ISOG-J WG1

脆弱性トリアージガイドライン作成の手引き

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

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』

ISOG-J WG1 リーダー
株式会社トライコーダ 上野 宣

01 脆弱性トリアージとは

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

脆弱性トリアージには何が必要なのか？

- **適切なトリアージを行うためには明確な判断基準が必要**
- **脆弱性の取扱はあなた自身で判断する必要がある**

- 組織のリソースは限りあるもの
- 発見されたすべての脆弱性に対応できるとは限らない
- 適切に優先順位を付けて対応していく必要がある

02 脆弱性トリアージガイドライン作成の手引き

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5月公開

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

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（現在ここまで公開）
- 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（**予定**）

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

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		

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。

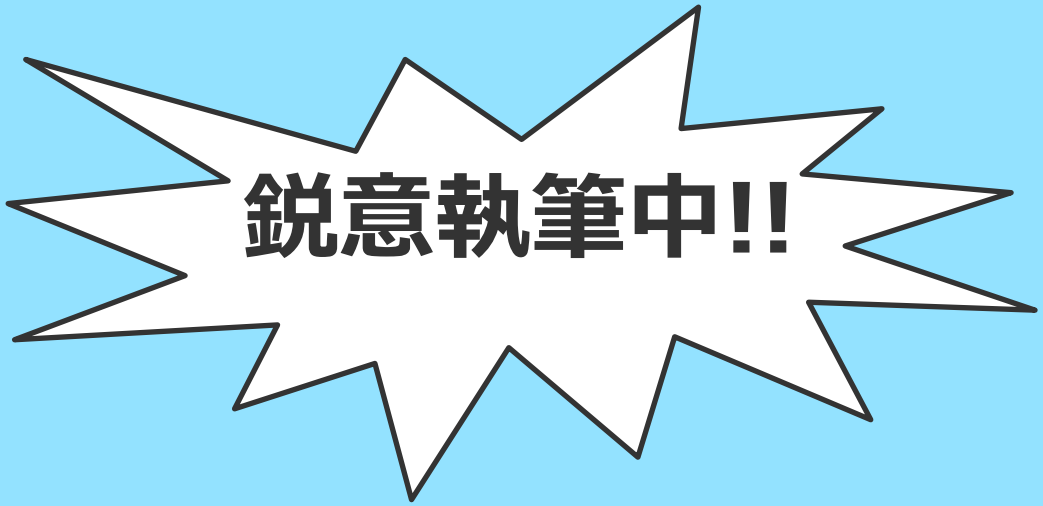
1.2 役割と責任

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章以降も乞うご期待!!

- **2章 トリアージの精度向上**
  - 脆弱性の影響範囲
  - 脆弱性の前提条件
  - Exploitの流通状況
  - Exploitを使う前提条件
  - Exploit開発の難易度
  - Infoで報告された脆弱性の扱い方



- **3章 トリアージに利用できるフレームワーク**
  - CVSS v2, v3.1, v4
  - SSVC
  - EPSS
  - SBOM
  - Known Exploited Vulnerability Catalog
  - Risk Rating Framework: OWASP Risk Rating Methodology
- **4章 対応について**
  - 恒久対策と暫定対策について
  - 修正コスト
  - 例外の想定
  - 事業影響
- **5章 事例**