これでわかる！2025年のセキュリティ組織とASMとトリアージ

日本セキュリティオペレーション事業者協議会
ISOG-J

2025.1.24

日本セキュリティオペレーション事業者協議会

Information Security Operation providers Group Japan(ISOG-J)

2008年設立、2025年1月現在69社加盟、およそ300人のメンバー
(親団体はJNSA。オブザーバーに総務省と経済産業省)

代表：武智 洋(日本電気株式会社)
副代表：阿部 慎司(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：早川 敦史(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：武井 滋紀(NTTテクノクロス株式会社)

セキュリティオペレーションガイドラインWG (WG1)	上野 宣(株式会社トライコーダ)
セキュリティオペレーション技術WG (WG2)	川口 洋(株式会社川口設計)
セキュリティオペレーション認知向上・普及啓発WG (WG4)	阿部 慎司(GMOサイバーセキュリティ byイエラエ株式会社)
セキュリティオペレーション連携 (WG6)	武井 滋紀(NTTテクノクロス株式会社)

このあとでこちらの成果物を紹介させていただきます！

各WG紹介(HPから)

【WG1】セキュリティオペレーションガイドラインWG（2012年7月発足）

脆弱性診断事業者・脆弱性診断士から開発会社向けまでセキュリティ技術の向上に役立つガイドライン作成を主目的としたWGです。

WGリーダー

上野 宣　株式会社トライコーダ

成果物	Webシステム／Webアプリケーションセキュリティ要件書 Webアプリケーション脆弱性診断ガイドライン 脆弱性診断士（Webアプリケーション）スキルマップ＆シラバス 脆弱性診断士（プラットフォーム）スキルマップ＆シラバス 脆弱性診断士倫理綱領 GraphQL 脆弱性診断ガイドライン ペネトレーションテストについて 脆弱性情報開示のためのチートシート その他、アジャイル開発におけるセキュリティなどに取り組んでいる
検討テーマ	要求にマッチしたセキュリティ診断サービスを的確に効率よく選択できるように、ユーザ向けセキュリティ診断サービスの解説書を作成する。セキュリティ診断サービスを向上するために、サービスを提供している技術者のレベルを計ることが可能な指標について検討する。
リーダーの思い	本WGではWG参加者同士が積極的に情報交換をする場を提供したいと考えています。ご自身の経験や知見を活かしてみたい方のご参加お待ち致しております。

【WG2】セキュリティオペレーション技術WG（2008年6月発足）

最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究し、技術者の交流を図ります。

WGリーダー

川口 洋　株式会社川口設計

成果物	最新技術レポート等（ISOG-J内限定）
検討テーマ	最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究、技術者の交流を図る
リーダーの思い	セキュリティオペレーション技術者同士の交流を活発にします

各WG紹介(HPから)

【WG4】セキュリティオペレーション認知向上・普及啓発WG（2008年6月発足）

セキュリティオペレーションの必要性についての認知度向上を目的とし、普及啓発活動を行います。

WGリーダー

阿部 慎司　GMOサイバーセキュリティ byイエラエ株式会社

成果物	イベント活動・各種広報資料（パンフレット等）
検討テーマ	セキュリティオペレーションの必要性について認知度向上を目的とした普及啓発活動を行う
リーダーの思い	セキュリティオペレーションの認知向上のみならず、他の団体やユーザとの連携強化を検討し、その価値を高められるよう様々な活動を行っていきます。

【WG6】セキュリティオペレーション連携WG（2016年4月発足）

セキュリティの運用について各社共通の課題の議論、検討を行います。

WGリーダー

武井　滋紀　NTTテクノクロス株式会社

成果物	セキュリティ対応組織(SOC/CSIRT)の教科書 セキュリティ対応組織の強化に向けたサイバーセキュリティ情報共有「5W1H」 マネージドセキュリティサービス(MSS)選定ガイドライン Ver.2.0 その他、共通課題の議論や検討の結果の発表や報告書など
検討テーマ	セキュリティオペレーション事業者間の共通の課題の認識および、課題の対応や対処について検討を行い、必要に応じて成果物を外部への公開を行う
リーダーの思い	セキュリティの運用がサービスとして一般化し、各社が提供するサービス内容や求められるサービス内容が多様化しています。このWGにおいては、各社のセキュリティの運用上の共通課題を抽出、議論を行うことで課題解決に結びつけることを目的に活動します。

2024年成果物

WG1

2024年5月、脆弱性トリアージガイドライン作成の手引き(1章まで)
2024年11月、ASM導入検討を進めるためのガイダンス(基礎編)
2024年11月、脆弱性トリアージガイドライン作成の手引き(2章以降)

この後解説です！

WG6

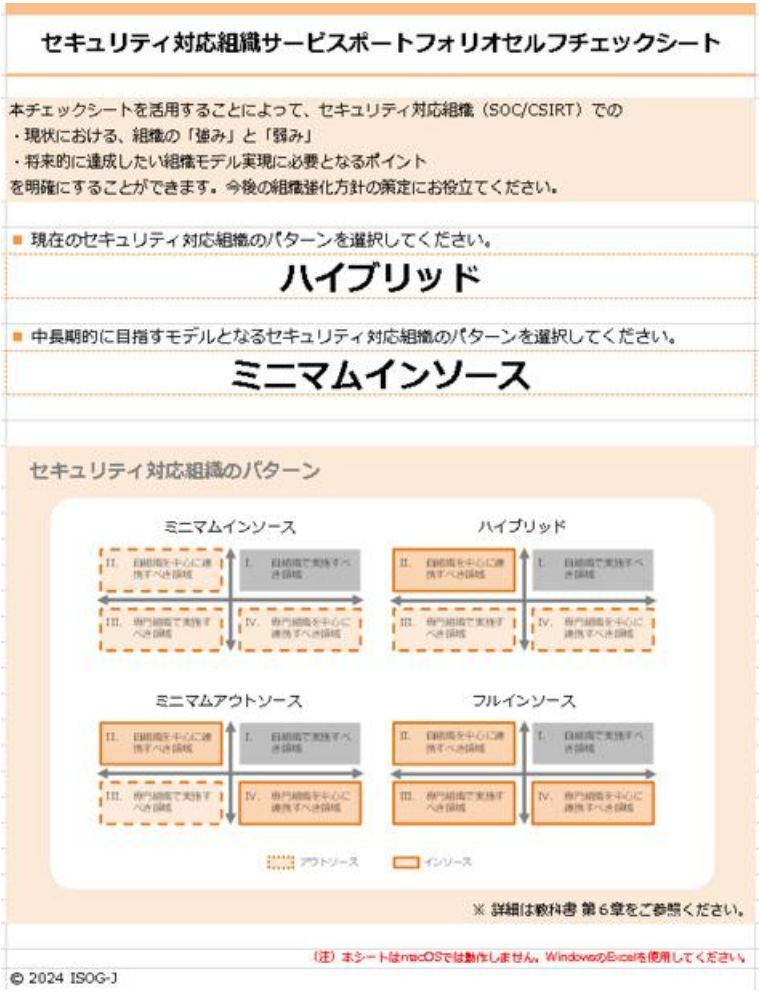
2024年10月、セキュリティ対応組織の教科書 第3.2版

セキュリティ対応組織の教科書　第3.2版

- 2024-10-17公開(第3.1版からちょうど1年)
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
- 第2.1版をITU-T勧告X.1060に合わせて改版したもの
- 執筆者
  - 野尻 泰弘, NECソリューションイノベータ株式会社
  - 吉田 佳音, NECソリューションイノベータ株式会社
  - 武井 滋紀, NTTテクノクロス株式会社
  - 彦坂 孝広, NTTテクノクロス株式会社
  - 河島 君知, NTT データ先端技術株式会社
  - 阿部 慎司, GMO サイバーセキュリティ byイエラエ株式会社
  - 早川 敦史, GMO サイバーセキュリティ byイエラエ株式会社
  - 井上 博文
  - 角田 玄司,ネットワンシステムズ株式会社
  - 青木 翔, 株式会社日立製作所
  - 後藤 啓太, SCSKセキュリティ株式会社
  - 川田 孝紀, NTT セキュリティ・ジャパン株式会社
  - 本橋 孝祐, NTT セキュリティ・ジャパン株式会社
  - 藤原 稔也, NTT データ先端技術株式会社
  - 石橋 拓己
  - 稲垣 洋平, 株式会社日本総合研究所
  - 竹之内 一晃, パーソルクロステクノロジー株式会社
  - 宇野 文康, 日立システムズ株式会社
  - 井上 圭, 株式会社ラック
  - ISOG-J WG6 メンバー

3.2版からの付録、セルフアセスメントシート

第2.1版のものからX.1060に合わせて刷新されました！



セキュリティ対応組織サービスポートフォリオセルフチェックシート

本チェックシートを活用することによって、セキュリティ対応組織（SOC/CSIRT）での
・現状における、組織の「強み」と「弱み」
・将来的に達成したい組織モデル実現に必要となるポイント
を明確にすることができます。今後の組織強化方針の策定にお役立てください。

■ 現在のセキュリティ対応組織のパターンを選択してください。

ハイブリッド

■ 中長期的に目指すモデルとなるセキュリティ対応組織のパターンを選択してください。

ミニマムインソース

セキュリティ対応組織のパターン

※ 詳細は教科書 第6章をご参照ください。

（注）本シートはmacOSでは動作しません。WindowsのExcelを使用してください。

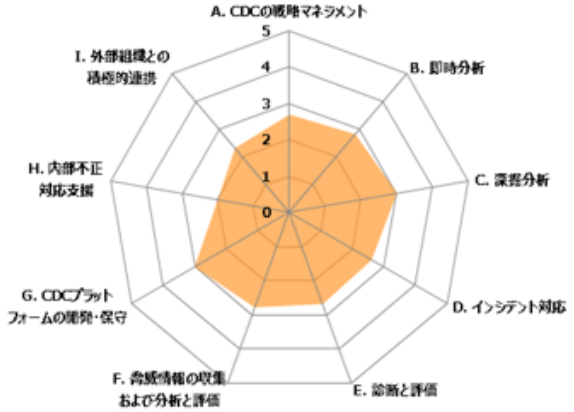
© 2024 ISOG-J

記入日 202X/YY/ZZ

			インソース						アウトソース						
			0 インソースでの実装を検討したものの、結果として実施しないと判断した	1 実施できていない	2 運用が明文化されておらず、担当者が業務を実施できる	3 運用が明文化されておらず、担当者に代わりに他者が緊急時で一部の業務を代行できる	4 運用が明文化されており、担当者と交代して他者が業務を実施できる	5 明文化された運用はCISOなど権限ある経営層に承認されている	0 アウトソースでの実装を検討したものの、結果として実施しないと判断した	1 結果や報告を確認できていない	2 サービス内容と得られる結果を理解できていない	3 サービス内容、得られる結果のいずれかが理解できていない	4 サービス内容と得られる結果を理解できているが、想定未満	5 サービス内容と得られる結果を理解でき、想定通り	※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。
カテゴリー	サービス	領域													備考
A.CISOの戦略マネジメント	A-1. リスクマネジメント	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-2. リスクアセスメント	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-3. ポリシーの企画立案	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-4. ポリシー管理	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-5. 事業継続性	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-6. 事業影響度分析	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-7. リソース管理	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-8. セキュリティアーキテクチャ設計	領域Ⅱ	●	○	○	○	○	○	○	○	○	○	○	○	

