コンピュータウイルス・不正アクセスの届出状況

［2019 年（1 月～12 月）］

本資料では、2019 年 1 月 1 日から 2019 年 12 月 31 日までの間にセキュリティセンターで受理した、コンピュータウイルスと不正アクセスに関する届出状況を報告する。

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. コンピュータウイルス届出状況

2019 年の 1 月から 12 月のコンピュータウイルス届出状況について示す。

近年、コンピュータウイルス（ここでは、マルウェア／不正プログラムと呼ばれる、利用者にとって期待しない動作をする、より広い意味での不正なソフトウェア全般を含む）が多様化するとともに、無数の亜種が存在することにより、発見された個々のウイルスを分類したり、それを数えるといった方法での分析が不確実なものとなった。また、例えば、届出で報告される、セキュリティソフトでウイルスを検知した際に表示される名称（検知名）からは、それが何らか不正なソフトウェアであることまでは分かるが、ウイルスの種類を判別するには不十分な情報であることが多い。

これらの状況から、この 2019 年より、ウイルスの検知名を基にした分類を取りやめるなど、集計方法を次の通り変更している。

<ウイルス届出の集計方法の変更点>

	2018 年まで	2019 年以降
ウイルス届出件数	1 回の届出において、複数のウイルス（の検知名）が届出様式に記入されている場合、別々の届出（ウイルス種別ごとに 1 件）として集計。	複数のウイルス（の検知名）が届出様式に含まれる場合でも、届出 1 回につき 1 件として集計。
ウイルス等検出件数、および検出ウイルスの種類	特性により「ウイルス」と「不正プログラム」を別々に集計。また、各ベンダが命名した一般的な検知名を「ウイルスの種類」とし、一部個別に集計。	ウイルス／不正プログラム等は区別せず集計。ウイルスの種類（検知名）による集計は行わない。

1-1. ウイルス届出件数

1-1-1. 年別推移

2019 年に寄せられたウイルス届出の年間件数は 259 件であり、その中で、ウイルス感染被害があった届出は 18 件であった。主なウイルス被害の内訳は Emotet 感染被害 5 件、ランサムウェア感染被害 5 件であった。

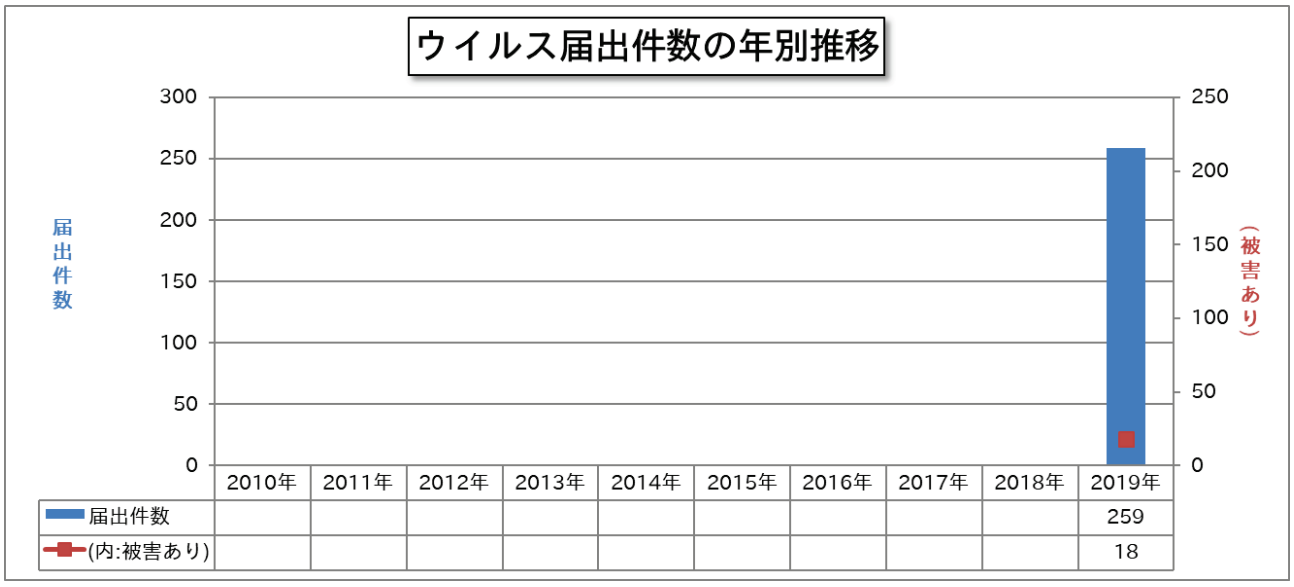
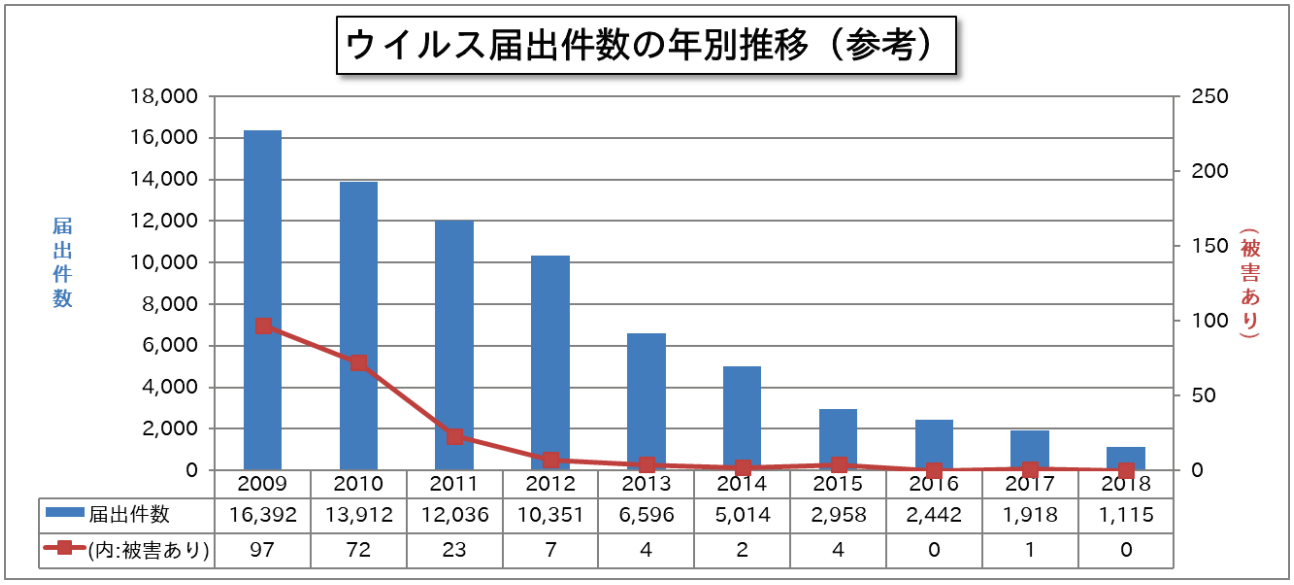


