IBC SOLUTION

脆弱性管理プラットフォーム

tenable.io

tenable.io は、サーバー、ネットワーク、クラウド、ウェブアプリケーションなど IT 資産のために設計された脆弱性管理プラットフォームです。世界で 160 万人ものユーザーに利用されている脆弱性診断ソフトウェア「Nessus®」のテクノロジーを基盤として構築されており、資産ベースのアプローチで脅威・脆弱性の把握と優先順位づけを可能にします。

脆弱性管理の必要性と課題

IPA 「情報セキュリティ 10 大脅威　2018」

順位	組織	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位
3位	ビジネスメール詐欺による被害	ランク外
4位	**脆弱性対策情報の公開に伴う悪用増加**	**ランク外**
5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	3位

※ 出典：情報処理推進機構（IPA）「情報セキュリティ10 大脅威 2018」

NISC「政府機関等の情報セキュリティ対策のための統一基準群の見直し（骨子）」

② IT 資産管理の自動化とソフトウェアの脆弱性への迅速な対応

- 情報システムが高度化・複雑化する中で、多様な脆弱性が発生し、脆弱性情報の公開直後にこれを突くような攻撃が後を絶たない。人手による脆弱性対応は運用が限界に近づきつつあり、脆弱性対応を含む IT 資産管理の自動化による対応が効果的。
- このような機能の導入は、継続的な「監査」機能と捉えることもできよう。

※ NISC＝内閣サイバーセキュリティセンター

定期的に脆弱性診断をしているが
対応状況の把握ができない

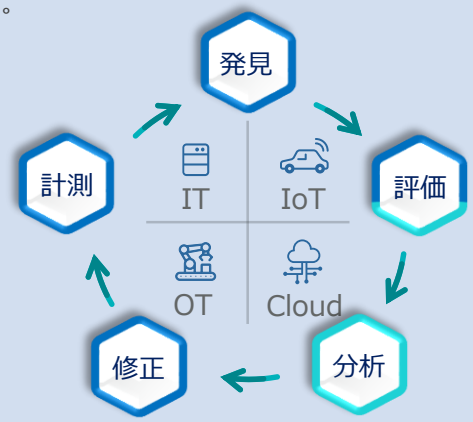
脆弱性診断対象となる
デバイスの把握が難しい

脆弱性診断結果に対する
優先順位づけがわからない

tenable.io™ による課題解決

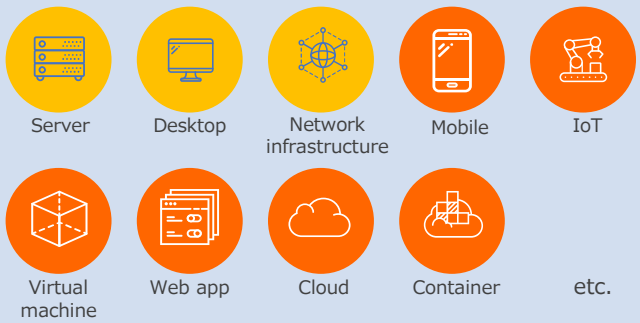
脅威へのアプローチ

「脆弱性管理対象となる資産の可視化」「脅威の優先づけ」「レポート」「判断」というライフサイクルを回すことにより、脆弱性や脅威に対してのアプローチを実現しています。



脆弱性状況の把握と管理が可能

エージェント型、アクティブスキャン、パッシブスキャンなど豊富な手法で、資産の継続的な管理が可能です。スキャン結果は脅威数の推移、段階、対応状況などのカテゴリー別に分類されているため、手間をかけずに現状の把握と分析をおこなえます。Tenable 社は Approved Scanning Vendor のため、ユーザー自身で PCI ASV 認証取得が可能です。



サイバーエクスポージャー

Tenable 社が提唱している「サイバーエクスポージャー」とは、最新のアタックサーフェスつまり攻撃される可能性のある領域全体を適切に管理、継続的に計測し、サイバーリスクを正確に把握、削除することです。

