不正アクセス行為の禁止等に関する法律の解説

１　法の目的、基本構成(第１条関係)

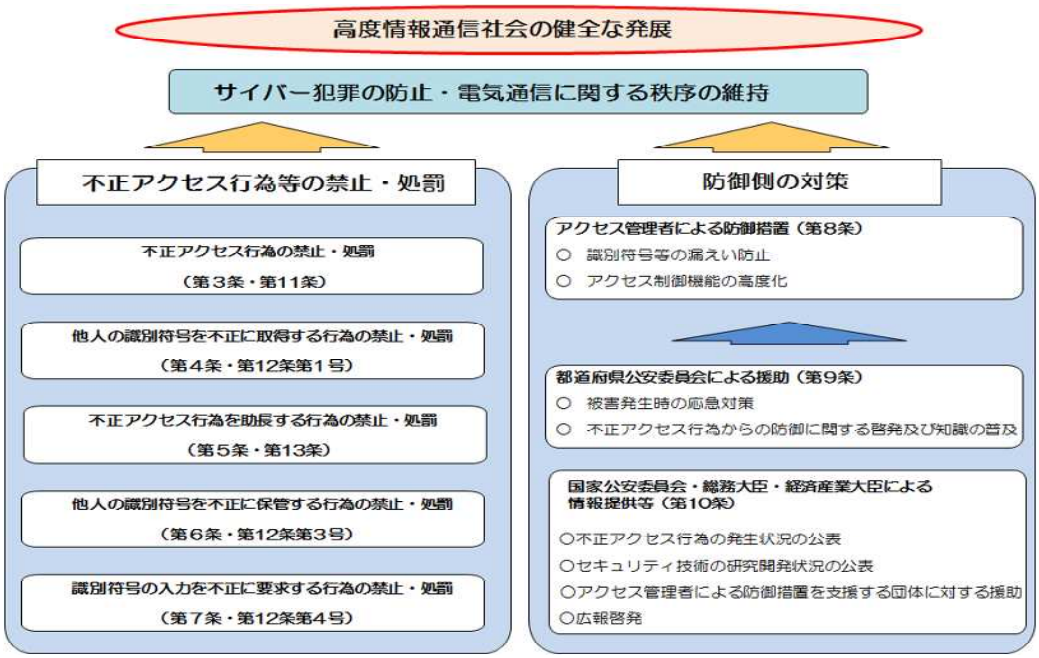
(1)　不正アクセス行為の禁止等に関する法律(以下「本法」といいます。)は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のため不正アクセス行為を受けたアクセス管理者に対する都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪(注)の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的としています。

(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。

不正アクセス行為の禁止等に関する法律の概要



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。

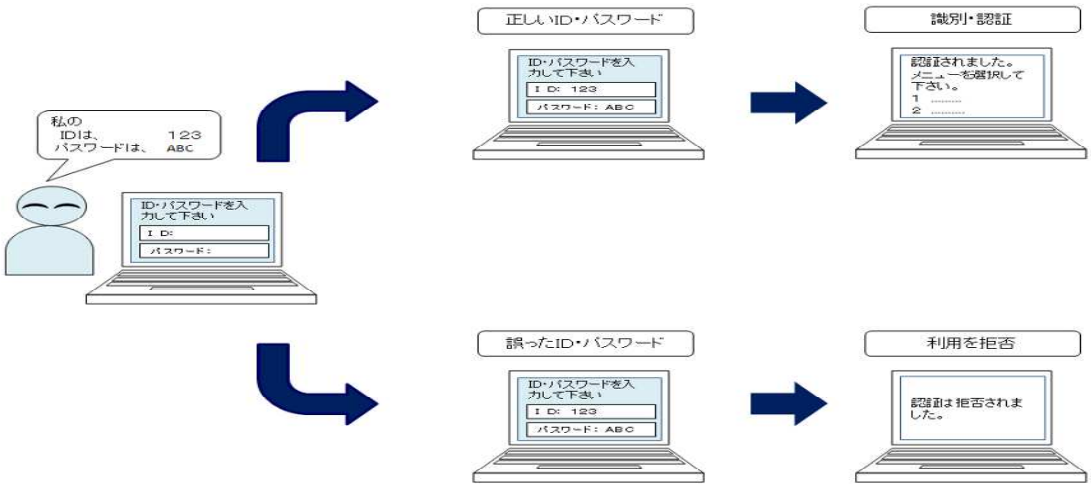
ウ　利用権者等の署名を用いてアクセス管理者が定める方法により作成される符号(第３号)。

