インシデント損害額
調査レポート
2021

JNSA

インシデント被害調査WG

Version 1.02

目次

Ⅰ　はじめに

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

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

また、実際のインシデント発生時には各種対応ほか、被害者からの損害賠償請求、事業中断による利益喪失などを想定した場合、中小企業においても数千万円単位、場合によって億単位のお金がかかることを認識している経営者は多くはないと想定されます。

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

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

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、システムの運用におけるセキュリティ上の問題として捉えられる事象（これらに繋がる可能性のある事象を含みます）を意味します。

また、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

マルウェアとは、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（広義のコンピュータウイルス）をいいます。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つの類型となります。

○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、サービスを提供できなくしてしまう種類の攻撃をいいます。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、DDoS攻撃（ディードス攻撃。Distributed Denial-of-Service attack）といいます。

○ウェブサイトの改ざん

○従業員の持ち出しなど内部不正

○自然災害等による機器の損壊

○機器の故障

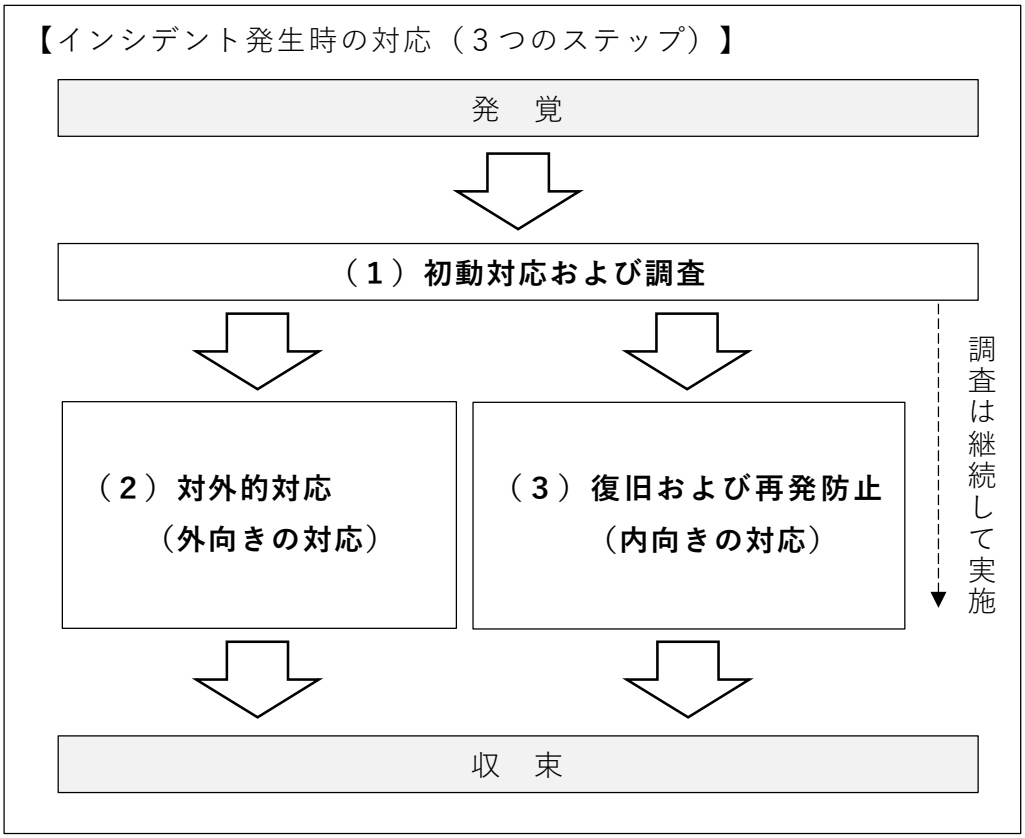
○電子メール、FAX、郵便物の誤送信・誤発送

○PCの紛失、USBメモリなどの記録媒体の紛失

２．インシデント発生時の対応の流れ

セキュリティ対策の主要な目的は、インシデントによるビジネスへの悪影響を極小化することにあります。しかし、適切な対策を実施したとしても、インシデントの発生を100％なくすことはできません。したがって、インシデントが発生した場合、事後的な対応、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も必要となります。

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「コンピュータセキュリティインシデント対応ガイド[1]」、JPCERT/CC「インシデントハンドリングマニュアル[2]」、IPA「情報漏えい発生時の対応ポイント集[3]」など）が参考資料として挙げられますが、この報告書では発覚から収束までの対応を単純化し、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、個人情報保護委員会等への報告（個人情報の漏えいがあった場合）、警察への相談等行政機関との連携、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。

この報告書では、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）に関して自社で直接、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、風評・レピュテーションに関して生じる損害などは、以下「２．賠償損害」～「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。

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

インシデントが発生した場合、インシデントレスポンスと呼ばれる事後的な対応が必要となります。これら対応の範囲は多岐に渡りますが、まずは、必要性や優先順位を踏まえつつ、初動対応として、ネットワークの遮断、証拠保全等を速やかに着手する必要があります。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、コンピュータや電子媒体の中に残された証拠を解析し、事故原因や影響・被害範囲の特定などの調査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。

