ネットワーク タイム プロトコル

ネットワーク タイム プロトコル（NTP）は、マシンのネットワークの時刻同期を行うように設計されたプロトコルです。NTP は UDP で稼働し、UDP は IP 上で稼働します。NTP バージョン 3 は、RFC 1305 に記載されています。

このモジュールでは、シスコ デバイスで Network Time Protocol を設定する方法について説明します。

ネットワー タイム プロトコルについて

時刻サービスとカレンダーサービス

システム上の時刻データのプライマリ ソースは、ソフトウェア クロックです。このクロックはシステムが起動した瞬間から稼働して、現在の日付と時刻を追跡します。ソフトウェア クロックは多数のソースから設定でき、さまざまなメカニズムを介して他のシステムに現在の時刻を配信するために使用できます。ハードウェアクロックが内蔵されたデバイスを初期化または再起動すると、ハードウェアクロックの時刻に基づいてソフトウェアクロックが初期設定されます。その後、ソフトウェア クロックは次のソースによって更新できます。

- 手動設定（ハードウェア クロックを使用）
- ネットワーク タイム プロトコル（NTP）
- 簡易ネットワーク管理プロトコル（SNMP）
- Virtual Integrated Network Service（VINES）タイムサービス

ソフトウェアクロックは動的に更新できるため、ハードウェアクロックよりも正確である可能性があります。

ソフトウェア クロックは次のサービスに時刻を提供できます。

- アクセス リスト
- ログおよびデバッグ メッセージ
- NTP
- ハードウェア クロック
- user **show** コマンド
- VINES 時刻サービス

（注） SNTP を使用してクロックを設定した場合、ソフトウェアクロックは NTP または VINES 時刻サービスに時刻を提供できません。

ソフトウェアクロックは、グリニッジ標準時（GMT）とも呼ばれる協定世界時（UTC）に基づいて内部的に時刻を追跡します。ローカル時間帯に対して時刻が正しく表示されるように、地域の時間帯とサマータイムに関する情報を設定できます。

ソフトウェアクロックは、時刻が「正規」であるかどうか（つまり、信頼できると見なされる時刻源によって設定されたかどうか）を追跡します。正規でない場合、時刻は表示のためだけに使用でき、再配信されません。

ネットワーク タイム プロトコル

ネットワーク タイム プロトコル（NTP）は、マシンのネットワークの時刻同期を行うように設計されたプロトコルです。NTP は UDP で稼働し、UDP は IP 上で稼働します。NTP バージョン 3（NTPv3）は、RFC 1305 に記載されています。

NTP ネットワークは通常、タイム サーバに接続されたラジオ クロックやアトミック クロックなど、正規の時刻源から時刻を取得します。NTP は、ネットワークにこの時刻を分配します。NTP はきわめて効率的です。毎分 1 パケットだけで、2 台のマシンが相互に 1 ミリ秒以内の精度で同期します。

NTP では、信頼できるタイム ソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。Stratum 1 タイムサーバーには通常、正規の時刻源（電波時計、原子時計、Global Positioning System（GPS）時刻源など）が直接接続されています。Stratum 2 タイムサーバーは、Stratum 1 タイムサーバーから NTP を介して時刻を受信し、それ以降のサーバーも続きます。

NTP は、次の 2 つの方法により、時刻が正確でない可能性があるマシンへの同期を回避します。NTP は、NTP と同期していないマシンとは同期しません。複数のマシンから報告された時刻を比較し、他のマシンと時刻が大きく異なるマシンとは、そのストラタムがより低くても同期しません。このようにして、NTP サーバのツリーは効率よく自律的に編成されています。

シスコの NTP 実装では、Stratum 1 サービスをサポートしていないため、電波時計や原子時計に接続することはできません（ただし、いくつかの特定のプラットフォームでは、GPS 時刻源

デバイスに接続できます）。ネットワークのタイムサービスは、IPインターネットで利用できるパブリック NTP サーバーから取得することをお勧めします。

ネットワークがインターネットから分離されている場合、NTPの実装により、実際にはネットワークが他の手段を使用して時刻を決定している場合でも、あたかも NTP 経由で同期しているかのように動作するようにマシンを構成できます。これにより、他のマシンが NTP を介してそのマシンと同期できるようになります。

多くの製造業者のホストシステムで、NTP ソフトウェアが導入されています。また、UNIX システム向けに公開されているバージョンもあります。また、このソフトウェアにより UNIX 派生サーバーは原子時計から時刻を直接取得することができ、シスコデバイスに時刻情報を伝えるようにすることもできます。

NTPを実行しているマシン間の通信（アソシエーション）は通常、静的に設定されており、各マシンには、アソシエーションを形成する必要があるすべてのマシンの IP アドレスが通知されます。アソシエーションが設定されたマシンの各ペアの間で NTP メッセージを交換することにより、正確な時刻管理が可能になります。

ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。この代替手段では、ブロードキャストメッセージを送受信するように各マシンを設定できるので、設定の複雑さが緩和されます。ただし、情報の流れが一方向のみであるため、計時精度はわずかに低下します。

マシン上の時刻は重要な情報であるため、NTPのセキュリティ機能を使用して、不正な時刻を誤って（または悪意を持って）設定できないように保護することを強く推奨します。アクセスリストベースの制約方式と、暗号化認証メカニズムの2つのセキュリティメカニズムが使用できます。

複数の時刻源（VINES、ハードウェア クロック、手動による設定）がある場合、NTP は常により信頼できる時刻源とされます。NTP の時刻は、他の方法による時刻に優先します。

