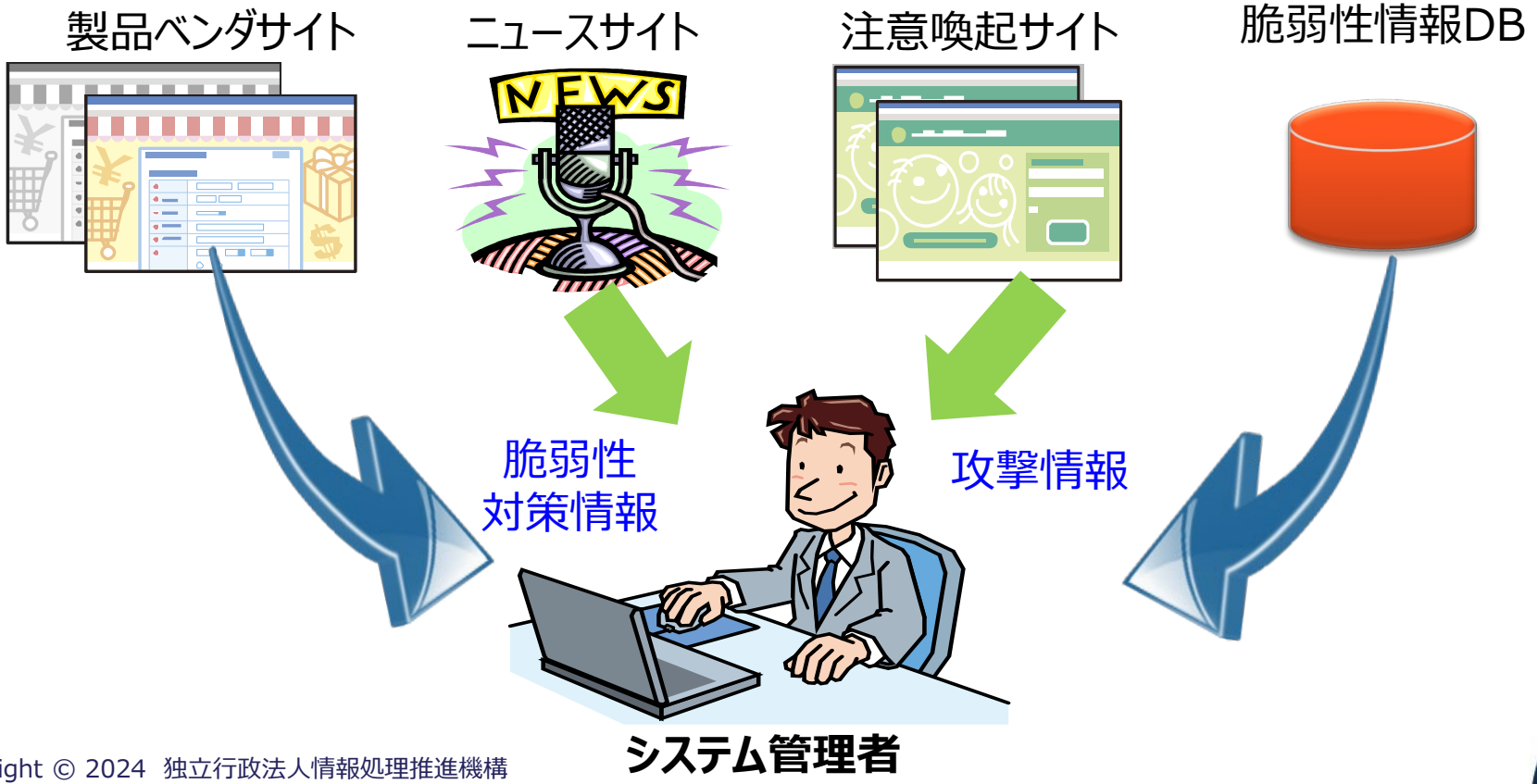
2. 脆弱性関連情報の収集

脆弱性関連情報の収集

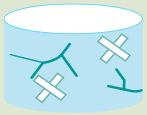
■ 脆弱性関連情報とは？

- 脆弱性対策を実施する際の判断要素となる情報
- 情報の内容も、情報元も様々



脆弱性関連情報の収集

