

平成15年上半期の不正アクセス行為の発生状況等について

平成15年上半期に全国の都道府県警察から警察庁に報告のあった不正アクセス行為が対象である。

なお、 が付された語句については、本文最後で説明している。

1 不正アクセス行為の発生状況及びその特徴

(1) 認知件数 (1) (2)

平成15年上半期の不正アクセス行為は114件で、前年同期の94件と比較して、20件増加した。

	平成12年		平成13年		平成14年		平成15年 上半期
	通年	法施行後 半年(注)	通年	上半期	通年	上半期	
認 知 件 数	106	35	1,253	959	329	94	114
海外からのアクセス	25	14	448	418	13	4	21
国内からのアクセス	73	20	258	165	286	71	83
アクセス元不明	8	1	547	376	30	19	10

注 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。）の施行日である平成12年2月13日から平成12年8月12日までの間をいう。以下同じ。

不正アクセス行為の認知件数は、自己増殖型プログラム（ワーム）によるホームページ書き換え事案（813件）等の事案が増加した平成13年を除き、不正アクセス禁止法を施行した平成12年から、増加傾向にある。

(2) 被害に係る特定電子計算機のアクセス管理者 (3)

被害に係る特定電子計算機のアクセス管理者を見ると、プロバイダが48件と最も多く、次いで一般企業の42件となっている。

被害に係る特定電子計算機の アクセス管理者	平成12年		平成13年		平成14年		平成15年 上半期
	通年	法施行後半年	通年	上半期	通年	上半期	
プロバイダ(注1)	59	18	182	75	243	55	48
大学、研究機関等(注2)	8	2	101	81	3	2	11
一般企業	25	12	429	330	62	25	42
その他	14	3	139	71	21	12	13
うち行政機関(注3)	-	-	-	-	12	8	2
不 明	0	0	402	402	0	0	0
計	106	35	1,253	959	329	94	114

注1 「プロバイダ」とは、インターネットに接続する機能を提供する事業者をいう。

- 2 「大学、研究機関等」には、大学、高等学校等の学校機関及びその附置機関を含む。
- 3 「その他」の「うち行政機関」には、国の行政機関、独立行政法人、特殊法人、地方公共団体及びこれらの附属機関を含む。

なお、平成12年及び13年は「その他」の内訳の集計をしていない。

(3) 認知の端緒

認知の端緒としては、警察職員によるいわゆるサイバーパトロールや被疑者の取調べ等の警察活動が65件と最も多く、次いで利用権者（ 4 ）からの届出が31件、発見者からの通報が12件、アクセス管理者からの届出が6件の順となっている。

認 知 の 端 緒	平成12年		平成13年		平成14年		平成15年
	通年	法施行後半年	通年	上半期	通年	上半期	上半期
アクセス管理者からの届出	30	15	168	74	47	19	6
利用権者からの届出	23	7	118	22	92	34	31
警 察 活 動	35	10	930	851	185	40	65
発 見 者 からの 通 報	7	2	21	12	0	0	12
そ の 他	11	1	16	0	5	1	0
計	106	35	1,253	959	329	94	114

(4) 不正アクセス行為後の行為

不正アクセス行為後の行為としては、ホームページの改ざんが30件、電子メールの盗み見等の情報の不正入手も30件で、ともに最も多く、他にインターネット・オークションの不正操作（他人になりすましての入札、販売代金の取得等）が14件、オンラインゲームの不正操作（アイテムの移動やキャラクターの消去等）が10件、インターネットの利用が4件等であった。

2 不正アクセス禁止法違反事件の検挙状況

不正アクセス禁止法違反の検挙事件数(5)は33事件(84件)、検挙人員は37人で、前年同期に比べ検挙事件数は6事件(21件)増加し、検挙人員は5人減少した。その内訳は、不正アクセス行為が33事件(83件)、37人であり、不正アクセス助長行為は1事件(1件)、1人であった。

