保存種別　第１種（永年）

各地方機関の長
各都道府県警察の長　殿
（参考送付先）
庁内各局部課長

警察庁丙生企発第31号、丙生環発第2号
丙技発第1号
平成１２年１月２１日
警察庁生活安全局長
警察庁情報通信局長

不正アクセス行為の禁止等に関する法律等の概要及び運用上の留意事項について

不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号。以下「法」という。）及び不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則（平成１１年国家公安委員会規則第１２号。以下「規則」という。）の制定の趣旨及び要点等については、「不正アクセス行為の禁止等に関する法律等の施行について（依命通達）」（平成１２年１月２１日付け警察庁乙生発第１号、乙官発第１号、乙情発第１号）のとおりであるが、これらの概要、運用上の留意事項は下記のとおりであるので、遺憾のないようにされたい。

記

第１　法等の概要

１　法の目的について（法第１条関係）

他人の識別符号（ＩＤ・パスワード等）を窃用等して電気通信回線を通じて電子計算機にアクセスする不正アクセス行為は、誰が当該電子計算機を利用しているかわからないという状態を作り出し、ネットワークを利用した犯罪を助長するとともに、ネットワークを無秩序な状態にして国民が安心してネットワークを利用できない事態を招くこととなる。

そこで、このような不正アクセス行為の問題点に着目し、電気通信回線を通じて行われ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、法が制定されたものである。

２　定義について（法第２条関係）

（１）アクセス管理者（同条第１項）

ア　概要

アクセス管理者とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者である。

イ　特定電子計算機

「電気通信回線」とは、電気通信を行うために設定される回線のことであり、有線に限定されるものではなく、無線も含まれる。「電気通信回線に接続している」とは、電気通信が可能な状態に構成されていることを指す。

「電子計算機」とは、コンピュータのことである。本法においては、一定の

独立性を有するものに限られ、各種機器に内蔵されているマイクロ・コンピュータは含まれない。

ウ　動作の管理

特定利用につき「特定電子計算機の動作を管理する」とは、特定電子計算機の特定利用を誰にどのような範囲で行わせるかを決定することを意味する。したがって、アクセス管理者は、単に特定電子計算機に係るシステムの運用管理を行っている者ではなく、当該システムを誰に利用させるか等を決定する権限のある者（企業等の法人であれば、法人そのもの）である。

また、「動作を管理する」者であることから、特定電子計算機を所有するかどうか、物理的に管理しているかどうかは問わない。

エ　特定利用

インターネットへの接続（インターネット接続事業者（以下「プロバイダ」という。）のダイアルアップルータの利用）、電子メールの送受信（プロバイダ等のメールサーバの利用）、ホームページの閲覧（企業、プロバイダ等のWWWサーバの利用）、ホームページを通じて行うインターネット・ショッピング（企業のWWWサーバの利用、注文等の処理を行うサーバの利用）等が具体例として挙げられる。

特定電子計算機の利用であっても、当該特定電子計算機のキーボードを直接操作することによって行うものは特定利用ではない。

（２）識別符号（同条第２項）

ア　概要

識別符号とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付された符号である。

イ　利用権者

「許諾」とは、その内容として何らかの権利設定を含む必要はない。その方式も、文書又は口頭、明示又は黙示を問わない。

利用権者の具体例としては、プロバイダの会員、ＬＡＮを構築している企業において当該ＬＡＮを通じてホスト・コンピュータを利用することを認められている社員等が挙げられる。個人だけでなく、法人も利用権者となり得る。

ウ　識別符号を付す主体

識別符号を利用権者等に付す主体は、アクセス管理者には限定されていない。アクセス管理者が、利用権者や第三者が付した符号を識別符号とすることを妨げるものではない。

エ　符号の形式

法では、その形式について、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものとしている。

① アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号（パスワード等）

② 利用権者等の身体の全部若しくは一部の影像又は音声を用いてアクセス管理者が定める方法により作成される符号（指紋、虹彩、音声等を数値化したもの）

③ 利用権者等の署名を用いてアクセス管理者が定める方法により作成される符号（署名の形態、筆圧、動作等を数値化したもの）

一般的に用いられているＩＤ・パスワードの場合は、パスワードが①に該当する符号、ＩＤがその他の符号であり、ＩＤとパスワードの組合せが「次のいずれかに該当する符号とその他の符号を組み合わせたもの」として識別符号に該当することとなる。

