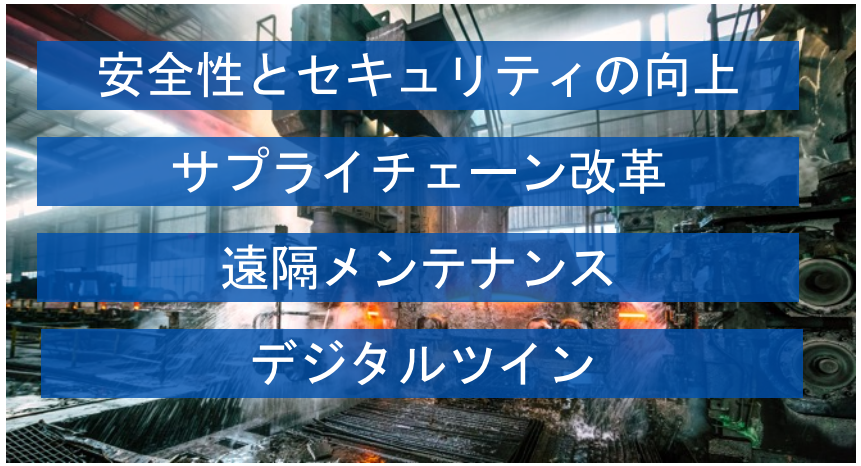
生産性向上に繋がる
新しいネットワークの姿とセキュリティ

中川 貴博

シスコシステムズ合同会社
I-IoT 事業部 IoT Product Sales Specialist

制御ネットワークからデータ活用のネットワークへ

生産現場の改善計画



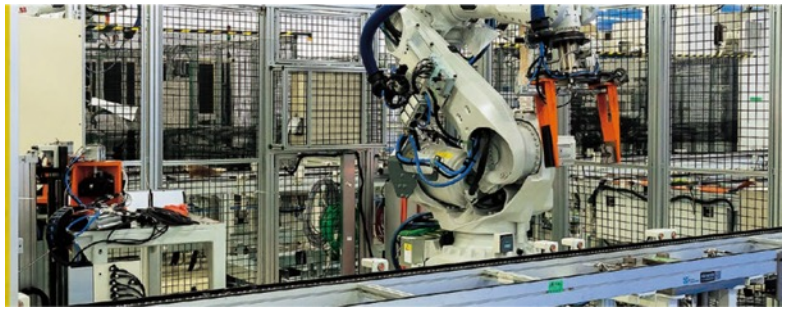
シスコ主要顧客の工場インフラ投資と導入効果

バッテリー工場 歩留まり改善	2021年、新工場構築後、2年以内に、旧工場と比較して、85%の歩留まり改善を達成。 背景として、「データアクセシビリティ」および「迅速な改善」の目標指標の策定があった。
海外完成車メーカー ダウンタイムの削減	「ギガファクトリー」、「アンボックストプロセス」といった様々な挑戦を支えるネットワークとして採用 迅速な工程変更やダウンタイムの削減に貢献。
海外完成車メーカー 運用の効率化 保守部材の削減	ネットワーク単独でのROIの算出を行い、標準化を実施。 予備品の在庫数の削減でコストをカット。 また、ネットワーク運用ツールを使い、設定作業を全てテンプレート化し、運用を改善。
国内完成車メーカー データの収集 セキュリティ対策 高速化	幹線ネットワークの10G化とセキュリティ対策を実施。 未許可の端末のネットワークへの接続防止や通信の可視化を行う。 またAGV向けに超低遅延無線を導入。

日産自動車株式会社

「生産技術のインテリジェント化」を目指し 最新技術を採用したIoTネットワークを構築

「クルマの未来」を提案し続ける日産自動車。同社は、新型クロスオーバーEVの生産ラインで、IoTを活用した生産技術革新に取り組んでいます。シスコのネットワーク製品による制御で、ITとOT（生産技術）を融合。「ニッサン インテリジェントファクトリー」の先駆け的取り組みとして期待されています。



課題

- 労働集約型の生産を脱却しつつ“匠”の技術を継承するため、**ロボットやIoTを活用した生産技術のインテリジェント化が重要に**
- 様々な機器やデジタル技術を工場に導入する際は、それらの**稼働を見える化し、適切に管理・制御する仕組みが不可欠**
- 生産ラインはビジネスの生命線であり、稼働を支えるIoTネットワークにも、**高い安定性・信頼性・拡張性**が求められる

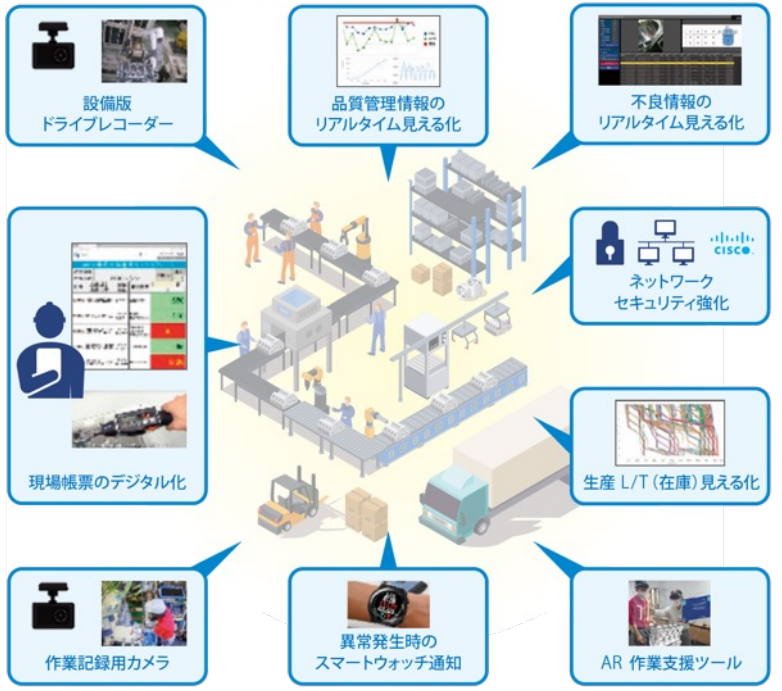
ソリューション

- **製造業界向けの多彩な製品ポートフォリオとグローバルの実績で培った技術力**を評価
- 産業用イーサネットスイッチのCisco IEシリーズをベースに、**生産系と情報系を連携した統合ネットワークを構築**
- Cisco Industrial Network Director（IND）とCisco Identity Services Engine（ISE）を活用した**IoTネットワーク接続デバイスのセキュリティ管理を実現**

結果～今後

- 正式稼働に向け、新ネットワークを活用した**e-パワートレイン自動生産ラインの立ち上げ作業が進行中**
- 新ネットワークは生産ラインのテスト段階から活用し、**品質課題や設備稼働ロスなどの洗い出し・改善**を進めている
- 情報系ネットワークとの連携メリットを活かしたリモートコミュニケーションを実施。**コロナ禍でも現場業務を継続**
- 栃木工場で実現した**ネットワークデザインを標準化し、統一されたポリシーをグローバルに展開**していく

栃木工場に適用されている様々な最新テクノロジー



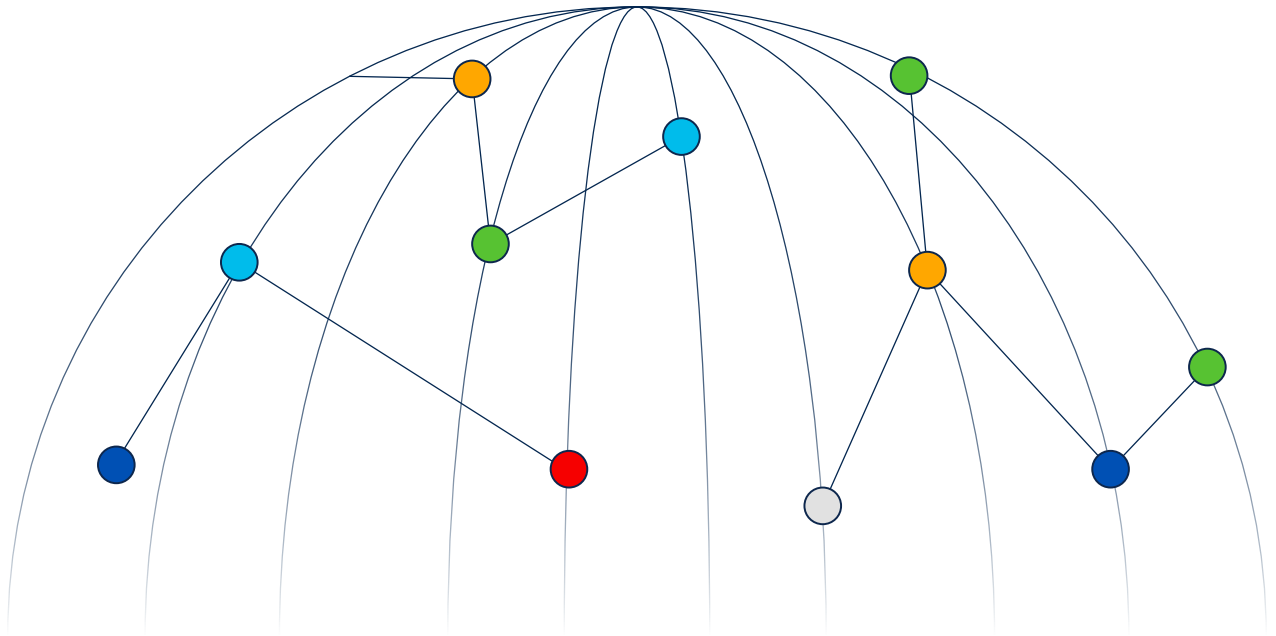
Why Cisco?

> 最新のデジタル技術をキャッチアップして生産技術をインテリジェント化していく。これが次世代のクルマづくりのカギになっています。この活動を推進する上で、ネットワークは極めて重要な役割を担います

― 日産自動車株式会社 パワートレイン技術企画部 主管　村井 勇一氏

詳細はこちら 》》 https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2171-nissan.htm

