不正アクセス行為の発生状況

第１　平成22年中の不正アクセス禁止法違反事件の認知・検挙状況等について

平成22年中に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を対象とした。

１　不正アクセス行為の認知状況

(1)　認知件数

平成22年中の不正アクセス行為の認知件数は1,885件で、前年と比べ、910件減少した。

表１－１　不正アクセス行為の認知件数の推移

区分＼年次	平成18年	平成19年	平成20年	平成21年	平成22年
認知件数（件）	946	1,818	2,289	2,795	1,885
海外からのアクセス	37	79	214	40	57
国内からのアクセス	855	1,684	1,993	2,673	1,755
アクセス元不明	54	55	82	82	73

(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（1,405件）、次いで一般企業（457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

区分＼年次	平成18年	平成19年	平成20年	平成21年	平成22年
プロバイダ（件）	602	1,372	1,589	2,321	1,405
一般企業	325	437	685	466	457
大学、研究機関等	6	1	5	4	2
その他	13	8	10	4	21
うち行政機関	5	5	6	3	13
不明	0	0	0	0	0
計	946	1,818	2,289	2,795	1,885

※　「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。

注1　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となる。

(3) 認知の端緒

認知の端緒としては、警察職員による被疑者の取調べ等の警察活動によるものが最も多く（1,488件）、次いで利用権者[注2]からの届出によるもの（314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（66件）、発見者からの通報によるもの（９件）の順となっている。

表１－３　認知の端緒の推移

区分＼年次	平成18年	平成19年	平成20年	平成21年	平成22年
警察活動　(件)	535	1,326	1,567	2,277	1,488
利用権者からの届出	358	415	656	487	314
アクセス管理者からの届出	45	61	60	21	66
発見者からの通報	3	2	4	7	9
その他	5	14	2	3	8
計	946	1,818	2,289	2,795	1,885

(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、情報の不正入手（個人情報の不正入手）が最も多く（1,453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）（255件）、ホームページの改ざん・消去（45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）（40件）、インターネットバンキングの不正送金（22件）、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等）（10件）の順となっている。

表１－４　不正アクセス行為後の行為の内訳

区分＼年次	平成21年	平成22年
情報の不正入手　(件)	185	1,453
オンラインゲームの不正操作	345	255
ホームページの改ざん・消去	33	45
不正ファイルの蔵置	2	40
インターネットバンキングの不正送金	34	22
インターネット・オークションの不正操作	2,152	10
その他	44	60

注2　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、当該特定電子計算機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　金融機関を装って電子メールを送信するなどして、受信者が偽のウェブサイトにアクセスするよう仕向け、そこに個人の識別符号（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。

2　不正アクセス禁止法違反事件の検挙状況

(1)　検挙件数等

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人と、前年と比べ、検挙件数は933件減少し、検挙人員は11人増加した。その内訳をみると、不正アクセス行為に係るものがそれぞれ1,598件、123人、不正アクセス助長行為[注4]に係るものがそれぞれ３件、４人であった。

表２－１　検挙件数等の推移

区分＼年次		平成18年	平成19年	平成20年	平成21年	平成22年
不正アクセス行為	検挙件数	698	1,438	1,737	2,532	1,598
	検挙事件数[注5]	84	86	101	95	103
	検挙人員	130	126	135	114	123
不正アクセス助長行為	検挙件数	5	4	3	2	3
	検挙事件数	3	2	3	1	3
	検挙人員	5	4	3	1	4
計	検挙件数（件）	703	1,442	1,740	2,534	1,601
	検挙事件数（事件）	84 (重複3)	86 (重複2)	101 (重複3)	95 (重複1)	104 (重複2)
	検挙人員（人）	130 (重複5)	126 (重複4)	137 (重複1)	114 (重複1)	125 (重複2)

※　(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6]が1,597件であり、セキュリティ・ホール攻撃型[注7]は１件であった。

注4　他人の識別符号をどのコンピュータに対する識別符号であるかを明らかにして、又はこれを知っている者の求めに応じて、アクセス管理者や利用権者に無断で第三者に提供する行為をいう。

注5　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6　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。

