サイバーセキュリティインシデントが発生したら？

～発生時の費用から見るインシデント～

2022/03/09

株式会社神戸デジタル・ラボ

演者自己紹介

- 久柴　克宏　（ひさしば　かつひろ）

(株)神戸デジタル・ラボ　セキュリティサービス
情報セキュリティコンサルタント

IPA　情報セキュリティマネジメント
ISACA　公認情報セキュリティマネージャー資格

保持

株式会社神戸デジタル・ラボで
企業の情報セキュリティガバナンスの成熟度測定や
CSIRT活動支援、リスクアセスメント、ドキュメント作成支援などに従事

- 経歴

  - 1996年にIT業界でのキャリアをスタート
  - その後はカスタマーサポートをメインに
  - 情報セキュリティに興味を持ち始めたのは2001年

演者自己紹介

・2001年何が起きた？

- 夏に登場したコンピュータウイルス
  「CodeRed」が
  インターネットを大混乱に

- CodeRedが行った膨大な通信により、世界の至る所でネットが繋がりにくくなる状態が発生し
  同7月19日は、
  人呼んで「インターネットが止まった日」に

・その日から私は・・・

- 数週間にわたり、ネットワークが停止した某企業で、

  全ての端末（3000台くらいに）にパッチを充て、

  ウィルス対策ソフトの更新をするために

  USBメモリやフロッピー、CDを持って、

  毎日朝8時から夜の8時まで2週間以上、走り回る生活に

・なぜ、そんな大規模な被害が？

- CodeRedが悪用した脆弱性には、パッチがなかった？

いいえ、1ヶ月前にはパッチが公開されていました。

しかし、

古いWindowsNTはもちろん、主流だったWindows98でも

パッチが適用されていない端末がほとんどだったのです。

・その経験を経て

便利なITを安心してみんなが使うためには、

多くの人にセキュリティ対策の必要性を理解してもらい、

積極的にセキュリティ対策に参加してもらえるようにしなければならない、

と思うようになりました。

ご注意！

・そのため

- 今日の内容は、「ITに詳しくない」とおっしゃる方にも

  ご理解していただけることを目的としておりますので、

  深い考察や専門的な知識は一切含まれていません！

ご注意！

・ですが、

- ご自分の組織で情報セキュリティ対策に対する理解がなかなか得られない、上司に説明するアイデアが欲しい

- 情報セキュリティ対策が必要なのはわかるが、どれくらいのお金をかけるべきなのか、調べる方法がわからない

という方のご参考にはなるかも知れません

ご注意！

・ゆえに

人によっては、「物足りない」「もっと技術的に深い話が聞きたかった」とお思いになるかも知れませんが、

何卒ご容赦ください

・本日の内容の詳細について

本日お話しする内容は、
JNSA　(日本ネットワークセキュリティ協会)が
公開されている
「インシデント損害額調査レポート」
を参考にさせていただき、
引用、参照させていただいております。

ですので、詳細や最新の情報をお知りになりたい方は、
当該サイトをご訪問いただき、確認いただけますようよろしくお願い申し上げます。

今そこにある脅威

～情報報セキュリティインシデントとは？～

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とは、

セキュリティインシデント、セキュリティ事故ともいいますが、

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

におかれることをいいます。

※情報資産

大雑把に言えば、情報を格納する器(パソコンやスマホ、紙)とそのデータをまとめて呼びます

情報セキュリティインシデントには、どんなものがあるのでしょう？

代表的なものだけでも、以下のようなものがあります

- コンピュータウイルス （マルウェア)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の総称であり、ランサムウェア（データを暗号化して身代金を要求するもの）が最近被害件数を増やしています。
- ネットワーク攻撃

  ネッ トワークに接続された機器に異常な負荷をかけ機能を停止させる行為
- 迷惑メール
- 情報の改ざん
- 不正アクセス

  (不正アクセスが原因となって上記が起きることも、上記が原因となって不正アクセスが起きることもあります)
- 地震、火災、水害等による機器の損壊 ・故障
- 電子メール、FAX、郵便物の誤送信・誤発送
- PC、USBメモリなどの記録媒体の紛失 、盗難