○ネットワーク遮断、証拠保全、被害拡大防止等の初動対応
○フォレンジック調査
○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
○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
○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、発覚直後からその完了まで、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、PC、サーバー内のログを専門家が長時間をかけて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から確認することが可能です。

●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[4]」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[5]」として公開しており、このリストからも事業者を確認することが可能です。

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。

会社	標準的なコスト		過去経験した高額事例のコスト
	初動対応	フォレンジック調査	
A社	150万円	PC：150万円/台 サーバー：200万円/台	―
B社	20万円	PC：120万円/台 サーバー：150万円/台	2,000万円超
C社	80万円	PC：100万円/台 サーバー：150万円/台	1,500万円超
D社	６万円/時間（実稼働時間でコストを計算）。数十時間程度は必要		―
E社	PC：220万円/台 報告会などは別料金		―
F社	最低300万円～		―

図表Ⅲ-１-１　事故原因・被害範囲調査費用

エ．コスト概括

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、フォレンジック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、その費用は**数千万円～**に及ぶ場合もあります。

（２）対外的対応（外向きの対応）

①　コンサルティング費用（PR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、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、慎重な検討が必要となります。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、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自体が危ぶまれたケースがあったことは周知の事実といえるでしょう。

そのため、これらの対応はその初期段階において危機管理・メディア対応を行う専門業者へ依頼することが無難といえます。専門業者はこれまでのノウハウの蓄積を踏まえ、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するといえます。

特に、PR会社といわれる企業の広報・PR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時間数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・ツールのチェックにつき、それぞれ数十万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～**程度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月施行予定の改正個人情報保護法においては一定の要件のもと、被害者通知の義務化等が実施されるため、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。

○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
○個人情報が漏えいし訴訟が提起された場合の各種対応
○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
○個人情報保護委員会への報告
○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、数十万円程度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～**。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～**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、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、ハガキ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	75,990円
B社	87,010円
C社	84,700円
平均	80,000円

図表Ⅲ-１-２　DM印刷、発送費

上記はハガキでの印刷・発送費の価格ですが、被害者感情を踏まえた場合には、封書での印刷・発送も検討する必要があります。この場合には、１通あたり100～200円程度の費用が必要となります。

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でありますが、実績・信用度を加味して、既に取引のある印刷業者等に依頼した場合には、より高い金額が必要となることも想定されます。

（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として、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　全国版新聞の臨時広告掲載料

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）
474,251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、ハガキ１通あたり**80円**前後、封書の場合**100～200円**となります。印刷部数が増えるにつれて、１通当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）、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等）、対応期間（何か月実施するか）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）は全体の１～３％程度であり、対応期間は１～６か月（２か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）と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。

○FAQやスクリプトの整備
○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
○電話番号の取得
○システムの改修・設定
○顧客等関係者からの電話受付などの受信業務
○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か月目以降は縮小） オペレーター10席程度を見込む 通信費は別途	録音は３か月保存が標準
B社	約550万円	初月約1,500万円（２か月目以降は縮小） 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100万円	初月約300万円（２か月目以降は縮小） オペレーター3席程度を見込む 通信費は別途	録音は６か月保存が標準

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金はおおむ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か月**120～200万円**程度の金額が必要となります。例えば、３か月の対応を実施する場合、初月はオペレーター３席、２か月目以降は１席としたときには、600～1,000万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おり、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）

QUOカードの購入費用の一例は次のとおりです。

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枚当たりの購入費用
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枚当たりの購入費用例

エ．コスト総括

プリペイドカード購入時には、１枚当たり額面＋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　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、自社以外の関係者にも大きな影響が発生するような情報が漏えいしたときは、これら関係者からの要請があることも含め、ダークウェブ上でその情報がやり取りされていないかを確認することの検討も必要になります。

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。脅威情報）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によると、調査の内容や対応する技術者のレベルによってばらつきはあるものの、概ね次の費用を要するようです。

・スポット検索調査（３か月）：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

技術者を介在させた調査を実施する場合、概ね**数百万～数千万円**程度のコストを要すると想定されます。これら調査費用は、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、そのボリュームに大きく左右されるようです。また、ダークウェブでは、英語以外の言語も多く使用されているため、これら言語に精通した要員を調達するためのコストも大きく影響するようです。

（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。

この報告書では、システム復旧費用を、復旧する対象によりデータ復旧費用とハードウェア復旧費用に分類した上で解説します。

区分	内容
データ復旧費用	データが消失し、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
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損傷、火災、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

図表Ⅲ-１-７　システム復旧費用の分類

（ア）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**。この場合、情報システムの規模やデータ量等に応じてITベンダーによる作業コストが発生します。

データ復旧費用が発生する原因は、サイバー攻撃、非サイバー攻撃それぞれによって生じる場合があります。

サイバー攻撃の場合には、攻撃者が「被害者にデータを復旧させない」という意図をもってデータが破壊され、バックアップされたデータにも影響が生じ、復旧が難しいケースもあると考えられます。

また、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「暗号化したデータを復旧することを条件に、身代金を要求する」という、その仕組み上、攻撃者に金銭を支払うことで復旧（暗号化を解除、復号）できるケースはあります。しかしながら、金銭の支払によりデータが復元される保証もなく、こうした支払が犯罪助長につながることからも、これは推奨されるもの

