不正アクセス行為の発生状況

第１　平成23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23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23年中の不正アクセス行為の認知件数は889件で、前年と比べ、996件減少した。

※　ここでいう認知件数とは、不正アクセス被害の届出を受理した場合のほか、余罪として確認した場合、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において、被疑者が行った構成要件に該当する行為の数をいう。

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19年	平成20年	平成21年	平成22年	平成23年
認知件数（件）	1,818	2,289	2,795	1,885	889
海外からのアクセス	79	214	40	57	110
国内からのアクセス	1,684	1,993	2,673	1,755	678
アクセス元不明	55	82	82	73	101

(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、一般企業が最も多く（762件）、次いでプロバイダ（115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19年	平成20年	平成21年	平成22年	平成23年
一般企業（件）	437	685	466	457	762
プロバイダ	1,372	1,589	2,321	1,405	115
大学、研究機関等	1	5	4	2	1
その他	8	10	4	21	11
うち行政機関	5	6	3	13	6
不明	0	0	0	0	0
計	1,818	2,289	2,795	1,885	889

※　「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、利用権者[注2]からの届出によるものが最も多く（680件）、次いで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（121件）、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（75件）、発見者からの通報によるもの（７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19年	平成20年	平成21年	平成22年	平成23年
利用権者からの届出　(件)	415	656	487	314	680
アクセス管理者からの届出	61	60	21	66	121
警察活動	1,326	1,567	2,277	1,488	75
発見者からの通報	2	4	7	9	7
その他	14	2	3	8	6
計	1,818	2,289	2,795	1,885	889

(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、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）が最も多く（358件）、次いでインターネットバンキングの不正送金（188件）、インターネットショッピングの不正購入（172件）、情報の不正入手（個人情報の不正入手）（74件）、ホームページの改ざん・消去（28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）（22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）（４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22年	平成23年
オンラインゲームの不正操作　(件)	255	358
インターネットバンキングの不正送金	22	188
インターネットショッピングの不正購入	12	172
情報の不正入手	1,453	74
ホームページの改ざん・消去	45	28
インターネット・オークションの不正操作	10	22
不正ファイルの蔵置	40	4
その他	48	43

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たり、受信者に添付ファイルを開かせることにより、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23年中における不正アクセス禁止法違反の検挙件数は248件、検挙人員は114人と、前年と比べ、検挙件数は1,353件減少し、検挙人員は11人減少した。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242件、110人、不正アクセス助長行為[注4]に係るものがそれぞれ６件、６人であった。

表２－１　検挙件数等の推移

区分 ＼ 年次		平成19年	平成20年	平成21年	平成22年	平成23年
不正アクセス行為	検挙件数	1,438	1,737	2,532	1,598	242
	検挙事件数[注5]	86	101	95	103	101
	検挙人員	126	135	114	123	110
不正アクセス助長行為	検挙件数	4	3	2	3	6
	検挙事件数	2	3	1	3	6
	検挙人員	4	3	1	4	6
計	検挙件数（件）	1,442	1,740	2,534	1,601	248
	検挙事件数（事件）	86 (重複2)	101 (重複3)	95 (重複1)	104 (重複2)	103 (重複4)
	検挙人員（人）	126 (重複4)	137 (重複1)	114 (重複1)	125 (重複2)	114 (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241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19年	平成20年	平成21年	平成22年	平成23年
識別符号窃用型	検挙件数	1,438	1,736	2,529	1,597	241
	検挙事件数	86	100	94	102	100
セキュリティ・ホール攻撃型	検挙件数	0	1	3	1	1
	検挙事件数	0	1	1	1	1
計	検挙件数（件）	1,438	1,737	2,532	1,598	242
	検挙事件数（事件）	86	101	95	103	101

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（59件）及び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（59件）が最も多く、次いで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（52件）となっている。また、共犯者等から入手したもの（38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（29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22年	平成23年
識別符号窃用型　(件)		1,597	241
	フィッシングサイトにより入手したもの	1,411	59
	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	59
	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	52
	共犯者等から入手したもの	12	38
	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	29
	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	1
	他人から購入したもの	4	0
	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	17	3
セキュリティ・ホール攻撃型		1	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、漏えいさせ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（54人）、次いで交友関係のない他人によるもの（34人）、ネットワーク上の知り合いによるもの（26人）となっている。

