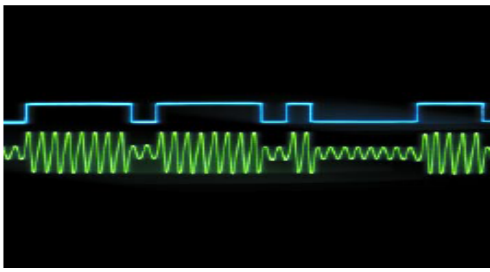
Symmetricom

ネットワークにおける時刻同期の重要性



ホワイトペーパー

丸文株式会社

ネットワークにおける時刻同期の重要性

はじめに

本書をお読みになっている今現在でも、皆様のワークステーションやサーバで構成されたネットワークには、それぞれ独自の時計でファイル、電子メール、トランザクションなどにタイムスタンプが付き、同時にすべての種類のトランザクションがサーバログに記録され、その情報が必要な場合に備えていることでしょう。また、1 日のある時点で、アーカイブやディレクトリ同期化、cron ジョブなどの自動プロセスが実行され、タイムスタンプに基づいてファイルが変更されていることでしょう。これらすべての根底にあるのは、「時刻は合っている」という前提です。時刻が完全に合っているわけではない場合でも、少なくとも時刻は「十分に合っている」と信じられているケースがかなりあります。ここでは、「十分に合っている」では正確なネットワーク時刻とは言えない理由と、ネットワークの時刻同期が非常に重要な理由について説明します。

コンピュータの内蔵時計は、狂いやすいことで有名です。通常、これらの時計は安価な発振回路またはバッテリバックアップ付きの水晶に基づいているため、1 日で数秒は簡単に狂う可能性があり、長期間ではかなりの誤差が発生することになります。分散コンピューティングの普及やネットワークインフラの相互依存の増大に伴い、このような多くの時計を個別に動作させることは、ネットワークインフラやそこで動作するアプリケーションを危険にさらすことになります。特に、ネットワーク処理やアプリケーション関連の動作は、時刻の非同期に関する問題が最も発生しやすいものです。

ネットワーク処理

ネットワーク処理では、最適なネットワークパフォーマンスを確保するために、時刻同期の取れた情報が必要です。通常、時刻の非同期は、何か問題が発生しない限り、障害や問題解決のための主要な要素になることはありません。しかし、別のシチュエーションでは、時刻が同期していないために、ネットワークプロセスが機能しないことがあります。時刻同期がネットワーク処理に直接影響を及ぼす主なケースは、次のとおりです。

・ログファイルの正確さ、検査、監視
・ネットワーク障害の診断と復旧
・ファイルのタイムスタンプ
・ディレクトリサービス
・アクセスセキュリティと認証
・分散コンピューティング
・スケジューリングされた処理
・実世界時刻

ログファイルの正確さ、検査、監視

サーバのログファイルとそのレポートデータを使用して、組織内の活動状況を評価することができます。これには、ファイアウォールやVPNセキュリティ関連の動作、帯域幅の使用率、および各種のログ記録、管理、認証、課金などの各機能が含まれます。サーバログは、様々なホストからの情報を編集したものなので、タイムスタンプが正しいことが必要不可欠です。正しくない場合、イベントを発生順に整列させたり、根本的な原因である問題を解決したりするのが難しくなります。時刻に関連するあらゆる要素についての統計情報は解釈できず、おそらく意味を持たないものになってしまいます。ログ記録されたルーターの設定イベントやシステムエラーメッセージ（ルーター設定の変更、インターフェースの送受信状況、モデムイベント、セキュリティ警告、環境の状態、トレースバック、CPU処理の過負荷など）でさえ、ネットワークの時刻同期を利用した正確なタイムスタンプによってそのデータに意味を持たせているのです。[1]

