TLP:CLEAR

# 脆弱性トリアージについて再考し、激動の時代を生き抜く！

NCA Annual Conference 2024

Room4 10:00-10:40

株式会社ラック
次世代セキュリティ技術研究所
井上圭
kei.inoue@lac.co.jp

TLP:CLEAR

# Profile

## 井上　圭

kei.inoue@lac.co.jp

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
兼　サイバーセキュリティプラットフォーム開発統括部　企画

非IT企業情報システム部、MSP（Managed Service Provider）、
セキュリティコンサルタントなどを経験し、2024年07月にラックに入社。
脆弱性管理やセキュリティ運用について研究や講演を行い
確かなテクノロジーで「信じられる社会」を目指す。

**最近の発表**

- CodeBlue 2022 Open Talks
- Janog 52 CFP
- Internet Week 2023 C6
- NCA Annual Conference 2023 車座1
- NCA Annual Conference 2023 CFP
- OWASP Nagoya Chapter/OWASP 758 Day
- Hardening Designers Conference 2024 Session4
- Internet Week SHOWCASE in 福岡
- Internet Week 2024 D1-2
- Internet Week 2024 BoF
- 他

**参加団体**

- 日本ネットワークセキュリティ協会（JNSA）
  - 社会活動部会
  - 教育部会
- 日本セキュリティオペレーション事業者協議会（ISOG-J）
  - WG1 “脆弱性トリアージガイドライン作成のための手引き”
  - WG6 “セキュリティ対応組織の教科書”
- 日本シーサート協議会（NCA）
  - インシデント対応訓練WG
  - 脆弱性管理WG
- セキュリティトランスペアレンシーコンソーシアム（STコンソーシアム）
- 他

TLP:CLEAR

# Agenda

1. 概要
2. 少し前の、　　脆弱性トリアージ
3. 今のトレンドの、　脆弱性トリアージ
4. 近い将来の、　　脆弱性トリアージ
5. とはいえ…
6. まとめ

Appendix

01

# 概要

# 本日の概要

TLP:CLEAR

本日は、脆弱性トリアージについて考えようと思います。

近年、トリアージの目的や手法が変化してきております。システムの価値や事業への影響を考慮することが求められており、影響の大きい脆弱性に注力する事が多くなりました。

今回は、今まで/現在/未来 のトリアージについて情報を提供します。
また、それらの適用についても考えます。

- 少し前の、脆弱性トリアージ
- 今トレンドの、脆弱性トリアージ
- 近い将来の、脆弱性トリアージ
- とはいえ…

過去と現在を俯瞰し、状況を把握する

脆弱性トリアージについて再考し、

今と今後に役立てる！
（本カンファレンスのサブタイトル）

激動の時代を生き抜く！

02

# 少し前の、脆弱性トリアージ

# 少し前の、脆弱性トリアージ

TLP:CLEAR

2019年ごろまでのトリアージでは、脆弱性それ自体の影響度を基に判断することが多かったように思われます。

- 2016年ごろから脆弱性情報が急増するまでは、それで問題がなかったのかもしれません。
  （＝まだ管理できる量の脆弱性しかなかった可能性）

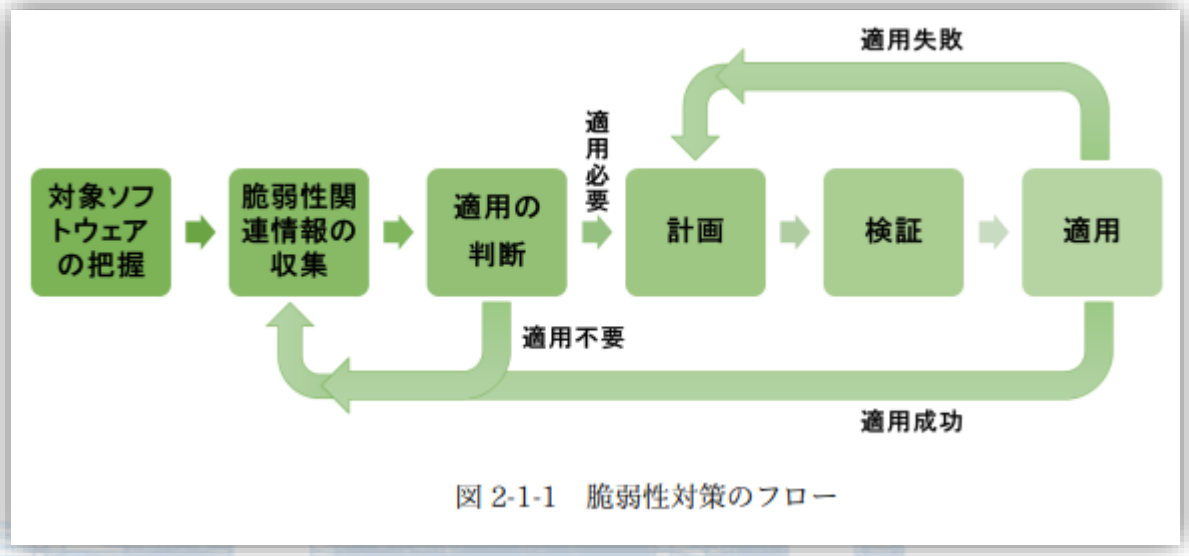
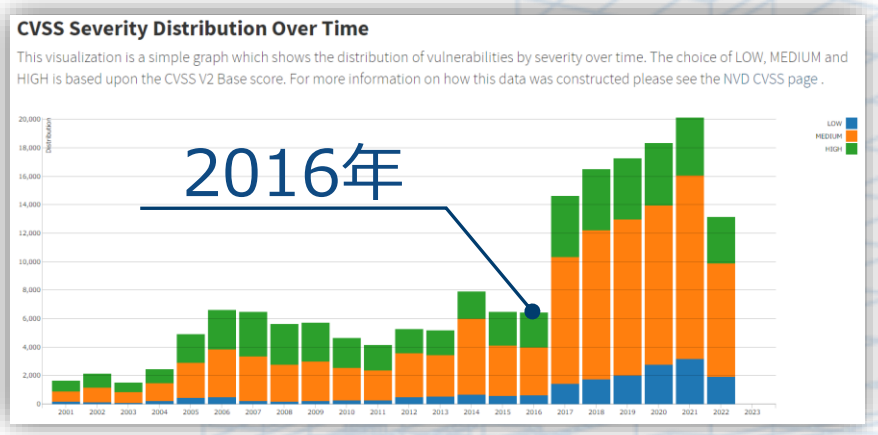



図 2-1-1　脆弱性対策のフロー

IPA:IPA Technical Watch 脆弱性対策の効果的な進め方（ツール編）:2019年
https://www.ipa.go.jp/security/reports/technicalwatch/20190221.html




NIST:CVSS Severity Distribution Over Time
https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time#CVSSSeverityOverTime

