コンピュータウイルス・不正アクセスの届出事例

［2022 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

2023 年 3 月 2 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、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、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。なお、届出される情報は断片的な場合があるため、原因・結果・対策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 年下半期（7 月～12 月。以下、今期）に受理した[6]コンピュータウイルス（以下、ウイルス）届出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 78 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　28 件（事例 1～28）
- 身代金を要求するサイバー攻撃の被害　18 件（事例 29～46）
- 脆弱性や設定不備を悪用された不正アクセス　20 件（事例 47～66）
- ID とパスワードによる認証を突破された不正アクセス　8 件　（事例 67～74）
- その他　4 件　（事例 75～78）

全体を通して見ると、これまでと同様に、基本的なセキュリティ対策を実施することで、被害を防ぐことができたと思われるものが多く見られた。脆弱性や設定不備を悪用された不正アクセス（2-3 節で説明）、ID とパスワードによる認証を突破された不正アクセス（2-4 節で説明）に分類した事例の多くはその典型であり、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）についても、大半は利用している VPN 装置等に存在した脆弱性を悪用され、外部からの侵入を許してしまったことが原因であった。攻撃の手口や被害原因、攻撃対象の機器がそれぞれ異なるものであったとしても、求められる対応は、ソフトウェアの更新や設定の見直し等といった基本的なセキュリティ対策である。改めてこれらの基本的な対策が漏れなく実施できているか、自組織の状況について点検することを勧める。その上で、組織としての対応体制をより強化していくために、CISO（Chief Information Security Officer）や CSIRT（Computer Security Incident Response Team）の設置、事業継続計画（BCP：Business Continuity Plan）の策定・見直し等も実施していただきたい。

2022 年上半期（1 月～6 月。以下、先期）に 174 件もの届出がされたコンピュータウイルスの検知・感染被害（2-1 節で説明）については、今期は 28 件と大幅に減少している。これは、先期のウイルス届出の大半を占めた「Emotet」と呼ばれるウイルス（以下、Emotet）

[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。

の検知や感染被害に関する届出が 164 件から 26 件と大きく減少したことが理由の一つである。これは、Emotet が不定期に休止・再開を繰り返しており、今期における攻撃活動はほぼ停止しているとみられる状況であったためである。しかし、今後、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考えられるため、引き続き警戒は必要である。

本紙に示した事例以外にも、ウイルスの発見、なりすましやフィッシング等の不審メールの受信、個人や組織で利用しているアカウントへの不正なログインの挙動検知なども複数寄せられている。これら届出全体の集計情報については、次の資料を参照いただきたい。

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

2-1. コンピュータウイルスの検知・感染被害

本節では、Emotet とそれ以外のウイルスの 2 つに分けて説明する。また、届出のうち、ランサムウェアの部類であると判断した事例については、2-2 節の分類としている。

今期におけるコンピュータウイルスの検知・感染被害の届出は 28 件あり、先期の 174 件から大幅に減少した。これは先述の通り、Emotet の検知や感染、Emotet への感染を狙った攻撃メールの着信に関する届出が大きく減ったためである。

（1） Emotet

Emotet は、情報の窃取に加え、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、攻撃メールに添付されたファイルや本文中のリンクを介して、パソコンやサーバに感染させるなどして、更なる感染の拡大が試みられている。

2021 年 11 月頃から 2022 年 7 月頃にかけて行われた攻撃では、多くの組織で Emotet の感染被害が相次ぎ、先期の届出においては 164 件の届出があった。

今期の 2022 年 7 月から 10 月末までに受理した届出においては、Emotet を検知・感染した日時は全て 7 月上旬以前のものであった。これは公開情報の 2022 年 7 月中旬頃から攻撃メールが観測されなくなった時期と一致している。その後、11 月 2 日に再び攻撃活動が観測されたとの公開情報もあったが、11 月から 12 月末までに届出された情報は 2 件のみであった（1 件は発見日時が 7 月上旬以前のもの）。

Emotet の攻撃メールに使われている手口については、これまでに確認されているものと同様に、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。

参考までに、IPA が 2022 年 11 月 2 日に確認したマクロを実行させるための新たな手口を次に記載する。対策としては、これまで同様「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」ことを利用者に徹底させるとともに、今回確認された新たな手口についても注意を呼び掛けてほしい。

■Excel ファイル内に書かれている偽の指示の変更について

2022 年 11 月 2 日から、メールに添付された Excel ファイル内に書かれている偽の指示が、コンテンツの有効化ボタンのクリックを促す内容から図 2-1 のように変化した。

この指示どおりに、Excel ファイルを、記載された「Templates」フォルダにコピーして開くと、マクロを無効化する設定にしていても、ファイルに含まれている悪意のあるマクロが強制的に実行されてしまう。これは、コピー先の Templates フォルダが信頼できる場所として OS にデフォルトで設定されているためで [7]、このフォルダに格納されたファイルは、安全性の高いファイルとみなされ、マクロが実行可能となる。

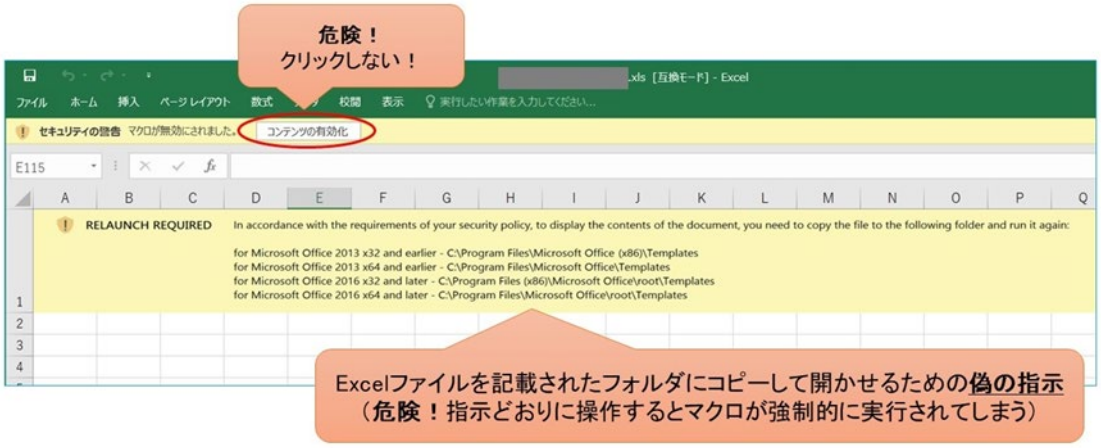

図 2-1 Excel ファイル内に書かれている新たな偽の指示

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。

[7] Microsoft「Office ファイルの信頼できる場所」
https://learn.microsoft.com/ja-jp/deployoffice/security/trusted-locations

- 「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

また、JPCERT/CC が公開している次のウェブサイトでは、Emotet の感染有無を確認する Emocheck と呼ばれるツールや Emotet への対応 FAQ 等も紹介している。こちらも参考にしていただきたい。

- 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

表 2-1 に、Emotet を検知・感染した届出を各月ごとに分けて掲載した。なお、各届出の詳細については省略する。

表 2-1 Emotet の検知・感染に関する届出状況

届出月	事例 No.	届出者の主体と件数		概要
2022/7	1～14 （14 件）	企業	13 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、Emotet に感染したパソコンから職員の名前を騙った不審なメールが外部へ発信された。 等
		教育・研究機関	1 件	
2022/8	15～18 （4 件）	企業	3 件	
		地方自治体	1 件	
2022/9	19～23 （5 件）	企業	3 件	
		一般団体	1 件	
		教育・研究機関	1 件	
2022/10	24 （1 件）	企業	1 件	
2022/11	25～26 （2 件）	医療法人	1 件	
		企業	1 件	
2022/12	－ （0 件）	－	0 件	

（2）　Emotet 以外のウイルス

Emotet 以外のウイルスに関する届出は 2 件あったが、どちらも詳細は不明であった。

なお、1 件のみ、ウェブサイトの閲覧により感染したことが原因であると届出者が推測している事例があった。

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

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

項番	届出日	概要
27	2022/8/5	届出者（企業）の従業員が使用するパソコンで、セキュリティソフトがウイルスを検知した。セキュリティソフトにより駆除されたため、詳細は不明である。再発防止に向け、ウイルス定義ファイルの最新化を行った。更に、EDR の導入検討やセキュリティインシデント発生時の対応体制の整備を行うとしている。
28	2022/10/18	届出者（企業）が所有するパソコン 1 台がウイルスに感染したことを確認した。原因はウェブサイトの閲覧により感染したものと推測しているが、詳しい感染経路や原因は不明である。対応として、感染したパソコンの初期化等を行うとともに、新規のパソコンを購入した。再発防止策として、ウェブサイト閲覧時におけるコンテンツフィルタリングを適用するとしている。

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もしくは消去して、その復旧と引き換えに、身代金として金銭を脅し取ろうとするサイバー攻撃を受けた 18 件の届出について紹介する。

なお、事例には攻撃者が組織内ネットワークへの侵入に成功してしまった原因として、VPN 装置に存在した未対応の脆弱性を悪用された事案、ファイアウォールに設定不備があった事案のほか、脆弱なパスワードを使用していたなどの事案も含めている。これらは、2-3 節、2-4 節の分類条件と重複するが、身代金を要求するサイバー攻撃の被害に関連する事例として本節に分類している。

また、届出の中にはファイル等の暗号化や削除が確認されたものの、脅迫文は確認されなかったとするものもあった。この場合、攻撃者の目的が身代金（金銭）ではなく、機密情報の窃取やサービスの妨害等であった可能性も考えられるが、これまでの届出事例を見ると、暗号化の手口や侵入の原因が類似していることから、本節の分類としている。

今期においては、フリーツールを悪用したファイルの暗号化や削除が行われ、身代金を要求された事例（事例 No.41）があった。その詳細について 3 章で紹介する。そのほかに、2019 年下半期に紹介した、攻撃者によりデータベースが消去され、身代金を要求する脅迫文が残されていたとする事例が再び確認された。攻撃の手口や取るべき対策等は、ほぼ同一であるため、詳細については 2019 年下半期の資料 [8]を参照していただきたい。