■ 例えば、脆弱性対策の参考となる情報として以下のものが考えられる。

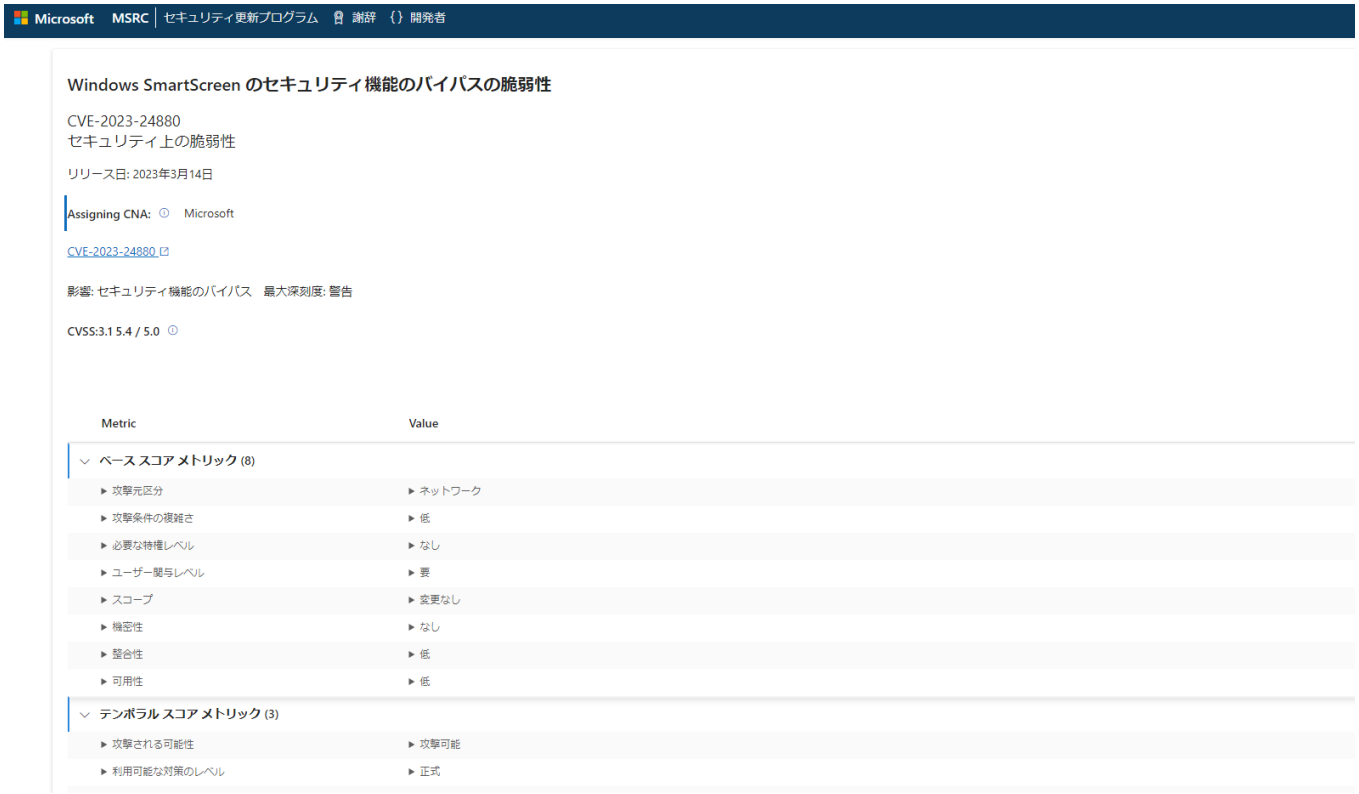
情報	内容	活用例
脆弱性情報 	脆弱性の内容、 脆弱性の深刻度、 影響を受けるバージョン、 対策の有無、 対策方法　　など	脆弱性の深刻度の評価、 影響の調査、 対策や回避策の実施
攻撃情報 	攻撃コードの公開状況、 実際の攻撃の有無 など	対策の緊急度の調査

