あつまれ！運用ピーポー
～脆弱性対応方法の振返りと、今後の展開～

2023年11月20日

フューチャー株式会社 Cyber Security Innovation Group
井上圭
k.inoue.xz@future.co.jp

[TLP:GREEN]

概要

運用での脆弱性対応は、何かと制限が多く大変だと思います。

今回は最近話題になっているSBOMやCVSS v4や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たいと思います。

本日は以下の話をします。

1. 脆弱性対応の現状
2. 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し運用を楽にする為に
- 現状を振り返り
- 新たなものがどのように使えるのか

を話すべきと考えています。

whoami

井上圭

- フューチャー株式会社 Cyber Security Innovation Group（CSIG）
- シニアコンサルタント
  - 脆弱性対応に関しての情報を提供し、対策を提示する仕事

業務内容

- セキュリティコンサルタント
- 脆弱性対応製品 FutureVuls 販売/サポート
- JNSA、ISOG-J加盟（JNSA教育部会、ISOG-J WG1,WG6,他）
- 講演等
  - NICTサイバーコロッセオ 脆弱性診断実務、Janog52、CodeBlue Opentalks、etc
- 勉強会開催
  - Vuls祭り、脆弱性対応勉強会、塩尻サイバーセキュリティ勉強会、他

業種	就業年
警備会社	約10年
MSP	約10年
健保組合	0.5年
コンサル	約5年

[TLP:GREEN]

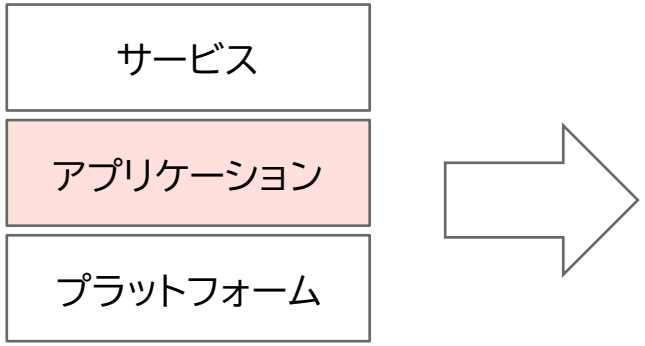
1. 脆弱性対応の現状

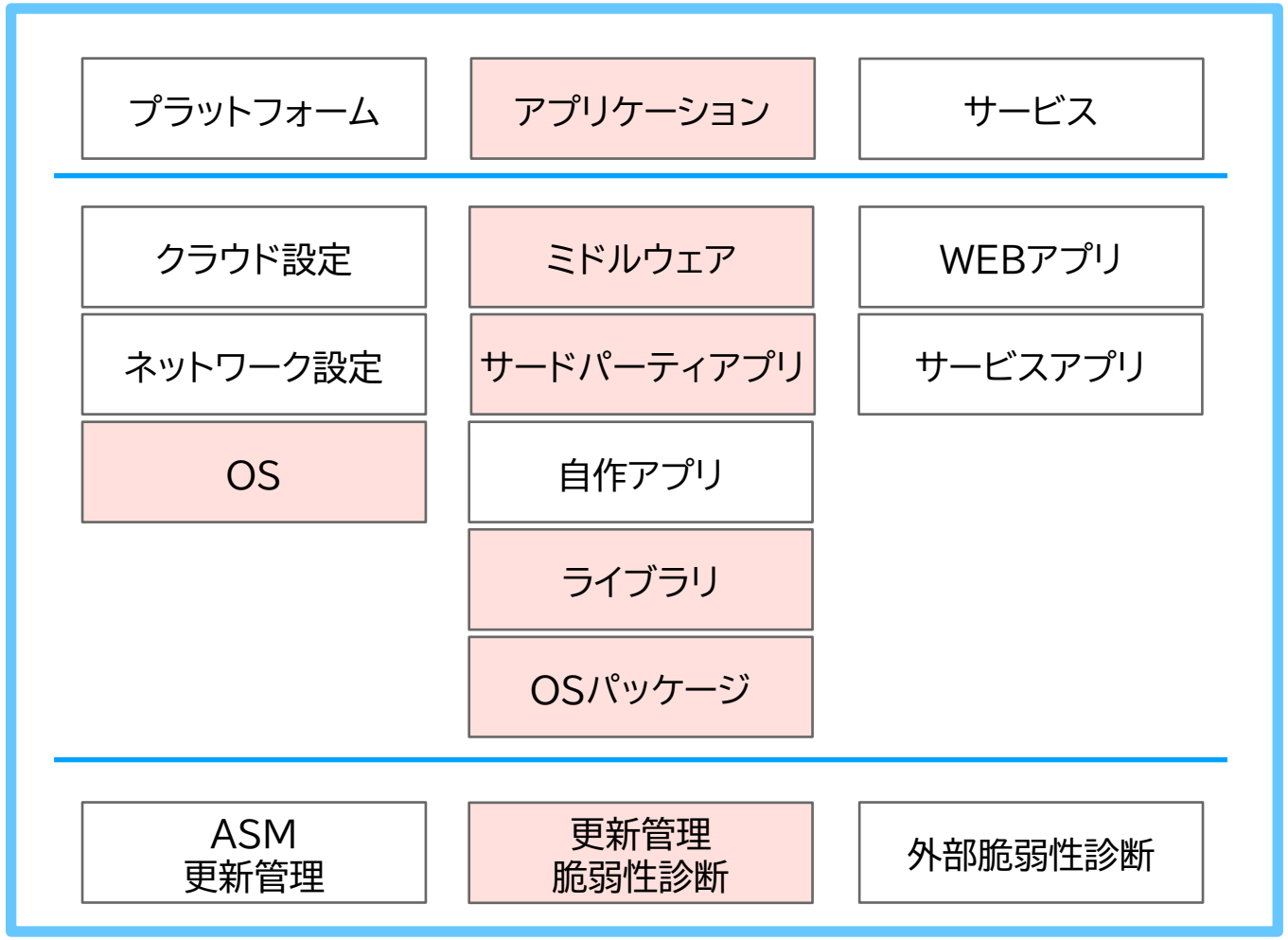
脆弱性対応の現状について、再確認

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渡るため、以下のような分類を持って考えることが多いです。



