不正アクセス禁止法における不正アクセス行為の概念

田中　規久雄

一　はじめに
二　用語の概念と疑問点
三　不正アクセス行為の概念と疑問点
四　まとめ

一　はじめに

「不正アクセス行為の禁止等に関する法律」（以下、「不正アクセス禁止法」又は「本法」）は、国際的な動向もあり[1]、平成一一年八月一三日に公布、平成一二年二月一三日に施行された。（都道府県公安委員会による援助を除く。全面施行は同年七月。）これには、「個人情報保護法（平成一五年成立、平成一七年全面施行。）」や、平成一五年の所謂「住民基本台帳ネット」本格稼働（「住民基本台帳法の一部を改正する法律」平成一一年）といった国内事情も影響したものと思われる[2]。

「不正アクセス禁止法」第一条によると同法は、「高度情報通信社会の健全な発展に寄与することを目的」に、

「電気通信回線を通じて行われる電子計算機に係る犯罪[3]の防止」と「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」がその保護法益だとされている。実際、不正アクセスはコンピュータ・電磁的記録対象犯罪の前提としてなされる事が多く[4]、また不正アクセス禁止法以前は、業務妨害等に至らない様な、単なる不正アクセスは処罰されなかったため[5]、「不正アクセス行為の横行によりアクセス制御機能による利用権者の識別に対する社会的信頼が失われ、それが犯罪の抑止力を低下させる点に着目し[6]」、こうした保護法益を設定したものだとされる。

本法は、第三条第二項の三つの号で不正アクセス行為を定義し、同条第一項で、「何人も、不正アクセス行為をしてはならない。」と規定し、違反に対し第八条で罰則を定めている[7]。

しかし本法は、テクノロジーを対象に法規制を行う点で、条文理解そのものが難解であり、解釈が難しい。そこで本稿では、本法の核心的概念である「不正アクセス行為」に焦点をあて、その概念について検討する。以下まずそれら不正アクセス行為に関する条文の一般的解釈と若干の疑問点を概観する[8]。

二　用語の概念と疑問点

不正アクセス禁止法は不正アクセス行為を定義する第三条に先立ち、そこで用いられている用語の定義を第二条で行っている。以下、その概念とそれに対する疑問点を示す。

二―一　特定電子計算機

特定電子計算機とは、「電気通信回線に接続している電子計算機」をいう（第二条第一項）。「電気通信回線」とは代表的にはインターネットであるが、音声電話回線、専用回線、外部に繋がっていない社内ＬＡＮ（Local Area

Network）等も含まれ[9]、「電気通信が可能な状態に構成されている電子計算機をいう。現に電気通信を行っている状態にあるかどうかは問わない[10]。」とされるので、外部からのネット接続機能をソフト上一切停止しているといったＰＣであっても、「特定電子計算機」であると考えるべきであろう。たとえ外部からのアクセスを一切認めていなくとも、セキュリティホール攻撃等で不正アクセスされる物理的状態にある計算機は保護するのが法の趣旨に合致すると思われるからである。

「電子計算機」とは、コンピュータのことであるが、組み込み型の専用機も含まれるとされる[11]。ただし、電話回線を通じて留守番録音を外部から確認できる電話機は、「現状では、家庭にあるような電話機を電子計算機と評価することはできないと解する[12]。」とされ、どの様な基準で「電子計算機」であるかを切り分けるかは不正アクセス禁止法上明らかではない。一般的な理解でいえば、ＣＰＵとソフトウェアを備えた、ノイマン型のシステムは電子計算機という事になり、例えば、ＣＰＵをもつルーター、電子辞書、ＧＰＳ等も「電子計算機」にあたるであろう。また、ソフトウェアの機能が論理デバイス上物理的に実現されているものも同様である。直観的には単なるダムハブは電子計算機に当たらないように思えるが、条文上は定かではない。判例上も、著名事件であるＡＣＣＳ事件判決[13]では、「『電子計算機』とは自動的に演算や情報処理を行う電子装置である物理的な機器をいう」とするのでダムハブも不正アクセス禁止法上の「電子計算機」に該当する様にすら思える。

また、ネット上一台に見えれば一台なのか、逆に有体物として一台でも、エイリアスなどが設定されたり、物理的に複数のＬＡＮカードが接続されたり、極端には複数のＯＳが一つのＣＰＵで走っている場合等、ネット上からは複数に見える場合はどうなのか、またそもそも一台という概念が措定されているのか、条文からだけでは、特定電子計算機の具体的存在形態の定義はよくわからない。上記ＡＣＣＳ事件判決は、「レンタルしていた物理的な機

器である本件サーバが特定電子計算機」としているが、本件の事実はともかく、クラスターサーバーやクラウドコンピューティングの場合、物理的な一台を特定する事は難しく、ネット上の見かけで判断する他ない様に思われるし、「電気通信に関する秩序の維持」という本法の趣旨からもそう見るべきだと思われる。この事は意外に重要であって、例えばＡＣＣＳ事件判決の様に、一部にアクセス制御がかかっていれば、その一台はアクセス制御のある特定電子計算機であると直線的に判断される場合と、ネット上、例えばプロトコル（protocol）[14]やサービス毎に別の特定電子計算機と判断されるのでは、判断に大きな差が出てくるからである。[15]

二―二　特定利用

特定電子計算機の「利用（当該電気通信回線を通じて行うものに限る。）」とされる（第二条第一項）。

「利用」そのものの定義は条文上なされていないが、「電気通信回線を通じて行う情報処理の意味で『特定利用』の語を用いている。[16]」とされていることから、「利用」とは「情報処理」という事になるが、それによって定義が明らかになるわけではなく、解釈上の疑義が生じる。また、本法の保護法益は電気通信によるものに特定されており（第一条）、回線経由でない電子計算機の直接利用やスタンドアローンは本法の対象外である。これは、直接利用の場合、「入退室管理の徹底等の手段による利用の制限[17]」等の責任が優先されるからである。

「特定利用」としては、「具体的には、インターネットへの接続（ダイアルアップ・ルータの利用）、電子メールの受信（メールサーバの利用）、インターネット・ショッピングのためのホームページの閲覧（ＷＷＷサーバの利用）等がこれに当たる。[18]」とされる。