図 1-1：ウイルス届出件数の年別推移（2019 年以降）

参考として、2018 年以前のウイルス届出件数を図 1-2 に示す。

<参考：2018 年以前のウイルス届出件数>

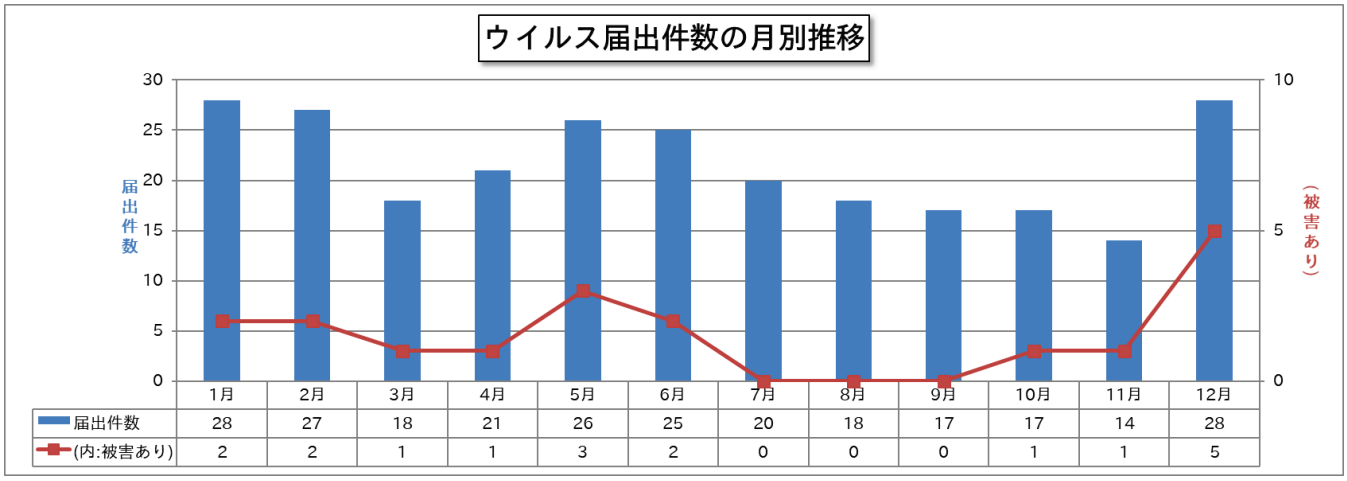


	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
届出件数	16,392	13,912	12,036	10,351	6,596	5,014	2,958	2,442	1,918	1,115
(内:被害あり)	97	72	23	7	4	2	4	0	1	0

