協調型高精度時刻同期システムの構築とその認証処理等への応用

小松久美子† 下代博之‡ 中野秀男† 辰巳昭治†

†大阪市立大学 ‡下代組機工，生石高原天文台

コンピュータネットワークにおける通信の高度化に伴い，今後，その時刻保持はさらに高精度化を求められるであろう．本論文は，現状のコンピュータネットワークにおける時刻同期の問題点について問い，その高精度化の必要性についての問題提起を行うものである．天文分野での超高精度時刻同期技術の応用としてハードウェアが比較的安価に実現できることから，GPS を利用した時刻同期システムを提案する．著者らはこの時刻同期システムを４拠点に設置したので，その実際を報告する．低コストで手軽に構築できることから，高精度時刻サーバの普及が期待できる．多数の高精度時刻サーバによる協調型時刻同期により実現できることやその応用には認証処理を始め，多くの可能性がある．問題提起の段階であるが，個々の高精度時刻サーバが相互に時刻監査する方法については研究対象となると思われる．

Construction of the Collaborative the High-Accurate Time Synchronization System and its Application to Authentication Processing

Kumiko Komatsu† Hiroyuki Geshiro‡ Hideo Nakano† Shouji Tatsumi†

†Osaka City University ‡Geshirogumi Kiko, Oishikogen Astronomical Observatory

According to the rapid progress of communication network, we are highly required the accuracy of time measurements. In this paper, we point out the some problems of time synchronization, and propose the necessity of more accuracy of time measurement. From the application of ultra highly accurate time synchronization system in astronomical field, we propose a time synchronization system using cheap GPS. We report a prototype our GPS with 4 bases. Because it is possible to construct low-cost and easily, the spread of the highly accurate time server can be expected. There are a lot of possibilities, for example, co-operative time synchronization system using many high accurate time servers, and some authentication systems in application. Though this paper is now under a stage of proposal level, it seems a new research field, especially for our method audited mutually by the individual, highly accurate time server at time.

1．はじめに

近年の情報通信技術，電子商取引，電子決済等の飛躍的な進展に伴い，コンピュータやそのネットワークにおける時刻取得，維持には正確かつ真正さが必要とされ，さらに超高精度化が望まれている．今後，分散協調処理はますます増加し，かつ重要になってくるであろう．高度な情報基盤の実現には時刻同期技術の発展は不可欠であると考える．本論文では，高精度時刻サーバの提案と構築の実際，さらに複数の高精度時刻サーバによる協調型時刻同期により実現できることの展望，特に認証処理への応用について述べる．

2．時刻同期の従来技術と技術動向

古来より正確な時間の計測や時刻同期にはさまざまな方法が使用されてきた．現代では時間や周波数の標準は科学技術や産業，ひいては生活の非常に重要な基盤となっている．

「協定世界時（UTC）」とは，全世界で時刻を記録する際に使われる公式な時刻である．「国際原子時（TAI）」に，地球の自転を観測して決められる「世界時（UT）」とのずれを調整するための「閏秒（うるうびょう）」を追加したものである．直近では 2006 年 1 月 1 日午前 9 時（日本時間）に，閏秒挿入が行われた．午前 8 時 59 分 60 秒の瞬間を報じるニュースをご覧になった方も多いことと思う．閏秒の制度が 1972 年に始まってから 23 回目で 7 年ぶりのことであった．

日本国における標準時の発生・維持のため，独立行政法人情報通信研究機構（NICT）が決定する「UTC（NICT）」が生成されている．世界各国の標準機関では，GPS タイムを仲介とする GPS コモンビュー方式や衛星双方向時刻比較方式を用いた時刻比較を行っている．GPS タイムと各国の標準機関の時刻比較データは国際時刻比較ネットワークを介して国際度量衡局（BIPM）へ送られ，BIPM ではそのデータを基に TAI と UTC を決定する．

時刻同期とは，この UTC に時計を正確に合わせることである．そして，コンピュータやそのネットワークにおける時刻同期とは，UTC にコンピュータの内部時計を正確に合わせることである．

コンピュータネットワークにおける時刻同期は，一般的には，Network Time Protocol（NTP）というプロトコルを用いて行われる．NTP による時刻調整は，stratum と呼ばれる階層構造を持つネットワークを介して下位のホストコンピュータが上位の時刻サーバ（NTP サーバ）から時刻を取得することにより行われる．最上位の時刻サーバは GPS や原子時計などから時刻を取得しているもので，stratum 1 と呼ばれる．NTP は，OS を問わず，さまざまなシステムで利用できる．各 NTP サーバは上位のサーバからだけでなく，同じ階層間でも相互に時刻情報をやりとりして，その揺らぎなどを統計的に処理することにより，インターネットを経由した場合でも数ミリ秒以下の誤差で時刻精度を保持している．

