論　説

不正アクセス行為概念再考

田中規久雄

一　はじめに

前稿[1]より一〇年程経ち、この間、衆参両院へのサイバー攻撃（平二三年）[2]、一般的にはフィッシング（Phish-

ing）詐欺[3]による不正送金[4]の激増等の社会的変化があり[5]、平成二四年、不正アクセス禁止法が大改正された。

不正アクセス行為概念に関連する改正の要点は、所謂「不正アクセス準備行為」の処罰化を中心とした下記の通りである（罰則は一一～一三条[6]）。

・フィッシングの処罰化（七条）。
・他人の識別符号提供の処罰範囲の拡大と重罰化（一二条）。
・他人の識別符号の不正取得、不正管理の処罰化（四条、六条）。
・不正アクセス行為自体の重罰化（一一条）。

しかし残念ながらと言うべきか、不正アクセス行為概念の定義は、平成二四年改正後も、条数が三条二項から二条四項に移動しただけで、文言は平成一一年制定当時と同一である。

以下、条文を示す。

［二条四項］

この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

一　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。）

二　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。）

三　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

二　審議過程での解釈

本条は、起案関係者自身が「お世辞にも平易でわかりやすい条文とは言い難い」[7]と自白しており、審議過程においても複雑で意味が取れないと指摘されているが、その審議過程を見てみよう[8]。

若干冗長になるが原文を引用する。

○大野元裕君　…略…　私、この改正案の条文を読ませていただいて、よく分からないというのが正直なところであります。条文の第二条の四におきましては、不正アクセス行為の定義が述べられています。その第一項について、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路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、これ、つまり、インターネット等を通じてパスワードが掛かっているコンピューターに対して不正にＩ

D、パスワードを入れて作動をさせる、こういうことだろうと私は理解をいたしました。

ここまではまだ私の平々凡々とした頭でも付いていけたんですけれども、二号と三号が正直幾ら読んでも分かりませんでした。

二号について言うと、アクセス制御機能を有する特定電子計算機、パスワードの掛かっているコンピューターに電気通信回路、つまり、インターネット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と。セキュリティ・ホールのことだろうと私は思っておりました。

三号なんですが、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路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。

これ、二と三の違いを含めて、大臣、御理解できますでしょうか。

○国務大臣（松原仁君）　大変に複雑な文章でありまして、大野委員の理解は非常に明快なものであるというふうにも承知をしているわけでありますが、二号と三号の違いというのは、いわゆる攻撃者、不正アクセス行為者がいて、攻撃対象の電子計算機に攻撃をして、その別の電子計算機に対しての影響を行使して犯罪を行うと、こういうことだろうと思っておりますが、…略…文言で書くと非常に難しいというふうに思っておりまして、法律用語ですから極めて難しいというのは仕方ないわけでありますが、このことをやはりどのように周知徹底させるかということに非常に気を配るということが我々としては大事だろうというふうな思いを致したところであります。

○大野元裕君　おっしゃるとおりだと私も思っておりまして、実は御説明に来ていただいて私なりに理解をして、

配っていただいた資料が添付している資料でございまして、縦長の方なんですが、第一号は、他人のＩＤやパスワード、識別符号を入れることによってインターネットを通じてどこかのコンピューターを使う。この一番上の図のところは私も理解はできたんですが、第二号と第三号の条文を読むだけでは私は想像すら付かず、二十分ぐらいいろいろと御説明をしていただいて、絵を見てやっと分かったというのが状況でございまして、大臣が先ほど実際にやってみて実感したというのもまさにそのとおりだろうと思っています。

第二号は、要するに不正アクセス行為者がセキュリティ・ホールをつく形で特定のコンピューターを動かすと、第三号は、別なところでセキュリティーを掛けているコンピューターがある中でインターネットを通じてセキュリティ・ホールをつくと、こういう行為だというのがやっと私も理解をした次第でございます。

以上の議論を見る限り、何らかの方法で他人の識別符号（代表的にはＩＤとパスワード）を用いてログインする所謂「なりすまし」は二号、三号の対象とは認識されていない。

三　警察庁の見解

現行の法執行において、警察庁の解釈が基準となるのは否めない。以下その要点を示す（傍線筆者）[9]。

三　不正アクセス行為の禁止、処罰（第二条第四項、第三条、第一一条関係）

不正アクセス行為とは、他人の識別符号を悪用したり（第二条第四項第一号）、コンピュータ・プログラムの不備を衝く（第二条第四項第二号、第三号）ことにより、本来アクセスする権限のないコンピューターを利用する行

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、三年以下の懲役又は一〇〇万円以下の罰金に処せられることとなっています（第一一条）。

（一）他人の識別符号を悪用する行為（第二条第四項第一号）

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ーを利用する行為、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、コンピューターのセキュリティ・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。

（二）コンピュータ・プログラムの不備を衝く行為（第二条第四項第二号、第三号）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二条第四項第二号及び第三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、この二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、コンピューターのセキュリティ・チェックを行う場合など。）が考えられるためです。

