ASHISUTO
TECHNICAL FORUM

【E-4】

# 対応が必要なのは全体の３％？！

## ～ 効率的な脆弱性対策のススメ ～

株式会社アシスト
システム基盤技術統括部　技術3部
中澤　浩二

# アジェンダ

- 脆弱性管理が注目される理由
- 脆弱性の現状と管理における課題
- ツール活用と選定ポイント
- 脆弱性管理ツール「tenable」のご紹介

ASHISUTO
TECHNICAL FORUM

# 脆弱性管理が注目される理由

# 世間を騒がせたWannaCry

- 世界で一気に大流行したランサムウェア
- Windowsの脆弱性をついたワームタイプのマルウェア
- 欧州では病院や銀行、有名企業で被害が発生
- 日本国内でも600か所、2000台以上が感染
- 修正パッチは流行の約2ヵ月前にリリース済み

# IPA 情報セキュリティ10大脅威(法人) 2019

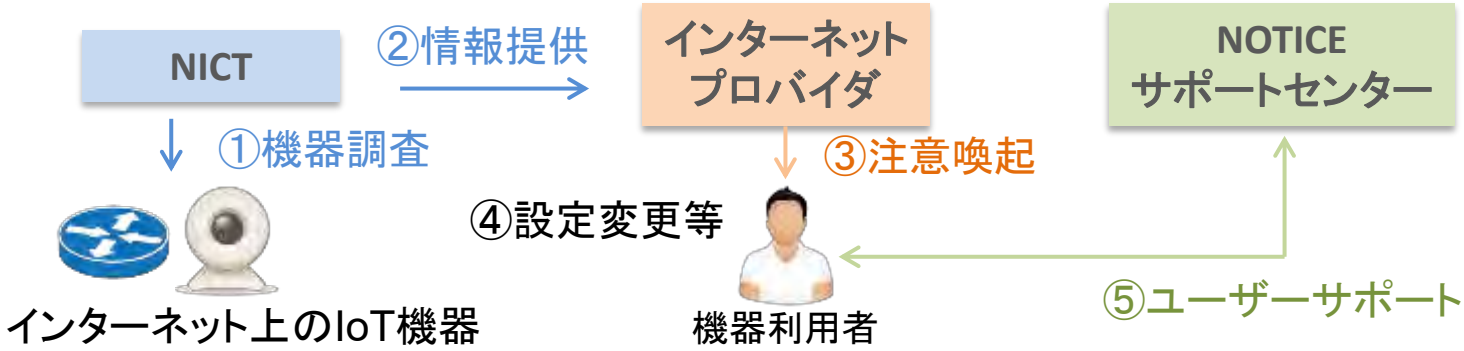
1. 標的型攻撃による被害
2. ビジネスメール詐欺による被害
3. ランサムウェアによる被害
4. サプライチェーンの弱点を悪用した攻撃の高まり
5. 内部不正による情報漏えい
6. サービス妨害攻撃によるサービスの停止
7. インターネットサービスからの個人情報の窃取
8. IoT機器の脆弱性の顕在化
9. 脆弱性対策情報の公開に伴う悪用増加
10. 不注意による情報漏えい


Sources: IPA 情報処理推進機構 情報セキュリティ10大脅威 2019
https://www.ipa.go.jp/security/vuln/10threats2019.html

# 総務省、NICTの取り組み

## IoT機器調査及び利用者への注意喚起の取組「NOTICE」

NOTICEは、総務省、国立研究開発法人情報通信研究機構（NICT）及びインターネットプロバイダが連携し、IoT機器へのアクセスによる、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取り組みです。




