

あつまれ！運用ピーポー

～脆弱性対応方法の振り返りと、今後の展開～

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部

井上圭



運用での脆弱性対応は、様々な制約が多く困難が多いと思います。

今回は最近話題になっている、SBOM/CVSS v4/EPSSなどを説明しつつ、脆弱性対応が少しでも楽になるための方法を考えてと思います。

Agendaは以下の通りです。

1. 脆弱性対応の現状
2. 脆弱性対応の課題
3. 課題に対するヒント
4. 未来に向けて（まとめ）

SBOMやCVSS v4などの新たな指標の話をします。

これらをうまく利用するために

- 現状の振り返り
- 新たな指標の意図と、どのように活用できるのかを話します。

Profile



井上圭

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 企画部

セキュリティ運用、特に脆弱性管理を検討や講演を行っています。
非IT企業の情報システム部やMSPでの他社システムの運用等を20年ほど行い、
その中で得た知見を基に脆弱性管理について検討や講演、個人主催の勉強会などを実施しています。

所属団体

- ・ ISOG-J WG1（トリアージガイドライン作成のための手引き）
- ・ ISOG-J WG6（セキュリティ対応組織の教科書 / X.1060）
- ・ JNSA 教育部会、産学連携プロジェクト/ゲーム教育WG
- ・ 一般社団法人日本シーサート協議会 脆弱性管理WG

