GUIDE

サイバーセキュリティインシデント最新対策ガイド

最新の脅威と損害に備える

2023.11.1

株式会社 神戸デジタル・ラボ

INTRODUCTION

はじめに

情報漏洩やサイバー攻撃など、サイバーセキュリティインシデントによる脅威が年々高まる中、その具体的な被害内容や、事前対策・事後対応の知識や準備はまだまだ会社毎に格差があります。
当資料では、その最新情報を、費用を中心に包括的に知ることで、自社が対策に取り組む足がかりとしていただくことを目的としています。

当資料の目的

- ✓ サイバーセキュリティインシデントに関する最新情報を知る
- ✓ インシデントの事前対策・事後対応の概要を知る

【注釈】 ※ 当資料はJNSA（日本ネットワークセキュリティ協会）「インシデント損害額調査レポート」を参考・引用のもと作成
※ 当資料では理解促進のため、マルウェアは「コンピュータウイルス」または「ウイルス」と明記

INDEX

01

サイバーセキュリティインシデントの概要と脅威

1. サイバーセキュリティインシデントとは？
2. コンピュータウイルスと不正アクセスの脅威について

1. サイバーセキュリティインシデントとは？

主なサイバーセキュリティインシデント

サイバーセキュリティインシデントの代表例として、以下があげられます


コンピュータウイルス(マルウェア)感染


ネットワーク攻撃


迷惑メール


不正アクセス


自然災害


誤送信・誤発送


情報の改竄


機器の紛失・盗難

情報(サイバー)セキュリティインシデントとは？

情報セキュリティインシデントは、
セキュリティインシデント、セキュリティ事故
とも言い、企業や組織において、
所有している情報資産が管理者の意図しない状態におかれることを指す。

※情報資産とは、広義では、情報を格納する器(PCやスマホ、紙)とそのデータのこと

1. サイバーセキュリティインシデントとは？

特に注意すべきサイバーセキュリティインシデント

サイバーセキュリティインシデントの中でも特に注意すべきなのは以下の 2 つです

コンピュータウイルス感染

不正な行動をする目的で作成された悪意のあるソフトやコードをコンピュータウイルスやマルウェアと呼ぶ

不正アクセス

不正アクセスにより他の被害が発生するケースと、他のインシデントにより不正アクセスが発生するケースがある

この 2 つは、ITに特有の事項が多いため、インシデント発生時に備えて必要な対処や費用を自社の担当者が把握し、事前対策を検討しておくべきである

2. コンピュータウイルスと不正アクセスの脅威について

コンピュータウイルスと不正アクセスについて

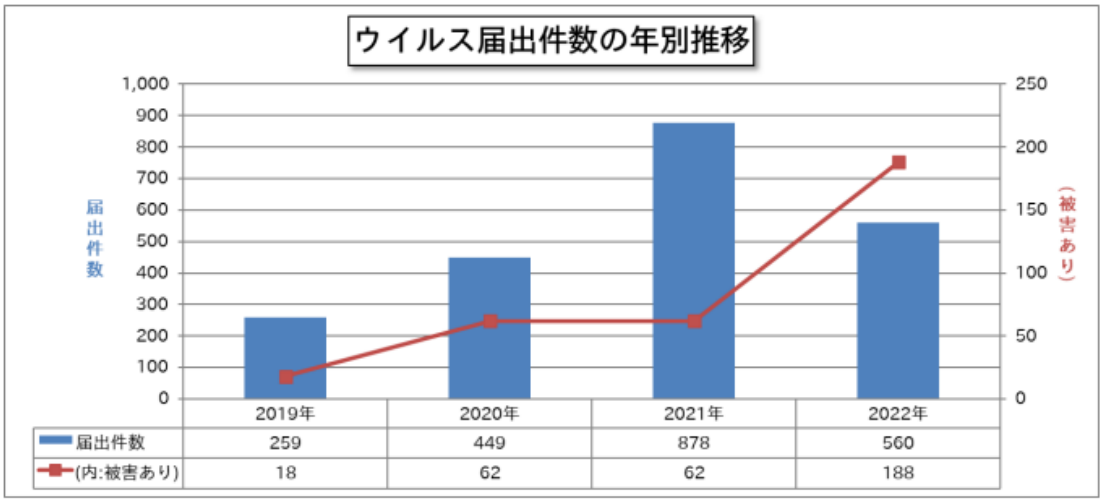
コンピュータウイルスや不正アクセスは近年増加傾向にあり、
日々の業務の中でも、その脅威が身近にあることが感じられます

セキュリティソフトの表示等から、その脅威を身近に感じやすいコンピュータウイルスや
不正アクセスだが、ソフトの検出率も100%ではないため、実際にはさらに数が多い

2. コンピュータウイルスと不正アクセスの脅威について

コンピュータウイルスの被害届提出件数

特に注意すべきインシデントである**コンピュータウイルス(マルウェア)**の
被害届提出件数は**年々増加傾向**にあります



1週間に10件の
被害届が提出！

【引用元】コンピュータウイルス・不正アクセスの届出状況 ［2022年（1月～12月）］Copyright 2023 IPA（※）

全当時者が報告しているわけではなく、IPAのアンケート調査では**6割が未公表**である。また、
攻撃されたこと自体に気づいていない被害者も考慮すると、実際は**さらに件数は多い**と想定される

