セキュリティ脆弱性診断支援システムの構築

田島浩一　西村浩二　岸場清悟　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コストを大幅に低減することができる．しかし，このような一括診断だけでは管理者やPC使用者が自ら行った対策の有効性を即時かつ容易に診断することができない．本稿では，認証の仕組みを利用することにより，誰でも自分の PC などに対して手軽にセキュリティ脆弱性診断が実施できるシステムについて述べ，診断システムの構築や有効性について実際の運用事例とともに報告する．

Implementation of Security Vulnerability diagnosis Support System

Kouichi Tashima　Kouji Nishimura　Seigo Kishiba　Reiji Aibara

Information Media Center Hiroshima 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. However, by batch diagnosis, network administrators or PC users cannot verify effects of their measure to keep network secure instantly and easily. In this paper, we describe the security vulnerability diagnosis support system by which anyone can diagnose vulnerability of their PC or network by themselves instantly and easily with authentication. We report implementation and validity of the system with practical example also.

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する必要がある．管理権限を管理者に分割委譲した例を図1に示す．この図で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，サブネット管理者)を置き，管理権限を委譲した例である．それぞれの管理者は自分の属する管理範囲(図1の斜線部)を担当する．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．セキュリティ情報収集にかかるコストを抑え，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]
- ○ 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提供であり，各管理者が日常的に行うネットワーク管理作業への対応はやりにくい．各管理者が組織内の事情に沿ってきめの細かなセキュリティ対策を実施するには，分担組織のセキュリティ情報がつねに即時的かつ容易に得られることが必要である．筆者

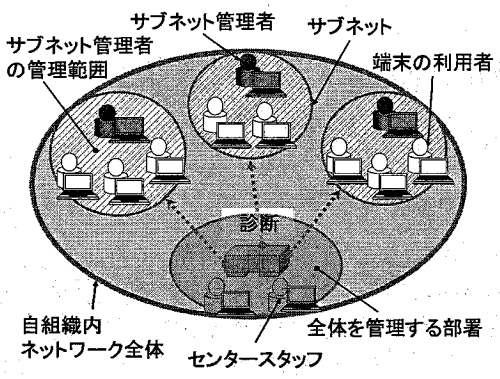

図1. 管理に関する概念図

らの組織においても定期的に一括実施による診断を実施しており，診断への問い合わせや対策後の再確認の要望などが寄せられていた．筆者らはこれらの要望を満たすため管理者のためのセキュリティ脆弱性診断支援システムを開発し 2003 年 7 月より利用対象者へ公開し運用を開始した．本稿ではシステムの構築やその経緯，運用事例と有効性について報告する．

2．セキュリティ診断の現状と要求

2．1 セキュリティ診断サービスの利用

商用のセキュリティ診断サービスは現在すでに多くのものが提供されており，組織外ネットワークからの診断や組織内に診断サーバを置いて診断するメニューが用意されている．ネットワーク管理者が診断サーバを設置，管理する必要はなく，一定の費用はかかるが手軽に詳細なセキュリティ診断結果が得られる．しかしネットワーク管理者としては，診断結果に基づき対策を実施したならばその結果をすぐに確認したいであろう．これらの診断サービスの多くは定期的もしくは依頼した日時の一括診断なので，その後個別の対策結果の確認を行うには次回の定期診断を待つか，別途費用をかけて個別に診断を受ける必要があり，時間的または経済的なコストが必要となる．そのため，確認の要求を満たす事が難しい．

2．2 セキュリティ診断ソフトウェアの利用

一方ネットワーク管理者が自ら診断サーバを設置運用してセキュリティ診断を実施することも考えられる．診断に使用されるソフトウェアは広範囲の脆弱性や設定などを診断対象としている点，脆弱性情報の公開後からその診断が可能になるまでの時間的な対応が早い点で，ISS 社の製品 Internet Scanner [4]やオープンソースの NESSUS [5]などが利用されている．一部の大学においてはこれらのソフトウェアがすでに利用されている．

これらのソフトウェアを準備し保守することで，診断を望む時間に望む回数実行できるが，必要な労力はけして小さくない．また，端末の利用者全てがこの仕組みを持つ事は現実的ではないなど，個別の診断環境構築は容易ではない．

2．3 セキュリティ診断への要求

ネットワークを分割して管理する場合，本来は脆弱性診断を実施するのはネットワーク管理者である．ネットワーク管理専従者を部局ごとに置くことが大学などにおいては困難なことも考慮すると，この診断は2．1で取り上げたセキュリティ診断サービスのように自分で診断サーバを運用しなくても手軽に診断結果が得られ，かつ診断結果は平易に書かれていて具体的な対策指針を立てることができ，また2．2の利用のように対策作業を実施したその場で作業結果を確認可能であることが必要である．

