不正アクセス行為の発生状況の現状と課題（３）

岡　田　好　史

Ⅴ　不正アクセス禁止法上の不正アクセスをめぐる課題

１．2012（平成24）年改正の背景と経緯

我が国においては，1994（平成６）年にインターネットの商用解放が実

現したが，その後のブロードバンド回線の普及や，携帯電話をはじめとするネットワーク対応型情報端末の普及等により，インターネットは社会インフラの一つとなりつつあり，東日本大震災の際にインターネット上のミニブログ Twitter が活用されたように，その重要性は増している。

電話による通信のように電話回線を一時的・固定的に使用するのと異なり，インターネットでの通信は，パケット交換方式を採っているため，その授受経路を確定しがたく定型性を欠いている。また，ネットワークがオープンであることから，ネットワーク全体を管理する管理者が存在せず，全体に適用されるべきルールを形成することは不可能である。さらに，時間と国境などの地理的制約を越えて情報の流通が行われる。この①匿名性，②不特定多数性，③空間超越性が，不正行為が行われた場合の「犯行」場所や，方法を確定しにくくしている。

基本的にインターネットでは匿名の世界であり，相手を確認する方法は ID やパスワード等の情報に依らざるをえず，名乗っている名前が実名かどうかをサイバースペース上で確認する術はない。他人の識別符号は，一度入手されてしまえば専門的知識・技術を有していなくても容易に不正アクセス行為を行うことができる場合が多く，相手方を識別する ID やパスワードを窃用された場合には，現実世界における対面や書面におけるものと異なり，ほぼ完全な「なりすまし」が可能になる。

インターネットを利用して犯罪が実行される場合，犯人は，当然ながらインターネットの特質を理解している。インターネットを介した犯罪は，犯人の顔を見えにくいものにする。顔のない犯人が，遠く離れた場所から犯行におよぶ。被害にあった側は，現実世界の場合と異なり犯人が近づいてきたことすらわからないし，最悪の場合には，どのような犯行が行われたのかわからないことすらありうる。不正アクセス行為を行う目的で他人の識別符号を入手した者が不正アクセス行為に及ぶことを阻止することは極めて困難である。

「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およ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」べく，不正アクセス行為の禁止の実効性を確保するためには，他人の識別符号の不正流出，不正流通を防止する必要がある。インターネットの急速な普及に伴い，不正アクセスをめぐる情勢が大きく変化したことは，すでに述べたとおりである。

Ⅲ章でみたように，旧法施行時と比べると不正アクセスの認知件数は2007（平成19）年以降急増しており，不正アクセス罪の検挙人員は増加傾向にある。当初は，識別符号窃用型の不正アクセス行為で検挙された事案における当該識別符号の入手方法は，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や，識別符号を知り得る立場にあった元従業員，知人等によるものが多く，特に高度なコンピュータ技術および電気通信技術を有していない者でも行える形態が目立っていたが，2006（平成18）年以降は，フィッシング（Phishing）により識別符号を入手したものや，トロイの木馬やスパイウエア等の不正なプログラム，キーロガー等のクラッキング・ツールを使用して識別符号を入手するなどの高度なコンピュータ技術を悪用したものもみられるようになってきた[1]。とりわけ，フィッシングは旧法制定時に想定されていなかった手口であり，社会問題化していたことから，産業界から犯罪化の要望が出されていた[2]。

また，インターネット利用者が利用するコンピュータのサービスの数がここ数年で増加しており，同一の識別符号を複数サイトで使い回ししている状況が一般化している[3]ことに伴い，連続自動入力プログラムを用いて不正アクセス行為を行う手口の攻撃（試行攻撃）がみられるようになった。この手口は，多数の識別符号を連続自動入力する際に，不正取得した他人の識別符号のリストを照合することで，一定程度の割合で不正アクセスを成功させてしまうというものである。連続自動入力プログラムを用いた不正アクセスは，同一のIPアドレスから，短時間の間になされた，多数の

識別符号の入力等により判断されうるが，正規の利用権者が行った正当なログインが含まれている可能性は理論的には排除できない。そのため，旧法における他人の識別符号の無断提供の禁止規定では，連続自動入力プログラムに悪用するための識別符号の不正流通に十分に対処することが困難であった。

さらに，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るため，旧法でも，アクセス管理者による防御措置の規定を設けて，アクセス管理者に防御措置の実施を促し，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てきたが，Ⅳ章において前述したように，利用権者のみならず，アクセス管理者においても，IDS の導入やセキュリティ監査の実施，OS へのセキュリティパッチの導入といった基本的な不正アクセス対策が十分に取られているとは言い難い。このことは，インターネットが私たちにとって社会インフラ化してきているとはいえ，人々のセキュリティに対する意識が高くないことを示唆しており，アクセス管理者が防御措置向上の努力義務を果たすためには，更なる環境整備を行う必要が生じていた。

2010（平成22）年に警察庁において開催された総合セキュリティ対策会議の報告書[4]において，不正アクセス行為に係る情報を収集・共有して不正アクセス行為に係る実態を詳細かつ正確に把握するとともに，不正アクセス行為に係る実態の把握を踏まえて問題点を抽出し，不正アクセス防止対策の官民の役割分担や連携施策を検討することが必要であるとの提言がなされ，不正アクセス行為に係る罰則の法定刑の引上げ，フィッシングによる識別符号の不正取得の防止，アクセス管理者による防御措置の促進・支援等について検討すべきとの提言もなされていた。

この提言を受けて，社会全体としての不正アクセス防止対策の推進に当たって必要となる施策に関して，現状の課題や改善方策について官民の意

見を集約するため，2011（平成23）年6月30日，警察庁，総務省および経済産業省は，民間事業者等と共同で不正アクセス防止対策に関する官民意見集約委員会（以下「官民ボード」という。）を設置した。

この官民ボードに設置された4つのワーキング・グループのうち，「不正アクセス行為防止方策ワーキング・グループ」において法改正についての議論がなされ，同年12月に「不正アクセス防止対策に関する行動計画」[5]（以下「行動計画」という。）が策定された。サイバー犯罪条約（Convention on Cybercrime）[6]においても，不正アクセス行為のほか，他人の識別符号の取得行為，保管行為および提供行為を犯罪化することが要請されており，この「行動計画」においても，フィッシング行為，他人の識別符号の不正取得行為や提供行為の法規制化の検討を行うことが盛り込まれたことから，不正アクセス禁止法の改正に向けた本格的な検討作業が，「不正アクセス行為防止方策ワーキング・グループ」を中心として進められた。

同ワーキング・グループでは，不正アクセス禁止法の所管官庁である警察庁，総務省および経済産業省のほか，同法の運用に関係する事業者や団体も交えて，改正すべき項目の選定の段階から幅広い議論が行われた。

以上のような状況に対応し，それまで禁止されていた他人の識別符号の提供行為の禁止範囲を拡張するとともに，フィッシング行為，取得行為および保管行為を不正アクセスに至る一連の行為として新たに禁止することにより，識別符号の不正流出，不正流通を防止し，不正アクセス行為の禁止の実効性を確保するための不正アクセス禁止法の改正が2012（平成24）年2月21日に閣議決定された（閣法37号）。そして，第180回国会において，改正案は衆議院に提出され，3月30日に参議院での審議を終了し，翌日に公布され（法律12号），5月1日から施行されることとなった。

2．2012（平成24）年改正法の主内容

（1）他人の識別符号の不正取得・不正保管の禁止

旧法においては，識別符号の不正入手の前段階となる保管・取得行為を取り締まる規定は存在していなかった。これは，情報の不正入手を原則として処罰していない現行法に配慮したのではないかとも受け取れる。しかし，識別符号は，ネットワーク上で個人を識別するための重要な個人情報でもあり，不正アクセス行為の禁止の実効性を確保するためには，他人の識別符号の不正取得や保管の犯罪化が求められていた。

そこで，改正法では，不正取得罪（改正法4条・12条1号）および不正保管罪（改正法6条・12条3号）を新設したが，いずれも「不正アクセス行為の用に供する目的」を要件として付している。これは，識別符号の取得行為や保管行為は，不正アクセス行為の用に供する目的がない場合には，不正アクセス行為につながる危険性が小さく，そのような行為まで禁止・処罰の対象とすることは適当でないとされたことによる[7・8]。

