不正アクセス防止法によるネットワーク管理上の防止義務とは何か？

Q

私はこのたび、ネットワーク管理者に指名されました。不正アクセスに対して、どのような点に注意をしたらよいのでしょうか。

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）。

そして、アクセス制御機能をコンピューター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ずる等の努力義務を負います（法第五条）。

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。

今回は、不正アクセス防止法によるネットワーク管理上の防止義務を中心に説明します。

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

識別符号の適正な管理とは、ソーシャル・エンジニアリング対策、パスワード管理ファイルの暗号化、利用者に対するID・PW（パスワード）の適切な指導等です。例えば、IDとパスワードが同一であったり、アルファベットの大文字、小文字の区別ができなかったり、パスワードに誕生日や簡単な英単語を設定しないように注意を促すこと等の措置が必要です。

2 アクセス制御機能の有効性を常に検証すること

アクセス制御機能の有効性を検証するためには、①不正アクセス行為に関する情報収集、②各種ツールを利用したクラッキング・テスト、③セキュリティホールやシステムの脆弱性が発見された場合に、コンピューターのベンダから提供される修正プログラムをインストールしたり、パッチファイルを適用したり、ソフトウェアおよびハードウェアのバージョン・アップをすること等が必要となります。

なお、ログイン情報・アクセス情報・課金情報・管理情報・エラー情報等の記録（ログ）を取っておくことは、システムを適正かつ安全に運用する上で重要です。ログの取得は不正アクセス行為の検知、事実の確認、被害の認定、さらには再発防止に欠かせない情報です。一方、ログには利用者の個人情報や利用履歴等のプライバシー情報が含まれています。ログの取り扱いには慎重な配慮が必要です。

ちなみに、本法案は、警察庁、郵政省、通産省の三省庁が共同してその策定作業を行いました。警察庁は識別情報に関するログについて三ヵ月間の保存義務を主張しました。これに対し、郵政省は通信の秘密の観点から難色を示し、最終的にはログ保存の義務化規定は盛り込まれていません。

3 必要に応じてその機能を高度化すること

不正アクセスを受けないためには複数の対策を併用することが大切です。

例えば、①ソフトウェアおよびハードウェアのバージョン・アップ、②必要のないサービスの停止、③通信の暗号化、④パスワード形式の高度化等、安全性の高いアクセス制御機能を利用する等、不正アクセスの方法の多様化、技術の進歩に伴い、反復継続的なセキュリティ対策の計画化、実行、再検討が必要です。

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ずること

(1) **物理的措置**

不正アクセス・侵入対策として、まず検討すべきはファイアーウォールの設置です。ファイアーウォールは、①パケット・フィルタリング方式、②アプリケーション・ゲートウェイ方式の2つの方式があります。

①パケット・フィルタリング方式

ネットワーク上を流れるIPパケットを一定のルールに基づいて振り分け、通すべきパケットとそうでないパケットを選別する方法です。

例えば、社内に入ってこようとするパケット、および社内から出ていこうとするパケットに対して、発信元IPアドレスや宛先IPアドレス、ポート番号、TCPやUDPなどのプロトコル種別をパラメータにして振り分けます。

②アプリケーション・ゲートウェイ方式

通信を中継するプロキシー（proxy＝代理サーバー）を利用して、社内LANとインターネットを切り離す方法です。

例えば、社内クライアントからインターネット上に存在するサーバーにアクセスする場合、ファイアーウォールが社内クライアントからの要求を受けてHTTPプロキシーを起動し、クライアントに代わって社外のサーバーにアクセスします。こうすることで、社内LANを外部から隠蔽し、外敵から守ることができます。

アプリケーション・ゲートウェイ方式は、アプリケーションが送受信するパケットの内容を監視するため、パケット・フィルタリング方式よりも細かな防御が可能となる反面、オーバーヘッドが大きく、一般にパケット・フィルタリング方式より通信速度が遅くなります。また、対応プログラムを用意する必要があり、管理運営業務が大きくなります。

(2) **人的措置**

ファイアーウォールはあくまで外部ネットワークとの通信を制限するもので、内部者からの不正アクセスを防止することはできません。また、ファイアーウォールのセキュリティ・ポリシーを強固にするだけでは、社内ユーザーの使い勝手が悪くなり、業務効率が下がります。導入後の管理者の運用・管理が重要となります。

管理者は、利用者に対しては不正アクセス行為を行わないような注意の喚起、外部者に対しては不正アクセスの踏み台にされないように、適切なシステム運用をする必要があります。また、セキュリティは管理者だけで守れるものではありません。内部規定を策定し、組織的な対策を講じておくことが重要です。