2020年度「個人情報の取扱いにおける事故報告集計結果」

一般財団法人日本情報経済社会推進協会（JIPDEC）
プライバシーマーク推進センター
2021年10月 5日公表
2021年10月15日更新

1. はじめに

本資料は、2020年度中にプライバシーマーク制度運営要領（JIP-PMK500「プライバシーマーク付与に関する規約」第11条）に基づき、プライバシーマーク付与事業者の皆さまより当協会及び審査機関にご報告いただいた個人情報の取扱いにおける事故等について、取りまとめ、集計したものです。

皆さまの個人情報保護へのご尽力、また事故等のご報告について感謝するとともに、個人情報の取扱いにおける事故の発生防止・再発防止等にご活用いただければ幸いです。

2. 概要

2020年度の事故等報告件数

1. 2020年度は、939の付与事業者より2,644件の事故報告があり、2019年度と比較すると、報告事業者数は減少、事故報告件数は増加となりました。（2019年度：報告事業者数985社、事故報告件数2,543件）

2. 2020年度末時点の付与事業者数に占める事故報告事業者の割合は5.6%となり、こちらは2019年度に比べ減少しています。（2019年度：6.0%）

報告内容の概要

1. 事故の原因を件数が多い順に見ると、「誤送付」（1,648件：62.3%）が最も多く、次いで「その他漏えい」（454件：17.2%）、「紛失」（394件：14.9%）、その他（140件：5.3%）となりました。

2. 「誤送付」の内訳では、多い順に見ると、「メール誤送信」（764件：28.9%）、「封入ミス」（323件：12.2%）、「宛名間違い等」（314件：11.9%）となりました。「メール誤送信」が2019年度よりも大きく増加しています。

3. 「その他漏えい」の内訳では、「関係者事務処理・作業ミス等」は、2019年度には2018年度より減少（205件→138件）しましたが、2020年度には2018年度を超える232件に増加しました。

また、2019年度に2018年度から大幅に増加（55件→185件）した「プログラム/システム設計・作業ミス[1]」は2020年度には102件に減少しましたが、一件あたりの事故による漏えい件数が増加傾向にあります。また「ウイルス感染」も2019年度の9件から2020年度は3倍以上増えて29件となっており、増加傾向にあります。

4. 「その他」の内訳では、2018年度から2019年度にかけて増加（24件→66件）した「誤廃棄」が2020年度には38件に減少しました。他に目立つ点としては、2019年度には8件だった「内部不正行為」が、2020年度には15件に増加しました。

5. 2020年度は、新型コロナウイルス感染症対策のための「テレワーク実施」「新たなコミュニケーションツールの利用」などの業務環境の変化の影響が、事故報告の内容にも見られます。

3. 全般的な状況

（1）事故報告の状況

2020年度の付与事業者から当協会及び審査機関に対する事故報告の状況は、報告事業者数が939社、事故報告件数が2,644件となり、前年度と比較すると、報告事業者数が減少、事故報告件数が増加となりました。各年度末における付与事業者数全体に占める報告事業者数の割合は前年度6.0%から5.6%に減少、過去5.5%前後で推移していた状況に戻りました。[2] [3]

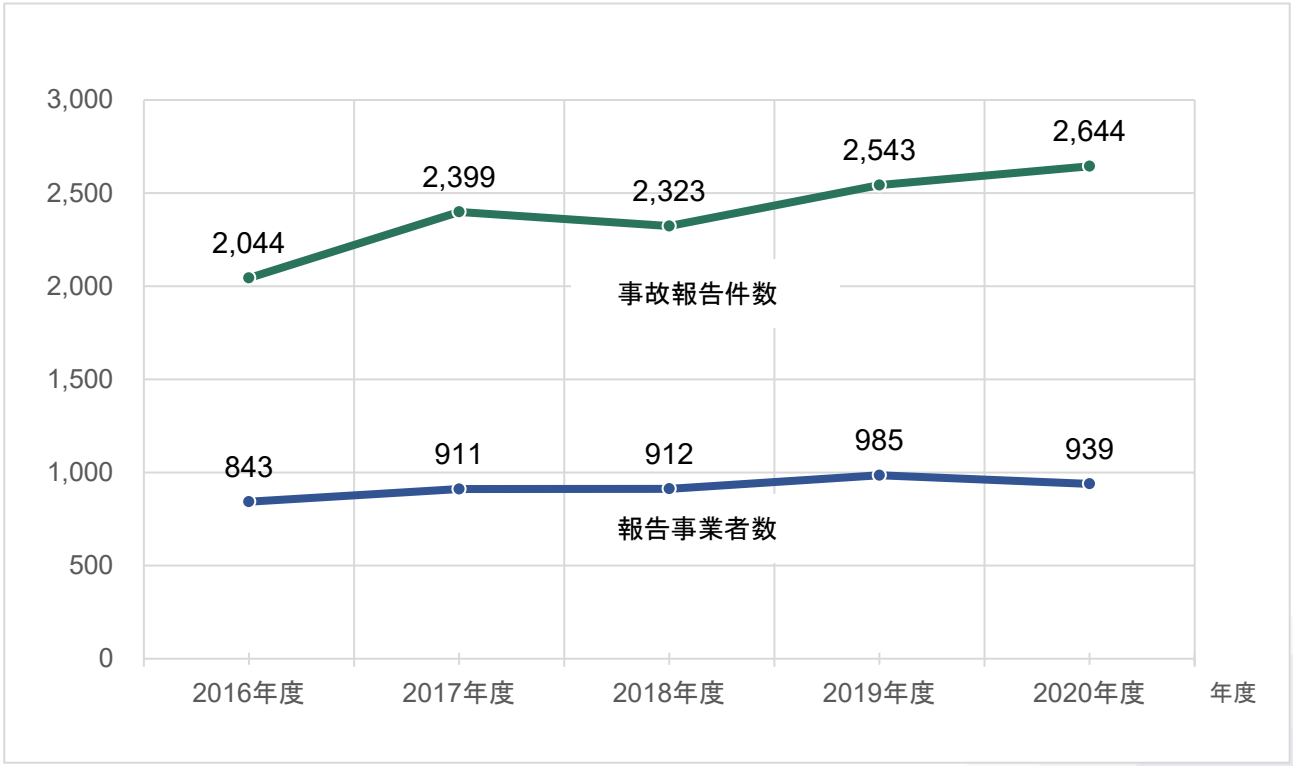


図 1：事故報告の状況

[1] 本年度より、「システムのバグ」の件数を「プログラム/システム設計・作業ミス」に含めて集計。
[2] 配達委託先が起因となり不可抗力と判断した事故の報告件数や報告事業者数は含まれない。また、同一の事業者から複数回事故報告書を提出された場合、「報告事業者数」は1社としてカウントした。
[3] 各年度末における付与事業者数全体に占める報告事業者数の割合は巻末のデータ編に記載。

(2) 原因別に見た事故報告状況

当協会及び審査機関に報告された事故報告について、発生原因別にみると、前年度に続き「誤送付」が1,648件（62.3%）と最も多く、次に「その他漏えい」454件（17.2%）、「紛失」394件（14.9%）の順となりました。

