不正アクセス禁止法制とインターネット

浜田　良樹

財団法人日本資産流動化研究所 研究部
東北大学大学院情報科学研究科博士後期課程
105-0001 東京都港区虎ノ門 1-19-9 虎ノ門 TBL ビル 3 F
TEL:03-3506-1071 FAX:03-3506-1080
E-mail:hamada@sfij.or.jp

要旨

コンピュータへの不正アクセスにより被害を受けるケースが最近続出している。日本刑法は現在のところ、単なるデータののぞき見やシステムの無権限利用を処罰していない。だが、これでは諸外国との間で著しく均衡を欠き、国際化するハイテク犯罪に対処できないことから、現在不正アクセス禁止法制の制定が郵政省、警察庁などによって検討中である。ところでインターネットには情報や計算機資源の共有という伝統を引き継ぎ、他人のシステムに迷惑をかけない限りにおいて無権限アクセスも許容される余地があると言う考え方が根強く存在する。本稿では、このような考え方を不正アクセス禁止法制に盛り込むことは可能なのかどうかについて検討し、インターネットにおける不正アクセス禁止法制のあり方を探る。

キーワード：不正アクセス、無権限アクセス、刑法、インターネット、ハイテク犯罪、ハッカー

The act of Unauthorized access to computer systems and the internet

Ryoju Hamada
Researcher, Structured Finance Institute of Japan
Graduated School of Information Science, Tohoku University
3F Toranomon TBL Bldg., 1-19-9 Toranomon, Minato Ward, Tokyo 105-0001 Japan
TEL:+81-3-3506-1071 FAX:+81-3-3506-1080
E-mail:hamada@sfij.or.jp

Abstract

Japanese National Police Agency and Ministry of Postal and Telecommunications, are trying to constitute the act to prohibit Unauthorized Access to computer systems. In this act, any unauthorized access will be purnished without considering his intention, whether he is going to steal personal datas, break the system, or just to access the computer. But especially in the internet, to a certain extent, unauthorized access wasn't apporopriated as a crime. It is required that this act should punish the harmful unauthorized access while supporting internet's tradition. In this essey, We'll try to get one model to solve this problem.

KeyWords: Unauthorized Access, criminal law, internet, high-tech crime, hacker

目次

序論

最近になって不正アクセス事件が各地で続発している。特に 97 年 10 月には NTT 情報通信研究所[*1]、東京大学大型計算機センター[*2]など最先端の研究機関が被害に遭っていたことが次々に判明した。しかし現行法は単なる侵入や課金逃れを処罰していないため、いずれも刑事事件にはなっていない。これでは諸外国との間で均衡を失し、ネットワークの安全が確保できないことになる。警察庁[*3]や郵政省[*4]では現在、この問題が討議される 98 年バーミンガム･サミットを念頭において不正アクセス禁止法制のあり方を検討中である。

ところが世界最大のコンピュータネットワークであるインターネットに対してこれを適用する場合、考えておく必要のある問題が残る。それは被侵入システムに迷惑をかけない限りにおいて技術を研鑽し、あるいは誇示するための侵入が認められるという考え方が存在するという問題である。もちろんインターネットにおいても破壊行為を行うことまでは容認されておらず、何らかの対策が必要であることは確かである。そこで生れるのは、行為者をシステムに侵入し、技術を競うだけの"ハッカー"、システムの破壊などを行う"クラッカー"に峻別し、前者は容認するが後者は処罰するべきだ、と言う考え方[*5]である。

不正アクセス禁止法制において、果たしてこの主張に沿ってハッカーを免責しクラッカーを効率的に処罰するということは可能なのだろうか。以下に検討する。

第 1 節 不正アクセス禁止法制のあり方

(1)不正アクセスとは

(a)定義

世界的に知られた定義としては、1986 年 OECD 最終報告書"コンピュータ犯罪～立法政策の分析"が挙げられる。これによると不正アクセスとは、"情報システムの安全対策を侵害し、またはその他の不法もしくは有害な意図を持ってコンピュータおよび電気通信システムの管理者から権限を与えられることなくなされた故意のコンピュータおよび電気通信システムへのアクセスや傍受"とされている。

