# コンピュータウイルス・不正アクセスの届出事例

［2023 年下半期（7 月～12 月）］

独立行政法人情報処理推進機構 セキュリティセンター

2024 年 3 月 27 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、2023 年上半期（1 月～6 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、掲載に足る情報がそろった事例については、2023 年下半期（7 月～12 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、61 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　5 件
- 身代金を要求するサイバー攻撃の被害　17 件
- 脆弱性や設定不備を悪用された不正アクセス　15 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　13 件
- その他　11 件

全体を通して見ると、ここ数年変わらず、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くあった。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）と、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る。また、身代金を要求するサイバー攻撃の被害（2-2 節で説明）についても、主に VPN 装置の脆弱性を悪用されたことや、何らかの理由で流出した認証情報を攻撃者に悪用されたことで、外部からの侵入を許してしまったというものであった。改めて、修正プログラムの適用や ID・パスワードの管理などが適切に行われているか、自組織のセキュリティ対策の実施状況を点検することを勧める。

各分類の件数に注目すると、身代金を要求するサイバー攻撃の被害に分類される事例が最も多かった。さらに、その攻撃内容別で見てみると、主に LockBit と呼ばれるランサムウェア（以下、LockBit）に関する被害が届出されており、その他に、Phobos の亜種（faust など）、Mallox などのランサムウェアに関する届出があった。また、届出された事例の中には、ファイルの暗号化はされず、窃取されたファイルの公開と引き換えに金銭を要求されたというものもあった。この事例は、昨年に警察庁が公開資料 [7]で取り上げていた「ノーウェ

[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。

[7] 警察庁 「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

アランサム攻撃」に類する事案であったと考える。

ノーウェアランサム攻撃は、従来の侵入型ランサムウェア攻撃と比べて、ファイルの暗号化などに掛かる工数が不要、また、暗号化によって EDR（Endpoint Detection and Response）に検知されるリスクを減らせるなどといった利点があることから、今後、同様の被害が発生することが懸念される。

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を企図した不審メールの受信、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いただいている。2023 年における届出全体の集計情報については、次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にしていただきたい。

- コンピュータウイルス・不正アクセスの届出状況［2023 年（1 月～12 月）］
  https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-report.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 5 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、それらの概要を紹介する。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る。

今期においては、Emotet の検知や感染被害に関する届出が 3 件あった。なお、いずれも 2022 年 3 月以前に発見されたものであった。届出の窓口にて把握している限りでは、2023 年 4 月以降、Emotet とみられる攻撃は確認されておらず、今期の攻撃活動としては停止している状況であったと推測している。なお、Emotet は不定期に休止・再開を繰り返しており、今後、再び大規模な攻撃活動が開始される可能性があるほか、新たに Emotet と類似した手口で拡散を図る、別のウイルスの攻撃が発生することも考えられるため、引き続き警戒と情報収集に努めていただきたい。

IPA では次のウェブサイトにおいて、Emotet に関する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。日々の情報収集や対策の参考として活用いただきたい。

- 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」と呼ばれるツールのほか、Emotet に感染した場合などの対応 FAQ を公開している [8]。こちらも参考としていただきたい。

（2） Emotet 以外のウイルス

Emotet 以外のウイルスに関する届出としては、従業員が使用するパソコンに偽の連絡メールが届き、そのメールの本文に記載されていた URL をクリックしたことで、ウイルスがダウンロードされ、パソコンがウイルスに感染してしまったという事例があった。

こうした事例の対策としては、組織内でのセキュリティ教育や注意喚起などを通じて、不用意に URL や添付ファイルを開かないよう、従業員・職員に徹底させるとともに、少しでも不審な点に気付いた場合、あるいは不審なメールを開いてしまった場合に、速やかに担当部署へ報告が届くよう、組織内における連絡フローの構築及び周知を行うことが重要である。また、ウイルス感染の被害を未然に防ぐためにも、OS やソフトウェア、セキュリティソフトを最新に保つなどといった、日々の運用も欠かさずに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 17 件の届出について、それらの概要を紹介する。

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。

冒頭でも述べた通り、今期においても、LockBit による被害を継続して確認している。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

[8] 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

まった事例を確認している。なお、2024 年２月に EUROPOL（欧州刑事警察機構）より、日本を含む 10 カ国の複数機関による共同捜査（Operation Cronos）によって、Lockbit に関与していた人物の逮捕やインフラのテイクダウンが行われたとの公表[9]がされた。しかしながら、その数日後に、Lockbit が新たなインフラを構築したとの情報[10]や、Lockbit の新バージョンとみられる「LockBit-NG-Dev」が確認された[11]との情報がセキュリティベンダーなどから公表されていることもあり、引き続き同グループへの警戒が必要な状況である

侵入の原因（推定も含む）について見てみると、先期から引き続き、VPN 装置の脆弱性を悪用された事例があったほか、詳しい経緯までは不明であるものの、何らかの理由で流出した認証情報が攻撃者に悪用され、組織内ネットワークへと侵入されたと推測している事例があった。また、調査を行ったが、調査に必要なログが適切に取得できておらず、侵入経路の解明に至らなかったという事例も確認している。通信ログやアクセスログ、イベントログなどは、被害発生時にどのような通信が行われていたか、また、システム内で何が発生したかなど、原因や影響範囲を特定する上で重要な記録情報である。今一度、組織内でログ管理方法について見直し、適切なログの取得・保管を行うようにしていただきたい。

本分類のような被害を防ぐための対策方法として、次の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
・脆弱性対策
・アクセス制御と認証の強化
・攻撃メール対策

続けて、組織内ネットワークに侵入されてしまった場合を想定し、侵害の範囲拡大を抑えるための対策の例を次に示す。

・必要最小限の権限付与
・パスワードの管理
・ネットワーク接続点のセキュリティ強化
・ドメインコントローラーのセキュリティ強化
・セキュリティソフトの導入

加えて、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のバックアップ方法の

---

[9] EUROPOL「Law enforcement disrupt world’s biggest ransomware operation」
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[10] 株式会社マイナビ「ランサムウェアグループ「LockBit」がもう復活、すでに 12 件の侵害公開」
https://news.mynavi.jp/techplus/article/20240228-2893776/

[11] トレンドマイクロ株式会社「ランサムウェア攻撃者グループ「LockBit」の摘発の影響と今後」
https://www.trendmicro.com/ja_jp/jp-security/24/b/expertview-20240228-02.html

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などを実施することも重要であると考える。

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。組織内の周知や対策の参考として活用いただきたい。

- 【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

また、JPCERT/CC では、侵入型ランサムウェア攻撃を受けた際の FAQ を公開している[12]。こちらも参考としていただきたい。

### 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 15 件の届出の概要を紹介する。あわせて、2-2 節で述べた、VPN 装置の脆弱性を悪用した攻撃及びその対策方法についても本節で説明する。

今期において、VPN 装置の脆弱性を悪用された事例は先期ほどの届出はなかった。しかしながら、VPN 装置の脆弱性を狙う攻撃は継続している状況であると推測される。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、自組織が対応可能な範囲を明確化し、契約している保守業者との契約内容を見直す。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。

また、設定不備を悪用された事例についても見てみると、ウェブサーバ上に外部から閲覧可能なセットアップファイルや別サーバの接続情報が書かれたファイルなどが誤って置かれており、それを攻撃者に悪用され、不正アクセスされた事例であった。その他にも、AWS のアクセスキーが外部に流出したことで不正アクセスされた事例なども確認している。こ

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

れらの事例は件数として多くはないが、毎年数件は届出を確認している。VPN 装置を含む脆弱性への対応も重要であるが、こうした被害が発生していることにも目を向け、組織で利用している機器が本来の利用に適した設定となっているか、アクセス権限が正しく設定されているかなど、点検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 13 件の届出の概要を紹介する。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。

今期においては、主に脆弱なパスワードを使用していたことで、ID・パスワードの認証が突破されたという事例が見られた。また、攻撃手口について見ると、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を複数確認している。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、本分類のような被害を防ぐためのアカウント管理方法として、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。

今期に届出された事例の中には、メールアカウントに不正アクセスしたのち、そのメールアカウント上のメール情報などを不正に入手した上で、実在する届出者の内部組織を装ったフィッシングメールが送信されたという事例があった。その詳細については、3 章で紹介する。

### 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・不正アクセスに該当しないものや、調査を行っても被害の詳細が判明しなかったもの等を分類している。今期においては、偽セキュリティ警告（サポート詐欺）に関する事例が複数届出されたため、その概要について説明する。

偽セキュリティ警告（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。電話をかけると、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。

今期に届出された事例においては、明確に金銭被害を受けたとする事例はなかったものの、警告画面に表示された電話番号に連絡し、指示に従い、パソコン内に遠隔操作ソフトウェアをインストールしてしまったという事例が散見された。この遠隔操作ソフトウェアをインストールし、第三者に操作の許可をしてしまうと、パソコン内の情報を閲覧されることになり、重要な情報が流出してしまう恐れがあるので、十分注意をしていただきたい。

IPA では、次のウェブサイトに偽セキュリティ警告（サポート詐欺）に関する専用ページを用意しており、偽の警告画面の閉じ方を学べる体験サイトも紹介している。こちらを社内の注意喚起に利用するなどして、対策に役立てていただきたい。

- 偽セキュリティ警告（サポート詐欺）対策特集ページ
  https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211116.html

また、届出者では原因不明とされた事例であっても、被害の内容から、ソフトウェアの脆弱性の悪用や認証情報の管理等の問題に起因していると推測されるものがあった。直接的な原因は異なっていたとしても、前節までで述べてきた対策を行うことは、セキュリティの向上につながり、ウイルス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ため、これまでに述べてきた内容を参考としていただきたい。

## 3. 事例：職員の認証情報が組織内外への攻撃に悪用された事例

### 3-1. 届出内容

（1）　発見経緯

届出者（教育・研究機関）の職員より、大量のエラーメールが届いている旨の報告があった。確認したところ、届出者内に実在する組織（以下、内部組織）を装ったフィッシングメールが職員あてに送信されていたことが判明した。調査の結果、複数名の職員に当該フィッシングメールが届き、その一部がフィッシングサイトに認証情報（ID・パスワード）を入力していたことや、攻撃者がその詐取した認証情報を基に、届出者のメールサーバを踏み台とした大量の迷惑メール送信を行っていたことなどが確認された。

（2）　攻撃の流れ

本事例で確認された攻撃の流れを図 3-1 に示す。

なお、ここでは分かりやすくするために、最初に不正アクセスの被害を受けた人物を職員A、その後にフィッシングメールを受信し、認証情報を入力してしまった人物を職員 B として表す。

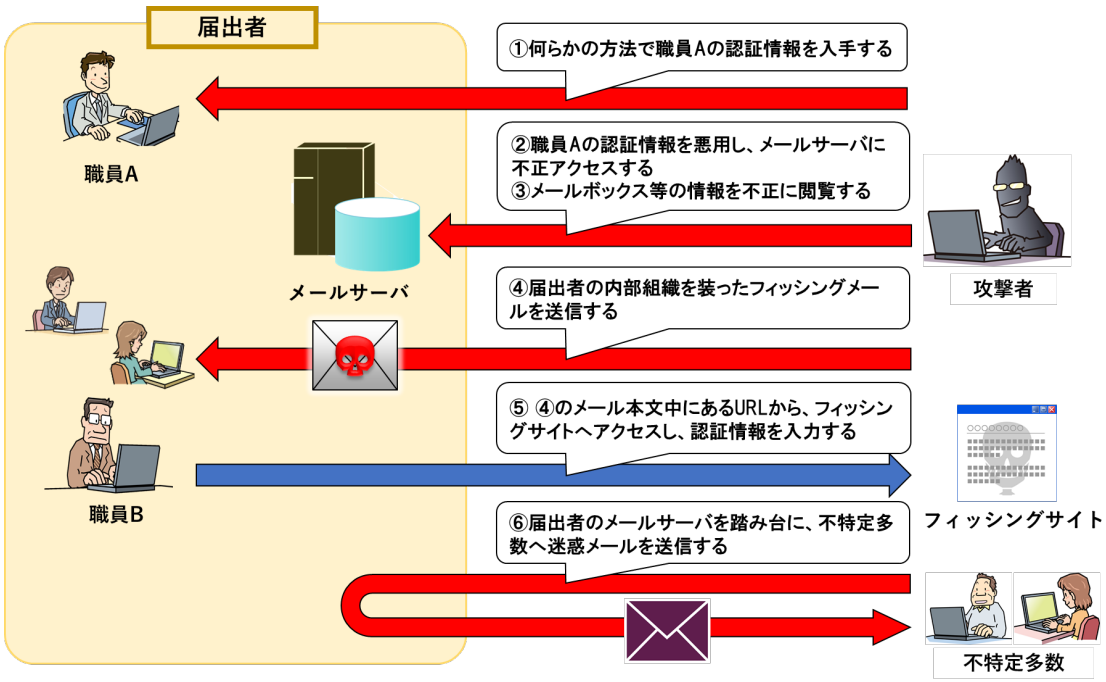


図 3-1 攻撃の流れ（※届出いただいた情報を基に IPA で作成）

① 攻撃者が何らかの方法で職員Ａの認証情報を入手する。
② 攻撃者が職員Ａの認証情報を悪用し、届出者のメールサーバに不正アクセスする。
なお、攻撃者はこの時点で迷惑メールの送信はしていなかった。これは、届出者のメールサーバ側でメールの送信制限を設定しており、攻撃者の目的である大量の迷惑メール送信を達成するためには、より多くのメールアカウントを入手する必要があったとみられる。
③ 攻撃者が職員Ａのメールアカウントで閲覧可能なメーリングリストやメールボックス内のメール情報などを不正に閲覧する。
④ ③で得た情報を基に、攻撃者が職員Ｂらに対して、届出者の内部組織を装ったフィッシングメールを送信する。
⑤ 職員Ｂがフィッシングメールと気づかずに、メール本文中の URL から、フィッシングサイトへアクセスし、認証情報を入力する。
⑥ 攻撃者が届出者のメールサーバを踏み台に、不特定多数へ迷惑メールを送信する。

