Announcing CVSS v4.0 の意訳

意訳：脆弱性対応研究会

初めに

CVSS v4がリリースされましたが、ざっくりと理解するための資料が必要と考えます。
現時点(2023/11/02 JST)で最適と思われたのが、FIRSTCON23の"Annoucing CVSS v4.0"と思われたので、一部を意訳したものを公開します。

- 原文
  - https://www.first.org/cvss/v4-0/cvss-v40-presentation.pdf
- 原作者
  - Dave Dugal (Juniper Networks, USA)
  - Dale Rich (Black & Veatch, USA)
- 備考
  - TLP:CLEARだが無断翻訳の為、原文を参照のこと。

以降、有用と思われる部分のページを意訳しています。

CVSS v4.0: アジェンダ

- 共通脆弱性スコアリングシステム(CVSS)の紹介
- CVSS v3.1で特定された課題と機会
- CVSS v4.0の高レベルの目標
- より細かい粒度
- 下流のスコア付けの曖昧さの除去(read: Scope)
- 脅威指標の簡素化とスコアリングへの影響の向上
- 脆弱性対応のための補足属性
- OT/ICS/IoTへの追加適用性
- 新しいCVSS v4.0 Caの紹介
- CVSS v4.0アジェンダ(続き)
- 技術的な重大度とリスク(Technical Severity vs. Risk)
- CVSSをEPSSおよびSSVCと対比して比較する
- ドキュメントやトレーニングなど、CVSSを正しく使用するための現在のベストプラクティスを示す
- CVSSは単なるベーススコア(CVSS-BTE)ではありません
- CVSS v4.0パブリック プレビュー🎉

CVSS年表

- 先史時代(2005年以前)
  - ベンダーは、互換性のないカスタムの評価システムを使用して重大度を定義しました
  - NIACは、ソフトウェアとプラットフォーム全体で脆弱性測定を標準化する必要性を認識しました
- 2005年02月: CVSS バージョン1
  - CVSS v1は、業界で広く採用されることを目的として、少数の「先駆者」によって開発されました
  - リリース前に査読はほとんど受けられず、リリース後には多くの批判を受けました
  - 指標の定義があいまいなため、スコアリングとスコアの解釈が困難になりました
  - 2005年04月、NIACは、将来の開発のためのCVSSの管理者として、インシデント対応およびセキュリティチームのフォーラム(FIRST)を選択しました
- 2007年06月: CVSS バージョン2
  - CVSS-SIGの12名を超えるメンバーは、2006年から2007年にかけて広範囲に協力して、数百の現実世界の脆弱性をテストおよび再テストすることで、CVSS v1を改訂および改善しました
  - 不一致が減少し、粒度が向上し、(当時の)多種多様な脆弱性がより正確に反映されました

CVSS年表(続き)

- 2015年06月: CVSS バージョン3.0
  - 1つのソフトウェアコンポーネントに存在するが、別のソフトウェア、ハードウェア、またはネットワークコンポーネントに影響を与える脆弱性のスコアリングを処理するために、「スコープ」の概念を導入しました
  - また、条件を更新し(アクセス -> 攻撃)、必要な権限を追加し、低/高の導入により部分的な影響の「中間90%(middle 90%)」の問題を解決しました
- 2019年06月: CVSS バージョン3.1
  - 新しい指標や値を導入することなく、バージョン 3.0を明確にし、改善しました
  - 概念の明確さを改善して、標準の全体的な使いやすさを向上しました
  - CVSS拡張フレームワークを追加し、用語集を更新しました
  - CVSSは脆弱性の重大度を測定するように設計されており、リスクを評価するために単独で使用しないでください

CVSS年表(続き)

- 2022: CVSS バージョン 4.0
  - 正確なスコアリングのために、脅威インテリジェンスと環境メトリクスを使用をするのは重要
  - 運用技術/安全性の指標
  - 「自動化可能」「復旧」「脆弱性対応の取り組み」の補足概念
  - CVSS標準におけるプロバイダー提供の緊急度の表現
  - ユーザーインタラクションの、Active vs. Passive
  - 「攻撃の複雑さ」対「攻撃の要件」
  - 命名法

CVSS 3.1 の課題と批判

- リスク分析への主要な入力として使用される、CVSS基本スコア
- リアルタイムの脅威と補足的な影響の詳細が十分に表現されていない
- ITシステムにのみ適用される
- 健康、人の安全、産業用制御システムについては十分に説明されていない
- ベンダーが公開するスコアは、多くの場合、高(High)または重大(Critical)(7.0+)
- 粒度が不十分: 実際には個別のCVSSスコアが99未満
- 時間的メトリクスは、最終的なCVSSスコアに効果的に影響を与えない
- 数学は複雑すぎて、直観に反しているように思えます
- どこでその奇抜な公式を思いついたのですか？？？

What’s New in CVSS v4.0?