データ活用のための工場ネットワーク

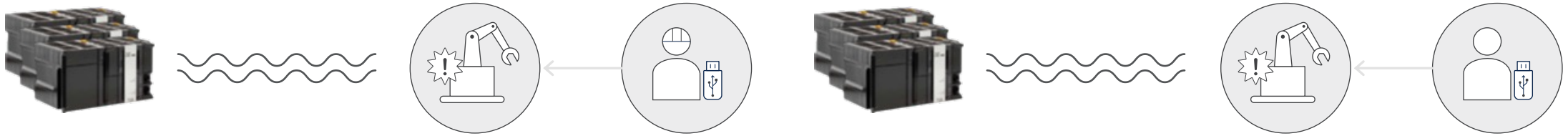


イーサネット技術活用によるデータ収集

データ収集を進めるためにシリアル通信をイーサネット通信へと変更することを進めています。

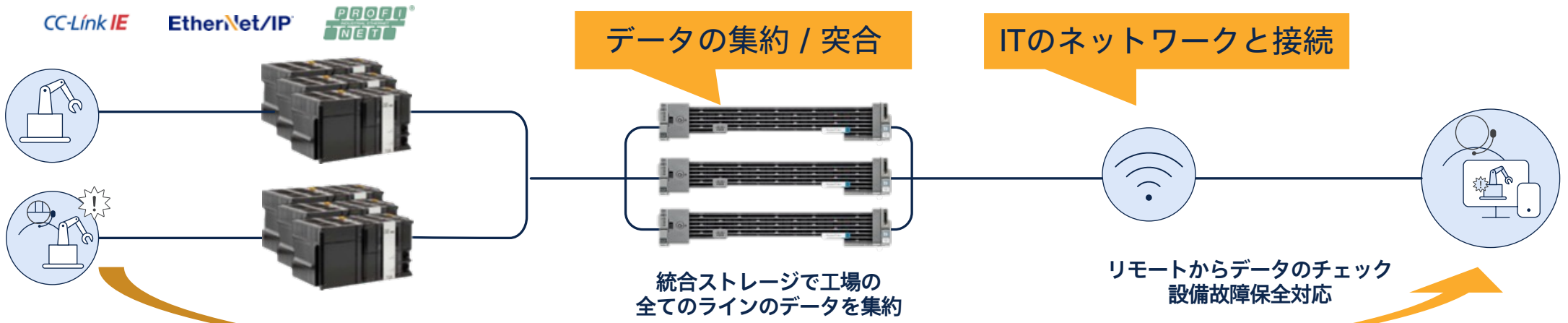
シリアル通信

転送速度が遅いので、設備のデータは現場まで向かって収拾



イーサネット通信

設備データも高速に転送できるので、統合ストレージに集中して保存できる

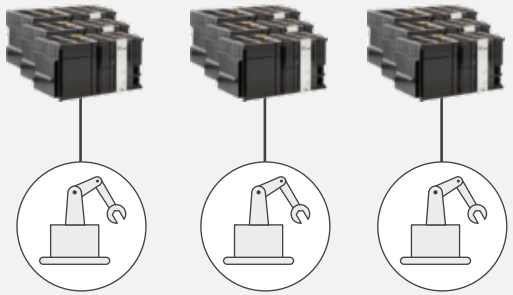


イーサネット技術活用による解決

複数のメーカーの機器が混在しているネットワーク構成を一本化することで、機器の節約、メンテナンス性の向上、
ケーブリングコストの削減を実現します。

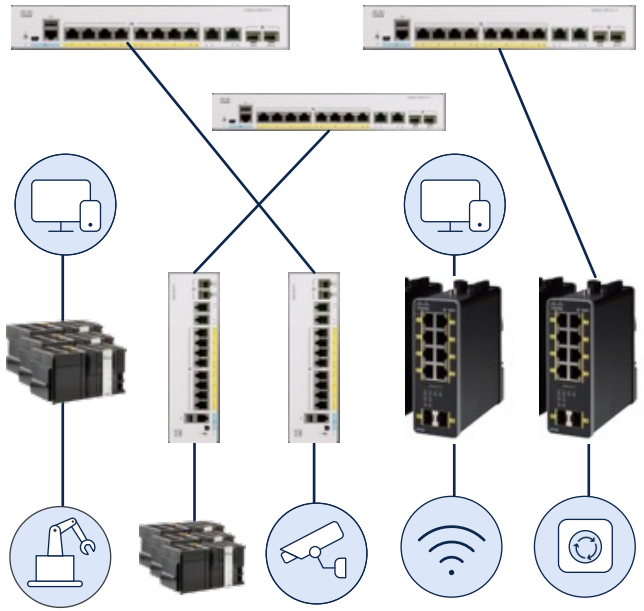
シリアル通信

転送速度が遅いので、
設備のデータは現場まで向かって収拾



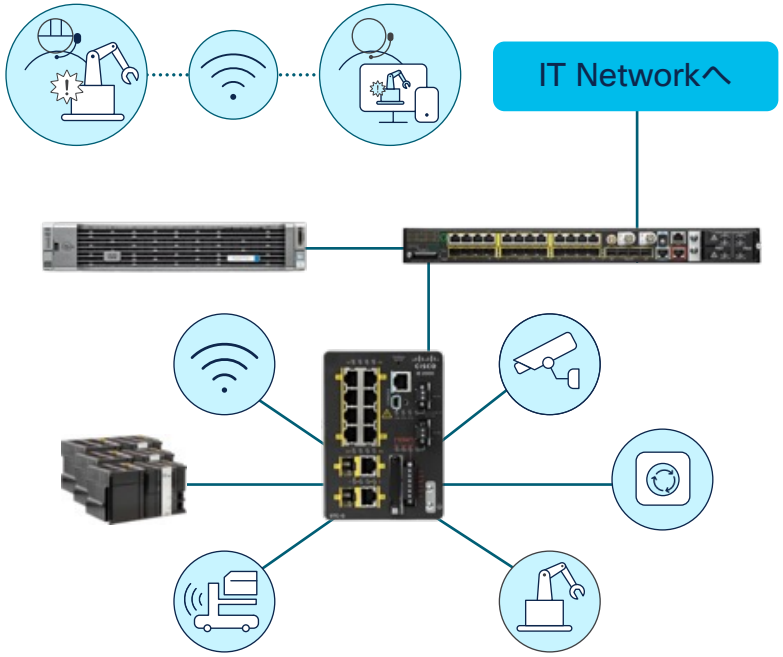
1:1の通信形態のため台数が増える

個別ネットワーク



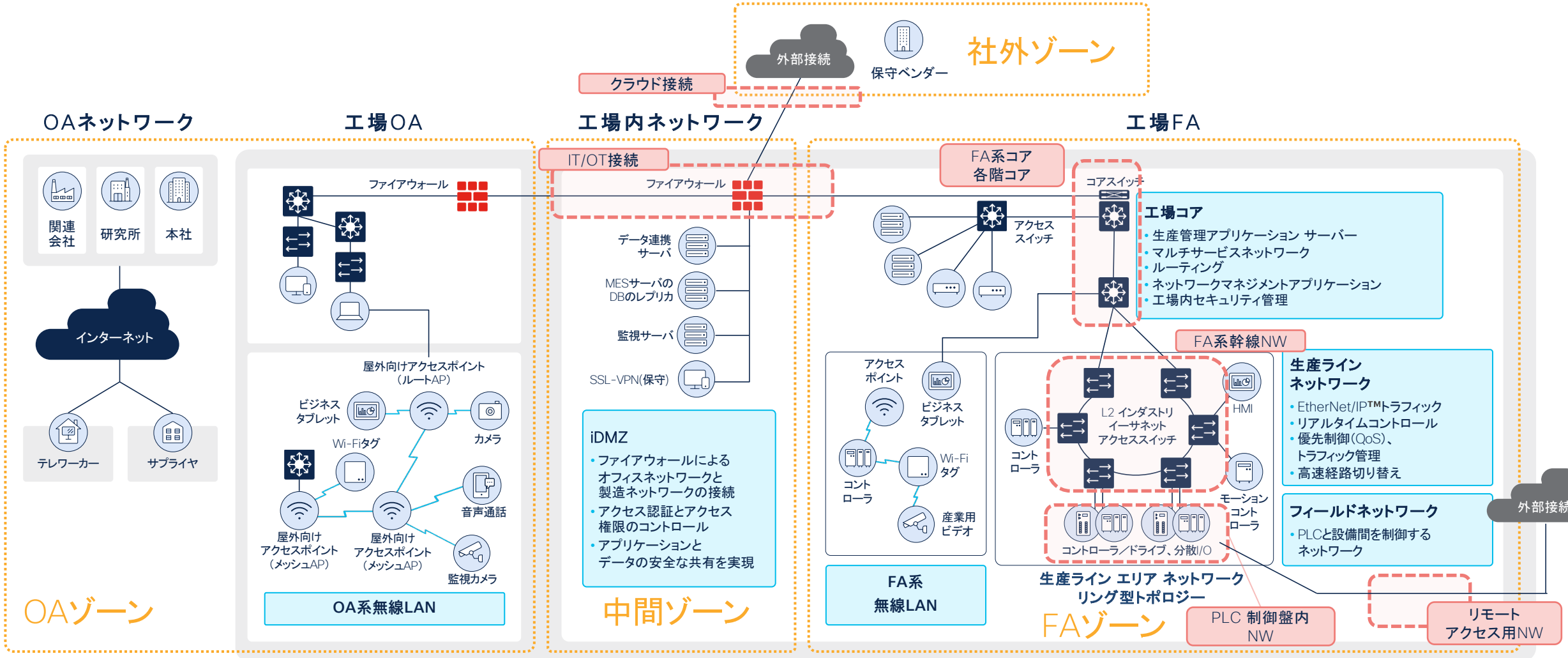
「部署が違う」「繋ぐものが違う」「施工業社が違う」
様々な理由でネットワークはバラバラに
ひかれてしまう為、監視管理が不可能
→ネットワーク不具合発生時の対応困難

統合ネットワーク



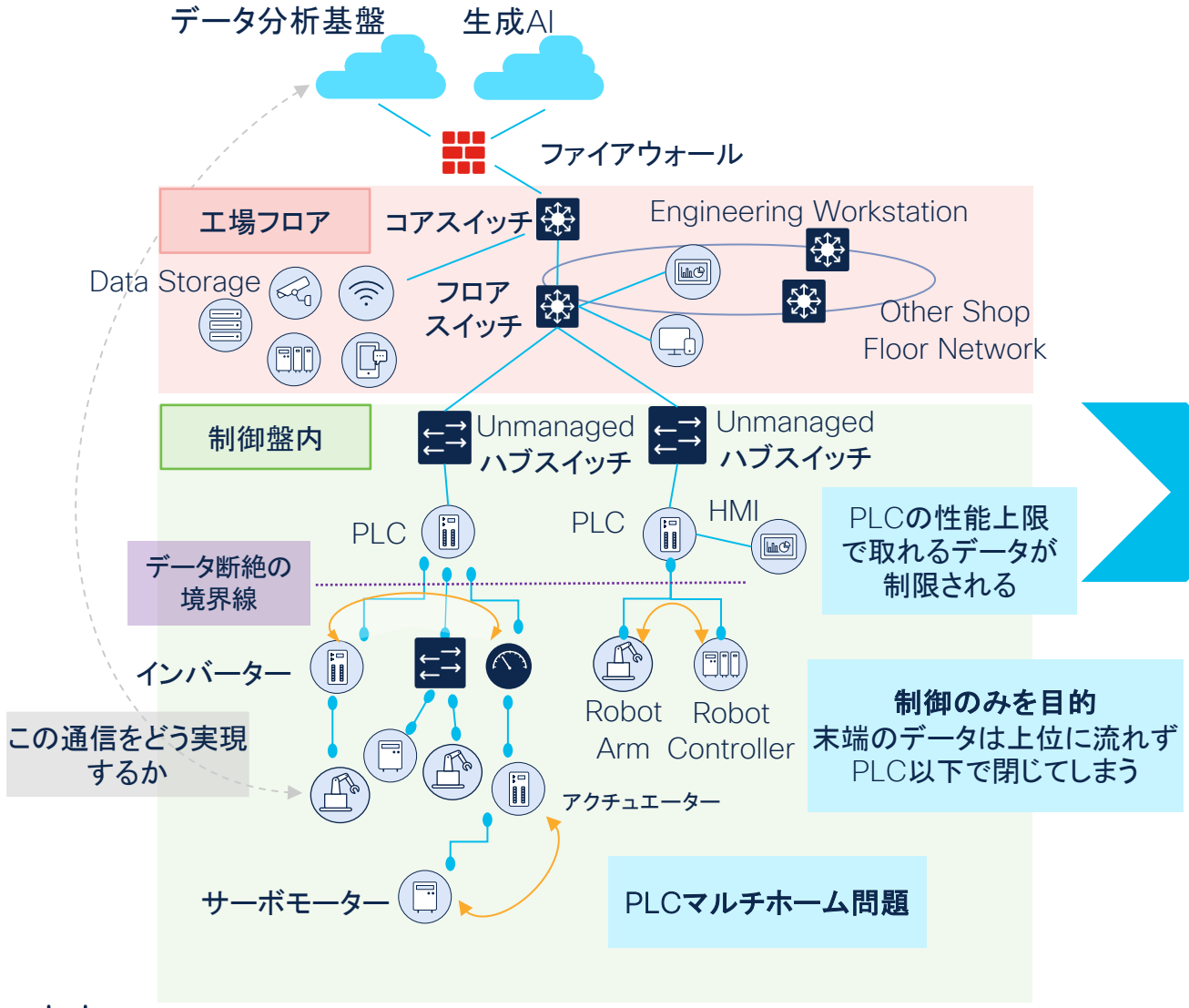
スイッチやPLCの台数節約→消費電力削減
セキュリティ機能
高速通信（アプリケーションサクサク）
工場全体での設計が大事

