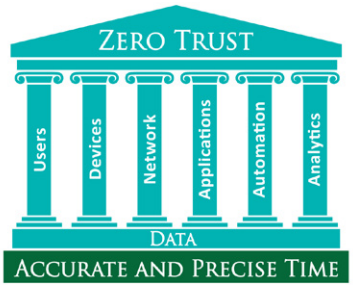
# ゼロトラスト ネットワークの Trusted Time

## SyncServer® S600 タイムサーバは Trusted Time の基盤となるソースとしてゼロトラスト ネットワークのスムーズな運用を可能にします。




### 概要

ゼロトラスト ネットワークにおける全てのアクティビティで「誰が」「何を」「いつ」「どこで」したかを定義する正確なログファイルにとって重要なのは時刻です。

正確で信頼性が高く安全な Trusted Time はゼロトラスト ネットワークの基盤です。それが欠けていれば、認証メカニズムは機能しなくなり、重要なログファイル タイムスタンプは一致しなくなり、ゼロトラスト分析の信頼性は損なわれ、フォレンジックが妨げられる他、多くの問題が考えられます。

時刻が正しいだけでなく、タイムサーバもゼロトラストの原則に準拠しゼロトラスト アーキテクチャに適合している必要があります。

SyncServer S600 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、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、ユーザ、デバイス、ネットワーク、分析等のゼロトラストの基本原則に準拠しています[i]。

### 主な特長

- 最もセキュアなネットワーク タイムサーバ
- 認証済みのタイムスタンプ
- セキュアな syslog
- X.509 証明書/PKI
- RADIUS/TACACS+/LDAP
- 強化されたユーザ インターフェイス
- タイムソースの検証
- ネットワーク セグメンテーションのサポート

**時刻の正確性はゼロトラストの基盤です。**時刻はゼロトラスト ネットワークの管理と監視における「誰が」「何を」「いつ」「どこで」の「いつ」に当たるものです。「いつ」とはログファイル内の正確なタイムスタンプです。NIST(米国標準技術研究所) によるゼロトラストの規格にはログのタイムスタンプが含まれており[ii]、最近米国政府が発行したゼロトラスト導入とサイバー セキュリティ インシデント修復能力に関する複数の大統領令によりログファイルのタイムスタンプ形式とタイムソースが定められています[iii]。

**サイバー セキュリティは精確なタイムスタンプを持つログファイルに依存しています。**ゼロトラスト分析で使われている SIEM(セキュリティ情報イベント監視) システムは正確かつ適時のネットワーク テレメトリに依存しています。これには、セキュリティ インシデント、ポリシー違反、不正行為、運用上の問題、監査とフォレンジック分析、内部調査、ベースラインの確立、運用トレンドと長期的問題の特定に役立つ正確なログファイル タイムスタンプが含まれています[iv]。

**タイムスタンプは時刻同期されたサーバとシステムから得られます。**SIEM 用のログファイルを生成する各システムは、タイムラインの混乱を防止して迅速なインシデント対応とフォルト診断を妨げないよう、少なくとも相互に時刻同期されている必要があります。