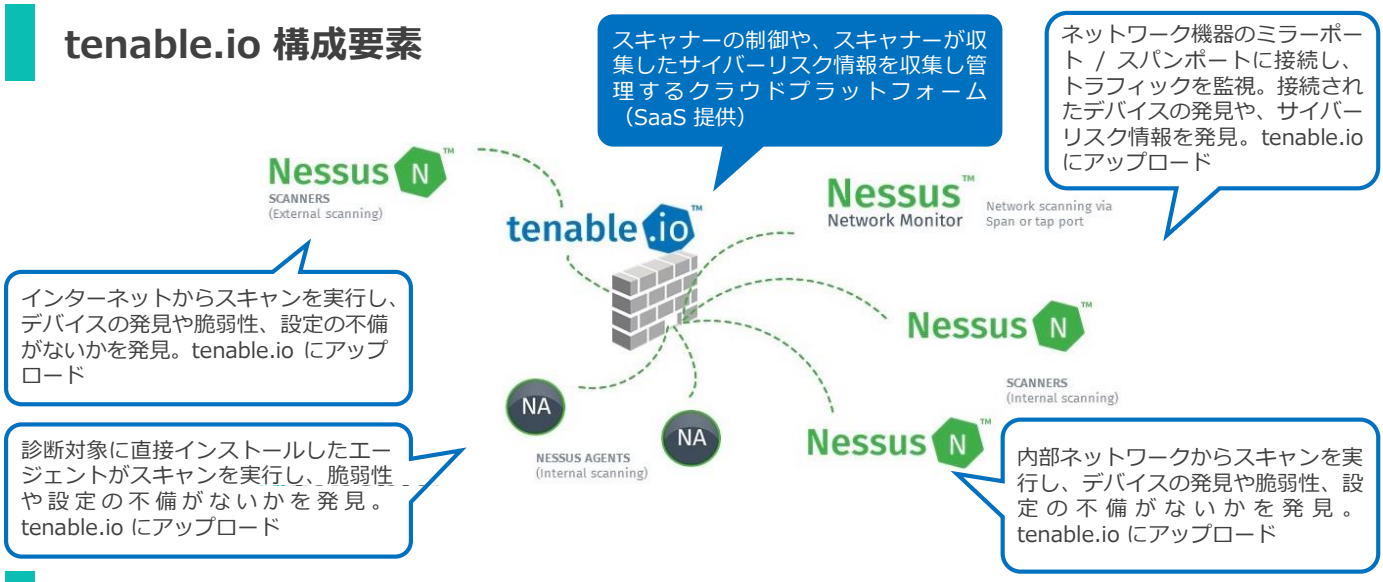
従来の脆弱性管理や資産管理

- 限定的な資産のみの把握
- 資産の不十分な発見
- IP ベースでの管理
- 可視化の間隔が長い
- 不十分な優先順位づけ
- 脆弱性情報だけにフォーカス
- 企業や組織全体のリスクが不明瞭

サイバーエクスポージャー

- 最新の多様化する資産にも対応
- 複数スキャナーによる全資産の網羅
- アセット（資産）単位での管理
- 継続的かつリアルタイムでの可視化
- 優れた分析と優先順位づけ
- CSIRT や経営層での適切な判断も可能
- 企業や組織全体のリスク管理を実現

tenable.io 構成要素



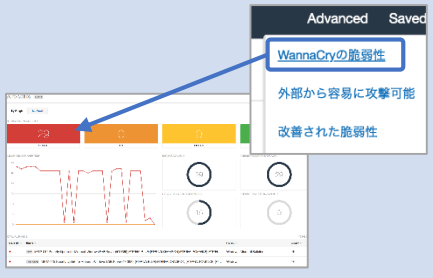
tenable.io 各種機能

わかりやすい GUI

スキャン結果をグラフィカルに可視化。展開されたスキャナー・エージェントの管理やスキャンのスケジュール実行も簡単におこなえます。

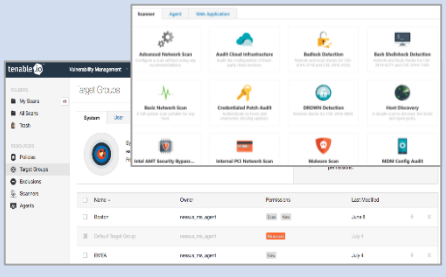
特定の脆弱性を調査

キーワード検索により素早く特定の脆弱性を把握できます。攻撃コードの存在有無、攻撃者目線での脆弱性の存在有無などの結果を項目別に分類します。



システム管理者ごとに権限譲渡

システム管理者ごとにスキャン実行や結果の確認が可能な範囲（IP アドレス範囲）を指定できます。各システム担当者へ展開することで、定期的に脅威を把握することができます。



IBC アイビーシー株式会社

[本社]
〒104-0033 東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780　fax.03-5117-2781

[西日本事業所]
〒532-0004大阪府大阪市淀川区西宮原2-7-38新大阪西浦ビル 3F
tel. 06-7653-1014