（3） 被害原因

本件の被害原因として、次の２つが挙げられる。

a) 多要素認証の未導入

攻撃者が職員Ａの認証情報を入手した経緯については不明である。しかしながら、被害状況より、届出者のメールサーバのログイン認証において、多要素認証が使われておらず、ID とパスワードのみでログイン可能な状況であったとみられる。そのため、フィッシング攻撃による認証情報の詐取やパスワードリスト攻撃、パスワード類推攻撃などの方法で認証を突破された可能性があると推測される。

b) 不正に入手された情報を悪用した巧妙な内容のフィッシングメール

本事例において、攻撃者はフィッシングメールを送信する前に、職員Ａのメールアカウントへ不正アクセスしており、メーリングリストや実在する組織の名称など、職員Ｂらを騙すための情報を入手し、フィッシングメールに悪用したものとみられる。その結果、当該フィッシングメールを受信した職員Ｂは、攻撃メールであると気づかずに、フィッシングサイトへアクセスし、認証情報を入力してしまった。

（4） 被害内容

本事例では、届出者の職員が管理するメールアカウントが攻撃者に不正アクセスされたことで、アドレス帳に登録された個人情報やメールボックス内のメール情報などが窃取さ

れてしまった。さらに、届出者のメールサーバを踏み台として、不特定多数の宛先に大量の迷惑メールが送信されてしまった。なお、その送信された迷惑メールの大半はエラーメールとして返送されていた。

（5）　被害対応

- 組織的対策
  - 組織内にフィッシングメール及びパスワード変更の注意喚起
  - 侵害されたメールアカウントのパスワード変更
- 組織外への報告等
  - 所管省庁への報告
  - 警察への報告
  - 個人情報保護委員会（PPC）への報告
  - 届出者のウェブサイトにて本被害を公表

（6）　再発防止策

- 技術的対策
  - パスワードポリシーの見直し
  - 多要素認証の実装検討
  - 導入しているセキュリティ製品の設定見直し
  - セキュリティソフトのアップデート
- 組織的対策
  - 全職員に向けたフィッシングメールなどの啓発・注意喚起の周知
  - 情報セキュリティに関する研修の実施

### 3-2. 着目点

（1）　届出者の内部組織を装ったフィッシングメール

本事例では、届出者の職員が管理する、メールアカウントのメール情報などを攻撃者に不正閲覧されたのち、届出者の内部組織を装ったフィッシングメールが送信されたことで被害が拡大した。

届出者の職員あてに送信されたフィッシングメールの例を図 3-2 に示す。

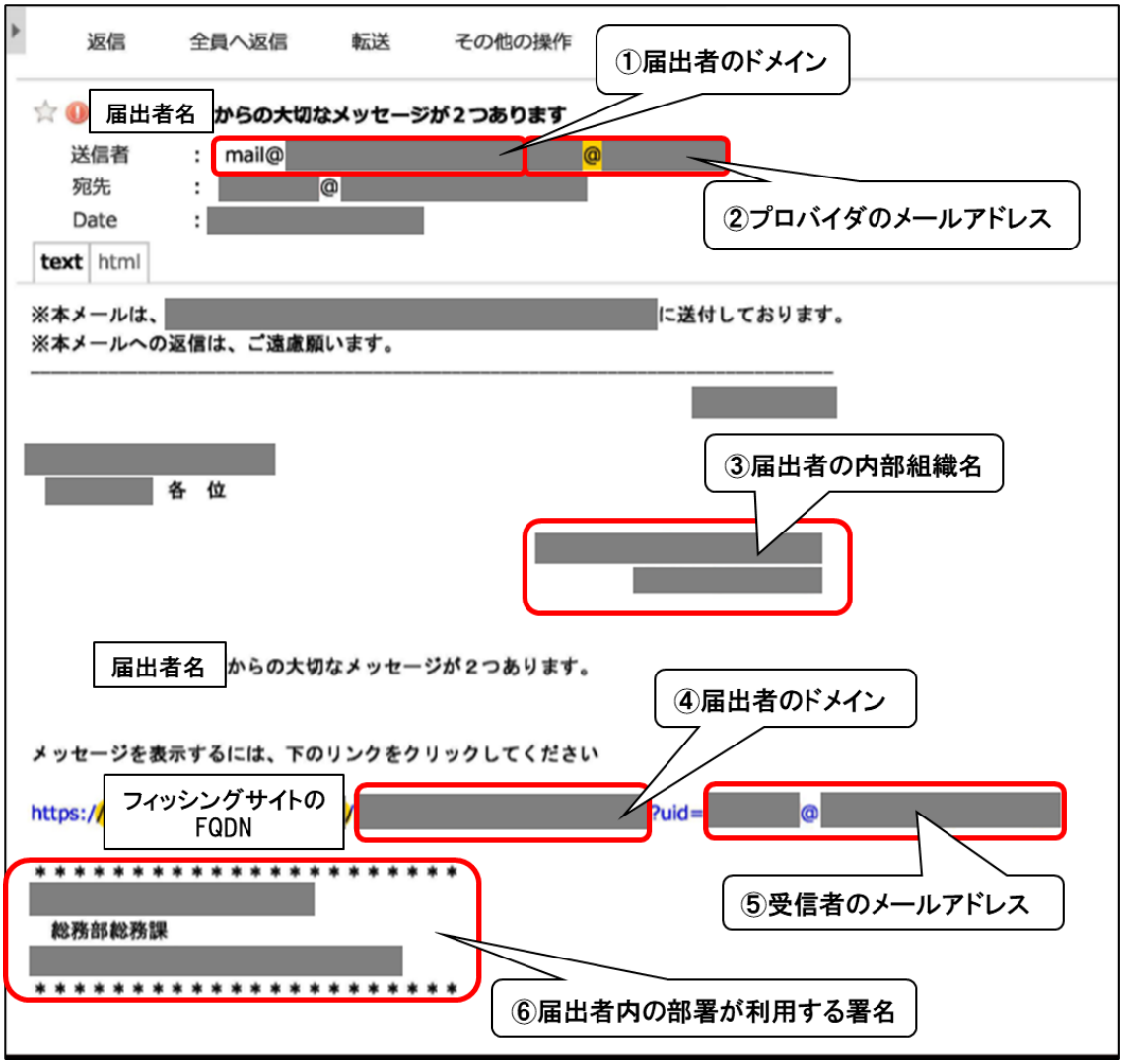


**図 3-2 届出者の職員あてに送信されたフィッシングメールの例**

当該メールを見ると、メール送信者の表示名には、届出者が管理するドメインのメールアドレスが使われていた（①）が、実際は、国内のプロバイダが提供するメールサービスを使用して送信されていた（②）。また、メール本文中にある、届出者の内部組織の名称（③）や署名（⑥）などに関しては、不正アクセス被害を受けた職員 A のメールボックスなどに存在していた情報を悪用されたものとみられる。さらに、本文中の URL を見ると、フィッ

シングサイトの FQDN の後には、届出者が管理するドメイン（④）や、メール受信者のものとみられるメールアドレスが含まれていた（⑤）。

上述した内容を踏まえると、送信者のメールアドレスや本文中の URL のドメインなどを注意深く確認することで、被害を未然に防げた可能性も考えられる。しかしながら、昨今では、フィッシングに使われる手口が巧妙化している傾向にあり、受信したメールや URL リンク先が正規のものであるかを誰もが確実に見極めることは難しい状況であると推察される。また、システム側で対策を行っていたとしても、メールのセキュリティ対策製品による検知をすり抜ける手法を用いたフィッシングメールも確認[13]されていることから、利用者の元にフィッシングメールが着信することを完全に防ぐのは困難であると考えられる。

フィッシング攻撃による被害を防ぐためには、組織内のセキュリティ教育や注意喚起を通じて、フィッシングメールなどに使われる攻撃手口を職員・従業員に知ってもらうことが重要である。その上で、少しでも不審に感じたら、添付ファイルや URL リンクを開かずに、所定の通報先に連絡することを職員・従業員が徹底するように、教育や啓発活動などを行っていただきたい。また、不審なメールの報告があった場合には、そのメールの調査を行い、必要に応じて、組織内への注意喚起やセキュリティ対策製品のフィルタリング設定の調整などを適切に実施可能か、自組織の対応手順の点検を勧める。

### （2） パスワードによる単一要素認証

本事例において、届出者のメールアカウントは、ID とパスワードのみでログイン可能な状態にあり、攻撃者に ID とパスワードを不正に入手されてしまったことで、メールサーバに保存されている情報の窃取やフィッシングメールの送信に繋がったものとみられる。この場合、ID とパスワードの単一要素認証ではなく、SMS など他の認証要素を組み合わせた認証手段を導入していれば、不正アクセスによる被害を防げていた可能性も考えられる。

パスワードによる認証は、他の認証手段と比較して導入が容易であることから、パソコンやサーバへのログインのみならず、インターネットからアクセス可能なクラウドサービスなどでも幅広く使用されている。その一方で、フィッシングによる認証情報の詐取やパスワードリスト攻撃、パスワード類推攻撃などにより、認証を突破される被害事例が後を絶たない状況でもある。特に Microsoft 365 や Google Workspace、VPN 装置などといった、組織内の重要な情報資産にアクセス可能なサービスやシステムである場合、不正アクセスされた際の影響がより深刻となることが懸念される。

こうした被害を防ぐために、SMS 認証や生体認証など、パスワードに依存しない認証手

---

[13] IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2023 年 10 月～12 月]」
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q3-report.pdf

段が利用可能である場合には、積極的に活用することを勧める。また、システム管理者においては、不正アクセスされた場合の影響が大きいと想定されるシステムやサービスに対して、可能な限り、多要素認証を導入することを検討していただきたい。多要素認証の導入が難しい場合でも、システムに対する組織外からのアクセス制限や不審なログインを検知する仕組みの導入といった、不正アクセスを検知・防御するために講じることができる複数の対策（多層防御）を確実に整備していくことが重要である。

## 4. 届出事例の概要

本章では、今期に取上げた 61 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 48 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、各分類の中で比較的多く届出される事例（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 4-1 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 に関する届出の一覧を示す。なお、それぞれの届出内容について、ほぼ差異は見られなかった。

**表 4-1 Emotet に関する届出の概要一覧**

| 項番 | 届出日 | 概要 |
|---|---|---|
| 1 | 2023/4/17 | 届出者（企業）のパソコン 2 台で Emotet 感染が確認された。対応として、外部業者にフォレンジック調査を依頼した。再発防止策としては、UTM（Unified Threat Management）の設置などを予定している。 |
| 2 | 2023/7/18 | 届出者（企業）のパソコン 1 台で Emotet 感染が確認された。対応として、パソコンを初期化した。再発防止策としては、セキュリティソフトの導入を検討している。 |
| 3 | 2023/8/3 | 届出者（企業）のパソコン 1 台で Emotet 感染が確認された。対応として、パソコンを初期化した。再発防止策としては、セキュリティソフトの導入を検討している。 |
| 4 | 2023/9/16 | 届出者（企業）のパソコン 1 台で Emotet 感染が確認された。対応として、パソコンを初期化した。再発防止策としては、セキュリティソフトの導入を検討している。 |