…図略…

不正アクセス行為には以上の二類型がありますが、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ー（ネットワークに接続されていないコンピューター）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ーであっても当該コンピューターのキーボード（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ー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ーである必要はなく、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ー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。

次頁に、上記解説を図示したものを示す。(10)

四　考察

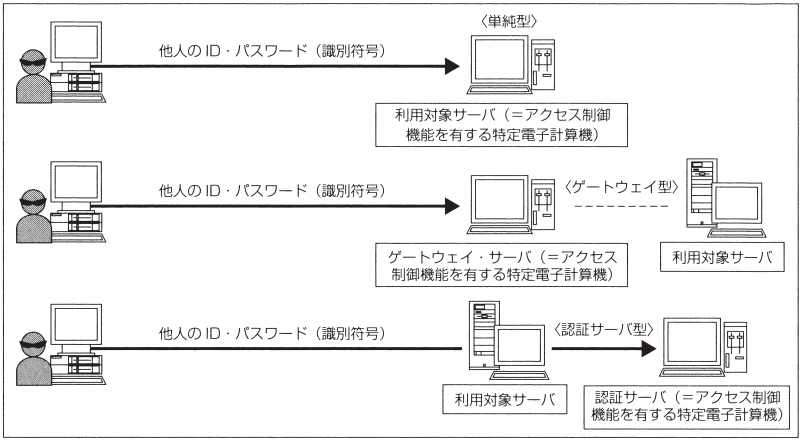
以下、大いに立法論となるが、現行の不正アクセス禁止法における不正アクセス概念について考察する。

四―一　設例

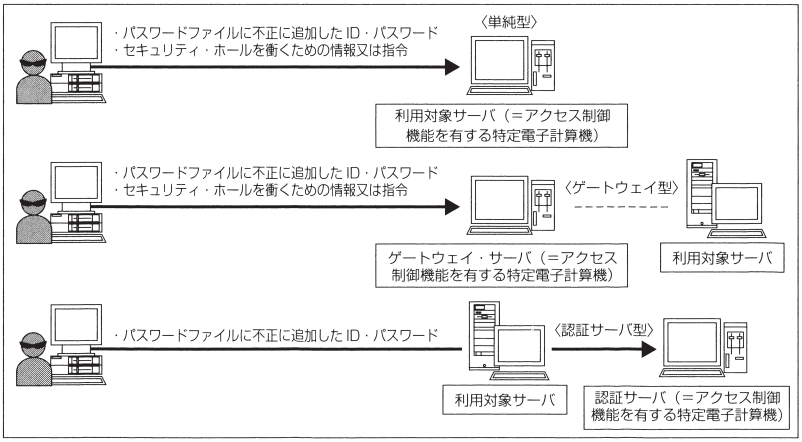
さて、ここで一つの設例を考えてみよう。次頁の様な設定のサーバーがあったとしよう。インターネット、すなわち不正アクセス禁止法上の電気通信回線には、http(11)しかないとする。こうした設定は不自然に思われるかもし

不正アクセス行為（第２条第４項）の類型（詳細版）

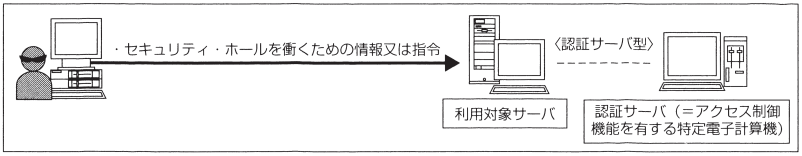
第１号（不正ログイン）



第２号（セキュリティ・ホール攻撃）



第３号（セキュリティ・ホール攻撃）



れないが、実際小規模のソフトウェアハウスで、不正アクセスを避けるため、ポートはhttpしか開けず、コンテンツのメンテナンスはネット経由では行わず、サーバーのキーボードで直接行っているという所を知っている。

この設定で、http://ccc.bbb.co.jp は公開されているが、一方、会員のアクセス状況を知る等のため、希望者には会員登録をさせ、会員はアクセス制御のある、http://aaa.bbb.co.jp からＩＤとパスワードを入力してアクセスする様にアクセス管理者から求められており、会員登録をしたくない者はアクセス制御がない、http://ccc.bbb.co.jp からアクセスしても良いとされているとする。（技術的にはエイリアス[12]で簡単にできる。）

今仮に、登録していないある者が、何らかの推測や手段（もしかして偶然）によって、http://aaa.bbb.co.jp というＵＲＬにアクセス制御を越えてコンテンツを見たとしたら、これは不正アクセスとなるのであろうか。

「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こととなる。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。[13]」という公権解釈からは、違法性阻却により不正アクセスではないということにもなろうかと斟酌するが、なんとなくすっきりしない。

逆に、http://aaa.bbb.co.jp を使うことを指定されていて、アクセス制御のない、http://ccc.bbb.co.jp にアクセスすることをアクセス管理者から（技術的ではなく利用契約上）禁止されて

