

## 平成16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16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16年上半期の不正アクセス行為は198件で、前年同期の114件と比較して、84件増加した。

	平成12年	平成13年	平成14年	平成15年		平成16年
				上半期	上半期	
認 知 件 数	106	1,253	329	212	114	198
海外からのアクセス	25	448	13	35	21	20
国内からのアクセス	73	258	286	158	83	172
アクセス元不明	8	547	30	19	10	6

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年以降減少していたものの、再び増加傾向にある。

#### (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、一般企業が123件と最も多く、次いでプロバイダの56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		平成16年
				上半期	上半期	
プ ロ バ イ ダ(注1)	59	182	243	98	48	56
一 般 企 業	25	429	62	76	42	123
大学、研究機関等(注2)	8	101	3	16	11	2
そ の 他	14	139	21	22	13	17
うち行政機関(注3)	-	-	12	3	2	8
不 明	0	402	0	0	0	0
計	106	1,253	329	212	114	198

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95件と最も多く、次いで利用権者（ 4 ）からの届出が80件、アクセス管理者からの届出が20件、発見者からの通報が1件となっている。

認 知 の 端 緒	平成12年	平成13年	平成14年	平成15年		平成16年
				上半期	上半期	
アクセス管理者からの届出	30	168	47	12	6	20
利用権者からの届出	23	118	92	78	31	80
警 察 活 動	35	930	185	100	65	95
発見者からの通報	7	21	0	19	12	1
そ の 他	11	16	5	3	0	2
計	106	1,253	329	212	114	198

### (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、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99件で最も多く、次いでインターネット・オークションの不正操作（他人になりすましての出品・入札等）が45件であり、他にホームページの改ざんが20件、電子メールの盗み見等の情報の不正入手が12件、不正ファイルの蔵置（フィッシング（ 5 ）用ホームページデータの蔵置等）が5件、利用権者のパスワード変更が5件等であった（重複計上あり）。

## 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（ 6 ）は27事件（66件） 検挙人員は39人で、前年同期に比べ検挙事件数は6事件（18件）減少し、検挙人員は2人増加した。すべての検挙が不正アクセス行為によるものであり、不正アクセス助長行為の検挙はなかった。

不正アクセス行為の態様については、識別符号窃用型（ 7 ）が25事件（59件）であり、セキュリティ・ホール攻撃型（ 8 ）が3事件（7件）であった（うち1事件は、識別符号窃用型とセキュリティ・ホール攻撃型の両方の行為が行われた。）。

なお、検挙人員39人中24人が成人であり、15人が少年であった。

		平成12年	平成13年	平成14年	平成15年		平成16年 上半期
					上半期	上半期	
不正 アクセス 行為	検挙事件数	30	35	51	58	33	27
	検挙件数	62	66	102	143	83	66
	検挙人員	34	51	68	76	37	39
不正 アクセス 助長行為	検挙事件数	4	1	2	2	1	0
	検挙件数	5	1	3	2	1	0
	検挙人員	5	1	3	2	1	0
計 (注)	検挙事件数	31 (重複3)	35 (重複1)	51 (重複2)	58 (重複2)	33 (重複1)	27
	検挙件数	67	67	105	145	84	66
	検挙人員	37 (重複2)	51 (重複1)	69 (重複2)	76 (重複2)	37 (重複1)	39

## 3 検挙事例

1	セキュリティ・ホール攻撃を利用した個人情報の記録ファイルの取得方法の公表に係る不正アクセス禁止法違反及び威力業務妨害事件
---	--

公務員の男（40）が、社団法人が一般からの情報受付のために公開したホームページに係るセキュリティ・ホールを指摘する目的で、平成15年11月、公開のイベント会場において、セキュリティ・ホールを攻撃する手法により社団法人のWebサーバに不正アクセスし、個人情報を記録したデータファイルを取得する手法を実演して、多数の参加者に公表した。16年2月、不正アクセス禁止法違反及び威力業務妨害で検挙した。さらに、16年3月、同手法をまねて同社団法人のWebサーバに不正アクセスしたイベント参加者の会社員ら3人を不正アクセス禁止法違反で検挙した（警視庁）。

2	キーロガー（ 9 ）を使用して入手した識別符号を窃用した不正アクセス禁止法違反事件
---	---

無職の男（31）が、大学内の学生用インターネット端末を使用して、部外者には許されていないインターネット利用をする目的で、平成15年10月、学生用端末にキーロガーを仕掛けて入手した学生2人のID及びパスワードを使用して不正アクセスし、インターネットに接続してホームページの閲覧等をした。16年1月、不正アクセス禁止法違反で検挙した（佐賀）。

