東京大学地震研究所技術研究報告，No. 10，32–42 頁，2004 年.
Technical Research Report, Earthquake Research Institute, The University of Tokyo, No. 10, pp. 32–42, 2004.

常時接続型通信回線を用いた地震観測点の設置技術とセキュリティー

芹澤正人*†・橋本信一*・羽田敏夫*・小林　勝*・五十嵐俊博**

Installation Technology and Security of the Station Observing Earthquake Always Using the Connected Type Communication Circuit

Masato SERIZAWA*†, Shinichi HASHIMOTO*, Toshio HANEDA*, Masaru KOBAYASHI* and Toshihiro IGARASHI**

Abstract

The paper describes the installation method, the maintenance, and the measure against security of an observing point which always used the connected type communication circuit. This system used "Flets group access". Moreover, it enabled them to shorten the working hours in the spot for installation sharply, and to start many observing points for a short period of time by using the remote setup by the ISDN.

Key words : Internet, ISDN, Flets, Group access, TCP/IP

は　じ　め　に

このたび，東京大学地震研究所は「大都市大震災軽減化特別プロジェクト」（略称「大大特」）において千葉県房総半島の地殻構造探査を行うことになり，房総半島を南北に貫く測線上に 30 点の観測点を設置した.

このうち 4 点は既に実績のある衛星テレメータを利用し，残りの 26 点については電話線を利用した有線テレメータを使用することとなった．今回は観測網のシステム設計と構築及び，有線テレメータ観測点の立ち上げについて報告する.

ネットワークの選定

収録用サーバーは地震研本館 6 階・テレメータ室に設置することとした．サーバーには 3 つのイーサネットポートを用意し，それぞれ，所内 LAN，所内サーバーからのブロードキャスト受信（Hi-net 他），有線テレメータ観測点のそれぞれのネットワークに接続してある.

衛星テレメータ観測点からのデータは所内サーバーを経由して本サーバーに蓄積される．有線テレメータについてはインターネット経由よりもコストパフォーマンスの高い，フレッツグループアクセスを利用することとなった.

フレッツグループアクセスは，NTT 東日本がフレッツ契約回線向けに提供しているプライベートネットワークサービスである.

インターネット経由の場合，観測点ごとにプロバイダー契約が必要となり，固定 IP アドレスを使用するためには使用料が非常に高額となってしまう.

フレッツグループアクセスでは，グループに対して NTT からプライベート IP アドレス群が割り当てられ，ユーザー ID とプライベート IP アドレスを 1 対 1 で対応させられるため，別途固定 IP アドレス使用料金を払う必要がない.

インターネットには接続できないが，今回はそれは必要ないため問題は無い．逆に他の無関係なパケットが入ってこない，完全に閉じたネットワークなのでセキュリティーが非常に高く，今回の目的には最適である.

今回はフレッツグループアクセス・ライトを利用し，3 つのグループを構築する.

なお，フレッツグループアクセス・プロでは 1 グループ

2004 年 10 月 6 日受付，2004 年 11 月 22 日受理.
† serizawa@eri.u-tokyo.ac.jp
* 東京大学地震研究所技術部総合観測室,
** 地震地殻変動観測センター.
* Technical Supporting Section for Observation Research,
** Earthquake Observation Center, Earthquake Research Institute, The University of Tokyo.

で最大 30 点を結ぶことができるが，利用料が高いのと，地震観測ではすべてが同一グループに所属している必要はないので見送った．

フレッツグループアクセスの受け口としてＢフレッツベーシックを 1 回線用意し，また，地震地殻変動観測センターが既に引いているＢフレッツも利用することになった．これは，グループアクセスでは 1 グループにつき 1 セッション必要となるが，Ｂフレッツ・ベーシックでは最大接続数が 2 セッションであり，3 グループの設置には 2 回線必要となるからである．

回線種別の選択

観測点においては，地震計からのアナログデータを 200 Hz/24 bit/3 ch で A/D 変換し，1 秒ごとに WIN フォーマットのパケットにした上で送信している．WIN フォーマットではΔPCM によって平常時にはパケットサイズが非常に小さくなるが，データの取りこぼしを防ぐためにイベント時のピークレートを最大値 Rmax として，この値よりも通信速度が速い回線を選択する必要がある．また，今回採用した LS-7000XT では，毎秒約 3 KB のステータスパケットが送られてくるのでこれも合算する．

今回の場合，1 観測点当たりのピークレートは

Rmax＝200×24×3＋1024×3×8＝38976（bps）

となり，フレッツシリーズの中で一番遅い ISDN の 64 Kbps（1 K＝1,024）よりも下回るため，理論上はフレッツシリーズのどの回線でも利用が可能である．今回はコストやメンテナンス上の理由から ISDN を選択した．

