コンピュータウイルス・不正アクセスの届出事例

［2019 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

2019 年 8 月 28 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

2019 年 1 月～6 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
1	2019/2/2	外部組織からの連絡により、届出者（企業）が運用するウェブサイトからのクレジットカード情報の漏えいが発覚。ウェブサーバを調査したところ、何者かによって EC サイトの決済画面が書き換えられ、入力されたクレジットカード情報が第三者に送信される状態となっていた。管理者アカウントのパスワード強度、アクセス制限が脆弱であったことが原因とみられる。 **※ 本事例は 3 章で紹介する。**
2	2019/2/18	外部組織からの連絡により、届出者（業界団体）が運用する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の漏えいが発覚。ウェブサーバで使用していたソフトウェアの脆弱性を悪用されたものと推測されるが、十分なログが残っておらず、原因の特定には至らなかった。
3	2019/3/1	利用者からの連絡により、届出者（地方自治体）が運用するウェブサイトの一部改ざんが発覚。当該ウェブサイトにアクセスするとフィッシング目的と見られる不審な別サイトにリダイレクトされる状態となっていた。原因は調査中（本紙執筆時点で続報無し）。
4	2019/3/14	届出者（企業）の内部システムにおいて、EDR 製品によるアラートが通知され、該当するパソコンのログを確認したところ、何者かによる管理者権限アカウントの不正利用と他のパソコンへのウイルス設置の試行が確認された。どのような手口で不正な操作が行われたかについて、原因は特定できなかった。

項番	届出日	概要
5	2019/3/25	届出者（企業）が運用するウェブサイトがブラウザで表示できない状況が発生。調査したところ、公開用ディレクトリのアクセス権限が意図せず変更されていた。また、不正プログラム（IPA が確認したところ、一般的に webshell と呼ばれる不正なファイルであった）の設置も確認された。ウェブサイトの公開を停止して 7 日間の調査を行った結果、データベースへの不正アクセスや改ざん等は確認されなかった。また、不正にウェブサーバへ侵入された原因の特定には至らなかった。対策として、全 FTP アカウントのパスワード変更、全 FTP アカウントの FTP プロトコルでのアクセス禁止（SCP でのアクセスに限定）、CMS 管理画面のアクセス URL の変更、CMS 管理用アカウントのパスワード変更および未使用アカウントの削除等を行った。
6	2019/4/7	届出者（個人）が使用している VPN サーバを定期点検したところ、海外の IP アドレスから不正なログイン試行の痕跡が確認された。試行されたアカウント名は admin、test、vpn といった、初期設定あるいはシステム構築時に使用されるアカウント名と見られる汎用的なものであったが、当該 VPN サーバでは第三者から特定されにくいアカウント名およびパスワードを設定していたため、被害は発生しなかった。
7	2019/4/18	届出者（企業）の内部のネットワーク負荷が高くなり、調査したところ、300 台を超えるパソコンおよびサーバ類でウイルス感染を確認した。原因を調査した結果、一時的にグローバル IP アドレスが付与された外部持出し用パソコンが感染源となり、組織内ネットワークへウイルスが拡散したことが判明した。 **※ 本事例は４章で紹介する。**

