不正アクセス事犯の取締りについて

警察庁生活安全局生活環境課
生活経済対策室
課長補佐心得
金 澤　正 和

1 不正アクセス禁止法の概要（別添1参照）

(1) 目的

電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与すること（第1条）

(2) 内容

ア. 不正アクセス行為の禁止、処罰（第3条、第8条第1号）

不正アクセス禁止法においては、アクセス制御機能に対する侵害行為の規制という観点から、ID・パスワードなどの識別符号を入力しなければ利用できないアクセス制御機能が施されたネットワーク・システム（特定電子計算機という。）に対し、正規の他人の識別符号を無断で入力し、又はアクセス制御機能による特定利用の制限を免れる情報等を入力し、利用可能な状態にするような行為を不正アクセス行為として禁止している（法第3条。なお、一般に不正アクセスと言われることの多い、いわゆるスパム・メール中継、ポートスキャン、DOS攻撃、コンピュータ・ウィルスの投与等の行為は、アクセス制御機能への侵害行為とはならないことから、不正アクセス禁止法の規制の対象から除外されている。

イ. 不正アクセス行為を助長する行為の禁止、処罰（第4条、第9条）

他人の識別符号をその識別符号がどの特定電子計算機の特定利用に係るもの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、無断で第三者に提供する行為を不正アクセス助長行為として禁止している（法第4条）。

ウ. アクセス管理者による防御措置（第5条）

アクセス管理者（特定電子計算機の利用につき当該特定電子計算機の動作を管理する者をいう。通常、法人たるプロバイダや企業が該当し、その職員たるいわゆるシステム管理者はこれには当たらない。）は、特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとされている。

エ. 都道府県公安委員会による援助（第6条）

都道府県公安委員会は、特定電子計算機に係るアクセス管理者からの申出に応じ、特定電子計算機を不正アクセス行為から防御するため必要な応急の措置が講じられるよう、必要な援助等を行うものとされている。

オ. 国による援助（第7条）

国家公安委員会、経済産業大臣及び総務大臣は、毎年少なくとも1回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとされている。

2 不正アクセス事犯の取締り状況(別添2参照)

(1) 平成12年中の不正アクセス行為の発生状況　106件

		認知件数
被害に係る特定電子計算機のアクセス管理者別	プロバイダ	59
	大 学	8
	情報通信企業	6
	そ の 他	33
	計	106

		認知件数
認 知 の 端 緒 別	アクセス管理者からの届出	30
	利用権者からの届出	23
	発見者からの通報	7
	被疑者の取調べ	35
	そ の 他	11
	計	106

○ ホームページ改ざん、消去を伴う事案が多い(33件)

○ アクセス管理者等から警察に届出があったもの(53件)

(2) 平成12年中の不正アクセス事犯の検挙状況

事 犯 別	検挙事件数	検挙件数	検挙人員
不正アクセス行為	30	62	34人
不正アクセス助長行為	4	5	5人
計	31 (重複3)	67	37人 (重複2人)

○ パスワード管理の甘さにつけ込んだ事案が多い(12件)

○ 識別符号の入手等にクラッキング・ツールを利用した事案が多い(8事件、14件)

3 警察における対応((1)(2):別添2、(3):別添3参照)

(1) 平成12年中の都道府県公安委員会による援助措置　6件

(2) 平成12年中の発生・検挙を踏まえた防御上の留意事項の公表

○ トロイの木馬対策

○ ID・パスワード等識別符号の適切な管理

○ セキュリティ・ホールの解消等サーバの適切な管理

(3) 連続発生事案等への対応

○ 迅速な捜査等の実施

○ 被害の拡大防止及び再被害の防止に配意した措置の実施

○ 被害拡大の防止に資する防御措置等の情報提供

別添1

不正アクセス行為の禁止等に関する法律の概要

1　法の目的、基本構成（第1条関係）

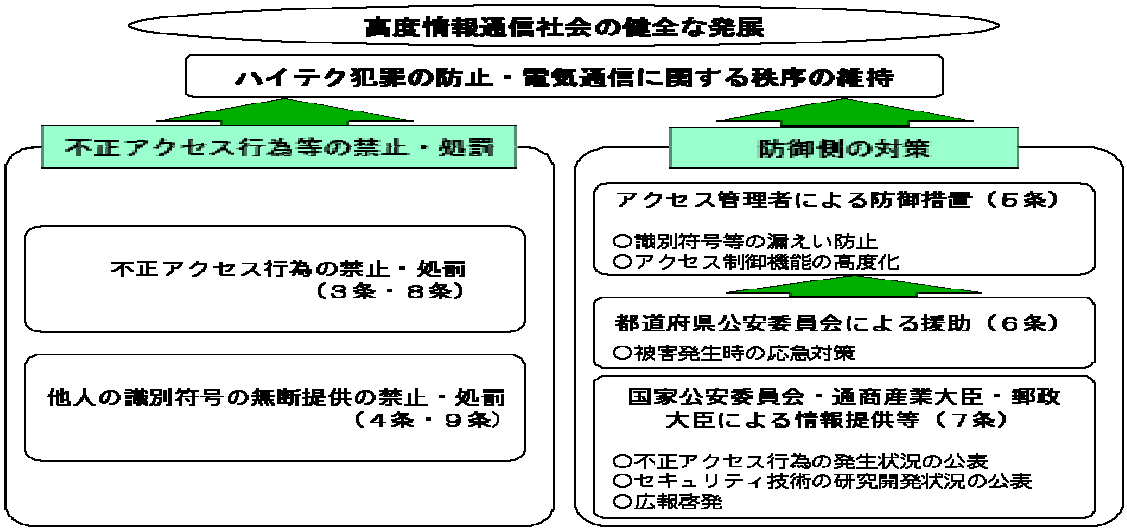
(1)法の目的

不正アクセス行為の禁止等に関する法律（以下「本法」といいます。）は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のため不正アクセス行為を受けたアクセス管理者に対する都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪（注）の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的としています。

（注）「電気通信回線を通じて行われる電子計算機に係る犯罪」とは、電子計算機使用詐欺、電子計算機損壊等業務妨害などコンピュータ・ネットワークを通じて、これに接続されたコンピュータを対象として行われる犯罪と、コンピュータ・ネットワークを通じて、これに接続されたコンピュータを利用して行われる詐欺、わいせつ物頒布、銃器・薬物の違法取引などの犯罪の両方を指しています。

(2)法の基本構成

本法は、不正アクセス行為等の禁止・処罰という行為者に対する規制と、不正アクセス行為を受ける立場にあるアクセス管理者に防御措置を求め、アクセス管理者がその防御措置を的確に講じられるよう行政が援助するという防御側の対策という2つの側面から、不正アクセス行為の防止を図ろうとするものです。



2　定義

(1)アクセス管理者（第2条第1項関係）

アクセス管理者とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」といいます。）の利用（電気通信回線を通じて行うものに限ります。以下「特定利用」といいます。）について特定電子計算機の動作を管理する者です。「管理」の主たる内容は、特定電子計算機をコンピュータ・ネットワーク経由で他人に利用させるか否か、利用させる場合にはどの範囲の利用をさせるかということを決定することで、これらのことを決定する権限を有している者がアクセス管理者ということになります。アクセス管理者は個人、法人の別を問いません。

ここで注意を要するのは、法人がコンピュータを運用している場合です。企業・学校等の法人の場合には、その職員の中からシステム管理者（一般に、「管理者」、「ルート」、「スーパーユーザ」などと呼ばれています。）を任命して「管理」の業務を行わせていますが、それらのシステム管理者は自分を任命した法人の意思に基づいて「管理」の業務を行っている者です。本法でいうアクセス管理者は、これらのシステム管理者ではなく、あくまで当該法人自体ということになります。

