L-051

テーブルオーバレイ方式によるセキュア VLAN 分析システム

A Secure VLAN Analysis System by Table-Overlay Method

園田 健太郎† 松田 勝志†
Kentaro Sonoda Katsushi Matsuda

1．はじめに

LAN スイッチ機器（以下，スイッチと呼ぶ）の重要な機能のひとつに VLAN がある．VLAN を使うことで，物理構成に依存しない仮想ネットワークを柔軟に構築できる．しかし，VLAN を使った仮想ネットワークの構成は，パケットの流れを把握することが難しく，ネットワーク管理者の意図しない通信を許可する接続ポートが存在する可能性があり，セキュリティ上非常に危険である．VLAN による通信許可の接続ポートを特定するためには，対象スイッチの全ての接続ポートの通信可否を調べる必要がある上，VLAN 間ルーティングやフィルタリング等の通信制御も考慮しなければならず，膨大な時間がかかってしまう．そこで，我々は管理者のネットワーク管理とセキュリティ管理の負荷軽減を実現する VLAN 設定分析の研究を行っている．

本稿では，VLAN の通信制御状態をあらかじめインデックス化するテーブルオーバレイ方式と，それを使って VLAN の通信範囲を高速に出力するセキュア VLAN 分析システムについて述べる．

2．仮想ネットワーク管理における課題

ネットワーク管理者は，VLAN による仮想ネットワーク構築時に，その通信制御状態が管理者の意図する通りであるかを確認する必要がある．通信制御状態の検査とは，検査対象となるスイッチの全接続ポート間で，コンフィグの設定上通信可能か否かを確認することである．全接続ポート間でパケットの通信可否を検査すると，スイッチや VLAN の数が何百となる通信キャリア等のネットワークでは，その計算時間は現実的なものではなくなる．その上，VLAN 間ルーティングによる通信範囲の拡大やフィルタリング等による通信制御機能が含まれていると，計算量がさらに増大してしまう．スイッチの接続ポートに設定される VLAN-ID を一元管理するシステム[1][2]や各接続ポートの通信状態を表すモデル[3]等を使って，接続ポート間の通信可否を調べることはできるが，全接続ポート間で検査を行うことに変わりないため，先に述べた計算量問題は解決できない．

また，仮想ネットワークの通信制御状態の検査を人手で実施することは，管理者の作業負荷が非常に大きい上に，通信可否を誤って判定してしまうような検査ミスの発生の可能性もある．

3．テーブルオーバレイ方式による検査高速化

これらの課題を解決するために，VLAN の通信制御状態をあらかじめインデックス化するテーブルオーバレイ方式を考案した．

† 日本電気株式会社　サービスプラットフォーム研究所

3.1 テーブルオーバレイ方式

テーブルオーバレイ方式は，レイヤ 1-2 間，及びレイヤ 2-3 間の通信制御状態を表すテーブルをそれぞれ作成する（図 1）．これによって，各レイヤ間の通信制御状態を組み合わせて最終的な接続ポート間の通信可否を求めることができる．

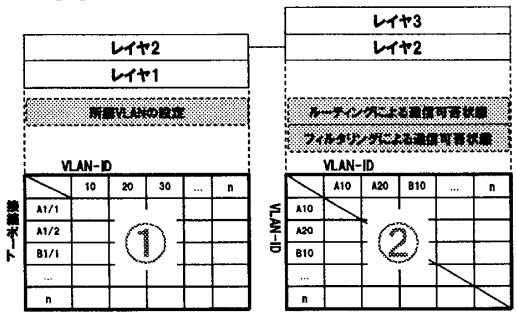

図 1　テーブルオーバレイ方式によるインデックス作成

図 1-①は，レイヤ 1-2 間の通信制御状態を表すテーブルであり，図 1-②は，レイヤ 2-3 間のテーブルである．前者は，各スイッチの接続ポートに設定される VLAN-ID の種類によって通信制御状態を表す．このテーブルは，コンフィグファイルの VLAN 設定コマンドを参照することで，容易に作成することができる．一方，後者は，各スイッチに設定される全 VLAN 間の通信制御状態を表す．後者のテーブルを使って通信可能な VLAN を調べ，その VLAN が設定される接続ポートを前者のテーブルを使って調べることで，通信範囲が特定できる．VLAN 同士の通信可否を計算するため，全接続ポート同士の場合より大幅に計算時間が短くて済む．

3.2 通信制御情報の重ね合わせ処理

テーブルオーバレイ方式では，レイヤ 1-2，レイヤ 2-3 のようにインデックスをレイヤ別に作成しているため，ベンダ機器独自のフィルタリング機能等が追加された場合においても，その機能のレイヤに通信制御情報を重ね合わせることができる（図 2）．

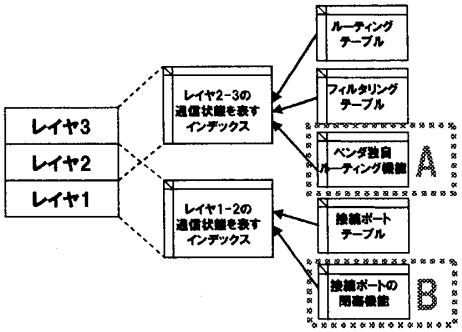

図 2　インデックスに対する通信制御情報の重ね合わせ

例えば，図 2-A ように，ベンダ独自のルーティング機能がある場合には，この機能による通信制御状態をレイヤ 2-3 の通信状態を表すテーブルと重ね合わせることで対応できる．また，図 2-B のような接続ポートを強制的に使用禁止にするような閉塞機能がある場合は，この機能によって通信不可となる接続ポートをレイヤ 1-2 の通信状態を表すテーブルと重ね合わせればよい．

