不正アクセス行為の発生状況

第１　平成20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20年中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20年中の不正アクセス行為の認知件数は2,289件で、前年と比べ、471件増加した。

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16年	平成17年	平成18年	平成19年	平成20年
認知件数（件）	356	592	946	1,818	2,289
海外からのアクセス	37	53	37	79	214
国内からのアクセス	303	487	855	1,684	1,993
アクセス元不明	16	52	54	55	82

(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（1,589件）、次いで一般企業（685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16年	平成17年	平成18年	平成19年	平成20年
プロバイダ（件）	126	356	602	1,372	1,589
一般企業	202	203	325	437	685
大学、研究機関等	6	12	6	1	5
その他	22	21	13	8	10
うち行政機関	12	17	5	5	6
不明	0	0	0	0	0
計	356	592	946	1,818	2,289

※　「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。

(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（1,567件）、次いで利用権者（注２）からの届出によるもの（656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（60件）、発見者からの通報によるもの（4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16年	平成17年	平成18年	平成19年	平成20年
警察活動（件）	146	33	535	1,326	1,567
利用権者からの届出	172	505	358	415	656
アクセス管理者からの届出	29	30	45	61	60
発見者からの通報	7	14	3	2	4
その他	2	10	5	14	2
計	356	592	946	1,818	2,289

(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、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）が最も多く（1,559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）（457件）、ホームページの改ざん・消去（152件）、情報の不正入手（電子メールの盗み見等）（46件）、インターネットバンキングの不正送金（37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等）（5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19年	平成20年
インターネット・オークションの不正操作（件）	1,347	1,559
オンラインゲームの不正操作	246	457
ホームページの改ざん・消去	25	152
情報の不正入手	55	46
インターネットバンキングの不正送金	113	37
不正ファイルの蔵置	1	5
その他	31	33

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20年中における不正アクセス禁止法違反の検挙件数は1,740件、検挙人員は137人と、前年と比べ、検挙件数は298件増加し、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1,737件、135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、3人であった。

表２－１　検挙事件数等の推移

区分＼年次		平成16年	平成17年	平成18年	平成19年	平成20年
不正アクセス行為	検挙件数	142	271	698	1,438	1,737
	検挙事件数（注５）	65	94	84	86	101
	検挙人員	88	113	130	126	135
不正アクセス助長行為	検挙件数	0	6	5	4	3
	検挙事件数	0	6	3	2	3
	検挙人員	0	6	5	4	3
計	検挙件数（件）	142	277	703	1,442	1,740
	検挙事件数（事件）	65	94 (重複6)	84 (重複3)	86 (重複2)	101 (重複3)
	検挙人員（人）	88	116 (重複3)	130 (重複5)	126 (重複4)	137 (重複1)

※　(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1,736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。

表２－２　不正アクセス行為の態様の推移

区分＼年次		平成16年	平成17年	平成18年	平成19年	平成20年
識別符号窃用型	検挙件数	131	264	698	1,438	1,736
	検挙事件数	62	90	84	86	100
セキュリティ・ホール攻撃型	検挙件数	11	7	0	0	1
	検挙事件数	4	5	0	0	1
計	検挙件数（件）	142	271	698	1,438	1,737
	検挙事件数（事件）	65 (重複1)	94 (重複1)	84	86	101

※　(重複)とは、識別符号窃用型とセキュリティホール攻撃型の重複を示す。

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、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もの（1,368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、知人等によるもの（163件）となっている。

また、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（88件）、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（48件）等、巧妙な手口により識別符号を入手したもの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19年	平成20年
識別符号窃用型（件）		1,438	1,736
	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	139	1,368
	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	39	163
	フィッシングサイトにより入手したもの	1,157	88
	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	55	48
	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	31	26
	他人から購入したもの	7	24
	共犯者等から入手したもの	3	7
	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	2	6
	その他	5	6
セキュリティ・ホール攻撃型		0	1

(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（60人）、次いで交友関係のない他人によるもの（55人）、ネットワーク上のみの知り合いによるもの（22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（48人）が最も多く、20歳代（42人）、30歳代（35人）、40歳代（11人）、50歳代（1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52歳であった。

