日本のサイバーセキュリティを「連携」「学び」「創造」

インシデントが発生するといったいいくらかかるのか

～インシデント損害額調査レポートについて～

調査研究部会 インシデント被害調査WG

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)
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

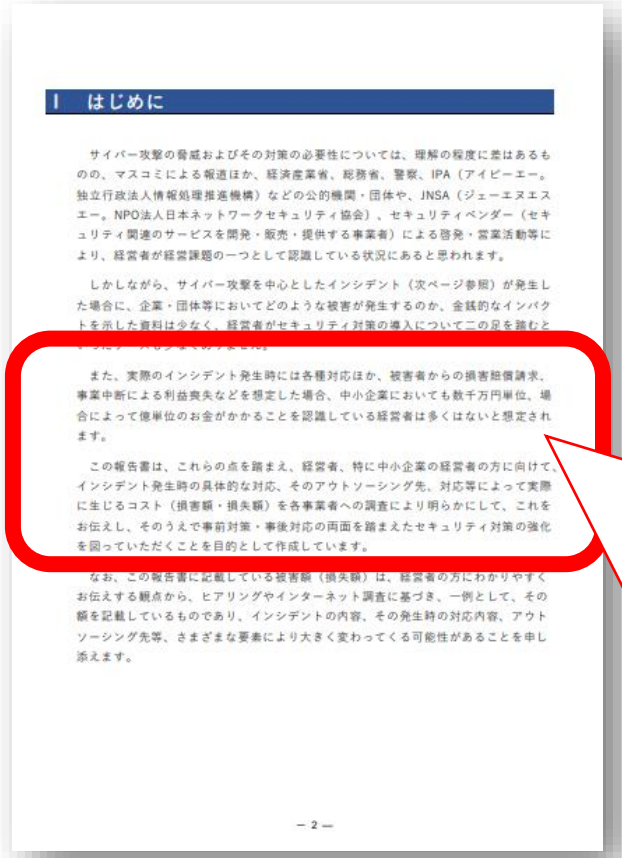
- 損保業界の商品開発部門に20数年勤務
- 入社以来、IT関連の保険（現サイバー保険）などの開発に携わる
- ここ５、６年はサイバー保険の企画・開発・推進を担当
- JNSAにて、今年8月「インシデント損害額調査レポート」を公表したが、そのWGリーダーを務める

目的

～本レポートの意図するところ～

レポートの目的（＆結論）

レポート「はじめに」



Ⅰ　はじめに

サイバー攻撃の脅威およびその対策の必要性については、理解の程度に差はあるものの、マスコミによる報道ほか、経済産業省、総務省、警察、IPA（アイピーエー。独立行政法人情報処理推進機構）などの公的機関・団体や、JNSA（ジェーエヌエスエー。NPO法人日本ネットワークセキュリティ協会）、セキュリティベンダー（セキュリティ関連のサービスを開発・販売・提供する事業者）による啓発・営業活動等により、経営者が経営課題の一つとして認識している状況にあると思われます。

しかしながら、サイバー攻撃を中心としたインシデント（次ページ参照）が発生した場合に、企業・団体等においてどのような被害が発生するのか、金銭的なインパクトを示した資料は少なく、経営者がセキュリティ対策の導入について二の足を踏むというケースも多いのではないでしょうか。

また、実際のインシデント発生時には各種対応ほか、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した場合、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を認識している経営者は多くはないと想定されます。

この報告書は、これらの点を踏まえ、経営者、特に中小企業の経営者の方に向けて、インシデント発生時の具体的な対応、そのアウトソーシング先、対応等によって実際に生じるコスト（損害額・損失額）を各事業者への調査により明らかにして、これをお伝えし、そのうえで事前対策・事後対応の両面を踏まえたセキュリティ対策の強化を図っていただくことを目的として作成しています。

なお、この報告書に記載している被害額（損失額）は、経営者の方にわかりやすくお伝えする観点から、ヒアリングやインターネット調査に基づき、一例として、その額を記載しているものであり、インシデントの内容、その発生時の対応内容、アウトソーシング先等、さまざまな要素により大きく変わってくる可能性があることを申し添えます。

－ 2 －

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**のお金がかかることを認識してる経営者は多くはないと想定されます。