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。

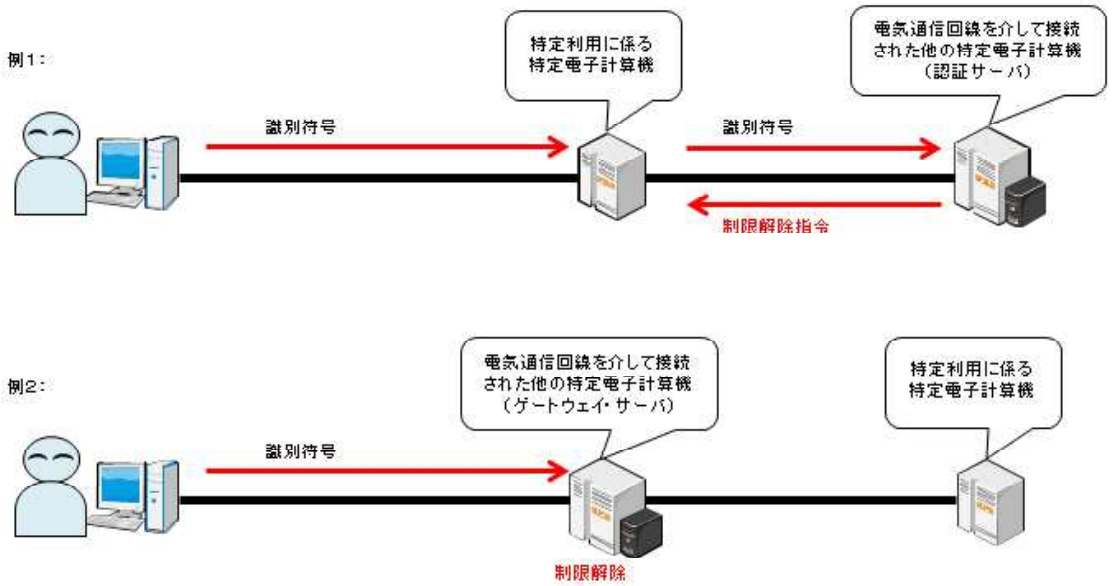
この第３号の場合についても、第２号と同様、第３号に該当する符号のみで識別符号となっているものもありますし、第３号に該当する符号とその他の符号(ＩＤなど)を組み合わせて識別符号となっているものもあります。

(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２条第４項、第３条、第11条関係)

不正アクセス行為とは、他人の識別符号を悪用したり(第２条第４項第１号)、コンピュータプログラムの不備を衝く(第２条第４項第２号、第３号)ことにより、本来アクセスする権限のないコンピュータを利用する行為のことをいいます。

なお、不正アクセス行為の禁止に違反した者は、３年以下の懲役又は100万円以下の罰金に処せられることとなっています(第11条)。

(1)　他人の識別符号を悪用する行為(第２条第４項第１号)

他人の識別符号を悪用することにより、本来アクセスする権限のないコンピュータを利用する行為、すなわち、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。

