ASM（Attack Surface Management）

導入ガイダンス

外部から把握出来る情報を用いて

自組織の IT 資産を発見し管理する

令和 5 年 5 月 29 日

経済産業省 商務情報政策局 サイバーセキュリティ課

改定履歴

改定年月日	改定箇所	改定内容
令和5年5月29日	-	・初版公表

目次

1章　はじめに

近年、我が国においては DX（Digital Transformation）が進められており、我々の社会活動における情報通信技術の役割は重要性を増している。一方で、サイバー攻撃による社会への影響も深刻なものとなっている。サイバー攻撃は、組織における経済的な損失のみならず、攻撃対象や手法によっては、国民の生活に影響を及ぼしうる。実例としては、2021 年に徳島県の公立病院がサイバー攻撃を受け、一般診療が約 2 か月間停止するという事件が発生した。

MITRE ATT&CK[1]によると、サイバー攻撃の初期段階では、公開されている情報やインターネットからアクセス可能な IT 資産から得られる情報を用いて攻撃対象を選定したり、攻撃手法を確立したりする「偵察」が行われるとされている。先に挙げた公立病院の事例では、診療システムの遠隔保守用の機器が、脆弱性を抱えたままインターネットからアクセス可能な状態になっており、これらが攻撃者の偵察行為で発見され、内部に侵入された可能性が高いとみられる。

サイバー攻撃から自社の IT 資産を守るために、上記のようにインターネットに向けて弱点を晒している IT 資産を特定し、セキュリティ対策に活用する Attack Surface Management（ASM）という手法がある。ASM とは、外部（インターネット）からアクセス可能な IT 資産の情報を調査し、それらに存在する脆弱性を継続的に評価する取り組みである。これらの取り組みには、専用のツールやサービスを活用して実施することが一般的であり、実際、インターネット上では、このような情報の調査のための通信も相当数観測されている。『NICTER 観測レポート 2022[2]』によると、国立研究開発法人情報通信研究機構（NICT）のダークネット観測[3]において、2022 年は 12,752 の IP アドレスからの約 2,871 億パケットが調査目的のスキャンとして判定され、これは 2022 年に観測された全パケットの約 54.9％を占めた。調査の目的は不明だが、好むと好まざるとにかかわらず、実際に相当数の偵察行為が行われていることをまずは認識いただきたい。

一方で、サイバー攻撃から守るべき対象である IT 資産に目を向けると、例えば IT 資産を

---

[1] 米国の非営利法人である MITRE 社によって公開されている、サイバー攻撃のプロセスを記述したナレッジベース

[2] 国立研究開発法人情報通信研究機構　「NICTER 観測レポート 2022」
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

[3] インターネット上で到達可能かつ未使用の IP アドレス宛に届くパケットを観測する手法

申告に基づいて管理している企業では、申告漏れや誤認によって、管理している情報と実態に乖離が生じている場合もある。また、買収や経営統合を経てグループ内に企業が多数存在し、管理すべき IT 資産が多岐で広範囲に存在するため管理しきれていない企業もあろう。これに対し ASM は、攻撃者の視点を持ち、実態をベースに、自社の IT 資産を発見するものであり、従来の IT 資産管理とあわせて実施することで自社の内部と外部、あるいは申告と実態からの二重のチェックを行うことができる。

本書の読者としては、企業の情報システムまたは情報セキュリティ部門にあって、セキュリティ向上施策、体制、ツールなどを検討する方を想定している。加えて、CIO（Chief Information Officer）や CISO（Chief Information Security Officer）などの情報セキュリティ戦略に責任を持つ経営層レベルの方にも内容を理解いただき、自社のセキュリティ戦略に組み込んでいただければ幸いである。

最後に本書の主な構成について記載する。2 章では ASM の基礎的事項。（ASM の定義や取り組みの全体像）をなるべく平易に解説する。ASM の基本的な考え方や特徴、期待される効果などについて確認いただきたい。3 章では、ASM の実施にあたって行うべきこと、また、それを支援するツールついて解説する。解説にあたっては、ツールの機能や、使用上の注意点などもまとめている。4 章では、民間事業者における取り組みの一部を事例として紹介する。

2章　ASM（Attack Surface Management）とは

2.1 ASM の定義

ASM という言葉について、米国を中心にいくつかの企業で定義が行われているが、その定義や範囲などにおいて解釈が分かれるケースがある。そこで、本書で取り扱う範囲を明確化する上で、ASM を以下のように定義する。

> **組織の外部（インターネット）からアクセス可能な IT 資産を発見し、**
> **それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス**

ここで、組織の外部（インターネット）からアクセス可能な IT 資産のことを特に「攻撃面」とする。外部からアクセス可能であるという点を強調して EASM（External Attack Surface Management）と紹介されることもあるが、本書では ASM と EASM を同じ意味として取り扱う。

なお、米国国立標準技術研究所（NIST）が SP800-53 として発行している『Security and Privacy Controls for Information Systems and Organizations[4]』で、「攻撃面（Attack Surface)」を以下のように定義している。

> *The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.*

この定義によれば、攻撃面の対象として組織の外部・内部については言及されていない。しかしながら、攻撃面は、組織外の攻撃者が容易に発見できるものであり、かつ、組織がセ

[4] NIST「NIST Special Publication 800-53 revision5　Security and Privacy Controls for Information Systems and Organizations」
(P.395)https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

キュリティ上より注視すべきであるものと考える。そのため、本書では、攻撃面（Attack Surface）を「組織の外部（インターネット）からアクセス可能な IT 資産」とする。

2.2 ASM のプロセス

ASMは、主に「(1) 攻撃面の発見」「(2) 攻撃面の情報収集」「(3) 攻撃面のリスク評価」の 3 つのプロセスで構成される。

(1) **攻撃面の発見**

はじめに、企業が保有または管理している外部（インターネット）からアクセス可能な IT 資産を発見する。具体的には IP アドレス・ホスト名のリストが本プロセスのアウトプットとなる。一般的には以下のような手順で行われる。

i. 組織名をもとに、当該組織が管理者となっているドメイン名を特定する。これは、例えば社外に公開している Web サイトや WHOIS[5]を利用して特定する。

ii. i.で特定したドメイン名に対して、DNS による検索や、ツールなどを活用して IP アドレス・ホスト名の一覧を取得する。

(2) **攻撃面の情報収集**

(1) で発見した IT 資産の情報を収集する。このプロセスで収集する情報には、攻撃面を構成する個々の IT 資産における OS、ソフトウェア、ソフトウェアのバージョン、オープンなポート番号などがある。一般的にこのプロセスは、調査対象に影響を及ぼさないよう、Web ページの表示など通常のアクセスの範囲で行われる。

(3) **攻撃面のリスク評価**

(2) で収集した情報をもとに攻撃面のリスクを評価する。一般的には、公開されている既知の脆弱性情報と、(2) で収集した情報を突合し、脆弱性が存在する可能性を識別する。

本書では、評価したリスクへの対応については ASM のプロセスには含めていない。しかしながら、自社のセキュリティリスクを減らすという目的においては、(3) 攻撃面のリスク評価後にリスクへの対応を実施すべきである。リスクへの対応は、そのリスクが顕在化した場合に想定される被害と修正にかかるコストを考慮して、パッチ適用（リスクの低減）や対策見送り（リスクの受容）など、脆弱性管理と同様のことを実施する必要がある。

