情報処理学会 コンピュータセキュリティ シンポジウム 2006, pp.203-208 (Oct.25-27, 2006)

CVSS を用いた脆弱性評価の検討

小林克巳[†1]　寺田真敏[†1]　山岸正[†1]　小林偉昭[†1]

[†1)] 独立行政法人　情報処理推進機構（IPA）
〒113-6591 東京都文京区本駒込 2-28-8
文京グリーンコート センターオフィス 16 階

概要：ソフトウエアの脆弱性が社会に与える影響が広まりつつある一方，脆弱性そのものが持つ特質や深刻度などに関する定量的な指標や評価情報は少ない．独自の基準により脆弱性評価を行っているセキュリティ企業があるが，この基準は共通化されていない．

近年，脆弱性の深刻度を理解するための共通言語として，CVSS（Common Vulnerability Scoring System）という脆弱性評価基準が検討されている．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，CVSS を用いて評価した結果について述べると共に，評価基準に関する課題について述べる．

キーワード：セキュリティ評価・監査，CVSS，脆弱性評価

Study of Vulnerability Assessment using CVSS

Katsumi KOBAYASHI[†1]　Masato TERADA[†1]　Tadashi YAMAGISHI[†1]　Hideaki KOBAYASHI[†1]

[†1)] Information-technology Promotion Agency, Japan
Honkomagome 2-28-8, Bunkyo, Tokyo, Japan

Abstract: While software vulnerabilities are now posing widespread threats to the Information Society, few quantitative indexes or assessments of the characteristics and severity of the vulnerabilities have been develped nor done. A number of computer security vendors have developed and implemented their own evaluation procedure to assess vulnerabilities. Unfortunately, they are not interoperable.

Recently, CVSS (Common Vulnerability Scoring System) has been introduced and promoted as a common language to discuss the severity and impact of a vulnerability by FIRST (Forum of Incident Response and Security Teams).

In this paper, we present the result of the CVSS scoring of the vulnerabilities reported to IPA (Information-Technology Promotion Agency, Japan),and address several issues in the scoring criteria used by CVSS.

Key words: Security evaluation and audit, CVSS, Vulnerability Scoring

1. はじめに

近年，ソフトウエアの脆弱性が社会に与える影響が広まりつつあり，脆弱性関連情報を公開されることの重要性が増してきている．しかし，公開されている脆弱性関連情報は技術者向けの専門的な情報が多く，また，脆弱性関連情報のほとんどが英語で書かれた文献であるため，利用者が脆弱性の深刻度を理解する際のハードルは高い．

IPA(Information-technology Promotion Agency, Japan)では平成 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）を受けて，情報セキュリティ早期警戒パートナーシップとして，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(JP Vendor Status Notes)[2)]で公開している．

本稿では，脆弱性の深刻度を表す指標として注目されている CVSS（Common Vulnerability Scoring System）[1)] を，利用者の脆弱性に関する理解を深める施策のひとつとして利用するために，IPA に報告された脆弱性関連情報に対して CVSS を適用して試行評価すると共に，CVSS の特性と課題について検討を行なった結果について述べる．

2 背景

2.1. 国内における脆弱性評価の状況

国内では，複数の IT(Information Technology)製品開発企業が自社製品に関する脆弱性関連情報を公開しており，また，セキュリティ企業などが海外・国内の脆弱性関連情報を独自にまとめた情報を公開されている．しかし，これらの脆弱性関連情報では，脆弱性の深刻度を包括的かつ汎用な評価指標として明示されていることは少ない．

IPA が情報セキュリティ早期警戒パートナーシップを基に報告を受けて，JVN で公開した脆弱性関連

情報においても，脆弱性の深刻度を包括的かつ汎用な評価指標として掲載するまでには至っていない.

2.2. 海外における脆弱性評価の状況

海外では，いくつかのセキュリティ企業などが脆弱性関連情報を独自の脆弱性評価基準とともに公開している.

