SECOMEA データシート

OTに最適化されたセキュアなリモートアクセス

接続性、自動化、インダストリー4.0技術などの進化により、産業分野の生産性や業務効率は大幅に向上しています。

しかし、従来のリモートアクセスツールでは、重要な産業オペレーションを保護するために必要な高度な制御、可視性、セキュリティを十分に確保することができません。

攻撃対象領域の拡大、脅威の巧妙化、規制の厳格化に伴い、IT向けに設計された旧来型ソリューションでは、進化するOTの要件に対応しきれなくなっています。

現代のOT向けセキュアリモートアクセスには、生産性の向上、複雑さの軽減、そして法規制への確実な対応が求められます。

主な課題

平均復旧時間（MTTR）の短縮
効率性および生産性の指標向上、突発的なダウンタイムの削減

サイバーリスクの深刻化
攻撃対象領域の拡大、頻発・巧妙化するサイバー攻撃

IT向けシステムの限界
VPN、VDI、ジャンプサーバー、PAMソリューションでは、OT特有のニーズに対応できない

コンプライアンス要件の厳格化
重要なオペレーションのセキュリティ強化を求める規制圧力の強まり

Secomeaのソリューション

Secomeaのセキュアリモートアクセスソリューションは、リモートアクセスの煩雑さを解消しつつ、セキュリティと制御を強化し、運用効率の向上と、社内・社外ユーザー双方のUX改善を実現します。

セキュリティ	OT／ICS環境に特化した設計	Secomeaのセキュアリモートアクセスソリューションは、複雑な運用技術（OT）および産業用制御システム（ICS）環境に特有の要件に対応するよう設計されています。
	アーキテクチャに最適化されたセキュリティ	Secomeaは、ゼロトラストモデルや多層防御といった業界のベストプラクティスを取り入れ、Purdueモデルなどの既存インフラに統合することで、サイバーフィジカルシステム（CPS）を保護します。
	規制要件への確実な対応	SecomeaはIEC 62443-4-1の認証を取得しており、IEC 62443-4-2およびIEC 62443-3-3にも準拠しています。 Secomeaのソリューションは、法的要件への対応とコンプライアンス違反リスクの低減を目的とした機能を備えています。
制御	シンプルなユーザーアクセス管理	直感的に操作できるアクセス管理サーバーを活用して、ユーザー権限の作成・付与・管理を行うことで、認証管理プロセスを効率化し、運用負荷を軽減します。
	不正アクセスリスクの低減	SSO（Azure AD、Oktaなど）によってユーザーを安全に認証し、最小権限の原則に基づいて許可された機器のみに接続を制限。ネットワーク内外への脅威拡散を防ぐために、横移動を抑制します。
	継続的な監視と管理	リモートアクセスのすべての活動を可視化・制御。現在の接続状況を一目で把握でき、ユーザーごとの操作履歴を記録したアクセス監査ログや、インシデントやコンプライアンスへの対応に活用できるセッション録画も確認できます。
効率	短時間で導入可能	OTに特化し、インフラを選ばない設計のSecomeaは、あらゆる運用環境にスムーズかつ迅速に導入でき、長時間のトレーニングなしですぐに使い始めることができます。
	応答時間の最適化	Secomeaの柔軟なソリューションは、場所を問わず、レイテンシの高い環境でも、安定したパフォーマンスと、ビジネスクリティカルな機器へのシームレスなアクセスを実現します。また、データに基づく予知保全により、ダウンタイムを未然に防ぎます。
	柔軟性の高いリモートアクセス	Secomeaは、幅広いリモートアクセス手段に対応しています。たとえば、Modbus、Profinet、Ethernet/IPなど機器固有のプロトコルを使用し、ポート443経由のVPNトンネリングによる直接アクセスが可能である一方、RDP、VNC、SSH、Telnetを利用したクライアントレスの間接アクセスにも対応しています。

クラウドベースソリューションのメリット

即時バージョンアップに対応：

新たなアップデートが利用可能になり次第、即座に適用されるため、拠点ごとに展開スケジュールを調整する煩雑さを解消し、運用を効率化します。

強固なサイバーセキュリティ：

ゼロトラストモデル、多層防御、Purdueモデルに基づくセキュリティバイデザインを採用。ソリューションはIEC 62443-4-1の認証を取得し、IEC 62443-4-2およびIEC 62443-3-3に準拠。また、組織としてのセキュリティ対策はISO 27002に基づいており、ISAE 3402報告書により保証されています。

