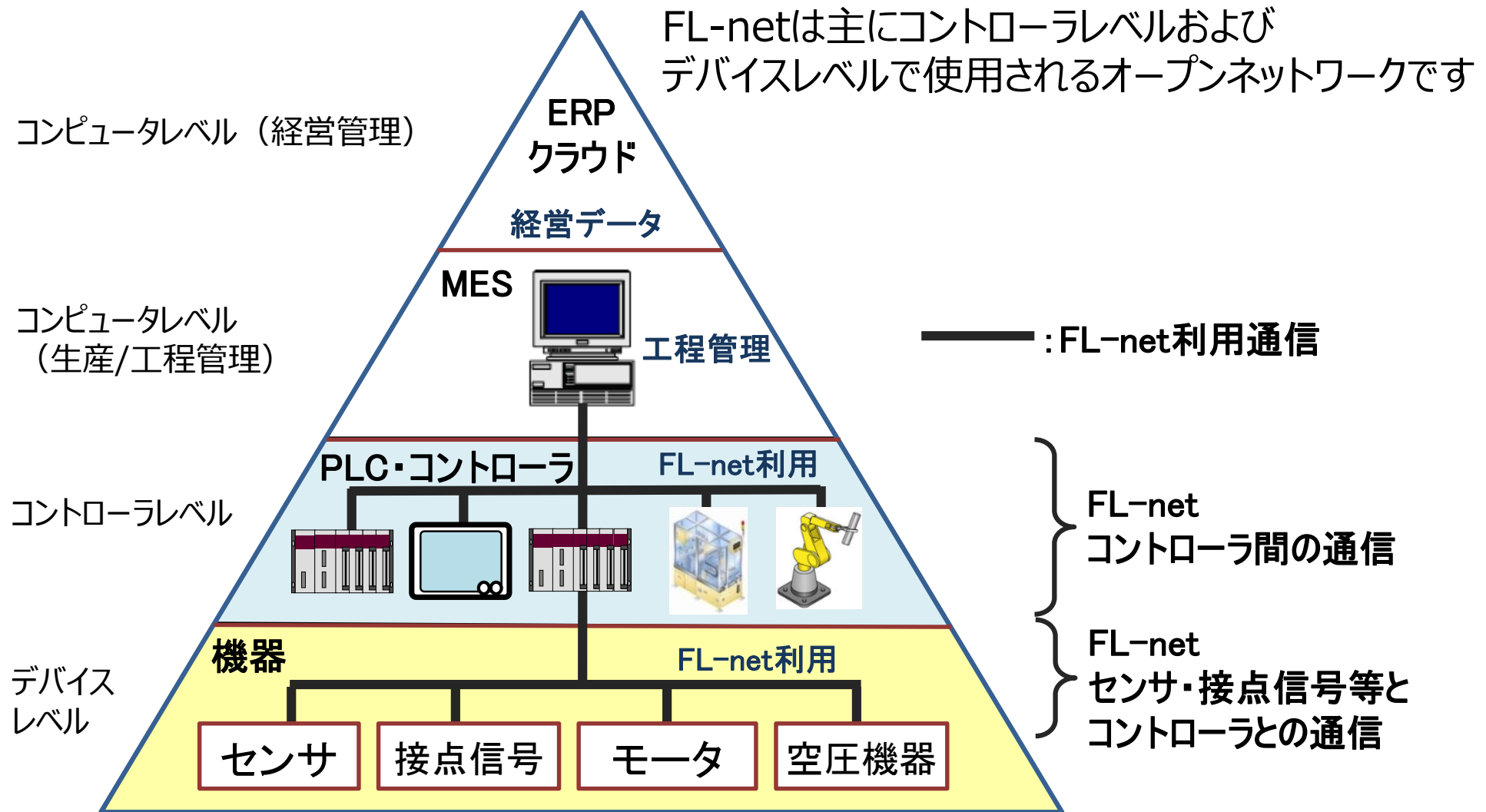


FL-netのセキュリティ対策

一般社団法人 日本電機工業会
FL-net推進委員会
2026年10月1日

- 本資料の目的
- はじめに -FL-netとは-
- 生産現場システムでセキュリティが必要とされる背景
- 生産現場システムでのセキュリティ対策の考え方
- FL-netを利用した生産現場システムでのセキュリティ対策の考え方
- 生産現場システムで想定されるセキュリティリスク
- 生産現場システムでのセキュリティ対策
- FL-netパートナー製品

- FL-netとはJEMAが標準化した、PLC、CNC、ロボットやSCADAなどを接続する産業用ネットワークです。
- FL-netが適用されるOT(Operational Technology)環境では、これまでクローズドな運用がされていましたが、近年のDX化の推進に伴い、IT(Information Technology)連携が進んでおり、セキュリティのリスクが増大しています。
- そこで本資料では、FL-netを用いたシステムにおけるセキュリティリスクとその対策の案を示しています。



