「マルチメディア，分散，協調とモバイル
(DICOMO2013)シンポジウム」 平成25年7月

脆弱性診断ツールの連携動作による セキュリティ診断システムの構築

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†

各種のサーバソフトをはじめとするソフトウェアの不具合等によるシステムの脆弱性と,それを利用した不正アクセスの危険性は現在でも続いており，特に近年では WEB サービスを提供する WEB サーバ自体の脆弱性をはじめとし，組み込まれる開発環境等フレームワークやミドルウェア，利用される多様なスクリプト言語，データベース等にもアップデート注意喚起が報告されている.
著者らの組織では商用のセキュリティ診断ソフトを用いて脆弱性診断を実施しているものの,既に公開されている脆弱性であっても診断時に全てを必ず検出可能ではない.
そこで本報告では,脆弱性情報の公開と合わせて公開される確認方法や確認可能なオープンソースのソフトも利用し，脆弱性診断が可能な複数の診断ツールが有効に機能する診断システムとして構成し，診断により検出した項目について追加で他の診断ソフトを自動実行する事を可能とする試作構した成例等について報告する.

Construction of Computer Security Management System Using Cooperation of Multiple Vulnerability Checker Tools

KOUICHI TASHIMA† SEIGO KISHIBA† TOHRU KONDO† TOSHIHIRO OHIGASHI† NORIKAZU IWATA† KOUJI NISHIMURA† REIJI AIBARA†

1. はじめに

各種サーバソフトをはじめとする，ソフトウェアの不具合や設定の間違い等による各種の情報システムの脆弱性を利用した不正アクセスやウィルスやワーム等の危険性は継続しており，インターネットセキュリティの動向報告例として, 近年の SANS (SysAdmin, Audit, Network, Security) Institute Top20 Security Risks では, クライアントで動作するブラウザその組み込み機能やオフィス製品等の脆弱性が脅威としてのランキングの上位であるものの，各種のサーバ側の脆弱性では WEB アプリケーションが 1 位とされている[1]. WEB アプリケーションにおける脆弱性の原因は，WEB サーバ自体の脆弱性をはじめとして，WEB サーバに組み込まれる開発環境やミドルウェア，そこで利用される多様なスクリプト言語，データベース等にも脆弱性の注意喚起が報告されている.

ネットワークの管理におけるセキュリティ対策として，ネットワークに接続している情報システム等の脆弱性を診断により発見し，それを改善することでセキュリティレベルの維持や向上が期待できる事は広く知られており，セキュリティ脆弱性の診断を行う診断ソフトウェア(以下では診断ツールとよぶ)としての提供や診断実行のサービスにより利用可能である.診断ソフトウェアを導入する場合は，構築や維持コストは必要であるが，頻度を問わずに組織内で繰り返し実施する事や，組織ネットワークの更新や構成変更時に柔軟に適用する事が可能など，定常的に利用するには診断システムを導入するメリットは大きい[2-5].

広島大学においても，平成 14 年度に脆弱性診断システムを学内に構築し，学内のホストを対象とした定期的なセキュリティ診断を開始し, 現在も継続中である[2]. その後，診断結果を受け取る学内の部局等の部分ネットワークの管理者が，診断結果対して実施した対策の確認や，不定期なシステム導入時などの臨時利用を目的として，学内の認証基盤による認証後に管理を担当するアドレス範囲の診断をオンデマンドに実行できる「診断支援システム」の試作およびその運用を行っている[2，4，5].

さらに，複数の診断ツールを用いて診断システムの拡張[6]を行う事で，これまでにより多様な脆弱性に対応して利用していたが，診断すべき項目が診断で検出されていない事が診断時のログ等で確認されていた．また，近年に特に WEB アプリケーションに限定した診断機能を持つ診断ツールがいくつも公開されているため，本論文ではこれら複数の診断ツールにより WEB アプリケーションをより網羅的に診断が可能となる構成について，試作した診断システムについて構築例等について報告する.

