SIEMENS

産業セキュリティ

ネットワークセキュリティ

siemens.com/networksecurity

ブローシャー

エディション
2018 年 4 月

インターネットはビジネスプロセスの極めて重要なアクセラレーターとして貢献しており、世界中の営業プロセスを改革しています。
これによってもたらされた製造産業における変化は、第 4 次産業革命とも呼ぶことができます。Industrie 4.0 は、産業のバリューチェーンの側面すべてに影響を及ぼしており、産業用通信やセキュリティといった重要な分野も例外ではありません。

ここで鍵となるのは、デジタル化や、拡大を続ける設備およびプラントのネットワーク接続において、データセキュリティを常に考慮するということです。そのため、産業のニーズに細やかに対応したデジタルセキュリティソリューションを使用することが根本的に重要であり、産業用通信と密接に結び付ける必要があります。

サイバーセキュリティについても、収束ネットワーク数の増加と共にますます重要性を増しています。サイバーセキュリティは長らく標準化が試行されており、国際委員会がサイバーセキュリティに関する統一規格の仕様を決定し、開発することを保証しています。
さらに現在では、特に増加するセキュリティ要件を満たすため、重要なインフラを対象とした法令によってセキュリティが規制されています。ドイツの IT セキュリティ法、フランスの ANSSI 認証、米国の NERC CIP、または IEC 62443-4-1 に基づいた TÜV SÜD 認証などがその例です。つまり、オープンな通信や生産システムのネットワーク接続の拡大は、大きなビジネスチャンスと同時に高いリスクも生み出しているということです。攻撃に対する包括的なセキュリティを産業用プラントに提供するには、適切な対策をとる必要があります。
シーメンスは産業セキュリティ用の統合ポートフォリオの一部としてこれらの対策を用意し、目的に合わせて実施することでお客様をサポートします。

目次

産業セキュリティ

産業セキュリティが重要な理由

No.	脅威	説明
1	ソーシャルエンジニアリングおよびフィッシング	ソーシャルエンジニアリングとは、多くの場合に技術的な方法ではなく、好意、信頼、恐れ、または権力に対する服従といった人間の特性を利用して情報や IT システムへの不正なアクセスを行う方法です。詐欺メール（フィッシングメール）がこの例です。詐欺メールは、従業員にマルウェアを含む添付ファイルを開かせようとしたり、不正なサイトへのリンクを含んでいたりします。
2	リムーバブルメディアや外部ハードウェア経由でのマルウェアの導入	USB スティックなどのリムーバブルメディアは、気づかずにマルウェアに感染することがあります。他の企業で使用されていた可能性がある外部データやメンテナンスソフトウェアが格納されたノートパソコンを使用することも危険です。
3	インターネットやイントラネット経由でのマルウェアへの感染	オペレーティングシステム、Web サーバー、およびデータベースといった一般的な IT の構成要素は、攻撃者に利用されかねないエラーや脆弱性を含んでいる可能性があります。
4	リモートメンテナンスアクセス経由での侵入	メンテナンス目的での ICS（産業用制御システム）への外部アクセスが、広く使用されています。メンテナンスのために 1 つのシステムにアクセスすると他のシステムにも容易に到達可能となるため、認証や承認の欠落、およびフラットなネットワーク階層がセキュリティの問題の原因となることがあります。
5	ヒューマンエラーおよび破壊工作	ICS 環境で働く作業員は、セキュリティに関して特別なポジションに就いています。これは、メンテナンスや設置作業に携わる企業の社員と外部作業員の両方に当てはまります。セキュリティは決して技術的な対策のみで保障されるものではなく、組織としての規定も必要となります。
6	インターネットに接続されている制御コンポーネント	プログラマブルロジックコントローラーなどのセキュアでない ICS コンポーネントが、製造元の推奨事項に反して十分なセキュリティ対策がなされずに、インターネットに直接接続されることはセキュリティ上のリスクです。
7	技術的な誤作動および不可抗力	過酷な環境の影響や技術的な欠陥による障害が発生する可能性は十分に考えられます。この場合、障害のリスクや可能性を低減させることしかできません。
8	エクストラネットおよびクラウドコンポーネントの制限	ICS においては、従来の IT から IT コンポーネントのアウトソーシングへという傾向が強まっています。たとえば、リモートメンテナンスソリューションのプロバイダーはクラウド内にリモートアクセス用のクライアントシステムを設置しますが、これらのコンポーネントのセキュリティに対してシステム所有者ができる制御は大幅に制限されます。
9	（D）DoS 攻撃	（分散型）サービス妨害攻撃は、ネットワーク接続や必要なリソースの妨害に使用され、ICS の機能が妨害されるなど、システムのクラッシュの原因となることがあります。
10	製造環境におけるスマートフォンの不正アクセス	スマートフォンやタブレット上で動作パラメーターや製造パラメーターを表示し、変更できる機能が、多くの ICS コンポーネントで使用されるようになっています。これにより、特殊なリモートメンテナンスアクセスが可能になり、スマートフォンを使用することで新たな攻撃対象が生み出されます。

脅威の概要

出典：
Industrial Control System Security: Top 10 Threats and Countermeasures Version 1.20
発行日：2016 年 8 月 1 日
注記：
この脅威のリストは、BSI（ドイツの連邦情報技術安全局）および業界を代表する企業が綿密に協力して作成しました。BSI の分析を使用し、連邦情報技術安全局（BSI）は統計やサイバーセキュリティを扱った最新情報のレポートを発行しています。コメントやメッセージは、すべて以下のアドレス宛てにお送りください。
cs-info@bsi.bund.de

多層防御

シーメンスの産業セキュリティコンセプトの核心部としてのネットワークセキュリティ

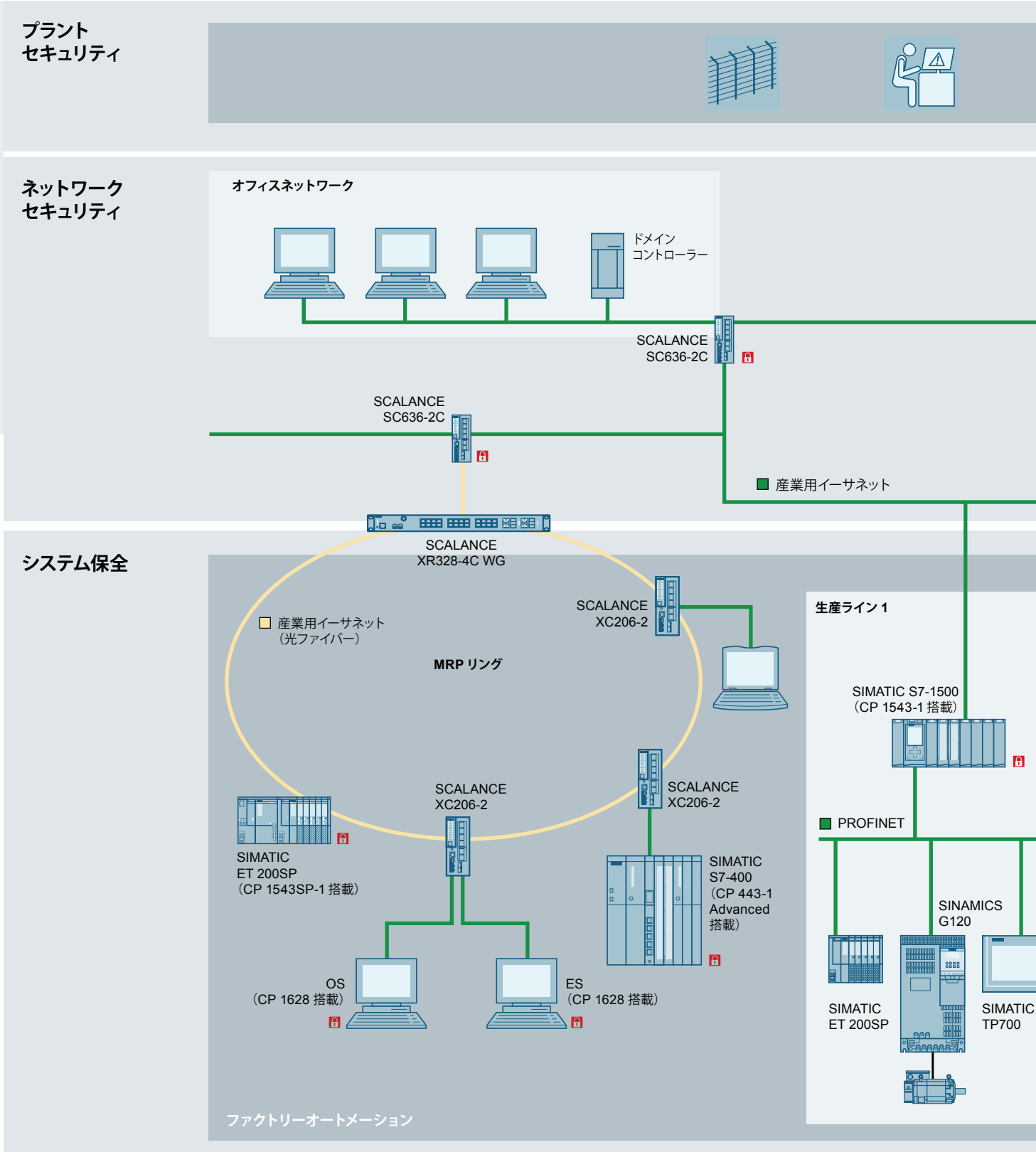
シーメンスは多層防御の考え方に基づいて、多角的で多層的なセキュリティを提供しています。このコンセプトはプラントセキュリティ、ネットワークセキュリティ、およびシステム保全に基づいており、産業用オートメーションのセキュリティの中心的な規格である IEC 62443 の推奨事項に準拠しています。

プラントセキュリティ
プラントセキュリティでは、権限のない人が重要なコンポーネントに物理的にアクセスすることを防止するため多数の異なる方法を使用します。これらの方法は、従来の建物へのアクセス制限から、キーカードによる機密領域の保護まで多岐にわたります。包括的なセキュリティモニタリングにより、生産施設のセキュリティ状態の透明性が高まります。継続的な分析や既存データの相関関係、産業セキュリティモニタリングと脅威インテリジェンス情報の照合などによって、セキュリティ関連のイベントを検出し、リスク要因に応じて分類することが可能です。これに基づき、プラントの所有者は生産施設における現在のセキュリティ状態の概要をステータスレポートの形式で取得し、脅威に対して迅速に対応することが可能になります。

ネットワークセキュリティ
ネットワークセキュリティは、不正アクセスからのオートメーションネットワークの保護を意味し、オフィスとプラントネットワーク間のインターフェースや、インターネットへのリモートメンテナンスアクセスといったすべてのインターフェースのモニタリングが含まれます。これはファイアウォールや、可能な場合はセキュアかつ保護された「非武装地帯」（DMZ）の構築によって実現が可能です。DMZ は、オートメーションネットワーク自体への直接アクセスを許可せずに、他のネットワークからのデータを利用するために使用されます。セキュリティを考慮して、プラントネットワークを個別に保護されたオートメーションセルにセグメント化することでリスクが低減し、セキュリティが強化されます。セル分割およびデバイス割り当ては、通信や保護の要件に基づいて行われます。データ転送は仮想プライベートネットワーク（VPN）を使用して暗号化できるため、データの諜報や改ざんを防止します。通信ノードはセキュアに認証されます。オートメーションネットワーク、オートメーションシステム、および産業用通信は、SCALANCE S 産業セキュリティ機器、SCALANCE M 産業用通信モデム、および SIMATIC 用セキュリティ通信プロセッサーによってセキュリティを強化できます。

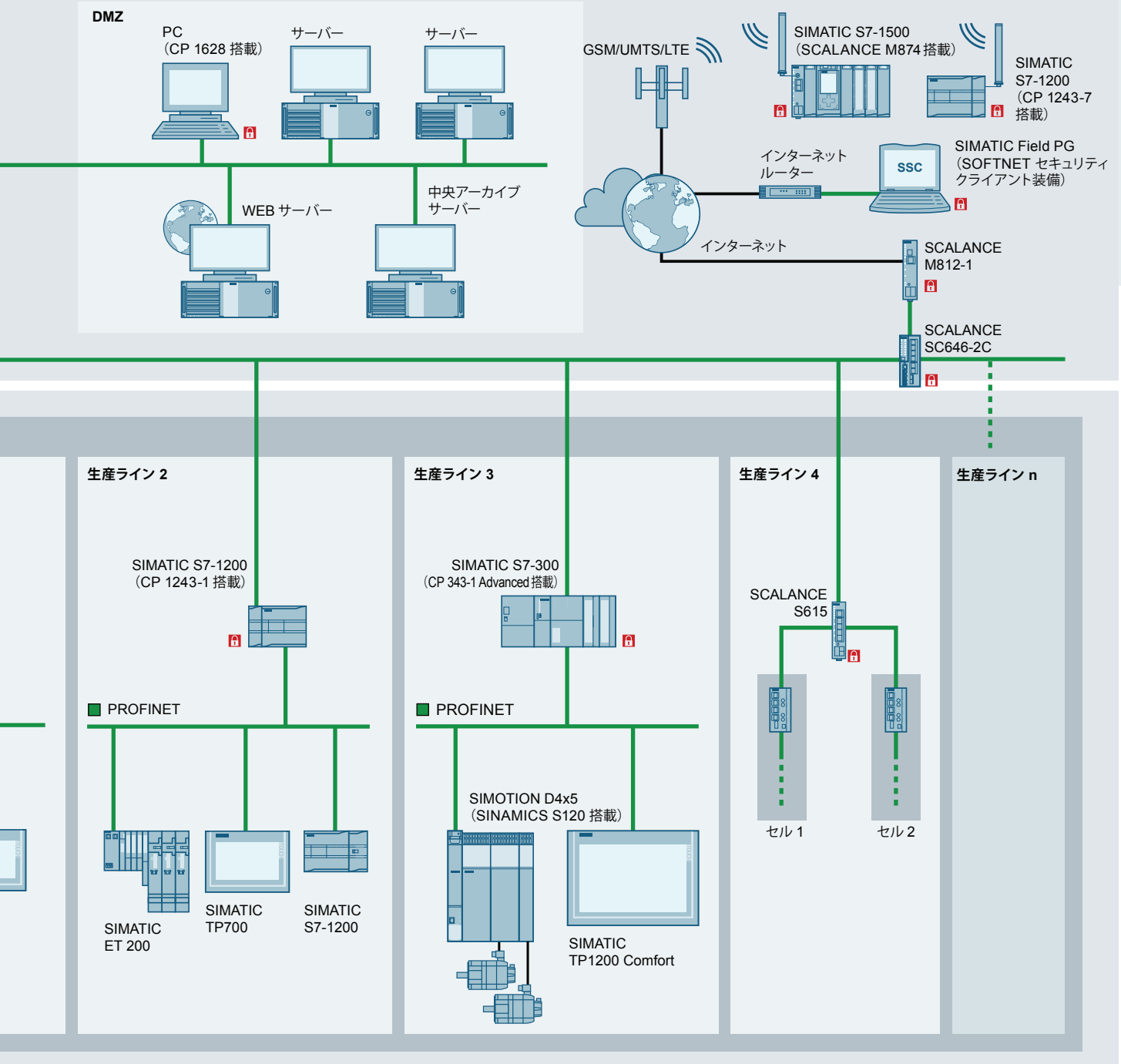
システム保全
多層防御の 3 つめの柱は、システム保全のセーフガードです。ここでは、オートメーションシステムや SIMATIC S7-1200、および S7-1500、SCADA および HMI システムといった制御コンポーネントを不正アクセスから保護し、ノウハウプロテクトなどの特殊な要件を満たすことに重点が置かれます。さらにシステム保全にはユーザー認証、アクセスや変更の承認、およびシステムハードニング、つまり攻撃に対するコンポーネントの堅牢性向上も含まれます。

