# コンピュータウイルス・不正アクセスの届出事例

［2019 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

2020 年 2 月 7 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]。

今後の攻撃の増加の可能性を含め、特に留意すべき事例は次の 2 点である。

- データベースを消去し脅迫する手口 ： 1-1 章および 3 章で紹介する。
- 「ラテラルフィッシング」と呼ばれる手口 ： 5 章で紹介する。

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。

## 1-1. 「データベースを消去し脅迫する手口」について

今期（7 月～12 月)、「何者か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」という被害が 4 件[6]、届出窓口へ報告された（前期、前々期は 0 件)。本章では、この攻撃手口について説明する。なお、代表的な 1 件について、事例を 3 章で紹介する。

### 1-1-1. 攻撃手口

この攻撃は次のような手口で行われる。

- 攻撃者が何らかの方法で企業等のデータベース等へ不正アクセスする。
- データを窃取した上で、当該データを**消去**する（ただし、攻撃者が「我々がデータを持っている」と脅迫文で主張しているのみであり、実際に窃取が成功しているか否かは定かではない)。
- データが保存されていた場所に、データの復旧等のために金銭を支払うよう要求する脅迫文を残す（現時点で確認されているのは全て英文)。
- 脅迫文には、「一定期間内に支払いがなければ（攻撃者の手元の）バックアップを削除する」という内容や、一部の事例では「支払いがなければデータを公開する」という内容が含まれる。

これは、ランサムウェアによる脅迫と同等の攻撃手口である。ランサムウェアの場合、感染させられたパソコンやサーバ内のファイルが暗号化され、ファイルの復号と引き換えに身代金が要求されることになる（ファイルの窃取も同時に行われ、支払わなければファイルを公開すると脅迫されるケースもある)。この手口では、アクセス制御が不十分なデータベースサーバや、データベースへアクセス可能なウェブアプリケーションが狙われている。

### 1-1-2. 観測状況と攻撃経路

IPA へ届出のあった 4 件については、次の攻撃経路（一部推定）を確認している。

- 2019 年 8 月、9 月：アクセス制御が不十分な phpMyAdmin 経由での攻撃（2 件）
- 2019 年 11 月、12 月：外部からアクセス可能な MySQL サーバへの攻撃（2 件）

[6] 表 2-1 の項番 1, 2, 5, 8 が該当する。

この「データベースを消去し脅迫する手口」自体は 2017 年 1 月頃から確認されている。2017 年当時は、外部からアクセス可能な MongoDB や Hadoop が攻撃の対象となり、数万件規模の被害が発生したと言われている [7,8]（IPA においても、2017 年には MongoDB での被害の届出を受理している）。その後、MongoDB への大規模な攻撃が再び発生したり [9]、データベースとは異なるが、特定の NAS に対して同様の攻撃が行われたり [10]といった情報がある。

2019 年 8 月以降、日本国内で 4 件の被害が立て続けに報告された原因は不明だが、確認できた範囲においては、脅迫文の文面が似ていることから、同一の攻撃者（攻撃グループ）が活動していた可能性がある。アクセス制御が不十分なシステムが今後も狙われる可能性があり、注意が必要である。

### 1-1-3. 対策

確認できている限り、この攻撃は特殊な不正アクセスの技術等によるものではなく、何らかアクセス制御の不備を突くものであった。このため、一般的な不正アクセス対策を確実に実施していただきたい。

- データベースサーバやデータベースへアクセス可能なウェブアプリケーション等の適切なアクセス制限の設定、脆弱性の解消
- 公開ウェブサイト等（テスト用のサーバ等を含む）にデータベース管理ツールが意図せず設置されていないか確認
- 複雑なパスワードの設定
- （データ消去や改ざんへの対策として）データ／ファイルのバックアップ

---

[7] ZDNet「「MongoDB」狙うランサムウェア攻撃で 2 万 7000 超のデータベースが被害に--研究者ら報告」(2017/1/10)
https://japan.zdnet.com/article/35094721/

[8] ITmedia「Hadoop や MongoDB のデータ消去被害が続出、世界各国で」(2017/1/20)
https://www.itmedia.co.jp/enterprise/articles/1701/20/news062.html

[9] ZDNet「「MongoDB」 に再びランサム攻撃 約 2 万 6000 件の被害」(2017/9/7)
https://japan.zdnet.com/article/35106907/

