

## アシスト、攻撃者視点でリスクを可視化する外部アタックサーフェス管理ソリューション「Tenable.asm」を販売開始

～ 外部攻撃対象領域を把握し、企業の資産を守る ～

株式会社アシスト(本社:東京都千代田区、URL:<https://www.ashisuto.co.jp/>、略記:アシスト)は、脆弱性管理プラットフォームと連携できる外部アタックサーフェス管理(EASM<sup>※</sup>)ソリューション「[Tenable.asm](#)」(開発元:米 Tenable, Inc.、略記:Tenable 社)を販売開始します。

※EASM:External Attack Surface Management の略。外部攻撃対象領域管理のこと

IaaS や PaaS の利用、インターネット上の資産、サービス、アプリケーションが増える中、脆弱性を突く攻撃は数や種類だけでなく巧妙さを増し、企業組織として守るべき資産の明確化とリスク評価に基づく迅速な対処が求められます。昨今の業務部門では SaaS の利用、Web サーバの構築・公開が手軽になった反面、IT 部門が把握していないサーバの公開や、不要なサービスの稼働、ポートの公開といった問題が増えているのが現状です。

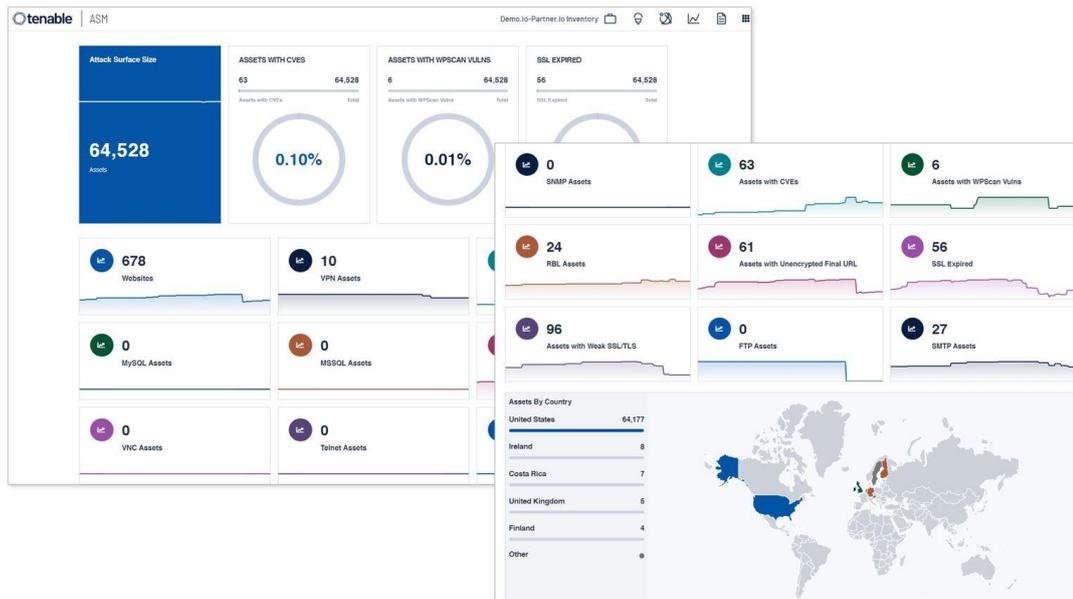
「Tenable.asm」では、インターネットに接続された既知・未知の資産を攻撃者の視点で継続的に確認することにより目に見えないリスクを可視化します。また、同製品群の「Tenable.io」と連動させることで、確認した資産に対してスキャンを行い、詳細に脆弱性リスクを評価することも可能です。SaaS 提供のため、実装から利用開始までの期間短縮や、ツールそのものの保守運用工数の大幅削減だけでなく、タイムリーな対処を可能にします。アシストは「Tenable.asm」をはじめとする Tenable 社製品の日本語サポートはもちろんのこと、PoC の提供や「Tenable.asm」と「Tenable.io」の連携部分の運用フォローなどを通じて、顧客企業のリスクマネジメントを強力に支援していきます。