図 1-2：ウイルス届出件数の年別推移（2018 年以前）

1-1-2. 月別推移

2019 年に寄せられたウイルス届出の月別件数は 1 月と 12 月が最も多く 28 件であった。また、被害件数は 12 月が最も多く 5 件であった。



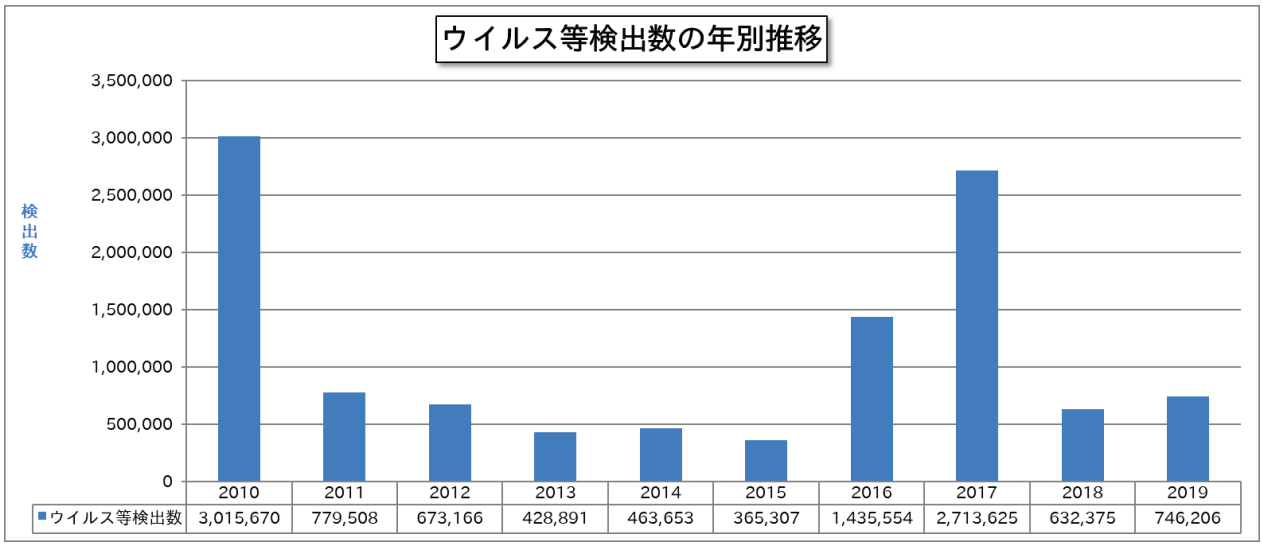
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
届出件数	28	27	18	21	26	25	20	18	17	17	14	28
(内:被害あり)	2	2	1	1	3	2	0	0	0	1	1	5

図 1-3：ウイルス届出件数の月別推移

1-2. ウイルス等検出件数

1-2-1. 年別推移

2019 年に寄せられたウイルス等検出数は、前年の 632,375 個より 113,831 個（約 18.0%）多い 746,206 個であった。



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
ウイルス等検出数	3,015,670	779,508	673,166	428,891	463,653	365,307	1,435,554	2,713,625	632,375	746,206

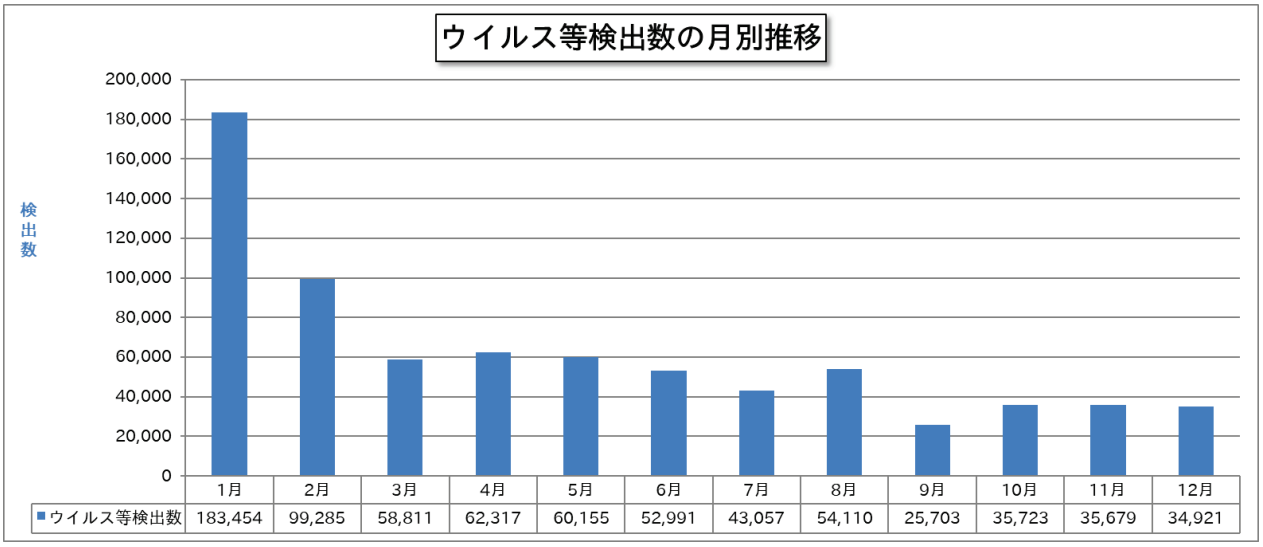
図 1-4：ウイルス届出件数の年別推移

1-2-2. 月別推移

2019 年の 1 月から 12 月に寄せられたウイルス等検出数は 1 月が最も多く 183,454 個であった。

1 月のウイルス等検出数の内訳は JS/Downloder が 135,771 個と最も多く、1 月の 74.0%を占めた。同様に 2 月においても、JS/Downloder が 51,884 個と最も多く、2 月の 52.3%を占めた。

