不正アクセス行為の発生状況の現状と課題（２）

岡　田　好　史

Ⅲ　不正アクセス関連行為の現状

６．送致の状況

2010（平成22）年中における不正アクセス禁止法違反の検挙件数は1,601件，検挙人員は125人であったが，送致された人員は102人であり，そのうち書類送致が67人となっている。前年と比べ，検挙件数は933件減

少したが，送致人員は 9 人増加した。送致人員は2005（平成17）年以降100名前後で推移しているが，身柄送致された人員は2006（平成18）年を除くと20～40人で推移している。

統計をみると，近年では，身柄送致された者よりも書類送致に留まる者の割合が増加していることがわかる。また，送致人員に占める少年および女性の割合はそう多くはなく，不正アクセス禁止法違反に基づく少年簡易送致は今のところ行われていない。

表 6－1－1　送致件数および措置別送致人員の推移[1]

	送致件数	送致人員						
		総数		うち）少年		身柄送致	書類送致（付）	少年簡易送致
			うち）女		うち）女			
2000年	60	31	1	6	0	20	11	－
2001年	61	49	7	2	0	38	11	－
2002年	91	69	14	6	1	30	39	－
2003年	123	62	11	14	2	26	36	－
2004年	227	82	8	28	4	28	54	－
2005年	231	97	17	32	6	40	57	－
2006年	303	115	15	39	8	62	53	－
2007年	1411	96	19	34	8	26	70	－
2008年	1094	106	15	42	5	38	68	－
2009年	2563	93	26	32	7	23	70	－
2010年	1601	102	19	26	7	35	67	－

7．検察における不正アクセス禁止法違反事件の受理状況等

（1）検察庁における新規通常受理の状況

検察庁が不正アクセス禁止法違反で新規に通常受理した人員は，2005年までは増加傾向にあったが，2008（平成21）年を除くと横ばい傾向にある。

通常受理は，警察官によるものがほとんどであり，特別司法警察員からなされたものはない。また，家庭裁判所からの受理も少年法20条に基づくものはなく，その他がわずかにあるのみである。

他の検察庁からの受理件数が多いのは，行為者は，地理的・時間的制約を受けることなく，遠隔地からも容易に不正アクセスが行いうるため，捜査を主体的に担当すべき検察庁が不明確となっているためではないかと思われる[2]。

表7－1－1　被疑事件の受理の状況[3]

	受理										
	総数	旧受[4]	新受								
			計	通常受理[5]				他の検察庁から[6]	家庭裁判所から[7]		再起[8]
				計	検察官認知・直受[9]	通常司法警察員から[10]	特別司法警察員から[11]		少年法20条	その他	
2000年	59	－	59	40	－	40	－	19	－	－	－
2001年	82	3	79	52	2	50	－	27	－	－	－
2002年	126	7	119	67	－	67	－	52	－	－	－
2003年	120	2	118	74	－	74	－	44	－	－	－
2004年	156	3	153	94	－	94	－	58	－	1	－
2005年	168	3	165	112	－	112	－	53	－	－	－
2006年	141	3	138	97	－	97	－	41	－	－	－
2007年	158	5	153	104	－	104	－	47	－	1	1
2008年	176	5	171	123	2	121	－	48	－	－	－
2009年	145	5	140	95	－	95	－	45	－	－	－
2010年	159	2	157	110	2	108	－	47	－	－	－

（2）起訴・不起訴人員

検察に送致され，受理された者のうち，起訴ないし不起訴等になった人

数は下記の表のとおりである。

検察において，既済とされた者は，当初は，起訴される割合が高かったが，近年では，不起訴処分となる割合が多くなってきている。また，他の検察庁に送致する数が多いのは，受理の場合と同じく行為者，捜査を主体的に担当すべき検察庁が不明確となっているためではないかと思われる。

表７－２－１　被疑事件の既済および未済の状況[12]

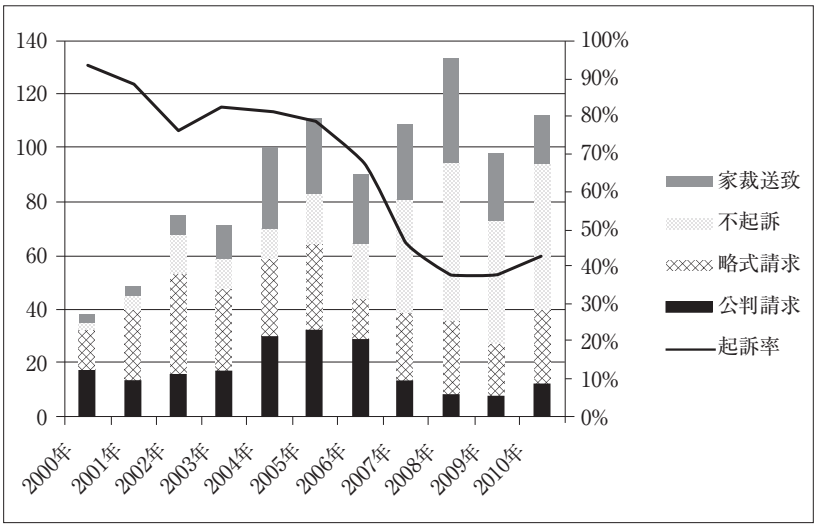
	既済																			未済[13]
	総数	起訴			不起訴												中止[14]	他の検察庁に送致[15]	家裁に送致[16]	
		計	公判請求	略式命令請求	計	起訴猶予	嫌疑不十分	嫌疑なし	罪とならず	刑事未成年	心神喪失	親告罪の告訴・告発・請求の欠如・無効・取消	確定判決・大赦・刑の廃止・刑の免除	時効完成	その他				
2000年	55	32	17	15	2	2	－	－	－	－	－	－	－	－	－	－	18	3	3
2001年	73	39	13	26	5	5	－	－	－	－	－	－	－	－	－	－	25	4	7
2002年	124	52	15	37	16	12	2	2	－	－	－	－	－	－	－	－	50	6	2
2003年	118	48	16	32	10	7	3	－	－	－	－	－	－	－	－	－	47	13	3
2004年	155	57	29	28	13	11	2	－	－	－	－	－	－	－	－	－	55	30	3
2005年	164	64	32	32	18	16	2	－	－	－	－	－	－	－	－	－	53	29	3
2006年	179	35	8	27	59	23	33	－	－	－	－	－	－	3	－	－	46	39	5
2007年	154	37	13	24	44	20	23	－	－	－	－	－	－	1	－	－	45	28	5
2008年	179	35	8	27	59	23	33	－	－	－	－	－	－	3	－	－	46	39	5
2009年	140	27	7	20	45	19	24	－	－	－	－	－	－	1	1	－	42	26	2
2010年	161	40	12	28	54	30	19	1	－	－	－	－	－	4	－	－	49	18	1

検察官は，少年の被疑事件について捜査を遂げた結果，犯罪の嫌疑があるものと思料するときは，少年法45条５号本文に規定する場合を除いて，家庭裁判所に送致しなければならないとされている。既済数においても，家裁送致の数が一定割合あるのは，不正アクセス禁止法違反の被疑者のうち10代の者が占める割合が，表５－２－２にみられるように上位にきている

ためであろう。

表7－2－2　被疑事件の起訴率

	総数	起訴		不起訴	家裁送致	起訴率[17]
		公判請求	略式請求			
2000年	37	17	15	2	3	94.1%
2001年	48	13	26	5	4	88.6%
2002年	74	15	37	16	6	76.5%
2003年	71	16	32	10	13	82.8%
2004年	100	29	28	13	30	81.4%
2005年	111	32	32	18	29	78.0%
2006年	90	28	16	20	26	68.8%
2007年	109	13	24	44	28	45.7%
2008年	133	8	27	59	39	37.2%
2009年	98	7	20	45	26	37.5%
2010年	112	12	28	54	18	42.6%



