今求められる脆弱性対策
～ 侵入経路として注目されるVPN装置の脆弱性と普及期に入ったSBOMでの管理 ～

株式会社サイバーセキュリティクラウド

会社紹介

世界有数のサイバー脅威インテリジェンスとAI技術を活用し、
全世界に安心安全なサイバー空間を創造するサービスを提供します。

CYBER SECURITY CLOUD

世界中の人々が安心安全に使える
サイバー空間を創造する

サイバー
セキュリティ

AI

サイバーセキュリティクラウドの提供サービス

自社開発・自社サポートで全世界に提供しています。

クラウド型WAF

攻撃遮断くん

外部からのサイバー攻撃を検知・遮断し、
情報漏えいやサービス停止などから
Webサーバ・Webサイトを守る
クラウド型Webセキュリティサービス

※1

WAF自動運用サービス

Waf Charm

パブリッククラウドで提供されている
WAFを「ビッグデータ」の活用で
自動運用することが可能なサービス

※2

AWS WAFルールセット

AWS WAF Managed Rules

AWS Marketplaceから購入可能な
世界90ヶ国以上へ提供する
AWS WAF専用のルールセット

※3

AWS環境フルマネージドセキュリティサービス

CloudFastener

AWSのセキュリティリスクの可視化、
OS・ソフトウェアの脆弱性や設定ミス、
クラウド環境の脅威を収集・分析し、
包括的に管理し運用するサービス

脆弱性情報収集・管理ツール

SIDfm

OS・アプリケーション・ネットワーク
製品の脆弱性情報を自動で収集・蓄積し
脆弱性対応の運用を効率化するツール

※4

脆弱性確認・検証

脆弱性診断サービス

診断ツールを使った自動診断と、
専門家による手動診断の
両方を合わせたハイブリッドで
高品質な脆弱性診断サービス

※1デロイト トーマツ ミック経済研究所調べ　調査概要：外部脅威対策ソリューション市場の現状と将来展望　2023年度
※2 日本マーケティングリサーチ機構調べ　調査概要：2020年7月期_実績調査
※3 2022年10月時点
※4 日本マーケティングリサーチ機構調べ　調査概要：2021年8月期_実績調査

昨今の脆弱性問題

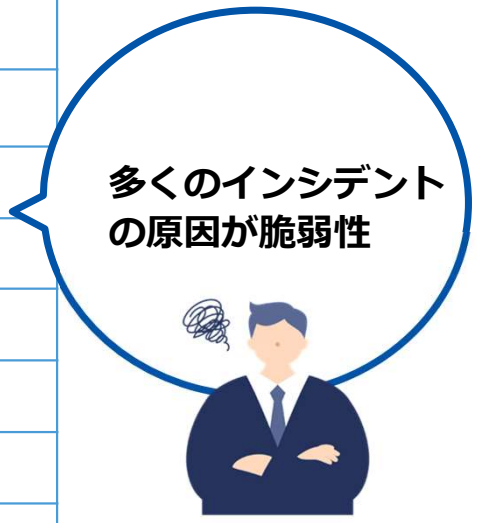
～侵入経路として注目されるVPN装置の脆弱性～

セキュリティ被害の多くの要因が脆弱性

IPA（独立行政法人情報処理推進機構）が発表した「情報セキュリティ10大脅威 2024」の発生要因の多くが脆弱性に関係しています。

順位	組織におけるセキュリティ被害	インシデントの発生要因
1位	ランサムウェアによる被害	OS・ソフトウェアの脆弱性／注意の欠落
2位	サプライチェーンの弱点を悪用した攻撃	OS・ソフトウェアの脆弱性／セキュリティ対策レベルの格差
3位	内部不正による情報漏えい	情報管理の不足
4位	標的型攻撃による機密情報の窃取	OS・ソフトウェアの脆弱性／注意の欠落
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	OS・ソフトウェアの脆弱性
6位	不注意による情報漏えい等の被害	注意の欠落
7位	脆弱性対策情報の公開に伴う悪用増加	OS・ソフトウェアの脆弱性／対応の遅れ
8位	ビジネスメール詐欺による金銭被害	注意の欠落
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	監視・社内連携の不備
10位	犯罪のビジネス化（アンダーグラウンドサービス）	OS・ソフトウェアの脆弱性／情報管理の不足

出典：IPA「情報セキュリティ10大脅威 2024　https://www.ipa.go.jp/security/10threats/10threats2024.html