※独立行政法人情報処理推進機構（IPA）は経済産業省のIT政策実施機関です。

2. コンピュータウイルスと不正アクセスの脅威について

1件でも重大化しやすいコンピュータウイルス被害

コンピュータウイルスの被害は、件数としては１件でも重大化するケースがあります

サイバー攻撃受けた部品会社に「脅迫メッセージ」…トヨタ国内全工場を停止、２日から稼働再開

2022/03/01 12:14 ウクライナ情勢　この記事をスクラップする

トヨタ自動車は１日、仕入れ先部品メーカーのシステム障害により部品供給が滞った影響で停止した国内全１４工場２８ラインについて、２日から稼働を再開すると発表した。被害を受けた小島プレス工業（愛知県豊田市）は１日、サイバー攻撃によるウイルス感染と、脅迫メッセージを受け取ったことを発表した。

【引用元】読売新聞2022年3月1日 12:14
https://www.yomiuri.co.jp/economy/20220301-OYT1T50125//

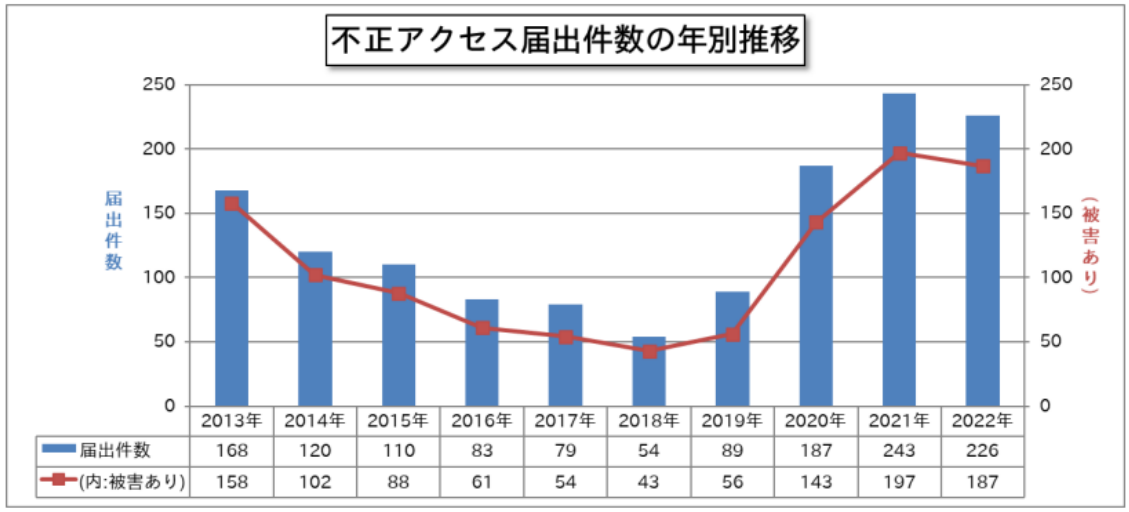
トヨタグループのような大企業では、下請け企業は4万社を越え、150万人前後が働いていると言われている。

下請け企業がサイバー攻撃を受ければ、従業員や家族等、数百万人に影響を与えうる

2. コンピュータウイルスと不正アクセスの脅威について

不正アクセスの被害届提出件数

同じく注意すべきインシデントである**不正アクセス**も、被害届提出件数が**急増**しています



	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	2022年
届出件数	168	120	110	83	79	54	89	187	243	226
(内:被害あり)	158	102	88	61	54	43	56	143	197	187

１週間に4件の
被害届が提出！

【引用元】引用元　コンピュータウイルス・不正アクセスの届出状況［2022年（1月～12月）］Copyright 2023 IPA

同じく、全当時者が報告しているわけではなく、IPAのアンケート調査では**6割が未公表**、
攻撃されたこと自体に気づいていない被害者も考慮すると、**実際はさらに件数が多い**

Examples of damage caused by cybersecurity incidents

02

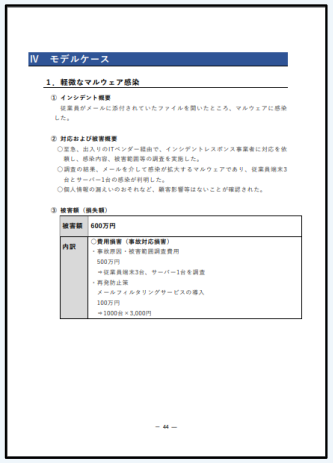
サイバーセキュリティインシデントの被害事例

1. 被害事例について
2. 被害事例A 軽微なコンピュータウイルス感染
3. 被害事例B ECサイトから情報漏洩
4. 被害事例C 大規模なコンピュータウイルス感染

1. 被害事例について

規模・パターン別の事例

実際に発生したサイバーインシデントの３つの事例を紹介します


Ⅳ　モデルケース

1．軽微なマルウェア感染

① インシデント概要

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、マルウェアに感染した。

② 対応および被害概要

○翌日、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し、感染内容、被害範囲等の調査を実施した。

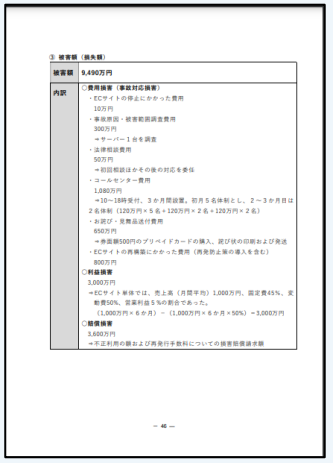
○調査の結果、メールを介して感染が拡大するマルウェアであり、従業員端末3台とサーバー1台の感染が利用した。