なお，この計算においては TCP/IP パケットサイズ 40 bytes を便宜的に省いた．このため実ピークレートはこの値の 1.2〜1.3 倍程度となる．

サーバー側においては，1 セッション当たり 9 観測点のデータをピーク時でも取りこぼさない程度の太い回線が必要となる．実際には 1 回線で最大 18 観測点のデータを受けるが，一般にはセッション当たりの最大通信速度を用いているためこのような計算となる．ただし，フレッツ網のハードウェア的制限から，Ｂフレッツにおいては現在のところ 1 回線当たり 100 Mbps（1 M＝1,024 K）が最大値となる．この制限についての技術的解説は本筋から外れるので割愛させていただく．

以上をまとめると，サーバー側の回線でのピークレート RSmax は，

RSmax＝Rmax×9＝38976×9＝350784（bps）

となり，Ｂフレッツ　ベーシックの最大通信速度である 100 Mbps を十分下回る．

なお，フレッツ ADSL の選択も可能であるが，ADSL の場合，その回線特性により通信速度が動的に変化し，安定した帯域確保が難しい．導入に当たっては十分に通信速度を調査して RSmax を下回らないことを確認する必要がある．Ｂフレッツの場合光ファイバーであるため外的要因による影響を受けにくく，通信速度が安定している．

観測点設置機器の選択

有線テレメータ観測点には以下のような機器の設置が必要となる．

・地震計
・避雷器
・A/D 変換装置
・WIN パケット生成装置
・IP パケット変換装置
・ルーター
・モデム（またはターミナルアダプタ）
・UPS
・その他

大大特においては，A/D 変換装置・WIN パケット生成装置・IP パケット変換装置の 3 つの機能を統合した製品として，LS-7000XT（白山工業(株）製）を採用した．ルーターにはターミナルアダプタ機能を内蔵している RTA55i（YAMAHA 製）を使用し，観測局舎内の省スペース化を図った．UPS は ES500（APC 製）を使うことで停電時約 1 時間の運用が可能となった．LS-7000XT には 128MB のコンパクトフラッシュ（CF）を挿入してあり，データを送信しながら CF 上に書き込んでいくため，理論上停電前 2〜3 日間＋停電後 1 時間程度のデータ記録が可能である．

これらの機器を選定するにあたり，「既製品」「入手が容易である」「低価格」「設置・設定作業がルーチン化できる」などといった点を重視した．一般的に屋外に設置する観測機器には耐久性を高めるために特注品であったり特殊加工されるものが多く，同等の民生品に比べて非常に高価であった．今回は房総半島というアクセスの良さを生かし，トラブル時には迅速に機器交換を行うことで耐久性をカバーすることとした．

サーバー設置作業

観測点を立ち上げる前にサーバーを設置し（図 1 及び図 2），Ｂフレッツ回線をルーター経由にて接続した．サーバーのスペックは表 1 のとおりである．衛星テレメータ観測点のデータについては所内 LAN を経由して受信し，Hi-net のデータも一部収録している．フレッツグループアクセスは事前に 3 つのグループを開設し，サーバーの回線が管理者となるように設定を行った．

ルーターはグループごとに 1 台ずつを割り当て，LAN 側は HUB でまとめてサーバーに繋がっている（図 3）．

ここで観測点からのパケットの流れを整理してみる．

各観測点の LS-7000XT から送信されたパケットはルー

図 1.　収録サーバーが格納されているラック

図 2.　収録サーバー（上段）
サーバーの下にはディスクアレイと DAT ドライブが置かれている

ターを 2 つ経由しグループアクセスのネットワークを越えて最終的にグループアクセスのプライベート IP アドレスを送信元とするパケットとしてサーバーで受信する．再送要求パケットも同様に観測点の LS-7000XT で受信する．これらの動作を実現するために，各ルーターは自分宛のパケットをすべて LAN 側の特定の IP アドレスへ送る設定（NAT および静的 IP マスカレード）が必要となる．

表 1.　サーバーのスペック（抜粋）

CPU	Intel XEON Processor ×2 (dual)
Memory	2GBytes
RAID	1.4TBytes
Ethernet	3channels
DAT	DDS-4

図 3.　サーバー側に設置したルーター

今回は
nat masquerade static 1 192.168.0.10*
などとして，WAN 側からのすべてのポートへのパケットをサーバーもしくは LS-7000XT に送る設定とした．また，サーバーのルーティングも設定し，観測点宛のパケットがそれぞれの所属するグループに接続されたルーターを経由するようにした．

観測点設置作業

観測点には引込柱を建て，機器類の収容ボックスをそれに抱かせるように設置し，その内部へ電気・電話を引き込んだ．ブレーカー・保安器等も内部設置とし，電気メーターと GPS アンテナのみを外付けとした．地震計はセメントを流し込んで作った地震計台の上に設置した（図 4 及び図 5）．

