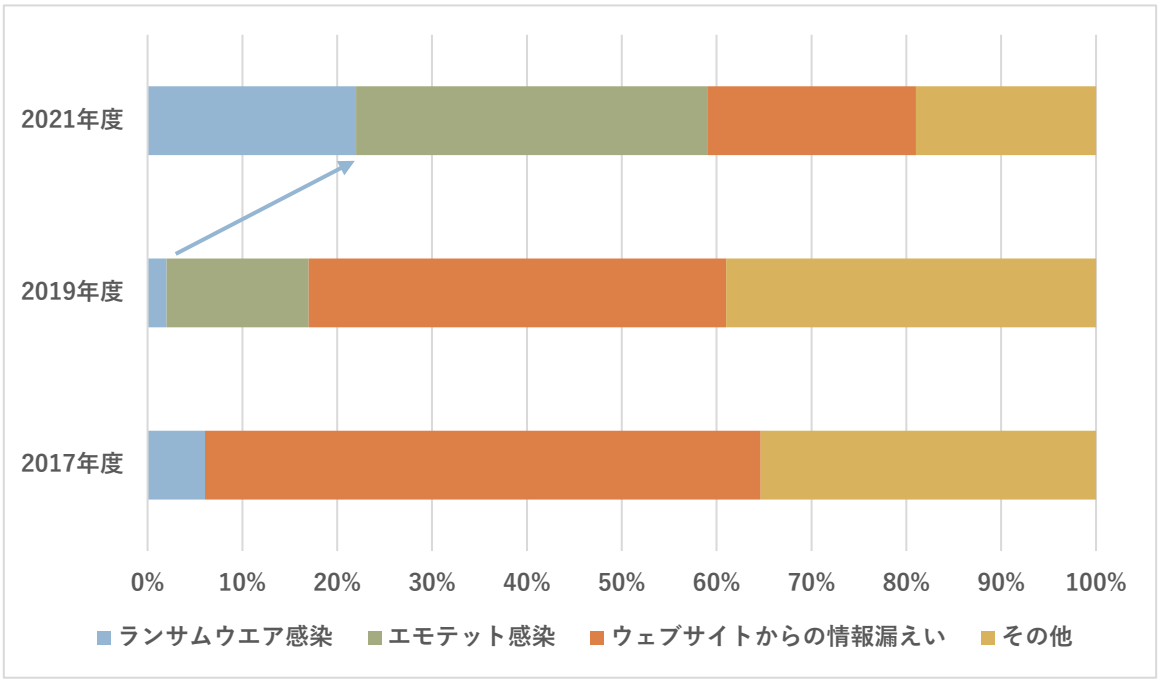
サイバー攻撃の種別構成は図Ⅱ-7のとおりです。「ランサムウェア感染」「エモテット感染」「ウェブサイトからの情報漏えい」が全体の7割を占めていることが分かります。ただし、サイバー攻撃の被害としてこれら3つの事象が多いということではなく、取引先・顧客への影響の大きさ等から、報道・公表がなされることが多いということが推測されます。



図Ⅱ-7 サイバー攻撃の種別構成（通年）

⑦ サイバー攻撃種別の年度別推移

公表されたサイバー攻撃種別を、2017年度から2年ごとに集計した結果は図Ⅱ-8のとおりです。被害件数の増加ほか、その種別構成も変容していることが分かります。「ランサムウェア感染」「エモテット感染」の被害公表が占める割合の変化が目立ちます。特に2019年度から2021年度のランサムウェアによる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[3]」の結果と同様の傾向を示すところです。



図Ⅱ-8 サイバー攻撃種別の年度別推移

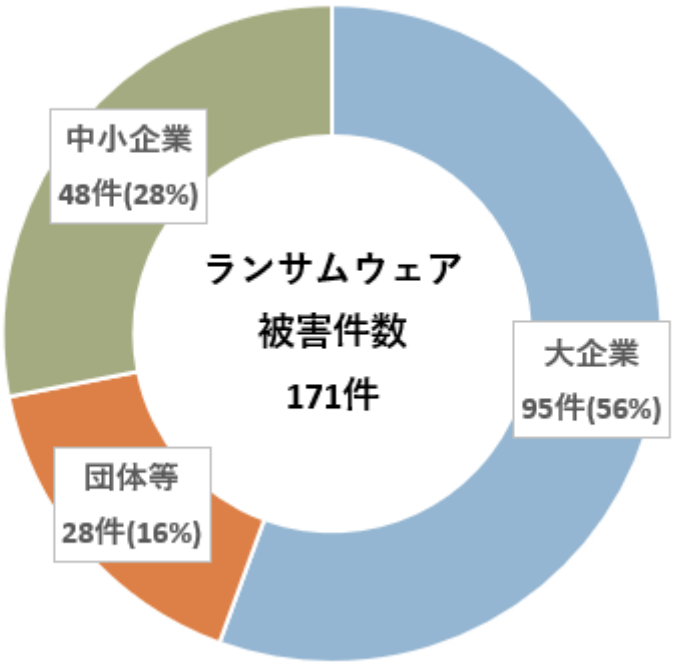
（２）サイバー攻撃ごとのデータ

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-9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、この違いは「（１）全体（約1,300組織）のデータ」で記載したとおり、被害公表を控える中小企業が一定数いることが理由として推定されます。