項番	届出日	概要
8	2019/4/19	届出者（教育機関）のサーバ死活監視で異常が見つかり、状況を確認したところ、サーバがランサムウェアに感染したことが発覚。組織内に提供しているメールサービスの一部機能が利用できなくなった。感染経路を確認したところ、当該サーバへのリモートデスクトップアクセスを許可していた業務委託先の作業パソコンを経由し、何者かが不正アクセスしていたことが判明した。 **※ 本事例は５章で紹介する。**
9	2019/4/24	届出者（企業）の IDS にて SQL インジェクション攻撃を検知。確認・調査したところ、公開ウェブサイトのシステム管理者向けログイン画面の脆弱性が悪用され、データベース内の顧客情報が窃取されていたことが判明した。システム管理者向けログイン画面は、本来企業内部からのみアクセスを許可する想定で、脆弱性対策が簡易的なものとなっていた。しかしその後、システムの利用状況が変わり、システム管理者向けのログイン画面に外部からもアクセスする必要が生じた。そのため、インターネットに公開することとなったが、その際に実施すべき本格的な脆弱性対策が実施されていなかった。
10	2019/5/13	外部組織からの連絡により、届出者（研究機関）が運用するウェブサイトの改ざんが発覚。フィッシングサイトにリダイレクトさせるページ改ざんが行われていた。原因を調査したところ、ウェブサイトの管理画面にアクセス制限が行われておらず、また、パスワードの強度が弱かったために不正アクセスされたことが判明した。
11	2019/5/16	外部組織からの連絡により、届出者（企業）が運用するウェブサイトの改ざんが発覚。フィッシングサイトにリダイレクトさせる改ざんが行われていた。原因を調査したところ、CMS のログインに関するアクセス制限の設定が脆弱であり、そこを悪用されて攻撃を受けていたことが判明した。

項番	届出日	概要
12	2019/5/24	ウェブサイトのホスティング会社からの連絡により、届出者（医療機関）が運用するウェブサイトに不正ファイル（ウイルス）がアップロードされていたことが発覚。その後に行ったウェブサイト復旧作業の中でログなどが消失してしまったため、不正アクセスの原因は特定できなかった。しかし、CMS プラグインのバージョンが古かったことから、そこに存在した脆弱性を悪用されたのではないかと見られる。

項番 1、7 および 8 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 2020 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

表 2-1 に示した被害の多くは、一部推測も含まれるが、修正プログラムの適用やアクセス制限などの基本的な対策を行っていれば防げた可能性が高いものであった。

それでも、基本的な対策が行われず、一部被害まで生じている背景には、人手や時間がないといった運用面の不備によって対策の着手が遅れたり、放置されたりしてしまう状況があることが考えられる。対策を着実に実行するためには、事業計画やシステム構築の検討段階から、セキュリティに関する運用面の設計や計画を行う必要がある。また、すでに運用中のシステムにおいて、事前の計画が十分でなかったとしても、万が一被害が発生した際の損害を想定し、必要な人員確保や運用の見直しを行っていただきたい。

古くから知られている、あるいは過去に流行した攻撃手口が世間で話題にならなくなったからと言って、必ずしも同様の攻撃が無くなっているわけではない。攻撃者らは日々世界中のネットワークをスキャンして、悪用できる脆弱性を見つければ攻撃してくる。すでに知られた攻撃手口での被害は確実に防止すべく、基本的な対策はしっかりと行うべきである。

3. 事例：EC サイト決済画面書き換えによるクレジットカード情報窃取

3-1. 届出内容

（1）　発見経緯

外部組織から、届出者（企業）が運営する EC サイトで情報漏えいが発生している模様との連絡があった。

（2）　被害内容

・顧客のクレジットカード情報が数百件窃取された。
・顧客の個人情報が数千件窃取された可能性がある。

（3）　被害原因

当該 EC サイトは本番環境のほかにバックアップサイトがあり、同一サーバ上に構築されていた。

セキュリティ会社によるフォレンジック調査により、バックアップサイトの管理者アカウントのパスワード強度およびアクセス制限が脆弱であったために不正侵入されていたことが判明した。また、バックアップサイトから本番環境へのアクセスが可能であったため、本番環境のウェブページ書き換えが発生していたことも判明した。

ウェブページの書き換えにより、クレジットカード決済画面が偽の外部ページに遷移する状態となり、偽のページに顧客が入力した情報が窃取されることとなった。

（4）　被害対応

・EC サイト閉鎖
・セキュリティ会社によるフォレンジック調査
・関係各所への報告

（5）　その他事項

被害発覚の契機となった外部組織からの連絡の前にも、顧客から「クレジットカード情報を 2 回入力したが異常はないか」との連絡を受けていたが、ウェブサイト運営委託先業者は顧客パソコンのセキュリティソフトの不具合などではないかと考えたため、攻撃に気付けなかった。