注7　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。

表２－２　不正アクセス行為の態様の推移

区分＼年次		平成18年	平成19年	平成20年	平成21年	平成22年
識別符号窃用型	検挙件数	698	1,438	1,736	2,529	1,597
	検挙事件数	84	86	100	94	102
セキュリティ・ホール攻撃型	検挙件数	0	0	1	3	1
	検挙事件数	0	0	1	1	1
計	検挙件数（件）	698	1,438	1,737	2,532	1,598
	検挙事件数（事件）	84	86	101	95	103

３　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手口についてみると、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（1,411件）が最も多く、次いで、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（70件）、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（57件）となっている。また、スパイウェア[注8]等のプログラムを使用して識別符号を入手したもの（14件）、共犯者等から入手したもの（12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（12件）等も依然として発生している。

表３－１　不正アクセス行為に係る犯行の手口の内訳

区分＼年次		平成21年	平成22年
識別符号窃用型　(件)		2,529	1,597
	フィッシングサイトにより入手したもの	2,084	1,411
	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	58	70
	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	61	57
	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	8	14
	共犯者等から入手したもの	167	12
	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	12	12
	他人から購入したもの	92	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	0	0
	その他	47	17
セキュリティ・ホール攻撃型		3	1

注8　パソコン内のファイル又は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をいう。

(2)　被疑者

不正アクセス禁止法違反に係る被疑者と識別符号を窃用された利用権者の関係についてみると、元交際相手や元従業員等の顔見知りの者によるものが最も多く（65人）、次いで交友関係のない他人によるもの（36人）、ネットワーク上の知り合いによるもの（24人）となっている。

また、被疑者の年齢についてみると、20歳代（39人）が最も多く、30歳代（35人）、10歳代（29人）、40歳代（17人）、50歳代（５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58歳であった。

表３－２　年代別被疑者数の推移

区分＼年次	平成18年	平成19年	平成20年	平成21年	平成22年
10歳代　(人)	40	39	48	31	29
20歳代	44	39	42	33	39
30歳代	28	34	35	35	35
40歳代	15	12	11	13	17
50歳代	2	2	1	2	5
60歳代	1	0	0	0	0
計	130	126	137	114	125

※　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（1,455件）が最も多く、次いで嫌がらせや仕返しのため（66件）、好奇心を満たすため（33件）、オンラインゲームで不正操作を行うため（19件）、顧客データの収集等情報を不正に入手するため（18件）、料金の請求を免れるため（４件）の順となっている。

表３－３　不正アクセス行為の動機の内訳

区分＼年次	平成21年	平成22年
不正に金を得るため　(件)	2,245	1,455
嫌がらせや仕返しのため	34	66
好奇心を満たすため	165	33
オンラインゲームで不正操作を行うため	63	19
顧客データの収集等情報を不正に入手するため	19	18
料金の請求を免れるため	4	4
その他	2	3
計	2,532	1,598

(4)　利用されたサービス

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為（1,597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をみると、会員専用・社員用内部サイトが最も多く（1,432件）、次いでオンラインゲーム（71件）、電子メール（36件）、ホームページ公開サービス（25件）、インターネットショッピング（16件）、インターネットバンキング（７件）、インターネット・オークション（２件）の順となっている。

表３－４　利用されたサービスの内訳

区分＼年次		平成21年	平成22年
識別符号窃用型　(件)		2,529	1,597
	会員専用・社員用内部サイト	10	1,432
	オンラインゲーム	88	71
	電子メール	167	36
	ホームページ公開サービス	16	25
	インターネットショッピング	3	16
	インターネットバンキング	83	7
	インターネット・オークション	2,147	2
	その他	15	8

4　都道府県公安委員会による援助措置

平成22年中、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・指導はなかった。

表４－１　都道府県公安委員会の援助措置実施件数の推移

区分＼年次	平成18年	平成19年	平成20年	平成21年	平成22年
援助措置　(件)	3	0	1	0	0

5　防御上の留意事項

(1)　利用権者の講ずべき措置

ア　フィッシングに対する注意

電子メールにより本物のウェブサイトに酷似したフィッシングサイトに誘導し、ＩＤ・パスワードやクレジットカード情報を不正に取得する事案が多発していることから、発信元に心当たりのない電子メールに注意する。また、金融機関等が電子メールで口座番号や暗証番号、個人情報を問い合わせることはなく、これらの情報の入力を求める電子メールはフィッシングメールであると考えられることから、情報を入力しない。

