Deloitte.
デロイト トーマツ

令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（外部から把握できる情報の活用に関する調査）

最終報告書

デロイト トーマツ サイバー合同会社

2023年3月29日

目次

1. 概要

概要

外部から把握できる情報の活用について、企業における取組実態を明らかにし、実効的なガイダンスを作成、セキュリティ対策への活用検討を実施しました

■ （**背景1**） DXが進展する中、クラウド利用の拡大に加え、企業が所有するIT資産が増加し、点在しています。また、コロナ禍によるテレワークの拡大などを通じて、社会全体でリモート化が進められています。これらにより、社会全体として**「サイバー攻撃の起点が増加」**している状況です

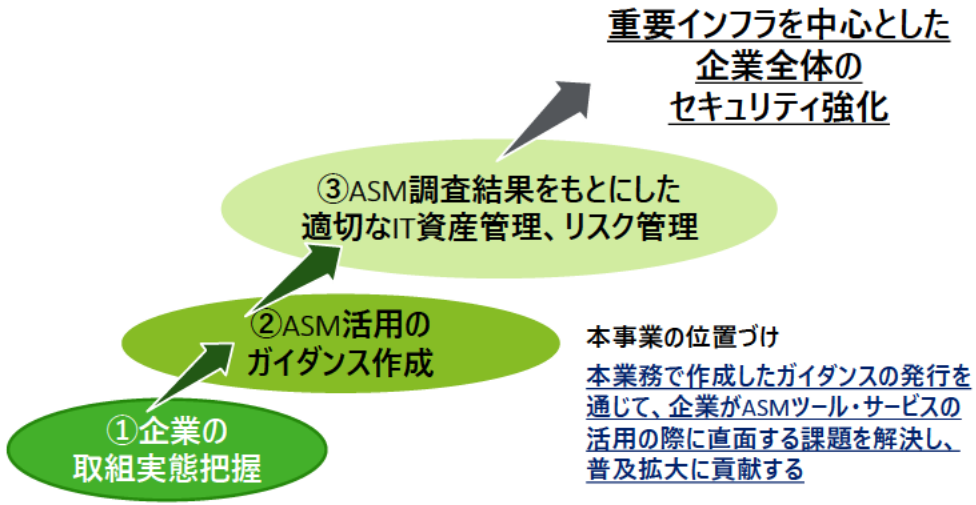
■ （**背景2**） 近年、企業などのネットワーク内に侵入しITシステム全体をダウンさせて金銭を要求する**「侵入型ランサムウェア*1攻撃」**が活発化し、さまざまな業種が攻撃対象となり、事業に大きく影響する被害事例が増加しています。この攻撃は「標的を決めてから弱点を探す」のではなく**「外部から見て弱点のある企業」を優先的に標的にする**、といわれています

■ （**背景3**） IT資産の適切な管理のためには、従来の「社内からの申告に基づく把握」では不十分であり、**外部から把握できる情報を利用**して、IT資産やリスクを洗い出し対処するような手法、中でも「攻撃者目線でどう見えているか」という観点で外部に公開されているIT資産の情報を収集・分析し、不正侵入経路となりうるポイントを把握し、適切な対処を行う”Attack Surface Management（ASM）”が注目されています

■ （**目的**） 本事業は、外部から把握できる情報を活用した適切な資産管理、リスク管理の**企業への普及拡大**のため、外部から把握できる情報を用いたツールやサービス活用の**企業における取組実態を明らかにする**とともに、ツールやサービスの特徴や活用方法について整理し、**ガイダンスを作成します**。また、ガイダンス案を踏まえて特定の企業に対して実際にツールやサービスを活用して調査を行い”**どのようにセキュリティ対策へ活用できるか**”**について検討**の上、検討結果をまとめます

■ （ゴール） 本事業を通じて作成するガイダンスおよびその他の活動によって、企業が外部から把握できる情報を利用して適切に資産管理を行う取り組みを実施する際に直面する**課題を解決し、取り組みが普及・拡大する流れを生み出す**こと

■ （あるべき姿） **自社が所有するIT資産を適切に把握、管理し起こり得るサイバー攻撃に備える**とともに、自社だけでなく**グループ企業やサプライチェーンなどの資産管理状況やサイバーリスクについても把握**、対処することなどによって、安心・安全で持続可能なサービス提供を産業一体となって推進する姿



*1 ：PCやサーバ内のデータを暗号化する不正ソフトウェア

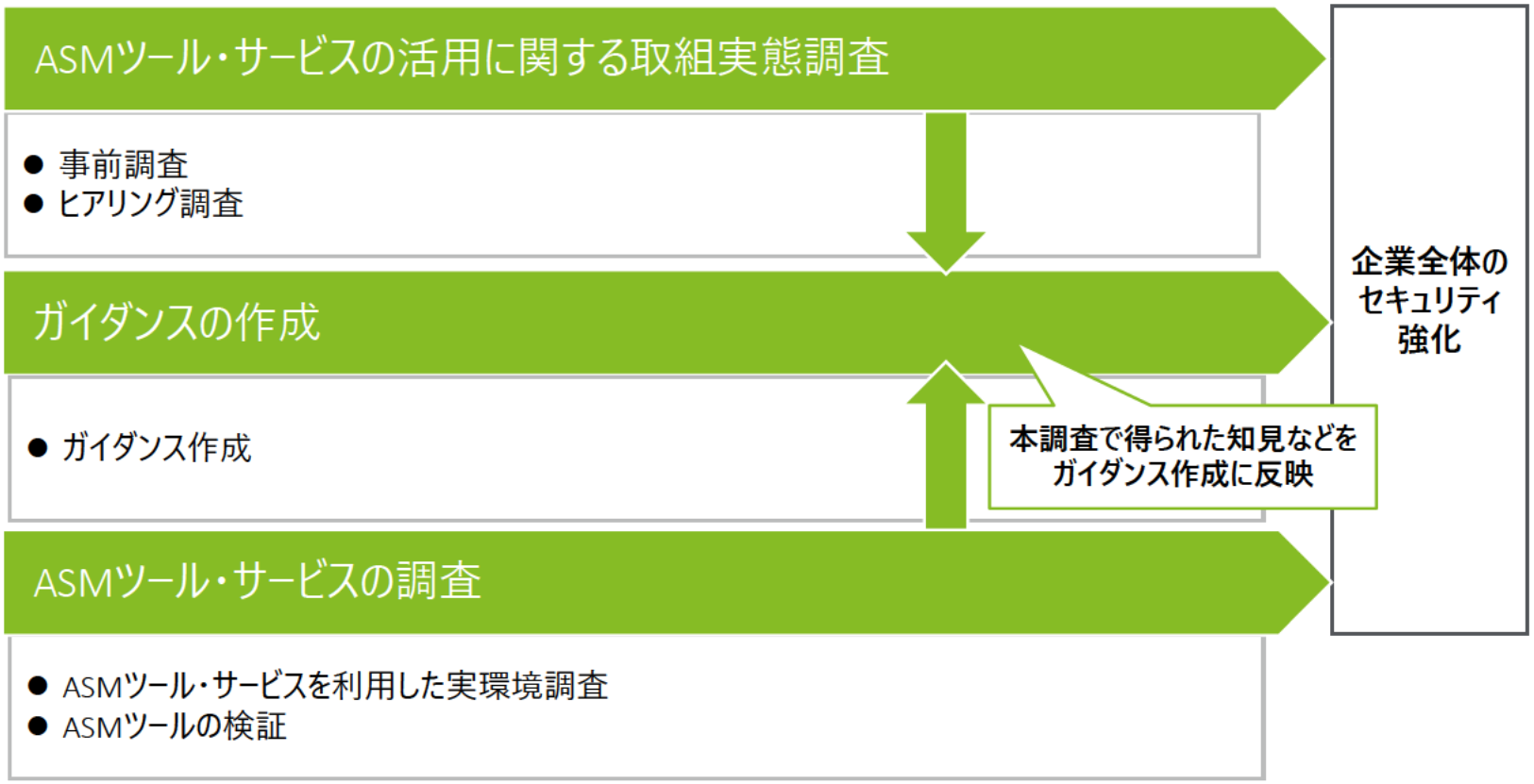
概要

Attack Surface Management(ASM)の企業における取組実態を明らかにし、ASMの活用促進に向け、ガイダンスを拡充することを目的とします

目的

本事業で作成したガイダンスの発行を通じて企業がASMツール・サービスの活用の際に直面する課題を解決し、企業全体のセキュリティ強化を実現すること

事業の全体像



2. ASMツール・サービスの活用に関する取組実態調査

2.1 取組実態調査の実施概要

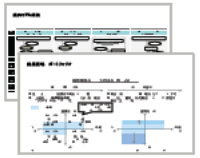
取組実態調査の実施概要

企業におけるASMの取組実態や抱える課題を深く理解するために、ASMツールなどについて公開情報をベースに事前調査を実施し、この結果を踏まえ、企業20社に対してヒアリング調査を行いました

事前調査

STEP 1 AS/ASMの定義

デスクトップサーチによって、**国内外のASMの定義について調査**し、本調査でのASMの意味を定義しました



STEP 2 ASMツール

デスクトップサーチやツールベンダへのヒアリングなどにより、**国内外のASMツールについて調査**し、まとめました

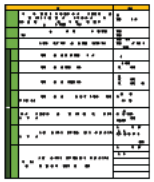
STEP 3 ASMサービス

デスクトップサーチやサービス企業へのヒアリングなどにより、**国内のASMサービスおよび国内におけるASM普及状況について調査**し、まとめました

ヒアリング調査

STEP 1 アンケート実施

240社に対しアンケート調査を実施し、65社から回答を回収し、分析しました



STEP 2 ヒアリング候補選定

ヒアリング候補はアンケートに回答のあった65社の中から、**ASM調査の実績がある企業を中心に20社を選定**しました

STEP 3 ヒアリング実施

選定した20社の企業情報やセキュリティ施策を調査し、**リモートで1h程度のヒアリングを実施**しました

STEP 4 結果取りまとめ

ヒアリング結果を分析し、**導入背景、利用状況、課題などの観点で**取りまとめました

2.2 事前調査

AS/ASMの定義に関する調査

Attack Surfaceについては、公的機関であるNISTなどによって定義されています

カテゴリ	機関・組織	説明内容（原文）	説明内容（日本語訳）	引用
Attack Surface	NIST	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.	システム、システムコンポーネント、または環境の境界上にあるポイントのセットで、攻撃者がそのシステム、コンポーネント、または環境に侵入したり、影響を与えたり、そこからデータを抽出したりする可能性があります	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
	CISA	The attack surface of an application represents the number of entry points exposed to a potential attacker of the software. The larger the attack surface, the larger the set of methods that can be used by an adversary to attack. "Definition: The set of ways in which an adversary can enter a system and potentially cause damage.	アプリケーションの攻撃対象領域は、ソフトウェアの潜在的な攻撃者に晒されるエントリポイントの数を表します。攻撃対象が大きければ大きいほど、攻撃者が攻撃するために使用することができる方法のセットが大きくなります 定義:攻撃者がシステムに侵入し、損害を与える可能性のある方法を指します	https://niccs.cisa.gov/cybersecurity-career-resources/glossary

AS/ASMの定義に関する調査

Attack Surfaceについては、公的機関であるNISTなどによって定義されています

カテゴリ	機関・組織	説明内容（原文）	説明内容（日本語訳）	引用
Attack Surface	OWASP	**Defining the Attack Surface of an Application** The Attack Surface describes all of the different points where an attacker could get into a system, and where they could get data out. The Attack Surface of an application is the sum of all paths for data/commands into and out of the application, and the code that protects these paths （including resource connection and authentication, authorization, activity logging, data validation and encoding） all valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and PII, and the code that protects these data （including encryption and checksums, access auditing, and data integrity and operational security controls）.	**アプリケーションの攻撃対象領域の定義** 攻撃対象領域とは、攻撃者がシステムに侵入したり、データを持ち出したりする可能性のあるすべての各種ポイントを表します アプリケーションのAttack Surface（AS）とはアプリケーションに入出力するデータ/コマンドのすべての経路と、これらの経路を保護するコード（リソース接続と認証、認可、アクティビティロギング、データ検証、エンコーディングを含む）の合計 、アプリケーションで使用するすべての重要なデータ（秘密と鍵、知的財産、重要ビジネスデータ、個人データ、PIIなど）とこれらのデータを保護するコード（暗号化とチェックサム、アクセス監査、データ整合性と運用セキュリティ制御など）のことを指します	https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

AS/ASMの定義に関する調査

Attack Surface Managementについては公的機関による定義はなく、一部の企業が使用しています

カテゴリ	機関・組織	定義（原文）	定義（日本語訳）	引用
Attack Surface Management (ASM)	IBM	Attack surface management （ASM） is the continuous discovery, analysis, remediation and monitoring of the cybersecurity vulnerabilities and potential attack vectors that make up an organization’s attack surface.	Attack Surface Management （ASM） は、組織の攻撃対象を構成するサイバーセキュリティの脆弱性と潜在的な攻撃ベクトルを継続的に検出、分析、修復、監視することです	https://www.ibm.com/topics/attack-surface-management
	SANS	Attack surface management （ASM） is an emerging category that aims to help organizations address these challenges by providing a continuous perspective of an organization's external attack surface.	Attack Surface Management （ASM） は、組織の外部の攻撃対象領域の継続的な視点を提供することによって、組織がこれらの課題に対処するのを支援することを目的とした新しいカテゴリです	https://www.sans.org/webcasts/guide-evaluating-attack-surface-management-116765/
External Attack Surface	Microsoft	An external attack surface is the entire area of an organization or system that is susceptible to an attack from an external source. An organization's attack surface is made up of all the points of access that an unauthorized person could use to enter their system. The larger your attack surface is, the harder it is to protect.	外部攻撃面とは、外部ソースからの攻撃の影響を受けやすい組織やシステムの領域全体のことです。組織の攻撃面は、承認されていないユーザーがシステムに入るために使用できるすべてのアクセスポイントで構成されます。攻撃面が大きいほど、保護が困難になります	https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/concept-easm

AS/ASMの定義に関する調査

本事業ではAttack Surface Managementを、「組織の外部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」と定義します

本事業での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。

出所：ASM（Attack Surface Management）導入ガイダンス 2章 2.1 ASMの定義

ASMツールに関する調査

国内外の主要なASMツール11種類について、公開情報をベースに各ツールの特徴などの調査を実施しました

#	ツール名	提供企業名	特徴	参考
1	Shodan	Shodan	10年以上ASMの領域で実績のあるツールです。ユーザーコミュニティも活発で、自動化できる機能も数多く提供しています	https://www.shodan.io/
2	Karma	00One	日本国内に流通するIoT機器の判別に特化した純国産の検索エンジンです。純国産のため、日本語検索もできます	https://www.00one.jp/karma/
3	Maltego	Maltego	IT資産の関係を示すグラフを作成するOSINTツール*1です。関係するドメイン名やサブドメインを洗い出す機能があり、未把握のIT資産を発見することも期待できます	https://www.maltego.com/
4	Censys	Censys	アメリカのミシガン大学の研究により開発された機器検索ツールです。クラウドとの連携ができ、オンプレミス以外のIT資産の継続的なリスク評価ができます	https://about.censys.io/
5	CyCognito	CyCognito	外部に公開されているIT資産を発見する機能に加え、脆弱性診断機能も具備しているツールです。継続的かつ自動的な脆弱性診断の運用もできます	https://www.cycognito.com/
6	Mandiant Attack Surface Management	Mandiant	外部に公開されているIT資産を発見する機能に加え、脆弱性診断機能も具備しているツールです。データソースやリスク可視化機能が充実しています	https://www.mandiant.jp/advantage/attack-surface-management