【FL-netとは】

- 主にコントローラ間のデータ連携を目的とした、Ethernetベースの産業用ネットワーク
- 多くのベンダが対応している日本発のオープンフィールドネットワーク

【FL-netの特長】

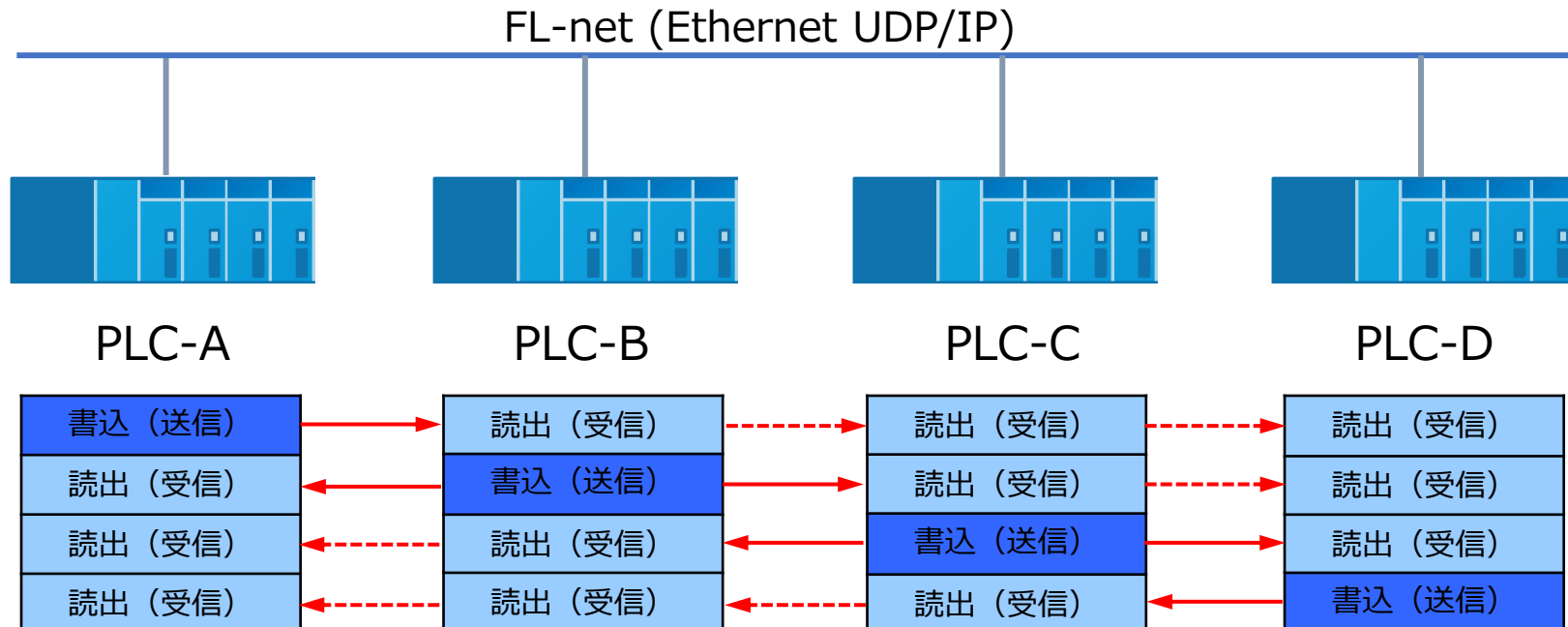
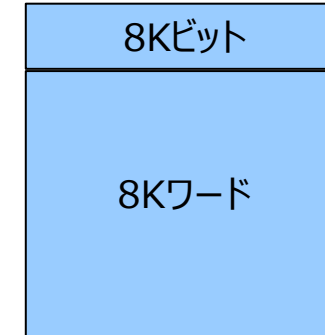
- コモンメモリによる、通信を意識しない簡単なユーザインタフェース
- マスタレスのトークンパス方式
- 標準のUDP/IP上のプロトコルなので市販のハブ、ケーブル使用可
- 254台のコントローラを接続でき大規模なネットワークにも対応
- コントローラからデバイスレベルまでカバー（Ver.3）
- 既存設備で稼働中のコントローラにFL-netモジュールを追加するだけで設備間のデータ連携が可能（国内の主要コントローラメーカーがFL-net対応機器をラインナップ）