また、アクセス管理者は、コンピュータの動作を「管理」していればよく、そのコンピュータを所有しているかどうかは無関係です。ですから、例えば、サーバ・コンピュータを所有していないインターネットのエンドユーザであっても、インターネット・サービス・プロバイダのサーバの一部を利用してホームページを開設し、そのホームページの閲覧を誰に認めるかということなどを「管理」する権限を有していれば、アクセス管理者となります（ただし、この場合、インターネット・サービス・プロバイダのサーバ上に存在するホームページの閲覧という特定利用に限ってのアクセス管理者であることに注意する必要があります。）。1つのコンピュータに対して2以上のアクセス管理者（例えば、そのコンピュータ全体のアクセス管理者と、そのコンピュータの一部を利用して開設されているホームページの閲覧についてのアクセス管理者など）が存在することもあり得ます。

なお、特定電子計算機という概念には、インターネット等のオープンネットワークに接続されているコンピュータ・ネットワーク上のコンピュータのほか、一部の企業内LANのように外部から独立したネットワークを構築しているコンピュータも含まれます。したがって、アクセス管理者には、インターネットに接続されておらず外部から独立している企業内LANを有している企業なども含まれることになります。

（2）識別符号（第2条第2項関係）

識別符号とは、特定電子計算機の特定利用をすることについてアクセス管理者の許諾を得た者（簡単にいえば、当該コンピュータのアカウントを、そのコンピュータのアクセス管理者から付与されている利用者のことです。この付与のされ方については、文書で行う、口頭で行うといった付与手段を問いません。明示的な付与手続によらずアクセス管理者の暗黙の了解によって付与されたものであっても構いません。以下「利用権者」といいます。）及びアクセス管理者（以下、利用権者とアクセス管理者を「利用権者等」とします。）ごとに定められている符号で、アクセス管理者がその利用権者等を他の利用権者等と区別して識別するために用いるものです。本法では、次のいずれかに該当する符号又は次のいずれかに該当する符号とその他の符号を組み合わせたものを識別符号としています。

ア. アクセス管理者によって、その内容をみだりに第三者に知らせてはならないものとされている符号（第1号）。

一般によく用いられているID・パスワードのうちのパスワードがこの代表例です。

なお、ID・パスワードの場合、第1号の符号に該当するパスワードのみでは識別符号の用をなさず、IDと組み合わせて初めて識別符号としての役割を果たすことになります。そのため、IDは、第1号の符号に該当する符号（パスワード）と組み合わせて用いられる「その他の符号」になります。IDとパスワードを組み合わせることによって、第1号の符号に該当するパスワードとその他の符号であるIDを「組み合わせた」識別符号になります。

イ. 利用権者等の身体の全部若しくは一部の影像又は音声を用いてアクセス管理者が定める方法により作成される符号（第2号）。

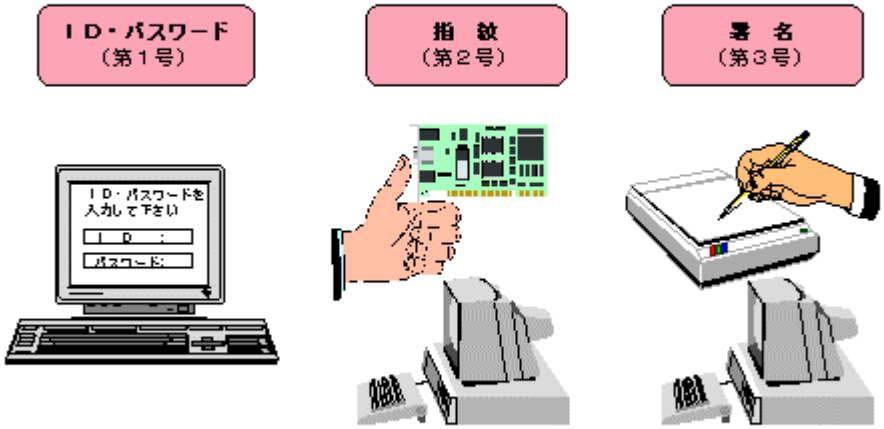
ここでいう影像の例としては、指紋や虹彩などがあります。アクセス管理者が定める方法とは、例えば指紋の場合でいえば、解像度いくらで読み取り特徴点の数やその位置関係をどのように数値化し符号化するかといったこと、音声の場合でいえば、周波数スペクトラムの時間的変化からどのように特徴を取り出して数値化し符号化するかといったことです。もちろん、この数値化及び符号化の方式はアクセス管理者が考案したものである必要はなく、既存の製品等を採用したものでよいのです。

なお、この第2号の場合には、第2号に該当する符号のみで識別符号となっているもの（例えば、指紋による認証システムなど）もありますし、第2号に該当する符号とその他の符号（IDなど）を組み合わせて識別符号となっているものもあります。

ウ．利用権者等の署名を用いてアクセス管理者が定める方法により作成される符号（第3号）。

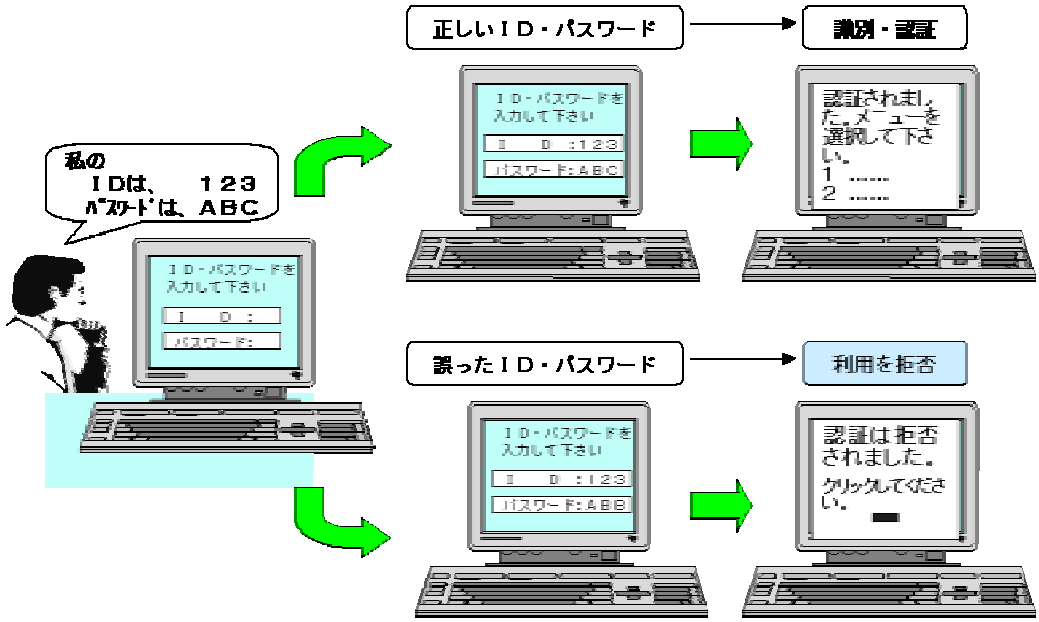
署名の形状やその筆圧、動態等から特徴を取り出して数値化し符号化するようなものを指しています。アクセス管理者が採用した方法で署名を数値化し符号化したものが識別符号となります。

この第3号の場合についても、第2号と同様、第3号に該当する符号のみで識別符号となっているものもありますし、第3号に該当する符号とその他の符号（IDなど）を組み合わせて識別符号となっているものもあります。

