コンピュータウイルス・不正アクセスの届出事例

［2020 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

2021 年 2 月 25 日

目次

1. はじめに

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

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

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

---

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

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

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

[4] IPA「不正アクセスに関する届出について」 https://www.ipa.go.jp/security/ciadr/index.html

[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

2020 年下半期（7 月～12 月。以下、今期）に受理した届出において、主な事例を 135 件取り上げ、次の 6 種に分類した。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感染の被害　（49 件）
- 身代金を要求するサイバー攻撃の被害　（21 件）
- 脆弱性を悪用された不正アクセス　（32 件）
- ID とパスワードによる認証を突破された不正アクセス　（22 件）
- クラウド環境への不正アクセス　（7 件）
- その他　（4 件）

今期に届出のあった被害について全体を通して見ると、これまでと同様に一般的によく知られたセキュリティ施策を実施していれば、被害を防げたと思われるものが大半を占めた。一方、主にデータを暗号化して復旧のための身代金を要求された被害の届出において、詳細に調査を行っても侵入の経路等、不正アクセスの手口が解明できなかったものがあった。また、様々な攻撃手法を駆使して、組織内のネットワークや組織が利用するクラウドサービス等へ侵害範囲を広げ、組織に甚大な被害をもたらしたもの等、高度な技術を持った攻撃者による、巧妙な侵入や被害拡大の手口が使われたものと思われる事例も見受けられた。身代金を要求するサイバー攻撃の被害については 2-2 節で説明する。

分類ごとの届出件数では、コンピュータウイルス（以下、ウイルス）（ランサムウェアと見なしたものは除く）の発見や感染被害の届出が 49 件と突出して多く、そのうち 44 件は「Emotet」と呼ばれるウイルス（以下、Emotet）に関わるものであった。ウイルス感染の被害については 2-1 節で説明する。

次いで多かったのが、製品やソフトウェアの不具合やセキュリティ設定の不備などの脆弱性を悪用された不正アクセスである。今期の特徴の一つに、テレワークへの対応時に、脆弱性対策やセキュリティ設定が不十分だったことが原因で不正アクセスにつながったとの事例が複数見受けられたことがある。脆弱性を悪用された不正アクセスについては 2-4 節で説明する。

その他には、クラウド型のサービスやクラウド上の開発環境等が攻撃の対象にされた事例が目立った。2-5 節で説明する。

なお、本紙に示した事例以外にも、ウイルスの発見・感染、フィッシングメールの受信、アカウント窃取等の情報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別途「コンピュータウイルス・不正アクセスの届出状況」として公開している。

2-1. コンピュータウイルス感染の被害

今期も、利用しているパソコンがウイルス感染の被害にあったという事例の届出が多く、そのほとんどは Emotet の検知や感染、または Emotet への感染を狙ったメールの着信の届出であった。他には「IcedID」[6]と呼ばれるウイルス（以下、IcedID）の検知や感染の事例も複数見られた。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 [7]。

IPA では 2019 年 9 月中旬頃から 2020 年 2 月上旬頃まで Emotet 感染を狙う攻撃メールが国内に広くばらまかれていることを観測していたが、その後、5 か月間程はメールのばらまきを観測しておらず、届出も月に数件であった。今期、7 月中旬頃から再び攻撃メールを観測するようになり、9 月にはパスワード付きの ZIP ファイルを添付した攻撃メールや、12 月には「クリスマス」や「賞与支給」といった年末の時期に合わせた件名や添付ファイル名の攻撃メールを確認している。添付ファイルにパスワードを設定する手口は、メール配送経路上でのセキュリティ製品の検知・検疫のすり抜けを狙ったものと思われる。時節柄に合わせた件名等で興味を引き、警戒心を薄れさせることも狙っており、攻撃者は手口を変えながら様々な方法で拡散を図っていたと考えられる。

なお、2021 年 1 月 27 日には、EUROPOL（欧州刑事警察機構）から、Emotet のばらまきに関わった攻撃者の一部を逮捕し、攻撃基盤の停止に至ったとの発表 [8]があった。その日以降、Emotet の検知・感染の届出はなく、攻撃メールのばらまきも観測していない。

---

6 トレンドマイクロ セキュリティブログ「「EMOTET」に続き「IcedID」の攻撃が本格化の兆し、パスワード付き圧縮ファイルに注意」
https://blog.trendmicro.co.jp/archives/26656

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

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

表 2-1 に Emotet を検知または感染した届出の一覧を示す。

表 2-1 Emotet 検知・感染に関する届出一覧

項番	届出日	届出者の主体	概要
1	2020/8/4	企業	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 Emotet を検知した。 ● 組織内に、Emotet への感染を狙ったと思われるマクロ付きの Word 文書ファイルが添付されたメールが着信した。 ● 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。
2	2020/8/17	企業	
3	2020/9/1	企業	
4	2020/9/1	企業	
5	2020/9/2	企業	
6	2020/9/3	非営利団体	
7	2020/9/4	企業	
8	2020/9/10	企業	
9	2020/9/11	企業	
10	2020/9/12	企業	
11	2020/9/16	企業	
12	2020/9/16	企業	
13	2020/9/19	企業	
14	2020/9/20	企業	
15	2020/9/20	企業	
16	2020/9/23	一般団体	
17	2020/9/23	企業	
18	2020/9/24	企業	
19	2020/9/24	企業	
20	2020/9/25	企業	
21	2020/9/25	一般団体	
22	2020/9/25	企業	
23	2020/9/28	企業	
24	2020/9/29	企業	
25	2020/9/30	企業	
26	2020/10/1	企業	
27	2020/10/2	企業	
28	2020/10/2	企業	
29	2020/10/5	一般団体	
30	2020/10/5	企業	
31	2020/10/20	業界団体	
32	2020/10/20	企業	
33	2020/10/21	企業	
34	2020/10/23	企業	
35	2020/10/23	企業	
36	2020/10/28	企業	
37	2020/11/2	企業	
38	2020/11/2	企業	
39	2020/11/4	企業	
40	2020/11/6	企業	
41	2020/11/12	企業	
42	2020/11/16	企業	
43	2020/12/2	企業	
44	2020/12/8	企業	

（2）　Emotet 以外のウイルス

Emotet 以外には、IcedID に関わる届出が複数見られた。IcedID は 2017 年 9 月に最初に発見されたとされるバンキングトロイ（インターネットバンキングの情報窃取を行うウイルス）であり、2020 年 10 月頃から、この IcedID への感染を狙ったとみられる攻撃メールがばらまかれていたことを観測している。これらの攻撃メールは Emotet の攻撃メールと類似しており、メールの返信を装った日本語のメールで、マクロが含まれた Word 文書ファイルがパスワード付き ZIP ファイルとして添付されていたものもあった。このケースでは Word 文書ファイルを開いてマクロを有効にすると、IcedID がダウンロードされ、パソコンに感染させられてしまう。IcedID は拡散や感染させるための手口が Emotet と似通っていたため、発見した当初は IcedID を Emotet と誤認し、調査や対策を行っていく中で誤認に気づき対策を変更した事例もあった。

Emotet や IcedID は正規のメールを装った攻撃メールによって拡散し、攻撃メールに添付されている文書ファイルのマクロを有効にすることで感染するものが多い。不審であると見破ることは難しいが、送信元や本文に見覚えがある返信メールの形態であっても、攻撃メールかもしれないと念頭に置くこと、および入手した文書ファイルが信用できると判断できない場合は「編集を有効にする」「コンテンツの有効化」のボタンはクリックしないことが重要である。

表 2-2 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 ウイルス感染に関する届出の概要一覧

項番	届出日	概要
45	2020/8/18	届出者（企業）のパソコンで、セキュリティソフトがウイルスを検知し削除した。同時期に同社のメールアカウントから迷惑メールがばらまかれる現象が発生しているが、当該ウイルス検知との因果関係は不明であった。
46	2020/11/5	届出者（一般団体）のパソコンでウイルスが検知された。セキュリティソフトにより削除されたため被害は特になかった。
47	2020/11/13	届出者（企業）のパソコンで、IcedID と呼ばれるウイルスをセキュリティソフトが検知し削除した。被害は発生していない。
48	2020/11/20	届出者（企業）のパソコンで、IcedID と呼ばれるウイルスをセキュリティソフトが検知し削除した。被害は発生していない。

項番	届出日	概要
49	2020/12/8	届出者（企業）から、IcedID と呼ばれるウイルスの感染を狙ったメールが届いたとの連絡が取引先からあった。当該メールは届出者のメールシステムから送られたようであったが、パソコンがウイルスに感染していたのか、メールシステムが不正アクセスされてメールの送信に悪用されたかは不明であった。

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[9]など、ファイルやデータを暗号化もしくは消去して、その復旧と引き換えに（身代金として）金銭を脅し取ろうとするサイバー攻撃の届出も多かった。事例には次のようなものがあった。

- ファイルが暗号化され、脅迫文のようなメッセージが表示されるパソコンが次々と発見されるといった事象より、組織内のネットワークを通じて数多くのマシンにランサムウェアによる被害が拡大したと思われるもの
- ウェブサーバやデータベースサーバ等からファイルやデータが消去され、代わりに脅迫文が残されていたといった事象より、外部から直接サーバ等へ不正アクセスしてデータ消去を行ったと思われるもの

組織内の多数のパソコンに感染し被害が拡大した事例には、攻撃者がパソコン等を遠隔操作で乗っ取り、そこから組織内ネットワークを密かに移動する活動（ラテラルムーブメント）の過程で、ドメインコントローラ等の管理サーバを発見すると更にそれを乗っ取り、アプリケーションの配布機能を悪用して組織内の多数のパソコン等に感染を拡げ、広範囲に及ぶ甚大な被害を及ぼした例があった。

サーバに直接不正アクセスしたと考えられる事例では、ファイルやデータの消去に加え、接続元アドレスや操作履歴等の記録が残るログファイルも消去されており、不正アクセスの痕跡の隠滅を図ったと思われる例があった。

いずれも攻撃の手口が巧妙化、高度化している例と考えられ、今後も更に高度化した手

---

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

口での攻撃が行われる恐れもあり、引き続き注意が必要である。

身代金を要求する攻撃に関する届出では、調査を行っても侵入経路等の究明に至らず原因は不明と記されていたものも複数見られた。しかし、そういった事例においても、脆弱性の対策が不十分な機器があったり、アクセス可能な IP アドレスの制限がなされていなかったり等、原因と考え得る箇所が見つかった例も多い。ランサムウェア対策の特設ページ[10]等を参考に、改めて基本的な対策ができているかを確認することを勧める。