MicrosoftのApplication Centerなどで使用される監視プロセスは、その同期プロセスと監視プロセスで時刻を使用します。クラスタ内の時刻が同期していないと、矛盾した動作が実行される可能性があります。たとえば、パフォーマンスカウンタデータのタイムシフトがあります。この場合、チャート化された値が、実際に実行された時刻よりも前または後に実行されたように表示されてしまいます(実行予定の場合でも同様です)。[2]

Sun Microsystemsのクラスタモードでは、管理者は実行中のクラスタノードの時刻を直接変更できないので、ログファイルの正確さを確保するために実行中の時刻同期がさらに重要になります。管理者は、date、rdate、ntpdateなどを使用して、クラスタの時刻を直接変更することさえできません。このようなコマンドを実行すれば、クラスタノードの時刻が突然変更されるため、エラーが発生する可能性があるからです。[3]

多くの企業は、悪評高い DoS(Denial of Service）攻撃に悩まされています。この場合、ネットワークセキュリティ専門家は、根本的な原因であるネットワークイベントの検出によく使われる RMON(Remote MONitoring)ログを使って、ネットワーク犯罪の現場を再現します。通過したネットワークパケットに正確なタイムスタンプが付いてい

れば、そのような作業を可能にする法的根拠を集めることができます。

ネットワーク障害の診断と復旧

大半の IT 企業は、ピーク時にネットワーク処理が維持できるかどうかでその実力を評価されます。許容できる中断時間に関する厳しい条件は、最も一般的な QoS（サービス品質）の測定基準の一つで、このことはすべての IT 部門で明確に認識されています。障害が発生した際に、その障害の診断と復旧を行うために正確なネットワーク時刻が非常に重要になります。

障害診断を支援するために、コネクションの消失、バッファオーバーフロー、パケットの消失、その他の主なネットワークイベントが、サーバやルーター、スイッチ、専用の機器などに常駐している RMON サービスによってトラップ、レポートされてログ記録されます。あるエラーが原因でネットワークがクラッシュした場合、RMON イベントが次々とレポートされます。これらのイベントは、レポートする RMON エージェントが添付したネットワークタイムスタンプを元にインデックス化されます。これらのタイムスタンプが同期していれば、適切な順番を確定できるため、根本的な原因を素早く特定できます。しかし、ネットワークの時刻が正確に同期していないと、根本的な原因の切り分けがあいまいになり、中断時間は長くなります。

ファイルのタイムスタンプ

あらゆるファイルシステムの完全性は、ファイル自体の名前と日付に大きく依存しています。通常、個々のファイルには、作成日、最終アクセス日、最終アーカイブ作成日、および最終変更日が記録されます。分散型のファイル共有システムの場合、マスタファイルは、NFS（Network File Sharing）サーバによって保持され、リモートクライアントから使用できるようになります。NFS では、ネットワークの時刻は非常に重要です。重複するファイル名が存在する場合には、最新のコピーを保存します。しかし、クライアントがリモートからアクセスしたファイルにタイムスタンプを付ける際、サーバにあるファイルのタイムスタンプよりも前の時刻にアクセスしたような場合は、そのクライアントファイルにどのような変更が加えられていても破棄されてしまいます。

ディレクトリサービス

ネットワークの時刻同期は、ネットワーク設計や実装の重要な要素です。たとえば、多くのネットワークディレクトリサービスシステムでは、タイムスタンプに従って情報を交換し、ディレクトリサービスデータベース内の変更を同期させます。グループウェアアプリケーションは、スケジューリングとコラボレーションのために正確な時刻を必要とします。ネットワークの時刻が同期していない場合、時刻依存の大きいシステムやアプリケーションは正常に動作しなくなります。Windows NTネットワークの場合、すべてのNTサーバとクライアントワークステーションを 1 つの正確な標準時刻ソースで同期する必要があります。[4] 同様に、NDS（Novell Directory Services）でも、イベントの順番を確定し、実時刻を記録するためにタイムスタンプが必要です。[5]