8．裁判における不正アクセス禁止法違反事件の概況等

（1）判例にみる不正アクセス禁止法違反事例

不正アクセス禁止法違反に問われた事件で，公刊物あるいは判例データベース[18]等で公表されたものは多くはない。その中でもっとも古い事件は，2002（平成14）年10月16日高松地裁丸亀支部判決である[19]。この事案は，他人の識別符号（ユーザ ID およびパスワード）を利用して不正アクセスを行った不正アクセス禁止法違反と，その際に他人の電子メールを盗み見た電気通信事業法違反のケースであった[20]。

不正アクセス禁止法違反に問われた事案の多くは，検挙事例にみられるように不正アクセス禁止法 3 条 1 項の識別符号窃用型の事案がほとんどである。また，キーロガー（Key logger）[21]やフィッシング（Phishing）を用いて知り得た他人の識別符号を窃用したケース[22,23]もみられるが，多くは単純に知り得た他人の識別符号を窃用したものである[24]。

最高裁まで争われ，公刊物に掲載された事案は，2012（平成24）年 5 月の時点で最二小決2007（平成19）年 8 月 8 日[25]のみである。本件は，被告人が，識別符号により会員のみに利用が制限されたインターネット・オークションを運営管理する会社のサーバ・コンピュータに対し，3 名の会員の識別符号を窃用して合計100回にわたり不正アクセスをしたという不正アクセス禁止法違反と，このうちの 2 回の不正アクセスの際に，2 名の会員のパスワードを不正に変更する私電磁的記録不正作出・同供用の行為をし，また，別の不正アクセスの際に，会員の 1 名になりすまして虚偽のオークション入札をして私電磁的記録不正作出・同供用の行為をしたという事案である[26]。

セキュリティ・ホール攻撃型の事案は，2012年 5 月の時点で東京地判2005（平成17）年 3 月25日[27]の 1 件しかない[28]。本件においては，被害にあったサーバの利用に当たって，識別符号の入力を要する FTP と，その入力を要しない HTTP というデータ転送形式が使用可能であったところ，

被告人は，セキュリティに関するイベントで発表するために，本件サーバで使用されていたCGIの脆弱性を利用し，HTTPを介して本来FTPによってのみ閲覧することができるファイルを閲覧したというものである。

不正アクセス禁止法違反事件において，言い渡された刑名・刑期は懲役2年以下が多く，3年以上の執行猶予の言渡しがなされているものが多い。

表8－1－1　判例データベース等にみられる刑および刑の執行猶予の言渡しを受けた者の人員

	総数	刑名・刑期							執行猶予の期間				
		懲役						罰金	1年以上	2年以上	3年以上	4年以上	5年
		無期	4年以下	3年以下	2年以下	1年以下	6月以下						
2000年	－	－	－	－	－	－	－	－	－	－	－	－	－
2001年	－	－	－	－	－	－	－	－	－	－	－	－	－
2002年	1	－	－	－	－	1	－	－	－	－	1	－	－
2003年	2	－	－	1	－	－	1	－	－	1	－	－	－
2004年	3	－	－	1	1	1	－	－	－	－	1	1	1
2005年	1	－	－	－	1	－	－	－	－	－	－	1	－
2006年	1	－	－	－	1	－	－	－	－	－	1	－	－
2007年	1	－	－	－	1	－	－	－	－	－	1	－	－
2008年	1[29]	－	1	－	－	－	－	1	－	－	－	－	－
2009年	1	－	－	－	1	－	－	－	－	－	－	－	－
2010年	1	－	－	－	1	－	－	－	－	－	－	－	－
2011年	1	1[30]	－	－	－	－	－	－	－	－	－	－	－

（２）刑の執行猶予の言渡しを受けた者の人員

刑の執行猶予の言渡しを受けた者のほとんどは，男性で，前に禁錮以上の刑に処せられたことがなく執行猶予とされている者である。刑法25条１項２号の「前に禁錮以上の刑に処せられたことがあっても，その執行を終わった日又はその執行の免除を得た日から５年以内に禁錮以上の刑に処せられたことがない者」はほとんどおらず，25条２項における，前に禁固以上の刑に処せられたことがあっても執行猶予中の者（ただし，保護観察中でない者）で，１年以下の懲役または禁固の言い渡しを受け，情状が特に軽いときに該当する者はいない。

警察庁の2009（平成21）年の調査[31]によると，犯行時に前科を有している被疑者の割合は，刑法犯全体では28.7％であるのに対し，ネットワーク利用犯罪[32]では20.1％，不正アクセス禁止法違反では8.1％となっており，不正アクセス禁止法違反においては，前科のない者が犯罪を敢行している割合が極めて高くなっている。

刑法25条１項１号に基づく執行猶予者が多いのは，警察庁の公表データが2009年のものしかないため推測になるが，このように前科を有していないからであろう。

表8－2－1　第一審において刑の執行猶予の言渡しを受けた者の人員[33]

	総数	性別等		該当法条					刑名・刑期						執行猶予の期間				
				刑法25条1項1号		同条1項2号		同条2項	懲役					罰金					
		男	女	保護観察又は補導処分に付する	保護観察又は補導処分に付さない	保護観察又は補導処分に付する	保護観察又は補導処分に付さない	保護観察又は補導処分に付する	計	3年以下	2年以下	1年以下	6月以下		1年以上	2年以上	3年以上	4年以上	5年
2000年	2	2	－	－	2	－	－	－	2	－	－	2	－	－	－	－	2	－	－
2001年	10	6	4	1	9	－	－	－	10	－	－	6	4	－	－	1	8	1	－
2002年	5	4	1	－	5	－	－	－	5	－	1	4	－	－	－	1	2	1	1
2003年	4	4	－		3	－	1	－	4	－	1	2	1	－	－	－	2	2	－
2004年	5	5	－	－	5	－	－	－	5	－	－	5	－	－	－	－	5	－	－
2005年	5	4	1	－	5	－	－	－	5	－	2	3	－	－	－	－	4	1	－
2006年	6	5	1	－	6	－	－	－	6	－	－	6	－	－	－	1	3	2	－
2007年	4	4	－	1	3	－	－	－	4	－	－	4	－	－	－	－	3	1	－
2008年	1	1	－	－	1	－	－	－	1	－	－	1	－	－	－	－	1	－	－
2009年	4	4	－	2	2	－	－	－	4	3	－	－	1	－	－	－	1	－	3
2010年	1	1	－	－	1	－	－	－	1	－	－	1	－	－	－	－	1	－	－

表８－２－２　控訴審において刑の執行猶予の言渡しを受けた者の人員[34]

	総数	性別等		該当法条					刑名・刑期							執行猶予の期間				
		男	女	刑法25条1項1号		同条1項2号		同条2項	懲役					罰金		1年以上	2年以上	3年以上	4年以上	5年
				保護観察又は補導処分に付する	保護観察又は補導処分に付さない	保護観察又は補導処分に付する	保護観察又は補導処分に付さない	保護観察又は補導処分に付する	計	3年以下	2年以下	1年以下	6月以下							
2000年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2001年	1	1	－	－	－	1	－	－	1	－	1	－	－	－	－	－	－	1	－	－
2002年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2003年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	1	－	－
2004年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2005年	1	1	－	－	1	－	－	－	1	－	－	1	－	－	－	－	－	－	－	－
2006年	1	1	－	－	1	－	－	－	1	－	1	－	－	－	－	－	－	1	－	－
2007年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2008年	1	1	－	－	1	－	－	－	1	－	－	1	－	－	－	－	－	1	－	－
2009年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2010年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

表8－2－3　上告審において刑の執行猶予の言渡しを受けた者の人員[35]