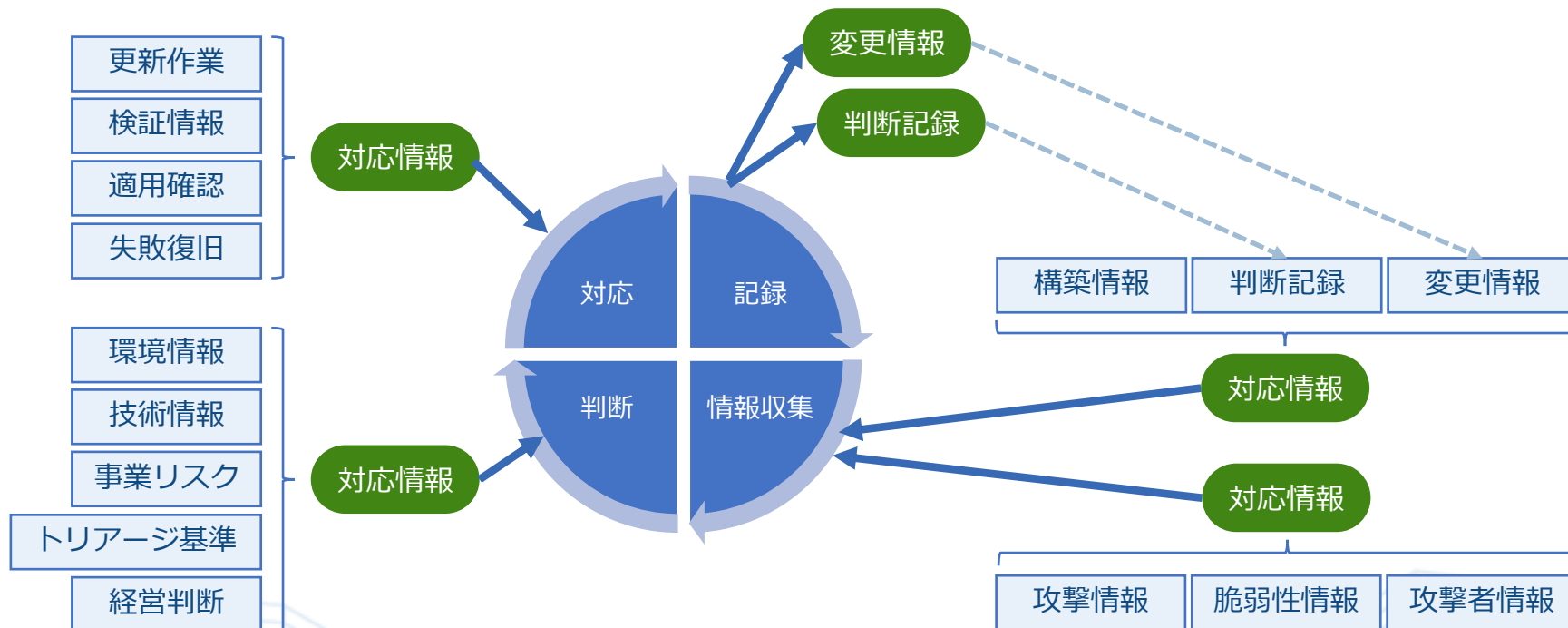
01 脆弱性対応の現状

脆弱性対応について、一般的な現状について振り返ります。
脆弱性対応といっても対象は多岐にわたる為、以下のような分類で考えることが多いです。



今回は、CVE-IDが付与されるような、主にアプリケーションおよびプラットフォームの脆弱性に関する話をします。

脆弱性対応の際に、以下のような運用フローを用いることが多いです。



この際、脆弱性対応として更新プログラム適用可否や対応順番の判断を、トライアージ（対応優先度判定）で決定していると思います。

トライアージをどのように行うかは、組織により異なります。

- CVSS Base Scoreが8.0以上は対応する、等

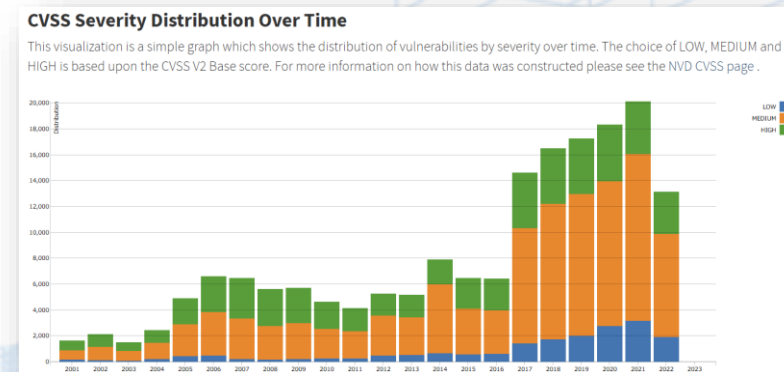
02 脆弱性対応の課題

先述のような脆弱性対応を行う場合、おおよそ以下のような課題が発生します。

- トリアージの判断基準はどうすればよいのか
 - ex.) CVSS Base Scoreが8.0以上の脆弱性に対応する、本当に8.0でいいのか…
- 脆弱性が多すぎて対応できない
 - ex.) Base Score 8.0以上だと、全体で1,000件以上未対応の脆弱性になる…
- そもそも、対象すべてを把握しているのか不明
 - ex.) 認知している アプリやライブラリ、これが全てなのか分からない…

これらを解決する助けとなる、最近話題になりつつあるフレームワークについてお話しします。

- CVSS v4, EPSS, KEV Catalog, SBOM



脆弱性は、近年大量に報告されている

出典：[NVD - CVSS Severity Distribution Over Time \(nist.gov\)](https://nvd.nist.gov/cvss-severity-distribution-over-time)

03 課題に対するヒント

脆弱性対応/管理は、多くの組織で課題を抱えています。一般的には以下の点を工夫することで、改善ができます。

- 組織体制
- システムの把握
- トリアージによる優先度選別
- 対応の省力化

今回はトリアージによる優先度選別について、課題解決のヒントになると思われるフレームワークを提示します。

これらのフレームワークを利用することで、以下の恩恵を得られます。

- トリアージにより、緊急性の低いものを後回しにする
- 緊急性が高いものを優先することで、攻撃されるリスクを下げる
- トリアージにより選別されることで、同時に対応しなければいけない脆弱性の数を減らせる



CVSS v4概要

- FIRSTから2023/11/01に正式発表された、ソフトウェアの脆弱性と重大度を伝達するためのフレームワークです。
- 4つの基準で構成されます。
 - 基本基準／環境基準／脅威評価基準／補足基準
- 既存のCVSS v3.1からの、項目更新や追加があります。
 - 現在のシステム環境に合わせて、評価項目が更新されています。


現時点ではまだCVSS v4での情報提供が標準化しているわけではありません。
実質的にはしばらく様子見をしつつ、順次 CVSS v3.1から切り替わると思われます。

Metrics

CVSS Version 4.0CVSS Version 3.xCVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

 **NIST: NVD**

N/A

NVD assessment not yet provided.

