Cisco Secure Equipment Access

2024 年 2 月

目次

Cisco® Secure Equipment Access を使用すると、事業部門の現場チームは遠隔のオペレーショナルテクノロジー（OT）設備に簡単に接続して、設定、保守、トラブルシューティングを行うことができます。これはシスコの産業用ネットワーク機器で動作するハイブリッド クラウド サービスであり、製造、公共交通、道路インフラ、再生可能エネルギー生産拠点、石油天然ガス、水道、EV 充電器などの現場環境で、ゼロ トラスト ネットワーク アクセス（ZTNA）アーキテクチャを実現します。

製品の概要

リモートアクセスは、事業部門、保守請負業者、および機械メーカーが、時間とコストのかかる現場への訪問を行わずに OT 設備を管理およびトラブルシューティングするための鍵です。ゼロ トラスト ネットワーク アクセス（ZTNA）ソリューションは、アンマネージド セルラー ゲートウェイや常時接続 VPN の代替となり、組織がセキュアなリモートアクセスを展開してサイバーリスクを軽減するために役立つものとして、勢いを増しています。

Secure Equipment Access（SEA）により、シスコは ZTNA のすべての利点を事業領域にもたらします。リモートユーザーはクラウドポータルに接続し、ここで認証されて、選択されたデバイスにのみ、指定されたプロトコルのみを使用して、許可された日時にのみアクセスできるようになります。既定動作で拒否する態勢から開始され、その時点で必要となる適切な信頼が適応的に提供されます。設備は探索から隠され、ラテラルムーブメントは不可能になっています。

Cisco SEA ポータルは ZTNA トラストブローカとして機能し、アイデンティティとコンテキストに基づいてポリシーを適用し、シスコの産業用スイッチおよびルータで実行されている SEA アプリケーションと連携して動作して、産業用ネットワーク機器を OT 設備との通信の確立を担当する ZTNA ゲートウェイに変えます。

ZTNA ゲートウェイ機能をシスコの産業用スイッチおよびルータに組み込むことで、ネットワークアドレス変換（NAT）の境界の背後にあるものも含めて、すべての設備へのリモートアクセスが容易になり、大規模な展開が簡素化されます。調達、設置、および管理する専用のハードウェアはありません。複雑な産業用 DMZ（iDMZ）ファイアウォールルールを設定する必要はありません。リモートアクセスを有効化するには、シスコの産業用ネットワーク機器でソフトウェア機能を有効にするだけです。

機能と利点

表 1. 機能と利点

機能	利点
OT ワークフロー向けに設計されたリモートアクセス	• 機械メーカー、産業用制御システム（ICS）ベンダー、保守請負業者、および事業部門自身が、設定、保守、またはトラブルシューティングのために遠隔の事業用設備にアクセスできるようにします。 • 業務責任者がベンダー接続用のログイン情報を簡単に作成して、業務の俊敏性や生産稼働時間に影響を与える可能性のある遅延を回避できるようにします。
最小権限アクセス制御	• ネットワーク全体へのアクセスは、誰にも許可されません。リモートアクセスは既定の動作で拒否されます。管理者は、アイデンティティとコンテキストに基づいてポリシーを定義する必要があります。 ◦ アイデンティティ：アクセス試行のたびにユーザーとデバイスのアイデンティティを確認して、ポリシーに準拠したデバイスからの、信頼できるユーザーにのみ、必要な設備のみへのアクセスが許可されるようにします。 ◦ スケジュール：リモートユーザーが、いつでもは接続できないようにします。各設備と各ユーザーの日時スケジュールを設定することで、必要なときに指定された期間のみアクセスを許可します。 ◦ アクセス方式：リモートオペレータは、選択されたプロトコル（セキュアシェル（SSH）、Remote Desktop Protocol（RDP）、Virtual Network Computing（VNC）、HTTP(S)、Telnet、または UDP、TCP、ICMP ベースのアプリケーション）以外を使用できなくなります。 • ユーザーアイデンティティ、遠隔設備、スケジュール、およびアクセス方式を組み合わせたアクセスグループを作成することで、大規模なポリシーの管理が容易になります。
セキュア認証	• 多要素認証（MFA）を適用することで、盗まれたログイン情報のリスクに対処します。 • アイデンティティ プロバイダー（IDP）を使用してシングルサインオン（SSO）とセキュリティ アサーション マークアップ言語（SAML）2.0 の統合を有効にすることで、ユーザー体験を合理化し、一元化された場所から厳格なユーザーポリシーを適用します。
デバイスポスチャチェック	• リモートユーザーが設備へのフル IP アクセスを必要とする場合、Cisco Duo を使用してリモートユーザーのセキュリティ態勢を評価します。 • 最新のオペレーティングシステムやマルウェア防御ソフトウェアがインストール・有効化されているなど、セキュリティポリシーに準拠しているリモートコンピュータにのみアクセスを許可します。
リモートアクセスセッションの完全な制御	• セッション監視：すべての稼働中のリモートアクセスセッションのリストが表示され、制御またはトレーニングの目的で、セッションに参加してリモートユーザーが行っていることをリアルタイムに表示できます。 • セッションの強制終了：管理者は、そもそも稼働してはならないにも関わらず稼働しているセッション、またはリモートユーザーが許可された行動から逸脱したセッションを強制終了できます。 • セッションの記録：インラインセッション記録をオンにして、監査証跡で使用するためセッションを保存します。必要に応じて、過去にさかのぼってリモートユーザーがシステムに対して行ったことを確認し、インシデントの調査を支援します。
リモート アクセス ダッシュボード	• リモート アクセス インフラストラクチャを単一の視点で簡単に監視し、セッション数、セッション種別、データ使用量、設備の正常性などの主要なデータポイントを強調表示します。
ガイド付き設定	• フローベースのユーザーインターフェイスにより、初めてのユーザーまたは IT 担当者ではないユーザーでも、リモートアクセスを簡単に設定し、目標を達成できます。上級ユーザーは、詳細メニューにもアクセスできます。