いる登録会員が、http://ccc.bbb.co.jp にアクセスした場合も、そもそも不正アクセスの構成要件に該当しないということになるのであろうか。

同様に、よく議論されるのに「隠しＵＲＬ[14]にアクセスするのは不正アクセスか。」という問題がある。本設例においても、アクセス管理者が、http://ccc.bbb.co.jp のＵＲＬは公開せず、自分用に秘匿していたらどうであろう。それでも http://aaa.bbb.co.jp になりすましアクセスするのは、不正アクセスではないのであろうか。不正アクセス禁止法はそういうものだということなのかも知れないが、やはり整合性に欠く様に思える。

更に言えば、サーバーのキーボードからの直接のなりすまし等は、「アクセス制御を有する特定電子計算機のキーボードを直接操作して、他人の識別符号を入力するような行為も、アクセス制御機能による利用権者等の識別が正しく行われているとの社会的信頼を害する行為であるとの考え方も成り立ち得る。しかしながら、このような行為によるコンピューターの無権限での利用の問題は、コンピューターをネットワークに接続しないで用いる場合（スタンド・アローンのコンピュータ）でも、同様に生じ得ること、特定電子計算機の在る部屋や建物への入退出管理の徹底等の手段による利用の制限（言い換えれば、なりすまし等によって利用権者等の識別が正しく行われないことの防止）ができることから、不正アクセス行為とはとらえないこととしているものである。[15]」。とされているが、立法論としては、規制してもいいのではないかと考える。

四―二　不正アクセスと無権限アクセス

こうした難しさを考える際に、キーとなるのが「無権限アクセス」と「不正アクセス」の違いである。

原則的に言えば「無権限アクセス」とは、技術的なアクセス制御の有無に関わらず、アクセスする事が許諾され

ていないアクセスを行うという社会的概念である。例えば、技術的には空く制御のない、公開されているホームページであっても、「以下の（サーバー内の）リンクにアクセスすることを禁じる。」と表示されていれば、アクセス制御がなくとも、そこにアクセスすることは「無権限アクセス」となる。

それに対し、我が国の「不正アクセス行為とは、他人のＩＤ・パスワードを悪用したり、コンピュータ・プログラムの不備をつくことにより、本来アクセスする権限のないコンピュータ（サーバ）を利用する行為[16]」であるというアクセス制御を越えることを前提とする技術的概念である。簡単に言えば「無権限アクセスの内、不正アクセスであるものを規制する。」と言う事になる。

一九九九年当初の立法頃の所謂先進国での不正アクセス禁止法は、後掲（資料一）[17]に示すように、ほとんど「無権限アクセス」を禁止する形になっており、当時の我が国での議論も「不正アクセス」という言葉も見られるものの、概念的には「無権限アクセス」についてなされている[18]。不正アクセス禁止法についても「無権限アクセス」で規定するか「不正アクセス」で規定するかの議論もあったが、一九九八年の警察庁のパブリックコメント募集の結果、「アクセス制御機能を侵害する行為を不正アクセス」とする事が適切だと判断され[19]、以後、本法は「不正アクセス」で起案されることとなった。つまり、「不正アクセスでない無権限アクセスは規制対象としない。」というのが立法者意思だという事となる。

英語では、unauthorized access が「無権限アクセス」に、illegal access が我が国の「不正アクセス」にあたることにはなるが、先述の如く当時の先進国は「無権限アクセス」＝「不正アクセス」として規制しており、この二つの言葉にはあまり区別がなく、主に、unauthorized access が用いられているようである。

「不正アクセス」という、グローバルにはマイナーな構成要件を設定した前提には、以下の事が考えられる。

（一）国際的な流れの中[20]、日本だけが不正アクセスを規制していなかったので、立法化することにしたのだが、一九八七（昭六二）年以降のサイバー犯罪対策の為の刑法改正、すなわち「電磁的記録不正作出及び供用」罪（刑一六一の二）、「電子計算機損壊等業務妨害」罪（刑二三四の二）等の条文との関係で、予備罪[21]や幇連犯[22]といった刑事法上の難しい問題を避けるという意図があったのではないか[23]。

（二）なんといっても、刑罰法規である以上、構成要件の明確化が求められる。無権限アクセス概念では、アクセス管理者の主観に依存したり、技術的にはできることが無権限アクセスとなり得るため係争が増える可能性がある。

本法が識別符号の貸し借りはアクセス管理者の許諾がなくとも合法だとするのも（二条四項一号）、構成要件からアクセス管理者の主観を排除するものであること[24]、先述の参議院「第一八〇回国会内閣委員会第四号」の国家公安委員長の発言や、審議過程における「犯罪構成要件の周知徹底」の附帯決議[25]に見るように、構成要件の限定明確化は罪刑法定主義の下必須であり、その意味では、条文が煩雑でも要件を明確化することは重要であった。

その為、我が国の不正アクセス禁止法は、「無権限アクセス」の内、技術的に限定された「不正アクセス」を定義しようとしており、その点は評価される。しかしながら先述したように、構成要件が狭すぎ、一般的な目から見れば同様の行為が、技術的前提によって有罪無罪に分かれるのには不公平感が残る。