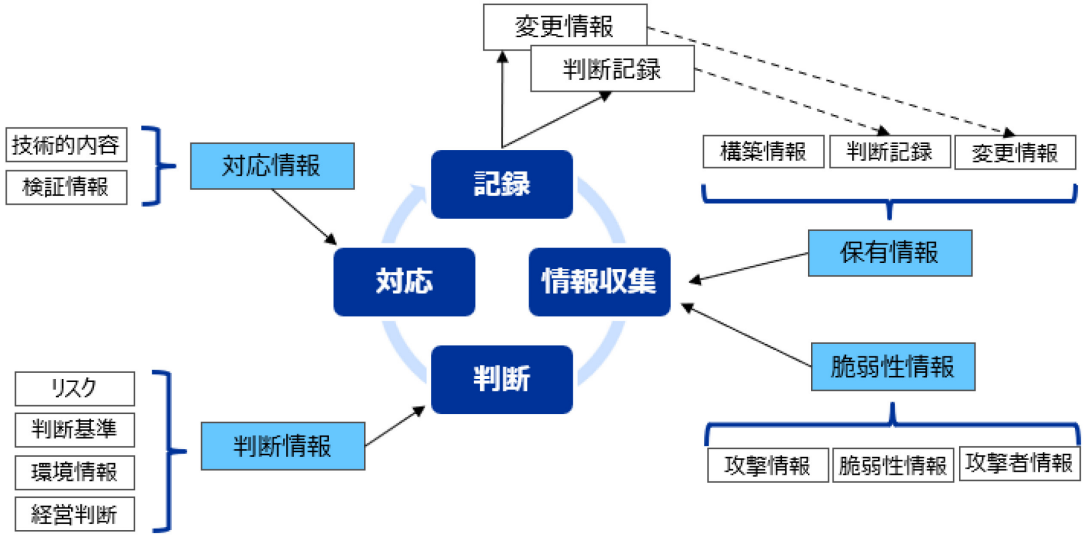


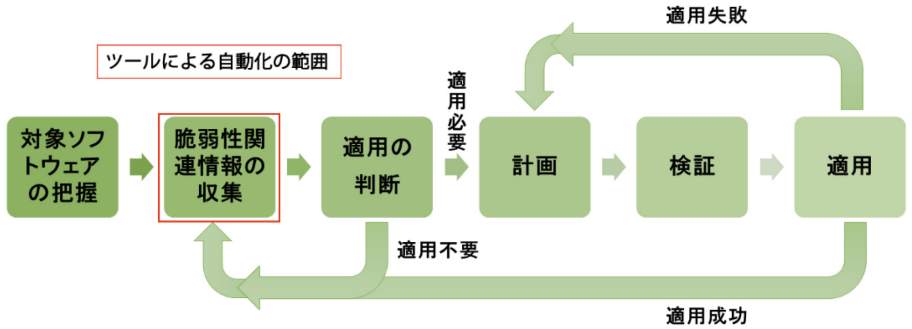
今回の話は、CVE-IDが付与されるような、主にアプリケーション脆弱性に関連する部分です。

[TLP:GREEN]

対応フロー

アプリケーションの脆弱性対応の際に、以下のような運用フローで対応することが多いと思います。





JPCERT/CC脆弱性対策の効果的な進め方 ツール活用編
https://www.ipa.go.jp/topic/isec-technicalwatch-201902.html

この際、脆弱性対応としての更新プログラム適用要否/対応順番の判断を、「トリアージ」で決定していると思います。

トリアージとしてどのように判断しているかは、組織により異なると思います。

- CVSS Base Scoreが8.0以上のものは対応する、等

[TLP:GREEN]

2. 課題

脆弱性運用における課題

脆弱性対応の課題

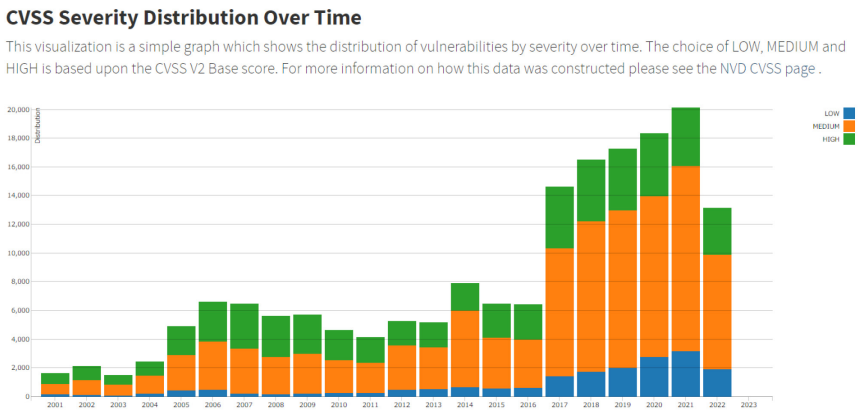
以上のような脆弱性対応をする場合、おおよそ以下のような課題が出てきます。

- トリアージの判断基準はどうすればいいのか
  - ex. CVSS v3.x BaseScoreが8.0以上は対応する社内ルール…
- 数が多すぎて対応ができない
  - ex. BaseScore8.0以上だと、全体で1,000件以上未対応の脆弱性がある…
- そもそも、全数を把握していたのか
  - ex. そもそも何のアプリを使っていたのか、使っているアプリはどのライブラリを使っているのか…

これらを解決する一助となる、最近話題になりつつある

- CVSSv4, EPSS, KEVCatalog SBOM

についてお話しようと思います。



出展:
https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

[TLP:GREEN]

