科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１７　日現在

機関番号：　１５４０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００８９

研究課題名（和文）セキュリティ脆弱性情報の関連性に着目した脆弱性診断支援システムの研究開発

研究課題名（英文）Research of vulnerability check support system that focuses on the relevance of security vulnerability

研究代表者
田島　浩一（Tashima, Kouichi）

広島大学・情報メディア教育研究センター・助教

研究者番号：５０３２５２０５

交付決定額（研究期間全体）：（直接経費）　　2,600,000円、（間接経費）　　780,000円

研究成果の概要（和文）：本研究では、コンピュータセキュリティにおける脆弱性を、診断ツールを用いて確認する際に複数の診断ツールを効果的に組み合わせて利用する方法についての研究および実装と運用評価を行った。その過程および成果において、「脆弱性関連データベースを自動的に生成及び更新する実装例を行いそれを可能とし」、また、「各種の診断ツールと脆弱性関連データベースを組み合わせ利用する事でより効果的利用が可能になる事」が確認された。

研究成果の概要（英文）：In this research, we tried to determine the way how to use the multiple security check tools in combination effectively. In the process and results, we confirmed the following two results.

o Our system could generate relevant database from multiple security check tools automatically.
o We have made it possible to use these tools with this relevant database more effectively.

研究分野：　総合領域

科研費の分科・細目：　情報学・計算機システム・ネットワーク

キーワード：　コンピュータセキュリティ　脆弱性診断

１．研究開始当初の背景

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は今日でも継続しており，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, サーバ側の脆弱性では WEB アプリケーションが１位と報告されている．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各種のコンピュータセキュリティ関連団体より公表されている．

これまでの著者らの組織では,オープンソースの脆弱性診断ソフトを用いて組織内ホストの脆弱性調査およびその対応を行っていたが，設定不足や機能不足により本来検出されるべきサービスやインストール済み機能の検出，さらにそれらの脆弱性が検出されていない場合があった．

診断ツールには，特定の診断に特化したものがあり，例えば WEB サービスを診断するツールには，デーベースを用いたコンテンツ管理機能を持つ構成の診断に機能を限定したものや，ある脆弱性注意喚起の公表後にその診断のみ可能という単機能のものなどがオープンソース等で公開されているが，診断ツールは基本的に単独の診断ツールで診断が実行できる様に構成されているため，ある診断ツール得られた結果により関連する別の診断ツールでさらに確認したいといった場合には，それらの機能や操作等を理解した者による実行操が必要であった．

そのため，それら複数の診断ソフトを効果的に利用する為には,調査したい箇所の選択や設定等を事前に検出して用意するなどの事前準備が必要であるものの，脆弱性によっては特定機能に特化されたオープンソースの診断ソフトの方がより詳細に診断可能である事をこれまでに確認していた．

２．研究の目的

本研究はセキュリティ対策に有効として提供されているさまざまなコンピュータセキュリティ脆弱性に対する診断ツールについて，より効果的な診断が可能となる利用方法および必要となる診断ツールの規格化について研究開発を行う．

具体的には，公開されている個々の脆弱性情報の間での関連性および脆弱性情報と診断ツールの関連性について公開情報等を基に診断ツールをうまく組み合わせて実行する方法について研究開発を行い，自組織におけるセキュリティ対策での利用を運用および評価の環境として利用する事で，その有効性を示す方法により研究を進める．

ここで，診断ツールの利用について，特に複数ツールを組み合わせて利用する際の問題点について要素となる技術の開発や規格化，およびその実装を行い全体として診断支援システムとして動作するシステムの開発を行い，自組織における利活用の運用を通して評価や改良を行う事とした．

図１に本件研究で解決する現状での問題点等を整理し，診断ツールを単独で利用する場合に必要な操作と複数利用する場合の例としてその操作の例をそれぞれ a）および b）に示すとともに，c）は個々の診断ツールを統括する機能を実装し b）への解決策となる診断を支援するシステム構成である．

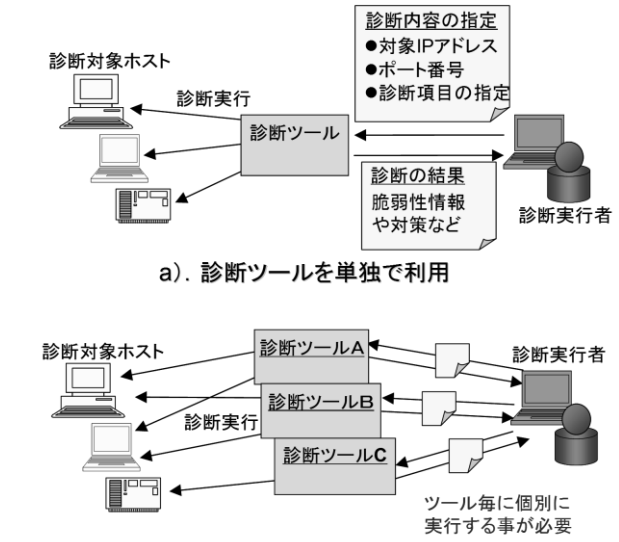

図 1　システムの動作イメージ

3．研究の方法

本研究では，自組織で研究開発と運用を行っている商用およびオープンソースの脆弱性診断ツールを用いた脆弱性診断システムについて，その診断実行部分について主に研究開発を行い，ここに，複数診断ツールの効果的な実行機能の実装およびその評価を行った．

