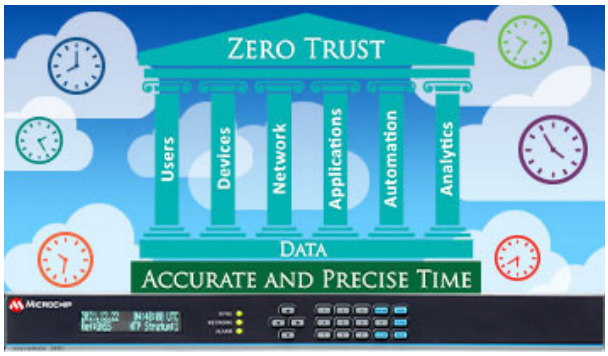
ゼロトラスト ネットワークの Trusted Time と インターネット NTP サーバプールの時刻との比較

概要

ゼロトラスト アーキテクチャを展開している組織はパブリックな NTP サーバプールから時刻を取得するのがいかに非合理で、ゼロトラストの基本概念にどう反しているかを理解する必要があります。正確な時刻はネットワークの運用に不可欠であり、ネットワークに接続されたタイムサーバのセキュリティの信頼性が様々な局面で確保されている必要があります。SyncServer® ネットワーク タイムサーバは正確な時刻を提供する能力だけではなく、ゼロトラスト原則に準拠しているという点で他の追随を許しません。



ネットワーク時刻同期という危険な選択

企業の基幹システムの時刻を同期するのに一般公開されている NTP サーバプールを使いたくなる事があるでしょう。例えば、法人向けエッジルータの中にも、その内部クロックを NTP (Network Time Protocol) を使ってインターネット上のどこかにあるタイムサーバと同期しているものがあります。その後、これらのルータは社内ネットワークの NTP サーバとして機能します。これはタイムスタンプを取得する手段として、低コストですがリスクの高いソリューションです。

また、プライマリ ドメイン コントローラを使ってファイアウォールの 123 番ポートを開放してインターネット タイムサーバの IP アドレスを参照するシナリオもあります。その後、このドメイン コントローラが時刻をネットワークを通してカスケードします。この方法はこれまでも随所で説明されており、かなり簡単に設定できます。しかし、インターネットから無償で取得した時刻は想定されるコスト削減とリスクに見合うものでしょうか。

不合理な信頼

ゼロトラスト ネットワークには 2 つの主要な概念があります。

- **ゼロトラスト :** 信頼は決して無条件に与えられるものではないというサイバー セキュリティ パラダイム
- **ゼロトラスト アーキテクチャ:** 企業リソースとデータ セキュリティに対するエンドツーエンドのアプローチ

ゼロトラストのモットーは「信じるな。常に検証せよ」

組織がインターネット ベースのタイムサーバに依拠している場合、検証できるのは NTP 時刻リクエストが特定の IP アドレスに送信されると 2 つの追加のタイムスタンプを含む NTP パケットが返されるという事だけです。それ以外にはありません。その正確性、信頼性、安全性を示す根拠は一切ありません。

なのにリモートのタイムサーバに対して無条件の信頼が与えられています。組織がエンドツーエンドの認証や承認を実装していないために、検証せずに信頼しているのです。これは不合理な信頼です。

別の言い方をすれば、ntppool.org で利用可能となっている 4,000 以上ある NTP サーバの 1 つから割り当てられた IP アドレスに対してファイアウォールのポート 123 を開放してネットワーク全体を同期させているとも言えます。こうした行為はリスクを伴います。

現実化する恐怖、不確実性、疑念

NTP サーバプールを信頼する事は不合理な信頼の良い例です。NTP タイムスタンプは常に平文で送信されるため、中間者攻撃シナリオによって簡単に操作される可能性があります。また、ntppool.org 等の NTP タイムサーバ プールに追加されるタイムサーバは審査されていないため、悪意を持った者は誰でもタイムサーバをプールに追加して、そのタイムサーバに割り当てられた NTP クライアントに提供されるタイムスタンプを操作できます。

実際にあった事例で、一見信頼性が高いように見えたインターネット タイムサーバでしたが、ある医療機関の NTP サーバに意図的に誤ったタイムスタンプを送信するよう設定されていました。これは、タイムサーバの所有者が、これらの NTP クライアントがあまりに頻繁に時刻を要求してくるのを不審に思った事から発覚しました。問題の原因が不正なインターネット タイムサーバにあると分かるまで、その医療機関のログファイルと患者データは夜通し被害を受け続けました。医療機関はその後同様のリスクが発生するのを防ぐため、社内に stratum 1 タイムサーバを導入する事にしました。