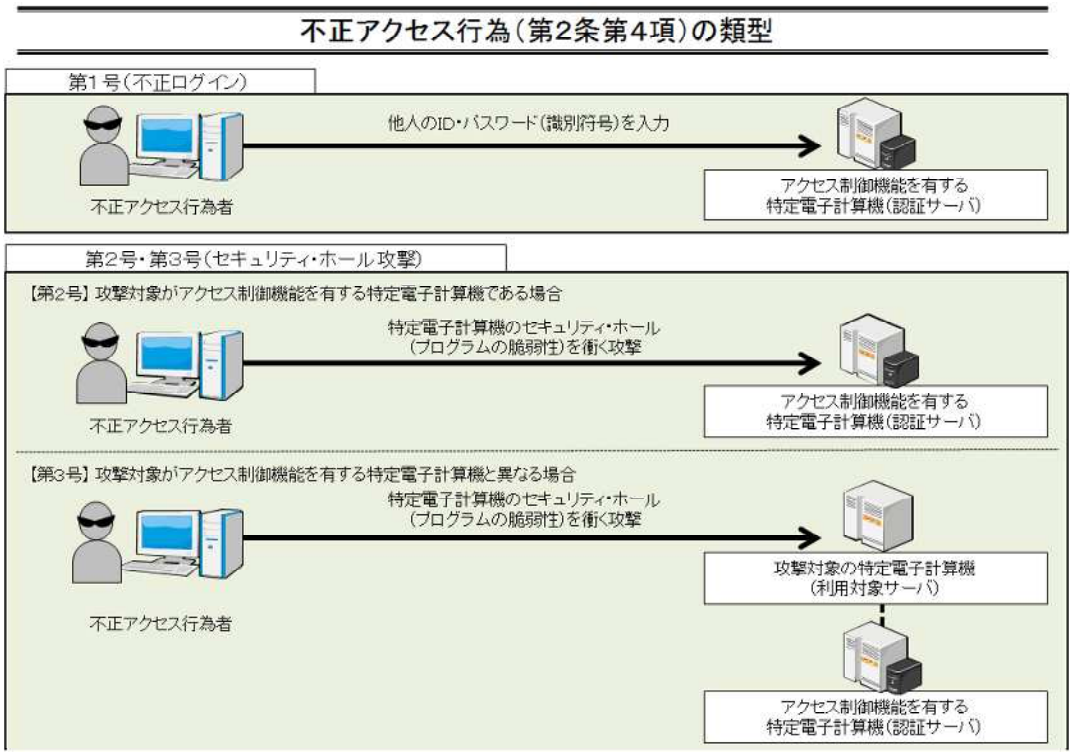
(2)　コンピュータプログラムの不備を衝く行為(第２条第４項第２号、第３号)

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２条第４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　他人の識別符号を不正に取得する行為の禁止、処罰(第４条、第12条第１号関係)

不正アクセス行為を禁止することの実効性を確保するため、平成24年の改正で、他人の識別符号を不正に取得する行為が新たに禁止対象となり、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。

この不正取得罪が成立するためには、他人の識別符号が「不正アクセス行為の用に供する目的」で取得されることが必要です。「不正アクセス行為の用に供する目的」とは、取得者自身に他人の識別符号を用いて不正アクセス行為を行う意図がある場合のほか、第三者に不正アクセス行為を行う意図がある場合に、そのことを認識しながら当該第三者に識別符号を提供する意図を持って取得する場合もこれに該当します。

「取得」とは、識別符号を自己の支配下に移す行為をいい、具体的には、識別符号が記載された紙や、識別符号が記録されたＵＳＢメモリ、ＩＣカード等の電磁的記録媒体を受け取る行為、自らが使用する通信端末機器の映像面に識別符号を表示させる行為、識別符号を知得する行為(再現可能な状態で記憶する行為)等が該当します。

なお、本罪が成立するには、取得者が取得することの認識を持つことが必要ですので、例えば、インターネット上での検索中にたまたま他人の識別符号が表示された場合や、他人の識別符号が電子メールで勝手に送りつけられてきたような場合には、取得することの認識がないことから、本条には違反しません。

５　不正アクセス行為を助長する行為の禁止、処罰(第５条、第12条第２号、第13条関係)

不正アクセス行為を禁止することの実効性を確保するため、平成24年の改正で、不正アクセス助長行為として規制されている他人の識別符号の提供範囲を拡張し、どの特定電子計算機の特定利用に係るものであるかが明らかでない識別符号を提供する行為が禁止・処罰の対象となり、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。

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、改正前は他人の識別符号を、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・処罰の対象としてきました。

しかし、近年、一人の人間が利用するコンピュータのサービスの数が増加しており、同一の識別符号を多数のサイトで使い回す例が一般化しています。その結果、提供された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が明らかでなくとも、多数の識別符号を入力すれば一定程度の割合で不正アクセスに成功する場合があることから、平成24年の改正により「業務その他正当な理由による場合」を除いて他人の識別符号を提供する行為が全て禁止されました。

