3Z-1

情報システムの脆弱性に対する客観的評価手法の提案

亀谷　直希†　　佐藤　直‡

情報セキュリティ大学院大学　情報セキュリティ研究科†‡

１．はじめに

近年，セキュリティに関するインシデントが数多く報告されており，自組織で管理している情報システムに対する脆弱性評価を行い，セキュリティインシデントを未然に防ぐ取組みが必要である．しかし，最近の情報システムは，複雑な構成で構築されている場合が多いため，評価しづらい側面がある．また，FIRST（CSIRT の世界的な集まりである国際的な非営利団体）が定めた CVSS（共通脆弱性評価システム）が従来から適用されているが，一部，評価者の主観が含まれるという問題がある．

本稿では，上述の問題の解決に向けて，新たな脆弱性評価手法を提案する．

２．ＣＶＳＳを用いた評価

２．１　評価基準

CVSS は，情報システムの脆弱性に対する汎用的な評価手法として公開されており，脆弱性深刻度を定量化することが可能となっている．

また，CVSS には，表 1 のように，3 つの評価基準が設けられている．

表１．CVSS による評価基準

脆弱性評価基準	概要
基本評価基準 (Base Metrics)	リリース時点のソフトウェア製品に対する脆弱性深刻度を評価する．
現状評価基準 (Temporal Metrics)	現時点のソフトウェア製品に対する脆弱性深刻度を評価する．
環境評価基準 (Environmental Metrics)	ソフトウェア製品の利用環境に対する脆弱性深刻度を評価する．

２．２　ＣＶＳＳを用いた評価による課題

表 1 の評価基準ごとに評価値（基本値，現状値，環境値）の算出法が定義されている．

基本値は，情報システムの構成や脆弱性対策状況といった条件によらず一定であるが，現状値，環境値はこれらの条件に依存する．また，両評価値の算出に用いるパラメータの値は，評価者の判断によって決めている．しかし，「二次的被害の可能性」や「攻撃される可能性」といったパラメータを机上で定義するのは困難であり，定義する場合でも，評価者が主観的に決めざるを得ないのが実状である．このように，現状の CVSS 評価法による現状値と環境値は，評価者の主観に左右されやすいため，客観的に評価する方法の開発が必要である．

３．関連研究

原田ら[1],[2]は，CVSS の環境評価基準の中で，主観的要素となり得る，「影響を受ける対象システムの範囲」と「二次的被害の可能性」を，ネットワークモデリング図を用いて評価範囲を客観的に求める手法を提案している．注目すべきは，CWE（Common Weakness Enumeration）と呼ばれる，脆弱性の種類の識別化で整理された情報から，影響範囲を特定している点である．具体的には，ファイル改ざんや情報漏えいなどのサーバ単体のみに影響を及ぼす脆弱性と CPU やメモリなどのサーバ間やネットワーク機器などのシステム全体に影響を及ぼす脆弱性に分けて評価していることが挙げられる．

４．提案評価手法

関連研究の考え方だけでは，全てを客観的に評価することは難しいため，従来の CVSS 評価法を参考にして，脆弱性を客観的に評価する手法を提案する．図 1 に提案手法の概要を示した．本提案の特徴は，評価値の算出に主観的要素を含まないことである．具体的に，提案手法は以下に示す STEP1 から STEP3 の 3 つのステップからなる．

STEP１では，対象システムの脆弱性箇所を調査し，脆弱性を検出する．さらに，脆弱性情報データベースから，検出した脆弱性に対する CVSS 基本値を求める．STEP2 では，対象システムにペネトレーションテストを行い，攻撃成功時間を実測する．ここで，攻撃成功時間とは，攻撃ツール（Metasploit FrameWork[3]など）の選定や攻撃実行までの準備に要する時間（本文

Proposal of objective assessment approach to vulnerability of information systems

† Naoki Kamegai・Institute of Information Security

‡ Naoshi Sato・Institute of Information Security

では１分と定義した）と，攻撃ツールによる攻撃開始から攻撃が成功するまでの時間の和（単位は分）とする．STEP3 は，STEP1 で求めた CVSS 基本値と STEP2 で求めた攻撃成功時間から，式(1)を用いて，実測値を求める．

実測値＝CVSS 基本値×（１／攻撃成功時間）(1)