NTP サービスは、デフォルトではすべてのインターフェイスで無効になっています。

NTP の詳細については、次の項を参照してください。

ポーリング ベースの NTP アソシエーション

NTP を実行しているネットワーキング デバイスは、時刻を基準時刻源と同期する際にさまざまなアソシエーションモードで動作するように設定できます。ネットワーキングデバイスは、2つの方法でネットワーク上の時刻情報を取得できます。それらは、ホストサービスのポーリングと NTP ブロードキャストのリスニングです。ここでは、ポーリングベースのアソシエーション モードを中心に説明します。ブロードキャスト ベースの NTP アソシエーションの詳細については、「ブロードキャスト ベースの NTP アソシエーション」を参照してください。

最も一般的に使用される 2 つのポーリングベースのアソシエーション モードは次のとおりです。

- クライアント モード
- 対称アクティブ モード

クライアント モードと対称アクティブ モードは、高レベルの時刻の精度と信頼性を提供するために NTP が必要になる場合に使用します。

クライアント モードで動作しているネットワーキング デバイスは、自身に割り当てられている時刻提供ホストをポーリングして現在の時刻を取得します。次に、ネットワーキングデバイスは、ポーリングされたすべてのタイム サーバーから、同期に使用するホストを選択します。この場合は、確立された関係がクライアントホスト関係なので、ホストがローカル クライアントデバイスから送信された時刻情報をキャプチャしたり使用したりすることはありません。このモードが最も適しているのは、他のローカル クライアントにどのような形式の時刻同期も提供する必要のない、ファイルサーバーおよびワークステーションのクライアントです。ネットワーキングデバイスを同期させるタイムサーバーを個別に指定し、クライアントモードで動作するようにネットワーキングデバイスを設定するには、**ntp server** コマンドを使用します。

対称アクティブ モードで動作しているネットワーキング デバイスは、自身に割り当てられている時刻提供ホストをポーリングして現在の時刻を取得し、そのホストによるポーリングに応答します。これはピアツーピアの関係なので、ホストは、通信相手のローカル ネットワーキング デバイスの時刻関連情報も保持します。このモードは、さまざまなネットワーク パスを経由で多数の冗長サーバーが相互接続されている場合に使用します。インターネット上のほとんどの Stratum 1 および Stratum 2 サーバーは、この形式のネットワーク設定を採用しています。ネットワーキングデバイスを同期させる時刻提供ホストを個別に指定し、対称アクティブモードで動作するようにネットワーキングデバイスを設定するには、**ntp peer** コマンドを使用します。

各ネットワーキング デバイスの設定モードを決定する際には、タイムキーピング デバイスとしてのそのデバイスの役割（サーバーかクライアントか）と、そのデバイスが Stratum 1 タイムキーピング サーバーにどれだけ近いかを主に考慮してください。

ネットワーキング デバイスは、クライアント モードでクライアントまたはホストとして動作する場合、または対称アクティブ モードでピアとして動作する場合にポーリングに関与します。通常、ポーリングによってメモリおよび CPU リソース（帯域幅など）に負荷が生じることはありませんが、システム上で進行または同時実行しているポーリングの数がきわめて多い場合には、システムの性能に深刻な影響があったり、特定のネットワークの性能が低下したりする可能性があります。過剰な数のポーリングがネットワーク上で進行することを防止するには、直接的なピアツーピア アソシエーションまたはクライアントからサーバーへのアソシエーションを制限する必要があります。代わりに、局所的なネットワーク内に NTP ブロードキャストを使用して時刻情報を伝播することを検討します。

ブロードキャスト ベースの NTP アソシエーション

ブロードキャストベースの NTP アソシエーションは、時刻の精度および信頼性要件が適度であり、ネットワークが局所的であり、クライアント数が 20 を超える場合に使用します。また、帯域幅、システム メモリ、または CPU リソースが制限されているネットワークにおいても、ブロードキャストベースの NTP アソシエーションの使用をお勧めします。

ブロードキャスト クライアント モードで動作しているネットワーキング デバイスはポーリングに関与しません。代わりに、ブロードキャスト タイム サーバーによって転送される NTP ブロードキャスト パケットを待ち受けます。その結果、時刻情報の流れが一方向に限られるため、時刻の精度がわずかに低下する可能性があります。

ネットワークを通じて伝播される NTP ブロードキャスト パケットをリッスンするようにネットワーキング デバイスを設定するには、**ntp broadcast client** コマンドを使用します。ブロードキャスト クライアント モードが動作するためには、ブロードキャスト サーバーとそのクライアントが同じサブネット上に存在する必要があります。**ntp broadcast** コマンドを使用して、特定のデバイスのインターフェイスで NTP ブロードキャストケットを送信するタイムサーバーを有効にする必要があります。

NTP アクセス グループ

アクセスリストベースの制限スキームを使用すると、ネットワーク全体、ネットワーク内のサブネット、またはサブネット内のホストに対し、特定のアクセス権限を許可または拒否できます。NTP アクセスグループを設定するには、グローバル コンフィギュレーション モードで **ntp access-group** コマンドを使用します。

アクセス グループのオプションは、次の順序で制限の緩いものから厳しいものへとスキャンされます。

1. **ipv4**：IPv4 アクセスリストを設定します。
2. **ipv6**：IPv6 アクセスリストを設定します。
3. **peer**：時刻要求と NTP 制御クエリを許可し、システムがアクセスリストの基準を満たすアドレスを持つ別のシステムに同期することを許可します。
4. **serve**：時刻要求と NTP 制御クエリーを許可しますが、システムがアクセスリストの基準を満たすアドレスを持つ別のシステムに同期することは許可しません。
5. **serve-only**：アクセスリストの条件を満たすアドレスを持つシステムからの時刻要求のみを許可します。
6. **query-only**：アクセスリストの基準を満たすアドレスを持つ別のシステムからの NTP 制御クエリーのみを許可します。