ではないといえるでしょう。なお、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」プロジェクトでは、そのサイトにおいて、150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（2021年7月12日現在）[6]。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。

（イ）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、最大でもその再調達の額となるといえます。

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もあります。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。

イ．アウトソーシング先

（ア）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、利用しているサービスプロバイダー等

B．バックアップが取得できていない場合

（A）紙情報からデータを再入力するとき

ITベンダー等

（B）損傷したメディアからのデータを修復・サルベージするとき

データ復旧業者

（イ）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

ウ．調査結果（ヒアリング・インターネット調査）

この報告書では、前述のとおり、システム復旧費用をデータ復旧費用とハードウェア復旧費用に２区分し、データ復旧費用についてはバックアップからの復旧、ハードウェア復旧費用は修理・再調達が必要となることを記載していますが、前者についてはデータ量等、後者については復旧を要する機器の範囲等その対応規模によって大きく異なることから、これらの額について、調査は行わず、データ復旧業者の費用について調査を実施しました。

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-１-８　データ復旧業者の費用

エ．コスト総括

前述のとおり、データ量、復旧を要する機器の範囲等その対応規模によって大きく異なることから、費用はケースバイケースであり、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）データ復旧費用

Ａ．バックアップが取得できている場合

対応規模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、利用しているサービスプロバイダー等への問い合わせが必要となります。

Ｂ．バックアップが取得できていない場合の場合

（Ａ）紙情報からのデータ再入力の場合

対応規模により大きく異なります。ITベンダーへの見積もりが必要となります。

（Ｂ）損傷したメディアからのデータを修復・サルベージするとき

HDD等のメディア１つ当たり**数万～数十万**の費用が想定されます。

（イ）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ベンダーへの見積も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．HDDなどの大容量メディアの物理的損傷の場合

HDD等のメディア１つ当たり数万～数十万の費用が想定されます。

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。

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、インシデントによって生じる損失（被害額）として捉えられるものではありませんが、この報告書では損失の一部として整理しています。また、インシデントにはよってとは再発防止策は、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が、この報告書では、再発防止費用を技術的な観点からのセキュリティ商材導入費用、組織的な観点からの組織編制費用、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解説します。

なお、再発防止策は、種々想定されるものであり、この報告書で掲げたセキュリティ商材に限るものではないことを申し添えます。

区分	内容
セキュリティ商材導入費用	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商材・サービスを導入した場合の費用
組織編制費用	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-１-９　再発防止費用の分類

（ア）セキュリティ商材導入費用

発生したインシデントがセキュリティ商材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商材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。

この報告書では、中小企業のインシデント再発防止を前提として、ウイルス対策ソフトおよびメールフィルタリングサービスの２つの商材に絞ったうえで、これを調査し、とりまとめています。

前者はIPAの「中小企業の情報セキュリティ対策ガイドライン[7]」でも第一に実施すべき対策として記載されているように、ベーシックなセキュリティ商材として浸透していること、後者はマルウェアの拡散などメールを契機とした攻撃は普遍的に発生しており、同サービスを導入されている企業も多いと考えられることから取り上げています。

（イ）組織編制費用

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。

この報告書では、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にヒアリングした結果を掲載しています。

（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、自社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ることもあります。

この報告書では、２つの事業者に、企業向けの教育サービスの価格をヒアリングした結果を掲載しています。

イ．アウトソーシング先

セキュリティベンダー

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）セキュリティ商材費用

ウイルス対策ソフトおよびメールフィルタリングサービスを提供している事業者をインターネット上で調査した結果は次のとおりです。

Ａ．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	2,000～3,000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により変動
Ｂ社	600～5,000円程度	価格は利用台数および契約年数により変動。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	500～2,000円程度	価格は利用台数および契約年数により変動

図表Ⅲ-１-10　ウイルス対策ソフトの価格

Ｂ．メールフィルタリングサービス

会社	価格 １ライセンス・１年	備考
Ａ社	3,000～6,000円程度	価格は利用ユーザ数により変動。ストレージサービスに対するスキャン機能も同時に提供
Ｂ社	3,000～9,000円程度	価格は利用ユーザ数により変動。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	500～1,500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-１-11　メールフィルタリングサービスの価格

（イ）組織編制費用

SOCを運営している１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	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日対応可能 複数機器を監視し、高度な相関分析を行う。
B	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日対応可能 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 - 12　組織編制費用

（ウ）セキュリティ教育費用

セキュリティ教育を提供している２つの事業者にヒアリングした結果は次のとおりです。

会社	費用 １ライセンス・１か月	備考
企業A	100～1,500円程度	３種類程度の教材を利用可能 価格はライセンス数によって変動
企業B	100～70,000円程度	20種類程度の教材を利用可能 価格は利用期間とライセンス数によって変動。高額なものはセキュリティ担当者向け

図表Ⅲ- 1 -13　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るところですが、この報告書でとりまとめた結果は次のとおりです。

（ア）セキュリティ商材導入費用

ウイルス対策ソフトおよびメールフィルタリングソフトは、それぞれ１ライセンスあたり年間**数百～数千円**で導入可能といえます。

（イ）組織編制費用

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～数百万円**で利用できるようです。

（ウ）セキュリティ教育費用

１ライセンスあたり**数百～数千円**程度、セキュリティ担当者向けでは数万円～のコストがかかります。

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。

この報告書では、情報漏えいを次の 4 区分に整理し解説します。

区分		損害賠償請求の内容
個人情報の漏えい	自社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．自社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．他社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ときは、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、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．自社が管理する個人情報を漏えいした場合

