トリアージの為の、組織体制と有用な指標

Hardening Designers Conference 2024
未解決の問題セッション4.トリアージの為の、組織体制と有用な指標

株式会社ラック
サイバー・グリッド・ジャパン
次世代セキュリティ技術研究所
井上圭

2024/07/06

Agenda

1. 概要
2. トリアージと組織体制
3. トリアージで有用な指標
4. トリアージの例
5. まとめ

Appendix

01 概要

上野さんから、トリアージそれ自体についての「トリアージガイドライン作成の手引き」についてお話があったと思います。

私のセクションでは、トリアージの周辺状況についてお話します。

- トリアージと組織体制
  - ITU-T X.1060 / セキュリティ対応組織の教科書を基に、体制検討の概要を示します
- トリアージで有用な指標
  - SSVC/EPSS/KEV Catalog/vulnrichment について、各指標の概要を示します
- トリアージの例
  - 上記氏表を用いたトリアージ方法について、トリアージ方針の概要を示します

02

トリアージと組織体制

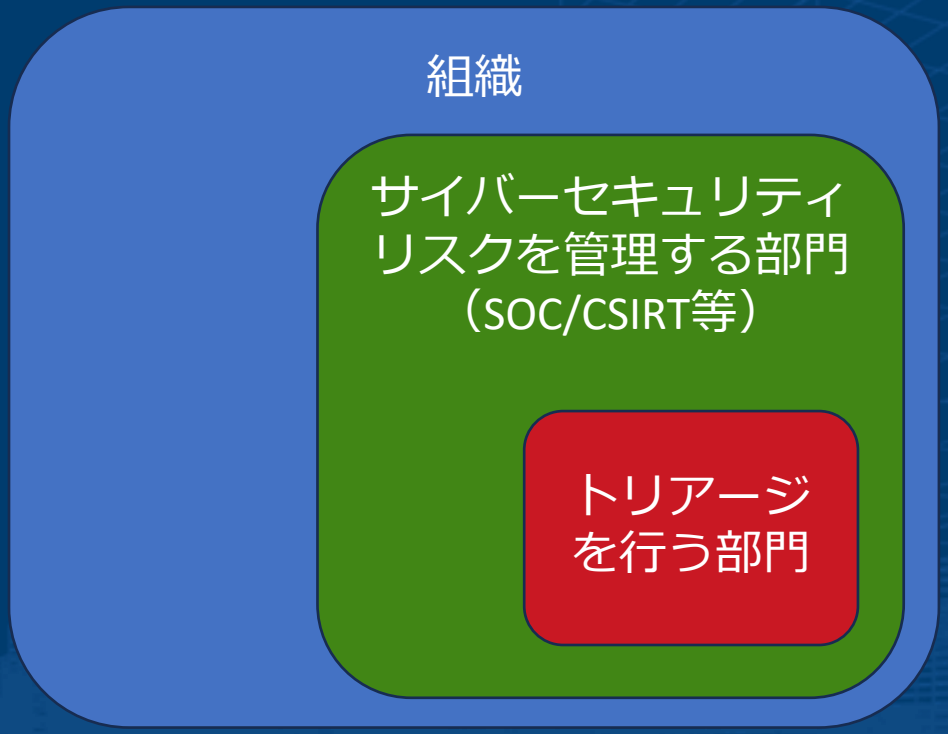
トリアージの、組織の中での位置づけ

組織には、サイバーセキュリティリスクを管理するための部門（例えばSOC/CSIRT等）があります。トリアージを行う部門は、一般的にその組織の配下に存在すると考えられます。

ここでは、「組織のサイバーセキュリティリスクを管理するための組織全体」を俯瞰しつつ、トリアージに必要な機能等について考えます。

- 現状の組織構成と比較し、考慮漏れや不足している機能がないかを確認することで、よりトリアージが行いやすい環境を整備できます。

組織のサイバーセキュリティ全体を考えるには、国連の専門機関ITU-T（国際電気通信連合電気通信標準化部門）で承認されたX.1060という勧告を参考にします。



サイバーセキュリティのフレームワーク X.1060

X.1060 Framework for the creation and operation of a cyber defence centre

- 国連の専門機関ITU-T（国際電気通信連合電気通信標準化部門）で承認された、業種や規模に関わらずさまざまな組織で利用できるサイバーセキュリティのフレームワークを定義した勧告文書です。
- 事業活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する組織内団体を、Cyber Defence Centre（以下「CDC」という）として呼称し、CDCが提供する「サービスの構築」「マネジメント」「評価」という3つのプロセスを循環させることにより、セキュリティ対策を推進します。
- X.1060は、主に日本のISOG-J（日本セキュリティオペレーション事業者協議会）に加盟する企業が中心になって執筆した「セキュリティ対応組織の教科書」を基にしています。
- X.1060は各国で使えるように詳細には踏み込んでいません。日本の場合は、ISOG-Jの「セキュリティ対応組織の教科書」で、より詳細に日本の状況に合わせて書かれています。

