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

田島 浩一 岸場 清悟 近堂 徹 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

ネットワーク管理におけるセキュリティ対策に，脆弱性診断ツールを用いた診断が効果的であることは広く知られている．多数のネットワーク管理者が点在する大規模組織においても，組織全体を一括して診断する事で個別に実施する場合に比べ，診断に要する実施の手間や診断サーバの維持といったコストを大幅に低減することができる．しかしながら診断を行うソフトウェアは，診断の実施者がその結果を自身で確認するように構成されている事など、組織内での使い方にあわせたカスタマイズが必要である。

本稿では，本学での定期的な診断実施のために構築した診断システムや実施方法についての説明とそれらの運用評価について報告する。

Evaluation and Execution of Vulnerability diagnosis System for Computer Security

Kouichi TASHIMA Seigo KISHIBA Tohru KONDO
Kouji NISHIMURA Reiji AIBARA

Information Media Center, Hiroshimaa University

It is well known that vulnerability diagnosis by checking tool is effective to keep network secure. In large-scale organization which has many network administrators, cost of network management will be decreased by batch diagnosis of whole organization. The work of execution that required for the vulnerability diagnosis and the maintenance of the servers are included in the cost. As the software was composed those who execute it about the diagnosis confirm the result, it is necessary to customize it to use in the organization.

In this paper, we describe the implementation and execution of the vulnerability diagnosis system with practical example.

1. はじめに

大規模組織のネットワークセキュリティ維持のためには脆弱性診断や不正侵入検知を通じたネットワーク全体のセキュリティ情報収集が必要である．小規模な企業などで情報部門が一括してネットワークや端末を管理できる場合とは異なり，大規模な企業や大学では，部門や学部等の単位で管理権限を分割委譲して運用されている．

図１は全体のネットワークをサブネットに分割し，それぞれのサブネット内を管理する管理者(以下，ネットワーク管理者)を置き，管理権限を委譲した例である．このような場合，管理範囲内のセキュリティ情報収集はネットワークの管理権限を委譲された各管理者が実施すべきものであるが，診断や検知を実行するサーバの準備や保守，使用するソフトウェアの仕様把握など実施する労力はけして小さくはない．

また組織全体のセキュリティレベルを維持するために，セキュリティ情報収集をセンター組織で行い管理者に通知する運用として，侵入検知システム（IDS）をセンターで一括して運用するセンター管理型不正アクセス検出システムの事例［1]セキュリティ情報収集にかかるコストを抑え，脆弱性診断ツールを用いたセキュリティ監査のセンターでの一括実施の事例[2]などが報告されている．しかしこれらは組織全体で一定のセキュリティレベルを維持するための情報収集が目的であり，点在する各管理者が

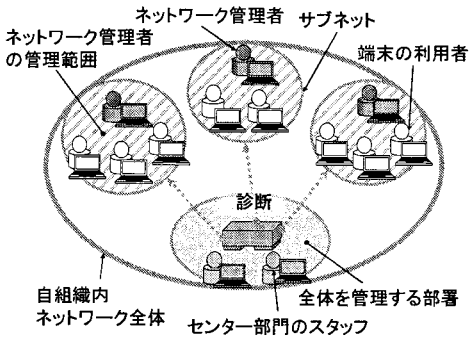


図 1　管理に関する概念図

日常的にそれらの結果を利用するような対応はやりにくいと考えられる.

著者らの組織においても過去に DNS サーバや SMTP サーバなど，特定のサーバソフトに絞ってソフトのバージョンを調査し，適切なバージョンアップを行うように対策を促す試みを行っていたが，一般的に言われる，「セキュリティ対策を障壁に例え、その障壁に低い部分が残る限り他の高い部分をより高くしても効果的ではないという事」から主要サーバソフトのバージョン調査をはじめとしてその設定の脆弱性の調査や UNIX 系 Windows 系 OS 特有の修正プログラムの適用状況などを総合的に診断する機能をもった診断プログラムを利用する事とした. 本稿では定期的な全学を対象としたセキュリティ脆弱性診断を行う診断システムの構築についてと運用評価について報告する.

2.　セキュリティ診断の実施

2.1 セキュリティ診断ソフトウェアの利用

診断ソフトウェアの利用については、商用のソフトウェアや一部の利用制限が課せられる場合も含みオープンソースのソフトウェアも選択できる.

