コンピュータウイルス・不正アクセスの届出事例

［2020 年上半期（1 月～6 月）］

独立行政法人情報処理推進機構 セキュリティセンター

2020 年 8 月 6 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. 届出事例概要一覧

2020 年 1 月～6 月の期間に受理した届出において、主な事例を次の 6 種に分類した。それぞれの届出の概要を表 2-1 に示す。

- ウイルス感染の被害 （9 件）
- メールシステムの不正利用・アカウントへの不正アクセス （13 件）
- パスワードリスト型攻撃による不正ログイン （3 件）
- ウェブサーバへの不正アクセス （7 件）
- アクセス制御不備・運用不備により攻撃を受けた事例 （6 件）
- その他 （8 件）

表 2-1 主な届出事例の概要一覧

項番	届出日	概要
ウイルス感染の被害		
1	2020/1/11	届出者（企業）がシステム構築等を行った先の企業のシステムがランサムウェアに感染し、サーバ内のファイルが暗号化されてシステムが起動しなくなる被害が発生した。調査したところ、設定していた外部からのアクセス制限が何らかの理由で適切に動作しなくなっており、攻撃者にリモートデスクトッププロトコルで侵入されたものと推測される状況であった。アクセス制限が動作しなくなった原因は不明である。 セキュリティ上重要な装置については、変更管理の徹底や、設定状態の定期的な確認が、リスク低減に繋がると考えられる。
2	2020/1/15	届出者（企業）で利用しているパソコンが「Emotet」と呼ばれるウイルス（以下、Emotet）に感染した。
3	2020/1/27	届出者（企業）の従業員になりすまして送信された不審なメールが、届出者の取引先に着信していることが発覚した。調査したところ、当該従業員が不審なメールの添付ファイルを開き、パソコンが Emotet に感染していたことが判明した。

項番	届出日	概要
4	2020/1/28	届出者（企業）の従業員が利用するパソコンで不審な挙動が確認され、外部との接続を制限する等の処置を行った上で調査したところ、ウイルスに感染していることが判明した。更に詳細に調査を実施したところ、セキュリティソフトの脆弱性を突いた不正アクセスにより、遠隔操作ウイルスを使用され、一部の情報が流出した可能性があることが判明した。
5	2020/2/12	届出者（企業）の社内サーバの一部に不正アクセスがあったことを発見した。調査したところ、社内のパソコンが外部の不審なサーバと通信を行っており、その通信を解読した結果、遠隔操作ウイルスを使用され、社内サーバのファイルに不正アクセスされていたことが判明した。感染したパソコンを隔離するとともに、外部の不正な通信先を特定して遮断する措置を行った。
6	2020/2/21	届出者（企業）の従業員が使用するパソコンが、Emotet に感染していることをセキュリティソフトが検知した。調査したところ、取引先になりすました不審メールが着信し、従業員が添付ファイルを開いたことでパソコンが Emotet に感染したことが判明した。更に、パソコン内のメールの情報が悪用され、組織内外へウイルス付のメールがばら撒かれた。 **※本事例は３章で紹介する。**
7	2020/5/13	届出者（企業）の従業員が使用するパソコンから不審なウェブサイトへの通信が発生していることを検知した。調査したところ、遠隔操作ウイルスの一種に感染しており、従業員等の個人情報が流出したことが判明した。ウイルス定義ファイルの更新、外部からのログイン試行回数の変更等の対策を実施し、全従業員に不審メール受信時における対応手順の周知徹底を行った。
8	2020/5/26	外部からの連絡により、届出者（企業）のウェブサイトの一部が改ざんされていることを確認した。調査したところ、従業員のパソコンのウェブブラウザに、不正な拡張機能がインストールされていたことが判明した。当該ブラウザで CMS を操作してウェブコンテンツを更新した際に、不正なスクリプトを埋め込まれたウェブページが生成されるようになっていた。

項番	届出日	概要
9	2020/6/23	届出者（公共機関）が組織内で使用している、インターネットからアクセス可能な複数台のサーバが、ランサムウェアに感染していることを発見した。調査により、当該サーバの認証がブルートフォース攻撃により突破されたことで侵入され、ランサムウェアを仕掛けられたものと推測された。サーバを再構築して復旧させた。
メールシステムの不正利用・アカウントへの不正アクセス		
10	2020/1/7	届出者（企業）の従業員のメールアカウントに、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、何らかの要因により当該アカウントのパスワードが窃取されたことで、アカウントに不正にログインされ、ばらまき型メールの送信に悪用されたことが判明した。全従業員にパスワードの見直しを周知したとともに、パスワードポリシーの変更を検討している。
11	2020/1/14	届出者（企業）が利用するクラウド型メールサービスから「大量の不正なメールが発信されたためメール送信を制限した」との警告メッセージが管理者に届いた。調査したところ、従業員のアカウントの 1 つが不正にログインされ、大量の迷惑メールの送信が試みられていた。当該アカウントに脆弱なパスワードが設定されていたことが原因と推測されたため、従業員のパスワードに複雑なものを設定することで対応した。
12	2020/1/14	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にログインされ、大量の迷惑メールが送信されたことを発見した。迷惑メールの送信先は、当該アカウントにて過去に送受信したメールの内容から抽出されたメールアドレスであったため、迷惑メールの送信だけでなく、関係者のメールアドレス流出の被害ともなった。不正アクセスを受けたアカウントの ID 変更、全従業員のパスワード変更を実施し、多要素認証の導入も検討している。