アクセスセキュリティと認証

Windows 2000 は、ネットワークの時刻同期が必要な例の中で最も有名かつ最新のものです。Windows 2000 では、デフォルトの認証プロトコル（MIT Kerberosバージョン 5）が認証チケット生成プロセスの一部としてワークステーションの時刻を使用するため、時刻同期は不可欠です。Windows 2000 に付属するW32Timeサービスツールにより、組織内にあるすべてのWindows 2000 が標準時刻を使用していることが保証されます。Timeサービスでは、適切な標準時刻の使用を保証するために、権限を制御し、ループを許可しない階層的な関係が使用されます。[6] すべてのクライアントデスクトップとメンバサーバは、受信認証を実行するドメインコントローラを、それぞれのタイムパートナーに指定します。これは、ツリー構造のルートにあるPDC（プライマリドメインコントローラ）までドメイン階層を辿ります。[7] このPDCは、専用ネットワークタイムサーバなどの信頼できる時刻ソースで同期するように設定されます。タイムサーバが利用できず、ドメインコントローラ間の時刻のずれがKerberosで許容された誤差を超えた場合、2 つのドメインコントローラ間の認証／ログオンは成功せずに、エラーメッセージが表示される可能性があります。[8]

分散コンピューティング

IBMは、かなり以前から同社のDCE（分散コンピューティング環境）における時刻同期の必要性を認識していました。DCEは、分散アプリケーションを開発、実行できる高レベルの首尾一貫した環境を構築するサービスセットです。DCEには、リモートプロシージャコール、ディレクトリサービス、セキュリティサービス、および分散タイムサービスという 4 つのコアサービスがあります。この分散タイムサービスによって、分散システム内にある様々なホストの時刻を同期できます。クライアントやサーバのグループにあるホストシステムクロックは、セキュリティサーバホスト上のクロックとの誤差を 5 分以内に収める必要があります。これらの 2 つのクロック間の誤差が 5 分を超えた場合、認証エラーが発生し、クライアント設定が失敗します。[9]

スケジュールされた処理

cron スクリプトや crontab は、指定された時刻にコンピュータの OS やアプリケーションサーバに対して実行されるコマンドリストです。各コマンドは、それぞれの指定時刻になると実行されます。通常、これらのコマンド（通常はデータバックアップ関連）は、夜間や終業後のスケジュールされた時刻に実行されます。ホストが 1 つの場合、コマンドを予定通りに実行するには、許容できる時刻ソースでそのホストを同期する必要があります。複数のホストで個別の cron ファイルの実行を担当する場合は、スケジュールされた処理を適切に調整するためにホスト間の時刻同期がさらに重要になります。

実世界時刻

実世界の時刻を使用したネットワーク処理に代わる手段はありません。ネットワークを間違った時刻に同期させて運用することもできますが、このポリシーは望ましいものではありません。ローカルネットワークは、より規模が大きなネットワーク（特にインターネット）と相互接続されるため、そこでの共通要素は正しい時刻だけになります。実世界時刻は、協定世界時（UTC）に基づいたものです。UTC はグリニッジ標準時（GMT）に基づいた最新の時刻です。基本となる UTC におけるネットワーク処理では、標準時刻が共有されます。UTC 時刻は、正確かつ安全で信頼できるソースから適切に取得され、そのソースを参照するすべての OS によって現地時間に変換されるのがベストです。この標準時刻を参照することで、ネットワークマネージャは、正確な時刻を持つ情報を得ることができます。このネットワークに関する情報を使用して、最適なパフォーマンスを確保したり、本書で説明する多くの問題を避けることができます。

アプリケーション

アプリケーションの多くは、測定データや生成データに対して、非常に大きな意味を付与する要素としてタイムスタンプを使用します。共有データベース、課金システム、トランザクションシステム、データ取得、電子メール、その他のアプリケーションは、様々な精度の正確なタイムスタンプに依存しています。タイムスタンプの使用範囲は無限ですが、一般的なアプリケーションでは、タイムスタンプに意味を持たせるためにネットワークの時刻同期が非常に重要になります。次のようなケースでは、時刻同期がアプリケーションに直接影響を及ぼします。

