実践で学ぶ、

一歩進んだサーバー構築・運用術

written by 仙石 浩明

第1回 ここまでできる充実環境

Linuxでのサーバー構築を紹介した書籍や雑誌記事は多数ありますが，セキュリティに配慮し，他のさまざまなサーバー類と連携した実稼働システムについての記事はそう多くはありません。本連載では，筆者が運営しているネットワークとそこで使用しているサーバー類の構築，運用法について紹介します。

転職します。のっけから唐突ですが，おかげで鬼のように忙しい今日このごろです。今は社宅に住んでいるので，当然退職すれば追い出されます。ですから，アパートを探さねばなりません。2〜3月は引っ越しシーズンでもあり，引っ越し業者に予約を早めに入れる必要もあります。

そして今使っている，OCNエコノミー*は契約し直す必要があります。単に解約して新規契約するというのではなく，工事日*1をうまく調整しないと，筆者の管理しているgcd.orgドメインが一時的にIPアンリーチャブルになってしまいます。さらに，ISDNの移転の日もうまく設定しないと，会員（後述）がアクセスできない日ができてしまいます。

さらにまだ続きがあります。お正月ごろPalm用*2の拙作シェアウエアを，PalmGear H.Q.*3に登録したのですが，世界中の人々にダウンロードされたようで，試用期間の1カ月が経とうとしている現在，世界各国の人たち*4から質問やバグ報告メールが届いているのです。私のつたない英語力だと1通返事を書くだけでも大変な労力と時間がかかってしまうのでした。

まったくもって，連載を始めようという時期に限ってなんでこんなに忙しくなるんだ，とぐちっていても仕方がないので，早速始めましょう。

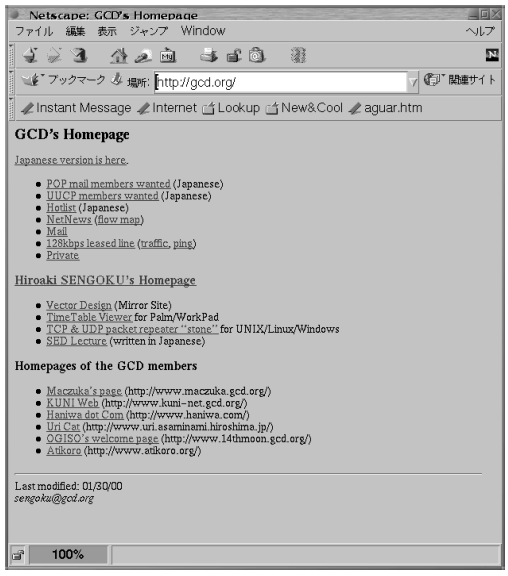

写真1 gcd.org
筆者の運営するgcd.orgドメインのWebページです。

任意団体GCDの紹介

gcd.org（**写真1**）は，私が道楽で運営しているドメインです。私は貧乏なくせに，月額3万2000円*5もするOCNエコノミーを契約しています。当然，こんな大金を毎月払うだけの余裕はありませんから，会員を募って任意団体GCD*6を作りました。つまりメールとネット・ニュースを会員に提供する代わ

【OCNエコノミー】
NTTが提供するインターネット接続サービス「OCN（Open Computer Network）」のサービスの一つです。OCNの中では，最も低料金の常時接続サービスです。最大通信速度が128Kビット/秒のベスト・エフォート型接続をとります。

＊1
OCNエコノミーは申し込みから開通まで1カ月もかかるので困ったものです。この秒進分歩の業界で，なんてのんびりしているんだろうと思います。

＊2
米Palm Computing社が開発し，米3Com社が販売するPDAシリーズの総称。IBMのWorkPadや，米HandSpring社のVISORなども含まれます。PalmOS機と呼ぶこともあります。

＊3
Palm用のシェアウエア&フリーソフトウエアのライブラリ・サイトとして有名です。http://www.palmgear.com/

＊4
非英語圏の人からのメールは，部分的にドイツ語やフランス語やその他の言語(私には判読できませんが)になっていたりすることがあって面白いです。

＊5
値下げ前は3万8000円もしました。

＊6
Greatest Common Divisor（最大公約数）の略。はるか昔，私がNIFTY-Serve（現，@nifty）の会員だったころの私のハンドルに由来します。

