

平成17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17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 発生状況

(1) 認知件数(1)(2)

	平12	平13	平14	平15	平16		平17 上半期	増減
					上半期			
認 知 件 数	106	1,253	329	212	356	198	317	+119
海外からのアクセス	25	448	13	35	37	20	31	+11
国内からのアクセス	73	258	286	158	303	172	265	+93
アクセス元不明	8	547	30	19	16	6	21	+15

(2) 被害に係る特定電子計算機のアクセス管理者(3)

	平12	平13	平14	平15	平16		平17 上半期	増減
					上半期			
プロバイダ(注1)	59	182	243	98	126	56	166	+110
一般企業	25	429	62	76	202	123	132	+9
大学、研究機関等(注2)	8	101	3	16	6	2	7	+5
その他	14	139	21	22	22	17	12	-5
うち行政機関(注3)	-	-	12	3	12	8	10	+2
不明	0	402	0	0	0	0	0	0
計	106	1,253	329	212	356	198	317	+119

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年及び平成13年は「その他」の内訳の集計をしていない。

(3) 認知の端緒

	平12	平13	平14	平15	平16		平17	増減
					上半期	上半期		
アクセス管理者からの届出	30	168	47	12	29	20	12	-8
利用者(4)からの届出	23	118	92	78	172	80	270	+190
警察活動	35	930	185	100	146	95	17	-78
発見者からの通報	7	21	0	19	7	1	11	+10
その他	11	16	5	3	2	2	7	+5
計	106	1,253	329	212	356	198	317	+119

(4) 不正アクセス行為の後の行動

	件数(注)
インターネット・オークションの不正利用	177
オンラインゲームのアイテム等の不正取得、消去等	114
ホームページの改ざん・消去	17
ファイルの蔵置(フィッシング(5)用ページ作り込みを含む)	9
電子メールの盗み見など情報の不正入手	8
管理者・利用者のパスワード等変更	6
他人へのなりすまし	4
インターネットの利用	3
バック・ドア等のプログラムを仕掛ける	3
その他	3

注 件数については、重複計上あり。

2 検挙状況

(1) 年別推移

		平12	平13	平14	平15	平16		平17	増減
						上半期	上半期		
不正 アクセス 行 為	検挙事件数 (6)	30	35	51	58	65	27	47	+20
	検挙件数	62	66	102	143	142	66	196	+130
	検挙人員	34	51	68	76	88	39	58	+19
不正 アクセス 助長行為	検挙事件数	4	1	2	2	0	0	2	+2
	検挙件数	5	1	3	2	0	0	2	+2
	検挙人員	5	1	3	2	0	0	2	+2
計	検挙事件数	31 (重複3)	35 (重複1)	51 (重複2)	58 (重複2)	65	27	47 (重複2)	+20
	検挙件数	67	67	105	145	142	66	198	+132
	検挙人員	37 (重複2)	51 (重複1)	69 (重複2)	76 (重複2)	88	39	58 (重複2)	+19

(2) 不正アクセス行為の手口別年別推移

		平12	平13	平14	平15	平16		平17 上半期	増減
						上半期	上半期		
識別符号 窃用型 (7)	検挙事件数	29	33	46	56	62	25	45	+20
	検挙件数	61	52	83	141	131	59	193	+134
セキュリティ・ホール 攻撃型 (8)	検挙事件数	1	3	5	2	4	3	3	0
	検挙件数	1	14	19	2	11	7	3	-4
計 (不正アクセス行為)	検挙事件数	30	35 (重複1)	51	58	65 (重複1)	27 (重複1)	47 (重複1)	+20
	検挙件数	62	66	102	143	142	66	196	+130

(3) 不正アクセス行為の後に利用されたサービス

		事件数 (注)	件数
識別符号窃用型		45	193
	オンラインゲーム	18	25
	電子メール	7	6
	インターネット・オークション	10	120
	ホームページ公開サービス	6	5
	インターネット・バンキング等	2	30
	会員専用・社員用内部サイト	4	7
セキュリティ・ホール攻撃型		3	3
	会員専用・社員用内部サイト	3	3

注 事件数については、重複計上あり。

(4) 識別符号窃用型の不正アクセス行為における識別符号の入手方法

		事件数 (注)	件数
識別符号窃用型		45	193
	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	16	64
	立場上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	9	12
	利用権者をだましたり入力を盗み見るなどして入手したもの	9	12
	キーロガー等の不正プログラムを使用して入手したもの	3	32
	他人から購入したもの	3	59
	共犯者等から入手したもの	4	12
	フィッシングサイトにより入手したもの	1	1
	その他	1	1