不正アクセス行為の態様については、32事件(82件)が識別符号窃用型(6)であり、1事件(1件)がセキュリティ・ホール攻撃型(7)であった。

なお、検挙人員37人中29人が成人であり、8人が少年であった。

		平成12年		平成13年		平成14年		平成15年 上半期
		通年	法施行後半年	通年	上半期	通年	上半期	
不正アクセス 行為	検挙事件数	30	8	35	13	51	27	33
	検 挙 件 数	62	14	66	17	102	62	83
	検 挙 人 員	34	8	51	15	68	42	37
不正アクセス 助長行為	検挙事件数	4	2	1	0	2	1	1
	検 挙 件 数	5	2	1	0	3	1	1
	検 挙 人 員	5	2	1	0	3	1	1
計 (注)	検挙事件数	31 (重複3)	9 (重複1)	35 (重複1)	13	51 (重複2)	27 (重複1)	33 (重複1)
	検 挙 件 数	67	16	67	17	105	63	84
	検 挙 人 員	37 (重複2)	9 (重複1)	51 (重複1)	15	69 (重複2)	42 (重複1)	37 (重複1)

注 重複計上あり。

3 検挙事例

1	セキュリティ・ホール攻撃によりホームページを改ざんした不正アクセス禁止法違反事件
---	---

高校生（15）が、自己の技量試しや愉悦感を味わう目的で、平成14年11月から15年4月までの間、Webサーバのホームページ管理プログラムに存在するセキュリティ・ホールを攻撃する手法等により、約23カ国・地域の140のWebサーバに不正アクセスしてホームページを改ざんした。15年6月、不正アクセス禁止法違反で検挙した（警視庁）。

2	インターネット・バンキング利用の不正送金に係る不正アクセス禁止法違反、私電磁的記録不正作出・同供用及び電子計算機使用詐欺事件
---	---

無職の男（35）が、他人の口座から金を不正に得る目的で、平成14年9月、銀行のインターネット・バンキング用の認証サーバに、あらかじめキーロガー（8）を用いて収集していた口座開設者5人のID及びパスワードを使用して不正アクセスし、うち1名の口座から、他の銀行に開設していた架空名義の口座へ約1,650万円の送金操作を行い、現金自動預払機から、同口座の現金1,600万円を引き出して窃取した。15年3月、不正アクセス禁止法違反、電子計算機使用詐欺、私電磁的記録不正作出・同供用、組織的犯罪処罰法違反（犯罪収益隠匿）などで、現金の引出操作をした会社員の男（27）と合わせて2人を検挙した（警視庁）。

3	インターネット・オークションに係る識別符号の販売を目的とした不正アクセス禁止法違反事件
---	--

無職の男（40）が、他人が使用するインターネット・オークション用のID及びパスワードを第三者に提供して不正に金を得る目的で、平成14年9月から11月までの間、多数のIDに対してパスワードを推測して入力する操作を行い、合致した15件のID及びパスワードにより、オークションサービスのサーバに不正アクセスした。15年5月、不正アクセス禁止法違反で検挙した（京都）。

4	インターネット・オークションの識別符号を窃用した不正アクセス禁止法違反及び詐欺事件
---	--

自営業の男（32）ら男女5人が、インターネット・オークションを利用して金をだまし取る目的で、平成14年5月から11月までの間、他人が使用するオークションサービス用ID164個のパスワードを推知して不正アクセスしたうえ、当IDを使用して架空のオークション出品操作を行い、偽名で開設した口座に現金を振り込ませる手口で、約39

0名から総額約1,200万円をだまし取った。平成14年12月、男2人を詐欺で検挙し、平成15年6月までに別の男1人女2人とともに、不正アクセス禁止法違反、詐欺、有印私文書偽造・同行使、組織的犯罪処罰法違反（犯罪収益等収受）で追送致した。（茨城、広島）