脅威1位の「ランサムウェア」被害事例

製造業

公表日/2022年3月1日

リモート接続機器にあった脆弱性がきっかけで、
ランサムウェアに感染。攻撃被害を受けた当日、
工場ラインをすべて停止

医療機関

公表日/2021年10月31日

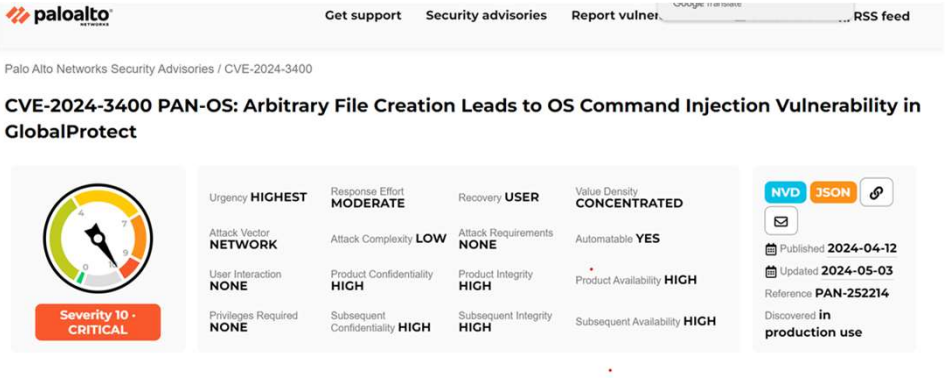
電子カルテをはじめとする院内システムがランサムウェアに
感染し、カルテが閲覧できなくなるなどの大きな被害が
生じる。復旧までに2か月の期間がかかる

ランサムウェア被害の多くの原因は
ハードウェアの基本的な制御を行うために機器に組み込まれた
ファームウェアを
アップデートせずに脆弱性を放置
してしまうこと

直近の脆弱性情報

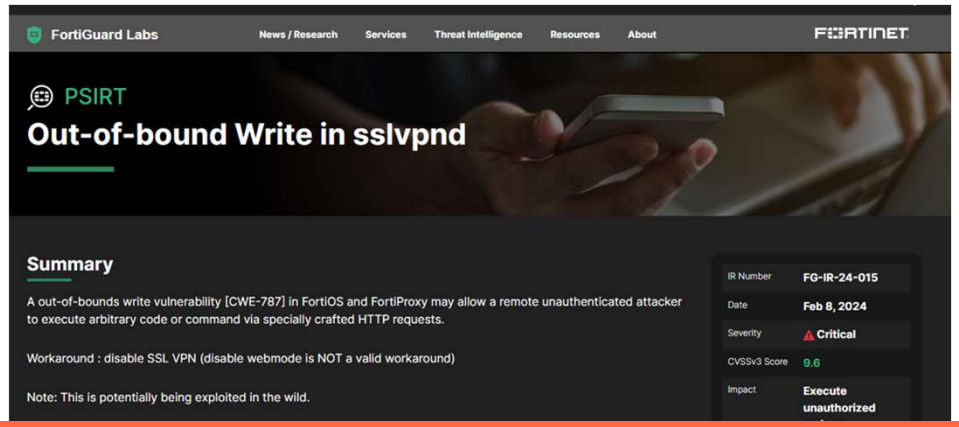
2024年4月
PAN-OS の GlobalProtect 機能に関する脆弱性

本脆弱性の悪用により、認証されていない遠隔の第三者が、ルート権限で任意のコードを実行する可能性があります。日本国内でもこの脆弱性による被害が報告された



2024年2月
Fortinet FortiOSで重大な脆弱性が発見

攻撃者がこの脆弱性を悪用することで、任意のコードやコマンドを実行する恐れがある。



このような脆弱性が発見されると、多くの場合、ソフトウェアを開発したメーカーが
更新プログラムを作成して提供します。

しかし、脆弱性は完全に対策を施すことが困難であり、次々と新たな脆弱性が発見されているのが現状です。

脆弱性対策に必要なこと

脆弱性は日々報告されるため、利用しているOSやソフトウェアに関する情報を正確に把握し、アップデートの必要性や優先順位を決め、最終的な対処の判断を迅速に行う日々の運用が必要となります。

情報収集			トリアージ		最終評価
対象製品	危険度	事象	判断基準	優先順位	対策
CentOS7	medium	サービス停止	不正アクセスではない	低い	3ヵ月以内に対応
WordPress	medium	情報漏洩	情報漏洩の可能性あり	高い	即時対応
FortiOS	high	任意のコード実行	情報漏洩の可能性あり	高い	該当モジュールの利用無し、対応不要

