「マルチメディア，分散，協調とモバイル
(DICOMO2017)シンポジウム」 平成29年6月

脆弱性診断と脆弱性情報公開サイトを用いた脆弱性更新通知機能の試作

田島 浩一，岸場 清悟，近堂 徹，渡邉 英伸，
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

概要： 各種のソフトウェアにおける脆弱性の情報は，新しい情報や追加情報の更新等が日々行われ続けている．組織のネットワークを管理する，システム管理者の立場からは，公開される脆弱性情報について「深刻度の高い脆弱性に該当するサーバやホストが自組織にあるかどうか」の情報確認の要求があり，また，ホスト管理を行う者にとっても，同様に自身の管理するホストに関係する脆弱性情報が適宜に届く事が望ましいと考えられる．他方，脆弱性診断を行う事で，ホストの脆弱性を見つける過程でホストで稼働させているサーバソフトの検出やそのバージョン等の基本的な情報を得る事も出来ているため，その情報を基に新しく公開された脆弱性情報について，利用中のサーバソフトであるか，また，バージョン等が該当するかの判定は，比較的複雑ではないテキストの比較処理により可能である．そこで本論文では，公開される脆弱性情報について，該当の有無の確認により重要な更新情報を自動通知する方法について，ホストの管理者，および，システム管理者への通知処理について必要機能の試作を行った．

Trial of Vulnerability Reporting Service using Security Vulnerability Check and Vulnerability Database WEB site.

Kouichi TASHIMA， Seigo KISHIBA， Tohru KONDO， Hidenobu WATANABE
Norikazu IWATA， Kouji NISHIMURA， Reiji AIBARA

Information Media Center, Hiroshima University

1. はじめに

サーバソフトやその設定の誤り等による各種の情報システムの脆弱性への対策は，現在でもシステムの安定運用には不可欠であり，脆弱性を悪用したウィルスやワーム，不正アクセス等の危険性は継続しており，インターネットにおけるセキュリティの動向例として，毎年発行される情報セキュリティ 10 大脅威 [1] においても，WEB サーバをはじめとするサーバソフトへの脅威や注意喚起は継続して出されて続けている．

この様な状況から，著者らの所属する広島大学においても，情報センターにおいてこれまでに脆弱性診断ソフトを用いて学内ホストや部局ネットワークの診断を行い，各部局やホストの管理者へ対策に求めてきた．ここで脆弱性診断を用いたセキュリティ対策のサイクルとして診断の実施と通知と各管理者の対策をほぼ毎月 1 回の実行間隔で継続している[2].

他方，脆弱性情報は JP-CERT より発行される Weekly -Report 等に毎週新規の情報が追加されるほか，脆弱性情報の受け付けや管理，情報公開等を合わせて行う国内国外の WEB サイト等も運用され，それられでは日々更新されているのが現状である．これらの脆弱性情報の公開については，組織のシステム管理者の立場から「学内で稼働中のサーバソフト等で深刻度（被害や影響）の高い脆弱性に該当する情報公開があった際に，対象ホストが自組織にあるかどうか」を確認したいといった要求や，ホストの管理者の立場としては，脆弱性情報のうち自身に関係する重要な情報が適宜に届く事が望ましい．そこで本論文では，これら重要な情報に該当し脆弱性診断により検出可能な事項について，以降の構成で情報の抽出と収集を行い該当するホスト管理者，および，システム管理者への通知処理の試作を行った．

2. 脆弱性情報公開サイトからの情報収集

脆弱性情報の公開は，取り扱う情報の性質により多くの場合，脆弱性対策に必要な修正プログラムやアップデート等の準備完了後となる場合が多い．このうち主要なサイトである NVD（National Vulnerability Database）[3]で公開される情報には，情報セキュリティに関する設定の共通化手順：SCAP [4]で採用されている共通脆弱性識別子 CVE[5]やタイトル（名称），脆弱性の内容，脆弱性の深刻度（SCAP

の 10 点評価による CVSS 値），等と合わせ SCAP の CPE（Common Platform Enumeration）形式で該当するソフトウェアの名称とバージョン番号が，プログラム等による機械処理が可能な書式で公開される．さらにこれらの情報は，公開後にもアップデート方法等の追加や更新，攻撃の流行等による深刻度の変化など情報の追加や更新等が行われる．

