# 中小企業のセキュリティー対策

—22—

# ソフトウエアの脆弱性

## 求められる迅速な対応

OS（基本ソフト）やオフィスソフトなどのソフトウエア製品に脆弱（ぜいじゃく）性が発見された場合、製品開発会社が脆弱性を修正するためのプログラム（パッチ）を作成する。その後、独立行政法人情報処理推進機構（IPA）などのセキュリティー対応機関などと連携するか、または製品開発会社自身で脆弱性対策情報として脆弱性の内容とパッチまたは対策方法を公開し、利用者へ対策を促す。

一方、攻撃者が公開された脆弱性対策情報を元に攻撃コードなどを作成し、パッチを適用していない利用者に対して脆弱性を悪用した攻撃を行う被害が確認されている。特に広く利用されているソフトウエアの脆弱性対策情報が公開された場合は、攻撃コードなどが公開されると被害が拡大する恐れがある。

攻撃を受けた企業に生じる被害は、情報漏えいに伴う補償や事業中断、復旧対策などの直接的なコストだけではない。それまで築き上げてきたブランドや社会的信用が失墜し、大切な顧客を失うこともあるので影響は深刻といえる。

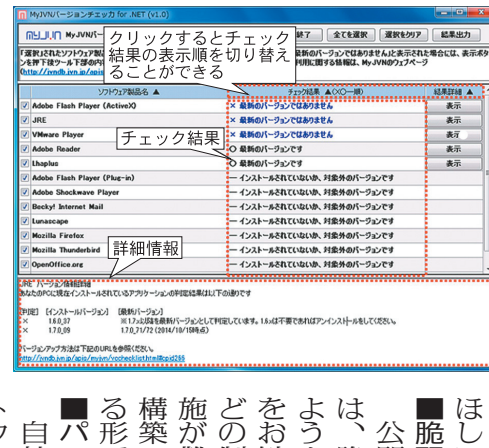
近年、脆弱性が発見されてからそれを悪用した攻撃が発生するまでの期間が一層短くなっている傾向がある。このため、より迅速な対応が求められている。

## 運用段階における四つのポイント

ソフトウエア製品の運用段階における脆弱性対策のポイントは以下の通りである。

### ■ソフトウエア構成や変更履歴の管理

公表された脆弱性が自社に影響するかどうかを判断するためには、自社のソフトウエア構成（ソフトウエアの種類、バージョンなど）や変更履歴（パッチの適用など）を把握しておくことが大切である。IPAでは利用しているソフトウエア製品が最新かどうかを簡単な操作で確認できる「MyJVNバージョンチェッカ」を無料提供しているので活用してほしい。



MyJVNバージョンチェッカ

### ■脆弱性情報の収集

脆弱性情報を収集し、自社に影響し得る脆弱性については対応を検討する。脆弱性情報は一部の例外を除き、製品開発会社から予告なく突然公表されるため、常に情報収集を心掛ける必要がある。IPAでは重要なセキュリティー情報をリアルタイムに配信するサイバーセキュリティー注意喚起サービス「icat for JSON」を無料提供しているので活用してほしい。

### ■脆弱性検査の実施

公開用ウェブサイトは、脆弱性検査を行うようルール化することをお勧めする。予算などの制約で定期的な実施が難しい場合には、構築・改変時に実施する形でも有効である。

### ■パッチの適用

自社で利用するソフトウエアに脆弱性が存在していると判明した場合、対策を適用すべきか否かを判断する必要がある。判断には専門的な知識が必要なため、製品開発会社の提供する脅威および修正適用に伴う影響の情報やセキュリティー製品・サービス提供会社が示す脅威レベルの評価などを参考にする。また、外部の事業者に運用を委託している場合は、相談することも有効である。

なお、近年増えている、未公表の脆弱性を悪用する「ゼロデイ攻撃」については、パッチが提供されるまでの間は一時的な対策としてIPS（侵入防御システム）やWAF（ウェブアプリケーションファイアウオール）で攻撃を抑止し、提供され次第パッチを適用するという対処が可能である。

IPAでは脆弱性対策情報や普及啓発資料を公開している。詳しくはウェブサイト（https://www.ipa.go.jp/security/vuln/index.html）を確認してほしい。

（独立行政法人情報処理推進機構・江島将和）