[10] BleepingComputer「Attackers Are Wiping Iomega NAS Devices, Leaving Ransom Notes」(2019/7/29)
https://www.bleepingcomputer.com/news/security/attackers-are-wiping-iomega-nas-devices-leaving-ransom-notes/

## 2. 届出事例概要一覧

2019 年 7 月～12 月の期間に受理した届出において、主な事例の概要の一覧を表 2-1 に示す。

**表 2-1 主な届出事例の概要一覧**

| 項番 | 届出日 | 概要 |
|---|---|---|
| アクセス制限の不備を悪用された被害 | | |
| 1 | 2019/8/14 | 届出者（企業）の社内グループウェアのデータベースが空の状態にされ、10 日以内に 0.03 ビットコインを支払わない場合バックアップファイルを削除する旨記載されたファイルが置かれていた。調査の結果、元々設置していた phpMyAdmin（ウェブブラウザでデータベースを管理するツール）へ第三者によるアクセスが可能であったこと、また、データベースの root ユーザでのログインが容易であったことが不正アクセスの原因として推測された。 |
| 2 | 2019/9/19 | 届出者（非営利団体）が運営する EC サイトのデータベースが消え、身に覚えのないデータベースが作成された。作成されたデータベースには、身代金を要求する内容の英文が格納されていた。不正アクセスの原因を調査したところ、管理用に設置していた phpMyAdmin が不正使用されていたことが判明した。<br>**※本事例は 3 章で紹介する。** |
| 3 | 2019/10/18 | 外部組織からの連絡により、届出者（公共機関）の組織内から外部へ大量の SSH 通信が行われていることが発覚。調査したところ、外部に公開していたウェブサーバから通信が発生していた。<br>当該サーバは SSH ログインに関するアクセス制限を行っていなかったため、総当たり攻撃により不正にログインされ、攻撃の踏み台にされていた。<br>**※本事例は 4 章で紹介する。** |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 4 | 2019/11/1 | 外部組織からの連絡により、届出者（企業）が管理するサーバから SSH の総当たり攻撃が行われていることが発覚。調査したところ、当該サーバは検証用として一時的に構築されたもので、アクセス制御が不十分であったところに総当たり攻撃を受け、SSH で不正にログインされていた。その後、当該サーバから外部組織のサーバへ SSH の総当たり攻撃が行われていた。 |
| 5 | 2019/11/6 | 届出者（企業）の社内で使用していたファイル共有システムで、データベース内の既存のテーブルが消され、データベースを復元したければビットコインを支払うよう要求するメッセージが書かれたテーブルが作成されていることが発覚。調査の結果、不正アクセスの原因は MySQL サーバのポート 3306 番のアクセス制限が行われていなかったことと推測された。 |
| 6 | 2019/11/7 | 届出者（公共機関）が管理するサーバに不審なファイルが複数作成されていることが発覚。ファイルの 1 つは、データ復元のために金銭を支払うよう要求する脅迫文が書かれたファイルであった。ただし、サーバ内のファイルの暗号化や削除等は行われていなかった。不審なファイルが作成された原因を調査したところ、保守作業の委託業者が作業用にインストールした Samba が外部からアクセス可能な状態のまま放置されており、更にログインパスワードが脆弱であったため不正にログインされ、ファイルが作成されてしまっていた。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 7 | 2019/11/13 | 届出者（企業）が運営するウェブアプリケーションシステムの利用者から、システム連絡先のメールアドレスから不審なメールが届くとの連絡があり、事案が発覚。確認したところ、当該システムのメールサーバから不特定多数のメールアドレスに対して不審なメールが送信されていた。原因を調査したところ、当該システムのメールサーバに登録していた複数のメールアカウントが、ユーザ名とパスワードが同一であったり、ユーザ名から推測可能で脆弱なパスワードであったりしていたことが判明。また、外部から恒常的な総当たりのログイン試行を受けていたことも判明した。 |