今そこにある危機

今日は、その中でも特に、

コンピュータウィルスや不正アクセスによって起きるインシデントに

フォーカスを当ててご説明したいと思います

理由は、

自然災害や火災などによるインシデント、人的ミスによるインシデントに比べて

ITに特有の事柄が多く、インシデントが起きた時に必要となる対処や費用について

ご存じない方が多いのではないかと思うからです

・コンピュータウィルスや不正アクセスってそんなに多い？

コンピュータウイルスや不正アクセスの被害が増えていると聞きますが、
そんなに被害が多くなっているのでしょうか？

※以前は「コンピュータウィルス」というのが一般的でしたが、現在は「マルウェア」という言葉が使われています。
しかし、未だにコンピュータウイルスという言葉の方がピンと来る方がが多いため、
この資料では、
コンピュータウイルス、あるいは、ウィルス
という言葉で表現しています

コンピューターウィルス(マルウェア)の届け出件数の推移

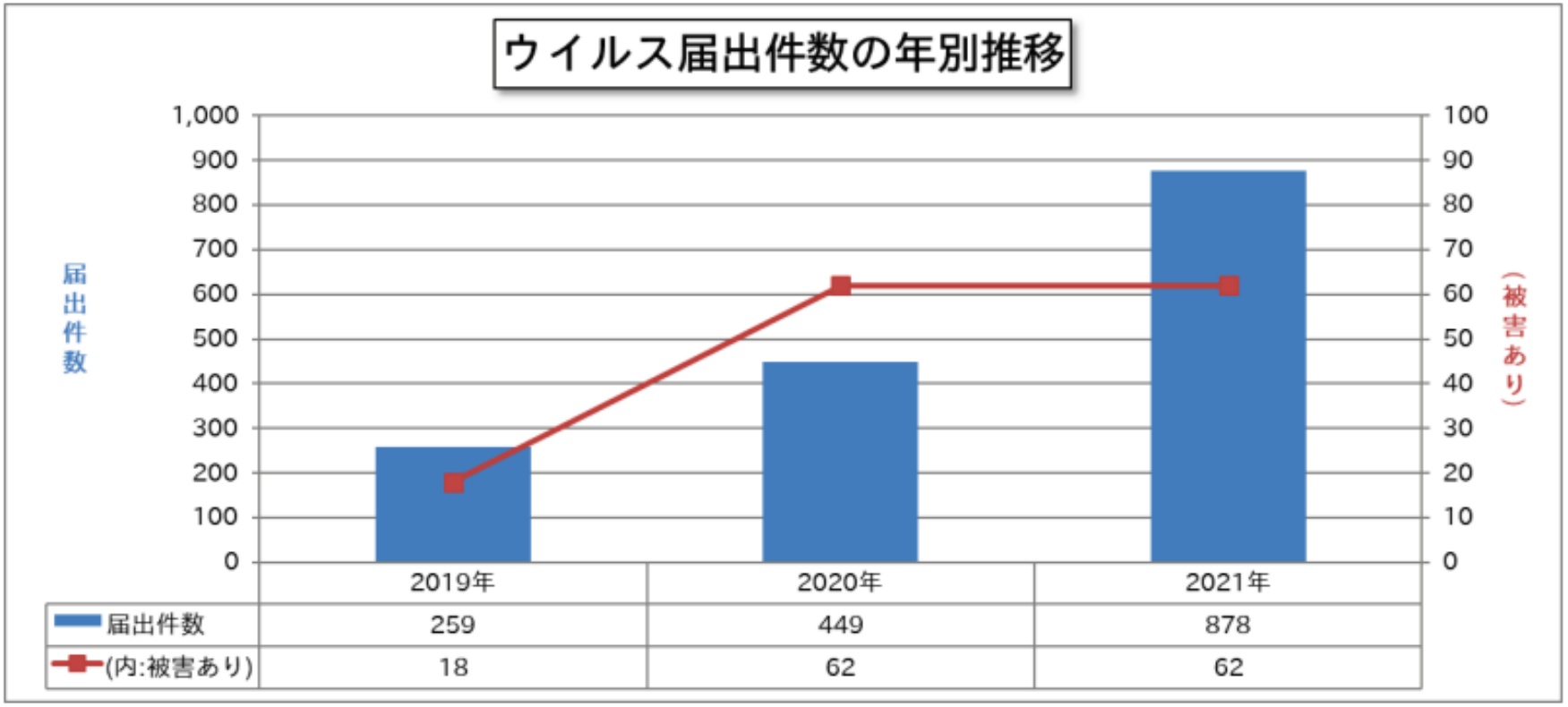


図 1-1：ウイルス届出件数の年別推移

引用元　コンピュータウイルス・不正アクセスの届出状況

今そこにある脅威

被害事例が年60件と言うことは、週に1件は出ていることになります。

これだけでも、結構な件数だと思えますが・・・

しかし

- 全ての当時者が律儀に報告しているわけではない
  →届け出は義務ではないし、特に被害が小規模の場合は口をつぐみがち
  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がどれだけいるかわからない
  →不審なメールやシステムのダウンなどがなければ気づきにくい