重要なのは後述のアクセス制御機能の利用自体は「特定利用」とされていない事である。条文上もあくまで、

「特定利用を自動的に制御するために…中略…付加されている機能」（第二条第三項、傍点筆者）とされており、「当然のことながら、利用対象サーバとは別にアクセス制御を有する認証サーバ等が設けられている場合は、他人の識別符号の入力先は認証サーバ等となるが、『特定利用をし得る状態』になる特定電子計算機は利用対象サーバである。[19]」とされている。立法論としては、アクセス制御機能の利用も特定利用に含めればどうかとも考えるが、その場合アクセス制御に限っては、不正アクセスの定義で「特定利用をし得る状態（本法第三条第二項）」ではなく、利用した事をもって不正アクセスとする必要はあるだろう。何故なら、アクセス制御機能を利用「し得る」状態を既に不正アクセスと捉えるなら、利用権のないサーバのログイン画面をネット経由で出しただけで不正アクセスとなってしまうからである。

二―三　アクセス管理者

特定電子計算機の特定利用につき「当該特定電子計算機の動作を管理する者」とされる（第二条第一項）。「特定電子計算機の『動作』とは、…中略…具体的には特定電子計算機による情報処理を[20]」指すとされるので、「動作」一般は、「情報処理」となり、先の「利用」と「動作」は、単に利用者側から捉えるか、管理者側から捉えるかの違いとなり、何れにせよ定義が明確なわけではない。

ただし、この「動作」はあくまで「特定電子計算機の特定利用」に対するものであり、ネット経由でない電子計算機の直接利用に対する動作について対象外としているのは、「利用」の場合と同じである。

次に「管理」とは、「一般に、財産、権利等についてその性質を変更しない範囲内での保存、利用、改良を目的とする行為をいう。本項における特定電子計算機の動作の『管理』もこの意味で用いている。[21]」とされ、本項にお

いては、「動作の管理の主たる内容は、誰に特定利用させるか（特定利用をさせる場合にはどの範囲とするか）を決定することを指す。前記の例でいえば、インターネットへの接続を誰に認めるか、電子メールの受信を誰に認めるか、ホームページの閲覧を誰に認めるか等がそれぞれ『管理』の具体的内容となる。[22]」とされ、その結果、「『アクセス管理者』とは、特定電子計算機を誰に特定利用させるか（特定利用をさせる場合にはどの範囲とするか）を決定する者を指す。[23]」とされる。なお、「許諾の方式は文書又は口頭、明示又は黙示を問わない。[24]」

しかし、「利用」の場合の例示が大まかなのはともかく、動作の管理の単位もその大まかな「利用」の括り毎にその全体に対して、「誰に」その特定利用を認めるだけかの様に解してはならない様に思われる。「誰にどの様な特定利用を認めるか」とは、例えば単純にプロトコルやサービス毎に一律に範囲が定まるわけではない。[25]同じメール利用でも、ある人には送信権限だけ与え、別の人には送受信双方の権限を与える、ＷＷＷでも特定の一部分は一部の人にのみ閲覧可能にする等様々な態様があり得る。

なお、ＩＳＰ（Internet Service Provider）とその契約利用者の様に、複数のアクセス管理者の存在が認められていること[26]から、アクセス管理者とは社会的に定まるものであり、プロトコルごとに異なるアクセス管理者がいたり、さらには同一プロトコルの中に複数のアクセス管理者がいたりすることもあり得る事となる。

二―四　利用権者

利用権者とは、「特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者」であり、これに当該アクセス管理者本人を加えて「利用権者等」とされる（第二条第二項、傍点筆者）。

「ホームページの公開のように、特定の者に限定せず、誰もが利用できるようにしている場合には、ネットワー

クに参加する全ての者にホームページの閲覧という特定利用を許諾している事となる。したがって、許諾した場合に必ず識別符号が付されるというものではない。[27]」とされる事から、アクセス制御のないＨＰ（Home Page, Web Page, ＷＷＷ）や匿名ＦＴＰ（anonymous FTP）等の場合は、アクセス制御がないことをもって万人が利用権者とされ、例えばアクセス制御はなされていないが「未成年閲覧禁止」との表示があるＨＰを未成年が閲覧しても、不正アクセスとはならないと考えられているが、アクセス制御をかけていないから万人が利用権者というのはあまりにも定義が曖昧過ぎる様に思われる。上記未成年の例も、当該未成年が「利用権者」であるからではなく、あくまでアクセス制御がないから不正アクセスにならないと考えるべきであろう。[28]

私見では利用権者の概念は社会的なものとして捉え、たとえアクセス制御がかかっていなくとも、アクセス管理者が利用を認めない者は非利用権者であるが、アクセス制御がかかっていない特定利用は単に不正アクセスとはならないだけだと考えるのが本法の趣旨に合致するように思われる。サーバも資産なのであって、どこかのマンションに物理的に誰でも駐車できる駐車場が有るからといって万人に駐車する権利があるわけではないのと同様、サーバの特定利用には本法もいうところの「許諾」が必要であろう。そしてアクセス制御がなければその許諾が万人に与えられていると捉えるのはあまりに素朴に過ぎる様に思われる。確かにインターネットはその根底に相互依存の精神があり、「できる事は許諾されている」と考えがちであるが、アクセス制御のないＨＰでも、例えば「許諾なしの閲覧を禁じます。」と書かれていれば、許諾されていない者は利用権者ではないのは明らかであろう。表示がないにしても、せめて社会通念上許諾が推認される程度の状態でなければ、利用権者とはいえないのではないだろうか。それ故、個人単位で秘密裏に運営されている場合等は、万人が利用権者とは考えるべきではないだろう。何らかの理由でそれを知った者がそこにアクセスしたとしても、それは単に事実上利用できただけであって、不正ア

クセスとはならないにしろ、利用権者として利用したと捉えるべきではないものと思われる。

二―五　識別符号

利用権者等に、「当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号」であって、第二条第二項の三つの号において定められている符号に、「該当するもの」又は、「該当する符号とその他の符号を組み合わせたもの」とされる（第二条第二項）。