イ　スパイウェア等の不正プログラムに対する注意

ファイル共有ソフトやウェブサイト上に蔵置したファイルを用い、スパイウェア等の不正プログラムに感染させ、他人のＩＤ・パスワードを不正に取得する事案が発生していることから、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。また、不特定多数が利用するコンピュータでは重要な情報を入力しない。さらに、スパイウェア対策やコンピュータ・ウイルス対策（対策ソフト、オペレーティングシステム及びソフトウェアのアップデート等）を適切に講ずる。

ウ　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の甘さにつけ込んだ不正アクセス行為、知人等による不正アクセス行為、他人から購入したＩＤ・パスワードによる不正アクセス行為が発生していることから、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やＩＤの一部を使ったパスワード等、パスワードの推測が容易なものは避ける、複数のサイトで同じパスワードを使用しないなどの対策を講じる。また、パスワードを定期的に変更する、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パスワードは適切に管理する。

(2)　アクセス管理者等の講ずべき措置

ア　フィッシング、スパイウェア等への対策

フィッシング、スパイウェ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が多発していることから、インターネットショッピング、オンラインゲーム、インターネットバンキング等のサービスを提供する事業者にあっては、ワンタイムパスワード[注9]等により個人認証を強化するなどの対策を講ずる。

イ　ＳＱＬインジェクション攻撃[注10]への対応

セキュリティホール攻撃の一つであるＳＱＬインジェクション攻撃を受け、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が発生していることから、アクセス管理者は、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し、ＳＱＬインジェクション攻撃に対する監視体制を強化する。

ウ　ウェブサイトの安全な管理

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が多発したことから、アクセス管理者は、ウェブサイトの更新の際には、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。

注9　インターネット銀行等における認証用のパスワードであって、認証の度にそれを構成する文字列が変わるものをいう。これを導入することにより、識別符号を盗まれても次回の利用時に使用できないこととなる。

注10　ＳＱＬというプログラム言語を用いて、企業等が個人情報を管理するデータベースを外部から不正に操作する行為をいう。

エ　識別符号の適切な管理

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も引き続き発生していることから、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。

オ　パスワードの適切な設定・運用体制の構築

利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為が発生していることから、アクセス管理者は、容易に推測されるパスワードを設定できないようにしたり、定期的にパスワードの変更を促す仕組みを構築したりするなどの措置を講ずる。

６　検挙事例

１	フィッシングにより他人のＩＤ・パスワードやクレジットカード番号等を不正に入手し、インターネットショッピングにおいて商品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（32）らは、平成20年９月から平成21年11月までの間、フィッシングにより他人のＩＤ・パスワードやクレジットカード番号等を入手し、会員専用サイトに不正アクセスを行い、個人情報を入手した上、それを用いて他人になりすましてインターネットショッピングにおいて商品をだまし取った。平成22年８月までに、不正アクセス禁止法違反及び詐欺罪で検挙した（広島、岡山、静岡、福岡、愛媛）。

２	スパイウェアにより他人のＩＤ・パスワードを不正に取得し、オンラインゲームに不正アクセスするなどした不正アクセス禁止法違反事件

会社員の男（29）らは、平成22年４月から６月までの間、スパイウェアを組み込んだウェブサイトを開設して他人のＩＤ・パスワードを不正に取得し、それを用いてオンラインゲームに不正アクセスを行い、入手したオンラインゲーム上のアイテムを現金に換金した。平成22年11月、不正アクセス禁止法違反で検挙した（神奈川）。

３	他人のＩＤ・パスワードを使用して航空会社のウェブサイトに不正アクセスを行い、マイレージをだまし取るなどした不正アクセス禁止法違反及び電子計算機使用詐欺等事件

会社役員の男（52）は、平成20年６月、取引先会社役員のＩＤ・パスワードを使用して航空会社のウェブサイトに不正アクセスを行い、同人の口座内のマイレージを自らが同人名義で開設したインターネットショッピングサイト内の口座に移し替え、それを使用して商品を購入した。平成22年４月、不正アクセス禁止法違反、電子計算機使用詐欺罪等で検挙した（警視庁）。