地震計からの信号はアレスタを通り端子盤を経由して LS-7000XT に入る．LS-7000XT とルーターは LAN で結ばれており，パケット化されたデータはルーターを経由してフレッツ網へと送られていく．原則としてすべての電源は UPS でバックアップしている．

図 4.　観測点全景
手前の円筒形容器内に地震計が入っている

機器設定作業（1）

観測点内のネットワークは以下の通りとした．

・ネットワークアドレス	192.168.0.0/24
・デフォルトゲートウェイ	192.168.0.1
・DNS	なし
・ルーター IP アドレス	192.168.0.1
・LS-7000XT IP アドレス	192.168.0.10

設定作業は様々な試行を繰り返し，以下のような手順に落ち着いた．

LS-7000XT は設定情報を CF にファイルとして保存するため，あらかじめパソコンで資料 1 のような設定ファイルを作って CF に保存しておく．

ルーターの電源を入れノートパソコンを LAN で接続し，パソコンの TCP/IP 設定を固定 IP で 192.168.0.0/24 の後方のアドレス（例えば 192.168.0.250）にする．これは，ルータの DHCP とコンフリクトするのを避ける為である．デフォルトゲートウェイはルーターのアドレスにする．

適当なブラウザーでルーターの初期画面を開いてパスワードを設定しておく．もしパスワードが設定されていない場合，ISDN 回線からの remote setup を受け付けないので注意が必要である．

その他，一部の回線では回線の極性が反転して，ルーターが正常に動作しない場合もあるので注意が必要である．実際，いくつかの観測点では極性が反転していたが，ルーターの極性反転スイッチを切り替えることで正常に接続できるようになった．

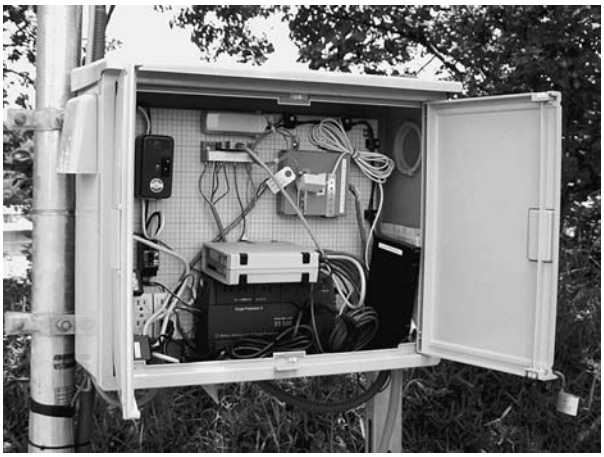

図 5.　格納ボックス内の様子

LS-7000XT の電源を入れ，待機状態になったらパソコンから telnet で LS-7000XT にアクセスし，TCAL コマンド等で正常動作していることを確認する．

ここまでの作業で，ルーターと LS-7000XT のネットワークが正しく接続されていることが確認できたので，ハードウェアの設置作業は終了である．

機器設定作業（2）

これ以降の作業については現地で行うこともできるが，遠隔地から ISDN 回線を使った設定もできる．観測点に引いている ISDN 回線は INS64 と呼ばれ，64 Kbps の同期通信が可能なチャンネル（B）を 2 本持っているため同時に 2 回線の通信が可能である．フレッツ ISDN は B チャンネルを 1 本占有するので，残った 1B で通話やダイヤルアップ接続を行うことができる．これを利用し，フレッツ接続を行いつつ，ルーターのリモートセットアップやダイヤルアップ接続によって各種設定を行う．ADSL で同様のシステムを実現するには観測点にアナログモデムやサーバーの設置が必要になる．

回線に観測点と同じルーターを接続し，パソコンを接続する．このとき，観測点側と同じネットワークアドレスではルーティングができないことがあるので，設定側 LAN を 192.168.100.0/24 のネットワークにするなどの処置が必要となる．

適当な telnet クライアントでルーターにアクセスする．
administrator mode に切り替えてから，
remote setup（観測点の電話番号）（Enter）
でルーター同士がセットアップモードで接続され，観測点側のルーターのパスワードを訊ねてくるので入力する．プ

ロンプトが出て入力待ちになるが，この時点で観測点のルーターにLANからtelnetで入ったのと同じ状態になっており，show configコマンドを実行すると観測点側ルーターの設定情報などが見れる．

再度administratorコマンドを実行して観測点側ルーターの設定が行えるように準備する．

ここからすべて手作業で入力することもできるが，非常に多くの手間がかかるため，事前に用意しておいた資料2のようなテキストファイルをテキストエディタでグループアクセスのユーザー名とパスワードの部分を適宜編集してから通信ソフトのファイル送信機能でルーターに流し込む．具体的にはpp select 1以下にあるpp auth mynameコマンドの引数を，先にグループ開設時にNTTから提供されたユーザー名とパスワードに変更する．例えばグループ名がes000999.galight.flets, ユーザー名がuser02, パスワードがuser02なら，

pp auth myname user02@es000999.galight.flets user02

となる．ただしこの時点ではまだグループアクセスの利用申請を行っていないため，

pp connect 1 (Enter)

