



# 不正アクセス防止法(1)総論

● ネットワーク管理者の許可なく、他人のコンピュータに侵入した者を処罰することは可能か？

弊社WWWサーバーに、

一日数回、同一の者からコマンドが送られています。中止するよう警告しましたが、一向にやめません。どのように対応すればよいのでしょうか。特に法的な措置をとることは可能なのでしょうか。

Q

月十三日から施行されています。不正アクセス防止法成立の背景

コンピュータ犯罪といわれるものは、多種多様なものがあります。不正アクセスは、他人のIDやパスワードなどを用いてコンピュータ・システムに侵入する行為であり、コンピュータ犯罪の「入り口」と言われます。

A

ハイテク犯罪に対する技術的・法的対応の強化が諸外国から指摘され、わが国は法整備を迫られました。それが契機となり、コンピュータ・ネットワークへの不正アクセス自体を犯罪として処罰する「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)が第一四回国会において可決成立し、一九九九(平成十一年)八月十三日に公布されました。なお、本法の中心となる不正アクセス行為の禁止とその処罰規定は、二〇〇〇(平成十二)年二

月十三日から施行されています。不正アクセス防止法成立の背景

不正アクセス防止法は全九条から構成されている法律です。主に電子通信回線を通じて行われる犯罪に対して、①不正アクセス行為の禁止、②不正アクセス行為を助長する行為の禁止、③アクセス管理者による防御措置、④再発防止のための都道府県公安委員会による援助措置、⑤違反者に対する罰則を規定しています。これによって、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ことを目的としています(法第一条)。

(三) 二項(一)号。

(2) アクセス制御機能のあるコンピュータに対し、特殊な情報または指令を入力して、制限されている利用を可能にする行為(三) 二項(二)号。

(3) ネットワークで接続された他のコンピュータのアクセス制御機能によって利用が制限されているコンピュータに対し、特殊な情報または指令を入力して、制限されている利用を可能にする行為(三) 二項(三)号。

なお、不正アクセスとなるためには、不正アクセスを受ける側が一定のセキュリティレベルを持っていることが前提となります。セキュリティ・コントロールをまったく行っていないプロバイダや組織においては、すべてのアクセスが適法となると考えられます。セキュリティ対策には十分な対策を講じる必要があります。

4 不正アクセス行為を助長する行為の禁止

不正アクセス行為そのものだけでなく、不正アクセス行為を助長する行為も処罰の対象となります。すなわち、他人の識別符号を、それがどのコンピュータで使えるかを明示したうえで、管理者や正規の利用者以外の者に提供してはならず(四) 条)、これに違反した者は三〇万円以下の罰金が科されます(九) 条)。

5 アクセス管理者による防御措置

アクセス制御機能をコンピュータに付加したアクセス管理者は、①識別符号またはそれを確認するために用いる符号を適正に管理すること、②アクセス制御機能の有効性を常に検証すること、③必要に応じてその機能を高度化すること、④その他不正アクセス行為を防御するために必要な措置を講じる等の努力義務を負います(五) 条)。

しかし、民事法上はこの規定を根拠として不法行為責任(民法七〇九条)、契約責任を問われる可能性があります。また、刑法の背任罪(刑法二四七条)になる可能性があります。

6 都道府県公安委員会による援助措置

都道府県公安委員会は、アクセス管理者から援助を受けたい旨の申出があり、その申し出を相当と認めるときは、必要な資料の提供、助言、指導その他の援助を行います(六) 条(一)項)。援助を受けるた

(国際捜査共助法二) 二条(二)号)。これらの犯罪に対処するためには、国際的な協力体制が必要となります。

2 不正アクセス防止法の目的

不正アクセス防止法は全九条から構成されている法律です。主に電子通信回線を通じて行われる犯罪に対して、①不正アクセス行為の禁止、②不正アクセス行為を助長する行為の禁止、③アクセス管理者による防御措置、④再発防止のための都道府県公安委員会による援助措置、⑤違反者に対する罰則を規定しています。これによって、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ことを目的としています(法第一条)。

3 不正アクセス行為の禁止

何人も不正アクセス行為をしてはならないとして(三) 条(一)項)、次の三類型が規定されました。違反者は、一年以下の懲役または五〇万円以下の罰金に処せられます(八) 条(一)号)。

(1) アクセス制御機能のあるコンピュータに対し、他人の識別符号を入力して、制限されている利用を可能にする行為

(表) 不正アクセス防止法における用語の定義(法第2条)

用語	定義	具体例
□ アクセス管理者	ネットワークに接続しているコンピュータの利用に関して、その動作を管理する者をいう(2) 条(1) 項)。すなわち、利用者が多数存在する大型コンピュータであっても、ネットワークに接続していなければ適用範囲外。しかし、利用者が1人だけでも、ネットワークに接続していれば、不正アクセス行為の対象となる。	UNIXでいう rootやWindowsでいう Administrator、自らのホームページで会員制のサービスを行う個人や組織など。
□ 識別符号	ネットワークを通じたコンピュータの利用に関して、利用者を他の利用者と区別するための符号のこと。	パスワード(2) 条(2) 項(1) 号)、音声・指紋・網膜などのバイオメトリクス情報(2) 条(2) 項(2) 号)、署名(2) 条(2) 項(3) 号)、およびそれらと組み合わせて用いられるユーザーID・パスワードのこと。
□ アクセス制御機能	利用者が入力したユーザーID・パスワードによって、コンピュータの利用制限を解除する機能のこと(2) 条(3) 項)。アクセス制御という言葉は、情報処理では、ファイアウォールによるパケットフィルタリングやルーティング制限、ファイルの利用パーミッション等を含むが、本法にいうアクセス制御は、識別符号による利用の制限に限定される。	通常のログイン手続きはもとより、目的とするコンピュータ以外のコンピュータ(RADIUSやKerberos等の認証サーバー)による認証も含まれる。