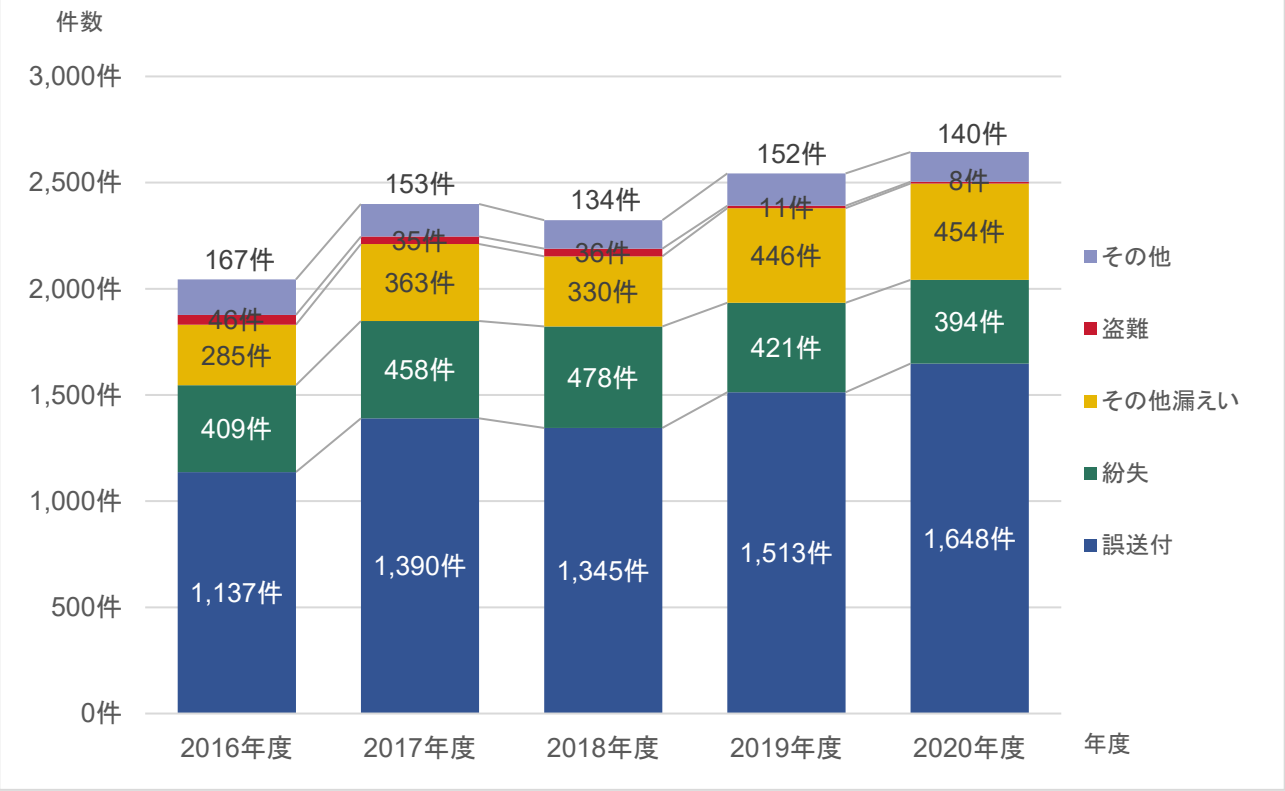


図 2: 原因別に見た事故報告件数の状況

図2の「誤送付」の内訳は、図3の通り、書類等送付時の「宛名間違い等」「封入ミス」「配達ミス」に「メール誤送信」「FAX誤送信」を加えたものです。そのうち「メール誤送信」は764件と事故報告全体の中でも最も報告件数が多く、誤送付の中で次に多かったのは「封入ミス」で323件でした。

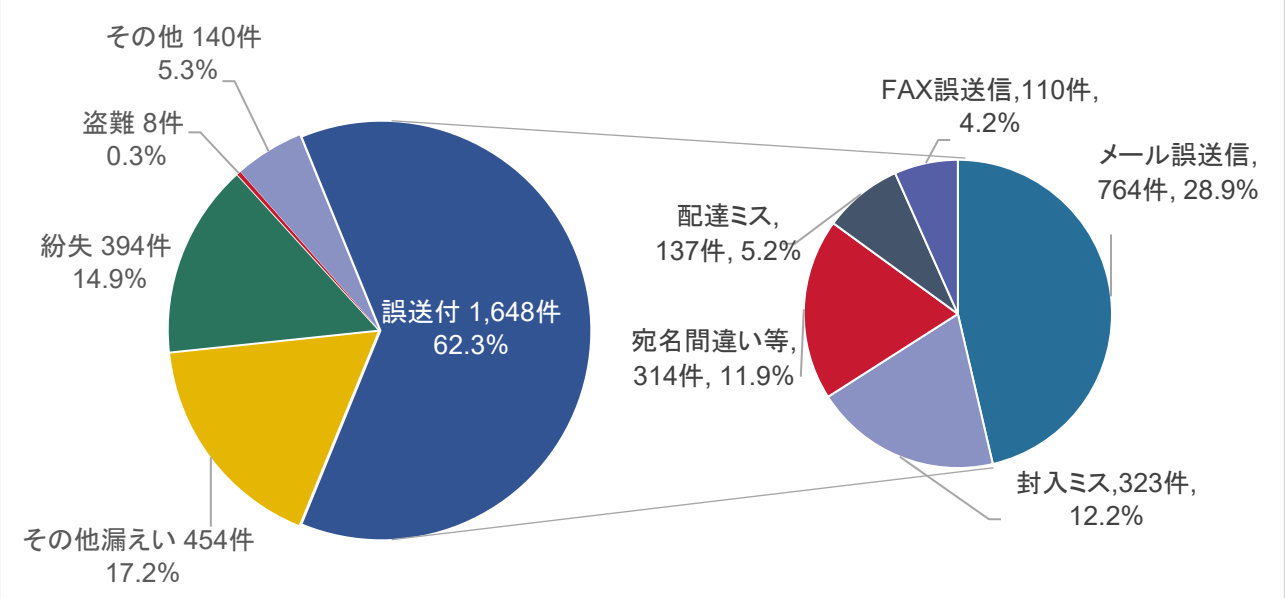


図 3: 原因別事故報告件数「誤送付」の内訳

ここ5年間の「誤送付」の内訳の原因別割合の推移をみると、「メール誤送信」は2020年度が最も高くなっているのに対し、紙媒体による「宛名間違い等」「封入ミス」「FAX誤送信」は2020年度が最も低くなっています。これは、新型コロナウイルス感染症対策のための「テレワーク」導入等による、通信手段・連絡手段の変化によるところと推測されます。

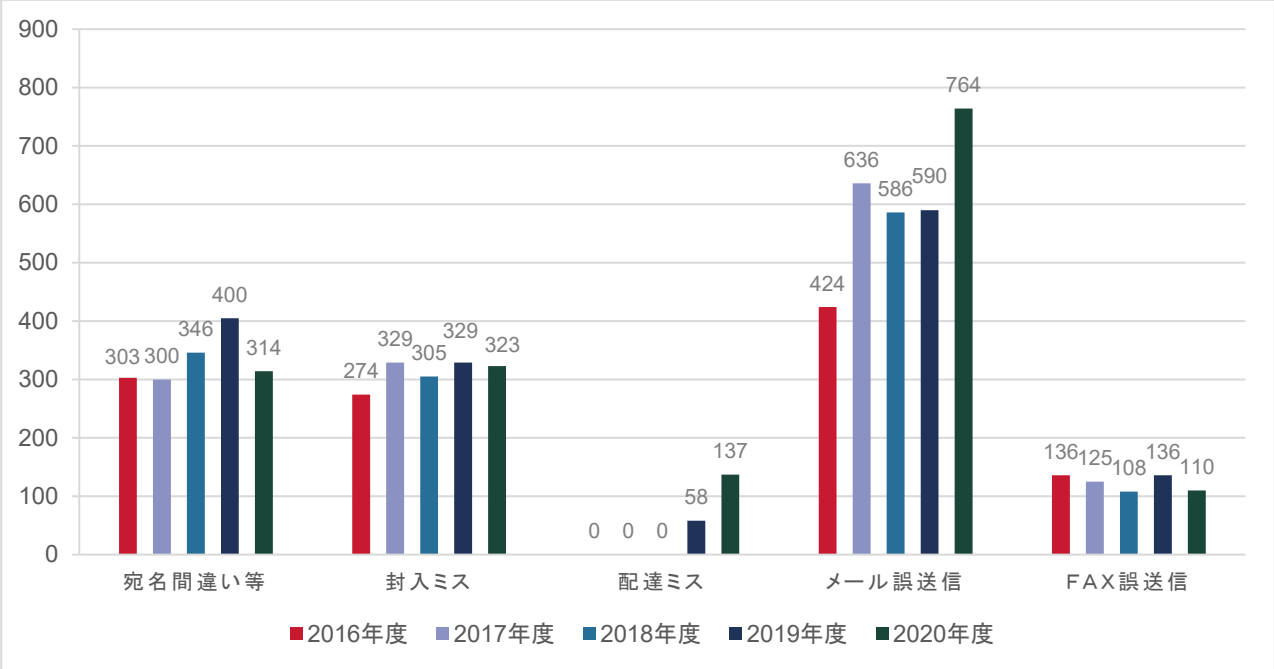


図 4: 原因別事故報告件数「誤送付」の内訳推移

また、今回の集計において、かつては見られなかったメッセージングサービス等の「新たなコミュニケーションツール」における誤送信事故は「メール誤送信」に含めており、その点においても、新型コロナウイルス感染症対策による業務のやり方の変化が集計から読み取れます。