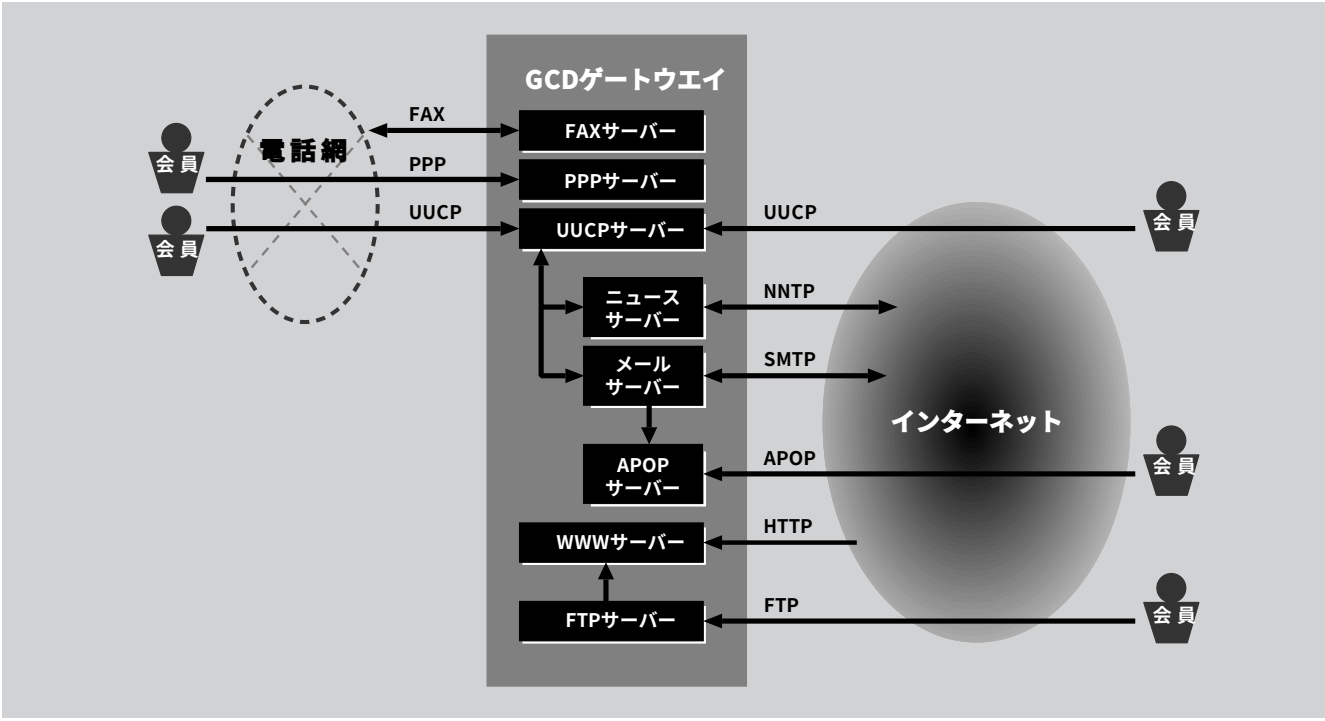

図1　GCDネットワーク構成図

りに会費を集め，OCNの代金の足しにしているわけです。

会員の多くは，UUCP*でgcd.orgのゲートウエイ・マシンに接続しています（**図1**）。UUCP接続の場合は，gcd.orgのサブドメイン，あるいは独自ドメインを使用することができます。言い替えると，メール・アドレスをいくつでも作ることができるわけです。

●ダイアルアップに適したＵＵＣＰ

ＵＵＣＰを過去のプロトコルだと思っている人がいるかも知れませんが，インターネットのユーザーすべてが常時接続するようになるまでは，まだまだUUCPは有用なプロトコルだと言えます。

多くの人，特にWindowsユーザーの大半が，PPP（Point-to-Point Protocol）でプロバイダへダイアルアップ接続し，SMTP（Simple Mail Transfer Protcol）でメールを送信し，POP（Post Office Protocol）でメールを受信し，そして，NNTP（Network News Transfer Protocol）でニュースを読み書きしているのではないかと思います。ところが，SMTP，POP，NNTPのいずれも，元々常時接続を前提としたプロトコルです。ダイアルアップ接続で使うのは変則的と言えるでしょう。