5

インターネット・オークションの識別符号を窃用して入札操作を行った不正アクセス禁止法違反及び私電磁的記録不正作出・同供用事件

無職の女（28）が、インターネット・オークションで取引した相手に嫌がらせをする目的で、平成15年1月、取引相手のオークションサービス用ID及びパスワードを使用してオークションサービスのサーバに不正にアクセスし、出品物15点に対して入札操作を行い、虚偽の入札情報を不正に作出した。15年5月、不正アクセス禁止法違反及び私電磁的記録不正作出・同供用で検挙した（福井、北海道）。

6

企業の業務用電子メールの盗み見に係る不正アクセス禁止法違反及び電子掲示板を利用した名誉毀損事件

会社員の男（45）が、元勤務先の商社を解雇させられたことを恨み、嫌がらせをする目的で、平成14年6月から9月までの間、同商社の社員7人が業務で使用する電子メール用のIDとパスワードを使用し、メールサーバに不正アクセスして電子メールの内容を盗み見したうえで、無料のインターネット電子掲示板に、商社の事業に関する内容虚偽の文言を投稿掲示した。平成15年1月、不正アクセス禁止法違反及び名誉毀損で検挙した（奈良）。

7

リマインダ機能（ 9 ）を利用して入手したパスワードの使用による出会い系サイトに係る不正アクセス禁止法違反

会社員の男（31）が、自己が開設したホームページを女性が開設したかのように装って閲覧者を増やす目的で、平成14年11月、リマインダ機能を利用して出会い系サイトの女性会員のパスワードを入手し、出会い系サイトの認証サーバに不正アクセスして、女性会員のプロフィール情報として自己のホームページのアドレスを登録した。また、別の会社員の男（27）が、出会い系サイトの女性会員の会員登録情報を盗み見る目的で、平成14年12月、上記女性会員のパスワードをリマインダ機能を利用して入手し、不正アクセスした。平成15年5月、6月、不正アクセス禁止法違反でそれぞれ検挙した（京都）。

8

インターネット・オンラインゲームに係る不正アクセス禁止法違反事件

中学生（14）が、インターネット・オンラインゲーム上で、友人の操るゲームキャラクターが持つ装備品を不正に入手する目的で、友人のID及びパスワードを使用して、オンラインゲームの認証サーバに不正アクセスし、装備品を自己が操るゲームキャラクターが所持するように移動させた。15年2月、不正アクセス禁止法違反で検挙した（神奈川）。

4 検挙事件の特徴

(1) 犯行の手口

検挙した不正アクセス行為のほとんど（32事件（78件））が識別符号窃用型であったが、当該識別符号（ID及びパスワード）の入手方法については、利用権者のパスワードの設定・管理の甘さにつけ込んだもの（ID等から容易に推知されるパスワードが利用されていたものなど）が前年同期と同じく最も多く、16事件（60件）であった。次いで元従業員等の立場上、識別符号を知りうる立場にあった者によるものが9事件（9件）であるほか、リマインダ機能における質問への安易な回答が設定されていたものが1事件（3件）、利用権者が話すのを聞いたものが1事件（1件）、利用権者から言葉巧みに聞き出したものが1事件（1件）等、特に高度な技術を有していない者でも行える形態が多かった。

しかし、プログラムの脆弱性を利用したホームページの改ざんのように、セキュリティの脆弱性を突くセキュリティ・ホール攻撃型も引き続きみられたほか、キーロガーを使用してIDを入手するなど、高度なコンピュータ技術を悪用したものもあった。

(2) 被疑者

アクセス管理者及び利用権者にとって、全くの他人による犯行は13事件（63件）、元交際相手や元従業員等顔見知りの者による犯行は11事件（11件）であり、実際には会ったことがないネットワーク上のみの知り合いによる犯行は8事件（8件）であった。（1事件は、利用権者と顔見知りの者及び他人の組み合わせの被疑者である。）