図2の「その他漏えい」(454件)の内訳は、図5の通り、「ウイルス感染」「プログラム/システム設計・作業ミス(システムのバグを含む)」「不正アクセス・不正ログイン」「口頭での漏えい」「関係者事務処理・作業ミス等」となります。

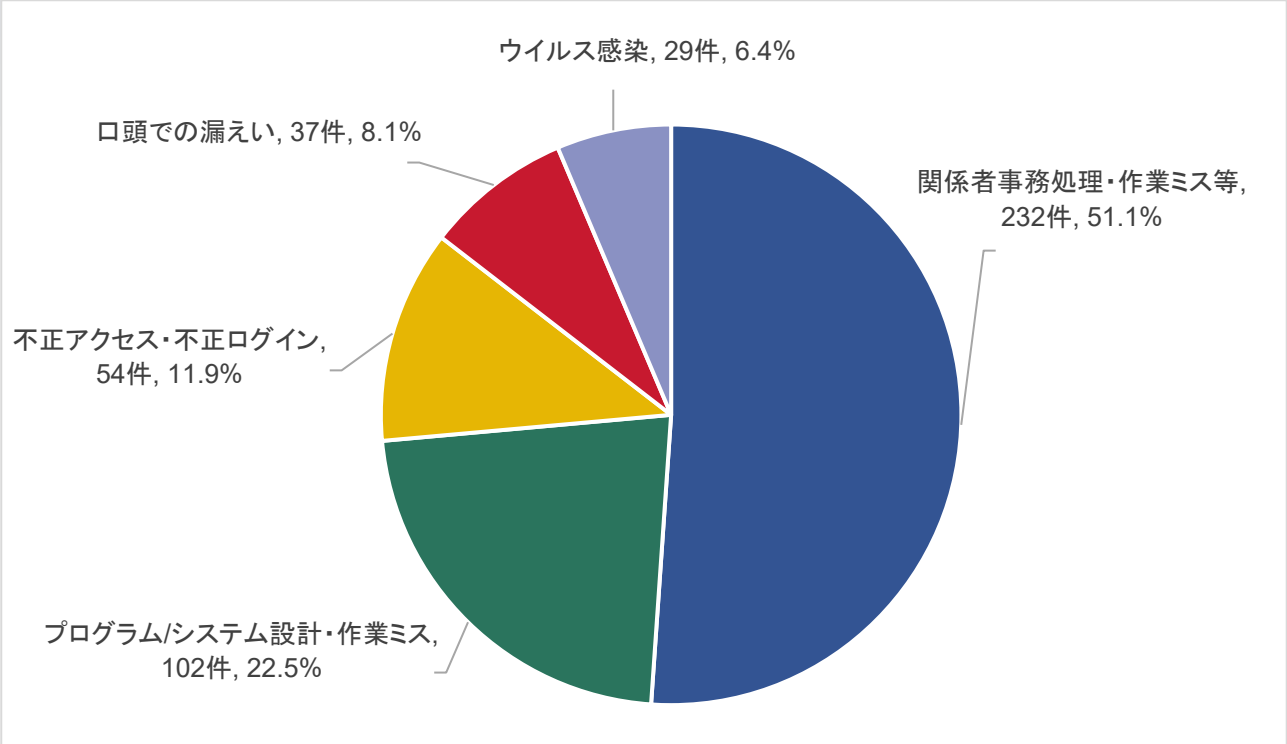


図 5: 原因別事故報告件数「その他漏えい」の内訳

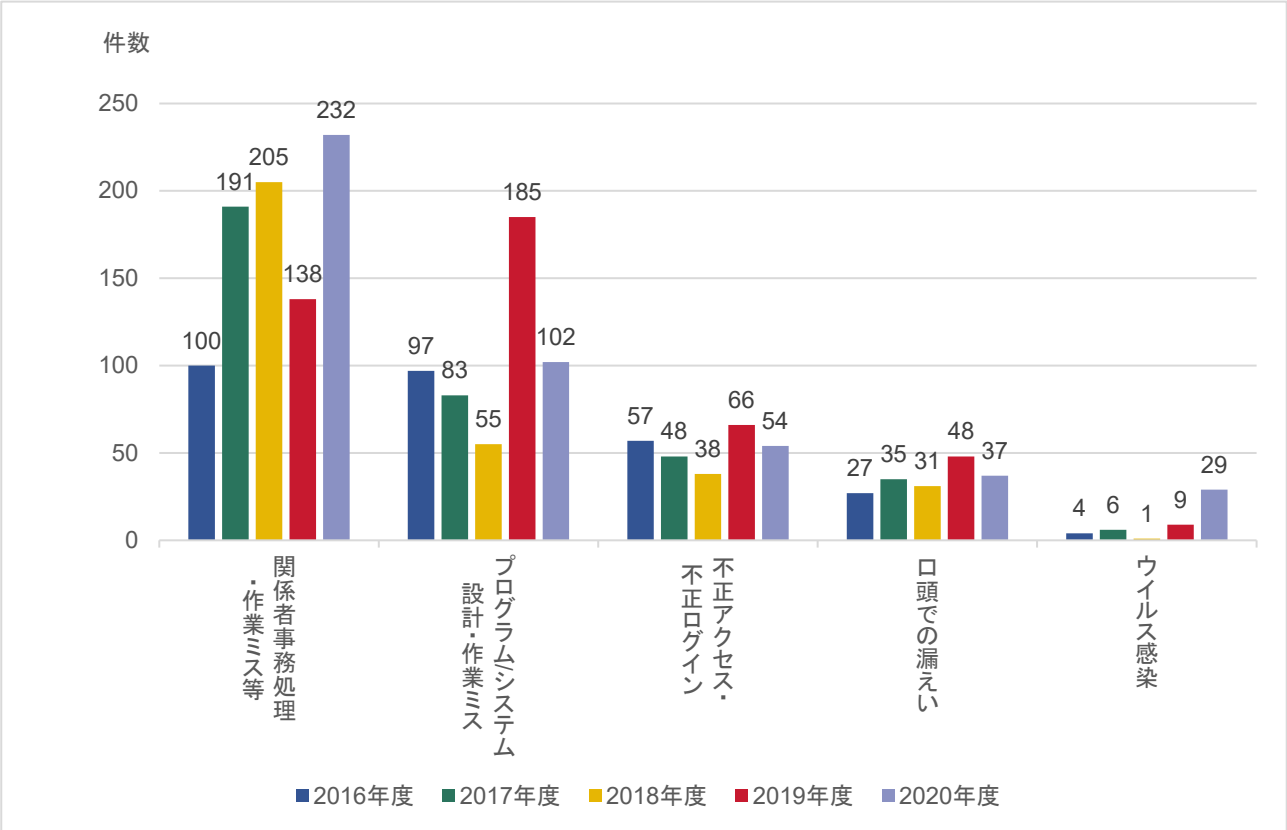


図 6: 原因別事故報告件数「その他漏えい」の内訳推移

図6の通り、関係者事務処理・作業ミス等はこれまでに比べて大きく増えており、新型コロナウイルス感染症対策のために、いつもと作業や手順が異なることで、発生したと言えるでしょう。

また、ウイルス感染も前年度から3倍以上に増えており、増加傾向にあることがわかります。

漏えい以外の事故である「その他」（140件）の内訳は、図7の通り、「不正取得」「目的外利用」「同意のない提供」「内部不正行為」「誤廃棄」「滅失、き損」「左記に分類できない内容」「評価対象外(事故対象に個人情報が含まれていなかった場合等)」となります。