- トランザクション処理
- ソフトウェア開発
- 電子メール
- 法律や規則上の要求事項
- パスワードとデジタル ID

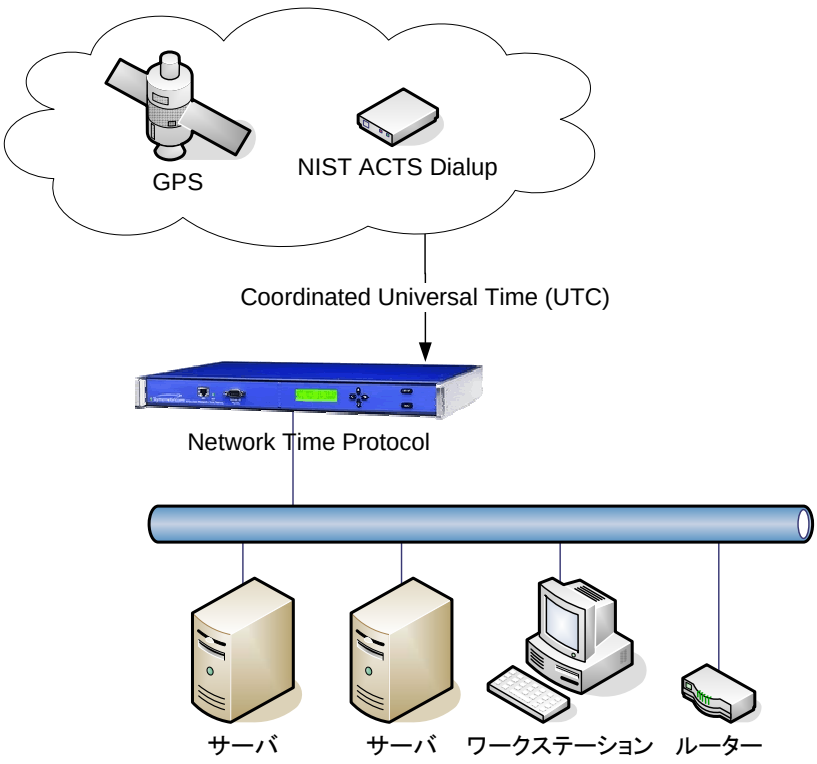


図 1. 正確な実世界時刻でネットワーク機器の同期を行う

トランザクション処理

トランザクション処理の時刻同期は、目新しいものではありません。1960 年代には、すでにIBMが、時刻同期が重要なトランザクションの実行に不可欠なことを認識していました。IBMの「Redbook」には、「データ処理においては、常に正確な日時情報に対するニーズが存在してきた。このニーズは、シングルシステムからマルチシステムへの移行に伴い、システム間の正確で一貫したクロックの必要性へと発展した。」と記述されています。[10]

今日では、種類や機能が異なる多くのサーバやワークステーションが使用されおり、そのすべてがネットワークに接続され、様々なトランザクションを実行しています。一般的に、アプリケーションのタイムスタンプには、（無条件で）誤差 1 秒未満という制限があります。基本的に、これらのタイムスタンプによって、トランザクションが発生した時刻（購入注文が発生した時刻、通話の開始や終了の時刻など）に関わる疑問が解決します。トランザクションタイムスタンプで 10 ミリ秒レベルの正確さが必要になるのは、トランザクションを正しい実行シーケンスに配置する必要がある場合や、特にほぼ同時に大量のトランザクションが発生する場合です（後述の「法律や規則上の要求事項」の項参照）。コンピュータ処理は自動的に素早く実行されるため、システムクロックは、最小限のトランザクション構成時間や転送時間より短い 5～20 ミリ秒にする必要があります。