また、被疑者の年齢についてみると、10歳代（51人）が最も多く、20歳代（30人）、30歳代（19人）、40歳代（10人）、50歳代（２人）及び60歳代（２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66歳であった。

表３－２　年代別被疑者数の推移

区分＼年次	平成19年	平成20年	平成21年	平成22年	平成23年
10歳代　(人)	39	48	31	29	51
20歳代	39	42	33	39	30
30歳代	34	35	35	35	19
40歳代	12	11	13	17	10
50歳代	2	1	2	5	2
60歳代	0	0	0	0	2
計	126	137	114	125	114

※　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、不正に経済的利益を得るため（97件）が最も多く、次いで嫌がらせや仕返しのため（58件）、オンラインゲームで不正操作を行うため（39件）、好奇心を満たすため（32件）、顧客データの収集等情報を不正に入手するため（15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22年	平成23年
不正に経済的利益を得るため　(件)	1,455	97
嫌がらせや仕返しのため	66	58
オンラインゲームで不正操作を行うため	19	39
好奇心を満たすため	33	32
顧客データの収集等情報を不正に入手するため	18	15
料金の請求を免れるため	4	0
その他	3	1
計	1,598	242

(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（241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、インターネットショッピングが最も多く（87件）、次いでオンラインゲーム（51件）、会員専用・社員用内部サイト（48件）、電子メール（23件）、インターネットバンキング（14件）、ホームページ公開サービス（５件）、インターネット・オークション（４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22年	平成23年
識別符号窃用型　(件)		1,597	241
	インターネットショッピング	16	87
	オンラインゲーム	71	51
	会員専用・社員用内部サイト	1,432	48
	電子メール	36	23
	インターネットバンキング	7	14
	ホームページ公開サービス	25	5
	インターネット・オークション	2	4
	その他	8	9

4　都道府県公安委員会による援助措置

平成23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19年	平成20年	平成21年	平成22年	平成23年
援助措置　(件)	0	1	0	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たり、添付されたファイルを開かせたりして、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　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、言葉巧みに聞き出した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、パスワードを他人に教えない、パスワードを定期的に変更するなど自己のパスワードを適切に管理する。

ウ　不正プログラムに対する注意

コンピュータに不正プログラムを感染させ、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、信頼できない電子メールに添付されたファイルを不用意に開いたり、信頼できないウェブサイト上に蔵置されたファイルを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、コンピュータ・ウイルス対策等の不正プログラム対策（ウイルス対策ソフトの利用のほか、オペレーティングシステムやウイルス対策ソフトを含む各種ソフトウェアのアップデート等）を適切に講ずる。

(2)　アクセス管理者等の講ずべき措置

ア　フィッシング等への対策

フィッシング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　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多発していることから、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。

ウ　ＩＤ・パスワードの適切な管理

ＩＤ・パスワード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。

エ　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。

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。

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

中古品買取業の男（27）らは、平成21年９月から平成23年６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、クレジットカード会社のウェブサイトに不正アクセスを行い、インターネットショッピング等において合計約１億円相当の商品をだまし取るなどした。平成23年11月までに、不正アクセス禁止法違反及び電子計算機使用詐欺罪等で検挙した（静岡、茨城、千葉、熊本、広島）。

2	他人のＩＤからそのパスワードを類推してＳＮＳ[注11]サイトに不正アクセスを行い、女性会員になりすましてメッセージを送信した不正アクセス禁止法違反事件

派遣社員の男（28）は、平成23年８月、他人のＩＤからそのパスワードを類推してＳＮＳサイトに不正アクセスを行い､女性会員になりすましてメッセージを送信した。平成23年12月、不正アクセス禁止法違反で検挙した（高知）。

3	在職中に入手した他人のＩＤ・パスワードを使用してインターネットバンキングに不正アクセスを行い、現金を不正送金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