4	パスワード再発行機能を悪用して他人のＩＤ・パスワードを不正入手し、オンラインゲームに不正アクセスするなどした不正アクセス禁止法違反等事件

無職の少年（18）らは、平成22年２月から３月までの間、オンラインゲームのパスワード再発行機能を悪用して他人のＩＤ・パスワードを不正に入手した上、それを用いてオンラインゲームに不正アクセスを行い、入手したオンラインゲームのアイテムや仮想通貨を現金に換金した。平成22年９月までに、不正アクセス禁止法違反等で検挙した（愛知、宮城、福島）。

5	フィッシングにより他人のＩＤ・パスワードを不正に入手してＳＮＳ[注11]に不正アクセスを行い、女性会員になりすまして出会い系サイトに勧誘した不正アクセス禁止法違反等事件

無職の男（24）らは、平成20年８月、フィッシングにより入手した他人のＩＤ・パスワードを用いてＳＮＳに不正アクセスを行い、女性会員になりすましてＳＮＳで出会った者に電子メールを送信し、自らが経営する出会い系サイトに誘導した。平成22年３月までに、不正アクセス禁止法違反等で検挙した（警視庁、宮城）。

注11　ソーシャルネットワーキングサービス（Social Networking Service）の略。登録したユーザのみが参加できるインターネット上のウェブサイトのことをいう。

第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

１　独立法人情報処理推進機構（ＩＰＡ）に届出のあったコンピュータ不正アクセスの届出状況について

平成 22 年 1 月 1 日から 12 月 31 日の間に IPA に届出のあったコンピュータ不正アクセス（注１）が対象である。

コンピュータ不正アクセスに関する届出件数は 197 件（平成 21 年：149 件）であった。（注２）

平成 22（2010）年は同 21（2009） 年と比べて、48 件（約 32%）増加した。

届出のうち実際に被害があったケースにおける被害内容の分類では、「侵入」および「なりすまし」による被害届出が多く寄せられた。

以下に、種々の切り口で分類した結果を示す。各々の件数には未遂（実際の被害はなかったもの）も含まれる。また、１件の届出にて複数の項目に該当するものがあるため、それぞれの分類での総計件数はこの数字に必ずしも一致しない。

(1) 手口別分類

意図的に行う攻撃行為による分類である。1 件の届出について複数の攻撃行為を受けている場合もあるため、届出件数とは一致せず総計は 365 件（平成 21 年：254 件）となる。

ア　侵入行為に関して

侵入行為に係わる攻撃等の届出は 309 件（平成 21 年：211 件）あった。

(ｱ) 侵入の事前調査行為

システム情報の調査、稼動サービスの調査、アカウント名の調査等である。

18 件の届出があり、ポートやセキュリティホールを探索するものであった。

(ｲ) 権限取得行為（侵入行為）

パスワード推測やソフトウェアのバグ等いわゆるセキュリティホールを利用した攻撃システムの設定内容を利用した攻撃など侵入のための行為である。

152 件の届出があり、これらのうち実際に侵入につながったものは 60 件である。

【主な内容】

パスワード推測：21 件

ソフトウェアの脆弱性やバグを利用した攻撃：11 件

(ｳ) 不正行為の実行及び目的達成後の行為

侵入その他､何らかの原因により不正行為を実行されたことについては139 件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：48 件

資源利用（ファイル、CPU 使用）：43 件

プログラムの作成・設置（インストール）、トロイの木馬などの埋め込み等：31 件

踏み台とされて他のサイトへのアクセスに利用された：14 件

イ　サービス妨害攻撃

過負荷を与えたり、例外処理を利用してサービスを不可もしくは低下させたりする攻撃である。8 件（平成 21 年：6 件）の届出があった。

ウ　その他

その他にはメール不正中継やメールアドレス詐称、正規ユーザになりすましてのサービス不正利用、ソーシャルエンジニアリングなどが含まれ、48 件（平成 21 年：37 件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：36 件