独自の脆弱性評価基準を公開している例として，情報セキュリティの研究機関である SANS が公開している CVA(Critical Vulnerability Analysis)[3]の評価基準を表 1 に示す.

表 1 SANS における評価基準

SANS CVA
How difficult is it to exploit the vulnerability? Remote/Local? Without Credentials or Physical Access?
Is the problem found in default configurations/installations?
How trivial is it for an informed attacker to devise his own exploit?
Does the attacker need to social engineer his victim? (e.g. clicking a link, visiting a site, connecting to a server, etc.).
Is exploit code publicly available?
Is the vulnerability being actively exploited in the wild?
Are technical vulnerability details available?
Is the network infrastructure affected (DNS, routers, firewalls)?
Are the affected assets high value (e.g. databases, e-commerce servers)?
Is the affected product widely deployed?
Is this a server or client compromise? At what privilege level?

CVA では, 脆弱性の特徴を細かく分類してあるため，深刻度を把握しやすいが，包括的かつ汎用な評価指標ではないため，他の組織が評価した結果との比較が難しい.

2004 年, 共通した評価基準が存在しないということから，米国政府の国家インフラストラクチャ保証評議会 NIAC(National Infrastructure Advisory Council)[4]におけるプロジェクトの一環として，セキュリティ企業を含む複数の企業や組織の相互協力のもとに，脆弱性の深刻度を包括的かつ汎用的に評価する共通言語として CVSS が開発された．CVSS は，米国連邦政府への展開が図られており，NIST(National Institute of Standards and Technology)[5]が運用している脆弱性データベース NVD(National Vulnerability Database)[6]に登録されている脆弱性関連情報の評価に用いられている．NVD に登録されている脆弱性関連情報は, 非営利団体の MITRE 社が運用している脆弱性リストの識別番号である CVE(Common Vulnerabilities and Exposures)[7]によって管理されており，1999 年以降に CVE 番号が割り当てられた約 13,000 件を超える脆弱性関連情報に，CVSS を用いた評価が行われている. その他に ISS(Internet Security Systems)社が脆弱性関連情報を提供しているウェブサイト X-Force[8]において，CVSS の評価基準を用いている.

3. CVSS の概要

3.1. 脆弱性の特徴の分類

CVSS は, 脆弱性を Base Metrics, Temporal Metrics, Enviromental Metrics という 3 つの特徴に分類し，脆弱性の特徴ごとにパラメタを定めている．これを規定の式に当てはめて計算することで脆弱性の深刻度を数値として表示する．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.

表 2 Base Metric Scoring

AccessVector	= case AccessVector of	
	local	0.7
	remote	1.0
AccessComplexity	= case AccessComplexity of	
	high	0.8
	low:	1.0
Authentication	= case Authentication of	
	required	0.6
	not-required	1.0
ConfImpact	= case ConfidentialityImpact of	
	none	0
	partial	0.7
	complete	1.0
ConfImpactBias	= case ImpactBias of	
	normal	0.333
	confidentiality	0.5
	integrity	0.25
	availability	0.25
IntegImpact	= case IntegrityImpact of	
	none	0
	partial	0.7
	complete	1.0
IntegImpactBias	= case ImpactBias of	
	normal	0.333
	confidentiality	0.25
	integrity:	0.5
	availability	0.25
AvailImpact	= case AvailabilityImpact of	
	none	0
	partial	0.7
	complete:	1.0
ImpactBias	= case ImpactBias of	
	normal	0.333
	confidentiality:	0.25
	integrity	0.25
	availability	0.5

```
BaseScore = round_to_1_decimal(10 *
AccessVector * AccessComplexity * Authentication
* ((ConfImpact * ConfImpactBias)
+ (IntegImpact * IntegImpactBias)
+ (AvailImpact * AvailImpactBias)))
```