出所：各社HPや公開情報をもとに作成　*1：一般公開されている情報を収集・分析するツール

ASMツールに関する調査

国内外の主要なASMツール11種類について、公開情報をベースに各ツールの特徴などの調査を実施しました

#	ツール名	提供企業名	特徴	参考
7	Risk IQ	Microsoft	外部に公開しているIT資産の探索やフィッシングサイト、不正モバイルアプリケーションの検出ができるツールです。Microsoftに買収されたことによってAzure環境への統合も期待されています	https://www.microsoft.com/en-us/security/blog/2021/07/12/microsoft-to-acquire-riskiq-to-strengthen-cybersecurity-of-digital-transformation-and-hybrid-work/
8	Cortex Xpanse	PaloAlto	外部に公開されているIT資産の探索や継続的な監視ができるツールです。パロアルトネットワークス社の他のソリューションと連携させ、より高度なセキュリティオペレーションに活用することができます	https://www.paloaltonetworks.jp/cortex/cortex-xpanse
9	Tenable ASM	Tenable	外部に公開されているIT資産の探索や継続的な監視ができるツールです。Tenable.ioと連携し、継続的にリスク評価することができます	https://www.tenable.com/products/tenable-asm
10	Randori Platform	IBM	IBMに買収されたASMツールです。QRadarをはじめ、Tenable、Cortex XSOARなどとも連携することができます	https://www.ibm.com/products/randori-recon
11	Security Scorecard	Security Scorecard	企業のドメイン名から独自のアルゴリズムを用いて、10カテゴリにおいて5段階でリスクを評価するツールです。自社の評価値と業界平均値を比較することができます	https://securityscorecard.com/product/

出所：各社HPや公開情報をもとに作成

ASMツールに関する調査

ASMツールの調査にあたり、以下の機能・非機能の観点より違いを整理しました

観点	#	カテゴリ	項目
機能	1	スキャン機能	スキャン開始のために必要な情報は何か
	2	スキャン機能	どのような情報が検出可能か
	3	スキャン機能	誤検出はどの程度か
	4	スキャン機能	スキャン方法はどのようなものか、また、それらは開示されているか
	5	スキャン機能	スキャン対象に与える影響はどのようなものか
	6	スキャン機能	判定根拠となる情報は保存しているか
	7	評価	どのような方法で脆弱性を評価するのか
	8	他システムとの連携	どのようなものとの連携が可能か、APIは提供されているか
	9	レポート機能	どのような項目が出力可能か
	10	通知機能	どのようなトリガが設定可能か

ASMツールに関する調査

ASMツールの調査にあたり、以下の機能・非機能の観点より違いを整理しました

観点	#	カテゴリ	項目
非機能	1	データ保管	保管場所はどこか、期間はどのくらいか
	2	提供形態	クラウドサービス、ソフトウェア（もしくはレポート（情報））
	3	ライセンス形態	買い切り、サブスク、MSP向けライセンス など
	4	課金単位・価格	スキャン、ドメイン、ノードなど
	5	製品のセキュリティ	MFA、ユーザごとに閲覧範囲や操作を制限できるかなど
	6	第三者への調査	第三者への調査に対するベンダの考え方、留意点など
	7	UI/UX	言語、操作感など
	8	トライアル版の有無	安価もしくは無償でトライアル可能か
	9	各種上限	検索対象などに上限はあるか
	10	SLA	稼働率など
	11	サポート	どのようなサポートがあるか（ヘルプデスクの有無など）

ASMサービスに関する調査

ASMサービス提供企業5社より、サービスの概要や国内におけるASMの普及状況についてヒアリングしました

#	提供企業名	サービス名	概要・特徴
1	株式会社 日立ソリューションズ	CyCognito	CyCognitoを使ってお客様の資産の探索と脆弱性診断を実施するサービスです。検出された脆弱性に対してセキュリティアナリストが分かりやすく解説し、適切なセキュリティ対策を提案します。このサービスのポイントは、脆弱性の検出から対策完了までASMの全運用サイクルを支援できることです。CyCognitoの自動化・運用支援機能でASM開始に伴う新たな運用負荷を軽減し、さらに脆弱性とその対策状況を見える化します
2	NRIセキュアテクノロジーズ 株式会社	GR360	NRIセキュアが国内で運営しているサービスで、インターネット上のお客様に関連するIT資産を探索（ディスカバリ）・棚卸するサービスです。基本的なセキュリティ対策状況の調査も行い、その結果をレポートします。国内で多くの実績を持つほか、NRIセキュアが独自に開発したアルゴリズムとアナリストの分析により、高いディスカバリ性能を持つ（探索範囲の広さと誤検知の少なさを両立）ことが特徴です
3	株式会社 マクニカ	Mpression Cyber Security Service™ Attack Surface Management サービス	本社やグループ企業のドメイン名からOSINTを駆使し、お客様の外部公開資産の洗い出しとリスク評価を実施するサービスです。発見した資産の対処・是正に向けたアドバイス支援も行います。このサービスのポイントは、攻撃者と同様の視点を持ち、OSINTスペシャリストが人の目で調査するため、資産発見の網羅性が高い点です。また、日本の組織を狙う脅威や脆弱性に関する脅威動向を踏まえ、現実的なリスクに基づきいた対処助言も可能です
4	テクマトリックス 株式会社	アタックサーフェス マネジメントサービス	Cortex Xpanseを利用する企業に運用を支援するサービスです。Cortex Xpanseの結果を分析し、要対策ホストリストの作成や要対策ホストへの脆弱性診断の実施や、再評価も実施します
5	デロイト トーマツ サイバー 合同会社	侵害リスク評価サービス	お客様の使用しているインターネット接続機器について、公開情報を使用して攻撃者視点で外部から侵害されるリスクがあるか評価するサービスです。お客様からいただくのは調査対象の組織名のみであるため、お客様で把握していないドメイン名を洗い出すことが可能です。疑似的な攻撃コードを送信しないため、事前調整不要で運用中の機器に対して安全に調査が可能です

出所：サービス提供企業へのヒアリングおよびサービス資料をもとに作成

ASMサービスに関する調査

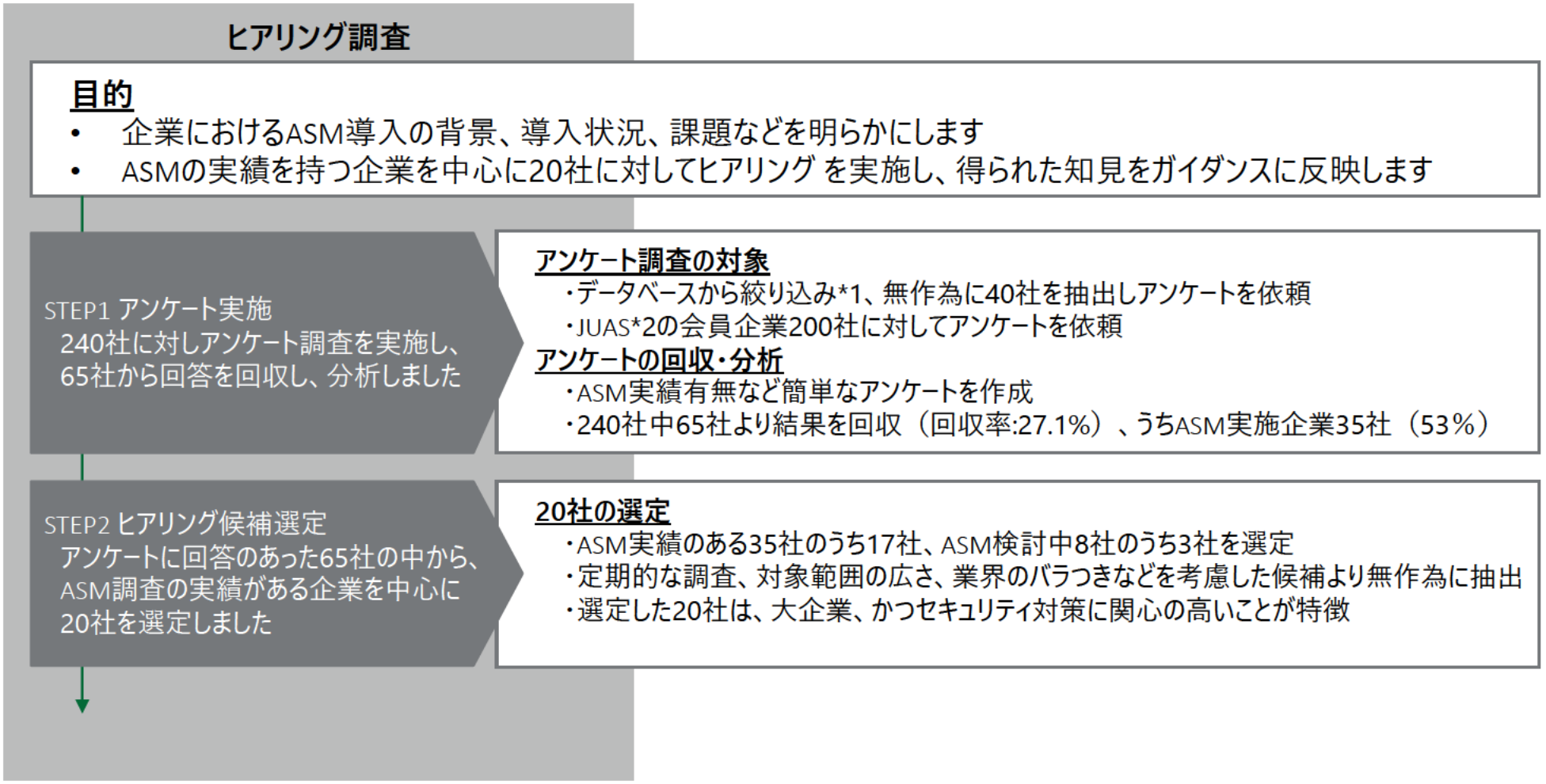
ASMサービス提供企業より普及状況をヒアリングした結果、製造業や金融業を中心に導入が進んでおり、幅広い業界から引き合いがある一方で、ASMに対する認知度が低いなどの課題も確認されました

国内における ASMの普及状況	• 海外のグループ企業や取引先の多い大手製造業を中心に、金融業、情報通信業などで導入が進んでいます
今後の見通し	• ASMの導入は着実に進展すると想定されます ✓ ランサムウェアなどのインシデントやサプライチェーンリスクの高まりなどから問い合わせ件数は1～2年で倍増しています ✓ 国内でASMツールを取り扱う代理店や新たにサービスを提供する企業は増加しています
海外と国内の ASMに対する認識の違い	• 国内と比較し、海外ではASMをテーマとしたカンファレンスなどが多く開催されています • ベンダーにより安全性が確認されたASMツールの脆弱性診断機能について、海外では一般的に使用されていますが、日本ではネガティブな反応を示す傾向が強く見られます
ASM導入の障壁	• ASMの効果などに対する認知度が低いです ✓ 感覚的に企業の約1/3はASMを認知していません • ASMで発見した脆弱性について、海外のグループ企業に是正させる際に長期間かかるケースがあります

2.3 ヒアリング調査

ヒアリング調査の流れ

企業におけるASM導入の背景、導入状況、課題などを明らかにするため、ASMの実績を持つ企業を中心に20社に対してヒアリングを実施し、得られた知見をガイダンスに反映しました



*1：データベース「D＆B Hoovers」から業種（ITサービス、重要インフラ、製造業）、従業員数などで絞り込み　*2：（一財）日本情報システムユーザー協会

ヒアリング調査の流れ

企業におけるASM導入の背景、導入状況、課題などを明らかにするため、ASMの実績を持つ企業を中心に20社に対してヒアリングを実施し、得られた知見をガイダンスに反映しました

ヒアリング調査

STEP3 ヒアリング実施
選定した20社の基礎情報やセキュリティ施策を調査し、リモートで1h程度のヒアリングを実施しました

事前準備
・選定した20社の従業員数、売上、海外拠点数、セキュリティ対策を公開情報より調査
・ヒアリング項目を検討（主要なセキュリティ施策、ASM導入の背景、導入状況、課題など）

ヒアリング
・情報システム・セキュリティ部門を対象に、リモートで1時間程度のヒアリングを実施

STEP4 ヒアリング結果の取りまとめ
ヒアリング結果を分析し、導入背景、利用状況、課題などの観点で取りまとめました

ヒアリング結果の分析
・全体傾向として、ASM導入の背景、導入目的、導入状況を分析
・ASM導入/運用の各フェーズにおける課題を抽出
・ASMの導入を検討する際に有用となる気づきやガイダンスへの要望を整理

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ためのツールやサービスの活用方法についてのガイダンス

アンケートの回収・分析

セキュリティ対策に関心の高い大企業65社より回収したアンケートを分析した結果、ASMは幅広い業界に導入されていると推測することができます

分野	業界	回答	ASM経験・予定		
			経験あり	経験なし・予定あり	経験なし・予定なし
重要インフラ 5分野（経産省管轄下）	クレカ	1	1（100%）	0	0
	電力	3	1（33%）	2	0
	ガス	4	1（25%）	1	2
	石油	-	-	-	-
	化学	7	3（42%）	1	3
重要インフラ 8分野	情報通信	5	1（20%）	1	3
	金融	4	3（75%）	1	0
	鉄道	2	1（50%）	0	1
	物流	1	0（0%）	0	1
	航空	1	1（100%）	0	0
	空港	-	-	-	-
	医療	-	-	-	-
	水道	-	-	-	-
その他分野	製造業	20	16（80%）	1	3
	サービス	5	1（20%）	1	3
	建設	4	2（50%）	2	0
	卸売	5	2（40%）	1	2
	保険	2	1（50%）	0	1
	その他	1	1（100%）	0	0
	合計	65	35（53%）	11	19