†広島大学 情報メディア教育研究センター
Information Media Center, Hiroshima University

2. 診断ツールの機能と利用

2.1 診断ツールの機能

商用の診断ツールの多くは，１つの診断ツールで Linux や Windows 等の各種 OS のコンピュータやネットワーク接続で利用するストレージ, ネットワーク機器などに対応し，また，OS に依存する脆弱性や各種サーバソフトの設定の脆弱性等の診断が可能な統合型の診断ツールとして構成されている．他方，特定の診断に特化した診断ツールには，WEB サーバの診断のみが可能な Nikto2[7]をはじめとして，脆弱性による攻撃手法の公開後にその確認する事に対応し機能を絞った特定の診断型の診断ツールとしては，SQL インジェクション検査用の SQLiX[8]ならびに DNS キャッシュポイゾニングのチェックツール[9]，WEB サイトで主にコンテンツ管理システム（CMS）で利用されている画像のサムネール作成機能の脆弱性確認用として公開された TimThumb Vulnerability Scanner[10]など，危険度の高い脆弱性情報が公開された際にいち早くこの脆弱性のみを診断できるツールもたびたび公開されている．

統合型の診断ツールでは，そのツールを実行する事で診断が完了する様に構成されており，診断対象のホストの存在確認やポートスキャンによりホストで稼働しているサービスの検出, 診断結果をファイル等に生成する事ができる．他方，個別の診断に特化したツールでは，診断機能のみが用意され，診断の実行管理や診断対象の検出機能を省略しているものや，診断結果の提供様式も規格化された形式とは限らない．

2.2 診断ツールの利用

ネットワークの管理方法において管理者を設定してホスト単位での接続管理を行う場合や，ネットワークを分割委譲して管理を委託する場合では，脆弱性診断の実施はそれら管理者が本来は管理作業として行う事が通常と考えられるため，個別型診断ツールの多くはその様な管理者が手動で操作実行する様に構成されているものが多い．

例えば WEB アプリケーションを個別型診断ツールで調査する場合は管理者がインストールや機能を有効にさせている項目等を把握していると考えられるため，調査すべき URL や項目の指定を実行時に診断対象として指定する利用が想定される．

2.3 診断ツールの複数の組み合わせ利用

個別の診断に特化した診断ツールは，各製造元やプロジェクト毎に目的を限定して早期に開発提供されるという配布形態からも，基本的に単独の診断ツールとして動作する事が可能なように構成されている．これは逆に考えると，ツール単独での動作が基本であるため，複数の診断ツール間で相互に動作や連動するような利用は想定されておらずそのような機能も用意されていない場合が多い．

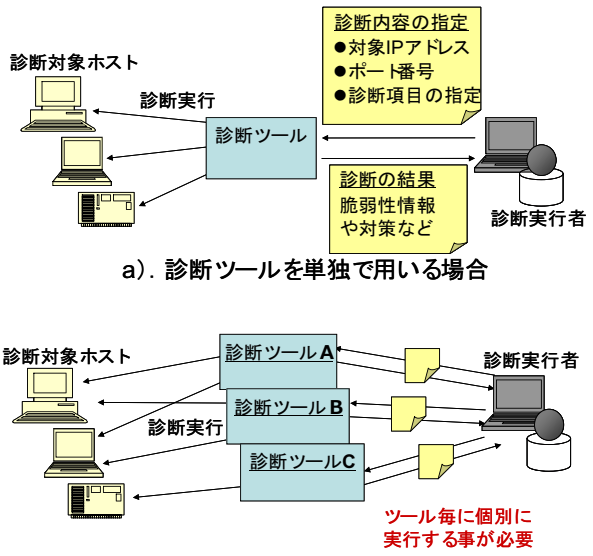

図１　診断ツールの利用イメージ

Figure 1 Example of the Usage of Multiple Security Check tools

図１に複数の診断ツールを利用する場合の診断ツールの実行イメージを示す．図１a)では１つの診断ツールを利用する場合に，その診断ツールの指定する実施方法を確認しコマンドラインの実行引数等診断ツールに用意されている実行様式で利用される．個別の診断ツールを複数利用する図１b)の場合には，さらにそれぞれの診断ツール毎に異なる操作実行が必要となるため，診断が有効である事が分かっていても診断実行に要する手間が問題となり，管理者毎にその様な診断利用が行われる事を期待する事は難しいと考えられる．

このような理由から，本論文での実装方法では個々の診断ツールの実行を管理プログラムから起動する構成とし，診断の実行者からは単独の診断と同様の手続きで診断が行える事とし，図２にその利用イメージを示す．実際の個別