3. 課題に対するヒント

新たに利用できる指標について

CVSSv4, EPSS, SBOM, KEV Catalog

脆弱性の評価手法である CVSS v4が2023/11/01に一般提供（GA）として正式にリリースされました。これに合わせるように、他の脆弱性管理で有用と思われる指標も注目されるようになりました。

各指標のの特徴や使い所についてお話します。

- CVSSv4（Common Vulnerability Scoring System）
- EPSS（The Exploit Prediction Scoring System）
- KEV Catalog（Known Exploited Vulnerability Catalog）
- SBOM（Software Bill-Of Material）

Common Vulnerability Scoring System(CVSS) v4(1/4)

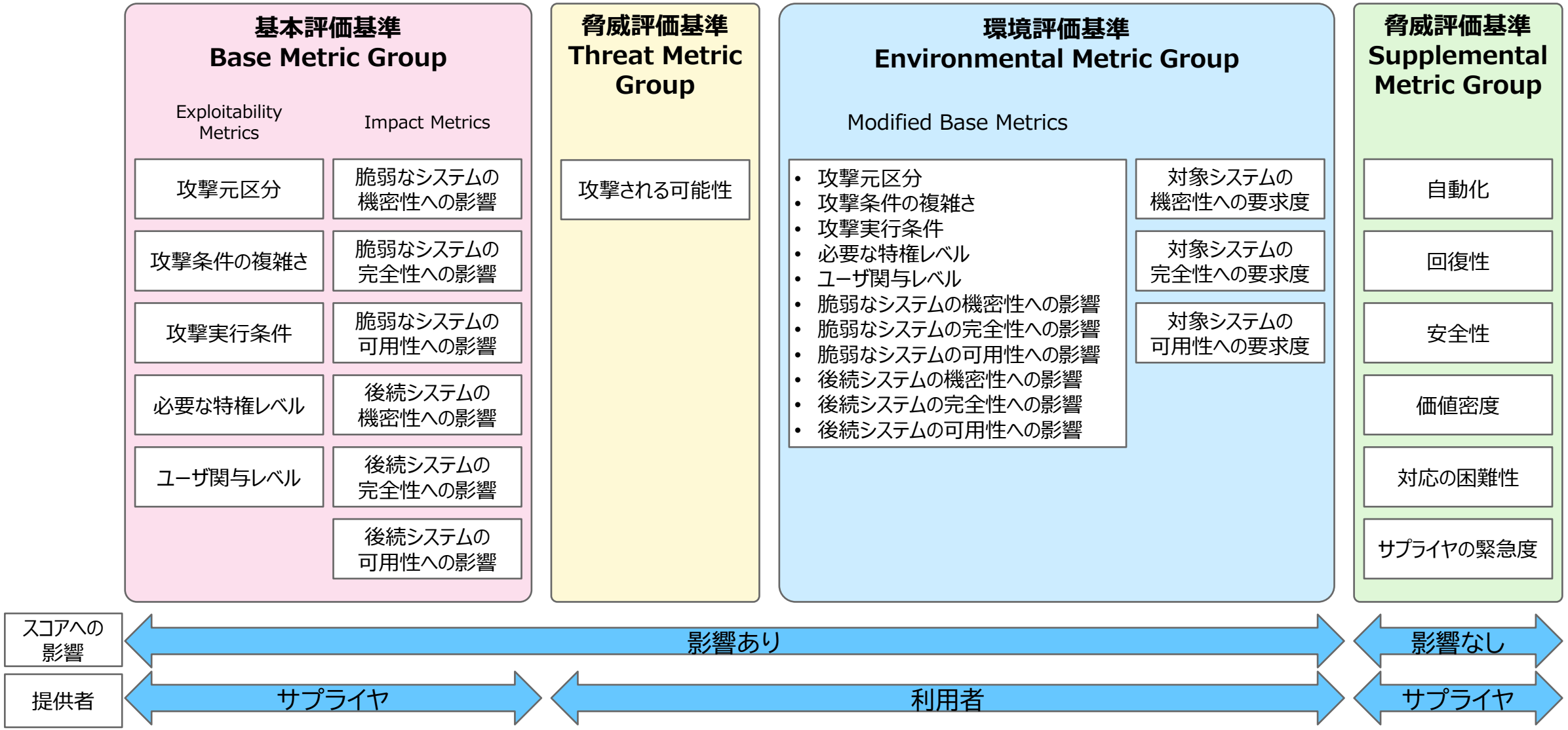
CVSS v4とは

- 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。
- 大きく３つの指標に分かれています。
  - 基本指標/環境指標/脅威指標 があり、補足情報としてのSupplemental Metricsも定義されています。
- 既存のCVSS v3.1から、項目の更新や追加があります。
  - 現在の環境に合わせて、評価項目が更新されています。
  - SSVC（Stakeholder-Specific Vulnerability Categorization）と互換のある項目も多いです。

Metrics	説明
Base Metrics （基本評価基準）	時間経過や環境に依存しない、脆弱性の本質的な性質を示す
Environmental Metrics （環境評価基準）	ユーザ固有の脆弱性の特性を示す
Threat Metrics （脅威評価基準）	時間の経過とともに変化する脆弱性の特性を示す
Supplemental Metrics （補足指標）	完全にオプションの、サプライヤやベンダからの情報