などとしても接続できない．

更に観測点へのダイヤルアップ接続を受け付けるために，pp select anonymous以下のpp auth usernameを適当なユーザー名とパスワードに変更する．このユーザー情報はセキュリティー上非常に重要なので取り扱いに注意する．

グループアクセスの利用申請を行うためにフレッツスクエアへ接続する必要があるが，先の設定ファイルのpp select 2以下がその接続設定となっており，

pp connect 2（Enter）

とするだけで接続できる．ここでエラーが出たり，

show status pp 2（Enter）

で接続できていない旨のメッセージが表示された場合にはフレッツISDNの利用契約が完了していない可能性がある．

接続を確認したらsaveしてからexitコマンドを数回実行してリモートセットアップを終了する．

観測点へダイヤルアップ接続するために，ルーターに端末型のダイヤルアップ接続設定を行う．ユーザー名とパスワードを先ほどpp select anonymous以下で設定したものにする．電話番号は観測点の電話番号である．

観測点にダイヤルアップ接続し，ブラウザーでhttp://www.flets/を開く．DNSがうまく引けない場合はパソコンのネットワーク設定でDNSサーバを手動設定する．DNSのアドレスはルーターにtelnetで入り，show status pp 2で得られるステータスのPPPオプションの中に書かれている．設定時のトラブルはほとんどこの部分に集中しており，その多くがdnsによるフレッツスクエアのwebサイトの参照ができないことである．今回使用したルーターはDNS代理応答が可能であるが，観測点ルーターがフレッツスクエアに未接続の状態ではDHCPの応答にDNSのIPアドレスが含まれていない．このため，DNSのアドレスを手作業でパソコンに登録する必要がある．しかし，OSによっては直前まで接続していたネットワークの設定やDNSキャッシュが反映されてしまうことがあり，この場合,．fletsというドメイン名を正しく認識できずドメイン正引きに失敗する．

このような障害が発生したときはしばらく放置することで正常動作するようになることもある．パソコンの再起動も有効な手段である．

以降はサーバーでのグループアクセスの利用登録と同様に行うが，既存のグループへの参加であることに留意する．

登録後，開通までの時間は半日〜1日程度である．

機器設定作業（3）

再度観測点へダイヤルアップ接続し，ルーターにtelnetでアクセスしてadministrator modeでpp2を切断し，pp1を接続してフレッツスクエアからグループアクセスに切り替える．show statusコマンドを実行すると，正常であればDHCPによってグループ内のユーザーIDに対応したIPアドレスが割り当てられているはずである．接続できない場合はpp2の接続が切れているか，ユーザーIDやパスワードが間違っていないかなどを確認する．

ここまでで，観測点はサーバーとネットワークで結ばれた状態になっているので，サーバーのルーティングテーブルを設定してtelnetで観測点にアクセスする．LS-7000XTがプロンプトを返したら

ZLT（Enter）

ALT（Enter）

で観測を停止→再起動（開始）させ，しばらく待ってからサーバーでWINパケットの受信を確認する．

サーバーから観測点にftpでアクセスすると，CFのデータをダウンロードしたり，設定ファイルをアップロードしたりすることができる．これを利用して，変更した設定ファイルをftpでCFのルートディレクトリにアップロードし，telnetで再起動をかけることでリモートでLS-7000XTの設定を変更することができる．ただし，この方法についてはメーカーでは公式に認めていない．

セキュリティーの確保

このようにして構築したフレッツグループアクセスによる地震観測ネットワークは，インターネットと直接接続されていないためインターネットからの一般的なクラッキン

グ攻撃を受ける心配がない．しかし二つのセキュリティーホールがある．

一つは観測点へのダイヤルアップ接続である．設定のために観測点へのダイヤルアップ接続が行えるようになっており，ここを踏み台としてサーバーへのアタックが可能である．また，LS-7000XT に telnet でログインし，観測を停止させることも不可能ではない．これを行うために必要な情報は，

・観測点の電話番号
・ダイヤルアップ接続のユーザー ID とパスワード
・サーバーの IP アドレス

である．ただし，設定終了後にダイヤルアップサーバー機能をオフにすることで，ここからの侵入は防ぐことができる．

もう一つの穴は観測点ルーターへのリモートセットアップである．アドミニストレーターモードまで入られた場合，ダイヤルアップ接続の情報などを盗まれてしまうだけでなく，設定を変更してデータが飛ばなくなるようにすること（クラッキング）もできてしまう．この場合，