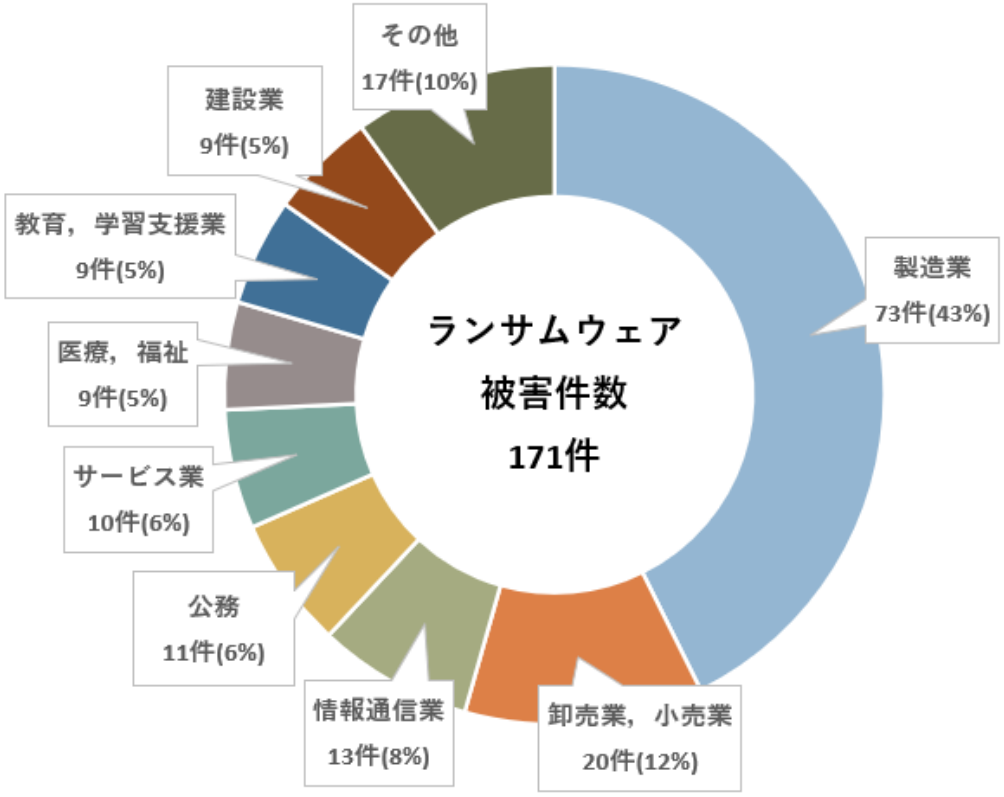
図Ⅱ-9 ランサムウェア被害組織の規模別割合

イ．業種

ランサムウェア被害組織の業種別件数、割合は図Ⅱ-10のとおりです。

製造業での被害が全体の43%を占め、大きく目立つ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が推定されます。その意味で完成品メーカーに迷惑をかけてはいけないという心理が働く、原材料・部品メーカー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。

