SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

共通脆弱性評価システム CVSS の現状と今後

The current situation and futures of CVSS

永安 佑希允* Yukinobu NAGAYASU
谷口 隼祐* Shunsuke TANIGUCHI
相馬 基邦* Motokuni SOUMA
寺田 真敏* Masato TERADA
山岸 正* Tadashi YAMAGISHI
小林 偉昭* Hideaki KOBAYASHI

あらまし 日々大量に報告される脆弱性関連情報にシステム管理者が対応するためには，優先順位をつけるための指標が必要である．CVSS は，特定のベンダによらない，開かれた脆弱性評価指標であり，国内外の組織で採用が進んでいる．本稿では，情報セキュリティ早期警戒パートナーシップに基づき報告された脆弱性関連情報を，IPA が CVSS を用いて評価した結果について現状を報告し，今後解決すべき課題と展望について述べる．

キーワード セキュリティ評価・監査，JVN，脆弱性，CVSS，脆弱性評価

1 はじめに

IPA （Information-technology Promotion Agency, Japan）は，平成 16 年に経済産業省が公示した「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）に基づき，情報セキュリティ早期警戒パートナーシップとして，脆弱性関連情報の届出を受け付け分析しており，報告された脆弱性関連情報を，JVN（Japan Vulnerability Notes）で公開している[1].

IPA は平成 19 年 2 月から，JVN で公開している脆弱性関連情報に対して，CVSS（Common Vulnerability Scoring System）[2] 基本評価基準による脆弱性深刻度評価の試行を開始しており，同年 12 月現在で 240 件以上の脆弱性関連情報について CVSS 評価を公表している．さらに同年 4 月から公開している JVN iPedia [3]では，NVD が評価した CVSS 評価を取り込む形で，国内で使用されているソフトウェアの脆弱性の CVSS 評価を公表しており，12 月現在で 4,300 件以上の脆弱性関連情報を取り扱っている．また 8 月には，CVSS が v2.0 に更新されたことに伴い，CVSS v1.0 で評価済であった脆弱性関連情報も含めて再評価を行った.

本稿では，これらの取組みを通じて得られた知見や，明らかになった課題を基に現状を考察し，より正確な脆弱性深刻度評価に向けた提案を行う．

* 独立行政法人情報処理推進機構, 東京都文京区本駒込二丁目 28 番 8 号 文京グリーンコートセンターオフィス 16 階,
Information-technology Promotion Agency, Japan,
2-28-8, Hon-Komagome, Bunkyo-ku, Tokyo

2 脆弱性深刻度指標の現状

2.1 脆弱性報告件数

システム管理者は日々，多くの脆弱性情報を取り扱う必要がある．CERT/CC が報告した 2006 年の脆弱性は 8,064 件となっており[4]，一日あたり 22 件程度の脆弱性情報が新たに報告されている．また，NIST（National Institute of Standards and Technology）が運営する NVD（National Vulnerability Database）でも 6,602 件となっており[5]，こちらを基に算出すると 18 件程度となる.

このような状況からも，脆弱性の影響度合いに応じて，優先度を変えて対策するための指標が求められている.

2.2 深刻度の指標

2007 年に入ってから, 国内でも脆弱性の影響度を指標化する試みが行なわれ始めている．本節では，国内での脆弱性の影響に関する指標化の活動について述べる.

2.2.1. JPCERT/CC

JPCERT/CC では，攻撃経路，認証レベル，攻撃成立に必要なユーザの関与，攻撃の難易度の視点から分析した結果を JVN で公表している（図 1）. この分析結果は，実際に脆弱性への対策を行う立場にある人が，脆弱性の脅威を判断するための判断材料となる項目となっている.