(1)Base Metrics

脆弱性そのものの特性を評価する基準である．この値は脆弱性の本質的な特徴を評価するため，異なった環境においても変化しない（表 2）．

脆弱性により情報システムが受けうる影響を，情報システムに求められる 3 つのセキュリティ特性，「Confidentiality(機密性)」，「Integrity(完全性)」，「Availability(可用性)」 (C.I.A.)のそれぞれに対し，COMPLETE（全体が影響を受ける），PARTIAL（一部が影響を受ける），NONE（全く影響を受けない）の三段階で評価する．この 3 つが Base Metrics の評価に大きく影響する．

また，対象の情報システムが C.I.A.のどこに重みを持つかを，Impact Bias で評価する．

(2)Temporal Metrics

攻撃コードの出現有無や対策情報が利用可能であるかといった，時間に依存した脆弱性の特徴を評価する．この値は Base Metrics の値に依存する（表 3）．

表 3　Temporal Metric Scoring

Exploitability	= case Exploitability of	
	unproven	0.85
	proof-of-concep	0.9
	functional	0.95
	high	1.00
RemediationLevel	= case RemediationLevel of	
	official-fix	0.87
	temporary-fix	0.90
	workaround	0.95
	unavailable	1.00
ReportConfidence	= case ReportConfidence of	
	unconfirmed	0.90
	uncorroborated	0.95
	confirmed	1.00
TemporalScore = round_to_1_decimal(BaseScore * Exploitability* RemediationLevel* ReportConfidence)		

表 4　Enviromental Metric Scoring

CollateralDamagePotential= case CollateralDamagePotential of		
	none	0
	low	0.1
	medium	0.3
	high	0.5
TargetDistribution	= case TargetDistribution of	
	none	0
	low	0.25
	medium	0.75
	high	1.00
EnvironmentalScore = round_to_1_decimal((TemporalScore + ((10 - TemporalScore) * CollateralDamagePotential)) * TargetDistribution)		

(3)Enviromental Metrics

攻撃を受けた場合の二次的な被害の大きさや，対象製品の使用状況といった利用環境を評価する（表 4）．この値は Temporal Metrics の値に依存する．

3.2. 脆弱性を評価する組織と役割

CVSS は，脆弱性関連情報を管理する企業やセキュリティ製品を開発している企業などといった，情報セキュリティに携わる組織が，脆弱性を調査・確認すると共に，製品利用者に通知するための取り組みに利用する．

情報セキュリティに携わる組織は，Base Metrics および Temporal Metrics を評価する．評価された Base Metrics，Temporal Metrics の値を元に，製品利用者が Enviromental Metrics を評価することにより，総合的な脆弱性の深刻度を評価する．

3.3. CVSS を用いた脆弱性評価の例

2003 年に報告されたアンチウイルスソフトウエアにおけるバッファオーバーフローの脆弱性(CVE-2003-0062)について，FIRST(Forum of Incident Response and Security Teams)が公開している評価事例[9]を表 5 に示す．この脆弱性は，アンチウイルスソフトである NOD32 を実行しているユーザの権限で，ローカルの第三者に任意のコードを実行されてしまう問題である．

表 5　CVSS 評価の一例

Vulnerability Common Name	Buffer Overflow In NOD32 Antivirus Software
CVE reference	CVE-2003-0062
Access Vector	LOCAL [0.7]
Access Complexity	HIGH [0.8]
Authentication	NOT-REQUIRED [1.0]
Confidentiality Impact	COMPLETE [1.0]
Integrity Impact	COMPLETE [1.0]
Availability Impact	COMPLETE [1.0]
Impact Bias	NORMAL [0.333]
BASE SCORE	(10 * 0.7 * 0.8 * 1.0 * (1.0 * 0.333) + (1.0 * 0.333) + (1.0 * 0.333)) = 5.6
Exploitability	PROOF-OF-CONCEPT [0.90]
Remediation Level	OFFICIAL-FIX [0.90]
Report Confidence	CONFIRMED [1.0]
TEMPORAL SCORE	(5.6 * 0.90 * 0.90 * 1.00) = 4.4
Collateral Damage Potential	None – High [0 - 0.5]
Target Distribution	None – High [0 - 1.0]
ENVIRONMENTAL SCORE	((4.4 + ((10 - 4.4) * {0 - 0.5})) * {0 - 1.00}) = (0.00～7.20)

