不正アクセス防止法（2）課題
（具体的侵害行為と本法の適用可否）

●不正アクセス防止法の適用が疑問視される問題とは何か？

Q

私はネットワーク管理を担当しています。侵入者（ハッカー）の攻撃に対して、法はどこまで適用されるのでしょうか。

A

「不正アクセス行為の禁止等に関する法律（平成十一年法律第一二八号）」（以下「不正アクセス防止法」と略す）は、電気通信回線（ネットワーク）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成立しました（法第一条）。

今回は、不正アクセス防止法の課題を中心に説明します。

1 はじめに

コンピューターやネットワークに関する問題は広域化、多様化しており、裁判所の判断を待たねば違法性の有無についての明確な区別は困難な状況です。しかし、現代社会における情報技術の発達は目覚ましく、ライフラインの一部と考えられるようになりました。ネットワーク社会の秩序を維持し、個人のプライバシーや組織の秘密を守ることは、とても重要な問題です。

情報科学技術の発展と法的整備の両面から対応策を立て、相互の密接な協力体制が必要となります。

2 問題となる事例の検討

不正アクセス防止法が成立したことで、一定のネットワーク社会の秩序維持機能を担うことが期待されています。しかし、情報技術の発達に伴う侵入者の行為のすべてを規制するものではありません。問題となる個々の事例について説明します。

(1) セキュリティホール攻撃

セキュリティホール攻撃とは、システムプログラム等に含まれるセキュリティ上の脆弱性をついて管理者権限を取得し、また、許可されていないコマンドを実行可能とするような行為をいいます。

侵害された側は致命的な打撃となり、多くの行為が本法三条二項二号の対象となるべきものですが、しかし、不正アクセス防止法には、未遂罪や予備罪を処罰する規定が存在しません。

(2) ブルート・フォース攻撃

ブルート・フォース攻撃とは、ＩＤ・パスワードの組み合わせを総当たりする行為です。しかし、不正アクセス防止法で「不正アクセス」と認められるためには、①不正アクセスの対象となるコンピューターにアクセス制御機能が存在すること、②ネットワークを通じたアクセスであることが必要です。

ブルート・フォース攻撃があっても、実際に「不正アクセス」の類型に当てはまらなければ、処罰されることはありません。

(3) ポートスキャン攻撃

ポートスキャン攻撃とは、ＴＣＰ／ＩＰポートを総当たりして、起動しているサービスを調査する行為です。

しかし、(1)と同様に、未遂罪や予備罪を処罰する規定は存在しません。

(4) 使用不能攻撃

使用不能攻撃とは、攻撃者が本来の目的とは異なる使い方で、ＣＰＵ、メモリ、ネットワークなどの資源を食いつぶすことで、コンピューターの使用を妨害する行為です。攻撃目標となるコンピューターに直接アクセスする場合は本法の適用の可能性がありますが、無差別的に大量のパケットを送信する行為や不正なコマンドを入力してサービスを停止させる行為は、刑法の電子計算機損壊等業務妨害罪（刑法二三四条の二）に該当する場合は別として、本法では処罰されません。

(5) スパム・メール

最近、電子メールの送受信の際、宣伝や勧誘のメールが頻繁に送られてきます。これをスパム・メールといって、大きな社会問題となっています。

米国ではCAN-SPAM法（Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003）が成立し、わが国でも迷惑メール法や特定商取引法により規制されていますが、一定の形式を具備すれば、数万件のメールを無差別に送付したとしても処罰されることはありません。

(6) 踏み台

踏み台とは、電子メールの発信元を詐称するために電子メールを不正に中継させる行為です。管理者によって中継機能が制限されている場合は本法の適用の可能性がありますが、電子メールの中継がオープンなサービスとなっている場合は、本法の規制の対象外です。

(7) コンピューターウィルス

コンピューターウィルスは多種多様なものがあり、本法に該当するか否かは個々のウィルスの性質ごとに判断する必要があります。

例えば、ワーム型といって、複数のコンピューター間に感染して増殖するだけのものは、不正アクセスとはいえません。しかし、アクセス制御機能による利用の制限を免れるようなウィルスであれば、本法を適用できる可能性があります。

(8) 組織内犯罪

コンピューター犯罪のうち、最も発生件数が多いのは内部犯罪です。しかし、不正アクセス防止法に言う電気通信回線（「ネットワーク」）が、公衆回線や専用線などの電気通信事業法に基づく回線に限定されるのか、外部回線に接続されている組織内部のＬＡＮまで包含するかは、議論があります。

また、不正アクセス防止法は、ネットワークに接続されていないコンピューターに侵入する行為、アクセス管理者や正規利用者による情報の不正入手や漏洩などは規制の対象から除外されています。

(9) セキュリティ・コントロールの懈怠

セキュリティ・コントロールをまったく行っていない組織においては、そもそもすべてのアクセスが本法の適用除外、すなわち、適法なアクセスになります。

例えば、パスワードが設定されていない、パスワードをシステム導入時から変更していない、アカウント・利用者のＩＤとパスワードが同じである場合は、アクセス制御機能がないといえます。したがって、「不正アクセス」の問題にならない可能性もあります。

(10) サイバーテロ

近時、サイバーテロリズムのような大規模なコンピューター犯罪が発生しています。

公法上は属地主義が原則であり、日本国内で行われた犯罪にわが国の法を適用することになります（刑事訴訟法二条一項、刑法一条一項）。

しかし、ネットワーク犯罪のように国境を超えて犯罪行為が行われる場合、実際の適用範囲の画定は容易ではありません。