商用ソフトでは、一般的に診断対象の IP アドレス数に応じた比較的に高額なライセンス料が必要であるものの、GUI により設定管理を行うように構成されている例が多く、そこで診断の実行やスケジュール管理により定期的な診断の実行が容易に設定できたりする。 WINDOWS 端末から直接操作できる設定のみを指定して実行する方法では、操作者の操作量が少なくて済むように実装されているものが多いものの、カスタマイズなどについて設定できる内容に制限があることや、特定処理を定期的に一括して実行するような毎回の操作を一括処理する設定に制限があったりと、用意されていない機能についての追加が基本的に困難である。その他、診断結果を各管理者に通知する際に、診断の結果も WINDOWS 端末ソフトを使って閲覧するように作成されていると、診断ソフト以外での閲覧が困難であったり、データとして CSV 形式程度でのエクスポート機能しか用意されていないソフトもある。

2.2 セキュリティ診断システムへの要求

ネットワークを分割して管理する場合，脆弱性診断を実施するのは，本来はネットワーク管理者であるが，ネットワーク管理のための専従者を学部等の管理単位で置くことが大学などでは困難な場合が多いことも考慮する必要がある。その場合，自身で診断サーバを運用しなくても診断が行える事が必要であること（各管理者が診断サーバを持つことが現実的ではないという判断）より，全学を一括して情報センター部署より実施し，その結果を各管理者に通知する方法とし，あわせて診断結果の安全な配布方法を考慮した診断システムについて学内での運用に適した形で構築することとした.

3.　診断システムの構成

3.1 システム構成

本システムは図 2 に示すように診断のスケジュール管理や診断実施の案内，診断結果の閲覧に利用するWWWサーバ 1 台と実際に診断を行う 1 台以上の診断サーバとで構成され，多数の対象を同時に診断する場合に複数台の診断サーバによって負荷分散を行っている.

WWWサーバ　WWWサーバ部は，著者らの所属するセンターで運用されている各種のＷＥＢサービスで用いられているサーバに，機能を実装し利用した．このサーバは ID/パスワード認証利用を想定し主要な認証機関のサーバ証明書を備えており適していた.

診断サーバ　維持管理と自組織内限定のアクセス制限が設定されていること想定して学内のグローバルアドレスに 10 台を設置し，また，OpenPROXY 問題のように組織外から検査が必要な診断のため商用プロバイダのアドレスをつけた診断サーバも 1 台設置している.

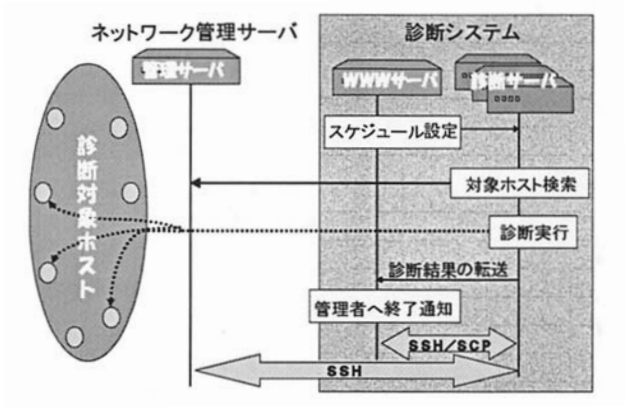


図２　診断システムの構成

ネットワーク管理サーバ　ネットワークの管理用に設置しているサーバで、ルータ等の機器に対して SNMP により ARP テーブルの取得を定期的に行っており，診断サーバから要求で，診断対象範囲内で接続して ARP に答えるホスト（生存していると考えられるホスト）のリストを提供している．

認証サーバ　**図 2 には含まれていないが**，認証には学内構成員の ID が登録され，広く全学で利用されている電子認証システムの LDAP サーバを認証利用し，このサーバとの通信には安全性のため LDAPS を利用している．