	総数	性別等		該当法条					刑名・刑期							執行猶予の期間				
				刑法25条1項1号		同条1項2号		同条2項	懲役						罰金					
		男	女	保護観察又は補導処分に付する	保護観察又は補導処分に付さない	保護観察又は補導処分に付する	保護観察又は補導処分に付さない	保護観察又は補導処分に付する	計	3年以下	2年以下	1年以下	6月以下			1年以上	2年以上	3年以上	4年以上	5年
2000年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2001年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2002年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2003年	1	1	－	－	1	－	1	－	1	－	－	－	1	－	－	1	－	－	－	－
2004年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2005年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2006年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2007年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2008年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2009年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2010年	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

9．小括

以上から，我が国においては，10歳代～30歳代の前科のない男性で，元交際相手や元従業員等の被害者と顔見知りの間柄にある者が，不正に金を得るためか，嫌がらせや仕返しのため，あるいはオンラインゲームで不正操作を行うために，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り，識別符号を知り得る立場を濫用したりして，被害者の識別符合を窃用し，日本国内から，電子メール・サービスや，インターネット・オークション・サービス，オンラインゲーム・サービス，会員専用・社員用内部サイトに対

して不正アクセスをし，情報の不正入手や，オンラインゲームの不正操作，ホームページの改ざん・消去，不正ファイルの蔵置，インターネット・バンキングの不正送金，インターネット・オークションの不正操作を行う傾向にあるということが伺える。

近年は金銭目的の犯罪が多い傾向にあることから，不正アクセス行為を電磁的記録不正作出・同供用，詐欺（詐欺および電子計算機使用詐欺），業務妨害（偽計・威力業務妨害，電子計算機損壊等業務妨害）の手段として利用することも多い。

現状をみる限り，不正アクセス禁止法は，立案当局の説明やマスコミ報道等では，ハッカー（hacker）[36]の取り締まりに効果があると喧伝されたが，ほとんどは，素人犯罪でしかなく，ハッカーに対しては効果がないと言ってもよい状況にある。

Ⅳ　防御上の留意事項

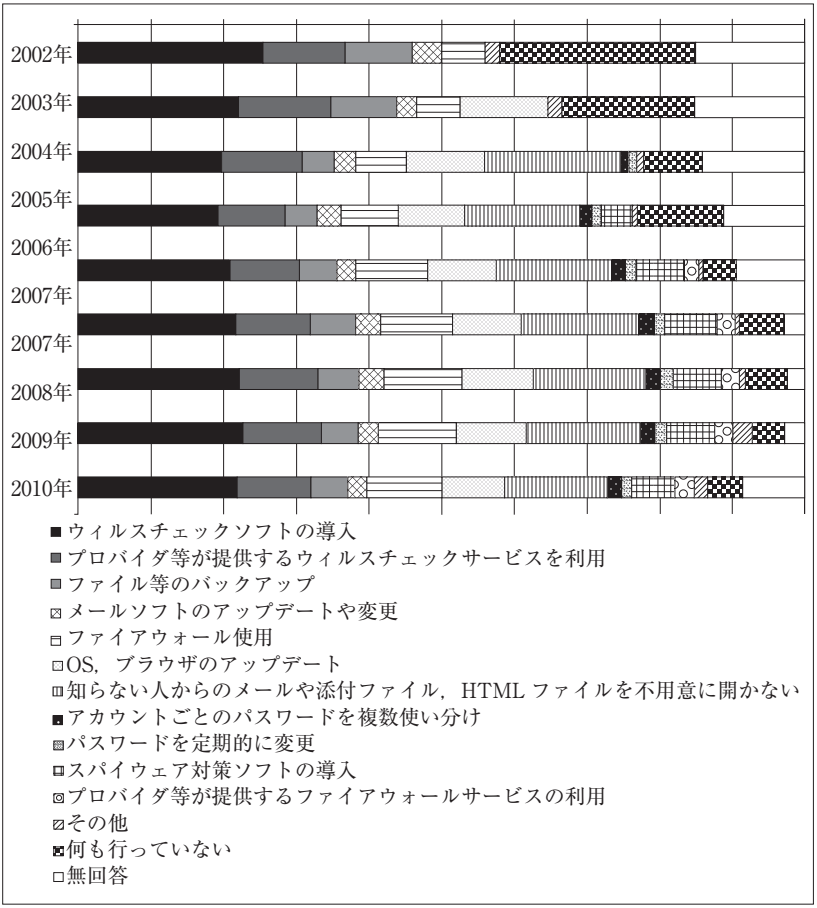
1．利用権者の講ずべき措置

総務省の「通信利用動向調査（世帯編）」において，インターネットを利用したことがある人が少なくとも１人はいる世帯に，コンピュータ・ウイルスや不正アクセスへの対応について尋ねたところ，2010（平成22）年においては，何らかのウイルス対策または不正アクセス対策を行っている世帯は，前年より減少して87.7％となった。具体的対応としては，「ウイルス対策ソフトの導入」が最も多く，次いで「知らない人からのメールや添付ファイル，HTML ファイルを不用意に開かない」，「プロバイダ等が提供するウイルス対策サービスを利用」，「ファイアウォールの使用」，「OS，ブラウザのアップデート」などの割合が高く2009（平成21）年と同じ傾向を維持している。

しかし，スパイウエア対策ソフトの導入や，アカウントごとのパスワー

表11-1-1　インターネットのウイルスや不正アクセス対策[37]

	集計人数	比重調整後集計人数[38]	インターネットのウイルスや不正アクセス対策（%）													
			ウィルスチェックソフトの導入	プロバイダ等が提供するウィルスチェックサービスを利用	ファイル等のバックアップ	メールソフトのアップデートや変更	ファイアウォール使用	OS，ブラウザのアップデート	知らない人からのメールや添付ファイル，HTMLファイルを不用意に開かない	アカウントごとにパスワードを複数使い分け	パスワードを定期的に変更	スパイウエア対策ソフトの導入	プロバイダ等が提供するファイアウォールサービスの利用	その他	何も行っていない	無回答
2002年	5,845	5,764	31.4	14.2	11.6	5.1	7.2	－	－	－	－	－	－	2.4	33.6	18.8
2003年	6,936	6,484	32.0	18.4	13.4	3.8	8.9	17.8	－	－	－	－	－	2.4	26.5	22.4
2004年	8,776	8,271	35.9	19.8	8.1	5.6	12.3	19.4	34.3	1.7	2.1	－	－	1.6	14.6	25.8
2005年	9,174	8,903	35.7	17.3	8.3	6.1	14.4	17.1	30.2	2.3	2.7	8.0	－	1.4	22.1	20.9
2006年	3,931	3,963	46.4	21.2	11.6	6.4	21.6	21.0	35.6	4.0	3.5	14.8	4.5	1.2	10.6	21.0
2007年	3,304	3,325	51.5	25.0	15.3	8.0	24.2	22.3	39.3	4.7	3.7	17.4	6.2	1.1	14.8	7.1
2008年	4,070	4,114	53.4	26.1	13.8	8.3	26.1	23.7	37.6	4.9	4.1	16.0	6.4	1.8	13.7	6.1
2009年	4,230	4,214	52.2	25.4	11.9	6.5	24.7	22.4	36.5	4.5	4.1	15.4	5.7	6.1	10.4	6.7
2010年	20,283	20,880	46.5	22.1	10.7	5.6	21.6	19.3	30.1	4.0	3.3	12.9	5.6	4.0	10.0	18.7



ドの使い分け，パスワードの定期的変更といった，OS やブラウザのアップデート，メールソフトのアップデートや変更といった基本的な不正アクセス対策は十分に取られているとは言い難い。このことは，インターネットが私たちの社会インフラ化してきているとはいえ，人々のセキュリティに対する意識が高くないことを示唆しているといえよう。

検挙された事案の多くが元社員や元交際相手等の顔見知りからパスワードを知り得た者，あるいはかつて当該パスワードを利用していた者や，利

用権者のパスワードをのぞき見ることができた者の犯行であり，アクセス管理者およ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。