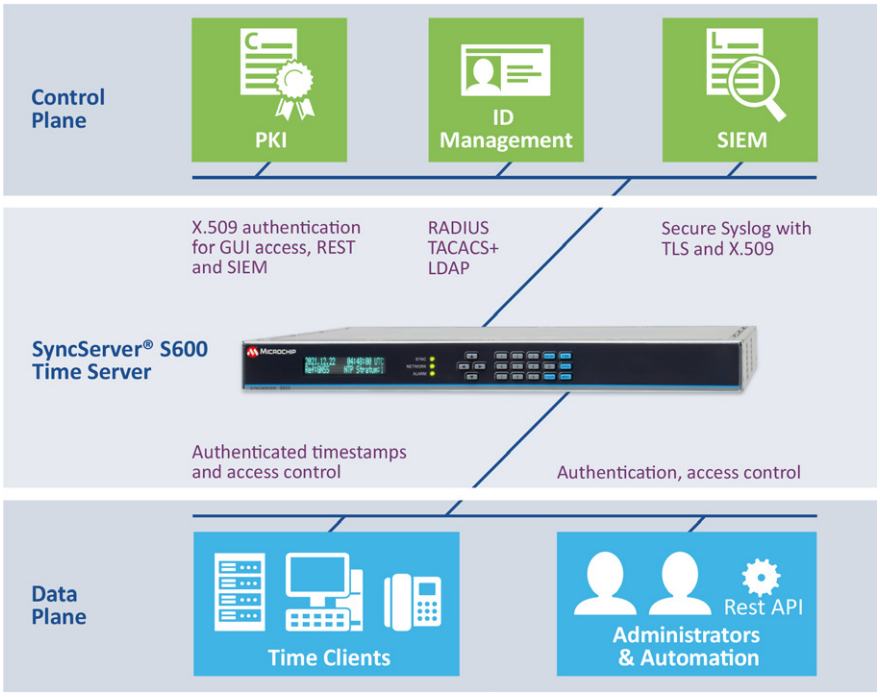
**タイムサーバはネットワーク サーバに時刻同期を提供します。**SyncServer S600 タイムサーバ等のデバイスは、SIEM に不可欠なログファイルを生成するクリティカルなネットワーク サーバ向けの正確で信頼性が高いセキュアなタイムソースです。

S600 はゼロトラスト ネットワークに配置するためにセキュリティが強化されています。これはゼロトラスト ネットワークへのタイムサービス プロバイダーとしての観点と、ゼロトラストのユーザ、デバイス、ネットワークという基本原則を設計に組み込むという観点から言えます。

**時刻の認証は重要です。**NTP (Network Time Protocol) パケットは規定上平文で送信されるため、転送中に容易に操作される可能性があります。ゼロトラスト時刻同期では、S600 と NTP クライアントのつながりが信頼できる事とタイムスタンプが改ざんされていない事を確認するために NTP 認証を有効にする必要があります。

**タイムサーバはゼロトラスト パラダイムに適合する必要があります。**Trusted Time は正しく機能する十分に強化されたゼロトラスト ネットワークに不可欠な要素です。ゼロトラスト ネットワーク全体で正確に同期された時刻という最も基本的な概念が欠けた場合、ゼロトラストの原則の多くは信頼性を持って機能しません。

**SyncServer S600 タイムサーバはゼロトラスト ネットワークに対応した信頼性の高い時刻です。**S600 はゼロトラスト ネットワークの柱を支える基盤です。セキュアで正確で信頼性の高いネットワーク全体の時刻同期により正確なログファイル タイムスタンプを可能にします。




## タイムサーバへの管理アクセス権を持つユーザには認証と承認が必要

Users

SyncServer S600 タイムサーバの防御の最前線に当たるのはネットワークの物理的および論理的なマイクロ セグメンテーションをサポートするポートごとの LAN アクセス制御リストです。

タイムサーバは手作業またはマシンによって設定される必要があるため、RADIUS、TACACS+、LDAP 等のプロトコルはアクセスに必要な堅牢な認証と承認を提供します。

また、タイムサーバは堅牢なパスワード要件、タイムアウト、有効期限、ローテーション等のローカルアクセスを厳密に制御する必要もあります。

SyncServer タイムサーバは全ての呼び出しについて認証情報または時間制限付きトークンで認証される事を要求する堅牢な REST API マシンインターフェイスも備えています。

## タイムサーバは全てが認証され信頼されている必要がある ゼロトラスト ネットワーク上のデバイスである

Devices

最も基本的なレベルにおいて、タイム クライアントと S600 の間で使われる対称キー認証はタイムパケットが転送中に改ざんされていない事を確実にします。タイミング パケットを認証するハッシュの作成には、SHA 256/512 等の強力なキーを使う必要があります。

