O-041

外部機器と連携したセキュリティ機器における セキュアな接続アーキテクチャの検討

A Study on Secure Connections Architecture for Security Device in cooperation with External Devices

本田 貴大 Takahiro Honda　佐々木 昌樹 Masaki Sasaki　明石 貴靖 Takayasu Akashi　名児耶 光一 Koichi Nagoya

株式会社ナカヨ 事業戦略本部 情報技術研究所
Information Technology Laboratory，Business Strategy Division，NAKAYO，INC.

1. はじめに

情報通信分野において，情報漏洩防止や侵入検知などセキュリティ確保に関心がもたれている．そのため次世代ファイアウォール機器の利用が加速しているが，運用には高度な知識が必要であり，強固なセキュリティ確保と容易な保守運用の両立が求められている．

そこで我々は，セキュリティ機器の防衛機能を利用するとともに外部機器と連携をとりセキュアな接続を実現するアーキテクチャを検討している．

本論文では，上記アーキテクチャの一実現形態として，内線電話システムとセキュリティ機器を連携させる端末のネットワークへの接続制御方法を提案し，有効性を示す．

2. ネットワークの接続制御方法

端末へのネットワークの接続制御方法として，一般に MAC(Media Access Control)アドレスフィルタリングが，用いられている．本章では MAC アドレスフィルタリングの概要について述べ，利用する上で想定される問題点を提示する．

2.1 概要

MAC アドレスフィルタリングは，ルータやスイッチングHUB(スイッチ)が備える機能の一つで，特定の MAC アドレスを持つ端末からしか接続できないようにするアクセス制限方式で，端末ごとに固有の MAC アドレスをルータなどに登録することで，登録されていない端末からは接続できないようにする機能である[1]．ルータやスイッチで MAC アドレスフィルタリングを利用するにあたっては，事前に MAC アドレスを登録し，登録された MAC アドレスを持つ機器の通信を許可する．

MAC アドレスを持つ機器であれば，OS や機器に依存することなく MAC アドレスフィルタリングによる制御対象にできる利点がある．

2.2 現状の課題

一般にルータやスイッチにおいて MAC アドレスフィルタリングを使う場合，ホワイトリスト方式で使われることが多い．

そのため，MAC アドレスによるフィルタリングは，フィルタリング機能を備えるルータやスイッチへのアクセス権限を持つネットワーク管理者による MAC アドレスの事前登録が必要である．

登録には，接続対象端末の MAC アドレス以外に，例えば接続ポートや，スイッチが複数存在する場合は対象端末と接続しているスイッチの情報も把握しなければならないため，登録対象の端末が多い場合や，端末の追加、変更が頻繁に起こり得るネットワーク環境では，管理者への負担が大きく管理面の負荷が大きい[2]．

さらに，登録する MAC アドレスの文字列は完全一致する必要があり，人為的ミスによって MAC アドレスフィルタリングが誤った設定になった場合，端末が接続できないという問題がある．

3. 提案方法

外部機器によって，ネットワークに接続されたセキュリティ機器を連携制御し，ユーザの利便性を損なわず，セキュリティを確保するネットワーク接続制御方法を提案する．

本章では，第 2 章で述べた MAC アドレスフィルタリングにおける課題を解決する接続アーキテクチャの一実現方法を提案する．

MAC アドレスフィルタリングを使いセキュリティと利便性を両立させるためには以下のような条件が必要となる．

（1）MAC アドレス，接続ポート，接続対象スイッチ情報の効率的な収集が行えること．
（2）ネットワーク管理者による許可対象端末の確認ができること．
（3）スイッチは許可端末以外の端末はネットワークへの接続を遮断すること．

以下で提案システムの動作を説明する．

3.1 提案システム概要

提案するシステムの構成を図 1 に示す．

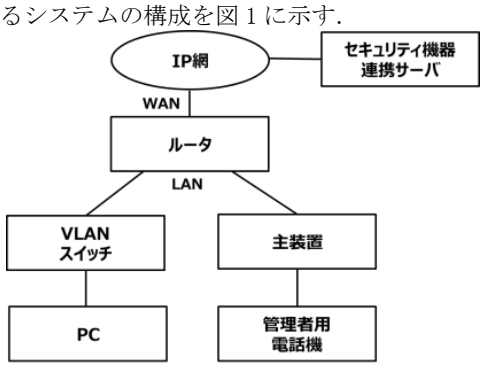

図 1. 提案システムの構成図

提案システムではルータの LAN 側に VLAN 機能を持つ VLAN 対応スイッチングハブ(VLAN スイッチ)と主装置を設置し，それぞれの配下の PC，管理者用電話機を接続する．WAN 側には VLAN スイッチの監視を行うセキュリティ機器連携サーバを設置する．