「業務その他正当な理由による場合」とは、社会通念上、正当と認められるような場合をいいます。例えば、

- ○　情報セキュリティ事業者が、インターネット上に流出している識別符号のリストを契約している企業に提供する行為
- ○　インターネット上に流出している他人の識別符号を発見した者が、これを情報セキュリティ事業者や公的機関に届け出る行為
- ○　識別符号としてよく用いられている単純な文字列を、識別符号として設定すべきでないものとして示す行為

等は、不正アクセス行為を防止する目的で行われるものであり、「業務その他正当な理由による場合」に該当します。

また、

○　情報セキュリティに関するセミナーの資料等において、識別符号のインターネット上への流出実態を示すために実際に流出した識別符号のリストを掲載する行為

等も、流出実態の危険性を訴えることや対応策を検討することを目的に行われるものであるので「業務その他正当な理由による場合」に該当します。

従来、アクセス管理者がする場合又はアクセス管理者若しくは利用権者の承諾を得てする場合は、ただし書の規定により助長罪の適用除外となっていましたが、これらの行為についても、通常、「業務その他正当な理由による場合」に該当すると解されます。ただし、あるアクセス管理者が、他のアクセス管理者が管理するウェブサイトに対する不正アクセス行為に用いられることを知りながら自らが管理する識別符号を提供する識別符号を提供するような場合は、「業務その他正当な理由による場合」に該当するとはいえず、本条に違反することとなります。

本条が成立するには、提供者に提供することについての認識が必要であり、したがって、例えば、電子メールで送信したデータの中に他人の識別符号が含まれており、送信者がそのことを認識していなかったような場合には、提供することの故意がないことから、本条には違反しません。

６　他人の識別符号を不正に保管する行為の禁止、処罰(第６条、第12条第３号関係)

不正アクセス行為を禁止することの実効性を確保するため、平成24年の改正で、他人の識別符号を不正に取得する行為が新たに禁止対象となり、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。

この不正保管罪が成立するためには、「不正に取得された他人の識別符号」が「不正アクセス行為の用に供する目的」で保管されることが必要です。「不正アクセス行為の用に供する目的」の意義は不正取得罪と同様です。

「不正に取得された」とは、正当な権限なく取得されたことをいい、他人の識別符号の不正流通を防止するために保管罪を設けるという趣旨を踏まえ、処罰対象が不当に拡大することのないよう処罰対象を限定する趣旨で「不正に」との要件を規定したものです。これは、保管罪の対象となる識別符号の属性として「不正に取得された」ものであることを意味するものであり、保管者が保管の前提として取得した際の行為が不正であることを意味するものではあ

りません。「不正に取得された」識別符号とは、具体的には、第4条に該当する行為により取得された識別符号や第5条に該当する行為により提供された識別符号が該当しますが、これに限定さるものではありません。例えば、不正アクセス行為の用に供する目的以外の別の目的で他人の識別符号を正当な権限なく取得した場合、第4条の禁止対象とはなりませんが、当該識別符号を不正アクセス行為の用に供する目的で保管した場合には本条に該当することとなります。

「不正に取得された」との要件を付すことにより、アクセス管理者である企業の従業員が正当な権限に基づいて他人の識別符号を取得し、保管を行っている場合に、当該従業員が保管の途中で不正アクセス行為の用に供する目的を生じた場合のように、正当な権限に基づき他人の識別符号を取得し、保管を始めた者の内心の変化が生じたにすぎない場合については、本条の禁止対象から除外されることとなります。

識別符号の「保管」とは、有体物の所持に相当する行為であり、識別符号を自己の実力支配内に置いておくことをいいます。具体的には、識別符号が記載された紙や、識別符号が記録されたＵＳＢメモリ、ＩＣカード等の電磁的記録媒体を保有する行為、自らが使用する通信端末機器に識別符号を保存する行為、遠隔地にあるデータセンター等に保存する行為等がこれに該当します。