産業セキュリティの概要

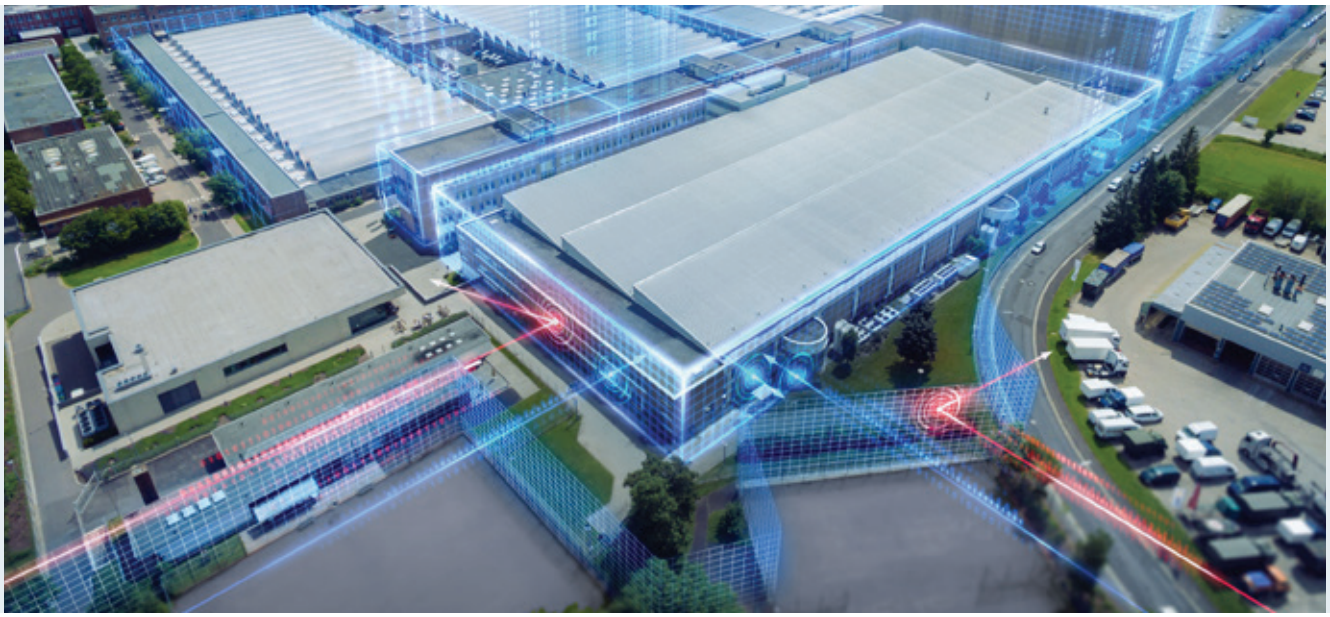


セキュリティ統合コンポーネントによるセキュアな通信、ネットワークアクセス保護、およびネットワークセグメンテーション

- 物理的保護
- セキュリティ管理
- セキュリティ運用センター



産業セキュリティ – デジタル化の前提条件



企業のデジタル化の促進、およびそれに付随するあらゆる分野でのネットワーク接続の増加により、経済発展の可能性が大いに高まります。しかし、それと同時にデジタル化によって、迅速で安定した応答というニーズに対応するための大規模なデータ通信やデータストレージ、そしてよりオープンな通信規格が必要となり、不正な攻撃に対する脆弱性という新たなリスクも発生します。このため、サイバーセキュリティおよび産業セキュリティは産業用通信や RFID 等の自動認識システムと同様に、企業のデジタル化にとって必要不可欠なのです。

TIA（Totally Integrated Automation）の一部としての産業セキュリティ

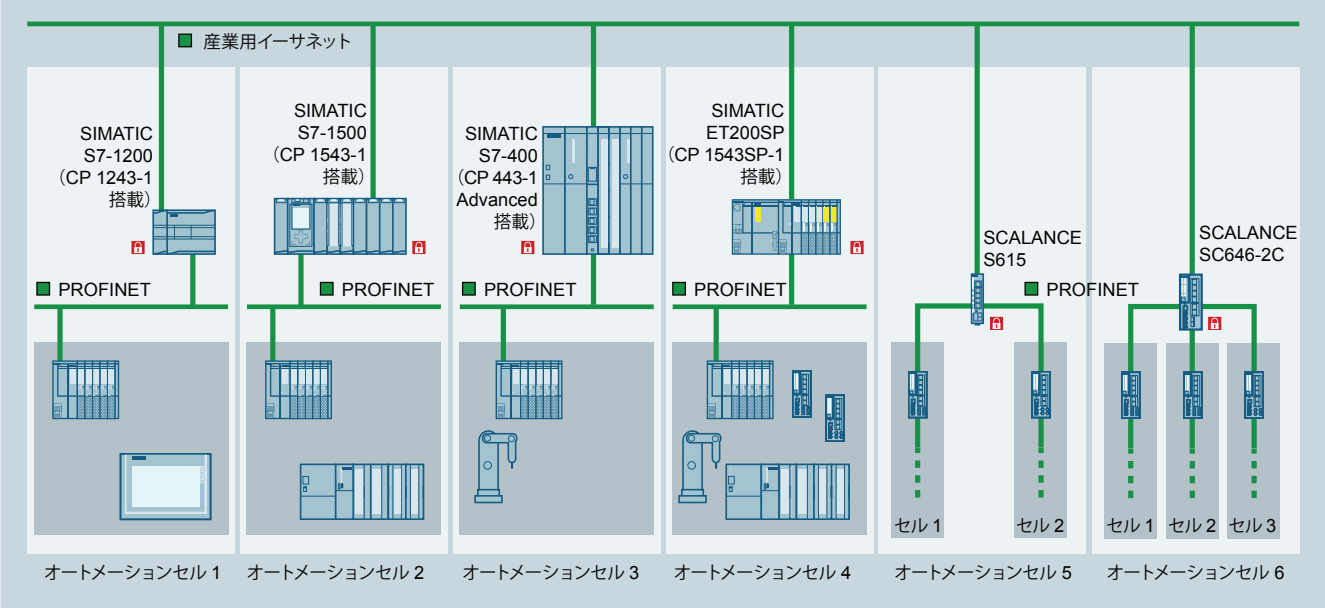
TIA（Totally Integrated Automation）:
すべてのオートメーションコンポーネント間での効率的なインタラクション

TIA ポータルに統合されたネットワークセキュリティおよびシステム保全に対応する産業互換のセキュリティ製品により、お客様のオートメーションソリューションを効率的に保護し、産業プラントやオートメーションシステムにおける多層防御コンセプトを実装することが可能です。

すべての産業セキュリティ機器およびリモートネットワークコンポーネントを TIA ポータルに統合し、そこでエンジニアリングすることができます。さらに、セキュリティ通信プロセッサーが TIA ポータル経由で自動的にファイアウォールルールに割り当てられます。

ネットワークセキュリティ

セルプロテクション・コンセプト



個別のオートメーションセルに統合されたセキュリティによるコンポーネント間でのセキュアな通信

産業用通信は企業が成功するための重要な要因ですが、ネットワークが保護されていることが前提条件です。セルプロテクション・コンセプトの実現のために、シーメンスはお客様と協力して、統合型通信機能だけでなく、ファイアウォールや VPN といった特殊なセキュリティ機能を搭載した Security Integrated コンポーネントを提供します。

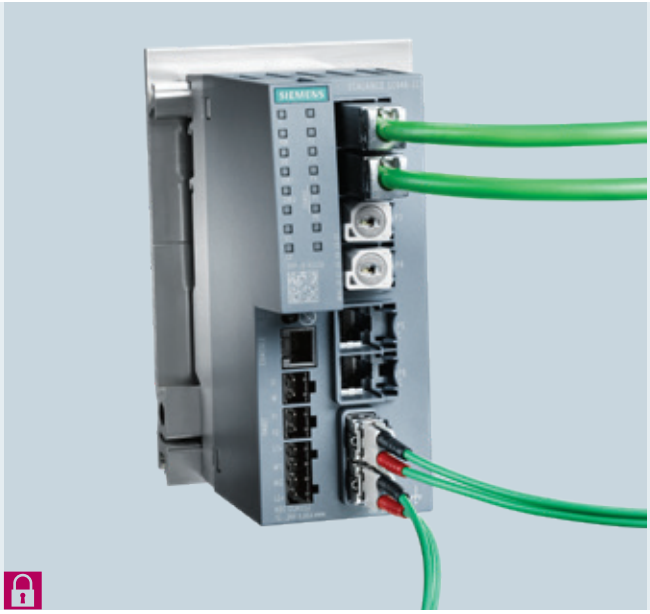
サイバーセキュリティ – 包括的なセキュリティメカニズム

シーメンスはお客様が技術革新の恩恵を受けられるようお手伝いするとともに、サイバーセキュリティなどにおけるリスクを可能な限り低減することに努めます。新たな脅威に継続的に対応できなければ、セキュリティソリューションが最適に実装されているとは言えません。そのため、シーメンスは自社に対する潜在的な脅威だけでなく、お客様が経験する脅威についても十分な注意を払っています。サイバーセキュリティに対応したシーメンスの製品、ソリューション、およびサービスは、産業プラント、オートメーションシステム、および電力プラントにおいて実績のあるセキュリティを提供します。

セルプロテクション・コンセプト

セルプロテクション・コンセプトによって、プラントネットワークは個々の保護されたオートメーションセルにセグメント化され、各セル内ではすべてのデバイスがセキュアに相互通信できます。個々のセルは、VPN とファイアウォールによってセキュアにプラントネットワークに接続され、生産プラント全体の耐障害性が高まり、可用性が向上します。このコンセプトに基づいたセキュリティは、SCALANCE S 産業セキュリティ機器や SIMATIC S7/PC 通信プロセッサーなどを使用し実装が可能です。

SCALANCE S 産業セキュリティ機器



SCALANCE S 産業セキュリティ機器は、ディスクリート製造およびプロセス製造における機器やネットワークのセキュリティを提供し、ステートフルインスペクションファイアウォールや仮想プライベートネットワーク（VPN）などのメカニズムによって産業用通信を保護します。
この産業セキュリティ機器は産業用途に最適化されており、要件に応じて異なるポート構成（2 ～ 6 ポート）、および機能範囲（ファイアウォール、またはファイアウォール + VPN）を選択して頂けます。
すべてのラインナップで、ウェブベースマネジメント（WBM）、コマンドラインインターフェース（CLI）、SNMP（Simple Network Management Protocol）、ネットワーク管理 SINEMA サーバー、TIA ポータル（V15 以降）での設定に対応しています。
SCALANCE S の全ての機器には VPN 接続を制御可能なデジタル入力（DI）が搭載されています。

産業用ファイアウォール機器

SCALANCE SC632-2C/SC636-2C

- 約 600 Mbit/s のファイアウォールまたは暗号化性能
- ネットワークアドレス変換（NAT）、ネットワークアドレスポート変換（NAPT）
- 長距離用の光ファイバー通信に対応（最大 200 km）
- プログラミングツールを使用した直接アクセス用のコンソールポート
- SINEMA Remote Connect を使用したセキュアなリモートアクセス
- C-PLUG を使用したシンプルなデバイス交換

産業用VPN機器

SCALANCE S615

- ファイアウォールおよび仮想プライベートネットワーク VPN（IPsec、OpenVPN をクライアントとして SINEMA Remote Connect への接続に使用）
- ポートベースの仮想ローカルエリアネットワーク（VLAN）ごとに最大で 5 つの異なるセキュリティゾーンを設定できるため、セキュリティゾーン、および必要に応じてセキュリティゾーン間のファイアウォールルールを設定可能
- 自動設定インターフェースにより、SINEMA Remote Connect への接続を簡単に設定可能
- 10/100 Mbit/s のポートでの接続
- C-PLUG を使用したシンプルなデバイス交換