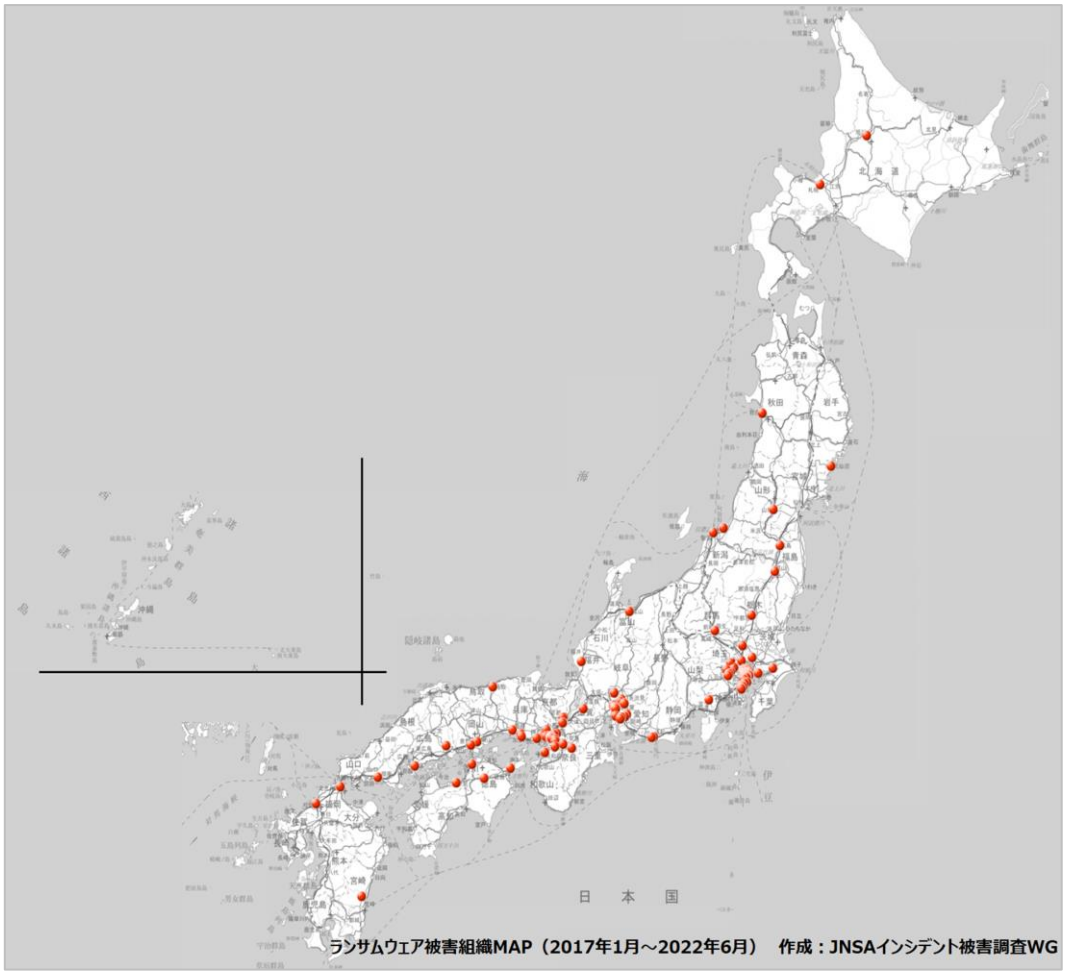


図Ⅱ-10 ランサムウェア被害組織の業種別割合

ウ．所在地分布

被害組織をマッピングした結果は図Ⅱ-11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-11 ランサムウェア感染組織の所在地分布

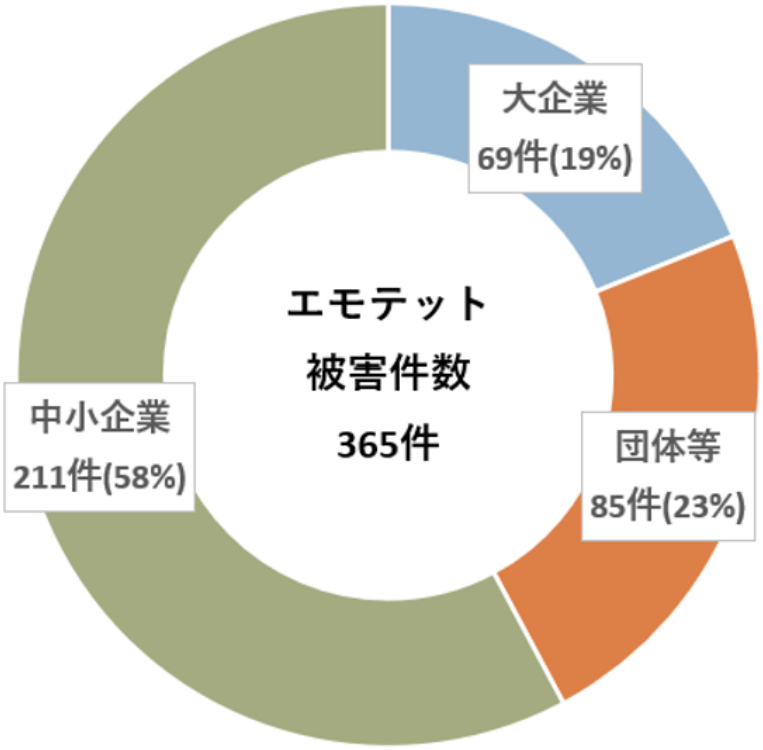
② エモテット感染

ア．規模

エモテット感染被害組織の規模別件数・割合は図Ⅱ-12のとおりです。

中小企業で発生した被害が全体の58%を占めています。

日本国内においてエモテットは感染拡大活動を活発に行う期間と、大きな活動が見られない休眠期が断続的に繰り返されていますが、大企業においてはエモテット流行初期に対策を実施した組織が多いと考えられる一方、中小企業には対策が追い付いていない組織が一定数いることなどが理由と推測されます。