また、検挙した被疑者の年齢は、30代が14人と最も多く、次いで20代が10人、10代が8人、40代が5人の順となっており、20代以下の割合は約5割を占めた。最年少の者は14歳であり、最年長の者は48歳であった。

(3) 犯行の動機

不正アクセス行為の動機としては、嫌がらせや仕返しのためが最も多く、元交際相手や元勤務先等に対するもののほか、気を紛らわすための無差別な嫌がらせも含め13事件（13件）であった。次いで不正に金を得るためが9事件（58件）、好奇心や自己の技量を計るために試みるものが7事件（23件）、メールを盗み見るためが2事件（4件）、ゲームのアイテム等を入手するためが2事件（2件）、自分のIDにはない機能を利用したかったため1事件（1件）の順となっている（重複計上あり）。

前年同期と比べると、嫌がらせや仕返しのためは13事件（13件）で変わらないが、好奇心や技量試しのためは1事件（3件）減少し、不正に金を得るためは7事件（52件）増加した。

(4) 利用されたサービス

識別符号窃用型の不正アクセス行為で検挙した32事件（82件）において、当該識別符号を入力することにより利用できるサービス別に見ると、電子メール・サービスが7事件（7件）と最も多く、次いでインターネット・オークション・サービスが6事件（6件）、インターネットのオンラインゲーム・サービスが6事件（6件）、掲示板等会員専用サイトの閲覧が4事件（22件）、ホームページ公開サービスが4事件（4件）、インターネット接続サービスが2事件（2件）、インターネット・バンキングが1事件（5件）等となっている。

(5) その他

不正アクセス禁止法違反のほか、他の罪についても検挙した事件は、9事件であった。

	事件数
覚せい剤取締法違反	1
麻薬及び向精神薬取締法違反	1
詐欺	1
窃盗	1
名誉毀損	1
わいせつ図画販売目的所持	1
電子計算機使用詐欺	1
電子計算機損壊等業務妨害	1
私電磁的記録不正作出・同供用	2
恐喝	1
組織犯罪処罰法違反	1
児童買春・児童ポルノ禁止法違反	1

注 重複計上あり。

5 都道府県公安委員会による援助措置

都道府県公安委員会は、不正アクセス行為を受けたアクセス管理者からの申出への対応として、不正アクセス禁止法第6条の援助規定に基づくアクセス管理者に対する助言・指導を4件（北海道1、宮城1、愛知1、佐賀1）実施した。

6 防御上の留意事項

(1) サーバの適切な管理

セキュリティ・ホール攻撃型の不正アクセス行為の発生は減少傾向にあるが、この種手口による事犯は、一旦発生すれば被害が大きくなる危険があることから、引き続き必要なセキュリティ水準の維持・向上が必要であり、特にサーバの管理者等はインターネット上などで常にセキュリティ情報を確認し、使用しているオペレーティングシステム又はアプリケーションプログラムにセキュリティ・ホールが発見されたことを知ったときは、速やかに修正プログラムをインストールするなどセキュリティ・ホールを解消するための措置を講じる必要がある。

(2) 識別符号等の適切な設定・管理

ア パスワード

識別符号窃用型の不正アクセス行為で検挙した32事件(82件)中、16事件(60件)では、パスワードがIDから容易に推知できるもの(IDが「keisatsu1234」に対して、パスワードが「keisatsu」や「1234」など)等であったことから、利用権者においては、他人による推知が難しいパスワードを設定する必要がある。

また、9事件(9件)が、かつて当該パスワードを管理していた者や、利用権者のパスワードを覗き見することができた者の犯行であり、アクセス管理者及び利用権者がパスワードの設定・管理を適切に行っていなかったことが問題点として挙げられる。利用権者等においては、パスワードを定期的に変更するなど識別符号を適切に設定・管理する必要がある。