[5] ドメイン名・IP アドレス・組織名などを検索するためのプロトコル。Web サービスでも提供されている。

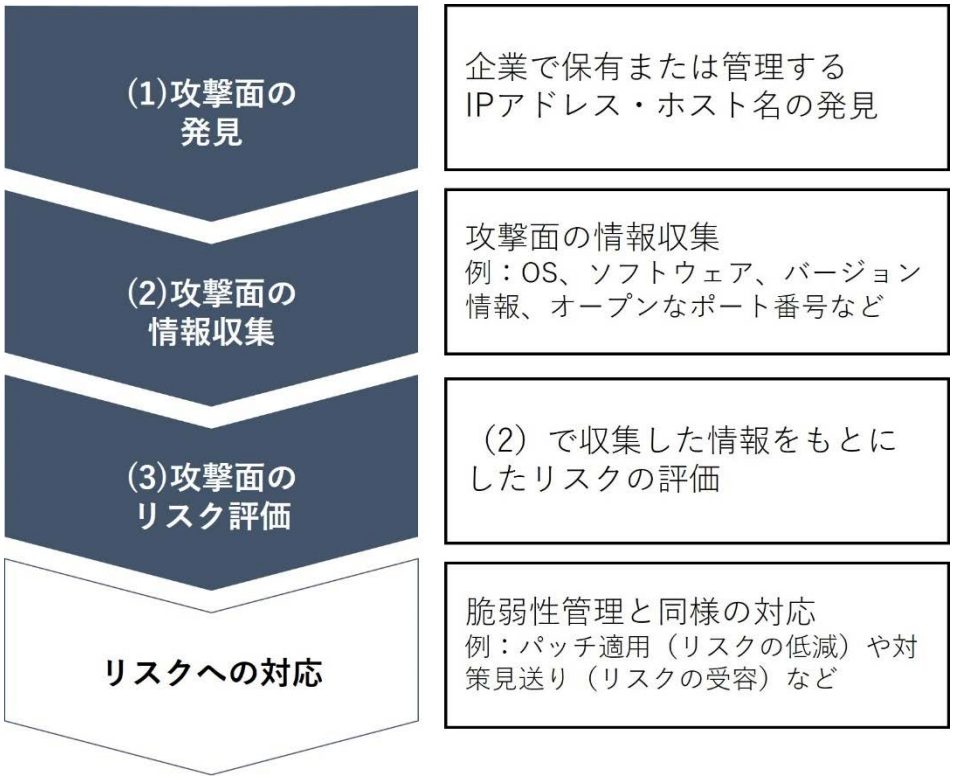

図 2-1 ASM のプロセス

2.3 ASM の特徴

ASM の特徴としては、以下が挙げられる。

✓ 情報システムを管理している部門が把握していない IT 資産を発見できること。
✓ 情報システムを管理している部門の想定と異なり、公開状態となっている IT 資産を発見できること。

リスク評価では、外部（インターネット）から確認できる情報のみを用いるため、脆弱性が存在する可能性の検知にとどまる、という特徴もあり留意が必要である。

■ ASM の活用シーン

上記の特徴により ASM では、以下のようなシーンで活用することができる。

✓ キャンペーン活動などに利用する Web サイトなど、情報システムを管理している部門以外が構築・運用している IT 資産を発見する。
✓ 設定ミスなどにより、外部（インターネット）からアクセス可能な状態となっている社

内システムなどを発見する。

✓ グループ企業における統制上の課題や地理的な要因によって、本社で一元的に管理できていない IT 資産を発見する。

2.4 ASM と脆弱性管理

本節では、ASM に対する理解をより深めるため、ASM と脆弱性管理の関係性、及び ASM と脆弱性診断の違いについて解説する。

■ ASM と脆弱性管理の関係性

はじめに、脆弱性管理のライフサイクルを整理する。以下の内容は、『脆弱性対策の効果的な進め方（ツール活用編）[6]』（独立行政法人情報処理推進機構（IPA））を参考にした脆弱性管理のライフサイクルである。

表 2-1 脆弱性管理のライフサイクル

対象ソフトウェアの把握[7]	サーバ内にインストールされているソフトウェアの情報を把握し、管理する。
脆弱性関連情報の収集	ソフトウェアの最新バージョンや脆弱性情報などを収集する。
適用の判断	収集した脆弱性関連情報の中に新しいバージョンのソフトウェアや脆弱性、攻撃などの情報を確認したら、新しいバージョンのリリースノートや CVSS、緊急度を確認し、脆弱性への対応の要否を判断する。
計画	対策が必要な脆弱性に対して、修正作業などを計画する。
検証	修正作業を本番環境へ適用する前に、検証環境に適用し、本番環境への適用可否を判断する。
適用	修正作業を実行する。

ASM と脆弱性管理の関係性で重要な点は以下の通りである。

1 つ目は、ASM は脆弱性管理の中で「対象ソフトウェアの把握」「脆弱性関連情報の収集」

[6] IPA「脆弱性対策の効果的な進め方（ツール活用編）」
https://www.ipa.go.jp/files/000071584.pdf

[7] 本書では、把握すべきソフトウェアの対象に VPN 装置や複合機上で動作するファームウェアも含む

「適用の判断」をカバーする、という点である。また、「適用の判断」で発見された脆弱性への対応の要否については、ASM のプロセスに含まれていない。

2 つ目は、対象となる IT 資産の範囲が異なるという点である。脆弱性管理は基本的に自社で把握している全ての IT 資産を対象とするが、ASM は未把握であるものも含め、外部（インターネット）からアクセス可能な IT 資産を発見する。つまり、ASM は未把握の IT 資産を発見する、という点において脆弱性管理や IT 資産管理を補完する取り組みと捉えることができる。

■ ASM と脆弱性診断の違い

ASM は、IT 資産に存在する脆弱性などのリスクを検出・評価するという目的において、脆弱性診断と同じであるが、いくつかの観点で異なる。ここでは、ASM と一般的な脆弱性診断との違いについて整理しておきたい。

1 つ目の観点は、対象とする IT 資産である。ASM は外部（インターネット）からアクセス可能な IT 資産が対象であり、これには未把握の IT 資産が含まれる。一方で、脆弱性診断では、把握済みの IT 資産が対象となる。

もう 1 つの観点は、脆弱性情報の確度である。ASM では、通常のアクセスの範囲で得られた情報をもとに、IT 資産に含まれている可能性のある脆弱性情報を提示する。しかし、あくまで可能性のレベルであり、脆弱性を特定しているわけではない。一方で、脆弱性診断では、対象となる IT 資産に攻撃を模したパケットを送信し、その応答を評価して脆弱性を特定する。よって、一般的には脆弱性診断のほうが脆弱性特定の確度は高い。

加えて、対象に及ぼす影響も異なる。脆弱性診断は、調査のためのパケットがセキュリティ監視装置に検出されアラートを発報する場合や、対象の IT 資産の動作に支障を及ぼす場合がある。一方で、ASM は対象の IT 資産への影響はほとんどない。

