様式 C-19

科学研究費補助金研究成果報告書

平成 21 年　6 月　4 日現在

研究種目：若手研究（B）
研究期間：2006　～　2008
課題番号：18700063
研究課題名（和文）　セキュリティ脆弱性診断支援システムの研究開発

研究課題名（英文）　Research and development of vulnerability diagnosis system for computer security

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

研究成果の概要：

ネットワークの管理者など，情報システムやパソコン等の管理者が，機器のセキュリティが気になる時にその確認ができるような，セキュリティの脆弱性診断を支援するシステムの研究開発を行った．研究開発したシステムを，所属する，全学の情報システムやネットワーク等を管理している情報センター部署で日頃の管理の一環として利用し，利用統計や利用の結果より組織内のコンピュータ脆弱性の改善例が多く得られその有効性が確認され，また効果的であったセキュリティ脆弱性診断支援システムの構成方法について，構築事例として一例を示した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	900,000	0	900,000
2007 年度	500,000	0	500,000
2008 年度	500,000	150,000	650,000
年度			
年度			
総　計	1,900,000	150,000	2,050,000

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：セキュリティ診断

１．研究開始当初の背景

パソコンやサーバなどネットワークに接続して使う機器を，ネットワークを経由した攻撃やワームなどの被害や妨害の脅威から安全に使うため，その安全性を セキュリティ脆弱性診断 で確認する方法があるが，主に次の ３項目の要因 が理由となり多くの組織では利用されていない．その理由として，まず「診断ツールは技術的な知識を持ついわゆる管理者向けに作られている事」があげられ，他にも「診断のためにサーバやソフトの設置や設定・指定などに手間やコストが必要な事」，「機器の脆弱性情報は，程度によるものの診断結果には欲しい情報以外にも多くの警告や注意点を含む場合が多い事」などがあげられる．診断を実施したい利用者に対して，これらの障壁を感じさせる事なく診断を行えるシステムについて，診断に必要なシステムの実装とその実環境での運用により調査研究を行う事とした．

２．研究の目的

本研究課題では，セキュリティ脆弱性診断の利用について，それを支援するシステムの開発及び実際の運用利用による評価を行い，既存の問題点である「利用するために必要とされる高度な技術的な知識」「診断を行うため手間やコスト」「セキュリティ対策に利用する際により効果の得られる診断内容の最適化」の見直しを重点的に行い，システムの構成や機能をどのように実装すれば，より利用しやすいシステムになるのかを明らかにする事を目的とした．

また，このシステムのイメージするコンセプトは，電子メールが使いたいときにはメールサーバを，ホームページを開設したい場合には WEB サーバをそれぞれ利用するという使い勝手で， 診断支援システムを利用してセキュリティ脆弱性診断を行える事を目標とした．

３．研究の方法

（１）本研究は，前述の脆弱性診断支援システムの調査・研究及びその開発であるが，目的で述べた実際に運用しての運用評価を行い本当に使えるシステムであるのかという検証を行うため，主に利用者の技術的なレベルを考慮してシステムの実装を次の 1)～3)の３段階に分けて行い，年度毎に対象者を拡大するようにシステム開発とその運用を開始した．

1) 組織全体の維持管理及び，学内の管理者との管理的な対応を行う情報センター職員向けの機能

2) 学内の部分ネットワークの管理を行うネットワークの管理者

3) 研究室などに用意された端末や，自分で持参したパソコン等の利用者

研究の進捗に応じて，随時研究開発の成果を学内ＬＡＮの運用に用いることで，研究成果の検証をあわせて行った．

（２）本研究開発において，実際にセキュリティ脆弱性診断を行う機能部分を実装する診断サーバ側には，診断ツールとしてオープンソースのセキュリティ診断ソフトウェアＮＥＳＳＵＳを利用した．ＮＥＳＳＵＳは診断機能の変更や拡張が比較的容易に行える簡易言語方式で提供され修正が容易に行えるようになっており，この機能により診断にかかる時間短縮の調整や，ここで対象とするセンター職員に適した診断結果（より詳しい情報を含むように）となるように診断項目の選択といった診断内容の見直しを行った．あわせて，前回の診断結果との差分によりどの程度改善されているのかを確認できる比較機能や前回問題のあった点のみを短時間で再確認できる機能の実装等を行った．