4. IPA での CVSS 適用試行報告と特徴

4.1. CVSS 適用試行の評価対象

情報セキュリティ早期警戒パートナーシップに基づき，2004 年 7 月以降に IPA が受付・分析した脆弱性関連情報に対して，CVSS を適用し評価した結果と，NVD に登録されている脆弱性関連情報を NIST が評価した結果を比較する．

本稿では，CVSS の値として，時間や環境に影響されない Base Metrics の値のみを対象に，その違いについて示すと共に要因を考察する．

4.2 NIST と IPA が評価した深刻度の比較

4.2.1. 深刻度分布から見る評価の違い

(1)適用結果

NVD に登録されている脆弱性関連情報を NIST が評価した件数を年別に分けたグラフを図 1 に，IPA が受付・分析した脆弱性関連情報の件数を年別に分けたグラフを図 2 に示す．

NIST は CVSS で評価した値を元に，0.0～3.9 の範囲を Low，4.0～6.9 の範囲を Medium，7.0～10.0 の範囲を High として深刻度を定義している．

国際的な整合性確保を目的として，IPA が受付・分析した脆弱性関連情報についても，NIST と同様に深刻度を分類すると同時に，脆弱性の種類別に集計した(図 3).

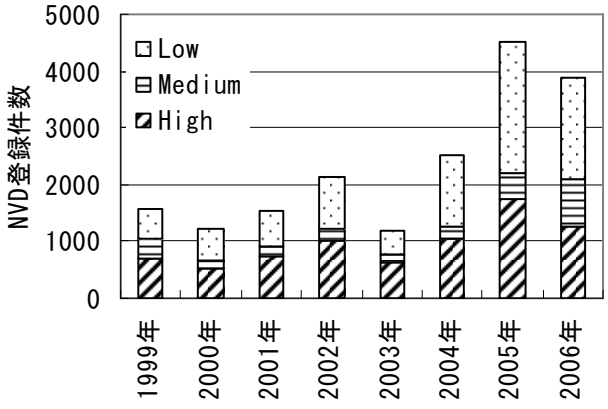

図 1　NIST が評価した年別の深刻度分布

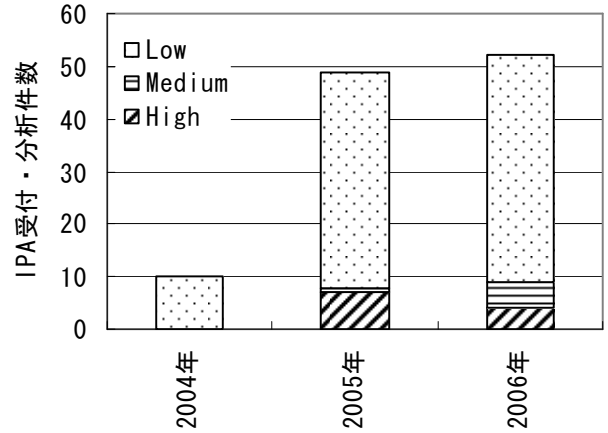

図 2　IPA が評価した年別の深刻度分布

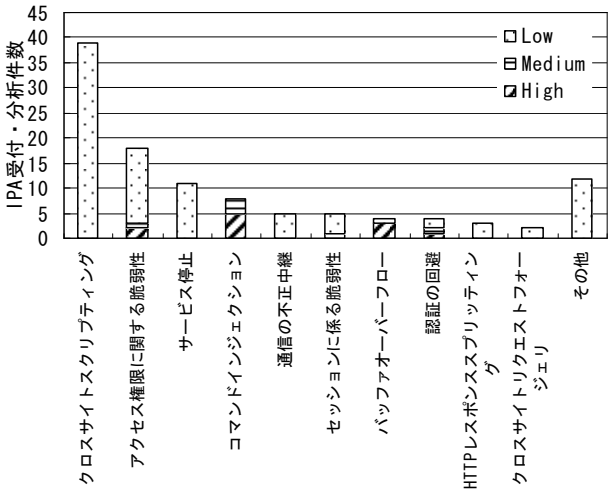

