コンピュータウイルス・不正アクセスの届出事例

［2021 年上半期（1 月～6 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

2021 年 8 月 23 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・考えう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 年上半期（1 月～6 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 127 件取り上げ、次の 6 種に分類した。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ている。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　14 件（項番 1～14）
- 身代金を要求するサイバー攻撃の被害　30 件（項番 15～44）
- ID とパスワードによる認証を突破された不正アクセス　31 件（項番 45～75）
- 脆弱性や設定不備を悪用された不正アクセス　24 件（項番 76～99）
- サプライチェーンに関するインシデント　23 件（項番 100～121）
- その他　6 件（項番 122～127）

今期に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（2-3 節で説明）や、脆弱性やセキュリティ設定の不備を悪用された事例（2-4 節で説明）の多くはその典型である。セキュリティ対策運用手順やセキュリティポリシーに基づいた利用規則などを確立して、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。

その一方で、業務委託先サーバへの侵害や、SaaS（Software as a Service）基盤利用時の設定不備による情報漏洩など、自組織のシステム管理者や利用者だけでは直接の対策が難しいサプライチェーンに関するインシデント（2-5 節で説明）の届出も多かった。

ウイルスの検知や感染被害（2-1 節で説明）の届出については、2020 年下半期（7 月～12 月。以下、先期）の 49 件と比較すると 14 件と大幅に減少した。先期のウイルス届出の大半を占めた「Emotet」と呼ばれるウイルス（以下、Emotet）の検知や感染被害の届出が 44 件から 6 件と大幅に減ったことが理由の一つである。とはいえ、Emotet と似た手口で感染活動をする別のウイルスや、ランサムウェア感染被害（身代金を要求するサイバー

[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。

攻撃の被害（2-2 節で説明）に分類）に関する届出は今期も多かった。今後も引き続きウイルスに対する注意は必要である。

なお、本紙に示した事例以外にも、ウイルスの発見・感染、なりすましやフィッシング等の不審メールの受信、SEO ポイズニングによる悪性サイトへの誘導等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 2022 年 1 月に「コンピュータウイルス・不正アクセスの届出状況」として公開する予定である。

2-1. コンピュータウイルスの検知・感染被害

今期は、利用しているパソコン等の機器がウイルスを検知したり、感染の被害に遭ったりしたという届出は比較的少なかった。先期までに猛威を振るい、多数の届出があった Emotet について、攻撃活動が次第に観測されなくなり、それと同時に Emotet に関する届出も大幅に減ったことが一因である。しかしその一方で、Emotet と同様の手口で、窃取した過去のメールを引用するなどして正規の返信を装ったメールを介して感染拡大を図る、別のウイルスに関する届出も見られた。なお、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別の分類として 2-2 節で説明する。

（1） Emotet

Emotet は、情報の窃取に加え、さら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）に添付されるなどして、感染の拡大が試みられていた [7]。

IPA では 2019 年 9 月中旬頃から 2020 年 2 月上旬頃までと、2020 年 7 月中旬頃から 2021 年 1 月中旬頃までの期間、Emotet への感染を狙う攻撃メールが国内に広くばらまかれていることを観測していた。また、コンピュータウイルス届出窓口においても多数の Emotet 感染や攻撃メールの着信に関する届出を受理していた。

今期に入り、2021 年 1 月 27 日、EUROPOL（欧州刑事警察機構）が、欧米 8 カ国の法執行機関・司法当局の協力により、Emotet の攻撃基盤をテイクダウンした（停止させた）との発表 [8]があった。それ以降、IPA では Emotet の攻撃メールのばらまきは観測していな

---

[7] IPA「「Emotet」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] EUROPOL「World's most dangerous malware EMOTET disrupted through global action」（英語）
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

い。届出窓口においては 6 件の Emotet 検知や感染の届出を受理したが、いずれも発見日は 1 月 27 日以前であった。

なお、1 月 27 日以降に Emotet に感染したことを公表している組織等がいくつか見受けられたが、局所的に Emotet の攻撃が継続していることは考えにくく、Emotet とは別のウイルスを Emotet と誤認している可能性が考えられる。次項で述べるとおり、Emotet と同様の手口が使われる別のウイルスの攻撃メールも存在し、それにより感染したと考えられる届出も寄せられている。感染防止のためには、Emotet と同様に不審なメールや添付ファイルは開かないといった対策が必要であるとともに、万一感染してしまった際には、ウイルス種別ごとに必要な対応が異なる場合があるため、種別を見極めて適切な対応を行うことが必要である。

（2）　返信を装った攻撃メールで感染を狙うウイルス

Emotet 以外には、「IcedID」と呼ばれるウイルス（以下、IcedID）や、「Qakbot」または「Qbot」と呼ばれるウイルス（以下、Qakbot）に関する届出が複数あった。IcedID は 2017 年 9 月に最初に発見されたとされるインターネットバンキングの情報窃取を行うウイルス（以下、バンキングトロイ）であり、2020 年 10 月頃から、この IcedID への感染を狙ったとみられる攻撃メールがばらまかれていたことを観測している [9]。Qakbot は、もともとはバンキングトロイであったが、多数の亜種が開発されて様々な攻撃に使用されているウイルスであり、2020 年以降被害が拡大傾向にある [10]。

これらのウイルスに関する届出事例では、いずれも届出者の組織にウイルス感染を狙った攻撃メールが着信していた。IcedID や Qakbot の攻撃メールは、マクロが含まれた Office 文書ファイルが ZIP 圧縮されて添付されているものが多い。添付された Office 文書ファイルを開いてマクロを有効にすると、IcedID や Qakbot がダウンロードされて実行され、感染に至る。攻撃メールには、過去のメールの本文が引用されていたり、日本語の件名が使われていたりなど、Emotet と同様、正規の返信メールを装う巧妙な細工が施されたものもあり、一見して不審であると見破ることは難しい。送信元や本文に見覚えがある返信メールであっても、攻撃メールである可能性を念頭に置いて添付ファイルを取り扱い、特にそれがマクロを含んだ Office 文書ファイルである場合は、マクロの有効化が必要であり、か

---

9 トレンドマイクロ セキュリティブログ 「「EMOTET」後のメール脅威状況：「IcedID」および「BazarCall」が 3 月に急増」https://blog.trendmicro.co.jp/archives/27732

10 サイバーリーズン ブログ 「被害が拡大しつつあるマルウェア「Qakbot」の傾向と対策を知る」
https://www.cybereason.co.jp/blog/cyberattack/5757/

つ安全であろうと判断できるまでは「編集を有効にする」「コンテンツの有効化」のボタンはクリックしないことが重要である。

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。また、返信を装った攻撃メールにより Qakbot ウイルスに感染した被害について、項番 11 の事例の詳細を 3 章で紹介する。

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 の検知や感染被害の事例		
1	2021/1/6	2020 年 11 月に、届出者（企業）のパソコン 2 台で Emotet を検知した。
2	2021/1/21	2021 年 1 月に、届出者（一般団体）のパソコンで Emotet を検知した。セキュリティソフトが駆除し被害はなかった。
3	2021/1/21	2020 年 11 月に、届出者（企業）のパソコンで Emotet を検知した。
4	2021/1/29	2020 年 10 月に、届出者（企業）のパソコンで Emotet を検知した。念のためパソコンを初期化し再セットアップして対応した。
5	2021/3/4	2020 年 9 月に、届出者（業界団体）のパソコンでセキュリティソフトがウイルスを検知した。調査したところ、Emotet をダウンロードしようとしている通信を検知していたことがわかった。感染はしておらず被害等は発生しなかった。
6	2021/3/5	2020 年 10 月に、届出者（公共機関）の委託先事業者を騙るなりすましメールが送信されていることが当該事業者より届出者に報告された。調査したところ、委託先の従業員がテレワークに使用していたパソコンが Emotet に感染しており、そこから不正なメールが送信されていたことが判明した。なりすましメールに対する注意喚起の発信、情報セキュリティに関する教育、情報セキュリティポリシーの遵守の定期点検、およびテレワークには組織で管理された専用のパソコンのみを使用するようにした。

返信を装った攻撃メールで感染を狙うウイルス被害の事例		
7	2021/3/8	届出者（企業）のメールアカウントが海外から不正アクセスを受け、過去にやり取りしたメールの件名や本文が引用されたウイルス付きメールが複数の宛先に対して送信された。IcedID への感染を狙った攻撃メールと見られ、メールサービスからのウイルス検知の通知により事象を認知した。従来メールシステムへのアクセスは社内ネットワークからのみに制限していたが、テレワーク対応のために社外からの接続を許可していたときに、強度の弱いパスワードを設定していたアカウントが不正アクセスされたことが原因と考えられる状況であった。社外からアクセスする場合はデジタル証明書を利用したデバイス認証を必須とし、またパスワード厳格化のポリシーを適用して再発防止を図った。
8	2021/3/12	届出者（非営利団体）において、長期間使用していなかったメールアカウントから、複数のメールアドレス宛てに IcedID への感染を狙った攻撃メールが送信された。組織内の受信者は不審に感じて添付ファイルは開かなかったため、感染の被害はなかった。原因については判明していないが、送信元となったアカウントのパスワードが攻撃者に推測された、総当たり攻撃で特定された等の可能性を考えている。当該メールアカウントは事案の発覚時点で削除した。今後の対策として、パスワードの定期的な変更と、不要になったメールアカウントは即時削除する運用とした。
9	2021/3/22	届出者（企業）の過去のメールが引用される形で、IcedID への感染を狙った攻撃メールが複数送信された。メールアカウントのパスワード強度が弱かったことが判明したため、攻撃者に認証を突破され、当該アカウントが攻撃メールの送信に悪用されたものと推測している。管理するメールアカウントのパスワードを全て変更するとともに、サーバでのメール保存期間を短縮し、万一不正アクセスを受けてもメール窃取の被害を減らせるように対策を講じた。

10	2021/5/12	届出者（企業）において、普段使用していないメールアカウントから組織のスタッフになりすました不審なメールが送信されていることに気づいた。送信された不審メールには、過去にやり取りしたメールの引用があり、本文は英文で添付ファイルも付けられていたことから、ウイルス感染を狙った攻撃メールが送信されたと推測される状況であった。本件を受けて、不審なメールが送信されたメールアカウントを削除し、さらに使用していたパソコンについてセキュリティソフトによるスキャンとパスワードの変更を行った。
11	2021/6/18	届出者（企業）において、不審なメールを受信した従業員が利用している仮想デスクトップ環境がウイルスに感染した。調査したところ、メールに添付されていた ZIP ファイルには、マクロ付きの Excel のファイルが含まれていた。また、そのマクロにより外部から Qakbot をダウンロードする動作が確認できたことから、Qakbot に感染していたことが判明した。仮想デスクトップ環境をリセットすることで回復を図り、また再発防止策として従業員への教育を実施することとした。
その他のウイルス被害の事例		
12	2021/3/4	届出者（企業）の従業員がウェブサイトを閲覧していたところ、偽のセキュリティ警告が表示された。当該従業員は、表示された偽のサポートの電話番号に連絡し、指示に従ってソフトウェアをインストールした時点で不審に感じ電話を切った。調査したところ、インストールさせられたソフトウェアは遠隔操作用のツールであったことが判明した。また、それに加えて少なくとも 1 種類の不審なプログラムが実行されていたことがわかったが、詳細な調査を行ってもそれ以上の不正な挙動は見つからなかった。当該パソコンを初期化し、当該従業員のユーザ ID とパスワードを変更することで対策を行った。さらに再発防止策として、リテラシー向上のための教育を実施することとした。
13	2021/3/18	届出者（企業）が利用しているパソコン 2 台に不具合が生じて動作しなくなった。状況から、取引先からのメールを開いた際にトロイの木馬型のウイルスに感染したとみられるが、詳細は不明である。

14	2021/6/22	届出者（教育・研究機関）が利用するクラウド型メールサービスにおいて職員 1 名のアカウントから不審なメールが送付されていた。そのメールを受信した他の職員からの連絡により発覚し、調査を行ったところ同様のメールが 1500 通以上送信されていたことが判明した。メールサービスのアカウント情報が窃取された原因は不明だが、当該職員が利用するパソコンにおいてウイルスが検知されたこと、および送信されたメールがウイルス感染を狙った内容であったことから、パソコンがウイルスに感染していたとみられ、その影響により認証情報が窃取されていた可能性がある。当該職員のメールアカウントを停止することで対応し、また再発防止策として、アカウント情報の漏洩を監視するサービスを契約して、さらにログイン時の多要素認証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

今期も、ランサムウェア攻撃 [11]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が多かった。侵入や感染の原因を、VPN 装置やサーバソフトウェアの脆弱性、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もあるため、分類としては 2-3 節、2-4 節と重複するが、身代金を要求する攻撃に関する事例は本項に分類した。

今期において目立ったのは、NAS（Network Attached Storage）やクラウドストレージが攻撃の対象となった事例である。

NAS には、アクセス制限やユーザ認証の機能に加えて、製品によっては外部ネットワークからのアクセスを想定した VPN 機能を実装しているものがある。届出事例においては、これらの機能を実装した NAS をインターネットからアクセス可能な箇所に設置し、テレワーク中の従業員や組織外とのファイル共有に使用していたところ、NAS の脆弱性を悪用されるなどしてランサムウェア攻撃の被害に遭った事例を確認した。このように、外部からのアクセスを可能にすることは、攻撃者にとってもアクセスが容易になることを意味するため、より一層のセキュリティ対策が必要になる。

---

11 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

クラウドストレージについても 3 件の届出があり、同様のことが言える。クラウドストレージでは多要素の認証方式やロールベースのアクセス制限など様々なセキュリティ機能が用意されているが、適切な設定がされていない場合、攻撃者が容易にアクセスできる状態となる恐れがある

