CWE を用いた脆弱性分類の検討

谷口 隼祐　　永安 佑希允　　相馬 基邦
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）
〒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

あらまし ソフトウェア等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分類などに関する共通の指標は少ない．独自の基準により脆弱性分類を行っている組織があるが，この基準は共通化されていない．近年，脆弱性用語の共通言語として，CWE（Common Weakness Enumeration）が注目されつつある．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，CWE を用いて分類した結果について述べると共に，分類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，脆弱性，CWE，脆弱性分類

Study of Vulnerability Classification using CWE

Shunsuke TANIGUCHI　Yukinobu NAGAYASU　Motokuni SOUMA
Masato TERADA　Tadashi YAMAGISHI　Hideaki KOBAYASHI

Information-technology Promotion Agency, Japan
Honkomagome 2-28-8, Bunkyo, Tokyo, Japan

Abstract While the impact that software vulnerabilities inflict upon the society is getting broader and more serious, there are still few standards that address vulnerabilities themselves, such as their characteristics and classification. Some organizations use their own classification schemes but they are not standardized.

In recent years, CWE (Common Weakness Enumeration) has emerged to provide a common ground in this arena. In this paper, we will discuss the result of classifying vulnerabilities reported under the Information Security Early Warning Partnership in Japan using CWE and the issues we see with CWE.
Key words: Security evaluation and audit, Vulnerability, CWE, Vulnerability Classification

1. はじめに

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）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いる．その取組みの中で，報告された脆弱性関連情報を独自の基準で分類し，四半期ごとに統計情報を IPA のウェブサイトで公開している[1].

その他，複数の組織が，それぞれ独自の基準により脆弱性を分類しているが，それらの基準の間に一貫性がないため，同一の脆弱性に対する分類の粒度や，どこまでを脆弱性とするかという認識に相違が生じており，相互に比較・検討することが困難である．

本稿では，脆弱性に対する認識の相違を防ぎ，ソフトウェア開発者や利用者に適切な脆弱性対策を促すために，脆弱性用語の共通言語である CWE（Common Weakness Enumeration）[2]を，IPA に報告された脆弱性関連情報の分類基準として試行利用すると共に，CWE の特性と課題について検討を行った結果について述べる．

2. 脆弱性分類の現状

現状，複数の組織がそれぞれ独自の基準で脆弱性を分類している．本章では，ウェブアプリケーションに特化した脆弱性分類，および汎用的な脆弱性分類の現状を述べる．

2.1. ウェブに特化した分類

(1) IPA

IPA では，四半期ごとに脆弱性関連情報の統計情報をウェブサイトで公開している．その中でウェブアプリケーションに関する脆弱性関連情報に

ついて，表 1 のように分類している．

表 1: ウェブアプリケーションの脆弱性の分類

ファイルの誤った公開
パス名パラメータの未チェック
ディレクトリ・トラバーサル
セッション管理の不備
SQL インジェクション
DNS 情報の設定不備
オープンプロキシ
クロスサイト・スクリプティング
クロスサイト・リクエスト・フォージェリ
HTTP レスポンス分割
セキュリティ設定の不適切な変更
リダイレクタの不適切な利用
フィルタリングの回避
OS コマンド・インジェクション
メールの第三者中継
HTTPS の不適切な利用
価格等の改ざん

これは，届出があった脆弱性関連情報を基に分類したものであり，網羅的かつ粒度の揃った分類ではないが，国内におけるウェブアプリケーションの脆弱性の傾向を反映した分類となっている．

(2) OWASP Top Ten Project

OWASP（Open Web Application Security Project）の Top Ten Project[3]では，ウェブアプリケーションの脆弱性対策の重要性について啓蒙することを目的とし，ウェブアプリケーションにおける深刻な脆弱性に絞り，上位 10 個の脆弱性に関してまとめている (表 2)．本取組みは，脆弱性対策の取り掛かりとして有用だが，深刻な脆弱性に対象を絞っており，範囲が限定されているため，脆弱性の共通の分類を目的とした利用は困難である．

