

## 脆弱性の深刻度評価の新バージョン CVSS v2 への移行について CVSS (Common Vulnerability Scoring System、共通脆弱性評価システム)

独立行政法人 情報処理推進機構(東京都文京区、理事長:藤原 武平太、略称:IPA)は、ソフトウェア製品の脆弱性(ソフトウェア等におけるセキュリティ上の弱点)の深刻度評価に採用している共通脆弱性評価システム CVSS (Common Vulnerability Scoring System)を、新バージョンの CVSS v2 へ移行しました。

IPA は、ソフトウェア製品の脆弱性の深刻度評価を、FIRST<sup>i</sup> が推進している、共通脆弱性評価システム CVSS を採用しています。

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、特定のベンダーに依存しない共通の評価方法として、脆弱性の深刻さを、製品利用者や SI 事業者、製品開発者などが、同一の基準の下で定量的に比較できるものです。

IPA では、脆弱性関連情報の届出受付において、届出られた脆弱性を CVSS を適用して深刻度評価を行っており、脆弱性対策情報の公表ページ<sup>ii</sup> でその評価結果を公表しています。また、2007年4月から公開している脆弱性対策情報データベース JVN iPedia<sup>iii</sup> でも CVSS による評価結果を公表しています。

この度、CVSS v2 の公開を受けて、脆弱性対策情報の公表ページ、および、JVN iPedia での深刻度評価を CVSS v2 へ移行しました。

### CVSS v2 の改善点

#### 脆弱性の深刻度の分布が、レベル II を中心に分散した形になりました

2005年6月に公開された CVSS v1 を各組織が実際の脆弱性へ適用し2年間運用してみると、脆弱性そのものの特性を評価する CVSS 基本値(0.0 から 10.0 の範囲に算出される)が特定の値に集中してしまう、また、低めの値を中心に分散してしまう等の課題が報告されていました。

そこで、CVSS v2 では、CVSS 基本評価基準の全ての組み合わせから算出される CVSS 基本値の出現頻度が、CVSS 基本値の中央を中心に分散するように、各評価項目の値や算出式が改善されました。

図1は、2007年8月20日までに脆弱性対策情報ポータルサイト JVN<sup>iv</sup> で脆弱性対策情報を公表した 201 件について、CVSS v1 と CVSS v2 で評価した脆弱性の深刻度分布です。

実際の脆弱性の深刻度分布も、深刻度の評価結果がレベル II を中心に分散した形となり、CVSS 利用者が脆弱性への対応の緊急度を、より迅速に意思決定しやすくなりました。