本罪にいう「取得」および「保管」の意義については，支払用カード電磁的記録不正作出準備罪（刑法163条の4），不正指令電磁的記録取得罪（刑法168条の3）における「取得」および「保管」と同義であると解される。すなわち，「取得」とは，識別符号を自己の支配下に移す一切の行為をいい，取得客体は，有体物に限られない。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データを記録した電磁的記録媒体といった，一定の媒体に記録された同様の情報を記録媒体ごと受け取る行為等がこれに当たる。業務その他正当な理由による場合を除き識別符号の利用権者以外の者から提供[9]を受ける行為も取得に該当する[10]。

「保管」とは，有体物の所持に相当する行為であり，他人の識別符号を自己の管理・実力的支配下に置いておくことをいう。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電磁的記録媒体を保存・保有する行為がこれに該当する[11]。

（2）他人の識別符号の提供行為の禁止・処罰の拡充

旧法により，目的如何にかかわらず他人の識別符号を第三者に譲りわたす行為は，不正アクセス助長罪（旧法4条・8条）として規制可能となったが，禁止行為は，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」提供する場合に限定されていた。その趣旨は，識別符号が提供されたとしても，それがどのサービスの利用に係るものであるかが明らかでない場合には，当該識別符号を用いて容易に不正アクセス行為を実行することができず，不正アクセス行為を助長することとはならないと考えられたからである。

しかしながら，コンピュータ・ネットワークの進展に伴い，利用権者がwww上で様々なサービスを利用する機会が増加し，その際に識別符号の設定を要求されることも多くなっている。先述したように，利用権者の多くはサービスごとに異なる識別符号を設定し使い分けることを煩雑に感じ，異なるサービスにおいても同一の識別符号を使い回す例が広くみられる。このため，連続自動入力プログラムを用いて識別符号データを様々なウェブサイトに入力して不正アクセス行為を試行する形態の攻撃がなされた場合に，利用権者が識別符号を使い回していると，一度の攻撃で相当程度高い頻度で不正アクセスがなされてしまう可能性がある。つまり，他人の識別符号を提供する側において，どのウェブサイトの利用に係るものであるかを明らかにしないとしても，提供を受けた側において試行攻撃を行うことによって，結果的に，どのウェブサイトの利用に係るものであるかを明らかにすることができることになる。そこで，今回の改正により，改正法5条の文言から，提供する識別符号に関する要件が削除されることとなった。

また，提供者が提供行為を行うに当たり，提供の相手方に不正アクセス行為の用に供する目的があると知りながら提供する場合と，そうでなく提

供する場合とでは，加えるべき法的非難の程度には差があることから，前者の場合（改正法12条２号）と後者の場合（改正法13条）を分け，処罰範囲が拡充された。

（３）フィッシング行為の禁止・処罰

世界的にみてもフィシング・サイトの数は日々増加している[12]。すでにみてきたように，2005（平成17）年以降，フィッシングによる他人の識別符号の不正取得とそれに基づく不正アクセスは多発傾向にある。

多くの場合，フィッシングの典型的な手口は，下記のように偽装メールと偽サイトの２段階により構成されている。

①フィッシング攻撃者（フィッシャー）が，有名な銀行やネット・ショッピング会社の担当者等になりすまし，メールの本文に「システムに不具合が起こったので情報を再入力してほしい」のように，メールを受信したユーザの関心を強く引くような記述がなされた「重要なおしらせ」を装った偽装メールを不特定多数のユーザに送信する。

②その文面に引かれたユーザが本文中のリンクをクリックすると，本物そっくりの偽の Web サイトに誘導され，騙されたユーザは，偽サイトのフォームにネット・バンクのアカウント情報やクレジットカード番号などの個人情報を入力させられ，フィッシャーに個人情報を詐取される。

フィッシングを行う際に，真正サイトをコピーして使用したのであれば著作権法違反になる余地がある[13]。登録商標を使用すれば商標法に，周知性を有する他人の表示を使用したような場合には不正競争防止法にも違反する場合があり得る。しかし，他人の知的財産権を侵害していないようなケースでは，不正アクセスおよびその後に続くコンピュータ犯罪が行われるまでは犯罪とならなかった[14]。また，不正アクセス行為の禁止の実効性

を確保するためには，他人の識別符号の不正探知・取得・保管等を規制する必要性があった。フィッシング行為は，他人の識別符号の取得につながる行為であるだけに，不正アクセス行為につながる危険性が非常に大きいことから，改正法において，フィッシング行為自体が規制されることとなった[15]。

改正法７条は，「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になりすまし，その他当該アクセス管理者であると誤認させ」フィッシング行為をすることを禁止している。本条では，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，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識別符号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る。すなわち，公開されたウェブサイトを閲覧する利用権者をして，フィッシングサイトをアクセス管理者がウェブサイトに公開した真正のものと誤認させる意図，または，送信された電子メールを受信する利用権者をして，アクセス管理者が電子メールにより送信した正規の電子メールであると誤認させようとする意図を持って行うことが必要である。

（４）不正アクセス罪の法定刑の引上げ

不正アクセス罪の法定刑は，旧法において１年以下の懲役又は50万円以下の罰金であった（旧法８条１号）が，立法当初から，この法定刑では「確信犯」的な犯罪者には効果が期待できない[16]等の批判がなされていた。そのため，改正法11条において，３年以下の懲役又は100万円以下の罰金に引き上げられた。理由としては，インターネットが社会・経済活動にとって極めて重要なインフラとして国民生活を支える状況となり，保護法益であるアクセス制御機能に対する社会的信頼の確保の重要性が増大していたことのほか，2011（平成23）年の刑法改正により新設された不正指令電磁的記録作成・供用等の罪の法定刑が３年以下の懲役又は50万円以下の罰

金とされたこと，旧法制定時に参考にした電気通信事業法の通信の秘密を侵害する罪の法定刑が，旧法制定時は１年以下の懲役又は20万円以下の罰金であったが，その後の改正で２年以下の懲役又は100万円以下の罰金に引き上げられていたこと等があげられる[17]。

（５）行政による援助等

インターネット利用が拡大していることおよび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，不正アクセス行為による被害を防止するためには，先に述べたようにアクセス管理者やエンドユーザ等による物理的対策，技術的対策のみならず，人的対策も重要になっている。

不正アクセス行為による被害を防止するために，行政は，これら関係者の活動が円滑に行われるよう各種施策を講じるとともに，啓発および知識の普及を行い，支援していく必要があることから，改正法９条５項に，「第一項に定めるもののほか，都道府県公安委員会は，アクセス制御機能を有する特定電子計算機の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。」として，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が明記された。

また，情報通信技術の進展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，旧法７条１項に基づく一般的な情報の公表による援助では，旧法５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ある。

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[18]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，改正法10条2項において，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ことにより，アクセス管理者による防御措置向上の取組を促すために規定が新設された。

3．現行法の問題点と課題

（1）不正アクセスをめぐる問題点

不正アクセス禁止法は，電気通信回線を通じて，他人の識別符号の窃用(改正法2条4項1号)[19]およびセキュリティ・ホール攻撃（改正法2条4項2号・3号)[20]により，「特定電子計算機を作動させ，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」を不正アクセス行為として犯罪化している（改正法3条)。

アクセス制御機能とは，改正法2条3項において「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。」と定義されている。すなわち，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また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をいう。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う。

セキュリティ・ホール攻撃型不正アクセスは，識別符号を入力しないでも，正しい識別符号が入力された場合と同様に利用制限を自動的に解除し，アクセスを可能とする攻撃手法である。この場合，セキュリティ・ホール攻撃型不正アクセスが可能になったのは，アクセス制御機能によるアクセス制限がそもそも存在しなかったためなのか，存在はしたものの，機能しなかったに過ぎないのか，この区別が問題となる。すなわち後者の場合であれば，不正アクセス行為に該当するが，前者であれば処罰し得ないことになるからである。

