

## 不正アクセス行為の発生状況

### 第1 平成14年中の不正アクセス禁止法違反事件の検挙状況等について

平成14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。

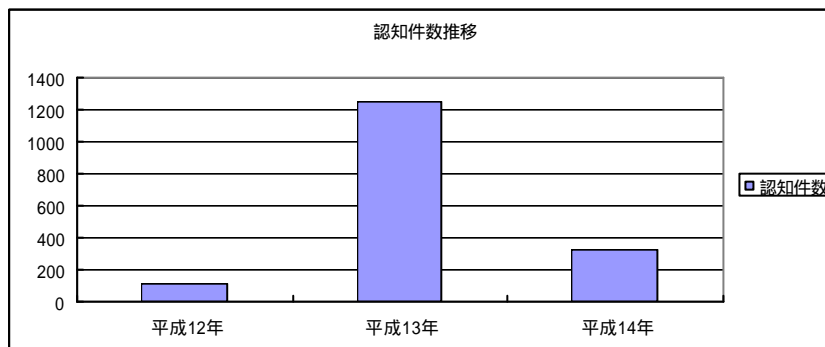
なお、本文中平成12年の数字は、不正アクセス禁止法の施行日である平成12年2月13日から平成12年12月31日までの間のものである。

#### 1 不正アクセス行為の発生状況及びその特徴

##### (1) 認知件数（注1）（注2）

平成14年中の不正アクセス行為の認知件数は329件で、前年と比べ、924件減の大幅減少となった。

減少の原因は、前年に多発したホームページ書き換えプログラムによるホームページ書き換え事案等（935件）のセキュリティ・ホール攻撃型（注3）事案が平成14年は激減したためであり、官民挙げた広報活動や、修正プログラムの普及によりセキュリティ・ホールの解消が進んだことがうかがえる。



	平成12年	平成13年	平成14年
認知件数	106	1,253	329
海外からのアクセス	25	448	13
国内からのアクセス	73	258	286
アクセス元不明	8	547	30

##### (2) 被害に係る特定電子計算機のアクセス管理者（注4）

被害に係る特定電子計算機のアクセス管理者別に見ると、プロバイダが243件と最も多く、次いで一般企業の62件となっている。

被害に係る特定電子計算機のアクセス管理者	平成12年	平成13年	平成14年
プロバイダ	59	182	243
一般企業	25	429	62
大学、研究機関等	8	101	3
その他	14	139	21
うち行政機関	-	-	12
不明	0	402	0
計	106	1,253	329

「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事業者をいう。  
「大学、研究機関等」には、大学、高等学校等の学校機関及びその附置機関を含む。  
「その他」の「うち行政機関」には、国の行政機関、独立行政法人、特殊法人、地方公共団体及びこれらの付属機関を含む。  
なお、平成12年及び平成13年は「その他」の内訳の集計をしていない。

### (3) 認知の端緒

認知の端緒としては、警察職員によるいわゆるサイバーパトロールや被疑者の取調べ等の警察活動が185件と最も多く、次いで利用権者（注5）からの届出が92件、アクセス管理者からの届出が47件の順となっている。

