Ｐマークニュース

＜２０２２年陽春号＞　Vol. ３９

株式会社トムソンネット　Ｐマークコンサルティンググループ

目 次 と 記 事 概 要

個人情報保護法３年毎見直し改正法が 2020. 6.12 公布され、その後「デジタル社会の形成を図るための関係法律の整備に関する法律案」として、個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の３本の法律を１本の法律に統合することとし、その追加公布は 2021. 5.19、施行は 2022.4. 1 にされています。

それでは、法改正に伴って具体的に何をすべきでしょうか？

最初にホームページ等に掲載している公表事項の改定について解説します。

2020 年に猛威を振るった Emotet は、昨年は概ね沈静化していましたが、今年に入ると、再び勢いを取り戻し、感染しメール送信に悪用される可能性のある.jp メールアドレス数が、2020 年の感染ピーク時の約 5 倍以上という状況になっています。

そこで今回の「事例に学ぶ」では、実際にマルウェア(ウイルスを含む不正ソフト)の一種である「Emotet」(エモテット)に感染した、或いは感染しているかもしれない時の対処について説明していますので、記事をじっくりお読み戴いて、万が一の場合に備えて戴ければと思います。

東京商工リサーチは、日本の上場企業とその子会社における「個人情報漏えい・紛失事故」の集計調査を毎年行っており、今年も年初に昨年の状況に関する調査結果を公表しています。

2021 年の全体の個人情報漏えい・紛失事故件数は 137 件、東京商工リサーチの調査統計としては、調査開始以来（10 年間）で最多となったことが明らかになりました。気になる事故原因ですが、「ウイルス感染・不正アクセス」が全体の約半分を占めており、特に近時の増加傾向が顕著です。

以上

1．改正個人情報保護法は 4 月 1 日からの施行です

―　まず、ホームページなどに掲載している公表事項の改定を　―

個人情報保護法 3 年毎見直し**改正法が** 2020. **6.12 公布され、その後**「デジタル社会の形成を図るための関係法律の整備に関する法律案」として、**個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の 3 本の法律を 1 本の法律に統合**することとしたため、その追加公布は **2021. 5.19、施行は 2022.4. 1** にされています。

（一部 2023.4.1 までの猶予あり） 具体的に何をすべきでしょうか？　最初にホームページ等に掲載している**公表事項の改定**について解説します。

（1）個人情報保護委員会が薦めるチェックポイント

個人情報保護委員会は、そのホームページで「令和 4 年 4 月 1 日改正個人情報保護法対応チェックポイント」と題して下記の 6 点をあげています。

①万が一に備え、漏えい等報告・本人通知の手順を整備しましょう。

②個人データを外国の第三者へ提供しているか確認しましょう。

③安全管理措置を公表する等、本人の知りうる状態に置きましょう。

④保有個人データを棚卸し、開示請求等に備えましょう。

⑤個人情報を不適切に利用していないか確認しましょう。

⑥個人関連情報の利用状況や提供先を確認しましょう。

今回は、事業者で、適用事例が少ないと思われる上記の②④⑥については省略し、①③⑤について、法令に基づきチェックすることとします。

当面、すぐにでも対応を要する③について考えます。

（2）公表すべき事項として、改訂を要する事項とは？

下記の事項があります。(条文番号は 2021.5.9 改正の保護法による表記)

①直接書面以外の方法で取得した個人情報の利用目的について(法 21 条 1 項　ガイドライン通則編 3-1-1)

何を(インプットする情報)何のために(利用目的)を明記することが求められており、その趣旨にあった表記への改定が必要です。

②保有個人データに関する周知について

・保有個人情報を保有している組織の氏名又は名称及び住所並びに法人にあってはその代表者の氏名の追記が必要です。(法 32 条 1 項　ガイドライン通則編 3-8-1)

・保有個人データの利用目的、何を(インプットする情報)何のために(利用目的)を明記することが求められており、その趣旨にあった表記への改定が必要です。(法 32 条 1 項　ガイドライン通則編 3-8-1)

・保有個人情報の安全管理措置についての表記が必要です。(法 32 条 4 項及び政令 8 条　ガイドライン通則編 3-8-1)