組織における関係者とその役割

まずは、組織における関係者とその役割を整理しましょう。

- CISO（最高情報セキュリティ責任者）
  - ➢ 経営にコミットした立ち位置で、セキュリティポリシーの決定などの意思決定を行う
- CDC（Cbyer Defence Centre: セキュリティ対応組織=SOC/CSIRTなど）
  - ➢ CISOから権限を付与され、セキュリティポリシーを実装する
- セキュリティチーム
  - ➢ 施策を実装する

組織体制としてはこれを参考とし、
次に実際のトリアージで使える指標を
示します。

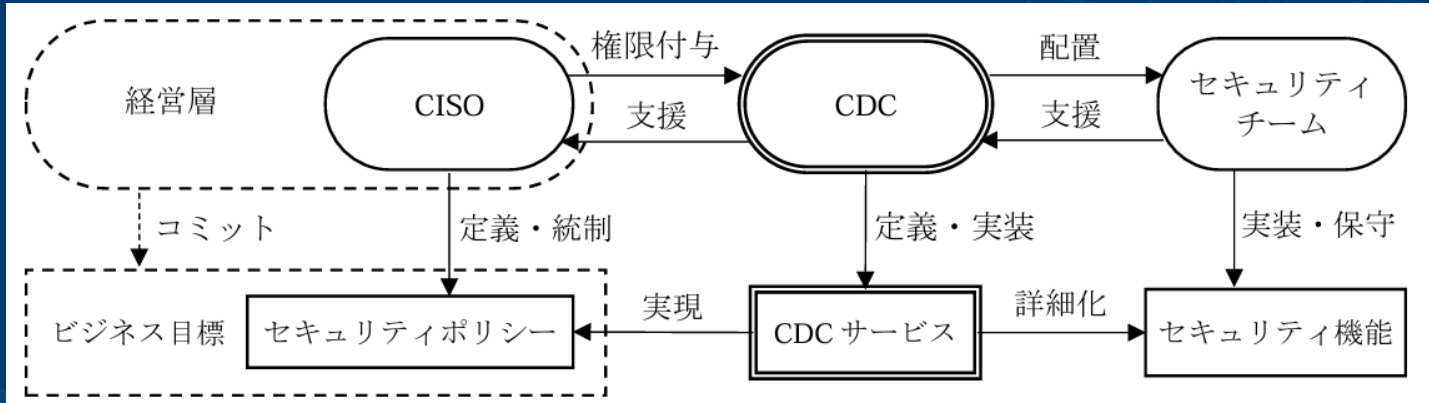


図 1　CDC の運営における関係者とその役割

実装すべきサービス

X.1060では、セキュリティ対応を行う組織が必要となる一般的なサービスリストを提供しています。

自組織での実装状況と比べてみてください。

- A. CDCの戦略マネジメント
- B. 即時分析
- C. 深堀分析
- D. インシデント対応
- E. 診断と評価
- F. 脅威情報の収集及び分析と評価
- G. CDCプラットフォームの開発・保守
- H. 内部不正対応支援
- I. 外部組織との積極的連携