一方ネットワークが分割管理されていても，ネットワーク全体を組織のセキュリティポリシーに基づき一定以上のセキュリティレベルを維持する必要がある．そのためには分割された各ネットワークのセキュリティ情報は，全体を統括する部署であるセンターに集約することになるだろう．脆弱性診断についても診断結果を集約して各管理者への技術的支援を行い，ネットワーク全体のセキュリティレベル維持に役立てる必要がある．多数の管理者を持つ組織では，この部署で診断サーバを準備する事でコストの集約が可能である．さらに，その部署に属する者であれば必要なときに診断できることが望まれる．

2．4 セキュリティ診断に求められる機能

2．3節で示した要求を実現するために，セキュリティ脆弱性診断システムには診断を実行する管理者の立場(端末の利用者も端末1台の管理者として含む)から以下の機能が必要である．

①オンデマンドでの診断実行環境

②平易な診断結果の提供

ネットワーク全体を統括するセンターの立場からは全ての機器のセキュリティレベルを維持するため，また，診断結果を統計的に利用し今後の方針決定に役立てるため以下の機能が必要であり，

③組織全体でセキュリティレベルを統一

④組織全体のセキュリティ情報を一元管理

近年，ワームなどネットワークを介しての被害が懸念された場合に以下の機能が必要である．

⑤早急に特定の脆弱性が確認できる機能

3．システム構成

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受付や結果の閲覧に利用するWWWサーバ1台と実際に診断を実行する1台以上の診断サーバとで構成される．

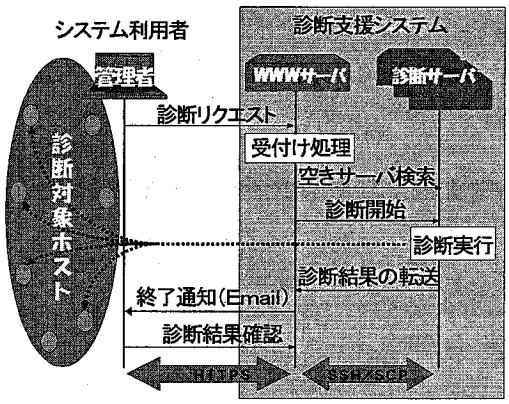

図2．システム構成図

この診断サーバを，自組織外に設置する事も可能であるが，組織外からのアクセス制限等で対策している機器へより多くの診断を可能とするため自組織内に設置し管理する．診断ソフトウェアの診断内容の更新はソフトの機能を設定する事で定期的に更新される．

Emailによる診断終了の通知以外の通信は，暗号化により機密性を確保する．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とハードウェアスペックを表1，表2に示した．利用者認証については，apacheのBASIC認証を，CGIやその他の設定・管理用プログラムは各サーバ内のスクリプト言語(sh, perl)を使用．サーバ間の通信には安全性を重視してSSHを採用した．また，診断結果は，WWWサーバに用意し閲覧にHTTPSを用い安全性を確保すると共に診断結果をシステム内に保持し2．4節の機能④の一元管理を満たす．

3．2 ユーザインタフェース

本学では，センターが一括実施する脆弱性診断結果を通知するためのWEBページを，本システム開以前の2002年度から作成運用していた．これはBASIC認証によりネットワーク管理区分ごとにアクセス制御を行い，各管理者が自分の分担するネットワークについての診断結果を閲覧するためのもので

表1．使用サーバソフト

WWWサーバ	Apache
サーバ間通信	OpenSSH
診断ソフト	NESSUS

表2．ハードウェアスペック

WWWサーバ	SOLARIS7	ULTRASparc200MHz memory 256MB
診断サーバ	Linux 2．4．7	Celeron900MHz memory 128MB

あった．本システムではこのページの認証を流用して，各管理者による診断の実行のための図3のようなWEBインタフェースを作成した．管理者が交代した場合の機能提供や診断結果の引継ぎもこの認証情報の更新により引き継がれる．利用者により選択できる項目などが異なり，図3①の画面は管理者用のものである．図3②のスタッフ用では診断対象IPアドレスは自組織内の全て範囲が指定でき，図3③利用者端末用では，対象の選択は無くEmail連絡先の指定が必須となり，図3③右画面での認証情報の入力が必須となる．