Sources: NOTICEホームページ https://notice.go.jp/

# 各種ガイドライン/認証規格より

| ガイドライン/認証規格 | 記載箇所 |
|---|---|
| サイバーセキュリティ経営ガイドライン Ver.2.0 | 指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定<br>特定した守るべき情報に対する**サイバー攻撃の脅威、脆弱性を識別し**、経営戦略を踏まえたサイバーセキュリティリスクとして把握している。<br>指示５ サイバーセキュリティリスクに対応するための仕組みの構築<br>システム等に対して**脆弱性診断を実施し、検出された脆弱性に対処**している。 |
| サイバーセキュリティフレームワーク（CSF）Ver.1.1 | ID.RA-1 **資産の脆弱性が、識別され**、文書化されている。<br>ID.RA-4 ビジネスに対する潜在的な影響とその発生可能性が、識別されている。<br>ID.RA-5 脅威、脆弱性、発生可能性、影響がリスクを判断する際に使用されている。<br>ID.RA-6 **リスク対応が、識別され、優先順位付け**されている。 |
| 情報セキュリティ管理基準（平成28年改正版） | 12.6.1 技術的ぜい弱性管理<br>利用中の情報システムの技術的**ぜい弱性に関する情報は、時機を失せずに獲得**する。また、そのような**ぜい弱性に組織がさらされている状況を評価**する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。 |
| PCIDSS Ver.3.2.1 | 要件6<br>6.1 セキュリティ脆弱性情報の信頼できる社外提供元を使ってセキュリティの脆弱性を特定し、新たに発見されたセキュリティの**脆弱性にリスクのランク（「高」、「中」、「低」など）を割り当てるプロセスを確立**する。<br>6.2 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、既知の脆弱性から保護されている。**重要なセキュリティパッチは、リリース後1カ月以内にインストール**する。 |

Sources:サイバーセキュリティ経営ガイドライン https://www.meti.go.jp/policy/netsecurity/mng_guide.html サイバーセキュリティフレームワーク https://www.ipa.go.jp/files/000071204.pdf
情報セキュリティ管理基準 https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000008.html PCIDSS https://www.pcisecuritystandards.org/document_library

# CIS Controls

## 全20の対策が優先度の高い順に記載


Sources: CIS Controls https://www.cisecurity.org/critical-controls.cfm

# 求められるプロアクティブな対応


脆弱性の識別、リスク評価等
**攻撃を未然に防ぐプロアクティブな対応**

アラート検知、アクセス制御や、データセキュリティ等の防御及び、継続的なモニタリングによる検知

対応計画の作成や、分析、復旧計画の作成等
リアクティブな対応

**今後求められる対応**

従来注力されていた対応

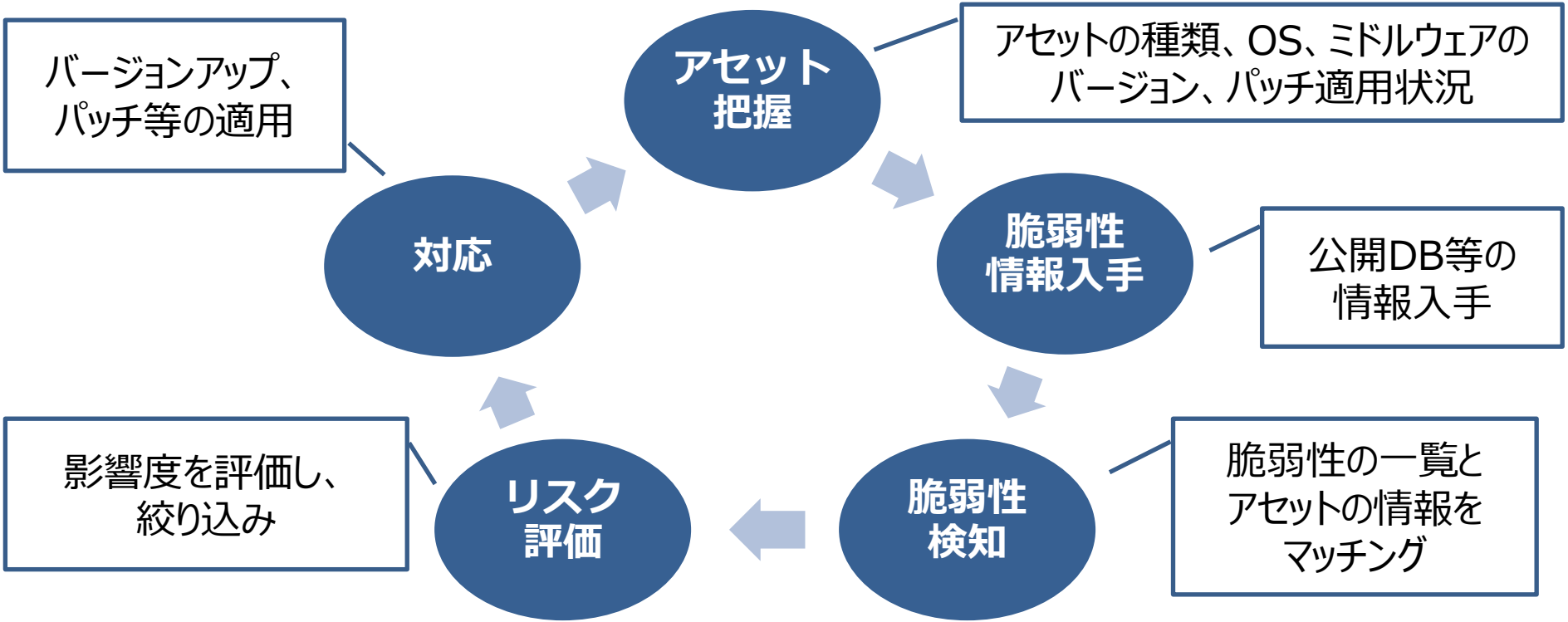
Sources:サイバーセキュリティフレームワーク https://www.ipa.go.jp/files/000071204.pdf

