インシデント損害額調査レポート

第2版

IDIR Incident Damage Investigation Report 2nd edition

JNSA

インシデント被害調査WG

Ver1.00

目次

エグゼクティブサマリー

インシデントが発生した場合、各種の事故対応ほか、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するに、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を要し、結果として経営に多大な影響が発生します。

中小企業を想定した具体的な損害額のイメージは、アウトソーシング先の料金等を踏まえるに、次のような額になります。インシデントの内容（情報漏えいの件数など）によって大きく異なるものの、中小企業であっても数千万円単位の損失を抱える可能性は否めません。

セキュリティ対策の強化は、常に経営において考慮すべき事項となっています。

損害の種類		中小企業における損害額のイメージ（参考値）
大区分	小区分	
費用損害（事故対応損害）	事故原因・被害範囲調査費用	300～400万円
	コンサルティング費用	10～100万円
	法律相談費用	30～100万円
	広告・宣伝活動費用	1万人にDM送付した場合、約130万円 地方紙への新聞広告を出稿した場合約50万円
	コールセンター費用	3ヶ月の対応で700～1,000万円
	見舞金・見舞品購入費用	1万人へのプリペイドカード送付で650万円
	ネット炎上防止費用	対応内容によって大きく異なるが300～900万円のケースも
	ダークウェブ調査費用	調査内容によって大きく異なるが数百万円以上の額となるケースも
	クレジット情報モニタリング費用	1ヶ月あたり100～500万円
	システム復旧費用	対応規模等によって大きく異なるが、数百～数千万円のケースも
	再発防止費用	対応規模等によって大きく異なるが、数百～数千万円のケースも
	超過人件費	対応規模等によって大きく異なるが、多くの従業員等が対応に追われるケースも
賠償損害	損害賠償金	委託先から預かった情報漏えい事案の場合、上記費用損害の合計額が委託先から求償されることも。ECサイトのクレジットカード情報漏えい事案の場合、不正利用の規模によるが数千万円以上の額の求償がなされるケースも
	弁護士費用等	損害賠償金に比例して高額に。
利益損害		数ヶ月の売上高の減少（利益喪失に加え、回避できない固定費の支払い）
金銭損害	ランサムウェアによる身代金	支払いは慎むべきだが、数千万円以上の額の要求がなされるケースも
行政損害		個人情報保護法上の罰金は最大1億円
無形損害		顧客離れ、株価下落など換算不能な損失が
合計		ケースバイケースではあるものの、中小企業で数千万円単位、場合によっては数億円単位の損失も。経営に多大な影響が…。

Ⅰ はじめに

この「インシデント損害額調査レポート」は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として2021年夏に初版を公表、今回のレポートはその第2版として位置づけられます。

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、マスコミ報道、公的機関・団体や、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するインシデント（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、不利益が発生するのか、金銭的なインパクトを適切に認識しないまま、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ったケースも少なくありません。

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するに、**中小企業においても数千万単位、場合によって億単位のお金がかかること、経営に多大な影響が発生してしまうこと**を認識している経営者は多くはないと想定されます。

このレポートは、これらの点を踏まえて以下を目的として作成したものです。インシデント発生時の具体的な対応、アウトソーシング先、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まとめておりますので、事前対策・事後対応の両面からセキュリティ対策の強化を図っていただければと存じます。

対象	目的（活用方法）
経営者 （特に中小企業の経営者）	サイバー攻撃を受けると「お金がかかる」こと、その結果として、経営に多大な影響を及ぼすため、セキュリティ対策の必要性を理解していただく
システム担当者	このレポートを活用し、経営者に「お金がかかる」こと、セキュリティ対策の必要性を訴えていただく
IT/セキュリティベンダー等、セキュリティ業界の方	このレポートを活用し、経営者、システム担当者にセキュリティ対策の必要性を訴えていただく

なお、このレポートに記載している被害額（損失額）は、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。

Ⅱ インシデントの概要

１．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で、情報セキュリティの世界では、システム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みます）を意味します。偶発的であるか意図的であるかは問わず、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。

インシデントの一例としては、次のものが挙げられます。

○マルウェア感染
マルウェア（不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称）に感染してしまうことをいいます。マルウェアの一例としては、近年、脅威を増している「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）や2022年3月に国内で被害組織が拡大した「エモテット」（Emotet。メールアドレス等の情報を窃取するマルウェア）などが挙げられます。

○ウェブサイトの改ざん等による情報漏えい
ECサイトを運営している場合、購入者にクレジットカード情報の入力を求めることが一般的ですが、これら情報を狙って何らかの手段により改ざんし、偽の入力画面を設置する等によりカード情報を窃取するケースが後を絶ちません。また、お問い合わせフォームに入力された内容などデータベースと繋がっている情報を窃取するケースもあります。

○サポート詐欺
インターネット閲覧時に実在するIT企業を装い、画面・音声によりマルウェア（トロイの木馬）に感染しているためサポートに電話するよう促すものです。画面に表示された電話番号にかけると、主に外国人（たどたどしい日本語）が応対し、復旧等のためにコンビニでの電子マネー購入など金銭を要求します（詐欺）。個人ほか法人（従業員）が被害に遭うケースもあり、電話の相手の指示に従うと、遠隔操作のソフトをインストールさせられてしまい、PC内の情報を閲覧されてしまう可能性があります。なお、IPAでは「偽セキュリティ警告画面の閉じ方体験サイト」[1]を公開しており、その手法のイメージを確認することができます。

○DoS攻撃/DDoS攻撃
DoS攻撃（ドス攻撃。Denial-of-Service attack）。ネットワーク、その接続された端末に過剰な負荷をかけ、サービス提供できなくしてしまう種類の攻撃をいいます。複数端末から分散的に行われるものをDistributedの頭文字を冠し、DDoS攻撃（ディードス攻撃）といいます。

○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

○PCの紛失、USBメモリなどの記録媒体の紛失

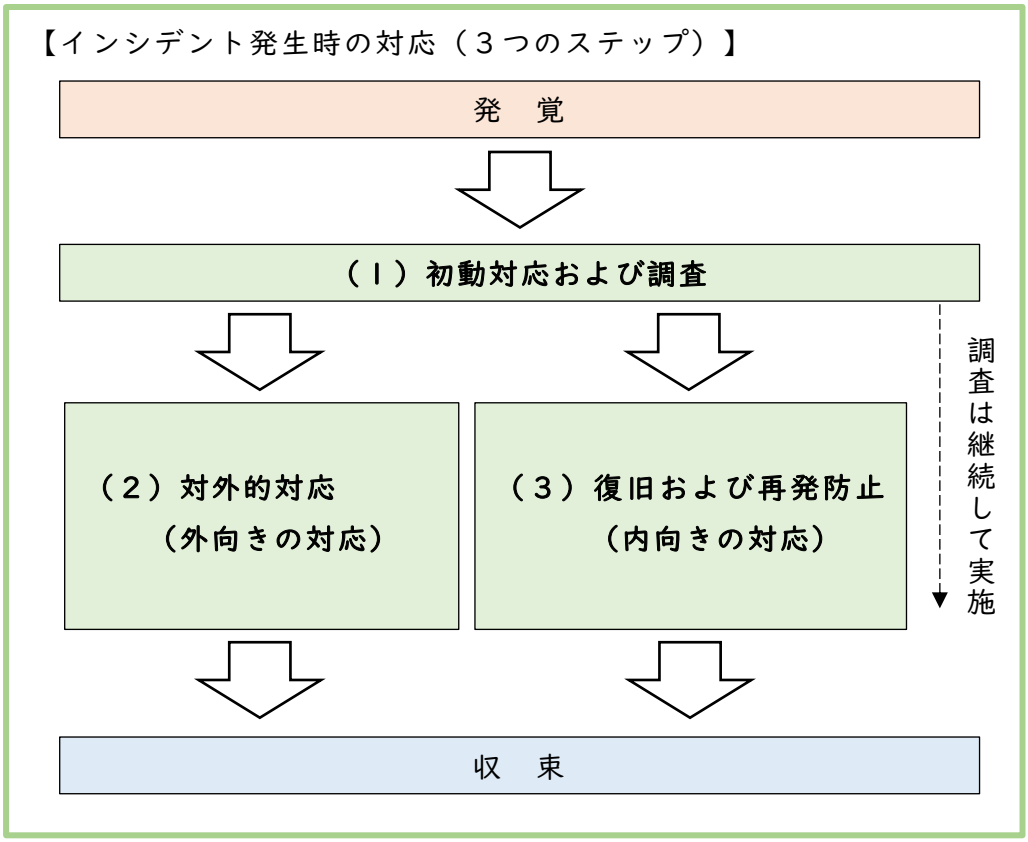
○電子メール、FAX、郵便物の誤送信・誤発送

２．インシデント発生時の対応の流れ

インシデントが発生した場合、ビジネスへの悪影響を極小化する必要があります。適切な対策を実施していたとしても、インシデントの発生を100%無くすことはできません。したがって、事後的な対応（事後対応・事後対策）、つまり、その被害を抑え、迅速な復旧・回復を図るための各種対応が必要となります。

インシデント対応の詳細なプロセスについては、各種団体・組織がとりまとめたマニュアル等（例：NIST SP800-61「コンピューターセキュリティインシデント対応ガイド[2]」、JPCERT/CC「インシデントハンドリングマニュアル[3]」、中小企業目線で考えるならば、IPA「中小企業の情報セキュリティ対策ガイドライン」の「付録8 中小企業のためのセキュリティインシデント対応手引き[4]」）が参考資料として挙げられます。

このレポートでは発覚から収束までの対応を極めて単純化し、次のとおり「（１）初動対応および調査」「（２）対外的対応（外向きの対応）」「（３）復旧および再発防止（内向きの対応）」の３つのステップに大別して説明します。



図表Ⅰ-１ インシデント発生時の対応（３つのステップ）

これら３つのステップごとの対応概要は次のとおりです。

（１）初動対応および調査

まず、インシデント発生直後には、ネットワークの遮断、影響を受けたサービスの停止、情報の隔離など、被害の拡大防止のために必要な措置を講じる必要があります。また、以降の対応方針を決定するためにも、インシデントの原因や影響・被害範囲の調査を行います。この調査活動はインシデントの対応が完了するまで継続して実施します。

（２）対外的対応（外向きの対応）

顧客、取引先など第三者に被害が発生する、または、その可能性がある場合には、被害の拡大防止を最優先として、インシデントの概要や対応方針等を通知・公表していく必要があります。

また、所定の要件に該当する個人情報（個人データ）の漏えいがあった場合には個人情報保護委員会等への報告および被害者本人への通知が必要になるほか、各都道府県警察のサイバー犯罪相談窓口[5]への連絡など行政機関との連携、上場企業等の場合は適時開示なども検討・実施していく必要があります。

（３）復旧および再発防止（内向きの対応）

対外的対応と並行して、インシデントにより情報システムが消失・改ざん・損傷した場合には、データやソフトウェアの復旧およびハードウェアの復旧を行います。

そして、同様の事案の発生、今後の再発を防ぎつつ、顧客、取引先等の関係者が納得する形での、技術・組織・人の3つの観点を踏まえた抜本的な再発防止策を策定し、これを実施していく必要があります。

３．インシデント発生時において生じる損害

インシデントが発生した場合には、前述のとおり、各種対応が必要となりますが、これには相当のコストを要することになります。

また、これら各種対応だけではなく、情報漏えいほか第三者に損害を与えた場合には損害賠償請求がなされる可能性もありますし、サイバー攻撃などによって事業が中断した場合の利益喪失も想定されます。

このレポートでは、各種対応だけでなく、インシデント発生時において生じる損害を次の６つに区分したうえで、それぞれの対応およびそのコストをまとめています。

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（「初動対応および調査」「対外的対応」「復旧および再発防止」等）に関してアウトソーシング先への支払を含め、自組織で直接、費用を負担することにより被る損害をいいます。損害賠償請求により被る損害、事業中断により発生する利益喪失等の損害などは、以下「２．賠償損害」から「６．無形損害」にて取り上げます。

2 賠償損害

情報漏えいなどにより、第三者（被害者個人ほか、委託契約における委託元、クレジットカード会社、取引先等の法人）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をいいます。

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をいいます。

4 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（自組織の資金）の支払いによる損害をいいます。

5 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。日本における個人情報保護法に相当）等において課される課徴金等の損害をいいます。

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をいいます。

～The 座談会「インシデントレスポンス事業者」編～

インシデントレスポンス事業者の方4名に、思うところを聞いてみた～♪（2023年12月実施）

司会　：みなさんおつかれさまです。今日はお呼びたてして申し訳ないです。今日は 4 名のインシデントレスポンスの実務をされている方に、普段思うこと、悩みなどをお聞きできればと思っています。事前にネタをいくつか連絡しましたけど、まずは、フォレンジック調査のレポートについてお聞きしたいと思っています。僕は仕事柄いろんな会社さんのレポートを見る機会があるのですが、インシデントレスポンスの事業者さんが増えているなかで、ナンチャッテ感があるものも散見されるのが気になっているのですが、いかがでしょう？

Ａさん：私も仕事柄、ほかの会社さんのレポートをみることがあるんですけど、確かに「どうなんだろう？」ってものはありますね。例えば、ネットワーク機器（VPN）から侵入されて、社内ネットワーク内で横展開されている場合に、その機器のログ調査だけで終わっていたりする…。「原因はよくわかりません」「それ以降の展開もよくわかりません」といった感じでお客さんが期待しているであろう踏み込んだ調査については、別にやらなくてもいいかのように中途半端に終わっているものもありますね。自分たちのできる範囲で作業を終わらせて当然のように振る舞われても…。

司会　：お客さん側のニーズ、立場を考えた内容になっているのかってところですかね。中途半端とはちょっと違うかもですが、例えば、分量稼ぎにログをベタっと貼っている報告書とかいろいろありますよね（笑）。コスト的な問題はあるかもしれませんけど、エグゼクティブサマリーを冒頭に持ってくるとか、今後の対策について別メニューでもよいので示すとかあったらいいなって思います。って意味だと、なんかフォーマットめいたものってあるんですか？

Ｂさん：フォーマットと呼べるものがあるわけじゃないのですが、見つかったマルウェアやログを並べるだけではどう読み解いてよいのかよくわからないので「なぜ発生したか」「どういう影響があったか」「どう建て直せばいいのか」など収束までわかるようにしつつ、総論をつけるようにしています。うちは、レビュアーを 2 人設けています。調査品質を担保する者、お客さまと相対している者です。後者はお客さまの理解度、要望にあっているかというチェックですね。

Ｃさん：うちも今、Ｂさんがおっしゃったようなことをフォーマットに落とし込みつつ、複数人のレビューをかけて品質を担保するということは必ずやっていますね。

Ｂさん：とはいえ、依頼をいただく企業さんの状況によってちょっと変わるところはあると思っています。インシデントの最初から最後まで調査報告対象にするのか一部分を対象にするのかとか。

Ａさん：確かにケースによって変わってくるというか、例えば、訴訟を意識した場面だと、保全手続きに関する説明の分量は多くなりますね。あとは、顧客の意向を踏まえて危機管理対応の経緯も書いたりとかします。ただ、いずれにしても、インシデントの原因ほかエグゼクティブサマリーや、結果を踏まえて今後どうあるべきかみたいなところを必ず書くようにしています。

司会　：大きく二つに分けて、わかる人とわからない人を意識したレポートだといいですよね。専門組織がある大企業であれば小難しいこと書いてもいいと思いますが、中小企業とかだと専門用語に抵抗感がある人もいるわけで。中小企業を意識した対応ってありますか？

Bさん：そうですね。技術に明るくない方を相手にするときは、注釈を増やす等の対応をしますね。

Cさん：小さい会社になると社長さんがでてきて「俺がIT担当をやっている」みたいな会社もあるんで、前半はやさしく書いて、後半に証跡として技術的な部分を書くとか。最近、裾野が広がってきたというか、中堅・中小の企業さんからの問い合わせが増えていると感じています。あと、中小企業だと価格重視になってしまう、とにかく安いところを選びがちというのは気になっています。この前、ランサムウェア被害に遭ったお客さまからの相談があったんですけど、ある業者に頼んだら「暗号化されたデータの解読は可能。調査は2週間でできます。」みたいな返事があり契約をしたら「データ解読はすぐにはできない、調査は5週間」と。なんとか早くなりませんかと聞いたら「プラス50万円」との返答があったと。調査において何か問題がみつかったら速報いれて欲しいと聞いたらそれも「プラス50万円」との返答があったと。といったところで、その会社信じられないのでぜひ御社にお願いしたいです。みたいな相談がありました（笑）

司会　：あ～。ありがちなやつですね…。緊急時であっても評判とかをみて、どういう業者を選べばいいかってのは考えないとですね。

Cさん：あと、これもつい最近あった別の話なんですけど、サポート詐欺にひっかかってしまった企業さんがいて、インターネットで探した業者に対応してもらったが、対応完了としか報告してもらえない。また、具体的に何をどう対応したのか、どのような被害を受けたかを提示してもらえないため不安になったということで相談を受けました。

司会　：サポート詐欺について、そもそもフォレンジック調査というのは必要なんですか？遠隔操作のソフト以外に、マルウェアが仕掛けられるとかはあるんですか？

Cさん：詐欺の相手方と電話を1時間、2時間繋ぎっぱなしで、遠隔操作までされていると情報漏えい等のおそれもあるのでファイルの転送ログの確認とかですかね。

Dさん：マルウェアを仕掛けるというか、マルウェアが含まれるサイトに誘導するとかはあるみたいですね。

司会　：なるほど。サポート詐欺の被害は確かに増えていますね。ところで先ほど、調査に際して追加費用を何回も請求してくる業者の話がありましたけど、みなさんの会社だと追加請求をお願いすることってあるんですか？

Bさん：基本的にはないですね。でも、マルウェア感染したPCが調査のなかで新たにでてくるとか、調査範囲の拡大が必要になったときは、お客さまとご相談のうえで対応することはあります。

Dさん：うちも事前のヒアリングでざーっと一通り聞いてみて、予算感もお聞きしつつ費用を決めたりとか、時間単価、マックス何時間くらいを要するみたいなことを決めてから着手しますね。

司会　：あと、ランサムウェアにより暗号化されたデータ復旧みたいなことをいう業者の話は気になったのですが、その点、みなさんいかがですか。

Cさん：暗号化されたデータを解読できますよみたいなことを、結構いい加減というか、軽く言っちゃう業者さんいますね。で「やっぱりできませんでした」と。

Ａさん：そうですね。ファイルの先頭部分だけが暗号化されており、一部復元できるとか例外がありますけど、基本的には、解読できないですよね。

Ｃさん：いい加減な業者が「解読できますよ」みたいなことを言って、その業者が優秀に見えてしまうのは辛いところですね（笑）

Ａさん：そういう業者ってマーケティング力は強かったりするんですよね（笑）

司会　：あ～（笑）。Google で最初にでてきたもので判断されちゃうのも考えものですよね…。あと、中小企業だと、フォレンジック調査を依頼して解読できないってことがわかると「じゃ、いいです～」ってなったりするのも考えものですよね。業者さんの選定をどうすべきか？は課題ですよね。

Ａさん：業者の選定って話だと、IDF（デジタル・フォレンジック研究会）や JNSA 等が連名で出しているチェックシート（注）は有用ですよね。

（注）「データ被害時のベンダー選定チェックシート Ver.1.0」。データ復旧事業者に復旧作業を依頼する際にトラブルに陥るケースがあることからその未然防止を目的として作成した選定にあたってのチェックシート
https://digitalforensic.jp/higai-checksheet/

司会　：アレを活用するのはいいですよね。暗号化データを解読可能みたいなことを言っている業者って複数いますし。全然話変わりますけど、ランサムウェアってメールを原因としたものみたことありますか？

全員　：ここ最近、ないですね～

Ｂさん：警察庁が出しているレポートでも割合として低いですよね。予想ですけど大規模な被害にならないからか我々のところまで依頼はきていないのかって感じですかね。

Ａさん：あんまりないですよね。海外だと Coveware（注）のレポートとか見ても一定数メールがランサムウェア攻撃の Initial Vector として記載されたりしてますけど。

（注）ランサムウェアのインシデント対応等の事業を行っている米国企業。ランサムウェアに関して４半期ごとに身代金支払額や侵入経路等のレポートを公表している。
https://www.coveware.com/

司会　：そうなんですよね～。でも「？」というか、日本だとどうなのかなぁと。

Ｂさん：ランサムウェアでメールを使って大規模にってのはないですかね。

司会　：あと、最近、VPN 等脆弱性やばそうなのいっぱいありますよね。A 社、B 社、C 社、D 社等々（実際は実名）

Ｃさん：結構、声かかっていますね。A 社とか B 社の製品・サービスの脆弱性について。

司会　：VPN だと、某省庁の通達なんかだと E 社ばかりが脚光浴びちゃっていますけど、なんかそれだけでいいのか？って感じがしているんですけど、大きく捉えてこの点いかがですか？

Ｂさん：特定の製品ということではなく、保守、アップデートが誰の責任でやることになっているのかというのは気になりますね。保守ベンダーにお金を払っているんだからベンダーがやってくれていると思ってたケースが結構あるんですよね。契約がどうなっているかの確認が必要というか。

司会　：よく聞く話ですよね。徳島の病院の件然り。保守なり更新なり誰がやるか決めましょうという以外に何かその真因に対する解決策みたいなものってないんですかね。

Aさん：保守・更新の対応をするという理想は置いておくとして「止まったらどうするんですか」「誰が責任取るんですか」「システム担当の問題でいいのですか」ということを踏まえた対応は必要なんですかね。「保守・更新をしてしまうと、ほかのシステムへの影響が出てしまう可能性があるので…。」そんな事情、理屈は、攻撃者には関係ないわけで…。

司会　：ユーザー側において、インシデントが起きた場合のことは考えていますか？っての重要ですよね…。では、テーマを変えたいと思うんですけど、何かありますか？

Dさん：技術的な話になってしまいますが、クラウド環境のフォレンジックってどうされていますか？ランサムウェアを含めてクラウド環境の侵害も増えていますけど。

Aさん：うちは、突発的な案件を受けるというより、年間契約での対応が基本なので、平時の段階からクラウド環境のデータをどう保全するのかということまでアドバイスしたうえで対応しています。

Cさん：クラウドも含めて、ネットワーク構成が結構複雑になってきて、フォレンジック調査がやりにくくなってきているというのは正直なところですね。お客さまが構成を理解していないケースとか。

Bさん：そうですね。オンプレはA社、クラウドはB社って感じに複数組み合わせると全体把握ができていなかったりしますよね。コンサルも含めて全体把握している人が必要かなとは思いますね。

司会　：わかりました。あざーっす。1ネタくらいあればと思うんですけど…。

Bさん：じゃぁ私から。件数としては少ないんですけど…。ITベンダーの圧ですかね。フォレンジック調査報告書に対して悪いように書くなみたいな…。ITベンダーが設定したファイアウォールのポリシーの不備が原因であったりすると、報告書は書くべきは書くんですけど、後で怒られるみたいな（笑）

Cさん：確かに。ユーザー企業に報告するときに、この項目は削除してくれないかとか。情報漏えいの痕跡がなくても、明らかに漏れている場合に「痕跡はないんですよね。漏えいしていないですよね」とか。

司会　：あ～。ITベンダーだけじゃなく被害企業からの圧というのもあるんでしょうね。報告書でも「漏えいの可能性がないとはいえない」とか二重否定とか結果的に遠回りな表現になっているのをみると、いろいろあるだろうなぁとか感じます。

Aさん：ただ、我々も言葉尻を捉えられて、変な風に不安にさせたりというのもまずいので、プロフェッショナルとして、例えば6割方やられただろうとか、そんなニュアンスがちゃんと伝わるように説明しないといかんだろうなというのはありますね。