JPCERT/CCによる脆弱性分析結果
2007.12.04における脆弱性分析結果

攻撃経路	物理アクセス	ローカルマシン	同一セグメント	インターネット経由
認証レベル	特権レベル	標準レベル	低レベル	なし
攻撃成立に必要なユーザの関与	積極的	–	消極的	関与させる必要なし
攻撃の難易度	高	中－高	低－中	低

図 1: JPCERT/CC による脆弱性分析結果例

2.2.2. JNSA

JNSA (NPO 日本ネットワークセキュリティ協会) は，脆弱性の定量化にあたり，脆弱性の定義，攻撃に至るまでの経緯等を要素に分解してモデル化し，最終的にトリアージ値として定式化を提案している[6]．この提案によれば，トリアージ値は包括的な処置の優先度を表す指標を目指したものとなっている．

また，トリアージ値とシステム管理者が感じる危険度の関係を，アンケートを通じて定量的に評価しており，これらの間には相関があることを報告している．検討の中では CVSS を含む他の評価手法との組み合わせが意識されており，CVSS の Base Metrics をトリアージ値算出上の入力とすることも提案している．

2.2.3. アンチウイルスベンダの指標

アンチウイルスベンダは，各不正プログラムに対して影響の度合いを公表している場合がある．たとえばトレンドマイクロ社は，「危険度」という指標を各不正プログラムに対して公表している．これは不正プログラムの活動内容と流行の度合いを総合して表している．

不正プログラムに対する指標は，脆弱性に対する指標とは対象が異なり，同列に比較することはできない．しかし，不正プログラムの中には脆弱性を悪用するものも多いため，ある脆弱性を悪用する不正プログラムの有無や流行の度合いは，CVSS の Temporal Metrics を採点する上での参考にすることは可能と考える．

3 CVSS

本章では，IPA で推進している脆弱性深刻度評価手法である CVSS の概要について述べる．

3.1 利用状況

CVSS 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たものである．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）で適用推進や仕様改善が行われている．2005 年 6 月に CVSS v1.0 が，2007 年 6 月に CVSS v2.0 が公開された．CVSS は，現在，30 を超える組織で採用されている．

利用事例としては，NVD では，28 万件以上の CVE 脆弱性情報について，CVSS v2.0 による評価を公開している．また，Payment Card Industry (PCI) Data Security Standard[7]においても，脆弱性評価指標として採用されるなど普及しつつある．

3.2 評価方法

CVSS は，脆弱性の性質を Base Metrics，Temporal Metrics，Environmental Metrics という 3 つの異なる観点から評価を行うことにより，包括的な指針として利用できる数値を出力する仕組みである．計算結果は，小数点以下第二位を四捨五入し，第一位まで表記する．10.0 が深刻度の最も高い値となり，0.0 が最も低い値となる．最低限 Base Metrics を評価する必要があり，Temporal Metrics および Environmental Metrics の評価は必須ではない．

3.2.1. Base Metrics（基本評価基準）

Base Metrics（基本評価基準）は，時間の経過やソフトウェアの利用環境に依存しない，脆弱性そのものの特性を評価するものである．6 つの評価項目からなり，そのうち攻撃の前提に関するものが 3 つ，被害に関するものが 3 つある（表 1）．

攻撃の前提に関する評価項目は，Access Vector（攻撃元区分），Access Complexity（攻撃条件の複雑さ），Authentication（攻撃前の認証要否）の 3 つがある．また，被害に関するものは，情報システムに求められる 3 つのセキュリティ特性に対する影響の度合いを，Confidentiality Impact（機密性への影響），Integrity Impact（完全性への影響），Availability Impact（可用性への影響）として評価する．

Base Metrics を評価するのは，ソフトウェアベンダやセキュリティベンダなど，脆弱性に関する詳細な情報を把握する立場にある者が適切である．

表 1: Base Metrics における評価項目

評価項目	選択肢
Access Vector	Local / Adjacent Network / Network
Access Complexity	Low / Medium / High
Authentication	None / Single / Multiple
Confidentiality Impact	None / Partial / Complete
Integrity Impact	None / Partial / Complete
Availability Impact	None / Partial / Complete

なお IPA では，Base Metrics の評価値に基づき，脆弱性に対して想定される脅威別に，深刻度としてレベル分けを行っている（表 2）．

表 2: IPA による深刻度のレベル分け

CVSS Base Metrics 評価値	深刻度
7.0 ～ 10.0	レベル III（危険）
4.0 ～ 6.8	レベル II（警告）
0.0 ～ 3.9	レベル I（注意）

