2003－DSM－30　(3)
2003／9／26

セキュリティ脆弱性診断支援システム

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として，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必要な大規模組織においても，脆弱性診断を一括実施することでコストを大幅に低減した診断ができる．しかし各管理者にとっては，自らが分掌するネットワーク内にほどこしたセキュリティ対策の有効性を即座にかつ容易に診断できる環境が必要である．これらの要求に応えるオンデマンド性を備えたセキュリティ脆弱性診断支援システムの構築について，実際の運用事例とともに報告する．

Security Vulnerability Check Support System

Kouichi Tashima Kouji Nishimura Seigo Kishiba Reiji Aibara

Information Media Center Hiroshima University

It is well known that diagnosis using a vulnerability checking tools is effective method for security maintenance in network management.　Also in the large-scale organization which many network administrators need, collective diagnosis can be run with low cost than non-collective one. However, each administrator needs environment of easy and immediate diagnosis, to verify security maintenance for managed network.　We report about the security vulnerability check support system with expectation of on demand requests, and its practical running case.

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．企業のように情報部門が一括してネットワークや端末を管理する場合とは異なり，大学の例で研究室のＰＣまでセンターが集中管理することは非現実的な場合，学部や部局等の単位で管理権限を分割委譲する必要があり，一例を図１に示す．この場合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にかかる労力はけして小さくは無い．

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一括して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 [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 [2]

などがあり，さらに一括調査によって得られたセキュリティ情報をネットワーク管理に有効活用する手法[3]についても報告されている．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となる．本稿ではこの要求に応えるためにセキュリティ脆弱性診断支援システムに求められる要件について，実際の運用事例とともに報告する．

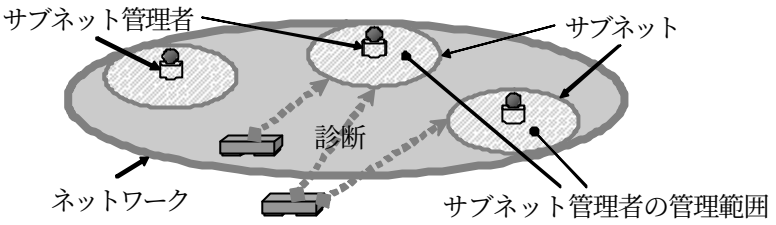

図１．管理に関する概念図

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（例えば[4]）．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かかってしまう．

２．２　セキュリティ診断ソフトウェアの利用

いっぽう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．診断に使用するソフトウェアとしては広範囲の脆弱性や設定などを診断対象としており脆弱性情報への対応も早いISS社の製品 Internet Scanner [5]やNESSUS [6]などがある．大学においてもこれらのソフトウェアが利用されている事例や導入計画がある（東京大学：サービスの解説[7]，北海道大学：導入計画[8]）．

２．３　診断への要求

ネットワークを分割して管理する場合，ネットワークの脆弱性診断を実施するのは分割した各ネットワークの管理者である．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，ネットワーク全体として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を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．

２．４　セキュリティ診断に求められる機能

２．３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
③診断のためのハードウェア・ソフトウェアの提供

ネットワーク全体を統括するセンターの立場からは以下の要求がある．

④組織全体でセキュリティレベルを統一
⑤組織全体のセキュリティ情報を一元管理

本システムでは一定の診断ソフトを搭載した診断サーバをセンターで設置して定期・不定期に脆弱性診断を実施することによって④をみたすとともに，診断サーバに各管理者が自分の管理するネットワークの脆弱性診断を容易に実行可能な利用インタフェースを用意することで①③と⑤を同時に実現する．また診断サーバを複数台で構成することによってネットワーク規模に応じた診断性能を確保し，診断結果の作成速度の点からもオンデマンド性を確保する．②については，診断結果表示は診断ソフトの機能により詳細な説明の付いたわかりやすいものになっている．

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．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．