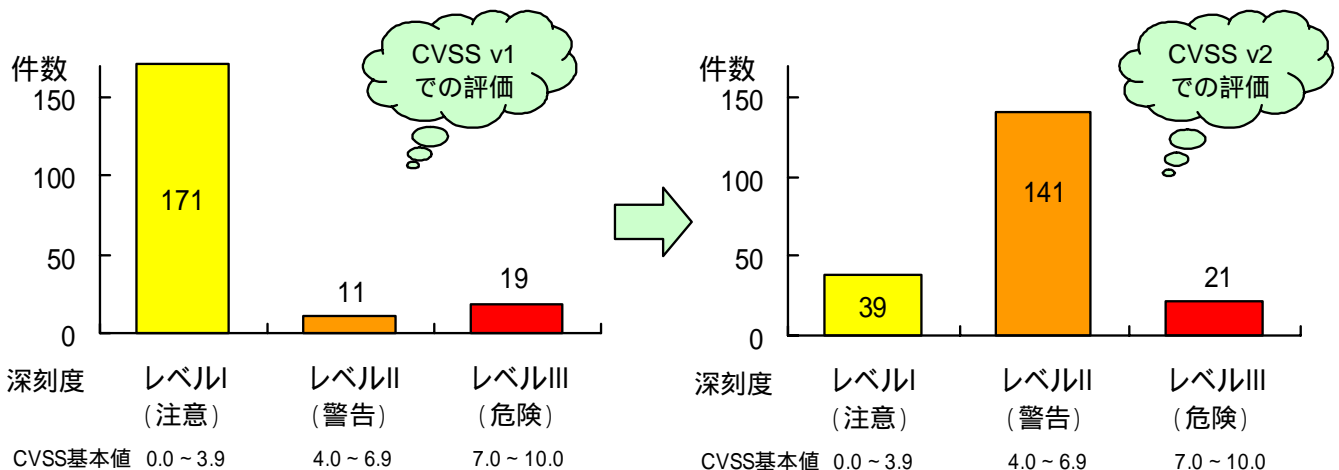


図1. JVNで公表した脆弱性の深刻度分布

## CVSS 基本値による深刻度のレベル分けについて

CVSS 基本値を基に、次の深刻度に分けて表示しています。

深刻度	CVSS 基本値	脆弱性に対して想定される脅威
レベル III (危険)	7.0 ~ 10.0	・リモートからシステムを完全に制御されるような脅威 ・大部分の情報が漏えいするような脅威 ・大部分の情報が改ざんされるような脅威 ・例えば、全てのシステムが停止するようなサービス運用妨害(DoS)、OS コマンド・インジェクション、SQL インジェクション、バッファオーバーフローによる任意の命令実行など
レベル II (警告)	4.0 ~ 6.9	・一部の情報が漏えいするような脅威 ・一部の情報が改ざんされるような脅威 ・サービス停止に繋がるような脅威 ・例えば、クロスサイト・スクリプティング、一部の情報が漏えいするようなディレクトリ・トラバーサル、一部のシステムが停止するようなサービス運用妨害(DoS)など ・その他、レベル III に該当するが再現性が低いもの
レベル I (注意)	0.0 ~ 3.9	・攻撃するために複雑な条件を必要とする脅威 ・その他、レベル II に該当するが再現性が低いもの

注) CVSS 基本値は、脆弱性そのものの特性を同一の基準の下で数値化したものです。各組織の脆弱性への対応は、CVSS 基本値に加え、CVSS 現状値(攻撃コードの出現有無、対策情報の適用可否など)や CVSS 環境値(各組織での対象製品の利用範囲、攻撃を受けた場合の被害の大きさなど)を加味して、製品利用者自身が総合的な評価を行う必要があります。

(参考)

(1) 共通脆弱性評価システム CVSS の新バージョンの公開について

[http://www.ipa.go.jp/security/vuln/200706\\_CVSSv2.html](http://www.ipa.go.jp/security/vuln/200706_CVSSv2.html)

(2) 共通脆弱性評価システム CVSS v2 概説

<http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html>

<sup>i</sup> Forum of Incident Response and Security Teams. コンピュータセキュリティインシデント対応チームフォーラム。コンピュータセキュリティに関するインシデント(事故)への対応・調整・サポートをする CSIRT(Computer Security Incident Response Team)の連合体。 <http://www.first.org/>

<sup>ii</sup> <http://www.ipa.go.jp/security/vuln/documents/index.html>

<sup>iii</sup> 日本向けの脆弱性対策情報データベースを目指し、JVN で公表した約 450 件に加え、米国 NIST(National Institute of Standard and Technology: 米国国立標準技術研究所)が運営する NVD(National Vulnerability Database: 国立脆弱性データベース)から情報を収集・翻訳し、4月25日に公開を開始しました。公開開始以降、毎月 100 件程度の情報を新規に登録し、現在、3,986 件の累計登録件数となっています。各脆弱性の概要、CVSS による深刻度、影響を受けるシステム、想定される影響、対策、ベンダ情報などが判りやすく参照できます。また、キーワード、製品別、ID、日付、CVSS による深刻度などから目的の脆弱性対策情報を容易に検索することができます。 <http://jvndb.jvn.jp/>

<sup>iv</sup> Japan Vulnerability Notes. 脆弱性対策情報ポータルサイト。国内製品開発者の脆弱性への対応状況を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。 <http://jvn.jp/>

本件に関するお問い合わせ先  
独立行政法人 情報処理推進機構 セキュリティセンター  
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: [vuln-inq@ipa.go.jp](mailto:vuln-inq@ipa.go.jp)  
報道関係からのお問い合わせ先  
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山 / 佐々木  
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: [pr-inq@ipa.go.jp](mailto:pr-inq@ipa.go.jp)