・認定個人情報保護団体に加入している場合はその表記が必要です。(法 32 条 4 項及び政令 8 条　ガイドライン通則編 3-8-1)

③開示について

・第三者提供記録を開示対象とすることが必要です。(法 33 条 5 項　ガイドライン通則編 3-8-3)

・開示の方法として、電磁的記録の提供による方法の追加が必要です。(法 33 条 1 項から 4 項　ガイドライン通則編 3-8-2)

④個人情報の共同利用がある場合の表記に、「責任を有する者の氏名又は名称及び住所並びに法人にあってはその代表者の氏名」を追加することが必要です。(法 27 条 5 項　ガイドライン通則編 3-6-3)

⑤インターネットにおける情報収集について（クッキーポリシー）

・「個人関連情報」の制定に関連して、自社 Web サイトで使用している主なクッキー等について、公表することが望ましいと思われます。(直接規定していないが関連するのは、法 31 条　ガイドライン通則編 3-7-1)

（3）公表すべき事項の詳細　保有個人情報の安全管理措置

公表すべき事項の充実は、「改正法に関連する政令・規則等の整備に向けた論点」（公表事項の充実)(令和 2 年 10 月 14 日個人情報保護委員会)における下記の検討結果から法定化されています。

「事業者の保有個人データの取扱いについて、本人がその内容を判断する材料は利用目的のみであり、現行法上、その取扱体制や講じている措置につい把握することは困難。たとえ利用目的が適正なものだとしても、体制整備や措置が不十分な場合は、本人が開示や利用停止等の請求を行う必要がある場合も考えられる。Ex.過去に漏えい事案等を発生させた事業者において、**安全管理措置**が不十分であると判断した本人が、利用停止等を請求する場合、従って事業者の取扱体制や講じている措置を本人が把握できることが必要ではないか」

保有個人情報に関しての安全管理措置について、法規定がやや抽象的でわかりにくいのですが、ガイドライン通則編3-8-1では下記のように解説しています。

【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】

（基本方針の策定）

事例)個人データの適正な取扱いの確保のため、「関係法令・ガイドライン等の遵守」、「質問及び苦情処理の窓口」等についての基本方針を策定

（個人データの取扱いに係る規律の整備）

事例：取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について個人データの取扱規程を策定

（組織的安全管理措置）

事例 1：個人データの取扱いに関する責任者を設置するとともに、個人データを取り扱う従業者及び当該従業者が取り扱う個人データの範囲を明確化し、法や取扱規程に違反している事実又は兆候を把握した場合の責任者への報告連絡体制を整備

事例2：個人データの取扱状況について、定期的に自己点検を実施するとともに、他部署や外部の者による監査を実施

（人的安全管理措置）

事例 1：個人データの取扱いに関する留意事項について、従業者に定期的な研修を実施

事例 2：個人データについての秘密保持に関する事項を就業規則に記載

（物理的安全管理措置）

事例 1：個人データを取り扱う区域において、従業者の入退室管理及び持ち込む機器等の制限を行うとともに、権限を有しない者による個人データの閲覧を防止する措置を実施

事例 2：個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を講じるとともに、事業所内の移動を含め、当該機器、電子媒体等を持ち運ぶ場合、容易に個人データが判明しないよう措置を実施

（技術的安全管理措置）

事例 1：アクセス制御を実施して、担当者及び取り扱う個人情報データベース等の範囲を限定

事例 2：個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入

（外的環境の把握）

事例：個人データを保管している A 国における個人情報の保護に関する制度を把握した上で安全管理措置を実施

【本人の知り得る状態に置くことにより支障を及ぼすおそれがあるものの事例】

事例 1：個人データが記録された機器等の廃棄方法、盗難防止のための管理方法

事例 2：個人データ管理区域の入退室管理方法

事例 3：アクセス制御の範囲、アクセス者の認証手法等事例4）不正アクセス防止措置の内容等

【中小規模事業者）における安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】

（基本方針の策定）

事例：個人データの適正な取扱いの確保のため、「関係法令・ガイドライン等の遵守」、「質問及び苦情処理の窓口」等についての基本方針を策定　（【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】と同様）