3.2.2. Temporal Metrics（現状評価基準）

Temporal Metrics（現状評価基準）は，脆弱性を取り巻く時間的な状況を評価する．一般に脆弱性が発見された後は，攻撃者の側においては実証コードやウイルス等の開発が進み，ベンダの側においては回避策やパッチの充実といった形で，状況が変化する．このような状況の変化を，Exploitability（攻撃される可能性），Remediation Level（利用可能な対策のレベル），Report Confidence（脆弱性情報の信頼性）の，3 つの項目で評価する（表 3）．

Temporal Metrics は，公開された情報に基づいて評価するため，誰でも評価することができる．しかし，状況の変化を常に追いかけて更新する必要があり，継続的な状況把握が必要となる．

表 3: Temporal Metrics における評価項目

評価項目	選択肢
Exploitability	Unproven / Proof-of-Concept / Functional / High / Not Defined
Remediation Level	Unconfirmed / Uncorroborated / Confirmed / Not Defined
Report Confidence	None / Low / Low-Medium / Medium-High / High / Not Defined

3.2.3. Environmental Metrics（環境評価基準）

Environmental Metrics（環境評価基準）は，そのソフトウェアを利用者側でどのように使っているかを評価するものであり，Collateral Damage Potential（二次的被害の可能性），Target Distribution（影響を受ける対象システムの範囲），Confidentiality Requirement（機密性の要求度），Integrity Requirement（完全性の要求度），Availability Requirement（可用性の要求度）を評価する（表 4）．

Environmental Metrics を評価するのは，ソフトウェアの利用者であり，いずれの評価項目も，詳細な評価方針は利用者が決定することとなる．

表 4: Environmental Metrics における評価項目

評価項目	選択肢
Collateral Damage Potential	None / Low / Low-Medium / Medium-High / High / Not Defined
Target Distribution	None / Low / Medium / High / Not Defined
Confidentiality Requirement	Low / Medium / High / Not Defined
Integrity Requirement	Low / Medium / High / Not Defined
Availability Requirement	Low / Medium / High / Not Defined

4 CVSS 評価の事例と留意点

本章では，CVSS 評価の事例に基づき，実際に評価するにあたっての留意点を示す．

4.1 IPA における評価体制

IPA では数名の合議により Base Metrics の評価を決定している．なお，評価に先立ち，FIRST のドキュメント「A Complete Guide to the Common Vulnerability Scoring System Version 2.0」の内容をベースとし，2 週間程度の練習期間を通して，レベルの均一化を図った．

4.2 評価事例

4.2.1. OS コマンドインジェクションの事例

IPA による CVSS 評価事例として，「『Webmin』における OS コマンドインジェクションの脆弱性」（JVN#61208749）を取り上げる（表 5）．Webmin には，Webmin の管理者ユーザが OS の管理者権限で OS コマンドを実行する機能がある．本脆弱性により Webmin の一般ユーザも OS の管理者権限で任意の OS コマンドを実行することができるようになる．

本事例の場合，アプリケーション実行権限の想定が評価ポイントとして重要である．具体的には，Confidentiality Impact，Integrity Impact，Availability Impact の評価がそれぞれ Partial か，それとも Complete かを判断するには，ソフトウェアがどのような権限下で稼働しているかが問題となる．脆弱性を攻略された場合，当該ソフトウェアが管理者権限で稼働している場合には評価が Complete となる可能性が大きく，一般ユーザ権限で稼働している場合は最大でも Partial となる．

ウェブアプリケーションの Remote Code Execution 脆弱性の場合，多くのウェブアプリケーションは一般ユーザ権限で稼働するため，評価は最大でも Partial となることが多い．しかし，同じウェブアプリケーションでも本事例のような，OS の管理者権限での動作を前提と