| 8 | 2019/12/5 | HTTP 監視サービスからの通知を受け、届出者（企業）が運営するウェブサイトがエラー（500 server error）となっていることが判明。確認したところ、サーバ内の MySQL のデータベースが書き換えられ、失われたデータベースを回復するには 0.06 ビットコインを指定のアドレス宛に送信するよう要求するメッセージが格納されていた。原因を調査したところ、当該サーバ上のデータベースは外部から接続可能な状態であり、パスワードなしでログインできるユーザが存在していたために侵入されていた。 |
| 9 | 2019/12/6 | 外部組織からの連絡により、届出者（公共機関）のサーバからフィッシングメールが送信されていることが発覚。調査したところ、外部に公開していたサーバの OS に安易なパスワードを設定したユーザが含まれており、また、アクセス制限を設けずに SSH を公開していたために不正にログインされ、フィッシングメールの中継サーバとして悪用されていた。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| リスト型攻撃による顧客アカウントの被害 | | |
| 10 | 2019/8/16 | 届出者（企業）が運営する EC サイトで、特定の IP アドレスから顧客アカウントに対する大量のログイン試行を検知。一部アカウントではログインに成功していた。ログイン試行の内容を調査したところ、個々のアカウントへのログイン試行回数は多くなく、多数のアカウントに対してログインを試みていたことから、リスト型攻撃であったと推測された。 |
| 11 | 2019/9/2 | 届出者（企業）が運営するショッピングサイトで、ログイン回数制限を超えるアラートが増加していることを発見。さらに顧客からも覚えのない注文メールが来たとの連絡を受けた。調査したところ、約 25 万件の不審なログイン試行があり、約 800 件のアカウントでは実際にログインも行われていた。ログイン試行のうち約 99%は登録されていないメールアドレスであったことから、外部から入手されたリストをもとに攻撃が行われたものと推測された。また、届出者は当該サイトに対して、ログイン試行回数に基づくブロック措置を講じていたが、ログイン試行で使われたと見られる IP アドレスが 1 万件以上あり、1IP アドレスあたりの試行回数、1 アカウントあたりの試行回数が少なかったため、ブロック措置が回避されていた。 |
| 12 | 2019/10/2 | 届出者（企業）が運営する会員制ウェブサイトで、ログイン試行が 10 分間に 400 件以上発生し、監視アラートが発報した。調査したところ、パスワードリスト攻撃により会員のアカウントが不正アクセスを受け、当該サービスで運用されているポイントが不正に引き換えられるといった被害が発生していた。 |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 13 | 2019/11/22 | 届出者（企業）が運営する会員制ウェブサイトを利用する顧客から、自身のアカウントで身に覚えのない操作履歴があるとの連絡を受け、不正ログインが発覚。調査の結果、原因は他社サービス等から不正に入手したと思われるメールアドレスとパスワードが使用されて、不正なログインが行われたためと推測された。 |
| CMS の脆弱性を悪用された被害 | | |
| 14 | 2019/9/5 | 届出者（非営利団体）が運営するウェブサイトの利用者から、ウェブサイトにアクセスするとフィッシングサイトにリダイレクトされるという連絡を受け事案が発覚。調査したところ、利用していた CMS のプラグインの脆弱性が悪用され、設定値が書き換えられたことにより、プラグインの機能によって意図しないサイトへのリダイレクトが実行されていた。届出者は月 1 回の頻度で定期的にプラグインの更新を行っていたものの、本事例では脆弱性対策済みのプラグインが公開されてから約 1 週間後の攻撃であったため、被害を防ぐことができなかった。 |
| 15 | 2019/11/29 | ホスティングサービスを運営する届出者（企業）が、メールサーバのメンテナンスでメールの滞留を発見。確認したところ、ホスティングサーバの顧客を装った不審メールが、当該顧客がウェブサイトを運用しているサーバから送信されていた。原因を調査したところ、当該ウェブサイトで使用されている CMS のメール送信機能が外部からアクセス可能な設定になっていたこと、CMS のバージョンが古く脆弱性が残っていたこと、webshell（ウェブサーバに不正に設置され、第三者による遠隔操作を可能とする不正プログラム）が設置されていたことが確認された。（被害の直接的な原因がいずれであったかの究明には至っていない） |