この実例から、問題の核心が浮き彫りになります。ログファイルと正確なタイムスタンプはきわめて重要なのです。

時刻はなぜ重要か

IT(情報技術) セキュリティはデータ、リソース、個人情報等を保護する役目をになっています。その役目には、全ネットワーク アクティビティについて「誰が」「何を」「どこで」「**いつ**」したかを管理する事と、組織のネットワークに接続する事を許可された全てのデバイスを検証する事が含まれます。ゼロトラスト アーキテクチャはこうしたセキュリティ上の課題に対処するために作成されました。

タイムスタンプの混乱を防ぐ

ネットワーク全体の時刻同期の正確性と、それがネットワーク管理とセキュリティに果たしている重要な役割は、多くの場合、当然の事であると考えられています。仮に全てのネットワーク デバイスの時刻がずれていたらどうなるか想像してみてください。組織のネットワーク全体が大混乱に陥るでしょう。ログとテレメトリのタイムスタンプの相互関係が崩れるため、ログファイルとネットワーク テレメトリは全く役に立たなくなります。例えば、syslog を仮にリアルタイムで受信していたとしても、タイムスタンプが先週の日付だったら意味がありません。ダッシュボードはエラーになるか、少なくとも表示されるデータは不正確となり、アラームが発生する可能性が高いでしょう。クリティカルなプロセスの開始が早まったり、遅れたりします。ネットワーク フォレンジックはほぼ不可能になり、監査は意味を為さなくなります。ビデオ タイムスタンプも不正確になります。組織のネットワーク全体で時刻が正確である事がいかに重要なのかが分かります。

ネットワーク タイムソースが重要

ネットワーク時刻同期のタイムソースについて、「誰が」「何を」「どこで」**「いつ」**提供しているのかを検討する事が重要です。その「何を」に当たるのが NTP (Network Time Protocol) タイムスタンプを提供しているタイムサーバです。「誰が」と「どこで」が単に任意のインターネット NTP サーバプール内のタイムサーバの IP アドレスである場合、受信した NTP タイムスタンプの「いつ」の妥当性と脆弱性を検討する必要があります。インターネットから取得した時刻はゼロトラストのほぼ全ての原則に違反しており、信頼できる時刻とみなす事はできません。

Trusted Time とは

自社ネットワークの時刻を NTP を使って適当な場所から同期すると仮定した場合、ゼロトラストは 2 つの重要な問題を投げ掛けます。その時刻が暗黙的に、または明示的に信頼されているのか、そして、タイムサーバ自体がその企業のネットワークに接続されるデバイスとしてゼロトラストのネットワーク技術と互換性があるかという問題です。

Trusted Time とは、時刻の正確性と正当性についてタイムサーバが信頼されている事を意味します。また、タイムサーバがネットワークに接続されるデバイスとして信頼されており、企業のゼロトラスト セキュリティ要件に準拠している事も意味しています。

SyncServer タイムサーバはなぜ Trusted Time サーバなのか

SyncServer® タイムサーバは現在市販されている最もセキュアで信頼できるタイム ネットワーク デバイスであり、ゼロトラスト モデルの基本原則* に準拠しています。図 1 に示すように、この基本原則にはユーザ、デバイス、ネットワーク、アプリケーション、分析が含まれます。

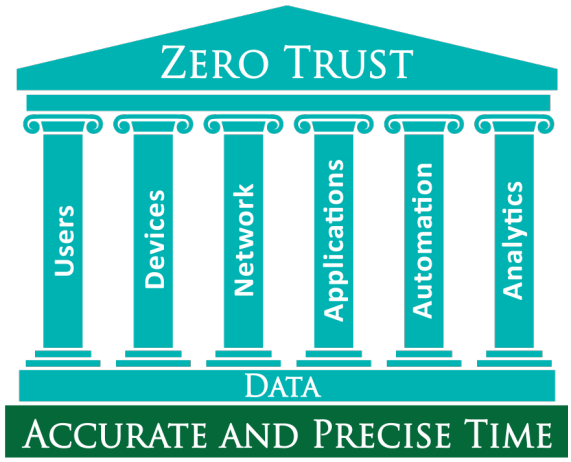


図 1. 精確な時刻はゼロトラスト ネットワークの基盤

SyncServer タイムサーバは『NIST Special Publication 800-207: Zero Trust Architecture』に記載されているコア コンポーネントにも準拠しています。該当するコア コンポーネントの簡略図を図 2 に示します。この図では SyncServer タイムサーバが NIST のデータプレーンと制御プレーンの間でどのように相互運用されるのかが分かります。