(3) WASC

WASC（Web Application Security Consortium）の Web Security Threat Classification[4]は，ウェブサイトのセキュリティに対する脅威を明らかにし，体系化するために，攻撃手法を基準として脆弱性を分類している．分類は，6 つの大分類と 24 つの細分類に分けられる．現状の攻撃手法を基準とした分類体系では，HTTP レスポンス分割などの脆弱性が分類できない問題があり，網羅的に脆弱性を分類するためには，分類体系の整備が必要である．

2.2. 汎用の分類

(1) SecurityFocus Vulnerability Database

SecurityFocus[3]は，すべてのプラットフォームやサービスを対象とした脆弱性関連情報を提供する，SecurityFocus Vulnerability Database を運営している．Vulnerability Database では，エラーの発生箇所を基に分類を行っている．分類は Class と呼ばれ，Boundary Condition Error（境界条件エラー）や，Access Validation Error（不正アクセスエラー），Input Validation Error（不正入力エラー）などがある．クロスサイト・スクリプティングや，SQL インジェクションなどウェブアプリケーションに関する脆弱性は，大抵 Input Validation Error（不正入力エラー）が該当する．

(2) CWE

CWE は，ソフトウェアの脆弱性の種類や関連する情報について列挙したものである．現時点の最新版である Draft9 では，695 種類が列挙されており，それらに対して識別子である CWE-ID を発行し管理している．また，CWE-ID が発行された脆弱性を階層構造で分類した Natural Hierarchy を公開している．

脆弱性が幅広く列挙され，かつ階層構造による脆弱性分類のため，分類の粒度の違いも客観的に把握することができる．

3. 共通の分類基準を使用する利点

同一の脆弱性に対する分類の粒度や，どこまでを脆弱性とするかという認識に相違が生じる原因のひとつとして，分類基準の一貫性がないことが挙げられる．

共通の分類基準を使用することで，ソフトウェア開発者や利用者の脆弱性理解を助け，その結果，適切な脆弱性対策の実装を促すことができる．また，脆弱性検査ツール等の客観的な性能比較が可能になる利点もある．

共通の分類基準の条件として，分類の粒度の違いが把握でき，網羅的に脆弱性が定義されていることが挙げられる．

その点，CWE は網羅的に脆弱性の種類が列挙され，さらに階層構造で分類されているため，分類の粒度の違いが把握でき，脆弱性の定義の共通化を図る基準となり得る．

以上より，IPA では，共通の分類基準の条件に合致する CWE を試行利用し，CWE の特性と課題について検討を行った．

4. CWE の概要

CWE は，国土安全保障省 DHS（U.S. Department of Homeland Security）の支援のもと，非営利団体の MITRE 社[5]が運用している，ソフトウェアの脆弱性の種類について列挙したものである．2006 年 3 月に CWE Draft1 が, 2008 年 4 月に CWE Draft9 が公開され, 現在 40 を超える組織により仕様改善や内容の拡充が行われている. 2008 年 8 月に CWE Version 1.0 がリリースされる予定である．

利用事例として，NIST（National Institute of Standards and Technology）が運営する NVD（National Vulnerability Database）[6]や，OWASP Top Ten Project がある. 以降, CWE の特徴を示す.

(1) CWE-ID の一意性

脆弱性の種類や関連する情報を列挙し，それらすべてに識別子である CWE-ID を発行しており，一部を除くすべての CWE-ID を階層構造で分類している. CWE-ID は Views, Categories, Weaknesses, Compound_Elements の 4 種類に分けられ，全体を通して一意の ID が発行される．

また, 個々の CWE-ID について, 脆弱性の概要, 一般的な脅威，軽減策，実際に起きたソフトウェア製品の脆弱性の事例紹介などの情報が記載されている．

(2) 階層構造による分類

CWE-ID は，脆弱性の種類が階層構造で分類されている．根に近いほど抽象的な分類を示し，末端にいくほど具体的な分類，もしくは個々の脆弱性を示す (図 1)．また，親ノードは子ノードの性質を備えているため，分類の粒度が異なる 2 つの統計情報を比較する場合，直近の共通の親同士を比較することで粒度の違いを吸収できる．