○個人情報の漏えいのおそれなど、損害影響等はないことが確認された。

③ 被害額（損失額）

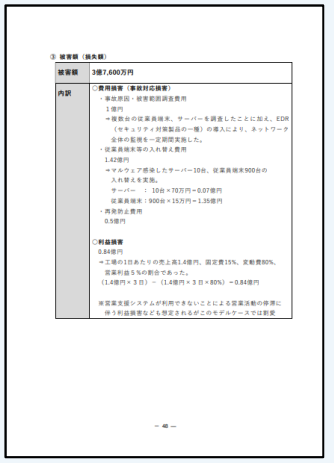
被害額	600万円
内訳	○費用損害（事故対応損害） ・事故原因・被害範囲調査費用 500万円 →従業員端末3台、サーバー1台を調査 ・再発防止策 メールフィルタリングサービスの導入 100万円 →1000台×3,000円

軽微なコンピュータウイルス感染
被害額 600万円


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 →初回相談は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

ECサイトから情報漏洩
被害額 9,490万円


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

大規模なコンピュータウイルス感染
被害額 3億7,600万円

【引用元】JNSA（※）「インシデント損害額調査レポート　2021年版」44~48ページ

被害額は会社や事業の規模と比例するわけではなく、インシデントによる被害の拡大状況により大きく変動する。自社は大丈夫と油断していると**思わぬ被害を被る**場合がある

※特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）は、ネットワークセキュリティに関する啓発、教育、調査研究及び情報提供に関する事業を行う、特定非営利活動法人です。

2. 被害事例A 軽微なコンピュータウイルス感染

添付ファイル開封からのウイルス感染

インシデント概要

従業員が**添付ファイル**を開封 → コンピュータウイルスに**感染**

対応、及び被害概要

事業者に感染内容、被害範囲を**調査依頼** → メール経由の**コンピュータウイルス**ということが判明 → 従業員端末3台とサーバ1台の**感染を確認(情報漏洩はなし)**

【参照元】JNSA「インシデント損害額調査レポート　2021年版」44ページ

社内のセキュリティ連絡や宅配業者を装ったメールが実は攻撃メールで、**添付ファイル開封**や**リンククリック**がトリガーになり感染するケースは、代表的な攻撃メールの一例

2. 被害事例A 軽微なコンピュータウイルス感染

軽微なウイルス感染による被害

被害額

被害額	**600万円**
内訳	• **事故要因・被害範囲調査費用** (従業員端末3台、サーバ1台) **500万円** • **再発防止策** メールフィルタリング サービス導入 **100万円**

【参照元】JNSA「インシデント損害額調査レポート　2021年版」44ページ

軽微な感染でも一定のコストや、被害拡大のリスクが

調査コストは、基本的には会社や事業規模に比例するが、基本費用や再発防止策など**一定のコスト**は掛かってしまう。自社や自分の事業は、インシデントと無関係と思っていると思わぬ被害を被る場合がある。また、被害事例Aでは情報漏洩は発生しなかったが、情報漏洩やランサムウェア感染が起きていれば、甚大な被害に**発展する危険性**があった。

3. 被害事例B ECサイトから情報漏洩

外部から偽フォームを作られ情報漏洩・不正利用

インシデント概要

ECの**決済代行会社**から連絡

ECサイトから**個人情報が漏洩**していることが発覚

対応、及び被害概要

ECサイトを停止し、事業者に**調査依頼**

何者かがECに**偽フォーム**を作っていることが発覚

1万件の情報漏洩と**2,500万円不正利用**が発覚

お詫び品を贈り、**6か月後**に運営再開。後日、決済代行会社より**損害賠償請求**

【参照元】JNSA「インシデント損害額調査レポート　2021年版」45-46ページ

ECやHPのシステムに脆弱性があると、不正アクセスや情報改竄を受けるケースがある。セキュリティコストを確保していない中小企業が想定外の被害額を被るケースも多い

3. 被害事例B ECサイトから情報漏洩

情報漏洩・不正利用による被害

被害額

被害額	**9,490万円**
内訳	• **ECサイト停止費用　10万円** • **事故要因・被害範囲調査費用 300万円** • **法律相談費用　50万円** • **コールセンター外注費用 1,080万円** • **お詫び品送付費用　650万円** • **ECサイト再構築費用　800万円** • **損害賠償　3,600万円** • **利益損害** (6か月間の営業停止) **3,000万円**

【参照元】JNSA「インシデント損害額調査レポート　2021年版」45-46ページ

信用失墜も含めると損害は計り知れない

事例Bでは月売上1,000万円規模のECが6か月で1億円近くの被害額を被った。インシデントの損害は調査や損害賠償といった分かりやすいものだけではなく、営業停止中の利益損害や人件費・固定費など、見えにくい損害もある。さらに、**信用失墜**で売上がインシデント前に戻らなければ実際の被害はさらに深刻なものとなってしまう。

4. 被害事例C 大規模なコンピュータウイルス感染

海外子会社経由でのランサムウェア攻撃

インシデント概要

海外子会社のサーバから本社のネットワークに侵入される

社内の各データが**ウイルス感染**、さらに**不正公開**される

データ復旧と公開停止を条件に**身代金**を請求される

対応、及び被害概要

攻撃により、社内ネット、メール、生産ラインが停止

事業者に**調査・復旧を依頼**

3日後にシステム復旧、完全復旧は端末入替等を経て**3か月後**

【参照元】JNSA「インシデント損害額調査レポート　2021年版」47-48ページ

ランサムウェアとは、ランサム(身代金)とソフトウェアを合わせた言葉で、データ復旧を条件に身代金を要求するウイルスを指す ※ただし、身代金を払ってもデータが復旧されるとは限らない

4. 被害事例C 大規模なコンピュータウイルス感染

大規模なコンピュータウイルス感染の被害

被害額

被害額	**3億7,600万円**
内訳	• **事故要因・被害範囲調査費用** **1億円** • **従業員端末入替費用** (サーバ10台＋端末900台) **1.42億円** • **再発防止費用** **0.5億円** • **利益損害** (3日間の出荷停止 ※営業活動停止分の利益損害は割愛) **0.84億円**