この点は，東京地判平成17年３月25日[21]のACCS事件において問題となった。ACCS事件では，被害にあったサーバは，１台を複数の顧客で共用させる形で顧客にレンタル利用されていた。レンタルの際，各顧客には一定のディスク領域が割り当てられるが，そのディスク領域には，サーバのためのシステムが格納されている領域と，顧客のためのデータを格納する領域が設定されており，顧客が，顧客使用領域にあるファイルを読み書きするためには，FTPを介してサーバにアクセスし，IDとパスワードを入力する必要があった。そして，FTPを使って顧客使用領域内のドキュメントルート以下の領域にHTMLファイル等を蔵置すると，ウェブサーバがインターネット閲覧者のリクエストに応じてドキュメントルート以下の領域のファイルを読み込み，HTTPを介し，ホームページのデータとして送信することとなっていた。ただし，cgiファイルについては，ウェブサーバの設定により，その内容を送信するのではなく，当該ファイルをCGIプログラムとして起動し，その処理結果をインターネット利用者が閲覧できるように送信などすることとなっていた。被告人は，このサーバ

で使用されていたCGIの脆弱性を利用し，HTTPを介して本来FTPによってのみ閲覧することができるファイルを閲覧したというものである。

弁護人は，アクセス制御機能の有無は個々のデータ転送方式（プロトコル）ごとに考えるべきであり，被告人のアクセス行為は，「アクセス制御機能」のない電子計算機に対するものだから，旧法3条2項2号に定める「不正アクセス行為」に当たらない等と主張した。

この点について東京地裁は弁護人の主張を否定したが，園田教授，石井教授は，サービスないしプロトコル単位でアクセス制御機能の有無を判断すべきであると指摘している[22]。しかし，プロトコルは構成要件に何ら規定されておらず，また，セキュリティ・ホール攻撃型不正アクセスを，特定利用を制限しようとする特定電子計算機自体に対する場合[23]（改正法2条4項2号（旧法3条2項2号））と，特定利用を制限しようとする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に対する場合[24]（改正法2条4項3号（旧法3条2項3号））とに分けて規定していることからすると，立法者は，アクセス制御の有無を物理的な電子計算機ごとに判断することを想定していたと考えるべきである[25]。

また，不正アクセス禁止法は，「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」を不正アクセス行為と規定している。今井教授は，アクセス制御機能を有する電子計算機とは，「特定の者に限定されたデータ処理がなされるべき電子計算機であって，このデータ処理への関与をアクセス制限の解除によって行うべきもの」[26]と解していることからすると，特定利用をし得る状態を「データ処理に関連させて（データ単位毎に）理解されるべき」であると解しておられる[27]ようである。しかし，データ処理を基に考えるということになると，識別符号盗用型不正アクセスにおいては，識別符号の入力によって，データ処理が実行されていることになり，特定利用を「利用し得る」状態ではなく，

「利用する」状態にあることになってしまう[28]。アクセス制御機能による特定利用の制限措置が侵害された状態を捕捉するために，「特定利用をし得る」状態を規定することとしたという立法趣旨[29]からすると，識別符号の入力や機能制限を免れることができる情報または指令の入力により，機能制限を解除し，正規の利用権者と同様に特定電子計算機の機能を使用することが可能な状態と解することが，「特定利用をし得る」状態と合致すると思われる。

したがって，アクセス制御機能の有無は，物理的な電子計算機ごとに判断すべきであり，不正アクセスがなされたか否かは，データ単位処理毎ではなく，機能制限を解除し，正規の利用権者と同様に特定電子計算機の機能を使用することが可能な状態となったか否かで判断すべきものと考える。

（2）「他人の」識別符号をめぐる問題

識別符号窃用型不正アクセスの場合に問題となるのは，他人名義や架空人名義で取得した識別符号を入力して侵入する場合である。この場合，アクセス管理者との関係では，当該識別符号の取得者がアクセス権者に該当するため，「他人の識別符号」を入力したことにはならず，不正アクセス罪の構成要件には該当しない[30]ことになるからである。

当該識別符号取得の過程で，文書偽造を行ったり電磁的記録の不正作出を行ったりすれば文書偽造罪や電磁的記録不正作出罪に問われることはあり得るが，当該不正アクセス自体を刑法により捕捉することはできるのであろうか。すなわち，他人名義もしくは架空人名義で取得した識別符号の使用により利用履歴（システム・ログ）が作成されたことをして，電磁的記録不正作出罪（刑法161条の２），あるいは電子計算機使用詐欺罪（刑法246条の２）に問いうるであろうか。

プロバイダーを通じてのインターネットへの接続などのような有料サービスの場合には，通常，システム・ログをログ・ファイルに自動的に残す

ようになっている。多数のものが使用するシステムの利用にあたっては，このようなログを前提に課金を行うことから，架空人名義で取得した識別符号によるアクセスが行われた場合には，不正利用者が利用代金の請求を免れることになる。これを，支払うべきサービス料金の免脱という点から捉えて電子計算機使用詐欺（刑法246条の２）に問うことは，可能であろうか。

電子計算機使用詐欺罪は，行為類型を前段と後段で二つに分けている。前段は，コンピュータに虚偽の情報または不正の指令を与えて財産権の得喪，変更に係る不実の電磁的記録を作成して，それにより自己または第三者に財産上の利益を与える行為である。後段は，財産権の得喪，変更に係る不実の電磁的記録を人の事務処理のように供して，それにより自己または第三者に財産上の利益を与える行為である。前段の行為は，さらに積極利得型と債務免脱型に区分される[31]。課金ファイルに誤った情報を記録させて有料サービスの課金を免れるような行為は，債務免脱型の行為に該当する事案である。

他人名義もしくは架空人名義で取得した識別符号を使用して，パソコン通信やプロバイダーを通じてのインターネットへの接続などのような有料サービスを享受した場合には，「自己」の識別符号を利用していることから，「虚偽の情報」には当たらず，「不実の電磁的記録」が作出されたとはいいにくいように見える[32]。しかし，条文には，そのような限定解釈をするに至る明文の根拠は見られず，また，行為者が不正なアクセスを行うことで，当該「他人」が利用したものとしてログの記録を変化させ，不正利用者は，その利用代金の請求を免れているわけであるので，架空名義・他人名義で取得した識別符号の入力は「虚偽の情報」を与えたといえ，ログの作成をもって「不実の電磁的記録」を作出したことに当たるといえよう。したがって，本来履行すべき債務を不正利用者が不正な手段で免れた場合に対しては，電子計算機使用詐欺罪に問うことは，不可能ではないと思わ

れる。

課金を前提としていない場合には，なりすました他人名義のシステム・ログが作成されたことをして，侵入先のコンピュータの中にあるデータの一部または全部に，新たな証明力が作出されたとして，電磁的記録不正作出罪が成立することになるのであろうか。

本罪の行為は不正に電磁的記録を作ることにある。「不正に」とは電磁的記録の作出権者の意図に反して，権限なく電磁的記録を作り出すことをいう[33]。架空人名義・他人名義の取得者は，「自己」の識別符号を利用しており，一定の作出権限を有する。しかし，架空人名義・他人名義でユーザー・アカウントを取得した者がコンピュータを使用することは，コンピュータの設置運営主体の意思に反するといってよいので，そのような不正利用者がアクセスをしてログが作成されたという点をもって，本条にいう「不正に」作出したという要件を充足していると思われる。

それでは，このような行為に「人の事務処理を誤らせる目的」があるということは出来るのであろうか。「人の事務処理を誤らせる目的」とは，不正に作られた電磁的記録が用いられることにより，他人の事務処理を誤らせる目的をいい，ここでいう「事務」とは，他人の社会生活に影響を与えることが出来る性質の事務処理を意味し，財産的なものに限られず，法律的事務であるか否か，業務として行われる事務か否か等を問わないとされている[34]。

また，本条が成立するためには不正に作出された電磁的記録が「権利，義務又は事実証明に関する」ものであることが必要である。「権利，義務又は事実証明に関する」電磁的記録とは，私文書偽造罪におけるものと同義であり，その内容が，権利・義務の発生，存続，変更，消滅などに関する事実を証明しうるか，または実社会生活に交渉を有する事項を証明するに足りるものをいう。ログは，当該コンピュータにアクセスする権利を有する者が当該コンピュータを利用したということを確認する記録であるこ