経営者の方に～、実際に生じるコストを～お伝えし、**セキュリティ対策の強化を図っていただく**ことを～

インシデントの概要

～インシデントとは、対応の流れ、発生時に生じる損害～

インシデントとは

「インシデント（incident）」とは、「事件」「出来事」といった意味をもった語

情報セキュリティの世界では、システムの運用におけるセキュリティ上の問題として捉えられる事象（これらに繋がる可能性のある事象を含む）を意味する。

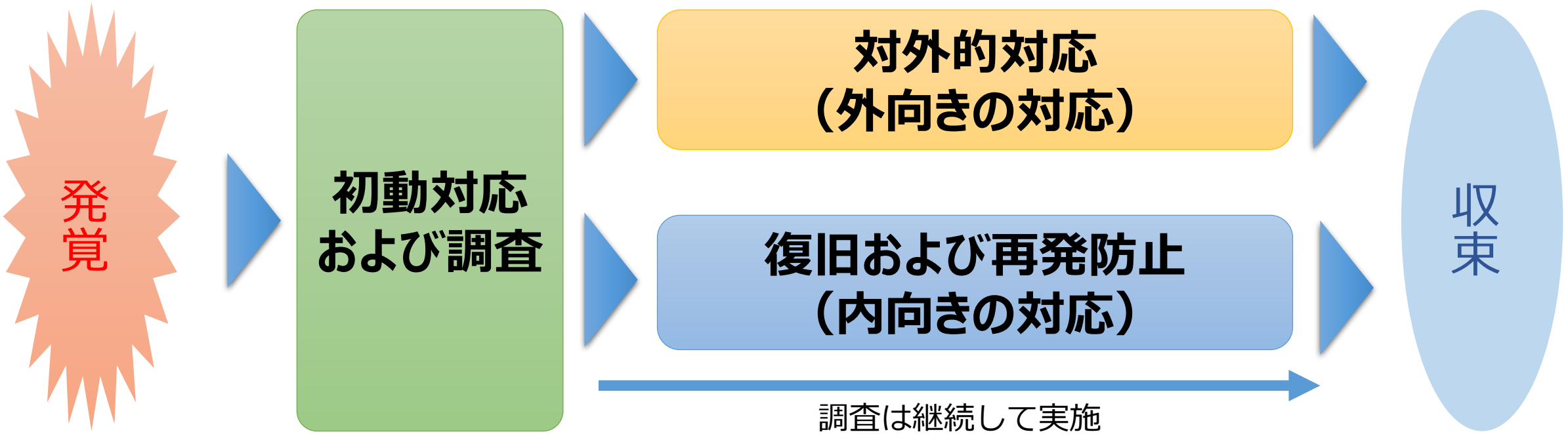
インシデントの一例

○マルウェア感染
○DoS攻撃/DDoS攻撃
○ウェブサイトの改ざん
○従業員の持ち出しなど内部不正
○自然災害等による機器の損壊
○機器の故障
○電子メール、FAX、郵便物の誤送信・誤発送
○PCの紛失、USBメモリなどの記録媒体の紛失

等

インシデント発生時の対応の流れ

３つのステップにカテゴライズ



インシデント発生時において生じる損害

６つの損害にカテゴライズ

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）**
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**

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自社で直接、
費用を負担することにより被る損害

初動対応および調査

事故原因・被害範囲調査費用

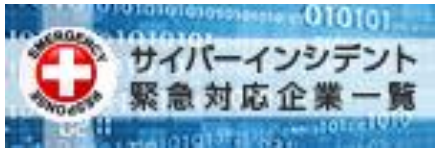
◆対応

・速やかに、**初動対応**として、ネットワークの遮断、証拠保全等の着手が必要

・その後、インシデントの内容の分析・調査、
特にサイバー攻撃の場合は**フォレンジック調査**（注）が必要

（注）電子媒体の中に残された証拠を解析し、事故原因や影響・被害範囲の特定などの調査

◆アウトソーシング先
インシデントレスポンス事業者



※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

◆コスト

３，４百万円～

対外的対応（外向きの対応）

コンサルティング費用

◆対応

・顧客、取引先などに、インシデントの概要、対応方針等を示していく必要あり
・二次被害を勘案した慎重な対応が必要
・危機管理・メディア対応を行う専門業者へ依頼することが無難

