

コンピュータウイルス・ 不正アクセスの届出状況

[2025年(1月~12月)]

本資料では、2025年1月1日から2025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コンピュータ不正アクセスに関する届出状況を報告する。

目次

1. コンピュータウイルス届出状況	- 1 -
1-1. ウイルス届出件数.....	- 1 -
1-1-1. 年別推移	- 1 -
1-1-2. 月別推移	- 1 -
1-2. ウイルス等検出数.....	- 2 -
1-2-1. 年別推移	- 2 -
1-2-2. 月別推移	- 2 -
1-3. ウイルス届出者別件数.....	- 3 -
1-3-1. 届出者の主体別届出件数.....	- 3 -
1-3-2. 届出者の業種別届出件数.....	- 4 -
1-4. ウイルス届出にみられた傾向	- 6 -
2. コンピュータ不正アクセス届出状況.....	- 7 -
2-1. 不正アクセス届出件数.....	- 7 -
2-1-1. 年別推移	- 7 -
2-1-2. 月別推移	- 7 -
2-2. 不正アクセス届出者別件数	- 8 -
2-2-1. 届出者の主体別届出件数.....	- 8 -
2-2-2. 届出者の業種別届出件数.....	- 9 -
2-3. 手口別件数.....	- 11 -
2-4. 被害内容別件数	- 12 -
2-5. 原因別件数.....	- 13 -
2-6. 電算機別件数	- 14 -
2-7. 電算機設置環境別件数.....	- 15 -
2-8. 不正アクセス届出にみられた傾向.....	- 16 -

1. コンピュータウイルス届出状況

2025年の1月から12月のコンピュータウイルス（以下、ウイルス）届出状況について示す。

1-1. ウイルス届出件数

1-1-1. 年別推移

2025年に寄せられたウイルス届出は、年間で前年の260件より76件（約30.5%）少ない、184件の届出があった。このうち、ウイルス感染被害（実被害）があった届出は15件であった。

