2021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
2022年10月7日

1. はじめに

本資料は、2021年度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12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。

また、ご報告いただいた事故等の中から、いくつかの事例をピックアップし、当協会が考える「原因」や「対策」をお示ししましたので、プライバシーマーク付与事業者の皆さまの対策の検討及び実施にご活用いただければ幸いです。

2. 概要

2021年度の事故等報告件数

1. 2021年度は、1,045社の付与事業者より3,048件の事故報告があり、2020年度と比較すると、報告事業者数、事故報告件数ともに増加となりました。（2020年度：報告事業者数939社、事故報告件数2,644件）

2. 2021年度末時点の付与事業者数に占める事故報告事業者数の割合は6.2%となり、2020年度に比べ増加しています。（2020年度：5.6%）

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」（1,938件：63.6%）が最も多く、次に「その他漏えい」（570件：18.7%）、「紛失」（380件：12.5%）、その他（142件：4.7%）の順となりました。

2. 「誤送付」の内訳では、多い順に見ると、「メール誤送信」（1,128件：37.0%）、「宛名間違い等」（353件：11.6%）、「封入ミス」（333件：10.9%）となりました。「メール誤送信」が2020年度よりも約1.5倍（764件→1,128件）に増加しています。なお、「メール誤送信」の分類には、SMSやメッセージアプリ等による誤送信を含めています。

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、2021年度は2020年度より減少（232件→150件）しました。また、「プログラム/システム設計・作業ミス[1]」が2020年度から約2.5倍増加（102件→250件）となり、「不正アクセス・不正ログイン」についても、約2.3倍と大幅に増加（54件→125件）し、リスク分析、技術的安全管理措置が不十分なことが原因の事故等が増加傾向にあります。

4. 「その他」の内訳では、「目的外利用」が増加（37件→50件）しました。

5. 2021年度は、2020年度に続き新型コロナウイルス感染症対策のための「テレワークの実施」「新たなコミュニケーションツールの利用」など、業務環境の変化による影響が事故報告の内容に見られました。

3. 全般的な状況

（1）事故報告の状況

2021年度の付与事業者から当協会及び審査機関にご報告いただいた事故報告の状況は、報告事業者数が1,045社、報告件数が3,048件となり、前年度と比較すると、報告事業者数と報告件数ともに増加となりました。特に報告件数については、2019年度から2020年度の増加率が約4%だったのに対し、2021年度は2020年度の約15.3%と大幅な増加となりました。

各年度の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5.6%から6.2%に増加しています。[2] [3]

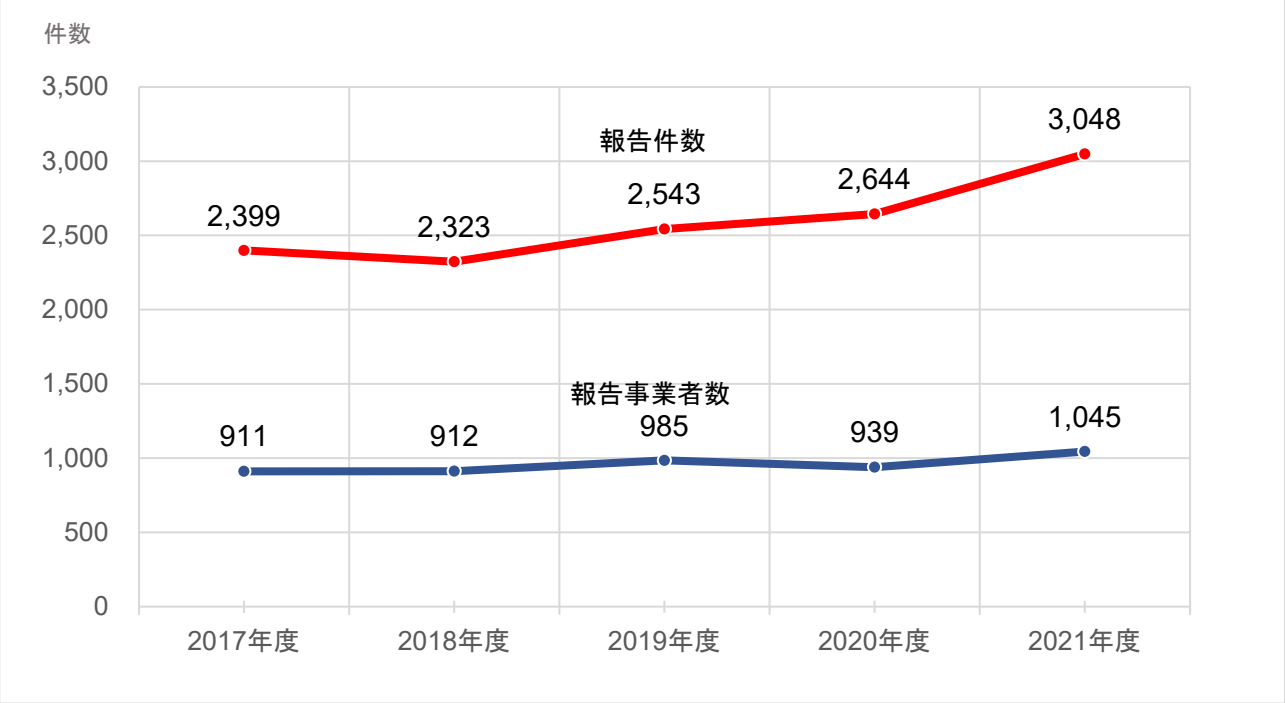


図 1：事故報告の状況

[1] 2020 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ご報告いただいた事故報告を発生原因別にみると、前年度に続き「誤送付」が1,938件（63.6%）と最も多く、次に「その他漏えい」570件（18.7%）、「紛失」380件（12.5%）、「その他」142件（4.7%）の順となりました。前年比では、「盗難」による事故が2.25倍（8件→18件）と最も増加し、「紛失」及び「盗難」の対象となった媒体としては、スマートフォンやノートPCが半数近くとなりました。