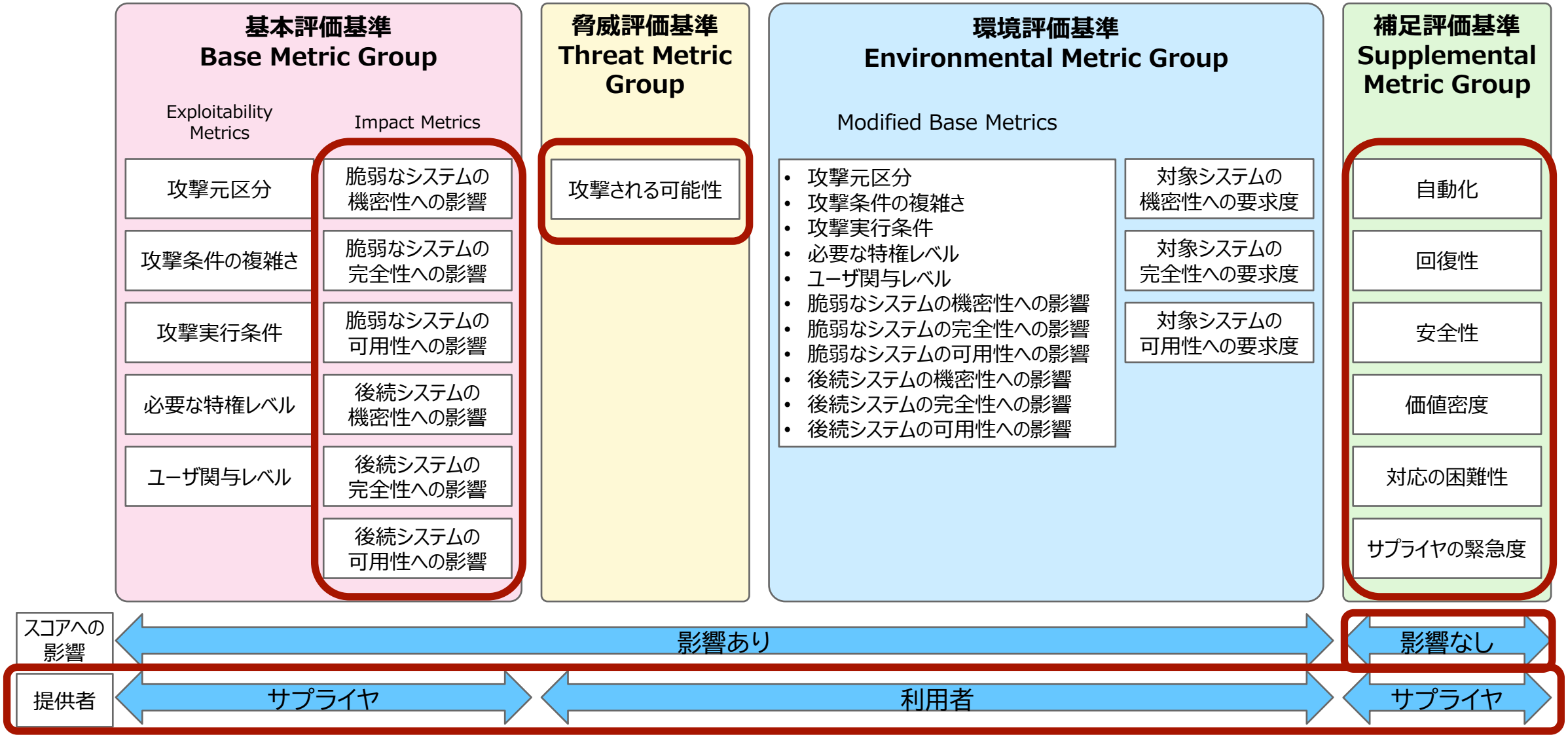
CVSSの命名法	使用されるメトリクス
CVSS-B	基本指標
CVSS-BE	基本指標と環境指標
CVSS-BT	基本指標と脅威指標
CVSS-BTE	基本、脅威、環境の指標

CVSS v4(2/4)



[TLP:GREEN]

CVSS v4(3/4)



[TLP:GREEN]

CVSS v4(4/4)

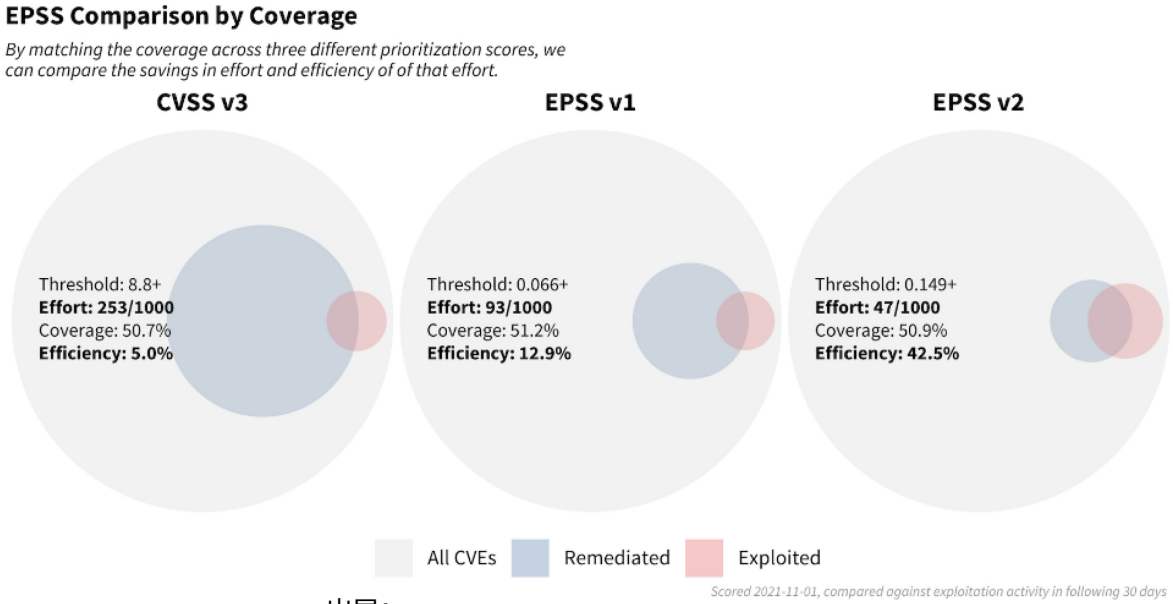
使い方

- Base metricsは、今まで通りの読み方でよいかもしれません
  - 一部項目統廃合はありますが、今まで通り理解は可能な内容のはずです。
- 基本的に、Base Metrics + Environmental Metrics (+Threat Metrics)を見るのが良いと思われます。
  - サプライヤが提供するBase Metricsに、システムの要求する（機密性|完全性|可用性）などを掛け合わせ、可能であればThreat Metricsとなる脅威情報（Exploit有無等）を含め、対応優先順位を決定するのが良いと思われます。
- 補足評価基準(Supplemental Metrics)を自ら用意することで、優先度判断に使えます。
  - 安全性（影響の大きさ）、回復性（攻撃実行後、自動回復可能か）、価値密度（対象のリソース）辺りは利用者で検討ができ、「リスクを低く見積もれる」のであれば優先度を下げられると思われます。
- 良い使い方は、CVSS v4でデータが提供されてから考えてもよさそうです
  - これを書いている2023/11/14時点では、NVDのデータではCVSS v4は提供されていません。

