

不正アクセス行為の発生状況

第 1 平成21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21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21年中の不正アクセス行為の認知件数は2,795件で、前年と比べ、506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 17年	平成 18年	平成 19年	平成 20年	平成 21年
認知件数（件）		592	946	1,818	2,289	2,795
	海外からのアクセス	53	37	79	214	40
	国内からのアクセス	487	855	1,684	1,993	2,673
	アクセス元不明	52	54	55	82	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（2,321件）次いで一般企業（466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 17年	平成 18年	平成 19年	平成 20年	平成 21年
プロバイダ（件）		356	602	1,372	1,589	2,321
一般企業		203	325	437	685	466
大学、研究機関等		12	6	1	5	4
その他		21	13	8	10	4
	うち行政機関	17	5	5	6	3
不明		0	0	0	0	0
計		592	946	1,818	2,289	2,795

「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（2,277件）、次いで利用権者（注2）からの届出によるもの（487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（21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 17年	平成 18年	平成 19年	平成 20年	平成 21年
警察活動（件）	33	535	1,326	1,567	2,277
利用権者からの届出	505	358	415	656	487
アクセス管理者からの届出	30	45	61	60	21
発見者からの通報	14	3	2	4	7
その他	10	5	14	2	3
計	592	946	1,818	2,289	2,795

(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（2,152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）（345件）、情報の不正入手（電子メールの盗み見等）（185件）、インターネットバンキングの不正送金（34件）、ホームページの改ざん・消去（33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）（2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20年	平成21年
インターネット・オークションの不正操作（件）	1,559	2,152
オンラインゲームの不正操作	457	345
情報の不正入手	46	185
インターネットバンキングの不正送金	37	34
ホームページの改ざん・消去	152	33
不正ファイルの蔵置	5	2
その他	33	44

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21年中における不正アクセス禁止法違反の検挙件数は2,534件、検挙人員は114人と、前年と比べ、検挙件数は794件増加し、検挙人員は23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2,532件、114人、不正アクセス助長行為（注4）に係るものがそれぞれ2件、1人であった。

表2 - 1 検挙件数等の推移

区分		年次	平成 17年	平成 18年	平成 19年	平成 20年	平成 21年
不正アクセス 行	検挙件数		271	698	1,438	1,737	2,532
	検挙事件数 (注5)		94	84	86	101	95
	検挙人員		113	130	126	135	114
不正アクセス 助長行為	検挙件数		6	5	4	3	2
	検挙事件数		6	3	2	3	1
	検挙人員		6	5	4	3	1
計	検挙件数 (件)		277	703	1,442	1,740	2,534
	検挙事件数 (事件)		94 (重複6)	84 (重複3)	86 (重複2)	101 (重複3)	95 (重複1)
	検挙人員 (人)		116 (重複3)	130 (重複5)	126 (重複4)	137 (重複1)	114 (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2,529件であり、セキュリティ・ホール攻撃型（注7）は3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 17年	平成 18年	平成 19年	平成 20年	平成 21年
識別符号窃用型	検挙件数		264	698	1,438	1,736	2,529
	検挙事件数		90	84	86	100	94
セキュリティ・ ホール攻撃型	検挙件数		7	0	0	1	3
	検挙事件数		5	0	0	1	1
計	検挙件数 (件)		271	698	1,438	1,737	2,532
	検挙事件数 (事件)		94 (重複1)	84	86	101	95

(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、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の(2,084件)が最も多く、次いで、共犯者等から入手したものの(167件)、他人から購入したものの(92件)となっている。

また、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(61件)、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)、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の(8件)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20年	平成21年
識別符号窃用型(件)		1,736	2,529
フィッシングサイトにより入手したものの		88	2,084
共犯者等から入手したものの		7	167
他人から購入したものの		24	92
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		163	61
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	58
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		26	12
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の		48	8
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の		6	0
その他		6	47
セキュリティ・ホール攻撃型		1	3

(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(57人)、次いで交友関係のない他人によるもの(49人)、ネットワーク上のみの知り合いによるもの(8人)となっている。

また、被疑者の年齢についてみると、30歳代(35人)が最も多く、20歳代(33人)、10歳代(31人)、40歳代(13人)、50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59歳であった。