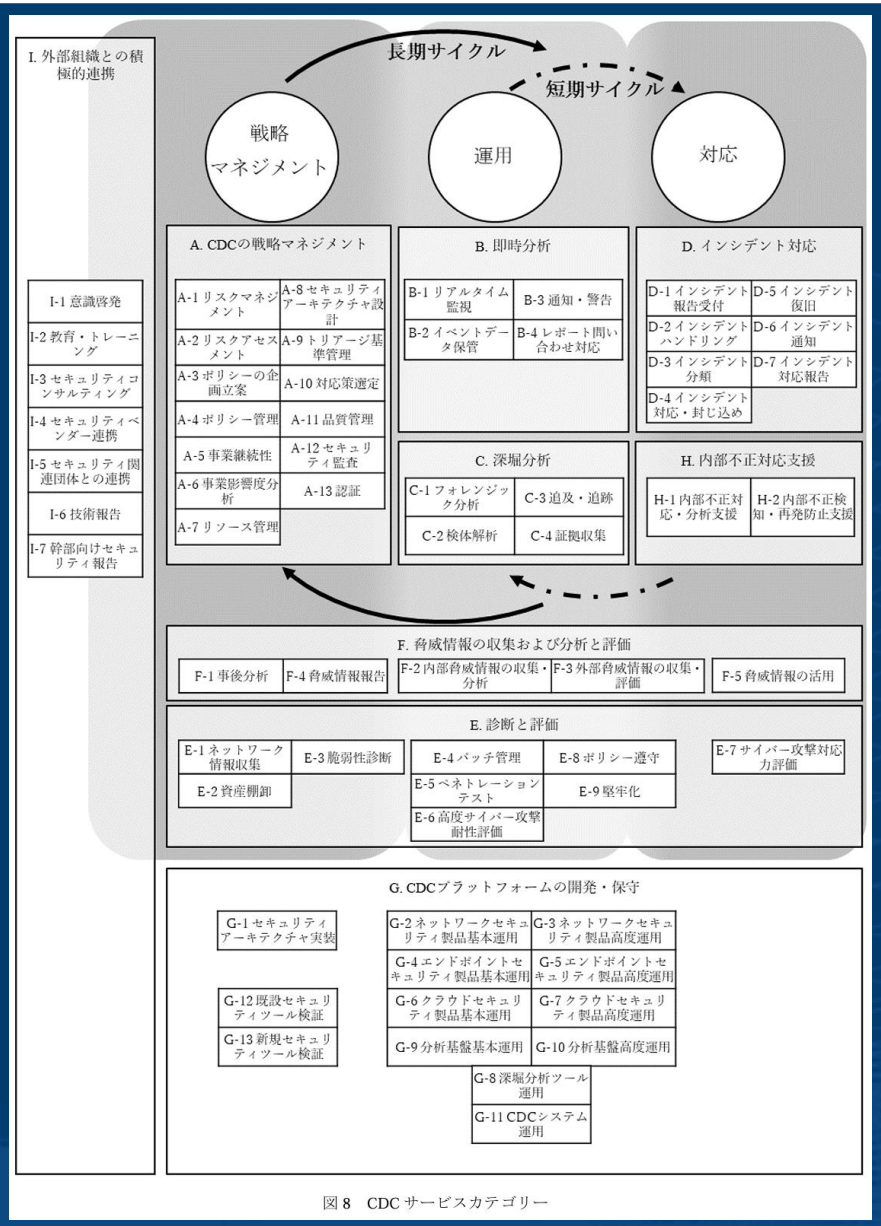


図 8　CDC サービスカテゴリー

トリアージに於いては、まずは以下の項目を確認したほうが良いでしょう。

- A.CDCの戦略マネジメント
- E.診断と評価
  - E-1.ネットワーク情報収集
  - E-2.資産棚卸
  - E-4.パッチ管理
  - E-8.ポリシー尊寿
- I.外部組織との積極的連携
  - I-2.教育・トレーニング
  - I-4.セキュリティベンダー連携
  - I-5.セキュリティ関連団体との連携

