

分散型ネットワークセキュリティシステム管理装置の研究開発

工藤 駿介† 松田 勝敏‡

東北工業大学大学院工学研究科† 東北工業大学工学部‡

1. はじめに

コンピュータネットワークには様々な脅威が存在し、利用する上でセキュリティ対策は欠かすことができない。特に、セキュリティ対策の初歩として用いられるファイアウォールでの通信制御は効果的な手段の一つである。

従来のネットワークでは、WAN に接続するネットワーク基幹部にアプライアンス型のファイアウォールを設置し、WAN からの脅威に対応している。また、各端末にはパーソナルファイアウォールを導入することで LAN 内部での脅威に対応している。しかし、これらのファイアウォールは自身を通過する通信を制御するため、ネットワーク中間層の通信を全て制御することが困難である。

我々は、ネットワーク中間層を対象としたセキュリティシステムについて研究を行っている[1][2]。今回は、システムのフィルタリング詳細化とログ情報の変更を行い、管理装置の改修と機能拡張を実施した。

2. システム概要

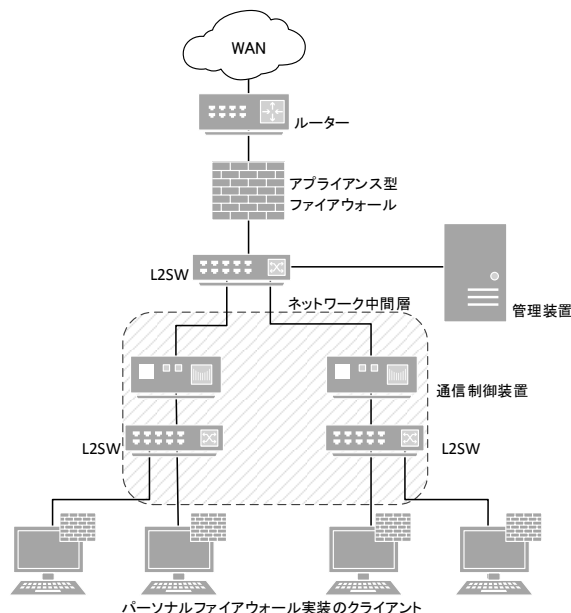


図1 システム概要図

本システム(図1)は、従来のファイアウォール構成では通信の制御が困難であるネットワーク中間層の通信を制御することができる。そのため本システムの導入により、従来のネットワークセキュリティをより向上させることが可能である。

ネットワーク中間層には、通信を制御するために通信制御装置を設置する。通信制御装置は、ネットワーク中間層に複数台設置しなければならない[2]ことから、低コストで実装可能な組み込みシステムを用いて実装を行った。また、透過的にネットワークに導入するため、レイヤー2で動作する。

これらの通信制御装置を一括管理するために、ネットワーク基幹部に管理装置を設置する。管理装置から通信制御装置を管理する方法としては、制御命令を Ethernet フレームに格納し、Ethernet にて通信する。通信制御装置は命令に従い、通信制御を始める。

2.1 フィルタリング

ネットワーク中間層の通信制御には通信制御装置を用いる。通信制御装置はレイヤー2で動作させており、通過する Ethernet フレームを判定して必要な処理(フレームの中継か破棄動作)を行う。

これまで Ethernet フレームの判定には、フレーム内の MAC アドレスを参照させ該当アドレスが登録されている場合に中継か破棄の動作を行わせることで通信の制御を行っていた。

今回はフレームの判定要素を追加し、これまでに比べ、より詳細なフィルタリングができるように変更を行った。判定要素は以下の通りである。

- ・宛先 MAC アドレス
- ・送信元 MAC アドレス
- ・フレームタイプ
- ・通信の方向
- ・フレームサイズ

これらの判定要素に基づきフィルタリングポリシーを作成し、Ethernet フレームの判定を行わせることで指定の処理を実行させる。また、ポリシー毎に優先度を設定できるようにした。

2.2 ログ

通信制御装置は、到着した Ethernet フレームを処理する毎に管理装置に処理情報をログとして送信する。ログの送信には Ethernet を用い、Ethernet フレームに処理情報を格納する。これまではログに

Research and Development of the Distributed Network Security System Management

†Shunsuke KUDOU, Graduate School of Engineering, Tohoku Institute of Technology

‡Masahiro MATSUDA, Faculty of Engineering, Tohoku Institute of Technology

以下の処理情報を格納していた．

- ・対象フレームに施した処理
- ・対象フレームの宛先 MAC アドレス
- ・対象フレームの送信元 MAC アドレス
- ・対象フレームのタイプ
- ・対象フレームのサイズ