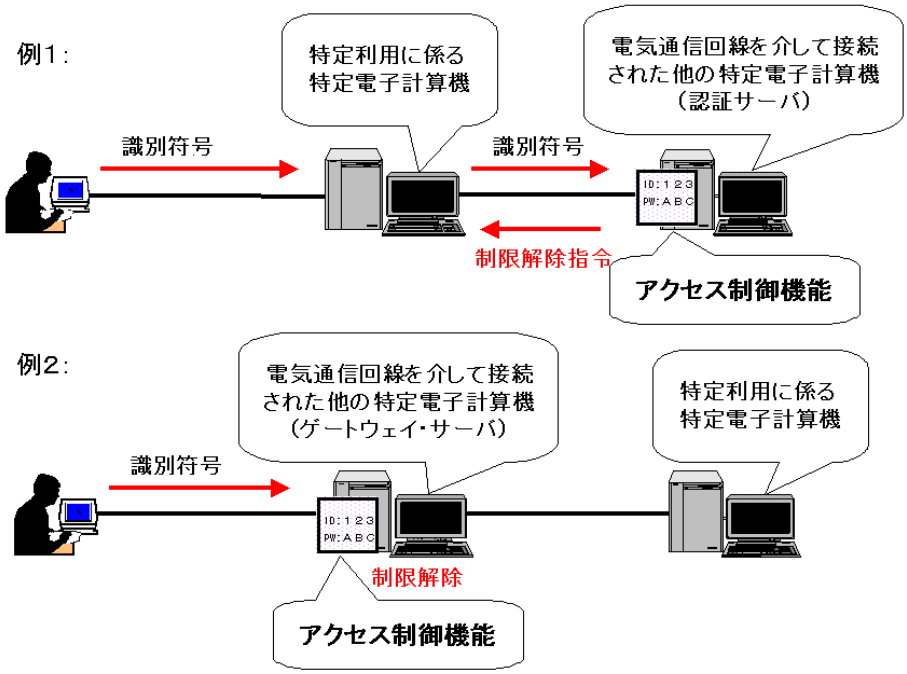


（3）アクセス制御機能（第2条第3項関係）

アクセス制御機能とは、特定電子計算機の特定利用を正規の利用権者等以外の者ができないように制限するために、アクセス管理者が特定電子計算機又は特定電子計算機と電気通信回線で接続されている電子計算機に持たせている機能です。具体的には、特定電子計算機の特定利用をしようとする者に電気通信回線を経由して識別符号（識別符号を用いてアクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。）の入力を求め、正しい識別符号が入力された場合にのみ利用制限を自動的に解除し、正しい識別符号ではなかった場合には利用を拒否するコンピュータの機能をいいます。

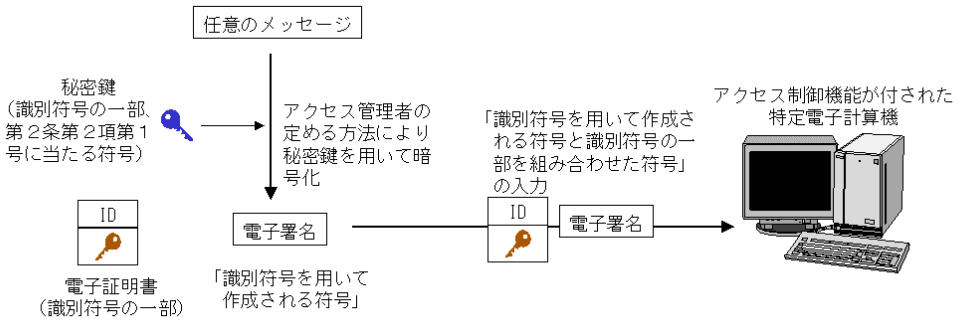


この機能を持たせる電子計算機は、その特定利用を制限しようとする特定電子計算機自体でも、その特定電子計算機と電気通信回線で接続されている他の電子計算機（例えば、別に設けた認証サーバ）であっても構いません。ですから、いわゆる認証サーバのように企業等のネットワークの内部に特定利用の制限及び制限の解除の指令を一元的に行うコンピュータを設置してこれによりアクセス制御を行うようなシステムであっても、いわゆるゲートウェイ・サーバのように企業等のネットワークの入り口に1台のコンピュータを設置してアクセス制御を一元的に行わせているようなシステムであってもよいことになります。



「識別符号を用いてアクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号」とは、公開鍵暗号方式を用いて利用権者等の認証を行っている場合に入力される、認証機関が発行する利用権者等の電子証明書（公開鍵証明書、ディジタル証明書ともいい、

ID情報、公開鍵情報を含んだものです。）と利用権者等の秘密鍵を用いて生成された電子署名とを組み合わせたもの等を指しています。公開鍵暗号方式による認証システムにおいて、ID・パスワード方式におけるパスワードに当たるもの（すなわち、本法第2条第2項第1号に当たる符号）はそれぞれの利用権者等が持っている秘密鍵であり、識別符号としては電子証明書と秘密鍵の組み合わせということになりますが、識別符号それ自体（秘密鍵）をアクセス制御機能が付された特定電子計算機に入力してはいません。そこで、本法第2条第2項にいう「識別符号」に「識別符号を用いてアクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号」を含めることとしました。ここで、「アクセス管理者の定める方法」とは具体的にはRSA、楕円暗号などの暗号化の方式を指し、「作成される符号」とは公開鍵暗号方式による電子署名を、「当該識別符号の一部」とは公開鍵暗号方式における電子証明書を指しています。



3　不正アクセス行為の禁止、処罰（第3条、第8条関係）

不正アクセス行為とは、アクセス制御機能による利用制限を免れて特定電子計算機の特定利用をできる状態にする行為です。

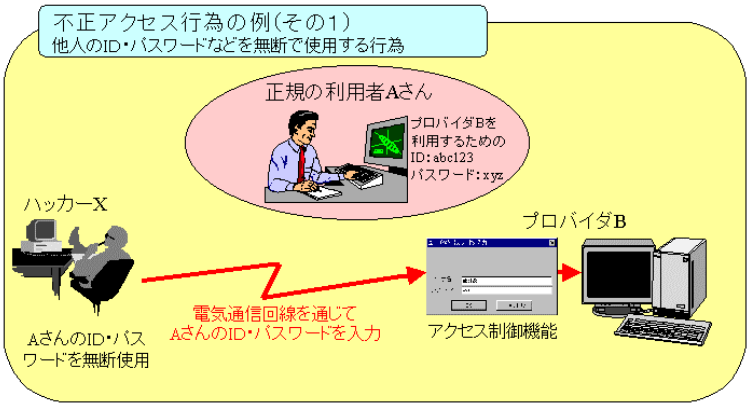
不正アクセス行為には、他人の識別符号を無断で入力する行為（第3条第2項第1号）と、識別符号以外の情報又は指令を入力する行為（同項第2号、第3号）の2つの類型があります。

なお、不正アクセス行為の禁止に違反した者は、1年以下の懲役又は50万円以下の罰金に処せられることとなっています（第8条第1号）。

（1）他人の識別符号を無断で入力する行為（第3条第2項第1号）

正規の利用権者等である他人の識別符号を無断で入力することによって利用制限を解除し、特定利用ができる状態にする行為です。

なお、アクセス管理者が行う場合及びアクセス管理者又は入力する識別符号を付与されている利用権者の承諾を得て行う場合は禁止の対象から除外しています。これは、正当な利用形態（例えば、コンピュータのセキュリティ・チェックを実施する場合や、会社の同僚に対して自分の代わりに電子メールが着信していないかどうかのチェックを依頼する場合など。）が考えられるためです。