一方でこんな課題があります

システムの安全を維持するために必要な脆弱性対策ですが、多くの手間を要するのが課題です。

情報収集

- JPCERT/CCやJVNの情報を日々チェックするのに時間を取られている
- 最適なパッチを探すのがかなり大変

影響する情報の特定

- どれが自分たちに必要な情報なのかわからない
- 英語の脆弱性情報を正しく理解することが難しい

評価・優先順位づけ

- パッチ適用は後回しになってしまい、未対応のままになっている
- 対策基準が属人化してしまっている

対処・管理

- 実際にどれほど対処されているのかわからず不安
- 対策状況に関する問い合わせへの対応に困る

その様な状況でも、
ますます求められる脆弱性の管理
～ 普及期に入ったSBOMでの管理 ～

脆弱性管理に関するガイドライン等

各種ガイドラインで脆弱性対応の義務化がすすんでいます。

PCI-DSS v4.0（クレジットカード業界のセキュリティ基準）
脆弱性管理に関する要件（要件6）

厚生労働省「医療機器の基本要件基準」
サイバーセキュリティに関する要求事項が第12条第3項として規定

経済産業省「ECサイト構築・運用セキュリティガイドライン」
2024年度末　脆弱性対策の義務化を予定

自動車産業サイバーセキュリティガイドライン
脆弱性にまつわる要求事項多数

SBOM（ソフトウェア部品表）
サイバーセキュリティ向上を目的とした米国大統領令が起点となり、世界的に普及が進行

SBOM（Software Bill of Materials）とは

SBOM とは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストのことで、日本語では「**ソフトウェア部品表**」とも呼ばれます。

SBOM は、米国商務省の電気通信情報局（NTIA）が 2018 年 7 月より開始した実証を通じて注目され始め、**2021 年 5月に米国バイデン大統領が署名した大統領令を一つの起点**として、世界的に普及が進みつつあります。

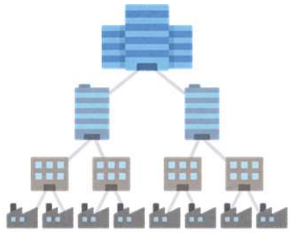
日本では経済産業省が2023年7月に「ソフトウェア管理に向けたSBOMの導入に関する手引」を公開しました。これらの取り組みにより、SBOMの導入サポートや生成ツールが多く登場し、SBOMを導入する企業が徐々に増加しています。

SBOMが求められる背景

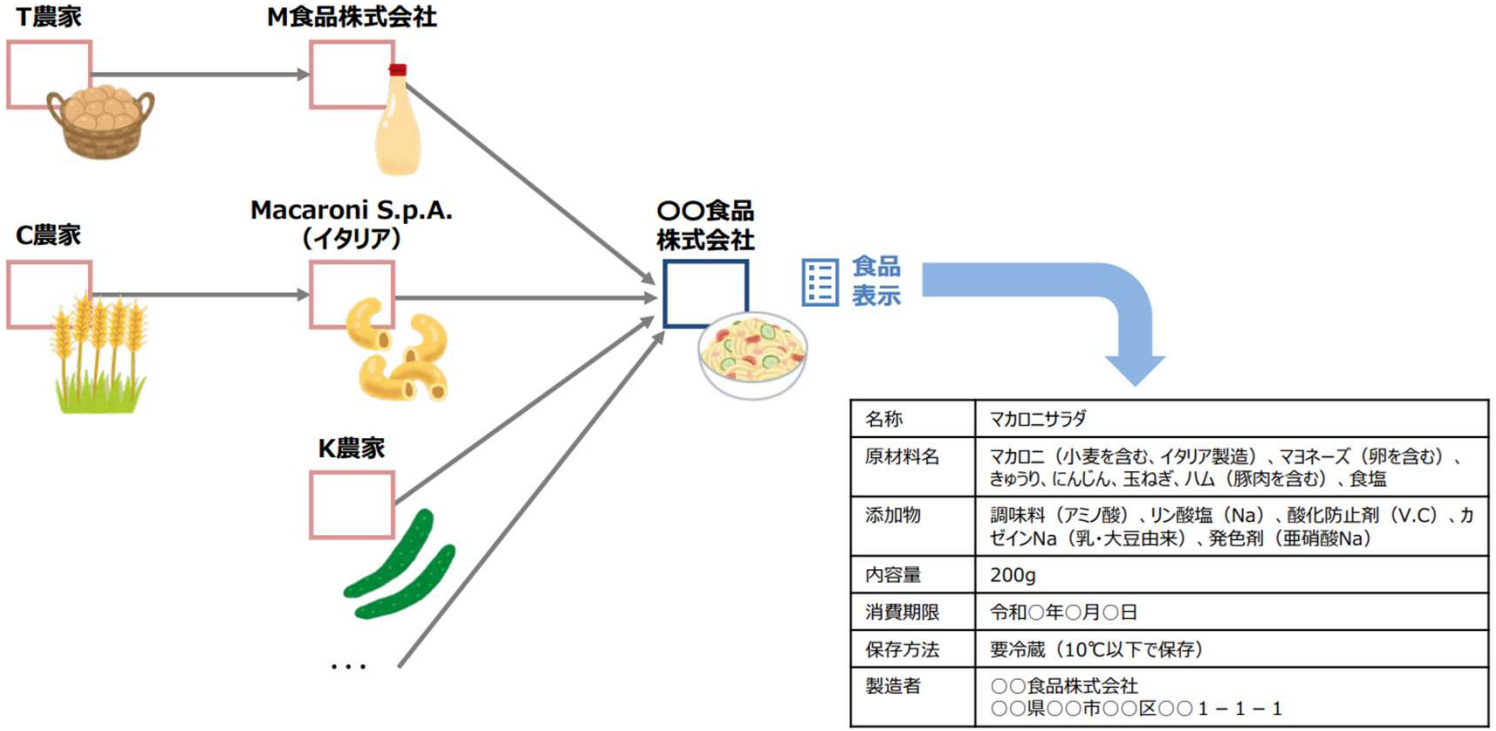
ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、自社製品において利用するソフトウェアであっても、コンポーネントとしてどのようなソフトウェアが含まれているのかを把握することが困難な状況があります。