以上のように、ASM と脆弱性診断は異なるものであり、目的に応じて使い分けや併用を検討すべきである。

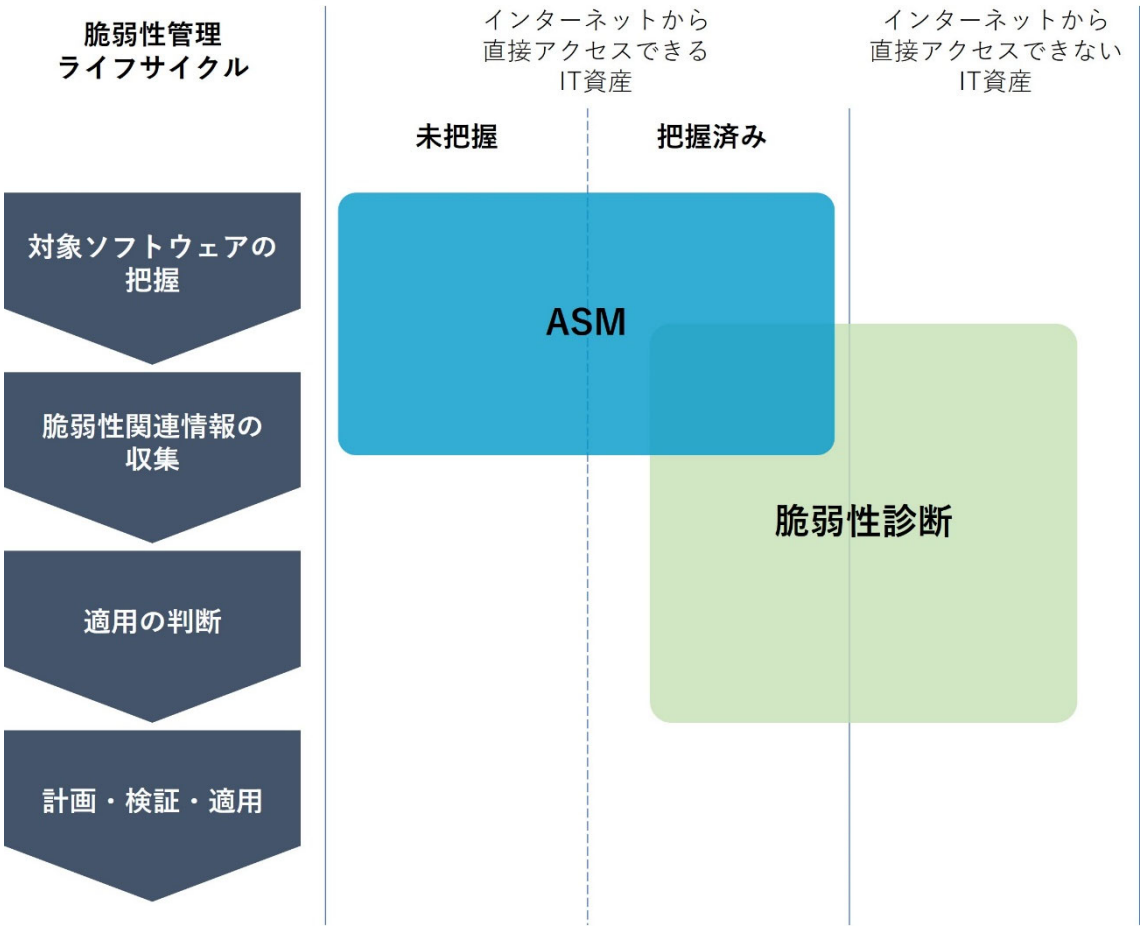

図 2-2 ASM と脆弱性診断の違い

表 1-1 ASM と脆弱性診断の関係性

	対象	脆弱性の特定確度	対象への影響
ASM	インターネット上を検索し、発見したものを対象とする	通常アクセスの範囲で行うため確度が低い可能性がある	パケットがセキュリティ監視装置に検出されることはほとんどない
脆弱性診断	対象をあらかじめ指定する	攻撃を模したパケットを送信し、その応答を評価することで一定の確度が確保される	セキュリティ監視装置でアラームを検出したりシステムダウンを誘発したりすることがある

3章　ASM の実施

3.1 実施計画の策定

他のセキュリティ施策同様、ASM も実施計画を策定しておくことが肝要である。ここでは、実施計画の策定にあたり、特に検討しておくべき事項を述べる。

- **導入目的**

ASM 導入の目的を明らかにしておくことは、他の項目を検討する際の基礎となるため、特に重要な項目である。例えば以下のようなことを取り決めておくことが望ましい。

✓ IT 資産管理を強化するため、未把握の IT 資産を発見する。
✓ グループ企業や海外拠点のセキュリティレベルの評価を行い、セキュリティガバナンス強化に活用する。
✓ 緊急性の高い脆弱性情報が公開された際に、自社の IT 資産に該当するかを簡易的に調査する。
✓ 脆弱性管理を導入する際の初期段階として、サイバー攻撃を受けやすい IT 資産を対象とした管理を実施する。
✓ 外部の組織から自社のセキュリティレベル提示を求められた際に提示する材料の一つとする。

- **調査対象範囲**

調査対象範囲は、ツール購入費用や人的リソースの確保に影響する項目である。以下のような単位で、どの範囲を対象とするのか、IT 資産の数などの規模とともに明確にしておく。

✓ 自社
✓ グループ企業
✓ サプライチェーンなどの取引先企業

- **運用**

[2.4 ASM と脆弱性管理]で解説した通り、ASM は脆弱性管理の一部である。すでに脆弱性管理に取り組んでいる組織であれば、その取り組みとの整合性なども鑑み、以下のような事項を整理しておくべきである。

✓ 調査の実施頻度
✓ 発見された IT 資産の管理者が不明の場合の対処

✓ 攻撃面やリスクが発見された場合の詳細な調査の方法（脆弱性診断の活用など）
✓ 上記で脆弱性が発見された場合の連絡方法
✓ 脆弱性への対応方法

特に、調査対象範囲を海外含むグループ企業全体にする場合、企業間で連絡方法や脆弱性対応する際の役割分担については事前に整理しておくことは、ASM ツールの運用を円滑に進めるために重要である。

- **ツール**

実際の攻撃面の調査と評価には、ツールの利用が実質不可欠である。ツールの選定にあたっては、上記で検討した事項とツール自身が備えている機能とを考慮し、決定する必要がある。ツールの機能については、次節で解説する。

本節で挙げた項目の検討において、机上での調査・検討が困難であることも予想される。そのため、少額の費用で実行できる範囲で PoC（概念実証）を実施することも有用である。

3.2 攻撃面の調査と評価

ASM は、全てを手作業で実施することは難しく、ASM の実施を支援する各種のツール（以降は ASM ツールと表記する）を活用するのが一般的である。本節では、ASM ツールの機能を中心に、事前に準備すべき事項、注意すべき事項などを解説する。

3.2.1 事前準備

組織名をもとに、調査の対象範囲となる組織が管理している IP アドレスやドメイン名、関連するドメイン名の洗い出しを実施する。洗い出しを実施する際に、WHOIS などを利用して特定する方法も有用である。なお、ASM ツールの中には、ドメイン名を入力すると関連する IP アドレスやドメイン名を発見する機能を備えているものもある。