EPSS(1/4)

EPSSとは

- 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。
- 0-1の確立スコアを生成し、スコアが高いほど脆弱性が悪用される可能性が高くなります。
- 随時EPSSモデルも更新されています。
  - 初回リリースは2021/01/07、前回のメジャーアップデートは2022/02/04、EPSSモデルの最新アップデートは2023/03/07



出展：
https://www.first.org/epss/model

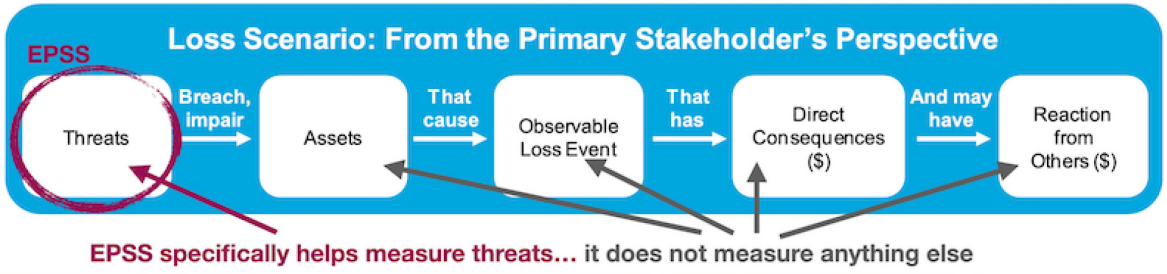
[TLP:GREEN]

EPSS(2/4)

FUTURE

注意点

- ExploitやCampaigns等の悪用の証拠がある場合は、EPSSは使用しないべきです。
  - EPSS は悪用活動の確率を推定するため、**他に積極的な悪用の証拠がない場合に EPSS を使用するのが最適**。
  - 悪用行為に関する証拠やその他の情報が入手可能な場合は、EPSS の推定値よりも優先されるべき 。
  - EPSS自体は、地域性のある攻撃や地域性のあるアプリケーションでは、正確に推定ができない。
    - ex. 日本だけでは使用されている攻撃、日本だけで使われているアプリケーション
- EPSS は、脆弱性が悪用される確率を推定しているだけです。**特定の環境やそれを補う制御を考慮せず、悪用された脆弱性の影響**を推定する試みも行いません。**EPSS はリスクの全体像ではありません。**
  - 所謂「リスク ＝ 脆弱性 x 脅威 x 資産」であり、脆弱性と脅威はCVSSやEPSSで表現できますが、脅威はシステムが置かれている環境に依存します。

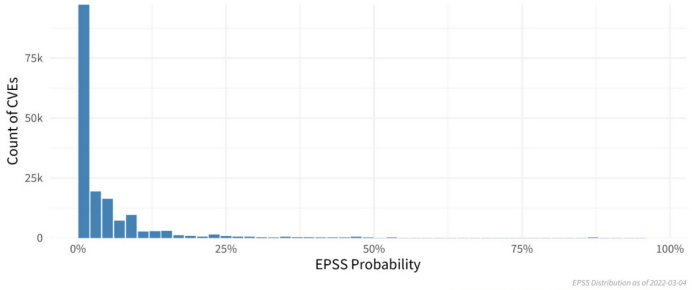


[TLP:GREEN]

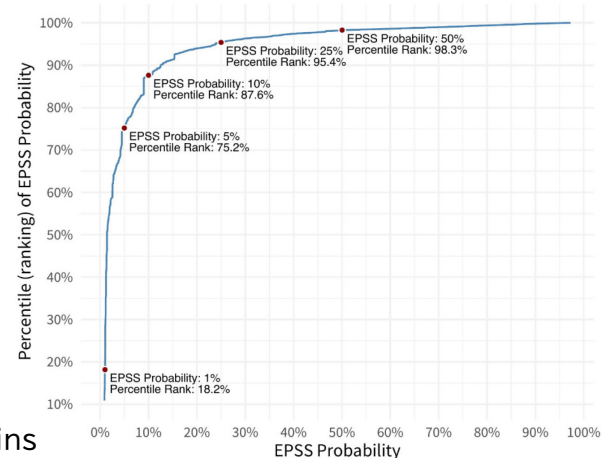
EPSS(3/5)

EPSSで提供される項目「EPSS Probability」「Percentile」は異なるので注意が必要。

- EPSS Probability
  - 所謂「今後30日の間に脆弱性が悪用される確率」で、スコアと呼ばれることが多いものです。
  - 対象の脆弱性それ自体の悪用される確率、として取り扱います。
  - 大多数の脆弱性のEPSSスコアは10-25%未満で、実際に悪用されるのは全脆弱性の5%の様です。
- Percentile
  - EPSSのスコアが、全体の中でどの位置にいるかを示すものです。
  - EPSSスコア10%の脆弱性は約88%タイルに相当します。EPSSでスコアリングされている脆弱性全体のうち88%の脆弱性は、この脆弱性より悪用される可能性が高いと読めます。
  - 但し、個別の脆弱性を検討する場合は、考慮しなくてもよいように思えます。



