ニューノーマル処方箋（第27回）

ゼロデイ攻撃はどう防ぐ？

2024.01.22

＜目次＞

未解決の脆弱性が狙われている

「ゼロデイ攻撃」という言葉をご存じでしょうか。これは、ソフトウエアやOSに脆弱性（セキュリティ上の欠陥、弱点）が発見され、修正プログラムが提供される前に、その脆弱性を狙って実行されるサイバー攻撃のことです。ユーザー側が脆弱性に対処するための期間が「0日（Zero-Day）」であることから、このように名付けられています。

脆弱性は一般的に、ソフトウエアやOSが発売された後、開発ベンダーによって発見され、その後、ベンダー側が修正プログラムを配布することによって修正されます。ただし、その脆弱性の存在を、悪意を持った攻撃者がベンダー側よりも先に発見した場合、ゼロデイ攻撃が行われ、当該ソフトウエア、当該OSを使用するユーザーがサイバー攻撃を受ける恐れがあります。

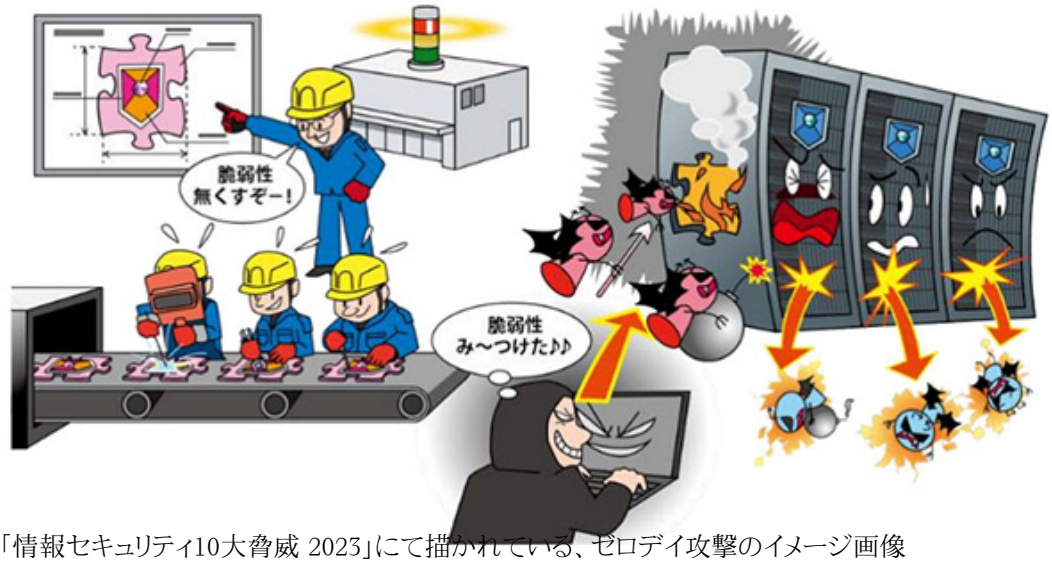
ゼロデイ攻撃はIPA（独立行政法人 情報処理推進機構）が2023年3月に発表した「情報セキュリティ10大脅威 2023」（組織編）の6位にランクインしています。ソフトウエアやOSに脆弱性が存在する限り、今後も発生する可能性は十分に考えられます。

ゼロデイ攻撃の被害を防ぐためには、どうすれば良いのでしょうか？IPAの資料から調査します。

気付かないうちに、今もゼロデイ攻撃を受けている！？

IPAの資料「情報セキュリティ10大脅威 2023」によると、ゼロデイ攻撃の被害は脆弱性の内容によって異なり、ウイルス感染や情報漏えい、Webページのデータ改ざんなど、さまざまなパターンがあるといいます。場合によっては、事業やサービスが停止する恐れもあるとしています。

ゼロデイ攻撃の怖いところは、こうした被害に加えて、防御策がほぼない点にあります。もちろん、すでに修正プログラムが配布済みであれば、それを使えば防ぐことはできますが、ゼロデイ攻撃は修正プログラムが配布される前に攻撃を行うため、ユーザー側は基本的には手の施しようがありません。



「情報セキュリティ10大脅威 2023」にて描かれている、ゼロデイ攻撃のイメージ画像

特に、広く利用されているソフトウエア・OSの脆弱性が、ゼロデイ攻撃に利用された場合、被害はさらに広がる恐れもあります。

2022年には、Microsoftのサービスにおける脆弱性を突いたゼロデイ攻撃が複数発生しました。同年9月、ベトナムのセキュリティ企業である「GTSC」社が、同社が使用するグループウエア「Microsoft Exchange Server」の未修正の脆弱性を悪用するゼロデイ攻撃を受けていたことを公表。これを受けMicrosoftでは、11月に修正プログラムがリリースされるまで、同社が公開している暫定的な緩和策を実施するよう、GTSC社に案内していたといいます。

同年12月には、Googleの脅威分析グループである「Google TAG（Threat Analysis Group）」が、10月に北朝鮮のサイバー犯罪グループによって、Microsoftブラウザー「Internet Explorer（以下、IE）」の脆弱性が悪用されていたことを発表。Google TAGでは、修正パッチの早急な適用と警戒を促しています。

同年12月にはさらに、セキュリティ会社のFortinet社が、同社のセキュリティ製品に搭載されているOS「FortiOS」に、第三者が認証を回避し、任意のコードやコマンドが実行される脆弱性があると発表。同社ではすでにこの脆弱性を悪用する攻撃を確認しているとし、攻撃のログや痕跡等の調査を推奨しています。

このように、ITベンダーが脆弱性を発見したとしても、その時点ですでにゼロデイ攻撃が行われている可能性は十分に考えられます。

ゼロデイ攻撃の対抗策とは… 続きを読む