JS/Downloader は JavaScript を利用し、Web サイトからウイルス等の不正なファイルをダウンロードして実行するウイルスである。キヤノン IT ソリューションズのレポート [1]によると、同種と思われるウイルスを添付したメールが 1 月から 2 月にかけて大量に出回ったとあり、届出による観測状況と一致している。



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
ウイルス等検出数	183,454	99,285	58,811	62,317	60,155	52,991	43,057	54,110	25,703	35,723	35,679	34,921

図 1-5：ウイルス等検出数の月別推移

[1] キヤノン IT ソリューションズ「2019 年 1 月・2 月 マルウェアレポート」
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1902.html

1-3. ウイルス届出者別件数

2019 年に寄せられたウイルス届出の届出者別件数は、「法人」が最も多く約 75%を占めた。

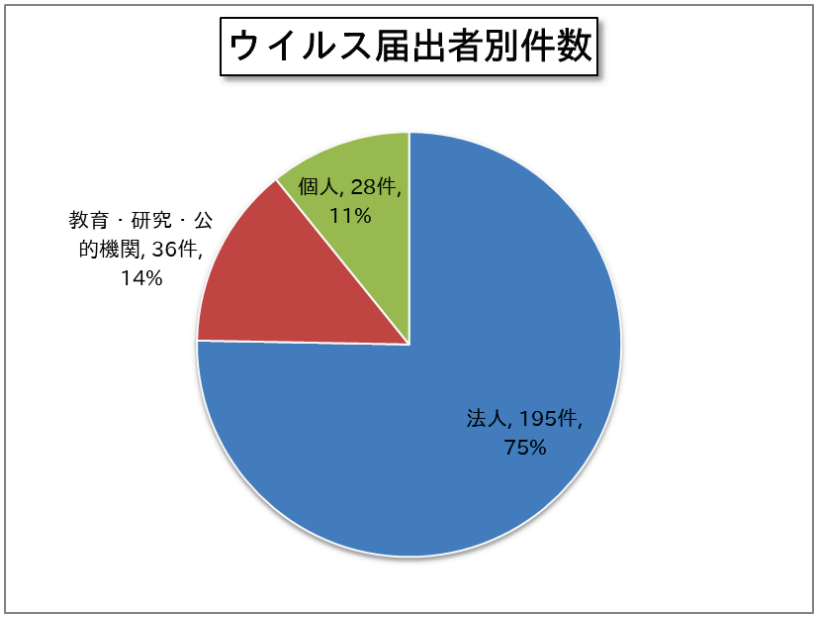


図 1-6：ウイルス届出者別件数（2019 年）

表 1-1：ウイルス届出者別件数

種別	2019 年
法人	195 件
教育・研究・公的機関	36 件
個人	28 件
合計	259 件

1-4. ウイルス届出にみられた傾向

2019 年では、10 月頃まで LokiBot と呼ばれるウイルスの検知情報が多く寄せられていたが、入れ替わるように 10 月頃から Emotet と呼ばれるウイルスの検知・感染被害の情報が寄せられるようになった。

なお、Emotet については 2019 年 1 月時点においても、検知・感染被害の情報が継続して寄せられている。

IPA では 2019 年 12 月に Emotet に関する情報の公開を行い、注意を呼び掛けている。Emotet に関する情報の周知と感染被害の拡大防止の観点から、ぜひ、下記ウェブサイトを参照していただきたい。