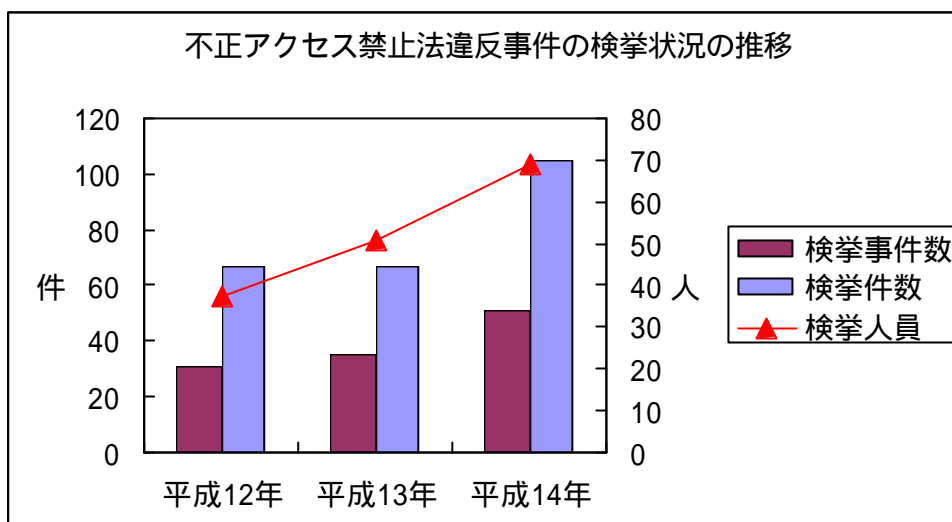
### (4) 不正アクセス行為後の行為

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入札、販売代金の取得等）が177件と最も多く、次いでホームページの改ざんが38件、インターネットの利用が18件、電子メールの盗み見が17件、パスワード変更が13件、バックドア（注6）・ツールを仕掛けたものが10件の順となっている。

## 2 不正アクセス禁止法違反事件の検挙状況

検挙状況は、検挙事件数（注7）、検挙件数及び検挙人員ともに増加している。

検挙事件の多くは識別符号窃用型（注8）であり、インターネット・オークションや電子メール等のサービスを対象とする事犯が目立ったほか、インターネット・バンキング等の金融サービスを対象とした事犯もみられた。これらの多くは、他人により推知されやすいパスワードが設定されていた。このほか、高度な技術を用いてサーバのセキュリティの脆弱性を突くセキュリティ・ホール攻撃型もみられた。



		平成12年	平成13年	平成14年
不正アクセス行為	検挙事件数	30	35	51
	検挙件数	62	66	102
	検挙人員	34	51	68
不正アクセス助長行為	検挙事件数	4	1	2
	検挙件数	5	1	3
	検挙人員	5	1	3
計	検挙事件数	31 (重複3)	35 (重複1)	51 (重複2)
	検挙件数	67	67	105
	検挙人員	37 (重複2)	51 (重複1)	69 (重複2)

### 3 不正アクセス行為の検挙事例

1	プロバイダの認証サーバに対するバッファ・オーバーフロー攻撃(注9)に係る不正アクセス禁止法違反事件
---	---

外国人留学生の男(24)が、自己の技量を試す目的で、プロバイダの認証サーバに対して、当該サーバのセキュリティ・ホールにバッファ・オーバーフロー攻撃を仕掛けて不正アクセスし、ハッキング・ツールの蔵置を行った。また、当該サーバを踏み台として、別のプロバイダの複数のサーバに対しても不正アクセスし、ホームページを改ざんした。14年1月、不正アクセス禁止法違反で検挙した(警視庁、滋賀)。

<b>2</b>	<b>インターネット・オークションの識別符号を窃用した不正アクセス禁止法違反及び詐欺事件</b>
----------	--

大学生の男(20)が、インターネット・オークションを利用して金を騙し取る目的で、他人のインターネット・オークション用ID及びパスワードを使用してオークションサービスのサーバに不正アクセスし、架空の出品を行い、落札者44人から総額約240万円を、インターネットを利用して購入した他人名義の銀行口座に振り込ませて騙し取った。14年1月、不正アクセス禁止法違反及び詐欺で検挙した(茨城、栃木)。

<b>3</b>	<b>他人の電話回線を利用した不正アクセス禁止法及び有線電気通信法違反事件</b>
----------	---

無職の男(36)が、通信料金及びインターネット接続料金の課金を免れる目的で、他人の電話回線に自己の電話回線を接続した上、別の他人のインターネット接続用ID及びパスワードを使用してプロバイダの認証サーバに不正アクセスし、インターネットを利用した。14年4月、不正アクセス禁止法違反で検挙し、5月、同人を有線電気通信法違反で追送致した(岐阜、福島)。

<b>4</b>	<b>リマインダ機能を利用して入手したパスワードを使用して他人の電子メールを盗み見した不正アクセス禁止法違反事件</b>
----------	--