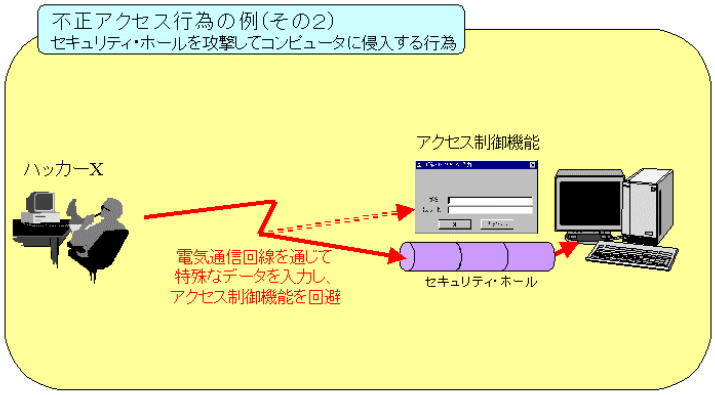


（2）アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力する行為（第3条第2項第2号、第3号）

いわゆるセキュリティ・ホール（アクセス制御機能のプログラムの瑕疵、アクセス管理者の設定上のミス等のコンピュータ・システムにおける安全対策上の不備）を攻撃する行為です。

セキュリティ・ホールがあるシステムに対して、特殊な情報又は指令を入力することにより、本来は識別符号を入力しなければ行うことができない特定利用が、これを入力することなしに行うことができるようになってしまう場合があります。この特殊な情報又は指令を入力して、特定利用ができる状態にする行為が第3条第2項第2号及び第3号に該当する不正アクセス行為です。ここで、「情報」とは電子計算機による処理の対象となるデータを、「指令」とは電子計算機に一定の動作をさせるためのコマンドのことを指していますが、ここでいう「情報又は指令」には、これらのそれぞれを単独で入力する場合のほか、この2つを組み合わせて入力するものも含んでいます。

なお、アクセス管理者又はその承諾を得た者が行う場合は禁止の対象から除外しています。これは、正当な利用形態（例えば、コンピュータのセキュリティ・チェックを行う場合など。）が考えられるためです。



不正アクセス行為には以上の2類型がありますが、いずれも「電気通信回線を通じて」行われるもの、すなわちコンピュータ・ネットワークを通じて行われるものに限定されています。したがって、スタンドアロンのコンピュータ(ネットワークに接続されていないコンピュータ)を無断で使用する行為や、ネットワークに接続されアクセス制御機能により特定利用が制限されているコンピュータであっても当該コンピュータのキーボード(コンソール)を直接操作して無断で使用する行為は、「電気通信回線を通じて」行われているわけではないため、不正アクセス行為には該当しないこととなります。

以上のことから、不正アクセス罪が成立するためには、

- 特定電子計算機、すなわちコンピュータ・ネットワークに接続されているコンピュータに対して行われたものであること。
- コンピュータ・ネットワークを通じて特定電子計算機へのアクセスが行われたものであること。
- 他人の識別符号又はアクセス制御機能による特定利用の制限を免れることができる情報又は指令が入力されたものであること。
- アクセス制御機能によって制限されている特定利用をすることができる状態にさせたもの(一部のセキュリティ・ホール攻撃のように、特定利用をすることができる状態に止まらず、特定利用をしてしまう行為をも含む。)であること。

が必要となります。この条件を満たせば不正アクセス行為となり、識別符号はどんな種類のもの(ID・パスワード、指紋、虹彩、音声、署名など)でもよく、特定利用についてはホームページの書き換え、インターネットショッピングの注文、データの閲覧、ファイル転送、ダイヤルアップ接続などその利用の内容に制限はありません。特定電子計算機は個人のものでも法人のものでもよく、対象となるコンピュータ・ネットワークにはインターネットなどのオープンネットワークのほか、企業内LANのように外部と接続していないものなども含まれます。識別符号を入力する端末機も必ずしもコンピュータである必要はなく、電話機からプッシュボタンを用いて他人の口座番号と暗証番号を入力し銀行のコンピュータに対してアクセスを行う行為なども不正アクセス行為に含まれることになります。

4　不正アクセス行為を助長する行為の禁止、処罰(第4条、第9条関係)

他人の識別符号を第三者に提供する行為、例えば、「○○システムを利用するためのIDは△△、パスワードは□□である。」と他人に口頭や電子メール、文書などで教えたり、電子掲示板などに掲示したりする行為は、その識別符号を利用すれば誰でも容易に不正アクセス行為を行うことが可能となる点で不正アクセス行為を助長するものですから、これを放置することは、不正アクセス行為を禁止することの実効性を著しく損なうこととなります。

そこで、他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるか（すなわち、どのコンピュータ（のサービス）に対する識別符号であるのかということ。）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、アクセス管理者や当該識別符号を付与されている利用権者に無断で第三者に提供する行為を禁止、処罰することとしています。

この不正アクセス行為助長罪が成立するためには、

- 識別符号が、それが付与された者に無断で提供されたこと。
- どの特定電子計算機の特定利用に係るもの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提供されたこと。

が必要です。識別符号の提供手段には限定がなく、電子掲示板に掲示する、電子メールで送付するといったオンラインで行うもののほか、口頭で伝達したり紙に印刷して手渡したりフロッピーディスクに記録して渡したりといったオフラインでの提供であっても犯罪は成立します。また、提供行為によって金銭的な利益を得たかどうかは犯罪の成立には無関係ですので、他人のID・パスワードを販売しても、無料で提供しても罪に問われます。

不正アクセス行為を助長する行為の禁止に違反した者は、30万円以下の罰金に処せられることとなっています（第9条）。

なお、アクセス管理者が行う場合及びアクセス管理者又は当該識別符号を所有している利用権者の承諾を得て行う場合については、これらの場合には他人の識別符号を入力しても不正アクセス行為には当たらないこととしていることから、不正アクセス行為を助長するおそれが認められないので、禁止の対象から除外しています。

5 アクセス管理者による防御措置（第5条関係）

不正アクセス行為の発生を防止するためには、その禁止・処罰に頼るのみではなく、不正アクセス行為が行われにくい環境を整備することが必要となります。そのためには、個々のアクセス管理者が自ら防御措置を講じることが必要となりますが、その実施状況は必ずしも十分ではないのが現状です。

そこで、アクセス管理者に防御措置の実施を促すため、アクセス管理者に不正アクセス行為からの防御措置を講ずべき責務があることを法律上明確にしました。そして、アクセス制御機能を特定電子計算機に付加したアクセス管理者は、ID・パスワードといった識別符号等の適正な管理に努めるとともに、常にアクセス制御機能の有効性を検証し、必要があると認めるときにはアクセス制御機能の高度化その他必要な措置を講ずるよう努めるものとしています。

アクセス管理者に求められる防御措置の主な内容としては、

- 利用権者の異動時における識別符号の確実な追加・削除、長期間利用されていない識別符号の確実な削除、パスワード・ファイルの暗号化といった識別符号の適正な管理
- アクセス制御機能として用いているシステムのセキュリティに関する情報（セキュリティ・ホール情報、バージョン・アップ情報など）の収集といったアクセス制御機能の有効性の検証
- パッチプログラムによるセキュリティ・ホールの解消、アクセス制御プログラムのバージョン・アップ、指紋・虹彩などを利用したアクセス制御システムの導入といったアクセス制御機能の高度化
- コンピュータ・ネットワークの状態を監視するのに必要なログを取得しその定期的な検査を行う、ログを利用して前回アクセス日時を表示し利用権者にその確認を求めるといったログの有効活用
- ネットワーク・セキュリティ責任者の設置

