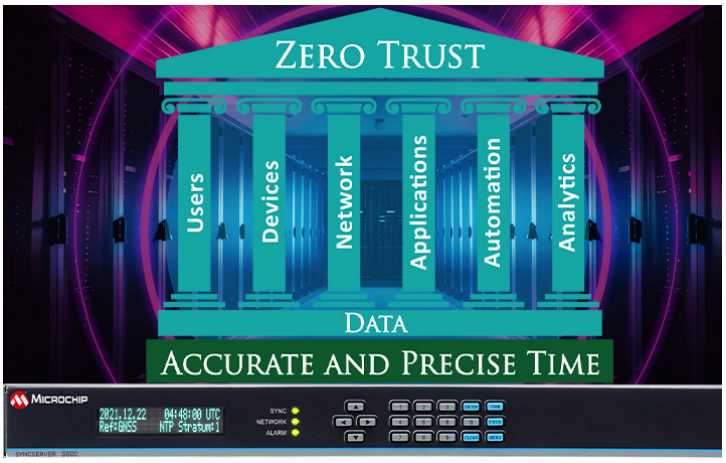
ゼロトラスト データセンター ネットワークにおいて Trusted Time とは何か、なぜ重要なのか

概要

ゼロトラスト アーキテクチャにオンプレミス データセンターとコロケーション データセンターのエンクレーブを展開しようとする組織は、その分散型ネットワークの正確な時刻同期と、時刻同期を提供しているタイムサーバのセキュリティに注意する必要があります。正確な時刻は分散型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。



時刻はなぜ重要なのか

IT(情報技術) セキュリティは分散配置されているデータセンター間でデータ、リソース、個人情報等を保護する役目を担っています。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。地理的に離れた場所にあるデータセンターはネットワーク アクティビティが「**いつ**」発生したかに関連する時刻同期の課題に直面します。単一のネットワーク タイムサーバーがネットワーク全体の同期を保つ事を期待する場合、データセンター間の経路遅延の非対称性により、時間のオフセットを把握するのはほぼ不可能です。時間のオフセットにより、ログファイルのタイムスタンプの整合性が取れなくなり、監視およびセキュリティ目的でネットワーク全体のアクティビティを集約しているネットワーク管理システムの整合性が損なわれます。

タイムスタンプの混乱を防ぐ

多くの場合、ネットワーク全体の時刻同期が正確である事と、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、あって当然のものとみなされています。仮に全てのデータセンターの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関関係が崩れるため、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、タイムスタンプが誤っていれば役に立ちません。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ます。監査は無意味になります。ビデオタイムスタンプも不正確になります。データセンター全体で時刻が正確である事は確かに重要です。

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」が単にデータセンターの近くにある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

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 サーバーなのか

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。

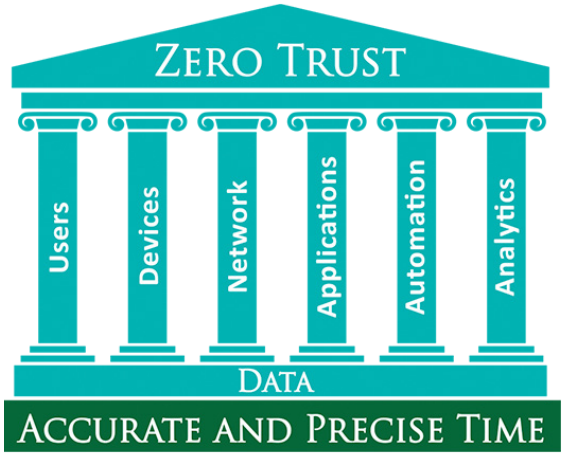


図 1. 精確な時刻はゼロトラスト ネットワークの基盤

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 で定義された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。

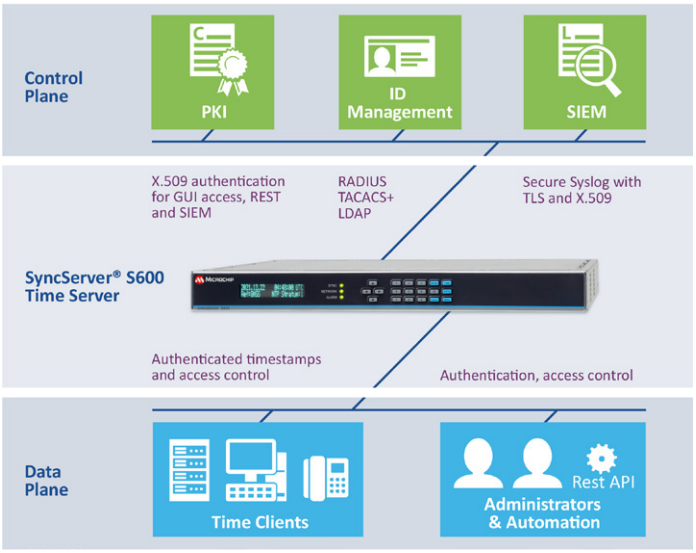


図 2.NIST で定義されたデータプレーンと制御プレーン間の SyncServer タイムサーバの相互運用性

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、何者にも盲目的な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多数考えられます。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、データセンター全体のゼロトラスト 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なのかを説明したアプリケーション ノートを作成しました。短い文書の中で 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かが記載されています。

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。

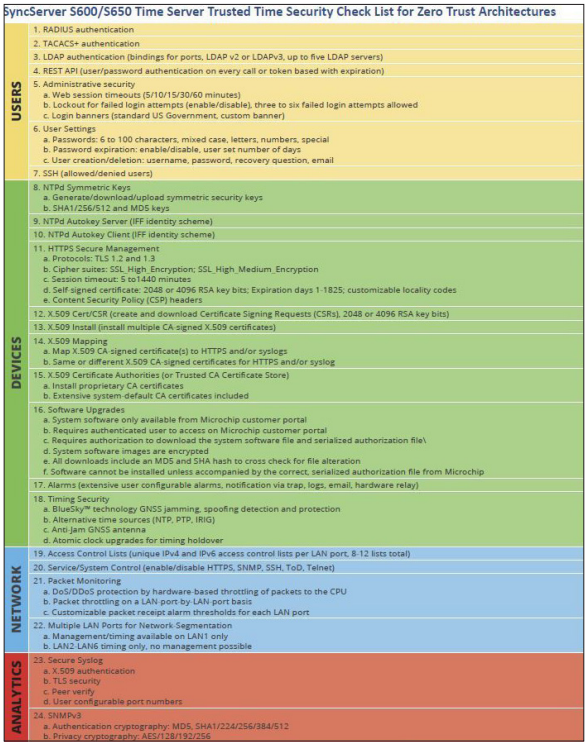


図 3.SyncServer S600/S650 タイムサーバのゼロトラスト アーキテクチャ向け Trusted Time セキュリティ チェックリスト

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、地理的に離れた場所にあるデータセンター間で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)