コンピュータウイルス・不正アクセスの届出事例

［2022 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

2022 年 8 月 26 日

目次

1. はじめに

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

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

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

---

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

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

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

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

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

2. 届出事例の傾向

2022 年上半期（1 月～6 月。以下、今期）に受理した [6]コンピュータウイルス（以下、ウイルス）届出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、主な事例を 263 件取り上げ､次の 5 種に分類した｡被害の原因に主眼を置いて分類しているが、その原因については、原則として届出者の申告に基づいている。また、複数の分類に該当し得る事例については、その事例の特徴を最も示していると考えたものに分類した。それぞれの分類ごとの届出の概要は次節以降に示す。

- コンピュータウイルスの検知・感染被害　174 件（事例 No.1～174）
- 身代金を要求するサイバー攻撃の被害　26 件（事例 No.175～200）
- 脆弱性や設定不備を悪用された不正アクセス　36 件（事例 No.201～236）
- ID とパスワードによる認証を突破された不正アクセス　16 件（事例 No.237～252）
- その他　11 件（事例 No.253～263）

全体を通して見ると、今期は、2021 年下半期（7 月～12 月。以下、先期）まで届出数が減少傾向にあったウイルスの検知・感染の被害（2-1 節で説明）の届出が大幅に増加した。中でも Emotet と呼ばれるウイルス（以下、Emotet）に関する届出が大半を占めた。2021 年 1 月に攻撃基盤の停止が報じられて以降、しばらく攻撃が観測されていなかった Emotet だが、2021 年 11 月頃より攻撃者の活動が再開したとの情報があった。ウイルス届出においても 2021 年 12 月から Emotet に関する届出が寄せられるようになり、特に 2022 年 2 月から届出が急増し、7 月頃まで継続して多数の届出を受理していた。ただし、7 月になると Emotet の届出は減少し、7 月以降に受理した Emotet の届出では、発見日時は全て 7 月上旬以前であった。また、IPA では 7 月中旬以降、Emotet の攻撃メールは観測していない。これらのことから、8 月現在では Emotet の攻撃活動は停止しているとみられる。しかし、再び大規模な攻撃活動が開始される可能性が考えられることや、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恐れもあるため、引き続き警戒は必要である。

他の届出に関しては、先期と比較すると届出の数は若干減少したが、これまでと同様に、一般的によく知られたセキュリティ施策を実施していれば、被害を防ぐことができたと思われるものが多かった。ID やパスワードの管理不備や強度不足により認証を突破された事

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

例（2-4 節で説明）の大半はその典型と言える。セキュリティポリシーに基づいた利用規則の策定やパスワードポリシーの設定等を行い、管理者や利用者一人ひとりがそれに従った運用・利用を行っていれば、被害を防ぐことができた可能性が高いと考えられるものであった。

同様に、脆弱性やセキュリティ設定の不備を悪用された事例（2-3 節で説明）の多くについても、修正プログラムの適用といった基本的な対策を徹底することにより、被害を防げた可能性があったと考えている。ランサムウェア等によ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）も、その多くは VPN 装置等に脆弱性が存在していて、外部から攻撃者の侵入を許してしまったことが原因と考えられる事例であり、同様に脆弱性対策が徹底されていれば被害を防止できた可能性があった。

また、脆弱性情報が公開されてからも長期間対策がなされていなかったシステムや、現在は利用していない古いシステムが脆弱な状態で放置されていて、攻撃の被害に遭った事例が複数見られた。脆弱性の管理は基本的かつ重要な対策であり、徹底することで多くの被害を避けることができるが、組織内の多数の機器を迅速かつ見逃しなくアップデートすることは簡単ではない。機器やソフトウェアバージョンの IT 資産管理、脆弱性情報の収集・アップデートを確実に実施できる運用手順の確立を進めていただきたい。

本紙に示した事例以外にも、ウイルスの発見・感染、なりすましやフィッシング等の不審なメールの受信、クラウドサービスのアカウントに対する不正なログインの挙動検知などの情報も複数寄せられた。これら届出全体の集計情報については 2023 年 1 月に「コンピュータウイルス・不正アクセスの届出状況」として公開する予定である。

2-1. コンピュータウイルスの検知・感染被害

今期は、利用しているパソコン等がウイルス感染の被害にあったという事例の届出が 174 件あった。先期の 7 件から今期は大幅に増加している。そのほとんどは Emotet の検知や感染、または Emotet への感染を狙った攻撃メールの着信の届出であった。本節では、Emotet に関する被害と、それ以外のウイルスについて、それぞれの項で説明する。なお、ランサムウェアの部類であると判断したウイルスに関する届出は別の分類としており、2-2 節で説明する。

（1） Emotet

Emotet は、情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大が試みられている。

2019 年 9 月頃から 2020 年 2 月頃まで、及び 2020 年 7 月頃から 2021 年 1 月頃までの間、多数の攻撃活動が観測された Emotet だが、2021 年 1 月 27 日に EUROPOL（欧州刑事警察機構）主導で攻撃基盤の停止措置が行われて以降、10 か月ほど攻撃は観測されていなかった。しかし、2021 年 11 月 14 日頃から、Emotet の攻撃活動再開の兆候が確認されたという情報があり、Emotet への感染を狙う攻撃メール（Emotet の攻撃メール）が着信したという情報も複数観測された。IPA へも企業等から被害の相談が多数寄せられ、ウイルス届出においても、今期だけで 164 件もの届出があった（Emotet を検知したのみで感染が認められなかった届出も含む）。中には、組織内で数百個以上という大量の Emotet を検知したという事例や、Emotet とともに CobaltStrike[7]と呼ばれる別のウイルスが検知された事例もあった。CobaltStrike は Emotet によってダウンロードされたことにより、同一の機器で 2 種類のウイルスが検知されたものと思われる。

Emotet の攻撃メールに使われている手口は、以前のものと同様に、正規のメールへの返信を装うなどして送信元を偽装したメールで行われる。そのメールに、Emotet をダウンロードするようなマクロが含まれた Office 文書ファイルを添付したり、メール本文に記載したリンクからダウンロードをさせたりして、受信者に開かせようとする。

なお、新たな手口として、2022 年 4 月 25 日頃より、Emotet をダウンロードするようなショートカットファイル（LNK ファイル）をメールに添付して Emotet へ感染させる手口を確認した。ショートカットファイルはメールに直接添付されている場合と、パスワード付き ZIP ファイルとして添付されている場合があり、このショートカットファイルをダブルクリックなどで開くと Emotet に感染してしまう。ショートカットファイルは、アイコンが文書ファイルのように偽装されていることや、Windows の標準設定では拡張子が表示されないといった特徴から攻撃ファイルであると見分けが付きにくく、誤って開いてしまう恐れがある。また、Office 文書ファイルのマクロを悪用した手口と異なり、Office アプリケーションで「コンテンツの有効化」ボタンをクリックしないでも感染してしまう（すなわち、利用者は特殊な操作をせず、ショートカットファイルを開くだけで感染する）。

対策としては、以前と同様に「添付ファイルを開かない」「URL リンクにアクセスしない」「マクロを有効にしない」ことを利用者に周知するとともに、新たな手口に対応するため、業務上必要がなければ、ショートカットファイル（拡張子 .LNK）が添付されたメールをブロックする設定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、Emotet に関する最新の情報を公開しており、動向

---

[7] CobaltStrike はペネトレーションツールであるが、攻撃者が悪用する事例もあり、セキュリティソフト等で悪性のソフトウェアとして検知される場合もあるため、本紙ではウイルスと表記する。

や攻撃手口に変化が見られた場合等に随時更新している。対策の参考にしていただきたい。

- 「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて
  https://www.ipa.go.jp/security/announce/20191202.html

表 2-1 に Emotet を検知、または Emotet に感染した届出の一覧を各月ごとに分けて掲載する。Emotet の届出については、個々の詳細は省略する。

表 2-1 Emotet 検知・感染に関する届出一覧

届出月	事例 No.	届出者の主体と件数		概要
2022/1	1 （1 件）	企業	1 件	共通して、次に挙げるような検知・感染の情報があった。 ● 組織内のパソコンやサーバにおいて、セキュリティソフトがウイルスを検知した。検知名などから 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た。 ● 顧客や取引先等に、Emotet への感染を狙ったメールが着信した。自組織を差出人に詐称されていたり、過去のメールが引用されていたりしたケースもあった。
2022/2	2～27 （26 件）	企業	23 件	
		一般団体	1 件	
		地方自治体	1 件	
		個人	1 件	
2022/3	28～90 （63 件）	企業	50 件	
		一般団体	9 件	
		教育・研究機関	2 件	
		個人	2 件	
2022/4	91～118 （28 件）	企業	21 件	
		一般団体	5 件	
		地方自治体	1 件	
		教育・研究機関	1 件	
2022/5	119～136 （18 件）	企業	13 件	
		一般団体	4 件	
		個人	1 件	
2022/6	137～164 （28 件）	企業	22 件	
		一般団体	6 件	

（2） Emotet 以外のウイルス

Emotet 以外には、Remcos と呼ばれるウイルスや Qakbot と呼ばれるウイルスに感染した疑いがあったものや、サーバから仮想通貨のマイニングを行うコインマイナーの類いが発見されたとの届出があったが、多くはウイルスの名称や被害の内容が不明とのことで

あった。中には Emotet による被害と推測される届出もあったが、明確に判別できない届出に関しては本項に分類している。

感染した原因についても不明とされているものが多かったが、その中には不審なメールが届き、添付されていたファイルを開いてしまったことが原因であると届出者が推測している事例が複数見られた。メールを起点とした攻撃に対しては、前項で述べた Emotet 同様、「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」といった対策を徹底することが重要になる。依然としてメールにより感染拡大を狙うウイルスが存在している以上、送信元や本文に見覚えがある返信メールや、自然な日本語で書かれたメールであっても、攻撃メールである可能性を念頭に置いて取り扱うことも必要であろう。

なお、サーバ機器でウイルスが発見された事例についても、原因が判明していないものは本項に分類している。特に外部に公開しているサーバに関しては、外部からの侵入を可能にしてしまうような脆弱性の悪用や、ID やパスワードなどの認証情報が何らかの理由で漏えいし攻撃者に悪用される等して、ウイルスに感染させられた可能性も考えられる。ウイルス対策とともに、2-3 節や 2-4 節を参考に、脆弱性対策や認証情報管理の見直しも検討していただきたい。

表 2-2 に Emotet 以外のウイルス感染に関する届出の概要一覧を示す。

表 2-2 Emotet 以外のウイルス被害に関する届出の概要一覧

事例 No.	届出日	概要
165	2022/3/4	届出者（企業）のパソコン 1 台が 2 つのコンピュータウイルスに感染した。セキュリティソフトがウイルスを検知し、駆除を行った。ファイアウォールやプロキシサーバを使用せずインターネットに接続された環境下のパソコンであったことから、不審なウェブサイトの閲覧、または何らかの脆弱性を悪用されてウイルスが侵入してきたことが考えられるが、感染した原因は不明である。再発防止に向け、システムやネットワークの構成を見直し、管理サーバによる機器管理や VPN の構築等を検討している。フォレンジック調査のため約 700 万円の費用が発生した。

事例No.	届出日	概要
166	2022/3/18	届出者（企業）の複数のパソコンやサーバが通常には生じない高負荷の状態になっていたため、調査を行ったところ、XMRig コインマイナーと呼ばれる不正なソフトウェアが見つかった。セキュリティソフトにより駆除を行った。不正アクセスの手口は不明だが、ファイアウォールのルール設定に不備があったことが原因と推測している。ファイアウォールの設定を見直すとともに、インターネットとの境界だけでなく拠点間の通信経路にもファイアウォールを設置して、被害拡大の防止を図ることを検討している。
167	2022/3/22	届出者（教育・研究機関）の組織内ネットワークからウイルスの C&C サーバへの通信が発生していることを、IPS が検知した。調査したところ、通信先の情報などから組織内の機器が Remcos と呼ばれるウイルスに感染した可能性が考えられたが、ウイルス自体は発見できなかった。発見後の対応として、不正通信の発信元となった機器において OS の再インストールを行った。
168	2022/4/8	届出者（企業）に対し、過去のメールが引用された不審なメールが届いたとの連絡が複数の顧客から寄せられた。調査を行ったところ、100 台を超える機器がウイルスに感染している疑いが判明した。特に疑わしいと判断した 3 台についてフォレンジック調査を実施したところ、うち 2 台から Qakbot と呼ばれるウイルスが発見された。また、組織内の認証サーバに対し、総当たり（ブルートフォース）攻撃により不正アクセスに成功された痕跡があることも判明した。ただし、認証サーバへのウイルス感染には至らなかった。本件への対処として、ウイルス感染の疑いのあるパソコンは初期化し、認証サーバは再構築を実施した。再発防止策として、メールサーバのセキュリティ強化のためのソフトウェアの導入、パソコンへの EDR の導入、認証サーバのログ監視ソフトの導入を進めている。認証サーバの再構築及びフォレンジック調査のため約 2,000 万円の費用が発生した。

事例No.	届出日	概要
169	2022/4/19	届出者（教育・研究機関）が組織内部で使用するシステムが利用できなくなっていることに職員が気づいた。調べたところ、複数のサーバで不具合が見つかったため、システムを停止して調査を行った。調査の結果、外部記憶媒体を介して何らかのウイルスに感染させられた疑いがあると推測している。また、組織内のパソコンやサーバにおいて、複数の OS が混在していたために、一部の機器でウイルス定義ファイルのアップデートが正しく実施できていなかったことが判明した。発覚後の対策として、感染したサーバは初期化し、バックアップデータを用いてシステムを再構築した。再発防止策として、外部記憶媒体の接続を制限することとし、接続が必要な場合にはウイルススキャンと接続履歴の記録を必須とすることとした。
170	2022/5/13	届出者（企業）が利用するパソコンで、セキュリティソフトが 2 件のウイルスを検知した。うち 1 件は検知後、感染前に駆除されたことが確認された。もう 1 件は、メールに添付されていたファイルを開いたときに検知がされたものであったため、セキュリティソフトが表示した案内に従い、パソコンを初期化した。なお、いずれもウイルスの名称は不明である。
171	2022/6/3	届出者（企業）のパソコン複数台がウイルスに感染し、社員を送信者に装った不審なメールが取引先等に送信された。感染の原因は不明だが、以前、社員に不審なメールが着信していたとのことで、そのメールによりウイルスに感染させられたと考えている。セキュリティソフトによりウイルスは駆除されたが、念のため感染が確認されたパソコンは全て初期化を行った。
172	2022/6/10	届出者（企業）のメールアドレスを送信者に装った不審なメールが届いたとの報告が、約 10 社の取引先等からあった。ウイルスに感染した疑いが生じたため、届出者はセキュリティソフトで社内のパソコン等のウイルススキャンを行ったが、ウイルスは発見されなかった。念のためメールサーバへアクセスする際のパスワードを変更し、引き続きセキュリティソフトでの監視を継続している。