調査数は統計に必要なサンプル数を下回っており、傾向を表すものでありません

（参考）アンケート項目

以下の質問項目でアンケート調査を実施し、65社から回答を回収しました

#	対象者	質問項目	回答方法
1	全員	ASMという用語の認知	選択式 （よく知っている、言葉を聞いたことがある、全く知らない）
2		外部から見た観点のセキュリティ対策の実施有無	選択式 （実施している、実施していない）
3		実施経験	選択式 （実施経験あり、実施経験はないが予定あり、経験・予定なし）
4	実施経験あり	定期的実施の有無	選択式 （はい、いいえ）
5		実施形態	選択式（複数回答） （サービスを利用、自社ツールを利用、その他）
6		適用範囲	選択式（複数回答） （自社のみ、自社・グループ企業、自社・グループ企業・取引先、その他）
7		活用目的	選択式（複数回答） （IT資産の洗い出し、攻撃面の把握、セキュリティ対策の立案、その他）
8	実施経験なし	必要性	選択式 （必要である、あればいいと思う、必要ではない・できない、内容がわからない）
9		導入の課題	自由記載
10	全員	ヒアリング調査対応可否	選択式 （協力可能、協力可能想定だが説明要、条件付きで協力可能、ASMの知見はないが協力可能）

ヒアリング対象企業

アンケートの回答から、定期的なASM調査、対象範囲の広さ、業態のバラつきなどを考慮し、20社を選定しました。対象企業は、大企業、かつセキュリティ対策に関心の高いことが特徴といえます

#	業界	企業名	売上高	従業員規模	海外拠点数（海外子会社含む）	CSIRT有無
1	製造	部品A社	1,000億円~4,999億円	10,000人~	10~49	−
2	製造	鉄鋼B社	1兆円~	10,000人~	50~	○
3	製造	一般消費財C社	1兆円~	10,000人~	50~	○
4	製造	家電・機械D社	1,000億円~4,999億円	10,000人~	10~49	−
5	製造	鉄鋼E社	1兆円~	10,000人~	50~	○
6	製造	部品F社	5,000億円~9,999億円	10,000人~	10~49	−
7	製造	部品G社	1,000億円~4,999億円	10,000人~	10~49	○
8	製造	家電・機械H社	1兆円~	10,000人~	50~	−
9	製造	家電・機械I社	1,000億円~4,999億円	5,000人~9,999人	10~49	−
10	建設	建設J社	1兆円~	5,000人~9,999人	10~49	○
11	建設	建設K社	1,000億円~4,999億円	5,000人~9,999人	~10	○
12	建設	建設L社	1兆円~	5,000人~9,999人	~10	○
13	運輸	公共交通M社	1兆円~	10,000人~	なし	○
14	運輸	公共交通N社	1兆円~	10,000人~	50~	○
15	クレジットカード	クレジットカードO社	1,000億円~4,999億円	~4,999人	10~49	○
16	ガス	ガスP社	1,000億円~4,999億円	~4,999人	未記載	○
17	電力	電力Q社	~999億円	~4,999人	未記載	−
18	化学	一般消費財R社	1兆円~	10,000人~	10~49	○
19	卸	精密機器S社	5,000億円~9,999億円	~4,999人	10~49	○
20	保険	保険T社	1,000億円~4,999億円	~4,999人	なし	○

ヒアリング結果のサマリー

20社へのヒアリングから導入状況、導入の背景、導入目的、導入の評価、ASMツールなどの全体傾向分析し、各企業の抱える課題を抽出しました

全体傾向

導入状況

ASMを推進している企業の多くは1～2年前にASMを導入しており、現在PoCを実施している企業の大半は2年以内に運用フェーズへの移行を予定しています

導入の背景

大半の企業が「海外を含むグループ企業のサイバー攻撃耐性強化」をASM導入の理由にあげています。ASMの実施範囲について、ほとんどの企業がグループ企業までを対象としています

導入目的

ASMの主な利用目的は「脆弱性管理」「資産把握」が多く、副次的な目的として「ガバナンス強化」や「第三者目線での自社リスク評価の把握」があげられていることがASMの特徴といえます

導入の評価

ASMに取り組む15社は、当初の想定に対して期待通りの効果を得られていると評価しています

ASMツール

ASMツールとしてリスクレーティングが多く使用されていますが、昨今では運用に合致したツールを選択する傾向があります。ASMツールと脆弱性診断ツールの組み合わせを検討している企業もあります

ASM導入における課題

- ❑「グループ企業のガバナンス」
  ASM調査で把握した脆弱性をグループ企業に是正させる際に、グループ企業とのコミュニケーション、是正の技術的支援などで一定程度のリソースが必要となります
- ❑「IT資産を管理する組織特定」
  ASM調査で発見した未把握のIT資産について、グループ企業を含め、IT資産を管理する部署や管理者の特定に時間がかかります
- ❑「ASMツールの結果解釈」
  リスクレーティングツールの評価、解釈について苦労している企業が多くみられます
- ❑「ASMに対する認識」
  ASMに対する正しい認識が不足しており、特に脆弱性診断との関係を整理する必要があります
- ❑「ツール・サービスの選択」
  昨今では多様なASMツール・サービスを国内で調達することができるため、自社の業務に最も適したものを選択することが重要となります

（参考）ヒアリング内容

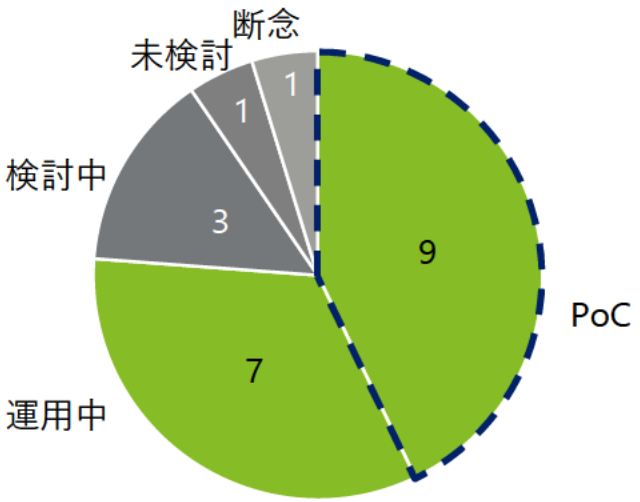
20社に対して、以下の項目についてヒアリングを実施しました

#	分野	質問項目
1	セキュリティ施策	セキュリティ推進体制
2		主要なセキュリティ施策
3		セキュリティポリシーの運用
4	ASM全般	導入の背景・目的
5		導入時期
6		対象範囲
7	ASMの導入・運用	導入のフェーズ
8		調査結果の活用方法
9		導入の課題
10		運用の課題
11	ガイダンス	ガイダンスへの要望

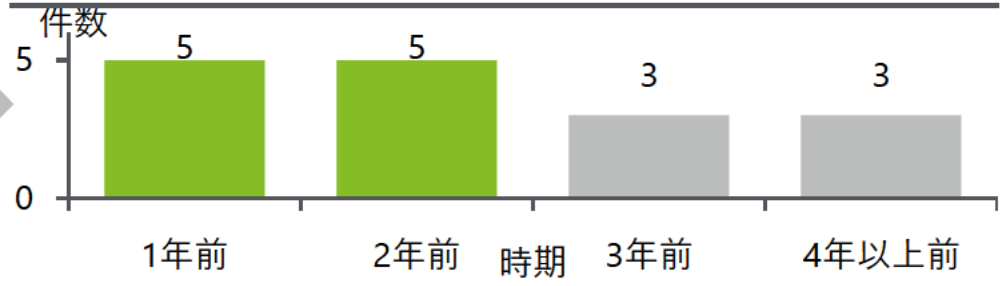
全体傾向　ASM導入状況

ASMを推進している企業の多くは1～2年前にASMを導入しており、現在PoCを実施している企業の大半は2年以内に運用フェーズへの移行を予定しています

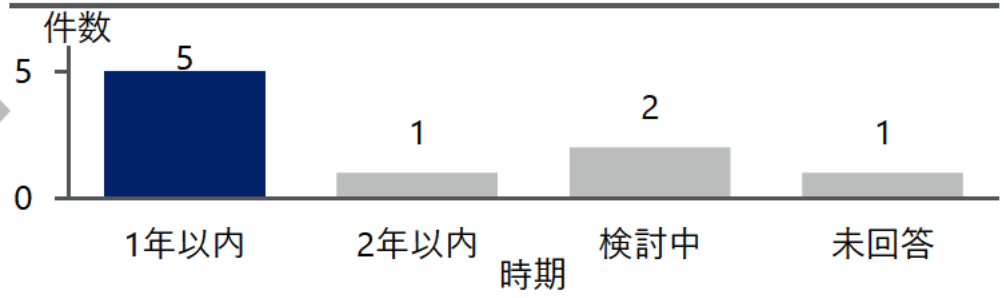
ヒアリングを実施した20社ASMの導入状況



ASMを導入した16社の導入時期



PoCを実施している9社の運用開始時期



■ ASMの導入フェーズではPoCが多く、導入時期も2年以内が大半であり、その過半数が2年以内に運用を開始する予定です。国内のASMの取り組みは始まったばかりであり、今後、サプライチェーンリスク対策として本格化すると推察できます

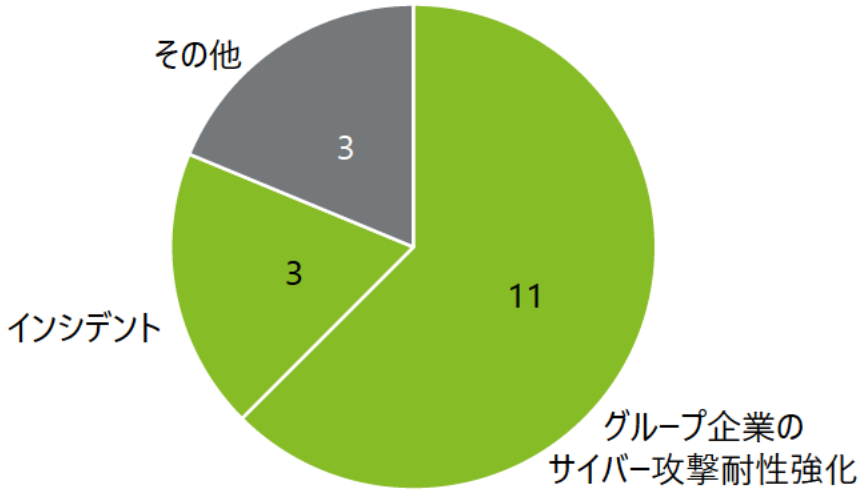
【コメントの抜粋】

- ✓ 昨年7月から100社以上のグループ会社を対象にスポットでASMを実施し、未把握のIT資産やセキュリティリスクの洗い出しを行った。2023年度より月1回以上の頻度で運用を開始する予定（鉄鋼B社）
- ✓ 2023年度、グループ全体の状況を把握し、レーティングが最低レベルの企業群の底上げのために本格的に運用する予定（鉄鋼E社）

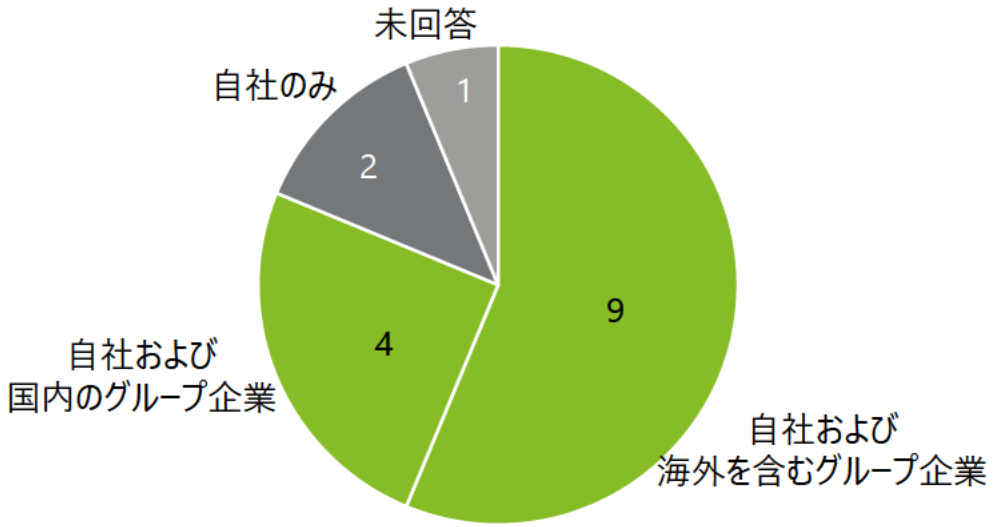
全体傾向　ASM導入の背景

大半の企業が「海外を含むグループ企業のサイバー攻撃耐性強化」をASM導入の理由にあげています。
ASMの実施範囲について、ほとんどの企業がグループ企業までを対象としています

ASMの導入理由（17社）



ASMの実施範囲（17社）



■ 大半の企業が、ASM導入の理由に「海外を含むグループ企業のサイバー攻撃耐性強化」「グループ企業のインシデント」をあげています。一部企業では、「取引先からの要請」「取引先からどのように見られるか」をあげていることもASMの特徴といえます

【コメントの抜粋】

- ✓ IT基盤が異なる海外グループ企業のセキュリティ対策の実施状況を確認するためにASMの導入を計画している

（建設J社）

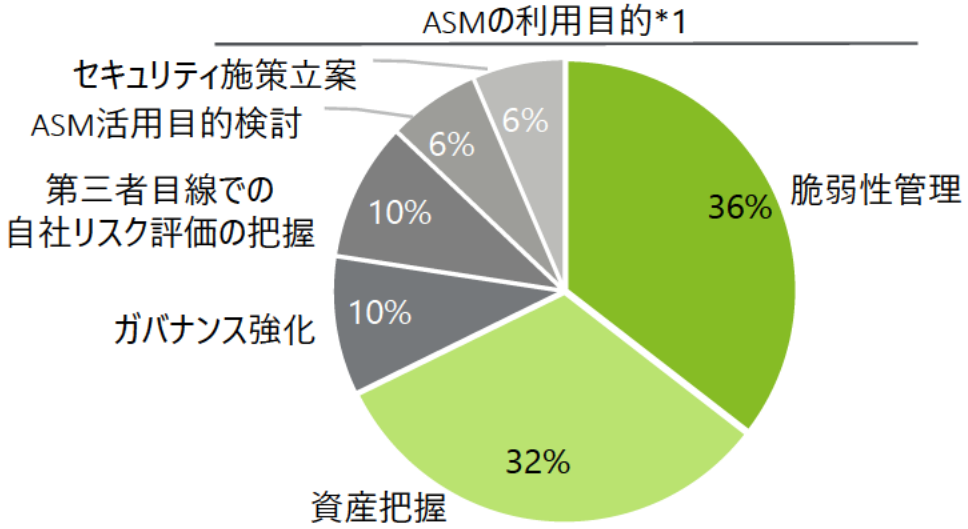
- ✓ 海外グループ企業でインシデントが発生したためASMを導入した。改めてグローバルでのIT資産の可視化できていないことが浮き彫りとなった

（家電・機械D社）

- ✓ 米国の取引先から勧められ、ASMを導入した（部品A社）

全体傾向　ASMの導入目的

ASMの主な利用目的は「脆弱性管理」「資産把握」が多く、副次的な目的として「ガバナンス強化」や「第三者目線での自社リスク評価の把握」があげられていることがASMの特徴といえます



