実務に活かせるガイドラインを目指して ISOG-J WG I 2024年度の成果紹介

日本セキュリティオペレーション事業者協議会
ISOG-J WG I

2025.7.24

アジェンダ

- ISOG-J WG1とは？
- 2024年度の成果物とポイント
  - ASM導入検討を進めるためのガイダンス
  - 脆弱性トリアージガイドライン作成の手引き
  - Newtechネタ（何かあれば）
- まとめ、今後に向けて

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(親団体はJNSA。オブザーバーに総務省と経済産業省)

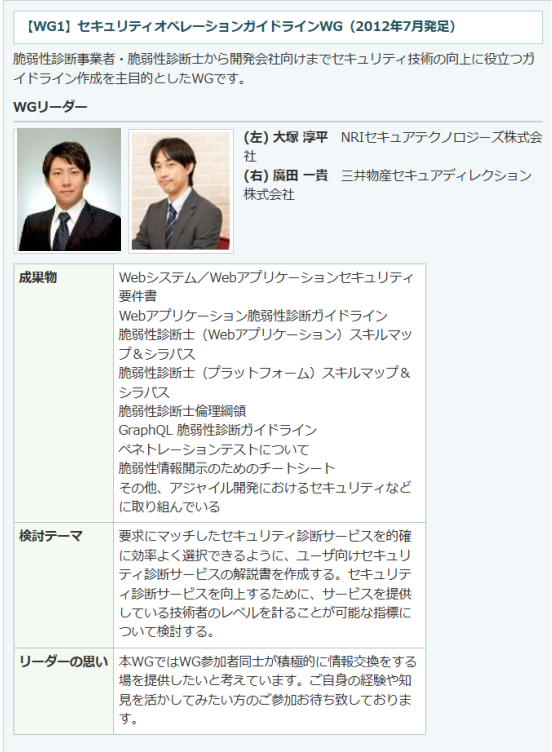
代表：武智 洋(日本電気株式会社)
副代表：阿部 慎司(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：早川 敦史(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：武井 滋紀(SCSKセキュリティ株式会社)

セキュリティオペレーションガイドラインWG (WG1)	大塚 淳平(NRIセキュアテクノロジーズ株式会社) 廣田 一貴(三井物産セキュアディレクション株式会社)
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(SCSKセキュリティ株式会社)

ISOG-J WG1とは

▶日本セキュリティオペレーション事業者協議会
- 通称：ISOG-J
- セキュリティオペレーションサービスの普及
- サービスレベルの向上
- セキュリティ事業者同士で協力して推進

▶セキュリティオペレーションガイドラインWG
- 通称：WG1
- OWASP Japanと連携！
- 主に脆弱性診断/ペネトレーションテスト に関するドキュメント（ガイドライン）を策定
- 最近では脆弱性トリアージやASMにも注目
- 2025年度リーダー交代



【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

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。

2024年度の主な成果物

WG1

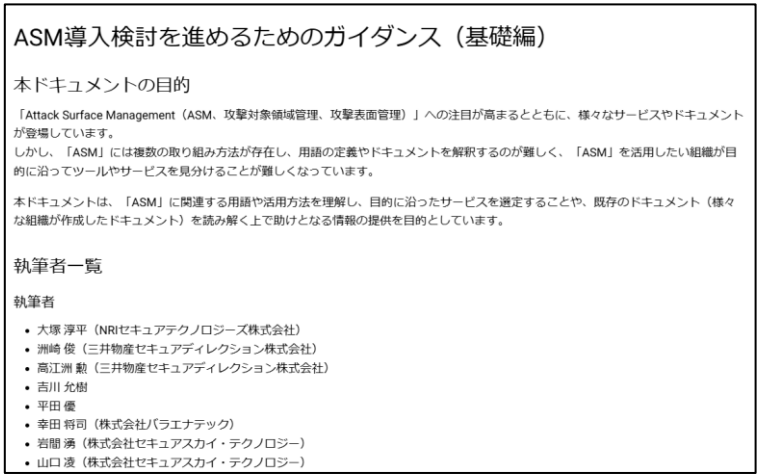
2024年5月、脆弱性トリアージガイドライン作成の手引き(1章まで)
2024年11月、ASM導入検討を進めるためのガイダンス(基礎編)
2024年11月、脆弱性トリアージガイドライン作成の手引き(2章以降)