SCALANCE SC642-2C/SC646-2C

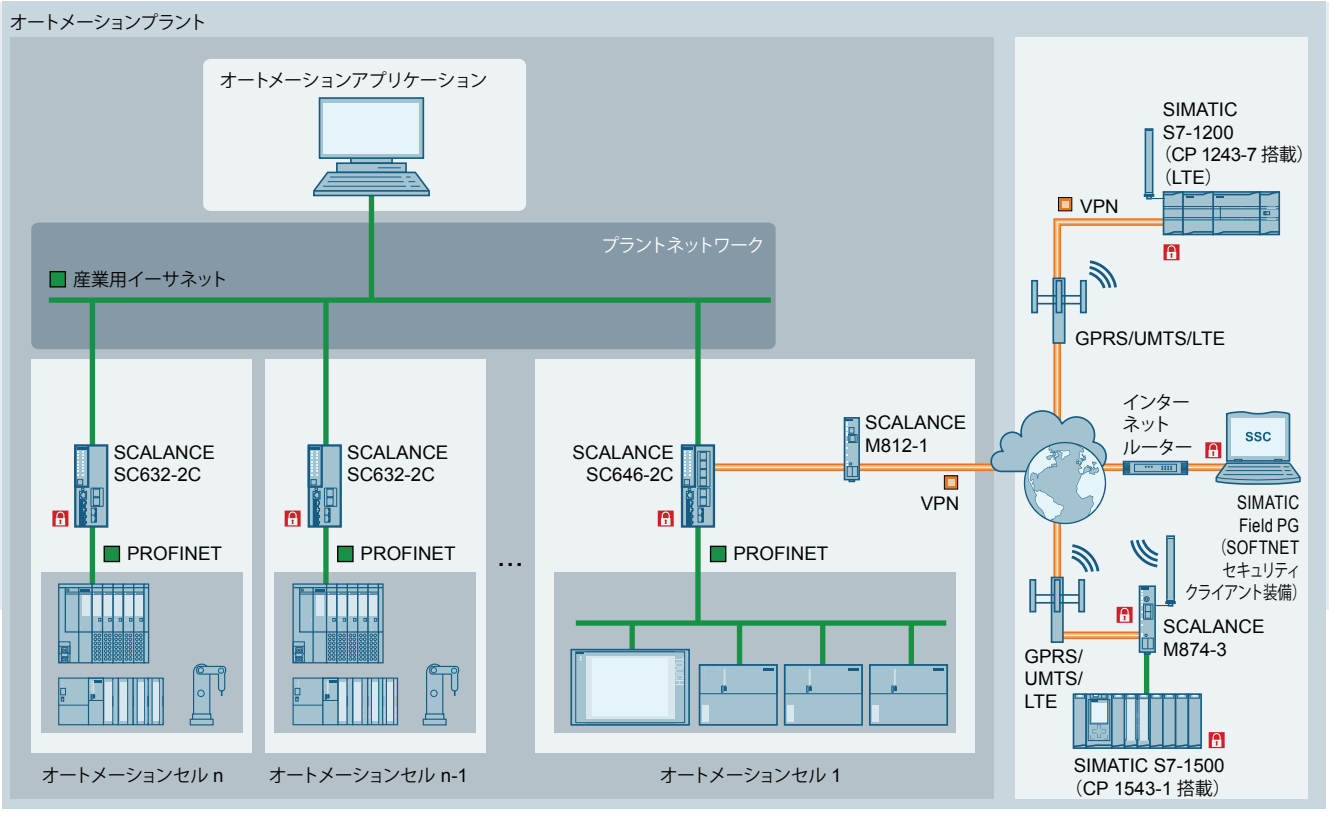
- 約 600 Mbit/s のファイアウォールまたは暗号化性能
- 最大 120 Mbit/s の VPN を接続数 200 まで管理
- ネットワークアドレス変換（NAT）、ネットワークアドレスポート変換（NAPT）
- 長距離用の光ファイバー通信に対応（最大 200 km）
- プログラミングツールを使用した直接アクセス用のコンソールポート
- SINEMA Remote Connect を使用したセキュアなリモートアクセス
- C-PLUG を使用したシンプルなデバイス交換

産業セキュリティ機器に関する詳細情報については、
以下のサイトを参照してください。

siemens.com/scalance-s

使用例

SCALANCE S によるセキュアなリモートメンテナンス



オートメーションネットワークに直接接続しない、SCALANCE S 産業セキュリティ機器を使用したセキュアなリモートアクセス

タスク

システムインテグレーターがメンテナンスのために、マシンをセキュアにインターネットにアクセスする、またはエンドユーザーのプラントにアクセスする必要があるが、特定のデバイスにのみアクセスを許可し、プラントネットワークへのアクセスはできないようにしたい。さらに、プラントからリモートステーションまで、モバイルネットワーク（UMTS や LTE など）経由でセキュアな接続を確立したい。

ソリューション

開始点の例：VPN クライアント（SOFTNET Security Client、CP 1628、SCALANCE M874-3）を使用するシステムインテグレーター

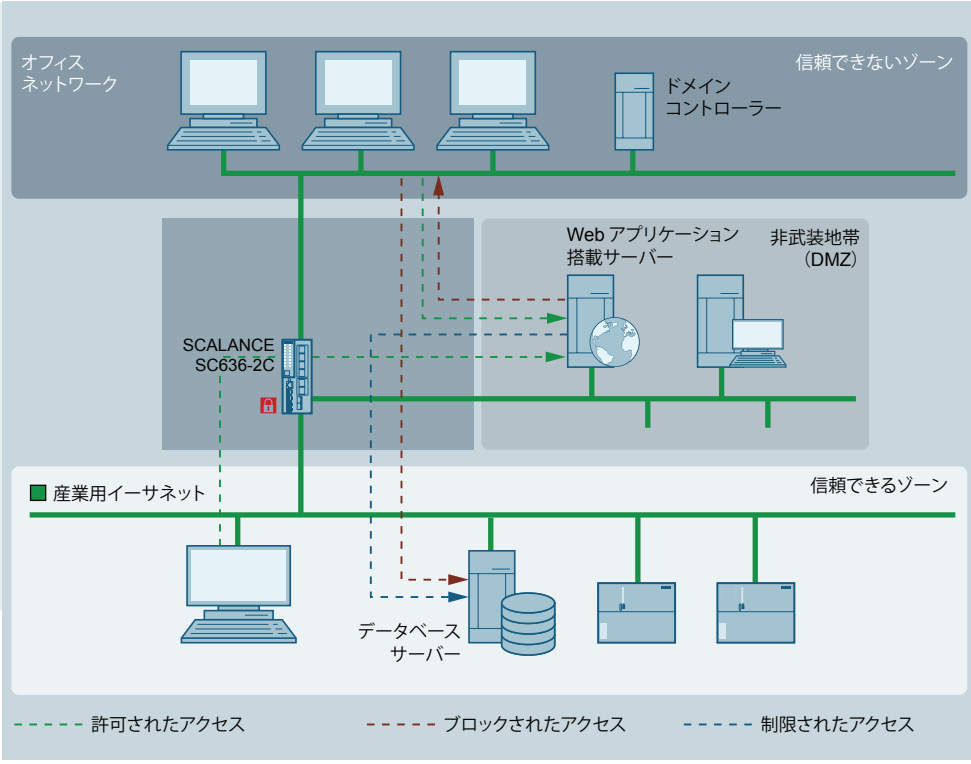
終了点（オートメーションシステム）：
VPN サーバーとしての SCALANCE SC646-2C

メリットの概要

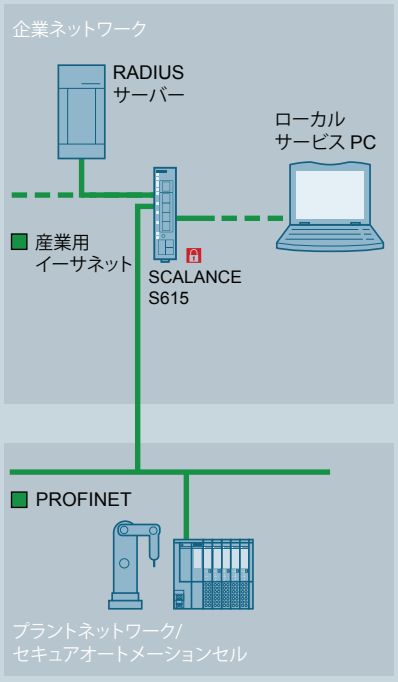
- VPN（IPsec）による通信保護により、インターネットおよび UMTS や LTE などのモバイルネットワーク経由でのセキュアなリモートアクセスを実現
- 内蔵されたファイアウォール機能によりアクセスを制限
- プラントネットワークに直接接続しない、SCALANCE SC646-2C ファイアウォールを使用したプラントユニットへのセキュアなリモートアクセス

使用例

DMZ によるネットワークアクセス保護



シーメンスの産業セキュリティコンセプトの核心部としてのネットワークセキュリティ



SCALANCE S615 の DMZ ポート経由で
ローカルサービス PC に接続

タスク
セキュアなネットワーク（プラントネットワーク）とセキュアでないネットワーク（オフィスネットワーク）を直接接続することなく、そのどちらからもネットワークノードまたはサーバー（MES サーバーなど）にアクセスできるようにしたい。

ソリューション
SCALANCE SC636-2C を使用することで、DMZ を設定できます。この DMZ 内にサーバーを配置できます。

メリットの概要

- DMZ 経由でのデータ交換によりセキュリティが向上し、オートメーションネットワークへの直接アクセスを防止
- ネットワーク境界において、オートメーションネットワークを不正アクセスから保護

タスク
ローカルネットワークを不正アクセスから保護し、承認された人が業務上必要なアクセスのみを行えるようにしたい。

ソリューション
SCALANCE S615 の DMZ ポートのみが、ローカルにアクセスできるポートです。
この産業セキュリティ機器をプラントネットワーク、および下位レベルのオートメーションセルに接続します。ユーザー固有のファイアウォールルールがユーザーごとに作成され、ネットワークにアクセスするには、ユーザーはユーザー名とパスワードを使用して SCALANCE S にログインする必要があります。

メリットの概要

- ローカルネットワークアクセスのセキュリティ強化
- 柔軟なユーザー固有のアクセス権
- RADIUS を使用した中央認証も可能

SCALANCE M 産業用通信モデム

SCALANCE M のポートフォリオは、遠隔制御、遠隔サービス、および産業用リモート通信のあらゆる用途に使用できるモデムとルーターで構成されています。
内蔵されたファイアウォールおよび VPN（IPsec、OpenVPN をクライアントとして SINEMA Remote Connect への接続に使用）セキュリティ機能で不正アクセスを防止し、データ転送のセキュリティを強化します。

リモートネットワークへの無線接続

SCALANCE M の無線デバイスは世界的に普及している公衆携帯電話ネットワーク（2G、3G、4G）をデータ伝送に使用します。

SCALANCE M874-2 は、GSM データサービスである GPRS（General Packet Radio Service）および EDGE（Enhanced Data Rates for GSM Evolution）をサポートしています。

SCALANCE M874-3 は UMTS データサービスである HSPA+（High Speed Packet Access）をサポートしており、下りで最大 14.4 Mbit/s、上り最大 5.76 Mbit/s の高速伝送が可能です。

SCALANCE M876-3 は、デュアルバンド CDMA2000 および UMTS データサービスである HSPA+ をサポートしており、下り最大 14.4 Mbit/s、上り最大 5.76 Mbit/s の高速伝送が可能です。

SCALANCE M876-4 は LTE（Long Term Evolution）をサポートしており、下り最大 100 Mbit/s、上り最大 50 Mbit/s の高速伝送が可能です。

リモートネットワークへの有線接続

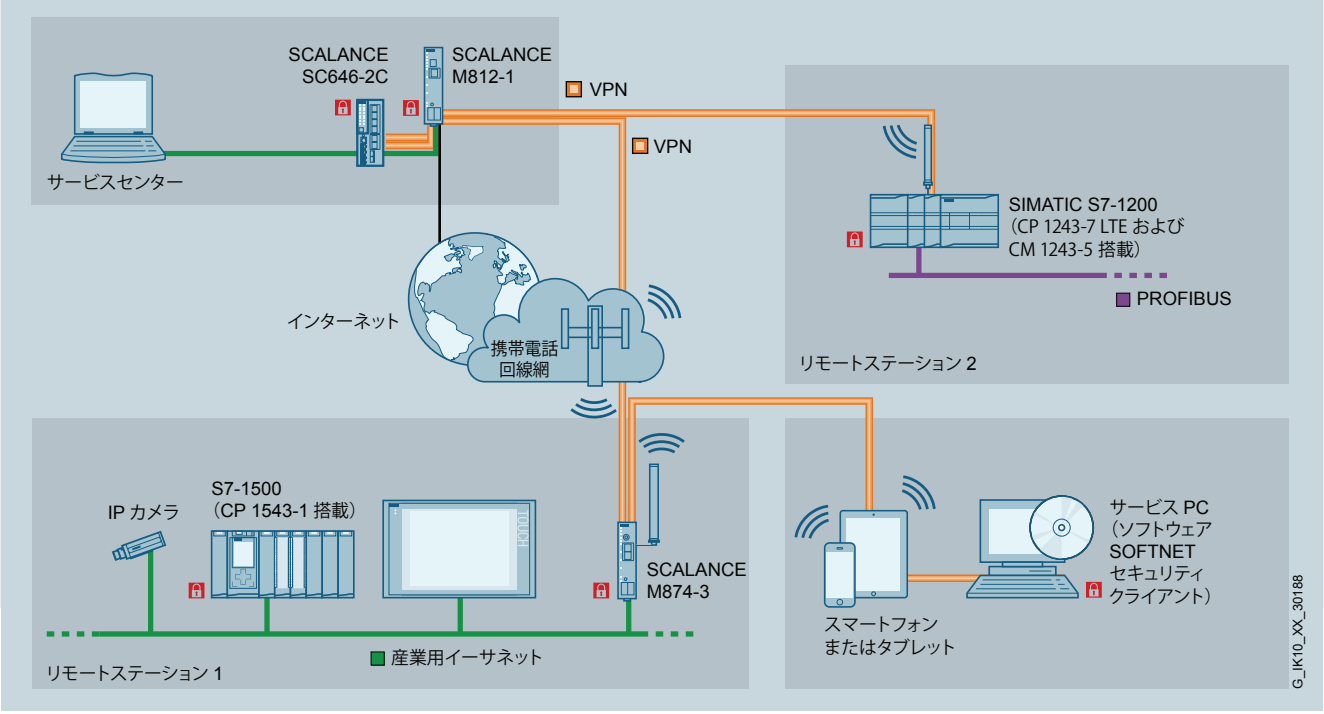
SCALANCE M シリーズの SHDSL および ADSL2 ルーターは、イーサネットベースのサブネットおよびオートメーションデバイスのコスト効率とセキュリティに優れた接続をサポートします。接続は既存の 2 線または標準ケーブルで行うことも、固定電話回線や DSL ネットワークで行うことも可能です。

SCALANCE M812-1 および SCALANCE M816-1 は固定電話回線や、ASDL2+（非対称デジタル加入者線）をサポートする DSL ネットワークへの接続用の DSL ルーターで、下り最大 25 Mbit/s、上り最大 1.4 Mbit/s の高速伝送が可能です。

SCALANCE M826-2 は、既存の 2 線または標準ケーブルでの接続用の SHDSL モデルであり、ITU-T 規格 G.991.2、または SHDSL.biz（シングルペア高速デジタル加入者線）をサポートしています。このため、このデバイスでは 1 つのワイヤーペアにつき最大で 15.3 Mbit/s の高速な非対称伝送が可能です。

使用例

モバイル無線ネットワーク経由でのプラントセクションへのセキュアなアクセス



SCALANCE M874-3 を使用した、VPN によるセキュアなリモートメンテナンス

タスク

サービスセンターにインターネット経由で接続し、リモートプログラミング、パラメーター割り当て、および診断といった一般的な用途だけでなく、世界中のマシンやプラントのモニタリングを可能にしたい。