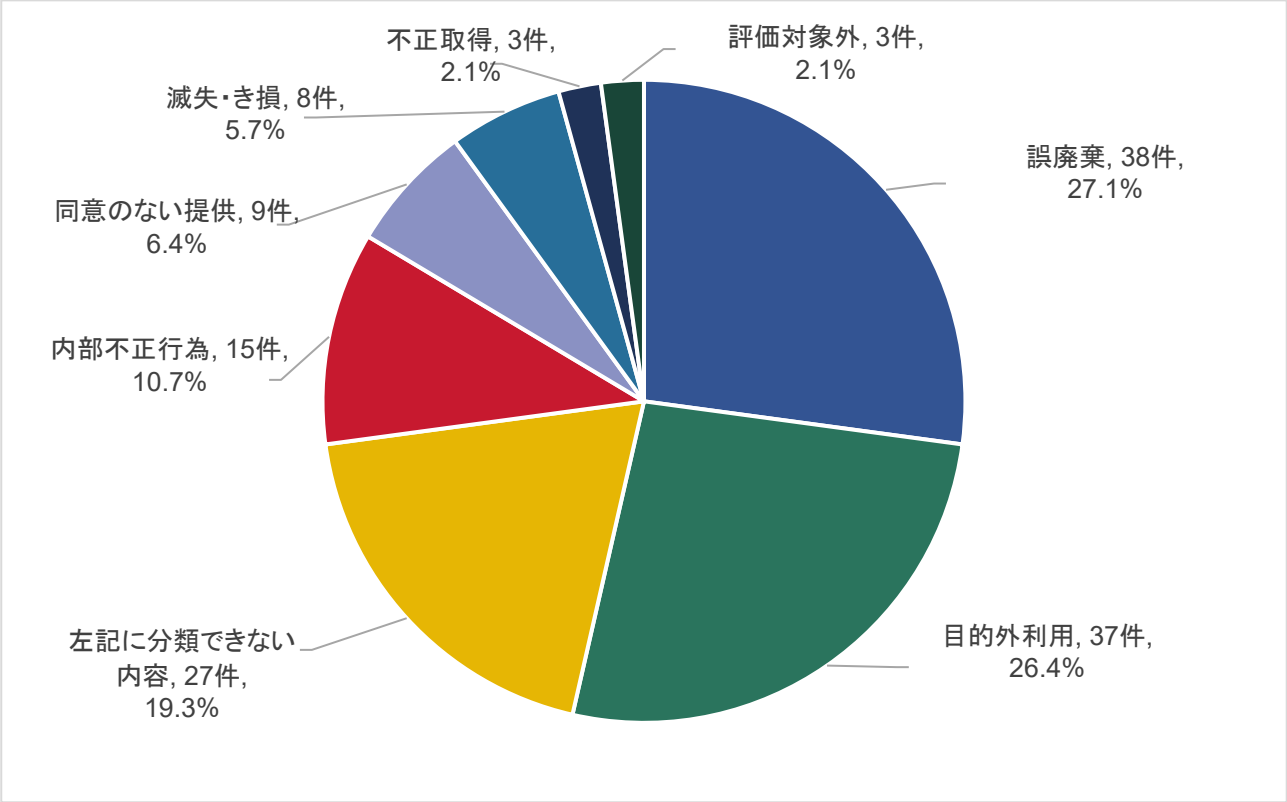


図 7： 原因別事故報告件数「その他」の内訳

4. 事故の発生傾向とその防止策について

今年度の事故報告書を分析すると、集計を始めた2005年から継続して発生している事例がある一方、「業種・業態」「IT環境」「働き方」などの進化や変化に伴って、「発生事象」「事故の原因」にも変化が見られることがわかります。

今回は特に注意が必要な4つの種類の事例をピックアップしてご紹介するとともに、それらを防止するための情報をお伝えしたいと思います。

（1） ソーシャルエンジニアリング

近年、付与事業者における事故において、「ソーシャルエンジニアリング」と呼ばれる事象の発生件数が増えています。ソーシャルエンジニアリングとは、個人情報等の情報を第三者が情報通信技術を使用せず、人間の心理的な隙や行動のミスを利用して盗み出す事象です。

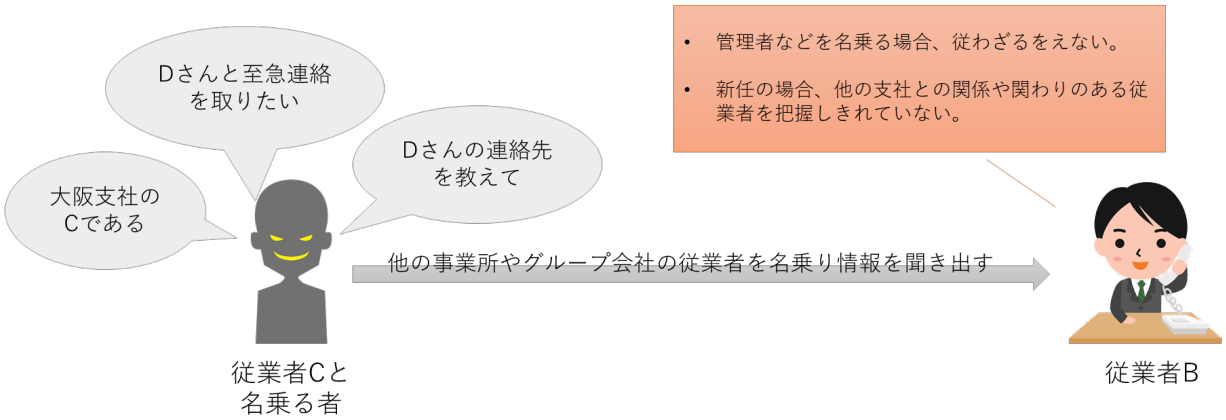
実際に付与事業者における事故としては、以下の事例が報告されています。古典的な手法ではありますが、特定の個人や集団を狙っており、特に注意が必要です。

＜事例①＞

A社は全国に複数の支社を持つ事業者であり、当該事業者の規模や組織体系から、一社員が他の支社の従業者の氏名や所属等を全て把握することは難しい状況にありました。

事故の発生は、東京本社に所属する従業者Bが受けた電話によるものであり、その電話は大阪支社に所属する従業者Cを名乗り、「東京本社のDさんに至急連絡を取りたいため、電話番号を教えて欲しい」という内容でした。従業者Bは従業者Dの緊急連絡先（携帯電話番号）を社員Cと名乗る者に教えました。

後日、従業者Bは従業者Cと名乗る者とのやり取りを従業者Dに伝えたところ、従業者Cと名乗る者から連絡はなく、その後の確認で大阪支社に所属する従業者Cという者は存在しないことが発覚しました。

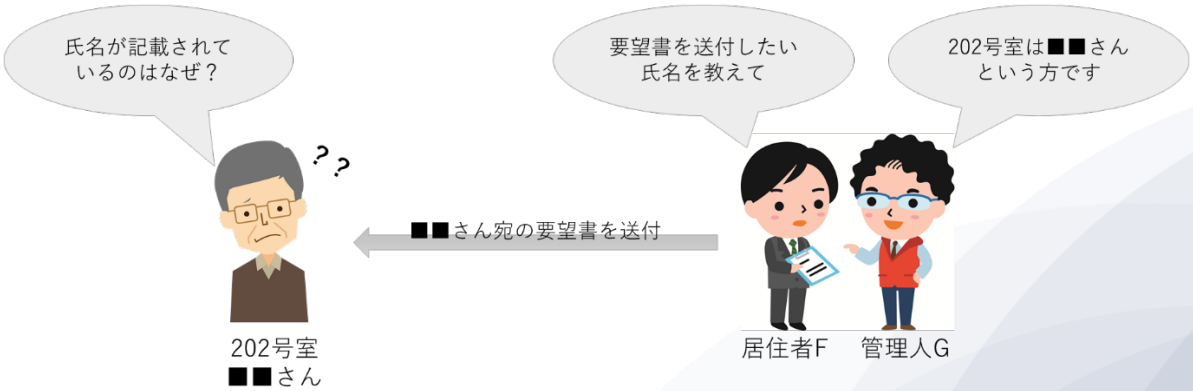


＜事例②＞

E社はマンション管理業務を行う事業者であり、従業者を管理する各マンションに管理人として常駐させていました。

事故の発生は、マンションの居住者Fからの騒音の苦情によるものであり、その苦情及びそれに伴う依頼は「202号室の騒音に日々悩まされており、202号室の居住者に要望書を提出する。要望書の作成にあたり202号室の居住者の氏名を教えて欲しい。」という内容でした。その依頼を受けた管理人Gは居住者Fに202号室の居住者の氏名を教えました。