司会　：はい。それでは時間も限りがありますので、これで終わりにしたいと思いますが、どなたか最後に一言いただけないですかね（笑）

Aさん：フォレンジックとかインシデントレスポンスの技術って完璧じゃないというか「手品じゃない」ってことは皆さん認識して欲しいなぁと思います（笑）

司会：「フォレンジックは手品じゃない！」ですね。〆の言葉、ありがとうございます！（笑）本日はお忙しい中、ありがとうございました！

Ⅲ インシデント発生時の対応およびそのコスト

1. 費用損害（事故対応損害）

（１）初動対応および調査

① 事故原因・被害範囲調査費用

ア．概要

インシデントの可能性や具体的な事象が判明した場合、インシデントレスポンスと呼ばれる対応が必要となります。

これら対応は、インシデントの発覚から収束まで、その範囲は多岐に渡りますが、まずは被害の拡大防止と原因調査のため、初動対応としてネットワークの遮断、証拠保全等の措置を速やかに講じる必要があります。

そして、その後の対応方針等を決定する観点からも、インシデントの内容を分析・調査する必要があります。

特にインシデントがサイバー攻撃またはこれに類するものであるときは、フォレンジック調査といわれる、コンピューターやネットワーク機器、クラウドサービス上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を実施していく必要があります。

これら初動対応およびフォレンジック調査は、高度な専門性を要するため、一般的には、インシデントレスポンス事業者と呼ばれる専門の事業者に委託するのが通例といえます。

インシデントレスポンス事業者が行う主な業務内容は、次のとおりです。

〇ネットワーク遮断、証拠保全、被害拡大防止等の初動対応
〇フォレンジック調査
〇初動対応・フォレンジック調査後の対応方針のアドバイス・支援
〇被害者への謝罪、メディアや関係機関などへのコミュニケーションの支援
〇クレジットカード会社との調整支援
※業者によっては、上記業務の一部は行っていない場合もあります。

各種調査は、インシデント発覚直後からその収束まで、継続的に実施することになりますが、例えば、フォレンジック調査は、コンピューターやネットワーク機器、クラウドサービスなどのログを専門家が長時間かけて分析・調査することになるため、場合によっては数週間以上の期間を要することもあります。

イ．アウトソーシング先

インシデントレスポンス事業者

インシデントレスポンスを提供している事業者は、セキュリティベンダーの中でも一部の事業者に限られます。また、大手ITベンダーや大手会計系コンサルティングファームがサービスを提供しているケースもあります。

なお、JNSAではインシデントレスポンス事業者の一覧を作成しており、次のURLからその事業者を確認することが可能です。

JNSA「サイバーインシデント緊急対応企業一覧」
URL: https://www.jnsa.org/emergency_response/

また、JNSAの一覧とは別に、IPAでは、経済産業省が策定した「情報セキュリティサービス基準[6]」に適合すると認められた事業者を「情報セキュリティサービス基準適合サービスリスト[7]」として公開しています。このリストは、複数のサービス分野ごとに分かれていますが「デジタルフォレンジックサービス」の分野でリスト化された事業者が概ねインシデントレスポンス事業を提供しています。次のURLからその事業者を確認することが可能です。

IPA「情報セキュリティサービス基準適合サービスリスト」
URL: https://www.ipa.go.jp/security/service_list.html

なお、このレポートでは、これらの一覧・リストに掲載されている事業者やサービスについての保証等を意味するものではありません。これらの事業者に委託する際には、各事業者とサービス内容や料金等を十分に確認することをおすすめします。

ウ．調査結果（ヒアリング・インターネット調査）

複数のインシデントレスポンス事業者へヒアリングした結果は次のとおりです。各事業者によって、見積りの単位に違いがあることに留意する必要があります。

なお、ファスト・フォレンジックとは、企業等におけるPCを全台調査する必要があるケースなど、早急な原因究明、侵入経路や不正な挙動を把握するため、最低限の必要なデータのみを抽出及びコピーし、解析する手法のことです。

会社	初動対応	フォレンジック費用（PC/サーバー）	ファスト・フォレンジック	過去経験した高額事例
A社	100万円	PC：180万円/台 サーバー：200万円/台	—	3,000万円
B社	個別見積りにて対応	PC：150万円/台 サーバー：250万円/台	300万円 ～5,000台まで	4,000万円超
C社	90万円/台	PC：150～180万円/台 サーバー：200万円/台	350万円 ～50台まで	3,000万円
D社	別途契約	PC/サーバー： 600万円～/1週間	—	1,000万円
E社	200万円/1週間	PC/サーバー： 初動対応費用で対応	初動対応費用で対応	-
F社	10万円/台	PC/サーバー： 100万円/台	—	5,000万円
G社	300万円～	PC/サーバー： 200～300万円/台	60万円/台	約5億円
H社	300～500万円/ 5営業日	PC/サーバー： 初動対応費用で対応 （1～2台）	初動対応費用で対応 10台まで	数千万円
I社	15,000円～/ 時間	PC/サーバー： 15,000円～/時間	15,000円～/時間	3,000万円超
J社	100万円	PC：150万円/台 サーバー：300万円/台	個別見積りにて対応	1,000万円超
K社	100万円～	PC/サーバー： 300万円～/台	900万円～	8,000万円
L社	144万円	PC/サーバー： 120～180万円/台	2,125,000円 ～100台まで	2,000万円超
M社	-	PC：150万円/台 サーバー：200万円/台	個別見積りにて対応	2,000万円超
N社	お客様でご対応	PC：100万円～ サーバー：200万円～	500万 ～50台まで	1,500万超
O社	100万円/ 5営業日	PC/サーバー： 300万円程度	3万円/台	1,700万円
P社	150万円	PC：72万円/台 サーバー：120万円/台	100台程度：6万円/台 1,000台以上：3万円/台	2,500万円超

図表Ⅲ-１-１　事故原因・被害範囲調査費用

エ．コスト総括

インシデントの内容や被害等の内容により調査対象となる端末の種類や数は大きく異なりますが、多くの事例では、フォレンジック調査の対象となる端末は数台となることが多いようです。

この点から、PCとサーバー数台程度の調査であれば、初動対応およびフォレンジック調査を合わせ、概ね300～400万円程度の金額が必要となります。

しかし、マルウェア感染の範囲が拡大した場合など、大規模な被害を受けたときは、ファスト・フォレンジックによる調査の活用も含め、調査の対象となる端末数が増加し、ネットワーク内の挙動等の調査も必要になるため、前頁の「過去経験した高額事例」のとおり、その費用は数千万円以上の額に及ぶ場合もあります。

セキュリティコラム①
「インシデント報告会について思うこと」

～犯人捜しはやめましょう～

様々な企業・団体において、セキュリティに関する障害やインシデントが発生しています。これらの障害・インシデント発生直後はその収束にいろいろ追われた経験をされた方も多いのではと思いますが、喉元過ぎれば何とやらで、その教訓を残して、再発防止に活用している企業・団体ばかりではないのも現状です。

一方で、発生した障害・インシデントの事例を分析し、組織内やベンダーの関係者を集めて、これら事例の報告会・情報共有を行っている企業・団体も存在します。このコラムでは、そういった企業・団体の取り組みを紹介することを通して、1社でも多くの企業・団体でセキュリティに関する障害やインシデントに対してのノウハウを蓄積し、結果としてこれら障害・インシデントの再発防止に寄与することを願って記載します。

障害・インシデント事例の報告会を実施する上での留意点は以下の3点と考えています。

1. 障害・インシデントの原因究明にあたって、犯人探しにならないように留意する
2. 障害・インシデントの真の発生原因まで掘り下げる
3. 取り扱う情報の機密性には注意する

1点目の留意点について

原因を究明するにあたって、どうしても個人の責任にしてしまうことが発生しがちです。

もちろん作業ミスによって発生してしまう障害やインシデントもありえますが、報告会を行う最大の目的は、そういった「犯人探し」ではなく、あくまでも障害やインシデントがどういった経緯で発生したのか、発生に対してどういった対応を行い、どう解決できたのか？を記録に残し、その記録を通して、同様の障害やインシデントが再発しないようにすることにあります。

いたずらに個人の責任を追及しないように留意することが大切です。

2点目の留意点について

発生したインシデントや障害の発生に至る経緯が複雑であるほど、どうしても表面的な原因追及に終始してしまいます。

しかしながら、報告会は、前述の障害・インシデントの再発防止を目的としているので、時間がかかってもしっかりと真の発生原因まで掘り下げていくことが大事です。

例を挙げると、例えば、担当者の操作ミスで情報漏えいが発生してしまった事象の場合、原因は操作ミスということになりますが、何故操作ミスを起こしてしまったのか、操作ミスを防止するための手段は何故有効でなかったのか？、仮に操作ミスを起こしたとしてもセーフティネット的な取り組みは実装されていなかったのか？など、操作ミスを誘発した真の発生原因まで掘り下げて対策を実施することで、次回からは確実に操作ミスを回避することが出来るようになると考えます。

また真の発生原因は、一人で検討するのではなく、複数人で原因を考え議論することで、思い込みや考慮不足を回避することが出来ます。

３番目の留意点について

障害やインシデントを検証する中で、実は企業・団体内の機密情報に触れざるを得ない場合があります。

具体的な例としてあげると、取り扱いに留意すべき個人情報の内容が漏れた事例において、情報漏えいの事実に留まらず、実際に漏れた情報の内容まで具体的に報告してしまうといったことが起こりえます。

しかしながら、報告会に必要なのは、情報漏えいの事実とその原因についてであり、漏れた情報の内容ではないはずです。その点を留意して、必要な情報を整理することが必要となります。

最後に

これらの留意点に留意の上で、障害やインシデントに関する報告をまとめ、報告会の場で社内・団体や関連する取引先・ベンダーにも共有していく中で、その企業・団体における障害・インシデントに関するノウハウ・経験値が蓄積され、セキュリティに関するリテラシーが向上することでしょう。

こういった取り組みをやっていない企業・団体の方も、まずは直近で発生した障害・インシデントの事例から、その原因・経緯を再整理することから始めてはいかがでしょうか？

すぐに結果は出ないかもしれませんが、2年・3年と続ける中で、これらの情報は企業・団体のノウハウ・経験となり、その企業・団体のセキュリティに関する姿勢が劇的に変化していくのではないでしょうか？

これこそがセキュリティに関する障害やインシデントの報告会を実施してく意義と考えます。またそういった企業・団体が増えていくことで、日本国内のセキュリティに関する取り組みも進化していくと信じてやみません。

執筆：「通りすがりのセキュリティエンジニア」

（２）対外的対応（外向きの対応）

①　コンサルティング費用

ア．概要

インシデントによって顧客、取引先など第三者に被害が発生する、または、その可能性がある場合には、被害を受けた（受けるであろう）第三者や世間の受け止め方を念頭にいれた上で、対外的にインシデントの概要や対応方針等を示していく必要があります。

この対外的な発信は、慎重に検討する必要があります。というのも、その内容によっては、顧客、取引先、世間の感情を害してしまい、二次被害ともいうべき事態を招く危険性があるからです。過去に発生した各種の不祥事を見返しても、発信内容に問題があったため、インターネット上での非難・批判（いわゆるネット炎上）を招き、顧客離れや組織の存続が危ぶまれたケース、組織自体が終焉を迎えたケースがあることは周知の事実といえるでしょう。

そのため、これら対応はその初期段階で危機管理・メディア対応を行っている専門業者へ依頼することが無難といえます。専門業者はこれまでのノウハウの蓄積から謝罪時期、謝罪文の内容等につきコンサルティングを実施します。

イ．アウトソーシング先

危機管理コンサルティング会社

危機管理・メディア対応を行う専門業者は、比較的規模の大きい企業から個人事業主まで幅広く存在します。特に、PR会社といわれる企業の広報・PR（パブリックリレーションズ）戦略の後方支援・アウトソーシングを担う会社がその業務の一環として実施しているケースが多いようです。

ウ．調査結果（ヒアリング・インターネット調査）

インターネット上の調査では、一般に危機管理コンサルティングにかかる費用は、一律に定まったものはなく、対応する事案の内容や、その企業との既取引状況（PR関連活動の業務委託内容等）によって左右されるようです。

ある事業者ではアドバイスを行うプロフェッショナル１名あたり１時間5～10万円程度の時間単価に加え、お詫び文等対外的に発信する文章・ツールのチェックでそれぞれ10～50万円程度の料金を設定していることが確認できました。

エ．コスト総括

前述のとおり、対応する事案の内容等によって変わってくるものの、概ね、数十万円以上の額を要することが想定されます。

②　法律相談費用

ア．概要

インシデントが発生した場合、リーガル面を考慮した対応も必要です。

例えば、個人情報（個人データ）の漏えいが発生した場合には、個人情報保護法等の各種関係法令を勘案した対応も考慮する必要があります。特に2022年4月に施行された改正個人情報保護法においては一定の要件のもと、個人情報保護委員会等への報告や、被害者への通知義務が課されているため、この点を踏まえた対応が必要となります。

上記を踏まえると、リーガル面での各種対応は法律事務所へ依頼するのが通例といえます。情報漏えい発生時における次のような各種対応を行う旨をホームページ等で掲げている法律事務所も数多く存在するようです。

〇被害者への通知、その他関係者に対する各種対応策の策定
〇個人情報が漏えいし訴訟が提起された場合の各種対応
〇クレジットカード情報が漏えいした場合の、クレジットカード会社との損害賠償等に関する折衝
〇個人情報保護委員会への報告
〇各国の法制度に即した報告　　等

イ．アウトソーシング先

法律事務所

企業法務を担う大手事務所から個人事務所まで規模感はさまざまです。

ウ．調査結果（ヒアリング・インターネット調査）

インターネット上での調査では、全般的な法律相談の料金として1時間1万円程度（無償としている弁護士事務所もあります）を設定していること、情報漏えい全般の対応など、その後の各種対応を含めた専門的な相談となると、数十万円以上の額を要することが確認できました。また、ヒアリング結果として、大規模な情報漏えい事案の対応を大手事務所に依頼した場合には数百万円以上の額を要することも確認できました。

エ．コスト総括

情報漏えいなど各種対応を依頼する場合には数十万円以上の額を要すること、さらに各国法制度に即した報告などのために大手事務所に依頼する場合には、対応規模にもよりますが、数百万円以上の額を要することが想定されます。

③　広告・宣伝活動費用

ア．概要

各種調査の結果、情報漏えいなど、顧客等に被害が発生していることが明らかとなった場合には、上記①「コンサルティング費用」における危機管理コンサルティング会社、および②「法律相談費用」における法律事務所のアドバイス等を踏まえ、経緯・現状・今後の対応等を記載したお詫び文を作成し、ホームページへの掲載、電子メールでの送付、場合によってはDM（ダイレクトメール）として送付することを検討する必要があります。

また、大量の個人情報が漏えいする等被害規模が大きい場合には、企業が把握できていない潜在的顧客やDMが不通となる顧客が多数存在することも想定されるため、広い範囲に周知する方法、具体的には、信用度・影響度が大きい媒体といえる新聞でのお詫び広告の出稿を検討する必要があるでしょう。

イ．アウトソーシング先

（ア）DM印刷・発送

DM印刷・発送業者

これら業者は、被害が発生した、または発生した可能性のある顧客へ状況、問い合わせ先の周知も含めたお詫び文のDMを送付します。

（イ）新聞広告

新聞社

新聞社のうち、全国紙への出稿は広く周知することが可能です。ただし、顧客層が特定の地域に偏っている場合には、費用も抑えられる地方紙への出稿も選択肢の一つとして考えられます。

ウ．調査結果（ヒアリング・インターネット調査）

（ア）DM印刷、発送

印刷部数、納品（発送）までの日数によって料金が変動しますが、1,000通の印刷・発送を前提として、インターネット上で複数の事業者における価格を調査した結果は次のとおりです。

会社	印刷・発送費
A社	131,425円
B社	122,180円
C社	159,060円
平均	131,425円

図表Ⅲ-Ⅰ-2　DM印刷・発送費

なお、これらの額はインターネット上で、比較的、割安料金にてサービスを提供している業者の価格になります。実績・信用度を加味し既に取引のある印刷業者等に依頼した場合や、追跡確認サービスなど配達状況の確認を実施した場合には、より高い金額が必要となります。

（イ）新聞広告

全国紙に10cm×２段のお詫び広告を出すことを前提に、インターネット上で新聞社各社の価格（臨時広告費用）を調査した結果は次のとおりです。

会社	掲載料
A社	3,520,000円
B社	3,586,000円
C社	2,380,000円
D社	1,600,000円
E社	1,100,000円
全国紙平均	2,437,200円

図表Ⅲ-１-３　全国紙の臨時広告掲載料

一方、地方紙で同様の調査を行った結果（各都道府県の主要地方紙の単純平均）は次のとおりです。

掲載料（平均）
482,894円

図表Ⅲ-１-４　地方紙新聞の臨時広告掲載料

エ．コスト総括

（ア）DM印刷、発送

DM1,000通を送付するにあたっての費用は、１通あたり130円前後となります。印刷部数が増えるにつれて、１通あたりの費用は安くなります。

（イ）新聞広告

新聞広告掲載料は、全国紙では240万円前後、地方紙では50万円前後となります。顧客層、地域ごとの発行部数を考慮しながらお詫び文の掲載紙を決定することが必要になります。

④　コールセンター費用

ア．概要

インシデントによって、顧客の個人情報の漏えい等が発生した場合、またはそのおそれを認識した場合には、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があります。

一般消費者向けの事業を行っている場合には、既にコールセンターを設置・運営しており、自ら対処することも可能かもしれませんが、その煩雑さ等を踏まえれば、コールセンター事業者へ委託するのが一般的といえます。

コールセンター事業者の委託にあたっては、インシデントの規模・内容を踏まえ、設置する場所（コールセンター事業者の施設か自社施設か等）、対応する曜日（土・日・休日を含むか）、時間帯（１日８時間を超過して対応するか）、対応期間（何ヶ月実施するか）等を決定していく必要があります。

情報漏えいのケースにおいては、反響率（被害者のうち問い合わせを実施する人の割合）は概ね全体の１～３％程度であり、対応期間を１～６ヶ月（２ヶ月目以降は問い合わせ数が減少するため、体制を縮小する）にて設定するのが一般的なようです。

コールセンター事業者が実施する主な業務内容は、次のとおりです。

〇FAQやスクリプトの整備
〇スーパーバイザー（オペレーターの管理や指導等を行う要員）やオペレーターへの研修
〇電話番号の取得
〇システムの改修・設定
〇顧客等関係者からの電話受付などの受信業務
〇報告・案内等の発信業務

イ．アウトソーシング先

コールセンター事業者

コールセンターは、コンタクトセンターなど別の名称で呼称される場合もあります。情報漏えいやリコール対応などのクレーム対応の実績を有する大手事業者から、秘書代行のように簡易な取次ぎを行う中小事業者まで、数多く、かつ、幅広く存在しています。

また、専業の事業者もあればBPOセンター（Business Process Outsourcing Center。ある程度まとまった単位の業務プロセスの運営を受託する事業者）や

ITアウトソーシングセンター等の事業者がコールセンターの設置運営も請け負うケースもあります。

ウ．調査結果（ヒアリング・インターネット調査）

個人データ10万件の漏えいで月3,000件受信可能なコールセンターを整備する場合を想定し、クレーム対応実績のある複数のコールセンター事業者へ確認した結果は次のとおりです。

会社	標準的なコスト		備考
	初期費用	運用費用	
A社	約500万円	初月約1,000万円（２ヶ月目以降は縮小） オペレーター10席程度を見込む 通信費は別途	録音は３ヶ月保存が標準
B社	約550万円	初月約1,500万円（２ヶ月目以降は縮小） オペレーター10席程度を見込む 通信費は別途	録音は１年保存が標準
C社	約200万円	初月約500万円（２ヶ月目以降は縮小） オペレーター8席程度を見込む 通信費は別途	録音は６ヶ月保存が標準

図表Ⅲ-１-５　コールセンター費用

なお、初期費用の内訳は、主に人件費（研修費用）、マニュアル等資料整備、設備関係費であり、運用費用の内訳は、主に人件費となります（コールセンター要員の時間単価は概ねスーパーバイザー4,000円～、オペレーター3,000円～）。

エ．コスト総括

初期費用と運用費用の合計について、オペレーター１席あたりの価格に引き直した場合、概ね1ヶ月100～200万円程度の金額が必要となります。例えば、３ヶ月の対応を実施する場合、初月はオペレーター３席、２ヶ月目以降は１席としたときには、700～1,000万円程度の金額が必要となります。

金額に幅があるのは、インシデントの内容、依頼事業者の方針、コールセンター事業者の特性等の費用の変動要素が大きいためと考えられます。

また、価格と品質には少なからず関連性があると推察され、金額ばかりを重視しすぎると本来の目的が果たせなくなる可能性もあります。インシデントは多くの関係者に影響を及ぼす事態とも言えるため、費用をかけて実績面から信頼のできる業者に任せるのも一つの考え方といえます。

⑤　見舞金・見舞品購入費用

ア．概要

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、実被害の状況やお客様との関係性などに配慮し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ります。

この見舞金・見舞品はプリペイドカードとすることが多く、券面額も500円とすることが多いといえます。

ただし「自分の個人情報の価値は500円なのか」と否定的に受け止める被害者も一定数います。株式会社クオカードによる調査[8]によると、個人情報漏えい発生時のお詫びとして、実際に受け取った金額は500円に対し、許せる金額は5,000円と被害者の意識には乖離がある結果が出ています。一方、企業から謝罪を受ける際に重視する項目として「迅速な対応」（88.0%）が最も支持を集め、次いで「謝罪の対応」（65.5%）、「再発防止への意欲」（63.5%）となっており「賠償の金額」は37.5%となっています。過去にはお詫び対応の不備も相俟って、集団訴訟が展開された事例もあるため、その対応の是非については慎重な判断が必要となります。

イ．アウトソーシング先

プリペイドカード販売業者

プリペイドカードも各種種類がありますが、最も普及しているQUOカードについては、正規販売店・正規代理店が多く存在しています。

ウ．調査結果（ヒアリング・インターネット調査）

見舞品として使用されることの多い500円程度の低額帯では、額面＋手数料がかかることがあります。また、カードに企業名等の印刷を施す場合には、印刷費用もかかります。印刷枚数によって料金が割り引かれる場合がありますが、１枚あたりの購入費用がカードの券面額以下になることはないようです。

プリペイドカード額面	１枚あたりの購入費用
500円	530円
700円	750円
1,000円	1,050円
2,000円	2,000円

図表Ⅲ-１-６　プリペイドカード１枚あたりの購入費用例

エ．コスト総括

プリペイドカード購入時には、１枚あたり額面＋手数料が必要となり、さらにその印刷料や送料等を考慮する必要あります。結果として、500円の券面額を有するプリペイドカードを送付する場合には、１枚あたり650円程度の額が必要となります。

⑥　ネット炎上防止費用

ア．概要

インターネット、SNSの利用が一般化した結果として「炎上」といわれる事態が目立つようになりました。ここでいう「炎上」とは、「SNSなどで特定の対象（個人・法人）に対して批判が起こり、それが拡散されて他のメディアも巻き込んで批判が殺到し収まりがつかなくなった状態」や「ニュース等での報道の結果、インターネット上で特定の話題に関する議論が盛り上がり、直接関係のない事象も含めてバッシングが行われてしまう状態」などを指します。

「炎上」による損害は、必ずしも金銭的なものに留まることなく、風評や対象者の心理的なものも含まれ、これをトリガーとして別の損害が発生するなど、影響が無視できないものになりつつあります。

このような「炎上」の拡大を防止するには、その火種ともなるべく事象について、事実かどうか確認できていない情報を発信しないこと、世間の受け止め方を理解しないまま拙速な対応を行わないこと（例：複数人での協議なしに経営者等の想いのみでの発信はしないこと）など、慎重な対応が必要となります。一方的に情報を遮断することなく、事実についてのみ、低姿勢で説明・謝罪することが大事です。