送信元 IP アドレスが複数のアクセス タイプのアクセス リストに一致する場合は、最初のアクセス タイプのアクセスが認可されます。アクセス グループが指定されていない場合は、すべてのシステムへのアクセスがすべてのアクセス タイプに対して認可されます。アクセス グループが指定されている場合は、指定されたアクセス タイプに対してのみアクセスが認可されます。

NTP 制御クエリーの詳細については、RFC 1305（NTP バージョン 3）を参照してください。

信頼できる形式のアクセス コントロールが必要な場合は、暗号化された NTP 認証方式を使用する必要があります。IP アドレスに基づくアクセス リスト ベースの制約方式とは異なり、暗号化認証方式では、認証キーと認証プロセスを使用して、ローカル ネットワーク上の指定されたピアまたはサーバーによって送信された NTP 同期パケットが信頼できると見なされるかどうかを、一緒に伝送された時刻情報を受け入れる前に判断します。

認証プロセスは、NTP パケットが作成されるとすぐに開始されます。暗号チェックサム キーは、Message-Digest Algorithm 5（MD5）を使用して生成され、受信側クライアントに送信される NTP 同期パケットに埋め込まれます。パケットがクライアントによって受信されると、暗号チェックサム キーが復号され、信頼できるキーのリストに対してチェックされます。一致す

る認証キーがパケットに含まれる場合、受信側クライアントは、パケットに含まれるタイムスタンプ情報を受け入れます。一致するオーセンティケータ キーが含まれていない NTP 同期パケットは無視されます。

（注） 信頼できるキーを多数設定する必要がある大規模なネットワークでは、信頼できるキーの範囲設定機能を使用して複数のキーを同時に有効にすることができます。

NTP 認証で使用される暗号化および復号化プロセスでは、CPU に非常に大きな負荷がかかる場合があり、ネットワーク内で伝播される時刻の精度が大きく低下する可能性があることに注意してください。より包括的なアクセス コントロール モデルを使用できるネットワーク構成の場合は、アクセス リスト ベースのコントロール方式を使用することを検討してください。

NTP認証が適切に設定されると、ネットワーキングデバイスは、信頼できる時刻源と同期し、信頼できる時刻源だけに同期を提供します。

特定のインターフェイス上の NTP サービス

Network Time Protocol（NTP）サービスは、デフォルトではすべてのインターフェイスで無効になっています。なんらかの NTP コマンドを入力すると、NTP がグローバルに有効になります。特定のインターフェイスを通じて特定のNTPパケットを受信しないように設定するには、インターフェイス コンフィギュレーション モードで **ntp disable** コマンドを使用します。

NTP パケットの送信元 IP アドレス

システムがNTPパケットを送信すると、通常、送信元IPアドレスは、そのNTPパケットの送信元であるインターフェイスのアドレスに設定されます。IP 送信元アドレスの取得元のインターフェイスを設定するには、グローバル コンフィギュレーション モードで **ntp source** *interface* コマンドを使用します。

このインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用されます。特定のアソシエーションに送信元アドレスを使用する場合は、**ntp peer** コマンドまたは **ntp server** コマンドで **source** キーワードを使用します。

正規の NTP サーバとしてのシステム

システムを正規の NTP サーバーにする場合は、グローバル コンフィギュレーション モードで **ntp** コマンドを使用します。これは、システムが外部の時刻源と同期されていない場合でも同じです。

（注） **ntp primary** コマンドの使用には注意が必要です。このコマンドを使用すると、有効な時刻源が容易に上書きされてしまいます。低いストラタム番号を設定する際には、特に注意が必要です。**ntp primary** コマンドを使用して同じネットワーク内の複数のマシンを設定した場合は、それらのマシンの時刻が一致していないと、時刻管理が不安定になることがあります。

孤立モード

NTP サブネットは、ローカル基準クロックまたはインターネット クロック サーバーから分離されることがあります。この分離期間中、サブネットサーバーとクライアントは共通のタイムスケールに同期されます。ローカルクロックドライバは、UTC ソースをシミュレートして、共通のタイムスケールを提供します。ドライバに直接または間接的に接続されたサーバーは、サブネット内の他のホストを同期します。

ローカルクロックドライバを使用すると、サブネットの回復不能な障害が発生する可能性があり、複数のサーバーを使用して冗長性を維持することは現実的ではありません。このような欠点のない孤立モード機能により、ローカルクロックドライバが不要になります。孤立モード機能は、複数のサーバーを備えた単一のシミュレートされた UTC ソースと、サーバーが障害から回復する際のシームレスな切り替えメカニズムを提供します。

プライベート ネットワークでは、通常、最下位のストラタムで動作する 1 つまたは複数のコアサーバーが含まれます。これらの各サーバーは、対称モードまたはブロードキャストモードを使用する他のサーバーのバックアップとして設定する必要があります。1 つのコアサーバーが UTC ソースに到達した場合でも、サブネット全体がシミュレートしているサーバーに同期されます。どのサーバーも UTC ソースに到達しない場合、いずれかのサーバー（孤立した親と呼ばれる）が UTC ソースをシミュレートし、サブネット内の他のすべてのホスト（孤立した子と呼ばれる）のシミュレートされた UTC ソースとして機能できます。