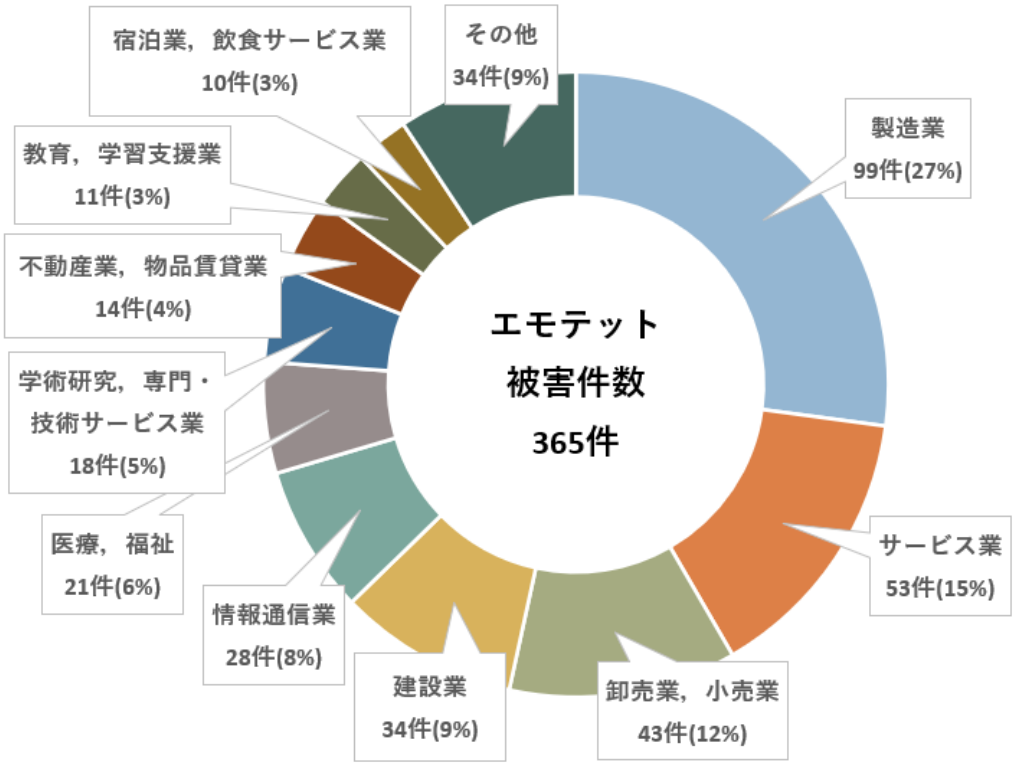
図Ⅱ-12 エモテット被害組織の規模別割合

イ．業種

エモテット被害組織の業種別件数、割合は図Ⅱ-13のとおりです。

他のサイバー攻撃に比し、比較的、サービス業、建設業の件数が多いという結果になっています。サービス業については、集計データ上は、政治・経済・文化団体での事例が多く散見されました。

サービス業については構成員経由で感染、建設業については下請の協力会社における同業他社経由で感染が推測されます。

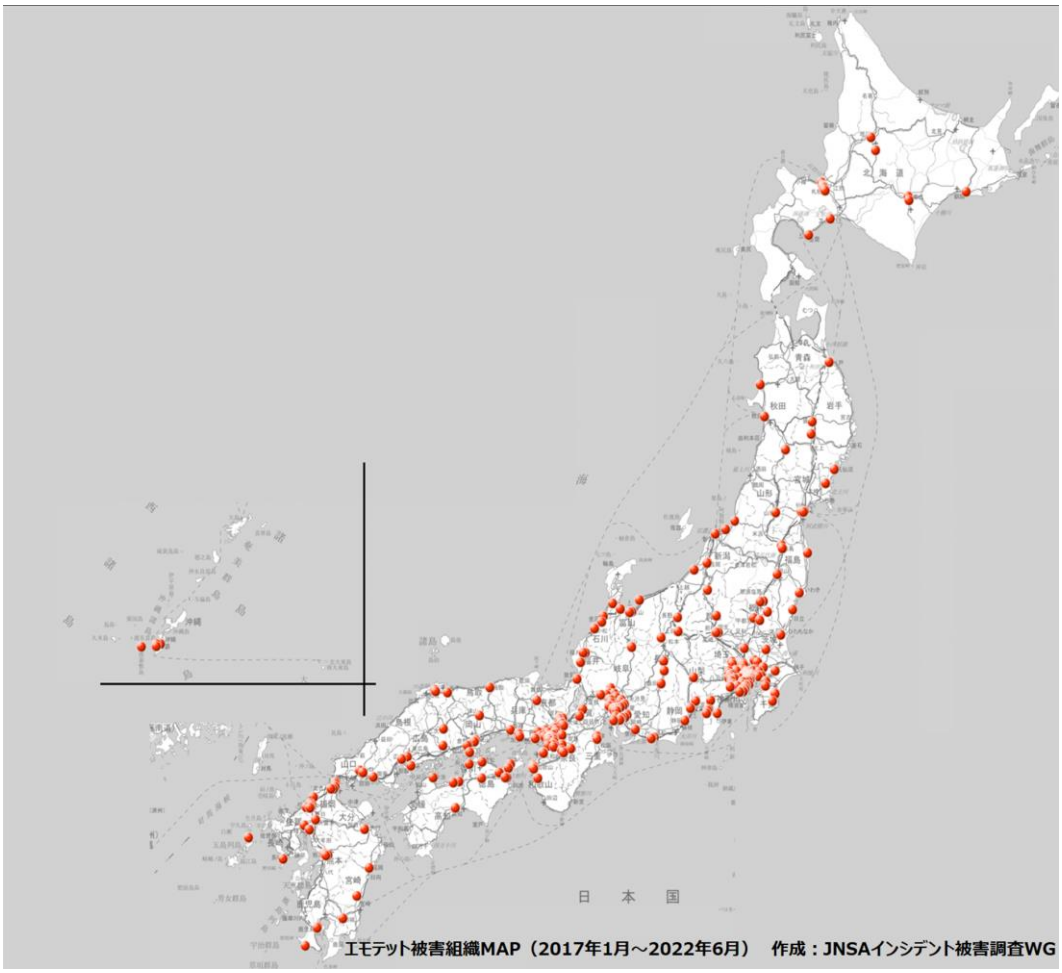


図Ⅱ-13 エモテット被害組織の業種別割合

ウ．所在地分布

被害組織をマッピングした結果は図Ⅱ-14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、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を分母とした被害組織の割合を鑑みても、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-14 エモテット感染被害組織の所在地