（個人データの取扱いに係る規律の整備）

事例：個人データの取得、利用、保存等を行う場合の基本的な取扱方法を整備

（組織的安全管理措置）

事例 1：整備した取扱方法に従って個人データが取り扱われていることを責任者が確認

事例 2：従業者から責任者に対する報告連絡体制を整備

（人的安全管理措置）

事例 1：個人データの取扱いに関する留意事項について、従業者に定期的な研修を実施　（【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】と同様）

事例 2：個人データについての秘密保持に関する事項を就業規則に記載　（【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】と同様）

（物理的安全管理措置）

事例1：個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧できないような措置を実施

事例 2：個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を講じるとともに、事業所内の移動を含め、当該機器、電子媒体等を持ち運ぶ場合、容易に個人データが判明しないよう措置を実施　（【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】と同様）

（技術的安全管理措置）

事例 1：個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止

事例 2：個人データを取り扱う機器を外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入

（外的環境の把握）

事例）個人データを保管している A 国における個人情報の保護に関する制度を把握した上で安全管理措置を実施　（【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】と同様）

（4）改定の具体例について

公表事項は、ホームページに「当社における個人情報の取扱について(公表事項)」などとして掲載している事業者が多いと思いますが、事業者によって、書きぶりは異なっています。

その例示については、弊社担当にご連絡いただければ、ご案内します。大企業の多くが適時に対応しています。事業者が、個人情報の取扱いについて、迅速に対応していることは、顧客の評価につながることでしょう。

２．事例に学ぶ：最恐のマルウェア「Emotet」にかかったかな？という時は

事例シリーズの第 15 弾です。これまでは情報セキュリティの脅威から如何にして防御するかの観点で各種の方策を検討してきましたが、今回は実際にマルウェア（ウイルスを含む不正ソフト）の一種である「Emotet」（エモテット）に感染した、或いは感染しているかもしれない時の対処について検討してみようと思います。

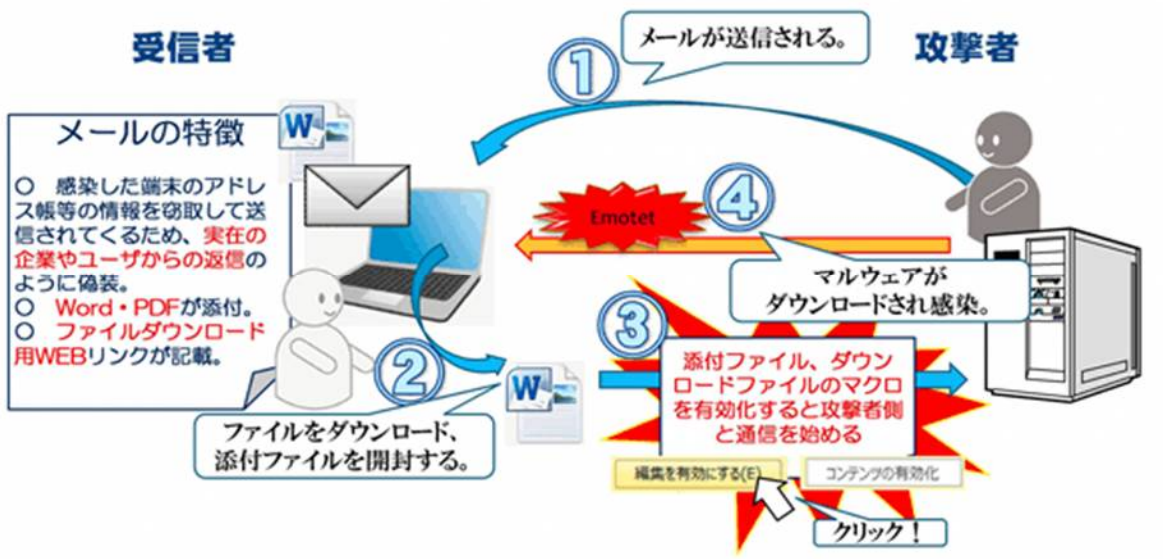
2022 年 4 月 4 日発の「JIPDEC プライバシーマーク推進センターからのお知らせメール」で「◆【注意喚起（再掲）】マルウェア Emotet の感染について」で従業者への周知、注意喚起が促されています。また、「ゴールデンウィークにおける情報セキュリティに関する注意喚起」（2022.4.26IPA 発表）でも Emotet について「不用意に不審なメールの添付ファイルを開かない、また不用意に本文中の URL にアクセスしないよう」等々の警告が公表されています。