注 事件数については、重複計上あり。

(5) 被疑者の年齢

	平12	平13	平14	平15	平16		平17	増減
					上半期	上半期		
10歳代	6	2	6	16	26	15	15	0
20歳代	13	28	30	26	21	10	22	+12
30歳代	16	5	26	24	23	8	15	+7
40歳代	2	16	7	9	17	6	5	-1
50歳代	0	0	0	1	1	0	1	+1
計	37	51	69	76	88	39	58	+19

(6) 犯行の動機

	事件数 (注)	件数
嫌がらせや仕返しのため	12	14
好奇心を満たすため	6	18
オンラインゲームで不正操作を行うため	7	13
不正に金を得るため	10	137
顧客データの収集など情報を不正に入手するため	10	11
自分の技量を計るため	4	2
その他	1	1

注 事件数については、重複計上あり。

3 都道府県公安委員会による援助措置の実施件数

	平12	平13	平14	平15	平16		平17	増減
					上半期	上半期		
援助措置実施件数	6	21	5	5	3	1	3	+2

4 検挙事例

1	公知のIDからパスワードを推測し、他人になりすましてインターネット・オークションに架空出品した不正アクセス禁止法違反、私電磁的記録不正作出・同供用及び詐欺事件
---	--

会社員の男(28)らが、インターネット・オークションの会員の公知のIDからパスワードを推測し、当該会員になりすまして不正アクセスを行った。また、同会員が登録していた電子メールアドレス等を、同会員が変更する手続きをとった旨の虚偽の情報を送信して事実証明に関する電磁的記録を不正に作出し、インターネット・オークション事業者の事務処理の用に供した。さらにそのインターネット・オークションにおいて携帯電話等を架空出品し、多数の落札者から代金をだまし取った。平成17年1月、不正アクセス禁止法違反並びに私電磁的記録不正作出・同供用罪及び詐欺罪で検挙した(大分、宮城、警視庁、茨城、兵庫、熊本)。

2	高校時代の同級生が開設するホームページ削除に係る不正アクセス禁止法違反事件
---	--

大学生の女(20)が、高校時代の同級生が開設していたホームページを削除することを目的として、平成16年12月、そのホームページを管理するホームページ作成サービス会社のコンピュータに同級生の生年月日等から推測したパスワード等を入力して不正アクセスし、同ホームページを削除した。平成17年2月、不正アクセス禁止法違反で検挙した(香川)。

3	他人のパスワードを推測し、事業者のコンピュータに入力した不正アクセス禁止法違反事件
---	--

無職の女(32)が、インターネット・オークションの会員に付与されているID・パスワードを不正に取得しそれを販売する目的で、平成16年10月頃、公開されているインターネット・オークションのIDからそのパスワードを類推し、それが実際に使用できることを確認するため、当該IDの利用権者になりすまして同オークションのコンピュータに不正アクセスを行った。平成17年3月、不正アクセス禁止法違反で検挙した(茨城)。

4	キーロガー(9)を使用して識別符号を不正取得するなどした不正アクセス禁止法違反事件
---	--

元大学教授の男(50)が、教え子の電子メールをのぞき見る目的で、勤務していた大学のコンピュータにキーロガーを仕掛け、当該コンピュータを利用した同大学の女子学生のID・パスワードを不正に入手した。また、平成16年11月から平成17年1月までの間、

これらのID・パスワードを使用して、自宅、同大学などに設置されたコンピュータから不正アクセスを行った。平成17年4月、不正アクセス禁止法違反で検挙した（広島）。

5	元社員によるメールサーバへの不正アクセス禁止法違反事件
----------	------------------------------------

会社員の男(39)が、以前コンピュータの管理を行っていた会社を退職させられたのを不満に思い、同社の業務を妨害する目的で、平成16年10月から平成17年1月頃までの間、在職時に自ら設定していたID・パスワードを用いて当時の勤務先等から同社のメールサーバに不正アクセスを行い、約1,000通のメールを閲覧したほか、数十通のメールを削除した。平成17年4月、不正アクセス禁止法違反で検挙した（愛知）。

6	ハッキングツールを使用して不正取得した識別符号を他の学校等に送りつけた不正アクセス禁止法違反事件
----------	---

無職の男(19)が、平成16年11月、当時在学していたコンピュータ専門学校のサーバコンピュータに対して、自分のハッキングの力量を試す目的でハッキングツールを使用して不正アクセスを行い、同校生徒約500人分の識別符号を不正に取得した。これが原因で退学処分となったため、同校の信用を毀損する目的で、平成17年2月、取得した識別符号を別の専門学校に電子メールで送信し不正アクセス行為を助長した。平成17年5月、不正アクセス禁止法違反で検挙した（京都）。