| 項番 | 届出日 | 概要 |
| --- | --- | --- |
| 独自プログラムの脆弱性を悪用された被害 | | |
| 16 | 2019/9/20 | 外部組織からの連絡により、届出者（企業）が運営するホスティングサーバ上の顧客ウェブサイトから、ウェブサイトで管理していたメールアドレスとパスワードが漏えいしていることが発覚。調査したところ、届出者が開発したプログラムに脆弱性があり、SQL インジェクション攻撃を受けていたことが判明した。 |
| 17 | 2019/11/6 | 外部委託している SOC から、届出者（企業）のウェブサイトに対する SQL インジェクション通信を検知した旨の通報を受け、攻撃が発覚。調査したところ、ウェブアプリケーションのプログラム上の脆弱性を悪用されていた。攻撃により、ウェブサイトの問合せフォームに入力された顧客のメールアドレス等の個人情報が漏えいした。 |
| フィッシング攻撃による被害 | | |
| 18 | 2019/10/17 | 届出者（公共機関）が運用するメールサーバから大量のフィッシングメールが当該組織内に送信されていることが発覚。調査したところ、複数の既存アカウントが悪用されてフィッシングメールが送信されていた。これらのアカウントでは以前にフィッシングメールを受信しており、ユーザが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）を窃取された可能性があった。<br>**※本事例は 5 章で紹介する。** |

届出には本紙に示した事例だけでなく、ウイルスの発見・感染、DoS 攻撃、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「届出状況」として公開する。

## 2-1. 着目点

2019 年下半期で届出のあった被害について全体を通して見ると、多くの被害は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防げた可能性のあるものと見受けられ、基本的なセキュリティ上の取り組みを着実に実施することの大切さがうかがえる。

情報システムの運用や管理に携わる方々には、これらの被害を他人事として捉えたり、情報セキュリティを過度に難しいことと捉えて手をこまねいたりせず、まずは、サーバのアクセス制限の状況確認や各種修正プログラムの適用など、基本的なセキュリティ上の取り組みを着実に実践していただきたい。

今期の届出は、表 2-1 に示した通り、大きく 5 種類の被害に分類できた。続いて、これらについて補足する。

### 2-1-1. アクセス制限の不備を悪用された被害

依然として、アクセス制限などの基本的な対策が行われずに通信サービスを公開してしまったために不正アクセス被害を受けた事例が見受けられる。

今期では、phpMyAdmin といったデータベース管理ツールが外部からアクセス可能になっていたために不正アクセスを受け、データベースを消去され身代金を要求されるといった被害や、ファイルサーバサービスを外部からアクセス可能な状態のまま放置していたために不正なファイルを設置された被害、SSH によるログインが外部から行える状態になっていたために不正にログインされ他組織への攻撃の踏み台にされたといった被害が届出られている。

インターネットに接続する機器は、通信のアクセス制限が必要であるか否かを漏れなく確認し、必要な場合には最小限の通信に限ってアクセスを許可すること（すべての通信を許可しない状態を土台とした上で、可能な限り条件を絞って許可する通信を設定していく）を心掛けていただきたい。そして、特にネットワーク経由で機器を操作する管理機能（ブラウザを使った管理機能、SSH や RDP といったリモートアクセス機能など）の制限については確実に実施していただきたい。

また、システム構築やメンテナンス作業で一時的に使用していたサービスや管理機能が本番稼働時に残存するといったことが起きないよう、不要なサービスや管理機能が稼働していないかの確認も行っていただきたい。

アクセス制限の不備を悪用された被害について、項番 2 の事例の詳細を 3 章で、項番 3 の事例の詳細を 4 章でそれぞれ紹介する。

### 2-1-2. リスト型攻撃による顧客アカウントの被害

リスト型攻撃によるアカウントの不正ログインは、現在でもしばしば被害が発生していることが分かる。

これらの攻撃に対しては、利用者とサービス提供者の双方で対策を進めるべきであり、そもそも、利用者側がパスワードの使いまわしをしないことが重要である。サービス提供者側のシステム的な施策としては、パスワードを用いない認証方法の導入や、不審なログインの試行を検知する仕組み、ログインが行われた時に利用者へ通知する仕組みを導入するといったことが考えられる。

### 2-1-3. CMS の脆弱性を悪用された被害

CMS の脆弱性を悪用された被害が今期でも発生している。

特に今期の事例では、普段から修正プログラムを定期的に適用していたにも関わらず、修正プログラムの公開から攻撃までの期間が短かったため、対応が間に合わず被害を受けたというものもあった。

