コンピュータウイルス・不正アクセスの届出事例

［2023 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

2023 年 9 月 29 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、被害の実態把握や同様の被害発生の防止を目的とし、個人の方や企業・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、同様の被害発生が想定される事例について、被害の未然防止や対策検討の参考情報になると判断した事例を紹介する。なお、届出された中には、被害の全貌把握や原因の特定ができていない事例も存在するため、当機構が把握できた範囲での説明となる場合や一部推測を含む場合がある[5]。

また、2022 年下半期（7 月～12 月。以下、先期）において、情報が不足している等の理由で、先期の掲載に至らない事例があった。その後、届出者から追加の情報提供を受けて、掲載に足る情報が揃った事例については、2023 年上半期（1 月～6 月。以下、今期）に届出された事例に加えて、一覧表に掲載した。詳細は 5 章を参照していただきたい。

本紙が、被害の未然防止や対策検討といったセキュリティ上の取り組みの促進につな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/todokede/crack-virus/about.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、又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等）により、利用者の意図に沿わずアクセスされた場合等、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

今期に受理したコンピュータウイルス（以下、ウイルス）届出及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、58 件の事例を取上げ、次の 5 種に分類した [6]。本分類は、被害の原因に主眼を置いているが、その原因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表していると判断したものに分類した。それぞれの分類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　9 件
- 身代金を要求するサイバー攻撃の被害　15 件
- 脆弱性や設定不備を悪用された不正アクセス　17 件
- ID とパスワードによる認証を突破された不正アクセス　9 件
- その他　8 件

全体を通して見ると、これまでと同様に、基本的なセキュリティ対策を実施することで、被害を未然に防ぐことが可能であったと考えられる事例が多数見られた。脆弱性や設定不備を悪用された不正アクセス（2-3 節で説明）や、ID とパスワードによる認証を突破された不正アクセス（2-4 節で説明）に分類した事例の多くはその典型であり、身代金を要求するサイバー攻撃を受けた事例（2-2 節で説明）についても、その多くは利用している VPN 装置に存在した脆弱性を悪用され、外部からの侵入を許してしまったことが原因であった。改めて、修正プログラムの適用や ID・パスワードの適切な管理などといった基本的な対策に漏れがないか、自組織のセキュリティ対策の実施状況を点検していただきたい。

各分類の届出件数を見ると、脆弱性や設定不備を悪用された不正アクセスが比較的多く、その分類の中では、CMS（Contents Management System）の脆弱性を悪用された事例が最も多かった。原因としては、脆弱性の管理に不備があった事例が散見されるため、脆弱性情報の収集・アップデートを確実に実施できる運用手順を確立しておくことを勧める。

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等に関する届出を複数受理している。昨年の届出全体の集計情報については、次ページのコンピュータウイルス・不正アクセスの届出状況を参考としていただきたい。

---

[6] 本章で紹介する届出事例の傾向は、今期中に IPA で受理した届出を対象としている。このため、今期に届出者より提出され、IPA が受理した届出に関しては傾向の対象に含めるが、1 章で述べた先期に届出された事例については傾向には含めていない。

- コンピュータウイルス・不正アクセスの届出状況［2022 年（1 月～12 月）］
  https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108005.pdf

2-1. コンピュータウイルスの検知・感染被害

本節では、コンピュータウイルスの検知・感染被害に分類した 9 件の届出について、Emotet とそれ以外のウイルスの 2 つに分けて紹介する。なお、届出された事例のうち、身代金を要求するサイバー攻撃の分類であると判断した事例については、2-2 節の分類とした。

（1） Emotet

Emotet は、メールアカウントやメールデータ等の情報窃取に加え、他のウイルスへの二次感染のために悪用されるウイルスである。このウイルスは、不正なメール（攻撃メール）に添付される不正なファイル等から感染の拡大が試みられている。

今期において、Emotet の検知・感染事例として受理した届出は 7 件あり、そのうち、3 月に発見されたものが 4 件、それ以外の 3 件は 2022 年以前のものであった。3 月に届出された事例については、2023 年 3 月中旬頃に Emotet が攻撃活動を再開した時期とほぼ重なっており、一部の届出者から提供された情報が、その攻撃内容と一致していたことを確認している。

参考までに、IPA が 2023 年 3 月 16 日に確認した、Emotet に感染させるための新たな手口について、次のページで紹介する。なお、対策としては、これまでと同様に「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」ことを利用者に徹底させるとともに、今回確認された新たな手口や、今後の動向についても注意を呼び掛けてほしい。

■ Microsoft OneNote 形式のファイルを悪用した攻撃（2023 年 3 月 17 日）

2023 年 3 月 16 日に、Microsoft OneNote 形式のファイル（拡張子「.one」）を悪用して Emotet へ感染させる新たな手口を確認した。この手口では、攻撃メールに添付された Microsoft OneNote 形式のファイルを開き、ファイル内に書かれた偽の指示に従って「View」ボタン（ボタンに模した画像）をダブルクリックすると、「View」ボタンの裏に隠されている悪意のあるファイルが実行され、Emotet に感染する恐れがある（図 2-1）。なお、攻撃メールの文面はこれまでと大きな違いは見られなかった。

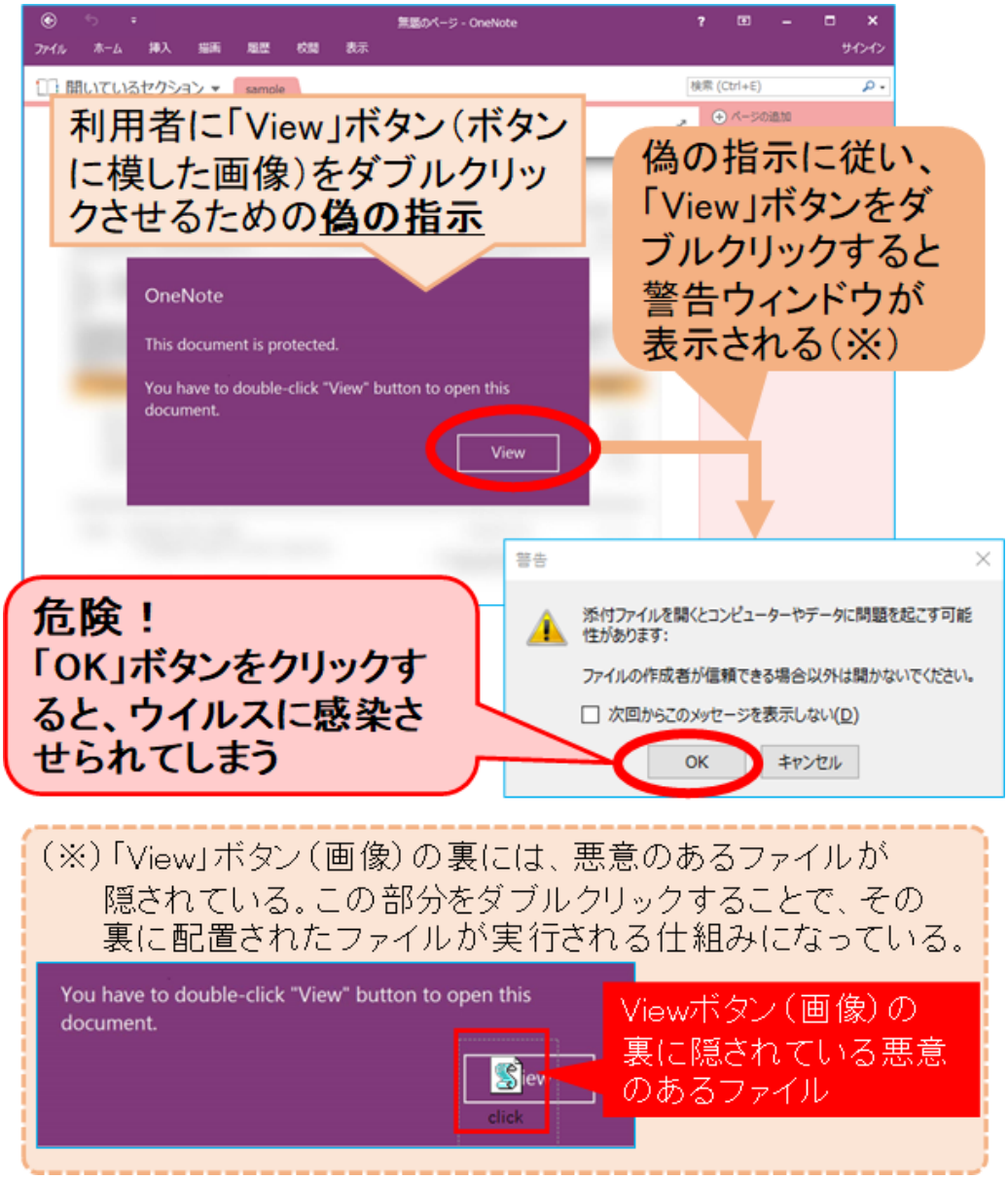

図 2-1 Microsoft OneNote 形式のファイルを開いてから Emotet 感染までの流れ

IPA では次のウェブページにおいて、Emotet に関する最新の情報を公開しており、攻撃の動向や攻撃手口の変化が見られた場合に随時更新している。対策の参考としていただきたい。

- Emotet（エモテット）関連情報
  https://www.ipa.go.jp/security/emotet/index.html

また、JPCERT/CC では、Emotet の感染有無を確認する Emocheck と呼ばれるツールや Emotet への対応 FAQ 等が紹介されている [7]。こちらも参考としていただきたい。

表 2-1 に、Emotet の検知・感染に関する今期の届出状況を掲載した。なお、各届出の詳細については省略する。

表 2-1 Emotet の検知・感染に関する届出状況

項番	届出月	届出者の主体と件数		概要
1	2023/1	企業	1 件	共通して、次に挙げる検知・感染の情報があった。 ● 組織内のパソコンにおいて、セキュリティソフトがウイルスを検知した。検知名等から Emotet と判断した。 ● 組織内に Emotet への感染を狙った攻撃メールが着信し、Emotet に感染したパソコンから、従業員・職員の名前を騙った不審なメールが発信された。 等
2	2023/2	地方自治体	1 件	
3	2023/2	一般団体	1 件	
4～5	2023/3	企業	2 件	
6～7	2023/4	企業	2 件	
－	2023/5	届出なし	0 件	
－	2023/6	届出なし	0 件	

[7] JPCERT/CC 「マルウェア Emotet の感染再拡大に関する注意喚起」
https://www.jpcert.or.jp/at/2022/at220006.html

（2）　Emotet 以外のウイルス

Emotet 以外のウイルスに関する届出については 2 件あった。このうちの 1 件は、ソフトウェア配布サイトからダウンロードしたソフトウェアに、第三者の通信を中継する機能を持ったツールがバンドルされていたという内容であった。利用者がそれを誤ってインストールしたことで、外部のサイトで発生した不正アクセス事案の踏み台となってしまった（事例 No.9）。詳細については 4 章で紹介する。

インターネットには、様々なウェブサイトが存在しており、その中には、悪意を持って詐欺やウイルス配布を行うものがある。また、悪意はなくとも、ウェブサイト管理者の意図に反して、第三者にウェブサイトを改ざんされることで、サイト閲覧者のパソコンにウイルスを感染させてしまうこともある。このため、日頃からセキュリティソフトで信頼できないと表示されるようなウェブサイト等には、できる限りアクセスしないよう心掛けるとともに、セキュリティソフトの導入、ウイルス定義ファイルを最新の状態に保つ等といった基本的な対策も実施していただきたい。

2-2. 身代金を要求するサイバー攻撃の被害

本節では、ランサムウェア攻撃など、ファイルやデータを暗号化・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攻撃を受けた 15 件の届出の概要を紹介する。

本節に分類される事例の中には、組織内ネットワークへと侵入されてしまった原因として、VPN 装置の脆弱性を悪用された事例のほか、設定不備を悪用された事例、総当たり攻撃などで認証を突破された事例も含めている。これらは、2-3 節、2-4 節の分類と重複しているが、身代金を要求するサイバー攻撃の被害に関連する事例として本節の分類とした。