ソリューション

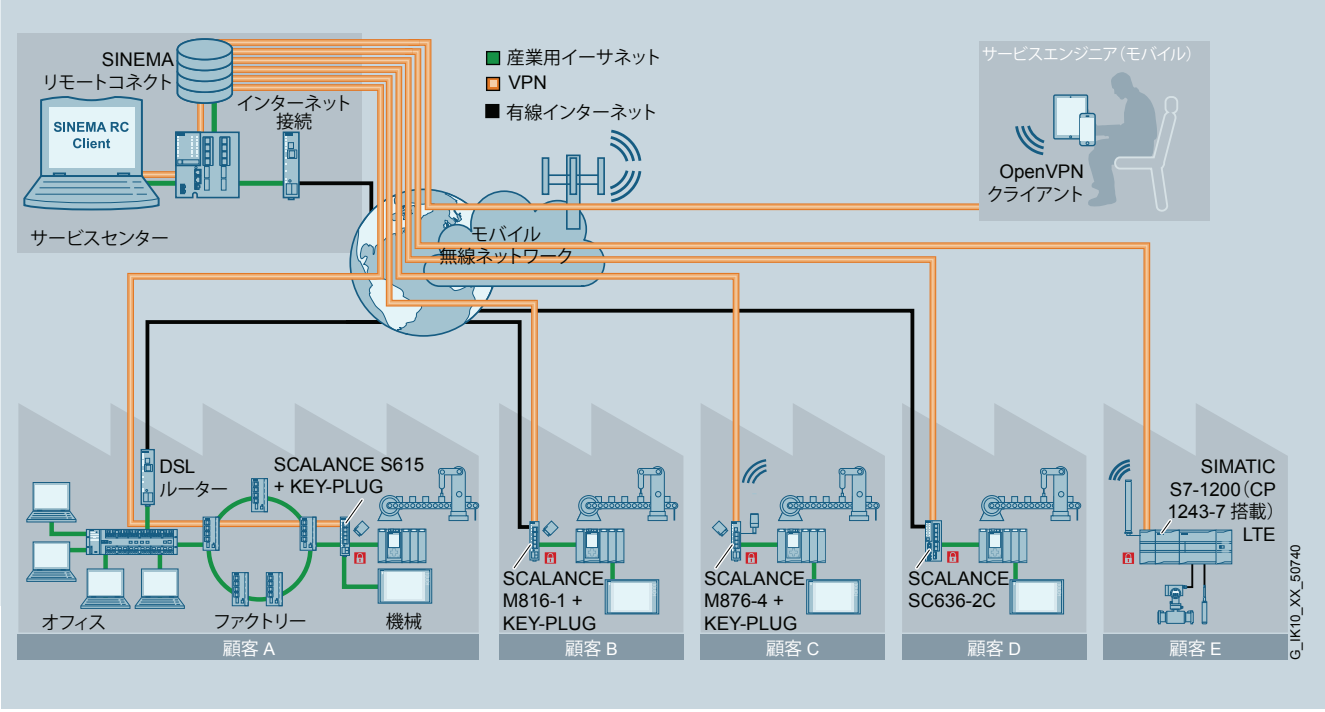
SCALANCE 通信モデム(SCALANCE M874-3)の内側にあるローカルネットワーク内すべての IP ベースのデバイス、特にオートメーションデバイスにアクセスできます。上りの帯域幅が広いため、動画のストリーミングなどのマルチメディアアプリケーションも実装できます。VPN 機能により、国や地域をまたいだデータ転送のセキュリティも強化されます。

メリットの概要

- 投資や運用コストを抑えてマシンおよび機器のリモートアクセスの強化が可能
- 3G/UMTS または 4G/LTE ネットワーク経由でのリモートプログラミングおよびリモート診断により交通費と電話代を削減
- Web インターフェースによるユーザーフレンドリーな診断
- HSPA+ をした高速伝送により伝送時間を短縮
- 内蔵されたファイアウォールおよび VPN による保護
- モバイル無線プロバイダーの既存の UMTS または LTE インフラを活用
- UMTS/GSM (クワッドバンド) 技術により世界中で使用可能。国ごとの認証にご注意ください。

使用例

SINEMA Remote Connect によるプラントセクションへのセキュアなアクセス



SINEMA Remote Connect の構成例 – 概要

タスク

- サブネットが同一の装置群および大規模プラントのリモートメンテナンス
- 用途が特殊なマシンおよび機密領域へのリモートアクセス。ステータス / メンテナンスデータ取得のために、接続の中央管理が必要
- ルーティング /NAT 情報によりデバイスを簡単に構成したい

ソリューション

- SINEMA Remote Connect でマシンおよびサービスエンジニアを中央管理
- ユーザー権限およびアクセス認証の割り当ておよび管理

一般的な使用分野

- プラントおよびマシンビルダ
- 送電所 / 変電所（地方自治体）
- 物流 / 港湾物流
- 高度道路交通システム（ITS）/ 運送会社
- 上下水道（地方自治体など）

メリットの概要

- 優れた透明性とセキュリティ
- アクセスのロギング
- 世界中どこからでもプラントセクションにセキュアかつ簡単にアクセス可能（OpenVPN および IPsec を使用）
- 最新の暗号化方法 TLS 1.2
- 同一ローカルサブネットの同一マシンを最適に接続（NAT）
- グループ管理により、異なるユーザー（サービスエンジニア）の管理の利便性が向上
- アドレス帳機能により、迅速かつ簡単に接続のセットアップが可能
- 既存インフラに簡単に統合可能
- ターミナルデバイスおよび SINAMA RC Client 用の自動設定可能かつシンプルなユーザーインターフェースにより、専門的な IT のノウハウが不要
- ユーザー名 / パスワードおよび PKI スマートカードによる多元的な認証により、セキュリティと利便性が向上
- 仮想環境での操作が可能

SIMATIC S7-1200、S7-1500、および ET 200SP CPU の セキュリティ通信プロセッサー

セキュリティ通信プロセッサーは、データの改ざんや諜報を防止するファイアウォール（データフローの制御）および VPN によってコントローラーを保護します。

CP 1243-1 および CP 1243-7 LTE
CP 1243-1 および CP 1243-7 LTE 通信プロセッサーは、SIMATIC S7-1200 コントローラーをイーサネット（CP 1243-1）、またはモバイル無線ネットワーク（CP 1243-7 LTE）に接続します。ファイアウォール（ステートフルインスペクション）と VPN（IPsec）セキュリティ機能により、この通信プロセッサーは S7-1200 ステーションおよび下位レベルのネットワークを不正アクセスから保護し、暗号化によってデータ伝送を改ざんや諜報からも保護します。さらに、CP を IP ベースのリモートネットワーク経由で S7-1200 ステーションの TeleControl Server Basic 制御センターソフトウェアへ統合することもできます。

メリットの概要

SIMATIC コントローラー用セキュリティ通信プロセッサーに特有のメリットは、TIA ポータルでの設定中にファイアウォールルールが自動作成されることです。
設定された通信接続がファイアウォール内で自動的に有効になるため、設定の手間やエラーの数を大幅に削減できます。

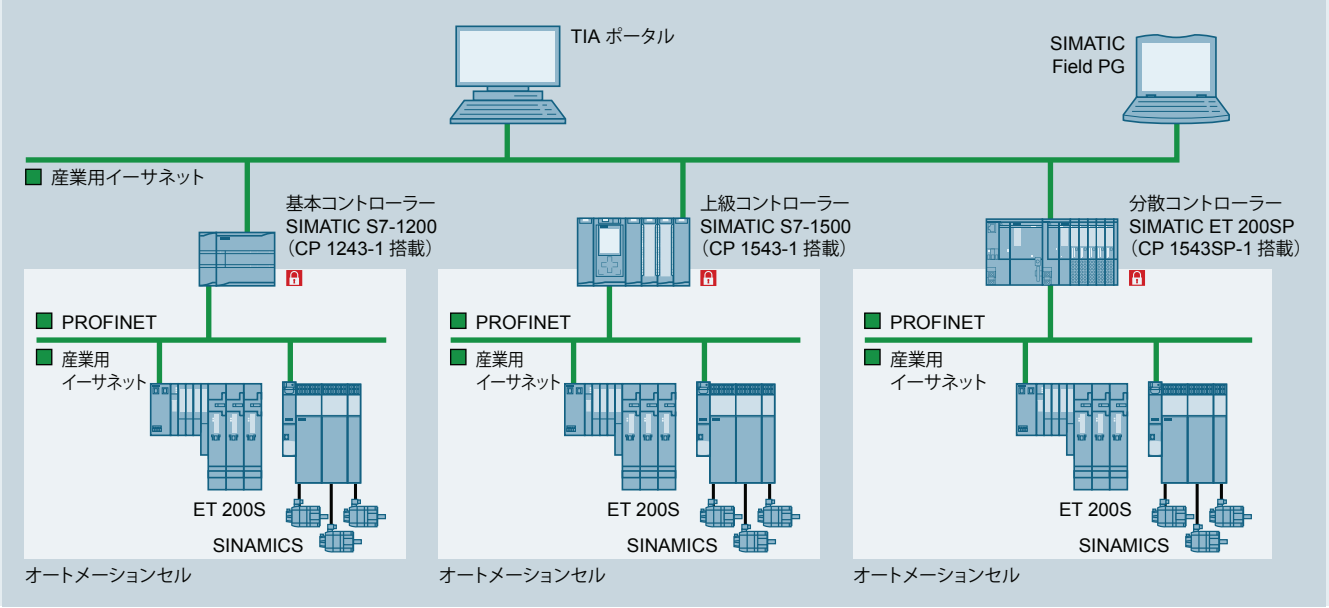
CP 1543SP-1
CP 1543SP-1 通信プロセッサーは、SIMATIC ET 200SP システムに産業用イーサネットインターフェースを追加することでシステムを柔軟に拡張できます。これにより、ネットワークセグメンテーションによる同一 IP アドレスの同一マシンのセットアップが可能になります。

また、SIMATIC ET 200SP にセキュアにアクセスするための、IPsec による VPN やステートフルインスペクションファイアウォールを使用したすべての伝送データの暗号化といった拡張セキュリティ機能も提供します。

CP 1543-1
CP 1543-1 通信プロセッサーは、SIMATIC S7-1500 コントローラーをイーサネットにセキュアに接続します。ファイアウォール（ステートフルインスペクション）と VPN（IPsec）セキュリティ機能、および FTPS や SNMPv3 などのデータ暗号化用プロトコルにより、この通信プロセッサーは S7-1500 ステーションおよび下位レベルのネットワークを不正アクセスから保護し、暗号化によってデータ伝送を改ざんや諜報からも保護します。この CP は、SMTPS（ポート 587 および 25）経由での暗号化された電子メール通信や、TCP/IP 経由でのセキュアかつオープンな通信も行います。

使用例

セキュリティ通信プロセッサーによるネットワークセグメンテーション



CP 1243-1、CP 1543-1、または CP 1543SP-1 でのネットワークのセグメンテーション、および SIMATIC コントローラー S7-1200、S7-1500、または SIMATIC ET 200SP CPU の保護

タスク

SIMATIC コントローラー上でのオートメーションネットワークと下位レベルのネットワーク間の通信セキュリティをアクセス制御によって強化したい。

ソリューション

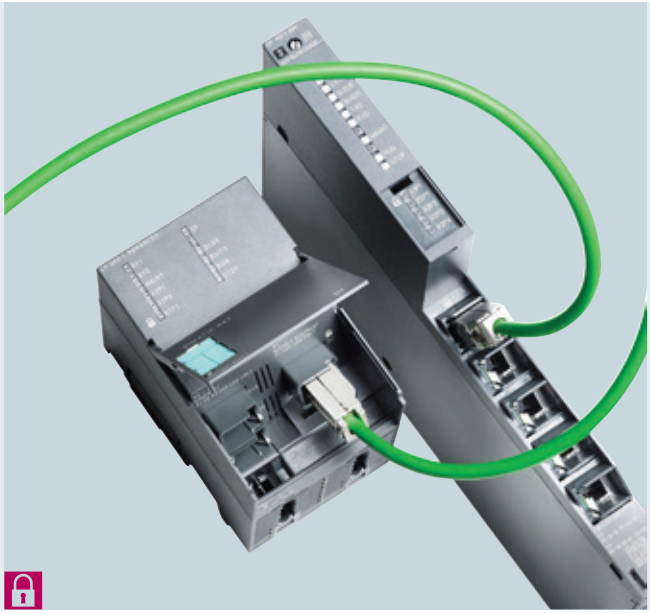
保護されるオートメーションセルの上流に位置する各ターゲットシステム（S7-1200、S7-1500、ET 200SP）のラック内に通信プロセッサーを配置します。これにより、SIMATIC CPU と下位レベルのオートメーションセル間の通信は、ファイアウォールルールによって許可された接続に制限され、必要に応じて VPN を設定することで改ざんや諜報から保護されます。

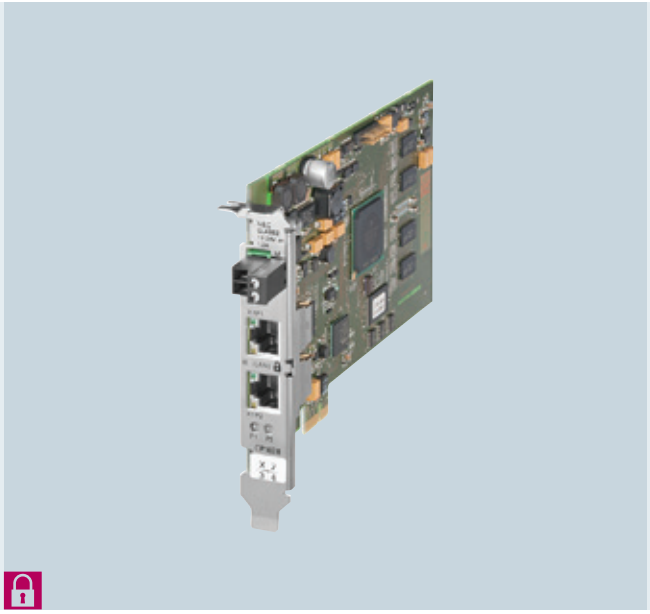
メリットの概要

- ステートフルインスペクションファイアウォールおよび VPN により、SIMATIC S7-1200、S7-1500、および ET 200SP CPU を産業用イーサネットにセキュアに接続
- セキュアな通信方法が追加：ファイル転送および電子メール
- IPv6 ベースのインフラでの使用が可能 [1)]