といったことが挙げられます。

具体的にシステムに対してどのような防御措置を講ずべきかについては、アクセス管理者が個々に判断することとなりますが、国家公安委員会（警察庁）、通商産業省及び郵政省からネットワーク・セキュリティに関するガイドラインが公表されておりますので、これらを参考として措置を講じてください。

各省庁から公表されているネットワーク・セキュリティに関するガイドライン

- 情報システム安全対策指針（平成9年国家公安委員会告示第9号）

  [http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm]
- コンピュータ不正アクセス対策基準（平成8年通商産業省告示第362号）

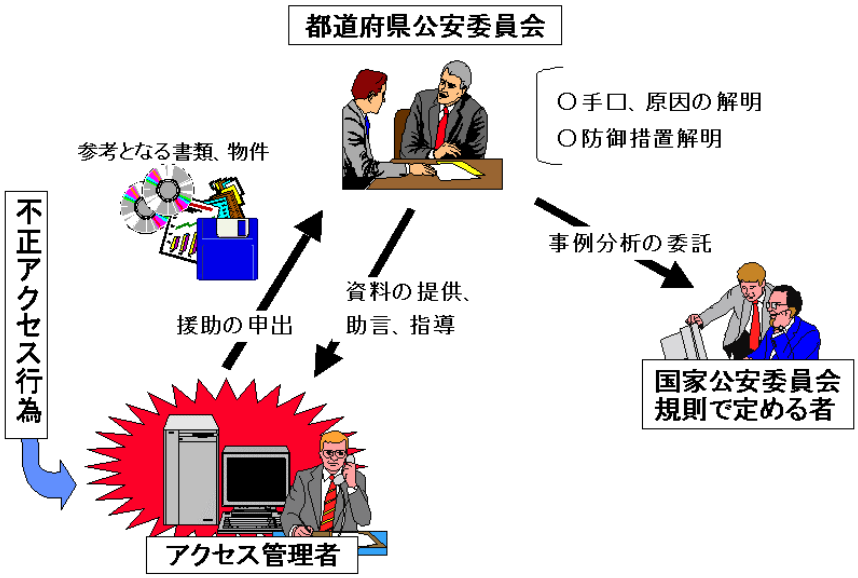
  [http://www.miti.go.jp/press-j/past/c60806a2.html]
- 情報システム安全対策基準（平成7年通商産業省告示第518号）
- 情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）

6 都道府県公安委員会による援助等

（1）都道府県公安委員会による援助（第6条関係）

都道府県公安委員会及び方面公安委員会（以下「公安委員会」といいます。）は、不正アクセス行為が行われたと認められる場合において、不正アクセス行為が行われた特定電子計算機のアクセス管理者から援助を受けたい旨の申出があり、その申出を相当と認めるときは、申出者に対して不正アクセス行為の再発防止のための援助を行うこととしています（第1項）。公安委員会が行う援助の内容は、申出者が再発防止措置を講ずることができるよう、その具体的方法について資料の提供、助言、指導等を行うことです。ここで注意しなければならないのは、公安委員会が行うのはあくまで再発防止措置（例えば、ソフトウェアの設定を適切なものに変更したりといったことなど。）についての資料提供や助言、指導のみであり、実際にそれらの再発防止措置を実施するのは申出人であるアクセス管理者自身であるということです。

公安委員会は、援助を行うために、不正アクセス行為の手口、不正アクセス行為を受けた原因、不正アクセス行為の再発防止措置のメニュー等を申出者から提出された資料等を基に解明し（これを「事例分析」といっています。）、その結果を踏まえて援助を行います。



アクセス管理者が公安委員会による援助を受けるに当たっては、いくつか要件があります。まず、本法に規定する不正アクセス行為を受けた者である必要があります。多量にメールを送りつけられた、過負荷攻撃を受けたといったことそのものは、多くは本法でいう不正アクセス行為には該当しませんから、援助の対象とはなりません（仮に、公安委員会に対して申出を行ったとしても、受理されません。）。また、不正アクセス行為の分析に必要な資料は申出を行ったアクセス管理者から提出される必要があり、これを拒んだ場合にも援助の対象とはなりません。さらに、公安委員会による援助は不正アクセス行為の再発防止のための応急措置に必要と考えられるものに限られますので、この範囲を逸脱するような援助をアクセス管理者が要求するようであれば、やはり援助の対象となりません。

（2）国による広報啓発活動（第7条関係）

アクセス管理者はもとより、ソフトウェア事業者、ハードウェア事業者、エンドユーザ等のコンピュータ・ネットワークに関係する者すべてが不正アクセス行為の危険性を正しく認識するとともに、それぞれの立場で不正アクセス行為を防御するための活動を行うことが、不正アクセス行為が行われにくい環境を整備するためには必要です。そこで、このようなそれぞれの立場で行われる活動に資すること

ができるように、国家公安委員会、通商産業大臣及び郵政大臣が、毎年少なくとも1回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表することとしています（第1項）。

また、国は、不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならないこととしています（第2項）。

7 施行期日

本法は、公布の日（平成11年8月13日）から起算して6箇月を経過した日（平成12年2月13日）から施行されます。ただし、6（1）項で説明した事項（公安委員会による、不正アクセス行為を受けたアクセス管理者に対する援助に関する規定）については公布の日から起算して1年を超えない範囲内において政令で定める日（平成12年7月1日）から施行されます。

8 その他

本法の全条文やその他不正アクセス行為対策に関する情報は、次の各省庁のホームページから得ることができます。

警察庁ホームページ：http://www.npa.go.jp
通商産業省ホームページ：http://www.miti.go.jp/
郵政省ホームページ：http://www.mpt.go.jp/

別添2

不正アクセス行為の発生状況

第1　平成12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

不正アクセス禁止法の施行日（平成12年2月13日）から平成12年12月31日までの間に警察庁に報告のあった不正アクセス行為（以下「期間中の不正アクセス行為」という。）が対象である。

1　不正アクセス行為の発生状況及びその特徴

期間中の不正アクセス行為は、106件であった。そのうち、海外から不正アクセス行為が行われたことが判明しているものは、25件あった。

		認知件数
被害に係る特定電子計算機のアクセス管理者別	プロバイダ	59
	大　学	8
	情報通信企業	6
	そ の 他	33
	計	106

		認知件数
認 知 の 端 緒 別	アクセス管理者からの届出	30
	利用権者からの届出	23
	発見者からの通報	7
	被疑者の取調べ	35
	そ の 他	11
	計	106

これらを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59件と最も多く、次いで大学が8件の順となっている。

また、認知の端緒の主なものとしては、警察への届出等が60件（アクセス管理者からの届出が30件、利用権者からの届出が23件、その他発見者からの通報が7件）、被疑者の取調べ等の警察活動が35件あった。

なお、不正アクセス行為後の行為としてホームページの改ざん、消去を伴うものが33件、DDoS用攻撃ツール（Trinity V3）（参考1を参照）を仕掛けられていたものが2件あった。

2　不正アクセス禁止法違反事件の検挙状況

期間中の不正アクセス禁止法違反の検挙件数は31事件（67件）、検挙人員は37人であった。その内訳は、不正アクセス行為が30事件（62件）、34人であり、不正アクセス助長行為が4事件（5件。3事件は不正アクセス行為でも検挙。）、5人（2人は不正アクセス行為でも検挙。）であった。