あなたのセキュリティ対応組織における"カテゴリー別"ポートフォリオ

202X/YY/ZZ



現状の組織（ハイブリッドパターン）におけるカテゴリー別成熟度を5段階で評価しています。
組織の「強み」と「弱み」を抽出し、現在のセキュリティ対応において有効に働いている機能と、改善が必要な機能を見える化しています。
マクロな観点での指標として、成熟度向上の方針策定にお役立てください。

カテゴリー	成熟度
A. CDCの戦略マネジメント	**2.7** /5
B. 即時分析	**2.8** /5
C. 深掘分析	**3.0** /5
D. インシデント対応	**2.6** /5
E. 診断と評価	**2.7** /5
F. 脅威情報の収集および分析と評価	**2.8** /5
G. CDCプラットフォームの開発・保守	**3.0** /5
H. 内部不正対応支援	**2.0** /5
I. 外部組織との積極的連携	**2.3** /5

現状のセキュリティ対応組織の強み

残念ながら「強み」と言えるサービスはありません。

現状のセキュリティ対応組織の弱み

H. 内部不正対応支援
内部統制、内部不正に関する対応の支援を十分行えておらず、ガバナンスやコンプライアンス面で貢献しにくくなっています。組織的に機能しているとは言えない状況で、着実に実施できるよう改めて業務を見直してください。

I. 外部組織との積極的連携
対外組織との連携が希薄であり、組織のレベルアップ、存在価値の向上につなげることができていません。組織的に機能しているとは言えない状況ですので、着実にできるよう改めて業務を見直してください。

v3.2

あなたのセキュリティ対応組織における"サービス別"ポートフォリオ

202X/YY/ZZ

現状の組織のサービス成熟度を5段階で示し、モデルとするミニマムインソースパターン到達へのポイントも列挙していますので、サービス強化にお役立てください。

より強化すべきインソースのサービス

自組織での能力をより高めるべきもの	I-5. セキュリティ関連団体との連携 I-7. 幹部向けセキュリティ報告 F-5. 脅威情報の活用

より強化すべきアウトソースのサービス

より効果的なアウトソースとなるよう改善すべきもの	A-12. セキュリティ監査 I-3. セキュリティコンサルティング G-13. 新規セキュリティツール検証

インソースへの切り替えを検討すべきサービス

インソースの方が対応力の強化につながるもの	I-2. 教育・トレーニング G-11. CDCシステム運用 D-6. インシデント通知

アウトソースへの切り替えを検討すべきサービス

アウトソースした方が強化しやすいもの	I-6. 技術報告 I-4. セキュリティベンダーとの連携 H-2. 内部不正検知・再発防止支援

v3.2

これでわかる！
ASMとトリアージ

ISOG-J WG1, OWASP Japan
脆弱性診断士スキルマッププロジェクト

NRIセキュアテクノロジーズ株式会社
大塚 淳平

株式会社セキュアスカイ・テクノロジー
岩間 湧

所属非公開
平田 優

Japan Network Security Association
Network Security Forum 2025
01.24 FRI

登壇者

NRIセキュアテクノロジーズ株式会社
大塚　淳平

略歴

脆弱性診断（Web、ネットワーク、エンドポイント）

リスク評価&セキュリティ関連コンサル

- 技術的セキュリティ
- 対策アドバイザリ、設計支援
- 自社関連トレーニング（自社コンテンツやSANSなどの講師・TA）

Webサイト探索＆脆弱性管理サービス

サービス開発および提供

- OSINT
- 脆弱性管理

ペネトレーションテスト

サービス開発および提供

- RedTeam
- 脅威インテリジェンス

リサーチ、技術アドバイザリ

脅威情報および技術動向の調査

- 脅威/脆弱性動向調査
- インテリジェンス活用＆サービス開発

専門領域

REDTeam系サービス

脆弱性管理関連

脅威インテリジェンス関連

定義が曖昧な領域に
比較的早くから取り組み

自己紹介

株式会社セキュアスカイ・テクノロジー

岩間 湧

業務　EASMクラウドサービス「Dredger(ドレッジャー)」 PdM

専門領域
- 脆弱性診断
- アタックサーフェス関連
- NWセキュリティ

WG活動
- 細かすぎるけど伝わってほしい脆弱性診断手法ドキュメント
- XS-Leaks Wiki(翻訳)
- GraphQL診断ガイドライン　など

自己紹介

平田 優

略歴

- セキュリティ製品の技術サポート、インシデント対応
- サイバー犯罪調査・分析
- 脅威インテリジェンスの提供
- 海外子会社のITセキュリティ管理
- 生成AIのビジネス応用研究

専門領域

- データ分析
- 脅威インテリジェンス
- セキュリティガバナンス

コメント

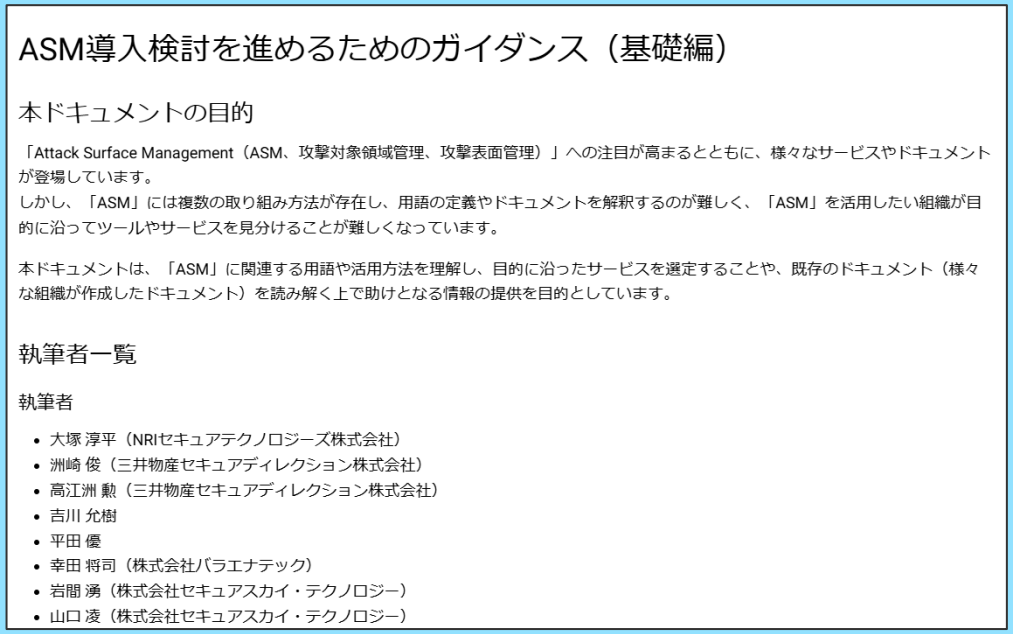
- 何でも屋です

本セッションのテーマ
「ASM」と「脆弱性トリアージ」

▶２つのテーマはIT資産の管理プロセス上で関係性が強い

ASM（アタックサーフェスマネジメント）

IT資産の管理やリスク評価（資産、脆弱性の検出）
発見されたIT資産や脆弱性への対応



ASM導入検討を進めるためのガイダンス（基礎編）

本ドキュメントの目的

「Attack Surface Management（ASM、攻撃対象領域管理、攻撃表面管理）」への注目が高まるとともに、様々なサービスやドキュメントが登場しています。
しかし、「ASM」には複数の取り組み方法が存在し、用語の定義やドキュメントを解釈するのが難しく、「ASM」を活用したい組織が目的に沿ってツールやサービスを見分けることが難しくなっています。

本ドキュメントは、「ASM」に関連する用語や活用方法を理解し、目的に沿ったサービスを選定することや、既存のドキュメント（様々な組織が作成したドキュメント）を読み解く上で助けとなる情報の提供を目的としています。

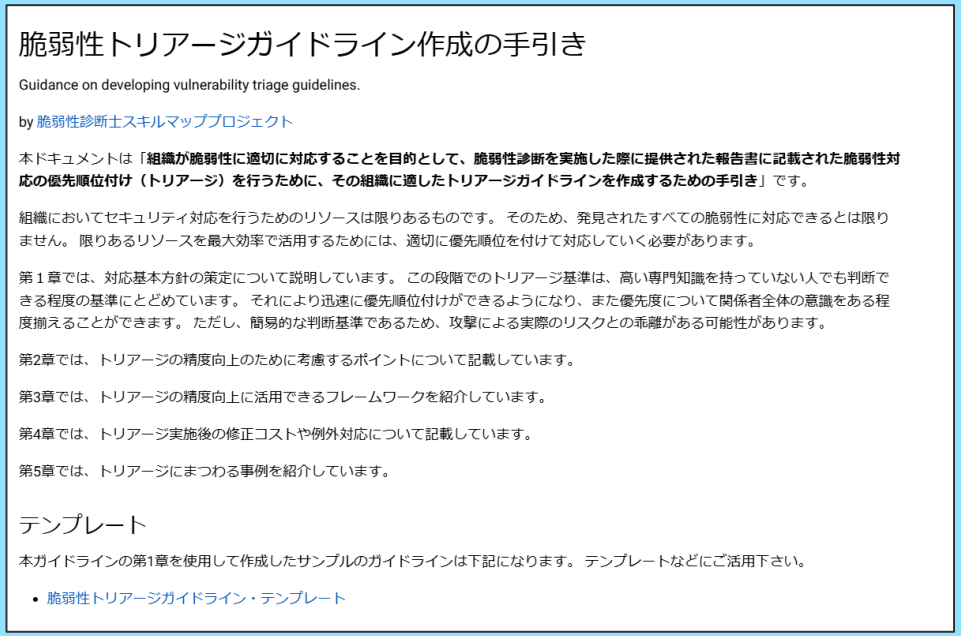
執筆者一覧

執筆者

- 大塚 淳平（NRIセキュアテクノロジーズ株式会社）
- 洲崎 俊（三井物産セキュアディレクション株式会社）
- 高江洲 勲（三井物産セキュアディレクション株式会社）
- 吉川 允樹
- 平田 優
- 幸田 将司（株式会社バラエナテック）
- 岩間 湧（株式会社セキュアスカイ・テクノロジー）
- 山口 凌（株式会社セキュアスカイ・テクノロジー）

脆弱性トリアージ

脆弱性情報や脆弱性診断結果への
対応方針の決定（トリアージ）



脆弱性トリアージガイドライン作成の手引き

Guidance on developing vulnerability triage guidelines.

by 脆弱性診断士スキルマッププロジェクト

本ドキュメントは「**組織が脆弱性に適切に対応することを目的として、脆弱性診断を実施した際に提供された報告書に記載された脆弱性対応の優先順位付け（トリアージ）を行うために、その組織に適したトリアージガイドラインを作成するための手引き**」です。

組織においてセキュリティ対応を行うためのリソースは限りあるものです。 そのため、発見されたすべての脆弱性に対応できるとは限りません。 限りあるリソースを最大効率で活用するためには、適切に優先順位を付けて対応していく必要があります。

第１章では、対応基本方針の策定について説明しています。 この段階でのトリアージ基準は、高い専門知識を持っていない人でも判断できる程度の基準にとどめています。 それにより迅速に優先順位付けができるようになり、また優先度について関係者全体の意識をある程度揃えることができます。 ただし、簡易的な判断基準であるため、攻撃による実際のリスクとの乖離がある可能性があります。