[1)] CP 1543-1 および CP 1543SP-1 の場合

SIMATIC S7-300、S7-400、および PG/PC のセキュリティ通信プロセッサー





CP 343-1 Advanced および CP 443-1 Advanced
SIMATIC S7-300 および S7-400 向けの産業用イーサネット通信プロセッサー CP 343-1 Advanced および CP 443-1 Advanced では、一般的な通信機能である統合スイッチやレイヤー 3 ルーティング機能に加えて、コントローラーおよび下位レベルのデバイスをセキュリティリスクから保護するステートフルインスペクションファイアウォールや VPN ゲートウェイといった Security Integrated を採用しています。

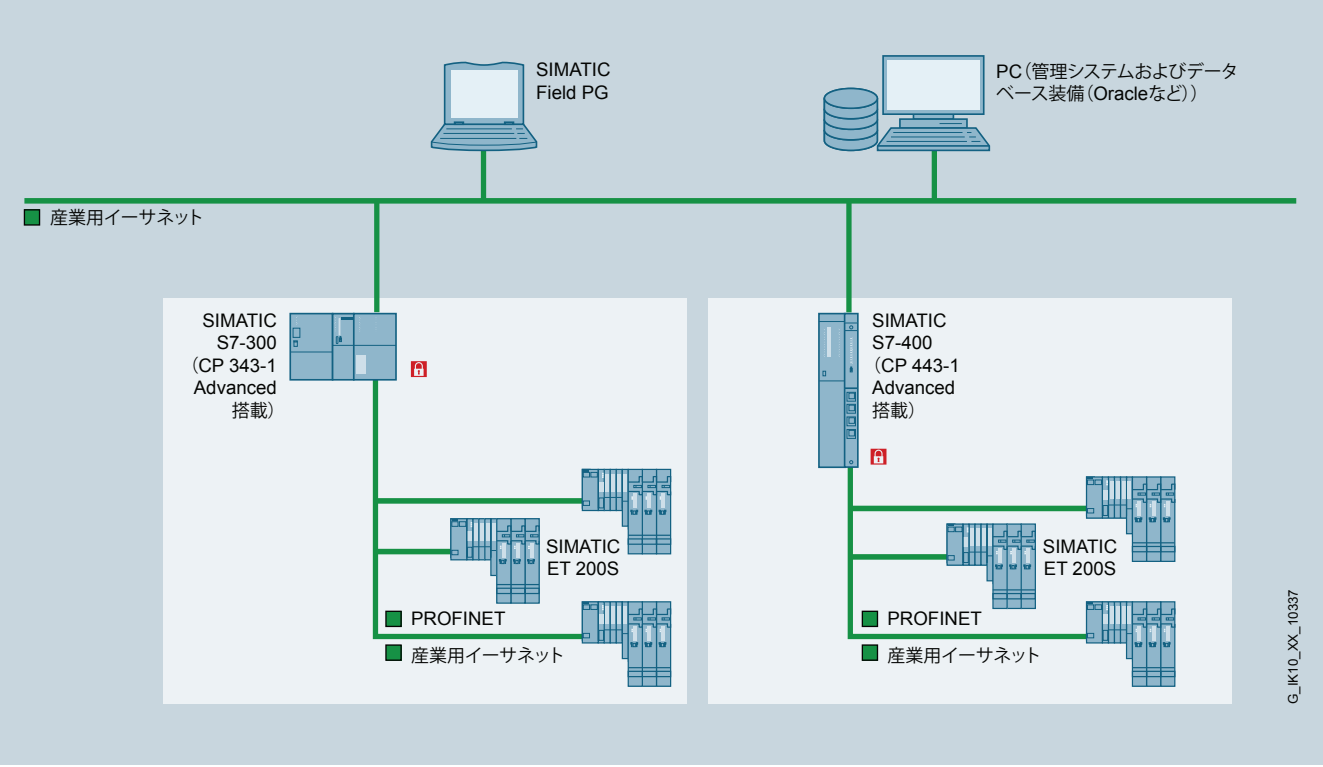
CP 1628
CP 1628 産業用イーサネット通信プロセッサーは、特別なオペレーティングシステムの設定をしなくてもセキュアな通信を実現できるファイアウォールおよび VPN によって産業用 PC を保護します。このため、このモジュールを搭載したコンピューターを保護されたセルに接続できます。CP 1628 を使用すると、SIMATIC PG/PC、および PCI Express スロットを搭載した PC を産業用イーサネット（10/100/1000 Mbit/s）に接続することが可能です。内蔵されたスイッチを経由して、追加のフィールドデバイスを産業用イーサネットに柔軟に接続できます。CP 1623 から採用されたオートメーション機能だけでなく、この通信プロセッサーでは PG/PC システムをセキュリティリスクから保護するステートフルインスペクションファイアウォールや VPN ゲートウェイといった Security Integrated も採用しています。

メリットの概要

SIMATIC コントローラー用セキュリティ通信プロセッサーに特有のメリットは、TIA ポータルでの設定中にファイアウォールルールが自動作成されることです。
設定された通信接続がファイアウォール内で自動的に有効になるため、設定の手間やエラーの数が大幅に削減されます。

使用例

セキュリティ通信プロセッサーによるネットワークセグメンテーション



CP 343-1 Advanced または CP 443-1 Advanced でのネットワークのセグメンテーションと、SIMATIC S7-300 および S7-400 コントローラーの保護

タスク

オフィスレベルの管理システムとオートメーションレベルの下位レベルネットワーク間の通信セキュリティをアクセス制御によって強化したい。

ソリューション

CP 343-1 Advanced および CP 443-1 Advanced を保護するオートメーションネットワークの上流に配置します。これによって、通信がファイアウォールルールによって許可された接続に制限されます。

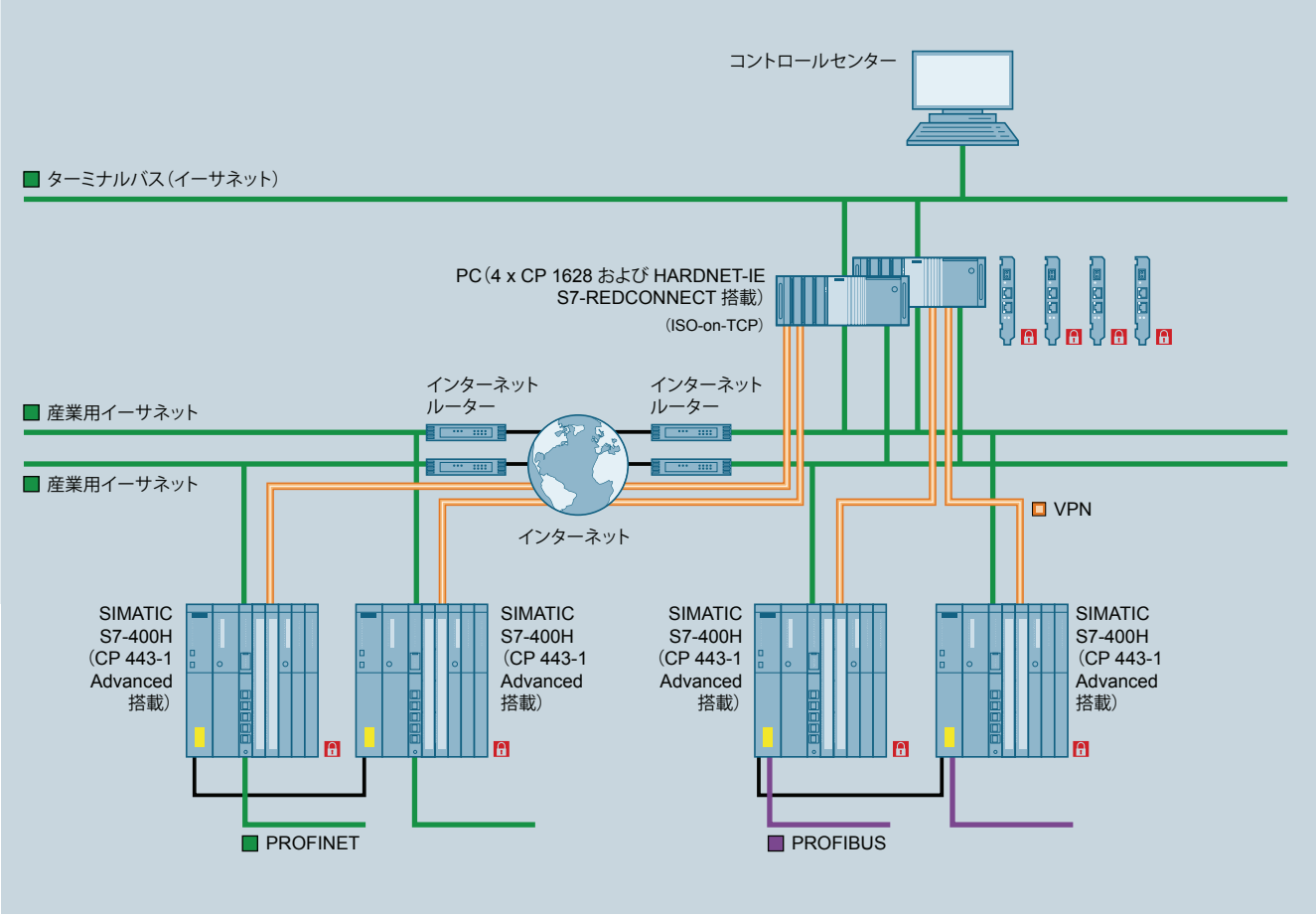
メリットの概要

- ファイアウォール、VPN ゲートウェイ、および CP を 1 つのデバイスに搭載：高度な CP とファイアウォール、および VPN セキュリティ機能を統合し、オートメーションセルとデータ伝送の保護を実現
- セキュアな通信を統合：CP を STEP 7 で簡単に設定可能。VPN を CP 間、または SCALANCE S、SOFTNET Security Client VPN ソフトウェア、CP 1628 PC モジュール、および SCALANCE M に対して設定可能

すべての CP 343-1 Advanced および CP 443-1 Advanced ユーザーは Security Integrated を利用でき、個別のハードウェアや SIMATIC S7 以外の特殊なツールがなくても産業プラントのセキュリティを設定可能です。

使用例

セキュリティ通信プロセッサーによるセキュアな冗長化



CP 1628 および CP 443-1 Advanced によるセキュアな冗長化

タスク

可用性の高いプラントでの PC システムと S7-400H コントローラー間の冗長化接続を保護したい。

ソリューション

VPN をセキュリティ通信プロセッサー CP 1628 と CP 443-1 Advanced 間に設定することで、H 通信のセキュアな伝送が可能になります。さらに、CP 1628 は内蔵されたファイアウォールによって PC システムを不正アクセスから保護します。

メリットの概要

- ファイアウォール、VPN ゲートウェイ、および CP を 1 つのデバイスに搭載：この製品により、ユーザーは内蔵された本格的なセキュリティモジュールを使用できるため、PC を改ざんや不正アクセスから保護できます。
- セキュアな通信を統合：CP を STEP 7/NCM PC（V5.5 SP3 以降）、または STEP 7（TIA ポータル）V12 SP1 以降で簡単に設定できます。

SOFTNET Security Client および SINEMA Remote Connect

SOFTNET Security Client

SOFTNET Security Client により、プログラミングツール、PC、およびノートパソコンで SCALANCE S、SCALANCE M、またはセキュリティ通信プロセッサーなどの他の VPN 機器への VPN 接続を設定できます。これにより、LAN 経由または WAN 経由（インターネット経由でのリモートメンテナンス時など）でのオートメーションシステムへのセキュアなクライアントアクセスが可能になります。承認されたプログラミングツールやノートパソコンしかオートメーションデバイスやオートメーションセルへのアクセスが許可されないため、プラントでの障害を防止できます。

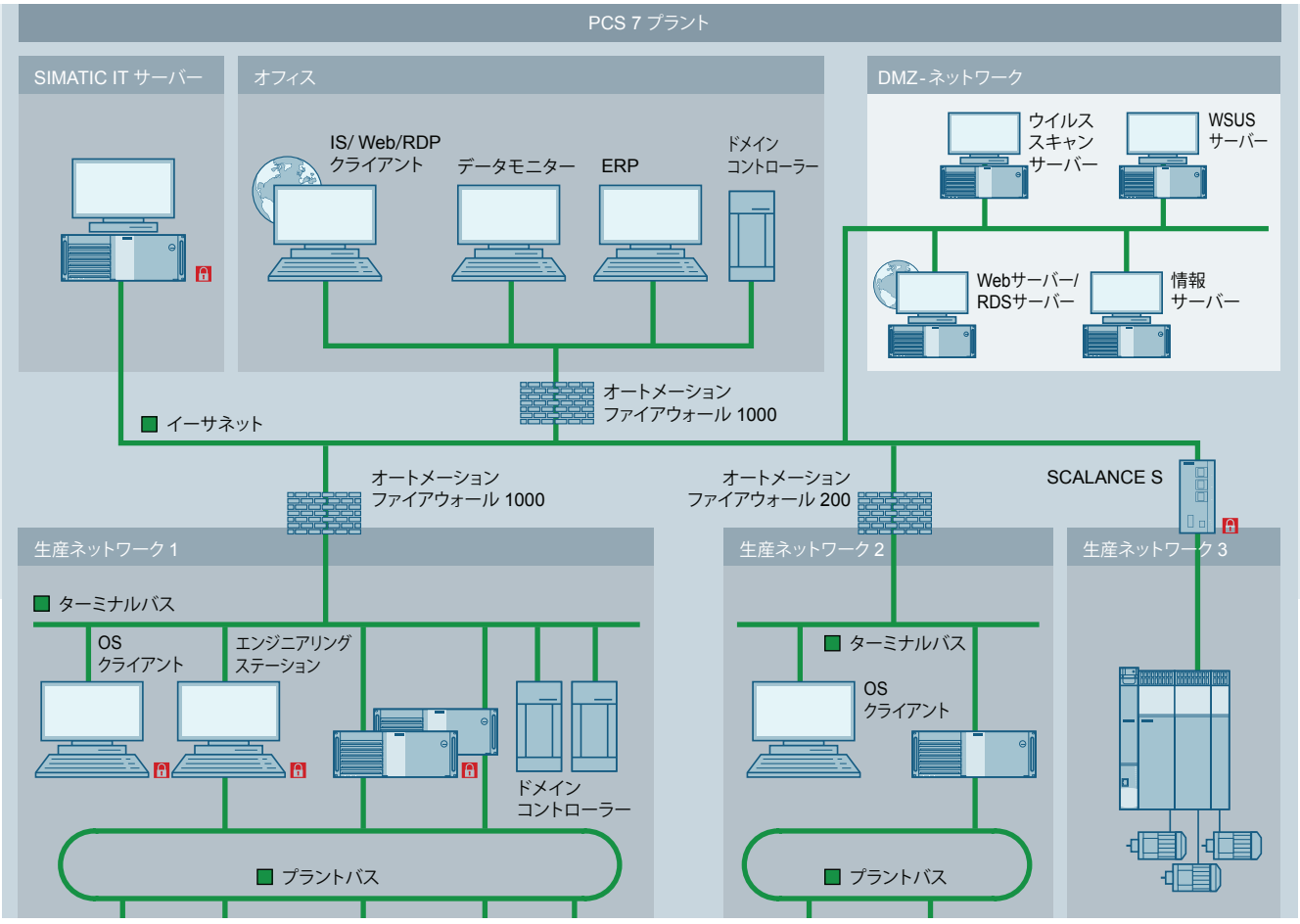
モバイル PC 上でソフトウェアを使用すると、通信を強化するためのハードウェアを追加する必要がないため、柔軟性が向上します。