日本には 2 つの不正アクセスにかかる定義が存在している。まず通商産業省がガイドライン[*6]を定めており、"システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと"という定義がなされている。また国家公安委員会の基準[*7]は"不正な手段により、ユーザ以外の者が行うアクセス又はユーザが行う権限外のアクセスをいう"としている。"無権限アクセス"とほぼ同義であると考えてよいだろう。

(b)不正アクセスの 3 要素

それでは不正アクセスとはどのような形態を取るものであろうか。以下のような 3 段階のプロセスに分けて考えることができる。

1. 正当な権限がないのに、片端からありそうなパスワードを試す、命令を忍ばせた電子メールを送るなどしてシステムに侵入を試みる（攻撃）。
2. 正当な権限がないのに、攻撃によって得た他人のＩＤを用いて他のシステムをほしいままに利用する行為（なりすまし）
3. システムの破壊、機密データの窃取、改ざんなどの無価値な結果を発生させる（結果発生）。

これらのプロセスは、一見するとまったく無関係にも見える。しかし、それらには厳然とした牽連関係があり、前に位置するプロセスを阻止すればかならず結果の発生を抑止できる[*8]のである。

(2)諸外国の立法例

コンピュータ犯罪が意識されるようになったのは 1980 年代の半ばである。欧米各国は相次いでコンピュータ犯罪を法制化し、ほとんどが無権限アクセスも含めている。

アメリカではフロリダ州、アリゾナ州で 1978 年に制定されたのを皮切りに、連邦刑法は 1986 年に改正[*9]され、現在ほとんどの州において不正アクセスを禁止する法律が存在する。イギリス（1990 年コンピュータ不正使用法）、フランス（1988 年情報処理関連不正行為に関する法律）、カナダ（1984 年刑法）もほぼこれに従っている。ドイツの場合、1986 年改正刑法で OECD の定義にほぼ沿う形で不正アクセスを処罰するほか、同年の不正競争防止法で営業秘密の奪取目的の不正アクセスを処罰している。

不正アクセスをコンピュータ犯罪に含めるかどうかについては日本でも議論された[*10]が、刑法はそもそも設備の無権限使用や単なるデータののぞき見を処罰しておらず、コンピュータシステムに限りこれを処罰することは均衡を欠く。また情報と言ってもその種類によってさまざまな保護形態があり、一律に保護規定を設けることは問題であるなどの理由から立法化は見送られた。結局不正アクセスに関する規定を除いた刑法改正が 1987 年に成立して現在に至っている。

(3)不正アクセスと現在の日本の法律

現在の刑法の限界についてはさまざまな議論[*11]があるが、基本的に何らかの結果が発生した場合に限って犯罪とする姿勢を取っているものと解してよいであろう。刑法にコンピュータ犯罪[*12]として定められているのは以下のようなものである。

・ 人の事務処理を誤らせる目的で、義務または事実証明に関するデータを不正に作った場合、または改ざんされたデータを利用する場合（刑法 161 条の 2）
・ システムを有形的にまたは無形的に破壊し、または妨害する場合（刑法 234 条の 2）
・ データを改ざんして、または虚偽のデータを用いて何らかの処分行為を行わせ、システム運営主体から何らかの処分行為を行わせ、不法の利益を得た場合（刑法 246 条の 2）
・ 公務所の用に供する、または権利または義務に関する他人の電磁的記録を毀棄した者（刑法 258 条、259 条）