CVSS v4.0 の新機能の概要

- 基本メトリクスのより細かい粒度
  - 攻撃要件(AT;Attack Requirements)を、基本指標(Base Metrics)として追加
  - 強化されたユーザーインタラクションの粒度 (None/Active/Passive)
- 下流のスコア付けの曖昧さの除去(スコープ)
  - C/I/Aを、"脆弱なシステムのC/I/A"と"後続システムのC/I/A"に拡張
- 脅威指標の簡素化とスコアリングへの影響の向上
  - 修復レベル(Remediation Level)/レポートの信頼性(Report Confidence)/ExploitCodeの成熟度(Exploit Code Maturity)を、Exploitの成熟度(Exploit Maturity)に簡略化
- 脆弱性対応のための補足属性
  - 補足指標(metric): 自動化可能性(Automatable)
  - 補足指標(metric): 回復(Recovery)
  - 補足指標(metric): 価値密度(Value Density)
  - 補足指標(metric): 脆弱性対応の取り組み(Vulnerability Response Effort)
  - 補足指標(metric): プロバイダーの緊急度(Provider Urgency)
- OT/ICS/IoTへの追加適用性
  - 環境指標(Environmental Metrics)に安全指標値(Safety Metric)を追加

命名法(Nomenclature)

よく知られている通り、CVSSは単なるBase Scoreではありません。
この考えを強調するために、新しい命名法が採用されました。

- CVSS-B: CVSS Base Score
- CVSS-BT: CVSS Base Score + 脅威スコア(Threat Score)
- CVSS-BE: CVSS Base Score + 環境スコア(Environmental Score)
- CVSS-BTE: CVSS Base Score + 脅威 + 環境スコア

新しい基本指標: 攻撃要件(Attack Requirements)

問題点:

> AC値の"高""低"は、複雑さ"高い"の定義で現在圧縮されている条件間の大きな違いを反映していません。
> たとえば、ASLRや暗号化などのセキュリティ緩和手法を回避するには、競合状態に勝つために攻撃を繰り返すよりも、客観的に見てはるかに高いエクスプロイトの複雑さが必要です。
> しかし、現時点ではどちらの条件も最終的な重大度スコアに対して同じ「ペナルティ」をもたらします。

この提案は、現在のACの定義を「攻撃の複雑さ」(AC)と「攻撃の要件」(AT)と呼ばれる2つの指標に分割することで、この問題に対処することを目的としています。これらの指標は、それぞれ以下の内容を伝えます。

- 攻撃の複雑さ
  - 防御テクノロジーまたはセキュリティ強化テクノロジーを、回避または回避するために必要なエクスプロイトエンジニアリングの複雑さを反映します。(防御手段)
- 攻撃要件
  - 攻撃を可能にする脆弱なコンポーネントの前提条件を反映します。

更新された基本指標: ユーザーインタラクション

この提案の目的は、ユーザーと脆弱なコンポーネントとの対話を考慮する際に、さらなる粒度を考慮することです。詳細は次のとおりです。

なし (N: None)	脆弱なシステムは、攻撃者以外の人間のユーザーによる介入なしに悪用される可能性があります。
パッシブ (P: Passive)	この脆弱性の悪用に成功するには、対象となるユーザーによる脆弱なコンポーネントおよび攻撃者のペイロードとの対話を制限する必要があります。 これらの対話は非自発的なものとみなされ、脆弱なコンポーネントに組み込まれた保護をユーザーが積極的に無効にする必要はありません。
アクティブ (A: Active)	この脆弱性の悪用に成功するには、対象となるユーザーが脆弱なコンポーネントおよび攻撃者のペイロードに対して特定の意識的な操作を実行する必要があります。そうしないと、ユーザーの操作により保護メカニズムが積極的に破壊され、脆弱性の悪用につながります。