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，誕生日などの個人情報に関連する番号を利用したパスワード等，他人による推知が容易なパスワードを設定している利用権者のパスワードの設定・管理の甘さにつけ込んで不正アクセス行為が行われることが多いため，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とともに，パスワードを定期的に変更する，複数のサイトで同じパスワードを使用しない，知人等に自己の識別符号の一時利用を認めた際は，その利用が終了した時点で確実にパスワードを変更するなどなどの対策を講じ，パスワードを適切に管理する必要がある。

パスワードを忘れてしまった場合，あらかじめ利用者が事前に設定しておいた特定の質問に答えることにより，本人確認ができたとみなされてパスワードが表示される機能（パスワードリマインダー機能）を悪用して，アクセス管理者から利用権者のパスワードを入手する手口もみられる。リマインダ機能の悪用の可能性に留意して，インターネット上における各種サービスを利用しなければならない。簡単な質問と答えを設定すると，第三者にパスワードを割り出される可能性が高いため，リマインダ機能を利用する場合には，パスワード再発行時に必要となる情報を，他人による推知が困難なものとすることが必要である。

また，利用権者が書き出したり，口にしたりしたパスワードを，偶然に見聞きした者による犯行や，後ろからのぞき見る，利用権者の周辺を探して見つけ出す，管理者を名乗るなどして，ソーシャル・エンジニアリングによって利用権者からパスワードを言葉巧みに聞き出す手口もみられるところである。

ソーシャル・エンジニアリングを用いるものとしては，近年，送信元ア

ドレスを偽装したメール等により，正規の組織からの通知に見せかけてユーザを詐称誘導し，ユーザの個人情報を偽の Web ページ等で入力させる等して詐取するフィッシングと呼ばれる手法が目立つようになってきている。2012（平成24年）３月に成立した不正アクセス禁止法改正によって，入手方法を問わず不正利用を目的とした識別符号の取得が処罰対象となるほか，フィッシングサイトの開設も処罰されることとなったが，フィッシングが厄介な点は，ユーザの心理を突くソーシャル・エンジニアリングの一種であることにある。メールの文面だけからフィッシングかどうかを判断することは難しい。フィッシャーは，あの手この手でユーザを騙そうとする。フィッシングのような攻撃は，我々の個人情報を目的としている。ユーザとしては，個人情報を要求するようなメールやサイトについては，まずは疑ってかかるぐらいの慎重さが必要である。騙されないためには，「偽サイトの見分け方」を周知させるよりも，発信元に心当たりのない電子メールに注意するとともに，ID・パスワードの入力を要求するサイトについては，まず真正な公式サイトにアクセスし，個人情報を入力させるような依頼を出しているかを確認するとともに，見ず知らずの第三者のサイトやメール中のリンクをクリックしてアクセスしたサイトでは，個人情報を絶対に入力しないことを徹底することが重要である。

フィッシングが識別符号の入力へと誘導するのに対し，スパイウエア等の不正プログラムを含んだ電子メールや CD-ROM を送りつけて言葉巧みに不正プログラムをインストールさせたり，不正プログラムを蔵置したサイトへと誘導する電子メールを送り付けて，サイト上の不正プログラムを含んだファイルにアクセスさせ，不正プログラムに感染させたりして，識別符号を入力するとそれを不正送信させる，あるいはインターネット・カフェ等のコンピュータにキーロガー等の不正プログラムを仕掛け，密かに他人の ID・パスワードを不正取得するなどの不正プログラムを使用した手口もみられるようになってきている。

不正プログラムによる識別符号の流出を防ぐためには，信頼できないファイルを不用意に開いたり，ダウンロードしたりしないように，また，不特定多数が利用す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留意し，識別符号を始め，口座番号やクレジットカード番号等の重要な個人情報を入力しないようにするか，入力を伴うサービスをできるだけ利用しないようにする必要がある。

さらに，最新のスパイウエア対策やコンピュータ・ウイルス対策ソフトウエアを導入したり，不正プログラム対策ソフトのパターンファイルやオペレーティング・システムのセキュリティパッチを常に最新のものに更新するなどの措置を適切に講ずる必要がある。

特に，他者のサーバを介してインターネット上で商品を販売する者等インターネット上で事業を営む者にあっては，不正プログラムに感染したサーバへのアクセスや顧客等とのメールのやり取り等を通じて不正プログラムに感染し，自己の感染した端末から保存されているインターネット・バンキングの預貯金口座等の情報や，サーバにアクセスするための識別符号等が流出する事案がみられるところである。これらを防ぐためには，インターネット・バンキング等に使用する端末と顧客との通信に使用する端末を分けて使用するなどの配慮が必要である。

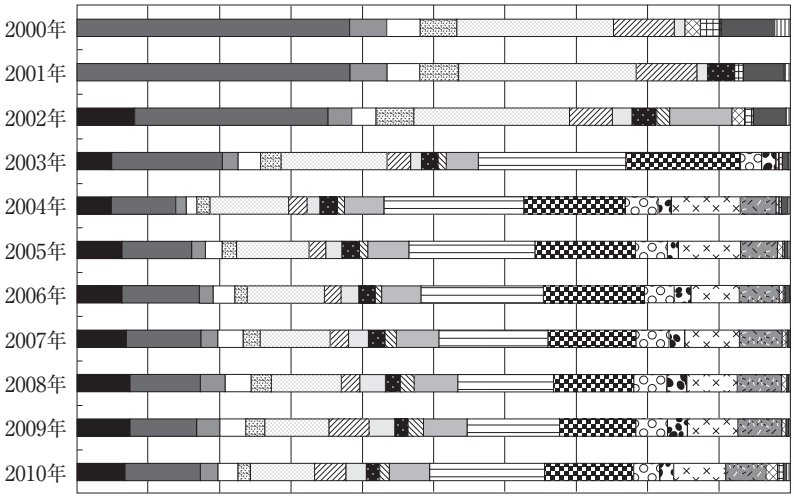
2．アクセス管理者の講ずべき措置

総務省の「通信利用動向調査（企業編）」においては，情報通信ネットワークを利用している企業にデータセキュリティへの対応について尋ねている。2010年の調査によると，何らかの対応をしている企業（全体から「特に対応していない」および「無回答」を除いた割合）は94.4％であり，多くの企業でデータセキュリティへの対応を行っていることがうかがえる。

具体的な対応は，「パソコンなどの端末（OS，ソフト等）にウイルス対策プログラムを導入」，「サーバにウィルス対策プログラムを導入」，「ID，

表11-2-1　ネットワークのデータセキュリティ対応[39]