基本評価基準

Base Metric Group

Exploitability Metrics

攻撃元区分

攻撃条件の複雑さ

攻撃実行条件

必要な特権レベル

ユーザ関与レベル

Impact Metrics

脆弱なシステムの
機密性への影響

脆弱なシステムの
完全性への影響

脆弱なシステムの
可用性への影響

後続システムの
機密性への影響

後続システムの
完全性への影響

後続システムの
可用性への影響

脅威評価基準

Threat Metric Group

脆弱なシステムの
機密性への影響

環境評価基準

Environmental Metric Group

Modified Base Metrics

- ・ 攻撃元区分
- ・ 攻撃条件の複雑さ
- ・ 攻撃実行条件
- ・ 必要な特権レベル
- ・ ユーザ関与レベル
- ・ 脆弱なシステムの機密性への影響
- ・ 脆弱なシステムの完全性への影響
- ・ 脆弱なシステムの可用性への影響
- ・ 後続システムの機密性への影響
- ・ 後続システムの完全性への影響
- ・ 後続システムの可用性への影響

対象システムの
機密性への要求度

対象システムの
完全性への要求度

対象システムの
可用性への要求度

補足評価基準

Supplemental Metric Group

自動化

回復性

安全性

価値密度

対応の困難性

サプライヤの緊急度

スコアへの
影響

影響あり

影響なし

提供者

サプライヤ

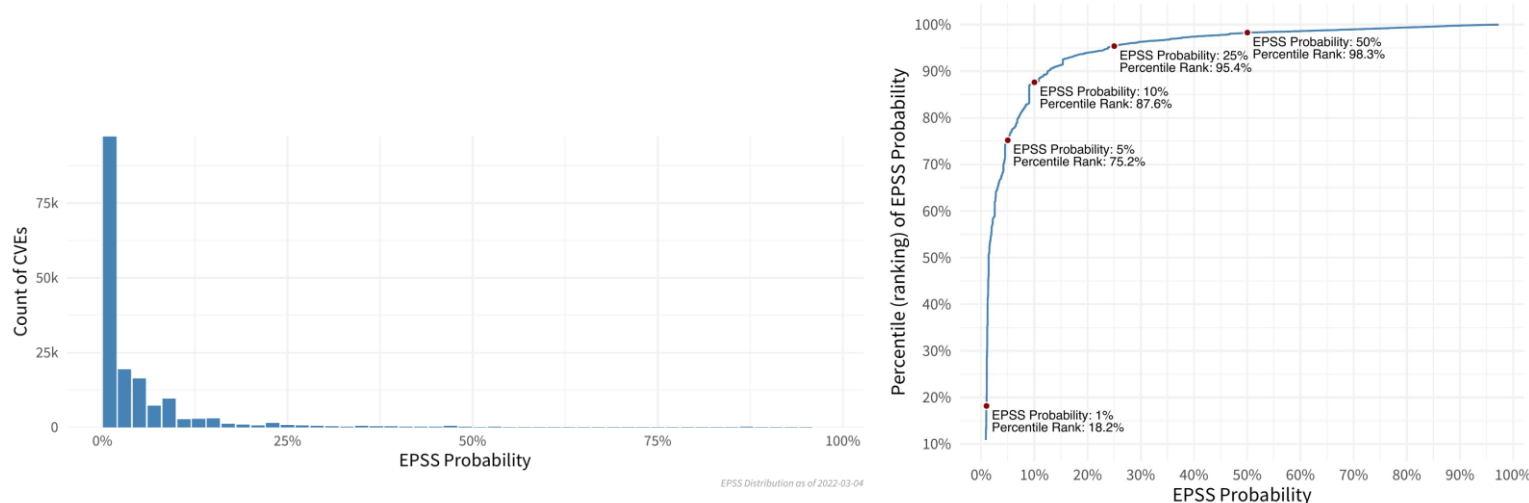
利用者

サプライヤ

EPSS概要

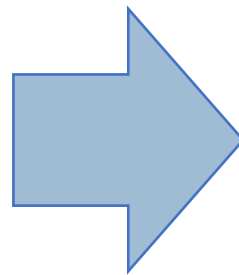
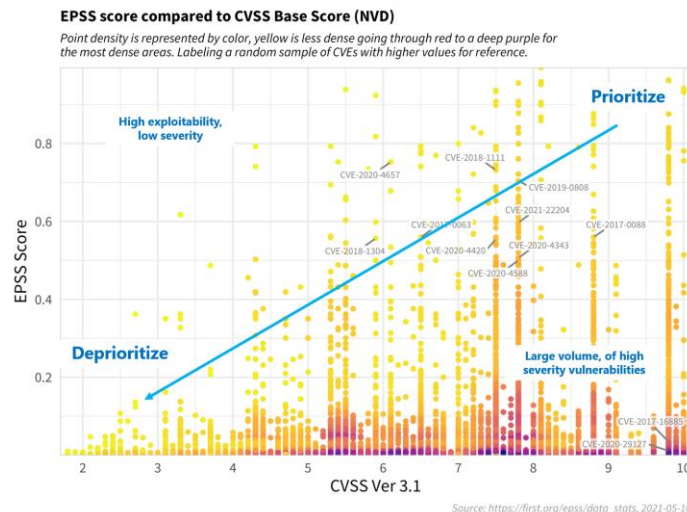
- Exploit予測スコアリングシステム、の略です。
- 今後30日以内に脆弱性が悪用される確率を示したものです。
 - Probability : 上記確率で、対象の脆弱性それ自体が悪用される