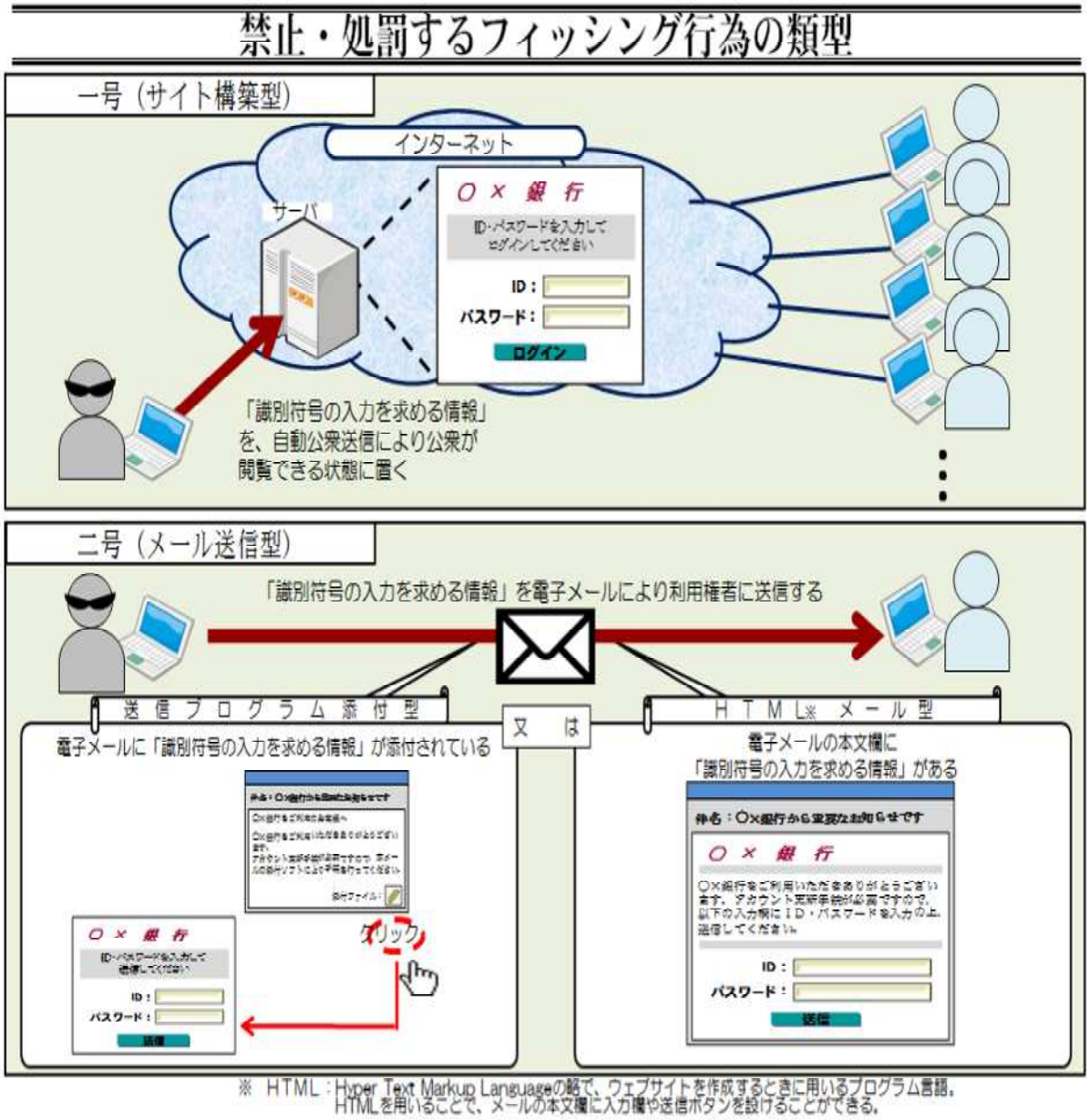
本罪が成立するには、保管者に、保管することの認識が必要であり、例えば、知らない間に他人の識別符号をダウンロードしていたような場合には、保管することの故意がないことから、本条には違反しません。