■ 主となるASMの導入目的として、グループ企業を含め未把握のIT資産の洗い出しおよび脆弱性リスクの把握が大多数を占めています。一方で、グループ企業のガバナンス強化や、取引先や他社からのリスク評価を副次的な目的としている企業も一定数あります

【コメントの抜粋】

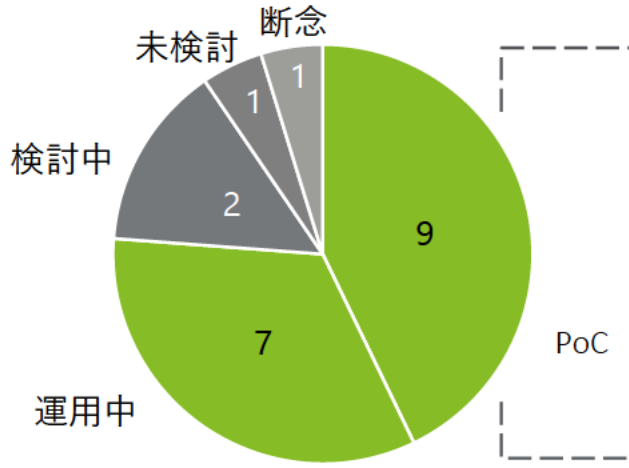
- ✓ 海外グループ企業の未把握なIT資産の洗い出しにASMを活用している（部品F社）
- ✓ ASMツールの導入により、グループ企業の外部から見えるIT資産の脆弱性対応状況のモニタリングがいつでも実施できるようになった。また、アンケート機能により、内部リスク評価も行っている（建設K社）
- ✓ 自社のセキュリティレベルに関して、他社との比較が容易にできることもASM導入の効果と考えている（公共交通N社）
- ✓ 取引先などの信頼獲得のために、自社のレーティングの評価を高める対策が必要と思う（一般消費財R社）

*1：複数回答

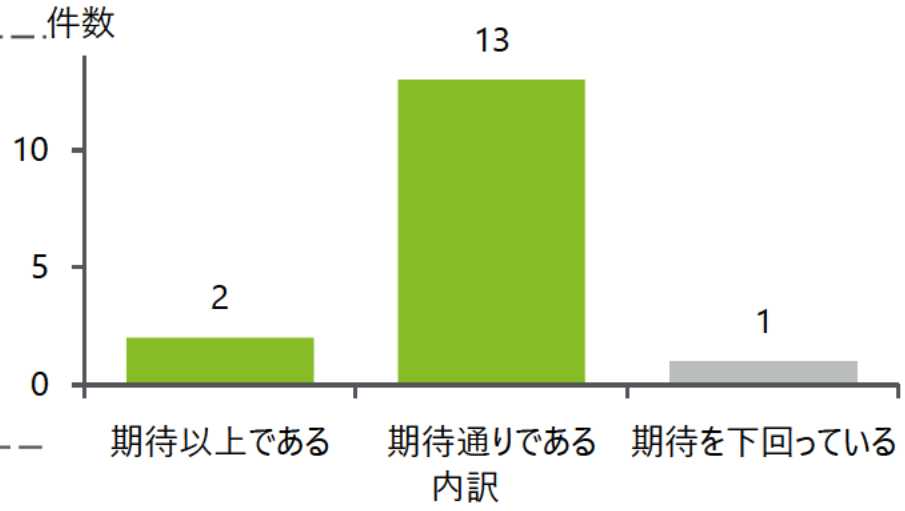
全体傾向　ASM導入の評価

ASMに取り組む15社は、当初の想定に対して期待通りの効果を得られていると評価しています

ヒアリングを実施した20社ASMの導入状況



ASMを運用中、PoCと回答した16社の導入評価



■ ASMを導入している企業の大半は「期待通り」以上とASMを評価しています、。ASMツール・サービスは未把握のIT資産を洗い出せることに加え、導入コストが安価、調査対象のカバレッジが広く、本番環境に影響を与えず短期間で導入できるなどの理由により選ばれていると分析しております

【コメントの抜粋】

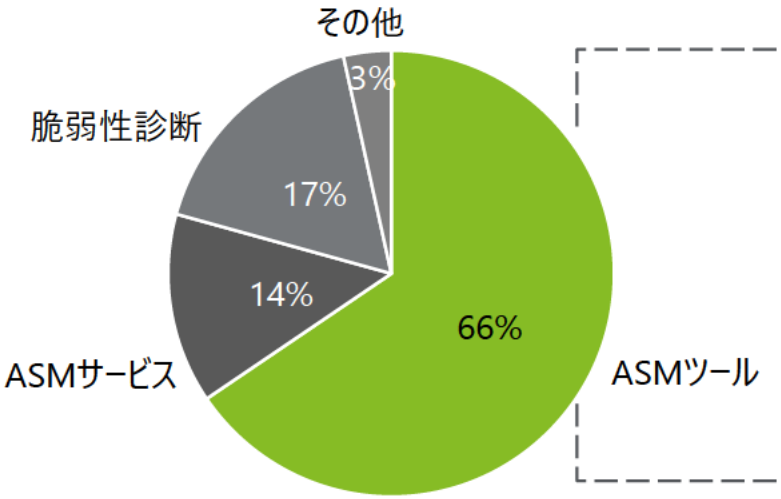
✓ レーティングスコアをベースとしたグループ企業のセキュリティ評価と是正を実施しており、期待以上の成果を出せている（一般消費財R社）

✓ 2022年度4QにASMサービスを発注した。本番環境に影響を与えず、1カ月程度で結果報告を受けることができ、金額もリーズナブルと感じている（ガスP社）

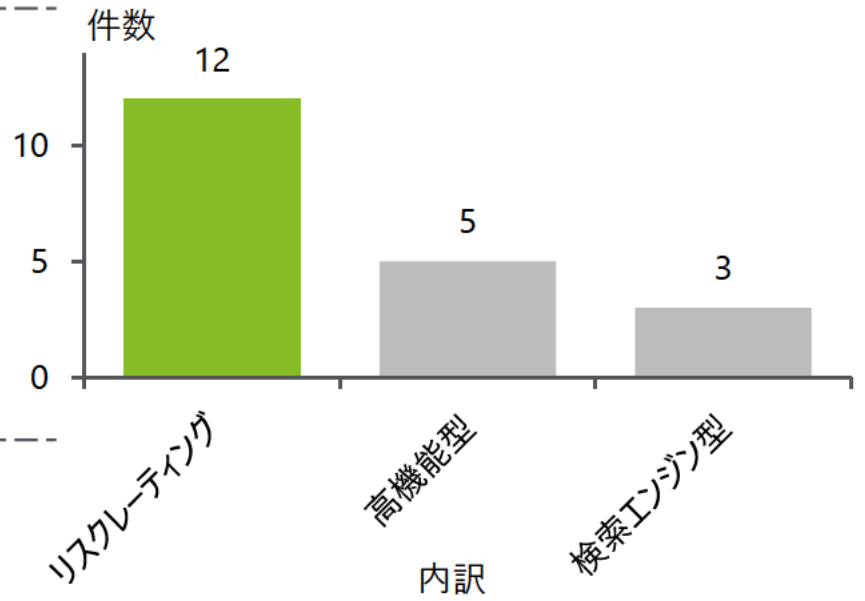
全体傾向　ASMツール（1/2）

ASMツールとしてリスクレーティングが多く使用されていますが、昨今では運用に合致したツールを選択する傾向があります。ASMツールと脆弱性診断ツールの組み合わせを検討している企業もあります

ASMツール・サービスの傾向*1



ASMツールの内訳*1



■ リスクレーティングツール*2が多く利用される理由として、国内ではASMツールの先駆けとして4～5年前から代理店が取り扱いはじめていること、知名度の高さ、対象範囲のカバレージの広さなどがあげられます

【コメントの抜粋】

✓ 導入当時はリスクレーティングツールしか選択肢がなく検証を実施、そのまま継続的に運用している　（公共交通N社）

✓ 数字でのリスク評価が出るので、経営幹部へ説明がしやすく説得力がある　（一般消費財R社）

*1：複数回答　*2：攻撃リスクを分析、定量評価しスコア（数値）として表示するASMツール

全体傾向　ASMツール（2/2）

ASMツールとしてリスクレーティングが多く使用されていますが、昨今では運用に合致したツールを選択する傾向があります。ASMツールと脆弱性診断ツールの組み合わせを検討している企業もあります

■ ASMツールと脆弱性診断ツールの組み合わせによる脆弱性管理を目指す企業や脆弱性診断機能を持つASMツールを検討する企業もあります

【コメントの抜粋】

- ✓ 社内IT資産については、脆弱性診断ツールでの月次調査や年1回のペネトレーションテストを実施している（建設K社）
- ✓ ASMサービスの利用に加え、脆弱性診断機能を持つASMツールのPoCを実施している（クレジットカードO社）

■ ASMサービスは事前準備が不要で、短期間で調査結果が得られるため、一旦ASMサービスで現状を把握し、結果踏まえてツール・サービスの運用方法を検討する企業も一定数あります

【コメントの抜粋】

- ✓ 初回はASMサービスでIT資産の洗い出しを行い、結果を踏まえ運用を検討する。定常的な運用はASMツールを活用する予定（建設J社）
- ✓ ASMサービスにより、低コストで迅速に未把握なIT資産の脆弱性を洗い出すことができた（家電・機械D社）

（参考） ヒアリングした20社が利用または検討しているツール・サービス

項目	分類	名称
ASMツール	リスクレーティング	SecurityScorecard
		Bitsight
		Panorays
	高機能型	ULTRA RED
		CyberPion
		RiskIQ
		Tenable.asm
		DECYFIR
	検索エンジン型	Shodan
		Maltego
ASMサービス		OSINT診断
		GR360
		Mpression Cyber Security Service™ Attack Surface Managementサービス
		侵害リスク評価サービス
脆弱性診断	ツール	Tenable.io
	サービス	タイガーチーム
その他		DarkBeast

ASM導入における課題　グループ企業のガバナンス

ASM調査で把握した脆弱性をグループ企業に是正させる際に、グループ企業とのコミュニケーション、是正の技術的支援などで一定程度のリソースが必要となります

課題

グループ企業のガバナンス

ASM調査をグループ企業まで実施する企業が多く、発見した未把握なIT資産の脆弱性の可能性について、脆弱性の確認および是正のため、グループ企業とのコミュニケーションが必要となり、一定程度の人的リソースが必要となります。また、是正にあたっては、特に規模が小さくセキュリティリソースが不足している企業への支援も検討する必要があります

課題への対処に関する考察

- 実施計画策定の段階より、グループ企業への脆弱性対応の運用を想定した要員計画を立案することが必要です。PoCの段階で具体的な運用方法、必要となる作業の洗い出し、要員計画の立案、外部委託の検討などを行うことも効果的といえます
- 発見されたIT資産の脆弱性に関して、優先順位付けを行い、リスクが高いものから対応を行うことも重要です

ヒアリング結果

- ASMに取り組みたいが、自社のシステム構成熟知し脆弱性対応の知見を持つ人材が不足している。是正対応を含めた運用が難しい（鉄鋼B社）
- 現在のPoCの人員体制では、グループ全体の運用は難しい。別部隊への移管などを検討している（鉄鋼E社）
- ツールの定常運用のための人的リソースの確保が課題である（家電・機械D社）
- ASMの運用では人的リソース不足が課題。脆弱性の是正については情報子会社へ外部委託する方向で検討している（公共交通N社）

ASM導入における課題　IT資産を管理する組織特定

ASM調査で発見した未把握のIT資産について、グループ企業を含め、IT資産を管理する部署や管理者の特定に時間がかかります

課題

IT資産を管理する組織特定

ASM調査で発見された脆弱性の可能性のある未把握なIT資産について、管理している部署を特定するのに時間がかかります。特に、発見したIT資産が海外のグループ企業所有の場合、想定以上に時間をかかるため留意する必要があります

課題への対処に関する考察

- 発見されたIT資産を管理する部署を早期に特定するためには、事業部門やグループ企業と定常的に連絡を取れる仕組みを構築しておく必要があります
- 特に海外のグループ企業では、利用しているセキュリティポリシーが異なっていたりIT基盤が統一されていないケースも多いため、グループにおけるセキュリティガバナンス強化の観点からもコミュニケーションを取れる体制を構築することが重要です

ヒアリング結果

- 海外グループ企業で未把握のIT資産が発見された場合、見つかったIT資産の管理者の特定と連絡に時間がかかる。その分是正対応も遅れてしまう

  （一般消費財R社）

- グループ企業で未把握のIT資産が発見された場合、管理者の特定に時間がかかり、セキュリティリスクの是正に時間を要する傾向がある　（鉄鋼B社）

- ASMで発見されたIT資産・脆弱性がどの組織・部門のものか、ツールの結果に表れないため組織の特定が難しい　（部品F社）

ASM導入における課題　ASMツールの結果解釈

リスクレーティングツールの評価、解釈について苦労している企業が多くみられます

課題

ASMツールの結果解釈

リスクレーティングツールの評価の捉え方について、低リスクの脆弱性が多数ある場合にもリスク評価が高くなるなど、ツールごとに特性があり、結果の評価の解釈に苦労している企業が多く見られています

課題への対処に関する考察

- OSINT情報をベースにIT資産の脆弱性を機械的に判断するというASMツールの特徴を踏まえたうえで、発見された脆弱性の実態調査を実施するなど脆弱性の有無を改めて確認し、結果を評価することが重要です

ヒアリング結果

- ツールによる評価結果には侵害を受けるリスクに直結しないものが多数含まれるため、必ずしも現状の組織のセキュリティ態勢を評価できるものではないと考えている　（建設L社）
- 自社と無関係のIT資産もリスク評価されてしまうケースがあり、評価が本来の評価より低くなっていることがある　（部品G社）
- 具体的に何点であれば良いのか判断がついておらず、スコアが出た後の対策が難しい　（家電・機械I社）

ASM導入における課題　ASMに対する認識

ASMに対する正しい認識が不足しており、特に脆弱性診断との関係を整理する必要があります

課題

ASMに対する認識

ASMに対する正しい認識が不足しています。特に、資産管理、脆弱性管理との関係、脆弱性診断との違いなど、OSINT情報をベースに脆弱性を判断するASMの限界などを正しく理解することが重要です

課題への対処に関する考察

- ASMは、OSINT情報をベースに外部に公開されているIT資産を発見するということが大きな特徴です。本調査で作成するガイダンスにて、資産管理、脆弱性管理との関係、脆弱性診断との違いを明確にしています