図 3　IPA が評価した脆弱性種類別の深刻度分布

(2)考察

NIST が評価した深刻度は，1999 年から継続して，Low と High の件数が同程度の割合を占めており，Medium の件数が少ない傾向がある．これと比較すると，IPA が評価した深刻度は，Low の件数が多く，High の件数が少ない．これは，IPA が受付・分析した脆弱性関連情報に，低く評価したクロスサイトスクリプティングの報告件数が多かったことが理由であると考えられる．

図 3 より，クロスサイトスクリプティングの脆弱性が多いことから，発見が容易な脆弱性に関する報告件数が増えているためと考えられる．

4.2.2. BaseMetrics 深刻度から見る評価特性

(1)適用結果

NVD に登録されている脆弱性関連情報を NIST が評価した件数を深刻度別に分けたグラフを図 4 に，IPA が受付・分析した脆弱性関連情報の件数を深刻度別に分けたグラフを図 5 に示す．

それぞれのグラフにおいて，4.2.1.と同様に NIST の深刻度の分類に合わせて，Low を点，Medium を横線，High を右上がり斜線として示す．

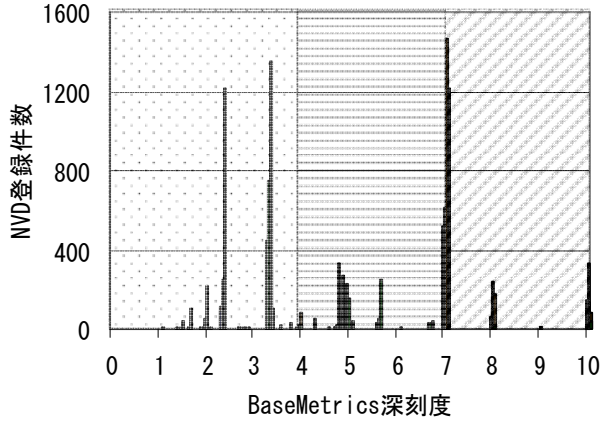

図 4　NIST が評価した深刻度分布

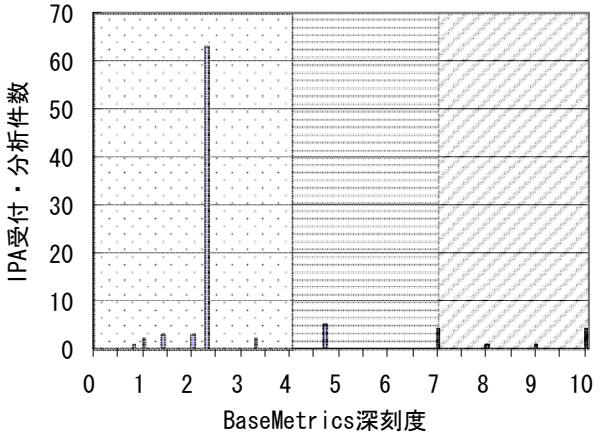

図 5　IPA が評価した深刻度分布

NVD に登録されている脆弱性関連情報を NIST が評価した結果は，2.3，3.3，7.0 に特に件数が集中している．同様に，JVN で公開している脆弱性関連情報を IPA が評価した結果は，2.3 に集中しており，深刻度は同じような値に集まる傾向がある．