【参照元】JNSA「インシデント損害額調査レポート　2021年版」47-48ページ

対応や被害が複雑化
しやすいランサムウェア

情報漏洩は、その件数や範囲だけではなく、特許等の知識財産なのか、炎上リスクがあるか、集団訴訟が起こりうるか等の拡大要因を有している。**ランサムウェア**では、ここに**身代金**を払うのか、支払いは**法的正当性**があるか(アメリカでは、身代金の支払いに法的責任を問われる場合もある)等、さらに複雑な判断やリスクに対面することとなる。

03

インシデント発生後の対応と損害対応にかかる費用

1. インシデントによる損害例
2. インシデントの損害対応にかかる費用
3. 事後対応のまとめ

1. インシデントによる損害例

サイバーセキュリティインシデントによる損害例

サイバーセキュリティインシデントによる損害の代表例として、以下があげられます

①損害対応費用
発生から収束までにかかる基本的な費用

②賠償責任
損害賠償金や弁護士費用

③損失利益
営業・生産停止による損害

④金銭被害
身代金や詐欺による直接的な支払い

⑤法的制裁
個人情報保護法違反等の課徴金

⑥無形損害
信用失墜、株価下落、従業員の意欲低下等

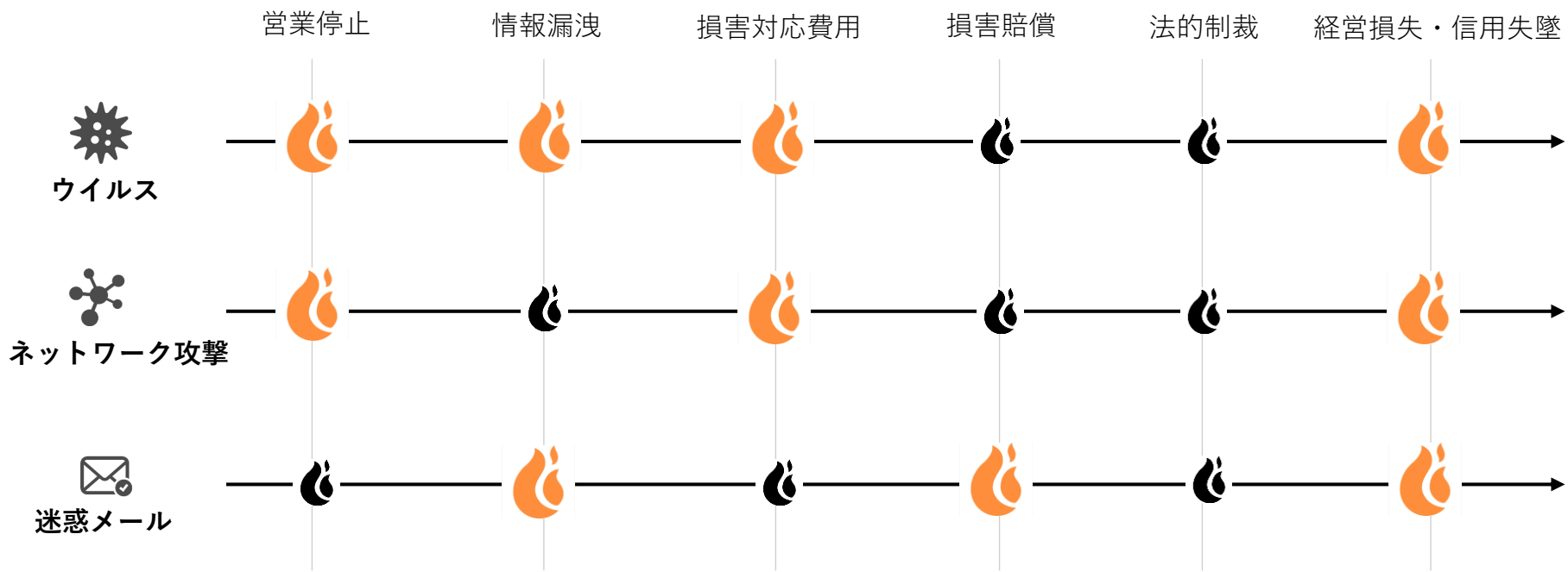
自社の抱えるリスクを把握する必要性

各企業の事業内容や規模、拠点所在地によって発生しやすいインシデントは異なる。さらに、各インシデントによって引き起こされる**損害の種類や規模**にも特徴があり、平時から自社の抱えるリスクはどんなインシデントで、どのような**損害に発展しやすいのか**把握する必要がある。