会社員の男（33）は、平成20年２月から４月までの間、在職中に入手した勤務先のインターネットバンキングのＩＤ・パスワードを使用して不正アクセスを行い、架空名義の健康保険証を使用して不正取得した銀行口座に不正送金した。平成23年３月、不正アクセス禁止法違反及び電子計算機使用詐欺等で検挙した（神奈川）。

4	パソコンに保存されていた他人のＩＤ・パスワードを使用してインターネットバンキングに不正アクセスを行い、現金を不正送金した不正アクセス禁止法違反及び電子計算機使用詐欺事件

通信販売業の男（46）は、平成22年８月、修理を頼まれたパソコンに保存されていた他人のインターネットバンキングのＩＤ・パスワードを使用して不正アクセスを行い、自己名義の銀行口座に不正送金した。平成23年８月、不正アクセス禁止法違反及び電子計算機使用詐欺で検挙した（埼玉）。

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をいう。

５	言葉巧みに聞き出した元同僚のＩＤ・パスワードを使用して、以前に勤務していた会社の顧客情報システムに不正アクセスを行い、顧客情報を入手した不正アクセス禁止法違反事件

会社員の男（54）は、平成23年８月から９月までの間、言葉巧みに聞き出した元同僚のＩＤ・パスワードを使用して、以前に勤務していた会社の顧客情報システムに不正アクセスを行い、氏名、住所、注文内容等の顧客情報を入手した上、それを用いて顧客と契約した。平成23年11月、不正アクセス禁止法違反で検挙した（新潟）。

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23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103件（平成22年：197件）であった。（注２）

平成23年は同22年と比べて、94件（約48%）減少した。

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」及び「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。個々の件数には未遂（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180件（平成22年：365件）となる。

ア　侵入行為に関して

侵入行為に係る攻撃等の届出は145件（平成22年：309件）あった。

(ｱ) 侵入の事前調査行為

システム情報の調査、稼働サービスの調査、アカウント名の調査等である。

１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等侵入のための行為である。

68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28件である。

【主な内容】

パスワード推測：８件

ソフトウェアのぜい弱性やバグを利用した攻撃：９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76件の届出があった。

【主な内容】

資源利用（ファイル、CPU使用）：21件

ファイル等の改ざん、破壊等：19件

プログラムの作成・設置（インストール）、トロイの木馬等の埋め込み等：16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：11件

証拠の隠滅（ログの消去等）：３件

裏口（バックドア）の作成：１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若しくは低下させたりする攻撃である。７件（平成22年：８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の不正利用、ソーシャルエンジニアリング等が含まれ、28件（平成22年：48件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：27件

メールの不正中継：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。

103件の届出中、実際に被害に遭った計75件（平成22年：123件）を分類すると次のようになる。

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、パッチ未導入等」が多くなっているなど、基本的なセキュリティ対策がな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：15件

古いバージョンの利用や、パッチ・必要なプラグイン等の未導入によるもの：12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：11 件
DoS 攻撃・その他によるもの：５件
原因不明：32 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：47 件
メールサーバ：19 件
クライアント：１件
その他のサーバ：16 件
不明：14 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

103 件の届出を被害内容で分類した 109 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 81 件（昨年：140 件）である。

なお、対処に係る工数やサービスの一時停止、代替機の準備等に関する被害は除外している。

【主な被害内容】
踏み台として悪用：27 件
オンラインサービスの不正利用：17 件
ホームページ改ざん：13 件
データの窃取や盗み見：８件
サービス低下：７件
ファイルの書換え：４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 23 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減少した反面、CMS（Contents Management System）のぜい弱性を悪用したウェブサイト改ざんが多かったといえる。また、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うかがえる。その他では、なりすましによってオンラインゲーム等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 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いえる。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。システム管理者は次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
- ぜい弱性の解消（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等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次の点に注意することが望まれる。

- Windows Update や Office Update 等、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等）
- 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。）

下記ページ等を参照し、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 5 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

「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/
「セーフティとセキュリティセンター」（日本マイクロソフト社）
http://www.microsoft.com/ja-jp/security/default.aspx
「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/
「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」
http://www.ipa.go.jp/security/topics/alert20110803.html

ウイルス対策を含むセキュリティ関係の情報・対策等については、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　ここに挙げた件数は、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 23 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。

