2022.12.23

サイバーセキュリティニュース ＜2022 No.002＞

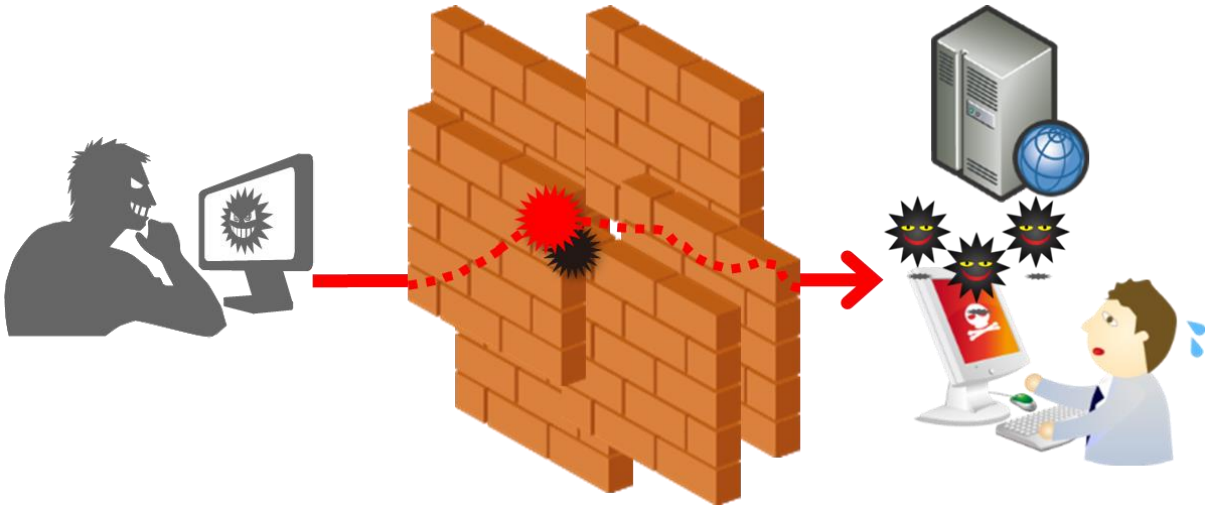
身近な情報機器に潜む「ゼロデイ脆弱性」とその対策

【要旨】
■ OS やソフトウェアにおける技術上の欠陥は日々多数発見されており、悪意をもった攻撃者たちが悪用してサイバー攻撃を仕掛けることができる。
■ 近年は、脆弱性が発見されてから短期間で攻撃が実行され、被害が発生している。
■ 本稿では、脆弱性およびゼロデイ攻撃と対策のポイントについて解説する。

１．脆弱性とは

脆弱性とは、コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを指し、「セキュリティホール」とも呼ばれる。脆弱性が存在すると、悪意をもった攻撃者たちが悪用してサイバー攻撃を仕掛けることができる。

脆弱性は、設定変更によりすぐに対処できる場合もあるが、ソフトウェアを開発したメーカーから脆弱性を解消するための修正プログラムが配布されるのを待たなければならないことも多い。ユーザーにおいては、修正プログラムが配布されたのち、OS やソフトウェアのアップデートが必要となる。たとえば、Windows の場合には Windows Update によってそれまでに発見された脆弱性を塞ぐことができる。修正プログラムは、自動で更新が行われるものもあれば、手動で更新を行わなければならないものもある。



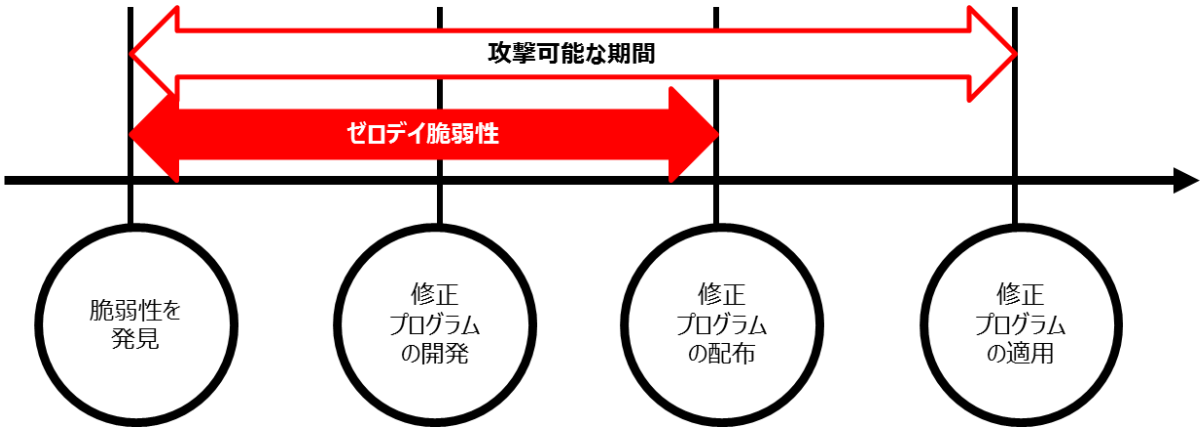
【図１】セキュリティホールのイメージ

２．ゼロデイ攻撃とは

近年は「ゼロデイ攻撃」と呼ばれる手法が増加している。ゼロデイ攻撃とは、OS やソフトウェアに対する脆弱性が発見されたときに、メーカーが修正プログラムを配布するまでの間に、その脆弱性を利用して行われる攻撃を指す。脆弱性情報を迅速に共有するために脆弱性情報データベースが構築されているが、悪意を持った攻撃者はこうした脆弱性情報を参照して、脆弱性が発見されてから短期間でエクスプロイト（脆弱性を利用した不正プログラム）を用いた攻撃を実行する。発見された脆弱性の内容によっては、非常に大きな脅威となる。