四―三　Lynx 事件判決

無権限アクセス規制の例として、イギリスでの著名事件である、Lynx 事件を見てみよう[26]。Lynx とはキャラクターベースのＷｅｂブラウザーである。

二〇〇四年、被告人は災害義援金寄付サイトにアクセスしたが、確認ページが現れなかった為、フィッシングではないかと疑い、受付ページのＵＲＬに、../../を加え、アッパーフォルダに移動して確認したところ、そのフォルダは通常の使用ではアクセス出来ないフォルダで、社会的には「無権限アクセス」であった訳である。システム的には、無権限アクセス検出ソフトに引っ掛かり、被害届が出たと言う事である。

このアクセス技法は、所謂ディレクトリートラバーサル[27]の初歩的な技法で、例えば何らかの検索をして、http://aaa.bbb.co.jp/ccc/ddd/sample.txt というファイルにたどり着いたとしよう。まず、sample.txt の部分を削除して、http://aaa.bbb.co.jp/ccc/ddd にアクセスしたら、そのフォルダーのほかのファイルが見えた、更に、ddd や ccc を削除していったら、様々なファイルが見えたとする。

英国「コンピューター不正使用禁止法（Computer Misuse Act 1990）」一条は、「コンピューター不正使用罪（Computer misuse offences）を以下の様に定義している[28]。

（一）以下の者は、有罪とする。

（a）コンピューター内に存するプログラムまたはデータにアクセスするために確実な手段[29]でコンピューターに何らかの機能を実行させた場合であって、

（b）その確実なアクセスが無権限のものであり、かつ、

（c）その者がコンピューターに当該機能を実行させた時点において、それがコンピューターに上記機能を実行させる故意を有している事。

（二）本条の罪を犯す者の故意は、以下のいずれに向けられたものであっても認められる。

（a）限定されていなくとも、すべてのプログラムもしくはデータ。

（b）種類が限定されていなくとも、すべてのプログラムもしくはデータ。
（c）限定されていなくとも、如何なるコンピューター内に保持されているプログラムもしくはデータ。
（三）略。

以上の様に、英国「コンピューター不正使用禁止法」は「無権限アクセス」を規制しているため、被告人は有罪となった訳である。

我が国の不正アクセス禁止法では、Lynx 事件で行われた様なアクセスには「アクセス制御がない」事になって、不正アクセスではないように思えるが、後述するように構成要件上不公平感があるのは否めない。

四―四　ACCS 事件判決

以上の問題意識の下、我が国不正アクセスの著名判決である ACCS 事件[30]を見る。

こちらは、上述の如く我が国の「不正アクセス」概念に基づいている。

本件においては、被告人がサーバーに不正指令を入力し、アクセス管理者が設定している利用方法では通常 ftp[31] でアクセス制御がかかっているフォルダーに対して、http プロトコルからアクセスしたという案件である。（当時の不正アクセス禁止法二条二項、現行二条四項二号違反。）

本件に対する疑問点は、以下の通りである。

ホームページに、設定されている以外の情報または指令を入力することは、不正アクセスの構成要件に当たるのか。

本件では確かに不正アクセス禁止法上「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」したのは間違いないのだが、仮に上述の設例の様にhttp://aaa.bbb.co.jpに続けて、「あるかもしれない」と思い、http://aaa.bbb.co.jp/tempと入力したらそのフォルダーが見えてしまったらどうであろう。これは不正指令の入力に当たるのだろうか。そうだとすれば、先述の隠しフォルダーに推測でアクセスする事も不正アクセスとしなくてはならないであろう。その意味で、技術的にフォルダーのURLを取得したら不正アクセスで、適当に想定して見るのは不正アクセスでは無いというのは、個人的には不公平感が否めない。

本判決では、そのフォルダー（ファイル）は、技術的にはhttpからアクセス制御なしに見えるのだが、通常httpから見ることは想定されておらず、ftpによってアクセス制御されていたとするが、こうした主観的な曖昧性は不正アクセス禁止法が「不正アクセス」を対象とするのに対し、判決等の運用は「無権限アクセス」をも射程にしている事にある様に思われ、構成要件を厳格にするという不正アクセス禁止法の立法趣旨に反するようにも思われる。

上記四―一の設例に当てはめてみると、会員資格の有無に関わらず、アクセス制御のある、http://aaa.bbb.co.jpから見えるフォルダーに、http://ccc.bbb.co.jpからアクセスするのは、（違法性はともかく）構成要件上は不正アクセスとなるのか、ならないのか不明確なのである。