項番	届出日	概要
13	2020/1/30	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、アカウントが悪用されて迷惑メールが送信されており、宛先不明等で大量のメールがエラーで戻ってきていたことが判明した。ウイルスの類は検出されなかった。このアカウントの利用者が外部サービスとパスワードの流用をしていたことなどから、当該アカウントへ不正にログインされた可能性がある。パスワードの流用の禁止などを周知徹底した。
14	2020/2/7	契約しているインターネットサービスプロバイダからの連絡により、届出者（公共機関）のメールサーバから大量の迷惑メールが送信されていることが分かった。調査したところ、外部からのメール中継の設定に誤りがあり、オープンリレー可能な状態になっていた。それによって迷惑メール中継の踏み台として悪用されていたことが判明した。
15	2020/2/27	届出者（教育・研究機関）の職員の 2 つのメールアカウントが不正アクセスを受け、メールを窃取されたり、フィッシングメールの送信に悪用されたりしていたことがわかった。 (1)従業員宛に、送信した覚えのないメールに対して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、当該アカウントにて本人の覚えのないメール自動転送設定がされていて、設定から発見までの約半年の間、メールが窃取されていたことが判明した。 (2)メールの受信者からの連絡により、別の従業員のアカウント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。 いずれも何らかの要因でメールアカウントのパスワード情報が窃取され、不正にログインされてメールアカウントが悪用されたものであった。当該アカウントのパスワードを変更し、全従業員に対して注意喚起を行った。また多要素認証の導入も検討している。

項番	届出日	概要
16	2020/3/2	契約しているインターネットサービスプロバイダからの連絡により、届出者（企業）の従業員のメールアカウントから、大量の迷惑メールが送信されていることを検知した。調査したところ、出張者が社外から利用するためのメールシステムに対して多数の不正なログイン試行があり、一部でログインに成功していることが判明した。メール送信サーバがパスワードリスト型攻撃を受けたものと推測されるものであった。アカウント名とパスワードを変更することで対応した。
17	2020/3/25	届出者（企業）の従業員のメールアカウント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。当該アカウントのパスワードが脆弱だった恐れがあり、不正にログインされて、ばらまき型メールの送信に悪用された。全メールアカウントのパスワードを、システムで生成した強固なものに変更する措置を行った。
18	2020/3/27	届出者（教育・研究機関）が利用するクラウド型メールサービスにおいて、職員のメールアカウント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。調査したところ、身に覚えのない日時にログインされた形跡があり、当該アカウントに不正にログインされて、ばらまき型メールの送信に悪用されたことが判明した。職員が外部サービスとパスワードの流用をしていたことが原因と推測している。組織内に注意喚起をするとともに、全アカウントで二段階認証を導入した。
19	2020/5/20	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取引先等に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、そこで詐取されたアカウント情報が悪用されたと推測される状況であった。端末認証の導入によりセキュリティ強化を図り、更に全従業員にセキュリティ教育を再実施した。

項番	届出日	概要
20	2020/5/21	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フィッシングメールが取引先等に送信されていることを発見した。調査したところ、アカウントに不正にログインされてメールが送信されていた。このアカウントの利用者は、以前に標的型攻撃メールを受信しており、その攻撃メールからフィッシングサイトに誘導されていた。フィッシングサイトにおいて、アカウント情報（ID およびパスワード）の入力を行っており、その時詐取されたアカウント情報が悪用されたものと推測される。 **※本事例は 4 章で紹介する。**
21	2020/6/2	届出者（公共機関）のメールサーバが、不正なメールを多数送信しているとして公開ブロックリストに登録されてしまい、外部に送信したメールが不達になる事態が発生した。調査したところ、メールサーバのアクセス制限の設定において、アクセスを許可する組織内部の IP アドレスの範囲を誤って 172.0.0.0/8 と設定していたために、この範囲に該当するグローバル IP アドレスからのメールを第三者に不正中継する踏み台として悪用されていたことが判明した。アクセスを許可するプライベート IP アドレスを正しく 172.16.0.0/12 に設定し、更に SMTP 認証の導入やファイアウォールによる通信制御を追加してセキュリティを強化した。
22	2020/6/24	届出者（業界団体）のメールサーバの負荷が高まり、メールの送信に異常に時間がかかる状態になっていることを発見した。調査したところ、大量の迷惑メールがキューイングされており、当該サーバが外部からの迷惑メールの中継に悪用されていたことが判明した。原因について詳細は調査中だが、メールサーバ利用時の認証が何らかの攻撃で突破されたものと推測しているため、パスワードを複雑なものに変更して対策した。更にメール送信時に利用するポート番号の変更（サブミッションポートの導入）も行った。
パスワードリスト型攻撃による不正ログイン		

項番	届出日	概要
23	2020/6/1	届出者（企業）が提供する会員ポイントサービスに対して不正なログインがあり、会員のポイントが攻撃者の電子マネー等に不正に交換されていたことを発見した。調査したところ、当該サービスからアカウント情報（ID やパスワード）が流出した形跡がないことから、他サービス等で利用されていたと思われる ID やパスワードを用いてリスト型攻撃が行われたと推測された。ログイン時の認証方法の追加や、大量の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。
24	2020/6/10	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、一部で不正なログインに成功していることを社内調査により発見した。更に詳細に調査したところ、多数のログイン試行を繰り返す、本サービス専用に開発されたログイン試行ツールを用いたリスト型攻撃が行われたものと推測された。会員に対してパスワードの流用防止と二段階認証の設定を推奨する通知を実施した。
25	2020/6/19	届出者（企業）が提供する会員サービスに対して、不正なログインの試行が多数行われていることを監視システムにて検知した。調査したところ、不正ログイン試行自体は常時発生しているが、ある時期より回数が急増していることが判明し、不正ログインに成功している事例も発見した。大規模なリスト型攻撃かブルートフォース攻撃が行われたものと推測される。ログイン成功時に会員にメールを送信する機能を追加し、会員に注意喚起を行った。
ウェブサーバへの不正アクセス		
26	2020/1/30	届出者（企業）のウェブサイトの一部が改ざんされ、サイトにアクセスすると、フィッシングサイトに転送されるようになっていた。調査したところ、古いバージョンの CMS を利用していたため、その脆弱性を悪用されウェブページを改ざんされたことが判明した。