スムーズな導入：

インフラに依存しないクラウドベースのソリューションにより、現地での設置が不要。関連するインフラ管理の負担が軽減され、TCO（総保有コスト）の削減につながります。

暗号化とネットワーク分離

TLS 1.2 & AES256

CIA三原則に基づくセキュリティと第三者認証

Secomeaの暗号化方式は、x.509証明書（1024ビット鍵）とAES256を用いたTLS 1.2接続に基づいており、CIA三原則（機密性・完全性・真正性）に沿って設計されています。

AES256による暗号化は、データを不正アクセスから保護し、機密性を確保します。x.509証明書とTLS 1.2プロトコルは、通信中の改ざんや破損を防ぎ、完全性を保証します。さらに、TLSとx.509証明書によって構成される堅牢な認証フレームワークが真正性を担保し、通信相手の正当性を検証することで、未承認のアクセスを防ぎます。

TRUST ON FIRST USE

MitM（中間者）攻撃に対する保護

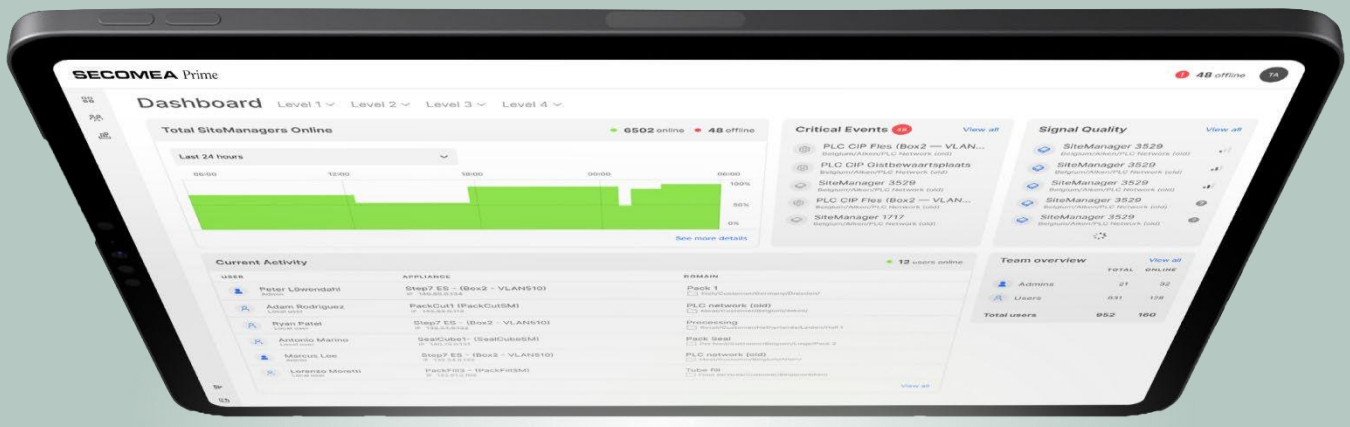
Secomeaは、TLSを基盤としたAES 256ビット暗号化トンネルを通じて機器を安全に接続します。物理制御用のI/Oポートを活用することで、リモートでも現場でも、各デバイスのIPアドレスやポート単位で接続を細かく制御できます。

Secomeaの各Access Managementサーバーには固有のTLS証明書／鍵が割り当てられており、ゲートウェイは初回接続時にその証明書に紐づけられます。これがいわゆるTrust-on-first- use（ ToFu、初回接続時の信頼）です 。以降の接続では、常にこの証明書に基づいて検証が行われます。ゲートウェイが信頼するサーバーを変更するには、Access Managementサーバーを手動で再設定する必要があります。攻撃者がこれを傍受のみで実行することはできません。手動での再設定を要件とすることで、不正な接続先への誘導を防止しています。

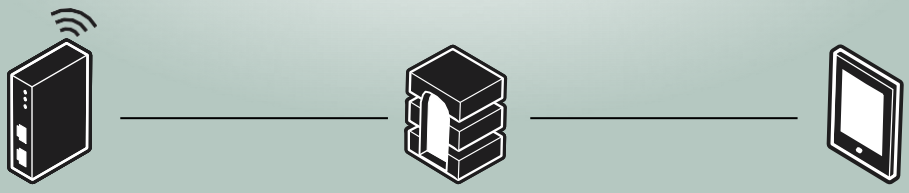
Secomeaのアーキテクチャ

製造業や重要インフラセクター向けに特化した設計により、Secomeaはサイバーリスクを低減し、事業継続性を高めるとともに、重要なCPSプロセスを保護します。

このソリューションには、遠隔でのプログラミングやトラブルシューティング、データに基づく意思決定まで、リモートアクセスやリモート保守に必要なソフトウェアとハードウェアがすべて含まれています。OT環境にふさわしい高度なセキュリティのもと、ユーザーアクセスの管理、リモートセッションのリアルタイム制御、機器データの収集が可能です。



