マルチメディア通信と分散処理　106－29
コンピュータセキュリティ　16－29
（２００２．２．１５）

セキュアNW動的再構築システムの検討

佐藤亮介　　種茂文之
{ryousuke,tanemo}@isl.ntt.co.jp

日本電信電話株式会社 情報流通プラットフォーム研究所
〒239-0847 神奈川県 横須賀市 光の丘 1-1

概要

近年インターネット上のホストマシンのセキュリティホールや設定ミス等をついた攻撃による被害件数が増えてきている。それらの攻撃は、ホストマシンの管理者が適切な設定やバージョンアップを行っていれば被害を受けることは少ないが、実際には技術者不足や管理者の認識不足により適切対策が取られていることが少ないのが現状である。そこで、本稿ではインターネット上の各種のサーバホストや FW や IDS 等のネットワーク構成装置に専用のエージェントプログラムを配置し、新たなセキュリティホール情報がシステムに入力されると同時に適切な対処策をエージェントプログラムに配信することによって、各種サーバホストマシンやネットワーク構成装置上での対策をエージェントプログラムが自動的に行うシステムを提案する。

A Study on a Dynamic Reconfiguration System to Keep a Network in a Secure Condition

Ryousuke SATO　　Fumiyuki TANEMO
{ryousuke, tanemo}@isl.ntt.co.jp

NTT Information Sharing Platform Laboratories
1-1 Hikarinooka, Yokosuka, Kanagawa, 239-0847, JAPAN

Abstract

Recently, attacks on Internet hosts have been increasing at an alarming rate. While these attacks can be easily prevented by proper system configuration, host machines are often left unprotected due to the lack of security technicians and awareness of security issues.

In this paper, we propose a new system that constantly keeps host machines secure. The basic idea is to dispatch small software agents to host machines that are to be protected. These agents await for commands from the system management module. On discovering new security holes, the system management module remotely instructs all agents to deploy countermeasures for the protected hosts and constantly keep these hosts immune to new threats.

1. はじめに

近年インターネット上のホストマシンのセキュリティホールや設定ミス等をついた攻撃による被害件数が増加している[1]。それらの攻撃は、ホストマシンの管理者が適切な設定やサーバソフトウェアのバージョンアップを適切に行っていれば被害を受けることは少ないが、実際には技術者不足や管理者の認識不足により適切な対策が取られているこ

とが少ないのが現状である。また、管理者の意識が高く日々セキュリティホール対策を行っているサイトにおいても、頻発するセキュリティホール発見とソフトウェアのバージョンアップやパッチのリリースにキャッチアップするだけでも膨大な作業となり、管理組織の人的リソースを圧迫している。

そこで、本稿では新たなセキュリティホール発見の情報と同時に、システム配下のホストについてセキュリティホールの検査を行い、問題が発見されかつ自動対処が可能なケースについては、エージェントプログラムを介して対処を自動実行するネットワークセキュリティ管理サービスを実現するシステムの提案を行う。

本稿の第 2 章で現行手法の問題点を明らかにし、第 3 章で必要機能の詳細化を行い、第 4 章で検討方式の動作の詳細について述べる。第 5 章で本システムを用いたサービス例を示し、第 6 章でまとめを述べる。

2. 現行手法の問題点

現行のセキュリティホールへの対処方式では、ネットワークのセキュリティ担当者が次に挙げるような手順を踏んでいるケースが多い[2]。

1. 新しいセキュリティホールの情報入手
2. 新しいセキュリティホールが自ネットワーク上のホストに影響を及ぼすか否かを、ホストマシンの情報とセキュリティホールの情報を照らし合わせてホストマシン毎に判断する。
3. 新たなセキュリティホールが自ネットワーク上のホストマシンに影響を及ぼすと判断される場合には、ホストマシン毎の対処策を策定して、ホストマシン毎に対処を実施する。

このような方式は、管理対象がごく限られている環境下では機能する可能性があるが、管理対象が増えた場合やネットワークサービスとしてセキュリティ管理を提供する場合には手間が掛かりすぎるために破綻してしまうことが容易に想像できる。

