



Simple Network Time Protocol

Simple Network Time Protocol (SNTP) は、Network Time Protocol (NTP) の簡易バージョンです。このモジュールでは、シスコデバイスで Simple Network Time Protocol を設定する方法について説明します。

- [Simple Network Time Protocol に関する制約事項 \(1 ページ\)](#)
- [Simple Network Time Protocol について \(1 ページ\)](#)
- [Simple Network Time Protocol の設定方法 \(2 ページ\)](#)
- [Simple Network Time Protocol の設定例 \(4 ページ\)](#)
- [Simple Network Time Protocol の追加資料 \(4 ページ\)](#)
- [SNTP の機能情報 \(5 ページ\)](#)

Simple Network Time Protocol に関する制約事項

- Simple Network Time Protocol (SNTP) と Network Time Protocol (NTP) は、同じポートを使用するため、同じマシン上で共存できません。つまり、これら2つのサービスをシステムで同時に設定することはできません。
- IPv6 アドレスのサポートは、イメージが IPv6 アドレッシングをサポートしている場合にのみ使用できます。

Simple Network Time Protocol について

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。

Simple Network Time Protocol の設定方法

Simple Network Time Protocol (SNTP) 認証の設定

Simple Network Time Protocol (SNTP) は、Network Time Protocol (SNTP) の簡易バージョンです。このモジュールでは、シスコデバイスで SNTP を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sntp authenticate**
4. **sntp authentication-key number md5 key**
5. **sntp trusted-key key-number [- end-key]**
6. **sntp server ip-address key key-id**
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	sntp authenticate 例： Device(config)# sntp authenticate	SNTP 認証機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	sntp authentication-key <i>number md5 key</i> 例： Device(config)# sntp authentication-key 1 md5 key1	認証キーを定義します。 <ul style="list-style-type: none"> 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。 追加の認証キーを定義するには、この手順を繰り返します。
ステップ 5	sntp trusted-key <i>key-number [- end-key]</i> 例： Device(config)# sntp trusted-key 1 - 3	信頼できる認証キーを定義します。 <ul style="list-style-type: none"> キーを信頼できる場合、このデバイスは、このキーを SNTP 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 6	sntp server <i>ip-address key key-id</i> 例： Device(config)# sntp server 172.16.22.44 key 2	SNTP 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。
ステップ 7	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。

Simple Network Time Protocol の確認とトラブルシューティング

Simple Network Time Protocol の設定を確認してトラブルシューティングするには、次のコマンドを使用します。

-

手順の概要

1. **enable**
2. **debug sntp packets [detail]**
3. **debug sntp select**
4. **show sntp**

手順の詳細

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 debug sntp packets [detail]

例 :

Device> debug sntp packets

送受信された NTP パケットを SNTP パケットフィールドとともに表示します。

ステップ 3 debug sntp select

例 :

Device> debug sntp select

IPv4 および IPv6 サーバーの SNTP サーバーの選択を表示します。

ステップ 4 show sntp

例 :

Device# show sntp

```
SNTP server      Stratum  Version  Last Receive
172.168.10.1    16       1        never
Broadcast client mode is enabled.
Multicast client 224.0.1.1 is enabled.
```

Cisco デバイスで使用可能な SNTP に関する情報を表示します。

Simple Network Time Protocol の設定例

例 : Simple Network Time Protocol の設定

```
clock timezone PST -8
clock summer-time PDT recurring
sntp update-calendar
sntp server 192.168.13.57
sntp server 192.168.11.58
interface Ethernet 0/0
 sntp broadcast
```

Simple Network Time Protocol の追加資料

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』

関連項目	マニュアルタイトル
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

SNTP 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 トレー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: *SNTPv4* の機能情報

機能名	リリース	機能情報
Simple Network Time Protocol		<p>Simple Network Time Protocol (SNTP) は、Network Time Protocol (NTP) の簡易バージョンです。このモジュールでは、シスコデバイスで Simple Network Time Protocol を設定する方法について説明します。</p> <p>次のコマンドが導入または変更されました。sntp server、sntp authenticate、sntp authentication-key、sntp multicast、sntp trusted-key。</p>

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。