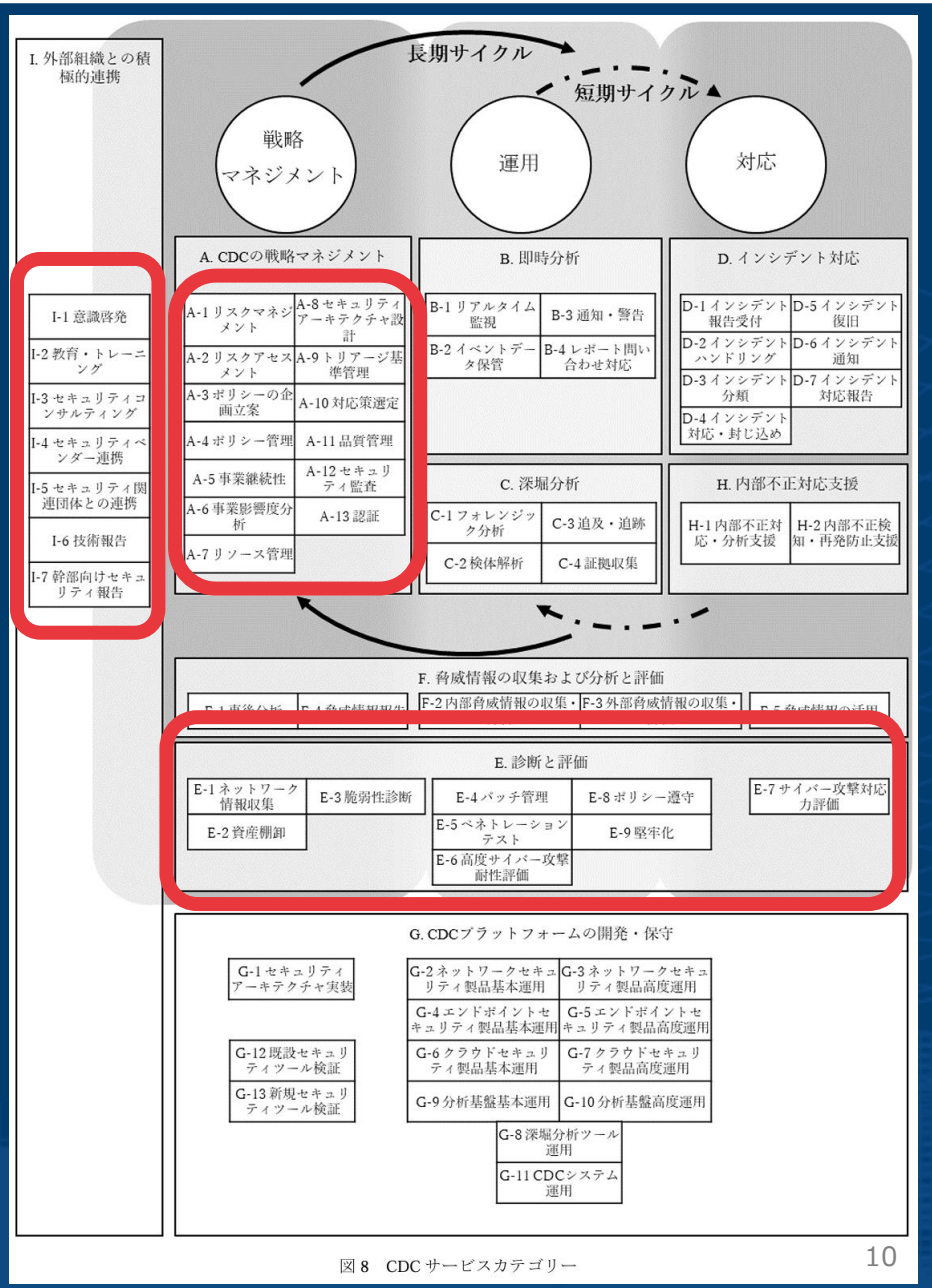


図 8　CDC サービスカテゴリー

03

トリアージで有用な指標

トリアージでは、以下の2つを考慮する必要があります。

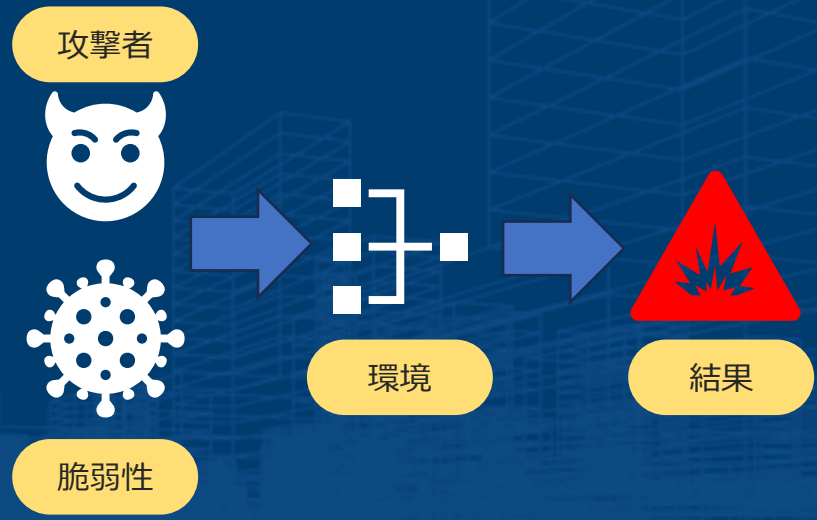
- 脆弱性それ自体の状況
- 組織ごとに異なる、脆弱性が発現や悪用される環境に関する状況

一般的に、第三者が汎用的に提示できるのは、前者の「脆弱性それ自体の状況」です。

本項では、脆弱性それ自体の状況を示す以下の指標と、それを利用した判断フレームワークを説明します。

- CVSS
- EPSS
- KEV Catalog
- vulnrichment
- SSVC

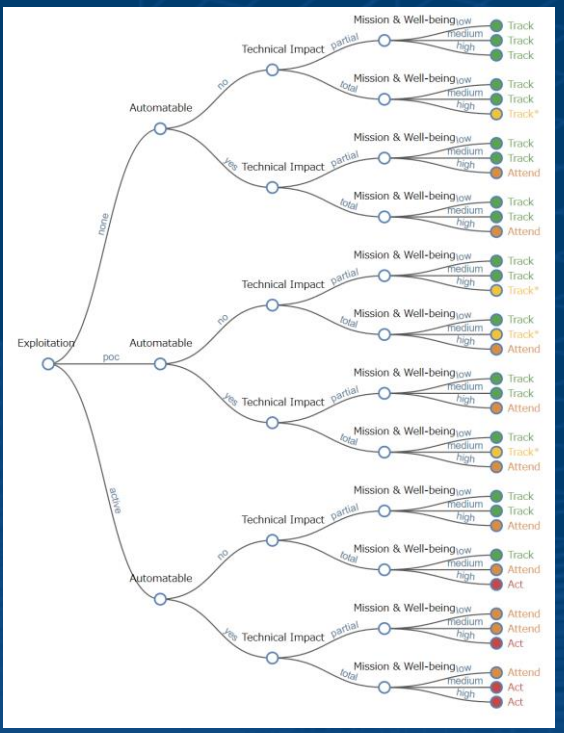
脆弱性それ自体の影響
脆弱性の発生確率
脆弱性の悪用状況
脆弱性の追加情報
トリアージフレームワーク