コモンメモリシステムとは

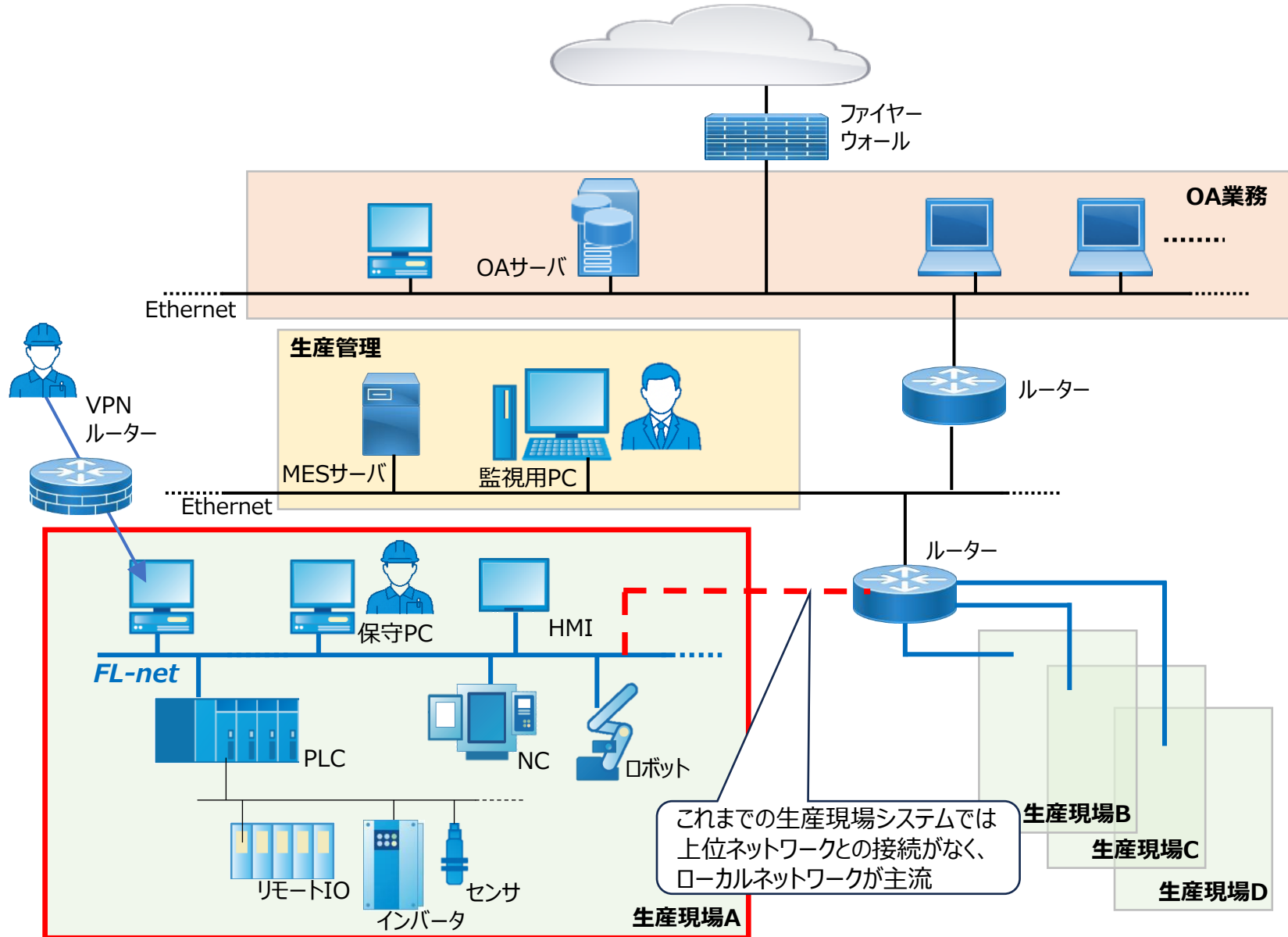
各コントローラでコモンメモリと呼ばれるひとつのメモリマップを共有し、すべてのコントローラからデータの読み書きができます。