表 4-2 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 4-2 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 |
|---|---|---|
| 5 | 2023/6/9<br>(先期分) | 届出者（企業）の従業員に外部サービスの利用登録に関する不審なメールが着信したとの報告を、そのメールの転送とともに受けた。その報告を受けた別の従業員がメール内の URL リンクにアクセスしたところ、警告と見られるポップアップウィンドウが表示された。その後、パソコンを使用していると、設定画面のウィンドウが勝手に開くなどの異常が確認されるようになった。異常発生の原因は、当該メールの URL リンクにアクセスしたことによるウイルス感染と届出者は推測しているが、ウイルスの特定には至っていない。また、当該メールは社内間で転送されたものであったため、メールシステムによる警告が表示されず、安易に URL リンクにアクセスしてしまう状況であった。対応として、ウイルス感染が疑われるパソコンの初期化を行った。再発防止策としては、インシデント情報を社内に周知するとともに、不審なメールが着信した際の社内報告窓口を設置した。 |
| 6 | 2023/6/12<br>(先期分) | 届出者（企業）が管理するパソコンに運送会社を装ったメールが着信した。そのメールに添付されていた Office ファイルを開いたところ、パソコンの再起動を指示する内容のポップアップが表示された。その指示に従って再起動をした結果、パソコンが正常に起動しない状態となった。外部業者に調査を依頼したところ、Office ファイル内のマクロが実行されたことで、当該パソコン内のシステムファイルに不具合が発生するようになっていたことが判明した。再発防止策として、本事象と不審メールに関しての注意喚起を行ったほか、Office ファイルのマクロ機能を無効化する設定を実施するよう周知した。 |

| | | |
|---|---|---|
| 7 | 2023/7/24 | 届出者（企業）が利用する外部サービスから不審な通知が配信されているとの連絡が当該サービスの提供業者よりあった。調査の結果、届出者が利用する当該サービスのシステムに攻撃者が不正アクセスしたことで、不正な通知が送信されたほか、システム上のデータが不正に改ざんされていることも判明した。不正アクセスの原因については、届出者の従業員のパソコンに偽の連絡メールが届き、従業員がそのメールの本文中に記載された URL にアクセスしたことで、ウイルスがダウンロードされ、パソコンがウイルス感染したものと推測している。対応として、感染したパソコンの隔離や当該サービスの機能を停止した上で、パスワードの変更などを行った。再発防止策として、EDR やウェブフィルタリングツールの導入などを実施した。 |
| 8 | 2023/8/4 | 届出者（企業）が利用するインターネット広告配信サービスのアカウントがログイン不可の状態になった。調査の結果、当該アカウントが攻撃者に乗っ取られたことで、不正な広告の配信に悪用されていることが判明した。また、不正な広告の配信費用として、数百万円に及ぶ金銭的被害も発生した。乗っ取りの原因については、パソコンがウイルスに感染したことで、攻撃者に認証情報を窃取されたものと推測しているが、特定には至っていない。対応としては、当該サービスにアクセスしていたパソコンの使用停止及び初期化を行った上で、広告配信サービスの提供会社にアカウントの復旧依頼と広告配信費用の返金交渉を行った。その結果、アカウントの復旧はできなかったが、一部返金が行われた。再発防止策として、本事象を社内に共有するとともに、パスワードの管理方法などを含めた社内の情報セキュリティルールの見直しなどを実施した。 |

## 4-2. 身代金を要求するサイバー攻撃の被害

表 4-3 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 ランサムウェアに関する届出の一覧を示す。

**表 4-3 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 |
|---|---|---|
| 9 | 2023/5/18<br>(先期分) | 届出者（公共機関）において、プリンタから印刷物が大量に出力されることや、ファイルサーバ上のファイルが開けなくなるといった事象を確認した。調査の結果、ファイルサーバや Active Directory サーバなどを含む、複数の機器がファイルの暗号化の被害を受けていることが判明した。また、攻撃者が残したとみられる脅迫文と暗号化されたファイルの拡張子から、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、導入していた VPN 装置（FortiGate）を経由して、組織内のネットワークに侵入されたものと推測している。感染が拡大した原因については、Active Directory サーバが侵害されたことで、複数の機器に感染が広がったものと推測している。そのほか、ログ管理や認証情報の管理にも不備があったことも確認された。対応として、暗号化被害を受けた機器の初期化を行った上で、外部業者にも調査を依頼した。なお、データの復旧には至っていない。再発防止策としては、VPN 装置の入替えとファームウェアの最新化、バックアップサーバの運用見直しなどを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 10 | 2023/6/12<br>(先期分) | 届出者（企業）が利用する監視システムにおいて、監視対象としていた機器との通信が切断され、ネットワークが不通となったことを確認した。調査の結果、仮想環境上のパソコンを含む数十台の機器が暗号化されていることが判明した。攻撃者が残したとみられる脅迫文と暗号化されたファイルの拡張子から、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について特定には至っていないものの、リモートデスクトップによる不正アクセスが確認された。対応として、ネットワークを遮断した上で、修正プログラムの適用やセキュリティソフトの最新化、パスワードの変更などを行った。暗号化の被害を受けた機器についてはバックアップから復旧させた。再発防止策としては、EDR の導入のほか、アクセス制限の見直しなどを実施した。 |
| 11 | 2023/6/25<br>(先期分) | 届出者（企業）が利用する複数の機器がランサムウェアに感染した。攻撃者が残したとみられる脅迫文と暗号化されたファイルの拡張子から、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。侵入の原因として、VPN 装置の管理者アカウントに対するアクセス試行のログが残っていたことから、パスワードリスト攻撃などの方法で認証を突破されたものと推測される。侵害が拡大した原因として、Active Direcorty サーバが侵害されたことで、複数の機器に感染が拡大したものと推測している。対応として、暗号化被害を受けた機器の初期化を行った。再発防止策としては、アカウント管理やバックアップ管理方法の見直し、EDR などの導入のほか、VPN 装置における多要素認証の導入を検討している。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 12 | 2023/7/3 | 届出者（企業）が利用する販売管理システムがログインできない状態にあることを確認した。調査の結果、販売管理システムのサーバを含む複数の機器が LockBit により暗号化されていることが判明した。侵入の原因や感染拡大の原因について特定には至っていないが、VPN 装置（FortiGate）からリモートデスクトップ接続が行われたことを示すログが確認されたほか、販売管理システムのサーバ上では、ネットワークスキャンツールなどの不正ファイルの存在が確認されたとしている。対応として、全機器のパスワード変更などを行った。再発防止策として、VPN 装置に多要素認証を導入したほか、ログ管理やバックアップ管理方法の見直しなどを実施した。 |
| 13 | 2023/7/7 | 届出者（企業）が利用するセキュリティソフトがサーバの異常を検知した。調査の結果、当該サーバが利用できない状態となり、画面上には LockBit のものとみられる脅迫文が表示されていることが判明した。侵入の原因は、VPN 装置（FortiGate）を経由して、組織内のネットワーク内に侵入されてしまったものと推測している。感染拡大の原因は、一部セキュリティソフトを導入していない機器が存在していたことで、攻撃の検知や拡大を防ぐための仕組みが不足していたためと推測している。対応として、ネットワークを遮断した上で、外部業者にフォレンジック調査を依頼した。暗号化の被害を受けた機器については、初期化による再構築やバックアップからの復旧を行った。再発防止策として、VPN 装置の接続時に用いる各ユーザのパスワード変更や IP アドレス制限を行ったほか、監視体制の強化なども実施するとしている。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 14 | 2023/8/30 | 届出者（企業）が利用するセキュリティソフトが異常を検知し、複数の機器がネットワークから隔離された。また、業務システムが起動しない事象も確認した。調査の結果、サーバやパソコンなど数百台以上の機器が LockBit3.0 に感染し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ないが、海外子会社のネットワークから侵入されたものと推測している。感染拡大の原因は、Active Direcorty サーバに対して総当たり攻撃が行われたことで、乗っ取られた可能性があると推定している。また、ファイルサーバや NAS のファイル共有機能も悪用されていたことも確認した。対応として、当該子会社とのネットワーク遮断をした上で、セキュリティの専門業者に対応を依頼した。暗号化の被害を受けた機器については、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。再発防止策としては、パスワードポリシーの厳格化を行ったほか、監視やネットワークセキュリティの強化、アクセス制限やログ管理の見直し、従業員に対するセキュリティ教育などを実施した。 |

表 4-4 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、その他のランサムウェアに関する届出の一覧を示す。