3．3 診断内容の選択機能

2．4節の求められる機能③より必要になる場合がある．2003年8月中旬より広範囲に広がった，亜種を含むBLASTER関連のワームは，診断により検出可能であったため，診断内容をこの原因に限定した診断を選択肢に追加した．前述の通り通常の診断では，目的とする診断以外の診断を実施するため，診断項目を限定し短時間で結果を提供する事を目的とした．この変更で診断項目数を，ホスト1台あたり最大1500項目の実行から2項目のみの実行とし，実診断時間で20分から10秒程度に短縮される．今後も必要時に診断の選択肢を若干の修正で追加対応する．

3．4 管理者用の診断の流れ

利用者はユーザ名／パスワードを入力してこのページを開き，診断の対象IPアドレス，終了後の連絡Emailアドレスをそれぞれ選択し記入する(図3①)．選択・記入事項に問題が無ければ確認画面に進み，確認後に診断を開始する．診断の対象は利用者が管理権限を持つネットワークに限られる．診断に要

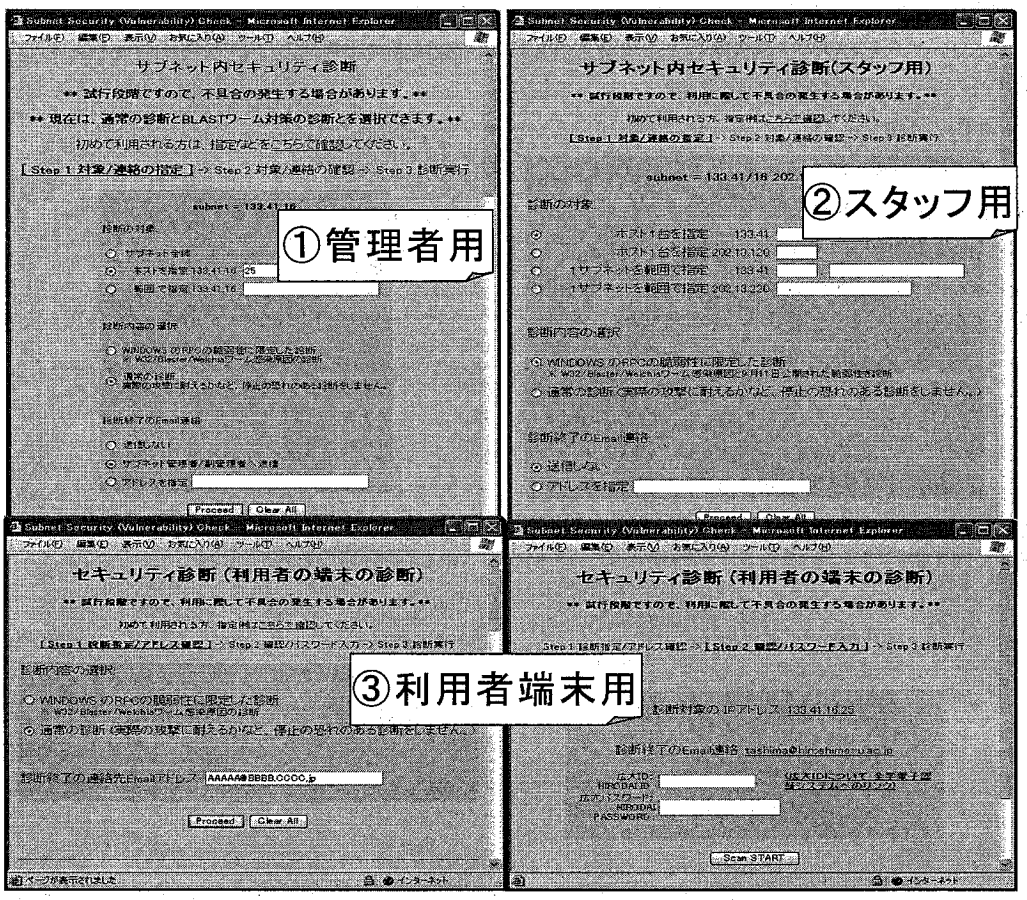

図3. ユーザインタフェース

する時間は対象ホストの数や対象ホストの処理能力により大きく異なる. 1ホストの診断なら数分程度で結果が出ることもあるが, サブネット全体の診断では長い場合に4,5 時間程度かかるため, 連絡先メールアドレスを指定して診断終了の通知を待つ.

終了通知メールには診断結果の URL が記され, 診断時と同じユーザ名／パスワードを使って診断結果を閲覧できる. また診断結果は apache のディレクトリインデックス機能によりこれまでのものと合わせて一覧表示され, 前回診断との異同を確認することができる.