廃止された基本指標: スコープ👋

スコープは、これまでで最も愛されておらず、最も理解されていない CVSS指標である可能性があります。

- 製品プロバイダー間でスコアの不一致が発生した
- 脆弱なシステムおよび影響を受けるシステムの、影響の暗黙の「非可逆圧縮」

解決策として、インパクト指標が2つのセットに拡張されました。

- 脆弱なシステムの機密性(VC)、完全性(VI)、可用性(VA)
- 後続のシステムの機密性(SC)、完全性(SI)、可用性(SA)

それに応じて、環境指標(Environmental Metrics)は適宜更新されました。

Temporal → Threat Metric Group

(時間的指標を、脅威指標グループへ)

- 修復レベル(通常は O)とレポートの信頼性(通常は C)は終了しました
- Exploit Code MaturityがExploit Maturityに名前変更されました
- 脅威メトリック値の影響を強化しました

脅威インテリジェンスを使用してCVSS-BTEスコアを下げることにより、「合理的な最悪のケース」の基本スコアを調整し、多くのCVSS(基本)スコアが高すぎるという懸念に対処します。

; CVSS-BE: CVSS Base Score + 環境スコア(Environmental Score)

新しいメトリックグループ: Supplemental Metrics Group

Supplimental Metrics Group(補足メトリック)は、脆弱性の追加の外部属性を記述/測定する新しいメトリクスを定義する機能を提供します。

情報利用者は、これらのSupplemental Metricsの値を使用して、そのメトリックスと値に局所的な重要度を適用して、選択した場合に追加のアクションを取ることができます。

最終的に計算されるCVSSスコア(CVSS-BTEなど)への数値的影響を定義する指標はありません。計算後に、組織は各指標の重要性および/または効果的な影響、または指標のセット/組み合わせを割り当てて、最終的なリスク分析に与える影響を大きくしたり、小さくしたり、あるいは全く与えなかったりすることができます。メトリクスと値は、単に、脆弱性自体の追加の外部特性を伝えるだけです。

注: 情報プロバイダーによって提供されるすべての補足メトリックはオプションです。

OTへの新たな焦点: 安全性の指標と値

今日の多くの脆弱性は、論理的影響という従来のC/I/Aの三要素以外の影響を持ちます。ますます一般的になっているのは、論理的影響が脆弱なシステムや影響を受けたシステムで認識されるかどうかは別として、脆弱性を悪用した結果、人間に具体的な危害が及ぶ可能性があるという懸念です。

IoT、ICS、ヘルスケア分野は特に、増大する懸念に合わせて問題の優先順位付けを推進するために、CVSS仕様の一部としてこの種の影響を特定できることを非常に重視しています。

OT: 消費者が提供する環境安全性

システムの使用目的や目的への適合性は直接的に安全性と一致していないが、システムの展開方法や場所によっては安全性に影響を与える可能性がある場合、そのシステム内の脆弱性が悪用されると安全性に影響を及ぼす可能性があります。これは、環境メトリクスグループで表すことができます。

安全性(Safety)メトリック値は、脆弱性が悪用された結果として予想通り負傷する可能性のある人間の行為者または参加者の安全性に関する影響を測定します。他の影響メトリック値とは異なり、安全性は後続システム影響セット(Subsequent System(s))にのみ関連付けることができ、可用性および完全性メトリックのN/L/H影響値に加えて考慮する必要があります。

OT: 消費者が提供する環境安全性(続き)

後続システムの変更された整合性: 安全性(MSI:S)

- 悪用に成功すると、脆弱なシステムの完全性が損なわれ（薬物注入ポンプの投与量の変更など）、その結果、人間の健康と安全に影響（傷害）が生じます。

後続システムの可用性の変更: 安全性(MSA: S)

- 悪用に成功すると、脆弱なシステムの可用性が損なわれ（車のブレーキ システムが使用できなくなるなど）、その結果、人間の健康と安全に影響（傷害）が生じます。

OT: プロバイダが提供する補足的な安全性(Supplimental Safety)