SINEMA Remote Connect

世界中のマシンおよび機器へのリモートアクセスを容易にする、リモートネットワーク管理プラットフォームです。SINEMA Remote Connect により、サービスセンター、サービスエンジニア、および設置された機器間の VPN 接続をセキュアに管理できます。
機器やマシンが含まれている企業ネットワークへの直接アクセスは、あらかじめ防止されています。サービスエンジニアおよびメンテナンス中のマシンは、SINEMA Remote Connect サーバーに個別に接続を確立します。サーバーが証明書の交換によって個々のステーションの同一性を確認するまで、マシンへのいかなるアクセスも許可されません。

SINEMA Remote Connect への接続は、携帯電話ネットワーク、DSL、または既存のプライベートネットワークインフラなどのさまざまな方法で確立できます。

SIMATIC PCS 7 のセキュリティ



SIMATIC PCS 7 のセキュリティ – システム例

PCS 7 の最優先事項は、操作作業員が常に生産およびプロセスを制御し続けることであり、これはセキュリティの脅威が発生している場合でも変わりません。完全なオペレーターコントロールとモニタリング機能は、プラントやネットワークにおける脅威を防止する、または封じ込めるためのアクションを取ることによって維持されます。PCS 7 のセキュリティコンセプトは、認証されたユーザーのみが、認証されたデバイス上で、承認された操作を実行できるようにすることです。これらの操作は、人、環境、製品、調整対象となる物品、企業のビジネスを危険にさらすことなく信頼性の高い生産やオーダーの調整ができるよう、明確に定義され、計画されたアプローチでのみ実行される必要があります。

PCS 7 のセキュリティコンセプトは、多層防御戦略に基づいています。つまり、リスクを最小限にとどめ、プラントのセキュリティを強化するよう、以下の機能によって複数の保護レベルを設けています。

- SIMATIC LOGON により、特定のユーザーにのみアクセス権を割り当て
- ファイアウォール：ネットワークのセグメンテーションや、セキュリティセル、ファイアウォール、および DMZ を使用し、特定のネットワーク領域をセグメント化してセキュリティを強化
- VPN：暗号化によるセキュアな通信
- 最新のウイルス検索プログラムを使用し、パッチ管理手法を採用することで、システムに対する危害のリスクを低減
- ホワイトリストによってシステム上で実行が許可されるプログラムを指定

PCS 7 セキュリティコンセプトのエレメント

- システムハードニング
- ユーザー管理（SIMATIC Logon）
- パッチ管理
- マルウェア検出および防止
- ファイアウォールおよびセルプロテクション
- トレーニングおよびプロセス

技術仕様

SCALANCE S 産業セキュリティ機器

	産業用ファイアウォール機器		産業用 VPN 機器		
品名	SCALANCE SC632-2C	SCALANCE SC636-2C	SCALANCE S615	SCALANCE SC642-2C	SCALANCE SC646-2C
型式	6GK5632-2GS00-2AC2	6GK5636-2GS00-2AC2	6GK5615-0AA00-2AA2	6GK5642-2GS00-2AC2	6GK5646-2GS00-2AC2
伝送速度					
伝送速度	10 / 100 / 1000 Mbit/s	10 / 100 / 1000 Mbit/s	10 / 100 Mbit/s	10 / 100 / 1000 Mbit/s	10 / 100 / 1000 Mbit/s
インターフェース					
電気ポート	RJ45 × 2	RJ45 × 6	RJ45 × 5	RJ45 × 2	RJ45 × 6
光ポート	SFP コンボポート× 2	SFP コンボポート× 2	–	SFP コンボポート× 2	SFP コンボポート× 2
信号接点	2 ピン端子台× 1	2 ピン端子台× 1	–	2 ピン端子台× 1	2 ピン端子台× 1
電源	4 ピン端子台× 1	4 ピン端子台× 1	5 ピン端子台× 1	4 ピン端子台× 1	4 ピン端子台× 1
C-PLUG 対応	○	○	○	○	○
電源					
電源電圧	DC 24V	DC 24V	DC 24V	DC 24V	DC 24V
範囲	DC 9.6～31.2 V	DC 9.6～31.2 V	DC 10.8～28.2 V	DC 9.6～31.2 V	DC 9.6～31.2 V
許容周囲条件					
周囲温度					
動作時	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃
保管時	-40 ℃ ～ +85 ℃	-40 ℃ ～ +85 ℃	-40 ℃ ～ +80 ℃	-40 ℃ ～ +85 ℃	-40 ℃ ～ +85 ℃
輸送時	-40 ℃ ～ +85 ℃	-40 ℃ ～ +85 ℃	-40 ℃ ～ +80 ℃	-40 ℃ ～ +85 ℃	-40 ℃ ～ +85 ℃
保護等級	IP20	IP20	IP20	IP20	IP20
設計、寸法、および重量					
設計	コンパクト	コンパクト	コンパクト	コンパクト	コンパクト
幅 / 高さ / 奥行き	60 mm / 145 mm / 125 mm	60 mm / 145 mm / 125 mm	35 mm / 147 mm / 127 mm	60 mm / 145 mm / 125 mm	60 mm / 145 mm / 125 mm
重量	0.58 kg	0.58 kg	0.4 kg	0.58 kg	0.58 kg
セキュリティ機能					
ファイアウォールのタイプ	ステートフルインスペクション	ステートフルインスペクション	ステートフルインスペクション	ステートフルインスペクション	ステートフルインスペクション
パスワード保護	○	○	○	○	○
VPN 接続での製品機能	OpenVPN（SINEMA RC のクライアント）	OpenVPN（SINEMA RC のクライアント）	IPsec、OpenVPN（SINEMA RC のクライアント）	IPsec、OpenVPN（SINEMA RC のクライアント）	IPsec、OpenVPN（SINEMA RC のクライアント）
IPsec VPN データスループット	–	–	35 Mbit/s	120 Mbit/s	120 Mbit/s
VPN 接続数	0	0	20	200	200
ファイアウォール データスループット	600 Mbit/s	600 Mbit/s	100 Mbit/s	600 Mbit/s	600 Mbit/s
NAT/NAPT	○	○	○	○	○
暗号化アルゴリズム	–	–	AES-256、AES-192、AES-128、3DES-168、DES-56	AES-256、AES-192、AES-128、3DES-168、DES-56	AES-256、AES-192、AES-128、3DES-168、DES-56
認証プロシージャ	–	–	事前共有鍵、X.509v3 証明書	事前共有鍵、X.509v3 証明書	事前共有鍵、X.509v3 証明書
ハッシュアルゴリズム	–	–	MD5、SHA-1、SHA-256、SHA-384、SHA-512	MD5、SHA-1	MD5、SHA-1

SCALANCE M 産業用通信モデム

品名	SCALANCE M 無線		SCALANCE M 有線		
	M874-2、M874-3	M876-3、M876-4	M812/M816		M826
型式	6GK5874-2AA00-2AA2 6GK5874-3AA00-2AA2	6GK5876-3AA02-2BA2 6GK5876-4AA00-2BA2	6GK5812-1BA00-2AA2 6GK5816-1BA00-2AA2		6GK5826-2AB00-2AB2
伝送速度					
産業用イーサネット	10/100 Mbit/s		10/100 Mbit/s		
GPRS 伝送上り / 下り（最大）	85.6 Kbit/s	85.6 Kbit/s	–		–
EDGE 伝送上り / 下り（最大）	237 Kbit/s	237 Kbit/s	–		–
HSPA+ 伝送上り / 下り（最大）	5.76 Mbit/s	14.4 Mbit/s	–		–
EV-DO 伝送フォワードリンク / リバースリンク	–	3.1 Mbit/s / 1.8 Mbit/s（M876-3 のみ）	–		–
LTE 伝送上り / 下り（最大）	–	50 Mbit/s / 100 Mbit/s（M876-4 のみ）	–		–
ADSL2+ 伝送上り / 下り（最大）	–	–	1.4 Mbit/s / 25 Mbit/s		–
SHDSL 伝送（最大）	–	–	–		15.3 Mbit/s
インターフェース					
電気インターフェース数					
- 内部ネットワーク用	2	4	1	4	4
- 外部ネットワーク用	1	2	1	1	2
- 電源用	2	2	2	2	2
電気ポート接続					
- 内部ネットワーク用	RJ45（10/100 Mbit/s、TP、オートクロスオーバー）		RJ45（10/100 Mbit/s、TP、オートクロスオーバー）		
- 外部ネットワーク用	SMA アンテナソケット（50 Ω）		RJ45 DSL ポート	–	端子ストリップ
- 電源用	端子ストリップ			–	–
電源電圧					
電源電圧 / 範囲	10.8 ～ 28.8 V		10.8 ～ 28.8 V		
許容周囲条件					
動作時周囲温度 [℃]	-20 ～ +60		-0 ～ +60	0 ～ +60	-40 ～ +70
保管時周囲温度 [℃]	-40 ～ +85		-40 ～ +70	-40 ～ +70	-40 ～ +80
保護等級	IP20		IP20		
設計、寸法、および重量					
モジュールタイプ	コンパクト		コンパクト		
幅 / 高さ / 奥行き	35 mm / 147 mm / 127 mm		35 mm / 147 mm / 127 mm		
重量	0.4 kg		0.4 kg		
セキュリティ機能					
ファイアウォールのタイプ	ステートフルインスペクション		ステートフルインスペクション		
パスワード保護	○		○		
パケットフィルタリング	○		○		
VPN 接続	IPsec、OpenVPN（クライアント）		IPsec、OpenVPN（クライアント）		
VPN 接続数	20		20		
VPN での PSK タイプ認証	○		○		
鍵の長さ					
1	2	3（VPN の IPsec AES）	128 ビット	192 ビット	256 ビット	128 ビット	192 ビット	256 ビット		
IPsec 3DES / 仮想プライベートネットワーク	168 ビット		168 ビット		
VPN のメインモードインターネット鍵交換	○		○		
VPN のクイックモードインターネット鍵交換	○		○		
VPN のパケット認証タイプ	MD5、SHA-1、SHA-256、SHA-384、SHA-512		MD5、SHA-1、SHA-256、SHA-384、SHA-512		

通信プロセッサー
CP 1243-1、CP 1243-7、CP 1543-1、および CP 1543SP-1

品名	CP 1243-1	CP 1243-7	CP 1543-1	CP 1543SP-1
型式	6GK7243-1BX30-0XE0	6GK7243-7KX30-0XE0	6GK7543-1AX00-0XE0	6GK7543-6WX00-0XE0
伝送速度				
インターフェース 1 / 2	10/100 Mbit/s / –	–	10/100/1000 Mbit/s / –	10/100 Mbit/s
インターフェース				
電気インターフェース				
IE 準拠インターフェース 1	RJ45 ポート× 1	–	RJ45 ポート× 1	RJ45 ポート× 2 （BusAdapter を使用）
IE 準拠インターフェース 2	–	–	–	–
電源用	–	1	–	–
C-PLUG 対応	–		–	–
電源電圧				
電源電圧				
バックプレーンバス	DC 5V	–	DC 15V	–
外部	–	DC 24V	–	DC 24V
許容周囲条件				
周囲温度				
動作時				
- 垂直設置時	-20 ℃ ～ +60 ℃	-20 ℃ ～ +60 ℃	0 ℃ ～ +40 ℃	0 ℃ ～ +50 ℃
- 水平設置時	-20 ℃ ～ +70 ℃	-20 ℃ ～ +70 ℃	0 ℃ ～ +60 ℃	0 ℃ ～ +60 ℃
保管時	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃
輸送時	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃
保護等級	IP20	IP20	IP20	IP20
設計、寸法、および重量				
モジュールタイプ	コンパクト S7-1200、 シングル幅	コンパクト S7-1200、 シングル幅	コンパクト S7-1500、 シングル幅	ET 200SP 用 コンパクトモジュール
幅 / 高さ / 奥行き	30 mm / 110 mm / 75 mm	30 mm / 100 mm / 75 mm	35 mm / 142 mm / 129 mm	60 mm / 117 mm / 74 mm
重量	0.122 kg	0.133 kg	0.35 kg	0.18 kg
セキュリティ機能				
ファイアウォールのタイプ	ステートフルインスペクション	ステートフルインスペクション	ステートフルインスペクション	ステートフルインスペクション
VPN 接続	IPsec	IPsec	IPsec	IPsec
VPN 接続での 暗号化アルゴリズムのタイプ	AES-256、AES-192、 AES-128、3DES-168	AES-256、AES-192、 AES-128、3DES-168、 DES-56	AES-256、AES-192、AES- 128、3DES-168、DES-56	AES-256、AES-192、 AES-128、3DES-168、DES- 56
VPN 接続での認証方法のタイプ	事前共有鍵（PSK）、 X.509v3 証明書	事前共有鍵（PSK）、 X.509v3 証明書	事前共有鍵（PSK）、 X.509v3 証明書	事前共有鍵（PSK）、 X.509v3 証明書
VPN 接続での ハッシュアルゴリズムのタイプ	MD5、SHA-1	MD5、SHA-1	MD5、SHA-1	MD5、SHA-1
VPN 接続数	8	1	16	4
製品機能				
Web アプリケーションの パスワード保護	×	–	×	–
ACL – IP ベース	×	–	×	–
ACL – IP ベース （PLC/ ルーティング用）	×	–	×	–
不要なサービスの無効化	○	–	○	○
物理ポートによる通信のブロック	×	–	×	○
不正アクセスのログファイル	×	–	○	○