今期においても、LockBit と呼ばれるランサムウェア（以下、LockBit）に関する被害が最も多く確認された。ランサムウェアの名称と同名の攻撃グループである LockBit は、データ復旧のために身代金を要求することに加えて、期限までに身代金を支払わなければ、窃取したデータをリークサイトで暴露すると脅迫する「二重の脅迫」を行う。実際に、このグループによる攻撃の被害に遭った届出の中には、窃取されたと考えられるデータがリークサイト上に公開されてしまった事例を確認している。また、LockBit は、攻撃手口のアップデートを繰り返し行っており、攻撃対象を Windows 搭載のパソコンやサーバだけでなく、Linux や macOS にも広げている。さらに、バグバウンティプログラム（バグや脆弱性を発見した者に対し、報奨金を支払う仕組み）を導入したとの情報もあるなど、積極的に活動している

ことが確認されている[8,9]。今後の動向にも注意を要する存在である。

本分類に該当する事例のうち、届出者が感染・侵入の原因（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した不正アクセスであった。当該脆弱性の対策方法に関しては 2-3 節で述べるが、感染・侵入の原因は脆弱性の悪用のみに限らず、総当たり攻撃などといった手口が使われる場合もあるため、次に示す組織内ネットワークの侵入対策が漏れなく実施できているか、点検することを勧める。

・攻撃対象領域（Attack Surface）の最小化
・アクセス制御と認証の強化
・脆弱性対策
・拠点間ネットワークの強化
・攻撃メール対策
・内部対策（ログ管理やネットワーク監視 等）

さらに、ランサムウェアによる暗号化・削除の被害を低減するためにバックアップ方法の見直しのほか、被害が発生した場合に備えて、事業継続計画（BCP）やインシデント体制の点検等も実施することも、併せて勧める。また、先期においては、過去に窃取された認証情報を用いて、ネットワーク内部に侵入された事例も散見された。認証情報の窃取が可能な脆弱性が公開された場合、VPN 装置の修正プログラムを適用するだけでなく、既に認証情報が窃取されていることを考慮し、必要に応じて、パスワード変更を行うことも検討していただきたい。

IPA では次のウェブサイトにおいて、「事業継続を脅かす新たなランサムウェア攻撃について」と題した注意喚起を行い、被害の事例や攻撃手口、推奨される対策について解説を行っている。こちらも対策の参考にしていただきたい。

- 【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/archive/security/security-alert/2020/ransom.html

---

[8] サイバーリーズン合同会社 「【脅威分析レポート】LockBit 3.0 ランサムウェア – ビルダーと DLL バイナリに関する調査」
https://www.cybereason.co.jp/blog/threat-analysis-report/10544/

[9] 株式会社カスペルスキー 「ランサムウェアグループ LockBit が攻撃範囲を拡大、macOS も標的に」
https://www.kaspersky.co.jp/about/press-releases/2023_vir23062023

2-3. 脆弱性や設定不備を悪用された不正アクセス

本節では、ソフトウェアやハードウェアにおけるセキュリティ上の不具合（脆弱性）、あるいは、セキュリティに関する設定不備が存在し、それらを攻撃者に悪用されて不正アクセス被害を受けた 17 件の届出の概要を紹介する。併せて、2-2 節で述べた、VPN 装置の脆弱性を悪用した攻撃及び対策方法についても本節で説明する。

VPN 装置の脆弱性を悪用された不正アクセス被害は、先期から引き続き、多数の届出があり、攻撃者から積極的に狙われている状況にある。一方で、被害に遭った組織においては、VPN 装置の脆弱性管理が適切に実施されておらず、既知の脆弱性を悪用された事例が多く確認されている。VPN 装置のように、組織において重要度の高い機器の脆弱性対応は、業務影響の検証等で負荷が大きく、容易に修正プログラムの適用を行うことは難しいものと考えられる。そのため、そうした機器の脆弱性の管理が確実に実施できるように、あらかじめ修正プログラムを適用するための計画の策定やリソースを確保した上で、ベンダからの脆弱性情報が漏れなく収集できているか、脆弱性を確認した際に影響の調査と対策の実施が速やかにできる運用となっているかなど、改めて、脆弱性の管理体制について見直しを実施していただきたい。もし、自組織での対応が難しい場合には、契約している保守業者との契約内容を見直し、自社が対応可能な範囲を明確化する。あるいは、外部の専門業者に保守を委託することを勧める。

VPN 装置の脆弱性を悪用された事例を除くと、今期においては、CMS の脆弱性を悪用された事例が比較的多くあった。原因としては、脆弱性の管理に不備があった事例が散見されるため、自組織の脆弱性管理が適切に実施できているかの点検をしていただきたい。また、事例の中には、別の CMS へと移行したはずが、ウェブサーバ上に移行前の CMS に関連するファイルが残存しており、そのファイルに存在した脆弱性を悪用されたことで、不正アクセスされた事例もあった。CMS を移行する場合は、移行前の不要なファイル等が残存した状態になっていないか、改めて確認を行うことを勧める。

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

本節では、ID やパスワードの運用・管理の問題により、不正アクセス被害を受けた事例に該当する 9 件の届出を紹介する。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に該当する事例は除いているため、認証を突破されたことが原因となる届出の総数はさらに多くなる。

今期において、ID・パスワードの認証突破による不正アクセスの攻撃対象はメールアカウントが最も多く、特に教育・研究機関で多数見られた。攻撃の手口としては、先期から引き続き、総当たり攻撃（ブルートフォース攻撃）により、認証を突破されたことが原因と推定している事例が多数見られた。

総当たり攻撃におけるシステム的な対応としては、まず、アクセス元の制限やログイン試

行回数の制限を行うことが挙げられる。例えば、ログインは特定の国や端末からのアクセスのみに制限する、ログイン試行を繰り返し行えないようロックアウト機能を設定するなどにより、総当たり攻撃による影響を低減させることが可能である。その上で、対象のメールシステムやウェブサイトにおいて、ワンタイムパスワード等の多要素認証のほか、CAPTCHA といった対策が利用可能である場合には、それらを活用することも検討していただきたい。

次に、アカウント管理の対応としては、利用者側が脆弱なパスワードを設定しないように、組織のパスワード管理ポリシーを見直すほか、従業員・職員向けにパスワード生成に関する注意喚起を実施することを勧める。また、過去の事例では、デフォルトで用意されているアカウントや脆弱なパスワードを持つ古いアカウントが有効の状態で放置されていた事例もあるため、そうしたアカウントが残存していないか、確認することも勧める。

2-5. その他

本節では、ここまでの分類に該当しなかった事例として、ウイルス感染や不正アクセスによる被害には該当しない事例のほか、調査を行っても被害原因が判明しなかった事例などを分類している。

今期においては、偽警告・サポート詐欺に関する事例や、クレジットマスター攻撃と呼ばれる事例が複数確認されたため、これらについて紹介する。

偽警告・サポート詐欺は、偽のセキュリティ警告をブラウザ等の画面上に表示し、その警告内に記載してある電話番号へ電話をかけるように誘導する。その後、警告で表示された問題を解決する代わりに金銭や有償のサポート契約を要求するというものである。届出された事例の中には、金銭的な被害には至らなかったものの、表示された電話番号に電話し、指示に従い、不正なツールのインストールをしてしまった事例もあった。こうした攻撃の対策としては、組織の従業員や職員にセキュリティ教育を行い、攻撃の手口や対処の方法について、周知徹底しておくことが重要である。

IPA の情報セキュリティ安心相談窓口では、次のウェブサイトに専用のページを用意している。こちらを社内の注意喚起に利用する等して、対策に役立てていただきたい。

- 偽のセキュリティ警告に表示された番号に電話をかけないで
  https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211116.html

次に、クレジットマスター攻撃とは、クレジットカード番号の規則性を悪用し、他人のカード番号を割り出す不正な行為を指す言葉である。クレジットカード番号は、クレジットカード会社を識別するための番号と個人用の番号といった、ある程度固定化された文字列

で構成されており、有効期限やセキュリティコードについても、パターンが限られている。クレジットマスター攻撃では、これらを組み合わせたツール等による総当たりを行うことで、利用可能なクレジットカード情報を特定するというものである [10]。今期に届出された事例では、届出者が運営する EC サイトがクレジットマスター攻撃の被害に遭い、サーバが高負荷の状態にされたため、EC サイトの運営に支障が生じたほか、カードが利用可能か確認する際に発生する費用が増大したことで、金銭的な被害も発生するといった事例もあった。こうした事例の対策としては、EC サイトにおけるアクセス制御や試行回数の制限に加え、3D セキュア等の本人認証機能の導入などを行うことが重要である。

届出される事例の中には、届出者の見解として原因不明と判断されたものであっても、ソフトウェアの脆弱性の悪用や、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ある。直接的な原因は異なっていたとしても、前節までに述べてきた対策を行うことは、セキュリティの向上にもつながり、ウイルス感染や不正アクセスによる被害のリスク軽減に有効であると考えられる。このため、2-3 節や 2-4 節の内容を参考に対策を検討していただきたい。

[10] 三井住友カード株式会社「多くの人が被害に遭っているクレジットマスターって知ってる？手口や被害を防ぐ方法を徹底解説！」
https://www.smbc-card.com/mem/hitotoki/solution/credit_master.jsp

3. 事例：ソフトウェア配布サイトから取得したツールのプロキシ機能に起因する不正アクセス被害

3-1. 届出内容

（1）　発見経緯

届出者（企業）が使用するグローバル IP アドレスが、外部のインターネットバンキングにおいて発生した不正アクセス事案のアクセス元になっていると、外部機関より連絡があった。調査の結果、組織内の従業員が使用していたパソコン（以下、被害パソコン）に、第三者の通信を中継する機能を持ったツール（以下、ツール）がインストールされており、攻撃者がその機能を経由して、インターネットバンキングに不正アクセスしていたことが確認された。

（2）　攻撃の流れ

本事例で確認された攻撃の流れを図 4-1 に示す。

なお、当該ツールの主たる機能は、デスクトップ画面の表示の一部を変更するというものであり、それに付随する形で、第三者の通信を中継するプロキシの機能も有していたことが判明している。

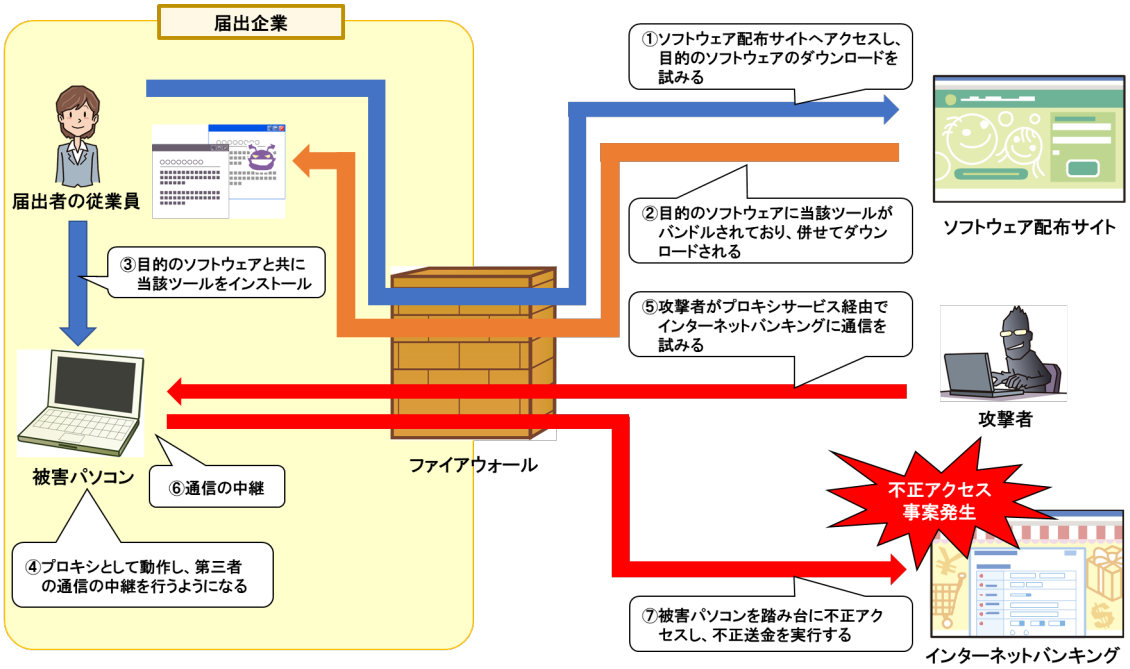

図 4-1 攻撃の流れ（※届出いただいた情報を基に IPA で作成）

① 届出者の従業員がソフトウェア配布サイトにアクセスし、目的のソフトウェアのダウンロードを行う。
② 目的のソフトウェアに当該ツールがバンドルされており、併せてダウンロードされる。
③ 従業員が目的のソフトウェアと共に当該ツールを被害パソコンにインストールする。
④ 当該ツールがプロキシとして動作し、第三者からの通信の中継が可能となる。
⑤ 攻撃者がプロキシサービスを経由し、インターネットバンキングに通信を試みる。
⑥ 当該ツールが攻撃者の通信を中継する（結果として、アクセス元が届出者のグローバル IP アドレスになる）。
⑦ 被害パソコンを踏み台に、攻撃者が外部のインターネットバンキングへ不正アクセスし、不正送金を実行する。