第2章では、トリアージの精度向上のために考慮するポイントについて記載しています。

第3章では、トリアージの精度向上に活用できるフレームワークを紹介しています。

第4章では、トリアージ実施後の修正コストや例外対応について記載しています。

第5章では、トリアージにまつわる事例を紹介しています。

テンプレート

本ガイドラインの第1章を使用して作成したサンプルのガイドラインは下記になります。 テンプレートなどにご活用下さい。

- 脆弱性トリアージガイドライン・テンプレート

ASM&脆弱性トリアージ
セッション

1. **『ASM導入検討を進めるためのガイダンス』**
   - ASMの必要性
   - 制作の経緯
   - 注目ポイントの紹介
   - 活用事例
2. **『脆弱性トリアージガイドライン作成の手引き』**
   - 注目ポイントの紹介
   - 活用方法

質問やコメントの受付

- **本講演に関するご質問やご意見を以下で受け付けます。**
- **講演終盤で頂いたご質問に回答します。**
  （時間の都合で割愛する可能性もあります）

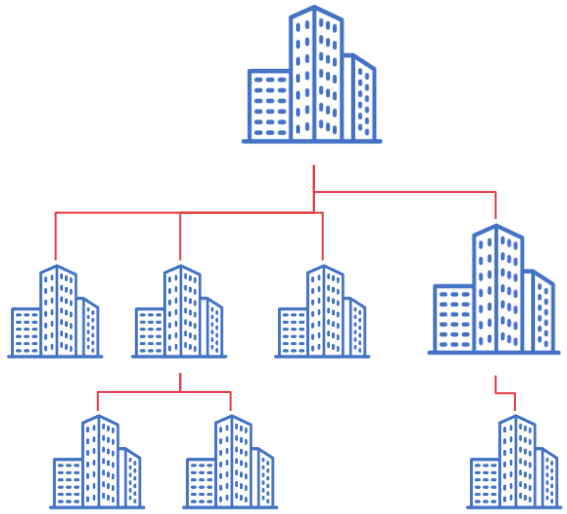
① **https://www.menti.com/**　にアクセス
② コードに **1372 4549** を入力

簡単なアンケートのあとに
質問（自由入力）が可能です
※回答者の情報や属性は取得していません

01 『ASM導入検討を進めるためのガイダンス』

ASMが必要とされる背景
攻撃者にとっての狙い目が増加

企業



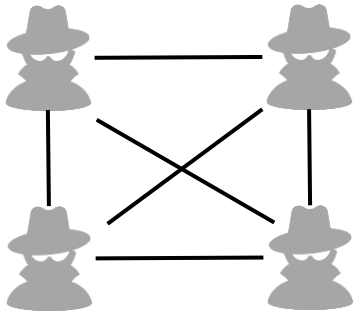
DXの進展（デジタル革命）

テレワーク積極活用

クラウド利用拡大

攻撃者

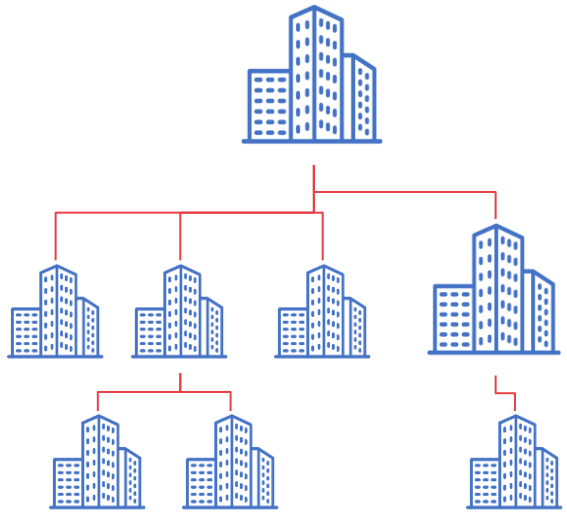
攻撃者間



組織化/分業体制

ASMが必要とされる背景
攻撃者にとっての狙い目が増加

企業



DXの進展（デジタル革命）

テレワーク積極活用

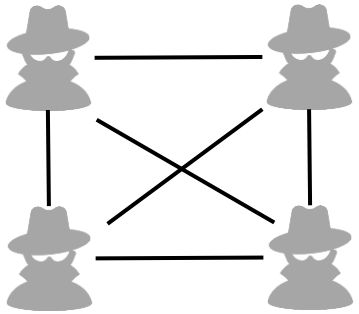
クラウド利用拡大

③管理しきれないIT資産

②攻撃の効率性

攻撃者

攻撃者間

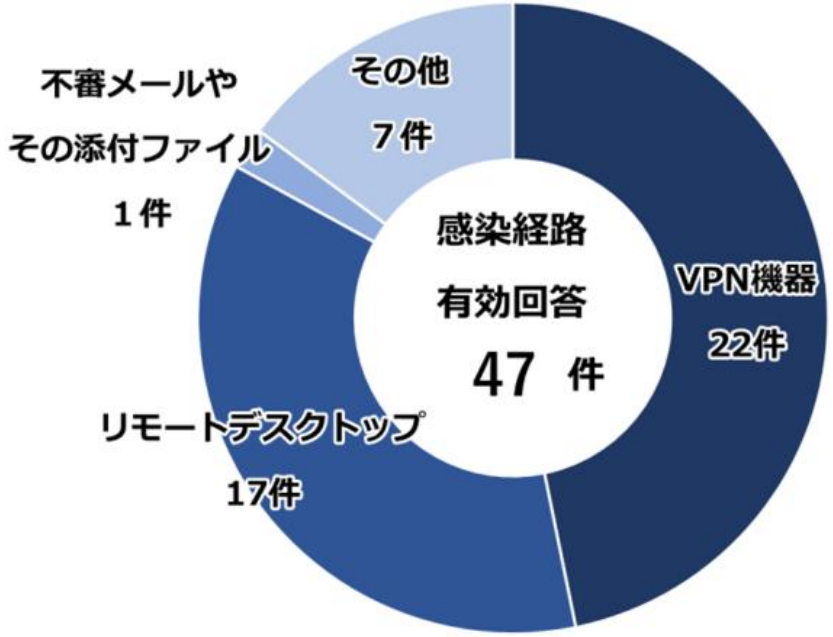


組織化/分業体制

①大量の脆弱性

ASMが必要とされる背景
ランサムウェアの感染経路

▶ランサムウェアの感染経路として、VPNやリモートデスクトップが大半を占める



出典：令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について （警察庁サイバー警察局、2024年9月）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

ASMが必要とされる背景
悪用される脆弱性の傾向

▶日常的且つ頻繁に悪用された脆弱性（2022年、2023年）
大半がネットワーク機器などインターネットからアクセス可能なもの

2023年Top15

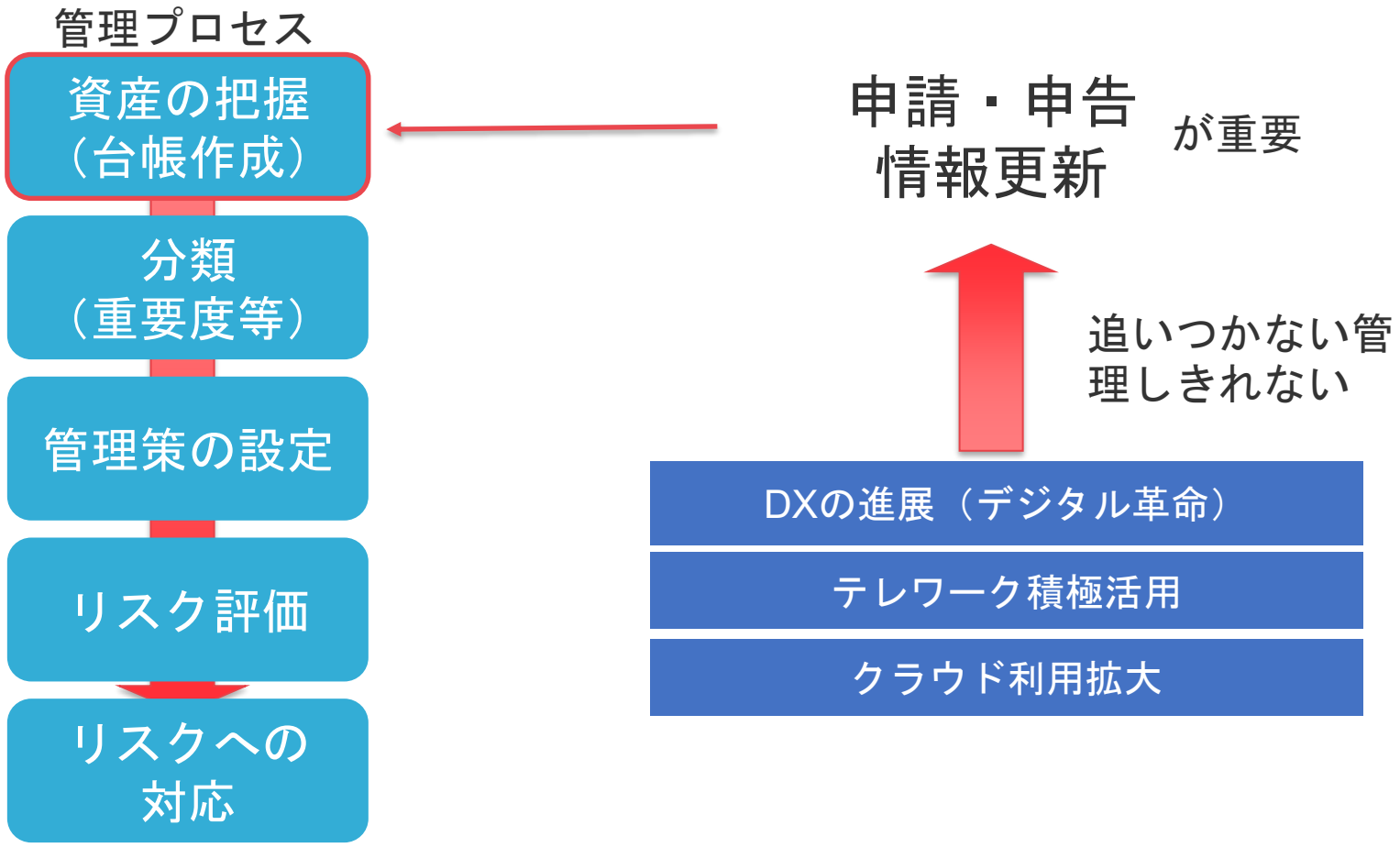
#	脆弱性	ベンダー / プロダクト
1	CVE-2023-3519	Citrix NetScaler ADC / Gateway
2	CVE-2023-4966	Citrix NetScaler ADC / Gateway
3	CVE-2023-20198	Cisco IOS XE Web UI
4	CVE-2023-20273	Cisco IOS XE
5	CVE-2023-27997	Fortinet FortiOS FortiProxy SSL-VPN
6	CVE-2023-34362	Progress MOVEit Transfer
7	CVE-2023-22515	Atlassian Confluence Data Center and Server
8	CVE-2021- 44228	Apache Log4j2
9	CVE-2023-2868	Barracuda Networks ESG Appliance
10	CVE-2022-47966	Zoho ManageEngine Multiple Products
11	CVE-2023-27350	PaperCut MF/NG
12	CVE-2020-1472	Microsoft Netlogon
13	CVE-2023-42793	JetBrains TeamCity
14	CVE-2023-23397	Microsoft Office Outlook
15	CVE-2023-49103	ownCloud graphapi