表 2-3 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。また、ランサムウェアによる攻撃の一例について、項番 66 の事例の詳細を 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

項番	届出日	概要
50	2020/7/7	届出者（企業）の複数のパソコンで、一部のファイルの拡張子が意図せず変更されていることを発見した。改ざんされたファイルと同じフォルダに金銭を要求する脅迫文のような英文が書かれたテキストファイルが置かれており、ランサムウェアに感染したと考えられる状況であった。改ざんされたファイルに重要な情報が含まれていなかったため、金銭の要求には応えず、改ざんされたファイルを削除することで対処した。
51	2020/7/9	届出者（企業）が提供するクラウドサービスのテスト用サーバにおいて、データベースの一部が削除され、復旧のために金銭を要求する脅迫文が残されていたことに担当者が気づいた。外部専門機関とともに調査を実施したところ、サーバに対するコマンドインジェクション攻撃による不正アクセスにより、データベースからユーザ情報が流出している可能性が判明した。サーバへアクセスできる IP アドレスの制限等の対策を実施した。

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

項番	届出日	概要
52	2020/7/14	届出者（企業）のウェブサイトに不正アクセスがあり、データを消去され、代わりに金銭を要求するような文章が保存されていたことが発覚した。使用しているソフトウェアが古かったことから、システムの脆弱性を悪用されて不正アクセスされたものと思われるが、アクセスログ等が消去されており詳細な原因は不明であった。システム運用会社も含めて運用体制を一新し、脆弱性対策の厳格化による再発防止を図った。
53	2020/7/22	届出者（企業）のサーバにおいて、データベースの一部が削除され、復旧のために仮想通貨を要求する脅迫文が残されていたことを発見した。調査を行ったところ、外部業者の作業用に開放していたポートから不正アクセスされたことが判明した。IDとパスワードが窃取された原因は特定できておらず、総当たり攻撃等によりパスワード認証を突破されたと推測される状況であった。パスワードを複雑なものに変更することで対策し、更に多要素認証の導入によりセキュリティを強化することを検討している。
54	2020/7/27	届出者（企業）が使用しているクラウド上のファイルサーバにおいて、ファイルが改ざんされた状態になっていることを発見した。改ざんされたファイルの拡張子名から、DHARMA と呼ばれるランサムウェアに感染し、ファイルが暗号化されたものと推測される状況であった。感染経路は不明。バックアップしていたデータを別のサーバにリストアすることでシステムを復旧させた。
55	2020/7/31	届出者（企業）のシステムにおいて、クラウドに保管したデータの取得ができなくなったことにシステム担当者が気づいた。調査により、クラウド上のサーバに不正アクセスがあり、攻撃者がデータベース上のデータを一部消去したり身代金要求メッセージに置き換えたりした痕跡が見つかった。従業員のテレワーク対応のためにファイアウォールの設定を変更する際、設定の誤りが生じたことが原因と推測される状況であった。ファイアウォールの設定を修正することで対策し、再発防止のため不正アクセス監視機能の導入を検討している。

項番	届出日	概要
56	2020/8/26	届出者（一般団体）の利用するシステムがランサムウェアに感染し、ファイルが暗号化され利用できない事態に陥った。被害はオンプレミスとクラウドの両環境に及び、調査を行ったがランサムウェアの侵入経路については不明であった。アクセス権限の管理方法を見直して再発防止を図った。
57	2020/9/11	届出者（企業）のパソコンやサーバにおいて、ほとんどのファイルが暗号化され、ファイル名に特徴的な拡張子が付加されていた。ランサムウェアの一種に感染したものと考えられる。
58	2020/11/2	届出者（企業）が、自社のデータベースサーバにアクセスできないことに気づき、サーバにログインして状況を確認すると、ファイルを暗号化したとの脅迫文のようなメッセージが表示された。状況から DHARMA と呼ばれるランサムウェアの亜種に感染したと思われる状況であった。詳細な原因は不明だが、十分なセキュリティ対策を講じる前に、テレワーク対応のためにリモートデスクトップのポートを開放していたことから、RDP（リモートデスクトッププロトコル）を悪用した不正アクセスにあったものと推測している。パスワードポリシーを変更して、より強固なパスワードを使用する等の対策を行った。
59	2020/11/10	届出者（企業）がクラウド環境で利用している社内システムが停止したため、調査したところ、サーバ内のファイルが暗号化されており、復旧と引き換えに金銭を要求する脅迫文のようなテキストファイルが見つかった。ファイルの特徴から Sodinokibi と呼ばれるランサムウェアに感染したと思われる。原因について詳細に調査を行ったところ、テレワークに対応するために、クラウドへアクセス可能な IP アドレスの制限を緩和し、インターネットからのアクセスを許可した結果、攻撃者に悪用され不正アクセスを受けたものと考えられる状況であった。IP アドレス制限を再設定して対策するとともに、WAF や監視システムの導入による再発防止策を実施した。

項番	届出日	概要
60	2020/11/11	届出者（企業）の社内システムにおいて、データの内容が表示されない不具合が発生した。調査したところデータベース上のデータが改ざんされ脅迫文のようなデータに書き換えられていたことが判明した。詳細な調査により、システム構築時に使用したデータベース管理ツールが、簡易なパスワードが設定された状態で外部に公開された状態にあり、そのツールを通じて不正アクセスされたことがアクセスログ等から判明した。データベース管理ツールへのアクセスにIPアドレス制限をする等して対策した。
61	2020/11/16	届出者（企業）のサーバにおいて、ほとんどのファイルが暗号化され、更にファイル名が改ざんされて特徴的な拡張子が付加されていた。また、脅迫文のような画面も表示された。ランサムウェアの一種に感染したものと考えられる。
62	2020/11/16	届出者（企業）の開発環境のアプリケーションが正常に動作していなかったため、調査したところ、データベースが削除され、脅迫文のような文章が残されていることを発見した。更に詳細に調査したところ、外部から開発環境へのアクセスが可能になっており、データベースに対しての多数のログイン試行があったことから、データベースに不正アクセスされ、データが削除されたものと推測される。対策として、外部からアプリケーションへアクセスできない設定に変更した。
63	2020/11/18	届出者（地方自治体）のウェブサイトが閲覧できないとの問い合わせがあり、保守業者が調査を行ったところ、ウェブサイトのデータが消去され、データの復旧に身代金を要求する脅迫文のようなデータが書き込まれていたことが判明した。原因について詳細に調査を行ったところ、ウェブサイトをリニューアルした際に残っていた古いページから、データベース管理ツールにアクセスできる経路が存在することが判明した。更にアクセスログから、攻撃者に当該経路を悪用されて管理ツールへ不正アクセスされ、データの改ざんが行われたことが分かった。古いウェブサイトやツールに関わる経路を廃止し、ウェブサイトへの接続は必ず WAF を経由するように経路を変更することでセキュリティの向上を図った。

項番	届出日	概要
64	2020/11/18	届出者（企業）のパソコンやサーバにおいて、セキュリティソフトがランサムウェアを検知した。
65	2020/12/4	届出者（企業）の社内の複数のシステムにおいて障害が発生し、調査したところ、ランサムウェアによる攻撃を受けていたことが判明した。詳細な調査により、顧客に関する情報等、内部データが攻撃者により窃取された恐れがあることも判明した。原因や障害規模の調査、および再発防止に向けた取り組みは現在も継続して検討中である。
66	2020/12/11	届出者（企業）が、社内システムにアクセスできないことを確認し、調査を行ったところ、多数のパソコンやサーバが Egregor と呼ばれるランサムウェアに感染しており、データの暗号化や窃取、セキュリティソフトのアンインストールが行われていたことが判明した。攻撃者が、取引先を装ったメールと遠隔操作ウイルスによって社内ネットワークに侵入し、ドメインコントローラを乗っ取り、配下のパソコン等へ感染を広げたと推測される状況であった。バックアップデータからパソコンやサーバの復旧を行い、再発防止のため、通信の流れやパソコンの挙動を監視するシステムを導入して、早期検知と対処を図るようにした。 **※本事例は３章で紹介する。**
67	2020/12/16	届出者（企業）の多数のサーバにおいて、ファイルが暗号化され各フォルダに脅迫のような文章が書かれたテキストファイルが作成されていることを発見した。Egregor と呼ばれるランサムウェアに感染したものと思われる。サーバを初期化し、データをバックアップから復元することによって復旧させた。
68	2020/12/16	届出者（一般団体）のパソコンで、ファイルが暗号化され、復旧のために金銭の支払いを要求する脅迫文のような画面が表示された。FONIX（Dapato）と呼ばれるランサムウェアに感染したものと思われる。

項番	届出日	概要
69	2020/12/18	届出者（企業）のファイルサーバ上のファイルが暗号化され、ファイル名の拡張子が変えられていることに気づき、ファイルサーバを停止して調査を行った。専門業者による調査の結果、複数のサーバとパソコンがランサムウェアに感染していることが判明した。また、社外接続の VPN アカウントやディレクトリサーバの管理者アカウントの情報も攻撃者が入手しており、外部から VPN 接続を悪用して社内ネットワークに侵入し、ディレクトリサーバに不正アクセスして、グループポリシーを改ざんすることにより社内のパソコンにランサムウェアを感染させたことも分かった。VPN 接続時の多要素認証を導入し、ネットワークやパソコンを監視するシステムを導入して再発防止を図った。
70	2020/12/18	クラウドに設置していた届出者（企業）のファイルサーバ上のほとんどのファイルに、特徴的な拡張子が付加され暗号化されていたこと、および各フォルダに脅迫のような文章が書かれたテキストファイルが作成されていることを発見した。MARS と呼ばれるランサムウェアに感染したと考えられる状況であったが、感染経路は不明である。バックアップからファイルを復元することで復旧させ、また、サーバへのアクセスのためのパスワードを強化することで再発防止を図った。

2-3. 脆弱性を悪用された不正アクセス

機器やソフトウェアの不具合、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による脆弱性が存在し、それが攻撃者に悪用されて不正アクセスを受けたと思われる事例の届出が 28 件あった。