機能	利点
クラウドベースの ZTNA ブローカ	• すべてのサイトでセキュアなリモートアクセスを迅速に稼働させます。複雑なサーバーの設置、設定、およびメンテナンスは必要ありません。Cisco SEA は、分散インフラストラクチャ全体のすべてのネットワーク接続された設備に到達でき、ニーズに合わせて拡張できる Software-as-a-Service（SaaS）ソリューションです。 • 攻撃対象領域を縮小します。ネットワークへの入り口が、攻撃者にとっては動く標的となります。 • 業務管理者が、すべてのサイトに対して単一のポータルを使用して、リモートアクセスを簡単に設定できるようにします。
シスコの産業用スイッチおよびルータに組み込まれた ZTNA ゲートウェイ	• セキュアなリモートアクセスを大規模に簡単に展開できます。Cisco SEA により、すべてのサイトで専用の ZTNA ゲートウェイハードウェアを調達、設置、および管理する必要がなくなります。 • より多くの設備に到達できるようになり、NAT 境界の背後にある設備にも到達できます。同じサブネット内のスイッチまたはルータは、NAT 戦略に関係なく、これらの設備へのゼロ トラスト リモート アクセスも提供するようになります。 • 完全な分離を適用します。設備が踏み台ホストとして使用されている場合、同じスイッチまたはルータでマイクロセグメンテーション ポリシーを適用して、ラテラルムーブメントを防ぐこともできます。 • 攻撃対象領域を縮小します。iDMZ 内の踏み台サーバーに IP アドレスを公開する必要はありません。 • 複雑なファイアウォールと iDMZ の設定に苦労せずに済みます。Cisco ZTNA ゲートウェイは、Cisco ZTNA トラストブローカへのアウトバウンド接続を確立して、リモートアクセスを提供するすべての OT 設備へのセキュアで制御された通信パスを作成します。
クライアントレスおよびエージェントベースの ZTNA	• クライアントレス：ユーザーが、RDP、VNC、HTTP(S)、SSH、または Telnet を使用してリモート OT 設備にアクセスするのに必要なのは、Web ブラウザのみです。 • エージェントベース（SEA Plus）：Cisco SEA は、ユーザーのコンピュータと OT 設備の間にセキュアな IP 通信チャネルを確立するため、ネイティブアプリケーションを使用したファイル転送やプログラマブル ロジック コントローラ（PLC）のプログラミングなどの高度なタスクのために、任意のデスクトップ アプリケーションを使用できます。
Role Based Access Control（RBAC）	• セキュリティを損なうことなく、リモートアクセス管理を簡単に委任できます。管理者は RBAC を使用して、リモートアクセスポリシーの作成時にユーザーが設定できる内容を制限できます。 • 特定のニーズに合わせてカスタムユーザーロールを作成するか、3 つの事前定義されたロールから選択します。
監査およびコンプライアンス情報	• コンプライアンス要件を満たし、システム生成イベントとユーザー生成イベントの両方の監査ログによる調査の実行を支援します（ユーザー名、時間、デバイスポスチャ、およびアクセスログによる、新しいユーザーまたは新しい設備をシステムに追加したユーザーや、リモートユーザーの認証方法の調査など）。 • 詳細なセッションログは、ユーザーインターフェイスを介して使用することも、CSV ファイルとしてエクスポートして、レポートに入力したり、コンプライアンスプロセスに対応させたりすることもできます。
プロセス自動化のためのプログラマビリティ	• Cisco SEA API は Swagger ユーザーインターフェイスで使用でき、リモートアクセスを保護するためのプログラムによるアプローチを実装することを希望するお客様やパートナーのカスタム自動化の開発を簡素化します。