あるコントローラの書き込み（送信）領域は、他のコントローラからは読み出し（受信）領域となります。

コモンメモリ



生産現場システムでセキュリティが必要とされる背景

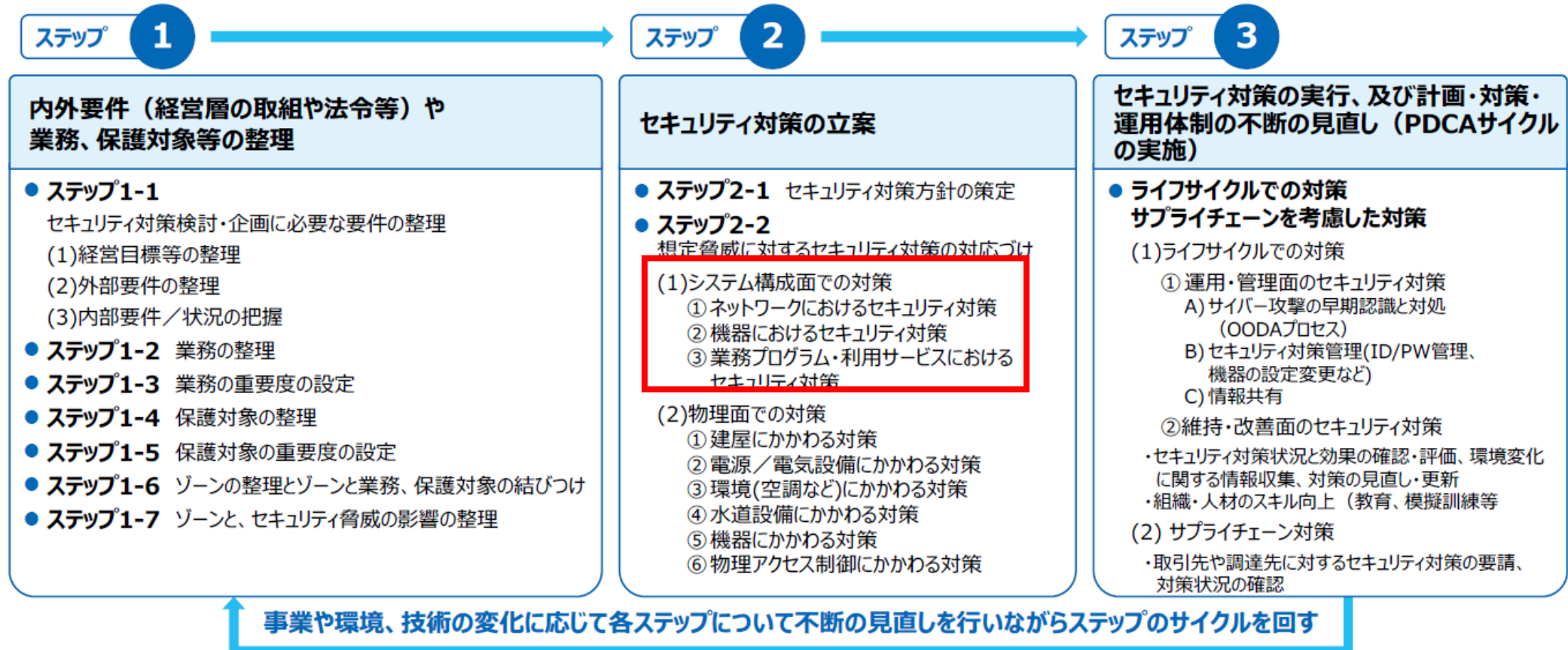


- これまで生産現場システムは、工場内のローカルなネットワークとして扱われ、セキュリティリスクの対応が不要なものとされてきていました。
- しかしながらDX化の推進に伴い、生産現場の各機器の稼働情報などが新たな価値を生むようになる中で、生産現場システム、現場機器に対してもセキュリティリスクを考慮する必要が出てきています。



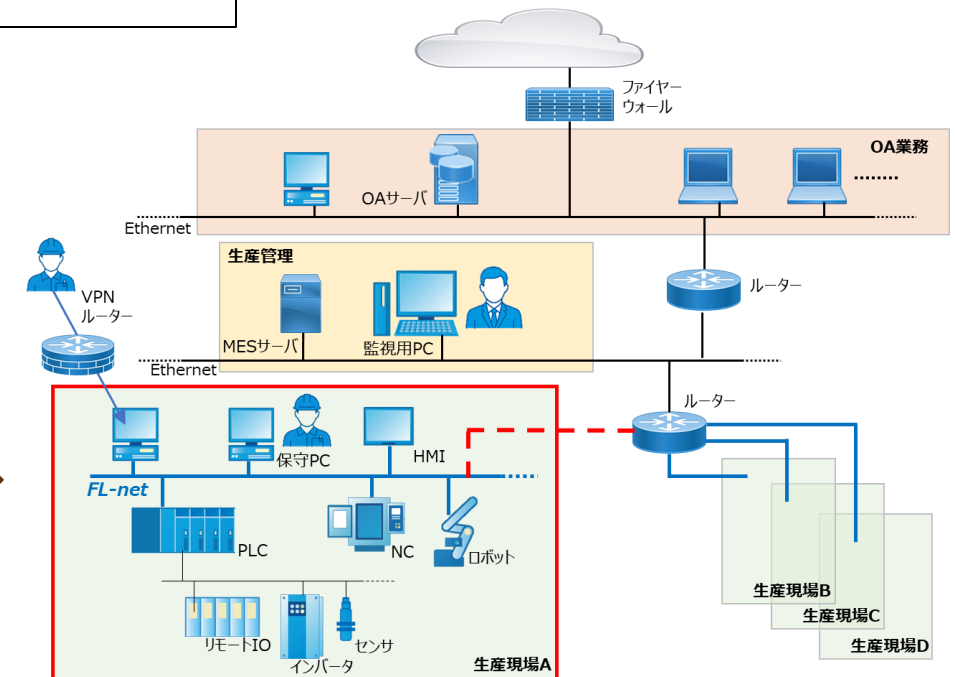
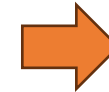
- 工場システム(OTシステム)に関するセキュリティ対策の進め方については、経済産業省からガイドラインが発行されています。
「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」Ver.1.1
(https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html)

- セキュリティ対策の進め方として、ガイドラインでは下図のようなステップを想定し、事業や技術の変化に応じて、このサイクルを回して運用していくことを推奨しています。
- 本書では、ステップ2-2(1)システム構成面での対策を中心に、FL-netでのセキュリティ対策について記載します。



- ステップ2-2
想定脅威に対するセキュリティ対策の対応づけ
(1) システム構成面での対策
 - ① ネットワークにおけるセキュリティ対策
 - ② 機器におけるセキュリティ対策
 - ③ 業務システム・利用サービスにおけるセキュリティ対策