脆弱性関連情報の収集先（1/4）

ベンダアドバイザリ

ベンダ（開発者）が製品の脆弱性情報・対策情報を提供

- 製品ベンダのサイトやブログ（セキュリティアドバイザリ）



Microsoft MSRC | セキュリティ更新プログラム 謝辞 {} 開発者

Windows SmartScreen のセキュリティ機能のバイパスの脆弱性

CVE-2023-24880
セキュリティ上の脆弱性

リリース日: 2023年3月14日

Assigning CNA: Microsoft

CVE-2023-24880

影響: セキュリティ機能のバイパス　最大深刻度: 警告

CVSS:3.1 5.4 / 5.0

Metric	Value
ベース スコア メトリック (8)	
攻撃元区分	ネットワーク
攻撃条件の複雑さ	低
必要な特権レベル	なし
ユーザー関与レベル	要
スコープ	変更なし
機密性	なし
整合性	低
可用性	低
テンポラル スコア メトリック (3)	
攻撃される可能性	攻撃可能
利用可能な対策のレベル	正式

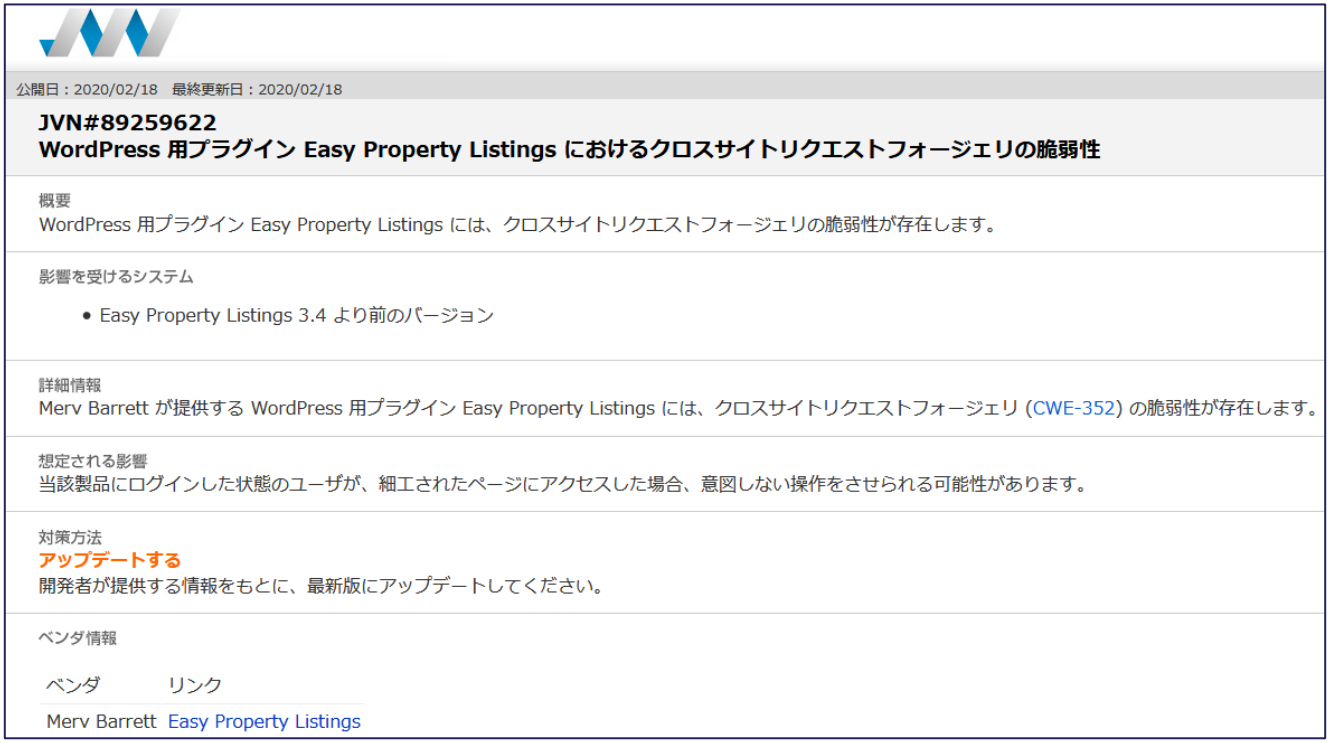
出典： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880