3.5 利用者端末の診断機能

3. 3節の追加に至った要因は, サーバとして用いられる端末が原因となる場合に加えて, 通常はサーバ機能を用いない端末である機器も加害ならびに被害の対象となる. そのため, これまでの診断結果を受け取る管理者への利用環境に加えて, 端末の利用者が自身で診断できるようにこの機能を追加した. もともとこれら端末の利用者は, 属する管理者より診断結果についての連絡があったと予想されることから, 管理者と同様に確認手段は必要であった.

管理者の場合と異なり登録されていない利用者がこの機能を利用するため, 診断には別途認証による記録を残す. 認証情報は昨年度稼動を開始した学内の全構成員が登録されている全学的な認証基盤[6]に対応し, SSL経由のLDAPを通信に用いる. 本機能を利用可能な対象者の数が管理者に比べて2桁以上多く, 最大2万程度となるため診断結果をサーバ側で保持する期間を1週間に限り, 8 日後に自動削除とした. 診断対象が現在利用中の(診断システムにアクセス中の)IPアドレスに限定される点のみ異なる.

3.6 機能提供の方針

この様な運用方針とする際に確認した事は以下の通りである. 管理者用は, 本システムの開発目的である診断を受ける側の確認手段としてこの機能を提供する

事に問題無いという判断である.

スタッフ用は問い合わせや苦情があった場合の確認や,侵入などの被害にあった場合に利用されたと思われるセキュリティホールを過去の診断結果より確認することなどに利用するため,可能な診断対象は自組織内全てとし,また全ての診断の結果が確認できる.

利用者端末用は,現在使用中の機器を確認する事で問題無いという判断である.

4 システムの運用・評価

4.1 運用事例

本学では2000年度より本学のアドレス空間に対してセンターによる一括脆弱性診断を実施しており,昨年度からは診断結果をユーザ名/パスワード認証付きWEBページにより通知している.現在の実装では本システムの管理者用の認証このパスワードを流用しているが,今後は利用者端末用と同じく学内の認証基盤に対応を予定し準備中である.本システムは複数台の診断サーバによって負荷分散するため,診断するネットワーク規模に応じた診断性能を持たせることができ,一部の診断サーバに障害が起きた時にも応答が無いサーバは利用しないため本システムは利用可能である.診断サーバの保守作業時には,WWW サーバ側の診断サーバ設定を一時的に半数のみを利用するように変更し2回に分けて作業を行うなど設定により柔軟に構成変更可能である.また,現在診断サーバを10台用意しており,定期的な診断にも兼用している.

本システムの稼動開始時に用意した機能は以下の(1),(2)であり(3)は文献[3]の時点では未確定であったが以下のとおり運用を開始した.

(1)サブネット管理者用　サブネット管理者が担当する24ビット長で割り当てられたサブネットアドレスで,4オクテット目が10－254の範囲のみを診断可能.(本学においてサブネット管理者とは,割り当てられたネットワーク範囲を担当し,管理範囲内のネットワーク利用についての問い合わせ窓口も兼ねる)

(2)センタースタッフ用　自組織に割り当てられたアドレス空間全体を診断可能であり,全ての診断結果の閲覧が可能である.

(3)利用者の端末用　診断用 WEB ページにアクセスしている現在使用中のホストのみ診断可能.

4.2 評価

2003年7月16日にセンタースタッフへ,8月7日に学内の管理者へ公開した.処理能力は診断サーバの性能に依存するが,現在まで問題無く動作中である.

4.2.1 診断時間の評価

最近の PC や Linux サーバ等は,OS にファイアウォール機能を内蔵するものが多く,ICMP や特定のポート番号でホストの存在を確認するができないため,診断の最適化による時間短縮が出来にくい.ファイアウォールの有無での診断時間の差は,PC 1台(OS Windows XP Pro/Dual Athlon1.8GHz)で比較すると,ファイアウォールを無効に設定した場合約1分で終了するのに対して,有効の場合は約17分を要し,他のホストでも平均すると20分前後の時間を要する.

4.2.2 診断サーバの処理能力の評価

本システムで利用した NESSUS の場合,診断対象1台の1項目を1プロセスで診断し,本スペックの診断サーバではプロセスが200を超えるとロードアベレージが1を大きく超える.現在の運用では,1回の診断リクエスト処理に対象5台を各10項目同時に診断する計50プロセスで行うように設定しており,1台あたり最大5箇所を超えると過負荷により診断時間が増加する.10 台の診断サーバに負荷分散させるため,全体で50程度のリクエストが処理可能である.全診断サーバで収容しきれない数の診断リクエストが来た場合は混雑中として,後ほど再度リクエストを出すよう促しているが,現在までその状態には至っていない.利用が見込まれる場合は,診断サーバの増設も容易であるため今後も問題とならないと判断している.

