９　インターネットを利用した産業機械の遠隔診断に必要な通信技術の開発（第３報）

村河亮利，岡野　仁，菊田敬一

Development of a remote monitoring system for industrial machines (3rd Report)

MURAKAWA Akitoshi, OKANO Hitoshi and KIKUTA Keiichi

This study proposes a communication method for remotely and securely monitoring by using the Internet without changing settings of routers and firewalls at least or at all. This study reports that the communication software was revised for speed-up of transmission rate and was implemented encryption of the communication data. Four improved points from the 2nd report are as follows.

1. The connection protocol between two terminals was improved, and was implemented exception handlings.
2. The RTP protocol used for the data communication channel was modified to the UDP protocol to speed up the transmission rate. In addition, the acknowledged response processing was improved. Therefore, the baud rate rose to 3.27Mbps, and the proposed protocol could be used for the dynamic picture image transmission.
3. The data channel between two terminals was encrypted.
4. Data communication to the remote two terminals was possible at the same time.

キーワード：遠隔診断，インターネット，プロトコル，セキュリティ，組み込み

１　緒　　言

現在，機器メーカがユーザの機器の稼動状態や故障情報等の遠隔監視を行う際には，通信回線として電話線が一般的に用いられているが，通信速度が遅く，費用も高価である。一方，高速で安価なインターネット回線が普及しているものの，機器１台ごとにグローバル IP アドレス（以下，グローバル IP）が必要，セキュリティ面で不安があるなどの問題があり，遠隔監視用途としては，インターネットはあまり利用されていない。

本研究では，ルータやファイアウォールの設定変更を最小限あるいは全く変更することなく，インターネット回線を使って安全に遠隔監視を行うことのできる通信方式を提案し，実装を行ってきた。本報では，通信速度の高速化，通信データの暗号化について報告する。

２　システム構成

本システムのハードウェアは，**図１**に示すとおりメーカ側に設置する保守管理端末，ユーザ側に設置する遠隔監視ユニット，およびこれらの端末を接続するための仲介サーバから構成される。Ａは通信制御を行なうソフトウェア，Ｂは遠隔監視ユニット内のみに関係するソフトウェアを示す。保守管理端末と，遠隔監視ユニットは，NAT の内側すなわち LAN 上に接続されており，仲介サーバは，NAT の外側すなわちインターネット上に接続されている。

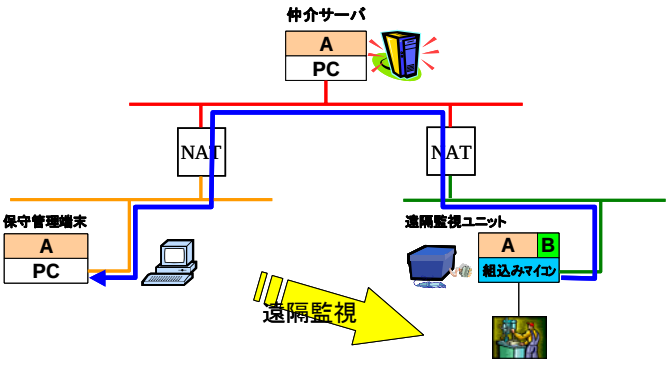

図１　端末接続のシステム概念図

３　通信プロトコル

本システムで提案するプロトコルは，保守管理端末と遠隔監視ユニットの各端末間の接続プロトコル（SIP），端末間のデータ通信プロトコルおよび認証・暗号化プロトコルから構成されている。

3.1 接続プロトコル（SIP）

接続プロトコル（以下，SIP）によるセッション制御の状態遷移図を**図２**に示す。Ｓは通信状態，Ｃはユーザ発呼要求状態，Ｕは着信許可 URL リスト登録の有無である。通常の発信，着信，切断の流れは矢印で示してある。発信する場合，相手端末の URL を登録し，通信相手端末に接続要求をする。その後接続処理中を経て相手端末に接続する。着信拒否が行われた場合は，発呼待ちの状態に遷移する。相手端末から着信した場合，登録 URL に着信端末の URL が登録されていれば接続処理を行い，URL が登録されていなければ，受信処理をキャンセルする。切断する場合，切断要求をすると切断処理中に遷移し切断処理を行う。登録されている URL を消去したい場合は，切断処理の途中で同時に URL 消去を行う。