私見では、不正アクセス禁止法の公権解釈に従うなら、ACCS事件は「信用毀損、業務妨害罪」（刑二三三条）で起訴されるべきではなかったのかと思われる。

五　まとめ

以上の考察から、立法論、政策論を述べる。

第一に、同様の行為であっても技術的なアクセス制御の在り方によって、不正アクセスの成否が異なるのは罪刑法定主義の立場からは疑問が生じる。ACCS事件の弁護団が言う様に、httpからアクセスするのに、そのフォルダーがftpによってアクセス制御されている事はアクセス者には分からない。仮にそのサーバーにはhttpしかなく、他にアクセス制御がない場合、本件は不正アクセスにならない訳であるが、私見では如何にも法的安定性に欠くように思われる。そこで構成要件の基本に、無権限アクセスを置いては如何であろうか。

この場合、構成要件が曖昧にならないように、制限する必要はある。

例えば、英国「コンピューター不正利用禁止法」に有る様に、「確実（secure）」な方法でアクセスしたことを一つの要件としつつも、tempやanonymous, admin, root, guestと言った、ありふれたＵＲＬでアクセスできてしまうのは、アクセス管理者の過失、怠慢として不正アクセスから排除すべきであろう[32]。

もう一つ、上述したように、アクセスが無権限としてアクセス管理者から禁止されていることが、技術的であろうが、利用契約といった社会的なものであろうが、アクセス禁止が、例え所謂社会通念上であったとしても、明確であることが必要である。

Lynx事件の様に、技術的にはアクセスできるのに、アクセス禁止の明示はなく、それにも関わらず、ディレクトリートラバーサルを無権限アクセスとして処罰するのは、確かに広汎に過ぎて明確性に欠くように思われる。

やはりアクセス管理者が技術的にアクセスを拒否し、access deniedと表示するようにしたり、index.html[33]を入れて、そこに「アクセス禁止」と表示するなりするのが筋だとは思うが、そうした技術的制限がなくとも利用規定をＨＰに掲示する等、何らかの権利制限が明白になっているべきだと思われる。ACCS事件の場合だと、「ＨＰ（ＣＧＩ[34]）の通常利用以外の使用を禁じる。」と明確に書いておくべきであったであろう。

但し、Lynx事件もACCS事件も、被告人は情報技術関係者であったので、専門家の「高度注意義務」の観点から、技術的制約に対する判断は、一般人に対する判断より厳しくなる可能性があることで、無権限アクセス概念を採用すると、現行の「不正アクセス」要件より曖昧になる点は否めないが、ACCS事件に関しては、明示がないとしても、入力が通常の使用ではなく無権限であることは、ftpによるアクセス制御があろうがなかろうが、「不正指令の入力」であると認定できるものだと思料するので、むしろ構成要件としては不正アクセスより、無権限アクセスの方が明確になるのではないかと思われる。

最近の不正アクセス事例では、後掲（資料二）の様に、オンラインゲームサイトにおいて、手口はターゲットユーザーの管理の甘さに付け込んで、そのSNSやメールアドレスからIDやパスワードを推測してなりすますというのが増加しており、予測される様に若年化が進み、被検挙者は未成年が四分の一という状況となっている。(35)

こうしたパスワード推測行為が無権限アクセスを前提とした場合、secureという要件に該当するかは若干疑問があるが、当初述べたように平二四年改正で準備行為も規制対象になったこともあり、準備行為の故意があれば、不正アクセスが成功した段階で無権限アクセスと捉えれば良いのではないだろうか。

要は、「アクセス制御」という技術的基準で構成要件を規定するのではなく、通常の犯罪の様に社会的基準で構成要件を定めた方が、総体的にはむしろ明確性が向上し不公平感がなくなり、罪刑法定主義の趣旨に沿うのではないかと思われるのである。

第二に「アクセス制御」を破る行為については、現行不正アクセス禁止法では「アクセス制御を作動させる」事自体は不正アクセスとしてカウントされていない。実際、筆者が瞥見し得た二〇余の判決例はすべて不正アクセス行為の構成要件をあくまでターゲットマシンを「利用可能な状態」にするまでは不正アクセスとはせず、アクセス

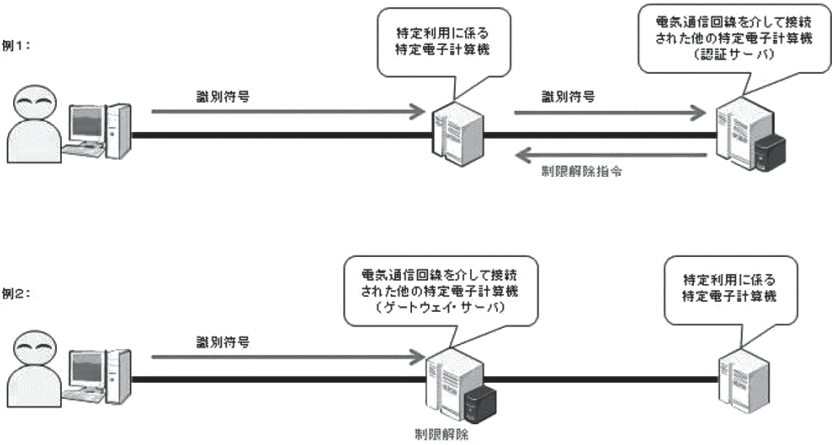
制御機能そのものを作動させること自体は不正アクセス回数にはカウントされていなかった[36]。