具体的には、コンピュータを特定利用するためのＩＤ・パスワードが代表的であるが、キャッシュカードの口座番号と暗証番号の組み合わせ等もこれにあたる。[29]

先述の様に、アクセス管理者が行う「特定電子計算機の動作の管理」とは、「誰にどの様な特定利用を認めるか」という事であるので、これを技術的に制限するものが識別符号という事ができる。

また、当該特定電子計算機に利用権者が一人しかいない場合（通常はアクセス管理者）、そのＩＤ、パスワード等は、「利用権者等を他の利用権者等と区別して識別する」ものではないので識別符号ではないとされるので、[30]それらは「特定利用の制限を免れることができる情報」（第三条第二項第二号、第三号）に該当することとなろう。

また、この解釈でいえば、識別符号が不要なＷＷＷや匿名ＦＴＰを設置してはいるが、識別符号はアクセス管理者だけにしか設定されていない様な場合も同様に思われるが、「利用権者等は複数存在し、符号によりアクセス管理者を他の利用権者と区別して識別することができるから、当該ＩＤ・パスワードは識別符号に該当する。[31]」とされ、識別符号を持たない利用権者全般とアクセス管理者の二者を切り分けるだけでも識別符号とされるので、一人の利用権者に付された複数の識別符号も、複数の利用権者に付された同一の識別符号も当然本法における識別符号

に該当することとなろう。その点、「識別符号であるためには、複数の利用権者等に同一の符号が付されないようにするとともに、どの利用権者等に付されたものであるかが分かるように付されていることが必要となる。[32]」というのは、望ましいかもしれないが必須ではないし現実的でもない。「同一の部署に属する複数の者が利用を認められているようなＩＤ、いわゆるグループＩＤについては、その態様にもよるが、アクセス管理者の直接の許諾を得た代表者を利用権者と見るべき場合が多いと思われる。[33]」とされているし、実際、一部のゲームサイトの様に、現実個人を特定することなくＩＤ・パスワードが発行されることも多い。[34]

先述の如く、「利用権者」の概念は、あくまで社会的に定まるものなので、例えばある社員の識別符号は、その社員が退職等で利用権者とは認められなくなった段階で、たとえそれがシステム上に残っていても識別符号ではなくなる[35]とされる。一方、「他人のＩＤ・パスワードを探知した者が利用権者に無断でパスワードのみを変更したにすぎない場合は、当該ＩＤによる本来の利用権者等と他の利用権者とを区別して識別する機能はなお失われていないことから、当該ＩＤ・パスワードは識別符号に該当する。[36]」とされる。後者の識別符号にはあくまで「利用権者」がいるからである。

また、「『guest』、『anonymous』等の誰もが特定電子計算機を利用できるように広く公開されているＩＤ・パスワード、不正アクセス行為を行った者がアクセス管理者に無断で特定電子計算機のパスワードファイルに追加したＩＤ・パスワードは、利用権者等に付されていないものであるか、利用権者等を区別して識別できるようにすることを目的としていないものであるから、いずれも識別符号に該当しない。[37]」とされているが、先述の如く、識別符号なしに公開されているＷＷＷにおける、アクセス管理者の唯一のＩＤ・パスワードですら識別符号であるという観点からすれば、guest、anonymous 等も、他に同一の特定利用を行うための識別符号が設定されていれば、それ

らは利用権者を区別する識別符号となろう。もちろん、無断で付加されたものは利用権者に付加されたものではないので識別符号ではなく、「特定利用の制限を免れることができる情報」となる。

さて識別符号は、あくまでアクセス管理者が利用権者とした特定（の範囲）の者に与えられたものと解釈される。それ故、利用権者が他人名義や架空の名義で取得したものも識別符号とされ[38]、さらには一切の個人情報の求めなく、識別符号を自由に登録できる場合であっても、管理者がシステム上区別できる限りにおいて、そのＩＤ・パスワード等は識別符号となることになる。例えば、サーチエンジンを回避する等の理由で、ＨＰのアクセスに公開の識別符号を付したり、ワンタイムパスワードやセッションＩＤを採用したりしている場合にも識別符号は存在することとなる。また、ゲームサイトの様に、利用者に応じて特定利用のパラメータをそれぞれ変更保存できるようにする場合、一人の利用者がいくつもの識別符号を所持する事もありうる。すなわち、利用権者を区別するとは、事実上、アクセス管理者が識別符号を区別できさえすればよいのであって、個人等、現実存在の特定は不要だという事であるという事となる。それ故、利用権者の承諾のある、他人のＩＤ・パスワード等の使用が不正アクセス行為とはされないのであろうし[39]、また利用権者の承諾を受けた非利用権者がログインした後パスワードを書き換え、本来の利用権者に利用できなくした状態での特定利用も、他の違法はともかく、不正アクセス行為とはされないのではないかと考えられる[40]。

この識別符号については、簡単にいうと他人による所謂「なりすまし」が行われていない事を確認できるものとされ[41]、三つの号で定義されている。

第一号は「当該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」で、典型的には所謂ＩＤとパスワードである。ＩＤは社員番号や学籍番号等の場合もあり、必ずしも「みだり

に第三者に知らせてはならないもの」ではなく「その他の符号」に該当する場合もあるが、パスワードは通常「みだりに第三者に知らせてはならないもの」とされるため、双方で「該当する符号とその他の符号を組み合わせたもの」となり、たとえ同一のパスワードであっても、ＩＤとの組み合わせで識別符号となる。ただし、ＩＤの入力が不要で、パスワードのみでログインできるシステムでは、パスワードそのものが識別符号となり、また、必ずしも秘匿情報とはいえない社員番号や学籍番号がパスワードになっているシステムであっても、「社員番号がパスワードである」ことを、「当該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」場合は、識別符号たりえることとなる。[42] また、「アクセス管理者が利用権者等に対して第三者に知らせないように求める方法に限定はない。…中略…暗黙の了解によることも否定されていない。[43]」とされる。