プラットフォームのサポート

Cisco Secure Equipment Access は、クラウドベースの ZTNA ブローカとリモート OT 設備の間にセキュアで制御された通信パスを確立するために、シスコの産業用スイッチまたはルータで実行される複数の ZTNA ゲートウェイで構成される独自のアーキテクチャに基づいて構築されています。SEA ZTNA ブローカは、無制限の数の ZTNA ゲートウェイをサポートしています。

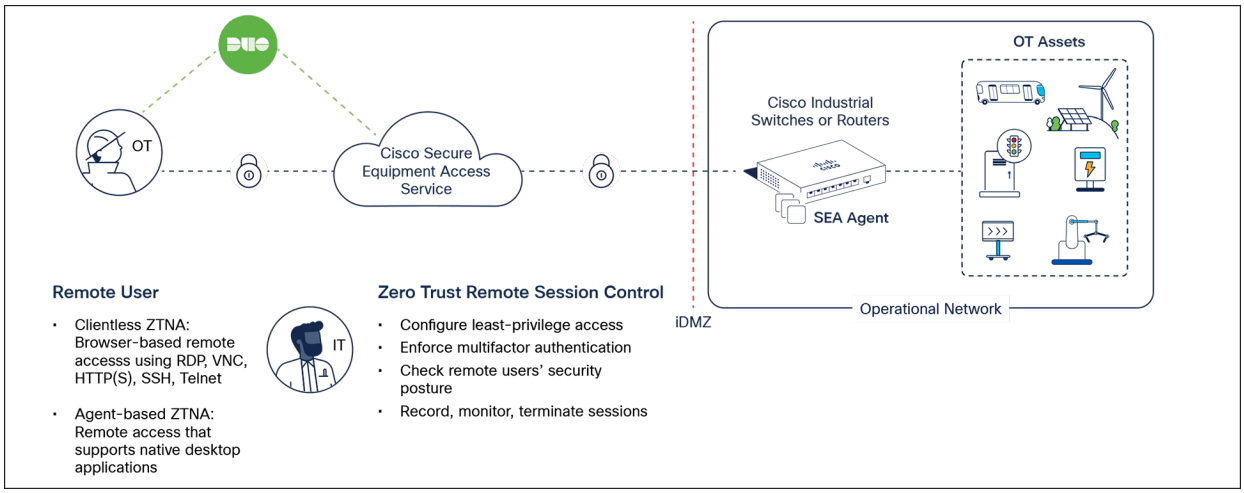

図 1.
Cisco Secure Equipment Access の ZTNA アーキテクチャ

ZTNA ゲートウェイ機能は、ルーティングまたはスイッチングのパフォーマンスやその他の機能に影響を与えることなく、ネットワーク機器の専用 CPU コアで実行される Cisco IOx アプリケーションである Cisco SEA エージェントによって有効になります。Cisco SEA エージェントは次の表に示すプラットフォームでサポートされています。

表 2. Cisco SEA エージェントをホスティングしているプラットフォーム

製品のタイプ	サポートされるプラットフォーム
産業用スイッチ	Cisco Catalyst® IE3300 高耐久性シリーズ スイッチ（4 GB RAM 搭載モデルのみ） Cisco Catalyst IE3400 高耐久性シリーズ スイッチ Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチ Cisco Catalyst IE3100 高耐久性シリーズ スイッチ
産業用ルータ	Cisco Catalyst IR1100 高耐久性シリーズ ルータ Cisco Catalyst IR1800 高耐久性シリーズ ルータ

Cisco SEA ZTNA ゲートウェイのハードウェア仕様

ハードウェアの仕様については、関連するデータシートを参照してください。

- Cisco Catalyst IE3300 高耐久性シリーズ スイッチ
- Cisco Catalyst IE3400 高耐久性シリーズ スイッチ
- Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチ
- Cisco Catalyst IE3100 高耐久性シリーズ スイッチ
- Cisco Catalyst IR1100 高耐久性シリーズ ルータ
- Cisco Catalyst IR1800 高耐久性シリーズ ルータ