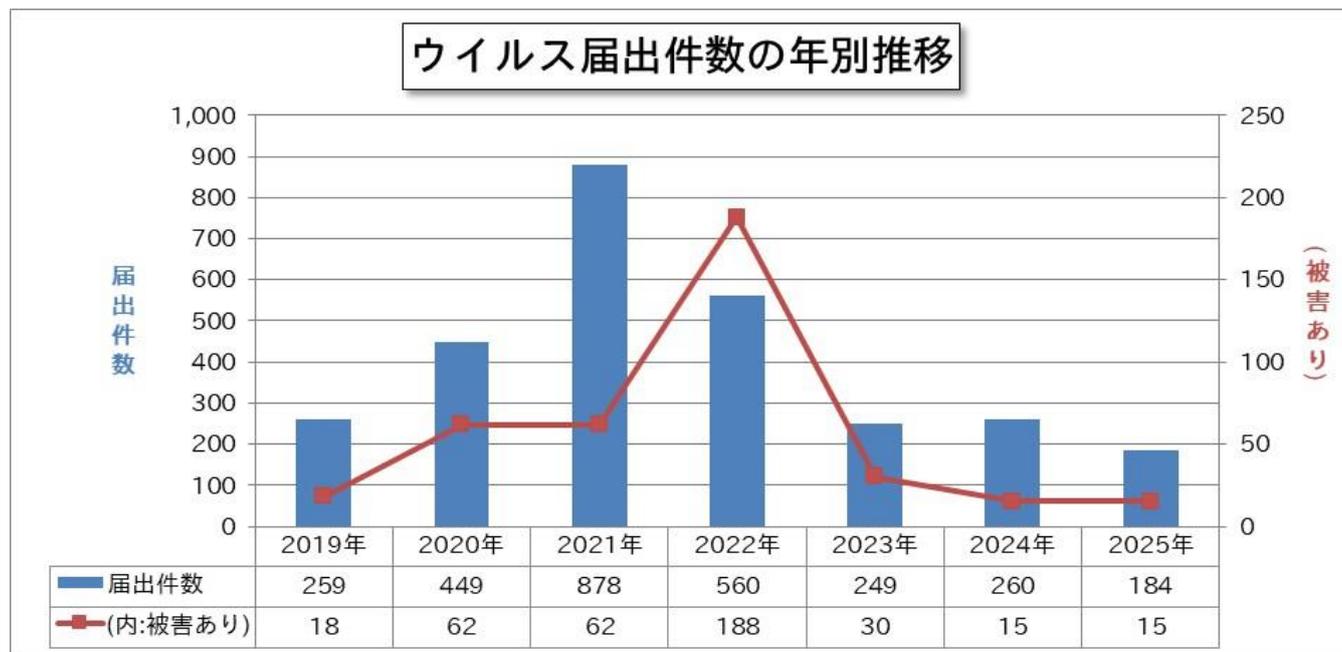


図 1-1：ウイルス届出件数の年別推移

1-1-2. 月別推移

2025年に寄せられたウイルス届出を月別に見ると、3月が最も多く、24件の届出があった。また、被害があった届出は4月と12月が最も多く3件であった。

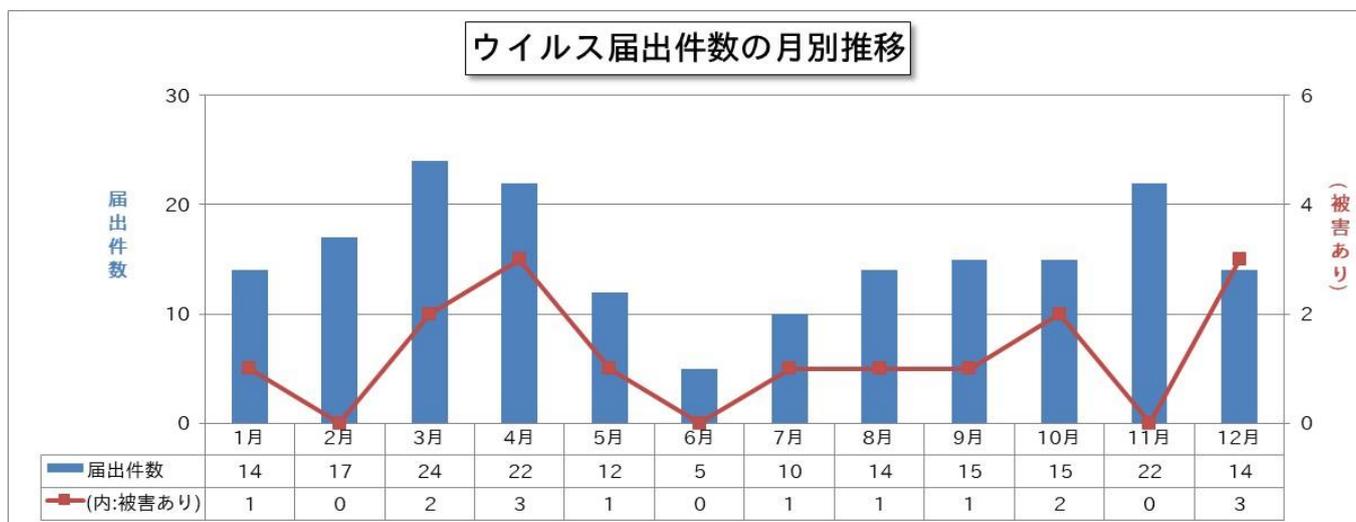


図 1-2：ウイルス届出件数の月別推移

1-2. ウイルス等検出数

1-2-1. 年別推移

2025年に寄せられたウイルス等検出数は、前年の215,662個より90,994個（約42.2%）少ない、124,668個であった。

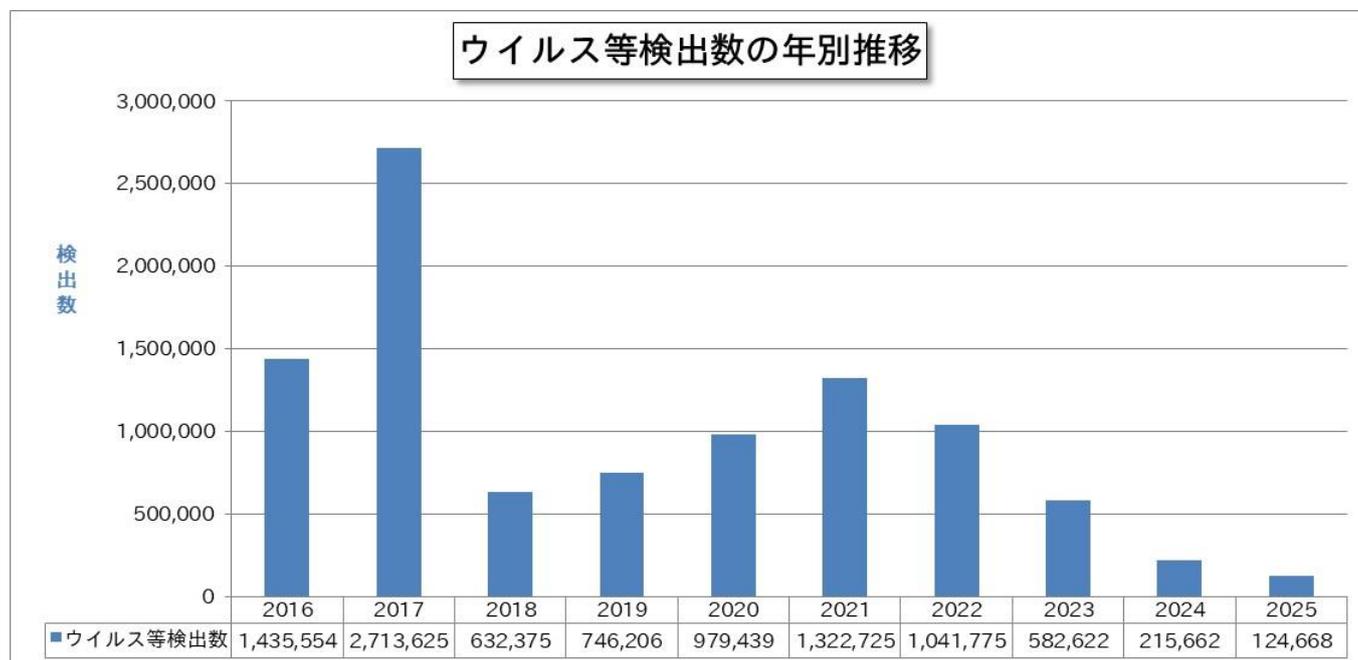


図 1-3 : ウイルス等検出数の年別推移

1-2-2. 月別推移

2025年に寄せられたウイルス等検出数を月別に見ると、4月が最も多く、16,904個であった。

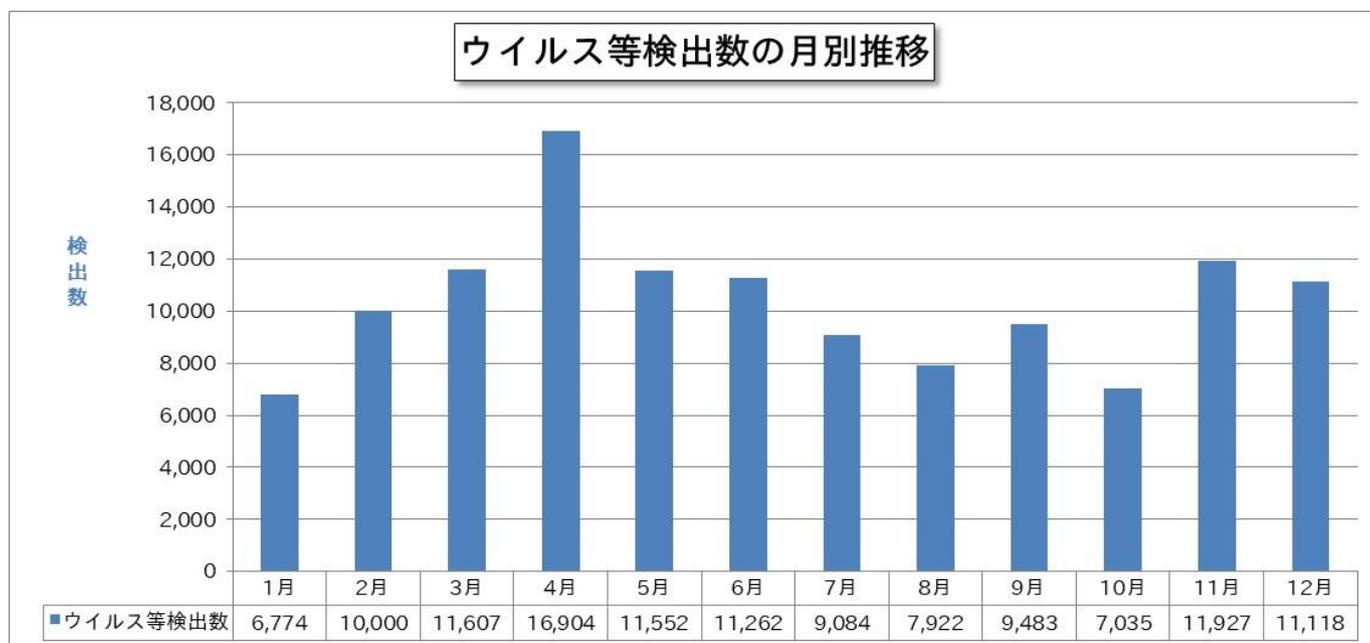


図 1-4 : ウイルス等検出数の月別推移

1-3. ウイルス届出者別件数

1-3-1. 届出者の主体別届出件数

2025年に寄せられたウイルス届出を、届出者の主体別に分類した比率および件数を次に示す。