1. インシデントによる損害例

各インシデントの損害における相関

各インシデントによって、発生するコストや被害範囲に特徴があります

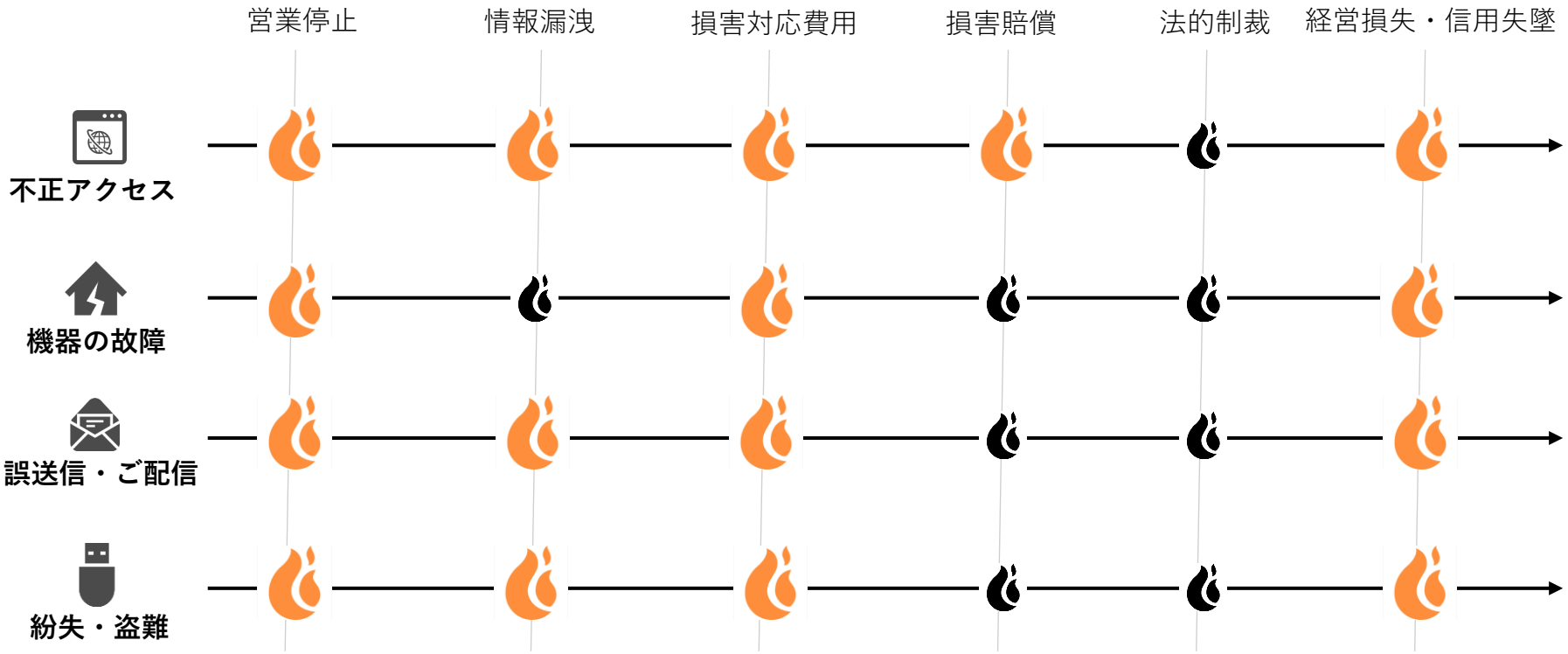


発生の可能性が極めて高い

状況(業種・対象となる情報)によっては発生しうる

1. インシデントによる損害例

各インシデントの損害における相関



発生の可能性が極めて高い

状況(業種・対象となる情報)によっては発生しうる

2. インシデントの損害対応にかかる費用

①損害対応費用 主な内訳

損害対応費用は発生から収束までの費用ですが、主に「調査」、「内部対応」、「外部対応」の各業務に費用が発生します

インシデントの対応フロー

2. インシデントの損害対応にかかる費用

①損害対応費用 内訳

調査費用は基本的に、「基本費用」＋「調査範囲」×「単価」で決まります

発生 ▶ 発覚 ▶ 初動対応 ┬ **調査** / 内部対応 / 外部対応 ▶ 収束

基本費用

- ✓**初動対応**の指示
- ✓**調査**の支援・実施
- ✓**対外対応**のアドバイス
- ✓**根本原因**の特定・対処
- ✓**復旧作業**の支援・実施
- ✓**報告書**の作成
- ✓**善後策**の提案

＋

調査対応の対象範囲(台数)

×

単価

＝ **損害対応費用**

不正アクセス等のサイバー攻撃の場合、機器やデータの中に残された証拠や痕跡を調査する必要があるため、社内での対応が難しく、専門事業者への依頼はほぼ必須となる

2. インシデントの損害対応にかかる費用

①損害対応費用 調査費用の相場

調査費用(PC100台とサーバ5台、スマホ10台の調査例)だけでも数百万円かかるケースが一般的です

発生 ▶ 発覚 ▶ 初動対応 ┬ **調査** ┬ 内部対応 ▶ 収束
　　　　　　　　　　　　└ 外部対応 ┘

	合計額※目安	基本費用	対応費用			その他
専門A社	580万円	定め無し (調査メイン)	PC5万円/台 ×100台＝500万円	サーバー10万円/台 ×5台＝50万円	スマホ3万円/1台 ×10台＝30万円	
専門B社	2,275万円 ＋基本費用	非公表	PC15万円/台 (正常なもの) ×100台＝1,500万円	サーバー30万円/台 (正常なもの) ×5台＝150万円	メディア5万円/台 (正常なもの) ×10台＝50万円	オンライン データの調査 5万円/1サービス ×計115台＝575万円
神戸デジタル・ラボ	200万円～	200万円～(5営業日2人体制で完了する場合の基本料金※規模により変動)				
大手E社	500万円～	500万円～(※事前コンサルティング等の複数サービスが含まれる総合契約)				

※インターネット検索で提示されていた概算データに基づく

2. インシデントの損害対応にかかる費用

①損害対応費用 内部対応の費用

インシデントの調査が進むと、内部対応として復旧・再発防止に取り組みます

発生 ▶ 発覚 ▶ 初動対応 ▶ 調査 / **内部対応** / 外部対応 ▶ 収束

復旧費用

小 ― コスト ― 大

- 設定変更
- OSの再インストール
- 端末の買換え
- ネットワーク機器の買換え
- 生産設備の更新

＋

再発防止費用

小 ― コスト ― 大

- 社内体制の整備
- システムの改修・導入

機器の買換えや生産設備の更新は、台数や種類によっては、莫大な金額になる場合がある。
また、ECサイト等の場合は、サイトそのものを作り直さないといけないケースも多い