ヒアリング結果

- 今回のヒアリングで改めてASMを理解し、自社の取り組みがASMで目指す方向と整合することを認識した　（家電・機械H社）
- 現在、定期的な脆弱性診断に加え、ASMのPoCを実施している。ASMを脆弱性診断の代替として検討している　（鉄鋼E社）
- ASMの定義と対策などを実施する範囲が不明瞭で、どこまで対策を実施するかを検討しながらPoCを進めている　（公共交通N社）
- ASMを正確に理解できておらず、ASMと脆弱性診断を併用して運用するイメージが掴めていない　（建設J社）

ASM導入における課題　ツール・サービスの選択

昨今では多様なASMツール・サービスを国内で調達することができるため、自社の業務に最も適したものを選択することが重要となります

課題

ツール・サービスの選択

昨今では多様なASMツールやサービスが多く提供され、国内でも調達できる環境が整ってきています。ASM導入の目的を明確化したうえで、自社の業務に最も適したツール・サービスを選択することが重要です

課題への対処に関する考察

- ASMを導入する際には、導入の目的、対象範囲、既存の脆弱性診断業務とのすみ分けについて整理を行った上で、運用を検討し、最適なツール・サービスを選択することが重要です
- ASMツール・サービスは、本番環境にほとんど影響を与えることなく低コストで現状の攻撃面における脆弱性の可能性を把握することができるため、PoCで現状を把握しながら、運用方法の検討や最適なASMツール・サービスを選択する方法も有効です

ヒアリング結果

- 自社に合うASMツールやサービスを比較検討のために、現在、ASMツールベンダ複数社（5社以上）からヒアリングを実施している（鉄鋼B社）
- 無料お試しサービスなどでいくつかツールを利用して、自社で運用できるツールを検討している（建設J社）
- 運用に合ったツールを2つPoCした。レポート機能が充実しており、複数の取引先でも使用されているツールを選定した（鉄鋼E社）

ヒアリング内の特筆すべきコメント

一部の企業からASMの導入の留意点や運用のポイント、いただいた特筆すべきコメントを紹介します

ASMの使用時の留意点	ASMは容易に他社を調査することができるため、攻撃面の脆弱性について取引先から指摘されるケース、競合他社と自社のリスク評価を比較するケース、重要取引先のリスクを評価するケースなど、「第三者目線で自社（他社）のリスクを評価」している企業が一定数あります。一方で、多くの企業はASM調査結果が取引条件になることを警戒しています	第三者による他社を評価する際の留意点をガイダンスに記載
ASMの高度な使用方法	複数のASMツールを業務で切り分けて使用している企業は1社だけ（未把握の資産の探索とメール未達のトラブルシューティングで使い分けている）で、他のセキュリティ関連ツールと連携している企業はありませんでした	高度なASM利用のユースケースを本報告書の4.3に記載
法的解釈	脆弱性診断機能を持つASMツールで他社を調査する際に、不正アクセス禁止法など法制度への抵触について漠然と不安を持っている企業が多いです	法的解釈についてはガイダンスに記載
脆弱性に対する関心	海外の大手クラウドサービスはDDoS攻撃以外の脆弱性診断を受容していますが、国内の一部のISPなどは脆弱性に関する指摘に対してすらネガティブな反応を示しています。攻撃面の脆弱性に対する関心を国内全体で高めなければ、先進国の中で日本が攻撃しやすい国とみなされる可能性があります	本調査で作成したガイダンスを周知していくことが重要

3. ガイダンスの作成

3.1 ガイダンスの概要

ガイダンスの概要

ASMを企業へ普及させるためにASMの定義や活用方法などを解説するガイダンスを作成しました

ガイダンスの目的	近年猛威を奮っているランサムウェア対策の一つであるASMについて、企業に広く普及させることを目的にガイダンスを作成しています。ASMが認知されてつつある現状を踏まえ、ASMの基礎的事項、導入の効果、ツールやサービスの特徴、活用する際に考慮すべき事項、取り組みの事例について記載しています
想定読者	経営層や管理者層を中心に自社のセキュリティ戦略を推進する人 ■ CIOやCISOなどの情報セキュリティ戦略に責任を持つ経営層 ■ 情報システム、情報セキュリティ部門でセキュリティ向上施策、体制、ツールを検討する管理者など
読了後の姿・レベル	ASMの特徴を理解し、自社のセキュリティ対策の強化としてASM導入のイメージを掴む ■ 脆弱性管理の中のASMの位置づけ、特徴、限界を理解できる ■ ASMツール・サービスの機能について理解できる ■ ASM導入の留意点について理解し、実施計画を検討できる

3.2 ガイダンス

ガイダンスの目次とポイント

取組実態調査やASMツール・サービスの調査を通じて得られた知見を踏まえ、ASMの定義やプロセス、脆弱性管理との関係性や活用にあたって注意すべき事項、事例について記載しました

章		節	ポイント
1	はじめに	はじめに	• 国内で発生したサイバー攻撃の事例や、ASMに類するパケットの増加が観測されていることなどを取り上げ、ASMに取り組む意義を訴えています
2	ASM（Attack Surface Management）とは	ASMの定義 ASMのプロセス ASMの特徴 ASMと脆弱性管理	• 海外含め、ASMの解釈が乱立しているなか、国内ではじめてASMの定義およびそのプロセスを打ち出しています • 脆弱性管理との関係および脆弱性診断の違いを明らかにすることで、ASMでできること・できないことを整理しています • ASMと脆弱性診断を混同して対策を誤ってしまうことを未然に防ぐことが期待されます
3	ASMの実施	実施計画の策定 攻撃面の調査と把握 継続的な対応	• ASMツール・サービスの調査を通じて得た知見を踏まえ、ASMツールが標準的に具備している機能を整理し、分かりやすく紹介しています • 取組実態調査およびASMツール・サービスの調査を通じて得た知見をツール利用にあたって注意すべき事項としてまとめています
4	事例	事例-A 事例-B	• 読者に活用のイメージをより明確に持ってもらえるよう、取組実態調査の結果を事例として取り上げ、活用方法の示唆を与えています
5	おわりに	おわりに	• 1-4章で論じた内容およびASMを実施するうえで参考となり得る情報をまとめています
6	付録	用語集 参考情報	

ASM（Attack Surface Management）とは

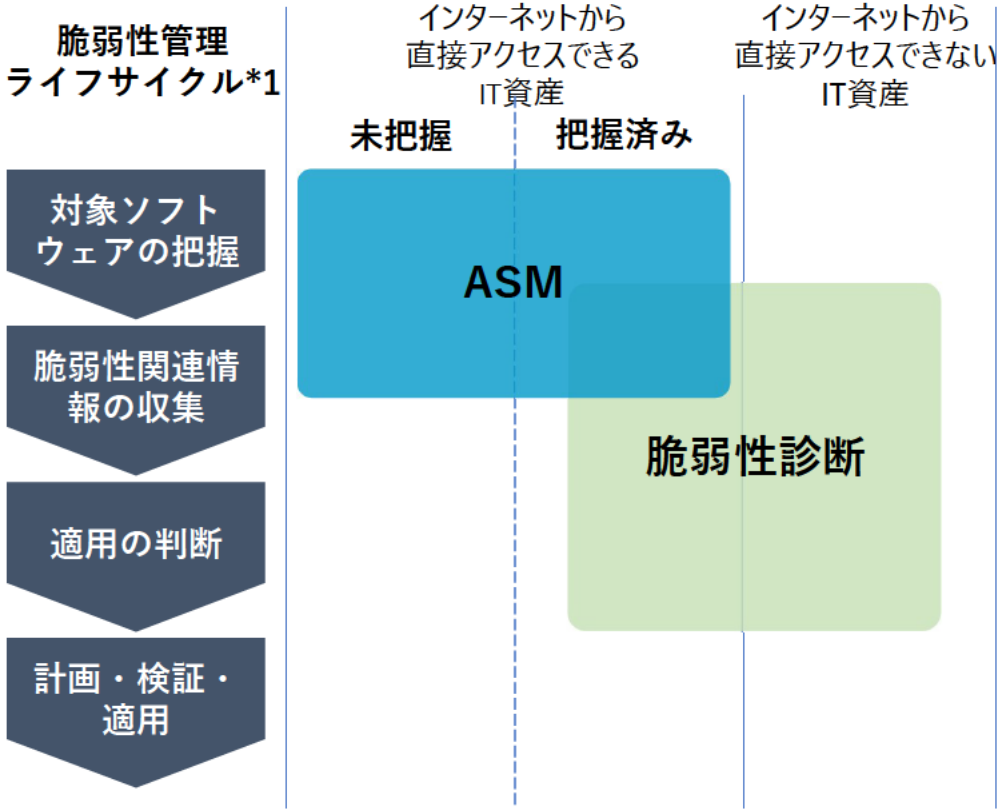
本ガイダンスではASMを「組織の外部（インターネット）からアクセス可能なIT資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス」と定義しました

ASMの定義

- 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
- 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

ASMのプロセス	詳細
（1）攻撃面の発見	企業で保有または管理するIPアドレス・ホスト名の発見
（2）攻撃面の情報収集	攻撃面の情報収集 例：OS、ソフトウェア、バージョン情報、オープンなポート番号など
（3）攻撃面のリスク評価	（2）で収集した情報をもとにしたリスク評価
リスクへの対応	脆弱性管理と同様の対応 例：パッチ適用（リスクの低減）、対策見送り（リスクの受容）など

ASMと脆弱性診断の違い



出所： ASM（Attack Surface Management）導入ガイダンス
*1：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

4. ASMツール・サービスの調査

4.1 ASMツール・サービスの調査の概要

ASMツール・サービスの調査の概要

3企業・団体の実環境に対して複数のASMツール・サービスを利用した調査を実施しました。併せてASMツールの機能や高度な利用方法の検証を行いました

ASMツール・サービスを利用した実環境調査

STEP 1 調査手法の決定

調査に利用するツール、調査の流れ、リスク評価基準、レポート・報告形式、その他調査手法の詳細を決定しました

STEP 2 調査範囲の決定

事前準備で洗い出したドメインリスト・IPアドレスリストをもとに、**各調査対象との協議の上調査範囲を決定**しました

STEP 3 調査結果取りまとめ

調査範囲に対して複数のASMツールを利用し調査を実施し、得られた調査の結果を取りまとめました

STEP 4 結果報告

報告書を作成し、**調査対象企業・団体の業務担当者向けに調査報告会を実施**し、報告に対する評価・フィードバックをいただきました

ASMツールの検証

STEP 1 評価・検証項目の決定

ASMツールを評価するための**評価・検証項目**を決定しました

STEP 2 ツールの機能調査

各ツールごとの**一般機能全般、ダッシュボード・モニタリング機能、高度な利用の可能性**について調査しました

STEP 3 高度な利用方法の検証

さらに、ASMツールの高度な利用が想定される3つのユースケースのシナリオを想定し、**自作のスクリプトの作成やツールの組み合わせによる検証**を行いました

4.2 ASMツール・サービスを利用した実環境調査

調査手法の決定　調査の流れ

3企業・団体に対する調査は、5つのツール・サービスを利用し、①ドメイン名の洗い出し ②調査対象機器の特定 ③情報収集 ④リスク評価の順に実施しました

今回利用したツール		
分類	ツール名	備考
検索エンジン型	Shodan	侵害リスク評価サービス内で利用
	Karma	–
	Maltego	–
高機能型	CyCognito	日立ソリューションズのサービスを併用
	Mandiant ASM	–

フェーズ区分	調査の流れ
① ドメイン名の洗い出し	➢ 調査対象企業・団体のドメイン名および組織名をもとに、紐づくドメイン名を洗い出し
② 調査対象機器の特定	➢ FQDN、IPアドレス、Webアプリケーション、証明書情報など、機器の情報を特定
③ 情報収集	➢ 各ツールを使用し機器情報を収集するとともに、通常のWebアクセスによりコンテンツの情報を取得 ➢ 一部企業・団体に対して、Mandiant ASMおよびCyCognitoの脆弱性診断機能を試用し、情報を収集
④ リスク評価	➢ 収集した情報をもとに各機器のリスクを評価

調査手法の決定　リスク評価基準

各ASMツール・サービスで使用されているリスク評価基準に微妙な違いが見られたため、本調査においては侵害リスク評価サービスの基準をもとに各機器が侵害されるリスクを評価しました

	侵害リスク評価サービス		CyCognito*1		Mandiant ASM*2	
レベル	リスク	概要	Severity	概要	Severity	概要
4	Critical	■ 悪用される可能性の高い問題が存在する	Critical	■ 直ちに対応すべきである問題が存在する	Critical	■ 攻撃者に悪用されると継続的な横方向への移動などが成功する恐れのある問題が存在する
3	High	■ 悪用される可能性のある問題が存在する	High	■ 速やかに対応することを推奨する	High	■ 攻撃者に悪用されると継続的または横方向の移動や未認証のアクションが実行される恐れのある問題が存在する
2	Medium	■ 攻撃者にとってヒントとなる情報が公開されているなど、注意すべき事項が存在する	Medium	■ より深刻な問題点への対処が終わってから対応を検討することを推奨する	Medium	■ 脆弱であるものの、MFAや追加アクセスの要件によってリスクが相殺される問題が存在する
1	Low	■ ほぼ問題がない	Low	■ 対応を行う必要性は低い	Low	■ 脆弱性・設定ミスなどがあるものの、直接的なリスクはない
0	Very Low	■ 問題点を確認できない	–	–	Informational	■ セキュリティ姿勢を改善するための継続的な取り組みの中で対処する必要がある

*1：CyCognito Knowledge Base　*2：Mandiant Advantage Documentation

調査結果取りまとめ

3企業・団体に向けた調査を行い、リスク評価結果の概要やリスク対応案などを記載したASMツール調査結果報告書および脆弱性情報一覧を作成しました

最終成果物

「ASMツール調査結果報告書」

別紙：脆弱性情報一覧
（エクセルファイル）

#	タイトル	内容
1	エグゼクティブ・サマリー	➢ 調査結果の概要 ➢ 改善の方向性
2	本事業の概要	➢ 本事業の概要・全体像 ➢ 本調査で利用したツール一覧
3	ASMツールを利用した調査の概要	➢ ASMとは ➢ 本調査の流れ・全体像
4	調査結果	➢ 調査結果（まとめ） ➢ リスクがHigh以上の機器の詳細情報
付録	問題点の深刻度と機器種別の判定	➢ 問題点の深刻度 ➢ 機器種別
付録	問題点の類型と対策	➢ 問題点類型別問題点の内容・対策の手順例　など
付録	各ツールの調査結果	➢ 調査範囲の差分による調査結果の差異に関する説明 ➢ 5つのツール・サービスの調査結果の概要

