コンピュータウイルス・不正アクセスの届出事例

［2021 年下半期（7 月～12 月）］

独立行政法人情報処理推進機構 セキュリティセンター

2022 年 2 月 28 日

目次

1. はじめに

IPA（独立行政法人情報処理推進機構）では、経済産業省の告示[1,2]に基づき、被害の状況把握や対策検討を目的とし、一般利用者の方や企業・組織の方から、広くコンピュータウイルス・不正アクセスに関する届出[3,4]を受け付けている。

本紙では、この制度のもと IPA が受理した届出のうち、特筆すべき事例（未然に防止できたものを含む）を紹介する。届出される情報は断片的な場合があるため、原因・結果・考え得る対策等の全貌が特定できていない事例もあり、把握できた範囲での説明や、一部推定を含む場合がある[5]。

本紙が、同様被害の早期発見や未然防止といったセキュリティ上の取り組みの促進に繋がることを期待する。

---

[1] 経済産業省「コンピュータウイルス対策基準」https://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

[2] 経済産業省「コンピュータ不正アクセス対策基準」https://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm

[3] IPA「コンピュータウイルス・不正アクセスに関する届出について」
https://www.ipa.go.jp/security/outline/todokede-j.html

[4] 届出制度で取り扱う事象は、広く一般にコンピュータウイルスや不正アクセスと呼ばれる事象、またはそれに類する事象全般を対象としており、必ずしも刑法上の「不正指令電磁的記録に関する罪（いわゆるコンピュータ・ウイルスに関する罪）」や「不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）」への該当有無を示すものではない。例えば本紙では、設定不備（アクセス制御機能の不存在など）により利用者の意図に沿わずアクセスされた場合など、刑法上の不正アクセスに該当しない可能性のある事例についても、不正アクセスと呼んでいる場合がある。

[5] 本紙の届出事例は、IPA で一部表現を整えた箇所を除き、基本的には届出で提供された情報のみを掲載している。届出の受理においては、完全なシステム構成やインシデントの詳細といった情報を求めていないため、事例紹介では内容が明瞭でない箇所も含まれる。ご了承いただきたい。

2. 届出事例の傾向

2021 年下半期（7 月～12 月。以下、今期）に受理した[6]コンピュータウイルス（以下、ウイルス）届出およびコンピュータ不正アクセス（以下、不正アクセス）届出において、主な事例を 125 件取り上げ、次の 5 種に分類した。被害の原因に主眼を置いて分類しているが、その原因については、原則として届出者の申告に基づいている。また、複数の分類に該当し得る事例については、その事例の特徴を最も示していると考えたものに分類した。それぞれの分類ごとの届出の概要は次節以降に示す。

- コンピュータウイルスの検知・感染被害　7 件（項番 1～7）
- 身代金を要求するサイバー攻撃の被害　33 件（項番 8～40）
- 脆弱性や設定不備を悪用された不正アクセス　41 件（項番 41～81）
- ID とパスワードによる認証を突破された不正アクセス　28 件（項番 82～109）
- その他　16 件（項番 110～125）

届出のあった被害について全体を通して見ると、これまでと同様に、一般的によく知られたセキュリティ施策を実施していれば、被害を防ぐことができたと思われるものが多かった。ID やパスワードの管理不備や強度不足により認証を突破された事例（2-4 節で説明）の大半はその典型である。セキュリティポリシーに基づいた利用規則の策定やパスワードポリシーの設定等を行い、管理者や利用者一人ひとりがそれに従った運用・利用を行っていれば、被害を防ぐことができた可能性が高いと考えられるものであった。

同様に、脆弱性やセキュリティ設定の不備を悪用された事例（2-3 節で説明）の多くについても、修正プログラムの適用といった基本的な対策を徹底することにより、被害を防げた可能性があったと考えている。例えば、脆弱性情報が公開されてからも長期間対策がなされていなかったために、脆弱性を悪用された攻撃を受けた事例がある。特に身代金を要求するサイバー攻撃の被害に遭った事例（2-2 節で説明）では、2 年近く前に公開された VPN 装置の脆弱性を悪用されて、組織内ネットワークに侵入され、ランサムウェア攻撃を受けたと考えられるものが多く見られた。

一方、今期に関しては、脆弱性情報が公開されてから、その脆弱性を悪用した攻撃が行

[6] 本紙では今期に IPA で受理した届出を対象としている。このため今期以外に発生もしくは発見した事象に関しても、今期に届出者により提出され、IPA で受理した届出については対象に含めている。

われるまでの時間が比較的短く、対策が間に合わなかったため、攻撃の被害に遭ったという事例もあった。

脆弱性の管理は基本的かつ重要な対策であり、徹底することで多くの被害を避けることができるが、組織内の多数の機器を迅速かつ見逃しなくアップデートするのは簡単ではない。機器やソフトウェアバージョンの IT 資産管理、脆弱性情報の収集・アップデートの運用手順の確立を進めていただきたい。

ウイルスの検知や感染被害（2-1 節で説明）に分類した届出は、比較的少なかった。しかし、過去猛威を振るった「Emotet」と呼ばれるウイルスの攻撃活動再開の兆候が確認されており、IPA へ Emotet に関する被害の相談が寄せられるようになってきたことなどから、引き続いての注意は必要と考える。

本紙に示した事例以外にも、ウイルスの発見、なりすましやフィッシング等の不審メールの受信、個人や組織で利用しているアカウントへの不正なログインの挙動検知などの情報も複数寄せられた。これら届出全体の集計情報については別途「コンピュータウイルス・不正アクセスの届出状況」として公開している。

2-1. コンピュータウイルスの検知・感染被害

本節で取り上げるウイルスの検知や感染被害の届出は 7 件であり、2021 年上半期の 14 件から半減した（2020 年下半期の 49 件からはさらに大幅に減少している）。ただし、ウイルスに関する届出のうち、ランサムウェアの部類であると判断した届出については、「身代金を要求するサイバー攻撃の被害」として 2-2 節で説明するため、本節での集計件数からは除外している。

2019 年頃から、2021 年 1 月頃までの間、多数の攻撃活動が観測された Emotet は、2021 年 1 月 27 日に EUROPOL（欧州刑事警察機構）主導で攻撃基盤のテイクダウンが行われた。それ以降しばらく、IPA では Emotet の攻撃メールのばらまきは観測しておらず、被害に遭ったという届出もなかった。しかし、2021 年 11 月 14 日頃から、Emotet の攻撃活動再開の兆候が確認されたという情報があり、Emotet への感染を狙う攻撃メール（Emotet の攻撃メール）が着信しているという情報も複数観測している。また、現在 IPA へも企業等か

ら被害の相談が複数寄せられている状況にある[7]。ウイルス届出においても、今期は 2 件と少数ながら Emotet を検知したとの届出があった。次回の報告の対象期間となるが、2022 年は 2 月末までに 26 件の届出が寄せられている。

2021 年 11 月以降の Emotet は、それ以前のものと比較すると、通信の方法やデータの暗号化手法などが異なるとされている[8]。一方で、攻撃メールに使われている手口としては、以前と同様である。攻撃は、正規のメールへの返信を装うなどして送信元を偽装したメールで行われる。そのメールに、マクロが含まれた Office 文書ファイルを添付したり、メール本文に記載したリンクからダウンロードをさせたりして、受信者に開かせようとする。Office 文書ファイルは、メール配送経路での検知・検疫を避けるため、パスワード付きの ZIP 圧縮ファイルとして添付されていて、メール本文に解凍するためのパスワードが記載されている場合もある。いずれも、Office 文書ファイルを開いてマクロを有効にすると、Emotet がダウンロードされ、感染に至る点も以前と同様である。

現時点で、感染を狙う手口に大きな変更が見られていないことから、感染を防ぐための対策についても、以前と同様に「添付ファイルを開かない」「URL リンクにアクセスしない」「マクロを有効にしない」ことが有効である。送信元や本文に見覚えがある返信メールや、自然な日本語で書かれたメールであっても、攻撃メールである可能性を念頭に置いて取り扱うことも必要であろう。

表 2-1 にコンピュータウイルスの検知・感染被害に関する届出の概要一覧を示す。

---

[7] IPA 「「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」
https://www.ipa.go.jp/security/announce/20191202.html

[8] LAC 「【注意喚起】マルウェア Emotet が 10 カ月ぶりに活動再開、日本も攻撃対象に」
https://www.lac.co.jp/lacwatch/alert/20211119_002801.html

表 2-1 コンピュータウイルスの検知・感染被害の概要一覧

項番	届出日	概要
Emotet ウイルス・攻撃メールの検知事例		
1	2021/7/2	2021 年 1 月 21 日に、届出者（企業）の得意先にウイルス感染を企図したと思われるメールが届いた。このため、社内のパソコンをセキュリティソフトで検査したところ、1 台のパソコンにおいて Emotet を検知した。感染経路はメールと推測しているが詳細は不明である。再発防止策として、社内の全パソコンについて OS の更新とセキュリティソフトの導入を行った。また、UTM を設置して更なるセキュリティ強化を図った。
2	2021/12/3	届出者（業界団体）のメールアドレス宛に、Emotet への感染を狙った攻撃メールが着信し、そのメールの添付ファイルに危険性があることをセキュリティソフトが検知した。メールの送信者として、過去にメールのやり取りを行ったことがある相手組織の従業員の名前が設定（詐称）されていた。ただし、当該従業員と直接メールを交わしたことはなかった。メールにはファイルが添付されており、メール本文は英語で添付ファイルを開くことを促す文章であった。また、メールの末尾には、当該従業員の署名があった。本件を受けて、送信元アドレスとして詐称された組織とやり取りのある従業員へ注意喚起を行った。
3	2021/12/28	届出者（企業）において、Emotet への感染を狙ったとみられる不正なメールが 100 件以上届いていることを検知した。組織内においては、感染などの被害は確認されていない。

その他ウイルスの被害事例		
4	2021/9/14	届出者（企業）が利用している IP アドレスの一つから迷惑メールが送信されているとの連絡がプロバイダからあった。調査により、当該IPアドレスを使用しているパソコンがウイルスに感染していること、600 万通ほどの偽のセクストーション（性的脅迫）と呼ばれる迷惑メールが送信された可能性があることが判明した。ただし、迷惑メールの送信がウイルスによるものであるかは厳密には不明である。また、ウイルスに感染した原因についても不明であった。本件を受けて、当該のパソコンは初期化を行った。また、ファイアウォール設定を見直してルールを厳格化するとともに、社内において Windows7 の廃止を行った。
5	2021/11/17	届出組織（公共機関）の従業員が私物のパソコンを組織のネットワークに接続して業務をしていたところ、ウェブサイト閲覧中に意図しないポップアップが繰り返し表示され、電子メールが消失する等の問題が発生した。事象発覚後、当該パソコンはネットワークから切り離し、また、組織内ネットワークからのインターネット接続を遮断する処置を行った。異常が見られたパソコンを最新のセキュリティソフトでスキャンしたところ、ウイルスが検知されたため駆除した。その他のパソコンについては、セキュリティソフトを更新した後にスキャンを実施し、ウイルスが存在しないことを確認した後で、組織内からのインターネット接続を再開した。ウイルス感染していたパソコンには 3 名分の顧客情報が保存されており、情報が流出した可能性を否定できなかったため、対象者には個別にお詫びを行った。再発防止策として、私用機器の持ち込みやネットワーク接続に関する規則を見直し、徹底することとした。
6	2021/11/19	届出者（一般団体）が使用するクラウド上のサーバにおいて、セキュリティソフトが不正なプログラムの振る舞いを検知した。クラウド事業者とともに調査や対策を行っていたが、1 か月ほど経った後に同一のサーバにおいて、再び同事象が検知された。さらにオンプレミスのサーバにおいても同事象が検知された。原因について調査を行う中で、組織内ネットワークに接続されたパソコンの 1 台において、不正アクセスが疑われる痕跡が発見された。しかし、それ以上は判明せず、原因は調査中である。

7	2021/11/30	届出者（企業）の従業員が、自身のメールアカウントから不審なメールが送信されていたことに気づいた。調査したところ、ウイルスが添付されたメール 300 通ほどが、複数の宛先に対して送信されていたことが判明した。メールサーバに対し不正なログインを試行されていたことも判明したが、いずれも失敗しており、メールサーバへの不正アクセスは確認されなかった。原因については調査中であるが、何らかのウイルスに感染した可能性を考えている。本件を受けて、セキュリティ教育の強化や EDR や MDR といったセキュリティ製品の導入を検討している。

2-2. 身代金を要求するサイバー攻撃の被害

ランサムウェア攻撃など、ファイルやデータを暗号化もしくは消去して、その復旧と引き換えに、身代金として金銭を脅し取ろうとするサイバー攻撃の届出は 33 件あった。この中には、組織内ネットワークへ侵入された原因などについて、VPN 装置などの脆弱性、リモートアクセスの設定ミスや脆弱なパスワードによるものと推測している事例が含まれる。これらは 2-3 節、2-4 節の分類条件と重複するが、身代金を要求する攻撃に関する事例は本節に分類した。

今期の特徴として、一般企業だけでなく、地方自治体、医療機関、各種団体など多岐にわたる組織や個人から届出があったことが挙げられる。ランサムウェア攻撃は、企業規模や業種等によらず、広く無差別に行われている可能性があると考えられる。

脅迫文の特徴や、暗号化後のファイル名に付与される拡張子などから、攻撃に使用されたランサムウェアの名称が推定できる事例もあり、今期の届出において目立ったのは、LockBit2.0 と呼ばれるランサムウェア（以下、LockBit）による被害であった。LockBit は、ウイルスと同名の攻撃グループ「LockBit2.0」が使用するランサムウェアである。この攻撃グループは、窃取したデータを暴露するサイト（リークサイト）を持つ。LockBit には、ファイルの暗号化を高速化させる複数の高度なテクニックが実装され、ドメインコントローラ感染時に特別な仕組みを発生させるなど、様々な手口のアイデアが機能として盛り込まれているとされる [9]。LockBit の被害に遭った届出の中には、Active Directory のサーバがウイルスに感染していたことが判明した事例や、LockBit がドメインコントローラを悪用したことにより、組織内のネットワークを通じて多数の機器に拡散し、ファイルの暗号化を

[9] 三井物産セキュアディレクション株式会社 「ランサムウェア「LockBit2.0」の内部構造を紐解く」
https://www.mbsd.jp/research/20211019/blog/

したと考えられる事例も複数見られた。

なお、LockBit 感染の事例を含め、本節で取り上げた事例において、届出者が感染の原因（推定も含む）として、最も多く挙げていたのは、VPN 装置の脆弱性を悪用された不正アクセスであった。その中には、システム運用保守を行う事業者が、自組織のネットワークからリモートで届出者（被害者）組織のシステム保守作業を行うために構築していた VPN において、その装置に脆弱性があり、不正アクセスされたという事例が複数あった。対策としては、VPN 装置など、外部からの攻撃の侵入口となり得る箇所（攻撃対象領域、Attack Surface と呼ばれる）を把握・特定して必要最小限とするとともに、セキュリティを高めて、攻撃者の侵入を防ぐことである。脆弱性への対策については、2-3 節で述べるが、運用保守業務を委託している場合などは、一般的な脆弱性対策に加えて、委託先業者が使用する部分も含めたシステム構成を把握し、責任分界点を明確にした上で、日ごろから抜け漏れなくセキュリティ対策作業ができるように、作業分担や対応手順を定めておくことも重要であると考える。

表 2-2 に身代金を要求するサイバー攻撃に関する届出の概要一覧を示す。また、侵入型ランサムウェア攻撃と呼ばれる被害の事例 3 件（項番 11、28、29）の詳細を 3 章で紹介する。

表 2-2 身代金を要求するサイバー攻撃に関する届出の概要一覧

項番	届出日	概要
LockBit ランサムウェアの被害事例		
8	2021/8/30	届出者（企業）のサーバが、LockBit に感染する被害に遭った。社内の基幹システムが利用できない状態になっていたため、サーバを確認したところ、ファイル名が LockBit という拡張子に変換されていたことに気づき、発覚した。ファイル拡張子の改ざんと暗号化の被害は複数のパソコンやサーバに及び、また、プリンタから英語の文書が大量に出力されるという事象も発生した。さらに、ファイルの一部は攻撃者によって窃取されていたと見られ、リークサイトと呼ばれる外部サイトに公開するとの脅迫を受けた。外部のセキュリティ専門家とともに、ネットワークセキュリティの強化策を検討している。

項番	届出日	概要
9	2021/8/31	届出者（地方自治体）の業務委託先のサーバが、LockBit に感染しファイルが暗号化される被害に遭った。委託先からの報告を受けて本事象の発生を認知した。技術的な対応は委託先業者が実施していたが、届出者においても、情報漏洩の有無の確認や、情報の公開、委託先との折衝など、予定外の対応が必要となった。委託元の観点で再発防止に向けて今後見直したいこととして、事前にインシデント発生時の対応体制が決まっておらず、調整が必要であったことや、委託業務に関するデータについて、委託先での作業環境やデータの保存状況等の把握が不十分であったこと、成果品データの扱いについて取り決めがあったが、必ずしも徹底されていない場合があったことを挙げており、改善に向けた取り組みを行う予定である。
10	2021/9/3	届出者（業界団体）が使用するサーバに異常が発生していることを、監視保守を行う業者が発見して通知した。状態を確認したところ、十数台のサーバが LockBit に感染していたことが判明した。業務の再開を優先するため、異常が見受けられたサーバは、初期化して再構築することにより復旧させた。ログ等から侵入経路や感染原因の調査を行ったが、原因の究明には至らなかった。再発防止策として、セキュリティソフトの更新の自動化や、パソコンやサーバの監視システムを強化して、異常を発見した際に自動でネットワークから切断する仕組みの導入を検討している。

項番	届出日	概要
11	2021/11/10	届出者（企業）が管理する情報システムにおいて、異常を知らせるアラートの通知があった。調査したところ、一部のパソコンが LockBit に感染していたことが判明した。そのため、即座に関連サーバをシャットダウンし、原因・影響等の調査を開始するとともに復旧作業を行った。調査の結果、外部からの運用保守で使用するリモートアクセス用のゲートウェイ機器に脆弱性が存在しており、その脆弱性を悪用され、不正アクセスを受けたことが原因と判明した。その他、グループ各社で個々に外部からのリモートアクセス環境を構築し、運用していたことなど、セキュリティ対策に関する方針やシステムが統一されていなかったことも要因の一つと捉えた。再発防止策として、セキュリティポリシーの共通化およびゲートウェイの整理・集約を検討している。 ※本事例は 3-2 節で紹介する。
12	2021/11/12	届出者（一般団体）の職員が、組織内のパソコンへのリモートログインができないことに気づき、現地でパソコンの状態を確認したところ、ファイルが暗号化されていたこと、画面に脅迫文のようなメッセージが表示されていたことを発見した。調査により、このパソコンに加え、さらに NAS 1 台に保存されていたファイルが LockBit により暗号化されていたことが判明した。暗号化されたファイルは、バックアップから復元し、バックアップがないファイルについては作成し直すことにした。不正アクセスの原因は不明だが、ファイアウォールのルール設定に不備があったことが要因と考えている。本件の対応には、約 3 週間（1 人）を要した。対策の中で、クラウド上のデータベースへのアクセスに二要素認証を導入するなど追加のセキュリティ施策を行った。