なお、修正プログラムがリリースされているのに、適用しないまま放置している原因として主に以下の３つが挙げられるが、「ゼロデイ」の状態が継続していることになり、非常に危険である。

・修正プログラムがリリースされていることを知らない
・レガシーシステム（メーカーのサポート対象外）を使用している
・自社の保有する IT 資産を把握していない



【図２】ゼロデイ脆弱性と攻撃可能な期間

独立行政法人情報処理推進機構（IPA）は、前年に発生した情報セキュリティ事故や攻撃の状況等から注意すべき脅威を選出した「情報セキュリティ 10 大脅威」を公開している。2022 年に発表された 10 大脅威の組織編 7 位に「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」が初めてランクインした。

【表１】「情報セキュリティ 10 大脅威 2022」2022 年 1 月 27 日公開（独立行政法人情報処理推進機構）

	10大脅威 2022（組織編）
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報の窃取
3位	サプライチェーンの弱点を悪用した攻撃
4位	テレワーク等ニューノーマルな働き方を狙った攻撃
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） 初
8位	ビジネスメール詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10 位	不注意による情報漏えい等の被害

３．ゼロデイ脆弱性の被害実例

以下にて近年公表された重大な脆弱性の一例を紹介する。

【表２】重大な脆弱性の事例

脆弱性	CVE[1]コード	概要
「Apache Log4j」に存在するリモートから悪用可能な脆弱性	CVE -2021-44228	Java のログ出力ライブラリである Apache Log4j が動作するサーバーにおいて、遠隔の第三者が本脆弱性を悪用する細工したデータを送信することで、任意のコードを実行する可能性がある
iOS 16（iPhone 8 以降）メモリ処理に関する脆弱性	CVE-2022-42795	悪意を持って作成された画像を処理すると、任意のコードが実行される可能性がある
Apple Music on Android の脆弱性	CVE-2022-32836	Android バージョン 5.0 以降の OS において、App が重要なユーザデータにアクセスできる可能性がある
Fortinet 製品の認証バイパスの脆弱性	CVE-2022-40684	認証されていない遠隔の第三者が、同製品の管理インタフェースに細工した HTTP あるいは HTTPS リクエストを送信し、結果として任意の操作を行う可能性がある

※公開情報をもとにＭＳ＆ＡＤインターリスク総研が作成

こうした重大な脆弱性を悪用され、被害が発生した実例は以下のとおり。

【表３】脆弱性を悪用した被害実例

時期	主体	被害	概要
2022 年 1 月	EC サイト運営企業	・15,000 件以上のカード情報漏えいのおそれ	■ EC サイトの脆弱性を悪用し不正な注文データを生成 ■ 決済代行業者からのクレジットカード不正利用の通報で発覚
2022 年 2 月	Web サイト運営企業	・顧客のメールアドレス約 10 万件が窃取	■ web サーバの異常な負荷を運用管理者が発見、脆弱性を悪用した SQL インジェクションの攻撃と判明
2022 年 4 月	一般企業	・ランサムウェアに感染	■ VPN 装置の脆弱性を悪用して認証情報を窃取し不正侵入、ランサムウェアに感染 ■ 企業の導入していた監視システムが異常を検知、フォレンジック調査等に約 1500 万円を要し、6 日間業務が停止した
2022 年 5 月	一般団体	・ランサムウェアに感染	■ VPN 装置（Fortigate）の脆弱性を悪用され、LockBit2.0 に感染し、システム障害が発生、脅迫文が大量に印刷され、一時業務停止となる
2022 年 11 月	医療機関	・電子カルテシステム障害 ・診療受付停止	■ 委託先の給食業者のリモートアクセスシステムの脆弱性を利用した攻撃によりランサムウェアに感染、電子カルテシステム等が停止

※公開情報をもとにＭＳ＆ＡＤインターリスク総研が作成

[1] 「CVE」は Common Vulnerabilities and Exposures（共通脆弱性識別子)は、個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子。脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利用している。個別製品中の脆弱性に一意の識別番号「CVE 識別番号(CVE-ID)」を付与することにより、組織 A の発行する脆弱性対策情報と、組織 X の発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付けに利用したりできる。

４．対策のポイント

日々新たな脆弱性が発見されており、「100%安全な製品・サービス」はなく、ゼロデイ攻撃を完全に防ぐことは非常に困難である。「侵入される確率を下げること」と「侵入された際に早期に発見できること」が被害を最小化する上で重要なポイントとなる。