攻撃手口については、届出では不明とされていたものが多かったが、先期と同様に、ドメインコントローラ等の管理サーバを乗っ取り、組織内の広範囲にわたって急速な感染を拡げるなどの巧妙な攻撃手口が使われた事例が複数あることを確認している。

ランサムウェア攻撃ではひとたび攻撃者に侵入を許してしまうと、被害が甚大になり復旧にも時間を要することが多い。届出事例においても、被害を受けたパソコン等をすべて初期化しての再構築作業を余儀なくされた事例や、バックアップからデータを復元したが最新の状態には復旧できなかった事例があった。

攻撃の手口や攻撃対象の機器が異なっても、脆弱性の解消や適切なセキュリティ設定など、基本的な対策が攻撃者の侵入防止のための重要な施策であることに変わりはない。ランサムウェア対策の特設ページ [12]等を参考に、改めて基本的な対策ができているかを確認することを勧める。

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、NAS の脆弱性を悪用されてランサムウェアに感染させられた被害事例(項番 19)の詳細を 4 章で、SaaS 基盤がランサムウェア攻撃を受けて ASP サービスが停止した事例（項番 39）の詳細を 5 章で紹介する。

[12] IPA 「ランサムウェア対策特設ページ」 https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

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
NAS へのランサムウェア攻撃の事例		
15	2021/2/22	届出者（企業）の NAS 上の 20 万個以上のファイルが「.mars」という拡張子に書き換えられ、復元のために身代金を要求するメッセージが置かれていたことを発見した。調査したところ、ファイル共有のためのポートが外部に開放されていたこと、およびファイルが暗号化された時間帯には従業員のパソコンからのアクセスがなかったことから、組織外部から直接 NAS に不正アクセスされたものと考えられる状況であった。従業員のテレワークに対応するため、外部から社内環境へのアクセスを設定した際に、誤ってファイル共有のポートも外部に開放してしまっていたことが原因と推測している。外部アクセスの設定を是正して対策した。また暗号化されたファイルの一部はバックアップから復元した。
16	2021/3/1	届出者（企業）が使用する取引先等とのデータ共有用の NAS がランサムウェアの攻撃を受け、ファイルが暗号化された。攻撃の経路は不明であるが、NAS は社外とのファイル共有用途に利用しており、インターネットから直接ファイル転送やサーバ管理用画面へのアクセスが可能な状態であったため、外部から不正アクセスを受けたと思われる。なお、当該 NAS は、届出者の社内ネットワークとは分離したセグメントに設置されており、社内のサーバやパソコンに影響はなかった。対策として、不正アクセスの監視や遮断を行えるように UTM を設置してセキュリティの向上を図った。
17	2021/3/4	2020 年 11 月に、届出者（企業）が保有するサーバと NAS が makop と呼ばれるランサムウェアの攻撃を受け、40 万個以上のファイルが被害にあった。サーバと NAS はインターネットに接続されており、何らかの方法で攻撃者によって不正にアクセスされたものと思われるが、詳細な原因は不明である。

項番	届出日	概要
18	2021/3/29	届出者（一般団体）が利用する NAS のファイルが暗号化されて使用できなくなった。また、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。脅迫文の内容等から、eCh0raix と呼ばれる NAS を攻撃対象とするランサムウェアに感染したものと推測される状況であった。NAS の VPN 機能を用いて外部からもアクセスできるように設定していたが、最新バージョンへの更新をしていなかったため、古いバージョンに存在していた脆弱性を悪用されて不正アクセスされたと推測している。
19	2021/4/27	届出者（個人）が使用している NAS 上の 30 万個以上のファイルが暗号化され、脅迫文が書かれたファイルが残されていた。調査したところ、NAS に脆弱性が存在しており、Qlocker と呼ばれる NAS を攻撃するランサムウェアに感染したと思われる状況であった。ベンダーから提供された駆除ツールとファイル復元ツールにより復旧を試みたが、一部のファイルは復元できなかった。最新のファームウェアに更新し、不要な機能を無効化して再発防止を図った。
クラウドストレージへ不正アクセスされファイルを暗号化された被害の事例		
20	2021/4/24	届出者（企業）が運用するクラウドストレージ上のファイルが削除され、復旧のために身代金を要求するような脅迫文が残されていることを発見した。調査したところ、クラウド上のアカウントを不正に使用されてファイルの削除等が行われたことが判明した。本件を受けて、多要素認証の導入、アカウント管理の徹底、監視体制の構築、バックアップの取得等を行った。
21	2021/4/26	届出者（企業）が運用するクラウドストレージ上の約 5 万個のファイルが削除され、復旧のために身代金を要求するような脅迫文が残されていることを発見した。調査の結果、同じクラウドサービス上に構築した別のサーバが不正アクセスされ踏み台にされたものと推測し、当該サーバを停止する処置を行った。不正アクセスの原因は調査中であり、判明次第再発防止策を検討する予定としている。

項番	届出日	概要
22	2021/4/30	届出者（企業）が利用しているクラウドストレージ上のファイルが削除され、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を発見した。調査したところ、インターネットからアクセスできるファイルにクラウドストレージへの認証情報が記載されており、それを悪用されて不正にアクセスされたことが判明した。本件を受けて、悪用された認証情報の無効化、認証情報が記載されていたファイルへのアクセスの遮断のほか、権限の見直し、クラウドストレージへのアクセス手法の変更、バックアップ機能の強化等を行った。
その他の身代金を要求するサイバー攻撃被害の事例		
23	2021/1/15	2020 年 10 月に、届出者（企業）の複数のパソコンやサーバが GandCrab と呼ばれるランサムウェアに感染し、ファイルサーバのファイルが暗号化されるなどの被害にあった。機器の OS を初期化することで対応した。
24	2021/2/4	届出者（企業）の数台のパソコンやサーバ上のファイルが暗号化されていることを確認した。調査したところ、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を有効にしていたパソコンへ攻撃者が不正アクセスし、そこから社内ネットワークに侵入。ドメインコントローラを乗っ取り、MedusaLocker と呼ばれるランサムウェアに感染させたことが判明した。感染したパソコン等は初期化の対応を行った。再発防止に向けた取り組みは検討中である。
25	2021/2/5	届出者（企業）の従業員がファイルサーバにアクセスしたところ、ファイルの拡張子が変更されていることに気付いた。調査したところ、複数のサーバやパソコンでファイルが暗号化された状態にされており、金銭を要求する脅迫文が画面に表示されていたことからランサムウェアに感染したと考えられる状況であった。感染経路は不明であるが、外部からのリモートデスクトップ接続を許可していたパソコンが複数台あったとのことから、パソコンが攻撃者に不正アクセスされ、ファイルサーバにも感染を拡げられたものと推測される。対策のためセキュリティソフトの導入を検討している。

項番	届出日	概要
26	2021/2/9	届出者（企業）が管理するファイルサーバと業務サーバの 2 台がシステム停止状態になった。サーバに残された脅迫文等の情報から Cring と呼ばれるランサムウェアの被害にあったと思われる状況であった。感染の経路は調査中だが SSL-VPN 装置の脆弱性を悪用して侵入されたと推測している。サーバを新たに構築してバックアップデータを復元することでシステムの復旧を実施した。
27	2021/2/11	届出者（企業）が利用するファイルサーバに格納していたファイルのファイル名が改ざんされていることに気づいた。ファイルは暗号化されており、復旧のために身代金を要求するメッセージが書かれたテキストファイルが置かれていたことから、ランサムウェアに感染したと思われる状況であった。感染経路は不明であるが、共有のユーザアカウントがファイルの暗号化に悪用されたことが判明したため、共有ユーザは使用しないこととし、アクセス権は個人ユーザ単位で付与することとすることで再発防止策とした。
28	2021/2/24	届出者（企業）が利用するサーバおよびパソコン上のファイルが暗号化されていることを確認した。セキュリティソフトで検査したところ、ネットワーク探査ツールとランサムウェアが発見されたため、何らかの手段で攻撃者に外部から侵入されたなどで、ランサムウェアが実行されたものと思われる状況であった。
29	2021/2/25	届出者（企業）で使用するサーバ上の 1 万個以上のファイルが暗号化されていることを発見した。調査したところ、ランサムウェアに感染していることが判明した。暗号化されたファイルはバックアップを用いて復旧した。届出者が所有するパソコンに対してウイルススキャンを実施し、端末管理ソフトの導入やファイルのバックアップ場所の追加等を検討している。

項番	届出日	概要
30	2021/2/26	届出者（企業）のサーバにおいて、ファイルの拡張子が改ざんされていることに気づいた。調査したところデータ復旧のために身代金を要求するメッセージが見つかり、ランサムウェアに感染したことが判明した。フォレンジック調査の結果、VPN 装置の脆弱性の悪用により組織内ネットワークへ侵入され、数台のサーバのリモートデスクトップサービスへログオンされたことが原因と判明した。VPN 装置の脆弱性対策を行い、さらに VPN の認証方式に多要素認証を導入することを検討している。また、ログ管理・監視の仕組みを強化し、セキュリティ専門の部署による運用体制の確立を行った。
31	2021/3/4	届出者（企業）で利用していたパソコン数台において、ファイルが暗号化されていることを発見した。調査したところ、ランサムウェアによってファイルが暗号化されたと思われる状況であった。ウェブサイトの閲覧により感染したものと推測しているが、詳しい感染経路や原因は不明である。
32	2021/3/18	届出者（企業）の海外のサーバがランサムウェアの被害に遭い、国内のシステムにも影響が生じ、情報漏洩の可能性が発生した。詳細は調査中である。
33	2021/3/22	届出者（企業）が利用するファイルサーバにおいて、ファイルが暗号化され、ファイル名の拡張子が改ざんされていることに気づいた。またデータ復元のために身代金を要求するメッセージが書かれたファイルが置かれていた。調査したところ、脆弱性のあるクライアント端末が見つかったため、それを悪用されて侵入されたと推測しているが、詳しい原因等は不明である。

項番	届出日	概要
34	2021/4/8	届出者（企業）のファイルサーバ上のファイルが暗号化され、ドメインコントローラのサーバにデータ復旧のために身代金を要求する脅迫文が置かれていたことを発見した。専門業者による調査結果では、クラウド上に設置していた仮想 VPN 装置の脆弱性の悪用により攻撃者が認証情報を窃取し、侵入したのちに当該サーバをランサムウェアに感染させたと推測している。当該 VPN 装置は評価用に準備したものであったため、本件を受け VPN 装置は停止させ、パスワードの変更も実施した。攻撃されたサーバはバックアップを用いて復旧させたが一部のデータは損失した。今後の対策として、システム構成の再検査や定期的な脆弱性診断、セキュリティ教育の実施等を進めていくとしている。
35	2021/4/8	届出者（企業）が利用しているサーバ上のファイルが暗号化されていることを発見した。調査したところ、サーバ上にデータ復旧に身代金を要求する脅迫文が書かれたファイルが存在していたことから、ランサムウェアに感染したと思われる状況であった。暗号化されたファイルはバックアップから復元した。本件を受け、すべてのパソコンに対してウイルスチェックを行うとともに、サーバやアカウントのパスワードポリシーの強化、バックアップ方法の変更を実施・検討している。
36	2021/4/9	届出者（企業）が使用するレンタルサーバの機能が動作せず、メールシステムや EC サイトを含むウェブサイトが表示されなくなった。運用保守業者に確認と復旧を依頼したところ、一部のファイルが削除されており、データ復旧のための身代金を要求する英文のメッセージが残されていたことが判明した。削除されたファイルに顧客情報が含まれていたことからカード情報等が流出した恐れがある。調査の結果、サーバの何らかの脆弱性を悪用して外部から OS コマンドの実行が可能な状態であったと考えられるが、ログ等に攻撃の証跡は確認できなかった。被害に遭った EC サイトは廃止して、カード情報をサーバに残さない構成となる新たな EC サイトをクラウド上に構築する予定である。

項番	届出日	概要
37	2021/4/14	届出者（企業）が利用するパソコンでウイルスが検知され、正常に動作しない状態に陥った。協力会社とともに調査を行ったところ、サーバのファイルが暗号化され、復旧のために身代金を要求する脅迫文が置かれていたことから、当該のパソコンやサーバを含めて 80 台以上の機器がランサムウェアの感染被害に遭っていたことが判明した。また、発生の数日前に不審なメールの添付ファイルを開いた従業員がいたことがわかり、さらに、別の従業員のパソコンから攻撃に使われたと思われる adfind と呼ばれる Active Directory からユーザ情報を収集するツールが発見された。これらのことから、攻撃メールにより攻撃者に組織内へ侵入され、認証サーバの情報を窃取されて被害が拡大したものと推測している。全てのパソコンとサーバに新しいセキュリティソフトを導入して対策した。また、システム構成や情報セキュリティ運用管理体制の見直しを検討している。
38	2021/4/26	届出者（企業）が運営する会員向けサービスのウェブサイトで、データの一部が欠損し画像等が表示されていないことを発見した。調査したところ、クラウド上の設定不備があったため、攻撃者からアクセスされてしまい、データを削除され、復旧のため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。本件の対応として情報管理や体制の見直しと強化、セキュリティ診断の実施、監視体制の強化を行った。
39	2021/5/6	届出者（企業）が提供する ASP サービスにおいてシステムエラーが発生したことを監視システムが検知した。調査したところ、複数のファイル暗号化やファイル名の改ざんがされたために、システムが停止していたことを発見した。さらにデータ復旧のために身代金を要求するような文面が記載されたファイルの存在も確認したことから、ランサムウェアによる攻撃を受けたものと判断した。一部サーバで外部からのリモートアクセスを許可していたことから、何らかの手段で認証を突破され不正アクセスされたと推測される状況であった。再発防止策として、ネットワークとエンドポイントの双方に監視・対策の装置やソフトウェアを導入してセキュリティの強化を図った。