第二号は、「当該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当該アクセス管理者が定める方法により作成される符号」とされる。例えば指紋、虹彩、網膜等によるものである。第三号は、「当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号」とされる。第二号、第三号の場合も、ＩＤ等「その他の符号を組み合わせたもの」も識別符号である。第二号、第三号の場合も計算機での内部処理は、第一号と同様である。

二―六　アクセス制御機能

後述の不正アクセス行為に共通するのが、「アクセス制御機能によって特定利用が制限されている特定電子計算機」のみが対象だという事であり、アクセス制御機能を有しない場合は、アクセス管理者が如何に特定利用を禁じていたとしても、他の違法はともかく、不正アクセス行為とはならないということで、「アクセス制御機能」は不

正アクセス禁止法のキー概念である（第二条第三項）。これは先述の如く、「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」（第一条）が保護法益であり、「アクセス制御に対する社会的信頼を確保する」のが立法趣旨とされる以上当然であろう。

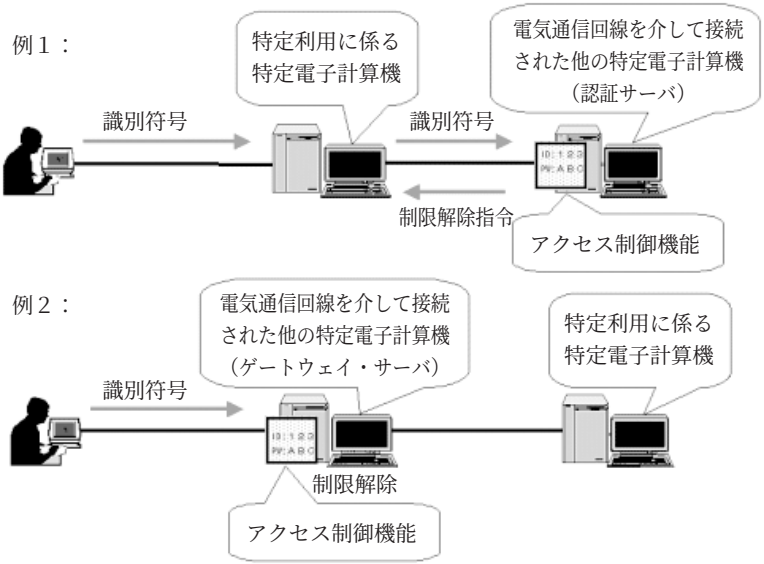
以上の事から、例えば、単に特定のＩＰ（Internet Protocol）やポート番号でアクセスを制限するパケットフィルタリングや、アプリケーションレベルゲートウェイ等は対象ではなく、あくまで「識別符号」を用いるアクセス制御がある場合のみが不正アクセス行為の対象とされている(44)。

条文上は、「特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該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。次条第二項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。」（第二条第三項）とされる。括弧内の「組み合わせた符号」には例えば暗号鍵により生成される符号等も含まれる。また、制限の「一部」とはプロトコル単位ではなく、読む事は公開されているが、書き込みにはアクセス制御がかかっている掲示板（ＢＢＳ）のような場合も含まれる(45)。

先述の如く、アクセス制御機能は「機能」であるので、たとえ誰にも識別情報が与えられていなくとも、アクセス制御機能が働いている場合はアクセス制御機能が存在すると解されるであろう。識別情報を確認するとは、すなわち識別情報でないものを確認することでもあるからである。例えば、ログイン画面が出るだけでユーザは誰も登録されていなくともセキュリティホール攻撃による不正アクセスは成立するという事となるが、逆にいえばネット

接続されていても外部からの特定利用はすべて停止されている場合、アクセス制御機能は付加されていない事となり、例えばウィルスによりバックドア（裏口）が作られても、他の違法はともかく、不正アクセスとはならない事となるが、こうした場合も立法論としては保護してはどうかと考える。

さて、「入力」とはネットを通じて、データを送信する事で、キーボードからの入力以外にも、ＩＣカードの挿入、スキャナ等の入力装置、電話機からの入力等があり、パソコンのインターネット接続ボタンを押すことまでが入力とされているが[46]、問題は、「当該機能を有する特定電子計算機に入力された」という文言の解釈である。前掲、警察庁「不正アクセス行為の禁止等に関する法律の概要」では、後述の本法第三条第二項の不正アクセスのパターン例として、下記の例１、例２を挙げているが、例１の認証サーバ方式の場合、この「当該機能を有する特定電子計算機」（認証サーバ）にデータが入力されるためには、ネットからの入力がまずは他の特定電子計算機になされ、その特定



電子計算機を経て認証サーバに到着するわけであるが、これを認証サーバに「入力された」と解していいかどうかである。

この点、第二条第三項は「当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（略）であることを確認して」（傍点筆者）と「入力」を定義していることから、例2の様にアクセス制御機能を有する特定電子計算機（アクセス制御機能とそれが制御する特定利用が一台の計算機に実装されている場合も当然含む）に対する直接入力は勿論、例1の様に、直接入力された特定電子計算機を経由して間接的に認証サーバ等に識別符号が到着している場合も、本法における「入力」であると解される。

先述の利用権者でなくなった者のＩＤ・パスワードやアクセス管理者に無断で付加されたＩＤ・パスワードが識別情報ではないとされる一方、プリペイドカードによるＩＳＰへのアクセスが、「識別符号の入力以外の方法による特定利用も…中略…、アクセス制御機能による制限をしていると評価することができる。[47]」とされ、アクセス制御は依然存在するとされる[48]のには注意を要する。

なお、クレジットカード番号やその有効期限は、「当該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」ではないとされ、それらの情報だけでアクセスできるシステムには、アクセス制御機能は存しないものとされ、他人のそれら情報の無断使用は、他の違法はともかく、不正アクセスとはされない[49]。

議論になるのは、所謂「隠しＵＲＬ（Uniform Resource Locator）」や「隠しフォルダ」といわれるものである。先述の如く、パスワードだけでも識別符号たり得る以上、暗号化ＵＲＬ等、例え単なるＵＲＬであってもパスワードと同様の機能を果たす場合もあるからである。しかし原則として、こうした場合にはアクセス制御がかかってい

