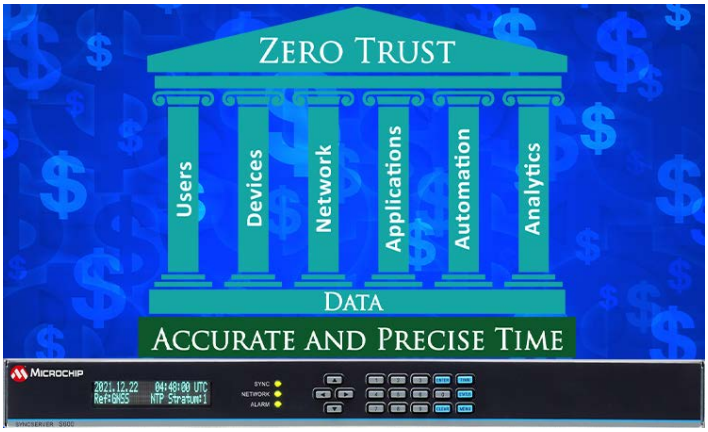
ゼロトラスト金融ネットワークにおいて Trusted Time とは何か、なぜ重要なのか

概要

ゼロトラスト アーキテクチャを展開している金融/銀行系企業は、ネットワークの正確な時刻同期とそれを提供するタイムサーバに細心の注意を払う必要があります。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面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 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

銀行の IT(情報技術) セキュリティはデータ、リソース、マネー、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、銀行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 アーキテクチャと PCI-DSS (Payment Card Industry Data Security Standard) 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。銀行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。銀行のネットワーク、または組織のネットワーク全体で時刻の正確性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

時刻は非常に重要であるため、「誰が」「何を」「どこで」**「いつ」**提供しているのかを検討する必要があります。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」が単にインターネット上またはインターネット 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取得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銀行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な Trusted Time™ 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。

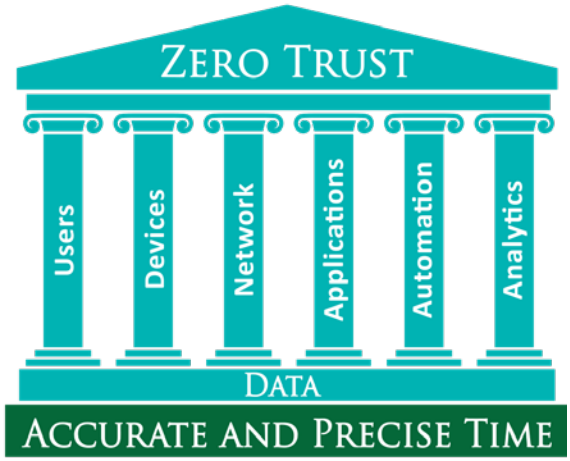


図 1. 精確な時刻はゼロトラスト ネットワークの基盤

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 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。

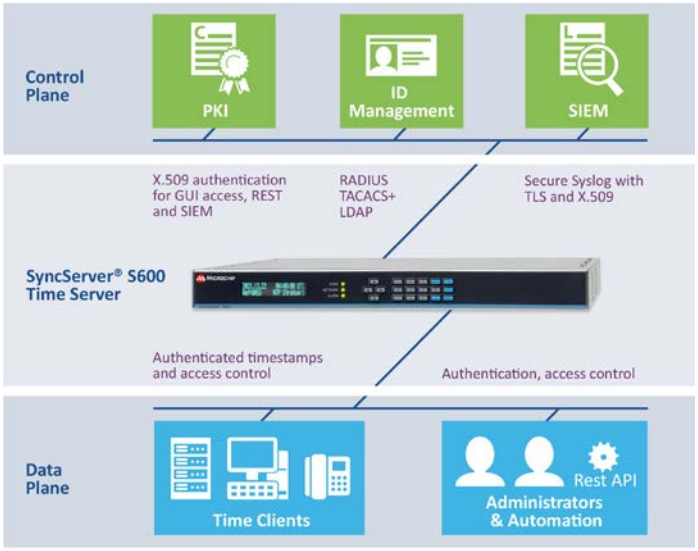


図 2. NIST で定義されたデータプレーンと制御プレーン間の SyncServer の相互運用性

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多く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こちらでご覧頂けます。

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 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 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 のチェックリストをお使い頂けます。

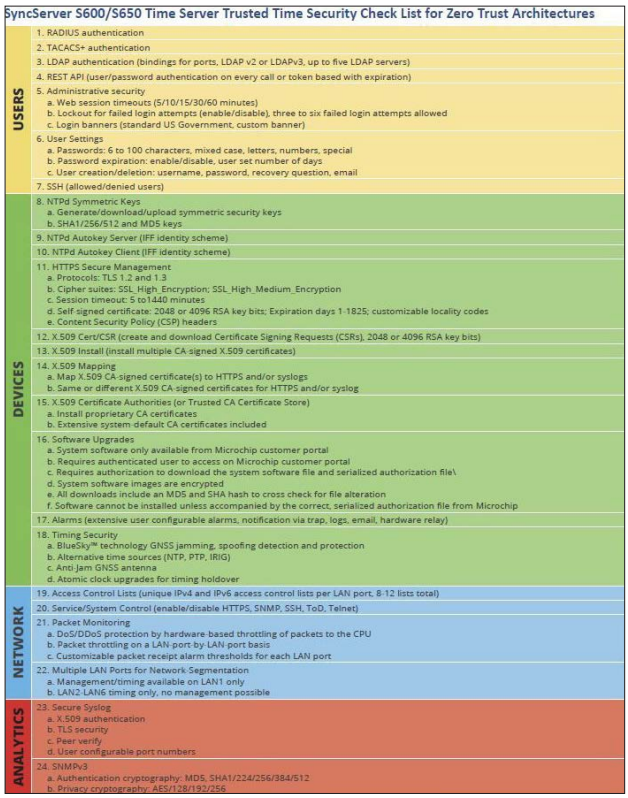


図 3. SyncServer S600/S650 タイムサーバのゼロトラスト アーキテクチャ向け Trusted Time セキュリティ チェックリスト

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、銀行と金融機関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)

Microchip 社の名称とロゴ、Microchip ロゴ、SyncServer は米国およびその他の国における Microchip Technology Incorporated の登録商標です。Trusted Time は米国およびその他の国における Microchip Technology Incorporated の商標です。その他の商標は各社に帰属します。
© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved. 8/23