(2)考察

2 つのグラフに共通して件数が多かった評価値 2.3 に着目すると，この値を導き出す評価項目は 13 種類の組み合わせが存在する．

OS や専門機器を除いた一般的なソフトウエアでは, Impact Bias が C.I.A.に評価されることは少ない．そのため, 13 種類ある組み合わせのうち, Impact Bias の項目を NORMAL と評価する組み合わせに限定すると，次に示す 3 種類の組み合わせが存在する．

(a) リモートから認証を必要とせずに攻撃可能であり，C.I.A.のうち一項目を PARTIAL，残る二項目を NONE と評価する．

(10 * 1.0 * 1.0 * 1.0 * (0.7 * 0.333) + (0 * 0.333) + (0 * 0.333)) = 2.331=2.3

(b) ローカルからのみ攻撃可能であり，C.I.A.のうち一項目を COMPLETE, 残る二項目を NONE と評価する

(10 * 0,7 * 1.0 * 1.0 * (1.0 * 0.333) + (0 * 0.333) + (0 * 0.333)) = 2.331=2.3

(c) ローカルから複雑な条件および認証を必要として攻撃可能であり，C.I.A.全てを PARTIAL と評価する

(10 * 0.7 * 0.8 * 0.6 * (0.7 * 0.333) + (0.7 * 0.333) + (0.7 * 0.333)) = 0.2349648=2.3

(a)～(c)の中で, 攻撃に必要な条件が最も少ない組み合わせは(a)であることから，評価値 2.3 の脆弱性のうち，発見が容易な脆弱性は(a)の組み合わせになることが考えられる．

4.2.3. 評価項目から見る深刻度の違いと課題

(1)適用結果

IPA が受付・分析した脆弱性関連情報のうち，CVE 番号が発行された 20 件について，NIST が評価した深刻度と比較した結果(表 6)，14 件の脆弱性関連情報の深刻度に差が生じた．このうち，4 件では NIST が定義した 3 段階の深刻度の分類に差が生じた．

深刻度の分類に差を生じた 4 件の中から，(CVE-2006-2501)の評価を表 7 に示し，深刻度に差が生じた要因を検証する．この脆弱性はクロスサイトスクリプティングであり，ユーザのブラウザ上で第三者が任意のスクリプトを実行できる問題である．NIST の評価は Confidentiality, Availability の評価項目を PARTIAL と評価しているが, IPA の評価では影響を受けないと判断し NONE と評価している．

表 6　CVE 番号別深刻度一覧

CVE 番号	NIST の評価		IPA の評価	
CVE-2004-1236	10.0	High	8.0	High
CVE-2005-0643	7.0	High	8.0	High
CVE-2005-0644	7.0	High	8.0	High
CVE-2005-0922	3.3	Low	3.3	Low
CVE-2005-0923	2.3	Low	2.3	Low
CVE-2005-2411	8.0	High	2.3	Low
CVE-2005-2336	3.3	Low	2.3	Low
CVE-2005-2803	3.3	Low	2.3	Low
CVE-2005-3042	7.0	High	9.0	High
CVE-2005-2337	7.0	High	1.6	Low
CVE-2005-2339	3.5	Low	2.3	Low
CVE-2005-2969	3.3	Low	2.3	Low
CVE-2005-2338	3.3	Low	2.3	Low
CVE-2005-3352	2.3	Low	2.3	Low
CVE-2006-0195	2.3	Low	2.3	Low
CVE-2006-2007	7.0	High	7.0	High
CVE-2006-1546	7.0	High	4.7	Medium
CVE-2006-2501	7.0	High	2.3	Low
CVE-2006-2517	7.0	High	7.0	High
CVE-2006-2384	3.7	Low	2.3	Low