SECOMEA Prime



IIoT Gateway

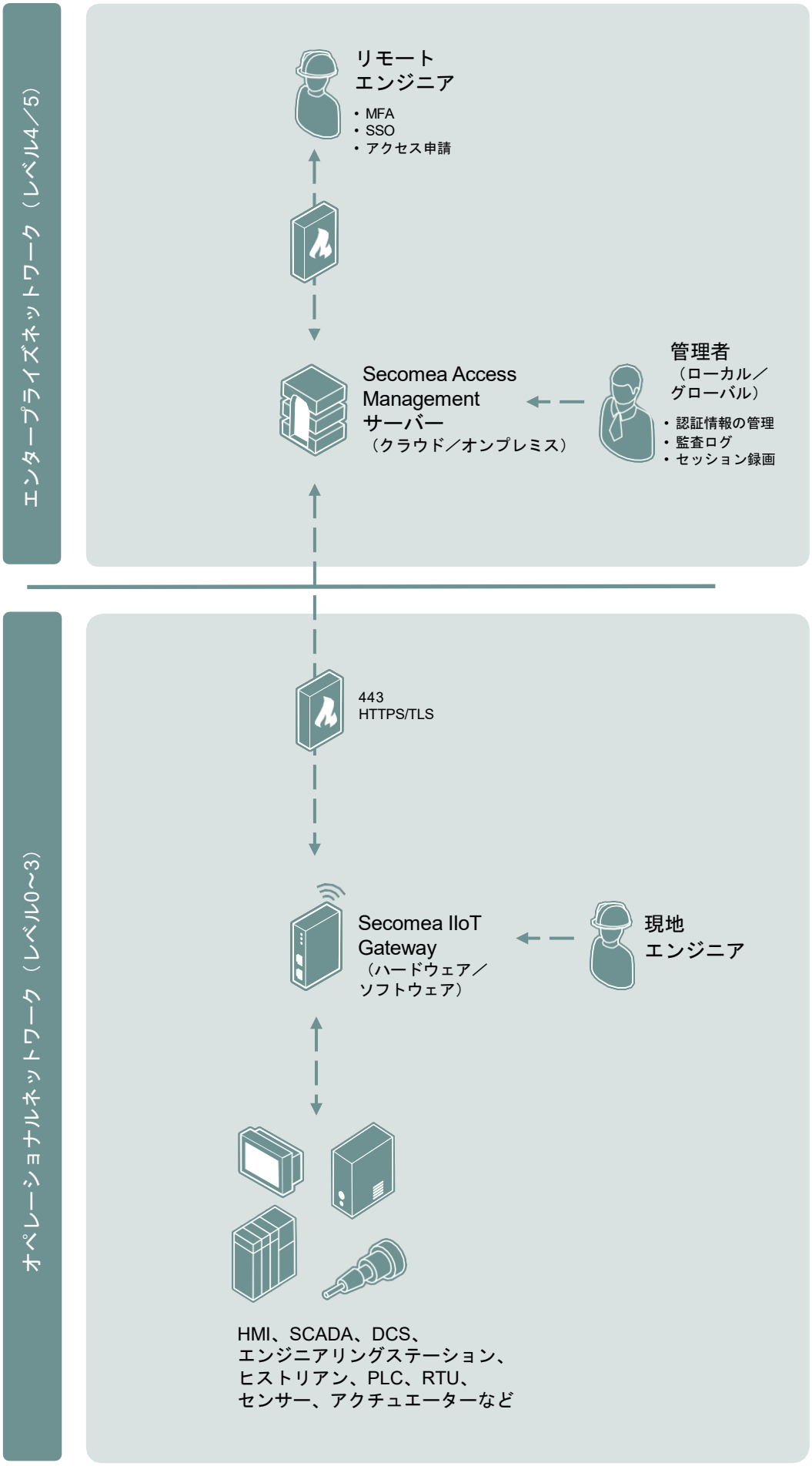
セキュアなリモートアクセスとデータ収集を実現する、プラグアンドプレイ対応の産業用IoTゲートウェイ（ハードウェアまたはソフトウェア）