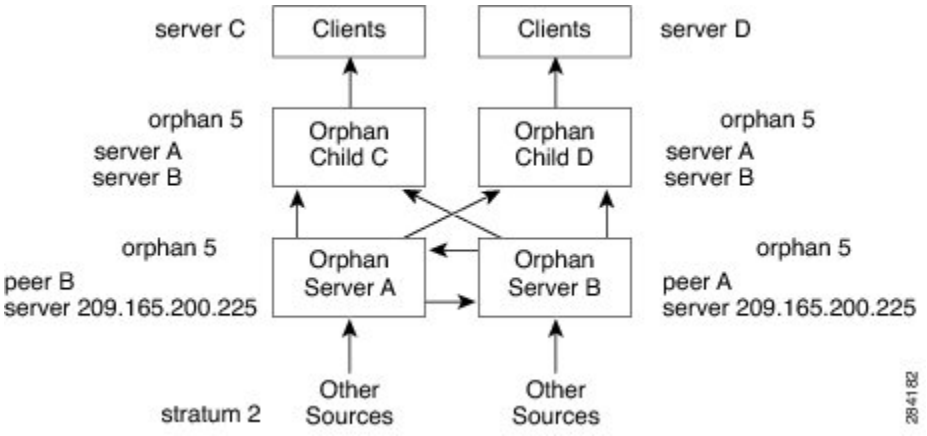
ntp orphan *stratum* コマンドを使用して、孤立モードのホストを有効にします。ここで、*stratum* は、16 未満で、設定されたインターネット タイム サーバーに出現するどのストラタム値よりも大きいストラタム値です。ただし、孤立した子に依存するすべてのサブネットホストのストラタム値が 16 未満になるように、十分なストラタムを指定する必要があります。他のサーバーまたは基準クロックのアソシエーションが設定されていない場合は、孤立ストラタム値を 1 に設定する必要があります。

ソースのないストラタム 1 で動作している孤立した親には、参照 ID LOOP が表示されます。ストラタム 1 で動作していない孤立した親は、UNIX ループバックアドレス 127.0.0.1 を表示します。通常の NTP クライアントは遅延と分散に基づく選択メトリックを使用しますが、孤立した子はサブネット内の各コアサーバーの IP アドレスから計算されたメトリックを使用します。各孤立した子は、最小のメトリックを持つ孤立した親をルートサーバーとして選択します。

すべてのソースを失ったサーバーは、ローカルクロックドライバを他のサーバーと継続的に同期させ、サーバーをバックアップします。コアサーバーと孤立した子でのみ孤立モードを有効にします。

次の図に、孤立モードのセットアップ方法とピアネットワーク設定を示します。この場合、2 台のプライマリまたはセカンダリ（ストラタム 2）サーバーが基準クロックまたはパブリック インターネット プライマリ サーバーで設定され、それぞれが対称モードを使用します。

図 *1:* 孤立モードの設定



孤立モードの前提条件

孤立モードをスムーズに機能させるには、同じストラタムで動作するように、使用可能なソースを使用して各コアサーバーを設定する必要があります。すべてのコアサーバーと孤立した子で **ntp orphan** コマンドを設定します。すべてのルートサーバーで孤立した子を設定します。

Simple Network Time Protocol

簡易ネットワーク タイム プロトコル（SNTP）とは、クライアント専用バージョンの簡易版 NTP です。SNTP は、NTP サーバから時刻を受信できるだけで、時刻サービスを他のシステムに提供できません。

通常、SNTP は 100 ミリ秒以内の精度で時刻を提供しますが、NTP のような複雑なフィルタリングや統計メカニズムは提供しません。また、拡張アクセスリストを設定することによってある程度の保護を提供できますが、トラフィックを認証できません。SNTP クライアントは、NTP クライアントよりも予期しない動作をするサーバーに対して脆弱であるため、強力な認証が必要ない状況でのみ使用する必要があります。

SNTP は、設定済みのサーバーからパケットを要求して受け入れるように設定するか、任意の送信元から NTP ブロードキャスト パケットを受け入れるように設定できます。複数の送信元が NTP パケットを送信している場合、最適な層にあるサーバーが選択されます（階層の説明については、3 ページの「*Network Time Protocol*」セクションを参照してください）。複数のサーバーのストラタムが同じだった場合は、ブロードキャスト サーバーよりも設定済みサーバーが優先されます。これらの両方を満たすサーバーが複数ある場合は、時刻パケットを最初に送信したサーバーが選択されます。SNTP が新しいサーバを選択するのは、現在選択しているサーバからのパケットの受信を停止している場合、または（上記の基準に従って）より適切なサーバが検出された場合だけです。

VINES 時刻サービス

Banyan VINES を設定すると、時刻サービスを使用できます。このプロトコルは、VINES の標準部分です。シスコの実装では、2つの方法でVINES時刻サービスを使用できます。最初の方

法では、他の時刻源から時刻を認識すると、システムは VINES タイム サーバとして動作し、VINES を実行している他のマシンに時刻を提供できます。2 番目の方法では、他の形式の時刻サービスを使用できない場合に、システムは VINES 時刻サービスを使用してソフトウェア クロックを設定できます。

（注） すべてのリリースで、Banyan VINE および Xerox Network Systems（XNS）のサポートが利用できるわけではありません。

ハードウェア クロック

一部のデバイスは、システムの再起動から電源停止に至る日付および時刻を追跡するバッテリ駆動式のハードウェアクロックを内蔵しています。システムの再起動時には、ハードウェア クロックを常に使用してソフトウェア クロックが初期化されます。

（注） CLI コマンド構文においては、ハードウェアクロックは「システムカレンダー」と呼ばれます。

他の時刻源を使用できない場合、ハードウェアクロックは正規の時刻源と見なされ、NTP を通じて再配信されます。NTP が実行されている場合、ハードウェアクロックは NTP から定期的に更新され、ハードウェアクロックが実行されたままになっている場合に一定のレートで一貫した時間の増加または損失である固有のドリフトを補正できます。

任意のデバイスのハードウェアクロック（システムカレンダー）がソフトウェアクロックから定期的に更新されるように設定できます。この設定は、NTP を使用するすべてのデバイスに推奨される方法です。それは、ハードウェアクロックの時刻設定は時間とともにわずかにドリフトする可能性があり、（NTP を使用して設定する）ソフトウェアクロックの時刻と日付の方がハードウェアクロックよりも正確であるためです。

