北日本新聞 2026.2.10

教えて！富山けいざい

ゼロデイ攻撃って？

◆対策公開前のサイバー攻撃／基本動作でリスク低減

Q－「ゼロデイ攻撃」って何ですか。ゲームの技かな。

Ａ－ゼロデイ攻撃とは、ソフトウエアやシステムの脆弱性（セキュリティホール）が発見され、対策が公開される前に、その脆弱性を悪用して行われるサイバー攻撃を言います。通常は脆弱性が見つかった場合、ソフトウエアの開発者から修正プログラム（パッチ）が提供されますが、脆弱性が発見されてから対策が講じられる前、つまり「パッチ公開日」より前の「０日」の攻撃ということです。事前の対策が難しいことが特徴で、情報処理推進機構（ＩＰＡ）によれば、脅威は年々拡大しています。

情報セキュリティ10大脅威

1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	システムの脆弱性を突いた攻撃
4	内部不正による情報漏えい
5	機密情報を狙った標的型攻撃
6	リモートワークの環境や仕組みを狙った攻撃
7	地政学的リスクに起因するサイバー攻撃
8	分散型サービス妨害攻撃（DDoS 攻撃）
9	ビジネスメール詐欺
10	不注意による情報漏えい

Q－どういう被害が発生しているの。

Ａ－不正アクセスによるシステムやデータの改ざんや破壊行為、業務データや機密情報の漏えいなどが挙げられます。そうした直接的な被害だけでなく、これらによって業務停止や経済的被害の発生、企業の社会的な信用が失われる事態に至ることもあります。

Q－被害に遭わないようにするには、どうすればいいの。

Ａ－ゼロデイ攻撃の特徴から、完全に防ぐのは困難ですが、主な攻撃の手口を見ていくと、リスクを減らしていくことは可能です。そのための対策は、▽ＰＣやネットワーク機器のＯＳやソフトウエアのアップデートを通じて常に最新の状態に保つ▽不審なメールやリンクを開かないなど基本動作の周知徹底▽ファイルやサーバーへのアクセス権限・ＰＣ管理権限の適切な設定▽データの暗号化やこまめなバックアップ▽サンドボックス（コンピュータに設けた仮想空間）の活用▽「ＥＤＲ」などの動作監視型セキュリティ対策の導入－です。

Q－もし攻撃に遭ったら、どうすればいいの。

Ａ－ゼロデイ攻撃に遭ったことが判明した場合は、まず攻撃された機器を直ちにネットワークから遮断します。その後、セキュリティ担当者に被害を報告し、ウイルス・スキャンを実施して被害拡大の防止を図る必要があります。攻撃への対策を含め、日頃からこうした基本的な動作やルールを確認しておくことが、重要と言えるでしょう。

（この連載は北陸経済研究所の倉嶋英二が担当しました。）