項番	届出日	概要
13	2021/12/9	システム運用業務を行っている届出者（企業）が管理するサーバが、不正アクセスを受け LockBit に感染した。これにより、同社に運用を委託している複数の組織のデータが暗号化され、利用できなくなった。不正アクセスの原因は、VPN 装置に存在していた脆弱性の悪用によるものと推測している。サーバをインターネットから切り離した上で調査を行ったが、攻撃の痕跡が削除されており、データ流出の有無や流出したデータ量は不明であった。対策として、インターネット上への顧客の情報流出状況の監視や、高度なセキュリティ体制の検討を行っている。
14	2021/12/22	届出者（企業）の内部で使用しているファイルサーバ上のデータが暗号化されていることを発見した。調査したところ、VPN から不正にアクセスされ内部ネットワークに侵入されていた。そして、管理サーバおよびファイルサーバが、LockBit に感染させられ、ファイルを暗号化されたと思われる状況であった。なお、管理サーバおよびファイルサーバに侵入された方法については判明していない。本件を受けて、VPN 装置のファームウェアのアップデート、パスワードポリシーの変更、EDR 監視の導入、個人情報の取り扱いルールの見直し、UTM の導入を行った。
その他の身代金を要求するサイバー攻撃被害の事例		
15	2021/7/12	届出者（企業）で使用する複数のサーバやパソコンにおいて、ファイルが暗号化されていることを発見した。状況から、Avaddon と呼ばれるランサムウェアに感染したと考えている。専門業者とともに侵入の経路や拡散の原因を調査したが、アクセスログ等を保管するログサーバもランサムウェアによりファイルが暗号化されていたため解明できなかった。被害に遭ったサーバはバックアップデータを用いて復旧させ、パソコンについてはウイルス駆除または初期化を行った。また、一部のファイルについては、攻撃者グループの活動停止に伴って公開された復号キーにより復元した。再発防止策として、アクセス許可が必要最小限となるようにファイアウォールの設定を見直し、社内の全パソコンにおいては、毎日ウイルスチェックを行うようにした。さらに、社員にセキュリティ教育を実施した。

項番	届出日	概要
16	2021/7/15	届出者（企業）が利用する数台のサーバにおいて、データが暗号化されていることを発見した。調査したところ、使用していた VPN 装置に脆弱性の存在が判明した。このことから、攻撃者に当該脆弱性を悪用されて、社内ネットワークに侵入され、ランサムウェアに感染させられたものと推測される状況であった。なお、ランサムウェアの種別は不明である。本件の対応として、暗号化されたデータをバックアップから復元することで、システムを復旧させた。また、再発防止策として、セキュリティソフトの導入やパスワードの変更、VPN 装置のファームウェアアップデート等を実施した。
17	2021/7/20	届出者（公共機関）で利用しているシステムが利用できなくなったため、システムの保守業者が調査したところ、サーバのファイルが暗号化されており、それが原因でソフトウェアが動作していなかったことが判明した。さらなる調査により、50 台以上のパソコンやサーバが、Sodinokibi と呼ばれるランサムウェアに感染したものと判断した。本件は、リモートアクセス用に設置していた VPN 装置のファームウェアが古かったことから、VPN 装置の脆弱性を悪用した不正アクセスを受け、ランサムウェアに感染させられたと推測される状況であった。対策として、VPN 装置のファームウェアおよびパソコンやサーバの OS アップデートを行った。
18	2021/7/23	届出者(一般団体)が利用している複数のファイルサーバと NAS 上のファイルが暗号化されていたこと、および脅迫文と思われるファイルがあることを発見した。調査により、Cring と呼ばれるランサムウェアに感染させられたことが判明した。感染や被害拡大の原因は、攻撃者に VPN 装置の脆弱性を悪用されて組織内のネットワークに侵入されたこと、管理サーバを乗っ取られて組織内の他のサーバにも感染を拡げられてしまったことと推測している。本件を受け、VPN 装置のファームウェアを更新して脆弱性の解消を行った。他の対策についても実施を検討している。

項番	届出日	概要
19	2021/8/2	届出者（企業）の社内ネットワーク上の複数のサーバにおいて、ファイルが暗号化され、システムが利用不能になっていることを発見した。また、データ復旧のために金銭を要求し、応じないとデータを公開するとの脅迫文が見つかったことから、ランサムウェア攻撃を受けたものと判断した。調査したところ、VPN 装置と AD サーバに脆弱性が見つかったことなどから、攻撃者がそれぞれの脆弱性を悪用して、社内ネットワークへの侵入と、ネットワーク内の機器に対する権限掌握をされたものと考えられる状況であった。対策として、セキュリティ対策装置の導入や、社内利用者のパスワード変更を行った。また、VPN 装置の脆弱性対策などの運用は外部に委託し、AD サーバの修正プログラムは無条件で即時適用するなど運用の変更を実施して、セキュリティ対策の強化を図った。
20	2021/8/5	届出者（企業）の従業員から、パソコン内のファイル拡張子が「.corona」となっていると連絡があった。調査したところ、ノート型２台とデスクトップ型１台の計３台のパソコン上のファイルが、ランサムウェアによって暗号化されていたことが判明した。ノート型のパソコンは SIM カードを内蔵しており、グローバル IP アドレスが付与され、インターネットから直接アクセスできる状況であった。攻撃者が脆弱性の悪用など、何らかの方法で外部から不正アクセスしたものと考えている。デスクトップ型は、不正アクセスされたノート型の 1 台からリモートデスクトップ接続により侵入されていた。また、ランサムウェアとは別に、Mimikatz と呼ばれるツールが発見された。ローカル Administrator のパスワードに同一のものを使用しており、攻撃者により窃取されたと思われる状況であった。パソコン 3 台の回復はさせず、SIM カードの廃止、ローカル Administrator のパスワードの複雑化・個別化を行った。今後はアクセスログの管理や監視方法の変更、ファイアウォールの設定の見直し等の対策を実施する予定である。パソコンのフォレンジックや組織内ネットワークの脅威ハンティングのため、1,000 万円程度の費用が発生した。

項番	届出日	概要
21	2021/8/19	届出者（企業）が使用するサーバが、eCh0raix と呼ばれるランサムウェアに感染した。届出者によると、詳細は不明だが、原因は脆弱性の悪用によるものと推測され、サーバに保存していたファイルの情報も漏洩した恐れがあると考えられるとのことであった。再発防止策として、セキュリティ機能に対応した機器の導入や、バックアップのポリシーや手順の見直しを行った。
22	2021/8/27	届出者（企業）で使用している Linux ファイルサーバと NAS のファイルが暗号化され、使用できなくなった。調査の結果、データ復元のために身代金を要求するメッセージがテキストファイルとして残されていたことから、ランサムウェア攻撃を受けたと判断した。侵入経路や拡散の手口は不明であるが、ログ等の調査により、1 台のパソコンを踏み台にして、不特定多数に不審なメールを送信していた形跡が見つかったため、これらのメールを介してランサムウェアに感染したものと推測している。再発防止策として、最新の UTM やセキュリティソフトを導入するとともに、標的型攻撃メール訓練を実施して従業員のセキュリティ意識向上を図った。

項番	届出日	概要
23	2021/8/31	届出者（企業）の複数の仮想サーバにおいて、ファイルが暗号化され、復元のために金銭を要求する脅迫文が置かれていることをシステム管理者が発見した。暗号化されたファイルや脅迫文の特徴から、Hive と呼ばれるランサムウェアに感染したと考えられ、数日間にわたって全業務が停止する事態に陥った。セキュリティ専門業者と調査を行ったところ、AD サーバ、アプリケーションサーバ、ファイルサーバ等、合計数十台のサーバが被害に遭っていたことが判明した。原因については、VPN 装置の脆弱性悪用で窃取された認証情報により、リモートデスクトップ接続の認証を突破されて、不正アクセスされたものと推定している。被害に遭った仮想サーバは初期化し、バックアップデータを用いて再構築を行うことで、システムを復旧させた。再発防止策として、サーバやパソコンの OS と VPN 装置のファームウェアを最新版に更新し、さらにパスワードの変更、セキュリティソフトの機能追加を行った。また、バックアップの運用方式も見直し、バックアップ取得の頻度を高めて、データはサーバから隔離した場所に保存するように変更した。
24	2021/9/1	届出者（企業）が運用するサービスのサイトに不正アクセスがあり、システム内の全データベースのデータが削除され、復旧のために金銭を要求する脅迫メッセージが残されていたことを発見した。調査会社とともに侵入経路や攻撃手法等について調査を行ったが、原因は特定できなかった。この結果を踏まえ、安全性が担保できないとして、当該サービスは終了することとした。今後のサービス開発や公開の際には、ログ取得レベルの強化や、外部セキュリティ監査機関による監査を必須とするとしている。

項番	届出日	概要
25	2021/9/8	届出者（個人）のパソコンにおいて、ファイルが暗号化され拡張子が改ざんされていたことを届出者自身が発見した。調査したところ、当該パソコンから個人の SNS アカウントへ心当たりのない不正なログインの形跡が見つかったことから、外部からの不正な遠隔操作により、SNS アカウントへの不正アクセスやファイルの暗号化がされたと考えられる状況であった。原因は不明であるが、届出者は、以前に不審なプログラムを実行した覚えがあった。何らかの経緯で、遠隔操作を可能にするウイルスに感染したものと推測している。パソコンはシステムを再インストールすることで復旧させた。
26	2021/9/17	届出者（企業）で利用するネットワークで、通信の不調が生じた。調査したところ、ドメインコントローラ上のファイルが破損し、データ復元に身代金を要求する脅迫文が残されていたことが判明した。届出者はこの状況から、ランサムウェア攻撃を受けたと判断した。なお、脅迫文には窃取した情報を公開するといった内容も書かれていたが、届出時点では、当該情報の公開は確認していない。調査の結果、合計 20 台以上のパソコンやサーバが被害を受けていたことが判明した。被害を受けたパソコンにおいて、セキュリティソフトがアンインストールされていたことや、外部からのリモート操作を可能にするアプリケーションがインストールされていたことも判明したが、原因となった不正アクセスの手口は特定できなかった。本件を受けて、パスワード変更、特権アカウントの管理の見直し、認証方式の設定見直しを行った。また、原因の特定に至らなかった要因の一つに、ログの取得量や種類が十分でなかったことがあるため、ログの取得や保管の設定を見直した。

項番	届出日	概要
27	2021/10/10	届出者（企業）が管理するサーバにおいて、外部から不正アクセスされた形跡を EDR が検知した。調査したところ、サーバ上のデータが窃取された可能性があり、また、一部のサーバについてはデータ復旧のために身代金を要求する脅迫文が残されていることが判明した。原因については、VPN 装置のファームウェアのバージョンが古く、認証情報が漏洩する脆弱性が存在していたことから、認証情報を窃取した攻撃者がネットワーク内に侵入し、ランサムウェア攻撃を行ったと推測される状況であった。対策として、VPN 装置のファームウェア更新による脆弱性の解消に加え、多要素認証の導入、バックアップ方式の見直し等を行った。
28	2021/10/13	届出者（企業）の複数の拠点において、パソコンから社内サーバにアクセスできない事象が発生した。社内の担当者が調べた結果、計 20 台以上のパソコンやサーバにおいて、ファイルの暗号化と拡張子の改ざんが行われていること、データの復旧のために指定のウェブサイトへアクセスするよう要求する画面が表示されたことが判明した。また、リークサイトと呼ばれる外部のサイトに、窃取されたファイルの一部が公開されていることも判明した。リークサイトの情報等から、本事象は Spook と呼ばれるランサムウェアに感染させられたと考えられる。この被害により、業務システムが使用できない状態が数日間継続し、業務影響があった。更なる調査をセキュリティ事業者とともに行ったところ、VPN 装置において、内部ファイルが外部から読み取り可能になる脆弱性の存在が判明した。このため、攻撃者が VPN 接続のための ID とパスワードを窃取し、社内ネットワークに侵入してランサムウェア攻撃を行ったと推測している。 対策として、VPN 装置のファームウェアを更新して当該脆弱性を解消した。また、VPN のユーザ情報は全て無効化を行い、当面の間、VPN を使用しないこととした。再開にあたっては、パスワードポリシーの策定など、認証方法を強化した上で行うとしている。 ※本事例は 3-3 節で紹介する。

項番	届出日	概要
29	2021/10/15	届出者（企業）の社内ネットワーク上の 20 台以上のサーバにおいて、ファイルが暗号化され、サーバ機能が停止する被害に遭った。調査の結果、攻撃者が VPN 装置の脆弱性を悪用して窃取した認証情報により、社内へ不正アクセスして、Zeppelin と呼ばれるランサムウェアに感染させたと推測される状況であった。なお、一部のサーバにおいては、VPN 装置のものと同一の ID やパスワードを使用していたことが判明し、これが感染拡大の要因になったと考えている。本件への対応として、外部の専門業者に復旧作業を依頼し、バックアップデータからの復元を行った。復旧には 10 日以上を要し、その間の業務停止による売り上げの減少や顧客への補填などの金銭的な被害も発生した。再発防止に向けた対策として、各システムのパスワード変更、推測されやすい管理者 ID の使用禁止、バックアップの強化、セキュリティソフトの設定見直しを行っている。今後、オフラインバックアップの取得、ファームウェアを定期更新する運用上の仕組みの構築、外部機関によるセキュリティ診断の実施を検討している。 ※本事例は 3-4 節で紹介する。
30	2021/10/20	届出者（地方自治体）が使用するファイルサーバ内のファイルとバックアップデータが暗号化される被害を受けた。職員がサーバ内のファイルを開こうとした際に、ファイル破損のエラーが表示されたことにより被害発生を認知した。また、ファイルサーバ内にデータ復元のために身代金を要求するメッセージがあったことから、ランサムウェア攻撃を受けたものと推測している。侵入の原因は、職員のウェブサイト閲覧、もしくはメールの添付ファイルによるウイルス感染と推測しているが、詳細は不明であった。なお、データの復旧はセキュリティ専門業者に依頼予定である。再発防止策として、システムのファームウェアの確認、パソコンの OS のバージョンアップおよびセキュリティソフトの最新版の適用、新たなセキュリティソフトの導入、職員への研修の実施を検討している。

項番	届出日	概要
31	2021/11/8	届出者（業界団体）のパソコン 1 台で、一部のファイルが暗号化され、拡張子が改ざんされていることを発見した。即座に当該パソコンをネットワークから切断して調査したところ、他のパソコン等では同事象の発生は確認されず、情報が窃取された形跡も見つからなかった。状況から、ランサムウェア攻撃を受けたものと推測しているが、感染の原因は不明である。
32	2021/11/19	届出者（個人）のパソコンにおいて、ファイルの暗号化と拡張子の改ざんが行われ、脅迫文のようなメッセージがテキストファイルとして残されていることを発見した。拡張子の特徴から、MAQL と呼ばれるランサムウェアに感染させられたものと推測される状況であった。セキュリティソフトにより、ランサムウェアは駆除したが、暗号化されたファイルの復旧はできていない。
33	2021/11/24	届出者（一般団体）が利用するサーバと NAS 上のファイルが暗号化され、拡張子が改ざんされていることを発見した。確認したところ、データ復元のために身代金を要求するメッセージが残されていたことから、ランサムウェア攻撃を受けたと推測される状況であった。本サーバはインターネットには接続せず、組織内の閉じたネットワークで使用していたが、サーバ運用業者のリモート保守用に、SSL-VPN で外部からリモートログインできるようにしていた。このため、攻撃者に VPN 装置の脆弱性を悪用した不正アクセスをされて、ランサムウェア攻撃を受けたものと考えている。対策として、VPN 装置のファームウェアの最新化による脆弱性の解消、SSL-VPN 接続時における二要素認証の適用、振る舞い検知機能をもったセキュリティソフトの導入によりセキュリティの向上を図った。さらに、オフラインのバックアップ環境を整備するなど運用面の改善も行った。

項番	届出日	概要
34	2021/11/24	届出者（一般団体）が利用するサーバにおいて、ファイルが暗号化されていたことを発見した。さらに脅迫文が残されていたこと、管理者用のパスワードが変更されていたことが発覚した。本件を受け、影響が及ぶ可能性のあるサーバの停止やネットワーク回線の遮断により、メールシステムを含む全てのシステムの使用を停止した。復旧について、複数のシステムでデータが暗号化されており回復が困難であったため、新規に別のシステムを導入することとし、安全性を確認した上でメールシステムを再開した。新たなメールシステムが稼働するまでの間、外部とのメールの送受信ができない影響が生じた。原因は調査中である。
35	2021/11/29	届出者（企業）の複数台のサーバにおいて、ファイルの暗号化に加え、拡張子が改ざんされる被害があった。また、データ復旧のために身代金を要求するメッセージが書かれた HTML ファイルが残されていることを発見した。被害状況から、Fileslock と呼ばれるランサムウェアに感染させられる攻撃を受けたものと推測される。引き続き調査および対策を行っている。
36	2021/12/3	届出者（企業）の使用するサーバにおいて、ファイルが暗号化されていることを発見した。ランサムウェア攻撃を受けたものと推測されるが、感染経路など、原因は不明である。
37	2021/12/15	届出者（企業）のシステムにおいて障害が発生した。システムを停止して外部機関とともに調査を行ったところ、障害の原因はサーバ上のファイルが暗号化されて機能不全に陥っていたこと、ファイルの暗号化はランサムウェアによるものであることが判明した。さらに調査した結果、攻撃者により、VPN 装置の脆弱性が悪用され、社内ネットワークに侵入された後、何らかの方法によりドメインコントローラに侵入され、ドメイン管理下の 20 台以上のサーバやパソコンにも侵入被害を受けていたことが判明した。対策として、ネットワークの出入口におけるセキュリティ強化、バックアップ体制の見直し、セキュリティポリシーの策定や社員教育を行うとしている。