ルーティングデバイスが NTP 経由で外部の時刻源と同期されている場合に、ハードウェアクロックを NTP 時刻に同期させるときは、グローバル コンフィギュレーション モードで次の **ntp update-calendar** コマンドを使用します。

時間範囲

シスコソフトウェアでは、時刻に基づいて機能を実装できます。**time-range** グローバル コンフィギュレーション コマンドを使用して、特定の日/曜日の時間を定義します。この時間を関数から参照することにより、関数そのものに時間的制約を設定することができます。

リリースによっては、時間範囲を使用できる機能は、IP および Internetwork Packet Exchange（IPX）拡張アクセスリストだけです。時間範囲を使用すると、ネットワーク管理者はアクセス リストで permit 文または deny 文がいつ有効になるかを定義できます。この機能が導入されるまで、アクセスリストの文は、いったん適用すると常に有効になったままでした。時間範囲は、名前付きアクセス リストと番号付きアクセス リストの両方から参照できます。

（注） 時間帯はシステムのソフトウェアクロックに基づきます。時間範囲機能が意図したとおりに機能するためには、信頼できるクロック ソースが必要になります。NTP を使用してシステムのソフトウェアクロックを同期させることを推奨します。

時間範囲の利点は次のとおりです。

- ネットワーク管理者は、リソースへのユーザーアクセスの許可または拒否の制御をより強化できます。これらのリソースとして、アプリケーション（IPアドレス/マスクペアとポート番号によって特定されます）、ポリシールーティング、またはオンデマンドリンク（ダイヤラへの関連トラフィックとして認識されます）があります。
- ネットワーク管理者は、次の内容を含む時間ベースのセキュリティポリシーを設定できます。
  - Cisco Firewall フィーチャセットまたはアクセスリストを使用する境界セキュリティなどがあります。
  - シスコ暗号化テクノロジーまたは IP セキュリティによるデータの機密性。
- ポリシーベース ルーティングおよび キューイング機能が拡張されています。
- プロバイダーのアクセスレートが時間帯によって異なる場合、トラフィックを自動的かつコスト効率よく再ルーティングできます。
- サービスプロバイダーは、特定の時間にネゴシエートされる Quality of Service（QoS）サービスレベル契約（SLA）をサポートするために専用アクセスレート（CAR）を動的に変更できます。

ネットワーク管理者は、ロギング メッセージを制御できます。アクセス リスト エントリは、一日の特定の時間帯にトラフィックをロギングすることはできますが、常にロギングすることはできません。したがって、管理者は、ピーク時に生成される多数のログを分析することなく、アクセスを拒否できます。

ネットワーク タイム プロトコルの設定方法

NTP の設定

ネットワーク タイム プロトコルに関する制約事項

Network Time Protocol（NTP）パッケージには、認証されていないリモート攻撃者がサービス妨害（DoS）状態を発生させる可能性がある脆弱性が含まれています。NTP バージョン 4.2.4p7 以前は脆弱です。

この脆弱性は、特定の不正メッセージの処理におけるエラーによるものです。認証されていないリモート攻撃者は、スプーフィングされた送信元 IP アドレスを使用して、悪意ある NTP パ

ケットを脆弱なホストに送信する可能性があります。このパケットを処理するホストは、送信者に応答パケットを返信します。この処理により、2 つのホスト間でメッセージのループが開始される可能性があります。その結果、両方のホストは、過剰な CPU リソースを消費し、ログファイルへのメッセージの書き込みにディスク スペースを使い切り、ネットワーク帯域幅を消費します。これにより、影響を受けたホスト上で DoS 状態が発生する可能性があります。

詳細については、Web ページ「Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability」を参照してください。

NTPv4 をサポートしている Cisco ソフトウェア リリースは影響を受けません。この問題は、その他すべての Cisco ソフトウェア バージョンに影響を及ぼします。

デバイスが NTP を使用するように設定されているかどうかを表示するには、**show running-config | include ntp** コマンドを使用します。出力に次のいずれかのコマンドが返された場合、そのデバイスは DoS 攻撃に対して脆弱です。

- **ntp broadcast client**
- **ntp primary**
- **ntp multicast client**
- **ntp peer**
- **ntp server**

Cisco ソフトウェア リリースの詳細については、『White Paper: Cisco IOS and NX-OS Software Reference Guide』を参照してください。

デバイスで NTP を無効にする以外にこの脆弱性に対する回避策はありません。この脆弱性を悪用できるのは、デバイス上の設定済み IP アドレスに宛てられたパケットだけです。中継トラフィックは、この脆弱性を悪用しません。

リリースによっては NTP モード 7 パケットが処理され、NTP のデバッグが有効になっている場合は「NTP: Receive: dropping message: Received NTP private mode 7 packet」というメッセージが表示されることがあります。**ntp allow mode private** コマンドを設定し、NTP モード 7 パケットを処理します。このコマンドは、デフォルトで無効になっています。

（注） NTP ピア認証は回避策ではなく、脆弱な設定です。

NTP サービスは、デフォルトではすべてのインターフェイスで無効になっています。

NTP を実行しているネットワーキング デバイスは、時刻を基準時刻源と同期する際にさまざまなアソシエーションモードで動作するように設定できます。ネットワーキング デバイスは、2 つの方法でネットワーク上の時刻情報を取得できます。それらは、ホスト サービスのポーリングと NTP ブロードキャストのリスニングです。

Line Aux 0 オプションはデフォルトで無効になっています。

Cisco IOS XE で同じ NTP サーバーの IP アドレスと FQDN の両方を設定すると、FQDN が同じ IP アドレスに解決された後、FQDN 設定のみが **show running-config** コマンド出力に表示されます。