項番	届出日	概要
27	2020/2/5	届出者（企業）が運営する EC サイトの利用者に関する情報が流出したことが発覚した。調査したところ、EC システムの脆弱性を悪用した不正アクセスが行われたことが判明した。更に流出した情報を悪用し、当該サイトの利用者に対して詐欺のメールを送る二次的な攻撃も行われた。
28	2020/4/17	届出者（企業）が運営する EC サイトの処理の挙動に不審な点があることを発見した。調査したところ、不正なプログラムが実行され顧客情報の一部が流出したことが判明した。EC システムの脆弱性を悪用した SQL インジェクション攻撃が行われたものと推測される状況であった。
29	2020/5/27	外部組織からの連絡により、届出者（企業）のウェブサイトの一部が改ざんされていたことを確認した。調査したところ、コンテンツ管理画面のアクセス制限の設定を誤って、外部に公開された状態になっていたことが判明した。設定を修正して管理画面に外部からアクセスできないようにした上で、更にログイン時の認証を追加してセキュリティ強化を行った。
30	2020/5/29	ウェブサイト利用者からの連絡により、届出者（非営利団体）のウェブサイトの一部が改ざんされ、届出者と無関係のウェブサイトが表示されるようになっていたことが発覚した。レンタルサーバ会社の調査によると、CMS の脆弱性を悪用され、管理画面に不正ログインされたと推測されるとのことであった。管理画面へのログインに二段階認証を行うように変更して対策した。
31	2020/6/5	届出者（業界団体）のウェブサイトが改ざんされ、サーバ上のプログラムに意図しないコードが含まれていることをウェブサイト管理作業者が発見した。詳細は調査中だが SQL インジェクションの脆弱性が存在し、その脆弱性を悪用した攻撃をされたものと推測している。

項番	届出日	概要
32	2020/6/10	カード決済代行業者からの連絡で、届出者（企業）が運営する EC サイトの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、EC システムの脆弱性を悪用し、偽の決済画面へ誘導するように、ウェブサイトが改ざんされていたことが判明した。ログインやファイルの変更を検知する仕組みを導入して監視を強化した。
アクセス制御不備・運用不備により攻撃を受けた事例		
33	2020/2/12	届出者（企業）のウェブシステムにログインができないことを開発担当業者が発見した。調査したところ、データベースの内容が削除されており、代わりに脅迫文のような文章が残されていたことが分かった。テスト環境の設定に誤りがあり、外部からアクセス可能な状態になっていたため、不正アクセスされ、データベースが削除されたものと推測される。
34	2020/3/5	届出者（公共機関）のサーバから、届出者とは無関係のインターネット上の掲示板に書き込みが行われていることを発見した。調査したところ、届出者のサーバに現在は使用していないアプリケーションが残っており、その中に不正なプログラムを設置され、掲示板書き込みの踏み台にされていたことが判明した。サーバを閉鎖しアプリケーションを削除するなどの対策を実施した。
35	2020/3/18	届出者（企業）が提供するサービスのアプリ開発において、テスト環境へ不正なアクセスがあったことを開発委託先の業者が発見した。調査したところ、次の 3 点の問題があった。 ・委託先業者がアプリのテストのために、一部実際の利用者のデータを格納したデータベースを作成していた。 ・当該データベースを外部からアクセス可能な状態にしていた。 ・ユーザ名とパスワードの設定が脆弱であった。 結果として、リスト型攻撃等によりサーバに不正アクセスされたと推測される。

項番	届出日	概要
36	2020/4/27	外部組織からの連絡により、届出者（企業）が運営するサイトのユーザ情報がダークウェブに公開されていることが発覚した。データベースの一部がシステムリプレース作業の際に誤って公開された状態になっており、そこからデータを窃取されたものと推測される。なおデータの内容やデータベースが誤って公開されていた時期から、データ窃取は数年前に行われたものと思われる。
37	2020/6/10	外部組織からの連絡により、届出者（企業）が運営するサイトに不正アクセスがあり、利用者の情報が流出した恐れがあることが発覚した。調査したところ、過去に運用されていたデータベースへの障害対応用のアクセス経路に問題があったことが判明し、そこが悪用されたと推測される状況であった。サイトの利用者に対して、パスワードの変更を推奨する通知を行った。
38	2020/6/30	届出者（企業）の社内サーバに対して不正アクセスがあり、一部の情報が流出した恐れがあることを発見した。調査したところ、新システムに移行済みで廃止予定だったネットワーク・サーバ環境のセキュリティ対策が一部更新されておらず、脆弱な箇所が存在することが判明し、そこが攻撃者に侵入経路として悪用されたものと推測される状況であった。
その他		
39	2020/1/30	届出者（企業）が使用している SSL VPN 装置のログ調査を行ったところ、当該機器の脆弱性を悪用した攻撃の形跡を発見した。詳細な調査により、別のセキュリティ機器の防御機能により攻撃は失敗していたことが判明した。
40	2020/2/18	外部 SOC からの連絡で調査を行ったところ、届出者（企業）のサーバにおける不審な挙動を確認した。その後の詳細な調査により、攻撃者が SSL VPN 装置の脆弱性を突いて社内サーバに侵入し、ユーザ情報やコンピュータ名を調査するプログラムの配置や、イベントログの削除などの行動を行ったことが判明した。