イ．アウトソーシング先

インターネット・SNS炎上対策会社

上記①「コンサルティング費用」における危機管理コンサルティング会社のほか、インターネットマーケティングを生業とする会社の中には「炎上」に関する対策を専門的に支援する会社があります。

これらの会社のサービス内容を見ると

・状況把握のためのインターネット・SNSモニタリング・投稿監視

・炎上傾向や投稿内容変化の分析

・実際の炎上発生や炎上発生抑止に関するコンサルティング

といった内容を提供しているようです。

ウ．調査結果（ヒアリング・インターネット調査）

複数の事業者についてインターネット調査を行ったところ、内容によってのばらつきはあるものの、概ね次の費用を要するようです。

・モニタリング・監視：10～20万円/月

・分析：100～300万円

・「炎上」発生対応や抑止に関するコンサルティング：100～500万円

エ．コスト総括

「炎上」に関する対応は、インターネット上での自組織に関する情報発信・流通の頻度に応じて状況が変わることから、まずはモニタリング・監視といった作業が発生します。その上での分析・コンサルティングとなるため、期間が短くても3ヶ月～1年はかかり、その期間にかかる技術者・コンサルタントの費用として、概ね300～900万円程度のコストを要すると想定されます。

⑦　ダークウェブ調査費用（被害範囲調査費用）

ア．概要

ダークウェブとは、一般的なウェブブラウザーでは閲覧することができない、匿名性の高いネットワーク上に構築されたサイト群をいいます。ドラッグ、銃、盗難物、クレジットカード情報、個人情報、機密情報などを販売・取引するサイトも存在し、マスコミ等では「闇サイト」と表現することも多いようです。

インシデントが情報漏えい事案であった場合、特に発注者や上流メーカー等取引先にも関連する情報など、自組織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強い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になります。

ダークウェブの調査は、高度な専門性を要し、不用意なアクセスは犯罪に巻き込まれるリスクもあるため、専門の事業者（ダークウェブ調査会社）への委託が必要となります。

イ．アウトソーシング先

ダークウェブ調査会社

セキュリティベンダーのなかでも、ごく一部の会社が提供しています。

スレットインテリジェンス（Threat Intelligence。脅威インテリジェンス）と呼ばれる、攻撃者の意図・目的等を証拠に基づきサイバー攻撃の脅威情報を提供するサービスの一環として行われることも多いといえます。

ウ．調査結果（ヒアリング・インターネット調査）

ある事業者へのヒアリングでは、調査の内容や対応する技術者のレベル（例：ダークウェブでやり取りされる各種の言語等の内容を踏まえた調査）によってばらつきはあるものの、次の費用を要するようです。

このヒアリングは一例に過ぎず、事業者によって調査内容のレベルには大きな差があり、簡易な調査であればインシデントレスポンス事業者がその一環として安価にて対応することもあるようです。

・スポット検索調査（３ヶ月）：500～1,000万円
・年間調査：1,500～4,000万円
・認証情報（ユーザIDなど）の情報流出調査：1,000～5,000万円

エ．コスト総括

ダークウェブの調査は、簡易なものから詳細なものまで多岐にわたるため、**調査内容等によってコストは大きく異なる**といえるでしょう。

より高度な技術者を介在させた調査を実施する場合、概ね500万～5,000万円程度のコストを要するケースがあるようですが、これは、機械的な検索結果に加えて人手による分析作業を行うためです。例えば、ダークウェブでは掲示板等のサイトの寿命が一般的なサイトと比較して極めて短くその動静を捉えていくのは難しいと言われています。また、英語以外の言語が使用されているハッキングフォーラム（ハッカーによる情報交換の場）ではそこで利用されるスラング（俗語）も含めこれら言語に精通した要員を調達する必要があります。こうした要素が大きくコストに影響してくるようです。

なお、サービスの契約形態には、定期的な調査を依頼する場合とスポット的に調査依頼する場合の両方のケースがあり、その調査頻度によっても金額は変動します。情報の価値（換金性の高い情報か否か）とダークウェブに流出した場合の影響、想定される調査依頼頻度を考慮しながらサービスの契約形態を決定することが必要になります。

⑧　クレジット情報モニタリング費用

ア．概要

クレジット情報モニタリング費用とは、銀行の口座番号やクレジットカード番号等の金銭決済に用いられる情報ほか、米国における社会保障番号（SSN。Social Security Number）など各種の個人情報、信用情報等が、その情報の所有者以外の者に知られた場合に、その不正使用を監視するために支出するモニ

タリング費用のことです。

クレジットカード情報については国際ペイメントブランド5社が共同で策定したクレジット業界におけるグローバルセキュリティ基準PCI DSS（Payment Card Industry Data Security Standard）において、暗号化など判読不能措置無しに、企業内のデータベースに保存することを禁じています。しかしながら、カード情報非保持のEC加盟店でも、いわゆる「カードスキミング」等のサイバー攻撃によってカード情報が漏えいしてしまうケースが多くみられ、クレジットカード会社を中心に相応のコストをかけてモニタリングが実施されています。

クレジット情報モニタリング費用は、クレジットカード情報以外にも各種の個人情報、信用情報等をモニタリングする費用ですが、このレポートでは、クレジットカード情報のモニタリングにかかるものに限って、そのコスト感をまとめます。

イ．アウトソーシング先

インターネット調査・分析会社、ネットワーク運用会社

現状、クレジット情報モニタリングを生業として事業展開している会社は無く、多くの場合はクレジットカード会社が、自社、または中小のクレジットカード会社であれば業務委託の形でインターネット調査・分析会社やネットワーク運用会社に対して、自社発行カードに関する流通・不正利用を、インターネットの通信ログ点検やカード不正利用検知システムを使って点検しています。

ウ．調査結果（ヒアリング・インターネット調査）

上記のとおり、モニタリングはクレジットカード会社の業務の一環として実施されていることが主体であるため、それにかかるコストは、概ねインターネット調査・分析会社やネットワーク運用会社に関する委託費として処理されていることが多いようです。

・スポット調査：200～500万円
・定期調査　　：100～300万円

エ．コスト総括

モニタリングはクレジットカード会社業務として実施されていることから、各社に対する委託費用として、概ね1ヶ月あたり100～500万円程度のコストを要すると想定されます。なお、大手のクレジットカード会社になると不正利用検知システム利用も一般化しており、業務委託費用以外に当該システム利用コストも委託費用と別に1ヶ月あたり200～300万円程度発生しているようです。

（３）復旧および再発防止（内向きの対応）

①　システム復旧費用

ア．概要

インシデントにより、情報システムが消失・改ざん・損傷した場合、これを復旧するための対応、そのためのコストが必要になります。

このレポートでは、システム復旧費用を、復旧する対象によって、ハードウェア復旧費用とデータ復旧費用に分類した上で説明します。

区分	内容
ハードウェア復旧費用	ハードウェアが損傷を負った場合の修理費用 【具体例】 処理能力を超える負荷による高熱等による損傷、火災や自然災害など外的要因等による損傷、経年劣化による損傷など
データ復旧費用	データが消失または改ざんされた場合におけるその復旧費用 【具体例】 Webページの改ざん、ランサムウェアなどのマルウェア感染によるデータ破壊・暗号化、通常利用で発生したファイルの破損・論理エラーなど

図表Ⅲ-１-７　システム復旧費用の分類

（ア）ハードウェア復旧費用

物理的に損傷を負ったサーバー、PCなどハードウェアの**修理または再調達（修理が困難の場合）が必要**となります。いずれのケースにおいても、そのためのコストが発生し、最大額としてはその再調達の額になります。

損傷の原因がハードウェアの欠陥である場合は、そのメーカー、販売会社との保守契約により修理を受けることができる場合があります。また、HDDなどの大容量メディアの物理的損傷の場合は、データ復旧業者による復旧が可能なケースがあります。

ハードウェア復旧後、初期設定やデータの復旧などの作業が発生することも考慮が必要となります。

（イ）データ復旧費用

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であり、そのための対応が必要となります。バックアップ対策はいわゆる3-2-1ルール、つまり、「3つのデータを作成」「2つの異なるメディアで保存」「1つは別の

場所で保管（オフラインでの保存）」がよく言われるところです。いずれにせよ、BCP対策として、自組織で復旧できる体制を事前用意することが望まれますが、緊急の場合、情報システムの規模やデータ量等に応じて外部に委託する作業コストが発生する可能性があります。

なお、サイバー攻撃を受け、PCがマルウェアに感染している疑いがある場合、これらPCを初期化した上で、バックアップからデータを復旧するため、初期化・初期設定およびデータ復旧のためのコストも発生する可能性があります。

バックアップデータがない、またはバックアップデータも被害にあった場合には、紙データがあればその紙データからの復旧も選択肢となります。数十枚程度であれば自組織でスキャンニングする方法もありますが、AI-OCRによるスキャンニングやデータ作成（WORD等のデータに復旧）の場合、データ量等に応じて外部に委託する作業コストが発生する可能性があります。

イ．アウトソーシング先

（ア）ハードウェア復旧費用

A．損傷を負ったサーバー、PCなどハードウェアを新規購入する場合

システムを構築したITベンダー、BPO事業者等

B．損傷の原因がハードウェアの欠陥であり、保証期間内だった場合

メーカー、販売会社

C．HDDなどの大容量メディアの物理的損傷の場合

データ復旧業者

（イ）データ復旧費用

A．バックアップが取得できている場合

システムを構築したITベンダー、BPO事業者等

B．バックアップが取得できていない場合

紙情報からデータを再入力するとき

OCR事業者、BPO事業者等

ウ．調査結果（ヒアリング・インターネット調査）

（ア）ハードウェア復旧費用

ハードウェア復旧費用は修理・再調達が必要となりますがこれらの費用は機器・スペック等により異なるため、再調達後の、初期設定費用等を調査しました。

Ａ．初期設定費用

初期設定費用とは、標準ソフトウェアを導入する、機器をネットワークに接続する等の費用を指します。

OSセットアップ（初期設定・アップデート）、ネットワーク設定、業務アプリケーションやセキュリティソフトの導入など、詳細は事業者と仕様を相談した上で費用を算出します。

会社	費用	備考
Ａ社	20万円～	機器台数10台程度 PC初期化、初期設定(導入するソフトウェア)等、作業内容をヒアリングの上、見積り提示 別途輸送費が必要
Ｂ社	100万円～	機器台数50台程度 PC初期化、初期設定(導入するソフトウェア)等、作業内容をヒアリングの上、見積り提示 別途輸送費が必要
Ｃ社	110万円～	機器台数50台程度(WindowsノートPC1機種) PC初期化、初期設定(導入するソフトウェア)等、基本仕様書作成(入荷・検品・保管/キッティング・出荷)時にヒアリングの上、見積り提示 別途輸送費が必要

図表Ⅲ-１-８　初期設定の費用

Ｂ．HDDなどの大容量メディアの物理的損傷の場合

大容量メディアの物理的損傷の場合、データ復旧業者にてデータの復旧が可能な場合があります。なお、物理的損傷がなくとも、ファイルシステムの破損、誤操作によるフォルダやファイルの削除、OSのブート障害などの論理障害が発生する場合もあり、さまざまな事象に対して、データ復旧が必要となるケースを考慮する必要があります。

会社	費用	備考
Ａ社	３～20万円程度。場合によって上記以上	定額制。HDDなどの大容量メディアは、障害レベル・メディアの種類・リモート復旧またはオンサイト復旧等によって費用が変動。 USBなどのフラッシュメモリは容量によって費用が変動。光学ディスクは種類による定額制
Ｂ社	４～20万円程度。場合によって上記以上	対象機器等の容量による定額制。対応メディアと障害レベルに応じて費用が異なる。PC・外付HDD・タブレット＞スマートフォン＞USBメモリ・光学ディスクの順で費用が高額になる
Ｃ社	5,000～30,000円程度。場合によって上記以上	総ディスク容量や故障箇所や障害レベルによる復旧工数により費用が変動

図表Ⅲ-１-９　データ復旧業者の費用

（イ）データ復旧費用

Ａ．バックアップが取得できている場合

バックアップが取得できている場合は、バックアップからリストアする作業費が発生します。

会社	費用	備考
Ａ社	7.5万円～	容量により、増加PC10台程度の場合 初期費用：50,000円 月額費用：25,000円（バックアップ容量500GB分を含む） 容量追加は100GB毎に3,000円/月
Ｂ社	15万円～	1日程度の作業 作業内容をヒアリングの上、応談
Ｃ社	20万円～	1チケット19,800円/4時間、購入は10チケット単位を購入し、定型業務1、非定型業務1.25チケットにて委託 週2～３日業務支援するサービスもあり(40万円～)

図表Ⅲ-１-10　リストア(バックアップデータの復旧)の費用

Ｂ．バックアップが取得できていない場合

バックアップが取得できていない場合、もしくはバックアップデータから復旧できない場合、紙情報からデータを作成する方法が考えられます。AI-OCRによるPDF化と人力による元データの復旧について調査しました。

紙情報からのデータ再入力の場合（AI-OCRによるPDF化）

会社	費用	備考
Ａ社	7万円程度～	A4用紙2,800枚想定 原稿状態が袋とじ、製本されている文書は、別途費用が発生
Ｂ社	13万円程度～	A4用紙700枚想定 ホチキス留めは20か所
Ｃ社	28万円程度～	A4用紙3,000枚想定 ホッチキス外しのみ対応・裁断あり 1契約書＝1PDFマルチPDF 任意のファイル名を付与可能

図表Ⅲ-１－11 紙情報からのデータ再入力(AI-OCRによるPDF)の費用

紙情報からのデータ再入力の場合（元データへ復元）

会社	費用	備考
Ａ社	5万円程度～	月20時間1ヶ月自動更新 有期契約の場合、1.2倍の費用
Ｂ社	10万円程度～	実働30時間程度の作業
Ｃ社	32万円程度～	営業事務・バックオフィス業務 初期費用20万円/60時間12万円

図表Ⅲ-１-12　紙情報からのデータ再入力（元データへ復元）の費用

エ．コスト総括

前述のとおり、復旧を要する機器の範囲、データ量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であり、インシデントごとにアウトソーシング先への問い合わせ、見積り依頼等が必要となります。

（ア）ハードウェア復旧費用

Ａ．損傷を負ったサーバー、PCなどハードウェアを新規購入する場合

対応規模や機器により大きく異なります。システムを構築したITベンダーへの見積りが必要となります。

Ｂ．損傷の原因がハードウェアの欠陥であり、保証期間内だった場合

メーカー、販売会社との保守契約により修理を受けることができる場合があります。

Ｃ．PCなどハードウェアを交換した後、標準ソフトウェアを導入する場合

機器をネットワークに接続する等、初期設定費用が必要となり、**数十万～百数十万円の**費用が想定されます。

Ｄ．損傷したメディアからのデータを修復・サルベージする場合

HDD等のメディア１つあたり**数万円～数十万円**の費用が想定されます。

（イ）データ復旧費用

Ａ．バックアップが取得できている場合

バックアップからリストアする場合、自組織で実施するかITベンダー・BPO事業者へ依頼します。費用は**数万円～数十万円**の費用が想定されます。

Ｂ．バックアップが取得できていない場合

紙情報からのデータ再入力の場合、AI-OCRによりPDF化するとき、費用は**数万円～数十万円**の費用が想定されます。元データへ復元する場合、BPO事業者へ依頼します。費用は数万～数十万円の費用が想定されます。

なお、サイバー攻撃がランサムウェアによるものであった場合には、暗号化したデータの復旧を条件とした身代金の要求や、あらかじめ窃取したデータの公表等による脅迫行為が実施されますが、復号（復旧、解除）やデータが公開されない保証はありません。国（経済産業省、厚生労働省、内閣サイバーセキュリティセンター等）においても、金銭の支払が犯罪組織への資金提供とみなされる場合もあり、ランサムウェア攻撃を助長しないよう、金銭の支払いは厳に慎むべきものとして注意喚起を行っています。

また、法執行機関および民間組織が連携してランサムウェア撲滅に向けて取り組むことを目的として2016年7月に設立された「No More Ransom」プロジェクト（https://www.nomoreransom.org/ja/index.html）では、そのサイトにおいて、173種類のランサムウェアに対応する無料復号ツールを公開しており（2023年12月26日現在）[9]。こうした復号ツールを利用することで暗号化を解除し復旧できる場合もあります。

② 再発防止費用

ア．概要

インシデントの収束に向けて特に重要となるのは、再発防止の対応です。

サイバー攻撃の場合、攻撃者はその攻撃に成功した場合、同じ企業・組織を再度狙う傾向があると言われており、同様の事案の発生、今後の再発を防ぐため、その防止策を講じる必要があります。

この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であるともいえます。関係者が納得する形での収束に向けて、抜本的な再発防止策を策定し、セキュリティ対策の強化に資するサービス・製品、教育などの導入に着手していく必要があります。

再発防止策を講じるための費用（再発防止費用）は、インシデントが発生したことにより生じる損失（被害額）として捉えられるものではありませんが、このレポートでは損失の一部として算入しています。再発防止策は、技術・組織・人の３つの観点を踏まえ、網羅的に講じていく必要があります。このレポートでは、再発防止費用を技術的な観点からのセキュリティ製品・サービス導入費用、組織的な観点からの体制構築費用、人的な観点からのセキュリティ教育実施費用に分類した上で説明します。

なお、再発防止策は、種々想定されるものであり、このレポートで掲げた内容（セキュリティ製品・サービス等）に限るものではないことを申し添えます。IPA「中小企業の情報セキュリティガイドライン」[10]やJNSAの「JNSAソリューションガイド」[11]などを参考に、情報資産やセキュリティポリシー、費用対効果等を考慮して製品・サービスを選定するようにしてください。

区分	内容
セキュリティ製品・サービス導入費用	同様のインシデントが生じないようにするためのセキュリティ製品・サービスを導入した場合の費用
体制構築費用	セキュリティ組織の立ち上げや、組織強化を行った場合の費用
セキュリティ教育実施費用	再発防止のためのセキュリティ教育を実施した場合の費用

図表Ⅲ-１-13　再発防止費用の分類

（ア）セキュリティ製品・サービス導入費用

発生したインシデントがセキュリティ製品・サービスの導入によって防げたものであった場合には、そのインシデントの内容に応じ、妥当・適切と判

断されるセキュリティ製品・サービスの導入を検討する必要があります。そして、その導入のためにはコストが発生します。この場合、費用対効果を踏まえた対応も求められるところです。

このレポートでは、中小企業のサイバー攻撃によるインシデント防止を前提として、入口・出口対策としての、メールフィルタリングソフト・サービス、Webフィルタリングソフト・サービス、デバイス制御ソフトを、侵入後の検知対策としてのウイルス対策ソフトおよびEDR（Endpoint Detection and Response）を、被害発生時のリカバリー対策としてのバックアップ、そしてランサムウェアのように情報を搾取する攻撃に対する対策としてファイル暗号化製品・サービスを調査し、とりまとめました。

（イ）体制構築費用

インシデントは、攻撃に対する監視・オペレーションの不備等、組織・体制上の問題を一因として発生するケースもあります。そのため、再発防止策の一環として、これら組織・体制の整備も検討する必要がありますが、その構築のためにはコストが発生します。

セキュリティに関する組織・体制は、大企業では自社でその全部または一部を運用していると考えられますが、中小企業においては人材の確保、コスト上の制約等を考えると、アウトソーシングを主体に検討していく必要があるでしょう。

このレポートでは、こうした状況を踏まえ、SOC（セキュリティオペレーションセンター。Security Operation Center。24時間365日体制でネットワーク等を監視し、サイバー攻撃の検知・分析・対応等を行う組織）のアウトソーシングサービスを提供している事業者を調査し、とりまとめました。

（ウ）セキュリティ教育費用

従業員端末においてマルウェアが添付されたメールを開封してしまう等、従業員のリテラシー不足を契機として、インシデントが発生することは少なくありません。そのため再発防止のためには、従業員教育を図るという視点も必要になります。

従業員に対するセキュリティ教育は、IPAの各種ツールを活用することで、自組織で実施するといったことも想定されますが、多くのセキュリティベンダーで、従業員教育サービスを提供しています。

このレポートでは、標的型メール訓練と、企業向けの教育サービスを調査し、とりまとめました。

イ．アウトソーシング先

セキュリティベンダー・教育事業者

技術・組織・人の３つ観点から網羅的にサービスを提供している事業者もあれば、それぞれの分野、さらに専門性を高めたうえでサービスを提供している事業者など、さまざま存在します。

ウ．調査結果（ヒアリング・インターネット調査）

（ア）セキュリティ製品・サービス費用

セキュリティ対策にかかる製品・サービスを提供している事業者を調査した結果は次のとおりです。

A．メールフィルタリングソフト・サービス

会社	価格 （1ライセンス/1年）	備考
Ａ社	6,000円程度	価格は利用ユーザー数で変動。ストレージサービスに対するスキャン機能も同時提供
Ｂ社	9,000円程度	価格は利用ユーザー数で変動。中小企業向けのライセンスも存在し、割安で購入可能
Ｃ社	1,500円程度	アンチスパム機能や、誤送信対策がオプションとして利用可能

図表Ⅲ-１-14　メールフィルタリングソフト・サービスの価格

B．Webフィルタリングソフト・サービス

会社	価格 （1ライセンス/1年）	備考
Ａ社	3,600円	5ライセンス以上（クライアントソフトを導入する端末）、1年単位での契約 149カテゴリを制御可能
Ｂ社	3,600円 （有害情報対策版） 6,000円 （標準サービス）	10ライセンス以上（インターネットに接続するユーザー数。ただし、認証方式が異なる場合は別ライセンスとしてカウント）。 1年単位での契約
Ｃ社	6,000円	10ライセンスごとに月単位での契約 プロキシを利用してWebトラフィックを危険なドメイン通信を検査

図表Ⅲ-１－15　Webフィルタリングソフト・サービスの価格

C．デバイス制御ソフト・サービス

会社	価格	備考
Ａ社	3,700円	1端末あたりの価格 オンプレミス版（別途サーバーが必要） 最低契約数50台、1年単位での契約 価格は利用台数で変動 別途保守料15%必要
Ｂ社	7,700円	1端末あたりの価格 オンプレミス版（別途サーバーが必要） 最低契約数1台、1年単位での契約 価格は利用台数で変動 初年度保守料込み（次年度以降保守料15%必要）
Ｃ社	300,000円	50端末までの価格 クラウドサービス、1年単位での契約50端末を超える場合、1端末あたり6,000円

図表Ⅲ-１－16　デバイス制御ソフト・サービスの価格

D．ウイルス対策ソフト

会社	価格 （1ライセンス/1年）	備考
Ａ社	3,000円程度	問題解決のサポート有 価格は利用台数および契約年数で変動
Ｂ社	5,000円程度	価格は利用台数および契約年数で変動 １台利用だと高くなるが、複数台利用の場合は安くなる
Ｃ社	2,000円程度	価格は利用台数および契約年数で変動

図表Ⅲ-１-17　ウイルス対策ソフトの価格

E．EDRサービス

会社	価格(1年)	備考
Ａ社	3,240円	最小1ライセンス EDRに加え、MDR（通知、分析、運用代行）を含む 別途初期費用22,000円必要 エージェントインストール設定料、 指導料（通知メール内容や対応方法指導）はオプション
Ｂ社	30,000円	最小5ライセンス 初期設定・導入サポート、EDRに加え、監視及びインシデント調査アラートメールサポートサービスを含む 5ライセンス以上は1ライセンスあたり6,000円
Ｃ社	12,000円	最小1ライセンス EPP+EDR機能/AI自動インシデント対応/ランサムウェア対策、MDR（通知、分析、運用代行）を含む