 - Percentile : EPSSスコアが同等またはそれ以下のすべてのスコアの割合
- 0～1の確率スコアを生成し、スコアが高いほど悪用される可能性が高くなります。

```
{
  "status": "OK",
  "status-code": 200,
  "version": "1.0",
  "access-control-allow-headers": "x-requested-with",
  "access": "public",
  "total": 1,
  "offset": 0,
  "limit": 100,
  "data": [
    {
      "cve": "CVE-2022-27225",
      "epss": "0.001500000",
      "percentile": "0.515590000",
      "date": "2024-07-10"
    }
  ]
}
```



考慮点

- 単独の確率スコアである probability では、判断が難しいです。
 - 悪用の証拠がある場合は、EPSSは使用しないべきです。（ExploitやCampaignsなど）
 - EPSSはリスク全体像ではありません。特定の環境やそれを補う制御全体を考慮せず、悪用された脆弱性の影響を推定する試みも行いません。
- 「リスク=脆弱性 x 脅威 x 資産」であり、CVSSやEPSSは「脆弱性」と「脅威」は表現できますが、資産や置かれている環境などの複合的な要因は考慮しません。

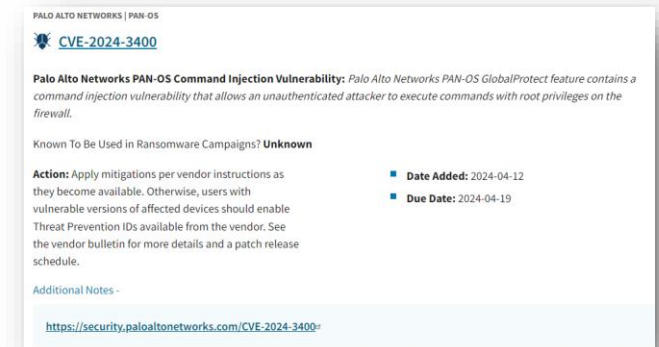


EPSS Score	悪用可能性：大 脆弱性影響：小 ＝事業リスク：小	悪用可能性：大 脆弱性影響：大 ＝事業リスク：大
	悪用可能性：大 脆弱性影響：小 ＝事業リスク：小	悪用可能性：小 脆弱性影響：大 ＝事業リスク：中
CVSS Base Score		

c. KEV Catalog(Known Exploited Vulnerability Catalog)