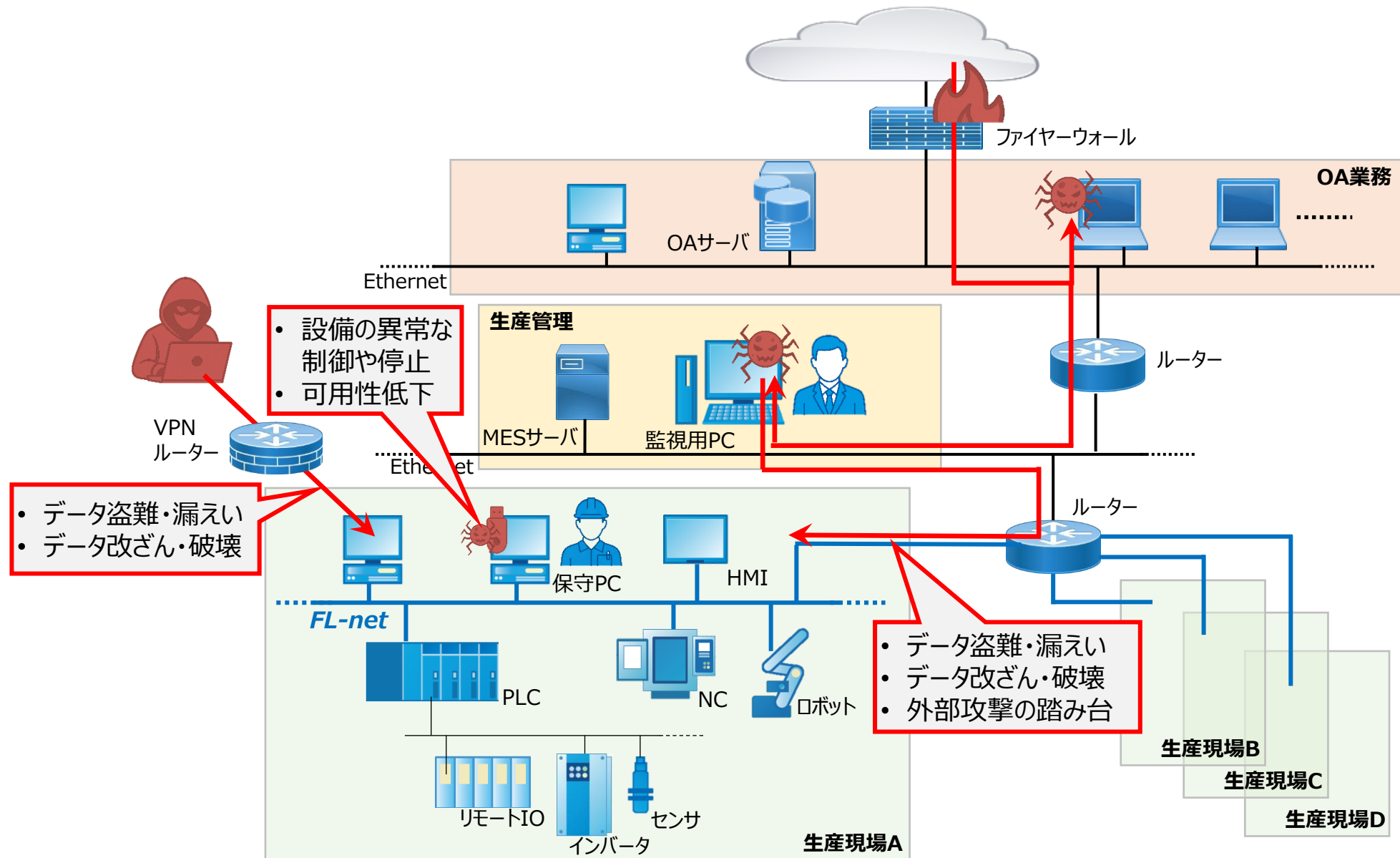
- FL-netでは、旧システムとの互換性を重視し、ネットワークプロトコルに依存したセキュリティ対策ではなく、旧システムとも共存を目指すセキュリティ対策を推奨します。
- FL-netは、生産現場システムで利用されるネットワークシステムのため、工場内のネットワークをゾーンに分割し、生産現場システムに特化したセキュリティ対策を提案します。