項番	届出日	概要
38	2021/12/16	届出者（企業）のサーバがファイルを暗号化される被害に遭い、受託管理しているウェブシステムが動作停止した。状況から、Malloxと呼ばれるランサムウェアに感染させられる攻撃を受けたものと推測している。バックアップデータの保存は行っていたが、フォレンジック調査等の環境保全のため、届出時点で復旧作業は行っておらず、システムの復旧には至っていない。原因等は調査中であり、結果を踏まえて再発防止策を検討予定である。
39	2021/12/24	届出者（企業）のサーバが停止したことを示すアラートが通知されていることを、監視業務の委託先業者が発見し、システム管理者に連絡した。調査したところ、サーバ上のファイルが暗号化され、脅迫メッセージが書かれたテキストファイルが残されていることが判明した。これらの状況からランサムウェア攻撃を受けたと考えている。さらに詳細に調査を行ったところ、攻撃者にサーバの管理者アカウントを掌握され、ランサムウェアを組織内の多数のサーバやパソコンに配布・実行され、機能停止やデータ消失の被害が発生していることが判明した。不正アクセスの原因としては、VPN 装置に脆弱性の存在を確認したことから、それをパスワードなどの認証情報の窃取に悪用され、侵入を受けたことによるものと考えている。対策は攻撃手口が詳細に解明でき次第検討することとしており、VPN 装置の脆弱性の解消、多要素認証の導入、組織内のサーバに対する脆弱性検査の実施等を予定している。
40	2021/12/31	届出者（企業）で使用するパソコンやサーバにおいて、ファイルの暗号化と、拡張子の改ざんの被害を受けていることに気づいた。拡張子の特徴などから、Nightsky と呼ばれるランサムウェアに感染させられたと考えている。ランサムウェアはセキュリティソフトが検知し駆除したとみられるが、ファイルの復元はできていない。感染の原因についても調査中であり、現時点で不明である。

2-3. 脆弱性や設定不備を悪用された不正アクセス

ソフトウェアのセキュリティ上の不具合（脆弱性）、またはサーバやネットワーク機器のセキュリティに関する設定不備が存在し、それが攻撃者に悪用されて不正アクセスを受けた事例の届出は、本節に分類したものだけで 41 件あった。なお、2-2 節で述べたとおり、身代金を要求するサイバー攻撃の被害を受けた事例において、脆弱性を悪用されて不正アクセスされたものはそちらに分類しているため、脆弱性の悪用が原因の届出の総数はさらに多くなる。

中でも、2020 年下半期ごろから届出が多く見られるようになった VPN 装置の脆弱性を悪用された不正アクセス被害が 14 件（2-2 節の事例のうち、VPN 装置の脆弱性が原因とされた届出の件数を含む）と多く、特に、2019 年に情報公開された脆弱性が 2 年間近く未対策のままにされていたため、攻撃者に悪用されたと思われる事例が目立った。

この脆弱性は、VPN 装置内部の任意のファイルを読み取ることができるというものであり、悪用された場合、VPN に接続する際の ID やパスワードといった認証情報を窃取される恐れがあった。これにより窃取されたと思われる大量の認証情報がダークウェブで公開されるなど [10]、攻撃者から積極的に狙われたものと考えている。対策としては、アップデートにより脆弱性を解消するだけでなく、既に認証情報が窃取されていた場合に備え、パスワード等を変更する必要がある。VPN 装置のような、外部から組織内ネットワークへの侵入経路になり得るような重要な機器については、多要素認証を導入するといった強化策も検討することが望ましい。

ウェブシステムや EC システムにおいては、以前から届出が多かった CMS（Contents Management System）の脆弱性だけでなく、自組織において開発したプログラムの部分に SQL インジェクション等の脆弱性があり、悪用されて不正アクセスを受けた事例があった。それぞれの事例について、当該プログラムが稼働開始した時期は不明であるが、システムを稼働させてサービスを開始した時期から脆弱性を含んだまま稼働していて、今期になって不正アクセスを受け、発覚した可能性もあり得る。

長期間、脆弱性対策がされていなかったことに起因すると思われる事例が多かった一方で、脆弱性が公開されてから比較的短い期間で、その脆弱性を悪用した攻撃が観測された例もあった。2021 年 10 月 20 日に情報が公開された CMS（Movable Type）の脆弱性については、1 週間後の 10 月 27 日には脆弱性の有無を確認するような通信が観測されてい

---

[10] JPCERT/CC 「Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について」https://www.jpcert.or.jp/newsflash/2020112701.html

る [11]。不正アクセス届出においても、当該脆弱性を悪用した攻撃により被害を受けたとの届出が 10 件あり、11 月の上旬に攻撃を受けたとされるものが多かった。同様に、2021 年 11 月ごろに報告されていた Java ベースのロギングライブラリである Log4j の脆弱性についても、12 月に被害を受けたという届出が 2 件あった。

このような場合の対策としては、迅速かつ確実な脆弱性対策を実施するに尽きる。脆弱性情報の公開から 1 週間程度で攻撃が観測されることもある状況においては、月に 1 回といった定期的な対策だけでは間に合わず、攻撃の被害を受ける恐れがある。自組織で使用しているすべてのハードウェア、ソフトウェア、サービスを把握した上で、それぞれに対して各ベンダ等から随時情報が取得できるようになっていること、脆弱性が確認されたときにはすぐに対策作業ができるようになっていることといった観点で、運用の体制や手順を点検することが重要と考える。

表 2-3 に脆弱性や設定不備を悪用された不正アクセスの届出の概要一覧を示す。Movable Type の脆弱性を悪用した攻撃による被害の事例（項番 48）の詳細を 4 章で、オンラインストアへの SQL インジェクション攻撃により顧客情報が流出した被害の事例（項番 68）の詳細を 5 章で紹介する。

[11] LAC 「【注意喚起】Movable Type の脆弱性を狙う悪質な攻撃を観測、至急対策を！」
https://www.lac.co.jp/lacwatch/alert/20211102_002780.html

表 2-3 脆弱性や設定不備を悪用された不正アクセスに関する届出の概要一覧

項番	届出日	概要
VPN 装置の脆弱性を悪用された事例		
41	2021/8/11	外部機関から、届出者（企業）が使用する VPN 装置に脆弱性があり、認証情報が漏洩している恐れがあるとの連絡があった。調査を行ったところ、VPN 装置の脆弱性を悪用されて、数十件のユーザアカウントとパスワードが窃取されたこと、および、それらを用いた社内ネットワークへの侵入を試みられていたことが判明した。ただし、VPN 装置は多要素認証を導入していたため、社内ネットワークへの不正アクセスに成功された形跡はなかった。届出者によると、悪用されたのは 2021 年 8 月に公開された脆弱性であると推測している。脆弱性の対策は随時実施してきたが、本攻撃は 2021 年 5 月から 7 月にかけて行われていたゼロデイ攻撃と見られ、当該脆弱性が公表される前であったため、脆弱性対応をする術がなかった。再発防止策として、VPN 装置をインターネットから遮断し、ファームウェアのアップデートを行う予定である。
42	2021/10/18	届出者（企業）が運営する EC サイトが不正アクセスを受け、クレジットカード情報を含む顧客情報が漏洩した恐れがあることが発覚した。届出者を送信者に装ったフィッシングメールを受信した顧客からの問合せにより本事象を認知し、調査を行った。その結果、この問合せの約 1 か月前に不正アクセスがあり、カード情報等が窃取されていたことが判明した。VPN 装置の脆弱性の悪用により、社内ネットワークへ侵入され、EC システムのソフトウェアの管理画面に不正アクセスされたことで、サーバ内の情報窃取と、システムの改ざんが行われたと推測される。再発防止策として、EC システムが稼働しているネットワークを社内ネットワークから隔離し、相互の通信を遮断するようにしたことで、侵入のリスクの低減を図った。また、EDR を導入してインシデントの監視や発生時の対応を強化した。

項番	届出日	概要
43	2021/10/19	外部のセキュリティ事業者から届出者（企業）に対して、届出者が管理している VPN 装置のシステム設定情報が漏洩している恐れがあるとの連絡があった。調査したところ、脆弱性のある古いバージョンの VPN 装置を使用していたことが判明し、認証情報が漏洩した懸念が生じたため、被害予防として一時的に VPN 機能を停止した。VPN 機能を停止したことで、被害発見から対応完了までの約 1 か月間、従業員のテレワークや、リモートでのサーバメンテナンスを行うことができなくなった。対策として、VPN 装置のバージョンアップによる脆弱性の解消に加えて、パスワードの変更、使用していないアカウントの削除等を行った。
44	2021/10/26	届出者（企業）で利用する VPN が使用できなくなったと、従業員から連絡があった。調査したところ、ネットワーク機器のサービス再起動が繰り返される状況となっており、復旧は不可能と判断して、再構築を行った。なお、調査を行った際に、不審な IP アドレスからの接続があったことが判明したため、詳細は不明ながら、何らかの不正アクセスが行われたと判断した。本件を受けて、ネットワーク機器の更新頻度の見直しや、外部からのアクセス制限の強化を行った。
CMS の脆弱性悪用の事例		
45	2021/7/27	届出者（企業）が運用するウェブサイトが改ざんされているとの連絡が、レンタルサーバ事業者からあった。調査したところ、ウェブサーバ上に不審なスクリプトやプラグインが追加されていること、ファイルが改ざんされていることを発見した。原因については、管理用のパスワードが漏洩したか、CMS（WordPress）の脆弱性を悪用されたことが考えられるため、パスワードの変更および CMS の脆弱性対策を行った。

項番	届出日	概要
46	2021/8/24	届出者（企業）で運営しているウェブサイトの管理画面にアクセスしようとしたところ、エラーとなることに気づいた。調査により、ウェブページが改ざんされ、管理画面にアクセスできないようにする設定と、サイトにアクセスしたユーザを偽のショッピングサイトへ誘導する不正なプログラムが仕掛けられていたことが判明した。不正プログラムは、起動されると自身のファイルを削除する仕組みであったことがわかったため、プロセスを停止させ、ファイルが削除されたことを確認した。しかし、翌日には再度不正なプログラムが存在していることを確認したため、システムを再構築することとした。不正なプログラムを配置・起動された原因については不明であるが、CMS（WordPress）の脆弱性が悪用された可能性を考えている。対象のウェブサーバの再構築には、最新版のソフトウェア（CMS や PHP）を用いることでリスク低減を図った。
47	2021/8/31	届出者（企業）のウェブサイトに不正なスクリプトが仕掛けられ、アクセスすると届出者と無関係のサイトへ遷移するように改ざんされていた。届出者は、顧客からの問合せがあり事象を認知したが、約 1 か月の間、改ざんされた状態にあったと考えている。原因は、CMS（WordPress）のバージョンが古く、また、修正プログラムが適用されていなかったことから、CMS の脆弱性が存在し、攻撃者に悪用されたものと推測される状況であった。対策として、CMS のバージョンアップとセキュリティ対策用のプラグインの導入、さらにプロバイダが提供するファイル改ざん検知機能の導入も実施した。あわせて、管理するウェブサイトの総点検を実施した。

項番	届出日	概要
48	2021/11/12	届出者（企業）のウェブサイトの動作が停止していることに、サイトの運営委託先の業者が気づいた。調査したところ、CMS（Movable Type）の脆弱性を悪用した不正アクセスを受け、複数のファイルが改ざんされていたために、サイトが動作停止していたことが判明した。届出者のウェブサイトのプラットフォームは、Movable Type から別の CMS に移行していたが、移行前の Movable Type が削除されていなかったため、未対策の脆弱性が存在していることを把握できず、攻撃者から不正アクセスを受けてしまった。本件を受けて、使われていない Movable Type のファイルはすべて削除したほか、委託先の業者との連携の強化、脆弱性情報の収集方法の強化等の施策を実施した。 ※本事例は４章で紹介する。
49	2021/11/16	届出者（企業）のウェブサーバに不正アクセスがあり、不正なツールが設置されるなどのウェブサイトの改ざんが行われた。届出者自身がウェブサイトにアクセスした際に正しく表示がされなかったことに気づき、改ざんが発覚した。専門業者とともに調査を行ったところ、CMS（Movable Type）の脆弱性があったことが判明し、攻撃者が当該脆弱性を悪用して不正なツールを設置し、サイトの改ざんを行ったと推測される状況であった。サーバに保持していた情報の窃取は確認されていないが、個人情報が漏洩した可能性がある顧客等に、メールで通知し謝罪した。対応として、CMS や EC システムのソフトウェアを最新のものに更新した上で、ウェブサイトを再構築し復旧させた。再発防止に向け、専門業者に定期的なメンテナンスを実施するように依頼した。

項番	届出日	概要
50	2021/12/3	届出者（企業）のウェブサーバに不正アクセスがあり、ウェブサイトが改ざんされた。運用を委託している事業者から連絡を受け、この事業者と調査を行ったところ、アクセス制御のためのファイル（.htaccess）の改ざんや、不正な PHP ファイルが複数設置されていたことが判明した。原因として、使用している CMS（Movable Type）に脆弱性があったため、当該脆弱性を悪用した不正アクセスを受け、改ざんが行われたと考えている。対策として、CMS のバージョンアップにより脆弱性を解消し、CMS やデータベース等のパスワード変更を行った。また、EDR の導入により更なるセキュリティ向上を図る。
51	2021/12/6	届出者（企業）のウェブサイトに対して、不正なファイルが設置されるなどの改ざんが行われた。アクセス制御のためのファイル（.htaccess）が改ざんされて、リダイレクト設定が動作しなくなっていたことに社員が気づき発覚した。ウェブサイトを閉鎖して調査を行ったところ、最新版ではない CMS（Movable Type）を使用していたことから、その脆弱性を悪用した不正アクセスを受けたものと推測される状況であった。対応として、古いバージョンの CMS の削除等を実施後、バックアップデータを用いてウェブサイトを復旧させた。再発防止策として、WAF の導入や定期的なウェブセキュリティ診断等の実施を予定している。
52	2021/12/7	届出者（教育・研究機関）のウェブサイトが、不正アクセスにより改ざんされた。職員がウェブサイトにアクセスできないことに気づき、サーバを調べたところファイルが改ざんされていることを発見した。使用していた CMS（Movable Type）に脆弱性があったことが判明したため、当該脆弱性を悪用した不正アクセスを受け、改ざんされたと推測している。本件を受け、組織内の全サーバに対して該当するバージョンの CMS の使用有無を確認し、使用していた場合はアップデートを行って脆弱性を解消する処置を行った。再発防止に向け、定期的に情報システム部門が脆弱性情報を確認して、必要に応じて組織内に注意喚起を行う仕組みを確立し、継続的に脆弱性対策を行っていく。

項番	届出日	概要
53	2021/12/10	届出者（企業）が保守管理作業を受託しているウェブサイトが、不正アクセスによる改ざんの被害に遭った。届出者がウェブサイトの動作に異常を認め、サーバを調査したところ、ファイルの改ざんや不審なファイルの設置がされていることを発見した。原因として、使用していたCMS（Movable Type）に脆弱性があったため、攻撃者に脆弱性を悪用した不正アクセスをされ、改ざんされたと考えられる状況であった。本件を受け、CMSの更新により脆弱性を解消した後、バックアップからデータを復元し、併せて、認証方式の変更や接続IPアドレスの制限の処置を行った。再発防止策として、脆弱性対策を含めた保守契約を追加するか、クラウド型のサービスへ移行することを検討している。
54	2021/12/27	届出者（企業）のウェブサイトが、不正アクセスを受け改ざんされた。届出者がサイトへアクセスした際にエラーが頻発したため、調査したところ、アクセス制御のためのファイル（.htaccess）が改ざんされていることに気づき、不正アクセスが発覚した。他にも複数のファイルが改ざんされたり、不正に設置されたりしていたことも発覚した。届出者は原因として、使用していたCMS（Movable Type）に脆弱性があったため、当該脆弱性を悪用された不正アクセスにより、改ざんされたと考えている。対応として、別のサーバ業者のプラットフォームに移行し、原因となったファイルの削除や、改ざんされたファイルの復元を行って復旧させた。CMSについては別のソフトウェアに移行することを検討中である。

項番	届出日	概要
55	2021/12/27	届出者（企業）の２つのウェブサイトが不正アクセスにより改ざんされた。届出者がサイトの更新作業を行おうとした際に、複数のファイルが改ざんされていたり、不正に設置されていたりすることに気づき、本件が発覚した。専門業者にフォレンジック調査を依頼して調査を行った結果、CMS（Movable Type）の脆弱性を悪用した不正アクセスを受け、攻撃者にバックドアやウェブシェル、不正メール送信プログラムを設置されたことが判明した。本件により不正なメール３件が外部に送信された可能性があるが、自社提供サービスへの影響、および個人情報等の機敏な情報が流出した痕跡は確認されなかった。事象確認後、CMS のアップデートによる脆弱性を解消、さらに WAF の導入等によるセキュリティ向上の施策を行った。
56	2021/12/27	届出者（教育・研究機関）が利用するウェブサーバが不正アクセスを受け、当該サーバ上に不審な PHP ファイルや HTML ファイルを設置された。本件は、監視サービスから攻撃被害の疑いがあるとのメールが届いたことで発覚した。原因は、届出者が利用していた CMS（PowerCMS）の脆弱性を攻撃者に悪用されたものとみられる。7 日間に約 200 回の不正アクセスの痕跡が確認された。対策として、当該 CMS の脆弱性対策や、管理者ページへのアクセス制限およびパスワード変更、保守業者と連携した緊急性の高いセキュリティ情報の共有を行う。
57	2021/12/28	届出者（企業）のウェブサイトが不正アクセスを受け、改ざんされた。社員が問合せフォーム用のメールを確認したところ、大量の送信エラーメールが着信していたため、異常を感じ、調査したところ、ウェブサーバに不正なファイルが設置されていたことが判明した。改ざんにより、届出者とは無関係のウェブページを作成されたり、メールを送信する機能を不正に作成されて、1000 通以上のフィッシングメールの送信に悪用されたりしたなどの被害も確認した。なお、顧客情報は当該サーバに保存しておらず漏洩の懸念はなかった。原因は、攻撃者に CMS（Movable Type）の脆弱性を悪用されたことと推測している。再発防止策として、WAF の設置や、改ざん検知サービスの導入を検討している。

項番	届出日	概要
EC システムの脆弱性悪用の事例		
58	2021/9/27	届出者（企業）が運営する EC サイトが、脆弱性を悪用した不正アクセスを受け、顧客のクレジットカード情報を窃取された。クレジットカード会社から、カード情報流出の懸念に関する連絡があり、本件が発覚した。原因は、攻撃者により不正なスクリプトを含む購入情報がデータベースに登録され、この購入情報を管理者が処理した際に、クロスサイトスクリプティング脆弱性を悪用した攻撃が作動するようにされていたことであった。この攻撃により有効なセッション ID が窃取され、不正アクセスに使用されたと考えている。攻撃者は EC システムに不正にログインして、バックドアの設置、ファイルの改ざん、不正プログラムの設置を行っていたことが判明しており、この一連の攻撃により、顧客のクレジットカード情報を窃取したと推測される状況であった。一時的な対策として、管理画面へのアクセス制限の実施、EC システムの更新による脆弱性の解消を行った。その後の対策として、既存の EC システムの利用を停止し、別の EC システムを用いてプラットフォームを再構築した。
59	2021/10/1	届出者（企業）が運営する EC サイトから顧客情報が漏洩した可能性があることが、決済代行業者からの連絡により発覚した。調査により、EC システムのソフトウェアにクロスサイトスクリプティングの脆弱性が存在していたため、当該脆弱性を悪用された攻撃を受け、不正アクセスされたものと推測される状況であった。対策として、ソフトウェアを脆弱性対策がなされたバージョンに更新するとともに、WAF やページ改ざん検知機能の導入などにより、セキュリティの向上を図った。再発防止策として、定期的な脆弱性診断の実施により脆弱性対策の強化を図った。

