

## 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決して小さくはない。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

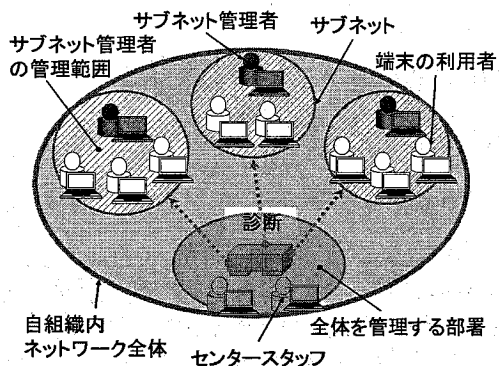


図1. 管理に関する概念図

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、必要な労力は決して小さくない。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。

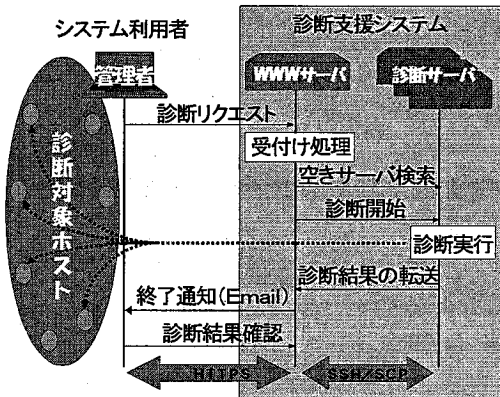


図2. システム構成図

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仕様を表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. ハードウェア仕様

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要となる。

#### 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

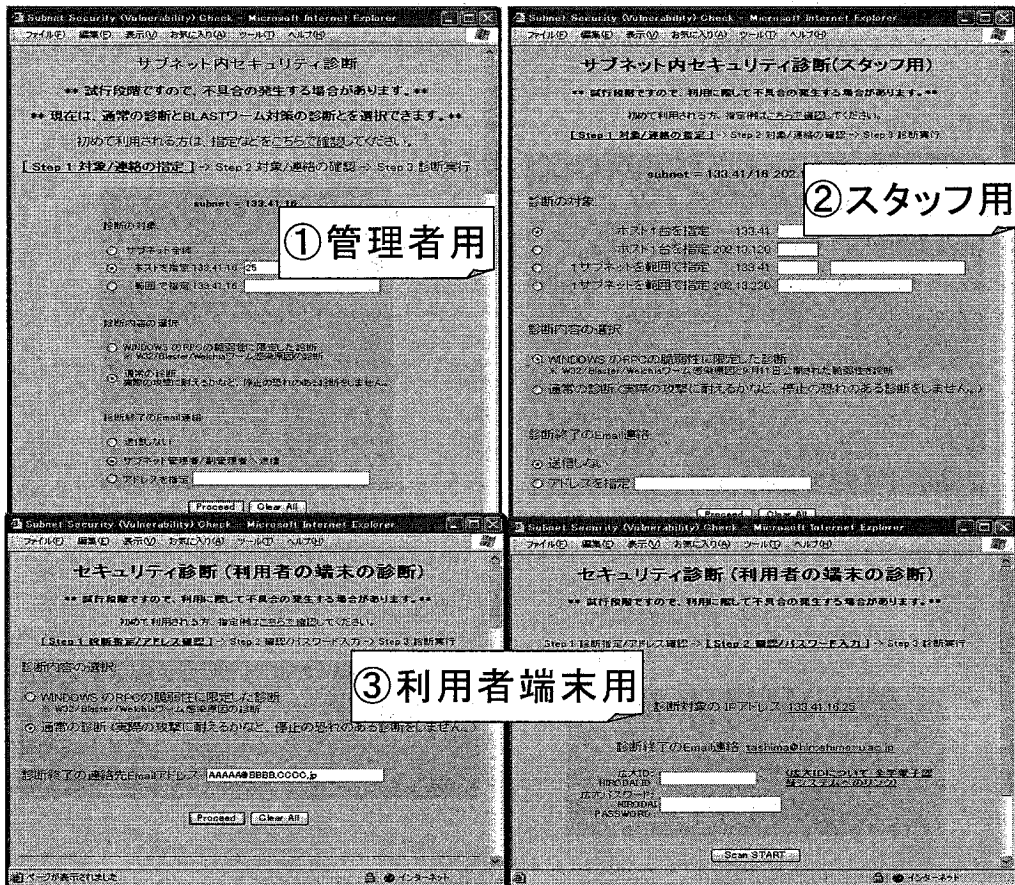


図3. ユーザインタフェース

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働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

このよう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