ASHISUTO
TECHNICAL FORUM

# 脆弱性の現状と管理における課題

# 脆弱性管理のライフサイクル

情報システムやアプリケーションにおける脆弱性を特定し、評価、修正するための継続的なプロセス



# 脆弱性の現状

**16,500+**

2018年に新たに発覚した脆弱性の数

**123,600+**

2019年現在の脆弱性の累計

# 脆弱性管理の基礎①

- CVE（Common Vulnerabilities and Exposures）
  - ◆一つ一つの脆弱性を識別するための共通の識別子

- CVSS（Common Vulnerability Scoring System）
  - ◆共通脆弱性評価システムのこと。脆弱性の深刻さを0～10のスコアで評価
    - – 7.0～10.0：レベルⅢ（危険）
    - – 4.0～6.9：レベルⅡ（警告）
    - – 0.0～3.9：レベルⅠ（注意）

# 脆弱性の現状

**9,500+**

**2018年に発覚した脆弱性のレベルⅢ（危険）CVSS 7~の数**
**2018年に発覚した脆弱性の約59%**

**2,500+**

**2018年に発覚した脆弱性の CVSS 9~の数**
**2018年に発覚した脆弱性の約15%**

# 脆弱性の現状


図1-2. 2013年から2017年までにJVN iPediaへ登録した脆弱性対策情報の推移

2018年は
15,238件

Sources: IPA 情報処理推進機構脆弱性対策情報データベースJVN iPediaの登録状況 https://www.ipa.go.jp/security/vuln/report/JVNiPedia2017q4.html

# 脆弱性管理の課題

- 脆弱性の有無、影響度の確認に膨大な工数がかかる
- パッチ適用の判断が難しい
- 人財の不足
- 多額のサービス費用
- 資産が把握しきれない
- 情報をどこから入手するべきか分からない
- 簡単にパッチ適用できない