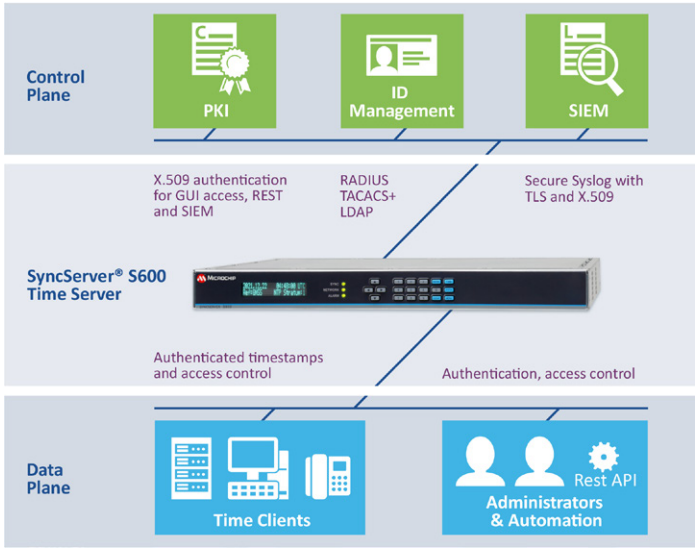


図 2. NIST で定義されたデータプレーンと制御プレーン間の SyncServer タイムサーバの相互運用性

ゼロトラストの大元の前提にあるのは、時刻とタイムサーバを含め、何者にも無条件の信頼を与えないという事です。SyncServer タイムサーバを使ってゼロトラスト アーキテクチャにおいて信頼できる時間を実装するシナリオはいくつも考えられます。これらのシナリオの一部を示すインフォグラフィックを作成しました。各図では、SyncServer タイムサーバに搭載されたセキュリティ技術と、それに関連するゼロトラスト原則が簡単に参照できるようにハイライトされています。全てのインフォグラフィックを Microchip 社の「ゼロトラスト ネットワークの Trusted Time」ウェブページでご覧頂けます。

Trusted Time に関する詳細情報

Microchip 社では、ゼロトラスト アーキテクチャへの移行をお考えの企業様向けに、ゼロトラスト ネットワークにおいて時刻の信頼性がなぜ重要かを説明したアプリケーション ノートを作成しました。ここで、SyncServer ネットワーク タイムサーバがいかにして時刻のセキュリティを確保し、ゼロトラスト原則に準拠しているかを端的に説明します。SyncServer タイムサーバのセキュリティ機能の詳細な一覧と、それらがゼロトラスト モデルの基本原則にいかに適合しているのかを記載しています。

SyncServer S600/S650 タイムサーバが自社のネットワーク セキュリティ要件に準拠しているかどうかを確かめるために、貴社のセキュリティ チームは図 3 に示すチェックリストをお使い頂けます。

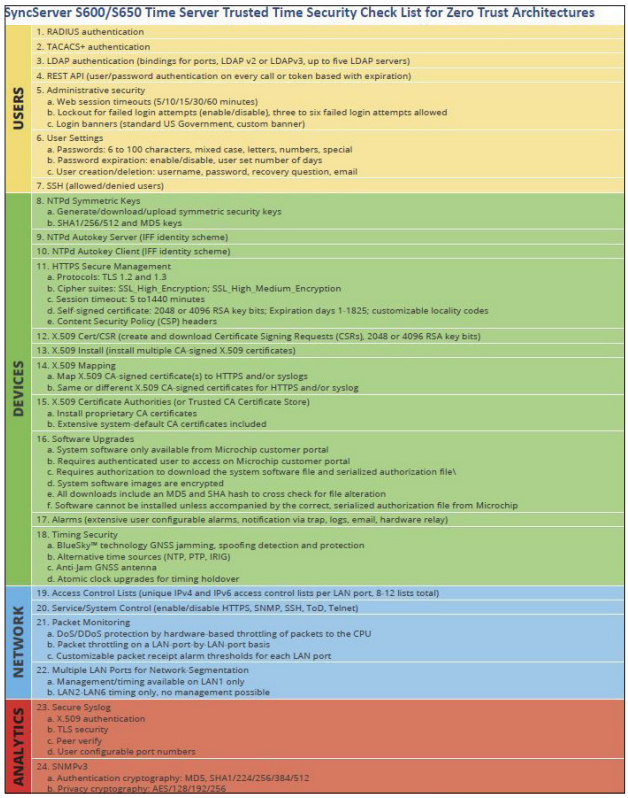


図 3. SyncServer S600/S650 タイムサーバ Trusted Time のゼロトラスト アーキテクチャ向けセキュリティ チェックリスト

時刻をゼロトラストに準拠させる

SyncServer タイムサーバは最もセキュアな Trusted Time ネットワーク デバイスであり、あらゆる組織におけるゼロトラストの取り組みをサポートするのに最適です。時刻とタイムソースのセキュリティを確保すると共に、ゼロトラストの基本原則に準拠しています。

資料へのリンク

ウェブページ : ゼロトラスト ネットワークの Trusted Time

アプリケーション ノート : ゼロトラスト ネットワークの Trusted Time

* ACT-IAC(米国技術協議会および産業諮問協議会)、Zero Trust Cybersecurity Current Trends (2019 年 4 月 18 日)