脆弱性関連情報の収集先（2/4）

注意喚起サイト

広く使われている製品の脆弱性を周知し、対策を呼び掛ける

- 国内：JPCERT/CC、警察庁、IPA等
- 海外：CISA等



公開日：2020/02/18　最終更新日：2020/02/18

JVN#89259622
WordPress 用プラグイン Easy Property Listings におけるクロスサイトリクエストフォージェリの脆弱性

概要
WordPress 用プラグイン Easy Property Listings には、クロスサイトリクエストフォージェリの脆弱性が存在します。

影響を受けるシステム
- Easy Property Listings 3.4 より前のバージョン

詳細情報
Merv Barrett が提供する WordPress 用プラグイン Easy Property Listings には、クロスサイトリクエストフォージェリ (CWE-352) の脆弱性が存在します。

想定される影響
当該製品にログインした状態のユーザが、細工されたページにアクセスした場合、意図しない操作をさせられる可能性があります。

対策方法
アップデートする
開発者が提供する情報をもとに、最新版にアップデートしてください。

ベンダ情報

ベンダ	リンク
Merv Barrett	Easy Property Listings

出典： https://jvn.jp/jp/JVN89259622/index.html

脆弱性関連情報の収集先（3/4）

ニュース記事

- 話題になっているセキュリティ情報を確認するのに便利
  - 国内：ZDNet Japan、SecurityNext、CNET、ITMedia等
  - 海外：Register、ComputerWorld等

ZDNet Japan　海外発　デジタル変革　CIO　ITインフラ　セキュリティ　クラ

ウイルスバスターに脆弱性情報、悪用攻撃が発生

ZDNet Japan Staff　2019-10-28 13:38

シェア Tweet　noteで書く　Pocket　20

トレンドマイクロは10月28日、法人向けのセキュリティ対策製品「ウイルスバスター コーポレートエディション」にディレクトリトラバーサルの脆弱性が存在し、この脆弱性を悪用するサイバー攻撃を確認したと発表した。

同社によると今回の脆弱性「CVE-2019-18187」は、ウイルスバスター コーポレートエディション 11.0とXG、XG SP1に影響する。攻撃者は、この脆弱性を悪用して該当製品のサーバーに任意のzip形式のファイルをアップロードし、このファイルをサーバー上の特定フォルダの配下に展開できる。これにより、管理コンソールで使用しているウェブサービスのアカウントで任意コードを実行できるようになるという。

- 話題性に欠ける製品や脆弱性は基本的に扱われない

出典： https://japan.zdnet.com/article/35144536/

脆弱性関連情報の収集先（4/4）

■ 脆弱性情報データベース

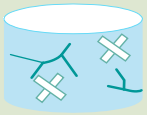
■ 脆弱性情報をデータベース化して提供
検索機能などにより、ピンポイントでの情報収集が可能

- 国内：JVN iPedia等
- 海外：NVD等

出典：https://jvndb.jvn.jp/

脆弱性関連情報の収集

■ 攻撃情報等も脆弱性対策の参考となる

情報	内容	活用例
脆弱性情報 	脆弱性の内容、 脆弱性の深刻度、 影響を受けるバージョン、 対策の有無、 対策方法　　など	脆弱性の深刻度の評価、 影響の調査、 対策や回避策の実施
攻撃情報 	攻撃コードの公開状況、 実際の攻撃の有無 など	対策の緊急度の調査

攻撃情報の収集先（1/3）

ベンダアドバイザリ・注意喚起サイト

- 脆弱性情報の一部として、攻撃の発生状況や攻撃コードの有無に関する情報を公開していることがある
  - ベンダアドバイザリ：Microsoft、Adobe、Oracle等
  - 注意喚起サイト：JPCERT/CC、警察庁、IPA等