表３－２　年代別被疑者数の推移

区分＼年次	平成16年	平成17年	平成18年	平成19年	平成20年
10歳代（人）	26	35	40	39	48
20歳代	21	40	44	39	42
30歳代	23	27	28	34	35
40歳代	17	9	15	12	11
50歳代	1	5	2	2	1
60歳代	0	0	1	0	0
計	88	116	130	126	137

※　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（1,498件）が最も多く、次いでオンラインゲームで不正操作を行うため（120件）、嫌がらせや仕返しのため（52件）、好奇心を満たすため（17件）、顧客データの収集等情報を不正に入手するため（12件）、料金の請求を免れるため（3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19年	平成20年
不正に金を得るため（件）	1,186	1,498
オンラインゲームで不正操作を行うため	133	120
嫌がらせや仕返しのため	62	52
好奇心を満たすため	55	17
顧客データの収集等情報を不正に入手するため	0	12
料金の請求を免れるため	2	3
その他	0	35
計	1,438	1,737

(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（1,736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・オークションが最も多く（1,381件）、次いでオンラインゲーム（138件）、ホームページ公開サービス（133件）、電子メール（39件）、会員専用・社員用内部サイト（21件）、インターネットバンキング（14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19年	平成20年
識別符号窃用型（件）		1,438	1,736
	インターネット・オークション	1,178	1,381
	オンラインゲーム	171	138
	ホームページ公開サービス	9	133
	電子メール	22	39
	会員専用・社員用内部サイト	46	21
	インターネットバンキング	4	14
	インターネットショッピング	3	5
	その他	5	5

４　都道府県公安委員会による援助措置

平成20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１件（滋賀）であった。

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16年	平成17年	平成18年	平成19年	平成20年
援助措置（件）	3	4	3	0	1

５　防御上の留意事項

(1)　利用権者の講ずべき措置

ア　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・管理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、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、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とともに、パスワードを他人に教えない、複数のサイトで同じパスワードを使用しない、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。

イ　フィッシングサイトに対する注意

電子メールにより本物のサイトに酷似したフィッシングサイトに誘導し、ＩＤ・パスワードを不正に取得する事案が引き続き発生していることから、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、金融機関等を装った偽のサイトではないかＵＲＬ等を確認する。

ウ　スパイウェア等の不正プログラムに対する注意

電子メールに添付し、若しくはサイト上に蔵置したファイルからスパイウェア等の不正プログラムに感染させ、又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（注９）等の不正プログラムを仕掛け、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よう、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ように注意する。また、スパイウェア対策やコンピュータ・ウイルス対策（最新の対策ソフト、オペレーティングシステムの利用）を適切に講ずる。

(2)　アクセス管理者の講ずべき措置

ア　パスワードの適切な設定

利用権者のパスワードの設定・管理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する仕組みを活用するなどの措置を講ずる。

イ　フィッシング・スパイウェア等への対策

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発生していることから、インターネット・オークション、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10）等により個人認証を強化するなどの対策を講ずる。

ウ　不特定多数の者が利用できるコンピュータの適切な管理

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管理者は、利用者の本人確認の励行、コンピュータへのリカバリーソフト（注11）の導入、利用終了時におけるブラウザ等の履歴の削除、プログラムのインストール制限を行うなどの措置を講ずるとともに、利用者に対してＩＤ・パスワード等を入力する際の危険性について注意喚起する。

6　検挙事例

１	インターネット・オークションサイトに表示されていた他人のＩＤから、そのパスワードを類推して、同サイトに不正アクセスするなどした不正アクセス禁止法違反及び組織的犯罪処罰法違反事件

無職の男（34）らは、平成18年10月から平成19年11月までの間、インターネット・オークションサイト上に表示されている他人のＩＤからそのパスワードを類推して、同サイトに対する不正アクセス行為を行い、商品を売ると偽り落札者から代金をだまし取った。平成20年３月までに、不正アクセス禁止法及び組織的犯罪処罰法違反（組織的な詐欺等）で検挙した（大阪、山形、栃木、静岡、和歌山、広島）。

２	フィッシングにより他人のＩＤ・パスワードを不正入手し、インターネット・オークションサイトに不正アクセスするなどした不正アクセス禁止法違反及び詐欺事件

無職の男（33）らは、平成17年12月から平成19年1月までの間、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、インターネット・オークションサイトに対する不正アクセス行為を行い､商品を売ると偽り落札者から代金をだまし取った。平成20年６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（大分、宮崎、佐賀、鹿児島、広島、福岡、岐阜)。