現在，日本では UTC を 9 時間進めた時刻である日本標準時（JST）の供給が標準周波数局 JJY，テレホン JJY，時報サービス（117）などにより行われており，さまざまな機関や機器が時刻を同期している．

コンピュータの時刻合わせには，公共機関，タイムビジネス認定の時刻配信業者，インターネット関連事業者等の法人を対象として，ネットワークによる時刻情報提供サービス（NTP サービス）が利用者の申請に基づき同機構から提供される．

最近では，NICT によるインターネット時刻供給サービスが 2006 年 6 月 12 日に開始された．高精度，高スループットの NTP サーバによる NTP サービスである．ハードウェア SNTP で，毎秒 100 万アクセス以上のクライアントからの時刻参照が可能だ．これにより現在の国内の需要を十分にカバーすることができる．現在，ntp.nict.jp で stratum 1 のパブリックサービスを行っている．

3. タイムビジネス　～政府の取り組み～

近年の電子商取引，電子決済等の進展，電子政府の発足に伴い，電子的手続きの安全性と信頼性を高めることがますます重要となり，それには正確な時刻情報が必要とされる．それに応じた政府の取り組みが「タイムビジネス」という概念である．総務省が推進するタイムビジネスは 2 つのサービスに分類され，「タイムビジネス認定制度」により認定された事業者はそれぞれ次のような業務を行う．

・標準時配信サービス　時刻配信と時刻監査
・時刻認証サービス　　タイムスタンプ付与

これらのサービス提供により，「電子データの原本性証明」，「取引時刻の正確な把握」，それらを「第三者へ証明すること」を実現する．タイムスタンプの精度は，UTC±1 秒以内（本認定精度基準）とされている．

電子署名とタイムスタンプの併用により，改ざんの有無だけでなく，ある時刻での存在証明と以降の変更がないことの証明が可能である．e-文書法等に対応した原本性の確保のためにも，タイムビジネスは時刻情報を考慮した公的情報通信基盤として不可欠であると考える．

4. 要求される時刻精度

コンピュータの時刻同期は，誤差 1 ミリ秒以下で高精度と言えよう．NTP では一般的に 1 ミリ秒以下の誤差で同期可能であるが，インターネットなどのネットワークを介している場合や NTP による階層構造の場合では，誤差が数ミリ秒程度になることもある．

次章で，天文台の超高精度時刻同期の事例を紹介する．この超高精度の事例では，マイクロ秒以下の誤差で時刻を同期することが可能である．

本論文で提案する高精度時刻同期システムでは，1 ミリ秒以下の精度を想定する．コンピュータにおける時刻同期の精度は OS に依存する[7]ため，マイクロ秒以下の精度までとはいかないが，正確な時刻を各コンピュータが保持することで，複数コンピュータ間で高速通信の同期を取る処理が可能になる．

既に述べたようにタイムビジネスにおけるタイムスタンプの精度は誤差 1 秒以内という基準が設けられている．文書の存在証明としては十分かもしれないが，電子商取引や電子決済のように 1 秒間に何回ものデータ送信が行われるものについては，事象の発生順序を正確に把握するために，その頻度に応じた精度が求められる．

5. 超高精度時刻同期の事例

兵庫県立西はりま天文台の 2m 望遠鏡は，現時点では国内最大の経緯台式架台の望遠鏡であ

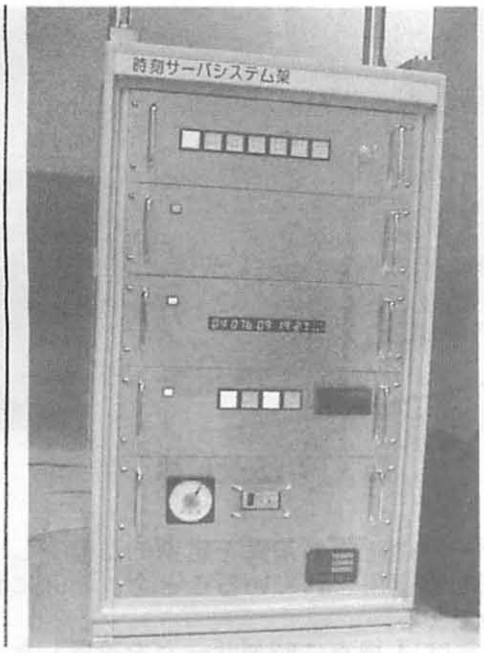

図 1　時刻サーバシステム

る．同天文台では，望遠鏡制御のため超高精度時刻同期システムを構築，運用している．[3]