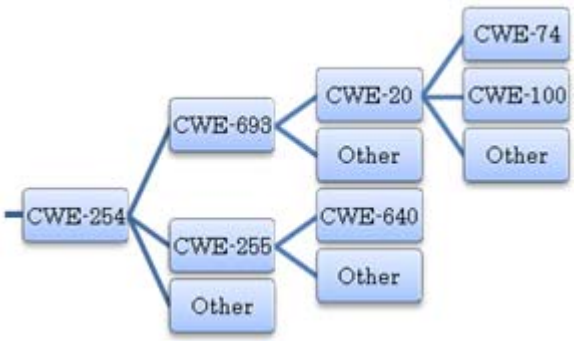

図 1:階層構造の例

(3) CWE-ID の種類

CWE-ID は 4 種類に分けられ，表 2 に示す特徴があり，いずれかひとつに属する．

表 2: CWE-ID の種類

種類	特徴
Views	ある観点からいくつかの脆弱性を選択してグループ化したものを表す.
Categories	共通の特性を持つ脆弱性をまとめたものを表す.
Weaknesses	個々の脆弱性を表す. Weaknesses は，さらに Class，Base，Variant の 3 つに細分化される. Class: 抽象的な脆弱性を表す Base: 特定のリソースや技術に依存しない脆弱性を表す Variant: 個々のリソースや技術, コンテキストが特定できる脆弱性を表す
Compound_Elements	複数の要因からなる脆弱性を表す.

Views は，特定の観点の脆弱性に焦点を絞る際に利用される．例えば，NIST の NVD で扱っている脆弱性の範囲を CWE-635: Weaknesses Used by NVD で，OWASP Top Ten Project で扱っている脆弱性の範囲を CWE-629: Weaknesses in OWASP Top Ten で定義している．

Categories は，CWE-310: Cryptographic Issues のように共通の技術的特性を持つ脆弱性をまとめたものを表し，Weaknesses は Categories よりも具体的な個々の脆弱性を表す．さらに Weaknesses は Class，Base，Variant に細分化されている．

Compound_Elements は，CWE-680: Integer Overflow to Buffer Overflow のように，ある問題が原因で別の問題が発生する等の複数の要因からなる脆弱性を表す.

(4) 個々の CWE-ID に関する情報

CWE-ID が発行されている脆弱性は，様々な情報が項目別に記載されている．記載されている項目数は CWE-ID 毎に異なり，3～16 個とばらつきが大きい．記載例として，CWE-79: Failure to Sanitize Directives in a Web Page (aka 'Cross-site scripting' (XSS))に関する項目を示す (表 3).

表 3: CWE-79 に関する記載項目一覧

項目名	内容の説明
Weakness ID	CWE-ID の番号と種類を表す 例: Weakness 79 (CWE-ID の番号が 79 で種類が Weakness の意)
Description	当該脆弱性の概要
Alternate Terms	当該脆弱性を表現する他の用語 例: CSS（Cross Site Scripting）
Likelihood of Exploit	攻撃の受けやすさ 例: High to Very High
Weakness Ordinality	独立して存在する脆弱性か，複数の要因が重なった結果，存在する脆弱性か　例: Resultant
Causal Nature	原因の所在の明確さ 例: Explicit
Common Consequences	攻撃による一般的な影響
Potential Mitigations	脆弱性の緩和策
Demonstrative Examples	脆弱なコード例
Observed Examples	該当する CVE-ID が発行されている脆弱性 例: CVE-2007-5727
Context Notes	当該脆弱性の補足説明
References	参考文献 例: M. Howard and D. LeBlanc. "Writing Secure Code". 2nd Edition. Microsoft. 2003.
Relationships	関連する CWE-ID 一覧 例: CWE-74，CWE-80，CWE-635
Source Taxonomies	その他の分類での呼称 例: PLOVER - Cross-site scripting (XSS)
Applicable Platforms	脆弱性が存在しうるプラットフォーム　例: All，Java，C++
Related Attack Patterns	関連する CAPEC-ID[7]一覧 例: CAPEC-91，CAPEC-19