事例No.	届出日	概要
173	2022/6/20	届出者（企業）のメールアドレスを送信者に装った不審なメールが社内外に送信されていたことが判明した。また、レンタルサーバ業者からは、大量の迷惑メールが送信されたためメールアカウントを一時停止したとの連絡があった。感染の原因は、以前に従業員が不審なメールに添付されていたファイルを開いてしまったことがあるため、悪意のある添付ファイルにより、Emotet などメールの内容を窃取するウイルスに感染したことと推測している。ただし、当該の従業員が使用していたパソコンは使用を停止したため、ウイルスの存在は確認していない。また他の機器ではウイルスは見つからなかった。再発防止策として、EDR ソフトの導入やセキュリティに関する社内教育の強化等を予定している。
174	2022/6/27	届出者（企業）で、社内から外部の不正なウェブサイトへの通信が発生したことをファイアウォールが検知し遮断した。外部からダウンロードした PDF ファイルに不正サイトへのリンクが含まれており、社内のパソコンで当該 PDF ファイルを開いたことで不正サイトへの通信が発生したと見られる。通信の検知後に、当該のパソコンに対し、セキュリティソフトによるスキャンを実施したところ 16 件の疑わしいファイルが検知された。なお、パソコンは検知後に初期化したため、不正な PDF ファイルとの関係は不明である。また、セキュリティソフトで社内の機器に対してウイルススキャンを行ったところ、ファイルサーバから 6 個の疑わしいファイルが発見されたため削除した。これらのファイルは数年前から存在するファイルであった。再発防止策として、全てのパソコン・サーバに新たなセキュリティソフトの導入と、ファイアウォールの検知精度を向上させるための設定を行った。

2-2. 身代金を要求するサイバー攻撃の被害

今期はランサムウェア攻撃など、ファイルやデータを暗号化もしくは消去して、その復旧と引き換えに、身代金として金銭等を脅し取ろうとするサイバー攻撃の届出が 26 件あり、中でも先期と同様に、LockBit2.0 と呼ばれるランサムウェアによる被害の届出が 7 件と多かった。

LockBit2.0 は、ウイルスと同名の攻撃グループ「LockBit」が使用するランサムウェアである [8]。この攻撃グループは、窃取したデータを暴露するサイト（リークサイト）を持ち、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 [9]」を行うとされる。実際に、LockBit2.0 の被害に遭った届出の中には、リークサイト上に窃取されたと思われるデータが公開されていた事例もあった。侵入の手口としては、VPN 装置の脆弱性や、リモートデスクトップサービスの脆弱性を悪用されたというものが目立った。脆弱性対策については、2-3 節にて詳しく述べる。

侵入後にネットワーク内で拡散を図る攻撃手口の一つとして、ドメインコントローラの乗っ取りがある。LockBit2.0 には、ドメインコントローラ感染時に特別な仕組みを発生させる機能を持っているとされるが [10]、LockBit2.0 だけでなく、他のランサムウェア攻撃においても Active Directory などのドメインコントローラを乗っ取ろうとするものはある。届出事例においてもドメインコントローラの機能を悪用して、組織のネットワーク内の多数の機器に拡散し、ファイルの暗号化をしたと考えられるものが複数見られた。ドメインコントローラが悪用されると、その管理下にある機器全てに影響が及び、甚大な被害につながる恐れがある。そのため、特にドメインコントローラの脆弱性対策や、パスワード等の認証情報管理は確実に実施することを勧める。

また、今期のランサムウェアによる被害の届出では、自組織のシステム運用やサービス提供のために利用していた外部のサービスや、業務委託先の事業者のシステムがランサムウェア攻撃を受け、その影響により自組織のシステムやサービスが停止した事案も複数見られた。受託者であるサービス運用事業者は、不正アクセスを防止するために、普段から

---

[8] 2022 年 7 月頃に LockBit ランサムウェアは「LockBit 3.0」にバージョンアップされた。
SentinelOne "LockBit 3.0 Update | Unpicking the Ransomware's Latest Anti-Analysis and Evasion Techniques"
https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/

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

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

サービス基盤のセキュリティ対策を行うことが重要であるとともに、委託者との責任分界点を明確にした上で、インシデント発生時の作業分担や対応フローを定義して委託者と共有しておき、有事の際には共同で迅速に対応できるようにしておくことも重要である。

表 2-3 に身代金を要求するサイバー攻撃に関する届出の概要一覧を示す。この中で、複数の脆弱性と BitLocker を悪用したランサムウェア攻撃の事例（事例 No.191）の詳細を 3 章で紹介する。

表 2-3 身代金を要求するサイバー攻撃に関する届出の概要一覧

事例 No.	届出日	概要
LockBit ランサムウェアの被害事例		
175	2022/1/5	届出者（企業）が管理しているシステムが故障していることを通知するメールを受信したため、調査したところ、一部の機器で LockBit2.0 によりファイルが暗号化されていることを発見した。原因は、リモートデスクトッププロトコルで社外からアクセス可能な機器が存在していたこと、及びリモートデスクトップ接続に関する脆弱性が存在していたことから、外部から当該脆弱性を悪用されて侵入されたものと考えられる。また攻撃者が、侵入後に管理者権限を取得して ID やパスワードを窃取し、それらを悪用して侵害範囲を拡大した結果、最終的に 9 台の機器へ不正接続され、内 6 台がランサムウェアによってファイルを暗号化された。ファイルを暗号化された機器は、初期化後、バックアップからファイルを復元し復旧させた。また、再発防止のためファイアウォールの設定の見直し、社外環境からの接続制限や社員教育を行った。

事例No.	届出日	概要
176	2022/1/7	届出者（地方自治体）のサービスを提供していた委託業者のシステムが不正アクセスに遭い、届出者のサービスが停止した。委託業者が管理するサーバの保守端末にリモートデスクトップ接続に関する脆弱性が存在し、それを悪用した不正アクセスによりLockBit の攻撃を受け、サーバ上のファイルが暗号化されたことが原因であった。クラウド上のサーバに代替システムを構築して切り替えることによりサービス提供を再開した。再発防止策として、委託業者は自身が管理する機器の脆弱性対策と社内教育の徹底を行うこととし、届出者はそれらを定期的にチェックすることとした。
177	2022/2/24	届出者（企業）のサーバやパソコンなど 300 台以上の機器が、LockBit による侵入型ランサムウェア攻撃に遭った。ランサムウェアにより、データの暗号化と窃取を伝える脅迫文が、社内のプリンタに大量出力されたことで発覚した。初期侵入の原因は、VPN 装置（Fortigate）の脆弱性を悪用した攻撃により、ID とパスワードが窃取されたことである。攻撃者は社内ネットワークに侵入後、窃取した認証情報をもとに類推したパスワードを使って、ドメインコントローラを含む社内機器に不正ログインしたと見られている。発覚後には、全てのパソコンやサーバをネットワークから切断した上で、ID とパスワードの変更とバックアップからデータを復元する作業を行った。なお一部のデータについては、バックアップがなかったり、バックアップデータそのものが暗号化されていたりしたため、復元ができなかったものもあった。再発防止策として、サーバ OS を最新に保てるような運用方法を保守ベンダに依頼し、さらに EDR の導入などを行ってセキュリティの向上を図った。

事例 No.	届出日	概要
178	2022/3/15	届出者（企業）が使用するドメインコントローラ（Active Directory）を含むサーバ 8 台のファイルと、NAS に保存していたファイルが暗号化され、拡張子が変更されていたことを発見した。状況から LockBit の攻撃を受けたものと考えられる。届出時点ではデータの流出は確認していないが、可能性は否定できない。攻撃者が社内ネットワークへ侵入した原因については不明である。なお、社内で複数の機器に被害が及んだ原因は、ランサムウェアの機能により Active Directory サーバを悪用されて拡散したものと推測している。被害に遭ったサーバはいずれも初期化した上でバックアップデータを用いて復旧させた。対応に約 40 日の期間と、800 万円ほどの費用が発生した。再発防止策として、ネットワークセグメントの分離を検討している。
179	2022/5/25	届出者（一般団体）が利用するシステムに障害が発生し、プリンタから英文の脅迫文が大量に印刷された。調査の結果、当該システムを構成するサーバが LockBit2.0 に感染していることが判明した。感染した原因は、VPN 装置（Fortigate）に存在していた脆弱性を悪用され、外部からの不正な侵入を許してしまったことである。なお、当該システムのデータは、外部業者の復旧作業により、欠損なく全て復旧することができた。再発防止策として、セキュリティソフトの導入や脆弱性診断の実施によりセキュリティ強化を図った。また、データの種別により、クラウドストレージへの保存や、ネットワークとは切り離したハードディスクへの保存など、データ保存場所と方法を見直すことを検討している。

事例No.	届出日	概要
180	2022/6/10	クラウド上にある届出者（企業）のサーバに障害が発生したため、状態を調査したところ、LockBit2.0 によりファイルが暗号化されていることが判明した。外部の専門機関に依頼して詳細な調査を行ったところ、VPN 装置（Fortigate）の脆弱性を悪用されたことが原因であった。なお、本件が発覚する 1 年ほど前に、VPN 装置のファームウェアをバージョンアップして脆弱性の解消は行っていた。しかしながら、パスワードの変更は行っていなかったことから、1 年以上前に窃取された ID とパスワードが悪用され、認証が突破されたと見られる。対策として、インターネット VPN を廃止し、閉域網を利用する方式に変更した。また再発防止に向け、脆弱性情報の定期的な確認と対策、データバックアップ方法の見直し、情報セキュリティ体制の強化、従業員に対する教育・研修を行うとしている。
181	2022/6/13	届出者（教育・研究機関）のシステム運用を委託していた業者において、複数台のサーバとパソコンが LockBit2.0 に感染した。届出者は委託先業者からの連絡を受け、事態を認識した。システム開発用のサーバに外部から不正なアクセスがあったことは判明しているが、具体的な手口等は不明である。攻撃者はリークサイトに窃取した情報を公開するとの脅迫をしていたが、セキュリティ専門業者が調査したところ、公開された情報に届出者のデータは含まれていなかったとのことであった。再発防止に向け、委託先業者とともに、IT セキュリティ及び情報管理体制の更なる強化を図るとしている。
その他の身代金を要求するサイバー攻撃被害の事例		
182	2022/1/13	届出者（企業）が使用しているパソコン、サーバや NAS において、保存しているほとんどのファイルの拡張子が.EKING になっており、使用ができない状態になっていることに気づいた。拡張子の特徴から、EKING と呼ばれるランサムウェアの攻撃を受けたものと推測される。外部から VPN 接続するための回線を設置していたことから、感染の原因は、攻撃者が何らかの方法で VPN 回線から侵入したためと考えている。対策として VPN 回線を遮断し使用を停止した。

事例No.	届出日	概要
183	2022/1/14	届出者（教育・研究機関）の仮想サーバ数台がランサムウェア攻撃の被害に遭った。Dharma と呼ばれるランサムウェアの一種と考えられる。原因は不明であるが、修正プログラムの適用がされていなかった箇所があったことが判明しており、仮想サーバに何らかの脆弱性が存在していて、それを悪用された恐れがある。被害発覚後には、不正アクセスを受けたサーバ群をネットワークから遮断する措置を行い、その後 IPS が導入されている別のデータセンタに構築したシステムに切り替えることで復旧させた。本件への対応には、100 万円以上の費用を要した。
184	2022/3/3	届出者（地方自治体）のシステムが使用できない状態となっていたことに職員が気づき、調べたところ、パソコンとサーバの各 1 台が Phobos と呼ばれるランサムウェアの攻撃に遭っていたことが判明した。侵入経路は不明である。日次でバックアップを取得していたため、被害に遭った機器は初期化した上で、前日のバックアップからデータを復元して復旧させた。再発防止策として、外部ベンダと不正アクセス監視及びインシデント対応サポートについての契約を検討している。
185	2022/3/8	届出者（地方自治体）のシステムのデータを収集するパソコンがランサムウェア攻撃の被害に遭い、対応のために当該システム及び同様の構成となっている装置を停止することとなった。本件は、関係者からシステム管理者に、データが更新されていない旨の連絡があり、業務委託先の調査により発覚した。侵入の原因は、当該パソコンのリモートデスクトップの接続設定において、アクセス制限等がされておらずインターネットから誰でもアクセス可能となっていたことから、攻撃者が外部から当該パソコンにリモートデスクトップで接続し、パスワードを推定した等で認証を突破して不正アクセスしたと考えている。再発防止策として、リモートデスクトップ接続を無効化し、パスワードを複雑なものした。また、システムの管理部門と業務委託先にて、定期的にセキュリティ対策の自己点検とセキュリティ監査を実施することとした。

事例No.	届出日	概要
186	2022/3/16	届出者（企業）が顧客に導入し運用管理を受託していた NAS のファイルがランサムウェアにより暗号化され、受発注などの取引データにアクセスができず顧客の業務が停止状態に陥った。当該顧客（被害企業）の利用者が NAS にアクセスした際にファイルが正常に開けず、代わりに英語の脅迫文のようなテキストが表示されたことで異常に気づき発覚した。調査を行ったところ、踏み台になったと思われるパソコン等は発見できなかったこと、及び外出先から NAS を利用するために、インターネットから NAS へアクセスできるようにルータの設定をしていたことから、攻撃者に何らかの手段で認証を突破されて、外部から直接 NAS に不正アクセスされたことが原因と推測している。再発防止策として、外付けハードディスクを用いたバックアップの取得、ルータ及びパソコン等の ID・パスワードを複雑なものに変更、外部アクセス機能の構成変更によるセキュリティ向上を行った。
187	2022/3/18	届出者（地方自治体）から業務を受託している事業者の複数のサーバがランサムウェア攻撃を受け、届出者に関するデータがファイルサーバの暗号化被害により使用できなくなった。届出者は当該事業者から連絡を受け、本事象を認識した。当該事業者はサーバをインターネットから切り離した上で専門業者とともに調査を行ったが、痕跡が削除されておりデータ漏えいの有無、及び漏えいしたデータ量は不明であった。本事象を受け、当該事業者はインターネット上への顧客の情報流出状況の監視や、高度なセキュリティ体制の検討を行っている。