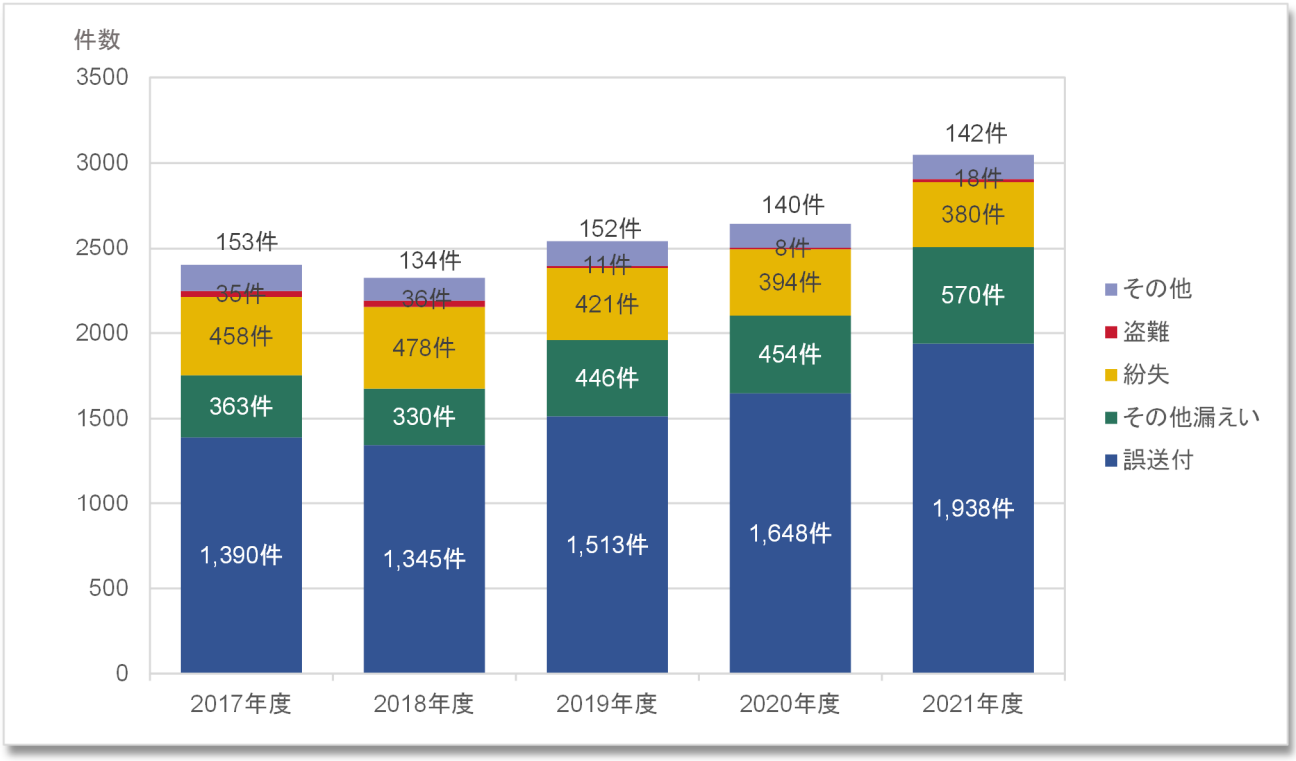


図 2: 原因別に見た事故報告件数の状況

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」」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1,128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「宛名間違い等」で353件でした。

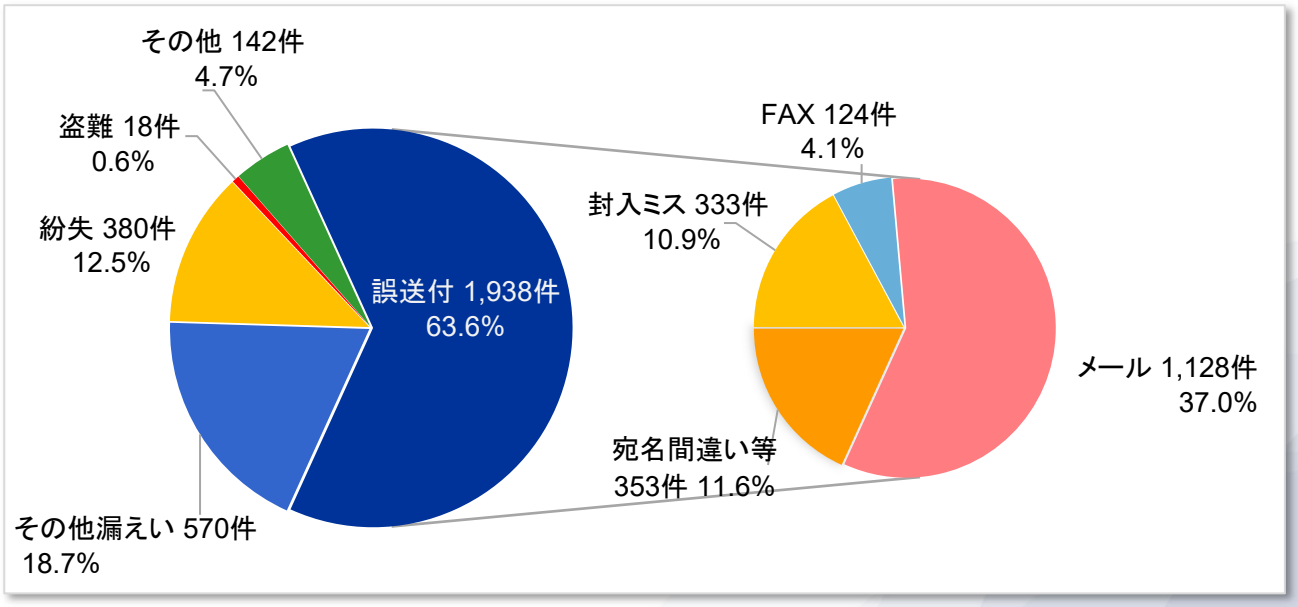


図 3: 2021年度原因別事故報告件数「誤送付」の内訳

過去5年間の「誤送付」の原因別件数の推移をみると、「メール誤送信」は2021年度が最も高くなっています。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。

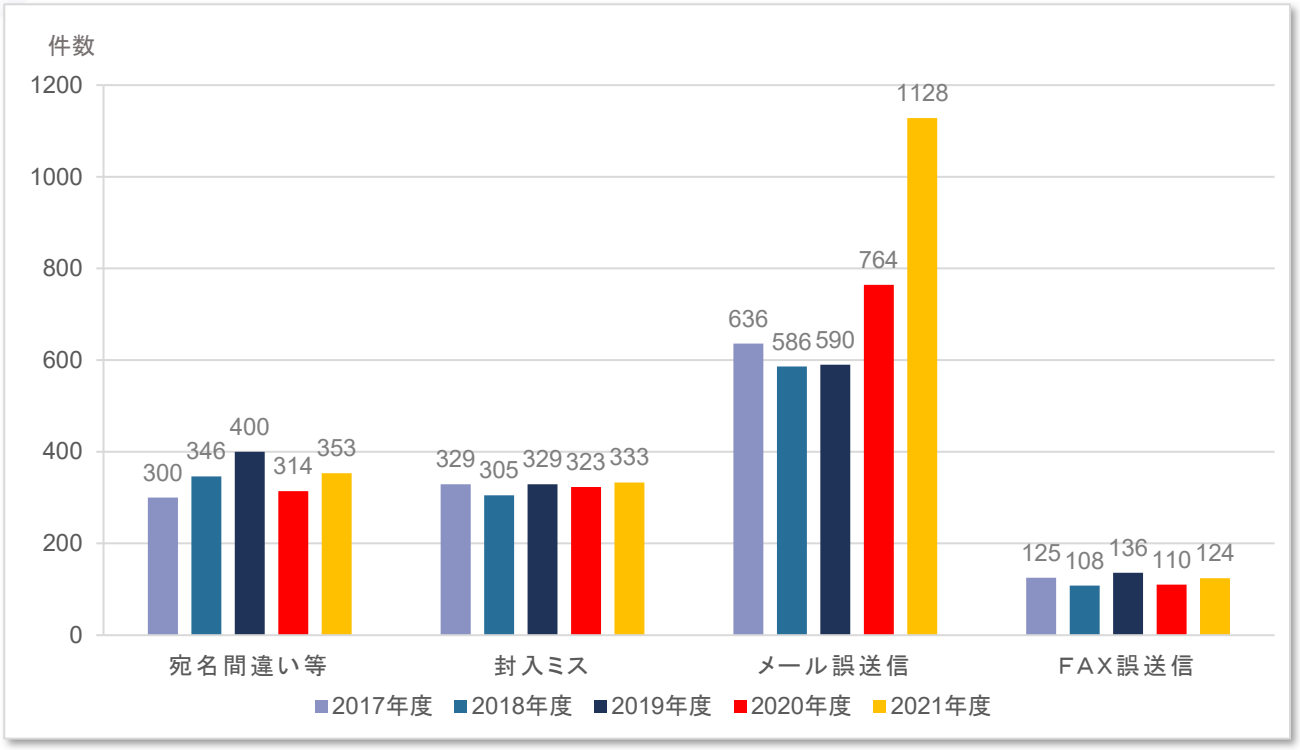


図 4: 原因別事故報告件数「誤送付」の内訳推移

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アプリ等の「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勤務形態の変化の影響が集計から読み取れます。