るとはいえない。何故なら先述の如く、アクセス制御機能とは、特定利用を自動的に制御するために「付加されている機能」であって、ＵＲＬを入力しさえすればＨＰが表示されると言った場合、そこには付加された機能は存在しないからである。しかし、利用権者の所で述べたように、アクセス制御がかかっていないから万人に利用権があるとするのは早計であり、隠しＵＲＬや隠しフォルダは万人に利用権を与えていないというアクセス管理者の意思が推定されるので、そこに別のアクセス制御がかかっていれば、たとえアクセス制御がないアクセス方法を経たとしても、不正アクセスとなりうる場合があるものと考えられる。

アクセス制御のかかっていない特定利用の禁止に関しては、「識別符号を入力する以外の方法によっても識別符号を入力した場合と同じ特定利用ができるようになっていることをもって、直ちに識別符号の入力により特定利用の制限を解除する機能がアクセス制御機能に該当しなくなるものではないが、識別符号を入力してもしなくとも同じ特定利用ができ、アクセス管理者が当該特定利用を誰にでも認めているような場合には、アクセス制御機能による特定利用の『制限』はないものと解されることとなる。[50]」（傍点筆者）とされるので、逆にいえば、「アクセス禁止」が明示するなどされていれば勿論、index.html があり下位フォルダが参照できない等、実態としてアクセス禁止が推認されれば足りると思料する。

例えば、隠しフォルダの利用は識別符号を付したＦＴＰによって行う事をアクセス管理者が設定していた場合、たとえＨＴＴＰによるアクセスに制御がなかったとしても、そもそもアクセス管理者がその隠しフォルダについてはＨＴＴＰによる利用権者を認めず、ＦＴＰによるアクセス制御を経て利用するための識別符号を与えられた者だけが利用権者と設定しているなら、アクセス制御がないからといって、そもそも利用権者でない者が利用して良いものではなく、ＨＴＴＰによるアクセスは不正アクセスと考えて良いものと思われる。これは前記ＡＣＣＳ事件判

決と同様の結論で、法一般の性質として、その概念は社会的構成物なのであって、技術的に可能であっても、アクセス管理者が想定していないような特定利用は、技術的にできるからといって行なってもいいという事ではないと考える点において共通している。その意味で、本法の趣旨から、例えば設定ミス、セキュリティホール等により、アクセス管理者が設定する以外の「当該特定利用の制限の全部又は一部を解除する」方法があったとしても、アクセス管理者が設定した制限は依然、「制限」とされているのも同旨であろう[51]。

同様に、例えばアクセス制御があり、ＩＤとパスワードを入力すると、特定のＵＲＬに遷移しＨＰが閲覧できるが、そのＨＰのＵＲＬ自体にはアクセス制御がかかっておらず（隠しＵＲＬ）、そのＵＲＬを直接入力すればアクセス制御を経ずに閲覧できるといった場合、アクセス制御のないＵＲＬの直接入力によるＨＰの閲覧は「特定利用の制限を免れることができる情報又は指令の入力」として不正アクセスたりえる。すなわち、アクセス制御を経ない特定利用は万人が利用権者であるとの理解を前提とし、その方法を用いる事はアクセス制御を有する特定電子計算機の利用とはならないと一律に考えるべきではなく、アクセス制御のないＵＲＬを設定することが、先述の「識別符号を入力してもしなくとも同じ特定利用ができ、アクセス管理者が当該特定利用を誰にでも認めているような場合」と推認されるのかどうかが解釈の分かれ目となるように思われる。先述の如く、私見ではアクセス制御のない特定利用に対しては万人が利用権者と考えるのではなく、たとえアクセス制御のない特定利用が可能でもその利用は禁止して、アクセス制御を経てその利用を行うようにアクセス管理者が設定しているなら、アクセス制御のない側の特定利用を行なう事もアクセス制御を免れる行為に該当する場合があると解する。

また、例えば社屋内等、一定範囲のＩＰからの特定利用にはアクセス制御がないが、外部からのアクセスにはパスワードなどのアクセス制御がある場合（典型的にはＶＰＮ[52]等）、内部端末からのアクセスには「建物の入退室管

理等による制限[53]」があり、全体としてアクセス制御があるものとされるので、「アクセス管理者が当該特定利用を誰にでも認めているような場合」は社屋に入っただけで利用権者となり、反対に来客には利用権を認めていない場合には、アクセス制御をかけていない社屋内の端末からの特定利用であっても不正アクセスとなる事もあろう。同様に、同一のＨＰの閲覧に対して、どちらも外部からはアクセスできるが、社員だけにはアクセス制御のないＵＲＬを教え、外部にはアクセス制御のあるＵＲＬを公開している場合、外部の人間がアクセス制御のないＵＲＬにアクセスした場合、不正アクセスとなる事もあるだろう。

以上の様に、同一の特定利用に対してアクセス制御がある場合とない場合で、ない方を使うと不正アクセスになるのかどうかは、結局のところアクセス管理者の利用権者の設定をどう社会的に捉えるかに依存しているといえる。[54]

なお、ＡＣＣＳ事件ではアクセス制御なしのＷＷＷであっても、なされた特定利用は本来ＦＴＰで行われることが前提で、そのＦＴＰにアクセス制御がかかっていたので不正アクセスが成立したが、もしＷＷＷのアクセスにはアクセス制御をかけずだれでも利用可能にしておき、その書き換え等の管理はネットからではなく、コンソール（本体のキーボード）からの当該コンピュータの直接利用でのみ行っており、他にはそのサーバに何らのアクセス制御もなされていなかった場合はどうであろうか。セキュリティの為に、ネットを用いるのはアクセス制御のないＷＷＷだけでその他の利用はすべて本体で直接行うというのはありうる事であるが、そうした場合は当該特定電子計算機にはアクセス制御がかかっていない事になり、ＨＴＴＰによる隠しフォルダの閲覧も不正アクセスとはならないこととなる。