3-2. 着目点

本事例で、IPA が特に着目した点を次に示す。

（1）　「脆弱なバックアップサイト」の存在

本事例では、バックアップサイトがインターネット上の第三者からアクセス可能な状態で存在していた。そして、パスワードが脆弱な状態であり、バックアップサイトから本番サイトへのアクセスも可能となっていたために攻撃を受けている。

ソフトウェア等のアップデート時の確認・テストや、本番環境の不具合に備えてバックアップサイトを設置することは一般的であるが、その場合、バックアップサイトのセキュリティも十分に担保する必要がある。また、やむをえず、バックアップサイトと本番サイトが同一サーバ上に存在する場合、サイバー攻撃を原因としたものに限らず、悪影響が相互に発生しうるため、環境や権限の分離等に注意する必要がある。

（2）　EC サイトへの新たな攻撃手口

本事例と同様に、クレジットカード情報を入力する際に偽の決済画面を表示させる手口は特に 2018 年頃から確認され始めている [6]。

このような手口では、偽の決済画面で顧客が情報を入力した後、情報に誤りがあるなどといったエラー表示をした後に正規の決済画面を表示させ、顧客に正規の決済も行わせることで、攻撃の発覚を回避しようとする。

本来不要と思われる状況で「クレジットカード情報を 2 回入力した」といった報告があった場合は、単なる利用者の入力ミスだけでなく、本事例のような手口の攻撃が行われている可能性も考慮していただきたい。また、ウェブサイトの改ざん検知の仕組み等を導入することも有効である。

---

[6] 「徳丸浩の日記　EC サイトからクレジットカード情報を盗み出す新たな手口」
https://blog.tokumaru.org/2018/10/ec.html

4. 事例：グローバル IP アドレスが付与されたパソコンからのワーム感染拡大

4-1. 届出内容

（1）　発見経緯

組織内のネットワーク負荷が高くなり、システム保守要員が調査したところ、複数のパソコンおよびサーバでのウイルス感染が確認された。

（2）　被害内容

ウイルスがワーム型であったため、組織内のネットワークに拡散した。セキュリティソフトの定義ファイルが更新されるまで、ネットワーク内のパソコンおよびサーバ約 300 台に感染を繰り返した。

（3）　被害原因

SIM 内蔵の外部持ち出し用モバイルパソコンが、組織外において、インターネットへ接続する際にグローバル IP アドレスが付与され、一時的にインターネット上からアクセス可能な状態となった。この状態で、当該パソコンが SMB プロトコルによる総当たり攻撃を受け、管理者権限を持つアカウントを窃取されてウイルスに感染した。さらに、当該モバイルパソコンが VPN 経由で組織内ネットワークへ接続した際、ウイルスのワーム機能により組織内のサーバおよびパソコンに感染が拡大した。