表3 - 2 年代別被疑者数の推移

区分 \ 年次	平成17年	平成18年	平成19年	平成20年	平成21年
10歳代(人)	35	40	39	48	31
20歳代	40	44	39	42	33
30歳代	27	28	34	35	35
40歳代	9	15	12	11	13
50歳代	5	2	2	1	2
60歳代	0	1	0	0	0
計	116	130	126	137	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、不正に金を得るため(2,245件)が最も多く、次いで好奇心を満たすため(165件)、オンラインゲームで不正操作を行うため(63件)、嫌がらせや仕返しのため(34件)、顧客データの収集等情報を不正に入手するため(19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20年	平成21年
不正に金を得るため(件)	1,498	2,245
好奇心を満たすため	17	165
オンラインゲームで不正操作を行うため	120	63
嫌がらせや仕返しのため	52	34
顧客データの収集等情報を不正に入手するため	12	19
料金の請求を免れるため	3	4
その他	35	2
計	1,737	2,532

(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(2,529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見ると、インターネット・オークションが最も多く(2,147件)、次いで電子メール(167件)、オンラインゲーム(88件)、インターネットバンキング(83件)、ホームページ公開サービス(16件)、会員専用・社員用内部サイト(10件)、インターネットショッピング(3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20年	平成21年
識別符号窃用型（件）		1,736	2,529
インターネット・オークション		1,381	2,147
電子メール		39	167
オンラインゲーム		138	88
インターネットバンキング		14	83
ホームページ公開サービス		133	16
会員専用・社員用内部サイト		21	10
インターネットショッピング		5	3
その他		5	15

4 都道府県公安委員会による援助措置

平成21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17年	平成18年	平成19年	平成20年	平成21年
援助措置（件）		4	3	0	1	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 パスワードの適切な管理・設定

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、知人等による不正アクセス行為、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、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を適切に管理する。また、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、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。

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。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。

(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・オークション、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10）等により個人認証を強化するなどの対策を講ずる。

イ 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。

ウ パスワードの適切な設定

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や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。

エ 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等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	関連会社社員のID・パスワードを用いて不正アクセスを行い、顧客情報を取得した上、その情報を書き込んだCD-Rを持ち出した不正アクセス禁止法違反及び窃盗事件
---	---

社内のシステム開発業務を担当していた男(44)は、会社が保有する顧客情報を不正に取得して売却しようとして、平成21年1月、同社の認証サーバーコンピュータに関連会社社員のID・パスワードを用いて不正アクセスを行い、顧客情報を取得した上、その顧客情報を書き込んだCD-Rを持ち出した。平成21年6月、不正アクセス禁止法違反及び窃盗罪で検挙した(警視庁)。

2	他人のID・パスワード等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、電子マネーを購入後、現金に換金してい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
---	--

無職の男(21)は、平成20年12月、出身高専のFTPサーバに侵入し、ファイルに書かれていた被害者のインターネットバンキングのID・パスワード等を入手してインターネットカフェ等から不正アクセスを行い、身元を隠すためいったん電子マネーを購入後、現金に換金した。平成21年4月、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(京都)。

3	メールを盗み見して入手したID・パスワード等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、現金を不正送金してい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
---	--

清掃業の男(35)は、平成21年1月、インターネットサイトに掲示されていたメールアドレス・パスワードを使用してメールを盗み見た後、メールに書かれていたインターネットバンキングのID・パスワード等を使用してインターネットカフェから不正アクセスを行い、拾得した他人の運転免許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21年7月、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(石川)。

4	インターネット・オークションに出品可能な他人のID・パスワードを販売するとともに、自らもオークション詐欺を行っていた不正アクセス禁止法違反及び詐欺事件
---	---

留学生の男(23)は、平成20年1月から3月までの間、共犯者から入手したID・パスワードがインターネット・オークションに出品可能かを確認するためそのID・パスワードを使用して不正アクセスを行い、出品可能なID・パスワードを販売して

いた。また、自らプラズマテレビをインターネット・オークションに架空出品し、詐欺を行った。平成21年3月、不正アクセス禁止法違反及び詐欺罪で検挙した（群馬）。

5

他人のID・パスワードを不正入手し、インターネット・オークションに不正アクセスを行った不正アクセス禁止法違反及び詐欺事件

とび職の男（24）らは、平成20年5月から6月までの間、インターネット上で購入した他人名義のID・パスワードを使用して、インターネットカフェからインターネット・オークションに不正アクセスを行い、商品を売ると偽り落札者から代金をだまし取った。平成21年10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（静岡）。

（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 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

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。

注9 キーロガー

キーボードでどの文字が入力されたか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。

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 21 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 149 件（平成 20 年：155 件）であった。（注 2）

平成 21（2009）年は同 20（2008）年と比べて、6 件（約 4%）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」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 254 件（平成 20 年：334 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 211 件（平成 20 年：276 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。

20 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。

110 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 37 件である。

【主な内容】

パスワード推測：42 件

ソフトウェアの脆弱性やバグを利用した攻撃：18 件

システムの設定内容を利用した攻撃：2 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 81 件の届出があった。

