分散型通信制御セキュリティシステムの組込み機器への実装に関する考察

佐々木　宏幸†　　松田　勝敬‡

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上には様々な脅威が存在する．それらの脅威を防ぐためのセキュリティ対策として，ファイアウォール等による通信制御が広く行われている．

ファイアウォールには，WAN と LAN の境界に設置するファイアウォールアプライアンスと，個々の端末に実装するパーソナルファイアウォールがある．ファイアウォールアプライアンスでは，LAN の内外からくる通信の制御を行うことで，LAN 内部のセキュリティを維持している．しかしながら，LAN 内部の端末から LAN 内部の端末への攻撃に対して防ぐことができない．パーソナルファイアウォールは，実装されている端末が受信・送信する通信を制御できる．しかし，実装された端末に関与しない通信は制御できない．ファイアウォールアプライアンスとパーソナルファイアウォールの両方を用いても，ネットワーク基幹部とネットワーク末端の端末間の通信の制御は難しい．

そこで我々は，LAN 内部の通信制御に特化したセキュリティシステムを安価で実現するシステムの研究・開発を行っている[1]．システムは通信制御装置と，それらを一括管理する管理装置から構成される．複雑な処理を管理サーバに行わせ，通信制御装置の機能を最小限とする事で，通信制御装置を安価な機器で実現可能となる．それにより LAN 内のセグメント毎に分散配置してもコストがかからず，システム全体の低コスト化に繋がる．

これまで通信制御装置を PC やボード PC を用い実装してきた．今回は安価な組込み機器を用いて実装を行い，検証を行った．

2. 分散型通信制御セキュリティシステム

概要を図 1 に示す．通信の制御を行うプログラムを実装した機器を L2 通信制御装置，それらの一括管理を行うプログラムを実装した機器を管理装置と呼ぶ．

L2 通信制御装置は，トランスペアレントに動作し，ログを管理装置に指定した時間ごとに送信する．そして管理装置から送信される制御命令に従って，セグメント内の通信制御を行う．管理装置は L2 通信制御装置より送られてくるログを保存し，L2 通信制御装置に向け通信の制御命令を送信する．

L2 通信制御装置を安価な機器で実現するために，フレームの通過と遮断，通信ログの記録機能のみを実装した．記録するフレームのログは送信元・宛先 MAC(Media Access Control)アドレス，タイプ，フレームの通過回数，

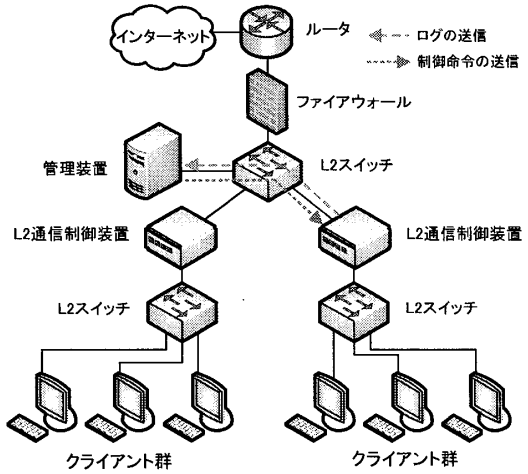

図 1　分散型通信制御セキュリティシステムの概要

入出力ポートを記録する．

また，L2 通信制御装置と管理装置の通信には，既存のネットワーク構成を崩さず機器の配置が行えるように，通信にはイーサネットフレーム[2]を用いる．

ログや制御命令の通信は，イーサネットのタイプ部に専用の番号を付け，通常の通信と区別している．

3. 組込み機器への実装

セグメント毎に配置する L2 通信制御装置は，システム全体のコストを下げるため，安価な機器である必要がある．そこで 1 台あたりの価格が安価である組込み機器を用いる．組込み機器は，Trinity 社製の PIC ネットワークボード(以下 PIC ボード)[3]を用いた．性能を表 1 に示す．この PIC ボードは，マイコンとイーサネットチップが同じパッケージに実装されており，安価である．プロトコルスタックは，Microchip 社の TCP/IP Protocol Stack[4]を元にした．

また L2 通信制御装置では，通信ポートが 2 つ必要となる．用いた PIC ボードは通信ポートが 1 つしかない為，PIC ボードをシリアル接続で 2 台接続し，機器間で受信フレームを受け渡す方法をとった．

3.1 組込み機器間の通信

PIC ボード間の通信は，同期式のシリアル通信を用い

表 1　用いた組込み機器の性能

搭載 CPU	PIC18F67J60-I/PT
動作クロック	41.666MHz
LAN	10BASE-T
プログラムメモリ	128kB
RAM	汎用：3.8kB イーサネット用：8kB

Consideration Implementation to Embedded System of Distributed Communication Control Security System

† Hiroyuki Sasaki, Graduate school of Engineering, Tohoku Institute of Technology

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

た．PIC に内蔵された MSSP(Master Synchronous Serial Port)モジュールを用い，SPI(Serial Peripheral Interface)モードで使用した．SPI モードでの PIC ボード間で受け渡しするデータは，SPI 通信専用のバッファに保存される．

SPI モードを用いた機器間の通信方法として，以下の 2 つの方式を検証した．

[PIC ボード間の通信方式 1]