ことを考えると実際はもっと件数は多いのではないかと思われます

今そこにある脅威

さらに2022年には、この件数が大きく増えることが予想されています。

理由は・・・・

Emotetと呼ばれることウィルスにあります。

数年前から大きな被害を出してきたEmotetが

昨年末からさらに多数の被害者を出しており、

今年に入ってその勢いは一向に衰えることなく、

2022年2月の1週間でIPAには、45件もの相談が寄せられ、

弊社にも多数の被害、対応の相談が寄せられていますし、

今月に入っても、多くの企業団体が被害を公表しています。

今そこにある脅威

また、被害の大きさについてですが、

先週、自動車メーカートヨタへ主要部品へ納入するメーカーがサイバー攻撃を受けたことで、その煽りでトヨタが丸1日操業を停止する事態になりました。

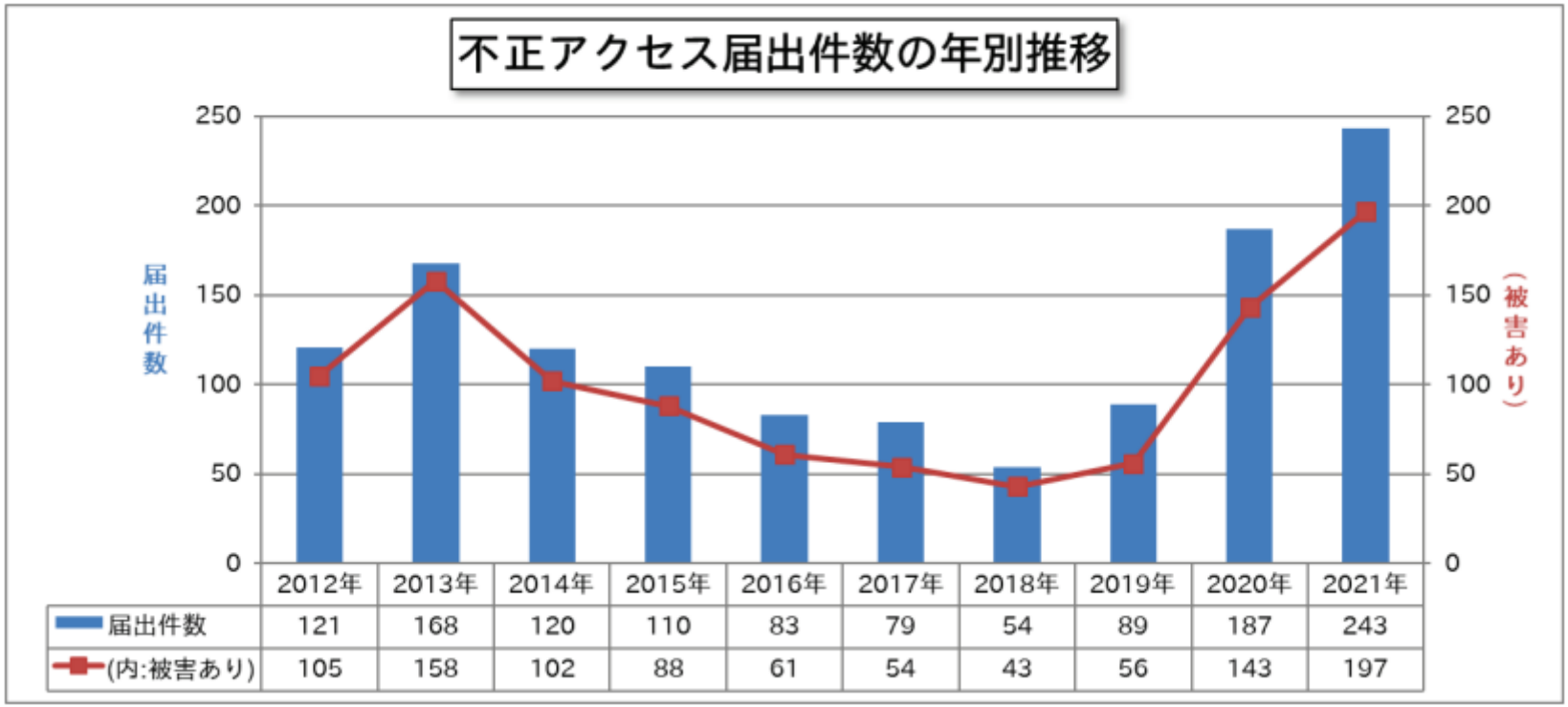
これも件数としては1件ですが、

トヨタグループの下請け企業は4万社を越え、150万人前後が働いていると言われていますので、このサイバー攻撃の影響は従業員の家族を含めて数百万人に及んだということが出来ます。

今そこにある脅威

一方不正アクセスについてですが

同IPAの資料に基づくと、2021年は243件の届出があり、
被害件数は197件に上っています。



	2012年	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年
届出件数	121	168	120	110	83	79	54	89	187	243
(内:被害あり)	105	158	102	88	61	54	43	56	143	197