以下にて対策の事例を示す。

（１）迅速なパッチ適用

OS やソフトウェアのアップデートが公表されたら、速やかに適用することが重要である。システムがバージョンアップされるとき、その更新内容には、バグへの対策や脆弱性を塞ぐ修正プログラムなどが含まれる。なお、パッチの適用により脆弱性を塞いでも新たな脆弱性が発見される可能性があるため、常に OS やソフトウェアの更新情報を収集して、できる限り迅速にアップデートを行う必要がある。また、システムの最新バージョンへの更新は、新機能の追加や既存機能の改善が含まれる場合もある。

なお､サポート対応を終了した旧バージョンの OS やソフトウェアにおいて不具合が生じても、メーカーによるサポートが受けられないケースがあることにも留意されたい。

メ リ ッ ト：(原則として)費用が掛からず、手軽にできる。

デメリット：開発元メーカーが配布した修正プログラムを適用するまで、悪意を持った攻撃に対しては無防備となる。更新プログラムの中には、自ら最新情報を探しに行く必要がある。

（２）サンドボックス

サンドボックスとは、仮想環境上に構築されたパソコンでファイルの挙動を観察し、不審な動きがないかを確認することで未知のマルウェアを検知し、侵入を防ぐ仕組みである。

例えば、受信メールをサンドボックス内で開封し、添付ファイルやメール内のリンクを検証、問題のあるプログラムが含まれていれば、ユーザーに通知するような機能である。

メ リ ッ ト：未知の脅威に対応でき、安全な環境下で動作確認・分析が可能で、削除等の対処を行うことができる。システム管理者などの運用の変更や負荷が生じづらい。

デメリット：導入コストがかかる。

（３）EDR

IPA は、前述の対策に加えて「外部からの侵入を検知および防御する機器を導入するなどの備えが重要」と呼び掛けており、この検知・防御機能を持ったセキュリティ製品の代表格が EDR である。

EDR は、Endpoint Detection and Response の略称であり、エンドポイントの不審な挙動を監視し、マルウェアが攻撃を開始する前、あるいは攻撃を開始した際にそれを検知し、ユーザーに通知して即時対処を行う機能を持つ。EDR を導入することで、マルウェアが侵入し攻撃を開始した初期段階で食い止め、被害を最小化することができる。

EDR サービスの選定にあたっては、自社の運用に無理なく組み込めるサポートサービスの有無が重要となる。IPA は、特に中小企業に使いやすいサービスとして「サイバーセキュリティお助け隊サービス制度」を立ち上げており、この制度に登録されたサービスのうち半数以上が EDR 製品である。

メ リ ッ ト：マルウェアの侵入や感染した場合、速やかな検知と対応が可能なため、被害を最小限に留めることができる。ログが残るので被害状況を確認するための情報収集が

容易となる。

デメリット：自社の業務内容に応じたチューニングが必要。チューニングが適切でないと過検知や誤検知により通常業務が阻害される可能性がある。監視サービスが有償、あるいは限定的なサービスとなっている場合は、コスト・運用負荷が高くなる。

発見された脆弱性への根本的な対応は、（1）迅速なパッチ適用である。迅速かつ確実な脆弱性対応を実施するためには、以下を実施・運用する体制や手順を整備することが重要である。

・あらかじめ自組織で使用している全てのハードウェア、ソフトウェア、サービスを把握できる
・タイムリーに脆弱性情報を取得できる
・脆弱性が確認されたときにはすぐに対応できる

昨今、サイバー攻撃は多様化・巧妙化しており、また、サプライチェーンを介したサイバーセキュリティ関連被害が拡大している。予防に傾注した対策だけでは被害の回避は不可能であり、自社の実態にあった効果的な対策を「多重的に」実施することが肝要となる。

自社を取り巻く現状とリスク対応能力を把握し、「自社でできること」と「専門家（外部）へアウトソースすること」を整理した上で更なる対策の強化や適切なリスク対応の実施が望まれる。

ＭＳ＆ＡＤインターリスク総研株式会社
リスクマネジメント第三部 サイバーリスクグループ
マネジャー・上席コンサルタント　槇　健介

ＭＳ＆ＡＤインターリスク総研株式会社の EDR サービス「防検サイバー」は、経産省・IPA によるサイバーセキュリテイお助け隊サービスに登録されており、簡易サイバー保険、緊急時の相談窓口、24時間の監視機能などを満たしたサービスとなっています。

詳しくは以下のホームページをご覧ください。

ＭＳ＆ＡＤインターリスク総研株式会社「防検サイバー」

https://www.irric.co.jp/lp/boukencyber/index.php

ＭＳ＆ＡＤインターリスク総研株式会社は、MS&AD インシュアランスグループに属する、リスクマネジメントについての調査研究及びコンサルティングに関する専門会社です。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
リスクマネジメント第三部 サイバーリスクグループ
東京都千代田区神田淡路町2-105　**TEL.03-5296-8932**
https://www.irric.co.jp/