**表 4-4 その他の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 |
|---|---|---|
| 15 | 2023/2/3<br>(先期分) | 届出者（企業）が利用する開発用のデータベースサーバにおいて、操作中にエラーが発生するとの報告があった。調査の結果、当該サーバ上の全データが削除され、金銭を要求する旨の脅迫文が残されていることが判明した。侵入の原因は、インターネットからデータベースを管理するツール（phpMyAdmin）の管理画面にアクセス可能な状態にあったこと。また、当該サーバのパスワードがデフォルトのものであったことから、外部から攻撃者に不正ログインされ、サーバ上のデータを削除されたものと推測される。対応として、当該サーバを停止し、アクセス制限を行った。再発防止策としては、全サーバから当該ツールを削除した。また、システム構成やアクセス制限の見直しを行ったほか、監視ツールの導入などを実施した。 |
| 16 | 2023/4/8<br>(先期分) | 届出者（企業）が利用するファイルサーバにおいて、サーバ上のファイルの拡張子が変更されたことに加え、攻撃者のものとみられる脅迫文が残されていることも確認された。なお、侵入の原因などについては届出時点で調査中であり、詳細については不明である。再発防止策としては、今後、被害発生時以上のセキュリティ強化を行う予定である。 |
| 17 | 2023/5/8<br>(先期分) | 届出者（企業）が利用する NAS にアクセスができないと社内から問い合わせがあった。調査した結果、NAS 上のファイルの拡張子が改ざんされ、攻撃者のものとみられる脅迫文が残されていることが確認された。攻撃内容から、IceFire 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。侵入の原因について特定には至っていないが、NAS の OS を更新していなかったため、何らかの脆弱性を悪用された可能性があると推測している。対応として、NAS をネットワークから遮断した上で、NAS にアクセス可能なパソコン等のウイルススキャンを行った。なお、届出時点では、暗号化されたデータの復旧には至っていない。再発防止策として、NAS の利用を止める判断をした。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 18 | 2023/5/9<br>(先期分) | 届出者（企業）が利用するファイルサーバがシャットダウンされ、アクセスできない状態となった。調査した結果、当該サーバを含む複数台のサーバが暗号化されていることが判明した。暗号化されたファイルの拡張子や攻撃者のものとみられる脅迫文の特徴から、Phobos と呼ばれるランサムウェアの亜種に感染したものと推定される。侵入の原因については、サポートが切れた OS の脆弱性を悪用するなどの方法で、ネットワーク内に侵入されたと推測している。また、感染拡大の原因としては、何らかの方法で認証情報が窃取されたのち、リモートデスクトッププロトコルやファイル共有機能を悪用されたものと推測している。対応として、ネットワーク遮断を行った上で、外部業者にフォレンジック調査も依頼した。再発防止策としては、情報資産の管理や脆弱性の管理方法などについて見直した。 |
| 19 | 2023/5/9<br>(先期分) | 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、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。攻撃の内容から、ランサムウェアの被害を受けたものと見られるが、詳細については不明である。また、侵入の原因についても不明であるが、UTM のログから感染源とみられるパソコン２台を特定したため、それらのパソコンの初期化を行った。暗号化されたファイルについては、バックアップから復旧させた。再発防止策としては、標的型メール訓練サービスやメールセキュリティ、クラウドバックアップの導入のほか、既存のセキュリティソフトにおいて、ランサムウェア対策に関する設定の見直しを実施した。 |
| 20 | 2023/5/15<br>(先期分) | 届出者（企業）が利用する EDR サービスでウイルス感染が検知された。調査の結果、組織内の全サーバのファイルが暗号化されていることが判明した。暗号化されたファイルの拡張子から Phobos 亜種に感染したものと推定される。なお、侵入の原因や感染拡大の原因は調査中であり、詳細については不明である。また、届出時点で復旧には至っていない。再発防止策として、全パソコンに対して EDR ソフトウェアを導入したほか、バックアップ方法の見直しなどを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 21 | 2023/5/24<br>(先期分) | 届出者（企業）が運用するウェブシステムがアクセス不可の状態にあることを発見した。外部業者に調査を依頼したところ、ウェブサーバ内のデータが全て暗号化されていることが判明した。暗号化されたファイルの拡張子や脅迫文の特徴から、Dharma と呼ばれるランサムウェアの亜種に感染したものと推定される。なお、侵入の原因について特定には至っていない。対応として、サーバ内にあるソフトウェアを再インストールするなどの対応を行った。再発防止策としては、外部業者が提供するセキュリティツールを導入したほか、アクセス制限の見直しなどを実施した。 |
| 22 | 2023/6/8<br>(先期分) | 届出者（企業）が利用するサーバにおいて、不正な拡張子が付与されたファイルを多数発見した。調査の結果、バックアップサーバを含む複数の機器が同様の被害を受けていることが判明した。攻撃の内容から、何らかのランサムウェアに感染したものとみられるが、詳細は不明である。侵入の原因は、当該サーバのイベントログにおいて、VPN 装置（FortiGate）経由でリモートデスクトップ接続を試みたログが存在し、かつ様々なユーザ名を用いて不正ログインを試みようとしていたことから、辞書攻撃などの方法で認証を突破されたものと推測される。感染拡大の原因としては、当該サーバのバックアップを RPS（Recovery Point Server）経由でバックアップサーバに接続可能な設定であったためと推測している。対応として、各サーバや VPN 装置などで使用していたパスワードを全て変更したほか、VPN 接続を国内のみに制限するなどの対応を行った。再発防止策としては、VPN 装置における多要素認証の導入やバックアップの強化方法を検討している。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 23 | 2023/6/30<br>(先期分) | 届出者（企業）の従業員がパソコンを起動したところ、多数の不正な拡張子が付与されたファイルが発見された。調査した結果、当該パソコンを含む複数の機器が同様の被害を受けていることが判明した。拡張子の特徴から、Dharma 亜種に感染したものと推定される。侵入の原因は届出時点で調査中であるが、不審なメールの添付ファイルを開いてしまった、あるいは VPN 装置の設定不備などを悪用された可能性があると推測している。対応として、被害を受けた機器をネットワークから隔離した。届出時点では、復旧には至っておらず、調査や再発防止策の検討が進められている。 |
| 24 | 2023/7/6 | 届出者（一般団体）が利用するサーバに異常が発生し、サーバ上のファイルが開けない状態にあることを発見した。調査の結果、Active Directory サーバを含む複数のサーバ内のファイルが暗号化され、画面上に身代金を要求する旨の脅迫文が表示されていることを確認した。拡張子の内容から、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。なお、侵入の原因や侵害拡大の原因について特定には至っていない。対応として、ネットワークを遮断した上で、ウイルススキャンやサーバの再構築などを行った。再発防止策としては、セキュリティソフトや EDR、SOC を含むパッケージサービスの導入のほか、システム構成やバックアップ環境の見直しなどを実施した。 |
| 25 | 2023/7/13 | 届出者（企業）の海外グループ企業が利用するファイルサーバとアプリケーションサーバの複数台がランサムウェアによる暗号化の被害を受けた。調査の結果、侵入の原因は、VPN 装置を利用するアカウントの認証情報が窃取され、組織内ネットワークに侵入されたと推測している。その後、何らかの方法で仮想基盤の管理者権限を乗っ取り、感染を広げたものとみられる。復旧対応と併せて、フォレンジック調査を進めている。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 26 | 2023/7/14 | 届出者（企業）が保有するパソコンに外付けしていた SSD 上のファイルが暗号化され、拡張子が変更されていることを発見した。ファイルの拡張子や脅迫文などから、GAZP というランサムウェアに感染したものと推定している。原因については、フリーソフトをインターネットからダウンロードし、インストールしたことで感染したものと推測している。対応として、感染したパソコンを初期化し、バックアップが存在するデータはそれを用いて復旧させた。再発防止策としては、セキュリティソフトを導入し、最新のバージョンに保つようにした。 |
| 27 | 2023/7/21 | 届出者（企業）が保有するファイルサーバ上のセキュリティソフトからアラートが発出していることを従業員が発見した。当該サーバを確認したところ、サーバ上に保存されていたファイルの拡張子が変更されていることを確認した。調査の結果、ファイルサーバのバックアップ用サーバも同様の被害を受け、各サーバの全データが暗号化されていることが判明した。被害状況から、Lucky と呼ばれるランサムウェアに感染したものと推定される。なお、感染経路を特定できる痕跡は発見されず、感染原因は不明であった。対応として、組織内の全パソコンのウイルスチェックを行った。また、暗号化されたデータの復元には至らなかったため、感染したサーバは初期化し、新規に構築し直した。再発防止策として、UTM の導入を実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 28 | 2023/7/22 | 届出者（企業）の従業員がメールシステムの異常を発見した。メールサーバを確認したところ、当該サーバ上に閲覧できない不審なフォルダが作成されていたことに加え、攻撃者が残したと見られる脅迫文が画面に表示されていた。調査したところ、当該サーバ上のファイルも暗号化されており、そのファイルの拡張子や脅迫文から、Dharma 亜種の攻撃を受けたものと推定される。侵入原因の特定には至ってはいないが、感染拡大の原因については、各サーバ間でリモート接続が可能であったこと、また、サーバ間で同一の ID とパスワードを使用していたためと推測している。対応として、VPN 装置を切断した上で、管理者パスワードの変更などを行った。また、感染したサーバについては、バックアップからの復元や初期化による再構築を行った。再発防止策としては、VPN 装置の二要素認証の導入などを検討している。 |
| 29 | 2023/8/4 | 届出者（企業）がレンタルサーバ上に構築していた顧客向けのシステムにおいて、顧客からアプリケーションの起動に失敗する旨の連絡があった。調査の結果、SQL 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。暗号化されたファイルの拡張子や攻撃者が残したとみられる脅迫文から、Mallox 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。侵入の原因については、特定には至っていないものの、FTP サーバ経由で侵入された可能性があると推測している。対応として、FTP サーバのポートを変更し、感染したサーバについては初期化を行った。再発防止策としては、レンタルサーバの契約を見直し、拠点間 VPN の構築を行った上で、SQL サーバの再構築を実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 30 | 2023/8/7 | 届出者（企業）の従業員がファイルサーバのフォルダを開いたところ、ファイルの拡張子が変更されていることを確認した。ファイルの拡張子や攻撃者が残したとみられる脅迫文から、Phobos 亜種に感染したものと推定される。侵入の原因については不明である。対応として、サーバの OS を再インストールした上で、バックアップからリストアした。また、利用していたファイルサーバに関するサービスの見直しも行った。再発防止策については、今後検討・対策を実施する予定としている。 |
| 31 | 2023/8/10 | 届出者（企業）が利用するサーバがアクセスできない状態にあることを確認した。調査の結果、複数のサーバがランサムウェアによる暗号化の被害を受けていることが判明した。なお、ランサムウェアの名称や侵入の原因については不明である。対応として、ウイルススキャンや各サーバの OS・ソフトウェアのアップデートなどを行った上、外部業者にもフォレンジック調査を依頼した。また、暗号化の被害を受けたサーバについては、再構築する措置を取った。再発防止策としては、アクセス制限や脆弱性管理の見直しなどを実施した。 |
| 32 | 2023/8/25 | 届出者（企業）が利用するネットワーク監視ソフトウェアにて、ファイルサーバのシステム障害を示すアラートが上がった。その調査の過程で、ファイルサーバ内に脅迫文が残されていることを発見した。その後の調査の結果、Active Directory サーバを含む複数台のサーバが暗号化の被害を受けていることが判明した。攻撃の内容から、Mallox の攻撃を受けたものと推定される。社内ネットワークの侵入の原因は、VPN 装置（FortiGate）の脆弱性（CVE-2023-27997）を悪用されたものとみられ、侵入後は、Active Directory サーバを侵害されたことで、各サーバに感染が拡大したものとみられる。対応として、フォレンジック調査などを行った。また、暗号化の被害を受けたサーバについては、OS のクリーンインストールを行い、データの安全を確認してから再構築を行った。再発防止策として、侵入原因となった VPN 装置を廃止した上で、社内ネットワークの再設計を行った。また、サーバ及びクライアント端末全台に EDR の導入を実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 33 | 2023/9/4 | 届出者（地方自治体）の業務委託先の従業員がファイルサーバにアクセスしたところ、アクセス不可の状態にあることを発見した。調査の結果、サーバ内に保存されていた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。なお、侵入の原因については特定には至っていない。対応として、外部業者にフォレンジック調査を依頼した。また、暗号化の被害を受けた機器については初期化を行った。再発防止策として、組織内のネットワーク環境やバックアップの体制、外部業者との連携も含めた保守体制の見直しなどを実施する予定としている。 |
| 34 | 2023/9/4 | 届出者（企業）が利用する機器において、見知らぬアプリケーションが起動しており、また、デスクトップ上にあったファイルの拡張子が改ざんされていることを確認した。攻撃の内容から、Dharma 亜種に感染したものと推定される。侵入の原因について特定には至っていないが、メンテナンス用に開けていたポートから、リモートデスクトッププロトコルで侵入された可能性があると推測している。対応として、ネットワーク上の全機器を停止後、当該機器を隔離した。暗号化されたデータは復旧には至っていない。再発防止策としては、ネットワーク管理方法の見直しを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 35 | 2023/10/12 | 届出者（企業）が導入していたセキュリティソフトからアラートメールの通知を確認した。通知内容より、該当するサーバを確認したところ、画面上に英語のメッセージが表示されていることを発見した。調査の結果、複数台のサーバが暗号化され、ファイルの拡張子に「.rocklee」の文字列が付与されていることが判明した。さらに、不正なプログラムがサーバ内にインストールされていたほか、ログが削除されていることも確認された。侵入の原因は、検証用として構築していたサーバにおいて、アクセスポリシーやプロトコルポリシーに関する設定不備があり、それを悪用されたものと推測している。侵害拡大の原因は、被害を受けた複数のサーバにセキュリティソフトを導入しておらず、何らかの方法で窃取された認証情報を用いたリモートデスクトップ接続が行われたことで、被害が拡大したものと推測している。対応として、社内ネットワークを遮断した上で、設定不備を修正し、全てのサーバに対して、管理者アカウントの認証情報を変更するなどの措置を取った。再発防止策としては、セキュリティソフトの導入及び最新化、アカウント管理やネットワーク構成の見直しを行ったほか、VPN 接続時における多要素認証を導入した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 36 | 2023/11/21 | 届出者（企業）の海外グループ会社から、委託先の組織が不正アクセスを受け、情報が流出した可能性がある旨の報告があった。当該委託先にて調査が行われた結果、不正アクセスされた複数のシステムに、不正なツールがインストールされており、そのツールを介して、個人情報等が窃取された可能性があること、また、その情報の公開と引き換えに金銭を要求されていることが確認された。なお、ファイルの暗号化は確認されなかった。侵入の原因は、利用していた VPN 装置の認証を何らかの方法で通り抜けたのち、リモートデスクトッププロトコルを悪用されたことで、複数のシステムに侵害が拡大したものと推測される。委託先の対応として、リモートアクセス機能の無効化、管理者アカウントのパスワードの再設定、全パソコンのウイルススキャンなどが行われた。届出者の再発防止策としては、営業時間外にインシデント報告があった場合でも速やかに対応できるように CSIRT の体制を整備した。 |
| 37 | 2023/12/1 | 届出者（企業）が利用する EDR の提供業者から、不審なアクセスを検知した旨の報告があった。調査の結果、海外拠点に設置していた VPN 装置を起点として、複数拠点の Active Directory サーバが侵害され、個人情報を含むデータを攻撃者に窃取されていたことが判明した。侵入の原因について、当該 VPN 装置のファームウェアが古く、多要素認証も未適用であったことから、それを突かれたものと推測している。また、Active Directory サーバが侵害された原因として、強度の低いパスワードが設定されていたため、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、不正アクセスされた疑いのある Active Directory サーバの隔離や全パスワードの変更、VPN 装置のファームウェアを最新にするなどの対応を行った。再発防止策については検討中である。 |

## 4-3. 脆弱性や設定不備を悪用された不正アクセス

表4-5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、CMSの脆弱性悪用に関する届出の一覧を示す（EC サイトの脆弱性が悪用された事例は除く）。