JNSA調査研究部会セキュリティ被害調査WGによる「情報セキュリティインシデントに関する調査報告書[8]」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か年平均	**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

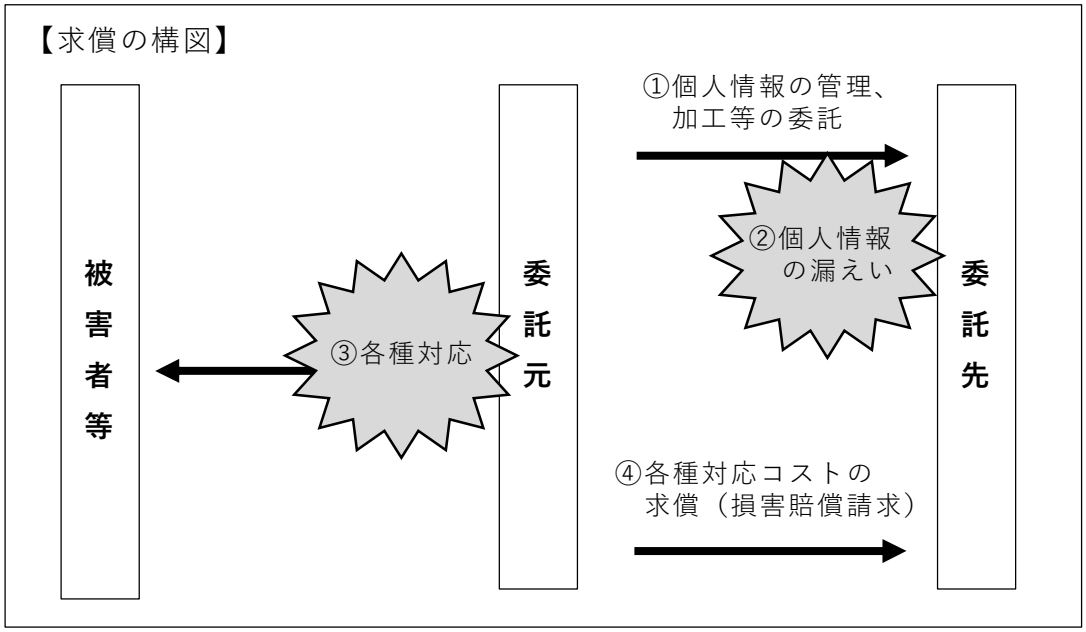
例えば、システム会社が他企業からデータ処理を依頼された個人情報を漏えいしたケースや、販売店や下請企業がメーカーや元請企業から管理を委託されている個人情報を漏えいしたケースなど、個人情報の管理、加工等を委託された企業がその個人情報を漏えいした場合は、通例、上流に位置する委託元企業において前述「１．費用損害（事故対応損害）」に記載したような各種事故対応が必要となります。

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～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[9]によると、全体として、2015年は120.95億円であったのに対し、2020年は251.0億円と倍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67.3億円であったのに対し、2020年には223.6億円と、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、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[10]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～」[11]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、この報告書では、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	２％＋369万円	４％＋738万円
30億円超	協議により決定	協議により決定

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。

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か月間、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。

4. 金銭損害

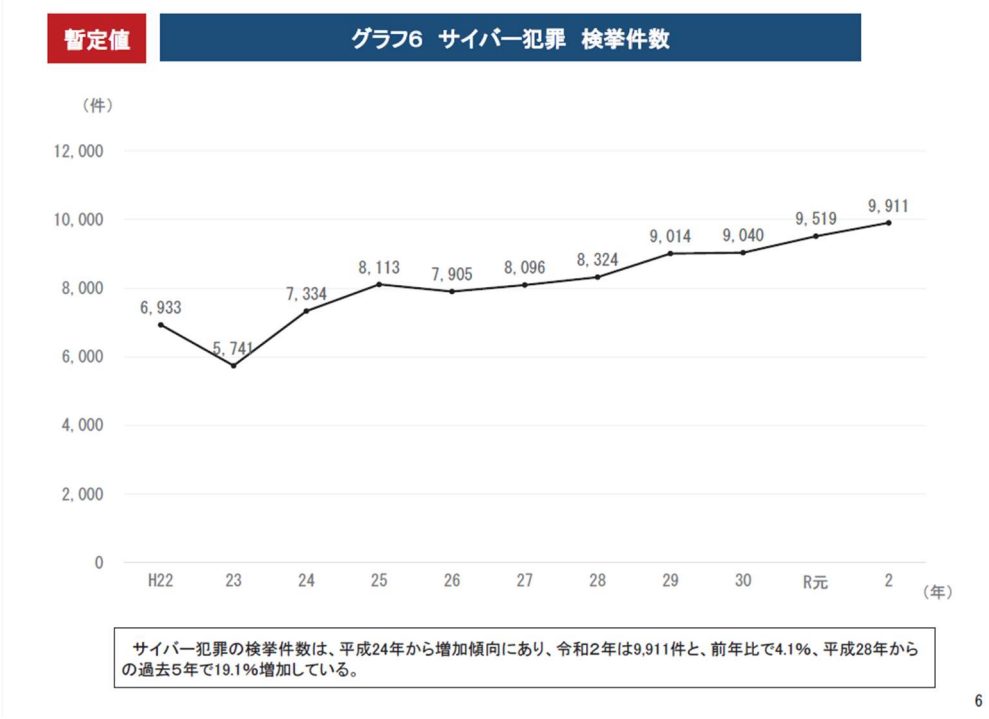
インシデントにより直接的な金銭損害を被るケースは珍しくありません。

警察庁が発表した「令和2年の犯罪情勢[12]」を見ると、日本国内においてもサイバー犯罪の検挙件数が増加を続けており、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。