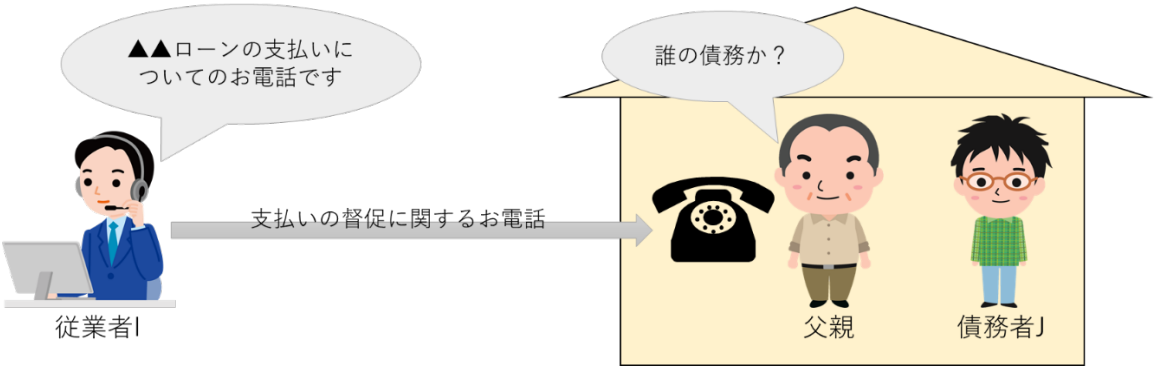
後日、202号室の居住者から「表札やメールボックスに氏名を表示していないが、要望書に氏名が記載されているのはなぜか。」という問合せがE社にあり、その後の確認で上記の事故が発覚しました。



＜事例③＞

H社は債権管理回収業を行う事業者であり、債権回収の通常業務において、H社から債務者に架電し、支払いの督促等を行います。

事故の発生は、H社の従業者Iが債務者Jの自宅に支払いの督促について架電した際、債務者Jの父親が電話を受けたことによるものであり、従業者Iは債務者Jの父親を債務者J本人と誤認し、ローン商品名及び金額を伝えてしまいました。その後、債務者Jの父親から誰の債務であるか問われたことにより、従業者Iは電話の相手が債務者Jではないことに気付き、事故が発覚しました。



＜原因及び対策＞

まず事例①について、事業者の規模や組織体系を利用した典型的なソーシャルエンジニアリングの事故と言えます。また、当該事故では大規模事業者の特性を利用していますが、中小企業においても注意が必要です。例えば、新任の従業者が電話を受け、他の部門の上司を名乗る者から当該事故のような依頼を受けた場合、心理的に断ることが難しいことも想定されます。そのため、当該事故への事業者の対策としては、『個人情報の取扱いの局面ごとの本人確認ルールの策定及び運用』が必要とされます。例えば、当該事故のような電話での個人情報の取扱いの場合、本人しか知り得ない情報（従業者番号、顧客番号、申込番号等）を提示いただき、本人であることを確認することが考えられます。ただし、上記の対策は知識情報（氏名、生年月日、識別番号等）のみによる本人確認であるため、悪意のある者が事前に知識情報を得ている場合、十分な対策とは言えない可能性があります。

付与事業者におきましては、局面ごとに個人情報の取扱いにおけるリスクを分析し、その結果に基づき本人確認ルールを策定し運用する、又は取扱う個人情報を限定する等の対応が求められます。

次に事例②について、一見すると従業者である管理人Gの軽微な不注意により発生し、また、仮に202号室の居住者が自宅前に表札を出していた場合、事故にもあたらない事例であるとの印象を持つ方が多いと思われます。しかし、居住者Fが管理人Gから聞き出した情報を悪用し、大きな被害に繋がっていた可能性があります。また、管理人Gは居住者F以外の居住者にも同様に個人情報を許可なく提供したり、配送業者や設備管理業者等の居住者以外にも個人の判断で提供したりする可能性もあったと言えます。

そのため、当該事故への事業者の対策としては、『従業者の個人情報の取扱いに関する意識の向上に向けた取組み』が必要となります。例えば、管理人の個人情報の漏えいがきっかけで近隣トラブルとなった事例を周知し、日頃の居住者との業務上の交流において留意するように働きかけることが考えられます。また、当該事故では居住者同士での個人情報を含む要望書のやり取りが行われていましたので、このような個人情報の取扱いに関する事故に発展するおそれのある居住者間の手続きを行わせないことも

考えられます。

最後に事例③について、本事例は事例①と同様に電話での業務における事故であり、原因も同じく本人確認の手続きが不十分であったことと言えます。そのため、今後の対策としても本人確認ルールの策定や実施が必要となります。

なお、本事例で注目していただきたい点は、漏えいした先が同居する本人の父親であるという点です。一見、社内や身内への漏えいと聞くと、本人への影響は小さいように見受けられますが、本人からすると自分に近い人だからこそ知られたくない個人情報である場合があります。その一つの例が本事例であり、また、社内への漏えいの場合では同僚の給与情報などが上記にあたる可能性があります。

そのため、個人情報の取扱いに関するルールを策定する前に実施する「リスク分析」では、上記のような漏えい先によって異なる本人への影響についても十分に理解した上で、実施する必要があると考えられます。

（2） 設定ミスによる誤公開

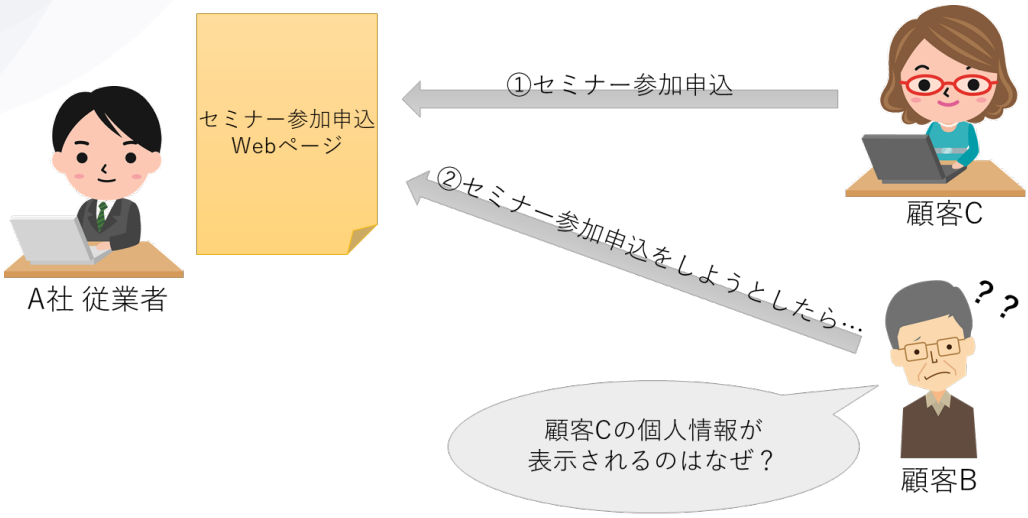
近年、様々な業界において、「電子化」や「ペーパーレス化」が進んでおり、それに伴う個人情報の取扱いに関する手順の策定や抜本的な見直しが必要な時期となっています。また、こうした紙媒体から電子媒体への変化だけではなく、インターネットを介した個人データの取扱いなどによる、これまで存在しなかった新たなリスクへの対策が必要となっています。

ここでは、インターネットを介した個人データの取扱いにおける留意点を実際に付与事業者で発生した事例を参照しながら説明します。

＜事例①＞

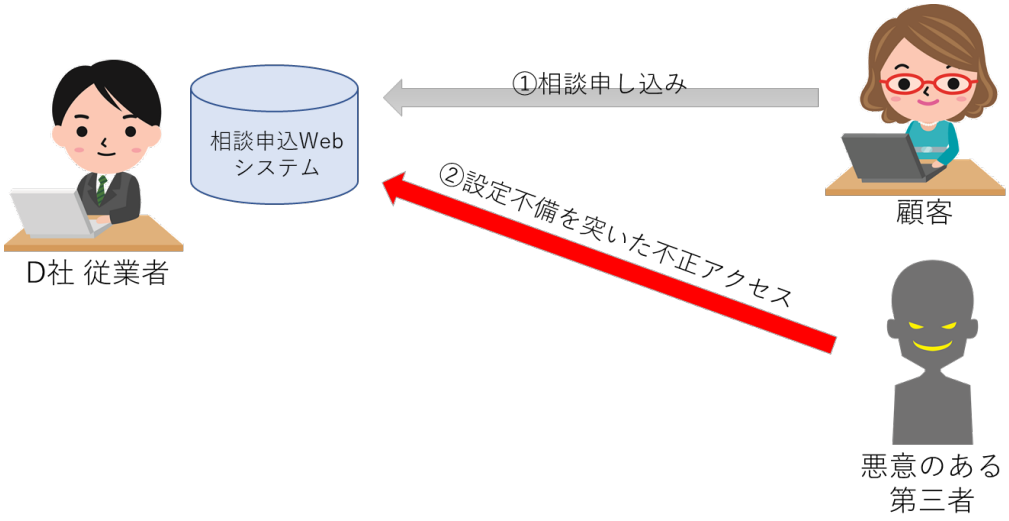
A社は顧客から個人情報を取得する際、インターネット上の無償で簡単に使えるサービスを提供しているサイトを利用し、A社主催のセミナー参加申込Webページを作成しています。セミナー参加希望者はインターネットを介して、セミナー参加申込Webページにアクセスして、「氏名」、「住所」、「電話番号」を入力します。A社は参加希望者が入力した個人情報を一覧として管理し、参加希望者は他の参加希望者が入力した個人情報を閲覧できないよう設定するルールとなっていました。