項番	届出日	概要
60	2021/10/18	届出者（企業）が運営する EC サイトが不正アクセスを受け、顧客情報が漏洩した可能性が確認された。本件は、セキュリティ強化業務を委託している専門業者からの報告により発覚した。原因は、攻撃者に当該サイトの脆弱性を悪用されたことにより、サーバ内に悪意のあるプログラムを設置され、決済情報プログラムの改ざんが行われたものと推測している。対策として、当該 EC サイトは閉鎖し、別のサービスプラットフォームにて EC システムを再構築するとともに、システムのセキュリティ対策および監視の体制を強化するなどで、再発防止を図るとしている。
61	2021/11/29	ASP 型 EC サイトのサービス提供事業者のシステムに不正アクセスがあった。当該サービスを利用した EC サイトを運営する届出者（企業）へ、サービス提供事業者から、顧客のクレジットカード情報が漏洩した懸念があるとの連絡があり、届出者が本件を認知した。EC サイトを停止し、セキュリティ専門業者とともに調査を行ったところ、数千件の顧客情報が漏洩した可能性があることが判明した。不正アクセスの原因は、サービス提供事業者によると EC システムに存在していたクロスサイトスクリプティングの脆弱性を攻撃者に悪用されたとのことであった。調査結果に基づいた再発防止策を検討中である。

項番	届出日	概要
62	2021/12/2	届出者（企業）の EC サイトが不正アクセスを受け、3000 件以上のクレジットカード情報を含む 20 万件以上の顧客情報が窃取された。届出者は、クレジットカード会社からの連絡により認知し、EC サイトを停止して専用コンタクトセンターを設置する対応を行った。インシデント対応費用は約 1 億円の見込みである。専門業者とともにフォレンジック調査などを行った結果、EC サイトにクロスサイトスクリプティングの脆弱性が存在しており、攻撃者が当該脆弱性を悪用して、プログラムに不正な JavaScript をロードするコードを挿入したことが判明した。この不正なコードにより、フォームに入力されたカード情報等がテキストファイルに保存されるようにされており、攻撃者はこのテキストファイルから、顧客情報を不正入手したと考えられる。EC システムの運用作業は委託先の事業者が行っており、届出者は使用されているソフトウェア名を知らず、その脆弱性の存在を把握していなかった。再発防止に向けて、フォレンジック調査結果を踏まえたセキュリティ設計による新システムを構築し、現行システムからの移行を検討している。また、脆弱性対策やインシデント対応等のポリシーおよび運用手順の確立、定期的なペネトレーションテストの実施等を行う予定である。
63	2021/12/16	届出者（企業）が運用する EC サイトに、不正なファイルが存在する可能性があるとの連絡を外部機関より受けた。また、クレジットカード会社から、EC サイト利用者のカード情報が漏洩した懸念があるとの連絡があった。調査したところ、EC サイトで利用していたプラグインにクロスサイトスクリプティングの脆弱性があり、攻撃者にその脆弱性を悪用されて、不正なファイルを設置されていたことが判明した。また、決済を行うプログラムが改ざんされていたことにより、1 万人以上のクレジットカード情報が漏洩した可能性があることも判明した。再発防止策については検討中である。

項番	届出日	概要
64	2021/12/17	届出者（企業）が運営する EC サイトに対して不正アクセスがあり、個人情報が漏洩した恐れがあることが発覚した。サイトの制作・保守作業を委託している業者からの報告により、本件を認知した。調査により、EC システムのソフトウェアにクロスサイトスクリプティングの脆弱性が存在していたことが判明し、当該脆弱性を悪用した不正アクセスを受け、データを窃取されたと推測している。当該 EC サイトは閉鎖し、ソフトウェアの脆弱性対策を行った。また、WAF を導入してセキュリティの向上を図るとしている。
その他の脆弱性悪用の事例		
65	2021/7/1	届出者（企業）が運営する EC サイトの会員情報が、インターネット上に不正に掲載されているとの連絡が警察からあった。調査の結果、ウェブサイトが SQL インジェクション攻撃を受け、会員情報に不正アクセスされた痕跡が見つかった。本件の対応として、新規会員の登録受付を停止し、サーバから会員情報を消去する処置を行った。また、再発防止策として、ウェブサイトの SQL インジェクションの脆弱性の修正、本件攻撃の発信元 IP アドレスを含む海外からのアクセスを遮断する設定を実施した。
66	2021/7/9	届出者（企業）の運用するウェブサイトが、本来とは異なる表示になっていたことに届出者が気づき、何者かにウェブサイトを改ざんされていたことが発覚した。調査により、脆弱性診断ツールによる探索が行われた形跡があったことから、攻撃者はツールを悪用してウェブサイトの脆弱な箇所を見つけ出し、それを悪用することで、不正侵入して改ざんを行ったと推測される状況であった。改ざんへの対策として、CMS において入力内容のチェック処理の追加、権限設定の変更、管理画面へのアクセス制限を設定した。また、ウェブサイトの運用会社には作業の都度記録を残すこと、サーバ管理会社にはシステムログを記録し定期的に提供することとして、作業管理や運用監視の手順や体制を整備した。

項番	届出日	概要
67	2021/7/19	届出者（企業）が提供するサービスにおいて、数十万件の認証情報が漏洩した可能性があることが判明した。本件の発覚の契機は、定期的に実施していたドメインコントローラへの検査において、不審なアカウントが作成されていたことを発見したことである。調査により、同システム内の認証基盤において、不正なプロセスが作成されていること、およびそこからドメインコントローラに対して不正なアクセスが発生していることが判明した。原因は、認証基盤で利用しているアプリケーションの脆弱性を攻撃者が悪用したことと推測している。再発防止のための対策として、WAF、IPS、EDR といった防御や監視のシステムを導入するとともに、脆弱性管理と対策の手順を見直し、体制の整備を行った。
68	2021/8/30	届出者（企業）が運営する EC サイトが、SQL インジェクション攻撃を受け、数十万件の顧客情報が漏洩する被害に遭った。データベースサーバの負荷が増大していることに担当者が気づき、調査を行ったところ、一部にプレースホルダを用いずに実装していた箇所があり、そこに対して、特定の発信元から通常は生じない大量（毎秒 6 回程）のアクセスがあったことが判明した。損失は総額で 2 億円以上になる見込みである。対策として、ソースコードを見直し、SQL インジェクションの脆弱性になり得る箇所について、エスケープ処理やプレースホルダ使用などで実装を修正した。また、第三者機関による脆弱性診断を行い、指摘事項への対策を実施した。今後は、ソースコードの複数名でのレビューや定期的な脆弱性診断を行う予定である。 ※本事例は 5 章で紹介する。

項番	届出日	概要
69	2021/9/21	届出者（企業）のウェブシステムにおいて、内部データに異常を発見したため、調査を行ったところ、不正アクセスにより、内部データの改ざんや窃取の被害を受けていたことが判明した。また、同じ時期にウイルス感染を狙ったとみられる、届出者を差出人に装ったなりすましのメールが数十通ほど確認されたが、不正アクセスで窃取された情報を悪用されたものかは不明である。当該ウェブシステムには SQL インジェクションの脆弱性が存在していたことを確認したことから、攻撃者はこの脆弱性を悪用して認証を回避して不正にログインしたのちに、データの改ざんや窃取を行ったものと推測される状況であった。対策として、プログラムを修正して SQL インジェクションの脆弱性を解消し、さらに認証方式の追加を行うことでセキュリティ強化を図った。
70	2021/10/11	届出者（企業）が利用するクラウド上のサーバにおいて、カナダの仮想通貨のマイニングサイトへの意図しないアクセスが発生した。本件は、想定していないドメインからのアクセスがあったことを届出者自身が発見したことで発覚した。原因は、サーバ上で稼働していたアプリケーションに脆弱性があり、攻撃者に当該脆弱性を悪用されたことで、外部からの不正アクセスを受けた可能性があるとしている。対策としては、当該アプリケーションソフトの修正プログラムを適用して脆弱性を解消し、さらに再発防止のため、クラウド上の WAF のバージョンアップや、EDR を導入してクラウド環境の監視強化を行うなどしてセキュリティの向上を図った。

項番	届出日	概要
71	2021/10/12	届出者（企業）のウェブサイトに対して SQL インジェクション攻撃が行われ、顧客のメールアドレスが十数万件窃取された。窃取されたメールアドレス宛に迷惑メールが送信され、受信した顧客からの連絡により本件が発覚した。調査により、当該ウェブサイトではURLパラメータの妥当性の確認を行う処理が実装されていなかったことが判明した。サイト内の商品紹介ページに対して、URL パラメータを悪用した SQL インジェクション攻撃が 5 日間で数十万回行われたことも判明した。本件の対応として、当該処理を実装して脆弱性を解消し、また、データベースに保管するデータの一部は暗号化した状態で保管するように処理を追加した。その上でさらにセキュリティを高めるためのシステムの再構築に着手した。本件によって、プログラム改修の対応に担当者 1 名が 10 日間、メールアドレスが流出した顧客へのお詫びの通知対応に担当者 2 名が 2 日間、顧客からの問い合わせ対応に担当者 2 名が 2 週間以上連日対応することになった。
72	2021/10/27	届出者（企業）が運営するサービスにおいて、サービス利用者が所有する一部の NFT（Non-Fungible Token）が外部に流出する事案が発生した。届出者が不審な取引ログを発見し、詳細に解析を行ったことで発覚した。原因は、取引を行うプログラムにセキュリティ上の脆弱性が存在していたため、攻撃者に権限を掌握され、不正に所有権を移動する取引が実行されたためと判明した。対策として、暗号化アルゴリズムの強化や実行権限の制限等により、プログラムの修正を行って脆弱性を解消した。さらにトランザクションを監視するシステムを導入して、再発防止を図ることとした。

項番	届出日	概要
73	2021/10/27	届出者（企業）がクラウド環境上に構築した EC システムに不正アクセスがあり、メール送信機能を悪用されて数百通の不審なメールが送信された。不審メールは、その内容からアカウント情報の詐取を目的としたフィッシングメールと思われる。メールサービス事業者が大量のメール送信を検知し、不審メール送信に悪用されている疑いがあるため、アカウントのパスワードを変更した。その連絡を受けて届出者は本事象を認知した。届出者は、EC システムにおいて、本番環境とは別にデバッグモードに設定していたテスト環境を使用しており、本件ではそのテスト環境が不正アクセスを受けた。デバッグモードでは、特定のリクエストを送信するとメールアカウントの ID やパスワードを確認できる機能があり、状況から攻撃者に本機能を悪用されて認証情報を窃取され、不正アクセスを受けたと推測している。再発防止策として、デバッグモードは原則使用しないこととし、使用する場合は IP アドレスによるアクセス制限を必須とした。また、WAF を導入してセキュリティの向上を図ることとした。
74	2021/11/3	届出者（企業）が運用する会員サイトにおいて、夜間にアクセス数が大幅に増加していることを検知した。調査により、会員情報取得のリクエストが大量に行われていたことが判明し、不正アクセスを受けて個人情報を窃取された可能性があると判断した。さらに調査したところ、アプリケーションに脆弱性があり、内部の情報が第三者から閲覧できる状況であったこと、および外部公開不要のサーバがインターネットからアクセス可能であったため、不正なリクエスト送信の踏み台にされていたことが判明した。本件を受けて、同一 IP アドレスからの短期間の大量アクセスを遮断する仕組みの導入、従業員による定期的なモニタリングの実施、会員情報取得リクエストの方式変更を実施した。

項番	届出日	概要
75	2021/11/9	届出者（教育・研究機関）が利用していた外部のウェブサービスの提供事業者のサーバが、不正アクセスによって改ざんされた。サービス提供事業者からの報告により届出者が認知した。調査により、不正なコードを書き込まれたことにより、データベースから個人情報を含む 1 万件以上のデータが盗み見られた可能性がある。対応として、当該ウェブサービスを停止して、関係者に説明と謝罪を行った。不正アクセスの原因は、サービスで利用していたミドルウェアに脆弱性が存在していたことであり、攻撃者に悪用されて改ざんが行われたと推測される状況であった。また、本脆弱性の情報が公開されてから被害発生までの 2 か月ほどの間、脆弱性対策はされていない状態であった。これは、修正プログラムの適用作業の計画が、サービス提供事業者の他業務により遅れたことによる。再発防止策として、脆弱性診断の実施、脆弱性対応のルールや体制の構築、WAF の導入等を実施するとしている。
76	2021/11/11	届出者（地方自治体）がウェブサイトの運用業務を委託している事業者から、届出者のウェブサイトに不正アクセスされた痕跡があるとの連絡があった。この事業者は外部からの通報により不正アクセスを認知したとのことであった。調査したところ、ウェブシステムに SQL インジェクションの脆弱性があり、個人情報等が漏洩した可能性があることが判明した。また、1 年前から不正アクセスされていた痕跡があったことも判明した。本件を受けて、一部機能の制限やウェブサイトへの WAF の導入といった対策を行った。また、届出者は事業者に対して、事案発生時の情報提供の手順に不備があり、状況把握に手間取ったとしており、改善の検討を依頼している。

項番	届出日	概要
77	2021/12/9	届出者（地方自治体）が使用するメールアカウントから、不審なメールが送信されていることを確認した。調査したところ、届出者が管理するウェブシステムにSQLインジェクションの脆弱性が存在しており、攻撃者に当該脆弱性を悪用されたことで、メールアカウントおよびパスワードを窃取され、不審メールを送信されたことが判明した。本システムでは、ファイアウォールや IDS・IPS といったセキュリティ機器を導入していたが、SSL/TLSおよびSSHなどの暗号化したトラフィックを検査する機能は利用しなかったことや、SQL インジェクション攻撃の振る舞いを検知する機能を持っていなかったため、この攻撃を防御できなかったと考えている。再発防止に向けて、プログラムの修正を行い脆弱性の解消をした。また、セキュリティ診断の実施および WAF の導入を検討している。
78	2021/12/21	届出者（一般団体）のウェブサイトに対して、通常のアクセス数を大幅に超える 1 日あたり数万件の大量アクセスがあったことを発見した。運用保守を行う事業者と分析を行った結果、これらの通信はサーバ内に保存していた顧客のメールアドレスを窃取する不正アクセスであったことが判明した。さらに調査を行ったところ、ウェブサイトに SQL インジェクションの脆弱性が存在することが判明したことから、攻撃者に当該脆弱性を悪用されて、個人情報が窃取されたと考えられる状況であった。脆弱性の修正を行い、意図しないデータベース通信は遮断するようにシステムを変更するなどの対処を行った。
79	2021/12/21	EC サイトを運営する届出者（企業）に対して、クレジットカード会社から、当該 EC サイトを利用した顧客のカード情報が漏洩している恐れがあるとの連絡があった。このため、カード決済機能を停止した上で、専門業者へフォレンジック調査を依頼したところ、EC サイトに SQL インジェクションの脆弱性があったこと、攻撃者からその脆弱性を悪用され 1000 件以上のカード情報が窃取された恐れがあることが判明した。本件を受け、不正アクセスを受けたサイトは閉鎖し、脆弱性対策を実施した新サイトを構築して移行した。新サイトにおいては脆弱性診断テストの実施を予定している。

項番	届出日	概要
80	2021/12/21	届出者（個人）が管理するサーバに対して、Log4j の脆弱性を悪用した攻撃があった。本件は、不正なコードを含んだメッセージを受信した際に、意図しないメッセンジャーアプリにメッセージ送信がなされたことに気づき発覚した。対策として、Log4j を最新版に更新した。
81	2021/12/22	届出者（企業）のサーバに不正アクセスがあり、コインマイナー等の不正なプログラムを設置され、サーバ負荷が上昇する被害があった。本件は、監視システムやセキュリティソフトが異常を検知したことにより発見した。原因等の詳細は不明であるが、届出者は状況から Log4j の脆弱性を悪用した攻撃を受けたものと推測している。対応として、脆弱性対策の処理を行った上で、現在もサーバのベンダやユーザサポートの業者とともに詳細を調査中である。

2-4. ID とパスワードによる認証を突破された不正アクセス

今期も、利用者やシステム管理者による ID やパスワード運用・管理の問題による不正アクセス被害の届出が多かった。なお、複数の要因が疑われる事例についても、届出者が ID やパスワード管理に問題があったことが原因と考えているものは本節に分類した。ただし、VPN 装置等の脆弱性により窃取された ID やパスワードの悪用で認証を突破されたと考えられる事例は 2-3 節（一部 2-2 節）に分類しており、本節には含めていない。

攻撃対象にされたものはメールシステムが多く、特に大学などの教育・研究機関において、メールサーバやアカウントへ不正にアクセスされ、フィッシングメール等の不正なメール送信の踏み台にされてしまったという事例が多かった。一部の事例には、SMTP 認証の ID とパスワードを突破されたと思われるものがあった。SMTP は古くから使用されているプロトコルで、多要素認証などの認証方式には対応していないこともあるため、不正アクセスの防止には ID とパスワードの強度や管理方法が重要な要素となる。しかし、組織の拡大などにより、メールシステムの利用者が増えると、脆弱なパスワードの使用や、他サービスで使用している ID やパスワードを流用する利用者も増える恐れがある。利用者全員に強固なパスワードの設定を促すなどの教育・啓発をしていくことが重要であることに変わりはないが、個人の管理だけに委ねず、接続元 IP アドレスの制限や多要素認証に対応したシステムへの移行等、システムによる対策を併用することが望ましい。

なお、再発防止に向けた対策として、多要素認証方式の導入をあげる届出者が多かった

が、今期は、二要素の認証を導入していたが、特定条件下でパスワード認証のみでシステム利用が可能になってしまったなど、想定通りに機能せず不正アクセスにつながってしまった事例が複数見られた。例えば海外にいる等で SMS 認証が利用しにくい状況でもシステムが利用できるようになど、利用者の利便性のために、使用環境に応じて認証方式を変更するといったセキュリティ設計が求められることもあり得る。しかし、その場合は特定条件下で脆弱な状態が生じないかなどを十分に確認し、必要であれば別の技術によるセキュリティ対策を加えることが必要となる。

多要素認証の導入やアクセス制限を行っても、完全に不正アクセスを防げるような万全のものではない。しかし、適切に設定を行った複数の技術を組み合わせてセキュリティ対策を行うことにより、パスワードのみといった単一の認証方式に比べ、セキュリティは大幅に向上する。積極的に導入を検討していただきたい。