この場合、下図の様な状態で[37]、アクセス制御サーバーは稼働しているが、ターゲットマシンの電源は、例えばメンテナスの為、全部切られていたといった状態であれば、内部ネットワークに侵入しても、現行不正アクセス禁止法では不正アクセスにあたらないであろう。

つまり、ターゲットマシンが「利用可能」になって初めて、不正アクセス禁止法上、アクセス制御を破ったことになるのだが、ターゲットマシンが一台も稼働していなくとも、社内ＬＡＮのＩＰを取得した段階で、不正アクセスとしてもいいのではないだろうか。

つまり、認証サーバーと言えども、特定電子計算機なのだし、そのアクセス制御を破ることは、そのこと自体を不正アクセスとして良いのではないかということである。

第三に、上述した様に、サーバーのキーボード（コンソール）からの直接アクセスも、無権限アクセスの立場からは規制しても良いのではないかということである。無権限アクセスを規制する上述、英国「コンピューター不正使用禁止法」も、我が国不正アクセス禁止法に言う「特定利用」にこだわらずコンソールからの無権限アクセスも、



特にこれを排除してはいない。

尤も、我が国不正アクセス禁止法の目的は「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」ることであるので[38]、必ずしも必須ではない様にも思われるが、「無権限アクセス」を要件にするなら、考慮せざるを得ないであろう。

（1）田中規久雄「不正アクセス禁止法における不正アクセス行為の概念」阪大法学六〇巻六号、平二三年三月、五三―八一頁。

（2）詳細は不明だが、ウイルスにより何らかの不正アクセスがなされたようである。

（3）フィッシングについては、警察庁「ＩＤ・パスワードが狙われています。～フィッシング～」、フィッシング対策協議会「フィッシングとは」。語源については、Russell Kay, The Origins of Phishing, COMPUTER WORLD, 2004.1.

（4）典型的には、東京高判平三一年三月二八日（一審、東京地判平二九年四月二七日、岡田好史「刑事法の諸問題（一〇）」専修大学法学研究所紀要四四、二〇一九年二月、九一～一〇四頁、参照）、東京地判平一七年九月一二日等。（尚、本稿の引用判決例はすべて不正アクセス禁止法違反の刑事事件に限る。）

（5）警察庁「不正アクセス行為の禁止等に関する法律の一部を改正する法律の概要」、「不正アクセス禁止法改正Ｑ＆Ａ」。蔵原智行（警察庁）「不正アクセス禁止法改正の概要」平二四年。実数の趨勢については、各年度の「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」『警察庁サイバー犯罪プロジェクト　統計』参照。

（6）高尾健一「最近のサイバー犯罪の発生状況」フィッシング対策協議会『フィッシング対策セミナー二〇一七年』。衆議院「第一八〇回国会内閣委員会第四号（平二四年三月十六日）」参照。

（7）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等に関する法律［第二版］』平二四年七月（以下『逐条』と略す。）一〇頁。