**表 4-5 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 |
|---|---|---|
| 38 | 2023/4/6<br>(先期分) | 届出者（企業）が運用するウェブサイトにおいて、ホームページ内のコンテンツが閲覧できない状態にあることを確認した。原因は、利用していた CMS（WordPress）の脆弱性を悪用されたと推測しているが、その詳細については不明である。対応として、当該 CMS を全削除した上で、最新バージョンで再構築を行った。 |
| 39 | 2023/4/24<br>(先期分) | 届出者（企業）が利用しているウェブサーバのインフラサービス提供業者から、不正アクセスを受けている可能性がある旨の連絡があった。調査の結果、ホームページが改ざんされ、当該サーバ上にフィッシングサイトへ誘導することを目的とした、複数の不正なファイルが置かれていることが判明した。原因は、利用していた CMS（Movable Type）の脆弱性（CVE-2021-20837）を悪用されたものと推測している。対応として、ホームページの機能を停止するとともに、脆弱性の悪用に使われたファイルのアクセス権限を変更するなどの対応を行った。再発防止策として、セキュリティチェック診断を行ったほか、保守委託先とのメンテナンスやアップデート対応に関する保守契約の見直しなどを実施した。 |
| 40 | 2023/4/24<br>(先期分) | 届出者（企業）のウェブサイトが、外部の別サイトへリダイレクトされる状態にあることを発見した。ウェブサーバを確認したところ、大量の不正な PHP ファイルが置かれていることが判明した。原因は、利用していた CMS（WordPress）の脆弱性（CVE-2021-21703）を悪用された可能性があると推測している。対応として、不正ファイルを削除した上で、サーバや WordPress などのパスワード変更を行った。再発防止策として、FTP 接続の IP アドレス制限やセキュリティプラグインの導入などを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 41 | 2023/4/25<br>(先期分) | 届出者（企業）の関連会社が保有するウェブサイトにおいて、通常とは異なる画面が表示されると顧客から問い合わせがあった。調査の結果、利用していた CMS（Movable Type）の脆弱性（CVE-2021-20837）を悪用され、不正なスクリプトを埋め込まれていたことが判明した。これにより、当該ウェブサイトにアクセスすると、不審な URL が表示されるようになっていた。対応として、ウェブサイトを停止した上で、ウェブサーバ上のデータを削除、バックアップから復旧させるとともに、CMS の提供元が公開している脆弱性の回避策も実施した。再発防止策として、ウェブサーバや CMS に対するアクセス制限や脆弱性の管理、ログ管理方法についての見直しなどを実施するとしている。 |
| 42 | 2023/5/26<br>(先期分) | 届出者（企業）のグループ会社のウェブサイトが改ざんされたことを改ざん検知システムが検知した。保守委託先の従業員が確認したところ、当該サイトのトップページに大量の隠しリンクが埋め込まれており、画面をクリックすると、外部の不審なウェブサイトに誘導されることが判明した。原因は、CMS（Movable Type）に存在していた何らかの脆弱性が悪用されたものと推測している。また、脆弱性が残存していた原因について、届出者のグループ会社が利用するウェブサーバ環境が、DBMS（Database Management System）の切り替え作業を容易にできない状態にあり、脆弱性対応が適切に実施できていなかったことが要因であった。対応として、ウェブサイトを停止し、バックアップから復旧させた。再発防止策としては、CMS の管理下にあるフォルダのアクセス権限を見直した。さらに、OS やミドルウェアなどについて、定期的なソフトウェア更新の実施を検討している。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 43 | 2023/6/13<br>(先期分) | 届出者（企業）のウェブサイトにアクセスすると、海外の不審な通販サイトに誘導されるとの連絡が顧客からあった。調査の結果、サーバ内に不正なファイルが設置され、そのファイルを介して、ウェブサイトの改ざんが行われていたことが判明した。原因は、ウェブサーバや CMS（WordPress）などに存在していた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、外部業者に修復依頼し、バックアップからウェブサイトを復旧させるとともに、ウェブサーバなどのアップデート対応も行った。再発防止策としては、ファイアウォールの設定見直しなどを実施した。 |
| 44 | 2023/8/9 | 届出者（企業）が管理するウェブシステム上にフィッシングサイトが存在しているとの連絡が、外部組織よりあった。調査の結果、当該ウェブシステムに不正アクセスが確認され、ウェブサーバ上に複数の不正なファイルが置かれていることが判明した。また、その不正ファイルには、フィッシングメールなどで入力されたデータを受信する機能が備わっていた。不正アクセスの原因は、ウェブサーバで利用していた CMS（WordPress）の何らかの脆弱性を悪用されたものとみられるが、詳細は不明である。対応として、外部の専門業者に対応を依頼し、不正ファイルの削除などを行った。再発防止策としては、CMS やそのプラグインのバージョンを最新に保つ運用に見直した。 |
| 45 | 2023/8/16 | 届出者（企業）が運用するウェブサーバのインフラサービス提供業者より、海外のメールアドレスに向けた大量のメール送信が確認されたとの連絡があった。調査の結果、当該ウェブサーバに不正アクセスが確認され、サーバ内に不正ファイルの設置やファイルの改ざんが行われていたことが判明した。原因は、利用していた CMS（WordPress）の脆弱性を悪用されたものと推測している。対応として、外部業者に復旧作業を依頼し、不正ファイルの削除や改ざんされたファイルの修復のほか、CMS やプラグインの最新化などを行った。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 46 | 2023/8/24 | 届出者（医療機関）が運用するウェブサイトにおいて、表示の遅延や一部サイトの閲覧不可が発生していることを確認した。調査の結果、ウェブサーバへの不正アクセスによる、ファイルの改ざんが行われたことが判明した。また、攻撃者は、当該ウェブサーバを踏み台に他のウェブサイトへ攻撃を仕掛けるための不正ファイルの設置を試みたが失敗しており、当該ファイルは動作不可能な状態にあったことが確認された。不正アクセスの原因は、CMS（WordPress）に存在していた XML-RPC の脆弱性、あるいは導入していたプラグインを悪用さ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などを全て削除し、CMS のプラグインのアップデートなどを行った上で、ウェブサイトを復旧させた。再発防止策としては、使用していないプラグインの無効化や CMS の管理画面に対する接続元 IP アドレスの制限などを行ったほか、サーバの契約内容の見直しも実施した。 |

表 4-6 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、EC サイトの脆弱性悪用に関する届出の一覧を示す。

**表 4-6 EC サイト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 | 2023/8/8 | 届出者（企業）が運用する EC サイトが改ざんされ、不審なスクリプトが設置された可能性があると外部機関より連絡があった。確認したところ、当該 EC サイトで利用していた JavaScript ファイルが改ざんされていることが判明したため、ファイルを元に戻し、ファイルの権限の見直しなどを行った。しかしながら、再び攻撃が確認されたため、更なる権限の見直しや脆弱性対策に関する外部サービスの導入を行った。その後、決済代行会社からの連絡があり、調査した結果、当該 EC サイトを利用した顧客のクレジットカード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 サイトで利用していた CMS（EC-CUBE）の脆弱性を悪用されたものと推測している。対応として、当該 EC サイトを停止した。再発防止策としては、アクセス制限の見直しのほか、サーバ管理を自社管理から ASP（Application Service Provider）のサービス上での管理に変更するとともに、PCIDSS に準拠したセキュリティ対策の実施を予定している。 |
| 48 | 2023/8/21 | 届出者（地方自治体）が運用するウェブサイトについて、クレジットカード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。調査の結果、当該ウェブサイトを利用した数千人分の個人情報が漏えいした可能性があり、そのうちの数百人については、カード情報も漏えいした可能性があることが判明した。原因は、当該ウェブ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悪用であった。攻撃者は当該脆弱性を起点として、ウェブサーバ上に不正なファイルを設置していたことが判明した。対応として、ウェブサイトの運用保守委託業者および第三者機関による調査を行った。再発防止策としては、ウェブサイトの管理体制や外部委託先の選定基準の見直しを行ったほか、WAF やウェブサイトの改ざんを検知するシステムの導入、さらに、定期的な脆弱性診断の実施やログ管理ポリシーの厳格化を行う予定。 |

表 4-7 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、SQL インジェクション攻撃に関する届出の一覧を示す。

**表 4-7 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 |
|---|---|---|
| 49 | 2023/5/31<br>(先期分) | 届出者（企業）のウェブサイトを運営管理している業務委託業者が、夜間のバッチ作業中に発生した遅延について確認をしたところ、不正アクセスが行われた痕跡を発見した。調査の結果、当該ウェブサイトに登録されたメールアドレス数万件が流出した可能性があることが判明した。原因は、当該ウェブサイトに存在していた SQL インジェクションの脆弱性を悪用されたものと推測している。また、当該ウェブサイトの通信経路上には WAF が設置されていたが、被害発生前の故障により、動作不良の状態となっていた。対応としては、ウェブサイトを停止した上で、脆弱性の修正のほか、セキュリティ対策を行った。再発防止策として、WAF の動作確認や監視体制の再構築を行ったほか、定期的な脆弱性診断の実施、サーバ機器などの定期的な更新計画の策定などを実施した。 |