三　不正アクセス行為の概念と疑問点

本法は第三条第一項で禁止されるところの「不正アクセス行為」について、第三条第二項の三つの号で定義している。第一号、第二号はアクセス制御機能を有する特定電子計算機に対して、第三号は他の特定電子計算機（ゲートウェイサーバや認証サーバ）によってアクセス制御がなされている利用対象の特定電子計算機に対して、利用権者をよそおう「他人の識別符号」の使用（なりすまし）や、利用権者を識別できなくする「特定利用の制限を免れることができる情報（識別符号を除く。）又は指令」の使用（セキュリティホール攻撃）により、対象特定電子計算機の特定利用をし得る状態にすることを不正アクセスと定義している。[55] それ故、先述の如くアクセス制御機能がない場合はそもそも不正アクセスが成立しない。[56]

本条で「不正アクセス行為」共通の要件とされているのは、要は各号に該当する方法で、アクセス制御機能によって「制限されている特定利用をし得る状態にさせる行為」であるが、先述の如くアクセス制御機能そのものは特定利用に「付加されている機能であって」特定利用そのものではないので、例えばＩＤとパスワードの入力画面にアクセスしても、当然のことながら特定利用したことにならない。途中で本当にログインしてよいかの確認画面が出ている段階もまだ特定利用し得る状態ではない。また、「通常は、他人のＩＤ・パスワードを正しく入力しさえすれば、途中で回線が切断されるようなことがない限り自動的に処理されて利用できる状態になるため、実質的には、他人のＩＤ・パスワードを入力する行為が禁止されることとなる。[57]」（傍点筆者）とされていることから、逆に言えば、たとえ他人のＩＤ・パスワードを入力しても利用対象のコンピュータが「利用できる状態」にならなければ不正アクセスとはならない事となる。すなわち、アクセス制御を破っても、特定利用し得る状態にできる電子

計算機がなかった場合も不正アクセスとはならない事になる。例えばＶＰＮサーバを破って社内ＬＡＮに侵入したとしても、メンテナンスやシャットダウンにより特定利用できる電子計算機がＬＡＮ内になかったり、ＬＡＮ内の計算機個別にすべて個別にアクセス制御がかかっていた場合は、不正アクセスとはならない訳である。[58] なお、単に「特定利用し得る状態」を超えて特定利用にまで至ってしまった場合は、「特定利用し得る状態」を経て特定利用したものと評価される。[59]

各号とも当該アクセス管理者自らが行なう場合、第一号に関してはアクセス管理者又は利用権者の承諾がある場合、第二号、第三号に関しては、アクセス管理者の承諾がある場合は、不正アクセス行為から除外されている。すなわち上位のアクセス管理者に許諾された下位のアクセス管理者、利用権者の特定利用につき、上位のアクセス管理者が下位のアクセス管理者や利用権者になりすましてその特定利用を行う事は不正アクセスではない。逆にいうと、ある特定利用、例えば同一の記憶領域の共有を許諾された正規の利用権者であっても、その特定利用に対する他の利用権者の識別符号を無断使用することや、識別符号以外の特定利用の制限を免れることができる情報又は指令でその特定利用を行なうのは不正アクセス行為であるという事となるが当然であろう。なお第一号で、アクセス管理者だけでなく、利用権者自体の承諾があれば他人の識別情報を使用しても不正アクセスにならない事になっているのは、アクセス管理者の主観的意図や利用契約によって犯罪の成否に差がつかない様にするためだとされる。[60] 例えば、企業や学校でパスワードの貸し借りが禁じられている場合であっても、懲戒や民事責任はともかく、不正アクセスとして罰せられることはないという事である。ただこうした承諾は識別符号等の情報や指令を「入力」する度に求められるのか、包括的な承諾も許されるのか条文上は定かではないが、現実的に考えて包括的な承諾をもって足りるであろう。

三―一　アクセス制御機能を有する特定電子計算機に対する他人の識別符号の無断入力

第一号は、「アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）」とされる。

アクセス制御機能が、「特定電子計算機の特定利用を自動的に制御するために…中略…当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（略）であることを確認」（第二条第三項、傍点筆者）するものであるとされ、「当該機能を有する特定電子計算機」が「当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能」（同条同項）である以上、先述の如く、他人の識別符号の無断入力は、アクセス制御機能と利用対象の特定利用機能が一台の計算機に実装されている場合はその計算機に対して、またアクセス制御機能のない利用対象計算機と、それに対しアクセス制御機能を付加している計算機がある場合はアクセス制御機能のある方の計算機に対して、何らかの経路で他人の識別符号が到着し、その制御下にあるいずれかの特定電子計算機の特定利用が可能になった段階で本号の対象となる。

三―二　アクセス制御機能を有する特定電子計算機に対するセキュリティホール攻撃

第二号は「アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該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（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を

作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）」とされる。

アクセス制御機能と利用対象の特定利用機能が一台の計算機に実装されている場合はその計算機に対して、またアクセス制御機能のない利用対象計算機と、それに対しアクセス制御機能を付加している計算機がある場合はアクセス制御機能のある方の計算機に対して、何らかの経路で他人の識別符号が到着し、その制御下にあるいずれかの特定電子計算機の特定利用が可能になった段階で本号の対象となるのは第一号と同様である。

「特定利用の制限を免れることができる情報（識別符号であるものを除く。）」と括弧書きで識別符号を除いているのは、第一号で既に他人の識別符号を用いた不正アクセスを既に規定しているからである。

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、「指令」とは電子計算機に一定の動作をさせるコマンドの意味とされるが、「両者を区別して論じる実益はない」[61]とされる。

さて、識別符号を除いた「当該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」する行為とは、一般的に設定の不備やシステムの脆弱性を突く「セキュリティホール攻撃」が典型であるが、必ずしもこれに限られるものではなく、利用権がなくなった退職社員の残留するＩＤ・パスワードは「識別符号」ではないとされるので（先述）、これを用いたアクセスは本項の「情報又は指令」と解される事となる。[62]識別符号の位置づけはアクセス管理者が定めるものであるので、利用権を取り消された者のＩＤ・パスワードによるアクセスは「誰によるものか識別できないアクセス」という事となるのである。

純然たるセキュリティホール攻撃の一例である「sendmail 攻撃（メールサーバのバグを利用してパスワードを書き換え又は追加等を行う。）」については、その攻撃メールが受信され「ファイルが書き換えられた段階で不正ア