脆弱性の公開（修正プログラムの公開）から、実際に攻撃が行われるまでの期間が短いケースがあることをふまえ、脆弱性対策では、修正プログラムの公開を速やかに把握できるよう日頃の情報収集が大切になる。また、速やかに修正プログラムを適用するための手順や体制を前もって整えておくことも重要である。

### 2-1-4. 独自プログラムの脆弱性を悪用された被害

ウェブアプリケーションにおいて独自に作成したプログラムの脆弱性が悪用され、SQL インジェクション攻撃の被害に遭ったという被害が今期でも発生している。

独自に作成するプログラムに関しては、まず開発段階でセキュアな設計を行い脆弱性を作りこまないようにし、システムリリース前にも脆弱性点検を行っておく必要がある。また、新たな攻撃手法にも随時対応していくために、定期的に脆弱性点検を行い、新たに発見される脆弱性を修正していく必要もある。

### 2-1-5. フィッシング攻撃による被害

フィッシング攻撃によるメールアカウント情報の窃取についても依然として被害が発生している。

メールアカウントが攻撃者に窃取されると、そのメールアドレスからフィッシングメールやウイルスメールを送るなどの攻撃の踏み台にされてしまい、周囲に被害を拡散しかねない。また、ビジネスメール詐欺の被害に繋がる可能性もある。

フィッシング攻撃に対しては、まずメール利用者自身がフィッシング攻撃の手口を認識

して、不審なメールの添付ファイルや URL リンクを開かないこと、また、本物ではないウェブサイトで ID やパスワードを入力しないことが重要である。企業・組織等においては、システム管理部門が定期的にフィッシング攻撃の手口について情報収集し、利用者に注意を促すといったことも有効である。

フィッシング攻撃による被害については、項番 18 の事例の詳細を別途 5 章で紹介する。

## 3. 事例：データベースを消去し脅迫する手口による攻撃

### 3-1. 届出内容

（1）　発見経緯

担当者が EC サイトのデータベースが消えていることに気づいた。

（2）　被害内容

- 既存のデータベースが消去され、脅迫文が格納されたデータベースが作成された。
  脅迫文には英文で以下のような内容が書かれていた。
  - データベースを戻すにはビットコインを支払い、メールで連絡せよ。
  - データベースは我々がダウンロードし、バックアップしている。
  - 10 日以内に支払いが行わなければ、バックアップは削除する。

- データベースに登録されていた EC サイト利用者の個人情報約 3,000 件が窃取された。

（3）　被害原因

アクセス制限が不十分な状態で phpMyAdmin を利用していた。

調査の結果、ログイン試行の形跡として、辞書攻撃が行われて 4 時間後、不正にログインされていたことが確認された。

（4）　被害対応

- phpMyAdmin の利用停止。
- MySQL の root パスワードを複雑なものに変更。

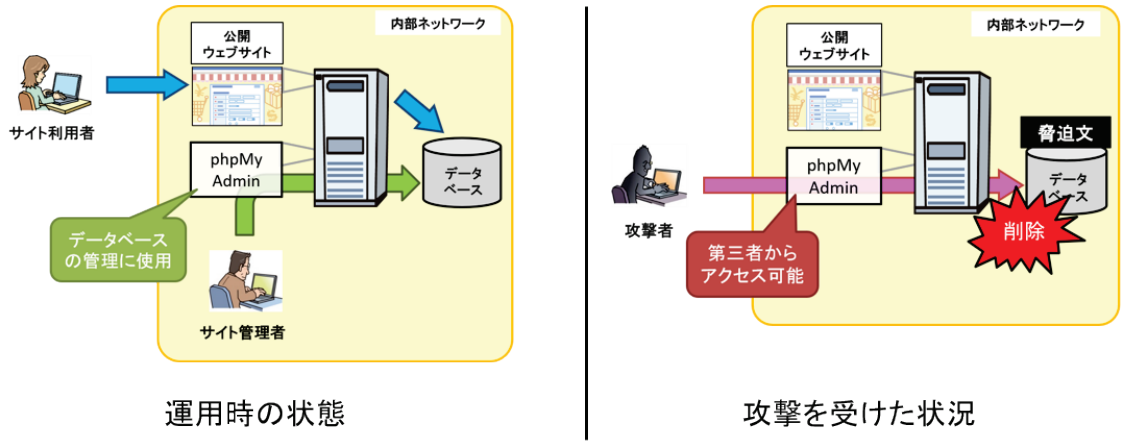


**図 3-1 事例の概要図**

### 3-2. 着目点

（1） データベースを消去し脅迫する手口

この事例は「データベースを消去し脅迫する手口」による攻撃が行われたものである（詳しくは 1-1 章を参照）。

（2） phpMyAdmin の利用

本事例では、phpMyAdmin を悪用されて攻撃を受けている。

phpMyAdmin はウェブサーバに設置して利用するデータベース管理ツールであり、ブラウザを使用して簡単にデータベース操作を行うことができるソフトウェアである。