表 4-8 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 の脆弱性悪用や 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 4-8 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 |
|---|---|---|
| 50 | 2023/5/8<br>(先期分) | 届出者（企業）が利用する VPN 装置（FortiGate）の保守作業を行っていた外部業者が大量のアクセス失敗ログを発見した。調査の結果、当該 VPN 装置に存在していた脆弱性（CVE-2022-40684）を悪用され、不正な VPN ユーザが登録されていることが判明した。なお、それ以外の被害は確認されていない。原因は、当該 VPN 装置のセキュリティ対策に関して、外部業者との保守契約に関する責任分界点が不明瞭であり、対策が不十分な状態になっていた。対応として、不正アクセス元 IP アドレスを遮断した上で、不正に作成された VPN ユーザの削除、VPN 装置のアップデート、設定のリストアなどを行った。再発防止策としては、脆弱性診断の実施や SOC 対応の見直しを行ったほか、外部業者との契約内容を見直し、責任分界点を明確化した。 |
| 51 | 2023/5/17<br>(先期分) | 届出者（企業）が運用するウェブサイトにおいて、不正なソフトウェアが検知されたとの連絡が外部業者からあった。確認したところ、ウェブサイトのトップページと利用していた CMS の管理画面がアクセスできない状態にあることを確認した。調査の結果、ウェブページが改ざんされ、不正なファイルが自動的にダウンロードされるようになっていたことが判明した。原因は、利用していた WAF がデフォルトのオフ設定の状態になっていたこと、また、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となっていたためと推測している。対応として、バックアップを元に改ざんされたファイルを復旧させた。再発防止策としては、よりセキュリティ設定が細かく設定可能なサーバに移行することを検討している。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 52 | 2023/6/14<br>(先期分) | 届出者（企業）が利用する外部のクラウドサービスにアクセスができなくなった。調査の結果、当該サービスの提供業者が導入していた VPN 装置の脆弱性を悪用されたことで、サービスの提供ができない状態になったことが判明した。対応として、サービス提供業者が復旧を行ったが詳細については不明である。再発防止策としては、情報漏えいなどが発生した時に備え、組織内のインシデント体制の見直しや緊急対応用の作業マニュアルの整備を実施した。 |
| 53 | 2023/6/16<br>(先期分) | 届出者（企業）が運用するウェブサイトの問い合わせページに対し、数千件の不審な投稿が行われたことを確認した。また、その投稿の一部には、SQL インジェクション攻撃を意図したと見られるスクリプトが埋め込まれていた。調査した結果、大量の投稿に加え、問合せページや利用していた CMS の管理ページに対する大量のアクセス試行も行われたことで、同一の機器上で稼働していたウェブサーバとメールサーバに遅延が発生したことも確認された。原因の詳細は不明であるものの、問い合わせページにおいて、大量投稿を抑止する仕組みがなかったことが要因と推測している。対応として、攻撃元とみられる IP アドレスからのアクセスをファイアウォールで遮断した。また、ウェブサイトを一時的に停止し、スクリプトによる影響がないことを確認したのち、再公開した。再発防止策としては、問い合わせページに reCAPTCHA を導入するとともに、問い合わせ内容は外部サービス上で管理することにした。また、ウェブサイトは動的サイトから静的サイトに移行する検討をしている。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 54 | 2023/6/20<br>(先期分) | 届出者（企業）の保有する情報が外部に漏えいしている可能性があるとの連絡が外部機関よりあった。調査の結果、社内サーバ内にインストールされていた GoAnywhere MTF の脆弱性（CVE-2023-0669）を悪用されたことで、攻撃者に情報を窃取されていたことが判明した。また、当該ソフトウェアは被害発生時点で使用されずに放置されており、外部からアクセス可能な状態にあったことも確認された。対応として、当該サーバをネットワークから遮断した上で、専門業者にフォレンジック調査を依頼した。その後、外部からのインターネット接続や VPN 接続も遮断した。再発防止策としては、EDR の導入やアクセス制限の見直し、情報資産管理やログ管理の徹底のほか、今後、社内システムなどに対する脆弱性診断を実施する予定としている。 |
| 55 | 2023/7/7 | 届出者（企業）のウェブサイトが閲覧できない状態にあることを保守作業時に確認した。調査の結果、ウェブサーバが不正アクセスを受け、サーバ内にバックドアや複数の不正なファイルが設置されていることが判明した。原因として、ウェブサーバ上に FTP の資格情報を記したファイルが公開状態で保存されており、攻撃者がその情報を元に FTP 接続することで、ウェブサーバに不正ファイルのアップロードを行ったものと推測している。対応として、当該ウェブサイトへのアクセスを遮断し、不正ファイルの隔離や認証情報の変更、バックアップファイルからの復元などを行った。再発防止策として、ウェブサーバや FTP 接続時における IP アドレス制限などを実施した。 |
| 56 | 2023/8/4 | 届出者（企業）が運用を委託しているウェブサイトにおいて、閲覧できない状態にあるとの連絡を委託先業者から受けた。このため、不正アクセスによる情報漏えいの可能性を考慮し、当該ウェブサイトの運用の中止や関係者への連絡などを行った。原因は、委託先業者の設定不備であった。対応については委託先業者が不正アクセス元の遮断などを行った。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 57 | 2023/8/9 | 届出者（企業）の従業員にスパムメールと見られる不審なメールが届いた。メールを調査したところ、届出者が運用管理するAWS 上のウェブサーバ（EC2）から、スパムメールが送信されていることが確認された。調査の結果、ウェブサーバ上に設置された不正なプログラムにより、AWS のメール送信サービス（SES）を悪用したスパムメールの送信が行われたことが判明した。さらに、当該サーバ環境と別のサーバ環境において、メール送信サービスとクラウドストレージサービス（S3）のアクセスキー情報が不正に参照されていたほか、二要素認証やサービスのログイン情報を外部に送信されていたことも判明した。原因は、ウェブサーバにおけるファイルアップロード機能の設定不備やファイルのアクセス権限の設定不備が存在していたためと推測している。対応として、設定ファイルによるスパムメール送信の遮断、改ざんされたファイルの隔離などを行った上で、ウェブサーバを停止し、新規に用意したサーバで再構築を行った。再発防止策としては、ファイルアップロード機能等の設定の見直しのほか、IDS・IPS の導入を実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 58 | 2023/8/31 | 届出者（企業）の従業員が日々のメールチェックをしたところ、自身が使用するメールアカウントから大量の不審メールが送信されていることを確認した。調査の結果、当該メールアカウントが不正アクセスされ、海外のメールアドレス宛に数千件のスパムメールが送信されていたことが判明した。原因は、届出者が利用しているメールサービスの設定が、外部からSMTP ポートに向けたアクセスを可能とするデフォルトの設定となっており、外部から認証試行が行える状態にあったことや、当該メールアカウントで推測されやすいパスワードを設定していたことから、数十回程度のログイン試行で認証を突破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を停止した上で、パスワードの変更を行った。また、外部からメールサーバに向けた、SMTP 通信を全て拒否する設定や、メールサービスのログイン時における IP アドレス制限も行った。再発防止策としては、パスワードポリシーを見直し、組織内で利用している全メールアカウントを対象にパスワード変更を実施した。 |
| 59 | 2023/9/4 | 届出者（企業）が利用するサーバが攻撃を受けた可能性があるとの連絡が外部のセキュリティ機関からあった。調査の結果、導入していたアプリケーションデリバリーコントローラー（Citrix ADC）の脆弱性（CVE-2023-3519）を悪用されたことで、サーバ内に不正なファイルが設置されていることが判明した。なお、不正ファイルの設置以外の被害については確認されなかった。原因として、当該脆弱性の対策は実施済みではあったが、不正ファイルの作成日付がそれ以前であったことから、対策が間に合っていなかったものと推測している。対応として、被害を受けたサーバを隔離し、影響調査で問題がないことを確認した上で再構築を行った。再発防止策としては、ネットワークのアクセスポリシーの見直しなどの実施を予定している。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 60 | 2023/9/7 | 届出者（地方自治体）が運用するメール配信システムにおいて、職員がログインを試みたところ、認証情報が誤っているとのエラーが表示された。システム保守業者に連絡をしたところ、当該システムが不正アクセスされ、認証情報が不正に変更されていることが確認された。調査の結果、認証情報の変更に加え、当該システム上に保存されていた個人情報の数千件分が窃取されていることも判明した。原因については、当該システムで利用していたメール配信ソフト（acmailer）に脆弱性のあるファイルが存在しており、外部の攻撃者がそのファイルに不正アクセスして、認証情報を不正に変更したものと推測している。対応として、当該システム関連のデータを全て削除した。再発防止策としては、よりセキュリティ強度の高いメール配信システムに移行したほか、ウェブサイトなどの保守管理の見直しの実施を予定している。 |
| 61 | 2023/9/21 | 届出者（一般団体）の複数の職員から迷惑メールを受信した旨の連絡があった。調査の結果、届出者が管理するサーバ上のメール配信ソフト（acmailer）を悪用した迷惑メールの送信が行われていたことが判明した。原因は、当該メール配信ソフトに存在していた脆弱性のあるファイルを攻撃者に悪用され、認証情報が変更されてしまったものと推測している。対応として、当該サーバの運用を停止し、新たなサーバへの移行を行った。再発防止策としては、ウェブセキュリティ診断サービスの導入やログ監視の強化のほか、情報管理体制の見直しなども実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 62 | 2023/9/25 | 届出者（教育・研究機関）が運用しているウェブサイトが改ざんされているとの連絡がウェブシステムの提供業者からあった。調査の結果、当該サイトのウェブサーバが不正アクセスされ、サーバ内に不正ファイルの設置やファイルの改ざんが行われていることが確認された。原因として、当該サーバ内に残存していた CMS のセットアップファイルが外部からアクセス可能な状態にあり、そのファイルを攻撃者が不正利用することで、不正ファイルの設置などを行ったものと推測している。対応として、当該サイトを閉鎖する措置を取った。再発防止策としては、よりセキュリティ強度の高い別サーバに移行し、CMS のアカウント管理に関する見直しなども実施した。 |
| 63 | 2023/9/26 | 届出者（企業）が利用するログ監視システムにおいて、外部からの大量のアクセスが検知された。調査の結果、当該システムが不正アクセスされ、複数のログを窃取された可能性のあることが判明した。原因は、ファイアウォールの設定不備により、外部からのアクセスが可能な状態になっていたものと推測している。対応として、原因となったファイアウォールの設定不備を修正し、不正アクセス元からのアクセスを遮断した。再発防止策としては、当該システムのアクセス制限も実施したほか、ログ管理方法の運用見直しなども行った。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 64 | 2023/9/29 | 届出者（教育・研究機関）が利用する CMS の管理画面にログインができないとの連絡があった。アクセスログを確認したところ、不審な IP アドレスからの大量のログイン試行が記録されていることを確認した。調査の結果、CMS に不正アクセスされ、管理者パスワードが変更されていたことが判明した。なお、ウェブサイト改ざんなどの被害は確認されなかった。原因は、ウェブサーバ上に CMS のセットアップファイルが存在しており、また、外部からのアクセスが可能な状態にあったことから、攻撃者が当該ファイルにアクセスし、不正利用することで、パスワードの初期化を行っ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し、ログ調査などを実施した上で、CMS の再インストールとパスワードの再設定を行った。再発防止策としては、CMS の最新化やセットアップファイルの無効化の確認のほか、アクセス制限の見直しや CMS の管理者向けに運用上の注意事項を周知した。 |