2022年Top12

#	脆弱性	ベンダー / プロダクト
1	CVE-2018-13379	Fortinet / FortiOS and FortiProxy
2	CVE-2021-34473	Microsoft / Exchange Server
3	CVE-2021-31207	Microsoft / Exchange Server
4	CVE-2021-34523	Microsoft / Exchange Server
5	CVE-2021-40539	Zoho / ManageEngine ADSelfService Plus
6	CVE-2021-26084	Atlassian / Confluence Server and Data Center
7	CVE-2021-44228	Apache / Log4j2
8	CVE-2022-22954	Apache / Log4j2
9	CVE-2022-22960	VMware / Workspace ONE Access, Identity Manager, and vRealize Automation
10	CVE-2022-1388	F5 Networks / BIG-IP
11	CVE-2022-30190	Microsoft / 複数製品
12	CVE-2022-26134	Atlassian / Confluence Server and Data Center

出典：2023 Top Routinely Exploited Vulnerabilities（CISA、FBI、NSA、他同盟諸国当局、2024年11月）、2022 Top Routinely Exploited Vulnerabilities （CISA、FBI、NSA、他同盟諸国当局、2023年8月）
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a

課題
従来（申告型）のIT資産管理プロセスの限界



課題への打ち手として期待
ASM（アタックサーフェスマネジメント）

「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

ただし、用語の使われ方、考え方の難しさなどから、
“ASM”が資産管理のためのプロセスであるのか、
ツールであるのか解釈が難しい

ASM導入検討を進めるためのガイダンス

「ASM」をわかりやすくするための
ドキュメント

- 関連する用語や活用方法
- 目的に沿ったサービスの選定
- 既存のドキュメントの読解

2024年11月　基礎編公開

- **https://webapppentestguidelines.github.io/ASMGuidance/**

ガイダンス本編

ガイダンスの構成

第1章：はじめに

ASM関連ドキュメント

- 経産省：「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～」
- CISA：BINDING OPERATIONAL DIRECTIVES 23-02（BOD 23-02：拘束力のある運用指令23-02）
- CISA：BOD 23-02: Implementation Guidance for Mitigating the Risk from Internet-Exposed Management Interfaces（BOD 23-02 実装ガイダンス）

1.1 ASM（Attack Surface Management）の必要性

現代の企業や組織では、DX推進やクラウド利用の拡大、テレワークの普及により、IT資産が急速に増加しています。Webサイトの構築、公開が手軽にできたり、社内のストレージ増強が難しいときにはクラウドを一時的に利用できたりと、企業や組織が保有するIT資産は変化する頻度が高い状況にあります。

このような状況においては、以下の課題があります。

昨今のIT資産管理の課題

- 企業や組織のIT資産は変化する頻度が高く、従来どおりの管理（ルールベースでの管理）には限界がある
- IT資産の把握や管理がしきれず、管理の抜けや漏れが発生する

管理されていない（管理しきれていない）インターネット上のIT資産は攻撃者にとって絶好の標的です。例えば攻撃者が標的組織に侵入したいという目的で攻撃を仕掛ける場合、どこか1か所でも侵入可能な綻びを見つけられれば攻撃者の目的が達成できてしまうため、インターネットから見える「隙」を作るのは、守る側としては望ましくない状況です。

上記課題への打ち手として、Attack Surface Management（ASM）が注目を集めています。
国内では経済産業省、海外では米国CISA（CISA:Cybersecurity and Infrastructure Security Agency、サイバーセキュリティ・インフラストラクチャセキュリティ庁）など、権威ある組織からASM活用を後押しするドキュメントが発行されています。

> **補足**
> 上記ドキュメントへのリンクは参考資料をご参照ください。

なお、経済産業省が発行したドキュメントはEASM（External Attack Surface Management）に注目しており、米国CISAが発行したドキュメントは直接ASMに言及しているものではありませんが、ASMが得意とする領域に言及しているため、ASMの活用検討時に役立つドキュメントとなっています。
（ASMが得意とする領域＝インターネットに公開すべきでないインターフェース、管理対象とすべき機器やサーバーやプロトコルの種別など）

第2章：Attack Surface Management（ASM）とは何か

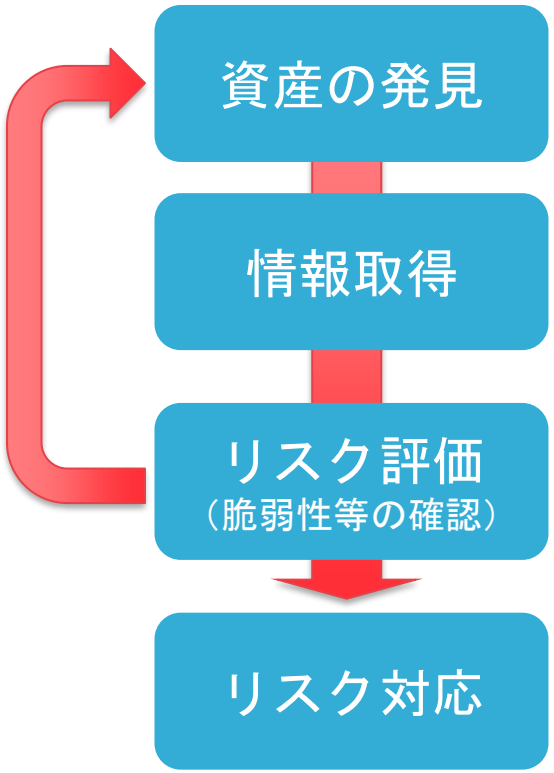
ASM関連用語

ASMの解釈や定義がドキュメントにより様々なため、読み解く上では確認が必要

用語	定義
AS、アタックサーフェス	組織の外部（インターネット）からアクセス可能な IT 資産（システムやサーバー、IPアドレス等）
ASM	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ツール	ASMのプロセスを実現もしくは補助するためのツール
ASMサービス	ASMのプロセスを実現もしくは補助するために外部組織（セキュリティベンダ等）から提供を受けるサービス

ASM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」



１．アタックサーフェスの検出（発見）
“外部からアクセス可能な資産”を検出する

２－１．付加情報の収集
発見したIT資産の構成情報を継続的に取得する

２－２．リスク評価
設定ミスや影響を受ける脆弱性があるかを継続的に確認する

３．リスクへの対応
IT資産管理とリスクへの対応に取り組む
（元から取り組んでいたIT資産管理と同様に対応する等）

ASMや類似とされることが多いツール/サービス

各ツールやサービスの目立った特徴に注目
利用目的により、資産の見え方や資産発見のアプローチが異なる

種別	主な利用目的	概要
EASM (External Attack Surface Management)	**インターネットからアクセス可能なIT資産の探索（未知の資産の発見も含む）、脆弱性の調査**	**インターネット上を探索し、自組織に関連したIT資産を発見、セキュリティチェックを実施し、リスクを評価する。**
CAASM (Cyber Asset Attack Surface Management)	IT資産の脆弱性や設定管理	クラウドサービスプロバイダのAPIや既存のセキュリティ製品の外部連携機能などを活用し、IT資産および利用製品、設定の情報を取得し、リスクを評価する。
DRPS (Digital Risk Protection Service)	外部からの脅威を検知・分析し、デジタルリスクを管理	自組織を狙う脅威の可視化、ブランド保護、データ漏洩検知を行い、デジタル資産のリスクを評価する。
TPRM (Third Party Risk Management)	ビジネス関係にある組織から生じるリスクの特定・評価、対応・管理	外部のサードパーティ企業との関係から生じるリスクを特定、評価、管理し、サプライチェーン全体のリスクを評価する。
セキュリティリスクレーティング、セキュリティスコアリング	組織のセキュリティ態勢を客観的にスコアリングし、リスクの高い領域の特定	外部から観測可能な情報を非侵入的に収集・分析することで、組織のセキュリティ状態を定量的に評価し、組織のサイバーセキュリティ状況をスコア化する。

※記載内容は各カテゴリの際立った特徴に注目したもので、特定の製品は想定していません

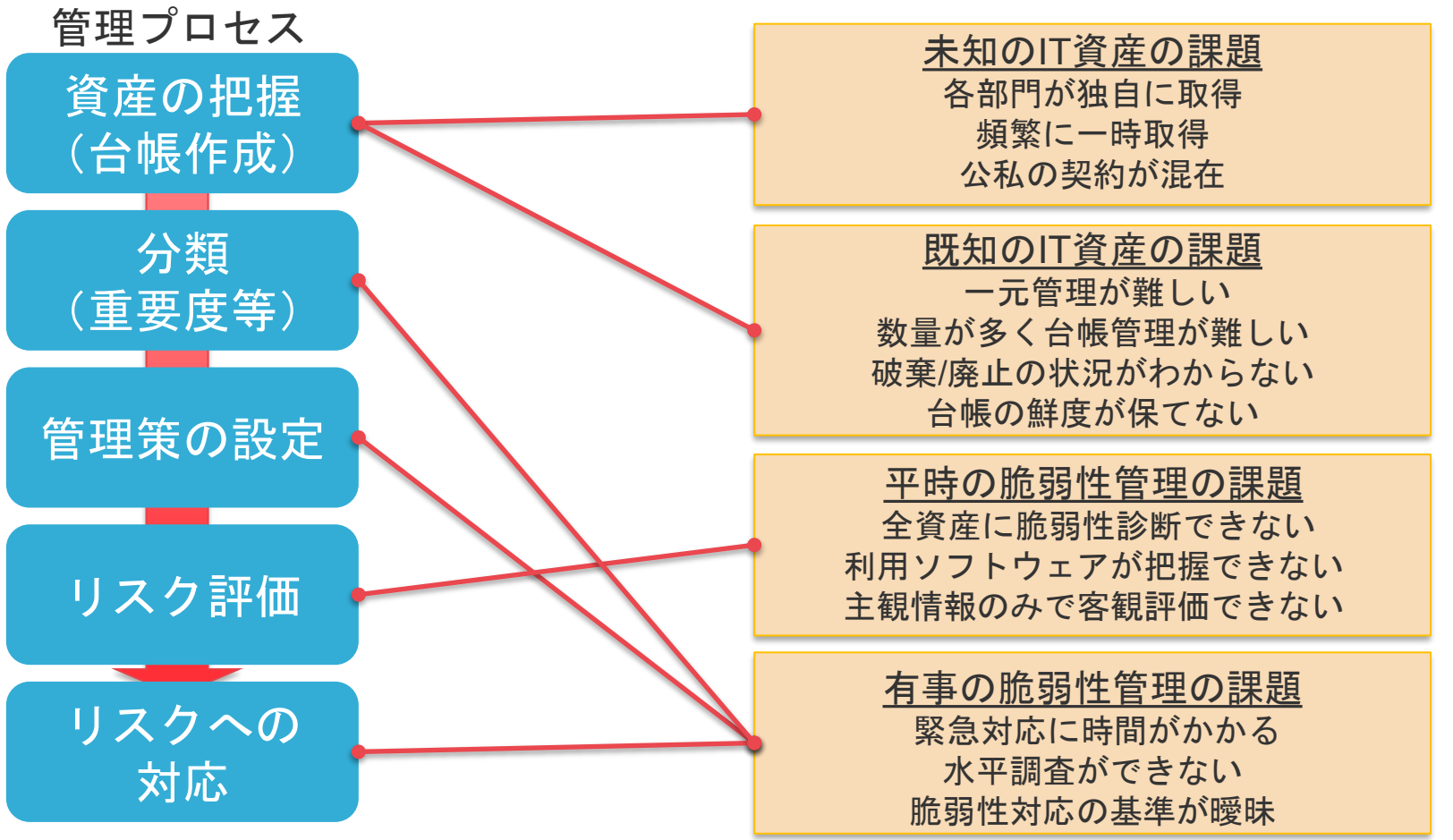
ASMツールは脆弱性診断の代わりになる？

結論から述べると、ASMツールは脆弱性診断の代わりにはなりません
その逆も同様に、脆弱性診断はASMツールの代わりにはなりません

	ASMツール	脆弱性診断（手動診断）
実施の目的	アタックサーフェスの検出と管理、リスクの早期発見	指定したIT資産の脆弱性の発見と対策
IT資産の発見	発見する	発見しない
対象の公開範囲	外部公開されているIT資産のみ	外部公開および内部(非公開)のIT資産
対象の選び方	発見したIT資産全てを対象にできる	自分たちで対象を指定
リスク評価が対象に及ぼす影響	脆弱性診断に比べ少ない	多数の疑似攻撃や検査用通信が発生（副作用の可能性あり）
リスク評価の頻度	高頻度	低頻度
リスク評価の精度	低い	高い
リスク評価のコスト	低い（安価）	高い（高価）