	集計企業数	比重調整後集計企業数[40]	ネットワークのデータセキュリティ対応																					
			セキュリティポリシー	ID，パスワードによるアクセス制御	認証技術の導入による利用者確認	データやネットワークの暗号化	回線監視	ファイアウォールの設置・導入	プロキシ（代理）サーバー等の利用	セキュリティ監視	セキュリティ管理のアウトソーシング	不正導入検知システム（IDS）の導入	社員教育	パソコンなどの端末（OS，ソフト等）にウィルス対策プログラムを導入	サーバにウィルス対策プログラムを導入	外部接続の際にウィルスウォールを構築	ウィルスチェック対応マニュアルを策定し，社内教育を充実	OSへのセキュリティパッチの導入	アクセスログの記録	Webアプリケーションファイアウォールの設置・導入	その他の対策	分からない	特に対応していない	無回答
2000年	1,838	1,838	－	67.5	9.6	8.3	9.0	39.1	14.8	2.9	－	－	－	－	－	－	－	－	－	－	3.9	5.2	13.3	4.0
2001年	1,858	1,578	－	72.0	9.8	8.3	10.5	46.8	15.9	2.8	7.1	－	－	－	－	－	－	－	－	－		2.6	10.7	1.5
2002年	1,804	1,847	19.1	64.9	7.7	8.2	12.5	52.0	14.5	6.5	8.6	4.0	20.9	－	－	－	－	－	－	－	4.2	2.9	11.0	1.4
2003年	2,251	2,239	17.1	54.2	7.8	11.0	10.2	52.2	11.9	5.3	8.1	4.0	15.7	72.7	56.5	10.5	6.9	－	－	－	1.4	1.7	3.2	1.0
2004年	1,855	1,850	19.8	37.6	8.0	6.1	7.6	46.4	10.0	7.7	10.3	4.1	23.7	81.0	58.0	19.4	7.7	40.0	20.9	－	1.8	1.2	3.7	1.7
2005年	1,891	1,373	28.9	44.6	8.2	10.7	9.0	46.8	11.2	9.4	11.7	4.8	26.4	80.5	64.3	20.4	8.9	39.4	23.7	－	3.4	1.0	2.3	1.8
2006年	1,823	1,817	29.1	51.0	9.6	13.9	8.3	51.3	10.5	11.7	10.8	4.6	25.7	80.9	66.1	20.1	10.8	31.6	26.6	－	2.7	0.6	3.4	0.7
2007年	1,969	1,992	36.9	57.6	12.9	19.4	13.4	53.8	13.4	15.6	12.7	8.4	32.6	84.1	67.1	25.2	12.7	41.4	32.8	－	3.4	1.0	1.5	0.5
2008年	1,996	1,996	45.3	63.3	20.5	22.9	18.3	60.7	16.9	21.9	13.0	12.4	38.8	83.6	70.3	29.1	16.4	45.2	39.2	－	4.0	－	2.2	1.4
2009年	1,830	1,832	48.7	62.0	20.5	23.7	17.6	57.1	37.1	23.6	11.9	13.4	39.3	84.3	68.9	29.0	18.0	45.6	39.7	－	4.0	－	2.1	1.8
2010年	2,108	2,107	32.9	53.9	12.5	14.4	8.8	45.4	22.0	14.6	9.1	8.8	29.4	80.9	62.6	18.6	10.1	36.6	28.2	8.3	3.5	－	2.9	2.7



- セキュリティポリシー
- ID，パスワードによるアクセス制御
- 認証技術の導入による利用者確認
- データやネットワークの暗号化
- 回線監視
- ファイアウィールの設置・導入
- プロキシ（代理）サーバ等の利用
- セキュリティ監査
- セキュリティ管理のアウトソーシング
- 不正侵入検知システム（IDS）の導入
- 社員教育
- パソコンなどの端末（OS，ソフト等）にウイルス対策プログラムを導入
- サーバにウィルス対策プログラムを導入
- 外部接続の際にウィルスウォールを構築
- ウィルスチェック対応マニュアルを策定し，社内教育を充実
- OS へのセキュリティパッチの導線
- アクセスログの記録
- Web アプリケーションファイアウォールの設置・導入
- その他の対策
- 分からない
- 特に対応していない
- 無回答

パスワードによるアクセス制御」,「ファイアウォールの設置・導入」の順で実施割合が高い。また，2009（平成22）年末からの新規項目である「Web アプリケーションファイアウォールの設置・導入」は8.3%となっている。

IBM の調査によると，2011年に報告された脆弱性のうち40%以上がWeb アプリケーションの脆弱性であり，その多くはクロスサイト・スクリプティング（xss/Cross Site Scripting）[41]と SQL[42]インジェクション[43]である[44]という。

SQL インジェクションによるセキュリティ・ホール攻撃によってクレジットカード番号等の個人情報が大量に流出する事案[45]にみられるように，セキュリティ・ホール攻撃型の不正アクセス行為が一旦行われると，被害が大きくなる危険がある[46]ことから，アクセス管理者には，セキュリティ水準の維持・向上が求められる。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，プログラムを点検してセキュリティ上の脆弱性を解消するとともに，攻撃の兆候を即座に検知するための侵入検知システム等を導入する等，攻撃に対する監視体制を強化するとともに，使用しているオペレーティング・システムまた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等セキュリティ・ホールを解消するための措置を講じ，適切に設定されたファイアウォールの設置，ログの保存・監査等サーバの適切な管理を行う必要がある。

不正アクセス行為の多くは，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であることから，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よう努める必要がある。

また，識別符号を知り得る立場にあった元従業員による不正アクセス行為を防ぐためには，従業員が退職した時や特定電子計算機を利用する立場でなくなった時には，当該従業員に割り当てていたIDを削除したり，パスワードを変更したりするなど識別符号の適切な管理を徹底することが重要である。

ウェブサイト管理用のID・パスワードが不正に取得されて，アクセス管理者の意図しない命令が入力され，ウェブサイトが閲覧された際にその命令が実行され，閲覧者をウイルス等が蔵置されたウェブサイトに誘導する事案については，ウェブサイトの更新の際にID・パスワードを暗号化することや更新に利用する端末を限定することなどにより安全な管理を徹底する必要がある。

さらには，攻撃されたときに迅速に対処するため，事後対応計画を策定しておき，冷静に行動できる体制を整えておく必要もあるだろう。

フィッシング，スパイウエア等により不正に取得したID・パスワードを使用した不正アクセス行為への対処としては，インターネット・オークション，インターネット・ショッピング，インターネット・バンキング，オンラインゲーム等のネットワーク上でサービスを提供する事業者にあっては，識別符号（ID・パスワード）に加え，ワンタイムパスワード等により個人認証を強化する，個人情報にかかる情報の送信を電子メールを用いて行う場合には，デジタル署名を付与するのも一つの手であろう。しかし，この点については，デジタル署名の意味をユーザに理解してもらわなければ，またセキュリティ・ベンダーに対応してもらえなければ，正しいデジタル署名付のメールをユーザが受信した際でも「メッセージが改ざんされている」と誤解されかねないため，事前にユーザへの周知も必要となろう。

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，利用者の本人確認の励行，利用者に

対してID・パスワード等の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，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ブラウザ等の履歴の削除，利用者によるプログラムのインストール制限等を実施することが必要である。

「通信利用動向調査（企業編）」によると，「ID，パスワードによるアクセス制御」，「ファイアウォールの設置・導入」は高い割合となっているが，不正侵入検知システム（IDS）や不正侵入防止システム（IPS）の導入，セキュリティ監査の実施，OSへのセキュリティパッチの導入といった基本的な不正アクセス対策は十分に取られているとは言い難い。このことは，企業においても目に見えるウイルス被害に対しては対処するようになってきているが，目に見えにくい不正アクセスに対する意識は，いまだ高くないことを示唆しているといえよう。

どのようなセキュリティ・システムにおいても，それを利用するのは人である。与えられた指令を忠実にこなすコンピュータと異なり，人は，感情，利益，慣れなどによって容易に行動を変えてしまうことがある。したがって，セキュリティを講じる際には，技術的のみならず人的対応についても考えなければならない。

最近は，さまざまなセキュリティ製品が市場にあふれている。たとえシステムで一時的に守れたとしても，攻撃者が戦略を変えればその防御方法は無力になる。セキュリティ製品等で攻撃を100％防ぐことは困難である。アクセス管理者は，技術的対策だけでなく，ユーザの教育も重要であることを認識し，サービス利用者に対してさらに注意喚起を行うべきであろう。

セキュリティ対策をしているので大丈夫という思い込みを排し，日頃からリスクを顕在化させ，既に実施しているセキュリティ対策と照らし合わせて残存リスクを明らかにし，足りていない対策をすぐに講じる必要がある。