ソフトウェア開発

ソフトウェア開発は、プログラマチームが異なるサーバ（地理的に異なる場所に配置される場合もある）に保存されているコードで開発を行うために、広範囲に渡って分散されたタスクになる可能性があります。最終的に、このコードは 1 つのプログラムにコンパイルされます。このように分散されたサーバからソフトウェアのコンパイルを管理するには、「makefile」機能やバージョン管理システムが使用されます。ファイルのタイムス

タンプは、ベースとなるソースファイルが変更された場合に、リビルドが必要なファイルの判別に使用されます。ディレクトリの一部が NFS にマウントされ、サーバやクライアントが異なる現在時刻を使用している場合、「make」関数は一部の導出オブジェクトのリビルドに失敗し、作成された実行ファイルが最新のソースに基づいたものではなくなる可能性があります。

エンジニアがソースコードに「fix」と入力したものの、最後の「make」処理中にその「fix」だけが欠落したため、結果的に企業にとって手間とコストがかかってしまった、といった事例が少なくありません。このような種類のエラーを検出するのは非常に困難です。初期の対応では、ほとんどの場合ソフトウェアバグが疑われます。しかし実際は、サーバ時刻の非同期が原因でファイルの変更が失われたというインフラ関連の問題であるため、アプリケーションコーディングチームは、バグ検出用のテストシナリオ作成に膨大な時間を浪費してしまうことになります。

電子メール

電子メールは、文書による通信の事実上の標準になりつつあります。IDCによると、1 日に送信される電子メールの平均件数は、2000 年末までに世界中で 100 億件に達すると予測されていました。2005 年までには、この 3 倍を超えて 1 日当たり 350 億件という驚異的な数字に到達する見込みです。[11] これらすべての電子メールメッセージは、発信元のタイムスタンプが付けられた状態でネットワークを通過します。このタイムスタンプが明らかに間違っている場合、受信側の一部で混乱を招く可能性があります。発信元の組織の信頼性が疑われるのは言うまでもありません。