とからこの要件を満たすと思われる。

本来アクセス権を有しない者により，あたかもアクセス権を有している者が利用したかのような記録が作成されることは，ログの証明機能を誤らせることになる。したがって，課金を前提としていない場合には，電磁的記録不正作出罪に問うことは，不可能ではないと思われる。

このようなコンピュータの無権限使用に際し，ログのような記録がある限りにおいて，電子計算機使用詐欺や電磁的記録不正作出に問うことができる場合もありえよう。

では，そのような記録がない場合はどうなるのであろうか。単なる利益窃盗に該当し，現行法の適用は出来ないとの見方がある一方で，電子計算機損壊等業務妨害の加害手段として，電子計算機損壊等業務妨害罪に情報処理阻害行為による類型が取り入れられたために，コンピュータの無権限使用やデータの不正入手の問題が234条の２の適用外に置かれるという解釈は，少なくとも文言上は明確とはいえない[35]という見解がある。

電子計算機損壊等業務妨害罪は三段階の構成をとっている。第一段階として，業務に使用する電子計算機または電磁的記録を損壊し，あるいはこれに虚偽の情報または不正の情報を与え，あるいはその他の方法で，第二段階として，電子計算機に使用目的にそうべき動作をさせず，あるいは使用目的に反する動作をさせて，第三段階として，業務を妨害したときに成立する。第一段階，第二段階の事態が現実に発生しない限り本罪は成立しないからこれらの間にはいずれも因果関係が存在することが必要である。

加害の手段としては，①人の業務に使用する電子計算機もしくはその用に供する電磁的記録を損壊する行為，②人の業務に使用する電子計算機に虚偽の情報もしくは不正の指令を与える行為，③その他の行為が定められている。

情報を不正に入手したり，覗き見たり，あるいは自己の情報処理のために他人のコンピュータを使用するために他人の識別符号を用いる等する行

為は，本条の第一段に該当することは異存がないと思われる。では，その後の行為は第二段，第三段に該当するのであろうか。

西田教授によれば，他人のパスワードを利用する行為は，第一段階の②の「虚偽の情報もしくは不正の指令を与え」たと解しうるとし，コンピュータ・データの不正入手や無権限使用は，コンピュータに「設置者の使用目的に違う動作をなさしめて業務を妨害した」とも解することができると述べておられる[36]。

このような解釈を立案当局は，二点理由を挙げて明確に否定している[37]。第一は，本条にいう「使用目的」とは，具体的な業務遂行の場面において，コンピュータの設置者が，当該コンピュータを使用して実現しようとしている目的をいい，不正アクセスを行ったものに情報提供したとしても「使用目的に反する動作」をさせたことにはならないというものであり，第二は，上のような類型の場合には，業務妨害の要件である業務遂行の外形的な妨害が欠如する，というものである。

これに対し神山教授は，他人のパスワードを利用する行為は「不正の指令を与え」たと解する余地があるとしながらも，当該パスワードによってコンピュータを使用することは，設置者の客観的目的に反していると見ることは無理であるとし，処理能力が大きく同時に多くの者が使用する大型コンピュータを使用して演算や検索をする場合には，無権限者の使用が他人の業務を妨害することは通常考えられないとして，構成要件該当性が欠けるものとされる[38]。

本条にいう「使用目的」には，限定がなく，コンピュータの機能という意味での使用目的と解釈することも可能であり[39]，「使用目的」が設置運用者の使用目的だとしても様々な段階のものが考えられ，結局は「目的」をどのように捉えるかによって解釈がわかれることになろう。

しかしながら，神山教授が述べておられるように，他人の識別符号を利用する行為が「不正の指令を与え」たと解する余地があるとしても，無権

限者によるコンピュータの使用が他人の業務を妨害することは，通常考えられない。また，電子計算機損壊等業務妨害罪の法定刑の加重理由としては，「重大かつ広範な被害を生じる可能性がある」という以上の説明はなされず，結果の重大性を示す文言が何ら条文化されていないことからも，利益窃盗の無限定な処罰を回避するためには，立法趣旨に沿った厳格な運用が求められよう。

（3）不正アクセス助長罪の問題点

不正アクセス禁止法は，不正アクセス助長罪という形で他人の識別符号を無断で第三者に提供する行為をも処罰している。不正アクセス行為をするためには，識別符号やセキュリティ・ホールの探知行為が必要となるが，そのためには，クラッキング・ツールの利用やソーシャル・エンジニアリング[40]の利用について，ある程度専門的知識・技術を必要とする場合がある。しかし，他人の識別符号を入手することができれば，容易に不正アクセスを行うことが可能となってしまう。本罪は，不正取得や不正保管と異なり，行為者の目的を要件としていないが，他人の識別符号を提供する行為は提供者の目的如何にかかわらず，提供を受けた者が容易に不正アクセス行為を実行することを可能とする点で，不正アクセス行為を実行することを可能とするものであり，放置すると不正アクセス行為の禁止の実効性を損なうことになるとともに，外形的行為自体に法益侵害の高度の危険性が認められることになる。

旧法4条は，「何人も，アクセス制御機能に係る他人の識別符号を，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，当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。ただし，当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合は，この限りでない。」

としていたが，今回の改正により，ただし書が削除され，「何人も，業務その他正当な理由による場合を除いては，アクセス制御機能に係る他人の識別符号を，当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。」と改められた。アクセス管理者が，自らが管理する他人の識別符号を提供するような行為は，通常，「業務その他正当な理由による場合」[41]に該当するためである。

罰則においては，提供者が提供行為を行うに当たり，提供の相手方に不正アクセス行為の用に供する目的があると知りながら提供する場合と，そうでなく提供する場合とでは，加えるべき法的非難の程度には差があるとして，前者の場合の法定刑は不正取得罪や不正保管罪と同様に１年以下の懲役又は50万円以下の罰金とされ（改正法12条２号），後者の場合には，旧法と同じく30万円以下の罰金とされた（改正法13条）。

しかし，不正アクセス禁止法が，不正アクセス助長行為を犯罪化したこと，改正法によって知情提供か否かで構成要件を分け，知情提供行為の法定刑を旧法における不正アクセス罪と同様とした点は評価できるとしても，他人の識別符号を無断で第三者に提供する行為は，セキュリティの高さのみで対抗できるものでなく，不正アクセスと同等か，あるいはそれ以上に「電気通信に関する秩序」を損ねかねない行為といえる。したがって，この点に関しては，少なくとも改正法において引き上げられた不正アクセス罪と同等の法定刑まで引き上げるべきであろう。

（４）フィッシング罪の問題点

不正アクセス禁止法の改正により，フィッシング行為の一部が犯罪化された。フィッシング行為は，識別符号の不正取得の前段階の行為に当たるが，識別符号の不正探知行為自体が有する危険性から，不正取得とは別の独立した行為として禁止されたことについては評価できる[42]。

改正法において犯罪化されたフィッシング行為は，警察庁の定義した

「銀行等の企業からのメールを装い，メールの受信者に偽のホームページにアクセスするよう仕向け，そのページにおいて個人の金融情報（クレジットカード番号，ID，パスワード等）を入力させるなどして個人の金融情報を不正に入手するような行為」[43]を前提としているようである。

確かにフィッシング行為の多くは，偽装メールと偽サイトにより識別符号を送信させる手口であるが，フィッシング行為には，様々な形態のものがあり，ソーシャル・エンジニアリングにより利用権者になりすましてアクセス管理者から直接聞きだす方法や，アクセス管理者になりすまして利用権者にファックスで個人情報を送信させる手口，クロスサイト・スクリプティング（XSS）脆弱性を利用した手口等もあり，必ずしも偽装メールと偽サイトにより識別符号を送信させる手口や偽装メールの返信として個人情報を送らせる手口だけで成り立っているわけではない。