また、脅迫文や暗号化されたファイルの拡張子から、攻撃者の名称が推定できる事例もある。今期においては、LockBit と呼ばれるランサムウェア（以下、LockBit）に関する被害が最も多く確認された。LockBit はランサムウェアの名称と同名の攻撃グループであり、この攻撃グループ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 [9]」を行う [10]。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、窃取されたと思われるデータがリークサイト上に公開されてしまった事例もあった。本節の事例では、LockBit、それ以外のランサムウェアと 2 つに分けて記載する。

本節で取り上げた事例のうち、攻撃の初期侵入（推定も含む）として最も多かったのは、VPN 装置の脆弱性悪用であった。脆弱性の対策方法に関しては 2-3 節で詳しく述べるが、

---

[8] IPA「コンピュータウイルス・不正アクセスの届出状況［2019 年下半期（7 月～12 月）］」
https://www.ipa.go.jp/files/000080223.pdf

[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/

それとは別に、外部からの攻撃の侵入口となり得る箇所（攻撃対象領域、Attack Surface と呼ばれる）を把握・特定し、必要最小限となっているかについて、改めて確認することを勧める。あわせて、過去に窃取された認証情報を用いて、ネットワーク内に侵入されたとする事例もあるため、バージョンアップ等で VPN 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ることを考慮し、必要に応じて、パスワード変更を実施していただきたい。

初期侵入後は、組織内ネットワークの中で侵害範囲を拡大する手口として、ドメインコントローラを乗っ取り、悪用する事例を多く確認している。ドメインコントローラが悪用された場合、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。このため、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を確実に実施してほしい。

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。

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

項番	届出日	概要
LockBit ランサムウェアの被害事例		
29	2022/7/5	届出者（一般団体）が利用するパソコンと複数のサーバにおいて、異常を発見した。被害状況から、届出者は LockBit3.0 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。原因はメールや外部からダウンロードしたファイルによる感染、あるいは何らかの脆弱性の悪用と推測している。再発防止策として、セキュリティ対策の強化を行った。

項番	届出日	概要
30	2022/7/13	届出者（企業）の共有サーバが使用不可になっていることを確認した。このため、外部機関に調査を依頼したところ、LockBit3.0 によりサーバ上のファイルが暗号化されていたことが判明した。更に調査の結果、セキュリティソフトのアンインストールやシャドウコピーサービスの停止といった不正操作も行われており、バックアップ取得用の外付けハードディスクも同様に暗号化されていた。侵入の原因は不明だが、VPN 装置（FortiGate）に対して、管理者 ID による複数の不正なログイン試行が確認されたことから、総当たり攻撃等により、認証を突破されたものと推測している。発覚後には、社内ネットワークを全て停止させ、セキュリティソフトの再インストール、ウイルススキャンの実施及びデータの復元対応を行った。しかしながら、復元に成功したデータはほとんどないとのことであった。再発防止策として、VPN 装置の管理者 ID の変更や VPN に接続する社員のパスワード変更、VPN 装置の開発元やシステム会社との保守契約を行った。
31	2022/7/19	届出者（企業）が利用するサーバにおいて、ランサムウェアとみられる不正なアクセスが確認された。調査したところ、数百台のパソコンが LockBit に感染していることが判明した。調査会社によれば、攻撃者が VPN 装置の脆弱性を悪用することで、届出者のシステム内に不正侵入し、パソコンの暗号化や情報窃取を行ったものと推定されている。対応として、ネットワークの遮断、OS 及びソフトウェアの最新化、セキュリティソフトによるフルスキャン等を実施した。再発防止策として、監視やセキュリティ管理体制の強化、EDR の導入を実施した。

項番	届出日	概要
32	2022/8/24	届出者（企業）が利用するサーバのデスクトップ画面に、金銭を要求する脅迫文が表示されていることを発見した。調査したところ、複数のサーバとパソコンに保存していたファイル、及びバックアップファイルが暗号化されていることが判明した。脅迫文の内容から、LockBit2.0 の攻撃を受けたものと推定された。原因は不明だが、パソコンに導入していたセキュリティソフトにおいて、メールにより感染したことを示すログが残っていたことに加え、ファイアウォール及び UTM により、外部からの不正アクセスやウェブ経由での侵入の可能性が低いことなどから、不正なメールがランサムウェア被害の原因となったと推測している。対応として、被害に遭った機器を初期化し、クラウド上に取得していたバックアップより復旧させた。なお、クラウド上にバックアップを取得していなかった一部データについては復旧できていない。再発防止策として、バックアップ運用方法の見直し、UTM の増設、社内のセキュリティ教育の強化を実施した

項番	届出日	概要
33	2022/9/19	届出者（企業）の従業員から社内システムが利用できないと連絡があった。外部機関に依頼して調査した結果、数十台以上のサーバとパソコンが LockBit2.0 によるランサムウェア攻撃を受け、ファイルの暗号化及び脅迫文の作成が行われたことが確認された。加えて、複数回に渡り、攻撃者が外部へデータ転送を行ったとみられる通信ログも確認された。侵入の原因は、VPN 装置（FortiGate）の脆弱性を悪用した攻撃により窃取された認証情報が使用され、不正アクセスが行われたものと推測している。更に、被害が拡大した原因については、攻撃手口の詳細は不明だが、攻撃者が Active Directory サーバを乗っ取り、サーバやパソコンを侵害したものと推測している。対応として、サーバ等が接続されたネットワークや VPN 装置の切り離しを行い、設定の再構築や初期化を実施した。また、侵害が確認されなかった機器においても、セキュリティソフトの更新後にフルスキャンを実施する等の対応を行った。暗号化されたデータについては、バックアップサーバも暗号化の被害に遭ったこともあり、復元はできなかった。再発防止策として、Active Directory サーバのパスワード設定の見直し等を行い、VPN 装置においては二段階認証の導入を実施した。そのほか、バックアップデータの保存方法の見直し、定期的なログのチェック、EDR の導入を検討している。

その他の身代金を要求するサイバー攻撃被害の事例		
34	2022/7/1	届出者（企業）の複数台のサーバとパソコン上のファイルが暗号化され、脅迫文とみられるテキストファイルが残されていたことに従業員が気づいた。脅迫文や暗号化されたファイルの拡張子などから、Cring 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。原因については、不審な VPN 接続ログが見つかったことから、VPN 装置（FortiGate）の脆弱性を悪用して社内に侵入されたものと推測している。発覚後、ファイルが暗号化された機器はネットワークから切断した上で、全ての機器に対してセキュリティソフトでのフルスキャンを実施した。被害を受けたサーバは、約２週間前のバックアップデータを基に復旧作業を行った。再発防止策として、従来のセキュリティソフトに加え、不審なプログラムの動作を検知し、抑止する機能を持つ別のセキュリティソフトを導入した。更に、資産管理ソフトの導入により、管理者によるアプリケーションの利用制限を行う仕組みとした。
35	2022/7/6	届出者（企業）が利用する NAS 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。拡張子や NAS に残されていた脅迫文の特徴から、eCh0raix 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。被害の原因は攻撃メールによるものと届出者は推測しているが当該メールは駆除済みのため、詳細は不明とのことであった。対応として、専門業者にデータ復旧を依頼し、大部分のデータを復旧することができたが、復旧までの約 2 週間は過去のバックアップデータを使用する縮退営業を余儀なくされた。再発防止策として、NAS のファームウェアを最新のものに更新した。

36	2022/7/8	届出者（企業）の従業員から、ファイルサーバにアクセスできないとの連絡があった。調査したところ、社内サーバ数十台でファイルの暗号化や消去が行われ、デスクトップに脅迫文とみられるテキストファイルが置かれていたことが判明した。状況から、ランサムウェアに感染した可能性が考えられるが、フォレンジック調査の結果、ファイルの暗号化や消去はフリーソフトを使用した手動による被害であった。侵入の原因は、VPN 装置（FortiGate）に脆弱性が存在していたことから、当該の脆弱性を悪用した攻撃により、認証情報を窃取され、不正アクセスが行われたものと推測している。再発防止に向け、セキュリティベンダから適宜情報を入手して、セキュリティ対策の処置を実施できるよう運用手順を定めたほか、多要素認証の導入等を行った。
37	2022/8/9	届出者（一般団体）が利用するシステムについて、職員よりログインが出来ない旨の報告があり、調査したところ、サーバ上のファイルが暗号化されていることが確認された。攻撃者が残したとみられる脅迫文やファイルの拡張子等から、Flamingo と呼ばれるランサムウェアに感染したものと推定している。侵入の原因については不明だが、届出者の端末を踏み台とした総当たり攻撃等により、サーバ内に不正アクセスされたものと推測している。対応として、サーバを新規に構築し、被害発生前の状態にリストアした。再発防止策としては、利用していたパスワードを長く複雑なものに変更するとともに、EDR 製品の導入も予定している。

38	2022/8/30	届出者（企業）が利用するサーバにおいて、保存していた一部のデータと全てのバックアップデータが暗号化され、拡張子が.ghost に変更されていることを確認した。攻撃の内容から、Cring ランサムウェアの攻撃を受けたものと推定している。侵入の原因は、VPN 装置に脆弱性が存在しており、外部から当該脆弱性を悪用され、組織内ネットワークに侵入されたものと推測している。対応として、暗号化の被害にあったサーバを初期化したのち、サーバの入れ替えを行った。再発防止策として、ファイアウォールを最新のものに変更し、利用していたパソコンのパスワードを長く複雑なものに変更した。加えて、EDR の導入も予定している。
39	2022/9/28	届出者（企業）が運営する施設のシステムに異常が発生していることを発見した。調査を行ったところ、そのシステムに関連する複数のパソコンとサーバ上のファイルが暗号化され、拡張子が.eight に変更されていることを確認した。攻撃者が残したとみられる脅迫文と拡張子から、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している。被害原因は、ネットワーク構築時における、ファイアウォールの初期設定不備により、外部からの不正アクセスが可能な状態にあったことが判明している。対応として、感染機器のネットワーク隔離やネットワーク内の機器に対するウイルスチェック、外部からのアクセスを制限する措置を行った。ランサムウェアにより暗号化されたファイルは復元できていない。また、当該ランサムウェア被害を受けて、届出者が運営する複数の施設に対して調査を行ったところ、1 件の別施設のネットワークが、同様の被害原因による不正アクセスを受けていたことが判明した。しかしながら、不正アクセス以外に被害は確認されておらず、関連等の詳細は不明である。2 つの被害を受けての再発防止策として、セキュリティソフトの設定やファイアウォールの設定の見直し、従業員向けにルール徹底に関する注意喚起を実施した。更に、システムで取り扱うデータをクラウド環境へ移行すること等を検討している。