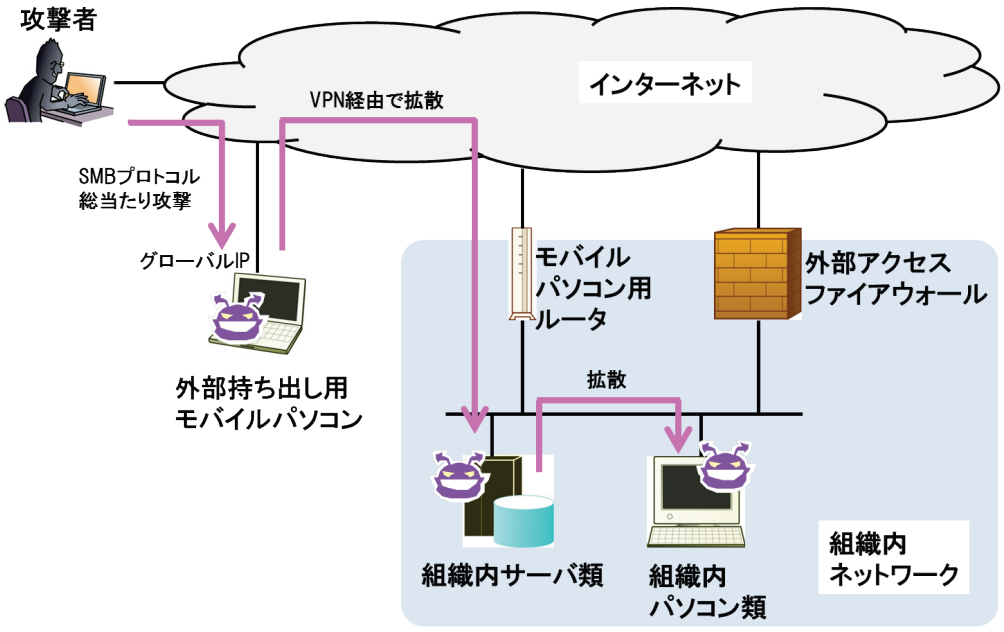

図 4-1 ウイルス感染拡大の様子

（4）　事後対策

外部持ち出し用モバイルパソコンの運用において、グローバル IP アドレスが付与されないモバイルルータの導入を検討。

4-2. 着目点

本事例で、IPA が特に着目した点を次に示す。

（1）　外部持ち出し用モバイルパソコンへのグローバル IP アドレスの付与

一般的に、企業等において、職員が外出先でも業務を行えるように持ち出し用のパソコンを用意することがある。そして、これらのパソコンで、メールの送受信や、VPN を使用した社内システムへのアクセスを可能とするため、インターネットへ接続できるように設定していることがある。

ここで、パソコンのインターネットへの接続の方式（使用する機器やプロバイダ等）によっては、グローバル IP アドレスが付与されるなどして、インターネットから直接、当該パソコンへ TCP/IP によるアクセスが可能な状態となる場合がある。その時、パソコンの設定等によっては不正アクセスを受けるリスクが生じる。本事例はこのリスクが顕在化したものであり、複数のセキュリティ関係機関からも本件と同様の事例が報告されている[7,8,9]ことから、注意を要する事象であることが分かる。

パソコンにグローバル IP アドレスが付与される場合であっても、セキュアな設定（脆弱性の解消、パーソナルファイアウォールの設定等）を適切に実施できていれば、被害を受ける可能性を十分に低減できる。一方、そもそも「グローバル IP アドレスが付与される可能性」が想定されていないケースも考えられるため、いま一度、持ち出し用パソコンのインターネット接続方式について確認いただきたい。

また、いずれにせよ、持ち出し用パソコンについては、その利用者によりシステム管理部門等の想定外の方法で使用される可能性があり（例えば、信頼できない公衆無線 LAN などに接続して第三者からアクセス可能な状況となってしまうなど）、できる限り、上述のような不正アクセス対策を講じておくことが望ましい。

---

[7] Secureworks 「日本国内でモバイルデータ通信端末経由のマルウェア感染事案が増加」
https://www.secureworks.jp/resources/at-portable-connection-devices-spreading-malware

[8] JC3 「グローバル IP アドレスを直接割り当てられた PC のセキュリティ対策について」
https://www.jc3.or.jp/topics/gip_sec.html

[9] JPCERT/CC 「インターネット経由の攻撃を受ける可能性のある PC やサーバに関する注意喚起」
https://www.jpcert.or.jp/at/2017/at170023.html

（2）　組織内ネットワークでのウイルス感染拡大

本事例において、組織内ネットワークでの感染拡大については、詳細な原因は把握できていない。ローカルの管理者アカウントのパスワードがサーバや他のパソコンと共通であったか、サーバや他のパソコンに対しても SMB プロトコルによる総当たり攻撃が可能であったという原因が考えられる。