同様に JVN（Japan Vulnerability Notes）[6] では，国内で利用されるソフトウェア等の脆弱性情報について，日本語での利用も可能な WEB サイトも公開されている．

これら主要な 2 箇所の脆弱性情報の WEB サイトでは，脆弱性情報がデータベース化されており，WEB インタフェースより検索等の参照が可能である事と合わせて，DB そのものの一括ダウンロードによる提供も行われている．

3. 脆弱性診断からのサーバソフト情報等の抽出

脆弱性診断は，一般的に次の様な工程で行われる．

＃１ホスト，サービスの検出　PING / ポートスキャン等での応答確認によるポートの状態やホストで稼働させているサービスの検出

＃２バージョン及び設定等の検出　ホストの OS，サービスやサーバソフトの種別，バージョン等の設定検出や確認

＃３検出内容の脆弱性判定　個々の検出について脆弱性の有無の判定を行い，診断結果を生成し出力する

ここで，診断結果には脆弱性が見つかったサーバソフトとそのバージョン情報等と合わせて，脆弱性が見つからなかった場合の情報も，脆弱性の警告ではないものの「関連情報として診断結果に出力可能」な場合が多く，本実装で用いた脆弱性診断用ソフトウェア NESSUS [7]も参考情報として Security Note のタグ付けで出力可能でありこの機能を利用した．

4. システム構成

システム全体の処理概要を図 1 に示す．本稿における機能実装を行った「脆弱性情報通知システム」以外に，外部の脆弱性情報 WEB サイトからの情報収集，及び，動作させるために連携の必要な関連システムについて，以下に列挙する．

4.1 システム構成と構成要素

ネットワーク管理システム　キャンパスネットワークの管理システムであり，キャンパスネットワークの運用にあわせて構築および順次機能整備しながら利用している既設システム [8]．このシステムでホストの登録情報の変更や管理者登録や変更等の手続きや更新管理を行っており，内部データベースに保存されている．あわせて，キャンパスネットワークに接続するホスト毎に，ＩＰアドレス，ＭＡＣアドレス，管理者のＩＤ，連絡先等キャンパスネットワークの運用に必要な情報を一元管理されている．

脆弱性診断システム　脆弱性診断の実行および診断結果の生成等，学内向けに実施している脆弱性診断用に運用しているシステムであり，を稼働させるとともに診断結果の生成，管理，提示用など運用に必要な機能の作りこみ等を行って運用中のシステムである．

脆弱性情報通知システム　連携するシステムから収集構成される 2 件の DB を基に，1 日 1 回の頻度で DB の更新確認および更新があった際の通知の生成を行う．後述するシステムの動作により生成される通知文の生成や保存，管理者への WEB インタフェースによる過去の通知の閲覧等の機能の実装を行った．

4.2 システムの処理概要

以降の説明等，本システムの構成で用いた主なソフトとそのバージョンを表 1 に示す．実際に通知を受け取り必要な対策を実行する事を考慮して，通知は 1 日 1 回まとめて行う事とし，図 1 の①～③の処理を行う．