項番	届出日	概要
41	2020/3/19	外部組織からの連絡により、届出者（企業）のシステムから、外部のサーバに対してブルートフォース攻撃が行われていることを確認した。外部向けの通信を遮断した上で調査を実施したが、特に問題は発見されなかった。再発防止のために、全ての端末のシステム再インストールを実施し、更に外部アクセス時のログ取得と保全環境を整備した。
42	2020/5/27	届出者（公共機関）のウェブサイトから大量の不正なメールが送信されていることを発見した。攻撃者は、届出者のウェブサイトの問い合わせフォームに入力を行うと、問い合わせ者のメールアドレス宛に、問い合わせ内容が記載された自動返信のメールが送信されることを悪用して、問い合わせ者の氏名に、不正なサイトの URL を記載することで、不正なメールを大量に送信していた。 **※本事例は 5 章で紹介する。**
43	2020/6/1	届出者（企業）の名前を騙ったなりすましメールの存在を確認したため、注意喚起をウェブサイトに掲載した。なりすましメールには、実際の会社ロゴや所在地の情報、実在する役職員の氏名が記載された、精巧な作りの契約書のようなファイルが添付されていた。
44	2020/6/11	届出者（企業）のメールアドレス宛に、なりすましのメールが着信した。なりすましメールの内容は、差出人名には届出者のメールアドレスが表示されるように偽装され、件名や本文にてサービス停止の恐れがあると騙り、本文に記載された届出者とは無関係の URL へ誘導する内容であった。
45	2020/6/16	届出者（企業）が提供するサービスのレスポンスが悪化していることを監視システムが検知した。調査したところ、届出者が利用するドメイン登録管理のサービスに不正アクセスがあり、ドメイン登録情報が改ざんされていることが発覚した。改ざんされていた期間、届出者宛に送信されたメールが攻撃者のメールサーバに配送され、窃取されていた可能性もあった。

項番	届出日	概要
46	2020/6/17	届出者（企業）が利用するドメイン登録管理のサービスに不正アクセスがあり、ドメイン登録情報が改ざんされていることを発見した。改ざんされたドメイン登録情報は届出者のサービス提供には使用していないドメインのものであったため、顧客への影響はなかった。

項番 6、20 および 42 については次章以降にて内容を詳しく紹介する。

なお、届出には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 2021 年 1 月に「届出状況」として公開する予定である。

2-1. 着目点

2020 年上半期で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多かった。また、組織の職員が簡単なパスワードを設定していたためにメールアカウントに不正にログインされ、社内外へのフィッシングメールの送信に悪用された事例など、まず組織に所属する個人が攻撃の対象となり、その後、組織全体へ影響を及ぼす被害に広がった事例や、自組織で管理運用するシステムが直接不正アクセスされたものでなく、利用する（依存している）他者のサービスが侵害されたことにより、被害を受けたという事例も見受けられた。

情報システムの運用や管理に携わる方々だけでなく、情報システム・サービスを利用する各個人についても、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に、まずは、利用しているシステムやサービスのセキュリティ設定を確認したり、パスワードに複雑なものを設定したり、フィッシング攻撃の被害に遭わないように注意するなど、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。

今期の届出を、表 2-1 に示した通り、大きく 6 種類の被害に分類した。続いて、これらについて補足する。

2-1-1. ウイルス感染の被害

依然として、利用しているパソコンがウイルス感染の被害に遭ったという事例が多く見受けられた。今期は、Emotet と呼ばれるウイルスに感染した事例と、ランサムウェアに感染した事例がそれぞれ複数あり、他にも遠隔操作ウイルス（RAT）と呼ばれる、感染パソコンを攻撃者が遠隔操作可能にするタイプのウイルスへの感染事例もあった。

また、ウェブブラウザにインストールしていた拡張機能が、ウイルスに変化したという事例もあった。この拡張機能は正規サイトからダウンロードしたものであり、インストール時点では有害な点は見受けられなかったが、自動アップデートが行われた際に、悪意のある者により、有害な動作を含む機能が追加されてしまったものである。ブラウザの拡張機能の信頼性の見極めは難しく、ウイルスの感染経路として注意が必要であろう。

Emotet は情報の窃取に加え、更に別のウイルスへ感染させるために悪用されるウイルスであり、最終的にどのような被害に繋がるか（どのようなウイルスに追加で感染させられるか）が様々であることが、対応を難しくしている。また、Emotet に感染させられると、メールの内容、アドレス帳、メールアカウント等が窃取される。攻撃者は、そうして得られた情報を基に、更に Emotet のウイルスメールをばら撒き、被害者を拡大させている。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確認していたが[6]、今期において 3 月以降はメールのばらまきは観測されておらず、Emotet 感染の届出もなかった。しかし、下半期に入った 7 月中旬より再び攻撃メールが出回っていることを確認しており、引き続き非常に警戒が必要である。

Emotet 感染の被害について、項番 6 の事例の詳細を 3 章で紹介する。

2-1-2. メールシステムの不正利用・アカウントへの不正アクセス

今期は、特にメールシステムが不正に利用されたり、メールアカウントへ不正アクセスされたりした事例が多く見受けられた。

原因の大半は、メールアカウントにアクセスするためのパスワードが窃取あるいは突破されたものであり、パスワードの使いまわしをしていたためにリスト型攻撃等により不正アクセスされたと思われるものや、フィッシングサイトにパスワードを入力してしまい詐取されたと思われるものなど、利用者個人の不注意により被害を受けたと考えられる事例も多かった。

中でも、近年普及が進んでいるクラウド型のメールサービスにおいて、アカウント情報が窃取され悪用された事例の届出が複数あり、注意が必要と考えられる。クラウド型のメールサービスは強固なセキュリティ設定が可能なものも多いが、ひとたび正規のアカウント情報が窃取されて悪用されてしまうと、却って攻撃の検知が困難になるケースもある。不正なログインの阻止は非常に重要な防御点の 1 つであるため、可能であればサービスログイン時の多要素認証の導入を含む、適切なセキュリティ設定をすることが重要であると考える。

クラウド型のメールサービスへの不正アクセス被害について、項番 20 の事例の詳細を 4 章で紹介する。

2-1-3. パスワードリスト型攻撃による不正ログイン

企業等が提供するウェブサイトに対して行われる、パスワードリスト型攻撃による不正ログインに分類した事例は、今期は比較的少なかった（メールサービスについては、2-1-2 項に分類している）。