システムが安全性を考慮した使用目的または目的適合性を備えている場合、そのシステム内の脆弱性の悪用により安全性への影響が生じる可能性があり、これを補足メトリクス グループで表すことができます。

安全性補足指標(Safety Supplimental Metric)に使用できる値は次のとおりです。

与える(?) (P: Present)	脆弱性の影響は、IEC 61508 の影響カテゴリの「限界的」、「重大」、または「壊滅的」の定義を満たしています。
無視できる (N: Negligible)	脆弱性の影響は、IEC 61508の影響カテゴリ「無視できる」の定義を満たしています。
未定義 (X: Not Defined)	このメトリックの値は、この脆弱性に対して定義されていません。

注: プロバイダーは補足メトリックを提供する必要はありません。これらは、プロバイダーがケースバイケースで伝達することを選択した内容のみに基づいて、必要に応じて提供できます。

The Supplemental Metrics

補足指標: 自動化可能(Automatable)

「自動化可能」メトリクスは、「攻撃者は複数のターゲットにわたってこの脆弱性の悪用を自動化できるか？」という問に対する答えを提供します。 キルチェーンのステップ1から4(偵察、武器化、配信、悪用)に基づいています。

No	攻撃者は、この脆弱性に対するキルチェーンのすべてのステップ (偵察、武器化、配信、悪用) を確実に自動化することはできません。	1. 脆弱なコンポーネントは検索または列挙できません。 2. 兵器化にはターゲットごとに人間の指示が必要です。 3. 配信では、ネットワーク セキュリティ構成がブロックするチャネルを使用します。 4. デフォルトで有効になっているエクスプロイト防止技術のため、エクスプロイトは信頼できません。
Yes	攻撃者は、キル チェーンのすべてのステップ (偵察、武器化、配信、悪用) を確実に自動化できます。	"Yes"の経験則の一つとして、脆弱性により認証されていないRemoteCode実行またはCommand Injectionが行われる場合、期待される応答は"Yes"です。 アナリストは、経験則のみに依存するのではなく、4つのステップすべてを自動化できるという議論や実証を提供する必要があります。

補足指標: 回復(Recovery)

このメトリクスは、攻撃が実行された後にパフォーマンスと可用性の観点からサービスを回復するための、コンポーネント/システムの回復力を表します。

自動 (A: Automatic)	コンポーネント/システムは攻撃後に自動的に回復します。
ユーザー (U: User)	コンポーネント/システムは、攻撃後にサービスを回復するためにユーザーによる手動介入を必要とします。
取り返しがつかない (I: Irrecoverable)	コンポーネント/システムは攻撃後、ユーザーが回復できなくなります。

補足指標: 値密度

値密度は、攻撃者が1回の悪用イベントで制御できるリソースを表します。 可能な値は、拡散と集中の2つです。

拡散 (Diffuse)	脆弱なコンポーネントを含むシステムのリソースは限られています。つまり、攻撃者が1回の悪用イベントで制御できるリソースは比較的小さいということです。
集中 (Concentrated)	脆弱なコンポーネントを含むシステムにはリソースが豊富にあります。経験則から考えると、このようなシステムは多くの場合、管理者ではなく「システムオペレータ」が直接責任を負います。

補足指標: 脆弱性対応の取り組み(Vulnerability Response Effort)

インフラストラクチャに展開されている製品およびサービスの脆弱性の影響に対して、消費者が初期対応を行うことがいかに難しいかについての補足情報を提供します。
消費者は、緩和策を適用したり修復をスケジュールしたりするときに、必要な労力に関するこの追加情報を考慮に入れることができます。

低 (L)	脆弱性に対応するために必要な労力は、少ない 若しくは 簡単です。
中 (M)	脆弱性に対応するために必要なアクションには、消費者に代わってある程度の労力が必要であり、実装するサービスへの影響は最小限に抑えられる可能性があります。
高 (H)	脆弱性に対応するために必要なアクションは重大かつ/または困難であり、スケジュールされたサービスへの影響が長引く可能性があります。あるいは、現場での脆弱性にリモートで対応することはできません。この脆弱性に対する唯一の解決策は、物理的な交換です。

補足指標: プロバイダーの緊急度(Provider Urgency)

プロバイダーが提供する追加的な評価を取り入れるための標準化された方法を促進するために、プロバイダー緊急度と呼ばれるオプションの「パススルー」補足メトリックが定義されています。