（3） 被害原因

本件の被害原因として、次に示す 2 つのセキュリティ上の問題を確認している。

a) バンドルされていた当該ツールのインストール

当該ツールが被害パソコン上に存在していた原因について、届出者は、ソフトウェア配布サイトからダウンロードした本来の目的であるソフトウェアに当該ツールがバンドルされており、従業員が誤ってインストールしてしまったと推測している。なお、当該ツールは、潜在的に悪意のあるプログラム（PUP[11]）として検知されていたが検疫等はされなかった。理由については情報提供外であるため不明である。

b) 不正アクセスの踏み台

当該ツールが持っていたプロキシの機能は、一般にレジデンシャルプロキシと呼ばれるサービスの一部として動作するものであった。そのサービスに組み込まれることで、第三者の通信を中継するようになり、本事例においては、攻撃者による不正アクセスの踏み台として悪用されてしまった。

レジデンシャルプロキシとは、ISP が一般家庭向けに配布している IP アドレスをプロキシの中継点として利用するサービスを指す。例えば、当該サービスを利用し、特定の地域の IP アドレスを中継点として設定することで、任意の場所からその地域向けに提供されているサービスなどを利用できる。また、複数の地点を経由した通信を行うことも可能である。一方で、一般的に使われる IP アドレスからアクセスが来

[11] Potentially Unwanted Program の略。該当するものとして、スパイウェア、アドウェア等がある。また、セキュリティベンダにより PUP、あるいは PUA（Probably Unwanted Application）とも呼ばれている。

ているように見えるため、検出や遮断がされにくいこと、アクセス先に対して本来のアクセス元を秘匿できることから、本事例のような攻撃に悪用されることもある[12]。

（4） 被害内容

本事例では、届出者の被害パソコンが、外部で発生した不正アクセス事案の踏み台として悪用される被害に遭った。その後、届出者は被害パソコンについて、フォレンジック調査を外部業者に依頼した結果、踏み台以外の不正操作や情報の改ざん、漏えい等の被害は確認されなかった。

（5） 被害対応

- 技術的対応
  - 発見した当該ツールを削除
  - 同様の事象が発生している機器の有無を調査
  - 当該ツールによるレジデンシャルプロキシに関する通信を遮断
  - 当該ツールをバンドルして配布していた可能性があるウェブサイトへのアクセスを遮断
  - 外部業者によるフォレンジック調査
- 組織外への報告等
  - 外部機関への報告・相談

（6） 再発防止策

- 技術的対策
  - TLS（SSL）インスペクションの適用による通信の可視化

3-2. 着目点

（1） インターネットから取得したソフトウェアを利用する上での注意

本事例は、ソフトウェア配布サイトから取得した、本来の目的であるソフトウェアに当該ツールがバンドルされており、届出者の従業員が誤ってインストールしたことで、被害につながったものである。

利用者においては、メーカーや開発元の公式サイト等といった信頼できるウェブサイトからソフトウェアを入手するようにしていただきたい。また、ソフトウェアの紹介や配布を

[12] 明治大学「Residential IP Proxy サービスに悪用される住宅用ホストの調査」
https://www.kikn.fms.meiji.ac.jp/paper/2020/master/hanzawa/CSS_2019_hanzawa.pdf

行うウェブサイトが無害であるとは限らないため、そのサイトに書かれている情報や説明等を十分に確認した上で入手することが望ましい。さらに、ソフトウェアをインストールする際にも注意が必要である。本事例で確認した当該ツールの場合、インストールする際に、通信を中継する機能がある旨の同意画面が表示されたものと見られる（図 3-2）。

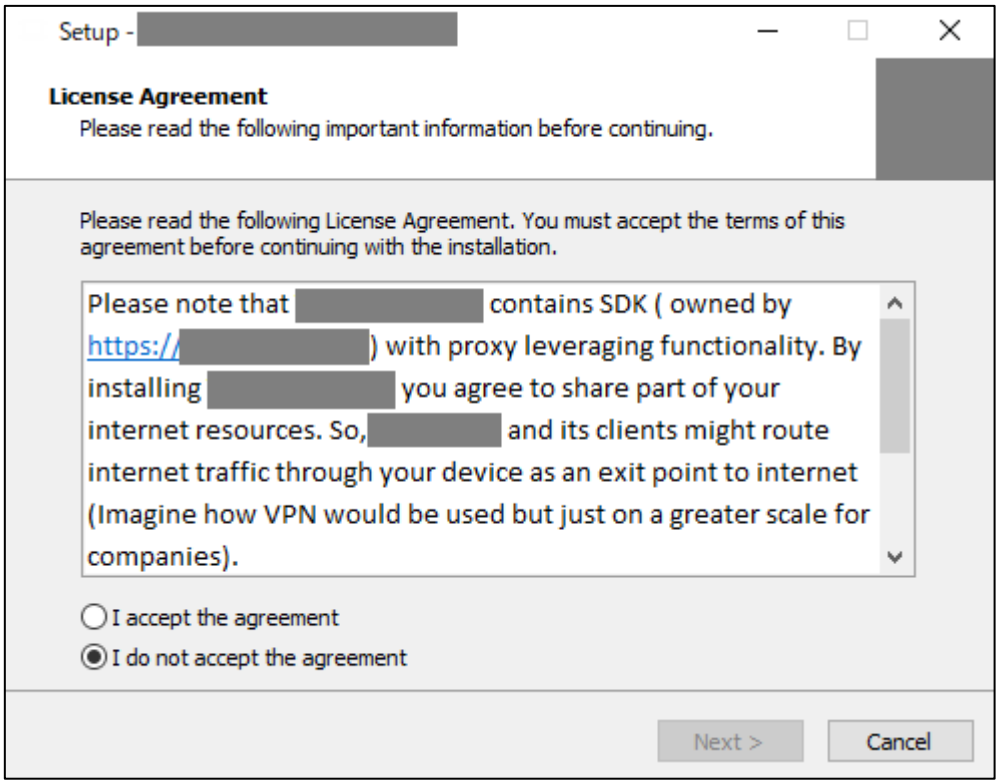

図 4-2 インストールする際の同意画面(通信を中継する旨が提示されている)

本事例においては、当該ツールが目的のソフトウェアにバンドルされていたため、被害パソコンの利用者は、目的のソフトウェアをインストールしているつもりで内容をよく確認せずに同意した可能性がある。このような状況を防ぐため、インターネットから入手したソフトウェアをインストールする場合には、ソフトウェア利用許諾等の文章に必要としない動作が含まれていないか、十分に確認していただきたい。ただし、提示される文章が長く専門的である等、利用者側で問題がないと判断することは難しい場合もあるため、利用の前に所属する組織のシステム管理者等に相談しておくことを勧める。

システム管理者においては、事前に URL フィルタリング等でソフトウェア配布サイトに向けたアクセスを遮断しておき、従業員や職員が不用意にソフトウェアをダウンロードしないよう制限しておくことが望ましい。そうしたサイトに向けたアクセスを許可する場合には、組織内で発生し得るリスクを十分に検討した上で判断していただきたい。また、組織内のパソコンやサーバ等にセキュリティソフトや EDR 等を導入しておき、不審な挙動や通

信が発生した際にいち早く検知・対処ができるようにしておくことも重要である。

（2）　レジデンシャルプロキシの悪用防止

本事例では、届出者が使用する被害パソコンが、外部で発生した不正アクセス事案の踏み台として悪用される被害に遭った。

本章の攻撃の流れや被害原因で紹介しているとおり、使用している機器がレジデンシャルプロキシの一部に加えられると、第三者の通信の中継が可能になる。レジデンシャルプロキシを利用する人物がそのサービスの目的に沿った利用をする場合には、本事例のような悪用に加担する恐れは低いと考えられるが、本来の目的とは異なる利用をされた場合は、使用者の意図しないところで不正な行為に加担してしまうことがある。

このため、次のような対応を実施することを勧める。

- 当該ツールのような通信の中継機能を持つソフトウェアを利用している場合には、利用の要否を見直す。
- 本事例のように意図せずインストールしている可能性も考慮し、身に覚えのないソフトウェアの有無を確認する。インストールしていた場合は削除を行う。
- セキュリティソフトや EDR 等を導入して、当該ツールのように PUP 等と判定されるソフトウェアのダウンロードや挙動を検知・検疫できる環境にする。
- セキュリティベンダ等で紹介されている IoC（Indicators of Compromise）[13]を参照し、組織内のインストール有無を調査する。該当するものがあれば削除を行う。

[13] トレンドマイクロ株式会社「通信帯域を乗っ取るプロキシウェア型アプリが引き起こすリスク」
https://www.trendmicro.com/ja_jp/research/23/d/hijacking-your-bandwidth-how-proxyware-apps-open-you-up-to-risk.html

4. 届出事例の概要

本章では、今期に取上げた 58 件の事例に加え、掲載に足る情報が揃ったと判断した先期分の 32 件の事例について、2 章の分類を基に各事例の届出日と概要を紹介する。さらに、各分類の中で件数が比較的多い事例（身代金を要求するサイバー攻撃の被害における LockBit ランサムウェアの被害事例 等）については、表を分割して示している。

4-1. コンピュータウイルスの検知・感染被害

表 5-1 は、2-1. コンピュータウイルスの検知・感染被害に該当する事例のうち、Emotet 以外のウイルス検知・感染に関する届出の一覧を示す。表の項番は 2 章の表 2-1 からの連番である。

表 5-1 Emotet 以外のウイルス被害に関する届出の概要一覧

項番	届出日	概要
8	2022/12/27	届出者（企業）が利用するパソコンの画面表示に異常が発生し、インターネット接続もできなくなる事象を確認した。対応として、セキュリティソフトでウイルススキャンを行ったところ、ウイルスと見られるデータを検知したため削除を行った。また、感染拡大の可能性を考慮し、当該パソコンを廃棄した。なお、ウイルスの感染経路は不明である。再発防止策として、UTM（Unified Threat Management）機器の更新を行った。
9	2023/1/20	届出者（企業）が使用するグローバル IP アドレスが、外部組織で発生した不正アクセス事案のアクセス元になっていると外部機関より連絡があった。調査したところ、自組織内のパソコンに通信の不正中継を行うソフトウェアがインストールされており、そのソフトウェアのプロキシ機能を攻撃者に悪用されたことで、プロキシサービスを経由した不正アクセスが行われていたことが判明した。原因については、届出者の従業員が業務で使用するためにダウンロードした、ソフウェアに当該ソフトウェアがバンドルされており、プロキシ機能を持つことに気づかず、インストールしてしまったものと推測している。対応として、当該ソフトウェアの削除やプロキシサービスに関わる通信の遮断等を行った。再発防止策として、ファイアウォールに SSL インスペクション機能を導入するなど、監視を強化することを検討している。

項番	届出日	概要
10	2023/3/3	届出者（企業）が導入している UTM のウェブフィルター機能において、通常では見られない大量のセッションが検知された。さらに、UTM が高負荷となったことにより、インターネットへの接続障害が発生した。原因の特定には至っていないが、2 件のウイルスの検知と UTM での不正な通信を遮断したとするログが確認されたことから、組織内のパソコンがウイルスに感染したことによるものと推測している。対応として、UTM のログを基にウイルスを駆除する対応を行った上で、外部機関にも調査を依頼した。再発防止策として、EDR の導入を予定している。