これらの対応策をとることによって，不正アクセス被害を減らすことは

可能であると思われる。

注

1　警察庁『犯罪統計書』2000（平成13）年～2010（平成23）年

2　この問題は，警察活動に対しても当てはまる。関係都道府県警察が捜査の重複を避けつつ，連携して対処する必要があることから，警察庁は情報技術犯罪対策課を2004（平成16）年設置するとともに，都道府県警察および都道府県情報通信部にサイバー犯罪対策に関する知識及び技能を有する捜査員等により構成されるサイバー犯罪対策プロジェクトを設置している。この体制の下で，警察庁は，都道府県警察が行うサイバー犯罪捜査に関する指導・調整を行っているほか，捜査員の能力向上のための研修，産業界や外国関係機関等との連携を推進している。しかし，地理的・時間的制約を受けることがないサイバースペースにおいては，捜査を主体的に担当すべき都道府県警察が不明確となり，その結果捜査の競合等が発生し，効率的な捜査を行うことが困難となっていたことから，効率的な捜査を進めるため，2010（平成22）年10月から2011（平成23）年６月までの間，インターネットホットラインセンターから警察庁に対して通報された違法情報の発信元を割り出すための初期捜査を警視庁が一元的に行い，捜査すべき都道府県警察を警察庁が調整する「全国協働捜査方式」の試行を行った。その結果，検挙件数の増加が顕著にみられたことから，同年７月から本格実施を開始している。

3　法務省『検察統計年報』2000（平成13）年～2010（平成23）年

4　統計期間の末日現在において事件が既済とならず，翌年に繰り越された事件をいう。

5　検察官が認知または直接受理した事件および司法警察員（特別司法警察員及び国税監察官を含む）から送致（付）された事件をいう。

6　他の検察庁の検察官から受理した事件をいう。

7　少年法第19条第２項，第20条，第23条第１項または第23条第３項の規定により家庭裁判所から受理した事件をいう。

8　不起訴若しくは中止の処分にした事件又は管轄違い若しくは公訴棄却の裁判があった事件で，同じ犯罪について再び捜査に着手した事件をいう。

9　検察官が自ら犯罪を認知若しくは直接に告訴・告発，自首または請求を受けて捜査に着手した事件をいう。

10　警察官から受理した事件をいう。

11　刑務官，麻薬取締官，労働基準監督官，自衛隊警務官等の司法警察員のほか，国税庁監察官から受理した事件をいう。

12　法務省『検察統計年報』2000（平成13）年～2010（平成23）年

13　統計期間の末日現在において事件の処理が既済とならないものをいう。

14　犯人不明，被疑者または重要参考人の所在不明，海外旅行あるいは心神喪失，病気等の理由により，これ以上捜査を継続することができず，かつ，当該捜査の障害となる理由が長期にわたり解消される見込みがないため，事件を長期間処理することができない場合で，中止の処分にした事件をいう。

15　他の検察庁の検察官に事件を送致した事件をいう。

16　少年法第42条第１項の規定により家庭裁判所に送致した事件をいう。

17「起訴率」とは，起訴人員／（起訴人員＋不起訴人員）×100の計算式で得た百分比をいう。

18　裁判所の判例データベースのほか，LEX/DB，D1-Law，LLi，Westlaw Japan 所収のものを対象とした。

19　http://www.courts.go.jp/hanrei/pdf/20061027151714.pdf（2012年５月10日確認）

20　評釈としては，立崎正夫 NBL 別冊79号84頁，拙稿専修ロージャーナル　１号163頁参照。

21「キーボードからの入力を監視して記録するソフト。もともとデバッグなどに利用するツールだったが，近年ではこっそり仕掛けてパスワードを盗むなど悪用される事例が増えている。

　常駐型のソフトとして別のソフトの使用中に透過的に動作するようになっており，複数の人間が利用するパソコンにこっそり仕掛けてパスワードやクレジットカード番号などを収集するなど，悪用されることが多い。実際，インターネット・カフェに仕掛けられたキーロガープログラムにより，ネットバンキングのパスワードが盗まれ，知らないうちに口座から現金が引き出されるといった被害が発生している。」IT 用語辞典 e-words〈http://e-words.jp/w/E382ADE383BCE383ADE382ACE383BC.html〉（2012年５月10日確認）

22　キーロガーを使用した事例としては，東京地判平成15年８月21日公刊物未登載（TKC 文献番号28095229）（被告人が，まんが喫茶等に設置されているインターネットに接続可能なパーソナルコンピュータに，キーロガーをしかけて入手した他人の識別符号等を利用して，クレジットカード会社のサーバ・コンピュータに不正にアクセスして会員が住所を変更した旨の虚偽の情報を記憶蔵置させ，当該会員になりすましてインターネット通信販売により商品を注文，受領して窃取するなどした事案）がある。

23　フィッシングの事例としては，東京地判平成17年９月12日公刊物未登載（TKC 文献番号28135296）（被告人が，A 株式会社が開設したホームページ画面タイトル部分を書き換えるなどしたホームページ画面を複製して，これをインターネット上で公開して著作権を侵害し，同サイトを閲覧した者からだまし取った識別符号を使用して不正アクセス行為をし，他人のメールをのぞき見するなどした事案）がある。

24　東京高判平成15年６月25日判時1846号155頁（原審東京地判平成14年12月25日判

時1846号159頁）（ソフトウエア会社に勤務し，以前同社に勤務していたAが作成したプログラムの更新作業を行っていた被告人が，同プログラムのソースコードを手に入れるため，勤務先および自宅から，Bが設置管理するサーバにAの識別符号を入力してアクセスした事案で，被告人は，本件各行為時に，アクセスしたサーバが，勤務先あるいは関連会社が管理するサーバではないことを認識していたと認めることができるとして，不正アクセス禁止法違反の故意を認めた上，仮に，本件ソースコードの著作権が関連会社にあるとしても，自救行為的な行為を認める緊急性も必要性もない等，被告人の行為は社会的相当性を欠いており，正当業務行為であるともいえないとした事案），東京地判平成15年12月11日公刊物未登載（TKC文献番号28095339）（被告人が，インターネット・オークションを悪用して財産上不法の利益を得ようと企て，多数回にわたり，オークションの運営会社のコンピュータに不正アクセスした上，被告人が他人名義で出品した架空の商品を，オークション会員が直ちに落札し，その落札代金立替払いサービスの利用を指定し，その落札代金相当額を被告人の管理する預金口座に送金依頼する旨の虚偽情報を送信して記憶蔵置させるとともに，金融機関のコンピュータにも自動送信させて，同預金口座の残高が増額した旨の虚偽情報を記憶蔵置させたほか，犯行が当該会員に発覚することのないよう，犯行の前後に会員のメールアドレスを変更したという事案），東京地判平成16年11月19日公刊物未登載（TKC文献番号28105268）（被告人Cが，大手IT情報関連会社である被害会社が管理するコンピュータに不正アクセスをして，顧客名簿を入手した被告人Dと共謀の上，被害会社の担当者に対し，入手した顧客情報を他に流出させて被害会社の信用・業務等に危害を加える旨の脅迫をして，多額の金員を恐喝しようとしたが，未遂に終わった事案），京都地判平成20年4月18日公刊物未登載（LLi文献番号06350106）（他人の識別符号を用いて，インターネット・オークションの商品落札代金を騙し取るため，不正アクセス，私電磁的記録不正作出・同供用，詐欺等を行ったという事案），東京高判平成22年3月9日公刊物未登載（TKC文献番号25462849）（原審東京地判平成21年11月12公刊物未搭載（TKC文献番号25462848））（被害会社の情報システムの運用等の業務を担当していた被告人が，被害会社の顧客情報データシステムが導入されたサーバ・コンピュータに3回にわたって不正アクセスし，それによって得た顧客データが記録されたCD-Rを窃取したほか，被害会社が情報会社から有償で入手した，1ヶ月分の企業情報のデータが記録されたCD-R 2枚を窃取した事実からなる事案），岐阜地判平成23年3月18日公刊物未登載（LLi文献番号06650129）（被告人Eが，Fと共謀の上，金品を強取した上，被害者Hを殺害しようと企て，Gに殺意をもって暴行を加え財物を強取した後に殺害し，Gを利用権者として付された識別符号を使用してネットバンクのサーバ・コンピュータに不正アクセスし，銀行の電子計算機に虚偽の情報を与えて，G名義の預金口座から，被告人管理にかかるI名義の預金口座の残高を増加させて，財産上不

