

平成18年上半期の不正アクセス行為の発生状況等について

1 不正アクセス行為の発生状況

(1) 認知件数

平成18年上半期の不正アクセス行為の認知件数は383件で、前年と比べ、66件増加した。

なお、平成13年中の不正アクセス行為の多発は、ホームページ書換えプログラム（コンピュータ・ワーム）の蔓延によるものである。

表1 - 1 不正アクセス行為の認知件数の推移

	平成	平成	平成	平成	平成	平成17年		平成18年
	12年	13年	14年	15年	16年	上半期	上半期	上半期
認知件数（件）	106	1,253	329	212	356	592	317	383
海外からのアクセス	25	448	13	35	37	53	31	14
国内からのアクセス	73	258	286	158	303	487	265	341
アクセス元不明	8	547	30	19	16	52	21	28

平成12年の数字は、不正アクセス禁止法の施行日である平成12年2月13日から12月31日までの間のものである。（以下同じ）

(2) 被害に係る特定電子計算機のアクセス管理者（注1）

被害に係る特定電子計算機のアクセス管理者をみると、プロバイダが最も多く（312件）、次いで一般企業（60件）となっている。

表1 - 2 被害を受けた特定電子計算機のアクセス管理者の推移（単位：件）

被害に係る特定電子計算機に係るアクセス管理者	平成	平成	平成	平成	平成	平成17年		平成18年
	12年	13年	14年	15年	16年	上半期	上半期	上半期
プロバイダ	59	182	243	98	126	356	166	312
一般企業	25	429	62	76	202	203	132	60
大学、研究機関等	8	101	3	16	6	12	7	6
その他	14	139	21	22	22	21	12	5
うち行政機関	-	-	12	3	12	17	10	1
不明	0	402	0	0	0	0	0	0
計	106	1,253	329	212	356	592	317	383

「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電気通信事業者をいう。

「大学、研究機関等」には、高等学校等の学校機関及びその附置機関を含む。

「その他」の「うち行政機関」には、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、利用権者（注2）からの届出によるものが最も多く（180件）、次いで警察職員によるサイバーパトロール、被疑者の取調べ等の警察活動によるもの（174件）、被害を受けた特定電子計算機のアクセス管理者からの届出によるもの（26件）、発見者からの通報によるもの（2件）の順となっている。

表1 - 3 認知の端緒の推移

認知の端緒（件）	平成	平成	平成	平成	平成	平成17年		平成18年
	12年	13年	14年	15年	16年		上半期	上半期
アクセス管理者からの届出	30	168	47	12	29	30	12	26
利用権者からの届出	23	118	92	78	172	505	270	180
警察活動	35	930	185	100	146	33	17	174
発見者からの通報	7	21	0	19	7	14	11	2
その他	11	16	5	3	2	10	7	1
計	106	1,253	329	212	356	592	317	383

(4) 不正アクセス行為後の行動

不正アクセス行為後の行動としては、インターネット・オークションに関する不正操作（他人になりすましての出品・入札等）が最も多く（312件）、次いでオンラインゲームの不正操作（他人のアイテムの不正取得等）（31件）、インターネットバンキングの不正送金・不正出金（20件）、ホームページの改ざん・消去（12件）、不正ファイルの蔵置（不正なプログラムやフィッシング（注3）用ホームページデータの蔵置等）（3件）、情報の不正入手（電子メールの盗み見等）（2件）の順となっている。

表1 - 4 不正アクセス行為後の行動の内訳

不正アクセス行為後の行動	件数（件）
インターネット・オークションに関する不正操作	312
オンラインゲームの不正操作	31
インターネットバンキングの不正送金・不正出金	20
ホームページの改ざん・消去	12
フィッシングサイト等不正ファイルの蔵置	3
情報の不正入手	2
その他	3

2 不正アクセス禁止法違反事件の検挙状況

(1) 検挙事件数等

平成18年上半期における不正アクセス禁止法違反の検挙件数は265件、検挙人員は63人と、前年同期と比べ、それぞれ67件・5人増加した。また、検挙件数、検挙人員の内訳をみると、不正アクセス行為に係るものがそれぞれ264件・63人、不正アクセス助長行為に係るものがそれぞれ1件・1人であった。