通信プロセッサー
CP 343-1 Advanced、CP 443-1 Advanced、および CP 1628

品名	CP 343-1 Advanced	CP 443-1 Advanced	CP 1628
型式	**6GK7343-1GX31-0XE0**	**6GK7443-1GX30-0XE0**	**6GK1162-8AA00**
伝送速度			
インターフェース 1 / 2	10/1000 Mbit/s / 10/100 Mbit/s	10/1000 Mbit/s / 10/100 Mbit/s	10/100/1000 Mbit/s / –
インターフェース			
電気インターフェース			
IE 準拠インターフェース 1	RJ45 × 1	RJ45 × 1	RJ45 × 2
IE 準拠インターフェース 2	RJ45 × 2	RJ45 × 4	–
バックプレーンバス			PCI Express × 1
電源用	2 ピンプラグイン端子ストリップ	–	2 ピン端子台× 1
C-PLUG 対応	○	○	
電源電圧			
電源電圧のタイプ	–	–	DC
電源電圧			
バックプレーンバスから 1 つ	DC 5V	DC 5V	
バックプレーンバスから 2 つ			3.3 V
外部	DC 24V	–	12 V
範囲	–	–	24 V 10.5 ～ 32 V
許容周囲条件			
周囲温度			
動作時		0 ℃ ～ +60 ℃	+5 ℃ ～ +55 ℃
- 垂直設置時	0 ℃ ～ +40 ℃	–	–
- 水平設置時	0 ℃ ～ +60 ℃	–	–
保管時	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-20 ℃ ～ +60 ℃
輸送時	-40 ℃ ～ +70 ℃	-40 ℃ ～ +70 ℃	-20 ℃ ～ +60 ℃
保護等級	IP20	IP20	–
設計、寸法、および重量			
モジュールタイプ	コンパクト	コンパクト S7-400 シングル幅	PCI Express × 1 (半分の長さ)
幅 / 高さ / 奥行き	80 mm / 125 mm / 120 mm	25 mm / 290 mm / 210 mm	18 mm / 111 mm / 167 mm
重量	0.8 kg	0.7 kg	0.124 kg
セキュリティ機能			
ファイアウォールのタイプ	ステートフルインスペクション	ステートフルインスペクション	ステートフルインスペクション
VPN 接続	IPsec	IPsec	IPsec
VPN 接続での暗号化アルゴリズムのタイプ	AES-256、AES-192、AES-128、3DES-168、DES-56	AES-256、AES-192、AES-128、3DES-168、DES-56	AES-256、AES-192、AES-128、3DES-168、DES-56
VPN 接続での認証方法のタイプ	事前共有鍵 (PSK)、 X.509v3 証明書	事前共有鍵 (PSK)、 X.509v3 証明書	事前共有鍵 (PSK)、 X.509v3 証明書
VPN 接続でのハッシュアルゴリズムのタイプ	MD5、SHA-1	MD5、SHA-1	MD5、SHA-1
VPN 接続数	32	32	64
製品機能			
Web アプリケーションのパスワード保護	○	○	–
ACL – IP ベース	○	○	–
ACL – IP ベース (PLC/ ルーティング用)	○	○	–
不要なサービスの無効化	○	○	–
物理ポートによる通信のブロック	○	○	–
不正アクセスのログファイル	×	×	–

SOFTNET Security Client および SINEMA Remote Connect

品名	SOFTNET Security Client	SINEMA Remote Connect	SINEMA RC Client
型式	**6GK1704-1VW04-0AA0**	**6GK1720-1AH01-0BV0**	**6GK1721-1XG01-0AA0**
伝送速度			
インターフェース 1 / 2	PC システムに依存		
セキュリティ機能			
ファイアウォールのタイプ	–	–	–
VPN 接続	IPsec	IPsec/OpenVPN	OpenVPN
VPN 接続での暗号化アルゴリズムのタイプ	AES-256、AES-192、AES-128、3DES、DES	AES-128、192、256: Advanced Encryption Standard（鍵の長さが 128 ビット、192 ビット、または 256 ビット、モード CBC） DES-EDE、DES-EDE3: Data Encryption Standard（鍵の長さが 128 ビット、または 192 ビット、モード CBC）	
VPN 接続での認証方法のタイプ	事前共有鍵（PSK）、X.509v3 証明書	証明書	証明書
VPN 接続でのハッシュアルゴリズムのタイプ	MD5、SHA-1	IPsec: SHA-1、256、384、512 OpenVPN: SHA-1、256、512	OpenVPN: SHA-1、256、512
VPN 接続数	無制限、またはコンピューターの設定に依存	無制限、またはターゲットシステムおよびネットワークに依存	SINEMA Remote Connect サーバーと 1:1 の関係

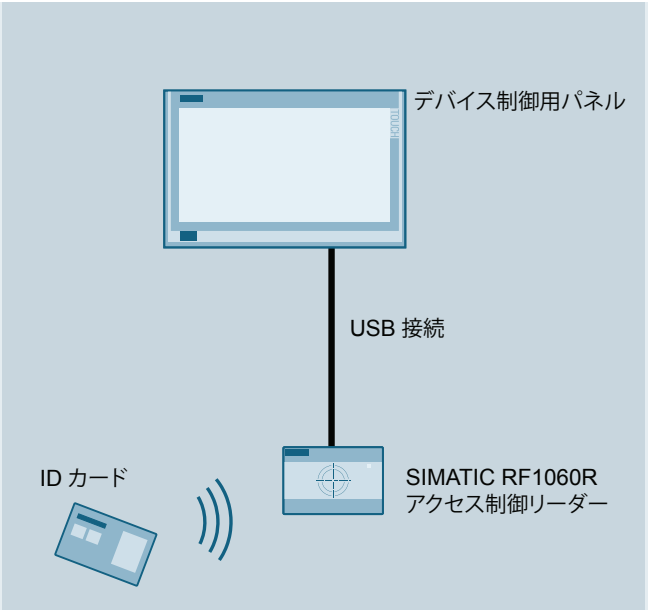
産業セキュリティ

IE RJ45 ポートロック

IE RJ45 ポートロック

IE RJ45 ポートロックによる物理的なネットワークアクセス保護
バランスの良い総合的なセキュリティコンセプトには、物理的な保護対策も含まれます。使用していない開いた RJ45 ポートを許可されていない人物に使用され、ネットワークにアクセスされてしまう、という問題が知られています。IE RJ45 ポートロックは、このリスクを低減するために開発されました。プラグインコネクタの形をしたポートロックの堅牢な設計で、RJ45 ポートを完全にふさぎます。これにより、RJ45 ケーブルの挿入を防止でき、ネットワークコンポーネント上の使用されていない RJ45 ポートを意図せず使用されることも防ぎます。RJ45 ポートロックの止め栓は、機械的なキーでしか解除できない内蔵型ロックでブロックされます。このポートロックは、RJ45 互換設計により工具を使わずに簡単に取り付けることが可能です。

SIMATIC RF1060R アクセス制御リーダー



既存の RFID ベース識別カードシステムでのマシンへのアクセス

SIMATIC RF1060R
セキュリティの必要性の高まりや、ドキュメント化の要件の増加により、マシンや機器へのアクセスをユーザーごとに制御できるソリューションが求められています。シーメンスの新しい SIMATIC RF1060R リーダーは、既存の従業員 ID をマシンの操作に使用する簡単な方法を提供します。これにより、細分化されたアクセスコンセプトの実装や、ユーザー固有の命令の保存などを 1 枚のカードで実現できます。既存の従業員 ID（ISO 14443A/B および ISO 15693）を使用することで、アクセス権を個別に制御できます。マシンや機器を操作する作業員の ID も、目的の検証や誤操作の防止に使用されます。コンパクトなデザインで、全体の奥行きも短い SIMATIC RF1060 リーダーは、既存のハードウェア（HMI デバイスや PC ベースのパネル）と組み合わせられるため、使い勝手が向上しています。高い保護等級（IP65、前面）と -25 ～ +55 °C の温度範囲により、過酷な産業環境でもマシンや機器に直接取り付けて使用できます。

SCALANCE X および SCALANCE W によるセキュリティ

SCALANCE X-200 シリーズ

SCALANCE W シリーズ

SCALANCE X

SCALANCE Xシリーズのマネージドスイッチは、ライン型、スター型、およびリング型構造に適しています。

SCALANCE X-200、X-300、X-400、および X-500 モジュールは、ネットワークアクセスを制御するとともに、以下のセキュリティ機能を備えています。

- ACL ポート /MAC、および IP ベース
- IEEE 802.1X (RADIUS)
- 802.1Q-VLAN – スイッチの既定ポート間でのデータトラフィックの論理分割が可能
- ブロードキャスト / マルチキャスト / ユニキャストリミッター
- ブロードキャストブロック

さらに、以下のセキュアなプロトコルがサポートされています。

- SSH (Telnet を代替)
- HTTPS (HTTP を代替)
- SNMP v3 (SNMP v1/v2 を代替)

SCALANCE W

WLAN 規格 IEEE 802.11n に準拠した、あらゆるオートメーションレベルに対応した信頼性の高い無線通信ソリューションである SCALANCE W (産業用無線 LAN) により、拡張性に富んだアプリケーションを実現できます。

SCALANCE W アクセスポイントおよびクライアントモジュールには、以下のセキュリティ機能が用意されています。

- IP ベースおよび MAC ベースのアクセス制御リスト (ZSL/ACL) による管理保護
- IEEE 802.1X (RADIUS)
- IEEE 802.11i 準拠のアクセス保護
- AES を使用した WPA2 (RADIUS) / WPA2-PSK

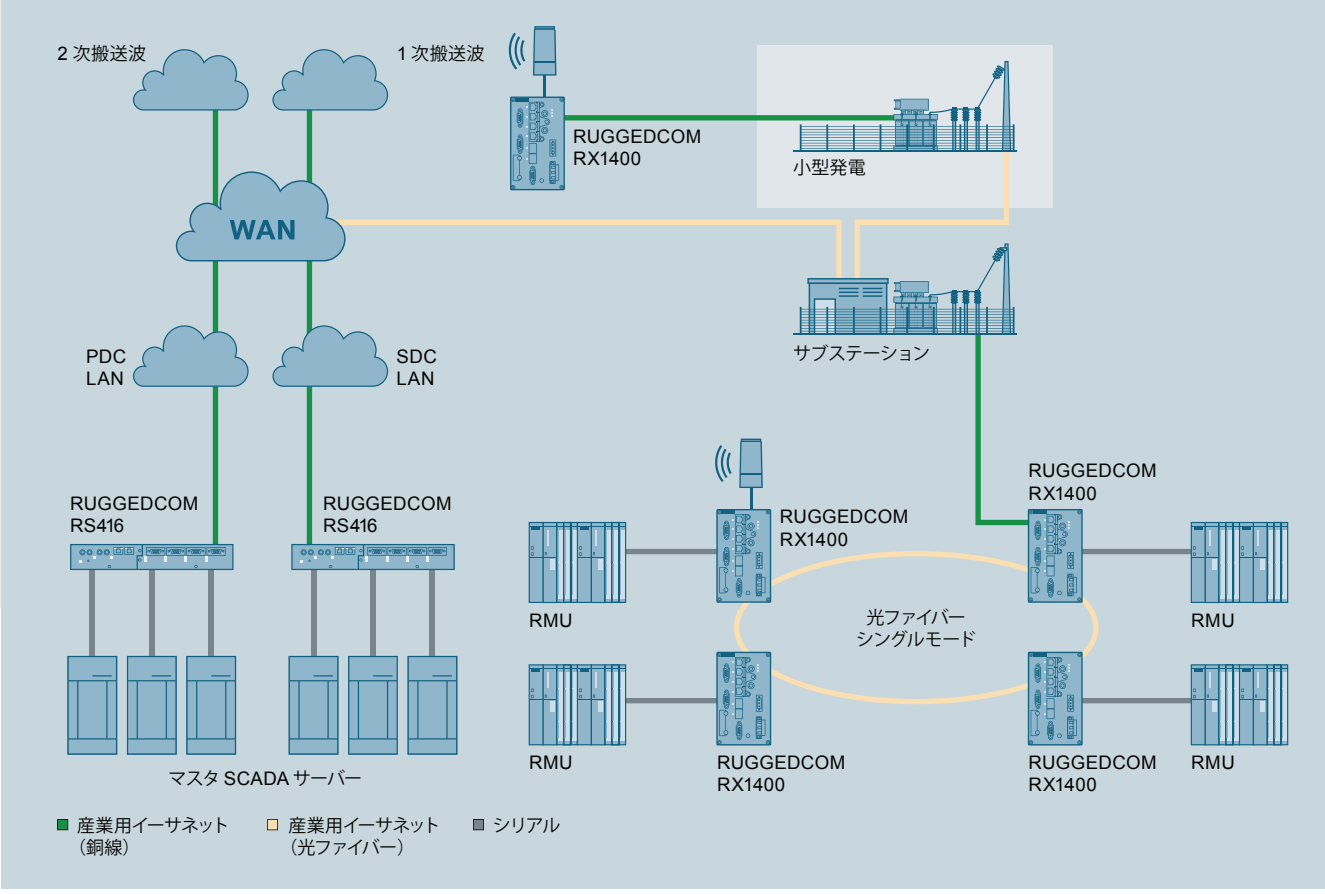
さらに、以下のセキュアなプロトコルがサポートされています。

- SSH
- HTTPS
- SNMP v3

Inter AP Blocking

ファームウェアバージョン 4.2 以降で使用可能です。
この機能によって、SCALANCE W のアクセスポイントが複数存在するネットワーク環境のセキュリティが強化されます。異なるアクセスポイントを使用し、レイヤー 2 ネットワーク (スイッチ) 経由で接続されている WLAN クライアントは、相互に直接通信できます。これにより、アプリケーションによってはセキュリティリスクが発生します。「Inter AP Blocking」を使用して、WLAN クライアントが通信を許可されている通信パートナーやゲートウェイを指定することで、セキュリティリスクを最小限にとどめられます。ネットワーク内の他のデバイスとの通信は、KEY-PLUG W700 セキュリティ (6GK5907-0PA00) を使用して防止されます。これは、KEY-PLUG スロットを搭載したすべての SCALANCE W アクセスポイントで使用可能です。