ソーシャルエンジニアリング：5 件

メールアドレス（ドメイン）の詐称：3 件

メール不正中継：1 件

(2) 原因別分類

不正アクセスを許した問題点／弱点による分類である。

197 件の届出中、実際に被害に遭った計 123 件（平成 21 年：96 件）を分類すると以下のようになる。

被害原因として「ID、パスワード管理不備」や「古いバージョン使用、パッチ未導入など」が多くなっているなど、基本的なセキュリティ対策が成されていないサイトが狙われていると推測される。また、原因が不明なケースがますます多くなっており、手口が巧妙化するとともに原因究明が困難な事例が多いことが推測される。

【主な要因】

ID、パスワード管理の不備によると思われるもの：16 件

古いバージョンの利用や、パッチ・必要なプラグインなどの未導入によるもの：13 件

設定の不備（セキュリティ上問題のあるデフォルト設定を含む）による

もの：7 件
DoS 攻撃・その他によるもの：12 件
原因不明：75 件

(3) 電算機分類

不正アクセス行為の対象となった機器による分類である。(被害の有無は問わない)

【主な対象】

WWW サーバ：98 件
メールサーバ：24 件
クライアント：15 件
ファイアウォール：2 件
ルータ：1 件
その他のサーバ：21 件
不明：3 件
※1 件の届出で複数の項目に該当するものがある

(4) 被害内容分類

197 件の届出を被害内容で分類した 214 件中、実際に被害に遭ったケースにおける被害内容による分類である。機器に対する実被害があった件数は 140 件（昨年：107 件）である。なお、対処にかかわる工数やサービスの一時停止、代替機の準備などに関する被害は除外している。

【主な被害内容】

ホームページ改ざん：35 件
オンラインサービスの不正利用：35 件
踏み台として悪用：25 件
ファイルの書き換え：20 件
サービス低下：6 件
データの窃取や盗み見：5 件
不正アカウントの作成：2 件
サーバダウン：1 件
※1 件の届出で複数の項目に該当するものがある

(5) 対策情報

平成 22（2010）年は、いわゆる「ガンブラー」によるウェブサイト改ざんの被害が特に多かったと言える。また、その被害原因の多くが不明なケースだったことから、こうした改ざんを行うための攻撃手口の巧妙化が伺える。その他では、なりすましによってオンラインゲームなどのサービスを勝手に使われて

金銭被害が出たケースや、SSH[1]で使用するポートへの攻撃で侵入（ID、パスワードの設定不備が主な原因）され、他のコンピュータを攻撃するための踏み台に悪用されていた被害も目立っていたと言える。主に原因不明なケースが多く見受けられたが、基本的なセキュリティ対策を実施していれば、被害を免れていたと思われるケースが多く見受けられる。システム管理者は以下の点を確認して総合的に対策を行うことが望まれる。

- ID やパスワードの厳重な管理及び設定
- 脆弱性の解消（修正プログラム適用不可の場合は、運用による回避策も含む）
- ルータやファイアウォールなどの設定やアクセス制御設定
- こまめなログのチェック

また、個人ユーザにおいても同様に以下の点に注意することが望まれる。

- Windows Update や Office Update など､OS やアプリケーションソフトのアップデート
- パスワードの設定と管理（複雑化、定期的に変更、安易に他人に教えないなど）
- ルータやパーソナルファイアウォールの活用
- 無線 LAN の暗号化設定確認（WEP は使用せず、できる限り WPA2 を使用する）

下記ページなどを参照し、今一度状況確認・対処されたい。

【システム管理者向け】

「情報セキュリティに関する啓発資料」
http://www.ipa.go.jp/security/fy18/reports/contents/

「脆弱性対策のチェックポイント」
http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

「安全なウェブサイトの作り方　改訂第 4 版」
http://www.ipa.go.jp/security/vuln/websecurity.html

「JVN (Japan Vulnerability Notes)」　※脆弱性対策情報ポータルサイト
http://jvn.jp/

「SQL インジェクション攻撃に関する注意喚起」
http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html