一般に天体望遠鏡の架台には，赤道儀式と経緯台式がある．2m クラスの望遠鏡になると，重量負荷の設計が容易な経緯台式架台を採用することが多くなってきている．赤道儀式には傾きがあり，1 軸を一定速度で回転させると天体の追尾ができる．しかし，経緯台式架台では垂直軸と水平軸の 2 軸の高精度な位置制御が天体の運動に合わせた追尾のために必要になる．さらに追尾による視野回転も補正しなければならない．それゆえ，望遠鏡を制御するコンピュータには，極めて高精度の時刻信号が必要とされ，正確な時刻と機器を同期させるためのタイミング信号が要求される．

同天文台の時刻サーバシステム（図 1）は，GPS による時刻信号を元に UTC に対して 1 マイクロ秒以内の精度で時刻を出力している．GPS 受信機から 1 秒毎に発生される 1PPS（Pulse Per Second）信号[4]を精度よく百万分割する．装置内の水晶発振器（10MHz，周波数偏差 0.1ppm）の 10MHz 出力を 1PPS 信号で毎秒校正することにより累積誤差のない時刻信号を発生させる．GPS 受信機から出力される 1PPS 信号の精度は公称±1 マイクロ秒であるが，実際には数百ナノ秒のゆらぎがある．これを平滑化するために水晶発振器の周波数追尾を時定数 1 分程度のゆっくりとしたものにして GPS 受信機からの 1PPS 信号のジッタ（ゆらぎ）を除去し，GPS 受信機の持つ性能以上の精度になるよう工夫されている．[3]

また，時刻信号の発生には長期安定性と信頼性を確保しなければならないため，同システムでは冗長化構成として GPS 二重化，GPS からの信号のゆらぎを平滑化する水晶発振器三重化が行われ，さらに地震や落雷等の災害対策がなされている．時刻サーバは望遠鏡制御コンピュータにフォトカプラ経由で BCD 形式の時刻データを出力し，また，制御室の LAN 内の NTP サーバとしても機能している．

6. 現状の問題点と問題提起

NTP では一般的に 1 ミリ秒以下の誤差で同期可能だが，それ以上の精度を必要とする場合にはネットワーク経由の時刻取得では十分ではなく，精度の限界がある．NTP サーバのツリー構造は最大 15 階層まであり，当然ながら階層が下になるほど時刻の精度が低くなる．

特定の NTP サーバに時刻問い合わせのアクセスが集中してしまうという問題がある．ある大学の NTP サーバへの【アクセスは毎秒 900 件に上り、大学の回線帯域を 2Mbps も使っているという】[5]ことである．問い合わせ先を意識せず使っている場合もあると考えられる．また，正確な時刻取得ができるにこしたことはないが，NTP が普及してきたため，NTP による同期である程度時刻が合っていれば，一般的にはさしたる不便や問題がなく，高精度の時刻取得は費用対効果からも考えて必要性を感じないというのが実情である．実際，Windows XP において時刻サーバへの同期は 1 週間に 1 回，自動的に行われる設定になっていて，その 1 週間に PC の内部時計に数秒以上の誤差が生じている．

コンピュータネットワークにおける時刻取得の実態や，NICT の新しい NTP サービスが開始されたことなどを周知することにより，時刻取得への関心が高まれば，特定サーバへのアクセス集中で混雑により精度が劣化するようなこともなくなる．

公的機関の時刻配信，時刻認証サービスは，電子政府，e-文書法等においては必要不可欠である．しかし，高速で 1 秒間に何回も行われる

図 2　GPS アンテナ

ような電子商取引，電子決済等においては誤差１秒以内という時刻認証は十分ではないと考える．世界各国が政府レベルで時刻をオーソライズし保時することは必要だが，インターネットにおいてオープンソース的に時刻取得やその技術を自分たちの手元に近づけることをしてもよいのではないだろうか．民間レベルの時刻認証や相互時刻監査ができるようになれば，さまざまな利用の可能性が開ける．

例えば，認証技術において，PKI （公開鍵基盤）が第三者である認証機関から証明書を発行する仕組みであるのに対して，PGP では信頼できる第三者が署名することによって公開鍵を確認するので認証局が存在しない．時刻認証においても，認証機関を介さずに時刻の正確さや事象の発生時刻を証明できれば，認証機関利用の費用が不要になるので，個人利用も含めた時刻認証の普及が見込める．