製品のサプライチェーンに沿ったプロバイダーは、次のような補足的な緊急度評価を提供する場合があります。

> 例えば：ライブラリ メンテナ → OS/ディストリビューション メンテナ → プロバイダ 1 ... プロバイダ n(PPP)→ コンシューマ

最後から2番目の製品プロバイダー (PPP) は、緊急度を直接評価するのに最適な立場にあります。

補足指標: プロバイダーの緊急度(Provider Urgency)(続き)

プロバイダー緊急度メトリック値:

赤(Red)	プロバイダーは、この脆弱性の影響が最も緊急性が高い(highest)と評価しました。
アンバー(Amber)	プロバイダーは、この脆弱性の影響を中程度の緊急性がある(moderate)と評価しました。
緑(Green)	プロバイダーは、この脆弱性の影響は緊急性が低い(reduced)と評価しています。
クリア(Clear)	プロバイダーは、この脆弱性の影響は緊急性が低い、または緊急性がない(low or no)と評価しています。(情報として)

数学への新しく斬新なアプローチ

（うまく訳せないから原文で…）

- Use metric groups to gather 15 million CVSS vectors into 271 equivalence sets
- Solicit expert opinion to compare vectors representing each equivalence set
- Calculate the order of vectors from least severe to most severe
- Determine boundaries between Qualitative Severity Ratings compatible with qualitative severity boundaries from CVSS v3.x.
- Compress the vector groups in each qualitative severity bin into the number of available scores in that bin(for example, 9.0 to 10.0 for critical, 7.0 to 8.9 for high, etc.)
- Leverage interpolation to adjust scores within a vector group to ensure changes in any metric value results in a score change.

さらに考慮すべき点

Technical Severity vs. Risk

CVSS基本スコア(CVSS-B)は「技術的重大度(Technical Severity)」を表します

- 脆弱性自体の属性のみを考慮します。
- 修復の優先順位を決定するために、これを単独で使用することはお勧めできません

「リスク」は宗教的な話題になることが多いですが…

- CVSS-BTE スコアでは、次の属性が考慮されます。
- 基本スコア
- 脆弱性に関連する脅威
- 環境制御 / 重要度

適切に使用されれば、CVSS-BTEスコアは、独自の「リスク」評価を生成するときに、多くの評価の高い第三者のセキュリティ組織が考慮した以上に、包括的な属性を表します。

CVSS and EPSS and SSVC

最近、脆弱性評価とパッチの優先順位の補完的な側面を処理するために、追加のスコアリングシステムが導入および採用されました。これらは脆弱性スコアリングツールボックスへの歓迎すべき追加であり、革新的なエクスプロイトの予測と意思決定のサポートを提供します。

- EPSS: エクスプロイト予測スコアリングシステム(The Exploit Prediction Scoring System)
  - ソフトウェアの脆弱性が30日以内に実際に悪用される可能性(確率)を推定するための、データ主導の取り組み。
  - https://first.org/epss
- SSVC: 利害関係者固有の脆弱性の分類(Stakeholder-Specific Vulnerability Categorization)
  - 脆弱性管理中に、アクションに優先順位を付けるための決定木システム。
  - https://cisa.gov/ssvc

CVSS の使用を成功させるためのベストプラクティス

データベースとデータフィードを使用して、脆弱性データの強化を自動化します。

- NVD(ベースメトリック値)
- 資産管理データベース（環境指標値）
- 脅威インテリジェンスデータ(脅威メトリック値)

重要な属性に基づいて脆弱性データを表示する方法を見つける

- 解決を担当するサポートチーム
- 重要なアプリケーション
- 内部向きと外部向き
- ビジネスユニット
- 規制要件

Links to Docs, Specs, and Training

脆弱性
対応
勉強会

- CVSS SIG: https://first.org/cvss
- CVSS Online Training Course: https://www.first.org/cvss/training
- CVSS v4.0 Public Preview: https://www.first.org/cvss/v4-0
- CVSS v4.0 Specification: https://www.first.org/cvss/v4-0/specification-document
- CVSS v4.0 User Guide: https://www.first.org/cvss/v4-0/user-guide
- CVSS v4.0 Calculator: https://www.first.org/cvss/calculator/v4-0