L-006

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
Development of Distributed Network Security System Using Embedded System

工藤　駿介†　　松田　勝敬†
Shunsuke Kudo　　Masahiro Matsuda

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する．ネットワーク外部からの脅威に対するセキュリティ対策だけではなく，ネットワーク内部からの脅威に対するセキュリティ対策も行う必要がある．

ネットワーク内部からの脅威を防ぐには，問題の発生原因周辺のネットワークを隔離することが有効である．ネットワークを隔離するに当たって他のネットワーク利用者への影響も考慮し，隔離するネットワークの範囲はできるだけ小さくするのが望ましい．それらを実現するためには，ネットワーク内部の通信を制御する装置（以下，通信制御装置）を，ネットワークセグメント毎に分散して配置するのが有効的である．また，通信制御装置を分散して配置するに当たって，安価な組込みシステムを用いることが望ましい．これによりシステム導入時のコストを抑えることが出来る．

我々は，ネットワーク内部を対象としたセキュリティ対策システムについて研究を行っている[1]．これまで通信制御装置は BOX-PC や単体の組込みシステムによる実装と検証を実施してきたが，今回は複数の組込みシステムによる実装を行い，動作検証を実施した．

2．システム概要

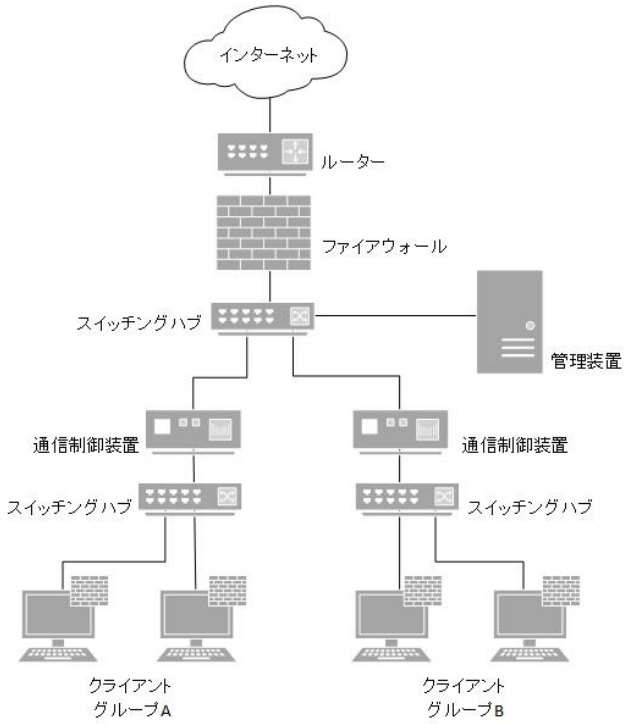

図１　システムの概要

本システムは，従来のネットワークセキュリティシステムに追加することで，ネットワーク外部からの脅威だけではなくネットワーク内部からの脅威に対しても対応できることを目的とした．

ネットワーク内部の各ネットワークセグメントに，一台ずつ組込みシステムで実装した通信制御装置を設置する．これによりネットワーク内部で問題が発生した場合に問題発生箇所を通信制御装置で隔離することで，被害を最小限に抑えることが可能である．また，これらの通信制御装置を管理する管理装置をネットワーク内に配置する．システムの概要を図１に示す．

また，通信制御装置と管理装置の通信には，Ethernet を用いた．通信制御装置は，管理装置から送信される制御命令に応じて Ethernet フレームの制御を行う．ネットワーク内部に問題の発生した場合は，問題発生箇所からのパケットを停止することでネットワークからの隔離を行う．

このとき通信制御装置は受信した Ethernet フレームの宛先 MAC アドレス，送信元 MAC アドレス，タイプ，フレームサイズをログとして管理装置に送信する．管理装置は各通信制御装置から送信されたログを受信し，情報収集を行う．

2.1　通信制御装置

通信制御装置には，パケット中継ができるように Ethernet ポートが 2 つ実装された組込みシステムを用いる．本システムで採用した組込みシステムには，Linux が実装されている．この Linux 上で通信制御を行うことが出来るプログラムを稼働させることにより通信制御装置として動作している．

また，通信制御装置はデータリンク層で動作させる．2 つの Ethernet ポートはプロミスキャスモードに設定し，宛先に関係無くネットワーク内のパケットを扱えるようにした．これにより透過的にネットワークに設置できるため，既存のネットワーク環境を崩さずに設置することが可能である．Ethernet のフレーム制御のために，RAW Socket を用いた．

通信制御装置には中継する Ethernet フレームの制御方法として，以下の４つの制御を実装した．通信制御の判断には Ethernet フレーム内の MAC アドレスを参照する方法を用いており，管理装置からの制御命令により動作する，

(1) 全ての機器の通信を通過させる．
(2) 全ての機器の通信を遮断する．
(3) 指定した機器の通信のみ遮断．
(4) 指定した機器の通信のみ通過させる．

2.2　管理装置

管理装置では，通信制御装置への制御命令の送信，ログの受信を行う．通信制御装置への制御命令の送信には Ethernet を用いる．また，管理装置での操作は GUI を採用し，専用のアプリケーションを作成した．

†東北工業大学, Tohoku Institute of Technology

管理装置では，各通信制御装置からのログの閲覧，通信制御装置への制御命令の送信が可能である．

2.3 制御命令・ログを送信するフレーム

通信制御装置と管理装置間の通信には Ethernet フレームを送受信する方法を用いた．送受信される通信は他の通信と区別させるため，Ethernet フレームのタイプ部に，実験用の番号を割り当てた．