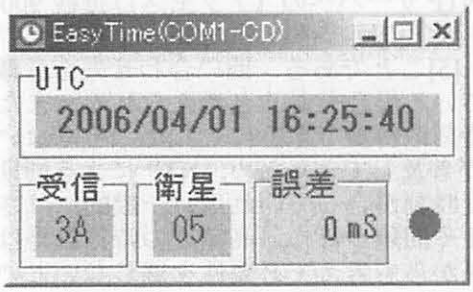

図４　Windows アプリケーション画面

7. 高精度時刻サーバの提案と実現できること

前述した天文分野での時刻同期技術の応用として，時刻サーバを手軽に設置できることがこの提案の動機である．天文台の時刻サーバシステムの冗長化構成部，災害対策部，フォトカプラ出力部を省き，ハードウェアの基本部分を利用すれば，GPS 受信機が安価に製作できる．

これまで NTP サーバ設置には相当の費用がかかっていた．また，自宅で GPS を利用した時刻取得をしている事例もあったが，NTP の普及によりある程度の時刻精度を保てることから，その必要がなくなったという考え方もある．

しかし，GPS 受信機のハードウェアが比較的安価に実現でき，ソフトウェアもオープンソースを利用することによって誰もが NTP サーバを手軽に設置，運用可能になったらどうだろう．GPS を介して協定世界時（UTC）を参照する stratum 1 がインターネット上に多数存在すれば，これまでの階層構造から脱却して，相互に時刻比較し監査することによって精度と信頼性の高い協調型の時刻同期ネットワークを構築していけるのではないだろうか．つまり，第三者による時刻監査サービスで証明するのではなく，互

図３　GPS 受信機

いのサーバの時刻の差異を定期的に監査し，時刻が正しく運用されていることを，相互に証明するのである．

著者らは 4 拠点に時刻サーバを設置した．具体的には，著者ら宅 2 カ所，大学及び和歌山県のみさと天文台に時刻サーバが設置されている．GPS アンテナ（図 2），GPS 受信機（図 3）と時刻サーバの PC から成る．GPS 受信機は精度良く１秒を百万分割（精度数百ナノ秒）し任意のタイミングで時刻を読み取る．自宅サーバは DELLPowerEdge SC430 小規模ネットワーク向けサーバマシンで，現在のところ Windows2000 のアプリケーション（図 4）として稼動している．みさと天文台では屋外の観測ドーム（図 5）に設置した．

ネットワーク上の時刻サーバ群で実現できることはいろいろある．期待される応用分野は，ネットワーク通信プロトコル，情報セキュリテ

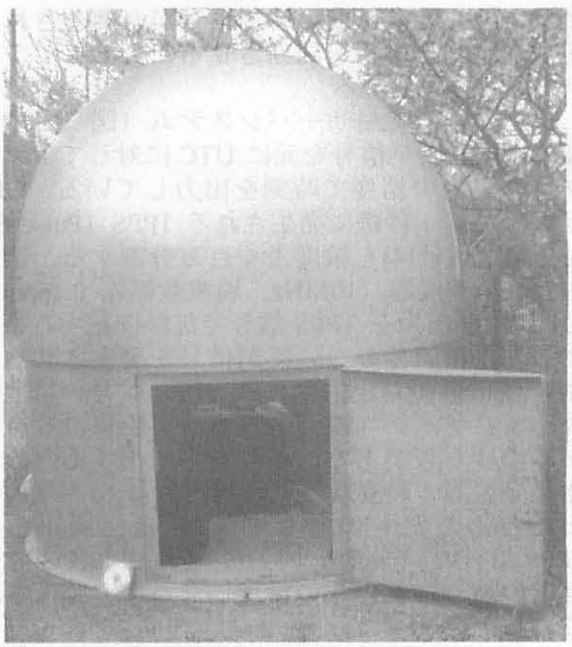

図５　みさと天文台観測ドーム

ィ，暗号化技術，時刻認証，時刻監査，時刻配信サービス，電子署名，電子商取引，オンラインゲームなど多岐に渡る．大規模無線ネットワークにおける通信衝突や情報伝達の遅れを解決するために高精度な時刻同期が必要であるという報告[6] がある．サーバや端末が時刻を正確に同期させることによって衝突のない高速通信が可能になる．

民間の時刻認証，時刻監査，時刻配信等各種サービスへの適応，正確な時刻同期によって実現される暗号化技術の開発などにおいても高精度時刻同期の技術を活かすことができるだろう．有効期限の極めて短いワンタイムパスワードで通信相手の認証を行うことや認証局を介さない当事者同士の認証，コミュニティでのタイムスタンプ利用などに同期された時間データを用いることも考えられる．