前年と比較すると、「教育・研究機関」のみ増加し、「法人」と「個人」の件数は減少した。比率では、「法人」からの届出が約53.8%（99件）と最も多かった。

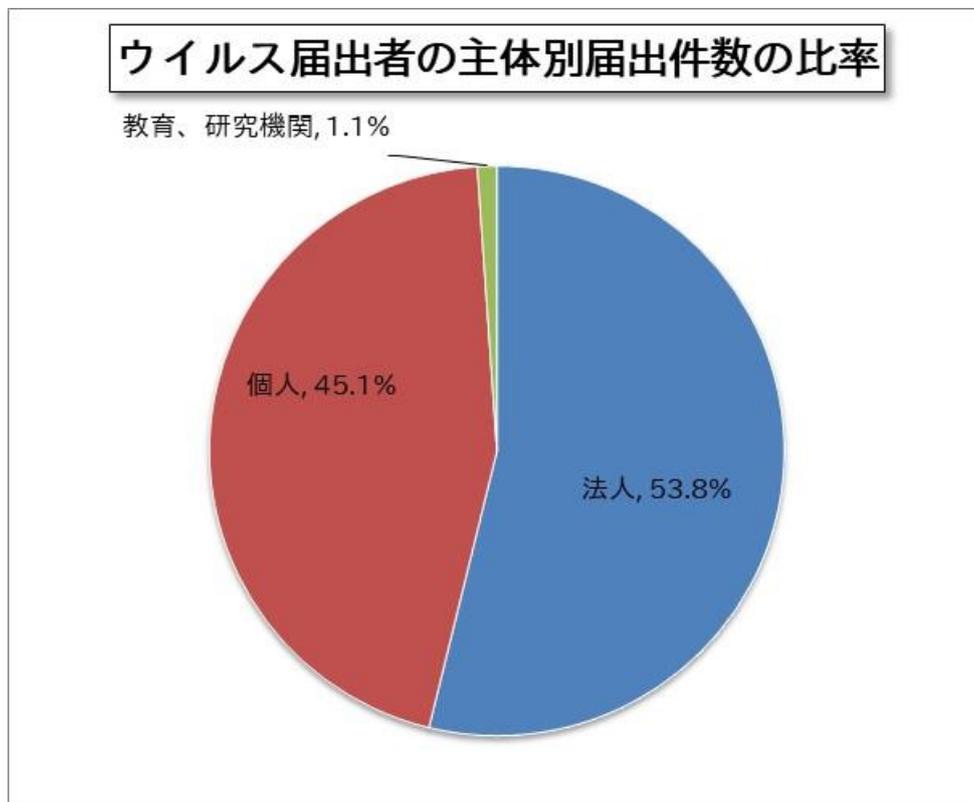


図 1-5：ウイルス届出者の主体別届出件数の比率（2025 年）

表 1-1：過去 3 年のウイルス届出者の主体別届出件数の推移

届出者の主体	2023 年	2024 年	2025 年
法人	166	125	99
個人	70	135	83
教育・研究機関	0	0	2
行政機関	13	0	0
合計（件）	249	260	183

1-3-2. 届出者の業種別届出件数

「1-3-1. 届出者の主体別届出件数」の個人を除く、ウイルス届出の届出者を総務省の日本標準産業分類¹により業種別で分類した比率および件数を次に示す。

比率では、「G.情報通信業」からの届出が約48.0%（49件）、次いで、「E.製造業」が約25.5%（26件）、「J.金融業，保険業」が約14.7%（15件）であった。

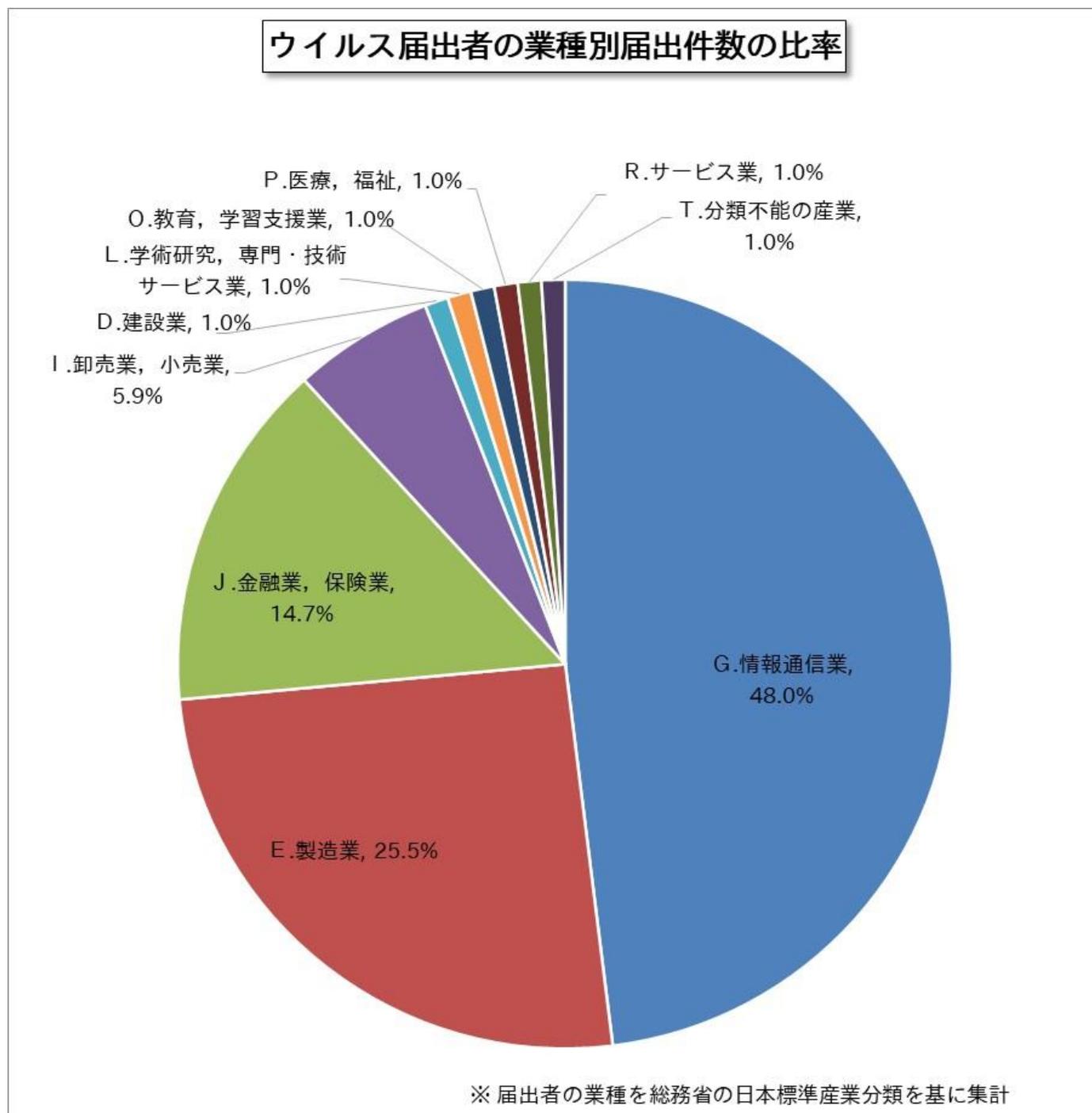


図 1-6：ウイルス届出者の業種別件数の比率（2025 年）

¹ 総務省：日本標準産業分類
https://www.soumu.go.jp/toukei_toukatsu/index/seido/sangyo/index.htm

