IT時事ネタキーワード「これが気になる！」（第106回）

「Log4Shell」にご注意。放置せず対策を

2022.09.30

2021年12月9日、英Apache Software Foundationは、同団体がOSS（オープンソースソフトウエア。ソースコードが公開され、無償で誰でも自由に改変、再配布が可能）として提供する「Apache Log4j」（以下、Log4j）の複数バージョンにリモートコード実行の脆弱性（CVE-2021-44228）が存在することを公表した。この脆弱性は「Log4Shell」と呼ばれている。

Log4jは、Java
言語で開発されたエラー情報などのログ（記録）を外部に出力する機能を提供するOSS。Webサーバーならユーザーからアクセスされたurlを記録する、チャットアプリならメッセージの履歴を記録するなどで使われる便利なソフトウエアパーツで、WindowsやLinux、Mac、IoT、家庭用デバイスなどで広く利用されている。

「Log4Shell」と呼ばれる脆弱性とは何か？

今回見つかった脆弱性は、ログとして記録された文字列から一部の文字列を変数として置きかえる機能「JNDI Lookup」を悪用、任意のコード（悪意のあるプログラムなど）を容易にリモート実行できてしまう危険性をはらんでいる。実際、Apache Software
Foundationは、Log4ShellのCVSSレーティング（脆弱性の危険度を表す国際基準）を最高値である「10」としている。

IPAも注意喚起。脆弱性は各種アプリケーションやWebサービスに存在… 続きを読む