利用イメージは図１の通りであり，システムを利用する者は WEB ブラウザを用いてシステムにアクセスを行い，①～⑥の流れで診断の実行と診断結果の確認を行う事とし，このように構成する事で，簡単な WEB 操作により管理範囲内のセキュリティ診断を容易に行えた事が，図２および図３の利用における操作ログやアクセスログから確認できた．

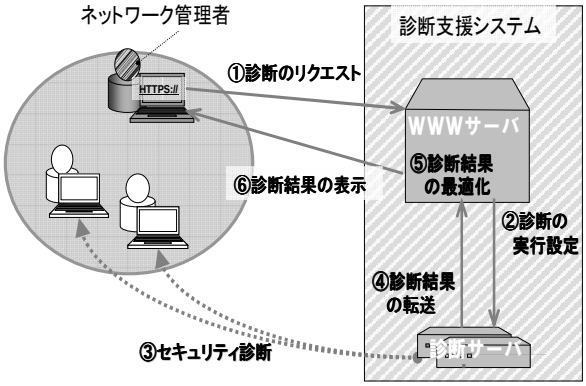

図１診断支援システムの利用イメージ

４．研究成果

（１）本研究では，診断実行の支援システムの構築やその運用，及び，診断結果の配布までをオープンソースの診断ツール等を用いる事で開発およびシステムの随時見直し等が円滑に行え，診断支援システムの構築およびこれを用いたセキュリティ対策についての報告等を行った．この報告では，キャンパスネットワークの実際の運用で用いた評価を行い，診断支援システムの利用により，以下の図２，図３の通り多くのシステムが脆弱であるかどうかの確認，および，利用した結果により診断結果に含まれる警告数の減少が多く見られ，組織内に診断支援システムを設置し構成員に利用を推奨することで，論文や研究発表等では具体的な数値は示していないが，診断結果の警告数には減少が見られ，セキュリティ向上が確認された．特に，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の増加や診断ソフトの改善等によるチェック項目数の増加を考慮すると，このようなシステムの利用は効果的であった．

また，同様の手法を他の組織でも行う事で各組織内のセキュリティ対策がより簡易に行う事ができ，セキュリティの向上が期待される．

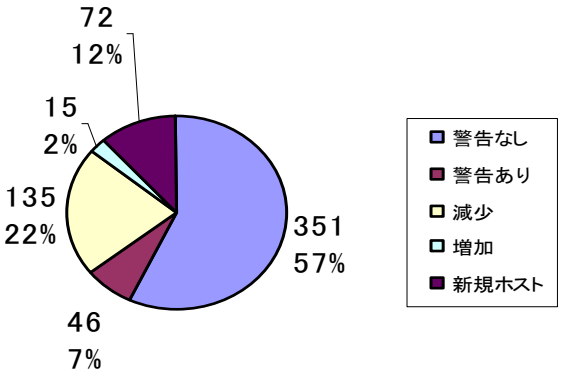

図２管理者向けの診断支援システムの利用結果

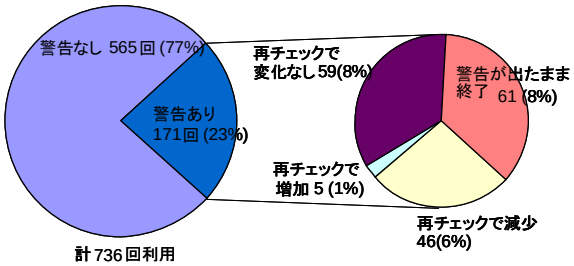

図３端末の利用者向けの診断支援システムの利用結果

（２）セキュリティを考慮したシステム構築について，一例としてキャンパスネットワーク構築について，ここで用いられる管理情報等の管理システムと診断支援システムとの間での連動方法やその構築事例について論文発表を行った．ここではネットワークの管理範囲＝セキュリティ管理の範囲とし，管理者情報を一元管理とする事で比較的大規模なキャンパスネットワークにおいても，図４の様な設置例とし，連動する事を想定した図５のシステム構成とすることで運用等のコストを低減した診断環境の構築ができた．