今回の実装において各サーバで使用した主なサーバソフトを表 1 に示すとおりであり，診断ソフトウェア以外は一般的なサーバソフトである．

表 1　使用サーバソフト

機能	利用サーバソフト
WWW サーバ	Apache2，OpenSSL，OpenLDAP
サーバ間通信用	OpenSSH
診断ソフトウェア	NESSUS 2 系

3.2 ユーザインタフェース

管理者の認証については，一般的なＷＥＢサービスでも利用されている BASIC 認証を用いている．BASIC 認証では，同一ディレクトリ配下の複数の診断結果ファイルを開く事や，同一のネットワーク管理者が複数の管理範囲内の結果等を同 ID の再入力なしに閲覧できるようにするために適しており利用した．その他，スケジュール等の設定をはじめとする管理用のプログラムは UNIX 系 OS での移植を容易にするため，各サーバ内のスクリプト言語を使用した．

診断ソフトウェアの診断内容を最新の状態に保つために，定期的な更新が必要であるが，この機能は診断ソフト NESSUS の機能を設定し利用する．

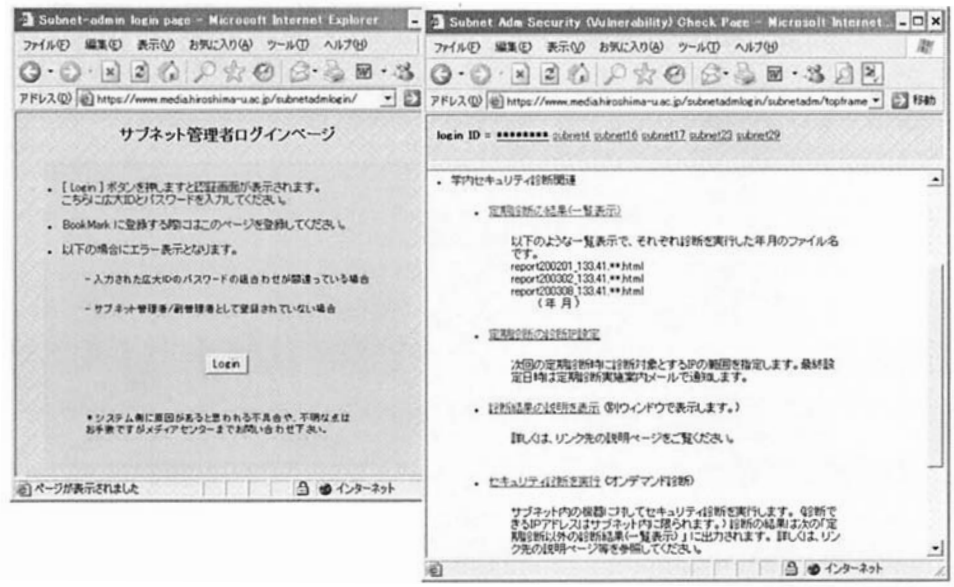
これら診断システム内のサーバ間の通信に加えて，管理者，外部の認証システムとの通信は，診断結果やパスワードなどセキュリティ情報を含む内容の通信を行うため，Email による診断の終了を知らせる管理者への通知以外は，暗号化により機密性を確保する．

管理者が診断結果の閲覧を行うＷＥＢインタフェースを図 4 に示す。管理者に通知しているＵＲＬを開くと a)のログイン画面が表示され、認証を経てｂ）のメニュー一覧に進み、ここから定期診断の結果の閲覧を行う。ここでは、管理者へのメニューとして、定期診断の閲覧以外に、定期診断時に診断の対象として診断の用不要を登録できるインタフェースや，別途報告を行っているオンデマンドで診断を実行する機能を用意している[3][4]。

4.　運用事例と評価

4.1 運用環境

筆者の大学では，2002 年度より一括診断およびその結果のＷＥＢページでの学内管理者への提供を開始している。



a) 管理者用ログインページ　　b）管理者用メニューページ

図３　管理者用 WEB インタフェース

図２に示した構成に対して，学内での運用は具体的に表２のスペックを用い以下のサーバの構成で行っている．文献[3][4]の報告

表 2　ハードウェアスペック
Table 2　Hardware spec.