KEV Catalog概要

- CISAが公開している、実際に悪用が確認された脆弱性のリストです。
 - CISA : Cybersecurity & Infrastructure Security Agency
- 米国に於いては、すべての連邦文民行政府機関は「拘束力のある運用指令22-01（BOD 22-01）」に基づき、所定期間内に対象の脆弱性に対応する必要があります。
 - 2021年より前に割り当てられたCVE-IDを持つ脆弱性は、6か月以内に対応する
 - その他すべての脆弱性は、2週間以内に対応する
 - 未対応については罰則が存在する
- CISAとしては、「脆弱性管理計画の一部としてKEVカタログの脆弱性に直ちに対処するという要件を含めることを強く推奨します」としています。



考慮点

- 基本的に米国での悪用状況を基にしているため、参考情報とすべきです。
 - 米国向けであり、他国という地域性は考慮されていない。日本向けの個別の悪用が存在したとしても、KEV Catalogには登録されないと考えられる
 - しかしながら、「米国で悪用される＝グローバルで悪用される」という可能性は高く、日本でも意味があると考えられる
- EPSSが「すでに悪用された情報があれば、そちらを参考にすべき」としている部分の、参考情報ともなります。
 - EPSSは「悪用される確率」だが、KEV Catalogは「悪用されたCVE-IDのリスト」

上記のような考慮点はあるものの、KEV Catalog記載のCVE-IDを優先的に対応することで、被害に遭う確率を低減できると考えられます。

SBOM概要

- ソフトウェアコンポーネントやそれらの依存関係を一覧化した、ソフトウェア部品表と呼ばれる管理手法です。
- 全体の説明としては、経済産業省の「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等の検討タスクフォースの検討の方向性」が良くまとまっています。



最小構成要素 (Minimum Elements)	
データフィールド	必要な各コンポーネントに関するベースライン情報を文書化： サプライヤー、コンポーネント名、コンポーネントのバージョン、その他一意の識別子、依存関係、SBOMデータの作成者、タイムスタンプ
自動化への対応	自動生成や自動化のサポート： 機械可読性、フォーマットとしてのSPDX/SWID tag/CycloneDX
慣行およびプロセス	SBOMのリクエスト/生成/使用などの定義： 頻度、改装の深さ、依存関係の未知の明示、配布/配信、アクセス制御、間違いの許容

出展：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/006_03_00.pdf

出展：The Minimum Elements For Software Bill of Materials(SBOM)
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

考慮点

- ツールを入れればよい、というものではないことに注意が必要です。
 - 出力すれば終わりではなく、都度更新が必要
 - ツールのカバー範囲は限度があり、どの範囲まで/どの粒度で 管理をするかは決める必要がある
- サプライチェーン管理で必要ですが、考慮点があります。
 - 委託先等に、SBOMを出力/維持管理する工数が必要
 - また、ツール利用を現契約のまま強制することは下請法上できず、調整が必要
- 資産管理の一部として実装し、次のステップで脆弱性管理に利用する、という導入のほうが一般的には良いかもしれません。



82ページほどありますが、経済産業省「ソフトウェア管理に向けたSBOMの導入に関する手引き」も参考にするのが良いと考えます。

- <https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html>

04 未来に向けて

脆弱性管理で有用なフレームワークについて紹介しました。

フレームワークではないですが、ISOG-Jから有用なガイドラインも出ているので、そちらも参考になると思います。

- ISOG-J WG1: 脆弱性トリアージガイドライン作成の手引き
 - 脆弱性トリアージをどのように設計するかのガイドライン
 - <https://isog-j.org/output/2024/TriageGuidelines.html>
- ISOG-J WG6: セキュリティ対応組織の教科書
 - CSIRTやSOCなどが、どのような機能を実装すべきか等が示されている
 - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html

これらの情報を基に、最終的には自分（自組織）で対応を決める必要があります。
本講演で紹介したものがその手助けになればと思います。

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。

※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。





※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。

※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。