最近問題になっている個人情報や企業機密の窃取[*13]を処罰する規定はないなど、その範囲は限定されて狭いものとなっている。

(4)問題点

不正アクセスが処罰されないと言うことは、不正アクセスを心理的に容易にし、その誘因となり得る。現在懸念されるのは、以下のような問題である。

(a)ネットワークの重要性は飛躍的に増大したが、これに比してセキュリティ意識が遅れている。その意味でセキュリティ・ホールが無数に存在しており、これを犯罪に使われる恐れがあること。
(b)ネットワークというものはさまざまなシステムが複雑に接続されており、１個所に対する攻撃の結果が予想もつかぬ場所、想像を超えた規模に拡大する可能性を持っていること。
(c)不正アクセスによって得られる環境は唯一の個人識別情報であるＩＤを偽った状態であり、高度の匿名性が出現すること。匿名性は犯罪の最高の温床である。
(d)外部からの攻撃によってＩＤを入手することに比べて、ひとたび内部に侵入した後で新しいＩＤを入手することはきわめて容易である。このように不正アクセスはさらに多くの不正アクセスを再生産し、もって著しくネットワークを不安定に陥れる。
(e)(2)項で述べたように、現在ほとんどの国において不正アクセスは犯罪とされている。しかしコンピュータネットワークは国境の存在を意識しないから、同じ不正アクセスでも形式的に行為地を日本にすれば処罰されないことになる。さらに日本では不正アクセスは犯罪ではないから、国際捜査共助法２条による諸外国の警察に対する協力をすることができなず（双方可罰性の欠如)、国際的に著しく均衡を欠く。

不正アクセス禁止法制は以上のような問題点を解決する一手段となり得る。

(5)不正アクセス禁止法制のあり方

(a)不正アクセス禁止法制の枠組み

不正アクセスを現状のまま放置することはできない。そこで新しい法律ということになるわけだが、せっかく作るのだから単に不正アクセスを違法であると宣言するだけにとどめず、社会全体で不正アクセスを可能な限り封じ込めるような枠組みを構成することを考えるべきである。

具体的には不正アクセス者のみならず、一般のユーザー、システム管理者、そして当局のすべてが名宛人として一定の義務を負うという形式[*14]が妥当である。

i.当局

違反者を迅速に検挙し、新手の不正アクセスにも柔軟に対応する能力を身に付けることが求められる。また、一般のユーザーを保護するための情報提供、啓蒙活動を行わせるなどの措置も必要である。

ii.システム管理者

そのシステムを一定の安全水準に維持する責任を負うこととする。これでかなりの不正アクセスを防ぐことができる。また攻撃があったときにはこれを放置せず、当局に通報し、捜査のためにログを保全し、ユーザーに警告するなどの措置を講じさせることが不可欠の役割として求められる。

iii.ユーザー

パスワード管理、捜査協力などにおいて最低限の義務を負うと考えるべきである。

(b)不正アクセス者に対する規制

一方、不正アクセス者に対してはどのような規制が行われることになるだろうか。

結果を発生させた場合に処罰されるのは当然[*15]としても、加えてその前プロセスである攻撃となりすましも同様に処罰することが必要であると考えられる。すなわち、

・ 何人も他人が利用するＩＤを不正に入手してはならないし、利用してはならない。
・ 何人も正当に利用する権限のないシステムを不正な方法で操作してはならない。

と、いうことになる。

この他、不正アクセスを容易にする手段

の提供の禁止を盛り込む必要があろう。具体的には、そのような目的に利用するためのソフトの頒布等の禁止、他人のＩＤ情報の頒布等の禁止などが必要になる。

第２節 インターネットとハッキング

(1)不正アクセス禁止法制と行為者の意思

不正アクセス禁止法制は、結果発生の有無を問わず、攻撃・なりすましを禁止する。実際の結果が出る前に処罰するので、当然に行為者が何を企図していたかも問わない。もし不正アクセスが大規模な破壊行為の準備としてなされ、摘発されて処罰されるならば問題ない。しかし、たとえば何ら害意を持たずに単なる好奇心や興味に基づいて大きなコンピュータに接続してみた、というような場合でも同様に処罰されてしまうことには問題がないだろうか。