不正アクセス行為の態様については、30事件中29事件（61件）が識別符号窃用型（不正アクセス禁止法第3条第2項第1号の他人の識別符号を無断で入力する行為をいう。）であり、残りの1事件（1件）がセキュリティ・ホール攻撃型（不正アクセス禁止法第3条第2項第2号及び第3号のアクセス制御機能による特定利用の制限を免れる情報又は指令を入力する行為をいう。）であった。また、不正アクセス助長行為で検挙した事件は、いずれも識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして提供していたものであった。

なお、検挙人員37人中31人が成人であり、6人が少年であった。

事 犯 別	検挙事件数	検挙件数	検挙人員
不正アクセス行為	30	62	34人
不正アクセス助長行為	4	5	5人
計	31 (重複3)	67	37人 （重複2人）

3　**検挙事例**

違法薬物販売目的の他人の識別符号を使用した不正アクセス禁止法違反等事件

無職の男(34)が、クラッキング・ツール等を利用して入手した他人のID・パスワードを使用して不正にインターネットに接続し、ホームページを開設した上、薬物販売の広告を掲示し、薬物の購入希望者とメールのやり取り等をするとともに、同ホームページで販売する目的で医薬品や向精神薬を自宅に所持していた。12年3月、不正アクセス禁止法違反、薬事法違反及び麻薬及び向精神薬取締法違反で検挙した（千葉）。

音楽配信会社のメールサーバに対する不正アクセス禁止法違反事件

音楽配信会社の元役員(32)が、役員当時知り得た社長等のID・パスワードを使用して同社のメールサーバに侵入し、電子メールの内容を盗み見た。12年6月、不正アクセス禁止法違反で検挙した（警視庁）。

2ショットチャット掲示板に対する不正アクセス禁止法違反事件

建設会社の会社員(32)が、被害者が開設した有料掲示板「2ショットチャット」に対し、認証機能が甘いことに乗じ、CGIプログラムを使用してセキュリティ・ホールを突き、識別符号を入力することなく接続した。12年6月、不正アクセス禁止法違反で検挙した（北海道、富山）。

オンラインゲームに係る不正アクセス禁止法違反事件

派遣会社の社員(23)が、クラッキング・ツールを利用して入手した他人のID・パスワードを使用して不正に米国のオンラインゲーム・サーバに侵入し、ゲームを行った。その際、同ゲームのチャット上で知り合った少年に対し同ID・パスワードを教示した。12年4月、不正アクセス禁止法違反で検挙した（警視庁）。

レンタル・サーバ業者のウェブ・サーバに対する不正アクセス禁止法違反等事 件

無職の男(33)が、総当たりにより探知した元勤務先の広告会社のID・パスワードを使用して同社の契約会社のウェブ・サーバに侵入し、ホームページのデータを削除した。12年8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（大阪）。

iモード電話機用のウェブ・サーバに対する不正アクセス禁止法違反事件

無職の男(23)が、iモード電話機用の掲示板から入手した他人のID・パスワードを同電話機のメール・サービスを利用してハッカー仲間である会社員(25)に提供、さらに、同会社員が、同ID等をハッカー仲間である大学生(25)に提供し、同大学生が、同ID等を使用して不正にiモード電話機用のウェブ・サーバに侵入し、掲示板の内容を書き換えるなどした。12年10月、不正アクセス禁止法違反で無職の男ら3人を検挙

した（警視庁）。

ホームページ提供サービス業者のウェブ・サーバに対する不正アクセス禁止法 違反等事件

韓国関連の情報交換のためのホームページを開設する会社員(31)が、自己のホームページの掲示板に嫌がらせの書き込みをされたことに立腹し、同書き込みをした者が開設する韓国関連のホームページに係るID・パスワードを推測により探知し、不正にホームページ提供サービス業者のウェブ・サーバに侵入し、本人に無断で退会届をすることにより同ホームページのデータを消去した。12年10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（警視庁）。

解雇された会社の識別符号を窃取した不正アクセス禁止法違反等事件

情報通信関連会社の元社員(25)が、同社を解雇されたことに立腹し、同社に金銭的損害を与える目的で、在職中に知り得た同社のID・パスワードを使用して不正にインターネットに接続するとともに、同社に高額のインターネット接続料が請求されるように契約内容を変更する旨の虚偽の情報をプロバイダのサーバに送信して事実証明に関する電磁的記録を不正に作出したほか、ホームページ上で前記ID等を公開した。12年10月、不正アクセス禁止法違反及び電磁的記録不正作出罪で検挙した（警視庁）。

広域にわたるハッカー・グループによる不正アクセス禁止法違反事件

ハッカー・グループの主犯格の男(30)が、クラッキング・ツール等を利用して入手した他人のID・パスワードを使用して不正に国立大学、観光協会及びプロバイダの各サーバに侵入するとともに、自己の運営する掲示板において、前記国立大学のサーバに係る同ID等の掲示、観光協会及びプロバイダに対する不正アクセス手法の教示等を行った。また、同教示を受けた同グループのメンバーである主婦(42)、大学生(23)が、それぞれクラッキング・ツールの利用等教示を受けた手法により入手した他人のID・パスワードを使用して不正に国立大学又は観光協会のサーバに侵入した。12年11月、不正アクセス禁止法違反で主犯格のほかハッカー・グループのメンバー2人を検挙した（愛知、秋田、宮城、警視庁、広島）。

4　検挙事件の特徴

(1) 犯行の手口

不正アクセス行為で検挙した30事件（62件）の手口としては、ユーザのパスワード管理の甘さにつけ込んだID・パスワードの入手が12事件（14件）と最も多く、次いでトロイの木馬（参考2を参照）系のコンピュータ・ウイルス等のクラッキング・ツールによるID・パスワードの入手やセキュリティ・ホール攻撃が8事件（14件）、他人からのID・パスワードの入手が6事件（25件）の順となっている。

なお、クラッキング・ツールの中では、トロイの木馬系のコンピュータ・ウイルスを利用したものが多く、識別符号の入手等にクラッキング・ツールを使用した事件中3事件（5件）で使用されていた。いずれの被疑者も、クラッキング・ツールをネットワーク上のホームページからダウンロードし、又は雑誌の付録CD等から入手していた。

このほか、犯行の発覚を免れるため、海外のプロキシ・サーバを使用していた事件（2事件（2件））もあった。

(2) 被疑者の特徴

検挙した37人の被疑者の年齢は、30代が16人と最も多く、次いで20代が13人、10代が6人の順とな

っている。最年長の者は48歳であり、最年少の者は15歳であった。

なお、検挙人員には含まれないものの、刑事責任の無い少年が不正アクセス行為を行っていたもの（補導処分）もある。

(3) 犯行の動機

不正アクセス行為の動機としては、利用料金の請求を免れるためが13事件（34件）と最も多く、次いで嫌がらせ・仕返しが5事件（7件）、メールの盗み見が5事件（5件）、なりすまして別の犯罪等の発覚を免れるためが3事件（7件）、いたずら目的が2事件（3件）の順となっている。少年被疑者にあっては、特段の罪悪感を持たずに犯行に至っているのが目立つ。

(4) その他

不正アクセス行為が別の犯罪の手段として利用されていた事案は、8事件（12件）であった（薬事法及び麻薬及び向精神薬取締法違反事件、業務妨害事件、詐欺事件、名誉毀損事件、電子計算機損壊等業務妨害事件、著作権法違反事件、電磁的記録不正作出事件）。