RUGGEDCOM によるセキュリティ

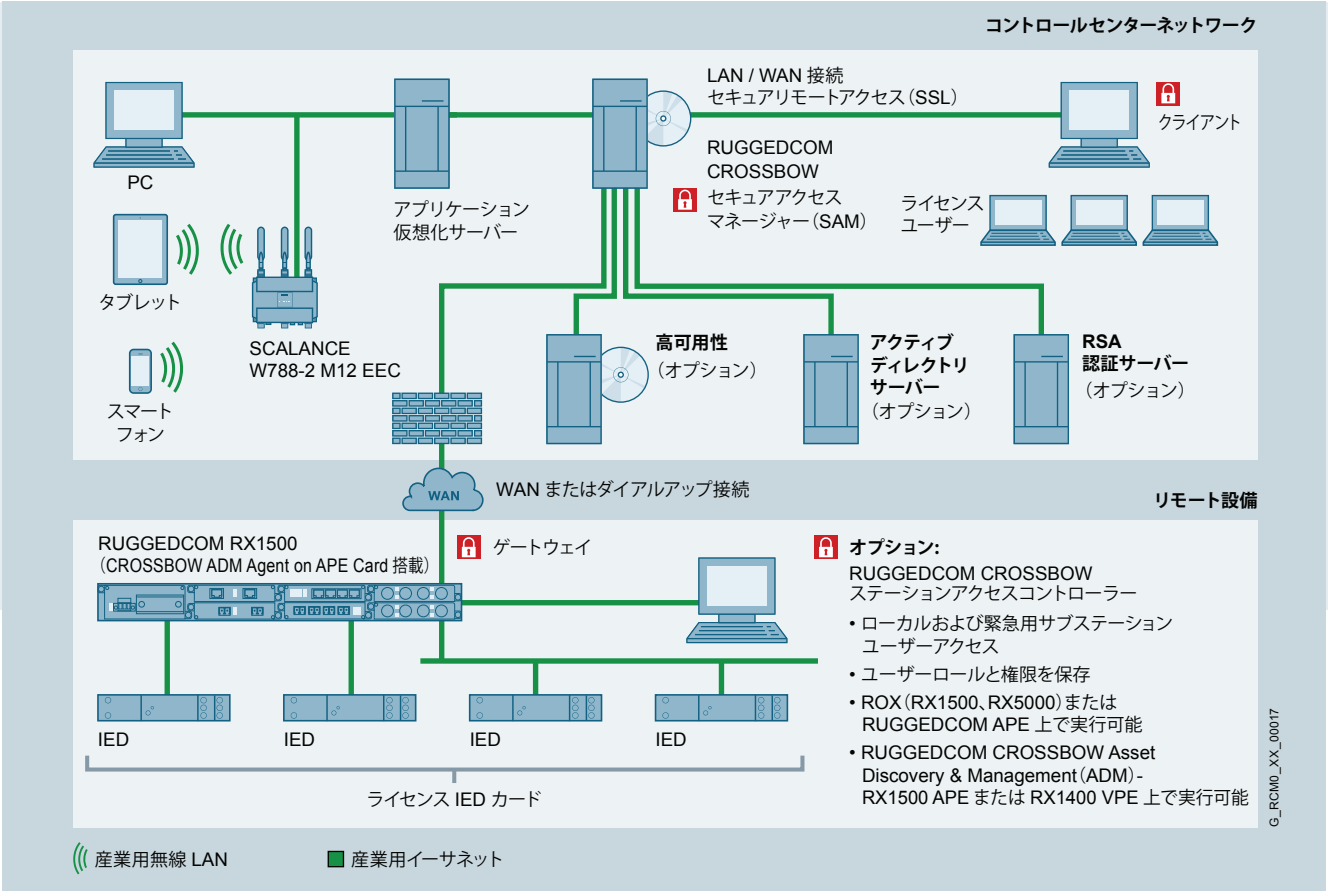


RUGGEDCOM RX1400 は、低圧変電所や分散型発電所の公衆モバイル無線ネットワーク経由での信頼性の高い接続を実現するのに適しています。

セキュリティ

電力セクターでは、セキュリティが特に重要です。オートメーションおよび通信ネットワークもミッションクリティカルなアプリケーションの重要な役割を担っており、高い可用性が非常に重要視されます。RUGGEDCOM RX1400 の以下の機能は、ネットワークレベルでのセキュリティの脅威を解決します。

- VPN（IPsec）– 内蔵されたハードウェア暗号化エンジンにより、メインプロセッサーを使用せずに非常に効率的な IPsec データ通信を実現
- パスワード – ACE RADIUS の認証オプションを含む、NERC ガイドラインに準拠しています。
- SSH / SSL – ネットワーク内での伝送時にパスワードとデータを暗号化するオプションを備えた、高度なパスワード保護
- ポートブロック – ポートをブロックする機能により、許可されていないデバイスによる使用されていないポートへの接続の確立を防止
- 802.1Q-VLAN – スイッチの設定でポート間でのデータトラフィックの論理分割が可能
- SNMPv3 – 暗号化された認証およびアクセス保護
- HTTPS – Web インターフェースへのセキュアなアクセス
- 802.1X – 許可されたフィールドデバイスのみがデバイスに接続可能
- MAC アドレスリスト – RADIUS をサポートしていないデバイスのアクセス制御



RUGGEDCOM CROSSBOW: アプリケーションの概要

システムアーキテクチャー

上の図は、RUGGEDCOM CROSSBOW を使用した公共事業の一般的なシステムアーキテクチャーを示しています。CROSSBOW セキュアアクセスマネージャー（SAM）は、すべてのリモートアクセス接続を確立する中央エンタープライズサーバーです。このサーバーは、インテリジェント電子デバイス（IED）の観点から、クライアントに対する唯一の信頼できるデータソースとしての役割を果たします。また、システムの心臓部として、ロールベースのアクセス制御や、Web サイトおよび IED アクセスの管理を行います。

リモート IED へのユーザーアクセスでは、CROSSBOW クライアントは SAM へのセキュアな SSL 接続を確立します。SAM は、RUGGEDCOM RX1500 やサポートされているその他のデバイスなどの、変電所のゲートウェイデバイスにセキュアな WAN 経由で接続されます。ゲートウェイは直接、または下位レベルのリモートターミナルユニット（RTU）経由で IED への接続を確立します。

また、CROSSBOW SAM では独自の直接モデムアクセスによる IED へのアクセスが可能です。この機能は鉄塔のアプリケーション、カウンターまたはプロセス制御、ステータスモニタリング用の IED、またはその他のホストコンピューター / サーバーなどに使用できます。CROSSBOW はセキュアな RBAC リモートアクセスをあらゆる IED に提供できるため、以下のような分野において、IED を使用したあらゆるアプリケーションにとって不可欠なツールとなります。

- 公共事業（電気、ガス、水道）
- 交通制御システム
- 工業および鉱業アプリケーション
- ビル管理システム

産業セキュリティサービス

生産現場やオフィスの相互接続が増加したことで、多くのプロセスが高速かつ簡単に行えるようになりました。同一のデータや情報を統一された方法で使用すると、相乗効果が生まれます。しかし、これによってリスクも高まります。

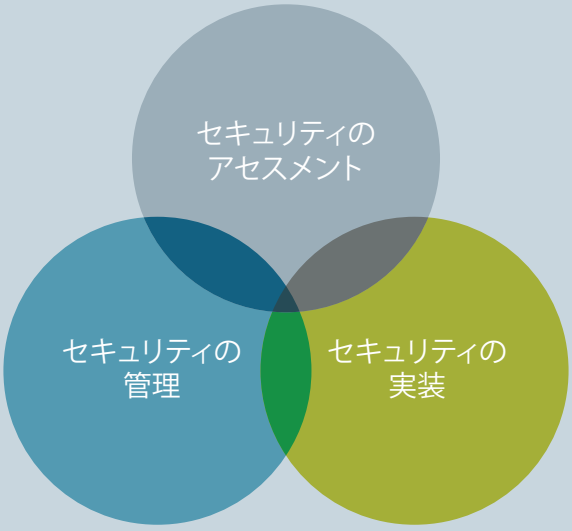
現在では、ウイルスやハッカー攻撃からの脅威にさらされているのはオフィス環境に限りません。生産施設においても、不正侵入、整合性への悪影響、およびノウハウの喪失のリスクがあります。そして多くの場合、セキュリティの弱点は一目でははっきりと分かりません。このため、プラントの稼動率を高いレベルで維持するには、既存のオートメーション環境のセキュリティを再検討して最適化することが推奨されます。

産業セキュリティサービスのポートフォリオは、多層防御コンセプトに基づいた戦略を検討、実装、および維持するための包括的な幅広い範囲の製品を提供します。この拡張性に富んだポートフォリオには、包括的なアドバイス（セキュリティのアセスメント）、技術的な実装（セキュリティの実装）、および継続的なサービス（セキュリティの管理）が含まれます。

セキュリティのアセスメント
セキュリティのアセスメントは、オートメーションシステム内の透明性を評価ベースで確認する複数のアセスメントで構成されています。ここでは、重要なコンポーネントの脆弱性を識別し、プロセスを入念に検査するために、お客様とともにシステムを分析します。

セキュリティの実装
セキュリティの実装は、生産施設のセキュリティレベルを向上させるセキュリティ対策の実装を意味します。ここでは、実際の攻撃を検出して防御できるシステムが設置されます。承認されていない人物が未知のウイルスやマルウェアを使用してシステムに侵入することを困難にする対策も盛り込まれます。

セキュリティの管理
セキュリティの管理によって、オートメーションシステムにおける既存のセキュリティ対策、パッチや脆弱性の管理、および障害処理を継続的にモニタリングし、定期的に調整や更新を行うことが可能になります。セキュリティ管理では、オートメーションに関するシーメンスの専門知識と、IEC 62443 および NERC-CIP 規格のベストプラクティスが組み合されます。



**リスクベースのセキュリティロードマップを策定する
セキュリティのアセスメント**

セキュリティのアセスメントには、包括的な脅威の分析、リスクの識別、および具体的なセキュリティ対策の推奨が含まれます。

- お客様のメリット：プラント特定のリスクベースのセキュリティロードマップにより、継続的に最適なセキュリティレベルを維持できます。

リスク削減対策としてのセキュリティの実装

セキュリティの実装は、プラントおよび生産施設のセキュリティレベルを向上させるセキュリティ対策の実装を意味します。

- お客様のメリット：技術的かつ組織的な対策により、セキュリティギャップの発生を防止し、サイバー犯罪からの保護を強化します。

包括的かつ継続的な保護を可能にするセキュリティの管理

セキュリティの管理は、シーメンスのセキュリティツールを使用した、既存のセキュリティ対策の継続的なモニタリング、定期的な調整および更新を意味します。

- お客様のメリット：機密性の高い産業用機器での使用に最適化された当社のセキュリティツールにより、お客様のプラントのセキュリティステータスに関する透明性を最大限に高め、可能性がある脅威のシナリオを事前に想定して防ぎます。

用語、定義

サイバーセキュリティ
サイバーセキュリティはコンピューターセキュリティ、または IT セキュリティとも呼ばれ、ハードウェア、ソフトウェア、情報、およびコンピューターベースのシステムに提供されるサービスを盗難、破壊、または悪用から保護することを意味します。

非武装地帯（DMZ）
非武装地帯（DMZ）は、セキュリティを考慮して、サーバーへのアクセスが制御されるコンピューターネットワークを意味します。DMZ 内のシステムは、ファイアウォールによって他のネットワーク（インターネットや LAN など）から分離されます。これによって外部サービス（電子メールなど）へのアクセスは可能にしつつ、内部ネットワーク（LAN）を不正アクセスから保護します。可能な限りセキュアに、WAN（インターネット）と LAN（イントラネット）の双方からコンピューターネットワークサービスを利用できるようにすることが重要です。DMZ による保護は、システムを複数のネットワークから隔離することで可能になります。

ファイアウォール
指定されたセキュリティ制限に基づき、相互接続されたネットワーク間でのデータ通信を許可または遮断するセキュリティコンポーネントです。データ通信の許可および遮断は、ファイアウォールルールを設定することで行えます。このため、たとえば特定の PC のみが特定のコントローラーにアクセスできるような指定が可能です。

産業セキュリティ
産業セキュリティは産業現場における情報やデータおよび知的財産を処理・伝送・保存というプロセスを通じて保護することを意味し、その可用性、整合性、および機密性が保護されます。産業セキュリティの目的は、攻撃、脅威、危険、および経済的損失を防ぎ、リスクを最小限にとどめることです。IEC 62443、ISO/IEC 27000、ISO/IEC 15408、および施行されている国の法律（例：ドイツの連邦データ保護法）など、さまざまな国家および国際規格で指針が示されています。

ポートセキュリティ
アクセス制御機能により、個々のポートを不明なノードから遮断できます。ポートでアクセス制御機能が有効である場合、不明な MAC アドレスから到達したパケットは直ちに破棄されます。既知のノードから到達したパケットのみが許可されます。

RADIUS（IEEE 802.1X）：
外部サーバーによる認証
RADIUS のコンセプトは、中央認証サーバーに基づいています。ターミナルデバイスは、デバイスのログオンデータが認証サーバーによって検証されるまで、ネットワークまたはネットワークリソースにアクセスできません。また、ターミナルデバイスと認証サーバーの両方が、拡張認証プロトコル（EAP）をサポートしている必要があります。

システムハードニング
システムハードニングには、不要なインターフェースおよびポートの無効化が含まれます。これによって、ネットワーク内外からの攻撃に対する脆弱性が低減されます。制御システム、ネットワークコンポーネント、PC ベースのシステム、プログラマブルロジックコントローラーなど、オートメーションシステムのすべてのレベルを考慮します。

仮想プライベートネットワーク（VPN）
VPN は、2 つ以上のネットワークノード（セキュリティコンポーネントなど）、およびそのノードの内側のネットワークセグメントを接続します。この VPN 内のデータを暗号化することで、セキュアでないネットワーク（インターネットなど）経由での伝送時でも、第三者はデータの盗聴や偽造ができません。

仮想 LAN（VLAN）
VLAN（IEEE 802.1Q）は、スイッチのあらかじめ定義されたポート間でのデータトラフィックの論理分割を可能にします。これにより、同一の物理ネットワーク上で複数の「仮想」ネットワークを構築できます。データ通信は、VLAN 内でのみしか行えません。

ホワイトリスト
ホワイトリスト（ポジティブリスト）は、信頼できると分類されるエレメントの集合を意味します。対象は個人、企業、またはプログラムなど、多岐にわたります。PC のホワイトリストでは、本当に必要なプログラムしか実行できないよう制御されます。

産業セキュリティの
すべてをご紹介します：

- 当社のセキュリティ製品およびサービスの概要
- 産業セキュリティ分野の最新技術
  www.siemens.com/industrial-security

Industrial
Security –
take a look!

以下のメディアでシーメンスをフォローしてください：

twitter.com/siemensindustry

youtube.com/siemens

製品に関する国内お問い合わせ先

製品の詳細およびお問い合わせ先は弊社ホームページにてご案内しております。
www.siemens.com/jp/ad

Siemens AG Industry Online Support

全てのマニュアル（一部日本語版あり）を登録不要・無料で
ダウンロードしていただけます。
https://support.industry.siemens.com

⚠ 安全に関するご注意

本カタログに記載された製品を正しくお使いいただくため
ご使用の前に必ず「取扱説明書」をよくお読みください。

2018年8月改訂（1808STA1K）