# 攻撃者が優位

- **新しい脆弱性に対して攻撃コードが公開されるまでの期間は2週間以内が50%**

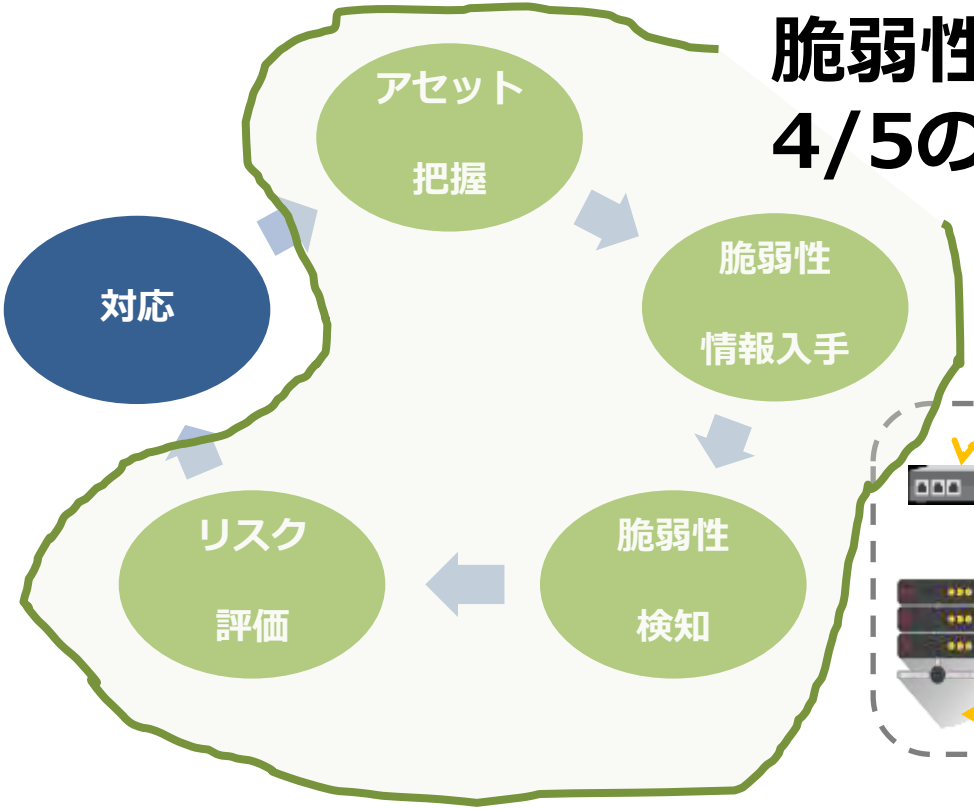
  https://www.kennasecurity.com/prioritization-to-prediction-report

