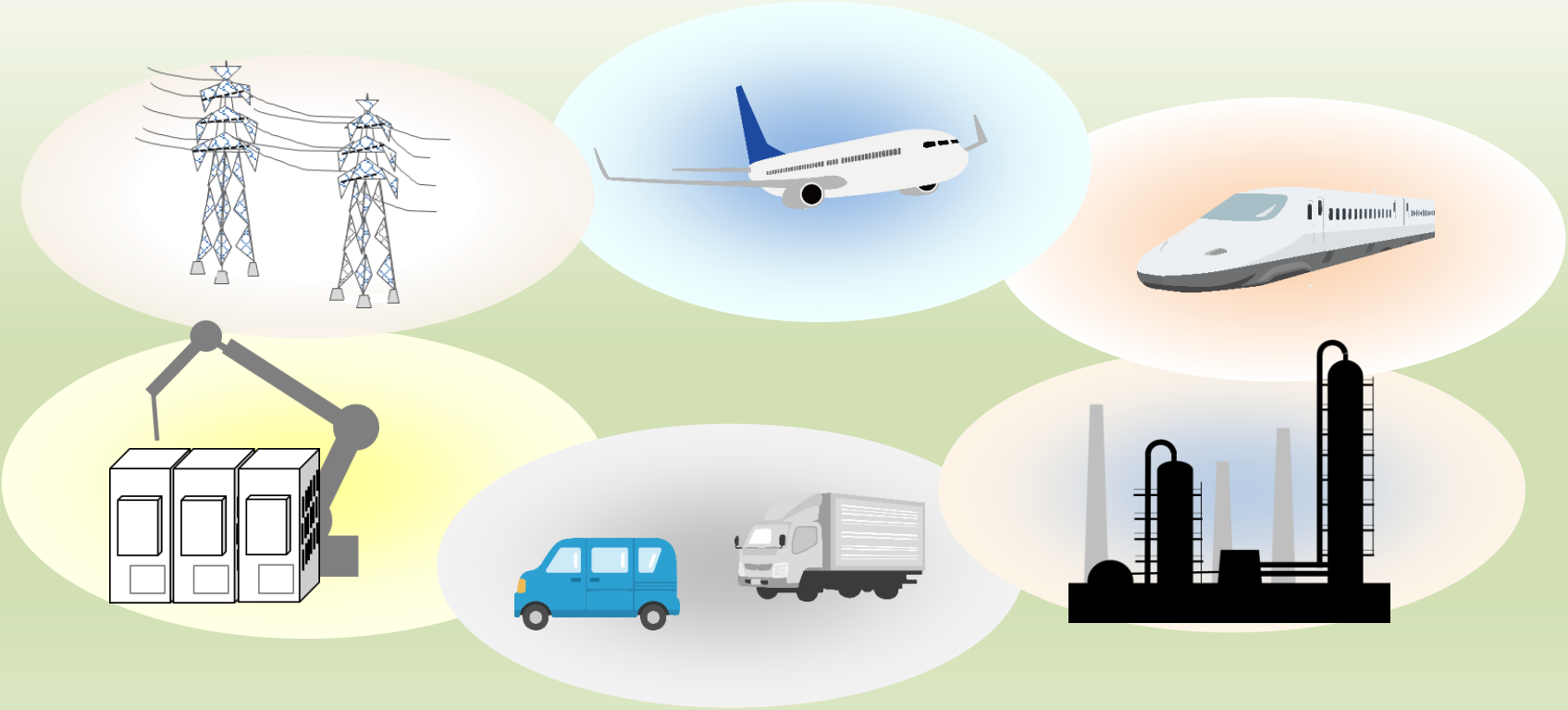
IPA

安全関連システムのセキュリティ向上にむけて

制御システム セーフティ・セキュリティ要件検討ガイド

–ケーススタディ編–



第1版

ケーススタディ編：目次

ケーススタディ編について

- 「ケーススタディ編」では、「基本編」で示した検討手順の理解を深めるために現実のシステムを抽象化したシステム（以下、検討システム）を用いた解説をしています。

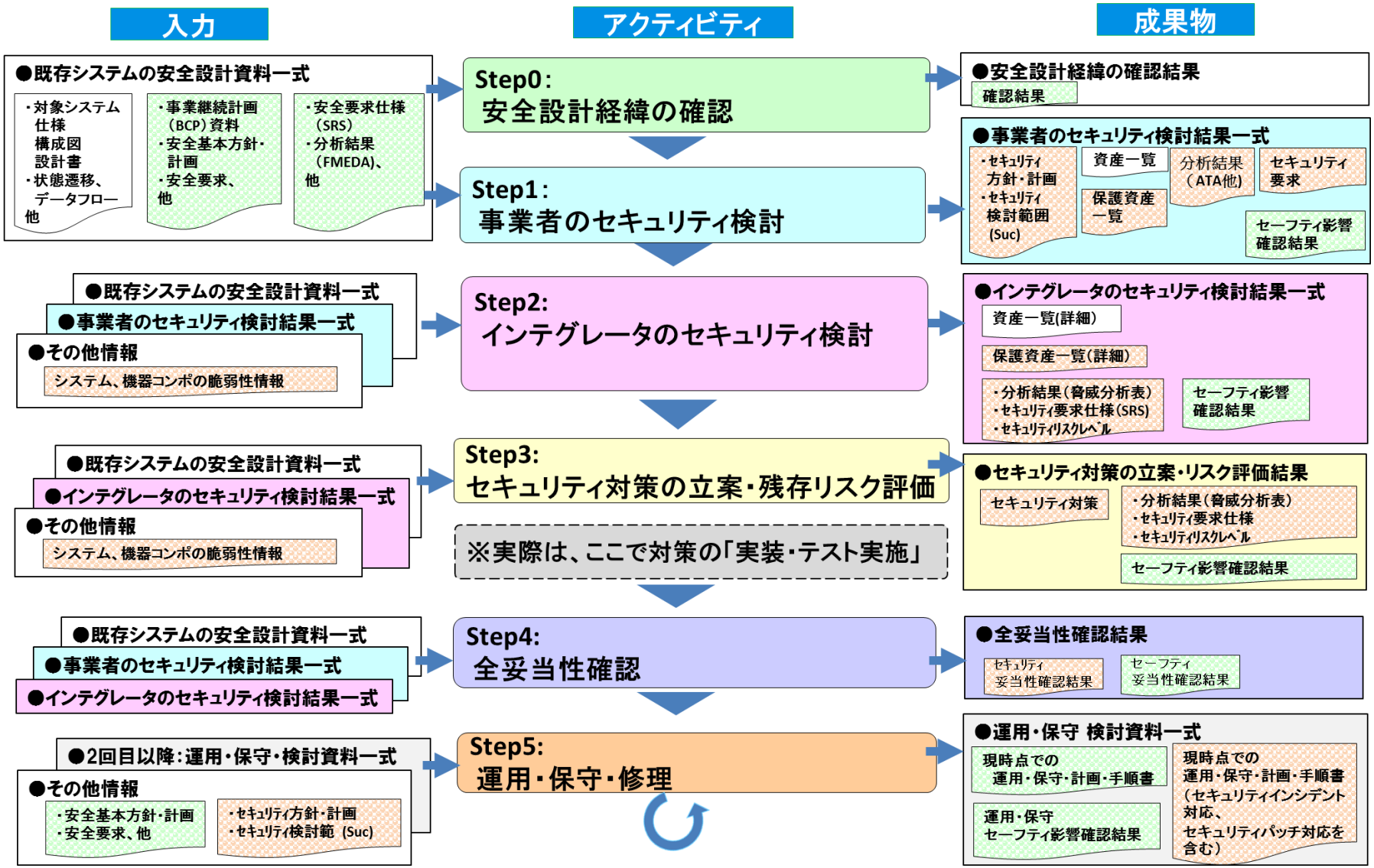
- 検討システムは実在するものではなく、既存の特定製品とは一切関係はありません。また本書に登場する事業者、インテグレータ等もすべて架空であるとします。

- 検討システムは産業用ロボットを含むFA（Factory Automation）システムです。セーフティシステム*1の典型的な構成は、非安全系（被制御機器の制御）と安全関連系が分離されていますが、本検討システムもこの構成となっています。

- ケーススタディ編では、検討を進める上でのポイントを説明する都合上、様々な仮定をしていることにご留意ください。

＊1）本書では便宜上「安全」を「セーフティ」、国際機能安全規格に適合したシステムを「セーフティシステム」と表記しています。またセーフティ・セキュリティをS&Sと表記している箇所もあります。

「既存の制御システム」に対する S&S 検討プロセス（全体像）



Step 0　安全設計経緯の確認

Step0　安全設計経緯の確認

入力	アクティビティ	成果物
・事業継続計画（BCP）資料 ・安全基本方針・計画 ・安全要求、他	0-1 検討システムの事業上のリスクを確認 ・事業リスクの確認 ・安全基本方針の確認	
・検討システム仕様・構成図・設計書 ・状態遷移、データフロー他	0-2 検討システムの概要を確認 ・概要 ・関係者 ・ライフサイクル ・安全対策の経緯 ・デフォルトのセキュリティ機能	確認結果