新工場ネットワークモデル（論理図）

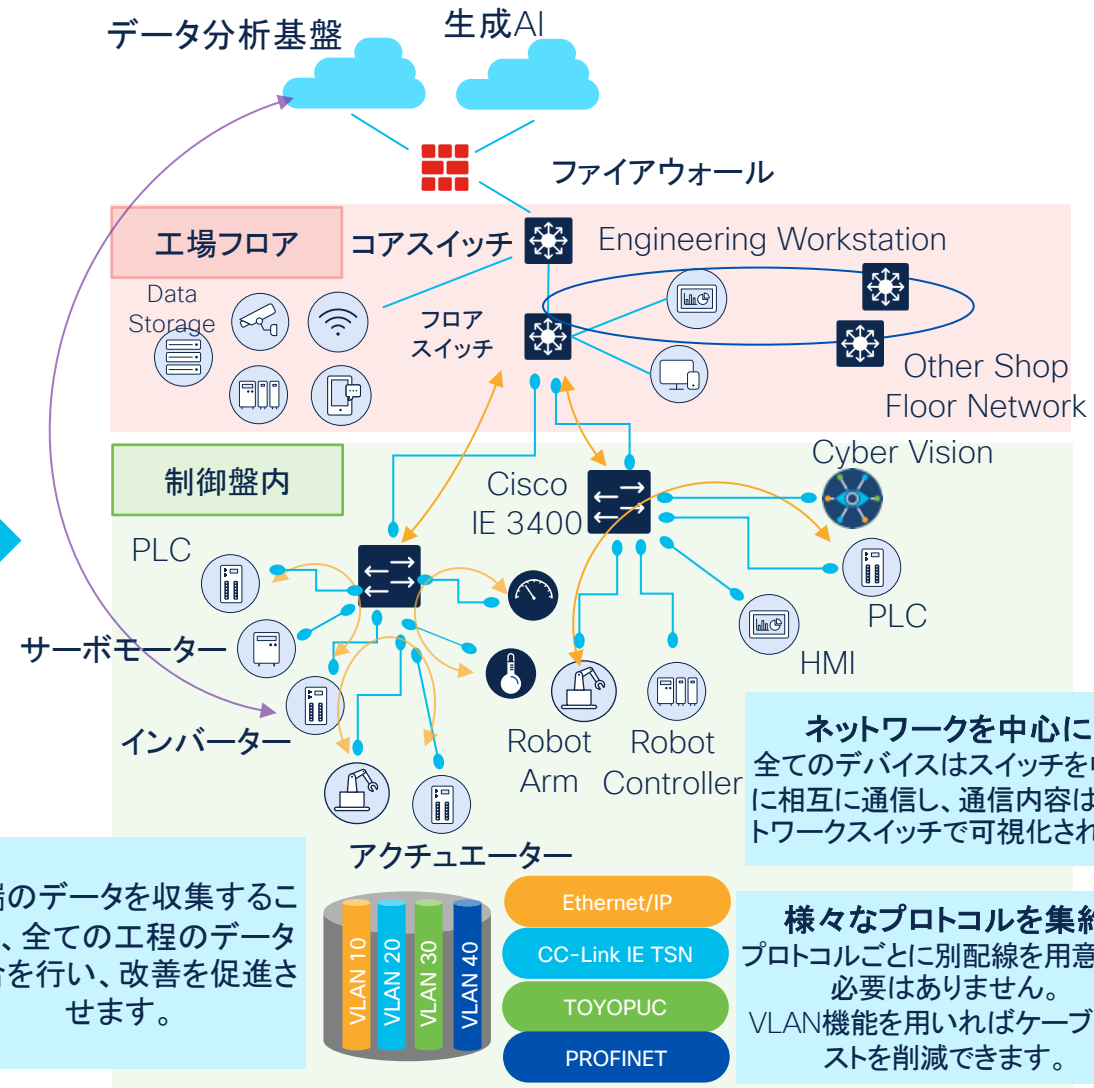


データ活用のためのネットワーク構成

As-Is: 制御中心のネットワーク

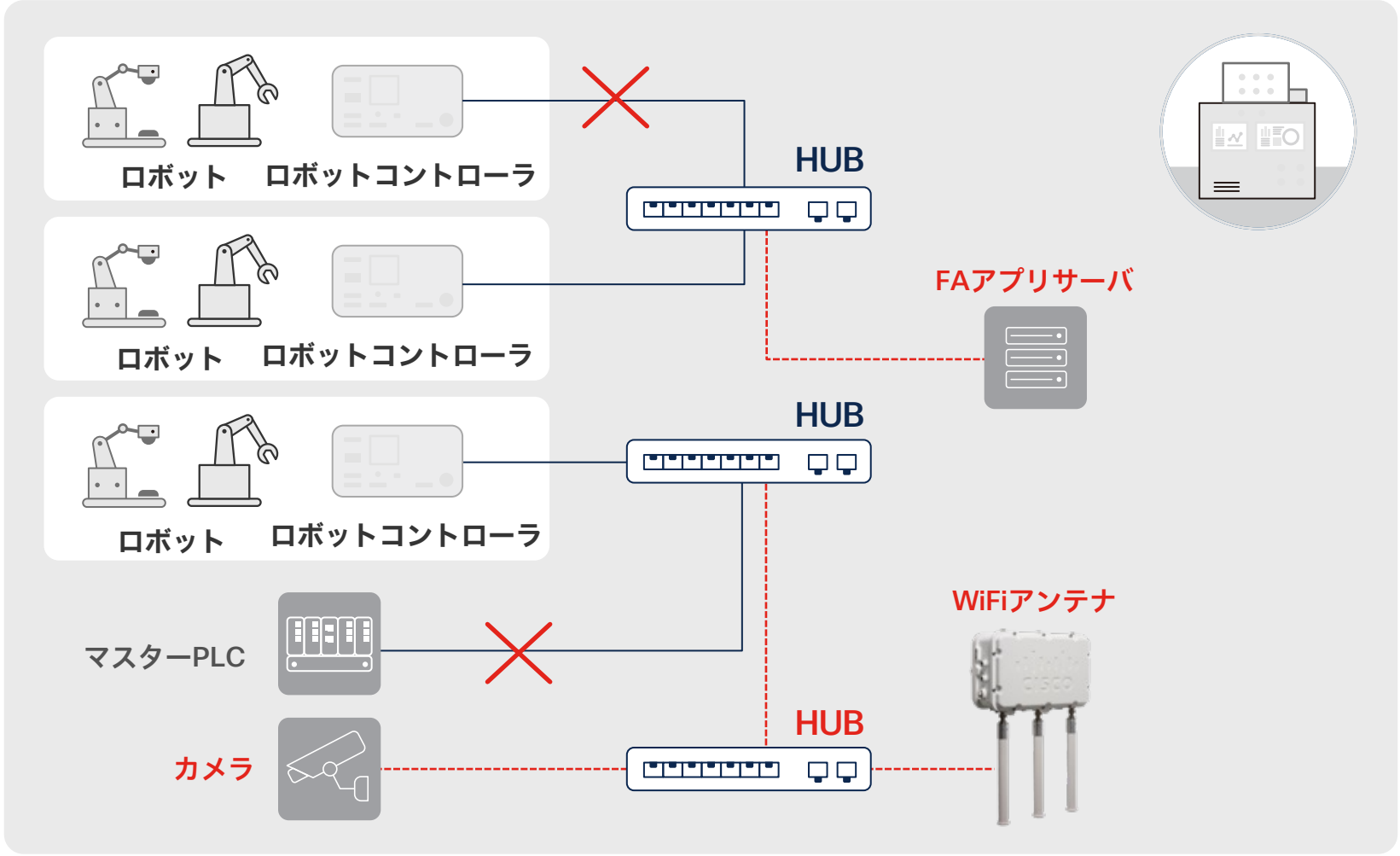


To-Be: 制御&データ活用



アンマネージドハブでは多くの要件に対応が出来ない

工場の高度化に向けて既存のネットワークに新たなアプリケーションやカメラなどを追加・接続する際、
ネットワーク遅延など新たな問題が生じることがあります。



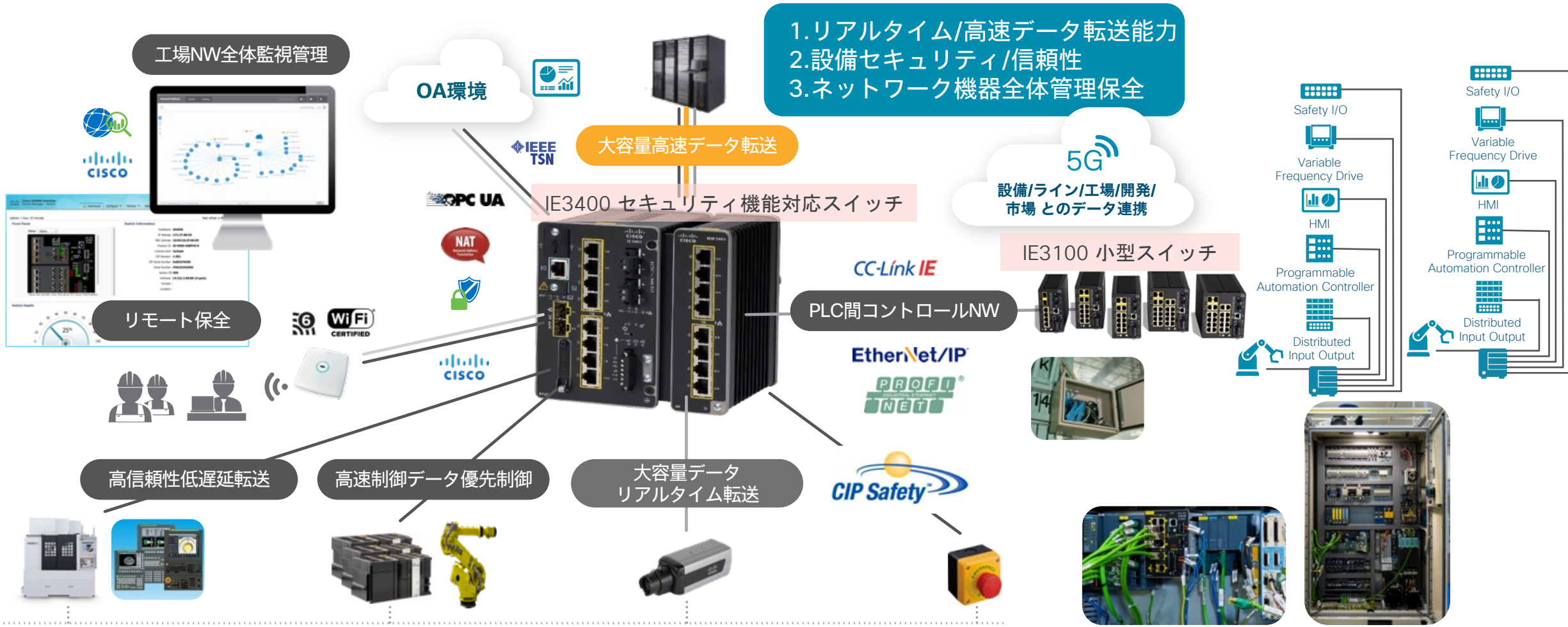
- ✕ 設備制御パケット損失が起きる
- ✕ 波形データがサーバ転送遅延する
- ✕ 高精度画像／動画転送が遅い
- ✕ 設備通信異常原因が特定できない
- ✕ 新機能（PC/CPU）追加ができない
- ✕ IPアドレス／設備接続数が不明

外部（オフィス / 在宅 / 設備メーカ / クラウド）接続

工作機 / PLC / ロボット / AGV / 電子工具データ統合

工場の現場に求められる「ネットワークのハブ」の役割

作業現場において、産業用スイッチはこれまで「制御系ネットワークのハブ」としての役割を果たしてきました。しかし、今後は工場のネットワーク化にともない、「情報インフラネットワークのハブ」としての機能も求められます。「リアルタイム/高速データ転送能力」「設備セキュリティ/信頼性」「ネットワーク機器全体管理保全」といった、OTとITのゲートウェイとして新たな技術に対応しうる機能が必要となります。