1）SSVC（Stakeholder-Specific Vulnerability Categorization）

カーネギーメロン大学とCISAが共同で2019年に作成した、脆弱性の悪用状況や安全性の影響などを考慮した脆弱性分析手法です。

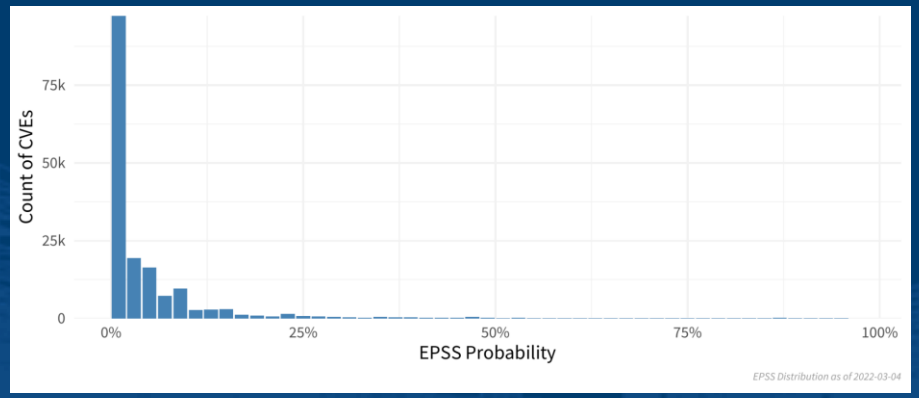
- データを決定木（decision tree）に当て込むことで、行動を決定するフレームワークです
  - 決定木はステークホルダー（利害関係者）毎に用意されています
- トリアージなどの脆弱性対応をする現場では「Deployer tree」を、ソフトウェアなどの供給者は「Supplier tree」を利用します
  - 国内では、Deployer treeが使われることが多いようです
- **以下の状況を基に、Actionを決定します。**
  - **脆弱性の状況**
    （Exploitation, Automatable）
  - **置かれている環境**
    （Exposure）
  - **安全性や組織のミッションへの影響**
    （Situated Safety Impact, Mission Impact）

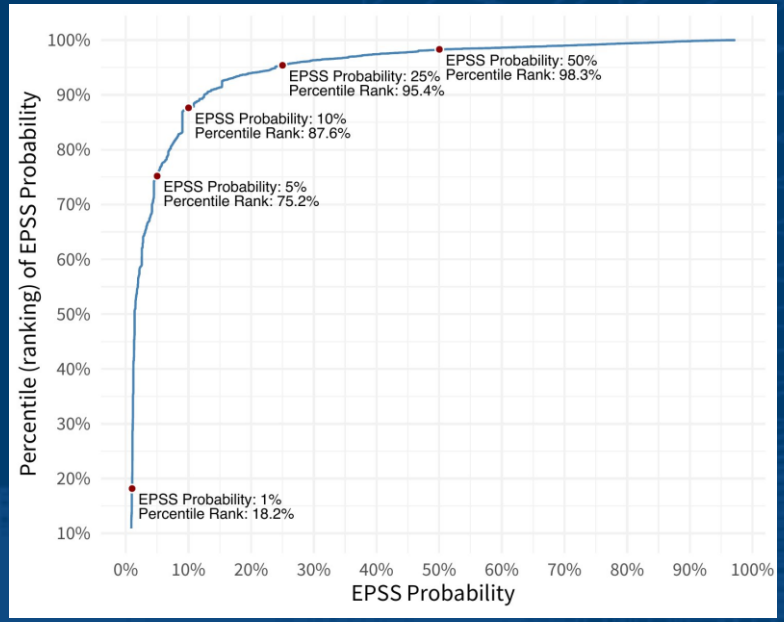


2) EPSS

FIRSTが提供する、「今後30日間の悪用確率」を示すEPSSスコアを提供します。

- EPSS: Exploit Prediction Scoring System（Exploit予測スコアリングシステム）
- 機械学習や他の指標（後述KEV Catalog登録有無など）を基に、自動的に算出された悪用の確率が提供されます
  - ➢ KEV Catalogとも相互に連動しているようです
  - ➢ 脆弱性が悪用される可能性を推定するだけで、環境や悪用された場合の影響を推定するものではありません
- EPSSの値とPercentileの取り扱いには、注意が必要です
  - ➢ 使う際の閾値等は、検討の余地があります



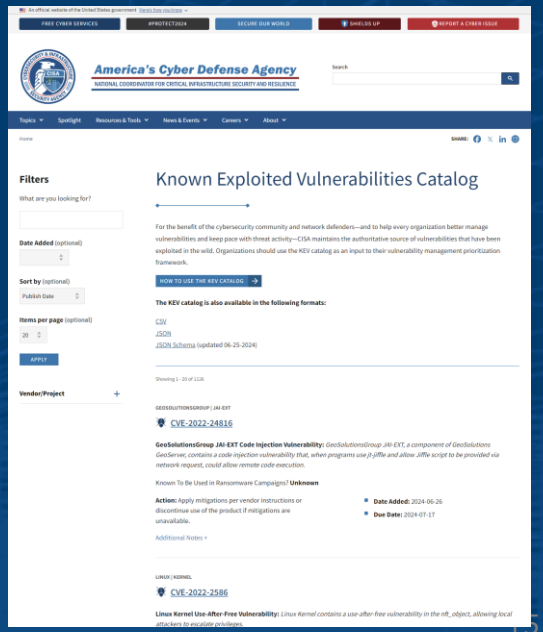


3) KEV Catalog(Known Exploited Vulnerability Catalog)