#	タイトル	内容
別紙	脆弱性情報一覧（エクセルファイル）	➢ 発見した脆弱性情報の一覧 ➢ 特定した全機器情報の一覧 ➢ 各ツールのアウトプット

結果報告

3企業・団体を調査した結果、すべての企業・団体でリスクHigh以上の機器が発見され、パッチ適用や脆弱性管理状況の確認を推奨しました

項目	事業者A	事業者B	事業者C
特定した機器の件数	2,027件	9,157件	92件
リスクHigh以上の機器	14件	44件	6件
特定したVPN機器	14件	51件	0件
利用したツール	Shodan、Karma、Maltego、CyCognito（探索）	Shodan、Karma、Maltego、CyCognito（探索）、Mandiant ASM	Shodan、Karma、Maltego、CyCognito（探索・診断）、Mandiant ASM
調査結果の概要	➢ リスクCriticalに該当する脆弱性は7件（OpenSSL、Apache HTTP Serverなどの深刻な脆弱性がある恐れ） ➢ 一部の機器に攻撃コードが公開されている脆弱性が推測されました ➢ 機器の脆弱性管理の状況を確認することを推奨しました	➢ リスクCriticalに該当する脆弱性は24件（PHP、Apache HTTP Serverなどの深刻な脆弱性がある恐れ） ➢ 一部の機器に攻撃コードが公開されている脆弱性が推測されました ➢ 機器の管理状況の確認およびパッチ適用などの実施を推奨しました	➢ リスクCriticalに該当する脆弱性は3件（OpenSSL、PHPの深刻な脆弱性がある恐れ） ➢ eコマース用のCMSが稼働する機器に複数の脆弱性が推測されました ➢ 機器の脆弱性管理の状況を確認することを推奨しました

結果報告

3企業・団体から調査結果と今後の利用に関するフィードバックをいただきました

分類	項目	フィードバック
調査結果	未把握だったIT資産の発見	■ 未把握のIT資産が発見された 本調査前に試験的に調査したときに把握していたIT資産が多かったものの、一部新しい発見もあった（事業者B）
	未把握だった脆弱性の発見	■ 未把握の脆弱性が発見された 各部署が運用するIT資産で脆弱性が発見されており、今回の結果を活用して対応につなげたい（事業者A）
	評価基準	■ 5段階によるリスク評価は、納得感があった 事業継続の影響度なども考慮する必要がある（事業者B） CVSSではなく、CISAのKEVを参照し優先順位付けを行うことを検討している（事業者C）
	推奨する対策の例示	■ 有効である 暫定対処と恒久対処を分けられているとより良かった（事業者B）
今後の利用	ツール・サービスの活用	■ 今後もASMツール・サービスを活用したい（事業者A、B、C）
	課題	■ 結果の活用 今回見つかった脆弱性について、精査を行った上で事業部門に説明する必要がある。説明の仕方に工夫が必要である（事業者B） 組織内部でどう活用していくか、今後検討する必要がある（事業者C） ■ リソースの確保と知見の獲得 ASMを運用するためには、調査結果を活用するリソースの確保とASMツールのノウハウの獲得が必要である（事業者A）

4.3 ASMツールの検証

評価・検証項目の決定

実環境調査で使用したツールに関して、機能・非機能の観点から検証項目を整理しました

今回検証したツール		
分類	ツール名	提供企業名
検索エンジン型	Shodan	Shodan
	Karma	00One
	Maltego	Maltego
高機能型	CyCognito	Cycognito
	Mandiant ASM	Mandiant

ツールの評価・検証項目			
観点	#	カテゴリ	項目
機能	1	スキャン機能	スキャンに必要な情報
	2	スキャン機能	発見可能なIT資産
	3	スキャン機能	発見可能な問題タイプ
	4	スキャン機能	脆弱性診断機能
	5	評価	リスク評価
	6	評価	対策の提示
	7	他システムとの連携	ダッシュボード
	8	他システムとの連携	自動化
非機能	9	トライアル版の有無	トライアル版の有無
	10	UI/UX	言語
	11	ライセンス形態	提供形態

評価・検証項目の決定

企業におけるASMの運用を想定し、他ツールとの連携や複数のASMツールの組み合わせ、自動化など高度な利用を実現するための検証項目を整理しました

高度な利用方法の評価・検証項目			
#	想定する企業	評価・検証項目	検証内容
1	■ 外部に露出しているIT資産を把握している企業 ■ 自動化を含めた常時モニタリングを検討している企業	■ 自動化 ✓ ASMツールの自動化に関する検証・評価 ■ 複数のASMツールの組み合わせ ✓ ツールの組み合わせによる高度化の検証・評価	■ API機能の充実度 ✓ APIで取得可能な情報 ✓ APIで実施可能な項目 ✓ 使用可能なプログラミング言語 ■ 他のシステムとの連携 ✓ 他プラットフォームとの連携 ✓ チケットシステムとの連携 ■ 複数のASMツールの組み合わせによる高度化 ✓ ASMの高度利用
2	■ 外部に露出しているIT資産をある程度把握している企業 ■ 定期的なモニタリングの実施を検討している企業 ■ 自社でツールを利用することを検討している企業	■ モニタリング ✓ ダッシュボード機能に関する検証・評価 ■ Mandiant ASMの試用 ✓ Mandiant ASMの利用難易度、効果的な運用方法、利用に向けた課題の抽出	■ ダッシュボード・レポート機能 ✓ ダッシュボードやレポート機能の充実度 ✓ 発見事項の説明情報が充実度 ✓ 推奨対応策の内容の充実度 ■ 想定利用者 ■ ダッシュボードのカスタマイズ ✓ リスクレベルや優先順位の調整 ✓ 他のダッシュボードからのインポート ✓ 他のダッシュボートへのエクスポート ■ 他のシステムとの連携 ✓ チケットシステムとの連携

ツールの機能調査

実環境調査で使用したツールについて、検証を通じて各ツールの特性や使用する際のポイントを整理しました

分類	ツール名	所感	ポイント
検索エンジン型	Shodan	■ IT資産や脆弱性はIPアドレスやFQDNを検索することで発見できます ■ 使用にあたり、事前にIPアドレスリストなどの準備が必要です ■ 検索操作は手動が基本となります ■ 大企業やIT資産を多く持つ企業は、Web APIを利用した自動化処理を推奨します	■ 事前に検索するIPアドレスリストなどの準備が必要 ■ リスク評価基準がシンプル
	Karma		■ 事前に検索するIPアドレスリストなどの準備が必要 ■ 独自で研究したIoT機器のゼロディ、EOLの可能性、初期状態、推測可能なWPAキーなどの検出が可能 ■ 主にIoTに関連する調査で効果大
	Maltego	■ 他の検索エンジン型ASMツールとは異なり、IT資産の関係を示すグラフを作成する点が特徴的です ■ Shodanとの連携により脆弱性を発見することもできますが、事前にツールの理解や連携方法の習得が必要です	■ ドメイン名のみで探索が可能 ■ IT資産同士の関係が把握可能 ■ リスク評価には別ツールが必要
高機能型	CyCognito	■ IT資産や脆弱性はドメイン名からでも発見できます ■ ソフトウェアの脆弱性以外の証明書や暗号に関する問題を発見できます ■ 検索エンジン型と比較して、機能が豊富であるため、セキュリティエンジニアなど専門家向けにデザインされている傾向があります	■ ドメイン名のみで探索が可能 ■ 機能が豊富であるためダッシュボードの操作の習得に時間がかかる ■ CVEに加え、脆弱性診断機能や脅威インテリジェンスによりリスクを評価
	Mandiant ASM		

ツールの機能調査

実環境調査で使用したツールについて、機能・非機能観点の調査および検証を行いました

分類	項目	Shodan	Karma	Maltego*1	CyCognito	Mandiant ASM
機能	スキャンに必要な情報	IPアドレス、FQDN	IPアドレス、FQDN	IPアドレス、FQDN	IPアドレス、ドメイン名	IPアドレス、ドメイン名
	発見可能なIT資産	インターネット接続している機器	インターネット接続している機器	IPアドレス、DNSレコード、CPE、CVE、ISP、Service、ポートなど	IPアドレス、ドメイン名、Webアプリケーション、サーバ証明書	IPアドレス、ドメイン名、Webアプリケーション、サーバ証明書など
	発見可能な問題タイプ	■ CVE情報 ■ 設定不備のあるIT資産など	■ 独自の脆弱性（パッチ状況、機器サポート、認証関連など）	■ CVE情報	■ CVE情報 ■ 証明書の有効性 ■ 暗号に関する問題 ■ 設定不備のあるIT資産など	■ CVE情報 ■ 証明書の有効性 ■ 暗号に関する問題 ■ 設定不備のあるIT資産 ■ IoC（侵害の痕跡）など
	脆弱性診断機能	なし	なし	なし	あり（機能OFF可）	あり（機能OFF不可）
	リスク評価	CVSSスコアの提示	2段階（高リスク、注意）	CVSSスコアのTransform機能と組み合わせ	4段階（Critical, High, Medium, Low）	5段階（Critical, High, Medium, Low, Informational）

*1：バナーとCPE情報からCVEを探し出すためのTransformのみ使用

ツールの機能調査

実環境調査で使用したツールについて、機能・非機能観点の調査および検証を行いました

分類	項目	Shodan	Karma	Maltego*1	CyCognito	Mandiant ASM
機能	対策の提示	なし	なし	なし	あり	あり
	ダッシュボード	あり	なし	なし	あり	あり
	自動化	■ Web APIにより自動化、他のシステムとの連携が可能	■ Web APIにより自動化、他のシステムとの連携が可能	■ Pythonにより独自のTransformの作成が可能	■ Web APIにより自動化、他システムとの連携が可能 ■ JIRA/ServiceNow/RPAツールと連携が可能	■ Web APIにより自動化、他システムとの連携が可能 ■ AWS/Azureと連携が可能 ■ JIRA/ServiceNowと連携が可能
非機能	無償版の有無	あり	なし	あり	なし	なし
	言語	英語	日本語	英語	英語	英語
	提供形態	クラウドサービス	クラウドサービス	ソフトウェア	クラウドサービス	クラウドサービス

*1：バナーとCPE情報からCVEを探し出すためのTransformのみ使用

ツールの機能調査

実環境調査で使用したツールについて、APIに関する機能を調査しました

項目	Shodan	Karma	Maltego*1	CyCognito	Mandiant ASM
認証方法	APIキー	Amazon Cognitoのみサポート	N/A	APIキー	APIキー
APIで取得可能な情報	サーバ場所、ポート、HTTP情報、バナー、CVE、CPEなど	サーバ場所、ポート、HTTP情報、バナー、Karma独自のセキュリティタグなど	N/A	Issue情報（ポート、CVE、タイプ、説明、深刻度、チケットステータス、コメント）、IT資産の情報、報告書のエクスポートなど	Issue情報（ポート、CVE、タイプ、説明、深刻度、チケットステータス、コメント）、IT資産の情報、Technologies情報、報告書のエクスポートなど
APIで実施可能な項目	■ リアルタイムのデータ取得 ■ ユーザ追加、管理など	■ クエリー結果の統計情報の取得など	N/A	■ 探索・診断スコープの設定 ■ IT資産を所有する組織情報の設定など	■ Collectionの管理、スキャンの実行 ■ 外部サービスと連携（GCP、Azure、AWS、GitHub、Akamaiなど）など
使用可能な言語	全13種類（Python、Ruby、PHP、Goなど）	NodeJS	Python	なし（curlコマンド使用）	なし（curlコマンド使用）
他プラットフォームの連携	可能	可能	可能	可能	可能

*1：バナーとCPE情報からCVEを探し出すためのTransformのみ使用

ツールの機能調査

実環境調査で使用したツールについて、ダッシュボード機能の違いを調査しました

項目	Shodan	CyCognito	Mandiant ASM
共通に得られる情報	公開ポート、サービス、CVE脆弱性、アクセスログ、タイムスタンプ		
Shodanと得られる情報の違い	–	CVE以外の発見、問題件数推移、説明、推奨対応策など	CVE以外の発見、問題件数推移、説明、推奨対応策、Technologies一覧など
想定利用者	エンジニア	マネージャ、エンジニア	マネージャ、エンジニア
チケットシステム	なし	ステータス管理（未調査、調査中、調査済み）、スヌーズ機能、深刻度の調整、担当者のアサインなど	ステータス管理（Open、Close、False Positiveなど）、担当者のアサインなど
アラート機能	ICS、IoT、マルウェア、脆弱性あるIT資産、データベースなどから設定が可能	深刻度、ステータス、IT資産タイプなどから設定が可能	スキャン結果のサマリーや差分をメールなどに通知する設定が可能
外部連携	メール、JIRA、Webhook（Slack、MS Teams）、REST API	メール、JIRA、Webhook（Slack）、ServiceNow、Workato、REST API	メール、JIRA、Splunk、ServiceNow、Webhook（Slack、MS Teams）、REST API

ツールの機能調査

実環境調査で使用した2つの高機能ツールについて、診断の仕組みを調査した結果、バナー情報を基にCVEの有無を推定し、追加で各社独自の手法を使って診断を行うことがわかりました

診断項目の詳細	CyCognito	Mandiant ASM
ダッシュボードの露出、サービスの露出など	○	○
2FA Bypass、認証Bypassなど	○	○
バッファーオーバーフロー、弱いSSL/TLS暗号の使用など	○	○
クロスサイトスクリプティング、SQLインジェクション、リモートコード実行など	○ (動的診断有)	○ (動的診断無)
DMARC設定の不備、サブドメインテイクオーバーなど	○	○
Pastebinによる情報漏洩、アカウントの漏洩、セキュリティトークンの漏洩など	×	○
不審なWebリダイレクト、Torrentに関するアクティビティなど	×	○
C2サーバとのやり取り、WebShell/Backdoor/CryptoMinerの存在など	×	○

CyCognitoとMandiant ASMの診断手法の比較結果

- 実環境調査で使用した2つの高機能ツールは、基本的にはバナー情報で該当するCVEの有無を推定し、さらに各社が独自で開発した手法を使って、脆弱性診断を行います
- CyCognitoは、Webサイトに存在する入力フィールドに対しても動的診断（ファジング）を実施しているため、バナー情報が無い場合であっても脆弱性の発見ができることが特徴です
- Mandiant ASMは、脅威インテリジェンスの活用によってマルウェア活動の発見ができることが特徴です

ツールの機能調査

実環境調査対象の2企業・団体から、Mandiant ASMの操作性や想定する運用について評価していただきました

分類	項目	評価結果
ツール	ダッシュボード・レポート	■ 専門家向けのダッシュボード 対策例がシンプルに表示されているなど、ある程度セキュリティの経験がある人向けに作られているように感じる
	想定利用者	■ 情報セキュリティ管理者 ■ エンジニア
運用方法	運用方法の想定	■ Mandiant ASM単体の利用 ■ 検索エンジン型（Shodanなど）と併用 ■ APIを利用し既存プラットフォームと連携
	課題	■ 調査範囲の設定 調査対象となるIT資産が多い場合、スキャンの実施や結果確認が難航するケースがあるため、細かく調査範囲を分割するなど、適切な調査範囲の設定が必要である ■ 参照するドキュメントやサンプルの充実 日本語のドキュメントやユースケースのサンプルが提示されているとより使用しやすい