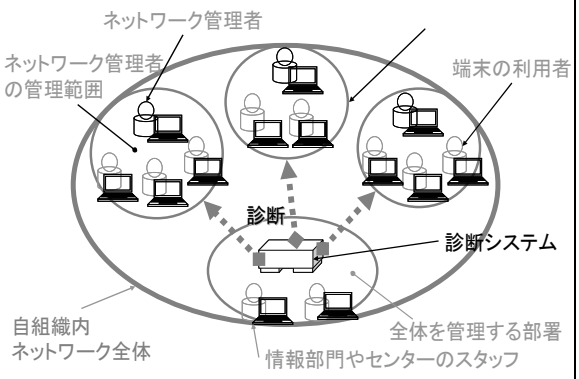

図４キャンパスネットワーク構築における診断システムの設置環境

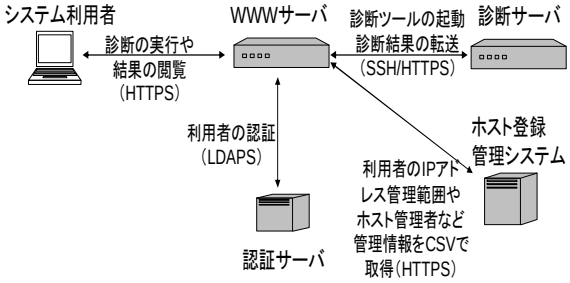

図５診断支援システムのネットワーク管理システムとの連携構成

また，図５は本研究で行った構成例であるが，図５中での認証サーバを利用したＬＤＡＰＳでの認証や，ＷＥＢインタフェースを持つ管理システムとの管理情報へのアクセスなどは一般的な構成であり，他の組織でも同様のシステム構成がされていると考えられ，同様の手法が適用可能と考えられる．

（３）本研究では，診断実行の支援システムの構築について，組織内のネットワーク管理者等システムの利用者が使いやすい診断支援システムの構築にターゲットを絞って研究開発およびその運用を行ってきたが，同様のシステムを他の組織で導入する場合には，どうしても，構築自体にある程度の作業が発生することがさけられないという問題点もあり，多機能なオープンソースや商用の診断ツールもそれぞれ一長一短があるため，それらを標準化されたツールやＡＰＩにより選択的利用できる診断支援システムの構築環境について，現在は研究開発を行っている．

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１件）

① 田島浩一, 西村浩二, 近堂徹, 岸場清悟, 相原玲二，ホスト登録を用いたネットワーク認証システムの実装と評価，学術情報処理研究 No. 11 pp. 42-49，2007 査読有り

〔学会発表〕（計４件）

① 田島 浩一，岸場 清悟，近堂 徹，大東俊博，西村 浩二，相原 玲二，複数の脆弱性診断ツールを用いたセキュリティ診断支援システムの構築, マルチメディア, 分散, 協調とモバイル DICOMO 2009 シンポジウム，（予稿集は

CDROMとオンラインのみ), 2009年7月9日 査読有り　@大分県別府市

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アドレス認証の管理手法, 電子情報通信学会技術研究報告 IA2008-112, vol.108, no.460, pp. 265-270, 2009年3月6日, 査読無し　@熊本県阿蘇郡南阿蘇村

③ 田島 浩一, 西村 浩二, 岸場 清悟, 相原 玲二, 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, 情報処理学会 EVA 研究会報告 Vol.2008, no.30, pp.1-6, 2008年3月19日, 査読無し　@広島県東広島市

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を用いたセキュリティ対策とその評価, DICOMO2007 シンポジウム, pp.851-856, 2007年7月5日, 査読有り　@三重県鳥羽市

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

(2)研究分担者

(3)連携研究者