図表Ⅲ-１-18　EDRサービスの価格

F．バックアップソフト・サービス

会社	価格	備考
Ａ社	40,000円程度	１サーバーバックアップ用ソフトウェアサブスクリプション１年。バックアップアプライアンス（保守5年付4TB）の場合、3,300,000円
Ｂ社	200,000円～	クラウドバックアップ500GB（以降1GB360円） 対象：サーバー・PC 特長： Google Workspace、 Microsoft365のバックアップ取得も可
Ｃ社	228,000円～	別途初期費用（100,000円）、オンサイト設置費用（50,000円）が必要 顧客宅内およびクラウドバックアップ500GB

図表Ⅲ-１-19　バックアップソフト・サービスの価格

G. ファイル暗号ソフト・サービス

会社	価格	備考
Ａ社	1,200～3,400円	オンプレミス版（別途サーバーが必要） 最低契約数50台、1年単位での契約 価格は利用台数で変動。別途保守料15%必要
Ｂ社	600,000円 （50ライセンス）	クラウド版50ID（端末）以内 1年単位での契約 50ID以上は1ID 12,000円/年
Ｃ社	2,000,000円 （30ライセンス）	オンプレミス版30ID（端末）以内 1年単位での契約。次年度以降保守料15%必要

図表Ⅲ-１-20　ファイル暗号化ソフト・サービスの価格

（イ）体制構築費用

SOCを運営している事業者にヒアリングした結果は次のとおりです。

サービス	費用	サービス概要
Ａ社α	初期費用：400万円程度（ログソースの決定、SIEMの検知ルールの作成などを行う） 年間費用：年間500万円程度 必要に応じて追加費用発生（回線準備やSIEMライセンス費用）	24時間365日対応 複数機器を監視し、高度な相関分析を行う
A社β	初期費用：30～40万円程度 年間費用：年間100～600万円程度(定期的な報告会/技術的問い合わせサポートの有無や、ルール/ポリシー設定変更の回数により金額が変動) 必要に応じて追加費用発生（回線準備やSIEM準備費用）	24時間365日対応 対象機器のセキュリティイベントログの分析を行う
B社	初期費用：45万円程度 監視対象：1,000台程度 年間費用：年間252～360万円程度 対象・サービス内容により金額が変動サービス内容(監視/緊急通報（一次通報）/解析通報（二次通報）/運用チューニング/レポート等)	24時間365日対応 対象機器のセキュリティイベントログの分析を行う

サービス	費用	サービス概要
C社	監視対象：5,000アカウントまで（5,000を超える場合は応談） 年間費用：年間480万円(1,000アカウントまで)～(予防/検知/対応/月次レポート/相談窓口他)	24時間365日対応 対象機器のセキュリティイベントログの分析を行う

図表Ⅲ-１-21　体制構築費用

（ウ）セキュリティ教育費用

セキュリティ教育とは従業員に注意喚起するものであり、マルウェアを添付した模擬メールを送信する標的型メール訓練と、Eラーニングによる教育コンテンツを提供している事業者にヒアリングした結果は次のとおりです。

A. 標的型メール訓練サービス

会社	価格	備考
A社	880円 （1人）	オペレーターによるメール訓練のコンサルティング及びユーザーポータルサイトの設定に関する操作説明 訓練結果報告はオプション
B社	300,000円 （配信数100通）	標的型攻撃メール訓練システムへのアクセスアカウントのみを発行し、利用者が自由に訓練内容や配信内容、配信対象を設定し、訓練をセルフサービスで実施可能。アンケート機能有
C社	650,000円 （500アドレスまで）	メール環境のテストから報告書作成まで、手厚くサポート 専門エンジニアの支援により、質の高い訓練や、より詳細な報告書の納品が可能。複数回オプション有

図表Ⅲ-１-22　標的型メール訓練サービス

B. セキュリティ教育サービス

会社	費用	備考
A社	2,000円 （1教材・1人あたり）	2種類（身近な事例で学ぶ情報セキュリティ／標的型メール攻撃とその対策）の教材を利用可能 最低人数100名
B社	80,000円/人	新社会人向けセキュリティ研修。攻撃を実際にデモとして体験したり、ケーススタディでは与えられた状況において実際に自分で考えるなど「確実に身につく」ことを目指した講義内容（集合研修：個社開催の場合は応相談） 全社員様向け教育（e-ラーニング）は338,000円/月（100ID）
C社	150,000円/月 （50IDまで）	初期費用10万円。標的型攻撃メール関連の5教材のみの場合、75,000円/月 E-ラーニング・標的型メール訓練・定期テスト・アンケート機能有

図表Ⅲ-１-23　セキュリティ教育費用

エ．コスト総括

前述のとおり、再発防止策は種々想定され、対応規模によって大きく異なるところですが、このレポートでとりまとめた結果は次のとおりです。

（ア）セキュリティ製品・サービス導入費用

各製品・サービスは、それぞれ１ライセンスあたり年間数千円～1万数千円で導入可能といえます。セキュリティ製品・サービスは導入するだけでなく、その後の運用が重要となるため、運用も想定して選定してください。

（イ）体制構築費用

SOCサービスのグレードによりますが、初期費用および年間費用で**数十万円～数百万円**で利用できます。SOC事業者からの報告を受け社内で対応する組織・フロー等の体制作りも重要となります。

（ウ）セキュリティ教育費用

標的型メール訓練の場合、１人あたり**数百円～数千円**程度、一般社員向けセキュリティ教育の場合、１人あたり**数百円～数千円**程度、セキュリティ担当者向けでは数万円以上のコストがかかります。

③　超過人件費

ア．概要

ここまで記載した「（１）初動対応および調査」「（２）対外的対応」「復旧および再発防止」の３つのステップに共通する費用になりますが、インシデント対応では、企業・団体等における従業員等においても一定の対応が発生します。お詫び、システム復旧などインシデントに直接的に対応する人員ほか、経理、販売等の各システムへの影響がでている場合には、これら影響をカバーするために通常の業務とは異なる対応を余儀なくされることとなります。

この場合、情報システム部門ほか各部門における従業員等の残業代等の超過人件費が発生することがあります。

イ．アウトソーシング先

自組織による対応を想定した項目としてここでは割愛します。

ウ．調査結果（ヒアリング・インターネット調査）

組織の規模、インシデントの規模（対応工数の違い）、その組織の賃金水準などにより大きく異なるため、ここでは割愛します。

エ．コスト総括

上記ウと同様ですが、従業員等への影響範囲等から対応規模により大きく異なります。数名程度による対応もあれば、数十名～数百名、あるいは組織全体での対応が必要になる場合も想定され、超過人件費として、高額な費用負担が発生する場合もあるでしょう。

セキュリティコラム②
「再発防止策の現場」

～「推進サイド」と「現場サイド」の葛藤～

インシデント発生後の再発防止策の現場では、何とかして再発を防ぎたいセキュリティ推進者（以下、推進サイド）と、追加的な業務負荷を増やしたくない現場担当者（現場サイド）で様々な葛藤が生じます。ここではそのような現場のよくある話を両方の立場で見てみます。

よくある話1：サーバーや端末などのIT資産がどこにどれだけあるかがわからない。そのため再発防止策の予想がたてづらい。

現場サイド：IT資産の棚卸には現場協力が必要だが、通常でも忙しいのにやりたくない。過去の担当者は異動しているので仮に指示しても全てを把握するのは難しい。実はキャビネットや倉庫に古い資産があるのだが、ほじくり返されたくない。

推進サイド：IT資産を正確に把握しないと、必要な対策のバリエーションを想定できないし、漏れが生じて再度のインシデント発生が危惧される。面倒がらずにIT資産の棚卸に協力してほしい。

よくある話2：セキュリティ点検を行うと、現場サイドから「〇」（問題なし）ばかりの回答が返ってくることがある。しかし、実態は×（問題あり）ばかりだった。

現場サイド：点検の項目には、100点満点のものはほとんどない。一部実施できている部分もあるが「〇」でない以上、何らかの改善指示がなされる可能性がある。負担を増やさないためにもひとまずは問題なしで乗り切りたい。

推進サイド：点検は再発リスクとなりうる要素を洗い出すためのものなのであり「〇」ばかりなのは通常あり得ない。点検項目の表現が不適切だったか、現場サイドで誤解（場合によっては曲解）している可能性がある。逆に再調査の必要がある。

よくある話3：セキュリティ点検の結果、リスクが大きい現場に対処を依頼すると、社内ルールに記載が無いですよね？という理由で拒否されることがある。

現場サイド：これまでルール違反として指摘されなかったのに急にこちらが悪いように言われても困る。また、既存のルールでも「定期的に」、「対策を導入すること」など表現が抽象的なものも多くどこまでやれば適切なのかわからない。

推進サイド：ルール改定は現在進行中。再発防止策として可能なことは早く実施しないとインシデント再発のおそれがある。それに実は既存ルールでも記載済みの対策が多く、新規の対処策はそれほど多くない。現場には多様なシステム環境、データ、業務等があるため、対策の具体化は現場で検討・判断していただくしかない。

よくある話4：ここまでやれば再発防止策は十分ですという基準やお墨付きを出せと言われることがある。（特に、外部のベンダーやコンサルが関与している場合）

現場サイド：再発防止策としてやるべきことが多いが、いつまでもお金や人を割くわけにもいかないし、長く続くと現場のモチベーションにも影響する。ここまで達成すればOK、という基準を設けてくれれば目標も見えて今後の計画も立てやすい。

推進サイド：攻撃者はわずかなセキュリティの弱点を突いて侵入してくる。そのため、必要な再発防止策はしっかりやって欲しい。また、基本的にリスクはゼロにならない。一度対策がなされても、攻撃者は新たな攻撃手法を作り出して侵入を試みる。これで終わり、というのではなく現場でも危機意識を持ち続けて欲しい。

他にも、サイバー攻撃に対する再発防止策の対処の途中で、なぜか役職が上の方ほどサイバー攻撃よりも従業員による内部不正を気にし出す、といったケースもよくある話です。企業がビジネスを展開する都合上、このような現場サイドと推進サイドの考え方には正解はありません。両者で対話を重ねてより良い再発防止策を実現していただくことが望ましいです。

執筆：「山とサウナを愛するコンサル」
（IT企業でよろずセキュリティ支援に従事）

セキュリティコラム③
「CSIRT 担当が思うこと」

～CSIRTにおける迅速なインシデント対応のポイント～

CSIRT（シーサート。Computer Security Incident Response Team）は、企業等においてセキュリティインシデントが発生した際、その対応を行うチームをいいます。多くの大企業で導入が進んでいます。

このCSIRTが、迅速にセキュリティインシデント対応するために2つのポイントを説明します。

一つ目のポイント

一つ目のポイントは、セキュリティインシデントが発生した現場が迅速に第一報を報告できるようにすることです。何はなくとも、インシデントが起きたらすぐにCSIRTへ報告さえしてくれれば、CSIRTメンバーからの適切な指示や各種支援が期待できます。そのためには、

1. CSIRTの連絡先、セキュリティインシデントの報告先がすぐわかるよう社内のポータルサイトのバナーにインシデント対応連絡先を載せる
2. セキュリティインシデントの報告基準を決めて現場へ周知する
3. CSIRTがセキュリティインシデントをトリアージ（緊急度の判断）するときに最低限必要な情報を決める。それを現場からの第一報の内容として必須化する。電話報告の場合は、連絡担当者(PoC)がヒアリングでその情報を集める

それぞれ、もう少し詳しく説明します。

■CSIRTの連絡先

なるべく目立つところで、すぐに見つかる場所に連絡先を載せましょう。

社内のポータルサイトのトップページの目立つ場所や緊急連絡先の一覧などが良いでしょう。

EメールやSlack，Microsoft Teamsなどのオンラインのコミュニケーションツールの連絡先だけでなく、電話やコミュニケーションツールの音声通話、LINE電話など、音声の連絡先も用意してください。急いで情報を収集したり、指示したりする場合は、やはり音声のコミュニケーションが一番です。

■セキュリティインシデントの報告基準

セキュリティインシデントに気づいたら現場からCSIRTへなるべく早く報告してもらい、すぐに対応を開始したいものです。

初動が早ければ早いほど、被害の拡大防止と復旧までの時間を短縮できます。そのためには、現場がセキュリティインシデントの緊急度を判断できる基準と、報告の目標時間を決めて、現場へ周知して普及を徹底します。一定の緊急度以上だったら、目標時間内に報告するルールにしましょう。

例えば、不正アクセスに気づいたら、かならず三時間以内に報告するよう定めます。軽微なセキュリティインシデントは、報告せずに現場だけで対応することがあります。軽微なセキュリティインシデントと思っても、実は気づかないところで深刻な侵害が起きているかもしれません。軽微でもサイバー攻撃だったら、誤検知かもしれない場合でも報告するようルール化すべきです。

■報告必須内容

現場へルールでインシデントの報告を義務付けると、報告の取りまとめに時間がかかり、セキュリティインシデント発見からCSIRTへ報告が届くまでの時間が長くなりがちです。かといって、不正確な情報を受け取っても困ります。

CSIRTがセキュリティインシデントをトリアージ（緊急度の判断）するために必要な最低限の情報を報告するよう指示します。電話など、音声で報告を受ける場合は、受付担当者が必要な情報を聞き漏らさないように、上記の最低限情報のリストを用意して対応します。

またインシデントの発生現場によっては、インシデントを隠蔽しようとする場合もあります。インシデントを起こしてしまったことよりも、報告ルールに違反して、インシデントを報告しないほうが被害も罪も大きくなることを理解しましょう。起きてしまったことを悔やんでも仕方がありません。まずは迅速に正しく報告して、すぐにインシデント対応を開始して、被害を最小限に抑え込みましょう。

二つ目のポイント

二つ目のポイントはセキュリティインシデントの発生を想定した報告訓練を定期的に行うことです。

報告ルールを決めて現場へ周知しただけでは、セキュリティインシデントが起きたときに、現場のセキュリティ担当者は焦ってうまく行動できません。現場のセキュリティ担当者が、CSIRTへ迅速に第一報を報告する報告訓練だけでも、年一回、実施しましょう。実際のセキュリティインシデントの報告手段を使って、できるだけ本物のセキュリティインシデント報告に近い報告訓練を実施してください。このセキュリティインシデントの第一報の報告訓練の経験があれば、本番でも訓練通りの行動ができて、第一報の報告は成功します。

CSIRTもセキュリティインシデントの対応件数が少なく、CSIRTメンバーの習熟度が低い場合は、年一回以上の訓練を行いましょう。誤った初動対応を防ぎ、CSIRTの指示でただしく証拠保全するためにも、報告優先の訓練は有効です。マルウェア感染したマシンをフォーマットしました！と報告が届いて、がっかりするケースもなくなります。

経営者のみなさん、まずは迅速なセキュリティインシデント報告ができる現場の組織作りから、はじめてみませんか。

執筆：「雪風凧インシデントマネージャ」
（大手IT企業でCSIRTマネジメント）

2. 賠償損害

① 損害賠償金

ア．概要

インシデントが発生した場合に想定される損害はさまざまあるものの、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ます。

情報漏えいについての損害賠償請求は、個人情報が漏えいした場合における被害者個人からの損害賠償請求がイメージされやすいところですが、実際には、他社から管理を受けている個人情報を漏えいした場合における委託元が支出した各種対応費用についての損害賠償請求（求償）など、被害者個人以外の者からの損害賠償請求も多く想定されます。

このレポートでは、情報漏えいを次の４区分に整理し説明します。

区分		損害賠償請求の内容
個人情報の漏えい	自組織が管理する個人情報の漏えい	情報漏えいの被害者個人からの損害賠償請求
	他社から管理の委託を受けている個人情報の漏えい	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

図表Ⅲ-２-１　損害賠償金の分類

（ア）個人情報の漏えい

Ａ．自組織が管理する個人情報の漏えい

被害者個人から慰謝料等についての損害賠償請求が想定されます。

現状は、過去の事例、訴訟への参加率等を考えるに、我が国においては、漏えいした情報の内容や流出規模にはよるものの、損害賠償額は一概に高額になるとは言い切れません。

Ｂ．他者から管理の委託を受けている個人情報の漏えい

個人情報の管理、加工等を委託された企業が、その個人情報を漏えいした場合は、委託元企業が実施した各種事故対応に要したコストの全額また

は一部について、損害賠償請求がなされる可能性があります。その損害賠償額は高額になる可能性があります。

（イ）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があり、その損害賠償額は高額になる可能性があります。

（ウ）他企業の機密情報の漏えい

発注者、上流メーカーなどの新製品情報、特にそれが大企業から預かっている情報が漏えいした場合を想定すれば、その損害賠償額は高額になる可能性があります。

イ．コスト総括

（ア）個人情報の漏えい

Ａ．自組織が管理する個人情報を漏えいした場合

JNSA調査研究部会インシデント被害調査WG（このレポートを作成しているWG）の前身である、セキュリティ被害調査WGが過去公表した「情報セキュリティインシデントに関する調査報告書[12]」では、個人情報漏えい1人あたりの平均想定損害賠償額を独自のモデリングにより算出しています。2016年～2018年の3年間における平均は次のとおりです。

したがって、漏えい人数に次の額を乗じた額が、個人情報の漏えいにおける最大の損害賠償額として見込むことができます。

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ヶ年平均	28,308円

図表Ⅲ-２-２　個人情報漏えい1人あたりの平均損害賠償額

（出典：JNSA）

【参考：訴訟参加率の考慮】

個人情報漏えい事案においては、漏えいした情報の内容に拠るものの、損害賠償請求に至るケースは現状、我が国では多くないといえます。

その一方で、企業による事故対応が不十分で被害者感情の高まりをみせた場合には、SNS等による呼びかけを契機として、集団訴訟が展開されるケースもあります。この点、我が国においては、大手教育企業の個人情報漏えい事件による集団訴訟が有名です。同事件では約3,500万人の被害者に対し、約１万人の方が訴訟に参加しており、１万人÷3,500万人で、訴訟参加率としては約0.03%という計算になります。

訴訟参加率は当然その事案の内容によって違いがでてくるものであり、単なる一つの目安ではあるものの、漏えい人数に対し、個人情報漏えい1人あたりの平均損害賠償額に対し、この約0.03%を乗じた額が情報漏えい１事案あたりの想定損害賠償額と推定することもできます。例えば、100万人の個人情報漏えい事件の場合であれば、1,000,000人×約**8.5円**（28,308円×0.03%）＝850万円を想定損害賠償額とみることもできるでしょう。

B．他社から管理の委託を受けている個人情報を漏えいした場合

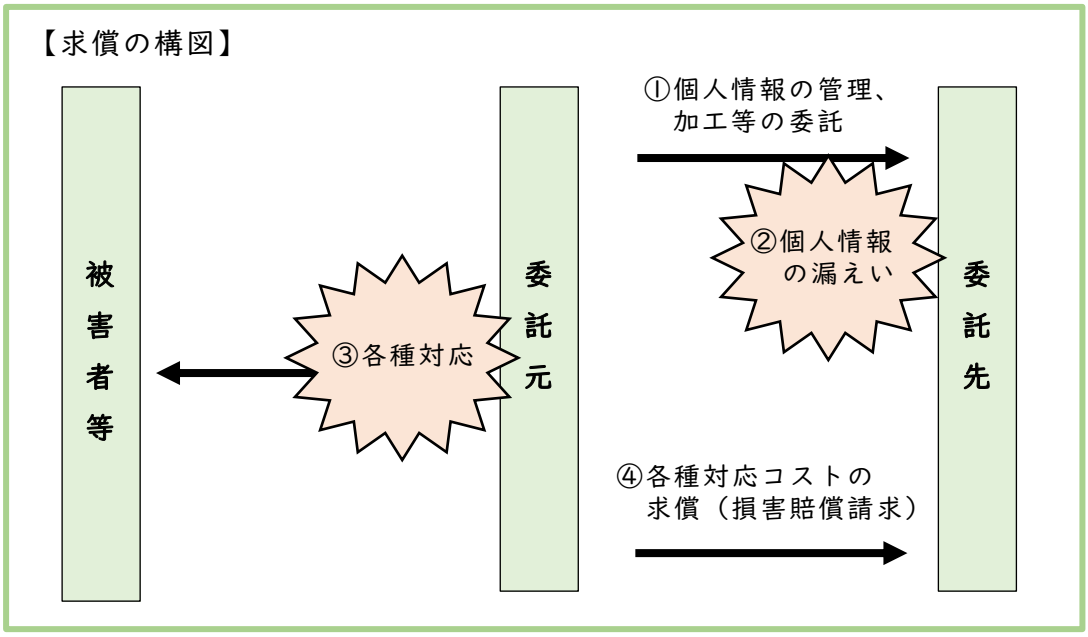
例えば、システム会社やSaaSなどのクラウドサービス事業者が他企業からデータ処理等を依頼された個人情報を漏えいしたケースや、販売店・下請企業がメーカーや元請企業から管理を委託されている個人情報を漏えいしたケースなど、個人情報の管理・加工等を委託された企業がその個人情報を漏えいした場合は、通例、委託元企業において前述「１．費用損害（事故対応損害）」に記載したような各種事故対応が必要となります。特に2022年4月の改正個人情報保護法の施行により、委託元においても個人情報保護委員会等への報告等の対応が必要となっていることも考慮する必要があります。

そして、最終的にはこれらの各種対応に要したコストが委託元から委託先への損害賠償請求（いわゆる「求償」）という形に変わって、委託先の損害として発生することになります。

この場合の損害賠償金の額は、各種事故対応に要したコストの合計額がベースとなります。

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りますが、結果として、損害賠償金の額は中小企業であったとしても**数千万円～数億円**といった額になることが想定されます。

なお、このような高額な損害賠償責任を負わないようにするため、契約書において損害賠償額の上限を設定する条項等を規定することが一般的といえますが、委託先に故意または重過失があった場合には、当該規定が認められない可能性が高いことにも留意する必要があります。



図表Ⅲ －２－３　求償の構図

（イ）クレジットカード情報の漏えいの場合

クレジットカードの不正利用は、年々増えており、一般社団法人日本クレジットカード協会の調査[13]によると、全体として、2015年は120.9億円であったのに対し、2023年は401.9億円と３倍強と急増している状況にあります。

特に特筆すべきは、ECサイトでの不正利用に代表される番号盗用被害です。2015年は72.2億円であったのに対し、2023年には376.3億円と、5倍強となり、不正利用全体の９割を占める状況にあります。

その一方で、インターネットでの通信販売に取り組む企業は、ここ数年で大きく増えています。Amazon、楽天などの大手ECサイトに出店するほか、自社でECサイトを構築する企業も多く存在します。自社構築の場合には、セキュリティ対策について相当のコストをかけ強化することが必要となりますが、不十分なため、サイトが改ざんされる等により、クレジットカード情報が攻撃者の手に渡るケースは枚挙に暇がなく[14]、中小企業においても多くの被害が発生しています。

ECサイトからクレジットカード情報が漏えいした場合には、加盟店契約に基づき、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ケース、またはチャージバック（クレジットカードの不正利用があった場合にカード会社がその販売代金について加盟店への支払を拒否するもしくは返還を求めること）といわれる制度により不正利用の額についてカード会社に対する請求が認められないケースが発生しえます。この場合、クレジットカード情報の漏えい件数が多い場合にはその額も高額となります。

2020年にある大手カード会社が行った調査[15]では、不正利用の被害額は平均で1枚あたり**約10万円**との結果が出ています。

したがって、例えば、カード情報が1,000件漏えいした場合を想定すると、不正利用される割合を30%とするならば、1,000件×10万円×30%で3,000万円、さらに再発行手数料（多くは1,100円）で1,000件×1,100円で110万円となり、合計3,110万円の損害賠償金が生じることが想定されます。