事例No.	届出日	概要
188	2022/3/23	届出者が個人宅で利用している NAS に格納していた 40TB 以上のファイルが暗号化された。バックアップ作業中にファイルが存在しないとの警告メッセージが表示されたことで事象を認識した。暗号化されたファイルの拡張子などから、DeadBolt と呼ばれるランサムウェアの攻撃を受けたものと判断した。侵入の原因は不明だが、NAS へインターネットからアクセスできる機能を有効にしていたため、攻撃者に外部から不正アクセスされたと考えている。再発防止策として NAS にアクセスするためのポート番号を初期設定値から変更した。なお、バックアップからのデータ復元ができたため、損失したファイルはなかったが、復旧作業には約 3 週間を要した。
189	2022/4/5	届出者（一般団体）が利用しているファイルサーバとパソコンにおいて、ファイルの拡張子が変更されていたこと、及び脅迫文と思われるファイルが置かれていることを発見した。脅迫文の内容から Phobos と呼ばれるランサムウェアに感染したと推測される。感染原因は不明である。感染した機器は初期化した上で、リモート環境に保存していたバックアップデータを復元してシステムを復旧させた。またパスワードのリセットも実施した。届出者は、被害発生前よりセキュリティソフトと UTM を導入していたが、本件を受け、更に EDR ツールの導入を検討している。
190	2022/4/7	届出者（企業）のシステムに異常が発生していることを監視システムが検知した。調査したところ、ランサムウェア攻撃により 3 台のサーバ上のファイルが暗号化され、拡張子が.CXRDMN に変更されていたことにより、システムが停止していたことが判明した。詳細な調査により、リモートアクセス用の VPN 装置に不正アクセスされていたことが判明した。Robinhood と呼ばれる攻撃者が、VPN 装置の脆弱性を悪用して窃取した認証情報を使って不正アクセスし、ランサムウェア攻撃を行ったものと推測している。暗号化されたデータはバックアップから復元してシステムを復旧させたが、業務の再開までに約 6 日間を要した。また、弁護士相談やフォレンジック調査等の対応に約 1,500 万円の費用が生じた。

事例No.	届出日	概要
191	2022/4/13	届出者（企業）のシステム管理者に、従業員から使用するパソコンで BitLocker が意図せず有効化されているとの連絡があった。更に社内システムへの接続不可に関する問合せの連絡があり、調査したところ、基幹システムのサーバにおいても BitLocker によるストレージの暗号化がされていることが判明した。その後の調査により約 130 台のパソコンやサーバで BitLocker 機能による暗号化が行われており、多数のシステムが停止を余儀なくされていたことが確認された。原因は不正アクセスによるものであり、VPN 装置（Pulse Secure）の脆弱性を悪用して認証情報を窃取した攻撃者が侵入し、更に Active Directory サーバの脆弱性（Zerologon）を悪用して、ドメインコントローラ管理下の複数の端末へ被害を広げていたことが判明した。対応として、被害を受けたパソコンとサーバは初期化し、バックアップデータを用いて再構築を行い、各端末のウイルススキャンや修正プログラムの適用を行った。再発防止策として、ドメインコントローラやネットワーク機器への脆弱性対策運用の確立、SSL-VPN サービスの全てのアカウントのパスワード変更等を行った。
192	2022/4/13	届出者（一般団体）がクローズドな環境で検査機器の操作のために使用していた、Windows 7, Vista, XP の各 OS が搭載されたパソコン 3 台において、WannaCry と呼ばれるランサムウェアが複数検知された。感染原因は不明である。

事例No.	届出日	概要
193	2022/4/18	届出者（教育・研究機関）のウェブサイトが表示できなくなったため、サーバ状態を調査したところ、ウェブコンテンツを格納するデータベースサーバのファイルが暗号化されていて、ウェブサーバが動作不能に陥っていたことを確認した。データベースサーバのファイルは拡張子が.bozon に変更されており、身代金を要求する脅迫文のテキストファイルが残されていることから、BOZONと呼ばれるランサムウェアの攻撃を受けたものと判断した。原因は、データベースサーバの一部のポート帯に対するアクセス制限に不備があり、インターネットからアクセス可能になっていたため、そこから侵入されたものと推定している。対策として、アクセス元 IP アドレスの制限、定期的な設定の精査、セキュリティ対策ソフトの導入と定期アップデートを実施した。
194	2022/4/21	届出者（企業）のシステムが停止していることを監視システムが検知したため、サーバの状態を確認したところ、複数のサーバ上のファイルが暗号化されていた。ファイル暗号化の被害はほとんどの業務サーバと一部のパソコンにも及んでいた。また、データ復元のためには攻撃者への連絡が必要であり、連絡がされなかった場合には窃取した情報を公開するとの脅迫文が残されていたことから、ランサムウェア攻撃を受けたと判断している。調査の結果、攻撃者は VPN 装置（SonicWall）の脆弱性を悪用して外部から侵入し、ドメインコントローラの管理者権限を乗っ取り、セキュリティソフトを無効化して、ランサムウェアを社内に拡散したと推測される。発覚後の対応として、全サーバとパソコンをネットワークから切り離した上で、バックアップからのデータ復元を行った。なお、バックアップサーバの一部も被害を受けていたため、被害前の状態に完全復旧させることはできなかった。再発防止策として、外部システムも含めてパスワードの変更を実施するとともに、セキュリティに関する設定強化やツールのアップデートを実施した。また、EDR を導入して更なるセキュリティ強化を図ることを検討している。

事例No.	届出日	概要
195	2022/4/26	届出者（地方自治体）が提供していたシステムにおいて、利用者から利用できないとの問い合わせを受けた。クラウドサービスを提供する委託事業者に確認したところ、サーバ上のファイルが暗号化されていたことを発見し、それが原因でシステムが利用不可になっていたことが発覚した。攻撃者が何らかの方法で管理者の ID とパスワードを特定し、それを悪用して届出者のシステムへ不正アクセスしたと推測している。本件発覚後、被害の拡大を防ぐため、各サーバのネットワーク接続を全て遮断した。また、情報セキュリティ専門の業者に依頼して詳細な被害状況や原因の調査を行っている。再発防止策として、多層防御を行うセキュリティ製品の導入、認証情報の管理強化、セキュリティ管理体制の強化を実施する。
196	2022/5/24	届出者（企業）において、従業員から、自身のパソコンで異常な画面が表示されていて使用ができないとの連絡があった。調査したところ、複数のサーバやパソコンで多数のファイルが暗号化され、拡張子が変更されていたことが判明した。また、ファイルサーバの一部のデータが窃取されていたことも判明した。Pandora 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。原因は、外部からアクセス可能にしていた仮想デスクトップ環境に脆弱性が存在していたため、攻撃者に悪用され外部から侵入されたことと考えている。被害を受けたサーバやパソコンは初期化し、ファイルサーバのデータはバックアップから復元して、システムを復旧させた。再発防止策として、外部からアクセス可能な機器の脆弱性点検、リモートアクセス方法の変更、アカウント管理やデータ管理方法の見直し、振る舞い検知機能の導入による監視の強化等を行った。

事例No.	届出日	概要
197	2022/5/27	届出者（企業）のシステムで障害を検知し、システム部門が状態を確認したところ、サーバがウイルスに感染していることが判明したため、ネットワークから切り離した。しかしその後、別のシステムでもファイルが暗号化されたり、プリンタから大量に脅迫文が出力されたりといった事態が見られたため、ランサムウェア攻撃を受けたものと判断した。状況から HIVE と呼ばれるランサムウェアに感染したと考えている。届出者は発覚後、被害を受けたシステムの外部ネットワーク接続を切断した上で、侵害状況を確認する専用ソフトウェアを使用して状況を確認したところ 40 台以上のパソコンやサーバが被害を受けていたことが判明した。感染に至った攻撃手口は不明である。なお、届出者は外部の専門事業者とともに攻撃者のリークサイトの監視をしているが、届出時点で届出者のデータの公開はされていない。再発防止策として、VPN 使用時の認証パスワード強化と二段階認証の導入、アクセス制限の設定、ファームウェアのアップデートによりセキュリティを強化した。また振る舞い検知の仕組みや、外部通信のモニタリングの導入も検討している。
198	2022/6/1	届出者（企業）が利用している業務用サーバ 3 台が、ランサムウェア攻撃を受け、ファイルが暗号化される被害に遭った。調査の結果、攻撃者は、届出者が DMZ 上で公開していたサーバのリモート接続用のポートに対して、総当たり攻撃を行い不正アクセスした後、当該サーバを踏み台にして 3 台のサーバへ侵入したと推定される。発覚後、専門業者を含めた調査を行うとともに、被害サーバの隔離や業務サーバの代替環境の構築を実施した。なお暗号化されたデータは、別環境に保存していたバックアップから復元した。再発防止策として、パスワードポリシーの強化、ネットワークログの取得期間の延長、社内規程の運用の厳格化等を行った。本件対応により、弁護士相談やフォレンジック調査等で約 1,000 万円の負担が発生した。

事例No.	届出日	概要
199	2022/6/13	届出者（企業）が、国内拠点へのアクセスのために海外に設置していたサーバについて、障害が発生しているとの連絡が現地の従業員からあった。国内からサーバの状態を確認したところ、現地のサーバだけでなく国内のサーバにおいてもファイルが暗号化されて動作不能な状態に陥っていることが判明した。暗号化されたファイルの拡張子（.Devos）や表示された脅迫文などから、Phobosランサムウェアに感染したと考えられる状況であった。調査の結果、攻撃者は総当たり攻撃等の手段によってサーバへのログイン認証を突破して、リモートデスクトッププロトコルでサーバに不正アクセスし、ランサムウェア攻撃を行っていたことが判明した。原因は、パスワードが比較的簡易なものであったことと、国内のサーバは IP アドレスによるアクセス制限を行っていたのに対し、海外のサーバはテレワークのために接続元 IP アドレスの制限を行っていなかったためと考えている。本件を受け、バックアップデータを用いて国内のサーバは再構築して復旧させたが、海外設置サーバについては利用方法を再検討し、復旧対象としないこととした。再発防止策として、クラウド上への新規サーバの設置、海外から国内拠点へのアクセス方法の変更、一部機能の別サービスへの移行、二要素認証の導入などを実施することとした。
200	2022/6/21	届出者（企業）において、複数のサーバで異常が発生していたため、状態を確認したところ、ファイルが暗号化されており、脅迫文が書かれたテキストファイルが残されていた。セキュリティ専門事業者にてフォレンジック調査をした結果、VPN 装置（Fortigate）の脆弱性を悪用した不正アクセスを受け、Babuk の亜種と思われるランサムウェアの攻撃を受けていたことが判明した。サーバをネットワークから切り離し、データ復元ツールによる復旧を試みたが有効に機能しなかったため、バックアップデータやスナップショットデータを用いて、サーバの再構築を行った。再発防止策として、EDR や IDS などを導入し、ネットワークやクライアントなど複数面でのセキュリティ強化策を実施した。

2-3. 脆弱性や設定不備を悪用された不正アクセス

今期も、ソフトウェアのセキュリティ上の不具合（脆弱性）、またはサーバやネットワーク機器のセキュリティに関する設定不備が存在し、それが攻撃者に悪用されて不正アクセスを受けた事例の届出は多く、本節に分類したものだけで 36 件あった。なお、2-2 節で述べたとおり、身代金を要求するサイバー攻撃の被害を受けた事例についても、侵入の原因は VPN 装置やリモートデスクトップサービス（以下、RDS）などの脆弱性を悪用されて不正アクセスされたことと判断しているものが多かった。そのため、脆弱性の悪用が原因である不正アクセス届出事例の総数は更に多い。

複数の届出事例において、攻撃への悪用があったとされた VPN 装置や RDS の脆弱性は、いずれも 2019 年に情報が公開されたものである。すなわち、今期においても複数の悪用事例があったことは、約 3 年が経った現在でも対策がされておらず、脆弱な状態にある機器等が存在すること、それらの脆弱性を狙った攻撃が継続していることを示している。特に、VPN 装置の脆弱性は、外部から装置内部の任意のファイルを読み取ることができるというものであり、VPN に接続する際の ID やパスワードといった認証情報を窃取される恐れがある。外部から攻撃の侵入口となり得る箇所（攻撃対象領域、Attack Surface と呼ばれる）については、把握・特定して必要最小限とするとともに、脆弱性対策がされていない箇所がないかを改めて確認いただきたい。また、対策を実施する際には、バージョンアップ等で装置のプログラム修正を行うだけでなく、既に認証情報が窃取されていた場合に備え、パスワード等を変更する必要があることにも留意が必要である。

長期間、脆弱な状態にあり対策がされていなかったことに起因すると思われる事例が多かった一方で、脆弱性情報が公開されてから比較的短い期間で、その脆弱性を悪用した攻撃が観測された例もあった。2021 年 10 月 20 日に情報が公開された CMS（Movable Type）の脆弱性については、1 週間後の 10 月 27 日には脆弱性の有無を確認するような通信が観測されている [11]。今期の不正アクセス届出においても、当該脆弱性を悪用したと思われる被害の届出を 10 件受理したが、そのうち 8 件は 2021 年 11 月に攻撃を受けたとされるものであった。同様に、2021 年 11 月頃に報告されていた Java ベースのロギングライブラリである Log4j の脆弱性を悪用した攻撃については、12 月に被害を受けたという届出が 3 件（内 2 件は先期報告済み）、1 月に被害を受けたとの届出が 1 件あった。その中には、Log4j が組み込まれたアプリケーションにおいて、当該アプリケーションのベンダから修正プログラムが公開されるよりも前から攻撃を受けていたこと（ゼロデイ攻撃）が判明した事例もある。

---

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

ゼロデイ攻撃を完全に防ぐことは非常に困難であるが、それでも迅速かつ確実な脆弱性対策を実施することは被害の抑止や低減につながる。月に 1 回といった定期的な対策だけではなく、あらかじめ自組織で使用している全てのハードウェア、ソフトウェア、サービスを把握した上で、それぞれに対して各ベンダ等から随時情報が取得できるようになっていること、脆弱性が確認されたときにはすぐに対策作業ができるようになっていることといった観点で、運用の体制や手順を点検することが重要と考える。