4.2.3 WWW サーバの処理能力の評価

WWW サーバは診断受け付け時に SSH を用いて複数の診断サーバに対し一斉に通信し,リクエスト先を検索するため,SSH 通信開始オーバヘッドにより若干の処理負荷がかかり10秒程度の待ち時間が発生する.しかし,同時5～6程度の診断リクエストであれば待ち時間なく処理を開始している.

4.2.4 診断システム利用の評価

(1)サブネット管理者用　図4の中では8月7日の開始案内,8月21,22,27日に臨時診断を実施しておりその前後に増加がみられる.診断結果の対策確認や,セキュリティホールを利用したワーム等の流行した時期でもあり利用が増加したことがわかる.

(2)センタースタッフ用　定期診断は自動で行いこの診断ページを利用することはないため,主にセンター内の脆弱性確認やセンター宛に情報が寄せられたワーム感染ホストの確認などに利用されている.これらの診断結果には,同一のホストに連続して診断し,診

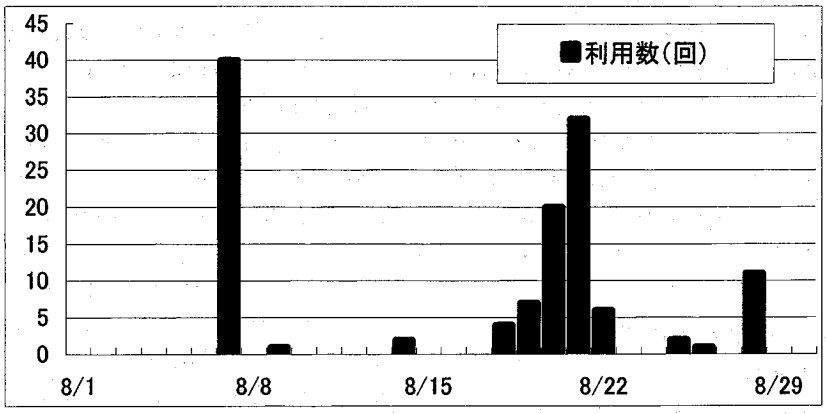

図4. 診断システムの1日の利用数(2003年8月分)

断結果の警告数が減少した例があるなど，本システムを利用し対策を行ったと思われる結果があり有効に利用されていると判断できる.

4．2．5 求められる機能の評価

2.4 節の求められる機能①に対して，診断開始までの時間 (4.2.3 節)，診断に必要な時間 (4.2.1 節)，また同時に処理可能な診断数(4.2.2 節)より，本システムは利用者にオンデマンドでの診断機能を十分提供していると判断している.

機能②に対しては，利用している診断結果の表示が診断ソフトの機能により対策例の付いたものであり，OS 毎の具体的な対応例や手順，関連情報，などへのリンクを追加して用意する診断結果の補足を講じた．また，診断内容の選択機能を用意した機能⑤は利用記録より多数利用されており診断時間の短縮や診断結果の情報量抑制の効果があったと考えている.

機能③に対しては，全構成員に診断機能を提供しており，一括して行う診断では収集できないであろう診断期間外に導入された機器などの診断に本システムを利用することで組織全体のセキュリティレベルの維持に有効である.

5．おわりに

本研究では学内の管理者やセンタースタッフ，端末の利用者を対象としたシステムを開発し，運用を開始した．現在も稼動中で多くの利用記録があり，大きな不具合や停止，利用者の混乱も生じていないことから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，構成員のセキュリティ意識の向上や，残存するセキュリティホールの減少，ワーム被害や外部からの苦情の減少が期待される．しかし，現在までの運用実績だけではまだ十分評価できる状態には至っておらず，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など今後の課題としたい．その他，利用者端末用の診断ページへブラウザを持たない機器(プリンタやブロードバンドルータなど)を同じ管理範囲内であれば診断できる機能の追加や，診断結果に OS 毎の具体的な対策例やその手順，関連情報の情報をより充実させることが課題として挙げられる.

謝辞

本システムの開発・支援・運営は広島大学情報メディア教育研究センター[7]のスタッフ，中国・四国インターネット協議会[8]の協力を得ています．ここに記して謝意を表します.

参考文献

[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] Internet Scanner. http://www.isskk.co.jp/

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

[6] 広島大学全学電子認証システム http://auth.hiroshima-u.ac.jp/

[7] 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/

[8] 中国・四国インターネット協議会 http://www.csi.ad.jp/