男子中学生(14)が、好奇心から、同級生である女子中学生の無料電子メール・サービス用のパスワードをリマインダ機能(注10)を利用して不正に入手した上、ID及び当該パスワードを使用してメール・サーバに不正アクセスし、電子メールを盗み見た。14年4月、不正アクセス禁止法違反で検挙した(徳島)。

<b>5</b>	<b>無料電子メールサービスの識別符号を窃用した不正アクセス禁止法及び電気通信事業法違反事件</b>
----------	--

会社員の男(32)が、嫌がらせの目的で、出会い系サイトで知り合った女性の電子メールアドレスのIDからパスワードを推測して電子メールサービス事業者のメールサーバに不正アクセスし、電子メールの内容を盗み見たほか、当該アドレスを使用して卑わいな内容の電子メールを送るなどした。14年5月、不正アクセス禁止法違反及び電気通信事業法違反で検挙した(香川)。

<b>6</b>	<b>特殊法人の研究開発用サーバに係る不正アクセス禁止法違反事件</b>
----------	--------------------------------------

会社員の男（28）が、他社の技術情報を盗み見る目的で、自社及び他社のデータが管理されている特殊法人の研究開発用サーバに他社の社員のID及びパスワードを使用して不正アクセスし、当該他社が開発していた部品に係る機密情報を入手した上、当該他社の社員のID及びパスワードを特定する方法を自社の社員に電子メールで通知した。また、当該電子メールを見た別の社員（40）ら2人が、別の他社社員のID及びパスワードを使用して当該研究開発用サーバに不正アクセスした。14年5月、不正アクセス禁止法違反で会社員3人を検挙した（警視庁）。

<b>7</b>	<b>インターネット・バンキング利用の不正送金事件に係る不正アクセス禁止法違反、私電磁的記録不正作出・同供用及び電子計算機使用詐欺事件</b>
----------	---

会社員の男（31）が、他人の口座から金を不正に得る目的で、銀行のインターネット・バンキング用の認証サーバに、当該銀行の顧客サポート・サービスに従事していた当時に知り得た口座開設者の口座番号、暗証番号等の識別符号を使用して不正アクセスし、当該口座をインターネット・バンキングが利用できる状態に変更した上、送金に必要な識別符号を使用して当該サーバに不正アクセスし、自己が開設した他人名義の銀行口座に不正に送金した。14年5月、不正アクセス禁止法違反、私電磁的記録不正作出・同供用及び電子計算機使用詐欺で検挙した（警視庁）。

<b>8</b>	<b>オンライン・トレード利用の株式取引に係る不正アクセス禁止法違反及び私電磁的記録不正作出・同供用事件</b>
----------	--

会社員の男（32）が、社内で自己に対する評価が低いことに不満を抱き、会社を困らせる目的で、自己が開発に携わった派遣先証券会社のオンライン・トレード用の認証サーバに、当該システムの開発時に盗み見た当該証券会社の口座開設者のID及びパスワードを使用して不正アクセスし、当該口座開設者になりすまして株式売買を行った。14年6月、不正アクセス禁止法違反及び私電磁的記録不正作出・同供用で検挙した（警視庁）。

<b>9</b>	<b>インターネット接続料金を免れる目的の不正アクセス禁止法違反事件</b>
----------	--

会社員の男（34）が、インターネット接続料金の課金を免れる目的で、勤務当時知り得た会社の顧客のインターネット接続用ID及びパスワードを使用してプロバイダの認証サーバに不正アクセスし、インターネットを利用した。14年10月、不正アクセス禁止

法違反で検挙した（愛知）。

#### 4 検挙事件の特徴

##### (1) 犯行の手口

識別符号窃用型の不正アクセス行為で検挙した46事件（83件）における当該識別符号（ID及びパスワード）の入手方法は、利用権者のパスワードの設定・管理の甘さにつけ込み入手するものが最も多く23事件（34件）であった。その内訳は、パスワードがIDから容易に推知できるもの（例えば、IDが「keisatsu1234」に対して、パスワードを「keisatsu」や「1234」としているもの。）や単純な文字列であったもの（例えば、パスワードを「aaaa」としているもの。）が17事件（28件）、リマインダ機能における質問への安易な回答が設定されていたものが6事件（6件）である。