◆アウトソーシング先

危機管理コンサルティング会社（PR会社）

◆コスト

数十万円～

対外的対応（外向きの対応）

法律相談費用

◆対応

・リーガル面（個人情報保護法等の各種関係法令を勘案した対応）を考慮する必要あり

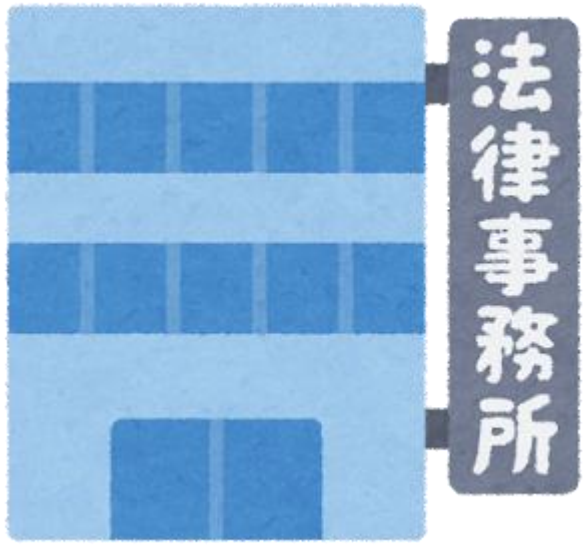
・法律事務所へ依頼するのが通例

◆アウトソーシング先

法律事務所

◆コスト

数十万円～



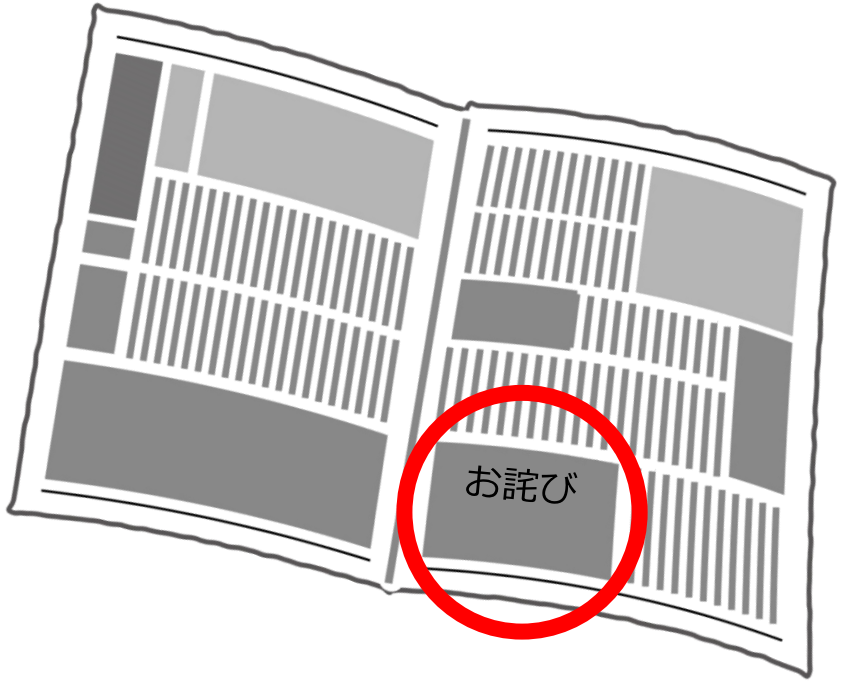
対外的対応（外向きの対応）

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送付等の必要あり
・新聞への出稿の検討必要性も

◆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
はがき80円～、封書100円～
・新聞（10cm2段）
全国紙240万円前後、地方紙50万円前後



対外的対応（外向きの対応）

コールセンター費用

◆対応

・被害者やその家族だけでなく、その企業のすべての顧客、部外者等からの問い合わせに対応するため、電話による受付体制を整備する必要あり

・煩雑さ、業務の停滞を踏まえれば、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**120万円～**

⇒３か月対応、初月はオペレーター３席、

２か月目以降は１席でも、**600万円～**

対外的対応（外向きの対応）

見舞金・見舞品購入費用

◆対応

・情報漏えい事故が発生した場合、我が国においては、損害賠償金とは別に、お詫びの一環として見舞金・見舞品を送付するケースがある。

・券面額の500円のプリペイドカードを送付することが多い（多かった？）。

・否定的に受け止める被害者も一定数おり、対応の是非については慎重な判断が必要

◆アウトソーシング先

プリペイドカード販売事業者

◆コスト

作成料、送料を踏まえると１枚**650円～**

対外的対応（外向きの対応）

ダークウェブ調査費用

◆対応

・自社以外の関係者にも大きな影響が発生するような情報が漏えいしたときは、これら関係者からの要請があることも含め、ダークウェブ上でその情報がやり取りされていないかを確認することの検討も必要

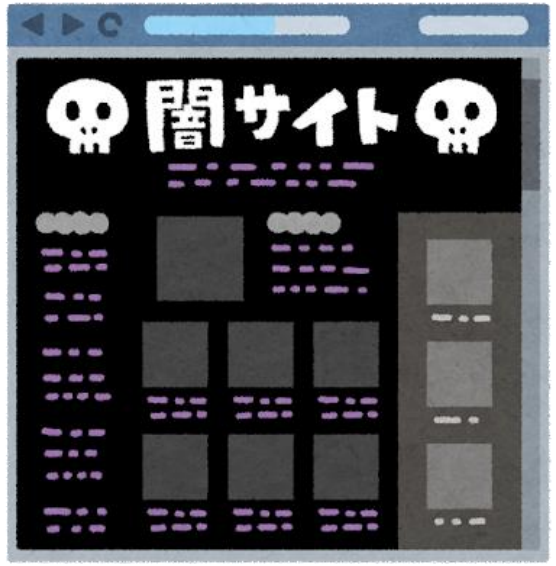
・ダークウェブの調査は、高度な専門性を要し、専門の事業者（ダークウェブ調査会社）への委託が必要