表 2-4 に ID とパスワードによる認証を突破された不正アクセスに関する届出の概要一覧を示す。

表 2-4 ID とパスワードによる認証を突破された不正アクセスに関する届出の概要一覧

項番	届出日	概要
メールシステムへの不正アクセスの事例		
82	2021/7/1	届出者（企業）が使用するクラウド型のメールサービスにおいて、管理者アカウントのアクセス履歴を確認したところ、2 つのアカウントに対して、海外の IP アドレスから不審なログインの試行が行われていたことを発見した。調査により、いずれも、ログインには失敗しており、被害はなかったことを確認している。その後も数日にわたり、1 日あたり 1000 回以上のログインの試行が見られたため、対策として、一時的にアカウントのロックを行ったところ、ログイン試行は見られなくなった。更なる対策として、管理者アカウントには二要素認証を導入した。一般アカウントへも導入を検討している。
83	2021/7/7	届出者（教育・研究機関）が利用する認証システムのレポート通知機能を有効化したところ、海外からの不審なログイン履歴が確認された。調査したところ、1 件のメールアカウントに対して不正なログインがあり、スパムメール送信に悪用されていることが判明した。不正にログインされた際にメールアカウントに保存されていた情報が不正に閲覧された可能性もある。メールサービスへのログインには多要素認証を有効にしていたが、特定条件下で認証要求が行われた際には、パスワードのみで認証可能となる場合があることが判明し、何らかの手段でパスワード認証を突破されたことが原因と推測している。対策として、不正アクセスされたアカウントのパスワードを初期化し、また、特定条件下においては認証を拒否する設定を行った。さらに、不審メールの注意喚起、パスワードの使いまわし禁止についての周知徹底、情報セキュリティ対策についての指導、研修を強化した。

項番	届出日	概要
84	2021/7/8	届出者（企業）が利用するメールサーバの管理者から、あるメールアカウントのパスワードを変更したとの連絡があった。当該アカウントから 1000 通ほどのメールが送信されていたため、不正アクセスの可能性を考慮したとのことであった。調査したところ、使用しなくなったメールアカウントが削除されておらず、パスワードが推測されやすいものとなっていたことが判明した。このため、攻撃者によって、パスワードが推測されて当該アカウントに不正アクセスされ、メール送信の踏み台にされたと推測される状況であった。対策として、メールアカウントの点検と不要なアカウントの削除、利用中のメールアカウントのパスワードが強固なものとなっているかの確認を行った。
85	2021/7/9	届出者（企業）が利用するクラウド型メールサービスで、従業員 3 名のアカウントに不正にログインされ、過去のメールが流出した。さらに、流出したメールが本文に引用され、当該従業員を差出人に装ったフィッシングメールが、別の従業員宛に送られたことも判明した。不正にログインされた原因は、別のサービスで使用していた ID とパスワードを本サービスにも使い回していたことと推測している。対応として、当該従業員にメールサービスと業務利用の各システムのパスワード変更を指示した。メールサービスについては、多要素認証の導入と、ログイン試行の回数制限と監視の設定を行い、パスワードの入力を一定回数誤った場合にはアカウントをロックしたり、危険なログインを検知し通報したりする仕組みを導入した。さらにパソコンのウイルスチェックや、メール以外のシステムへの多要素認証の導入検討、インシデント発生時の手順と体制の整備、全社員への社員教育を実施予定である。

項番	届出日	概要
86	2021/7/21	届出者（企業）のメールアカウントから不審なメールが送られてきたと、外部組織より報告を受けた。調査したところ、メールアカウントに不正なログインがされており、ウイルスに感染させる目的の攻撃メールが送信されていることが判明した。メールサービスには多要素認証を設定していたが、設定に不備があり、特定の条件においては、ユーザ ID とパスワードのみでログインできる状況であった。また、不正アクセスされたメールアカウントのパスワードは他の外部サービスで利用していたパスワードと同一であったこと、および当該パスワードが漏洩していたという情報を確認している。すなわち、外部サービスのセキュリティインシデントにより漏洩したパスワードが、本件で悪用されたと考えている。本件を受けて、アカウントのパスワード変更、アクセス監視や利用監視のシステム導入等を行っている。
87	2021/8/2	届出者（教育・研究機関）の職員が、身に覚えのないメールの送信履歴があったことに気づき、システム担当者に報告した。調査したところ、当該職員のメールアカウントに不正なログインがあり、5 千通以上の不正なメールが送信されていたことが発覚した。対応として、当該メールアカウントのパスワードを変更し、不正なメールが送信された宛先に対して削除を依頼するメールを送った。再発防止策として、パスワード管理の徹底を周知し、認証方式を ID とパスワードを用いた認証から、OAuth を用いた方式に変更した。

項番	届出日	概要
88	2021/8/23	届出者（企業）が使用するクラウド型のメールサービスにおいて、海外の従業員のメールアカウントに不正アクセスがあり、組織外のメールアドレス約 200 件を含む、国内外の約 600 件の宛先にフィッシングメールが送信された。フィッシングメールを受信した社内の従業員から情報セキュリティ部門に多数の報告があり、本件が発覚した。調査の結果、不正アクセスされたアカウントを使用していた従業員が、以前に別のフィッシングメールを受信した際に、メールから誘導されたフィッシングサイトで、ID やパスワードの情報を入力していたことが判明した。攻撃者がフィッシングサイトで窃取した認証情報をもとに、当該従業員のアカウントへ不正にログインして、参照可能なメールアドレスのリストを窃取し、フィッシングメールを送信したと推測される。本件への対応として、当該アカウントの即時停止、フィッシングサイト URL へのアクセス制限の追加、従業員への注意喚起を行った。さらに再発防止策として、情報機器の運用管理方法の見直しや、多要素認証の導入などによる認証基盤の強化を予定している。
89	2021/8/31	届出者（教育・研究機関）において、1 つのメールアカウントに不正なログインがあり、数万通のフィッシングメールが送信されていた。本件は、メールシステムを提供・運用していた事業者の監視で発覚した。不正アクセスの原因は、当該アカウントの使用者が過去、フィッシングメールに誘導され、パスワードなどの認証情報を詐取されてしまったことと推測される。本件が発覚した際、メールシステム事業者が当該アカウントのパスワード変更を行うことにより当面の対策とした。再発防止策として、定期的なパスワード変更を必須とし、また組織内でフィッシングメールのサンプルを活用した教育を行うこととした。

項番	届出日	概要
90	2021/9/15	届出者（企業）の従業員を差出人に装った、フィッシングメールが社内外に数十通送信されたことが、メール受信者からの報告により発覚した。調査したところ、従業員が使用するメールアカウントに、本人の心当たりがない転送設定がなされていることを確認した。このことから、何らかの手段によりパスワード認証を突破した攻撃者が、メールサービスのアカウントに不正アクセスし、転送設定によるメールの窃取や、不正メールの送信を行ったと推測される状況であった。対応として、差出人とされた従業員のアカウントのパスワードを変更したが、約 1 か月後に同社の別のメールアドレスを差出人としたフィッシングメールが確認された。このため、全従業員のパスワード変更を行った。再発防止策として、セキュリティ規程の変更を計画している。
91	2021/9/17	届出者（教育、研究機関）において、職員のメールアカウントの 1 つが不正使用され、組織外に 4 日間で合計数万通の不審なメールが送信された。当該職員宛に配送エラーを通知するメールが大量に届いたことにより発覚した。本インシデントにより、担当者 2 名が 1 日間、計画外の対応を行った。メールアカウントが不正使用された原因は不明だが、調査の過程で当該職員が他のサービスで使用していたパスワードを使い回していたことが判明したため、そのサービスから攻撃者にパスワードが窃取されたものと推測している。再発防止策として、適切なパスワードの管理を全職員に周知した。また、メールアカウントの認証に多要素認証を導入予定である。
92	2021/10/20	届出者（企業）のメールサーバにおいて、大量のメールが配信されたことを示すアラートが発せられた。調査したところ、メールアカウントに不正アクセスがあり、乗っ取られたメールアカウントからフィッシングメールと思われるメールが大量に送信されていることが判明した。対応として、当該アカウントのパスワードを変更したところ、以降は同事象が発生していない。攻撃者は何らかの手段でパスワードを窃取して不正アクセスを行ったと考えているが、原因は不明である。

項番	届出日	概要
93	2021/10/27	届出者（一般団体）が利用していたメールサーバから、数百通の迷惑メールが送信されていた。メールサービスの事業者が発見して、届出者に連絡したことで届出者が認知した。原因は、メール送信に 1 つのメールアカウントを共有しており、当該アカウントのパスワードに脆弱なものを設定していたことから、攻撃者にパスワードを推測されてしまい、不正にログインされ、迷惑メール送信に悪用されたものと推測される。対応として、利用していた全アカウントのパスワードを変更するとともに、メールサービス事業者から入手した送受信ログを元に関係者等へ連絡を行った。再発防止策として、パスワードポリシーを改訂して、複雑なパスワードを必須とし、さらに定期的な変更などパスワードを一括管理する機能を導入した。また、不審メールの送受信を確認した場合の報告を徹底するように教育を実施する予定である。
94	2021/11/16	届出者（教育・研究機関）が利用するメールサービスにおいて、組織の職員を差出人に装った不審なメールが、1 日に数百通送信されていたことが確認された。調査により、当該職員のメールアカウントに不正アクセスがあり、大量の不審メールが送信されたこと、およびメールボックスに保存していたメールを窃取された可能性が発覚した。さらに調査を行ったところ、海外から不審なログインの試行があり、その回数に対する成功率が高かったことが判明したため、攻撃者が何らかの方法で入手した当該アカウントの認証情報を悪用して不正アクセスしたものと推定される状況であった。発覚後、すぐにアカウントのパスワードを変更して対策を行った。また、再発防止のための対策として、多要素認証の導入を行う予定である。

項番	届出日	概要
95	2021/12/2	届出者（教育・研究機関）の関係者が利用するメールサーバのアカウントが乗っ取られ、数十万通のメールが送信された。本件は、メールサービス利用者に大量のエラーメールが着信しているとの連絡により発覚した。調査により、不正なログインは海外の IP アドレスから行われていたことと、送信されたメールはフィッシングメールであることが判明した。対応として、パスワードを変更したところ、以降は同事象が発生していない。攻撃者が何らかの手段でパスワードを窃取し、不正アクセスしたと考えているが、原因は不明である。対策として、組織外アドレスからのアクセス制限、不正なログインの試みを監視する仕組みの導入を行った。なお、将来的に当該サーバは廃止する予定とし、移行等の調整を進めている。
96	2021/12/14	届出者（業界団体）のメールアカウントに不正アクセスがあり、当該アカウントから数万通もの不審なメールが送信された。本件は、送信エラーを通知するメールが大量に届いたことに気づき、発覚した。調査により、職員が過去にフィッシングサイトへ当該アカウントのパスワードを入力してしまった恐れがあることが判明した。フィッシングサイトで詐取された認証情報が攻撃者に悪用されて、不正アクセスを受けたことが原因と推測している。対策として、当該アカウントのパスワード変更、当該メールアドレスの利用停止、ファイアウォールの設定変更等を行った。
その他の ID とパスワード認証突破による不正アクセスの事例		

項番	届出日	概要
97	2021/7/2	届出者（企業）がクラウド上に構築中だったウェブサーバが不正アクセスの被害に遭った。クラウドのモニタリングツールが異常を検知したことで発覚した。システム構築作業は業者と協業で実施していたが、作業時の利便性のため、管理者権限のある、構築作業用アカウントに比較的簡易なパスワードを設定していたことが原因で、攻撃者にパスワードを推測され、不正ログインされたものと考えている。また、不正ログインにより、攻撃者から、ウェブサイトの改ざんや、ウェブシェルと呼ばれる不正プログラムの挿入などの操作が行われたが、本番稼働前のシステムであったため、情報漏洩の被害はなく業務影響は小さかった。対策として、作業用アカウントの ID とパスワードの変更、CMS プラグインの整理と更新、接続元 IP アドレスによるアクセス制限等を行った。
98	2021/7/6	届出者（企業）が利用するノートパソコンに不正アクセスされ、管理者アカウントのパスワードが変更されていることを発見した。また、その影響により、社内ネットワークへの VPN 接続ができなくなった。調査したところ、不正アクセスされたノートパソコンには、グローバル IP アドレスが割り当てられていたこと、およびインターネットからのリモートデスクトップ接続が許可されていたことが判明した。推測されやすいパスワードを設定していたことから、外部からリモートデスクトッププロトコルで接続され、パスワード認証を突破されて、不正アクセスを受けたと推測される状況であった。本件を受けて、ファイアウォールの設定見直し、管理者アカウントの削除、パソコンの OS アップデートや脆弱性管理体制の導入を行った。

項番	届出日	概要
99	2021/7/13	届出者（企業）が運営する EC サイトから、クレジットカードの有効性チェックの要求がクレジットカード会社のシステムに対して大量に行われていることが発覚した。クレジットカード会社からの連絡により届出者が認知した。調査の結果、過去に運営していた旧サービスの会員アカウント 3 つに不正アクセスを受け、会員が使用するクレジットカードの登録・変更機能を悪用されて、約 15 万回という大量のカード有効性チェックが不正に行われたことが判明した。対応として、クレジットカードの登録・変更機能を停止するとともに、EC サイトの全アカウントに対するログインを一時的に停止した。不正使用された 3 アカウントについてはパスワードの強制リセットを行った。原因は、旧サービスでは ID とパスワードのみでログインが可能となっていたことから、パスワードリスト攻撃により、3 つのアカウントが不正アクセスされたためと推測している。再発防止策として、旧サービスのアカウントによるログインの停止、二要素認証の導入、大量アクセスの監視、および EC システムの改修を行った。
100	2021/7/30	届出者（企業）のウェブサイトが改ざんされ、フィッシング目的と思われるウェブコンテンツが不正に作成されていたことが発覚した。届出者は、関係会社からの連絡を受け本件を認知した。対応として、発覚から対策完了まで当該ウェブサイトを停止した。原因は、ウェブシステムの構築時に作成したアカウントが、簡易なパスワードのまま長期間放置されていたことを確認したことから、何らかの手段でパスワード認証を突破した攻撃者に、アカウントを悪用されたことと推測している。未使用のアカウントが放置されていた理由としては、システム担当者が変更になった際に、アカウント情報を含むシステム管理情報が適切に引き継がれていなかったことがある。対策として、アカウントの整理とパスワードの変更、ウェブサーバ上の全てのコンテンツを削除した上で、ウェブサイトを再構築した。また、再発防止に向けて、改ざん検知・防止のシステムを導入した。

項番	届出日	概要
101	2021/8/24	届出者（企業）が運用するウェブサイトが改ざんされ、スマートフォンからアクセスした際に、出会い系のサイトへ遷移するように設定されていたことを、従業員が発見した。調査により、サイトを管理している CMS のアカウントに不正なログインがあり、サイト内のデータを改ざんされていたことが判明した。CMS のアカウントのパスワード認証が突破された原因は不明である。本件を受けて、CMS のアカウントのパスワード変更を実施した。
102	2021/8/25	届出者（企業）が運営するウェブサイトに不正アクセスがあり、数十人分の利用者の個人情報等が流出した。利用者から問合せがあり、調査を行ったところ、不正アクセスの痕跡を発見した。原因については、当該ウェブページのアクセス数が通常の 1 万倍近くに増えていたことなどから、総当たり攻撃によって、パスワード認証を突破されたと推測される状況であった。対応として、ウェブサイトを停止して、攻撃を受けたページを含むウェブサイトの脆弱性診断を実施した。脆弱性診断における重要度の高い指摘事項についてはすぐに対応を行った。再発防止策として、連続してログインが失敗した場合にアカウントをロックすることによる総当たり攻撃対策や、ログ管理プロセスの整備、脆弱性診断の全指摘項目への対応などを行っている。なお、セキュリティ施策を見直した運用案を検討しており、完了後にウェブサイトを再開する予定としている。

項番	届出日	概要
103	2021/9/10	届出者（企業）が運営する EC サイトからの 1500 件以上のクレジットカード情報の漏洩が、カード会社からの連絡をきっかけに発覚した。調査したところ、システムにバックドアが設置されていたことが判明したため、それにより、不正アクセスを受け、システムの管理機能を悪用されたものと推測しているが、詳細な手口は不明であった。原因は、管理アカウントの認証パスワードが脆弱であったことから、攻撃者にパスワードを推測され、認証を突破されたことと考えている。本件を受け、社内のパスワードポリシーを強化した上で、それに準じたパスワードに変更を行った。また、システムを構成するソフトウェアの一部のバージョンが古く、脆弱性が存在していた可能性も考えられたため、再発防止策の一環として、ASP サービスのプラットフォームに移行し、新たなシステムを再構築した。
104	2021/9/16	届出者（企業）が管理するウェブサイトが不正アクセスを受け、アクセスすると無関係の海外のサイトへ自動的に遷移するように改ざんされていた。本件は、外部からの報告により発覚した。調査の結果、CMS の管理画面に対し、管理者権限を持つアカウントにより、不正にログインされていたことが判明した。原因として、当該アカウントのパスワードは容易に推測可能な脆弱なものであったため、攻撃者にパスワード認証を突破され、不正なログインを受け、ウェブサイトを改ざんされたものと推測された。対応として、ウェブサイトを停止し、CMS の全アカウントのパスワード変更を行った。その後で、公開前のコンテンツを管理するサーバにあった、改ざんをされていないファイル等を用いてウェブサイトを復旧した。再発防止のための対策として、CMS のアカウントを整理して、不要なアカウントを削除し、管理画面へのアクセスを社内のみに制限する措置を行った。

項番	届出日	概要
105	2021/9/22	届出者（企業）が管理するパソコンやサーバ数台に、複数の不審なファイルが設置されていた。本件は、セキュリティソフトがそれらのファイルをウイルスとして検知したことで発覚した。調査したところ、それらの不審なファイルはマイニングツールやバックドアを作成するツールであったことが判明した。攻撃者により、外部から不正アクセスを受け、ツール等を設置されたものと判断している。原因については、当該パソコン等ではインターネットからのリモートデスクトップ接続を許可していたため、辞書攻撃や総当たり攻撃で認証を突破され、外部からのリモートデスクトップ接続により、侵入されたものと推測している。本件を受け、パスワードの変更や、インターネットからの直接通信を防止するためのルータを設置する等の対応を行った。
106	2021/9/30	サーバ事業者からの連絡により、届出者（一般団体）が以前に使用していたクラウド環境上の仮想サーバに不正アクセスがあったことが発覚した。被害状況を調査したところ、届出者と無関係のサーバに対する攻撃の踏み台に悪用されていたことが判明した。なお、攻撃対象となったサーバへの攻撃が成功した形跡は確認されていない。また、不正アクセスを受けたサーバについては、サーバ内に保管されていた個人情報を含むデータが不正に閲覧された可能性があることも発覚した。本サーバは、過去にインターネットから SSH で接続できるように設定を行い、使用していたが、サーバの使用停止以降も、管理者と運営者との間で取扱いを決めておらず、稼働状態を継続していた。さらに、外部からの接続パスワードが一般的な語彙の文字列を入れ替えたものにしていたことから、攻撃者による総当たり攻撃によって、パスワード認証が突破されたことが原因と推測している。再発防止策として、使用していないサーバは完全に廃止し、サービスの基盤をレンタルサーバのサービスから、届出者によるサーバ管理が不要なブログサービスへ移行した。あわせて、不要なアカウントの削除や多要素認証の導入によりセキュリティ強化を図った。