一般的な情報セキュリティ対策に混じり、固有名詞を挙げて注意喚起を呼びかけているのは Emotet だけです。

自分にはそんな危険メールが送られて来るはずがないと思い込んでいないでしょうか？数年前の日本年金機構の標的型攻撃でも被害の発端は職員のその感覚でした。

（１）Emotet に感染したらどうなるのか

Emotet をダウンロードしインストールしたとしても、それ自体が悪行を働くことはありませんが「悪の根源」になります。感染した PC は犯人からのリモートアクセスに対して無防備になり、情報流出に加えて他のマルウェアの媒介も行います。一度侵入されれば、ランサムウェアなどの深刻なウイルスを呼び込んだり、社内の全 PC や送信メールによって取引先の PC も感染したりしてしまうため、甚大な被害に発展する危険性があります。

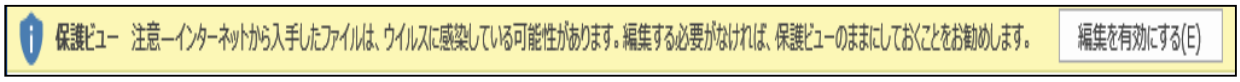


引用：栃木県警 HP

（2）どうしたら感染するのか

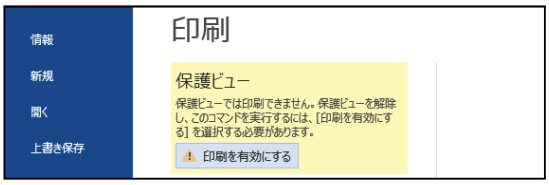
感染ルートは大半がメールです。添付ファイルがマイクロソフトの Office(Word、Excel、Powerpoint)のマクロとして仕込まれ、それを開くと感染します。Zip 圧縮で感染した Office ファイルをオブラートでくるんでいる場合もあります。Zip 圧縮で暗号化したファイルはウイルス対策ソフトで検査ができず、すり抜けることがあるからです。

Emotet は、Office ファイルを開いた際に下の警告が表示された時［**編集を有効にする**］をクリックすることによりインストールされます。



この表示があっても［編集を有効にする］をクリックせず無視した場合には読み取り専用として保護ビューで開かれます。

保護ビューのまま印刷しようとするとそこでも右のような表示が現れ、保護ビューの解除を促されます。ここで解除すると［編集を有効にする］をクリックしたのと同じことになります。



（3）疑わしい時はどうするか

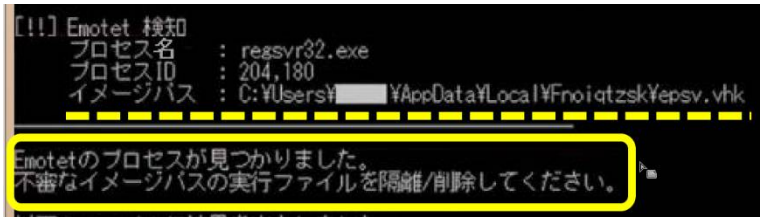
保護ビューを無意識に解除した時が問題です。信頼できるファイルであればいいのですが、少しでも疑いがあった場合は以下の手順で被害を最小限食い止めましょう。この間、状況を残す(保全する)ため **PC の電源を切らないこと（〝状態の保全〟）が重要**です。

①感染した PC を LAN から外す(有線であればケーブルを抜き、無線であれば〝切断〟する)

②情報セキュリティ管理者に連絡する

③「EmoCheck」によるチェックを実行する

※他の PC で JPCERT/CC ページからダウンロードし、当該の PC にコピーして起動



※バージョンアップが行われているため、都度最新版の入手が求められる

EmoCheck は実行中のプロセス名のチェックを行い、図のように「**Emotet のプロセスが見つかりました**」と表示された場合は次項の対処が必要になります。