クセス行為となる。[63]」とされるが、それによって作成されたＩＤやパスワードが「アクセス制御機能を有する特定電子計算機」に入力されてログインされた段階で初めて「制限されている特定利用をし得る状態にさせ」た事になるのであって、メール機能の利用にアクセス制御がなされておりそれを破って攻撃したのならともかく、「ファイルが書き換えられた段階で」、「制限されている特定利用をし得る状態にさせ」たとはいえないであろう。

三―三　別の特定電子計算機がアクセス制御機能を有している利用対象計算機に対するセキュリティホール攻撃

特定利用し得る状態にされる特定電子計算機（利用対象計算機）に接続された他の特定電子計算機がアクセス制御機能を持っている場合の第三号の条文は、「電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為」である。これは、第一号第二号の様に、アクセス制御機能を有する計算機に情報等が入力されることが要件であると、アクセス制御をかけている認証サーバ等には情報等の入力をしないまま、利用対象計算機のみを攻撃し、その計算機に不正アクセスするというパターンが規制できないために規定されているものである。[64]従って利用対象計算機のみのクラックが対象となっている。ただし、第二号と異なり、「（識別符号であるものを除く。）」との括弧書きはなく、また第二号の「（識別符号であるものを除く。）」の括弧書きの中に「次号において同じ」との付記もないため、第三号の「制限を免れることができる情報」には他人の識別符号を含むものと解されるが、この点『逐条』では、「第二号と第三号はいずれも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（識別符号を除く）又は指令を入力する不正アクセス行為について規定している[65]」と、第二号の場合と同様、識別

符号を含まないものとしている。これは、「利用対象サーバとは別にアクセス制御機能を付加された特定電子計算機（認証サーバ等）が設置されている場合、組合せとしては、他人の識別符号が利用対象サーバを経由して認証サーバ等に入力され、認証サーバが作動して利用対象サーバの特定利用ができるようになる場合があるが、この場合、他人の識別符号は結局のところ認証サーバ等に入力されていると評価することができる。したがって、他人の識別符号の無断入力については、セキュリティ・ホール攻撃についての第三号に相当する入力先に係る規定を設ける必要がない。[66]」すなわちそうした場合は第一号の対象であるとの理解に基づいている。

また、第二条第三項の識別符号に対する括弧書きにおいては、「次条第二項第一号及び第二号において同じ。」とされ、第三条第二項第三号には言及されていない事も、第三号にいう「情報」に「識別符号」が含まれていない印象を与えるが、それは単に第三条第二項第一号及び第二号には明示的に「識別符号」の語が現れ、第三号には現れないために過ぎないからだと思われる。

しかし以上の様に考えたとしても、実際は「他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機」だけに識別符号を入力して、その計算機自体を作動させるというのはあり得ない。それ故、「制限を免れることができる情報」に識別情報が入っていてもいなくとも結果は同じである。ただ文言上は第三号の「制限を免れることができる情報」には形式的には識別情報が含まれると解すべきではあろう。いずれにしろ、第一号、第二号は、利用対象計算機以外の計算機（Aとする）からアクセス制御機能を有するサーバにアクセスして、その制限を外し、その結果アクセスできるようになる計算機がA以外のものであって良いのに対し、第三号では、必ず利用対象計算機にアクセス制御を免れる情報を入力し、直にその計算機を特定利用可能にすることが要件となっている事には注意を要する。

四　まとめ

最後に不正アクセス概念をまとめておこう。

簡単にいうと、不正アクセスが成立するためには、ネットから入力される情報が「他人の識別情報」または「セキュリティホール攻撃情報」であり、入力先は、「アクセス制御を有する計算機」または「別の計算機によってアクセス制御されている計算機」であって、結果としてアクセス制御されている特定電子計算機が利用できる状態になればよい。この組み合わせは四パターンあるが（一つには意味がない。先述。）、其々本法第三条第二項の各号の何れに該当するかを示す。

㈠「アクセス制御を有する計算機」に「他人の識別情報」を入力する場合――第一号

㈡「アクセス制御を有する計算機」に「セキュリティホール攻撃情報」を入力する場合――第二号

㈢「別の計算機によってアクセス制御されている計算機」自体に「セキュリティホール攻撃情報」を入力する場合――第三号

適用上の解釈問題として大きな事は、同様の特定利用に対して「アクセス制御」がかかったアクセス方法とかかっていないアクセス方法があった場合、どの様な要件事実をもって、どの様な特定利用にアクセス制御があると判断するのか、あるいはアクセス制御がかかっていないアクセス方法でのアクセスにはアクセス制御がないとするのかである。私見では先述の如く、アクセス管理者の設定する利用権の範囲が一つの大きな目安になるものと考える。

その他、疑問の提示にとどまった問題がほとんどであるが今後の課題としたい。また法益論や罪数論、可罰的違

法性といった刑事法的に純理論的な問題は筆者の手の及ぶところではないので対象とせず、技術と法の関わりで条文の文理解釈を扱った点はご容赦頂きたい。

（1）例えば一九八六年ＯＥＣＤ「コンピュータ犯罪――立法政策の分析」以降の各国の不正アクセスの犯罪化や、二〇〇一年、欧州評議会（Council of Europe）「サイバー犯罪条約（Cybercrime Convention）」（二〇〇四年、日本批准）等。山口厚「サイバー犯罪条約の実体法的意義」法とコンピュータNo.21、二〇〇三年、五二―五五頁参照。

（2）「第四五回国会衆議院・地方行政委員会議録」第二〇号、一九九九年、三四〇頁参照。

（3）「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、「①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電磁的記録不正作出罪、電子計算機損壊等業務妨害罪、電子計算機使用詐欺罪等、②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薬物事犯、詐欺事犯、わいせつ事犯等（電子掲示板やホームページを利用したもの等）を指す。」とされる。（不正アクセス対策法制研究会編著『逐条・不正アクセス行為の禁止に関する法律［補訂第二版］』立花書房、二〇〇八年、二八頁。以下本書を『逐条』と略す。）