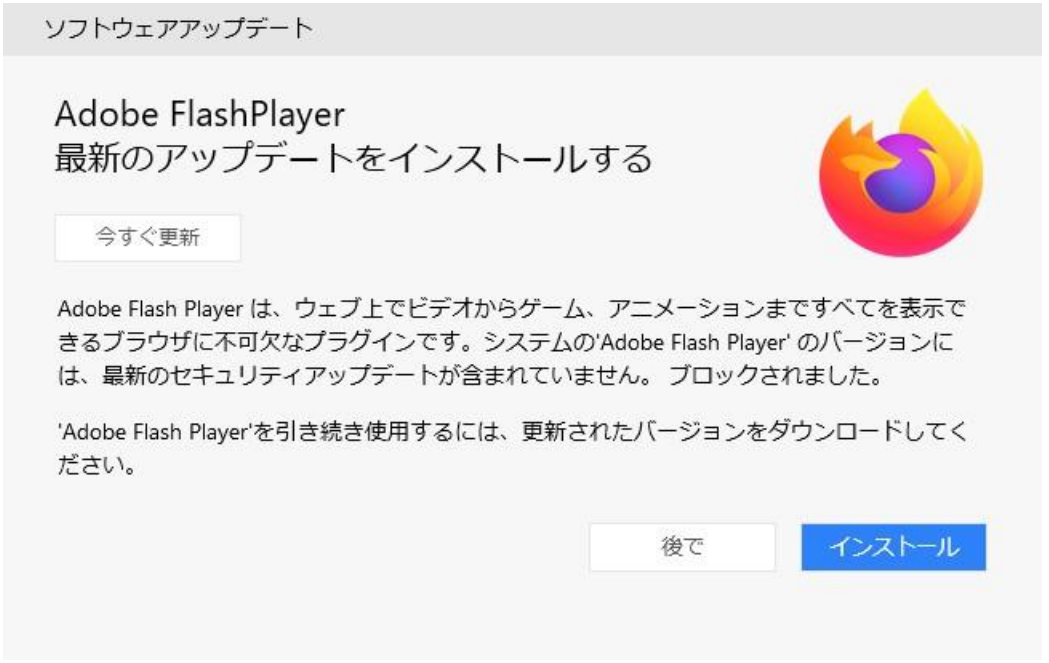
引用元　コンピュータウイルス・不正アクセスの届出状況

今そこにある脅威

このように、不正アクセスや、不正アクセスを狙った下準備の行為は

日常的に行われており、私たちが普段見ているWebサイトにも

それらの攻撃の一端が現われる事があります。



情報セキュリティインシデントによる損害

情報セキュリティインシデントが発生したら？

主なインシデントと起こりうる主な被害の関係性

	直接			間接			
	業務停止	情報漏洩	対策コスト	損害賠償	公的処罰	経営損失	信用失墜
ウィルス	◎	◎	◎	○	○	◎	◎
ネットワーク攻撃	◎	○	◎	○	○	◎	◎
迷惑メール	○	◎	○	◎	○	◎	◎
情報の改ざん	○	◎	◎	○	○	◎	◎
不正アクセス	◎	◎	◎	◎	○	◎	◎
機器の故障、損壊	◎	○	◎	○	○	◎	◎
誤配信・誤発送	◎	◎	◎	○	○	◎	◎
紛失・盗難	◎	◎	◎	○	○	◎	◎