4-2. 身代金を要求するサイバー攻撃の被害

表 5-2 は、2-2. 身代金を要求するサイバー攻撃の被害に該当する事例のうち、LockBit ランサムウェアに関する届出の一覧を示す。

表 5-2 Lockit ランサムウェアに関する届出の概要一覧

項番	届出日	概要
11	2022/10/25	届出者（企業）の従業員から、ファイルサーバにアクセスできないとの報告があった。確認したところ、当該サーバ内のファイルが暗号化され、脅迫文が残されていることを発見した。調査の結果、LockBit3.0 によるランサムウェア被害であることを確認した。この被害により、サーバ内に保管していた数万件の個人情報等が流出した可能性のあることが判明した。また、サーバ内のデータが暗号化された状態で、バックアップ処理が行われたため、遠隔地に設置しているバックアップサーバにも影響が及んだ。侵入の原因は不明だが、VPN 装置（FortiGate）の脆弱性（CVE-2018-13379）を悪用されたものと推測している。対応として、侵害の原因となった VPN 装置のファームウェアアップデートや設定の見直しを行った。また、感染したサーバについては初期化したのち、暗号化の影響を受けなかったバックアップサーバのデータから復旧させた。再発防止策として、EDR の導入などを行った。

項番	届出日	概要
12	2022/12/17	届出者（企業）が利用するファイルサーバ等に接続できなくなったので、保守業者に連絡をしたところ、LockBit により当該サーバ内のファイルが暗号化されていたことが判明した。さらに、他のサーバやパソコンにおいても同様の被害が確認され、プリンタからは複数回に分けて脅迫メールが印刷された。外部機関の調査により、VPN 装置（FortiGate）に存在していた脆弱性を悪用されたことで、攻撃者に認証情報を窃取され、社内ネットワークに侵入されたものと推定している。対応として、暗号化の被害に遭ったサーバや VPN 装置を停止させた。再発防止策として、全ユーザーのパスワードをより強固なものに変更し、VPN 接続時における二要素認証の徹底や、ネットワーク構成の見直しなどに加え、定期的な脆弱性情報の収集や従業員向けの情報セキュリティ研修の実施等も検討するとしている。
13	2022/12/19	届出者（企業）が利用するファイルサーバにおいて、サーバ内に保存していたファイルの拡張子が書き換えられていることを確認した。拡張子の内容から、LockBit2.0 によるランサムウェア攻撃を受けたものと推定される。調査の結果、バックアップ用の NAS においても同様の被害が発生していることが判明した。侵入の原因は、VPN 装置（FortiGate）の脆弱性を悪用した攻撃による、認証情報の窃取であった。なお、認証情報が窃取された時期は不明であった。暗号化の被害に遭ったサーバと NAS が侵害された原因は、管理者アカウントに脆弱なパスワードを使用していたために、総当たり攻撃などの方法によって認証を突破されたものと推測している。対応として、ファイルサーバや VPN 装置を停止し、外部から社内ネットワークへの通信を遮断する等の措置を行った。なお、バックアップ用のデータも暗号化の被害を受けたため、復旧には至っていない。再発防止策として、SIEM（Security Information and Event Management）の導入や SOC サービスの契約によるセキュリティ体制の強化、セキュリティ診断の実施、全従業員に対するセキュリティ教育等を行った。

項番	届出日	概要
14	2022/12/27	届出者（企業）の従業員より、デスクトップ上のファイルが暗号化されているとの連絡があった。調査したところ、パソコンやファイルサーバ等、数百台が暗号化の被害を受けていることが判明した。また、英語で書かれた脅迫文が大量に印刷されるという事象も確認した。脅迫文や拡張子の特徴から、LockBit2.0によるランサムウェア攻撃を受けたものと推定される。侵入の原因は、VPN 装置（Cisco ASA）の脆弱性の悪用により、窃取された認証情報を使用して、社内ネットワークに侵入されたものと推測している。複数の機器に被害が拡大した原因は、攻撃者が何らかの方法で Active Directory サーバの管理者情報を乗っ取り、ドメイン管理下のパソコンやサーバに対して侵害を広げたものと推測している。対応として、VPN 装置や侵害が確認された各機器を社内ネットワークから切り離したのち、バックアップやスナップショットを利用して復旧させた。再発防止策として、社内運用体制の見直し、パスワードポリシーや監視機能の強化、EDR の導入等を実施するとしている。
15	2022/12/29	届出者（企業）の従業員からファイルが開けないとの連絡があった。確認したところ、仮想サーバを含む十数台の機器に保存されたファイルが暗号化されていることが確認された。さらに、バックアップ用の NAS のデータが全て削除されていることも判明した。暗号化されたファイルの拡張子や脅迫文の特徴から、LockBit2.0 によるランサムウェア攻撃を受けたものと推定している。侵入の原因や侵害が拡大した原因の特定には至っていないが、何らかの脆弱性の悪用により、社内ネットワークに侵入されたのち、侵害した Active Directory サーバの情報を基にランサムウェアの拡散をされたものと推測している。対応として、侵害を受けた機器をネットワークから切り離した上で、管理者 ID やパスワードの変更、再構築等を行った。バックアップ用の NAS は、外部業者に復旧を依頼した。再発防止策として、EDR の導入やバックアップ方法の見直し等を実施した。

項番	届出日	概要
16	2023/1/19	届出者（企業）の業務システムが停止したため、サーバの状態を確認したところ、サーバ内の複数ファイルの拡張子が改ざんされ、画面に脅迫文が表示されていることを発見した。調査の結果、複数台のサーバ及びパソコン、バックアップ用の NAS が LockBit3.0 に感染していることが判明した。侵入の原因は、VPN 装置（Cisco VPN)において、多要素認証やアカウントロック機能等の不正ログイン対策が不足していたこと、パスワードの設定が英数字や数字のみといった脆弱な状態で運用していたことから、総当たり攻撃などの方法で認証を突破されたと推測している。また、被害が拡大した原因は、攻撃者が Microsoft 社製のリモートプログラム実行ツールである PSexec の悪用や総当たり攻撃を行うことで、複数のサーバ及びパソコンなどに被害が拡大したと推測している。対応として、被害に遭ったサーバをネットワークから遮断し、ウイルススキャンやパスワード変更、データの復旧作業などを行った上で、外部機関にもフォレンジック調査の依頼をした。再発防止策として、パスワードポリシーやバックアップ方法の見直し、VPN 装置への多要素認証の導入等を検討するとしている。
17	2023/1/27	届出者（企業）が利用しているサーバに不具合が発生していると連絡がサーバの管理業者からあった。調査したところ、複数のサーバのデスクトップ画面が身代金を要求する内容のメッセージに変更され、サーバ内のファイルも暗号化されていることが判明した。被害状況から、LockBit によるランサムウェア攻撃を受けたものと推定される。侵入の原因は、VPN 装置（FortiGate）に存在した脆弱性を攻撃者に悪用され、認証情報を窃取されたことで、社内ネットワークに侵入したものと推測している。ランサムウェアが組織内で拡散した原因は不明である。対応として、被害を受けたサーバをネットワークから切り離すなどの対応を行った上で、専門業者に調査を依頼した。再発防止策として、被害の原因となった VPN 装置の利用停止や EDR の導入などを実施するとしている。

項番	届出日	概要
18	2023/2/10	届出者（企業）のサーバ数十台が LockBit 3.0 に感染していることが判明した。原因は脆弱性の悪用としているが詳細は不明である。対応として、被害に遭ったサーバを初期化し、再構築を行った。再発防止策として、EDR の導入を実施した。
19	2023/3/14	届出者（公共機関）が運用している業務システムが起動できない状態であることを発見した。調査したところ、複数台のサーバとそのバックアップ用の機器に保管されていたファイルなどが暗号化され、デスクトップ画面には金銭を要求する脅迫文が表示されていたことが判明した。被害状況から、LockBit3.0 の攻撃を受けたものと推定される。侵入及び侵害拡大の原因は、利用していた VPN 装置（FortiGate）を脆弱な状態で放置していたため、攻撃者が VPN 装置の脆弱性悪用、あるいは総当たり攻撃などの方法により、外部から侵入したのち、認証情報取得ツールを用いて、組織内ネットワークのサーバなどにランサムウェア感染を拡散させたものと推測している。対応として、VPN 装置を停止させ、クラウドサービス上にサーバの再構築を行い、バックアップデータからの復旧を行った。再発防止策として、管理者パスワードの変更などといったシステム的な対策のほか、外部業者との契約内容を見直し、責任分界点の明確化等を実施した。
20	2023/3/17	届出者（企業）の業務システムが動作しなくなったため、サーバを確認したところ、画面上に LockBit2.0 と表示されていることが判明した。被害状況から、LockBit2.0 によるランサムウェアの攻撃を受けたものと推定している。侵入の原因は、VPN 装置（FortiGate）の脆弱性（CVE-2023-25610）を悪用され、当該システムに不正侵入されたものと推測している。対応として、ネットワークの遮断を行った上で、外部の専門業者に調査を依頼した。また、感染したサーバについては、初期化後にバックアップデータから復旧させた。再発防止策として、VPN 接続時における認証機能の強化、EDR の導入などを実施した。

表 5-3 は、2-2. 身代金を要求するサイバー攻撃の被害に該当する事例のうち、LockBit ランサムウェアを除いた、その他の身代金ランサムウェアに関する届出の一覧を示す。

表 5-3 その他の身代金ランサムウェアに関する届出の概要一覧

項番	届出日	概要
21	2022/9/8	届出者（企業）の従業員が社内システムにアクセスできない状態にあることを発見した。確認したところ、複数のサーバ内のファイルが暗号化されていることが判明した。設置された脅迫文等の内容から、MedusaLocker ランサムウェア、あるいはその亜種に感染したものと推測している。外部の専門機関に調査を依頼した結果、過去に VPN 装置の脆弱性の悪用により、窃取された認証情報を用いて、不正アクセスを行ったと見られる痕跡が確認された。なお、データ流出の可能性を示す痕跡は確認されなかった。対応として、侵害されたサーバをネットワークから切り離し、全ての機器に対してウイルススキャンを実施した。再発防止策として、VPN 装置の多要素認証の導入、バックアップ環境の整備、従業員に対するセキュリティ教育等を実施するとしている。
22	2022/10/20	届出者（企業）の従業員から、社内ネットワークにアクセスできないとの問い合わせが複数寄せられた。調査した結果、複数のサーバが暗号化の被害に遭っていることが確認された。侵入の原因は不明だが、テレワークで貸与しているパソコンが何らかのウイルスに感染し、社内ネットワークへの侵入の踏み台にされたものと推測している。対応として、被害に遭った機器をネットワークから切り離し、全ての機器でウイルススキャンの実施及びサーバの管理者パスワードの変更を行った。再発防止策として、ネットワーク構成の強化及び侵入検知ツールの導入、バックアップ方法の見直し等を検討するとしている。

項番	届出日	概要
23	2022/11/2	届出者（企業）が利用するサーバ上のファイルが暗号化され、画面に脅迫文が表示されていることを発見した。暗号化されたファイルの拡張子や脅迫文から TargetCompany の亜種と推定している。調査の結果、海外拠点を含む数十台のサーバや NAS が暗号化の被害を受けたことが判明した。侵入の原因は不明であるが、被害が拡大した原因について、届出者の社内ネットワーク上でリモートデスクトップでのアクセスが許可されていたこと、また、脆弱なパスワードを利用している機器が存在していたことから、総当たり攻撃等の方法によって、認証を突破されたものと推測している。対応として、侵害された機器をネットワークから切り離したのち、バックアップデータがあるものは復元し、それ以外のものは新規に再構築した。再発防止策として、セキュリティソフトと EDR 導入の徹底、社内規程の運用の厳格化等を行った。さらに、ネットワーク構成や認証基盤の見直し等を検討するとしている。
24	2022/11/30	届出者（企業）が利用する RADIUS サーバと Active Directory サーバにおいて、異常が発生したことを示す通知を確認した。調査したところ、Active Directory サーバの機能が停止しており、さらに、基幹サーバを含む複数のサーバ上のファイルが暗号化され、デスクトップ画面に脅迫文が表示されていることを確認した。脅迫文の特徴から、Blackcat によるランサムウェア攻撃を受けたものと推定される。侵入の原因や侵害拡大の原因については不明である。対応として、全機器に対してウイルスキャンを実施し、基幹サーバについてはバックアップデータを基に復旧させた。