◆アウトソーシング先

ダークウェブ調査会社

◆コスト

数百～数千万円



復旧および再発防止（内向きの対応）

システム復旧費用

◆対応

・情報システムが消失・改ざん・損傷した場合、データ復旧が必要。場合によってはハードウェアの復旧費用も…。

・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

データ量、復旧を要する機器の範囲等その対応規模によって大きく異なることから、費用はケースバイケース

復旧および再発防止（内向きの対応）

再発防止費用

◆対応

・収束に向けて重要となるのは、再発防止の対応。今後の再発を防ぐためその防止策を講じる必要あり

・再発防止策は内向きの対応であると同時に、顧客、取引先等の関係者に対する外向きの対応ともいえる。

◆アウトソーシング先

セキュリティベンダー等

◆コスト

再発防止策により、費用はケースバイケース

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

損害賠償金

情報漏えいなど、第三者に対して損害を与えた場合には
損害賠償請求がなされ、損害賠償金を支出することが想定される

区分		損害賠償請求の内容
個人情報の漏えい	自社管理	情報漏えいの被害者個人からの損害賠償請求
	他社からの管理委託	各種対応を実施した委託元からの損害賠償請求
クレジットカード情報の漏えい		クレジットカード会社からの不正利用や再発行費用にかかる損害賠償請求
他企業の機密情報の漏えい		将来利益等の損失を被った他企業からの損害賠償請求

損害賠償金のコスト

個人情報の漏えい

自社管理の個人情報
被害者個人から慰謝料等についての
損害賠償請求

個人情報漏えい1人あたりの平均損害賠償額(※)

調査年	1人あたり平均想定損害賠償額
2016年	31,646円
2017年	23,601円
2018年	29,768円
3か年平均	**28,308円**

他社から管理委託を受けた個人情報
委託元企業が実施した各種事故対応に
要したコストについて、
損害賠償請求「求償」がなされる

委託元にも一定の責任があるとして
過失相殺が認められるケースもあるが、
損害賠償金の額は
中小企業であったとしても
数千万～数億円

（※）JNSAセキュリティ被害調査WGの調査結果より作成

損害賠償金のコスト

クレジットカード情報の漏えい

カード会社から加盟店に対し再発行に要した費用や
不正利用の額についての損害賠償請求がなされる可能性

不正利用の平均被害額は１枚あたり**約10万円**

コスト（例）

クレジットカード情報が1,000件漏えいし、その30%が不正利用された場合

- 不正利用額
  1,000件×10万円×30%＝3,000万円
- 再発行手数料
  1,000件×1,100円＝110万円

合計**3,110万円**の損害賠償金が発生

出典：三井住友カード：【ヒトトキ調査】クレジットカードの不正利用被害にあった500人に聞いた！
私のカードでテーマパークのチケットが買われていた？？　https://www.smbc-card.com/mem/hitotoki/learn/survey_abuse.jsp

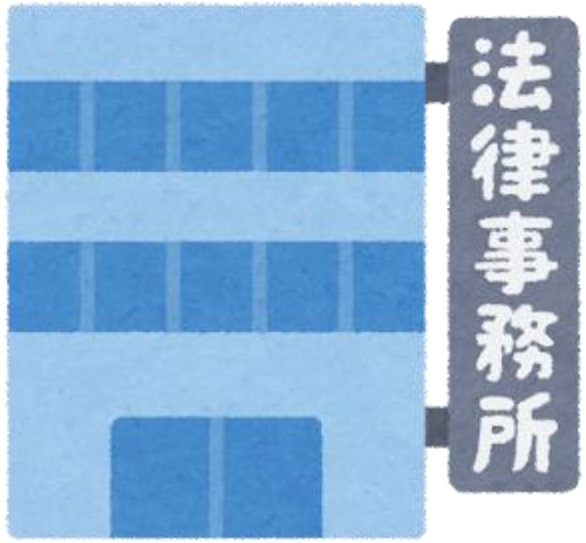
弁護士費用等その他各種費用

法的課題への対処には弁護士への委任検討が必要

訴訟に発展する前の和解交渉や訴訟に発展した場合には、
民事訴訟法に基づく訴訟費用や、
裁判に対応するための各種人件費等も発生

弁護士費用（日本弁護士連合会旧基準）

経済的利益の額	着手金	報酬金
300万円以下	８％	16%
300万円超3,000万円以下	５％＋９万円	10%＋18万円
3,000万円超３億円以下	３％＋69万円	６％＋138万円
３億円超30億円以下	２％＋369万円	４％＋738万円
30億円超	協議により決定	協議により決定