・観測点の電話番号
・ルーターのパスワード

が必要だが，同じ機種同士でなければリモートセットアップできないため，カジュアルクラッキング的な行為ではアタックされることはないと思われる．しかし，悪意を持った第三者が観測点の電話番号に関する情報を得た場合，誰にも気づかれずに総当り的なパスワードクラッキングが可能になるため，非常に危険である．

これらに共通するのは観測点の電話番号である．ルーターに設定した各種パスワードも厳重な扱いが必要だが，電話番号もそれと同等に扱いには十分気をつけなければならない．また，観測点のパスワードは定期的に変更することも重要である．

運用中のメンテナンス

実際に観測が始まると，いくつかの問題が浮き彫りになった．

LS-7000XT のデジタルフィルターの特性を変更するためにサーバーから ftp で観測点の LS-7000XT にアクセスし，設定ファイルを書き換えてから telnet でリブートをかけたところ観測が再開しなかった．現地で LS-7000XT をチェックすると，設定ファイルに異常があるというメッセージを出したまま停止していた．設定ファイルの記述ミスによって起動中にエラーで停止していることがわかったが，例えば設定ファイルをネットワーク関係・A/D 変換関係といった具合に項目別に分けて，読み込み時にエラーが発生しても無関係な設定情報には影響を与えずにできるだけ起動する方向に自己修復する機能があればこのようなトラブルでも現地作業無しに復旧することが可能であろうと思われる．

設置機器の耐久性という面では，設置開始初年度の夏季に日中気温が上昇するのに比例して局舎内部温度も上昇し，LS-7000XT が動作可能温度を超えてハングアップしてしまうというトラブルに何度か見舞われた．これについてはファームウェアのバージョンアップによって気温低下後の復旧確率が上がり，現地での復旧作業が格段に減った．その他ルーターなどは特に故障は無く，民生品のほうが非常に安定している結果となった．

地域 IP 網の工事などによって回線が切断されることがあるが，概ね回線復旧後に再接続が成功している．Link Down 状態が長時間続くとルーターの仕様により自動再接続しないことがあるが，この場合はリモートセットアップで connect コマンドを送ることで手動接続する．

今 後 の 課 題

システム上の制限により，9 観測点につきサーバー側回線 1 セッションが必要になるため大規模な観測網ではサーバー側に必要な回線が多くなり，非常に効率が悪くなってしまう．これを解消するためには，観測点をグループ同士のブリッジとして利用し，データを中継することでサーバー側回線のセッション数を減らす方法がある．この方法では，サーバーがグループアクセス経由で直接アクセスできない観測点が生じるため，それらに対する制御や再送要求などをどのように行うかという課題がある．

また，前述したように現在のシステムでは回線障害などからの復旧時にフレッツ網への再接続がうまくいかない場合には手作業で接続する必要があるが，この作業を含め観測点の異常を検知し，自動的に対処するサーバーの設置を検討中である．このサーバーは収録サーバー側ルーターと収録サーバーの間に設置し，観測点からのパケットロストなどの監視を行いつつデータを転送するものである．また，メンテナンス用ルーターを接続し，リモートセットアップにも対応する．このサーバーの設置により，観測網のメンテナンス性が向上するものと期待される．

謝　辞：今回のシステム設計にあたり，グループアクセスについての情報を提供して下さった日立エンジニアリング（株）コミュニケーションシステム部の小野寺様，サーバー側回線の引き込みについてのアドバイスや既設回線の借用を快諾して下さった地震地殻変動観測センターの卜部助教授，およびプロジェクト全般に渡ってご協力いただいた地震地殻変動観測センターの皆様に厚く御礼申し上げます．

資料 1.　LS-7000XT の設定ファイル
（一部マスク処理）

```
<?xml version="1.0" ?>
<ls7000 version="0.91">
        <title>DATAMARK</title>
        <measure>
                <channel>
                        <ch>1</ch>
                        <win>****</win>
                        <gain unit="dB">0</gain>
                        <frequency unit="Hz"> 200</frequency>
                        <bits>24</bits>
                </channel>
                <channel>
                        <ch>2</ch>
                        <win>****</win>
                        <gain unit="dB">0</gain>
                        <frequency unit="Hz"> 200</frequency>
                        <bits>24</bits>
                </channel>
                <channel>
                        <ch>3</ch>
                        <win>****</win>
                        <gain unit="dB">0</gain>
                        <frequency unit="Hz"> 200</frequency>
                        <bits>24</bits>
                </channel>
                <channel>
                        <ch>4</ch>
                        <win>0003</win>
                        <gain unit="dB">OFF</gain>
                        <frequency unit="Hz"> 100</frequency>
                        <bits>24</bits>
                </channel>
                <channel>
                        <ch>5</ch>
                        <win>0004</win>
                        <gain unit="dB">OFF</gain>
                        <frequency unit="Hz"> 100</frequency>
                        <bits>24</bits>
                </channel>
                <channel>
                        <ch>6</ch>
                        <win>0005</win>
                        <gain unit="dB">OFF</gain>
                        <frequency unit="Hz"> 100</frequency>
                        <bits>24</bits>
                </channel>
                <filter>LINEAR</filter>
                <cut_off unit="%">20</cut_off>
        </measure>
        <trigger>
                <sta_lta_trigger>
                        <channel>1</channel>
                        <lopass>   40</lopass>
                        <hipass> 160</hipass>
                        <sta> 1280</sta>
                        <lta>10240</lta>
                        <s_l_begin> 3</s_l_begin>
                        <s_l_end> 2</s_l_end>
                        <s_l_count> 3</s_l_count>
                </sta_lta_trigger>
                <level_trigger>
                        <channel>1</channel>
                        <level unit="count">      50</level>
                </level_trigger>
        </trigger>
        <record>
                <trigger>ALL</trigger>
                <pre_trigger unit="sec"> 20</pre_trigger>
```