検証済みガイドを活用して、ネットワークデザインを実行

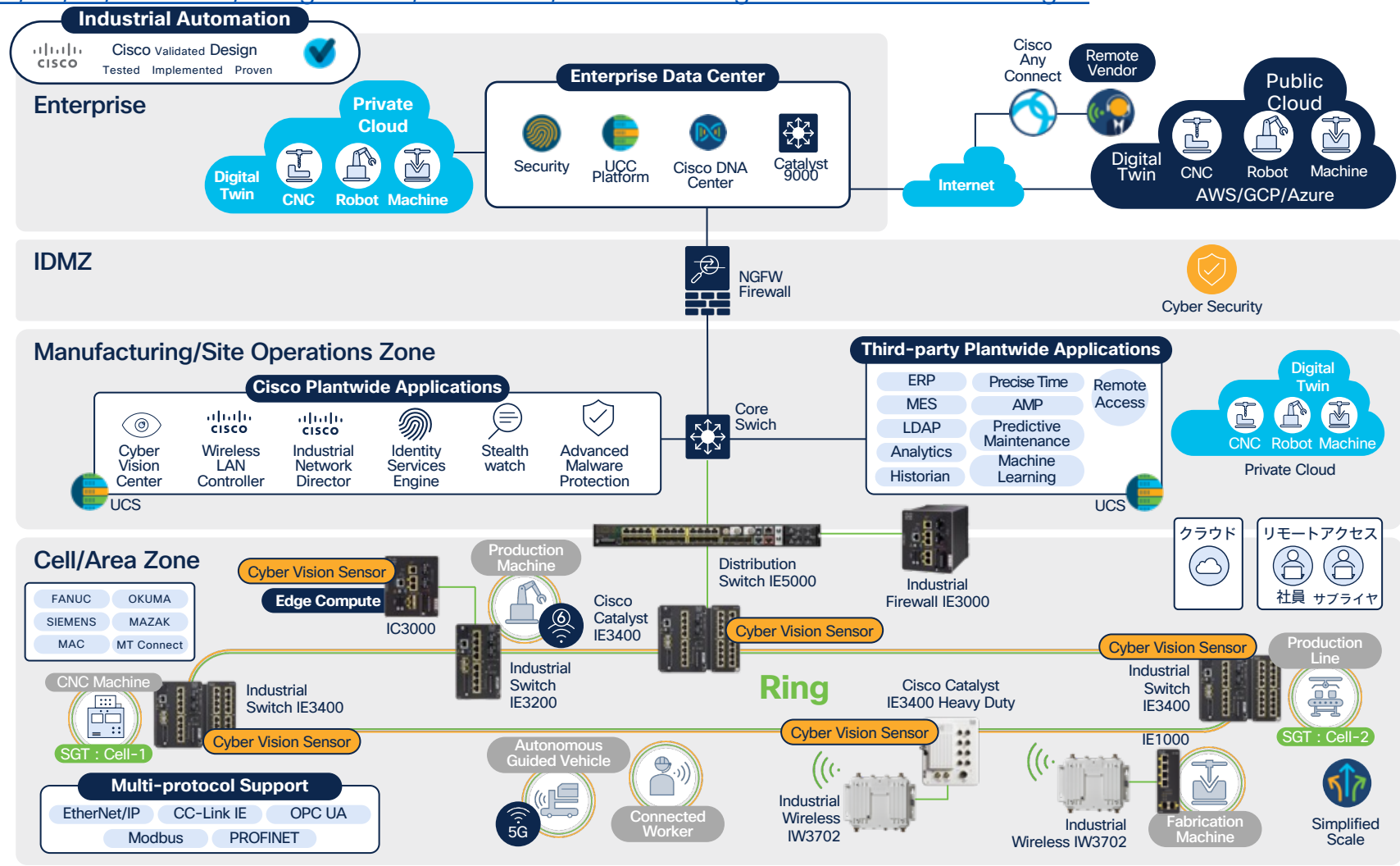
Industrial Automation Cisco 検証済みデザイン
https://www.cisco.com/c/en/us/solutions/design-zone/industries/manufacturing.html#~validated-designs

1
シスコは、
産業ネットワークにおける
信頼できるリーダーです

2
シスコは、
ITとOT（およびそれらの
統合）を理解していま
す。

3
開発するすべてのものに
堅牢なセキュリティが
組み込まれています。

4
シスコは
産業用ワイヤレス特有の
課題を理解しており、
それを解決することが
できます。



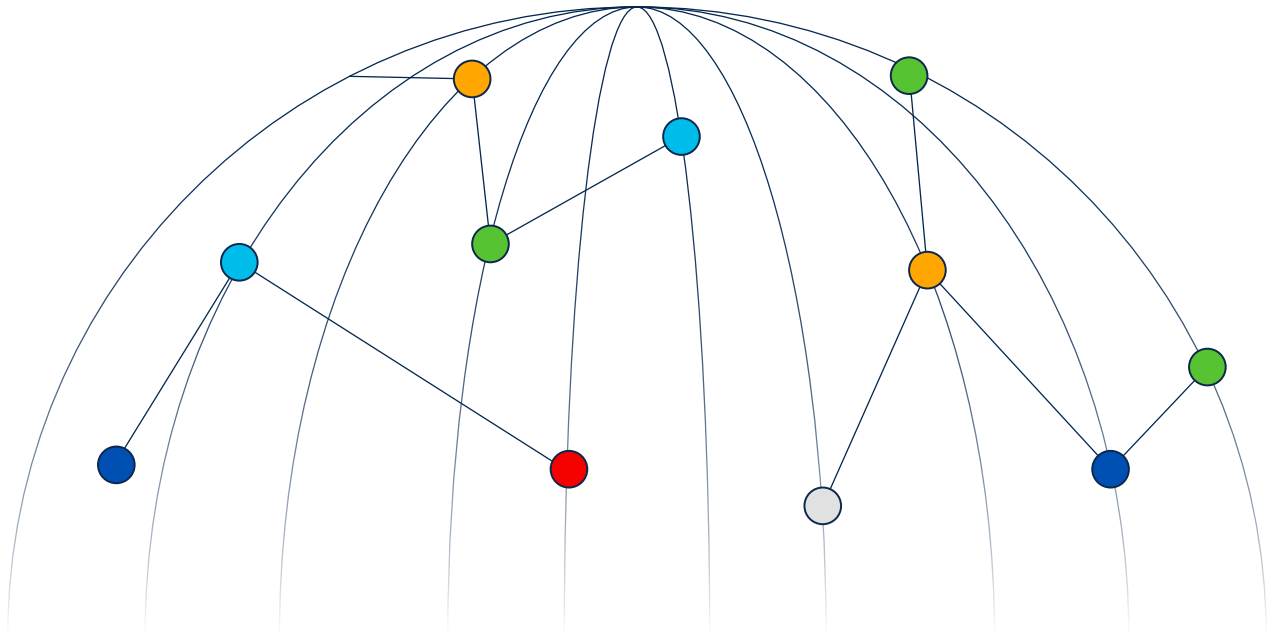
IT/OTネットワーク統合
- i-DMZ(IT/OT-GW)設計
- 工場セキュリティデザイン
- 生産設備NW運用管理

IoTデータプラットフォーム
- 設備Edge Computing
- 生産App-Data Storage
- 生産Appコンテナ Platform

設備データインフラ設計
- 制御/生産IoT-NW統合
- 生産設備セキュリティ
- 産業プロトコル(CIP等)

Proven to work with: Rockwell Automation SIEMENS Schneider Electric MITSUBISHI ELECTRIC

工場のセキュリティ対策



IEC62443への準拠方法をドキュメントで公開中

ホワイトペーパー

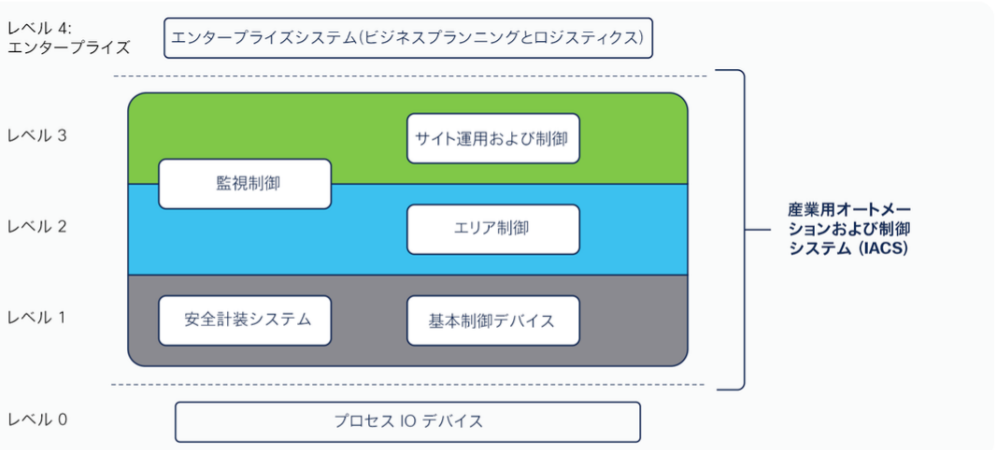
Cisco public

産業用オートメーション および制御システムを保護する サイバーセキュリティ フレームワーク

ISA/IEC-62443-3-3

ゾーンとコンジット

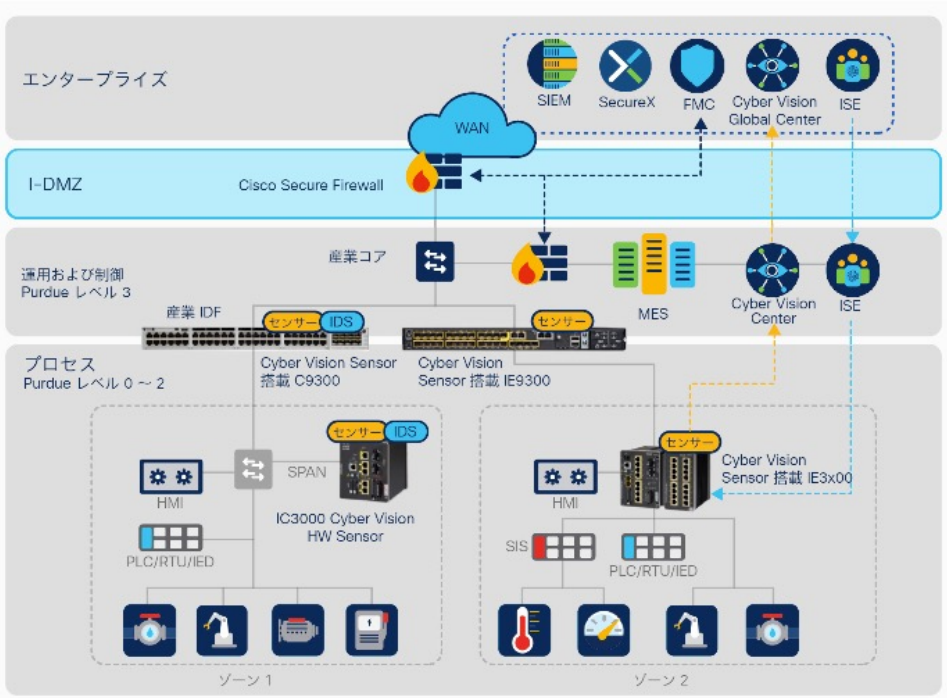
ISA/IEC-62443 は、これらの原則に基づいて、ISA95 で使用される Purdue 参照モデル（図 1）を活用し、これらの機能レベルをゾーンとコンジット（図 2）にセグメント化する産業用制御システムアーキテクチャを提案しています。セグメンテーションは、ISA/IEC-62443-3-2 に規定されているセキュリティリスク評価の結果生まれたものです。



シスコ検証済みデザイン（CVD）

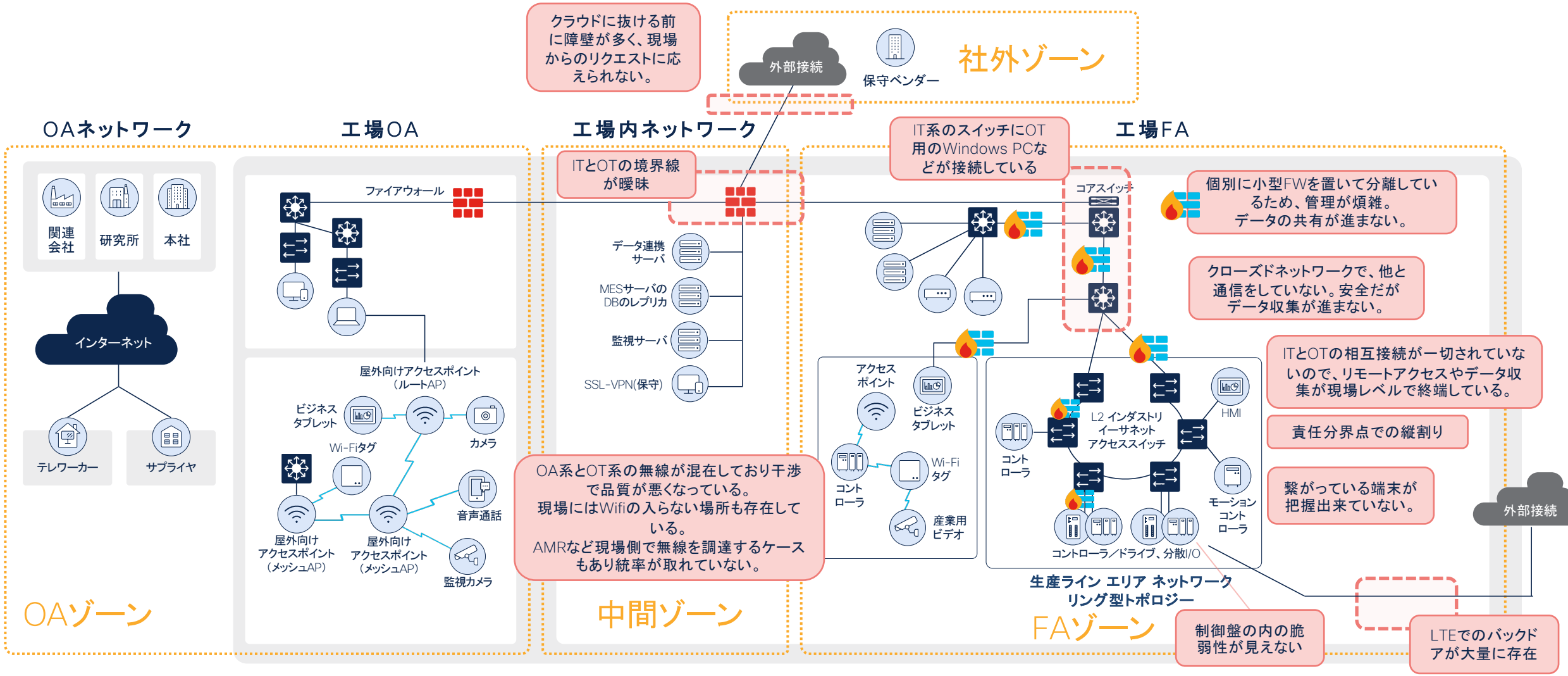
シスコ OT セキュリティ リファレンス デザインは、安全かつ堅牢で信頼性の高い産業用ネットワークのブループリントです。シスコの包括的なネットワーキングとセキュリティのテクノロジーを活用して、産業用資産の可視化、マクロ/ゾーンセグメンテーション、ゾーンアクセス制御、脅威検出および対応機能を提供します。このデザインでは、情報セキュリティとの調整を通じて、一貫性あるアクセスポリシー管理と、セキュリティ オペレーション センター（SOC）への産業セキュリティイベントの集約を実現できます。