するものでは，Complete となる可能性がある．

表 5: JVN#61208749 の CVSS 評価

評価項目	評価 / 理由
Access Vector	Network / 攻撃者はウェブブラウザを使ってネットワーク経由の攻撃が可能.
Access Complexity	Low / 能動的攻撃であり，認証を除けば特に前提条件はない．認証については本評価項目では評価の対象としない.
Authentication	Single / 攻撃にあたっては，Webmin の一般ユーザとしてログインする必要がある.
Confidentiality Impact	Complete / OS の管理者権限で任意のコマンドを実行されるため，ホスト上の全情報が漏洩する可能性.
Integrity Impact	Complete / OS の管理者権限で任意のコマンドを実行されるため，ホスト上の全情報が破壊される可能性.
Availability Impact	Complete / OS の管理者権限で任意のコマンドを実行されるため，ホストそのものを停止される可能性.

CVSS が規定する計算式に当てはめると，評価値は 9.0 となり，IPA による深刻度はレベル III（危険）となる（表 5）．レベル III（危険）の脅威は，「リモートからシステムを完全に制御されるような脅威」等と想定されており，これは本脆弱性によって実際に生じうる脅威と合致する．

4.2.2. CSRF の事例

ウェブアプリケーションにおける CSRF（Cross-Site Request Forgeries）は，アプリケーションが処理する情報の内容によって脅威が変わるため，同じ CSRF の問題であっても，CVSS 評価が大幅に変わり得る．

「『AirStation』シリーズおよび『BroadStation』シリーズにおけるクロスサイト・リクエスト・フォージェリの脆弱性」（JVN#71872818）は，ルータの設定が意図せず変更させられてしまう問題である（表 6）．評価にあたっては，対象製品の詳しい機能を勘案する必要がある．

また，本事例のような，受動的攻撃を前提とした脆弱性においては，Access Complexity が評価ポイントとして重要となる．Access Complexity を判断するにあたっては，CVSS v2.0 ドキュメント中の下記記述が主な拠所となる．

> ***Access Complexity: Middle***
>
> *The attack requires a small amount of social engineering that might occasionally fool cautious users (e.g., phishing attacks that modify a web browser's status bar to show a false link, having to be on someone's "buddy" list before sending an IM exploit).*
>
> ***（訳）攻撃条件の複雑さ：中***
>
> *攻撃にあたり，用心深い利用者を時折だませる程度のソーシャルエンジニアリングを必要とする場合（例えば，ウェブブラウザのステータスバー改変を含むフィッシングや，友達リストからの IM Exploit など）.*

「cautious users（用心深い利用者）」像は，評価相違の要因となる．用心深い利用者はどのような行動をとるかは，評価者の経験に依存する部分であり，従って主観が入りやすい部分である．

また，利用者像はソフトウェアによっても異なる．たとえば，サーバソフトウェアやシステム管理ソフトウェアの平均的な利用者は，ウェブブラウザやオフィスソフトウェアの平均的な利用者よりも専門知識が豊富であり，より適切な注意を払うことができると想定できる．

表 6: JVN#71872818 の CVSS 評価

評価項目	評価 / 理由
Access Vector	Network / 攻撃者はウェブやメールを経由して管理者（被害者）を罠ページに誘導する.
Access Complexity	High / 複数の条件が必要．一つは受動的攻撃であるため，攻撃者は管理者（被害者）を罠に誘導する必要がある．もう一つは，管理者（被害者）は認証を通過している必要がある.
Authentication	None / 管理者（被害者）は本製品の認証を通過している必要があるものの，本項目は攻撃者にとっての認証有無を評価する項目であるため，本項目が評価対象とする認証は今回存在しない.
Confidentiality Impact	None / CSRF が成立した時点では，特に情報の漏洩が生じる余地はない．CSRF で管理者パスワードを書き換えられた結果，不正ログインを受けて情報が漏洩する等の可能性はあるものの，それは二次的な影響であるため本評価項目には含まれない.
Integrity Impact	Partial / CSRF によって管理者（被害者）の意図しない設定

	変更が生じるため, 完全性に影響する. 変更が生じる範囲は設定のみであり, 製品機能全体が変更される等の全面的な影響はない.
Availability Impact	Partial / CSRF によって接続切断等が行われ, ルータとしての可用性が一時的に損なわれる. 損なわれる範囲は部分的であり, 再接続等の操作を行うことで復旧できる.

