公表マニュアル 付録 1

共通脆弱性評価システム CVSS v3 について
～脆弱性の深刻度を評価するための指標～

2020 年 3 月

独立行政法人情報処理推進機構
セキュリティセンター

1 はじめに

共通脆弱性評価システム CVSS(Common Vulnerability Scoring System)は、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指し、米国家インフラストラクチャ諮問委員会(NIAC: National Infrastructure Advisory Council)のプロジェクトで 2004 年 10 月に原案が作成されました。

その後、CVSS の管理母体として FIRST(Forum of Incident Response and Security Teams)が選ばれ、FIRST の CVSS-SIG(Special Interest Group)[1] で適用推進や仕様改善が行われており、2005 年 6 月に CVSS v1 が、2007 年 6 月に CVSS v2 が公開されました。CVSS v3[2] は、仮想化やサンドボックス化などが進んできていることから、利用状況の変化を取り込んだ仕様とすべく、2015 年 6 月にリリースされました。

IPA は、CVSS-SIG に参画しており、これまで JVN 脆弱性対策機械処理基盤の整備の一環として、脆弱性対策情報ポータルサイト JVN[3]、脆弱性対策情報データベース JVN iPedia[4]や脆弱性関連情報の調査結果のウェブサイトでの CVSS v3 基本値の公表、CVSS 計算ソフトウェアの多国語版として、CVSS v3 版[5]を提供してきました 。

本資料は、IPA のウェブサイト『共通脆弱性評価システム CVSS v3 概説[6]』の記載から「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」に関連する CVSSv3 の基本評価基準(Base Metrics)の説明箇所を抜粋したものです。

2 概要

2.1 CVSS とは

CVSS は、情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダーに依存しない共通の評価方法を提供しています。CVSSv3 の基本評価基準(Base Metrics)を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになります。また、ベンダー、セキュリティ専門家、管理者、ユーザ等の間で、脆弱性に関して共通の言葉で議論できるようになります。

・基本評価基準(Base Metrics)
脆弱性そのものの特性を評価する基準です。情報システムに求められる 3 つのセキュリティ特性、『機密性(Confidentiality Impact)』、『完全性(Integrity Impact)』、『可用性(Availability Impact)』に対する影響を、ネットワークから攻撃可能かどうかといった基準で評価し、CVSS 基本値(Base Score)を算出します。この基準による評価結果は固定していて、時間の経過や利用環境の異なりによって変化しません。ベンダーや脆弱性を公表する組織などが、脆弱性の固有の深刻度を表すために評価する基準です。
詳細は、『共通脆弱性評価システム CVSS v3 概説』を参照下さい。

---

1 Common Vulnerability Scoring System (CVSS-SIG)
http://www.first.org/cvss
2 Common Vulnerability Scoring System version 3.0
https://www.first.org/cvss/v3-0/
3 JVN: Japan Vulnerability Notes
http://jvn.jp/
4 JVN iPedia
http://jvndb.jvn.jp/
5 CVSS v3 計算ソフトウェア多国語版
http://jvndb.jvn.jp/cvss/v3/
6 共通脆弱性評価システム CVSS v3 概説
https://www.ipa.go.jp/security/vuln/CVSSv3.html

3 脆弱性評価項目

3.1 基本評価基準(Base Metrics)

3.1.1. 攻撃元区分(AV：Attack Vector)

脆弱性のあるコンポーネントをどこから攻撃可能であるかを評価します。

v3	内容
ネットワーク(N)	対象コンポーネントをネットワーク経由でリモートから攻撃可能である。 例えば、インターネットからの攻撃など
隣接(A)	対象コンポーネントを隣接ネットワークから攻撃する必要がある。 例えば、ローカル IP サブネット、ブルートゥース、IEEE 802.11 など
ローカル(L)	対象コンポーネントをローカル環境から攻撃する必要がある。 例えば、ローカルアクセス権限での攻撃が必要、ワープロのアプリケーションに不正なファイルを読み込ませる攻撃が必要など
物理(P)	対象コンポーネントを物理アクセス環境から攻撃する必要がある。 例えば、IEEE 1394、USB 経由で攻撃が必要など