（ウ）他企業の機密情報の漏えいの場合

企業が有する機密情報の経済価値は、個人情報のそれとは大きく異なることはいうまでもありません。

例えば、部品・原材料等を製造する下請メーカーが完成品メーカーから預かった新製品に関する情報、金融機関が預かっている顧客等の信用情報、建設業者が預かっている顧客の新築建物の警備状況等のわかる図面など、これら情報が漏えいした場合には、その被害の規模からして、高額な損害賠償請求がなされるおそれがあることは、想像に容易いといえるでしょう。

この点、経済産業省では「営業秘密～営業秘密を守り活用する～」[16]としてそのサイトにおいて各種資料を取りまとめています。同資料では営業秘密の漏えいにより**数百億円**規模の訴訟が提起された事例が挙げられていることからもわかるように、他企業の機密情報の漏えいは、計り知れない損害を招くことが想定されます。

②　弁護士費用等その他各種費用

ア．概要

損害賠償請求がなされた場合、その結果として生じる損害は損害賠償金だけではありません。

まず、法的課題に対処していくためには弁護士への委任を検討する必要が生じます。

また、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想定されるところです。

以下、このレポートでは、弁護士に委任を行った場合のその費用にスポットを当て、そのコストについて記載していきます。

イ．コスト総括

弁護士費用は、着手金と報酬金の2種類に分かれます。前者は結果の如何に関わらず支払う必要がある費用、後者は結果が成功した場合に支払う費用となります。

弁護士費用は、2004年4月から、それまで日弁連が定めていた報酬基準（旧基準）が撤廃されており、個々の弁護士がその基準を定めることになっています。その意味では、いくらくらいかかるか？といったことは、ケースバイケースということになりますが、旧基準に拠る弁護士事務所も多く、この基準が一つの目安になるといえるでしょう。

旧基準の額は次のとおりです。したがって、例えば、損害賠償請求訴訟の額が1億円である場合には、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）ということになります。

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	3%＋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

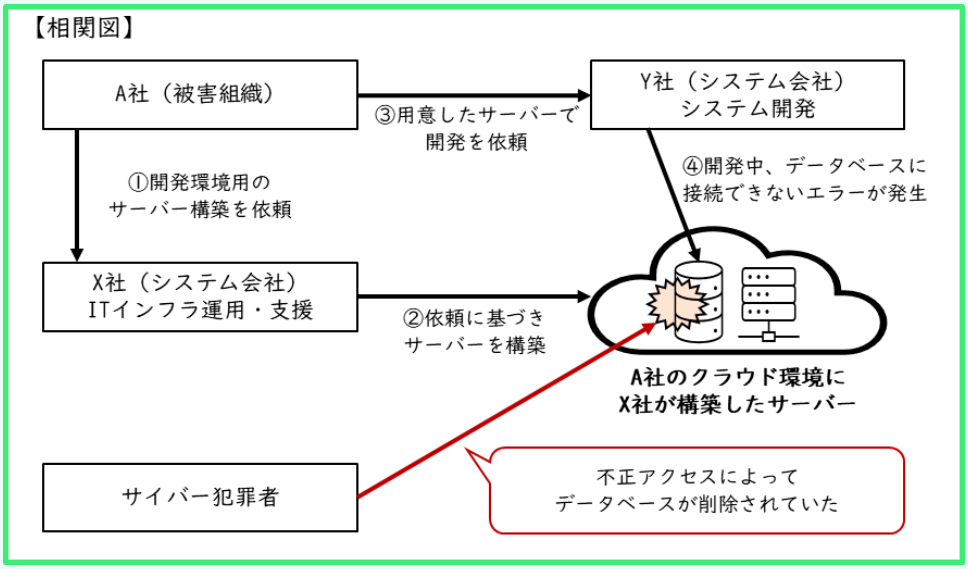
図表Ⅲ-２-４　弁護士費用等その他各種費用

なお、訴訟で勝訴したとしても、相手方が認容された損害賠償額を支払わない場合には、民事執行手続を実施する必要があり、この場合、別途費用が発生することにも留意する必要があります。

セキュリティコラム④
「リスクコミュニケーションの重要性」

～インシデント対応の現場から　その１～

インシデントレスポンスの現場では、被害を受けた端末やサーバー、ネットワーク機器等の設定・運用を行う会社など、被害組織以外にも様々な利害関係者が存在することがあります。これら利害関係者の責任範囲が明確になっていない場合、インシデントに対する認知や認識、各々が抱く懸念などによって意見の対立や衝突が発生し結果として、復旧までに多大な時間と費用を要することがあります。
本コラムでは、筆者がフォレンジック調査を対応した案件で実際にあった、利害関係者間のトラブル事例をご紹介します。



そのインシデントは、A社（被害組織）のITインフラ運用・支援を行っていたX社（システム会社）が構築したサーバーで発生しました。A社には直接開発や運用を行う部門が存在せず、システムの開発を行う際は、A社から依頼を受けたX社がサーバーの構築を行っていました。これらサーバーは、A社が契約するY社（X社とは別のシステム会社）へ提供され、システムの開発が行われる体制となっていました。

ある日、A社の担当者が開発中のシステムの状況を確認するため、アクセスしたところ画面にエラーが表示されてしまい、利用することができなくなっていました。A社の担当者はY社へ問い合わせを実施、Y社が状況を確認したところ、システムのデータベースが壊れているとの回答がありました。また、X社にも問い合わせたところデータベースが削除されていることがわかりました。

この時、A社は、Y社が誤って削除したのだろうと、X社にデータベースの再作成を依頼しました。Y社にはデータベースが消えていたので再作成をX社に依頼した旨を伝えて、もともと予定していた開発工程に再着手するよう指示しました。しかし、数日後、開発中のシステムで同様の事象が発生し、今度はX社に原因の詳細調査を依頼したところ、サーバーのログから、データベースの削除は不正アクセスによって行われた可能性が高いことが判明しました。

当該システムは開発中であったため、本番環境における利用者の個人情報などは含まれていませんでしたが、検証用に登録したA社とY社の従業員の個人情報が含まれていました（テスト環境で実際の個人情報を使用することが問題ですが…。）。そこで、A社はX社に対して、より詳細な調査を求めました。そこで、筆者が所属する企業がフォレンジック調査の対応をすることになりました。

調査の結果、開発中のシステムにはアクセス制限が行われておらず開発や検証に利用されていたデータベースの管理ツールにも、容易に推測可能なユーザー名、パスワードが設定されていたため、データベースの管理ツールに不正アクセスされてしまい、データベースが削除されていたことが判明しました。

その後、A社、X社、Y社の担当者が参加のもと、フォレンジック調査の報告会が開催されました。不正アクセスの原因については全員が理解したものの、A社やY社の従業員の個人情報漏えいや、不正アクセス被害によって発生した調査費用を誰がどのように負担するのかその責任が誰にあるのかで議論が紛糾しました。

A社は、セキュリティはX社やY社が適切に対応していると考えていました。一方、X社は、依頼に基づく構築・設定作業を行う立場であり、アクセス制限の設定依頼は受けておらず、要件通りの対応を行っていると考えていました。また、Y社は、A社から開発用に安全な環境が提供されているものと考えており、提供されたアカウントのパスワード変更や開発しているシステム以外のログ確認などは行っていなかったため、不正アクセスに気付くことはありませんでした。

A社は当初、調査結果に基づく対策を講じなければ開発の再開は行えないというスタンスのもと、責任がX社にあるならば費用はX社が負担すべき、また、責任がY社にあるならば費用はY社が負担すべきといった考えを持っていました。しかし、最終的には、X社では依頼された作業を要件どおりに対応していること、Y社は不特定多数からアクセスされる状況は想定していなかったことから、A社がアクセス制限設定を配慮していなかったこと（X社に依頼をしていなかったこと）が原因であるとして、不正アクセスにかかる調査費用の負担はA社とすることが決まりました。ところが、調査費用の負担とは別に、検証用に登録されていた個人情報の漏えいの責任については、その後も3社間で話がまとまらず、開発は長期に渡って凍結されることになりました。

このように、利害関係者間の適切なコミュニケーションが図られていないと、インシデント発生時の初動対応や復旧作業に支障を来すほか、復旧後も意見の対立や議論の紛糾が起きてその後の組織運営や業務に大きな影響を及ぼします。近年、急速なデジタル化やクラウドサービスの活用によって利害関係者が増え、誰が何に責任を負うのかを的確に把握することが難しくなっていますが、ITインフラの運用管理やセキュリティ対策でトラブルを起こさないためにも、すべての利害関係者は予め発生する可能性のあるリスクについて話し合い、相互理解を深めながら合意を得ていく、リスクコミュニケーションを行っていくことが大切です。

様々なリスクが取り巻く状況の中、たとえインシデントが発生してしまった場合にも不要なトラブルが防げるよう関係者間でリスクコミュニケーションを行い、信頼関係を構築していきましょう。

執筆：「お酒を愛するフォレンジッカー」
（インシデントレスポンス会社で業務に従事）

～The 座談会「弁護士」編～

サイバーセキュリティに携わる弁護士の方4名に、思うところを聞いてみた～♪（2023年12月実施）

司会　：みなさま、おつかれさまです。なんかすごいメンバーにお集まりいただきましたけど、今日はIT・セキュリティにも知見の深い4名の弁護士の方にいろいろお話をお聞きできればと思っています。事前に連絡しましたが、論議したいネタがいっぱいあるんですけど、長時間拘束するわけにもいかないので、どのネタにしましょう。

A先生：絞るとすれば、SaaS事業者がサイバー攻撃を受けた場合の責任論とかはどうでしょうか。今年は、SaaS事業者がランサムウェア感染して、そのユーザー企業等が影響を受けた事案が多かったように思います。

司会　：そうですね。今年の印象的な出来事ですもんね。法律論って意味でも論じるところは多々ありそうですよね。では、それでいきましょう。

A先生：SaaS事業者の責任論でいうと、抽象的にはセキュリティ義務という考え方があると思います。その違反ですね。もう少し具体化すると、契約において秘密保持義務というのもあると思います。秘密保持義務違反。また、サービスが提供できなかったところでの提供義務違反。こういった2つ又は3つの義務違反があるのかなと。また、契約書の免責条項との関係であったり、生じた損害についてどこまでが認められるかという損害論もポイントになってくるかと思います。

B先生：そうですね。ランサムウェア感染が発生した場合、いろいろな損害が発生します。SaaS事業者のユーザー企業のデータが暗号化されて、元に戻せなかった場合の責任追及が典型ですね。あるいは、サービスを利用できないことでユーザー企業のビジネスが停止したことへの責任追及とか。そういったいろいろな損害について、ランサムウェア感染による直接損害だけを捉えるか、間接損害も含められるのかどうか。特にビジネス停止に起因する損害に関しては、SaaS事業者側の復旧が遅れてユーザー企業のビジネスに影響がでた場合に、その復旧遅延を捉えて損害賠償請求が認められるかといったところも論点になりそうです。そして、A先生がおっしゃたように、契約書の免責条項や損害賠償の制限条項が、故意・重過失を絡めてどこまで認められるかも実務上問題になってくるのかなと。

C先生：事前対策と事後対応との関係性で、事前対策が十分であったとしても、事後対応が不十分だったらそれについて損害賠償請求もあり得るということですよね。

B先生：はい。損害の拡大を招いたみたいな場面ですね。

A先生：事後対応の適否が問われると、ランサムウェアによる身代金を払わなかったがゆえ回復が遅れたみたいなことも言われかねず悩ましくなってきますね。

C先生：バックアップデータも一緒に暗号化された場合に、オフラインでバックアップをしておく等の対応をしていなかったことが故意・重過失にあたるかとかも結構難しい問題ですよね。

司会　：確かに今年起きた事象でも、完全復旧まで相当期間を要した事例はありましたね。長期化することで賠償問題どうなるんだろうみたいな。

D先生：SaaS事業者とそのユーザー企業、さらにそのユーザー企業に顧客がいる場合（注）までを考えた場合さらに難しくなりますよね。例えば、SaaS事業者のサービスが止まったとしても、ユーザー企業がこのことを踏まえた自らのBCP（事業継続計画）をしっかり策定していれば、ユーザー企業の顧客への影響もないわけで。そういったところでの議論もあり得ますよね。

（注）SaaS事業者がユーザー企業（典型的には法人や個人事業主）にサービスを提供し、当該ユーザー企業がSaaS事業者のサービスを前提に、当該ユーザー企業の顧客に対して、さらにサービスを提供する場合

C先生：ユーザー企業は、ユーザー企業の顧客に対してサービスを提供するためにSaaS事業者のサービスを使っているわけですが、SaaS事業者のサービスはかなり複雑化していますね。そのため、ユーザー企業が仲介事業者のような立場で、そのサービスに対する専門性を有していないケースもあったりするわけですが、例えば、顧客の方がユーザー企業よりもセキュリティレベルが高い場合もあり得ます。このような状況下で、ユーザー企業の顧客に被害が発生した場合に、ユーザー企業がその被害を法的に保護しなければならないのかというのも難しいですよね。

D先生：あと、ユーザー企業の顧客に発生した被害について、ユーザー企業が責任を負うとするならば、ユーザー企業がその賠償等を負担することによって生じた損害をSaaS事業者に対して求償請求するわけですよね。

A先生：全額求償請求できるとは限らないですよね。SaaS事業者からすれば相当因果関係の範囲でのみ賠償責任を負うとして対抗しますよね。

C先生：SaaS事業者は、ユーザー企業に対して、例えば、冗長化であったり、代替手段を用意したりするなど、どこまで義務があるかってことなんですかね。SaaS事業者からすれば、ユーザー企業が顧客に対して提供するサービスをSaaS事業者に丸投げした形で利用しているのだから、ユーザー企業の顧客の損害についてまで面倒見切れないみたいな話になっていて、契約で限定するのが通常でしょう。

B先生：サービス提供者がユーザー企業のデータを消失してしまった場合に、ユーザー企業がサービス提供者を訴えるというのは過去の裁判例でも見られますが、ユーザー企業がバックアップを取っていればよかったわけで、そのバックアップの義務があるかどうかは契約の内容とかから考えるということかと思うんですけど、今の議論も契約上、ユーザー企業にどこまでの義務があったかというところによってくるんでしょうね。

A先生：過失相殺を考えた場合、請求者（ユーザー企業）側の義務違反または過失を考える必要はでてきますね。

B先生：過失を分解すると、結局、予見可能性と結果回避義務になりますね。

C先生：そうすると、やはり注意義務違反が問題になりますね。

D先生：結局、契約上明確に義務内容を規定すれば非常にわかりやすいけれども、ない場合どうするのかみたいなことですかね。過去の裁判例で、ECサイトを構築したベンダーの責任に関するものがありますけど、その裁判例では、契約上明確な規定がない事案において、その当時の技術水準に沿ったセキュリティ対策を実施することが黙示的に合意されていたと認定されています。そうすると、SaaS事業者側が当然やるべきことはやったのかという議論になりやすく、事案にもよりますが、ユーザー企業にも過失相殺における過失があるというSaaS事業者からの主張は難しい傾向にあるのかもしれませんね。

C先生：その事案において、他にユーザー企業側の注意義務が考えられるかですよね。

A先生：コストを抑える観点からある一つのSaaS事業者のサービスを使っていたがゆえ、人的リソースを確保できておらず、その結果、有事に十分に備えていなかったという点で、の義務違反又は過失を見いだすのはどうでしょうか。

B先生：損害防止軽減義務みたいな議論はありますよね。SaaS事業者が止まっちゃったから何もできませんってのは違うでしょ、って話はあり得るかと。

A先生：確かにそうですね。

司会　：SaaS事業者への責任追及、SaaS事業者の対抗の視点みたいなさまざまな観点からのお話になっていますが、ところで、SaaS事業者というかベンダー目線で考えた場合、契約料金的にそこまでの責任は負えないと言いたい事案もあると思うんですけど、その点いかがですか？

D先生：裁判所の考え方としては、そうした発想も持っているのではないかと思います。例えば、1億円の損害が発生しそうな業務を、月2万円の料金の業務のなかで対応しなければならないのか？みたいなことですよね。お互いの契約のなかで、合理的な意思解釈として、どこまでの業務をやることを約束していたのか、という視点が重要になってくるかと思います。

B先生：契約書で明文化されていれば従うことになりますし、ない場合には、契約締結に至った過程とかも踏まえた契約の趣旨の解釈みたいな話になるんでしょうかね。

C先生：今の話だと、契約書に記載があればそれで結論が決まってしまい、記載がなければどっちに倒れるかわからないみたいな印象を持ちましたけど、もちろん基本は契約書が第一義的ではあるものの、それだけではないというところもあるかなとは思います。

B先生：失礼しました。確かに仰るとおり、文言上義務があるとしても、解釈の幅はありますね。さきほど挙がった契約金額についても、義務の具体的内容を社会通念に照らして導き出すための要素の一つだと思います。

司会　：まとめるのが難しくなってきましたね（笑）。形式論から実質論まで議論が始まってしまうと（笑）乱暴ですけど、話の流れからして、各当事者において契約書、そして契約上の義務を考えておく必要があるというところでしょうか。あとは損害論も話したかったところですかね。

D先生：各当事者において発生する責任を考えた場合、まずは契約内容をしっかり考えましょう、ということですかね。

A先生：そうですね。義務は「情報漏えいについての秘密保持義務違反」あとは「サービス提供義務違反」この2つにスポットを当てればいのかなと。

C先生：損害論ですけど、ランサムウェアの二重脅迫の被害に遭って、被害組織の取引先等の情報が晒されてしまったようなケースを想定した場合、データが漏えいしたおそれがあることよりも、リークされたことによって損害が拡大するのかという点は、気になっているんですよね。

D先生：リークされたことにより損害は拡大する傾向にあるのではないかとは思っています。リークサイト（注）に掲載がなく、データが漏えいしたおそれがあるにとどまる状態だと、そもそも損害の立証が難しいかなと。ただ、リークサイトに掲載されたとしても、結局、それがどう悪用されたのかもわからないので、損害の算定は難しい面がありますよね。

（注）ランサムウェアの犯罪者グループが窃取した情報を晒しているサイト。主にダークウェブ上に設置されている。

B先生：情報が漏れた場合にその情報の価値をどう損害として算定するかってのは一般的に難しいですよね。結局は調査にかかった費用などの実費ベースでの賠償問題になりますかね。

C先生：実際に漏えいしたってケースと、漏えいしたおそれのあるケースとで、損害の範囲も立証の困難性も異なるってことですかね。

B先生：おそれのケースだと、具体的な損害額の立証はさらに難しいですよね。

D先生：おそれのケースでも、例えば、極めて機密性が重視される重要インフラ設備などの図面や仕様書が漏れたような場合で、セキュリティ対策のために改修をしたとかであれば、損害が認定されるケースもあるようには思われますが、例外的な事例ですね。

C先生：そうだとするなら、データが漏えいしたおそれがある状況からリークサイトに掲載されましたというケースに発展した場合において、被害が増えるのかというと変わらない可能性もあるんですよね。リークされる場合と、されない場合とで何か違いはあるのかってことをアメリカの弁護士にも聞いたことあるのですが、わからないって言っていましたね。

B先生：グローバルにみると結構、国によって違う感じはありますよね。日本の個人情報保護法だと「おそれ」の概念があるけど、GDPRにはなかったり。

A先生：アメリカだと、サイバー攻撃事案は、原告弁護士としても経済的にメリットがあるためか、クラスアクション（集団代表訴訟）が起きやすくなっていますね。クラスアクションでは、最終的に和解に進み、高額な賠償金支払いとして終わるので、「おそれ」かどうかってのはあまり関係ないというのもありそうです。別の話でいうと、アメリカでは、リークサイトに掲載されるとクラスアクションでの賠償額が増加しかねないので身代金を支払うべき、という助言をする弁護士もいると聞いたことがあります。

司会　：議論が尽きませんね（笑）。いろいろなネタがあるので何時間あっても足りないところですが、時間もきたところでこの辺で終わりですかね。どうまとめればいいのかわかりませんが、何か結論めいたものを示すということではなく、契約、義務、損害論等々について、いろいろな論点、そして考え方があるということで、この座談会に意義があったというところでしょうか（笑）本日は長時間ありがとうございました。

3. 利益損害

ア．概要

サイバー攻撃が発生した場合に想定される損害として看過できないものとして、利益損害が挙げられます。

企業によるITの利活用が進む中で、製造業における制御システム、飲食・小売業におけるPOSシステム、通販業におけるECサイトなど、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は、これらシステムが停止することで事業中断が発生し、直接的に売上高の減少をもたらすことは想像に容易いといえます。

この場合、留意すべきは、損失は売上高の減少額そのものではないということです。変動費について支出を免れることを踏まえると、次のイメージのとおり、固定費の負担と営業利益の喪失といえます。

【利益損害のイメージ】

ネットワーク停止によって数ヶ月間、営業活動が停止。売上高が４割減少した（10億円⇒6億円）。結果として、営業損失▲0.2億円として、▲0.2億円－1億円＝1.2億円の損失が発生した（売上高は4億円減収したが、変動費2.8億円の支出はなかった）。

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

図表Ⅲ-３-１　利益損害のイメージ

イ．コスト総括

利益損害として発生する損失がいくらになるかは、企業規模によって大きく変わってくるため、**平均的にいくらといった額を示すことができるものではありません。**当該企業における平時の売上高・固定費・変動費・営業利益の額を確認し、予想されるシステム停止期間ごとにいくらの損失となるかを想定しておくということになります。

セキュリティコラム⑤
「ランサムウェア被害で倒産した中小企業のハナシ」

～インシデント対応の現場から その2～

警察庁が年2回公表している「サイバー空間をめぐる脅威の情勢等について」によると、ここ数年企業・団体等におけるランサムウェア被害が相次いでおり、特に中小企業の被害は、令和3年以降常に全体の50%以上を占めています。

ひとたびランサムウェア被害に遭ってしまうと、調査・復旧・対策強化などに多大な費用がかかるほか、情報漏えいによる社会的信用の低下、顧客からの取引縮小など、経営に直結する重大なリスクが発生しますが、資本力の乏しい中小企業にとって、これは死活問題であり実際、倒産に追い込まれるケースも発生しています。
本コラムでは、ランサムウェア被害によって業務が停止してしまい、その後復旧したものの取引縮小などが起因して倒産してしまった中小企業のハナシをご紹介します。

その企業は従業員数十人規模の物流会社で、社内にはシステム会社が開発した発注・配送・仕分け・勤怠などの自社専用システムが複数存在していました。システム部門が存在していなかったため、開発や運用はすべて社長自らが、システム会社と協議しながら進められていました。
関係は非常に良好で何かトラブルがあった場合にはすぐに駆けつけてくれるといった間柄でした。

しかし、新型コロナウイルス感染症の流行により、定期的に行われていたシステム会社による訪問が難しくなりました。協議の結果、システム会社がリモートからでも対応出来るよう、企業側のネットワーク機器の設定変更が行われることになりました。しかし、システム会社にはネットワーク機器の設定変更等に対応できる技術者がおらず、企業側でネットワーク機器の設定代行業者へ依頼し設定変更が行われました。結果的に、システム会社は企業側のネットワークに対しリモートアクセスすることができるようになったのですが、インターネットから企業へのリモートアクセス設定に制限がかけられておらず、新たに外部からサイバー攻撃を受けるリスクも生じていました。

そして、ネットワーク機器の設定変更から約2日、社長がいつものように端末の前に座ってシステムを利用しようとした時に、悲劇は起きました。社長が利用していた端末の画面には英語の理解不能な文章が表示されており、ブラウザーを起動して各種システムへアクセスを試みても、すべてのシステムがエラーで利用出来ない状況となっていました。経理を担当していた社員の端末にも、同様に英語の文章が表示されており、社長は急いでシステム会社へ連絡して調査を依頼しましたが、システム会社側では詳細な原因がわからず、ランサムウェアに感染している可能性のみが報告されました。