上記のスケーラビリティの問題以外にも、全てのインターネット上の各種サーバホスト毎に、常にセキュリティ情報を収集している専任の管理者がついているか否か、セキュリティ情報から自分のホストマシンが影響を受けるか否かを管理者が判断できるかどうか、影響を受けると判断した際にホストマシン毎に正確かつ適切な対処を管理者が行うことが出来るか否か、新しいセキュリティホールの発見の報告と同時にセキュリティホールへの対策を行うことが出来るか否かという様な、ホストマシンを管理する管理者のスキルや稼動等についての問題も考慮しなければならない。

また、セキュリティホールの存在確認の為に市販のリモートセキュリティ診断ツール[1]を用いて診断を行っているケースも多い。リモートセキュリティ診断ツールは、発表されるセキュリティホール情報のうち、どのセキュリティホールが管理下のサーバホストに存在しているのかの選別に利用し、セキュリティホール存在確認の手間を削減することが出来る。しかしながら、リモートセキュリティ診断ツールが必ずしも正しい診断結果を返してくるとは限らない。なぜならリモートセキュリティ診断ツールは診断対象ホストに関する情報のうち、特定のパケットに対して診断対象ホストがどのようなパケットを返してくるのかという情報しか判断に用いていないからである。そのため、外部からのパケットを遮断しているようなサービスに関する診断項目については正しい結果を得られない等のケースが考えられる。ローカルセキュリティ診断ツール[2]を用いると、診断対象毎にシステムの設定ファイルなどの情報を使ってよりきめ細かな診断を行うことが可能となり、リモートセキュリティ診断ツールでは診断できなかったことについても診断できるものの、現状では確認の意味もこめてリモートセキュリティ診断ツールも併用するのが一般的であり、システマティックにリモート、ローカルの診断を行う仕組みがない。また、ローカルセキュリティ診断ツールの診断結果を参照して適切な対処策をホスト毎に適用する能力も管理者に求められる。

このような多様な問題を十分に理解し、適切に処理できるスキルを持った管理者は少なく、結果

[1] 代表的な製品に ISS 社の InternetScanner™等がある。
[2] 代表的な製品に ISS 社の SystemScanner™等がある。

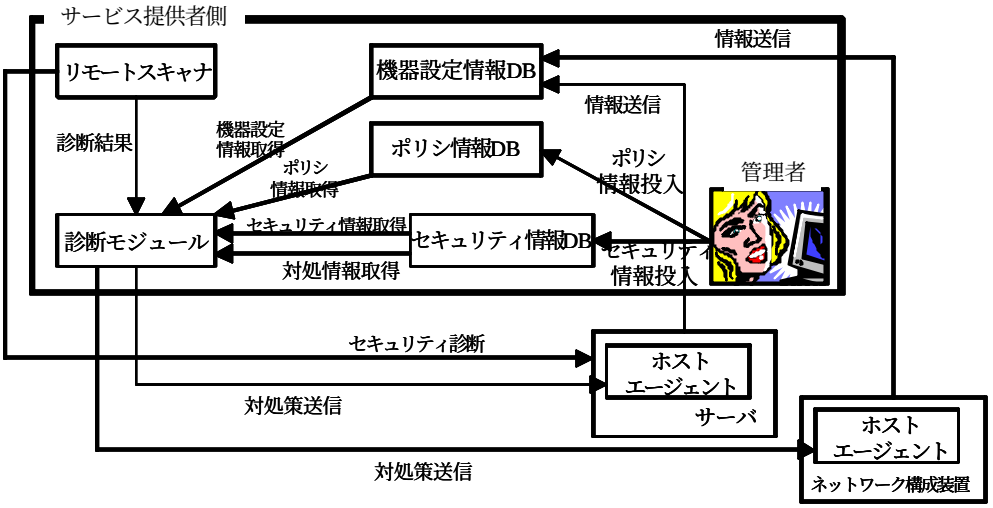

図1 本方式の機能ブロック

としてインターネット上のホストマシンで十分な対策が取られていないケースが多い。

3. セキュア NW 動的再構築システムの検討

2 章で述べた問題点を解決するネットワークセキュリティ管理サービスを実現するために、次の４つの項目について検討を行った。

① リモート診断、ローカル診断を組み合わせた信頼性の高い診断方法の提供
② 診断結果に基づいた OS、アプリケーションサーバ(web,mail,dns)に関するセキュリティホールへの対処の自動化
③ 新しいセキュリティホール発見と同時に自動的に診断、対処を行う仕組み
④ ネットワーク装置の設定の自動化