3.2.2　ASM ツール

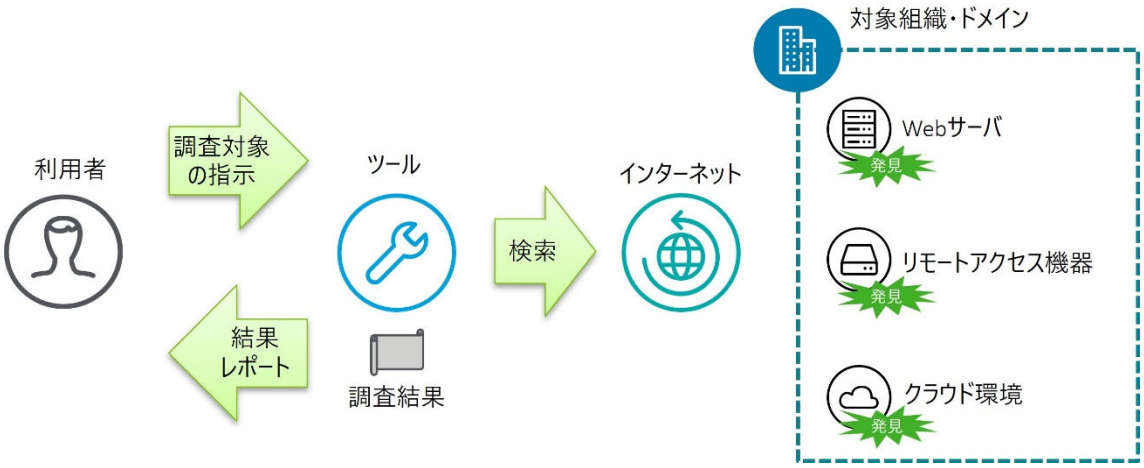

図 3-1 ASM ツールの動作

上記の図 3-1 は、ASM ツールの動作の概略を示したものである。ASM ツールは、検索した攻撃面の情報やそれらの情報をもとに算出したリスク評価の情報を可視化するツールである。また、可視化した情報をレポートとして出力可能なツールも存在する。

ASM ツールは、主に下記の「検索エンジン型」と「オンアクセス型」に分類される。

- **検索エンジン型**
  ASM ツールを提供している事業者が、独自に収集した情報を事業者が管理するデータベースに保存し、ユーザーがツール操作時にデータベース上で攻撃面の検索・閲覧する型。
- **オンアクセス型**
  ユーザーが検索を実行したタイミングで、対象への通信を行い攻撃面の情報を収集する型。

表 3-1 では、一般的な ASM ツールが備える機能を挙げる。

表 3-1 ASM ツール機能（プロセス別）

分類	機能
攻撃面の発見	● **IP アドレス・ホスト名の一覧表示機能** ドメイン名などから、関連する IP アドレス・ホスト名の一覧を表示する。
攻撃面の	● **攻撃面の詳細情報表示機能**

情報収集	特定の攻撃面における詳細情報を表示する。
	● **ダッシュボード機能** グラフやマップなどを用いて情報をグラフィカルに表示する。
攻撃面の リスク評価	● **リスク評価機能** 攻撃面の危険度もしくは成熟度を評価する。 ● **レポート機能** 評価結果のレポートを生成・出力する。
その他	● **リスク対応補助機能** 対応優先度を付与する。 ● **ファイル出力機能** 発見した攻撃面や脆弱性情報を CSV などで出力する。 ● **通知機能** 特定の情報をトリガーとしてユーザーに通知する。 ● **ログ機能** ツール操作のログを収集する。 ● **アクセス制御** ロールを設定し、各ユーザーの操作を制限する。 ● **対応状況管理機能** 調査中や調査済みなどの対応状況のタグを付与する。

- **IP アドレス・ホスト名の一覧表示機能**

  ドメイン名から攻撃面の IP アドレス・ホスト名の一覧を表示する機能。

図 3-2 では、攻撃面の IP アドレス・ホスト名を一覧で表示した画面である。一覧は IP アドレス・ホスト名に加え、OS などの情報が表示されている。OS、ミドルウェア、ポート番号（稼働しているサービス）、CVE、発見された時刻などの情報で絞り込みが可能な場合が多い。

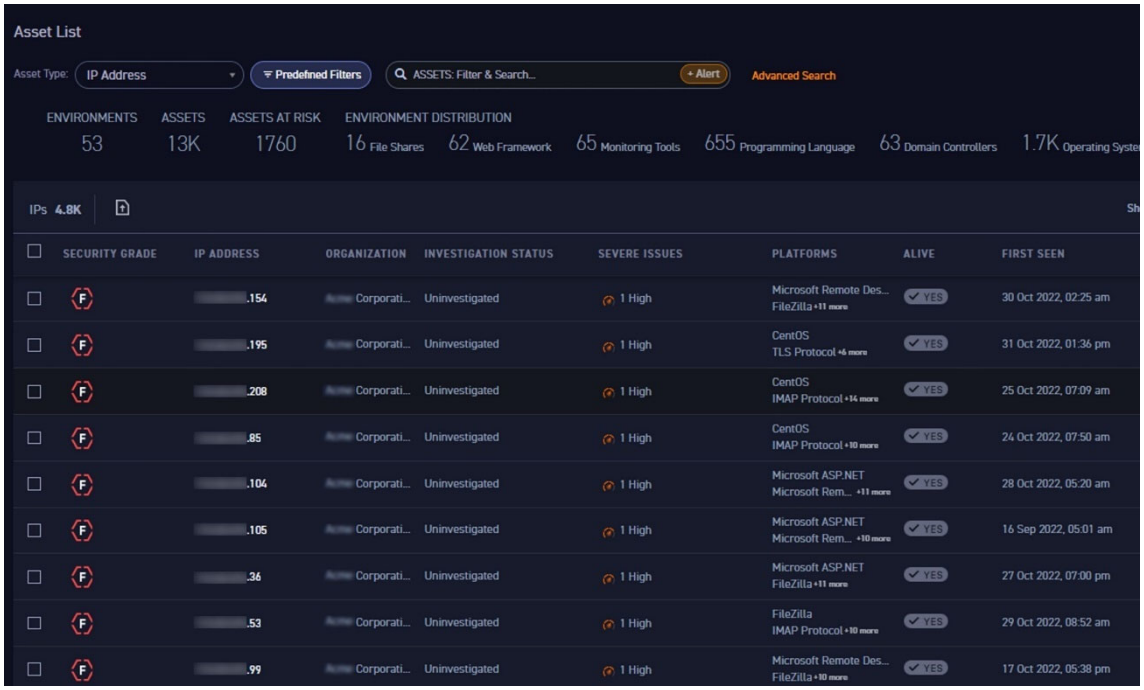

図 3-2 攻撃面の情報収集機能の表示例

- **攻撃面の詳細情報表示機能**

攻撃面の詳細情報を表示する機能。IP アドレス・ホスト名の一覧において 1 つの攻撃面を選択することで確認することができる。以下のような情報が確認可能である。

✓ 対象ホスト名
✓ IP アドレス
✓ OS、OS のバージョン
✓ ソフトウェア、ソフトウェアのバージョン
✓ アクセス可能なポート番号
✓ クラウドのベンダー情報
✓ 攻撃面を発見した日付