また、元システム管理者など、立場上、識別符号を知りうる者によるものが17事件（33件）、識別符号が記された電子メールや封書の誤配によるものが2事件（2件）みられた。

一方で、サーバのセキュリティ・ホールにバッファ・オーバーフロー攻撃を仕掛けた事案のように、高度なコンピュータ技術及び電気通信技術を用いてセキュリティの脆弱性を突くセキュリティ・ホール攻撃型も引き続きみられた。

##### (2) 被疑者

元社員や元交際相手等利用権者の顔見知りの者による犯行は33事件（56件）であり、全くの他人による犯行は19事件（49件）であった。（1事件は、利用権者と顔見知りの者及び他人の複数の被疑者がいる。）

また、検挙した被疑者の年齢は、20代が30人と最も多く、次いで30代が26人、40代が7人、10代が6人の順となっている。最年少の者は14歳であり、最年長の者は47歳であった。

##### (3) 犯行の動機

不正アクセス行為の動機としては、元勤務先や元交際相手等に対する嫌がらせや仕返し19事件（29件）と最も多く、次いで好奇心や自己の技量を計るために試みるものが13事件（32件）、利用料金の請求を免れるための5事件（14件）、メールを盗み見るための3事件（6件）、不正に金を得るための2事件（6件）の順となっている。（重複計上あり。）

##### (4) 利用されたサービス

識別符号窃用型の不正アクセス行為で検挙した46事件（83件）において、当該識別符号を入力することにより利用できるサービス別に見ると、無料電子メールなどの電子メール・サービスが11事件（19件）と最も多く、次いでインターネット・オークション・サービスが10事件（13件）、インターネットへの接続サービス（ダイヤルアップ・サービス）が6事件（15件）、無料ホームページ作成サービスが6事件（9件）、金融サービス（インターネット・バンキング等）が3事件（8件）の順となっている。

(5) その他

不正アクセス禁止違法違反のほか、他の罪についても検挙した事件は、17事件であった。

	事 件 数
電子計算機損壊等業務妨害	2
電気通信事業法違反	3
詐欺	2
電子計算機使用詐欺	1
私電磁的記録不正作出・同供用	7
恐喝未遂	1
有線電気通信法違反	1
組織的な犯罪の処罰及び犯罪収益の規制等に関する法律違反	1
偽計業務妨害	2
医師法違反	1
有印私文書偽造・同行使	1

重複計上あり。

## 5 都道府県公安委員会による援助措置

都道府県公安委員会は、不正アクセス行為を受けたアクセス管理者からの申出への対応として、不正アクセス禁止法第6条の援助規定に基づくアクセス管理者に対する助言・指導を5件（北海道1、愛知2、大阪1、島根1）実施した。

## 6 防御上の留意事項

### (1) サーバの適切な管理

セキュリティ・ホール攻撃型の不正アクセス行為の発生件数は大幅に減少したが、この種手口による事犯は、一旦発生すれば被害が大きくなる危険があることから、引き続きセキュリティ水準の維持・向上が必要であり、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、使用しているオペレーティング・システム又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などセキュリティ・ホールを解消するための措置を講じる必要がある。

### (2) 識別符号の適切な設定・管理

識別符号窃用型の不正アクセス行為で検挙した46事件（83件）中、23事件（34件）が利用権者のパスワードの設定・管理の甘さにつけ込んで入手するものであったことから、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こと、リマインダ機能に関しては、アクセス管理者及び利用権者において、パスワード再発行時に必要となる情報（質問に対する回答）を、他人による推知が困難となるような仕組み及び内容とすることが必要である。

そのほか、利用権者等においては、パスワードを定期的に変更するなど識別符号を適切に設定・管理する必要がある。

一方で、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。

(注1) 認知

ここで認知とは、被害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としている。

(注2) 件数

件数とは、被疑者が行った犯罪構成要件に該当する行為の数をいう。

なお、不正アクセス行為の件数の計上については、ひとつのアクセス制御機能に対するひとつの手口による侵害行為が1回あったことをもって1件としている。ただし、被疑者が異なる場合(共犯を除く。)はそれぞれ1件として計上し、短期間にひとつのアクセス制御機能に対して同一手口による侵害が連続的に行われ、実質上1回の行為とみなしうる場合は包括して1件としている。