出展:
https://www.first.org/epss/articles/prob_percentile_bins

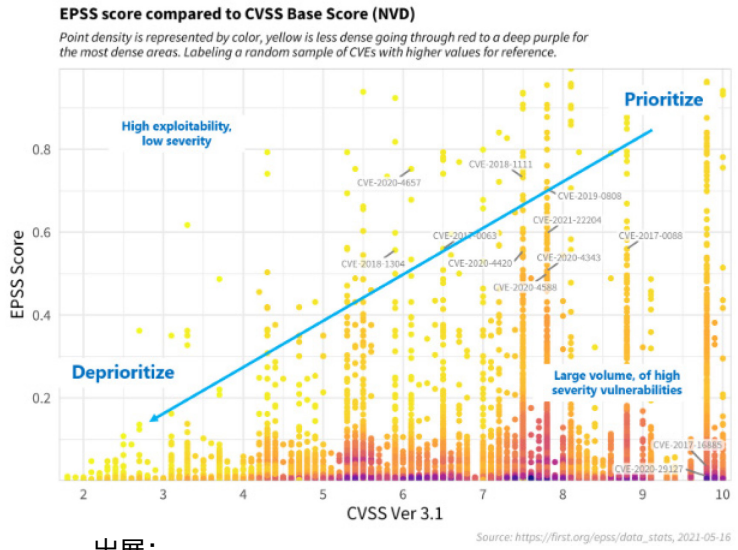


[TLP:GREEN]

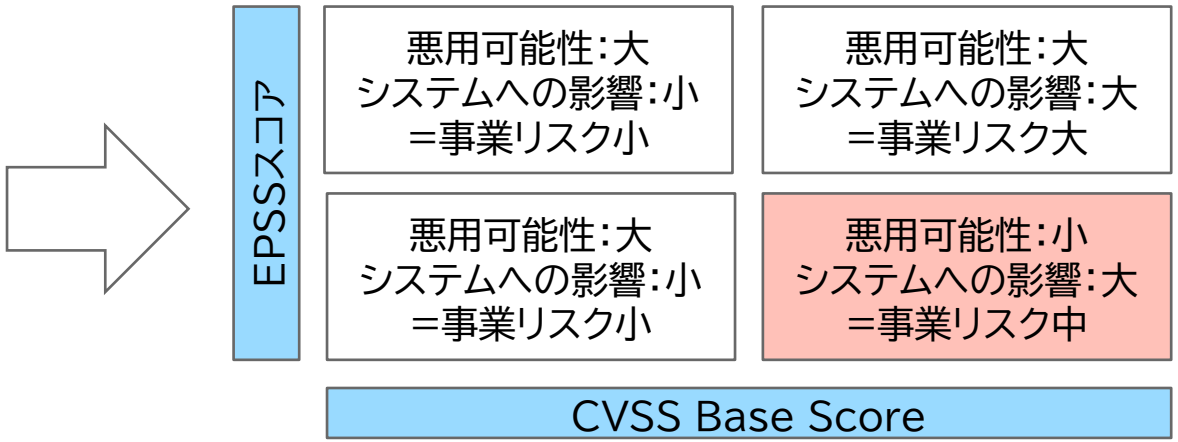
EPSS(4/5)

使い方

- 判断での活用方法
  - ➢CVSS Base ScoreとEPSSを比べ、双方のスコアが高いものから対応する、という判断ができます。
    - 左下：悪用化される可能性/システムに与える影響は低く、優先度を下げることができる
    - 左上：悪用される可能性は高いが、システムに与える影響は低く、優先度は高くないと言える
    - 右下：深刻な影響を与える可能性はあるものの、悪用される可能性は低く、要注意とする
    - 右上：悪用される可能性/システムに与える影響は高く、最初にパッチ適用すべきもの



出展:
https://www.first.org/epss/user-guide



EPSSスコアは、0.5を超える脆弱性は極わずかであり、判断基準とする際はこの値をベースに調整すると良いと思われる。

EPSSスコアだけを見るのではなく、情報システムに与える重大度という観点が必要。その際に、例えばCVSS Base Scoreを参考にする。

[TLP:GREEN]

EPSS(5/5)

FUTURE

使い方

- データを得る方法
  - ➢https://www.first.org/epss/api を参照します
  - APIで、期間やCVE-IDでフィルタして取得します
    - https://api.first.org/data/v1/epss?cve=CVE-2022-27225
    - https://api.first.org/data/v1/epss?cve=CVE-2022-42475&scope=time-series
    - https://api.first.org/data/v1/epss?order=!epss
  - 過去30日より前のデータが欲しい場合は、日付を指定してその日の全EPSSデータを取得します
    - https://epss.cyentia.com/epss_scores-YYYY-MM-DD.csv.gz
    - これをデータベース化する必要があるが、運用では必要ないと思われる
  - EPSSに対応した脆弱性管理製品を使うのが良いと思われます


```
{
  "status": "OK",
  "status-code": 200,
  "version": "1.0",
  "access": "public",
  "total": 1,
  "offset": 0,
  "limit": 100,
  "data": [
    {
      "cve": "CVE-2022-42475",
      "epss": "0.439150000",
      "percentile": "0.969990000",
      "date": "2023-11-12"
    }
  ]
}
```


[TLP:GREEN]

Known Exploited Vulnerability Catalog(KEV Catalog)

KEV Catalogとは

- 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
  - SSVCなどの脆弱性管理フレームワークで、脆弱性の悪用ステータスとして使用されることが想定されている
- 米国においては、すべての連邦文民行政府機関は「拘束力のある運用指令(BOD)22-01」に基づき、所定期間内にKEV Catalogに記載された脆弱性に対応する必要があります。
  - 2021年より前に割当てられた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
- 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。