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（平成12年7月1日施行）に基づくアクセス管理者に対する助言・指導を、平成12年12月31日までに6件（東京、滋賀、大阪、北海道、京都、神奈川）実施している。

6 防御上の留意事項

(1) トロイの木馬対策

トロイの木馬系のコンピュータ・ウイルスの感染を予防するため、不審な電子メールを受信した場合にはメールの添付ファイルを不用意に開かないことなどに留意する。

(2) 識別符号の適切な管理

推測されやすいパスワードの解消、パスワードの定期的な変更、使用されなくなったID・パスワードの抹消等識別符号の適切な管理を行う。

(3) サーバの適切な管理

セキュリティ・ホールの解消、適切に設定されたファイアウォールの設置、ログの保存・監査等サーバの適切な管理を行う。

(4) その他

・「情報システム安全対策指針」（平成11年国家公安委員会告示第19号）を参考に一般的な対策も併せて講ずることが望ましい。

・都道府県警察においては、不正アクセス禁止法に基づく援助を行っているほか、ハイテク犯罪相談を行っているので、被害が発生した場合には、都道府県警察のハイテク犯罪相談窓口に連絡する（相談窓口一覧：警察庁ホームページhttp://www.npa.go.jp/）。

（参考）

1 DDoS(Distributed Denial of Service)攻撃ツール（Trinity V3）について

DDoS攻撃とは、インターネット上の複数のコンピュータにDoS攻撃（標的となるサーバコンピュータに過剰な負荷をかけるなどして当該サーバコンピュータのサービスを妨害する攻撃）用のツールを仕掛け、攻撃者の使用するコンピュータからの命令により一斉にDoS攻撃を行い、標的となるサーバコンピュータのサービスを妨害するものである。

DDoS攻撃ツールが仕掛けられていた場合は、システムの再インストールにより攻撃用ツールを削除するとともに、OS及びアプリケーションのバージョンアップ並びに定期的点検等により再発に注意しなければなら

ない。

なお、Trinity V3は、昨年9月に発見されたDDoS攻撃ツールの一種で、検出のためには次の2つの項目の確認が必要とされている。

①ポート33270の開閉状態を確認する。

通常は使用されていないポート番号のため閉じられているが、DDoS攻撃ツール(Trinity V3)が仕掛けられると解放状態となる。

②ファイルを点検する。

DDoS攻撃ツール(Trinity V3)を仕掛けられたコンピュータには、

/usr/lib/のディレクトリー下にidle.soというファイル及び/var/spool/uucp/のディレクトリー下にuuicoというファイルが存在する。

2 トロイの木馬について

○ トロイの木馬とは

「トロイの木馬」は、コンピュータに悪影響を及ぼしたり、ユーザを欺くプログラムを内包していながら、普通のアプリケーションプログラム等の体裁を有しているプログラムであり、通常、コンピュータ・ウイルスの一種として扱われている。パソコンにトロイの木馬が仕掛けられると、ユーザは業務処理やゲームなどをしているつもりでも、背後では別の機能が作動していて、パスワードを盗むなどの被害を与えている。トロイの木馬の語源は、古代ギリシャのトロイ戦争で、都市国家トロイが、中に敵軍兵士が潜んでいるとも知らずに、門前におかれた大きな木馬を内部に引き入れ、敗れたという故事にちなんでいる。

トロイの木馬は、実際に発生している不正アクセス禁止法違反事件でも使用されており、不正アクセス行為の発生の一因にもなっている。

○ トロイの木馬の特徴

トロイの木馬には多くの種類があるが、これらのほとんどはインターネットから容易に入手することができる。これまで検挙された不正アクセス禁止法違反事件では、SubSeven、BackOrifice及びDeepThroatという名称のトロイの木馬が用いられた。これらは、不正アクセス行為の対象となるコンピュータに仕掛けるプログラム（サーバプログラム）とサーバプログラムが仕掛けられているコンピュータを遠隔操作するため他のコンピュータ（行為者のパソコン等）において作動するプログラム(クライアントプログラム)により構成される。

不正アクセス禁止法違反事件において識別符号を窃取されたコンピュータのいくつかには、実際にこれらのサーバプログラムが仕掛けられていた。これらは、インターネットを経由した遠隔操作により、Windowsにおいて用いられるインターネット接続用のID・パスワードの窃取、情報の改ざん等を行う機能を有している。

○ 被害の予防方法

トロイの木馬は、サーバプログラムとクライアントプログラムが連携して機能するものであるから、被害を予防するには、サーバプログラムが仕掛けられることを防ぐのが第一である。そのためには、コンピュータ・ウイルスの感染予防と同様に、メール等により外部から送られてきた添付ファイルやいかがわしいサイトからダウンロードしたプログラムを不用意に実行しないなどの注意が必要である。このようなプログラムを添付されたメールは、件名を偽りソフトウェアベンダからのバージョンアップ等の案内になりすましたもの、添付ファイルの種類を変更し画像ファイルやビデオファイルになりすましたもの等さまざまな偽装を施していることがほとんどであることに注意しなければならない。

ほとんどのサーバプログラムは、コンピュータ・ウイルスのワクチンソフトにより検出・駆除が可能であることから、それらを導入・常駐させることも有効な予防方法である。また、シェアウェアのトロイの木馬専用の検出・駆除ソフトウェアがインターネット上で提供されている。（ソフト名The Cleaner、http://www.moosof

t.com/）

（注1）

不正アクセス行為の認知の考え方

認知とは、被害届を受理した場合のほか、余罪として発覚した場合、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等不正アクセス行為の事実確認ができた場合とすることとしている。

（注2）

不正アクセス行為の件数の計上について

・ 一のアクセス制御機能に対する一の手口による侵害行為を1件とする。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、短期間に一のアクセス制御機能に対して同一手口による侵害が継続的に行われた場合は包括して1件とする。

・ 不正アクセス行為と他の罪とが併合罪又は観念的競合の関係にある場合、これを別件として扱い、1件計上する。

別添3

更新:平成13年5月17日_警　　察　　庁_

ホームページ書き換え事案に関する対策について

○ ホームページ書き換えプログラムによる事案

平成13年5月17日:販売企業18社に対する要請_平成13年5月10日:事案の概要と注意喚起

○ 日本企業等に対するホームページ書き換え事案

平成13年3月　8日:具体的な情報セキュリティ対策に関する情報提供_平成13年2月23日:事案の概要と注意喚起

ホームページ書き換えプログラムによる事案_

平成13年5月17日_

1　被害状況

平成13年5月10日にホームページ書き換えプログラムに関する対策について公表したところであり、都道府県警察においては当該書き換えプログラムによってホームページを改ざんされた地方公共団体、民間企業、大学等からの相談及び被害届を、97件（5月17日正午現在）受理しているところであります。

当該書き換えプログラムは、書き換えについては、OSとしてWindowsNTを使用しているサーバー（以下「Windowsサーバー」という。）を対象とするとともに、OSとしてSolarisを使用しているサーバー（以下「Solarisサーバー」という。）にSolarisのセキュリティホールを突いて自動的に自己を複写することによって増殖を繰り返す性能を有しています。_ したがって、被害が顕在化しないSolarisサーバーについて適切なセキュリティ対策が講じられない場合、攻撃する拠点であるSolarisサーバーが増加することによって、Windowsサーバーに対する書き換え被害が爆発的に拡大するおそれがあります。