「ウェブサイトで利用されている DNS サーバの既知の脆弱性への注意喚起」
http://www.ipa.go.jp/security/vuln/documents/2009/200912_dns.html

[1] SSH(Secure Shell) : ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。

「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」
http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html
「ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起」
http://www.ipa.go.jp/security/topics/20091224.html

【個人ユーザ向け】
「IPA セキュリティセンター・個人ユーザ向けページ」
http://www.ipa.go.jp/security/personal/
「マイクロソフトセキュリティ At Home」（マイクロソフト社）
http://www.microsoft.com/japan/protect/default.mspx
「MyJVN」（セキュリティ設定チェッカ、バージョンチェッカ）
http://jvndb.jvn.jp/apis/myjvn/
「一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起」
http://www.ipa.go.jp/security/topics/20091224.html

ウイルス対策を含むセキュリティ関係の情報・対策などについては、下記ページを参照のこと。
「IPA セキュリティセンタートップページ」
http://www.ipa.go.jp/security/

注１　コンピュータ不正アクセス
システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うこと。

注２　ここにあげた件数は、コンピュータ不正アクセスの届出を IPA が受理した件であり、不正アクセスやアタック等に関して実際の発生件数や被害件数を直接類推できるような数値ではない。

2　JPCERT コーディネーションセンター（以下、JPCERT/CC）に報告（調整対応依頼）があった不正アクセス関連行為の状況について

平成 22 年 1 月 1 日から 12 月 31 日の間に JPCERT/CC に報告（調整対応依頼）のあったコンピュータ不正アクセスが対象である。

※本年度、データ集計カテゴリの見直しを行った結果、集計結果に以下の変更があります。
- 「ウ　電子メールの送信ヘッダを詐称したメールの配送」は廃止し、報告件数は「カ その他」に集計。
- 「カ その他」にて集計していたマルウエア配布サイトやマルウエア公開サイトに関する報告は、新たに「ウ マルウエア」を新設し、集計。

(1) 不正アクセス関連行為の特徴および件数

報告（調整対応依頼）のあった不正アクセス関連行為(注１)に係わる報告件数(注２)は 11,769 件であった。

ア　プローブ、スキャン、その他不審なアクセスに関する報告

防御に成功したアタックや、コンピュータ／サービス／弱点の探査を意図したアクセス、その他の不審なアクセス等、システムのアクセス権において影響を生じないか、無視できるアクセスについて 2,291 件の報告があった。

[1/1-3/31: 322 件、4/1-6/30:349 件、7/1-9/30:492 件、10/1-12/31: 1128 件]

イ　システムへの侵入

管理者権限の盗用が認められる場合やワーム等を含め、システムへの侵入について 1,922 件の報告があった。

[1/1-3/31: 809 件、4/1-6/30: 561 件、7/1-9/30:353 件、10/1-12/31: 199 件]

ウ　マルウエアサイト

閲覧することで PC がマルウエアに感染してしまう攻撃用サイトや攻撃に使用するマルウエアを公開しているサイトについて 4,425 件の報告があった。

[1/1-3/31: 1,410 件、4/1-6/30: 1,478 件、7/1-9/30:965 件、10/1-12/31: 572 件]

エ　ネットワークやコンピュータの運用を妨害しようとする攻撃

大量のパケットや予期しないデータの送信によって、サイトのネットワークやホストのサービス運用を妨害しようとするアクセスについて 11 件の報告があった。

[1/1-3/31:0 件、4/1-6/30:2 件、7/1-9/30:5 件、10/1-12/31:4 件]

オ　Web 偽装事案(phishing)

Web のフォームなどから入力された口座番号やキャッシュカードの暗証番号といった個人情報を盗み取る Web 偽装事案について 1,786 件の報告があった。

[1/1-3/31: 373 件、4/1-6/30: 388 件、7/1-9/30: 487 件、10/1-12/31:538 件]

カ　その他

コンピュータウイルス、SPAM メールの受信等について 1,334 件の報告があった。

[1/1-3/31:271 件、4/1　-6/30:407 件、7/1-9/30:459 件、10/1-12/31:197 件]