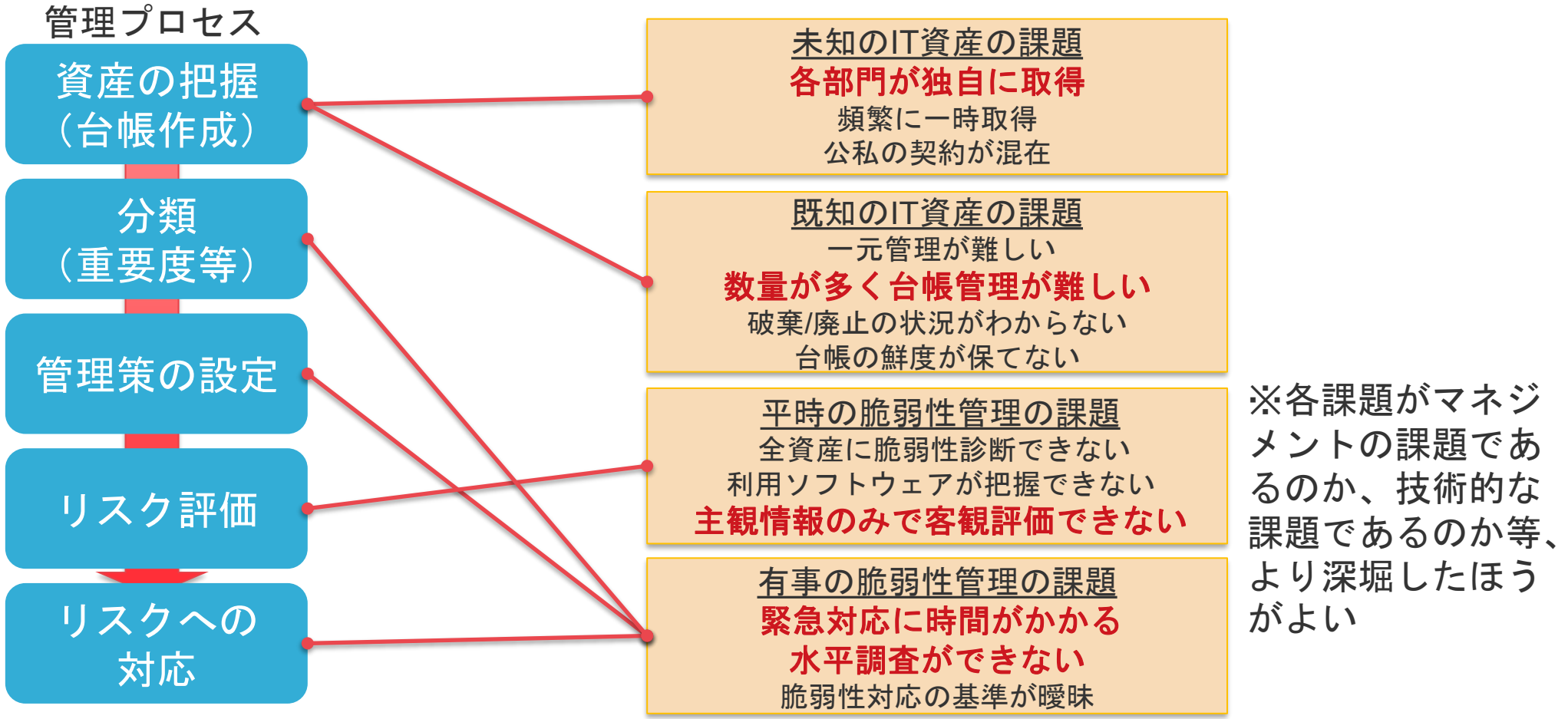
第3章：ASM導入が必要であるかの判断

現在の管理方法での課題を確認



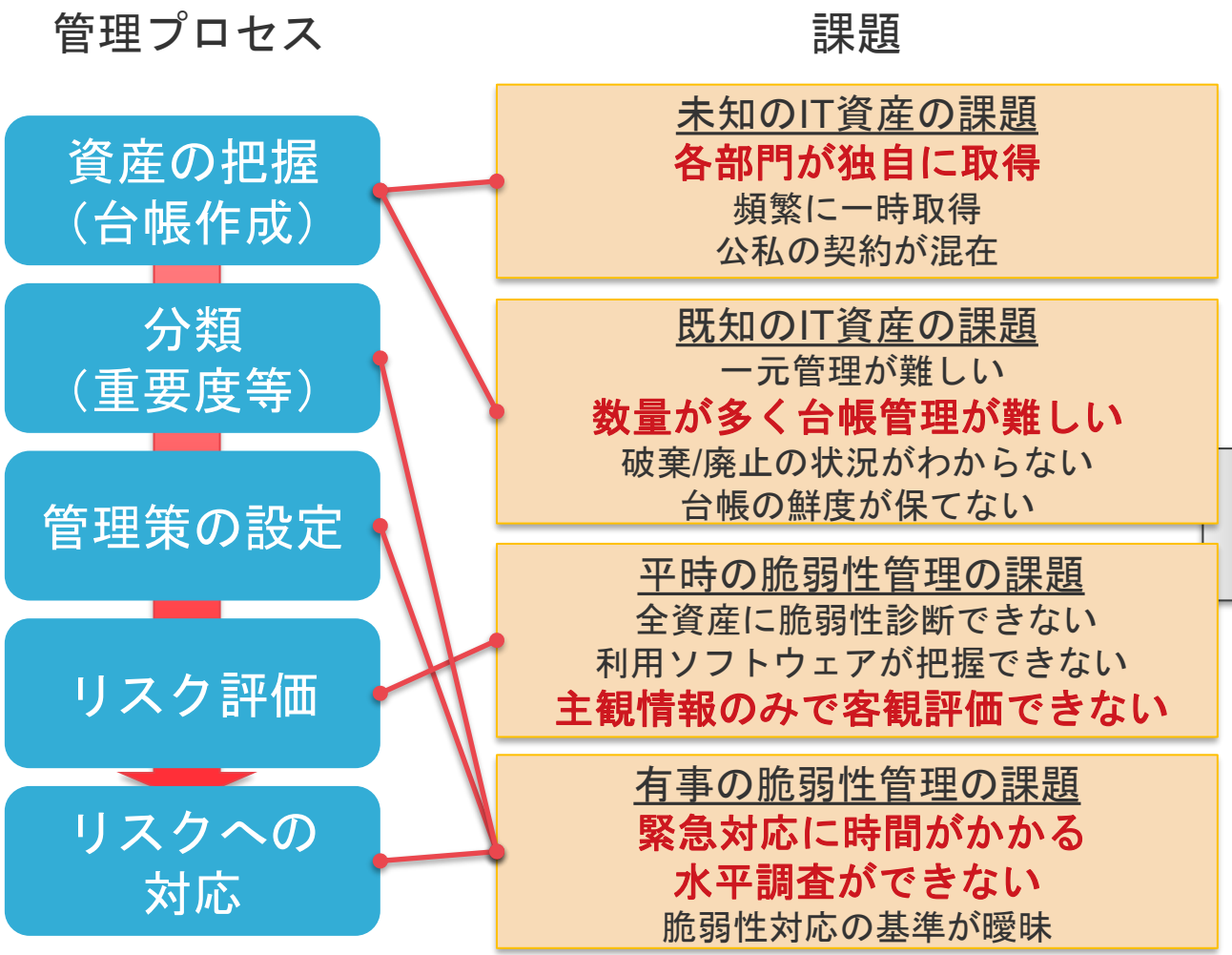
※各課題がマネジメントの課題であるのか、技術的な課題であるのか等、より深堀したほうがよい