法の利益を得るなどした事案）等。

25　刑集61巻５号576頁，判タ1252号173頁，判時1987号159頁（一審京都地判平成18年５月30日刑集61巻５号581頁，控訴審大阪高判平成19年３月27日刑集61巻５号588頁，判タ1252号174頁）

26　本事案は，一審以来，事実関係に争いはないが，原判決において，弁護人は，上記の各私電磁的記録不正作出・同供用は，いずれも不正アクセス行為を手段として犯されたもので，このような対応関係にある不正アクセス行為と私電磁的記録作出とは，併合罪ではなく牽連犯の関係にあるとの主張がされていたが，原判決は，両者はその罪質上通例として，前者が後者の手段又は結果となる関係にあるものとはいえないから，両者が牽連犯の関係にあると解するのは相当ではないとして，併合罪として処断したため，被告人側が上告していた。

27　判例タ1213号314頁，判時1899号155頁（被告人側が控訴していたが2005（平成17）年６月６日付で控訴を取り下げたため，地裁判決が確定した）。

28　宮崎香織「実例捜査セミナー 少年によるホームページ改ざん事件の捜査について」捜査研究53巻１号（2004年）42頁においては，東京家庭裁判所平成15年６月24日受理少年保護事件として，ハッカーにあこがれ，中学２年ごろから独学でコンピュータの勉強を始めた中学３年の少年が，インターネットでセキュリティ・ホールを攻撃するハッキング用プログラムを入手し，2003（平成15）年３月28日にこのプログラムを使って，スロバキアのサーバから，タイ国内のサーバを中継して東京都内の会社員が運営するWebサイトのデータが記憶・蔵置されたサーバに不正アクセスしたに上で，イラク戦争に対する反戦メッセージを表示するようサイトを改ざんしたほか，23カ国124サイトを改ざんして反戦メッセージを表示させた事例が紹介されている。

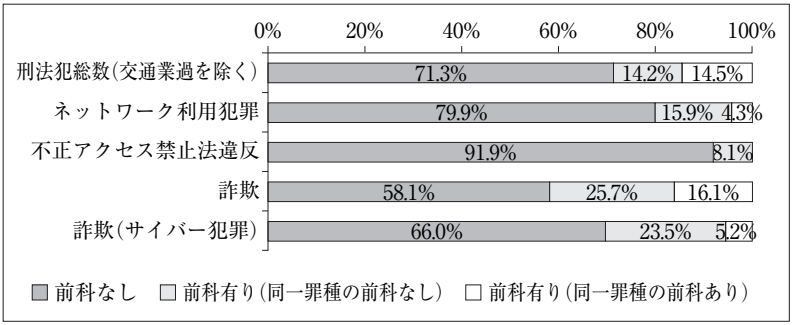
29　懲役３年６月に加え罰金100万円が併科されているため総数は１となっている。

30　窃盗，有印私文書偽造，同行使，偽造有印公文書行使，詐欺，旅券法違反，出入国管理および難民認定法違反，不正アクセス行為の禁止等に関する法律違反，電子計算機使用詐欺，強盗殺人被告事件のため，求刑も無期懲役となっている。

31　警察庁編『平成23年版警察白書』佐伯印刷（2011年）21頁

	総数				
		前科なし	前科有り		
			総数	同一罪種の前科なし	同一罪種の前科あり
刑法犯総数（交通業過を除く）	242,606	173,035	69,571	34,343	35,228
ネットワーク利用犯罪	1,853	1,480	373	294	79
不正アクセス禁止法違反	62	57	5	5	－
詐欺	11,504	6,687	4,817	2,962	1,855
詐欺（サイバー犯罪※）	153	101	52	36	8

※　警察庁の定義では，「高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪」を指す。



32　警察庁の定義では，「その実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪」を指す。

33　法務省『検察統計年報』2000（平成13）年～2010（平成23）年

34　法務省『検察統計年報』2000（平成13）年～2010（平成23）年

35　法務省『検察統計年報』2000（平成13）年～2010（平成23）年

36　Eric S. Raymond ed., The New Hacker's Dictionary 3rd ed.（1996）（福崎俊博訳『ハッカーズ大辞典（改訂新版）』アスキー（2002年））によれば，ハッカーとは，プログラム可能なシステムの細かい部分を探ったり，その機能を拡張する方法を探究したりするのに喜びを感じる人。熱中して（さらには取りつかれたように）プログラミングする人，またはプログラミングを単に理論化するのではなく，プログラミングを楽しむ人。ハック価値（hack value＝無駄と思われる目標に向かって労力を費やす理由やその動機としてよく引き合いに出される価値）を評価できる人，等とあり，誤用として「あちこち調べ回って機密情報を探りだそうとする

悪意の詮索好き」としている。

それに対して，クラッカー（cracker）とは，システムのセキュリティを破る人物であり，マスコミに間違った使われ方をする「ハッカー」という語を守るため，1985年頃ハッカーによって考案されたとされる。

「ハッカー」という言葉自体は，黎明期のコンピュータ研究者や優秀なコンピュータ・エンジニアに対して付けられた尊称のようなものであり，コンピュータ専門家，あるいはそこから転じて，コンピュータに全てを捧げているようなコンピュータ中毒症者という程度のニュアンスのものとして使われていた。コンピュータ・ネットワークに侵入し，データの入手や，さらにはデータの変造，破壊，不正コピー等を行う者をクラッカー（cracker，kracker）やヴァンダル（vandal）等と呼びハッカーと区別しようとする向きもあるが，コンピュータ・テクノロジーに精通している人たちの間での区別であり，また，ハッカーとクラッカーらを厳密に区別することは出来ないという点をも考慮し，ハッカーをクラッカーとほぼ同義のものとして扱うことにする。

なお，ハッカーについては，Donn B. Parker, Fighting Computer Crime（1983）pp. 157-187（鵜沢昌和訳『コンピュータ犯罪研究総論』秀潤社（1984年）175頁以下），Steaven Levy, Hackers: Heroes of The Computer Revolution（1984）（古橋芳恵・松田信子訳『ハッカーズ』工学社（1987年）），Clifford Stoll, The Cuckoo's Egg: Tracking A Spy Through The Maze of Computer Espionage（1989）（池央耿訳『カッコウはコンピュータに卵を産む（上）（下）』草思社（1991年）），Zachary Margulis & Carol Palechi, Berkeley Hackers（1991）（広谷渉訳『バークレイ・ハッカーズ』ビレッジセンター出版局（1992年）），Paul A. Taylor, Hackers（1999），山口英・鈴木裕信編『情報セキュリティ』（共立出版，2000年）所収の古瀬論文，上野論文，Andrew Ross, *Hacking Away at the Counter-Culture*, *in* The Cybercultures Reader（David Bell & Barbara M. Kennedy eds., 2000）pp. 254-267，Steven Furnell, Cybercrime（2002）pp. 41-93 等参照。

37　総務省「通信利用動向調査（世帯編）」2002（平成15）年～2010（平成23）年。表中の数値は，全体における個々の比率を示しているが，調査が複数回答を含んでいるので，総計が100になるとは限らない。

なお，インターネット利用におけるウイルスや不正アクセスへの対応については，調査対象が2004（平成17）年調査までは世帯構成員，2005（平成18）年調査以降は世帯全体であるため，比較には注意を要する。また，2001（平成14）年以前の調査においては，インターネット利用におけるウイルスや不正アクセスへの対応についての調査項目がないため除外している。

38　調査対象の選定においては，都市規模ごとの世帯数を反映させるように配慮した層化二段無作為抽出法を採用しているが，回収率が都道府県，世帯主の年齢により異なっており，回収結果の都道府県・世帯主年齢の構成は母集団と多少の乖

離が生じているため，母集団を正しく推計することが困難となるため，通信利用動向調査（世帯編）では，比重値を回収結果に乗じ，母集団の都道府県・世帯主年齢構成と一致する比重調整を行った上で分析している。また同様の理由により，世帯人員についても比重調整を行っている。