その企業は、毎日店舗に配送される食品などの日配品を多く取り扱っており、感染直前に配送が開始されていた商品については無事届けられたものの、配送ドライバーの退勤を含む感染以降のすべての業務は停止、システム会社にもセキュリティ専門の担当者がいなかったため、筆者が所属する会社にインシデントレスポンスの支援依頼がきました。

そして、初動調査開始から約半日、分析の結果から、侵入原因はリモートアクセス環境へのブルートフォース攻撃（総当たり攻撃）であったこと、端末やサーバーでは共通のパスワードが設定されていたため、攻撃者がネットワークへの侵入後、ラテラルムーブメント（ネットワーク内の横展開）によって感染が拡大してしまったことなどが判明しました。

調査が完了した翌日、応急処置としてリモートアクセス設定を一旦削除した後、現地においてシステム会社による各種システムの再構築が開始されました。しかし、OSやドライバディスクの入手、バックアップデータのリストアなどに手間取り、完全復旧までにはさらに4日を要しました。
結果として、被害を受けた企業は計5日間にわたる業務停止と、調査および再構築費用が発生し、経営に大きな影響を及ぼしました。そのうえ、復旧後にも取引先から再発防止のため、セキュリティコンサルティング会社との契約や、高度なセキュリティソリューションの導入を求められて大きな負担となりました。

また、被害発生時に、取引先に対して、復旧に要する時間を明確に提示することが出来ていなかったため、業務停止以降、取引先では別の物流会社を利用する検討が進められ、被害発生から4ヶ月後には一部の取引先が契約を解除、さらにその数ヶ月後にも一部の取引先との契約が終了となり、仕事の激減によって資金繰りが悪化していきました。

そして被害発生から約1年…。状況が良くなる見通しが全く立たなくなった企業は、これ以上負債が増える前にと、倒産することを決断しました。

近年、中小企業においても様々な分野でIT導入が進み、デジタル技術が活用されています。一方でサイバー攻撃は業種や規模を問わず、多くの企業・団体等が脅威に晒されています。高度化・巧妙化が進むサイバー攻撃の被害に遭わないためにも、サプライチェーン全体でサイバーセキュリティ対策強化に取り組み、リスクを最小限にする努力を怠らないことが重要と考えます。

令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

執筆：「お酒を愛するフォレンジッカー」
（インシデントレスポンス会社で業務に従事）

セキュリティコラム⑥
「サイバー保険」

～IT・セキュリティ業界の方に知っておいて欲しい、サイバー保険（損害保険）のハナシ～

■はじめに

サイバー保険は、名前からも想像できるとおり「サイバー攻撃を対象とする」保険です。
しかし、さらに掘り下げて理解されている方は多くはないかと思います。このコラムではサイバー保険（というよりかは、どちらかといえば損害保険）を簡単に説明していきたいと思います。

■損害保険と生命保険

保険業界は、損保（損害保険会社）と生保（生命保険会社）の2つの業界に分かれますが、扱っている商品は大きく異なります。損保が扱っているのは損害保険（自動車保険、火災保険等）、生保が扱っているのは生命保険になります。そして、サイバー保険は損害保険の一種、損保の商品だということを認識していただければと存じます。

■損害保険って？

損害保険と生命保険に触れたのには、理由があります。
生命保険は、所定の事故が起きた場合に「定額」をお支払いする商品です。例えば、医療保険であれば「入院したら1日につき5,000円支払う」といった具合です。
一方、損害保険は所定の事故が起きた場合に「所定の損害」に対してお支払いする商品です。ポイントは「所定の損害」です。事故によって生じる損害といってもさまざまなものあります。損害保険はその一切合切、すべての損害に対して支払うものではありません。また、定額ではなく実損害額に対して支払います。
サイバー保険についても同様です。サイバー攻撃によって生じる損害はこのレポートで6つの類型を示していますが、そのすべてが対象になるものではありませんし（後述）、サイバー攻撃を受けたら損害の有無にかかわらず定額（例：1,000万円）を支払うものでもありません。

■覚えておきたい保険用語

世の中、業界ごとの専門用語が存在します。その業界の人は他業界の人に対して何気なく専門用語を使うことがありますが、相手方はその語が何を意味しているのかわからないこともあるでしょう。保険業界にもいろいろな専門用語がありますが、ここでいくつかの用語の意味を説明しておきます。これらの用語を知っておくと、保険提案の場面での理解も早いと思います。
例えば、「保険金」と「保険料」の違いをご存じない方も多いのではないでしょうか。

用語	説明
保険金	保険会社がお支払いするお金
保険料	料金。保険契約者が保険会社に支払うお金
保険金額・支払限度額	契約に際して設定する、お支払いする保険金の上限額
保険契約者	保険契約をする人、かつ、保険料を支払う人
被保険者	保険金を受け取る人（損害保険の場合）
免責	保険金を支払わないこと

■補償内容（損害保険約款を理解するためのポイント）

1．総論

保険商品では、不特定多数の人と同一の契約を迅速・効率的に締結するための定型的な文書である「保険約款」を使用します。保険約款には種々の規定がありますが、損害保険の補償内容についてポイントというべき主なパーツは次の3つかと思います。まずは、この3つを押さえることが補償内容を理解することに繋がります。

パーツ	内容
保険金を支払う場合	どのような事故が発生した場合に、保険金を支払うか
保険金を支払わない場合	どのような場合に、保険金を支払わないか
損害の範囲(支払保険金)	どのような損害に対して、保険金を支払うか

2. サイバー保険

日本のサイバー保険における上記3つのパーツの内容は概ね次のとおりです。

※ざっくりと理解するために簡略化しています。保険会社による違いがあることも含め、検討にあたっては、 約款等により十分確認していただけたらと存じます。

(1) 保険金を支払う場合

サイバー保険は、その歴史として、情報漏えいの保険からの派生または影響を受けていることもあり、サイバー攻撃だけではなく、他人の情報の漏えいも対象にしています。具体的には、PCや鞄などの紛失・盗難、誤送付、従業員の持出しなど、フィジカル空間において生じた情報漏えいも対象となります。

保険金を支払う場合(対象となる事由、事故)
① サイバー攻撃 ② 他人の情報(注)の漏えい(おそれを含む) ③ IT利活用に伴う他人の損失の発生

(注)通例、個人情報であるか否かは問いません。

(2) 保険金を支払わない場合

他の保険商品と同様、戦争、地震など同時多発的に大きな損失が発生するようなリスクや、モラル的に問題のあるリスクについては、免責となります。

保険金を支払わない場合
(一例)戦争、地震、犯罪行為、故意・重過失による法令違反など

なお、よくある疑問について2点説明します。

○犯罪行為は免責となります。ただし、従業員の犯罪行為、例えば、従業員の持出しは、免責とせずに、補償されるのが通例です。

○セキュリティ対策が不適切、不十分であることの免責規定はありません(故意・重過失法令違反等は除く)。セキュリティの対策状況は、保険料に反映されること(例:対策状況が良好であれば割引)が一般的です。

(3) 損害の範囲(支払保険金)

国内損保において、サイバー保険で補償する損害は、このレポートで示している次の6つの損害のうち、基本的には次の①から③までの損害です。「金銭損害」「行政損害」「無形損害は対象にしていませんが、欧米の損保では「金銭損害」「行政損害」を対象としているケースがあります。

損害の範囲(支払保険金)
① 費用損害(事故対応損害) ② 賠償損害 ③ 利益損害

※費用損害は、事故対応に要したすべての費用を対象とするものではなく、所定の費用が対象となります。このレポートの費用損害の項目において示している費用については、概ね補償されます。

※利益損害はオプションとしているのが通例です。また、費用損害や賠償損害と異なり、サイバー攻撃や情報漏えいに起因するものに限定せず、プログラムのバグ、ヒューマンエラー等も含め、突発的事象による自組織のネットワーク停止全般を対象とするのが通例です。

※一部の国内損保では「金銭損害」について、インターネットバンキングにおける不正送金被害や、ビジネスメール詐欺等をオプションとして補償しているケースがあります。一方、ランサムウェア感染時の身代金は犯罪助長に繋がる(身代金を補償する保険があるがゆえ狙われる、ゆえにランサムウェア犯罪が拡大している)として、国内損保では補償していません。

■保険料

1. 総論

個々の契約において提示される保険料は、（当然ながら）その保険会社としてあらかじめ用意している料金体系・テーブルに基づくものです。この料金体系・テーブルは統計数字等を基に作成することになりますが、その作成における考え方の一例を、ちょっとだけカンタンに説明してみます（うまく説明できているかわかりませんが…）。

保険料の作成の考え方（一例）
○ある事故については、統計的に年間100件につき5件に損害が発生することがわかっている。つまり、その頻度（Frequency）は5%である。 ○したがって、仮に1,000万円の定額を支払う商品であれば、1,000万×5%＝50万円が保険料の原価となる（裏を返せば、契約100件×50万円で5,000万円を集めれば支払う保険金と一致する）。 ○ただし、損害保険は実損害額を支払う商品である。したがって、頻度に加えて、損傷度（Severity）も考慮する必要がある。例えば、保険金額1,000万円を設定した場合、実損害額は800万円のケースもあれば、20万円のケースもある。ので、平均的にどのくらいの割合を支払うことになるかということも考慮する。 ○ゆえ、仮に統計的に保険金額1,000万円を設定した場合の損傷度が30%ならば、1,000万円×5%（頻度）×30%（損傷度）＝15万円が原価となる。 ○上記のような考え方を基本としつつ「**リスクに関する他の要素**」や、保険金額を引き上げた場合の傾向値等も加味する。 ○最終的に、原価に対して事業コスト（販売組織に支払う販売手数料、保険会社自身の事務・システムコストや人件費など）も加味し、保険料を決定する。

2. サイバー保険

サイバー保険において、上記の考え方のうち「リスクに関するほかの要素」は複数ありますが、大きくは次の3つです。 したがって、個々の契約の保険料設計にあたっては、保険会社に主に次の3つを伝えることになります。

要素	リスクの違いの具体例
会社規模（売上高）	全国展開しているファミレスと、1店舗のみのすし屋
業種	要配慮情報を多く取扱う医療機関と、個人情報の少ない建設業
セキュリティ対策状況	UTMやEDRを導入している企業と、まったくセキュリティ対策を導入していない企業

■サービス

自動車保険は保険金を支払うだけではなく、示談代行やロードサービスといったサービス面も機能の一つとなっています。サイバー保険の場合も同様で、未然防止に繋がるアセスメント・リスク評価や、インシデント対応の支援も大きな機能となっています。各損保によってラインアップは異なるのでサービスについても確認されることをおすすめします。

以上「サイバー保険」をカンタンに説明してみましたが、詳細については、各保険会社の違いも含め、検討してみることをおすすめします。

執筆：「見習ふぐ調理師」

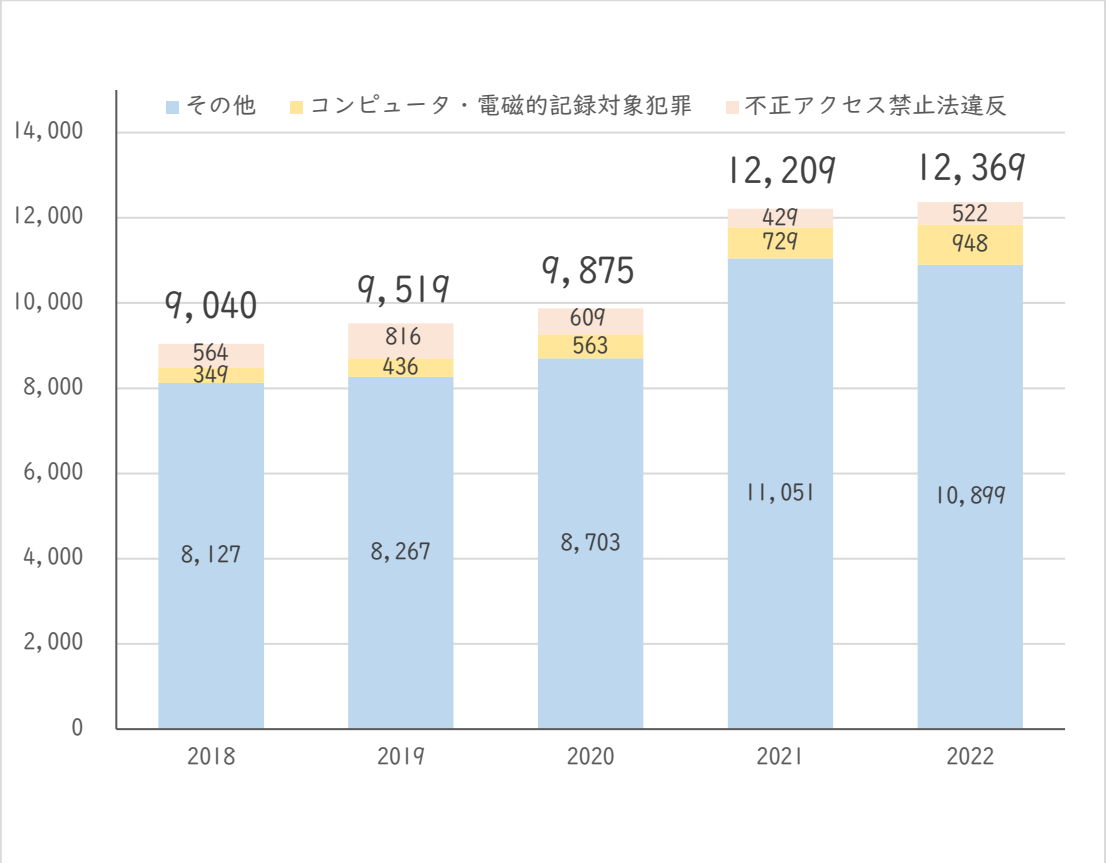
4. 金銭損害

インシデントにより直接的な金銭損害を被るケースは珍しくありません。

警察庁が年2回公表している「サイバー空間をめぐる脅威の情勢等[17]」を見ると、日本国内においてもサイバー犯罪の検挙件数は、高い水準で推移しています。

このことは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と読み取ることができます。大企業のサイバー犯罪被害に関する報道は毎日のように目にしますが、中小企業・小規模事業者のサイバー犯罪被害も報道を目にする機会は少ないものの、大企業同様に増加しています。

このレポートでは、企業・組織が被害を受け得る、インシデントによる直接的な金銭侵害の例として、ランサムウェア、ビジネスメール詐欺（BEC）、インターネットバンキングによる不正送金を取り上げ、それぞれの被害金額の推定を行います。



図表Ⅲ-４-１　国内のサイバー犯罪検挙件数の推移（出典：警察庁）

① ランサムウェアによる身代金

ア．概要

ランサムウェアとは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。感染したパソコンなどの端末やサーバー上のデータを暗号化するなどして使用不可にし、これらを復旧することと引き換えにランサム（＝身代金）を支払うように促す脅迫メッセージを表示する不正プログラムを指します。

近年では、このランサムウェアへの感染に加え、暗号化する前にデータを窃取しておき、身代金を支払わなければデータを公開すると脅迫する「二重の脅迫（double extortion）」と呼ばれる攻撃が一般化しており、また、データの暗号化はせずにデータの窃取のみで脅迫する手法（前述の警察庁「サイバー空間をめぐる脅威の情勢等」では「ノーウェアランサム」と表現）も出現しています。

ランサムウェアによる金銭損害は、前述の端末・データを復旧するための身代金要求を受けた場合のその支払です。

ランサムウェアを使った攻撃は、過去は明確な標的を定めない広く無差別な攻撃（メールによりばらまくといった方法など）がありましたが、ここ数年は個人よりも多額の金銭の支払いが見込めるためか、企業・組織が狙われやすい傾向にあります。

脅迫に従うことによる金銭的被害に加え、暗号化および窃取されたデータが組織にとって重要な情報であった場合、業務の遂行に大きな支障が出たり、個人情報漏えいによる信用の失墜や賠償損害などの経済的損失につながったりするなどの二次被害につながるおそれがあります。

なお、金銭を支払っても暗号化されたデータが復旧される保証はないこと（二重の脅迫により窃取されたデータが削除される保証はないこと）、身代金の支払が犯罪助長につながることからも、身代金支払は推奨されるものではないことを申し添えます。

イ．被害金額（身代金要求額）の傾向

国内の被害組織において、身代金要求額がいくらであったかを公表している事例はほとんどありません。

しかし、ランサムウェアを使用する攻撃者グループの多くは国外を拠点に活動しており、身代金もBitcoinなどの暗号資産（仮想通貨）で要求されるケースが多いことから、国ごとに大きな傾向の差異は少ないと考えられます。

そこで、このレポートでは米国の統計データをもとに被害金額の傾向を推定

していきます。

被害金額の実態を表すものとしては、米国のサイバーセキュリティ企業Coveware社のレポートが参考になります。同社の「Ransomware Quarterly Reports[18]」では、自社でのインシデント対応等のデータを基として四半期ごとに身代金支払額の平均値および中央値を公表しています。

集計時期		平均値（ドル）	中央値（ドル）
2021年	第1Q	220,298	78,398
	第2Q	136,576	47,008
	第3Q	139,739	71,674
	第4Q	322,168	117,116
2022年	第1Q	211,529	73,906
	第2Q	228,125	36,360
	第3Q	258,143	41,987
	第4Q	408,644	185,972
2023年	第1Q	327,883	158,076
	第2Q	740,144	190,424
	第3Q	850,700	200,000
	第4Q	568,705	200,000

図表Ⅲ－４－１ 身代金支払額の推移（米国Coveware社のデータに基づき集計）

なお、国内組織における著名なランサムウェア感染事例としては、2021年10月に徳島の病院において院内のシステムが使えず診療停止に追い込まれ、市民生活に多大な影響を与えた事例[19]、奇しくもその1年後の2022年10月に大阪の病院が同様に診療停止などの被害を受けた事例[20]、2021年3月にサプライヤーがランサムウェアに感染したため、大手自動車メーカーが国内全工場の操業を1日停止した事例[21]、2023年7月に名古屋港のコンテナターミナルでランサムウェア感染により港湾施設の運営がストップした事例[22]が挙げられます。

ウ．コスト総括

Coveware社のレポートにおける2023年の身代金支払額（第1～4Qの単純平均）を日本円に換算すると、平均値で1億円弱、中央値で3,000万円弱となります（1ドル＝150円換算）。ただし、ランサムウェアによる身代金要求額は事例ごとに大きく異なる場合が多いため、公開されている平均値や中央値はあくまで目安と考える必要があります。

② ビジネスメール詐欺（BEC）による金銭被害

ア．概要

ビジネスメール詐欺（Business E-mail Compromise：BEC）は、取引先や経営者等を装った巧妙な偽メールにより従業員を騙し、送金取引に関わる資金を詐取するなどの金銭被害をもたらすサイバー攻撃の一種です。

BECによる金銭被害は、2013年ごろから海外で確認されるようになり、米国IC3（インターネット犯罪苦情センター）では2015年頃から注意喚起を行っています[23]。その後、国内でも被害が確認されるようになり、一般社団法人全国銀行協会（全銀協）[24]や警察庁[25]、IPAなどが注意喚起を行っています。2022年には、手口や対策等をまとめた特設ページをIPAが開設しています[26]。

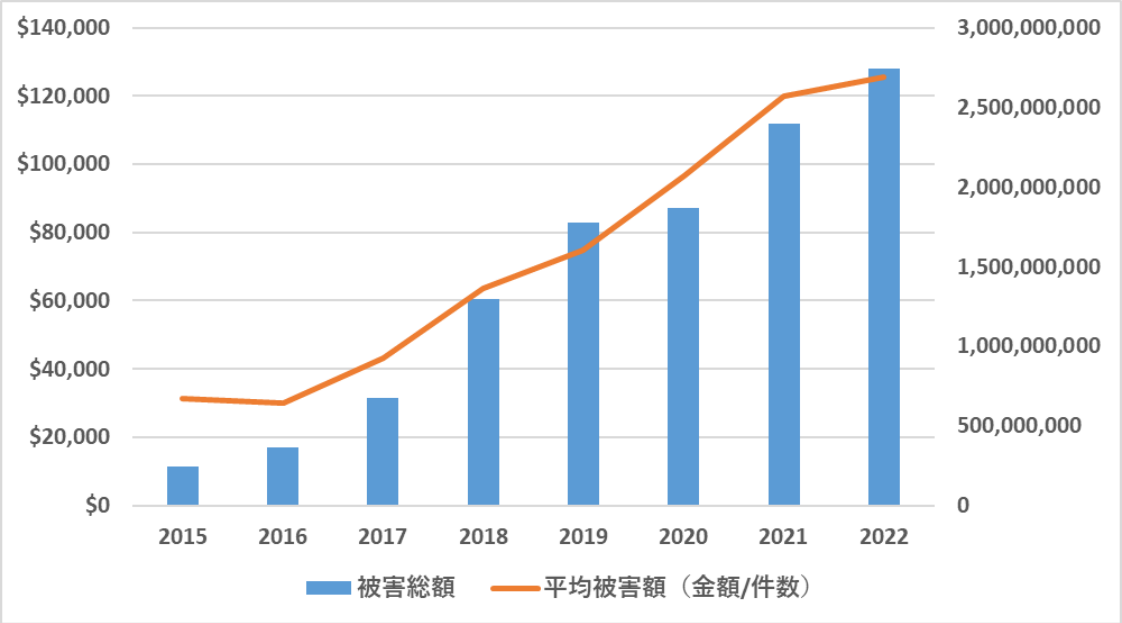
手口としては、差出人（送信元）メールアドレスが取引先を模したメールアドレスだったり、本物のメールアドレスが表示名に使われていたり[27]、メールの返信や転送を装ったり[28]、自然な日本語の本文が使われたりなど、本物のメールかどうかを見分けることが困難な事例が確認されています。また、偽造された証明書類を添付して信じ込ませようとする事例も確認されています[29]。近年では、AI音声技術（ディープフェイクボイス）の進化に伴い、偽のメールと合わせて、役員の声を模倣した電話を併用する事例も確認されています[30] [31] [32]。

ビジネスメール詐欺は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い傾向があり、組織が被害に遭った際の影響が大きいサイバー攻撃といえます。

イ．被害金額の傾向

米国IC3のインターネット犯罪レポート（年次レポート）によると、BECによる被害総額と平均被害額は年々増加傾向にあり、次のとおりです。

2022年の被害総額は約27.4億ドル、1件あたりの被害額（平均被害額）は約12.7万ドルとなっています。



図表Ⅲ－４－４　米国IC3　年次報告書におけるBEC被害総額と平均被害額

国内におけるビジネスメール詐欺の被害調査としてはJPCERT/CCが2019年、国内12組織を対象に実施した実態調査[33]があります。本調査によると被害の有無に関わらない不正な請求額の合計は約24億円とされています。なお、請求は基本的に外貨建ての送金を指示するものであり、大半の事案ではBECと気づいて実害には至っていません。しかし、被害を回避した事案がある一方、日本円に換算すると数百万円～数千万円単位の被害に遭った事案も報告されています。

また、トレンドマイクロ株式会社とNPO法人　CIO　Lounge　が2023年、国内の法人組織（従業員500名以上）に勤めるセキュリティやリスクマネジメントの責任者（部長職以上）305人を対象に実施した「サイバー攻撃による法人組織の被害状況調査」[34] [35] [36]によると、ランサムウェア攻撃に次いで、ビジネスメール詐欺が「過去3年間で最も被害コストが大きかったサイバー攻撃」とされており、被害の1件あたりの平均金額は5,484万1,772円だったとのことです。