現在の管理方法での課題を確認



※各課題がマネジメントの課題であるのか、技術的な課題であるのか等、より深堀したほうがよい

ASMに求めることを明確にする

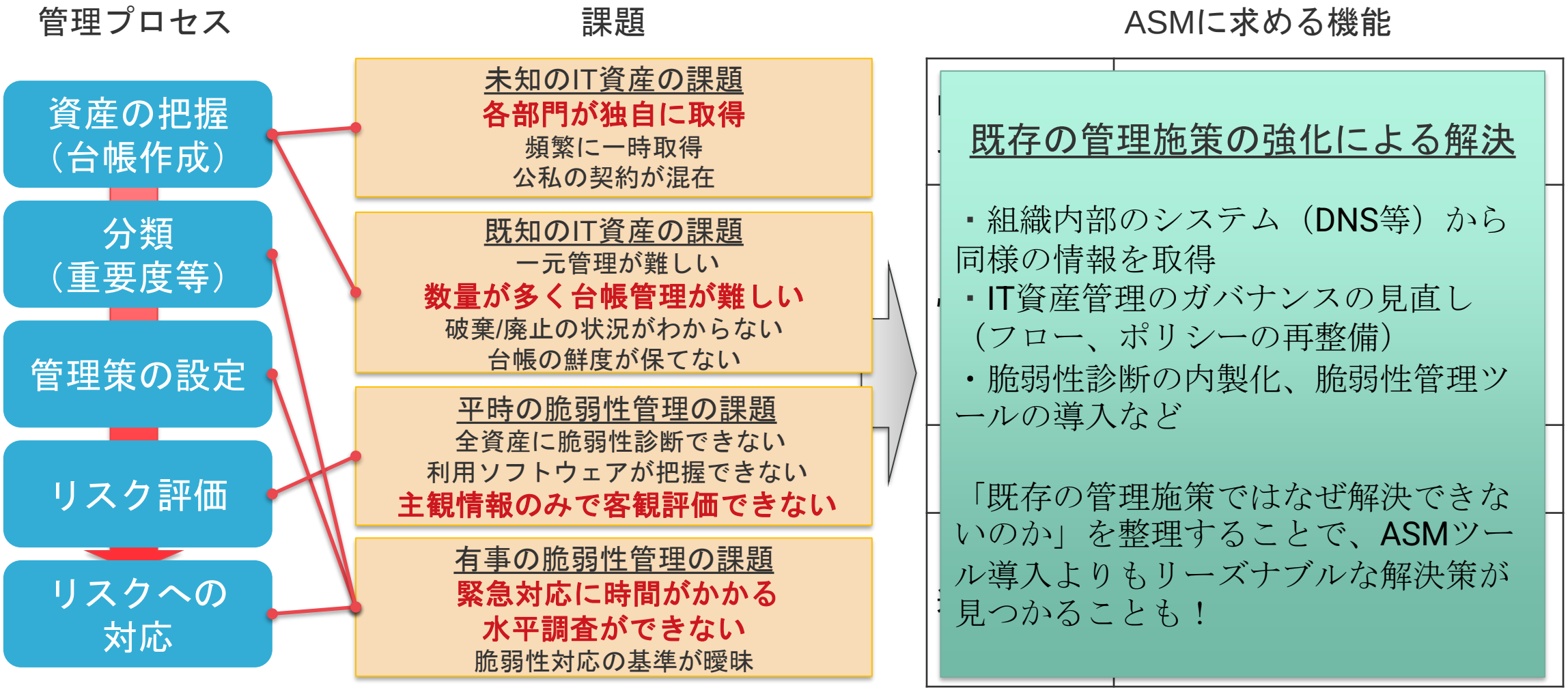


ASMに求める機能

IT資産の発見	・ドメインからFQDN一覧を発見すること ・FQDNと紐付くIPアドレスを発見すること ・組織名からドメインを発見すること
情報収集	・IT資産にアクセス可能なポート、製品、ライブラリ等を検出すること ・検出した内容からIT資産の用途を推測できること ・バージョン情報を収集すること ・検出結果の履歴を持つこと ・再現方法が提示されていること ・修正方法が提示されていること
リスク評価	・利用している脆弱性情報 ・リスクが提示されていること ・CVSS/EPSS等が提示されていること
運用面	・IT資産の除外ができること ・検出結果へ誤検知等のマーキングができること ・検出結果への対応ステータスを設定できること ・キーワードで検索できること

※記載内容は特定の製品を想定していない例です

本当にASMが必要か？を確認



※記載内容は特定の製品を想定していない例です

第4章：ASMツール/サービスの選定

選定のポイント
機能＋運用を見越した要件設定が重要

主要機能

IT資産の発見	・ドメインからFQDN一覧を発見すること ・FQDNと紐付くIPアドレスを発見すること ・組織名からドメインを発見すること
情報収集	・IT資産にアクセス可能なポート、製品、ライブラリ等を検出すること ・検出した内容からIT資産の用途を推測できること ・バージョン情報を収集すること ・検出結果の履歴を持つこと ・再現方法が提示されていること ・修正方法が提示されていること
リスク評価	・利用している脆弱性情報 ・リスクが提示されていること ・CVSS/EPSS等が提示されていること
運用面	・IT資産の除外ができること ・検出結果へ誤検知等のマーキングができること ・検出結果への対応ステータスを設定できること ・キーワードで検索できること

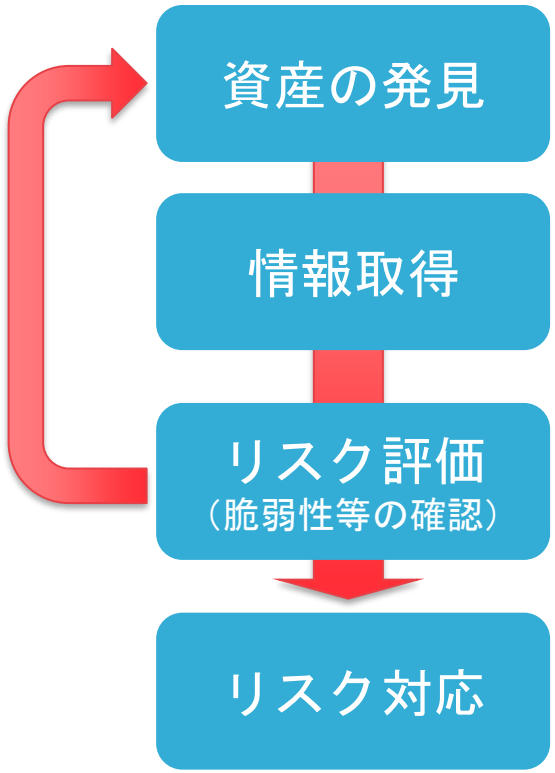
運用支援機能

報告・レポーティング	ダッシュボード機能 レポート機能
資産管理	IT資産の登録機能（追加機能） 他システム連携機能
組織管理	担当者の管理機能 タスク管理機能 通知機能/コミュニケーション機能 監査機能

※記載内容は特定の製品を想定していない例です

選定のポイント
ASMツール/サービスの注意点

ASMのプロセス



	注意点（例）
IT資産の誤検出	・存在していない資産の発見 ・自組織と関係ない資産の発見
IT資産の検出方法（探索範囲）	・どのように資産を検出しているか ・高精度＝探索範囲が狭くないか？
情報取得（スキャン）のタイミング	・誤検出と自動スキャンの関係 ・攻撃性の強いスキャンの実施
リスク評価（スキャン内容）と正確性	・全ての脆弱性は特定できない ・高精度＝EASMの場合、攻撃性が高い可能性
リスク対応	・問題発見の根拠情報があるか ・対策に必要な情報が揃っているか
料金体系	・金額算出の根拠は何か？（組織規模、組織数、ドメイン数、利用機能など）

導入して終わりではなく始まり

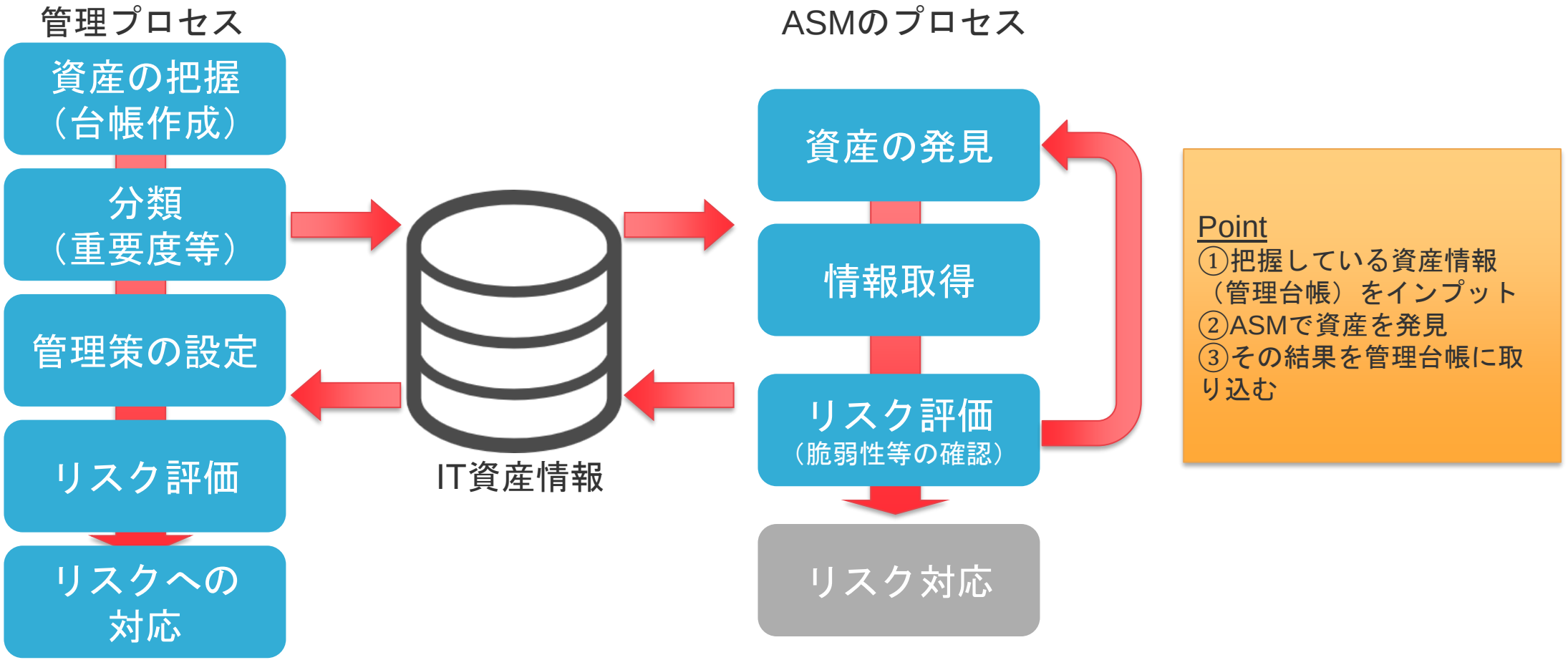
運用上の負担も事前に確認

- **未把握のIT資産や脆弱性が大量に検出されると運用負荷が高くなる**
- **具体的な運用負荷を確認するために、購入前のトライアルを推奨します**
- **運用における観点は第5章も参考**