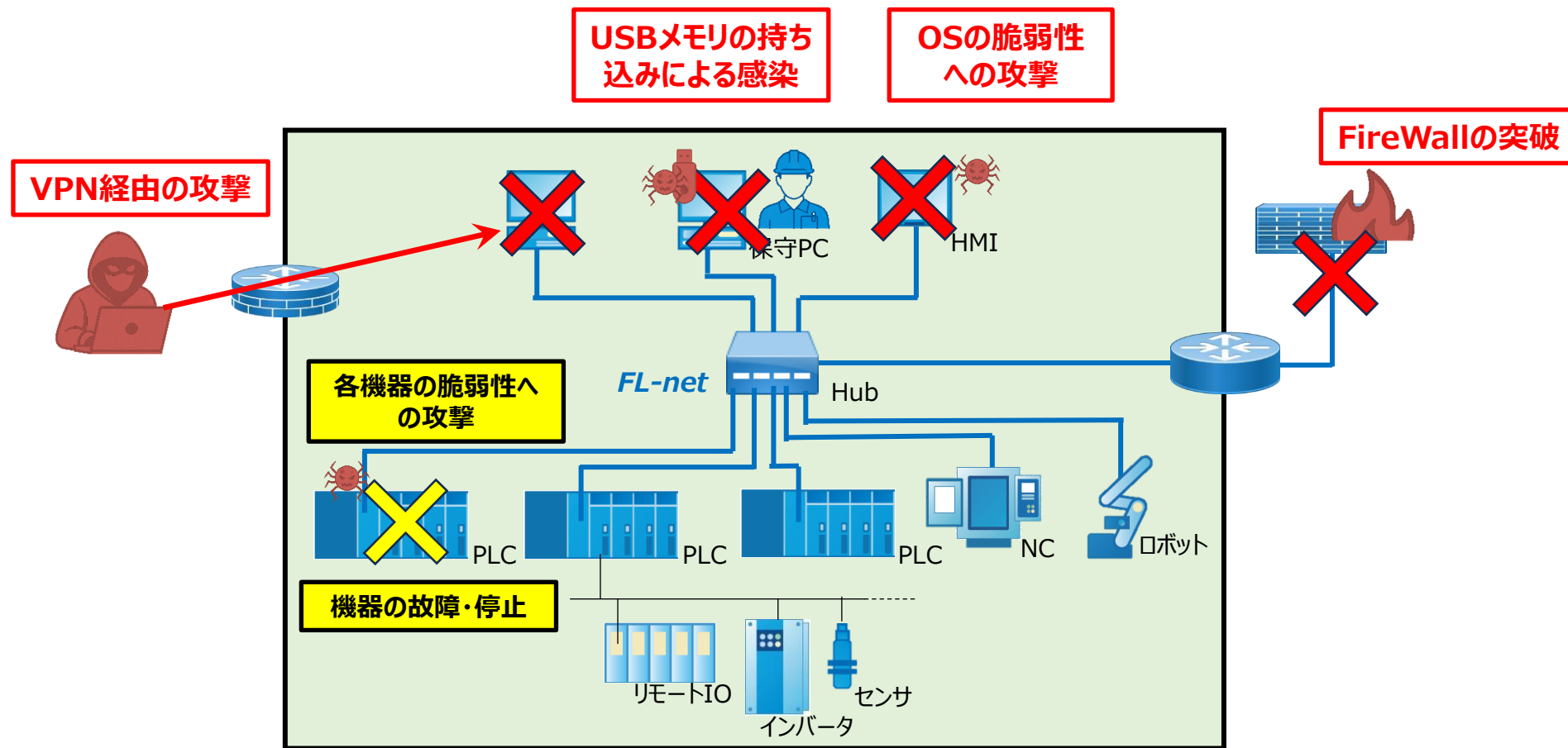
- 工場システムの脅威による生産・事業への影響として、生産現場では下記のようなことが考えられます。
- 本資料では、物理的攻撃以外の脅威に対するセキュリティ対策を説明します。

脅威種別	脅威内容	精算・事業への影響
機器の盗難、システム・機器に対する破壊・不正操作	- 物理的な侵入による、システム・機器に対する直接的な破壊・盗難・不正操作 - 直接的な不正接続によるシステム・機器の破壊・不正操作 - ネットワーク経由の侵入、または内部からの不正通信（バックドアやコネクトバック通信）を利用したシステム・機器の破壊、不正操作	- 生産性低下による納期遅れや原価上昇 - 設備故障、盗難による損害システム・機器材に対する破壊行為による生産停止等
設備の異常な制御や停止	- 設備の不正な制御や停止 - 設備へ異常負荷をかけての停止 - 設備の安全制御の機能停止	- 品質不良や、それに伴うブランド毀損 - 生産性低下による納期遅れや原価上昇 - 設備の誤動作による人身事故や災害の発生 - 設備故障による損害
データ盗難・漏えい	- USBなどへの不正コピー - 不正なサーバへのアップロード - パケットの盗聴(通信データの盗聴)	- 生産情報や品質保証ノウハウの流出 - 顧客情報の流出と、それに伴うブランド毀損
データ改ざん・破壊	- データやプログラムの改ざん・消去 - 設備設定値の悪意ある変更・消去 - パケットの改ざん(通信データの改ざん)	- 品質不良や、それに伴うブランド毀損 - 生産性低下による納期遅れや原価上昇 - 設備の誤動作による人身事故や災害の発生 - 設備故障による損害
可用性低下	- ネットワーク停止 - ネットワーク停止・容量オーバー - 設備・サーバ・PCの停止 - リソースの不足	- 生産性低下による納期遅れや原価上昇 - 設備制御不能による人身事故や災害の発生 - 品質不良や、それに伴うブランド毀損
外部への攻撃の踏み台として利用	外部サーバ／ネットワークへの攻撃	- ブランド毀損 - 操作中のライン停止に伴う納期遅れの発生