項番	届出日	概要
25	2022/12/2	届出者（企業）が利用するファイルサーバにおいて、データの取得が失敗することを発見した。調査を実施したところ、サーバ内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が確認された。拡張子の特徴から、DeadBolt と呼ばれるランサムウェアの攻撃を受けたものと推定される。なお、脅迫文は確認されなかった。原因の特定には至っていないが、使用していた VPN 装置を経由して、不正侵入された可能性があると推測している。対応として、被害に遭ったサーバを初期化した上でバックアップから復旧した。再発防止策として、UTM の導入のほか、システム構成の見直しを実施した。
26	2022/12/14	届出者（教育・研究機関）の組織内で利用している端末がインターネットに接続できない状態になったため、保守業者に連絡をしたところ、バックアップサーバ上のファイルが暗号化され、脅迫文と見られるテキストファイルが作成されていることを発見した。さらに、ファイルサーバや Active Directory サーバ等も被害を受けていたことが判明した。暗号化されたファイルの拡張子や脅迫文から Blackcat と呼ばれるランサムウェアの攻撃を受けたものと推定される。侵入の原因や感染が拡大した原因は、届出時点では不明であり、復旧には至っていない。対応として、更なる感染拡大を避けるため、ネットワークを切り離した上で調査が進められている。
27	2022/12/16	届出者（企業）が利用するサーバに対して、不審なリモートデスクトップ接続が確認された。調査したところ、サーバ内にウェブブラウザが不正にインストールされ、アラビア語の画面が表示されていることが確認された。さらに、サーバ上で稼働していたタスクも全て停止されていることが判明した。サーバ内のファイルの拡張子が.nemesis に変更されていたことから、Nemesis と呼ばれるランサムウェアの攻撃を受けたものと推定される。侵入の原因は届出時点で不明である。対応として、影響を受けたサーバをネットワークから切り離し、リストアを実施した。

項番	届出日	概要
28	2022/12/16	届出者（医療機関）の職員が電子カルテを使用していたところ、サーバとの通信が切断されたとの警告が表示された。外部業者に調査を依頼したところ、届出者が利用する NAS に保存していたファイルの拡張子が.faust に変更され、管理画面に脅迫文が表示されていることが確認された。ファイルの拡張子から Phobos の亜種によるランサムウェアの攻撃を受けたものと推定される。本件ではサーバ 2 台と NAS が暗号化の被害に遭った。侵入の原因は不明だが、届出者は、被害を受けたサーバが外部からリモートデスクトップ接続が可能な状態にあったことから、総当たり攻撃等により認証を突破された、あるいは、VPN 装置の脆弱性悪用により認証情報を窃取され、不正侵入されたものと推測している。対応として、ネットワーク遮断を行い、暗号化の被害に遭った機器については初期化後、オフラインバックアップのデータから復旧させた。再発防止策として、ファイアウォールの最新化、VPN 装置の ID とパスワードの変更、セキュリティソフトの導入等を実施した。
29	2022/12/23	届出者（教育・研究機関）が運用するアカウント管理システムにおいて、利用者からパスワード変更ができないとの連絡があった。当該システムのサーバを確認したところ、サーバ内に脅迫文が残されていることが判明した。設置された脅迫文等の特徴から、Venus と呼ばれるランサムウェアの攻撃を受けたものと推定している。侵入の原因は不明だが、ファイアウォールにアクセス制限に関する設定不備が存在していたことから、何らかの方法で認証を突破されたものと推測している。他サーバへの侵害拡大は確認されていない。対応として、原因となった設定不備を修正し、当該サーバをネットワークから切り離した。さらに、全てのアカウントのパスワード変更や不正アクセス元の遮断、サーバの初期化等の対応を行った。再発防止策として、設計・構築時におけるセキュリティ評価や運用体制の見直し等を実施するとしている。

項番	届出日	概要
30	2023/1/11	届出者（一般団体）のパソコン及びサーバが複数台、ランサムウェア感染の被害を受けた。暗号化されたファイルの拡張子や脅迫文から、Faust ランサムウェアと呼ばれる攻撃を受けたものと推定される。原因は、サーバ内の PDF ファイルを閲覧したことにより感染したものと推定している。対応として、ランサムウェア被害からの回復のために初期化を行った。再発防止策として、ランサムウェアを検知・遮断するセキュリティソフトを導入した。
31	2023/1/31	届出者（企業）の基幹システムが停止していることを発見したため、サーバの状態を確認したところ、複数のサーバ内にあるファイルの拡張子が.Elbie に改ざんされていることが判明した。拡張子の特徴から、Elbie ランサムウェアによる攻撃を受けたものと推定している。侵入の原因は不明であるが、侵害が拡大した原因は、利用していたファイルサーバや外付けハードディスクでファイル共有機能を使用していたためと推測している。対応として、VPN 装置のパスワードを変更し、暗号化の被害に遭った機器全ての初期化などを行った上で、外部組織にも調査を依頼した。再発防止策として、EDR の導入を実施するとしている。

項番	届出日	概要
32	2023/2/6	届出者（一般団体）の職員が、ファイル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。サーバ内を調査した結果、ファイルの暗号化のほかに金銭を要求する内容の脅迫文が残されていることも確認された。暗号化されたファイルの拡張子や脅迫文から、DRCRM と呼ばれるランサムウェアの攻撃を受けたものと推定している。侵入の原因は、利用していた Active Directory サーバにおいて、IP アドレス制限やロックアウト設定をしていなかったことや、管理者権限を持つパスワードが脆弱なアカウントを放置していたことにより、総当たり攻撃による認証を突破されたと推測している。これにより、侵害した Active Directory サーバを介して、組織内の複数の端末に被害が拡大したと推測している。対応として、影響を受けたサーバ等を隔離し、全てのアカウントのパスワード変更やウイルススキャンを行った上で、外部業者に調査を依頼した。再発防止策として、セキュリティが強化されたクラウドサービス上に移行するとともに、アクセス元の制限やパスワードポリシーの見直し、監視体制の強化等を実施するとしている。
33	2023/2/9	届出者（企業）が利用するバックアップサーバにログインできなくなったため、バックアップ管理用サーバを確認したところ、デスクトップに脅迫文が残されていることが判明した。脅迫文の特徴などから、RCRU64 と呼ばれるランサムウェアの攻撃を受けたものと推定される。侵入の原因として、検証用のサーバ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ことや、多数のログイン試行の失敗ログが確認されたことから、総当たり攻撃により、認証を突破されたものと推測している。さらに、当該サーバを踏み台として、脆弱なパスワードを設定していたバックアップサーバなどに不正なリモートデスクトップ接続をされ、被害が拡大したと推測している。対応として、不正アクセス元の遮断や全機器の ID 及びパスワード変更などを行った。再発防止策として、認証システムや監視サービスの導入のほか、構成管理やアクセス制限の見直しなどを実施した。

項番	届出日	概要
34	2023/2/28	届出者（教育・研究機関）が利用する NAS 上のファイルが開けない状態であることを発見した。確認したところ、NAS に保存していたファイルが暗号化され、拡張子が.Elbie や.eking に変更されていたことが判明した。被害状況から、Phobos ランサムウェアの攻撃を受けたものと推定している。侵入の原因は、アクセス制限の設定不備により、外部から NAS に直接アクセスできる状態にあったこと、また、NAS で設定していたパスワードが脆弱なものであったことにより、パスワードリスト攻撃などの方法で侵入されたものと推測している。さらに、NAS はファイル共有の機能を有していたため、ほかの NAS 複数台に感染が拡大した。対応として、ネットワークを遮断するとともに、NAS を利用していたパソコンのウイルスキャンなどを行った。暗号化の被害に遭った NAS については初期化し、バックアップデータから復旧させた。再発防止策として、NAS の利用を停止し、グループウェアの利用に移行した。

項番	届出日	概要
35	2023/3/17	届出者（企業）の従業員が、業務で使用するパソコンが起動できない状態であることを発見した。調査したところ、社内に存在するサーバ数台、パソコン数百台において、ファイルが暗号化されていることが判明した。脅迫文の特徴から、Ragnar Lockerと呼ばれるランサムウェアの攻撃を受けたものと推定している。侵入の原因は、リモートワークを実施している従業員の自宅パソコンが何らかのウイルスに感染した、あるいは社内で利用していた VPN 装置（SonicWall）の何らかの脆弱性を悪用されたことにより、認証情報が窃取され、社内ネットワークに侵入されたものと推測している。侵害拡大の原因は、攻撃者によりログが削除されていたため、詳細な攻撃手口は不明であるものの、社内の Acrive Directory サーバが不正アクセスされ、管理者権限を乗っ取られたことで、ドメイン管理下にある機器にランサムウェアが拡散されたものと推測している。対応として、ネットワークを遮断し、感染した機器は初期化やバックアップデータのリストアにより復旧させた上で、専門業者にも調査を依頼した。再発防止策として、導入していた UTM 機器の設定やドメインコントローラーの権限設定等の見直し、監視機能やパスワードポリシーの強化、VPN 接続時における多要素認証の導入等を実施した。

項番	届出日	概要
36	2023/3/22	届出者（企業）が利用している基幹システムで異常が発生したため、当該システムのサーバ内を確認したところ、ファイルが暗号化され、脅迫文が残されていることを発見した。調査の結果、当該サーバに加え、NAS に保管されていたファイルも暗号化されていることが判明した。被害状況から、Cring ランサムウェアの攻撃を受けたものと推定している。侵入の原因について特定には至っていないが、VPN 装置（FortiGate）の脆弱性を悪用された可能性があると推測している。侵害が拡大した原因は、仮想サーバと NAS 間でファイル共有機能の利用していたためと推測している。対応として、社内ネットワークの切断を行った。影響を受けた機器については初期化したのち、バックアップファイルから復旧させた。再発防止策として、VPN 接続時における二段階認証の導入、利用している機器のセキュリティ更新の徹底、ファイル共有機能のクラウド化などを実施した。
37	2023/3/24	届出者（企業）が利用しているシステムに不具合が発生したため、サーバを確認したところ、画面に暗号化を告知した文面が表示されていることを発見した。調査の結果、基幹システムを構成するサーバ内のファイルの暗号化やパスワードの変更の被害を受けたことで、他のシステムに影響が生じ、運用不能になったほか、バックアップデータも暗号化の被害に遭っていることが判明した。侵入の原因について特定には至っていないが、VPN 装置（Fortigate）の脆弱性を悪用されたものと推測している。対応として、ネットワークの遮断やウイルススキャン、VPN 装置のアップデート、VPN 装置・サーバのパスワード変更等を実施した。

項番	届出日	概要
38	2023/3/27	届出者（企業）が利用している数百台の機器においてアラートが発生したため、調査を行ったところ、Active Direcroty サーバが乗っ取られていること、また、一部のサーバにおけるファイルの暗号化や脅迫文が残されていることが判明した。被害状況から、届出者は Cheerscrypt と呼ばれるランサムウェアの攻撃を受けたものと推定している。侵入及び侵害拡大の原因については特定に至っていないが、外部の組織が管理する管理サーバが攻撃者に乗っ取られたことで、そのサーバを経由して、侵入されたものと推測している。対応として、被害に遭ったサーバを停止し、ネットワークから遮断した上で、外部専門機関にフォレンジック調査を依頼した。また、暗号化されたファイルについては、バックアップを基に復旧させた。再発防止策として、アカウント管理やシステム構成の見直し、二段階認証の導入、アクセス制限等を実施した。さらに、ネットワーク監視ツールや EDR の導入などを実施するとしている。
39	2023/3/29	届出者（一般団体）のウェブシステムがランサムウェア攻撃の被害を受けた。調査を行ったところ、攻撃者が残したと見られる脅迫文と暗号化されたファイルの拡張子から、ESXiArgs ランサムウェアの攻撃を受けたものと推定している。侵入の原因は、利用していた VMware ESXi の脆弱性対策が不十分であり、当該製品に発見されたヒープオーバーフローの脆弱性（CVE-2021-21974）を悪用されたものと推測している。対応として、外部からのアクセスを遮断する措置を行った。再発防止策として、新規に構築したサーバの導入を予定している。