ポーリング ベースの NTP アソシエーションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**]
4. **ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**] 例： `Device(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer`	他のシステムとのピアアソシエーションを形成します。
ステップ 4	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] 例： `Device(config)# ntp server 192.168.10.1 version 2 prefer`	他のシステムとのサーバーアソシエーションを形成します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ブロードキャスト ベースの NTP アソシエーションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ntp broadcast version** *number*
5. **ntp broadcast client**
6. **ntp broadcastdelay** *microseconds*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ntp broadcast version** *number* 例： `Device(config-if)# ntp broadcast version 2`	指定されたインターフェイスがNTPブロードキャスト パケットを送信するように設定します。
ステップ 5	**ntp broadcast client** 例： `Device(config-if)# ntp broadcast client`	指定されたインターフェイスがNTPブロードキャスト パケットを受信するように設定します。
ステップ 6	**ntp broadcastdelay** *microseconds* 例： `Device(config-if)# ntp broadcastdelay 100`	NTPブロードキャストの推定ラウンドトリップ遅延を調整します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NTP 認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp authenticate**
4. **ntp authentication-key** *number* **md5** *key*
5. **ntp authentication-key** *number* **md5** *key*
6. **ntp authentication-key** *number* **md5** *key*
7. **ntp trusted-key** *key-number* [**-** *end-key*]
8. **ntp server** *ip-address* **key** *key-id*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ntp authenticate** 例： `Device(config)# ntp authenticate`	NTP 認証機能を有効にします。
ステップ 4	**ntp authentication-key** *number* **md5** *key* 例：	認証キーを定義します。 • キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。
ステップ 5	**ntp authentication-key** *number* **md5** *key* 例：	認証キーを定義します。

	コマンドまたはアクション	目的
		• キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。
ステップ 6	**ntp authentication-key** *number* **md5** *key* 例： `Device(config)# ntp trusted-key 1 - 3`	認証キーを定義します。 • キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。
ステップ 7	**ntp trusted-key** *key-number* [- *end-key*] 例： `Device(config)# ntp trusted-key 1 - 3`	信頼できる認証キーを定義します。 • キーを信頼できる場合、このデバイスは、このキーをNTPパケット内で使用する別のシステムに同期できます。
ステップ 8	**ntp server** *ip-address* **key** *key-id* 例： `Device(config)# ntp server 172.16.22.44 key 2`	NTP タイム サーバーによってソフトウェア クロックが同期されるように設定します。 （注） 複数の NTP サーバーが設定され、ロギングが有効になっている場合、クロック同期損失メッセージがデバイスでランダムに表示されます。この問題を解決するには、**peer** キーワードを使用して NTP サーバーを設定します。 `Device(config)# ntp server ip-address [version number] [key key-id] [prefer]`
ステップ 9	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

外部基準クロックの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **line aux** *line-number*
4. **end**
5. **show ntp associations**
6. **show ntp status**
7. **debug ntp refclock**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line aux** *line-number* 例： `Device(config)# line aux 0`	補助ポート 0 のライン コンフィギュレーション モードを開始します。
ステップ 4	**end** 例： `Device(config-line)# end`	回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。
ステップ 5	**show ntp associations** 例： `Device# show ntp associations`	NTP アソシエーションのステータスを表示します（GPS 基準クロックのステータスを含みます）。
ステップ 6	**show ntp status** 例： `Device# show ntp status`	NTP のステータスを表示します。
ステップ 7	**debug ntp refclock** 例： `Device# debug ntp refclock`	デバッグを目的とした基準クロック動作の拡張モニタリングを許可します。

孤立モードの設定

孤立モードを設定するには、少なくとも 2 つのクライアントが必要です。次のタスクは、1 つのクライアントで孤立モードを設定する方法を示しています。他のクライアントで手順を繰り返します。

手順の概要

1. **enable**

2. **configure terminal**
3. **ntp server** *ip-address*
4. **ntp peer** *ip-address*
5. **ntp orphan** *stratum*
6. 他のクライアントでも手順 1 ～ 5 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ntp server** *ip-address* 例： `Router(config)# ntp server 10.1.1.1`	他のシステムとのサーバーアソシエーションを形成します。
ステップ 4	**ntp peer** *ip-address* 例： `Router(config)# ntp peer 172.16.0.1`	他のシステムとのピアアソシエーションを形成します。 （注） 他のクライアントでピアを設定するときに、設定したばかりの IP アドレスとは異なる IP アドレス（172.16.0.2 など）を使用します。
ステップ 5	**ntp orphan** *stratum* 例： `Router(config)# ntp orphan 4`	ホストで孤立モードを有効にします。
ステップ 6	他のクライアントでも手順 1 ～ 5 を繰り返します。	

SNTP の設定

SNTP は通常、NTP をサポートしていないプラットフォームでサポートされます。SNTP は、デフォルトでディセーブルになっています。SNTP を構成するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **sntp server** {*address* | *hostname*} [**version** *number*]
4. **sntp broadcast client**
5. **exit**
6. **show sntp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sntp server** {*address* | *hostname*} [**version** *number*] 例： `Device(config)# sntp server 192.168.2.1 version 2`	NTP サーバーからの NTP パケットを要求するように SNTP を設定します。 • 各 NTP サーバーについて、**sntp server** コマンドを 1 回入力します。NTP サーバーは、デバイスからの SNTP メッセージに応答するように設定する必要があります。
ステップ 4	**sntp broadcast client** 例： `Device(config)# sntp broadcast client`	任意の NTP ブロードキャストからの NTP パケットを受け入れるように SNTP を設定します。 （注） **sntp server** コマンドと **sntp broadcast client** コマンドの両方を入力した場合、層が同じであるとすると、デバイスはブロードキャストサーバーからの時刻を受け入れますが、設定されたサーバーからの時刻を優先します。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show sntp** 例： `Device# show sntp`	SNTP に関する情報を表示します。

VINES 時刻サービスの設定

Banyan VINES を設定すると、時刻サービスを使用できます。このプロトコルは、VINES の標準部分です。VINE タイムサービスを設定するには、次のタスクを実行します。