2. インシデントの損害対応にかかる費用

①損害対応費用 外部対応の費用

内部対応と並行して、外部対応とそれに伴う費用が発生します

発生 ▶ 発覚 ▶ 初動対応 ┬ 調査
　　　　　　　　　　　　 ├ 内部対応
　　　　　　　　　　　　 └ **外部対応** ▶ 収束

法的相談
行政手続きや
訴訟対応

危機管理専門家相談
謝罪文や謝罪会見に
関する相談

広告宣伝費
被害者宛DMや
広告・マスコミ費

コールセンター依頼
被害者が多い場合や、社内に
窓口が無い場合に利用

お詫び品
訴訟とは別に
謝意として使用

被害額が拡大するリスクを抱える対外対応

現在の社会では、対応を誤ると、いわゆる**炎上のリスク**があり、インシデント自体はそれほど大きなことではなかったにもかかわらず、事業活動の維持に多大な影響を及ぼす危険性がある。企業の規模が小さくとも、**大量のデジタルデータ**を保有している企業は被害規模や炎上のリスクが高いので、特に注意したい。

2. インシデントの損害対応にかかる費用

②賠償責任 主な賠償例

賠償責任により発生する費用の代表は以下の3つです

クレジットカード関係
カード停止、再発行の費用、
不正利用の賠償

個人情報漏洩の賠償
特に管理を外部から委託
されていた場合は高額に

知的財産漏洩の賠償
特許等の漏洩は、賠償範囲が
広く、莫大な金額に

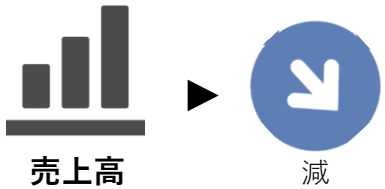
被害範囲より、賠償の費用は連鎖的に高額となる

賠償請求は、社内の要員で対応するのは通常不可能なため、**弁護士**に依頼することとなる。
直接的な賠償ではないが、弁護士費用は被害のスケールに比例して高額になるので、賠償責任に係る**費用は連鎖的に膨らんでいく**ということを留意すべきである。

2. インシデントの損害対応にかかる費用

③損失利益

営業や生産が出来なくなった場合、その期間に**本来得ることができるはずだった金額**を**損失**したこととなります



利益が損失される期間が長期に及ぶケースも多い

単純な計算の例としては、1日500万円の純利益を生み出すECサイトが1週間停止して注文が受けられなかった場合、3,500万円の利益を得る機会を失ったことになる。
停止期間はケースバイケースだが、会社のコンピュータが数百台全て被害に遭った場合は、**数週間から月単位の影響が出ることを考慮**する必要がある。

2. インシデントの損害対応にかかる費用

④金銭被害 主な被害例

直接的に金銭を奪われる金銭被害は、近年話題のランサムウェア等、手口が巧妙化し、被害も増加傾向にあります

ランサムウェア
システムやデータの復旧を
条件に身代金を要求される

ビジネスメール詐欺
自社の社長からの業務
メールを装って、金銭を
振り込ませる等の例がある

**ネットバンクの
不正アクセス**
IDやパスワードが奪われ、
ネットバンクに侵入される

身代金を支払えば解決ではない ランサムウェアの脅威

ランサム(身代金)とソフトウェアを組み合わせたランサムウェアは近年ますます被害数を増加させている。身代金を払えば、必ず復旧されるというわけでもないので、**対応方針を事前**に社内で決めておかないと、被害が拡大する恐れがある。実際に、身代金を払っても復旧されず、業者に改めて調査・復旧を依頼し、結果的に二重に費用が発生したという例も少なくない。

2. インシデントの損害対応にかかる費用

⑤法的制裁

不正アクセスされること自体は犯罪ではないが、個人情報漏洩の経緯や対応に落ち度があれば、日本・諸外国の法的制裁を受ける可能性があります

地域	該当する法律(通称)
日本	個人情報保護法
EU	GDPR(一般データ保護規則)
アメリカ	CPRA(カルフォニアプライバシー権法)

厳罰化されていく 個人情報保護法の罰則

日本の個人情報保護法は、2022年4月施行の法改正により30万円以下、50万円以下の罰金だったものがどちらも**1億円**以下に引き上げられた。
アメリカのCCPAも2023年1月に現CPRAに変更され、より消費者の権利が強化されたと同時に、日本企業にとっては**国際法務**への対応がますます重要となった。

2. インシデントの損害対応にかかる費用

⑥無形損害

大規模なインシデントを発生させてしまった企業や団体が被る被害には、はっきりと金銭としてわかる損害の他に、無形の損害もあります

信用の低下
最悪の場合、取引停止や
顧客離れ、操業中止の場合も

株価の下落
投資家の意欲低下により、
株価に影響が出ることも

従業員の意欲低下
従業員のエンゲージ
メントや採用力の低下

信用など目に見えない被害は取返しがつかない場合も

サイバーセキュリティインシデントによる株価の下落は、数十パーセント下落をした事例もある。これらの被害額は一概にいくらと言い切れないものがあるが、誤った対応や、炎上を起こしてしまった場合、**失った信用は二度と戻ってこず**、そのまま廃業を余儀なくされるという最悪の事態もありえる。