国内の調査データを見てみると、4年前の2017年6月に、大阪商工会議所が大阪の中小企業を対象に、サイバー攻撃に対する意識調査、現状の対策、被害状況についてアンケート調査を行いました。その結果、標的型攻撃メールを受信したことがある企業が18%、ランサムウェア（身代金ウイルス）による被害を受けた企業が全体の7%もあり、その約半数が攻撃者の要求に応じて身代金を支払ったことが示されています。[13][14]

この報告書では、企業・組織が被害を受け得る、セキュリティ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。感染したパソコン等の端末やサーバー上のデータを暗号化する等して使用不可にし、そ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される「二重の脅迫（double extortion）」と呼ばれる攻撃も報告されています。

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、明確な標的を定めない広く無差別な攻撃（ウイルスメールをばらまくといった方法など）が主でしたが、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

公開されている国内の被害情報は多くありません。

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等の暗号資産（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。

このことから、この報告書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。

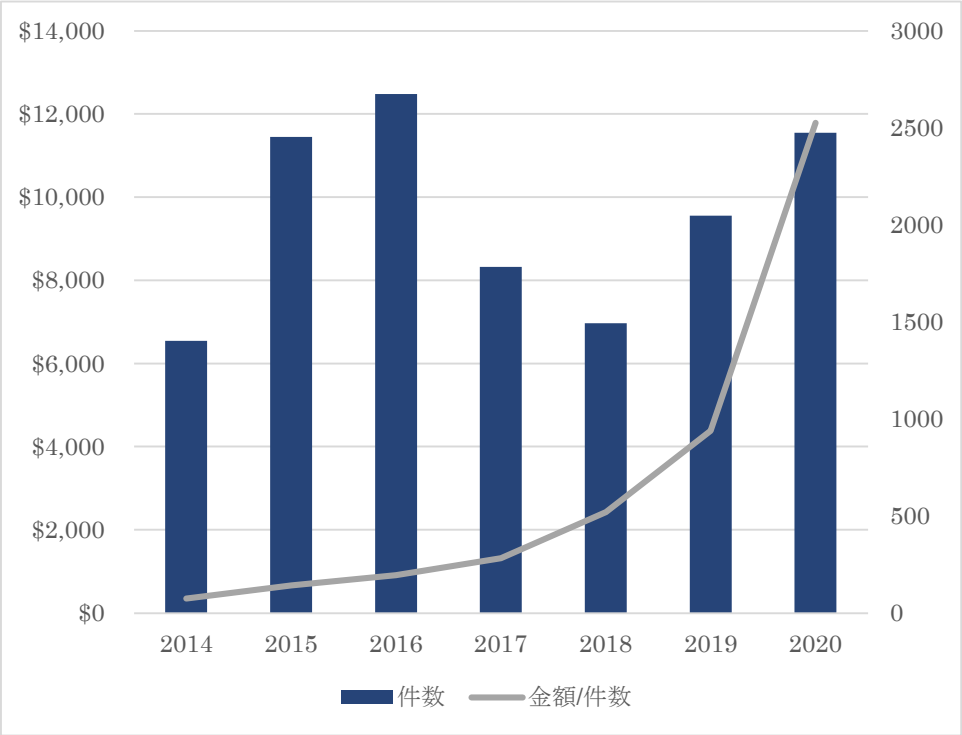
図表Ⅲ-４-２は、米国インターネット犯罪苦情センター（IC3）[15]が、毎年、同センターに寄せられた年間情報をまとめたレポート、「Internet Crime Report」の2014年から2020年の情報をもとに作成したグラフです。

件数には波がありますが、ここ数年は増加傾向であり、件数当たりの身代金

要求金額は増加の一途をたどっています。この増加傾向は今後も続くと考えられます。なお、同レポートにおける2020年のランサムウェア被害１件当たりの平均的な被害額はUS＄11,786となっていますが、件数のなかには、被害額が報告されていないデータが含まれており、被害金額の実態を表しているとはいえません。

被害金額の実態を表す数値としては、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「Coveware Quarterly Ransomware Report[16]」では、2021年第１四半期の身代金支払額は平均値US$220,298、中央値US$78,398と報じています。

なお、国内組織において身代金が要求された著名な事例としては、2020年11月に大手ゲーム会社がサイバー犯罪集団に社内データを盗まれ、データを消す代わりに身代金を要求された事例[17]（米メディアは身代金要求額を1,100万ドル（約11億5,000万円）相当と報じています[18]）が挙げられます。また、身代金要求額は明らかにされていませんが、2020年6月には大手自動車メーカーにてランサムウェア被害により工場の生産停止を余儀なくされた事例[1920]が挙げられます。