**増加する脆弱性に対して、タイムリーに、且つ効率よく対応していく必要があります。**

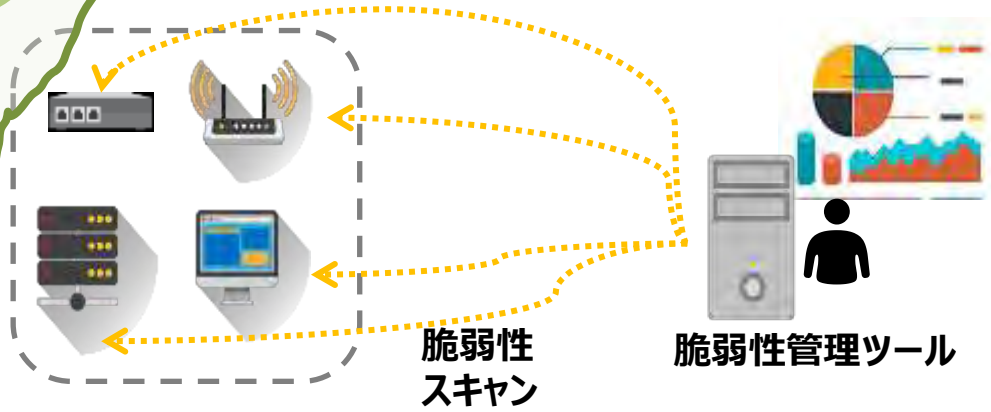
ASHISUTO
TECHNICAL FORUM

# ツール活用と選定ポイント

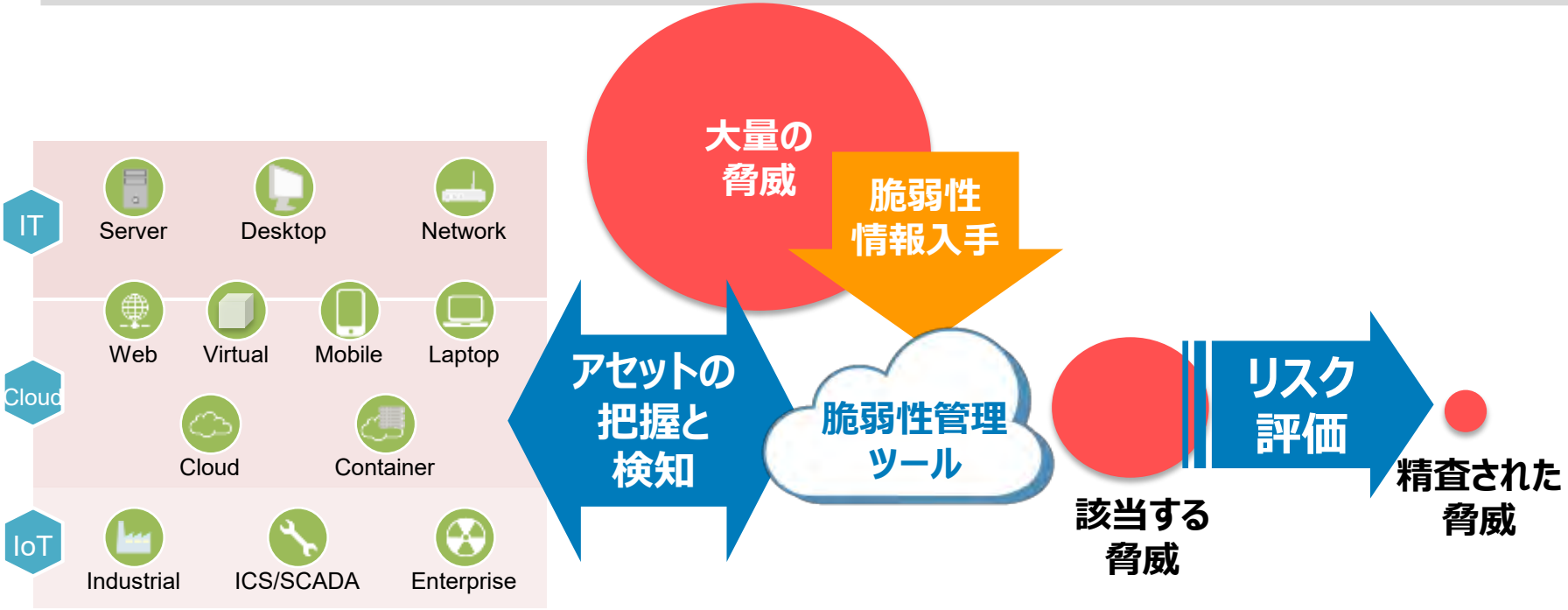
# 脆弱性管理ツールの活用をおすすめ




## 脆弱性管理ツールを使うことで、4/5のサイクルに対応



# 脆弱性管理ツールの適用イメージ




**定期的に実施** することで **常にセキュアな環境** を維持

# 脆弱性管理ツールの選定ポイント ～アセット把握～

- アセットの把握 ≒ スキャン対象環境
- 対象環境は製品によって異なる
  - IT（Windows、Linux、UNIX、etc... ）
  - クラウド（AWS、Azure、etc... ）
  - Container
  - OT（PLC、SCADA、etc... ）
- アセットの重要度の判定