表 1-2 : ウイルス届出者の業種別届出件数

届出者の業種	2025 年
G.情報通信業	49
E.製造業	26
J.金融業, 保険業	15
I.卸売業, 小売業	6
D.建設業	1
L.学術研究, 専門・技術サービス業	1
O.教育, 学習支援業	1
P.医療, 福祉	1
R.サービス業	1
T.分類不能の産業	1
合計 (件)	102

1-4. ウイルス届出にみられた傾向

ウイルス届出の内容を見ると、実被害が発生する前に検知した「ウイルス検知」の届出がその大半を占めており、被害ありの届出の中では、9件のランサムウェア被害が寄せられた。

届出内容を被害原因別で見ると、「原因不明」となっているものが例年同様多い。これは、攻撃者側の手口の巧妙化や痕跡の隠ぺい等によるケースも考えられるが、被害の原因を特定する調査に適したログが取得されていなかった等の被害者側の環境に由来するケースも考えられる。侵害調査には調査に適したログ取得が必須である。自組織のログ等の取得や管理方法について適時見直し、適切なログ取得・保管ができているか定期的・継続的に点検することを勧める。

・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。

○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）

2. コンピュータ不正アクセス届出状況

2025年の1月から12月のコンピュータ不正アクセス（以下、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

2025年に寄せられた不正アクセス届出は、年間で前年の166件より57件（約34.3%）少ない、109件の届出があった。このうち、実被害があった届出は85件であり、全体の約78.0%を占めた。



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

2025年に寄せられた不正アクセス届出を月別に見ると、7月が最も多く18件の届出があった。また、被害があった届出も7月が最も多く、15件の届出であった。

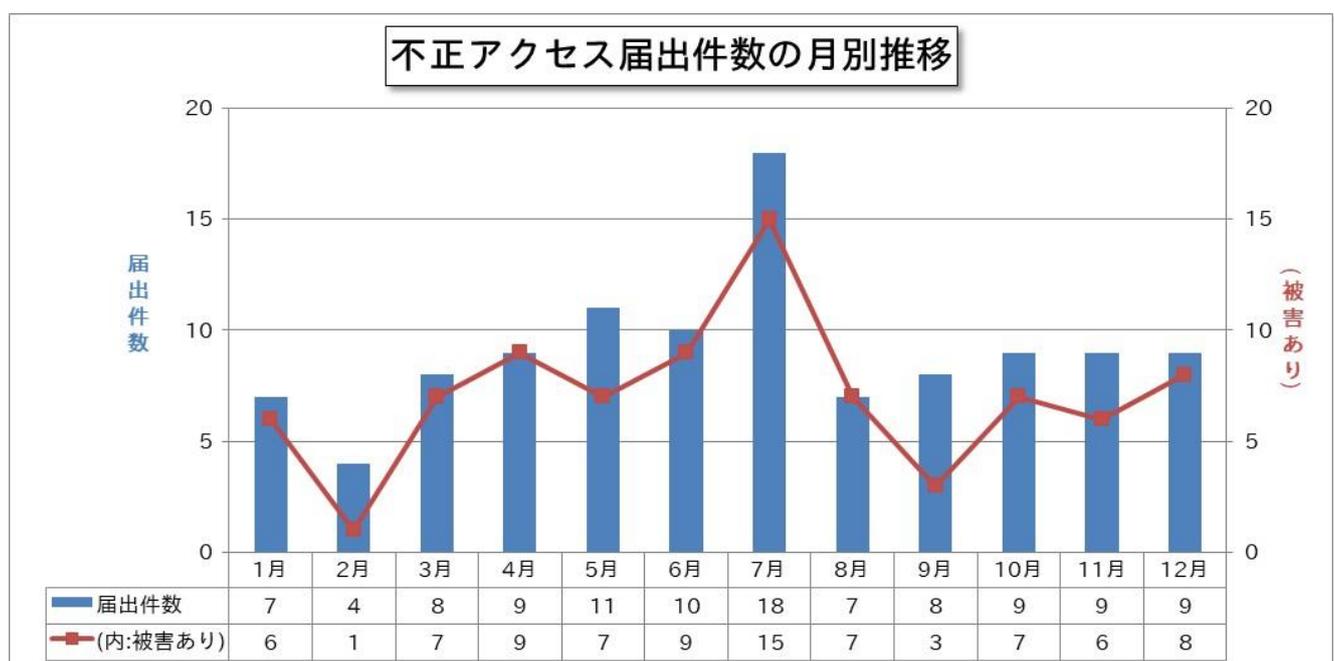


図 2-2：不正アクセス届出件数の月別推移

2-2. 不正アクセス届出者別件数

2-2-1. 届出者の主体別届出件数

2025年に寄せられた不正アクセス届出を、届出者の主体別に分類した比率および件数を次に示す。

前年と比較すると、件数は「個人」のみ増加し、その他は減少した。比率では、「法人」からの届出が約81.7%（89件）と最も多かった。

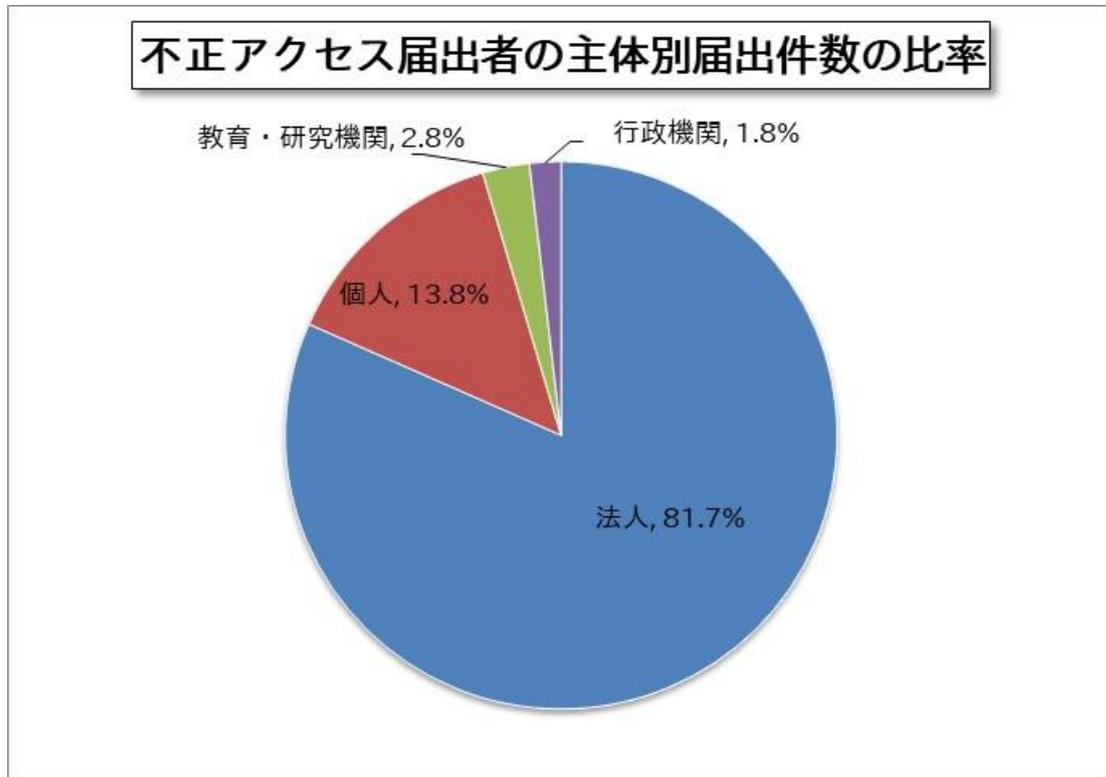


図 2-3：不正アクセス届出者の主体別届出件数の比率（2025年）

表 2-1：過去3年の不正アクセス届出者の主体別届出件数の推移

届出者の主体	2023年	2024年	2025年
法人	183	136	89
個人	29	11	15
教育・研究機関	19	15	3
行政機関	12	4	2
合計	243	166	109