なお，比重値の計算は，2002年～2005年までは，「平成12年国勢調査第1次集計結果第13表」および前年の「通信利用動向調査世帯用」の有効回答を用いて，2006年～2010年までは，平成17年国勢調査第1次基本集計第13表「世帯主の男女，世帯主の年齢（5歳階級）」（世帯用），平成17年国勢調査第1次基本集計第16表「一般世帯人員：男」「一般世帯人員：女」（世帯人員用），第20回完全生命表および前年の「通信利用動向調査世帯編」の有効回答を用いて行っている。

39　総務省「通信利用動向調査（企業編）」2002（平成15）年～2010（平成23）年。表中の数値は，全体における個々の比率を示しているが，調査が複数回答を含んでいるので，総計が100になるとは限らない。

40　調査対象の選定においては，産業・従業者規模ごとに企業数を反映させるように配意した業種別の系統抽出法を採用しているが，回収率が産業・従業者規模により異なっており，回収結果の地方別産業構成は母集団と多少の乖離が生じているため，母集団を正しく推計することが困難となるため，通信利用動向調査（企業編）では，2000（平成12）年においては，全体に対する比重が母集団と一致するように業種と規模を基準としたウェイト値を算出し，規正回収結果を得た上で分析を行い，2001（平成13）年以降は，比重値を回収結果に乗じ，母集団の産業・従業者規模構成と一致する比重調整を行った上で分析している。

なお，比重値の計算は，2001年は，「平成11年事業所・企業統計調査報告第3巻企業に関する集計会社企業（全国）編」中，「第6表企業産業（中分類），企業常用雇用者規模（11区分），企業類型（2区分），経営組織（3区分）別企業数―全国」（総務省）および「通信利用動向調査企業編」の有効回答を用い，2002年～2005年までは，「平成13年事業所・企業統計調査調査結果第2表」および前年の「通信利用動向調査企業編」の有効回答を用いて，2006年～2010年は，「平成16年事業所・企業統計調査調査結果」および前年の「通信利用動向調査企業編」の有効回答を用いている。

41　「ソフトウエアのセキュリティホールの一つで，Webサイトの訪問者の入力をそのまま画面に表示する掲示板などのプログラムが，悪意のあるコードを訪問者のブラウザに送ってしまう脆弱性のこと。

悪意を持ったユーザがフォームなどを通してJava Scriptなどのスクリプトコードを入力した時に，プログラム側に適切なチェック機構がないと，そのスクリプト内容がそのままHTMLに埋め込まれ，ページを閲覧したコンピュータでスクリプトが実行されてしまうことがある。

このような形でページに埋め込まれてしまったスクリプトは，Webブラウザで

はページ作成者以外が埋め込んだものであると認識できないため，ブラウザ側でこの問題を防止するには，スクリプトを使用しない設定にするほかなく，スクリプトを使用する場合には常にこの問題が発生しうる。

悪意のあるコードを直接埋め込んで実行させるほかに，ユーザに認識のないまま他所のスクリプトを呼び出して実行するよう仕向けることが可能なため，「クロスサイト」の名がついている。

スクリプトの内容によってはCookieデータの盗聴や改竄などが可能なため，商取引に使ったCookieを横取りして，本人になりすまして物品の購入を行ったり，Cookieを認証やセッション管理に使っているサイトに侵入したり，より広範かつ深刻な損害を与える可能性がある。

対策としては，訪問者からの入力内容をそのまま表示せずに，スクリプトなどのコードを識別して無効化する処理を施すことが必要である。」IT用語辞典e-words〈http: //e-words. jp/w/E382AFE383ADE382B9E382B5E382A4E38388E382B9E382AEF383AAE38397E38386E382A3E383B3E382B0.html〉（2012年5月10日確認）

42 「SQLとは，リレーショナルデータベースの操作を行うための言語の一つ。IBM社が開発したもので，ANSI（アメリカ規格協会）やISO（国際標準化機構）によって標準として規格化されている。

SQLは大きく分けてデータ定義言語（DDL：Data Definition Language），データ操作言語（DML：Data Manipulation Language），データ制御言語（DCL：Data Control Language）の3種類から構成される。DDLにはテーブルや制約条件などを定義するCREATE文や，テーブルなどを削除するDROP文などがある。DMLにはレコードの抽出を行うSELECT文や，テーブルにレコードを挿入するINSERT文，レコードを削除するDELETE文，特定のレコードのフィールドを更新するUPDATE文などがある。DCLにはトランザクション処理の開始を宣言するBEGIN文，トランザクションの完了を指示するCOMMIT文，トランザクションを取り消すROLLBACK文などが含まれる。

ソフトウェアからデータベースを操作する場合には，プログラム上でSQL文を生成してこれをRDBMSに発行し，操作を実行する。このため，多くのプログラミング言語処理系や実行環境では，RDBMSに接続してSQL文を発行し結果を受け取るためのプログラミングインターフェースが用意されている。

SQLにはANSIなどが定めた「SQL92」や「SQL99」といった標準規格はあるものの，個々のRDBMSによる独自拡張が数多くあり，システム開発の現場では拡張仕様を駆使してソフトウェアを開発するのが常態となっているため，互換性の確保はなかなか進んでいない。なお，「Structured Query Language」という略称はIBM社の言語についてのものであり，標準規格のSQLの方は公式には何の略でもないということになっている。」IT用語辞典e-words〈http://e-words.jp/w/SQL.

html〉（2012年5月10日確認）

43 「データベースと連動したWebサイトで，データベースへの問い合わせや操作を行うプログラムにパラメータとしてSQL文の断片を与えることにより，データベースを改ざんしたり不正に情報を入手する攻撃。また，そのような攻撃を許してしまうプログラムの脆弱性のこと。

多くのWebアプリケーションではデータベースの操作にSQLという言語を利用しており，ユーザがフォームから送信した検索語などのパラメータを受け取り，これをSQL文に埋め込んでデータベースへの問い合わせや操作を行う。このとき，SQL文の断片として解釈できる文字列をパラメータに含めることで，プログラムが想定していないSQL文を合成し，不正にデータベースの内容を削除したり，本来アクセスできない情報を表示させたりすることができてしまう場合がある。このような攻撃手法をSQLインジェクションという。「インジェクション」（injection）とは「注入」という意味。

SQLインジェクションはパラメータをSQL文に埋め込む際にきちんとチェックが行われていないために起こる。パラメータ中にSQL構文やSQL文で特殊な意味を持つ文字が含まれていないか調べ，含まれていた場合はこれを削除したり別の文字列に変換（エスケープ）するといった処理を組み込む必要がある。」IT用語辞典e-words〈http://e-words.jp/w/SQLE382A4E383B3E382B8E382A7E382AFE382B7E383A7E383B3.html〉（2012年5月10日確認）

44 IBMX-Force 2011 TREND AND RISK REPOT（2012）pp. 74-77.

45 2011年5月には，ソニー・コンピュータエンタテインメントのインターネット配信サービスにおいて，SQLインジェクションによりアプリケーションサーバの脆弱性を突かれて，何者かに不正ツールを埋め込まれ，外部からの侵入経路が確立された結果，侵入者にデータベースのアクセス権限を奪取され，個人情報が保管されているデータベースへの不正アクセスを許してしまったという。これにより会員の個人情報が約7,700万件，クレジットカード情報が約1,000万件流出した可能性があると報道された（2011年5月1日付日本経済新聞，同5月2日付読売新聞等）。

46 たとえば，2011年12月25日付けのウォールストリートジャーナルやワシントンポストによると，国際的ハッカー集団Anonymousにより，米大手シンクタンクStratforがサイバー攻撃を仕掛けられ，電子メールやクレジットカード情報が盗まれ，Anonymousに関連のあるTwitterアカウントで，4,000件のクレジットカード番号などが含まれた複数の暗号化されたファイルへのリンクが投稿されたという。