顧客BがA社のセミナー参加申込Webページにアクセスした際、顧客Cの個人情報が表示されたことで事故が発覚しました。本来、他の人の情報を閲覧できないようにするはずでしたが、作業者のミスにより公開設定となっていたため発生しました。顧客BがA社に本事例について問合せを行い、はじめて事故に気づいた事例です。



＜事例②＞

D社は顧客が入力した個人情報を相談申込Webシステムの個人情報データベース上で管理し、権限を持つ者のみが当該データにアクセスできるよう設定していました。しかし、社外の不特定のユーザに対しても当該データの閲覧の権限が設定されてしまっていることに気づきませんでした。事故の発生は、この権限設定の不備をついて社外の第三者が当該データへアクセス（閲覧）したことによる個人データの漏えい事故となります。



＜原因及び対策＞

まず事例①について、A社は無償で使えるサービスを利用して、セミナー参加申込Webページを作成し、セミナー参加希望者から個人情報を取得していました。なお、昨今では専門的な知識を持たずとも簡便にイベント参加申込Webページやアンケートページを作成することができるツールが登場しています。また、このようなツールは無償もしくは利用料も安価であることが多く、利用に伴う事業者内の手続きも簡素化されている場合もあります。こうした事業者の利用状況から、知らず知らずのうちに「個人情報保護の意識」や「セキュリティへの配慮」が薄れ、システム設定の不備による漏えい事故が発生したと思われます。

そのため、当該事故への事業者の対策としては、『新たなサービス等を利用する際、個人情報の取扱い並びにセキュリティ設定に関する検討・確認ルールの策定及び運用』が必要となります。例えば、新た

なサービスを利用する際の選定においては、「①サービス上で取扱う個人情報の特定」、「②特定した個人情報の保護に必要なサービス要件の設定」、「③設定したサービス要件を満たすサービスを選定」等の手順が考えられます。その他にも、試験運用を行うことや、運用開始前の確認項目及び手順の策定等の対策も検討する必要があります。

特に個人情報を取扱うサービスの選定においては、「有名なサービスだから」や「他社でも利用しているから」といった理由ではなく、サービスの特徴や機能を理解したうえで適切なリスク分析を行い、自社のPMS（個人情報保護マネジメントシステム（Personal Information Protection Management Systems））に沿った選定や運用が必要となります。

次に事例②です。昨今、クラウド上に展開されている顧客管理プラットフォーム上に、事業者がサービスを構築して運用しているケースが増えています。こうしたプラットフォームを提供する事業者（以下、「プラットフォーマー」といいます）は、提供しているプラットフォームサービスのセキュリティや利便性の強化のために、随時機能改善のアップデートを行っています。

事例②の直接的な原因は、アクセス権限の設定不備であり、設定及び確認の手順を策定し、実施することが対策として必要となります。ただし、根本的な原因は利用サービスに関する最新情報を収集し適切に理解できていなかったことであったことから、プラットフォーマーが提供するセキュリティガイド等の情報を深く理解し、内部ユーザ・外部ユーザにかかわらずデータへのアクセス権限の設定を正しく設計し、定期的に見直すことが重要となります。クラウド上のプラットフォームを利用する際は、プラットフォーマーからの情報提供を確実に受領し、セキュリティの強化を継続的に行う必要があります。

（3）ランサムウェア

不正アクセスのターゲットとなるのは大企業だけと思いがちですが、ランサムウェアに関しては中小企業での被害も多く、業種業態や規模の大小に関わらず、事故報告が増えており、全ての企業にとっての脅威となっています。

2021年2月には警視庁から注意喚起もされています[4]。また、ランサムウェアによる被害は、IPAの「情報セキュリティ10大脅威　2021」でも組織の項目で1位となっています（2020では5位）[5]。

＜ランサムウェアとは？＞

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、攻撃者が身代金の獲得を目的に開発されたマルウェアのことです。感染したパソコンになんらかの制限をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムのことをランサムウェアと呼びます。パソコンに保存されているファイルを暗号化し、元の状態に戻すことと引き換えに金銭を要求するタイプのランサムウェアが主流でしたが、近年、不正なツールが多く作成されており、ネットワークを介して攻撃パケットを送出することで感染拡大を図るタイプが急増しています。海外を中心に工場やプラントの操業が止まるケースや、医療機関へのランサムウェアによる攻撃などもあり、パソコン1台に限定されず、社会へ大きく影響を及ぼす事例が発生しています。世界的にみても被害の拡大傾向であり、最近は、特定の企業を標的にしたケースも増えています。

ここでは、会社のファイルサーバがランサムウェアの被害に合ったケースを説明します。

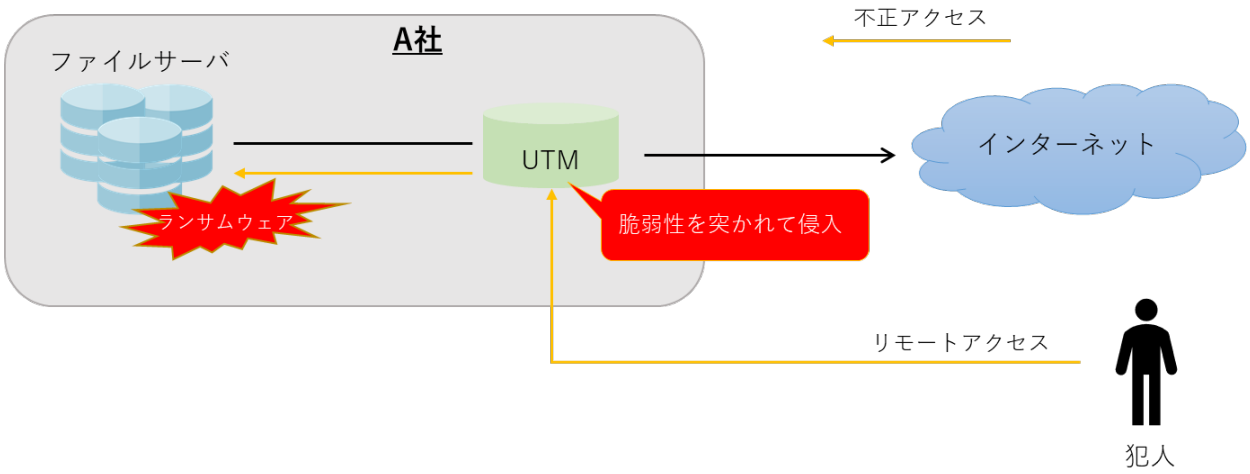
---

4 https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/ransomware.html
5 https://www.ipa.go.jp/security/vuln/10threats2021.html

＜事例＞

A社は社員専用の社内ファイルサーバを用意し、社員の多くが様々なファイルをおいて利用していました。今まではリモートアクセス用の設定はしていませんでしたが、新型コロナウイルス感染症の影響もあり、リモートワークも増えたため、リモートアクセスできるUTM（統合脅威管理(Unified Threat Management)）を経由して、外部からでもアクセスできる運用を開始しました。

ところが、そのUTMに脆弱性があり、リモートアクセスの経路で不正に社内に侵入され、ファイルサーバがランサムウェアの被害にあいました。ファイルサーバ内には、ファイルを戻したければ、身代金を払えという要求が書かれたファイルが残されていました。