40	2022/10/24	届出者（企業）のサーバ内にあるファイルが暗号化される被害に遭った。2 台のサーバがランサムウェアに感染し、仮復旧までに一週間程度を要した。原因は外部からの不正アクセスとみられるが、詳細は不明である。サーバは初期化により復旧した。再発防止策として、VPN 装置のアップデートを実施する等の対応を行った。
41	2022/10/28	届出者（企業）が利用する社内システムにおいて、サービス停止が発生したことを監視システムが検知した。調査の結果、オンプレミスとクラウドに設置していた複数台のサーバがフリーツールによる暗号化及び削除の被害に遭い、攻撃者のものとみられる脅迫文が残されていることを確認した。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、不正アクセスが行われたもの推測している。攻撃者は社内ネットワークに侵入後、業務用サーバ 1 台に対する複数回の認証試行を行ったのち、不正ログインに成功した。そのほかのサーバについては、ログインに使用されていたパスワードが平易なものであったこと等があり、不正アクセスの要因になったと推測している。対応として、サーバの停止やインターネット接続の切断等を実施した。その後、バックアップデータから各サーバを復旧させた。再発防止策として、各種サーバの管理者アカウントの見直し及びパスワードの複雑化を行った。更に、多要素認証の導入やログ監視の強化のほか、セキュリティ対応の体制の見直し等を実施した。 ※本事例は 3 章で紹介する。
42	2022/10/28	届出者（企業）が利用するウェブシステムの管理画面においてエラーが発生することを発見した。調査したところ、当該システム内のデータが削除され、脅迫文が書かれたテキストファイルが残されていることが判明した。原因は、当該サイトにプレースホルダの実装不備があったために、SQL インジェクション攻撃を受け、不正アクセスが行われたものと推測している。対応として、被害を受けたシステムを調査完了後に廃棄することにした。再発防止策として、情報の管理体制の見直し等を行うとしている。

43	2022/10/31	届出者（企業）が管理しているウェブサイトにアクセスした際、エラーメッセージが表示されることを発見した。調査した結果、データベース内のデータが全て削除されており、金銭を要求する旨が記された脅迫文が残されていたことが判明した。原因は、インターネットからデータベース管理画面へのアクセスが可能であり、かつ有効になっていた匿名ユーザのパスワードが推測可能なものであったため、辞書攻撃等の手口で不正ログインを行い、データベースを削除したものと推測している。対応として、データベースでの匿名ユーザのログイン不可設定、サーバ環境の初期化及び再構築等を実施した。再発防止策として、サーバの管理画面をメンテナンス時のみの利用に制限する設定を行ったほか、多要素認証の導入やセキュリティが強化されたサーバ環境への移行を検討するとしている。
44	2022/11/9	届出者（企業）が利用する NAS において、不審なファイルの設置と保管していたファイルが改ざんされていたことを発見した。NAS 内には脅迫文が残されており、その内容から Checkmate と呼ばれるランサムウェア攻撃を受けたものと推定される。侵入経路は不明ながら、届出者は使用しているファイアウォール製品の脆弱性を悪用されたことにより、不正アクセスを受けた可能性があると推測している(※)。本事象の発覚後、NAS をネットワークから切り離し、組織内の全機器に対してウイルススキャンを実施した。なお、NAS 以外の被害は確認されなかった。また、改ざんされたデータの一部がバックアップ装置にバックアップされていたため、バックアップ装置内の正常なデータを一時退避して、同装置を初期化した後にデータ復元を行った。再発防止策として、VPN 装置や社内パソコンから NAS へアクセスする際に求められるパスワードをより強固なものに変更するとともに、アクセスログの確認を強化する等といった体制の強化を行うとしている。(※)Checkmate ランサムウェアは、QNAP 社製の NAS に対して、SMB 機能を利用した辞書攻撃により侵入する手口が確認されていることから、本件も同様の手口が使われた可能性が考えられる。

45	2022/11/14	届出者（企業）が利用するパソコンに導入していた EDR において、ランサムウェアが検知されたと関係会社から連絡があった。調査の結果、Active Directory サーバやバックアップサーバを含む複数のサーバ内のデータが暗号化され、脅迫文とみられるファイルが残されていることも発見された。脅迫文の内容から Hive と呼ばれるランサムウェアの攻撃を受けたものと推定される。侵入及び侵害拡大の原因は、VPN 装置（SonicWall）を脆弱な状態で放置し、かつ各サーバ間の通信制御が不十分であったため、攻撃者が VPN 装置の脆弱性を悪用して外部から侵入したのち、ドメインコントローラの管理者権限を乗っ取り、データセンター内に設置していたサーバや社内ネットワーク内の端末にランサムウェアを拡散したものと推測される。対応として、ネットワークの切断や外部からのアクセス制限を行うとともに、社内ネットワークの再構築等を実施した。再発防止策として、原因となった VPN 装置を廃止し、ネットワーク構成や資産管理運用、バックアップ管理方法の見直し等を実施した。

46	2022/11/16	届出者（企業）の従業員から社内システムに接続できないとの連絡があり、システム内を確認したところ、サーバの画面に身代金を要求する内容の脅迫文が表示されていた。調査の結果、外部のデータセンターにおいて、VMware ESXi 上に構築していた Active Directory サーバやバックアップサーバを含む全ての仮想サーバが暗号化され、更に、バックアップデータを複製保存していた社内のサーバも暗号化されていたことが判明した。攻撃者が残したとみられる脅迫文の内容から、RedAlert 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ている。詳細な原因は不明だが、届出者は VPN 装置や Active Directory サーバ等で設定していたパスワードが脆弱であったため、攻撃者に総当たり攻撃とみられる手段によって不正アクセスされ、更に、VMware ESXi の脆弱性を悪用されたことで、各種サーバを暗号化されたものと推定している。対応として、外部の IaaS 環境に代替システムを構築して業務を再開するとともに、暗号化の被害に遭わなかったデータからシステムの復旧を行った。再発防止策として、パスワードを強固なものとするよう運用を変更するとともに、UTM 等の導入による監視体制の強化や情報セキュリティに関する研修の実施等を検討している。

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、それを攻撃者に悪用されて不正アクセス被害を受けた 20 件の届出について紹介する。あわせて、VPN 装置の脆弱性に関する概要や対策方法等についても本節で説明する。

今期においても、VPN 装置の脆弱性を悪用された不正アクセス事例が比較的多く確認されており、先期から引き続き、攻撃者から積極的に狙われている状況と考えられる。VPN 装置は、外部から組織内のネットワークへの安全なリモートアクセスの実現に使われている技術であり、攻撃者から組織内の情報資産を守るための重要なセキュリティ要素といえる。一方で、VPN 装置の脆弱性悪用により認証を突破され、攻撃者に侵入を許してしまうと、組織内ネットワークにある多数のサーバやパソコン等に甚大な被害が発生する可能性がある。また、VPN 装置のように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、簡単に修正プログラムの適用を行うことは難しいものと推察される。そのため、VPN 装置などの脆弱性の管理が確実に実施できるように、ベンダー等から情報が漏れなく収集できているか、脆弱性が確認された際に、迅速に影響の調査・検証と対策の実施ができる運用になっているか等、改めて組織内の体制や手順の点検を実施しておくことを勧める。あわせて、2-2 節で述べた脆弱性対策以外の対応も並行して実施していただきたい。

CMS や EC ソフトウェアの脆弱性を悪用されたとする届出については、ウェブサーバ内への不正ファイルの設置や正規ファイルの改ざんにより、ウェブサイト利用者の個人情報を窃取される、スパムメールの踏み台として悪用される等の事案が依然として確認されている。その中には、CMS の脆弱性を悪用した不正ファイルの設置を受け、初動対応として、パスワード変更や不正ファイルの削除などを実施したが、再び攻撃を受けてしまい、複数の影響が発生したとする事例（事例 No. 48）もあった。その詳細については 4 章で紹介する。これらの原因としては、主に古いバージョンの利用によるものが多い傾向にあることから、基本的な対策であるソフトウェアの更新を漏れなく実施していただきたい。

また、今期に届出された事例の中には、自組織のサービス提供のために利用していた外部のサービスや、業務委託先事業者のシステムで発生した不正アクセスにより、情報漏えいの被害を受けたとする届出もあった。

外部サービスの利用におけるキュリティ対策は、サービス提供者側で実施される傾向にあるが、利用者側で適切な対応が行われているかを直接確認することは容易ではない。そのため、外部サービスの選定や契約時に、セキュリティ確保のために必要な事項を十分に考慮した、外部サービスの選定基準とセキュリティ要件を準備し、それを満たすものであるかを確認することが重要である。

業務委託においては、委託者と受託者での作業分担が明確になっておらず、脆弱性が放置

されていたという届出が依然として確認されている。そのため、業務委託の契約書を確認し、責任分界点を正確に把握した上で、自組織で実施すべき定期的なセキュリティ対策作業や被害発生時の対応フロー等を明確化しておくことを勧める。

万が一、何らかのセキュリティインシデントが生じた場合に、損害を最小限に抑えつつ、事業の継続や早急な復旧を図るためにも、自組織に適した BCP を策定し、適切に実施可能か点検しておくことも重要である。

表 2-4 に脆弱性や設定不備を悪用された不正アクセスの届出の概要一覧を示す。

表 2-4 脆弱性や設定不備を悪用された不正アクセスに関する届出の概要一覧

項番	届出日	概要
CMS の脆弱性が悪用された事例		
47	2022/8/23	届出者（企業）のウェブサイトに不審なファイルが設置されていることをウェブサイトの監視業務を委託している事業者より、報告を受けた。調査の結果、CMS（Movable Type）のウェブインターフェースである XMLRPC API の脆弱性（CVE-2021-20837）を悪用されて、ウェブサイトにバックドア等の不正ファイルを設置されていたことが判明した。外部からバックドアへのアクセスは WAF によりブロックしていたため、不正ファイルの設置以外の被害は確認されていない。発覚後、当該不正ファイルを削除し、対策を行った。原因はウェブサイトの保守・運用の業務は外部に委託していたが、CMS のバージョンアップや修正プログラム適用の作業は委託業務に含まれていなかったため、CMS が更新されずに脆弱性が残存していた。再発防止策として、CMS のバージョン管理を届出者自身で行い、アップデートや修正プログラム適用の作業は、その都度、外部委託先へ対応を依頼する体制とした。