図2の「その他漏えい」(570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。

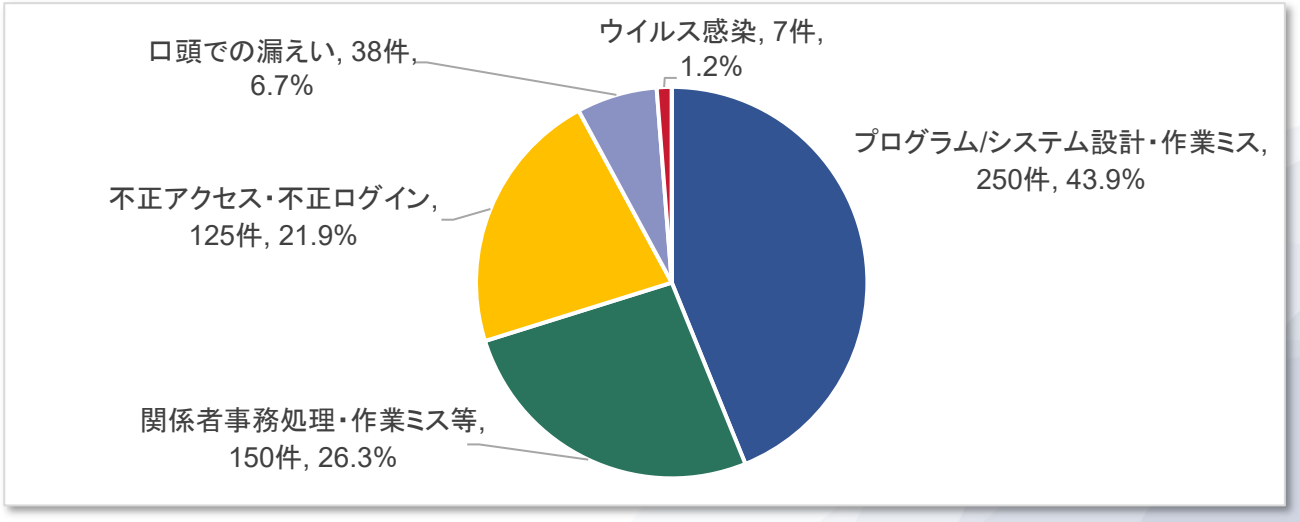


図 5: 原因別事故報告件数「その他漏えい」の内訳

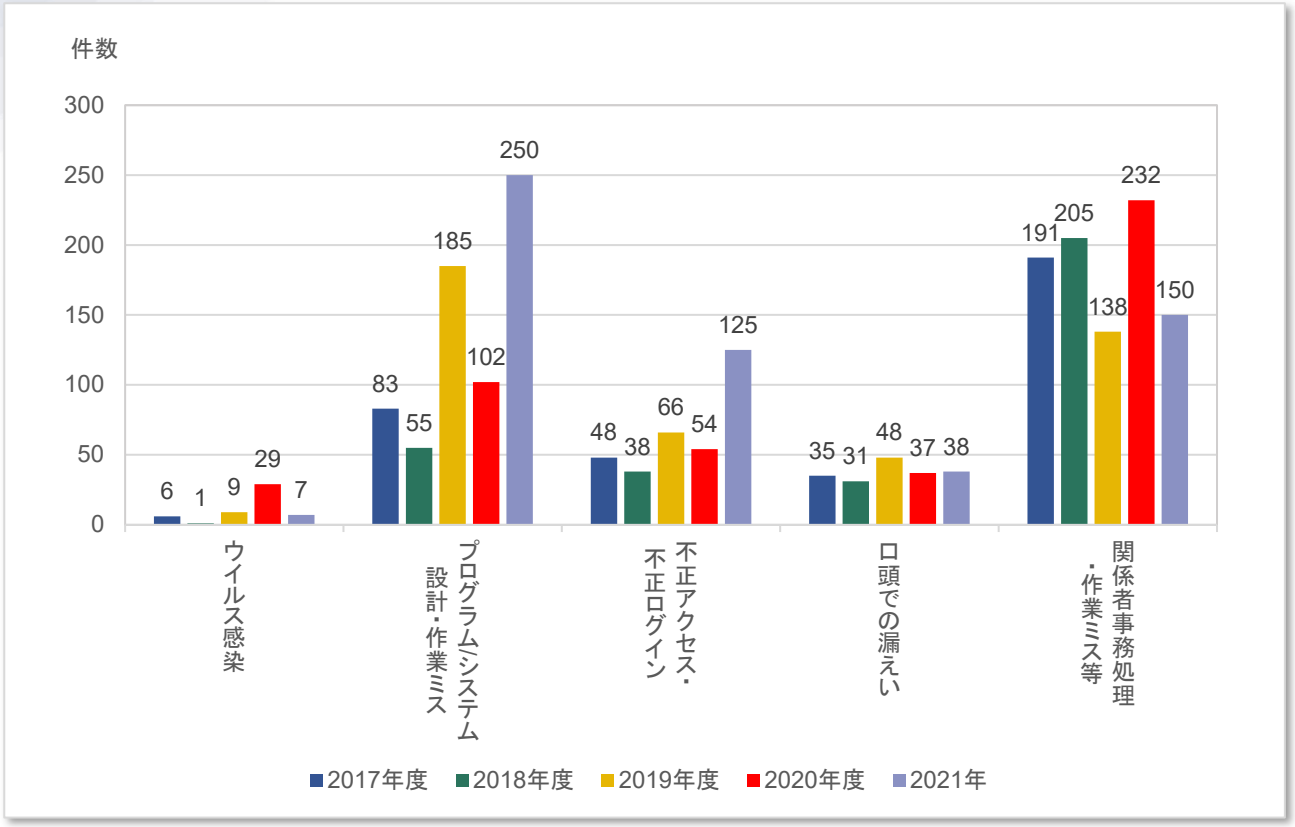


図 6: 原因別事故報告件数「その他漏えい」の内訳推移

過去5年間の「その他漏えい」の内訳件数の推移をみると、図6の通り、「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）」は、これまでに比べて大きく増加しており、新型コロナウイルス感染症対策のために、テレワーク等によりいつもと作業や手順が異なることや手順・ルールの未策定により、発生したと読み取れます。また、「不正アクセス・不正ログイン」が増加した背景には、2021年に開催された東京オリンピック・パラリンピックを目標とした攻撃が要因にあると推測します。

漏えい以外の事故である「その他」（142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」となります。

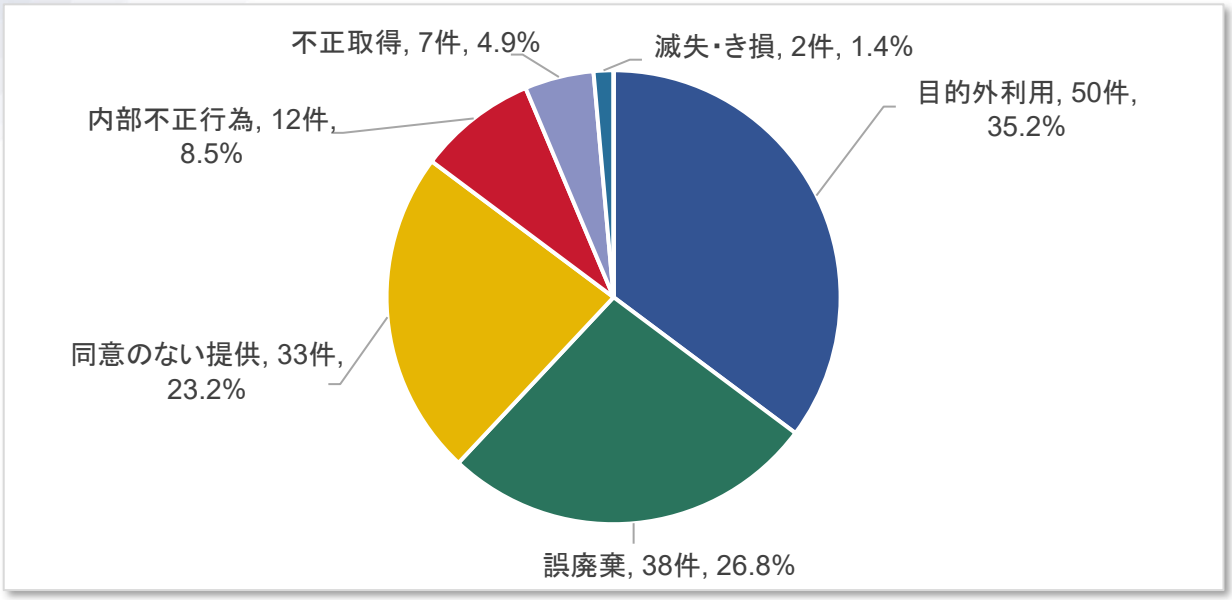


図 7: 原因別事故報告件数「その他」の内訳

4. 事故等の発生傾向とその防止策について

2021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、「社会環境」「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分かります。