4-3. 脆弱性や設定不備を悪用された不正アクセス

表 5-4 は、2-3. 脆弱性や設定不備を悪用された不正アクセスに該当する事例のうち、CMS の脆弱性悪用に関する届出の一覧を示す。

表 5-4 CMS の脆弱性悪用に関する届出の概要一覧

項番	届出日	概要
40	2022/12/1	届出者（一般団体）が利用する CMS（WordPress）の管理画面上に見覚えのないプラグインを発見した。調査したところ、ウェブサーバに不正ログインが確認され、不正なディレクトリの作成や不正なプラグインの実行が行われていたことが判明した。不正ログインが成功した原因は不明であるが、届出者が利用する CMS に仕様上の問題があり、アップデートを保留としていたため、何らかの未対応の脆弱性を悪用されたものと推測している。対応として、アクセス制限や管理者パスワードの変更を行い、ウェブサーバを停止させた。再発防止策として、アカウント管理やアクセス権限、アップデート方法等の見直しを実施した。さらに、専門業者との保守契約の締結も検討するとしている。
41	2022/12/16	届出者（企業）が運営するウェブサイトにおいて、コンテンツ表示の異常が発生していることを発見した。調査の結果、サーバ内に WebShell と呼ばれるツールが設置されており、そのツールを経由して、ファイルの改ざんや不正ファイルの設置、違法サイトの公開が行われていたことが確認された。原因は、当該サイトで利用していた CMS（PowerCMS）の OS コマンドインジェクションの脆弱性を悪用されたものと推定している。対応として、当該サーバを停止し、代替となる新規サーバを構築するとともに、認証設定の見直し等を行った。

項番	届出日	概要
42	2023/1/19	届出者（企業）の顧客・取引先から、届出者の運営するウェブサイトにアクセスすると、アダルトサイトに誘導される旨の連絡があった。調査したところ、ウェブサイトに不正なスクリプトが埋め込まれていることが判明した。原因は、利用していた CMS（WordPress）を更新していなかったため、何らかの脆弱性を悪用され、当該サイトが改ざんされたと推定している。対応として、CMS アカウントをデフォルトのものから変更するとともに、外部業者にサイトの修復を依頼した。再発防止策として、CMS のバージョンアップやサーバの死活監視 などを行う保守サービスの契約やインシデント体制の見直しを行った。
43	2023/2/7	届出者（企業）のウェブサイトが不正アクセスされている可能性があるとウェブサイト制作会社より連絡があった。調査の結果、ウェブサーバ上に不正ファイルの設置やデータの削除などが確認され、ウェブサイトを利用した顧客の個人情報数万件が漏えいした可能性があることも判明した。不正アクセスの原因は、過去にウェブサーバで利用していた CMS（Movable Type）が残存しており、その未修正の脆弱性を悪用されたことで、不正侵入されたものと推測している。対応として、残存していた Movable Type のファイルを削除した上で、ウェブサーバを停止させ、ウェブサイトを非公開とした。再発防止策として、脆弱性診断の実施のほか、ソフトウェアのバージョン管理やアクセス制限の見直しなどを実施するとしている。

項番	届出日	概要
44	2023/3/23	届出者（企業）のウェブサイトが、ブラウザの検索エンジン経由でアクセスできないと従業員から連絡があった。確認したところ、当該サイトが改ざんされていることが判明した。原因は、届出者が過去に利用していた CMS（Movable Type）がウェブサーバ上に残存しており、その未修正の脆弱性を悪用されたことで、サーバ内へのバックドア等の設置やファイルの改ざんが行われたものと推測している。対応として、改ざんされたファイルや不要ファイルの削除及びアクセス制限などを行った。再発防止策として、現行 CMS のセキュリティ対策の見直しを実施した。
45	2023/3/27	届出者（企業）が運営する EC サイトにおいて、顧客のクレジットカード情報が漏えいした恐れがあると決済代行会社より連絡があった。調査の結果、バックドアの設置やカード情報を窃取するためのファイルの改ざんが確認され、顧客のカード情報数十万件が漏えいした恐れがあることが判明した。原因は、CMS（Sitecore）の脆弱性（CVE-2021-42237）を悪用されたことにより、バックドアを経由して改ざんが行われたものと推測している。対応として、当該サイトの決済機能を停止した上で、調査会社に調査を依頼した。再発防止策として、EC サイトの決済方式の変更を含めたシステムの刷新を行ったほか、脆弱性管理の見直し及びアクセス管理の強化、監視ツールの導入などを実施するとしている。
46	2023/3/28	届出者（企業）が運用しているウェブサイトにおいて、サイト上のコンテンツが表示されない状態にあることを発見した。調査したところ、ウェブサーバ上に不正ファイルが設置され、ファイルの改ざんも行われていることが判明した。原因は、利用していた CMS（WordPress）等が古いバージョンであったため、何らかの脆弱性を悪用されたものと推測している。対応として、設置された不正ファイルの削除、CMS 等のバージョンを最新のものに更新した。

表 5-5 は、2-3. 脆弱性や設定不備を悪用された不正アクセスに該当する事例のうち、EC ソフトウェアの脆弱性悪用に関する届出の一覧を示す。

表 5-5 EC ソフトウェアの脆弱性悪用に関する届出の概要一覧

項番	届出日	概要
47	2023/1/10	届出者（企業）が運営する EC サイトに対して、決済代行業者からクレジットカード情報の漏えいの疑いに関する連絡があった。調査の結果、顧客数百件分のカード情報が漏えいした可能性があることが確認された。また、EC サイトで使用していた CMS（EC-CUBE）の脆弱性（CVE-2013-3651）を悪用されたことで、ウェブサーバ内にバックドア等の不正なファイルが設置されていたことが判明した。その不正ファイルには、EC サイト利用者が入力したカード情報などをサーバ内のファイルに書き出す仕組みがあり、攻撃者は不正なファイルの設置後に期間を空けて当該ファイルを参照することで、その情報を窃取していたものと推測している。対応として、EC サイトのカード決済機能を停止させた上で、外部の専門機関に調査を依頼した。再発防止策として、EC サイトをサービス提供事業者がセキュリティ管理を担う SaaS 型のクラウドサービスに移行した。

項番	届出日	概要
48	2023/1/18	届出者（企業）が利用する決済代行サービスの提供事業者から、届出者の EC サイトを利用した顧客のクレジットカード情報が漏えいした疑いがあると連絡があった。調査の結果、クレジットカード情報を含む顧客の個人情報数千件が漏えいした可能性があることが判明した。原因は、EC サイトで使用していた CMS（EC-CUBE）に存在するクロスサイトスクリプティングの脆弱性の悪用であった。攻撃者は当該脆弱性を起点として、CMS の管理画面の内部に侵入し、商品購入時の処理に不正なプログラムを書き込むことで情報の窃取を試みたと推定される。対応として、EC サイトのカード決済を停止させた上で、調査機関に調査を依頼した。再発防止策として、監視体制の強化を実施した。さらに、本件発生の背景には、脆弱性の管理が不十分であったことが挙げられるとして、EC サイトの脆弱性管理を自社ではなく、サービスの提供事業者が管理するサービスに移行した。
49	2023/2/21	届出者（企業）が運営する EC サイトにおいて、顧客のクレジットカード情報が漏えいした恐れがあると決済代行会社より連絡があった。調査の結果、数千件のカード情報が漏えいした可能性があることが判明した。原因は、EC サイトで利用していた CMS（EC-CUBE）に存在するクロスサイトスクリプティングの脆弱性（CVE-2021-20750）を悪用されたことにより、サーバにバックドアが設置され、カード情報を窃取するためのファイルの改ざんが行われたものと推定している。対応として、当該 EC サイトを閉鎖した。再発防止策として、個人情報の取り扱いの見直しや、第三者機関による継続的な脆弱性診断の実施などを予定している。

表 5-6 は、2-3. 脆弱性や設定不備を悪用された不正アクセスに該当する事例のうち、SQL インジェクション攻撃に関する届出の一覧を示す。

表 5-6 SQL インジェクション攻撃に関する届出の概要一覧

項番	届出日	概要
50	2022/8/11	届出者（企業）の顧客・取引先から、届出者の運営するウェブサイトにアクセスすると、アダルトサイトへ誘導される旨の連絡があった。調査したところ、ウェブサイトに不正なスクリプトが埋め込まれていることが判明した。原因について届出者は、利用していた CMS（WordPress）を更新していない状態だったために、何らかの脆弱性を悪用され、当該サイトを改ざんされたものと推測している。対応として、CMS アカウントをデフォルトのものから変更するとともに、外部業者にサイトの修復を依頼した。再発防止策として、保守サービスを契約し、バージョンアップ対応やサーバの死活監視の実施に加え、インシデント体制の見直しも行った。
51	2023/2/28	届出者（企業）がウェブサイトのアクセス集計を行っていたところ、通常の数十倍もの大量のアクセス情報が記録されていることを発見した。調査の結果、当該ウェブサイトに外部からの不正アクセスが確認され、顧客の個人情報数千件分が流出したことが判明した。原因は、ウェブサイトに SQL インジェクションの脆弱性が存在しており、その脆弱性を悪用した攻撃を受けたことであった。その後の調査により、被害発生の前に脆弱性の有無を調査する通信があったことや、一部のエスケープ処理に不備が存在していたことも判明した。対応として、ウェブサイトを停止した上で、外部にフォレンジック調査を依頼した。再発防止策として、WAF の導入や定期的な脆弱性診断などを実施するとしている。

項番	届出日	概要
52	2023/3/2	届出者（企業）が運用している EC サイトにおいて、不審なログが検知されたと監視業者より連絡があった。外部業者に調査を依頼したところ、SQL インジェクションの脆弱性を悪用した攻撃を示すログなどが確認された。さらに、ログの解析結果より、攻撃にはオープンソースの脆弱性診断ツールである sqlmap が悪用されたことや、不正な SQL クエリーが実行されたことで、当該 EC サイト利用者の個人情報約数十万件分が流出した可能性があることが判明した。原因は、EC サイトに SQL インジェクション対策の不備があったことや、sqlmap による不正アクセスの認識及び対応が遅れたためとしている。対応として、攻撃元からのアクセスを遮断するとともに、EC サイトの脆弱性を修正する措置を行った。再発防止策として、WAF の SQL インジェクション対策の設定追加や定期的な脆弱性診断の実施、監視体制の見直しなどを実施するとしている。

表 5-7 は、2-3. 脆弱性や設定不備を悪用された不正アクセスに該当する事例のうち、CMS の脆弱性悪用、EC ソフトウェアの脆弱性悪用、SQL インジェクション攻撃を除いた、その他の脆弱性や設定不備を悪用された不正アクセスの届出の一覧を示す。

表 5-7 その他、脆弱性や設定不備を悪用された届出の概要一覧

項番	届出日	概要
53	2022/11/2	届出者（地方自治体）が運営を委託しているウェブサイトが改ざんされ、不審なリンクが掲載されているとの情報提供が外部からあった。調査の結果、不正アクセスにより、ウェブサイトのコンテンツが複数回、書き換えられていることを確認した。原因は不明だが、ウェブサーバで利用していた OS やソフトウェアのバージョンが古く、何らかの脆弱性を悪用されたことで、サイト管理用の ID・パスワードが窃取され、不正アクセスされたものと推測している。対応として、ウェブサイトを停止し、他のサイトにおいても同様の被害が発生していないかの調査を行った。再発防止策については、届出時点で検討中である。

項番	届出日	概要
54	2022/11/24	届出者（地方自治体）が運営するウェブサイトのメール配信システムにおいて、外部機関から、当該システムで使用しているドメインを送信元とした不審メールが発信されているとの連絡があった。調査したところ、ウェブサーバ上のメール配信ソフトウェアに不正なアカウントが作成されており、数万件の不審メールが発信されていたことが判明した。さらに、インターネット上の掲示板において、管理者アカウントの情報が掲載されていることも確認された。不正アクセスの原因は、利用していたメール配信ソフトウェアの脆弱性の悪用により、管理者情報を窃取され、不正ログインされたものと推測している。対応として、該当するシステムを停止させるとともに、他のウェブサイトにおいても同様の被害有無の確認を行った。再発防止策として、代替のサービスにより運用を再開するとともに、システムのセキュリティ強化等を実施した。
55	2022/11/25	届出者（企業）が利用する外部のサービスから、クレジットカード情報が漏えいした疑いがあるとの連絡がサービス提供元よりあった。調査の結果、サービス提供元のシステムが改ざんされたことにより、当該サービスを利用していた届出者のサイトから、数千件のカード情報が漏えいした可能性があることが判明した。対応として、当該サービスの利用を停止し、自社システムの調査を実施した。なお、調査の結果、届出者のサイトには攻撃を受けた痕跡は発見されなかった。再発防止策として、決済方式の変更等を実施した。