表 2-4 に脆弱性や設定不備を悪用された不正アクセスの届出の概要一覧を示す。この中で、Log4j の脆弱性を悪用したゼロデイ攻撃の被害事例（事例 No.229）の詳細を 4 章で紹介する。

表 2-4 脆弱性や設定不備を悪用された不正アクセスに関する届出の概要一覧

事例 No.	届出日	概要
CMS の脆弱性や設定不備が悪用された事例		
201	2022/1/5	届出者（教育・研究機関）が管理するウェブサイトが改ざんの被害に遭った。ウェブサイトにアクセスができないことに気づき、サイトを再構築して復旧させたが、数日後に同じ現象が再発した。そのため、詳細に調査したところ、CMS（Movable Type）の脆弱性を悪用した不正アクセスにより、サーバ上に複数の不審なファイルを設置されていたことが判明した。対策として、改ざんされたファイルの削除と復元、最新バージョンへのアップデートによる脆弱性の解消、CMS のパスワード変更、及び CMS と同一のパスワードを使用していたシステムのパスワード変更を行った。また、これまで明確な取り決めがなかった保守業者との役割分担を明確にし、バージョンアップ等の脆弱性対策作業は保守業者が実施することとした。

事例 No.	届出日	概要
202	2022/1/6	届出者（企業）のサーバが不正アクセスを受け、ウェブページを改ざんされて利用者向けサービスが一時停止し、更に不正なメール送信の踏み台に悪用される被害に遭った。サーバの保守を行う業者がウェブサイトの動作に異常があることを発見し、調査したところ不正な PHP ファイルが複数設置されていたことが判明した。原因として、使用していた CMS（Movable Type）に脆弱性があったため、攻撃者に脆弱性を悪用した不正アクセスをされ、ウェブの改ざんをされたと考えられる状況であった。本件を受け、不正なファイルを削除し、管理画面へのアクセスに対する認証の追加を行った。再発防止に向け CMS を更新して脆弱性の解消を行い、更に今後、別のサーバへ移行することを検討している。
203	2022/1/7	届出者（公共機関）のウェブサイトが、CMS（Movable Type）の脆弱性を悪用した攻撃を受け、ファイルを改ざんされる被害に遭った。届出者の公式 SNS アカウント宛に情報提供があり被害発生を認識した。当該ウェブシステムは、公開用と非公開の各サーバから成るが、CMS は非公開サーバ用にクローズドネットワークで使用しており、最新の状態にしていなかったところ、同様の状態の CMS を誤って公開サーバにも設置してしまったため、脆弱性のあるサーバが公開された状態になっていた。本件の発覚後に、一時的にウェブサイトを停止して CMS 提供元にて示されていた対応策を実施し、脆弱性を解消した。また再発防止策として、IPS 及び WAF でカスタムシグネチャを定義して、SOC でインシデントを検知できるようにした。利用者への被害はないが、保守業者の対応工数として約 50 人日を要した。

事例No.	届出日	概要
204	2022/1/11	届出者（公共機関）が運営するウェブサイトにアクセスができなくなった。また検索サイトで当該ウェブサイトを検索した際に無関係の通販サイトが上位に表示されるようになっていた。届出者組織の職員が気づき、ウェブサイトの保守業者が調査を行ったところ、ウェブサイトが改ざんされていたことが発覚した。更に調査したところ、CMS を初期設定のままで使用していたため、管理者画面等へアクセスする URL が容易に推測可能だったことに加え、ログインのための ID やパスワードも比較的簡易なものであったことが判明し、総当たり攻撃によって不正にアクセスされ改ざんを受けたものと推測される状況であった。本件への対応として、ウェブサーバ上の全データを削除しバックアップから復元したのちに、管理画面の URL 変更、ID とパスワードの変更、不正アクセスに使用されたものを含め不要なプロトコルの無効化を行った上でウェブサイトを復旧させたが、十分な対策ができているかを検証するため、再度ウェブサイトは閉鎖し調査や対策を継続している。
205	2022/1/18	届出者（企業）が管理するウェブサイトが閲覧不能になっていたことを、顧客からの連絡により認識した。サイト管理に使用していたプログラムが不正アクセスされ、ウェブサイトの動作を設定するファイルが改ざんされたことが原因であることが判明した。不正アクセスされた原因は判明していないが、サイト管理の作業時に当該プログラムが生成するファイルが、作業後にも消されずに残っていたことから、攻撃者に当該ファイルの内容を悪用されて不正アクセスされたと推測している。ウェブサイトを一時停止して、当該プログラムのアンインストール、残存していた生成ファイルの削除、脆弱性診断の受診と指摘箇所の修正を行った。再発防止策として、パスワードの変更、定期的な脆弱性診断と対策を実施する体制を構築することとした。

事例No.	届出日	概要
206	2022/1/18	届出者（企業）が管理するウェブサイトが閲覧不能になっていたことに気づき、調査を行ったところアクセス制御のためのファイル（.htaccess）が改ざんされていたことが原因と判明した。使用していた CMS（Movable Type）に脆弱性が存在していたことを確認したため、攻撃者がその脆弱性を悪用して不正アクセスし、ファイルの改ざんを行ったと推測される状況であった。ウェブサイトを一時停止して、改ざんされたファイルをバックアップから復元し、CMS の脆弱性対策を実施した上で、改めて脆弱性診断を受診して脆弱性がないことを確認した。再発防止策として、当該 CMS を使用しない構成への変更を行った上で、別のウェブサーバへ移行することを検討している。
207	2022/1/19	届出者（企業）が自身のウェブサイトの更新を行おうとしたときに、CMS（Movable Type）にアクセスできないこと、及び一部のコンテンツが改ざんされていることに気づいた。その後ウェブページの表示に異常が見られたため、ウェブサイトを閉鎖してサーバ管理会社とともに調査を行った。原因については、CMS に脆弱性が存在し、それを悪用した攻撃を受けたものと推測している。バックアップデータの復元を試みたが、作業中にバックアップのデータにも攻撃を受けた形跡が見られたため復旧作業を中止し、新たなデータを用いてウェブサイトを新規に構築することでサービスを復旧させた。再発防止策として、使用する CMS の変更を予定している。

事例No.	届出日	概要
208	2022/1/25	届出者（地方自治体）に対して、ウェブサイトが改ざんされている可能性があるとの匿名での情報提供があり、調査した結果、不正アクセスによる改ざんがされており、届出者とは無関係のコンテンツが表示される状態になっていたことが判明した。また、アクセス制御のためのファイル（.htaccess）の改ざんや、不正な PHP ファイルが設置されていたことも確認された。原因としては、脆弱性のあるバージョンの CMS（Movable Type）を使用していたため、その脆弱性を悪用した攻撃を受けたものと推測している。対策として、ウェブサイトの公開を停止して、サーバやデータベースの初期化、パスワードの変更、CMS のバージョンアップを行った上で、外部業者による脆弱性診断を受け安全性の確認を実施した。更に再発防止に向けた施策として、ウェブ改ざん検知サービスへの加入と CMS 提供元とのメンテナンス契約を行った。
209	2022/2/7	届出者（企業）のウェブページの一部がフィッシングサイトに改ざんされていたことを発見した。即座にウェブサイトを停止し、ネットワークから切断してサーバの状態等を調査した。調査の結果、外部から不正アクセスを受けていたことが判明し、その原因は、使用していた CMS（WordPress）や PHP のバージョンが古かったことから、何らかの脆弱性が存在していて攻撃者に悪用されたためと推測している。再発防止策として、サーバを移行し、最新版の CMS を用いて新たにウェブサイトを構築した。加えてアクセス元の IP アドレスの制限などを実施し、セキュリティの向上を図った。

事例No.	届出日	概要
210	2022/2/10	届出者（教育・研究機関）のウェブページの一部が閲覧不能になっていることを確認し、調査によってファイルの改ざん、バックドアの設置、サーバの遠隔操作等の被害を受けていたことが判明した。ウェブサイトのアクセスログを確認したところ、CMS（Movable Type）の脆弱性を悪用した攻撃の痕跡が見つかった。発見当時、当該 CMS は使用していなかったが、使用を停止したソフトウェアやサーバの保守に関する取り決めが明確でなかったために 4 か月ほど残置されており、攻撃を受けた。被害を発見した当日中に改ざんされたファイルの復元等を行い、一度ウェブサイトを復旧させた。しかし原因究明と対策が完了するまでウェブサイトは停止することとして、パスワードの変更やセキュリティ対策の再確認を実施した。再発防止策として、情報システムの脆弱性対策実施フローの再確認と関係者間での共有、システム管理を委託する業者とのセキュリティ対策の責任分界点の明確化を行った。また、ウェブサイトの構築や運用を委託する際の契約ひな形を作成して組織内で活用する予定としている。
211	2022/2/10	届出者（地方自治体）のウェブサーバに不審なファイルが設置されていることが発覚し、調査を行ったところ、外部から不正アクセスされた疑いが確認された。当該ウェブサーバには、当時利用していなかった古いバージョンの CMS が稼働していたため、その脆弱性を悪用した攻撃を受け、公開ディレクトリ内に不正なファイルがアップロードされたことが判明した。対応として、古い CMS は削除し、更に当該サイトは停止することとした。再発防止策として、セキュリティ情報の収集やソフトウェアアップデートを適切に行うとしている。

事例No.	届出日	概要
212	2022/3/8	届出者（企業）のウェブサーバにおいて、コンテンツ管理者が CMS（WordPress）の管理画面にアクセスできない状況になっていることに気づいた。調査により、ログインのための認証情報が改ざんされていたことと、サーバ内に不正な PHP ファイルを設置されていたことが判明した。原因は不明であるが、当該サーバは構築後ほとんど使用されておらず、CMS 等のソフトウェアが構築当初のバージョンのままになっていたことから、何らかの脆弱性が存在しており、それを悪用した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、アカウント情報の変更、PHP や CMS のバージョンアップを実施した。また、再発防止策として、定期的に CMS 及びプラグインのバージョンをアップデートする運用手順と体制を作成した。
213	2022/4/1	届出者（企業）が運営するブログが閲覧できなくなり、ウェブサイトの管理会社に調査を依頼したところ、ウェブサイトのプログラムが改ざんされていることが発覚した。調査の結果、利用していた CMS（Movable Type）の脆弱性を悪用した攻撃により、ウェブサーバ上のファイルの改ざんや不正プログラムの設置が行われたと推測される状況であった。サーバ上のファイルを全て削除した上で再構築を実施することでウェブサイトを復旧させた。ただし、過去のブログ記事はバックアップを取得していなかったため消失してしまった。再発防止策として、CMS のバージョンアップや定期的なウェブサイトのバックアップを行う運用手順を確立することとした。

事例No.	届出日	概要
214	2022/4/11	届出者（企業）のウェブページが表示されなくなっていることに気づき、調査を行った結果、不正アクセスによりウェブサーバ上のファイルが改ざんされ、更に複数の不審なファイルがサーバ上に設置されていたことが判明した。また、不正に設置されたファイルの一部にはメール送信機能があり、不正なメールの配信に悪用されていて、メールの滞留が発生していたことも確認された。レンタルサーバ事業者の調査によると、使用していた CMS（Movable Type）の脆弱性を悪用された攻撃を受けたことが原因と推測される状況であるが、詳細は不明である。対応として、ウェブコンテンツの制作会社と連携して、不審ファイルを削除した。再発防止策として、今後は CMS を利用しない方針として Movable Type を削除した。またサーバの EV SSL 認証設定等を行った。
215	2022/5/19	届出者（企業）が運営するウェブサーバから不審なメールが送信されているとの連絡がホスティング事業者からあった。調査の結果、当該サーバ上に不正なプログラムが設置されており、不審なメールの送信に悪用されていることが判明した。届出者はウェブページ制作会社と連携して不正に設置されたファイルを削除したが、その数日後に再び設置されていたことが判明したため、ウェブサイトをお詫びページのみ表示されるように設定して、その他のコンテンツは全て削除した。不正なファイルが設置された原因は、使用していた CMS（Movable Type）の脆弱性（CVE-2021-20837）を悪用されたことと推測している。再発防止策として、セキュリティが強化された IaaS 環境への移行と、社内の運用体制の見直し等を実施した。
216	2022/6/18	届出者（一般団体）のウェブサイトの管理用ページに異常な表示があることを従業員が発見し、ウェブサイトの管理業者にて調査したところ、外部から改ざんされていたことが判明した。原因は不明だが、使用していた CMS（WordPress）が最新ではなかったため、何らかの脆弱性が存在していて攻撃者に悪用された恐れがある。ウェブサイトの管理ツールを使用して復旧作業を行うとともに、管理者パスワードの変更、CMS を含むソフトウェアのバージョンアップを行い、再発防止を図った。

事例 No.	届出日	概要
EC ソフトウェアの脆弱性や設定不備が悪用された事例		
217	2022/1/7	EC プラットフォームのサービスを提供する届出者（企業）に対して、サービスの利用者から障害に関する問合せがあった。サーバの状態を確認したところ、サーバ上に不正なファイルが設置され、サイトの画面を作るテンプレートが改ざんされていることを発見した。更に個人情報やクレジットカード情報等が漏えいした可能性があることも確認された。原因はクロスサイトスクリプティングの脆弱性を悪用されたものと推測しているが、詳細は不明である。本件への対応として、WAF の導入、IPS とウイルスチェックサービスの運用拡充、新たな不正ファイル検知機能の追加等を実施した。
218	2022/1/29	EC サイトを運営する届出者（企業）に対し、決済代行サービス会社から、クレジットカード不正利用の疑いがあるためカード決済を停止する旨の連絡があった。EC サービス提供事業者が調査したところ、不正アクセスの可能性があることが発覚し、15,000 件以上の EC サイト利用者のカード情報や個人情報が漏えいした可能性があることが判明した。EC サイトを停止して外部専門機関によるフォレンジック調査を実施した結果、EC システムに脆弱性が存在しており、注文データに不正なスクリプトが含まれていると、管理画面で当該データを表示した際にスクリプトが実行され、サーバ内に不正なプログラムのファイルが生成される仕組みになっていたことが判明した。対応として不正なファイルの削除と EC システムの脆弱性の解消を行い、再発防止策として WAF の導入、不正ファイル設置の監視機能の導入を行った。更に個人情報の暗号化や管理画面からファイル更新機能の削除といったプログラムの改修、サイバー保険の見直し等を検討している。