今回は2021年度にご報告いただいた事故等の中から、特徴的な5つの種類の事例をピックアップしてご紹介します。事故等の特徴から事故の原因をご理解いただき、安全管理措置の検討や見直し、実施にお役立ていただけると幸いです。

(1) メッセージアプリ・SNSにおける誤送信

1990年代以前の電子的な連絡及び情報伝達の方法は、電話やFAX、電子メール(eメール)が中心でしたが、2000年代以降は新たにメッセージアプリやSNS(ソーシャルネットワーキングサービス)でのコミュニケーションが生活に広く浸透し、現在の我々の生活に必要不可欠なものとなりました。また、その利用範囲はビジネスシーンにも広がり、組織内外を問わず、様々な場面で利用されています。

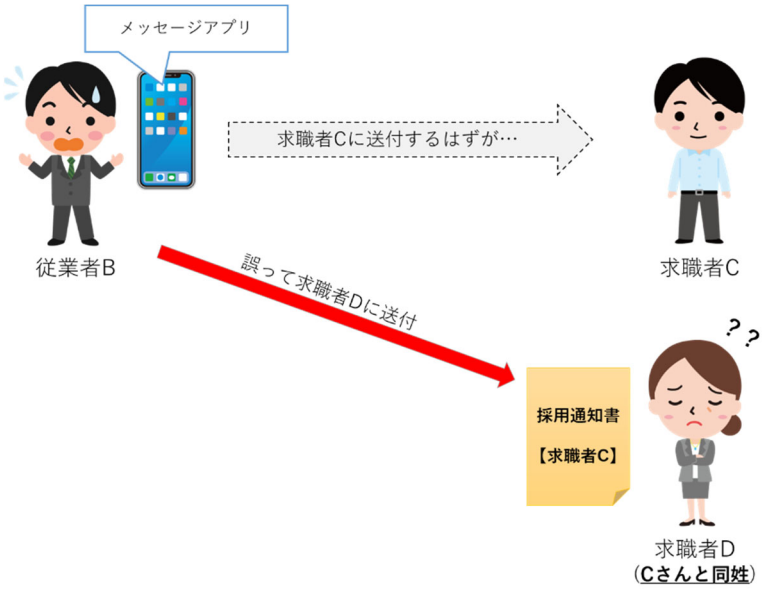
しかし、その急速な普及に伴い、事業者におけるメッセージアプリやSNSの利用に伴う事故件数も増加しています。ここでは、実際の事例にもとづき、その原因と対策を考えていきます。

＜事例＞

A社は、2021年4月から自社の採用活動において、求職者との連絡及び電子ファイルのやり取りをスマートフォン用メッセージアプリにて行っていました。1回の採用活動における求職者数は約50名で、求職者にメッセージや電子ファイルを送信する際は、担当者が求職者の氏名(姓・名)を選択し、メッセージや電子ファイルの送信を行っていました。

こうした中で、2021年5月にA社の担当者Bが、求職者Cに採用通知書を送信する際、送信先を誤って選択し、求職者Cと同じ姓の不採用者の求職者Dに送信してしまいました。採用通知書を受信した求職者Dは、採用通知書の宛名が自身の氏名ではなかったためA社に連絡し、A社において調査した結果、誤送

信していたことが発覚しました。



＜原因＞

直接的な原因は、担当者Bが送信先の選択において、氏名の姓のみで判断してしまった点ですが、担当者BのミスはA社における根本的な原因に起因するものではないかと想定されます。

① 手順書の策定

A社は、2021年4月から自社の採用活動におけるメッセージアプリの利用を開始しました。そのため、事故発生時点では運用ルールを十分に手順書や業務マニュアルに落とし込めていなかったことが原因の可能性があります。

② リスクに対する認識

新たなツールによる個人情報の取扱いにおいては、従業者におけるルールの理解度や日々の利用による習熟度が上がらないと、ミスを起こしやすくなります。

＜対策＞

上記の＜原因＞に記載した、想定される根本的な原因に対し、それぞれ必要となる対策を考えていきます。

① 手順書の策定

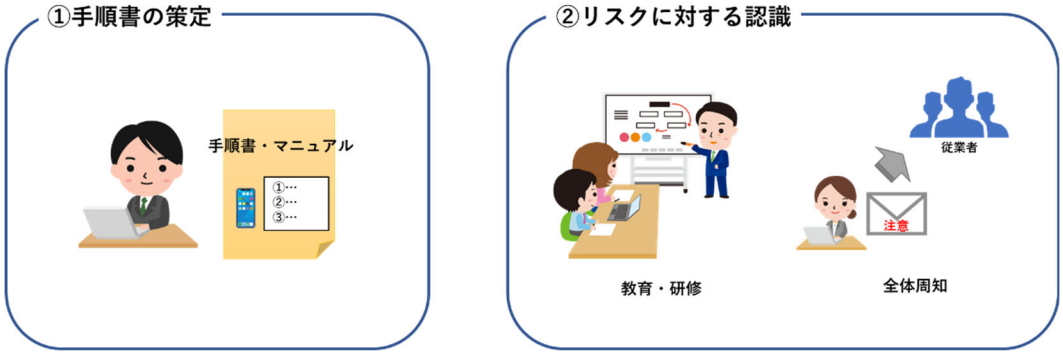
今回のような新たにツールを利用する場合や業務手順が変更となる場合は、業務の実施におけるリスクを踏まえ、組織体制及び担当者の力量に適する手順書やマニュアルを業務の実施前に策定する必要があります。また、策定時のポイントの一つに、「手順書等の種類の選択」があります。例えば、業務の細かな手順や方法を担当者にて判断することが求められる場合は、フローチャートで示したり、担当者が不慣れな操作画面による作業が求められる場合は、操作画面のスクリーンショットを付けた画像付きマニュアルにしたりすることで、担当者が適切に作業を実施することができると考えます。

② リスクに対する認識

上記のA社のように従業者が業務においてメッセージアプリを利用する際、取扱う情報の重要度を認識し、従業者一人ひとりが十分に留意した上で、利用しなくてはなりません。

従って、ツールの利用開始当初は、従業者へのルールの周知や運用の確認頻度を上げることも対策としては有効であると考えます。また、従業者がヒヤリハットした事象を収集して、他の従業者への情報共有を行うことで、組織全体としてのリスクに対する認識を高めることに繋がると考えます。

上記のとおり、メッセージアプリなどの利用により、業務が効率化される一方で、それに伴うリスクを考慮し、手順及びルールの見直しや従業者のルールの理解度向上について、検討することが必要となります。



（2） 業務環境変化に伴う体制構築・手順策定の不備

2022年度も引き続き新型コロナウイルス感染症拡大が続く中、テレワークの導入が進み、多くの企業で働き方が大きく遷移しています。

テレワークの普及に伴い、働く場所の変化、オンラインストレージやクラウドサービス等の外部サービスの利用が急速に進む中、個人情報を含む情報漏えいへの対策が最重要課題となっています。

それでは、実際の付与事業者の事故の事例にもとづき、原因と対策を考えていきます。

＜事例＞

事例①:

A社では、新型コロナウイルス感染症拡大前は、外部へのメール送信時のルールとして、宛先や本文、添付ファイルに間違えがないか出社している複数人でのダブルチェックを実施していました。新型コロナウイルス感染症拡大後は、テレワークが導入され、テレワーク時のメール送信ルールとして、送信前に各自が複数回、本文、宛先、添付ファイルの間違いがないかをチェックするというルールを策定しました。担当者Bは、テレワーク時にメールを送信する際に、このルールに基づき、自身での確認の上、メール送信を行いましたが、メールの宛先が間違っていることに気付かず、別の事業者の担当者に誤送信をしてしまいました。

事例②:

B社では、テレワークで増えたVPN機器等のリモートアクセス環境管理の不備を突かれ、外部からの不正アクセスによりサーバが攻撃されました。ランサムウェア攻撃により、感染したサーバの管理用PCのデスクトップ上に身代金要求の英文が表示されました。

また、感染したサーバ内に保管されていた業務関連のデータファイルの一部が不正に圧縮、暗号化され、復元できないことが判明しました。

事例③:

C社では、他社に書類を送付する際に、宛名ラベルが貼られた封筒に書類の封入間違いがないよう、複数人でダブルチェックを行っていました。新型コロナウイルス感染症対策に伴い、オフィスに出社する人数が制限され、担当者Aは、複数人でのダブルチェックを行うことができず、封入間違いに気付かずB社に送る書類をD社に誤送付してしまいました。

＜原因＞

事例①:

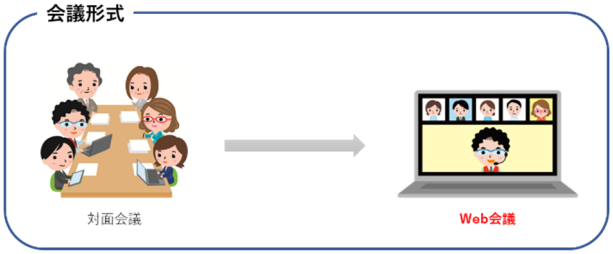
メールの誤送信は、近年最も事故報告件数が多い事象となっています。新型コロナウイルス感染症の影響により、出社人数が制限されたオフィスや店舗で、複数人での送信前のダブルチェックが難しくなったことが背景にあり、これに伴うルールの整備が不十分であったことが原因と考えられます。

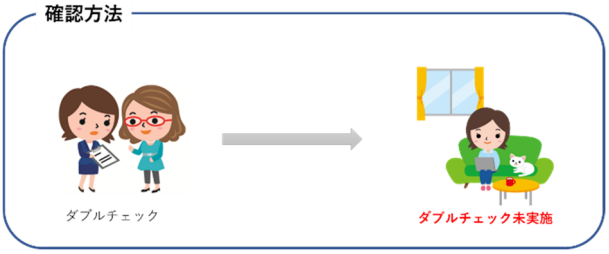
事例②:

今回の事故を誘発した原因は「B社のネットワークには、B社が承認したPCなどの機器以外は接続できない」というルールが徹底されていなかったことにあり、テレワークにより管理外機器の接続が可能になっていたことで、不正に侵入されています。

事例③:

働き方が変化したことで、従来のルールで運用ができなくなることを想定できていなかったことが原因と考えられます。





＜対策＞

事例①:

2021年度の付与事業者の事故報告のうち、メールの誤送信に対する再発防止策では、出社人数が制限されたオフィスや店舗、テレワークの環境下で一人でもチェックができる仕組みを構築するために、誤送信防止ツールを導入する事業者が増加するという変化が見られました。

メールの誤送信については、誰でも起こり得る事故だからこそ、「よくある事故」として起きた事象だけで判断するのではなく、事故が起きた状況や経緯、環境の変化も踏まえ、再発防止策を考える必要があります。

再発防止策は、「組織的安全管理措置」「人的安全管理措置」「物理的安全管理措置」「技術的安全管理措置」の4つの視点を組み合わせることで「必要かつ適切な措置」を講じることができると考えます。

個人情報保護マネジメントシステム（PMS）の観点から、状況の変化に応じた再発防止策の策定や社内ルールや規程を常に見直し、適正な運用と体制を構築し続けることが事業者の信頼獲得に重要となっています。

［4つの安全管理措置］

	内容
組織的安全管理措置	安全管理についての従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備・運用し、その実施状況を確認すること。
人的安全管理措置	従業者に対する業務上秘密と指定された個人情報の非開示契約の締結や教育・訓練等を行うこと。
物理的安全管理措置	入退室（館）管理、個人情報の盗難の防止等の物理的な安全管理措置を行うこと。
技術的安全管理措置	個人情報を取扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視、個人情報に対する技術的な安全管理措置を行うこと。

［事故対応に関するPDCA］

	実施事例（例）
P（Plan）	・ リスク分析（事故等の原因の特定） ・ 是正処置、予防処置の計画
D（Do）	・ 情報システム上の安全管理措置 ・ 従業者の作業手順の見直しと徹底 ・ 承認手順や確認手順の見直しと徹底 ・ 改善・変更したルールの文書化（規程化） ・ 改善・変更したルールの従業者への教育 ・ 委託先の監督の見直し（委託契約や実施作業の見直しを含む）
C（Check）	・ 対策の有効性のレビュー（運用の確認、内部監査）
A（Act）	・ レビュー結果に基づく見直し（代表者による見直し）及び必要な指示

事例②:

事業者ごとのテレワークに対する考え方や実施内容は多種多様になってきています。テレワークには、働く場所で分類すると、自宅で働く在宅勤務、移動中や出先で働くモバイル勤務、本拠地以外の施設で働くサテライトオフィス勤務に分けることができます。

［働く場所によるテレワークの種別］

テレワーク種別	想定する働く場所	
在宅勤務	自宅	
モバイル勤務	出張や営業移動中の交通機関や顧客先、カフェ、ホテル、空港のラウンジなど	
サテライトオフィス勤務	専用型	自社や自社グループ専用で利用するサテライトオフィス
	共用型	自社専用ではなく、複数の企業や個人事業主が共用するオフィス（シェアオフィスまたはコワーキングスペース）

オフィス以外で仕事をするということは、セキュリティなどにおけるリスクを洗い出した上で、社内ルールを見直す必要があります。

不特定多数の人が利用する場所では、PCの盗難や覗き見（ショルダーハッキング）、携帯電話やスマートフォンでの会話の盗み聞きなどのソーシャルエンジニアリングによる個人情報の漏えいがリスクとして考えられます。

また、シェアオフィスやコワーキングスペースの導入を検討する際には、1名用の個室型や電話専用ブースの有無、入退室管理、防犯カメラの設置などを導入しているか考慮することも選定の要素となります。また、公衆無線LAN等の不特定の利用者が共有するネットワークの接続を許可するかどうかなどの検討も重要な要素と言えます。

さらに、技術的安全管理措置として、ノートPCに覗き見防止フィルターを貼ること、離席時にパスワード付きスクリーンセーバを起動すること、盗難対策としてPCは肌身離さず持ち歩くこと、万が一PCが盗難、紛失した場合に盗難、紛失したPCをリモート操作でロックできるソフトウェアをインストールことなども必要な対策として挙げられます。

加えて、セキュリティ脅威の動向及び最新ツールに関する情報収集や、導入したツールやシステムの使用時の手順やルールを随時見直すこと、社員に対するeラーニングなどを活用した情報セキュリティ教育の実施なども重要となります。

コロナウイルス感染症対策で暫定的なテレワークを導入した2020年度と、テレワークが浸透し、デジタルトランスフォーメーション（DX）が加速、システムやツールの導入から定着へと状況が変化した2021年度では、大きく状況が変化しています。そのため、個人情報の本人の権利利益を侵害するおそれのあるリスクを特定、リスクの分析・評価を含むプロセス全体を見据えたリスクアセスメント及びリスク対応を改めて行うことが重要となります。