そこでは，必要な要素技術となる診断ツール実行方法の規格化によりツール実行に対する実行環境や実行方法，診断対象の指定方法などの抽象化を行い，診断ツールの診断結果出力およびその提供方法の規格化により，連携動作で利用しやすい形式での診断結果の出力についての規格化を行い再利用ならびに有効利用を可能とし，これら 2 点の作成

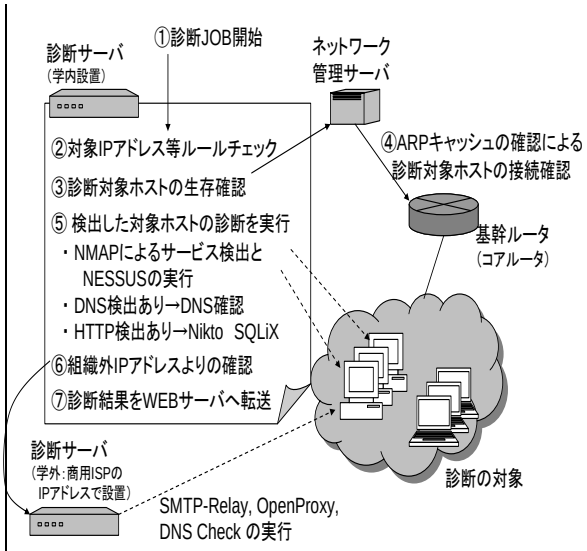

図２　システム構成図

する規格の元に，診断ツールの連動動作の開発を行った．

完成した脆弱性診断支援システムは，個々の診断ツールの違い等を気にすることなく，規格化された（統一化された）利用インタフェースにより脆弱性診断の実行および，結果としての脆弱性情報を得る事を可能とした．

平成 23 年度には，これまでの研究代表者らの研究開発した診断システムを基にして研究開発を行い，構築したシステム全体の構成図を図 2 に示す．システムを利用する者はＷＥＢブラウザを用いて診断支援システムにアクセスを行い，図 2 の①～⑥の順で診断が実行され，出力される診断結果の確認を行う．構築済みの機能には，利用者向けの WEB インタフェースや，管理者の認証や IP アドレス等管理情報の利用など診断実行の基本的な動作環境は継承した．

機能実装の方法は，診断ツールの多くが主に UNIX 系 OS 向けに CUI で作られている事から，診断サーバの Linux 上で動作する診断支援サービスとして実装を行った．診断サーバの構成は，診断ツールの設置および本研究で開発を行う脆弱性情報関連性の収集用のデータベース，診断ツールより構成される．なお診断ツールのインストール等追加操作については，各種の Linux で採用されているパ

ッケージ管理によるソフトウェアの管理を利用する事とし，診断ツールの実行について個々のツールに対して，診断支援システムの管理プログラムとの間での命令インタフェースを規格化し，これらの診断ツール実行との間でのアダプタを実装し利用する事とした．

具体的な，診断サーバの実装方法は，規格化および連動動作について以下に述べる機能の研究開発を行い，開発段階においてそれぞれ全体として診断支援システムとして動作するようにシステムの開発を行い，開発の段階毎にシステムの所属部署での運用およびその評価を行った．

1)　診断ツール実行方法の規格化

診断ツールは，実行時に必要とされる引数や設定する実行パラメータが存在し各診断ツールにより独自の実装方法で実現されているため互換性が無いが，診断ツールという機能より対象を指定する IP アドレスやポート番号の指定など，指定方法が異なるものの共通するパラメータもあり，実行指定についての規格化は，XML による診断対象の指定から各診断ツール実行に必要な CUI のコマンドオプション等の記述や指定に必要な設定を行うアダプタを個別に作成する事で可能となった．

2)　診断ツールの診断結果出力およびその提供方法の規格化

診断により得られる診断結果についても考慮が必要であり，ツールによっては終了時のステータスコード（戻り値）や簡単な文字列による診断結果（場合によっては OK の表示みなど）を提供するものや，どのように対策すべきかについての説明等が含まれるものなどがあり，人の可読な情報の維持とプログラムによる自動処理が可能となる条件で，書式を XML による表記に統一する規格化を行った．実装方法は，１）の診断ツール実行方法の規格化と同様に各診断ツール個別のアダプタに機能を組み込む事とした．