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Known to be Used in Ransomware Campaigns	Notes
CVE-2023-47246	SysAid	SysAid Server	SysAid Server Path Traversal Vulnerability	2023-11-13	SysAid Server (on-premises version) contains a path traversal vulnerability that loads to code execution.	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.	2023-12-04	Unknown	https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification
CVE-2023-36844	Juniper	Junos OS	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	2023-11-13	Juniper Junos OS on EX Series contains a PHP external variable modification vulnerability that allows an unauthenticated, network-based attacker to control certain, important environment variables. Using a crafted request an attacker is able to modify certain PHP environment variables, leading to partial loss of integrity, which may allow chaining to other vulnerabilities.	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.	2023-11-17	Unknown	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US
					Juniper Junos OS on EX Series and SRX Series contains a PHP external				

[TLP:GREEN]

KEV Catalog(2/3)

使い方

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog にレコードが追加されます。
- “Due Data”は先述の、対処完了させる日（2週間or6か月）です。
- “Known to be used in Ransomware Campaigns”は、ランサムウェアキャンペーンで利用された場合に表示されます。
- 基本的には、悪用が確認された脆弱性であるため、必須で対処すべきものとして扱うのが良いと考えます。

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Due Date	Known to be Used in Ransomware Campaigns
CVE-2023-29552	IETF	Service Location Protocol (SLP)	Service Location Protocol (SLP) Denial-of-Service Vulnerability	2023-11-08	The Service Location Protocol (SLP) contains a denial-of-service (DoS) vulnerability that could allow an unauthenticated, remote attacker to register services and use spoofed UDP traffic to conduct a denial-of-service (DoS) attack with a significant amplification factor.	2023-11-29	Unknown

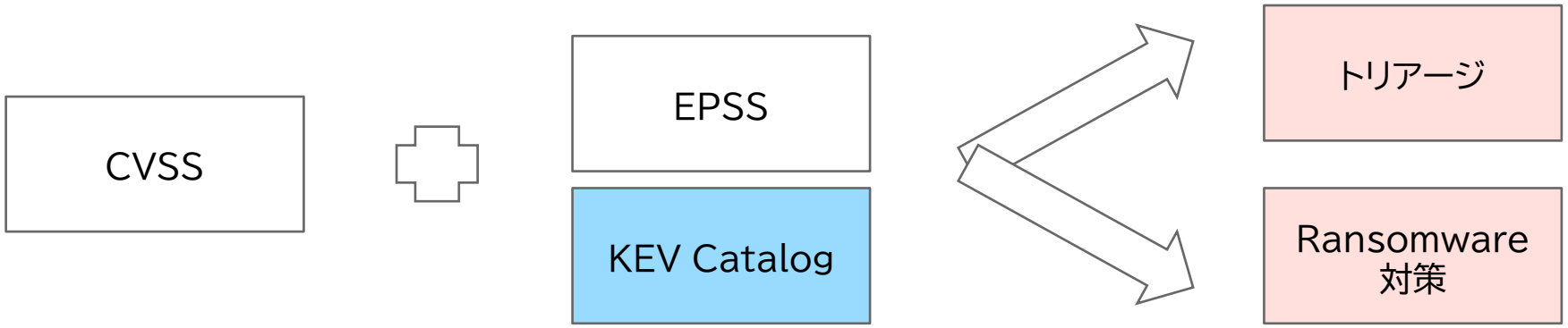
Action Apply mitigations per vendor instructions or disable SLP service or port 427/UDP on all systems running on untrusted networks, including those directly connected to the Internet.

Notes https://blogs.vmware.com/security/2023/04/vmware-response-to-cve-2023-29552-reflective-denial-of-service-dos-amplification-vulnerability-in-slp.html, https://www.suse.com/support/kb/doc/?id=000021051, https://security.netapp.com/advisory/ntap-20230426-0001/, https://www.cisa.gov/news-events/alerts/2023/04/25/abuse-service-location-protocol-may-lead-dos-attacks

KEV Catalog(3/3)

使い方

- 基本的には、KEV Catalogに登録されたものは、優先度高く対応したほうが良いと考えられます。
  - 日本では罰則のある対応ではない為、影響を受けるか/軽減策は取っているか などを優先的に調べる、という利用法になると考えます。
- 地域性等は考慮されていない為、「このリストに対応しておけば、他はやらなくてよい」というわけではないです。
  - なのでEPSS同様に、CVSS Base Scoreと合わせて判断を行う基準とするのが良いと思われます。



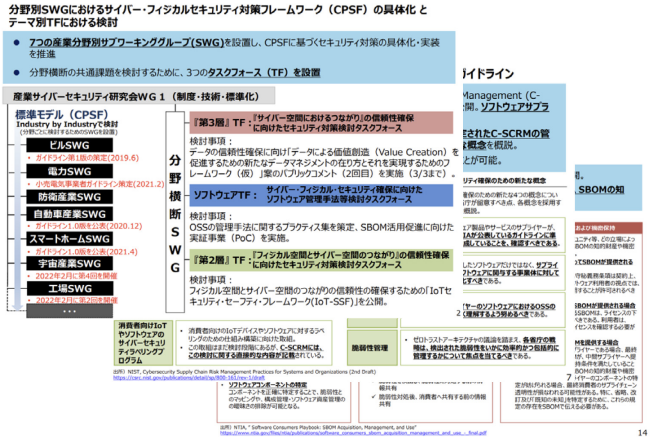
まとめ：どう使えるのか

各指標はおおよそ以下のように使えると考えます。

- CVSSv4（Common Vulnerability Scoring System）
  - 基本的なスコアリングで利用
  - 利用環境となるEnvironmentalを自分で用意することで、リスク判断精度が向上する
- EPSS（The Exploit Predicition Scoring System）
  - 脆弱性の危険度判断で利用
  - 但し、脆弱性の脅威の尺度であり、脅威情報があればそちらを優先し、CVSSのスコアに組込まない
- KEV Catalog（Known Exploited Vulnerability Catalog）
  - 既に悪用がされている脆弱性＝優先修正対象、と考えて対応を検討する材料
  - Ransomware Campaigns項目は、脆弱性管理対象によっては有用
- SBOM（Software Bill-Of Material）
  - どのようなソフトウェアやライブラリなどが使われているかを、まとめて記載するもの
  - 急ぐ必要はないが、今後対応ができるようにしていく必要がある
  - どこまでを責任範囲にするか、を今から議論していく必要がある

