2F-2

CVSS を用いた脆弱性評価の検討

小林克巳† 寺田真敏† 山岸正† 小林偉昭†
独立行政法人 情報処理推進機構（IPA）†

1 はじめに

近年，IT インフラの発達によりビジネスにおけるウェブサイトの利用が増加してきた．これに伴い，ソフトウェアの脆弱性が社会に与える影響が広まりつつあり，脆弱性関連情報を用いた対策推進の重要性が増してきている．

IPA では経済産業省の公示「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」[1]を推進している．パートナーシップにおける IPA の役割は，ソフトウェア製品およびウェブアプリケーション（ウェブサイト）の脆弱性に関する情報の届出を受付け，分析を行なうこと，報告された脆弱性関連情報を JPCERT/CC と共同運営の JVN(JP Vendor Status Notes)[2]で公開していくこと，脆弱性の深刻度の評価指標を作成することなどが挙げられる．特に，深刻度の評価指標については，ソフトウェア製品とウェブサイトの双方に適用可能な指標を作成するため，これまで届けられたソフトウェア製品の脆弱性関連情報の深刻度を CVSS(Common Vulnerability Scoring System)[3]を用いて評価を行なってきた[4].

本稿では，パートナーシップで届けられたウェブサイトの脆弱性の深刻度評価に，CVSS を適用した結果について述べる．

2 CVSS の背景と特徴

CVSS は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，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開発された．2006 年 10 月には，CVSS が 34 の組織で実利用されている．

CVSS は，“Base Metrics（基本評価基準）”，“Temporal Metrics（現状評価基準）”と“Environmental Metrics（環境評価基準）”の 3 つの評価特性を持ち，特性ごとに細分化され数値が定められている．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 0～10.0 に数値化する．個々の特性については，主に情報セキュリティに携わる組織が，“Base Metrics”，“Temporal Metrics”の値を提供し，利用者はその値に基づき“Environmental Metrics”を算出し最終結果を出す．

Study of Vulnerability Assessment using CVSS
† Katsumi KOBAYASHI, Masato TERADA, Tadashi YAMAGISHI, Hideaki KOBAYASHI, "Information-technology Promotion Agency, Japan."(IPA)

3 ウェブサイトの深刻度評価

本節では，ウェブサイトの脆弱性の深刻度評価に，CVSS を適用した結果を示す．尚，評価にあたっては時間や環境に影響されない“Base Metrics”を検討対象とする．

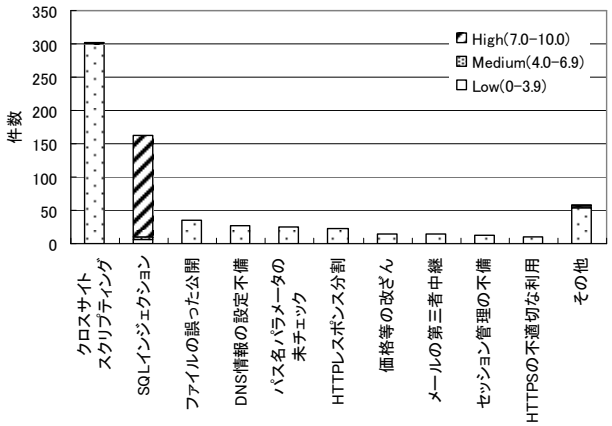

図 1 ウェブサイトの脆弱性の種類別深刻度分布

3.1 評価結果

2004 年 7 月から 2006 年 12 月までに IPA に報告された約 750 件のウェブサイトの脆弱性関連情報を，CVSS で評価し，脆弱性の種類別に分類したデータを図 1 に示す．

一般に脅威が高いと言われている“SQL インジェクション”は High に区分され，脅威が低いと言われている“クロスサイトスクリプティング”などは Low に区分されたことから，CVSS はウェブサイトの脆弱性の深刻度評価について妥当な値を算出していると考えられる．

3.2 ウェブサイトとソフトウェア製品の評価項目の差異

ソフトウェア製品とウェブサイトで評価した際の評価項目の差を提示するため，“クロスサイトスクリプティング”と“SQL インジェクション”の脆弱性を評価した例を表 1 に示す．

脆弱性の種類別に深刻度は異なるものの，ソフトウェア製品とウェブサイトで CVSS の評価パターンに差が生じず，同じ深刻度となることが分かった．

この結果から，ウェブサイトの脆弱性深刻度とソフトウェア製品の深刻度には類似性があると判断でき，ソフトウェア製品の深刻度と同様にウェブサイトの脆弱性に CVSS が適用できると考えられる．

表 1　クロスサイトスクリプティングと SQL インジェクションの評価比較

CVSS 評価項目	クロスサイトスクリプティング		SQL インジェクション	
	ソフトウェア製品	ウェブサイト	ソフトウェア製品	ウェブサイト
Access Vector	Remote	←	Remote	←
Access Complexity	Low	←	Low	←
Authentication	Not Required	←	Not Required	←
Confidentiality Impact	None	←	Partial	←
Integrity Impact	Partial	←	Partial	←
Availability Impact	None	←	Partial	←
Impact Bias	Normal	←	Normal	←

