

規制の事前評価書

1 規制の名称

識別符号の不正流通に関する行為についての規制の強化

2 担当部局

生活安全局情報技術犯罪対策課

3 評価実施時期及び分析対象期間

(1) 評価実施時期

平成24年2月

(2) 分析対象期間

平成12年2月から規制の新設に係る条項の施行の1年後までの間

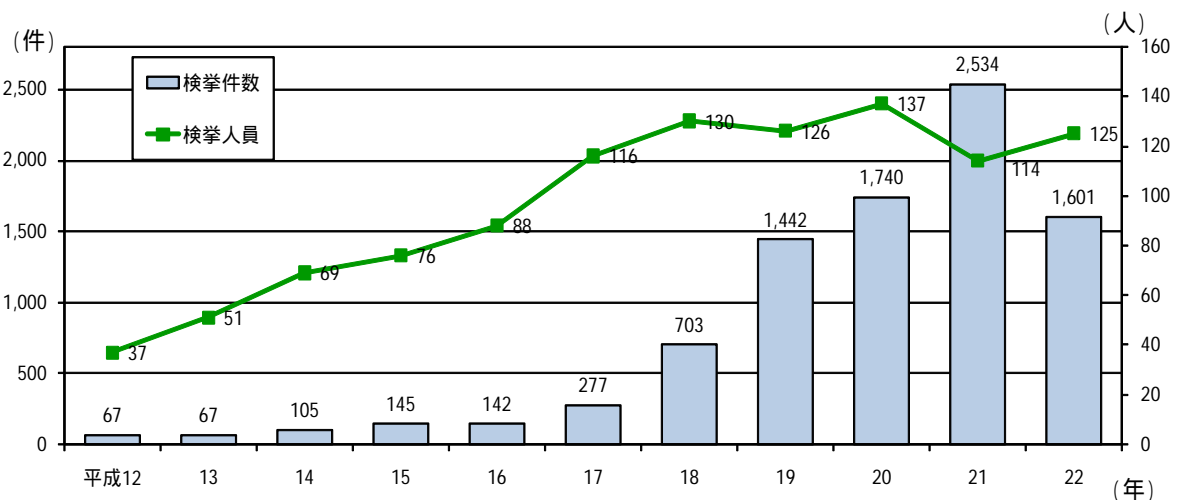
4 規制の目的、内容及び必要性

(1) 現状

ア 不正アクセス行為の現状

不正アクセス行為の禁止等に関する法律（平成11年法律第128号。以下「不正アクセス禁止法」という。）違反の検挙件数・人員は、次表のとおり、不正アクセス禁止法制定以降、増加傾向にある。特に、検挙件数については、平成19年には1,442件、20年には1,740件、21年には2,534件、22年には1,601件と高水準で推移しており、不正アクセス禁止法違反についての情勢は深刻な状況にある。

【不正アクセス禁止法違反の検挙件数の推移（平成12～22年）】

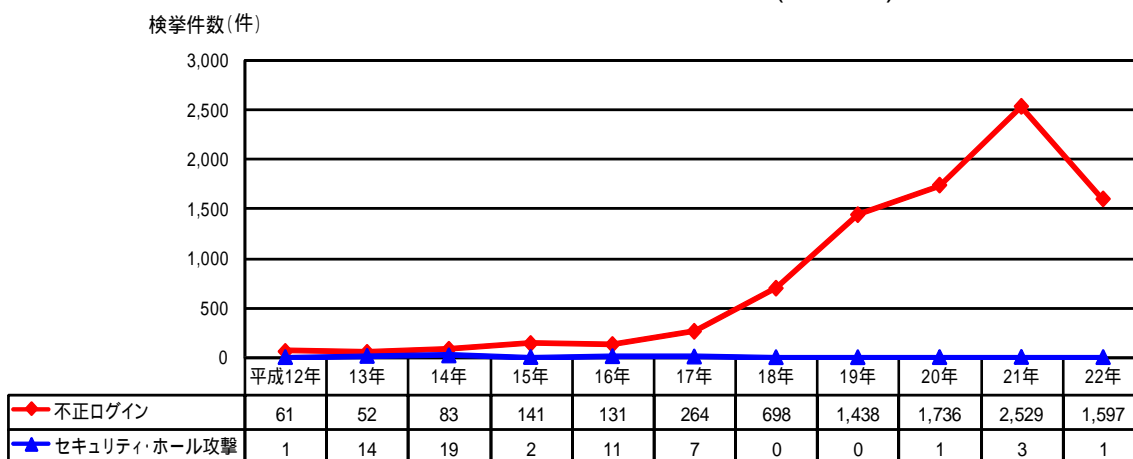


不正アクセス行為(不正アクセス禁止法第3条第2項に規定する不正アクセス行

為をいう。以下同じ。)とは、アクセス制御機能による特定電子計算機の特定利用の制限を免れて、その制限されている特定利用をし得る状態にさせる行為をいうが、その類型は、セキュリティ・ホール攻撃^{注1}によるものと、他人の識別符号の無断入力によるもの(不正ログイン行為)に区分される。