第5章：ASMの運用体制の構築

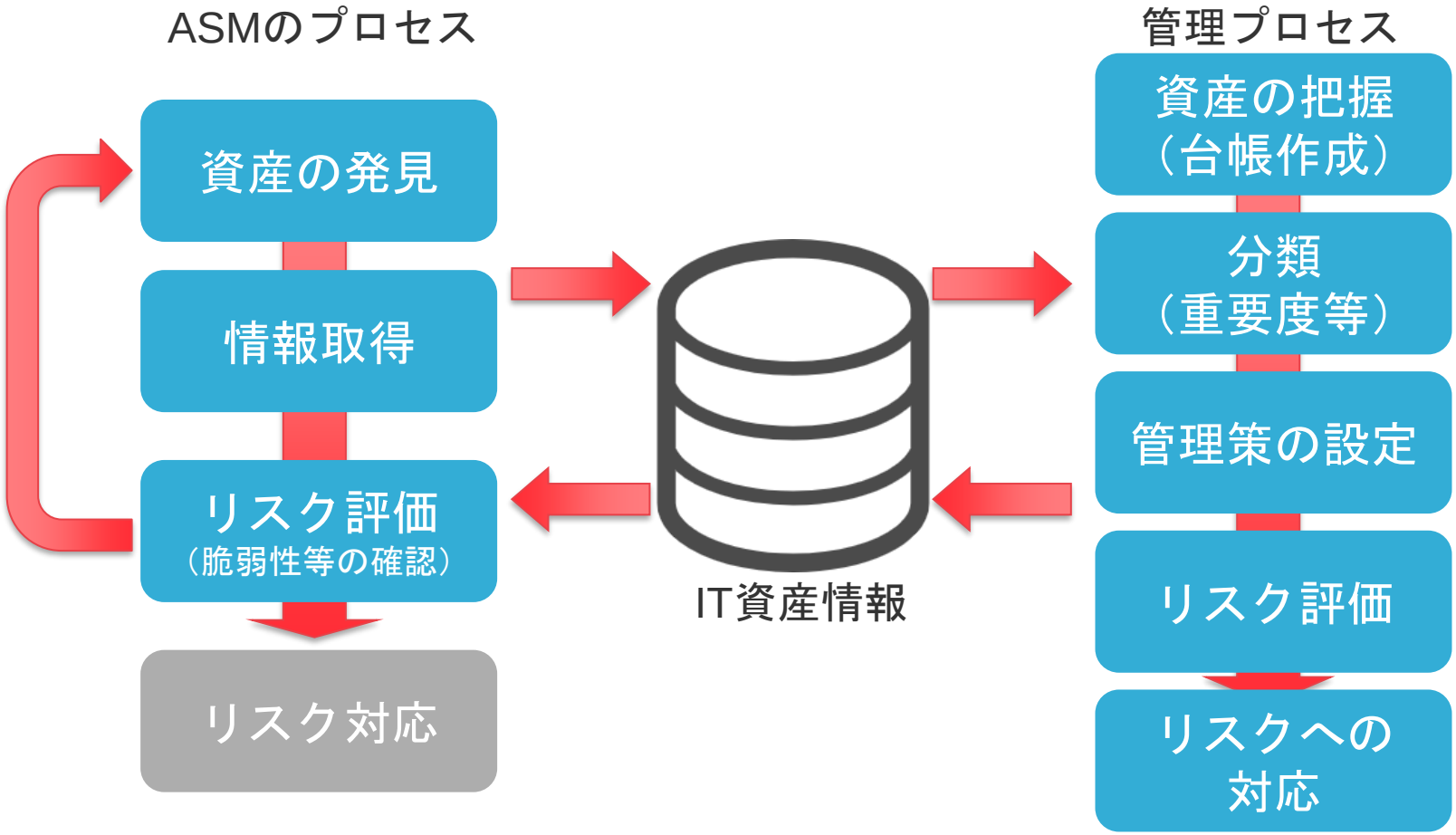
ASMは運用してこそ価値を発揮

ASMを従来の管理プロセス（＝自社の運用）と組み合わせることが重要
管理プロセス（管理策）がない場合、予め決定しておく



ASMから始めるのも手段の１つ

管理台帳的なものが存在していない場合は、ASMツール/サービスから始める手もある



Point
ASMから始める場合、最初は管理者情報がほとんど無い状態。予め主管や対応方針（行使してよい権限）を決めておくことが重要。

ASMで発見された後の対応

未把握のIT資産に対する対応

- 自組織と関係ないIT資産の除外
- 把握していないIT資産は、管理者を特定するための準備が必要
- よく発見される対象は・・・
  公開Webサーバー
  勝手に接続されたなにか
  忘れ去られているシャドーIT

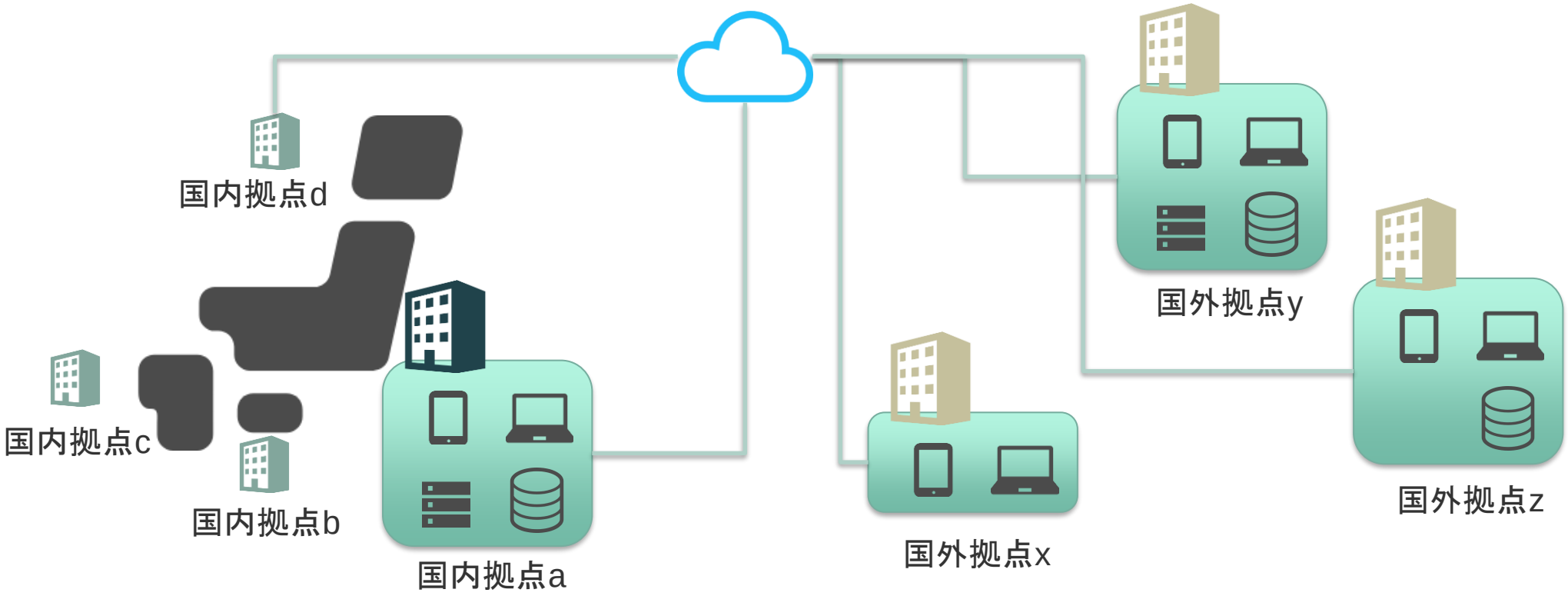
脆弱なIT資産に対する対応

- 誤検知の除外
- 脆弱性の対応優先度
- 対応する場合の修正対応の依頼フロー
- 対応後の脆弱性のステータス管理・追跡

第6章：ASM活用事例

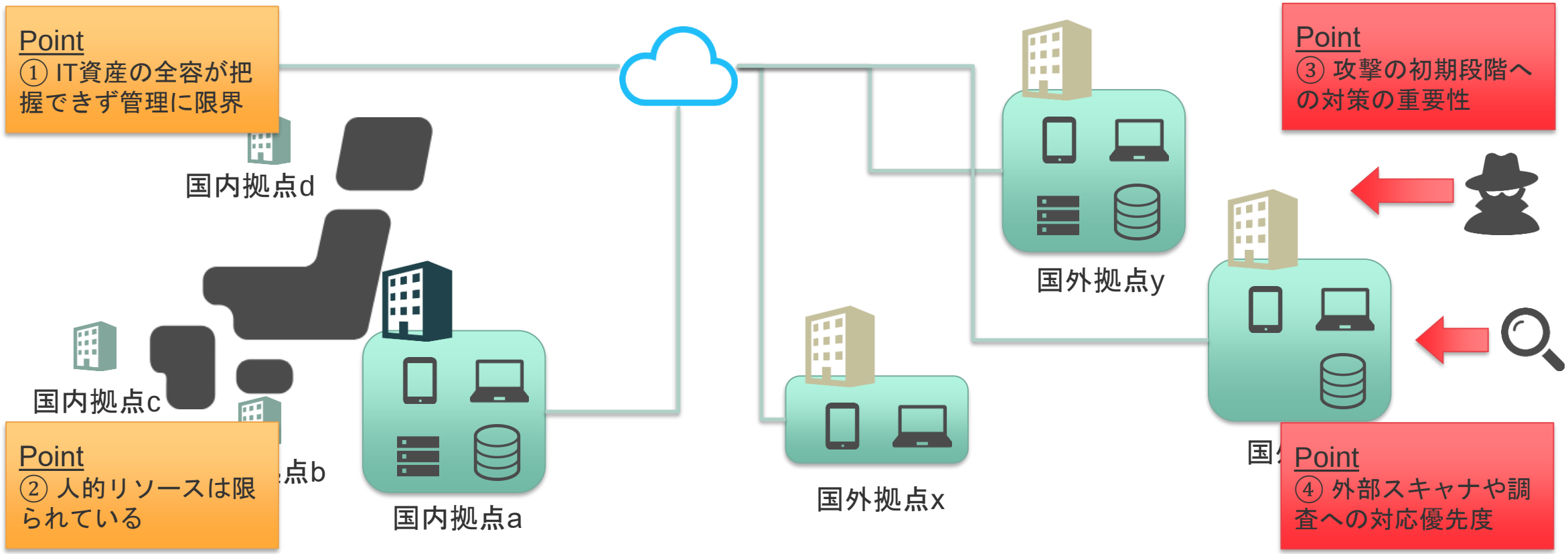
企業Aは国内外で多種サービスを利用

▶アセット管理は、国内事業はある程度統制し（全容は未把握）、海外グループは各自にお任せ
▶オンプレ、クラウド環境が事業ニーズに応じて利用されており、現場運用に依存



課題を整理して対応方針を決定

▶アセット管理は、国内事業はある程度統制し（全容は未把握）、海外グループは各自にお任せ
▶オンプレ、クラウド環境が事業ニーズに応じて利用されており、現場運用に依存



課題を整理して対応方針を決定

- アセット管理は、国内事業はある程度統制し（全容は未把握）、海外グループは各自にお任せ
- オンプレ、クラウド環境が事業ニーズに応じて利用されており、現場運用に依存

導入後の振り返り

▶導入効果（Good）

- IT資産の可視性が向上した
- 事前にコミュニケーションパスやリスクレベル、対応範囲、対象者への周知を実施したためハレーションが発生しなかった
- 運用プロセスを回せ、関係者のセキュリティに対する理解が向上した

▶改善・反省点（Bad）

- ASMは銀の弾丸ではない：検知漏れ、資産管理、サービス品質
- リスクが顕在化しないと効果訴求が困難：費用対効果
- IT資産への負荷はモニタリングが必要
- 運用負荷の改善が必要：誤検知、再検知、コミュニケーション

トリアージへ

02

組織に適したトリアージガイドラインを作るための『脆弱性トリアージガイドライン作成の手引き』

「ASM」と「脆弱性トリアージ」

２つのテーマはIT資産の管理プロセス上で関係性が強い

ASM（アタックサーフェスマネジメント）

IT資産の管理やリスク評価（資産、脆弱性の検出）
発見されたIT資産や脆弱性への対応

ASM導入検討を進めるためのガイダンス（基礎編）

本ドキュメントの目的

「Attack Surface Management（ASM、攻撃対象領域管理、攻撃表面管理）」への注目が高まるとともに、様々なサービスやドキュメントが登場しています。
しかし、「ASM」には複数の取り組み方法が存在し、用語の定義やドキュメントを解釈するのが難しく、「ASM」を活用したい組織が目的に沿ってツールやサービスを見分けることが難しくなっています。

本ドキュメントは、「ASM」に関連する用語や活用方法を理解し、目的に沿ったサービスを選定することや、既存のドキュメント（様々な組織が作成したドキュメント）を読み解く上で助けとなる情報の提供を目的としています。

執筆者一覧

執筆者

- 大塚 淳平（NRIセキュアテクノロジーズ株式会社）
- 洲崎 俊（三井物産セキュアディレクション株式会社）
- 高江洲 勲（三井物産セキュアディレクション株式会社）
- 吉川 允樹
- 平田 優
- 幸田 将司（株式会社バラエナテック）
- 岩間 湧（株式会社セキュアスカイ・テクノロジー）
- 山口 凌（株式会社セキュアスカイ・テクノロジー）

脆弱性トリアージ

脆弱性情報や脆弱性診断結果への
対応方針の決定（トリアージ）

脆弱性トリアージガイドライン作成の手引き

Guidance on developing vulnerability triage guidelines.

by 脆弱性診断士スキルマッププロジェクト

本ドキュメントは「**組織が脆弱性に適切に対応することを目的として、脆弱性診断を実施した際に提供された報告書に記載された脆弱性対応の優先順位付け（トリアージ）を行うために、その組織に適したトリアージガイドラインを作成するための手引き**」です。