本報では，発呼時の URL エラー処理や着信拒否処理などの例外処理機能を追加した。

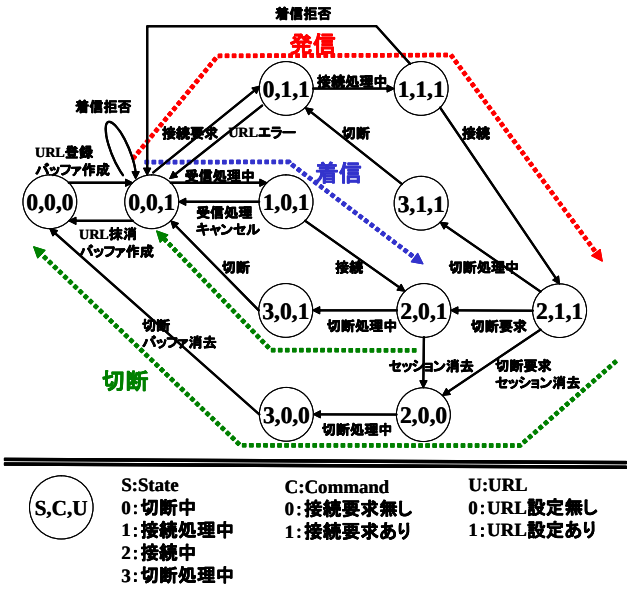

図２　SIP 状態遷移図

3.2 データ通信プロトコル

前報[1)]ではデータ転送方式に，RFC4040 をベースとした擬似コーデックを利用する，RTP 単方向転送を提案したが，転送速度が遅いという課題があった。

そこで本報では，転送速度の高速化を図るため，RTP 非依存の UDP 転送に独自の確認応答（以下，ACK）返信を実装した方式を提案する。

送信データは送信用 API を通じて暗号化され，**図３**に示す暗号化データを生成する。このデータを，あらかじめ SIP により指定された IP アドレス，ポートに向けて送信する。送信用 API は送信要求に対し，暗号化データを UDP パケットサイズに分割して枝番号を付与する。パケットは，データ種別，シーケンス番号，枝番号，枝番号の総数で構成されるヘッダと，暗号化されたデータを連結したものである。枝番号を用いることにより，受信側の ACK 返信を待つことなく送信可能となる。一方受信側では，同一シーケンス番号で異なる枝番号の UDP パケットを受信し，ACK 返信が行われる。ACK パケットは，枝番号のデータ受信状態をフラグで示す（**図４**）。受信した枝番号データが届いていれば，その枝番号フラグを１，それ以外は０と定義した。**図４**の例では４番目のデータが到達していないことを示している。