### ■「Tenable.asm」について

#### ▼特長

##### 1. 外部公開資産を直感的に表示

- 登録ドメインに関連する外部公開サーバ、ネットワーク機器などインターネットに接する全ての既知・未知の資産の情報を収集してダッシュボード上に表示
- 期限切れの SSL 証明書や CVE などの脆弱性が存在するインベントリを把握可能
- VPN サービスや RDP が稼働している資産の数、Web サイト数などの推移をカテゴリごとに表示



ダッシュボードイメージ

## 2. 資産の情報を詳細に可視化

- 実行中のサービスや使用ポートなど 200 超の項目の資産情報を収集可能
- 想定される検索条件があらかじめ用意されており、一覧の資産情報を容易にソート、フィルタリングすることが可能なため、瞬時に必要な情報を把握可能

Table showing asset details for tenabledemo.com:

Search	Host	Record Type	IP	ASN	Ports	Screenshot
	tenabledemo.com	SOA	205.251.198.75	AMAZON-02	-	-
	tenabledemo.com	NS	2600:9000:5306:4b00::1	AMAZON-02	-	-
	target1.pubtarg.tenabledemo.com	A	44.241.194.21	AMAZON-02	22, 80	-
	target2.pubtarg.tenabledemo.com	CNAME	44.242.109.183	AMAZON-02	22, 80	-
	target4.pubtarg.tenabledemo.com	AAAA	2600:1113:941:d000:1ade:34f...	AMAZON-02	22, 80, 111	-
	target3.pubtarg.tenabledemo.com	A	44.241.160.134	AMAZON-02	22, 80	-

一覧表示イメージ

## 3. ポリシーに違反する資産を通知

- ポリシーに違反する資産が検出された際は、メールや Slack などで管理者に通知することが可能
- Log4shell に該当する資産など、多くのポリシーがあらかじめ用意されているため、容易にポリシーの登録が可能

## 4. サイバーリスクの正確な評価を容易に実現

- Tenable.io と連動させることで、数回のクリックでより詳細に脆弱性を検知・評価することが可能
- 監視対象ドメインに関連しそうなドメイン情報を示唆する機能により、サブドメインやグループ会社の資産も漏れなく把握可能

## ▼製品の導入対象顧客(一例)

- 高いセキュリティレベルが求められる企業
- 外部公開資産を多く持つ企業
- IaaS、PaaSなどのクラウド利用企業
- グループ会社・サプライチェーンのリスクを把握したい企業

金融業や、ワールドワイドで活動する製造業で先行して導入されています。

## ▼提供価格

65 オブジェクト 年間利用料 380,000 円(税別・アシストのプロダクトサポート料込)～

以下、Tenable Network Security Japan 株式会社からのコメントです。

株式会社アシストと連携し、インターネットに公開されている資産を確認できる Tenable.asm の機能をお客様に提供できることを嬉しく思います。インターネットにさらされた資産は、外部の攻撃者からアクセスしやすいため、高い脅威に直面しています。Tenable.asm は、企業資産をインターネット側から継続的にモニタリングすることで、この問題を解消し、お客様がサイバー犯罪者の攻撃対象となり得るすべての外部向け資産を迅速に発見・特定できます。(カントリーマネージャー 貴島直也氏)

## ■「Tenable」製品ラインナップ

Tenable は、アタックサーフェス全体の包括的・継続的な脆弱性管理を実現します。

管理対象	目的	対応製品
OS/ミドルウェア/ Web サイト	資産の可視化、脆弱性の検出および高度な優先度付け	<a href="#">Tenable.io</a>
Active Directory (AD)	AD の設定不備の検出、攻撃を受けた際の通知	<a href="#">Tenable.ad</a>
外部公開資産	外部公開資産の可視化、詳細な資産情報の収集、ポリシー違反の検出	<a href="#">Tenable.asm</a>

URL : <https://www.ashisuto.co.jp/product/category/vulnerability-management/tenable/>

## ■「Tenable」に関するお問い合わせ

株式会社アシスト ビジネス推進本部

URL : <https://www.ashisuto.co.jp/pa/contact/tenable.html>

## ■プレスリリースに関するお問い合わせ

株式会社アシスト 広報担当: 田口、曾根原

TEL: 03-5276-5850

URL : <https://www.ashisuto.co.jp/contact/press/>

※ 記載されている会社名、製品名は、各社の商標または登録商標です。

※ プレスリリースに記載された製品／サービスの内容、価格、仕様、お問い合わせなどは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。