項目①では、リモート診断及び従来のローカル診断相当の機能をサービス提供者が実施する。このうち、サービス提供者側でのローカル診断相当の機能を実施するためには、ユーザの機器設定情報をサービス提供者に送信し、サービス提供者が持つセキュリティホール情報に基づき、ユーザのサーバホスト上にセキュリティホールがあるか否かを判断する機能が必要となる。リモート診断の結果についても、ローカル診断と同様のセキュリティホール情報及び機器設定情報に基づき、セキュリティホールの有無の確認や、セキュリティホールの原因の特定等について解析が可能となる。

項目②では、項目①の診断結果を用いて、サーバホストやアプリケーションサーバの設定を変更等することにより行う。これは、項目①で受信した機器設定情報を自動的に編集して、サーバホストに送信して再設定の実施又は、サーバホスト上で実行すべきコマンドを記載したスクリプトを送信して実施等の方法で行う。この際必要となる機器の再設定方法やコマンドスクリプトについては、ベースとなるデータをセキュリティホール情報の項目に対応させて保持する必要がある。

項目③は頻発するセキュリティホール情報追加に追随し、常にユーザネットワークをセキュアな状態にするために必要であり、サービス提供者がセキュリティホール情報を追加したことを契機として、直ちに項目①の診断と項目②の自動対処を行うことで実現可能である。

項目④は、FW や IDS 等のネットワーク構成装置(サービス提供者管理)によりユーザネットワークをセキュアな状態にすることを想定している。これは、ユーザの提供サービス等の情報を予め登録し、これに基づきネットワーク構成装置を制御することにより実現可能である。

・ ホストエージェント：サーバホストやネットワ

ーク構成装置に導入され、設定情報送信や、対処策の受信、実行を行う。

- 機器設定情報 DB：ホストエージェントが送信したの設定情報を格納している。
- セキュリティ情報 DB：セキュリティホール情報を収集して DB 化。セキュリティホールに関する情報と対処方法等の情報を格納。
- ポリシ情報DB： ユーザのネットワーク利用ポリシを格納している。
- 診断モジュール：セキュリティホールの存在の有無を診断する機能、セキュリティホールへの対処策を DB から抽出する機能、ホストエージェントに向けて対処策を送信する機能、ポリシ情報DB の内容を分析する機能を有する。本モジュールはシステムで中心的な役割を果たす。

4. 動作詳細

次にセキュア NW 動的再構築システムの詳細な動作方式について述べる。セキュア NW 動的再構築システムでは、4 つのフェーズからなる。まず、各フェーズの動作概要について説明する。

- 初期導入フェーズ
  セキュア NW 動的再構築システムによるサービスを受けるサーバホストが新たに増えた際に実施され、既知のセキュリティホールに関する診断及び対処を自動的に実施する。
- 設定情報収集フェーズ
  各サーバやネットワーク構成装置のある時点での、設定状況やパッチの適用状況などをホストエージェント経由で定期的に収集し機器設定情報 DB に蓄積する。
- 新セキュリティホール対処フェーズ
  新たなセキュリティホールがシステムのセキュリティ情報DB に追加された際に、サービスを利用しているサーバホストの診断を行い、セキュリティホールが存在する場合には対処を自動的に実施する。
- リモート診断フェーズ
  市販のセキュリティ診断ツール等でリモートからサーバホストの診断を行い、問題があれば対処を実施する。

以上が各フェーズでの動作概要である。次に各フェーズの動作の詳細について述べる。

4.1. 初期導入フェーズ

本フェーズでは、まず新しく管理対象となったサーバホストのサービスや OS の情報を管理者がポリシ情報 DB に投入する。セキュア NW 動的再構築システムにおけるポリシ情報 DB に入力する項目としては、対象となるホストマシンの IP アドレスやホスト名、及びそのホストマシン上で提供するサービスの情報、各サービスの大まかな設定がある。次に、新しいサーバホストに関するポリシ情報を診断モジュールがポリシ情報 DB から読み取る。新しいサーバホストの提供するサービス等を勘案して FW のフィルタリングルールを作成し、ネットワーク構成装置上のホストエージェントに送信する。同時に、現時点で所有しているセキュリティ情報 DB の情報を参照して、新しく追加されたサーバホストに既知セキュリティホールに起因するセキュリティ上の問題が生じない OS 及びサーバホストの設定を作成し、サーバホスト上のホストエージェントに送信する。新しい設定を受け取ったサーバホストとネットワーク構成装置上のホストエージェントは、その設定をそれぞれ適用する事によって初期設定と問題の解決を行う。