◎ 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

※情報が漏えいした結果、他のインシデントが起きる可能性もあることに注意が必要

情報セキュリティインシデントによる損害

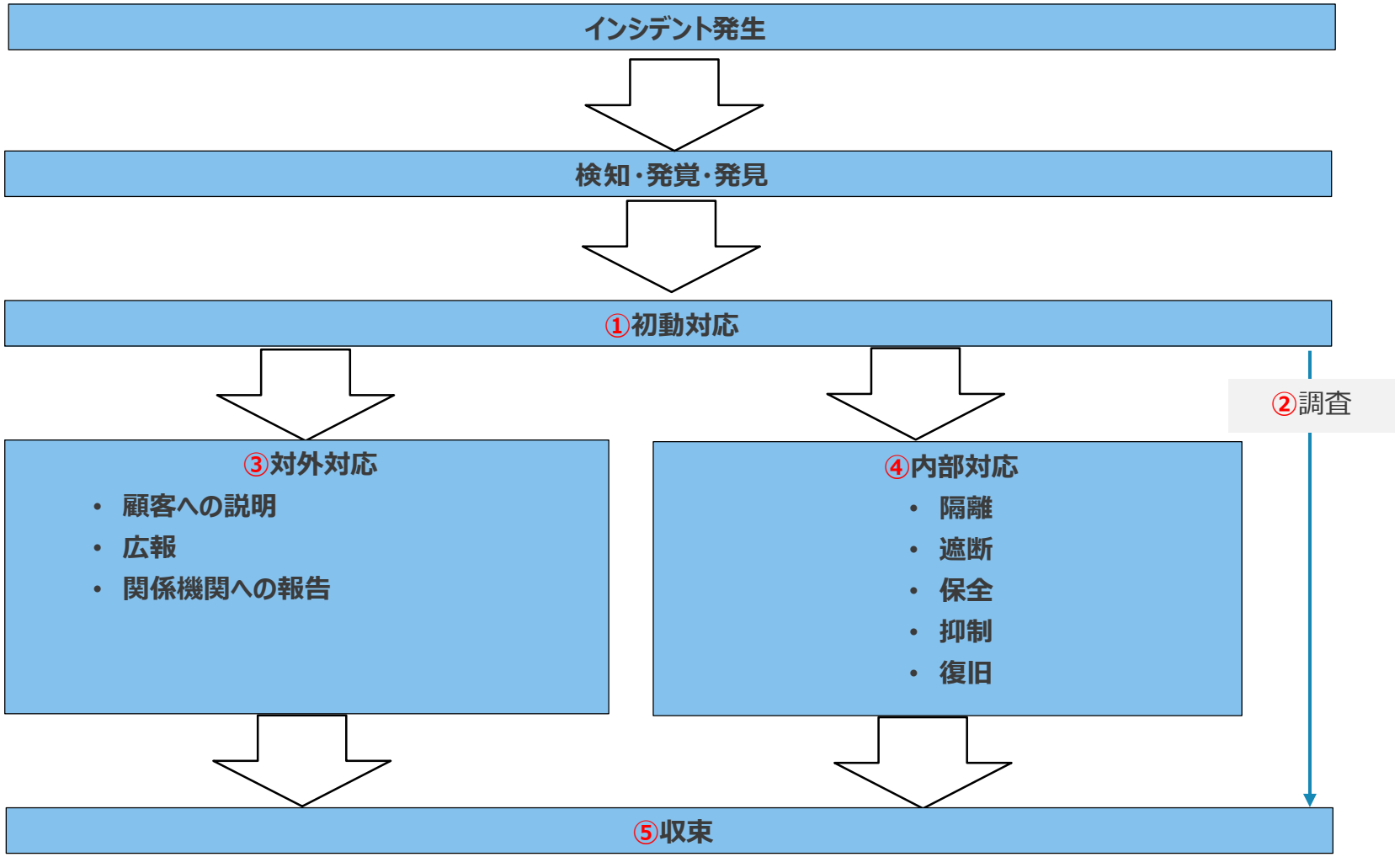
インシデントが発生した時に生じる損害には以下のようなものがあります

損害の種類	主な支出項目
①対策費用	インシデント発生から収束に至るまでの費用(余剰で発生する組織員の人件費、対応ベンダーの費用など)
②賠償責任	クレジットカード情報や契約先の機密情報が漏えいしたことにより発生した被害に関して損害賠償請求を求められた場合の賠償金や弁護士費用
③遺失利益	Webストア停止による売り上げの低下、受発注システムや生産管理システムの停止で事業中断が発生した場合などで発生する損害
④金銭被害	ビジネスメール詐欺、インターネットバンキングのアカウント窃取による直接的に金銭を奪われた場合の損害
⑤法的制裁	各種法令違反に対する罰金、GDPR、個人情報保護法ようなデータ保護に関する規則に違反したことで課される課徴金等
⑥無形損害	インシデントを発生させたことによる風評被害、企業イメージの低下、投資家のモチベーション低下による株価下落、組織員のエンゲージメント低下など単純な金額換算が難しい損害

①対策費用

①対策費用

インシデントが発生した後の対応



大きく分けて①～⑤の対応が必要になります
②と③と④は時間的に並行して行われます。

①対策費用

インシデントが発生すると

インシデントレスポンスと呼ばれる対応を開始します。

単純な紛失や誤発送、誤配信などは社内での対応が可能かも知れませんが