表 7　NIST と IPA の評価内容の比較

	NIST の評価	IPA の評価
Vulnerability Common Name	Sun Java System Web Server におけるクロスサイトスクリプティングの脆弱性	
CVE reference	CVE-2006-2501	
Access Vector	Remote	Remote
AccessComplexity	Local	Local
Authentication	Not-Required	Not-Required
Confidentiality Impact	Partial	None
Integrity Impact	Partial	Partial
Availability Impact	Partial	None
Impact Bias	Nomal	Normal
BASE SCORE	7.0	2.3

(2)考察

深刻度にこのような差が生じる要因として，次のことが考えられる．

(a) 評価組織ごとの脆弱性関連情報に差がある
- 例えば，具体的な攻撃手法の知識の有無により，C.I.A.の評価が異なり，値が変わる

(b) 評価組織ごとに評価判断基準が異なる
- 例えば，対象システムとして評価する範囲が異なることで，Access Vector や Access Complexity の評価が異なり，値が変わる

(c) 複数の脆弱性がある場合に，公開の仕方に差がある
- 例えば，一つの製品にクロスサイトスクリプティングとバッファオーバーフローが存在する場合に，脆弱性関連情報を一つずつ評価し公開する場合と，二つの脆弱性関連情報を評価し，深刻な脆弱性の評価に絞って，まとめた情報として公開する場合では，利用者に伝わる評価の値が変わる

表 7 に示した脆弱性関連情報は，一つの脆弱性に関する情報であるため，(a)もしくは(b)により深刻度に差が生じたことが考えられる．さらに，表 7 では，Base Metrics の計算において重要な評価項目である Confidentiality，Availability が異なったことから，深刻度に大きい差が生じたと考える．

5. 課題

CVSS にはいくつかの課題が残されている．

まず，Temporal Metrics の評価は，時間が経過すると変化していく評価項目であるため，日々新たに発見・報告される脆弱性を継続的に評価し続ける手順の確立が必要である．情報を収集する時間の範囲に制限を設けるなど，評価方法に基準を設けるといった運用に関する課題を解決しなければならない．

そして，4.2.4 節で示したように深刻度の違いは，利用者に混乱を招く要因となる．

今後，深刻度の差を無くすための活動として，評価組織ごとに評価した深刻度を共有する仕組み作りを検討していくことが必要であろう．

6. おわりに

本稿では，脆弱性関連情報の利用者の脆弱性に関する理解を深める施策のひとつとして CVSS に着目し，実際に報告された脆弱性関連情報を評価すると共に，CVSS の特性と課題について述べた．

CVSS は，包括的かつ汎用的な評価手法として注目されている．今後の課題として，CVSS を用いたソフトウエアの評価における課題を解決しつつ，ウェブアプリケーションに特有の脆弱性についても，CVSS を適用して評価し，課題を検討していきたい．

また，評価組織によって深刻度に差を生じさせない仕組みについては，NIST など CVSS を利用している組織との連携を進め解決を図って行きたい．

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) CVSS (Common Vulnerability Scoring System)
http://www.first.org/cvss/
2) JVN (JP Vendor Status Notes)
http://jvn.jp/
3) SANS CVA (Critical Vulnerability Analysis)
http://www.sans.org/newsletters/cva/
4) NIAC (National Infrastructure Advisory Council)
http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0353.xml
5) NIST (National Institute of Standards and Technology)
http://www.nist.gov/
6) NVD (National Vulnerability Database)
http://nvd.nist.gov/
7) CVE (Common Vulnerabilities and Exposures)
http://cve.mitre.org/
8) ISSKK X-Force セキュリティアラート&アドバイザリ
http://www.isskk.co.jp/support/techinfo/X-ForceAlerts.html
9) FIRST (Forum for Incident Response and Security Teams)
Complete CVSS Guide
http://www.first.org/cvss/cvss-guide.html
10) 情報処理推進機構：セキュリティセンター：脆弱性関連情報取扱い
http://www.ipa.go.jp/security/vuln/index.html
11) The RSA Conference, February 2005
The Common Vulnerability Scoring System
http://www.packetfactory.net/papers/CVSS/cvss-ppt.pdf