改正法7条1号は，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禁止規定となっている。本条では，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，当該サイトに識別符号を「入力することを求める旨の情報」があることが要件となる。典型的には，識別符号を入力するよう求める文章や，入力欄および送信用のボタンを表示し，アクセス管理者の名称や商標等を用い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偽装サイトを構築し，ネットワーク上に公開して公衆が閲覧できる状態に置く行為が該当することになる。

XSS脆弱性を利用すると，細工を施したリンクをユーザにクリックさせることで，XSS脆弱性が存在するWebサイトを経由して，任意のHTMLをユーザのブラウザに送り込める。すなわち，スクリプトの実行によってブラウザに表示されるページを動的に書き換えることができるため，コンテンツの一部を改変したウェブサイトを表示させることが可能となる。具体的には，ドメイン名もサーバ証明書も本物のウェブサイト上に嘘の情報

を追加したり，偽の入力フォームを作成したりすることが可能となる。したがって，XSS 脆弱性を悪用して Web ページ上に追加された嘘の情報や，偽の入力フォームは，URL やデジタル証明書（SSL 証明書）を確認しても，偽物であることは分からないため，ユーザは識別符号等を詐取されようとしていることに気付かないまま識別符号等を入力させられ，入力された記録を悪意のある第三者に送信されてしまうことがありうる。

XSS 脆弱性を使ったページの偽装が可能かどうかは，そのサイトのページ構成などに依存するとされているが，XSS 脆弱性が存在するサイトのほとんどで，ページの偽装が可能だといわれている。偽サイトの構築よりも，正規サイトに偽装リンク等を埋め込まれて改変されるフィッシングの方が，被害者がより被害に気付きにくい点で深刻である。

XSS 脆弱性によりフィッシャーが識別符号を詐取する手順としては，以下のものが考えられる。

①フィッシャーは，XSS 脆弱性のあるサイトにユーザを誘導するためのサーバを事前に立ち上げておき，そこに識別符号やユーザ端末の個人識別情報等を収集サイトに送る内容のスクリプトを含んだリンクを仕掛け，偽の案内メールなど何らかの手段を使ってユーザを，誘導サイトにアクセスさせる。

②ユーザが誘導サイトにアクセスすると，ブラウザに誘導サイトのページが表示され，誘導サイト上のリンクをクリックすると，正規サイトに遷移する。

③正規サイト上で動作している Web アプリケーションに脆弱性があるため，ユーザがリンクをクリックした際に，リンクに仕込まれた悪意のスクリプトが正規サイトに埋め込まれる。

④③のスクリプトは，正規サイトに個人識別情報を送信するとともに，当該スクリプトをそのままユーザ端末に返送し，ユーザ端末は受け取ったスクリプトを実行することで，情報をフィッシャーの情報収

集サーバに送信する。

改正法7条1号では，「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になりすまし，その他当該アクセス管理者であると誤認させて，次に掲げる行為をしてはならない」との要件を付しているが，この要件は，アクセス管理者そのものであると偽ることのみならず，アクセス管理者であるかのような紛らわしい表示を用いることにより，アクセス管理者であると誤って認識させることを意味するものである。また，「入力することを求める旨の情報」に該当するかは，公開されたウェブサイト上の表示全体から総合的に判断される。

XSS脆弱性に基づき，識別符号を送信するスクリプトが埋め込まれている場合には，偽の入力フォームなどは本物のサイトの一部として表示される。入力フォームだけみれば，「入力することを求める旨の情報」に該当することになるが，正規のアクセス管理者が公開したウェブサイトのであるため，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って認識させるものではない。また，上記②の段階で構築・公開されている誘導サイトは，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って認識させるものではあるが，単なるリンクは，「入力することを求める旨の情報」には該当しない。したがって，XSS脆弱性を利用したフィッシング行為の場合には，フィッシング罪の構成要件には該当しないことになり，処罰の間隙が生じていることになる[44]。

では，この悪意のスクリプトを正規サイトに埋め込むことは，不正指令電磁的記録に関する罪に当たるのであろうか。

刑法168条の2第1項1号は，人の計算機における実行の用に供する目的で，「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず，又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」の作成，提供，取得，保管を処罰し，同2項において供用を可罰化している。

電子計算機は今日の社会において重要な機能を有するため，不正なプログラムが実行された場合広く社会に被害を与えることになり，これを放置すれば正当な使用者は電子計算機による情報処理のためのプログラムを信頼して実行することができなくなり，電子計算機による情報処理がうまく機能しなくなることが考えられる。このため，不正指令電磁的記録に関する罪の保護法益は，電子計算機のプログラムに対する社会一般の者の社会的信頼であると考えられる。

不正指令電磁的記録に関する罪にいう「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず，又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」とは，使用者の意図と異なる動作を電子計算機にさせる不正な指令を与える電磁的記録をいう。プログラムに対する社会的信頼という保護法益からすると，不正な指令が与えられることで動作阻害が生じたといえるためには，一般通常人がプログラムを使用するにあたって想定すべき用途・動作と異なる動作が行われたか否かを問題とすべきであろう。すなわち，当該電磁的記録が不正指令電磁的記録であることを知らない人の電子計算機において，使用者の実質的利益を害するような，使用者の想定していない動作の指令を与えることが不正な指令を与えるということであり，この不正の指令により一般の使用者が想定すべき用途・動作と異なる動作をさせる電磁的記録が不正指令電磁的記録ということになる。

通常，スクリプトとは，プログラムはプログラマの書いたソースコードをもとにコンピュータの理解できる機械語に変換して実行されるが，そのプロセスを自動化して簡単に実行できるようにしたものをいい，Web ページ上では，HTML だけではできない様々な機能を利用するための簡易的なプログラムを指すことがある。XSS 脆弱性攻撃は，アプリケーションの脆弱性ゆえに，スクリプトの機能を悪用するものである。スクリプトは，定められた文法に乗っ取っていれば自動的に動作するものであるため，不

正指令電磁的記録に関する罪にいう「不正指令電磁的記録」に当たらないようにもみえる。しかし，不正指令電磁的記録であるといえるためには，人の電子計算機において，使用者の想定される動作と異なる動作の指令を与えれば足りるのである。XSS の手順をみればわかるように，情報を送信するスクリプトがユーザ端末に送信され，意図した送信先とは別のところにも情報を送信させられた場合には，当該スクリプトは，「不正指令電磁的記録」の要件を充たすことになる。

不正指令電磁的記録に関する罪が成立するためには，「人の電子計算機における実行の用に供する目的」という供用目的が必要である。すなわち，電子計算機の使用者の意図と異なる動作をさせる指令を与えることの目的をいうことになる[45]。XSS の場合には，使用者は実際の動作を認識せずに，スクリプトが実行されるのであるから，個人情報を送信させる目的で，悪意のスクリプトを埋め込む場合には，供用目的があるといってよい。

不正指令電磁的記録に関する罪の実行行為としては，不正指令電磁的記録の作成，提供，供用，供用未遂，取得，保管が規定されており，供用・供用未遂は刑法168条の 2 第 1 項 1 号に規定された実行可能な不正指令電磁的記録に客体が限られているが，他の場合には同条 1 項 1 号に限らず 2 号のものも客体に含まれる。

では，供用目的でのスクリプトの挿入が「作成」といえるのであろうか。「作成」とは，不正指令電磁的記録等を新たに記録媒体上に存在するに至らしめることをいう。作成が既遂に達するためには，「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず，又はその意図に反する動作をさせるべき不正な指令」として機能し得る内容のものを実質的に存在するに至らしめることを要する。識別符号を送信させるスクリプトは，XSS 脆弱性を利用して正規サイトに埋め込まれた段階で，「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず，又はその意図に反する動作をさせるべき不正な指令」として機能し得る内容のものを実質

的に存在するに至らしめることとなるのであって，最終的に不正指令電磁的記録に該当する場合があり得るとしても，スクリプトを作り出した段階ではいまだ「作成」と評価することはできないと思われる。

したがって，スクリプトの挿入行為は，不正指令電磁的記録を，不正指令電磁的記録であることの情を知らない第三者のコンピュータで実行され得る状態に置いたにすぎないため，供用罪（刑法第168条の２第２項）としての評価にとどまるであろう。