8. 開発課題

まず，ハードウェア的には，GPS 受信機とコンピュータ間のインターフェースにおいて，次のような課題がある．

現在，著者らが使用しているシステムでは，GPS 受信機から出力される UTC に同期した 1PPS（Pulse Per Second）信号[4]を，コンピュータ側では一定間隔で割込み処理を行い，時刻を取得するのであるが，次の時刻取得までの間の精度補償を高める方法についてもまだ考える余地がある．現にノート型パソコンではこの割込み処理がうまくいかないことがある．割込みではなく CPU からのリクエストで時刻取得できるしくみにすることでより高精度になるのではないかとも考えている．

また，OS 側の時刻取得については，次のような問題点が考えられる．

- Windows は時刻取得の精度についてあまり考慮されていないようである．[7]
- Linux 等 Unix 系 OS もリアルタイム OS ではない．

今回提案する高精度の時刻取得は，リアルタイム OS への適応によって真価が発揮できるので，TRON などへの移植と実験も視野に入れる必要がありそうである．

NTP Version 3 では，それほど多くないサーバ間の時刻同期について考えられている．100 や 1000 といった多数のサーバ間の協調を考慮するしくみについて考える必要がある．

9. 今後の予定

既に述べたように，4 拠点に GPS 受信機を備えた時刻サーバを設置した．今後は次のような実験から始めていくこととする．

- 単一システムの時刻精度を計測する．
- コミュニティ内の時刻データを比較する．

このようなコミュニティ内のインターネットを介したネットワークで，NTP で時刻データを相互に収集比較することにより，時刻サーバ相互に時刻をチェックし，時刻監査をして GPS 衛星が捕捉できない，断線，ハードウェア故障などの異常があれば知らせるような時刻比較ネットワークを形成していくことを考えたい．

また，GPS を参照する時刻サーバの設置方法を一般に向けて告知していく予定である．GPS 受信機の製作方法とソフトウェアをウェブで公開する．現在 GPS 受信機の時刻データを受け取るパソコン側のソフトウェアは Windows 用である．このソフトウェアを Linux 対応のものに移植し，オープンソースとして公開する．また，GPS 受信機の部品構成と部品入手方法も含めてその製作方法を公開する．

オープンソースとして公開することによって，誰にでも手の届く高精度時刻同期が可能になることが期待される．また，時刻同期に対する取り組みや事例を紹介し，時刻同期に対する意識向上に役立つ情報発信もしていきたい．

今後は，アドホック無線ネットワークにおける通信衝突の回避や情報伝達の遅れ解消，有効期限の極めて短いワンタイムパスワードの発行，認証局を介さない当事者同士の認証などの実現に向けて考えてみたい．

10. まとめ

低コストで手軽に構築できる高精度時刻同期システムを提案した．これにより，具体的には GPS を利用した stratum1 の NTP サーバの導入，普及が期待できる．そして，このようなサーバがネットワーク上に多数存在し，それぞれが他と協調して時刻同期，時刻監査することによって，精度と信頼性の高い時刻同期ネットワークの構築が可能であることを示唆した．導入コストを抑えたネットワークでの有効なアプリケーション例を示すことで，普及が進むと考えている．

システム開発状況は，4 拠点の GPS を利用した NTP サーバ設置であり，現在のところ Windows の PC 上で稼働している．PC 側のソフトウェアを Linux 対応のものに移植し，ハードウェアの製作方法と共にオープンソースとして

公開することにより，ネットワークの拡大が期待される．

参考文献

[1] 情報通信研究機構　日本標準時グループ，http://jjy.nict.go.jp/（2006年10月確認）

[2] タイムビジネス推進協議会，http://www.scat.or.jp/time/（2006年10月確認）

[3] 下代博之：西はりま天文台2m望遠鏡時刻サーバ装置の開発，兵庫県立西はりま天文台年報，(2005).

[4] 早水勉，相馬充，下代博之，橘口隆：GPSによる汎用時刻保持装置の開発，国立天文台報，第5巻，73-79 (2001).

[5] ITmediaニュース：福岡大のNTPサーバがアクセス集中で悲鳴，http://www.itmedia.co.jp/news/articles/0501/21/news059.html　(2006年10月確認)

[6] 徳永雄一，西山博仁，三部健：無線センサネットワークにおける高精度時刻同期ノードの設計，情報処理学会 研究報告 ユビキタスコンピューティングシステム，Vol.2005 No.107 pp.65-68 2005-UBI-009 (2005).

[7] NTP時刻同期精度のOS依存性について，国立天文台・水沢観測センター　佐藤克久、浅利一善，http://www.miz.nao.ac.jp/staffs/hisa/01TEsympo.html　(2006年10月確認)