（4）感染したらどうするか

「コンピュータ緊急対応センター」としての第三者機関・一般社団法人 JPCERT コーディネーションセンター(略称：JPCERT/CC)の HP を参考に、Emotet の感染が判明した際の対処をご紹介します。**最終的には当該の PC を初期化**(工場出荷状態に)することになります。

①Emotet の削除

・タスクマネージャーを開き、EmoCheck 画面で示されたプロセス ID のタスクを強制終了　(別のマルウェア・Trickbot などが見つかった場合にはそれらも同様)

・エクスプローラを開き、イメージパスに示されたフォルダから該当ファイルを削除

②メールパスワードの変更

・メールサーバの管理画面から当該アカウントのパスワードを変更

(当該のアカウントでのメール送信を停止)

③感染した PC が接続していた組織内ネットワーク内の全 PC の調査

・当該 PC が繋がっている LAN に接続している全 PC について EmoCheck の実行

(感染が発見された PC は当初感染した PC と同じく①と②を実行する)

④他のマルウェアの感染有無の確認

・Emotet は別のマルウェアに感染させる機能を持っているため、ウイルス対策ソフトなどで Emotet 以外にも感染していないか調査

(日本では Ursnif、Trickbot、Qbot、ZLoader などの不正送金マルウェア、海外では標的型ランサムウェアの感染などの事例あり)

⑤被害を受ける(攻撃者にメールアドレスが窃取された)可能性のある関係者への注意喚起

・上の調査で確認した対象メール、およびアドレス帳に含まれていたメールアドレスを対象とする

(不正メールがばらまかれた(＝標的型攻撃が現出)としても、感染した PC やメールサーバの送信フォルダに痕跡を残さない方法もあり得る)

⑥感染した PC の初期化

(レジストリに手を加えられていれば、再度に亘って感染の可能性があるため)

(5) まとめ

先に公表された「情報セキュリティ 10 大脅威 2022」には〝Emotet〟の名称が登場しませんが、Emotet は「組織向け脅威」のワーストスリーである「ランサムウェアによる被害」、「標的型攻撃による機密情報の窃取」、「サプライチェーンの弱点を悪用した攻撃」の原因になり得ることから「最恐のマルウェア」と呼ばれています。感染ルートはメール添付ファイルに限らず、採用募集画面の履歴書など **Web サイトの入力フォームからファイルを入手**する場合や、**メール本文に表示された URL をアクセス**するなどもあります。

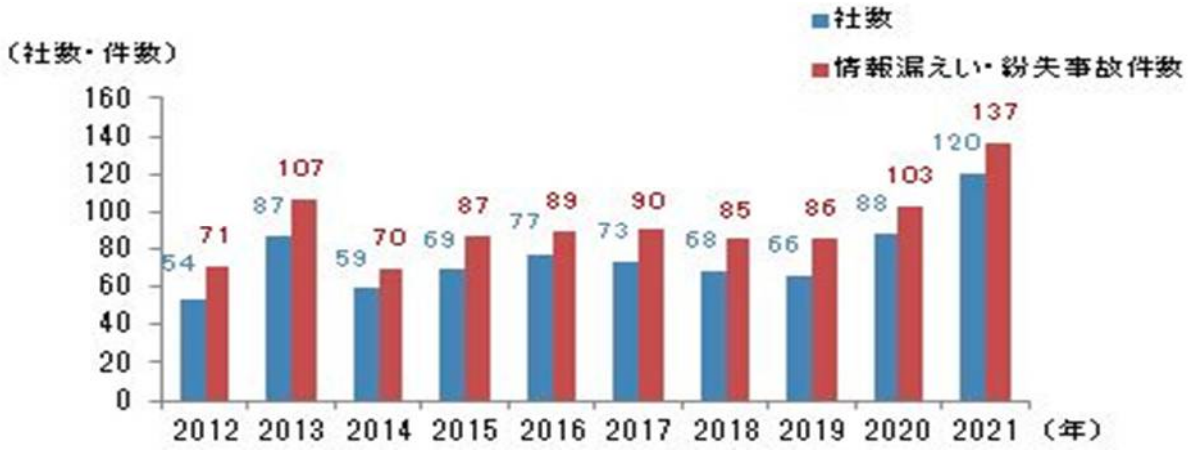
ウイルス対策ソフトには Emotet を検出する機能が含まれていますが、100%の検出は過剰期待です。受信したファイルを開く際には信頼できる場合に限る、やマクロ付きの Office ファイルは開かない等々で予防を図ったとしてもうっかりして Emotet(に限りませんが)をダウンロードしてしまうことがありそうです。その際には適切な対処を採られ、被害を最小限に抑えていただくことを切望します。