ワーム機能を持ったウイルスの感染拡大防止策としては、ネットワークセグメントの分割、端末間・セグメント間での不要な通信の遮断、認証の試行回数の制限、各サーバやパソコンで使用するローカル管理者アカウントの認証情報をそれぞれ異なるものに設定するといった対策が考えられる。また、持ち出し用パソコンからの侵入を防止するという観点では、持ち出し用パソコンからの組織内ネットワークへアクセス可能な範囲を最低限度に制限するといった対策も考えられる。

5. 事例：業務委託先を経由したランサムウェア感染

5-1. 届出内容

（1）　発見経緯

組織内のサーバが Ping に応答しなかったため確認を行ったところ、ランサムウェア被害を発見した。

（2）　被害内容

組織内で使用するサーバ上のデータが暗号化されてしまったことにより、組織内に提供しているメールサービスの一部機能が利用できなくなった。

（3）　被害原因

被害にあったサーバではメールサービスシステムを運用しており、システムの構築・運用はベンダに委託していた。

当該サーバは、委託先ベンダからのリモートデスクトップ（RDP プロトコル）によるアクセスを許可しており、ベンダは、ベンダ社内パソコンから遠隔で管理していた。サーバ側では、接続元 IP アドレスによるアクセス制限を設定しており、ベンダの社内ネットワーク以外からのアクセスは行えないようにしていた。

一方、ベンダはサーバの運用管理にベンダ社内パソコンを使用していたものの、業務都合により担当者が社外にいることが多々あったため、社外からベンダ社内パソコンへのリモートデスクトップ（RDP プロトコル）操作を可能としていた（図 5-1）。

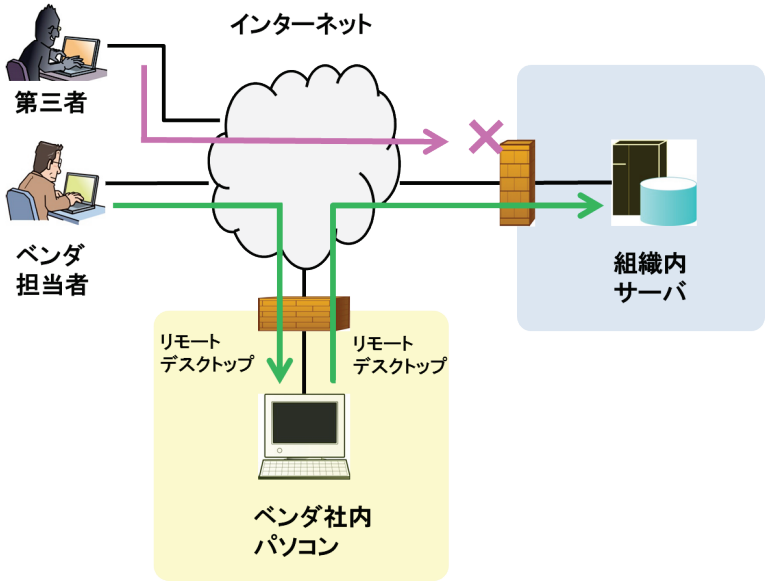

図 5-1 ネットワーク概略図

社外からベンダ社内パソコンへのリモートデスクトップ接続については、固定 IP アドレスを持たない環境からのアクセスを前提としていたため、接続元 IP アドレスによるアクセス制限は行っていなかった。したがって、ベンダ社内パソコンはインターネット上の第三者からのアクセス試行が可能な状態であり、今回、攻撃者による総当たり攻撃により、不正アクセスされることとなった。さらに、ベンダ社内パソコンから組織内サーバに対してもリモートデスクトップにより侵入され、ランサムウェアを感染させられることとなった（図 5-2）。