# また、緊急度判断としてCVSS **BaseScore**とCVSS **BaseMetrics**（所謂Vector値）を参照することを重視していました。

- 今ほど情報が多様に存在していない、というのもあり CVSSの情報に頼る形になっていたと考えます。

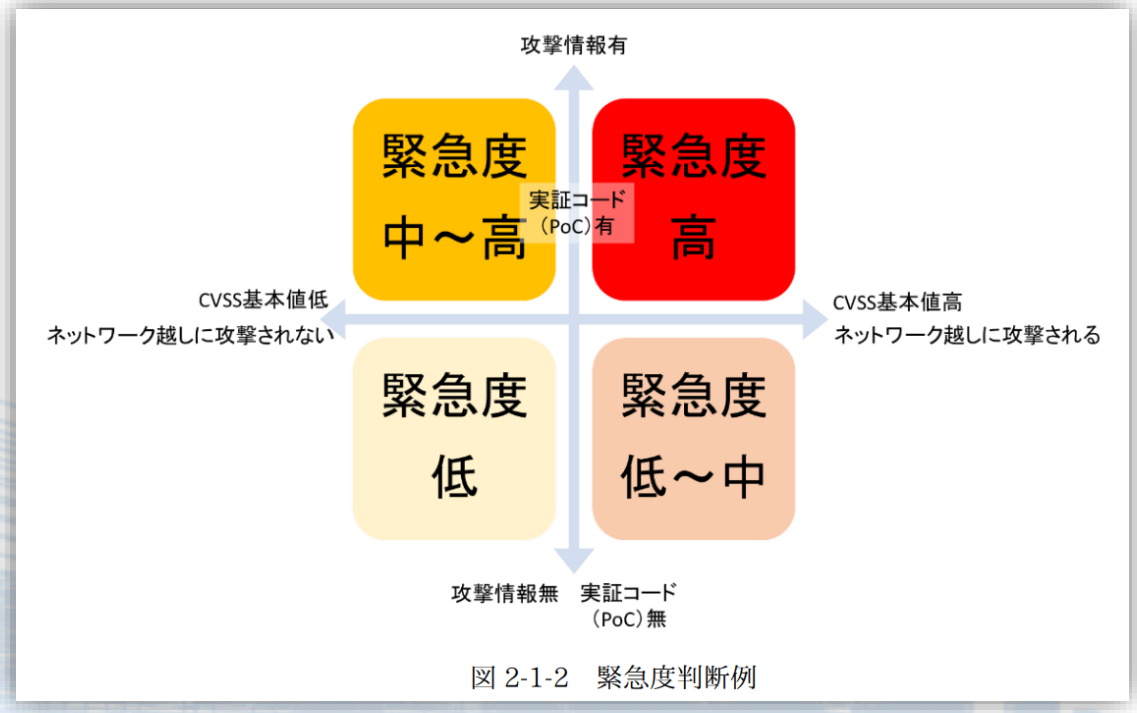



図 2-1-2　緊急度判断例

IPA:IPA Technical Watch 脆弱性対策の効果的な進め方（ツール編）:2019年
https://www.ipa.go.jp/security/reports/technicalwatch/20190221.html

主に利用した指標

- CVSS Base Score　：総合評価
- CVSS Base Metrics
  - Attack Vector　：攻撃元区分
  - Attack Complexity　：攻撃条件複雑さ
- CVSS Temporal Metrics
  - Exploit Code Maturity　：攻撃コード有無

Exploit有無は、CVSSでは提供されない

CVSSの値は、提供者で異なる事がある

Vectorは、解釈に経験が必要（？）

年々CVE-IDの登録が増え、対処不能な数

Scoreのみで評価という現実
=
Score8.0以上は全て対応…

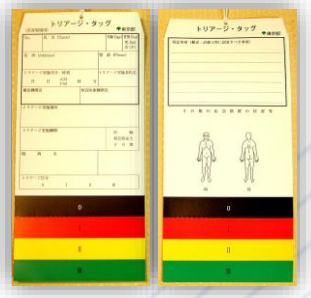
03

# 今トレンドの、脆弱性トリアージ

# トリアージのトレンド

TLP:CLEAR

「脆弱性それ自体に対する影響」から対応を決めるのではなく、
**「事業リスク」として対応**を決めるように変わってきました。



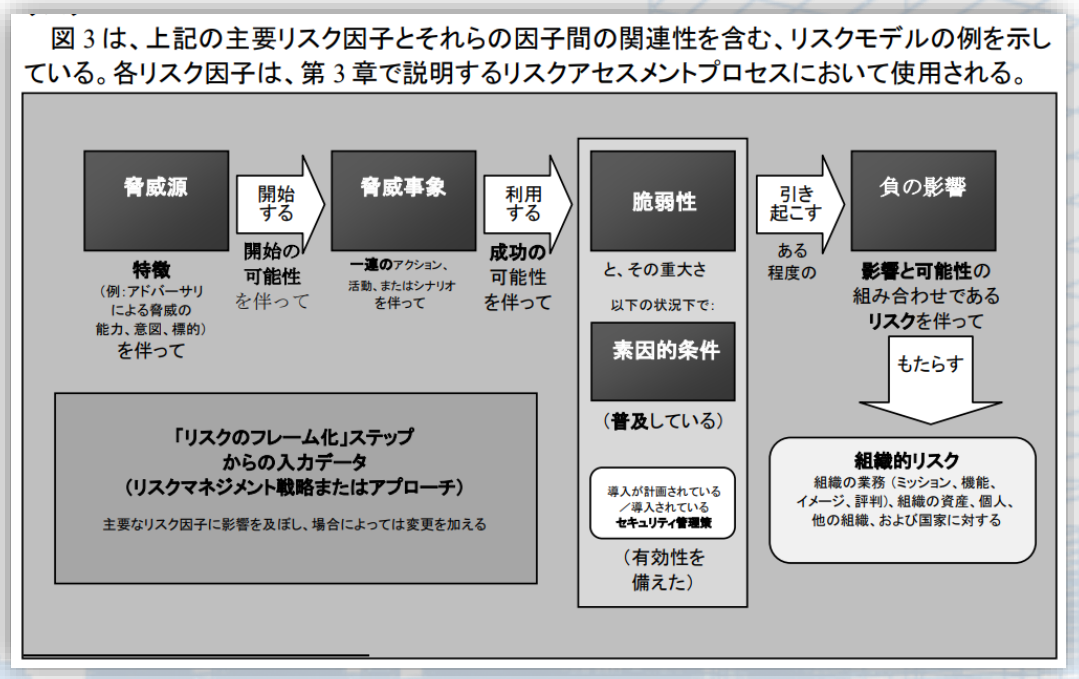
東京都保健医療局：トリアージ
https://www.hokeniryo.metro.tokyo.lg.jp/iryo/kyuukyuu/saigai/triage.html