ユニットの設定に使われる非常に多機能な S600 のウェブ GUI は使いやすさの面では優れていますが、そのインターフェイスは極限まで強化する必要があります。そのためには、非常にセキュアな TLS 1.3 ベースのリンクの暗号化と合わせて、X.509 CA 署名証明書を使ってユーザのブラウザに対して S600 を認証する必要があります。

ゼロトラストにはタイムサーバのソフトウェア アップデートも含まれます。認証および承認されたユーザのみが S600 のソフトウェア ダウンロードにアクセスできます。ソフトウェア イメージは改ざんを防ぐために暗号化されており、転送中に改ざんされていない事を確認するためのハッシュが用意されています。これらのダウンロードには、S600 のソフトウェアのインストールを制御する暗号化された認証ファイルも含まれています。ソフトウェアをインストールする前に、S600 はシリアル番号、バージョン、ソフトウェアの整合性を認証します。

SyncServer タイムサーバのシステム ソフトウェアはカスタムメイドで強化された最新の組み込み Linux® ディストリビューションであり、カスタム ハードウェアを操作するために必要な要素のみを含んでいます。したがって、広範な Linux ディストリビューションの CVE (Common Vulnerability and Exposure：共通脆弱性・暴露) に関連するものがあったとしても、S600 に存在しない/ロードされていない可能性が高いため、潜在的な攻撃対象領域が大幅に縮小されます。

Stratum 1 S600 が時刻を取得している GNSS 衛星システムはもはや信頼できるものとみなす事ができません。GNSS の妨害となりすましの脅威はますます蔓延しています。つまり、ゼロトラスト体制を敷く必要があるという事です。

GNSS の検証はローカル RF 環境に異常がないか監視し、受信した GNSS 信号のデータを検証するという形を取ります。S600 では組み込みの BlueSky™ テクノロジによる妨害およびなりすまし検出保護機能を使ってこれを行い、GNSS を継続的に検証しています。

## タイムサーバは DoS 攻撃に対して防御すると共にネットワークを物理的および論理的にセグメント化する必要がある

Network

ゼロトラスト ネットワークのセグメント化境界を容易にするため、S600 は最大 6 つの異なるネットワーク セグメントに NTP/PTP タイミング サービスを提供する 4～6 の分離された LAN ポートを備えています。ポート間のクロス トラフィックはありません。各ポートには二重のアクセス制御リストがあり、全てのポートが独自のネットワーク設定を持つ事ができます。ネットワークからの分離を強化するため、管理アクセスは 1 つの LAN ポートに厳密に制限されています。

DoS 攻撃から保護するため、S600 は独自の NTP Reflector テクノロジを採用しています。このテクノロジは高速の回線速度、大容量の NTP サービス、ホストのオーバーランとアラームを防止するパケット制限を提供しています。ユーザ設定のしきい値を超えるネットワーク トラフィックが発生するとアラームは作動しますが、S600 はタイミング パケットのみを処理します。そのため、DoS 負荷によって S600 の CPU に障害が発生する事は決してありません。

## タイムサーバはリアルタイム防御管理に必要な信頼性の高いタイムライン基盤分析を提供する

Analytics

分析は、ゼロトラストを実装するためのインサイトを提供するのにネットワーク テレメトリデータに依拠しています。根本的に、これらのデータはイベントまたはアクティビティが「いつ」発生したかが記録されたタイムスタンプを含むログファイルです。S600 はネットワーク上でログを送信する全てのデバイスを時刻同期するだけでなく、重要なログも提供します。ログは決して平文で送信してはならず[v]、セキュアな syslog で送信する必要があります。S600 のセキュアな syslog には、ログを送信する前に、SIEM によって認証される X.509 CA 署名証明書と SIEM の X.509 証明書をチェックするピア検証済み認証が組み込まれます。信頼が確立されると、ログファイルの改ざんや盗聴を防ぐため、TLS 経由で syslog データが送信されます。