項番	届出日	概要
107	2021/10/13	届出者（教育・研究機関）が管理するウェブサイトにアクセスすると、届出者と無関係の内容が書かれたページや、エラー画面が表示されるなど、正しく表示がされない状態になっていた。ウェブサーバを調査したところ、一部ファイルの改ざんや、心当たりのないファイルが見つかった。さらに詳しく調査したところ、フィッシングサイトへの改ざんや、ウェブシェルと呼ばれる不正プログラムの挿入、メール送信機能を持つウェブページの追加などが行われていたことが判明した。不正アクセスによる改ざんがされたと考えられる状況であった。原因は、CMSの管理用ID･パスワードが類推しやすいものであったことから、パスワード認証を突破されて不正にログインされたことと推測している。本件への対応として、当該ウェブサイトのサブドメイン登録を削除することでURLによるアクセスを不能にして、その後ウェブサーバの停止を行った。再発防止策として、管理者IDの無効化、強度の高いパスワードへの変更を実施した。また、被害発生時にサーバ運用事業者との連絡がつかず緊急対応が遅れたことや、アクセスログ保管期間が短く調査に難が生じたことへの対策として、運用事業者と協議し、責任範囲の明確化と連絡体制の整備、およびアクセスログの保存期間の延長を行った。
108	2021/10/13	届出者（教育・研究機関）で使用していたクラウドサーバから、1週間ほどの間に5万通を超える大量の迷惑メールが送信されていた。本件は、保守会社が発見して、届出者に連絡したことで発覚した。原因としては、当該クラウドサーバで利用していたアカウントのパスワード強度が弱かったことが判明しており、辞書攻撃等で不正にログインされたことによると推測される状況であった。なお、定期的にセキュリティ脆弱性診断を実施していたが、パスワードが脆弱であったことは発見できていなかった。対応としては、当該クラウドサーバは廃止し、セキュリティを考慮した上で別のサーバを再構築した。再発防止策には、類似サーバの見直しと、サーバ管理者に対するセキュリティ指導・啓発を行う予定である。

項番	届出日	概要
109	2021/12/10	届出者（企業）の従業員が個人的に利用するアカウントに対して、不正アクセスがあったことを確認した。この従業員は、個人で使用するクラウドサービスの ID マネージャーを用いて、所属企業のアカウントのパスワードを管理していた。個人アカウントに不正アクセスがあったため、企業用のアカウントのパスワードも窃取された可能性が考えられる。調査したが、個人的なアカウントに不正アクセスされた原因は不明であった。対応として、パスワードの変更を行い、念のためパソコンを初期化し再構築した。

2-5. その他

その他、ここまでの分類に該当しない届出事例を表 2-5 に示す。調査等を行っても原因が判明しなかったものや、現時点でも調査を継続しているものについても本節に分類した。届出者では原因不明とされたものであっても、中には、ソフトウェアの脆弱性の悪用や、パスワードなど認証情報の管理上の問題に起因していると推測される事例も見られた。直接的な原因は異なっていたとしても、前節までで述べてきた対策を行うことは、セキュリティ向上につながり、ウイルスや不正アクセスのリスク軽減に有効であると考えられるため、2-3 節や 2-4 節の内容も参考にしていただきたい。

表 2-5 その他の届出事例の概要一覧

項番	届出日	概要
110	2021/7/8	届出者（企業）が運営する EC サイトが不正アクセスを受け、顧客のクレジットカード情報が窃取された。本件は、決済会社から、カード情報が漏洩している可能性について指摘があり発覚した。調査により、EC サイトで使用していた CMS において、認証済みのセッション ID が出力されたログファイルが、インターネットから閲覧可能な状態になっていたことが判明した。このことから、攻撃者にセッション ID を悪用した不正アクセスをされ、バックドアの設置をされた可能性があり、そこから、攻撃者はカード情報をサーバ内に記録するように決済機能を改ざんして、蓄積したカード情報を外部に持ち出したと推測される。本件を受け、クレジットカード決済を停止し、ウェブサイトに対してはアクセス制限や、発見した悪性ファイルの削除等の措置を行った。なお、ウェブサイトは再構築により復旧するが、被害を受けたサイトのデータは一切使用せずに新規で構築することとした。再発防止策として、CMS を定期的にアップデートすること、決済用のプラグインを PCI DSS に準拠したものにすることを検討している。
111	2021/7/15	届出者（企業）が運営しているウェブサーバにおいて、レスポンスが悪化し、ウェブサイトが表示できない状態になっていることを確認した。調査したところ、事象確認後から少なくとも 5 時間以上にわたり、SQL インジェクション攻撃を含む不正アクセスが試行されていることが判明した。対応として、ファイアウォールの設定を変更し、攻撃の発信元からの通信を遮断する措置を行った。なお、調査の結果、システムには SQL インジェクションの脆弱性は見つからず、アクセスログ解析の結果からも、SQL インジェクション攻撃の成功は無く、データの改ざんや流出の形跡は見つからなかった。再発防止として、WAF の導入を検討している。

項番	届出日	概要
112	2021/7/26	届出者（企業）が利用していたツールの提供元のサーバが不正アクセスされ、数千人のメールアドレス等の情報が漏洩した。本件の連絡を受け、届出者はツールの提供元に対して、セキュリティ体制の強化等を依頼した。
113	2021/7/29	届出者（教育・研究機関）がクラウド上に設置しているウェブサーバにおいて、データの改ざんや消去が行われた。検索サイトから当該ウェブサイトへアクセスすると、届出者と無関係のショッピングサイトへ遷移することを担当者が発見したため、バックアップデータを用いてウェブサーバのデータを復元してサイトを復旧させた。しかし、一度復旧させた後も、表示の乱れや、意図しないサイトへの自動遷移が確認されたため、サーバ内の全ファイルを確認したところ、複数のファイルが改ざんや消去されていたことが判明した。不正アクセスの被害を受けている可能性が強く疑われたため、ウェブサーバを一時停止した。不正アクセスの原因は調査中であるが、対策として CMS の定期的なアップデートや、サーバ OS のアップデート等を行う予定である。
114	2021/8/3	届出者（一般団体）が運営する会員向けのウェブサイトに不正アクセスがあり、数千人分の会員情報が漏洩した。本件は、アンダーグラウンドのサイトに届出者の情報が掲載されていることを発見した報道機関からの連絡により発覚した。原因については、外部機関との協力のもと、調査中である。対策として、ウェブサイトの常時 SSL 化や UTM の導入によるセキュリティ強化を推進しており、また再発防止の観点で、定期的な保守管理の実施に向け、保守業者と協議中である。

項番	届出日	概要
115	2021/8/3	メールを受信した外部組織からの連絡により、届出者（業界団体）のメールアカウントから、不審なメールが送信されていたことが発覚した。調査したところ、差出人とされたアカウントの使用者は、過去に当該不審メールに類似したメールを受信していた。このことから、原因はメールに記載されていたURLのリンク先にアクセスし、ウイルス感染させられたか、またはフィッシング等により認証情報を詐取されたと推測している。本件への対応として、差出人とされたアカウントを削除するとともに、ウイルス感染が疑われるため、使用者のパソコンは初期化した。さらに他の職員についても、メールアカウントのパスワード変更と、不審なアクティビティ履歴がないかを確認するようにした。
116	2021/8/18	ECサイトを運営する届出者（企業）に対して、決済代行会社から、クレジットカード情報が漏洩している懸念があるため、カードによる決済を停止するとの連絡があった。第三者機関によるフォレンジック調査を実施してもカード情報の漏洩の痕跡は確認されなかったが、本事案を受けて、各種アカウントの再発行、各種ソフトウェアの最新版への更新、クラウドサービスの管理コンソールアクセス時の二要素認証の導入、脆弱性診断の実施と発見された脆弱性への対応、およびセキュリティ機器のログ保存等を実施してセキュリティの強化を図った。
117	2021/9/14	届出者（企業）が提供している動画配信サービスおいて、本来は特定の利用者しか閲覧できない動画が不正にダウンロードされ、他の動画共有サイトにアップロードされていた。本件は、サービスの利用者からの報告により発覚した。原因としては、正確なURLを知っている場合のみ、動画へのアクセスできる仕組みであったところ、ファイルがCDN（Content Delivery Network）のキャッシュに保持されている間は、そのキャッシュデータにアクセスするためのURLが推測可能なものであったため、URLが特定されてしまったことと考えている。対策として、キャッシュ保持時間の短縮化、国内限定にサービス仕様を変更して、それに伴うアクセス元IPアドレスの制限の実施などを行った。社内体制の整備や社員教育も行う予定である。

項番	届出日	概要
118	2021/9/29	届出者（地方自治体）が業務を委託していた事業者のシステムに不正アクセスがあり、システムの利用者十数名分に関する情報が漏洩したことが判明した。届出者は委託先事業者からの報告により認知した。委託先事業者が外部専門家の協力のもと、調査を進めているが、届出の時点では原因は不明である。本件を受け、届出者は個人情報保護の遵守とセキュリティ体制強化に取り組むよう、委託先事業者を指導した。また、契約においてもセキュリティに関する条項を追加することを検討している。
119	2021/9/30	届出者（企業）のウェブサーバに不正アクセスがあり、サーバ内の処理が停止または遅延する事象が発生した。詳細は調査中であるが、外部から意図しないアクセスのログがあったこと、セキュリティソフトがコインマイナーを検知したことなどから、何らかの手口により、サーバに不正アクセスした攻撃者が、システム設定を改ざんして、サーバ本来のタスクを停止した上で、コインマイナーを設置して稼働させたものと推測される。不正アクセスの原因も調査中だが、OS コマンド・インジェクションの攻撃が行われたものと届出者は推測している。対策として UTM の導入やウェブシステムの認証に多要素認証を採用するなどの施策を行い、セキュリティの強化を図った。
120	2021/9/30	届出者（企業）が利用しているクラウドサービスにおいて、攻撃者に管理者キーを悪用され、不正にドメインが作成され DNS サービスに登録される事象が発生した。本件はクラウドサービスの事業者からの連絡により発覚し、即座にドメイン登録を削除した。調査したところ、不正に登録されたドメインが悪用されるなどの、他の被害は確認されていない。管理者キーが漏洩した原因について調査を行ったが特定には至らず、数年以上前に漏洩したものが今年に入って悪用されたものと推測している。再発防止策として、管理者キーの管理方法を変更して、通常時の使用を禁止する等の措置を行った。また、インシデントの迅速な検知と対応ができるように SIEM 環境の再構築を行った。

項番	届出日	概要
121	2021/10/12	届出者（企業）が運営する EC サイトが不正アクセスを受け、サイト内に不正なプログラムを設置された。この不正プログラムは、取引実行時にクレジットカード情報等を窃取するものであり、設置されていた間に行われた取引で使用された顧客数百名分のカード情報が漏洩した可能性があることが判明した。原因は、サーバにアクセスするためのパスワードが、何らかの方法で攻撃者に窃取されて悪用された疑いがあるが、調査では特定に至らず不明である。対策としては、当該サイトを新しい仕組みで再構築し、サーバへログイン可能な IP アドレスの制限、パスワードの定期的な変更を実施する予定である。加えて、EC システムを提供する事業者においても、セキュリティ強化のため WAF や監視サービスを導入する予定である。
122	2021/10/27	届出者（企業）の海外子会社社員が使用する、クラウド型メールサービスのアカウント 1 つが不正アクセスされ、同社員になりすましたフィシングメールが社内外に約 2500 通送信された。社内のシステム部門が本事象に気づき、調査を行ったが、不正アクセスの原因は特定できなかった。本事象による業務影響はなかったが、インシデントの収束までに数名の担当者が 3 日間ほど対応に追われた。再発防止策として、パスワードポリシーを強化した。また、海外子会社からクラウドサービスへのアクセス制御の設定を見直し、国内事業所で導入していたセキュリティ製品を海外にも適用して、国内と同様のアクセス制御を海外でも実施するようにした。

項番	届出日	概要
123	2021/11/10	届出者（一般団体）が利用するクラウド型のメールサービスにおいて、職員のアカウントに不正アクセスがあり、当該職員のアカウントからフィッシングメールが数百通送付された。本件は組織内の複数の職員からの報告と、メールサービスからの警告メールにより発覚した。調査により、不正アクセスは海外の IP アドレスから行われていたこと、およびフィッシングメールを受信した別の職員 1 名のアカウント情報が、フィッシングサイトを通じて詐取され、同一の IP アドレスから不正アクセスされたことが判明した。最初に被害を受けたアカウントへの不正アクセスの原因は、当該職員にヒアリングしたが心当たりがなく不明であった。対策として、海外 IP アドレスに対するアクセス制限、リスクベース認証の採用、フィッシング対策訓練の実施を検討中である。
124	2021/12/2	届出者（企業）が自社内に設置しているサーバから、大量のポートスキャンが行われていることを IDS が検知した。調査したところ、当該サーバに不正アクセスがあったことを確認した。また、ファイルサーバへの不正アクセスがあったことも判明し、一部のデータが窃取された可能性があることが発覚した。不正アクセスの原因は調査中であり、詳細が判明し次第、再発防止策を検討する予定である。
125	2021/12/22	届出者（企業）のウェブサイトが閲覧できなくなっていたことに気づいた。従業員が状態を確認するため、CMS へのログインを試みたがログインができず、FTP によるファイル操作で一時ウェブサイトを停止した。その後、ウェブホスティングの事業者から、サイトが改ざんされた懸念があるとの連絡があった。原因については不明であるが、攻撃者に何らかの手段で不正アクセスされ、ウェブコンテンツを改ざんされたものと推測している。対応として、関係する全システムのパスワードの変更、CMS への多要素認証の追加、WAF や監視機能の設定見直し等を行った上でウェブサイトを再開した。

3. 事例：侵入型ランサムウェア攻撃の被害

3-1. 概要

本章では、攻撃者が組織の内部ネットワークへ侵入し、管理サーバ等を侵害したのち、組織内システムがランサムウェアに感染させられた事例（侵入型ランサムウェア攻撃）を 3 つ紹介する。同種の攻撃の被害にあった組織からの届出が継続して多く寄せられており、被害によるビジネス影響が大きい傾向がある。

このような手口のランサムウェア攻撃について、IPA では 2020 年 8 月に「事業継続を脅かす新たなランサムウェア攻撃について」として注意喚起 [12]を行っている。さらに JPCERT/CC では、2022 年 1 月にこれらの手口を「侵入型ランサムウェア攻撃」と呼び、被害が発生した際の対応方法等を FAQ という形で紹介 [13]している。

侵入型ランサムウェア攻撃の具体的な攻撃の流れの例を次に示す。

① 組織内ネットワークへの初期侵入

組織内ネットワークとインターネットとの境界に設置される VPN 装置の脆弱性の悪用、リモートデスクトップサービスなど外部からのリモートアクセス手段の悪用、または、ウイルス付きメールを従業員に送りつけるといった手口で、組織内ネットワークに侵入する。パソコンやサーバに遠隔操作ウイルスを感染させるなどして、攻撃者は組織内ネットワークで継続的に悪意のある行為ができるようにする。

② 組織内での侵害範囲拡大

組織内ネットワークへ侵入後、標的型攻撃と同様の手口を用いて組織内での侵害範囲を拡大する。例えば、ネットワーク上に存在するマシンやアカウントを調査したり、別のウイルスや攻撃ツールを送り込んだりして、攻撃基盤の構築を行う。これらを基に、組織内ネットワーク上のサーバ類（Active Directory やファイルサーバ、バックアップ用サーバ）への侵害を試みる。

③ データの窃取

「二重の脅迫」を狙う場合、侵害したパソコンやサーバからデータの窃取を行う。

---

[12] IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について」
https://www.ipa.go.jp/security/announce/2020-ransom.html

[13] JPCERT/CC 「侵入型ランサムウェア攻撃を受けたら読む FAQ」
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

※「二重の脅迫」：暗号化したファイルの復号と引き換えに身代金を要求するだけでなく、身代金を支払わなければ窃取した情報を公開すると脅す手口。

④　データの暗号化・システム停止

侵害したパソコンやサーバ上のデータをランサムウェアで暗号化する。その結果、事業継続に関わる重要なデータにアクセスできなくなったり、システムが停止することがある。容易に復旧されないよう、バックアップのデータやマシンも狙うことがある。

⑤　窃取したデータの公開（脅迫）

「二重の脅迫」の場合、窃取したデータの一部をリークサイトで公開し、指定した期限までに身代金が払われない場合には、すべてのデータを公開するなどと脅迫を行う。身代金の支払いには攻撃者が指定するチャット等の方法にて指示されるケースもある。

この攻撃は、ウイルスが自動的に組織内で感染したり情報窃取を行うものではなく、攻撃者の手作業によって行われる（この特徴から「人手によるランサムウェア攻撃」とも呼ぶ）。攻撃の流れのイメージを図 3-1 に示す。