3. まとめ

損害と事後対応

発生する損害はケースバイケースで、全てを解決できるような対策はありません。
自社での解決は難しく、専門家の協力が必要です

✓ 全てを自社で対応するのは難しい

①損害対応費用
発生から収束までにかかる基本的な費用

②賠償責任
損害賠償金や弁護士費用

③損失利益
営業・生産停止による損害

④金銭被害
身代金や詐欺による直接的な支払い

⑤法的制裁
個人情報保護法違反等の課徴金

⑥無形損害
信用失墜、株価下落、従業員の意欲低下等

事後対応には限界があるので事前対策が重要

ウイルス感染の範囲、営業停止期間、サイバー犯罪の手口、炎上リスク等、被害の範囲を事前に完全に予測するのは難しいが、自社の規模や事業、拠点場所から発生しうる損害の種類や傾向を予想することはできる。損害を極力拡大させない努力は勿論だが、**想定外の範囲や被害額に発展させない**ような対策や準備も同様に必要である。

04

インシデントの事前対策

1. 一般的な事前対策
2. 神戸デジタル・ラボが提供する対策
3. まずはこちらから

1. 一般的な事前対策

サイバーセキュリティインシデントの事前対策

サイバーセキュリティインシデント事前対策の代表例として、以下があげられます

	社内体制の整備	情報資産の把握	従業員教育	システムの強化
内容	対策チームの配置、 インシデント発生時の 取り決め設定	デジタル資産を把握し、 リスク範囲を シミュレーション	リテラシー教育や模擬訓練、 導入しているソフトの 理解促進	セキュリティソフト、 バックアップ、 異常ログの検知ツール等
効果	インシデント時の早急な対応、二次被害の防止	自社の抱えるリスクを把握・対策ができる	インシデント発生の 事前防止、発生時の 適切な対応	インシデント発生の 事前防止、発生時の 適切な対応や被害拡大防止
コスト	低～	中～	中～	高～