例
損害賠償請求訴訟の額が1億円である場合、

- **着手金**は**369万円**
  （１億円×３％＋69万円）
- **報酬金**は**738万円**
  （１億円×６％＋138万円）

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

事業中断による機会損失

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

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

利益損害 ≠ 売上高の減少額

変動費の支出を免れるケースでは
利益損害と売上高の減少額は一致しない

営業利益の差である1.2億円が
利益損害となる

▲0.2億円－1億円＝▲1.2億円

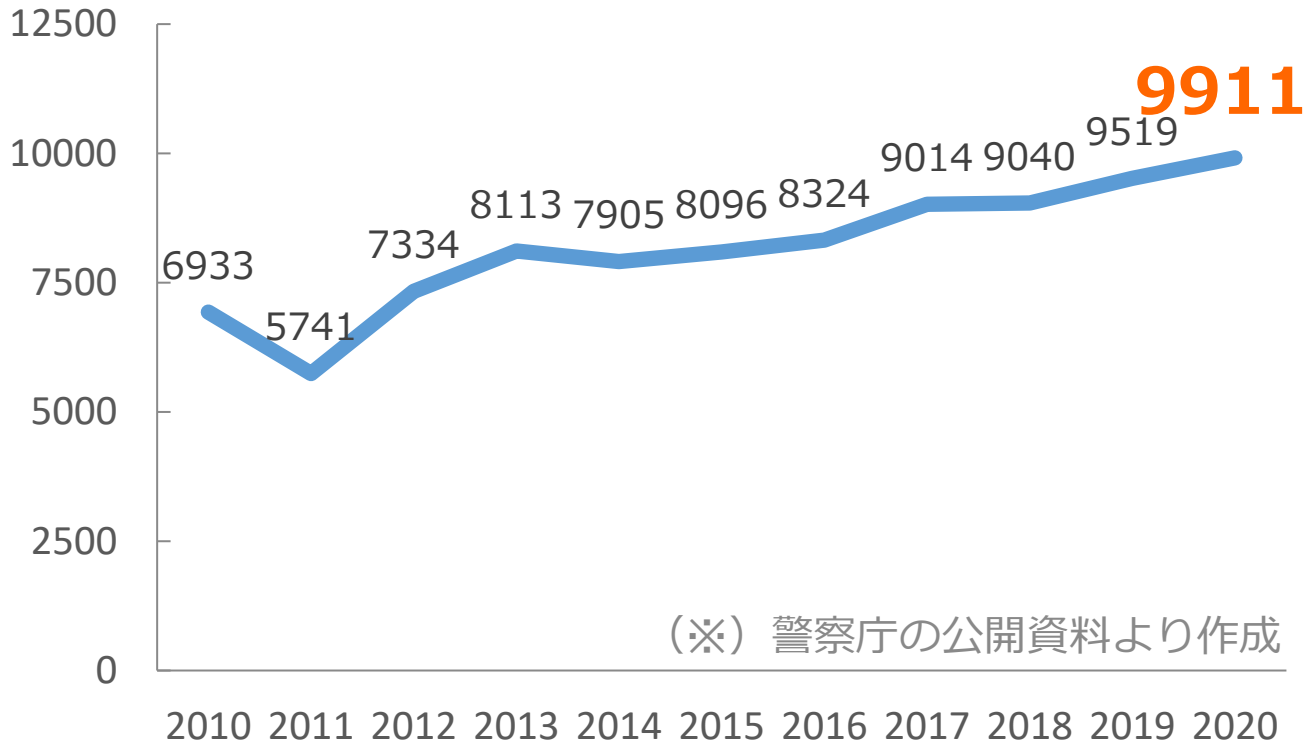
金銭損害

ランサムウェアをはじめとするマルウェア感染、ビジネスメール詐欺、
インターネットバンキングでのなりすまし等による
直接的な金銭の支払いによる損害

金銭損害

インシデントにより発生する直接的な金銭損害

サイバー犯罪検挙件数推移（国内）



サイバー犯罪の検挙件数が増加

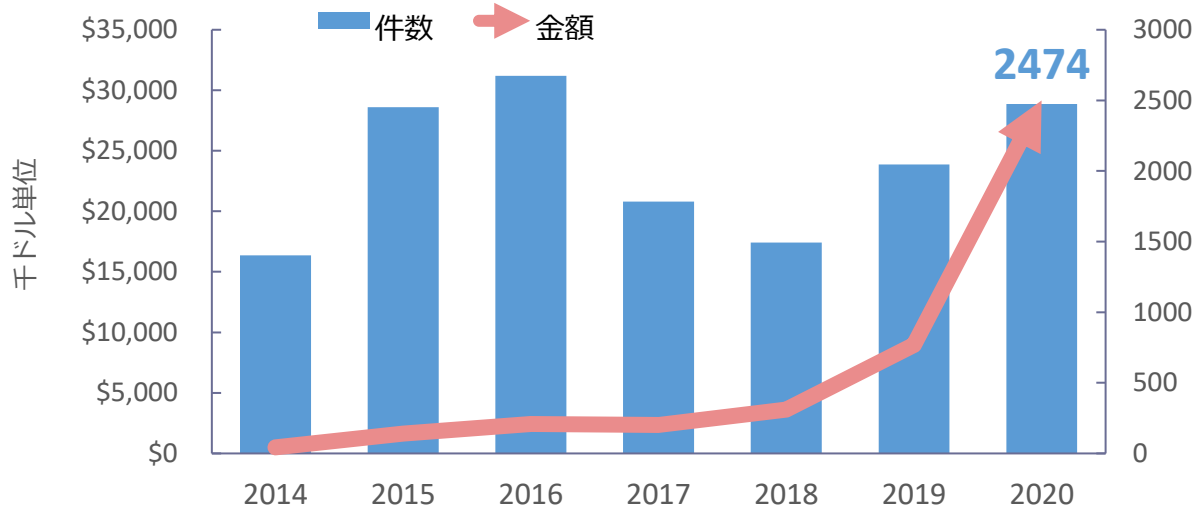
サイバー犯罪がより身近なものに
なっていることを示しており、
被害を受ける可能性が高まっている