本文では，この実測値を，現状値及び環境値に変わる評価値とすることを目的とするために，CVSS 評価値のスコア範囲である 0～10 に対して，実測値のスコア範囲も，0～10 となるようにした．例えば，攻撃が成功しない場合は，攻撃成功時間が 0 分であることから，実測値は 0 となる．また，攻撃成功時間に比例して，実測値は小さくなり，実測値の最大値は 10 とすることができる．

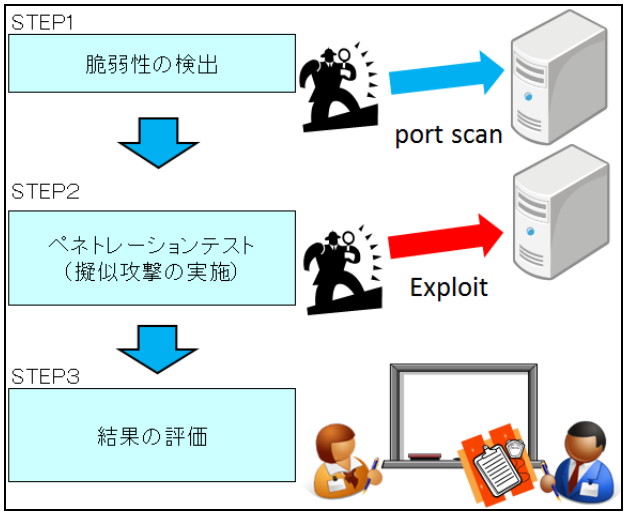

図１．提案手法

５．評価実験

提案手法の妥当性を検証するための評価実験を実施した．評価の対象システムは Web サーバとし，対象システムの OS は，Windows2000，Web 用ソフトウェアは，Apache2.0 とした．ペネトレーションテストには，BackTrack5[4]を使用した．

実験では．STEP1 の脆弱性の検出を行うために，nmap と呼ばれるポートスキャンツールを用いて，対象システムで使用しているソフトウェア製品のバージョン情報を取得した．取得した情報から，脆弱性を特定し，脆弱性情報データベース（NVD）をもとに CVSS 基本値を定めた．次に STEP2 のペネトレーションテストでは，脆弱性に対応する攻撃ツールを，Metasploit FrameWork から選定して実行した．また，攻撃成功時間は，パケットモニタリングツール（Wireshark）やコマンドラインの結果を用いて，通信の確立からツールの実行完了までの時間を測定した．最後に，STEP3 では，STEP1 と STEP2 の結果をもとに，式(1)から実測値を求めた．評価結果の一部を表 2 に示す．同表には参考として，CVSS 現状値も示した．

表 2．実測値と CVSS 現状値のスコア

脆弱性情報	実測値	CVSS 現状値
CVE-2004-0206	0.0	0.0
CVE-2008-4250	9.5	8.7
CVE-2005-1983	9.5	8.7
CVE-2003-0109	7.5	6.5

なお，対象システムに複数の脆弱性が存在し，各脆弱性に対して実測値を定義する場合は，式(2)をもとに，システム全体の評価を行うことが考えられる．

システム全体の実測値＝MAX（実測値 A，実測値 B，実測値 C，・・・）　(2)

６．まとめと今後の課題

情報システムの脆弱性を客観的に評価する手法として，ペネトレーションテストを実施して攻撃成功時間を測定し，CVSS の基本値とこの攻撃成功時間から，脆弱性の実測値を算出する手法を提案した．実際の情報システムは，サーバ単体で動くことはなく，ネットワーク機器を含めた環境で動作することから，今後は，ネットワーク環境も含めた形での評価法を検討する．

参考文献

[1] 原田敏樹，金岡晃，岡本英司，加藤雅彦，CVSS を用いたネットワークシステムの危険度測定手法の検討，電子情報通信学会技術研究報告 SITE，Vol. 109，No .114，pp.189-194，2009-06-25

[2] 原田敏樹，金岡晃，岡本英司，加藤雅彦，ネットワークシステムにおける CVSS を用いた脆弱性影響範囲特定手法の検討，電子情報通信学会論文，Vol. 109，No.285，pp.1-6，2009-11-06

[3] David Kennedy ほか，実践 Metasploit-ペネトレーションテストによる脆弱性評価，岡真由美(訳)，オライリー ジャパン，Tokyo，2012-05-22

[4] BackTrack Linux - Penetration Testing Distribution，http://www.backtrack-linux.org/ ，2013-11-06