項番	届出日	概要
56	2023/1/10	届出者（企業）がウェブアプリケーションの開発・保守をするために利用している AWS のアカウントにおいて、外部業者からアカウント侵害の可能性がある旨の連絡があった。調査したところ、大量の不正な EC2 インスタンスなどが構築されており、さらに、不正メールの大量送信が行われていることも確認された。原因は、ウェブサーバ上の環境設定ファイルが、設定不備により外部から参照可能な状態となっていたところ、攻撃者により、ファイル内のアクセスキー情報を窃取されたものと推測している。これにより、攻撃者は窃取したアクセスキーを悪用し、不正な IAM ユーザーを作成することで、EC2 インスタンスの構築などといった不正操作を行ったものと推測している。対応として、不正に作成された IAM ユーザーや EC2 インスタンス等を無効化・削除するとともに、攻撃者によって削除されていた正規の IAM ユーザーの再作成等を行った。再発防止策として、AWS のセキュリティ機能を導入し、攻撃を受けた際に検知できる体制を構築する対応を実施した。
57	2023/1/20	届出者（医療機関）が FortiOS の脆弱性情報（CVE-2022-42475）を確認し、ネットワーク機器の保守ベンダにログ調査を依頼したところ、当該脆弱性の悪用を試みた痕跡が発見された。原因は、当該脆弱性の対策バージョンに更新していなかったことであるが、不審なファイルの設置などを行った痕跡はなく、実被害は確認されなかった。対応として、最新の対策バージョンへの更新や SSL-VPN 機能の無効化、保守用の ID とパスワードを変更する措置を行った。再発防止策として、バージョン更新の迅速化、脆弱性情報の収集体制の強化等を実施した。さらに、組織内ネットワークの監視強化を検討している。

項番	届出日	概要
58	2023/1/24	届出者（企業）が利用するウェブサービスの提供業者から、顧客の個人情報が漏えいした疑いがあるとの連絡があった。調査の結果、サービス提供業者のシステムが不正に改ざんされたことにより、届出者のウェブサイトを利用した顧客数千人分のカード情報が漏えいした可能性があることが判明した。対応として、当該サービスの利用を停止し、サイト上のカード決済を停止する措置を行った。再発防止策として、今後のサービス利用の選定時におけるセキュリティ条件の見直しを実施した。
59	2023/1/26	届出者（企業）が利用するウェブサービスの提供業者から、顧客のクレジットカード情報が漏えいした疑いがあるとの連絡があった。調査の結果、サービス提供業者のシステムが不正に改ざんされたことにより、届出者のウェブサイトを利用した顧客数百人分のカード情報が漏えいした可能性があることが判明した。対応として、ウェブサイト上のカード決済を停止した。再発防止策として、許可したサービス以外の利用を原則禁止する措置を行った。
60	2023/3/23	届出者（企業）の従業員や顧客に不審なメールが発信されていることを確認した。調査の結果、届出者の業務委託先のウェブサーバが不正アクセスされ、WebShell と呼ばれるツールの設置やウェブサイトの改ざん、不正にインストールされたメール配信ツールによる不正メールの送信などが行われていたことが判明した。不正メールには、改ざんされたウェブサイトに誘導する URL リンク等が記載されており、そのウェブサイトには、窃取した情報の公開と引き換えに、金銭を要求する旨の脅迫内容が書かれていた。原因は、ウェブサーバのファイルアップロード機能に存在していた脆弱性を悪用されたことであった。対応として、当該ウェブサーバを停止し、ネットワークから切り離した上で、外部機関に調査を依頼した。再発防止策として、ネットワーク監視体制やサーバのセキュリティ機能の強化等を実施した。さらに、委託先業者の選定やセキュリティに関する確認事項や確認方法の見直しなどを実施するとしている。

項番	届出日	概要
61	2023/4/14	届出者（企業）が運用するウェブサイトにおいて、大量の不正アクセスが確認されたとの連絡が保守業者よりあった。調査したところ、XPath インジェクションと呼ばれる脆弱性を悪用した攻撃により、顧客の個人情報数千件分が漏えいした可能性があることが判明した。原因は、当該脆弱性の対策不足や設定不備などであると推定している。対応として、ウェブサイトを停止し、脆弱性の修正を行った上で、外部の専門組織に調査を依頼した。再発防止策として、監視体制の強化、WAF の導入、定期的な脆弱性診断などを実施するとしている。
62	2023/4/18	届出者（企業）の従業員や顧客の個人情報が海外のサイトで公開されていると外部から連絡があった。調査したところ、当該サイトで公開された情報の中に、届出者に関連する情報が含まれていることが確認された。原因は、届出者の業務委託先で構築されたシステムにおいて、ログイン時の認証が回避可能となる設定不備が存在していたため、攻撃者に不正アクセスされ、サーバの認証情報や個人情報等を窃取されたものとしている。対応として、当該サーバのデータを削除した上で、IP アドレスによるアクセス制限や権限設定の見直し等を行った。再発防止策として、委託先との情報の取り扱いに関する契約の見直しのほか、設定不備を検知するシステムの導入等を検討するとしている。

4-4. ID とパスワードによる認証を突破された不正アクセス

表 5-8 は、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一覧を示す。

表 5-8 ID とパスワードによる認証を突破された不正アクセスの概要一覧

項番	届出日	概要
63	2022/8/24	届出者（企業）が運営する EC サイトにおいて、決済代行会社からクレジットカード情報の漏えい疑いに関する連絡があった。調査したところ、ウェブサーバ上に不正ファイルの設置や決済を行うプログラムに改ざんが行われていることが判明した。これにより、EC サイト利用者が商品購入の際に、偽のクレジットカード情報の入力画面が表示され、入力したカード番号等の情報が第三者に転送されるようになっていた。原因は、EC サイトの販売管理システムの管理画面において、アクセス制限が設定されていなかったため、総当たり攻撃等の方法により、認証を突破されたものと推測している。本件の対応として、ファイル変更を監視する仕組みの導入、EC サイト管理画面へのアクセス制限、事故対応体制の見直し等を実施した。
64	2022/11/11	届出者（企業）の海外子会社が利用するシステムに不正アクセスが確認され、調査を実施したところ、届出者のグループ企業が保管する企業情報等が外部に流出した可能性があることが判明した。専門機関に調査を依頼した結果、初期侵入はメールが起因であり、その後、リモートデスクトッププロトコルや Cobalt Strike と呼ばれるツール等を悪用されたことで、侵害範囲がグループ企業に拡大したものと推定している。対応として、インターネット接続の遮断や侵害された機器の切り離し等を行った。再発防止策として、ネットワーク構成の見直し、運用体制や監視体制の強化等を実施するとしている。

項番	届出日	概要
65	2022/11/16	届出者（一般団体）が運営するウェブサイトに不審な書き込みが行われているとの連絡が利用者からあった。当該サイトの管理業者が調査した結果、不審な書き込みは管理者アカウントで実行されていることが判明した。さらに、操作ログより、利用者情報を外部に出力したと見られる痕跡も発見された。不正アクセスの原因は、システムの構築時に作成された初期設定の脆弱なパスワードを持つ管理者アカウントが残存していたため、総当たり攻撃等の方法によって不正アクセスされたものと推測している。対応として、不正利用された管理者アカウントを削除するとともに、他のアカウントについてもパスワードを再設定する措置を行った。再発防止策として、パスワードポリシーやアカウント管理方法の見直し等を行った。
66	2022/11/16	届出者（企業）が構築・運用を受託するウェブシステムの複数のウェブページに、不審な JavaScript のコードが埋め込まれていることを発見した。原因は不明だが、届出者が利用していた CMS（WordPress）のアカウントに脆弱なパスワードを設定していたため、総当たり攻撃等の方法により認証を突破され、当該ウェブページが改ざんされたものと推測している。対応として、改ざん部分の削除や別サーバ上での再構築等を行った。再発防止策として、CMS 等のパスワード変更や CMS プラグインの整理や更新、WAF の導入等を実施した。
67	2022/11/17	届出者（地方自治体）が運営するウェブサイトの一部が改ざんされていることを発見した。調査したところ、ウェブサイトの管理画面に対して、総当たり攻撃と見られる大量のアクセスがあり、一部のアカウントは不正ログインに成功していたことが判明した。なお、改ざんされたウェブサイトは、公開設定を行う前であったため、一般には公開されなかった。対応として、システムを停止させ、当該サイトの利用を制限する措置を行った。再発防止策として、認証機能の見直しや複数回パスワードを間違えた場合のログイン制限等を実施した。

項番	届出日	概要
68	2022/11/21	届出者（企業）が運営する EC サイトにおいて、利用者から身に覚えのない購入連絡のメールを受信したとの連絡があった。調査したところ、当該アカウントに不正ログインが確認され、商品の購入では不正ログインされた利用者と関係の無い名義のクレジットカードが使われていたことが判明した。不正アクセスの原因は、特定のメールアドレスのリストを使用したログイン試行の形跡等が発見されたことから、何らかの理由で漏えいした情報を攻撃者が不正に入手し、本件の攻撃で悪用したものと推測している。対応として、不正アクセス元の遮断や利用者アカウントのパスワード初期化を実施した。再発防止策として、パスワードの運用に関する注意喚起や監視体制の強化等を実施するとしている。
69	2022/11/30	届出者（企業）が公開しているウェブサイトにおいて、動作遅延が発生していることを確認した。調査の結果、ウェブサーバ内に 2 つの不審なファイルが設置されており、これらのファイルに対して大量の不正アクセスが行われたことで、サーバに負荷が掛かっていたことが判明した。原因としては、外部業者に貸し出していた CMS（WordPress）の管理用アカウントにおいて、推測可能なパスワードが使われていたことや、外部から CMS の管理画面にアクセスするためのアクセス制限をしていなかったことから、何らかの方法で攻撃者に認証を突破され、不正アクセスされたものと推測している。対応として、ウェブサイトを停止し、CMS の管理者パスワードの変更、不正ファイルの削除等を行った。再発防止策として、CMS の管理画面に対する外部 IP アドレスからのアクセス制限を設けた上で、外部から正規のアクセスをする際には VPN 装置を経由するように規定した。

項番	届出日	概要
70	2022/12/19	届出者（教育・研究機関）が運用するウェブサーバに障害が発生し、ホームページや管理画面へのアクセスができない状態にあることを発見した。調査したところ、サーバ内に不正なプラグインがインストールされたことにより、当該サーバ上で利用していた CMS（WordPress）の動作に異常が発生していたことが判明した。また、数万件の迷惑メール送信の踏み台として悪用されていたことも確認された。原因は、ウェブサイトの管理画面が外部からアクセス可能な状態であり、かつ利用していたアカウントのパスワードが十分な強度ではなかったため、総当たり攻撃により認証を突破されたものと推測している。対応として、ウェブサイトを停止し、ホームページの全てのコンテンツを削除した上で、別に保存していたバックアップデータから復旧させた。再発防止策として、パスワードポリシーやネットワーク構成の見直し等を実施した。
71	2022/12/19	届出者（教育・研究機関）の職員から多数のエラーメールを受信したとの連絡があった。調査の結果、当該職員のメールアカウントから不審なメールが数十件発信されており、その他に千件近いメールがシステムで差し止められていたことが判明した。さらに、そのメールアカウントに対して、海外からの大量のログイン履歴があることも確認した。原因は、当該メールアカウントにおいて、脆弱なパスワードを設定し、かつ他のサービスにパスワードを使い回していたため、パスワードリスト攻撃等により認証を突破されたものと推測している。対応として、当該アカウントのパスワードを変更するなどの対応を行った。再発防止策として、認証機能の利用を厳格化させるとともに、個人情報の取り扱い等に関する周知を実施した。

項番	届出日	概要
72	2023/1/11	届出者（一般団体）が運営するウェブサイトにおいて、表示点検を行ったところ、当該サイトとは関係のない英文が挿入されていることを発見した。なお、当事象による第三者への被害等は確認されていない。原因については、利用していた CMS（WordPress）において、類推しやすいパスワードを設定していたため、辞書攻撃などの方法により認証を突破され、CMS の XML-RPC 機能を悪用されたことでウェブサイトの改ざんが行われたものと推定している。対応として、改ざんされたサイトの修正やパスワードの変更、アクセス元 IP アドレスの制限等を行った。再発防止策として、CMS のバージョンを最新に保つための体制強化を行うとしている。
73	2023/1/17	届出者（一般団体）の職員から、業務で使用しているメールアカウントのメールが削除されているとの連絡があった。調査の結果、当該メールアカウントに対して大量のログイン試行の形跡が確認されたとのことから、総当たり攻撃などの方法によって認証を突破されたことで、メールが削除されたものと推定している。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、使用を停止する措置を行った。再発防止策として、ログイン時における二要素認証の追加などを実施したほか、今後、よりセキュリティ機能が充実したメールサービスへの移行を検討するとしている。