2-2-2. 届出者の業種別届出件数

「2-2-1. 届出者の主体別届出件数」の個人を除いた、不正アクセス届出の届出者を総務省の日本標準産業分類により業種別で分類した比率および件数を次に示す。

比率では、「E.製造業」からの届出が約22.3%（21件）と最も多く、次いで「G.情報通信業」が約19.1%（18件）、「I.卸売業，小売業」が約14.9%（14件）であった。

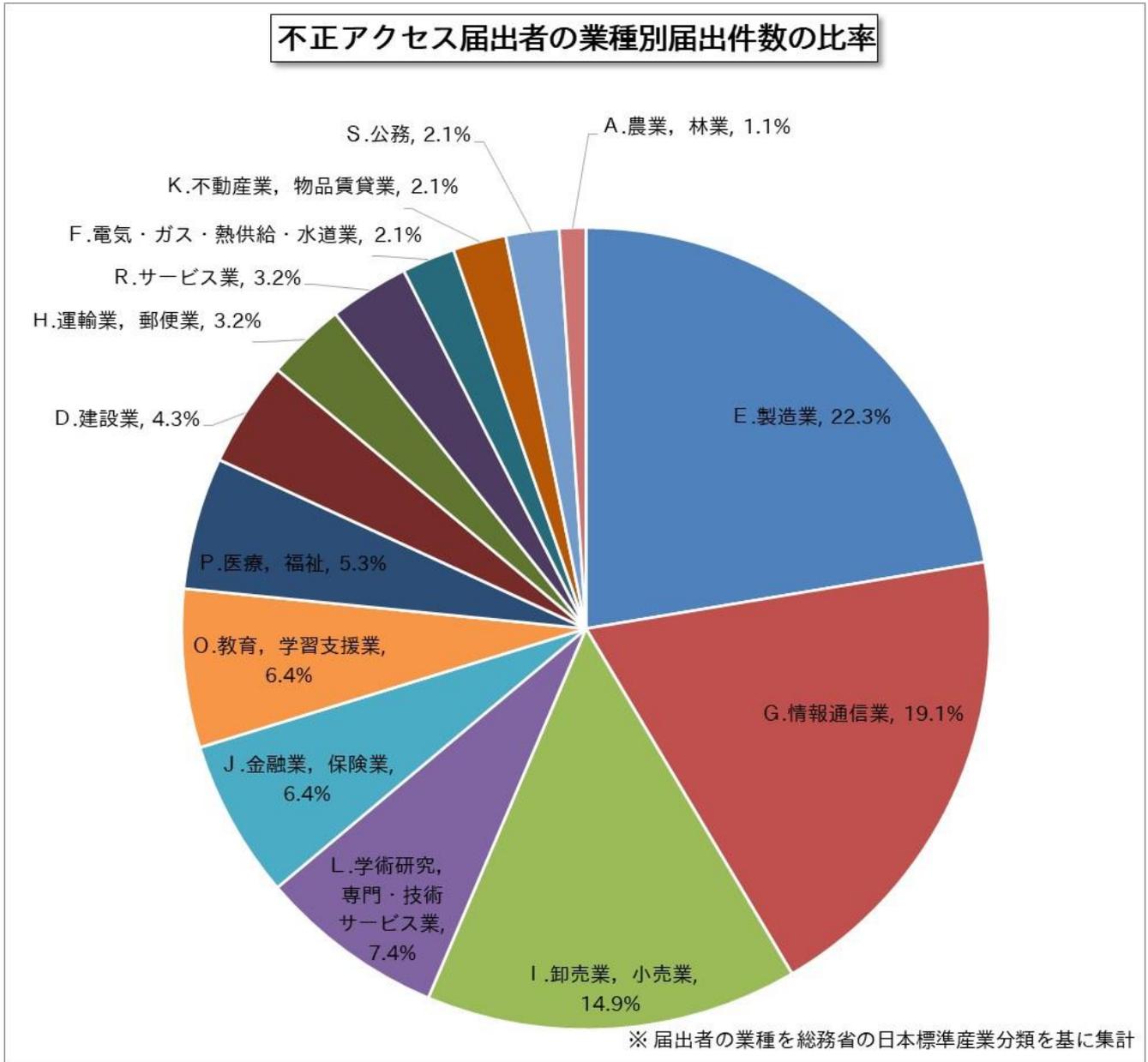


図 2-4：不正アクセス届出者の業種別届出件数の比率（2025 年）

表 2-2：不正アクセス届出者の業種別届出件数

届出者の業種	2025年
E.製造業	21
G.情報通信業	18
I.卸売業，小売業	14
L.学術研究，専門・技術サービス業	7
J.金融業，保険業	6
O.教育，学習支援業	6
P.医療，福祉	5
D.建設業	4
H.運輸業，郵便業	3
R.サービス業	3
F.電気・ガス・熱供給・水道業	2
K.不動産業，物品賃貸業	2
S.公務	2
A.農業，林業	1
合計（件）	94

2-3. 手口別件数

2025年に寄せられた不正アクセス届出を攻撃行為（手口）により分類したものである。

なお、1つの届出について、複数の攻撃行為を受けている場合は、該当する項目のそれぞれにカウントした。

2025年の届出において最も多く見られた手口は、前年と同様に「ファイル／データ窃取、改ざん等」で65件あり、次いで「不正プログラムの埋め込み」が34件、「パスワード推測」が31件であった。