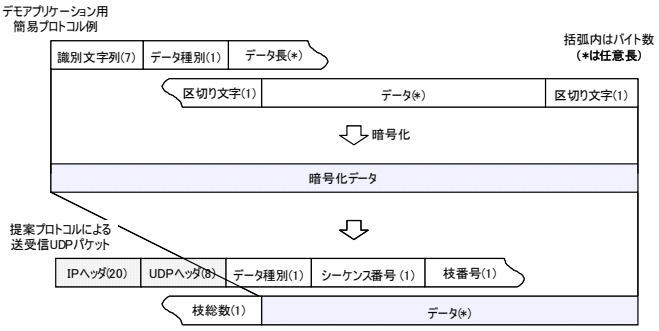

図３　汎用データ転送のための UDP ペイロード

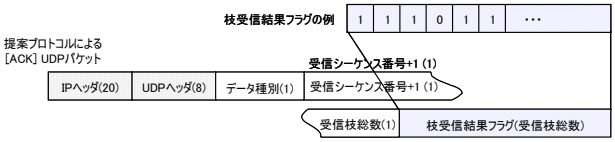

図４　ACK UDP パケット

具体的な自動発呼シーケンス例を**図５**に示す。遠隔監視ユニットのアプリケーションは，RS-232C シリアルポートから入力されたデータを，送信用データの引数として，送信用 API を呼ぶ。送信用 API は，遠隔監視ユニットと仲介サーバ間で認証を行い，その後遠隔監視ユニットと保守管理端末間でセッションが成立すると，UDP によるデータ通信が開始される。遠隔監視ユニットから，複数の UDP パケットに対して受信側が ACK を返信し，同一シーケンス番号の全ての枝パケットが受信されるまで，未到達枝データの再送を行う。アプリケーションがデータ送信を完了し，接続終了 API を呼ぶと，コネクション切断が行われる。

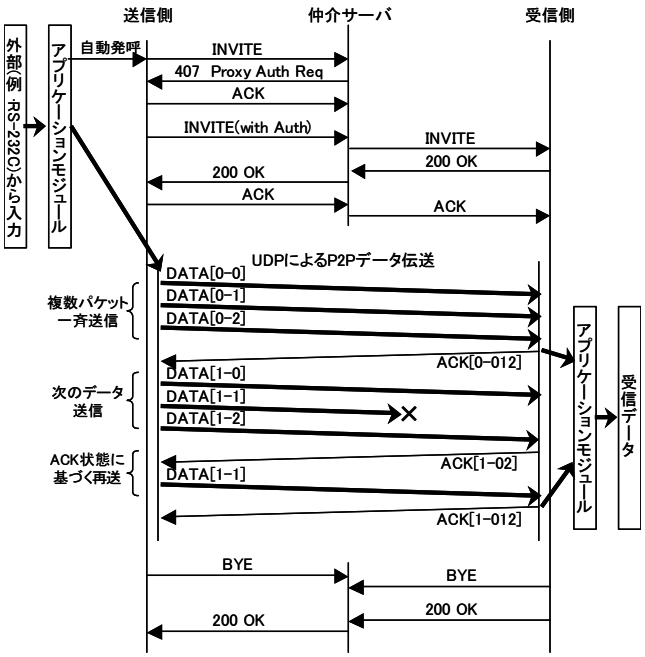

図５　提案方式による通信シーケンス

3.3　認証・暗号化プロトコル

通信相手のなりすまし，および通信データの盗聴や改竄を防ぐために，端末間接続プロトコルに認証および暗号化，データ通信プロトコルに暗号化を実装した。暗号化ソフトウェアとして，オープンソフトウェアの1つである OpenSSL[2] を用いた。

A．接続プロトコル（SIP）

相互に端末の認証を行うために独自に認証局を用意し，この認証局から発行された証明書を用いて，仲介サーバと保守管理端末間，および仲介サーバと遠隔監視ユニット間の相互認証を TLS 方式で行った。また，仲介サーバへの問い合わせや，IP アドレスなどのデータ登録時に行うデータ送受信の暗号化は，AES 方式で行った。

B．データ通信プロトコル

SIP セッション終了後にデータ通信を行うが，データ暗号化に，共通鍵（AES 256bit）を用いた。共通鍵はあらかじめ保守管理端末，遠隔監視ユニット両方に同じ鍵テーブルを持ち，仲介サーバにはないため，仲介サーバが保守管理端末，遠隔監視ユニット間のデータを中継してもデータを盗聴することは困難である。

4　通信試験

前報で記した仲介サーバ，保守管理端末，遠隔監視ユニットとして SH ボードで通信試験を行った。遠隔監視ユニットには USB カメラを接続し，２つの NAT には Symmetric NAT を用いた。Symmetric NAT では，通信開始毎に WAN 側に割り当てられるポートが変化するため，保守管理端末と遠隔監視ユニット間のデータ送受信すべて仲介サーバを中継させた。通信試験の全体概観写真を**図６**に示す。

SIP のデータが暗号化されているか確認するため，パケットモニタリングソフト（WireShark[3]）を用いて通信のモニタリングを行った。**図７**のモニタリング結果より，仲介サーバと保守管理端末間，仲介サーバと遠隔監視ユニット間で暗号化が行われている様子が確認できる。