近年、は、アクセス制御機能に係るソフトウェアの改良その他アクセス制御機能の高度化により、技術的な対処が可能である一方で、は、他人の識別符号を取得してしまえば、アクセス管理者のアクセス制御機能によっては防御することができない性質のものであり、不正アクセス禁止法制定以降増加傾向にある。

【不正アクセス行為の検挙件数の推移(類型別)】



特に、不正ログイン行為は、アクセス制御機能の本質が、当該アクセス制御機能に係る正しい識別符号が入力される限り、それが適法なものであるか否かについてコンピュータの使用記録等から明らかになる性質のものではないことから、そもそも潜在化し発覚が遅れやすく、発覚の時点において既に被害等が拡大しているケースが多い。具体的には、他人の識別符号を用いて不正アクセス行為を行い、利用権者になりすましてインターネットショッピングをしたりインターネットバンキングで不正送金をするなどにより金銭的被害を発生するケースが認められている(事例1参照)。また、利用権者が別々のサイトにおいても同一の識別符号を使い回す例が一般化している事情があると言われており、これを背景に、利用権者以外の第三者から不正取得した識別符号データを連続自動入力するプログラムを用いて様々なサイトに試行入力して不正アクセス行為を敢行する形態のものも認知されている(事例2参照)。このように、いったん不正ログイン行為が行われると金銭的被害等が拡大していくほか、正しい識別符号が入力される限り、技術的に不正ログイン行為を防止することは極めて困難であることから、不正ログイン対策が急務となっている。

注1:「セキュリティ・ホール攻撃」とは、コンピュータのプログラムの瑕疵等により、アクセス管理者の意に反してアクセス制御機能により制限された特定利用をし得る状態にすることができる一定の情報又は指令を入力する行為をいう。

【事例1】会社員の男(33)は、平成19年6月から同年10月までの間、ファイル共有ソフト「ウィニー」の使用によりインターネット上に流出していた他人の識別符号データを入手し、これを用いて不正アクセス行為を行った上で、インターネットショッピングにおける商品の詐取、インターネットバンキングにおける自己名義の銀行口座への不正送金を行った。同年10月、不正アクセス禁止法違反、詐欺罪及び電子計算機使用詐欺罪で検挙した(愛知、警視庁、高知)。

【事例2】あるオンラインゲームサイトに対し、他のサービスから流出したと思われる大量のID・パスワードを順に試行入力していく形態の攻撃が認知されている。当該オンラインゲームサイト運営企業の観測によれば、月に約30万回前後の試行入力があり、概ね20回から30回に一度程度の頻度でログインが成功している状況である。また、異なる時間帯に異なるIPアドレスから同じID・パスワードが試行入力されている事実も観測されている。

イ 識別符号の不正流通の現状

上記のとおり、識別符号が不正アクセス行為目的を有する者の手に渡った場合、不正ログイン行為を技術的に防ぐことは極めて困難であるところ、不正ログイン行為の増加の背景には、識別符号が利用権者又はアクセス管理者(以下「利用権者等」という。)の承諾なく不正に流通している現状がある。すなわち、利用権者等以外の者が、利用権者等から識別符号を詐取して不正ログイン行為を行ったり、あるいは、詐取した識別符号をさらに第三者に転売するなどの提供行為を行い、提供を受けた者が不正ログイン行為を行うという事態が生じている。

このような状況の中で、不正ログイン行為を防ぐためには、不正ログイン行為の準備段階の行為を規制して、他人の識別符号の不正流通を防止するしかないという現状になっている。