インターネット上に公開するウェブサーバに phpMyAdmin を設置する場合は、アクセス制限を適切に設定していないと、第三者が phpMyAdmin にアクセスできてしまうという危険な状態になりかねない点に注意が必要である。

phpMyAdmin の利用については慎重な検討が必要であり、利用する場合には、適切なアクセス制限が必須である。また、システム公開前の構築作業等で一時的に利用するといった場合は、システム公開前に削除したことを必ず確認する。システム構築中やサーバがテスト環境であるといった場合でも、当該サーバをインターネットに接続する場合は、本番環境と同等のアクセス制限が必要である。

（3） データベースのパスワード設定

本事例では、最終的にはデータベースのパスワードが辞書攻撃により突破され、データが消去されることとなった。OS 等のアカウントのパスワードと同様に、これらのパスワードも十分複雑なものに設定しておく必要がある。

なお、本事例では、ログイン試行は約 4 時間続いていることも判明している。不正なロ

グイン試行を検知する仕組みがなければ、長時間に渡り攻撃が試みられるものと考えられ、多少複雑な程度のパスワードでは危険であることが分かる。

## 4. 事例：アクセス制限されていない SSH サービスに対する執拗な攻撃

### 4-1. 届出内容

（1）　発見経緯

外部組織から連絡を受けて事案が発覚。

（2）　被害内容

- 外部公開していたウェブサーバに SSH で不正にログインされた。
- 当該サーバが攻撃の踏み台とされ、1 時間あたり 3,000 ヵ所近い IP アドレスに対して SSH 通信が試行されることとなった。

（3）　被害原因

ウェブサーバの SSH サービスを接続元 IP アドレス等で制限せずに公開していた。

当該ウェブサーバは外部から毎日数千～1 万回近い SSH ログインが試行されており、いつパスワードを破られてもおかしくない状態にあった。

（4）　被害対応

- 当該サーバについてはネットワークの接続を停止し、別途新規サーバを構築した。
- 新規サーバにおいては通信経路にあるルータ等で SSH を通過させないなど、適切なアクセス制御を実施した。

