Ksisnetだより
発行:Ksisnet事務局
令和 4年 3月23日
Vol.104

## 不正アクセス行為の禁止等に関する法律第8条

# アクセス管理者による防御措置

不正アクセス行為の禁止等に関する法律第８条では、

**アクセス管理者は、アクセス制御機能を付加し、必要に応じて**
**不正アクセス行為から防御するための必要な措置を講じなければならない**

とされています。

不正アクセス行為の発生を防止するためには、その禁止・処罰に頼るのみではなく、不正アクセス行為が行われにくい環境を整備することが必要となります。そのためには、個々のアクセス管理者が自ら防御措置を講じることが必要となりますが、その実施状況は必ずしも充分ではないのが現状です。

そこで、アクセス管理者に防御措置の実施を促すため、

**アクセス管理者に不正アクセス行為からの防御措置を講ずべき責務があること**

を法律上明確にしたのです。

## アクセス管理者とは…

**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、その利用権（ID・パスワードなど）を誰に付与するかを決定する権限を有する者のことをいいます。**

法人がコンピュータを運用している場合は、職員がシステム管理者として管理業務を行っている場合がほとんどだと思いますが、それらのシステム管理者は自分を任命した法人の意思に基づいて管理業務を行っています。

**不正アクセス禁止法でいうアクセス管理者は、**これらのシステム管理者ではなく、**当該法人自体**ということになります。

## アクセス管理者に求められる防御措置の主なもの

### 1 識別符号の適正な管理

利用権者の異動時におけるＩＤ・パスワードの確実な削除やパスワード・ファイルの暗号化など、識別符号を適正に管理する。

### 2 アクセス制御機能の有効性の検証

アクセス制御機能として用いているシステムのセキュリティに関する情報の収集といったアクセス制御機能の有効性を検証する。

### 3 アクセス制御機能の高度化

パッチプログラムによるセキュリティ・ホールの解消、アクセス制御プログラムのバージョン・アップ、指紋等を利用したアクセス制御システムの導入など、アクセス制御機能の高度化を図る。

### 4 他人に窃用されにくい識別符号の採用

ワンタイム・パスワードや指紋、暗号鍵などを利用する。

### 5 ログの有効活用

コンピューター・ネットワークの状態を監視するのに必要なログを取得してその定期的な検査を行ったり、ログを利用して前回アクセス日時を表示し、利用権者にその確認を求めるなどする。

### 6 ネットワーク・セキュリティ責任者の設置

ＩＴシステムに関する技術に詳しい人材をネットワーク・セキュリティ責任者に任命する。

情報セキュリティ対策には高度な技術が必要なため、専門的な外部サービスの利用も検討する。

**まもなくやってくる春の異動時期などに、忙しさに紛れてつい後回しにしてしまったり、忘れてしまったりして情報セキュリティ対策を怠ると、思わぬ被害に遭うことも考えられますので、必要な対策は早急に実施するようにしましょう。**

参考　ＮＰＡ（警察庁）