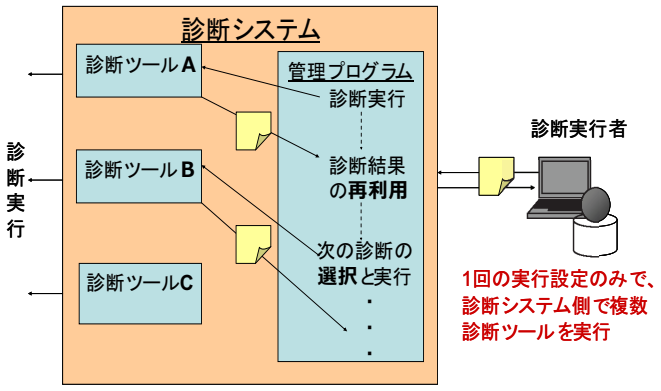

図２　複数の診断ツールの連携動作での利用イメージ

Figure 2　Example of the Cooperating Usage of Multiple Security Check Tools

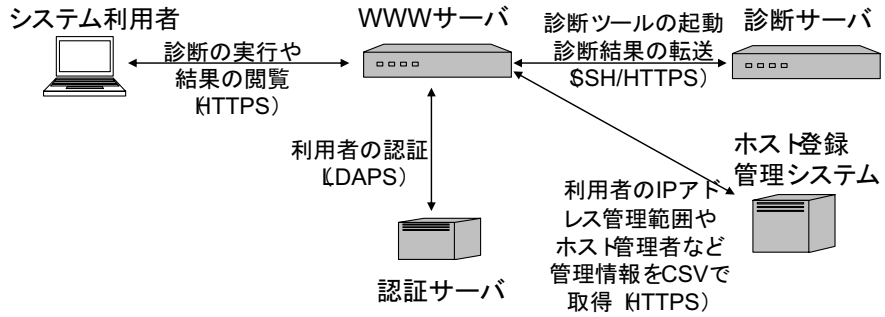

図３　診断システムのサーバ構成

Figure 3　Server Configuration of Security Check System

の診断ツールの実行と診断結果の統合処理は，診断システム内の管理プログラムより個々の診断ツールが連携動作する様に行い，診断実行者は診断システムを１つの診断ツールとして利用し診断を行う．

3. システム構成

3.1 サーバ構成

図３に実装した診断システムの全体構成を示す．構成で用いた既設のサーバなど各種のサーバはそれぞれ以下の機能を持ち，脆弱性情報の伝送等と行うため診断システムと各サーバ間の通信路等は暗号化を用いる構成としている．

WWW サーバ　システム利用者による ID/パスワード認証利用と脆弱性情報の閲覧に用いられるためサーバ証明書を備える必要がある．そのため著者の所属する情報センターで運用されている各種の WEB サービス提供に用いられているサーバを利用した．

診断サーバ　実際の診断を行うサーバであり，本論文で用いた各種の診断ツールをインストールして構成し，学内の複数の異なるネットワークへの定期的な診断等にも利用するため複数のネットワークインタフェースで複数の学内の IP アドレス，および，学外の IP アドレスとして商用プロバイダの IP アドレス等複数のネットワーク接続を備え，診断方法により異なる経路で学内のホストの診断を行う．

認証サーバ　ネットワークの認証利用をはじめとする全ての構成員の ID が登録されている既設の認証サーバで，学内の各種情報サービスでの認証に用いられる認証システム．

ホスト登録管理システム　キャンパスネットワークの利用申請や管理を行う既設の管理用のサーバで，ネットワークでの接続（サブネット接続）についてはネットワーク管理者やその管理するアドレスの範囲などが，ホスト単位での接続ではそのホストの管理者等の管理情報を内部 DB に保存している．

3.2 診断サーバのシステム構成

診断サーバに設定し診断に用いる診断ツールを表１に示す．各診断ツールは，検出した脆弱性情報をテキスト出

表　1　使用した診断ツール

Table　1　Used Security Check Tools.

名称/バージョン	機能	BID	CVE	OSVBD
NESSUS[11] / 5.0.1	統合型の診断ツールで診断実行以外に HTML 形式で全体の警告数の集計やホスト毎の集計など診断結果の整形に利用	○	○	○
Nikto2 / 2.1.5	WEB アプリや WEB サーバの設定確認やアクセス統計 WEB 管理システムなど WEB を利用した管理ソフト診断に利用	○	○	○
CMS-Explorer[12] / 1.0	主要な CMS 本体およびそのプラグインインストールや設定状況等の診断機能を持つ	×	×	○
Whatweb [13] / 0.4.7	WEB サーバ本体および組み込まれている機能や有効な設定等を確認可能	×	○	×
NMAP[14] / 4.11	ポートスキャンによるサービスの検出に利用. ポートスキャンに特化されスキャンが早く，OS 検出も可能	−	−	−
wget / 1.12	本来は診断ツールではないが，診断結果で警告対象となった URL の記録および検証用として取得保存に利用	−	−	−