資料 1. （つづき）

```
                <post_trigger unit="sec"> 60</post_trigger>
                <overwrite>YES</overwrite>
        </record>
        <communication>
                <com1>
                        <baud unit="bps">38400</baud>
                        <bits>8</bits>
                        <parity>none</parity>
                        <stopbits>1</stopbits>
                        <flowctrl>NONE</flowctrl>
                </com1>
                <com2>
                        <baud unit="bps">38400</baud>
                        <bits>8</bits>
                        <parity>none</parity>
                        <stopbits>1</stopbits>
                        <flowctrl>NONE</flowctrl>
                </com2>
                <tcpip>
                        <IPaddress>***.***.***.***</IPaddress>
                        <netmask>255.255.255.000</netmask>
                        <default_gateway>***.***.***.***</default_gateway>
                        <device>ETHERNET</device>
                </tcpip>
                <win_udp>
                        <IPaddress>***.***.***.***</IPaddress>
                        <win_port> ****</win_port>
                        <mywin_port> ****</mywin_port>
                        <status_port> ****</status_port>
                        <mystatus_port> ****</mystatus_port>
                </win_udp>
                <realtime_output>
                        <device>WIN_UDP</device>
                        <win_format>A0</win_format>
                        <setting_output>MINUTE</setting_output>
                        <motion_output>MINUTE</motion_output>
                </realtime_output>
        </communication>
        <time_cal>
                <location>
                        <timezone>-09:00</timezone>
                        <latitude>N3540.4362</latitude>
                        <longitude>E13928.3876</longitude>
                        <altitude>000108.0</altitude>
                </location>
                <mode>AUTO</mode>
                <interval> 0:00</interval>
                <adjust>ON</adjust>
        </time_cal>
</ls7000>
```