これらのプロトコルは常時接続が前提ですから，通信時間を短くしようとする工夫は一切入っていません。それどころか，NNTPの場合，サーバーの過負荷を回避するために，集中的にデータが流れないように（つまり，通信時間が長くなるように）する仕掛けすらあります。ダイアルアップで使うのは，はなはだ不適当と言えるでしょう。日本のように電話代が高い国ではなおさらです。

一方，UUCPは元々ダイアルアップで使うことが前提です。通信時間を少しでも短くするために，転送するデータをあらかじめ用意しておき，ダイアルアップしたら一気に転送してしまいます。通信中のサーバー側の仕事は，単にファイルを転送することだけですから，多少マシンの負荷が高い時でも転送速度は落ちません。さらに，ニュースの場合は，あらかじめ複数記事をまとめて圧縮しておくので，転送するデータの量が半分以下で済みます。

例えば，主に日本語が使われるニュース・グループ群として有名なfjを購読するだけなら，1日に10分程度UUCPでダイアルアップするだけで済みます。NNTPだと少なくともこの10倍くらいの時間がかかるでしょう。サーバーの負荷が高い場合は，もっとかかるかも知れません*7。

【UUCP】
Unix to Unix CoPyの略。UNIXマシン間で，バッチ処理でデータ転送を行うための一連のコマンド群を指しています。転じてそれらのコマンド群でデータを転送するような接続形態をUUCP接続と呼びます。マシンからマシンへバケツ・リレーのようにデータを転送することができ，比較的安価にネットワークを構築する手段として重宝されてきました。Usenet（Users'network）のような世界的なネットワークも構築されています。ただし，インターネットのようなIPネットワークと異なり，メールやニュースの転送以外にはほとんど使えません。

＊7
もっとも，NNTPを使っているダイアルアップ・ユーザーのほとんどは，fjの全ニュース・グループを購読しようとは思いもしないかも知れませんね。

このように，ダイアルアップ環境にとって最適なUUCPなのに，UUCPサービスを提供するプロバイダがほとんど無いのは不可解なことです。もっとも，UUCPサービスを提供するプロバイダが少ないおかげで，GCDのようなプロバイダもどきの存在価値が出てくるわけですが。

さてGCDは，1996年1月の発足以来*8，順調に会員数を伸ばし，現在1日当たりのUUCP接続受付け回数は90回を超えています。しかし接続時間は1日あたり90分程度に過ぎず，ISDNの2回線が両方とも埋まってBUSYになることは，まずありません。1回あたりの接続時間が短いUUCPならではですね。会員数が現在の倍になったとしても，恐らく大丈夫でしょう。

しかし，そこそこ会員が集まった現在も収支は依然として大赤字のままです。累積で言えば一体どのくらいの赤字か，考えたくもありません。やはり個人ユーザーにとってOCNエコノミーは高額すぎると思いますが，かくも多額のお金を払っても，自宅を常時接続にできるのは魅力です。いったん常時接続を体験すると，ダイアルアップ接続には戻れません。

常時接続の魅力というと，いつでもWebに何時間でもアクセスできる，というメリットを第1に思い浮かべる人が多いかも知れません。しかし，これは私にとっては大した魅力ではありません。実際，Webにアクセスするだけならダイアルアップ接続でもさほど見劣りのしない環境を作れます。ISDNならば接続は2，3秒で済みますから，最初にブラウザをクリックしたときに2，3秒余計にかかることを除けば，常時接続とほとんど変わらないことでしょう。しかも，常時接続よりよっぽど安くつきます*9。

CATVを利用したインターネット接続が可能な地域では，さらに安く接続できますね。残念なことにCATVプロバイダの多くが，動的にIPアドレスを割り当てているか，あるいはプライベートIPアドレス*を用いているため，Webにアクセスするくらいしか使い道がありません。

では，常時接続の魅力とは何か。それは各種サーバーを自由に立ち上げられることに尽きます。本連載では，私のマシンで走らせているサーバーを思いつくままに紹介し，セキュリティを意識した構築，運用法を解説していきます。連載のネタが尽きるころまでに，読者の皆さんが常時接続の魅力にとりつかれれば，本連載の目的が達成されたことになります。