2　Solarisサーバーの管理者が採るべき措置

検知プログラムの利用又は「/dev/cub」及び「/dev/cuc」というフォルダの検索により、当該書き換えプログラムの有無を確認した上で

○ 最新のパッチプログラムを適用する。_○ 111番ポート(SUN Remote Procedure Call)を閉じる。

等の措置を採ってください。また、当該書き換えプログラムを発見した場合には、当該書き換えプログラムの伝搬ルートを追跡し、発信元のSolarisサーバーに対して被害拡大の防止措置を採る必要があることから、都道府県警察のハイテク犯罪相談窓口にご連絡下さい。

3　警察庁から販売企業に対する要請（平成13年5月17日実施）

上記措置を確実に採っていただくことにより今後の被害拡大を防止するために、当庁よりSolarisサーバーを販売する18社に対し、その顧客に向けて

○ ホームページ書き換えプログラムの 検知プログラムの提供 _○ 未知のフォルダ及び未知のプログラムの確認依頼 _○ 最新のパッチプログラム の適用依頼 _○ ファイアウォール等による適切なフィルタリングの依頼 _○ 都道府県警察のハイテク犯罪相談窓口情報の提供

を実施するように要請いたしました。

平成13年5月10日_

平成13年5月1日以降、都道府県警察において、地方公共団体、民間企業等のホームページが書き換えられる事案を15件（5月10日午前10時現在）把握しております。それらは、いずれも同種のホームページ書き換えプログラムが使用されております。

当該書き換えプログラムの概要は、次のとおりです。

1 Solaris上で動作するsadmind（システム管理用プログラム）のセキュリティホールを突いてサーバーに侵入し、「/dev/cub」と「/dev/cuc」というフォルダを作成し、当該書き換えプログラムを蔵置する。

2 他のサーバーの調査を行い、使用しているOSがSolarisであれば1を試みると同時にWindows（NT又は2000）であればIIS4.0/5.0（Web用プログラム）のセキュリティホールを突いてホームページの改ざんを試みる。

3 改ざんされたホームページには、次の内容が表示される。

「fuck USA Government

fuck Poizonb0x
contact:sysadmcn@yahoo.com.cn」

このように、当該書き換えプログラムは、他人のサーバーのホームページを改ざんするとともに、自己を他のサーバーに複写し、これを繰り返す機能を有するので、適切なセキュリティ対策が講じられていないと他のサーバーに被害を拡大させたり、同じサーバーが再び被害に遭う可能性があります。サーバー内に上記フォルダが作成され、未知のプログラムが蔵置されていないか確認し、今後の被害防止のために下記の対策を行ってください。

○ OSがSolarisでsadmindを使用している場合
（原因）sadmindのセキュリティホール
（対策）sadmindを停止するか最新パッチプログラムを適用する。

○ OSがWindows（NT又は2000）でIIS4.0/5.0を使用している場合
（原因）IIS4.0/5.0のセキュリティホール
（対策）最新パッチプログラムを適用する。

上記フォルダや未知のプログラムが発見されたり、ホームページが改ざんされたりして被害が発生した場合には、 都道府県警察のハイテク犯罪相談窓口 に連絡してください。 不正アクセス禁止法の援助規定等に基づく助言・指導も実施いたします。また、「情報システム安全対策指針」（平成11年国家公安委員会告示第19号）も参考にしてください。

日本企業等に対するホームページ書き換え事案_

平成13年3月8日_

平成13年2月23日に海外のサイトからと思われる日本企業等に対するホームページ書き換え事案に関する対策について公表したところですが、3月8日午前0時現在、全国で104件の書き換えを把握しています。全国の都道府県警察における解析の結果により、現在判明しているホームページを書き換えられた主な原因及び今後の被害防止のための対策については、下記のとおりですので参考にしてください。

○（原因）IIS(Web用プログラム)のセキュリティホール
（対策）サービスパック等、最新 パッチプログラム を適用する。

○（原因）BIND(DNSサーバー用プログラム)のセキュリティホール
（対策）最新 パッチプログラムを適用する。

○（原因）Front Page Server Extensions(ホームページ作成・管理プログラム)の設定ミス
（対策）設定の再確認（参照：対策1、対策2）又は不必要な場合当該プログラムの削除を行う。

○（原因）不適切なアクセス制御
（対策）ID・パスワードに代表される識別符号によりサーバーに対する適切なアクセス制御を行ってください。特にパスワードの未設定による被害が見受けられます。また、推測されやすいパスワードも攻撃の対象となり得ます。

なお、当該事案において不正プログラムが蔵置されている被害サーバーも見られることから、DDoS攻撃ツール等による第三者に対する攻撃の踏み台となることを防ぐため、サーバー内に未知のファイルが保存されていないか、既知のファイルが書き換えられていないかなど確認をしてください。

平成13年2月23日_

平成13年2月19日に、海外のサイトに我が国のサイトに対する攻撃を予告する内容が掲載されているとの情報を入手しましたが、これに関係すると思われる日本企業等に対するホームページ書き換え事案が発生しています。_ 2月23日午前0時現在、全国で70件の書き換えを把握しています。今後の被害防止のための当面の対応策として下記の点について確認することが重要です。

1 基本ソフトウェア（OS）、アプリケーションプログラムを最新のバージョンに更新し適切な修正プログラム（パッチ）を適用するようにして下さい。_ 特に、今回多数の攻撃対象となっているWindowsNT、IIS4.0を利用しているユーザは注意してください。

2 ルータ、ファイアウォールで外部からのアクセスを制御する等システムのアクセス制御を厳密に行ってください。

3 不必要なネットワークサービス、CGIプログラムの停止及び不要ポートを閉鎖して下さい。_ 裏口として使用されている可能性のある99番ポートはもちろん、その他の通信ポートも含めて、通信ポート検査用プログラムを用いて検査して下さい。検査の結果、動作中であると判明した通信ポートのそれぞれについて、裏口や必要でない通信ポートであることが確認された場合はそれらを停止してください。

4 登録ユーザの再確認、ホームページの目視等、定期的点検を励行して下さい。

5 システムのアクセス記録を保存して下さい。_ 必要なログを保存するため、保存するログの範囲及び保存期間を定めて、コンピータにおいて保存の設定を行ってください。その際、ログの定期的なバックアップ、他のコンピュータ（外部から直接アクセスできないコンピュータ等）へのログの保存など、ログが安全に保存されるよ

う留意して下さい。_ また、ログは、随時監視し、入力データの異常、プログラムの異常終了等の発見に努めることが必要です。

6 DDoS攻撃用ツールに注意してください。

DDoS攻撃とは、インターネット上の複数のコンピュータにDoS攻撃（標的となるサーバコンピュータに過剰な負荷をかけるなどして当該サーバコンピュータのサービスを妨害する攻撃）用のツールを仕掛け、攻撃者の使用するコンピュータからの命令により一斉にDoS攻撃を行い、標的となるサーバコンピュータのサービスを妨害するものです。_ DDoS攻撃ツールが仕掛けられていた場合は、システムの再インストールにより攻撃用ツールを削除するとともに、OS及びアプリケーションのバージョンアップ並びに定期的点検等を実施して下さい。_ 昨年の不正アクセスの例では、Trinity V3というツールが使われているものがありますが、こうしたツールを発見するためのプログラムが http://www.nipc.gov/warnings/advisories/2000/00-055.htm にあります。

また、 不正アクセス行為の発生状況の公表を参照して下さい。

7 その他

「 情報システム安全対策指針 」（平成11年国家公安委員会告示第19号）も参考にして下さい。

都道府県警察においては、 不正アクセス禁止法に基づく援助 を行っているほか、ハイテク犯罪相談を行っているので、被害が発生した場合には、 都道府県警察のハイテク犯罪相談窓口 に連絡して下さい。