情報セキュリティインシデントの多くの場合では、専門家の協力が必要になります。

さらに、機器の故障などではないインシデントの場合、ネットワークやサーバーの業者が通常の保守契約の範囲で対応してくれるケースは少ないです。

特に、不正アクセスなど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ります。

当然ですが、専門の事業者に依頼するのですから、**費用が発生**します。

これらの費用が、情報セキュリティインシデントでまず最初に発生する損害となります

①対策費用

調査費用はいくらかかる？

決まった価格体系がないので、基本的に業者次第にはなりますが、

基本費用(規模の大小にかかわらず、調査を行ったことで発生する費用)と
調査対応を行った対象の範囲(台数)に単価を掛け合わせたものになるケースが多いようです

※基本費用には
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、調査、復旧作業の支援・実施、報告書の作成、
善後策の提案などが含まれます。

ただし、全てを行っている業者もあれば、
一部だけを担っている業者もあるため、複数の業者に依頼することも普通に行われます。

①対策費用

詳細が公表されていないケースが多いため、概算の参考事例ですが

たとえば。下記A社でサーバー5台、クライアントPC100台、スマホ50台を調査すると
サーバー　　10万　＊　5台　＝50万円
クライアントPC　　5万　＊　100台　＝　500万円
スマホ　　3万円　＊　10台　＝　30万円
で、端末だけでも580万円の費用がかかります。
これ以外にもネットワーク機器の精査などを行えば1台当たり数十万円の費用がかかります