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

・コンピュータウイルスに関する届出制度について

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。

〇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）

〇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）

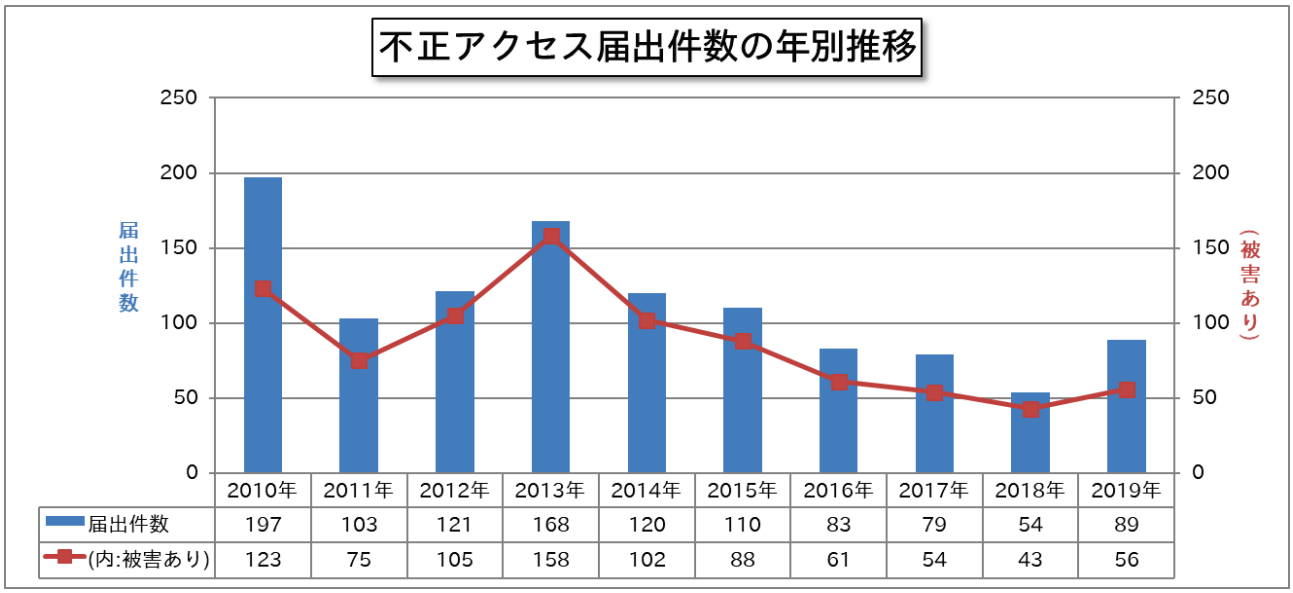
2. コンピュータ不正アクセス届出状況

2019 年の 1 月から 12 月の不正アクセス届出状況について示す。

2-1. 不正アクセス届出件数

2-1-1. 年別推移

2019 年に寄せられた不正アクセス届出件数の年間件数は、前年の 54 件より、35 件(約 64.8%)多い 89 件であった。そのうち、被害のあった届出は 56 件で全体の約 62.9%を占めた。

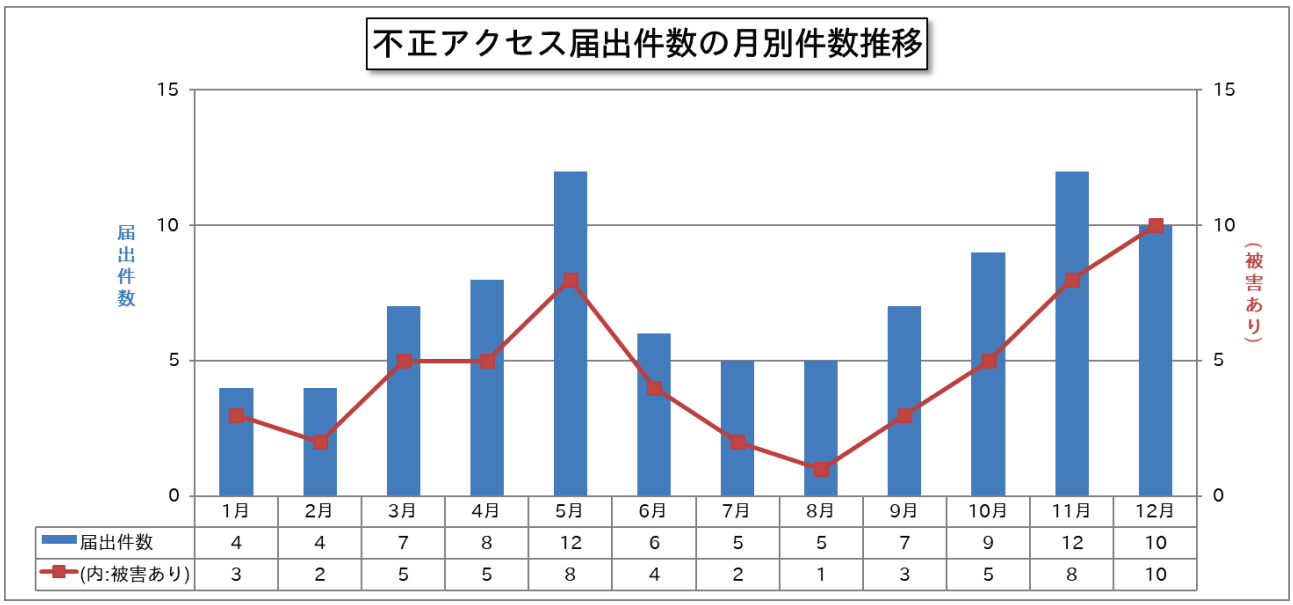


	2010年	2011年	2012年	2013年	2014年	2015年	2016年	2017年	2018年	2019年
届出件数	197	103	121	168	120	110	83	79	54	89
(内:被害あり)	123	75	105	158	102	88	61	54	43	56

図 2-1：不正アクセス届出件数の年別推移

2-1-2. 月別推移

不正アクセス届出の月別件数を示す。月により増減はあるが、毎月届出を受理している状況である。



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
届出件数	4	4	7	8	12	6	5	5	7	9	12	10
(内:被害あり)	3	2	5	5	8	4	2	1	3	5	8	10