パスワードリスト型攻撃（またはブルートフォース攻撃）でパスワード認証を突破しようとする攻撃に対しては、利用者とサービス提供者の双方での対策が重要である。利用者側はパスワードの使いまわしをしないことや ID 等から類推できない強固なパスワードを設定することが最低限求められる。また、パスワードに加えて、多要素での認証方式等が提供され

---

[6] 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

ている場合は、積極的に利用を検討していただきたい。

サービス提供者側のシステム的な施策としては、パスワード以外の認証方法の提供などで不正ログインを阻止する仕組みの提供に加え、多数のログイン試行など不審な挙動を検知する仕組みや、通常と異なるログインがあった場合に利用者へ通知する仕組みの導入などで、不正ログインがあった場合にすぐに検知し、対処できる仕組みを確立することも重要である。

2-1-4. ウェブサーバへの不正アクセス

ウェブサーバに対する不正アクセス被害のほとんどは、EC サイト構築用のソフトウェアに存在する脆弱性を悪用されて、SQL インジェクションなどの攻撃を受けたものや、CMS の脆弱性を悪用されてウェブページを改ざんされたものであった。

EC ソフトウェアや CMS の脆弱性を悪用された被害は以前から確認しているが、現在でも継続的に発生していることがうかがえる。悪用された脆弱性はソフトウェア製造元から修正版が提供されていたり、脆弱性の悪用を回避する方法が提示されていたりするなど、対策方法が明確になっているものがほとんどであったと思われる。脆弱性対策にはシステムの動作検証作業や、サービスの一時停止などコストや機会損失が生じるケースも考えられるため、一概に即時の対策を行うことが難しい場合もあるが、現在でも継続して攻撃が行われていること、および攻撃を受けたときの被害の影響等も考慮し、適切な脆弱性管理の計画を立て、対策を行っていっていただきたい。

2-1-5. アクセス制御不備・運用不備により攻撃を受けた事例

今期の届出においては、テスト用に構築していたデータベース、現在は利用されていないサーバやネットワークなど、第三者からアクセスされるべきでない環境が、アクセス制御の不備や、適切な運用がなされていなかったため、攻撃を受けた事例も目立った。

このような環境は、セキュリティの対策が後回しになっていたり、監視対象から外されていたりして侵入などの事象が発生しても検知できないケースもあるため、攻撃者の標的になりやすいと考えられる。どのような環境であれ、アクセス制限を含む適切なセキュリティ対策を行う必要があるが、特に外部公開しているシステムの更新や移行作業の際には、システムのライフサイクルの観点で、利用しなくなった旧環境の停止・廃棄までを管理することが重要である。止むを得ず旧環境を外部公開状態で並行稼働する必要がある場合などには、本番環境と同様のセキュリティ対策を継続的に行っていくことが不可欠である。

2-1-6. その他

その他には次のような被害事例があった。

（1）　製品の脆弱性の悪用により侵入された被害

ネットワーク機器などの製品に脆弱性があり、修正プログラムの適用作業前に外部からの侵入を受けた事例があった。脆弱性の問題に対しては、組織ごとの脆弱性管理の方針に基づき対策していくことが重要であるが、とりわけ外部からの侵入など、影響の大きな被害につながる恐れのある箇所の脆弱性対策は速やかに実施することを勧める。一方で、セキュリティ機器の防御機能により攻撃が失敗し、直接の被害を受けなかった事例もあった。複数のセキュリティ対策を組み合わせることによってセキュリティを高める、いわゆる多層防御の導入も有効であると考えられる。

（2）　自組織のドメイン登録情報を改ざんされた被害

自組織が利用するドメイン登録管理サービスへ不正アクセスが行われ、自組織のドメイン登録情報を改ざんされた被害に遭った事例があった。ドメイン登録情報とは、ウェブサイトの URL やメールアドレスに含まれる組織を表す文字列と、実際のサーバ等の所在地である IP アドレスを結びつけるための重要な情報である。

今回の届出事例では、届出者は定期的な監視により一部のサービスレスポンスの低下を検知したことで、異常に気付くことができた。ただ、このような攻撃は、検知が非常に難しい可能性がある。自組織の重要な事業やサービスが、他者が提供するサービス等に依存している場合、そこで何らかの障害や想定外の問題が発生する可能性を考慮し、正常性の監視や問題発生時の対応策を用意しておく必要がある。

（3）　問い合わせフォームの自動返信機能を悪用された被害

届出者が、利用者からの意見や問い合わせを受け付けるために、ウェブサイトに設置していた問い合わせフォームを悪用され、届出者の名前で迷惑メールがばらまかれるという事例があった。本件は技術的には不正アクセス行為と呼ぶものではないが、参考として、項番 42 の事例の詳細を 5 章で紹介する。

3. 事例：「Emotet」と呼ばれるウイルスの感染被害

3-1. 届出内容

（1）　発見経緯

セキュリティソフトの警告により、パソコンがウイルスに感染していることに気づいた。

（2）　被害内容

- 組織内の複数台のパソコンが Emotet に感染した。
- 更に、組織内や組織外の取引先等に、Emotet への感染を狙う攻撃メールがばらまかれた。
- ばらまかれた攻撃メールには、感染したパソコンに保存されていたメールアドレスやメール本文が含まれていたため、これらに記載されていた個人名やメールアドレスなどの情報が流出した。

（3）　被害原因

従業員が、取引先を装ったなりすましメールの添付ファイル（Word 文書ファイル）を開いたことによりパソコンが Emotet に感染した。また、感染した端末から更に組織内外へ Emotet 感染を狙う攻撃メールが送信された。攻撃メールを受信した別の従業員が同様に添付ファイルを開いたことにより、組織内の複数台のパソコンに感染が拡大した。