7　識別符号の入力を不正に要求する行為の禁止、処罰(第７条、第12条第４号関係)

本条は、いわゆるフィッシング行為を禁止する規定です。一般にフィッシングと呼ばれる行為は、その行為を詳細に見れば様々な形態のものがありますが、共通する特徴点は、アクセス管理者が公開したウェブサイト又はアクセス管理者が送信した電子メールであると利用権者に誤認させて、アクセス管理者がＩＤ・パスワードの入力を求める旨の情報を閲覧させようとすることにあります。そして、このような行為の結果、当該情報を閲覧した利用権者にＩＤ・パスワードを入力させてだまし取ることを企図しているものです。今回の改正で新たに禁止対象となり、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。

本条では、第１号が、いわゆるフィッシングサイトを公開することを手口とするフィッシング行為の、第２号が、いわゆるフィッシングサイトを用いず、電子メールによってＩＤ・パスワードを詐取しようとするフィッシング行為の禁止規定となってい

ます。



以下では、禁止・処罰の対象となるフィッシング行為について説明していきます。

○　第７条第１号(サイト構築型)

　第７条第１号は、フィッシングサイトを公開することを手口とするフィッシング行為を禁止している規定です。公開されたサイトが「正規のアクセス管理者が公開したウェブサイトであると誤認させるウェブサイト」であることが要件です。典型的にはアクセス管理者の名称や口ゴを用いているウェブサイトがこれに該当します。

　また、フィッシング行為は他人のＩＤ・パスワードを詐取するために用いられる手口ですから、当該サイトに「ＩＤ・パスワードを入力することを求める旨の

情報」があることが要件となっています。典型的にはウェブサイト上にＩＤ・パスワードを入力するよう求める文章、入力欄及び送信用のボタンが表示されている場合がこれに該当します。

　したがって、第７条第１号で規定している行為は、利用権者を誤認させようとする意図を持って、「正規のアクセス管理者が公開したウェブサイトであると誤認させるウェブサイト」であって「ＩＤ・パスワードを入力することを求める旨の情報」があるウェブサイトをネットワーク上に公開して公衆が見ることができる状態に置く行為ということになります。

○　第７条第２号(メール送信型)

　第７条第２号は、フィッシングサイトを用いず、電子メールによってＩＤ・パスワードを詐取しようとするフィッシング行為を禁止している規定ですので、送信された電子メールが「正規のアクセス管理者が送信した電子メールであると誤認させる電子メール」であることが要件です。典型的にはアクセス管理者の名称やロゴを用いている電子メールが該当します。

　また、第１号と同様に当該電子メールに「ＩＤ・パスワードを入力することを求める旨の情報」があることが要件となっています。典型的にはＨＴＭＬ(ＨＴＭＬとは、Hyper Text Markup Languageの略で、主にウェブサイトを作成するときに用いるプログラム言語です。ＨＴＭＬを用いることで、電子メールの本文欄に、ＩＤ・パスワードの入力欄や送信ボタンを設けることが可能となります。)を用いて電子メールの本文欄にＩＤ・パスワードを入力するよう求める文章、入力欄及び送信ボタンが表示されている場合や、これらの情報が表示されるプログラムが添付されている場合がこれに該当します。

　したがって、第７条第２号で規定している行為は、利用権者を誤認させようとする意図を持って、「正規のアクセス管理者が送信した電子メールであると誤認させる電子メール」であって「ＩＤ・パスワードを入力することを求める旨の情報」がある電子メールを、利用権者に送信する行為ということになります。

　実際に他人の識別符号を取得することは要件ではありませんが、行為者は、本条第１号又は第２号に該当する行為を、利用権者を誤認させようとする意図を持って行うことが必要です。したがって、例えば、

○　実際に発生したフィッシングの画面を、被害にあったアクセス管理者や情報セキュリティ事業者が注意喚起目的で公開する行為

○　ミラーサイトと呼ばれる、一つのウェブサイトにアクセスが集中してサーバ・コンピュータが過負荷になることを防止するために開設される元のウェブサイトのコピーサイトを公開する行為