高度な利用方法の検証

ユースケース１：Web APIを活用した検索の自動化

大量のIPアドレスやドメインに対してKarma Web APIを活用した検索の自動化を検証しました

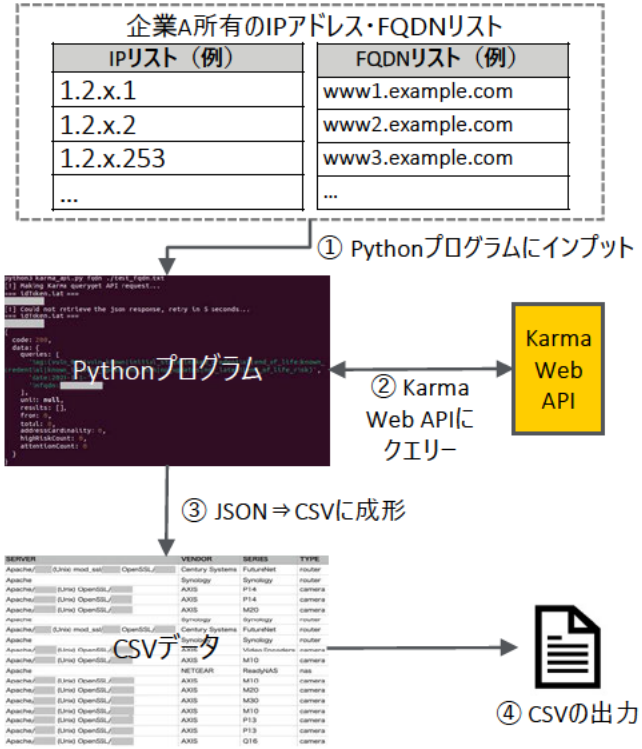
シナリオ	検証方法
企業Aは、大量なIPアドレスとドメインを所有しています。現在、Karmaのような検索エンジン型ツールの利用していますが、手動で個別のシードを入力する必要があるため、自動化による作業の効率化の必要性を感じています	Pythonプログラムを作成し、シードのリストをインプットすると自動的に「Karma Web API」にクエリーを行い、検索結果をCSVファイルとして出力するプロセスを検証しました

検証結果

Karma Web APIを利用し複数のシードのリストから自動的に検索できるようにするPythonプログラムを作成しました。また、Karma Web APIのアウトプットは基本的にはJSON形式であるため、可読性の観点からCSVフォーマットへの成形と出力まで実装しました

【検証手順】
① 自動化スクリプトに対象IPアドレスとFQDNのリストをインプット
② Karma Web APIにクエリーをする
  ➢ FQDNクエリー例：tag:対象セキュリティタグ fqdn:対象FQDN
③ Karma Web APIクエリー結果（JSON形式）をPythonライブラリーでCSVに成形
④ CSVファイルの出力

【考察】
■ IPアドレス/ドメインの数に関係なく、効率的に検索が可能です
■ CSVファイルが自動生成されることで、ITチームや他の開発チームへの情報共有がより簡単になります
■ さらにチケットシステムと連携し、対応チームの自動指定も実装することで、より効率的に問題への対処が可能です



高度な利用方法の検証

ユースケース2：ElasticSearch・Splunkなどを利用したダッシュボード機能の生成

検索エンジン型ツールとデータ統合プラットフォームを連携し、ダッシュボード機能の実装を検証しました

シナリオ	検証方法
企業Bは、IoT機器を幅広く利用しており、Karmaの導入を検討しています。企業全体の状況を一目で確認したいと考えていますが、Karmaには企業全体の状況を示すダッシュボード機能がないため、導入を悩んでいます	Karma Web APIを利用して、ElasticSearchやSplunkなどのツールにデータをインポートすることでダッシュボード機能を実現し、継続的なモニタリングが可能か検証しました

検証結果

Karma Web APIを利用してFileBeatからのデータをElasticSearchにインポートすることで、ダッシュボード機能を実装しました

【検証手順】

① FileBeatコンフィグにAPIからデータを取得するように設定
※FileBeatはKarmaの認証機能をサポートしていないため、仲介API Serverを経由させることで認証問題の解決が必要

② Karma Web APIのクエリー結果からデータを取得

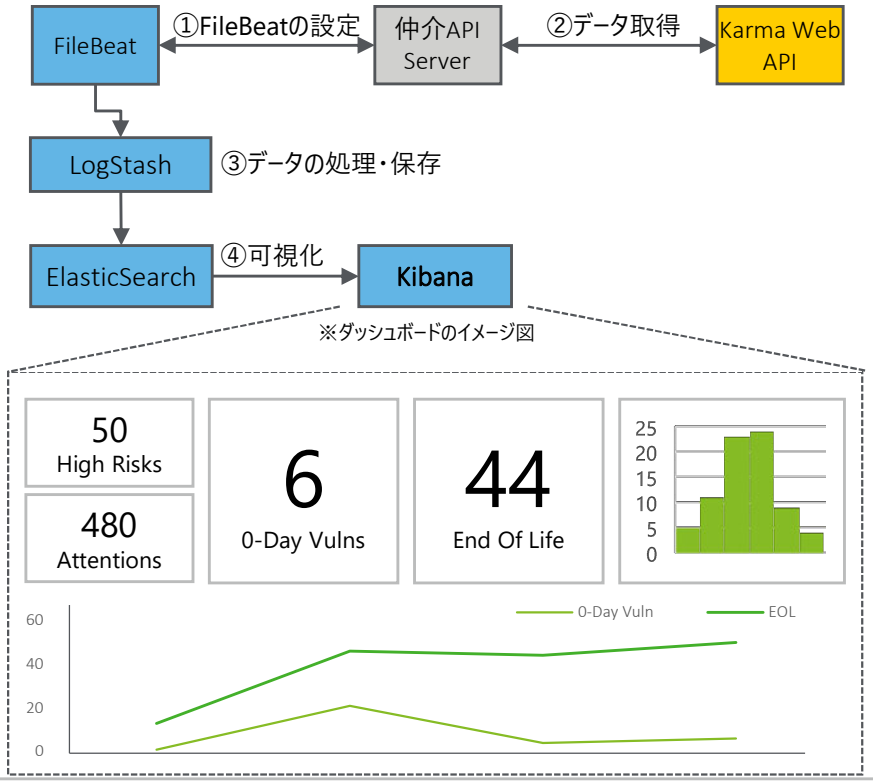
③ FileBeatからLogStashにデータをインポートし、LogStashがデータを成形しElasticSearchに保存

④ Kibanaでダッシュボードを作成し、モニタリングを開始

【考察】

■ モニタリングしたい項目（例:EOL、ゼロデイ） の変化分析が可能となり、対応方針の決定や経営層への提案が容易になります

■ 企業のニーズに合わせてダッシュボードの構成をカスタマイズすることで、検索エンジン型ツールから取得したデータをより有効に活用することが可能です



高度な利用方法の検証

ユースケース3：Karma Web APIを利用した複数のASMツールの組み合わせの検証

Karmaの検索結果をAPIでMaltegoにインプットし、IT資産の情報を可視化しました

シナリオ	検証方法
企業Cは、IT資産管理の一環としてMaltegoを活用し、自社のIT資産の関係図を作成しています。自社の国内にあるIoT機器に関する情報を補足するため、KarmaのデータをMaltegoに連携することを検討しています	MaltegoのLocal Transformを利用し、Karma Web APIで取得したデータをMaltegoのUI上に表示させ、Karmaから得られるIoT機器の情報が含まれた関係図の作成を検証しました

検証結果

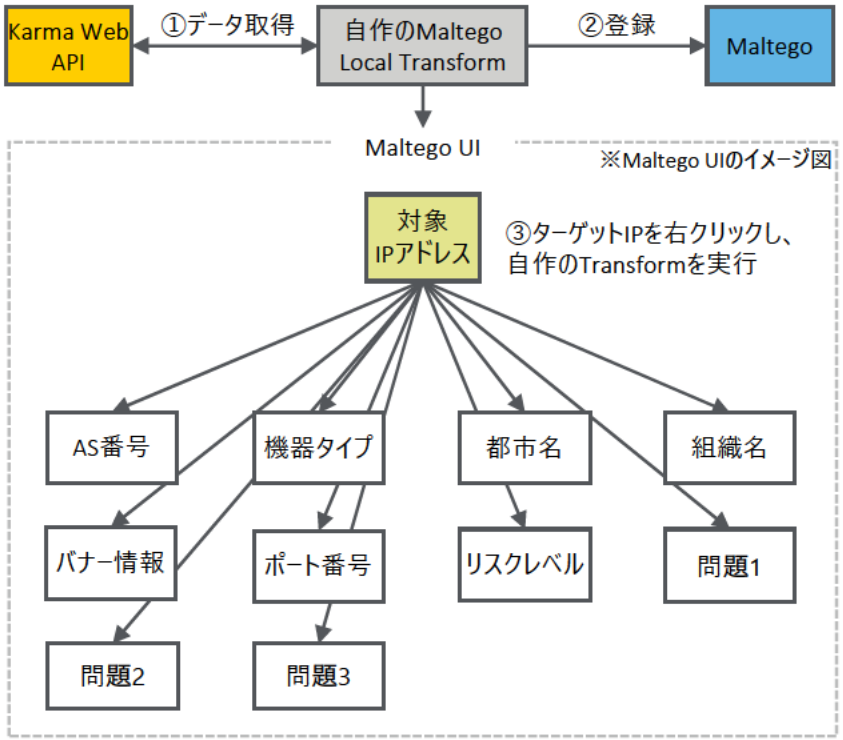
Karma Web APIを利用して取得したKarmaのデータをMaltego UIに表示させ、IoT機器の情報が含まれた関係図の作成しました

【検証手順】

① Karma Web APIからデータを取得するためのMaltego Local TransformをPythonで実装（本検証では、Maltego_trxライブラリを使用）
② Local TransformをMaltegoに登録
③ Maltego UI上で対象IPアドレスを右クリック⇒①で登録したLocal Transformを選択し、実行
   - Karmaに該当IPアドレスのデータがあれば、対応するAS番号、機器タイプ、都市名、組織名、バナー情報、ポート番号、リスク一覧などが取得可能

【考察】

- 複数のASMツールを組み合わせることにより、自社にとって最適なASMを実施することが可能です
- 00One社独自のセキュリティ調査結果を有効活用することで、CVE以外の問題の発見も可能です



円滑なASM調査の実施に向けて

ASMツールを使用した実環境調査や複数のツールの検証を通じて得た知見をもとに、ASM調査の各フェーズにおける留意点や気づきを整理しました

#	フェーズ	課題
1	事前準備	経営層へのASMの説明と実施の決裁、関係者へのASMの概要や機能の説明
		IT資産リスト、調査対象IT資産リストの準備
		組織（部署・グループ企業）の連絡窓口の洗い出し
		発見できる問題の優先順位決め
		ASM調査のスコープ設定、要件定義
2	ツール選定	ASMツールの理解（検索エンジン型、高機能型、サービス、診断機能の有無）
		ASM調査の要件に応じた人材の確保（自動化、結果分析、コンサル、内部連携など）
		実施日程、送信元IPアドレスの把握、自社SOCとの調整
3	結果分析と利用	WAF/IDS/IPSなどのセキュリティ機器の情報と合わせた結果の分析と判断
		ツールのリスク基準の既存リスク評価基準への統合、既存リスク評価基準の見直し
		結果の精査・エビデンス収集
		結果を活用した他セキュリティ施策への橋渡し（脆弱性診断、ペネトレーションテストなど）
		マルウェア関連活動の疑いがある場合の即時対応の判断
4	継続的運用	探索の頻度とリソースの兼ね合い
		自動化の必要性の検討、他のシステムとの連携
		チケットシステムとの連携、是正対応状況の可視化

5. 総括

総括

取組実態調査やASMツール・サービスの調査を通じて得られた知見をガイダンスと報告書にまとめました
これらが広く周知されることにより、ASM導入が加速されることを期待します

本調査におけるASMの定義

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

ASMの普及に向けて

- 近年、サプライチェーンリスクの高まりなどから、ASMを導入する企業は増加しています
- 一方で、ASMに関する公的機関による定義はなく、脆弱性診断との違いなど正しい認識は広まっていません
- ASMはOSINT情報をベースに外部に公開されているIT資産を発見することが最大の特徴です。一方で、発見した脆弱性の可能性は実態調査による確認が必要となります
- ヒアリング調査から、確認した脆弱性の是正にあたり、IT資産を管理する組織の特定および是正対応に時間がかかることが判明しました
- 特に、海外のグループ企業など組織を超えた連携が必要になる場合が多く、セキュリティに関する定常的なコミュニケーションの構築がASM導入効果の最大化の鍵となります
- 昨今では、多様なASMツールを国内で調達できる環境が整っており、自社の運用に最適なツールの選定が重要となります
- 実環境調査により、未把握なIT資産の脆弱性を発見するなどの効果を3企業・団体で検証しました。また、複数のツールの組み合わせやSIEMなど他のセキュリティ製品とのAPI連携も検証しました
- 加えて、ASM調査の事前準備、ツール選定、調査結果分析、運用の各フェーズにおける留意点、必要となるスキルなども整理しました
- 取組実態調査やASMツール・サービスの調査を通じて得られた知見は本報告書にまとめており、特に重要なポイントはガイダンスに記載しています
- 本報告書およびガイダンスによって、企業におけるASMの導入が加速し、国内のサプライチェーンリスクの低減につながっていくことを期待します

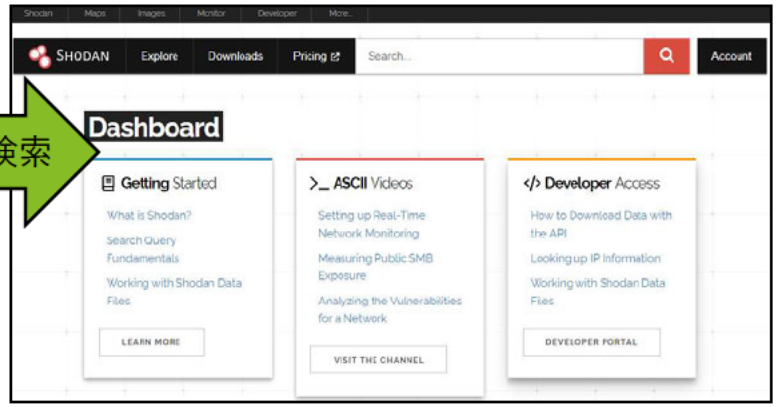
6. 付録

Shodan

Shodanは2009年からサービスを開始しています。インターネットに接続している機器の状態を検索できるShodan Searchをはじめ、モニタリングできるShodan Monitorなどを提供しています