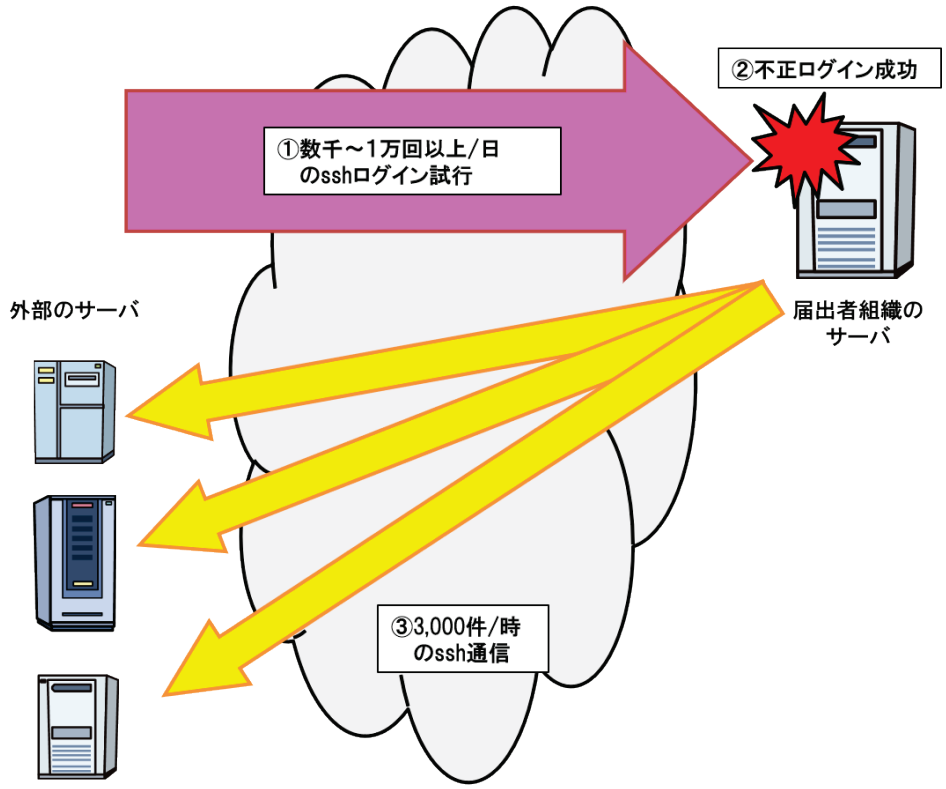


**図 4-1 攻撃の様子**

## 4-2. 着目点

（1） 執拗かつ連鎖的な攻撃

本事例では、被害を受けたサーバが外部から毎日数千～1 万回近い SSH ログイン試行を受けていたことが判明している。また、不正にログインされた後は、そのサーバから 1 時間あたり 3,000 ヵ所近い IP アドレスに対して SSH 通信が試行されている。

すなわち、3 章の事例と同様に、外部からアクセス可能な経路については、ログイン試行が際限なく行われており、また、本事例では攻撃が成功した場合、そのサーバを悪用して更なる攻撃が行われるという連鎖的な状況も見て取れる。

現在のインターネット環境ではこのような攻撃が常態化しており、適切なアクセス制限を施していない機器をインターネットに接続すると、すぐに攻撃の対象となる。そればかりか、機器が乗っ取られて、他者への攻撃に加担してしまう恐れもある。

重要なサーバもさることながら、たとえ試作環境やテスト環境といったコンピュータであって、攻撃を受けても自身の損害は小さいといった場合でも、他者への攻撃に悪用される危険性を考慮し、アクセス制限は適切に行っていただきたい。

## 5. 事例：ターゲット組織のウェブメールサービスを模造したフィッシング

### 5-1. 届出内容

（1） 発見経緯

届出者（公共機関）が管理するメールサーバから組織内に大量のフィッシングメールが着信した。

（2） 被害内容

- 届出者組織内の数名のメールアカウントを使用して 4 万件以上のフィッシングメールが発信された。
- 窃取された数十名のアカウントが保持するメールについて、氏名、メールアドレス等の個人情報が覗き見られた可能性がある。

（3） 被害原因

本事案発見以前より、外部から届出者組織内に対しフィッシングメールが届いており、それらのメールからフィッシングサイトに誘導され、メールアカウントが窃取された可能性がある。

フィッシングメールは、メールサーバからの通知であるように見せかけたもので、メールアカウントに関する情報を確認するよう促す文面で、不正な URL リンクをクリックさせるものであった。また、URL リンク先は届出者組織独自のウェブメーラのログイン画面を模造したフィッシングサイトになっていた。