EC サイトの脆弱性を悪用されたものが 11 件、ウェブシステムや CMS の脆弱性を悪用されたものが 9 件と、以前から被害の届出があったものが依然として多かったことに加えて、今期は VPN 装置の脆弱性を悪用された不正アクセス被害の届出も 3 件あった。

悪用された VPN 装置の脆弱性は 2019 年に公開されたものであり、2020 年上半期の届

出事例においても、2 月に 1 件の同様の不正アクセス届出事例を掲載している。その後、10 か月程の間、同様の不正アクセスの届出はなかったが、12 月になり 3 件、2021 年 1 月に 2 件の届出があった。11 月に脆弱性が残存する機器のリストが公開されたこと[11]を契機に、組織内および外部機関による調査等の対応が進み、不正アクセスが発覚したものと思われる。

脆弱性の存在や不正アクセスに気づいた契機は、次の 2 つのケースが多かった。

- VPN 装置の脆弱性について、前述の脆弱な機器のリストを入手した外部の機関からの連絡
- EC サイトの脆弱性について、クレジットカード番号の流出懸念を確認した金融機関（カード会社や決済代行会社）からの連絡

外部機関が脆弱性を認知している時点で、攻撃者も同様に脆弱性の存在を認知していると考えられ、すでに攻撃が実施されている可能性が高い。自組織の脆弱性対策は、計画的に実施し、外部に認知される前に自組織で対応できるような体制や運用手順を確立することが望ましい。

表 2-4 に脆弱性を悪用された不正アクセスの届出の概要一覧を示す。また、テレワーク対応時に脆弱性対策の不備が生じたことによる不正アクセス被害について、項番 71 の事例の詳細を 4 章で紹介する。

---

11 BLEEPINGCOMPUTER "Hacker posts exploits for over 49,000 vulnerable Fortinet VPNs" （英語）
https://www.bleepingcomputer.com/news/security/hacker-posts-exploits-for-over-49-000-vulnerable-fortinet-vpns/

表 2-4 脆弱性や設定ミス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
VPN 装置の脆弱性悪用の事例		
71	2020/12/7	届出者（企業）の VPN 装置の設定情報がダークウェブに公開されていることが、関連会社からの連絡により発覚した。調査を行ったところ、VPN 装置の脆弱性を悪用された不正アクセスを受け、装置内のファイルが窃取されたものと考えられる状況であった。もともと当該装置はファイアウォール機能のみを利用していたが、テレワーク対応のため当該装置の VPN 機能を有効化した。その際、VPN 機能に関する脆弱性対応ができておらず、脆弱性が残存していた。VPN 装置のバージョンアップにより、VPN 機能の脆弱性を修正する対策を行った。 **※本事例は 4 章で紹介する。**
72	2020/12/11	届出者（教育・研究機関）が使用する VPN 装置の脆弱性が悪用され、従業員のアカウント情報が窃取され、インターネット上に公開された。なお、アカウントのパスワードは窃取されていなかったため、公開もされていない。届出者は、外部の組織からの取材、および別の外部の組織から公開されたアカウント情報に関する連絡を受けて、被害に気づいた。届出者は、年に 2 回程度脆弱性対応を行っていたが、本件の脆弱性情報を認知しておらず、未対応であった。また、保守業者との契約に、脆弱性情報の提供および対応が含まれていたが、保守業者から連絡はなかった。このため、脆弱性が放置された状態となった。届出者は、今後の対策として、保守業者と連携して脆弱性対策を行うとともに、パスワードの定期的な変更を行うとしている。
73	2020/12/25	外部組織からの連絡により、届出者（企業）の VPN 装置の情報と思われるデータが漏洩していることが発覚した。調査したところ、漏洩していたデータは届出者の装置の設定情報やログ情報との一致が見られ、VPN 装置の脆弱性を悪用した不正アクセスにより、当該装置から情報が窃取されたものと推測される状況であった。脆弱性対策がなされた最新版に更新することに加え、定期的に脆弱性対策を行う運用を確立して、再発防止を図った。

項番	届出日	概要
EC サイトの脆弱性悪用の事例		
74	2020/7/2	クレジットカード会社からの連絡で、届出者（企業）が運営する EC サイト利用者のカード情報が漏洩している恐れがあることが発覚した。EC サイトの脆弱性を悪用した不正アクセスにより、ウェブサイトが改ざんされ、カード情報が不正に転送される仕組みになっていた恐れがあるが、原因の詳細は不明であった。EC サイトは閉鎖しており再開は未定である。
75	2020/7/4	クレジットカード会社からの連絡で、届出者（企業）が運営する EC サイト利用者のカード情報が漏洩している恐れがあることが発覚した。調査の結果、EC サイトの脆弱性を悪用されたことが原因と推測している。脆弱性のあったシステムを廃止し、別の決済サービスを利用した新たな EC サイトを構築し移行することで、セキュリティの強化を図った。
76	2020/8/7	クレジットカード会社からの連絡で、届出者（企業）が運営する EC サイト利用者のカード情報が漏洩している恐れがあることが発覚した。調査の結果、EC サイトの脆弱性を悪用され、購買の際に偽の決済画面へ誘導するようなプログラムが仕掛けられていたと推測している。自社運営の EC サイトは閉鎖し、オンラインモールのサービスを利用する形態に移行する予定である。
77	2020/9/6	クレジットカード会社からの連絡で、届出者（企業）が運営する EC サイト利用者のカード情報が漏洩している恐れがあることが発覚した。調査の結果、EC サイトの脆弱性を悪用した不正アクセスによりウェブサイトが改ざんされ、偽の決済画面へ誘導される仕組みが仕込まれていたことが判明した。
78	2020/9/10	届出者（企業）が運営する EC サイトに海外の IP アドレスからの不審なアクセスがあり、データベースに登録されていた EC サイトの購入情報が漏洩した。原因は、社内向けに利用するプログラム実行ファイルが、アクセス制限の設定漏れにより社外からもアクセス出来るようになっていたことによる。対策として、IP アドレスによる当該実行ファイルへのアクセス制限を実施した。

項番	届出日	概要
79	2020/10/2	カード決済代行会社からの連絡により、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等が流出した恐れがあることが発覚した。状況から、以前に運用していた EC サイト（閉鎖済み）において流出したと考えられたため、旧サイトを調査したところ、脆弱性の懸念が見つかり、ログからは不正アクセスと思われる形跡が発見された。EC サイトの脆弱性を悪用した不正アクセスにより、利用者の情報が窃取されたと推測している。自社運営の EC サイトから、オンラインモールのサービスを利用する形態に移行済みであったため、特に EC サイトへのセキュリティ対策は実施していないが、情報流出した可能性のある顧客へ個別に連絡する等の対応を行った。
80	2020/10/5	クレジットカード会社からの連絡により、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等が流出した恐れがあることが発覚した。調査会社による調査を行ったところ、EC サイトの脆弱性を悪用した不正アクセスがあり、偽の決済画面へ誘導してカード情報を詐取するプログラムが埋め込まれていたことが判明した。システムの改修等で対策をすることは困難と判断し、EC サイトはオンラインモールのサービスを利用する形態に移行し、自社運営の EC サイトは閉鎖することとした。
81	2020/10/13	届出者（企業）が運用する EC サイトの利用者に関する情報が流出した可能性があることが発覚した。調査したところ、運用で使用している EC サイトの管理画面の他に、EC サイト構築時のデフォルトの管理画面が、パスワードの設定なしの状態で削除されずに残っていた。このため、デフォルトの管理画面から EC サイトに不正侵入され、EC サイトの利用者情報の漏洩となった。独自に構築した EC サイトから、ASP 形式の EC サイトへの移行を予定している。

項番	届出日	概要
82	2020/10/30	クレジットカード会社からの連絡で、届出者（企業）が運営する EC サイト利用者のカード情報が漏洩している恐れがあることが発覚した。調査したところ、一部のウェブページが外部から書き換えることが可能になっていたことが判明し、攻撃者により改ざんされてしまったことが原因と推測している。セキュリティが強化された別の EC サービスに移行することを検討している。
83	2020/12/21	届出者（企業）の EC サイトに対して、不審なアクセスのログがあることをサイト運用業者が発見した。詳細を調査したところ、不正なプログラムが設置されていたこと、および決済画面が改ざんされていたことが判明し、クレジットカード番号等の情報が窃取された恐れがあることが発覚した。原因は調査中であるが、攻撃者が何らかの方法でサイト管理用の ID とパスワードを入手し、不正アクセスをして改ざんを行ったものと推測している。
84	2020/12/23	クレジットカード会社からの連絡により、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等が流出した恐れがあることが発覚した。調査したところ、EC サイトにバックドアの役割をするプログラムが仕掛けられており、カード支払い用のページが改ざんされていたことが判明した。再発を防止するために、セキュリティ機能を追加した新規環境へ新たに EC サイトを構築することを検討している。
ウェブサイトや CMS の脆弱性悪用の事例		
85	2020/7/17	届出者（教育・研究機関）のウェブシステムのアカウント情報が販売されていることを外部機関が確認した。当該システムへの不正アクセスについて調査を行ったところ、CMS の脆弱性を悪用した攻撃の痕跡が見つかった。更に SQL インジェクション攻撃を防御するための CMS のモジュールの設定に誤りが見つかり、攻撃を防げなかったと推測される状況であった。ログイン画面へのアクセス制限、CMS のモジュールのバージョンアップと設定の是正を行った。

項番	届出日	概要
86	2020/8/18	クラウド上に構築していた届出者（企業）のウェブサイトにアクセスすると、無関係のサイトへ転送され、ウイルスがダウンロードされるように改ざんされていたことが発覚した。管理者がサーバへアクセスするためには秘密鍵を必要とし、パスワードも強固なものを使用する等の対策は実施していたが、使用していた CMS とそのプラグインのバージョンが古かったため、解消されていなかった脆弱性を悪用されて、自動転送のスクリプトを埋め込まれたと推測される状況であった。CMS を最新版にバージョンアップするとともに、サーバインスタンスの入れ替えやアカウントの再発行により再発防止を図った。
87	2020/9/3	届出者（地方自治体）のウェブサイトが改ざんされ、海外のフィッシングサイトに誘導するページが作成されていたことを、監視システムが検知した。調査したところ、使用していた CMS のバージョンが古く、脆弱性を悪用されて WebShell（ウェブサーバを遠隔操作可能とする不正ツール）を仕掛けられ、それを用いて改ざんされたと推測される状況であった。対策として、CMS を含めた使用ソフトウェアを最新版にバージョンアップし、管理者画面に接続可能な IP アドレスの制限やパスワードの変更を実施した。
88	2020/9/4	届出者（企業）のウェブサーバにおいて、セキュリティソフトがウイルスを検知したため、ウェブサイトを閉鎖した。レンタルサーバ会社と調査を行ったところ、CMS の脆弱性を悪用されて WebShell が仕掛けられていたことが分かった。CMS の自動更新機能は有効化していたが、対策版の公開から更新処理までにタイムラグが生じたため、脆弱性を悪用されたと推測している。外部からの脆弱性検査を併用し、脆弱性情報を確認して適宜対策を行うような運用に変更した。