図表Ⅲ-４-２　米国におけるランサムウェア被害件数と１件当たりの平均被害額

ウ．コスト総括

Coveware社のレポートにおける2021年第１四半期の身代金支払額を日本円に換算すると、平均値**約2,400万円**、中央値**約860万円**（2021年8月1日現在）となります。ただし、前述のとおり、ランサムウェアによる身代金要求額は年々増加している傾向にあるため、今後、より高くなるおそれがあります。

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、「取引先などになりすました電子メールを送って送金を促す詐欺行為」を指します。取引先や自社の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等の金銭被害をもたらすサイバー攻撃の一種です。自社の経営者（CEOや経営幹部）になりすまし、従業員に偽の送金依頼メールを送るタイプのビジネスメール詐欺は「CEO詐欺」とも呼ばれます。

差出人（送信元）のメールアドレスに取引先を模したメールアドレスや本物のメールアドレスが使われていたり[21]、メールの返信や転送を装ったり[22]、自然な日本語の本文が使われたり等、本物のメールを見分けることが困難な事例も確認されています。

ビジネスメール詐欺については、様々な組織が情報を発信しています。2015年初め頃から、米国インターネット犯罪苦情センター（IC3）がBECに関する警告を公開し始め、同年1月にはBECを、「定期的に海外のサプライヤーや取引先と電信送金を行う組織を標的とした、高度な詐欺行為」として説明しています[23]。

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です。

イ．被害金額の傾向

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[24]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～数千万単位の被害に遭った事案も報告されています。

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[25]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[26]、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[27]などが挙げられます。

ウ．コスト総括

ビジネスメール詐欺による被害金額は、被害組織の取引規模により大きくことなるため、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。

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ウイルス感染などにより、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