（4）　被害対応

- セキュリティソフトによるウイルスの駆除。一部の機器については初期化を実施。
- 個人情報が流出した恐れのある相手に、お詫びと、なりすましメールに対する注意喚起の連絡。

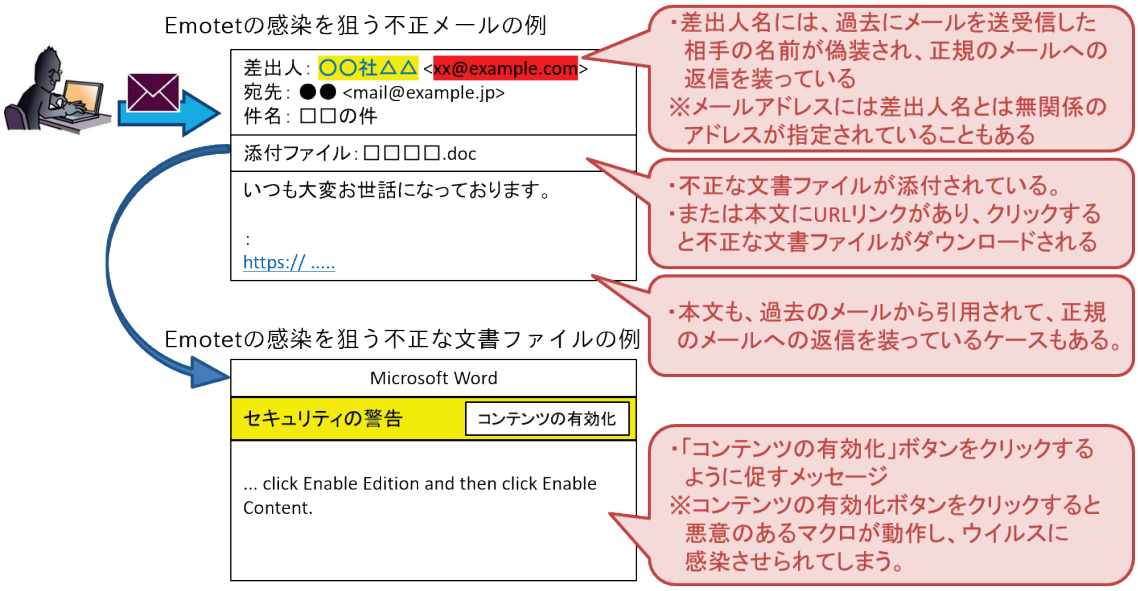

図 3-1 Emotet 感染を狙う不正メール・文書ファイルの例

3-2. 着目点

（1） 組織を横断する感染拡大

本事例で、この組織が最初に受信したと思われるウイルスメールは「取引先とのメールへの返信を装ったなりすましメール」であった。すなわち、取引先が先に Emotet に感染したことが、この組織への攻撃の契機となっている。そして、この組織（のパソコン）も Emotet に感染し、感染が社内に広がったとともに、社外の別の組織への攻撃の契機ともなったと思われる。

2019 年末頃から 2020 年初頭にかけて、多くの企業から Emotet の被害が公表・報告されていたが、この事例はその一端を示すものである。この時期、ある企業が Emotet に感染し、その取引先へ詐称メールが送信され、更にその企業が感染し、という悪循環が繰り返されてしまっていたと考えられる。

この時期に観測されていた Emotet の感染を狙う攻撃メールのうち、特に危険であった「正規メールの返信を装う手口」の特徴を図 3-1 に示す。この手口では、受信者（攻撃対象）は攻撃メールの差出人名や引用されている本文に身に覚えがあることから、正規の相手から送信されたものと思い込み、警戒することなく添付ファイルを開いてしまう。これが被害拡大の要因の 1 つだと思われる。今後も Emotet に限らず、類似する攻撃が継続することが懸念されるため、「送信元や本文に身に覚えがある、返信メールのような形態であったとしても、攻撃（ウイルスメール）の可能性がある」ことを念頭に置く必要がある。

また、返信を装うものではないが、Emotet の感染を狙う攻撃メールに関して、2019 年 12 月には賞与支給について、2020 年 1 月下旬からは新型コロナウイルスについて書かれた攻撃メールが確認されるなど、時節柄を踏まえて興味関心を惹く内容を日本語で記載す

る等で、受信者が一見して不審と判断できず、正規のメールと思い込ませるような工夫がされているものも確認している。

（2）　Word 文書ファイルのマクロの悪用

本事例では、攻撃メールに添付されていた Word 文書ファイルを開いたことが Emotet の感染につながった。

把握できている限り、Emotet の感染事例では、攻撃メールに添付されている、もしくは攻撃メールに記載された URL のリンク先からダウンロードされる Word 文書ファイルに仕掛けられたマクロ機能によって、Emotet に感染する仕掛けとなっていた。Microsoft Office の設定を変更していない限り、Word 文書ファイルを開いただけではマクロ機能は動作しないため、Emotet には感染しない。感染に至った事例では、Word 文書ファイルを開いた際に「編集を有効にする」「コンテンツの有効化」のボタンをクリックして、マクロ機能を有効にしてしまったものと思われる。

入手したファイルが信用できるもの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」というボタンはクリックしないことが重要である。1 台のパソコンの Emotet への感染であっても、組織内外へ大きな被害をもたらす可能性があることを、利用者に周知徹底する必要がある。

4. 事例：クラウド型メールサービスのアカウントへの不正アクセス

4-1. 届出内容

（1）　発見経緯

従業員（以下、一次被害者）が、自組織が利用するクラウド型メールサービスにおける自身のメールアカウントからフィッシングメールが送信されていることに、フィッシングメールの受信者（二次被害者）からの連絡で気づき、システム管理部門に報告した。