項番	届出日	概要
40	2021/5/15	届出者（企業）のサーバがランサムウェアに感染した。何らかの脆弱性を悪用されたと推測しているが原因の詳細は不明である。
41	2021/5/25	届出者（企業）の社内設置サーバ 2 台が外部ネットワークから不正アクセスされ、ランサムウェア攻撃の被害に遭った。ランサムウェアにより、サーバ内のファイルが暗号化されサーバが動作不能になり、業務の一時停止に陥った。バックアップからデータを復元することでサーバは復旧した。不正アクセスの原因は VPN 装置の脆弱性を悪用されたものと推測しており、再発防止策として、VPN 装置のファームウェアを脆弱性対策済みのものにアップデートした。
42	2021/5/26	届出者（企業）の業務用サーバ 10 台のファイルが暗号化されていることに気づき、調査した結果、Sodinokibi と呼ばれるランサムウェアに感染したと判断した。攻撃者は何らかの方法で社内端末にバックドアを仕掛け、社内ネットワークに侵入し、内部偵察を行って攻撃対象サーバの特定や認証情報の窃取をしたのちにサーバに侵入したと思われる。事象発覚後、各サーバを初期化し、バックアップからデータを復元してシステムを復旧させ、セキュリティソフトを導入して再発防止を図った。全サーバを復旧するのに 5 日間ほどを要した。

項番	届出日	概要
43	2021/6/10	届出者（企業）の複数のパソコンがランサムウェアに感染したことと、10 台以上のファイルサーバのデータが外部に漏洩したことが発覚した。調査会社によるフォレンジック調査の結果、攻撃者は VPN 装置の脆弱性を悪用して社内ネットワークに侵入した後に、AD サーバを乗っ取り、ランサムウェアを拡散したことが判明した。さらに攻撃者は、ファイルサーバに、インターネット上のオンラインストレージへデータを転送する正規のソフトウェアを仕込みデータを窃取し、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行っていた。感染したシステムは初期化し、バックアップデータから復旧させた。対策としてシステムアップデート、アカウント無効化と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製品の追加導入を行い、さらにセキュリティインシデントの常時監視や、脆弱性対応の強化を実施するとしている。
44	2021/6/16	届出者（企業）の社内システムが障害を検知し、確認したところ、複数台のサーバ上のファイルが暗号化されていることが判明した。セキュリティ専門業者とともに調査したところ、外部から不正にリモートアクセスされた痕跡が見つかったため、攻撃者が VPN の認証を何らかの方法によって突破し、サーバに侵入してランサムウェアを実行したと思われる状況であった。本件への対応として、暗号化されたファイルをバックアップから復元することでシステムを復旧し、さらに再発防止に向け EDR の導入、ソフトウェアのバージョンアップ等を実施した。

2-3. ID とパスワードによる認証を突破された不正アクセス

利用者やシステム管理者による ID やパスワード運用・管理の問題によって不正アクセス被害に繋がったと思われる事案の届出が 31 件と多く、中でも特にメールシステムのアカウントに不正アクセスされ、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 19 件と最も多かった。

メール送信の踏み台にされた事例は、大きく分けて SMTP 認証の ID とパスワードを突破されてしまったものと、クラウド型のメールサービスのアカウントへ不正にログインされてしまったものがあった。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り、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。また、様々な認証方式が提供されているクラウド型のサービスにおいても、多要素認証を使用しておらず ID・パスワード認証のみで利用可能としているのであれば同じことが言える。さらに一部のクラウドサービスでは、SMTP サービスが有効化されているなど、システム管理者が想定しているログイン時の認証方式によらず ID・パスワードのみでメール送信が可能な場合もある。いずれにせよ ID やパスワードの管理強化が不正アクセスへの耐性に大きく影響するため、適切なパスワードを設定し、ID とともに厳重に管理することが重要である。あわせて可能であればアクセス制限や多要素認証など他の技術も組み合わせ、セキュリティ強化を図ることが望ましい。

なお、先期に多く見られた、企業等が提供する会員向けサービスのログインページへ大量のログイン試行を行う攻撃に関する届出は、今期は 5 件と比較的少なかった。このうち 1 件は、以前に不正アクセスの被害に遭い、サービス提供者側で対策を行ったが、一部の利用者（会員）のパスワード管理の問題により再度被害に遭ったと考えられるものであった。具体的には、1 回目の被害の際に、パスワード情報が漏洩した可能性を考え、対策として会員のログインパスワードをリセットする処置を行ったが、一部の会員は以前と全く同じパスワードを設定していたため、パスワードリスト攻撃の被害に遭ったというものである。

ID とパスワードによる認証方式を突破される不正アクセスは、古くからある被害の一つであり、現在でも継続して多くの被害が発生している。メールシステムの場合は、過去に送受信したメール（機密情報・個人情報）の漏えいに繋がったり、踏み台にされて攻撃メールを外部にばら撒くことで、関係者に被害をもたらしたりすることがあり得る。EC サイトや会員制ウェブサイトの場合は、個人情報に加えて金銭的な被害に直結することもある。これらは攻撃者から狙いやすい標的であり、被害防止のため利用者とサービス提供者の双方での対策が重要である。サービス提供者側は、強固なパスワードの設定を促したり、多要素認証方式を提供したりして、利用者側がそれらを適切に活用することが理想である。また、不正アクセスが発生し得るという前提で、大量のログイン試行や不正なログインを早期に検知できる仕組みといった対策も導入することが望ましい。

表 2-3 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 2-3 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		
45	2021/1/6	届出者（企業）が使用するシステムにおいて、一部のアカウント情報が窃取され、過去にメールを送った届出者の顧客に対して、届出者からの返信を装った不審メールが 1500 通以上送信された。パスワードをさらに強固なものに変更することで対策を行い、さらに本件の調査完了後には不審メールの送信に使われたアカウントを削除する予定である。
46	2021/1/14	届出者（企業）の従業員から不審なメールが送られてきたとの報告が別の従業員からあった。調査したところ、送信者である従業員のメールアカウント情報が過去にフィッシングメールによって詐取されており、攻撃者がそのアカウント情報を悪用して不正にログインし、フィッシングメールを数百件にわたり社内外に送信していたことが判明した。当該従業員のメールアカウントを停止する措置を行うとともに、再発防止のためメールシステムの二要素認証やメール大量配信の自動停止の仕組みの導入、全従業員に対する不審メールに関する教育の実施などを行った。
47	2021/1/18	届出者（地方自治体）の組織内でメールの送信遅延が発生したため調査したところ、メールアカウントの一つが海外から不正アクセスを受け、スパムメールの配信の踏み台にされていることが判明した。調査の結果、当該アカウントの認証がパスワードリスト攻撃により突破されたと考えられる状況であったが、詳細な手口については不明である。対策として、メールアカウントのパスワードの文字数を増やして強度を上げた。また、メールシステムへ接続できる IP アドレスを国内だけに制限し、さらに細かいアクセス制限の実施を検討している。

項番	届出日	概要
48	2021/1/20	届出者（企業）が利用するメールサービスのアカウントから、ウイルス感染を狙ったと思われるメールが送信されていた。専門業者の調査により、クラウド型メールサービスの SMTP サーバに対する届出者組織の ID での不審なアクセスが見つかった。何らかの手段でメールアカウントの認証情報を入手した攻撃者が、それを悪用して攻撃メールをばらまいたものと推測される状況であった。
49	2021/2/12	届出者（企業）が利用するクラウド型メールサービスのアカウントに不正にログインされ、大量の迷惑メールが送信されたことを発見した。調査したところ、攻撃者は何らかの方法によって、アカウント情報を不正に入手したと考えられることが判明した。本件を受けた対策として二要素認証の導入、パスワードポリシーの徹底や日次でのセキュリティソフトのアップデートとスキャンを行うこととした。
50	2021/3/1	届出者（企業）が利用するメールアカウントの一つにおいて、メールの送受信ができない状況になっていた。メールサーバの業者に確認したところ、当該アカウントから約 1500 通の不審なメールが送信されていたため、アカウントの停止措置が取られていたことが判明した。専門業者とともに調査したが、社内からウイルス等は見つからなかったことから、メールアカウントの認証情報を不正に入手した攻撃者が、メールサーバを踏み台にして不正なメールをばらまいていたと推測される状況であった。社内のセキュリティ規程を改定し、設定変更等を実施しセキュリティ強化を図った。

項番	届出日	概要
51	2021/3/2	届出者（企業）において、自組織内の利用者より突然大量のエラーメールを受信するようになったとの報告があった。調査したところ、自組織のメールサーバから外部宛てに数千件のスパムメールを送信していたことが判明し、宛先不明等で戻ってきたエラーメールを多数受信している状態であることがわかった。当該利用者のパスワードがアカウント名から推測されやすいものであったため、アカウントが乗っ取られスパムメール送信の踏み台にされたと推測している。外部からメールサーバへのアクセスを制限するとともに、監視を行うこととし、また定期的にパスワード変更を行うことで再発防止を図った。
52	2021/3/17	届出者（地方自治体）が契約しているメールサービスの事業者から、短期間に大量のメール送信が発生しているとの連絡があった。調査の結果、攻撃者が何らかの方法で正規のメールアカウントの認証情報を窃取して不正アクセスし、当該アカウントから 2 千通以上のメールを送信した可能性が高いと考えられる状況であった。発覚後すぐに、当該メールアカウントのパスワードを変更し、利用していないメールアドレスの削除等の棚卸を実施した。まず短期的な対策としてパスワードを定期的に変更する運用とし、長期的な対策としては、よりセキュリティレベルの高いサービスへの移行や、利用端末の制限などを実施する予定としている。
53	2021/3/18	届出者（教育・研究機関）が管理するメールシステムで、複数のアカウントに対して不正アクセスされ、組織外に対して不審なメールが送付された。ID とパスワードが漏洩したことが原因としているが流出経路等は不明であり、関係機関と連携してフォレンジック調査を実施している。対策として、不正アクセスされたことが判明したアカウント含め、関係者のパスワード変更を実施した。根本対策や再発防止策は調査の結果を受けて検討する予定としている。

項番	届出日	概要
54	2021/4/9	メールサーバ管理会社からの連絡により、届出者（企業）のメールサーバから数百通の不審メールが送信されていることが発覚した。調査したところ、メールアカウントのパスワードが予測されやすいものであったため、攻撃者に認証を突破されて不正アクセスされ、不正なメールの送信が行われたと判断した。対策として、不正アクセスを受けたアカウントのパスワード変更を行い、また、メールシステムも社内ネットワークから VPN で接続するものへ移行した。
55	2021/4/22	届出者（教育・研究機関）が運営するメールサービスの利用者から、大量の配送エラーのメールが着信していることが報告された。調査したところ、当該利用者のメールアカウントに不正アクセスされ、千通以上の迷惑メールを送信されていたことが判明した。なお、不正にログインされた原因は不明であった。職員など全利用者に対して注意喚起等を行った。
56	2021/5/14	届出者（公共機関）のメールサーバから不審なメールが送信されていたことが、利用するメールサービスの業者からの連絡により発覚した。過去にメールシステムを更新した際に、外部から SMTP サーバへのアクセスを許可する必要が生じたため、外部からのアクセス制限をしていなかったことと、SMTP 認証のパスワード強度が低いアカウントが存在していたことにより、外部からの不正なメール送信に悪用されたと考えられる状況であった。対策として、システム構成を見直し外部からのアクセスを制限するとともに、アカウント管理ポリシーを変更してセキュリティ強化を図った。

項番	届出日	概要
57	2021/5/19	届出者（一般団体）が利用するクラウド型メールサービスのアカウントに不正にログインされ、不審なメールを送信されていたことが、メール受信者からの問い合わせによって発覚した。送信されたメールは、過去に送信した正規のメールが引用されており、さらに不審なファイルの添付や不審な URL リンクが本文に記載されていた。不正なログインの原因は定かではないが、ログイン試行回数の制限を設けていたため、総当たり攻撃ではなく、フィッシング等で窃取したパスワードを悪用された可能性が高いと推測している。再発防止策として、海外からのアクセスを拒否するようにアクセス制限を実施し、さらにログイン時の二段階認証の導入を検討している。
58	2021/6/8	届出者（企業）が利用するクラウド型メールサービスのアカウントに不正にログインされ、不審な URL が記載されたメールが数十件送信された。本事案は不正アクセスされたアカウントに配信エラーのメールが複数届いたことで発覚した。原因は不明だが、当該アカウントのパスワード強度が低かったため、何らかの方法で認証を突破されたと推測している。再発防止策として、パスワード設定方法について全社への注意喚起を行うとしている。
59	2021/6/9	届出者（一般団体）が利用するメールアカウントに、送信した覚えのないメールが送信先不明でエラーとなって、配送不能を通知するメールが数十通着信していることを発見した。調査したところ、何らかの手段で当該メールアカウントのパスワード情報を窃取した攻撃者にメールアカウントを悪用され、メールの送信がされたと思われる状況であった。本件を受けて、メールアカウントのパスワード変更およびウイルススキャンの対応を行った。