3

**不正登録IDの使用及びシステム管理者の識別符号の窃用等による不正アクセス禁止法違反事件**

大学職員の男（47）が、不本意な職務替えをうらみ、学内ネットワークの運用を混乱させることを目的に、平成15年10月から12月までの間、勤務先の学内用メールサーバに、元システム管理者であったことを利用して不正登録したIDを使用して不正アクセス（法第3条第2項第2号）し、システム管理者の電子メールを盗み見て、学内ネットワークの管理者用のIDとパスワードを入手し、同ID及びパスワードを窃用して学内ネットワークの認証サーバに不正アクセス（法第3条第2項第1号）し、利用停止となっていたIDを管理者権限で利用可能な状態にした後、同IDを使用して学内ネットワークのWebサーバに不正アクセス（法第3条第2項第2号）し、学内用電子掲示板のデータを消去するなどした。16年5月、不正アクセス禁止法違反で検挙した（警視庁）。

4

**識別符号通知プログラムを使用して収集した識別符号の窃用によるオンラインゲーム・サービスに係る不正アクセス禁止法違反事件**

コンピュータ保守管理作業員の男（20）が、オンラインゲームで使用するアイテムを他人から不正に取得する目的で、平成14年12月から15年7月までの間、ID及びパスワードを自動的に通知する自作のプログラムを電子掲示板等で機能を偽って配付し、同プログラムの使用者から収集したオンラインゲーム・サービスのID及びパスワードを窃用して不正アクセスし、他のオンラインゲーム利用者が保有していたアイテムを、不正に自己の保有となるよう移動させた。16年3月、不正アクセス禁止法違反で検挙した（北海道、埼玉、熊本）。

5

**電子メール等により言葉巧みにだまして入手した識別符号の窃用によるオンラインゲーム・サービスに係る不正アクセス禁止法違反事件**

中学生（14）らが、オンラインゲームで使用するアイテムを他人から不正に取得する目的で、平成15年8月ころから11月までの間、電子メール等を利用して「アイテムを譲る」等と言葉巧みに持ちかけてだます方法で、他人が使用するオンラインゲーム・サービス用ID15個のパスワードを入手して不正アクセスした上、他人が保有するアイテム

を不正に自己の保有となるよう移動させた。16年4月、不正アクセス禁止法違反で2人を検挙した（京都）。

6

**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**

無職の男（31）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15年8月から16年1月までの間、他人が使用するオークションサービス用ID12個のパスワードを推知して不正アクセスし、当該IDを出品者IDと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等に現金を振り込ませる手口で、31名から総額約400万円をだまし取った。平成16年2月、不正アクセス禁止法違反、詐欺、私電磁的記録不正作出・同供用で検挙した（埼玉、山形、茨城、京都、岡山）。

7

**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（44）が、他人の口座から金を不正に得る目的で、平成15年10月、銀行のインターネット・バンキング用の認証サーバに、在職時に業務上で知り得た勤務先会社名義の口座のオンライン取引にかかる暗証番号等を使用して不正アクセスし、配偶者名義の口座へ510万円の送金操作を行い、同口座から現金を引き出した。16年2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・同供用で検挙した（警視庁）。

8

**リマインダ機能（10）を利用した電子メール・サービス及びオンラインゲーム・サービスに係る不正アクセス禁止法違反事件**

大学生の男（19）が、ゲームの結果奪われたオンラインゲーム用のアイテムを取り返す目的で、平成15年12月、リマインダ機能を利用して相手の使用する電子メールアドレスに係るパスワードを入手した上で、オンラインゲーム・サービスのリマインダ機能を利用して、オンラインゲームに係るパスワードを同電子メールアドレス宛にメール送信させて入手し、オンラインゲーム・サービスのサーバに不正アクセスして、奪われたアイテムを不正に自己の保有となるよう移動させた。16年2月、不正アクセス禁止法違反で検挙した（千葉）。

9

**電子メールアドレスの入手を目的とした不正アクセス及びいわゆる架空請求メールに係る不正アクセス禁止法違反及び詐欺事件**

出会い系サイト運営者の男(33)ら3人が共謀し、運営している出会い系サイトの宣伝・勧誘の電子メールを送信するための電子メールアドレスを入手する目的で、平成15年10月、他人が運営する出会い系サイトの会員管理用のパスワードを元従業員の男(29)から聞き出した上で、別の男(38)に作成させた電子メールアドレス等の自動抽出プログラムを使用して不正アクセスし、他人運営に係る出会い系サイトの会員情報を入手した。また、プログラムを作成した男が単独で、いわゆる架空請求メールを送信し、他人名義の口座に振り込ませる手口で81名から約200万円をだまし取った。16年5月、不正アクセス禁止法違反で4人を検挙し、6月、不正アクセス禁止法違反及び詐欺で1人を検挙した(鹿児島)。