また、無償で手に入る脆弱性に関する情報も増え、
**「優先順位付け＝脆弱性トリアージ」**
も広く使われるようになってきました。

全ての脆弱性に対応しようとせず、
事業影響のあるものに注力することで
即時対応すべきものを減らすという意図

リスク＝「目的に対する不確かさの影響」
（JIS Q 270000:2019, 31000:2019等）

「事業への」リスクを示すための方法は
様々なリスク評価指標が存在します。



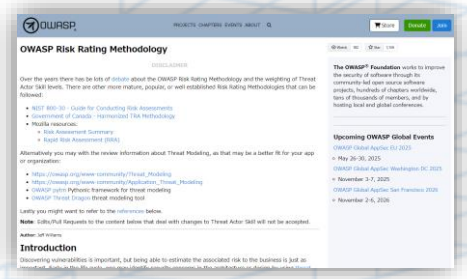

IPA翻訳:NIST Special Puublication 800-30 リスクアセスメント実施の手引き
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000balw.pdf

# リスク評価

TLP:CLEAR

リスク評価手法としては、おおよそ以下のようなものがあります。

- 一般論として
  - リスク ＝ 脆弱性 × 発生可能性 × 影響
    - ✓ 脆弱性 ：脆弱性それ自体の影響（CVSS Score等）
    - ✓ 発生可能性 ：脆弱性を使われる可能性（KEVC、EPSS、構成等）
    - ✓ 影響 ：システムの価値（保有データ等）
- OWASP Risk Rating Methodology（OWASPリスク格付け手法）
  - リスク ＝ 可能性 × インパクト （Informal Methodでの言及）
    - ✓ 可能性 ：脅威の要因、脆弱性の要因
    - ✓ インパクト ：技術的な影響、ビジネスへの影響




**OWASP : Risk Rating Methodology**
https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

| | | | | |
|---|---|---|---|---|
| 脅威の要因 | スキルレベル | 動機 | 機会 | サイズ |
| 脆弱性の要因 | 検出の容易さ | 悪用の容易さ | 認識 | 侵入検知 |
| 技術的な影響 | 機密性の喪失 | 整合性の喪失 | 可用性の喪失 | 説明責任の喪失 |
| ビジネスへの影響 | 金銭的損害 | 評判の低下 | コンプライアンス違反 | プライバシー侵害 |

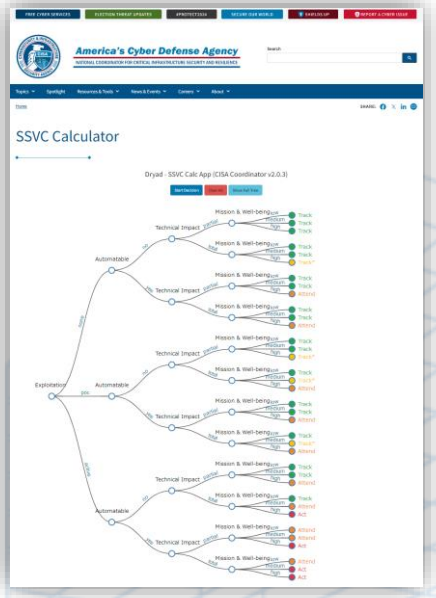
# リスク評価(SSVC)

TLP:CLEAR

また、SSVCでは

- SSVC：Stakeholder-Specific Vulnerability Categorization
- Stakeholder（利害関係者）毎に、異なる決定木があります。
  - Supplier　　：パッチ提供者向け
  - Deployer　　：パッチ適用者向け
  - Coordinator：パッチ調整者向け

運用/脆弱性管理で使える




**CISA:SSVC Calculator**
https://www.cisa.gov/ssvc-calculator

どこに価値を置いているのか
が分かりやすい

| | | | | |
|---|---|---|---|---|
| Supplier | Exploitation | Utility | Technical Impact | Public-Safety Impact |
| Deployer | Exploitation | Exposure | Automatable | Human Impact |
| Coordinator | Exploitation | Automatable | Technical Impact | Mission & Well-being |

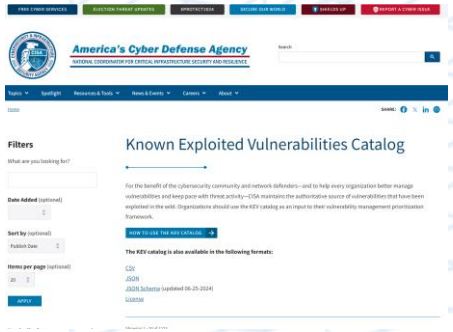
# その他指標

TLP:CLEAR

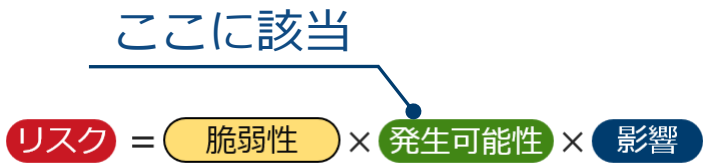
よく使われる指標について、簡単に示します。

- EPSS（Exploit Prediction Scoreing System:エクスプロイト予測スコアリングシステム）
  - CVE-ID毎に今後30日以内に脆弱性が悪用される確率
  - 0-1で表示される確率、全体での位置、が提供される
- KEV Catalog（Known Exploited Vulnerabilities Catalog:既知の悪用された脆弱性カタログ）
  - 悪用が確認された脆弱性について、米国政府関連で対応必須のものを、示したリスト
    - 登録が告示無く取り消される場合がある（ようだ）
    - 対応策があるもののみ登録される（未対応罰則があるため、か？）