（注） リリースに応じて、Banyan VINE および XNS は Cisco ソフトウェアで使用できます。 **vines time set-system** および **vines time use-system** コマンドは、一部のリリースでは使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **vines time use-system**
4. **vines time set-system**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vines time use-system** 例： `Device(config)# vines time use-system`	システムのソフトウェア クロック時刻を他の VINES システムに配信します。
ステップ 4	**vines time set-system** 例： `Device(config)# vines time set-system`	VINES タイムサービスから導出されたソフトウェア クロック システムの時刻と日付を設定します。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

日付と時刻の設定

他の時刻源を使用できない場合は、システムの再起動後に現在の時刻と日付を手動で設定できます。設定した時刻は、次回システムを再起動するまで正確に維持されます。手動設定は最後の手段としてのみ使用することを推奨します。

デバイスが同期できる外部の時刻源がある場合は、ソフトウェアクロックを手動で設定できないことがあります。時刻と日付を手動で設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **clock timezone** *zone hours-offset* [*minutes-offset*]
4. **clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]
5. **clock summer-time** *zone* **date** *date month year hh*:*mm date month year hh*:*mm* [*offset*]
6. **exit**
7. **clock set** *hh*:*mm*:*ss date month year*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock timezone** *zone hours-offset* [*minutes-offset*] 例： `Device(config)# clock timezone PST 2 30`	シスコソフトウェアで使用されるタイムゾーンを設定します。 （注） **clock timezone** コマンドの *minutes-offset* 引数は、ローカル時間帯が UTC/GMT と 1 時間の何 % 異なるかによって表される場合に使用できます。たとえば、アトランティックカナダの一部の地域の時間帯（大西洋標準時（AST））は UTC-3.5 です。この場合に必要なコマンドは、**clock timezone AST –3 30** です。
ステップ 4	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]] 例：	サマータイム（夏時間）を毎年特定の曜日に開始および終了する地域で設定します。

	コマンドまたはアクション	目的
	`Device(config)# clock summer-time PST recurring 1 monday january 12:12 4 Tuesday december 12:12 120`	
ステップ 5	**clock summer-time** *zone* **date** *date month year hh*:*mm date month year hh*:*mm* [*offset*] 例： `Device(config)# clock summer-time PST date 1 january 1999 12:12 4 december 2001 12:12 120`	特定のサマー タイムの開始日と終了日を設定します。 • *offset* 引数は、UTC との時間帯の時差（時間数）です。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**clock set** *hh*:*mm*:*ss date month year* 例： `Device# clock set 12:12:12 1 january 2011`	ソフトウェア クロックを設定します。 • 他の時刻源を使用できない場合は、次のコマンドを使用してください。このコマンドで指定する時刻は、設定されている時間帯に対応します。 （注） 一般に、NTP や VINES クロック ソースなどの有効な外部の時刻メカニズムによってシステムが同期されている場合や、ハードウェアクロックを内蔵したデバイスを使用する場合には、ソフトウェアクロックを設定する必要があります。

ハードウェア クロックの設定

ほとんどのシスコデバイスは、ソフトウェアベースのクロックに加えて、別個のハードウェアベースのクロックを内蔵しています。ハードウェアクロックは、デバイスの各再起動間で時刻および日付情報を維持できる充電式バックアップ バッテリを備えたチップです。

ネットワーク上の正規の時刻源からの最も正確な時刻のアップデートを維持するため、ソフトウェアクロックは、ネットワーク上の正規の時刻源から時刻のアップデートを受信する必要があります。ハードウェア クロックは、システムが稼働している間、ソフトウェア クロック から定期的に更新される必要があります。

ハードウェア クロック（システム カレンダー）は、ソフトウェア クロックとは別に時刻を維持しています。システムを再起動した場合や、電源を遮断した場合でも、ハードウェア クロックは動作し続けます。通常、ハードウェアクロックは、システムのインストール時に1回だけ手動で設定する必要があります。

信頼できる外部時刻ソースにアクセスできる場合は、ハードウェアクロックを設定しないでください。代わりに、NTP を使用して時刻同期を確立する必要があります。

ハードウェアクロックを設定するには、次のタスクを実行します。

始める前に

（注） リリースに応じて、NTP は Linux カーネルの時刻を更新する IOS デーモン（IOSd）内で実行されます。Linux カーネルは 11 分ごとにハードウェアクロックを更新するため、NTP はハードウェアクロックと直接対話しません。したがって、カレンダー関連のコマンドは必要ありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **clock calendar-valid**
4. **exit**
5. **clock read-calendar**
6. **clock update-calendar**
7. **show calendar**
8. **show clock** [**detail**]
9. **show ntp associations** [**detail**]
10. **show ntp status**
11. **show sntp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock calendar-valid** 例： `Device(config)# clock calendar-valid`	ネットワークピアを同期できる有効な時刻源としてデバイスが動作できるようにします。 • デフォルトでは、ソフトウェアクロックで維持される時刻は信頼できるものとみなされず、NTP または VINES タイムサービスと同期され

	コマンドまたはアクション	目的
		ません。ハードウェアクロックを有効な時刻源として設定するには、このコマンドを使用します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**clock read-calendar** 例： `Device# clock read-calendar`	ソフトウェアクロックを新しいハードウェアクロック設定に設定します。
ステップ 6	**clock update-calendar** 例： `Device# clock update-calendar`	新しいソフトウェアクロック設定でハードウェアクロックを更新します。
ステップ 7	**show calendar** 例： `Device# show calendar`	ハードウェア クロックの現在の時刻を表示します。
ステップ 8	**show clock** [**detail**] 例： `Device# show clock detail`	ソフトウェア クロックの現在の時刻を表示します。
ステップ 9	**show ntp associations** [**detail**] 例： `Device# show ntp associations detail`	NTP アソシエーションのステータスを表示します。
ステップ 10	**show ntp status** 例： `Device# show ntp status`	NTP のステータスを表示します。
ステップ 11	**show sntp** 例： `Device# show sntp`	SNTP に関する情報を表示します。