常時接続の魅力

「各種サーバーを自由に立ち上げられることが魅力」，と言ってもいまいちピンとこないかもしれませんので，いくつか具体例を紹介してみます。

●Webサーバー

プロバイダのWebサーバーを間借りするのと，自分でWebサーバーを立ち上げるのとでは，いろいろ事情が変わってきます。プロバイダのWebサーバーだと，例えば

- ほとんどの場合，容量制限がある
- プロバイダが使用しているWebサーバーの種類によってできることが限定される
- 多機能なWebサーバーであったとしても，全機能がユーザーに解放されているわけではない

といった制約があります。

現在，ハード・ディスクの値段はタダ同然*10ですから，自前のWebサーバーならいくらでも容量を増やせます。また，自分のマシンですから，好みのWebサーバーを立ち上げられますし，もちろんそのWebサーバーのすべての機能を活用できます。さらに，他のサーバーと連携させることだって可能です。

●メール・サーバー

多くの人が迷惑メールに悩まされていると思いますが，自前のメール・サーバーなら迷惑メールの撃退が可能になります。プロバイダが提供するメール・サーバーでも，メーラーによっては迷惑メールを表示しない，あるいはPOPサーバーからダウンロードしないような設定が可能ですが，迷惑メール対策としては消極的*11である感を拭えません。

なぜなら，迷惑メールの送信者側から見ると，メールはプロバイダのメール・サーバーには届いているわけで，その後，受信者が読んだか，読んで捨てたか，メーラーの機能を使って読む前に捨てたかは判別する方法がありません。受信者が読もうが読むまいが構わず送りつけるのが迷惑メールのゆえんであるわけで，この場合送信者は迷惑メールを送り続けることでしょう。

一方，自前のメール・サーバーならば，迷

＊8
OCN エコノミー（1997年の終わりごろ，私の住んでいるエリアでサービス開始）を契約してIPリーチャブルになったのは1998年1月です。それまではテレホーダイを利用していました。

＊9
毎日寝食を忘れてWebに没頭したりすると，話は変わってきますが，普通の人なら1カ月もすれば飽きますよね?

【プライベートIPアドレス】
インターネットに直接接続する必要がないLANで，ネットワーク・アドレスとして自由に利用できるIPアドレスのことです。RFC 1918で規定されています。ネットワークの規模により，「10.0.0.0～10.255.255.255」（クラスA），「172.16.0.0～172.31.255.255」（クラスB），「192.168.0.0～192.168.255.255」（クラスC）のいずれかを選択することができます。

＊10
27Gバイトが2万円強で売られていたりするのですから，隔世の感があります。

＊11
もっと消極的な迷惑メール対策は，メール・アドレスを公開しない，ニュースに投稿する時は別のアドレスを使う，という方法ですが，メール・アドレスは広く一般に公開してこそ役に立つのであって，知人にしか教えないのであればメリット半減です。

惑メールがメール・サーバーに届けられる前に拒否できます。この場合，送信者にはエラー・メールが返ります。つまり送信者にもメールが届いていないことがはっきり分かるのです。何度出しても届かなければそのうちあきらめるでしょう。仮にあきらめなかったとしても，こちらは痛くもかゆくもありません。メール本体が送られてくるまえにSMTP接続を切ってしまえるのですから。

●ニュース・サーバー

迷惑メールと同様，ネット・ニュースのSPAM*記事は迷惑なものです。多くの人がニュース・リーダーの機能を使って，SPAM記事が表示されないようにしているのではないでしょうか。

自前のニュース・サーバーならSPAM記事の配送自体を拒否することができ，微力ながらもSPAM記事の広がりの制限に一役かったという満足感が得られます。

【スパム】
同一メッセージのコピーを大量にさまざまな電子メール・アドレスやニュース・グループに送信すること，またそのように送信された記事などを「SPAM」（スパム）といいます。SPAMの語源は米Hormel foods社の缶詰（写真）にありますが，同社が上記のような記事を送信したということではなく，TVコメディ「モンティ・パイソン」の1エピソードに由来しています。
【ssh】
Secure SHellの略。安全なリモート・ログインやリモート・コマンド実行のためのプログラムです。機能的にはrlogin，rcpやrshといったコマンドに良く似ていますが，認証機構の改善や通信データの暗号化など，セキュリティに配慮されています。フィンランドのSSH Communications Security社が開発しています。
＊12
最近は10Gバイト超のハード・ディスク内蔵のノート・パソコンも珍しくなくなってきました。

また，自前のニュース・サーバーを立ち上げるということは，過去何カ月分かの記事がすべて自分のマシンに蓄えられているということです。namazuなどのフリーソフトウエアを使って全文検索することが可能になります。