【不正ログインに至る経緯】



他人の識別符号の不正流通

(2) 規制の目的及び必要性

ア 規制の現状

不正アクセス禁止法は、電気通信回線を通じて行われる電子計算機に係る犯罪の防止という目的を達成するため、不正アクセス行為を禁止及び処罰することにより、不正アクセス行為の予防を図ることとしている。また、不正アクセス行為を助長する行為については、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じ、利用権者等以外の者に提供することを禁止及び処罰することとしている。すなわち、不正アクセス禁止法は、不正アクセス行為にあつては、当該行為の行われる時点を捉え、不正アクセス行為に直結し得る助長行為にあつては、他人が容易に不正アクセス行為を行い得る状態にした時点を捉え、すなわち、行為の危険性が発現した時点を捉えて禁止及び処罰することを基本にしている。

イ 規制の目的及び必要性

上記(1)のとおり、近年、不正ログイン行為が増加傾向にあることから、不正ログイン行為を防止するため、次のとおり不正ログイン行為の準備段階の行為を規制して、他人の識別符号の不正流通を防止する必要がある。

(ア) フィッシング行為の規制

フィッシング行為とは、アクセス管理者になりすまし、その他アクセス管理者であると誤認させて、

アクセス管理者が利用権者に対し識別符号を入力することを求める旨の情報を、インターネット等を利用して公衆が閲覧することができる状態に置く行為

アクセス管理者が利用権者に対し識別符号を入力することを求める旨の情報を、電子メールにより送信する行為

を行うこといい、不正アクセス禁止法制定時には想定されておらず、平成16年に初めて認知されたものである。この行為のうち主なものは一つ目ののものであり、具体的にはアクセス管理者が利用権者に対し識別符号を入力することを求めているかのような内容のウェブサイト（フィッシングサイト）をインターネット上に開設し、これを閲覧した利用権者を錯誤に陥れて識別符号を詐取する行為である。また、二つ目のものは、同様の情報を電子メールにより利用権者に送信するなどして識別符号を詐取する行為をいう。

このようなフィッシング行為は、他人の識別符号の不正取得手段として多用されている状況にあり、平成21年は約8割が、平成22年は約9割がフィッシング行為により他人の識別符号を詐取している^{注2}。

フィッシング行為は、フィッシングサイト等を同時に多数の者に閲覧させて、それらの者を錯誤に陥れる手口であることから、一度に多数の識別符号を詐取することを可能にし、多くの被害を発生させる危険性の高い行為であり、当該

注2：不正アクセス行為で検挙した事件における他人の識別符号の入手方法のうち、フィッシング行為により入手した数の割合。

行為を禁止及び処罰の対象とする必要がある（事例3参照）。

なお、フィッシング行為により利用権者が識別符号を入力し詐取された時点では、フィッシングの行為者以外の誰も不正取得の事実を認識することができない状態にあり、これより以前の段階を捉えない限り、識別符号の不正流通を防止できず、不正アクセス行為の禁止の実効性を担保することができないことから、フィッシングサイトをインターネット上に開設した時点で、又は、アクセス管理者が利用権者に対し識別符号を入力することを求める旨の情報を電子メールにより利用権者に送信した時点で、識別符号の不正取得の有無にかかわらず、禁止及び処罰の対象とする必要がある。

【事例3】無職の男（32）らは、平成20年9月から平成21年11月までの間、フィッシングにより他人のID・パスワードやクレジットカード番号等を入手し、会員専用サイトに不正アクセス行為を行い、住所等の個人情報を入手した上、それを用いて他人になりすましてインターネットショッピングにおいて総額約8,500万円相当の商品をだまし取った。平成22年8月までに、不正アクセス禁止法違反及び詐欺罪で検挙した（広島、静岡、岡山、愛媛、福岡）。警察は平成20年9月にフィッシングサイトの存在を認知していたが、フィッシング犯の検挙（詐欺罪）に至ったのは平成22年4月であった。

(1) 不正アクセス行為を助長する行為の規制の強化

現行不正アクセス禁止法では、(2)アのとおり、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じ、利用権者等以外の者に提供することを禁止及び処罰することとしている。しかし、近年、利用権者が識別符号を使い回している実態及び識別符号データを連続自動入力プログラムを用いて様々なサイトに試行入力する攻撃の出現により、どの特定電子計算機の特定利用に係るものであるかが明らかでない識別符号であっても不正アクセス行為を行うための「道具」となっている状況に鑑み、不正アクセス行為を助長する行為の範囲を拡張し、どの特定電子計算機の特定利用に係るものであるかが明らかでない識別符号であっても、アクセス制御機能に係る他人の識別符号の提供行為を禁止及び処罰する必要がある。