**FIRST : EPSS**
https://www.first.org/epss/




**CISA : Known Exploited Vulnerabilites Catalog**
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

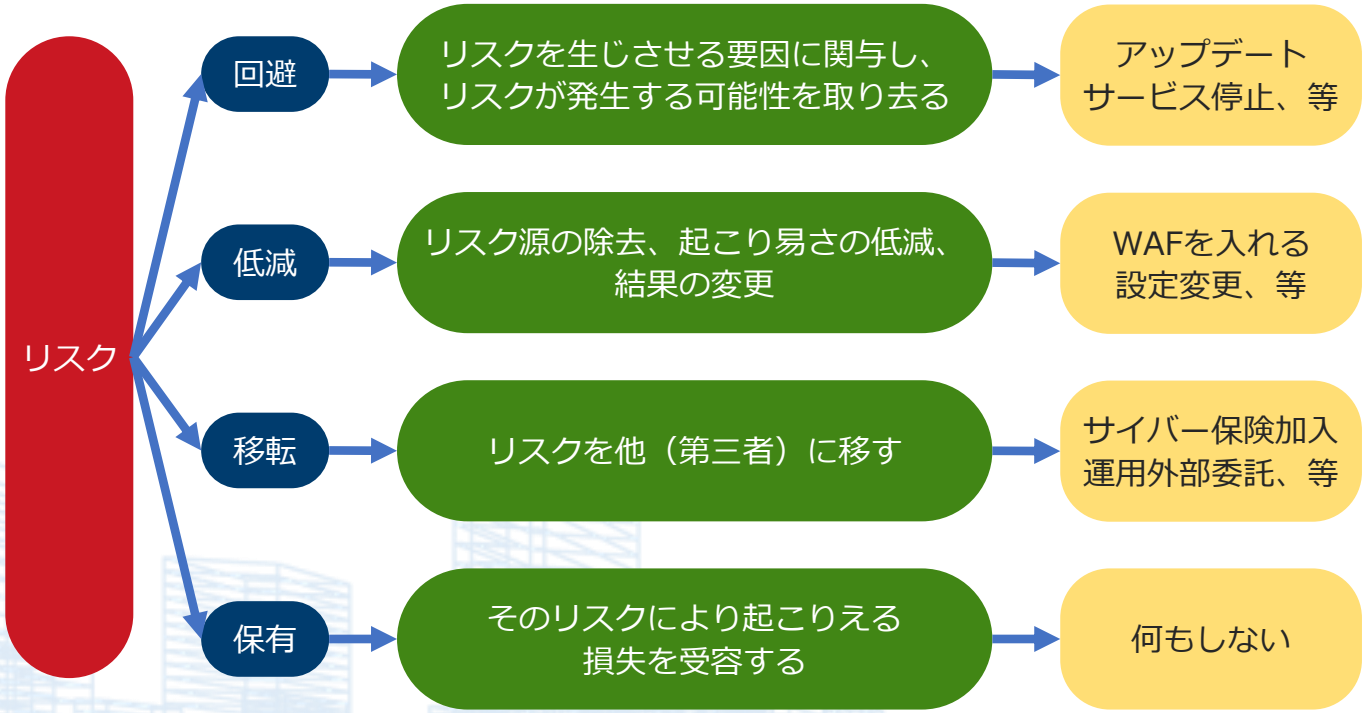



これらの指標を合わせて、事業に対するリスクとしてトリアージを行います。

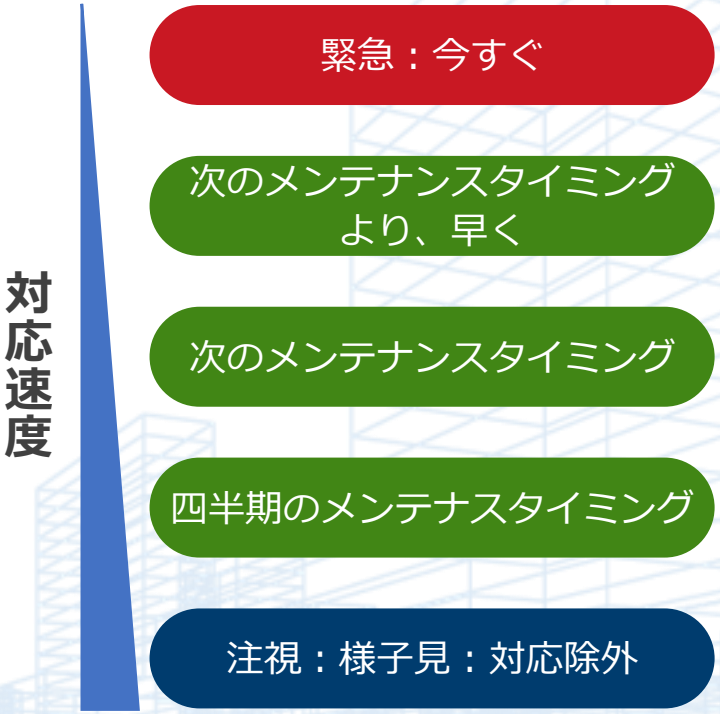
# 対応方法と期日

TLP:CLEAR

また、今までは「アップデートを行うか/否か」で判断でしたが、近年は**リスクに対する対応**という観点で対応方法を検討し、対応方法と期日を組み合わせています。




図：リスクと取り得る対応




図：脆弱性への対応速度

04

# 近い将来の、脆弱性トリアージ

# 近い将来の、脆弱性トリアージ

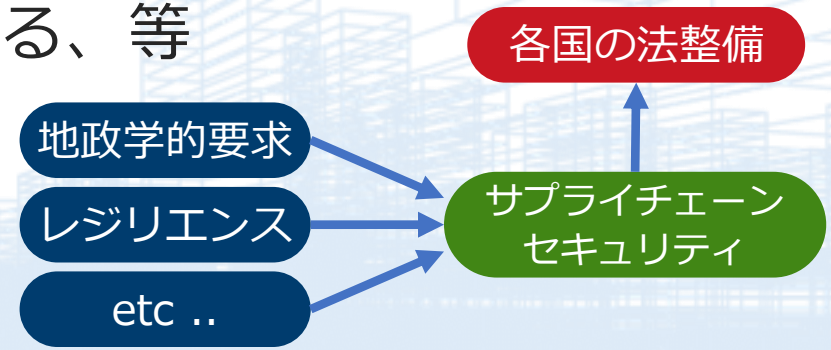
TLP:CLEAR

近年のサイバー攻撃から、**サプライチェーンセキュリティ対策**が求められるようになってきました。

- サイバーレジリエンス法（EU）、Code of Practice for Software Vendors（英）、Supply Chain Cybersecurity Principles（米）、etc..