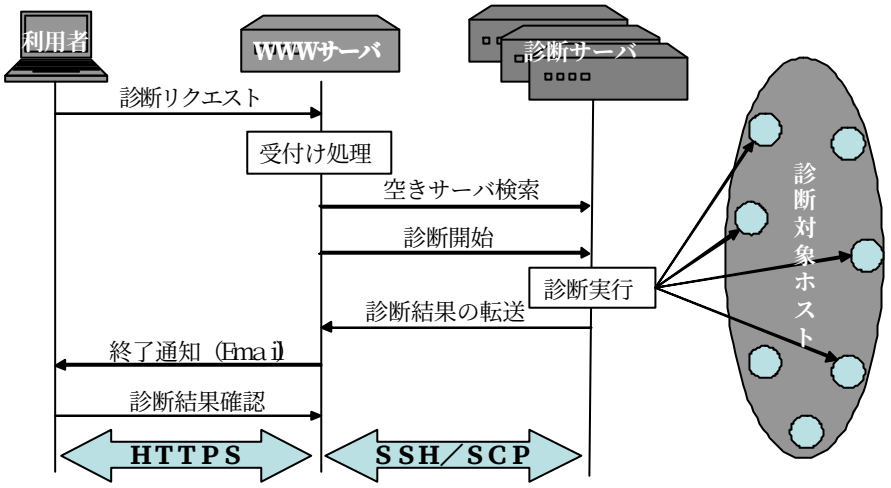

図２．システム構成図

表１．使用サーバソフト

WWWサーバ	Apache_1.3.27
サーバ間通信	OpenSSH 3.4p1
診断ソフト	NESSUS 2.07

表２．ハードウェアスペック

WWWサーバ	SOLARIS 7	ULTRASparc200MHz mem256MB
診断サーバ	LINUX 2.4.7	Celeron900MHz mem128M

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．

３．２　ユーザインターフェース

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，本システム開発以前の 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．

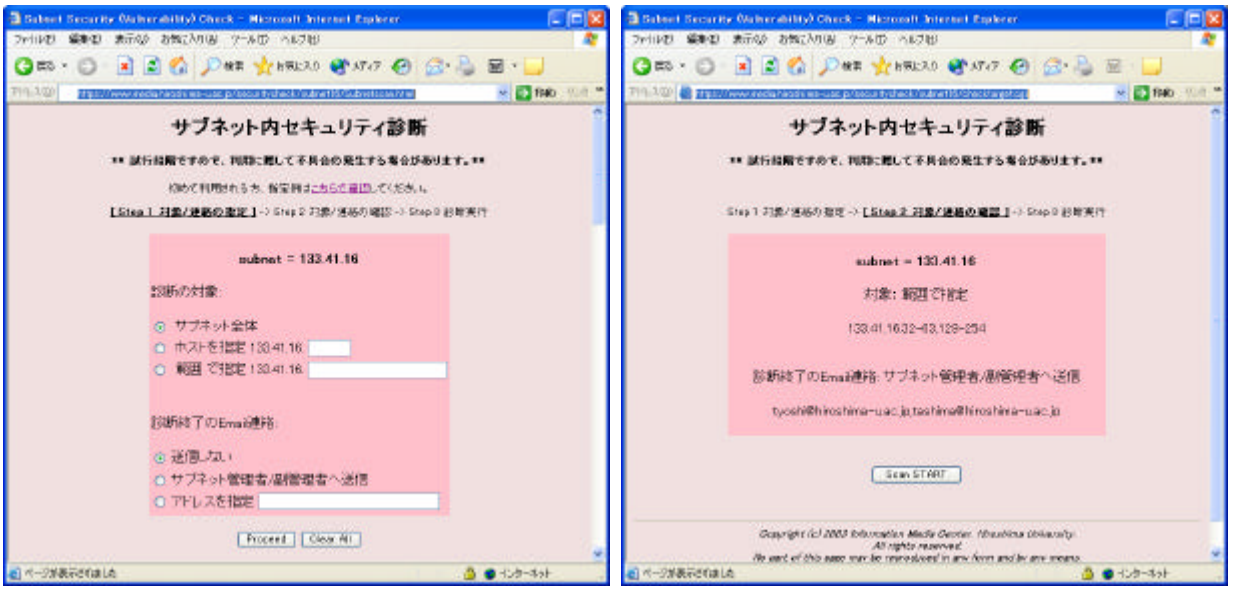

図３．ユーザインターフェース

３．３　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３左画面）．選択・記入事項に問題が無ければ確認画面（図３右画面）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ＨＴＭＬ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．管理者が交代した場合の診断結果の引継ぎも容易である．

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利用時認証にこのパスワードを流用しているが，これについては昨年度稼動を開始した学内の全学的な認証基盤[9]に対応を予定している．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，一部のサーバが障害を起こした時にも利用可能である．本システムでは現在診断サーバを１０台用意しており，定期的な診断にも兼用している．

本システムの利用メニューには以下のものがある．

（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するネットワーク管理者であり，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

（※センタースタッフとは基幹ネットワークならびに基幹ネットワークサーバを管理し，全体のサブネットの管理を担当する．）自組織に割り当てられたアドレス空間全体を診断可能．