サイト構築型およびメール送信型フィッシング行為が犯罪化されたことにより，今後は両者以外の犯罪化されていない形態のフィッシング行為が増加する懸念がある。とりわけウェブ・アプリケーションの脆弱性を利用したフィッシング行為は，アクセス管理者が公開した正規のウェブサイトを悪用するだけに，コンピュータ・ネットワーク利用者のアクセス制御機能に対する信頼を大きく損なうものである。先に検討したように，ウェブ・アプリケーションの脆弱性を利用したフィッシング行為の場合には，不正指令電磁的記録供用罪で補足できる場合もあり得るが，フィッシング行為独自の当罰性ゆえに規定を制定した経緯からすると，「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」という本法の目的を達成するためには，少なくともウェブ・アプリケーションの脆弱性を利用したフィッシング行為を含めた規定に改めるべきであろう。

Ⅵ　おわりに

以上みてきたように，不正アクセス行為は，嫌がらせや仕返しといった経済的利益を意図しない攻撃から，不正に金を得るためや，オンライン・サービスで不正操作を行うためといった攻撃者の経済的利益を確保する攻撃へと変化してきていることが明らかになった。

実態把握の方策として，不正アクセス行為の発生件数を量的に把握し，

その傾向や特徴を分析，分類することが重要になるが，統計情報をそれぞれ公表している警察庁，IPA，JPCERT/CC において，各組織が独自の考え方に基づき件数の単位や分類等を行っており，現状においては，各組織の公開されている各組織の統計情報は，そのままでは単純な相互比較しかなしえず，有意な統計情報とはなっていないことも明らかとなった。今後も不正アクセス行為を量的に把握するためには，各組織間で共通となる統計の枠組みについても検討を行う必要があるだろう。

不正アクセス行為に対処するための方策は，大別して三つ考えられる。

不正アクセス行為をめぐる問題は，技術に対する依存度が極めて高く，また技術の進展の早さゆえに行政上の対応は遅れがちであることから，必然的に技術的対応も検討する必要がある。生活の各部面におけるオープン・ネットワークの利用が拡大すればするほど，外部のコンピュータとの接続機会は増えていく。そのため，ICT が我々の社会活動を支える上で，そのプラットフォーム自身の技術的信頼性を確立することが不可欠となってくる。

そして，優れた技術でコンピュータ・システムやネットワークをいくらセキュアにしても，それを利用するのは人である。与えられた指令を忠実にこなすコンピュータと異なり，人は，感情，利益，慣れなどによって容易に行動を変えてしまうことがある。そのため，現在の情報社会を主体的に生きていくために，我々自身が生活者としての立場で，セキュリティの問題に対し関心を持ち，情報倫理の視点をもって克服していくことが大事なものとなる。

しかし，コンピュータ・ネットワークが社会インフラ化し，多様な人々が利用をしている今日にあっては，個々人の内面的倫理観だけに頼る時代ではなくなってきている。そのため，より広い立場からの対応として，その法的対応，とりわけ加害行為に対する刑事法的対応を検討する必要がある。

不正アクセスは，ソーシャル・エンジニアリングによるパスワード窃取の例のように，技術的手段だけでは防ぎ得ないこともあるので，処罰することについて一定の合理性が認められる。コンピュータおよびコンピュータ・ネットワークの社会経済的重要性が増大しつつある今日においては，システム自体に法的保護を与えることは必要であろう。

2011（平成23）年に成立した情報処理の高度化等に対処するための刑法等の一部を改正する法律（法律74号）（刑法一部改正法）により，サイバー犯罪条約を締結するための法整備が行われたが，その中で，不正アクセス禁止法を改正し，不正アクセス罪について一定の範囲で国外犯を処罰することとし，刑法４条の２の例によることとする規定を設けた（刑法一部改正法６条）[46]。同規定の施行期日はサイバー犯罪条約の効力発生日とされており，サイバー犯罪条約は2012年11月１日より，我が国についての効力が発生する予定である。

本条約での効力が我が国でも発生することを踏まえれば，今後は，可罰的行為の適切な処罰や，捜査手続の迅速・円滑な実施のみならず，個人情報の保護や，民間事業者への過重なコスト負担の回避という観点も踏まえた上で，国際的にも調和のとれた，バランスのとれた法制度の整備を目指す必要があろう。

高度情報通信ネットワーク社会形成基本法22条は，「高度情報通信ネットワーク社会の形成に関する施策に当たっては，高度情報通信ネットワークの安全性及び信頼性の確保，個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない」としている。また，不正アクセス禁止法８条においても，「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，当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに，常に当該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

きは速やかにその機能の高度化その他当該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する。」とされており，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，個々のアクセス管理者が自ら防御措置を講ずべき責務があることを法律上明確に定め，アクセス管理者に防御措置の実施を促している。

刑法の断片性，補充性，謙抑性といった基本的な性格に加えて，現代の刑法・刑事政策思想からコンピュータの普及がもたらした犯罪化，刑罰化の方向は，その行き過ぎを戒められなければならない。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である。そのためには，刑罰による威嚇に頼りすぎることなく，セキュリティ向上などの合理的・効果的な施策を講じていくことこそが，重要である。

注

1　警察庁「インターネットバンキングに係る不正アクセス禁止法違反等事件の発生状況等について」〈http://www.npa.go.jp/cyber/warning/h23/111215_1.pdf〉（2012年9月19日確認）によると，フィッシングで取得した識別符号や，何らかの方法でインターネットバンキング利用権者の端末に不正プログラムを送り込み，利用権者の知らない間に取得された識別符号を使いインターネットバンキングに不正アクセスし，他人の口座へ送金する事案が多発していると報告されている。2012（平成23）年3月末以降，11月24日までの都道府県警察から報告された被害状況は，35都道府県の56の金融機関の160口座（未遂40口座を含む。）が被害にあい，不正送金総額は約3億円になるという。

2　フィッシング行為の可罰化について，2011（平成22）年11月に一般社団法人eビジネス推進連合会（現：新経済連盟）から（参考資料〈http://jane.or.jp/img/pdf/ebusiness_shoshu2012.pdf〉（2012年）4頁（2012年9月19日確認）），同年12月には一般社団法人全国銀行協会から（2011年12月16日日本経済新聞朝刊），それぞれ，国家公安委員会委員長宛てに要望書が提出された。

3　野村総合研究所が2009（平成21）年3月に行った，全国の16歳以上69歳以下の男女を対象としたインターネットで使用するIDとパスワードに関する意識についてのアンケート調査では，サイトへのログイン時などにID・パスワードを自分で設定する場合にどのようにしているかという項目では，「すでに自分が持つ『いく

つかのID・パスワードから選んで設定する』」人が66.7%，「ひとつに統一する」人が25.8%であり，9割以上の回答者が少数のＩＤ・パスワードを複数のサイトで併用しているという回答であった。

IDとパスワードを使ってログインするサイト数を利用頻度別に聞いたところ，「ほぼ毎日使うサイト」は平均6.7サイト，「たまに使うサイト」も平均6.7サイトで，これらを合わせると，インターネットユーザーがIDとパスワードを使ってログインするサイト数は平均13.4，「IDは持っているがほとんど使わないサイト」（平均5.8サイト）を加えると，その数は平均19.2サイトとなっており，Webメール，ネットショップ，ネットバンキングが使用頻度の高いサイトとなっている。また，インターネットユーザーが確実に記憶できるID・パスワード数の平均は3.1組となり，ログインするサイト数とのギャップが見られた（野村総合研究所「インターネットユーザーのIDに関する意識についてアンケート調査を実施」（2009年）〈http://www.nri.co.jp/news/2009/090611.html〉（2012年9月19日確認））。

4　総合セキュリティ対策会議『安全・安心で責任あるサイバー市民社会の実現に向けた対策について　平成22年度総合セキュリティ対策会議　報告書』（2011年）〈http://www.npa.go.jp/cyber/csmeeting/h22/pdf/pdf22.pdf〉

5　官民ボード「不正アクセス防止対策に関する行動計画」（2011年）〈http://www.npa.go.jp/cyber/kanminboard/ketteijikou/honbun.pdf〉（2012年9月19日確認）