国内組織に関連する被害額の大きな事例としては、2017年9月下旬に大手航空会社が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にあった事例[37]や、2019年8月に大手自動車部品メーカーの欧州の子会社で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した事例[38]、2019年9月下旬に大手新聞社の米国の子会社で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）が流出した事例[39]などが挙げられます。これら３つの事案はマスコミ報道があったものですが、上場企業では証券取引所のルールである適時開示制度により「資金流

出」の語をもって公表するケースもあります。国内組織における主な報道・公表事例（メールによるものか確認できない事象を含む）は次のとおりです。

ソース	発生年月	業種	被害額	海外現法・支店事案
報道	2017年8月	航空	350万ドル	
報道	2017年11月	アパレル	280万ドル	
報道	2018年10月	製造	20万ドル	
報道	2019年2月	製造	40万ドル	○
報道	2019年8月	製造	約40億円	○
報道	2019年9月	マスコミ	2,900万ドル	○
IR情報	2020年	製造	519百万円	○
報道	2020年4月	製造	150万円	
IR情報	2020年度第1Q	製造	38億円	○
IR情報	2020年	製造	0.58億円	○
IR情報	2020年	製造	9.84億円	○
報道	2020年度第3Q	製造	8000ユーロ	○
IR情報	2020年12月	製造	約1億円	○
IR情報	2020年度第4Q	製造	1.54億円	○
報道	2021年2月	製造	4.8億円	○
報道	2021年3月	飲食	1.7億円	○
IR情報	2021年第1or2Q	製造	5.38億円	○
IR情報	2021年4月	製造	約2.8億円	○
報道	2021年10月	製造	約1億円	○
IR情報	2021年11月	小売	8.23千ドル	
報道	2021年12月	小売	442万円	
IR情報	2022年1月	建設	7.34億円	○
IR情報	2022年3月	製造	1.87億円	○
IR情報	2022年3月	製造	8.18億円	○
IR情報	2022年7月	製造	360万ドル	○
IR情報	2022年9月	サービス	2.6万ドル	○
IR情報	2022年12月	製造	0.55億円	
IR情報	2023年3月	製造	2.8億円	○
IR情報	2023年4月	製造	2.7億円	○
IR情報	2023年7月	製造	0.8億円	○
IR情報	2023年7月	製造	1.62億円	○
報道	2023年8月	放送	？	
IR情報	2023年12月	製造	136万ドル	
報道	2023年12月	製造	34億円	○

図表Ⅲ-４-５　国内組織におけるBEC被害事例

ウ．コスト総括

ビジネスメール詐欺による被害金額は、被害組織における送金の取引規模等により大きく異なるため、**一概に算出することが難しいといえます。**

しかしながら、ビジネスメール詐欺が取引先や経営層などになりすました電子メールを送って送金を促すという性質上、組織の業務において日常的に授受される金額が要求された場合には、電子メールの内容に違和感を覚えづらく、騙されてしまう可能性が高いと考えられます。

被害に遭った場合の被害額としては、組織の送金担当者が日常的に取り扱う金額が目安となりますが、企業の買収をテーマとしたCEO詐欺の場合など送金額の大きい取扱いにおいては、その被害額は数千万円～数十億円にのぼる場合があります。

③　インターネットバンキングによる被害金額

ア．概要

フィッシング詐欺やマルウェア感染などにより、攻撃者にインターネットバンキングの認証情報（ログインID、パスワード等）を窃取される被害が継続して確認されています。インターネットバンキングの認証情報が漏えいしたことにより、被害者が持つインターネットバンキングアカウントに不正ログインされ、攻撃者が作成した別の口座に不正送金されたり、インターネットバンキング上のサービスを不正利用されたりする等の被害に遭うおそれがあります。

フィッシング詐欺

実在する金融機関等を装ったメールやSMSからフィッシングサイト（偽のウェブサイト）へと誘導され、偽物であると気付かずにインターネットバンキングのログインID、パスワード等の認証情報を入力してしまい、攻撃者に認証情報を詐取される

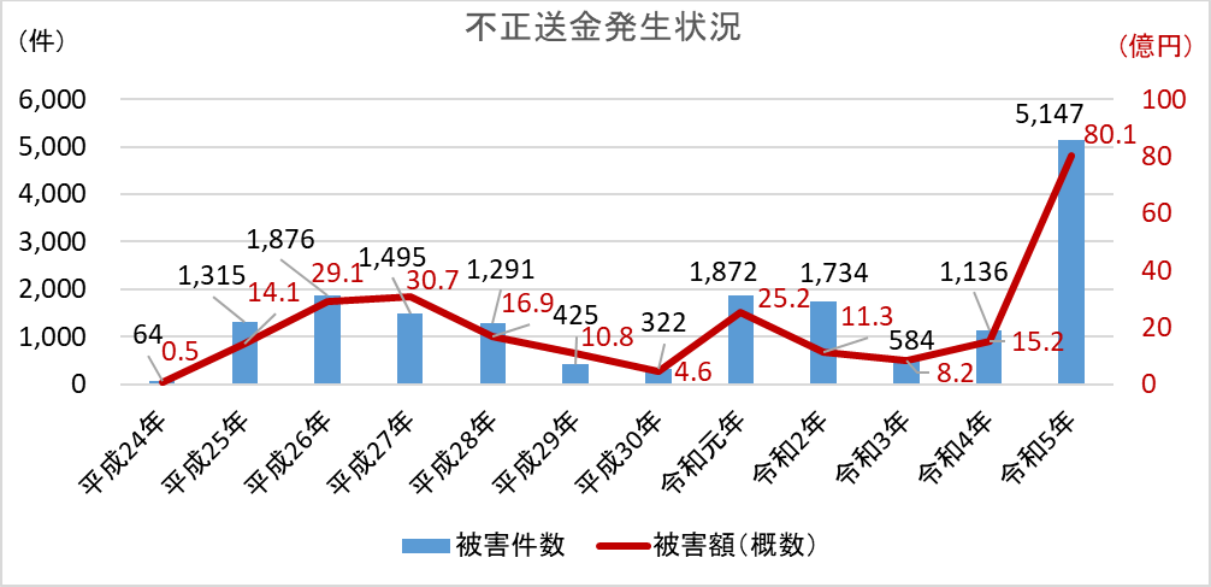
マルウェア感染

メールの添付ファイルを開いたり、URLをクリックしてダウンロードしたファイルを開いたりした場合などに、端末をマルウェアに感染させられ、攻撃者に認証情報を窃取される

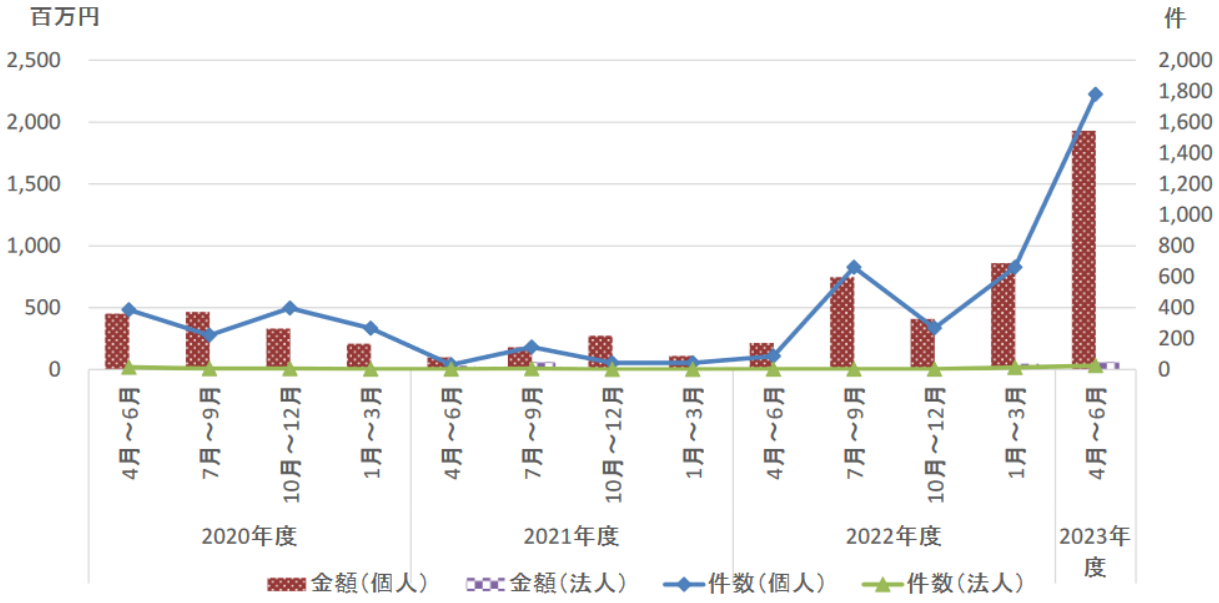
イ．被害金額の傾向

インターネットバンキングに係る不正送金事犯の発生件数及び被害額について、2022年（令和4年）8月下旬から9月にかけて被害が急増して以来、落ち着きを見せていましたが、2023年（令和5年）2月以降、再度被害が急増しているとして、警察庁と金融庁の連名で注意喚起[40]を行っています。2023年（令和5年）11月末における被害件数は5,147件、被害額は約80.1億円となり、いずれも過去最多を更新しているとのことです。

全銀協によると、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・金額は、2021年度から増加しており、2022年度のインターネットバンキングの不正払戻し件数は1,696件、被害金額は約22億9,300万円でした。さらに、2023年度4月～6月の件数は1,804件、被害金額は約19億9,300万円と急増しており、2022年度の1年間の件数・金額に匹敵する規模となっています。なお、法人顧客の不正送金被害件数は全体の数%程度であり、被害の多くは個人顧客である状況が続いています[41]。



図表Ⅲ-４-６　国内のインターネットバンキングに係る不正送金事犯
（出典：警察庁・金融庁）



図表Ⅲ-４-７　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）

ウ．コスト総括

全銀協の公表する2022年度の被害事例をもとに、１件あたりの平均被害額を求めると、法人顧客の被害額は約310万円となります。なお、個人顧客の被害金額は約133万円です。

5. 行政損害

ア．概要

世界各国には、個人情報保護に関する法令が存在します。これらの法令では個人情報が漏えいした場合等に、刑法上の刑を科すもの、刑法とは別の制裁を科すもの等の違いはあるものの、行政上の義務違反に対する金銭的制裁として罰金、過料、制裁金、課徴金など定めているものがあります。

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の各種対応が求められることになりますが、特に海外の法令への対応となったとき、高度な専門性を要するため、大手弁護士事務所、外資系コンサルティングファーム等、専門の事業者へその業務を委託するのが通例といえます。

したがって、これら罰金等を支出した場合、各種対応を要した場合には、企業として損害（損失）が発生することが想定されます。

なお、日本企業に関係する主だった個人情報保護に関する法令としては次のものが挙げられます。

地域	通称	正式名
日本	個人情報保護法	個人情報の保護に関する法律
EU（EEA）	GDPR	General Data Protection Regulation（一般データ保護規則）
米国（加州）	CPRA（改正CCPA）	California Privacy Rights Act of 2020（カリフォルニア州プライバシー権法）

図表Ⅲ-５-１　地域ごとのプライバシー関連法令

日本の法令である個人情報保護法に注意すべきことは当然のことですが、海外の法令であるGDPRやCPRAについても、日本企業が適用対象となることがあるので留意が必要となります。例えば、GDPRでは、EU域内に拠点（支店・子会社など）を有している場合や、EU域内の個人に対して商品・サービスを提供している場合には、日本企業であっても企業規模問わず適用対象となります。米国では、カリフォルニア州以外でもプライバシー関連法令が制定されている州があるので注意が必要です。

イ．コスト総括

前述の法令において定められている法人に課される罰金等の額は次のとおりです。これらはあくまでも最大額であって、違反の度合いや影響度等を勘案して決定されることになります。

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のとおり 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 なお、次のサイトでは、これまで、制裁金が課された組織、制裁金の額等がとりまとめられています。 https://www.enforcementtracker.com/
米国（加州）	CPRA	消費者1名あたり**最大2,500ドル** （故意だと最大7,500ドル）

図表Ⅲ-5-2　地域ごとのプライバシー関連法令と罰則

6. 無形損害

① ブランドイメージ毀損

ア．概要

インシデントの発生に伴い、企業が培ってきたブランドイメージの毀損は少なからず発生します。毀損の度合いは、その後の復旧期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するため、インシデントが直接引き起こした損害の定量的な評価は非常に難しいのが実情といえます。

なお、過去の例でいえば、インシデントによるブランドイメージ毀損がきっかけとなって、サービスの廃止や長期間の利用停止、上場の廃止を余儀なくされた事例が複数確認されています。具体例としては次の事例が挙げられます。

・IT企業：ファイル交換サービス（2019）
・大手流通業：バーコード決済サービス（2019）
・大手通信業：電子マネー口座からの不正引き出し（2020）
・サービス業（ファイナンス事業）：不正アクセスによる情報漏えい（2022）

イ．コスト総括

前述のとおり、定量的な評価は難しいですが、本来提供されるべきサービス自体の廃止や長期間の利用停止による収益がゼロになることを踏まえると、その企業の売上高に対し**数十%程度**の損失を引き起こすことも想定されます。

② 株価下落

ア．概要

インシデントが上場企業において発生した場合には、当該企業の株価の下落につながる可能性があります。株価の下落は、企業の格付け等にも影響が及ぶことも考えられます。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あります。

日本サイバーセキュリティ・イノベーション委員会（JCIC）が日本国内で情報流出等の適時開示を行った企業 47 社を対象に行った調査結果では、適時開示の50日後には**株価が平均 6.3%下落**したことが示されています[42]。また、

過去の例でいえば、次の事例が挙げられます。

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

なお、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します。図 1はランサムウェア被害やサイバー攻撃による情漏えい被害を開示した組織の株価の推移を被害公表前日の終値を1として示しています。サイバー攻撃被害公表後に低下した株価が1ヶ月程度で元の水準に回復するケースもあれば、長期にわたって株価が低迷するケースも確認されています。株価の推移には市場全体の変動や被害組織を取り巻く様々な要素があり定量的な評価が困難ですが、インシデント発生後の対応に問題がある場合などは、長期の株価低迷に陥りやすいと考えられます。

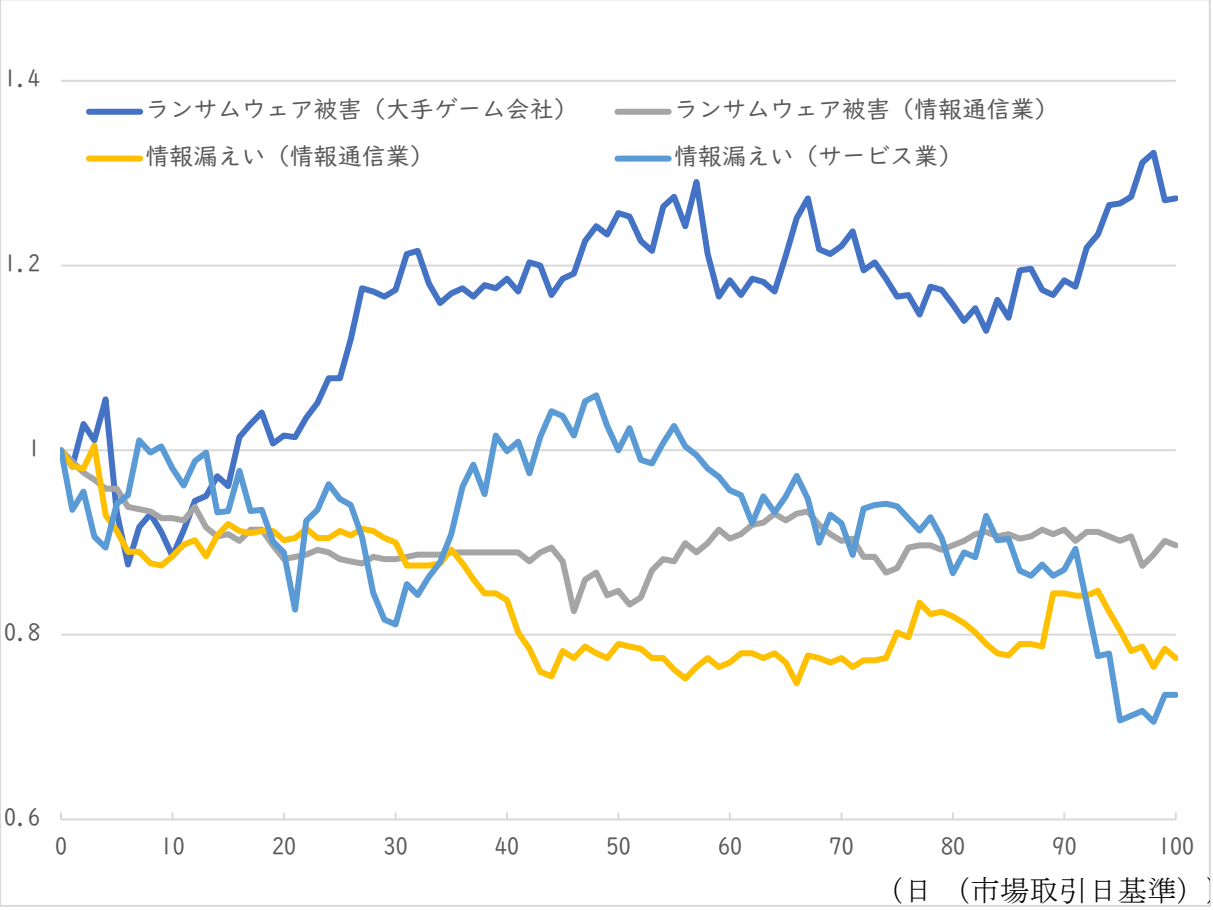


図 1 サイバー攻撃被害開示日からの株価推移

イ．コスト概括

株価下落による被害額（損失額）は、発行済みの株式数やインシデント発生直前の株価の額、インシデント復旧後の見通しなどによって変動するので、ブランドイメージ毀損額同様、定量的な評価は難しいのが実情です。

過去の例でいえば、株価時価として、数十%程度の下落を招くこともあるようです。その後、株価水準が復調した企業もありますが、企業のインシデント後の対応内容によって左右されていると考えられます。

～The 座談会「マスコミ」編～

サイバーセキュリティに携わるマスコミの方4名に、思うところを聞いてみた～♪（2023年12月実施）

司会　：みなさんおつかれさまです。今日は、セキュリティ関連記事をご担当されることも多いマスコミの方 4 名にお集まりいただき、いくつかご意見等を頂戴できればと思っています。まず、私が前から気になっているところなんですが、言葉遣いというか、用語について、どう考えていらっしゃるかについてコメントいただけると幸いです。

Ａさん：確かに、セキュリティの世界って専門用語が多いので、苦労しているところですね。わかりやすくするために大雑把に表現してしまうと、取材先から「不正確だ」と指摘を受けたりします。とはいえ、取材先の言葉を使うと、一般の読者にはわからないであろうところで、どう折り合いをつけるかって話ですね。例えば、ウイルスという言葉。セキュリティ業界ではマルウェアって言葉を使うと思うんですね。昔、誰かに言われたんですけど「読者を甘やかすな」と。だからといって、いきなりマルウェアを多用するわけにはいかないですよね。なので、専門用語も少しずつ増やすようにして、読者をならしていくってことが必要なのかなと思っています。

Ｂさん：そうですね。例えば、ランサムウェアなんかでも「身代金要求型コンピューターウイルス」って表現することが多いんですけど、専門家の方からそういうの要らないんじゃないかと言われることもありますね。でも、セキュリティ業界の方が思っているほど、ランサムウェアって浸透していないんですよね。我々としては、ランサムウェアって言うだけで伝わるようにしなければならないと思いますけど、一般の人と均衡点を図っていくという必要はありますよね。

Ｃさん：僕らって、この情報を誰に伝えたいのかっていう、ターゲッティングを考えるんですよね。だからセキュリティ業界の方にも、誰に向けて説明するのかってことは意識して欲しいんですよね。我々に対してもセキュリティ村の一員みたいに話してくるわけですけど（笑）、1 億 2,000 万人を意識してどう伝えるべきかを考える必要はあるかと。ちなみに、私は最近、思いっきりかみ砕くパターンと、全く忖度しないで専門用語を使うパターンを分けていますね。ただ、砕きすぎてもそもそも一般の人には読まれないような記事もあるので、ターゲッティングを考えているってことです。そういったことも考えて発信するフェーズに来ているかなと思っています。

Ｄさん：うちは読者がセキュリティ業界寄りなので、どちらかといえば、読者を甘やかす必要のないメディアなんですけど（笑）、新しい言葉が出てくるとどう伝えればよいかは考えますね。例えば、攻撃手法も時代によって言い方が変わったりしますし。ただ、役所が公表するドキュメントは一般的な言葉になる傾向があるので、そういったことも考慮しますね。

司会　：ところで、言葉に対する補足説明とかはどうですかね。

Ａさん：次の行やカッコでもって説明するとかはありますね。言葉も出始めは補足説明することも多いですけど、こなれてくるとカッコがとれてくるんですよね。

司会　：では、ここまで「言葉遣い」「用語」といったテーマだったわけですけど、広く捉えれば、世間に対する「発信」「伝え方」みたいなことになってくると思うんですけど、そのあたりで思うことってありますか？

Cさん：まず、一般社会に対してどうやって発信すべきか、我々マスコミだけでなく、それぞれの立場で考える必要があるのではということは思っています。例えば、セキュリティ業界であれば、 以前に比べて注目されているわけですから、社会に向けて伝えるという目線も考えていくべきとかですかね。発信の仕方を勉強する場を作るとか。本当の専門家っていうのは、相手の目線にあわせて喋ることのできる人だと思うんです。セキュリティ業界でもそういう方が増えていけばいいなと思います。

Aさん：そうですね。例えば、セキュリティ業界からマスコミ、記者に向けた勉強会っていうのをもう少しやってもいいのかなと思いますね。お互いのコミュケーションを普段から取っていれば、この記者はこういう情報を欲しがっているんだろうなとか、こういう説明をしたらわかってくれるんだろうなとか、発信の仕方も変わってくるんだろうなと。

Cさん：もちろん、セキュリティ業界にも世の中にどう伝えればいいかってことを考えている人はいますね。私の知り合いでも、若い頃に自分の言葉が世の中に伝わらないことを痛感して、その手の本を読むなど努力を重ねて、今や発信力の強い人もいますし。

司会　：なるほどですね。セキュリティ業界も発信の仕方を考えていく必要がありますね。

Cさん：あと、レポートの類もそうですね。世の中に発信していくことを考えたレポートもあれば、一方、そうでないものもありますよね。

Dさん：確かに。せっかく作ったのに発信できていないものもありますね。

Cさん：いろんな調査してデータもあるのに、全く表にでてきていないのがありますよね。それって何か社会的損失だと思います。

Aさん：PR を考えないとですね

Cさん：お。Aさん：定年退職後はセキュリティ業界の広報活動のアドバイザーになるのどうですか？笑

Aさん：（苦笑）

Cさん：あと、作り手の満足というか、レポートのテーマも内向きになってしまうところもありますかね。世の中に発信するというのを意識するとテーマも変わってくるでしょうし、何を発信すればよいかということも考えるようになるのかなと。

司会　：では、この話はこの辺にして…。ほかに何か取り上げたいネタってありますか？

Dさん：はい。僕、前から思っていることあるんですけど…。サイバー攻撃ってメディアに取り上げられると、攻撃を受けた会社は被害者なのに、世間から叩かれるじゃないですか。もちろん、その会社にも落ち度はあるかもしれませんけど、あくまで悪いのは攻撃者じゃないですか…。攻撃者のほうが、圧倒的優位な状況なわけで、そういうところも、もうちょっとうまく伝えられればと思います。

Bさん：私が最近やっているのは、被害企業って謝罪コメントも出してくるじゃないですか。「申し訳ございません」とか。結構、最近はカットしますね。いたずらに謝らせてそれを報じるというのも、ちょっとよくないなと思っています。