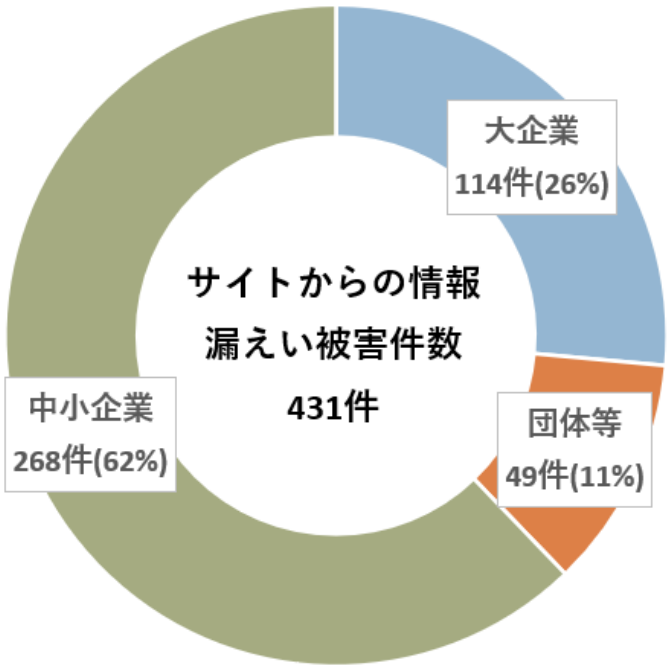
③ ウェブサイトからの情報漏えい被害

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-15のとおりです。中小企業で発生した被害が全体の62%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て、CMS（コンテンツマネジメントシステム。ウェブサイトを管理するシステム）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。



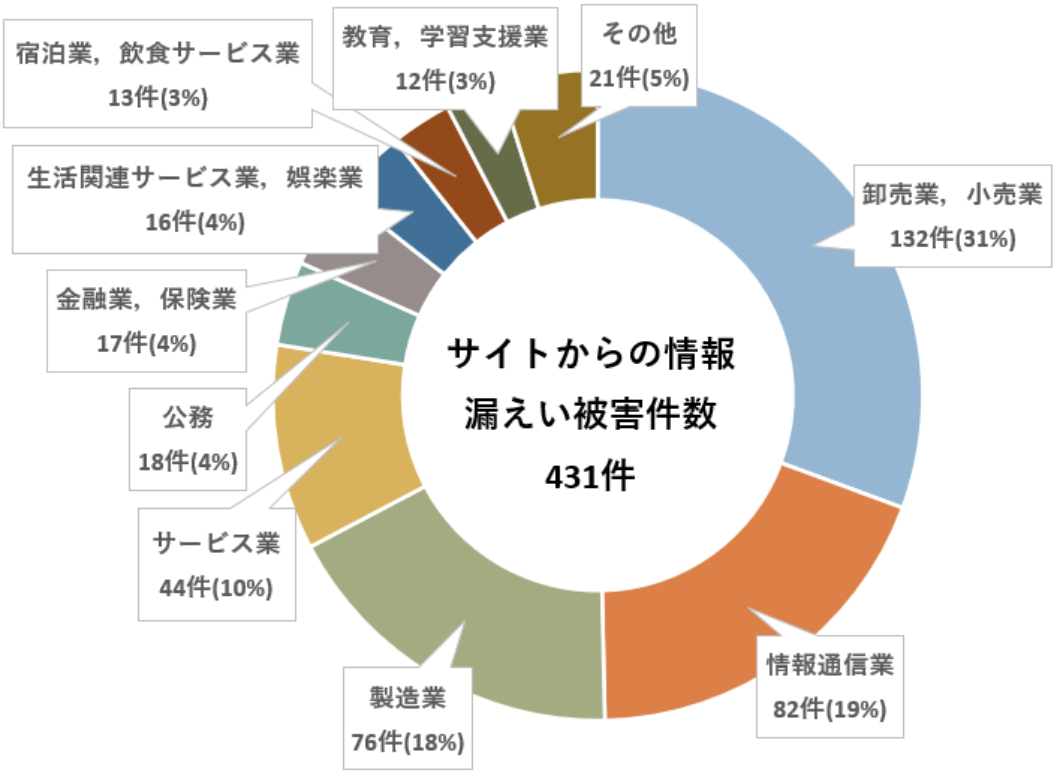
図Ⅱ-15 ウェブサイトからの情報漏えい被害組織の規模別割合

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、割合被害組織の業種の割合は、図Ⅱ-16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（製造・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サイトで販売を行う卸売業、小売業、製造業や、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-16 ウェブサイトからの情報漏えい被害組織の業種別割合