CVSS が規定する計算式に当てはめると, 評価値は 4.0 となり, IPA による深刻度はレベル II（警告）となる（表 5）. レベル II（警告）の脅威は,「一部の情報が改ざんされるような脅威」等としており, これは本脆弱性によって実際に生じうる脅威と合致する.

5 今後の検討課題

本章では, 評価事例で指摘した事項以外の留意点と対応についてまとめる.

5.1 IPA と NIST の間における評価の相違

IPA が 2006 年 6 月 23 日から 2007 年 10 月 5 日までの間に評価を行った CVSS Base Metrics のうち, 89 件は NIST NVD でも評価を行っている. これらの評価結果を比較したところ, 65 件（73%）について, 評価の相違がみられた.

これは, 次節で述べる観点の問題に加え, 保有している情報源にも差異があるものと考えられる. IPA では, 評価に相違がある案件については, NIST との間で評価のすり合わせを通して, 評価の整合性確保を今後も続けていく予定である.

5.2 評価にあたっての留意点

5.2.1. アプリケーションの実行権限の想定

4.2.1 で留意したように, アプリケーションの実行権限の想定は評価相違の要因となる. 特に, 権限設定がアプリケーションの使い方による場合には, 評価者間での相違が起きやすくなる. たとえば Windows 上のオフィスアプリケーションは, 一般ユーザ権限で動かすことが可能であり, セキュリティ上の推奨事項でもあるが, 管理者権限で利用される場合も多い. このため現状では Complete と評価する場合が多い.

5.2.2. ソフトウェア利用者像の想定

4.2.2 で留意したように, ソフトウェア利用者像の想定は, 受動的攻撃における評価相違の要因となる.

さらに, 攻撃トレンドの変化も影響する. たとえばウェブサイトにマルウェアを仕掛ける攻撃を想定すると, 以前は利用者自身が不審なウェブサイトを閲覧するかどうかが問題であり, 利用者は注意することができた. しかし近年は正規のウェブサイトであっても改ざんの被害を受けることが増えており, この場合には利用者として注意する方法がない.

このような相違を解決するためには, ソフトウェアの種類ごとに利用者のモデルケースを定めることが有効と考えられる. その際には,「情報セキュリティに関する脅威に対する意識調査」[8] や「通信利用動向調査」[9] などの調査結果を基にできる可能性がある.

5.2.3. 情報不足の際の評価方法

IPA では, 届出を受けたソフトウェアの脆弱性については, 再現検証を行っているため, CVSS 評価にあたり十分な情報があるものが多い. しかし, 中には再現検証ができない脆弱性など, 十分な情報が揃わないものがある. また, ソフトウェアベンダと比較して IPA は, 当該ソフトウェアに関する詳しい動作情報を考慮した評価は難しい.

このような情報不足の場合に, まず情報収集を最大限に行う事となる. このため, 類似案件からの推測など, 根拠に乏しい情報を判断材料にせざるを得ない場合もあり, 評価の相違が生じやすい.

同様の問題は, セキュリティベンダ等の第三者が評価する際にも生じると考えられる. また IPA も, ソフトウェアベンダと比較すれば, 当該ソフトウェアに関する保有情報が少ない場合もあり, 異なる評価をする可能性がある.

解決策として, 情報の正しさの度合いは, Temporal Metrics の Report Confidence で評価することができるため, Base Metrics だけでなく Temporal Metrics も含め評価する方法が考えられる.

5.3 対象システムの範囲

CVSS でウェブアプリケーションの脆弱性を評価する場合, サーバ側の影響のみを考慮し, クライアント側の影響は考慮しないこととして, 下記のように規定されている.

SCORING TIP #2:

When scoring a vulnerability, consider the direct impact to the target host only. For example, consider a cross-site scripting vulnerability: the impact to a user's system could be much greater than the impact to the target host. However, this is an indirect impact. Cross-site scripting vulnerabilities should be scored with no impact to confidentiality or availability, and partial impact to integrity.