図 2-2：不正アクセス届出件数の月別推移

2-2. 不正アクセス届出者別件数

2019 年に寄せられた不正アクセス届出の届出者別件数は、昨年と同様に「法人」が最も多く、約 55.1%を占めた。

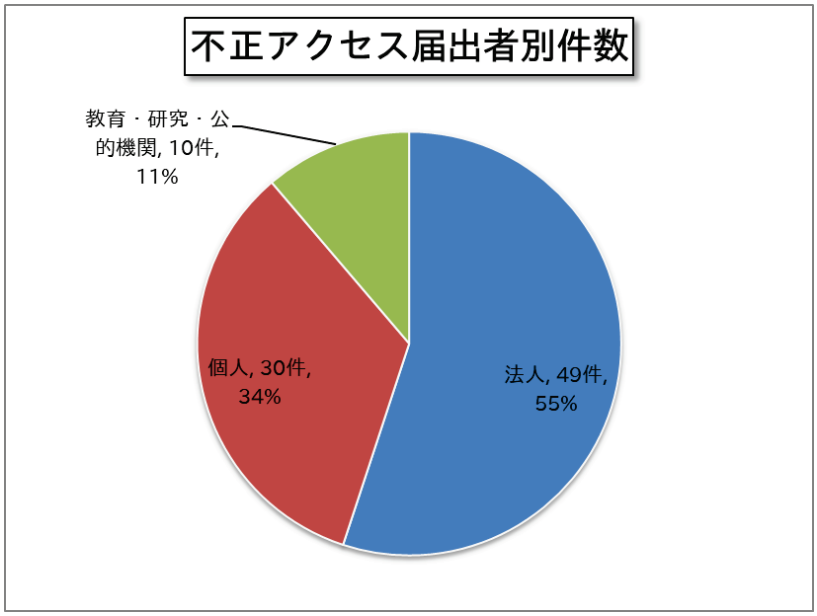


図 2-3：不正アクセス届出者別件数（2019 年）

表 2-1：過去 3 年の不正アクセス届出者別件数の推移

種別	2017 年	2018 年	2019 年
法人	46 件	35 件	49 件
個人	23 件	14 件	30 件
教育・研究・公的機関	10 件	5 件	10 件
合計（件）	79 件	54 件	89 件