表2 - 1 検挙事件数等の推移

		平成	平成	平成	平成	平成	平成17年		平成18年
		12年	13年	14年	15年	16年	上半期	上半期	
不正アクセス 行 為	検挙事件数 (注4)	30	35	51	58	65	94	47	43
	検挙件数	62	66	102	143	142	271	196	264
	検挙人員	34	51	68	76	88	113	58	63
不正アクセス 助長行為	検挙事件数	4	1	2	2	0	6	2	1
	検挙件数	5	1	3	2	0	6	2	1
	検挙人員	5	1	3	2	0	6	2	1
計	検挙事件数 (事件)	31 (重複3)	35 (重複1)	51 (重複2)	58 (重複2)	65	94 (重複6)	47 (重複2)	43 (重複1)
	検挙件数 (件)	67	67	105	145	142	277	198	265
	検挙人員 (人)	37 (重複2)	51 (重複1)	69 (重複2)	76 (重複2)	88	116 (重複3)	58 (重複2)	63 (重複1)

(重複)とは、不正アクセス行為と不正アクセス助長行為の重複を示す。

(2) 不正アクセス行為の態様

検挙事件数を不正アクセス行為の態様別にみると、識別符号窃用型(注5)が43事件であり、セキュリティ・ホール攻撃型(注6)はなかった。

表2 - 2 不正アクセス行為の態様の推移

		平成	平成	平成	平成	平成	平成17年		平成18年
		12年	13年	14年	15年	16年	上半期	上半期	
識 別 符 号 窃 用 型	検挙事件数	29	33	46	56	62	90	45	43
	検挙件数	61	52	83	141	131	264	193	264
セ キ ュ リ テ ィ ・ ホ ール 攻 撃 型	検挙事件数	1	3	5	2	4	5	3	0
	検挙件数	1	14	19	2	11	7	3	0
計	検挙事件数 (事件)	30	35 (重複1)	51	58	65 (重複1)	94 (重複1)	47 (重複1)	43
	検挙件数 (件)	62	66	102	143	142	271	196	264

(重複)とは、識別符号窃用型とセキュリティホール攻撃型の重複を示す。

3 検挙事例

- | | |
|----------|--|
| 1 | インターネットサービス会社のホームページを複製したいわゆるフィッシングサイトで入手した識別符号で他人になりすまし同社オークションで架空出品して代金をだまし取った不正アクセス禁止法違反及び詐欺事件 |
|----------|--|

無職の男(34)らは、インターネットサービス会社の偽のログイン画面を設置し、同ログイン画面へ誘導する電子メールを同社会員に送信し、これを本物のログイン画面と誤信した会員が入力した識別符号を不正に入手した。当該識別符号を使用して同社のコンピュータに不正アクセス行為を行い会員になりすまし、同社オークションにおいて商品を売ると偽り多数の落札者から代金をだまし取った。平成18年5月、不正アクセス禁止法違反、詐欺罪で検挙した(京都、静岡、熊本)。

- | | |
|----------|---|
| 2 | 勤務先のインターネットカフェにキーロガー(注7)を仕掛けて入手した他人の識別符号を用いてオンラインゲーム上のアイテムを収集した不正アクセス禁止法違反事件 |
|----------|---|

会社員の男(26)は、オンラインゲーム上のアイテムを収集する目的で、勤務先のインターネットカフェのコンピュータにキーロガーを仕掛け、同店を利用した客の識別符号を入手し、平成17年1月、同店のコンピュータから客になりすまして当該オンラインゲーム会社のコンピュータに不正アクセス行為を行った。平成18年5月、不正アクセス禁止法違反で検挙した(岡山)。

- | | |
|----------|--|
| 3 | インターネットバンキングのセキュリティ対策ソフトウェアをかたったスパイウェア(注8)をCDで送りつけ識別符号を盗み取り、使用した不正アクセス禁止法違反、電子計算機使用詐欺及び電子計算機損壊等業務妨害事件 |
|----------|--|

無職の男(31)は、平成17年10月、インターネットバンキングを利用している法人に対して、インターネットバンキングのセキュリティ対策ソフトウェアをかたったスパイウェアを記録したCD-Rを送りつけ、同法人のインターネットバンキング利用に係る識別符号等を取得し、インターネットバンキングのコンピュータに不正アクセス行為を行って、同法人の口座から自己の管理する他人名義の口座に対して約300万円の送金操作を行った。また、スパイウェアが識別符号等を外部に送信させることによって、同法人の業務を妨害したものである。平成18年4月、不正アクセス禁止法違反、電子計算機使用詐欺罪及び電子計算機損壊等業務妨害罪で検挙した(千葉)。