個々の CWE-ID について，概要や原因，実際に CVE-ID[8]が発行された脆弱性等の情報が記載されている．しかし現時点での最新版 Draft9 では，CWE-ID 毎に記載されている情報量のばらつきが大きく，すべての CWE-ID に記載すべきとされる Context Notes が記載されていないものも多く存在する．

5. IPA での CWE 適用試行

5.1. CWE 適用試行の評価対象

CWE 適用試行の評価対象は，情報セキュリティ早期警戒パートナーシップに基づき，2004 年 7 月から 2008 年 7 月までに IPA が受付・分析した脆弱性関連情報とする．

5.2. CWE 評価結果と NIST との比較

独自に脆弱性を分類している組織が CWE を採用する際に生じうる課題について，IPA の分類を CWE の分類に対応付けした結果と，NIST の NVD に登録されている脆弱性関連情報の CWE の分類を比較すると共に考察する．

(1) IPA の分類と CWE の分類の対応付け

受付・分析したウェブアプリケーションに関する脆弱性関連情報における IPA の独自分類の粒度と，同程度の粒度の CWE の分類に対応付けした結果を表 4 に，その結果を用いて分類した脆弱性関連情報の件数上位 10 位までを図 2 に示す．

表 4: 対応付け結果

ファイルの誤った公開 CWE-538: File and Directory Information Leaks
パス名パラメータの未チェック CWE-36: Absolute Path Traversal
ディレクトリ・トラバーサル CWE-23: Relative Path Traversal
セッション管理の不備 CWE-340: Predictability Problems CWE-384: Session Fixation CWE-592: Authentication Bypass Issues CWE-614: Sensitive Cookie in HTTPS Session Without "Secure" Attribute
SQL インジェクション CWE-89: SQL Injection
DNS 情報の設定不備 CWE-16: Configuration
オープンプロキシ CWE-441: Unintended Proxy/Intermediary
クロスサイト・スクリプティング CWE-79: Cross-site scripting' (XSS)
クロスサイト・リクエスト・フォージェリ CWE-352: Cross-Site Request Forgery (CSRF)
HTTP レスポンス分割 CWE-113: HTTP Response Splitting'
セキュリティ設定の不適切な変更 CWE-272: Least Privilege Violation
リダイレクタの不適切な利用 CWE-601: URL Redirection to Untrusted Site
フィルタリングの回避 CWE-441: Unintended Proxy/Intermediary
OS コマンド・インジェクション CWE-78: Configuration
メールの第三者中継 CWE-472: External Control of Assumed-Immutable Web Parameter CWE-657: Violation of Secure Design Principles
HTTPS の不適切な利用 CWE-326: Weak Encryption CWE-16:　Configuration
価格等の改ざん CWE-472: External Control of Assumed-Immutable Web Parameter

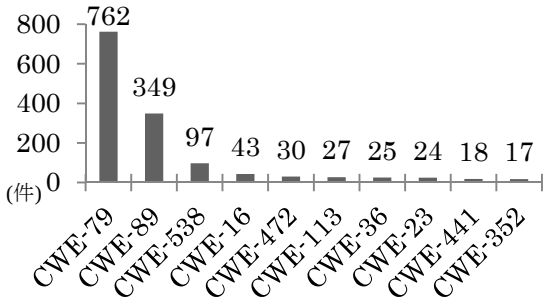

図2: CWEで分類した脆弱性関連情報の件数

IPA 分類の「セッション管理の不備」，「メールの第三者中継」，「HTTPS の不適切な利用」については, 検討した結果, それぞれ複数の CWE-ID が対応付けられるのが妥当であると判断した.