CISAが公開している、既に悪用が確認された脆弱性の一覧です。

- 米国内では、すべての連邦民間行政機関に対し「拘束力のある運用指令 22-01（BOD 22-01）」にて、特定期間内に対応することが求められています。
  - 罰則のある規定で、登録から2週間以内に対応をすることとなっています
  - 例えば近年多発しているVPN機器やD-Link Routerなどの脆弱性なども登録されています
- ここに登録された脆弱性は既に悪用が確認されているため、対応が必須と考えてよいと思われます。
  - 「ランサムウェアのキャンペーンで使用されたか（Known Ransomware Campaign Use）」、という項目もあります

	A	B	C	D	E	F	G	H	I	J	K
1	cveID	vendorPro	product	vulnerabili	dateAdde	shortDesc	requiredA	dueDate	knownRansomwareCampaignUse	notes	cwes
2	CVE-2021	Accellion	FTA	Accellion	#######	Accellion	Apply upd	#######	Known		
3	CVE-2021	Accellion	FTA	Accellion	#######	Accellion	Apply upd	#######	Known		
4	CVE-2021	Accellion	FTA	Accellion	#######	Accellion	Apply upd	#######	Known		
5	CVE-2021	Accellion	FTA	Accellion	#######	Accellion	Apply upd	#######	Known		
6	CVE-2021	Adobe	Acrobat ar	Adobe Acr	#######	Acrobat A	Apply upd	#######	Unknown		
7	CVE-2021	Adobe	Acrobat ar	Adobe Acr	#######	Adobe Acr	Apply upd	#######	Unknown		

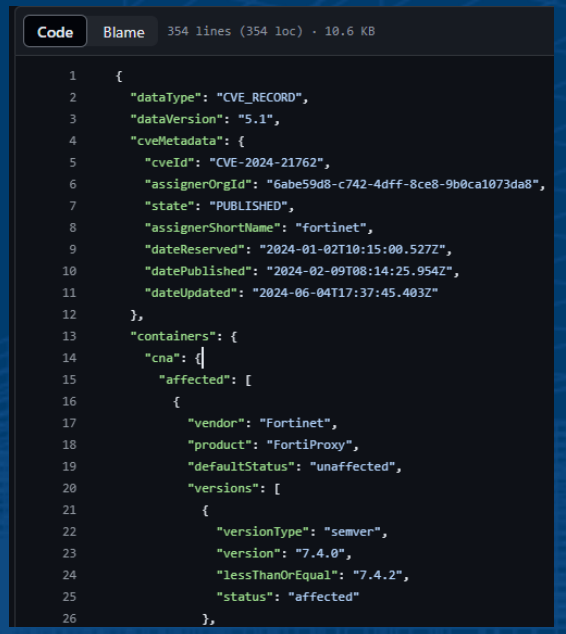


4) vulnrichment

NVDの提供するCVSSの情報を拡張したものです。

- githubで公開されています。
  - https://github.com/cisagov/vulnrichment
- 現時点では開発中のステータスであり、今すぐ実用にはならないかもしれません。
- 今後、よりトリアージ精度を高めるために利用できると思われます。
  - SSVCの Exploitation/Automatable/TechnicalImpact の値を提供している
  - 再計算されたSSVCデータを提供している
  - KEV Catalogへの登録状況も提供している

Decision tree	VulnrichmentがDecision Pointのデータ			
CISA-Coordinator	Exploitation	Automatable	Technical Impact	Mission&Well-biing
Deployer	Exploitation	Exposure	Automatable	Human Impact



04

トリアージの例

トリアージと指標

サイバーセキュリティに於いてのトリアージは、近年では一般的に以下のように示されます。

- リスク＝脅威 x 脆弱性 x 価値
  - リスク：目的に対する不確かさの影響
  - 脅威　：システムまたは組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因
  - 脆弱性：一つ以上の脅威によって付け込まれる可能性のある、資産または管理策の弱点
  - 価値　：システムに於ける情報の有用性などの、資産価値

先ほどの指標を複数用いてトリアージを行うツールやフレームワークがあるので、紹介します。

- 脆弱性の状況からトリアージをするツール
  - CVE_Prioritizer
  - SploitScan
- 脆弱性の状況と組織への影響からトリアージをするフレームワーク
  - SSVC

1) CVE_Prioritizer

CVSS、EPSS、KEV Catalog（、とその他データソース）を利用した、脆弱性パッチ適用順位付けプログラムです。

- 例示としてCVE-2020-29127を示します。
  - Fujitsu Eternus Storage DX200 S4 には、認証に関する脆弱性（KEVなし）

CVSS 3.x Severity and Vector Strings:

NVD **NIST:** NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

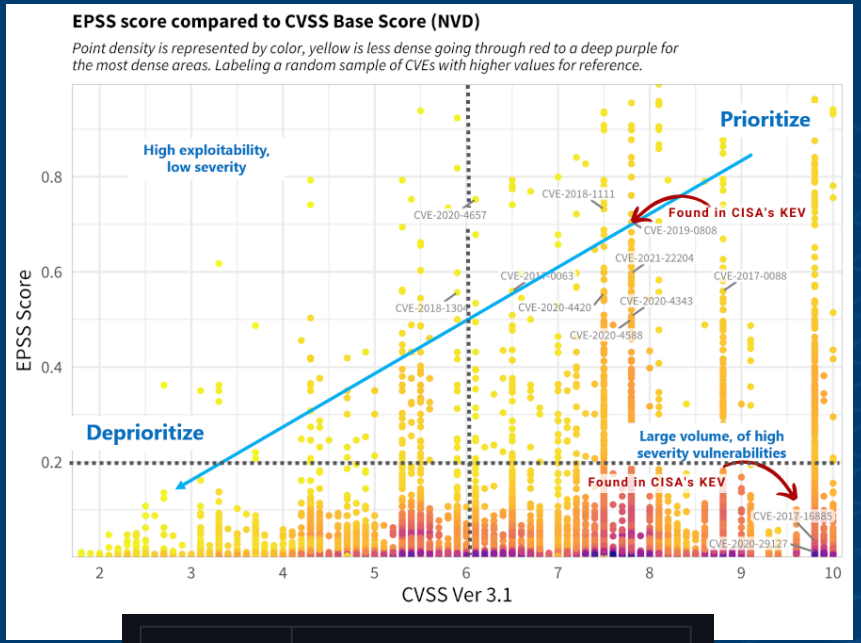
cve	epss	percentile	model	date
CVE-2020-29127	0.41089	0.97316	v2023.03.01	2024-07-01

```
root@06868d66e5c5:/opt/CVE_Prioritizer# python3 cve_prioritizer.py -c CVE-2020-29127

#     ______   ______
#    / ___/ | / / __/
#   / /__ | |/ / _/
#   \___/_|___/___/          _ __  _
#     / _ \____(_)__  ____(_) /_(_)__ ___ ____
#    / ___/ __/ / _ \/ __/ / __/ /_ // -_) __/
#   /_/  /_/ /_/\___/_/ /_/\__/_//__/\__/_/
#   v1.6.4                              BY TURROKS

Warning: Using this tool without specifying a NIST API may result in errors

CVE-ID             Priority
------------------------------
CVE-2020-29127     Priority 1
root@06868d66e5c5:/opt/CVE_Prioritizer#
```



Priority	Description
Priority 1+	CVEs found in CISA's KEV
Priority 1	CVEs in the Upper Right Quadrant
Priority 2	CVEs in the Lower Right Quadrant
Priority 3	CVEs in the Upper Left Quadrant
Priority 4	CVEs in the Lower Left Quadrant

https://github.com/TURROKS/CVE_Prioritizer

2) SploitScan

SploitScanは、CVE_Prioritizerと同様ですが、データソースとスコアリング方法が少々異なります。

パッチ適用優先順位システム

SploitScan のパッチ優先順位付けシステムは、脆弱性の重大度と悪用可能性に基づいてセキュリティ パッチを優先順位付けする戦略的なアプローチを提供します。これは、 CVE Prioritizerのモデルの影響を受けており、公開されているエクスプロイトを処理するための機能強化が行われています。仕組みは次のとおりです。

- A+ 優先度: CISA の KEV にリストされている CVE または公開されているエクスプロイトがある CVE に割り当てられます。これは、パッチ適用のリスクと緊急性が最も高いことを表します。
- A ～ D の優先度: CVSS スコアと EPSS 確率パーセンテージの組み合わせに基づきます。決定マトリックスは次のとおりです。
  - A: CVSS スコア >= 6.0、EPSS スコア >= 0.2。深刻度が高く、悪用される可能性がかなり高い。
  - B: CVSS スコア >= 6.0 だが EPSS スコア < 0.2。重大度は高いが、悪用される可能性は低い。
  - C: CVSS スコア < 6.0 かつ EPSS スコア >= 0.2。重大度は低いが、悪用される可能性は高い。
  - D: CVSS スコア < 6.0 かつ EPSS スコア < 0.2。重大度が低く、悪用される可能性が低い。

このシステムは、潜在的な影響と悪用される可能性の両方を考慮し、どの脆弱性を最初に修正するかについて、ユーザーが十分な情報に基づいて決定を下せるよう支援します。しきい値は、ビジネス ニーズに合わせて変更できます。

```
[ HackerOne Hacktivity ]
Rank:       6795
Reports:    0
Severity:   Unknown: 0 / None: 0 / Low: 0 / Medium: 0 / High: 0 / Critical: 0
```