（8）参議院「第一八〇回国会内閣委員会第四号（平二四年三月二十九日）」大野元裕議員、国家公安委員長の発言。

（9）警察庁「不正アクセス行為の禁止等に関する法律の解説」六頁～。

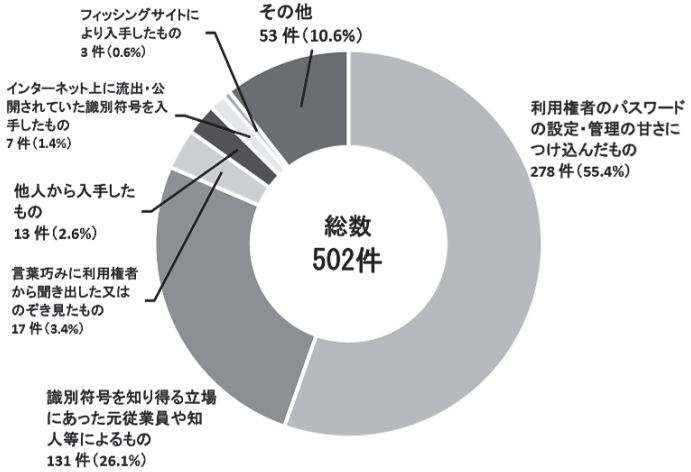
（資料一）

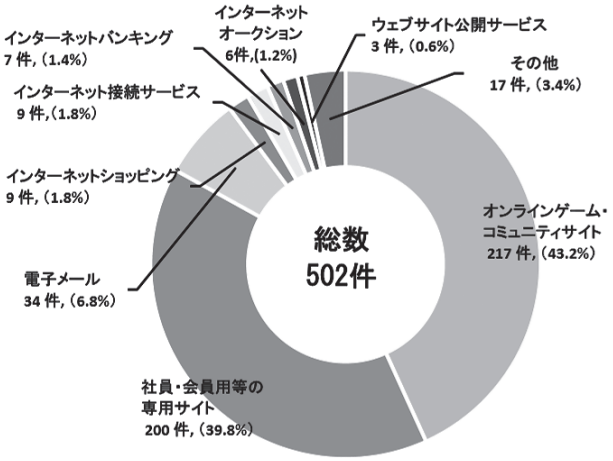
国　名	法律名	規　定
◆米国	1996年国家情報インフラ防護法	第1030条(a)　コンピュータに関連する詐欺及びその他の活動 (1)　故意に無権限で、若しくはアクセス権限を越えてコンピュータにアクセスし、かつ当該行為により、大統領命令若しくは法令に基づく合衆国政府の決定により国防若しくは外交上の理由から無権限の漏示に対する保護が必要であるとされた情報若しくは1954年原子力エネルギー法11条ｙ項に規定された秘密データを合衆国の利益を害し若しくは外国の利益のために使用されると信ずるに足る理由がありながら取得し、故意に当該情報若しくは秘密データを受理する権限のない者に伝達し、交付し、転送し、若しくはそのような状態にし、若しくはその未遂をし、又は故意に当該情報又は秘密データを保持し、それを受理する権限のある合衆国の公務員に渡らないようにした者 (2)　故意に無権限で、又はアクセス権限を越えてコンピュータにアクセスし、かつ当該行為により以下の情報を取得した者 (A)　金融機関若しくは15編1602条ｎ項に規定されたカード発行人の財務記録に含まれている情報又は公正信用報告法（合衆国法典15編1681条以下）に規定された消費者信用情報機関のファイルに含まれている消費者に関する情報 (B)　合衆国の部局又は機関からの情報 (C)　当該行為が州際間の又は外国との通信と関連する場合における防護されたコンピュータからの情報 (3)　故意に、合衆国の部局若しくは機関のコンピュータで公共の用に供していないものにアクセスする権限がないにもかかわらず、
	コネチカット州刑法（例）	第53条ａ-251　コンピュータ犯罪 (b)　コンピュータ・システムへの不正アクセス (1)　コンピュータ・システムにアクセスする権限がないことを知りながら、アクセスし、又はそのような状態にした者は、コンピュータ・システムへの不正アクセスとして有責である。
	デラウェア州刑法（例）	第932条　不正アクセス コンピュータ・システムにアクセスする権限がないことを知りながら、アクセスし、又はそのような状態にした者は、コンピュータ・システムへの不正アクセスとして有責である。

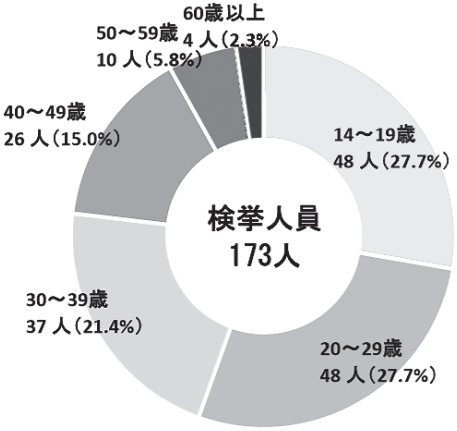
◆イギリス	1990年コンピュータ不正使用法	第１条　コンピュータ処理記録への無権限アクセス (1)　次の行為を行った者は、有責である。 (a)　コンピュータに蓄積されたプログラム又はデータにアクセスする意図をもってコンピュータを作動させること (b)　そのアクセスが無権限であること (c)　コンピュータを作動させる時点において、アクセスが無権限であることを知っていること (2)　本条に規定する犯罪の意図は、次に掲げるものに向けられたものであることを要しない。 (a)　特定のプログラム又はデータ (b)　特定の種類のプログラム又はデータ (c)　特定のコンピュータに蓄積されたプログラム又はデータ (3)　本条の罪を犯した者は、略式起訴により６カ月以下の禁錮若しくは標準レベル５以下の罰金又はその両方の刑に処する。
◆ドイツ	第２次経済犯罪対策法	第202条ａ　データの探知 (1)　自己の用に供するものでなく、かつ、無権限のアクセスに対して特別に保護されているデータを、権限なく取得し、又は他人をしてこれを取得せしめた者は、３年以下の自由刑又は罰金に処する。
◆フランス	情報処理関連不正行為に関する1988年１月５日の法律	第323-１条（不正アクセス等）　①　不法に、データの自動処理システムの全体又は一部にアクセスし、又は滞留する行為は、１年の拘禁刑及び100,000フランの罰金で罰する。 ②　前項の行為により、システム中のデータを消去若しくは改変、又はシステムの動作の悪化が生じた場合、刑を２年の拘禁刑及び200,000フランの罰金とする。 第323-２条（コンピュータ業務妨害）　データの自動処理システムの動作を妨害し、又は不調にする行為は、３年の拘禁刑及び300,000フランの罰金で罰する。 第323-３条（データの不正操作）　不法に自動処理システムにデータを入力し、又は、そのシステムが収納するデータを不法に消去若しくは改変する行為は、３年の拘禁刑及び300,000フランの罰金で罰する。
◆イタリア	刑法	第615条の３（情報通信システムへの不正アクセス） 正当な権利なく、防護措置によって守られた情報通信システムに侵入し、又はこれを排除する権利を有する者の明示的若しくは暗黙の意思に反してシステムに留まった者は、３年以下の