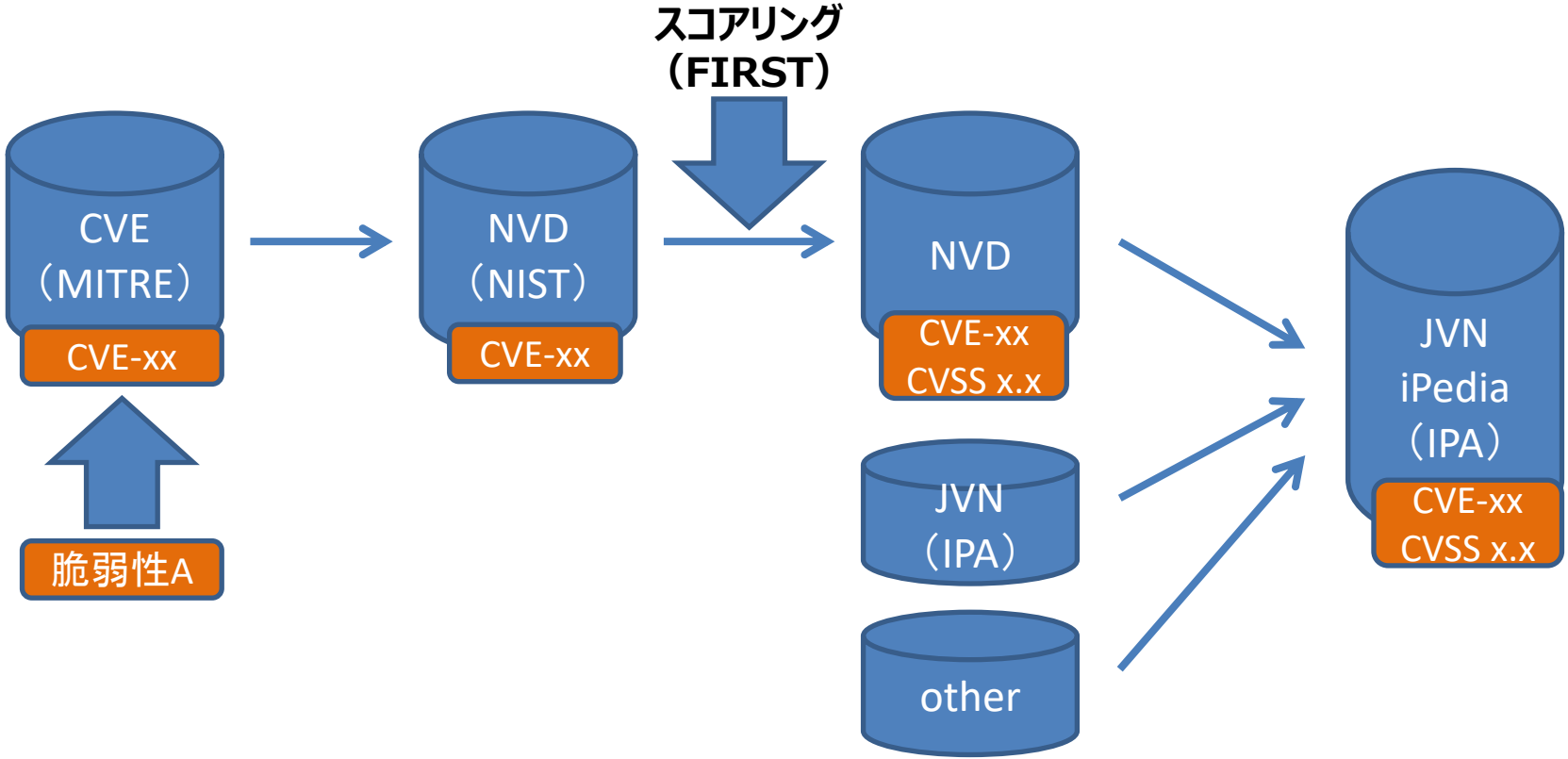
# 脆弱性管理ツールの選定ポイント ～脆弱性情報の入手～

- 製品によって利用するDBは様々
  - 無償DB
  - 有償DB
  - 独自DB
- 脆弱性が公開されてから、DBに情報が反映されるまでの時間
- コンプライアンス対応

# 脆弱性管理の基礎②

- NVD（National Vulnerability Database）
  - NISTが運営する脆弱性データベース。CVEの詳細情報や、CVSSが提供される。
- JVN（Japan Vulnerability Notes）
  - JPCERT/CCとIPAが共同で運営している脆弱性対策情報ポータルサイト。
    日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供。
- JVN iPedia
  - JVNに掲載される脆弱性対策情報のほか、国内外問わず公開された脆弱性対策情報を広く公開対象としたデータベース。

# 脆弱性の登録・管理イメージ



# 脆弱性管理ツールの選定ポイント ～脆弱性検知～

- スキャン方式
  - リモート方式（クレデンシャル、ノンクレデンシャル）
  - エージェント方式
  - パッシブ方式　⇒　パッシブ方式が無いとOTには対応不可
- 提供形態
  - クラウド
  - オンプレミス
  - クラウド×オンプレミス