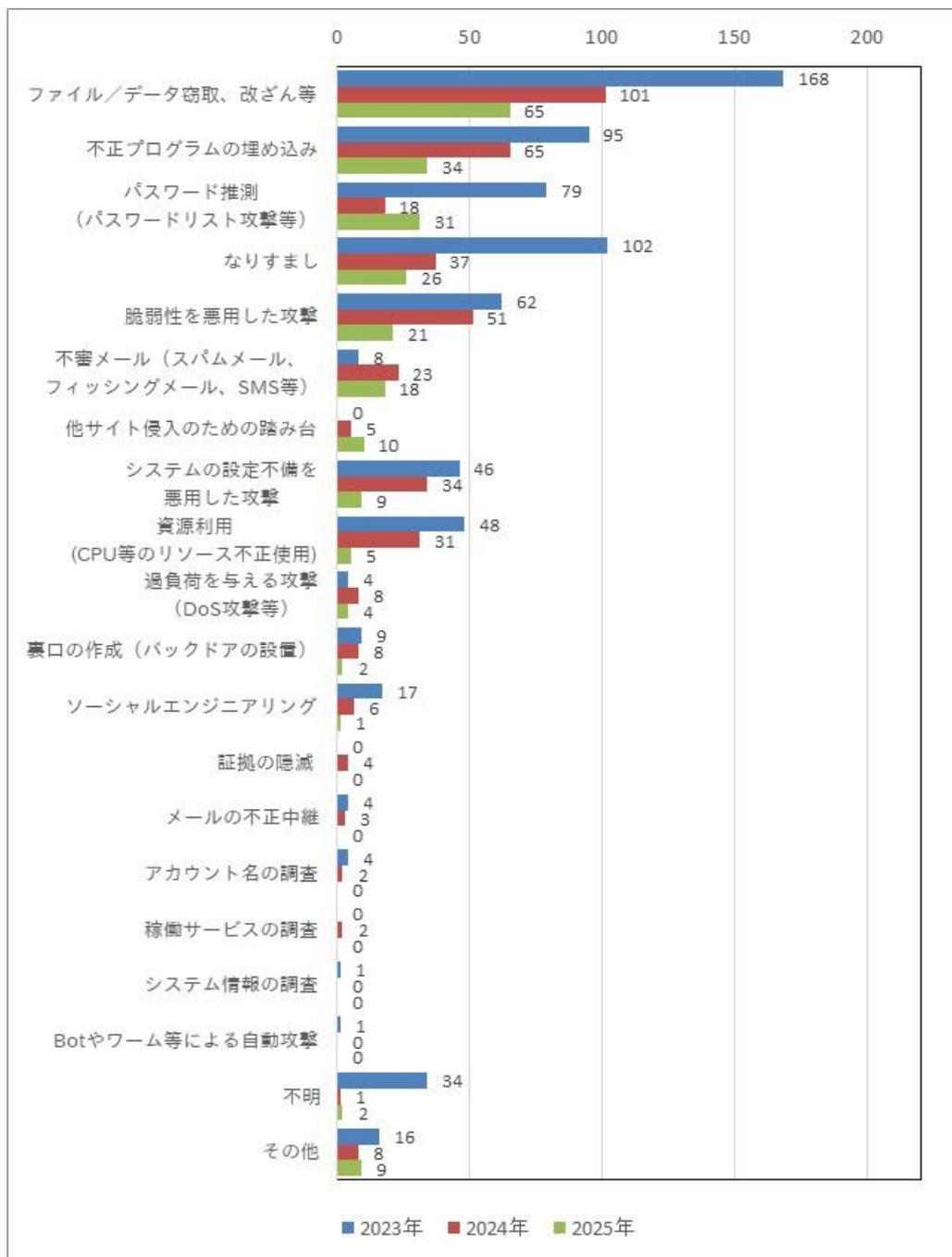


図 2-5：不正アクセス手口別件数の推移（2023年～2025年）

2-4. 被害内容別件数

2025年に寄せられた不正アクセス届出のうち、実際に被害に遭った届出について、被害内容により分類したものである。

なお、1つの届出について、複数の被害内容が存在する場合は、該当する項目のそれぞれにカウントした。

2025年において最も多く見られた被害内容は、「データの窃取、盗み見」が44件であり、次いで「ファイルの書き換え」が34件、「不正プログラムの埋め込み」が32件であった。

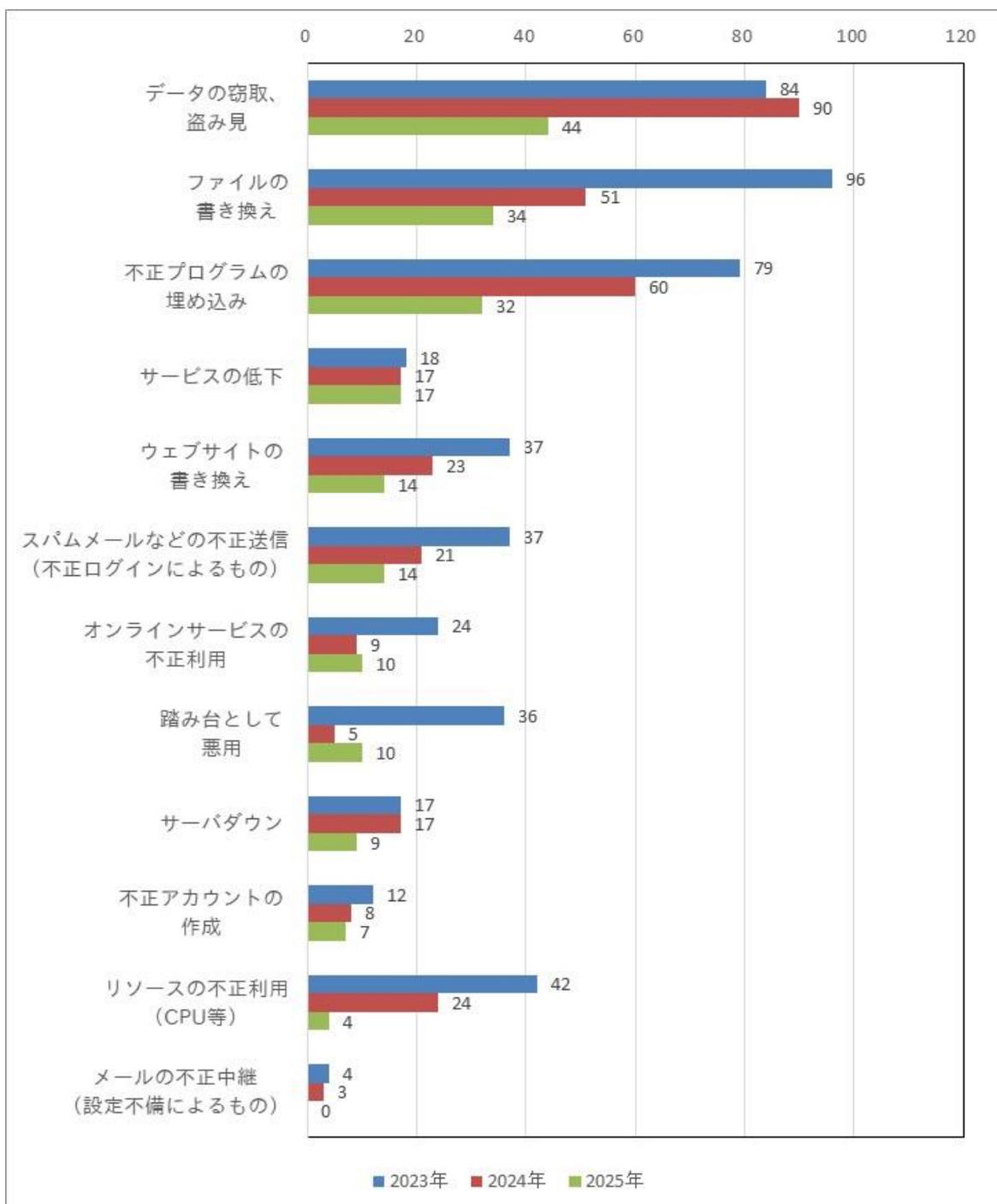


図 2-6 : 不正アクセス被害内容別件数の推移 (2023年~2025年)