（2）　被害内容

一次被害者のアカウントへのログイン情報（ID、パスワード）が詐取され、不正にログインされたことにより、次の被害が発生した。

- 一次被害者が過去に送受信していたメールの内容を盗み見られ、顧客や取引先のメールアドレスが流出し、フィッシングメールの送信先に使用された。
- 一次被害者を差出人とした 1,000 件以上のフィッシングメールが組織内外へ発信された（二次被害者への攻撃）。

（3）　被害原因

一次被害者が、その関係者から届いたフィッシングメールに記載されていた URL のリンク先にアクセスし、フィッシングサイトへ誘導され、ID やパスワードを入力してしまったため、アカウント情報が詐取された。

（4）　被害対応

- 一次被害者のログインパスワードを強制変更。
- 個人情報が流出した恐れのある相手に、お詫びとフィッシングメールに対する注意喚起の連絡。
- 多要素認証の導入検討。

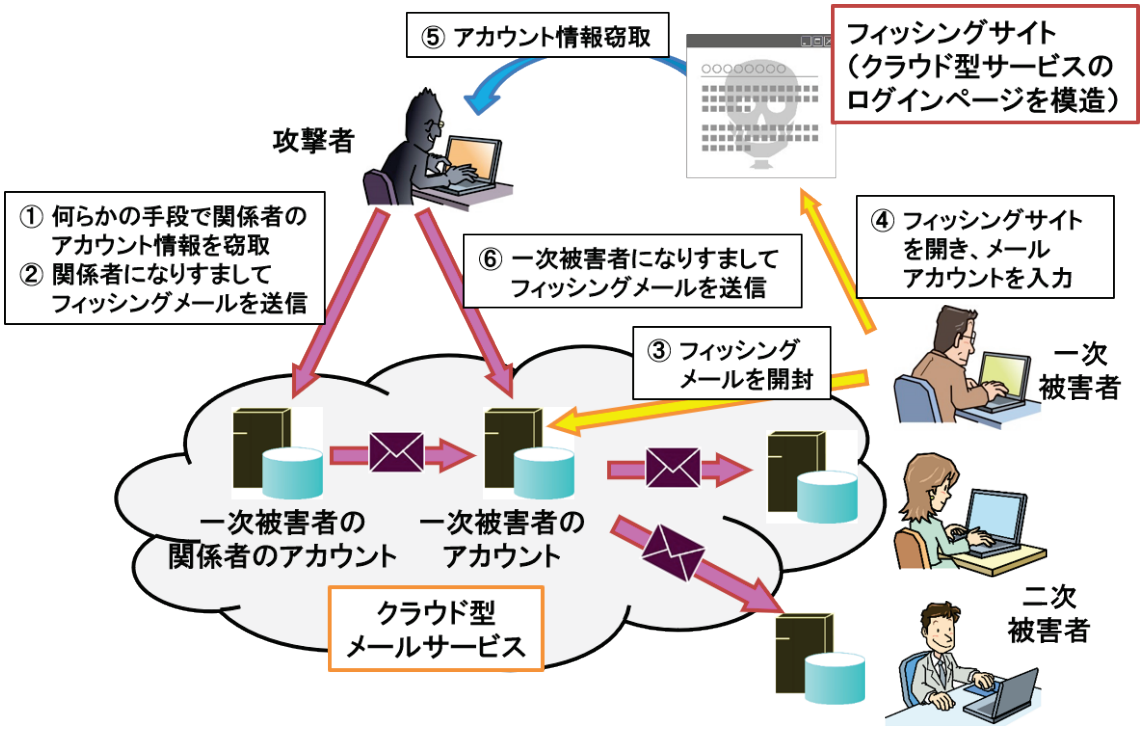

図 4-1 フィッシング攻撃の流れ

4-2. 着目点

（1） クラウド型サービスのサイトや通知メールを装うフィッシング

本事例では、攻撃者は事前に、一次被害者の関係者のアカウント情報の窃取を行っていたと思われ、フィッシングメールは、不正にログインしたアカウントから送信されていた。更に、フィッシングメールの内容は、このクラウド型サービスのファイルサーバに関するファイル更新通知を装い、フィッシングサイトへ誘導するものであった。

クラウド型の統合サービスは普及が進んでおり、一般的なログイン画面や通知メールの様式が広く知られている。このため、組織固有のシステムの場合と比較して、攻撃者がフィッシングサイトやメールを模倣することが容易であると考えられる。今後も同様の攻撃は継続して行われる可能性が高く、注意が必要である。

クラウド型サービスでは、通知メールに書かれた URL のリンク先で認証を求められることも多いため、フィッシング攻撃によりアカウント情報が詐取される可能性は常に存在する。メール等に書かれた URL をクリックする前や、ログインページに ID やパスワードを入力する際に URL を確認すること等を利用者に啓発することがリスクの低減にはなるが、十分とは言えない。アカウントが乗っ取られる事例は他にも非常に多くあるため、後述するように多要素認証の導入等が重要な役目を果たすと考える。

（2）　詐取したアカウントから組織内に攻撃を拡大する「ラテラルフィッシング」

本事例では、最初にログイン情報を窃取された一次被害者のアカウントから、社内外へフィッシングメールがばらまかれた。こうして二次被害者も騙し、攻撃者はより多くのアカウント情報を詐取することで、情報窃取や乗っ取りの範囲の拡大（ラテラルフィッシング）が試みられたものとみられる。

クラウド型のサービスは、不正アクセスされてしまうと、過去に送受信したメール、アカウントに登録した連絡先（アドレス帳）の情報に加え、ファイルサーバを提供しているサービスであれば、個人で保有しているファイルや組織で共有されているファイルまで盗み見される恐れがある。

本事例では、一次被害者が普段からメールのやり取りを行っていたアドレスへフィッシングメールが送られており、メールデータの履歴が悪用されている。攻撃者に乗っ取られたアカウントから送信されたメールは、送信者の名前やメールアドレス、送信経路といった情報は正規のものであるため、偽のメールと見破ることが難しくなる。システム管理部門は、正規のアカウントを使った悪意のあるメールが組織内に出回り、連鎖的に被害に遭う状況があり得るという点を認識しておく必要がある。