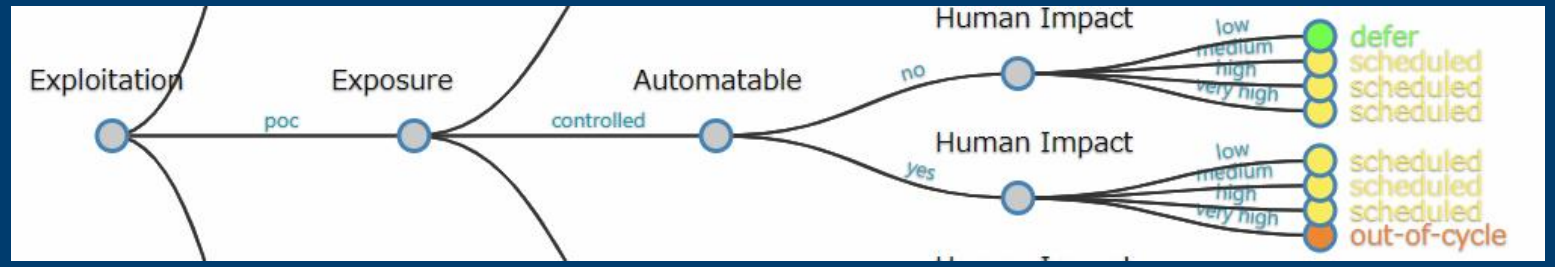
```
[ ⚠ Patching Priority Rating ]
Priority:   C
```

https://github.com/xaitax/SploitScan

3) SSVC

SSVCは、対象の環境を考慮しているため、画一的なデータ出力にはなりません。
ここでは、前項と同じ CVE-2022-29127 で例示します。

- SSVCの “Exploitation””Automatable”はvulnrichmentから取得できればよかったのですが、07/02時点では提供されていないため、推定値です



脆弱性だけではなく、システムの置かれている状況により、対応優先度判断が変わる。

	SSVC Decision point				Action
	Exploitation	Exposure	Automatable	Human Impact	
CVE-2022-29127	PoC	CONTROLLED	NO	LOW	defer
				MEDIUM	scheduled
				HIGH	scheduled
				VERIYHIGH	scheduled

Exploitの有無

ネットワークの状況

攻撃の自動化可否

システムの価値など

各トリアージスキームの比較

「リスク＝脅威×脆弱性×価値」という観点で見ると、各ツールやフレームワークは対応範囲が異なります。

- CVE_Prioritizer
  - CVSSとKEV Catalog, EPSSを利用したトリアージ
- SploitScan
  - 上記に加え、Exploit codeの有無を利用したトリアージ
- SSVC
  - 情報源は異なるが上記を考慮し、システムの価値も考慮したフレームワーク

これらのツール結果を自組織に適用する場合、自組織の環境も考慮する必要があります。
トリアージの一番最初の「各脆弱性の対応ベースライン」を決定する段階で利用できると考えられます。

05 まとめ

脆弱性対応の優先順位付けとしてのトリアージは、平時からの準備が必要です。
重大な脆弱性が突然発見される前に準備をしておくことで、対応の負荷が下がります。

- 組織として
  - 事業に対するリスク、という観点でも判断ができるような組織づくり
  - ガイドラインの事前作成
- トリアージ基準として　使う指標を選定し、使い方に習熟しておく
- 自組織の環境（ネットワーク構成や使用ライブラリ、システムやデータの価値）を把握し、まとめておく

すべてを一気に整備するのは難しいため、少しづつ不足部分を把握/改善していくのが良いと考えます。

まずは紹介した SploitScanやCVE_PrioritizerやSSVCなどを使い、自組織で有効かを見てみるのが良いでしょう。

Thank you!

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。
※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。

Appendix

X.1060

https://www.itu.int/rec/T-REC-X.1060-202106-I

日本語版(JT-X1060)

https://www.ttc.or.jp/document_db/information/view_express_entity/1423

X.1060エディタの武井氏による記事

https://enterprisezine.jp/article/detail/15278 (全4回連載)

ISOG-J セキュリティ対応組織の教科書

https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html

EPSS

https://www.first.org/epss/

KEV

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Vulnrichment

https://github.com/cisagov/vulnrichment

CVE_Prioritizer

https://github.com/TURROKS/CVE_Prioritizer

SploitScan

https://github.com/xaitax/SploitScan

SSVC

https://insights.sei.cmu.edu/library/prioritizing-vulnerability-response-a-stakeholder-specific-vulnerability-categorization-version-20/

全体的な説明

https://www.nri-secure.co.jp/blog/vulnerability-categorization-ssvc

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/stakeholder-specific-vulnerability-categorization.html

Dryad - SSVC Calc App

https://certcc.github.io/SSVC/ssvc-calc/

リスク関連

「脆弱性」「脅威」「リスク」の再整理（はせがわようすけ氏）

https://www.docswell.com/s/hasegawa/ZW19QR-threatmodeling

いまだから再認識したいセキュリティの原則（pwc丸山氏）

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/security-principles02.html