サーバ種別	ハードスペック
WWW サーバ	Itanium2 x 2, memory 512MB
診断サーバ	Pentium4 2.4GHz memory 512MB

時には WWW サーバに ULTRA-Sparc 200 MHz，診断サーバも Celeron 900MHz のハードとくらべて大きく同時処理能力が改善している．　また文献[3][4]の報告において，診断サーバの処理能力の評価を行っており，本論文の構成の場合，40 程度の同時診断が問題なく行えることを示している。

4.2 ネットワークプリンタへの対策

ネットワークプリンタの多くは、HTTP や TELNET による設定管理が行えるものや、FTP を用いて印刷するファイルを PUT して利用するような受け付け方法に対応しているため，ネットワークプリンタを診断した場合には、HTTP，TELNET，FTP 等のサーバとして検出される。FTP サーバの診断として通常診断時に実行される，anonymous やパスワード制限等のない方法で無制限に書き込みが可能であるかといった診断が実行されるため、この診断により白紙や無意味な文字列を印刷してしまう事が生じる。また、無制限に書き込める場合などにセキュリティホールが存在する FTP サーバとして判断される場合や、診断のアクセスがネットワークプリンタ側で想定していないアクセスである事などが原因で、診断のアクセスによりネットワークプリンタが高い確率のハングアップする事がわかっており、ネットワークプリンタへの対策が必要となる。

これら無駄になる印刷やハングアップを避けるために、診断の対象がプリンタであると判別された場合には、その対象への診断を実行しないように診断ソフトのカスタマイズを行った。使用している診断ソフトである NESSUS には、独自のスクリプト言語によるプラグインの追加や変更が可能になっており、各種の診断の実行する前に、検出を行う機能を追加実装した。

ネットワークプリンタの検出方法として、FTP や TELNET 等でプリンタに接続した際のサーバからの応答メッセージが図４に示すような機種や製造元により特定の応答メッ

セージである事から、これらの文字列の検出と，事前に把握しているネットワークプリンタのメッセージとのマッチングを行い，一致した場合には対象への診断は「ネットワークプリンタとして検出されたため診断しない」という趣旨を表示するのみで診断を実行しないように構成した。

```
OKI 製ネットワークプリンタ：
220 EthernetBoard MLETB09 Ver * FTP server.
EthernetBoard MLETB09 Ver * TELNET server.

EPSON 製プリンタサーバ：
220 JC-CONNECT E-8600TNE Ver * FTP server.
JC-CONNECT E-8600TNE Ver * TELNET server.
```

図４．ネットワークプリンタの FTP/TELNET の応答メッセージ例

4.3 定期診断の実施方法

本学で診断に利用しているソフトウェアはオープンソースであり、これまでに不完全状態でバージョンアップが公開され不具合により正常に診断できなかった例や、追加された診断機能の事前の確認を行うため、以下の様な手順により学内全体を対象とした診断を実行する事としている。

Step 1 定期診断の実行時点で診断システムの更新を行い最新の状態にする
Step 2 情報センター内の一部サブネットで実施し不具合や変更点の確認
Step 3 情報センター内の全サブネットで実施し不具合や変更点の確認
Step 4 学内行事や診断に要する時間より診断日時のスケジュールを作成し学内に案内
Step 5 全学の診断を開始

Step1 では，診断ソフトバージョンアップやパターンファイルの更新等を行うとともに，診断サーバ自身の診断を試行し動作の確認を行う簡単なスクリプトを作成しており、自動で実行している。

Step2 では著者の所属する情報センター内のサブネットで、センター内の職員が主に管理用として PC やサーバを接続しての利用している一部のサブネットを対象に診断を実行し、職員に診断結果を通知するとともに、PC やサーバでの不具合やログ等での問題点の無い事を確認し、あわせて、以前の診断結果と比較し、しく診断されているかの確認を行っている。また、診断に要する時間について予定時間内に終了しているかの確認も行っている。

Step3 の診断では対象から除外するホストとして、センターに情報コンセントサービスや VPN 等で接続しているサービス利用者の端末や、教育用端末室の端末は同じ設定で多数存在するため診断はそのうちの数台を対象とするような、一部の例外を除いては，センター内で研究やサービス用などに用いられている PC やサーバなど全てのホストを対象として診断を行い、スタッフ宛に診断結果を通知し、Step2 と同様に問題点の確認を行っている。

ここで Step2/3 において、端末がハングアップするなど不具合が生じる診断については、その検証を行い原因となるアクセスを行っている診断を定期診断時には実施しないように設定している。1 度不具合が生じた場合でも以降の更新時に診断ソフトで対策されている場合が多く変更された際に確認しており、多くても 10 個程度以下がこれに該当する。