Ａさん：私も思います。やっぱり被害者なので。必要以上に謝ることはないんじゃないかなといつも思います。例えば、記者会見をするケース。檀上にあがって説明する人、その一方でそれを聞く記者、それぞれがちゃんとインシデントを理解しないなかで、謝罪し、それを叩く。そんな構図になってしまっている気がします。素人の記者にわかるように説明がなされれば、叩くということはないのかなと思います。

Ｃさん：やっぱり叩くべきはサイバー犯罪者ですよね。発信する側も受信する側も責任があると思っているんですけど、こういうことが起きる背後には常に攻撃者がいるってことをちゃんと認知できていない現状にあるのかなと。僕らも紙面なり放送なりで努力しなきゃいけないし、世間もそれを理解する、そんな社会的な認識共有が早くできればと思います。あと、記者会見を開く際に専門家が入ったりしますが、メディア・マスコミ対策って目線が強いのは気になります。公表という社会に発信する数少ない機会は、マスコミに向けたものではなく、世の中に自分たちの置かれている状況をきちんと説明する、そういう根底を発信する側も理解する必要があるかと思います。私も、サイバー攻撃は必ず攻撃者がいるんだっていう構図を書こうとして、そのための質問しているんですけど、発信する側の意識が足りないのか、調査中で何も言えませんとかわかりませんと…。専門家が余計なことを言うなとかアドバイスをしているのかもしれませんが、何のための情報発信なのかということを考えれば、もう少し違ってくるのかなと。

司会　：攻撃者が悪いということを発信していくという意味だと、被害組織やマスコミ以外、例えばIT ベンダーに対してこうあるべきじゃないか、みたいなものってありますか？

Ａさん：インシデントが起きた場合、調査をするということがあると思うんですけど、その調査結果について、必要以上に情報を出すな、やめた方がよいみたいなことは言わないで欲しいなと思います。こういった情報は出したほうがよいといったアドバイスをするようになって欲しいなと思います。

司会　：それでは、時間も限りがあるということで…。今日は、貴重なお話ありがとうございました。

Ⅳ モデルケース（フィクション）

１．サポート詐欺

① インシデント概要

従業員がインターネットで調べものをしていたところ、突然、女性の声による案内と共に、実在するIT企業を騙った画面が表示された。その画面には、マルウェアに感染しているため、サポートが必要であり、画面に表示されたTEL番号（国際電話）に電話をする旨の指示があった。

自ら招いた出来事として後ろめたさもあり、誰に相談することもなく、電話をかけたところ、日本語に違和感のある外国人のオペレーターから、遠隔操作のソフトウェアをインストールするよう促された。なすがままオペレーターの指示に従い、ソフトウェアをインストールしてしまった。

さらに、そのオペレーターからは、サポート料と称して数万円の金額を払うよう指示された。

その金額の支払方法についても説明があったが、コンビニエンスストアへ行き、画面に表示されていたIT企業とは別のIT企業の電子マネーを買う旨であったため、明らかに怪しいと思い、電話を切った。

② 対応および被害概要

〇遠隔操作のソフトウェアをインストールした後、長時間、オペレーターとやり取りをしてしまったことから、その従業員のPC内にあった顧客情報等が漏えいまたはそのおそれの可能性があるため、フォレンジック調査を実施した。

〇情報漏えいのおそれがあるとして、ホームページにお詫び文を掲載した。

③ 被害額（損失額）

被害額	**100万円**
内訳	**〇費用損害（事故対応損害）** ・事故原因・被害範囲調査費用 100万円

２．軽微なマルウェア感染（エモテット）

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（ワードファイルを開き、コンテンツの有効化をしたところ）、エモテットに感染した。

② 対応および被害概要

○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し、感染内容、被害範囲等の調査を実施した。

○調査の結果、エモテットであること、従業員端末3台とサーバー1台が感染していること等が判明した。

○取引先のメールアドレスの流出可能性はあるものの、大きな影響等はないことが確認された。

③ 被害額（損失額）

被害額	**800万円**
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 300万円 ⇒1,000台×3,000円

３．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サイトにおけるクレジットカードの入力フォームが改ざんされたことが判明。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ECサイトの制作会社に依頼するとともに、決済代行会社から紹介されたインシデントレスポンス事業者に対応を依頼し、攻撃手法、被害範囲等の調査を実施した。

○インシデントレスポンス事業者や決済代行会社による調査の結果、ECサイトの構築システムの脆弱性が狙われ、サイトが改ざんされており、利用者が入力したクレジットカード番号などの各種情報が、攻撃者設置の偽の入力フォームを通じて10,000件漏えいしていること、さらにクレジットカードの不正利用が合計で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、弁護士にお詫び文の確認依頼ほか、今後の対応方針を相談した。

○ホームページにお詫び文を掲載し、コールセンター事業者に問い合わせ対応を委託した。また、被害者10,000人に対してお詫び文とともに券面額500円のプリペイドカードを送付した。

○ECサイトの再開までには、クレジットカード会社との調整などに6ヶ月を要した。その間のECサイトでの売上がゼロとなり、会社全体として大きく売上高の減少が発生した。また、再開にあたっては、セキュリティ対策を大幅に強化したサイトを新たに構築することとした。

○事態が概ね収束した後、クレジットカード会社からは不正利用の額および再発行にかかる手数料について損害賠償請求がなされた。

③ 被害額（損失額）

被害額	**9,490万円**
内訳	**〇費用損害（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ヶ月間設置。初月５名体制とし、２～３ヶ月目は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 **〇利益損害** 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ヶ月）－（1,000万円×６ヶ月×50%）＝3,000万円 **〇賠償損害** 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

４．ランサムウェア感染

① インシデント概要

〇海外子会社において、VPN機器を経由した不正アクセスを受けた。

〇攻撃者は侵入後、短期間で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。

〇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、暗号化を実施した。

〇攻撃者はその10日後、既に窃取したデータの一部をダークウェブ上で公開し、データの回復およびデータの公開をやめることと引き換えに身代金を払うよう当該企業に要求した（二重の脅迫）。

②　対応・被害概要

〇休日の出来事であり、感染後の一連の攻撃の結果として、社内ネットワーク全体が停止し、社内外とのメールのやり取りができない、生産ラインで使用するシステムが利用できず製品を出荷停止せざるを得ないなど、多くの影響が生じた。

〇情報システム部門を中心に、ITベンダーとの連携のもと、インシデントレスポンス事業者による調査、データ復旧などの各種対応を実施した。

〇感染直後の休み明けには、経営層を含めた緊急会議が開催され、その後の対応ついて協議がなされたが、対応内容について部門間の立場の違いもあり、会議は紛糾した。

〇個人情報の漏えいのおそれもあったため、個人情報保護委員会への報告を行ったほか、ホームページによる個人情報漏えいの被害者への通知ほか、県警サイバーセキュリティ対策課への相談、監督官庁への報告等、対外的な対応に追われた。

〇納入遅延等の可能性もあったため、営業社員および担当役員が総出で、取引先に対するお詫び対応を実施した。

〇生産ラインほか、主要なシステムはバックアップデータにより、3日で復旧したものの、従業員端末の入れ替え等が必要となり、完全な収束には3ヶ月を要した。

③ 被害額（損失額）

被害額	**3億7,600万円**
内訳	**〇費用損害（事故対応損害）** ・事故原因・被害範囲調査費用 1億円 ⇒ファスト・フォレンジックを活用しつつ、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 ⇒ランサムウェアに感染したサーバー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 **〇利益損害** 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

Ⅴ あとがき

～情報を共有しましょう。そのための体制をつくりましょう～

随分前から言われてきたことですが、公共的あるいは非営利団体などを中心として、セキュリティ事案の情報を集約・共有する仕組みや試みは、日本国内でもいくつか存在し、機能しています。一方、欧米ではSEC(米国証券取引委員会)の開示規則やGDPRの中で、強制力のあるセキュリティ事故報告義務を対象企業に課しています。義務化の枠組みがあるという意味では、一歩踏み込んでいると言えるでしょう。

現状それで十分なのか…。

この問いに対しては、必ずしも Yes と 言える状況にはないと思います。

他組織のセキュリティ事案情報を平時に入手することは、事前警戒の意味合いで非常に有用です。なかでも、実際の事故事例に関する情報は、受け取る側にとって自組織の防御体制やシステムを再点検するために非常に役に立ちます。反面、それを出す側に立つと「何にために他社に共有するのか」「公表する必要はあるのか」といった疑問が常につきまといます。

ここまで、「共有」「公表」をあえて、ひとまとめで表現しましたが、本来十把一絡げに扱うべきものではありません。必要に応じて、範囲や内容を熟慮すべきです。

セキュリティ事案の情報共有で範囲が比較的小さいものとしては、組織内が考えられます。事故対処を実施した後には、再発防止策を講じる必要があります。不足している製品・サービスの導入、対応組織強化、従業員教育などが考えられますが、事故の教訓を活用するためには、対応が一段落したのちにその記録を文書化し、教育や訓練に活用することにより組織として「伝承」することも重要ではないでしょうか。

組織に属する人財は異動や退職、世代交代などで入れ替わっていきます。再発防止策を講じ、それが有効に機能したとしても、サイバー攻撃を完全に防ぐことは不可能ですから、いつなんどき攻撃に遭遇したとしても、過去の経験は対処・対応に活かすべきです。言い換えると、「当時の実担当者がいなくなったので情報がない」状態は回避すべきです。報告・告知の範囲としては、直接影響があった顧客や取引先・関係者はもちろんのこと、同業者や業界団体、業種・業態によっては監督官庁、個人情報漏えいの際には個人情報保護委員会、警察への相談など、状況やケースによって様々なパターンと組み合わせが考えられます。内容を吟味したうえで、事故の公表に踏み切った方が良いこともあるでしょう。

平時における整理と文書化が必要です。

今回の報告書を作成するにあたり、インシデント被害調査WGは「果敢な挑戦」を行ったと感じています。それは、被害企業に対するアンケートおよびヒアリングの実施です。

事故に遭った組織としては、正直「蒸し返したくない・蒸し返されたくない」という思いがあるのも自然なことだと思います。そのなかで、実施したアンケートやヒアリングにご協力をいただいた企業の皆様に対しては、感謝の念に堪えません。本当にありがとうございました。

さいごに。報告書執筆メンバーは、本業の傍らで、平日の夜や休日に「我が国のセキュリティ対策向上に貢献したい！」という想いのもと、ボランティアでこのレポートを作成しています。このレポートの内容が企業等の経営者・経営層に意見を具申する方々・そうしたユーザー企業にセキュリティ製品・サービスを提案する方々に十分に伝わり、ひいては我が国のセキュリティ向上に少しでも繋がることを願います。

調査研究部会長

執筆

リーダー

神山太朗（あいおいニッセイ同和損害保険株式会社）

サブリーダー

西浦真一（キヤノンITソリューションズ株式会社）

メンバー（五十音順）

大谷尚通（株式会社NTTデータグループ）

竹内智子（株式会社クレスコ・デジタルテクノロジーズ）

戸田勝之（NTTデータ先端技術株式会社）

西原真仁（日本アイ・ビー・エム株式会社）

本多規克（アルプス システム インテグレーション株式会社）

三国貴正（株式会社YONA）

山田道洋（日本電気株式会社）

サポート

前田典彦（株式会社FFRIセキュリティ、JNSA調査研究部会 部会長）

Special Thanks To ！！！！！！！！！！　①（あいうえお順）
青嶋信仁（株式会社ディアイティ）、赤松孝彬（EY新日本有限責任監査法人）、
新井悠（株式会社NTTデータグループ）、伊藤祐樹（トレンドマイクロ株式会社）、
井上健一（デロイト トーマツ サイバー合同会社）、上野宣（株式会社トライコーダ）、
大久保修一（サイバーリーズン合同会社）、大西翔太（株式会社神戸デジタルラボ）、
岡田良太郎（株式会社アスタリスク・リサーチ）、神薗雅紀（デロイト トーマツ サイバー合同会社）、
キタきつね（セキュリティリサーチャー）、佐久間貴（株式会社網屋）、
杉山一郎（EY新日本有限責任監査法人）、鈴木貴志（グローバルセキュリティエキスパート株式会社）、
関宏介（株式会社ラック）、田渕浩光（株式会社ブロードバンドセキュリティ）、
竹下宏樹（NTTデータ先端技術株式会社）、蔦大輔、寺門峻佑（TMI総合法律事務所）、
東定治（トレンドマイクロ株式会社）、徳田敏文（インターネットセキュアサービス株式会社）、
淵上真一（日本電気株式会社）、北條孝佳、松本隆（株式会社ディー・エヌ・エー）、
丸山司郎（株式会社FFRIセキュリティ）、村田学（GMOサイバーセキュリティbyイエラエ株式会社）、
森田善明（AOSデータ株式会社）、山岡裕明（八雲法律事務所）、
吉野雅樹（SBテクノロジー株式会社）
…その他ご協力いただいた非常に多くの皆様

Special Thanks To　！！！！！！！！！！　②
Security NEXT、Scan Net Security、サイバーセキュリティ.com

※このレポートは、JNSA調査研究部会 インシデント被害調査WGとしてとりまとめたものであり、**所属企業・団体の立場、見解等を代表するものではありません。**

Ⅵ 用語集

	用語	説明
あ	IPA	アイピーエー。独立行政法人情報処理推進機構。経済産業省所管の独立行政法人。サイバー攻撃から企業・組織を守る取り組み等を実施。「中小企業の情報セキュリティ対策ガイドライン」など中小企業向けに多くのセキュリティ関連のコンテンツを公開
い	EDR	イーディーアール。Endpoint Detection & Response（エンドポイントでの検出と対応）。エンドポイント（主に従業員端末）において、防御だけでなく脅威の侵入を素早く検知し、被害最小化のための対応を実現するセキュリティ対策製品。ここ数年、大企業を中心に導入が進んでいる。
い	インシデント	元来「事件」「出来事」といった意味をもった語で、分野や業界によって細かな定義は異なる。情報セキュリティの世界では、システム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みます）を意味する。偶発的であるか意図的であるかは問わず、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す。
い	インシデントレスポンス	インシデントが発生した場合における、侵入経路、情報漏えいの有無、窃取された情報の内容・件数などの調査やその後の対応方針の決定など、これらインシデント発生後の事後的な対応
い	インシデントレスポンス事業者	インシデントレスポンスを提供する事業者
え	エモテット	メールアドレスほかメールに関するデータを窃取するマルウェア。メールによって拡散し、他のマルウェアの二次感染のために悪用されることもある。感染にはいくつかのパターンがあるが、メールに添付されたワードやエクセルのファイルを開きコンテンツの有効化（マクロの有効化）を実行することで感染する事例が多い。

	用語	説明
		感染拡大と、対策強化等に伴う収束を繰り返しているが、国内においては、2020年9月、2022年3月に多くの被害が発生した。このレポート作成時点においては小康状態にあるが、同種のマルウェアを含め今後の動向を注視する必要がある。
さ	サポート詐欺	インターネット閲覧時に実在するIT企業を装い、画面・音声によりマルウェア（トロイの木馬）に感染しているためサポートに電話するよう促すもの。画面に表示された電話番号にかけると、主に外国人（たどたどしい日本語）が応対し、復旧等のためにコンビニでの電子マネー購入など金銭を要求する（詐欺）。個人ほか法人（従業員）が被害に遭うケースもあり、電話の相手の指示に従うと、遠隔操作のソフトをインストールさせられてしまい、PC内の情報を閲覧されてしまう可能性がある。
し	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。ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業を行うセキュリティベンダーを中心に構成される業界団体
し	GDPR	ジーディーピーアール。EU一般データ保護規則。日本における個人情報保護法に相当
せ	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
た	ダークウェブ	一般的なウェブブラウザーでは閲覧することができない、匿名性の高いネットワーク上に構築されたサイト群。ドラッグ、偽造品、麻薬、銃、盗難物、クレジットカード情報、個人情報などを販売・取引するサイトも存在する。マスコミ等においては「闇サイト」と表現することもある
ち	チャージバック	クレジットカードの不正利用があった場合にカード会社がその販売代金について加盟店への支払を拒否するもしくは返還を求めること
と	DoS攻撃/DDoS攻撃	ドス攻撃（Denial-of-Service attack）。ネットワークまたはネットワークに接続された端末に過剰な負荷をかけ、サービスを提供することをできなくしてしまう種類の攻

	用語	説明
		撃。複数の端末から分散的に行われるものをDistributedの頭文字を冠し、ディードス攻撃（DDoS攻撃。Distributed Denial-of-Service attack）という
ひ	ビジネスメール詐欺	取引先、自社内の役員等になりすました電子メールによって、特定の口座への入金を促す詐欺。ベックまたはビーイーシー（BEC。Business Email Compromise)とも呼ばれる。
ま	マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。以前はコンピューターウイルスと呼ばれた時代もあるが、いまはコンピュータウイルスもマルウェアの一種として位置付けられる。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）への感染もマルウェア感染の１つの類型
ら	ランサムウェア	データを暗号化する等により、その復号と引き換えに身代金を要求するマルウェア。Ransom＝身代金、Software＝ソフトウェアをかけあわせた語

Ⅶ 参考文献・資料

[1] IPA（2023）：「偽セキュリティ警告画面の閉じ方体験サイト」
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

[2] IPA（2008）：NIST SP800-61 コンピューターセキュリティインシデント対応ガイド
https://www.ipa.go.jp/files/000025341.pdf

[3] JPCERT/CC（2021）：インシデントハンドリングマニュアル
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

[4] IPA（2023）：「中小企業の情報セキュリティ対策ガイドライン」「付録8：中小企業のためのセキュリティインシデント対応手引き」
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf

[5] 警察庁サイバー警察局：都道府県警察本部サイバー犯罪相談窓口一覧（リンク集）
https://www.npa.go.jp/bureau/cyber/soudan.html

[6] 経済産業省 ：情報セキュリティサービス審査登録制度
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

[7] IPA（2021）：情報セキュリティサービス基準適合サービスリストの公開
https://www.ipa.go.jp/security/it-service/service_list.html

[8] 株式会社クオカード「謝罪」に関する実態調査（2021年12月
https://www.quocard.com/pay/business/column/shazai-owabi/owabi_01/

[9] The No More Ransom Project
https://www.nomoreransom.org/ja/index.html

[10] IPA（2023）：中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/guide/sme/about.html

[11] JNSAソリューションガイド
https://sg.jnsa.org/

[12] JNSA（2019）：2018年 情報セキュリティインシデントに関する調査報告書【速報版】（セキュリティ被害調査ワーキンググループ）
https://www.jnsa.org/result/incident/2018.html

[13] 一般社団法人日本クレジット協会：クレジットカード不正利用被害額調査（2023年12月）
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

[14] セゾンカード　セキュリティ情報
https://www.saisoncard.co.jp/customer-support/security/
[15] 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
[16] 経済産業省：営業秘密～営業秘密を守り活用する～
https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html
[17] 警察庁（2023）：サイバー空間をめぐる脅威の情勢等
https://www.npa.go.jp/publications/statistics/cybersecurity/
[18] Coveware：Ransomware Quarterly Reports
https://www.coveware.com/ransomware-quarterly-reports
[19] 朝日新聞（2021）：消えた電子カルテ、お産もできない…田舎の病院を襲ったサイバー攻撃
https://digital.asahi.com/articles/ASPCW5SYHPCSULZU00Z.html
[20] 朝日新聞（2022）：電子カルテ失われ、この患者「誰やねん」　「記憶喪失」に陥った病院
https://digital.asahi.com/articles/ASQD176W4QD1ULZU00P.html
[21] 讀賣新聞（2022）：トヨタ工場の停止、ハッカー集団「ロビンフッド」関与…未確認ウイルスのため即復旧を断念
https://www.yomiuri.co.jp/national/20220613-OYT1T50213/
[22] NHK（2023）：名古屋港にサイバー攻撃？ ランサムウェアの被害とは？
https://www.nhk.or.jp/nagoya/lreport/article/001/44/
[23] 米国インターネット犯罪苦情センター（IC3）（2015）：Business E-mail Compromise
https://www.ic3.gov/media/2015/150122.aspx
[24] 全銀協 ： 法人間の外国送金の資金をだまし取る詐欺にご注意！　（BEC（Business E-mail Compromise）_ foreign remittance fraud）
https://www.zenginkyo.or.jp/topic/detail/nid/3561/
[25] 警察庁 ： ビジネスメール詐欺に注意！
https://www.npa.go.jp/bureau/cyber/countermeasures/bec.html
[26] IPA ： ビジネスメール詐欺（BEC）対策
https://www.ipa.go.jp/security/bec/index.html

[27] IPA（2017）：【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口
https://www.ipa.go.jp/archive/security/security-alert/2017/0403-bec.html

[28] IPA（2018）：【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報）
https://www.ipa.go.jp/archive/security/security-alert/2018/08-bec.html

[29] IPA：ビジネスメール詐欺の事例集を見る
https://www.ipa.go.jp/security/bec/bec_cases.html

[30] Forbes（2021）：Fraudsters Cloned Company Director’s Voice In $35 Million Heist, Police Find
https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/

[31] 在香港日本国総領事館（2023）：その電話、詐欺かも！？（電話詐欺に関する注意喚起）
https://www.hk.emb-japan.go.jp/itpr_ja/scam_call.html

[32] IPA（2023）：サイバー情報共有イニシアティブ（J-CSIP） 運用状況［2023年4月～6月］3.1 海外関連会社を狙った電話を併用する攻撃
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q1-report.pdf

[33] JPCERT/CC（2020）：ビジネスメール詐欺の実態調査報告書
https://www.jpcert.or.jp/research/BEC-survey.html

[34] トレンドマイクロ株式会社（2023）：国内の平均被害額5,000万円以上－BEC(ビジネスメール詐欺)被害の日本企業における実態と今求められる対策とは？
https://www.trendmicro.com/ja_jp/jp-security/23/l/expertview-20231204-01.html

[35] トレンドマイクロ株式会社（2023）：過去3年間で56.8%がサイバー攻撃の被害を経験、3年間の累計被害額は平均1.3億円、 ランサムウェア被害経験企業では平均1.8億円
https://www.trendmicro.com/ja_jp/about/press-release/2023/pr-20231101-01.html

[36] NPO法人 CIO Lounge（2023）：CIO Lounge/トレンドマイクロ「サイバー攻撃による被害状況調査」
https://www.ciolounge.org/info-list/cio-lounge-%E3%83%88%E3%83%AC%E3%83%B3%E3%83%89%E3%83%9E%E3%82%A4%E3%82%AF%E3%83%AD%E3%80%8C%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%94%BB%E6%92%83%E3%81%AB%E3%82%88%E3%82%8B%E8%A2%AB%E5%AE%B3%E7%8A%B6/

[37] 日本経済新聞（2017）：日本航空、偽メールで3億8千万円詐欺被害
https://www.nikkei.com/article/DGXMZO24866680Q7A221C1CC1000/

[38] 日本経済新聞（2019）：トヨタ紡織、欧州で最大 40 億円流出　業績修正を検討
https://www.nikkei.com/article/DGXMZO49508720W9A900C1CN8000/

[39] 日本経済新聞（2019）：日経米子会社、香港に32億円流出　詐欺被害か
https://www.nikkei.com/article/DGXMZO51583520Q9A031C1SHA000/

[40] 警察庁（2023）：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf
金融庁（2023）：インターネットバンキングによる預金の不正送金事案が多発しています。
https://www.fsa.go.jp/ordinary/internet-bank_2.html

[41] 全銀協（2023）：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/2023/n092501/

[42] 日本サイバーセキュリティ・イノベーション委員会（JCIC）- 社内のセキュリティリソースは「0.5%以上」を確保せよ
https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf

変更履歴

Version	日付	修正内容
1.00	2023/2/9	Ver1.00公開