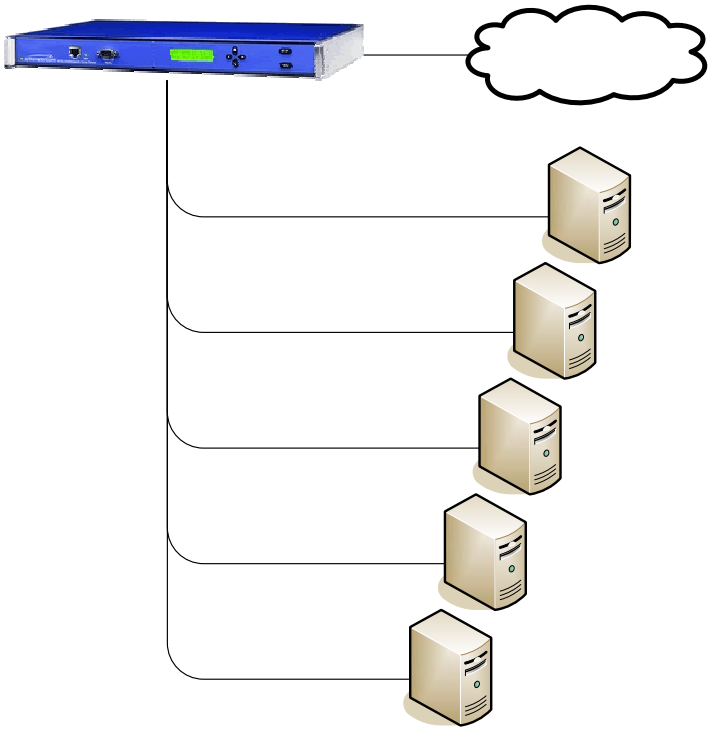


図 2. 時刻同期が必要な典型的なアプリケーション

法律や規則上の要求事項

トレース可能な正確なネットワーク時刻は、その業界を管理する法律や規則による要求に応じて、提出しなければならない場合もあります。たとえば、NASD（National Association of Security Dealers：全米証券業者協会）では、そのメンバに対して、NIST（National Institute of Standards and Technology：米国政府標準技術研究所）の UTC を 3 秒以内でトレースできる精度のタイムスタンプを株式取引に付けるよう要求しています。NASD には 5,500 のメンバが登録されており、その支店数は全米で 82,000 を超えるため、これは多量に渡る同期試行の発行を示唆しています。同期されたトレースできる時刻は、順番を検査する際に、トランザクションが発生した時刻を確認するために必要になります。法律、医療、通信関連などその他のアプリケーションも、トレースできる標準時刻をネットワーク運営ポリシーの一部として採用すると想定されます。

パスワードとデジタル ID

2000 年に、米国で電子署名法案が可決されました。この法案により、適切に保護・識別されたコンピュータに対して代理人としての権限が付与され、それを管理する組織に契約上の義務が課せられます。コンピュータまたは個人が正しいパスワードまたはデジタル ID を所有していれば、ビジネス活動の権限を持っていることになります。したがって、パスワードまたはデジタル証明書が取り消されると、すぐにアクセスを拒否できることが重要になります。典型的な例は、デジタル証明書を使って会社のアカウントにアクセスしていた従業員がその会社を退職する場合です。この場合、証明書を無効にしてそれ以降のアクセスを防ぐ必要があります。デジタル ID 証明書は「サイバースペース」内に存在するため、証明書の破棄時刻もサイバースペースに記録されている必要があり、また、この証明書を使用するあらゆるプロセスで、証明書がその破棄時刻を経過したかどうかを正確に判別できるようにネットワーククロックが同期されていなければなりません。

まとめ

Symmetricom 社は、顧客とのやり取りの中で培った経験を通じて、ネットワークの時刻同期の重要性について学んできました。我々は日々、企業をスムーズに運営するためのネットワーク機能支援に従事している顧客をサポートしています。このような顧客は、多くのネットワーク処理やアプリケーションを正常に機能させたり、障害発生時に管理しやすくするには、ネットワークの正常な時刻同期が重要であることを認識しています。

弊社では、高品質なネットワークの時刻同期システムの構築に関して積極的に取り組むことは、現在および将来にわたってお役に立てると強く確信しています。そのようなシステムの基盤を構成するのが、Symmetricom 社の NTS-150、NTS-200 のような GPS ネットワークタイムサーバです。

参考文献

[1]Cisco Systems; Using Syslog, NTP, and Modem Call Records to Isolate and Troubleshoot Faults; http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/dialsol/nmssol/syslog.htm

[2]Time and Date Synchronization; http://support.microsoft.com; Q216734

[3]Sun Microsystems; Administering Sun? Cluster 2.2 Environments, October 2000

[4]Time Synchronization in an NT Network, Windows Magazine, Tao Zhou

[5]Novell Timesysc NLM FAQ

[6]How to Configure an Authoritative Time Server in Windows 2000; http://support.microsoft.com; Q216734

[7]Basic Operation of the Windows Time Service; http://support.microsoft.com; Q224799

[8]RPC Error Messages Returned for Active Directory Replication when Time is Out of Synchronization; http://support.microsoft.com

[9]IBM Distributed Computing Environment Base Services/400; SC09-1712-00

[10]S/390 Time Management and IBM 9037 Sysplex Timer; http://www.redbooks.ibm.com/redbooks/SG242070.html

[11]IDC, Email Deluge Continues with No End in Sight, Oct 2000; http://www.idc.com/software/press/PR/SW101000pr.stm

丸文株式会社

東京都中央区日本橋大伝馬町8-1 丸文ダイヤビル 〒103-8577
システム営業本部　情報機器部　TEL 03-3639-9881　FAX 03-5644-7627　http://www.marubun.co.jp/comnet