ネット・ニュースの記事は玉石混交で，役に立つ記事も多いのですが，それ以上にくだらない記事がたくさんあります。とても全記事に目を通す暇がない，という場合に全文検索は非常に有効です。

さらに，ニュース・サーバーで扱うのはネット・ニュースの記事に限りません。メーリング・リストのメールを記事としてニュース・サーバーへ与えることも可能です。記事としてニュース・リーダーで読むようにすれば，かなり流量の多いメーリング・リストでも目を通すことができるようになるでしょう。あるいは読むのをやめてしまって，後日全文検索で有用な記事だけ選び出す，という読み方もできます。

●telnet/sshサーバー

シェル・サービス（ユーザーがプロバイダのマシンにインターネットからtelnet等でloginできるサービス）を提供するプロバイダはもともと多くは無かったのですが，セキュリティ上の都合からか，サービスを廃止するプロバイダが相次ぎました。

インターネット上にloginできるマシンがあるのと無いのとでは，インターネットでできることがだいぶ変わってくるのですが，loginできるマシンがあると悪事も働かされやすくなるので，プロバイダにとっては提供したくないサービスの筆頭と言えるでしょう。

自分のマシンをインターネットに常時接続すれば，インターネットからloginできるだけでなく，そのマシンの特権ユーザー（root）になれますから，どんなことでもできます。ssh*を使ってloginセッションを暗号化しておけば，他者に盗聴される心配もありません。

このような，インターネットからloginして自由に操作できるマシンは，インターネットの世界における「自分の家」のようなものです。どこからインターネットに接続しても（例えば旅先から現地のプロバイダを利用して接続），「自分の家」に帰って普段と変わらない作業が継続できます。メールやニュースの読み書きをしたり，書きかけの原稿の続きを書いたり，等々。もしこのマシンにFAXモデムが接続されていれば，FAXの送受信だってできます。

VPN（Virtual Private Network）を使えばloginだけでなく，あらゆるプロトコルを，他者に盗聴される恐れなく，使うことができます。まさに何でもできて，しかもプライバシーが守られる，「自分の家」ですね。

一方，「自分の家」を持たず，ダイアルアップ接続によるインターネット接続しかインターネットへの接続手段を持っていないのは，住所不定のようなもので，はなはだ頼りないものです。

もちろん，巨大なハード・ディスク内蔵のノートパソコン*12を持ち歩けば，普段の作業に必要なデータをすべてハード・ディスクへ入れておくことも不可能ではありませんが，これではまるで自分の家をトレーラに積んで旅しているような感じです。特定の仕事の限られたデータだけを持ち運ぶだけならまだしも，日常の作業で必要になるかもしれないデータのすべてを持ち運ぶのは現実的ではないでしょう。

例えば私は，ニュース・サーバーに蓄えられた半年分の記事を対象に全文検索することがよくありますが，ノート・パソコンにニュース・サーバーをインストールし，かつ蓄えられた記事を常に最新に保つ，などということはあまり考えたくありません。

●NTPサーバー

0.1秒と狂わない正確な時計が手元にあるというのはいいものです。ダイアルアップ接続でも工夫すれば正確な時計合わせが可能ですが，常時接続ならNTPサーバーを走らせておくだけで簡単に正確な時刻が得られます。NTP（Network Time Protocol）は，遅延の生じるネットワークで，正確な時刻情報をやりとりするために開発されたプロトコルです。そしてこのNTPサーバーを基準時計として，LANに接続した他のすべてのPCの時計を合わせられます。

NTPの詳細については「Time server」（**写真2**）を参照にしてください。

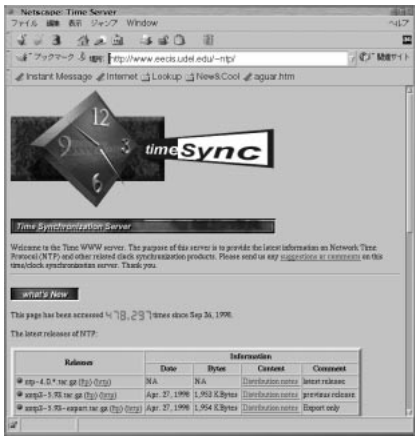

写真2　Time Server
NTPについての情報やソフトウエアは，こちらのWebページ（http://www.eecis.udel.edu/~ntp/）から入手できます。