図 3-3 は、図 3-2 の一覧から 1 つの攻撃面を選択した場合に表示される詳細情報の画面である。一覧表示と比較し、より詳細な情報が確認可能である。

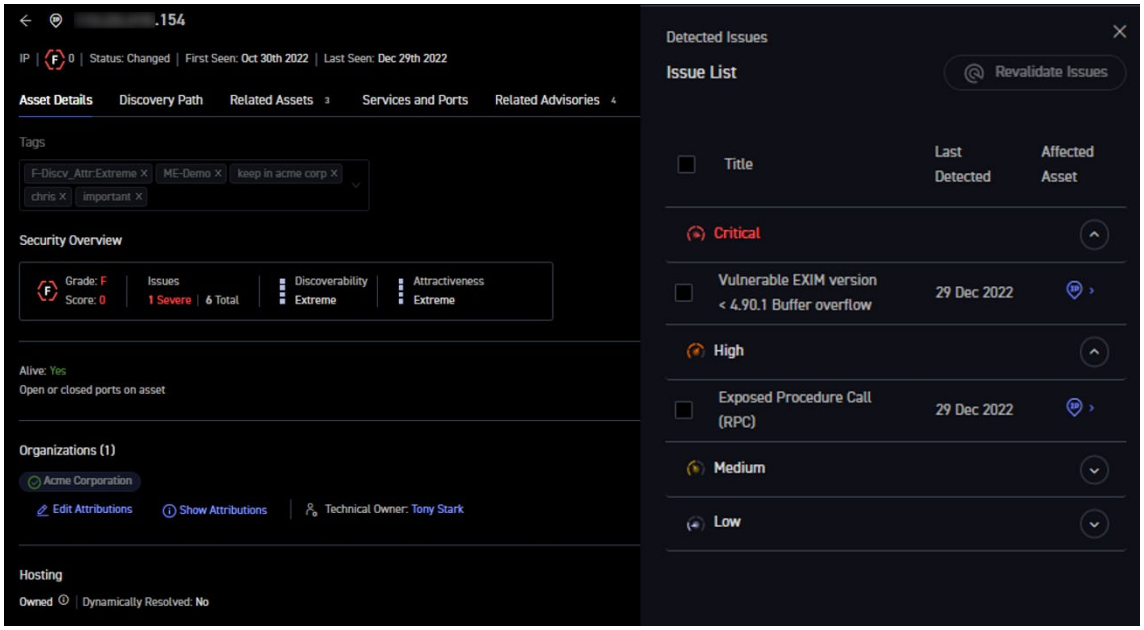

図 3-3 情報表示機能例の表示例

- **ダッシュボード機能**

グラフやマップなどを用いてグラフィカルに情報を表示する機能。全体の傾向を確認する際に有用である。攻撃面に関する数の変化や種別、攻撃面が存在する国のマップなどの項目が表示される場合が多い。

図 3-4 のダッシュボード機能では、攻撃面の数や攻撃面全体を評価したグラフ、IP アドレス情報を参考にした攻撃面の分布がマップに表示されている。

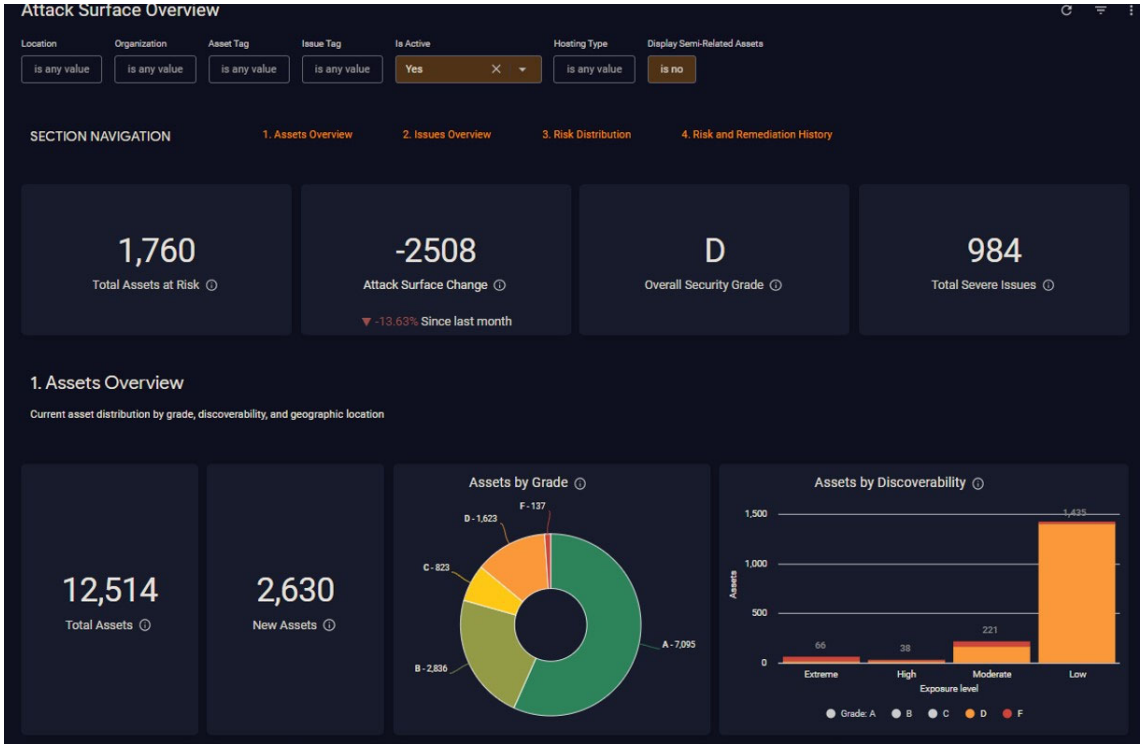

図 3-4 ダッシュボード機能の表示例

- **リスク評価機能**

検索によって得られた情報をもとにした攻撃面のリスクを表示する機能。攻撃面の危険度を評価するものが多いが、攻撃面全体の成熟度を表示するツールも存在する。また、リスクの評価基準は、CVSS の情報を使用するものが多いが、悪用可能性などの複数の要素を組み合わせて独自のロジックで評価結果を算出するツールも存在する。

ASM ツールにおけるリスク評価をもとに対応を検討する際には、注意すべき点がある。詳細は[3.2.3 活用にあたって注意すべき事項]をご確認いただきたい。

図 3-5 は、図 3-3 からリスク評価に関する項目をピックアップした画面である。

図 3-5 リスク評価機能の表示例

- **レポート機能**

  算出されたリスク評価をレポート（PDF）形式で生成・出力する機能。

- **リスク対応補助機能**

  対応優先度順位や対応方法などを提示し、リスク対応の補助となる機能。

- **ファイル出力機能**

  攻撃面や脆弱性情報などの一覧を CSV などでエクスポートする機能。

- **通知機能**

  特定の情報をトリガーとしてユーザーに通知する機能。独自にチケット発行システムを備えているものやメールやチャットのシステムと連携するものがある。

- **アクセス制御機能**

  登録されたアカウントによるコンソール画面での操作・閲覧を制限する機能。

- **ログ機能**

  ユーザー操作のログを収集・保存する機能。保存先として Syslog サーバや SIEM が選択可能な場合がある。

- **対応状況管理機能**

  調査中や調査済みなどの対応状況のタグを付与する機能。

3.2.3　必要となる知識・スキル

本項では、ASM ツールの活用にあたって備えていると望ましい知識・スキルを紹介する。本項で取り上げる内容は ASM ツールの管理者としてだけではなく、組織として備えていると望ましいものも挙げている。