事例No.	届出日	概要
219	2022/3/17	決済代行会社から、届出者（企業）が運営するECサイトで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の連絡があった。調査したところ、当該ECサイトのシステムにクロスサイトスクリプティングの脆弱性が存在し、それを悪用した攻撃を受け、顧客のカード情報約3千件が漏えいした恐れがあることが判明した。本件への対応として、フォレンジック調査により原因の解明とその対策を講じた後、脆弱性診断を実施して脆弱な箇所がないことを確認した。また、再発防止策としてセキュリティソフトの導入、及び管理画面ログイン時における二段階認証の導入を予定している。
220	2022/6/8	届出者（企業）が運営するECサイトにおいて、クレジットカード情報が漏えいしている恐れがあるとの連絡を決済代行会社から受けた。外部機関に依頼して調査した結果、海外からCMS（EC-CUBE）の脆弱性を悪用した攻撃を受けて、当該ECサイトから3,000件近くのカード情報を窃取されていたことが判明した。発覚後、ECサイトは停止し、情報が漏えいした顧客へのお詫びなどを行った。再発防止策として、WAFの導入、海外からのアクセス制限、改ざん検知機能等を導入した新たなECサイトを構築している。
221	2022/6/16	届出者（企業）が運営するECサイトにおいて、クレジットカード情報が漏えいしている恐れがあるとの連絡を外部から受けた。外部のセキュリティ専門業者による調査の結果、ECサイトを含む複数のウェブサイトが不正アクセスを受け、5,000件以上の個人情報と400件以上のクレジットカード情報が漏えいしている可能性があることが判明した。CMS（EC-CUBE）の脆弱性を悪用した攻撃により外部から不正にアクセスされ、バックドア等の不正ファイルの設置や既存ファイルの改ざん等が行われたとのことだった。再発防止策として、ウェブサイトの脆弱性検知や改ざん検知の仕組みの導入、CMSのバージョンアップ等の保守業務をベンダに委託する等の対策を行った。また、サーバ内に個人情報を保持しない構成への変更、定期的なログ監査の実施についても検討している。

事例 No.	届出日	概要
SQL インジェクション攻撃を受けた事例		
222	2022/1/26	届出者（企業）が提供する決済管理サービスのシステムに不正アクセスがあり、数十万件のカード情報や個人情報が漏えいしたことが、クレジットカード会社からの連絡により発覚した。調査により、SQL インジェクションの脆弱性を悪用した攻撃が半年間近くにわたって行われていたことが判明した。本件の発覚後にはクレジット決済を停止した上で、調査会社にフォレンジック調査を依頼するとともに、並行して情報流出が懸念される顧客や関係機関への報告を行った。調査の結果、アプリケーションのエスケープ処理に不十分な点があったことが原因と判明した。再発防止に向けた対策として、管理画面への接続制限と認証の強化、システム構成の見直し、脆弱性が生じていたエスケープ処理の修正、ファイアウォールによる IP アドレスフィルタリング、及び IPS 等の検知ルールと体制の見直しを行った。更に SIEM の導入による監視の強化も実施する予定である。なお、顧客対応等の費用も含めると、被害額は 1 億円を超える見込みである。
223	2022/2/2	届出者（企業）のウェブサーバに異常な負荷が発生していることを、サーバ運用管理業者が発見した。調査により、自社製プログラムに存在した SQL インジェクションの脆弱性を悪用した攻撃を受け、サーバの CPU 稼働率が 100%に達していたことが確認された。更に調査した結果、この攻撃により顧客のメールアドレス約 10 万件が窃取されていたことが判明した。本件への対策として、脆弱性が存在した自社製プログラムの使用を禁止した。また、本件に関する問い合わせ窓口を設置し顧客対応を行った。再発防止策として、WAF 製品の追加導入やシステム倫理委員会の設置等を行うとしている。

事例No.	届出日	概要
224	2022/3/7	届出者（企業）が提供するサービスの利用者から、当該サービスでのみ利用しているメールアドレスに対してフィッシングメールを受信したとの問い合わせがあった。調査したところ、ウェブシステムに SQL インジェクションの脆弱性が存在し、それを悪用した攻撃によりシステム内の情報が窃取されていたことが判明した。本件への対応として、プログラムを修正して脆弱性を解消し、WAF の設定追加によるアクセス制御を行った。再発防止に向け、データの保持方針の見直しを行い、古いデータは公開サーバに置かず、アクセス制限された環境へ退避することとした。更に他のウェブシステムについても脆弱性診断と WAF の設定追加を行い、脆弱性への対応ができていることを確認した。
225	2022/3/7	届出者（企業）のウェブサイトが DoS 攻撃により一時的にサービス停止した。 攻撃元からの通信を遮断することによりサービスは復旧したが、アクセスログを解析した結果、当該の通信はウェブページに存在した SQL インジェクションの脆弱性を悪用した攻撃であったことを確認した。影響範囲の調査により、2 万以上のメールアドレスなどの情報が漏えいした恐れがあることが判明した。発覚した当日中に脆弱性を解消する対策を行った。また、再発防止策として、ウェブページが取得するデータ項目を見直して必要最小限になるように修正を行った。更に不正アクセス監視体制の強化、ウェブページ公開時のセキュリティチェックの強化を検討している。

事例 No.	届出日	概要
226	2022/3/14	届出者（企業）の会員向けサービスのサーバにおいて、空きストレージ容量の逼迫を検知した。サーバ状態を確認したところ、大量のアクセスによるアクセスログの肥大化によることが判明した。更に調査を行った結果、大量のアクセスは同一の接続元 IP アドレスから行われた攻撃の通信であったことが判明し、ウェブシステムに SQL インジェクションの脆弱性が存在していたため一部の攻撃が成功して、サーバ上のデータベースに保管していた情報が漏えいした恐れがあることが発覚した。脆弱性が存在したウェブページは削除した上で、不正アクセスの発信元 IP アドレスからの通信は遮断するように設定して対策を行った。再発防止策として、プログラムの改修により不正なリクエストがあったときの処理を改善した。また WAF の導入、IPS・IDS の設定見直しによりセキュリティ強化を図った。
227	2022/5/25	届出者（企業）が提供するサービスにおいて、サーバが高負荷状態にあることを監視ツールが検知した。システム開発・運用を行う事業者とともに調査を行ったところ、外部から SQL インジェクション攻撃が行われていたために負荷が高騰したものと推定される状況であった。攻撃により、サービス利用者のメールアドレスが漏えいした恐れがあるが、詳細は調査中である。発覚後、すぐにサービスを停止し、SQL インジェクションの脆弱性が存在した箇所は処理を変更する修正を行った。再発防止策として、全ウェブページに対して脆弱性診断を実施し、脆弱性が見つかった箇所は対策を行った。また WAF の導入、及び WAF の運用サービスの導入を行い、ネットワーク上での対策を追加することを検討中である。
Log4j の脆弱性を悪用された事例		

事例No.	届出日	概要
228	2022/1/20	届出者（企業）が使用するネットワークにおいて、セキュリティソフトが不正な通信を検知した。調査により、組織内のサーバにLog4j の脆弱性が存在し、それを悪用した不正アクセスによりマイニングツールの一種を不正に設置されたと推測される状況であった。通信ログ等からマイニングツールが設置されたサーバを特定して駆除を行った上で、Log4j の脆弱性対策と OS の更新、サーバのパスワード変更、ファイアウォールや IPS による不正通信先との通信遮断を行った。再発防止に向け、修正プログラム適用ルールの見直しを行う予定である。
229	2022/3/17	届出者（企業）が VDI システムのゲートウェイサーバ及びコネクションサーバに対して、Log4j の脆弱性対策の修正プログラムを適用しようとしたところ、既に脆弱性が悪用された侵害をされている恐れがあることの通知がされた。サーバをネットワークから切断して、セキュリティベンダにフォレンジック調査を依頼して調べたところ、Log4j の脆弱性を悪用した改ざんによりバックドアが作成されていたことが判明した。ただし、それ以上の攻撃の形跡や、情報漏えいの痕跡は確認されなかった。本件への対応として、サーバを再構築した上で修正プログラムを適用して脆弱性の解消を行った。また再発防止策として、脆弱性管理ツールの導入、ファイアウォールに設定を追加して監視を強化することとした。
その他、脆弱性や設定不備を悪用された事例		
230	2022/4/15	届出者（企業）がシステム構築・管理し、顧客向けに提供していたメールサービスにおいて、設定変更時の作業不備により送信メールサーバがオープンリレー可能な状態になっており、大量のスパムメール送信に悪用された。設定不備を修正するまでの約 3 時間で数十万件のスパムメールが不正に中継された。更にこの影響を受け、当該メールサーバが受信拒否リストに追加されたことにより、約 2 日間サービス利用者がメールを送信できない状態となった。設定ミスの再発防止策として、二重チェックの徹底や、作業記録の音声・動画による保存等を実施する予定としている。

事例No.	届出日	概要
231	2022/3/22	届出者（3 地方自治体）が使用する送信メールサーバが悪用されて、送信者を届出者のメールアドレスに装った大量のスパムメールが送信された。その影響で当該サーバが受信拒否リストに登録されてしまい、届出者が正規のメールを送信することもできなくなった。調査により、送信メールサーバに設定不備がありオープンリレー可能な状態となっていたことで、大量のメール送信に悪用されていたことが原因であった。また、設定不備が生じたのは、サーバ管理を委託していた業者が、保守管理作業を実施した際に設定ミスがあったことによるものであった。本件を受けて、届出者は委託先事業者に対し作業チェック体制の強化、メールの不正中継の監視を行うように指示した。
232	2022/3/31	
233	2022/4/19	
234	2022/1/24	届出者（企業）の管理するウェブサイトが不正アクセスを受け、不正なスクリプトを設置されて実行された。セキュリティ業務を運用する業者が、IPS が外部から不正なコマンドを実行する通信を検知し、サーバ上に不審なファイルが存在していることを発見して届出者に連絡した。調査の結果、現在利用していないウェブサーバが停止されず公開された状態になっており、当該サーバに存在していたブログエンジンの脆弱性を攻撃者に悪用されて、WebShell と呼ばれるツールなどを設置され、サーバ上の情報を窃取されていたことが判明した。発覚後の対応として、当該サーバは停止したのち、初期化と再構築を実施した。再発防止策として、社内のサーバ等に対して類似の状態のものがないかの確認を行った。更に WAF 等の導入によりセキュリティ向上を図ることを検討している。

事例No.	届出日	概要
235	2022/5/23	届出者（企業）が利用しているファイルサーバにおいて、パフォーマンスの悪化が見られたため、調査したところ、ファイルサーバ上で不正なプログラムが動作していることが確認された。サーバのネットワーク通信を遮断し、不正プログラムは強制停止を行った。専門業者によるフォレンジック調査を行った結果、業務システムの検証用に利用している外部公開サーバが、プログラムの脆弱性を悪用した攻撃を受け、ファイルサーバ上に社内ネットワークの侵害を行うためのツールなどを設置されていたことが判明した。攻撃者は、ファイルサーバ上のファイル窃取を図ったとみられるが、実際に情報が漏えいしたかどうかは不明であった。本件を受け、パスワードの変更や、社内に類似の脅威がないかの確認を行い、更に監視項目や内容を見直して監視強化を図った。また、情報セキュリティ対策を行うための組織を新設した。
236	2022/6/3	ウェブサーバ・コンテンツの運用を行う届出者（企業）が、運用作業を受託していた顧客のウェブサイトが表示されなくなったため、サーバの状態を確認したところ、ファイルの改ざんや不正ファイルの設置、サーバの構成情報が外部から閲覧できる状態にあったことが確認された。原因は不明だが、何らかの方法で認証情報を取得した攻撃者が、当該サーバに不正アクセスしてサーバを操作した可能性がある。対応として、サイトを一時閉鎖して、バックアップデータを用いて被害発覚前日の状態に復元した。更に CMS のアップデートや FTP のパスワード変更を実施した。再発防止策として、 脆弱性診断ツールやアクセス制限用のツールを導入するとしている。

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

利用者やシステム管理者による ID やパスワード運用・管理の問題による不正アクセス被害の届出は、今期は 16 件と先期以前と比較すると少なかった。なお、VPN 装置など、脆弱性を悪用した攻撃で窃取された ID やパスワードにより、認証を突破されたと考えられる事例は 2-2 節や 2-3 節に分類しており、本節には含めていない。

今期に目立ったのは、届出者が、ブルートフォース攻撃（総当たり攻撃）により、認証を突破されたことが不正アクセスの原因と推定している事例である。ID とパスワードによる認証システムに対して不正なログインを試みる攻撃には、ブルートフォース攻撃の他にも、過去に何らかの理由で漏えいした ID とパスワードの組合せを不正に入手して、ログインを試行するパスワードリスト攻撃などがある。アクセスログや認証成否のログなどから、攻撃の種類を推定することは可能だが、正確に攻撃の種類を特定することは難しい。それにもかかわらず、届出者がブルートフォース攻撃であったと判断したのは、パスワードが、文字数の少ない単純な文字列であった、ID と類似した文字列であったなど、強度の弱いパスワードを使用していたことが発覚し、そのアカウントが、不正アクセスに使用されたことが判明したためとのことであった。

多要素認証を使用しておらず、ID・パスワード認証のみで利用可能としているシステムにおいては、当然ながら不正アクセスの防止は ID とパスワードの管理方法が重要な要素となる。いわゆる「強力な」パスワードを設定することに加えて、弱いパスワードが設定されたまま、現在使用していない古いアカウントが有効になっていないかなど、アカウント（ID）の管理方法についても見直しを勧める。

ID・パスワード認証を突破された事例とは異なるが、クラウドサービスへのアクセスキーを窃取されて不正アクセスに遭ったとの届出もあった。ID・パスワードに限らず、サービス利用のための認証に必要となる情報は、厳重に管理することが必要である。

あわせて可能であればアクセス制限や多要素認証など他の技術も組み合わせ、セキュリティ強化を図ることが望ましい。複数の技術を組み合わせたセキュリティ対策を行っても完全に不正アクセスを防げるような万全のものにはなり得ないが、パスワードのみといった単一の認証方式に比べ、セキュリティを大幅に向上することができる。積極的に導入を検討していただきたい。

表 2-5 に ID とパスワードによる認証を突破された不正アクセスに関する届出の概要一覧を示す。この中で、クラウドサービスのアクセスキーが漏えいして、クラウドストレージのデータを不正に操作された事例（事例 No.249）の詳細を 5 章で紹介する。