筆者の家庭内LANの構成

最後に我が家のLANの構成*13を紹介しましょう。**図2**に示すように，ファイアウオールを兼ねているゲートウエイとノートPCから成る単純なものです。

GCDのゲートウエイの役割を果たす「toyokawa」はCPUにPentiumII 400MHzを搭載したIBM PC AT互換機で，もちろん24時間運転です。OSはLinux 2.2.13*14を使っています。TAが2台つながっていますが，片方のTAがモデム機能を内蔵しているため，モデムはありません。

「asao」はCeleron 366MHz*15を搭載したマシンで，予備のゲートウエイです。toyokawaのハード・ディスクの内容を丸ごとコピーしてあるので，いつでもゲートウエイの役割を代行することができます。toyokawaとasaoは共に100Mビット/秒のスイッチング・ハブにつないであるので，高速にコピーできます。

すべての部屋*16に10Mビット/秒のダム・ハブを置いてあるので，どの部屋でもノートPCを持ちこんで，LANに接続できます。IPアドレスはゲートウエイ上のDHCPサーバーによって動的に割り当てられます。

ゲートウエイ以外のマシン（ノートPCのほか，asaoでもWindows 98を走らせることがあります）は，インターネットとの直接の通信を，ルーターの設定で禁止しています。これらのマシンは，ゲートウエイ経由でインターネットへアクセスすることになります。このため，ゲートウエイ上のファイアウオールによって守られます。

以上，筆者が構築，運用しているネットワーク環境について紹介してきました。次回からは，具体的なサーバー構築，運用法について解説して行きたいと思っています。

＊13
引っ越し後は多少変更する予定です。
＊14
そろそろアップデートする必要がありますね。
＊15
バス・クロックを75MHzに設定して，412MHzで使っています。
＊16
2DKのアパートなので，全部で3部屋しかありませんが。残念ながらトイレにはハブは設置していません。

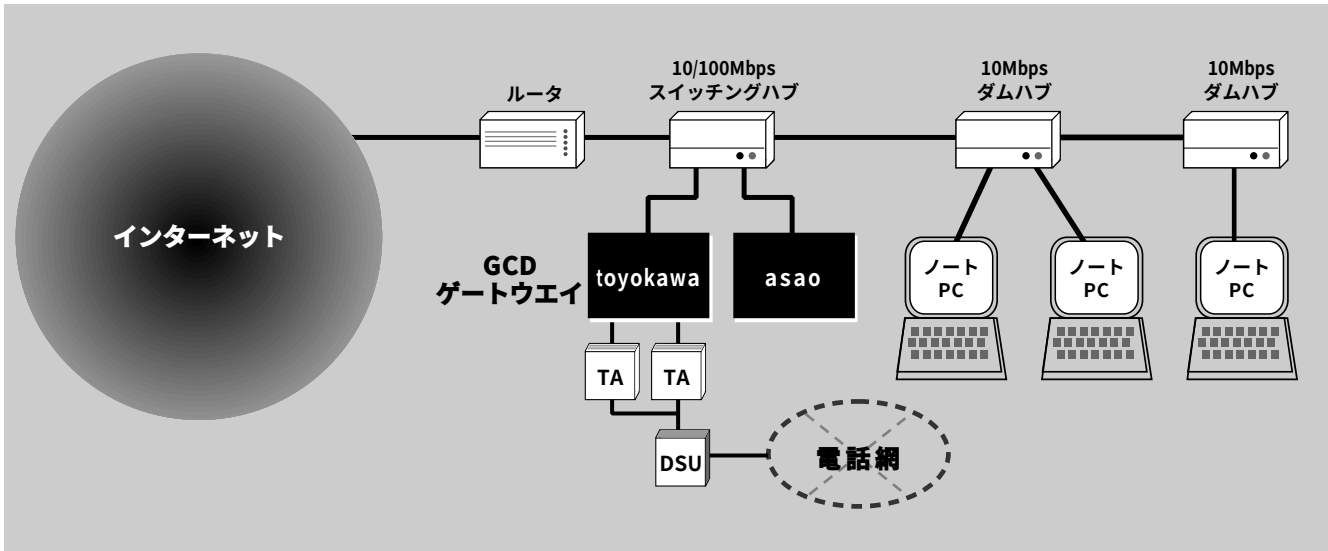

図2　筆者のLAN環境