組織内の IT システムで利用されているソフトウェアを資産管理している組織は多いが、開発者が直接利用している上位のコンポーネントのみが資産管理の対象となり、直接利用のコンポーネントに内包されて間接的に利用される下位のコンポーネントの多くは資産管理の対象外となっています。

したがって、脆弱性情報と資産管理台帳を照らし合わせるだけでは、下位のコンポーネントとして利用される OSS のようなコンポーネントにおいて脆弱性が発見された場合に、間接的な脆弱性の影響を検知することができません。



SBOMを例えるなら「食品表示」



名称	マカロニサラダ
原材料名	マカロニ（小麦を含む、イタリア製造）、マヨネーズ（卵を含む）、きゅうり、にんじん、玉ねぎ、ハム（豚肉を含む）、食塩
添加物	調味料（アミノ酸）、リン酸塩（Na）、酸化防止剤（V.C）、カゼインNa（乳・大豆由来）、発色剤（亜硝酸Na）
内容量	200g
消費期限	令和〇年〇月〇日
保存方法	要冷蔵（10℃以下で保存）
製造者	〇〇食品株式会社 〇〇県〇〇市〇〇区〇〇１－１－１

食品サプライチェーン及び食品表示の概念的イメージ

食品表示と異なり、SBOM はコンポーネント名だけでなく、そのバージョンや依存関係についても記載するため、食品表示より複雑なリストとなる。
また、多くの SBOM は作成後も動的に変更されるため、SBOM 利用者での管理が重要となる。

出典：経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引Ver.1.0」

SBOMのメリット

○ 脆弱性管理のメリット

- 脆弱性に関する情報を収集し、SBOM の情報と突合して脆弱性を検出することで、**ソフトウェアにおいて脆弱性が残留するリスクを低減**できる。
- SBOM ツール等を用いることにより新たな脆弱性をリアルタイムで検出し、影響を判断することで、**初動期間を短縮**できる。
- SBOM ツールを用いた自動管理により、手動での管理と比較して、**管理コストを低減**できる。

○ ライセンス管理のメリット

- OSS の特定漏れによる**ライセンス違反のリスクを低減**できる。
- SBOM ツールを用いた自動管理により、手動での管理と比較して、**管理コストを低減**できる。