2-3. 手口別件数

2019 年に寄せられた不正アクセス届出より、意図的に行う攻撃行為により分類した項目の件数を以下に示す。

1 件の届出について複数の攻撃行為を受けている場合があるため、届出件数とは一致せず、2019 年の総計は 126 件（昨年：73 件）である。

主な手口の内訳は、侵入行為 59 件、サービス妨害攻撃 12 件、なりすまし 21 件であった。

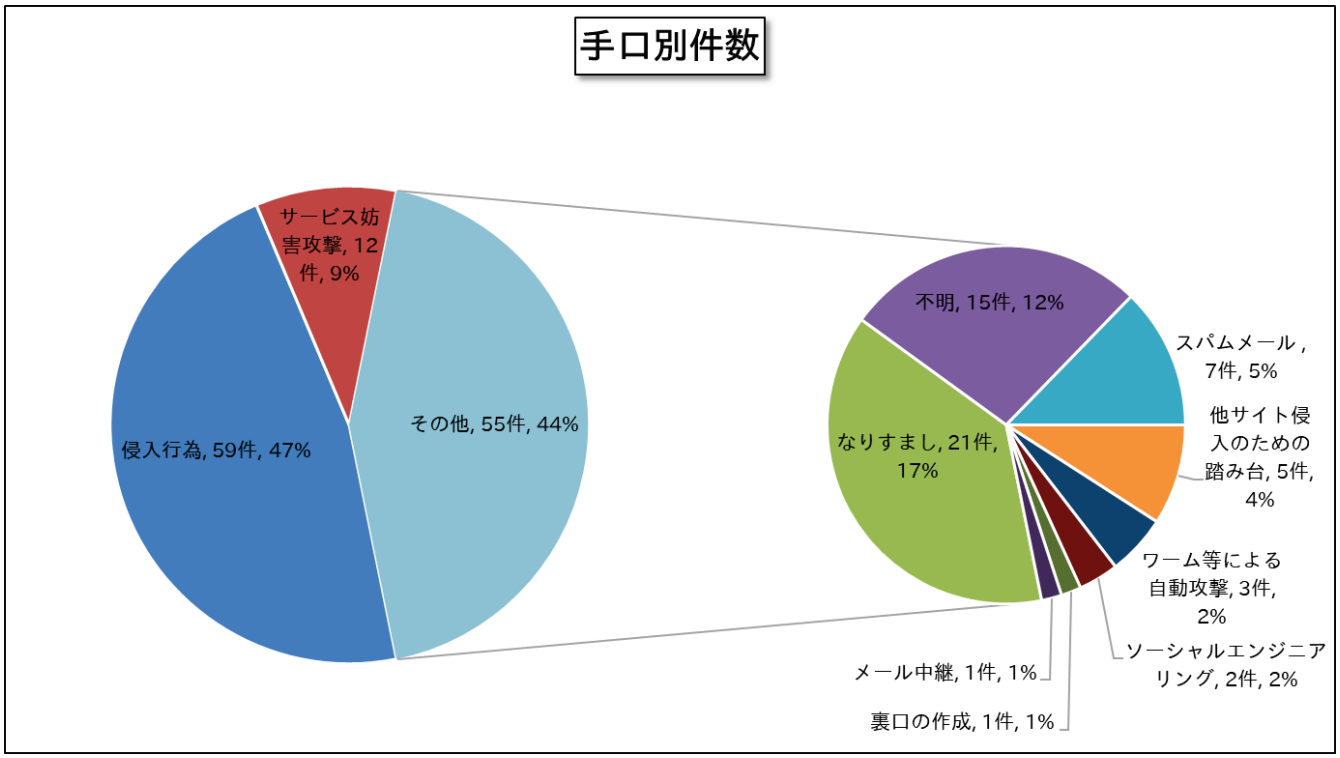


図 2-4：手口別件数（2019 年）

表 2-2：過去 3 年の手口別件数の推移

種別	2017 年	2018 年	2019 年
侵入行為	55 件	33 件	59 件
サービス妨害攻撃	12 件	11 件	12 件
なりすまし	10 件	18 件	21 件
不明	2 件	1 件	15 件
スパムメール	1 件	8 件	7 件
他サイト侵入のための踏み台	0 件	0 件	5 件
ワーム等による自動攻撃	0 件	0 件	3 件
ソーシャルエンジニアリング	0 件	0 件	2 件
裏口の作成	0 件	0 件	1 件
メール中継	3 件	0 件	1 件
証拠の隠滅	0 件	1 件	0 件
メールアドレス詐称	0 件	1 件	0 件
その他	4 件	0 件	0 件
合計（件）	87 件	73 件	126 件

2-4. 原因別件数

2019 年に寄せられた不正アクセス届出より、被害のあった届出について、不正アクセスの原因となった問題点／弱点で分類した件数を以下に示す。

89 件の届出のうち、実際に被害に遭ったのは計 56 件（2018 年：43 件）であり、被害原因としては「設定不備」が 15 件と多かった。一方「不明」も 15 件あり、手口の巧妙化や、ログ等の保存が不十分であるといった理由により、原因の特定に至らない事例が多いものと思われる。

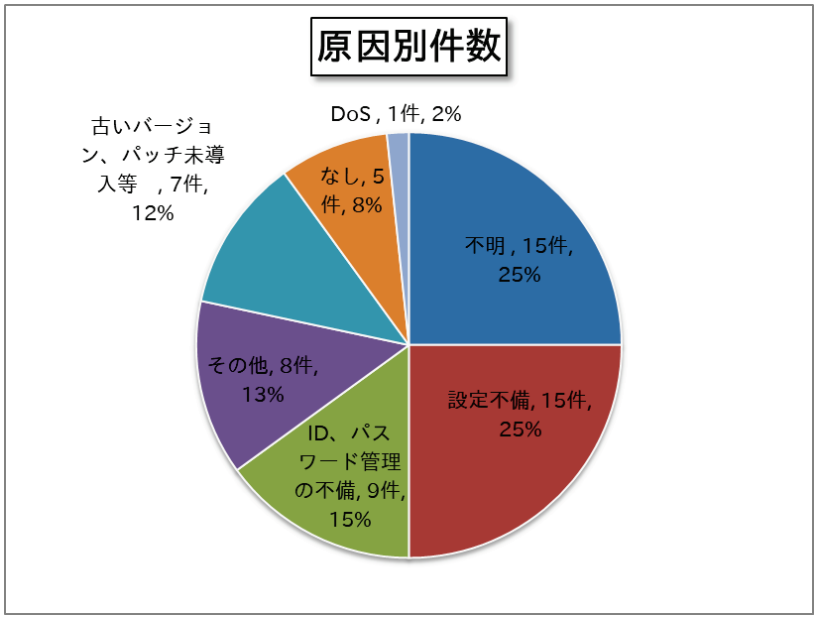


図 2-5：原因別件数（2019 年）

表 2-3：過去 3 年の原因別件数の推移

原因内容	2017 年	2018 年	2019 年
設定不備	7 件	7 件	15 件
不明	11 件	8 件	15 件
ID、パスワード管理の不備	20 件	23 件	9 件
その他	0 件	0 件	8 件
古いバージョン、パッチ未導入など	11 件	1 件	7 件
なし	0 件	0 件	5 件
DoS	5 件	4 件	1 件
合計（件）	54 件	43 件	60 件

2-5. 電算機別件数

2019 年に寄せられた不正アクセス届出より、不正アクセス行為の対象となった機器で分類した件数を以下に示す。なお、1 件の届出について、複数の機器に対して不正アクセスを受けている場合があり、届出件数とは一致しない。「WWW サーバ」が最も多く、29 件であった。