	基本費用	対応費用			その他
専門A社	定め無し(調査メイン)	PC5万円/台	サーバー10万円/台	スマホ3万円/1台	
専門B社	非公表	PC15万円/台 (正常なもの)	サーバー30万円/台 (正常なもの)	メディア5万円/台 (正常なもの)	オンラインデータの調査 5万円/1サービス
専門C社	非公表	PC4万円/台	不明	メディア2万円/台	
KDL	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～(ただし、事前のコンサルティングなどの複数の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

①対策費用

復旧及び再発防止

インシデントの内容、原因、対策、などの調査が進むと
次は、システムの復旧をはじめることになります。

復旧作業は、影響を受けたシステムの範囲にも依りますが、
単にパッチを充てたり、設定を変更する、
あるいはOSを再インストールするだけで済む場合もあれば、
機器が古くて、メーカーのサポートが切れており、
新しいものに買い換えない限り問題が解決しない場合もあります。

パソコンを何十台も買い換えたり、ネットワーク機器を買い換えるだけでも
多大な費用がかかりますが
生産設備などを更新する必要などが生じれば、
その額は簡単に数千万単位になることも予想されます。

①対策費用

一方、情報セキュリティインシデントの調査や復旧が行われてる間も
並行して企業は対外的な対応を行っていく必要があります。

対外的な対応とは、つまり、
顧客、取引先、株主、被害者(個人情報洩や機密情報の漏えい、盗難、紛失があった場合)、
そして最近では、世間に対するケアのことも意味します

現在の社会では、直接的な関係者ではない第3者といえど、そこに対する対応を誤ると、自組織に対する反感が社会的なムーブメント（いわゆる炎上）になり、副次的な被害が発生し、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ります。

そのため、小規模な事故であっても、対外対応は慎重に、且つ的確に進める必要があります。
多くの企業では、そのようなケースに社内の要員が慣れていないため、ここでも専門家のアドバイスや支援を受ける必要性が出てきます

①対策費用

インシデントの内容次第ですが、以下のような出費が必要になるかも知れません

- **法的な相談、法的な手続きの代行者への依頼**

  改正個人情報保護法への対応など行政的な手続きから、被害者からの訴訟対応
- **危機管理専門家への依頼**

  謝罪会見や謝罪文のタイミング・内容などを相談する必要があります
- **広告宣伝費**

  被害者個別への連絡に使うダイレクトメールの発送や、被害者が多く個別連絡で完全に管理出来ない場合には、マスコミを通じて行う告知や謝罪が必要になります
- **コールセンターの依頼料**

  被害者が多い場合、企業が直接被害者からの連絡を処理するのは不可能なため、外部のコールセンターに委託して、対応する必要があります
- **お詫びの品・見舞金(品)**

  訴訟とは別に、謝意を表わす目的での品になります

①対策費用

以上のような費用が、必要となりますが、

インシデントの内容、被害規模によって、その費用は数万円から数千万円まで
大きく変化することになります。

さらに、物理的な大きさを持たないデジタルデータの場合、
企業の規模が小さくとも、大量の情報資産を保有する可能性があることで
被害額が大きくなることに注意が必要です

賠償責任

賠償責任

情報セキュリティインシデントによって情報が漏えいした場合、
漏えいした情報の種類によっては損害賠償が発生します。

賠償の内容には、以下のような物があります

クレジットカードのチャージバックや再発行費用

クレジットカードの情報が漏えいして不正利用された場合、通常、カードの所有者は支払いを拒否します。その際、漏えいに関して責任を持つ組織に対して、信販会社が請求してきます。
また、カード停止、再発行に関する費用の賠償請求も考慮する必要があります

知財の漏えいに対する賠償

他企業から提供を受けていた特許など知的財産を漏えいさせたことによる損害賠償
将来的にその知的財産から生み出される利益を想定して請求されると、莫大な額の請求になる可能性があります。

個人情報の漏えいに対する賠償

自社で収集した情報と他の組織から提供された情報があり得ますが、
一般的に他の組織から提供された個人情報の方が賠償額が高額になる可能性があります

賠償責任

さらに、賠償請求に組織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になりますが、

賠償額が高額になるということは、弁護士費用にも反映される可能性があるということを留意すべきです

遺失利益

遺失利益

不正アクセスやコンピュータウイルスの蔓延により、事業が停止した場合、
その間に本来得られたはずの利益が得られなくなりますので、
「利益が入手出来ない」という損失が発生します。