＜事例の説明＞

A社ではUTMの脆弱性を突かれて、社内に侵入されてしまい、ランサムウェアの被害にあってしまいました。UTMベンダーからは脆弱性に対するパッチがリリースされていましたが、A社での確認が漏れており、対応が遅れたことが被害につながりました。

また、ファイルサーバのバックアップデータが古く、最近作ったファイルが全て消えてしまい、業務上大きな問題となりました。取引先の一覧のデータなども入っており、お詫びの対応などで時間がかかりました。

＜一般的な感染経路＞

他の多くのマルウェアと同様に、メールとWebサイトが主体です。Webサイト経由の感染は、不審なURLのクリックに加え、ブラウザのプラグインやアドオンのインストールなどで生じることも多いです。メールを使った感染は、添付ファイルの開封ならびに、メール内のURLクリックが主となります。

＜ランサムウェアによる被害＞

ランサムウェアの被害にあっても、身代金を払わなければ、金銭的被害は発生しないと考える人もいるかもしれませんが、正しい認識ではありません。被害にあった企業の生産性は低下し、事故対応にあたる人員の確保、その時間とコストによる影響が大きいです。また、取得していたバックアップが古い、バックアップがなかったなどのケースでは、元のデータを復元するにも膨大なコストがかかります。実際に、バックアップをとっていなかったために、元の情報を復元することができず、関係各社へ大事な情報が消えて元に戻せないことをお詫びしたケースや、データの再作成に膨大なコストがかかるケースも報告されています。また、取引先からの信用がなくなり、契約破棄となるケースもありました。お客様の会員情報や取引情

報、大事な設計図面のデータがなくなる等の最悪のケースでは、事業継続が困難になることもあります。

フォレンジック調査を行うにしても一般的に数百万円のコストがかかることが多く、調査費用だけでも膨大になります。また、自社だけでなく、パートナー企業、顧客、広く社会全般に大きな影響を及ぼすといっても過言ではありません。

全ての企業において注意が必要で、例外の企業はありません。ECサイトなどの大規模なサーバを運営していないから大丈夫なのではなく、事例にあるような会社内で用いている共有ファイルサーバでの感染報告もあります。たまたまローカルのPCに同じファイルがあった、過去のメールを見返したら添付ファイルについていた等でリカバリすることができるケースもありますが、万が一メールサーバもランサムウェアの被害にあっていた場合は、復旧は困難となります。また、財務会計サーバ、販売管理サーバなどが被害にあったケースなどを想像すると、非常に影響が大きいことがわかると思います。

なお、ランサムウェアは個人データが復元できない場合や、利用できなくなった場合に該当すると思いますが、漏えいの痕跡がなくとも、個人データの滅失又はき損として、個人情報の事故となり、事故報告書の提出が必要です。ご注意ください。

＜対策＞

多くのランサムウェアはOSの脆弱性などをついて、感染を広げます。WindowsなどのOSやブラウザをはじめとするソフトウェアを最新状態に保ち、アンチウィルス等のセキュリティ対策ソフトの導入が基本となります。全ての不正アクセス対策の基礎となりますが、定期的な脆弱性情報の収集、定期的なパッチ適用の継続は不可欠です。

最近は新型コロナウイルス感染症の影響でテレワークも増えており、VPN機器等のリモートアクセス環境の不備をついた侵入も増えているため、今まで以上にこれらの機器に対する注意が必要です。事例にあるように、UTMやVPN機器の不備を突く攻撃で侵入している事故報告もありました。

ランサムウェアの場合、事故後の業務への影響を考えると、バックアップ取得の有無が万が一被害にあった場合の明暗を分けることになります。ただバックアップをとるだけでなく、そのバックアップデータをオフラインで保存することも大切です。なぜなら、同じネットワークセグメントにあるバックアップサーバの場合、同様にランサムウェアに感染するケースも多く、折角のバックアップの意味がなかったというケースも報告されています。さらに、復旧手順の確保も重要です。実際にリカバリまで行うリハーサルをやっておくことが望ましいです。

最もよいのは通常使うデータそのものを暗号化しておくことであり、情報漏えい等の被害を最小限にすることができます。多くのデータ、重要な個人情報などを扱う場合にはぜひ検討して欲しいと思います。ランサムウェアは常に攻撃手法や身代金の要求パターンを変更しており、進化を続けています。実際に身代金を払わないと、取得した情報を小出しに公開されたりするパターンも発生しています。今後、対応策も変わっていく可能性はありますが、現在のビジネスシーンにおいては各種サーバやパソコンを使わないという選択肢はなく、常に情報セキュリティに関する情報収集をして、対策をしていくしかありません。ランサムウェアによる個人情報漏えい事故は、どの企業にも起こりうることです。他人事と思わず、自分事として対応していって欲しいと思います。

（4） 環境変化による事故（新型コロナウイルス感染症対策より）

2020年度は、新型コロナウイルス感染症拡大の中でのスタートとなり、4月7日には、政府が7都府県を対象に第1回の緊急事態宣言を発令し、東京都からは緊急事態措置として不要不急の外出自粛などの要請が行われました。多くの企業、組織で急遽テレワークが導入され、「業務内容」「業務のやり方」「業務環境」などの変更（イレギュラーオペレーション）を余儀なくされる状況となり、多かれ少なかれ、（業務上の）混乱が生じたことは記憶に新しいところです。

そういう中で発生した事故についてご紹介し、思いもよらない状況になった時でも事故を発生させずに業務を行うことができる体制へと強化を図るきっかけとしていただければと思います。

＜イレギュラーオペレーションの状況・環境とリスク要因等＞

通常と異なる状況・環境		可能性として考えられるリスク要因
テレワーク（自宅、シェアオフィス等）	セキュリティ環境	● 職場と比べてセキュリティ対策が不十分
	確認体制・環境	● ルール・手順で定められたチェックを行えない ● 職場よりも小さな画面での作業
	持出資料管理	● 保管場所の確保が難しい ● 保管場所のセキュリティが不十分
	その他	● 緊張感の維持困難（気のゆるみ）
出勤制限（自社・他社）	対応人数の不足	● 一人当たりの業務量増加　⇒　時間的な余裕の欠如 ● ダブルチェック省略
	担当者以外の対応	● 該当の業務に不慣れ
	イレギュラーな業務フロー	● 本来とは異なる暫定フロー
新規ツール導入	機能や設定に関する理解	● 機能について理解不十分なまま、とりあえず使い始めた場合 ● 初期設定未確認の場合
追加業務	イレギュラーオペレーションの要因に対する追加業務の発生	● 緊急事態への対応として、（通常業務に）新たな業務が追加された場合
その他	業務上のコミュニケーションの取り方の変化	● 相談したいタイミングでコンタクトがとれない ● コミュニケーションツールが使いこなせない

＜事故事例＞

ここで、いくつかの事故報告事例をご紹介させていただきますが、これらからは複合的要因により事故が発生する場合が多いことが読みとれます。

	事例	主な発生要因
1	複数社より受託している契約業務において、複数書類をチェックし、それぞれ該当の委託元に送付する際に、A 社分に B 社分も入れて送付してしまった。	● 一次チェック（送付先確認）は、本来紙媒体にて行うが、担当者がテレワークにてPC画面にてチェック。要領が異なり、精度が不十分。 ● 二次チェック（送付先と内容物の一致確認）実施者は当該業務に不慣れ
2	出社規制中に、通常は同じ宛先に対して別々に作業を行っている 2 つの業務の担当者が、協力して	● マニュアルにないイレギュラー処理による事故

	2 つの業務を合わせて送付作業を行った際、誤送付が発生した。	
3	新型コロナウイルス感染症対策で店舗を休業していたため、問合せ対応電話にてそのまま注文受付をしたが、同時に受けた住所変更手続きの一部を失念し、旧住所へ送付してしまった。	● 店舗対応が不可 ● お客様希望による通常（ネット通販）とは異なる対応
4	A 社あてに急ぎの書類を発送する際、誤って B 社あての宛先ラベルを出力し、そのまま封筒に貼付して送付してしまった。	● 新型コロナウイルス感染症対策で郵便局の受付終了時間が早められた（当時）ことにより、十分な準備時間・確認時間を確保できないまま作業 ● 納期延長という選択には思い至らなかった。
5	テレワーク時に委託先へ個人情報記載書類をリモートファックスで送信したところ、誤操作により無関係の宛先複数件にも同時送信してしまった。	● 運用変更に関する見直し不十分（従来は、ファックス使用禁止） ● 不慣れな操作
6	テレワーク中のイベント参加予定者に個別に新型コロナウイルス感染症対策によるイベント中止連絡メールを送信する際に、相手を取り違えて送信してしまった。	● テレワーク中のセルフチェック対応 ● 中止連絡メール送信が続く中での慣れと気の緩み
7	受託している契約業務において、担当者 A がペンディング処理にした案件を、担当者 A の自宅待機中（1 週間）に、担当者 B、C が進めたが、担当者 A 出勤時に確認したところ、関係書類が所在不明となっていた。（担当者 B、C には、処理の記憶がなかった。）誤廃棄を起こしやすい書類の重ね方（コピーが上、原本が下）をしていたため、誤廃棄の可能性が高い。	● 処理をペンディングにする際の書類の管理方法が適切に定められていなかった。 ● 新型コロナウイルス感染症対策によるイレギュラー対応による混乱（引継ぎや連携がうまくいっていない）