表 1 にセキュリティ情報 DB の例を挙げる。

名前	詳細	対象OS	対応策	Ref
CVE-1999-0139	mkcookie の bof。Root 権限取得可能	Solairs 2.5(x86) 2.6(x86) 2.7(x86)	mkcookie のモードを 711 に変更	XF: sol-mkcookie (1429)
CVE-2001-0115	arp の bof	Solaris 2.4,2.5,2.5.1,2.6	パッチ 2.5: 109707-01	N/A

表 1 セキュリティ情報 DB(CVE[3])

実際のシステムにおいては、CVE の情報だけではなくベンダ等が提供する情報に関するテーブルもセキュリティ情報 DB に作成する。

4.2. 機器設定情報収集フェーズ

本フェーズではサーバホストやネットワーク構成装置の状態をシステム側の機器設定情報 DB に格納するためにホストエージェントが情報収集して送信する。送信する具体的な内容としては、OS 種別、OS バージョン、OS 固有の設定ファイル(起動用スクリプトファイル等)、各種アプリケーションサーバの設定ファイルの絶対パス名及び設定ファイルの内容などが含まれている。表 2 に OS の機器設定情報 DB の例を挙げる。

IP ｱﾄﾞﾚｽ	OS 種別、ﾊﾞｰｼﾞｮﾝ	パッチ情報	設定ファイルパス	ファイル内容
x.x.x.x	Solaris2.6	108707-1	/etc/	
y.y.y.y	Linux2.4.1	ac9	/etc/	

表 2 機器設定情報 DB(OS)

実際のシステムにおいては、OS についてだけではなく、本方式でのサービス対象となるサービス(web, mail, dns….)についてもサービス毎にテーブルを機器設定情報 DB に作成する。

4.3. 新セキュリティホール対処フェーズ

本フェーズでは、管理者によりシステム内のセキュリティ情報 DB に新たなセキュリティホール情報が投入されると、まず診断モジュールが管理下のサーバホストに関する OS のバージョン、パッチレベル、起動スクリプトやアプリケーションサーバの設定ファイル内容などの情報を機器設定情報 DB から取得する。その情報を元に新たにセキュリティ情報 DB に追加されたセキュリティホールが管理下のどのサーバホストに影響を及ぼすかを判断する。判断を行った結果、管理下に新たなセキュリティホールによる影響を受けるサーバホストが発見された場合には、セキュリティ情報 DB から新しいセキュリティホールの対処策を引き出し、ホストエージェントに送信する。その後、対処策を受信したホストエージェントはサーバホスト上で対処策を自動実行することによってセキュリティホールへの対処を行う。

4.4. リモート診断フェーズ

セキュア NW 動的再構築システムでは、セキュリティホール発見の補助的な手段として、市販のセキュリティ診断ツールも利用する。市販のセキュリティ診断ツールで管理下のサーバホストを診断した結果を解析モジュールが受け取る。解析モジュールは診断結果でセキュリティホールが発見されていた際にはそのセキュリティホールに関する情報をセキュリティ情報 DB から取得し、該当サーバホスト上にそのセキュリティホールが存在しうるかを機器設定情報 DB 上の該当サーバホストの情報を元に判断を行い、リモートセキュリティ診断ツールの出す結果の信頼性の向上を図る。解析モジュールが解析を行った結果、問題があると診断された場合には、発見されたセキュリティホールの対処策をセキュリティ情報 DB から取得し、対処策をホストエージェントに送信する。その後、対処策を受け取ったホストエージェントはサーバホスト上で対処策を実施することによってセキュリティホールへの対処を行う。