【主な内容】

- ファイル等の改ざん、破壊等：32 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：19 件
- 資源利用（ファイル、CPU 使用）：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：5 件
- 証拠の隠滅（ログの消去など）：2 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もしくは低下させたりする攻撃である。6 件（平成 20 年：14 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、37 件（平成 20 年：44 件）の届出があった。

【主な内容】

- 正規ユーザへのなりすまし：31 件
- メール不正中継：2 件
- メールアドレス（ドメイン）の詐称：2 件
- ソーシャルエンジニアリング：1 件
- オープンプロキシ：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。

149 件の届出中、実際に被害に遭った計 96 件（平成 20 年：120 件）を分類すると以下のようなになる。

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】

- 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
- ID、パスワード管理の不備によると思われるもの：11 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：6 件
- DoS 攻撃・その他によるもの：9 件
- 原因不明：54 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：62 件
クライアント：23 件
メールサーバ：20 件
ルータ：4 件
ファイアウォール：2 件
その他のサーバ：12 件
不明：2 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

149 件の届出を被害内容で分類した 160 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 107 件(平成 20 年：156 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】

オンラインサービスの不正利用：32 件
ファイルの書き換え：30 件
ホームページ改ざん：14 件
踏み台として悪用：7 件
データの窃取や盗み見：7 件
サービス低下：5 件
メール不正中継：2 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 21 年は、ID/パスワード不備や脆弱性が原因でサイトに侵入されて他サイト攻撃のための踏み台にされたりウェブページを改ざんされたりしたケースや、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が特に目立っていたと言える。特に「なりすまし」被害については、原因が不明なケースがほとんどであった。「なりすまし」被害以外では、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>

「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

【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.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/>

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 21 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 7,435 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 1,146 件の報告があった。

[1/1-3/31: 171 件、4/1-6/30: 278 件、7/1-9/30:469 件、10/1-12/31: 228 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 500 件の報告があった。

[1/1-3/31: 26 件、4/1-6/30: 74 件、7/1-9/30:28 件、10/1-12/31: 372 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 2 件の報告があった。

[1/1-3/31: 2 件、4/1-6/30: 0 件、7/1-9/30:0 件、10/1-12/31: 0 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 20 件の報告があった。

[1/1-3/31:3 件、4/1-6/30:6 件、7/1-9/30:4 件、10/1-12/31:7 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盗み取る Web 偽装事案について 1,021 件の報告があった。

[1/1-3/31: 182 件、4/1-6/30: 200 件、7/1-9/30: 303 件、10/1-12/31:336 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 4,746 件の報告があった。

[1/1-3/31:300 件、4/1-6/30:823 件、7/1-9/30:2,337 件、10/1-12/31:1,286 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.jpccert.or.jp/>参照。)

ア 注意喚起

[新規]

- 2009 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
- 2009 年 2 月 Microsoft セキュリティ情報 (緊急 2 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
- 2009 年 3 月 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
- 2009 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
- 2009 年 5 月 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
JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起
- 2009 年 6 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起
- 2009 年 7 月 韓国、米国で発生している DDoS 攻撃に関する注意喚起
Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
Microsoft ATL を使用した複数製品の脆弱性に関する注意喚起
Adobe Flash Player 及び Adobe Acrobat/Reader の脆弱性に関する注意喚起
ISC BIND 9 の脆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
- 2009 年 8 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起
- 2009 年 9 月 Microsoft セキュリティ情報 (緊急 5 件) に関する注意喚起
複数製品の TCP プロトコルの脆弱性に関する注意喚起
- 2009 年 10 月 Microsoft セキュリティ情報 (緊急 8 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
マイクロソフト社を騙るマルウェア添付メールに関する注意喚起
Web サイト経由でのマルウェア感染拡大に関する注意喚起
- 2009 年 11 月 Microsoft セキュリティ情報 (緊急 3 件) に関する注意喚起
- 2009 年 12 月 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 の脆弱性に関する注意喚起

Adobe Reader 及び Acrobat の未修正の脆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：2010-01-12 [2009年10月1日～2009年12月31日]

発行日：2009-10-08 [2009年7月1日～2009年9月30日]

発行日：2009-07-09 [2009年4月1日～2009年6月30日]

発行日：2009-04-07 [2009年1月1日～2009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] 264 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 143 件であった(詳細は <http://jvn.jp/> 参照。)

[1/1-3/31:31 件、4/1-6/30: 45 件、7/1-9/30: 36 件、10/1-12/31: 31 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 79 件であった。

[1/1-3/31:16 件、4/1-6/30: 30 件、7/1-9/30: 17 件、10/1-12/31: 16 件]