項番	届出日	概要
60	2021/6/10	届出者（企業）が利用するクラウド型メールサービスのアカウントに不正にログインされ、不審な URL リンクが記載されたメールが従業員や取引先へ送信されたことを、受信者からの連絡により発見した。また、当該アカウントに保存されていたメールが漏洩した可能性がある。不正アクセスの原因は不明であるが、別のサービスとのパスワードの使い回しがあったことから、何らかの原因で漏洩したパスワードを不正アクセスに悪用された可能性がある。再発防止策としてパスワードの変更、多要素認証の導入、FIDO の導入を行う。
61	2021/6/26	届出者（非営利団体）の職員のメールアカウントに、2 千通以上の配送エラーを通知するメールが着信した。エラー通知メールの内容を確認したところ、海外の不審な IP アドレスからメールサーバへアクセスがあったことと、当該職員のメールアカウントからフィッシングメールが多数の宛先に向けて送信されていたことが判明した。当該職員のアカウントに着信したメールは宛先不明等で配信できなかったことを通知する内容であった。何らかの手段によりメールアカウントの認証情報が窃取され、不正アクセスされたと推定される状況であった。このため、当該アカウントのパスワードを変更することで対策した。
62	2021/6/28	届出者（教育・研究機関）が利用するクラウド型メールサービスにおいて、職員のメールアカウントに不正アクセスがあり、送受信したメールと、それらメール内に記載されたメールアドレスの情報が窃取された。窃取されたメールアドレスが悪用されて、外部のサーバから当該職員を装った不審メールが組織内外に送られていたことに、メールを受信した別の職員が気づき発覚した。送られたメールには、過去にやり取りしたメールの内容が記載されており、また、ZIP ファイルをダウンロードさせようとする不審な URL リンクが記載されていた。不正アクセスの原因は不明だが、パスワードの使い回しによる流出やフィッシング等による流出した認証情報を悪用されたものと推測している。再発防止策として、導入済みだった多要素認証を必須化することとし認証の厳格化を図った。

項番	届出日	概要
63	2021/6/28	届出者（教育・研究機関）が利用しているメールアカウントにおいて、約 7 千通の配送エラーを通知するメールが届いていることを発見した。メール送信(SMTP)のログを確認した結果、当該アカウントから、心当たりのないメールが大量に送信されていることが判明した。それらのメールは 1 秒間に 6 通ほどのペースで、計 2 万件以上のアドレスに送信されていた。利用していたメールサーバでは SMTP 認証を必須としていたため、何らかの理由で当該アカウントの認証情報が漏洩し、不審メールの送信の踏み台にされたと推測される状況であった。再発防止のためにメールサービスの利用制限設定を変更し、ウェブメールのみ使用可能として SMTP による送信を禁止する措置を取った。
パスワードリスト攻撃など大量ログイン試行による不正アクセスの事例		
64	2021/2/10	届出者（企業）が提供する EC サイトにおいて、数十件ほどのログイン試行がされていることを WAF が検知した。調査により、一部は不正なログインに成功されてポイント交換（未遂）等の不正使用が行われていたことが判明した。このサイトは以前、不正アクセスの被害に遭った際、会員のパスワードを強制リセットする対策をしていたが、一部の利用者はリセット後も同一のパスワードを再設定していた。今回の不正アクセスには、これら一部の利用者の認証情報が悪用されたことがわかった。対策として、接続元 IP アドレスの制限と再度のパスワード変更を行った。さらに再発防止策として、ワンタイムパスワード認証の導入と、前回と同じパスワードの設定禁止といった対策を予定している。

項番	届出日	概要
65	2021/2/10	届出者（企業）が提供する EC サイトにおいて、単一の発信元 IP アドレスから複数の ID でログインの試行がされていることを WAF 機器が検知した。調査したところ、他にも国内外から多数のログイン試行があり、一部は不正なログインに成功され、数十のアカウントについて、会員情報の閲覧やクレジットカードの不正使用等が行われていたことが判明した。不正ログインされたアカウントの利用者に確認したところ、全員が過去にフィッシングサイトへ認証情報を入力してしまったことがあることがわかった。この攻撃では、その他の情報源を基にして作られたリストによるパスワードリスト攻撃が行われたと考えられる。対策として、接続元 IP アドレスの制限や、ワンタイムパスワードによる認証の導入、被害に遭った利用者のパスワード変更およびクレジットカード情報の変更を行った。
66	2021/2/17	届出者（企業）が提供するサービスのウェブサイトが不正アクセスされ、利用者の情報などが不正に閲覧された。WAF による DDoS への対策は行っていたが、不正なログインは検知することができず、アクセスログが異常に増大したことにより攻撃に気づいた。不正なログインに悪用された ID が、過去に別サービス等から漏洩したものであったことなどから、パスワードリスト攻撃を受けたものと推測される状況であった。対策として、不正アクセスの発信元 IP アドレスからの通信を遮断することに加え、不正アクセス検知ができるように WAF の設定を追加する対策を実施した。また ID とパスワード以外の認証方式を追加で導入することを検討している。
67	2021/5/17	届出者（企業）が提供する会員向けサービスの利用者 1 名から、サービスへのログインができなくなったと問い合わせがあった。調査したところ、パスワードリスト攻撃が行われていたことが発覚し、当該利用者のアカウントに不正アクセスされ、ログイン ID を変更されていたことが判明した。対策として、連続したログイン試行や特定 IP アドレスから複数の ID に対するログイン試行があった場合の対策処置を行い、さらにパスワードポリシーの強化や reCAPTCHA の導入を行った。

項番	届出日	概要
68	2021/6/29	届出者（企業）の提供する利用者向けウェブサイトの高負荷を検知した。調査を行ったところ、複数の IP アドレスから大量にログインが試行されていたことが判明し、約 1 万件の利用者の ID への不正アクセスに成功され、一部の利用者の情報が不正に閲覧されたことも判明した。パスワードリスト攻撃により認証を突破されたことが原因と推測している。事前に WAF によって一定時間当たりのアクセス件数を監視していたが、設定していた閾値に届かない程度のスローペースでログイン試行が行われたため、検知することができなかった。本件の対策として、WAF の設定変更を実施した。さらに、多要素認証や画像認証等の認証方式の導入を検討中である。
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		
69	2021/1/14	届出者（教育機関）のメールサーバを踏み台にして、3 万通以上のスパムメールを送信されたことが、外部組織からの指摘により発覚した。調査したところ、踏み台にされたアカウントは 2 つあり、双方とも認証情報が漏洩したと報じられた外部のサービスと同一の ID とパスワードを使用していたことが判明した。また、当該アカウント以外でのログイン試行や認証エラーが見られないことから、当該外部サービスから漏洩した認証情報を攻撃者に入手され悪用されたと推測される。対策として、当該アカウントを停止するとともに、メールサーバにおいて外部からのメール配信の制限を行った。また、利用者へはパスワードの使い回しをしないように注意喚起し、さらにパスワードポリシーを変更してパスワードの強化を図った。上記に加え、二要素認証や一定回数のログイン失敗に対するロックアウト機能の導入も検討している。

項番	届出日	概要
70	2021/1/19	届出者（自治体）が管理提供するウェブサイトが改ざんされていることを確認した。調査の結果、海外から管理者 ID による不正なログインをされていたことが判明した。さらに、ウェブページへの不正な記事の投稿や、ウェブサイトの一部の利用者のメールアドレスが閲覧された恐れがあることを確認した。攻撃者は何らかの方法で管理者の ID とパスワードを入手し、それを悪用してログインしたと思われるが、認証情報の流出原因は不明である。対策として、不要な ID の無効化、パスワードの定期的な変更、管理者画面へのアクセス制限を行った。
71	2021/1/20	届出者（企業）が運用するウェブサーバから多数のメールが送信されていると外部から連絡を受けた。調査したところ、ウェブサイトの管理者画面に不正にアクセスされ、メールを送信する不正なプログラムの設置と実行により、数千通の不正なフィッシングメールが送信されていたことを確認した。対策として、不正アクセスを受けた管理者 ID の管理やパスワード管理の運用徹底、および管理者画面へのアクセス制限等を行った。
72	2021/4/13	届出者（企業）が運用する EC サイトの管理者の一人に、サーバの異常を知らせる偽のメールが着信した。当該管理者は偽のメールであることに気づかず、文中の URL リンク先のページにアクセスし、サイト管理者の ID とパスワードを入力した。その後、当該メールがフィッシングメールであることが発覚したため、管理画面へのアクセスログを調査したところ、不審な IP アドレスからのアクセスがあり、情報を閲覧された形跡があることを確認した。本件を受けて、全従業員に対してフィッシングメールに関する注意喚起を行った。

項番	届出日	概要
73	2021/4/20	届出者（教育・研究機関）のメールサーバから意図せず大量のメールが送信された。原因を調査したところ、あるメールアカウントに不正にログインされて大量の不審メールが送信されたことが分かった。当該アカウントのユーザは以前にフィッシングメールに記載されたURLにアクセスしてフィッシングサイトにアカウント情報を入力したことがあり、そこでアカウントの認証情報を窃取されたと推測される状況であった。再発防止策として、不正にアクセスされたアカウントのパスワードを変更し、さらに組織内の関係者へ本件に関する注意喚起文を発出した。
74	2021/5/18	届出者（企業）において、従業員のメールアカウントが無効化されメール送信ができなくなったことに気づいた。この際、当該アカウントへの不正アクセスをメールサービスが検知し、アカウントが無効化され、管理者へアラートメールが届いていたが、それに気付かず、管理者が当該アカウントを有効化した。その後、当該アカウントから１万通以上の何らかの不正なメールが送信された。調査したところ、海外の複数の国からログインの試行があったことが判明した。当該メールアカウントのパスワードは、パスワードポリシーに従ってはいたものの、人名と４桁の数値といった設定であったため、パスワードリスト攻撃等によって不正アクセスされたと考えている。本件を受けて、侵害を受けたアカウントのパスワード変更、パスワードポリシーの見直しおよびアカウントの運用管理の徹底等を行った。

項番	届出日	概要
75	2021/6/2	届出者（企業）が社内に設置したサーバが不正アクセスを受け、他社への攻撃の踏み台にされていたことが判明した。不正アクセスによりサーバの管理者アカウントのパスワードを変更されたため、正規のログインができなくなっていたことに気づき不正アクセスが発覚した。調査により、サーバの管理画面へ外部からアクセス可能な状態となっていたことがわかり、管理者アカウントのパスワードが脆弱だったため攻撃者に特定されてしまい、サーバに不正にログインされたものと推測している。再発防止のための対策として、サーバは社外とのアクセスは双方向とも遮断するように設定し、社外からのサーバ作業が必要な場合のみ、その都度通信先アドレスを限定したアクセスを許可するようにした。

2-4. 脆弱性や設定不備を悪用された不正アクセス

今期も、機器や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と思われる事例の届出が多く、本項に分類したものだけで 24 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ついては、脆弱性を悪用されて不正アクセスされたものであってもそちらに分類している。

内訳としては、ウェブシステムや CMS（Contents Management System）の脆弱性・設定不備の悪用の被害が 15 件と最も多く、EC サイトソフトウェアの脆弱性悪用による被害も依然として継続しており 3 件の届出があった。

そして、先期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 5 件と、先期の 3 件から増加した。身代金を要求するサイバー攻撃の事例に分類した届出の中にも VPN 装置の脆弱性が原因とされているものが 6 件あるため、合計すると 11 件となる。下半期に入った 2021 年 7 月以降も現時点で 5 件の届出を受領しており、現在も被害が継続して発生していると考えられる。

VPN は、テレワークなどを実現するため、外部から組織内のネットワークへの安全なリモートアクセスの実現に使われている技術であり、攻撃者から組織内の情報資産を守るためには最重要ともいえるセキュリティ要素である。VPN の認証等を突破されるなどして、ひとたび攻撃者に侵入を許してしまうと、被害は組織内ネットワークにある多数のサーバやパソコンなど、組織全体に及ぶこともあり得る。実際にそのような攻撃に遭い、甚大な

被害を受けた事例もあった。脆弱な状態の VPN 装置は攻撃者から積極的に狙われている状況であり、VPN 装置の脆弱性対策は優先度を上げて対応することを検討いただきたい。

なお、VPN に限らず脆弱性が悪用された事例では、脆弱性が長らく放置状態にあり、不正アクセスの発生後に、システムの利用者からの報告や外部機関からの通知などの外部からの連絡によって発覚し、システム運用担当者がその時点で初めて認知したというケースも見られた。ベンダーが公開した脆弱性が自組織のシステムに該当する場合、その対策を実施することは、システム管理者が能動的に実施できて、かつ効果が高いセキュリティ対策である。定期的に脆弱性情報を確認して計画的に対策ができるような体制や運用手順を確立することは非常に重要である。

表 2-4 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。

表 2-4 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
ウェブシステムや CMS の脆弱性・設定不備の悪用の事例		
76	2021/1/15	届出者（企業）が運営するウェブサイトに登録されていた個人情報が流出していると外部から連絡があった。調査したところ、ウェブサイトの脆弱性を悪用した不正アクセスにより個人情報が流出した可能性が高いと判断し、当該ウェブサービスの停止を行った。また、流出したデータには暗号化されてない状態のパスワードも含まれていたため、別のウェブサイトなどでパスワードの使い回しをしている利用者向けに、パスワード変更の要請を行った。当該ウェブサイトは停止し、別途新規にウェブサイトの構築を検討している。
77	2021/1/18	届出者（企業）が運営するサービスで使用しているサーバにおいて、CPU リソースの高負荷を検知した。調査したところ、不審なアクセス元から SQL インジェクションの脆弱性を悪用した不正アクセスされたことが判明した。不正アクセスにより 10 万件以上のメールアドレスの情報が窃取されたことが確認され、利用者からはそれらのメールアドレス宛のスパムメールに関する問い合わせが複数寄せられた。対策として、不正アクセス元からの通信を遮断し、SQL インジェクションの脆弱性修正を実施した。

