

IT時事ネタキーワード「これが気になる！」(第113回)

サイバー攻撃に遭わないための脆弱性対策

2022.12.19



セキュリティ対策関連でよく聞く「脆弱性」という言葉。発見から1年過ぎた今でも対策が困難で問題となっている「Log4Shell」の脆弱性をこの連載で取り上げたのは記憶に新しいだろう。

攻撃は脆弱性を突く。そもそも脆弱性とは？

近年のサイバー攻撃は、不特定多数相手のやたらな「ばらまき」ではなく、ターゲットを決めて計画的に攻撃を仕掛ける、そしていつでも進化し続け効果的な方法を模索している、ということを再三述べているが、そうなると、おのおのの組織が抱えている「脆弱性」が大きな問題となってくる。トレンドマイクロの「サイバー犯罪者はどの脆弱性を悪用しようとしているのか？」によれば、2022年4月27日に米国CISAが公開した「2021年に日常的に悪用された脆弱性」において、最も悪用された脆弱性は、先述の「Log4Shell」だったという。

脆弱性を放置すると、社内システムに侵入されランサムウェア攻撃を仕掛けられるなど組織にとって致命傷を負いかねない。具体的に脆弱性はどこに存在するのか、何からどう塞ぐのかをよく理解して、計画的に対策を行いたい。この点、総務省「国民のためのサイバーセキュリティサイト」の「脆弱性とは」によれば、「ゼロデイ攻撃」も増えているという。情報が公開されたタイミングからできる限り早く対策することが大切だろう。

脆弱性はどこに存在するのか？(技術・プロセス・人・物)… 続きを読む