図 4 に示すように、このデザインは Purdue/ISA95 モデルに従い、ISA/IEC-62443-3 に準拠するための詳細な設計および実装のガイドラインを提供します。



IEC62443概要と対策方法
https://www.cisco.com/c/ja_jp/products/collateral/security/isaiec-62443-3-3-wp.html

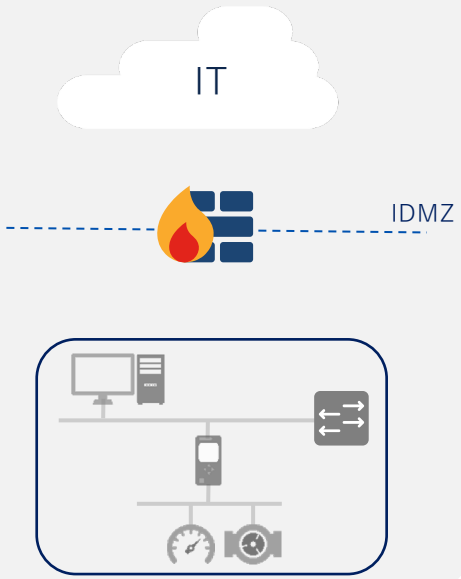
新工場ネットワークモデルとセキュリティ



産業ネットワークの保護への道のり

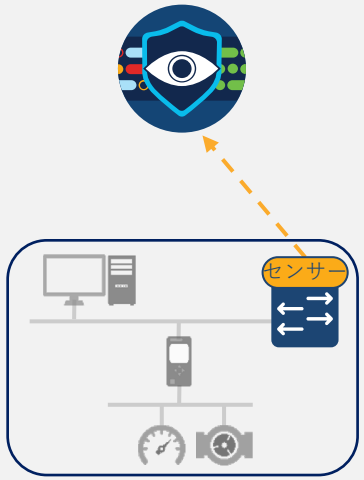
1 セキュリティ基盤の構築

IT/OT 境界を定義



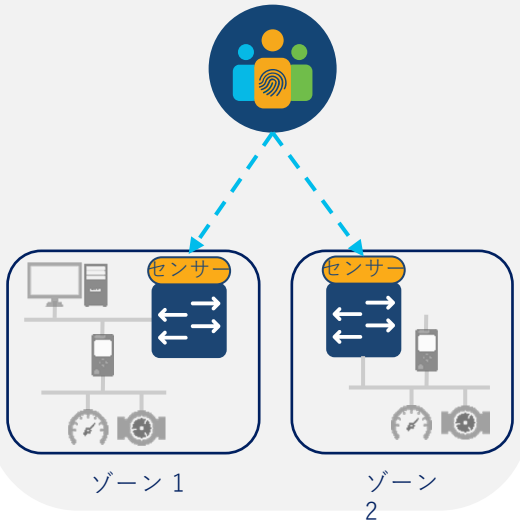
2 可視性と装置の態勢の獲得

Cisco Cyber Vision による可視化



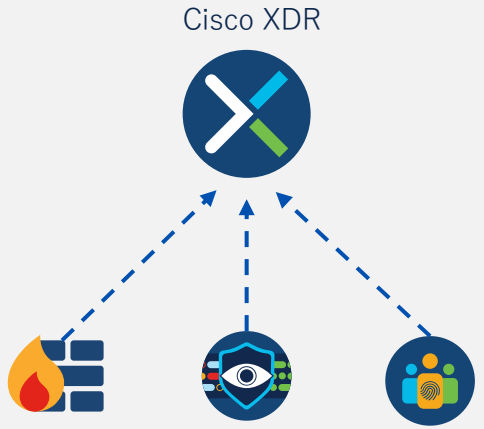
3 ネットワークをより小さな信頼ゾーンにセグメント化

Cisco ISE を使用したマイクロセグメンテーション



4 インシデントの調査と対応計画の作成

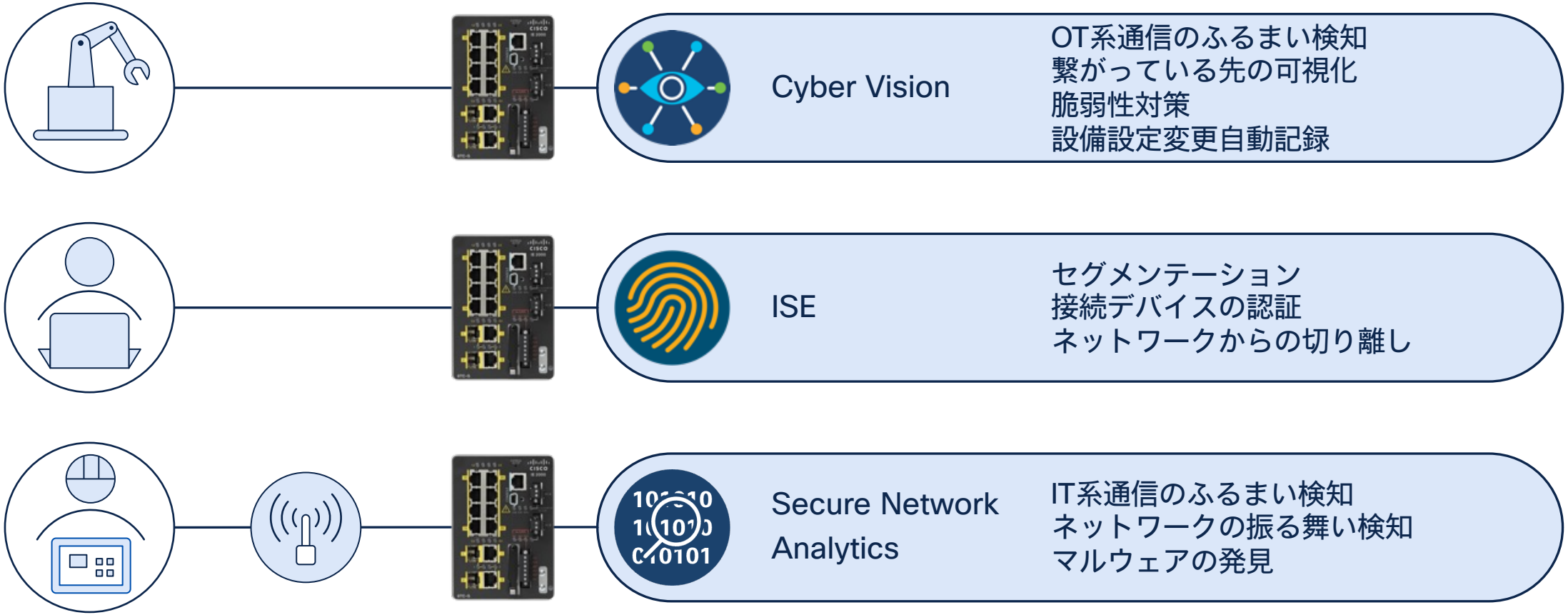
Cisco XDRによる脅威の調査と対応の調整



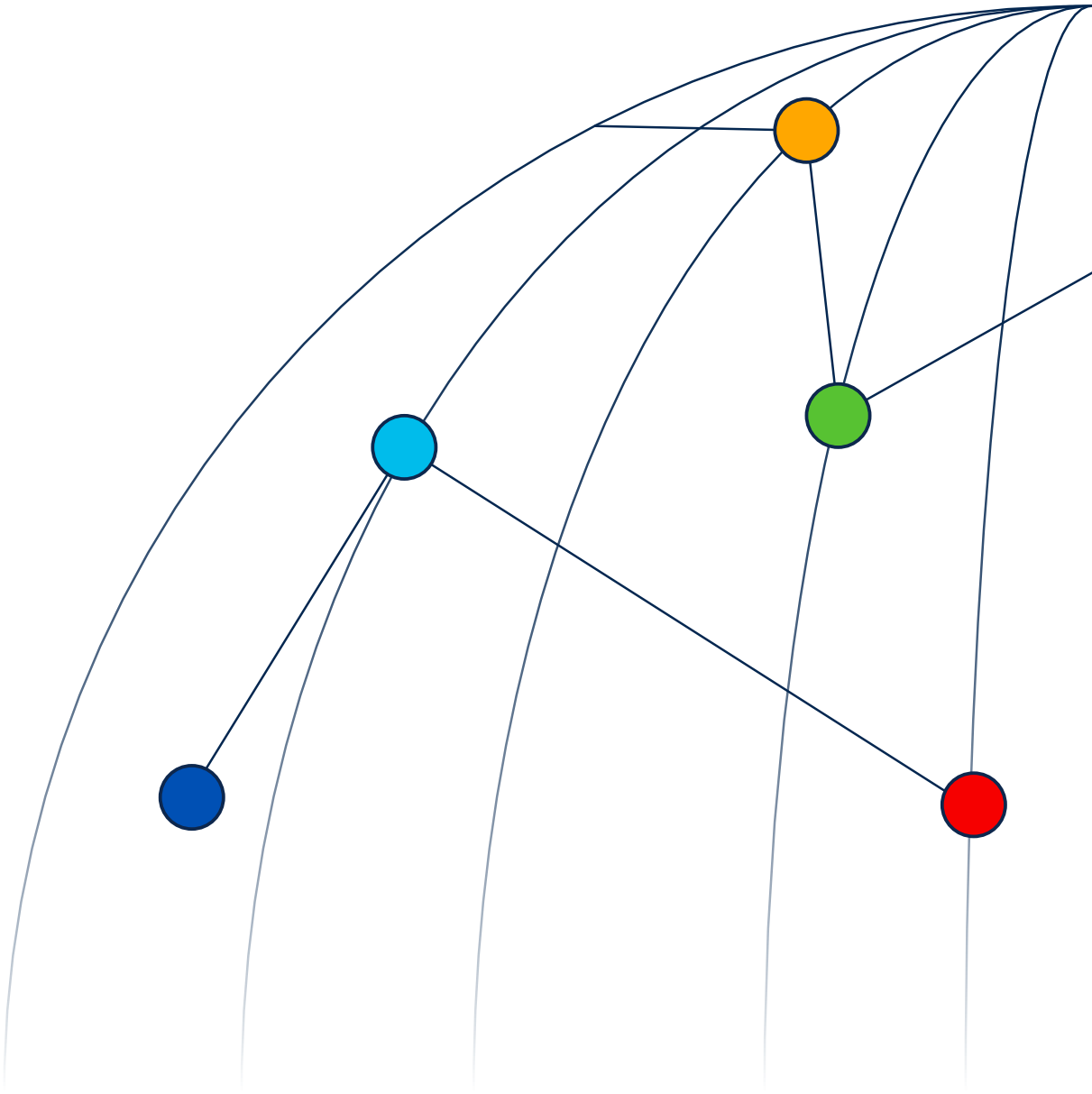
スイッチによるマイクロセグメンテーション

適切なスイッチを導入することで、スイッチ自体が備えるさまざまなセキュリティ機能によってネットワークの安全性を高めることができます。

工場の広いネットワークをスイッチで保護



Cisco Cyber Vision



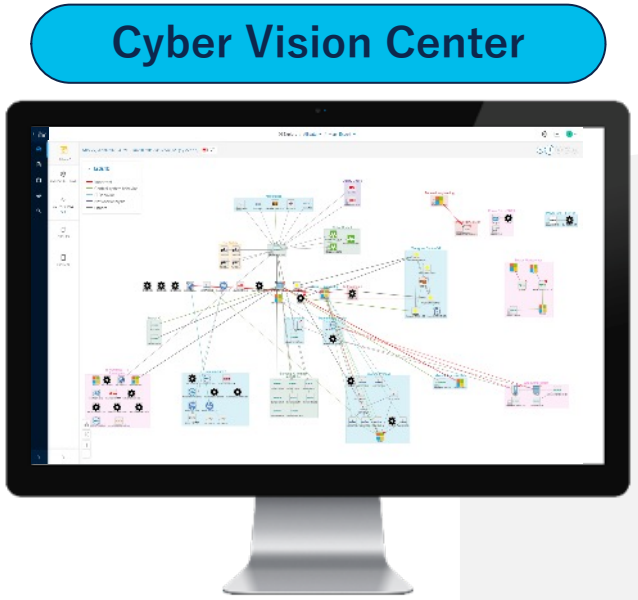
OT ネットワークをセキュリティに参加
Cisco Cyber Vision を組み込むことで全てを可視化させる