表 2-5 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

事例 No.	届出日	概要
237	2022/1/6	届出者（企業）の EC サイトにて、正規会員になりすました不正な注文が複数回行われた。限度額を超えた注文で、通常とは異なる配送先が指定されていたことから、当該会員に確認したところ本人に心当たりがないとのことで、不正アクセスが発覚した。発覚後、すぐに出荷処理を停止したため金銭的な被害は未然に防ぐことができた。不正アクセスの原因は、攻撃者が何らかの方法で当該会員の ID とパスワードを窃取し不正に使用したことであるが、届出者のシステムから漏えいした痕跡はないため、当該会員がパスワードを他のサービスと共通にしていてそちらから漏えいした、簡易な文字列で推測されやすかったなど、パスワードが脆弱であった可能性を考えている。対策として、注文情報を監視して本件と同様の配送先が指定された注文は一時停止し確認を行うようにしている。また再発防止策として、会員向けにパスワード設定に関する注意喚起を行った。
238	2022/1/11	届出者（企業）のメールアカウントが不正アクセスを受け、約 9 万件のフィッシングメールが送信された。届出者が利用するメールサーバ会社がメールの滞留を検知し、調査したところ、海外の IP アドレスから不正アクセスがあり、大量に不正なメールを送信されていたことが原因であることが確認された。不正アクセスされた原因は不明だが、フィッシングによるアカウント情報の詐取や、パスワードが簡易だったり使い回ししていたりしたこと等により、攻撃者に推測されてしまったことなどが考えられる。再発防止策として、被害に遭ったアカウントとリスクが高いと判断されたメールアカウントについて、パスワードを堅牢なものへ変更した。更に全社員に向けて、不審なウェブサイトやメールを不用意に開かないことの徹底と、適切なパスワードの設定方法を周知するなどの対応を行った。

事例No.	届出日	概要
239	2022/1/13	届出者（教育・研究機関）のメールアカウントから、多数のフィッシングメールが送信された。更にメールの受信者の一部はそのメールからフィッシングサイトへ誘導され ID やパスワードを入力してしまったため、認証情報を詐取された恐れがある。攻撃者は事前に届出者のドメインを模したフィッシングサイトを作成していて、その URL を記したメールを届出者のメールアカウントから送信することにより、正規のメール・ウェブサイトを装っていた。認証情報が詐取された恐れのある全てのアカウントに対してパスワードの強制リセットを実施し、またフィッシングサイトへのアクセスを遮断することで対策した。再発防止策として、多要素認証の導入を検討している。
240	2022/1/28	届出者（教育・研究機関）の 1 つのメールアカウントに不正なログインがあり、約 2,500 通のメールが外部へ送信された。大量メール送信を監視していたため事態を認識した。不正アクセスの原因は、当該アカウントのパスワードに、利用者の氏名の文字列を含むパスワードが設定されていたため、攻撃者にパスワードを推測されたことが考えられる。氏名を含むパスワードは設定できないパスワードポリシーとしていたが、当該アカウントのパスワードはポリシーの更新前から変更されていなかったため、古いポリシーのままの脆弱なパスワードになっていた。対策として、当該アカウントのパスワードを変更することで大量メール送付を遮断した。また、再発防止策として、アカウント利用者全員へのパスワード変更を促した。
241	2022/2/9	届出者（企業）のメールアカウントが不正アクセスされ、大量のメール送信に悪用された。当該アカウントは部署で使用していた共有のアカウントであり、配送エラーを通知するメールが大量に着信したことに気づき、本件が発覚した。攻撃者が何らかの手段によりメールアカウントの認証を突破して不正なメールの大量送信を行ったと考えられるが、原因は不明である。再発防止に向けた対策として、文字数を増やした複雑なパスワードに変更した。

事例No.	届出日	概要
242	2022/2/16	届出者（地方自治体）のメールサーバに不正アクセスがあり、大量のメール送信に悪用された。メール送信業務を担う業者が発見し、連絡を受け届出者が認知した。調査により、約 3 日間に 30 万通以上の当選詐欺等の不審なメールが送付されていたことが判明した。原因は、SMTP サーバに対する外部からのアクセス制限がされていなかったことと、メールアカウントの ID やパスワードが簡易であったことであり、攻撃者に認証情報を推定されてしまい、外部からメールの不正中継に悪用されたものと考えている。メールアカウントのパスワードを変更し、ファイアウォール等によりアクセス制限やメールリレー制限を施した上でメールサーバを復旧させた。
243	2022/3/2	届出者（企業）が運営するウェブサイトの管理画面にエラーが表示されていることをシステム管理者が発見した。調査したところ、約 3 万の発信元から数百万回にも及ぶ不正ログイン試行が行われており、そのログ等でディスクの空き容量が枯渇したことによるものであることが判明した。総当たり攻撃またはパスワードリスト攻撃を受けたものと推測している。本件への対応として、機械的な大量のアクセスを遮断するシステムを導入するとともに、不正なログインに成功された恐れのあるアカウントについてはパスワードをリセットした。また緊急対策本部を設置してフォレンジック調査や監督省庁への報告などを行い、利用者に対してはパスワードの使い回しに関する注意喚起を行った。再発防止策として、多段階認証の仕組みを導入するとしている。

事例No.	届出日	概要
244	2022/3/7	EC サイトにおいて、届出者（企業）が使用していたアカウントが不正使用され、届出者とは無関係の注文が行われた。EC サイトの運営会社が当該の注文を不審に思い、届出者に確認した上で注文処理を停止したため被害は生じなかった。アカウントが不正使用された原因は判明していないが、届出者は他のサービスで使用していたものと同一のパスワードを本 EC サイトでも使用していたため、攻撃者に何らかの手段で認証情報を不正に取得された恐れがあると考えている。再発防止策として、外部サービスで使用するパスワードは使い回しを避け、かつ長く複雑なものとし、定期的にパスワード変更するように社内のセキュリティポリシーを定めた。
245	2022/3/9	届出者（教育・研究機関）のメールアドレスを送信者に装った、不審なメールが大量に発見された。調査の結果、約 7 カ月間にわたって、海外の IP アドレスから届出者のメールサーバに対して、不正にログインを試行した形跡があり、3 つのアカウントについて不正ログインに成功されていたことが判明した。不正なメールの送信に悪用されたことに加え、当該アカウントのメールやアドレス帳などの情報を不正に閲覧された恐れがある。不正アクセスの原因は明確にはなっていないが、2 つのアカウントについてはログ等から総当たり攻撃によるもの、1 つのアカウントでは他サービスと同一のパスワードを使い回していたことから、パスワードリスト攻撃によりパスワード認証が突破されたと推測される状況であった。再発防止策として、総当たり攻撃の対策の強化、多要素認証の導入、情報セキュリティに関する研修の強化を検討している。

事例No.	届出日	概要
246	2022/3/14	届出者（教育・研究機関）の複数の職員のメールアカウントに海外の IP アドレスから不正にログインされ、過去に送受信したメール等の不正な閲覧や、送信者を職員に装った、なりすましメールの送付が行われた。不正に閲覧されたメールには関係者の個人情報が含まれていた。原因は、フィッシングのメールを受信した職員が、そのメールから誘導されたサイトへ ID やパスワードを入力したことがあることが判明したため、攻撃者がフィッシングサイトを使用して認証情報を詐取したことによると考えている。対策として、認証情報が詐取されたと考えられるメールアカウントを無効化した。また、再発防止策として、セキュリティ教育の強化と多要素認証の導入を行った。
247	2022/3/18	届出者（公共機関）が使用するメールアカウントに不正なログインがあり、外部への不正なメールの送信に悪用された。当該メールアカウントのパスワードが比較的簡易なものであったことから、総当たり攻撃などによりメールアカウントの認証を突破されて不正アクセスされたと考えられる状況であった。対策として、メールアドレスとパスワードの変更を行い、メールアドレスは関係者以外に開示しないこととした。また、再発防止策として、パスワードの複雑化と定期的な変更をルール化し徹底することとした。
248	2022/4/14	届出者（教育・研究機関）が所有するサーバを保守運用していた業者が、サーバの認証ログに不審な ID でのアクセスがあることを発見した。調査した結果、当該サーバに不正アクセスがあり、同じ ID でログインが可能だった他の数台のサーバに不正アクセスされ、コインマイナーが不正に設置されていたことが判明した。不正アクセスの原因は、総当たり攻撃によりパスワード認証が突破されたものと推定している。本件への対応として、対象のサーバは初期化して再構築した。また再発防止策として、通信許可設定の見直し、利用可能な ID の棚卸し、組織内への注意喚起等を実施した。

事例No.	届出日	概要
249	2022/5/9	届出者（企業）がクラウド上に構築していた業務システムに不正アクセスがあり、クラウドストレージに保存していた情報が削除された。運用業務の委託先事業者が発見した。調査したところ、攻撃者が何らかの手段で不正に入手したクラウドサービスへのアクセスキーを悪用し、外部ネットワークからの API を経由してクラウドストレージ上のデータを削除していたことが判明した。なお、複数のアクセスキーが不正に使用されたことがわかっているが、攻撃者がキーを窃取した手口は不明である。不正使用されたアクセスキーを無効化し、外部からのアクセスを遮断する対策を行ったのちに、被害にあったシステムとは別のシステムにあったデータを用いてデータの復旧を行った。ただし一部のデータはバックアップを取得しておらず復元できなかった。再発防止に向け、データ削除を行うロールの限定や多要素認証の導入、ログ管理や不正アクセス監視の機能の適用による監視の強化等を行った。
250	2022/5/18	届出者（研究・教育機関）のウェブサーバのサイト管理ページに不正アクセスがあり、同サーバ上に構築されていた約 50 のウェブサイトが改ざんされ、届出者とは無関係なサイトに誘導される状態になっていた。管理者が改ざんを発見し、直ちにサーバを停止して調査会社とともに調査を行ったところ、不正アクセスの原因は、管理ページの URL が CMS の初期状態のままであったこと、比較的簡易なパスワードを設定していたこと等から、長い時間をかけた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。一度ウェブサイトを復旧させたが、再び管理ページに対する総当たり攻撃を検知したため、再度サーバを停止して管理用パスワードの変更と、管理ページへのアクセスを組織内からのみに限定するアクセス制限を行った。完全な復旧までに 6 日間を要した。

事例No.	届出日	概要
251	2022/6/9	届出者（企業）が送信するほとんどのメールが不達となり、エラーとして返送される事態が発生した。調査したところ、届出者が利用するメールアカウントの１つが不正アクセスされ、約５万件という大量の迷惑メール送信に悪用されたことにより、送信メールサーバがブラックリストに登録され、届出者企業から送信されるメールが不正なメールとして判定されるようになっ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のパスワードが、アカウント名から容易に推測できるような簡易なものになっていたためと考えている。本件を受け、当該メールアカウントは削除し、その後のアカウントへのログイン試行がないか監視を行うとともに、ブラックリスト登録解除の申請を行った。再発防止策として、別のメールサーバへの移行や、利用実態を踏まえたメールアカウント管理を行うことを検討している。
252	2022/6/15	届出者（地方自治体）の一部のウェブページが改ざんされ、複数の不審な URL リンクが掲載されていることを確認した。ウェブサイトを一時閉鎖して調査したところ、特定のページに海外のオンラインカジノの関係と見られる URL が大量に書き込まれていた。原因は、当該ページの編集用として過去に使用していたアカウントが、脆弱なパスワードのまま残存していたことから、総当たり攻撃等で認証を突破されてしまったためと推測される状況であった。バックアップからデータ復元し、当該アカウントを含む全アカウントのパスワードを変更してからウェブサイトの公開を再開した。更に再発防止策として、ウェブサイトの管理ページアクセス時の認証の追加、組織内からのみに接続を限定するアクセス制限を行った。

2-5. その他

その他、ここまでの分類に該当しない届出事例を表 2-6 に示す。調査等を行っても被害の詳細や原因が判明しなかったもの、及び本紙の作成時点で調査を継続しているものについても本節に分類した。届出者では原因不明とされたものであっても、中には、ソフトウェアの脆弱性の悪用や、パスワードなど認証情報の管理上の問題に起因していると推測される事例も見られた。直接的な原因は異なっていたとしても、前節までで述べてきた対策を行うことは、セキュリティ向上につながり、ウイルスや不正アクセス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、2-3 節や 2-4 節の内容も参考にしていただきたい。

表 2-6 その他の届出事例の概要一覧

事例 No.	届出日	概要
253	2022/1/7	届出者（企業）のファイルサーバに不正アクセスがあり、サーバに保存していた個人情報等を含むデータを不正に閲覧された。なお情報が外部に漏えいした形跡は確認されなかった。海外拠点のサーバを経由して国内のサーバにアクセスされた形跡が見つかったが、侵入された原因やサーバのアクセス権を窃取された手口等は不明である。ファイルサーバ利用者のパスワードをリセットし、サーバアクセスの監視の強化を行った。外部のセキュリティ事業者とともに詳細な調査や再発防止策の検討を実施している。
254	2022/1/21	届出者（一般団体）がウェブサイト運営のために使用していたサーバが不正アクセスされ、不正なメールが約 2 万件送信された。当該サーバ上で稼働していたウェブサイトは停止して、新たに別のウェブサイトを作成して移行することとした。

事例No.	届出日	概要
255	2022/1/26	届出者（企業）が使用するウェブアプリケーションの動作速度が低下していたため、レンタルサーバの状態を確認したところ、通常時は生じない異常な高負荷になっていることを確認した。調査を行ったところ、コインマイナーの一種が不正に設置され、マイニングと送金を行う処理が稼働していたことが判明した。不正アクセスの原因は不明である。なお、CPU 等のリソースを不正に使用されたこと以外の被害は見つかっていない。コインマイナー自体とコインマイナーが不正に作成したり改ざんしたりしたファイル等は削除または修正し、リソースの状態が正常値に戻ったことを確認した。再発防止の対策として、ツールが使用していたと思われる通信を遮断する設定を行った。
256	2022/1/27	届出者（一般団体）が過去に使用していたウェブサーバが不正アクセスを受け、ファイル改ざんや不正なプログラムの埋め込みがされた結果、届出者とは関係のない内容のウェブページが表示されるようにされていた。外部からの情報提供により発覚した。届出者のウェブシステムは新しいサーバに移行済みで、攻撃を受けた古いウェブサーバは使用していなかったが停止させずに稼働している状態にあった。詳しい原因は不明だが、修正プログラムの適用等が行われていなかったため、CMS 等に脆弱性が存在していて、それを悪用された恐れが考えられる。対策として、保守業者とともにアクセス制御のためのファイル（.htaccess）など改ざんされたファイルの修正や不要なファイルの削除を行った。再発防止策として、パスワードの変更を行った。
257	2022/3/8	届出者（企業）が使用するメールアカウントからのメール送信ができなくなった。メールサービスの事業者に確認したところ、当該アカウントから多数の不審なメールが送信されており、不正アクセスまたはウイルス感染が疑われたため、メール送信を制限したとのことであった。原因は不明である。再発防止のため、本件を全従業員に共有した。また、セキュリティ体制の強化を予定している。