○　アーカイブサイトと呼ばれる、ある時点のウェブサイトの画面を資料として保存することを目的とする元のウェブサイトのコピーサイトを公開する行為

○　ウェブ変換サービスと呼ばれる、あるウェブサイトの画面に振り仮名を付すなどのサービスにより元のウェブサイトから変換された後のウェブサイトを公開する行為

等は、そのウェブサイトの画面にたまたま元のアクセス管理者が識別符号の入力を求める旨の情報が表示されていたとしても、このようなウェブサイトを公開する者には、通常、元のウェブサイトの利用権者を誤認させようとする意図はないことから、本条による禁止の対象には含まれません。また、公開したウェブサイトが偶然ある既存のウェブサイトと似ており、既存のウェブサイトの利用権者が誤認してしまったような場合も、ウェブサイト公開者には、既存のウェブサイトの利用権者を誤認させようとする意図はないことから、本条には違反しません。

8　アクセス管理者による防御措置(第８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
○　ワンタイム・パスワードや指紋、暗号鍵等の他人に窃用されにくい識別符号の採用
○　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。

9　都道府県公安委員会による援助等(第９条、第10条関係)

(1)　都道府県公安委員会による援助(第９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、本法に基づく援助の対

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。

また、平成24年の改正で、都道府県公安委員会も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ることとなりました。

これは、従来から都道府県警察では、捜査を通じて蓄積した知見等を活用し、不正アクセス行為を始めとするサイバー犯罪を未然に防止し、国民の情報セキュリティに関する意識及び知識の向上を図るために、啓発及び知識の普及の活動を実施しているところであり、このような都道府県警察の活動が不正アクセス行為の防止に果たす役割の重要性に鑑み、本法において、都道府県公安委員会に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を図るべき責務があることを明記することとしたものです。

(2)　国による広報啓発活動(第10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、コンピュータ・ネットワークに関する技術の進歩に伴い不正アクセス行為の手口が巧妙化・深刻化していることから、アクセス管理者には、これに対応して防御措置を講じていく必要が生じており、結果的に、第１項に基づく一般的な情報の公表による援助では、第８条に規定する防御措置の責務の履行をアクセス管理者に期待するのは困難な状況が生じていました。アクセス管理者が不正アクセス行為の手口の巧妙化・深刻化という情勢の変化に対応して必要な防御措置を講じていくためには、アクセス管理者に対し、アクセス管理者が講ずるべき措置に関する情報の提供や、高度の専門的知識及び技術を有していないアクセス管理者でも容易に実

行可能な有効性検証ツールの開発や最新の手口にも対応したアクセス制御機能の高度化プログラムの提供などアクセス管理者の需要に応じた情報セキュリティサービスの提供がなされることが必要です。

そのための取組として、アクセス制御機能の高度化に係る事業を行っているセキュリティ事業者等が自発的に団体を組織し、情報セキュリティの向上のための活動を行っていることから、平成24年の改正により、国による新たな援助として、当該団体に対し、国家公安委員会、総務大臣及び経済産業大臣が必要な情報の提供その他の援助を行う規定が新設されました。これにより、アクセス管理者による防御措置向上の取組を促されることが期待されます。

必要な情報の提供その他の援助とは、具体的には、

○　国家公安委員会が、不正アクセス行為の具体的手口に関する最新の情報を提供すること

○　総務大臣が、総務省及び独立行政法人情報通信研究機構によるアクセス制御機能の高度化に資する研究開発の成果等の情報を提供すること

○　経済産業大臣が、独立行政法人情報処理推進機構を通じて不正アクセス行為に関する注意喚起を行うことやガイドライン策定等により対策情報を提供すること

等が考えられます。

援助先の団体としては、日本セキュリティオペレーション事業者協議会(ＩＳＯＧ－Ｊ)及びフィッシング対策協議会を想定しています(平成24年４月現在)。

ただし、当然これらの団体に限られるものではなく、第10条第２項に規定する要件を満たす団体には情報提供を行うことになります。団体の法人格の有無は問いませんが、本項の援助の対象となるのは事業者が集まって組織した団体であって、個々の企業や個人は援助の対象とはなりません(第２項)。

また、国はこれらのほかに、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３項)。