資料 2.　ルーターの設定ファイル
一部セキュリティ上の都合によりマスクしてある

```
# RTA55i Rev.4.06.54 (Thu Apr 24 01:58:55 2003)
# MAC Address : 00:**:**:**:**:**, 00:**:**:**:**:**
# Memory 8Mbytes, 2LAN, 1BRI
ip filter 1 pass * * * * *
ip filter 100000 reject * * udp,tcp 135 *
ip filter comment 100000 "Windows: DCE RPC"
ip filter 100001 reject * * udp,tcp * 135
ip filter comment 100001 "Windows: DCE RPC"
ip filter 100002 reject * * udp,tcp netbios_ns-netbios_dgm *
ip filter comment 100002 "Windows: NetBIOS (NS,Datagram)"
ip filter 100003 reject * * udp,tcp * netbios_ns-netbios_dgm
ip filter comment 100003 "Windows: NetBIOS (NS,Datagram)"
ip filter 100004 reject * * udp,tcp netbios_ssn *
ip filter comment 100004 "Windows: NetBIOS (SSN)"
ip filter 100005 reject * * udp,tcp * netbios_ssn
ip filter comment 100005 "Windows: NetBIOS (SSN)"
ip filter 100006 reject * * udp,tcp 445 *
ip filter comment 100006 "Windows: Direct Hosting SMB"
ip filter 100007 reject * * udp,tcp * 445
ip filter comment 100007 "Windows: Direct Hosting SMB"
ip filter 100099 pass * * * * *
ip filter comment 100099 "pass all"
ip filter 200000 reject 10.0.0.0/8 * * * *
ip filter comment 200000 "Ingress/in: Private A"
ip filter 200001 reject 172.16.0.0/12 * * * *
ip filter comment 200001 "Ingress/in: Private B"
ip filter 200002 reject 192.168.0.0/16 * * * *
ip filter comment 200002 "Ingress/in: Private C"
ip filter 200003 reject 192.168.0.0/24 * * * *
ip filter comment 200003 "Ingress/in: LAN1 Primary"
ip filter 200010 reject * 10.0.0.0/8 * * *
ip filter comment 200010 "Ingress/out: Private A"
ip filter 200011 reject * 172.16.0.0/12 * * *
ip filter comment 200011 "Ingress/out: Private B"
ip filter 200012 reject * 192.168.0.0/16 * * *
ip filter comment 200012 "Ingress/out: Private C"
ip filter 200013 reject * 192.168.0.0/24 * * *
ip filter comment 200013 "Ingress/out: LAN1 Primary"
ip filter 200020 reject * * udp,tcp 135 *
ip filter comment 200020 "Windows: DCE RPC"
ip filter 200021 reject * * udp,tcp * 135
ip filter 200022 reject * * udp,tcp netbios_ns-netbios_ssn *
ip filter comment 200022 "Windows: NetBIOS"
ip filter 200023 reject * * udp,tcp * netbios_ns-netbios_ssn
ip filter comment 200023 "Windows: NetBIOS"
ip filter 200024 reject * * udp,tcp 445 *
ip filter comment 200024 "Windows: Direct Hosting SMB"
ip filter 200025 reject * * udp,tcp * 445
ip filter comment 200025 "Windows: Direct Hosting SMB"
ip filter 200026 restrict * * tcpfin * www,21,nntp
ip filter comment 200026 "Netscape: connect on finished"
ip filter 200027 restrict * * tcprst * www,21,nntp
ip filter comment 200027 "Netscape: connect on finished"
ip filter 200030 pass * 192.168.0.0/24 icmp * *
ip filter comment 200030 "LAN1 Primary/in: ICMP (ping,traceroute,...)"
ip filter 200031 pass * 192.168.0.0/24 established * *
ip filter comment 200031 "LAN1 Primary/in: TCP Connection (established)"
ip filter 200032 pass * 192.168.0.0/24 tcp * ident
ip filter comment 200032 "LAN1 Primary/in: ident for SMTP,... (e-mail)"
ip filter 200035 pass * 192.168.0.0/24 udp domain *
ip filter comment 200035 "LAN1 Primary/in: dns resolv"
ip filter 200036 pass * 192.168.0.0/24 udp * ntp
ip filter comment 200036 "LAN1 Primary/in: NTP server"
ip filter 200037 pass * 192.168.0.0/24 udp ntp *
ip filter comment 200037 "LAN1 Primary/in: NTP client"
ip filter 200099 pass * * * * *
ip filter comment 200099 "pass all"
ip filter 201000 reject 10.0.0.0/8 * * * *
```

資料 2. （つづき）

```
ip filter comment 201000 "Ingress/in: Private A"
ip filter 201001 reject 172.16.0.0/12 * * * *
ip filter comment 201001 "Ingress/in: Private B"
ip filter 201002 reject 192.168.0.0/16 * * * *
ip filter comment 201002 "Ingress/in: Private C"
ip filter 201003 reject 192.168.0.0/24 * * * *
ip filter comment 201003 "Ingress/in: LAN1 Primary"
ip filter 201010 reject * 10.0.0.0/8 * * *
ip filter comment 201010 "Ingress/out: Private A"
ip filter 201011 reject * 172.16.0.0/12 * * *
ip filter comment 201011 "Ingress/out: Private B"
ip filter 201013 reject * 192.168.0.0/24 * * *
ip filter comment 201013 "Ingress/out: LAN1 Primary"
ip filter 201020 reject * * udp,tcp 135 *
ip filter comment 201020 "Windows: DCE RPC"
ip filter 201021 reject * * udp,tcp * 135
ip filter comment 201021 "Windows: DCE RPC"
ip filter 201022 reject * * udp,tcp netbios_ns-netbios_ssn *
ip filter comment 201022 "Windows: NetBIOS"
ip filter 201023 reject * * udp,tcp * netbios_ns-netbios_ssn
ip filter comment 201023 "Windows: NetBIOS"
ip filter 201024 reject * * udp,tcp 445 *
ip filter comment 201024 "Windows: Direct Hosting SMB"
ip filter 201025 reject * * udp,tcp * 445
ip filter comment 201025 "Windows: Direct Hosting SMB"
ip filter 201026 restrict * * tcpfin * www,21,nntp
ip filter comment 201026 "Netscape: connect on finished"
ip filter 201027 restrict * * tcprst * www,21,nntp
ip filter comment 201027 "Netscape: connect on finished"
ip filter 201030 pass * 192.168.0.0/24 icmp * *
ip filter 201032 pass * 192.168.0.0/24 tcp * ident
ip filter comment 201032 "LAN1 Primary/in: ident for SMTP,... (e-mail)"
ip filter 201033 pass * 192.168.0.0/24 tcp ftpdata *
ip filter comment 201033 "LAN1 Primary/in: ftp client (PORT)"
ip filter 201034 pass * 192.168.0.0/24 tcp,udp * domain
ip filter comment 201034 "LAN1 Primary/in: dns server"
ip filter 201035 pass * 192.168.0.0/24 udp domain *
ip filter comment 201035 "LAN1 Primary/in: dns resolv"
ip filter 201036 pass * 192.168.0.0/24 udp * ntp
ip filter comment 201036 "LAN1 Primary/in: NTP server"
ip filter 201037 pass * 192.168.0.0/24 udp ntp *
ip filter comment 201037 "LAN1 Primary/in: NTP client"
ip filter 201099 pass * * * * *
ip filter comment 201099 "pass all"
ip filter 500000 restrict * * * * *
ip filter dynamic 200080 * * ftp
ip filter dynamic comment 200080 "FTP connection (tcp)"
ip filter dynamic 200081 * * domain
ip filter dynamic comment 200081 "DNS resolv,... (tcp,udp)"
ip filter dynamic 200082 * * www
ip filter dynamic comment 200083 "SMTP connection (tcp)"
ip filter dynamic 200084 * * pop3
ip filter dynamic comment 200084 "POP3 connection (tcp)"
ip filter dynamic 200098 * * tcp
ip filter dynamic comment 200098 "TCP Connection"
ip filter dynamic 200099 * * udp
ip filter dynamic comment 200099 "UDP Connection"
ip filter dynamic 201080 * * ftp
ip filter dynamic comment 201080 "FTP connection (tcp)"
ip filter dynamic 201081 * * domain
ip filter dynamic comment 201081 "DNS resolv,... (tcp,udp)"
ip filter dynamic 201082 * * www
ip filter dynamic comment 201082 "WWW Browser,... (tcp)"
ip filter dynamic 201083 * * smtp
ip filter dynamic comment 201083 "SMTP connection (tcp)"
ip filter dynamic 201084 * * pop3
ip filter dynamic comment 201084 "POP3 connection (tcp)"
ip filter dynamic 201098 * * tcp
ip filter dynamic comment 201098 "TCP Connection"
ip filter dynamic 201099 * * udp
```