○ 開発生産性向上のメリット

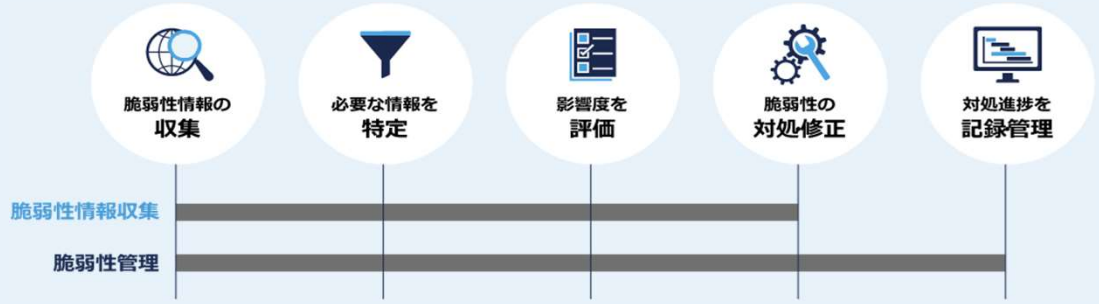
- コンポーネントに関する問題を早期に特定することで、**開発遅延の発生を防ぐ**ことができる。
- コンポーネントに関する問題を早期に特定することで、**対応コストを低減**できる。
- 使用するコンポーネントを選定する際、類似製品に関する過去の SBOM を参照することで、**選定に関する工数を削減**できる。
- 認証対応、法令対応、輸出規制管理対応などの効率化

脆弱性情報収集・管理ツール 「SIDfm」のご紹介

脆弱性情報収集・管理ツール「SIDfm（エス・アイ・ディー・エフエム）」とは

「SIDfm」は、脆弱性対応の運用を効率化するツールです。
OS・アプリケーション・ネットワーク製品の脆弱性情報を世界中から**自動で収集・蓄積**します。自社に必要な情報だけをすぐに特定できる機能で対策すべき脆弱性とその**対策内容が一目でわかります**。さらに、脆弱性の対処進捗の**記録・管理**まで行うことができます。

SIDfm



「SIDfm」ラインアップ

あなたの会社のニーズや環境にあわせて選べる3つのタイプ

脆弱性情報 収集サービス	システムの脆弱性対策のために、環境に合わせた脆弱性情報の収集効率をあげたい方。	SIDfm IG
脆弱性管理 サービス	ホストの実態把握から脆弱性状態管理まで行いたい方、または自社のセキュリティポリシーに合わせたトリアージや通知をしたいなど、独自ルールで運用を自動化したい方	SIDfm VM
脆弱性情報 コンテンツ提供	既存のシステムやプラットフォームに脆弱性情報コンテンツを取り込み、自社独自のシステムを構築したい方。	SIDfm API