# 脆弱性管理ツールの選定ポイント ～リスク評価～

- CVEの表示や対応方法
- スコアリングの精度
- アセットの状況等からスコアリング

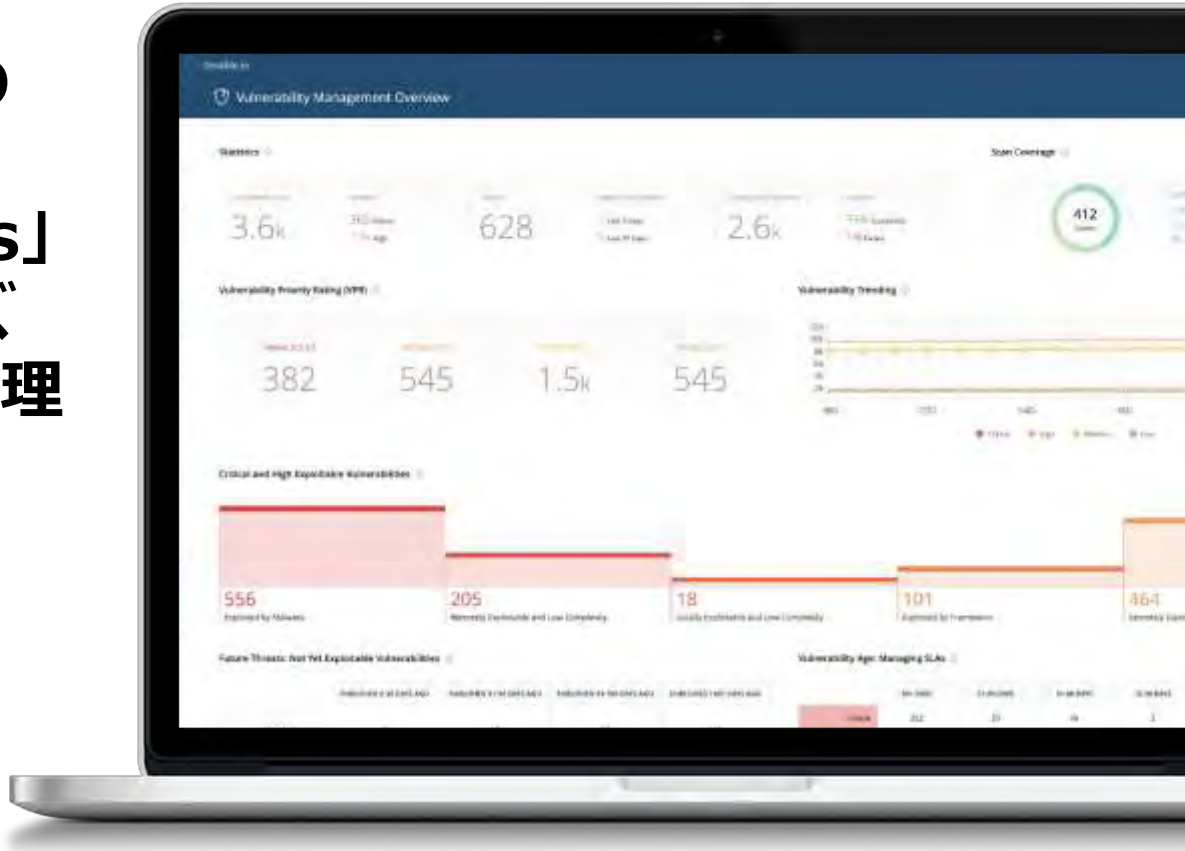
⇒ いかに適切に絞り込みができるかが重要

ASHISUTO
TECHNICAL FORUM

# 脆弱性管理ツール「tenable」のご紹介

# 脆弱性管理ツール「tenable」

「tenable」は、脆弱性のスキャナーとして圧倒的な支持を得ている「Nessus」の作者がエンタープライズ向けに開発した脆弱性管理プラットフォーム。



# 優れたデータベース

tenable独自のスコアリングにより、**緊急で対応が必要と言われる脆弱性（CVSSのスコア7以上）を3%に絞り込み。**


※ Vulnerability Priority Rating（ VPR ）：優先的に対処すべき脆弱性を表すTenableのスコア

# 優先的に対処すべき脆弱性を正確に予測

## 2018年に悪用された脆弱性Top5

| | CVSSv2 Score (Acccording to NVD) | CVSSv3 Score (Acccording to NVD) | Tenable (Vulnerability Priority Rating) |
|---|---|---|---|
| CVE-2018-8174 | 7.6 | 7.5 | 9.9 |
| CVE-2018-4878 | 7.5 | 9.8 | 9.5 |
| CVE-2017-11882 | 9.3 | 7.8 | 9.9 |
| CVE-2017-8750 | 7.6 | 7.5 | 9.4 |
| CVE-2017-0199 | 9.3 | 7.8 | 9.9 |