時間範囲の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **time-range** *time-range-name*
4. 次のいずれか 1 つを入力します。
   - **absolute** [**start** *hh*:*mm date month year*] [**end** *hh*:*mm date month year*]
   - **periodic** *day-of-the-week hh*:*mm* **to** [*day-of-the-week*] *hh*:*mm*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**time-range** *time-range-name* 例： `Device(config)# time-range range1`	設定する時間範囲に名前を割り当て、時間範囲コンフィギュレーション モードを開始します。

ステップ 4	次のいずれか 1 つを入力します。
	• **absolute** [**start** *hh*:*mm date month year*] [**end** *hh*:*mm date month year*]
	• **periodic** *day-of-the-week hh*:*mm* **to** [*day-of-the-week*] *hh*:*mm*
	例：
	`Device(config-time-range)# absolute start 12:12 30 January 1999 end 12:12 30 December 2000`
	`Device(config-time-range)# periodic monday 12:12 to friday 12:12`
		時間範囲が有効になる時期を指定します。
		• これらのコマンドをいくつか組み合わせて使用します。 **periodic** コマンドは複数指定できます。**absolute** コマンドは 1 つしか指定できません。

ステップ 5	**end** 例：	時間範囲コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-time-range)# end`	

ネットワーク タイム プロトコルの確認

手順の概要

1. **show clock** [**detail**]
2. **show ntp associations detail**
3. **show ntp status**

手順の詳細

ステップ 1 show clock [detail]

このコマンドを使用すると、ソフトウェア クロックの現在の時刻が表示されます。次に、このコマンドの出力例を示します。

例：

```
Device# show clock detail

*18:38:21.655 UTC Tue Jan 4 2011
Time source is hardware calendar
```

ステップ 2 show ntp associations detail

このコマンドを使用すると、NTP アソシエーションのステータスが表示されます。次に、このコマンドの出力例を示します。

例：

```
Device# show ntp associations detail

192.168.10.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode active, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.56
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time D0CDE881.9A6A9005 (18:42:09.603 UTC Tue Jan 4 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
192.168.45.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 16003.08
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**24, version 4
```

```
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
```

ステップ 3 **show ntp status**

このコマンドを使用すると、NTPのステータスが表示されます。次に、このコマンドの出力例を示します。

例：

```
Device# show ntp status

Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
reference time is D25AF07C.4B439650 (15:26:04.294 PDT Tue Oct 21 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.31 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 10 sec ago.
```

ネットワーク タイム プロトコルの設定例

例：ネットワーク タイム プロトコルの設定

次の例では、ハードウェア クロックを内蔵したデバイスが、他の 2 つのシステムとのサーバアソシエーションを確立し、ブロードキャスト NTP パケットを送信し、ハードウェア クロックを定期的に更新し、時刻を VINES に再配信します。

```
clock timezone PST -8
clock summer-time PDT recurring

ntp server 192.168.13.57
ntp server 192.168.11.58
interface GigabitEthernet 0/0
 ntp broadcast
vines time use-system
```

次の例では、ハードウェア クロックを内蔵したデバイスは外部の時刻源を持たないため、ハードウェア クロックを正規の時刻源として使用し、NTP ブロードキャスト パケットを介して時刻を配信します。

```
clock timezone MET 2
clock calendar-valid
ntp master
interface vlan 3
 ntp broadcast
```

次の例は、Line Aux 0 オプションがデフォルトで無効になっていることを示しています。

```
config-register 0x0
reload
rommon 1 > set
rommon 2 >  AUX_PORT=1
rommon 3 > SYNC
rommon 4 > reset
rommon 1 > set
rommon 2 > confreg 0x2102
rommon 3 > reset
```

ネットワーク タイム プロトコルの関連資料

関連資料

関連項目	マニュアル タイトル
基本的なシステム管理コマンド	『Basic System Management Command Reference』
IPv6 の NTP4	『*Cisco IOS Basic System Management Guide*』
IP 拡張アクセス リスト	『*Cisco IOS IP Addressing Configuration Guide*』
IPX 拡張アクセス リスト	『*Novell IPX Configuration Guide*』
NTP パッケージの脆弱性	『*Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability*』
Cisco IOS および NX-OS ソフトウェア リリース	『*White Paper: Cisco IOS and NX-OS Software Reference Guide*』

標準および RFC

標準および RFC	タイトル
RFC 1305	『*Network Time Protocol (Version 3) Specification, Implementation and Analysis*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ネットワーク タイム プロトコルの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1:* ネットワーク タイム プロトコルの機能情報

機能名	リリース	機能情報
ネットワーク タイム プロトコル	11.2(1) 12.2(28)SB 12.2(33)SRA 12.2(33)SXI 12.2(33)SXJ 12.2(50)SY 12.2(58)SE 15.0(1)M 15.1(2)S 15.1(2)SG Cisco IOS XE リリース 3E	NTP は、ネットワーク接続されたマシンの時刻を同期させる目的で設計されたプロトコルです。NTP は UDP で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 で規定されています。 次のコマンドが導入または変更されました。**ntp access-group**、**ntp allow mode passive**、**ntp authenticate**、**ntp authentication-key**、**ntp broadcast, ntp broadcast client**、**ntp broadcastdelay**、**ntp clear drift**、**ntp clock-period**、**ntp disable**、**ntp logging**、**ntp primary**、**ntp max-associations**、**ntp multicast**、**ntp multicast client**、**ntp server**、**ntp source**、**ntp trusted-key** および **ntp update-calendar**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。