4	オンラインゲーム会社のホームページを複製していわゆるフィッシングサイトを開設した不正アクセス禁止法違反及び著作権法違反事件
----------	--

中学生の男(14)は、オンラインゲーム会社のホームページを複製したフィッシングサイトを開設し、同ゲームの運営者を装い「違反行為をしたが反省文を入力すれば罰則を免除する」旨のメールを会員に送りつけ、当該フィッシングサイトに誘導し識別符号、反省文等を入力させ、平成18年2月から同年3月までの間、不正に入手した識別符号を使用して同ゲームのコンピュータに不正アクセス行為を行った。平成18年5月、不正アクセス禁止法違反及び著作権法違反で検挙した(警視庁)。

5	国家試験の受験申請データを見るために元勤務先の財団法人の識別符号を不正に使用した不正アクセス禁止法違反事件
----------	--

無職の男(61)は、平成18年2月、興味本位から元勤務先の財団法人が管理する国家試験受験申請用のコンピュータに、在職中に知り得た識別符号を使用して不正アクセス行為を行い、約6,100件の申請者データを読み出した。平成18年4月、不正アクセス禁止法違反で検挙した(警視庁)。

4 検挙事件の特徴

(1) 不正アクセス行為の手口

検挙した不正アクセス禁止法違反に係る不正アクセス行為のすべてが識別符号窃用型であった（43事件（264件））。その多くは、ID等から容易に推測されるパスワードが使用されていたなど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（18事件（115件））、識別符号を知り得る立場にあった元従業員、知人等によるもの（11事件（35件））、言葉巧みに利用権者から聞き出した又はのぞき見たもの（2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ものであったが、スパイウェア等の不正なプログラムを使用して、識別符号を入手したものの（3事件（4件））やフィッシングサイトを開設して識別符号を入手したものの（4事件（102件））があるなど、コンピュータ技術を悪用したり利用権者を誤信させたりするものも発生している。

表4 - 1 不正アクセス行為に係る犯行の手口の内訳

犯行の手口	事件数（事件）	件数（件）
識別符号窃用型	43	264
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	18	115
識別符号を知り得る立場にあった元従業員や知人等によるもの	11	35
フィッシングサイトにより入手したものの	4	102
スパイウェア等のプログラムを使用して識別符号を入手したものの	3	4
ファイル交換ソフトや暴露ウイルスで流出した識別符号を含む情報を利用したものの	2	3
言葉巧みに利用権者から聞き出した又はのぞき見たもの	2	2
他人から購入したものの	2	2
その他	1	1
セキュリティ・ホール攻撃型	0	0

(2) 被疑者

不正アクセス禁止法違反に係る被疑者についてみると、面識のない他人によるものが最も多く（29事件（243件））、次いで元交際相手や元従業員等の顔見知りの者によるもの（12事件（20件））、ネットワーク上のみの知り合いによるもの（2事件（2件））となっている。

また、被疑者の年齢についてみると、20歳代が最も多く（22人）、次いで30歳代（19人）、10歳代（14人）、40歳代（6人）、50歳代（1人）、60歳代（1人）の順となっている。

なお、最年少の者は14歳、最年長の者は61歳であった。

表4 - 2 年代別被疑者数の推移 (単位：人)

年齢	平成	平成	平成	平成	平成	平成17年		平成18年
	12年	13年	14年	15年	16年	上半期	上半期	上半期
10歳代	6	2	6	16	26	35	15	14
20歳代	13	28	30	26	21	40	22	22
30歳代	16	5	26	24	23	27	15	19
40歳代	2	16	7	9	17	9	5	6
50歳代	0	0	0	1	1	5	1	1
60歳代	0	0	0	0	0	0	0	1
計	37	51	69	76	88	116	58	63

不正アクセス助長行為に係る被疑者を含む。

(3) 不正アクセス行為の動機

不正アクセス行為の動機としては、不正に金を得るため(21事件(230件))が最も多く、次いで元交際相手、元勤務先等に対する嫌がらせや仕返しのため(10事件(10件))、好奇心を満たすため(7事件(19件))、オンラインゲームで不正操作を行うため(3事件(3件))の順となっている。

表4 - 3 不正アクセス行為の動機の内訳

動機	事件数(事件)	件数(件)
不正に金を得るため	21	230
嫌がらせや仕返しのため	10	10
好奇心を満たすため	7	19
オンラインゲームで不正操作を行うため	3	3
顧客データの収集等情報を不正に入手するため	1	1
料金の請求を免れる	1	1