カ　留意点

（ア）企業や同一部署に属する者が共同で利用することが認められている識別符号（いわゆるグループＩＤ）については、その態様にもよるが、アクセス管理者の直接の許諾を得た代表者を利用権者とし、他の者は利用権者から承諾を得て利用している（法第３条第２項第１号参照）ものと解することができる。

（イ）次のようなＩＤ・パスワードは、いずれも利用権者等に付されている符号ではないか、利用権者等を区別して識別することができるように付されていないため、識別符号には該当しない。

○ アクセス管理者が特定電子計算機のパスワード・ファイルから消去し忘れている利用権者等でなくなった者のＩＤ・パスワード

○ アクセス管理者に無断で特定電子計算機のパスワード・ファイルに追加されたＩＤ・パスワード

○ コンピュータの出荷時に初期設定としてパスワード・ファイルに登録されているＩＤ・パスワード

○ アクセス制御機能により会員のみに特定電子計算機の特定利用を制限しているプロバイダ等のアクセス管理者が、入会希望者の「お試し利用」等のために公にし、不特定多数の者が用いることができることとしているＩＤ・　パスワード

（３）アクセス制御機能（同条第３項）

ア　概要

アクセス制御機能とは、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等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である。

アクセス制御機能は、アクセス管理者が特定電子計算機の動作の管理を実現

するための手段である。

イ　アクセス制御機能を付加する主体

アクセス制御機能を付加する主体は、特定利用に係るアクセス管理者である。「付加する」とは、パスワード・ファイルの設定を行って特定電子計算機の特定利用を制御するためのプログラムを機能するように設定したり新たに追加すること等によって、特定電子計算機が特定利用に係る識別符号が入力された場合に当該特定利用の制限を解除するという動作をし得る状態にすることである。

ウ　アクセス制御機能が付加される特定電子計算機

アクセス制御機能は、特定利用に係る特定電子計算機又は当該特定電子計算機と電気通信回線を介して接続した他の特定電子計算機に付加される。複数の電子計算機で構成されるシステムにおいては、一般的に、識別符号の照合を一元的に行う電子計算機（認証サーバ）を設置等しており、これが「特定電子計算機と電気通信回線を介して接続した他の特定電子計算機」に該当することとなる。

エ　入力

法においては、特定利用に係る特定電子計算機に識別符号等の情報が伝達されることをとらえて「入力」としている。

オ　識別符号を用いてアクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号

「識別符号を用いてアクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号」をアクセス制御機能による利用権者等の識別に用いる例としては、公開鍵暗号技術を利用した特定利用の制限の方式が挙げられる。

公開鍵暗号技術を利用したアクセス制御機能においては、利用権者を区別して識別できるよう付されているのは秘密鍵（法第２条第２項第１号の符号に該当）及び電子証明書（公開鍵及びそれが誰のものであるかを明らかにするデータを含むもの。ＩＤの機能を有する。）である（秘密鍵と電子証明書の組合せが識別符号となる。）が、アクセス制御機能を付加された特定電子計算機に入力されるのは当該秘密鍵により作成された電子署名（秘密鍵で一定のデータを暗号化したもの。入力の都度、内容が変わる。）と公開鍵証明書となる。

そこで、公開鍵暗号技術を利用したものもアクセス制御機能となるよう、法第２条第３項において、「識別符号」を「識別符号を用いて当該アクセス管理者の定める方法により作成される符号（秘密鍵により作成される電子署名）と当該識別符号の一部（電子証明書）を組み合わせた符号を含む。」としたものである。