Step4 では、診断の実行日を決める際には、入学試験など特定の行事の日を避け、センター内の診断に要した時間から全学内を対象とする診断スケジュールを作成し、学内に案内を出すとともに診断システムに設定を行い、スケジュールにしたがって Step5 の学内診断を開始している。

4.4 定期診断での診断の有効性について

図 5 に学内のホスト数の推移を示す。図のグラフは、平日の例として 2007 年 1 月２６日金曜日に診断の対象となるホスト数（＝IP アドレスの数）を、それらのホストを収容しているルータの ARP テーブルについて 5 分毎に集計したグラフである。
始業開始の時間の 8 時 30 分の前後に多くのホストが電源投入され、ホスト数が増加し、診断実行時間として案内している 9 時～18 時の間にホスト数のピークも含まれており、多くのホストが診断対象に含まれていると考えられる。 図 4 では、センターのサービス時間外である 6 時以降も継続して利用されるホストがあり、この中には 6 時以降に電源をいれて利用されていると考えられるホストがある。これらのホストは、夕方電源が

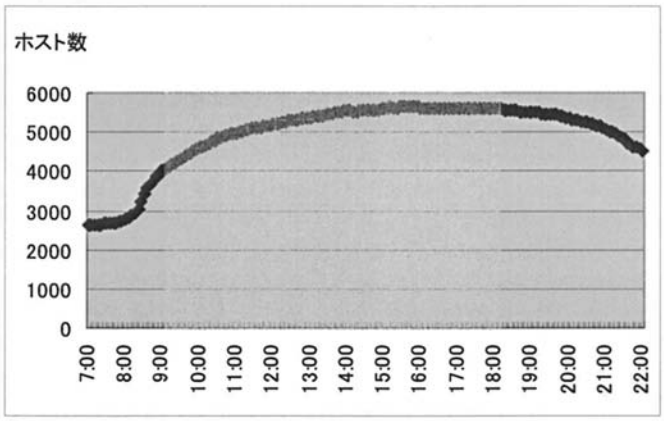


図５．学内ルータで観測したホスト数推移の例（2007 年 1 月 26 日）

入り、夜間～深夜にかけて減少していることから、クライアント端末の利用であろうと想定している。これらの端末も診断するために、時間を夜間まで延長する事について検討したが、上記より不具合時に対処できないことと常時電源の入っていない端末であるため、運用方法での対処として、学内向けの診断スケジュールを通知するさいにこのような端末は、診断日にはサービス時間内に電源を入れておいてもらうように案内する方法をとっている。

5. おわりに

本報告では，学内の全ホストを対象とした診断システムを構築し，学内ネットワークの管理に適用するという運用評価について述べた．診断システムは現在も継続して利用されており，大きな不具合や停止等も生じておらず本システムは順調に稼動していると評価している．

本システム導入による具体的な効果として，本報告中では具体的な数値は示していないが、用意したオープン PROXY の検出や、診断結果の警告数には減少が見られている．何も対策をしていない状態では新たに生じるセキュリティホール等の診断項目数の増加を考慮すると、減少の内容については、各種の更新や修正プログラムの適用をはじめ、サーバプログラムやサーバ自体の停止など詳細について今後は検討したい。

また、今後は，残存するセキュリティ警告数のさらなる減少，ワーム被害や外部からの苦情の減少等の評価を行いたいと考えており，運用実績とあわせてアンケート等でシステム利用者の評価を収集し検討する事などを今後の課題としたい．

謝辞

本論文中の診断システムの開発・支援・運営は広島大学情報メディア教育研究センター[6] のスタッフ，中国・四国インターネット協議会[7] の協力を得ています．ここに記して謝意を表します．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（18700063，19300019）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．

[1] 大塚 丈司，白石 善明，森井 晶克，センター管理型不正アクセス検知システムの提案，情報処理学会 CSEC 研究会報告 Vol. 2002，No. 18-007，pp. 39-44，2002

[2] 萩原 洋一，佐藤 克巳， 美宅 成樹，ネットワークセキュリティ総合監査とその評価，情報処理学会ＤＳＭ研究会報告 Vol. 2002， no. 25-002, pp. 7-12，2002

[3] 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

[4] 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の構築，情報処理学会 DSM シンポジウム，Vol. 2004，no. 3，pp. 7-12，2004

[5] NESSUS project. http://www.nessus.org/

[6] 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/

[7] 中国・四国インターネット協議会