今回は対象フレームの流れを把握できるよう，対象フレームが到着した通信制御装置の Ethernet ポートをログに追加するようにした．

3. 管理装置

管理装置では，ネットワーク中間層に配置した複数台の通信制御装置の一括管理を行う．管理には，専用の GUI アプリケーションを用いる．管理装置と通信制御装置の通信には Ethernet を用い，Ethernet フレームに制御命令を格納して送ることで通信制御装置を操作することが可能である．また，通信制御装置から送られるログの受信が可能である．今回は，フィルタリングの詳細化とログ情報の変更に従い，改修を行った．

管理装置では，以下の操作をすることができる．

- ・各通信制御装置の登録
- ・フィルタリングポリシーの作成と送信
- ・通信制御装置から送られるログの閲覧

3.1 フィルタリングポリシー

フィルタリングポリシーは，管理装置の GUI アプリケーションで作成と送信を行うことができる．以下の項目について設定が可能である．

- (1) 宛先 MAC アドレス
- (2) 送信元 MAC アドレス
- (3) フレームタイプ
- (4) 通信の方向
- (5) フレームサイズ
- (6) (1)～(5) 当該する場合の処理

フレームサイズの項目では，対象とするフレームのサイズの範囲を指定することができる．当該する場合の処理の項目では，対象フレームの中継か破棄を指定できる．当該する場合の処理の項目以外では，値の指定が特に無い場合は全ての条件を満たす ALL を指定することができる．

3.2 ログの管理

通信制御装置は，Ethernet フレームを処理する毎に管理装置に処理情報をログとして随時送信する．管理装置では，通信制御装置からのログを受信し，閲覧可能な状態とする．

これまで GUI アプリケーションでは，受信したログを一時的に保管し，閲覧可能な状態に展開するのみでログを保存する機能は無かった．そのため，今回は受信したログをデータベースで管理するように機能拡張を施した．ログは通信制御装置

毎に格納するテーブルを分けてデータベースに保存する．またデータベースへ格納するデータとして，ログに格納されている情報以外にログが管理装置に到着した時間を追加する．

4. 検証

今回は，変更を行ったシステムが想定通りに動作するか検証を行った．検証を行う主な項目は以下の通りである．

- ・変更したフィルタリングが正常に動作するか
 - ・通信制御装置から出力されるログが設計通りか
 - ・管理装置から通信制御装置を正常に操作可能か
 - ・ログがデータベースに正常に格納されているか
- システムを実際に検証用ネットワーク(図2)にて動作させ，確認を行った．結果，期待通りの動作を確認できた．

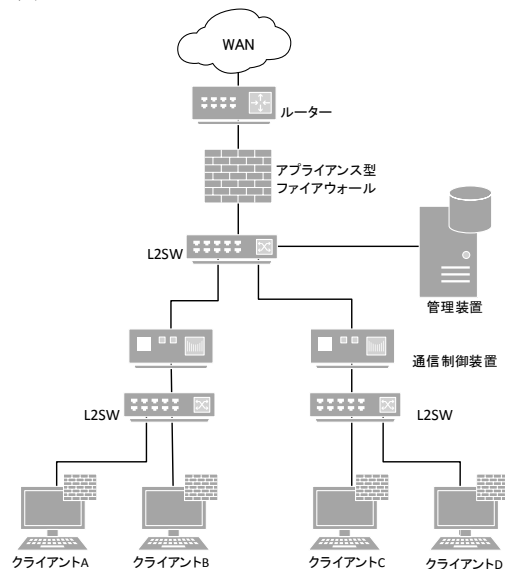


図2 検証用ネットワーク

5. まとめと今後の課題

今回は，システムのフィルタリング詳細化とログ情報の変更に従い，管理装置の GUI アプリケーションの改修を行った．また，管理装置の GUI アプリケーションとデータベースを連携させ，ログをデータベースに格納するように機能拡張を行った．検証結果としては，正常にシステムが動作していることが確認できた．

今後は，データベースに格納したログを解析することでネットワークの不審な挙動を検知する機能を設ける．

参考文献

- [1] 佐々木宏幸，松田勝敬：分散型通信制御セキュリティシステムの開発，第8回情報科学技術フォーラム講演論文集，第4分冊，P.133-134(2009)．
- [2] 工藤駿介，松田勝敬：組込みシステムを用いた分散型ネットワークセキュリティシステムの研究，第12回情報科学技術フォーラム講演論文集，第4分冊，P.205-206(2013)．