以上の 4 つのフェーズを組み合わせることによって 3 章で述べたような機能を実現する。その具体的な実施例を次章で述べる。

5. 実施例

本章では、セキュアNW 動的再構築システムを用いたネットワークサービス実施例を示す。図 2 に示すように、本方式を利用する際にはインターネットとユーザ網の間に、本方式を用いたサービス提供者網が入る。サービス提供者網には、ユーザにネットワークサービスとして提供するためのファ

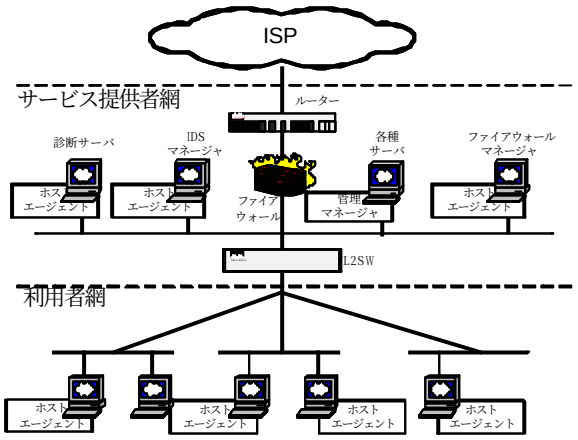

図 2 サービス提供案

イアウォール、IDS、診断サーバ等を設置し、図 1 における診断モジュール、機器設定情報 DB、ポリシ情報 DB、セキュリティ情報 DB などを備えた管理マネージャも設置する。また、ホストエージェントはファイアウォールマネージャ、IDS マネージャ、セキュリティ診断ツールがインストールされている診断サーバとユーザ所有のホストマシンのうち、セキュア NW 動的再構築システムによるサービスを利用するホストマシンにインストールする。

上記環境において、まず初期導入フェーズの処理が行われて各サーバ**ホスト**にその時点での安全な設定の通知が行われ、設定変更も実施される。設定変更で対応できないようなセキュリティ上の問題がある場合には、対処方法を記述した電子メールがユーザに送付される。

初期導入処理が終了すると定期的に機器設定情報収集フェーズが実行され、ホストエージェントが管理マネージャ内の機器設定情報 DB に管理対象の OS 情報や設定情報の登録を行う。

セキュア NW 動的再構築システムでは、管理マネージャ内のセキュリティ情報 DB をメンテナンスする管理者の存在を前提としている。管理者によるセキュリティ情報 DB への新しいセキュリティホール情報の投入を契機として新セキュリティホール対処フェーズが実行される。つまり、管理下のどの**サーバ**ホストが、新しいセキュリティホールの影響を受けるかを診断モジュールが機器設定情報 DB の情報を用いて判断する。問題があれば対処策をセキュリティ情報 DB から抽出して、ホストエージェントに向けて送信し、ホストエージェントにサーバホスト上での対処策を行わせる。自動対処が不可能な場合にはユーザに対処方法を記述した電子メールの送付を行う。

また、定期的に実行されるリモート診断フェーズによってセキュリティホールが発見された際にも上記と同様の動作を行い、セキュリティホールへの対処を実施する。

6. 終わりに

本稿では、セキュリティ診断からその対処にいたるまでのプロセスを自動化する一手法についての提案を行った。今後、本手法の実装を行い有効性の確認を行っていく予定である。また、検討に当たって以下のような課題があることが分かった。本システムの実用化に当たってはこれらの課題を解決する必要があるので、今後の検討項目としたい。

- **サーバホスト上のソフトウェアへの自動的なパッチの適用及びバージョンアップ手法の検討**
- **現在の方式ではホストエージェントが常にポートを開いて待ち受け状態にあるのでセキュリティ上の問題が発生する恐れがある。それを防ぐためにホストエージェントの通信を全て能動的に行わせる方式の検討**

【参考文献】

[1] JPCERT:**コンピュータセキュリティインシデント報告件数の推移**, *http://www.jpcert.or.jp/stat/reports.html*

[2] IPA:**小規模サイト管理者向けセキュリティ対策マニュアル**,*http://www.ipa.go.jp/security/fy12/contents/crack/soho/soho/index.html*

[3] Common Vulnerability and Exposures: *http://www.cve.mitre.org/*