３．後を絶たない個人情報漏洩事故（上場企業における 2021 年の実態を探る）

株式会社東京商工リサーチは、上場企業とその子会社における「個人情報漏えい・紛失事故」の集計調査を毎年行っており、今年も昨年（2021 年）の結果を公表しています。

昨年の事故件数は 137 件です。2012 年の調査開始以来で最多になりました。以下では東京商工リサーチが公表した調査結果に基づきポイントを見て行きます。

（１）2021 年「個人情報漏えい・紛失事故」の概況



上図のグラフから明らかな通り、2019 年から 2021 年にかけて事故件数が増加しており、気掛かりです。また事故が発生した社数も、2021 年は 120 社（前年比 36.3%増）で、こちらも調査以来、最多になっています。

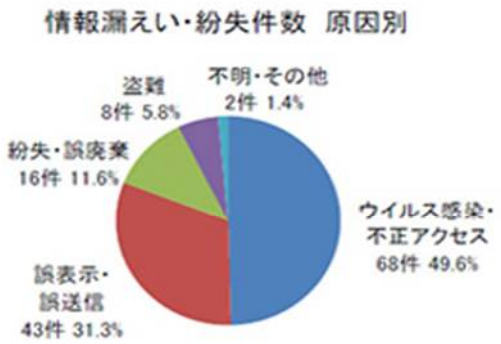
（２）2021 年に発生した主な個人情報漏えい・紛失事故は下表の通りです

2021年　情報漏えい・紛失件数上位

社名	産業	市場	理由	漏えい・紛失件数	内容
ネットマーケティング	サービス	東証1部	不正アクセス	1,711,756件	当社提供の恋活・婚活マッチングアプリ「Omiai」を管理するサーバーが不正アクセスを受け、会員情報の一部が流出。
ANAホールディングス［全日本空輸］	運輸	東証1部	不正アクセス	1,000,000件	国際航空情報通信機構（SITA社、スイス）のシステムに対する不正アクセスでマイレージ情報が流出。
日本航空	運輸	東証1部	不正アクセス	920,000件	国際航空情報通信機構（SITA社、スイス）のシステムに対する不正アクセスでマイレージ情報が流出。
新生銀行［アプラス］	金融・保険	東証1部	誤表示・誤送信	475,813件	会員向けページのログインID・パスワード情報を委託業者に誤って提供。
ライトオン	小売	東証1部	不正アクセス	247,600件	公式オンラインショップに対して外部からの不正アクセスで顧客情報が流出。
リニカル	サービス	東証1部	不正アクセス	222,022件	本社および台湾拠点のサーバーに対して不正アクセス。株主情報や採用応募者などの個人情報が流出。
日本郵政［日本郵便・ゆうちょ銀行］	サービス	東証1部	紛失・誤廃棄	214,000件	投資信託取引などに関する「金融商品仲介補助簿」、払込取扱票などの控え書類の社内紛失。