(注3) 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、バッファ・オーバーフロー攻撃による不正アクセス行為が該当する。

(注4) アクセス管理者

アクセス管理者とは、ネットワークに接続しているコンピュータ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店主がそれぞれアクセス管理者である。

(注5) 利用権者

利用権者とは、ネットワークに接続されたコンピュータ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6) バックドア

バックドアとは、部外からネットワークを通じて不正にサーバに侵入するための裏口のことであり、クラッカー等は、一度侵入に成功したサーバにバックドアを設置することにより、当該バックドアを通じて次回以降の侵入を容易に行うことが可能となる。バックドアの設置方法は巧妙化してきており、当該サーバのアクセス管理者が存在に気付かない場合があるほか、削除しても再起動後に自動的にバックドアが設置されるツールが当該サーバに組み込まれている場合もある。バックドアが設置されたサーバから確実に当該バックドアを駆除するためには、オペレーティングシステムの再インストール及び修正プログラムのインストールを行うことが望ましい。

(注7) 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には1事件と数える。

(注8) 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ID及びパスワードを使用して、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9) バッファ・オーバーフロー攻撃

コンピュータに対して、通常処理できる容量を超えるデータを送信することにより、当該コンピュータへのプログラムの追加、改ざんを行うことをいう。

(注10) リマインダ機能

利用権者がパスワードを忘れてしまった時に、アクセス管理者が何らかの方法で本人確認を行った上でパスワードを再発行する機能である。本人確認の方法としては、サービス利用のための登録時に、本人が決めた情報を登録しておき、パスワードの再発行時にその情報を利用権者に入力させるもの(例えば、「出身小学校は?」等の質問に対して、あらかじめ登録しておいた情報を答えとして入力すると、パスワードが再発行される)などがある。

## 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 情報処理振興事業協会(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14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被害届出件数は619件(昨年:550件)であった(注2)。平成14年は、ワーム感染及びワーム形跡(未感染)に関する届出が大幅に減少した一方、侵

入やアクセス形跡、DoS（サービス妨害）の届出が増加し、ワーム感染以外の実被害届出件数が219件（昨年：197件）と増加した。

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分類に該当するものがあるため、それぞれの項目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。重複があるため、届出件数とは異なり総計は790件（昨年：333件）となる。なお、この件数には、ワームに関する届出は含まれていない。

##### ア 侵入行為に関して

侵入行為に係わる攻撃等の届出は671件（昨年：193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。94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。そのなかで実際に侵入の被害を受けたのは4件であった。

##### (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。135件の届出があり、これらのうち実際に侵入を受けたものは106件である。

パスワード推測：4件

ソフトウェアのバグを利用した攻撃：47件

システムの設定内容を利用した攻撃：33件

##### (ウ) 不正行為の実行及び目的達成後の行為

実際に侵入を受けた106件について、その後行われた種々の行為である。1件の侵入で種々の行為が行われているため重複がある。

ファイル等の改ざん、破壊等：65件

プログラムの作成（インストール）、システムファイルの改ざん、トロイの木馬などの埋め込み等：42件

資源利用（ファイル、CPU使用）：20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：24件

裏口の作成：5件

証拠の隠滅：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る攻撃である。22件（昨年：11件）の届出があった。

過負荷を与える攻撃：15件

例外処理を利用した攻撃：3件

SPAMメール：4件

##### ウ その他

その他には、ソーシャルエンジニアリングや、サービスの外部からの利用が含まれ、97件（昨年：94件）の届出があった。

メール中継に関するもの：18件

そのうちメール中継に実際に利用されたもの：16件

メールアドレス(ドメイン)の詐称：48件

その他：31件

## (2) ワーム別の分類

ワームの種類による分類である。ワームに関する届出は、実際にワームに感染した届出6件、ワームには感染しなかった届出34件、合計40件であった。主なワームの届出件数は以下の通りである。