警察庁の広報資料「平成二一年中のサイバー犯罪の検挙状況等について（平成二二年三月）」（http://www.npa.go.jp/cyber/statics/backup/h21/pdf01.pdf）では、前者を「コンピュータ・電磁的記録対象犯罪」、後者を「ネットワーク利用犯罪」とし、これに「不正アクセス禁止法違反」自体を加えて「サイバー犯罪（情報技術を利用する犯罪）」と呼んでいる。本資料によると、不正アクセス禁止法違反による検挙件数は、平成一七年から二一年で、二七七、七〇三、一四四二、一七四〇、二五三四件と急速に増加している。

なお、以下、「電気通信回線」ないし「電気通信」を「ネット」等と、「電子計算機」を「コンピュータ」、「ＰＣ」、「サーバ」等と表記する場合がある。

（4）ただし、あくまでアクセス制御に対する社会的信頼を確保するために、「不正アクセス行為」自体を処罰するもので、予備罪として構成されるものではない。すなわち、他の犯罪の手段かどうかとは無関係である。「平成一一年六月二四日、第一四五国会衆議院地方行政委員会政府委員（小林奉文警察庁生活安全局長）答弁」参照。しかし、こうした立法方針は「場当たり的で、しかも立法の動機が回顧的で、過去の事象への対処におわっており、将来的な展望あるいは横断的な立

法ポリシーが欠如しているように思われる。」との批判もある。（石井徹哉「W．ベール『電気通信に対する刑事訴訟的侵害に際して生じる諸問題の現状』」早稲田法学七七巻二号、二〇〇二年、二九九頁。）

(5) 浜田良樹「不正アクセス法制とインターネット」情報処理学会研究報告、ＥＩＰ『電子化知的財産・社会基盤』九八（五二）、一九九八年、三九―四七頁参照。

(6) 『逐条』二九頁。

(7) 所謂自然犯規制の起案ではなく、行政犯規制の起案がなされており、刑法の様に条文内には罰則を定めていない。これは、「前法律的に反規範性を有する行為とまではいえない」からだとされる（同六八頁）。

(8) 以下基本的に、警察実務上の実際的な参照文献である前掲『逐条』、ならびに、警察庁「不正アクセス行為の禁止等に関する法律の概要」（http://www.npa.go.jp/cyber/legislation/gaiyou/gaiyou.htm）による。

(9) 電気通信事業法第九条、第三三条第一項参照。

(10) 『逐条』三四頁。

(11) 同八頁参照。

(12) 同八四頁。

(13) 東京地判平成一七年三月二五日。

(14) ＷＷＷのためのＨＴＴＰ、ファイル送受信のためのＦＴＰ等、特定利用のための通信規約。

(15) 高木浩光「不正アクセス行為の２つの文理解釈について」情報ネットワーク・ローレビュー第５巻、二〇〇六年、三九頁、園田寿「不正アクセス禁止法における『不正アクセス』の概念」甲南法務研究一号、二〇〇五年、一一〇―一一三頁、成瀬幸典「不正アクセス罪についての一考察」『刑事法学の現代的課題』第一法規、二〇〇四年、三六七頁参照。

(16) 『逐条』三四頁。

(17) 同七四頁。

(18) 同三四―三五頁。

(19) 同七七頁。同七九頁参照。

(20) 同三五頁。

(21) 同上。
(22) 同上。
(23) 同上。
(24) 同三九頁。
(25) 前記ＡＣＣＳ事件判決参照。
(26) 『逐条』三六頁。
(27) 同三九頁。
(28) 諸外国では不正アクセスを「無権限（原）アクセス」(Unauthorized Access) と捉えている場合が多い。See, Computer Misuse Act 1990, U.K., § 1, 加藤敏幸「不正アクセス」刑法雑誌四一巻一号、二〇〇二年、八一―八三頁参照。
(29) 『逐条』八三頁。
(30) 同四〇―四一頁。
(31) 同四一頁。
(32) 同四〇頁。
(33) 同三九頁。
(34) 前掲、成瀬、三七四頁注二八参照。
(35) 『逐条』四〇頁。
(36) 同四一頁。
(37) 同上。
(38) 同七四頁。
(39) 同八二頁、本法第三条第二項参照。
(40) 大阪高判平成一九年三月二七日参照。
(41) 『逐条』四二頁参照。
(42) 同四三―四四頁参照。

(43) 同四四頁。
(44) 同四七頁。
(45) 同五五、六三頁注一参照。
(46) 同五四、七五、七六、八〇頁参照。
(47) 同上。
(48) 同六一頁。
(49) 同六二頁参照。
(50) 同五九頁。
(51) 同九頁参照。
(52) Virtual Private Network. 社内ＬＡＮに外部から接続し、その外部ＰＣに社内ＬＡＮ内のＩＰやアドレスを付与して、社内ＬＡＮ内にあるように見せかける機能。
(53) 『逐条』六〇頁。
(54) 勿論、アクセス管理者の主観ではなく、一定の社会的客観性は必要である。石井徹哉「不正アクセス禁止法の意義と限界」千葉大学法学論集一九巻三号、二〇〇四年、二九―三〇頁、大橋充直「検証ハイテク犯罪の捜査（第四七回）」捜査研究六四七号、二〇〇五年、八一頁注八、高橋郁夫「脆弱性にかかわる法的側面について」情報処理四六巻六号、二〇〇五年、六五八―六五九頁参照。
(55) 『逐条』六九頁参照。
(56) 同六七頁、前記ＡＣＣＳ事件判決参照。
(57) 『逐条』七一頁注三。
(58) 東京地判平成二一年一一月一二日や前掲、大阪高判平成一九年三月二七日等の様に、少なくともアクセス制御の一つである認証サーバそのものに対する不正アクセスは観念されていない。
(59) 『逐条』七七、八〇頁参照。
(60) 同八二頁参照

(61) 同七九頁。以下、「情報」と包括的に表記する（識別情報を含む）。
(62) 前掲、東京地判平成二一年一一月一二日参照。
(63) 『逐条』七一頁注三。
(64) 同七八頁。
(65) 同上。
(66) 同七三頁。