脆弱性対策ソリューション

増加するソフトウェアの脆弱性

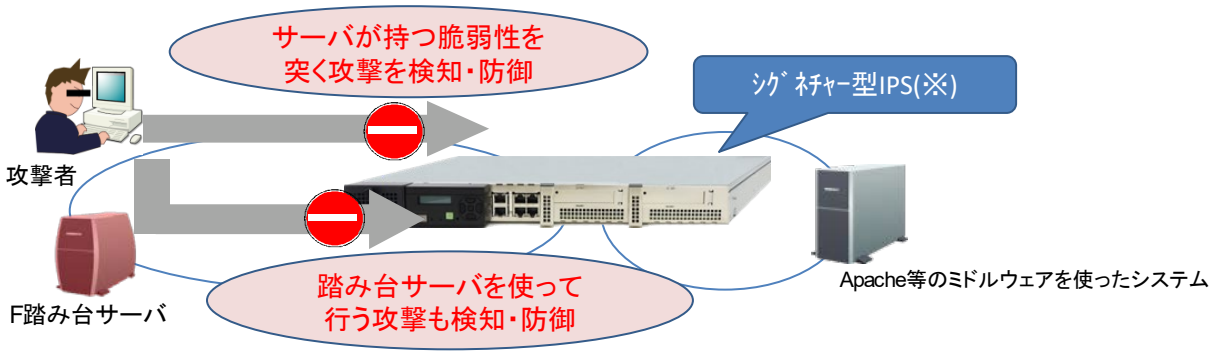
- 最近、重要なソフトウェアにおいて、致命的な脆弱性が見つかっており、社会問題となっています。
- ソフトウェア改版は時間がかかり(情報収集、検証、適用など)、適用時にサービスが停止する場合があります。

ネットワークアプライアンスで迅速に脆弱性対策を実現する方法がお勧め！

最近のソフトウェア脆弱性を、IPCOM EX2シリーズを使って対策する方法

脆弱性	影響	対策ソリューション
CVE-2021-44228	Apache Log4j には任意のコードが実行可能な脆弱性があります。 この脆弱性により、これにより、遠隔の攻撃者が細工した 文字列を脆弱なシステムのログに記載させ、結果として 任意の Java コードをシステムに実行させることが可能です。	シグネチャー型IPSの導入

シグネチャー型IPSでは、過去にもOpenSSLの脆弱性(CVE-2014-0160)、Strutsの脆弱性(CVE-2014-0094他) の脆弱性に対応したソリューションもありました。



※シグネチャー型IPSを使っている場合は、最新のシグネチャーを適用するだけで攻撃検知が可能で、警察庁(注)によれば12/15から本脆弱性を突いた攻撃の増加が観測されていますが、IPCOMのシグネチャーは攻撃が本格化する前の12/14にシグネチャーを公開済。
注: https://www.npa.go.jp/cyberpolice/important/2021/202112141.html

- 価格例

製品名	型名	標準価格(税別)	備考
IPCOM EX2-3200(※1)	IX2S082A	¥1,980,000	
100V電源ケーブル(※1)	IX2HPCNA	¥5,500	
IPCOM EX2-3500/3200用HDD1(※1)	IX2HHD1A	¥110,000	
IPCOM EX2-3000 SCソフトウェア V01(※1)	NB7548101	¥198,000	
シグネチャー型IPSサポートサービス(EX2-3200)(※1)	NSIPES02N	¥396,000	年額：脆弱性を突く攻撃を検知・防御
WAFライセンス(※2)	NB754098	¥1,320,000	Webアプリケーションの脆弱性を突く攻撃を検知・防御

※1： 本ソリューションの対策製品・サービス
※2： Webアプリケーションの脆弱性として導入を推奨

商品・サービスについてのお問い合わせは
富士通コンタクトライン（総合窓口） 0120-933-200
受付時間：9:00～12:00および13:00～17:30（土曜・日曜・祝日・当社指定の休業日を除く）
富士通公開サイト https://jp.fujitsu.com/ 詳細はこちら https://www.fujitsu.com/jp/nwps/ipcom/