＜事故発生防止策＞

セキュリティ確保	● 業務利用PCのセキュリティ対策の確認・徹底
ミスの未然防止	● 各業務における「間違う可能性のある場面とチェックポイント」の洗出し ● チェックの徹底 ➢ イレギュラー処理の場合こそ、チェックが重要 ✧ ダブルチェック、クロスチェック（※） ➢ セルフチェックをせざるを得ない時のコツ ✧ セルフダブルチェックの工夫 指差し確認、声出し確認
物品・書類の管理	● クリーンデスクの徹底 ➢ 職場、自宅ともに業務を行う場所のクリーンデスクを徹底 ● テレワーク時の使用機器・書類等の保管場所設定
便利な機能を正しく活用する	● 新規ツール（機器、システム等）導入時には操作や初期設定の確認を必ず行い、ミスが発生しやすい部分については、そのリスクおよび回避方法について周知
コミュニケーション確保	● 意識的にコミュニケーションをとる
安全確保のための柔軟性	● ルール・手順は状況と目的に合わせて、見直す ● ルール・手順通りにできないからしないのではなく、できることをする

（※）クロスチェック：確認や検証の精度や信頼性を高める手法の一つで、二つ以上の異なる方法や観点、資料などによりチェックを行うこと。

最後に、ルールの見直しの際は、変更箇所とそれに対するリスク分析及び対応策をセットに行いましょう。作業手順（マニュアル・フロー）の整備は必要ですが、最も大事なのは「事故防止の意識が重要」だということです。たとえ、何かの事情で通常通りの作業手順で行うことができなくなったとしても、業務を行う際の事故防止の基本ルール・基本動作が身についていれば、安全に柔軟な対応を行うことができます。意識付けのための一助として、プライバシーマーク制度サイトの以下の社内教育用参考資料も活用していただければ幸いです。

基本編：個人情報管理の重要性
：個人情報の取扱いに関する事故を起こさないために
https://privacymark.jp/system/reference/index.html#tools

5. まとめ

個人情報に関する事故は年々増加しています。その手法も古典的なソーシャルエンジニアリングから攻撃手法も多様化しているランサムウェアまで様々です。取るべき対策は個人情報保護のための計画（Plan）、実行（Do）、評価（Check）、改善（Act）のサイクルを回すことであり、継続的に取り組むしかありません。最近ではニュースでも不正アクセスやランサムウェアの被害が多く報道がされていますので、個人情報や情報セキュリティに関する感度を高めるとともに、定期的なシステムのアップデート、環境に応じたルールの見直しなどをタイムリーに実施していくことが必要です。

なお、2022年4月には改正個人情報保護法が施行されますが、その中で、重大事故発生時の個人情報保護委員会への報告が義務化されます。これに伴い、事故に関する届け出、またその報道などが増えていくことが予想され、世の中の事故への関心が高まることが予想されます。

大きな事故の迅速な報告はもちろんですが、小さな事故でも届け出ることで、PDCAサイクルをきちんと運用することができるようになりますので、事故報告書の提出を恐れずにご対応いただくようよろしくお願いいたします。

データ編

1. 事故報告書を提出した付与事業者数と事故報告件数

「プライバシーマーク付与に関する規約（PMK500）」第5章第11条に基づき、付与事業者から当協会及び審査機関に報告された事故の状況は、以下の通り。

年　度	報告事業者数（事業者）	事故報告件数（件）	有効付与事業者数（事業者）	報告事業者数が有効付与事業者数に占める割合（%）
2016年度	843	2,044	15,297	5.5
2017年度	911	2,399	15,788	5.8
2018年度	912	2,323	16,275	5.6
2019年度	985	2,543	16,477	6.0
2020年度	939	2,644	16,678	5.6

注：1.配送委託先が起因となり不可抗力と判断した事故は含まない。
2.同一の事業者から複数回事故報告書を提出された場合、「報告事業者数」1社としてカウントした。
3.有効付与事業者数とは、各年度末までに付与適格決定を受けた事業者から中止等の事業者を除いた付与事業者数。

2. 付与事業者から報告された原因別事故報告件数と割合

付与事業者からの事故報告件数について、(1)の通り原因別に集計を行った。このうち「その他漏えい」および「その他」と分類した事故報告件数については、それぞれ内訳を集計し、(2)および(3)で示した。

(1) 原因別事故報告件数

原因		漏えい						紛失・盗難			その他	合計
		誤送付					その他漏えい	紛失	盗難			
		宛名間違い等	封入ミス	配達ミス	メール誤送信	FAX誤送信			車上荒し	置き引き等		
2016年度	報告件数	303	274	0	424	136	285	409	9	37	167	2,044
	割合(%)	14.8	13.4	0.0	20.7	6.7	13.9	20.0	0.4	1.8	8.2	100.0
2017年度	報告件数	300	329	0	636	125	363	458	10	25	153	2,399
	割合(%)	12.5	13.7	0.0	26.5	5.2	15.2	19.1	0.4	1.0	6.4	100.0
2018年度	報告件数	346	305	0	586	108	330	478	5	31	134	2,323
	割合(%)	14.9	13.1	0.0	25.2	4.7	14.2	20.6	0.2	1.3	5.8	100.0
2019年度	報告件数	400	329	58	590	136	446	421	5	6	152	2,543
	割合(%)	15.7	12.9	2.3	23.2	5.3	17.5	16.6	0.2	0.2	6.0	100.0
2020年度	報告件数	314	323	137	764	110	454	394	5	3	140	2,644
	割合(%)	11.9	12.2	5.2	28.9	4.2	17.2	14.9	0.2	0.1	5.3	100.0

注:
1.配送委託先が起因となり不可抗力と判断した事故は含まない。
2.「誤送付」のうち「宛名間違い等」は、誤送付の原因となる配送に関係する事務処理上のミス(宛名書き間違い、誤登録・誤入力等)および渡し間違いである。「配達ミス」は、配送を業とする付与事業者自らが配達した際の間違い等である。
3.「その他漏えい」の内訳については、後述の(2)参照。
4.「その他」の内訳については、後述の(3)参照。
5.「割合」は各媒体の「報告件数」を「合計」で割った値。小数点以下第2位を四捨五入して出しているため、合計が100%にならないことがある。

(2) 原因別事故報告件数における「その他漏えい」の内訳

内　容		ウイルス感染	プログラム／システム設計・作業ミス	不正アクセス・不正ログイン	口頭での漏えい	関係者事務処理・作業ミス等	合計
2016年度	報告件数	4	97	57	27	100	285
2017年度	報告件数	6	83	48	35	191	363
2018年度	報告件数	1	55	38	31	205	330
2019年度	報告件数	9	185	66	48	138	446
2020年度	報告件数	29	102	54	37	232	454

注：2019年度までは、「システムのバグ」を分けて集計していたが、件数が少ないことから、今回より「プログラム/システム設計・作業ミス」に含めて集計を行うこととした。

(3)　原因別事故報告件数における「その他」の内訳

内　容		不正取得	目的外利用	同意のない提供	内部不正行為	誤廃棄	滅失・き損	左記に分類できない内容	評価対象外	合計
2016年度	報告件数	3	23	6	7	27	6	66	29	167
2017年度	報告件数	2	18	8	15	30	9	13	58	153
2018年度	報告件数	4	41	6	1	24	8	10	40	134
2019年度	報告件数	2	47	12	8	66	9	3	5	152
2020年度	報告件数	3	37	9	15	38	8	27	3	140

以上