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通販サイトが1週間停止して注文が受けられなかった場合、
3500万円の利益を得る機会を失ったことになります

どれくらいの規模の組織でどれくらいの期間停止するかは千差万別のため、
単純な概算は出せませんが、
会社の中のコンピュータが数百台全て被害に遭った場合などは、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ります。

金銭被害

金銭被害

金融庁のレポートによると、2020年のオンラインバンキングの被害は16億円超、

警察庁の統計では、オンラインバンキングに関係する不正送金事犯は2019年、2020年と

1800件前後であり、

非常に多くの被害が生まれています。

また、最近話題になることが多い、コンピュータウイルスの一種ランサムウェアは、
組織のコンピュータを使えなくすることで身代金(ランサム)を請求しますが
これらの要求額も増加の一途を辿っています。

ただし、身代金を請求されたからといって、
要求通りに支払っても、元通りになるかどうかは保証がありませんし、
盗まれた情報はすでに流出した後かも知れません。

さらに、アメリカでは、特定の国・地域や個人、団体に対して金銭を支払うことに禁じており、
それらの相手に金銭を支払うことで、後々制裁を受ける危険性もあります

法的制裁

法的制裁

コンピュータウィルスに感染したり、不正アクセスされること自体は犯罪ではありませんが
個人情報が漏えいした場合に、その経緯や取扱・対応に落ち度があることが発覚すると
日本のみならず、諸外国の法的制裁を受ける可能性があります。

日本では、個人情報保護法というものがあり、
来月に施行される改正個人情報保護法では、
法令違反に対するペナルティが強化されました。

特に、法人に対する罰金刑が引き上げられ、
改正前は、30万円以下、50万円以下の罰金だったものがどちらも1億円以下と
大幅に引き上げられています。

無形損害

無形損害

大規模な情報セキュリティインシデントを発生させてしまった企業や団体が蒙る被害には、
ハッキリと金銭としてわかる損害の他に、無形の損害も発生します

例えば、

信用の低下

個人情報や営業上機密のような重要な情報を漏えいさせてしまった企業は、
当然ながら、社会的に信用が低下します。
最悪の場合、取引の停止や顧客離れ、結果、操業の中止を招くこともあります

株価の下落

インシデントの結果、業績に大きな影響が出る、あるいは出ることが予想されると
投資家のモチベーション低下により、株価に影響が出ることもあります

総括

総括

これまでご覧いただいたように、

コンピュータウイルスの感染や不正アクセスによるシステムの停止は、

地震や火災のよる被害のように、見てすぐわかるものではありませんが、

その被害は大規模な自然災害と同じくらいのものになる危険性があります。

皆さんの不安感を煽ったり、やたらに恐怖心を植え付けたいわけではありませんが

火災や自然災害に備えるのと同じように、

情報セキュリティインシデントにも備えていただく時代はすでに来ていると思います。

総括

だからといって、

無制限に対策に費用をかけるわけにはいかないという事情も当然あると思います。

そこで、

ご自身の所属される企業・団体で情報セキュリティインシデントが発生する前に

どのような情報を保有していて、

それが盗まれたり、破壊されたりした場合、どれくらいの損害が出るのかを

大まかにでもいいので、試算していただくことをお勧めします。

1000万の価値の資産に500万の対策費を払う必要はありませんが、

年間1億の価値を生む資産が年に500万円で守れることは多々あります。

最後に

本講演の元になっており、全般的に多くの引用参照をさせていただきました、
「情報セキュリティインシデント対応費用レポート」を作成された
JNSA(日本ネットワークセキュリティ協会)の
インシデント被害調査ワーキンググループの方には、
大変素晴らしいレポートを作成していただいたことに
心から感謝を申し上げます。

出来ましたら、皆様が当該レポートに興味を持っていただき、
結果、積極的に情報セキュリティ対策をとっていただければ、
と心より願って、本日の講演を終りたいと存じます

ご清聴ありがとうございました。