組織においてセキュリティ対応を行うためのリソースは限りあるものです。 そのため、発見されたすべての脆弱性に対応できるとは限りません。 限りあるリソースを最大効率で活用するためには、適切に優先順位を付けて対応していく必要があります。

第１章では、対応基本方針の策定について説明しています。 この段階でのトリアージ基準は、高い専門知識を持っていない人でも判断できる程度の基準にとどめています。 それにより迅速に優先順位付けができるようになり、また優先度について関係者全体の意識をある程度揃えることができます。 ただし、簡易的な判断基準であるため、攻撃による実際のリスクとの乖離がある可能性があります。

第2章では、トリアージの精度向上のために考慮するポイントについて記載しています。

第3章では、トリアージの精度向上に活用できるフレームワークを紹介しています。

第4章では、トリアージ実施後の修正コストや例外対応について記載しています。

第5章では、トリアージにまつわる事例を紹介しています。

テンプレート

本ガイドラインの第1章を使用して作成したサンプルのガイドラインは下記になります。 テンプレートなどにご活用下さい。

- 脆弱性トリアージガイドライン・テンプレート

脆弱性トリアージとは

発見された複数の脆弱性を評価し

その重要度や緊急性に基づいて優先順位を付け

対応の順序を決定するプロセス

医療分野のトリアージと同様に
限られたリソースを最も効果的に配分することが重要

脆弱性トリアージガイドライン作成の手引き

組織が脆弱性に適切に対応することを目的として、脆弱性診断を実施した際に提供された報告書に記載された脆弱性対応の優先順位付け（トリアージ）を行うために、**その組織に適したトリアージガイドラインを作成するための手引き**

2024年05月　1章公開
2024年11月　フル版公開

https://github.com/WebAppPentestGuidelines/TriageGuidelines/

目次

- **1章トリアージガイドラインの作成**
  - 最低限のトリアージ体制を作る
- **2章 トリアージの精度向上**
  - 脆弱性の影響範囲などを考慮して精度を向上
- **3章 トリアージに利用できるフレームワーク**
- **4章トリアージ後の対応**
  - 修正コストの試算と対応。例外の想定
- **5章 事例**

今日はここがメイン

脆弱性の認知/検知時の対応判断フロー

1. 実際に脆弱性の影響を受けるのか、その範囲はどの程度なのかを分析
2. 脆弱性の危険度や対象の重要度などからリスクを評価
3. 対象の脆弱性の対応方針を決定

- 各要素について対応判断毎に検討するよりも、対応方基本方針（ガイドライン）として、評価や判断時の基準を決めておくことで、脆弱性認知/検知時に円滑に対応することが可能となる

トリアージガイドライン運用のためのフロー

① 最低限のトリアージ体制を作る

- 第１章では、対応基本方針の策定について説明
- 高い専門知識を持っていない人でも判断できる程度の基準
- 迅速な優先順位付け、関係者全体の意識を揃えることがでる
- ただし、実際の攻撃によるリスクと乖離する可能性がある

② トリアージの精度を向上させる

- 第２章以降では、高度な専門知識をもった人がリスク判定の精度を上げるための手法について説明する

ガイドラインは一度作成したものを使い続けるのではなく、脆弱性対応が完了した後に、改善点を踏まえ、アップデートすることを推奨

迅速に最低限のトリアージが可能な体制を構築する

- **良い点**
  - 脆弱性やリスク評価に関する専門知識がなくても、素早くトリアージを行うことができる
  - 主観的な判断が入らず、誰がトリアージしても同じ結果となる

- **悪い点（２章の対応で解消）**
  - 攻撃コードの存在の有無などによって、実際に脅威が発生するリスクと乖離する可能性がある
  - 素早くトリアージを行うことができる反面、対応しなければならない脆弱性が多くなり、対応が過剰になる可能性がある

関係者の役割と適用範囲の決定

- **関係者の役割と責任範囲を明確にする**
  - 明確でない場合、脆弱性対応時の判断に遅れが生じたり、情報共有や対応の連携に手間取る場合がある
- **トリアージガイドラインの適用範囲の決定**
  - このガイドラインをどの範囲のシステムに適用するのか
  - システムの重要度によって基準が異なることがある

トリアージで決めるべきこと

対応優先度 = 対象資産の重要度 × 脆弱性の危険度

- 対象の重要度評価
- 脆弱性の危険度評価
- 対応の優先度を決める
- 対応の要否と期限を決める

対象の重要度評価の例

- **資産の種類に基づく分類**
  - 高: 金融データ、顧客情報、特許性を有する製品や技術情報
  - 中: 業務データ、従業員の勤怠情報
  - 低: ホームページ等で既に公開されている情報
- **影響度の規模（利用者の規模）に基づく分類**
  - 高: 利用者数1万人以上
  - 中: 利用者数1000人以上
  - 低: 利用者数1000人未満
- **利用者層に基づく分類**
  - 高: 官公庁利用者(政府調達等)
  - 中: 技術者、システム管理者、企業の担当者
  - 低: 一般の利用者(BtoCのサービス等)

脆弱性の危険度評価の例

- **評価方針の設定**
  - 脆弱性の危険度評価のために、CVSS基本値や脆弱性診断事業者が提供する危険度評価を参考にし、各評価を基に脆弱性の緊急度を分類
    - CVSSの「攻撃元区分」「攻撃条件の複雑さ」「攻撃前の認証要否」など、から特に重視する項目があれば基準の一つとしても良い

- **危険度評価の定義例 (3段階の場合)**
  - 高：CVSS 7.0 - 10.0
  - 中：CVSS 4.0 - 6.9
  - 低：CVSS 0.0 - 3.9

対応の優先度を決める

- 脆弱性の危険度評価と対象の重要度評価から、優先度マトリックスを作成して対応の優先度を決める

	重要度 高	重要度 中	重要度 低
危険度 高	緊急	高	中
危険度 中	高	中	低
危険度 低	中	低	低

対応の要否と期限を決める

対応の要否判断の例

- 脆弱性の危険度を基準に判断
- 資産や規模の影響度を基準に判断
- 攻撃の影響をすぐに受けるかを基準に判断

対応期限の例

- 何日以内にやるかなど日数
- 毎月の月末にやるなど特定の時期
- 影響度合い
- 即時、次回メンテナンスなどイベント単位

優先度マトリックスの例

CVSS	高	中 (30日以内)	高 (10日以内)	緊急 (5日以内)
	中	低 (90日以内)	中 (30日以内)	高 (10日以内)
	低	低 (90日以内)	低 (90日以内)	中 (30日以内)
		低	中	高
		資産重要度		

脆弱性の管理方法

- **記録すべき情報**
  - 脆弱性概要/名称/CVE番号(公開されている脆弱性の場合のみ)
  - 対象情報
  - ステータス(未対応/対応済/保留/対応しない など)
  - 対応期限
  - トリアージ結果（区分・危険度・優先度）
  - 起票日
  - 対応完了日/対応しないことを決めた日
  - 担当者
  - 対応方針(例外対応が発生する場合はその内容も含む)
  - 対応の記録（対応実施日、対応実施内容）

脆弱性の管理方法

- **管理方法**
  - EXCEL
  - GithubのissueやProject
  - Jira
  - OWASP Defectdojo
  - 普段使っているツール（Slack、Teamsなど）

テンプレートもあるよ!!

トリアージガイドライン【テンプレート】

1. 総則

1.1 本ガイドラインの目的

本ガイドラインは、〇〇株式会社（以下当社）で新規開発するシステムや運用中のシステムについて、脆弱性診断や外部からの報告などにより実際に脆弱性の存在が発覚した場合に、そのトリアージ（対応優先度の判断）や対応方針を事前に定めておくことによって、迅速かつ正確な脆弱性対応をすることを目的とします。 なお、日々公表されている脆弱性情報の収集や、その影響有無や範囲の確認の手順等については、本ガイドラインの対象外です。

1.2 役割と責任

本ガイドラインにおける役割と責任は次のとおりです。

1. CISO CISOは、当社規程の定めに従い任命されます。 CISOは、当社が開発・運用するすべてのシステムについて、リスク管理の責任を負います。インシデント対応や準備に対してかかる費用についての全決裁権を持つものとします。
2. セキュリティ統括室 セキュリティ統括室は、各事業部門のシステムで発覚した脆弱性や対応状況について、管理・監督する責任を負います。 本ガイドラインで定めた対応方針とは異なる対応を行う必要がある場合、セキュリティ統括室が判断・承認するものとします。
3. システム管理責任者 マネージャ以上の役職者とし、対象システムに応じて所管部門から選出します。 対象システムの管理業務の推進と維持管理に必要な実務全般の判断・承認の責任を負います。 システム管理責任者は、本ガイドラインに沿ってトリアージを行い、脆弱性対応を行い、結果及び対応状況をセキュリティ統括室に報告する責任を負います。
4. システム管理担当者 システム管理責任者の指示のもと、対象システムの管理業務の推進と維持管理に必要な実務作業を担当します。

2章 トリアージの精度向上

２章では、１章の基本的な判断基準で簡易的な評価に、攻撃可能性やビジネス影響、組織に適した評価を行いトリアージの精度を向上する

▶精度向上のために考慮するポイント

- 脆弱性の影響範囲
  - システム構成や攻撃シナリオの理解
- 脆弱性の前提条件
  - 脆弱性が特定のモジュールや設定に依存する
- Exploitの流通状況
  - 悪用する攻撃コードの流通状況
- Exploitの実現性
  - 攻撃を実行できる人の数やスキルなど

3章 トリアージに利用できるフレームワーク

活用できるフレームワーク

- CVSS
  - 脆弱性の深刻度を数値化するためのフレームワーク
- SSVC
  - 脆弱性管理を目的とした決定木モデルに基づくフレームワーク。組織の特性やニーズに応じた具体的な対応方針を導き出すことが可能。
- EPSS
  - 今後30日以内に脆弱性が悪用される蓋然性を一定の計算式によって算出するもの。
- SBOM
  - ソフトウェア製品に含まれるコンポーネント(部品)をリスト化し管理
- CISA KEVカタログ
  - 悪用が観測された脆弱性の一覧をまとめたカタログ
- OWASP Risk Rating Methodology
  - アプリケーションセキュリティに特化

4章 修正コストについて

- **脆弱性の対応とコスト**
  - 対策の際には修正コストを把握する
  - 修正コストが、経済的な損失を大きく上回る場合には修正以外の対応方法を検討する
- **例外対応の想定**
  - 修正が難しい場合には、期限を設定したうえで緩和策など例外的な対応などを想定しておく
  - どのようなフローで決定するのか事前に決めておく

5章 事例

- **トリアージを取り入れ運用し発生した事例**
  - 脆弱性対応フローが明確化されていなかった組織事例
  - ビジネスインパクトを考慮した結果優先度が下がった事例
  - 経営者の指示による優先度変更

質問やコメントの受付

- **本講演に関するご質問やご意見を以下で受け付けます。**
- **講演終盤で頂いたご質問に回答します。**
  （時間の都合で割愛する可能性もあります）

① **https://www.menti.com/**　にアクセス
② コードに **1372 4549** を入力

簡単なアンケートのあとに
質問（自由入力）が可能です
※回答者の情報や属性は取得していません

ご静聴ありがとうございました