このようなケースは、特にインターネットにおいては容易に起こり得る。それはインターネットに不正アクセス禁止法制を適用する場合に何らかの問題が発生する可能性を示唆している。

(2) インターネットの歴史とハッカー

インターネットにおいて、不正アクセスはリアルワールドとはやや違う受け止め方をされる場合がある。それは、そのシステムに迷惑をかけない限りにおいて、技術を誇示しあるいは研鑽するための攻撃やなりすましは容認される余地がある、というものである。そういう行為をハッキングと呼び、行為者をハッカーと呼ぶ。

これらの言葉は1970年代にアメリカで生まれたとされる。計算機資源の希少さは、特定の誰かがこれを独占してはならずすべからく平等に使われるべきで、それによって得られた情報もすべからく共有されるべきだという発想を生み出す。さらに誰も使っていない計算機に入り込んで計算をさせても困る者はいない。むしろ資源の有効利用であって推奨されるべきだ、という考え方が生れた。実際ハッキングと言う手法は強いシステムの構築に向けて間違いなく有効だった。また、情報はすべからく共有と言う精神のもとで優秀なソフトウェア[*16]や、RFC[*17]と呼ばれる規約など多くの果実が生まれ、インターネットの大発展の基礎をなしたことは事実である。

しかし、もし不正アクセス禁止法制が行為者の意思を問わず一律に適用されるのであれば、このような良き伝統が葬り去られてしまう可能性を持っている。

(3)ハッカー・クラッカー峻別論

しかし、実際にインターネットにおいてもさまざまな不正アクセスが問題化していることは確かである。そのような行為を行う者に何らかの対策が必要であると言うことは異論を挟む余地がない。そこで出てくるのが、システムへの無権限アクセスを行為者の意思のあり方によって２つに峻別する考え方[*18]である。

a. ハッカー：言葉の語源どおり、技術の研鑽、誇示を目的とする行為者のことで、システムに侵入するが破壊行為や改ざんは行わない。
b. クラッカー：システムに侵入し、データを改ざんしたり窃取したりして被侵入システムに害を与える目的の行為者。

その上で、ハッカーの行為は容認するが、クラッカーの行為は処罰されても仕方がない、という結論が導かれる。これがハッカー・クラッカー峻別論である。

インターネットが世界最大のコンピュータネットワークである以上、不正アクセス禁止法制を制定する際に、その独自の文化や慣習を顧みないというのは確かに不合理

である。しかし法制として、このような立場に基づきハッカーを免責してクラッカーだけを処罰するということは可能であろうか。

第3節 ハッカー・クラッカー峻別論と不正アクセス禁止法制

不正アクセス禁止法制のもとでハッカー・クラッカー峻別論を適用するとすれば、外形的には同じ行為であっても、無価値な結果を発生させる意思の有無によって処罰の有無が分かれるということになる。これを実装した場合、どんな問題が発生するだろうか。

(1)攻撃

不正アクセスの第一段階である攻撃の時点では、攻撃者はネットワークを経由して侵入を試みてはいるが、侵入には至っていない。この場合短時間の間に非常に不自然なログイン失敗や不審な電子メールが集中するので感知しやすい。攻撃を受けたという記録はログインの失敗歴として残る。攻撃者は侵入に成功していないからこの記録を抹消することはできない。

ここで峻別論を導入した場合、クラッカーを処罰することの可否は当該攻撃が何らかの結果を発生させる意思で行われたと言えるかどうかにかかる。しかし外形的に残る記録は単なるアクセスに失敗した履歴であって、その先にどういう行為が準備されていたかを証明する力はない。これをもってクラッキングの意思を持っていたことを断定することは不可能であると言わざるを得ない。行為者は必ずや害意を否認するであろうから、結論としてすべての攻撃が不可罰になってしまうだろう。