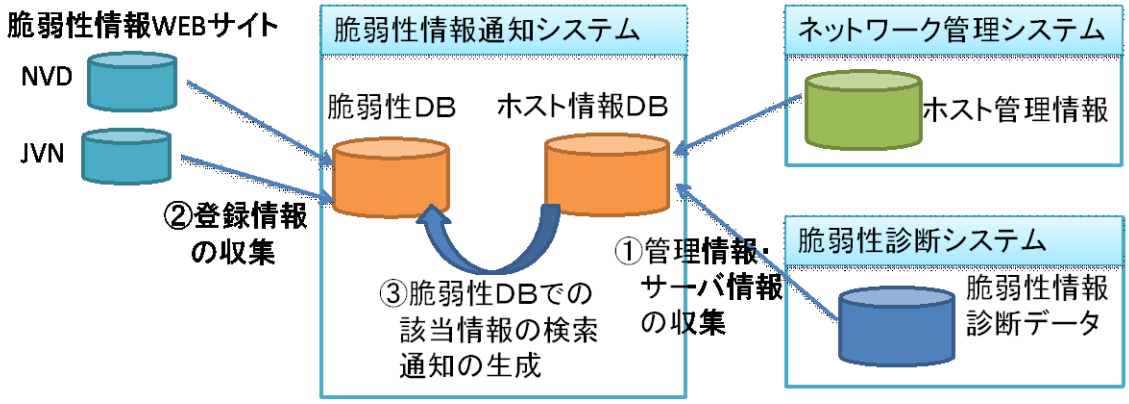

図 1　システム構成と処理概要

表 1　実装に用いたサーバソフト

用途	名称とバージョン
脆弱性診断用	NESSUS ver 6.9.1
脆弱性情報 WEB サイトの DB ダウンロード	vuls v0.1.0

①の処理では，ホストの管理者変更や追加修正，および，ホストの管理者によりオンデマンドで脆弱性診断が可能な状態としている事からホスト毎の管理情報として，ホスト管理システムより，ホストの IP アドレス，管理者 ID，ホストの情報（登録時のホスト名等の情報），登録されている MAC アドレス等のホストの識別情報としてホスト情報 DB に登録する．あわせて登録した各ホストについて，脆弱性診断システムより，CPE 表示（表 2 の例の cpe_name 文字列の例の表記）でのソフトウェアの製造元，名称，バージョン，と合わせて稼働ポート番号とセットでホスト情報 DB に登録を行う．

②の処理では，脆弱性情報 WEB サイトからの DB のダウンロードには，本来脆弱性診断ソフトとして公開されている vuls [9]を用いる．この診断ソフトには，NVD および JVN からの DB の一括ダウンロード機能，および，脆弱性 DB として SQL 形式の DB に登録する機能有し，同様の機能が必要となるためこの機能を用いる事とした．

③ホスト情報 DB に登録されている各ソフトウェア（主にサーバソフト）について CPE の書式による文字列一致の判定を行う． CPE 表記での文字列比較による判定の例として，drupal 8.2.x 系の脆弱性の例 CVE-2017-6379 に該当するバージョンをリスト形式で表 2 に示す．

表 2　CVE-2017-6379 の判定のためのバージョン表示例

vender	product	ver	update	cpe_name
drupal	drupal	8.2.0		cpe:/a:drupal:drupal:8.2.0
drupal	drupal	8.2.0	beta1	cpe:/a:drupal:drupal:8.2.0:beta1
drupal	drupal	8.2.0	beta2	cpe:/a:drupal:drupal:8.2.0:beta2
drupal	drupal	8.2.0	beta3	cpe:/a:drupal:drupal:8.2.0:beta3
drupal	drupal	8.2.0	rc1	cpe:/a:drupal:drupal:8.2.0:rc1
drupal	drupal	8.2.0	rc2	cpe:/a:drupal:drupal:8.2.0:rc2
drupal	drupal	8.2.1		cpe:/a:drupal:drupal:8.2.1
drupal	drupal	8.2.2		cpe:/a:drupal:drupal:8.2.2
drupal	drupal	8.2.3		cpe:/a:drupal:drupal:8.2.3
drupal	drupal	8.2.4		cpe:/a:drupal:drupal:8.2.4
drupal	drupal	8.2.5		cpe:/a:drupal:drupal:8.2.5
drupal	drupal	8.2.6		cpe:/a:drupal:drupal:8.2.6

表 2 の通り比較する文字列の対象として，drupal 8.2.x 系該当する場合には，drupal の各バージョン表記の全てが含まれる形式で，cpe_name の文字列の通り公開され取得できる．以降の処理では，比較による一致で該当が見つかった場合，続く 4.2 節の通知の判定および通知文の生成を行う．

4.3 通知文の生成

CPE の該当判定により，該当する事が確認されると以下の生成手順を実行する．

１）脆弱性の危険度判定と通知の必要性の確認

公開される脆弱性の危険性の度合いとして，永安ら IPA（独立行政法人 情報処理推進機構）により CVSS 値[10]の利用が評価および検証されその妥当性等がまとめられており[11]，現在では広く利用されており本実装でもこれを用いる．CVSS 値では，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が，本実装では「Base Metrics 値（基本評価基準 値）」を用いる．この値，脆弱性の発見時に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求められ，また，固定値である事から継続して利用しやすい事も理由である．具体的な CVSS 値により，分類とタグ付けは， 0.0～3.9　危険度が低いため通知から除外，4.0～6.9 「警告」のタグ付けし表示する，7.0～9.9 「危険」と，10.0「緊急」も同様である．