項番	届出日	概要
78	2021/2/5	届出者（企業）が提供するウェブサイトおよびアプリに、企業と無関係な海外のサイトへ遷移するリンクが不正に掲載されていることを利用者からの連絡により認知した。管理者用サイトへの攻撃を疑い調査した結果、不正アクセスされ、ウェブサイトの利用者のメールアドレス数千件が流出した痕跡を発見した。詳細な原因は不明だが、当該サイトのセキュリティは、事前の内部審査により許可を受けていた運用と実際の運用が一部異なった状態であったことが判明し、十分なセキュリティレベルを確保できていなかった恐れがある。再発防止策として、セキュリティ審査を実施するルールの再徹底や不正アクセス等の監視の強化を行った。
79	2021/2/12	届出者（一般団体）が運営している複数のウェブサイトにおいて、管理画面にログインできなくなっていること、および不審なファイルがウェブサーバ上に置かれていることを発見した。サーバを提供するレンタルサーバ事業者と調査した結果、原因は不明であるが、CMS のバージョンが古かったことや、管理者の ID やパスワードの強度が弱かったことから、それらを悪用されて不正アクセスされたものと推測している。対策として、管理画面へのアクセス制限、各機能の自動アップデート運用を適用した。
80	2021/2/22	届出者（一般団体）が運用するウェブサイトが閲覧できなくなっていることを確認した。調査したところ、利用していた CMS の管理画面に不正にログインされ、一部のファイルが削除されていたことが判明した。当該ウェブサイトについては再構築を行った。再発防止策として、CMS について最新バージョンへのアップデート、ユーザパスワードの複雑化、管理者画面へのアクセス制限、管理者画面へのアクセス URL をデフォルト設定から変更する等の措置を行った。

項番	届出日	概要
81	2021/3/2	届出者（企業）が運営するウェブサービスに対して不正アクセスが行われていることを、当該サービスの保守業者が発見した。調査したところ、当該サービス上に SQL インジェクションの脆弱性があることが発覚した。この脆弱性を悪用されて外部から不正アクセスを受け、個人情報が漏洩した可能性が考えられることも判明した。本事案への対策として、ウェブサービスの脆弱性の対応、新基盤への移行を行い、定期的な脆弱性診断の実施および監視を行うことにした。
82	2021/3/23	届出者（企業）が運用するウェブサーバが閲覧・管理できなくなった。調査したところ、配置した覚えのない大量の不審な php ファイルが存在することを発見した。設定不備により、サーバ上にインストールのみされた未設定状態の CMS があり、それを攻撃者により不正に操作され、ファイルが設置されたことが判明した。当該サーバ上の不審なファイルを削除し、CMS 設置時のルールの策定や WAF の導入等により再発防止を図った。
83	2021/4/13	届出者（企業）の顧客に対して、届出者を装う数万通の偽メールが一斉送付された。当該メールを届出者自身も受信したことで発覚した。調査の結果から推定する限り、届出者のウェブサイトに存在した脆弱性の悪用により不正アクセスされ、さらにウェブサイトからメール配信システムを悪用されて、大量のメールが送られたものと考えられる。対策として、ファイアウォールによるアクセス可能な IP アドレスの制限等を実施し、さらに脆弱性検査や WAF の導入等で更なるセキュリティ強化策を検討している。
84	2021/4/21	届出者（企業）のウェブサーバ内の複数ファイルに不正なスクリプトが仕込まれ、ウェブサイトの訪問者が、閲覧中に意図しない外部サイトに遷移させられることを確認した。ウェブコンテンツの管理に利用していたソフトウェアの脆弱性を悪用され、ファイルが改ざんされたと推測している。なお、当該システムには WAF が導入されていたが、正規の通信と判断され検知・防御することができなかった。対策として、原因と思われる箇所を修正し、また再発防止策として、定期的な脆弱性検査を実施することとした。

項番	届出日	概要
85	2021/4/25	届出者（企業）が委託運営するウェブサイトが改ざんされて別のサイトに遷移するようになっているとの報告をウェブサイトの利用者から受けた。調査により、サーバ内に不正なプログラムが配置されていることを発見したが、配置された原因は不明であった。本件の届出者はサイトのコンテンツ等の運用のみを委託されている立場であり、委託元で脆弱性対応を行う体制が存在していなかったことから、再発防止策として、セキュリティを含む保守を行う業者の調達や、適宜 CMS のバージョンアップを行うよう、委託元へ提案することとした。
86	2021/5/24	届出者（教育・研究機関）のウェブシステムのコンテンツが改ざんされ、不審な URL リンクが埋め込まれていることに気づいた。ウェブシステムを構成する PHP のプログラムが古く、SQL インジェクションやディレクトリトラバーサルの脆弱性が見つかったことから、それらの脆弱性を悪用されて、不正アクセスによる改ざんをされたと推測される状況であった。本システムは、組織で実施していたセキュリティ施策の対象から外れていたため、それら対策が有効に機能していなかった。再発防止策として、組織内で稼働しているシステムの棚卸しをして、施策の対象外となっているシステムがないことを確認した上で、トラフィックやログの監視強化、EDR システムの導入などを進めている。
87	2021/6/7	届出者（企業）が自組織内に設置して運用するサーバにおいて、ウイルスを検知した。調査を行ったところ、独自開発したアプリケーションに脆弱性が存在しており、外部からその脆弱性を悪用した SQL インジェクション攻撃が行われて、ウイルスが外部から不正にダウンロードされ、実行されていたことが判明した。また、サーバ内部に保存していた個人情報が流出した可能性があることも判明した。このため、別の手段により当該システムの機能を代替することとして、被害に遭ったサーバは停止した。再発防止策として、定期的な脆弱性診断と監査を行うこととし、対策すべき内容をサーバ管理者へ周知するように社内ルール化した。

項番	届出日	概要
88	2021/6/8	届出者（企業）が運用するウェブページのレスポンスが悪化しているとの報告があった。調査したところ、ウェブサーバへのブラインド SQL インジェクション攻撃が行われていたため、負荷が大きくなり、レスポンス低下を招いていたことがわかった。また、ウェブサーバで SQL インジェクション攻撃が行われた際のエラー結果がブラウザへ出力される設定となっていたことにより、会員のメールアドレスが窃取された恐れがあることも発覚した。本件を受けて、プログラムを修正し、SQL インジェクション攻撃への対策と、エラー結果表示の是正を行った。さらに再発防止のため、WAF の導入、既存のサーバの安全性確認、社内の開発におけるセキュリティ機能のチェックの強化、従業員への教育の強化等を検討している。
89	2021/6/14	届出者（一般団体）が運用するサーバが、外部のサーバを攻撃していると海外の組織から連絡があった。調査したところ、当該サーバ上に CMS の初期設定のためのファイルが第三者からアクセス可能な状態で置かれていたため、そのファイルを悪用されて管理権限を奪われ、他のサーバへの攻撃が行われていたこと、また当該サーバに保存していた数千件の個人情報等が窃取された恐れがあることが判明した。本件の対応として、サーバの移転および個人データの管理方法の徹底を行った。
90	2021/6/24	届出者（企業）が運用するウェブサイトにアクセスできなくなっていることを発見した。調査したところ、CMS の管理画面に不正にログインされ、多数の不審なファイルを設置され、サイトに対してアクセスすると強制的に別のサイトへリダイレクトする設定がされていた。本件を受けてサーバの移転および WAF の設定等を行った。

EC サイトソフトウェアの脆弱性悪用の事例		
91	2021/2/15	届出者（業界団体）が外部業者に委託して運営するオンラインストアが、第三者からの不正アクセスを受け、顧客情報が流出したことが、クレジットカード会社からの連絡により発覚した。調査により、システムの一部に脆弱な箇所があったことが判明したが詳しい原因は不明である。対策として、システム基盤にセキュリティ機能を備えたサービスを採用し、定期的なペネトレーションテストや教育等を行うこととした。また、外部委託の契約時には、セキュリティ条項の定義を行うことを必須とした。
92	2021/4/26	届出者（企業）が運営する EC サイトにおいて、クレジットカード情報が漏洩している可能性があるとの連絡を外部から受けた。決済システムを停止して専門業者による調査を実施したところ、当該サイトで使用していた EC サイトソフトウェアにおいて未対応の脆弱性が存在していたことが判明し、この脆弱性を悪用した不正アクセスが行われたと推測される状況であった。再発防止を含む対応として、すべてのサイトで SSL へ移行を実施し、EC システムは ASP 型のサービスに移行した上でセキュリティ維持運用サービスを利用することとした。
93	2021/5/18	届出者（企業）が運営する EC サイトが改ざんされ、外部から任意のプログラムが実行可能になるようなバックドアを仕込まれた。EC システムからサイト運用者へ送信されるメールに意図しない文字列が含まれていることに気づき、調査を行ったことにより発覚した。サイトを構成する EC サイトソフトウェアの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存在し、それを悪用されて、最終的に不正アクセスされたと考えられる。プラグイン提供元に修正を依頼し、対策版を適用することで対策した（ゼロデイ攻撃であった）。さらに再発防止のため、脆弱性診断の実施とクラウド型 WAF の導入を予定している。

VPN 装置の脆弱性悪用の事例		
94	2021/1/4	届出者（地方自治体）が利用する VPN 装置に未対策の脆弱性があることが、当該装置のメーカーからの連絡により発覚した。不正アクセスの形跡や情報の漏洩はなかったことを確認している。ネットワークを運用管理する業者と協議し、セキュリティアップデートを実施することで脆弱性対策を実施した。また、早期警戒情報などを活用して、最新の脆弱性対策情報をネットワーク管理業者と共有して対策していくことにより再発防止を図った。
95	2021/1/28	届出者（地方自治体）が利用する VPN 装置に未対策の脆弱性があることが判明した。脆弱性対策がされていない VPN 装置の IP アドレス一覧を入手した報道機関からの連絡により発覚した。VPN 装置の管理は保守業者に委託しており、業者によると、脆弱性の対象となる機能は利用していなかったことから、危険性はないと判断して本脆弱性対策は実施していなかったとのことだった。本件の発覚を受けて業者と協議し、当該装置のログ調査とバージョンアップ作業を実施した。不正アクセスの形跡や情報の漏洩はなかったことを確認している。
96	2021/3/7	届出者（教育機関）において、組織内の利用者が VPN 接続に使用する認証情報が外部に漏洩していたことを確認した。VPN 装置に脆弱性が存在していたため、それを悪用した攻撃により装置内部に格納されていた情報を窃取されたと考えられる。対策として、最新の修正プログラムを適用して脆弱性を解消するとともに、漏洩した認証情報を無効化して利用者に新たな認証情報を付与した。

97	2021/5/31	届出者（企業）のサーバにおいて、ウイルスが検知されたため調査したところ、攻撃者が使ったと思われるツール等が発見され、不正アクセスされていたことが発覚した。また、ファイルサーバを含む業務システムのサーバやクラウドサービスのアカウントにも不正アクセスされた痕跡が見つかり、個人情報を含むデータの窃取や、クラウドサービスからの不審なメールの送信が行われたことが判明した。詳細な原因は調査中だが、状況から VPN 装置の脆弱性を悪用され、アカウント情報が窃取されたことが原因と推測している。再発防止策として、多要素認証の導入等で認証方式の強化を図り、さらに監視運用管理の体制を強化することとした。
98	2021/6/10	届出者（企業）の従業員が、別の従業員から送られた不審なメールを受信したため、調査を行ったところ、社内外に対してそれぞれ数通ずつ、不審なファイルが添付されたメールが意図せず送信されていることが判明した。VPN 装置およびメールサーバへ侵入された痕跡を発見したことから、外部から VPN を経由してメールサーバに不正アクセスされたことが原因と推測している。なお、全ての受信者で添付ファイルの開封はしていないことを確認できている。本件を受けて、パスワードの再設定、セキュリティソフトの更新、VPN の再構築等を行い、標的型攻撃メールの対応訓練を行った。
その他の脆弱性悪用の事例		
99	2021/3/5	サーバソフトウェアの脆弱性がベンダーにより公開されたため、届出者（教育・研究機関）が自組織のシステムの調査を行ったところ、脆弱性を悪用した攻撃の可能性があるログを発見した。更なる調査を行い外部の専門家にも相談した結果、偵察行為のみで被害はなかったと判断した。本件の対応として、サービスを停止して本脆弱性への修正プログラムの適用を行った。

2-5. サプライチェーンに関するインシデント

今期の特徴として、自組織のシステム開発やサービス提供のために利用していた外部のサービスや、業務を委託していた先の事業者のシステムに対して不正アクセスがあり、そ

の影響を受けて、自組織のシステムやサービスが停止したり、情報が漏洩したりした事案の届出が目立ったことがあげられる。昨今、企業等の活動において、サービスや製品等の供給と利用が複雑に絡み合っているなか、その一部が被害に遭うなどして、関係組織や全体が影響を受けるという、サプライチェーンに関するリスクやインシデントの発生が社会的な課題となっている。

SaaS 等の形態で提供されるサービスを活用してシステムを構築することは、機器の調達や導入の作業、基本ソフトウェアの初期設定作業が不要なため、短いリードタイムでシステムを稼働できること等の利便性から、普及が進んでいる。さらに、基盤部分に対する修正プログラム適用やバージョンアップといったメンテナンス作業もサービス提供者に任せることができ、利用者側はいつでも最適な環境が利用できることも大きなメリットと言える。その一方で、メンテナンス作業は基本的に提供者側の裁量で行われるため、例えばバージョンアップに伴う仕様変更等があっても、利用者側でその内容を正確に把握して追随することが難しい場合もある。届出の中には、仕様変更に伴って利用者側での設定変更が必要だったにもかかわらず、正確な反映ができずに、設定不備が生じてしまった事例があった。今後とも、必要なセキュリティ措置がなされるよう、サービスやソフトウェアの供給者側からの十分な情報提供と、利用者側での注意の両方が求められるであろう。