3.3　ウェブサイトの脆弱性深刻度の需要検討

脆弱性を評価する各組織は，CVSS をソフトウェア製品の脆弱性に関する深刻度評価に利用している．今回，新たな試みとしてウェブサイトの脆弱性の深刻度評価に CVSS を適用した結果から，ウェブサイトの脆弱性深刻度を評価することの必要性を検討した結果について述べる．

ソフトウェア製品とウェブサイトの脆弱性深刻度のデータを図 2 と図 3 に示す. また, 図 2 のうち 53%を占めるウェブサイトで利用されるソフトウェア製品の脆弱性深刻度のデータを図 4 に示す.

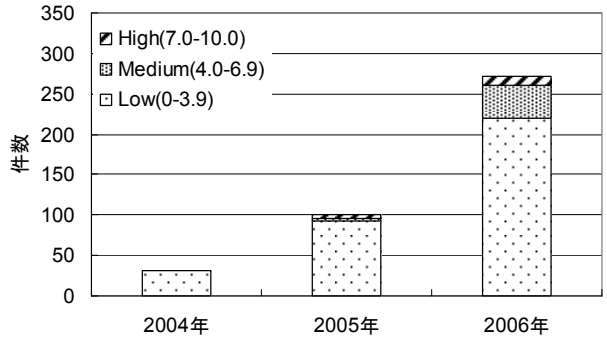

図 2　ソフトウェア製品の脆弱性深刻度推移

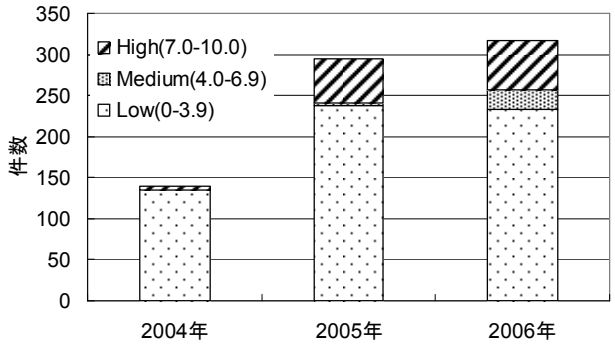

図 3　ウェブサイトの脆弱性深刻度推移

図 2，図 3 を比較すると，国内で報告されている脆弱性は，ウェブサイトがソフトウェア製品に比べて深刻度の高い脆弱性が多く，報告件数も多い．また図 4 より，ソフトウェア製品の脆弱性のうちウェブサイトの脆弱性が増加していることから，ウェブサイト運営者やソフトウェア製品開発者が脆弱性の深刻度を理解するうえで，定量的かつ包括的な深刻度を評価するフレームワークの必要性は高い．

CVSS は包括的かつ汎用的なフレームワークであること，ソフトウェア製品の脆弱性評価との整合性確保の点からも，ウェブサイトの脆弱性深刻度を評価するフレームワークとして適していると考える．

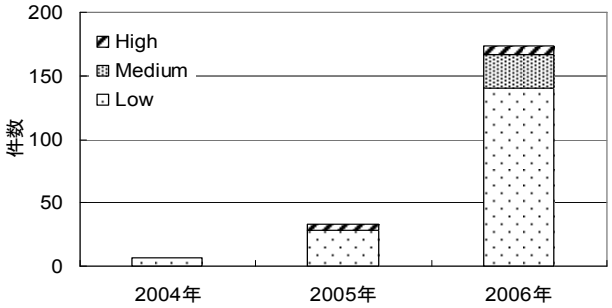

図 4　ソフトウェア製品の脆弱性のうち ウェブサイトの脆弱性の深刻度推移

4　おわりに

今回，ウェブサイトの脆弱性の深刻度を CVSS で評価することにより，ウェブサイトの脆弱性の深刻度評価に CVSS の適用性を検証すると共に，ウェブサイトにおける脆弱性を評価するフレームワークの必要性について述べた．また，本稿の検討結果として，ウェブサイトの脆弱性について CVSS 用いた深刻度評価が可能であることを示した．

今後も CVSS を用いた深刻度の評価を継続し，ウェブサイトの脆弱性の分析を行うと共に，ソフトウェア製品とウェブサイトの脆弱性の深刻度評価の整合性を図っていく．また，評価組織間で深刻度が一致しない場合に整合性を確保する仕組みについても検討していく予定である．

参考文献

[1]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
[2] JVN (JP Vendor Status Notes), http://jvn.jp/
[3] Complete CVSS Guide,
http://www.first.org/cvss/cvss-guide.html
[4]小林克巳 他，“CVSS を用いた脆弱性評価の検討”, 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 (2006)