（4） 被害対応

- 組織内のユーザに対し、パスワード変更を行うよう周知徹底した。
- 多要素認証の導入を検討中。

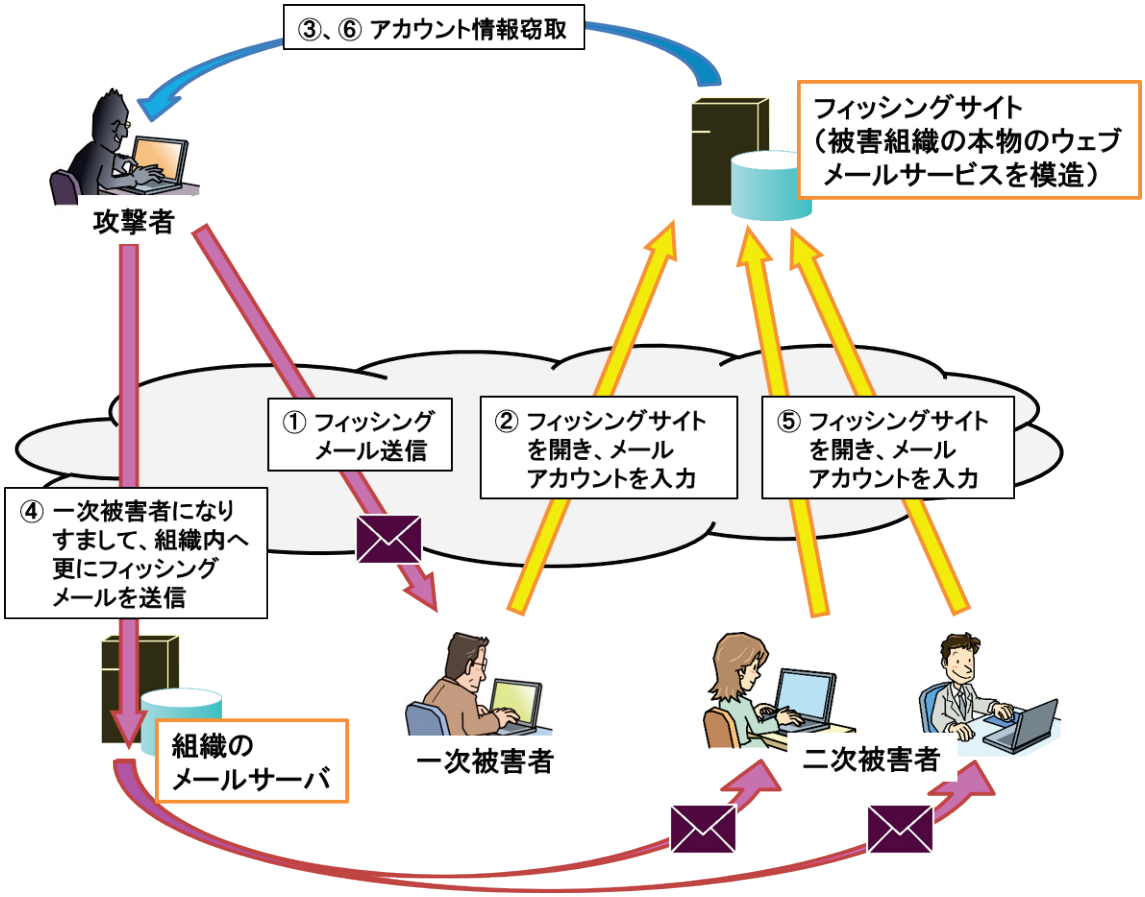


**図 5-1 フィッシング攻撃の流れ**

## 5-2. 着目点

（1） 特定の組織を狙うフィッシング攻撃＋ラテラルフィッシング

本事例で攻撃者が作成したフィッシングサイトは、届出者の組織独自のウェブメールサービスのログイン画面を模造したものであった。また、最初に窃取したアカウント情報を用いて、組織の正規のメールサーバを使用し、更に組織内の別の利用者へも攻撃が行われた。このような、信用されやすい組織内のアカウントやサーバを悪用し、組織内へ攻撃範囲を拡大していく手口は**「ラテラルフィッシング」**（lateral phishing）と呼ばれる。本事例は、届出者組織を明確に狙った攻撃であったと考えられる。

フィッシング攻撃は、不特定多数にばらまかれ、ネットバンキングやクレジットカード情報を窃取するような金銭目的のものとは別に、本事例のように、特定の組織を狙い、機密情報の窃取を目的とするものも存在することに留意する必要がある。

（2） 巧妙化するフィッシング攻撃への対策

巧妙化するフィッシング攻撃に対しては、専門知識を持たない一般の利用者に対しても、

メールの内容やリンク先のサイトの見た目だけではなく、メールの送信元アドレスやウェブサイトの URL が正規のものであるかといった細かい点に注意するよう求めたり、正規のポータルサイトやブックマークからログイン画面を開くといったことを徹底したりする必要があるが、一方で限界もある。

アカウント情報が窃取された場合、あるいは窃取が試みられた場合に備えて、不審なログインを検知する仕組みや、ログインした場合に利用者へ通知する仕組みなどの導入、また、システム管理者が事案の早期発見、対処を行えるよう、通報窓口の周知を徹底すること、インシデント対応の体制を整えておくということも重要である。

## 6. 届出のお願い

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、類似の被害の早期発見や被害の低減等に役立てていただくことを目的としています。

IPA では、日々国内の様々なセキュリティ動向を調査しており、特に、日本国内で発生しているサイバー攻撃等に関する状況や、具体的な攻撃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）