3.1.2. 攻撃条件の複雑さ(AC：Attack Complexity)

脆弱性のあるコンポーネントを攻撃する際に必要な条件の複雑さを評価します。

v3	内容
低(L)	特別な攻撃条件を必要とせず、対象コンポーネントを常に攻撃可能である。
高(H)	攻撃者以外に依存する攻撃条件が存在する。例えば、次のいずれかの条件に合致する場合などが該当する。 攻撃者は、設定情報、シーケンス番号、共有鍵など、攻撃対象の情報収集が事前に必要となる。 攻撃者は、競合が発生する条件、ヒープスプレイを成功させるための条件など、攻撃を成功させるための環境条件を明らかにする必要がある。 攻撃者は、中間者攻撃のため環境が必要となる。

3.1.3. 必要な特権レベル(PR：Privileges Required)

脆弱性のあるコンポーネントを攻撃する際に必要な特権のレベルを評価します。

v3	内容
不要(N)	特別な権限を有する必要はない。
低(L)	コンポーネントに対する基本的な権限を有していれば良い。 例えば、秘密情報以外にアクセスできるなど
高(H)	コンポーネントに対する管理者権限相当を有する必要がある。 例えば、秘密情報にアクセスできるなど

3.1.4. ユーザ関与レベル(UI：User Interaction)

脆弱性のあるコンポーネントを攻撃する際に必要なユーザ関与レベルを評価します。

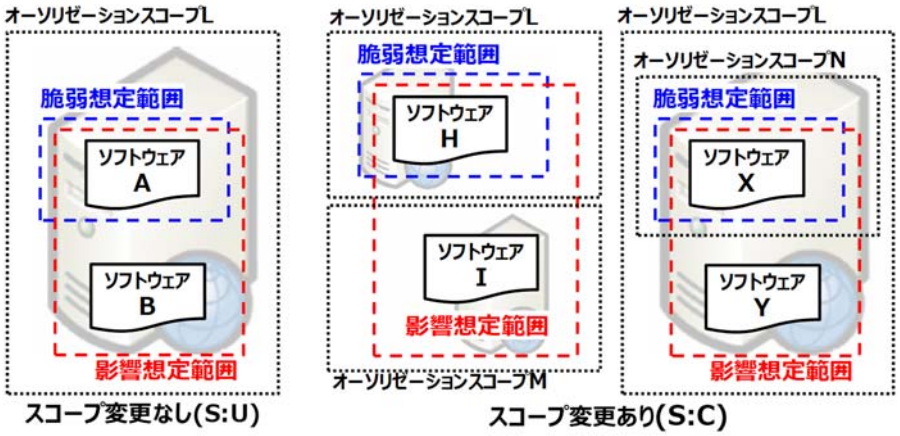
v3	内容
不要(N)	ユーザが何もしなくても脆弱性が攻撃される可能性がある。
要(R)	リンクのクリック、ファイル閲覧、設定の変更など、ユーザ動作が必要である。

3.1.5.スコープ(S：Scope)

脆弱性のあるコンポーネントへの攻撃による影響範囲を評価します。

v3	内容
変更なし(U)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープに留まる。
変更あり(C)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープ以外にも広がる可能性がある。 例えば、クロスサイトスクリプティング、リフレクター攻撃に悪用される可能性のある脆弱性など

注)スコープを評価する際には、計算機資源に対する管理権限の範囲(オーソリゼーションスコープ；Authorization Scope)という概念を考慮する必要があります。例えば、脆弱性のあるコンポーネント(ソフトウェア A)を攻撃し、その影響が他のコンポーネント(ソフトウェア B)に及んだとしても、同じオーソリゼーションスコープ内にあれば、「スコープ変更なし」となります。一方、脆弱性のあるコンポーネント(ソフトウェア H や X)を攻撃した結果、他のオーソリゼーションスコープにある他のコンポーネント(ソフトウェア I や Y)に及んだ場合には、同じホスト内であっても「スコープ変更あり」となります。



3.1.6.機密性への影響(情報漏えいの可能性、C：Confidentiality Impact)