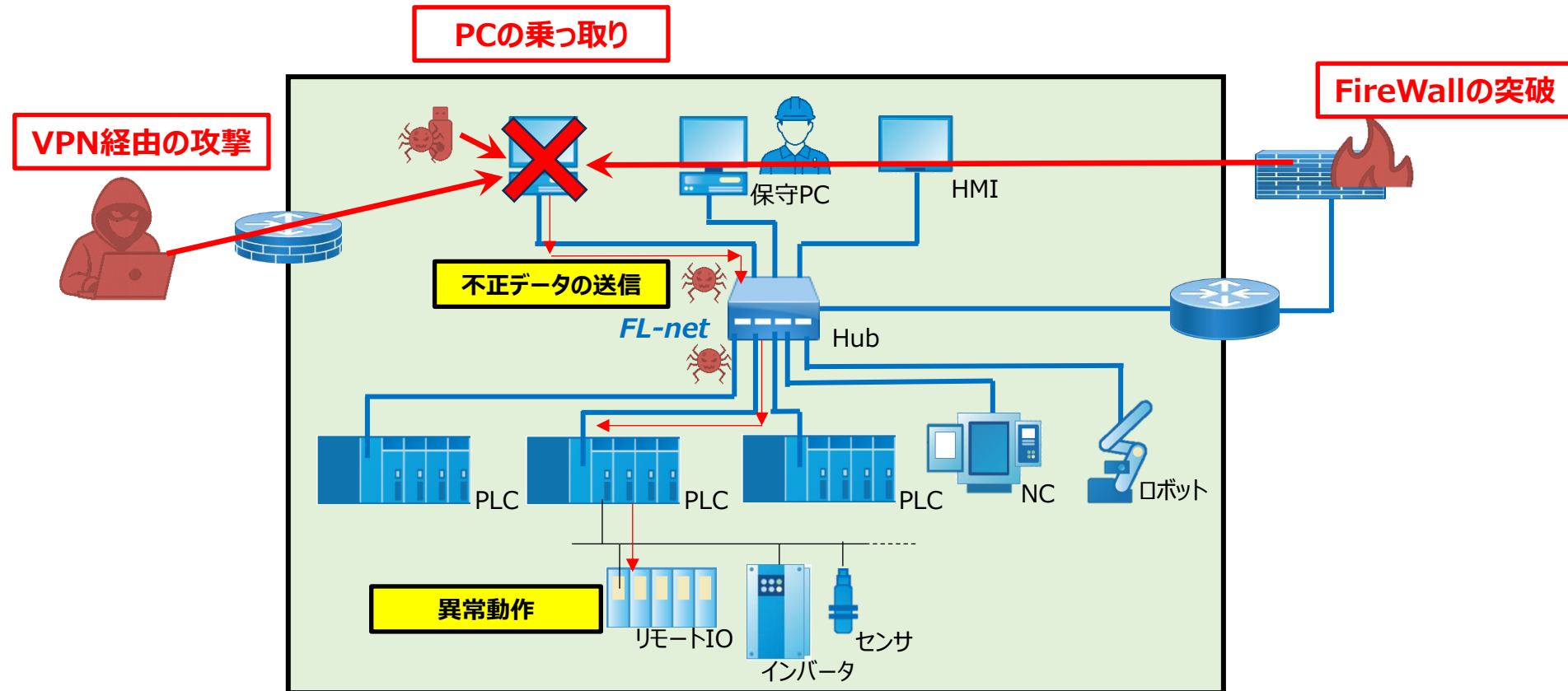
工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer1.1より抜粋



- Firewallの突破、VPN経由の攻撃、USBからのウイルス感染等により、FL-net機器の脆弱性への攻撃が行われ、FL-net機器が故障、異常停止する可能性があります。



- Firewallの突破、VPN経由の攻撃、USBからPCが乗っ取られ、PCから不正なデータを送信し、FL-netのシステムに異常な動作をさせる可能性があります。