また、業務委託のケースでは、委託者と受託者での作業分担が明確になっておらず、定期的なセキュリティ対策作業が実施されず脆弱性が放置されてしまっていた事例があった。SaaS 等のサービス仕様や、業務委託の契約書を確認して責任分界点を正確に把握した上で、定期的なセキュリティ対策作業や、不正アクセスを含めたインシデント発生時の作業分担と対応フローを明確にしておくことが重要である。

表 2-5 にサプライチェーンに関するインシデントの届出の概要一覧を示す。また、ASP サービス基盤への不正アクセスによりサービス停止に陥った被害について、項番 116 の事例の詳細を 5 章で紹介する。

表 2-5 サプライチェーンに関するインシデントの届出の概要一覧

項番	届出日	概要
100	2021/2/4	届出者（企業）の管理するクラウド上のシステムに対して、外部から設定不備の連絡を受けた。調査したところ、SaaS 基盤使用時の設定に不備があり、攻撃者に悪用されてシステムにアクセスされ、数百件の個人情報が流出したことを確認した。システムを一時停止し、セキュリティ管理の見直しとシステムの再構築の検討を行った。

項番	届出日	概要
101	2021/2/16	届出者（地方自治体）が利用しているクラウドサービスに関して、委託先の事業者から設定不備の恐れがあるとの連絡を受けた。調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されてシステムにアクセスされ、個人情報が不正に閲覧されたことを確認した。委託業者が設定を修正して問題を解消するまで一時的にシステムを停止する対応を行った。
102	2021/2/17	届出者（地方自治体）が利用しているクラウドサービスに関して、委託先の事業者から設定不備の恐れがあるとの連絡を受けた。調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されてシステムにアクセスされ、個人情報が不正に閲覧されたことを確認した。委託業者に対して設定の修正を依頼し対応するとともに、再発防止策の検討を要請した。
103	2021/2/22	届出者（企業）が SaaS 基盤を利用して提供していたシステムに関して、内部の情報に対する、外部からの意図しないアクセスがあったことが確認された。調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されて情報を不正に閲覧されたことが判明した。ただちに設定を是正する対応を行った。
104	2021/2/24	届出者（地方自治体）が利用しているクラウドサービスに関して、委託先の事業者から設定不備の恐れがあるとの連絡を受けた。調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されてシステムにアクセスされ、個人情報が不正に閲覧されたことを確認した。委託業者が設定を修正する対応を行った。
105	2021/2/25	届出者（地方自治体）が利用しているクラウドサービスに関して、委託先の事業者から設定不備の恐れがあるとの連絡を受けた。調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されてシステムに不正にアクセスされ、個人情報が不正に閲覧されたことを確認した。委託業者が設定を修正する対応を行った。

項番	届出日	概要
106	2021/3/11	届出者（地方自治体）が利用しているクラウドサービスに関して、監督官庁からセキュリティ設定の確認依頼があった。委託先の事業者と調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されてシステムにアクセスされ、個人情報が不正に閲覧されたことを確認した。委託業者が設定を修正する対応を行った。届出者は委託業者と連携して、インシデント発生時の対応体制の見直しを実施した。
107	2021/3/11	届出者（一般団体）の管理するクラウド上のシステムにおいて、第三者からのアクセスにより、内部の情報が意図せず不正に閲覧されていたことがわかった。システムの運用業者によると、SaaS 基盤の設定変更の伝達に不備があり、一部に誤ったセキュリティ設定を行っていたために外部から情報が閲覧可能になっていたとのことであった。届出者は運用業者に対して、設定変更等を行う際には、意図や解釈を含めて事前に届出者へ連絡するようにすることを依頼した。
108	2021/3/16	届出者（地方自治体）の業務委託先のサーバ内のファイルが暗号化され、サーバに保管していた個人情報が流出した可能性も発覚した。委託先の担当者がサーバにアクセスしたところ、ファイル名が改ざんされていることを確認したため、ランサムウェアによる攻撃と判断し、届出者に連絡した。届出者は対策として、個人情報保護条例と情報セキュリティポリシーの職員への周知徹底したうえで、対応マニュアルの整備を行い、対応体制の強化を行った。
109	2021/4/6	届出者（企業）が管理するクラウド上のシステムに関して、内部の情報が閲覧できる状態になっているとの連絡を外部から受けた。調査したところ、SaaS 基盤使用時の設定に不備があり、意図せずに外部からの情報閲覧ができるようになっていたこと、および個人情報が不正に閲覧されていたことを確認した。設定を再確認して是正する処置を行った。

項番	届出日	概要
110	2021/5/6	届出者（企業）が管理するクラウド上のシステムにおいて、第三者からのアクセスにより、意図せず個人情報が閲覧されていた可能性が発覚した。委託業者により調査したところ、SaaS 基盤使用時の設定に不備があり、外部から情報が閲覧できるようになっていたこと、および個人情報が不正に閲覧されていたことを確認した。設定を是正して対応するとともに、再発防止のためシステム設定内容の検証強化やセキュリティ診断の実施、ログ保全方法の見直しを行った。
111	2021/5/17	届出者（企業）が管理するクラウド上のシステムにおいて、第三者からのアクセスにより、個人情報が不正に閲覧されていた可能性が発覚した。調査したところ、SaaS 基盤使用時の設定に不備があり、意図せず外部から情報が閲覧できるようになっていたこと、および個人情報が不正に閲覧されていたことを確認した。設定を是正して対応するとともに、クラウドサービス事業者や SaaS 基盤の提供事業者との連携を強化し、システム設定の変更や更新時の確認手順の追加等で再発防止を図った。
112	2021/5/24	届出者（企業）が利用している外部のサービス提供元から、不正アクセスの可能性が疑われるとの通知があった。調査したところ、当該外部サービスに脆弱性が存在し、それを悪用されて認証情報が窃取され、不正アクセスをされていたことが判明した。また不正アクセスにより、個人情報等が漏洩したことも判明した。本件の対応として、脆弱性のあった外部サービスの利用の一時停止、認証情報の無効化および漏洩した情報の影響の調査を行った。
113	2021/5/26	届出者（地方自治体）が利用しているクラウドサービスに関して、情報漏洩の恐れがあるとの連絡を外部から受けた。調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されてシステムにアクセスされ、個人情報が不正に閲覧されたことを確認した。SaaS 基盤の提供事業者との連携を強化して、情報の収集、管理、共有体制の見直しを行った。

項番	届出日	概要
114	2021/5/26	届出者（企業）が EC サービスを提供するために使用していた外部サービスの SaaS 基盤に不正アクセスがあり、EC サイトに不正なプログラムを設置されてカード情報が窃取された。外部サービスの提供元からの連絡で本件が発覚した。対応として、EC サイトにおけるカード支払いを無効にしていたが、その数日後に EC サイトを停止することとした。サービス提供元にて調査を行ったが原因は不明とのことだった。対策として、ID やパスワードの変更、UTM の導入、自社のパソコン・サーバへの EDR の導入、PCI DSS に準拠したセキュリティ対策を行い、さらに利用する外部サービスの変更も検討している。
115	2021/6/2	届出者（地方自治体）が管理するクラウド上のシステムにおいて、第三者からのアクセスにより、内部の情報が不正に閲覧されていたことがわかった。調査したところ、システム開発運用を委託してした事業者が実施した SaaS 基盤使用時の設定に不備があり、意図せず外部から情報が閲覧できるようになっていたことが判明した。対策として、委託業者が設定を是正する処置を行った。また届出者は委託業者や SaaS 基盤の提供事業者との連携を強め、セキュリティ管理の強化と定期的な確認を実施することとしている。
116	2021/6/2	届出者（企業）が提供している会員向けサービスが利用できなくなった。本サービスで使用している ASP サービスの運用元から、システム異常を検知したとの報告があり発覚した。調査したところ、ASP のシステムがランサムウェアに感染し、ファイルが暗号化されたため、サービスが動作しなくなっている状況であることがわかった。本件の対応として、代替の ASP サービスの利用の検討、および外部委託先管理の強化として事前に評価サービスを利用することとした。

項番	届出日	概要
117	2021/6/4	届出者（公共機関）が利用するクラウド型システムに関して、設定の再確認やアクセスログの調査を行ったところ、設定に不備があり、第三者がシステム内部の情報にアクセスしていたことが判明した。ただちに設定を是正して意図しないアクセスを遮断し、その後プログラムの修正も行って脆弱性を解消した。クラウドサービスに関する脆弱性情報や仕様変更があったときの情報収集の体制を整え、対応手順を確立することで再発防止を図った。
118	2021/6/10	届出者（地方自治体）が利用しているクラウドサービスに関して、監督官庁からセキュリティ設定の確認依頼があった。委託先の事業者と調査したところ、SaaS 基盤使用時の設定に不備があり、何者かに悪用されてシステムに不正にアクセスされ、個人情報が不正に閲覧されたことを確認した。委託業者が設定を修正して問題を解消する対応を行った。届出者は委託業者に対して、SaaS 基盤の提供事業者と連携してのサポート体制の強化を依頼した。
119	2021/6/10	届出者（企業）が利用している SaaS 基盤において、設定によっては意図せず外部から内部データを参照可能になることがわかり、システム保守を行う事業者とともに調査を行ったところ、当該の設定になっていて外部からデータが参照できる状態になっていたことが判明した。さらに個人情報を含む一部のデータが第三者によって不正に閲覧されていたことも判明した。

項番	届出日	概要
120	2021/6/21	届出者（一般団体）のメールアカウントに、メール不達を通知するエラーメールが大量に着信したことで、届出者になりすました不審なメールが多数送信されていることが発覚した。調査会社が全パソコンを調べたがウイルス感染やパスワード漏洩は確認されなかったため、利用していたメールサービスの提供元に調査を依頼したところ、同サービスの別の利用者のアカウントが不正アクセスされていたことが判明した。このメールサービスではログインしたメールアドレスと異なるアドレスでのメール送信が可能だったため、他の組織のアカウントに不正にログインした攻撃者が届出者になりすましてメールを送信していた。メールサービス提供元の処置により、なりすましメールの送信は止まった。届出者は本メールサービスの利用を止め、別のメールシステムの導入を検討している。
121	2021/6/24	届出者（地方自治体）の業務委託先のサーバがランサムウェアに感染し、サーバに保管していた情報が流出した可能性があるとの連絡を委託先業者から受けた。その後の調査により、届出者に関わるデータの漏洩は確認されなかった。届出者は対策として、業務委託の契約を見直し、不正アクセス等のインシデントの予防に向けた取り組みや発生時の対応についての取り決めの確認を行うとしている。

2-6. 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 2-6 に示す。

表 2-6 その他の届出事例の概要一覧

項番	届出日	概要
122	2021/2/16	届出者（企業）が運営するサービスの問い合わせフォームに対して、海外から不審なログインの試行があったことを監視システムが検知した。不正なログインに成功されると登録されている会員情報を窃取される恐れがあったが、被害は確認されていない。状況から、情報窃取が目的でなく、ID とパスワードの組み合わせが有効であるかを調べていた可能性が高いと推測している。対策として、問い合わせフォームでは未対応であった二段階認証の導入などセキュリティ施策を追加した。
123	2021/3/1	届出者（企業）が運営する EC サイトにアクセスしたユーザから不正なポップアップが表示されたという問い合わせがあり、この EC サイトのウェブページに埋め込んでいたマーケティングツールへのリンクが原因であると判明した。ツールのサービスが終了していたが、リンクを削除していなかったところ、攻撃者により当該サービスのドメイン名が購入され、悪意のあるファイルが EC サイトのページに読み込まれる状態となっていた。EC サイトからマーケティングツールのリンクを削除することで対応し、再発防止策としてサイトの定期パトロールの委託を検討している。
124	2021/4/5	届出者（企業）がクラウドサービス上で運用しているサーバにおいて、不正アクセスを試みていると思われる通信を複数回受信していることをセキュリティソフトが検知した。発信元は毎回異なる IP アドレスであり、そのほとんどが海外のものであった。セキュリティソフトが検知し遮断したため実質的な被害はなかった。

項番	届出日	概要
125	2021/5/26	届出者（企業）が提供する会員向けのサービスにおいて、トラフィック監視で異常な値を認めたため調査したところ、海外のIP アドレスとの間で、一般利用者が通常は使用しない通信が発生していたことがわかった。サイバー攻撃の可能性を考え、当該 IP アドレスとの通信を遮断した上で、調査会社とフォレンジック調査を行った結果、利用していたクラウドストレージから個人情報を含むデータが窃取されたことが判明した。詳細な原因は不明であり調査を継続中である。
126	2021/6/3	届出者（企業）が従業員向けに提供している VPN が利用できないとの報告があった。調査したところ、公開鍵暗号を使用した認証機能に対してブルートフォース攻撃が行われ、その影響を受け複数台のVPN サーバのうち 1 台が停止していたことが判明した。攻撃の対象となったのはスマートデバイスからの接続用に用意していた接続方式・経路であったため、当該機能を無効にすることで対応した。また、許可したデバイスのみ VPN サーバに通信を許可するようにするため、それに対応した機器を導入し、さらに認証方式は証明書を用いた方式のみに限定することで再発防止を図った。
127	2021/6/4	届出者（企業）の会員向けサービスのウェブサイトに不正アクセスがあり、会員の個人情報が不正に閲覧された可能性があることがわかった。当該サイトでは会員向けページにログインする際の認証方式として、アクセストークン付き URL を発行し、それを短縮URL としたものを事前に登録されたメールアドレスや SMS で送付するようにしていた。会員からログインしようとしていないのに短縮 URL が送付されてきたとの連絡があり、問題が発覚した。ログ調査等により、短縮 URL に対する総当たり攻撃が行われていたとの判断に至った（短縮 URL を使用したことで、アクセストークンの推測への耐性が損なわれた）。対応として有効期限内であったアクセストークンの無効化を行い、また今後、短縮 URL は利用しないように仕様を変更して再発防止を図った。