項番	届出日	概要
48	2022/9/7	届出者（企業）が運用するレンタルサーバのウェブサイト上に不審なページが公開されていることをレンタルサーバの提供会社から連絡があった。調査の結果、サーバ内に複数のフィッシングサイトが設置されており、更に、フィッシングサイトに入力された認証情報を外部にメール送信しようとした痕跡も確認された。しかし、メールは導入していた誤送信防止システムにより、外部への送信には至らなかった。その後、届出者が復旧作業を進める中で、サーバが動作不能な状態となったため、再調査を行ったところ、サーバ上のシステム領域も含めたファイルの消去が行われたことが判明した。原因は、脆弱なバージョンの 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。対応として、当初、脆弱性の存在に気づかず、不正に作成されたサイトを削除する等の措置であったため、再び不正アクセスが確認されたことから、ウェブサイトを停止し、社外からウェブサーバへのアクセスを遮断した。再発防止策として、ウェブサイトを閉鎖し、不正アクセスの原因に対する対策を実施した上で、セキュリティが強化されたサービスへと移行した。 ※本事例は４章で紹介する。

EC ソフトウェアの脆弱性が悪用された事例		
49	2022/8/9	届出者（企業）が運営する EC サイトからクレジットカード情報が漏えいした疑いがあるとクレジットカード会社より連絡があった。調査の結果、当該 EC サイトを利用した顧客のカード情報数万件が漏えいした可能性があることが判明した。原因は、当該 EC サイトのシステムに存在していたクロスサイトスクリプティングの脆弱性を悪用した攻撃を受けたことによる。本件への対応として、EC サイトの決済方式の変更を含めたシステムの刷新を行った。更に、システム会社から保守やセキュリティ対応に関するサービスを受けられるよう契約の変更を行った。
50	2022/9/8	届出者（企業）が運営する EC サイトから利用者のクレジットカード情報が漏えいした可能性があるとクレジットカード会社より連絡があった。外部の調査機関による調査の結果、当該 EC サイトへの不正アクセスを確認し、更にサイト利用者の個人情報やクレジットカード情報等、十数万件以上が漏えいした可能性があることが判明した。原因は、EC サイトに存在していたクロスサイトスクリプティングの脆弱性を悪用されたもので、外部から寄せられた問い合わせのデータ内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、管理画面への不正アクセスが可能となる状態となっていた。対応として、当該 EC サイトの決済機能を停止後、サーバを破棄し、新サーバへの移設を行った。再発防止策として、サーバの運用や管理体制の見直し、定期的な脆弱性診断とペネトレーションテストの実施等を行うこととした。

51	2022/9/22	届出者（企業）が運営する EC サイトにおいて、顧客のクレジットカードが不正利用されている可能性があると、決済代行会社より連絡を受けた。外部業者にフォレンジック調査を依頼したところ、当該 EC サイトを利用した顧客数百件のカード情報が漏えいした可能性があることが確認された。原因は、EC サイトで利用していた CMS（EC-CUBE）にクロスサイトスクリプティングの脆弱性が存在したためである。その脆弱性を悪用した攻撃により、注文システム内に、決済を行った顧客のクレジットカード情報や個人情報等が攻撃者に送信する仕組みの不正ファイルを攻撃者に設置された。本件の対応として、EC サイトにおけるクレジットカード決済の停止や不正ファイルの削除を行ったのち、EC サイトを閉鎖した。再発防止策として、WAF の導入やセキュリティ運用体制の見直し、定期的な脆弱性診断の実施等を検討している。
52	2022/10/18	届出者（企業）が運営する EC サイトからクレジットカード情報が漏えいした疑いがあると、クレジットカード会社から連絡があった。調査機関にフォレンジック調査を依頼したところ、CMS（EC-CUBE）に存在していたクロスサイトスクリプティングの脆弱性悪用により、ファイルの改ざんや不正ファイルの設置が行われたこと、更に、数百件のカード情報が漏えいした可能性があることが確認された。情報漏えいの原因はこの設置された不正ファイル経由でカード情報を窃取されたものと推測している。対応として、EC サイトでのカード決済機能を即日停止させたのち、調査結果を踏まえて当該サイトを閉鎖した。今後はセキュリティが強化された別の EC サイトで再開する予定としている。

SQL インジェクション攻撃を受けた事例		
53	2022/7/5	届出者（教育・研究機関）が運用するウェブシステムに不正アクセスがあり、システム内に保存されていたメールアドレス数千件が漏えいした可能性があることが発覚した。原因を調査したところ、当該システムにブラインド SQL インジェクションの脆弱性が存在しており、その脆弱性を悪用した攻撃を受けたことが判明した。本件の対応として、プログラムの修正を行い、当該システムの脆弱性を解消させた。再発防止策として、WAF を導入した。あわせて、脆弱性診断を可能な範囲で実施し、サーバの管理や情報セキュリティに関する教育研修の強化を検討している。
54	2022/7/25	届出者（企業）が提供するサービスにおいて、データベースの動作が遅くなっていることに気づき、ログを確認したところ、不審な SQL 命令が実行されていたことを発見した。調査を行ったところ、自社で構築した API に存在していた SQL インジェクションの脆弱性を悪用した攻撃を受け、顧客情報数百万件以上が窃取された恐れがあることが判明した。発覚後、すぐにサービスを停止し、プログラムの改修による脆弱性の解消、及び他のウェブページに存在していた同様の脆弱性の修正を行った。API の脆弱性が残存されていた原因は定期的な脆弱性診断を実施しなかったことであった。再発防止策として、脆弱性診断の実施、WAF の導入等を行った。
55	2022/10/14	届出者（一般団体）が業務委託しているウェブシステムが不正アクセスされ、当該システムの利用者情報と管理者情報が漏えいした恐れがあると委託先業者から連絡があった。調査したところ、利用者のメールアドレス数十万件と管理者の情報数十件が流出した可能性があることが判明した。原因は、当該システムに対して実施した脆弱性診断に不備があり、SQL インジェクションの脆弱性が残存していたこと、その脆弱性を悪用した攻撃を受けたことによる。対応として、委託先業者によりシステムの停止や脆弱なプログラムの修正等を行った。再発防止策として、管理者情報の変更や管理者用サイトにおける認証機能の見直しを行った。更に、委託先業者に対し、定期的に脆弱性診断を実施するよう指示した。

56	2022/11/4	届出者（一般団体）が業務委託しているウェブシステムが不正アクセスされた恐れがあると委託先業者から連絡があった。調査したところ、当該システム利用者のメールアドレス数千件と管理者の情報数件が流出した可能性があることが判明した。原因は、当該システムに対して実施した脆弱性診断に不備があり、SQL インジェクションの脆弱性が残存していたこと、その脆弱性を悪用した攻撃を受けたことによる。対応として、委託先事業者によりシステムの停止や脆弱なプログラムの修正を行った。再発防止策として、委託先事業者が WAF の導入を実施していることを審査条件に加えた。

その他、脆弱性や設定不備を悪用された事例		
57	2022/7/6	届出者（企業）が利用するウェブサーバが第三者に乗っ取られている疑いがあると外部機関より連絡があった。調査したところ、当該サーバ内に複数の不正なファイルが設置されており、数万件に及ぶスパムメール送信が行われたほか、サーバ内に保存されていた個人情報が外部に流出したことも確認された。原因は、ウェブサイトのファイルアップロード機能に存在していた脆弱性を悪用されたものと推測している。対応として、当該サーバをネットワークから切り離して、必要最低限のIP アドレスのみアクセスできるよう制限を掛けた。更に、流出した情報を悪用した不正ログインを防ぐため、届出者が提供しているウェブシステムのパスワード初期化を実施した。再発防止策として、本件の原因となったファイルアップロード機能を停止し、ウェブサイトのアクセス権限の見直しやWAF の導入を行った。
58	2022/9/7	届出者（一般団体）が運用するメールサーバが大量のスパムメール送信に悪用され、サーバ負荷の増加によるメール配信遅延が発生しているとサーバの保守業者より連絡があった。調査したところ、プロキシサーバのリプレイス時に行った設定変更に作業不備があり、メールの不正中継が可能な状態になっていたことが判明した。対応として、当該設定不備を修正し、配信遅延により滞留していたメールを削除した。再発防止として、リプレイス時におけるテスト設計及び検証方法の見直しを実施するとしている。

59	2022/9/16	届出者（企業）が利用する業務用サーバにおいて不正プログラムが検知されたと契約している SOC より通報があった。調査を行ったところ、サーバの遠隔操作を可能にする不正プログラム等が設置されていることが確認された。不正アクセスの原因は不明とのことであったが、届出より、使用しているネットワーク機器の Citrix NetScaler のファームウェアが古いことやログから管理者を含む複数のアカウントで不正ログインが発生していたことから、攻撃者が脆弱性の悪用を含む何らかの方法で ID とパスワードを入手し、それを悪用して当該サーバに不正アクセスしたものと推測される。対応として、影響を受けたシステムを停止させ、不正プログラムの削除及び攻撃元からの通信を遮断したのち、システムを復旧させた。再発防止策として、全アカウントのパスワードを変更し、攻撃元 IP アドレス及び不正プログラムのブラックリスト登録を行った。
60	2022/10/3	届出者（企業）が管理している顧客のネットワーク環境において、インターネットへの接続障害が発生した。調査したところ、顧客建物内に設置された他社管理のウェブカメラから、ルータの CPU 稼働率が 100%に達する程の大量の通信が発生していたことが判明した。原因は不明だが、ウェブカメラが外部にポート開放されていたことから、何らかの脆弱性を悪用した攻撃を受けたものと推測している。対応として、ウェブカメラの管理会社に状況を報告したところ、設定の初期化が行われたとのことであった。