２）通知本文の生成

表 3 に通知に表示する脆弱性情報の説明表示例を示す．ホスト管理者向け通知には JVN の説明を優先とし，NVD と JVN に同じ脆弱性の掲載がある場合は，日本語表記の説明文を用いる事とした．

表 3　NVD と JVN の CVE-2017-5487 の脆弱性情報の表示例

NVD	wp-includes/rest-api/endpoints/class-wp-rest-users-controller.php in the REST API implementation in WordPress 4.7 before 4.7.1 does not properly restrict listings of post authors, which allows remote attackers to obtain sensitive information via a wp-json/wp/v2/users request.
JVN	WordPress の REST API の実装の wp-includes/rest-api/endpoints/class-wp-rest-users-controller.php は，投稿作成者のリストを適切に制限しないため，重要な情報を取得される脆弱性が存在します．

また，本文の生成時には，メール送信による通知と合わせ，これまでの通知一覧表示の確認を可能とするため，脆弱性診断の結果閲覧用に用意しているＷＥＢサーバに，脆弱性診断と同様にホスト管理者のＩＤによる認証を経ての確認するＷＥＢページにリスト形式でファイルとしても生成する．

4.4 処理実行例

学内で定期実施中の脆弱性診断で，2017 年 4 月 19 日に実行した診断結果より対象とした処理結果の概要を表 4 に示す.

表 4　処理結果の例（2017/04/19）

診断対象	
診断対象 IP 数	1370
対象管理者数	207
診断結果	
サーバソフト等の検出数	261
判定結果の一致数	694

診断実施日の時点で，診断対象は管理者の実数 207 名，IP アドレス数は 1370 台（複数の IP のホストを 1 人管理者が管理している場合が多いため管理者数＜IP アドレス数となっている）. 診断結果より検出された稼働中のサーバソフト数は 261 件の情報は，図 1 の脆弱性 DB に登録され，同じく図 1 の③の脆弱性 DB への該当有無の判定には約 20 秒の処理時間を要し，結果として比較により一致した数は 694 件あり，ホスト毎の一致数の最大は 17 件（＝17 件のアップデート通知）であった.

5. まとめ

本稿では，脆弱性情報公開サイトに日々公開される脆弱性情報について，脆弱性に該当するサーバソフトの利用者にその脆弱性情報を通知する手法として脆弱性診断を用い，診断過程で収集されるサーバソフトの情報を基に，サーバソフトの稼働状況を把握し，公開された脆弱性情報への該当の有無を CPE を用いて判定し確認する方法について示した．また，広島大学で実施している学内ホストを対象とした脆弱性診断の環境に適用し，処理数および判定に要する処理時間についての確認を行った．4.3 節の処理結果例よりホストの管理者が受け取る通知数に比べて，全体の通知を受け取る著者らを含むシステム管理者にとって，約 700 件の通知はすべての閲覧確認は困難な結果であったが，CVSS 値による緊急度のタグ付けにより優先度をつけて確認する事可能であった.

謝辞

本学におけるセキュリティ脆弱性診断の実施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，本研究およびシステム構成の主要設備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] 土屋正，辻博郷，亀山友彦，他，独立行政法人情報処理推進機構(IPA)：2017年版情報セキュリティ10大脅威，2017年3月30日
[2] 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] WEBサイト, “National Vulnerability Database”, https://nvd.nist.gov/ , 2017/05/10確認
[4] David Waltermire, Stephen Quinn, Karen Scarfone, Adam Halbardier, “The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2”，アメリカ国立標準技術研究所, NIST SP 800-126, 2012
[5] WEBサイト, “Common Vulnerabilities and Exposures”, http://cve.mitre.org/ , 2017/05/10確認
[6] WEBサイト, “Japan Vulnerability Notes”, https://jvn.jp/ , 2017/05/10確認
[7] Tenable Network Security社 Nessus: Vulnerability Scanner, http://www.tenable.com/products/nessus
[8] 近堂徹，田島浩一，岸場清悟，大東俊博，岩田則和，西村浩二，相原玲二，利用者認証機能を備えた大規模キャンパスネットワークの性能評価，第1回IOTシンポジウム2008論文集，pp．121～128，2008
[9] WEBサイト, “github　vuls”, https://github.com/future-architect/vuls , 2017/05/10確認
[10] WEBサイト，” Common Vulnerability Scoring System (CVSS-SIG)”，https://www.first.org/cvss ， 2017/05/10確認
[11] 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