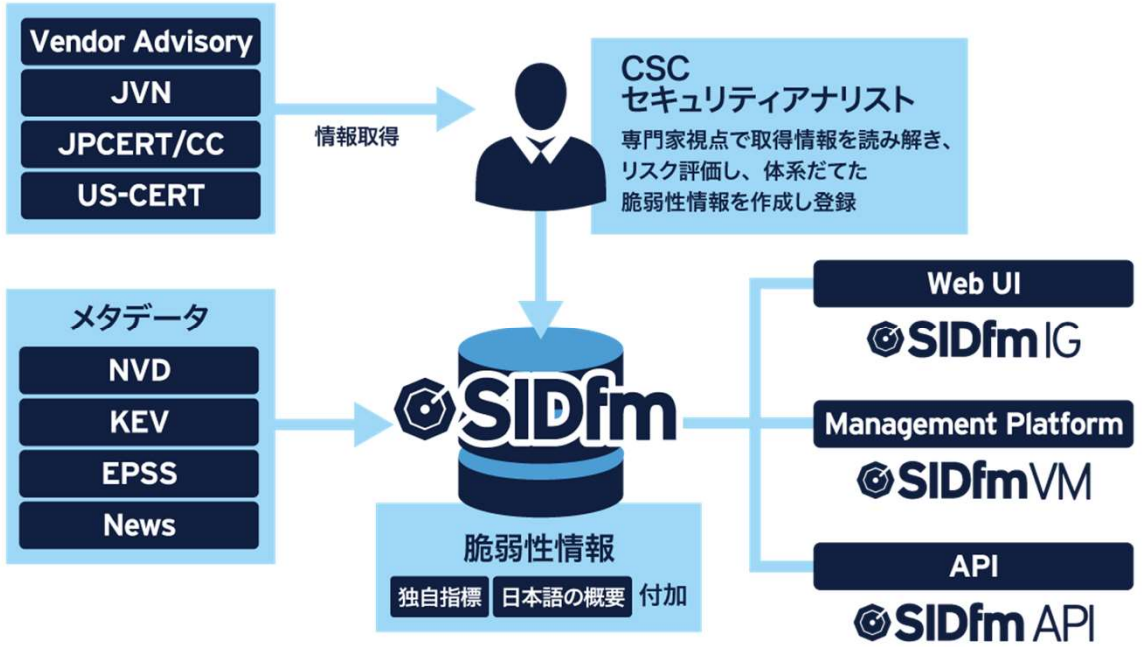
VPN機器の脆弱性にも対応

SBOMにも対応

SIDfmの最大の特徴は、そのコンテンツの質です！

「SIDfm」の最大の特徴はコンテンツの質です。NVD、KEVなどのメタデータとベンダーのアドバイザリー情報、JVNなどの情報をセキュリティアナリストが専門家視点で読み解きリスク評価し**「独自指標」「日本語の解説」を付加**した脆弱性情報を提供しています。

「SIDfm」の情報だけで、概要から影響を受けるバージョンや対処方法などが**日本語ですぐに理解・把握できるため、優先すべき脆弱性の対処にリソースを集中させることができます。**



特徴1

工数削減

フィルタ機能で必要な脆弱性情報だけをピックアップ

- フィルタ機能で必要な製品を登録することで、自社に必要な脆弱性情報の収集が可能。
- 製品名だけでなく、CVSS基本値、危険度、影響範囲、特定日を設定することにより、その条件にマッチする脆弱性情報を収集することが可能です。
- メール通知やチャット投稿にも対応しているので、登録した製品の脆弱性情報が発見された場合、SIDfmにログインすることなく脆弱性情報を確認できます。

特徴2

通知内容を確認するだけで脆弱性情報が理解できるので、担当者はその内容を確認するだけで対応可能

- 世界中の脆弱性情報をSIDfmが収集。**日本語のコンテンツ**で脆弱性の内容、パッチ情報や回避方法などの対策情報も含めて一目で確認可能です。

- いままで行っていたベンダーサイトを閲覧して対処方法の確認をする手間がなくなるので、工数を大幅削減できます。

特徴3

定量的な数値で脆弱度を判断することができるので属人的な運用から脱却できる

- 共通脆弱性評価システムCVSSを採用し、個々のセキュリティホールの脆弱度を定量的に数値で評価。組織内で共通の基準で判断することができます。

- 影響を受けるシステム(プロダクト)が実際に攻撃されたときの脅威(深刻度)も細かく分類されているため、自社で所有している資産の「リスク分析」も一瞬で可能です。

特徴4

脆弱性の対処状況を一元管理できる

- IT資産の脆弱性の対策状態管理や作業記録などをパッケージ単位で組織内一元管理。CVE毎に対応を検討する必要がないので、効率的に管理ができます。

- 脆弱性チケットごとの対応予定日のスケジュールやステータス、作業メモをSIDfmVM上でリアルタイムに共有できるため、日々の進捗管理を効率化できます。

導入実績

1999年に日本で初めて脆弱性情報の提供を開始。
業界を問わず多くのお客様にご利用いただいています。

累計導入社数 1,500社以上

※ 日本マーケティングリサーチ機構調べ　調査概要：2021年8月期_実態調査

導入企業様
一例

導入事例：株式会社クロス・プロップワークス

脆弱性情報の収集業務に費やしていた時間をおよそ10分の1に削減できたことで、運用範囲を拡大できました。

企業概要
株式会社クロス・コミュニケーションの100%出資子会社として2015年4月に設立。ITソリューションマーケティングリサーチを中心とした各種BPO事業を展開。拠点は函館にあり、従業員は道内出身者が7割、関東圏等本州出身者が3割の130名体制で、クロス・コミュニケーショングループ内のマーケティング活動における各種業務やウェブサイトの保守運用などを担当している。

導入前の課題

- 数多くのアプリ・システムの運用を実施しているため脆弱性情報の収集をアプリごと・システムごとに実施する必要があり多くの工数がかかっていた。
- 開発後年数が経過しているアプリ・システムもあり、バーションアップ情報も含めて様々な情報を得たいと考えていた。

導入後の成果

- SIDfmを導入し、脆弱性情報が一括で収集できるようになり、大幅な工数を削減できるようになった。
- 工数を削減できたことに伴い、今までは調査対象を絞っていたが運用範囲を拡大することができた。
- バージョンごとの脆弱性の調査に今まで時間がかかっていたが、フィルタ機能で瞬時に判断できるようになった。