また、「情報セキュリティの知識」は、IPA の情報セキュリティマネジメント試験[8]のシラバスから、ASM ツールの取り扱いにおいて必要と思われる要素を抽出したものである。

- **情報セキュリティの知識**

  ASM ツールに表示された情報を正確に読み解くには、情報セキュリティの基礎的な考え

[8] IPA　「情報セキュリティマネジメント試験」
https://www.jitec.ipa.go.jp/sg/

方や各種プロトコル・ネットワークなどの技術的な知識が必要となる。

表 3-2 ASM の活用に必要となる情報セキュリティの知識

分類	項目
情報セキュリティ	✓ 情報セキュリティの目的と考え方 ✓ 情報セキュリティの重要性 ✓ 脆弱性 ✓ 攻撃の種類 ✓ 攻撃の動機 ✓ サイバー攻撃手法 ✓ 情報セキュリティ技術（公開鍵基盤）
情報セキュリティ管理	✓ 情報セキュリティ管理 ✓ リスク分析と評価 （情報資産の調査・分類） （リスクの種類） （情報セキュリティアセスメント） （情報セキュリティリスク対応） ✓ 情報セキュリティ諸規程（情報セキュリティポリシーを含む組織内規程） ✓ 情報セキュリティ組織・機関
情報セキュリティ対策	✓ 人的セキュリティ対策 ✓ 技術的セキュリティ対策 ✓ 物理的セキュリティ対策
セキュリティ実装技術	✓ セキュアプロトコル ✓ ネットワークセキュリティ ✓ アプリケーションセキュリティ
セキュリティ関連法規	✓ 不正アクセス禁止法 ✓ その他のセキュリティ関連法規
ネットワーク方式	✓ ネットワークの種類と特徴 ✓ インターネット技術
データ通信と制御	✓ 伝送方式と回線 ✓ ネットワーク接続
通信プロトコル	✓ プロトコルとインターフェース （ネットワーク層、トランスポート層） （アプリケーション層）
情報資産管理の計画	✓ 情報資産の特定及び価値の明確化

	✓ 管理責任及び利用の許容範囲の明確化 ✓ 資産管理台帳の作成
情報セキュリティリスクアセスメント及びリスク対応	✓ リスクの特定・分析・評価 ✓ リスク対応策の検討 ✓ リスク対応計画の策定
情報資産の管理	✓ 情報資産台帳の維持管理 ✓ 利用状況の記録
部門の情報システム利用時の情報セキュリティの確保	✓ 脆弱性管理
情報セキュリティに関する動向・事例情報の収集と評価	✓ 情報セキュリティに関する動向・事例情報の収集と評価

- **ヒューマンスキル**

ASM ツールの管理者は、発見した脆弱性を関係者に報告する役割を担うことが想定されるため、コミュニケーションスキルやレポーティングスキルが求められる。また、公開される最新の脆弱性情報は一次情報が英語であることが多いため、英語で書かれた情報を読み解くスキルを持つことが望ましい。

表 3-3 ASM の活用に必要となるヒューマンスキル

項目	補足
コミュニケーションスキル	✓ 口頭もしくは文章にて効果的に伝聞するスキル ✓ 関係部署や担当者と折衝・協力する能力
レポーティングスキル	✓ 技術的に難解な内容を相手に合わせて書き砕くスキル
英語力	✓ 英語で書かれた情報を正確に読み解くスキル

- **組織・体制の知識**

ASM を活用する上で、自社に関する下記の知識を備えておくことが望ましい。

表 3-4 ASM の活用に必要となる組織・体制の知識

項目	補足
組織体制に関する知識	✓ 自社システムの責任者やセキュリティ対応体制の知識
システム構成やアーキテクチャに関する知識	✓ 自社のシステム構成やアーキテクチャに関する知識
セキュリティポリシーに	✓ 自社で定めた情報セキュリティのポリシーやスタンダー

関する知識	ドなどの知識

上記に挙げた知識やスキルは、ASM ツールを利用する上で、以下のタスクに対応する際に必要となる。

表 3-5 実行するタスクと必要となる知識・スキル

タスク	タスクに関連する知識・能力
実施計画を策定する （PoC の実施、ツールの選定など）	✓ 情報セキュリティの知識 ✓ ヒューマンスキル ✓ 組織・体制の知識
ASM ツールの機能を活用し、攻撃面や脆弱性情報を見つけ出す	✓ 情報セキュリティの知識
脆弱性診断などを実施し、脆弱性が含まれているかを確認する	✓ 情報セキュリティの知識
脆弱性の悪用可能性を考慮し、攻撃の受けやすさを判断する	✓ 情報セキュリティの知識
攻撃の受けやすさと、自社における IT 資産の重要度から対応すべきものか判断する	✓ 情報セキュリティの知識 ✓ 組織・体制の知識
IT 資産の管理者など、関係部署に適切に伝達する	✓ 情報セキュリティの知識 ✓ ヒューマンスキル ✓ 組織・体制の知識
IT 資産管理者の脆弱性対応をサポートする	✓ 情報セキュリティの知識 ✓ ヒューマンスキル

3.2.4 注意すべき事項

本項では、ASM ツールを活用するにあたって注意すべき事項を解説する。

- **不正確な情報の検知**

ASM ツールの画面に表示された情報の中には、不確かな情報や実態に即していない情報が表示されることがある。ASM の情報を読み解く際は以下に注意する必要がある。また、以下の注意点があるため、ASM ツールの評価結果をもとにした評価対象企業への是正措置の強要は控え、セキュリティレベルの評価、公表については慎重に行うべきである。

1 つ目は、自社で管理していない攻撃面が発見される点である。対象となる攻撃面が CDN やクラウド上の IT 資産である場合は、IT 資産に割り当てられている IP アドレスが変更さ

れることが想定される。また、ホスト名で検索した場合は DNS レコードの状態によって、自社で管理していない IT 資産の IP アドレスが正引きされることが想定される。

2 つ目は、脆弱性情報の確度という点である。検索エンジン型の ASM ツールでは、各攻撃面に関して OS やソフトウェア、それらのバージョン情報を収集し、その情報をもとに脆弱性情報を表示するものがある。そのため、実際に脆弱性を確認しているのではなく、あくまで含まれている可能性のある脆弱性を評価結果として表示する。また、リスク評価機能は、確度の低い脆弱性情報をもとに算出しているため、実態に即していない可能性がある。

3 つ目は、偽陽性・偽陰性（フォールスポジティブ・フォールスネガティブ）という点である。ASM ツールは、脆弱性が存在しないにも関わらず脆弱性が表示されること（偽陽性）や、脆弱性が存在するにも関わらず脆弱性がないと表示されること（偽陰性）がある。偽陽性が発生する理由としては、検索エンジン型の場合、データベース情報が最新でないことや、パッチ適用前後でバージョン番号が変化しないことなどが挙げられる。また、偽陰性が発生する理由としては、対象となる IT 資産で脆弱性判定の根拠となるバナー情報を非表示にするなどの設定をしていることが挙げられる。