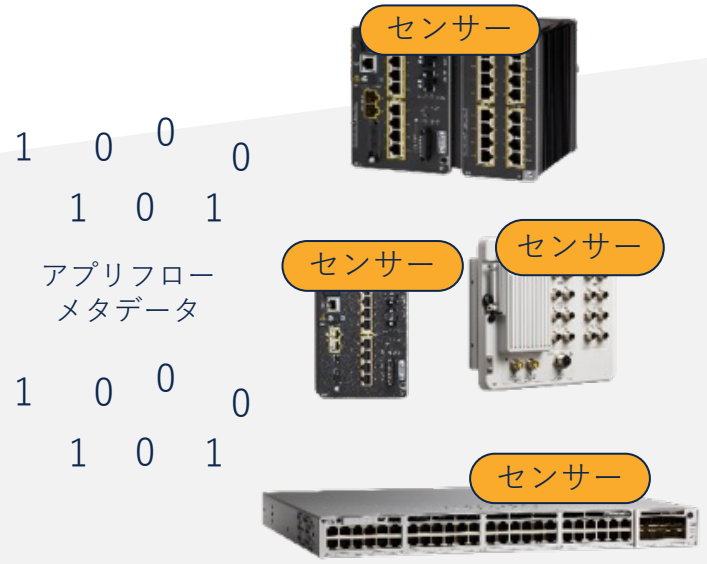
繋がることで守られる

OT ネットワークの可視性を獲得
包括的な設備インベントリ
通信パターンのマップ

セキュリティの情報収集
装置の脆弱性を特定
リスクを点数づけ

運用状況の把握により生産を改善
装置の変更を記録
ネットワークの問題と装置の設定ミスを特定





ネットワーク製品に組み込み型
（追加の製品は不要）

Cisco Catalyst スイッチは、接続されている全てのものを認識し、大規模な OT ネットワークを保護

Cisco Cyber Vision

資産の可視性を獲得

資産台帳

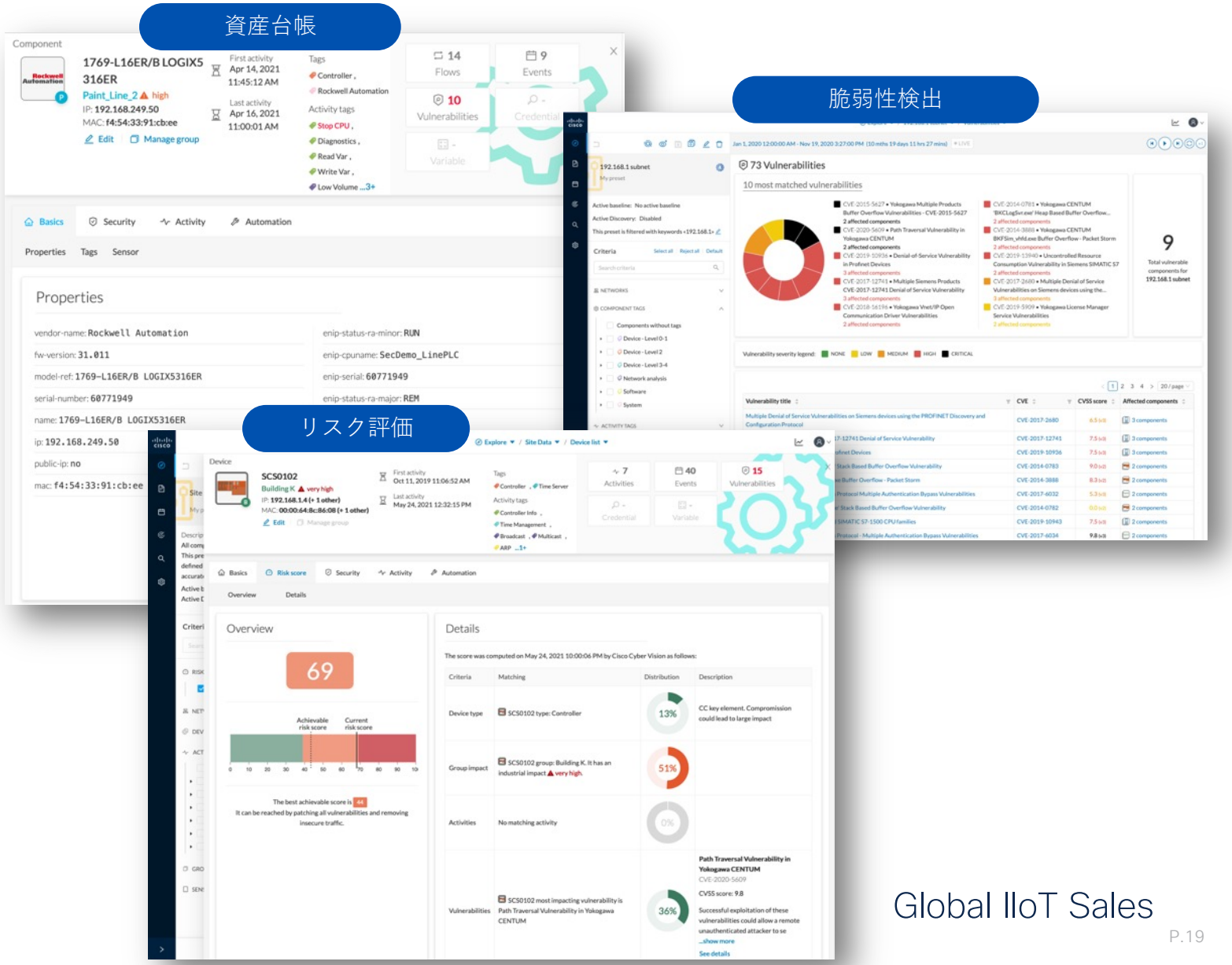
環境中の全ての資産の包括的かつ最新の台帳

脆弱性検出

侵害される前にパッチが当てられるよう資産の既知の脆弱性を識別

リスク評価

資産のリスクを影響度と可能性に基づいて評点しコンプライアンス向上を支援



Cisco Cyber Vision

通信パターン

詳細なアプリケーションフローラベル情報付き動的通信マップ

制御システムアクティビティ

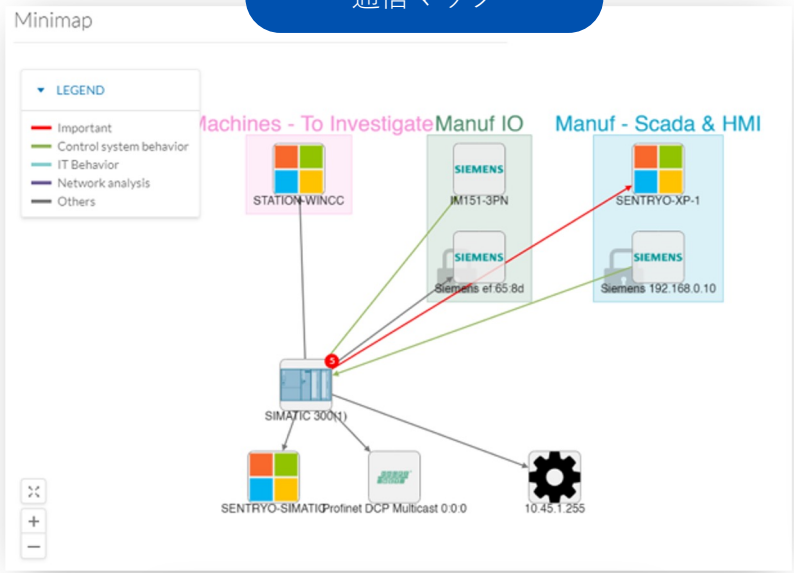
プロセス変更の追跡
設定変更の識別
制御システムイベントの記録

変数アクセス

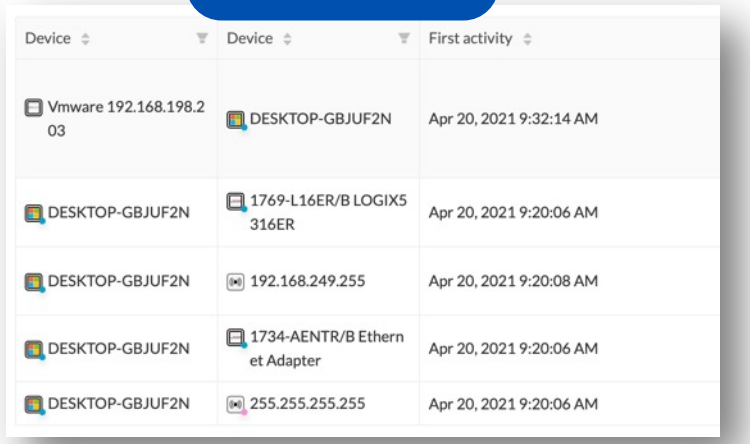
変数、オブジェクト、セットポイントの読み出しや書き込み操作を記録

運用状況の把握

通信マップ

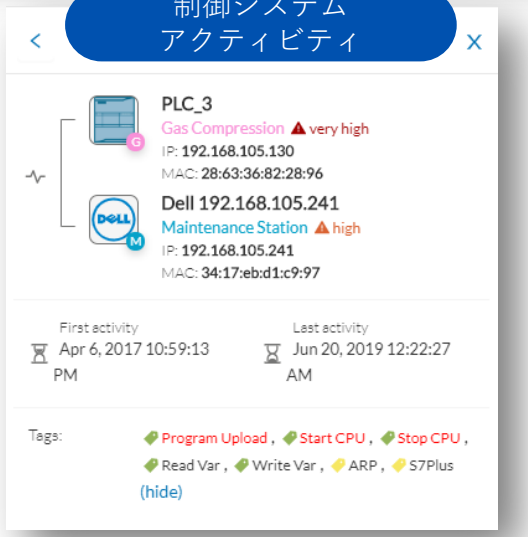


アプリフロー

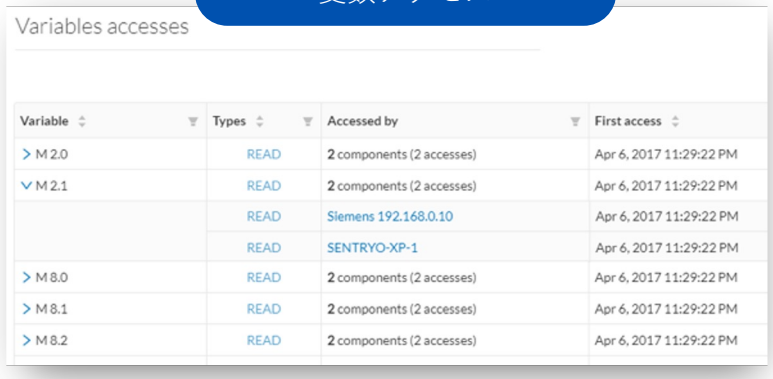


Device	Device	First activity
Vmware 192.168.198.203	DESKTOP-GBJUF2N	Apr 20, 2021 9:32:14 AM
DESKTOP-GBJUF2N	1769-L16ER/B LOGIX5316ER	Apr 20, 2021 9:20:06 AM
DESKTOP-GBJUF2N	192.168.249.255	Apr 20, 2021 9:20:08 AM
DESKTOP-GBJUF2N	1734-AENTR/B Ethernet Adapter	Apr 20, 2021 9:20:06 AM
DESKTOP-GBJUF2N	255.255.255.255	Apr 20, 2021 9:20:06 AM

制御システム
アクティビティ



変数アクセス



Variables accesses

Variable	Types	Accessed by	First access
> M 2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
v M 2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM
> M 8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
> M 8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
> M 8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM

Cisco Cyber Vision

異常検知

振る舞い分析による OT 資産変更の試みの検知、変化点検出のためのベースライン作成

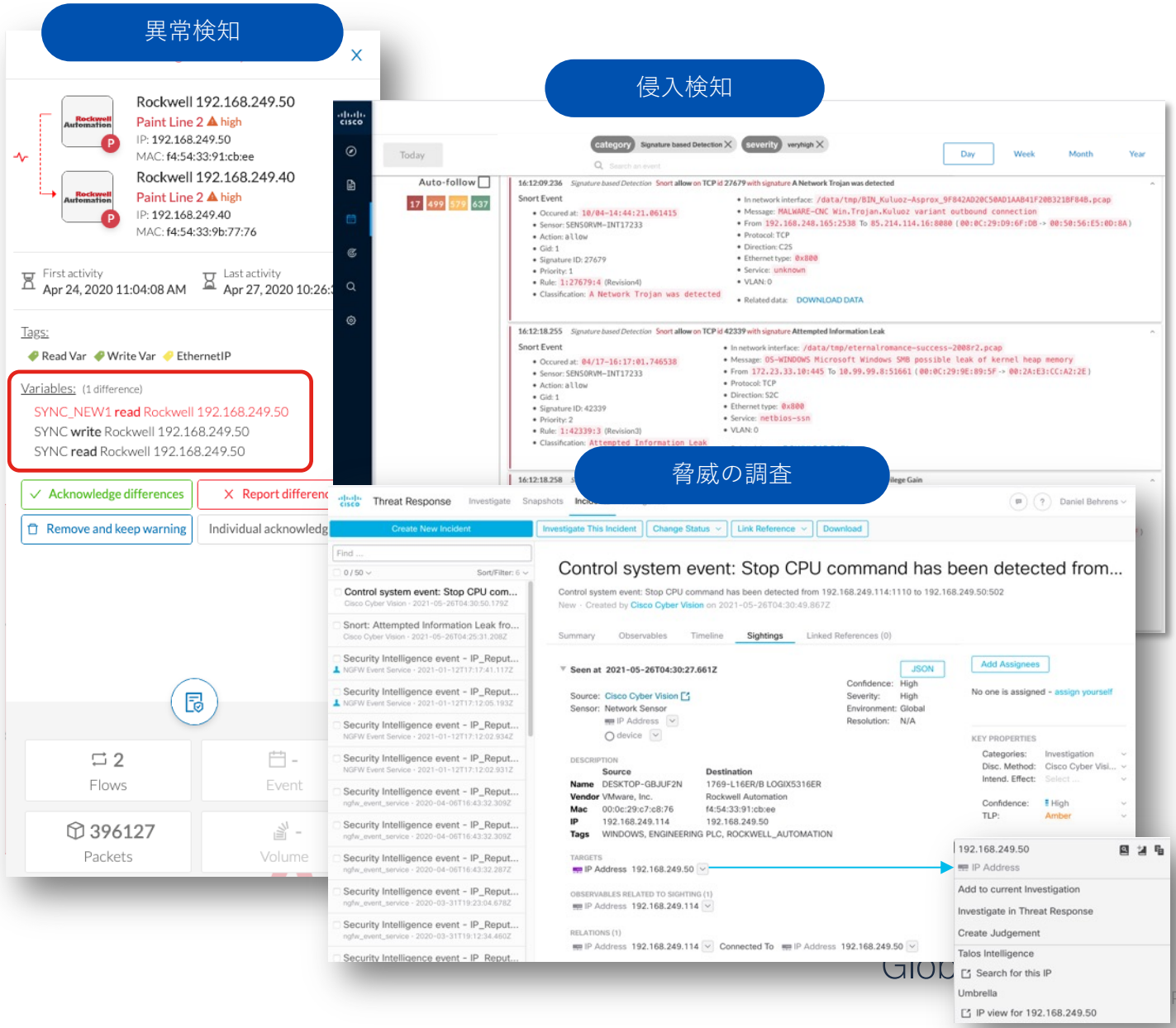
侵入検知

Snort IDS と Talos 脅威調査機関による侵入の検知

脅威の調査

SecureX インシデントマネージャーによる、Cisco と他社セキュリティ製品からの情報も統合したイベント調査

脅威の検知と調査



Cyber Visionにより危険を回避できた例

サイバー攻撃対策・ダウンタイムの減少・未然に防ぐ対策立案・ネットワークの設計見直し

バックドアの発見

メーカーの設備に保守メンテナンス用のポートがあり、誤ったネットワークに接続されていたことを検出。
情報流出やマルウェアの侵入を防ぐとことに繋がった。

異常な通信の検出

生産エリアのネットワークで通常よりも高い通信量を検出。原因となったデバイスを特定することで、被害の拡大を防いだ。

乗っ取りの有無の確認

現場の意図していない設定値に変更されている機材を発見。どのデバイスと通信をし、過去の設定変更がいつ行われたかを遡ることで、乗っ取りの可能性があるデバイスを検出することが出来た。

チョコ停対策
設備メーカーの操作確認

チョコ停が起きた際にどの設備が原因かすぐに調べることが出来、復旧時間の短縮が出来た。
保守保全用途で設備メーカーが定期的に行う操作で正しくない操作が確認された。
設定を修正する事で、生産停止のリスクを未然に防ぐことが出来た。

リスクの高い脆弱性の検出

機器の中にEternalBlueと呼ばれ、2017年頃に世界中に伝播したマルウェア「WannaCry」が使用していた脆弱性を発見。早期にアップデート促すことが出来た。

リモート操作のリスク検出

Windowsマシンのリモート操作を行なっている企業で、異常な振る舞いを検出。

不正な通信の検出

境界線ファイアウォールを抜けて通信を行っているデバイスを検出。正しい設定とネットワーク設計に修正することで、リスクを未然に防いだ。

ネットワーク設計のミスを発見

マップの表示機能により、通信経路の設計にミスがあることが発覚。IPアドレス重複対策のL2NATなどの問題も同時に存在し、ネットワーク設計の見直しのきっかけになった。

セキュリティ計画の立案

Cyber Visionで得た脆弱性リストや資産リストを元にIT部門とOT部門で協力して、ネットワークの分割案及びセキュリティ対策方針を決定。
ファームウェアのアップグレードが出来ない設備の多い領域などを迅速にネットワークから切り離すなど、効果的な対策を取ることができた。

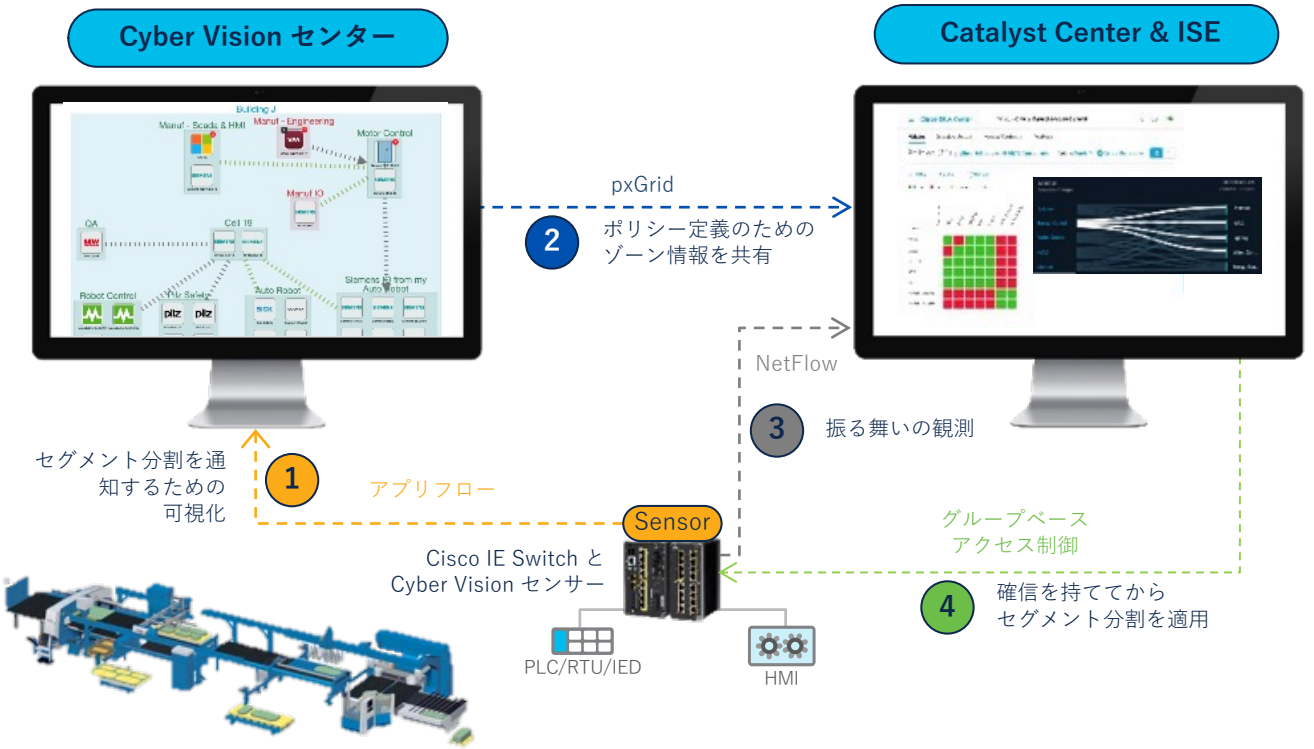
可視性と分析でネットワークをセグメント化
Cyber Vision、Cisco Catalyst Center、ISE を利用

トータルソリューションの強み

IEC62443ゾーンとコンジットの可視化
Cyber Vision のもたらす可視性を活用してゾーンを作成し、Cisco ISE と詳細を共有

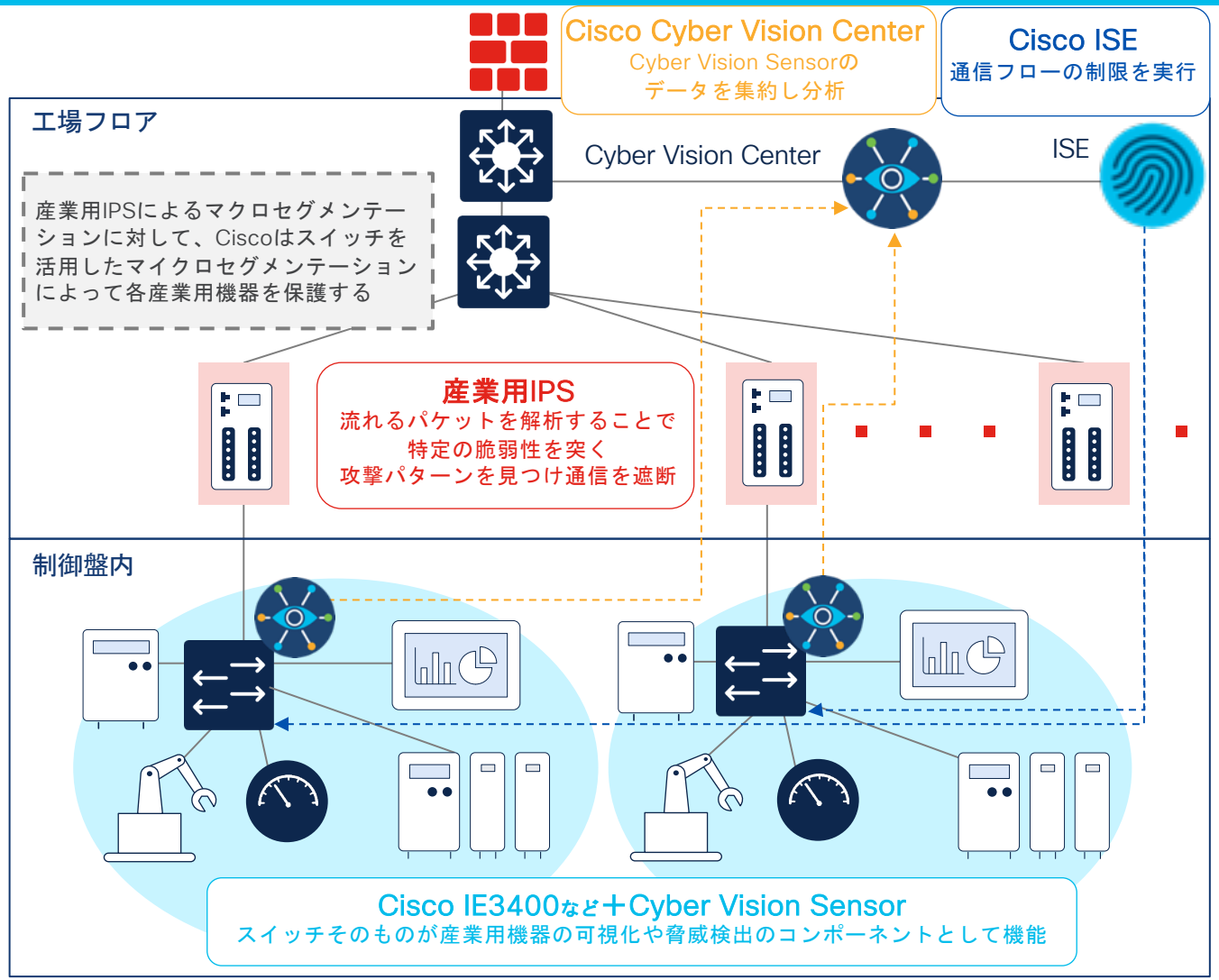
動的ネットワークセグメント分割の実現
Cyber Vision のグループ化により、ISE を介した端末へのグループベースのポリシーの動的な割り当てを実現