(2)なりすまし

なりすましの時点ではアクセスに何らかの形で成功し、システムの内部に侵入している。したがって正規のユーザーがアクセスしていない時刻にアクセスログにログイン成功の履歴が残っていれば証拠[*19]になる。また、その行為者が行った操作記録もシステム内部に残り、これを解析することによって侵入者が何を試みていたのかを明らかにできる可能性がある。

ここで峻別論を導入する。最初に懸念されるのは、許されるハッキングと言う概念がきわめてあいまいであり、侵入者の勝手な解釈を許す恐れが高いことである。どこまで許されるかについて、明確なコンセンサスはない。行為者は自ら行った行為について、その多寡にかかわらずこれは善意のハッキングであると主張することができる。客観的な定義がない以上、それを一概に否定し去ることは難しい。

次に、操作記録といってもしょせんは計算機に対する指令であって、その表現方法は自ずから限定されている。同じ命令やプログラムであってもまったく違った目的で使用される場合があり、行為者の善意害意を明らかにすることが困難な場合も発生することが予想される。しかも行為者は内部への侵入にすでに成功しており、その証拠を隠滅することが容易にできる。意思をあらわす可能性がある唯一の証拠であるログを抹消されてしまえば、もはや害意の存在など証明不可能になる。

このように、不正アクセスにおいて、行為者の意思を区別して扱うことは非常に難しいと言わなければならない。

第4節 峻別の意義

不正アクセス禁止法制のもとではハッカーは存在し得ず、消えて行くことを余儀なくされることがわかった。ただし第2節で論じたように、インターネットにおいてハ

ッカーがこれまで何らかの役割をになってきたことは確かだから、それによって失われるものも確かに存在するだろう。以下、ハッカーないしハッキングがこれまでに果たしてきた役割を検証し、その失われるメリットと不正アクセス禁止法制のメリットを比較してみよう。

(1)システムの安全性を高めるハッキング

第一の考え方は、システムの安全性を高めることにハッキングが貢献していると言うものである。システムの検査としてハッキングを位置づけると、システム開発者との間に意思の疎通がないから開発者が気づかないようなセキュリティ・ホールが見つかることが多い。

しかし普通のシステム管理者ならば、ネットワークの向こうの匿名の何者かにシステムの安全をテストしてもらうことは好まないだろう。その者がその先に進まないと言う確信は持てないし、何か細工を施された可能性は否定できないからである。

システム管理者としてはセキュリティホール探しは、リアルワールドにきちんとした実体を持った信頼のおける個人か会社に行わせ、最低でもレポートという形で、結果をきちんと伝えてもらうことを望むだろう[*20]。したがって、被侵入システムのテストなどの例外は認める必要はあるが、勝手連的なハッカーや匿名のハッカーに至るまですべて正当化する必要はない。

(2)相互に依存するインターネット

インターネットの場合はシステムの多くの機能が単独では成立し得ず、相互に依存しあっている場合がある。隣のシステムにおいて適切な管理を行っていることは自分のシステムを安全に維持するための前提条件となる。隣のシステムをのぞき見る以外にそれを試す方法はない。この点に鑑みて、ハッキングを限定的に認めてはどうか。これが第二の考え方である。

確かにインターネットが相互にいろいろなシステムに依存することは事実であるが、だからと言って他人が管理するシステムに侵入を許すほどの積極的理由になるであろうか。侵入される"隣"にしてみればそのような行為は迷惑以外の何者でもなく、不安をかきたてられるだけである。隣のシステム管理者への注意喚起なら他にも方法があるだろうし、自分のシステムの安全を守るためなら接続ルートを変更すればよい。結局この考え方もハッキングまで認める理由にはならない。