項番	届出日	概要
74	2023/1/25	届出者（教育・研究機関）の職員が使用するメールアカウントにおいて、大量のエラーメールが受信されていることを発見した。調査したところ、当該アカウントへの不正ログインが確認され、大量の迷惑メール送信が行われていたことが判明した。また、送信されたメールの多くはメールシステムのセキュリティ機能により発信抑止されていたが、一部のメールは送信先に到達していたことが確認された。原因の特定には至っていないが、ログの調査結果より、ログイン試行が初回で成功していたことから、何らかの方法で入手した認証情報が悪用されたものと推測している。対応として、当該メールアカウントのパスワード変更や多要素認証の設定を行った。再発防止策として、多要素認証を全職員に徹底したほか、メールシステムのセキュリティ機能を利用し、不正なログイン試行を検知した場合にアクセスを遮断する設定を追加した。
75	2023/1/27	届出者（企業）の顧客・取引先から、ホームページが表示できないとの連絡があった。ウェブサーバを調査したところ、サーバ内に不正ファイルの設置やウェブサイトの改ざんが行われていることが判明した。なお、攻撃者が設置した不正ファイルに一部不備があったため、攻撃者の意図したとおりに動作していない状況であった。原因は、利用している CMS（WordPress）の設定を悪用した総当たり攻撃により、不正アクセスされたものと推測している。対応として、パスワードの変更等を行った上で、フォレンジック調査も依頼した。再発防止策として、ログイン時における認証機能の強化のほか、総当たり攻撃を防ぐためのロックアウト設定を追加した。

項番	届出日	概要
76	2023/2/1	届出者（企業）が利用するメールシステムにおいて、外部にメール送信ができない状態にあることを発見した。調査したところ、通常では見られない大量のメール送信が行われていたことが確認された。原因は、当該メールシステムの管理者用 ID とパスワードが何らかの方法で流出し、それらを悪用した攻撃者により、メールシステムに不正な設定変更が加えられたことで、メールの不正中継の踏み台として悪用されてしまったと推測している。対応として、不正な設定の削除、２段階認証の設定などを行った。再発防止策として、不審なアクセスログの確認などといった監視の強化のほか、端末認証の導入も検討するとしている。
77	2023/2/2	届出者（企業）の従業員が利用しているメールアカウントにおいて、海外からの不正アクセスが検知されたとの連絡がメールサーバ管理会社からあった。調査したところ、複数のメールアカウントが不正アクセスされ、不特定多数宛に大量の迷惑メールが送信されていたことが判明した。不正アクセスの原因は、当該メールアカウントにおいて、推測されやすいパスワードなどを設定していたことや、海外からのアクセス制限を設定していなかったことと推測している。対応として、該当アカウントのパスワード変更を行った。再発防止策として、セキュリティ対策や監視体制の強化、従業員向けのリテラシー教育を実施するとしている。
78	2023/3/1	届出者（一般団体）の職員が利用する複数のメールアカウントにおいて、メールの送受信ができない状態にあることが確認された。調査したところ、メールサーバの管理者アカウントが不正アクセスされ、不特定多数宛に数十万件ものフィッシングメールが送信されていたことが判明した。原因の特定には至っていないが、メールサーバの管理者アカウントを初期パスワードから変更していなかったため、何らかの方法で特定されたものと推測している。対応として、不正アクセス元からのアクセス遮断やパスワードの変更、ウイルススキャン等を行った。再発防止策として、アカウント管理の見直しを実施した。

項番	届出日	概要
79	2023/4/24	届出者（教育・研究機関）の職員からメールアカウントの不調に関する連絡があった。調査したところ、当該職員のメールアカウントに海外の IP アドレスからの不正ログインと、数千件ものフィッシングメールが外部に発信されていることを確認した。また、そのほかの数名の職員においても、同様の事象が発生していることが判明した。原因の特定には至っていないが、フィッシングメールにより、メールアカウントの認証情報が流出したことで、攻撃者に不正ログインされた可能性があると推測している。対応として、不正アクセスを受けたメールアカウントを停止し、パスワードの変更などを行った上で、フォレンジック調査も依頼した。再発防止策として、メールシステムに二要素認証の導入やメール送信に関する監視の強化、全職員を対象にセキュリティに関する講習などを実施した。
80	2023/5/19	届出者（教育・研究機関）の職員が利用するメールアカウントから大量の迷惑メールが送信されているとの連絡が外部業者よりあった。調査したところ、数千件もの迷惑メールが不特定多数宛に送信されていることが判明した。原因は、通常では見られない回数の認証試行の失敗が確認されたことから、総当たり攻撃による認証突破によるものと推測している。なお、認証試行については、数か月前から複数の職員のメールアカウントやメーリングリストに行われており、さらに、同一 IP アドレスの使用による不正アクセス検知を避けるため、1 つの IP アドレスを用いた試行は 3 回までに留められていたことも判明した。対応として、被害に遭ったメールアカウントのパスワード変更などを行った上で、ログ調査も実施した。再発防止策として、セキュリティ機能がより充実した別事業者のメールサービスに移行を検討するとしている。

4-5. その他

表 5-9 は、ここまでの分類に該当しない、その他の届出事例に関する一覧を示す。

表 5-9 その他の届出事例の概要一覧

項番	届出日	概要
81	2022/11/17	届出者（企業）が提供する通信サービスにおいて、一部の利用者がインターネット接続できない事象が発生した。調査の結果、アクセスポイントの脆弱性を悪用した攻撃により、不正なスクリプトが埋め込まれ、それにより、アクセスポイントが海外サーバに対する DDoS 攻撃の踏み台として悪用されていたことが判明した。この DDoS 攻撃による通信の急増の結果、上位の回線業者が通信制限を実施したことで、インターネットに接続ができない状態となっていた。対応として、不正なスクリプトを削除し、不正な通信を遮断する等の措置を行った。再発防止策として、利用している製品のアップデートや異常を検知するための仕組みを導入するとしている。
82	2022/12/27	届出者（企業）の従業員がインターネット検索をしていたところ、パソコンの画面にウイルス感染したことを示す、セキュリティ警告が表示された。当該従業員は画面に表示された電話番号に連絡し、指示どおりにパソコンを操作してしまい、パソコンが遠隔操作される事態になった。状況から、偽警告・サポート詐欺と推定している。対応として、パソコンのウイルススキャンと初期化を実施した上で、調査会社にも調査を依頼した。再発防止策として、セキュリティ体制の見直し等を実施するとしている。

項番	届出日	概要
83	2023/1/11	届出者（企業）の従業員が特定の企業名をインターネット検索し、検索結果に表示されたリンクにアクセスしたところ、偽の警告画面が表示されるとともに警告音が鳴った。当該従業員は警告画面に表示された電話番号に連絡し、指示に従い、リモート操作ツールをダウンロードしてしまった。その後、問題の解決に費用が掛かる旨の指示があり、不審に思った従業員が社内の IT 部門へ連絡をしたことで、偽警告・サポート詐欺であることが判明した。対応として、利用していたパソコンをネットワークから遮断し、ウイルススキャンを行った上で、フォレンジック調査の依頼も行った。再発防止策として、社内周知を行ったほか、当該従業員へのセキュリティ教育を実施した。
84	2023/2/14	届出者（一般団体）が利用するパソコンにおいて、ウイルスが検知されたとの警告画面が表示された。表示された電話番号に連絡したところ、遠隔操作ツールをダウンロードするよう誘導され、パソコン内に当該ツールをダウンロードしてしまった。状況から、偽警告・サポート詐欺と見られる。その後、修復に関する料金説明が行われた際に不審であると判断し、切電した。対応として、フォレンジック調査を実施した。
85	2023/2/24	届出者（企業）が利用している監視ツールにおいて、アウトバウンド通信に関するトラフィックが急増していることを発見した。調査の結果、届出者が運用管理しているサーバに不正アクセスが確認され、サーバ内に DDoS を目的としたツールなどが設置されていること、また、不正アクセスにより、当該サーバ内に保存されていた情報数万件が流出した可能性があることも判明した。被害原因は、ファイアウォールの設定に不備があったこと、また、当該サーバで利用していたアカウントのパスワードがデフォルトのものであったため、総当たり攻撃などにより、認証を突破されたものと推測している。対応として、当該サーバをネットワークから切り離し、サーバを停止させた上で、外部の専門機関に調査を依頼した。再発防止策として、アカウントの管理方法やアクセス制限、ログの取得方法等に関する見直しを実施した。

項番	届出日	概要
86	2023/3/24	届出者（企業）が運営する EC サイトにおいて、クレジットマスター攻撃が行われた可能性があるとの連絡が外部の決済サービス業者からあった。調査の結果、１日当たり数十万件もの決済試行が行われていたことが確認された。被害原因は、当該 EC サイトにおいて、カード情報の入力可能な回数に上限などを設けていなかったためと推測している。対応として、カード決済の試行回数の制限、IP アドレス制限等を行った。再発防止策として、決済試行に複数回失敗した場合に、一定時間決済を利用できなくするロック機能を導入した。さらに、3D セキュアの導入を検討するとしている。
87	2023/3/31	届出者（企業）が利用しているメールサービスにおいて、サービス提供事業者から、メールアカウントが乗っ取られた疑いがあるとの連絡があった。調査の結果、メールアカウントの乗っ取りは誤検知であり、正しくは、攻撃者が使い捨てのメールアドレスを用いて、届出者の EC システムに多数のアカウント登録を行ったことで、仮登録時に発信される大量の自動配信メールが乗っ取りによるものと誤検知したものであった。その後の調査により、攻撃者は EC サイトに登録した大量のアカウントを用いて、クレジットマスター攻撃を行っていたことも判明した。被害原因は、当該 EC サイトの上でのアカウント登録やクレジットカードの有効性確認が容易に行えたこと、また、ボット対策など未導入であったことが要因と推測している。対応として、不正アクセス元からのアクセスを遮断するなどの措置を行った。再発防止策として、WAF によるアクセス制限、クレジットカードの認証時における試行回数の制限、3D セキュアの導入などを実施した。

項番	届出日	概要
88	2023/5/15	届出者（企業）が利用している外部サービスにおいて、届出者の従業員のアカウントが不正アクセスされた可能性があるとサービス提供事業者より連絡があった。調査したところ、サービス提供事業者を名乗る偽の担当者から当該従業員宛に、メールと電話による連絡があり、認証情報を伝えてしまっていたことが判明した。さらに、アカウントが不正アクセスされたことにより、当該サービスに登録されていた数万件の個人情報が流出した可能性があることも確認された。対応として、当該アカウントの停止、全アカウントのパスワードの初期化、全従業員への注意喚起を行った。再発防止策として、当該サービスのアクセス時における二要素認証の導入や全従業員への継続的な教育を実施するとしている。
89	2023/3/9	届出者（企業）が利用する監視ツールにおいて、特定のユーザーの認証エラーが発生していることを確認した。調査したところ、ウェブシステムに外部からの不正アクセスが確認され、サーバ内に複数の不正なツールを設置されていることが判明した。不正アクセスの原因については不明である。対応として、外部からのアクセスを遮断した上で、外部の専門機関による調査を行った。再発防止策として、脆弱性対応をはじめとした改善項目の洗い出しとそれをシステム運用に反映するとしている。
90	2023/3/24	届出者（企業）の従業員が自組織のウェブページを確認したところ、一部の表示が不審な内容に改ざんされていることを発見した。対象のウェブサーバを調査したところ、ウェブページを構成するソースコードの改ざん､利用していたCMS（WordPress）の削除、サーバに保管していたバックアップデータの改ざんなどが判明した。被害原因については届出時点で不明であり、調査が進められている。対応として、パスワードの変更やサーバの再構築を行った。再発防止策として、外部業者との保守管理体制の見直しや認証情報の管理を徹底するとしている。

5. 届出へのご協力のお願い

本紙の内容は、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 に届出いただいた情報を基にしています。これらの情報を事例として公開することにより、同様被害の未然防止や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/todokede/crack-virus/about.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つなげられるよう、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）