7	大手インターネットサービス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著作権法違反及び不正アクセス禁止法違反事件
----------	---

会社員の男(42)が、インターネットサービス会社が会員に付与したID・パスワードを不正に入手する目的で、平成17年2月、同社が著作権を有するホームページに酷似した「ログイン画面」をインターネット上に公開し、これを本物の「ログイン画面」であると誤信した者が入力したID・パスワードを不正に入手した。また、これらのID・パスワードを使用して不正アクセスを行った。平成17年6月、著作権法違反及び不正アクセス禁止法違反で検挙した（警視庁）。

8	セキュリティの脆弱性をついた不正アクセスにより個人情報を入力した不正アクセス禁止法違反事件
----------	--

大学生の男(27)が、個人情報を入力する目的で、平成17年3月、旅行会社が設置管理するサーバコンピュータにセキュリティの脆弱性をついた攻撃による不正アクセスを約19万回行い、同社の会員の氏名、住所、パスワードなどの個人情報約16万件を不正に入

手した。平成17年6月、不正アクセス禁止法違反で検挙した（警視庁）。

9

他人の識別符号を利用してオンラインゲームを利用しキャラクタの移動を他人にさせるなどした不正アクセス禁止法違反事件

パート従業員の男(30)が、平成16年8月、オンラインゲーム上で使用するキャラクタ・アイテムを不正に取得する目的で、当該オンラインゲーム上の知人のメールに記載されていたID・パスワードを使用してこの知人になりすまし、不正アクセスした。また、ゲーム中で知り合った中学生にもこの知人のID・パスワードを教えてアクセスさせ、知人のアイテムを男のキャラクタに移動する作業をさせた。平成17年6月、不正アクセス禁止法違反で検挙した（北海道）。

5 都道府県公安委員会による援助措置の事例

平成17年4月、企業が管理するサーバコンピュータが不正アクセスされ、ホームページの一部が改ざんされた。当該企業から再発を防止するための援助を受けたい旨の申し出があったことを受け、警察において当該サーバへの接続記録等を解析したところ、当該不正アクセスの手法が特定できた。さらに当該サーバを調査したところ、オペレーティングシステムに脆弱性があること、データベースソフトウェアが本来不要である管理者の権限で動作していること等が判明し、特定した不正アクセスの手法が実行可能であったことを確認した。

そこで、公安委員会から当該企業に対し、安全な運用を行うため以下の助言を行った。

- (1) オペレーティングシステム等のソフトウェアの脆弱性を改善するため、最新のセキュリティ修正プログラムを適用すること。
- (2) データベース等、ソフトウェアの実行権限を適切に設定すること。
- (3) 侵入検出装置の設置、接続記録の監視等、侵入を監視するしくみを導入すること。

6 防御上の留意事項

(1) 利用権者の講ずべき措置等

利用権者においては、識別符号窃用型の不正アクセス行為による事件の多くが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であったことから、パスワードの設定に当たっては、IDと全く同じパスワードやIDの一部を使ったパスワードなどは避け、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。

さらに、本物のサイトに酷似したフィッシングサイトを開設し、誤信した人が入力した個人情報（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ため、心当たりのない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個人情報等を入力しないよう注意するとともに、コンピュータ・ウイルスやスパイウェア対策（オペレーティングシステムのバージョンアップや最新ウイルス

対策ソフトの利用等)を適切に講じる必要がある。

(2) アクセス管理者の講ずべき措置等

今期もセキュリティ・ホール攻撃型の不正アクセス行為による事件が発生しているが、この種の事件は、ひとたび発生すると被害を受けた企業の情報セキュリティや個人情報保護に関する取組姿勢が問われるばかりでなく、企業イメージや信用までもが大きく傷つくことになり、また、フィッシングサイトが蔵置された場合等は、個人情報の窃取による二次的被害が発生するなど、さらに被害が大きくなる危険もある。これらのことを踏まえ、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随時確認すること、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こと、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こと、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ことなどにより、不正アクセス行為を防止するための措置を講ずることが必要である。

また、インターネット・カフェ等の不特定多数の人が利用する場所に設置された端末の管理者、運営者等は、これらの端末で取り扱った情報が盗まれる等の事案が発生していることにかんがみ、利用者に対して個人情報等を入力する際の危険性について注意喚起を行うとともに、端末へのリカバリーソフトの導入、利用終了時における不必要な履歴の削除、プログラムのインストール制限の実施等により、利用者とともに情報セキュリティに配慮した取り組みを行っていく必要がある。

(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

ここでは、インストールされたパソコンにおいて、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。