対策実行前の最終確認
Cisco DNA Center でネットワークの動作を視覚化し、確信を持ってから適用



Cyber Visionが他のシスコツールに情報を提供
ネットワーク管理・セキュリティ対策のレベルが向上

OTセキュリティ
産業用IPSとCiscoソリューションの守備範囲

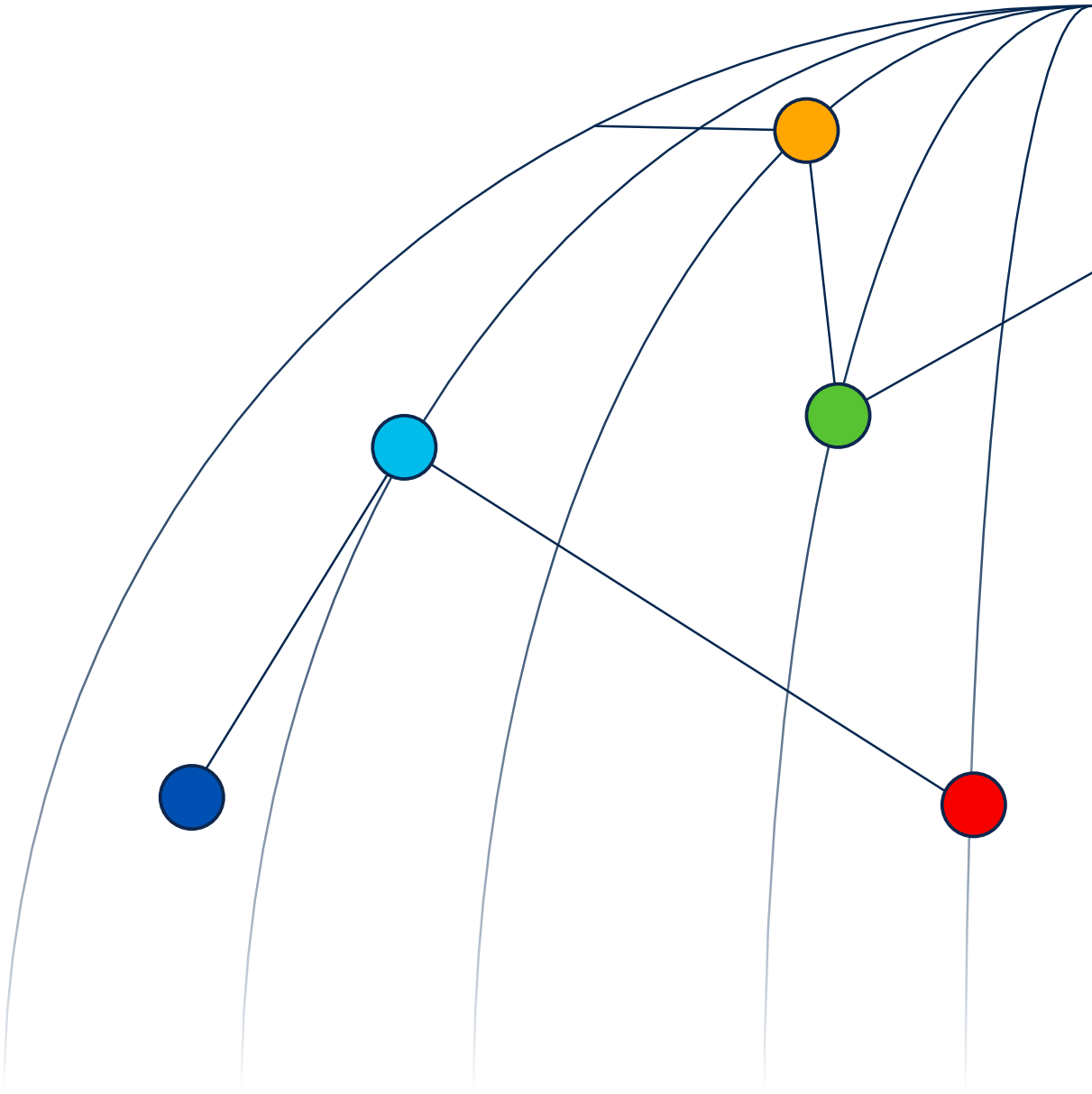


	ポイント	導入のユースケース
産業用IPS	• 保護したいエリアや機器が少ない場合は侵入防止としてピンポイントでの対策は可能 • ただし、各産業用機器自体の脆弱性把握や脅威検出は不可 • また、産業用IPSの数が増えると、本体費用及びバージョンアップやパッチ適用といった運用コストが増加	• 小規模な工場 • 自動化されていない個産品の生産ライン
Cisco	• Cyber Visionによる産業用機器の包括的な可視化と脅威検出 • また、Cyber Visionで産業用機器を論理ゾーンにグループ化しコンジットを通過するデータを視覚化。その論理的な区切りはISEと共有され、通信フローを適切に制限	• 比較的規模が大きい工場 • 自動化されている量産品の生産ライン
産業用IPS＋Cisco	• 産業用IPSによる侵入防止とCiscoの可視化・脅威検出、通信フローの制限によるトータルなセキュリティ対策 • Ciscoスイッチとつながっていない機器への産業用IPSによるピンポイントでの対策	• 強固なセキュリティ対策が必要なケース • 自動化と人手の生産が混在するライン

Ciscoのソリューションは産業用機器の包括的な可視化・脅威検出に加え、ゾーンのセグメンテーションが可能

Cisco SEA ご紹介（リモートアクセス）

- Secure Equipment Access

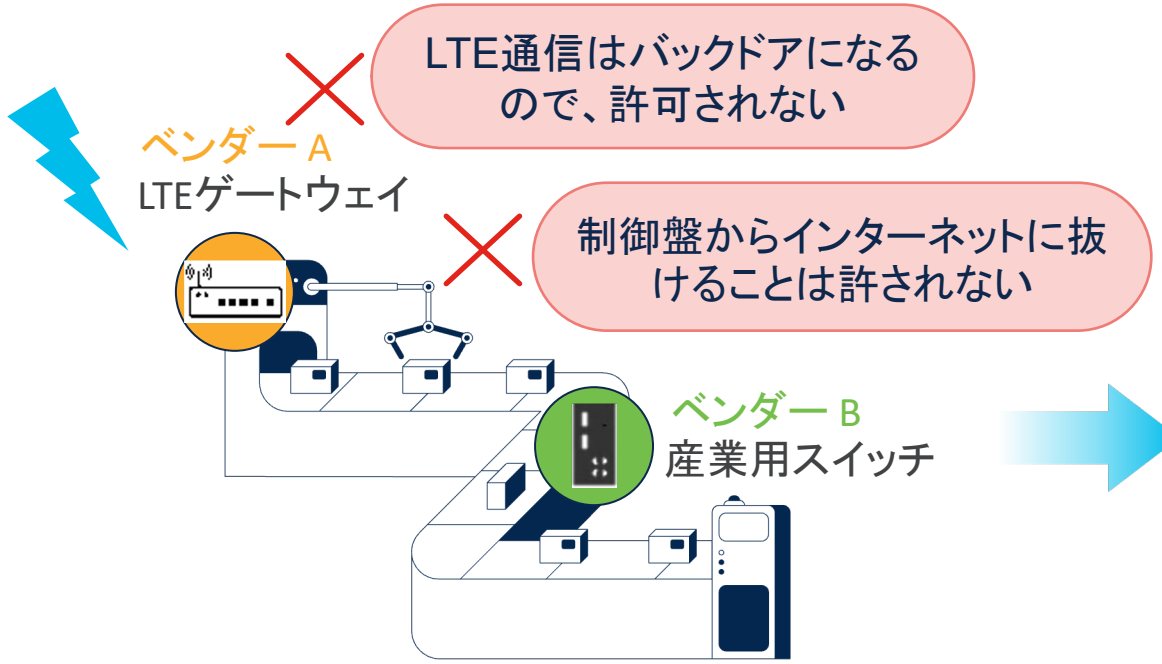


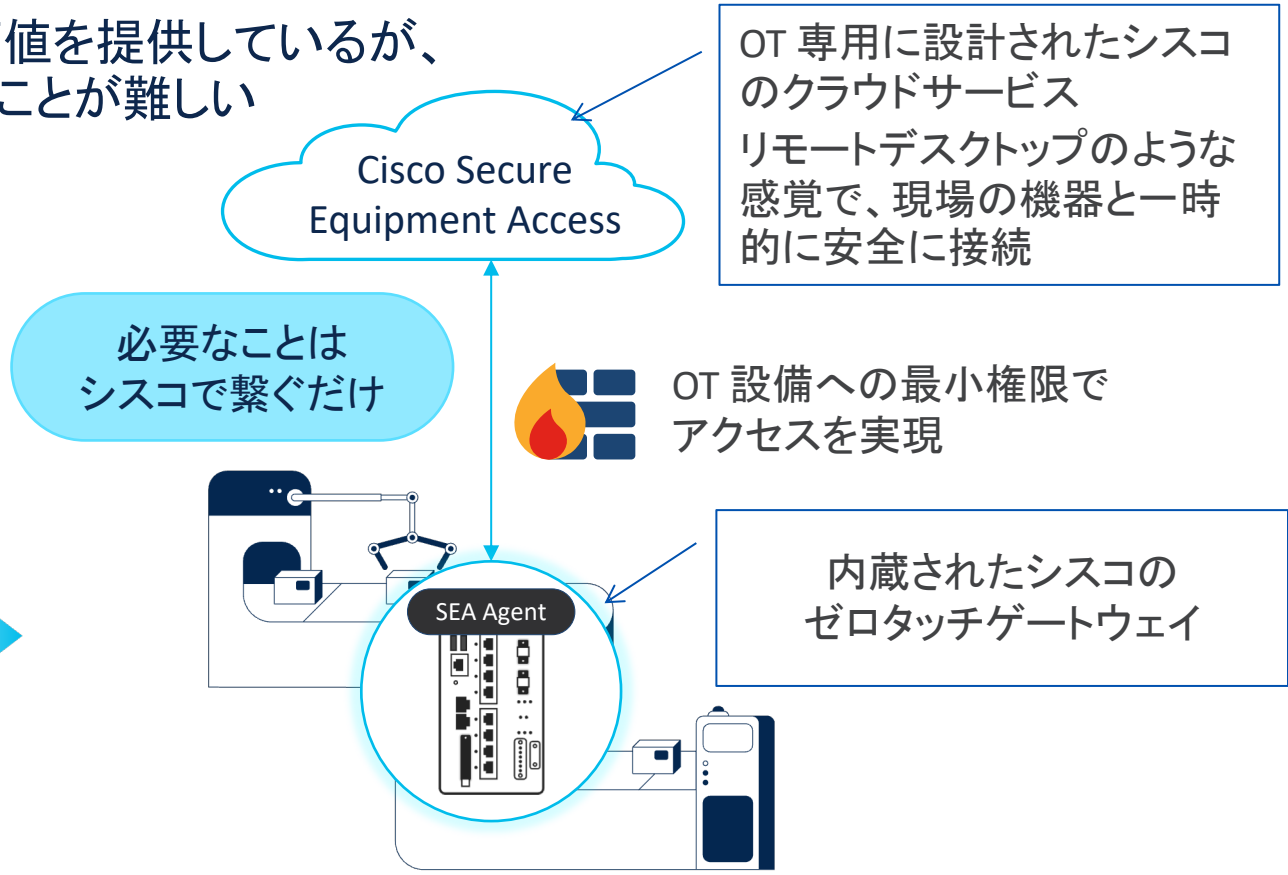
安全なリモートアクセスの実現方法

新機能

Cisco Secure Equipment Access（SEA）

設備ベンダーはリモートメンテナンスをサービス化し、付加価値を提供しているが、
現在の日本の工場では外部から現場の設備にアクセスすることが難しい





ロボットへの遠隔接続をLTEではなく有線ネットワークで実現
企業のFWを超えて安全に産業機器へアクセスが可能

The bridge to possible