ただし、提供行為全般を禁止した場合、例えば、情報セキュリティ事業者が、流出している識別符号のリストを、不正アクセス行為に用いられるおそれがある危険な識別符号であるとして、契約している企業に提供する行為（提供を受けた契約企業は、同一の識別符号が自らのサイトでも使い回されているかどうかを確認し、使われている場合には当該識別符号の利用権者に識別符号の変更を促す）も禁止及び処罰の対象となってしまう。このような行為は不正アクセス行為を助長するものではなく、不正アクセス行為の防止に資する事業であることから禁止及び処罰の対象となることは適当ではない。したがって、このような行為を禁止及び処罰の対象から除外し、不正アクセス行為につながるおそれがある行為に限って規制する必要がある。

(ウ) 他人の識別符号を不正に取得する行為の規制

識別符号の取得そのものについても、いったん不正取得が成功すれば、どの特定電子計算機の特定利用に係るものか明らかであるかないかを問わず、不正アクセス行為を容易に行い得ることから、不正アクセス行為の禁止の実効性を担保するため、他人の識別符号を不正取得する行為を禁止及び処罰する必要がある。

(イ) 他人の識別符号を不正に保管する行為の規制

他人の識別符号を保管する行為は、識別符号の不正取得により生じる不正アクセス行為に直結する危険性が継続して生じている状態にあると言える。このため、他人の識別符号を保管する行為についても、不正取得から不正アクセス行為に至る一連の行為の一つとして規制する必要がある。

(3) 規制の内容

ア フィッシング行為の規制

フィッシング行為を禁止及び処罰する。

イ 不正アクセス行為を助長する行為の規制の強化

どの特定電子計算機の特定利用に係るものであるかを明らかにしたり、又はこれを知っている者の求めに応じたものでなくても、業務その他正当な理由による場合を除き、他人の識別符号を提供する行為を禁止及び処罰する。

ウ 他人の識別符号を不正に取得する行為の規制

不正アクセス行為の用に供する目的で、他人の識別符号を取得する行為を禁止及び処罰する。

エ 他人の識別符号を不正に保管する行為の規制

不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管する行為を禁止及び処罰する。

5 法令の名称・関連条項とその内容

不正アクセス禁止法第3条（不正アクセス行為の禁止）及び第4条（不正アクセス行為を助長する行為の禁止）

6 想定される代替案

4(3)に掲げる各行為について行わないことをそれぞれ努力義務とする。

7 規制の費用

(1) 遵守費用

改正案、代替案のいずれを前提とした場合であっても、遵守費用は発生しない。

(2) 行政費用

改正案を前提とした場合には、規制を導入しないときと比較し、違反行為の取締りに係る費用が発生するが、代替案を前提とした場合には、これは発生しない。

(3) その他の社会的費用

改正案、代替案のいずれを前提とした場合であっても、その他の社会的費用は発生

しない。

8 規制の便益

改正案を前提とした場合、4(3)に掲げる各行為を禁止し、違反者に対する取締りを行うことで、他人の識別符号の不正流通が防止され、不正アクセス行為を未然に防止することができることと期待される。これに対し、代替案を前提とした場合には、違反した場合の罰則による強制力のない努力義務では実効性を担保できないことから、改正案と同程度の便益は期待できない。

9 政策評価の結果（費用と便益の関係の分析等）

改正案を前提とした場合、取締りに係る費用が発生するものの、4(3)に示した各行為を禁止することで、他人の識別符号の不正流通が防止され、不正アクセス行為を未然に防止することが期待できる。また、当該費用は、規制により得られる便益と比較して正当化される範囲内のものであると考えられる。

これに対し、代替案を前提とした場合、費用は発生しないが、他人の識別符号の不正流通は防止されず、不正アクセス行為を未然に防止することができない。

このため、本改正案の導入は適切であると考えられる。

10 有識者の見解その他の関連事項

平成23年6月から、社会全体として不正アクセス防止対策を推進するに当たり、現状の課題と改善方策に係る官民の幅広い意見を集約するため「官民意見集約委員会（官民ボード）」を設置し、幅広く検討が行われ、平成23年12月に「不正アクセス防止対策に関する行動計画」が策定されたところ、その中で、他人の識別符号の不正取得行為、提供行為及びフィッシング行為の法規制化について検討することとされている。

11 レビューを行う時期又は条件

改正法の施行後、不正アクセス行為が増加しているにもかかわらず、本規制による検挙によっても不正アクセス行為の未然防止につながっていないなど、本規制の適用状況及び不正アクセス行為の発生状況等を勘案し、必要と認められる時期にレビューを行う。