 出典： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880

攻撃情報の収集先（2/3）

ニュース記事

- 組織等への攻撃に使われた脆弱性の場合、ニュース記事やセキュリティベンダの分析レポート等に記載されることがある
  - ニュース：ZDNet Japan、SecurityNext、CNET、マイナビ等

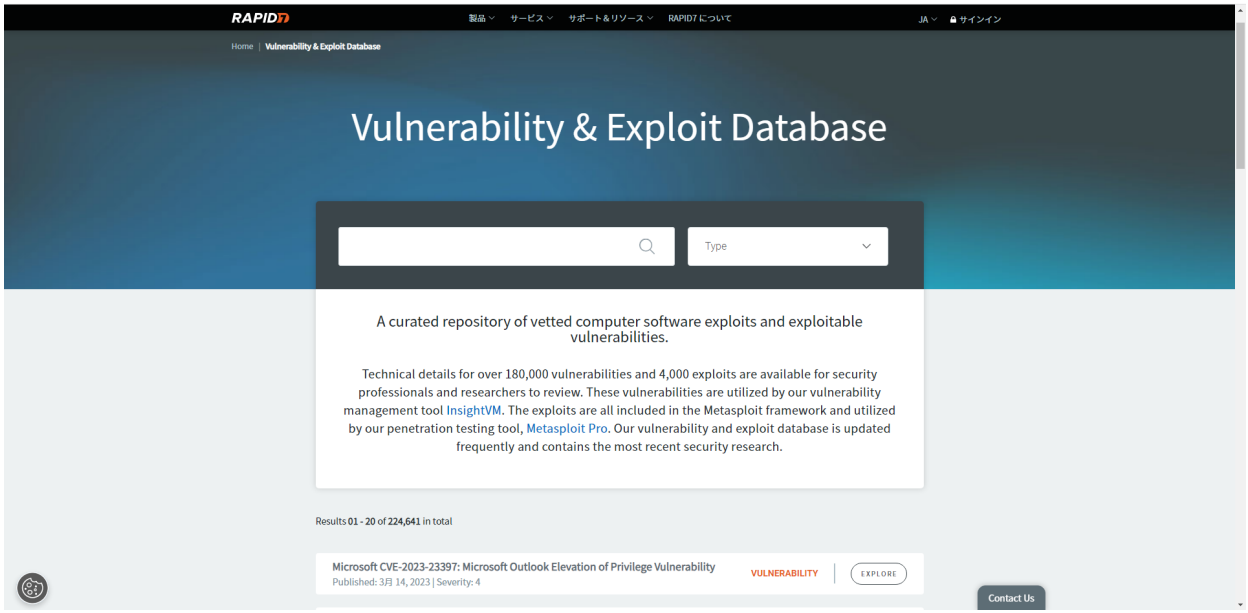
攻撃の具体的な内容

出典： https://japan.zdnet.com/article/35144536/

攻撃情報の収集先（3/3）

攻撃コードデータベース

- 脆弱性等を悪用する攻撃コード（Exploit：エクスプロイト）をデータベース化して提供
  - Metasploit、Exploit DB等



※攻撃情報を検証する場合は、他に影響を与えないようにご注意ください。

出典： https://www.rapid7.com/ja/db/

脆弱性関連情報の収集

あちこち見てはみたけれど・・・

製品ベンダのサイトに載っている脆弱性と、ニュース記事の脆弱性は同じもの？

「深刻な脆弱性が発見されました」ってあるけど、どのくらい深刻なの？理由は？

脆弱性情報の収集に役立つキーワードについて知ろう

知っていますか？CVE、CWE、CVSS

IPA

■ 脆弱性情報を効率的に収集する為に有効なキーワード

・・・脆弱性を一意に識別する番号

・・・脆弱性のタイプを体系的に分類する番号

・・・脆弱性の深刻度を評価する数値指標

製品ベンダのアドバイザリ、セキュリティサイトの
注意喚起、ニュース記事等でも広く使用される

これらのキーワードの解説資料
https://www.ipa.go.jp/security/vuln/scap/index.html

CVEとは
～発見された脆弱性に一意の番号を割り当て、識別を可能に～

IPA