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
調査期間	2023 年7 月 24 日から 9月30 日
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：70件（回答率：約6%）

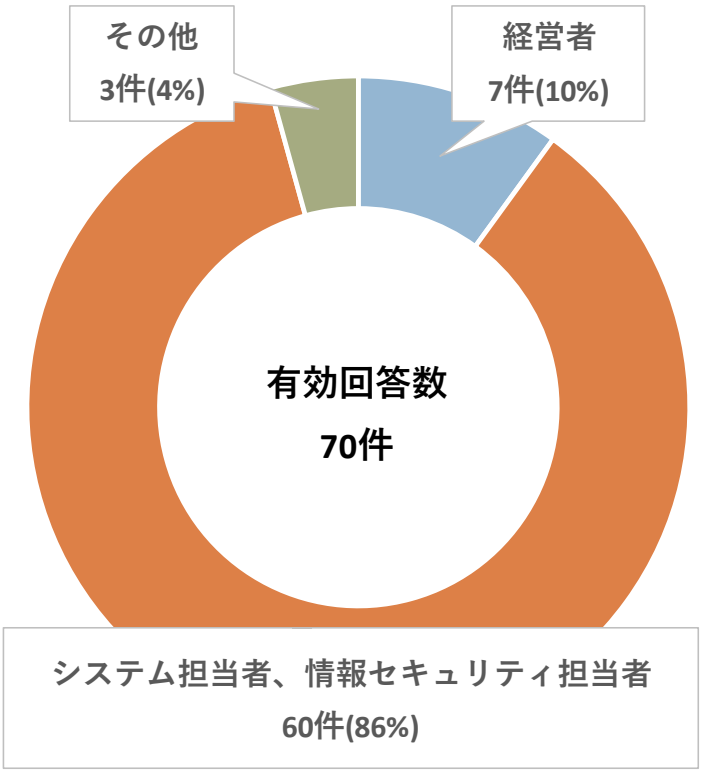
２．主なアンケート項目

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
- 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

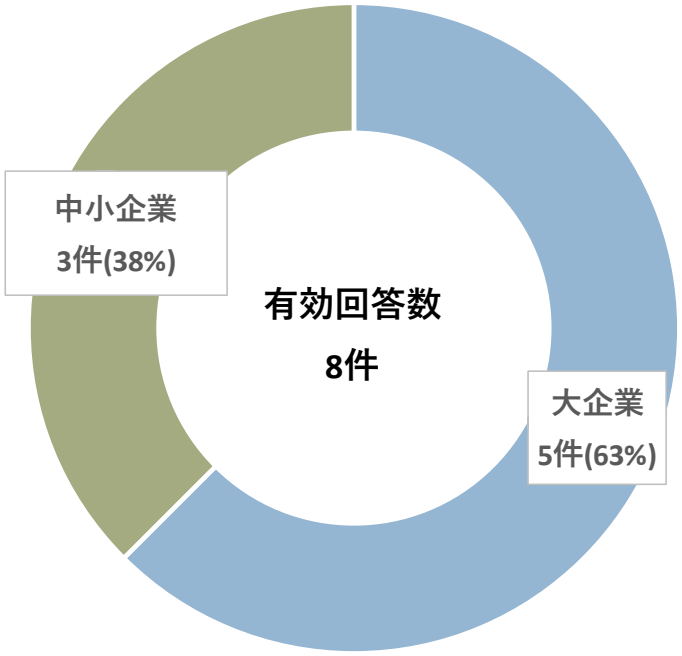
アンケート回答者の属性（立場や職種）の内訳は、図Ⅲ-1のとおりです。



図Ⅲ-1 回答者の属性

４．ランサムウェア感染被害組織の被害金額

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8件でした。回答した被害組織の規模別内訳は、図Ⅲ-2のとおりです。



図Ⅲ-2 ランサムウェア感染被害：回答組織の内訳（企業・団体等の規模別）

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**2,386万円**でした。しかし、被害組織の多くが、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、データの消失による利益の喪失、機会損失などによる損害額の全体は把握していない旨を回答しており、回答された被害金額に計上されていません。また、被害組織が事故対応に要した内部工数（人月）（注）は回答の平均値が**27.7人月**でしたが、組織内部の従業員や職員による対応に要したコストが被害金額に計上されていないケースが多々見られました。このため、実際に被害組織が被った金銭損害の実態は、より大きな金額であることが推測されます。なお、アンケートに回答したすべての被害組織がランサムウェア攻撃者に対して身代金は支払っていないと回答していたことを書き添えておきます。