（３）各端末の利用者用

脆弱性診断ページにアクセスする端末１台のみを診断可能とする機能だが，現在はまだ運用方法の検討中．

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現在までのところ大きなトラブル無く動作しているが，システムの処理能力には診断サーバのハードウェア性能に依存した制約がある．診断内容を診断対象ホストの OS 検出などによる最適化をしない全項目を診断した場合には，診断サーバ１台あたり５箇所を超える診断を同時に実施するとロードアベレージが大きく１を超えた状態が続くため，診断サーバ１台が同時に診断するのは５箇所までとした．全サーバでも収容しきれない数の診断リクエストが行われた場合は混雑中として受け付けず，後ほど再度開始リクエストを出すよう促しているが，現在のところその状態には至っていない．WEB サーバについては診断受付時に SSH を用いて多数の診断サーバに対し一斉にリクエストを発行するため，通信オーバヘッドにより若干の処理負荷がかかる．しかし５～６箇所程度のリクエストならばほぼ待ち時間なしで処理を開始している．

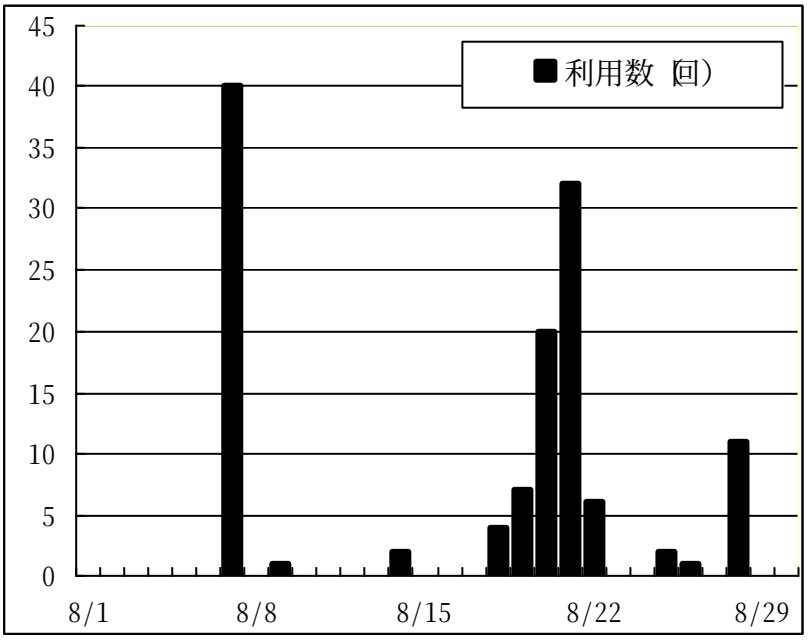

図４．診断システムの１日の利用数（2003 年８月分）

４．１の利用形態（１）～（３）についての評価を行う．

（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 日に臨時診断を案内し実施しておりその前後に増加がみられる．診断の結果通知後の対策確認や，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

定期的な脆弱性診断は自動で行っており，この診断ページを利用することはない．主にセンター内の脆弱性確認やアドレスの利用状況確認に利用されている．また，外部機関等からセンター宛に情報が寄せられたワーム感染ホストのセキュリティホール確認に利用されている．

（３）各端末の利用者用

現在まだ運用を開始していない．これは未解決の課題が多く残っているためである．たとえばPROXY 経由でのアクセスの場合, PROXY サーバを診断することになり利用者の意図とは異なる結果になる．また逆にアクセス端末本体ではなく手近にあるブラウザを持たない機器，たとえばプリンタやブロードバンドルータなどを診断したい要求に対して，診断の実施方法や認証の問題が未解決である．

5．おわりに

本システムは学内のサブネット管理者やセンタースタッフを対象として現在も稼動中であり，多くの利用記録が残されていること，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できる．本システム導入の具体的な効果として，ネットワークホストに残存するセキュリティホールの減少やワームによる被害の減少が期待されるが，現在はまだその評価には至っておらず今後の課題としたい．

その他の課題としては，端末利用者用ページの運用開始の障害になっている問題の解決のほか，診断実施者が診断結果に対する対策を容易に行えるように診断後のサポートをきめ細かくする事が必要と思われる．

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[10]のスタッフ，中国・四国インターネット協議会[11]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, 2002

[3] 萱島 信，寺田 真敏，永井 康彦，礒川 弘実，統合セキュリティ運用管理システムの提案，情報処理学会 CSEC 研究会報告 Vol. 2000, No. 011-015, 2000

[4] 日立システム＆サービス http://www.hitachi-system.co.jp/security/

[5] Internet Scanner (ISS co.) http://www.isskk.co.jp/

[6] NESSUS Security Scanner http://www.nessus.org/

[7] 東京大学 http://www.itc.u-tokyo.ac.jp/Seminar/007_20000811/

[8] 北海道大学 http://www.hokudai.ac.jp/hines/HINESworld/No.52/hw52_3.html

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

[10] 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/

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