項番	届出日	概要
89	2020/9/23	届出者（非営利団体）が、外部業者による自組織のシステムへのセキュリティ診断を実施していた際、ログ調査により、ウェブサイトに不正なアクセスがあり、データベースから情報漏洩が発生していた恐れが指摘された。ウェブサイトの一時閉鎖とデータベースの退避を行った上で、対象範囲を広げて詳細に調査を行ったところ、ウェブサイトに脆弱性が見つかり、それを悪用されたデータベースの不正アクセスによる情報窃取であることが判明した。再発防止策として、不正アクセスを検知、遮断する仕組みを導入するとともに、定期的に脆弱性検査とログ解析を実施することとした。
90	2020/10/2	届出者（企業）のウェブサイトの一部が改ざんされ、不審な文面と URL が追加されていたことを発見した。調査したところ、海外から、コンテンツ管理画面への不正なアクセスがあったことが判明し、その際に改ざんされたものと考えられた。管理画面の URL やログイン ID とパスワードが漏洩した原因は不明である。再発防止策として、外部からの管理画面へのアクセスを遮断する設定を行った。
91	2020/11/3	届出者（企業）が、自社のウェブサイトへアクセスすると無関係なウェブサイトへ転送されることに気づいた。調査したところ、ウェブサーバ上に覚えのない不審な PHP ファイルが置かれていたことが判明し、そのファイルはセキュリティソフトでバックドアとして判定された。詳細な原因は不明だが、使用していた CMS のバージョンが最新ではなかったことから、CMS の脆弱性を悪用した不正アクセスにより、遠隔操作のためのファイルが仕掛けられ、ウェブページを改ざんされたと推測される状況であった。パスワードの変更と CMS の最新版へのバージョンアップにより対策した。

項番	届出日	概要
92	2020/12/16	クラウド運営会社から、届出者（企業）がクラウド上に設置していたウェブサイトに不正アクセスがあったとの連絡があった。調査を行ったところ、ログからサーバ内の情報の一部が窃取されたことが判明した。詳細は調査中であり原因は不明だが、ウェブサイトの脆弱性を悪用されてクラウドへのアクセスキーが窃取され、サーバへ不正アクセスされたものと推測される状況であった。所有するウェブサイトのすべてに脆弱性検査を行い、更にウェブサイトのページ更新の際に脆弱性検査を行う仕組みを導入することで対策を実施した。
93	2020/12/18	届出者（一般団体）が運営するウェブサイトが閲覧できなったことに保守業者が気づき、調査を行った。使用していた CMS のプラグインに存在していた脆弱性が悪用され、コンテンツの一部が削除されたり、不審なファイルを設置されたりしていたことが判明した。脆弱性診断や監視システムを導入したウェブシステムを新規に構築することで対策と再発防止を図った。
その他の脆弱性悪用の事例		
94	2020/9/11	届出者（企業）のシステム運用の委託先会社が不正アクセスを示すログを発見し、専門業者とともに調査を行った。調査の結果、脆弱性のあったサーバを踏み台にした不正なアクセスを受け、顧客データベースの一部の情報を盗み見られた可能性が高いことが判明したが、具体的な侵入の手口については不明であった。脆弱性のあったサーバへのアクセスを遮断し、修正プログラムによる脆弱性対策を実施した。また、脆弱性情報を収集して対策する体制を整えるとともに、定期的にペネトレーションテストを実施する運用により、再発防止を図ることとした。
95	2020/9/14	届出者（地方自治体）が運営を委託しているウェブサイトの問合せ用メールアドレスに、大量の送信エラーを通知するメールが着信していることを発見した。調査により、ウェブサーバ上のメール送信機能を悪用され、ばらまき型メールの送信に悪用されたと考えられる状況であった。原因の詳細は不明。メール送信機能に関わるパスワードを変更することで対策を行った。

項番	届出日	概要
96	2020/10/13	届出者（医療法人）のウェブサイトが改ざんされ、閲覧ができなくなったり、届出者とは無関係のコンテンツが表示されるようになったりしたことを発見した。ウェブサイトの運用業者が調査したところ、ウェブサーバの FTP サービスに接続元のアドレス制限を設けていなかったことから、海外より不正なファイルがアップロードされていたことが判明した。攻撃者が何らかの手段でウェブサーバへのアクセス情報を入手し、改ざんを行ったものと推測している。接続可能な IP アドレスを制限することや WAF の定義ファイルを更新することで、再発防止を図った。
97	2020/10/13	届出者（教育・研究機関）が管理する公開サーバから、フィッシングメールが送信されていることを確認した。原因を調査したところ、当該サーバ上で SMTP 中継の機能が動作しており、安易なパスワードを設定していたアカウントが存在していた。これにより SMTP の認証を突破されてしまい、フィッシングメール送信の踏み台として悪用された。
98	2020/10/15	届出者（地方自治体）が運用するメールサーバに不正アクセスがあり、迷惑メール送信の中継に悪用されていたことがプロバイダからの連絡により発覚した。原因は調査中だが、送信元を制限する設定に不備があったため、オープンリレーの状態になっており、外部からのメール中継の踏み台にされたものと推測している。
99	2020/11/9	届出者（教育・研究機関）の職員のメールボックスに、宛先不明を伝えるメールが大量に着信していることに気づいた。調査を行ったところ、メールシステムの設定に誤りがあり、外部からのメールをリレーする設定になっていた。この設定が悪用され、当該職員のメールアドレスを差出人とした詐称メールのばらまきが行われたことが判明した。メールのリレーを許可する IP アドレスを組織内の IP アドレスのみに制限することで対策した。

項番	届出日	概要
100	2020/12/15	届出者（企業）が提供するサービスのアプリケーション開発委託先業者が不正アクセスを受け、顧客に関するデータが流出した恐れがあることが発覚した。調査により、外部からの不要なアクセスを遮断するためのファイアウォールの設定に誤りがあったことが判明し、攻撃者から不正アクセスを受けたものと推測される状況であった。ファイアウォールの設定を是正し、更に構成変更の検討や監視機能の追加等でセキュリティの向上を図り再発防止に努めることとしている。
101	2020/12/23	届出者（企業）が保持する顧客データが海外のウェブサイトに公開されている可能性があるとの連絡を外部組織から受けた。調査したところ、届出者が管理するウェブサイトに対して、何者かが URL に admin という文字列が含まれるページを探索し、該当する URL に SQL インジェクション攻撃を行ったことが判明した。これにより、管理者画面にアクセスされ、顧客データが不正に引き出されたことが分かった。不正アクセスへの対策として、ウェブサイト上で顧客データを保存しないようにし、また不正侵入検知やウェブ改ざん検知の仕組みを導入した。
102	2020/12/28	届出者（企業）の顧客から、迷惑メールが届いたという問い合わせを受けた。調査したところ、届出者（企業）のシステムの脆弱性が悪用されて不正アクセスを受け、システムに登録されていた顧客のメールアドレス情報が流出したことが判明した。脆弱性の修正対応、WAF の導入、監視体制の強化、外部機関によるウェブサイト診断等を行う対策を行った。

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

ID とパスワードによる認証を行っているシステムで、利用者やシステム管理者による運用・管理の問題によって不正アクセス被害に繋がったと思われる事例を挙げる。

（1） 大量ログイン試行による不正アクセス

企業等が提供する会員向けサービスのログインページへ大量のログイン試行を行う攻撃に関する届出は、比較的少なかった 2020 年上半期の 3 件に対して、今期は 12 件と大幅に増加した。届出の大半は、総当たり方式でログインの試行を繰り返すブルートフォース攻

撃ではなく、何らかの方法で攻撃者が入手した ID とパスワードの組合せを用いた、パスワードリスト攻撃が行われたと届出者が判断したものであった。

届出者がパスワードリスト攻撃と判断した理由は主に 2 つあり、1 つは相当数の実在するユーザ ID が不正ログインの試行に使用されていたこと、もう 1 つは少数の試行でログインに成功されてしまった等、ログイン試行数に対するログイン成功率が高かったことである。すなわち、何らかの原因で他サービスから流出した ID とパスワードのリストが攻撃者の手に渡り、届出者が提供するサービスへの攻撃に悪用されたものと考えられる。サービスの利用者が、同じ ID とパスワードの組合せを複数のサービスで流用（使いまわし）をしていた場合、不正なログインが成功してしまう。

（2）　その他アカウント管理不備による不正アクセス

その他、ID やパスワードの管理不備が原因であると分類した届出は 10 件あった。ログインアカウントを作成後、退職等の理由によりアカウント使用者が不在となった後も、使われていないアカウントが簡易なパスワードのまま残っていたケースや、複数人で共用するアカウントについて、複雑なパスワードを設定していなかったケース等、パスワードだけでなくアカウントそのものの管理方法にも問題があったと思えるものが見受けられた。

ID とパスワードによる認証方式を突破される不正アクセスは、最も古くからある問題の一つだが、現在でも継続して発生していることがうかがえる。ログインの失敗が一定回数以上発生した場合や、同一の接続元から複数の ID でログインが試行された場合等に警告を発するような監視システムを導入して、攻撃を迅速に検知し対処できた事例もある。この方法は、正しい ID とパスワードの組合せが使われた攻撃に対する効果は低いため、パスワードのみに頼らない、多要素認証方式の積極的な導入や利用について、サービス提供者側と利用者側の双方で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。