(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事件(43事件(264件))について、当該識別符号を入力することにより利用されたサービスについてみると、インターネット・オークションが最も多く(18事件(213件))、次いでオンラインゲーム(10事件(11件))、ホームページ公開サービス(5事件(5件))、インターネットバンキング(4事件(21件))の順となっている。

表4 - 4 利用されたサービスの内訳

利用されたサービス	事件数(事件)	件数(件)
識別符号窃用型	43	264
インターネット・オークション	18	213
オンラインゲーム	10	11
ホームページ公開サービス	5	5
インターネットバンキング	4	21
電子メール	2	10
会員・顧客データベース	2	2
会員専用・社員用内部サイト	1	1
その他	1	1

(5) その他

不正アクセス禁止法違反の他の罪についても併せて検挙した事件は16事件あり、その内訳は次のとおりである。

表4 - 5 併せて検挙した事件の内訳

罪名	事件数(事件)()
詐欺	7
電子計算機損壊等業務妨害	5
電子計算機使用詐欺	3
電磁的記録不正作出・同供用	2
窃盗	1
文書偽造	1
著作権法違反	1
恐喝	1

事件数については、重複計上あり。

5 都道府県公安委員会による援助措置

平成18年上半期、不正アクセス禁止法第6条の規定に基づき、都道府県公安委員会がアクセス管理者に対して行った助言・指導は1件(北海道)であった。

表5 - 1 都道府県公安委員会の援助措置実施件数の推移

	平成 12年	平成 13年	平成 14年	平成 15年	平成 16年	平成17年 上半期	平成18年 上半期
援助措置(件)	6	21	5	5	3	4	3

6 防御上の留意事項

(1) 利用権者の講ずべき措置

ア パスワードの適切な設定・管理

利用権者のパスワードの設定・管理の甘さにつけ込んだ不正アクセス行為が多発していることから、利用権者がパスワードを設定する場合には、IDと全く同じパスワード、IDの一部を使ったパスワード等は避け、ID等からの推定が難しいものとするとともに、パスワードを他人に教えない、パスワードを定期的に変更するなどの対策を講じて、自己の識別符号を適切に設定・管理する必要がある。

イ ホームページでのID・パスワード等の入力に関する注意

本物のサイトに酷似したフィッシングサイトを開設し、本物と誤信した者が入力したID・パスワード等を使用した不正アクセス事件が発生している。そのため、心当たりのない電子メールやそれにより誘導されるなどしたホームページの指示をうのみにしてID・パスワード等を入力しないよう注意する必要がある。

ウ 不正プログラムへの対策

スパイウェア等の不正プログラムを含んだ電子メールやCDを送りつけ、それらによりID・パスワード等を不正に取得した手口がみられたことから、コンピュータ・ウイルス対策やスパイウェア対策（最新のコンピュータ・ウイルス対策ソフトの利用、オペレーティングシステムのバージョンアップ等）を適切に講ずる必要がある。

また、インターネットカフェ等における不特定多数の者が利用できるコンピュータでは、不正プログラムが動作している可能性があることにも注意する必要がある。

(2) アクセス管理者の講ずべき措置

ア 利用権者に対する注意喚起等

利用権者のパスワードの設定・管理の甘さにつけ込んだ不正アクセス行為が多発していることから、アクセス管理者は、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、容易に推測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の措置を講ずる必要がある。

イ 不特定多数の者が利用できるコンピュータの適切な管理

インターネットカフェ等の不特定多数の者が利用する場所に設置されたコンピュータのアクセス管理者は、利用者に対してID・パスワード等を入力する際の危険性について注意喚起するとともに、コンピュータへのリカバリーソフトの導入、利用終了時における履歴の削除、プログラムのインストール制限を行うなどの措置を講ずる必要がある。

(注)

注1 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経営者が、それぞれアクセス管理者である。

注2 利用権者

利用権者とは、特定電子計算機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。

注3 フィッシング

金融機関等を装って電子メールを送信し、受信者が偽のウェブサイトアクセスするよう仕向け、そこで個人の識別符号（ID、パスワード等）、クレジットカード番号等を入力させ、それらを不正に入手する行為をいう。

注4 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は1事件と数える。

注5 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・オークション用の識別符号を使用して、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。

注6 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、セキュリティの脆弱性を突いて操作指令を与えるなどの手法による不正アクセス行為が該当する。

注7 キーロガー

インストールしたコンピュータにおいて、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のことをいう。

注8 スパイウェア

パソコン内のファイル、キーボードの入力情報、表示画面の情報等を取り出して、漏えいする機能を持つプログラムのことをいう。