なお、総務省ホームページでは、「テレワークセキュリティガイドライン」を公開している他、日本テレワーク協会作成の「テレワーク関連ツール一覧」「中堅・中小企業におすすめのテレワーク製品一覧」「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」などテレワークに対する情報発信をしておりますので、参考にしていただければと思います。

（参考）

テレワークにおけるセキュリティ確保：総務省

テレワーク導入ガイドライン：日本テレワーク協会
在宅勤務をご検討なら：テレワーク相談センター（厚生労働省委託事業）

事例③：
2022年1月に電子帳簿保存法が改正され、各税法で原則紙での保存が義務づけられている帳簿書類について一定の要件を満たした上で電磁的記録（電子データ）による保存が可能となり、電子化へ追い風となりました。
しかしながら、企業間取引における実務においては、電子化が難しいケースも多くあるかと思います。事故報告書の中では、従来は送付状と請求書を同封していたが、請求書のみを送付するとした封入書類の変更や、宛名ラベルを廃止し、請求書に郵送先や宛名を印字できるようにしたシステムや書式の変更など、再発防止への取り組みが見られました。
また、封入の準備段階で、色分けしたクリアファイルで封入書類を分別し、他の書類が混在しないようにする工夫もみられました。こうした日々の取り組みや工夫が積み重ねとなり、各事業者が誤送付を防止することに取り組んでいます。
事業者によってはシステム導入など大きな変更が難しい場合もありますので、事故の原因を特定し、自社に最適な再発防止策を考えることが重要となります。

（3） 従業者における不正行為

独立行政法人情報処理推進機構（IPA）が公開している「情報セキュリティ10大脅威 2022※」によると、「内部不正による情報漏えい」は、昨年の6位から5位へと順位が上昇しています。
従業者によって持ち出された情報の内容によっては、営業秘密にあたり不正競争防止法に抵触する可能性もあり、この場合、従業者が不正に持ち出したデータの保有者と持ち出したデータを取得した者（転職先等）にも罰則が定められています。その結果、両者ともに社会的な信頼を失ってしまう可能性もあります。そのため、内部不正が引き起こすリスクは、経営課題の1つとして重要視されています。

※ 「情報セキュリティ10大脅威 2022」は、2021年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約150名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

＜事例＞

事例①：
A社で勤務していた従業員Xは、A社を退職して同業種であるB社に転職をしました。従業員XはA社で担当していた取引先担当者の名刺を持ち出し、本人の同意を得ないまま、B社での営業で名刺の個人情報を流用し、メルマガ配信を行いました。

事例②：
C社で勤務する従業員Yは、個人情報を管理する社内システムへの管理画面のログイン権限を持っていませんでした。従業員Yは社内システムへの管理用パスワードを意図せず入手できたことから、不正アクセスを行い、興味本位で社内システムから個人情報を不正にダウンロードしました。

＜原因＞

内部不正行為が起きる要因として、アメリカの組織犯罪研究者であるドナルド・R・クレッシーが「不正のトライアングル理論」を提唱しています。当該理論では、不正は「動機」「機会」「正当化」という3つの要因がそろった時に発生するとされています。

［不正のトライアングルの要素］

要素	内容
動機	不正行為に至るきっかけ （例．処遇への不満、業務ノルマへのプレッシャー、借金がある、残業、ハラスメント、業務上のミスなど）
機会	不正行為を実行可能・容易にする環境 （例．秘密裏に情報へアクセスでき、持ち出し可能な環境、内部統制や監視が機能していない、内部統制や監視を無視できる立場にあることで不正行為の実行が可能な状況にあることなど）
正当化	倫理感の欠如や行動が適切であると正当化する姿勢など、不正行為への抵抗が低い心理状態 （例．やらなければ倒産してしまう、ばれなければいいだろう、自分は評価されるべきだから当然など）

＜対策＞

内部不正行為と聞くと、悪意を持った行為と考える方も多くいるかと思います。しかし実際には、前述の付与事業者の事故の事例にもあるように、悪意を持って行ったものだけではなく、不正行為と知らずに行ったケースも見受けられます。

全ての従業者（正社員、役員、派遣社員、パート・アルバイト等）に対し、日頃から実務内容に関係する内部不正行為の事例を示し、個人情報保護の教育を実施することが防止に繋がると考えられます。

また、従業者の管理監督手法として、退職時の人事手続きで、秘密保持契約（誓約書を含む）を締結することや、不正行為による影響が会社のみならず、自身にも及んでしまうことを周知し、貸与品の返却の管理、アクセス権の解除を確実に行うことも重要です。

内部不正行為を発生させないためには、不正行為を起こすきっかけを作らないことも大切です。人事部門が主体となり、従業者の評価制度を整備することが必要となります。また、従業者が特定の業務を長期間にわたり担当している場合には、適切な人員配置及び定期的な配置転換を行うことが環境面での対策となると言われています。

また相談しやすい環境を整備し、職場の信頼関係に配慮するとともに、業務の支援や上司や同僚との良好なコミュニケーションがとれる環境を推進し、長時間残業の是正や有休が取得しやすい職場作りなど不満がまん延しないよう、風通しのよい職場づくりをすることも内部不正行為を防ぐことに繋がると考えます。

技術的安全管理措置として、内部不正行為が起きないよう、必要な人にのみ個人情報や重要情報へのアクセスを許可すること（Need To Knowの原則）や、承認を受けていない機器の使用制限といった不正な侵入を事前に防止する入口対策をするとともに、万が一内部不正行為が発覚した場合に備え、情報システムにおける出口対策として、社外のアクセス先の限定や操作ログ・証跡の記録により犯人を特定すること、外部に情報を持ち出されないよう対策をすることが重要となっています。

（参考）

情報セキュリティ10大脅威 2022：独立行政法人情報処理推進機構

内部不正の防止には、経営層を含めた組織横断的防御を！！：独立行政法人情報処理推進機構

組織における内部不正防止ガイドライン：独立行政法人情報処理推進機構

（4）Emotet感染

2019年11月末頃から多くのメディアで取り上げられ、広く知れ渡った「Emotet（※）」は、2020年2月上旬以降、大きな動きがありませんでしたが、2020年7月中頃から攻撃活動の再開が確認されました。その後、2021年1月に欧州刑事警察機構（Europol）による大規模な対策が成功したため、Emotetの脅威は去ったかと思われました。しかし、2021年11月から攻撃活動が再開し、多くの被害が発生していると同時にその攻撃手法も多様化しております。

事業者は、Emotetに感染すると、自社で管理する個人情報が漏えいしてしまうことはもちろん、取引先や顧客の情報が漏えい及び不正に利用されてしまうおそれがあります。

※ Emotetは、情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大が試みられています。Emotetへの感染を狙う攻撃メールの中には、正規のメールへの返信を装う手口が使われている場合があります。これは、攻撃対象者（攻撃メールの受信者）が過去にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容等の一部が流用された、あたかもその相手からの返信メールであるかのように見える攻撃メールです。このようなメールは、Emotetに感染してしまった組織から窃取された、正規のメール文面やメールアドレス等の情報が使われていると考えられます。すなわち、Emotetへの感染被害による情報窃取が、他者に対する新たな攻撃メールの材料とされてしまう悪循環が発生しているおそれがあります。

