5E-05

コンピュータセキュリティ対策におけるサーバ管理者向けスコアリング手法の試作

田島　浩一，岸場　清悟，近堂　徹，大東　俊博，
岩田　則和，西村　浩二，相原　玲二 †

広島大学 情報メディア教育研究センター †

1. はじめに

インターネットにおけるセキュリティ動向として，2014 年版情報セキュリティ 10 大脅威[1] では，近年のクライアント OS 用アプリケーションの脆弱性による脅威がランキングの半数を占める一方，WEB サーバをはじめとするサーバ利用されるホストの脆弱性も主要な脅威とされており，WEB サーバの例ではサーバソフト自体や設定の不備による脆弱性，コンテンツ管理に用いるデータベースソフト等 WEB アプリケーションに関連する脆弱性への注意喚起が公表されている．

広島大学では，著者らの所属する情報メディア教育研究センターにおいてキャンパスネットワークのセキュリティ対策の一環として，脆弱性診断を実施しており，診断結果をそれぞれのホストの管理者（主にサーバ管理者）に通知し対策を依頼している[2]．ここで，脆弱性診断を実施の目的は，診断により存在する脆弱性をより正確に確認する事と合わせて，見つかった脆弱性に対して対策が行われなければキャンパスネットワークのセキュリティ対策の向上は図れない．そこで本研究では，本学で行っている脆弱性診断の実施環境において，対策の基となる診断結果に評価点を設定表示し，対策の優先度を示す事および診断漏れによる未対策ホストの放置等について診断されるサーバ管理者向けの提供方法についての試作を行った．

2. 診断結果への評価点の設定

脆弱性診断の結果において，見つかった脆弱性がどの程度の危険性であるのかを評価する指数として，永安ら IPA（独立行政法人 情報処理推進機構）により CVSS 値[3]が評価および検証されその妥当性等がまとめられている[4]．本学で脆弱性診断に用いているソフトウェア NESSUS[5]は，この CVSS 値への対応として NIST (National Institute of Standards and Technology) により提供されている CVSS v2 に対応しており，この値を主に指標として用いる．

2.1. CVSS 値の利用

CVSS では，対象となる脆弱性を次の３つの指数により評価し指数化されている．

１）**Base Metrics 値**（基本評価基準値）
脆弱性の発見時に設定される値であり，リモートからの攻撃可否など脆弱性の攻撃利用の容易さや，破壊や漏洩，サービス妨害等受ける被害範囲より算出される固定値．

２）**Temporal Metrics 値**（現状評価基準値）
実証コードや攻撃ツール，脆弱性を利用するウィルス等の公開や流通の有無等の攻撃環境と，回避のための設定の容易さや修正プログラムの公開の有無など，環境の変化に伴い変更される．

３）**Environmental Metrics 値**（環境評価基準）
脆弱性の悪用により，生じる被害について評価で，利用者が独自に評価し値を設定する．

2.2. 評価値の提供

キャンパスネットワークの運用方針として，ホストの接続には管理者の設定を必須としており，管理者不在時の備えとして可能な限り副管理者も設ける事を推奨しており，表１のホスト数および管理者数は 2014 年 12 月時点の登録数で，管理者数は重複を除外した実数である．

管理者が診断結果へのアクセスページに認証を経てアクセスし，表示される管理ホストの一覧の画面例を図１に示す．ホスト毎に診断結果より出力される CVSS 値により，0～3.9/状態:良好/緑色表示，4.0～6.9/状態:警告(Security Warning)/黄色表示，7.0～9.9/状態:危険

Trial of creating a scoring method in computer security measures for server administrator

† Kouichi TASHIMA, Seigo KISHIBA, Tohru KONDO, Toshihiro OHIGASHI, Norikazu IWATA, Kouji NISHIMURA, and Reiji AIBARA
Information Media Center, Hiroshima University
4-2, Kagamiyama 1chome, HigashiHiroshima,739-8526, JAPAN
{ tashima, kishiba, tkondo, ohigashi, norita, kouji, ray }@hiroshima-u.ac.jp

図 1　診断結果へのアクセスページ

表 1　脆弱性診断の対象ゾーン

ゾーン 略称	グローバルゾーン・ゾーン A
主用途	学外向けサーバ接続
IP アドレス	固定グローバル IP アドレス
ホストの接続	MAC アドレス登録と MAC 認証
登録数	450 台
実管理者数	201 名

(Security Hole)/赤色表示，10.0/状態:緊急/赤色表示と合わせてホスト名の赤色表示とした．診断ソフトより出力される脆弱性の原因等や対策例は，このページの各枠内のリンクより別画面に詳細表示され，CVSS 値 7.0 以上の危険または緊急の状態をサーバ管理者の対策により回避を促すため，診断結果の中で優先して対策すべき項目の強調表示や，どの対策を完了すると現在の状態（赤色表示から黄色表示への遷移など）からより CVSS 値の低い状態になるのかについて表示される．また，CVSS 値 10 点等で JPCERT/CC からの緊急対策が出ている件については，診断結果の通知と合わせて別途に個別の緊急対策依頼を送信する対応を予定している．

また，診断日に電源が入っておらず診断できていないなどで未診断状態が継続する場合に，CVSS 値の本来の表示値より 1 段高い表示色で診断を促し，次回の定期的な診断を待たずに管理者に提供している自身で操作して管理ホストを診断する機能の利用に誘導し確認を促す．

集計に用いる CVSS 値は，診断結果より脆弱性管理 ID で同一の脆弱性を排除して集計し，それぞれに対応する CVSS 値を集計する．サーバ管理者に実施してほしい対策について，対策が必要な分量ホスト毎の評価合計点とし，各ホストにおける対策の優先度を各要素点として提示する事とし，CVSS 値 7 未満のホストの場合は下限 50 点とした 100-CVSS 値の合計とし，7 以上のホストは下限を 0 点とした 50-CVSS 値の合計で評価点を集計する．

3. まとめ

本研究で試作した評価値は，試作段階であり今後学内での運用評価を行う予定であるが，学内の管理者等により実利用されるため，情報提供や環境の運用している環境での変更であるため，事前段階として著者らの所属する情報センター内のシステム管理者により評価中である．

謝辞

脆弱性診断に関する運用やユーザ対応等について日頃から尽力いただいている情報メディア教育研究センターの関係者に感謝いたします．また，本研究は日本学術振興会科学研究費補助金課題番号(23500089，24300025)の支援を受けて実施しています．ここに記して謝意を表します．

参考文献

[1] 大森,中西,棚町,「独立行政法人情報処理推進機構(IPA)：2014 年版情報セキュリティ 10 大脅威」,独立行政法人情報処理推進機構,2014 年
[2] 田島,岸場,近堂,大東,岩田,西村,相原,「広島大学におけるセキュリティ脆弱性診断の実施とその評価」,学術情報処理研究，vol.18,pp.16-23，2014 年
[3] CVSS (Common Vulnerability Scoring System)，http://www.first.org/cvss
[4] 永安,谷口,相馬,寺田,山岸,小林,「共通脆弱性評価システム CVSS の現状と今後」,暗号と情報セキュリティシンポジウム SCIS2008,2008 年
[5] Tenable Network Security 社 Nessus: Vulnerability Scanner, http://www.tenable.com/products/nessus