ク　留意点

（ア）アクセス制御機能による特定利用の制限が完全なものである必要はない（このことは、法第３条第２項第２号及び第３号の規定があることからも明らかである。）。特定利用を行う場合に、通常、当該特定利用の制限を解除す

るための識別符号を入力するようになっていれば、アクセス制御機能による特定利用の制限がなされていると解してよい。したがって、既に利用権者でなくなった者のＩＤ・パスワード等の識別符号以外の符号（２（２）カ（イ）参照）がパスワード・ファイルに登録されていること等をもって、アクセス制御機能による特定利用の制限がないこととはならない。

（イ）識別符号がホームページで公開等されており、利用権者等でない第三者が当該識別符号を入力できるような場合であっても、アクセス制御機能により特定利用の制限がされていることには変わりはない。

3　不正アクセス行為の禁止、処罰（法第３条及び第８条第１号関係）

（１）概要

法においては、次の３つの類型を不正アクセス行為として禁止、処罰することとしている。

①　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（法第３条第２項第１号）

②　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（同項第２号）

③　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（同項第３号）

（２）他人の識別符号を無断で入力して行う行為（（１）①）

「他人の識別符号」とは、自分に付されていない識別符号である。他人名義や架空名義でプロバイダと契約する等して入手したＩＤ・パスワードはその入手した本人に付された識別符号であり、これを入手した本人が入力したとしても、不正アクセス行為には該当しない。

２（２）カ（イ）で例示した識別符号に該当しないＩＤ・パスワードを入力する場合は、当該ＩＤ・パスワードが「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。）」に該当するため、（１）②（第３条第２項第２号）に該当することとなる。

なお、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が付されている利用権者の承諾を得てするものは、禁止の対象から除外されている。

（３）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その他の情報又は指令を入力して行う行為（（１）②、③）

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）やアクセス管理者に無断でパスワード・ファイルに追加したＩＤ・パスワード等を悪用して、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識別符号以外の情報又は指令を入力して行うものである。

複数の特定電子計算機でシステムが構成され、識別符号の照合を一元的に行う認証サーバが設けられている場合には、いわゆるセキュリティ・ホールを攻撃する方法として、認証サーバのセキュリティ・ホールを攻撃するものと、特定利用に係る特定電子計算機のセキュリティ・ホールを攻撃するものとが想定されるため、前者については（１）②、後者については③で規定したものである。

なお、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禁止の対象から除外している。

（４）制限されている特定利用をし得る状態にさせる

法においては、不正アクセス行為をアクセス制御機能による特定利用の制限に対する侵害行為として捉えて禁止することとしているため、これを「特定利用をし得る状態にさせる」行為と規定したものである。

識別符号等が入力されれば、単に特定利用をし得る状態となるだけでなく、特定利用がされてしまう場合もあるが、このような場合にも観念的には「特定利用をし得る状態」を経て特定利用がされたものと解することができるため、このような場合も含めて「特定利用をし得る状態にさせる」と規定した。

（５）留意点

ア　電気通信回線を通じて行われるものに限定されており、アクセス制御機能を有する特定電子計算機や、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、そのキーボードを直接操作して識別符号又はアクセス制御機能による制限を免れることができる情報若しくは指令を入力する場合は、不正アクセス行為には該当しない。

イ　識別符号の入力元の入力装置は、電子計算機に限定されていない。したがって、電話機から識別符号を入力する場合や、識別符号が指紋である場合の読取装置（スキャナ等）のような入力装置から入力する場合も対象となる。

（６）罰則

不正アクセス行為の禁止に違反した者は、１年以下の懲役又は５０万円以下の罰金に処せられることとなる（法第８条第１号）。

なお、不正アクセス行為罪は、不正アクセス行為によりし得る状態になった特定利用を制限していたアクセス制御機能を単位として成立するが、アクセス制御機能の単位はこれを付加したアクセス管理者ごとに判断されることとなる。

また、不正アクセス行為後に引き続いて電子計算機損壊等業務妨害罪、詐欺等の他の犯罪が行われた場合の両者の関係は、併合罪となると考えられる。

４　不正アクセス行為を助長する行為の禁止、処罰（法第４条及び第９条関係）

（１）概要

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、第三者に無断で提供する行為を禁止、処罰することとしている。