SBOM(Software Bill of Material)(1/)

- what is SBOM
  - 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。
  - フォーマットは、SPDX、SWID、CycloneDXなど複数が存在しています。
  - 構成要素として、最小要素は定義されています。
    - SBOMを出力するソフトウェア間で、最小要素を特定のフォーマットを通じて共有ができるように設計されています。
  - 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る。



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

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SPDX, SWIDタグ, CycloneDX
慣行及びプロセス	SBOMのリクエスト/生成/使用などの定義： 頻度、階層の深さ、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:The Minimum Elements For Software Bill of Materials(SBOM)
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[TLP:GREEN]

SBOM(2/)

本日ここで述べるべきは、技術的な観点ではなく、運用的な観点と考えます。

注意点（Negative）

- SBOMは、サプライチェーンセキュリティ対策で「使える」ものですが、SBOMがあればサプライチェーンを守れる、というものではないです。
  - 一部で、目的と手段の混同が見受けられます。「どのタイミングで取得するのか」「対象となる範囲はどうするのか」「どのように活用するのか」等は運用側で決めていく必要があり、それらが整備されていなければSBOMは持っていても価値はないです。
- どこまでをSBOMの依存関係に含めるのか、責任範囲はどこまでとするのかの議論がされていません。
  - 例えば、クラウドサービスであれば事業者と利用者の責任分界点はよく話題になります。
  - SBOMに関しては、どこまでSBOMを追跡するのかという点が議論されていません。
    - ルータのSBOMは、ユーザ側で必要でしょうか？ルータのopensslのバージョンをユーザが管理できますか？
- SBOM自体で脆弱性が正確に特定できるわけではないです。
  - 記載されているCPEやpurlなどを脆弱性データベースと突き合わせて特定します。CPEは精度が低いです。

SBOM(3/)

注意点（negative）

- 国としての方針が、現時点では定まっていません。
  - 米国では大統領の指示を受けたNISTがガイダンスとして出しています。これは連邦政府機関を守る＝国防 という観点で全体を進めていることを示しています。
  - 対して日本では、経済産業省や総務省が取り組みを進めていますが、上記のようなポリシーで進めているようではなく、実証実験後の総括もなく、国としてどう進めるべきかが明確となっていません。
  - 結果、責任分界点の議論等はされておらず、SBOMを使うためのSBOMの話になってきているように見える。
- ベンダやサプライチェーン下流がまだ対応していない事が多い
  - 大企業であればサプライチェーン全体で対応可能だが、現状はそうではない事が多い。

注意点（positive）

- 利用コンポーネントが特定できるようになり、インシデント対応が楽になる。
  - “log4jを使っているか？”などを調べることができるようになり、サプライチェーン全体でSBOMの管理ができるようになれば「自身は使っていないが、納品物には含まれているコンポーネント」なども分かる。

SBOM(4/)

どうあるべきか

- 全体として、急いで対応する必要はなさそうだが、対応できる準備を進めていく必要がある。
  - 医療や自動車業界など必須業界以外では、法的制限が無い為に急速に普及するとは思えません。
  - 現時点ではSBOMに対応したソフトウェア管理システムは少ないが、今後利活用が活発になるにことで使い勝手の良い製品が出てくると思われます。
  - フォーマット変換をすれば互換性があるはずなので、特定製品に依存はしなくてよくなるはずです。
- SBOM適用範囲を責任分界点で考える必要がある。
  - Q：「CiscoがSBOMを提供するといっていますが、御社には必要ですか？」
  - 何のためにSBOMを導入するのかを考え、自社の責任範囲/他社(ベンダ等)の責任範囲を切り分け、SBOMを取得/管理する範囲を考える必要があります。知っておきたいという好奇心と、業務で自社でやらなければいけない責任範囲、は異なります。

SBOMに関しては、「急いで入れる」よりも、「何のためにどこまでSBOMで保護するか」を考え、「責任分界点を決める」（SBOMを管理する範囲を決める）ことが現時点で重要と考えます。

4. 未来に向けて

SBOMやCVSS v4等の脆弱性対応で使えそうなものは出てきました。

しかしながらこれらを手動で組み合わせて使うのは、負荷が高いように思えます。自動化を意識した構成になっているため、何らかのツールや商用製品により自動化を進めるのが良いと考えます。

- トリアージであれば、SSVC（Stakeholder-Specific Vulnerability Categorization）などと連携ができ、自動で対応判断がある程度できます。

また、なるべく適用しないではなく、適用しても動くような構成にすることも必要です。運用者と開発者が協力することで、システム設計段階からセキュリティの考慮ができたシステムを作る、シフトレフトにより運用時の負荷を下げることができると考えます。

とはいえ、今できるところから利用していくとよいと思います。

まとめ

- CVSS v4
  - 脆弱性情報でv4が提供され始めてから、順次利用しましょう
  - Environmental Metricsや一部のSupplemental Metricsは、先に調べておいた方がよさそうです
- EPSS
  - 基本的には、脆弱性管理ツールが対応するのを待った方が良いと思います
  - とはいえ、APIで個別CVE-IDごとにデータを取り出し、トリアージで使ってみるとよいかもしれません
- KEV Catalog
  - 個人的には、記載されたものは対応必須とした方が安全と思われます
  - ransomwareに関連する項目は、クライアントの脆弱性管理の際には有用と思われます
- SBOM
  - 業界や法的に必須でなければ、浸透は遅いと思われます
  - しかしながら、準備をしておくことで、脆弱性対応などで役立ちます
  - まずは、なぜ/どこまでSBOMを使うのかを検討し、責任範囲を決めるのが重要と思われます

FUTURE

以上、ご清聴ありがとうございました。

時間により一部省略しておりますが、詳しい議論をしたい場合は、JNSAやISOG-J、脆弱性対応勉強会に参加いただくとよいと思われます。