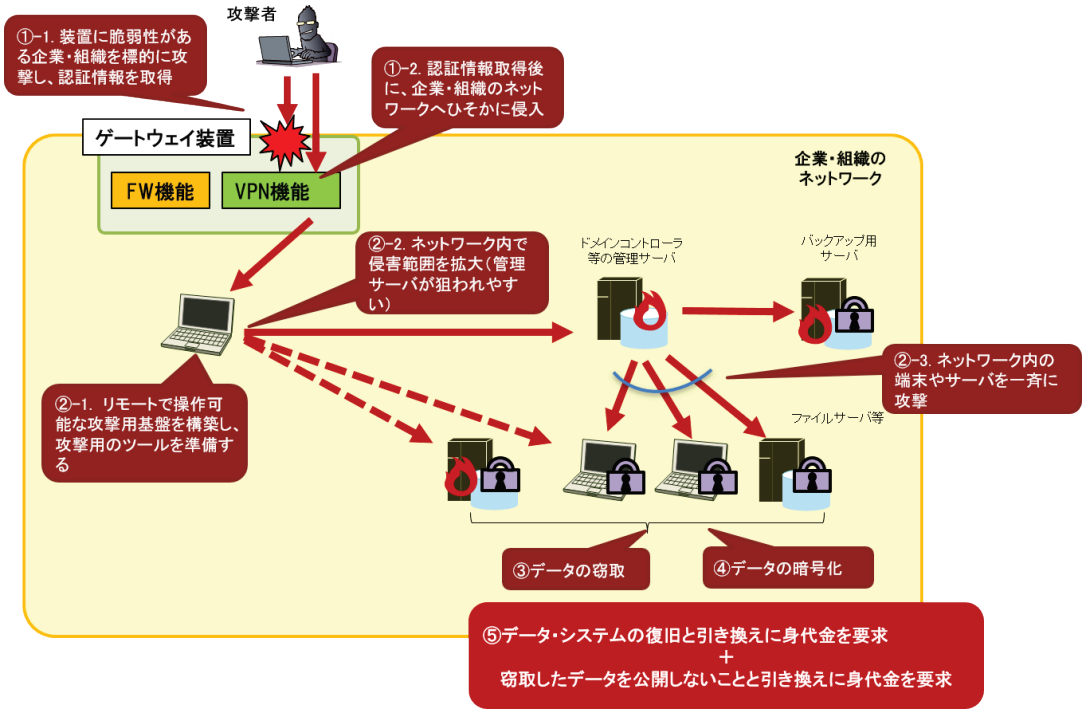

図 3-1 侵入型ランサムウェア攻撃の流れのイメージ

今期の届出から、侵入型ランサムウェア攻撃の被害の事例を 3 つ紹介する。

3-2. 事例 1：VPN 装置経由の侵入後に LockBit2.0 へ感染させられた被害

（1）　発見経緯

本件の届出者（被害企業）を A 社と呼ぶ。

A 社内のパソコンで、セキュリティソフトがウイルス感染を検知したことが、発見の契機となった。他の機器についても調査を行ったところ、一部のパソコンにおいてデータが暗号化されていたことが発覚した。

（2）　被害原因

セキュリティ専門企業の調査の結果、VPN 装置の脆弱性が悪用されたことが判明した。この VPN 装置は、2 年ほど前に稼働した基幹システムの保守用に用意したものだった。感染したウイルスは、LockBit2.0 ランサムウェアであった。

今回の攻撃の数か月前にも、VPN 装置の脆弱性を狙った不正アクセスが発生していたことが判明し、同じ攻撃者によるものと考えられる状況であった。

（3）　被害内容

数台のパソコンやサーバがランサムウェアに感染した。加えて、影響が及ぶ可能性があると判断した数十台のサーバ等の停止を余儀なくされ、業務が停止した。

被害を報告した警察から、ダークウェブ上のリークサイトに犯行予告と思われるものを確認したとの連絡があった。これを受けて届出者はリークサイトの監視を行っている。なお、届出時点では情報の流出は確認されていなかった。

（4）　被害対応

A 社では、被害発見からの数日間で次の対応を行った。

- 安全確保のため、影響が及ぶ可能性のあるサーバをシャットダウン
- 原因や影響の調査と、再構築によるシステム復旧
- 対策本部を立ち上げ、インシデント対応の統制を行うとともに、A 社ウェブサイトで不正アクセス被害の公表、また自社システム停止に対する社内説明会を実施
- 関係組織（警察、監督官庁、JPCERT/CC、個人情報保護委員会、関連協会、取引先等）への報告
- セキュリティ専門企業への調査依頼

被害にあったシステムは、原則、初期化による再構築を行った。これらも含めた対応や対策実施には、自社要員で 30 人日程度の工数が発生し、復旧費用としては 1 ～ 2 億円を見

込んでいる。

システムの再構築による復旧は完了までに発生から 4 か月程度かかったが、代替手段での対応や優先度を明確にした復旧方法により、必要な業務は 1 か月程度で通常運用できるまで回復した。また、リークサイト上の犯行予告確認後、警察、セキュリティ専門企業、顧問弁護士と相談したのち、身代金の支払い等には一切応じないこととした。

（5） 再発防止策

- VPN 装置のアップデート
- ウイルス対策製品の刷新やセキュリティ装置の設定の見直し
- 定期的なログのモニタリング
- 所属企業グループ内でのセキュリティ水準の向上（ゲートウェイの整理と集約など）

3-3. 事例 2：Active Directory やバックアップ用サーバが侵害された被害

（1） 発見経緯

本件の届出者（被害企業）を B 社と呼ぶ。

B 社社員が出社し、パソコンを立ち上げたところ、システムが利用できないことが判明した。これを受け社内調査を実施したところ、複数拠点において、社員が使用するパソコンのファイルが暗号化され拡張子が変更されていることを確認した。また、それらパソコンでは、データ復旧のためにダークウェブ上のチャットで連絡することを求めるメッセージが表示されていた。さらに、VPN 装置への不正アクセスや、Active Directory 等のサーバへの不正アクセスとファイルの暗号化も確認された。

警察に被害相談を行ったところ、警察による調査も行われ、リークサイト上に B 社の情報と、窃取されたと思われるファイルがあることも確認された。

（2） 被害原因

セキュリティ専門企業の調査の結果、VPN 装置の脆弱性が悪用され、VPN 接続用の認証情報が窃取されており、その認証情報を使って不正にアクセスされていたことが判明した。攻撃者は B 社内ネットワークに侵入したのち、具体的な手口は不明ではあるが、遠隔操作可能な環境をネットワーク内に構築したと考えられる。また Mimikatz というツールを使用して認証情報の取得を行うなどし、Active Directory サーバを侵害したと思われる。

（3） 被害内容

サーバ 6 台、パソコン 15 台が、Spook と呼ばれるランサムウェアに感染させられ、1 万以上のファイルが暗号化された。

侵害されたマシンでは、システムを復旧するためのデータや、各種ログが削除されてい

た。Active Directory 侵害後、バックアップ用サーバも侵害され、機能しない状態とされたため、システムの復旧に甚大な影響を及ぼした。これらの被害により、約 1 か月間、業務管理のためのシステムの利用ができないまま業務運営を行うこととなった。

（4）　被害対応

B 社では、被害発見後、次の対応を行った。

- ウイルスに感染したパソコンをネットワークから切断
- 関係組織（警察、監督官庁、個人情報保護委員会、関連協会等）への報告
- VPN 装置やサーバのログ収集と、セキュリティ専門企業によるフォレンジック調査
- VPN 装置のアップデート、社内パソコンのウイルス対策ソフトウェアの更新
- サーバやパソコンの再構築（OS の再インストールを実施）

また、暫定的な運用として、VPN 装置に登録されているユーザすべてを無効化し、リモート接続できないようにした。

（5）　再発防止策

- パスワードポリシーの策定と運用（多要素認証や、移動や退職時等の管理、パスワード桁数など）
- ログ取得設定の見直し（取得ログ種別、期間）

3-4. 事例 3：複数のシステムで共通の認証情報が悪用された被害

（1）　発見経緯・初動対応

本件の届出者（被害企業）を C 社と呼ぶ。

始業時間前に、C 社の社内システムが稼働していないと社員から報告があり、当該サーバを確認したところ、サーバ内のファイルが暗号化されていることを発見した。すぐに他のサーバも確認すると、ランサムウェアによる暗号化処理が進行中のサーバがあったため、急遽、全サーバをネットワークから遮断した。

その後、暗号化処理が停止していることを確認し、被害があったサーバに、まだ暗号化されていないファイルがあることが判明したため、当該ファイルを退避させた。

（2）　被害原因

C 社拠点の一つにおいて、使用していた VPN 装置のファームウェアが古かったことや、パスワードが簡単なものであったことから、そこから侵入されたと考えられる。ただし、当該装置でログの取得をしていなかったため、詳細な調査ができておらず、具体的な侵入の手口は不明である。

被害を拡大させた要因として、ランサムウェア被害にあったサーバでは、VPN 装置の管理者パスワードと同じパスワードを使用していたことが挙げられる。攻撃者は VPN 装置の管理者パスワードを脆弱性の悪用により不正に入手し、そのパスワードを用いて、組織内ネットワークでの侵害範囲の拡大を行ったと考えられる。加えて、一部のサーバにはゲストアカウントでアクセスできる共有フォルダがあったことも、被害範囲を広げた原因とのことであった。

（3）　被害内容

全国の複数拠点のサーバがランサムウェア被害に遭い、20 台以上のサーバの機能が停止した。そのうち 10 台弱のサーバでは一部もしくは全てのデータが損失した。外部組織による調査の結果、本件で使用されたのは Zeppelin と呼ばれるランサムウェアとのことであった。

届出者が運営する一般利用者向け施設では、社内システムが利用できず、非効率な手作業での対応、現金以外の支払い不可といった影響があった。さらに料金の前払い状況のデータも暗号化されて使用できなくなったため、その補填による金銭的被害も生じた。

被害が発生した日より復旧対応を進め、すべてのサーバが復旧するまで 15 日程度かかった。この間、1 日あたり 2.5 名～5 名程度の工数が割かれたとのことであった。

（4）　被害対応

C 社では、被害発見後、次の対応を行った。

【発見当日】

- 稼働中の全サーバのネットワークを遮断
- 最新のセキュリティ対策ソフトのインストールと、フルスキャンを実施
- 暗号化されていないファイルの退避
- 全サーバのパスワードを変更

【発見から数日以内】

- 侵入経路調査と、外部業者への復旧支援依頼
- 廃棄予定サーバを活用して、主要サーバの仮復旧を実施

【発見から 2 週間以内】

- バックアップデータがあるサーバを本番環境で復旧
- 暗号化されたデータの復元作業依頼を実施
- 各拠点でのゲートウェイ装置のアップデート
- ほぼすべてのサーバの復旧が完了

（5）　再発防止策

- VPN 装置上のすべての認証情報（ID・パスワード）に対して、使いまわしの禁止やパスワードの複雑化等、見直しを実施
- SSL-VPN 接続時の認証にワンタイムパスワード認証を追加
- 社内サーバの認証情報を 1 台ごとに固有で複雑なものを設定
- ファイルサーバ等のゲストユーザ権限でのアクセスを制限
- 振る舞い検知が可能なセキュリティソフトに変更
- データのバックアップ先を複数にする
- バックアップデータのオフライン保管
- ゲートウェイ装置での定期的なファームウェア更新を行う仕組みの構築
- 外部機関によるセキュリティ診断の実施と、結果に基づいた対策の実施

3-5. 着目点

3-1 で侵入型ランサムウェア攻撃の概要と攻撃の流れを説明し、3-2 から 3-4 で具体的な 3 つの事例を紹介した。この脅威は「人手による」攻撃と呼ばれているとおり、大まかな共通点はあれど、個々の事例ごとに攻撃手口や被害内容が異なる。ここでは、特に重要と思われる着目点を挙げる。

（1）　VPN 装置からの侵入 ～ 攻撃対象領域管理の必要性

侵入型ランサムウェア攻撃では、標的型攻撃と同様、攻撃者が組織内ネットワークへのアクセス経路を得る（初期侵入）ところから始まる。事例から分かるように、侵入された後の対応や調査は難しくなるため、100%でなくとも、この初期侵入を防ぐことが重要である。

取り上げた 3 つの事例は、初期侵入に VPN 装置の脆弱性を悪用したもので、これは、今期受理したランサムウェア攻撃被害の届出でも多く見られた手口である。これら悪用された VPN 装置の脆弱性については最近公表されたものではなく、公表から長期間経過しているものがほとんどであった。また、事例 1 では、保守用のアクセス経路が攻撃された。VPN 装置の脆弱性の把握が不十分であったり、把握していても解消が難しかったり、あるいはそもそも機器が十分に管理されていなかった可能性が考えられる。

初期侵入の経路は、このほかにも、外部からアクセス可能なリモートデスクトップサービスが悪用されたり、サーバの脆弱性が悪用されたりする。これら、インターネットからアクセス可能な（攻撃対象となり得る）箇所を、攻撃対象領域（Attack Surface）と呼ぶ。また、これらを適切に把握・管理し、リスクを低減することを攻撃対象領域管理と呼ぶ。

攻撃対象領域に関する対策の観点を次に挙げる。

- 把握:外部からアクセス可能なサーバやサービスを洗い出す。設定ミスやシャドーIT、あるいは悪意のある者が設置したバックドアなど、組織が把握できていないアクセス点が存在する可能性がある。例えば外部からのスキャンなど、自組織の攻撃対象領域がどのように見えているかを継続的に監視する手法がある。
- 最小化とアクセス制御：攻撃対象領域自体を必要最低限としたり、アクセス制御を行ったりして、攻撃を受けにくくする。攻撃を受けた場合に備えて、その機器からアクセス可能な組織内ネットワークの範囲を制限するといった対策もあり得る。
- 堅牢化と監視：脆弱性対策や、認証を強化（複雑なパスワードの設定、多要素認証の採用など）して、攻撃を防ぐ。また、攻撃を受けていないか監視を行う。

全てのサーバやサービスを把握し、完全に対策を行うことは、必要であるが非常に難しいことでもある。しかし、脆弱な攻撃対象領域は、組織にとって大きなダメージをもたらし得るリスクであり、優先的に対応していただきたい。

（2） 組織内ネットワークへの攻撃

取り上げた 3 つの事例では、初期侵入の後、攻撃者が組織内ネットワークに侵害範囲を拡大し、複数のパソコンやサーバが被害に遭っている。特に、事例 2 では、Active Directory サーバまで攻撃されたことが明らかとなっている。

攻撃者が Active Directory の侵害に成功すると、その管理下のマシン、場合によっては組織全体のシステムに管理者権限でアクセスができる可能性がある。例えば Active Directory の機能であるグループポリシーを悪用することで、管理下の多数のマシンにランサムウェアなどの不正なファイルを送り込み、実行することも可能となる。実際に、事例 1 で使われた LockBit2.0 ランサムウェアは、Active Directory が稼働しているサーバに感染すると、不正なグループポリシーを配信し、感染拡大を自動で行う機能を備えているという解析情報がある [14]。ランサムウェア攻撃の被害においては、Active Directory まで侵害されるか否かは一つの重要な分岐点である。

一方、事例 3 では、VPN 装置に侵入した際に入手した認証情報を使って、組織内の別のマシンへのアクセスが試みられた。そして、同一のパスワードを使用していたマシンへ侵入され、被害が拡大している。

このように、攻撃者は組織内ネットワークへの攻撃において、認証情報の奪取や、Active

---

[14] 2-2 節でも紹介した三井物産セキュアディレクション株式会社の下記のブログより
「ランサムウェア「LockBit2.0」の内部構造を紐解く」https://www.mbsd.jp/research/20211019/blog/

Directory といった管理サーバの侵害を狙う。攻撃は手作業で行われるため、組織内のシステム構成や脆弱な点に合わせた攻撃手口が使われる。このため、脆弱性対策の徹底はもちろんのこと、脆弱な／同一のパスワードの使用や、一般ユーザ向けの不要な権限の付与といった設定を避ける必要がある。ランサムウェア攻撃を含む、サイバー攻撃対策のための Windows システムの設定・運用方法については、Microsoft 社の資料 [15]や Software-ISAC の資料 [16]が公開されているため、参考としていただきたい。

（3）　バックアップとシステム再構築

ランサムウェア攻撃は、個人的なパソコンのデータにとどまらず、組織の情報資産や事業そのものに影響する被害をもたらす。取り上げた 3 つの事例でも、システム再構築に近い対応が余儀なくされるなど、大きな被害と復旧のためのコストが生じている。

この脅威に対し、バックアップが重要であることは改めて挙げるまでもないが、単なるデータのバックアップだけでなく、いざという時にシステムの再構築が可能なだけの十分なバックアップがなされているか、復旧手順は準備されているか、また、業務継続はどのようにして行うかという観点で、改めて確認することを勧める。

攻撃者は、復旧を阻害して身代金を得られる可能性を高めるため、バックアップを狙って攻撃してくる可能性がある。難しい運用が求められるが、バックアップを複数保持すること、オフラインで保管することといった対策を検討いただきたい。

---

[15] Microsoft「Human-operated ransomware attacks: A preventable disaster」
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

[16] Software-ISAC「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」 ー 「セキュリティガイドライン Windows Active Directory 編」
https://www.softwareisac.jp/ipa/index.php

4. 事例：Movable Type の脆弱性を悪用した攻撃による被害

4-1. 届出内容

（1）　発見経緯

届出者が所有するウェブサイトがサービス停止していることを、サーバの保守運用を担っていた委託業者が発見した。調査を行ったところ、ウェブサーバ上にあったファイルの改ざんや不正なファイルの設置により、サービス停止が発生したことが確認された。

（2）　被害原因

当時、届出者のウェブサイトは Movable Type から別の CMS へと移行していた。しかし、移行前に使用していた Movable Type が、適切な脆弱性の対策がなされていないまま動作している状況にあった。そのため、Movable Type に存在した脆弱性を攻撃者に悪用された。

（3）　被害内容

本件では、ウェブサイト上の複数のファイルの改ざんおよび不正ファイルの設置が行われた。攻撃者は、ウェブサイトが Movable Type で動作していることを前提としたファイルの改ざんを行った。その結果、移行先である CMS の機能が停止し、ウェブサイトへアクセスできなくなった。

なお、この時点で攻撃者からのアクセスを遮断したため、ファイルの改ざんや不正なファイルの設置、ウェブサイトのサービス停止以外の被害は確認されなかった。

（4）　被害対応

- 攻撃の発信元とみられる IP アドレスからのアクセスを遮断。
- 攻撃者によって改ざんおよび不正に設置されたファイルを確認して隔離。
- 利用をやめた Movable Type に関連するファイルを全て削除。