導入事例：伊藤忠テクノソリューションズ株式会社

脆弱性の脅威レベルが明確になり、運用工数を大幅に削減できました。

企業概要
コンピュータ、ネットワーク、アプリケーションによるコンサルティングからシステムの開発、運用・保守、管理、アウトソーシングなどのトータル・ソリューションの提供を行なうシステムインテグレーター。伊藤忠商事グループの主要子会社。略称CTC。東京証券取引所市場第一部上場。

導入前の課題

- マルチベンダー環境において、さまざまな情報元から脆弱性情報を収集・確認しなければならない。
- メーカーからの脆弱性通知のレベルは、それぞれの基準で通知されるため、お客様への対応基準の説明が困難だった。

導入後の成果

- 脆弱性情報の収集工数、サービス運用工数が大幅に削減でき、費用対効果が非常に高い。
- 運用上の脆弱性対応基準が明確になり、お客様が安心いただけるサービス品質を保つことができる。
- 脆弱性の脅威レベルが明確になった。

まとめ

- ✓ VPN機器を含めた自社に必要な脆弱性情報だけを収集可能できる。
- ✓ パッチ情報・対処方法も日本語でわかりやすいのでベンダーサイトで調べ直す必要なし。
- ✓ 定量的な数字で対応基準を決めることができるので脱属人化できる。
- ✓ 脆弱性の対応状況・作業記録を一元管理できる
- ✓ SBOMでの脆弱性管理もできる

SIDfmで自社に必要な脆弱性情報から対応状況の一元管理まで行うことが出来るため脆弱性情報の収集・管理を効率化・工数削減することが出来ます！

SIDfm

CYBER SECURITY CLOUD

世界中の人々が安心安全に使える
サイバー空間を創造する

Apendix

SIDfmとJVNの情報の違い

SIDfmは、**正しくリスクを判断できるだけの情報**を提供しています！

SIDfm

Linux Kernel の ALSA シーケンサの処理にサービスを妨害される問題

ID	28397	登録日	2018/04/05	最終更新日	-
CVSSスコア	6.6	影響範囲	ローカル	危険度	M

CVE	CVE-2017-16528				
攻撃コード	攻撃コード・実証コードは確認されていません。				
CVSS	UI PR AC S AV C A I 6.6	攻撃元区分 (AV)	物理 (P)	ローカル (L)	隣接 (A) ネットワーク (N)
		攻撃条件の複雑さ (AC)	高 (H)		低 (L)
		必要な特権レベル (PR)	高 (H)	低 (L)	不要 (N)
		ユーザ関与レベル (UI)	要 (R)		不要 (N)
		スコープ (S)	変更なし (U)		変更あり (C)
		機密性への影響 (C)	なし (N)	低 (L)	高 (H)
		完全性への影響 (I)	なし (N)	低 (L)	高 (H)
		可用性への影響 (A)	なし (N)	低 (L)	高 (H)

概要 | 影響を受ける製品 | 影響などの確認方法 | 対処方法 | 関連情報 | 更新履歴 | 一括表示

Linux Kernel は OS の基本的な機能 (アプリケーションソフトウェアや周辺装置の監視、ディスクやメモリなどの管理、プロセス間通信など) を提供します。

Linux Kernel は、ALSA シーケンサの処理が原因でセキュリティホールが存在します。

このセキュリティホールを利用された場合、ローカルの攻撃者に細工された USB デバイスを使用されることによって、システムを不正に停止されサービスを妨害されるなどの攻撃を受ける可能性があります。

これは Linux Kernel の snd_seq_device_load_drivers 関数および snd_seq_device_dev_free 関数 (sound/core/seq_device.c) において、デバイスの取り外しを適切に行っていないため、競合状態を起こすことで解放したメモリ領域へアクセスする可能性のあることが原因となります。

JVN

最終更新日：2017/11/21

JVN iPedia 脆弱性対策情報データベース

【活用ガイド】

JVNDB-2017-009755

Linux kernel における解放済みメモリの使用に関する脆弱性

概要

Linux kernel には、解放済みメモリの使用に関する脆弱性が存在します。

CVSS による深刻度 (CVSS とは?)