（２）趣旨

他人の識別符号を無断で提供する行為は、その提供を受けた者の知識、技術に係わらず、容易に不正アクセス行為の実行を可能とするものであり、不正アクセス行為を助長する危険性が極めて高く、これを放置すれば不正アクセス行為を禁止する実効性を損なうこととなりかねない。そこで、他人の識別符号を無断で提供する行為を禁止、処罰することとしたものである。

（３）提供の形態

「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」とは、提供される識別符号の入力先を明らかにすることを指す。特定電子計算機の名称や設置場所まで明らかにする必要はなく、例えば、「ＩＤ××、パスワード○○をhttp://www.□□□.co.jpで入力すれば、□□□データベースが利用できます。」とか、「プロバイダ△△のアカウント、ＩＤ××、パスワード○○」というように、提供する識別符号の入力先のＵＲＬ（ホームページの場所）や、ダイアルアップ接続の電話番号が公表されている場合の識別符号に係るプロバイダ名を示すなど、一般人にとって容易にどの特定電子計算機の特定利用に係るものか、どこに識別符号を入力すればよいかを特定することができる情報を提供すれば、「明らかにして」提供したこととなる。

「これを知っている者の求めに応じて」とは、提供される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知っている者からの求めに応じて提供することを指す。

（４）識別符号の提供

「提供」とは、識別符号を第三者が利用できる状態に置くことをいう。特定の者に提供する場合だけでなく、インターネットのホームページで公開する等不特定多数の者に提供する場合も含む。その手段、方法は問わず、口頭で教示する、紙に書いて渡す、電子メールで送信する、ホームページや電子掲示板で公開する、識別符号が記録されたフロッピーディスク等の電磁的記録媒体を渡す行為等も「提供」に当たる。

提供する識別符号に係るアクセス管理者及び利用権者に対する提供は禁止されていない。また、識別符号に係るアクセス管理者による提供及び当該アクセス管理者又は識別符号に係る利用権者の承諾を得て行う提供は禁止の対象から除外されている。

（５）留意点

ア　他人名義や架空名義でプロバイダと契約する等して入手したＩＤ・パスワードはその入手した本人に付された識別符号であり、これを入手した本人が第三者に提供したとしても、禁止に違反しない。また、２（２）カ（イ）に例示したＩＤ・パスワードの提供は、識別符号の提供に該当しない。

イ　識別符号がＩＤとパスワードからなる場合に、その一部のみ（例えばパスワ

ードのみ）を提供しても原則として本条には違反しないが、次のような場合にはパスワードのみ（識別符号の一部のみ）の提供であっても識別符号を提供していると評価でき、本条に違反したこととなる。

○　パスワードに対応するＩＤを知っている者に、当該パスワードを提供する場合

○　パスワードとそれに対応するＩＤを特定することができる情報を併せて提供する場合

（６）罰則

助長行為の禁止に違反した者は、３０万円以下の罰金に処せられることとなる。

なお、識別符号の提供行為が不正アクセス行為の教唆、幇助に該当する場合には、本罪は不正アクセス行為の教唆罪、幇助罪に吸収されることとなる。

5　アクセス管理者による防御措置（法第５条関係）

（１）概要

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等の適正な管理に努めるとともに、当該アクセス制御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している。

（２）趣旨

不正アクセス行為の発生を防止するには、その禁止、処罰にのみ頼るのでは不十分であり、個々のアクセス管理者が自ら防御措置を講じることが非常に重要である。そこで、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等の適正な管理に努めるとともに、当該アクセス制御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し、その実施を促すこととしたものである