脆弱性管理も、サプライチェーンセキュリティ対策の中の一つの施策として機能させる必要があります。

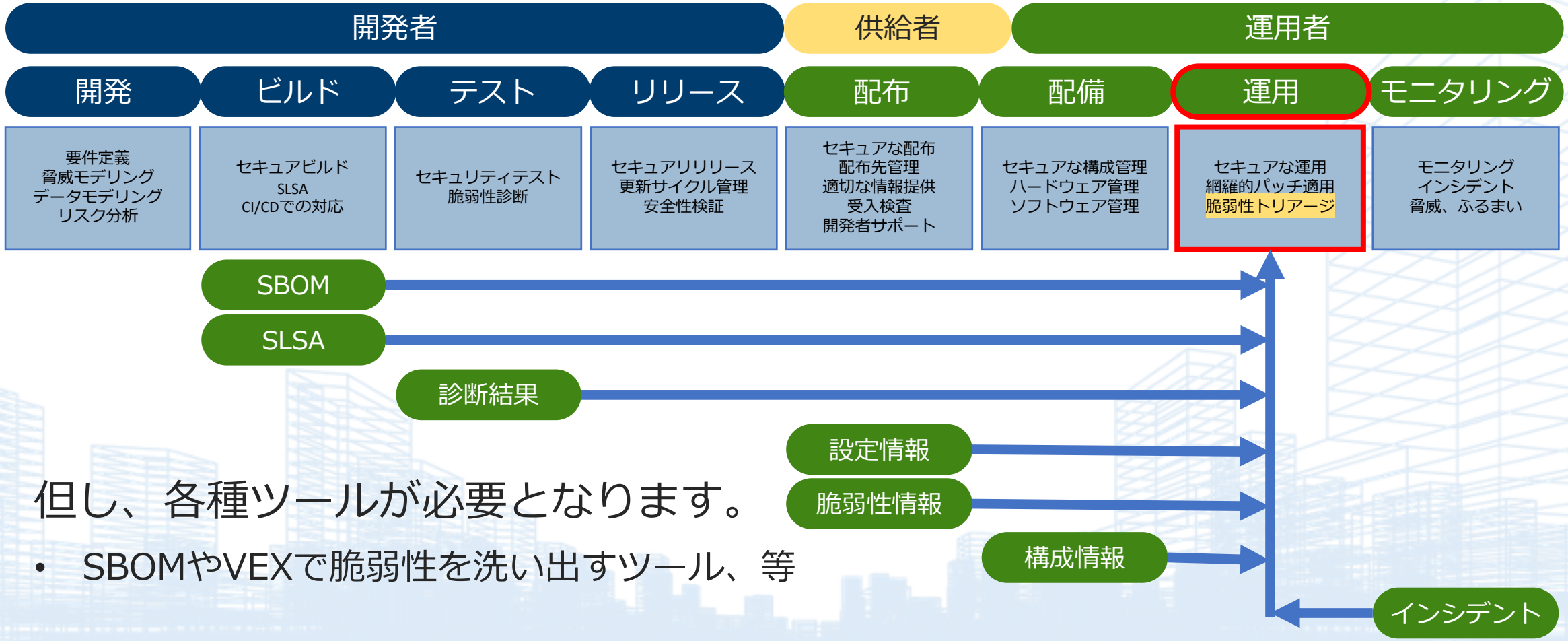
- 「脆弱性管理」という点では実施内容に大きな差はないと考えられますが、データフローは変わるように思われます。
  - ソフトウェア資産把握としてSBOMを利用する、等
- DevSecOpsなどとも連携する必要があります。



# サプライチェーンセキュリティと脆弱性管理とトリアージと

TLP:CLEAR

楽観的な見方をすれば、各役割が明確化され、運用部門ですべての情報を作り出す必要がなくなる、かもしれません。




但し、各種ツールが必要となります。

- SBOMやVEXで脆弱性を洗い出すツール、等

# 05 とはいえ…

# とはいえ、現行から帰るのは難しい

TLP:CLEAR

「今のトレンド」や「近い将来の」話をしましたが、実際に運用に適用できますか？

実運用への適用が難しいことが多いように思われます。

リスクベースのトリアージに変えるには、以下のような方法が有効です。

- ツールを突破口にする
- 組織体制を見直す

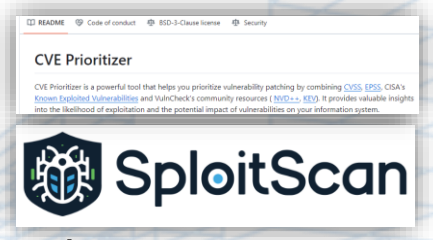
# ツールを突破口にする

TLP:CLEAR

まずはリスクベース脆弱性トリアージを行うと、現状とどう変わるのかを知る必要があると考えます。

商用製品やオープンソースのツールで対応が可能であり、自社にとっての有用性が確認できれば導入する、というのもよいと考えます。

- 商用脆弱性検知/管理ツールでは、優先順位を提示する機能があるものがあります。
  - 脆弱性スキャンとトリアージが一体化しているため、運用負荷が低いと思われます。
  - しかしながら、有償かつツール導入が必要になるため、導入障壁が高いと考えます。
- オープンソースツールも存在します。
  - CVE_Prioritizer：https://github.com/TURROKS/CVE_Prioritizer
  - SploitScan　　：https://github.com/xaitax/SploitScan
    - EPSSやKEV Catalogを考慮した、優先順位付けを行うツールです。
    - 既に何らかの方法で取得しているCVE-IDを渡すことで、優先順位付けをします。
    - その為、脆弱性スキャンツールは別途必要です。



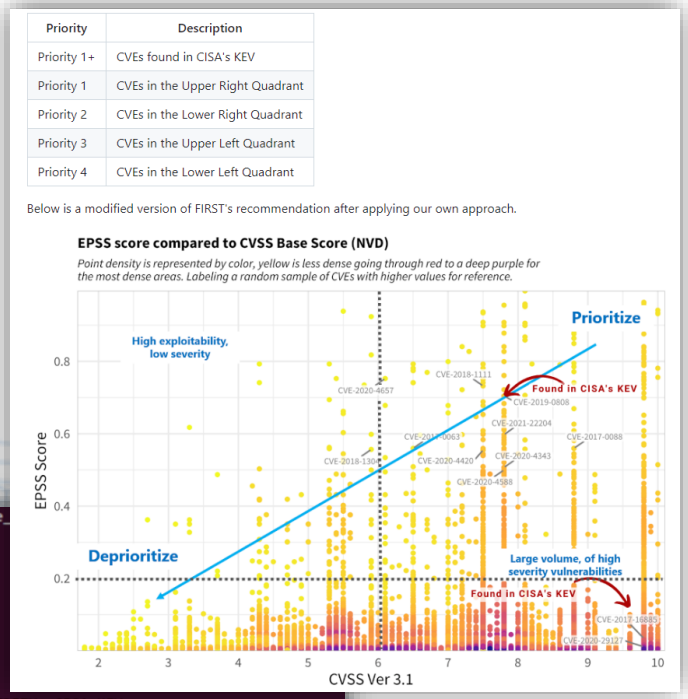
# ツールを突破口にする:オープンソースツール

ポイント：ツール自体より、どのようにトリアージを考えているかの参考にしてください。

TLP:CLEAR

## CVE_Prioritizer

- 特徴
  - CVSS, EPSS, KEV Catalogを利用した脆弱性トリアージを行います。



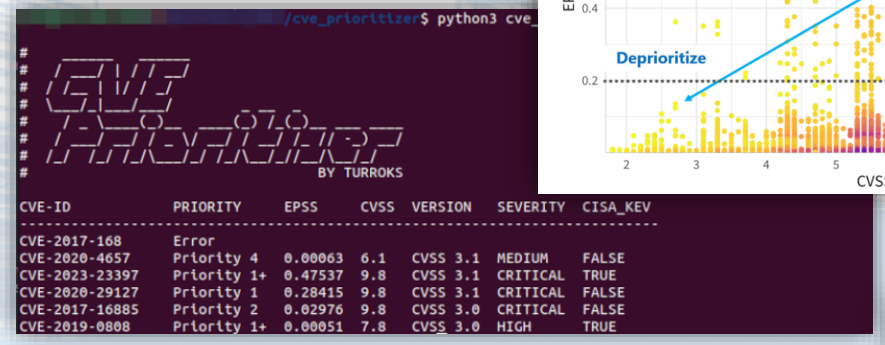
| Priority | Description |
|---|---|
| Priority 1+ | CVEs found in CISA's KEV |
| Priority 1 | CVEs in the Upper Right Quadrant |
| Priority 2 | CVEs in the Lower Right Quadrant |
| Priority 3 | CVEs in the Upper Left Quadrant |
| Priority 4 | CVEs in the Lower Left Quadrant |

Below is a modified version of FIRST's recommendation after applying our own approach.