(1) 不正アクセス関連行為の特徴及び件数

報告（調整対応依頼）のあった不正アクセス関連行為(注１)に係る報告件数(注２)は 7,722 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 4,580 件の報告があった。

[1/1-3/31: 919 件、4/1-6/30:958 件、7/1-9/30:1,079 件、10/1-12/31: 1,624 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 320 件の報告があった。

[1/1-3/31: 49 件、4/1-6/30: 34 件、7/1-9/30:73 件、10/1-12/31: 164 件]

ウ　マルウェアサイト

閲覧することで PC がマルウェ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ェアを公開しているサイトについて 789 件の報告があった。

[1/1-3/31: 352 件、4/1-6/30: 121 件、7/1-9/30:185 件、10/1-12/31: 131 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５件の報告があった。

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

オ　Web 偽装事案(phishing)

Web のフォーム等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 1,270 件の報告があった。

[1/1-3/31: 405 件、4/1-6/30: 325 件、7/1-9/30: 226 件、10/1-12/31:314 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 496 件の報告があった。

[1/1-3/31:155 件、4/1-6/30:123 件、7/1-9/30:113 件、10/1-12/31:105 件]

(2) 防御に関する啓発及び対策措置の普及

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等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、次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]

平成23年1月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起
平成23年2月	主に UNIX / Linux 系サーバを対象としたインターネット公開サーバのセキュリティ設定に関する注意喚起 Microsoft セキュリティ情報（緊急 3 件含む。）に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起
平成23年3月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起 Adobe Flash Player 及び Adobe Reader / Acrobat のぜい弱性に関する注意喚起
平成23年4月	Microsoft セキュリティ情報（緊急 9 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 情報流出に伴う ID とパスワードの不正使用に関する注意喚起
平成23年5月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 ISC BIND 9 のぜい弱性を使用したサービス運用妨害攻撃に関する注意喚起
平成23年6月	Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 Microsoft セキュリティ情報（緊急 9 件含む。）に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起
平成23年7月	ISC BIND 9 サービス運用妨害のぜい弱性に関する注意喚起

	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起
平成 23 年 8 月	Microsoft セキュリティ情報（緊急 2 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 Apache HTTP Server のサービス運用妨害のぜい弱性に関する注意喚起
平成 23 年 9 月	Remote Desktop (RDP) が使用する 3389 番ポートへのスキャンに関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起
平成 23 年 10 月	Microsoft セキュリティ情報（緊急 2 件含む。）に関する注意喚起 標的型メール攻撃に関する注意喚起
平成 23 年 11 月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 ISC BIND 9 サービス運用妨害のぜい弱性に関する注意喚起
平成 23 年 12 月	Java SE を対象とした既知のぜい弱性を狙う攻撃に関する注意喚起 Microsoft セキュリティ情報（緊急 3 件含む。）に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起

イ　活動概要（報告状況等の公表）

発行日：2012-01-12 [平成 23 年 10 月 1 日～ 12 月 31 日]
発行日：2011-10-11 [平成 23 年 7 月 1 日 ～ 9 月 30 日]
発行日：2011-07-11 [平成 23 年 4 月 1 日 ～ 6 月 30 日]
発行日：2011-04-12 [平成 23 年 1 月 1 日 ～ 3 月 31 日]

ウ　JPCERT/CC レポート

[発行件数] 50 件
[取り扱ったセキュリティ関連情報数] 286 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等、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(又は偶発的) に発生する全ての事象が対象になる。

注２　ここに挙げた件数は、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　ぜい弱性対策情報について

日本国内の製品開発者(ベンダ) 等の関連組織とのコーディネーションを行い、JVN (Japan Vulnerability Notes) にて公開したぜい弱性情報は 266 件であった(詳細は http://jvn.jp/参照)。
[1/1-3/31:68 件、4/1-6/30:64 件、7/1-9/30:55 件、10/1-12/31:79 件]

そのうち、平成 16 年７月の経済産業省告示「ソフトウェア等ぜい弱性関連情報取扱基準」に従って、JVN にて公開したぜい弱性情報は 114 件であった。
[1/1-3/31:24 件、4/1-6/30:26 件、7/1-9/30:29 件、10/1-12/31:35 件]