資料 2. （つづき）

```
ip filter dynamic comment 201099 "UDP Connection"
ip filter source-route on
ip filter directed-broadcast on
ip lan1 address 192.168.0.1/24
ip lan1 routing protocol none
ip lan1 rip listen none
ip lan1 secure filter in 100000 100001 100002 100003 100004 100005 100006 100007 100099
ip lan2 routing protocol none
ip lan2 rip listen none
ip route 172.26.0.0/16 gateway pp 2
ip route default gateway pp 1 filter 500000 gateway pp 1
nat descriptor type 1000 masquerade
nat descriptor masquerade incoming 1000 forward 192.168.0.10
nat descriptor type 1100 masquerade
provider type isdn-terminal
provider filter routing connection
provider lan1 name LAN:
pp select 1
pp name PRV/1/1/1/0:
isdn remote address call 1861492
isdn auto disconnect off
isdn call prohibit auth-error count off
ip pp secure filter in 1 200020 200021 200022 200023 200024 200025 200099
ip pp secure filter out 1 200020 200021 200022 200023 200024 200025 200026 200027 200099
ip pp nat descriptor 1000
pp auth accept pap chap
pp auth myname user**@es******.galight.flets ******
ppp ipcp ipaddress on
ppp ipcp msext on
pp enable 1
provider set on 1
provider dns server pp 1 1
provider select 1
provider ipv6 connect pp 1 on
pp select 2
pp name PRV/2/1/5/0:
isdn remote address call 1861492
isdn auto disconnect off
ip pp secure filter in 201003 201020 201021 201022 201023 201024 201025 201030 201032
ip pp secure filter out 201013 201020 201021 201022 201023 201024 201025 201026 201027 201099 dynamic
201080 201081 201082 201083 201084 201098 201099
ip pp nat descriptor 1100
pp auth accept pap chap
pp auth myname guest@flets guest
ppp ipcp ipaddress on
ppp ipcp msext on
pp enable 2
provider set on 2
provider dns server pp 2 2
provider ipv6 connect pp 2 on
pp select anonymous
ip pp remote address pool ***.***.***.***
pp auth request chap-pap
pp auth username ******** ********
pp enable anonymous
httpd frame use on 1
httpd host any
dhcp service server
dhcp server rfc2131 compliant except remain-silent
dhcp scope 1 192.168.0.2-192.168.0.191/24
dns server pp 1
dns server select 1 pp 2 any .flets
dns server select 2 pp 1 any .
dns server select 500001 pp 1 any . restrict pp 1
dns private address spoof on
analog supplementary-service pseudo call-waiting
analog extension dial prefix line
analog extension dial prefix sip 9#
alarm entire off
```