(2) 防御に関する啓発および対策措置の普及

JPCERT/CC は、日本国内のインターネット利用者に対して、不正アクセス関連行為を防止するための予防措置や、発生した場合の緊急措置などに関する情報を提供し、不正アクセス関連行為への認識の向上や適切な対策を促進するため、以下の文書を公開している(詳細は http://www.jpcert.or.jp/参照。)

ア　注意喚起

[新規]

2010 年 1 月	Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起 Microsoft セキュリティ情報 (緊急 1 件) に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起
2010 年 2 月	FTP アカウント情報を盗むマルウエアに関する注意喚起 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起
2010 年 3 月	Microsoft Internet Explorer の脆弱性 (MS10-018) に関する注意喚起
2010 年 4 月	Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 Oracle Sun JDK および JRE の脆弱性に関する注意喚起 いわゆる Gumblar ウイルスによってダウンロードされる DDoS 攻撃を行うマルウエアに関する注意喚起
2010 年 5 月	Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起
2010 年 6 月	社内 PC のマルウエア感染調査を騙るマルウエア添付メールに関する注意喚起 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 Adobe Flash Player および Adobe Acrobat/Reader の脆弱性に関

	する注意喚起 Windows のヘルプとサポートセンターの未修正の脆弱性に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2010 年 7 月	Microsoft セキュリティ情報（緊急 3 件含）に関する注意喚起
2010 年 8 月	Windows シェルの脆弱性（MS10-046）に関する注意喚起 Microsoft セキュリティ情報（緊急 8 件含）に関する注意喚起 Adobe Flash Player の脆弱性に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2010 年 9 月	Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起 Adobe Flash Player の脆弱性に関する注意喚起
2010 年 10 月	攻撃用ツールキットを使用した Web サイト経由での攻撃に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起 アクセス解析サービスを使用した Web サイト経由での攻撃に関する注意喚起
2010 年 11 月	Adobe Flash Player の脆弱性に関する注意喚起 Microsoft セキュリティ情報（緊急 1 件含）に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2010 年 12 月	不適切な設定で Asterisk を利用した場合に発生し得る不正利用に関する注意喚起 Microsoft セキュリティ情報（緊急 2 件含）に関する注意喚起

イ　活動概要（報告状況等の公表）

発行日：2011-01-12 [2010 年 10 月 1 日～ 2010 年 12 月 31 日]
発行日：2010-10-07 [2010 年 7 月 1 日 ～ 2010 年 9 月 30 日]
発行日：2010-07-07 [2010 年 4 月 1 日 ～ 2010 年 6 月 30 日]
発行日：2010-04-08 [2010 年 1 月 1 日 ～ 2010 年 3 月 31 日]

ウ　JPCERT/CC レポート

[発行件数] 49 件
[取り扱ったセキュリティ関連情報数] 287 件

(3) 定点観測システム

インターネット定点観測システム（ISDAS）を運用することによってワームやウイルスの感染活動や弱点探索のためのスキャンなど、セキュリティ上の脅

威となるトラフィックの観測を行い、JPCERT/CC における分析や情報発信に活用しているほか、ウェブサイトにて観測情報を提供している。
（詳細は http://www.jpcert.or.jp/isdas/参照。）

注１　不正アクセス関連行為とは、コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的(または、偶発的) に発生する全ての事象が対象になる。

注２　ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際のアタックの発生件数や、被害件数を類推できるような数値ではない。また類型ごとの実際の発生比率を示すものでもない。一定以上の期間に渡るアクセスの要約レポートも含まれるため、アクセスの回数と報告件数も一般に対応しない。報告元には、国内外のサイトが含まれる。

3　脆弱性対策情報について

日本国内の製品開発者(ベンダ) などの関連組織とのコーディネーションを行ない、JVN (Japan Vulnerability Notes) にて公開した脆弱性情報は 181 件であっ た(詳細は http://jvn.jp/参照。)
[1/1-3/31:26 件、4/1-6/30:41 件、7/1-9/30:41 件、10/1-12/31:73 件]

そのうち、平成 16 年 7 月の経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に従って、JVN にて公開した脆弱性情報は 66 件であった。
[1/1-3/31:06 件、4/1-6/30:20 件、7/1-9/30:09 件、10/1-12/31:31 件]