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に関する届出の概要一覧

項番	届出日	概要
大量ログイン試行による不正アクセスの事例		
103	2020/8/5	届出者（企業）が提供する EC サイトや会員向けサービスサイトにおいて、利用者から身に覚えのないログイン通知が来たとの問い合わせが急増した。調査したところ、海外から多数のログイン試行があり、一部は不正なログインに成功し、会員情報を閲覧されていたことが判明した。パスワードリスト攻撃を受けたものと推測している。接続元 IP アドレスの制限とボット対策ツールの導入、WAF の設定強化等の対策を実施した。
104	2020/8/17	届出者（企業）の会員向けサービスサイトに対して大量のアクセスがあったことを監視システムが検知した。アクセスログを調査したところ、同一の接続元 IP アドレスから複数の ID でのログイン試行が行われ、一部はログインに成功していたことが判明した。攻撃者が何らかの手段で不正に入手した ID とパスワードによる、パスワードリスト攻撃を受けたと推測される状況であった。また、この不正アクセスにより、会員情報の閲覧やメールアドレスの変更が行われたことも判明した。対策として、ログイン時の二段階認証を導入した。
105	2020/8/26	届出者（企業）の会員向けサービスサイトに対して不正なログインがあり、会員のポイントが不正に交換されていたことが会員からの問い合わせにより発覚した。調査したところ、同一の接続元IP アドレスから複数のアカウントへのログイン試行が確認されたことから、パスワードリスト攻撃が行われたものと判断した。二要素認証の導入やパスワード有効期限の短縮によりセキュリティの向上を図り、同一接続元からの大量アクセスを検知し遮断する機能を導入して対策を行った。

項番	届出日	概要
106	2020/8/28	届出者（企業）が提供する会員ポイントサービスにおいて、利用者から身に覚えのないポイント交換が行われたようだとの連絡があり、アクセスログを調査した。その結果、不正なログインが行われたことが判明したため、ポイント交換の処理を停止した。状況からブルートフォース（総当たり）攻撃の一種であるパスワードスプレー攻撃が行われたものと推測している。パスワードポリシーを変更し、長くて複雑なパスワードを必須とすることでセキュリティの強化を図った。
107	2020/9/11	届出者（企業）が運営するサービスの利用者から不正利用の疑いに関する報告が複数あり、調査を行った。同一の接続元から複数の ID でのログイン試行があったり、同一 ID でのログイン失敗数が少なかったりしたことから、他サービス等で利用されていた ID やパスワードを用いたパスワードリスト攻撃を受けたと推測される状況であった。同一接続元から複数 ID によるログインを制限する機能や reCAPTCHA のようなボット対策機能を追加する等の対策により、再発防止を図った。
108	2020/9/14	届出者（企業）が提供するサービスにおいて、大量の認証試行が行われていることを監視システムが検知した。攻撃に使用された ID とパスワードは実際に利用されている組み合わせが多く、パスワードリスト攻撃が行われたものと推測された。しかし、認証の手順が正式な認証処理のものと一部異なっていたため、不正なログインの成功はなかった。攻撃者の目的は不正なログインではなく、入手したパスワードリストの精度の検証であった可能性がある。一部のユーザに対して、パスワードの強制リセットと再設定依頼を行うとともに、当該サービスに二段階認証を導入してセキュリティ向上を図った。

項番	届出日	概要
109	2020/9/29	届出者（企業）が運営するサービスの会員向けウェブサイトに対して、海外からの攻撃と思われる通信があったことを監視システムが検知した。海外からのアクセスを遮断した上で詳細な調査したところ、状況から他サービス等で利用されていた ID やパスワードを用いたパスワードリスト攻撃が行われ、一部は不正なログインに成功し、会員情報が窃取された恐れがある状況であった。不正にログインされたユーザのパスワードを強制変更して再発防止を図った。
110	2020/10/2	届出者（企業）が提供するサービスにおいて、利用者から、身に覚えのないアカウントロックが発生しているとの問い合わせがあった。調査したところ、平時の 30 倍ほどの大量のログイン試行が行われていたことが判明した。不正なログインの成功率の高さから、攻撃者が何らかの手段で入手した ID とパスワードを用いた、パスワードリスト攻撃を受けたものと推測している。なお、金銭が関わる処理にはログイン時とは別のパスワードが必要であったため、金銭的な被害はなかった。接続元の IP アドレスの制限や、別のパスワード入力が必須となる範囲の拡大等の対策を行った。
111	2020/10/16	届出者（企業）が提供する会員ポイントサービスの利用者から、身に覚えのないポイント交換を通知するメールが届いたとの連絡があった。調査したところ、海外から不正なアクセスがあり、ポイント交換がされていたことが判明した。不正なログインの成功率の高さから、攻撃者が何らかの手段で入手した ID とパスワードによる、パスワードリスト攻撃を受けたと推測される状況であった。ポイント交換サービスを一時停止し、一部の海外からのアクセスを遮断する等の対策を実施した。

項番	届出日	概要
112	2020/12/4	届出者（企業）の会員向けサービスに対して大量のログイン試行が行われていることを社内の技術者が発見した。調査したところ、一部の会員 ID については不正にログインされ、有料コンテンツの購入や、登録されている個人情報が閲覧されたことも判明した。状況から、攻撃者が別のサービス等から何らかの手段で入手した ID とパスワードによる、パスワードリスト攻撃を受けたと推測される。パスワードを強制リセットし、ログイン時に通知のメールを送る機能を追加する等の対策を行った。
113	2020/12/10	届出者（企業）が運営するサービスの利用者から、不正利用に関する連絡を受けた。調査したところ、当該サービスを利用するためのウェブサイトに不正にログインされていたことが発覚した。更に調査を進めたところ、パスワードリスト攻撃によって複数の利用者が不正にログインされ、個人情報が漏洩した可能性があることが発覚した。本件に対する対策として、サービスの一時停止を行い、不正なログイン試行に対するアクセス検知の仕組みや監視体制の検討を行っている。
114	2020/12/24	届出者（企業）が提供する会員サービスに対して、大量のログイン試行があり、そのうちの一部のアカウントで不正なログインに成功していることを発見した。ログを調査した結果、存在しない ID でのログイン試行が大多数を占めていたことや、短時間での試行回数が異常に多かったこと等から、他のサービスやシステムで漏洩した ID とパスワードを悪用したパスワードリスト攻撃が行われたと推測される。なお、届出者のシステムでは、多要素認証等のセキュリティ強化機能を有していたが、利用者側で任意に利用を選択できる仕様であり、被害を受けたアカウントは多要素認証を利用していなかった。対策として、被害を受けたアカウントのパスワードのリセットをするとともに、利用者に多要素認証の推奨とパスワードの使い回しへの注意喚起等を行った。
その他アカウント管理不備による不正アクセスの事例		

項番	届出日	概要
115	2020/7/3	届出者（教育・研究機関）が利用するメールサービスにおいて、大量の送信エラーを通知するメールが着信していることを発見した。調査したところ、未使用の状態にあったメールアカウントが不正アクセスされ、大量の迷惑メールの送信が行われた結果、宛先不明等でメールがエラーで戻ってきていたことが判明した。当該アカウントのパスワードは初期設定の簡易なパスワードから変更されていなかった。パスワード管理の厳格化を組織内に周知し、未使用アカウントを残さない等アカウント管理の厳正化の再徹底も行った。
116	2020/7/9	届出者（企業）が利用するクラウド型メールサービスのアカウントから、不審メールが送信されていたことを発見した。調査したところ、複数人で共用していたアカウントに対して不正なログインがあり、そのアカウントのアドレス帳に保管されていたメールアドレス宛にフィッシングメールが送信されていたことが判明した。個人用のアカウントに対しては多要素認証を導入していたが、共用アカウントには適用しておらず、またパスワードが平易なものになっていた可能性もあったことから、このことが原因であると推測している。共用アカウントを廃止し、全アカウントで多要素認証を必須とする対策を行った。
117	2020/7/21	届出者（企業）が提供する会員制サービスサイトのユーザ情報がダークウェブで販売されているとの情報提供があった。情報が流出した原因は不明であるが、何らかの理由でクラウドサービスにログインするための ID とパスワード、アクセスキーが窃取され、それを悪用して不正アクセスされた可能性が高いと推測される状況であった。パスワードを変更して対策するとともに、多要素認証の必須化や、ログインや設定変更時にアラートを発生させる監視の仕組みを導入して再発防止を図った。

項番	届出日	概要
118	2020/8/25	利用しているプロバイダからの連絡により、届出者（企業）のメールアカウントの 1 つが大量の迷惑メールの配信に悪用されていたことが発覚した。プロバイダによる、メールアカウントのパスワードの強制変更により、迷惑メールの配信が停止したことから、届出者のアカウント情報が漏洩し悪用されたものと思われる。パスワードポリシーを強化し、従業員に周知することで再発防止を図った。
119	2020/9/15	届出者（業界団体）の職員 1 名のメールが利用できなくなった。メールアカウントのパスワードをリセットして再度ログインしたところ、大量の送信エラーを通知するメールが着信していることを発見した。状況から、何者かにメールアカウントのパスワード認証が突破された後、パスワードが変更され、迷惑メールの送信に悪用されたものと考えられる。メールシステムへのログインを許可する接続元IP アドレスを限定することで再発防止を図った。
120	2020/9/29	届出者（企業）が利用するクラウド型メールサービスから大量の迷惑メールが送信されていることを発見した。調査したところ、従業員のアカウントに不正にログインされ、メールが不正に送信されていた。当該従業員は、以前フィッシングサイトに誘導され、アカウント情報（ID およびパスワード）を入力してしまったことがあり、そうして詐取された情報が悪用されたと推測される。多要素認証の導入により再発防止を図った。
121	2020/10/28	届出者（企業）のウェブサイトが改ざんされていることに気づき、サイトを一時閉鎖して調査を行った。その結果、ウェブサイト管理用の CMS のアカウントを変更した際に、古い管理者用アカウントの削除ができておらず、パスワードの更新もされないまま残存していた。このため、何らかの方法で当該アカウントの ID とパスワードを入手した攻撃者により不正アクセスを受け、改ざんが行われたことが判明した。古い管理者用アカウントを削除するとともに、他のアカウントのパスワード変更も実施した。更に管理画面へのアクセス制限と不正アクセス対策のプラグインの導入も実施予定である。