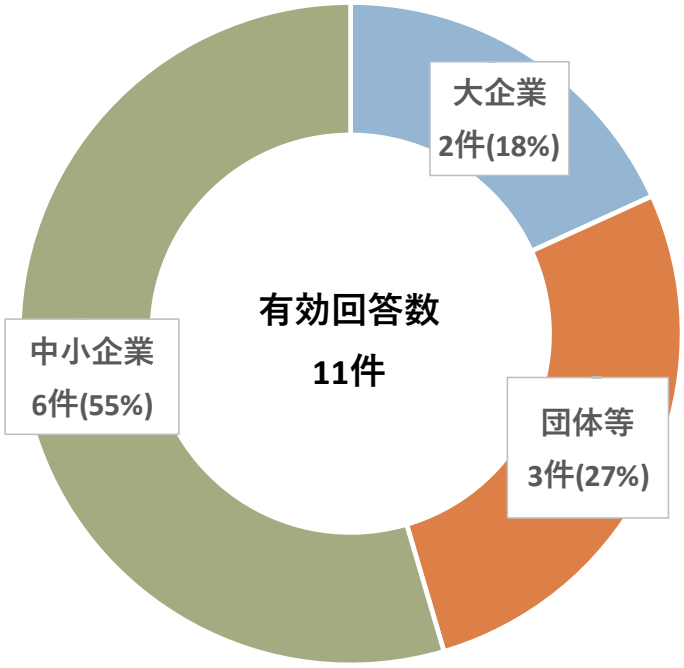
（注）1人が1ヶ月間働いた作業量を1とするもの。
例）10人が業務時間の半分を3ヶ月費やした場合、10人×50%×3ヶ月＝15人月

〇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ませんでした。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、組織内のNASに保存していたバックデータも暗号化されてしまったという回答も見られるなど、バックアップデータも暗号化されてしまったケースも見られました。

５．エモテット感染組織の被害金額

エモテット感染被害組織からのアンケート回答数は11件でした。回答した被害組織の規模別内訳は、図Ⅲ-3のとおりです。



図Ⅲ-3 エモテット感染被害：回答組織の内訳（企業・団体等の規模別）

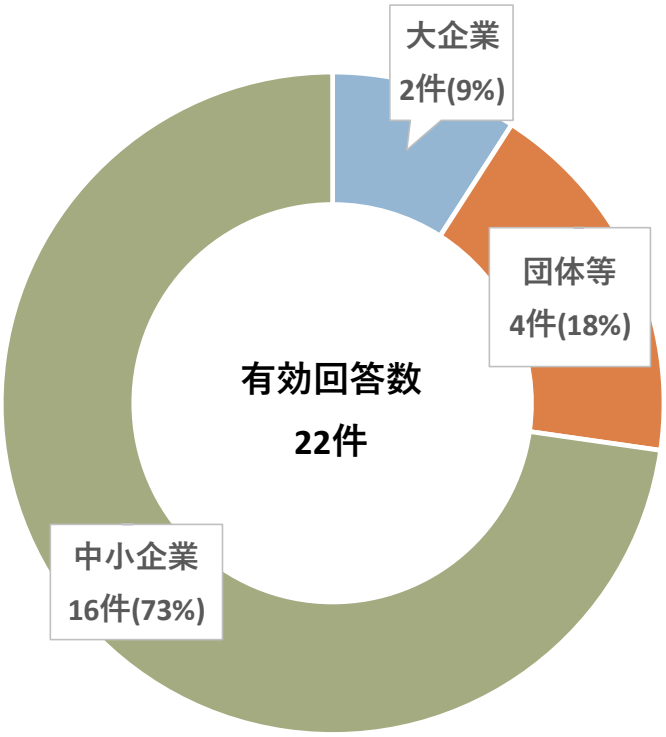
エモテット感染被害を受けた組織にて生じた被害金額は回答組織ごとに大きな開きがありました。被害金額を2,000万円以上と回答した組織がある一方で、被害金額が極端に低い組織（数10万円以下や対応工数のみなど）も見られ、回答の平均値は**1,030万円**でした。事故原因調査や対外発表、再発防止策をしっかりと行った組織と、感染端末の再インストールのみを行った組織に分かれた結果と推測されます。また、被害組織が事故対応に要した内部工数（人月）は、回答の平均値が**2.9人月**でした。ランサムウェア被害と同様に、組織内部の従業員や職員による対応に要したコストが被害金額に計上されていないケースが多々見られました。

○取引先・顧客からの連絡で感染が発覚した組織は約半数

被害発覚の経緯に関するアンケート回答11件のうち、「自組織で感染に気付いた」と回答した組織は6件でした。残り5件のケースは「取引先・顧客からの指摘によって発覚した」と回答されています。エモテットは感染端末のメーラーに保存されている情報を窃取・悪用し、正規のメールと判別が困難な攻撃メールを送信する手口を使用することが知られています[4]。こうした攻撃メールを受信した取引先・顧客など外部からの指摘・問合せによって感染が発覚することが多いこともエモテット感染被害の特徴です。

６．ウェブサイトからの情報漏えい被害組織の被害金額

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22件でした。回答した被害組織の規模別内訳は、図Ⅲ-4のとおりです。