脆弱性を攻撃された際に受ける重要な情報への影響の有無を評価します。

v3	内容
高(H)	機密情報や重要なシステムファイルが参照可能であり、その問題による影響が全体に及ぶ。
低(L)	情報漏えいやアクセス制限の回避などが発生はするが、その問題による影響が限定的である。
なし(N)	機密性への影響はない

3.1.7.完全性への影響(情報改ざんの可能性、I：Integrity Impact)

脆弱性を攻撃された際に受ける重要な情報への影響の有無を評価します。

v3	内容
高(H)	機密情報や重要なシステムファイルの改ざんが可能で、その問題による影響が全体に及ぶ。
低(L)	情報の改ざんが可能ではあるが、機密情報や重要なシステムファイルの改ざんはできないために、その問題による影響が限定的である。
なし(N)	完全性への影響はない

3.1.8.可用性への影響(業務停止の可能性、A：Availability Impact)

脆弱性を攻撃された際に、対象とする影響想定範囲の業務が遅延・停止する可能性を評価します。

v3	内容
高(H)	リソース(ネットワーク帯域、プロセッサ処理、ディスクスペースなど)を完全に枯渇させたり、完全に停止させることが可能である。
低(L)	リソースを一時的に枯渇させたり、業務の遅延や一時中断が可能である。
なし(N)	可用性への影響はない

4 値の算出方法

CVSS では、脆弱性の技術的な特性を評価する基準(基本評価基準：Base Metrics)を評価することで、脆弱性の深刻度を 0(低)～10.0(高)の数値で表します。

・深刻度レベル分け
CVSS v3 では、深刻度レベル分けを次のように設定しています。

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

4.1 基本評価基準(Base Metrics)

(1)影響度
調整前影響度 = 1 - (1 - C)×(1 - I)×(1 - A) …式(1)
影響度(スコープ変更なし)= 6.42×調整前影響度 …式(2)
影響度(スコープ変更あり)= 7.52×(調整前影響度 - 0.029) - 3.25×(調整前影響度 - 0.02)^{15} …式(3)

(2)攻撃容易性
攻撃容易性 = 8.22×AV×AC×PR×UI …式(4)

(3)基本値
影響度がゼロ以下の場合
基本値 = 0 …式(5)

影響度がゼロよりも大きい場合
スコープ変更なし
基本値 = RoundUp1(min [(影響度＋攻撃容易性), 10]) …式(6)
(小数点第 1 位切り上げ)

スコープ変更あり
基本値 = RoundUp1(min [(1.08×(影響度＋攻撃容易性)), 10]) …式(7)
(小数点第 1 位切り上げ)

評価項目	評価結果	値	スコープ 変更あり
攻撃元区分(AV)	ネットワーク(N)	0.85	
	隣接(A)	0.62	
	ローカル(L)	0.55	
	物理(P)	0.20	
攻撃条件の複雑さ(AC)	低(L)	0.77	
	高(H)	0.44	
必要な特権レベル(PR)	不要(N)	0.85	
	低(L)	0.62	0.68
	高(H)	0.27	0.50
ユーザ関与レベル(UI)	不要(N)	0.85	
	要(R)	0.62	
スコープ(S)	変更なし(U)	－	
	変更あり(C)	－	
機密性への影響(C)	高(H)	0.56	
	低(L)	0.22	
	なし(N)	0	
完全性への影響(I)	高(H)	0.56	
	低(L)	0.22	
	なし(N)	0	
可用性への影響(A)	高(H)	0.56	
	低(L)	0.22	
	なし(N)	0	

5　パラメーターの短縮表記

CVSS v3 では、先頭にバージョン 3 であることを示すプレフィックス CVSS:3.0 の後に、パラメーターの短縮表記として、各評価の項目とその選択肢を記載します。例えば攻撃元区分の項目名は AV、選択肢はローカル：L、隣接ネットワーク：A、ネットワーク：N、物理：P です。(CVSS:3.0/AV:N/AC:L/ PR:N/S:U/C:L/I:L/A:L)は、『CVSS バージョン 3.0 で、攻撃元区分：ネットワーク、攻撃条件の複雑さ：低、特権レベル：不要、スコープ：変更なし、機密性/完全性/可用性への影響：低』を意味します。