※ 情報漏えい・紛失件数は「可能性がある」を含む

（3）個人情報漏えい・紛失事故の原因について

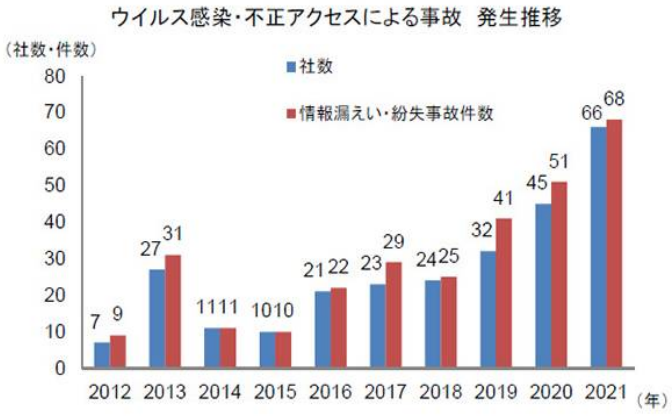


情報漏えい・紛失原因別

主な理由	事故件数	漏えい・紛失件数（平均）
ウイルス感染・不正アクセス	68件	110,745件
誤表示・誤送信	43件	16,966件
紛失・誤廃棄	16件	32,818件
盗難	8件	2,844件
不明・その他	2件	166件
合計	137件	

※「漏えいの可能性がある」ものも含む
※ 漏えい・紛失件数の平均は、各原因別の漏えい・紛失件数の総数を件数開示のある事故件数を分母として算出

2021 年の事故要因のトップは「ウイルス感染・不正アクセス」の 68 件（構成比 49.6%）で、次いで「誤表示・誤送信」が 43 件（同 31.3%）、「紛失・誤廃棄」が 16 件（同 11.6%）と続いています。なお 1 事故あたりの情報漏えい・紛失件数の平均は、「ウイルス感染・不正アクセス」が 11 万 745 件と突出しています。



左図に示したのは「ウイルス感染・不正アクセス」の事故件数の年度推移です。ここ数年はずっと右肩上がりで、この「ウイルス感染・不正アクセス」の増加事故件数が、当該年度の全体の事故件数の増加となっているようです。すなわち他の要因による事故件数は横ばいであるにも拘わらず、「ウイルス感染・不正アクセス」事故が、全体の事故件数を押し上げています。

（4）事故発生の原因となった媒体について

2021 年の情報漏えい・紛失事故 137 件のうち、原因となった媒体は「社内システム・サーバー」が 81 件（構成比 59.1%）と最も多く、次いで「パソコン」が 30 件（同 21.9%）、「書類」が 15 件（同 10.9%）、「その他・不明」が 8 件（同 5.8%）と続いています。

情報漏えい・紛失　媒体別

主な媒体	事故件数	漏えい・紛失件数（平均）
社内システム・サーバー	81件	52,443件
パソコン	30件	2,818件
書類	15件	34,602件
携帯電話	2件	118件
記録メディア	1件	28,553件
その他・不明	8件	399,796件
合計	137件	

※「漏えいの可能性がある」ものも含んだ数値
※ 漏えい・紛失件数の平均は、各媒体別の漏えい・紛失件数の総数を分子、件数開示のある事故件数を分母として算出

1 事故あたりの情報漏えい・紛失件数の平均では、「その他・不明」が 39 万 9796 件で突出していますが、これは社外のシステムへの不正アクセスを受けた ANA ホールディングス（紛失件数 100 万件）、日本航空（同 92 万件）の数字が大きく影響しているためです。

４．お知らせ（トムソンネットについて）

弊社は、保険業務の様々な分野で培った豊富な業務経験やシステム経験を有するスタッフ（コンサルタント）が、みなさまのお役に立つことを願って、スタンバイしております。

以下の通り、対応する業務分野も年々広がっておりますので、気になる分野がございましたホームページにアクセスして戴き、支援業務の内容をご確認の上、下記に気軽にお声掛け下さい。

以上

Ｐマークをはじめとして各種ご相談は下記で承っています。ご気軽にどうぞ！

連絡先　　株式会社トムソンネット　（https://www.tmsn.net/）
〒101-0062 東京都千代田区神田駿河台４－６　御茶ノ水ソラシティ１３階
電話　03-3527-1666　　FAX03-5298-2556

担当:　岩原 秀雄（Mail：iwaharahi1017@tmsn.net）　　平泉 哲史（Mail：s.hiraizumi@tmsn.net）
本間 晋吾（Mail: s.honma@tmsn.net）