2-5. 原因別件数

2025年に寄せられた不正アクセス届出のうち、実際に被害に遭った届出について、不正アクセスの原因となった問題点／弱点により分類したものである。

なお、1つの届出について、複数の被害原因が存在する場合は、該当する項目のそれぞれにカウントした。

2025年において最も多く見られた被害原因は、「ID、パスワード管理の不備」で30件あり、次いで「古いバージョンの利用や修正プログラム・必要なプラグイン等の未導入によるもの」が18件、「設定の不備」が7件であった。

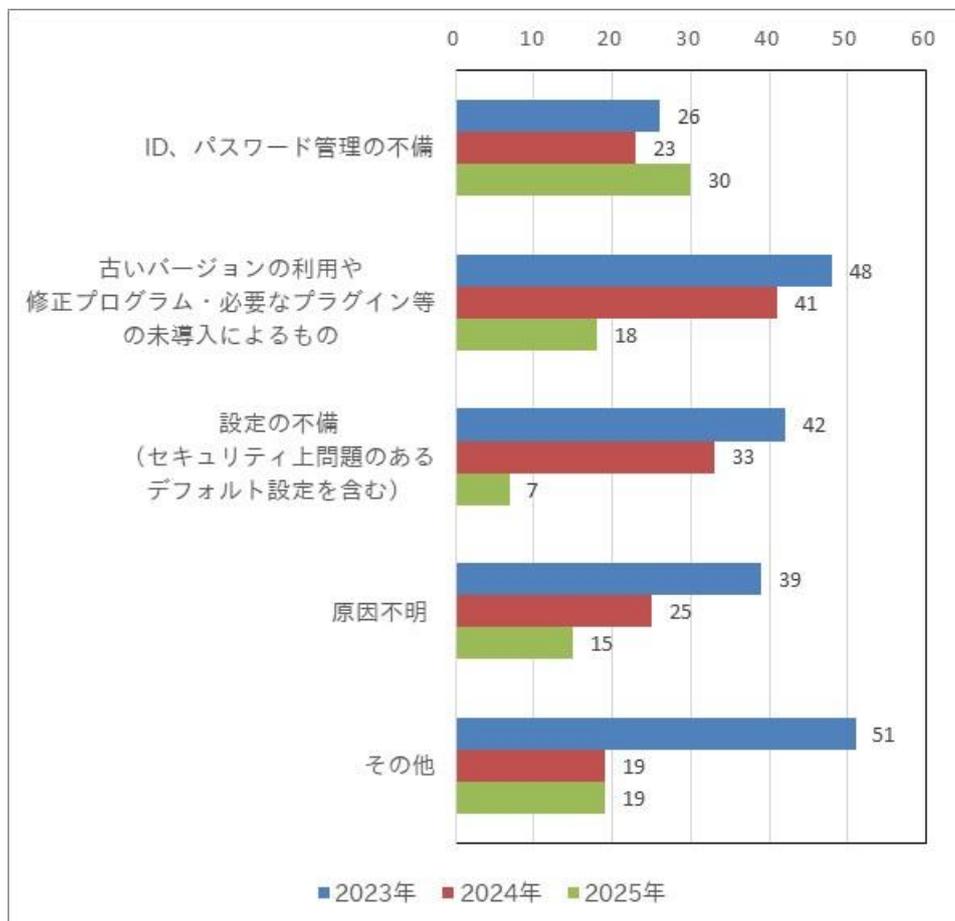


図 2-7：不正アクセス原因別件数の推移（2023年～2025年）

2-6. 電算機別件数

2025年に寄せられた不正アクセス届出のうち、不正アクセス行為の対象となった電算機の種別により分類したものである。なお、1つの届出について、複数の電算機が不正アクセスの被害を受けた場合は、該当する項目のそれぞれにカウントした。