6　都道府県公安委員会による援助等

（１）都道府県公安委員会による援助等（法第６条及び第８条第２号並びに規則関係）

ア　概要

都道府県公安委員会（道警察本部の所在地を包括する方面を除く方面にあっては、方面公安委員会。以下「公安委員会」という。）は、不正アクセス行為が行われたと認められる場合において、アクセス管理者から、その再発を防止するため、援助を受けたい旨の申出があり、その申出を相当と認めるときは、当該アクセス管理者に対し、当該不正アクセス行為に係る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応急の措置が的確に講じられるよう、必要な資料の提供、助言、指導その他の援助を行うものとしている。

イ　趣旨

不正アクセス行為が行われた特定電子計算機を放置すれば、同一の手口による不正アクセス行為の再発を招きかねず、さらに、当該特定電子計算機を他の特定電子計算に対して不正アクセス行為を行う際の拠点（踏み台）として利用されることにもなりかねない。したがって、不正アクセス行為が行われた場合

には直ちに再発防止措置を講じることが重要であるが、アクセス管理者の中には、再発防止措置を講じようとしても、そのための知識、技術を有していない者がいることも想定される。

そこで、公安委員会が、アクセス管理者が再発防止のための応急措置を的確に講じることができるよう、その申出に応じて、必要な資料の提供、助言、指導その他の援助を行うこととしたものである。

ウ　援助の申出

援助は、不正アクセス行為に係る特定電子計算機に係るアクセス管理者からの申出が前提となる。

援助の申出は、規則別記様式で定める援助申出書に、援助の参考となるべき事項に関する書類その他の物件を添えて、当該特定電子計算機の設置の場所を管轄する公安委員会に提出することとされている（規則第１条第１項）。

エ　参考となるべき事項に関する書類その他の物件

「不正アクセス行為が行われた際の当該特定電子計算機の作動状況及び管理状況その他の参考となるべき事項に関する書類その他の物件」とは、不正アクセス行為に係る特定電子計算機に係るシステムの構成に関する資料（システム構成図等）、当該特定電子計算機等に入力された識別符号その他の情報又は指令に関する記録等（ログ）に関する資料、これらの資料の内容を記録したフロッピーディスク等の電磁的記録媒体等である。

なお、申出を受けた公安委員会が援助に必要な事例分析（不正アクセス行為の手口、それが行われた原因等に関する技術的な調査及び分析をいう。以下同じ。）等の作業を進める上で、援助申出書に添えられた資料その他の物件に援助を行うために必要なものが含まれていないと認めるときは、公安委員会は必要な書類その他の物件の提出を申出人に求めることができる（規則第１条第２項）。

オ　援助の内容

援助の内容は、アクセス管理者が再発防止のための措置を講じるのに必要な資料の提供、助言、指導等である。具体的には、申出の内容に応じて、次のような援助措置を採ることとなる（規則第２条）。

○　事例分析の結果に関する資料を提供すること。

○　アクセス管理者が講ずることが適当であると認められる再発防止措置に関し必要な資料の提供、助言、指導を行うこと。

○　不正アクセス行為からの防御に資する事業を行うことを目的とする民間団体、企業等を教示すること。

○　不正アクセス行為からの防御措置を記載した資料、書籍、ホームページ等を教示すること。

○　その他不正アクセス行為からの防御に資すると認められる事項を教示すること。

カ　事例分析の実施の事務の委託

公安委員会は、援助を行うために必要な事例分析の実施の事務の全部又は一部を、事例分析の実施に関する事務を適正かつ確実に行うことができる技術的能力を有し、かつ、十分な社会的信用を有すると公安委員会が認める者に委託することができる（法第６条第２項及び規則第３条）。法人に限定されず、個人に委託することもできる。

なお、委託された事例分析の実施の事務に従事した者には、秘密保持義務が課され（法第６条第３項）、これに違反した者は、１年以下の懲役又は５０万円以下の罰金に処せられる（法第８条第２号）。

（２）国による援助（法第７条関係）

ア　概要

国家公安委員会、通商産業大臣及び郵政大臣は、毎年少なくとも一回、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を公表するとともに（第１項）、国は、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ものとした（第２項）。