**EPSS score compared to CVSS Base Score (NVD)**

*Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.*





```
/cve_prioritizer$ python3 cve_
BY TURROKS

CVE-ID          PRIORITY     EPSS     CVSS  VERSION   SEVERITY  CISA_KEV
-------------------------------------------------------------------------
CVE-2017-168    Error
CVE-2020-4657   Priority 4   0.00063  6.1   CVSS 3.1  MEDIUM    FALSE
CVE-2023-23397  Priority 1+  0.47537  9.8   CVSS 3.1  CRITICAL  TRUE
CVE-2020-29127  Priority 1   0.28415  9.8   CVSS 3.1  CRITICAL  FALSE
CVE-2017-16885  Priority 2   0.02976  9.8   CVSS 3.0  CRITICAL  FALSE
CVE-2019-0808   Priority 1+  0.00051  7.8   CVSS 3.0  HIGH      TRUE
```

## SploitScan

- 特徴
  - CVSS, EPSS, KEV Catalog, Exploit情報を利用した脆弱性トリアージを行います。
  - AI-Powered Risk Assessment機能がある（未確認）

```
PS C:\Users\ah\Documents\GitHub\SploitScan> python .\sploitscan.py CVE-2024-28995
SPLOITSCAN
v0.10.4 / Alexander Hagenah / @xaitax / ah@primepage.de
CVE ID: CVE-2024-28995
[ Vulnerability information ]
Published:    2024-06-06
Base Score:   8.6 (HIGH)
Vector:       CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:
Description:  SolarWinds Serv-U was suscep
              access to read sensitive files
[ Exploit Prediction Score (EPSS) ]
EPSS Score:   96.00% Probability of exploitat
[ CISA KEV Catalog ]
Listed:       Yes
Ransomware:   Unknown
```

### Patching Priority System

The Patching Prioritization System in SploitScan provides a strategic approach to prioritizing security patches based on the severity and exploitability of vulnerabilities. It's influenced by the model from CVE Prioritizer, with enhancements for handling publicly available exploits. Here's how it works:

- A+ Priority: Assigned to CVEs listed in CISA's KEV or those with publicly available exploits. This reflects the highest risk and urgency for patching.
- A to D Priority: Based on a combination of CVSS scores and EPSS probability percentages. The decision matrix is as follows:
  - A: CVSS score >= 6.0 and EPSS score >= 0.2. High severity with a significant probability of exploitation.
  - B: CVSS score >= 6.0 but EPSS score < 0.2. High severity but lower probability of exploitation.
  - C: CVSS score < 6.0 and EPSS score >= 0.2. Lower severity but higher probability of exploitation.
  - D: CVSS score < 6.0 and EPSS score < 0.2. Lower severity and lower probability of exploitation.

This system assists users in making informed decisions on which vulnerabilities to patch first, considering both their potential impact and the likelihood of exploitation. Thresholds can be changed to your business needs.

リスク ＝ 脆弱性 × 発生可能性 × 影響

# 組織体制を見直す

TLP:CLEAR

状況により、トリアージを含む「脆弱性管理」のための組織設計を更新したほうがいい場合があります。

ITU-TのX.1060や、ISOG-Jの教科書が役に立つ場合があります。

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


  - CDC（Cyber Defence Centre:組織のサイバーセキュリティ部門; SoC/CSIRT等）を構築するためのフレームワークです。
  - CDCが備えると考えられる機能の一覧（CDCサービス）や、CDCサービスの選択方法、インソース/アウトソースの選択方法、等が記載されています。

- ISOG-J セキュリティ対応組織の教科書 3.2版


  - 上記X.1060の元になったもので、X.1060で日本に該当する参考資料などを追加されているものです。
  - 経済産業省のサイバーセキュリティ経営ガイドラインなど、国ごとのものを取り込んでいます。

# 組織体制を見直す:X.1060/セキュリティ対応組織の教科書

TLP:CLEAR

SOC/CSIRTとして提供される機能の一覧があり、これを基に自社の脆弱性対応について必要なCDCサービスを取捨選択し、必要なものが実装されている状態にする必要があります。

- 全てを実装する必要はありません。対象組織で必要なサービスを実装するための、抜け漏れ確認として利用できます。
- やる事/やらない事、外部委託/自社対応 などをまとめることで、活動の過不足を整理できます。
- この整理の中で、脆弱性管理に必要なサービスが充足しているかを再検討します。
    - 人員や連携機能の不足により機能しないのか、それを行うためのプラットフォームがないのか、等を見つけだす必要があります。