管理装置から通信制御装置への制御命令に使うフォーマットには，データ部の先頭に行わせる通信制御を区別させる識別番号を付け，それ以降には処理に必要な情報が記述される(図２)．指定した機器の通信のみを遮断などの時には，遮断する機器の MAC アドレスが入る．また，Ethernet フレームのデータ部のサイズは最低で 46 バイト，最大で 1500 バイトと規定されている．最低サイズに満たない場合は，足りないサイズ分だけ空のデータを補充し，最大サイズを超える場合は分割して送信を行う．

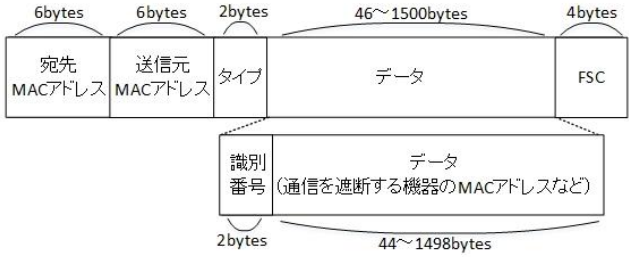

図 2　制御命令フォーマット

通信制御装置から管理装置へのログ送信に使うフォーマットには，データ部の先頭にログを区別させる識別番号を付け，それ以降にログを記述する(図３)．送信するログには，通信制御装置が受信した Ethernet フレーム内の宛先 MAC アドレス，送信元 MAC アドレス，タイプ，Ethernet フレームサイズが記述される．また，最低サイズに満たない場合は，足りないサイズ分だけ空のデータを補充する．

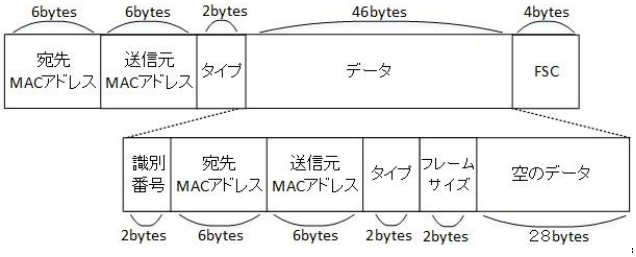

図 3　ログフォーマット

3. 動作概要

管理装置から通信制御装置へ制御命令を送信するには，設置した通信制御装置の MAC アドレスが分からなければならない．そのため，管理装置は最初に各通信制御装置にブロードキャストアドレスにて MAC アドレス送信命令を送る．この通信を受け取った通信制御装置は，送られてきた命令から管理装置の MAC アドレスを知る．通信制御装置は，この MAC アドレス宛てに応答を返す．これにより，管理装置・通信制御装置がお互いに MAC アドレスを知ることができ制御命令が送信可能になる．

通信制御は，管理装置のプログラムで制御内容を入力し，その内容に基づいた，制御信号が対象の通信制御装置に Ethernet フレームで送信される．これを制御命令と呼ぶ．

通信制御装置の動作ログは，管理装置と通信制御装置は MAC アドレスの交換をした後，通信制御装置はすべてのフレームを中継する動作を開始する．通信制御装置がフレームを中継すると，1 フレームごとに管理装置にログを送信する．ログの内容は，中継したフレームの宛先 MAC アドレスと送信元 MAC アドレス，フレームのタイプ，フレームサイズである．中継した場合は，フレームのデータ部の識別番号を中継したことを示す値でログ送信する．

管理装置からの制御命令により，中継しなかったフレームが発生した場合は，フレームを中継しなかった動作の内容も含めたログを管理装置に送信する．送信するログの内容は，フレームを中継した場合と同様であるが，ログフレームのデータ部先頭の識別番号は，フレームを破棄したことを示す値にして送信する．

4. 検証

通信制御装置にてネットワーク内部の通信を制御できるか検証を行った．今回は，組込みシステムで 2 台の通信制御装置を実装し，同時に動作させた．図４に検証環境を示す．

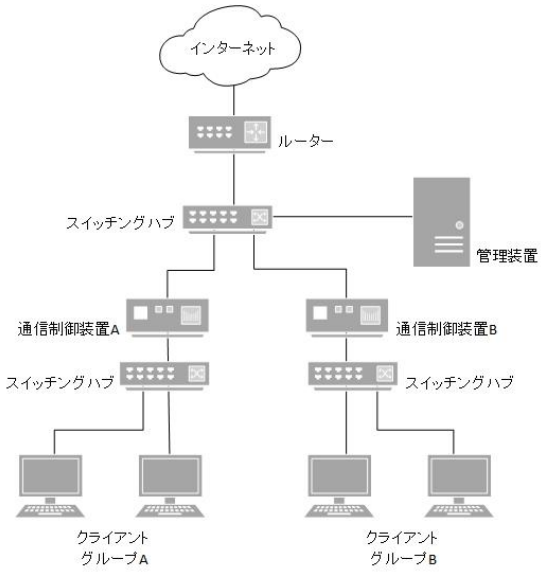

図 4　検証環境

5. 考察とまとめ

通信制御装置を組込みシステムで 2 台実装し，システムの動作を検証した．その結果，問題なく動作し，組込みシステムで通信制御装置を構成した場合も，動作に問題がないことがわかった．

今後は，システムのスループットの検証や，管理装置での機能を拡充する予定である．

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).