- これらの脅威からFL-netのシステムを守る対策として、次のような対策が考えられます。

・各機器にセキュリティ対策ソフトの導入

・USBメモリなどデバイス管理のルール化
・USBポートの封止

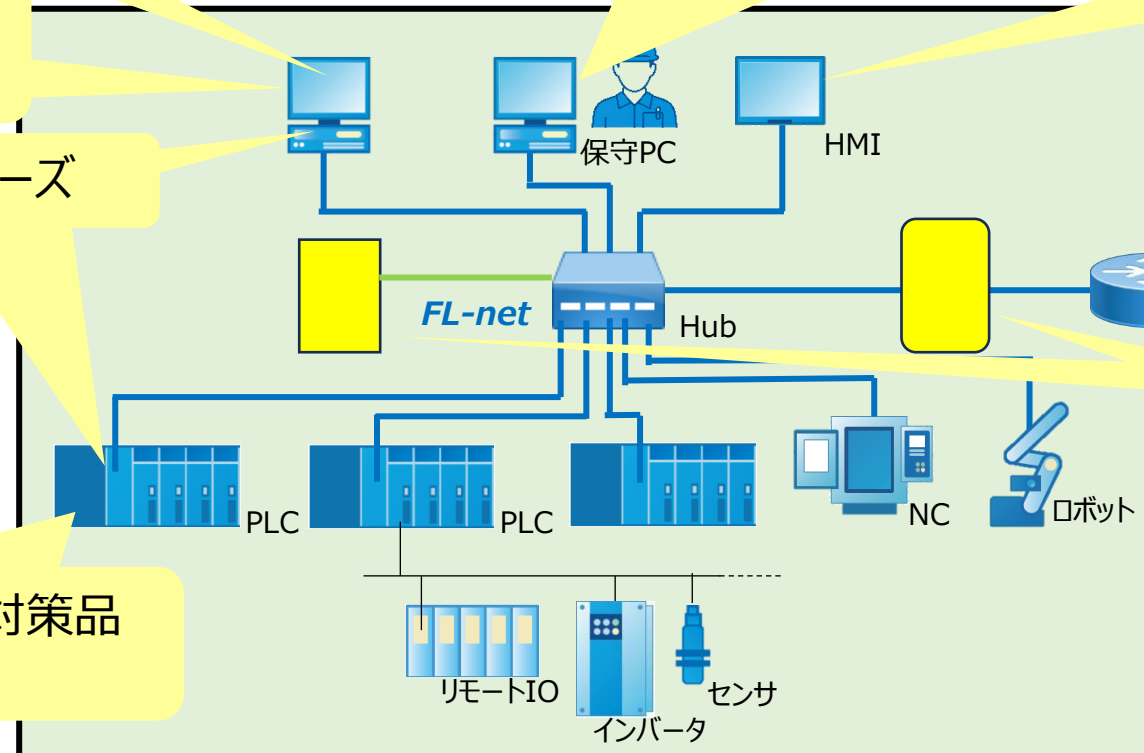
・最新OS、セキュリティパッチの適用

・USBタイプのセキュリティツールの導入

・不要ポートのクローズ

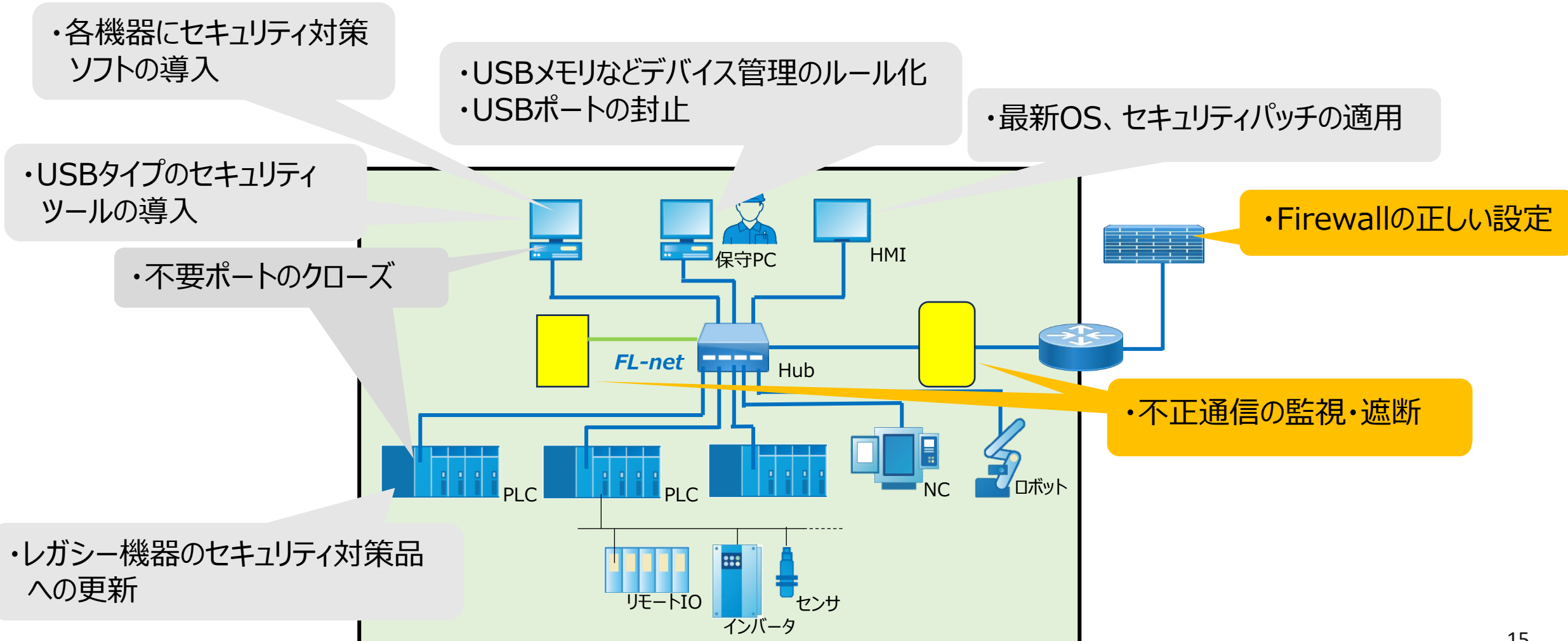
・Firewallの正しい設定

・レガシー機器のセキュリティ対策品への更新



・不正通信の監視・遮断

- 一部の対策として、FL-netのパートナー製品を活用できます。



FL-netでは、パートナー製品登録制度を開始しました。

パートナー製品：FL-netの利便性を向上する製品



セキュリティ対策関連のパートナー製品も登録しています。

※今後もパートナー製品を順次拡大予定です。

登録製品



・TXOne Edgeシリーズ