- **対象となる企業への影響**

対象となる攻撃面が、他社によって管理・運用されているシステムである場合は、情報を収集する前に対象となる会社に承認を得ることを推奨する。

[3.2.1 ASM ツール]で解説したように、ASM ツールの攻撃面の情報収集方法には、対象となる攻撃面へ通信を行い、情報を収集するオンアクセス型が存在する。オンアクセス型は、情報を収集する際に対象環境に負荷を与え、業務に影響を及ぼす可能性がある。そのため、オンアクセス型の ASM ツールで他社が管理･運用している攻撃面の情報を収集する前には、事前に確認を行い、承認を得ることを推奨する。

承認を得ないまま、他社のシステムで障害を発生させた場合は、民法の不法行為による損害賠償や刑法の電子計算機損壊等業務妨害罪、不正アクセス禁止法等による訴訟に発展する可能性がある。

一方で、検索エンジン型の ASM ツールは、ツールを提供する事業者側の責任で情報を収集するため、その法的責任については本書では取り扱わない。

- **脆弱性評価の方法**

ASM ツールでは、CVE・CVSS などを活用し、脆弱性情報と評価結果を表示しているツ

ールが多い。また、一部の ASM ツールでは、Snyk Vulnerability Database[9]や独自のロジックなどをもとに評価している。そのため、自社で脆弱性情報の評価基準として既に活用しているものがあれば、ASM ツールの評価基準を自社の基準にマッピングするなどの工夫が必要である。

- **リスク評価指標の活用方法**

ASM ツールのリスク評価は実態に即していない可能性がある。上記で解説した通り、ASM ツールでは CVE・CVSS などのオープンな評価手法や独自ロジックに基づいて評価している。攻撃面のリスク評価が CVSS のハイスコア評価であっても悪用行為が確認されていなければスコア通りの対応優先度とはならないケースも想定される。

- **検索エンジン型の更新頻度**

検索エンジン型の ASM ツールにおける情報の更新頻度は注意が必要である。検索エンジン型の場合、[3.2.2 ASM ツール]で解説した通り、攻撃面の情報は事業者が収集したタイミングのものがデータベースに保存され、ユーザーは、データベースを検索している。そのため、ユーザーが閲覧する情報は検索を行った時点の情報ではない可能性が高い。

検索エンジン型の ASM ツールでは、攻撃面の詳細情報表示画面で攻撃面を確認した日時が表示される。攻撃面の詳細情報を確認する際は、日時の情報もあわせて確認するべきである。

3.2.5 ASM サービス

ASM サービスとは、外部の事業者が契約内容に基づき、ASM の取り組みをサポートするものである。提供されるサービスはさまざまである。攻撃面のリスク評価を行い、調査結果のレポートと専門家による詳細な解説を提供するものや ASM ツールの運用を代行するものがある。

そのため、自社内に ASM ツールを扱うスキルを有する人材的余裕や導入を検討する時間的余裕がない場合でも ASM を実施することが可能である。また、本格導入前の評価リソースの確保や計画策定に資する情報を収集することなども可能である。

自社の状況や目的に合わせて、ASM ツールの代わりに ASM サービスを活用することは有用である。

---

[9] Snyk Limited「Snyk Vulnerability Database | Snyk」
https://security.snyk.io/

3.3 継続的な対応

上記の[3.2.3 活用にあたって注意すべき事項]でも解説した通り、自社が持つ IT 資産に関する状況は時間経過によって変化する。IT 資産の増加または変化や IT 資産における脆弱性の発見などがそれにあたる。そのため、ASM は継続的に取り組む必要がある。

ASM 実施については、より頻繁に実施したほうサイバー攻撃のリスクを低減できるが、その分業務負荷が高くなる。実施の頻度は自社のセキュリティポリシーや業務負荷、サイバー攻撃の流行などの内外部の要因をもとに総合的に判断いただきたい。

4章　事例

本書を作成するにあたり、日本国内に本社を持つ企業に対して ASM の取組実態と課題を明らかにするためのヒアリングを実施した。本章では、これから ASM に取り組む企業に対して有益であると推察される 2 つの事例をヒアリングの中から取り上げ、解説する。

1 つ目の事例-A は、ビジネスの特性上、発生しやすい脆弱性を ASM で解決している事例である。2 つ目の事例-B は、ASM に取り組んでいる企業の多くから課題として聞かれた「発見された脆弱性への対応」に対し、網羅性と迅速性のある脆弱性管理を実現させている事例である。

3.4 事例-A

取組実態調査のヒアリングした企業のうち、ビジネス特性上、発生しやすい脆弱性管理の課題を ASM で対応している事例を紹介する。

- **背景と課題**

事例-A の企業は、一般消費財の製造・販売を中心としたビジネスを展開している。ビジネスを展開する際にプロモーションやキャンペーン活動を頻繁に実施しており、それらの活動ごとにドメインや IP アドレスを新しく取得していた。そのため、本社の情報システム部門で把握・管理ができていないドメインや IP アドレスが複数存在していた。一方で非管理ドメインや IP アドレスが原因のインシデントが発生したため、攻撃面の把握と脆弱性管理が急務となった。

本企業の課題は、以下の 2 点であった。

(1) 本社の情報システム部門が把握・管理ができていないドメインや IP アドレスが国内外に複数存在しており、完全には管理できていなかった。
(2) プロモーションやキャンペーンのサイトに含まれている脆弱性などを十分には管理できていなかった。

- **アプローチ**

本企業は、サイバー攻撃を受けたことをきっかけとして、上記 2 点の課題を解決するために、ASM ツールが導入された。

（1）の課題に対しては、ASM ツールの機能により毎日検索を実行し、最新の情報が把握

できるようにした。また、ASM ツールの管理者は必要に応じて手動で登録することで、より幅広い IT 資産の把握が可能となった。

（2）の課題に対し、本社 CSIRT メンバーが運用フローに加わり、EC サイト管理者の対応をサポートする体制を構築した。ASM ツールではリスク評価結果をメールで関係者に送付するように設定し、受け取った関係者は詳細を調査する。その後、EC サイト管理者に連絡をしている。本社 CSIRT メンバーは対応に必要なアクションを EC サイト管理者に共有することで、「なぜ対応しなければならないか」「何をどうしなければいけないか」が明確になり、迅速にリスク対応に取り組むことが可能となった。

- **事例-A のポイント**

事例-A のポイントは、以下の通りである。

✓ ASM ツールの機能と手動による対応で、常に最新の IT 資産情報を確認できるようになった。
✓ ツール管理者とサイト管理者だけでなく、CSIRT メンバーを運用フローに組み込むことで、迅速なリスク対応を可能とした。

また、ASM ツールのリスク評価機能であるスコアリングシステムの利用により、以下の副次的なメリットがもたらされた。

✓ 関係者間で対応優先度の共通認識を持てた。
（ツール導入前は関係者における認識の違いから、対応優先度に差が生じていた）
✓ 脆弱性の対応によりスコアが上昇するため、対応メンバーにおける意識の高まり、対応スピードの向上に繋がった。
✓ 脆弱性対応に関する上層部への説明が容易になった。

3.5 事例-B

ASM に取り組んでいる企業の多くから、「ASM ツールで見つかった資産がどの部門のものであるか特定することが難しい」や「見つかった脆弱性は誰がどのように対応するのか、調整が難しい」という声が聞かれた。特に、海外拠点や海外グループ企業で見つかった脆弱性の対応に課題を抱えている企業が多かった。