61	2022/10/11	届出者（企業）が利用するサーバ上のセキュリティソフトより、ウイルスを駆除したことを示すアラートメールを受信した。調査機関に調査を依頼した結果、当該サーバが外部からの不正アクセスを受け、複数の不正なファイルを設置されていたことが判明した。セキュリティソフトの検知名から、トロイの木馬やバックドア等が設置されたものと推定される。それ以外のデータの改ざんや流出等の被害は確認されなかった。不正アクセスを受けた原因は、当該サーバで利用していたVMware Identity Manager のリモートコード実行の脆弱性（CVE-2022-22954）を攻撃者に悪用されたものと推測している。対応として、ネットワークの切断やサービスの停止、ソフトウェアのバージョンアップ、不正アクセスを受けたサーバのパスワード変更等を行った。再発防止策として、監視体制の強化を実施するとしている。
62	2022/10/14	届出者（教育・研究機関）が管理するウェブサイトの表示が本来とは異なるものになっていることを職員が発見した。調査したところ、当該サイトで利用していたCMS（WordPress）が不正アクセスされたことにより、ウェブサーバ内に複数の不正なファイルが設置され、フィッシングサイトが表示されるようになっていたことが判明した。更に、当該フィッシングサイトへ誘導する目的とみられる不正なメールの送信も確認された。原因は、サーバ移行時に利用した、WordPress のプラグインであるDuplicator のインストーラが外部からアクセス可能なディレクトリに残存されていたことから、攻撃者が何らかの方法でDuplicator の機能を悪用して、ウェブサイトの改ざんを行ったものと推測している。対応として、攻撃者に改ざんされたファイルの修正や設置された不正ファイルの削除を実施した。被害に遭ったウェブサーバについては、今後再構築する方針としている。再発防止策として、外部からのディレクトリに対するアクセス制限やプラグインの利用に関する見直し等を行った。

63	2022/10/25	届出者（企業）が利用する CMS（Wordpress）の管理画面にて、担当者が登録した覚えのないユーザ情報が追加されていることを発見した。調査したところ、ユーザ情報の登録だけでなく、ウェブページのソースコードも改ざんされ、外部サイトへの不正なリンクが数十件埋め込まれていた。更に、サーバ内に複数の不正なファイルが設置されていることも確認された。原因は、CMS にインストールしていた古いプラグインの脆弱性を悪用されたものと推測している。対応として、当該サーバへのアクセス制限を行うとともに、ウェブシステムを構成する MySQL や FTP のパスワード変更、発見した不正ファイルの削除等を行った。再発防止策として、CMS やプラグインの管理体制やアクセス制限の見直し、WAF の導入を実施するとしている。
64	2022/10/27	届出者（教育機関）が利用するプロキシサーバのセキュリティ設定の不備により、当該サーバが外部からアクセス可能な状態（オープンプロキシ）となり、自組織外のウェブサイトに対する DoS 攻撃の踏み台として悪用された。原因は、外部接続用のファイアウォールにて、当該サーバの保護が適切に行われていなかったこと、かつ当該サーバで発生していた不具合の調査にて、ファイアウォールの機能を無効化した状態のままに戻さなかったことであった。対応として、ファイアウォールを再有効化して、当該サーバに対する外部からのアクセスを遮断した。再発防止策として、ファイアウォール設定や設定の変更時における作業手順の見直しを行った。

65	2022/11/14	EC サイトを運営する届出者（企業）に対し、外部から顧客情報が流出しているとの連絡があった。社内調査では、データ流出の痕跡は確認できなかったが、海外の違法サイトにて、顧客情報がダウンロード可能な状態になっていたことを発見した。調査会社にフォレンジック調査を依頼した結果、届出者のサーバ上で行った MySQL コンテナの構築作業において、意図しない特権アカウントの作成及びポートの開放が行われていたこと、かつゲートウェイサーバにおいて、当該サーバをリモートからメンテナンスするために行った設定変更により、第三者が当該サーバに対し、インターネットからのアクセス及び不正操作が可能な状態になっていたことが判明した。これにより、攻撃者が当該サーバへと侵入し、顧客情報を含むデータを窃取したものと推測している。対応として、EC サイトを停止し、サーバへのアクセス制限を行った。再発防止策として、WAF の設置、アクセス権限設定の見直し、及び監査体制の強化等を実施した。
66	2022/11/15	届出者（企業）が利用するウェブサービスの提供業者から、顧客のクレジットカード情報が漏えいした疑いがあると連絡があった。調査の結果、サービス提供業者のシステムが不正に改ざんされたことにより、届出者のウェブサイトを利用した顧客数百人分のカード情報が漏えいした可能性があることが判明した。原因は、サービス提供業者が管理するウェブサーバ上のファイルに設定不備があり、公開状態となっていたことから、それを改ざんされ、届出者のサイトで入力したカード情報が第三者のサーバに送信されるようになっていた。対応として、サイト上のカード決済を停止するとともに、当該サービスの切り離しを行った。再発防止策として、当該サービスの利用を停止し、今後のサービス提供業者の選定時におけるセキュリティ基準の策定を検討する等としている。

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

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 8 件の届出を紹介する。

なお、2-2 節で述べた通り、VPN 装置の脆弱性を悪用した攻撃等で、窃取された認証情報を基に不正アクセスされた事例は除いているため、認証を突破されたことが不正アクセスの原因とする届出の総数は更に多くなる。

今期は、先期から引き続き、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原因と推定している事例が比較的多くあった。特に Microsoft365 のようなクラウドサービスの利用者や EC サイト等のショッピングサイトの利用者が単純なパスワードを使用しており、総当たり攻撃による不正アクセスを受けたことで、情報流出やアカウント不正利用の被害に遭ったとする事例が依然として確認されている。企業・組織のシステム管理者や EC サイト等のウェブサイト運営事業者においては、利用者が ID とパスワードを適切に運用できるよう、パスワード設定時に単純な文字列を許容しない仕組みの導入や、ワンタイムパスワード等といった多要素認証を提供する等の方法で、アカウントの安全性を高めるようにしていただきたい。あわせて、弱いパスワードが設定可能な状態になっていないか、利用されていない古いアカウントが有効のままになっていないかなど、アカウントの管理方法についても見直すことを検討してほしい。

今期に届出された事例の中には、短期間に数百万回もの不正ログイン試行が行われたのち、数万件のアカウントが不正アクセスされたとする事案もあった。こうした攻撃には、ログインの試行やパスワードの入力回数に上限を設けることに加え、不審な IP アドレスからのアクセスを遮断する等の対策を講じることが望ましい。

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。

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

項番	届出日	概要
67	2022/7/7	届出者（企業）が運営する EC サイトにおいて、WAF が DoS 攻撃を検知した。調査したところ、同一の攻撃元 IP アドレスからの大量のログイン試行が行われ、数万件以上のクレジットカード情報を含む会員情報が不正に閲覧された恐れがあることが判明した。原因は、通常のサイト利用にはない機械的なアクセスが確認されたことから、外部で流出したメールアドレスやパスワードを用いたパスワードリスト攻撃が行われたものと推測している。対応として、当該アドレスからのアクセスを遮断し、不正にログインされた会員のパスワードリセットを実施した。更に、複数の攻撃元 IP アドレスから同様の攻撃を受けるようになっていたため、ログイン時にボット対策（reCAPTCHA）を導入する等の措置を行った。再発防止策として、ログインページへのアクセス制限やパスワードの使い回しに関する注意喚起の実施、二段階認証の導入等を検討している。
68	2022/8/8	届出者（企業）が利用するクラウドサービスにおいて、従業員 1 名のアカウントがログインできなくなった。調査したところ、当該アカウントにて不正ログインが確認され、メールが盗み見された恐れがあることが判明した。なお、それ以外の被害は確認されていない。原因は、何らかの理由で当該アカウントの ID とパスワードを攻撃者に窃取されたためと推測しているが、詳細は不明である。再発防止策として、多要素認証方式を導入し、旧来の認証方式でのログインを禁止する設定を行うことにより不正アクセスの抑止を図った。

項番	届出日	概要
69	2022/8/10	届出者（教育・研究機関）の職員が利用するメールアカウントにおいて、海外からの不正なログインが検出されたと外部のメールサーバ運用会社より連絡があった。調査したところ、当該アカウントが保存していたメールの内容を不正に閲覧された可能性があった。原因は、設定していたパスワードが英単語を想起する英小文字と数字のみの比較的簡易なものであったため、攻撃者にパスワードを推測されたものとみられる。対応として、当該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、適切な強度のパスワードを設定するよう全職員に周知するとともに、多要素認証を利用可能なメールサービスへの移行を検討するとしている。
70	2022/8/11	届出者（一般団体）のメールアカウントからスパムメールが送信されたため、該当アカウントのパスワード変更を実施したとメールサーバの提供業者より連絡があった。原因は、攻撃者が何らかの方法で該当アカウントの認証情報を窃取したと推測されるが、詳細は不明である。再発防止策として、当該アカウントのパスワードをより強度が高いものへと変更した。それ以外のアカウントのパスワードについても順次強度の高いものへと変更する予定としている。
71	2022/9/8	届出者（企業）が運用するウェブサイトに対して、同一の発信元 IP アドレスからの大量のアクセスが発生しているとサーバの運営委託業者より連絡があった。調査したところ、当該サイトへ約 7 百万回にも及ぶ総当たり攻撃が行われており、一部のアカウントが不正アクセスされ、会員情報が閲覧された可能性があることが判明した。更に、一部のアカウントではポイントが不正に利用される被害が発生していることも確認された。原因は、システム移行作業に伴うセキュリティ設定の変更を行っている間、一時的に脆弱な状態が生じており、そこを攻撃者に狙われたことであった。本件の対応として、CDN（Content Delivery Network）と WAF によるアクセス制御を行った。また、不正ログインされたアカウントについてはパスワードの強制リセットを実施した。再発防止策として、アクセス制限の見直しや監視の強化を実施するとしている。

項番	届出日	概要
72	2022/10/19	届出者（企業）が利用する在宅勤務用のゲートウェイサーバのアクセスログを確認したところ、通常の数十倍ものログイン試行が行われていることを発見した。調査の結果、いずれもログインには失敗しており、被害は確認されなかった。その後も数日にわたり、同程度のログイン試行が見られたが、発見から 1 週間程度で観測されなくなった。再発防止として、ゲートウェイサーバのグローバル IP アドレスを変更し、今後は IP アドレスの遮断や攻撃を自動検知する仕組みの導入等を検討している。
73	2022/10/30	届出者（企業）が運営する EC サービスにおいて不審なアクセスが検知された。調査した結果、届出者が提供するアプリから EC サイトへアクセスする際に使われる非公開の API について、それを利用した数百万件以上にも及ぶログイン試行が確認された。そのうちの数千件がログインに成功していたことから、パスワードリスト攻撃が行われたものと推定している。当該サービスでは、公開されているログイン画面に対するパスワードリスト攻撃の対策は行っていたが、アプリで利用する API からのアクセスに対しては同様の対策を行っていなかった。このため、攻撃が成功したものと推測している。対応として、不正ログインに成功したアカウントのパスワードをリセットした。更に、攻撃元 IP アドレスの遮断を実施した。再発防止策として、API の利用やセキュリティ機器の設定見直し、監視体制の強化等を行った。