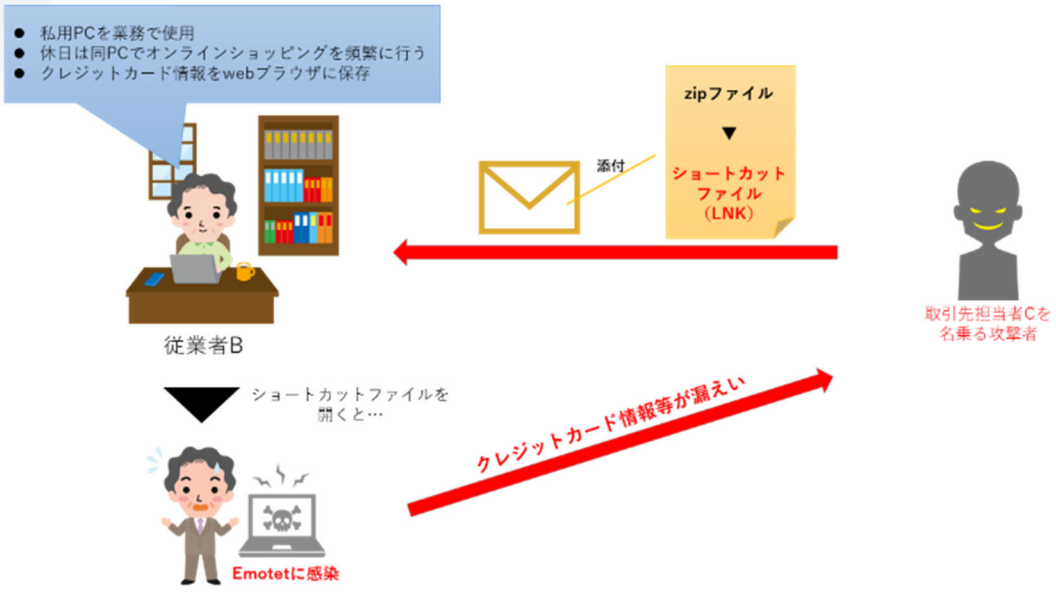
（引用）

「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて：独立行政法人情報処理推進機構

＜事例＞

A社は、全従業者に業務用のPCを配布していますが、セキュリティ要件を満たし、社内承認を受けた私用PCを業務で使用することも認めています。従業者Bは、自宅でも業務を実施できるよう申請を行い、私用PCにて業務を行っていました。また、従業者Bは、休日には私用PCで、オンラインショッピングを頻繁に利用するため、Webブラウザにクレジットカード情報を登録していました。

ある日、従業者Bは、自宅で私用PCにて業務を行っている際、取引先担当者Cを名乗る差出人からのメールを受領し、添付されているzipファイルを解凍、その中に保存されていたファイルをショートカットファイル（LNKファイル）と認識せずに開きました。その結果、従業者Bの私用PCはEmotetに感染し、当該PCに保存されていたメールの連絡先情報及び本文が外部へ漏えいしました。さらに、この感染によって従業者Bの私用PCのWebブラウザに保存されていたクレジットカード情報も外部へ漏えいし、当該クレジットカード情報を攻撃者に不正に利用されてしまいました。



＜原因＞

上記事象の直接的な原因は、従業者Bが不用意に攻撃メールを閲覧し、不正ファイルを開いてしまった点ですが、A社における根本的な原因に起因する事故と想定されます。

① 従業者への教育

A社は、従業者に対して、メールに添付されているファイルを開く上で確認すべきポイントや不審なメールを受信した際の対処方法を十分に教育できていなかったことが想定されます。

② 攻撃メールの検知・対処

A社は、メールシステムにおけるフィルタリングやセキュリティツールによる検知・対処など、各従業者へ到達する前の組織における技術的安全管理措置が不十分であったことが想定されます。

＜対策＞

想定される根本的な原因に対し、それぞれ必要となる対策を考えていきます。

① 従業者への教育

組織は、日々の業務の中に潜むリスク及び注意すべき事項を研修などによって、従業者に認識させる必要があります。A社の事例では、従業者Bは取引先担当者Cを名乗る攻撃者から送られた、不正なプログラムが仕込まれたショートカットファイル（LNKファイル）を開いてしまい、PCがEmotetに感染しました。従業者Bとしては、「差出人」、「メール本文の内容」、「添付ファイル（ファイル名、拡張子など）」から、ファイル開封前に「怪しい」と思うことができた可能性があります。

Emotetの攻撃は巧妙であり、システム上での入口対策が難しくなっていることから、関係各所が発出している注意喚起などから攻撃の特徴などの最新情報を収集し、日々従業者に周知を行うと共に、定期的な訓練を実施することで、従業者の注意力の向上を図ることが必要となります。

② 攻撃メールの検知・対処

上記の「①従業者への教育」で記載したとおり、Emotetの攻撃は巧妙であり、システム上での入口対

策が難しくなっています。その一方で、こうした状況を受けて、Emotetに対するセキュリティソフトがリリースされており、その利用もEmotetに対する有効な手段であると思われます。

Emotetの攻撃手法の一つには、メールに添付されたWord・Excelファイルのマクロを有効にすると、不正プログラムが起動し、操作端末がEmotetに感染するというものがあります。これに対して、セキュリティソフトによって、マクロが埋め込まれているファイルを検知し、マクロを無効化することが可能です。

また、最近の攻撃では、Word・Excelファイルのようなユーザの環境に左右されるファイル形式ではなく、A社の事例のように、ショートカットファイル（LNKファイル）を利用した攻撃手法が確認されています。これに対しては、（ショートカットファイルが格納されている）zipファイル内のファイルの拡張子を確認し、ショートカットファイルをブロックすることもセキュリティソフトによっては可能です。

巧妙な攻撃に対して、セキュリティソフトによる防御機能も向上しているため、セキュリティソフトに関する最新情報を収集し、利用を検討する必要があると考えます。

上記のとおり、事業者はEmotetに関する攻撃手段やセキュリティ対策にかかる最新の情報を収集し、従業者に教育すること、並びに組織としてのセキュリティ対策を実施することが重要となります。

（5）ソフトウェアの脆弱性を突いた不正アクセス

昨今の日本社会における変化について考えた際、まず思い浮かべることとして、「買い物」を挙げる人は少なくないと思います。以前は、欲しい商品がある場合、店舗に行き、現金を支払い、購入するという流れが当たり前でした。しかし、現在はインターネット上で商品を選択し、オンライン決済、商品が自宅へ配達されるといった流れが社会全体に広く普及してきました。この変化の要因は、単なる消費者の購買行動の変化のみではなく、これまで店舗でしか商品販売、サービス提供をしていなかった事業者が、インターネットを介して商品やサービスを提供するようになったことが大きな要因であると考えます。また、それを後押ししたのは、専門知識がない人でも手軽にEC（Electronic Commerce）サイトを構築・運営する手段が生まれ、多様化していることです。

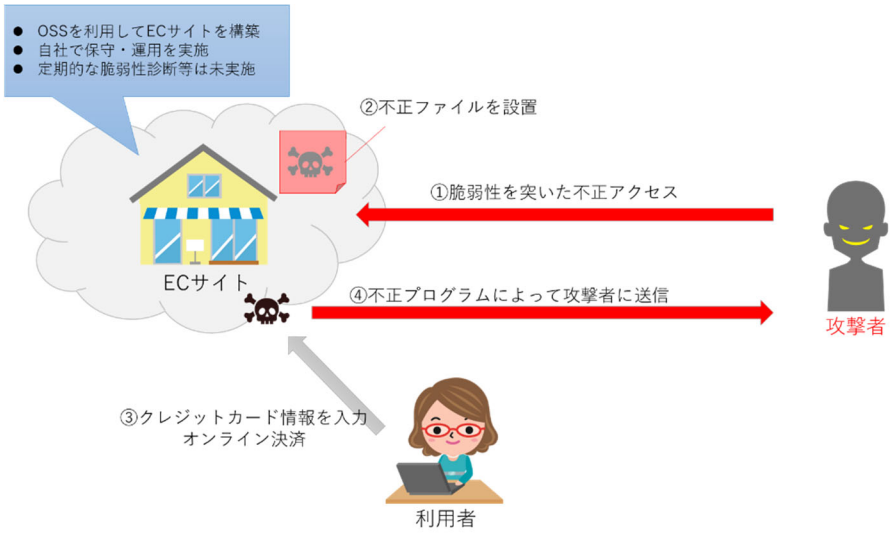
ECサイトの構築方法については、ゼロから構築を行う「スクラッチ開発」、他社が有償で提供するプラットフォームを利用して構築する「パッケージソフトウェア開発」、無償で提供されているソースコードを利用して構築する「オープンソースソフトウェア（OSS）開発」などがあります。2021年度の事故報告では、「OSS開発」で構築されたECサイトに関する事故が多く報告されており、対策が急務となっています。