## 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多く(25事件(59件))が識別符号窃用型であった。

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、9事件(30件)であった。次いで、元従業員や友人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7事件(8件)、言葉巧みにメール等で聞き出したものが2事件(8件)、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1事件(2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情報の不正取得のように、セキュリティの脆弱性を突くセキュリティ・ホール攻撃型が3事件(7件)(うち1事件は、識別符号窃用型とセキュリティ・ホール攻撃型の両方の行為が行われた。)識別符号窃用型のうちキーロガー等の不正プログラムを使用してIDを入手したものが3事件(7件)と、高度なコンピュータ技術を悪用するものも増加している。

### (2) 被疑者

アクセス管理者及び利用権者にとって、全く面識のない他人による犯行は12事件(47件)、元交際相手や元従業員等顔見知りの者による犯行は10事件(13件)(うち1事件(1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。)であり、ネットワーク上の知り合いによる犯行は5事件(6件)であった。

また、検挙した被疑者の年齢は、10代が15人と最も多く、次いで20代が10人、30代が8人、40代が6人の順となっており、20代以下の割合が6割以上を占めた。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、ゲームのアイテム等を不正取得するため8事件(29件)と最も多く、次いで嫌がらせや仕返しのため6事件(9件)、好奇心を満たすため又はいたずらが5事件(8件)、不正に金を得るため3事件(14件)、情報を不正に入手するため2事件(3件)、料金の請求を免れるため2事件(3件)等となっている。

前年同期と比べると、嫌がらせや仕返しのためは7事件(4件)、好奇心を満たすため又はいたずらが2事件(15件)、不正に金を得るためが6事件(44件)、それぞれ減少し、ゲームのアイテム等を不正取得するためが6事件(27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25事件(59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、インターネットのオンラインゲームが13事件(33件)と最も多く、次いで電子メールが4事件(5件)、インターネット・オークションが2事件(13件)、インターネット接続サービスが2事件(3件)、ホームページ公開サービスが1事件(1件)、インターネット・ショッピングが1事件(1件)、インターネット・バンキングが1事件(1件)等となっている(重複計上あり)。

#### (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、7事件であった。

	事件数
詐欺	3
電子計算機使用詐欺	2
私電磁的記録不正作出・同供用	2
威力業務妨害	1
恐喝未遂	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1件(愛知)実施した。

### 6 防御上の留意事項

#### (1) 利用権者の講ずべき措置等

##### ア パスワードの適切な設定・管理

識別符号窃用型の不正アクセス行為で検挙した25事件(59件)中、9事件(30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、7事件(8件)が、かつて当該パスワードを管理していた者や、利用権者の知人でパスワードを知ることができた者の犯行であるほか、2事件(8件)が言葉巧みにメール等で聞き出したものであるなど、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いことが問題点として挙げられる。

利用権者等においては、パスワードを不用意に教えない、また、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 リマインダ機能の適切な設定

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 不特定多数の人が利用できる端末を利用する際の注意

インターネット・カフェ等のパソコン端末に、キーロガーを仕掛け、IDやパスワード等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、IDやパスワードをはじめ、口座番号やクレジットカード番号、個人情報等の入力を伴うサービスを出来るだけ利用しないようにする必要がある。

### (2) アクセス管理者の講ずべき措置等

#### ア セキュリティ・ホールに関する対策

セキュリティ・ホール攻撃型の不正アクセス行為の発生が増加しており、また、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、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で公表される最新の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。

#### イ 不特定多数の人が利用できる端末の適切な管理

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場所におけ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、リカバリーソフト（コンピュータ内の情報を利用前の状態に戻すソフト）の導入、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の措置を実施することが必要である。

#### ウ その他

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 特定電子計算機のアクセス管理者

特定電子計算機とは、ネットワークに接続されたコンピュータをいい、アクセス管理者とは、特定電子計算機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 フィッシング

銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジット番号、ID、パスワード等）を入力させるなどして個人の金融情報を不正に入手するような行為をいう。その情報を元に金銭をだまし取る手口がフィッシング詐欺といわれる。

### 6 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。

### 7 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。

### 8 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、IDを不正に登録して使用する行為や、セキュリティの脆弱性について操作指令を与える等の手法による不正アクセス行為が該当する。

#### 9 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。

#### 10 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、「ペットの名前は？」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。