項番	届出日	概要
122	2020/11/16	届出者（教育・研究機関）が利用するサーバに不正にログインされたことを発見した。調査したところ、攻撃者は何らかの手段で入手したアカウント情報を用いてサーバへ不正にログインした後、組織内部のウェブサーバに構築した CMS への不正なログインおよび脆弱性を悪用したファイルアップロード等を行い、組織の関連人物の個人情報や関連組織の組織情報等を窃取した可能性があることが判明した。本事案の対策として、悪用されたアカウントのパスワード変更、代替サービスの検討、脆弱性の修正を実施した。また、CSIRT を設置し、インシデント発生時の対応体制を整えた。
123	2020/11/24	届出者（一般団体）が使用するメーリングリストのシステムを悪用した不審なメールが配信された。調査すると、メーリングリストシステムの管理画面が外部からアクセス可能になっており、攻撃者が何らかの手段で窃取した ID とパスワードにより不正にアクセスされ、迷惑メールの送信に悪用されたと考えられる。パスワードをより複雑なものに変更し、ログイン状況の監視ができるサーバに移行することで再発防止を図った。
124	2020/11/25	届出者（企業）が提供する会員向けの金融サービスから、不正に作成された銀行口座へ資金移動の処理が行われたことが、金融機関からの連絡により発覚した。何者かが何らかの手段で入手した会員のログイン ID とパスワードを悪用して不正にログインし、出金先となる金融機関と口座番号を変更した上で、当該口座へ出金の処理を行い、不正に金銭を窃取したと考えられる。出金に関わる手続きには二段階認証を必須とすることで再発を防止する策とした。

2-5. クラウド環境への不正アクセス

メールクライアントやファイルサーバ等、複数のサービスをシングルサインオンで統合的に提供するクラウドサービスを利用するなど、一般業務のクラウド化の普及が進んでいる。近年ではシステムの開発環境やテスト環境をクラウド上に構築することも一般的になってきている。それに伴って、クラウド上の開発環境等からのアクセス情報流出に起因すると思われる不正アクセス被害の届出も増えてきている。

（1）　クラウド上の開発環境への不正アクセス

システムの開発に必要なため、本番システムへのアクセス情報等をクラウド上の開発環境に保持していたところ、その情報が何らかの原因で漏洩し、本番システムのデータベースに不正アクセスされた事例があった。また、クラウドサービスのアクセスキーが窃取され、その権限で、攻撃者によりデータ窃取用の踏み台サーバをクラウド上に構築されてしまった事例もあった。

ID やパスワード、アクセスキー等のアクセス情報が漏洩しないよう厳密に管理することはもちろんのこと、クラウドサービスのガイドライン等を参照して、開発に適したバーチャルネットワークの設計や、適切なアクセス制限等の設定を確実に行うことが重要であると考える。

（2）　クラウドサービスへの不正アクセス

依然としてクラウド型のメールサービスへの不正アクセスも発生しており、今期も複数の届出があった。メールだけでなく他のサービスと統合的に提供されていることが多いため、ひとたび不正なログインを許してしまうと、メールを盗み見されたり、迷惑メールの送信に悪用されたりといったメールに関わる被害だけでなく、例えばファイルサーバからファイルを窃取されたり、ウェブシステムに不正なファイルを設置されたりする等、シングルサインオンで利用可能な他のサービスに関する被害も発生する可能性が高い。従って、パスワード認証方式だけによらない多要素認証の導入等により不正なログインをさせないことが重要な防御の一つとなる。もちろん、多要素認証も万全ではないが、セキュリティ対策は多層に重ねていくことで効果を発揮していくものであり、それに伴って不正アクセスのリスクも、ゼロにはできずとも大幅に減らすことが可能である。利用者の利便性とのバランスを考慮しながら、可能な限りの施策を追加していくことが望ましい。

表 2-6 にクラウド環境への不正アクセスの届出の概要一覧を示す。また、クラウド上の開発環境から認証情報を窃取されて不正アクセスされた被害について、項番 131 の事例の詳細を 5 章で紹介する。

表 2-6 クラウド環境への不正アクセスに関する届出の概要一覧

項番	届出日	概要
125	2020/7/15	届出者（企業）が提供する会員制サービスのサーバが停止し、調査したところ、不正アクセスされたと思われる形跡が見つかった。更に調査したところ、会員 ID、暗号化（ハッシュ化を指していると思われる）されたパスワード文字列、および一部個人情報が含まれるテキストデータが第三者に閲覧された可能性があることが発覚した。開発担当者に届いたフィッシングメールにより、クラウド上の開発環境の認証情報が詐取された。そして、開発環境に保存されていたクラウドサービスへのアクセストークンが窃取されたことが不正アクセスの原因と思われた。多要素認証を導入する等、複数の対策を行った。
126	2020/8/20	届出者（企業）が、顧客向けにクラウド上に構築して運用保守しているシステムにおいて、意図しないデータベースの操作が行われていることに気づいた。調査を行ったところ、クラウドサービスへのアクセスキーを窃取されたことにより、外部から不正アクセスが行われたことが判明した。管理者権限を悪用されたため、データベースに格納された個人情報を含むデータを盗み見され、流出した可能性がある。アクセスキーを窃取された原因は不明であるため、クラウドサービスに関わるアクセスキーを交換することで本件への対策、および今後の再発防止策とした。
127	2020/9/3	届出者（企業）が利用するクラウド型メールサービスのアカウントに不正ログインされ、大量の迷惑メールが送信されたことを発見した。原因は開発に利用していたクラウド上の開発環境が公開状態になっており、そこに保存していたアカウント情報が窃取され、メールサービスへのログインが行われていたことであった。窃取されたアカウントを削除し、開発環境の公開設定の見直しを行った。

項番	届出日	概要
128	2020/10/13	届出者（企業）が運営する、クラウド上に設置したウェブアプリケーションサービスが停止していることを発見した。調査したところ、クラウドサービスの管理者用のアクセスキーが流出しており、クラウド上のデータベースに外部からアクセスが可能になるように改ざんされ、データベースのパスワードが変更されていたことが判明した。管理者用のアクセスキーの停止およびクラウドサービス上のすべてのアカウント管理徹底を行い、またログを迅速に確認できるような環境を整えた。
129	2020/11/19	届出者（企業）が利用する、クラウド型の統合サービスに不正アクセスがあったことを監視システムが検知した。調査したところ、詳細な原因は不明であるがディレクトリサーバの認証を突破されて、クラウド上のファイルサーバのサービスから不正にファイルをダウンロードされていたことが判明した。詳細調査および再発防止に向けた取り組みは実施・検討中である。
130	2020/12/11	外部からの連絡により、届出者（企業）が運営する会員向けサービスサイトに対して不正アクセスがあり、個人情報を窃取された可能性が発覚した。調査したところ、クラウドサービスへアクセスするためのアクセスキーが何らかの方法によって不正に入手され、クラウド上に保管していた個人情報が流出していることが判明した。対策として、アクセスキーの変更や不正検知の仕組みの導入を実施した。
131	2020/12/21	届出者（企業）が、クラウド環境に構築したデータベース上の情報が流出している恐れがあるとの報告を外部から受けた。調査したところ、クラウド上で管理していたソースコードが窃取され、その中に含まれていたデータベースサーバへのアクセスのための認証情報を悪用されて、情報が窃取されたことが判明した。パスワードやアクセスキーを変更して対策するとともに、プログラムの改良を行い、ソースコードに認証情報を含まない方式に変更することで再発防止を図った。 **※本事例は５章で紹介する。**

2-6. その他

その他、ここまでの分類に該当しない届出事例を表 2-7 に示す。

表 2-7 その他の届出事例の概要一覧

項番	届出日	概要
132	2020/11/26	決済代行会社からの連絡で、届出者（企業）が運営する EC サイトからのクレジットカード与信照会の回数が急増しているとの連絡があった。調査したところ、複数の接続元 IP アドレスから、クレジット与信を繰り返し行う攻撃（クレジットカードの有効性確認と思われる）が行われていると推測された。当該接続元からの通信を遮断する対策を行った。
133	2020/12/9	届出者（企業）が利用する監視サービスの監視装置に不正アクセスがあった。監視装置は届出者のネットワーク内にあり、インターネット接続はなかったが、監視サービスの管理用ネットワークと繋がっていた。この管理用ネットワークはインターネット接続があり、この管理用のネットワークを経由して、届出者の監視装置が不正アクセスを受けた。なお、監視装置から届出者の監視対象サーバへの不正アクセスやウイルス感染は確認されなかった。届出者は、監視対象サーバの監視方法を変更し、当該監視サービスの利用を停止した。
134	2020/12/23	届出者（企業）のウェブサイトにアクセスすると、不審な広告が表示されることを発見した。調査したところ、過去に届出者が利用していた外部のウェブサイト分析サービス「Dot Metrix」のウェブサイトから、ブラウザ内に広告を表示するような不正なコンテンツがダウンロードされるようになっていたことが判明した。当該サービスはすでに終了していたが、届出者のウェブページには分析サービスを使用するための HTML コードが残っていた。悪意のある者が当該サービスのドメインを取得し、不正なコンテンツを配布する手段として悪用していたと考えられる状況であった。同様の事例が公開情報上で複数確認されている。

項番	届出日	概要
135	2020/12/25	届出者（企業）の多数のメールアカウントに、届出者組織内のメールアドレスを差出人に装った不審なメールが着信した。海外のストレージサービスから、ファイル共有のための URL を通知するメールであった。URL にアクセスすると PDF 文書ファイルがダウンロードでき、その内容にはフィッシングサイトと思われる URL へのリンクが書かれていた。正規のストレージサービスとその通知機能を組み合わせて悪用したフィッシング攻撃だと思われる。受信者および差出人として偽装されたメールアドレスの流出経路は不明である。

3. 事例：ランサムウェアによる攻撃

3-1. 届出内容

（1）　発見経緯

届出者の社内システムにアクセスできない現象が確認されたため、調査を行ったところ、社内の多数のパソコンやサーバのデータが暗号化されていることを発見した。

（2）　被害内容

詳細な調査をした結果、350 台以上のサーバやパソコンがランサムウェアに感染したとみられ、次の被害が判明した。

- ファイルが暗号化された。
- パソコンに導入していたセキュリティソフトが無効化され、ランサムウェアの検知や駆除ができないようにされていた。
- 一部のサーバについては、暗号化したファイルの復旧のための取引を求める脅迫文のような文章が残されていた。