Common Vulnerabilities and Exposures（共通脆弱性識別子）

CVE識別番号の構成

CVE-西暦-連番

CVE-2018-1000
CVE-2018-10000
CVE-2018-1000000

連番は4桁から始まり、
必要に応じて桁を拡張

- 様々な情報元が公開する脆弱性情報について、
  - 同じ脆弱性に関する情報なのかを見分ける
  - CVEを介して情報を紐づける

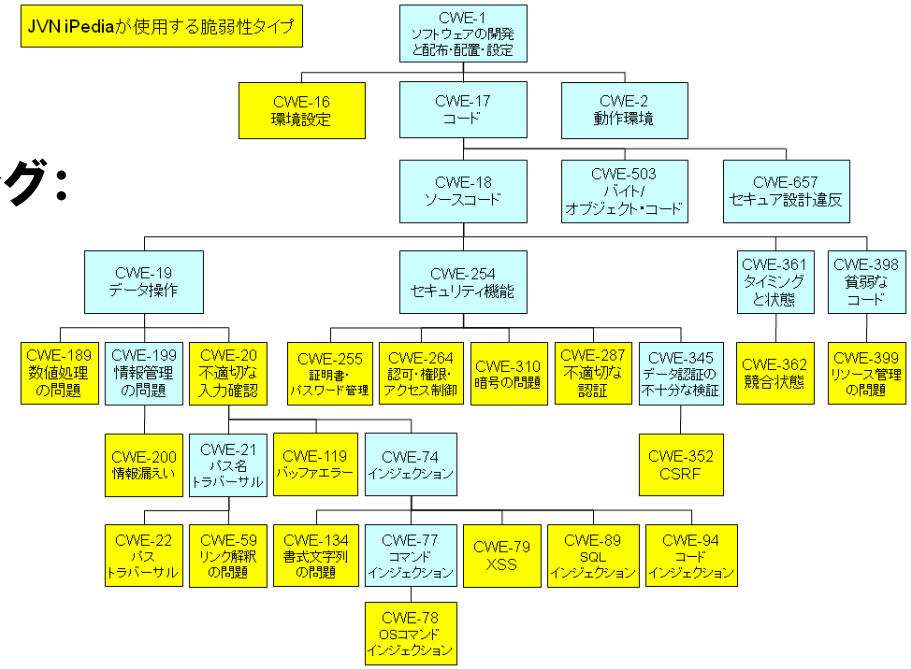
出典： https://japan.zdnet.com/article/35144536/

CWEとは
～脆弱性のタイプを体系立てて分類し、どんな脆弱性か示す～

- **Common Weakness Enumeration（共通脆弱性タイプ一覧）**
- **タイプから脅威や危険性の想定も可能**

【CWE-79】クロスサイトスクリプティング：
- **正規サイトにおける偽ページの表示**
- **他の不正サイトへ誘導させられる**

【CWE-89】SQLインジェクション：
- **データベースを不正に操作される**



CVSSとは
～脆弱性の深刻度を数値で示す～

- **Common Vulnerability Scoring System（共通脆弱性評価システム）**
- **脆弱性の深刻度を0.0～10.0のスコアで評価**

**脆弱性の深刻度を表すバロメータとして
CVSSが活用されている**

次の3章・4章で詳しく見ていきます！

まとめ（2章）

- **脆弱性関連情報の収集**
  - **脆弱性情報の収集**
    - ✓ベンダアドバイザリ
    - ✓注意喚起サイト
    - ✓ニュース記事
    - ✓脆弱性情報データベース
  - **攻撃情報の収集**
    - ✓ベンダアドバイザリ
    - ✓注意喚起サイト
    - ✓ニュース記事
    - ✓攻撃コードデータベース
- **キーワード**
  - ✓CVE、CWE、CVSS