図８に保守管理端末が，遠隔監視ユニットをモニタリングしている様子を示す。２つの遠隔監視ユニット

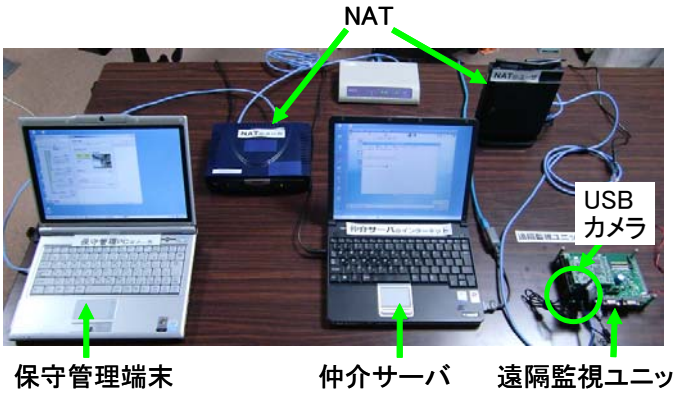

図６　通信試験の様子

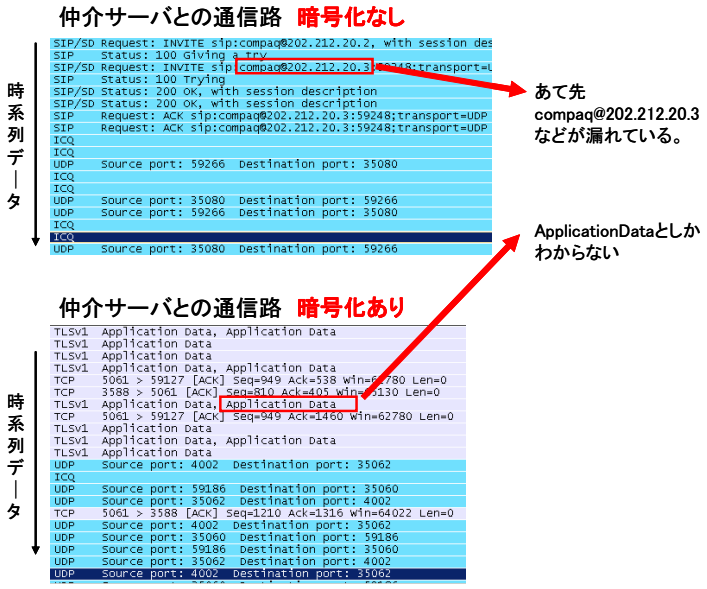

図７　仲介サーバと保守管理端末間の接続プロトコルの暗号化

を同時にモニタリングできていることがわかる。

データ転送速度は，平均 3.27Mbps であった。動画像伝送の標準方式の 1 つとして MPEG1 があるが，この映像伝送に必要なデータ転送速度は 1.150Mbps である。通信試験の結果(3.27Mbps)は，MPEG1 に必要なデータ転送速度の２倍以上であるため，提案したデータ通信方式が動画像伝送にも対応できることがわかる。

図８　保守管理端末画面

５　結　　言

本報では，前報で示したプロトコルの改善，実装時の通信速度計測，および動作確認を行った。詳細を以下に示す。

１．端末間接続プロトコルの改善を行い，例外処理に対応可能とした。
２．通信速度を高速化するために，データ通信に用いた RTP プロトコルから UDP プロトコルへ変更し，さらに確認応答処理の改善を行った。その結果データ転送速度が 3.27Mbps となり，動画像伝送にも使用可能であることがわかった。
３．仲介サーバと保守管理端末および遠隔監視ユニットの接続プロトコルの暗号化および認証を実装した。
４．保守管理端末から同時に２箇所の遠隔監視ユニットへ，データ通信を可能とした。

文　　献

１）村河他：広島県西部工技研究報告，51（2008），１
２）http://www.openssl.org/
３）http://www.wireshark.org/