Access Management サーバー

ユーザーのアクセス管理と監査を統合的に行う、一元型のIndustrial Access Managementサーバーおよびm2mサーバー

リモートアクセス

あらゆる場所、あらゆるデバイスからの接続を可能にする、ダイレクトまたはクライアントレス方式の多様なリモートアクセスオプション


エンタープライズネットワーク（レベル4／5）
リモート
エンジニア
• MFA
• SSO
• アクセス申請
Secomea Access
Management
サーバー
（クラウド／オンプレミス）
管理者
（ローカル／
グローバル）
• 認証情報の管理
• 監査ログ
• セッション録画
オペレーショナルネットワーク（レベル0～3）
443
HTTPS/TLS
Secomea IIoT
Gateway
（ハードウェア／
ソフトウェア）
現地
エンジニア
HMI、SCADA、DCS、
エンジニアリングステーション、
ヒストリアン、PLC、RTU、
センサー、アクチュエーターなど

Secomeaの機能と特長

アイデンティティおよびアクセス管理	特権アクセス管理	最小権限の原則に基づいた階層型ユーザーロールの設定
	きめ細かなアクセスコントロール	細かな権限設定が可能な個別レベルのアクセス制御
	高度なグルーピング	ユーザー権限の一括管理
	ジャストインタイム（JIT）アクセス	特定の機器への一時的または予定されたアクセス権の付与
	常時接続アクセス	2つの異なるネットワーク間で静的かつ永続的なトンネル接続の設定
	アクセス申請	ユーザーによる特定機器へのアクセスリクエスト、管理者によるワンクリックでの承認
	多要素認証（MFA）	SMS認証を用いたMFAによるユーザー認証
	シングルサインオン（SSO）	Azure ADまたはOktaを使用したシングルサインオン（SSO）によるユーザー認証のセキュリティ強化
リモートアクセス	エージェントレスのウェブベースシステム	ブラウザから直接Secomeaを使用 – プラグインやアプリケーションのインストールが不要
	軽量クライアントによる直接アクセス	Modbus、Profinet、EtherCAT、Ethernet/IPなどのOTプロトコルに対応
	間接的なクライアントレスアクセス	RDP、VNC、SSH、Telnet、HTTPSを使用したブラウザからのリモートアクセスに対応
	安全なファイル転送	リモートで転送されたファイルのウイルスやマルウェアをスキャンし、安全性を評価
監査およびモニタリング	リアルタイムの活動監視	Prime Dashboardから進行中のリモートアクセスセッションの概要を確認
	監査ログ	機器上で行われたすべての活動を追跡し、誰が何をいつ行ったかを記録
	セッション録画	リモートアクセスセッションの動画をキャプチャし、トラブルシューティングや監査に使用
	アラートと自動化アクション	特定のイベントに対してSMS/email通知を受け取り、トリガーされたアクションを自動的に実行
	アクセスゲートウェイ情報	すべてのゲートウェイの概要を一元的に確認し、詳細情報（シリアル番号、IP、ファームウェア、最終ハートビート）を表示。運用を効率化するために、物理的な位置情報や連絡先情報も登録
	脆弱性ハブ	最新のファームウェアバージョンが適用されていないゲートウェイや、サポート終了またはEOLに近いゲートウェイを特定し、タイムリーなアップデートや交換を確実に実施
カスタマイズおよび統合	API アクセス	Secomeaを、運用に使用している他のツールと統合
	AD統合	Microsoft Azure Active Directoryで実施された変更を、Secomeaのアクセス管理サーバーと毎時同期
	セキュリティ情報およびイベント管理（SIEM）統合	SIEMシステム（Syslog、Splunkなど）をSecomeaと統合
	データ収集モジュール（DCM）およびクラウド統合	産業機器からのデータ収集（OPC UA、Modbus TCP、Siemens S7、Ethernet/IP、MQTTなどのネイティブプロトコルを使用）。さらなる処理のために、選択したクラウドソリューション（Microsoft Azure IoT Hub、Amazon AWS IoT Core、Software AG Cumulocity IoT、Aveva Insight、MQTTデータサーバーなど）への送信
	サポートシステム統合	サポートシステムをSecomeaと統合し、チケット管理を一元化
	ブランディング	URLおよびログインページをカスタマイズし、企業のブランディングに合わせる