ウイルス感染

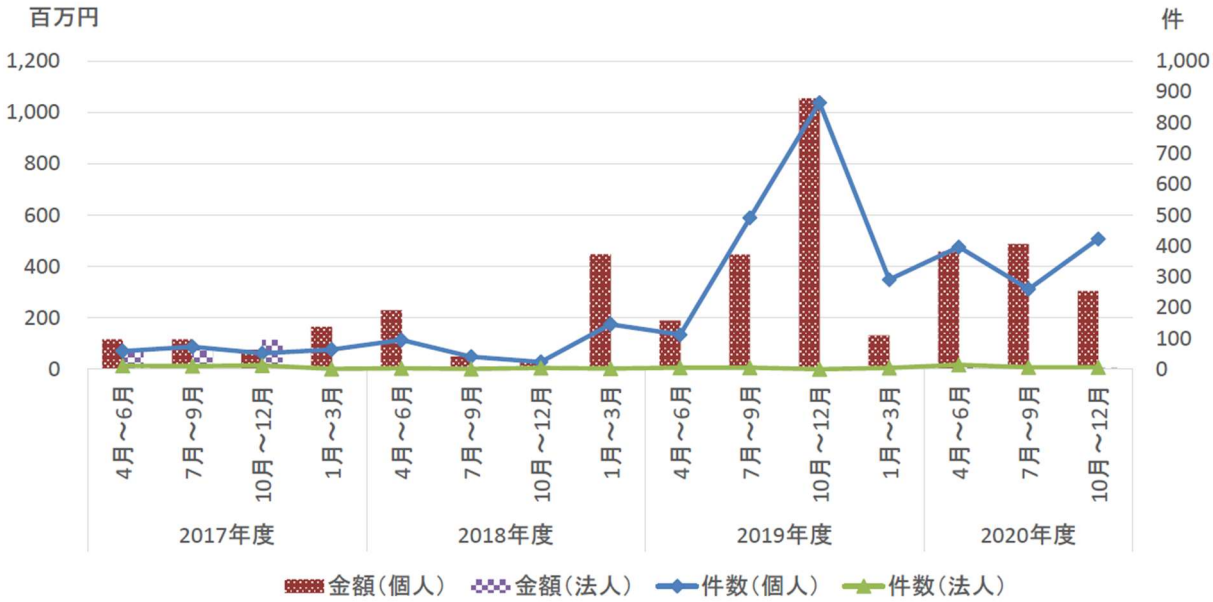
メールに添付された悪意あるファイルを開いて、端末をウイルスに感染させ

てしまい、攻撃者に認証情報を窃取される

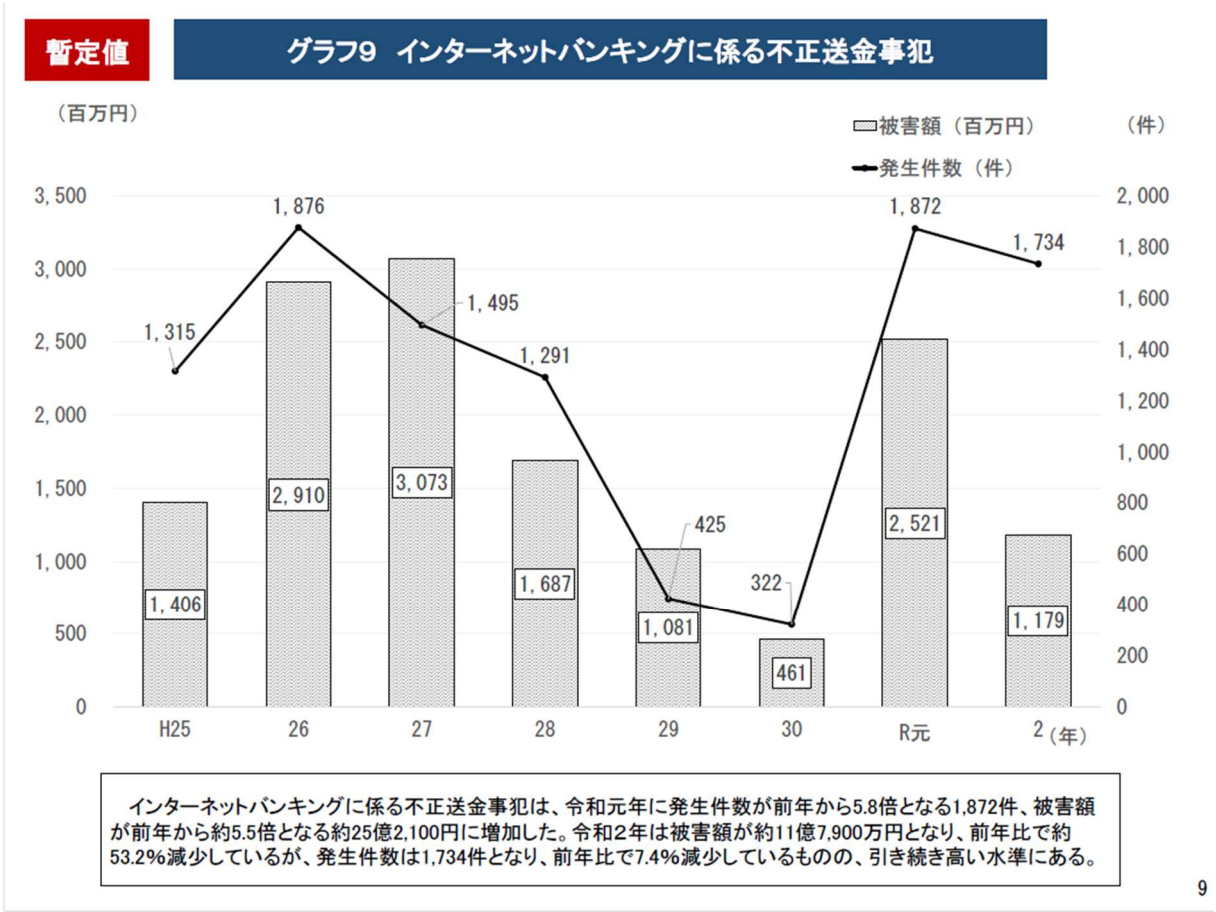
イ．被害金額の傾向

警察庁によると、2016年（平成28年）以降、金融機関のセキュリティ対策の強化等により減少傾向が続いていた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は、2019年（令和元年）に大きく増加しており、2020年（令和2年）中は、前年比では共に減少となっているものの、発生件数は引き続き高い水準となっています。

一般社団法人全国銀行協会によると、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、2019年から増加しており、2020年のインターネットバンキングの不正払戻し件数は1,401件、被害金額は約14億2,400万円でした。2019年の1,626件、約21億6,400万円からは減少しているものの高い水準となっています。なお、2020年の被害件数1,401件中の1,371件、約14億2,400万円中の約13億8,200万円は個人顧客の不正送金被害であり、被害件数の多くを占める状況が続いています。[28]



図表Ⅲ-４-３　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）



図表Ⅲ-４-４　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）

ウ．コスト総括

一般社団法人全国銀行協会の公表する2020年の被害事例をもとに、１件当たりの平均被害額を求めると、法人顧客の被害額は**約140万円**、個人顧客の被害金額は**約101万円**となります。

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	GDPR	General Data Protection Regulation （一般データ保護規則）
米国 （加州）	CCPA	California Consumer Privacy Act （カリフォルニア州消費者プライバシー法） なお、2023年1月には、改正法として、より消費者の権利を強化する内容となったCPRA（California Privacy Rights Act。カリフォルニアプライバシー権法）が施行される予定です

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CCPA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。

イ．アウトソーシング先

大手法律事務所、外資系コンサルティングファームほか、一部のITベンダー

ウ．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
米国（加州）	CCPA	消費者１名あたり**最大2,500ドル** （故意だと7,500ドル）

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、その後のインシデント復旧時間やインシデントが及ぼす影響範囲、対象企業の対応内容等によって大きく変動するため、セキュリティ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、セキュリティ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を余儀なくされたものが複数例あります。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）

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**数十パーセント程度**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、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。

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。また、インシ

デント発生後の対応に問題がある場合には、長期に渡って株価低迷を招くリスクがあります。

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。

過去の例で言えば、株価時価として、**数十パーセント程度**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。

Ⅳ　モデルケース

１．軽微なマルウェア感染

① インシデント概要

従業員がメールに添付されていたファイルを開いたところ、マルウェアに感染した。

② 対応および被害概要

○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、メールを介して感染が拡大するマルウェアであり、従業員端末3台とサーバー1台の感染が判明した。