事例 No.	届出日	概要
258	2022/3/11	届出者（教育・研究機関）の組織内で利用していたパソコンから、海外の IP アドレスに対して意図しない通信が発生していることを、組織内の IPS が検知した。当該通信は IPS が遮断した。通信の発信元となったパソコンの利用者へ連絡しネットワークから切断して、セキュリティソフトによりウイルススキャンを行ったがウイルスは検知されなかった。そのため通信が発生していた原因は不明であるが、何らかの未知のウイルスに感染したものと届出者は推測している。
259	2022/3/24	社外の組織より、届出者（企業）のパソコンが、フリーマーケットサイトの悪用被害の踏み台にされている恐れがあるとの報告があった。社内で調査を行ったところ、社内のパソコンに MaskVPN という VPN ソフトウェアが使用者の意図なくインストールされていたこと、及び当該パソコンがフリーマーケットサイトへの踏み台として悪用されていたことが判明した。MaskVPN がインストールされた原因等については専門業者にフォレンジック調査を依頼して調査中である。
260	2022/4/6	届出者（企業）の管理者に対して、従業員から自分のパソコンが遠隔操作されているとの報告があった。当該のパソコンをセキュリティソフトでスキャンしたところ、2 つのファイルが不審と判定された。しかし、それらのファイルをセキュリティ専門業者で詳細に調査したが、不審な点は認められず、原因や被害内容は不明である。当該のパソコンは初期化して再構築を行った。
261	2022/4/13	届出者（教育・研究機関）の職員が自宅でテレワークをしていた際に、パソコンに偽のセキュリティ警告画面が表示された。職員は偽物と気づかずに、画面に表示された電話番号に連絡して指示通りに操作したところ、パソコンを遠隔操作するソフトウェアがインストールされた。その後、実際に遠隔操作を行われて、有料のセキュリティソフトを購入するよう案内されたため、サポート詐欺であると判断した。関係機関への連絡と調査を行った結果、パソコンに保存されていたデータ等の流出は確認されなかったが、画面に表示していた情報が読み取られた可能性があるため、関係者への連絡と謝罪を行った。

事例No.	届出日	概要
262	2022/4/27	届出者（企業）が利用するパソコンの画面に偽のセキュリティ警告画面が表示された。届出者は警告画面に記載されている偽のサポート連絡先に電話連絡し、指示に従ってしまったことで、外部からの遠隔操作を可能にするソフトウェアをインストールされる等の被害に遭った。なお、届出者は電話の途中でサポートを名乗る偽の担当者の言葉遣いや指示内容を不審に思ったため、パソコンをネットワークから切断した。その後、専門業者や外部機関へ連絡・相談し、パソコンの再設定やセキュリティソフトの更新等を行った。再発防止策として、類似の事案が生じないよう、社員向けにセキュリティ講習を行い、周知を図るとしている。
263	2022/6/24	届出者（企業）を送信者に装ったなりすましのメールが取引先に送られた。ウイルスに感染したと考えているが詳細は不明である。

3. 事例：複数の脆弱性と BitLocker を悪用した侵入型ランサムウェア攻撃

3-1. 届出内容

（1）　発見経緯

届出者（企業）の社員より、利用しているパソコンの BitLocker が有効にされたとの連絡があった。それとは別に、社内システムへの接続不可に関する問い合わせが寄せられるようになり、調査したところ、基幹システムのサーバを含む複数の機器のデータが BitLocker により暗号化されていることが確認された。

（2）　被害原因

VPN 装置に存在した脆弱性を悪用され、組織内ネットワークに侵入された。ネットワーク内で侵害範囲を拡大されたのは、Active Directory サーバに存在していた脆弱性を悪用されたことによる。いずれも脆弱性管理が適切に実施されていなかったために脆弱性が対策されずに残存していた。

（3）　被害内容

本件では、届出者が所有する 130 台以上の機器が、BitLocker による暗号化の被害に遭った。侵害された機器には、攻撃者からのメッセージが残されており、データを暗号化したことや攻撃者の連絡先、データの復号のために連絡を促す内容等が書かれていた。

また、暗号化の影響により、組織内ネットワークの障害と基幹システムの停止も発生しており、届出者によれば、本件の対応費用として約 6,000 万円以上の金銭的被害が生じたとのことである。

（4）　被害対応

- 関係会社・警察への報告
- サーバのログ収集と、セキュリティ専門企業への調査依頼
- バックアップをもとに Active Directory サーバを再構築して先行復旧
- 組織内ネットワークの復旧
- 暗号化の被害に遭っていない機器に対するウイルススキャン実施
- バックアップをもとに暗号化の被害に遭ったサーバを再構築して復旧、ウイルススキャン実施、アップデート
- 被害に遭ったパソコンの初期化
- 情報漏えいの有無に関するログ調査

（5）　再発防止策

- Active Directory サーバの脆弱性の修正
- 侵入の原因となった VPN 装置の使用停止と、継続利用する SSL-VPN サービスの全 ID のパスワード変更
- 利用しているネットワーク機器のファームウェアアップデート
- Active Directory サーバのグループポリシーに不審な設定がないか調査
- Active Directory サーバにおける全ての特権ユーザのパスワード変更
- 各機器におけるイベントログ設定の見直し
- サーバ保守業者に脆弱性管理を依頼し、その管理状況の確認を実施

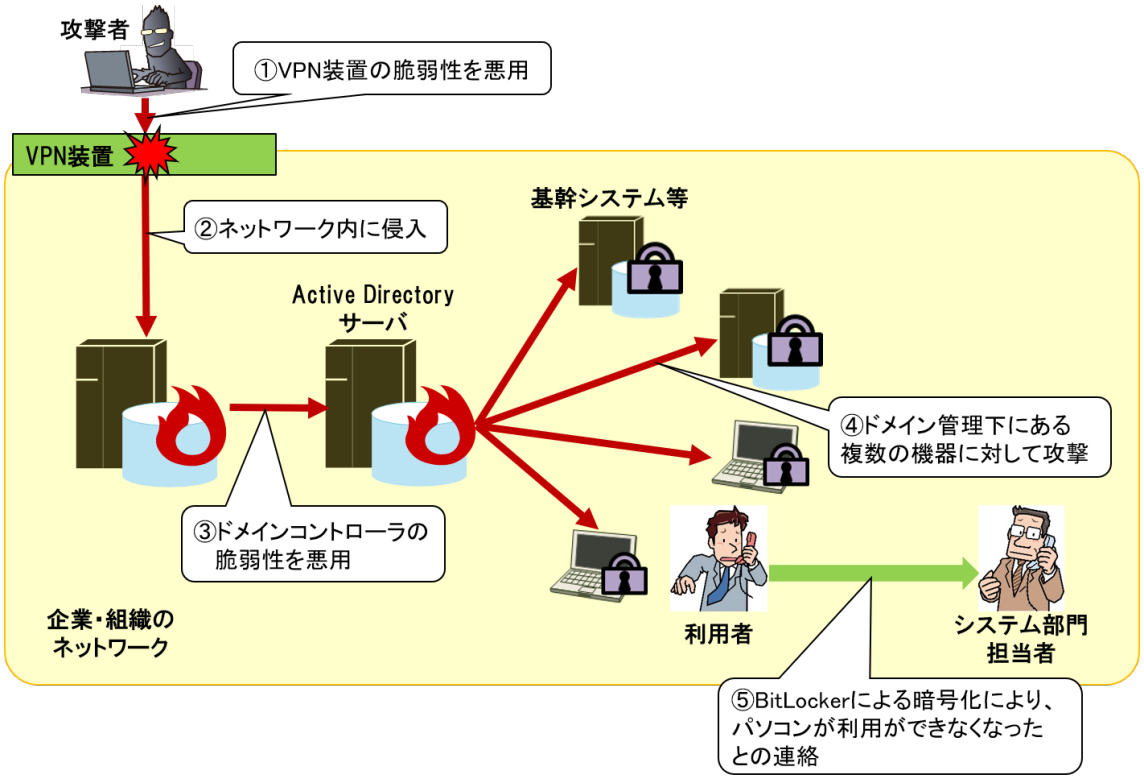

図 3-1 本事例の概要

3-2. 着目点

（1）　複数の脆弱性を悪用した攻撃

本事例は、攻撃者が組織内ネットワークへ侵入して、管理サーバ等を侵害したのち、組織内のデータを暗号化するといった侵入型ランサムウェア攻撃と呼ばれる攻撃の被害にあったものである。侵入型ランサムウェア攻撃では、①組織内ネットワークへの初期侵入、②組織内での侵害範囲拡大、③データの窃取、④データの暗号化・システム停止、⑤窃取したデータの公開（脅迫）といった流れで攻撃が行われるところ、本事例では、①組織内ネットワー

クへの初期侵入、②組織内での侵害範囲拡大において、それぞれ次の脆弱性が悪用されたとみられている。なお、本事例では、③データの窃取及び⑤窃取したデータの公開（脅迫）は確認されていない。④データの暗号化・システム停止については次項で説明する。

- Pulse Secure の脆弱性（CVE-2019-11510 もしくは CVE-2021-22893）
- Active Directory サーバにおける特権昇格の脆弱性（CVE-2020-1472）

本件の Pulse Secure の脆弱性を含む、VPN 装置の脆弱性を悪用した組織内ネットワークへの侵入については、これまでに受理した、侵入型ランサムウェア攻撃の被害の届出において多く見られた手口である。VPN 装置のようなネットワーク機器の脆弱性対応は、対策作業時にネットワークを止める必要が生じたり、不具合が発生した場合に業務に大きな影響が出たりする恐れがあるため、後回しにせざるを得ないこともあるが、脆弱性が原因で本件のような被害に遭い、更に大きな業務影響が出る恐れも踏まえ、迅速に脆弱性対応を行ってほしい。

Active Directory サーバにおける特権昇格の脆弱性（CVE-2020-1472）を悪用した組織内での侵害範囲拡大についても、これまでの侵入型ランサムウェア攻撃の被害の届出において見られた手口である。攻撃者に Active Directory サーバの侵害に成功されてしまうと、そのドメインの管理下にある機器、例えば、本件のように基幹システムを含む各機器のデータが暗号化されてしまうといった、深刻な被害が発生する恐れが考えられる。VPN 装置同様、業務影響を考慮して、対応が後回しになることがあるかもしれないが、迅速に対応を行ってほしい。また、脆弱性対応を実施することに加え、Active Directory サーバへの侵害リスクを可能な限り低減するために、単純で推測されやすいパスワードの使用、パスワードの流用、不要な権限の付与は避けることが望ましい。

なお、本件で確認された Pulse Secure の脆弱性及び Active Directory サーバにおける特権昇格の脆弱性については、数年前に開発元から公開されていた情報であり、いずれも積極的な脆弱性悪用の試みが確認されているとして、様々な組織から注意喚起が公表されていた。こういった、特に危険とされる脆弱性については、対策や修正プログラムが公開され次第速やかに対応すること、また、対応の遅れや漏れ等が発生しないよう日頃から脆弱性の管理を適切に実施できる体制を整えておくことが重要である。

（2）　正規の機能である BitLocker を悪用した暗号化

本事例では、侵入型ランサムウェア攻撃の流れの④データの暗号化・システム停止において、Windows 10 や Windows Server 2016 以降の Windows OS に標準搭載されている BitLocker を悪用され、基幹システムを含むサーバやパソコンのデータが暗号化された。

BitLocker は本来、パソコンのディスクを紛失したり盗まれたりしたとしても、第三者が情報を容易に抜き出すことができないようにするための正規の機能である。しかし、本件のように、BitLocker を悪用された場合、セキュリティ製品等でランサムウェアを検知・除外できる仕組みを備えていたとしても、BitLocker が正規のプログラムであるために検知等がされずに、本件と同様の被害に遭う可能性が考えられる。なお、BitLocker が悪用された事例としては、先期に別の組織からも、同様の暗号化被害が発生したとの届出があった。更に、企業や政府機関を標的とする攻撃グループが BitLocker を悪用していたとする情報も公開されている[12]。

本件のように正規の機能を悪用された場合であっても、暗号化されたファイルの復元は困難なため、他のランサムウェアによる暗号化被害への対策と同様に、事前にバックアップを取得しておくことが重要である。なお、攻撃者はバックアップも狙って攻撃してくる可能性があるため、バックアップは複数保持すること、オフラインで保管する等といった対策を取ることが望ましい。また、侵入型ランサムウェア攻撃では、本件のように大量の機器のデータが暗号化される恐れがあるため、データのバックアップのみにとどまらず、システムの再構築に十分なバックアップが取得できているか、復旧のための手順は整備されているか、業務継続をどのようにして行うかといったことも検討しておくことが重要である。

---

[12] NTT Com DD 株式会社
「予測不能に進化し続けるネットワークの脅威 – 最近のランサムウェアとマルウェアはどんなもの？」
https://nttcdd.jp/blog/2107/

4. 事例：Apache Log4j の脆弱性を悪用されたことによる被害

4-1. 届出内容

（1）　発見経緯

届出者（企業）が Apache Log4j（以下、Log4j）の脆弱性である、CVE-2021-44228（Log4Shell）と CVE-2021-45046 への対策として、VMware Horizon に修正プログラムを適用しようとしたところ、修正プログラムに同梱されたチェックツールが、既に脆弱性悪用による侵害がされている旨のメッセージを表示した。その後の調査で不正アクセス被害を受けていたことが発覚した。