(3)インターネットの発展を阻害する恐れ

インターネットにおいては他人の設定をのぞき見して、自分の設定を行うとか、他のシステムの設計をそっくりコピーするなどの行為が日常的に行われてきた。こうした自由さによって非常に使いやすい環境が作り出され、問題点が明らかになればネットニュースで議論され次世代の規約に反映されるなどして、インターネットの進化にも寄与してきた。しかし厳格な不正アクセス禁止法制はそういう余地を残さないから、今後のインターネットの発展が阻害されるのではないか。これが第三の考え方である。

しかし、この主張はきわめて大きなポイントをひとつ見逃している。それはインターネットにおける自由な環境の維持にあたっての前提条件であった研究者ネットワークであることと、情報の共有という原則が商業利用解禁[*21]とネットワーク人口の大爆発[*22]で崩れてしまっていることである。

かつての牧歌的なインターネット・ビレッジは今や普通の社会になった。構成員には犯罪者も少なからず混ざっている。公開を前提としない経済的な価値の高い情報が

増え、ハッキングによって得られる情報も一定の経済的価値を持つようになった。そのような環境下で自由や大らかさを追求することは全体を利することにならず、犯罪者に付け入られるだけである。

また、ネットワーク技術の進化にハッキングが寄与することがあるという考え方にしても、これほどまでに大規模化し、複雑化したシステムに対して、ひとりの試みがどれほどの効果を持つか疑問である。あえてそれを許容したとして、クラッキングによる弊害を上回るだけの果実が期待できないのではないだろうか。

以上のことから、もはやハッキングにはあえて認めなければならないほどの意義は認められないと考えられる。

展望

以上のように、ハッカー·クラッカー峻別論に沿ってハッカーを許容しクラッカーを処罰すると言うことはかなり難しく、それを認める意義も乏しい。

インターネットへの適用については、確かに厳格にして過剰であるという側面はある。しかしインターネットは今まさに過渡期を迎えており、それゆえにはっきりとした枠組みの構成が緊急に必要である。新しい枠組みを反映した立法が現在の基準に照らしてやや唐突に見えるのは当然のことである。

ゆえに不正アクセス禁止法制は行為者の意思にかかわらず、一定の形式に該当する行為を行った者は処罰されるという方法で作られるべきである。

主要参考文献

1.郵政省『高度情報通信社会に向けた環境整備に関する研究会報告書』(郵政省、1998年)

2.警察庁『不正アクセス対策法制に関する調査研究報告書』(警察庁、1998年)

3.(財)社会安全研究財団情報セキュリティ調査研究委員会『情報セキュリティ調査研究報告書』((財)社会安全研究財団、1996年)

4.通商産業省大規模プラント・ネットワーク・セキュリティ対策委員会『大規模プラント・ネットワーク・セキュリティについて・中間報告書』(通商産業省、1998年)

5.大野幸夫「コンピュータ犯罪とは何か」bit別冊『コンピュータと法律』所収、115頁以下(共立出版社、1992年)

6.安富 潔『刑事手続とコンピュータ犯罪』(慶応義塾大学法学研究会、1992年)

7.名和小太郎「情報システムの脆弱性」法とコンピュータ第11号所収、3頁以下(法とコンピュータ学会、1993年)

8.村井純『インターネット』(岩波新書、1996年)

9.Steven Levy 著、古橋芳恵、松田信子共訳『ハッカーズ』(工学社、1987年)

10.Bruce Starling 著、今岡清訳『ハッカーを追え!』(アスキー出版局、1993年)

11.白田 秀彰「ハッカー倫理と情報公開・プライバシー」高度情報化の法体系と社会制度科学研究費補助金・重点領域研究報告書所収(1995年)

12.山根 信二、小笹 裕昌「真のハッカーがクラッキングをしない理由」信学技報・FACE96-21(電子情報通信学会、1996年)