３	勤務先のインターネットカフェの客用コンピュータにキーロガーを仕掛けて他人のＩＤ・パスワードを不正入手し、インターネットバンキングに不正アクセスするなどした不正アクセス禁止法違反、電子計算機使用詐欺等事件

ネットカフェのアルバイト店員の男(25)は、平成20年１月、客用のコンピュータに仕掛けておいたキーロガーにより、客が入力したインターネットバンキングに係るＩＤ・パスワードを不正に入手し、インターネットバンキングに対する不正アクセス行為を行い、客の口座から自らが管理する電子マネーカードに不正にチャージするなどし、財産上不法の利益を得た。平成20年３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（千葉)。

４	出会い系サイト事業者によるセキュリティホール攻撃を手口とする不正アクセス禁止法違反及び電子計算機損壊等業務妨害事件

出会い系サイト事業者(27)らは、平成19年５月、セキュリティ上の脆弱性を有するプログラムを使用していたホームページに対し、セキュリティホール攻撃による不正アクセス行為を行い、出会い系サイトを宣伝する卑猥な文言等を同ホームページに書き込み、正規のホームページを閲覧不能にした。平成20年２月、不正アクセス禁止法違反及び電子計算機損壊等業務妨害罪で検挙した（滋賀)。

５	自ら作成した不正プログラムにより取得した他人のＩＤ・パスワードを用いた不正アクセス禁止法違反事件

高校生の男（18）は、自ら作成した不正プログラムをファイル共有ソフト（注12）を利用して頒布し、不正プログラムに感染したコンピュータから他人のＩＤ・パスワードを不正に取得し、自ら不正アクセス行為を行うとともに、インターネット・オークションを利用して偽ブランド品を出品販売していた男らに、不正に取得したＩＤ・パスワードを販売し、その不正アクセス行為を幇助した。平成20年９月、不正アクセス禁止法違反で検挙した（群馬)。

（注）

注１　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、特定電子計算機をだれ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。

注２　利用権者

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。

注３　フィッシング

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。

注４　不正アクセス助長行為

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

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　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・オークション用の識別符号を使用して、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。

注７　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、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。

注８　スパイウェア

　コンピュータのハードディスク等に記録された情報、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。

注９　キーロガー

　インストールしたコンピュータにおいて、キーボードの入力情報を記録するプログラムをいう。

注10　ワンタイムパスワード

　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、認証のたびにそれを構成する文字列が変わるもの。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11　リカバリーソフト

　正常に動作しているコンピュータの状態を記録しておき、必要に応じてその状態に戻すソフトをいう。

注12　ファイル共有ソフト

　同種のソフトウェアを利用する不特定多数のコンピュータの中から特定の情報を持つコンピュータを探し出し、特定のサーバコンピュータを経由せずに、不特定多数の者が相互に直接情報を共有するソフトをいう。

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２０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 155 件（平成 19 年：218 件）であった。（注２）

平成 20(2008) 年は同 19(2007) 年と比べて、63 件（約 29%）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、ファイルの書き換え（プログラムの埋め込み含む）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 334 件（昨年：430 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 276 件（昨年：392 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。

17 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。

101 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 52 件である。

【主な内容】

パスワード推測：51 件

ソフトウェアの脆弱性やバグを利用した攻撃：23 件

システムの設定内容を利用した攻撃：1 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 158 件の届出があった。

【主な内容】

資源利用（ファイル、CPU 使用）：42 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：40 件
ファイル等の改ざん、破壊等：39 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：27 件
裏口（バックドア）の作成：2 件
証拠の隠滅（ログの消去など）：2 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。14 件（昨年：7 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、44 件（昨年：31 件）の届出があった。

【主な内容】
正規ユーザへのなりすまし：28 件
メールアドレス(ドメイン)の詐称：9 件
ソーシャルエンジニアリング：2 件
オープンプロキシ：1 件
掲示板荒らし：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。

155 件の届出中、実際に被害に遭った計 120 件（昨年：162 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も多くなっており、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：35 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：16 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：4 件
DoS 攻撃・その他によるもの：26 件
原因不明：39 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 サーバー：26 件