表 3. Cisco SEA プラットフォームの仕様

プラットフォーム	同時リモートアクセスセッションの最大数	Cisco IOS の最小バージョン	Cisco IOS の推奨バージョン
Cisco Catalyst IE3300 高耐久性シリーズ スイッチ	10	17.12.01	17.13.01
Cisco Catalyst IE3400 高耐久性シリーズ スイッチ	10	17.12.01	17.13.01
Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチ	10	17.12.01	17.13.01
Cisco Catalyst IE3100 高耐久性シリーズ スイッチ	5	17.12.01	17.13.01
Cisco Catalyst IR1100 高耐久性シリーズ ルータ	10	17.04.01	17.13.01a
Cisco Catalyst IR1800 高耐久性シリーズ ルータ	10	17.11.01	17.13.01a

注： SEA エージェントがデバイスにインストールされている唯一のアプリケーションである場合に適用可能な同時セッションの最大数が提供されています。複数の同時 SEA セッションを使用する場合は、使用可能なアップリンク帯域幅を慎重に考慮する必要があります。

ライセンス

Cisco Secure Equipment Access は、アクセス可能な OT 設備またはエンドポイントの数に基づいた定期的なサブスクリプションモデルを使用してライセンスが供与され、1 年、3 年、5 年、および 7 年の期間で利用できます。各 SEA ライセンスには、遠隔設備にアクセスするための 1 Gbps/月/エンドポイントが付属しています。組織内のライセンスとトラフィックの許容量は、クラウド内のプールと見なされます。このようなプールは、すべてのターゲットサイトと OT 設備の任意の分散モデルで使用できます。ライセンスは、特定の要件を満たすためのさまざまなレベルの機能を提供する 2 つの階層（Essentials と Advantage）で使用できます。この製品は、Cisco Smart Licensing を使用します。SEA ライセンスには、SEA クラウドポータルと、無制限の数の ZTNA ゲートウェイの展開を可能にする無制限の数の SEA エージェントが含まれています。

表 4. ライセンス階層

ライセンス階層	
Essentials	**メリット**
• すべてのアクセス方式： ◦ クライアントレス ZTNA（RDP、VNC、HTTP/S、SSH、Telnet） ◦ エージェントベースの ZTNA（SEA Plus） • ジャストインタイムのアクセス（スケジュールされたアクセス） • アクセス制御グループ • プラットフォームレベルのセキュリティ管理（SSO、MFA、RBAC）	• Essential 機能の他以下を搭載 • アクティブセッションの監視 • セッションの指揮（セッション参加） • セッションの強制終了 • インライン セッション レコーディング（ストレージには AWS S3 アカウントが必要） • SEA Plus アクセス方式を使用する場合の追加のセキュリティのための、Cisco Duo を介したホストのセキュリティ態勢チェック（Duo アカウントが必要）

Secure Equipment Access ライセンスには、Basic ソフトウェアのサポートが付属しています。利用可能なすべてのソフトウェアサポートレベルの詳細については、こちらを参照してください。

発注情報

Cisco Secure Equipment Access は、本日注文することができます。詳細については、シスコの購入案内のページを参照してください。

表 5. Cisco SEA 製品 ID

製品 ID	製品の説明
SEA-LICENSE	ATO 製品 ID
SEA-E	OT 設備用 Cisco Secure Equipment Access **Essentials** ライセンス
SEA-A	OT 設備用 Cisco Secure Equipment Access **Advantage** ライセンス

保証

保証情報については、Cisco SEA エージェントを実行しているハードウェア プラットフォームのそれぞれのデータシートを参照してください。

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用、拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを次の表に示します。

表 6. 固有の環境保全に関するトピックへの参照リンク

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

シスコおよびパートナーの提供サービス

計画、展開、およびサポートのためのサービス

シスコとシスコの認定パートナーが提供するサービスは、お客様の Cisco SEA プロジェクトの設計、展開、運用の各フェーズでご利用いただけます。必要とされているのがエキスパートのアドバイスでもプロジェクト全体のサポートでもその間の何らかのサポートでも、シスコはパートナーとともにお客様の成功を支援するエキスパートと専門知識を提供できます。詳細については、https://www.cisco.com/go/services [英語] を参照してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
ドキュメントの作成		2023 年 10 月 16 日
新しいプラットフォームの新機能とサポート	表 1、2、および 3	2024 年 1 月

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-3966856-01 02/23