イ リマインダ機能

リマインダ機能を悪用して、アクセス管理者からパスワードを入手する手口が引き続き見られた。アクセス管理者及び利用権者においては、パスワード再発行時に必要となる情報(質問に対する回答)について、他人による推察が困難となるような仕組み及び内容とする必要がある。

ウ キーロガーによるIDの入手

インターネット・カフェ等のパソコン端末に、キーボードの打鍵文字を記録するプログラムを仕掛け、インターネット・バンキングのIDやパスワードを入手する手口が見られたため、不特定多数の人が利用できるような端末では、個人情報等の入力を伴うサービスを利用しないようにする必要がある。

(3) その他

ア 不特定多数の人が利用できる端末の管理

インターネット・カフェ等の不特定多数の人が利用できる端末の管理者及び運営者は、個人情報等の入力については十分注意を払うよう利用者に注意喚起を行うとともに、不必要な履歴の削除や利用者に対するプログラムのインストールの制限等を実施することが必要である。

イ アクセス管理者

アクセス管理者は、サーバを適切に管理するだけでなく、利用権者に対して識別符号の適切な設定・管理について注意喚起を行うほか、容易に推知されるおそれの

あるパスワードを設定できないようにする仕組みを活用するなど、不正アクセス行為を防止するために必要な措置を講ずる必要がある。

(参考)

1 認知

認知とは、被害届出の受理をした場合のほか、余罪として発覚した場合、報道を踏まえて確認した場合、援助の申出を受理した場合その他関係資料により不正アクセス行為の事実確認ができた場合をいうものとしている。

2 件数

件数とは、犯罪構成要件に該当する行為を被疑者が行った数をいう。

なお、不正アクセス行為の件数の計上については、ひとつのアクセス制御機能に対するひとつの手口による侵害行為が1回あったことをもって1件としている。ただし、被疑者が異なる場合(共犯を除く。)はそれぞれ1件として計上し、短期間にひとつのアクセス制御機能に対して同一手口による侵害が連続的に行われ、実質上1回の行為とみなしうる場合は包括して1件としている。

3 アクセス管理者

アクセス管理者とは、ネットワークに接続しているコンピュータを誰に利用させるかを決定する者をいう。

例えば、インターネットへの接続や電子メールの受信についてはプロバイダが、インターネットショッピング用のホームページの閲覧についてはその店主が、それぞれアクセス管理者である。

4 利用権者

利用権者とは、ネットワークに接続されたコンピュータをネットワークを通じて利用することについて、当該コンピュータのアクセス管理者の許諾を得た者をいう。

例えば、プロバイダからインターネット接続サービスを受けることを認められた会員や、企業からLANを利用することを認められた社員が該当する。

5 事件数

事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合も1事件と数える。

6 識別符号窃用型

アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為(不正アクセス禁止法第3条第2項第1号に該当する行為)をいう。

例えば、他人のインターネット・オークション用のID及びパスワードを使用して、当該インターネット・オークションを利用する行為が該当する。

7 セキュリティ・ホール攻撃型

アクセス制御されているサーバに、ネットワークを通じて情報（他人の識別符号を入力する場合を除く。）や指令を入力して不正に利用する行為（不正アクセス禁止法第3条第2項第2号又は第3号に該当する行為）をいう。

例えば、バッファ・オーバーフロー攻撃による不正アクセス行為が該当する。

8 キーロガー

インストールしたパソコン端末において、キーボードでどの文字を打鍵したかを記録するプログラムである。

9 リマインダ機能

利用権者がパスワードを忘れてしまった時に、アクセス管理者が何らかの方法で本人確認を行った上でパスワードを再発行する機能である。本人確認の方法としては、サービス利用のための登録時に、本人が決めた情報を登録しておき、パスワードの再発行時にその情報を利用権者に入力させるもの（例えば、「出身小学校は？」等の質問に対して、あらかじめ登録しておいた情報を答えとして入力すると、パスワードが再発行される）などがある。