2025年において最も多く見られた電算機は、「クライアント」で28件あり、次いで「ウェブサーバ」が27件、「ファイルサーバ」が19件であった。

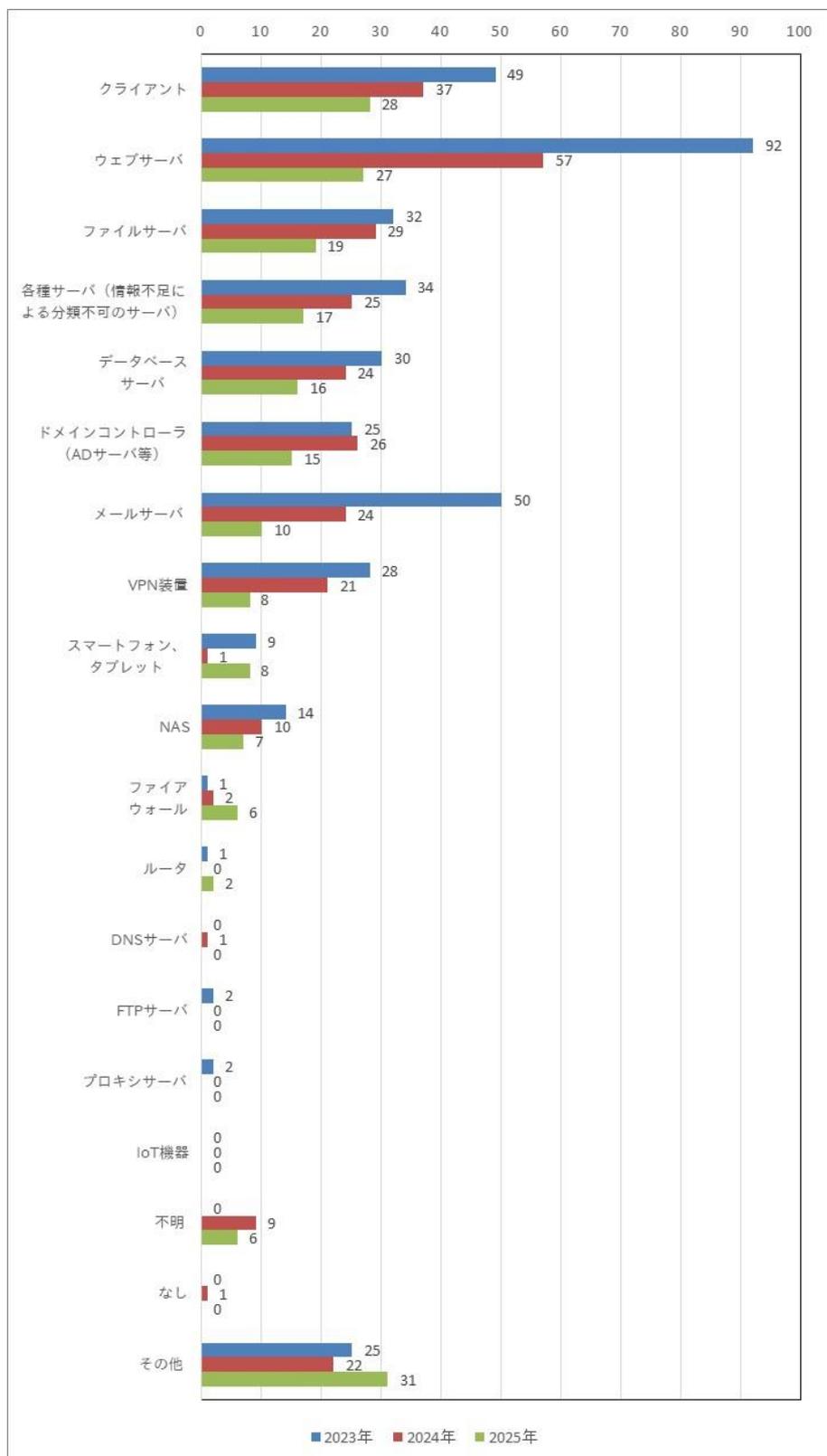


図 2-8：不正アクセス電算機別件数の推移（2023年～2025年）

2-7. 電算機設置環境別件数

2025年に寄せられた不正アクセス届出のうち、不正アクセス行為の対象となった電算機の設置環境により分類したものである。なお、1つの届出について、複数の異なる設置環境が不正アクセスを受けた場合は、該当する項目のそれぞれにカウントした。

2025年において最も多く見られた設置環境は、「自組織内（オンプレミス）」で42件あり、次いで「レンタルサーバ（ホスティング）」が17件、「クラウド環境（AWS,Azure等）」が17件であった。

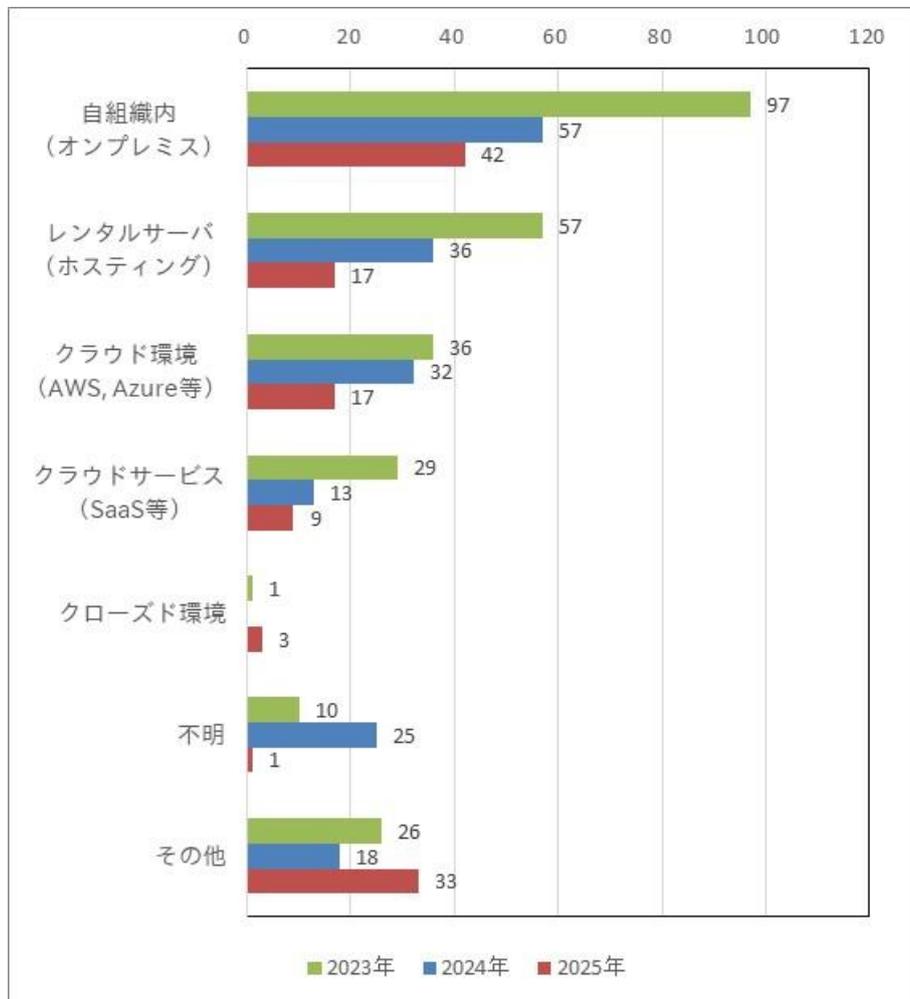


図 2-9：不正アクセス電算機設置環境別件数の推移（2023年～2025年）

2-8. 不正アクセス届出にみられた傾向

1-4.と同じく、不正アクセスとして届出がなされた中には、被害の全容把握や原因の特定に至っていないと思われる事案も多い。侵入経路が判明しているケースでは、届出で主に見受けられたものとして、VPN 装置のぜい弱性の悪用や認証情報の不正利用を侵入経路としたランサムウェア攻撃（データを暗号化しない攻撃も含む。）があった。そのほか、ウェブサイト（EC サイトを含む。）のぜい弱性を悪用した攻撃による改ざん被害、インターネットサービス（Microsoft 365 等）アカウントを乗っ取られたことによる不正メールの送信被害等も見られた。

被害原因別に見ると、ID、パスワード管理の不備が多く、悪用できるぜい弱性のある古いバージョンの利用や、適切なプラグインが未導入のままの運用といったものも前年同様多い傾向にある。他者に推測されにくい複雑なパスワードを設定する、パスワードの使い回しをしない、多要素認証等のセキュリティオプションを積極的に採用する等の適切なアカウント管理や、自組織が利用している機器やソフトウェアに関するぜい弱性情報の把握と修正プログラムの迅速な適用といった、基本的な対策の徹底が必要である。

また、不正アクセスの原因を「原因不明」とする届出も多いことから、調査に適したログが取得されていない、調査に対応した体制ができていない等もあると推測される。先に述べた基本的な対策の徹底に加えて、ログ取得や保管の方法、取得する期間を見直すほか、外部機関に対応を依頼する等の体制作りも必要であると考ええる。

ぜい弱性情報の把握やウェブサイトの安全な運用管理については、下記ウェブページに情報を記載しているので、参考にしていきたい。

対策に関する参考情報)

・「ランサムウェア対策特設ページ」

https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html

・「中小企業の情報セキュリティ対策ガイドライン」

<https://www.ipa.go.jp/security/guide/sme/about.html>

・「安全なウェブサイトの運用管理に向けての 20 ケ条
～セキュリティ対策のチェックポイント～」

<https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html>

・「安全なウェブサイトの作り方」

<https://www.ipa.go.jp/security/vuln/websecurity/about.html>

・「EC サイト構築・運用セキュリティガイドライン」

<https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html>

・「JVN (Japan Vulnerability Notes)」 ※ぜい弱性対策情報ポータルサイト

<https://jvn.jp/>

・「高度標的型攻撃」対策に向けたシステム設計ガイド

<https://warp.ndl.go.jp/web/20230118000000/www.ipa.go.jp/security/vuln/newattack.html>

・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）