

不正アクセス行為の発生状況等の公表について

不正アクセス行為の禁止等に関する法律第7条第1項の規定に基づき、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を国家公安委員会、総務大臣及び経済産業大臣が公表するもの。

1 不正アクセス行為の発生状況

(1) 平成16年中の不正アクセス禁止法違反事件の検挙状況等について

ア 認知件数 356件（前年比 144件の増加）[1 頁]

イ 検挙状況 65事件 142件 88人（前年比 +7事件 -3件 +12人）[1 頁]

ウ 検挙事件の特徴 [2 ~ 3 頁]

識別符号窃用型が大半（62事件131件）で、ID等から容易に推測されるパスワードが利用されていたもの等が多くを占めた（31事件65件）が、キーロガー（打鍵情報を記録するプログラム）等のプログラムを使用して識別符号を窃用した事件の検挙も見られた（4事件19件）。

セキュリティの脆弱性を突くセキュリティ・ホール攻撃型の事件も見られた（4事件11件）。

検挙人員のうち26人が少年であった。

エ 都道府県公安委員会による援助措置 3件 [4 頁]

援助の申出のあったアクセス管理者に対し再被害防止のための助言を行った。

オ 防御上の留意事項 [4 頁]

他人に推測されにくいパスワードの設定やパスワードの定期的な変更など、識別符号を適切に設定・管理すること。

フィッシング事案による被害の増加が懸念されていることから、個人情報情報を聞き出そうとするメールに対しては十分注意を払うこと。

セキュリティ・ホールに対する修正プログラムのインストールなど、サーバを適切に管理すること。

不特定多数の人が利用できる端末の管理者等は、個人情報等の入力についての注意喚起や不必要な履歴の削除などを実施すること。

(2) 不正アクセス関連行為の関係団体への届出状況について

（他省庁関連につき略）

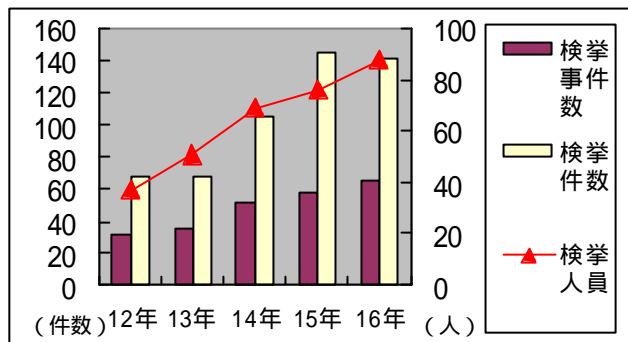
2 アクセス制御機能に関する技術の研究開発状況 [5 頁]

総務省に係るもの 7件、経済産業省に係るもの 1件

国による公募に対し応募のあったもの（民間企業） 6件

警察庁が実施した調査で把握した民間企業等によるもの 88件

【検挙件数の年別推移】



平成16年中の不正アクセス禁止法違反事件の検挙状況等について

1 認知件数

	平12	平13	平14	平15	平16	
						増減
認知件数	106	1,253	329	212	356	+144
海外からのアクセス	25	448	13	35	37	+2
国内からのアクセス	73	258	286	158	303	+145
アクセス元不明	8	547	30	19	16	-3

2 検挙状況

		平12	平13	平14	平15	平16	
							増減
不正アクセス行為	検挙事件数	30	35	51	58	65	+7
	検挙件数	62	66	102	143	142	-1
	検挙人員	34	51	68	76	88	+12
不正アクセス助長行為	検挙事件数	4	1	2	2	0	-2
	検挙件数	5	1	3	2	0	-2
	検挙人員	5	1	3	2	0	-2
計	検挙事件数	31 (重複3)	35 (重複1)	51 (重複2)	58 (重複2)	65	+7
	検挙件数	67	67	105	145	142	-3
	検挙人員	37 (重複2)	51 (重複1)	69 (重複2)	76 (重複2)	88	+12

3 検挙事件の特徴

(1) 犯行の手口

	事件数 (1)	件数
識別符号窃用型 (2)	62	131
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	31	65
立场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	13	21
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	7	14
キーロガー等のプログラムを使用して識別符号を入手したもの	4	19
その他	11	12
セキュリティ・ホール攻撃型 (3)	4	11

1 事件数については、重複計上あり。

2 識別符号窃用型とは、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。

3 セキュリティ・ホール攻撃型とは、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を突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。

検挙状況の類型別年別推移は次のとおりである。

		平12	平13	平14	平15	平16	
						増減	
識別符号窃用型	検挙事件数	29	33	46	56	62	+6
	検挙件数	61	52	83	141	131	-10
セキュリティ・ホール 攻 撃 型	検挙事件数	1	3	5	2	4	+2
	検挙件数	1	14	19	2	11	+9
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)	+7
	検挙件数	62	66	102	143	142	-1

(2) 被疑者(人数)

	平成12年	平成13年	平成14年	平成15年	平成16年	
						増減
10代	6	2	6	16	26	+10
20代	13	28	30	26	21	-5
30代	16	5	26	24	23	-1
40代	2	16	7	9	17	+8
50代	0	0	0	1	1	±0
計	37	51	69	76	88	+12

(3) 犯行の動機

	事件数(1)	件数
嫌がらせや仕返しのため	23	35
好奇心を満たすため	15	23
オンラインゲームで不正操作を行うため	10	31
不正に金を得るため	9	32
顧客データの収集など情報を不正に入手するため	5	12
その他	3	9

1 事件数については、重複計上あり。

(4) 利用されたサービス

	事件数(1)	件数
識別符号窃用型	62	131
オンラインゲーム	23	47
電子メール	15	24
インターネット・オークション	7	34
ホームページ公開サービス	6	6
インターネット・バンキング	4	4
その他	9	16
セキュリティ・ホール攻撃型	4	11

1 事件数については、重複計上あり。

4 都道府県公安委員会による援助措置

	平成12年	平成13年	平成14年	平成15年	平成16年	
						増減
援助措置	6	21	5	5	3	-2

5 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、IDからパスワードを推測されて不正アクセスされることを防ぐため、他人による推測が難しいパスワードを設定する必要がある。

また、パスワードを不用意に教えない、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。

さらに、フィッシング事案による被害の増加が懸念されていることから、個人情報聞き出そうとするメールに対し、不用意に回答しないよう注意する必要がある。

(2) アクセス管理者の講ずべき措置等

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。

また、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、リカバリーソフトの導入、不必要な履歴の削除、利用者によるプログラムのインストールの制限等の措置を講ずる必要がある。

アクセス制御機能に関する技術の研究開発の状況

1 国で実施しているもの

総務省又は経済産業省のいずれかに係るアクセス制御機能の研究開発に関してとりまとめたものである。具体的には、独立行政法人等による研究や国からの委託研究及び国からの補助事業により実施している研究である。

総務省に係るもの 7件

経済産業省に係るもの 1件

2 民間企業等で研究を実施したもの

(1) 公募

警察庁、総務省及び経済産業省が平成16年11月26日から12月27日までの間にアクセス制御技術に関する研究開発状況の募集を行い、その間、応募のあったものを取りまとめたものである。

4社6件

(2) 調査

警察庁が平成16年12月に実施したアンケート調査に対し、アクセス制御技術に関する研究開発を実施しているとして大学及び企業から回答があったものを取りまとめたものである。

大学：1大学1件

企業：33社87件