ランサムウェアによる身代金

ファイルの暗号化、機密情報の暴露をたてに身代金要求

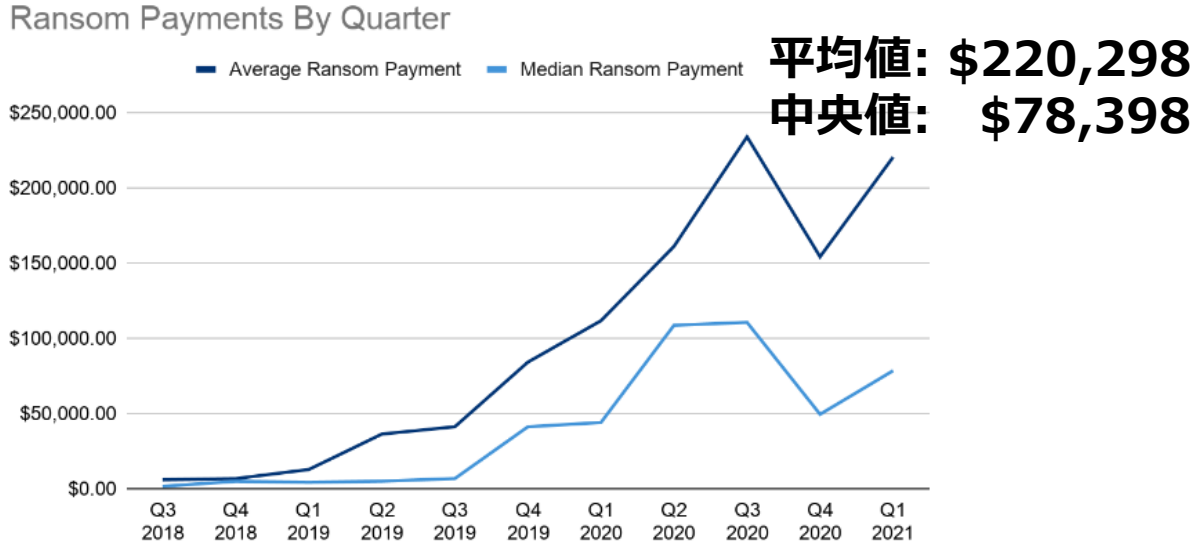
ランサムウェア攻撃者の攻撃手法の凶悪化とともに
ランサムウェア被害の発生件数と被害金額が増加
2021年1Qの身代金平均額は**$220,298（約2,400万円）**（Coveware社）