# 優れたデータベース

**100+**

90名を超えるリサーチャーが
過去3年間で100以上の
ゼロデイ脆弱性を発見

**150**

150の異なる要素を
独自のデータサイエンスに
もとづいて分析

**24h**

脆弱性の公開から24時間
以内にスコアリング、
新たなプラグインをリリース

**130,000+**

100以上のプラグインを毎週
リリースし、累計13万以上の
プラグインをリリース

# tenableの特徴

## 幅広い対応環境

クラウド環境、Container、
OT等、幅広い環境の
脆弱性に対応

## 複数のスキャン方式

リモートスキャン、
パッシブスキャン、エージェント等
様々なスキャン方式を提供

## 柔軟なサービス形態

要望にあわせてクラウド、
オンプレミス、クラウド×オンプレミス
を選択可能

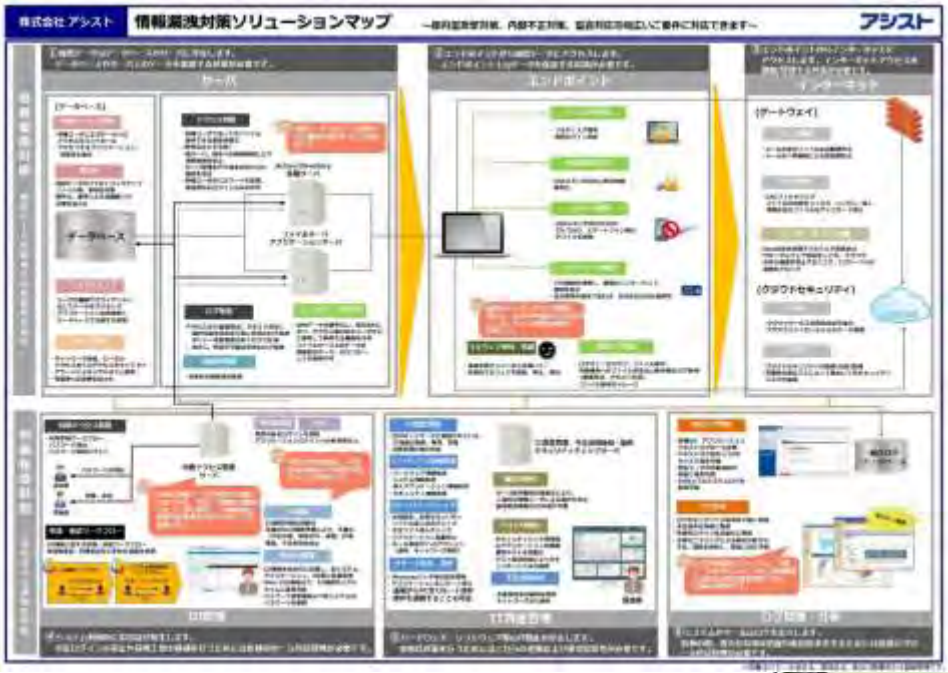
## 優秀なレポート

脆弱性のスコアリングに加え、
アセット（資産）の重要度も
含め総合的にリスクを評価

# 最後に

- 攻撃の未然防止には脆弱性管理が有効
- 脆弱性管理にはツールの活用をおすすめ
- 選定は機能面だけでなく、脆弱性情報のDBもポイント

# 情報漏洩対策ソリューションマップ





超サポ
愉快カンパニー
アシスト

※本資料に記載している情報は、2019年10月17日現在のものです。
※本資料の内容は、今後予告なく変更されることがあります。
※OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。
※文中の社名、商品名等は各社の商標または登録商標である場合があります。