（5）　再発防止策

- 届出者と委託業者間での緊急対策体制やフローの整備。
- 利用する製品に影響する脆弱性が公開されていないか確認するフローの整備。

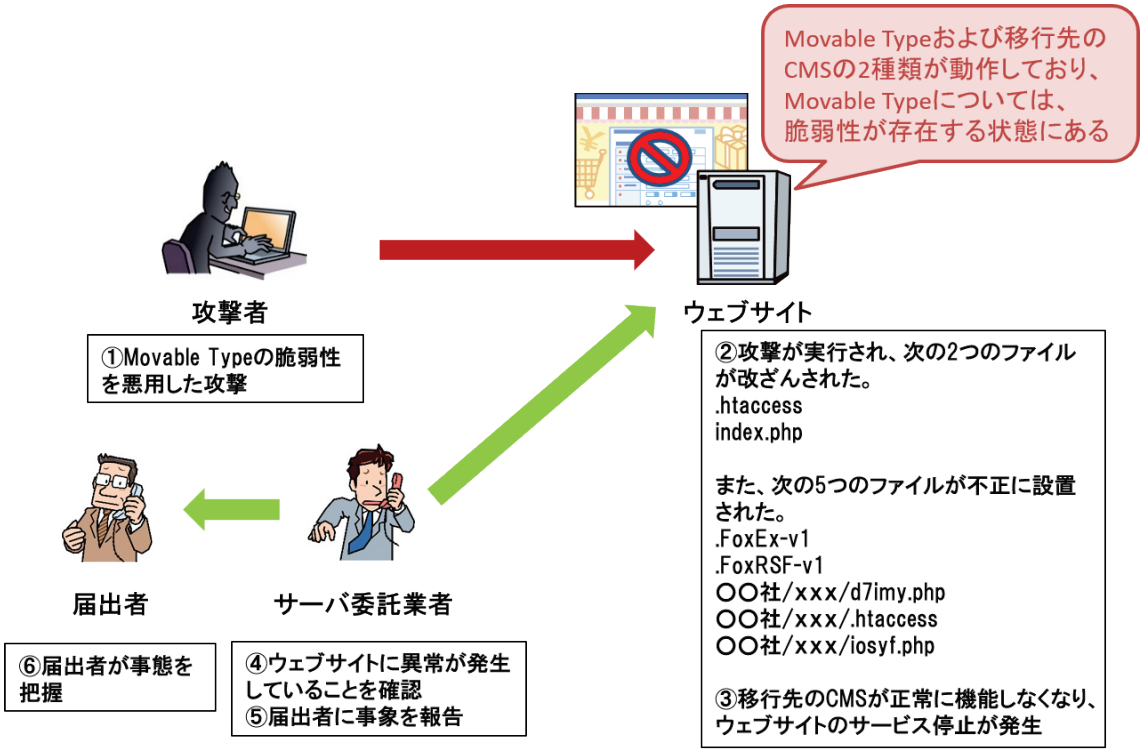

図 4-1 本事例の概要

4-2. 着目点

（1） Movable Type の脆弱性を悪用した攻撃

本事例は、Movable Type の ウェブインタフェースである XMLRPC API に発見された、OS コマンド・インジェクションの脆弱性（CVE-2021-20837）を攻撃者に悪用されたものである。本脆弱性は 2021 年 10 月 20 日に公開され、同月の 26 日に本脆弱性を実証するコード（PoC）が公開されると、脆弱性の有無を調査する通信や、脆弱な環境に不正ファイルを設置する通信が多数観測されるようになる等、積極的な脆弱性悪用の試みが確認された。

本紙の「2-3 脆弱性や設定不備を悪用された不正アクセス」で紹介しているとおり、複数の組織が本脆弱性を悪用した攻撃による被害を受けたことを確認している。

対策としては、脆弱性が公開された際は、影響を受けるかを速やかに確認し、開発者が提供している情報をもとに脆弱性対策を実施することが重要である。本脆弱性のように PoC が一般に公開された場合、攻撃者による脆弱性の有無を調査する試みや、侵害を目的とした攻撃が急増する傾向にある。そのため、脆弱性の収集に関して、PoC が公開されていないか、どの程度利用され易いものなのか等も併せて確認する運用を構築しておくことが望ましい。さらに、脆弱性悪用が確認された場合に備え、対応のフローや組織内外への連絡体制に問題がないか等の見直しをしておくことも重要である。

（2）　２種のバックドアの使用

本事例において、攻撃者は Movable Type の脆弱性を悪用し、ウェブサイト上にあった２つのファイルを改ざんするとともに、５つの不正ファイルの設置を行った。この不正に設置された５つのファイルのうち、iosyf.php および d7imy.php という２つのファイルについて、届出者からの提供があった[17]。

これらはランダムな英数字５文字が付けられたと思われる PHP ファイルであり、攻撃者が仕掛けたバックドア（攻撃者のサーバへの再侵入や遠隔操作を可能とする設定や不正プログラム）であることを確認している。iosyf.php については、簡易的なファイルアップローダの機能を持っていた。また、d7imy.php については、様々な機能を持ったバックドアであったことを確認している。

d7imy.php にアクセスすると、FoxWSO という名称の管理画面が表示される（図 4-2）。この画面には、リモートデスクトップ接続のアカウントを作成する機能や、cPanel と呼ばれるコントロールパネル製品のパスワードをリセットして、アクセス権を取得しようとする機能等が存在する。攻撃者はこのバックドアを使用することで、侵害範囲をより広げようとする狙いがあったものとみられる。

類似する攻撃手口や、ファイルの詳細について「Japan Security Analyst Conference (JSAC) 2022」の講演[18]で紹介されたため、参考にしていただきたい。

---

[17] 他のファイルは未提供。.FoxEx-v1 および.FoxRSF-v1 の２つは、空ファイルであったとのことであった。空ファイルであった理由は不明だが、攻撃者によって削除された可能性がある。

[18] Japan Security Analyst Conference (JSAC) 2022
「日本にシェアが集中する CMS を狙う特異な攻撃者と侵害ツールの調査」
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_1_tsuji-nishibe_jp.pdf

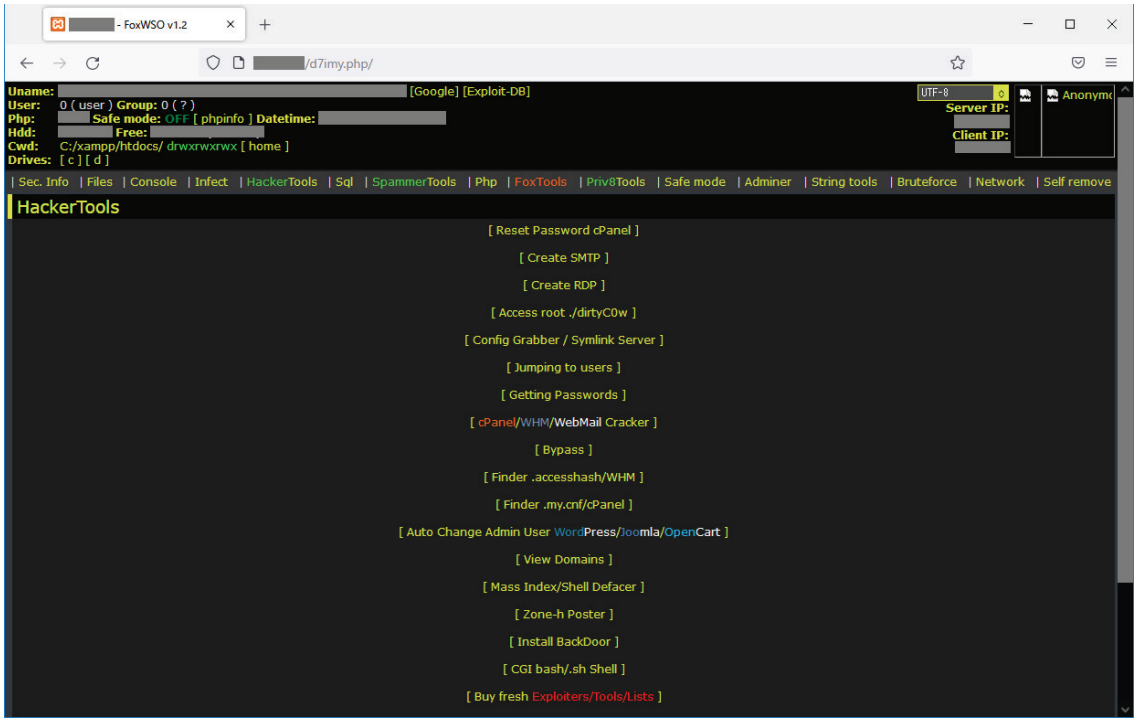

図 4-2 d7imy.php の実行画面例

（3） ウェブサイトの脆弱性管理

本事例において、脆弱性悪用の原因となったのは、届出者が使用していた移行前の Movable Type が、ウェブサイト上で動作する状態のままで置かれ、脆弱性管理が適切に実施されていなかったためである。CMS を移行する際、移行前の CMS を確実に削除する、あるいは利用が出来ないよう停止する等の対応を行うまでは、その CMS の脆弱性管理を継続する必要がある。このような、移行前のファイルの処置については、盲点となる可能性があり、注意いただきたい。

また、CMS に限らず、ウェブサイト上で不要なソフトウェアが動作している場合には、そのソフトウェアが悪用されることを防ぐため、必要のないソフトウェアは停止、あるいは削除することを推奨する。利用しているソフトウェア及びそのソフトウェアに関連する脆弱性を網羅的に把握、管理することが困難である場合には、IT 資産管理ソフト等の脆弱性対策を支援するツールを導入したり、必要に応じて、システムの開発者等から技術的なサポートを受けられるように保守契約を締結したりすることも検討いただきたい。

IPA ではウェブサイト運営者、システムおよびネットワーク管理者向けに、ウェブサイトのセキュリティ対策のチェックポイントをまとめた次の資料を公開している。適切な対策がとられていない項目があった場合には、早急に対策を実施いただきたい。

- 安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～
  https://www.ipa.go.jp/security/vuln/websitecheck.html

5. 事例：SQL インジェクション攻撃により顧客情報が流出した被害

5-1. 届出内容

（1）　発見経緯

届出者が運営する EC サイトにおいて、特定の IP アドレスからのアクセスによるデータベースの負荷増大を発見した。負荷増大の原因を調査した結果、長時間滞留している SQL 処理があることを発見した。

（2）　被害原因

脆弱性があり、EC サイトに対して SQL インジェクション攻撃を受けた。届出者は SQL インジェクション攻撃の対策のため、プレースホルダを用いた実装を行っていたが、一部の箇所でプレースホルダの実装漏れがあり、そこに攻撃を受けた。

（3）　被害内容

- 届出者が保有している顧客情報（数十万件分）が漏洩した。
- 売上減や対象顧客への見舞金等により、総額２億円以上の損失になる見込みである。

（4）　被害対応

- 不正アクセスを発見し、原因を特定して、SQL インジェクション攻撃の対策（プレースホルダを用いた実装やエスケープ処理の実装）を実施した。不正アクセスを発見したのは、不正アクセスが開始された翌日であった。
- 漏洩した個人情報の範囲を特定し、対象者への連絡や問い合わせ窓口の設置を行った。
- WAF（Web Application Firewall）の導入を行った。
- 第三者機関によるセキュリティ診断を実施し、診断にて検出された脆弱性の改修を行った。このとき検出された脆弱性は、本件の攻撃で悪用されたものとは別の脆弱性であった。

（5）　再発防止策

・開発部分のソースコードについて、複数名でのレビューの実施。

・定期的な脆弱性診断の実施。

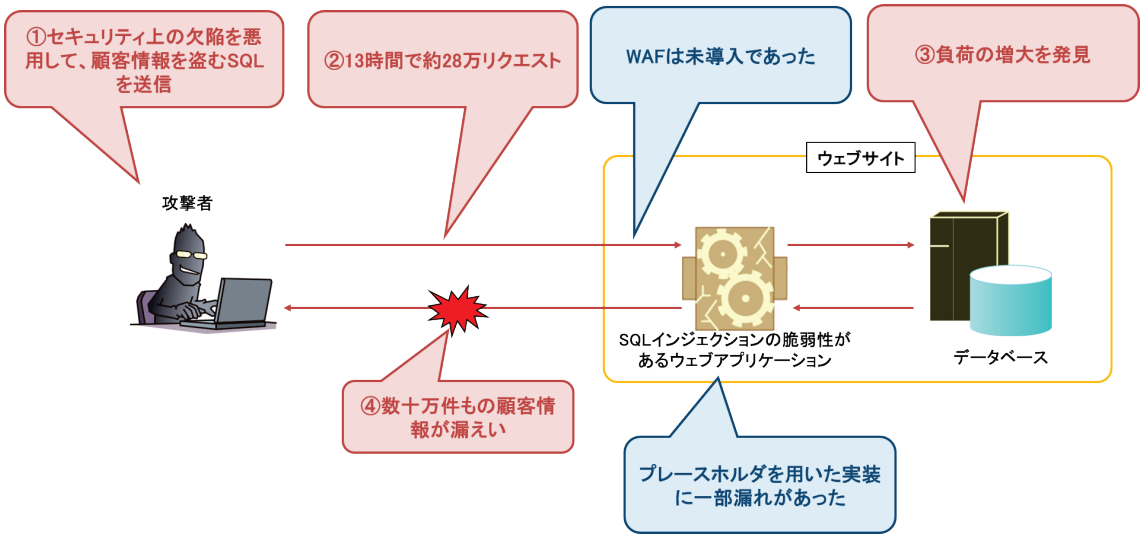

図 5-1 本事例の概要

5-2. 着目点

（1） 自組織で開発したウェブアプリケーションの脆弱性

本件は、自組織で開発したウェブアプリケーションに SQL インジェクションの脆弱性が存在し、その脆弱性が悪用され、顧客情報が漏洩した事例である。具体的にはプレースホルダを用いた実装に一部漏れがあったために被害を受けたもので、今期は、本件以外にも、プレースホルダを用いた実装の漏れやエスケープ処理の漏れがあったために、SQL インジェクション攻撃を受け、顧客情報が数万、数十万件漏洩した事例が複数あった。いずれの事例でも正しい実装がされていれば、被害を防げたであろう。

自組織で開発したウェブアプリケーションの脆弱性は、CMS 等の脆弱性のようにベンダから公開されることはないため、基本的に自組織で検出し対応する必要がある。開発時の人手によるソースコードレビューの徹底や、ツールを用いた自動のソースコードレビュー、脆弱性診断等を行って、開発時に脆弱性を検出し、作り込まないようにすることが重要である。

IPA ではウェブサイト開発者や運営者が適切なセキュリティを考慮したウェブサイトを作成するための、次の資料を公開しているので、開発時の参考にしていただきたい。

- 安全なウェブサイトの作り方
  https://www.ipa.go.jp/security/vuln/websecurity.html
- 安全な SQL の呼び出し方
  https://www.ipa.go.jp/files/000017320.pdf

また、WAF の導入も効果的であると考えられる。WAF の導入は、脆弱性の修正といった

ウェブアプリケーションの実装面での根本的な対策ではないが、WAF が攻撃の通信を遮断することにより、脆弱性が残っていても攻撃を防げる場合がある。なお、WAF を導入したとしても、攻撃を検知できないと効果が少ないため、適切な検知パターンの設定や、定期的な検知パターンの見直しが重要である。IPA では、ウェブサイト運営者が WAF の導入を検討する際に、WAF の理解を手助けするための次の資料を公開しているので、参考にしていただきたい。

- Web Application Firewall 読本
  https://www.ipa.go.jp/security/vuln/waf.html

ベンダ等から公開される脆弱性だけでなく、自組織で開発したアプリケーションの脆弱性、およびそこに対して行われる攻撃についても注意が必要である。本件の攻撃手法は目新しいものではなく、典型的な SQL インジェクション攻撃であった。広く知られた攻撃手法であるが、未だに攻撃が行われていること、また、万一被害を受けた場合には、数十万件の情報漏洩や、数億円の損失に至る可能性があることを認識し、適切な対策を行っていただきたい。

（2）　被害の発見のためのリソースやアクセス数の監視

本件で被害発見の契機となったのは、特定の IP アドレスからのアクセスによるデータベース負荷の増大を検知したことである。もし、負荷の増大を検知していなければ、攻撃の発見や対処が遅れ、さらに多くの顧客情報が漏洩するなど、被害が拡大していた可能性がある。被害の軽減のためにも攻撃を早期に発見することは重要であり、データベース等の負荷を監視するなどして、異常の発生を迅速に検知できるようにしておくべきであろう。

また、本件は、ウェブサイトに単一の IP アドレスから、13 時間で約 28 万回（毎秒 6 回程）もの大量のアクセスがあった。これは当該サイトでは通常は発生し得ない異常な値である。データベース等の負荷の監視だけでなく、特定の IP アドレスからの単位時間当たりのアクセス数を監視することも、早期の攻撃発見に有効である。

不正アクセス被害を受けないことが理想ではあるが、必ずしも被害を防げるわけではないため、被害を受けないための対策に加えて、リソースやアクセス数の監視といった、早期に攻撃を検知し、被害を軽減するための対策も重要である。

6. 届出へのご協力のお願い

本レポートの内容は、すべて実際に国内で発生したコンピュータウイルスの発見や感染、不正アクセスの試みや被害の情報について、IPA へ届出いただいた情報を基としています。これらを事例として公開することにより、同様被害の早期発見や未然防止、被害の低減等に役立てていただくことを目的としています。

IPA では、日々国内の様々なセキュリティ動向を調査しており、特に、日本国内で発生しているサイバー攻撃等に関する状況や、具体的な攻撃の手口の把握のためには、**皆様からの届出情報が不可欠です**。IPA は、経済産業省が告示で定めている、ウイルス・不正アクセスの**国内唯一の届出機関**です。可能な範囲で結構ですので、コンピュータウイルスの発見や感染、不正アクセスの試みや被害を確認した際は、下記の窓口への届出・ご協力をお願いいたします。

- コンピュータウイルス・不正アクセスに関する届出について
  https://www.ipa.go.jp/security/outline/todokede-j.html

最後に、届出にご協力をいただいている皆様へ、ここに改めて感謝申し上げます。
今後とも、日本全体での情報セキュリティの取り組みの促進へ繋げられるよう、引き続き本届出制度へのご協力をお願いいたします。

【コンピュータウイルスに関する届出制度】

コンピュータウイルスに関する届出制度は、経済産業省のコンピュータウイルス対策基準に基づき、1990 年 4 月にスタートした制度であり、コンピュータウイルスを発見したものは被害の拡大と再発を防ぐために必要な情報を IPA に届け出ることとされている。
IPA では、個別に届出者への対応を行っているが、同時に受理した届出等を基に、コンピュータウイルス対策を検討している。また、受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表している。

○コンピュータウイルス対策基準
平成 7 年 7 月 7 日（通商産業省告示 第 429 号）（制定）
平成 9 年 9 月 24 日（通商産業省告示 第 535 号）（改定）
平成 12 年 12 月 28 日（通商産業省告示 第 952 号）（最終改定）
○経済産業大臣が別に指定する者
平成 16 年 1 月 5 日（経済産業省告示 第 2 号）

【コンピュータ不正アクセス被害の届出制度】

コンピュータ不正アクセス被害の届出制度は、経済産業省のコンピュータ不正アクセス対策基準に基づき、1996 年 8 月にスタートした制度であり、同基準において、コンピュータ不正アクセスの被害を受けた者は、被害の拡大と再発を防ぐために必要な情報を IPA に届け出ることとされている。
IPA では、個別に届出者への対応を行っているが、同時に受理した届出等を基に、コンピュータ不正アクセス対策を検討している。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表している。

○コンピュータ不正アクセス対策基準
平成 8 年 8 月 8 日（通商産業省告示 第 362 号）（制定）
平成 9 年 9 月 24 日（通商産業省告示 第 534 号）（改定）
平成 12 年 12 月 28 日（通商産業省告示 第 950 号）（最終改定）
○経済産業大臣が別に指定する者
平成 16 年 1 月 5 日（経済産業省告示 第 3 号）