## 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 4-9 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 4-9 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 |
|---|---|---|
| 65 | 2023/4/18<br>(先期分) | 届出者（企業）が利用するメールサービスにおいて、一部のメールアカウントから大量のスパムメールが配信されたとの連絡がサービス提供業者よりあった。原因は、当該メールアカウントで脆弱なパスワードを使用していたためと推測している。対応として、サービス提供業者にて強制的にパスワードの変更が行われた。さらに、メールアカウントを利用していた端末上でウイルススキャンを行った。再発防止策としては、全従業員に脆弱なパスワードを変更するよう通知を行うとともに、アクセス制限や認証情報の保護に関する見直しを実施した。 |
| 66 | 2023/4/29<br>(先期分) | 届出者（企業）が利用する社内用のグループウェアにアクセスができない状況になった。調査の結果、グループウェアが稼働するサーバが攻撃者に不正アクセスされ、再インストールを実行されたことにより、サーバ内に保管していたデータが全て消去されていたことが判明した。原因は、当該サーバの管理画面に対する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、管理画面のログインアカウントのパスワード変更を行った。さらに、二段階認証を設定した。再発防止策としては、バックアップ方法の見直しのほか、グループウェアを自社管理から、クラウド型のグループウェアに移行した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 67 | 2023/5/22<br>(先期分) | 届出者（一般団体）が利用するメールシステムにおいて、外部業者からメールアカウントが不正利用されている可能性があるとの連絡があった。調査の結果、メールシステムへの不正ログインにより、数万件の迷惑メールが外部へと送信された可能性があることが判明した。原因は、利用していたパスワードが簡易な文字列、かつ推測されやすいものであったため、総当たり攻撃またはパスワードリストなどの方法で認証が突破されてしまったと推測している。対応として、外部業者にて強制的にパスワードの変更が行われた。再発防止策としては、パスワードをより複雑なものに変更した。 |
| 68 | 2023/6/5<br>(先期分) | 届出者（企業）が日々実施しているログ監視にて、不審なアクセスログを発見した。調査の結果、不正な端末一台から届出者が運営する EC サイトの顧客アカウントに対する不正ログイン試行が行われていることが判明した。また、一部のアカウントについては不正ログインに成功しており、登録されていたメールアドレスが不正に変更されていることも確認された。原因は、パスワードリスト攻撃によるものと推測している。対応として、接続元 IP アドレスの遮断や不正アクセスの監視体制の整備を行った。再発防止策としては、ログイン時における二要素認証機能の導入のほか、不正アクセス対策の見直しなどを検討している。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 69 | 2023/6/6<br>(先期分) | 届出者（企業）のウェブサイト運用を受託している業務委託先が、当該ウェブサイトにアクセスしたところ、外部のサイトにリダイレクトされる状態にあることを発見した。調査の結果、ウェブサイトに対する不正アクセスにより、複数のウェブページが改ざんされていたことが判明した。なお、リダイレクト先のウェブサイトは、届出者とは無関係な EC サイトであった。原因は、CMS（WordPress）のアカウントにおいて、容易に推測可能なパスワードを設定していたためと推測している。対応として、サーバ内の不正ファイルを削除した上で、サーバ内に保存してあったデータを 1 日前のデータに復元した。再発防止策としては、WordPress 管理画面の URL を変更したほか、パスワードの管理方法やアクセス権限の見直しを実施した。 |
| 70 | 2023/6/6<br>(先期分) | 届出者（企業）と海外取引先間のやり取りにおいて、海外取引先から入金に関する連絡があったが、届出者の銀行口座には入金されていないことを確認した。調査の結果、届出者になりすました偽のメールが取引先に送られ、取引先はそのメールの指示に従い、指定の口座へ約数百万円（日本円換算）の送金を行っていたことが判明した。また、届出者のメールサーバを調査した結果、通常とは異なる IP アドレスからのアクセスログも確認された。状況から、ビジネスメール詐欺の被害を受けたものと見られる。原因は、届出者のメールアカウントが不正ログインされ、取引先とのやり取りを攻撃者に盗み見られたのち、偽のメールを送信されたものと推測されるが、詳細については不明である。対応として、当該メールアカウントの隔離と全社員が使用しているパスワードの変更を行った。再発防止策としては、多要素認証の導入を実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 71 | 2023/6/9<br>(先期分) | 届出者（一般団体）が利用するメールサービスの提供業者より、届出者のメールアカウントから数千件の不審なメールが発信されたとの連絡があった。調査の結果、当該サービスのログイン履歴に不審な IP アドレスが記録されていることを確認した。不正アクセスの原因は、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、被害を受けたアカウントとその他のアカウントも含め、パスワード変更を行った。また、使用していたパソコンのウイルス感染の可能性も考慮し、ネットワークの遮断後にウイルススキャンなどを行った。再発防止策としては、メールアカウントのパスワードをより強固なものに変更したほか、担当者にセキュリティ教育を実施した。また、別のメールサービスへの移行を検討している。 |
| 72 | 2023/6/14<br>(先期分) | 届出者（地方自治体）が管理する教育機関から、複数の職員が利用しているクラウドストレージサービスのアカウントが不正アクセスされ、保存していたファイルの共有設定の変更や削除などが行われたとの報告があった。原因は、初回ログイン時にパスワードを変更する運用であったが徹底されておらず、また、初期パスワードも ID から類推可能なものであったためと推測している。また、当該システムの運用において、個人情報が含まれるファイルのアップロードをしないよう定めていたが、守られていなかったことなども判明した。対応として、全アカウントの利用を停止した上で、強制的にパスワードを変更し、当該サービス上に保存すべきでないファイルを削除した。再発防止策としては、パスワードポリシーの見直し、業務上必要なアカウントのみ運用する形とした。また、個人情報の取り扱い基準の策定および周知も実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 73 | 2023/6/22<br>(先期分) | 届出者（企業）が管理するウェブサイトが本来とは異なる内容に書き換えられ、また、ウェブサーバ内には不正なファイルが設置されていることを確認した。原因は、利用していた CMS（WordPress）のログインパスワードが推測されやすいものであったためと推測している。対応として、ウェブサイトを停止した上で、被害を受けたウェブサーバを再構築して復旧させた。再発防止策としては、パスワードポリシーの見直しのほか、新規にセキュリティソフトを導入した。 |
| 74 | 2023/7/5 | 届出者（教育・研究機関）の学生から、メールアカウントに大量の不審なメールが届いたとの連絡があった。調査の結果、当該メールアカウントが乗っ取られ、数百件に及ぶスパムメールが送信されたこと、また、当該学生が閲覧可能なウェブサービス上の情報が漏洩した可能性があることが判明した。原因は、メールアカウントのパスワードを別のウェブサービスで使い回しており、何らかの理由により漏えいしたことで、不正アクセスされたものと推測している。対応として、メールアカウントのパスワード変更やアクセス制限を行った。再発防止策としては、多要素認証の導入などの実施を検討している。 |
| 75 | 2023/7/10 | 届出者（教育・研究機関）に所属する職員のメールアカウントから大量のスパムメール送信が行われた。調査の結果、当該メールアカウントに対する不正ログインの痕跡が確認された。また、個人情報を含んだメールを攻撃者に閲覧された可能性があることやメール送信数の上限に達したことで、メール送信ができなくなっていることも判明した。原因について特定には至っていないが、初回の認証試行でログインに成功していたことから、何らかの理由で認証情報が漏えいしており、それを攻撃者に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を停止した上で、パスワードの変更を行った。さらに、対象のメールサーバに対するアクセス制限も行った。再発防止策としては、パスワードポリシーの見直しなどを実施したほか、今後、メールサーバに侵入防止ソフトウェアの導入や多要素認証等の導入による認証強化の実施を予定している。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 76 | 2023/7/13 | 届出者（教育・研究機関）に所属する職員から、大量のエラーメールが届いているとの連絡があった。調査の結果、当該職員のメールアカウントが不正ログインされ、数千件の迷惑メールが外部に送信されていたことが判明した。不正ログインされた原因の特定には至っていないが、何らかの方法で当該職員の認証情報が流出した可能性があると推測している。対応として、パスワードを変更した上で、メールアカウントの利用も停止した。さらに、利用していた端末のネットワーク遮断なども行った。再発防止策としては、メールシステムへのアクセス制限や接続認証の制限、メール送信数の制限などを実施した。 |
| 77 | 2023/7/14 | 届出者（企業）が契約しているインターネットサービスプロバイダより、届出者の使用する機器がスパムメール送信の踏み台となっている可能性がある旨のメールが届いた。稼働中のサーバなどを確認したところ、ウェブサーバ上で不審なプロセスが動作していることを発見した。調査の結果、ウェブサーバへの不正アクセスにより、サーバ上に WebShell を設置され、それを利用してメールの不正送信が行われていたことが判明した。なお、攻撃は少なくとも 1 ヵ月ほど前から行われていたことも確認された。原因は、CMS（WordPress）の管理者アカウントに設定していたパスワードが単純なものであったこと、また、外部から管理画面に対してのアクセスが許可された状態であったため、CMS の管理画面に対する総当たり攻撃により、認証を突破されたものと推測される。対応として、当該サーバをネットワークから遮断した上で、不審なプロセスの停止などを行い、その後、外部の専門機関によるフォレンジック調査を実施した。再発防止策としては、認証情報を強固なものに再設定し、管理画面へのアクセス制限を行ったほか、WordPress のセキュリティプラグインを導入した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 78 | 2023/7/26 | 届出者（教育・研究機関）に所属する職員から、メールの送受信ができないとの連絡が複数寄せられた。調査の結果、複数あるメールサーバのうちの一つから、基幹メールサーバを経由し、数百万件にも及ぶ迷惑メールが送信されていることが確認された。さらに、基幹メールサーバが、外部組織が管理するメールブラックリストに登録されてしまっていることも判明した。原因は、当該メールサーバに登録されていたメールアカウントにおいて、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、当該メールサーバの運用を停止し、ブラックリストの管理元に登録の解除申請などを行った。再発防止策としては、メールサーバのセキュリティ対策に関する自己点検の実施ほか、パスワード設定などのアカウント管理に関する注意喚起を実施した。 |
| 79 | 2023/8/7 | 届出者（企業）の従業員が、外部組織向けに提供しているシステムのサーバへログインした際、通常時とは異なる違和感を覚えたため、調査を行ったところ、サーバ内に不審なファイルが設置されていることを発見した。調査の結果、当該サーバ内にバックドアファイルを設置され、そのバックドアファイルを介して、システムを改ざんしていたことが確認された。原因は、インターネット上に公開されていた、当該システムの管理者用ログインサイトに対する総当たり攻撃によって侵入され、当該システムの正規機能であるファイルアップロード機能を悪用し、バックドアファイルを設置したものとみられる。対応として、当該システムを停止し、外部からのアクセスを遮断した上で、パスワードポリシーの見直しやロックアウト機能の導入、ファイルアップロード機能の制限などを行った。再発防止策としては、不正アクセスや改ざんを検知するシステムの導入のほか、ログの収集及び監視の強化、インシデント対応体制の整備や従業員へのセキュリティ教育の強化などを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 80 | 2023/8/8 | 届出者（企業）が利用するインターネット広告配信サービスの提供会社から、規約違反を示すメールが届いた。不審に思った担当者が同サービスの利用状況を確認したところ、管理者権限が付与されたアカウントが攻撃者に乗っ取られ、不正な広告の配信に悪用されていることを発見した。さらに、不正な広告の配信により、広告配信費用として数千万に及ぶ金銭被害が発生していることも確認された。原因は、フィッシング攻撃による認証情報の漏えい、もしくは当該アカウントの ID とパスワードの使い回しによる漏えいと推測している。対応として、別のアカウントにて不正な広告の配信を停止し、乗っ取られたアカウントについては、広告配信サービスの提供会社に削除依頼をした。再発防止策として、社内の運用ルールの見直しを行い、多要素認証の徹底や社内で管理者権限を付与する際の基準の策定、権限を付与する際のリスク説明などを実施することにした。 |
| 81 | 2023/8/28 | 届出者（地方自治体）の職員が、数百件に及ぶ大量のエラーメールを受信していることを発見した。調査の結果、届出者が利用するメールサービス上のアカウントが不正アクセスされ、届出者になりすました不正メールが送信されていたことが判明した。なお、送信されたメールの大半は、送信不能のエラーメールとして届いたとのことだった。不正アクセスの原因は、対象のアカウントのパスワードを何らかの方法で特定されたためと推測している。対応として、対象アカウントのパスワード変更を行った。再発防止として、メールサーバ接続時における IP アドレス制限を実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 82 | 2023/9/6 | 届出者（教育・研究機関）の組織内ネットワークに一時的に設置していた外部事業者の接続用 VPN 装置において、当該装置を介した大量の迷惑メール送信が行われたことを確認した。原因は、システム構築のために外部事業者が設置した当該装置の設定に不備があり、それ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、ネットワークの設定見直しを行った。再発防止策としては、外部事業者が持ち込む機器のセキュリティチェックや使用状況などの報告を義務付けた。その後さらに届出者が管理するメールサーバが不正アクセスされたことによる迷惑メールの送信事案も確認された。対応として、不正アクセスが確認されたメール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、パスワード設定の見直しを行ったほか、多要素認証の導入の実施を検討している。 |
| 83 | 2023/9/7 | 届出者（企業）が利用しているメールアカウントがログインできない状態にあることを発見した。メールサービス提供業者に連絡したところ、当該メールアカウントが乗っ取られ、大量のスパムメールが送信されていることが判明した。原因は、当該メールサービス提供業者を騙る偽のメールが届き、それを受信者が気づかずにメール本文中のリンクにアクセスしたものと推測している。対応として、メールサービス提供業者にてメールアカウントを停止する措置を取った。再発防止策としては、社内周知を行ったほか、メールサービス提供業者との契約内容を見直し、不審なメールをより判別し易くするための設定などを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 84 | 2023/9/15 | 届出者（企業）の従業員が利用するメールアカウントが乗っ取られ、外部に迷惑メールの送信をされていることが判明した。原因は、メールアカウントのパスワードに強度の低いものを設定していたこと、また、外部からメールシステムへの接続が可能な設定していたことによる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外部からのアクセスを遮断した。再発防止策としては、メールアカウントのパスワードポリシーを見直した上で、全従業員のパスワード変更を実施したほか、従業員向けにセキュリティ教育の実施を予定している。 |
| 85 | 2023/9/25 | 届出者（教育・研究機関）が運用しているウェブサーバから迷惑メールが送信されているとの連絡が外部からあった。調査の結果、当該サーバに対する不正アクセスが確認され、不正ファイルの設置やファイルの改ざんが行われていたことが判明した。原因は、当該サーバで利用していた CMS の認証情報が、何らかの方法で攻撃者に窃取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遮断するなどの対応を行った。再発防止策としては、職員や学生向けに、インシデント発生時の対応に関する注意喚起を行ったほか、全職員向けに情報セキュリティに関する研修を実施した。 |
| 86 | 2023/11/8 | 届出者（企業）が管理するメールアドレスを送信元とするフィッシングメールが着信したとの連絡が外部からあった。調査の結果、届出者が利用する複数のメールアカウントが不正アクセスを受け、大量のフィッシングメールを送信していたことが判明した。原因は不明であった。対応として、当該メールアカウントのパスワードを変更するなどの対応を行った |

## 4-5. その他

表 4-10 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 4-10 その他の届出事例の概要一覧**