（3）　被害原因

取引先を装った、ウイルスが添付されたメールが着信し、メールを受信した従業員が添付ファイルを開いたことで、パソコンが遠隔操作ウイルスに感染した。攻撃者はこのパソコンを足掛かりに、他のパソコン等の組織内ネットワークへ侵入を拡大、さらにドメインコントローラやセキュリティソフトのサーバといった管理サーバをも乗っ取り、これらのサーバの機能を悪用して多数の機器へ攻撃を行った。

（4）　被害対応

ファイルが暗号化された機器については、バックアップしていたデータをリストアすることで復旧させた。また再発防止のために、次の施策を実施した。

- セキュリティソフトを高機能なものにバージョンアップし、各パソコンの挙動を監視する機能を追加した。
- 通信を監視し、不審なデータの流れを検知する機器を新たに設置した。

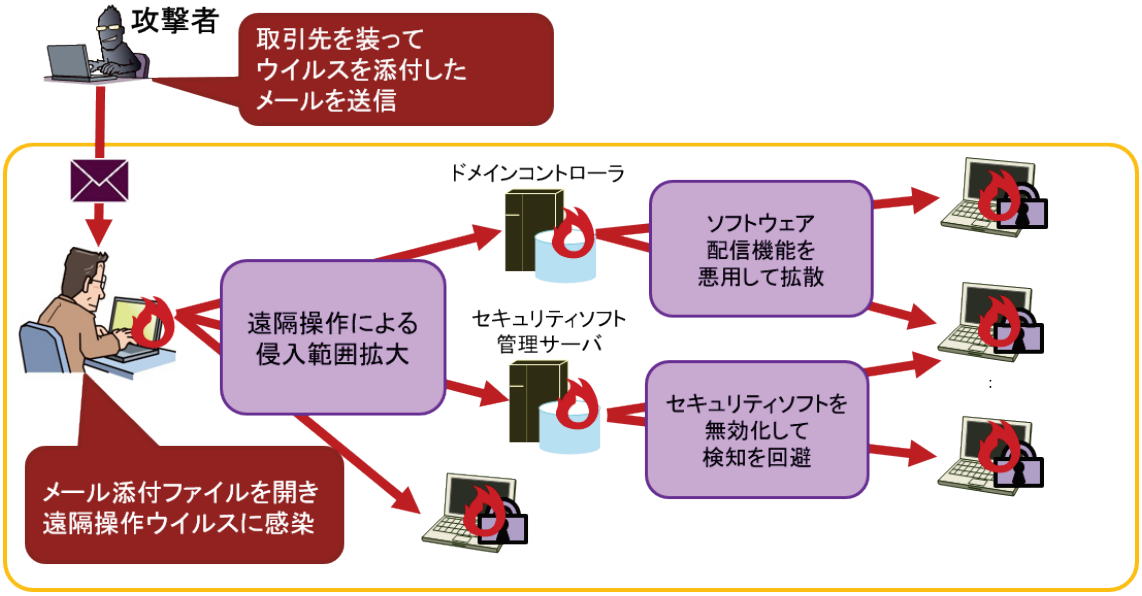

図 3-1 本事例におけるランサムウェアの攻撃の流れ

3-2. 着目点

（1） 管理サーバの乗っ取りによる被害拡大

本事例は、被害にあったパソコンやサーバが 350 台以上と、大規模なランサムウェア感染被害であった。被害が拡がった主な要因は、攻撃者が社内システムの管理サーバを乗っ取り、それらサーバの管理機能を悪用することで、管理下の多数のパソコン等へ一斉にランサムウェアを感染させたことである。

ドメインコントローラには、管理下のパソコン等の設定を変更したり、アプリケーションを配布してインストールしたりする機能を持たせることができる。また、セキュリティソフトの管理サーバにも、管理下のパソコン等のセキュリティソフトの設定を変更したり、一部機能を無効化したりする機能がある。これらは、組織内の多数のパソコン等を統合的に管理し、一斉に修正プログラムを適用する等、システム管理者にとって非常に有用な機能である。一方、これらのサーバを攻撃者が操作できるようになってしまうと、セキュリティソフトを無効化した上で一斉にウイルスを配布する等、攻撃者にとっても有用な機能となる。

対策としては、やはり管理サーバを一層厳重に防御することが重要となる。管理サーバの乗っ取りを許してしまったということは、管理サーバ自体や関係システムの運用方法において何らかの脆弱な点があったと考えられる。例えば本事例では、一般職員が使用するパソコンから管理サーバへのリモートログインが可能であったといった可能性がある。管理サーバが乗っ取られた場合の組織内全体に及ぼす影響の度合いを踏まえ、管理サーバへは専用の管理端末からのみアクセス可能としたり、管理サーバ上でのログオンやユーザの

挙動を監視したりする等、より厳重なセキュリティを検討していただきたい。

（2）　メール添付ファイルからの感染

今期のランサムウェア攻撃に関する届出では、侵入経路は不明であったものが多かったが、本事例では、差出人を取引先に装ったメールが着信し、添付ファイルを開いたことが原因であろうと推測できるものであった。

数々の高度な攻撃手口を駆使して侵入範囲を拡大していったと思われる攻撃者だが、侵入の契機になったのは、以前から多く見られる手口であった。完全な防御は難しいが、基本的な対策を徹底していれば、初期段階で防御できた可能性もある。

改めて、メールの差出人は簡単に偽装ができること、あるいはメール送信者が正しくてもアカウントの乗っ取り等が行われている恐れもあること等を意識し、特に添付ファイルを開くときには、メールが信用できるものかを十分に検討し、不審な点が見受けられた場合はメール以外の方法で送信者に確認する等の対応も重要である。

4. 事例：テレワーク対応時の脆弱性対策の不備で不正アクセスされた事例

4-1. 届出内容

（1）　発見経緯

社内の調査により、自社の VPN 装置の設定情報がダークウェブに掲載されていることに気づいた。

（2）　被害内容

従業員のテレワークを可能とするために設置していた VPN 装置から、装置内のファイルが窃取され、その情報がダークウェブに公開された。公開された設定ファイルやログファイルに、当該装置の IP アドレスや認証 ID として使用していたメールアドレスが含まれていたため、情報が漏洩となった。なお、パスワードは暗号化されていたことと、VPN の接続には二要素認証を導入していたことにより、不正に社内ネットワークへ侵入された被害はなかった。

（3）　被害原因

当該 VPN 装置に、外部から装置内のファイルが読み取り可能になる脆弱性が存在していたため、攻撃者が外部から不正にファイルを取得したと考えられる。当該装置は、当初ファイアウォールとして導入したものであり、ファイアウォール機能に関する脆弱性対策は実施してきたが、従業員のテレワークのために VPN 機能を有効にした際に、この脆弱性を悪用した攻撃が可能となってしまっていた。

（4）　被害対応

- VPN 装置のファームウェアバージョンアップによる脆弱性対策
- 既存機器で新機能を導入する際の、新規機器導入時と同様の脆弱性診断の実施

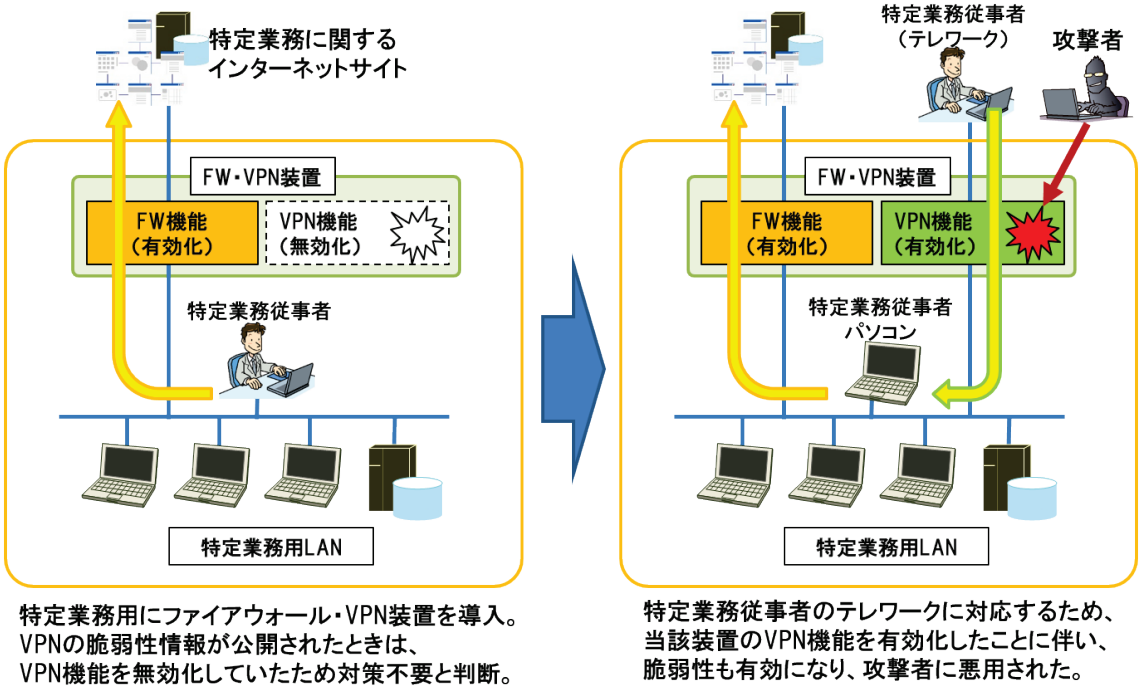

図 4-1 本事例の概要

4-2. 着目点

（1） 1 年以上前に公開された VPN 装置の脆弱性の存在

本事例は、脆弱性が残存していた VPN 装置に不正アクセスがあり、機器の設定ファイルやログファイルが窃取されてしまい、機器の IP アドレスを含む機器の設定情報がダークウェブに公開されたものだった。

VPN 装置については、複数の機器製造元から、各社の機器の脆弱性情報が公開されている。今期の届出事例においては、悪用されたと考えられる脆弱性はいずれも 2019 年に公開されたものであった。本事例も同様で、2019 年の脆弱性の公開から、届出者が認知し対策するまでに 1 年以上を要しており、その間、脆弱な状態が継続していたことになる。なお、本事例は該当しないが、2020 年 11 月に脆弱性のある機器のリストが公開されたことを受け、セキュリティ関連機関等が連絡可能な対象組織に情報提供の連絡を行っており、その連絡を受けて初めて脆弱性の存在を認知したという事例もあった。