「セッション管理の不備」は, CWE-254: Security Features にまとめることも可能であったが, CWE-254 は，IPA が想定していた脆弱性の範囲よりも広く，抽象的な分類であるため，試行評価ではより具体的な 4 つの CWE-ID を割り当てることが妥当と判断した. また,「メールの第三者中継」および「HTTPS の不適切な利用」については，問題の原因が混在するため，共通する親ノードが存在しない複数の CWE-ID が対応付けられるのが妥当と判断した.

(2) NVD との比較

IPA が受付・分析したウェブアプリケーション, およびソフトウェア製品に関する脆弱性関連情報と，NIST が運営する NVD に登録されている脆弱性関連情報において，情報の収集範囲が重複しているものについて，CWE を用いて比較する．IPA のソフトウェア製品に関する脆弱性関連情報の CWE 分類の対応付けは, NIST の CWE 評価を参考に行った．なお，分類の粒度が異なる場合は共通の親ノードを比較対象とした(表 5).

表 5:NIST と IPA の CWE-ID の比較対象一覧

NIST	IPA（ウェブ）	IPA（製品）
CWE-79	CWE-79	CWE-79
CWE-89	CWE-89	CWE-89
CWE-119	該当なし	CWE-119
CWE-264	該当なし	CWE-264
CWE-20	CWE-113	CWE-20, CWE-93, CWE-113
CWE-22	CWE-23，CWE-36	CWE-22
CWE-200	CWE-538	CWE-200
CWE-352	CWE-352	CWE-352
CWE-16	CWE-16	該当なし

2008 年 7 月末時点で NVD に登録されている脆弱性関連情報のうち, CWE 評価されているものは約 6,000 件ある．IPA は，ウェブアプリケーションに関する脆弱性関連情報約 1400 件, ソフトウェア製品に関する脆弱性関連情報約 500 件について CWE 評価を行った．NIST の CWE 分類の上位 13 位までを図 3 に, NIST と IPA の脆弱性関連情報と比較した結果を図 4 に示す.

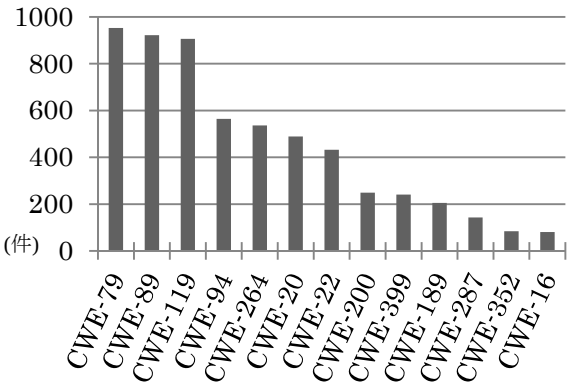

図3 :NISTにおける脆弱性関連情報の件数

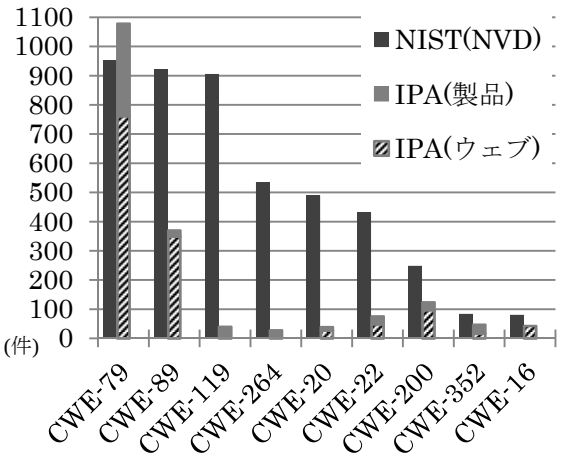

図4 :NISTとIPAの脆弱性関連情報の件数比較

NVD では，CWE-79(XSS)，CWE-89(SQL インジェクション), CWE-119(バッファオーバーフロー), CWE-94(コード・インジェクション)，CWE-264(許可、権限、アクセス制御)，CWE-20(不十分な入力確認)，CWE-22(パス・トラバーサル)，CWE-200(情報漏えい)，CWE-399(リソース管理の問題), CWE-189(数値演算の問題)，CWE-287(不適切な認証)，CWE-352(CSRF)，CWE-16(環境設定)の順となっている。

NVD では上位 3 種類の件数が同程度であるのに対し，IPA のものは，ウェブアプリケーション，ソフトウェア製品共に，クロスサイト・スクリプティングを示す CWE-79 の件数が突出している.