「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。

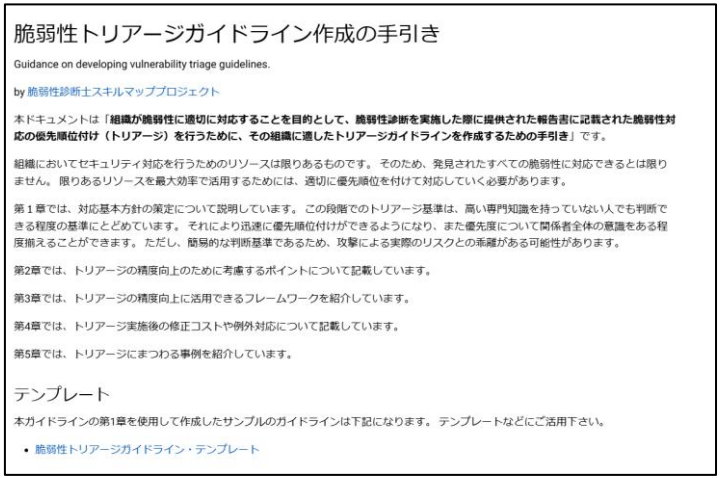
執筆者一覧

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（株式会社パラエナテック）
- 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。

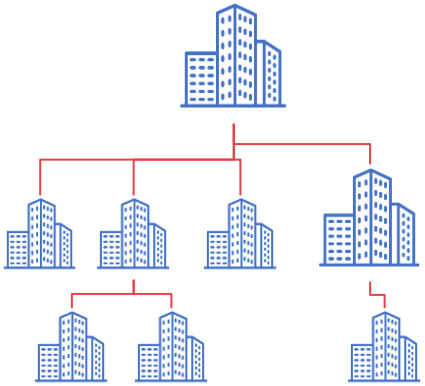
テンプレート

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」が必要とされる背景（課題）

企業



DXの進展（デジタル革命）

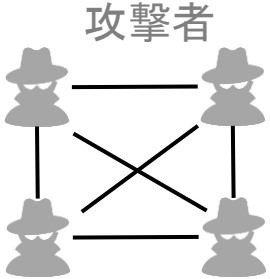
テレワーク積極活用

クラウド利用拡大

①管理しきれないIT資産

攻撃者

③狙い目増による攻撃の効率性



組織化/分業体制

②大量の脆弱性

「ASM」は解決策として注目

ASMとは
「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

知見や実務として取り組んでいる人
＝セキュリティ事業者同士で協力して整理しよう

「ASM導入検討を進めるためのガイダンス」

第1章：はじめに
第2章：Attack Surface Management（ASM）とは何か
第3章：ASM導入が必要であるかの判断
第4章：ASMツール/サービスの選定
第5章：ASMの運用体制の構築
第6章：ASM活用事例
コラム

https://wg1.isog-j.org/ASMGuidance/

「脆弱性トリアージ」

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

脆弱性診断の結果を受け取った後の判断についての悩みをよく聞く
＝セキュリティ事業者同士で協力して整理しよう

「ASM導入検討を進めるためのガイダンス」

第1章：トリアージガイドラインの作成
　→最低限の体制を作る
第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
第3章：トリアージに利用できるフレームワーク
第4章：トリアージ後の対応
　→修正コスト試算や対応。例外の想定
第5章 事例
テンプレート

https://wg1.isog-j.org/TriageGuidelines/

「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」更新！

By Newtechグループ

雑多に書きたいことを書いた診断手法ドキュメント

- human readableではないパラメータとの向き合い方（仮）（新規）
- SSRF（新規）
- Web Cache Poisoning
- 意図しないサインアップ経路の存在

https://wg1.isog-j.org/newtechtestdoc/

「今後に向けて」

▶セキュリティオペレーションガイドラインWG（通称：WG1）

- 脆弱性診断/ペネトレーションテストなど攻撃者目線での評価に関するドキュメント（ガイドライン）を策定
- 用語やサービスの「曖昧、難しい」を「わかりやすく」、「使える」を目指す

▶直近のテーマ・活動（成果）

- 脆弱性情報開示のためのチートシート更新 ※OWASPのドキュメントの翻訳
- ドキュメントのメンテナンス（CI周り、データ移行等）

ISOG-J WG1の活動成果を是非ご活用ください！
活動自体に興味がある方はISOG-Jまでご連絡ください！

ご静聴ありがとうございました