| 項番 | 届出日 | 概要 |
|---|---|---|
| 87 | 2023/4/3<br>(先期分) | 届出者（企業）が運用するウェブサイトが閲覧不可の状態にあるとの連絡が従業員からあった。調査の結果、ウェブサーバ内に不正ファイルが設置され、そのファイルを悪用することで、ウェブサイトの改ざんなどが行われていることが判明した。原因は、ログが残っていなかったため不明であった。対応として、当該サーバへのアクセス制限を行った上で、データの全削除を行った。再発防止策としては、アカウント管理方法の見直しなどを検討している。 |
| 88 | 2023/4/24<br>(先期分) | 届出者（企業）の自社ウェブサイトにアクセスすると、海外の不審なサイトに遷移される状態にあることを発見した。調査の結果、ウェブサーバへの不正アクセスにより、利用していたCMS（WordPress）の認証情報が何らかの方法で変更され、攻撃者にウェブサイトを改ざんされていたことが判明した。なお、不正アクセスの原因について特定には至っていない。対応として、異なるウェブサーバにウェブサイトを移行した。再発防止策としては、使用するパスワードの複雑化などを実施した。 |
| 89 | 2023/5/1<br>(先期分) | 届出者（企業）が利用するメールサーバから不審なメールが送信されているとの連絡がサーバ事業者から連絡があった。調査したところ、数十万件の不審なメールが送信されていることが判明した。メールサーバに侵入された原因については不明である。対応として、メールサーバを停止した上で、サーバ内のデータを削除し、OS の再インストールも行った。再発防止策としては、自組織でのサーバ管理を取りやめ、サービス事業者が提供するメールシステムの利用に移行した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 90 | 2023/5/11<br>(先期分) | 届出者（企業）の従業員が利用するパソコンの画面に、セキュリティ警告が表示されるとともに警告音が鳴った。状況から、偽セキュリティ警告（サポート詐欺）と推定される。当該従業員は画面に表示された電話番号に連絡をしてしまったが、偽の担当者の言葉遣いや指示内容を不審に感じたため、すぐに通話を終了した。その後、パソコンをネットワークから切断した上で、外部の専門業者に対応を依頼した。また、パソコンに導入していたセキュリティソフトによるウイルススキャンを実施したところ、1 件のトロイの木馬が検知されたため、駆除を行った。再発防止策として、組織内に本事案を周知するとともに、対応マニュアルの整備などの実施を予定している。 |
| 91 | 2023/5/16<br>(先期分) | 届出者（企業）の従業員が使用するパソコンの画面上に、ウイルスに感染したことを示す偽のセキュリティ警告が表示された。 当該従業員が画面に表示された電話番号に架電したところ、サポートデスクを名乗る担当者から、パソコンをリモート操作するソフトウェアをインストールするよう誘導され、ダウンロードしてしまった。また、その担当者から、個人情報の漏えいを止めるための費用として、至急金銭を振り込むよう指示があった。当該従業員は対応内容を不審に思い、社内に報告を行ったことで、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た上で、シャットダウンを行った。その後、外部機関による調査を受け、個人情報の漏えいやウイルスの感染がないことを確認した。再発防止策としては、全従業員にインシデント発生時の対応に関するセキュリティ教育を実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 92 | 2023/5/29<br>(先期分) | 届出者（企業）の従業員が日次作業としている SYSLOG のチェックを行ったところ、インターネット接続に利用するルータから大量の SSH 認証失敗ログが記録されていることを確認した。調査の結果、海外の特定 IP アドレスから、届出者が所有する複数のグローバル IP アドレスに対して、数分間の間に数万件の認証試行が行われていたこと、また、行われた認証試行は全て失敗していたことが確認された。対応として、該当する不正アクセス元 IP アドレスからの TCP 通信を遮断する設定を行った。 |
| 93 | 2023/6/12<br>(先期分) | 届出者（教育・研究機関）に所属する職員から詐欺に遭った疑いがあるとの連絡があった。当該職員が業務で利用するパソコンでニュースサイトと見られるサイトを閲覧していたところ、ウイルス感染を装った警告画面が表示された。記載されていた電話番号に連絡し、指示に従った結果、遠隔操作ツールである AnyDesk をパソコン内にインストールしてしまい、接続用 ID を伝えたことで外部からの操作を受け付ける状態になってしまった。状況から、偽セキュリティ警告（サポート詐欺）を受けたものと見られる。その後、ウイルス感染の対応費用を請求された際に、詐欺ではないかという疑いを持ち、当該パソコンをネットワークから遮断した上で、届出者に連絡を行った。対応として、外部業者に調査を依頼した上で、パソコンの初期化を行った。また、当該人物が使用するアカウントを一時的に停止する措置を取った。再発防止策としては、アカウント管理に関する見直しを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 94 | 2023/6/12<br>(先期分) | 届出者（企業）が運用するウェブサイトの管理画面にアクセスしたところ、担当者が登録した覚えのないユーザが追加されていることを発見した。調査の結果、不正なユーザ情報の登録だけでなく、不正なプラグインのインストール、ウェブページの改ざんによる不正なリンクの埋め込みなどが行われていたことが判明した。原因の特定には至っていない。対応として、不正なプラグインの削除、ウェブサイトで利用していた CMS（WordPress）の再インストールなどを行った。再発防止策としては、管理者アカウントのパスワード変更やセキュリティプラグインの見直し、海外の IP アドレスからの接続を遮断するなどの対応を実施した。 |
| 95 | 2023/6/19<br>(先期分) | 届出者（教育・研究機関）が利用するメールサービスのサービス提供事業者から、学生が使うメールアカウントのメール送信を停止した旨の連絡があった。調査の結果、当該メールアカウントに対する不正アクセスが確認され、当該学生を送信元とする数万件のスパム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については不明である。対応として、当該メールアカウントのパスワード変更を行った。再発防止策としては、学生向けの情報セキュリティ研修の実施や二段階認証の導入を行う予定である。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 96 | 2023/6/28<br>(先期分) | 届出者（教育・研究機関）が提供しているメールサービスのメールアカウントを持つ利用者より、海外からの不審なログイン履歴を発見した旨の報告があった。調査の結果、当該メールアカウントが不正アクセスされたことで、大量のフィッシングメールが送信されていることが判明した。さらに、一部の受信者においては、フィッシングメール内のリンクをクリックしたほか、アカウント情報の入力をしていたことも確認された。不正アクセスされた原因の特定には至っていない。対応として、当該メールアカウントを停止する措置を取った。また、不審メールに関する注意喚起を行い、一部の受信者にはパスワード変更とウイルススキャンを実施するよう案内した。再発防止策としては、メールアカウントを管理するサーバのログ監視を強化するとともに、不正アクセスを確認した際に即座にアカウントをロックする運用とした。 |
| 97 | 2023/6/28<br>(先期分) | 届出者（企業）が運営する EC サイトにおいて、外部の決済代行業者からクレジットマスター攻撃を検知した旨の連絡があった。調査の結果、クレジットカード認証のエラーログが数百件記録されていることが判明した。これを受け、届出者は決済代行業者が提供している攻撃遮断サービスを導入したが、その後、当該サービスを上回る程の大量の攻撃が確認された。原因は、当該 EC サイトにおいて、クレジットカード情報の入力可能な回数に上限を設けていなかったためと推測している。対応として、EC サイトのカード決済を停止した上で、カード決済における試行回数の制限などを設けた。再発防止策としては、3D セキュアと reCAPTCHA を導入した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 98 | 2023/6/29<br>(先期分) | 届出者（地方自治体）が管轄する複数の組織から、メールの送受信が行えない旨の連絡があった。外部業者に調査を依頼した結果、メールサーバにおいて、メールの不正中継が可能な状態にあり、スパムメールの送信に悪用されたこと、また、当該メールサーバが不正なサーバとしてブラックリストに登録されたことで、メールの送受信が行えなくなったことが判明した。原因は、被害発生前に業務委託先が行った、ファイアウォールの通信設定に不備があったためと推測している。対応として、当該の設定不備を修正するとともに、通信先のメールサーバに対してブラックリストの解除申請を行った。再発防止策としては、ログの管理方法などを見直すとともに、業務委託先との連携などに関しても見直しを行う予定である。 |
| 99 | 2023/7/11 | 届出者（企業）のウェブサイトが不正アクセスされ、詐欺サイトの踏み台になっている旨の連絡が第三者からあった。外部業者に確認を依頼したところ、自組織のウェブサイトが表示されずに、他のウェブサイトが表示されるようになっていることが確認された。原因は不明である。対応として、バックアップデータを別のウェブサーバに展開し、ウェブサイトを復旧させた。また、不正アクセスされたサーバのデータは削除した。再発防止策としては、ウェブサイトにアクセスするパソコンのセキュリティソフトの更新やパスワード管理の見直しなどを実施する予定である。 |
| 100 | 2023/8/9 | 届出者（地方自治体）の業務委託先の従業員が利用していたパソコンに、セキュリティ警告画面が表示された。当該従業員は、画面内に表示された電話番号に連絡して、指示どおりにパソコンを操作してしまい、リモート操作ツールをインストールしてしまった。その後の調査の結果、本事案は偽セキュリティ警告（サポート詐欺）であることが判明した。対応として、業務委託先ではインターネットの遮断を行い、届出者は関係者への周知などを行った。再発防止策としては、個人情報の取り扱いに関する見直しなどを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 101 | 2023/8/23 | 届出者（企業）の役員が利用するパソコンにおいて、詐欺画面が表示されたとの報告があった。確認したところ、当該役員は画面に表示された指定の電話番号に連絡してしまい、遠隔操作ツールをダウンロードするよう誘導され、パソコン内にインストールしてしまった。状況から、偽セキュリティ警告（サポート詐欺）と見られる。対応として、外部業者にフォレンジック調査を依頼した。再発防止策としては、詐欺サイトや不審メールに関する注記喚起を実施するとともに、不要ファイルの削除などに関する運用の見直しを実施した。 |
| 102 | 2023/8/23 | 届出者（企業）の従業員が利用するパソコンにおいて、偽セキュリティ警告（サポート詐欺）による事案が発生した。従業員が当該パソコンにて、利用者がウェブサイトを閲覧していたところ、ウイルス感染の警告画面が表示されたので、そこに記載されていた連絡先に電話をした。そこで、偽のオペレータの指示に従いリモート操作ツールをインストールしたあとに、パソコン内のデータが削除されていたことに気づき、また、支払いの指示があったので、不審であると判断。対応として、契約プロバイダに連絡後、電話を切り、パソコンをネットワークから隔離した。再発防止策として、契約プロバイダと協議の上、社内周知を行ったほか、UTM などの導入、データのバックアップ用として NAS の導入も検討している。 |
| 103 | 2023/9/2 | 届出者（企業）のウェブサイトが不正アクセスを受け、サイトの内容が改ざんされているとの連絡がセキュリティベンダーよりあった。連絡内容は、当該ウェブサイトにアクセスすると、偽の通販サイトへ遷移するように不正なスクリプトが埋め込まれていること。また、当該ウェブサイトへのアクセスを遮断したとのことであった。届出者が調査したところ、当該ウェブサイトと同じ URL を持つフィッシングサイトが作成されていることを確認した。原因については不明である。対応として、当該ウェブサイトの公開を停止し、新規にウェブサイトを再構築した。再発防止策としては、よりセキュリティ強度の高いネットワーク機器の導入などを実施した。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 104 | 2023/9/11 | 届出者（企業）が運用するウェブサイトが改ざんされているとの連絡がサーバ提供業者よりあった。調査した結果、当該ウェブサイト上に海外の銀行サイトを模したフィッシングサイトが設置されていることが判明した。原因の特定には至っていない。対応として、当該ウェブサイトの公開を停止し、不正なファイルを削除したのち、安全が確認されたファイルのみを残して再公開を行った。再発防止策としては、パスワードを複雑なものに再設定するとともに、ログイン時の二段階認証の必須化などを実施した。 |
| 105 | 2023/9/12 | 届出者（企業）の従業員が自宅のパソコンを操作していたところ、画面上にパソコンが壊れた旨のメッセージとサポートの電話番号が表示された。その電話番号に連絡し、電話口の相手の指示に従ったところ、パソコンを遠隔操作され、修理代金としてギフトカードで金銭を支払うよう要求された。そのため、購入したギフトカードの番号を伝えたところ、その番号は失効となった、という理由で再度カードを購入するよう要求された。そこで騙されていることに気付き、被害を認識した。状況から偽セキュリティ警告（サポート詐欺）の被害にあったものと推定している。また、被害を受けたパソコンには、当該従業員が業務で使用する顧客情報も保存されており、遠隔操作を受けた際にそれらの情報が不正に窃取された可能性もあることが確認された。従業員は、当該の詐欺について認識していたが、自分が騙されるとは思わず、被害を受けてしまったとのことであった。対応として、外部機関や保険会社に連絡を行った上で、フォレンジック調査の実施を検討している。再発防止策として、業務で使用するパソコンについて業務外での使用を実施行わないことにした。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 106 | 2023/9/25 | 届出者（企業）が利用する IP 多機能電話機（IP-PBX）において、電気通信事業者より多数の不審な国際発信が確認されたとの連絡があった。調査の結果、当該機器から数百回に及ぶ不正発信が行われ、その発信による数十万円分の通話料金が発生していることが確認された。原因は、当該機器が遠隔から内線を使用できる構成になっており、外部の第三者が何らかの方法で主装置に不正アクセスし、当該機器から発信を行ったものとみられるが、詳細については不明である。対応として、電気通信事業者側で国際発信を停止した。再発防止策としては、電気通信事業者と当該機器のサービス提供元にて発信規制を行ったほか、利用している各機器のパスワードをより強固なものに変更するなどを実施した。 |
| 107 | 2023/9/28 | 届出者（企業）の複数部署から、メール送受信に遅延が発生している旨の連絡があった。調査の結果、届出者のメールサーバがメール不正中継の踏み台として悪用され、外部に数万件のスパムメールが送信されていたことが判明した。原因は、導入していたファイアウォール機器にて、スパムメールを防ぐためのフィルターを設定・更新していたが、当該スパムメールの送信元には、メールドメインが付与されていないメールアドレスが指定されており、そのようなメールに対して、フィルターの検知・遮断を設定していなかった。対応として、メールサーバとファイアウォール機器でスパムメールの送受信を遮断し、セキュリティソフトを用いたウイルススキャンも行った。再発防止策としては、メールサーバとファイアウォール機器に原因となった当該フィルターの設定を行った。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 108 | 2023/10/2 | 届出者（企業）の従業員から、不審な業者に電話をしてしまい、ソフトウェアを遠隔でインストールする旨の要求を受けたとの連絡があった。確認したところ、当該従業員がインターネット検索をしていたところ、不正なウェブサイトにアクセスしてしまい、インターネットブラウザが操作不能となった。このため、画面に表示された電話番号に連絡したとのことであった。調査したところ、電話先の指示どおりにパソコンを操作したことで、遠隔操作ツールを通じて、当該パソコンの画面を不正に閲覧された可能性があることが確認された。状況から、偽セキュリティ警告（サポート詐欺）と推定している。対応として、当該パソコンの利用を停止したのち、不正に閲覧されたと見られるサービスの停止やパスワード変更を行った上で、フォレンジック調査も依頼した。再発防止策としては、社内周知を含めたセキュリティ教育を実施した。 |
| 109 | 2023/10/13 | 届出者（地方自治体）のウェブサイトに対する大量のアクセスが行われ、サイトの閲覧が困難な状態にあることをウェブサイトの管理委託業者が発見した。調査の結果、海外から 1 時間に最大数百万件に及ぶ規模の DDoS 攻撃が行われたことが判明した。対応として、利用しているセキュリティ製品にて海外からのアクセスを遮断した。再発防止策としては、セキュリティ製品の監視設定を見直したほか、緊急時の連絡体制も見直す予定である。 |

## 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）