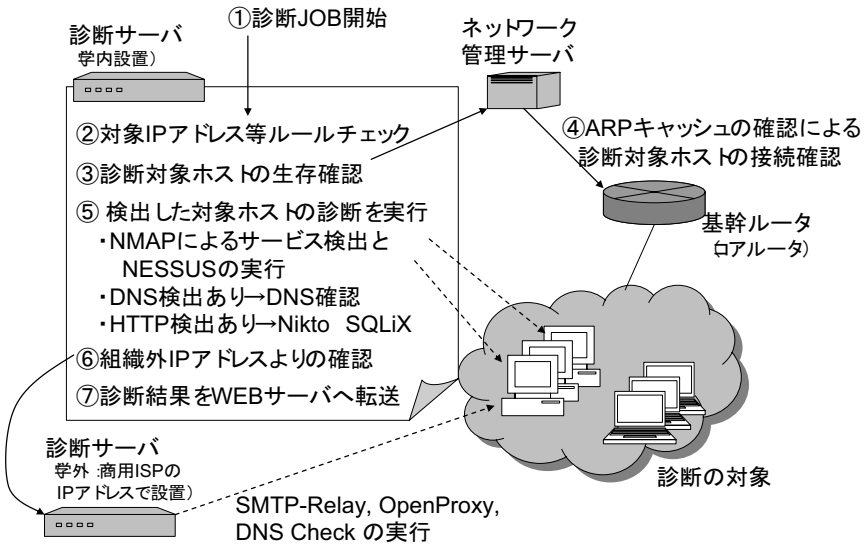

図４　診断システムのシステム構成とその動作例

Figure 4　System Configuration of Security Check System and its Example of the Operation.

力する際に脆弱性情報が公開される際の管理番号の主要なものに対応しており，本実装では Bugtraq ID（BID），Common Vulnerabilities and Exposures(CVE)，Open Sourced Vulnerability Database(OSVDB)を用いた．

これらの診断ツールの実行は，図４の①～⑦順に動作するように診断サーバに診断機能を設定し構成しており，コマンドラインから診断ツールの起動や，その結果に応じて次の診断ツールを起動する事や，外部サーバとのファイル転送等の機能で十分であるため，これらはスクリプト言語で実装した．

図４①により診断を開始すると図４②～④によりネットワーク管理サーバを用いてネットワーク機器へ管理アクセスにより ARP 等による診断対象ホストの接続状態を実行時にリアルタイムに取得する．

⑤の動作では, NMAP 及び NESSUS の診断結果より, HTTP のサービスが検出された場合には, WEB アプリケーションの詳細な調査を複数の診断ツールによる連係動作としては以下の実行ルール A～E により診断を行う．

A. 診断により確認された WEB サービスのポートに対して、診断時に検出された URL に対して連係動作する診断ツールで通常設定により診断を行う．なお診断時には設定により調査した URL が記録可能な詳細情報出力機能は有効として断実行する．

B. 診断の結果より，調査した URL，URL へのアクセス時のファイルの有無や応答，脆弱性の有無を記録，URL を検出した診断ソフトを記録する．

C. 既に検出済みの全ての URL への診断が実行されていれば診断を終了して⑥の処理へ進む．

D. CMS-Explorer による診断結果で，異なる URL で同一のファイルが返答される場合には URL アクセスへの動的生成で返答されている場合と判断し，同一のファイルが返答される URL への診断は終了する事とした．（本実装で用いた診断ツールのうち CMS-Explorer が初期状態で診断する URL 数が最多であるため判定に用いた）

E. 未調査の URL に対して診断ツールでの診断を実行し B. の診断結果の処理から再開する．

⑥⑦で残る診断と WEB サーバへ診断結果を転送するとともに，⑤の処理で NESSUS 以外の診断ツールにより警告等が検出された場合は，各診断ツールが対応する表１の脆弱性情報管理番号による NESSUS の結果との重複を削除後に，診断結果の HTML ファイルにテキスト形式で追記を行う．さらに，診断終了により診断結果が閲覧可能な状態になった事を管理者へ通知して確認を促す構成とした．

図５に WEB サーバに実装した利用者が操作を行う WEB インタフェースを示す．図５の a)～d)の順に，a)認証によるログイン，b)管理しているホストの診断実行，e)診断結果の選択，d)診断結果の確認の順に操作を行い利用する．

4. 評価

4.1 診断時間の評価

表２に本実装例および評価に用いたサーバのスペックを示す．

表２　サーバハードウェアのスペック

Tables 2 Server Specifications and OS.

サーバ種別	ハードスペックと OS
WWW サーバ	Xeon E5540 2.53GHz / memory 18GB / Red Hat Enterprise Server 5.8
診断サーバ	Core2 Quad Q9550 2.83GHz / memory 4GB / CentOS 5.8

図５　利用者の WEB インタフェース

Figure 5　WEB Interface for Users.