CVSS v3 による深刻度
基本値: 6.6 (警告) [NVD値]

- 攻撃元区分: 物理
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 低
- 利用者の関与: 不要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 高
- 完全性への影響(I): 高
- 可用性への影響(A): 高

CVSS v2 による深刻度
基本値: 7.2 (危険) [NVD値]

- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 低
- 攻撃前の認証要否: 不要
- 機密性への影響(C): 全面的
- 完全性への影響(I): 全面的
- 可用性への影響(A): 全面的

SIDfmとJVNの情報の違い

SIDfmは、**過去のバージョンも提供**しています！

SIDfm

Linux Kernel の ALSA シーケンサの処理にサービスを妨害される問題

ID	28397	登録日	2018/04/05	最終更新日	-
CVSSスコア	6.6	影響範囲	ローカル	危険度	M

CVE	CVE-2017-16528				
攻撃コード	攻撃コード・実証コードは確認されていません。				
CVSS	UI PR AC S AV C A I 6.6	攻撃元区分 (AV)	物理 (P)	ローカル (L)	隣接 (A) ネットワーク (N)
		攻撃条件の複雑さ (AC)	高 (H)		低 (L)
		必要な特権レベル (PR)	高 (H)	低 (L)	不要 (N)
		ユーザ関与レベル (UI)	要 (R)		不要 (N)
		スコープ (S)	変更なし (U)		変更あり (C)
		機密性への影響 (C)	なし (N)	低 (L)	高 (H)
		完全性への影響 (I)	なし (N)	低 (L)	高 (H)
		可用性への影響 (A)	なし (N)	低 (L)	高 (H)

概要 | 影響を受ける製品 | 影響などの確認方法 | 対処方法 | 関連情報 | 更新履歴 | 一括表示

- **Linux Kernel**
  4.14 未満 (4.x)
  3.x
  2.6.x

JVN

最終更新日：2017/11/21

JVN iPedia 脆弱性対策情報データベース

【活用ガイド】

JVNDB-2017-009755

Linux kernel における解放済みメモリの使用に関する脆弱性

影響を受けるシステム

Linux

- Linux Kernel 4.13.4 未満

想定される影響

情報を取得される、情報を改ざんされる、およびサービス運用妨害（DoS）状態にされる可能性があります。

SIDfmとJVNの情報の違い

SIDfmは、**直接修正プログラムにたどり着けます。**
修正プログラムのための再調査を必要ありません！

SIDfm

Linux Kernel の ALSA シーケンサの処理にサービスを妨害される問題

ID	28397	登録日	2018/04/05	最終更新日	-
CVSSスコア	6.6	影響範囲	ローカル	危険度	M

CVE	CVE-2017-16528				
攻撃コード	攻撃コード・実証コードは確認されていません。				
CVSS	UI PR AC S AV C A I 6.6	攻撃元区分 (AV)	物理 (P)	ローカル (L)	隣接 (A) ネットワーク (N)
		攻撃条件の複雑さ (AC)	高 (H)		低 (L)
		必要な特権レベル (PR)	高 (H)	低 (L)	不要 (N)
		ユーザ関与レベル (UI)	要 (R)		不要 (N)
		スコープ (S)	変更なし (U)		変更あり (C)
		機密性への影響 (C)	なし (N)	低 (L)	高 (H)
		完全性への影響 (I)	なし (N)	低 (L)	高 (H)
		可用性への影響 (A)	なし (N)	低 (L)	高 (H)

概要 | 影響を受ける製品 | 影響などの確認方法 | 対処方法 | 関連情報 | 更新履歴 | 一括表示

- **Linux Kernel**
  修正プログラムを適用してください。
  - **Linux Kernel 4.14 未満 (4.x)**
    Linux Kernel 4.14 以上 [http]
- **ベンダーの対処方法を適用しない場合の回避方法**
  - 適切な回避方法はありません。

回避方法については操作性/機能性などを制限することで回避される一時的なものであり、セキュリティホールが修正されたことにはなりません のでご注意ください。

JVN

最終更新日:2017/11/21

JVN iPedia 脆弱性対策情報データベース

【活用ガイド】

JVNDB-2017-009755
Linux kernel における解放済みメモリの使用に関する脆弱性

想定される影響

情報を取得される、情報を改ざんされる、およびサービス運用妨害 (DoS) 状態にされる可能性があります。

対策

ベンダより正式な対策が公開されています。ベンダ情報を参照して適切な対策を実施してください。

SIDfmの提供情報

- ✓ ベンダ毎に整理された日本語のアドバイザリ情報
- ✓ CVSSリスク評価基準全面採用
- ✓ 攻撃コードの有無
- ✓ IPA警告注意情報
- ✓ セキュリティニュース
- ✓ ソフトウェアの最新バージョン
- ✓ EOL情報

など

既存システム連携したい方向け：SIDfm API

SIDfm APIは、APIを通じて
脆弱性情報を提供します。

これにより、顧客のニーズに応じて、
json形式で取得した情報を活用したシステムを構築することができます。

さまざまな利用シーンに
対応することが可能になります。