6　犯罪に関する欧州評議会（Council of Europe）によって1996（平成8）年11月に設立されたサイバー犯罪に関する専門家委員会は，コンピュータおよびインターネットを利用した様々な犯罪に対する検討を行い，そのような犯罪に対する包括的な条約いわゆるサイバー犯罪条約の最終案を2000（平成12）年12月22日に発表した。同条約は2001（平成13）年11月8日に正式に採択され，アメリカやカナダなどとともにオブザーバーとして検討に参加してきた我が国も同年11月23日に同条約に署名し，2004（平成16）年4月21日に国会でその締結につき承認を得た。そして，同年7月1日に効力が発生した。2011（平成23）年6月17日には，国内担保法（情報処理の高度化等に対処するための刑法等の一部を改正する法律（平成23年法律74号））が成立し，サイバー犯罪条約は，2012（平成24）年7月4日に公布および告示がなされ（平成24年条約7号および外務省告示231号），11月1日より，我が国についての効力が発生する予定である。

サイバー犯罪条約は，第1章から第4章までの4章48条文で構成されている。第1章では基本用語の定義，第2章では，刑事実体法として，コンピュータ・システムへの「不正アクセス（Illegal access）」（2条），コンピュータ・データの「不正傍受（Illegal interception）」（3条），「データ妨害（Data interference）」（4条），「システム妨害（System interference）」（5条），「装置の濫用（Misuse of device）」（6条），「コンピュータ関連偽造（Computer-related forgery）」（7条），「コンピュータ関連詐欺（Computer-related fraud）」（8条），「児童ポルノ関連犯罪

（Offences related to child pornography）」（9条），「著作権および関連諸権利の侵害に関連する犯罪（Offences related to infringements of copyright and related rights）」（10条）をサイバー犯罪とし，構成要件を規定するとともに，コンピュータ・データの応急保全や部分開示，捜索・押収，トラフィック・データ（通信記録）のリアルタイム収集や通信内容の傍受などに関する手続法を定め，第3章においては，第2章で規定した犯罪についての相互援助および引渡し命令を含む国際協力について規定し，第4章では最終条項として，欧州評議会条約の標準規定について述べている。

サイバー犯罪条約は，情報通信技術の急速な発達により，国境を越えたコンピュータ・ネットワークの利用が可能となったことに伴い，コンピュータおよびコンピュータ・ネットワークに関連する犯罪も増加している状況を受け，サイバー犯罪対策分野における国際的な法的枠組みを定めた世界初の条約であり，サイバー犯罪に効果的かつ迅速に対処するために国際協力を行い，共通の刑事政策を採択することを目指しているものであるとされる。

なお，サイバー犯罪条約については，園田寿「サイバー犯罪条約」現代刑事法3巻9号（2001年）29頁以下，石井徹哉「サイバー犯罪条約に関する覚書き」奈良法学会雑誌15巻1・2号（2002年）47頁以下，サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」（2002年）〈http://www.meti.go.jp/policy/netsecurity/downloadfiles/Cybercriminallawreport.pdf〉（2012年9月19日確認），*Mike Keyser, The Council of Europe Convention on Cybercrime*, 12 J. Transnational L. & Policy 287-326（2002-2003），*Amalie M. Weber, The Council of Europe's Convention on Cybercrime*, 18 Berkeley Tech. L. J. 425-446（2003），*Miriam F. Miquelson-Weismann, The Convention on Cybercrime: A Harmonized Implementation of International penal Law: What Prospects for Procedural Due Process?*, 23（2）J. Marshall Computer & Information L. 329-361（2005）等参照。

7　蔵原智行「法令解説　フィッシング行為，ID・パスワードの不正取得等の禁止・処罰等」時の法令1909号（2012年）12頁。

8　警察庁の蔵原氏は，「一般人が，ある企業のID・パスワードのリストがインターネット上に流出しているとの情報に接し，当該情報の真偽を確かめることを目的に当該リストを検索し，自らが使用するパソコンの映像面に表示させた場合，その行為は他人の識別符号の不正な（無権限の）取得であるが，目的要件があることにより，このような行為が禁止・処罰の対象から除外される」としている（前掲注7論文12頁）。

9　他人の識別符号を，事実上相手方が利用できる状態に置くことをいう。

10　インターネット上に流出している他人の識別符号を，不正アクセス行為の用に供する目的で，自らが使用するコンピュータのディスプレイに表示させる行為等がこれに該当すると思われる。

11　識別符号不正保管罪で初めて摘発されたと報じられたのは，不正アクセスする目的で，以前に交際していた相手のインターネット通販で使う ID とパスワードが記された手帳を不正に取得し保管していたという事案であった（2012年 9 月14日毎日新聞，読売新聞，朝日新聞，産経新聞夕刊）。

12　米国のフィッシングの手口や対策を調査する団体 Anti-Phishing Working Group（APWG）は，2012年 2 月にフィッシングサイトの数が56,859件にも上り，過去最高を記録したと報告している（*Phishing Activity Trends Report 1st Quarter 2012*, 4（2012）〈http: //apwg. org/reports/apwg_trends_report_q1_2012. pdf〉（2012年 9 月19日確認））。フィッシング対策協議会の報告書においても，日本国内でのフィッシングサイトの件数が，2009 年度の260件から，2010年度は516件，2011年度は582件と増加していると報告されている（フィッシング対策協議会「フィッシングレポート 2012」〈https: //www. antiphishing. jp/report/pdf/phishing_report_2012. pdf〉（2012） 1 頁（2012年 9 月19日確認））。

13　東京地判平成17年 9 月12日公刊物未登載（TKC 文献番号28135296）においては，フィッシングサイトを作るに当たり，他人が開設したホームページ画面のタイトル部分を書換えるなどしたホームページ画面を複製し，これをインターネット上で公開した行為を著作権法違反としている。

14　京都地判平成20年 4 月18日公刊物未登載（LLi 文献番号06350106）では，被告人は，自ら設置したフィッシングサイトを通じて入手した他人のクレジットカード情報等を用いてオークションサイトに会員登録等しているが，不正アクセス禁止法違反には問われているものの，フィッシングサイトの開設について著作権法違反等には問われていない。

15　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などに関する法律［第 2 版］』立花書房（2012）98頁において，立法当局者は，フィッシング行為を犯罪化した理由の一つとして，「アクセス管理者であると誤認させて利用権者に識別符号を入力させようと仕向ける行為は，……何らの社会的有用性が認められないものであ」り，フィッシング行為の悪質性と危険性を踏まえて犯罪化したと説明している。しかしながら，刑法の目的は，法益保護にあるのであって，法益を侵害するか，あるいは危殆化する行態だけが社会侵害的なものであり，それのみが犯罪化することを許されているのである（Hans-Ludwig Günther, *Die Genese eines Straftatbestandes: Eine Einführung in Fragen der Strafgesetzgebungslehre*, 1 JUS 9（1978）.）。フィッシング行為が犯罪化されたのは，「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」を目的の一つとしている不正アクセス禁止法の「アクセス制御機能に対する社会的信頼」という法益を危殆化する行為だからであり，行為が社会的有用性を有していないという行為反価値性から基礎づけられるべきではない。

16　園田寿・野村隆昌・山川健『ハッカー VS. 不正アクセス禁止法』日本評論社

（2000年）239頁，248頁，「検証不正アクセス対策法」ハッカージャパン4号（1999年）147頁，151頁等。

17　前掲注15『逐条』142頁。

18　前掲注15『逐条』136頁によると，2012年4月現在における「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が第八条の規定により講ずる措置を支援することを目的としてアクセス制御機能の高度化に係る事業を行う者が組織する団体」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およびフィッシング対策協議会がこれに該当するものと考えられるとされている。なお，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，上記2団体に限られるものではなく，要件を満たせば本条にいう団体に該当し，団体の法人格の有無は問われない。

19　「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。）」

20　(a)「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。）」（改正法2条4項2号）

(b)「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」（改正法2条4項3号）

21　判タ1213号314頁，判時1899号155頁。

22　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19巻3号（2004年）30頁以下，園田寿「不正アクセス禁止法における『不正アクセス』の概念について」甲南法務研究1号（2005年）111頁以下参照。