これらのハードウェアによる診断で，情報センターで管理運用しているホストで WEB サービスを稼働させているホストについて診断を実行し評価を行った. CMS 等動的なコンテンツ生成機能の有無により診断に要する時間が異なり，静的なコンテンツで構成された WEB サーバの場合はホスト 1 台の診断時間は１０分以内で完了し, CMS 等動的コンテンツで構成されている場合でも 20 分以内に完了する事を確認した. 各診断ツールによる診断時間の例として既設の WEB サーバ（CPU Xeon E3110 3.0GHz / memory 4GB / Cent OS 5.8）での CMS として WordPress 日本語版 バージョン 3.5.1 の設置の有無による測定結果を表 3 に示す. 診断時間は NESSUS による診断が主であり， CMS 等が利用されていない場合の WEB サーバの診断時間は 5 分前後，CMS 等が検出されてそれらの診断が行われた場合には 9 分前後の診断時間が必要であった.

表３　診断ツールによる WEB サーバの診断時間

Tables 3　Execution Time of the WEB Server Scanning.

診断ツールの名称	CMS あり	CMS なし
NESSUS	549 sec	328 sec
Nikto2	106 sec	15 sec
CMS-Explorer	89 sec	73 sec
Whatweb	2 sec	2 sec

4.2 診断結果についての評価

前述のとおり，個別の診断に特化した診断ツールではサービスの検出自体が困難であったが，診断ツールの単独実行では診断されていなかった URL への診断実行を確認し，CMS 本体およびそのプラグインが検出されていなかった点事が確認され，またより多くの警告（要改善点）が検出された.

5. まとめ

本報告では，診断システムを導入して組織内の脆弱性診断を定期的に行う構成例について，複数の診断ツールを用いた診断支援システムについて，構成ならびにその評価について述べた. 構成では，各種診断ツールの違いにより，サービス自体の検出可能や不可能などを考慮し，事前にサービス検出を行う事，および，個々の WEB アプリケーションの診断を複数の診断ツールの診断結果を再利用し網羅的に診断する事で，個々の診断ツールを単独で実行する場合よりもより詳細な診断を行える構成となった.

評価については，評価環境が情報センターという情報システムの研究者の利用するネットワークや各種の運営・管理システムが存在する事は想像されていたが，結果としてはサービスポートを変更した各種の WEB ベースの管理システム等について，もこれまでの単独での診断ツール実行

では検出が困難だった項目についても診断が可能である事が確認された.

謝辞

本研究の遂行、および，セキュリティ脆弱性診断に関する学内運用，ユーザ対応等について尽力いただいている情報メディア教育研究センター[15]の関係者に感謝いたします．また，本研究の一部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] SANS Top-20 Security Risks, http://www.sans.org/top20/
[2] 田島 浩一，西村 浩二，岸場 清悟，相原 玲二，セキュリティ脆弱性診断支援システム，情報処理学会 DSM 研究会報告 Vol.2003，no.30-002，pp.13-18，2003
[3] 毛利公美, 高橋 秀郎, 広岡 俊彦, 曽根 直人, 森井昌克, ネットワーク資源に対する脆弱性自動監査システムの開発, 信学技報(OIS2004-11)，Vol.104No.69，pp．13-18，2004
[4] 田島 浩一，岸場 清悟，西村 浩二，相原 玲二，セキュリティ脆弱性診断支援システムを用いたセキュリティ対策とその評価，DICOMO2007 シンポジウム，pp.851-856, 2007
[5] 田島 浩一，岸場 清悟，近堂 徹，西村 浩二，相原 玲二，コンピュータセキュリティ脆弱性診断の実施方法についての運用評価，情報処理学会 EVA 研究会報告 Vol.2008, no.30, pp.1-6, 2008
[6] 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，複数の脆弱性**診断**ツールを用いたセキュリティ**診断**支援システムの構築，DICOMO2009 シンポジウム, pp.1297-1302, 2009
[7] Nikto2, A web server scanner, http://www.cirt.net/nikto2
[8] OWASP SQLiX Project, http://www.owasp.org/
[9] DoxPara Research DNS Checker, http://www.dospara.com/
[10] TimThumb Vulnerability Scanner, http://wordpress.org/extend/plugins/timthumb-vulnerability-scanner/
[11] Nessus Vulnerability Scanner, http://www.tenable.com/products/nessus
[12] CMS-Explorer, http://code.google.com/p/cms-explorer/
[13] Whatweb, http://www.morningstarsecurity.com/research/whatweb
[14] NMAP, Security Scanner , http://nmap.org/
[15] 広島大学情報メディア教育研究センター, http://www.media.hiroshima-u.ac.jp/