3.2 提案システムの動作

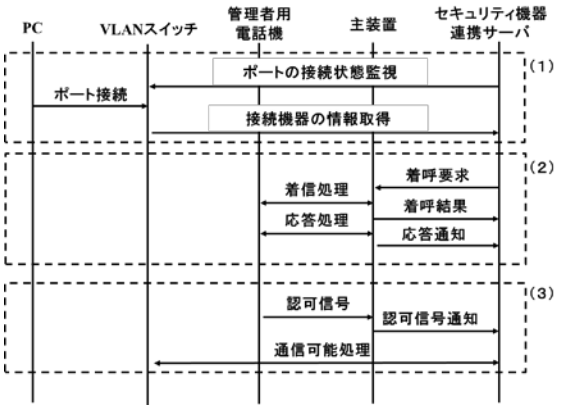

図 2．提案システムの動作

提案システムの一連の動作は以下の通りである．

（1）VLAN スイッチとセキュリティ機器連携サーバは TELNET 経由で常に接続状態であり，VLAN スイッチの FDB(Forwarding Data Base)を常時監視し，FDB の変化で端末が接続されたことを検出する．端末の接続を検出した場合，FDB の内容から接続された端末の MAC アドレスと接続ポートを特定する．

（2）接続された端末 MAC アドレスが，VLAN スイッチの FDB に登録されていない MAC アドレスだった場合，セキュリティ機器連携サーバが主装置を経由し，管理者用電話機に通知を行う．

（3）通知を受けた管理者は，電話機に表示される MAC アドレスを確認し，許可しても良い MAC アドレスだった場合，電話機による所定の操作を行うことで許可信号を主装置経由でセキュリティ機器連動サーバに通知する．通知を受けたセキュリティ機器連動サーバは，許可 MAC アドレスとして新規に登録することで接続ポートの VLAN 設定を有効にし，端末の通信を有効にする．

ここで，MAC アドレスフィルタリングではなく，VLAN を使用した理由としては，多くの MAC アドレスフィルタリングでは，ポートに接続された許可端末以外の端末から発せられるフレームは全て遮断するため， MAC アドレスの学習ができず，MAC アドレス収集ができないため，本方法を用いてセキュリティ機器連動サーバにより VLAN スイッチのポート間転送をコントロールすることでネットワークへの接続制御を実現した．

これにより，VLAN スイッチでの MAC アドレス収集が可能となり，許可した端末にのみ接続許可を与えることができる．

4. 評価

4.1 比較・考察

提案システムについて，従来の MAC アドレスフィルタリング手法と比較して考察を述べる．従来の MAC アドレスフィルタとポートベース VLAN を用いた提案システムを管理面に関して比較したものを表 1 に示す．

従来の仕組みとして，事前に接続対象の端末の MAC アドレスを調査し，権限を持つ管理者が PC を用いてネットワーク機器にログインすることで新規に登録する．ユーザと管理者にとって煩雑な操作が必要であった．

本提案では，監視サーバによって VLAN ポートに接続された端末 MAC アドレスを動的に収集するため、アドレスの調査を必要とせず，管理者の電話機操作だけで設定ができるため，手間が少ないという利点がある．

表 1．管理面の比較

	MAC アドレスフィルタリング	提案手法
MAC アドレス調査	必要	不要
アドレス管理	必要	不要
管理者 PC 端末	必要	不要

5. まとめ

MAC アドレスフィルタリングは管理対象外の端末を排除する手段として有効な技術であるが，ネットワーク管理者による，端末追加の都度 MAC アドレスの事前登録が必要であり，管理運用面で課題がある．

そこで，セキュリティ機器連携サーバによって VLAN スイッチのポート状態を監視し，動的に MAC アドレスを収集し，電話機の操作をすることで MAC アドレスフィルタの設定の手間を削減するシステムを提案した．

今後の課題として，ポートベース VLAN 技術を使用しているため 1 ポート 1 端末という制限がある．小規模のネットワーク以外では適用が困難である点について提案手法を改良し，対策を行いたい．

参考文献

[1] MAC アドレスフィルタリング
http://e-words.p/w/MAC アドレスフィルタリング.html

[2] 三宅猛,鈴木春洋,北野文章,村瀬晋二,若山公威,岩田彰“ARP テーブルの集中管理による認証ネットワーク上の不正接続検出と排除方法の提案”,情報処理学会研究報告,2008-CSEC-40,pp.71-176, 2008.