23　ネットワーク上において行為者が利用する電子計算機と特定利用の制限および制限の解除の指令を行うアクセス制御を行うコンピュータが同一の場合がこれに該当する。

24　ネットワーク上において特定利用の制限および制限の解除の指令を行うアクセス制御を行うコンピュータと行為者が利用する電子計算機とが別個の場合がこれに該当する。

25　この点について，大橋検事は，「特定電子計算機をサービス（プロセス）と捉えると」，同一のサービス（プロトコル）である限り，「特定利用を制御する機能が付加されたコンピュータが入力対象のコンピュータとは別のコンピュータであって，複数のコンピュータが存在する場合であっても」，全体として１つの特定電子計算機となり，条文の規定と矛盾すると述べておられる（大橋充直「検証　ハイテク犯罪の捜査　情報漏えい犯罪の新判例（ACCS 事件）」捜査研究647号（2005年）74頁）。

26　今井猛嘉「『不正アクセス』の意義をめぐって」研修719号（2008年）10頁。

27　今井・前掲注26論文，同「ネットワーク犯罪」法学教室303号（2005年）55頁。

28　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５巻１号（2006年）27頁。

29　前掲注15『逐条』69頁。

30　前掲注15『逐条』66頁。

31　西田典之『刑法各論［第６版］』弘文堂（2012年）217頁以下。

32　立案担当者は，有償によるサービス対価の支払いを免れた場合には，電子計算機使用詐欺罪を適用しないと説明してきた（米澤慶治編『刑法等一部改正法の解説』立花書房（1988年）131頁以下）。なお，自己の課金ファイルを改竄して国際電話の通話料金支払いを逃れたという事案について，電子計算機使用詐欺罪を認めた事例として，東京地判平成７年２月13日（判時1529号158頁）がある。

33　日弁連刑法改正対策委員会編『コンピュータ犯罪と現代刑法』三省堂（1990年）181頁。

34　鶴田六郎・横畠裕介「刑法等一部改正法概説（３）」警察学論集40巻10号（1987年）203頁，団藤重光『刑法綱要各論［第３版］』創文社（1990年）687頁，大塚仁『刑法概説各論［第３版増補版］』有斐閣（2005年）490頁，大谷實『刑法講義各論［新版第３版］』成文堂（2009年）465頁等。なお，「不正に」の文言に，権限を濫用して虚偽記録を作出する場合を含むかにつき争いがある（山口厚「電磁的記録と文書犯罪規定の改正」ジュリスト885号（1987年）８頁，中森喜彦「コンピュータ犯罪と刑法の一部改正」法学教室81号（1987年）90頁）。

35　西田典之「コンピュータと業務妨害・財産罪」刑法雑誌28巻４号（1988年）517頁。

36　西田・前掲注35論文517頁。

37　横畠裕介「刑法等一部改正法概説（４）」警察学論集40巻11号（1987年）115頁。

38　神山敏雄「コンピュータ犯罪立法の批判的考察」法律時報60巻１号（1988年）80頁。

39　芝原邦爾「コンピュータによる情報処理と業務妨害罪」ジュリスト885号（1987年）15頁。

40　1980年代にハッカーたちは，技術的でない手段によって情報を得るための戦略

を説明するためにこの言葉を使い始めたという（Ira Winkler, Corporate Espionage 94（1997）（稲垣伸子訳『現代産業スパイ事情』日経BP社（1998年）127頁））。

『ハッカーズ大辞典』によると「ソフトウエアではなくウェットウエア（wetware）の弱点を利用したクラッキングテクニックを表す。これの狙いは，人をだまして，狙ったシステムのセキュリティを危険にさらすパスワードその他の情報を暴露させること」をいうとされる（Eric S. Raymond ed., The New Hacker's Dictionary 3rd ed.（1996）（福崎俊博訳『ハッカーズ大辞典（改訂新版）』アスキー（2002年）520頁））。

41　法律上，「業務その他正当な理由」の有無が問題とされるものとしては，「業務その他正当な理由による場合」を除いて，刃体の長さが6 cmを超える刃物を携帯してはならないとする銃砲刀剣類所持等取締法（以下，銃刀法）22条のほか，「何人も，業務その他正当な理由による場合を除いては，模造刀剣類（金属で作られ，かつ，刀剣類に著しく類似する形態を有する物で内閣府令で定めるものをいう。）を携帯してはならない。」とする同法22条の4，「業務その他正当な理由による場合」を除いて特殊開錠用具の所持を禁止する特殊開錠用具の所持の禁止等に関する法律（以下「ピッキング防止法」）3条，「業務その他正当な理由による場合」を除いて指定侵入工具の隠匿携帯を禁止する同法4条，「業務その他正当な理由によることなく所持することの情を知って特殊開錠用具を販売し，又は授与した者」を処罰する同法15条，「引火性，発火性又は爆発性のある毒物又は劇物であって政令で定めるものは，業務その他正当な理由による場合を除いては，所持してはならない。」とする毒物及び劇物取締法（以下，毒劇法）3条の4，その罰則規定であり「業務その他正当な理由によることなく所持することの情を知って第3条の4に規定する政令で定める物を販売し，又は授与した者」を処罰する同法24条の2第2号でも「業務その他正当な理由」という文言が使用されている。

「業務」とは「人が職業その他の社会生活上の地位に基づき，継続的に行う事務又は事業」であり，「その他正当な理由」とは，銃刀法においては，社会通念上その刃物を携帯することが当然に認められるような理由を想定しているとされる。ピッキング防止法においては，指定侵入工具を所持することが，職務上あるいは日常生活上の必要性から，社会通念上，正当と認められる場合をいうと解されており，そのような正当な理由に該当するか否かは，特殊開錠用具を所持する者の職業や周囲の状況等の客観的要素，その者の当該携帯に係る動機，目的，認識等の主観的要素を総合的に勘案して判断すべきものと解されている。さらに，毒劇法においては，社会通念によって決せられ，毒物又は劇物営業者がその業務上当然に所持する場合や，研究・鑑定等の目的で所持の必要がある場合などがこれに当たるとされている。したがって，本罪における「業務その他正当な理由」も，他人の識別符号を有する者が，利用権者以外の者に識別符号を提供することが，職務上あるいは日常生活上，または研究等の目的で必要がある場合に認められ，

社会通念によって判断されることになる。

42　諸外国においては，2012年の不正アクセス禁止法改正前の我が国と同様に，当該フィッシング行為が他の刑罰法規に触れる限りにおいて規制している。英国の2006年詐欺法２条，７条，米国の連邦刑法典1028条（a）（７），1028A 条，1029条，ドイツ刑法典263a 条，フランス知的所有権法 L713条，刑法典226-18条，313-1条，434-23条等参照。

43 「いわゆる『フィッシング』事案への注意喚起について」（警察庁）〈http://www.npa.go.jp/cyber/warning/chuikanki/170527.htm〉（2012年９月15日確認）。

44　もちろん，ここで得られた識別を取得・保管すれば，識別符号不正取得罪・保管罪は成立することになり，識別符号を使用すれば識別符号窃用型不正アクセス罪に該当する。また，当該サイトで取得された cookie 等を利用してセッションハイジャックのアクセスをすれば改正法２条４項２号のセキュリティホール攻撃型不正アクセス行為に該当し，処罰は可能であると思われる。

45　電子計算機の使用者が不正指令電磁的記録であることの認識を欠いていること，すなわち，電子計算機の使用者において実際の動作，それが意図に反する動作をすることを認識していないことが前提となる。

46　不正アクセス禁止法律の一部を改正するとして，旧法８条に２項を新設し，「前項第一号の罪は，刑法（明治40年法律第45号）第４条の２の例に従う。」とした。この規定は，2012年の改正において，14条に改められ，「第11条及び第12条第１号から第３号までの罪は，刑法（明治40年法律第45号）第四条の二の例に従う。」とされた。

【付記】

裁判例の収集にあたっては，奥村徹弁護士に貴重な資料を御提供いただき大変お世話になった。ここに深謝する次第である。