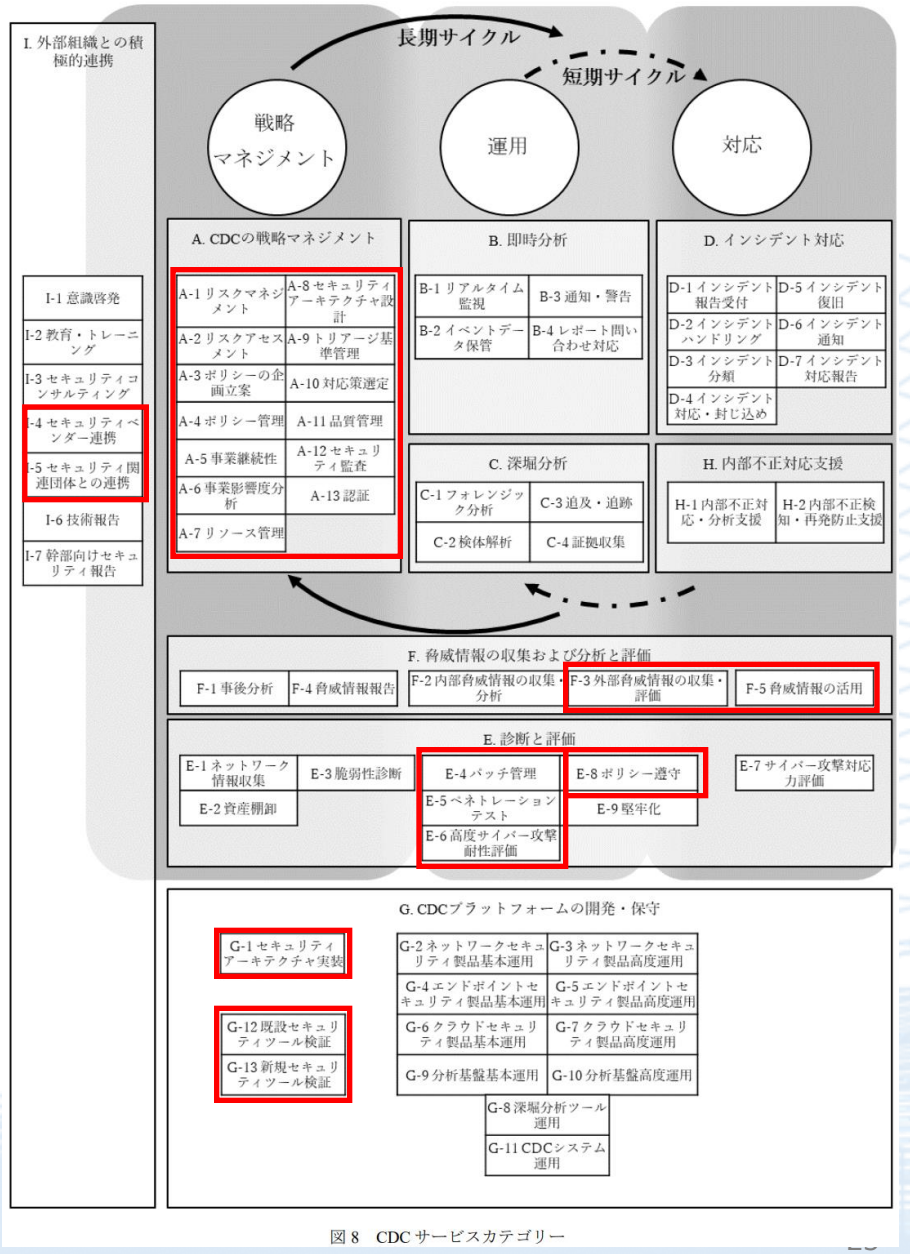
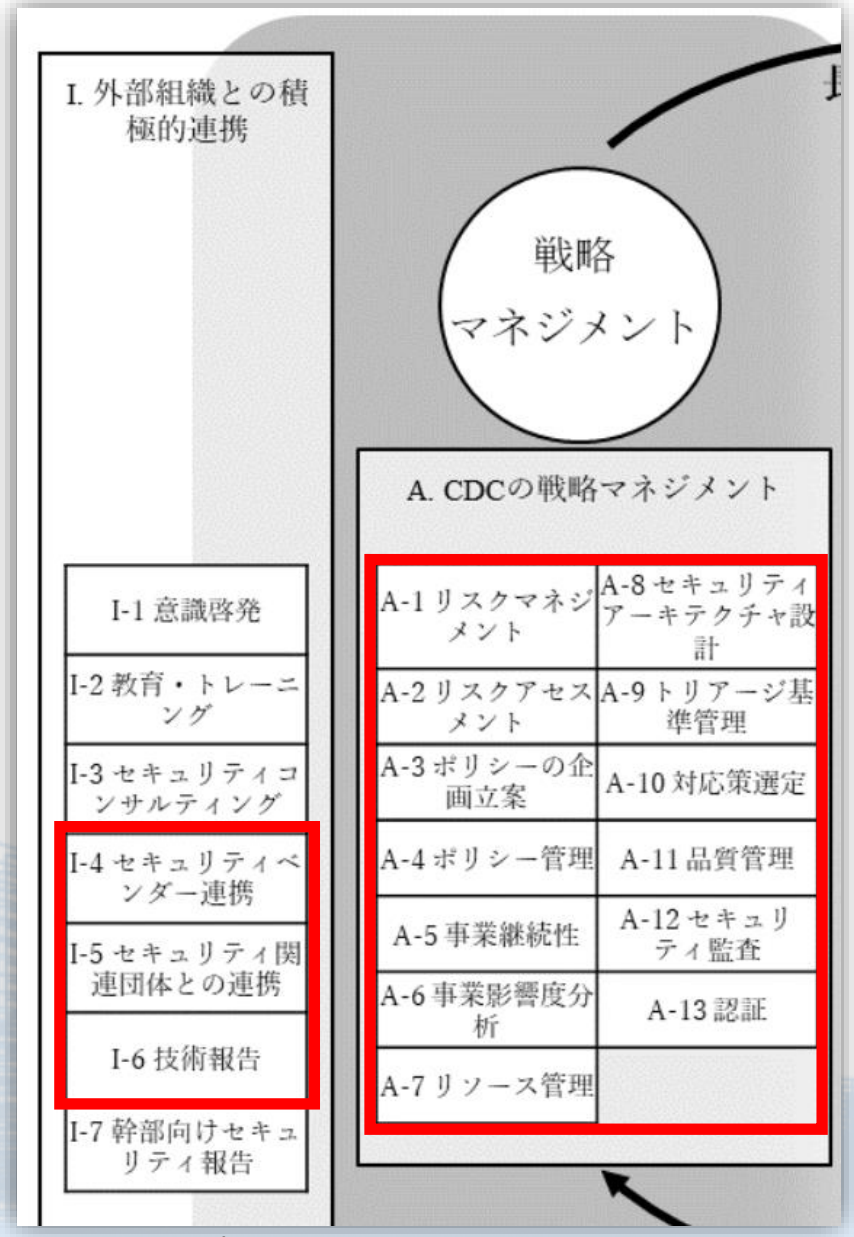
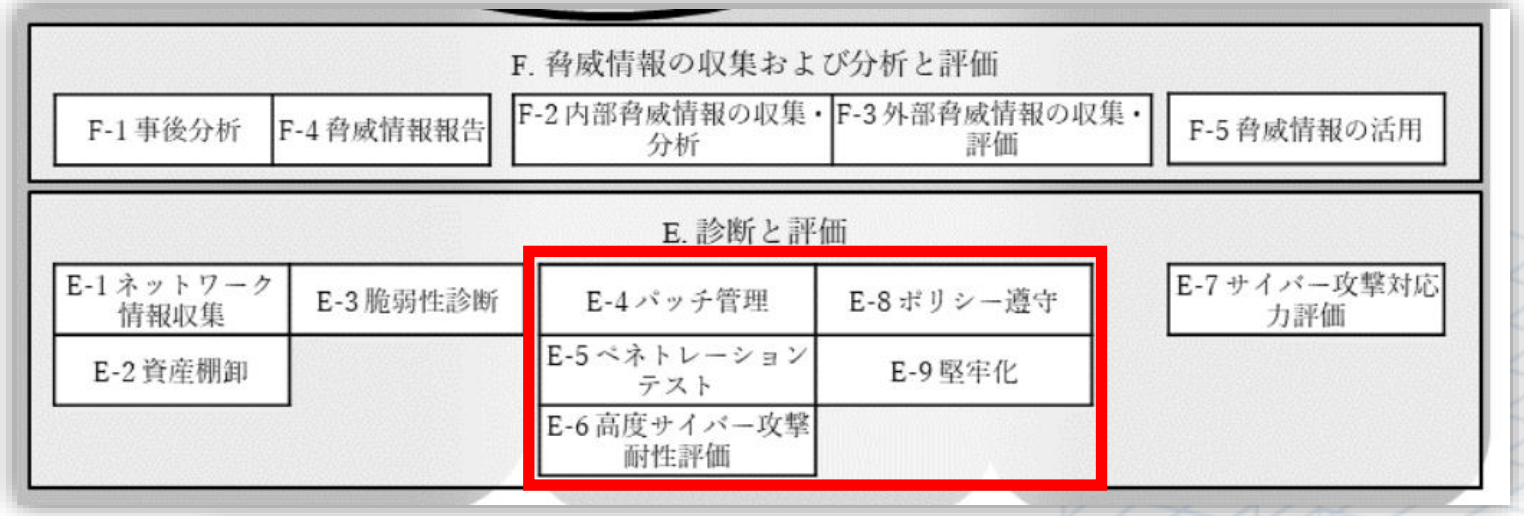
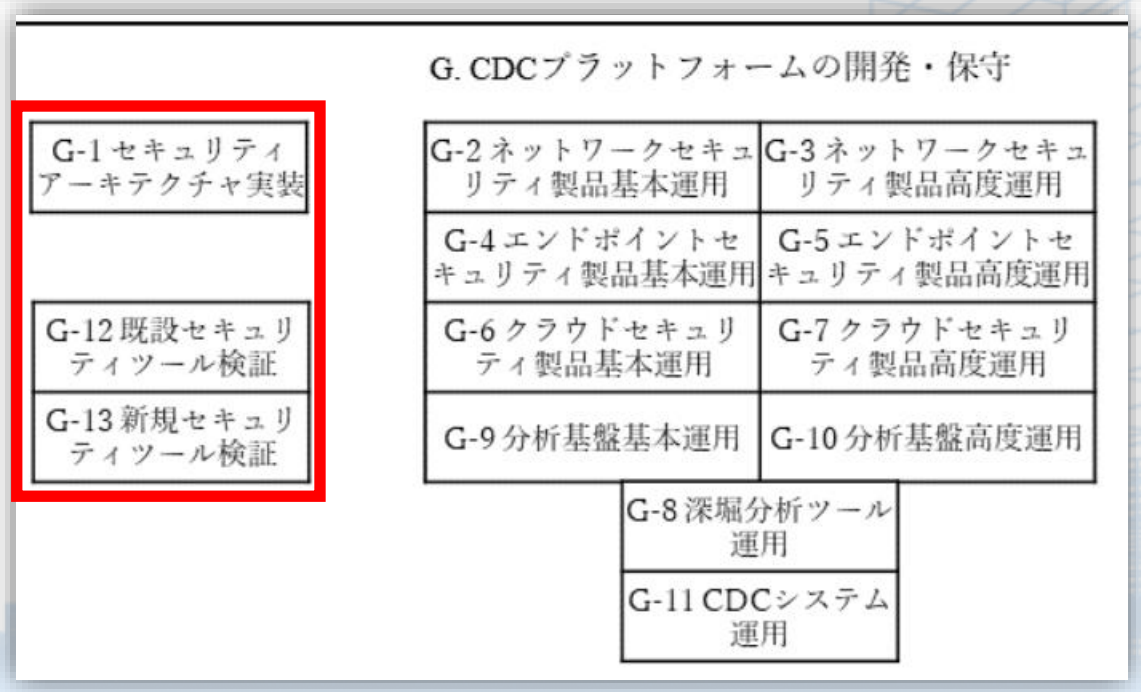