注釈

以下に記載するURLはいずれも1998年4月1日現在のものである、同日付で著者が保存している。入手できない場合は問い合わせられたい。

[*1] 「NTT研通信網に侵入～業務ソフト漏洩」(毎日新聞1997年10月6日)など多数。

[*2] 「不正アクセス10年～東大の大型計算機センター」(毎日新聞1997年10月16日)など多数。

[*3] 前述参考文献1『不正アクセス対策法制に関する調査研究報告書』のほか、警察庁『情報システムの安全対策に関する中間報告書』第2編

（1996 年 4 月）、前述参考文献 3『情報セキュリティビジョン策定委員会報告書』第 2 部第 2 章。

[*4] 郵政省『情報通信ネットワークの安全･信頼性に関する研究会報告書』第 2 章（1997 年 6 月）、前述参考文献 1『高度情報通信社会に向けた環境整備に関する研究会報告書』25 頁以下。

[*5] 日本における活動の典型例としては「ハッカーはクラッカーじゃないと主張する会」が挙げられる。これに関連する資料は"http://www.vacia.is.tohoku.ac.jp/~s-yamane/articles/hacker.html")などに豊富。

[*6] 「コンピュータ不正アクセス対策基準」平成 8 年 8 月 8 日通商産業省告示第 362 号。

[*7] 「情報システム安全対策指針」平成 9 年 9 月 18 日国家公安委員会告示第 9 号。

[*8] 権限愉越の不正アクセス（内部犯行）においては必ずしもこうはならない。そもそも内部犯行に対しては、不正アクセス禁止法制による以前に労働契約、就業規則等によって実際に相当程度防ぐことができるため、同列に扱うことは必ずしも妥当ではない。

[*9] 18 U.S.C. 1030 et seq.。

[*10] 的場純男「コンピュータ犯罪に関する刑事法上の問題点」ジュリスト 846 号所収、15 頁以下（有斐閣、1985 年）など。

[*11] 最近の例としては園田寿、北岡弘章「不正アクセスと刑法」関西大学法学論集第 47 巻第 6 号所収、42 頁以下（関西大学、1998 年）など。

[*12] すべて昭和 62 年法 52 号。詳細は前述参考文献 5、大野「コンピュータ犯罪とは何か」など。

[*13] 不正競争防止法 3 条による差止請求、同 4 条に基づく損害賠償に関する適用があることに注意せよ。

[*14] 新しい解説として、『消費者教育読本・マルチメディア時代を生きる』60 頁以下（東京都消費生活総合センター、1998 年）。

[*15] 結果発生の段階においても追加的措置が必要であることは当然である。前述参考文献 1、郵政省報告書は"無権限アクセスによる情報の窃取"を情報窃盗またはプライバシーの侵害として刑法改正によって処罰することに言及している（34 頁）。

[*16] 特に UNIX に関しては非常に多くのソフトウェアが無料で出回っており、OS からアプリケーションまで購入しなければならないものはほとんど見当たらないほどである。

[*17] Request For Comments の頭文字。ネットニュースによる公開の議論によって成立し、インターネット上で広く公開されている技術標準のことである。

[*18] ハッカー・クラッカーの定義はインターネットの頻出用語集である RFC1983、俗語集である"The New Hacker's Dictionary"などが存在しており、これを浜田が要約した。

[*19] http://www.ash.ne.jp/~joe/hack/hack.htm,"Joe のハッカー観察日記"は好例。

[*20] 現実の動きとしては、「太田昭和系ギャブコンサルティング、ハッカー対策、総合的に」（日本経済新聞 97 年 10 月 6 日）「疑似ハッカーで安全チェック、富士通も参入～企業通信網向けに」（日本経済新聞 98 年 3 月 10 日）などが挙げられる。

[*21] 1991 年から商業ネットワークとの間で相互接続を開始している。

[*22] 米ネットワークウィザード社の統計("http://www.nw.com/zone/WWW/report.html")によれば、93 年 1 月の時点でホスト数 1,313,000 個所だったのが 97 年 6 月には 19,540,000 個所となっており、4 年でおよそ 20 倍になっている。