発生件数と被害金額（米国）



参考：Internet Crime Complaint Center (IC3) のデータをもとに作成
https://www.ic3.gov/

ランサムウェアによって支払われた身代金



出典：Coveware
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

ビジネスメール詐欺（BEC）

取引先などになりすました電子メールを送って送金を促す詐欺

組織内外における金銭の授受を装うため、高額な金銭損害につながりやすく、
組織が被害に遭った際の影響が大きい

コスト（損害額）
送金金額に違和感を覚えづらい、**日常的に授受される金額**の被害が多いと考えられる

国内組織に関連する被害額の大きな事例

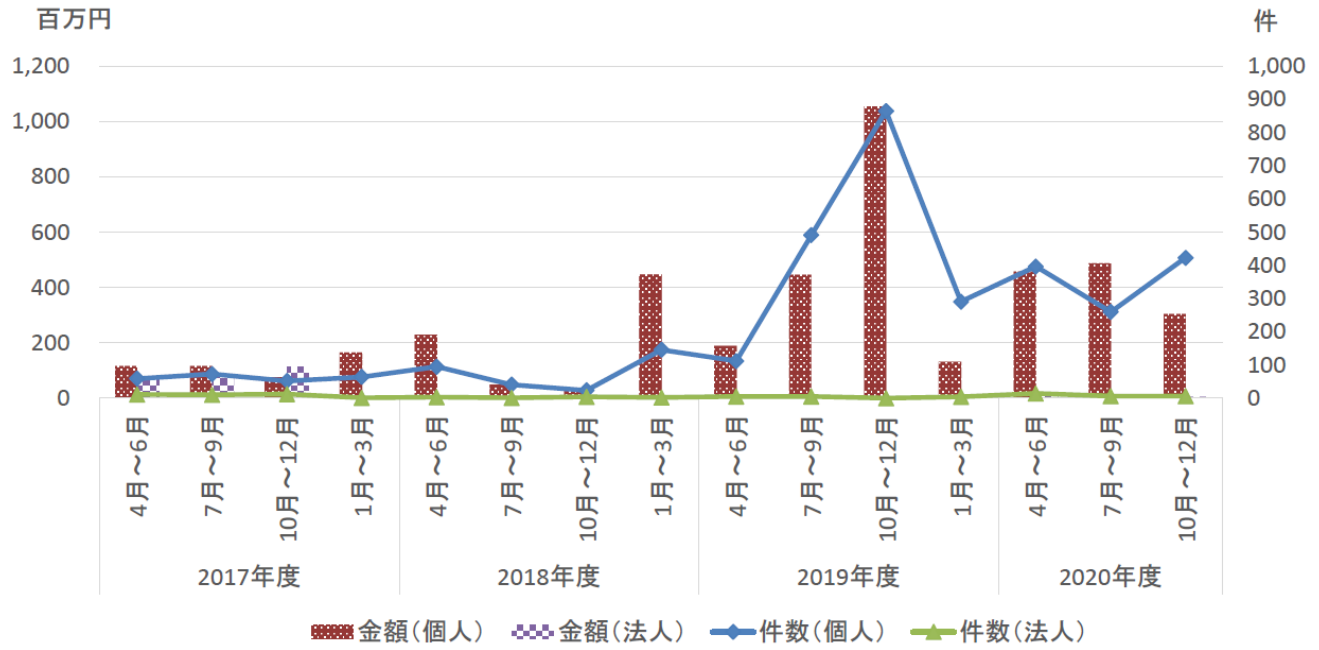
2017	大手航空会社	取引先の担当者を装った第三者からの偽メールにより **約3億8400万円**の詐欺被害
2019	大手自動車部品メーカーの 欧州の子会社	外部の第三者による虚偽の指示により**約40億円**の資金が流出
2019	大手新聞社の米国の子会社	経営幹部を装った攻撃者による虚偽の指示に基づいて、 米子会社の資金**約2,900万ドル（約32億円）**が流出

インターネットバンキングによる被害金額

インターネットバンキングの悪用による不正送金

攻撃者にインターネットバンキングの認証情報を窃取された結果、
銀行預金を不正送金・不正利用される被害が発生

法人顧客の１件当たりの平均被害額は**約140万円**（出典：一般社団法人全国銀行協会）



インターネット・バンキングによる預金等の不正払戻し件数・金額について
（出典：一般社団法人全国銀行協会）

出典：一般社団法人全国銀行協会 (2021) : 盗難通帳、インターネットバンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正利用に関するアンケート結果について https://www.zenginkyo.or.jp/news/2021/n031101/

行政損害

個人情報保護法において命令違反等により科される罰金、
GDPR（EU一般データ保護規則）等において課される
課徴金等の損害

行政損害

行政上の義務違反に対する金銭的制裁

世界各国には、個人情報保護に関する法令が存在

個人情報が漏えいした場合には、これら法令に基づき
行政当局への報告など各種対応が必要

<u>アウトソーシング先</u>

- 大手弁護士事務所
- 外資系コンサルティングファーム
- 一部のITベンダー

など

日本企業に関連する
主なプライバシー関連法令と罰則の例

地域	法令通称	罰金等の額
日本	個人情報保護法	データベース等不正提供罪、委員会による命令違反の場合、 最大1億円
EU	GDPR	違反内容により次の①または② ①「情報漏えいの発生時に監督機関へ72時間以内に報告しなかった」「データ保護責任者の任命が義務付けられているにもかかわらず任命していなかった」などの場合 最大1,000万ユーロまたは全世界年間売上高の2%のいずれか高い額 ②「個人データの処理に関する原則に違反した」「監督機関からの命令に従わなかった」などの場合 最大2,000万ユーロまたは全世界年間売上高の4%のいずれか高い額
米国 （加州）	CCPA	消費者１名あたり最大2,500ドル （故意だと7,500ドル）

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

ブランドイメージ毀損

損害の定量的な評価は困難

毀損の度合いは、その後のインシデント復旧時間や
インシデントが及ぼす影響範囲、
対象企業の対応内容等によって大きく変動

コスト（損失額）

企業の売上高に対し**数十パーセント程度**

ブランドイメージ毀損をきっかけとしたサービスの廃止・長期間の利用停止例

2019　IT企業・ファイル交換サービス	大規模な不正アクセス被害をきっかけにサービスを廃止
2019　大手流通業・バーコード決済サービス	大規模な不正利用事件によりサービスを廃止
2020　大手通信業・電子マネー口座からの不正引き出し	認証機能の不備により不正引き出し被害が発生。 一部のサービスの提供を中断

株価下落

インシデント影響が、企業の株価にまで及ぶ可能性

下落率は、発生したインシデントの復旧時間、
インシデントが及ぼす影響範囲、
対象企業の対応内容などによって大きく変動

企業の格付けに影響が及ぶと資金調達コストが
上昇する可能性も考えられる

インシデント被害と株価への影響例

2020　大手自動車メーカー・サイバー攻撃	株価が一時5%下落
2020　大手ゲーム会社・サイバー攻撃	株価が一時16%下落
2021　婚活サイト運営会社情報漏えい	株価が事件発覚前より43%下落（2021.7時点）