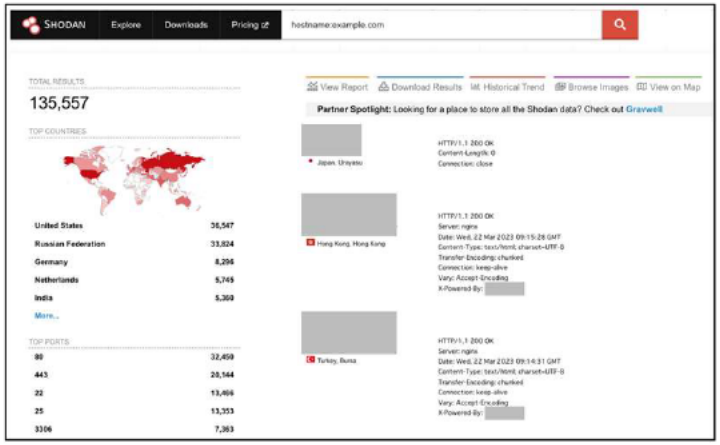
入力

IP/FQDNで検索



出力

例）hostname:example.comで検索した結果



Search**以外の主なサービス**

ラベル	説明
Monitor	対象のIT資産に対する継続的モニタリングを実現する機能
Maps	地図上にインターネット接続しているデバイスを表示、検索可能な機能
Images	インターネット上に公開しているIT資産のスクリーンショットをデータベース化した機能
InternetDB API	対象IPアドレスに関する情報や関連CVEを検索できる無料API機能
Enterprise	制限なしでShodanのすべてのサービスにアクセス可能なライセンス

Shodan Search**の活用ポイント、特徴**

■ 検索演算子を活用した検索結果のフィルタリング

検索例	クエリー
HTTPSを使用するIT資産	HTTP Strict-Transport-Security
Bootstrap CSSを使用しているIT資産	http.component:bootstrap
22や3333番ポートに稼働しているSSHサービス	ssh port:22,3333
日本国内にCVE-2019-19781の脆弱性があるIT資産	vuln:CVE-2019-19781 country: JP
ICS関連プロトコールを使っているIT資産	tag: ics

■ 検索件数が多い場合はAPIによる自動化の処理が必要

Karma

Karmaは日本国内のIoT機器の可視化を目的とした検索エンジン型ツールです。IoT機器のシグネチャを独自開発しており、IoT機器に関する発見に特化しています

入力

アセットID	ベンダー	シリーズ	モデル	セキュリティタグ
1001	A	Z1	aa.0	初期状態
1002	A	Z1	aa.2	ゼロデイ
1003	B	B01	zy01	なし
…	…	…	…	…

※表はイメージ

出力

ツールの活用ポイント

■ 検索演算子を活用した検索結果のフィルタリング

1. 特定IPアドレスの検索：「ip:x.x.x.x」
2. 特定FQDNの検索：「fqdn:www.example.com」
3. 特定タグ（例：ゼロデイ）の検索：「tag:vuln_001」
4. 特定IPアドレスに複数な特定タグの検索：「ip:x.x.x.x tag:（vuln_001|known_vuln|end_of_life）」

■ 検索件数が多い場合はAPIによる自動化の処理が必要

Karma分析エンジン

00Oneが開発したIoTシグネチャ

セキュリティタグ

※対象は日本のIPアドレスのみ
シグネチャを使用しIoT機器情報にマッピングする
1. ベンダー
2. シリーズ
3. モデル

高リスク	詳細
サポート終了	1年以上更新なし
初期状態	最新状態にしていない
認証情報が漏洩	認証情報が既出
既知の脆弱性	認証機構無し
ゼロデイ	初期IDが既出
	初期WPAキーが容易に推測可能

■ 高リスクのセキュリティタグは、00One社独自の研究成果とOSINT情報を併用し整理したもの

■ 00One社が発見した脆弱性のうち、未公開の脆弱性は「ゼロデイ」、公開されたものは「既知の脆弱性」に分類

Maltego

MaltegoはIT資産の関係図を作成するツールです。複数の外部データソースから情報を取得して
Maltegoのフォーマットに成形し、関係図を描写します

入力

IP/FQDN

Transform

Transformのタイプ

Tranformタイプ名	数	ASMと関連するデータソース
CLICK-AND-RUN – LIMITED	24	Censys, WhoisXML
CLICK-AND-RUN – UNLIMITED	16	NIST NVD, Shodan InternetDB
FREE DATA (API KEY REQUIRED)	12	Shodan, VirusTotal
DATA SUBSCRIPTIONS	11	Intel471
BRING YOUR OWN KEY	56	Flashpoint, CrowdStrike

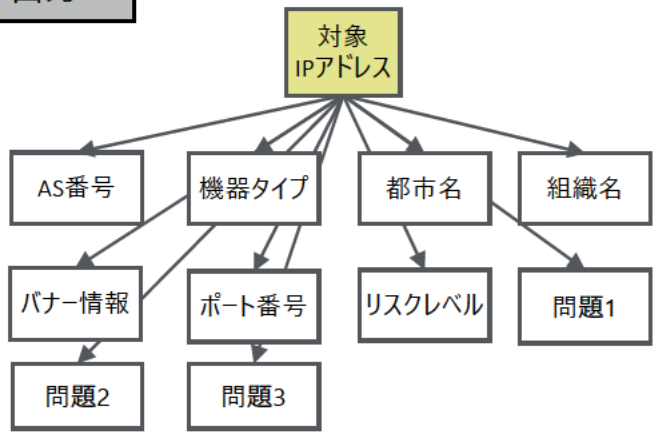
※ FREE DATAは商用利用に制限があります

Transform処理の例
ユーザが実行したTransformを実行します

データソース	Input	Output
Censys	Port	IPv4
	Service	IPv4
Shodan	Service	Banner
	Phrase	IPv4
	IPv4	Organization
	IPv4	CVE
…	…	…

出力

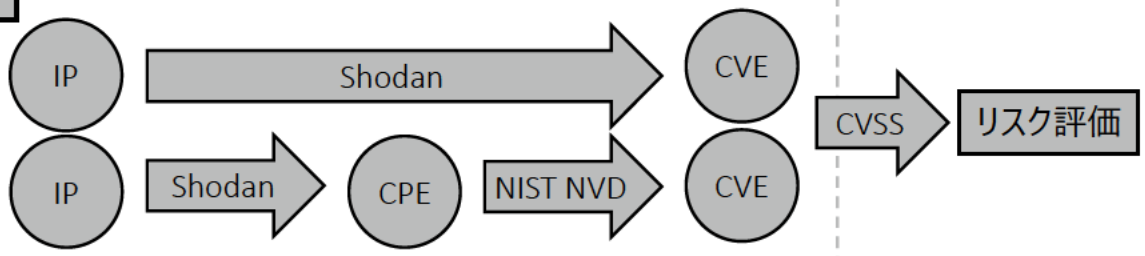
Maltegoのイメージ図



今回調査の流れ

「CLICK-AND-RUN – UNLIMITED」タイプのTransformを使用し、対象機器のCVE情報の洗い出し調査を行いました。また、別途CVSSを取得し、リスク評価基準に従ってリスク評価をしています

Transform



CyCognito

入力

ドメイン名

探索時

Whois、DNS、企業ロゴ、アイコン、年次報告書の情報を使用し、ツール側で機械学習とNLP技術でアセットの関係図を作成

組織1

組織2

.....

組織N

アセット1

.....

アセットN

1. IPアドレス
2. ドメイン名
3. Webアプリケーション
4. サーバ証明書

対象選定

探索により発見

脆弱性診断

1. 認証（例: 匿名ログイン）
2. ネットワーク （例: 証明書）
3. 資産管理 （例: 不正なファイル）
4. Web診断 （例: RCE）
5. フィッシング （例: SPFレコード）

問題点1

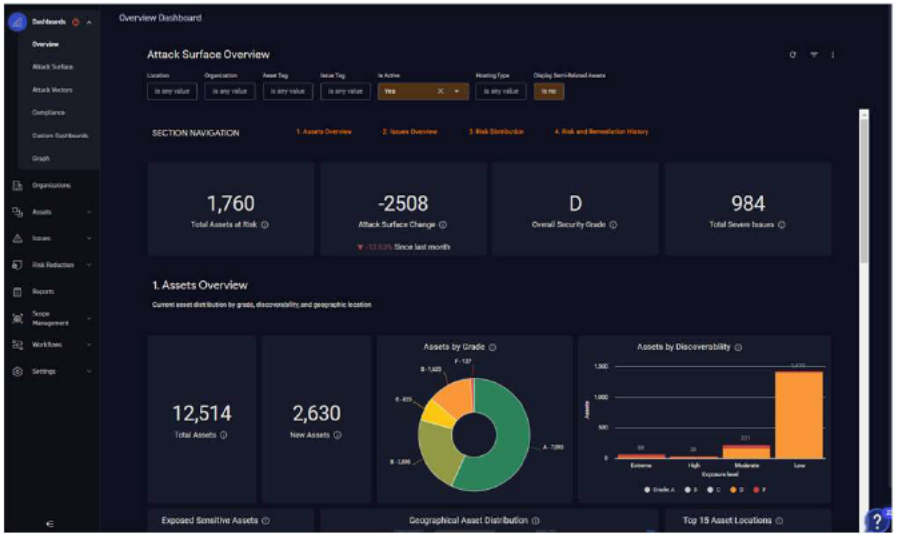
.....

問題点N

1. 証明書の有効性
2. 暗号に関する問題
3. 設定不備のあるIT資産
4. 脆弱なソフトウェア

出力

CyCognitoのダッシュボード



脆弱性深刻度レベル

即座の対処が必要

Critical

High

Medium

Low

直ぐ修正する必要がない

ツールの特徴、活用ポイント

- ダッシュボードからIT資産や問題のフィルタリングが可能
- エキスポート機能とレポート作成機能（サマリー）あり
- 外部のRPAソリューションとの連携機能があり、発見した問題の自動化処理も可能
- チケット管理機能があり、また、外部サービス（JIRA、ServiceNow）との連携も可能

Mandiant ASM

入力

プロジェクト

シード

シードの例：
1. IPアドレス
2. ドメイン名

コレクション1
コレクション2
.....
コレクションN

探索/診断

コレクション単位で診断

エンティティ example.com
エンティティ a.example.com
エンティティ b.a.example.com
エンティティ
エンティティ

問題

例：関連脆弱性情報

テクノロジー

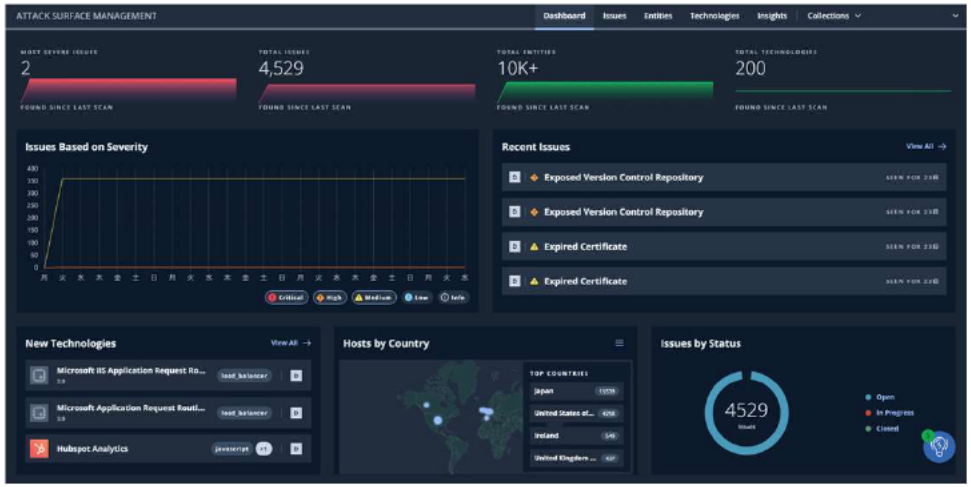
例：アプリケーション情報

- コレクションは、より良い資産管理を行うために、事業別や子会社単位で調査範囲を分ける機能です
- 脆弱性診断機能はOFFにできません

出力

ラベル	説明
Critical	組織に悪影響をおよぼす可能性がある
High	悪用可能な脆弱性、設定ミス、または露出がある
Medium	脆弱性はあるが、悪用するには難易度が高い
Low	脅威者の偵察活動を助長する脆弱性可能性があるが、直接的なリスクはない
Informational	すぐに対応する必要は無いが、継続的な取り組みの中で対処することを推奨する

Mandiant ASMダッシュボード



発見できる問題分類

脆弱性
設定の不備
IoC
情報漏洩
失効の証明書
不意に公開した開発環境
脆弱なCookie
脆弱なRDP
権限設定に不備があるS3 Bucket

ツールの特徴、活用ポイント

■ 探索・診断に機械学習機能を用いているため、2～3回スキャンを実施し、結果を安定させることが重要

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約1万7千名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約415,000名の人材の活動の詳細については、（www.deloitte.com）をご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited

二次利用未承諾リスト

報告書の題名
令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（外部から把握できる情報の活用に関する調査）報告書

委託事業名
令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（外部から把握できる情報の活用に関する調査）

受注事業者名　デロイトトーマツサイバー合同会社

頁	図表番号	タイトル
4		概要
5		概要
8		取組実態調査の実施概要
10		AS/ASMの定義に関する調査
11		AS/ASMの定義に関する調査
12		AS/ASMの定義に関する調査
13		AS/ASMの定義に関する調査
14		ASMツールに関する調査
15		ASMツールに関する調査
16		ASMツールに関する調査
17		ASMツールに関する調査
18		ASMサービスに関する調査
19		ASMサービスに関する調査
21		ヒアリング調査の流れ
22		ヒアリング調査の流れ
23		アンケートの回収・分析
24		（参考）アンケート項目
25		ヒアリング対象企業
26		ヒアリング結果のサマリー
27		（参考）ヒアリング内容
28		全体傾向　ASM導入状況
29		全体傾向　ASM導入の背景
30		全体傾向　ASMの導入目的
31		全体傾向　ASM導入の評価
32		全体傾向　ASMツール(1/2)
33		全体傾向　ASMツール(2/2)
34		（参考）ヒアリングした20社が利用または検討しているツール・サービス
35		ASM導入における課題　グループ会社のガバナンス
36		ASM導入における課題　IT資産を管理する組織特定
37		ASM導入における課題　ASMツールの結果解釈
38		ASM導入における課題　ASMに対する認識
39		ASM導入のおける課題　ツール・サービスの選択
40		ヒアリング内の特筆すべきコメント
43		ガイダンスの概要
45		ガイダンスの目次とポイント
46		ASM（Attack Surface Management）とは
49		ASMツール・サービスの調査の概要
51		調査手法の決定　調査の流れ
52		調査手法の決定　リスク評価基準
53		調査結果取りまとめ
54		結果報告
55		結果報告
57		評価・検証項目の決定
58		評価・検証項目の決定
59		ツールの機能調査
60		ツールの機能調査
61		ツールの機能調査
62		ツールの機能調査
63		ツールの機能調査
64		ツールの機能調査
65		ツールの機能調査
66		高度な利用方法の検証
67		高度な利用方法の検証
68		高度な利用方法の検証
69		円滑なASM調査の実施に向けて
71		総括
73		Shodan
74		Karma
75		Maltego
76		CyCognito
77		Mandiant ASM