クライアント：25 件

メールサーバー：11 件

ルータ：8 件

ファイアウォール：3 件

その他のサーバー：39 件

不明：4 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

155 件の届出を被害内容で分類した 191 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 156 件（昨年：237 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】

ファイルの書き換え：54 件

サービス低下：10 件

ホームページ改ざん：5 件

サーバーのダウン：1 件

オープンプロキシ：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 20(2008)年は、SSH で使用するポートへの攻撃で侵入された被害（ID、パスワードの設定不備が主な原因）やオンラインサービスで本人になりすまして不正にサービスを利用された被害、ウェブアプリケーションなどの脆弱性を突かれたことによる被害が特に目立っていたと言える。ここ数年の傾向が同様に続いている。しかしながら、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非常に多く見受けられる。改めて原点を見つめ直し、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 3 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://www.ipa.go.jp/security/news/news.html
SQL インジェクション検出ツール「iLogScanner」
http://www.ipa.go.jp/security/vuln/iLogScanner.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

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）に届出があった不正アクセス関連行為の状況について

平成２０年１月１日から１２月３１日の間に JPCERT/CC に届出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および件数

届出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 3,553 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 959 件の報告があった。

[1/1-3/31: 300 件、4/1-6/30: 350 件、7/1-9/30:161 件、10/1-12/31: 148 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 51 件の報告があった。

[1/1-3/31: 10 件、4/1-6/30: 18 件、7/1-9/30: 11 件、10/1-12/31: 12 件]

ウ　電子メールの送信ヘッダを詐称したメールの配送

電子メールの送信ヘッダを詐称した電子メールの配送について 21 件の報告があった。

[1/1-3/31: 0 件、4/1-6/30: 7 件、7/1-9/30:3 件、10/1-12/31: 11 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 19 件の報告があった。

[1/1-3/31:1 件、4/1-6/30:9 件、7/1-9/30:6 件、10/1-12/31:3 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 655 件の報告があった。

[1/1-3/31: 188 件、4/1-6/30: 138 件、7/1-9/30: 150 件、10/1-12/31:179 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 1,848 件の報告があった。
[1/1-3/31:185 件、4/1-6/30:212 件、7/1-9/30:1,162 件、10/1-12/31:289 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]

08 年 1 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
国内ブランドを装ったフィッシングサイトに関する注意喚起
08 年 2 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起
08 年 3 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
SQL インジェクションによる Web サイト改ざんに関する注意喚起
08 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
08 年 5 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
DebianGNU/Linux に含まれる OpenSSL/OpenSSH の脆弱性に関する注意喚起
Adobe Flash Player の未修正の脆弱性に関する注意喚起
08 年 6 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
SNMPv3 を実装した複数製品の認証回避の脆弱性に関する注意喚起
Adobe Acrobat 及び Adobe Reader の脆弱性に関する注意喚起
複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性
08 年 8 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起
08 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
08 年 10 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
Microsoft Server サービスの脆弱性 (MS08-067) に関する注意喚起
TCP 445 番ポートへのスキャン増加に関する注意喚起
Adobe Acrobat 及び Adobe Reader の脆弱性に関する注意喚起
08 年 11 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
08 年 12 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起
Microsoft Internet Explorer の脆弱性 (MS08-078) に関する注意喚起

イ　活動概要（届出状況等の公表）

発行日：2009-01-16 [2008 年 10 月 1 日～ 2008 年 12 月 31 日]

発行日：2008-10-09 [2008 年 7 月 1 日 ～ 2008 年 9 月 30 日]

発行日：2008-07-07 [2008 年 4 月 1 日 ～ 2008 年 6 月 30 日]

発行日：2008-04-07 [2008 年 1 月 1 日 ～ 2008 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] 307 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。）

(4) 脆弱性情報流通

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 168 件であった(詳細は http://jvn.jp/参照。)

[1/1-3/31: 44 件、4/1-6/30: 42 件、7/1-9/30: 43 件、10/1-12/31: 39 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、独立行政法人情報処理推進機構(IPA) に報告され、JVN にて公開した脆弱性情報は 79 件であった。

[1/1-3/31:19 件、4/1-6/30: 13 件、7/1-9/30: 25 件、10/1-12/31: 22 件]

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。