イ　趣旨

不正アクセス行為の発生を防止するには、アクセス管理者、利用権者、コンピュータ等の製造業者、ソフトウェア事業者等の関係者が、それぞれの立場で不正アクセス行為を防御するための活動を行うことが重要である。これらの活動が有効かつ適切に行われるようにするため、国が情報提供を行うこととしたものである。

なお、本条の規定は、都道府県公安委員会において不正アクセス行為についての広報啓発活動を行うことを妨げるものではない。

第２　運用上の留意事項

１　取締り及び援助体制の確立

不正アクセス行為の取締り及び援助の実施の双方について、各都道府県警察本部における担当課及び担当者を明確にすること。また、警察署における担当部署、担当者を明確にし、各都道府県警察本部の担当課との連絡体制を確立するとともに、警察署における被害の届出の受理時の対応要領を確立すること。

なお、援助については、申出に係る特定電子計算機のシステム構成等の技術的事項を聴取する必要があり、コンピュータ及びコンピュータ・ネットワーク等に関する専門的知識を有する者が対応する必要があるので、受理は都道府県警察本部又は専門的知識を有する職員が配置された警察署において行い、それ以外の警察署においては受理担当部署を教示することとするなど、これを踏まえて受理及び実施の担当部署並びに受理のための連絡体制を決定すること。

２　組織的対応の推進

（１）不正アクセス行為の取締り担当部署に不正アクセス行為に係る情報が集約されるよう、組織的な情報収集体制の確保に努めること。また、不正アクセス行為は、ハイテク犯罪の犯行手段として利用される事例も多いと予想されることから、不

正アクセス行為の取締り担当部署と他のハイテク犯罪取締り担当部署との連携強化に努めること。

（2）不正アクセス行為は、広域性を有する犯罪であることから、効率的な取締りを実施するため、都道府県警察間における共同捜査及び合同捜査を積極的に推進すること。

3　装備資機材の確保

不正アクセス行為の手口解明や証拠資料の収集のためには、コンピュータや電磁的記録媒体のコピー装置等の装備資機材が必要となるため、国費配分されるもののほか、各都道府県警察においても独自に予算措置等を講ずることにより、その整備に努めること。また、必要に応じて、他の部署に配備されたこれら装備資機材の有効活用や民間からの借上げ等を行うことができるよう、関係部署等との調整を行うこと。

さらに、事案発生時にこれら装備資機材を的確に活用できるよう、担当者にその取扱いについて習熟させておくこと。

4　専門的知識を有する職員の確保

不正アクセス行為の取締り、援助を実施するためには、コンピュータ及びコンピュータ・ネットワーク等に関する高度な専門的知識が必要となることから、これら専門的知識を有する職員を担当者として配置するほか、事案発生時には情報管理部門等に配置された専門的知識を有する職員を活用し、組織の総合力が発揮できる体制を構築すること。

また、警察庁又は他の都道府県警察の職員の支援が必要な場合に備え、その要請手続きについて確認しておくこと。

5　広報啓発等の不正アクセス行為に関する防犯活動の推進

不正アクセス行為の防御措置についての広報啓発活動及び不正アクセス行為発生時の被害状況の保存、警察への迅速な通報等についての防犯指導を積極的に行うこと。その際には、プロバイダ等との連絡協議会を通じて実施するなど、関係業界、団体等と連携してその効果的な推進を図ること。

なお、その推進に当たっては、各都道府県警察において設置を進めている情報セキュリティ・アドバイザーの活用を図ること。

6　指導、教養の徹底

取締り等担当者のみならず、警察署又は他部門の関係職員においても不正アクセス行為等の相談対応等を的確に行うことができるよう、不正アクセス行為の構成要件、都道府県公安委員会による援助の対象、手続等について、集合教養、巡回教養等あらゆる機会を活用して指導、教養を実施し、その周知徹底に努めること。

7　事案認知時等における警察庁への報告連絡の徹底

不正アクセス行為及び助長行為の取締り並びに援助の実施に当たっては、警察庁に対する適時適切な連絡を行うこと。特に、不正アクセス行為等の認知、事件着手等については、警察庁に対する報告連絡を徹底すること。