事例-B は ASM ツールを導入している事例ではないが、脆弱性管理において海外グループ企業を含めてグローバルに脆弱性の対応を可能とする体制を整えている企業の事例を紹

介する。

- **背景と課題**

事例-B の企業は製造業を中心としてビジネスを展開し、世界各国に数百のグループ企業を持つグローバル企業である。この企業は、これまでにも脆弱性管理を本社主導で実施していたが、海外拠点の企業では、国内と同じレベルの脆弱性管理は実施できなかった。

本企業は海外拠点の企業における脆弱性管理の課題として、具体的に以下 2 点を抱えていた。

(1) 本社主導で脆弱性診断を実施するため、海外拠点の各企業から対象となる IT 資産の情報を収集しようとしたができなかった。
(2) 海外拠点の各企業でセキュリティ人材を確保できていないため、脆弱性診断後の是正対応ができていなかった。

- **アプローチ**

本企業は（1）(2）の課題に対して、各地域で脆弱性管理のサポートを役割とした中核企業を選定し、海外拠点の企業にサポートが行き届く体制を構築した。

本社は数百のグループ企業から各地域の橋渡しとなる中核企業を 20 社ピックアップし、協力関係を築いた。関係構築後、本社と中核企業で役割分担を行った。本社は中核企業へ脆弱性診断実施の連絡から脆弱性の是正方法までを提示する役割を担い、中核企業は本社の脆弱性管理の取り組みを地域のグループ企業に広めるための役割を担うことにした。役割を分担し体制を整えたことで、中核企業から海外拠点の企業へ手厚いサポートが行き届くようになった。

現在はピックアップした中核企業 20 社に対して、セキュリティスキルを高めるための教育施策を展開し、セキュリティスキルの底上げを目指している。

- **事例-B のポイント**

事例-B のポイントは、脆弱性管理をグループ企業全体で実施するために、IT 資産管理から脆弱性診断後の是正対応をサポートする体制をグループ企業全体で構築した点である。これは、ASM の実施にも応用できる。

ASM では、発見された IT 資産の所有者を特定することや発見された脆弱性の是正対応をすることについてはカバーできないものが多い。取組実態調査にてヒアリングした多くの

企業では、これらのカバーできない対応について課題を抱えていた。ASM ツールで対応できない脆弱性の対応については、組織的に体制を構築することで、より細やかなで柔軟な対応が可能となる。

5章　おわりに

本書では、外部から把握できる情報を用いて IT 資産を適切に管理する手法として、ASM を取り上げ、その概念やツール、活用事例について解説してきた。

ASM は、攻撃者視点を持つという特徴がある。攻撃者は ASM で確認可能な情報を用いてサイバー攻撃の活動を実施する場合が多い。防御側が攻撃者と同じ視点で自社をチェックすることで、これまでのように攻撃被害が発生してから IT 資産の課題に気づくのではなく、攻撃被害の発生前に IT 資産の課題に気づくことが可能となる。

一方で、ASM で確認可能な情報については、注意を要するものもある。発見される脆弱性情報については、ソフトウェアやバージョン情報をもとにしているため、脆弱性診断と比べ確度が低い可能性がある。また、リスク評価については、確度が低い脆弱性情報であることに加え、悪用の可能性などを考慮していないため、実態に即していない可能性がある。

そのため、ASM を効果的に活用し、自社のセキュリティ強化に繋げるためには、継続的な取り組みや担当者のスキル向上、システム管理者との連携などが必要となる。また、IT 資産管理や脆弱性管理など他施策との連携も重要なポイントである。

近年、サイバー攻撃の実社会に与える影響は益々増大しており、サイバー攻撃の対象や攻撃手法によっては国民の生活に影響を及ぼしうる。本書が ASM への取り組みのきっかけとなり、読者の皆様が所属している企業、ひいては社会全体のセキュリティ強化の一助になることを期待する。

6章　付録

6.1 用語集

用語	解説
ASM （ Attack Surface Management）	外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス。 詳細は「2.1 ASM の定義」を参照。
AS （ Attack Surface、攻撃面）	組織の外部（インターネット）からアクセス可能な IT 資産のこと。日本国内では「攻撃対象領域」と表記される場合があるが、本書では「攻撃面」と表記する。 詳細は「2.1 ASM の定義」を参照。
IT 資産	企業活動を行う上で必要となる IT 機器や IT システム。
ASM ツール	組織の外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスを実行するツール。 SaaS 型で利用可能であるものと、ソフトウェア型で購入後インストール作業が必要なものもある。
ASM サービス	外部の事業者が契約内容に基づき、ASM の取り組みをサポートするもの。 攻撃面のリスク評価を行い、調査結果のレポートと詳細な解説を提供するものや ASM ツールの運用を代行するものがある。
脆弱性診断	ネットワーク、OS、ミドルウェア、アプリケーションなどに脆弱性がないかを確認するセキュリティテストのこと。本書では、ネットワーク、OS、ミドルウェアを対象とした所謂プラットフォーム診断を ASM の比較対象としている。
CVE	個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子のこと。
CVSS	情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダーに依存しない共通の評価方法。基本評価基準（Base Metrics）・現状評価基準（Temporal Metrics）・環境評価基準（Environmental Metrics）の 3 つの基準で評価する。
電子計算機損壊等業務妨害	刑法第二百三十四条の二。 電子計算機の損壊行為や電磁的記録の損壊行為、虚偽の情報や不正指令を与える行為などにより人の業務を妨害した者に、五年以下の懲役

	又は百万円以下の罰金に処される。
不正アクセス行為の禁止等に関する法律	平成十一年法律第百二十八号。 不正アクセス行為の禁止（第三条）や不正アクセス行為を助長する行為の禁止（第五条）が含まれる。 https://elaws.e-gov.go.jp/document?lawid=411AC0000000128

6.2 参考情報

- NICT 情報通信研究機構 - NICTER 観測レポート
  https://www.nict.go.jp/cyber/report.html
- NICT 情報通信研究機構 - NICTER Blog
  https://blog.nicter.jp/
- NIST National Institute of Standards and Technology – SP 800-53 Rev.5
  https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/archive/2020-09-23
- IPA 情報処理推進機構 – セキュリティ関連文書『NIST SP800-53 Rev.5』
  https://www.ipa.go.jp/files/000092657.pdf
- MITER - MITER ATT&CK
  https://attack.mitre.org/
- IPA - 脆弱性対策の効果的な進め方（ツール活用編）
  https://www.ipa.go.jp/files/000071584.pdf
- IPA - 情報セキュリティマネジメント試験（レベル２）シラバス
  https://www.jitec.ipa.go.jp/1_13download/syllabus_sg_ver3_3.pdf
- IPA - 共通脆弱性識別子 CVE 概説
  https://www.ipa.go.jp/security/vuln/CVE.html
- IPA - 共通脆弱性評価システム CVSS 概説
  https://www.ipa.go.jp/security/vuln/CVSS.html
- IPA - JVN iPedia 脆弱性対策情報データベース
  https://jvndb.jvn.jp/index.html
- NIST – NVD
  https://nvd.nist.gov/
- Snyk Limited - Snyk Vulnerability Database
  https://security.snyk.io/