項番	届出日	概要
74	2022/11/7	届出者（企業）が運営する EC サイトにおいて、特定の会員から短時間に複数回の注文が行われたことを発見した。調査の結果、当該 EC サイトにおいて、攻撃者が不正に会員登録を行い、クレジットマスター攻撃と呼ばれる、クレジットカードの有効性を確認する総当たり攻撃が行われたことが判明した。原因については不明だが、当該サイトにて、クレジットカード情報の入力回数に制限を設けていなかったため、攻撃者に悪用されたものと推測される。対応として、発見した不正な注文を削除したが、攻撃が継続して行われたため、当該サイトとカード決済を停止する措置を取った。再発防止策として、クレジットカード入力回数の制限や攻撃と判断したアクセスを遮断する機能を持つサービスを導入した。

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、サービス妨害を目的とした攻撃（以下、サービス妨害攻撃）や、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等について分類している。

今期においては、サービス妨害攻撃に関する事例が 2 件確認された。この攻撃の標的となった場合、ウェブサイトやサーバのレスポンスの遅延、あるいは機能が停止する等して、業務遂行に支障が出るだけでなく、組織によっては機会損失による損害が発生する可能性がある。そのため、攻撃の影響を緩和する ISP（Internet Service Provider）や CDN の利用、WAF を導入する等の対策を事前に実施しておくことが望ましい。あるいは、不正アクセス元の IP アドレス等を迅速に特定・遮断（制限）するための手順の確立等を検討してほしい。

また、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ある。直接的な原因は異なっていたとしても、前節までに述べてきた対策を行うことは、セキュリティの向上につながり、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。このため、2-3 節や 2-4 節の内容を参考に対策を検討していただきたい。

表 2-6 にその他の届出事例に関する概要一覧を示す。

表 2-6 その他の届出事例の概要一覧

項番	届出日	概要
75	2022/7/28	届出者（一般団体）の取引先から、過去に送受信したメールの本文を引用した不審なメールが届いていると連絡があった。当該メールには、Excel ファイルや PDF ファイル、iso ファイル等が添付されているものもあった。組織内のパソコン等を調査したが、当該のメールを送信したログはなく、ウイルス等も発見できなかった。職員全員がパソコンのログインパスワードを変更しても事象が継続したため、メールサーバ等のシステムを一新したところ、不審なメールは発信されなくなった。原因について届出者は、クラウド上に設置したサーバにバックドアを仕掛けられ、メールの送信の踏み台にされたものと推測している。再発防止策として、組織内の全てのパソコンにセキュリティソフトを導入した。

項番	届出日	概要
76	2022/9/16	届出者（企業）が利用するインターネット接続用のネットワーク機器において、一部の通信の応答がないことを監視システムが検知した。調査したところ、インターネット上の不明な機器から当該ネットワーク機器に対して、数 Mbps 程度の不正なパケットが送り付けられていることが確認された。また、一部の通信の応答がなくなった原因について、届出者は当該ネットワーク機器の不要なパケットを破棄するソフトの処理に負荷が掛かり、あて先情報管理テーブルが正常に更新されなかったため、当該機器を経由する通信ができなくなったものと推定している。対応として、不正アクセス元からのアクセスを遮断した。更に、同様の事象が発生した際に、業務影響を低減させるため、あて先情報管理テーブルの一部を動的レコードから静的レコードへと変更した。再発防止として、アクセス制限の見直しを行った。
77	2022/9/23	届出者（企業）の従業員からの問い合わせにより、ウェブサーバ内に保管していたメールアドレス等の個人情報数万件が流出したことが判明した。更に、流出したメールアドレス宛に不正なメール送信が行われていることも確認された。原因は、外部からサーバに対して不正アクセスされたものと推測されるが、具体的な手口は不明である。対応として、当該サイトを停止させ、個人情報が流出した可能性のある対象者に注意喚起を行った。再発防止策として、利用していたシステムとプラットフォームの刷新、アクセス制限や監視体制の強化、従業員に対する研修等を実施した。
78	2022/10/4	届出者（企業）のウェブサイトにてエラーが頻繁に発生し、サイトの利用が困難な状態になっていることを確認した。届出者のシステム管理の委託業者に調査を依頼したところ、ウェブサーバ内の特定のファイルを狙った大量の不正アクセスが行われていることが判明した。不正アクセスの内容から、分散反射型の DoS 攻撃（DRDoS）を受けたものと推定している。対応として、攻撃元の IP アドレスを遮断する等の措置を行った。

3. 事例：フリーツールを悪用したファイルの暗号化及び削除による被害

3-1. 届出内容

（1）　発見経緯

届出者（企業）が利用する社内システムにおいて、サービス停止が発生したことを監視システムが検知した。調査を行ったところ、オンプレミスとクラウド（AWS）に設置していた複数台のサーバが第三者からの不正アクセスを受け、サーバ内に保管していた一部のファイルが暗号化されていることが確認された。

（2）　被害原因

本事例における被害原因を、攻撃の流れ（初期侵入から暗号化及び削除の被害を受けるまで）とともに、順に説明する。

本事例の攻撃の流れを図 3-1 に示す。

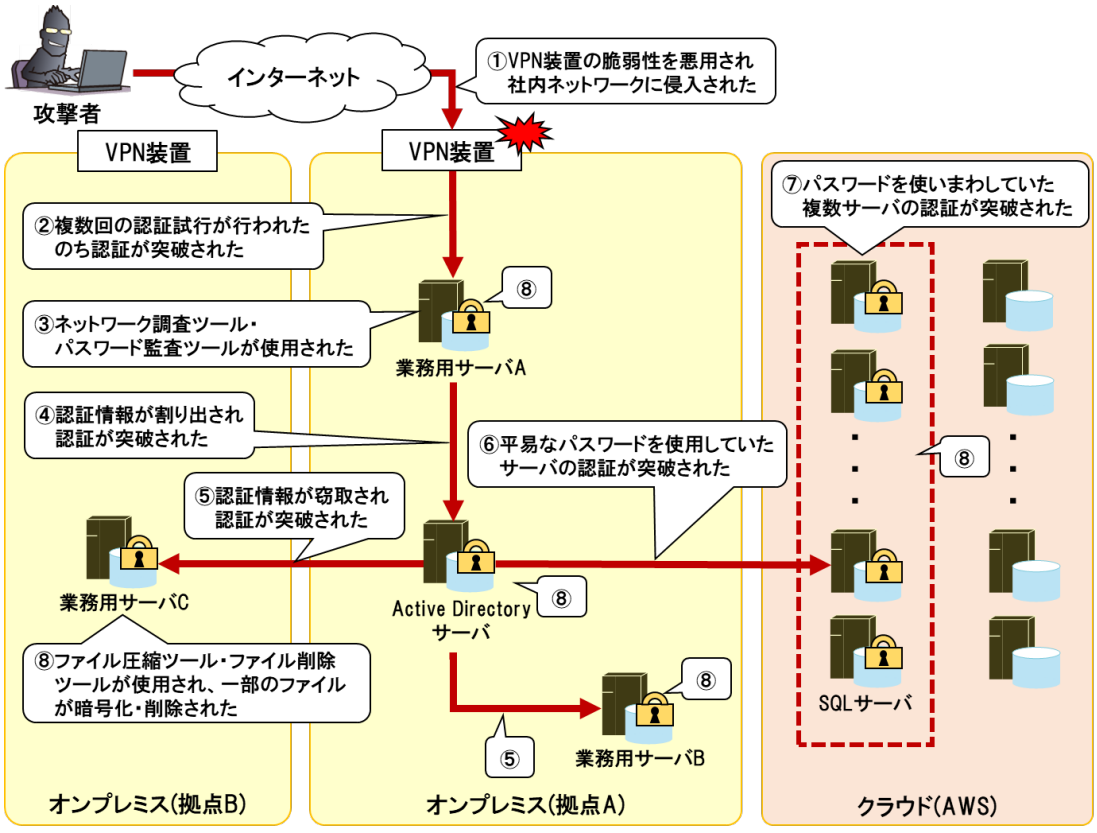

図 3-1 攻撃の流れ（※届出いただいた情報を基に IPA で作成）

a) 初期侵入の原因

VPN 装置（FortiGate）の脆弱性（CVE-2018-13379）を悪用され、社内ネットワークに侵入された（図 3-1 ①）。

当該脆弱性が残存していた理由は、届出者と保守委託業者との間で、VPN 装置の脆弱性対応に関する取り決め等が定められておらず、脆弱性管理が適切に実施されていなかったためである。

b) サーバ侵害の原因

社内ネットワークへの侵入後、オンプレミスに設置していた業務用サーバ 1 台（図 3-1 業務用サーバ A）に対して、複数回の認証試行が行われたのち、認証を突破された（図 3-1 ②）。この業務用サーバ A が侵害された原因は、ドメイン名やコンピュータ名等から容易に推測可能なパスワードを使用していたためである。

c) 侵害範囲拡大の原因

業務用サーバ A の侵害後、サーバ上でフリーツール[11]のネットワーク調査ツールとパスワード監査ツールが使用された（図 3-1 ③）。これにより、Active Directory サーバが特定され、認証情報が割り出されたことで認証が突破された（図 3-1 ④）。その後、オンプレミスに設置していた別の業務用サーバ 2 台（図 3-1 業務用サーバ B・C）とクラウドに設置していた SQL サーバ 20 台の認証が突破され、侵害範囲が拡大した。