（訳）SCORING TIP #2

脆弱性の重み付けをする場合, ターゲットホストへの直接的

な影響だけ考慮する．例えば，クロスサイト・スクリプティングの脆弱性の場合，ユーザのシステムへの影響は，ターゲットホストへの影響よりも遥かに大きいと考えられる．しかしながら，これは間接的な影響となる．

クロスサイト・スクリプティングの脆弱性は，機密性または可用性に影響せず，完全性に部分的 (partial)に影響すると評価すべき．

しかし近年のウェブアプリケーションは，サーバとクライアントが連携して一つのシステムを形成している．クロスサイト・スクリプティングの問題においては，Cookie 等の情報の漏えいも脅威の一つとなっている．しかし,機密性に影響がないと評価してしまっているため，実際の脅威よりも低く見積もられてしまう懸念がある．

今後の CVSS においては，複数のホストが連携するシステムに関しても，システム全体を捉えて評価する必要があると考える．

5.4 スコア算出の根拠

CVSS 評価によって算出されるスコアは，スコア同士を比較可能な順序尺度である．しかし，算出されるスコアについては，測量における単位のような定義はなく，根拠を説明するのは難しい．

今後 CVSS についても，JNSA が脆弱性定量化検討の折に行ったようなアンケート調査を適用することにより，算出されたスコアとシステム管理者が感じる危険度との関係を示すことができると考えられる．

5.5 受け手の行動指針

CVSS スコアは，脆弱性の深刻度を数値として示すことができるが，CVSS スコアを受け手の行動に結び付けるためには，スコア毎の行動ガイドラインが必要である．

現在，公的なガイドラインは存在していないが，大企業向けの行動指針が FIRST の CVSS-SIG の中で提案されている（表 7）[10].

表 7: CVSS スコア別行動指針（大企業向）

スコア	対策期間
0～3	次のサービスパック
4～5	次のパッチサイクル
6～7	14 日程度
7～10	今週中に対策完了のこと

今後は，より詳細な指針の策定が必要になると考えられる．

6 おわりに

本稿では，脆弱性の評価指標として広まりつつある CVSS について，IPA が実際に評価した経験から得られた課題と今後をまとめた．

特に，Base Metrics における評価の相違について詳細な検討を行い，より正確な評価に向けての提言を行った．他の Metrics の評価値も，Base Metrics の評価値を基準として算出されるものであるから Base Metrics 評価の正確さが問われるものとなる．

今後 CVSS-SIG においてもさらに検討を重ね，より正確な評価ができるよう解決を図っていきたい．

謝辞

本稿は，平成 16 年に経済産業省が公示した「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）を受けた，ソフトウエア製品およびウェブアプリケーションの脆弱性に関する情報の届出の枠組みに関する研究である．本研究を進めるにあたり，助言を頂いた関係者各位に感謝する．

参考文献

[1] JVN (Japan Vulnerability Notes), http://jvn.jp/
[2] CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
[3] JVN iPedia, http://jvndb.jvn.jp/
[4] CERT Statistics: Vulnerability Remediation, http://www.cert.org/stats/vulnerability_remediation.html
[5] NIST NVD, CVE Statistics, http://nvd.nist.gov/statistics.cfm?results=1
[6] JNSA，脆弱性定量化に向けての検討報告書, http://www.jnsa.org/result/2006/tech/vulnera/index.html
[7] Payment Card Industry (PCI) Data Security Standard, https://www.pcisecuritystandards.org/pdfs/pci_dss_technical_and_operational_requirements_for_approved_scanning_vendors_ASVs_v1-1.pdf
[8] IPA，情報セキュリティに関する脅威に対する意識調査, http://www.ipa.go.jp/security/fy19/reports/ishiki01/index.html
[9] 総務省，通信利用動向調査, http://www.johotsusintokei.soumu.go.jp/statistics/houdou05.html
[10] Gavin Reid, The Common Vulnerability Scoring System (CVSS) v2, October 2007 FIRST Technical Colloquium