図Ⅲ-4 ウェブサイトからの情報漏えい被害：回答組織の内訳（企業・団体等の規模別）

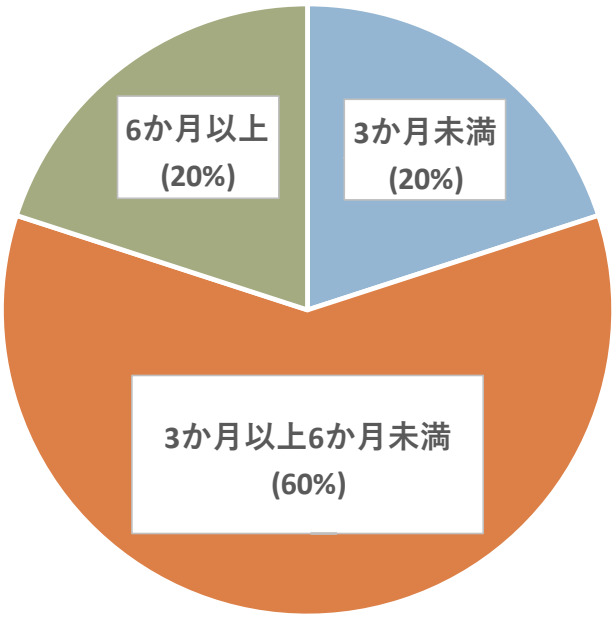
ウェブサイトからの情報漏えい被害を受けた組織にて生じた被害金額は漏えいした情報の内容により大きな開きがありました。個人情報のみが漏えいした被害における、被害金額の回答平均値が**2,955万円**だったのに対し、漏えいした情報にクレジットカード情報が含まれている被害における被害金額の回答平均値は**3,843万円**でした。また、被害組織が事故対応に要した内部工数（人月）の回答平均値は、個人情報のみが漏えいした被害の場合は**13.3人月**、クレジットカード情報を含む情報漏えい被害の場合は**13.5人月**でした。他の被害項目と同様に、組織内部の従業員や職員による対応に要したコストが被害金額に計上されていないケースが多々見られました。なお、組織

内部の従業員や職員による対応に要したコストは、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ませんでした。

漏えい情報にクレジットカード情報を含む被害と個人情報のみの被害の金額を比較すると、賠償損害の項目で大きく差異がありました。差異の内容としては、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ます。

７．クレジットカード情報を含む情報漏えい被害

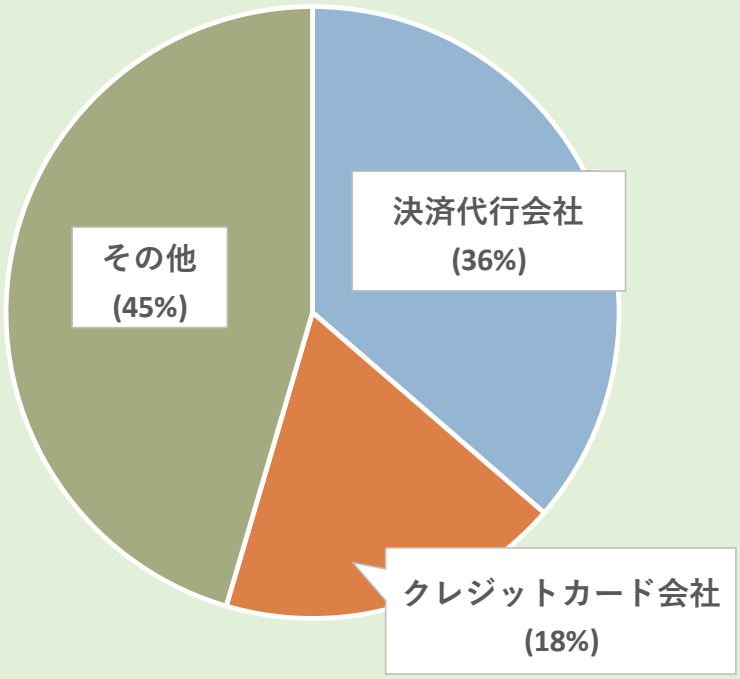
クレジットカード情報を含む情報漏えい被害の損害額が大きくなる要因の一つに、被害発生から問題解決までの間に、クレジットカード決済を停止せざるを得ないことによる機会損失があります。クレジットカード情報を含む情報漏えいの被害組織の多くは、ECサイトを運用しており、クレジットカード決済の停止は売り上げの減少に直結するケースが多いためと推測されます。アンケートに回答したクレジットカード情報の漏えい被害組織のクレジットカード決済を停止した期間の内訳は図Ⅲ-5のとおりです。被害組織の80％が3ヶ月以上、クレジットカード決済を停止したと回答しています。



図Ⅲ-5 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-6のとおりです。



図Ⅲ-6 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。1ヶ月から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てみました（次頁以降）。

エモテット感染、ランサムウェア感染それぞれにつき、2組織、合計4組織のインタビューとなっています。

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 ○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

（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

○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。

○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。

○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。

○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

○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、Web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。

〇インデント対応に関し、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。

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。

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ヶ月から2ヶ月、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

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。データを暗号化された。
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。被害がないことは後日確認された。
〇被害を受けた社内システムの復旧には２ヶ月を要した。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ヶ月を要した。

（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

（注）本件は今回のアンケート調査の対象期間外の事例であるが、接点をもつメンバーからの依頼により、ご好意によりヒアリングを実施したものとなります。

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/

[4] IPA：Emotet（エモテット）攻撃の手口
https://www.ipa.go.jp/security/emotet/attack.html

変更履歴

Version	日付	修正内容
1.00	2024/2/9	Ver1.00公開