Active Directory サーバの認証情報がパスワード監査ツールにより割り出された原因は、使用していたパスワードが平易なものであったためである。Active Direcroty サーバと同拠点にある業務用サーバ B と、別拠点に設置していた業務用サーバ C の認証情報は、Active Directory サーバの侵害後、何らかの方法で窃取されたものとみられる（図 3-1 ⑤）。クラウドに設置していた SQL サーバが侵害された原因は、平易なパスワードを使用しており（図 3-1 ⑥）、かつ、パスワードの使いまわしをしていたためである（図 3-1 ⑦）。

d) 暗号化被害の原因

侵害範囲の拡大後、各種サーバに保管していた一部のファイルが暗号化され、暗号化前のファイルについては削除された（図 3-1 ⑧）。このファイルの暗号化と削除に

[11] 本紙では、フリーソフトやフリーウェア、GitHub から入手可能なソフトウェアやソースコード等を総称して「フリーツール」と呼ぶ。

は、攻撃者によって不正にインストールされたファイル圧縮ツールとファイル削除ツールが利用されたことが判明している。

（3）　被害内容

本事例では、オンプレミスに設置していたサーバ 4 台とクラウドに設置していたサーバ 20 台が不正アクセスを受け、各種サーバに保管していた一部のファイルが暗号化及び削除の被害に遭った。また、サーバ内には、攻撃者が設置したとみられる脅迫文（テキストファイル）が残されていることも確認された（図 3-2）。

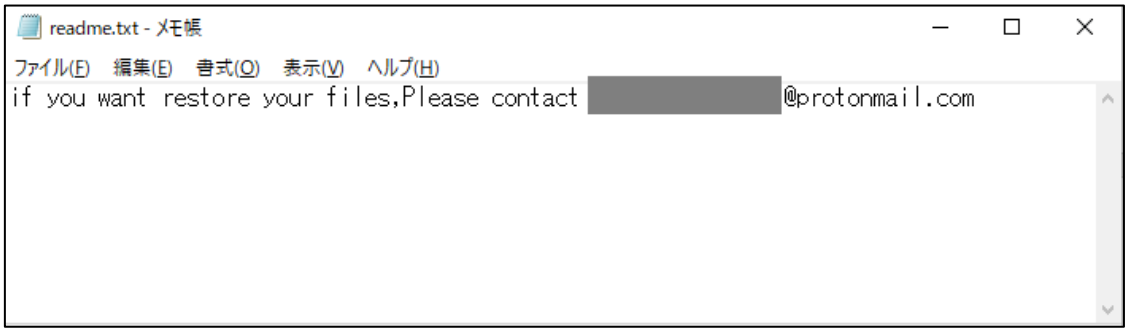

図 3-2 脅迫文（※届出いただいた情報を基に IPA が作成）

なお、被害を受けたサーバはバックアップから復旧できたため、社内システムの停止による業務への影響は少なかったとのことであった。

その後の調査の結果、攻撃者によってサーバ内のデータが外部へ転送された痕跡は確認されなかったものの、攻撃者が届出者のネットワークに侵入してから約 60 時間の間、各種サーバ上のファイルにアクセスしていたことから、サーバに保管していた数百万件以上の顧客データや社内データ等を不正に閲覧された可能性がある。

（4）　被害対応

- 技術的対策
  - 各種サーバの停止とインターネット接続の切断
  - 各種サーバをバックアップデータから復旧
  - 外部調査機関による詳細調査を実施
- 組織的対策
  - 本被害の対策本部を設置
  - コールセンターの設置
- 組織外への報告等
  - ウェブページにて本被害について公表

- 個人情報保護委員会への報告

（5） 再発防止策

- 技術的対策
  - 各種サーバの管理者アカウントの見直しとパスワードの複雑化
  - 各種サーバのアクセス制限の見直し
  - 多要素認証の導入によるユーザ認証の強化
  - 社内及び社外ネットワークにおける通信の暗号化
  - 社内ネットワークにおけるログ監視の強化
- 組織的対策
  - サーバ運用作業に関する記録の徹底
  - 脆弱性対応及びインシデント対応の体制見直し
- 人的対策
  - 従業員に対するセキュリティ教育・研修制度の整備

3-2. 着目点

（1） フリーツールを悪用した攻撃

本事例では、次のフリーツールを悪用した攻撃が確認された。いずれのツールについても、届出者が対象のサーバに導入していたセキュリティソフトでは、検知・駆除されなかったとのことであった。

- netscanold [12]：ネットワーク調査ツール
- SNETCracker[13]：パスワード監査ツール
- 7-Zip[14]：ファイル圧縮ツール
- WipeFile[15]：ファイル削除ツール

これらのツールは、無料で公開されており、誰もが簡単に入手・利用できるものである。また、ツール自体は不正なものではなく、一部のツールは広く利用されていることから、攻撃者がセキュリティソフトの検知を回避する目的で悪用する場合がある。また、本事例で確

[12] ネットワークに関する情報を取得するために利用されるツール

[13] 脆弱なパスワードを使用するアカウント等を検出するために利用されるツール

[14] ファイルやフォルダを圧縮・解凍するために利用されるツール（圧縮する際に、任意のパスワードを設定することで、圧縮したファイル等を暗号化できる）

[15] ファイルやフォルダを削除するために利用されるツール（削除した内容は復元できないとされている）

認されたフリーツール以外にも、公開情報では、オープンソースのエクスプロイトツールである Mimikatz やリモート操作ツールの AnyDesk 等がランサムウェア攻撃に悪用されているとして注意が呼び掛けられている [16]。

こうしたフリーツールを悪用した攻撃への対策としては、企業・組織内で許可していないツールのインストールを禁ずる等といった対応が求められる。また、フリーツールの利用を検討する、あるいは継続的に利用する場合には、自組織内で慎重に評価を行い、安全であると確認できたツールのみ利用するといった対応が望ましい。

（2） バックアップによるデータの復元

本事例では、ランサムウェアを用いた暗号化ではなく、フリーツールにより暗号化及び削除が行われた。フリーツールによる暗号化被害においても、ランサムウェアによる被害と同様に、データを復元することは困難な場合がある。

そのため、被害を受けた場合に備え、事前にデータのバックアップの取得と復元手順の確認をしておくことが重要である。しかしながら、攻撃者はそれを見越して、バックアップデータも暗号化することで、データを復元できないようにした事例もあることから、複数のバックアップを保持し、ネットワークから隔離された環境で保管するといった対策を検討する必要があるだろう。

（3） 脆弱性の管理不足

本事例では、届出者と VPN 装置の保守委託業者との間で、脆弱性対応に関する取り決め等が定められておらず、脆弱性管理が適切に実施されていなかった。

組織内で利用している製品やサービスの運用・保守を外部に委託している場合において、適切な脆弱性対応を実施していくためには、委託先との責任分界点を正確に把握した上で、自組織の対応範囲となるセキュリティ対策の作業や被害発生時の対応フロー等を明確化しておくことが重要である。

また、本事例のように、FortiGate の脆弱性（CVE-2018-13379）の悪用によって、不正アクセス被害を受けたとする届出を複数確認している。当該脆弱性については、2020 年に影響を受けたとみられるホストの一覧が外部に流出したと報じられており [17]、FortiGate を

---

[16] Sophos「政府機関のコンピュータに数か月潜伏した後、Lockbit ランサムウェアを展開した攻撃者」
https://news.sophos.com/ja-jp/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware-jp/

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

脆弱性の影響を受けないバージョンにアップデート対応していたとしても、対応前に脆弱性を悪用され、認証情報が窃取されている恐れがある。そのため、既に対応済みであったとしても、アカウントのパスワード変更を実施しておくことを勧める。

（4）　脆弱なパスワードの使用と使いまわしによるサーバの侵害

本事例では、複数台のサーバにおいて、脆弱なパスワードの使用やパスワードの使いまわしが行われていたため、攻撃者に認証を突破され、侵害範囲が拡大した。

組織において、パスワード認証は、パソコンやサーバへのログイン時だけでなく、VPN 装置やリモートデスクトップサービスを利用したリモート接続時、Microsoft 365 のようなクラウドサービスへのログイン時等といった重要な場面でも行われている。このような状況において、脆弱なパスワードの使用やパスワードの使いまわし、あるいはデフォルトの ID（root や Administrator 等）を変更せず使用していた場合、攻撃者によるパスワードの推測やパスワードリスト攻撃等の方法で認証が突破されてしまい、社内ネットワークへの不正侵入やアカウントの不正利用による様々な被害が発生する可能性がある。このような被害を防ぐために、組織内で、単純で推測されやすいパスワードを使用していないか、パスワードの使いまわしが行われていないか、デフォルトの認証情報を変更しないまま使用していないか等を確認し、該当するアカウントがあれば、即座にパスワード変更を実施していただきたい。

また、多要素認証の導入やパスワードポリシーの設定、パスワード認証時の試行回数に制限を設けるといった対策も有効といえる。万が一、悪意のある第三者に認証が突破された場合に備えて、アカウントに付与する権限を必要最小限にしておくことが望ましい。

（5）　Active Directory サーバを狙った攻撃

今期においても、本事例のように初期侵入の後、攻撃者によって Active Directory サーバを侵害され、被害範囲が拡大したとする届出を複数確認している。Active Directory サーバは、ネットワーク内のユーザやコンピュータを一元管理できるため多くの組織が導入している一方で、侵害範囲を拡大する目的で攻撃者に狙われる傾向にある。このため、脆弱性対策の徹底はもちろんのこと、脆弱なパスワードの使用や不要なアクセス権限が設定されていないか等を見直す必要がある。Windows システムの設定・運用方法については、Microsoft 社から資料[18]が公開されているため、参考としていただきたい。

---

[18] Microsoft「Active Directory のセキュリティ保護に関するベスト プラクティス」
https://learn.microsoft.com/ja-jp/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

4. 事例：初動対応後に再度の攻撃と複数の影響が発生した被害

4-1. 届出内容

（1）　発見経緯

届出者（企業）が運用するウェブサイト上に不審なページが公開されていることを第三者が発見し、その連絡がレンタルサーバの提供業者（以下、サーバ提供業者）を通して、届出者へと報告された。

本事例では、脆弱性の悪用による初回の攻撃と、初動対応後に再度の攻撃が行われる、といった 2 回の攻撃による被害を受けた。図 4-1 では、初回の攻撃が発生してから届出者がその被害に関する報告を受けるまでの流れを示す。