3. 事例：返信を装うメールにより Qakbot に感染した被害

3-1. 届出内容

（1）　発見経緯

本件の届出者（被害企業）を A 社と呼ぶ。本件について、A 社は次の 2 つの事象から被害を発見した。

・社外の方から、「過去に A 社とやりとりしていたメールを引用した、第三者からの不審なメールが届いたが、これは何か」と連絡があった。これは、Qakbot によって A 社から窃取されたメールが、社外の方への攻撃メールに転用されたものであった。
・A 社の従業員（B 氏と呼ぶ）が使用していた業務用仮想デスクトップ環境※1 から、不正な通信が行われていることを、ウェブゲートウェイ※2 のセキュリティ機能が検知し、調査を行った。これは、Qakbot ウイルスの C&C 通信であった。

※1 A 社では、従業員の業務用に仮想デスクトップ基盤を使用していた。従業員の手元には、仮想デスクトップへ接続し操作するためのクライアントマシンがあり、そのマシンには業務のデータは残らない。また、仮想デスクトップは、従業員がログインするたびに新たな環境が生成され、ログアウトすると破棄される仕組みとなっていた。
※2 ウェブゲートウェイとは、社内のマシンから外部ウェブサイトの閲覧などのためアクセスする際、通信経路として通過するように設置しておき、不正な通信などが発生していないかを検査するための装置・仕組み。

（2）　被害原因および被害内容

・過去 A 社が送信したメールの内容を流用し、そのメールへの返信のような形で B 氏へウイルスメールが着信した。ただし、メールの送信元は第三者のものであった。B 氏がメールに添付されていた ZIP ファイルに含まれていた Excel ファイルを開き、更にマクロを有効にする操作をしたことで、マクロによって外部のウェブサイトから Qakbot がダウンロードされ、B 氏が使用していた業務用仮想デスクトップ環境 1 台（1 インスタンス）に感染させられた。
・このとき、ウェブゲートウェイでは、Qakbot がダウンロードされる通信を検知できなかった。また、Qakbot 感染後の C&C 通信については検知していたが、不正な動作を止めるには至らなかった。（IPA 補足：仮想デスクトップ環境にも何らかのセキュリティ機能があったと思われるが、B 氏が開いた不正な Excel ファイルや Qakbot ウイルスの検知・検疫もされなかった状況と思われる）

・Qakbot により、B 氏の業務用仮想デスクトップ環境から、B 氏が過去に送受信したメールデータ（メールの内容やメールアドレス）が、攻撃者のもとへ窃取されたと思われる。
・B 氏と過去やり取りのあったメールアドレスに対し、実際のメール内容を流用して返信のような形で不審メール※3 が送信された。A 社へ連絡してきた当該メールの受信者によると、メールの送信元は第三者のメールアドレスとなっていた。

※3 明確になっていないが、この不審メールもまた Qakbot への感染を狙うウイルスメールであったと思われる。

（3） 被害対応
・被害原因および被害内容については、プロキシサーバの通信ログ、資産管理ソフトが収集する操作ログなどをあわせて調査した。データが流出した決定的なログは確認できていないが、状況から B 氏のメールデータが流出した前提でインシデント対応を進めた。
・ウイルス感染した業務用仮想デスクトップ環境を破棄した（B 氏がログアウトすると自動的に破棄される）。
・B 氏のユーザープロファイル（利用者に紐づいて記録されている、設定などの情報）を初期化した。
・従業員に対して、セキュリティ教育を実施する予定。

3-2. 着目点

（1） 正規の返信メールを装う攻撃メール

本事例において、ウイルス感染の直接の原因となったのは、攻撃メールを受信した従業員が、メールの添付ファイルを開いて Excel ファイルのマクロを有効化したことであった。Qakbot だけでなく、先期から多数の届出がある Emotet や IcedID など、メールの添付ファイルを開いたことを契機に感染するウイルスは多く観測されている。

感染を狙った攻撃メールと添付ファイルの例を図 3-1 に示す。また、本事例で実際に B 氏に着信した攻撃メールの添付ファイル（Qakbot をダウンロードするマクロが仕掛けられている Excel ファイル）の見た目を図 3-2 に示す。これらのメールを不審と感じずに、添付ファイルを開いて感染してしまうことが多いのは、過去に自分が送受信したメールの本文が引用されていたり、件名に日本語が使われていたりするなど、正規の返信メールと思い込ませるような手口が使われていることが一因である。

正規の返信メールを装うことで受信者（攻撃対象）の警戒心を薄れさせて、添付ファイルを開かせようとする手口は、昨年から継続して見られることから、今後も同様な手口に

よる攻撃が行われることが懸念される。件名や本文に身に覚えがある、返信メールのような形態であったとしても、攻撃（ウイルスメール）の可能性があるということを念頭に置き、特にファイルが添付されている場合は、送信者のメールアドレスや本文に追加された文面などから、正規のメールかを見極めてから添付ファイルを取り扱うようにしていただきたい。

なお、これらの攻撃メールの添付ファイルでは、マクロ機能が悪用されていた。添付ファイルを開いただけでは感染せず、Office 文書ファイルのマクロを有効にする操作を利用者に行わせることで、外部のサイトからウイルスがダウンロードされ感染させられる手口である。この手口は今後も継続して悪用される可能性があるが、添付ファイルを開いてしまった場合でも、基本的にはマクロを有効にしないように注意し、有効化が必要であれば、メールが信用できるものかを十分に確認したり、不審な点が見受けられた場合はメール以外の方法で送信者に確認する等の対応も重要である。

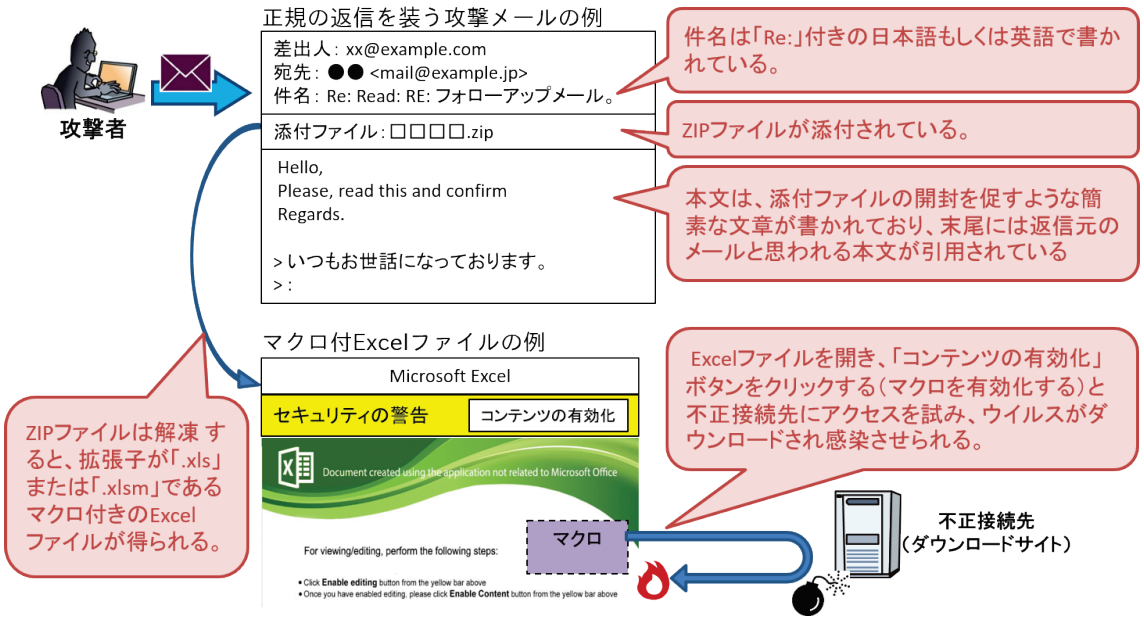

図 3-1 正規の返信メールを装う攻撃メールと添付ファイルの例

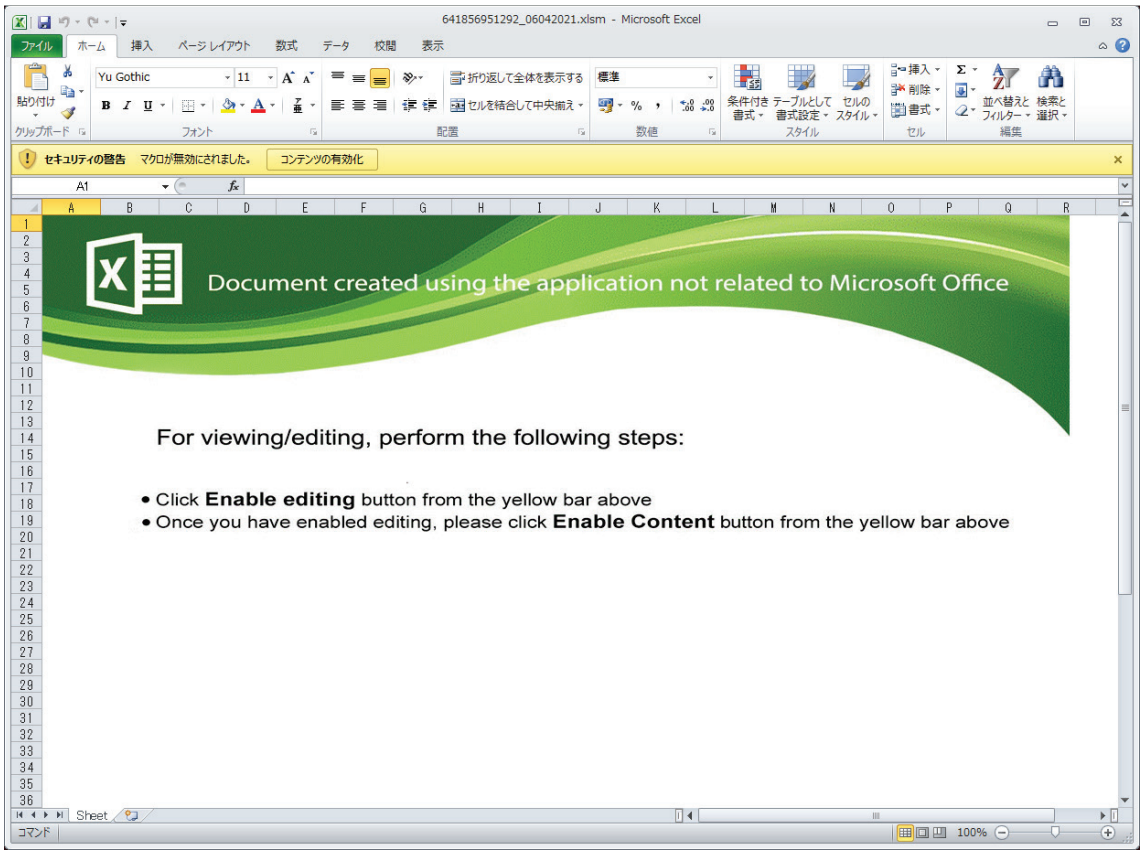

図 3-2 攻撃メールに添付されていた Excel ファイルの見た目

（2） Qakbot ウイルス

Qakbot に感染した事例の届出は、今期は本件の 1 件のみであった。しかし公開情報等によると、Qakbot への感染を狙った攻撃メールが多数観測されている。また、今期の届出においても、メールアカウントへの不正アクセスにより、Qakbot への感染を狙ったと思われる攻撃メール送信の踏み台にされた事例が 1 件あった。（項番 62）

Qakbot は、もともとはインターネットバンキング狙いのウイルスとされているが、追加機能や別のウイルスを順次ダウンロードするなどにより、様々な機能を持ち得るため、感染するとパソコンが遠隔操作される可能性もある。また一度感染してしまうと、Qakbot に感染したパソコンを起点として、組織内ネットワークへの侵入の拡大や、別のウイルス、例えばランサムウェア攻撃につながる可能性がある。いくつかの国内外で報じられている深刻なランサムウェア攻撃の被害は、Qakbot の感染から始まったとしているセキュリティベンダもある。Emotet と同様、更なるサイバー攻撃の足掛かりとなる「攻撃のインフラ」として感染の拡大が企図されていると考えられ、非常に注意が必要である。

対策としては、当然ながらまずは感染しないことが最重要である。Qakbot の感染を狙った攻撃メールが多数観測されている状況のため、前項で述べたとおり攻撃メールへの対策

が重要となる。

システム管理者が実施できる対策として、メールサーバやパソコンでのウイルス対策の徹底と、利用者に対する不審なメール・ファイルは開かない、Office 文書のマクロは安易に有効にしないといった啓発が必要である。手口が巧妙化しているため、セキュリティソフトで検知しなかったり、利用者の注意力では防げなかったりと、単一の防御策だけでは不十分である可能性がある。これらを多層の防御策として実施しつつ、可能であれば、マクロ機能の無効化を標準の設定とすることや、ウェブゲートウェイのセキュリティ装置により不審な外部サイトへの通信を遮断することも有効であると考える。