図 8　CDC サービスカテゴリー



06

# まとめ

# まとめ

TLP:CLEAR

「脆弱性管理トリアージ」という観点では、以下のようになると考えます。

- これから
  - 「事業へのリスク」という観点でトリアージが必要
  - 個別で人間で判断するのは難しいので、何らかのツールを使うほうが良い
- 近い将来に向けて
  - SBOMは着実に「必須化」の流れが見え始めた
  - サプライチェーンセキュリティ対策の流れに対応できる準備が必要

自社だけで対応することが難しい場合、共助の観点で他社と連携することをお勧めします。

- 日本シーサート協議会（NCA）、日本ネットワーク協会（JNSA）、日本セキュリティオペレーション事業者協議会（ISOG-J）、…
- または、NCA Annual Conferenceの懇親会に参加したり、登壇者と話すことも有用です。

まずは、できるところから変えていく、必要があると考えます。

# Appendix

- 脆弱性管理
  - JIS Q 27000/31000
    - https://www.jisc.go.jp/index.html：検索ののち、利用者登録が必要
  - KEV Catalog
    - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
  - EPSS
    - https://www.first.org/epss/
    - My favorite tool
      - https://github.com/hogehuga/epss-db：EPSSを分析できるツール
      - https://github.com/hogehuga/threatWatchDog：EPSSの前日差分を通知するツール
- リスク評価/管理
  - NIST SP 800-30
    - https://www.ipa.go.jp/security/reports/oversea/nist/about.html：PDFへのリンク一覧
  - OWASP Risk Rating Methodorogy
    - https://owasp.org/www-community/OWASP_Risk_Rating_Methodology：英語リソース
    - https://blog.owaspjapan.org/post/168241186214/owaspriskratingmethodologyjapanese：日本語リソース
- リスクベース脆弱性管理
  - ツール
    - https://github.com/TURROKS/CVE_Prioritizer：CVE_Prioritizer
    - https://github.com/xaitax/SploitScan：SploitScan
  - ITU-T X.1060
    - https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/X1060.aspx：特設サイト
    - https://www.itu.int/rec/T-REC-X.1060-202106-I：ITU-T掲示
    - https://www.ttc.or.jp/document_db/information/view_express_entity/1423：日本語版
  - ISOG-J セキュリティ対応組織の教科書 3.2版
    - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
  - ISOG-J トリアージガイドライン作成の手引き
    - https://isog-j.org/output/2024/TriageGuidelines.html
  - NCA 脆弱性管理の手引書 システム管理者編1.0版
    - https://www.nca.gr.jp/activity/pub_doc/_10.html
  - 経済産業省 サイバーセキュリティ経営ガイドライン
    - https://www.meti.go.jp/policy/netsecurity/mng_guide.html

- SSVC
  - CISA
    - https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc
    - https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf
  - Carnegie Mellon University
    - https://insights.sei.cmu.edu/library/prioritizing-vulnerability-response-a-stakeholder-specific-vulnerability-categorization-version-20/
  - SSVC Calcurator
    - https://www.cisa.gov/ssvc-calculator
      - CISA Coordinator Treeのみ利用可能
    - https://certcc.github.io/SSVC/ssvc-calc/
      - 色々なDecision Treeを確認できる

TLP:CLEAR

※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。