○個人情報の漏えいのおそれなど、顧客影響等はないことが確認された。

③ 被害額（損失額）

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

２．ECサイトからのクレジットカード情報等の漏えい

① インシデント概要

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

② 対応および被害概要

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

３．大規模なマルウェア感染

① インシデント概要

○海外子会社のサーバーがサイバー攻撃を受けた。その後、攻撃者は各種資格情報を取得したうえでネットワークへの侵入を続け、本社が管理するサーバーにアクセスするに至った。

○攻撃者はさらにネットワーク内に存在する各種データをランサムウェアに感染させ、暗号化するとともに、既に窃取したデータの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

○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。

○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。

○生産ラインほか、主要なシステムは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か月を要した。

③ 被害額（損失額）

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

V　あとがき

インシデント被害調査WGは、2020年度のはじめに発足したWGで、この報告書をとりまとめることにより、インシデント発生時に必要となる対応や、インシデントにより生じる各種の損害（被害額・損失額）が高額になることを世間一般に広く知って欲しい、特にセキュリティベンダーの方々に理解いただき、中小企業を中心とした企業・組織に広く伝えて欲しいという想いのもと活動を開始しました。

しかしながら、折しものコロナ禍により、ヒアリングを中心としたその活動が十分に行えなかったことから、この報告書も加筆・修正の余地があるのも事実であり、次回以降さらなるバージョンアップを図っていきたいと考えています。

サイバー攻撃による被害は増加の一途を辿っています。この報告書を読んでいただくことにより、大企業・中小企業のいずれにおいても、セキュリティ対策の必要性を認識いただき、その強化が図られることを願います。

執筆（あいうえお順）
井田潤一（NTTデータ先端技術）
大谷尚通（NTTデータ）
神山太朗（あいおいニッセイ同和損害保険）（リーダー）
戸田勝之（NTTデータ先端技術）
西浦真一（キヤノンITソリューションズ）（サブリーダー）
西原真仁（JSOL）
山田道洋（日本電気）

Special Thanks To（あいうえお順）
岡田良太郎（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）、
軍司祐介（マキナレコード）、高田雄太（デロイト トーマツ サイバー）、
淵上真一（日本電気）、前田典彦（FFRIセキュリティ）、丸山司郎（FFRIセキュリティ）、
鷲尾浩之（ラック）、その他ご協力いただいた多数の皆様

※この報告書は、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	「II　インシデントの概要　1. インシデントとは」参照
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
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

	用語	説明
		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。広義にはコンピュータウイルス。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つの類型となります。
ら	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。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 (2008) : NIST SP800-61 コンピュータ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
[2] JPCERT/CC (2015) : 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_20151126.pdf
[3] IPA (2012) : 情報漏えい発生時の対応ポイント集(第3版)
https://www.ipa.go.jp/security/awareness/johorouei/
[4] 経済産業省(2018) : 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
[5] 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
[6] No More Ransomポータルサイト：https://www.nomoreransom.org/ja/index.html
[7] IPA (2021) : 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/keihatsu/sme/guideline/
[8] 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
[9] 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（2021年6月）https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf
[10] 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
[11] 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
[12] 警察庁（2021）: 令和2年の犯罪情勢【暫定値】
https://www.npa.go.jp/news/release/2021/20210128001.html
[13] 大阪商工会議所（2017）: 「中小企業向けサイバー攻撃対策支援事業の開始」ならびに「中小企業におけるサイバー攻撃対策に関するアンケート調査結果」について
https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf
[14] 商工総合研究所（2019）: 中小企業へのサイバー攻撃の現状とその被害調査結果に関して ―IPAおよび大阪商工会議所の調査結果から見えること―
https://www.shokosoken.or.jp/shokokinyuu/2019/10/201910_5.pdf

[15] 米国インターネット犯罪苦情センター（IC3）：https://www.ic3.gov/
[16] Coveware（2021）：Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
[17] 日本経済新聞（2020）：カプコン、不正アクセスで個人情報最大35万件流出 https://www.nikkei.com/article/DGXMZO66282210W0A111C2AC8Z00/
[18] BLEEPING COMPUTER (2020) : Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/
[19] 日本経済新聞（2020）：ホンダ、サイバー攻撃でシステム障害　生産を一部停止 https://www.nikkei.com/article/DGXMZO60154690Z00C20A6916M00/
[20] ITmedia エンタープライズ（2020）：ホンダのシステム障害、原因は産業制御システムを狙うランサムウェア「Ekans」か https://www.itmedia.co.jp/enterprise/articles/2006/11/news059.html
[21] 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/security/english/virus/press/200611/20170403-bec.html
[22] 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/security/announce/201808-bec.html
[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] 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
[25] 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/
[26] 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/
[27] 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/
[28] 一般社団法人全国銀行協会（2021）：盗難通帳、インターネットバンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正利用に関するアンケート結果について https://www.zenginkyo.or.jp/news/2021/n031101/

変更履歴

Version	日付	修正内容
1.00	2021/8/18	
1.01	2021/8/25	P28単位誤り修正、P5,6,42一部補記、P49誤字修正
1.02	2021/9/10	P48計算誤り等修正、P44、46誤植修正