（2）　被害原因

Log4j の脆弱性を悪用されたことが原因となる。

（3）　被害内容

本件では不正アクセスが発覚したのち、外部セキュリティベンダによるフォレンジック調査を行った。その結果、次の事項が判明している。

- VMware Horizon のアクセスゲートウェイ（Unified Access Gateway）とコネクションサーバ（Horizon Connection Server）に、Log4j の脆弱性を悪用したアクセスを受けた痕跡が認められた。
- Log4j の脆弱性を悪用したアクセスには、コインマイナーをダウンロードして実行するものや、脆弱性のスキャンを行うもの、C&C とみられる悪意のあるサーバから命令を受け実行するものなどの攻撃コードが含まれていた。期間は 2021 年 12 月 13 日から、被害が発覚した 2022 年 1 月中旬頃まで継続しており、複数の IP アドレスからアクセスが行われていた。
- コネクションサーバでは、コンテンツの改ざんによるバックドア（外部から命令を実行できるようにするためのコード）の存在が確認されたが、ウイルスのダウンロードは認められなかった。
- 組織内ネットワークでの横展開（ラテラルムーブメント）は、確認されなかった。
- 情報漏えいを示す明確な痕跡は確認されなかったが、バックドアの存在からコネクションサーバ内部の情報が漏えいした可能性は否定できない状況である。

本事例の概要図を図 4-1 に示す。

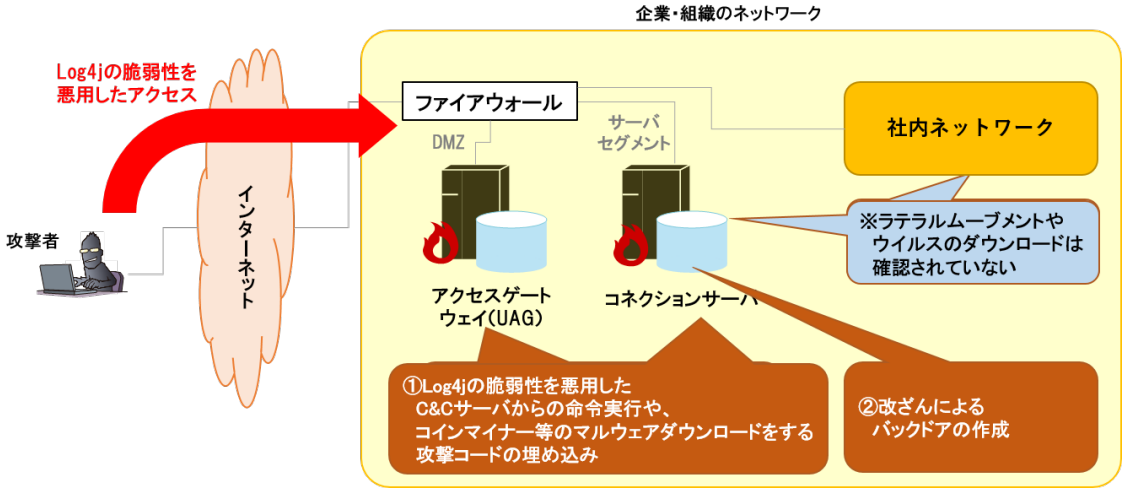

図 4-1 本事例の概要図

（4） 被害対応

- 侵害がされていて修正プログラムの適用ができなかったサーバをネットワークから切断
- システム運用事業者に、ファイアウォール等のログ解析を依頼
- 外部セキュリティベンダに、アクセスゲートウェイ及びコネクションサーバのフォレンジック調査を依頼
- フォレンジック調査結果の受領後に、侵害されたサーバを OS から再構築

（5） 再発防止策

- 侵害されたサーバの再構築時に、修正プログラムを適用
- ファイアウォールで SSL/TLS 通信を検査する機能の有効化
- 脆弱性の可視化と管理を強化するソリューションの導入

4-2. 着目点

（1） 緊急かつ広範囲に調査が及ぶ脆弱性への対応

本事例では、VMware Horizon 製品内で利用していた Log4j というオープンソースのコンポーネントの脆弱性が悪用された。Log4j は VMware Horizon 以外にも多くのソフトウェアで利用されていることや、Log4Shell の脆弱性で影響を受ける最初のバージョンが 2013 年の Log4j と古かったことなどから、幅広いソフトウェアがその影響を受けた。

Log4Shell の攻撃手口は、脆弱な Log4j が稼働する対象システムに特定の文字列と攻撃コードを送り、それをログに記録させることにより、遠隔で任意のコードを実行可能にすることである。また、2021 年 12 月 10 日に脆弱性が公表された時点で、脆弱性の検証用コー

ドが公開されていた。このため、脆弱性の公表直後から、同脆弱性の悪用を試みる通信が多数観測されている。製品ベンダや利用者には緊急の対応が求められ、利用者においては自社システムを広範囲に確認する必要があったため、利用者組織のシステム管理者に混乱が生じていたことが想像できる。

VMware Horizon 製品の対応状況に関して、VMware 社が公開した情報では 2021 年 12 月 10 日（脆弱性公表日）に、Log4Shell に関して最初の注意喚起が行われた。また、アクセスゲートウェイについては、12 月 11 日に回避策が提示され、12 月 16 日に修正プログラムが公開された。これに対して本事例では、修正プログラムの公開前となる 12 月 13 日から Log4Shell に関連した攻撃通信を受信していたことが判明しており、ゼロデイ攻撃を受けていたと言える。しかしながら、12 月 13 日から受信していた攻撃の通信は、届出者のシステムで利用していた OS とは異なる OS を攻撃対象とした通信であったため、いずれも失敗していた。その後、25 日になって初めて攻撃に成功され、バックドアを作成する改ざんがされた。脆弱性公表から数日以内で対応することは難しかったとしても、早期に回避策の実施または修正プログラムの適用ができていれば、不正アクセスによるバックドアの作成は防げた可能性が高い。

多数のシステムを運用するような組織においては、緊急でかつ広範囲の調査・対策が必要な脆弱性が発生することを想定し、対策を行うシステムの優先順位の決定や、実行する体制の整備が重要である。日頃から、自組織のシステムで利用している全ての機器やソフトウェアの把握、システムの利用目的や外部からのアクセス可否、ベンダから提供される修正プログラムの確認方法や、問い合わせ時のサポート契約の条件などを確認しておきたい。

（2）　修正プログラム適用前の侵害状況の確認

本件の届出によれば、修正プログラムを適用しようとしたところ、「既に侵害がされている」旨を示すメッセージが表示されたため侵害に気が付いたとのことだった。しかしながら、必ずしも全てのソフトウェアや修正プログラムにそのような機能があるわけではない。

また前項にも記載した通り、VMware 製品を含め、多くのソフトウェアで修正プログラムのリリース前に、Log4Shell の脆弱性が悪用した攻撃が行われていたことが推測される。早急に修正プログラムを適用した場合でも、それ以前にバックドアを設置され、そのまま気づかないこともあり得る。

自組織で利用している機器・ソフトウェアに脆弱性があり、公開情報等でその脆弱性に対してゼロデイ攻撃が報告されている場合には、修正プログラムの適用だけでなく、既にバックドアが作成されている等の攻撃による侵害がされている恐れを考慮して、当該機器の不審な動作やログ等を調査・監視することを勧める。

（3）　脆弱性有無の再点検

2021 年 12 月の脆弱性情報の公開や修正プログラムの提供開始以降も、VMware Horizon 製品の Log4Shell 脆弱性を悪用した攻撃は継続している。これを受け 2022 年 6 月には、CISA（米国 Cybersecurity and Infrastructure Security Agency）と CGCYBER（米国 United States Coast Guard Cyber Command）が、修正プログラムの適用を勧告する共同セキュリティアドバイザリー（AA22-174A）を発出している[13]。

このような勧告を出した背景には、修正プログラムが提供されてから数か月が経っても、対策が未実施のシステムが多く存在していることがうかがえる。未実施の原因としては、システム管理者や運用者が当該システムの重大な脆弱性に気づいていないケースや、何らかの理由で管理対象とされていないケース等が考えられる。

VMware Horizon 製品含め、利用しているシステムに重大な脆弱性が内在していないか、管理されていないシステムがないかなど、今一度、自組織の状況について点検してほしい。

[13] CISA「Alert (AA22-174A) Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems」https://www.cisa.gov/uscert/ncas/alerts/aa22-174a

5. 事例：AWS アクセスキーの漏えいによる Amazon S3 への不正操作被害

5-1. 届出内容

（1）　発見経緯

届出者（企業）が利用する業務システムにおいて、サーバ上のデータが削除されたことを、委託業者より報告を受けた。調査を行ったところ、当該業務システムで利用している Amazon S3（以下、S3）[14]に対して外部からの不正アクセスを受け、S3 バケット [15]を削除されたことが確認された。

（2）　被害原因

AWS のサービスを利用するための認証情報であるアクセスキーを、攻撃者が不正に入手し、外部ネットワークから API を経由して、届出者が利用する S3 にアクセスしていたことが判明した。なお、外部調査機関による調査において、4 つのアクセスキーが攻撃者によって、不正に使用されていたことが判明しているが、当該アクセスキーの漏えい原因は不明である。

（3）　被害内容

届出者が S3 に格納していた全ての情報が削除され、攻撃者によって作成されたと思われる脅迫文 [16]が残されていた。また、攻撃者は S3 のデータを読み取ることが可能であったため、格納していたデータが流出した可能性も考えられる状況であった。

攻撃により流出した可能性のあるデータは、約 5 万件以上の顧客情報及び画像データであった。

（4）　被害対応

- AWS CloudTrail[17]を利用し、不正アクセスに使用されているアクセスキーを特定して無効化
- 不正アクセスの発信元 IP アドレスからのアクセスを遮断
- マスターデータから、削除された一部の情報を復旧
- 外部調査機関による、被害や原因についての詳細な調査を実施

---

[14] AWS（Amazon Web Service）が提供するストレージサービス

[15] S3 におけるオブジェクト（データ）を保存する場所

[16] 脅迫文の具体的な内容については、提供いただいていないため不明である。

[17] AWS の各種サービスに対する操作ログを記録するサービス

また、被害に遭ったシステムの復旧や調査に約 70 人日の工数が発生し、顧客への対応や外部調査機関による調査等の費用として約 2,000 万円を要した。

（5） 再発防止策

- 不必要なネットワークからのアクセスを制限し、特定の IP アドレスからのアクセスのみを許可する設定を実施
- AWS リソースに対する操作ログ、及び S3 バケットへのアクセスログの取得を徹底
- S3 に保存したデータを削除する際に、多要素認証を必須とする仕組みである S3 MFA Delete を導入
- AWS が公開している、AWS サービスのベストプラクティスを実施
- バックアップデータの取得を徹底
- ペネトレーションテストの実施

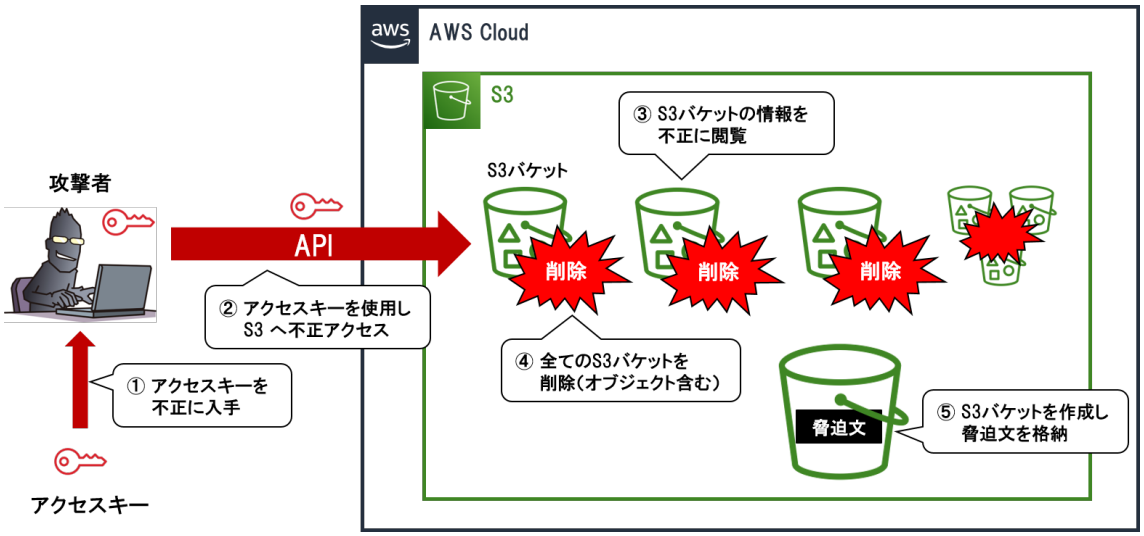

図 5-1 本事例の概要

5-2. 着目点

（1） アクセスキーの管理

本事例では、4 つのアクセスキーが攻撃者によって不正に使用されていた。アクセスキーの漏えい原因は不明であるが、外部調査機関による調査の結果、システムに対する不正なログイン、ウイルス感染、システムの脆弱性を悪用した痕跡、及びアクセスキーが記載されたファイルを閲覧された痕跡がなかったことを確認している。このことから、攻撃者はシステムに攻撃するよりも前に、何らかの方法でアクセスキーを不正に入手していたと考えられ

る。日頃からアクセスキーが使用されている箇所や用途等を把握しておくことで、漏えいした原因を特定できた可能性がある。

AWS におけるアクセスキーの漏えいを原因とする不正アクセス等の事案は、過去にも複数確認している。AWS では、アクセスキーを持っているユーザは、正規のユーザではなくても、AWS リソースに対しての操作が可能となる。そのため、アクセスキーを適切に管理するとともに、アクセスキーで行える操作を最小限にすることが重要である。

アクセスキーの管理方法については、AWS から、ベストプラクティスが公開されているため、参考にしていただきたい。

- AWS アクセスキーを管理するためのベストプラクティス
  https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws-access-keys-best-practices.html

（2） システムにおけるアクセス制御

届出者が利用していたシステムにおいて、S3 へのアクセスを外部ネットワークから行う必要はなかった。しかし、外部ネットワークからの S3 に対するアクセスを制限していなかったため、攻撃者は、不正に入手したアクセスキーを使用して、S3 へアクセスすることができた。適切なアクセス制御を実施していれば、被害を防げた可能性がある。

AWS といったクラウドサービスに限らず、不必要なネットワークからのアクセスを拒否するといったアクセス制御を行うことは、不正アクセスを防止するのに有効である。システムに対して、適切なアクセス制御が設定されているか見直していただきたい。

6. 届出へのご協力のお願い

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

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

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

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

【コンピュータウイルスに関する届出制度】

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

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

【コンピュータ不正アクセス被害の届出制度】

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

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