アカウントの乗っ取りを防止する対策も重要である。各利用者が強固なパスワードを設定することはもちろんのこと、システム管理部門においては、ID とパスワードが詐取・窃取された場合に備え、クラウド型サービスが提供する各認証方式の特徴を踏まえ、組織に合った認証方式を加えた多要素認証の導入も検討いただきたい。更に、多数のログイン試行や、通常と異なるログインがあった場合など、不審な挙動を検知する仕組みの導入によって、万が一不正アクセスされてしまった場合でも、すみやかに対処できるよう備えておくことも効果があると思われる。

5. 事例：問い合わせフォームの自動返信機能の悪用

5-1. 届出内容

（1）　発見経緯

届出者が外部に公開していたウェブサイトには問い合わせフォームが存在し、問い合わせフォームに意見等を投稿すると、投稿者へ自動的に受付のメールが返信される機能があった。ウェブサイト管理業者が、この自動返信メールが異常なほど大量に送信されていることに気づき、届出者に連絡した。

（2）　被害内容

- 自動返信の機能を悪用され、フィッシングサイトと思われる URL が記載された不正なメールが 10 万件以上送信された。
- 大量の不正なメールが送信されたことにより、届出者のメールサーバが公開ブロックリストに登録されてしまい、当該サーバからの正規の業務メールの送信に支障が生じた（当該公開ブロックリストを採用している組織へのメールがブロックされてしまうようになった）。

（3）　被害原因

問い合わせフォームの投稿者氏名欄に入力された情報について、そのまま自動返信メールに記載して投稿者へ送信する仕様となっていたため、攻撃者に悪用された。投稿者氏名欄に不正サイトの URL、メールアドレス欄に不特定多数のメールアドレスが入力され、不正な URL が書かれたメールを大量に送信させられた。

（4）　被害対応

- 投稿者の氏名の情報を自動返信メールに記載しないように変更。
- 不正メールの発信に関するお詫びと注意喚起の掲載。
- 不正メールに関する公開ブロックリストの管理者へ、登録解除の手続きを実施。
- 機械的な動作による投稿を抑止する機能の導入検討。

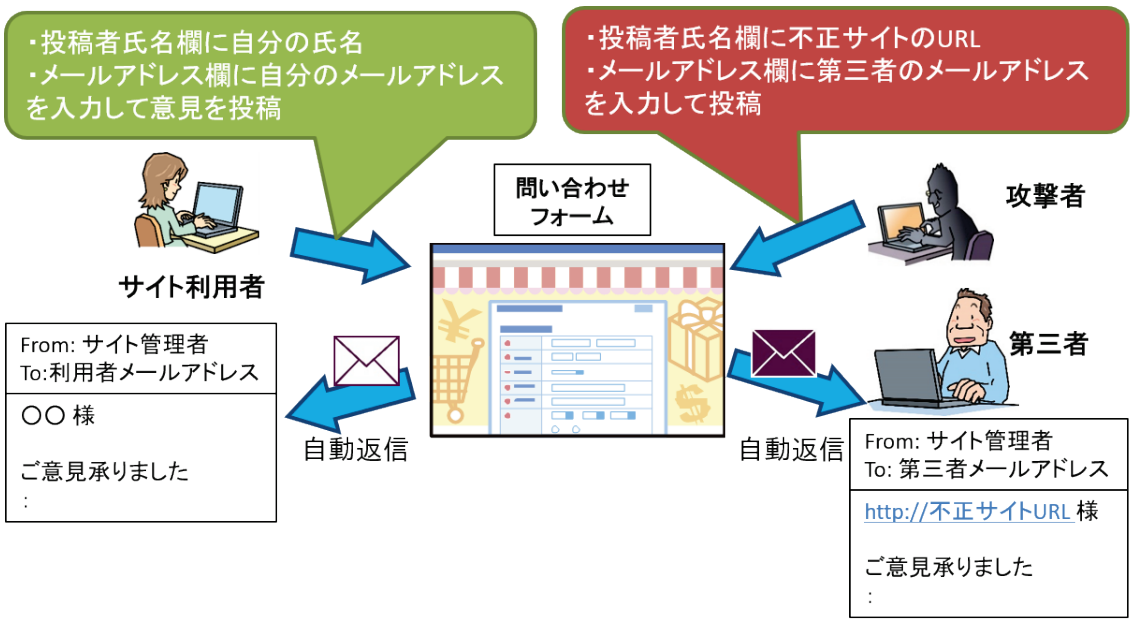

図 5-1 本事例の概要

5-2. 着目点

（1） 自動返信機能の悪用

本事例は、ウェブサイト上の問い合わせフォームにおけるメールの自動返信機能が攻撃者に悪用されたものであった。

問い合わせフォームには、返信先として問い合わせ者の名前やメールアドレスの記入欄を設けるのが一般的で、問い合わせ等が投稿されると、受け付けた旨を伝えるメールが自動的に問い合わせ者に送信されるようにしているものも多い。

自動返信されるメールは、ウェブサイトの管理者が設置したメールシステムから送信されるため、差出人は当該組織（国内の正規のドメイン）となる。本事例では、メール本文の冒頭に問い合わせ者の名前（正確には、問い合わせ者が「投稿者氏名」の欄に入力した文字列）を記載して送信するようにしていた。攻撃者は、問い合わせ者の「投稿者氏名」としてフィッシングサイトの URL を入力することで、メールの冒頭に当該 URL が存在するようなフィッシングメールを送信していた。

このような悪用を防止するため、機械的な動作による投稿を排除する仕組みの導入、自動返信するメールには投稿者が入力した文字列は含めないようにする、あるいは URL のような文字列は受け付けないといった対策が考えられる。

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）