中小企業の

セキュリティー対策

—32—

設定不備による被害も

ソフトウエアのインストール直後やインターネットサービスの利用開始時、サーバーやネットワーク対応機器などの購入時点では、不要な機能が有効になっている製品・サービスや、機能へのアクセス制限が設定されていない製品・サービスがある。これに気付かずに利用開始することで情報漏えいや乗っ取りなどの被害が発生することがある。

2013年、情報共有を行うインターネットサービスを利用し、関係者でやりとりをしていたメールが、同サービス利用者であれば誰でも閲覧できる状態になっており、その結果機密情報が漏えいしてしまった、という報道が相次いだ。16年、インターネットに接続された複合機などの設定に不備があるため、機器内に保存されたデータが外部から閲覧できてしまう問題が依然続いていることが報道された。19年、総務省および関係機関が実施した、脆弱（ぜいじゃく）なID・パスワード設定などのためサイバー攻撃に悪用される恐れのあるIoT機器の調査においても、第2四半期までに505件の注意喚起が行われた。

企業は設定の不備による情報漏えいや乗っ取りなどの被害を防止するため、製品・サービスの利用開始時の設定確認や定期的な設定の見直しを行う必要がある。

必要に応じ初期設定を変更

■利用開始時に設定を確認する

利用しない機能や不要な設定は無効にする。また、セキュリティーを強化する機能や設定は有効にする。必要性が分からない場合は、マニュアルやインターネット上の情報を確認して、必要か不要か判断する。特に、ブロードバンドルーターや、複合機、ウェブカメラなどのネットワーク対応機器の各種機能の設定、例えばユーザー認証の有効化設定やファイル共有設定などを、必要に応じて適切な設定に変更する。また、パソコンに初期インストールされているソフトウエアについても不要と判断できるものはアンインストールしておくことで、リスクを低減できる。

■アクセス制限や権限を設定する

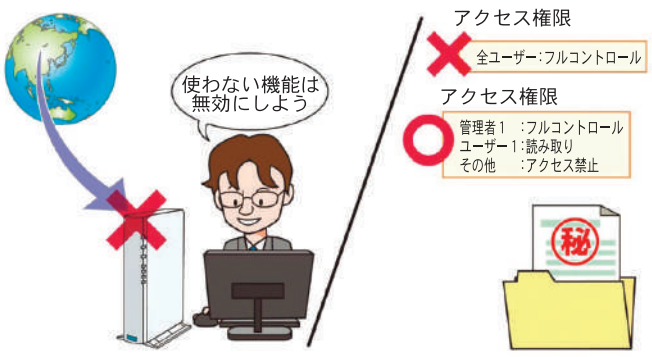
初期状態においてアクセス制限されておらず、管理機能やデータを誰でも利用できるように設定されている製品・サービスが存在する。攻撃者に、機密情報を閲覧される、設定変更されるなどの被害を防止するためには、利用開始前にアクセス制限機能を有効にし、利用者ごとのユーザーアカウントの作成とアクセス権限の付与を適切に行う必要がある。特に、重要なファイルが保存されているフォルダのアクセス権限は、全アカウントが閲覧や削除ができる設定（フルコントロール）にせずに、特定のアカウントのみがアクセスできるように設定する。

■設定の見直しを実施する

従業員の退職時には速やかにユーザーアカウントを抹消する。また、従業員の部署異動時には、アカウントに付与したアクセス権限を見直す必要がある。

マニュアルを読まなくても使い始めることができるソフトウエアやインターネットサービス、LANケーブルを差し込めばすぐに使えるネットワーク対応機器が増えているが、利用に当たっては製品・サービスの設定について必ず確認してほしい。

（独立行政法人情報処理推進機構・江島将和）



利用しない機能の無効化やアクセス制限の設定が必要