Nimda：16件（うち感染：0件）

CodeRed：12件（うち感染：2件）

Spida：9件（うち感染：0件）

その他（Slapperなど）：21件（うち感染：4件）

## (3) 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。

実際に侵入を受けた106件（昨年：97件）、ワームに感染した6件（昨年184件）、メール中継に係わる問題（弱点）のあった16件（昨年：25件）などの計151件（昨年：307件）を分類すると以下ようになる。

ID、パスワード管理の不備によると思われるもの：3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：48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：33件

不明：67件

## (4) 電算機分類

攻撃や被害の対象となった機器による分類である。

WWWサーバ：86件

メールサーバ：29件

DNSサーバ：5件

FTPサーバ：10件

ファイアウォール：7件

ルータ：3件

Proxyサーバ：2件

その他のサーバ・不明：68件

クライアント：410件

## (5) 被害内容分類

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届出件数は225件（昨年

: 375件)である。

WWW書き換えの被害は26件(昨年:177件)と減少したが、ファイルの書き換え(プログラム埋め込み、ファイル削除含む)77件(昨年39件)、不正アカウント作成12件(昨年:4件)、パスワードファイルの盗用7件(昨年:4件)と被害内容が深刻になってきている。

なお、対処に係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。

メール中継に利用された:16件

サーバダウン:4件

不正アカウント作成:12件

WWW書き換え:26件

パスワードファイル盗用:7件

サービス低下:15件

オープンプロキシ:1件

ファイルの書き換え:77件

その他:110件

#### (6) 対策情報

(2)の被害原因分類にもあるように、基本的な(既知の)対策をとっていなかったために被害にあってしまったものが増えている。下記ページなどを参照し、今一度状況確認・対処されたい。

「セキュリティ対策セルフチェックシート」

<http://www.ipa.go.jp/security/ciadr/checksheet.html>

「コンピュータ不正アクセス被害防止対策集」

<http://www.ipa.go.jp/security/ciadr/cm01.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/index.html>

#### (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が受理した件数であり、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 コンピュータ緊急対応センター（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14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）に係わる報告件数は1,435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1,160件の報告があった。  
[1/1-3/31: 289件、4/1-6/30: 199件、7/1-9/30: 304件、10/1-12/31: 368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57件の報告があった。  
[1/1-3/31: 24件、4/1-6/30: 14件、7/1-9/30: 9件、10/1-12/31: 10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39件の報告があった。  
[1/1-3/31: 15件、4/1-6/30: 4件、7/1-9/30: 12件、10/1-12/31: 8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: 6件、4/1-6/30: 4件、7/1-9/30: 4件、10/1-12/31: 6件]

#### オ その他

コンピュータウィルス、SPAMメールの受信、電子メール配送プログラムへの電子メールの中継を目的としたアクセス等について176件の報告があった。  
[1/1-3/31: 31件、4/1-6/30: 51件、7/1-9/30: 44件、10/1-12/31: 50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 ]

DNS resolver の脆弱性に関する注意喚起  
OpenSSH サーバプログラムの脆弱性に関する注意喚起  
Apache Web サーバプログラムの脆弱性に関する注意喚起  
TCP 1433番ポートへのスキャンの増加に関する注意喚起  
SNMPv1 の実装に含まれる脆弱性に関する注意喚起

## イ 緊急報告

[ 新規 ]

OpenSSL の脆弱性を使って伝播する Apache/mod\_ssl ワーム

[ 更新 ]

OpenSSL の脆弱性を使って伝播する Apache/mod\_ssl ワーム (更新)

## ウ 技術メモ

[ 更新 ]

コンピュータセキュリティインシデントへの対応 (Version 4)  
関係サイトとの情報交換 (Version 4)

## エ 活動概要 (届出状況等の公表)

発行日: 2003-01-17 [ 2002年10月1日 ~ 2002年12月31日 ]  
発行日: 2002-10-18 [ 2002年7月1日 ~ 2002年9月30日 ]  
発行日: 2002-07-19 [ 2002年4月1日 ~ 2002年6月30日 ]  
発行日: 2002-04-23 [ 2002年1月1日 ~ 2002年3月31日 ]

## オ 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 ] 217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

の攻撃の発生件数や、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。