セキュアな syslog と HTTPS ウェブ GUI 用に別の X.509 CA 署名証明書を使うと S600 をさらに強化できます。

## 「インターネット上で無償で提供されている時刻」を盲目的に信頼する事の不合理

パブリックなインターネット タイムサーバから時刻を取得するという事は、ゼロトラストのあらゆる主義原則を覆し、時刻の NTP リクエストにたまたま応答しただけのインターネットのどこかにある IP アドレスを盲目的に信頼するという事です。

パブリックにアドバタイズされている未認証のタイムサーバは、あらゆるゼロトラスト セキュリティ境界の外部にあり、その他のパブリックにアドバタイズされているタイムサーバを含むプール内に存在しています。このような未認証のタイムサーバは、転送中に容易に改ざんされるタイムスタンプを提供しており、DoS 攻撃を受けてサービスを停止させ、あるいは DoS 増幅攻撃に使われたり、GNSS の妨害またはなりすましの対象になる可能性があります。

不正なタイムスタンプを追跡するのはほぼ不可能であるだけでなく、リモートのタイムサーバがどこで時刻を取得しているのか、その管理に関連する制御の可視化またはコントロールが不可能であるため、パブリックのタイムサーバーはゼロトラスト ネットワークで使うタイムサービス リソースとしては不適切です。

ゼロトラストでは、重要かつ不可欠なタイムサーバを境界内に配置して保護し、認証し、監視して、ネットワークの基盤となるタイムサービスのセキュリティ、正確性、信頼性を守る事が求められます。

## 次のゼロトラスト監査は SyncServer S600 シリーズのタイムサーバで合格しよう

ゼロトラスト ネットワーク用に正しく設定された SyncServer S600 タイムサーバは、該当するあらゆる基本原則を満たし、正確で信頼性が高くセキュアな Trusted Time をゼロトラスト ネットワークに提供します。

TRUSTED TIME™ FOR ZERO TRUST NETWORKS

## 参考文献


i 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)

ii NIST Special Publication 800-207 Zero Trust Architecture (2020 年 8 月)

iii ホワイトハウス、Executive Order on Improving the Nation's Cybersecurity (2021 年 5 月 12 日)

Executive Office of The President, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, M-21-31 (2021 年 8 月 27 日)

Executive Office of The President, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, M-22-09 (2022 年 1 月 26 日)

iv NIST Special Publication 800-92, Guide to Computer Security Log Management

v National Security Agency Cybersecurity Report, Hardening SIEM Solutions, A Technical Report from Network Infrastructure Security (2019 年 10 月 29 日)