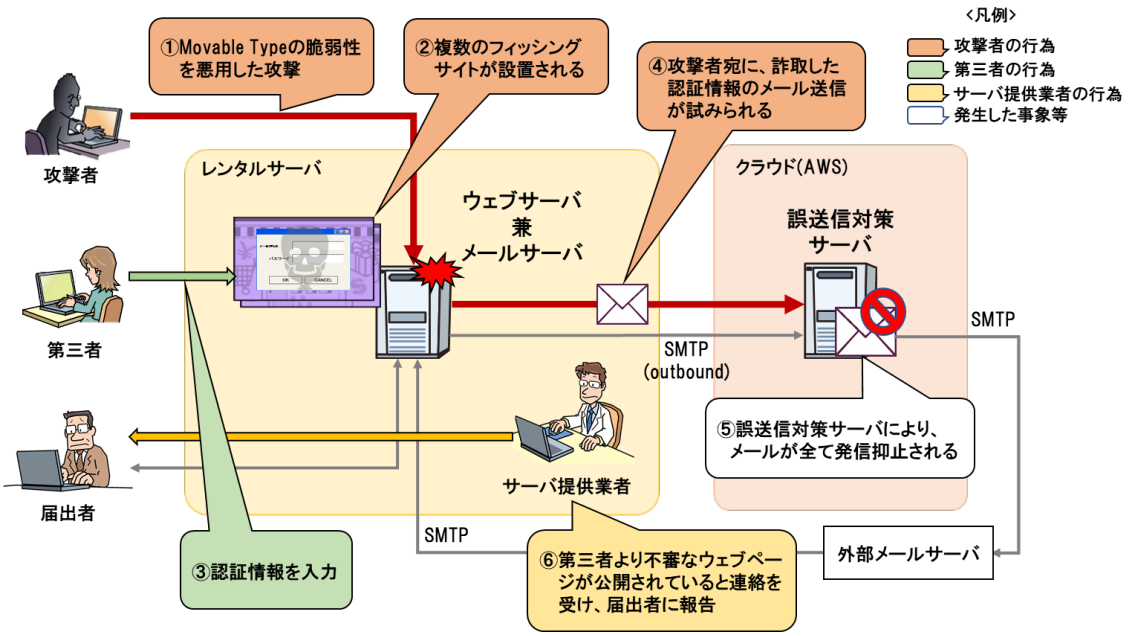

図 4-1 初回の攻撃の流れ（※届出いただいた情報を基に IPA が作成）

次の図 4-2 では、届出者が初動対応を実施した後に、再度の攻撃が行われ、届出者がその発生した影響の調査報告を受けるまでの流れを示す。

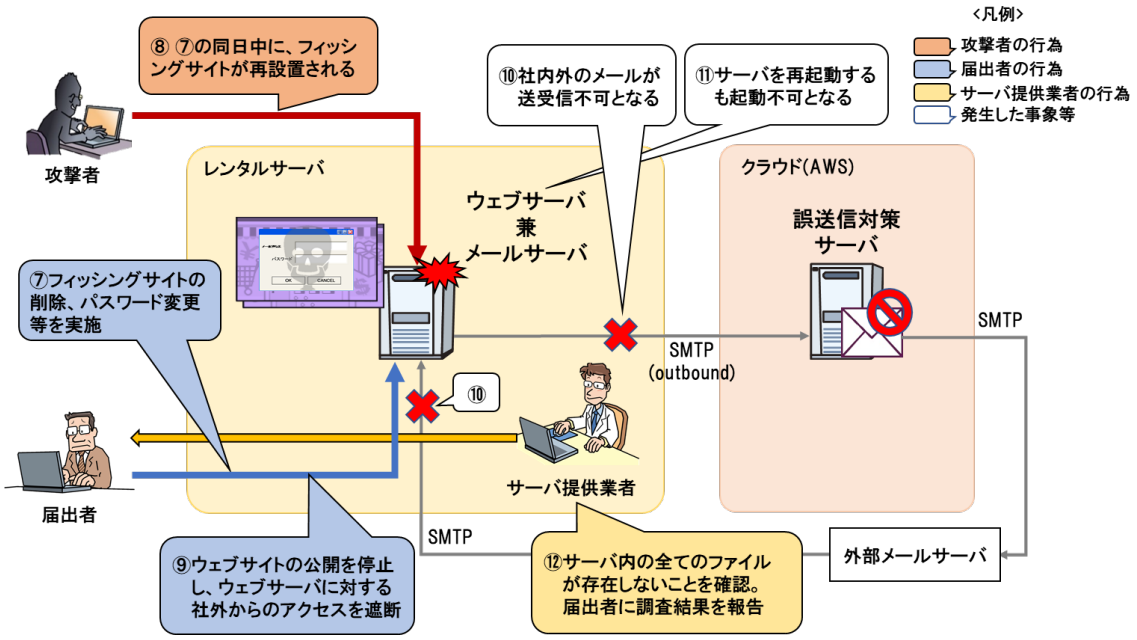

図 4-2 初動対応後の流れ（※届出いただいた情報を基に IPA が作成）

（2） 被害原因

被害に遭ったウェブサイトは、サイトの運用・管理に Movable Type を利用していた。当時利用していた Movable Type は最新バージョンではなく、Movable Type の XMLRPC API における OS コマンド・インジェクションの脆弱性（CVE-2021-20837）が確認されているバージョンであった。このため、当該脆弱性を悪用した攻撃[19]により、フィッシングサイトが設置されたものと推測している。

当該脆弱性が残存していた理由は、届出者内でサーバの保守や運用に関する体制が適切に整備されておらず、担当者が脆弱性の存在に気づく前に攻撃を受けてしまったとのことであった。

（3） 被害内容

本事例では、Movable Type の脆弱性を悪用した攻撃により、クラウド上のレンタルサーバに設置した届出者のサーバ（ウェブサーバとメールサーバを兼用）が不正アクセスされ、サーバ内に複数のフィッシングサイトが設置された。当該フィッシングサイトは、偽のメール等から誘導された第三者が入力した認証情報を、攻撃者にメール送信する仕掛けがあった。

---

[19] 株式会社ラック「【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

届出者は、サーバ提供業者からの報告を受け、サーバに設置されたフィッシングサイトの削除やパスワードの変更等を実施した。

しかし、同日、攻撃者によりフィッシングサイトの再設置が行われた。その後、当該サーバにおいて、社内間のやり取りを含む、全てのメール送受信ができなくなっていることが確認された。更に、サーバ自体の再起動もできなくなっていたため、サーバ提供業者に原因調査を依頼したところ、攻撃者により、サーバ内のシステム領域とユーザ領域を含めた全てのファイルが消去されたことが判明した。なお、攻撃者がどのようにファイルの消去を行ったかについては不明である。

本件の対応にあたり、フォレンジック調査やホームページ復旧に外部業者の協力を受け、数百万円の費用が発生した。

（4） 被害対応

a) 初回の攻撃に対して実施した内容

- 技術的対策
  - 攻撃者によって設置された複数のフィッシングサイトの削除
  - パスワードの変更を実施
  - アクセス元の IP アドレスを記録するサービスの導入
  - 外部業者へフォレンジック調査及びホームページ復旧の協力を依頼

b) 再度の攻撃に対して実施した内容

- 技術的対策
  - ウェブサイトの停止
  - 社外からウェブサーバへのアクセスを遮断
  - メールデータの復旧
- 組織外への報告等
  - 個人情報保護委員会（PPC）、日本情報経済社会推進協会（JIPDEC）へ届出を実施

（5） 再発防止策

- 技術的対策
  - 不正アクセスが行われたウェブサイトを閉鎖
  - 不正アクセスの原因に対する対策を実施
  - サービス提供元が異なる「ホームページホスティングサービス」「メールサービス」の利用に切り替え

4-2. 着目点

（1）　事業継続性計画と緊急対応手順の整備

不正アクセスをはじめ、サイバー攻撃による被害を最小限に抑えるためには、事前に情報セキュリティの観点を組み込んだ BCP を策定し、インシデントの影響度に応じた対応計画を講じておく必要がある。本事例のような不正アクセスが確認された場合、攻撃対象となっているサーバを外部ネットワークから切り離すことも一案として考えられるが、組織の基幹システムや EC サイトを運営しているサーバなどが被害対象である場合、初動からネットワークの切り離しを行ってしまうと、業務影響や機会損失が深刻となり得る可能性がある。そのため、自組織で被害が確認された場合に、初動対応としてどこまで実施すべきか等を明確化しておく必要がある。その状況に応じて、システムの停止や縮退運転の判断、関係組織への協力依頼などを速やかに行うことが望ましい。なお、本事例のように、メールサーバにも被害が波及し、外部への連絡が取れなくなる事態が発生する可能性もあることから、連絡の代替手段等も確認しておくことを勧める。

もし、これらの対応が組織内での人員不足で難しい場合や、策定はしたが実効性に不安がある場合などは、外部の専門業者から技術的なサポートを受けられるように、インシデント対応支援サービスの導入等も検討していただきたい。

（2）　サーバの兼用による被害拡大

本事例では、ウェブサーバとメールサーバを兼用していたため、サイト改ざんの被害だけでなく、メールの送受信不可という被害も発生した。一台のサーバを複数の用途に利用していると本事例のように、別のサービス運用にまで影響が及ぶ可能性がある。そのため、重要なシステムはサーバを分け、サーバを特定の用途のみに限定することが望ましい。

サーバを兼用する場合には、アクセス権限設定や脆弱性対策の管理等といった基本的な防御策をより一層徹底することが重要である。

（3）　脆弱性管理の重要性

本事例では、サーバの保守や運用に関する体制が適切に整備されておらず、担当者が脆弱性対応の必要性を認識する前に攻撃を受けてしまった。脆弱性の管理を適切に実施するためには、自組織内で利用している製品を把握し、その製品に関連する脆弱性情報を収集して、影響を受ける脆弱性の評価を行い、対応計画のもと修正プログラムを適用する、といった一連の作業を継続的に実行していく必要がある。更に、脆弱性は日々発見されており、その中には、攻撃者が容易に悪用可能な脆弱性が見つかることもあるため、公表された脆弱性に対しては、時期を逸しない対応が求められる。また、ゼロデイ攻撃の場合、脆弱性の修正プログラムが公開される前に脆弱性を悪用した攻撃が行われるため、開発元などが公開する回

避策や緩和策の適用、必要に応じて、該当する製品や機能を一時的に停止するなどの対応が求められる。

IPA が公開している次の資料では、脆弱性対策を実施する上での考え方や、具体的な脆弱性関連情報の収集先、脆弱性の分析方法などを解説している。こちらを参考に、自組織の脆弱性管理を見直すことを勧める。

- 脆弱性対策の効果的な進め方（実践編）第 2 版～脆弱性情報の早期把握、収集、活用のスヽメ～
  https://www.ipa.go.jp/files/000071660.pdf

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 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）