3)　診断ツールの連動動作の研究開発

診断支援システムの利用者が要求した診断に対して，診断の開始から終了までに実行する複数の診断ツールの実行過程で，それぞれの診断結果に応じて次に起動する診断ツールの選択や適した実行指定を可能とする方法について基本的な設計および実装とその評価を行った．

４．研究成果

（１）脆弱性関連データベースの生成に関して

本研究では，診断ツールを用いて脆弱性診断を行う際に，どの診断ツールで何の脆弱性が診断可能であるのかについて，まず明確にするため，脆弱性関連データベースを生成可能な限り自動的に生成及び更新する事とした．ここでは，脆弱性情報の公表時に各団体が管理している脆弱性識別用の管理 ID を利用し，本研究で用いた各診断ツールにおける脆弱性管理 ID への対応状況は表１の通りであった．

表 １　本研究で用いた診断ツールと脆弱性管理 ID の対応状況

名称	主機能	BID	CVE	OSVDB	ライセンスと提供形態
NESSUS	統合型診断ツールで対策方法も提示	○	○	○	商用ライセンス実行バイナリ形式
Nikto-2	CGI 等 WEB 診断用	○	○	○	オープンソース

CMS-Explorer	CMS 診断用	×	×	○	オープンソース
What-web	WEB 本体と組み込み機能判定	×	○	×	オープンソース
SQL MAP	SQL インジェクション	×	×	×	オープンソース

実装についての報告（学会発表①，2013/07/09）時点での実装で用いた管理 ID とその登録数は次の通りであった．

- CVE (Common Vulnerabilities and Exposures)
  http://cve.mitre.org/cve/
  登録数:56,965
- OSVDB (Open Sourced Vulnerability Database)
  http://www.osvdb.org/
  登録数:93,667
- BID (Bugtraq ID)
  http://www.securityfocus.com/bid
  登録数:58,604

これらの脆弱性管理 ID に対して各診断ツールが対応しシステムで利用可能な脆弱性管理 ID は表２の通りであった．

表 2 診断ツールが対応する脆弱性管理 ID (2013/07/09 の報告時点)

管理 ID	エントリ数
BID	16,144
CVE	34,443
OSVDB	17,084
合計	67,671

（２）診断ツールの連動動作に関して

研究の背景で述べた，本来は検出されるべきサービスや機能等およびその脆弱性に関して,例として WEB サービスの診断において，単独のツールで検出できていなかった CMS を検出した場合の評価として，診断に要する時間の例を表３示す．この例ではインストール先ディレクトリとしてデフォルト（HTML のトップディレクトリ）以外を指定して構成した CMS（ WordPress）に対して，連動動作により CMS が検出された場合との診断に要する時間の結果例を示す．

表 3　ホスト１台の診断時間（WEB サーバの例）

	CMS あり	CMS なし
診断時間（合計）	750 [sec]	450 [sec]
（内訳）		
NESSUS	549 [sec]	328 [sec]
Nikto2	106 [sec]	15 [sec]
CMS-Explorer	89 [sec]	73 [sec]
Whatweb	2 [sec]	2 [sec]

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 自体が検出されていなかった点およびより多くの警告（要改善点）が確認できた．

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　２件）

① 藤村喬寿，西村浩二，近堂徹，大東俊博，田島浩一，相原玲二，スイッチベース認証ネットワークへのシングルサインオン機能の実装と評価," 情報処理学会論文誌，vol.53，no.3，pp.958-968, 2012 年. 査読有

② 田島浩一, 近堂徹, 岸場清悟, 大東俊博, 岩田則和，西村浩二，相原玲二，大規模キャンパスネットワークにおけるMAC アドレス認証端末の移動管理," 学術情報処理研究，原著論文，no.15，pp.53-60, 2011 年. 査読有

〔学会発表〕（計　2 件）

① 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, 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，DICOMO2013 シンポジウム論文集，pp.749-754, 2013 年. 査読有 @北海道河東郡音更町

② 田島 浩一・西村 浩二・近堂 徹・岸場清悟・大東 俊博・岩田 則和・相原 玲二,ネットワーク機器動作ログ参照サービスの試作," 情報処理学会研究報告 Vol. 2013-IOT-20, No. 34, pp.1-4, 2013 年. 査読無 @奈良県奈良市

〔図書〕（計　0 件）
該当なし

〔産業財産権〕
該当なし

〔その他〕
該当なし

６．研究組織
(1)研究代表者
田島　浩一（TASHIMA　KOUICHI）
広島大学・情報メディア教育研究センター・助教

研究者番号：　50325205