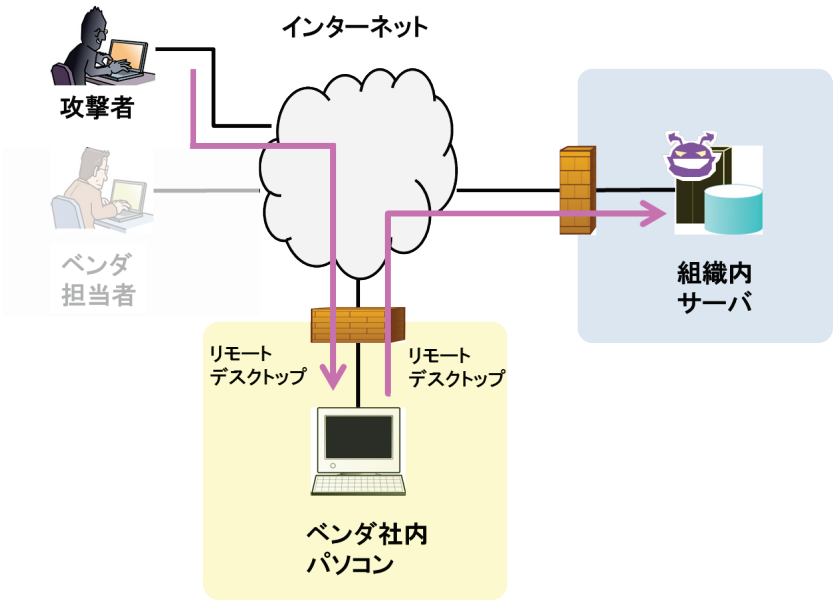

図 5-2 不正アクセスの様子

（4）　被害対応・事後対策

・ランサムウェアに感染したサーバは完全停止させ、新たなサーバによるシステム構築を行った。

・同様の委託を行っているベンダに調査と社内で注意喚起を行うよう指示をした。

・組織内にとどまらず、委託先のセキュリティ環境の事前調査を厳格にするとともに、委託先への啓発についても定期的に行うこととした。

5-2. 着目点

本事例で、IPA が特に着目した点を次に示す。

（1）　脆弱なアクセス制限でのリモートデスクトップの運用

本事例でランサムウェア感染を許してしまった根本の原因は、委託先ベンダの社内パソコンに対するリモートデスクトップのアクセス制限が不適切だったことである。リモートデスクトップで攻撃者に侵入されると、情報窃取や破壊、別の攻撃の踏み台にされる等、あらゆる被害に繋がる恐れがある。

リモートデスクトップに限ったことではないが、リモートアクセスは必要最小限のアクセスのみに制限する必要がある。さらに、リモートデスクトップについては、不正アクセスされた場合の影響が大きく、リモートデスクトップの要否自体についても十分検討する必要がある。いずれにせよ、強固な認証やアクセス制限を行う、認証試行回数に制限を設けるといった方法で、総当たり攻撃をはじめとする不正アクセスへの複合的な対策を併せて実施すべきである。

（2）　サプライチェーンによるリスク

本事例では、届出者自身はリモートデスクトップのアクセスについて、接続元 IP アドレスによる制限での対策を実施していたが、委託先ベンダのセキュリティが脆弱であったため、被害を受けてしまった。

このような問題は、一般的にサプライチェーンによるリスク [10]と呼ばれる。解決が非常に難しい問題ではあるが、このようなリスクに対応するためには、業務委託先にも十分な対策を求める必要がある。そのためには、委託元組織と委託先組織の情報セキュリティ上の責任範囲を明確化し、合意を得ておくことが重要となる。また、委託元組織が責任をもって委託先組織の対策状況の実態を定期的に確認することも重要となる。

---

[10] 製造における部品等の供給関係でのサプライチェーンに加え、業務で使用するソフトウェアやサービス等も含めて、サプライチェーンが構成されている。IPA の情報セキュリティ 10 大脅威では、組織向け脅威の第 4 位に挙げている。
IPA 「情報セキュリティ 10 大脅威 2019」
https://www.ipa.go.jp/security/vuln/10threats2019.html

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）