		禁錮に処する。
◆カナダ	刑法	第242.1条 (1) 詐欺的にかつ権限なく (a) 直接若しくは間接にコンピュータ・サービスを取得し、 (b) 電磁的、音響的、機械的若しくはその他の手段により、直接若しくは間接に、コンピュータの作用を妨害し、若しくは妨害を受ける状態にし、 (c) (a)項、(b)項に規定する犯罪若しくはデータ若しくはコンピュータ・システムに関連して430条に規定する犯罪を犯す目的で、直接若しくは間接にコンピュータ・システムを使用し、又はそのような状態にし、 (d) (a)、(b)、(c)の罪を犯す目的で、コンピュータのパスワードを利用し、所有し、取引し若しくは他の者にそのパスワードを利用できるようにした者は、正式起訴犯罪として10年以下の拘禁刑に処し、又は略式手続犯罪として処罰する。

（資料二）




インターネットバンキング
7 件,（1.4%）
インターネット
オークション
6件,(1.2%)
ウェブサイト公開サービス
3 件,（0.6%）
その他
17 件,（3.4%）
インターネット接続サービス
9 件,(1.8%)
インターネットショッピング
9 件,（1.8%）
総数
502件
オンラインゲーム・
コミュニティサイト
217 件,（43.2%）
電子メール
34 件,（6.8%）
社員・会員用等の
専用サイト
200 件,（39.8%）


60歳以上
4 人（2.3%）
50〜59歳
10 人（5.8%）
40〜49歳
26 人（15.0%）
14〜19歳
48 人（27.7%）
検挙人員
173人
30〜39歳
37 人（21.4%）
20〜29歳
48 人（27.7%）

(10) 『逐条』六八頁。
(11) Hyper Text Transfer Protocol　所謂ホームページ。
(12) Alias　同一のアクセス対象に別名を付けること。例えば、Windows（©Microsoft）で言えば、ショートカットがこれにあたる。
(13) 『注釈』四〇頁。
(14) Uniform Resource Locator　要はサーバーにアクセスするためのアドレスのようなものである。プロトコルごとに区別され、ホームページだと、http://…、ftp だと、ftp://…といった具合になる。
(15) 『逐条』六五～六六頁。
(16) 註五、蔵原。
(17) 平成一〇年版　警察白書第一章第二節「表一―一「不正アクセスの処罰に関する外国法制」」『逐条』五～九頁より転載。
(18) 平成一〇年版　通信白書第一章第四節「二　無権限アクセス対策」。
(19) 『逐条』一三頁。
(20) 例えば、ＯＥＣＤ「コンピューター犯罪」一九八五年。
(21) 予備罪ではないとされている。（『逐条』二八～二九頁。）
(22) 後続の犯罪に対する牽連犯ではなく併合罪となるとされている（最二決平一九年八月八日）。
(23) 『逐条』二七頁、参照。
(24) 『逐条』七三～七四頁。
(25) 衆議院地方行政委員会、参議院地方行政警察委員会、平二年。
(26) See, 'Tsunami hacker convicted - Fine + costs for Daniel Cuthbert' The Register, 2005.10.6, Security pros savage Tsunami hacker verdict', Security Focus, 2005.10.11, et al.　加藤敏幸「不正アクセス」刑法雑誌一巻一号、平一四年、八一―八三頁、等参照。
(27) directory traversal　無権限アクセスかどうかはともかく、現時点にいるＵＲＬから、アクセス可能なフォルダーを推測し、そこにアクセスする技法。バックトラッキング（back tracking）等とも言われる。

(28) 原文は以下の通りである。

(1) A person is guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorized; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(29) 我が国不正アクセス禁止法における「なりすまし」や「クラッキング」の事と思われる。

(30) 東京地判平一七年三月二五日。

(31) File Transfer Protocol　ネットを通じてファイルを読み書きするプロトコル。

(32) 『逐条』四二頁、参照。

(33) http でアクセスされた場合、一般的にデフォルトでブラウザーに表示されるファイル。

(34) Common Gateway Interface　Ｗｅｂ（ＨＰ）の裏でプログラムを稼働させる仕組み。

(35) 「平成三〇年におけるサイバー空間をめぐる脅威の情勢等について」警察庁。

(36) 福岡地判平三〇年二月一九日、佐賀地判平二九年一二月一一日（同旨、、佐賀地判平二九年九月二九日）等。

(37) 註九、五頁。

(38) 不正アクセス禁止法一条。

（ネットで検索できるものについては、詳しい書誌は省略している。Accessed at 2019.10.　英数字に関しては、帳合の為、適宜置き換えている。技術的理解については、養老真一教授にご助言を賜った。感謝致します。）