VPN は、インターネット等外部のネットワークから組織内のネットワークに安全に接続する一般的な技術であり、従来から利用されていたが、昨年、従業員のテレワーク対応のために新規に導入した組織も多いと考えられる。2019 年に公開された脆弱性が、1 年以上の期間を経ても未対策のまま放置されていた機器が多数あったことを考えると、現在でも多数の未対策の VPN 装置が存在する可能性が懸念される。VPN 装置はその役割の性質上、外部のネットワークからアクセス可能な位置に設置されることが多いため、外部の攻撃者

から攻撃しやすく、脆弱性が存在していると格好の標的になり得る。改めて VPN 装置のベンダーのウェブサイト等を確認し、未対策の脆弱性がないか点検することを勧める。

（2）　要件変更時のセキュリティ対策見直しの重要性

本事例の届出者は、脆弱性対策を重要視していたとみられ、定期的な情報収集を行い、脆弱性情報が公開されると自組織での利用状況に合わせて対策を決定し、必要に応じて修正プログラムの適用等の対策を行うような体制を確立していた。それにもかかわらず、本事例の発生時には脆弱性が残存し、攻撃者に悪用されてしまったのは、機器の利用用途が変わり、必要なセキュリティ対策も変わっていたことの考慮が漏れていたことが原因の一つと考えられる。

今回、攻撃の対象となった機器は、従来ファイアウォールとして利用していたものであり、過去に公開された脆弱性について、ファイアウォール機能に関するものは解消済みであった。その一方で、VPN 機能に関する脆弱性は、当時の利用形態から対応不要とされていた。脆弱性が残った状態にあっても、VPN 機能を利用していなかったために特に問題は生じていなかったが、昨年、テレワークに対応するために、当該機器の VPN 機能を有効化したことにより、脆弱性も顕在化してしまった。

サーバ、パソコン、ネットワーク機器、およびその上で稼働するソフトウェア等、使用する機器が多岐に渡ると、日々公開される脆弱性情報をキャッチアップしていくだけでも労力を要する。過去に公開された脆弱性情報まで遡って対策の検討をするのは更に労力が必要で、容易に実行できない作業であると考える。しかし、利用用途の変更等でシステムの構成変更や機器の設定変更が行われるときは、セキュリティ要件の変更にも着目し、適切なセキュリティ設定や脆弱性対策ができているかの確認を行うことが重要である。必要に応じて脆弱性診断を受診することも検討していただきたい。

5. 事例：クラウド上の開発環境からの認証情報窃取による不正アクセス

5-1. 届出内容

（1）　発見経緯

外部のセキュリティ研究者から、届出者と無関係の海外のウェブサイトで届出者企業の内部情報と思われる情報が公開されているという連絡があった。調査を行ったところ、クラウド上に構築していたデータベースに不正アクセスがあり、データが窃取されていたことが判明した。

（2）　被害内容と被害原因

1. ウェブアプリケーションのソースコードを管理するクラウド型プラットフォームへ不正アクセスされ、ソースコードが窃取された。このプラットフォームにアクセスするためのアカウントには二要素認証を設定していたが、通常のログイン方法とは別に、二要素認証が動作しないアクセス経路が存在していたことが分かった。調査の結果から、攻撃者は、この経路を使用して認証を突破したと推測している。
2. ソースコード内に含まれていた認証キーを悪用され、サービスサイトの本番環境が稼働するクラウドサービスに不正アクセスされた。さらにクラウド上にデータ窃取用の踏み台サーバを作成された。
3. 踏み台サーバを経由されたことでアクセス制限設定が回避され、同クラウド上のデータベースサーバのデータが窃取された。

（3）　被害対応

- ソースコードからキー情報を削除（プログラム内にキー情報を保管する方式から、都度アクセスのための情報を取得する方式へ変更）
- 定期的なキーの変更
- 不正アクセスの監視機能の導入

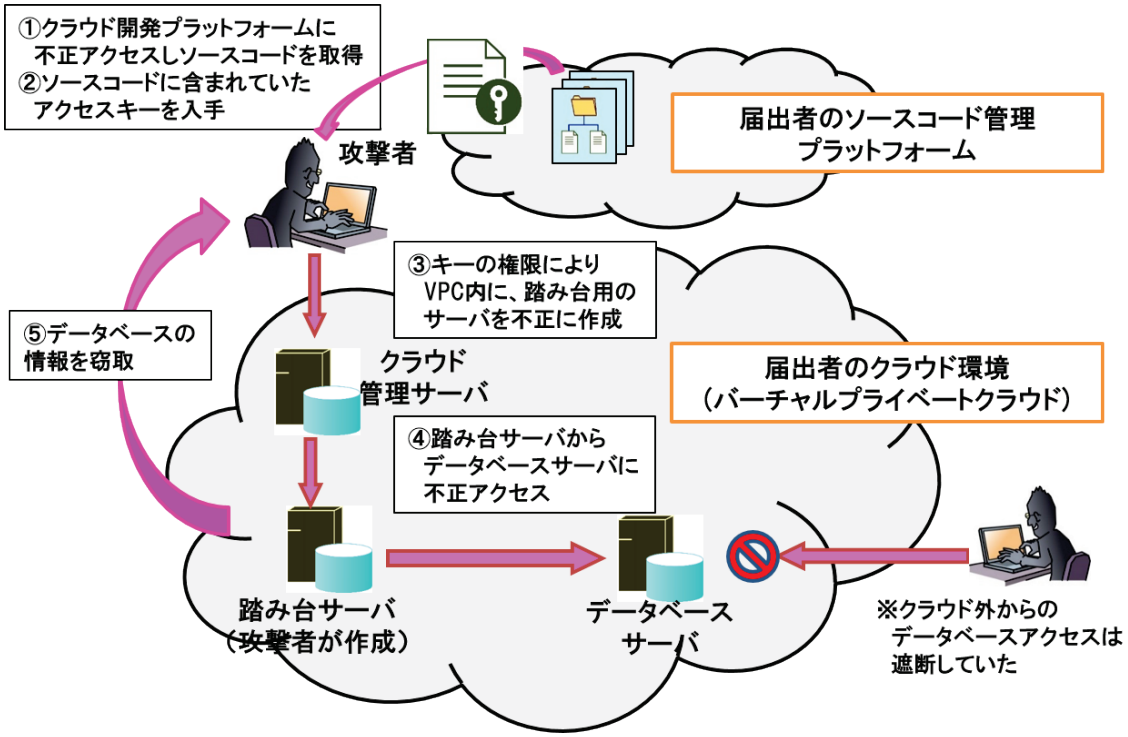

図 5-1 本事例での攻撃の流れ

5-2. 着目点

（1） 開発環境からの認証情報流出

届出者は、ソフトウェア開発のソースコードをクラウド上のプラットフォームで管理していた。ソースコードが窃取されて、内包していた本番システムへアクセスするための認証情報（キー）が奪われ、最終的にクラウド上のデータベースまで侵害された。

この事例に限らず、本番システムへアクセスするための認証情報等が、開発環境やテスト環境から流出したという事例が見られるようになってきている。

従来は、システムやソフトウェアの開発は組織内やクローズドなネットワークに構築する等して、場合によっては入室可能な人員を制限する等の物理セキュリティも含め、攻撃や漏洩等のリスクから守られてきた。近年では、本番システムだけでなく、開発環境もクラウドへの移行が進み、それにより攻撃を許す隙が生じているケースがある。開発環境にも本番環境と同等のセキュリティの確保が必要である。

この事例の場合、設定していた二要素認証が迂回されるという、事前に想定し対策することが難しい攻撃が行われたと思われる状況であった。一方、クラウドサービス等の外部サービスを使用する際、把握していなかった仕様や設定項目が存在し、抜け穴となってしまうような事例は他にもある。リスク管理やセキュリティの検討において注意が必要な観点と考えられる。

（2）　クラウドサービスへアクセスするための認証情報の不正利用

クラウドサービスの中には、システム開発や構築のガイドラインが提示されている場合がある。例えば、データベースサーバは外部からアクセスできないプライベートサブネットに構築し、接続可能な IP アドレスを限定するといった、推奨されるネットワーク構成やセキュリティ設定が示されていることもある。

この事例において、届出者はガイドライン等を考慮したセキュリティ設計をしていたと思われ、データベースへアクセス可能な IP アドレスは同じバーチャルネットワーク内のものに制限する等の設定をしていた。しかし、窃取されたキーがクラウド上にサーバを作成できる権限を持っていたため、攻撃者はバーチャルネットワーク内にサーバを自由に構築することが可能であった。データベースへのアクセスは制限されていたにもかかわらず、攻撃者に踏み台用のサーバをバーチャルネットワークに作成されてしまったことで、アクセス制限を回避され、データベースに不正アクセスされてしまった。また、攻撃者は当初データベースサーバに外部からアクセスできるように、当該キーを用いてアクセス制限を変更しようとした。しかし、このキーにはアクセス制限を変更する権限がなかったため、失敗に終わっている。

本事例はセキュリティを考慮した設計が行われていたと思われるが、攻撃方法によっては、不正アクセスをされてしまうことがあり得ることを示している。そのため、セキュリティを考慮した設計や設定を行うと同時に、クラウド環境への不正なアクセスや意図しない変更が行われた場合に、早期に検知できるような仕組みを導入することも重要である。

また、類似の事例としてクラウドサービスの管理者用のキーが漏洩した事例もあり、管理者用のキーを悪用されて管理者権限を持ったアカウントを作成されてしまったり、セキュリティ設定を変更されて外部からのアクセスを可能にされてしまったりしたものを確認している。

攻撃者に管理者権限を掌握されてしまうと、情報が窃取されるだけに留まらず、正規の管理者のログイン妨害や、アクセスの痕跡の隠滅等も行われる恐れがある。これにより、インシデント対応の実施、被害原因や被害範囲の特定等が困難になる可能性がある。管理者用のキーは厳密に管理するとともに、可能ならば、用途別に必要な権限に絞ったキーを発行するといった運用が望ましい。

今期確認した、管理者キー漏洩の届出では、管理者のキーが悪用されたことは確かであろうものの、漏洩した理由は不明とのことであった。まずは現在の運用管理方法を確認し、どこにどのような形でキーが保存されているか、それらが漏洩しないような対策がなされているかを検証していただきたい。

6. 届出へのご協力のお願い

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

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

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