モデルケース

モデルケース

軽微なマルウェア感染

従業員がメールに添付されていたファイルを開いたところ、マルウェアに感染

- 至急、出入りのITベンダー経由で、インシデントレスポンス事業者に対応を依頼
  感染内容、被害範囲等の調査を実施
- 調査の結果、メールを介して感染が拡大するマルウェアであり、
  従業員端末3台とサーバー1台の感染が判明
- 個人情報の漏えいのおそれなど、
  顧客影響等はないことが確認

損害額：600万円

内訳

- 事故原因・被害範囲調査
  500万円
  - 端末3台、サーバー1台の調査
- 再発防止策：100万
  - メールフィルタリングサービスの導入

その他のモデルケース

2．ECサイトからのクレジットカード情報等の漏えい

① インシデント概要

ECサイトから、利用者の氏名、住所、クレジットカード情報、セキュリティコード等が漏えいしていることが、決済代行会社からの通報により判明した。

② 対応および被害概要

○至急、ECサイトの停止を制作会社に依頼す
されたインシデントレスポンス事業者に対
の調査を実施した。
○インシデントレスポンス事業者や決済代行会
構築システムの脆弱性が狙われ、サイトが
たクレジットカード番号などの各種情報が、
通じて10,000件漏えいしていること、さら
計で2,500万円発生していることが判明した
○顧客に被害が生じていることから、弁護士
対応方針を相談した。
○ホームページにお詫び文を掲載し、コール
委託した。また、被害者10,000人に対して
ドカードを送付した。
○ECサイトの再開までには６か月を要した。
ったため、利益損失が発生した。また、再
を大幅に強化したサイトを新たに構築する
○事態が概ね収束した後、クレジットカード
行にかかる手数料について損害賠償請求が

③ 被害額（損失額）

被害額	9,490万円
内訳	○費用損害（事故対応損害） ・ECサイトの停止にかかった費用 10万円 ・事故原因・被害範囲調査費用 300万円 ⇒サーバー１台を調査 ・法律相談費用 50万円 ⇒初回相談ほかその後の対応を委任 ・コールセンター費用 1,080万円 ⇒10～18時受付、３か月間設置。初月５名体制とし、２～３か月目は２名体制（120万円×５名＋120万円×２名＋120万円×２名） ・お詫び・見舞品送付費用 650万円 ⇒券面額500円のプリペイドカードの購入、詫び状の印刷および発送 ・ECサイトの再構築にかかった費用（再発防止策の導入を含む） 800万円 ○利益損害 3,000万円 ⇒ECサイト単体では、売上高（月間平均）1,000万円、固定費45%、変動費50%、営業利益５%の割合であった。 （1,000万円×６か月）－（1,000万円×６か月×50%）＝3,000万円 ○賠償損害 3,600万円 ⇒不正利用の額および再発行手数料についての損害賠償請求額

3．大規模なマルウェア感染

① インシデント概要

○海外子会社のサーバーがサイバー攻撃を受けた。その後、攻撃者は各種資格情報を取得したうえでネットワークへの侵入を続け、本社が管理するサーバーにアクセスするに至った。
○攻撃者はさらにネットワーク内に存在する各種データをランサムウェアに感染させ、暗号化するとともに、既に窃取したデータの
開し、データの回復およびデータの公開をやめる
うよう当該企業に要求した（二重の脅迫）。

② 対応・被害概要

○一連の攻撃の結果として、社内ネットワーク全体
のやり取りができない、生産ラインで使用するシ
荷停止せざるを得ないなど、多くの影響が生じた。
○情報システム部門を中心に、ITベンダーとの連携
ンス事業者による調査、データ復旧などの各種対
○生産ラインほか、主要なシステムは3日で復旧し
替え等が必要となり、完全な収束には３か月を要し

③ 被害額（損失額）

被害額	3億7,600万円
内訳	○費用損害（事故対応損害） ・事故原因・被害範囲調査費用 １億円 ⇒複数台の従業員端末、サーバーを調査したことに加え、EDR（セキュリティ対策製品の一種）の導入により、ネットワーク全体の監視を一定期間実施した。 ・従業員端末等の入れ替え費用 1.42億円 ⇒マルウェア感染したサーバー10台、従業員端末900台の入れ替えを実施。 サーバー　：　10台×70万円＝0.07億円 従業員端末：900台×15万円＝1.35億円 ・再発防止費用 0.5億円 ○利益損害 0.84億円 ⇒工場の1日あたりの売上高1.4億円、固定費15%、変動費80%、営業利益５%の割合であった。 （1.4億円×３日）－（1.4億円×３日×80%）＝0.84億円 ※営業支援システムが利用できないことによる営業活動の停滞に伴う利益損害なども想定されるがこのモデルケースでは割愛

さいごに

ぜひ、報告書本紙もご一読いただき、
ご活用いただけましたら幸いです