以上のように，共通の脆弱性分類基準として CWE を利用した統計情報を比較した結果, 客観的にそれぞれの傾向の把握が可能になった.

(3) 考察

IPA の分類を CWE の分類に対応付けした際に生じた課題について考察する.

(a) CWE の分類の対応付けにおける課題

IPA の分類と CWE の分類が一対多になるものがいくつか存在した.

IPA では実際に届出があった脆弱性関連情報を基に分類しており，脆弱性の原因で分類しているものと脆弱性を悪用された結果起こり得る問題で分類しているものが混在している．そのため，後者の基準で分類したものについては脆弱性の原因が複数存在しているため, CWE の分類との対応付けが一対多になったと考えられる．今後，独自分類をしている組織が CWE を利用するにあたり，今回の試行評価と同様の問題が発生する可能性がある．対応として，CWE に完全に移行する，もしくは既存の独自分類を残し，その分類に該当する CWE-ID を併記することが考えられる.

(b) CWE 展開にあたっての課題

CWE を展開するにあたり, 次のような課題がある.

- CWE-ID に関する情報の充実

個々の CWE-ID に関する情報の充実が挙げられる．CWE-79 などの特定の脆弱性に対しては非常に詳細な情報が記載されているが, CWE 全体を見ると情報量に偏りがあり，情報が少ない CWE-ID について，分類に相違が生じる可能性がある.

- CWE-ID 対応付けに伴う整合性確保

次に，特定の脆弱性において，分類の範囲を限定させる対応する適切な CWE-ID がない点が挙げられる．例えば，IPA 分類の「DNS 情報の設定不備」が，DNS に限らずソフトウェアの設定の不備全般を表す CWE-16: Configuration としか対応付けられなかった点がある.

CWE は階層構造で脆弱性を分類していることから，抽象的な分類においては問題なく分類することができる．しかし，より具体的に脆弱性分類を示したい場合に，対応する CWE-ID が存在しないことがあるため，対応付けられる CWE-ID の追加の検討が必要になる.

6. おわりに

本稿では，脆弱性分類の基準として CWE に着目し，IPA に実際に報告されたウェブアプリケーションにおける脆弱性関連情報を分類すると共に, CWE の特性と課題について述べた．CWE を脆弱性の分類基準に使用することは有用であると考えるが，課題も残されている．課題については，MITRE 社や CWE を利用している組織との連携を進め解決を図っていきたい.

今後は IPA に届け出られたウェブアプリケーション，およびソフトウェア製品に関する脆弱性関連情報について CWE を試行運用し，CWE を用いて脆弱性を分類した統計情報を，分類基準と共に一般に公開することを検討していく．また，JVN iPedia[9]においても同様に CWE を用いた脆弱性分類を検討する.

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] 情報処理推進機構：脆弱性関連情報に関する届出状況
http://www.ipa.go.jp/security/vuln/index.html
[2] CWE - Common Weakness Enumeration
http://cwe.mitre.org/
[3] SecurityFocus
http://www.securityfocus.com/
[4] OWASP Top Ten Project - OWASP
http://www.owasp.org/index.php/OWASP_Top_Ten_Project
[5] Threat Classification - Web Application Security Consortium
http://www.webappsec.org/projects/threat/
[6] MITRE
http://www.mitre.org/
[7] National Vulnerability Database Home
http://nvd.nist.gov/
[8] CAPEC - Common Attack Pattern Enumeration and Classification
http://capec.mitre.org/
[9] CVE - Common Vulnerabilities and Exposures
http://cve.mitre.org/
[10] JVN iPedia - 脆弱性対策情報データベース
http://jvndb.jvn.jp/