＜事例＞

A社は、食器を販売する店舗を従業員5名によって営業してきましたが、この度「より多くの人に当社の商品を見て、買って欲しい」という社長の思いから、ECサイトの構築・運営を行うことになりました。社長は導入費用が安価な「OSS開発」によるECサイトの構築を選択し、担当者にITリテラシーが比較的高い、20代の従業者Bを指名しました。従業者Bは初めての業務ながら、2週間でECサイトを構築し、当該ECサイト上でクレジットカードによるオンライン決済も可能としました。なお、オンライン決済に関しては、自社でクレジットカード情報を保有しない、決済代行サービスを利用しました。

ECサイトのオープンから1年後のある日、決済代行サービスを提供する決済代行会社から、「A社のECサイトの利用者のクレジットカード情報が漏えいしている可能性がある」との連絡を受け、当該ECサイトによるオンライン決済を停止し、専門機関によるフォレンジック調査（PCやサーバなどに記録されたログ等から法的な証拠となるデータの収集や分析・解析を行うもの）を依頼しました。調査の結果、攻撃者はA社の

ECサイトの管理画面に不正にログインし、不正ファイルを設置、その後不正ファイルに仕込まれたプログラムを実行させ、クレジットカード情報を保有しないECサイトであるにも関わらず、利用者のクレジットカード情報を盗み出しました。



＜原因＞

直接的な原因は、当該ECサイトにおける脆弱性への対応が十分に実施されていなかったことですが、A社における根本的な原因はいくつか想定されます。

① 構築・運営方法の決定

A社は、ECサイト構築・運営手段の決定において、「導入費用が安価」という理由からOSS開発を選択しています。また、従業者の役割の決定や担当者の選定においても明確な基準に則った決定がなされていません。決定した内容自体に問題があった訳ではなく、リスク分析及び組織の力量の把握等の決定までの一連のプロセスに問題があったと思われます。

② 脆弱性の把握・対応

A社は、ECサイト構築後、当該ECサイトのシステム運用・保守を自社で行っていました。そのため、A社は当該ECサイトに係る脆弱性を把握し、速やかに対応することが必要となりますが、具体的な手順の策定及び実施・確認体制の構築が不十分であったことが想定されます。

＜対策＞

上記の＜原因＞に記載した、想定される根本的な原因に対し、それぞれ必要となる対策を考えていきます。

① 構築・運営方法の決定

本来、ECサイト構築・運営手段及び従業者への役割の割り当ては、取扱う個人情報の重要性並びに組織の力量を踏まえたリスク分析の結果に基づき決定する必要があります。また、オンライン決済機能を持つECサイトは攻撃の標的となりやすく、クレジットカード情報を非保持化していてもA社のように外部へ漏えいする可能性があります。そのため、こうしたリスクに対して必要となるセキュリティ対策な

どが自社内のリソースで実施できない場合は、システム運用・保守を専門業者に委託することが考えられます。しかし、専門業者に委託する場合においても、委託元として以下の点に注意しなくてはなりません。

専門業者への委託する場合の注意すべき点は、「明確に業務内容を指示すること」及び「業務の実施状況を確認すること」です。委託元は契約書（仕様書、発注書を含む）で可能な限り、委託業務内容を明確に記載し、足りない部分は打合せなどで具体的に指示、その記録を保管・共有することが望ましいと考えます。また、指示通りに実施されているかを確認することが必要ですが、専門知識がない委託元の場合は、専門業者による脆弱性診断やペネトレーションテスト（侵入テスト）を行うことも考えられます。

② 脆弱性の把握・対応

当然のことながら、ECサイトを構築・運営する際は、ECサイトに係る脆弱性を把握し、セキュリティパッチを当てたり、ソフトウェアを更新したりすることが必要となります。そのため、事業者はそうした脆弱性に関する情報を収集、対応するための手順の策定及び体制の構築をあらかじめしなくてはなりません。

脆弱性の把握については、例えばOSSの場合、OSS提供事業者のWebサイトやJVN（※）等を定期的に確認することが想定され、定めるルールとしては「誰が」、「いつ」、「何を」確認するかを明確にすることが必要です。また、脆弱性への対応についても組織として十分な検討を行った上で、具体的な実施事項や実施者を決定することが必要であり、そうした決定における手順を明確に定めることが求められます。

上記のとおり、安価で手軽に構築・運営が可能となったECサイトですが、取扱う個人情報等を鑑みた、リスク分析を行い、組織として必要な決定及び対応をしなくてはなりません。また、社会全体のセキュリティ人材の不足も相まって、システムの運用・保守業務が一部の担当者に属人化したり、引継ぎが適切に行われなかったりすることも多く見受けられますので、これらの点においても留意して取り組むことが重要となります。

※ JVN は、"Japan Vulnerability Notes" の略です。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトです。脆弱性関連情報の受付と安全な流通を目的とした「情報セキュリティ早期警戒パートナーシップ」に基いて、2004年7月よりJPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)が共同で運営しています。

（引用）

JVNとは？ JVNとは何ですか？：JPCERT コーディネーションセンター／独立行政法人情報処理推進機構

5. まとめ

2020 年初頭から始まった新型コロナウイルスの感染拡大により、事業者やその従業者は、テレワークによる勤務形態や業務環境の変化を受け、新たなコミュニケーションツールを利用した業務の推進などへの対応を余儀なくされ、それに伴う業務手順の見直しや新たなルールの策定が重要となっています。

また、2021 年度もそうした対応を継続した 1 年だったと思います。こうした中、外出自粛など行動制限を受けた消費者に商品を届けることができる EC サイトの利用が増加傾向にあり、それに伴って、事故も増加しています。EC サイトの決済手段として、クレジットカードを利用する消費者も多くなる一方で、クレジットカード情報を狙った攻撃は後を絶たず、そうした攻撃に対応するように、事業者は決済代行サービスを利用し、自社のシステム内部にクレジットカード情報を保持しない「非保持化」を進め、リスク回避をしてきました。しかし、攻撃者は攻撃手法を変え、利用者が初回登録時にクレジットカード情報を入力したときの情報を入手するなど、事業者の対策に対応してきています。

このように、クレジットカード情報を取扱う Web サイトに対する攻撃手法は、日々刻々と変化してくることから、プライバシーマーク付与事業者におかれましては、最新の関係法令の洗い出しに加え、自社で利用しているソフトウェアの把握、そのソフトウェアに関して専門機関や関係監督官庁が公表している最新の攻撃手法や脆弱性情報の収集に努め、自社のサービスやデータに異常がないか定期的に確認する手順を検討、構築するなど、変化へ対応できるように社内ルールを定期的に見直し、PMS をスパイラルアップすることが重要であることを再度認識いただければと思います。

データ編

6. 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12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、以下の通りです。

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（%）
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
2021年度	1,045	3,048	16,957	6.2

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。

7. 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」及び「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)及び(3)で示します。

(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		
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
2021年度	報告件数	353	333	0	1,128	124	570	380	4	14	142	3,048
	割合(%)	11.6	10.9	0	37.0	4.1	18.7	12.5	0.1	0.5	4.7	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)及び渡し間違いである。「配達ミス」は、2020年度は、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を含んでいたが、2021年度は配送委託先が起因となり不可抗力と判断した事故のみとして集計した。
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
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
2021年度	報告件数	7	250	125	38	150	570

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
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
2021年度	報告件数	7	50	33	12	38	2	―	―	142

以上