4．セキュア VLAN 分析システム

テーブルオーバレイ方式を用いて，VLAN の通信範囲を特定するセキュア VLAN 分析システムを試作した．

4.1 VLAN 通信範囲検査用インデックスの作成

本システムでは，まず以下の 2 ステップで VLAN の通信範囲を特定するための検査用インデックスを作成する．

(1) 管理対象ネットワーク上の L2 スイッチや L3 スイッチのコンフィグをインポートする．

(2) テーブルオーバレイ方式による VLAN 通信範囲検査用インデックスの作成を行う．

4.2 VLAN 通信範囲の特定

ネットワーク管理者は，本システムを使って任意のスイッチに設定されている VLAN-ID を指定するだけで，その通信範囲となる接続ポートを知ることができる．本システムが出力する VLAN の通信範囲結果は，以下の 4 つに区分される．

1. 同一 VLAN で通信可能な接続ポート（図 3-①）
2. 異なる VLAN で通信可能な接続ポート（図 3-②）
3. 部分的に通信可／不可の接続ポート（図 3-③）
4. 通信不可の接続ポート（図 3-④）

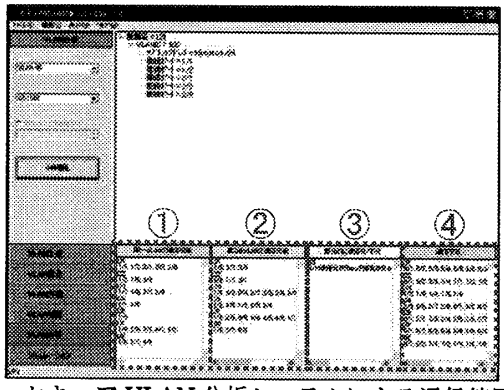

図 3　セキュア VLAN 分析システムによる通信範囲結果

ネットワーク管理者は，管理者自身が想定する VLAN の通信制御状態と，この VLAN 通信範囲結果を，VLAN 間ルーティングやフィルタリング等による通信制御を含めて比較することができ，想定と異なる通信制御となっているスイッチの接続ポートを容易に発見できる．

また，本システムでは，VLAN を指定してその通信範囲となる接続ポートを出力する他に，スイッチの接続ポートを指定した場合の通信範囲特定や，始点及び終点となる接続ポート間の通信可否検査等を実現している．

5．評価実験

セキュア VLAN 分析システムによる VLAN の通信範囲検査時間と手作業による検査時間を比較し，検査作業の効率化の度合を計った．

5.1 検査時間の定義と実験環境

セキュア VLAN 分析システムによる検査時間とは，コンフィグのインポート，検査用インデックス作成，全ての VLAN の通信範囲特定，及び出力結果の確認までの一連の作業にかかった時間を指す．一方，手作業による検査時間とは，コンフィグを参照しながら全ての VLAN の通信範囲を特定してその結果を一覧表にし，再度結果の確認を行うまでの作業にかかった時間を指す．

想定ネットワーク上のスイッチは，L2 スイッチ 8 台，L3 スイッチ 2 台の計 10 台で，このネットワーク上に構築される VLAN は 10 個である．

5.2 実験結果

手作業検査にかかった時間は，約 4 時間であった．また，手作業検査では，検査ミスが多発した．この検査ミスの発生箇所の再検査にかかる時間が大きく，4 時間のうち約 1 時間を費やした．なお，検査ミスの発見作業は，人手による検査結果とシステムの検査結果を比較し，異なった箇所を人手で確認するという方法で行った．

一方，セキュア VLAN 分析システムを使った検査時間は，約 3 分であった．インデックス作成に約 8 秒，各 VLAN の通信範囲検査は 1 秒以内で完了したため，3 分のほとんどを出力結果の確認作業に費やした．手作業検査と比較して，検査時間を 1/80 に短縮することができた．

また，スイッチ数と VLAN 数を変えた処理時間の測定を行った（表 1）．小中規模の仮想ネットワークであれば，現実的な処理速度で実行可能であることが判明した．

スイッチ台数/VLAN個数	インデックス作成時間	通信範囲検査時間
10台/10個	8秒	1秒以内
10台/50個	76秒(1分16秒)	1秒以内
10台/100個	537秒(8分57秒)	1秒以内

表 1　インデックス作成時間と通信範囲検査時間

6．おわりに

本稿では，VLAN の通信制御状態をあらかじめインデックス化するテーブルオーバレイ方式と，それを用いたセキュア VLAN 分析システムについて述べた．また，スイッチ数及び VLAN 数が数十で構成される小中規模のネットワークにおける VLAN の通信範囲検査に対して，セキュア VLAN 分析システムが十分利用できることを示した．今後，スイッチ数や VLAN 数が数百～数千の大規模ネットワークへの適用へ向けて，テーブルオーバレイ方式の改良や本方式を土台とした新手法の検討を行っていく予定である．

参考文献

[1]T. Tamura, T. Miyamoto, R. Suzuki, T. Hiraoka and H. Matsuo, “A Web-based Network Management System with Network Device Configuring Capability”, HITACHI CABLE REVIEW No.18, October 1999.

[2]宮本，田村，鈴木，平岡，松尾，泉，福永，“インターネット応用システムの構築と運用管理　大規模ネットワークにおける VLAN 管理システム”，情報処理学会論文誌 Vol.41/No.12, pp.3234-3244, 2000.

[3]H. Sakurada, “タグスイッチネットワークのモデル検査による漏洩検査”，情報処理学会研究報告，Vol.2004/No.54, pp.49-54, 2004.