4. 事例：NAS の脆弱性を悪用されたランサムウェア感染

4-1. 届出内容

（1）　発見経緯

届出者（個人）が使用している NAS 上のファイルが暗号化され、データの復旧のために金銭の支払いを要求する脅迫文が書かれたファイルが、NAS 上に残されていることに気づいた。

（2）　被害内容

VPN によるインターネットからのアクセスを可能にしていた NAS が、Qlocker と呼ばれるランサムウェア（以下、Qlocker）の攻撃を受けた。これにより、NAS に保存していたほとんどのファイルが暗号化され、ファイル名の拡張子が改ざんされた。約 30 万個のファイルが使用不能になった。

（3）　被害原因

・NAS をインターネットからアクセス可能なように設定していた。
・その NAS のソフトウェアに不具合があり、NAS の権限を不正に取得できてしまう脆弱性が存在していた。

（4）　被害対応

・NAS のベンダーから提供された駆除ツールを使用して、ランサムウェアの活動停止と駆除を行った。
・ソフトウェアを、当該脆弱性の修正がされた最新版のものに更新し、使用していない NAS の機能は無効化した。
・NAS のベンダーが提供しているファイル復旧ツールを使用して、暗号化される前のファイルの復元を行い、一部のファイルの復元に成功した。

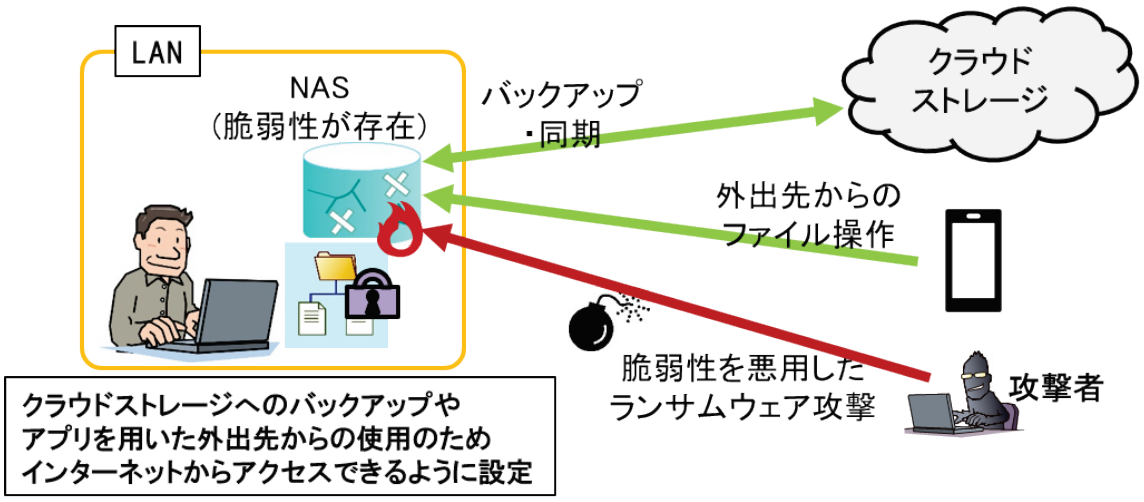

図 4-1 本事例の概要

4-2. 着目点

（1） NAS を攻撃するランサムウェア

本件は、NAS が攻撃の対象とされ、ランサムウェアの被害に遭った事例である。今期は、他にもインターネットに接続された NAS のファイルが暗号化された被害の届出が複数あり、その多くは、ファイル共有のためのポートが意図せず外部に開放されていたといった設定ミスに起因するものや、組織外の人とのファイル共有のためにパスワード認証のみで使用可能とし、かつパスワードが推測可能なものであったことが原因で不正アクセスを受けたと考えられるものであった。

本件は、NAS のソフトウェアの更新がされておらず、存在していた脆弱性を悪用されたことにより、NAS がランサムウェアに感染したと推測される状況であった。Qlocker は NAS のファームウェアに対して、悪意のあるコードを挿入することにより、NAS 上でファイル暗号化などの攻撃を行うランサムウェアである。

対策としては、アクセス制限など適切なセキュリティ設定を行うこと、および強固なパスワードを使用するといった基本的な施策を行うことに加えて、最新のソフトウェアへの更新などで脆弱性を解消することが重要である。特に、インターネットから直接アクセスが可能な機器に対しては、次項で述べるとおり、組織内のパソコンやサーバ以上のセキュリティ対策が必要と捉えて対策していく必要がある。

（2） インターネットに接続された機器の脆弱性対策

本件では、NAS をインターネットから直接アクセスできるように設定していた。従来は組織内でのファイル共有に使用するために、外部からアクセスできない組織内のネットワークに配置されることが多かった NAS だが、近年は外出先など組織外のネットワークから

NAS のファイルを参照したり、クラウドストレージサービスとの双方向バックアップを実施したりするなどの需要があるため、インターネットから接続可能な箇所に配置することも増えてきた。外部からのアクセスを可能にすることは、攻撃者にとってもアクセスが容易になることを意味するため、より一層のセキュリティ対策が必要になる。

NAS に限らず、VPN 装置やブロードバンドルータといったネットワーク機器等の、インターネットに直結されて利用されることが多い機器についても同様のことが言える。OS などのソフトウェアについては、定期的にセキュリティ更新プログラムが公開されることから、随時脆弱性情報を確認して、定期的なメンテナンスの時間を確保し、修正プログラムの適用を行う作業を実施している組織が多いと考える。一方、インターネットに直結される VPN 装置や NAS 等の機器は、攻撃者に狙われるリスクを考慮すると、パソコンやサーバ以上のセキュリティ対策が必要であると言え、受動的な脆弱性情報の確認、定期的な適用という運用方法では対策が間に合わない場合もあり得る。これらの機器へのセキュリティ対策の重要性を認識し、随時脆弱性情報を入手できる体制として、速やかな適用が可能なように手順やリソースなどを確立しておくことが重要である。

5. 事例：ASP への不正アクセスによるテナントサービスの停止

本章では、1 つの事案について、2 つの届出者から、それぞれの立場による届出を受けた事例を紹介する。項番 39 の届出者 C（企業）は、SaaS の形態でソフトウェアサービスを提供する事業者（ASP の事業者）であり、項番 116 の届出者 D（企業）は、その ASP サービスの利用者（テナント）である。

5-1. 届出内容 1 ：SaaS 基盤へのランサムウェア攻撃（項番 39）

（1） 発見経緯

届出者 C の監視システムが、アプリケーションの動作エラーを検知して障害発生を認知した。エラー発生の原因を調べたところ、アプリケーションが読み込むファイルが暗号化され、ファイル名も改ざんされていることを発見した。さらに複数のサーバでファイルが暗号化されていること、およびデータ復旧のために金銭を要求する脅迫文がサーバ上に残されていることを発見したため、ランサムウェア攻撃を受けたと判断した。

（2） 被害内容

・合計 7 台のサーバにおいて、複数のファイルが暗号化された。
・ファイルが暗号化されたサーバには、SaaS 基盤のサーバが含まれていた。当該サーバ上のアプリケーションが動作しなくなったために、届出者 C が提供する ASP サービスが停止した。
・パソコンやサーバの認証情報を窃取しようとするツールが稼働していた痕跡が見つかった。ただし、ログ等の調査結果から認証情報の窃取には失敗したと判断している。

（3） 被害原因

・外部からのリモートアクセスを可能にしていたサーバが存在していたため、何らかの方法で認証を突破されて、当該サーバへ不正アクセスされたものと推定している。
・ファイル授受のためにネットワーク共有フォルダを有効にしていたことにより、ランサムウェアによって共有フォルダのファイルが暗号化される被害が拡大した。

（4） 被害対応

・対象のサーバをシャットダウンして ASP サービスを停止し、サービス利用者（テナント）である届出者 D へ報告した。
・再発防止策として、従来から導入していたセキュリティソフトに追加して、ネットワーク侵入対策とエンドポイント監視を行うために、それぞれ専用のセキュリティシステムを導入した。

5-2. 届出内容２：ASP サービス利用者（テナント）のサービス停止（項番 116）

（1）　発見経緯

届出者 D が利用する ASP サービスの提供元（届出者 C）から、システム障害発生の連絡を受けて、届出者 D が顧客向けに提供しているオンラインサービスが停止したことを認知した。

（2）　被害内容

・自社の顧客向けにオンラインで提供しているサービスが停止した。
・ASP サービスのシステムで保管していた個人情報を含むデータが、第三者から不正に閲覧できる状態にあった。なお、調査の結果、データが外部に持ち出された形跡は確認されず、情報漏洩はなかったと判断した。

（3）　被害原因

ASP（届出者 C）が管理する SaaS 基盤のサーバがランサムウェア感染したことにより、ASP がシステムをシャットダウンしたため。

（4）　被害対応

・ASP（届出者 C）と情報共有や協議の場を設け、随時調査状況や対応策に関する報告を受けられるようにした。
・並行して、セキュリティ調査会社とともに自社内のシステムに関しての調査や確認を行った。
・早期のサービス再開のため、別の事業者のシステムを利用した新サイトに移行して、サービスを再開した。
・今後の対応として、サービス利用時にサプライチェーンのリスク評価を行う等により外部委託先管理の強化を図る。

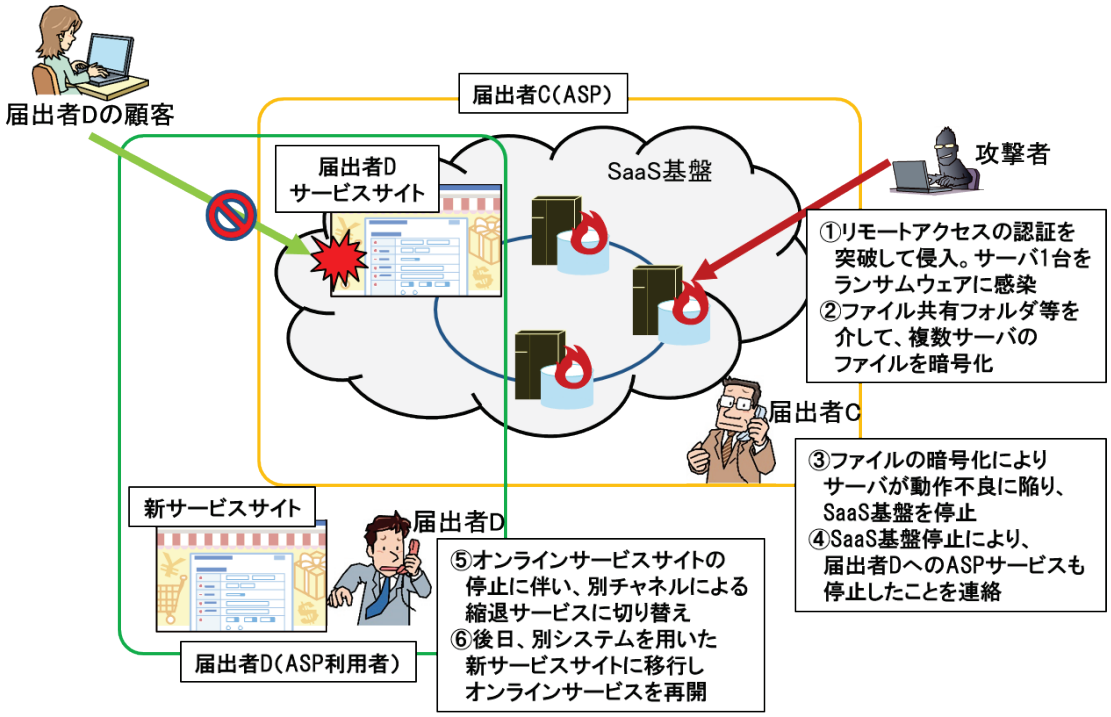

図 5-1 本事例の概要

5-3. 着目点

（1） サプライチェーンへの攻撃リスクを踏まえた事業者評価の重要性

今期は、委託業務の受託者や ASP の基盤側への不正アクセスにより、自組織のシステムやサービスが停止したり、自組織で管理している情報が漏洩したりした事案が多かった。本件は届出者 A の SaaS 基盤がランサムウェアに感染したことで、ASP サービスを利用して自社のオンラインサービスサイトを運用していた届出者 B のサービス停止と情報漏洩の懸念が発生した事例である。

ASP などの外部サービスを利用することは、システム導入のコストやリードタイムを小さくでき、修正プログラム適用などのメンテナンス作業も ASP が実施するため、運用コストも小さくできる。その反面、基盤部分にシステム障害が発生した場合の復旧作業も ASP が実施し、自力では実施できないため稼働率や目標復旧時間は ASP に依存する。高い稼働率が求められるシステムを運用したい場合は、事前に ASP サービスの SLA（Service Level Agreement）を確認して稼働率等を把握しておく必要がある。

不正アクセスなどのセキュリティインシデントが発生した場合も同様となる。セキュリティに関しては、例えば金融取引を行うシステムなど、高いセキュリティ要件が求められるシステムを運用する場合には、稼働率以外の要素も重要になるため、セキュリティ要件も含めた SLA を確認する必要がある。

本事例では、届出者 C のインシデント対応や再発防止策が、セキュリティ要件を満たし

ているかの審査を経て、システム再稼働・サービス再開までに要する時間が長かったため、届出者 D は自社が求めるリードタイムの条件を満たせないと判断し、別の事業者が提供するシステムに移行することを決めた。事業者の選定にあたっては、サプライチェーンのリスク評価サービスを導入して主にセキュリティポリシーや対策状況に関する審査を行ったとのことであった。外部委託先管理の一環として、外部委託サービスの導入基準を定め、基準に従ったリスク評価を必須にすることも有効であると考えられる。

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）