100万円の価値の資産に500万円の事前対策費を払う必要はないが、
年間1億円の価値を生む資産が、年に500万円で守れることは多い

2. 神戸デジタル・ラボが提供する対策

神戸デジタル・ラボが提案する対策

サイバーセキュリティインシデントの事前対策に、3つの提案をいたします

セキュリティ
アドバイザリーサービス

「ちょっと困った、相談したい」
時のためにすぐに聞ける人をそばにおく
サービス。情報セキュリティの
課題解決のハードルを下げる

セキュリティリスク対策
プランニングサービス

システムと組織のリスクを洗い出し、
被害想定金額を算出した上で、今後の
セキュリティ対策の方針、優先度、
予算をご提案

ログ設定診断
サービス

各種システムログの設定状況や
有効性を確認し、インシデント時に
判断可能な内容を明示しつつ、
管理に関する改善点をご提示

事前対策はコストではなく予算という考えが少しずつ日本でも浸透してきているが、
いきなり高額な予算を使うのではなく、まずは必要な箇所に手を付けたい

2. 神戸デジタル・ラボが提供する対策

神戸デジタル・ラボが提案する対策①セキュリティアドバイザリーサービス

専門家が、具体的な実現案を即座に回答し、課題が小さいうちに対策します

解決する課題

- ✓ 社内に専門家がいない
- ✓ 具体的な事前対策が分からない
- ✓ いきなり高額な予算はかけられない

データベース暗号化、Cookie設定、名刺管理システム等、リスクが高く、具体的な対策が難しいものほど、低コストで受けられる専門家によるアドバイスが効果的

2. 神戸デジタル・ラボが提供する対策

神戸デジタル・ラボが提案する対策②セキュリティリスク策プランニングサービス

セキュリティを人、モノ、運用からリスク分析し、必要な対応をご提案します

解決する課題

どのリスクから手を付ければいいのか**分からない**…

攻撃の**頻度**と**想定**被害、**売上**への寄与、**資産**規模から、
リスクの対応優先度を見積ります

社内で、セキュリティ対策の**予算**に対する意見が**まとまらない**

実際に情報漏洩が発生した際の**想定被害金額**を算出したり、
運用で対処する案を出したり、貴社の状況に寄り添います

インシデントには事件の話題性や、業界内での噂等、論理的に優先度を考えることを難しくさせる要素も少なくないので、客観的に「頻度」と「影響度」を算出することが効果的

2. 神戸デジタル・ラボが提供する対策

神戸デジタル・ラボが提案する対策③ログ設定診断サービス

インシデント発生時にログの管理不備で調査不能になるケースがあります。
専門家がログ設定の確認・改善提案を行います

ログの適切な取得で解決できる課題

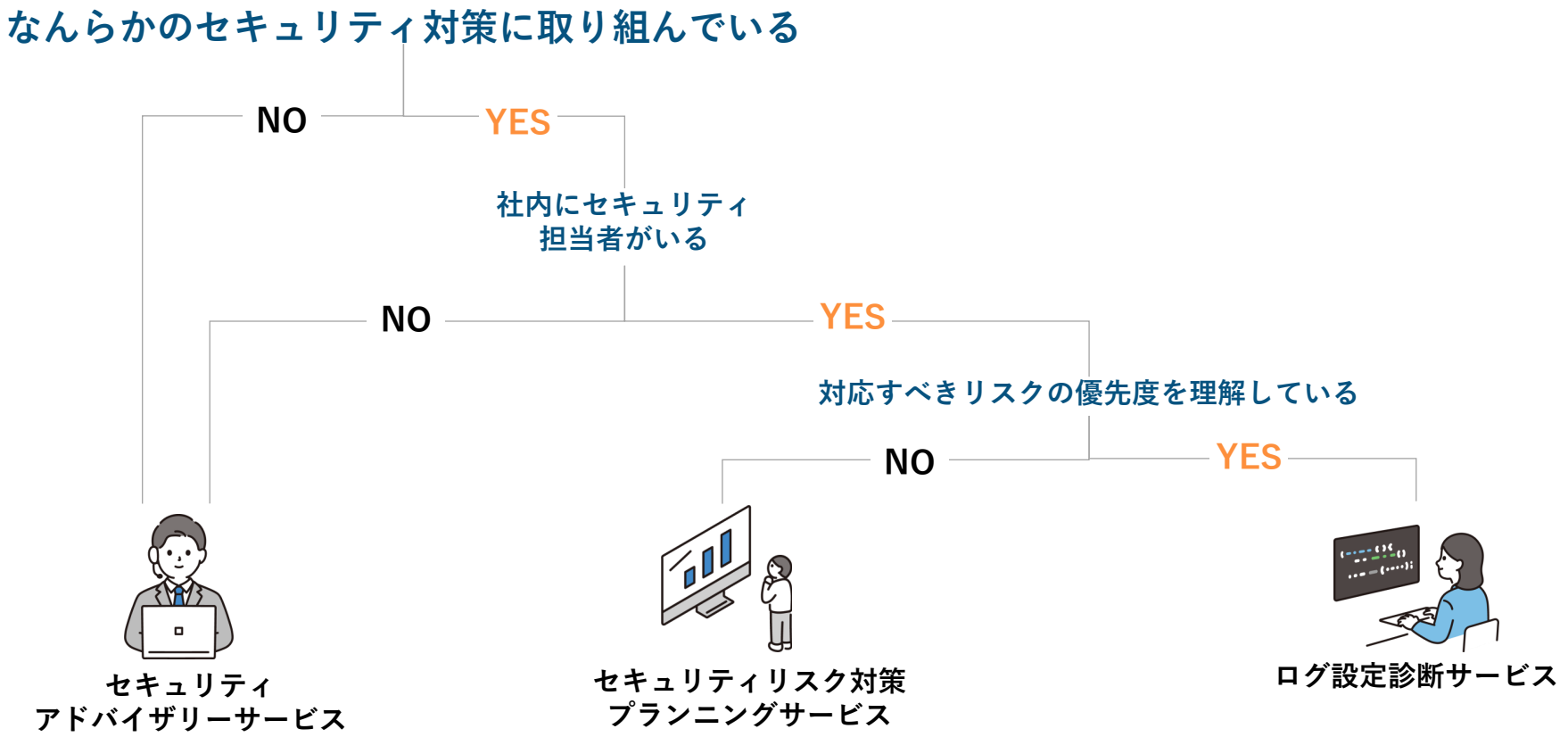
- インシデント発生時に**必要な情報が何か**、それが**自社にあるのか**わからない
- 導入した**セキュリティツール**のランニングコストが高いが、**継続すべきか**わからない
- 経営層に**費用対効果**を説明する際に使用する**第三者評価**が欲しい
- 実際にどれくらいの**攻撃**があって、どれくらい防げているか**可視化**したいが専門家がいない

近年、世間を騒がせた大阪急性期・総合医療センターのランサムウェア事件では、発覚時に事業者側で更新をしてしまい、不正アクセスの記録が消えたことで調査困難になった

2. 神戸デジタル・ラボが提供する対策

神戸デジタル・ラボが提案する対策 自社に必要なサービス

自社に**必要なサービスの参考**に以下ご活用ください



2. 神戸デジタル・ラボが提供する対策

神戸デジタル・ラボが提案するその他のサービス

コンサルティング CONSULTING	リスク対策プランニング	リスクを洗い出し、優先的に対策すべき施策と必要な予算を見える化
	テレワークリスクアセスメント	テレワーク環境のリスクを洗い出し、対策すべきポイントなどをご報告
	アドバイザリー	「ちょっと困った」というときに気軽に相談できる月額制サービス
	公開画面調査	外部に公開されている画面（制御用コンソール）の設定状況を調査
	ログ設定診断	貴社が収集すべきログが適切に取得・管理できているかを調査
脆弱性診断 ASSESSMENT	Webアプリケーション脆弱性診断	ツール・手作業による疑似攻撃診断で脆弱性の有無と対策を明らかに
	スマートフォンアプリ脆弱性診断	スマホアプリおよび連携するサーバプログラムを診断（Android・iOS）
	WebAPI/IoTサーバサイド 脆弱性診断	アプリの通信先WebAPIに対して疑似攻撃を仕掛け脆弱性を診断
	プラットフォーム脆弱性診断	コンピュータやネットワーク全体の弱点となる問題がないか診断
	クラウドセキュリティ設定診断	AWS、Microsoft Azure環境に設定ミスがないかを診断
トレーニング TRAINING	標的型攻撃メール訓練	疑似標的型攻撃メールによる訓練で従業員のセキュリティ意識を向上
	脆弱性診断トレーニング	Webサイトの脆弱性診断ができる人材を企業内に育てる支援サービス

3. まずはこちらから

神戸デジタル・ラボへのご連絡

まずは簡単なご相談や、お見積り依頼でも結構です。お気軽にお問合せください

https://www.proactivedefense.jp/#footer-contact

お問合わせフォームに遷移します

株式会社 神戸デジタル・ラボ

住所：兵庫県神戸市中央区　TEL：078-327-2280(平日10:00～17:00)

ブログにて随時お役立ち情報更新中！

https://www.proactivedefense.jp/

（左図のページに遷移します）

CONCLUSION

まとめ

サイバーセキュリティインシデントの脅威は年々高まっているにも関わらず、具体的な被害や対応の知識、事前対策としてすべきことを十分に理解・実行できている企業はまだまだ多くありません。
自社の価値や取引先、顧客を守るため、ぜひ、専門家の知見や協力をご利用ください。

Kobe Digital Labo ITで未来を創る