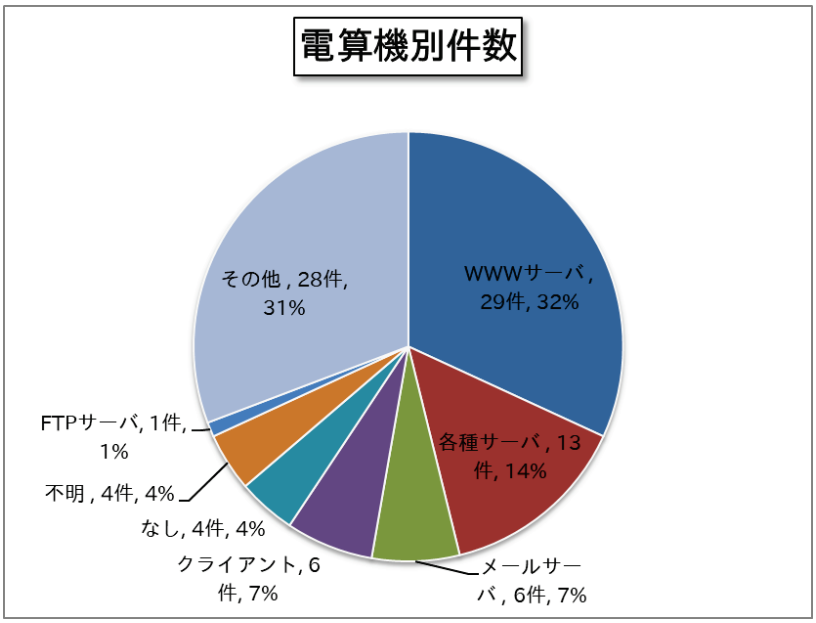


図 2-6：電算機別件数（2019 年）

表 2-4：過去 3 年の電算機別件数の推移

電算機種別	2017 年	2018 年	2019 年
WWW サーバ	29 件	19 件	29 件
各種サーバ	1 件	3 件	13 件
メールサーバ	15 件	14 件	6 件
クライアント	0 件	1 件	6 件
なし	3 件	0 件	4 件
不明	17 件	6 件	4 件
FTP サーバ	0 件	0 件	1 件
ファイアウォール	2 件	4 件	0 件
その他	18 件	8 件	28 件
合計	85 件	55 件	91 件

2-6. 被害内容別件数

2019 年に寄せられた不正アクセス届出より、被害のあった届出の被害内容で分類した件数を以下に示す。

実被害があった件数は 82 件（2018 年：47 件）である。このうち、「データの搾取、盗み見」が最も多く、28 件であった。

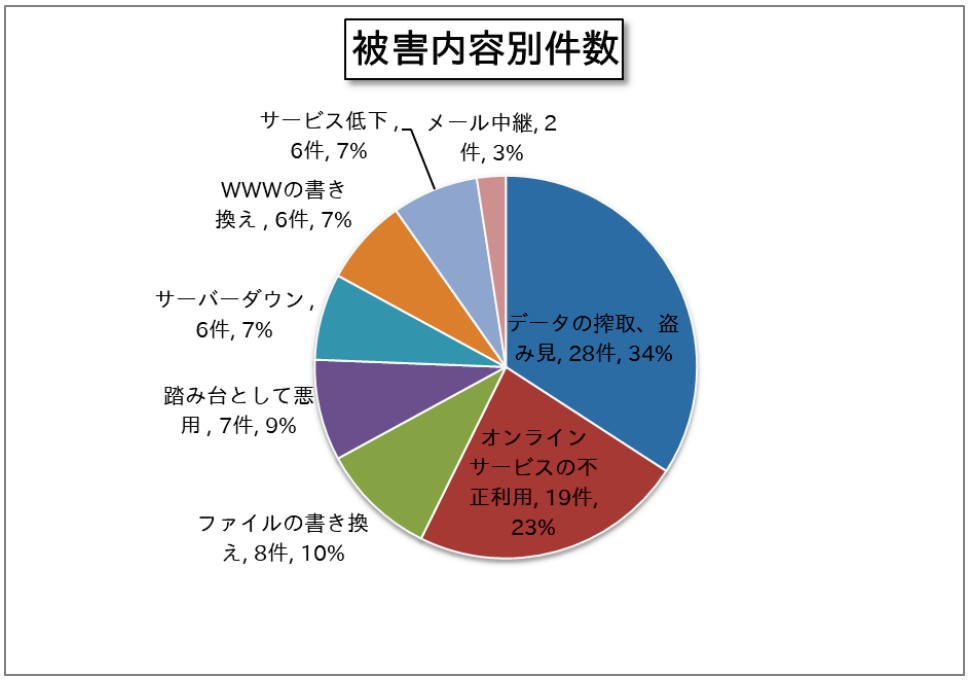


図 2-7：被害内容別件数（2019 年）

表 2-5：過去 3 年の被害内容別件数の推移

被害内容	2017 年	2018 年	2019 年
データの搾取、盗み見	11 件	9 件	28 件
オンラインサービスの不正利用	0 件	10 件	19 件
ファイルの書き換え	6 件	3 件	8 件
踏み台として悪用	7 件	13 件	7 件
サーバーダウン	0 件	1 件	6 件
WWW の書き換え	12 件	5 件	6 件
サービス低下	9 件	5 件	6 件
メール中継	5 件	0 件	2 件
不正アカウントの作成	2 件	1 件	0 件
合計	52 件	47 件	82 件

2-7. 不正アクセス届出にみられた傾向

2019 年では、依然として、ウェブサーバやオンラインサービスに関する不正アクセスの届出が多く寄せられた。特にオンラインサービスについては、企業だけでなく個人からも被害（未遂含む）の届出が寄せられている。オンラインサービスを利用されている方は、企業・個人にかかわらず、被害に遭わないよう、ぜひ、セキュリティ設定やパスワードの見直し等を行っていただきたい。

特記すべき事例として、データベースに不正アクセスされ、データを消されるとともに、身代金を要求する脅迫文が残されていたという被害を受けた届出が複数寄せられた。詳細については「コンピュータウイルス・不正アクセスの届出事例」において紹介しているため、ぜひ、参考にしていただきたい。

・コンピュータ不正アクセス被害の届出制度について

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）