# 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

| | |
|---|---|
| ユーザ | 1. RADIUS 認証 (1024～49151 のユーザ設定可能な IP ポート番号) |
| | 2. TACACS+ 認証 (1024～49151 のユーザ設定可能な IP ポート番号と標準ポート 49) |
| | 3. LDAP 認証 (ポートのバインディング、LDAP v2 または LDAPv3、最大 5 台の LDAP サーバ) |
| | 4. REST API(全ての呼び出しでユーザ/パスワード認証または有効期限付きのトークンベース認証) |
| | 5. 管理セキュリティ<br>a. ウェブセッション タイムアウト (5/10/15/30/60 分)<br>b. ログイン失敗時のロックアウト (有効/無効)、3～6 回のログイン試行失敗を許可<br>c. ログインバナー(米国政府標準、カスタムバナー) |
| | 6. ユーザ設定<br>a. パスワード : 6～100 文字、大文字と小文字混在、半角英数字、特殊文字<br>b. パスワードの有効期限 : 有効/無効、ユーザ設定の日数<br>c. ユーザの作成/削除 : ユーザ名、パスワード、パスワードを忘れた時の質問、メール |
| | 7. SSH(許可/拒否ユーザ) |
| デバイス | 8. NTPd 対称キー<br>a. 対称セキュリティキーの生成/ダウンロード/アップロード<br>b. SHA1/256/512 キーと MD5 キー |
| | 9. NTPd Autokey サーバ (IFF 識別スキーム) |
| | 10. NTPd Autokey クライアント (IFF 識別スキーム) |
| | 11. HTTPS セキュア管理<br>a. プロトコル : TLS 1.2 および 1.3<br>b. 暗号スイート : SSL_High_Encryption、SSL_High_Medium_Encryption<br>c. セッション タイムアウト 5～1440 分<br>d. 自己署名証明書 : 2048 または 4096 RSA キービット、有効期限 1～1825 日、カスタマイズ可能なローカリティ コード<br>e. CSP(コンテンツ セキュリティ ポリシー) ヘッダ |
| | 12. X.509 証明書/CSR (CSR(証明書署名要求) の作成とダウンロード、2048 または 4096 RSA キービット) |
| | 13. X.509 インストール (複数の CA 署名 X.509 証明書のインストール) |
| | 14. X.509 マッピング<br>a. X.509 CA 署名証明書を HTTPS および/または syslogs にマッピング<br>b. HTTPS および/または syslog に同一または異なる X.509 CA 署名証明書 |
| | 15. X.509 認証局 (または信頼できる CA 証明書ストア)<br>a. 独自 CA 証明書のインストール<br>b. 広範なシステム既定の CA 証明書を含む |
| | 16. ソフトウェア アップグレード<br>a. システム ソフトウェアは Microchip 社お客様ポータルのみで入手可能<br>b. Microchip 社お客様ポータルへのアクセスには認証済みユーザが必要<br>c. システム ソフトウェア ファイルとシリアル番号付き認証ファイルをダウンロードするには認証が必要<br>d. システム ソフトウェア イメージは暗号化済み<br>e. 全てのダウンロードにはファイルの改ざんをクロスチェックするための MD5 および SHA ハッシュ付き<br>f. Microchip 社発行の正当なシリアル番号付き認証ファイルがない場合、ソフトウェアはインストール不可 |
| | 17. アラーム (ユーザ設定可能な豊富なアラーム、トラップ、ログ、メール、ハードウェア リレーによる通知) |
| | 18. タイミング セキュリティ<br>a. BlueSky™ テクノロジによる GNSS の妨害、なりすまし検出と保護<br>b. 代替タイムソース (NTP、PTP、IRIG)<br>c. 妨害防止 GNSS アンテナ<br>d. タイミング ホールドオーバーのための原子時計アップグレード |
| ネットワーク | 19. アクセス制御リスト (LAN ポートごとの独自の IPv4 および IPv6 アクセス制御リスト、合計 8～12 個のリスト) |
| | 20. サービス/システム制御 (HTTPS、SNMP、SSH、ToD、Telnet の有効/無効) |
| | 21. パケット監視<br>a. CPU へのパケットのハードウェア ベースのスロットルによる DoS/DDoS 保護<br>b. LAN ポートごとのパケット スロットル<br>c. パケット受信アラームしきい値を LAN ポートごとにカスタマイズ可能 |
| | 22. 複数の LAN ポートでネットワーク セグメンテーションが可能<br>a. LAN1 のみで管理/タイミングを利用可能<br>b. LAN2-LAN6 はタイミングのみ、管理不可 |
| 分析 | 23. セキュアな Syslog<br>a. X.509 認証<br>b. TLS セキュリティ<br>c. ピア検証<br>d. ユーザ設定可能なポート番号 |
| | 24. SNMPv3<br>a. 認証の暗号化 : MD5、SHA1/224/256/384/512<br>b. プライバシーの暗号化 : AES/128/192/256 |


DS00004549B_JP

MICROCHIP