あらかじめ一方の PIC ボードを SPI マスタモード，もう一方を SPI スレーブモードに設定する．マスタモード側の PIC ボードにフレームが届くと，制御命令用の通信であるかの確認と，ログの記録を行う．その後イーサネットの受信バッファから，スレーブモード側の PIC ボードに 1 バイトずつフレームを送信する．フレームの送信が完了すると，割り込み信号をスレーブモード側 PIC ボードに送る．スレーブモード側 PIC ボードは，SPI 通信専用のバッファからイーサネット送信バッファに，順次フレームを格納する．割り込み信号を受け取ると，送信バッファに格納されたフレームを送信する．

[PIC ボード間の通信方式 2]

フレームを受け取った PIC ボードは，上記同様，制御命令の確認とログを記録した後，もう一方の PIC ボードに向け割り込み信号を送信し，SPI マスタモードに設定する．割り込み信号を受け取った PIC ボードは SPI スレーブモードに設定される．SPI マスタモードの PIC ボードは，送信する最初の 2 バイトでフレームサイズを通知し，以降イーサネットの受信バッファより 1 バイトずつフレームを送信する．フレームを送信し終えたら，SPI マスタモードを終了する．

SPI スレーブモードの PIC ボードは，最初の 2 バイトで受け取るフレームサイズを確認する．その後送信されたフレームを順次イーサネットの送信バッファに格納する．フレームサイズ分受信したら，イーサネット送信バッファに格納されたフレームを送信し，SPI スレーブモードを終了する．

3.2 イーサネットバッファ

PIC に内蔵されたイーサネットの送受信バッファは 8kB であり，送信・受信バッファを自由に割り振ることが可能である．また受信バッファはリングバッファになっており，受信バッファ以上の通信を受信した場合，通信は破棄される．破棄によるフレームロスを抑える為に，送信バッファをフレームの最大長である 1518byte とし，残りを全て受信バッファとした．

4. 検証

通信方式 1 と 2 について，PIC ボードに実装した．この PIC ボードを用いて，L2 通信制御装置の通信能力を検証する為，RFC2544[5]に基づいたフレーム損失率の測定を行った．

4.1 検証環境

検証環境を図 2 に示す．テスターのポート 1 からポート 2 に向けテストフレームを 60 秒間送信する．ポート 1 で送信したフレーム数と，ポート 2 で正しく受信できたフレーム数からフレーム損失率を求める．テストフレームのサイズは 64byte，128byte，256byte，512byte，1024byte，1280byte，1518byte について，それぞれ 3 回ずつ測定し，平均値を求めた．

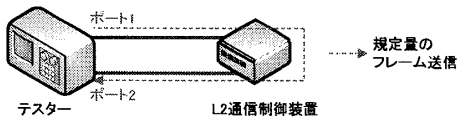

図 2　検証環境

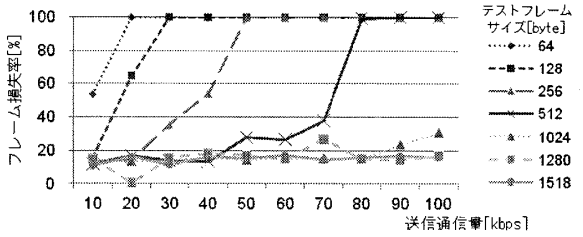

図 3　通信方式 1 でのフレーム損失率

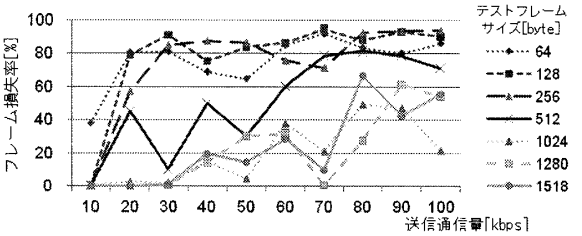

図 4　通信方式 2 でのフレーム損失率

4.2 検証結果

PIC ボード間の通信方式の検証結果を図 3，図 4 に示す．通信方式 1 と 2 共に，テストフレームのサイズが小さい程，フレームの損失が多い．通信方式 1 では，常にフレーム損失率が 10%程度発生する．通信方式 2 では，テストフレームを 60 秒間送信する間にスレーブ側の PIC ボードがフリーズする場面が多く見られたため，安定しない結果となっている．正常に動作した場合でも，1%未満のフレーム損失が発生している．

5. 考察とまとめ

テストフレームサイズが小さい程フレーム損失率が高い結果となった．これは同一の送信通信量において，フレームサイズが小さいほど単位時間内に送信されるフレーム数が多い事から，単位時間に送信されるフレーム数が多い程通信能力が下がる結果と思われる．

また通信方式 1 と 2 で，正常に通信が行えても常にフレーム損失が発生している．この為，スループットが低い事が予想され，実用的とはいえない．

よって 1 つのマイコンにイーサネットチップが 2 つ実装されたボード等，ハードウェア設計の面からも検討の必要がある．

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第 4 分冊，pp.133-134 (2009).
[2] IEEE: IEEE802.3 ETHERNET, IEEE(オンライン), 入手先〈http://grouper.ieee.org/groups/802/3〉.
[3] Trinity LLC: Trinity ◇PIC ネットワークボード【概要】, Trinity(オンライン), 入手先〈http://www.itrinity.jp/products/pic18f_lan/features.html〉.
[4] Microchip Technology Inc.: Ethernet Solutions Design Center, Microchip Technology Inc. (オンライン), 入手先〈http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=2504〉.
[5] IETF: RFC2544 - Benchmarking Methodology for Networks Interconnect Devices, IETF(オンライン) 入手先〈http://www.ietf.org/rfc/rfc2544.txt〉.