・安全要求仕様（SRS） ・分析結果（FMEDA）、他		

Step1　事業者のセキュリティ検討

＜入力・成果物の区分＞

一般要求事項　セーフティ　セキュリティ

事業リスクの確認

- セキュリティ検討に先立ち、現状のシステムに関わる背景、経緯を再確認します。
- 本システムを所有する国内事業者が認識する事業リスク及び、運用方針は、以下の通りです。

IEC 62443で定義されるリスク	生産システムでの事業リスク	生産システム運用方針
死亡、負傷などの要員の安全性リスク	工程作業者の負傷、死亡（※）	・労働安全衛生マネジメントの推進 -労働安全の徹底と維持（労災0件）
機器の損害、事業中断などのプロセスの安全性リスク	生産装置の損壊、意図しない生産作業の中断	・設備稼働率の向上 -リモート監視による予防保全 -計画外停止時間〇〇H ・QMSによる品質マネジメントの推進
コスト、法律違反、ブランドイメージ喪失などの情報セキュリティリスク	不良製品の市場クレームによる企業イメージの喪失	・QMSによる品質マネジメントの推進 ・お客様サポートセンターによる対応
違反の通知、法律への違反、重大な影響などの環境リスク	有害物質の建屋内及び周辺地域への流出による環境汚染	・環境マネジメントシステムの推進 -ISO 14001に基づく運用 ・コンプライアンスリスクマネジメント -企業倫理リスクマネジメント委員会運営

※本ケーススタディ編では、作業者の人命に関わるリスクに焦点を絞った解説をしています。

安全基本方針の確認

■一般に企業では、労働安全に関する基本方針を定めて運用しています。
本例における事業者でも、以下のような基本方針が運用されています。

当社は、従業員の安全衛生を最重要経営課題の一つと位置づけ、安全で快適な職場環境づくりと心身の健康維持と醸成に努めます。

【労働安全衛生の基本方針】

1．法令の遵守
安全衛生関する法令、規格・基準に定められた義務を遵守します。

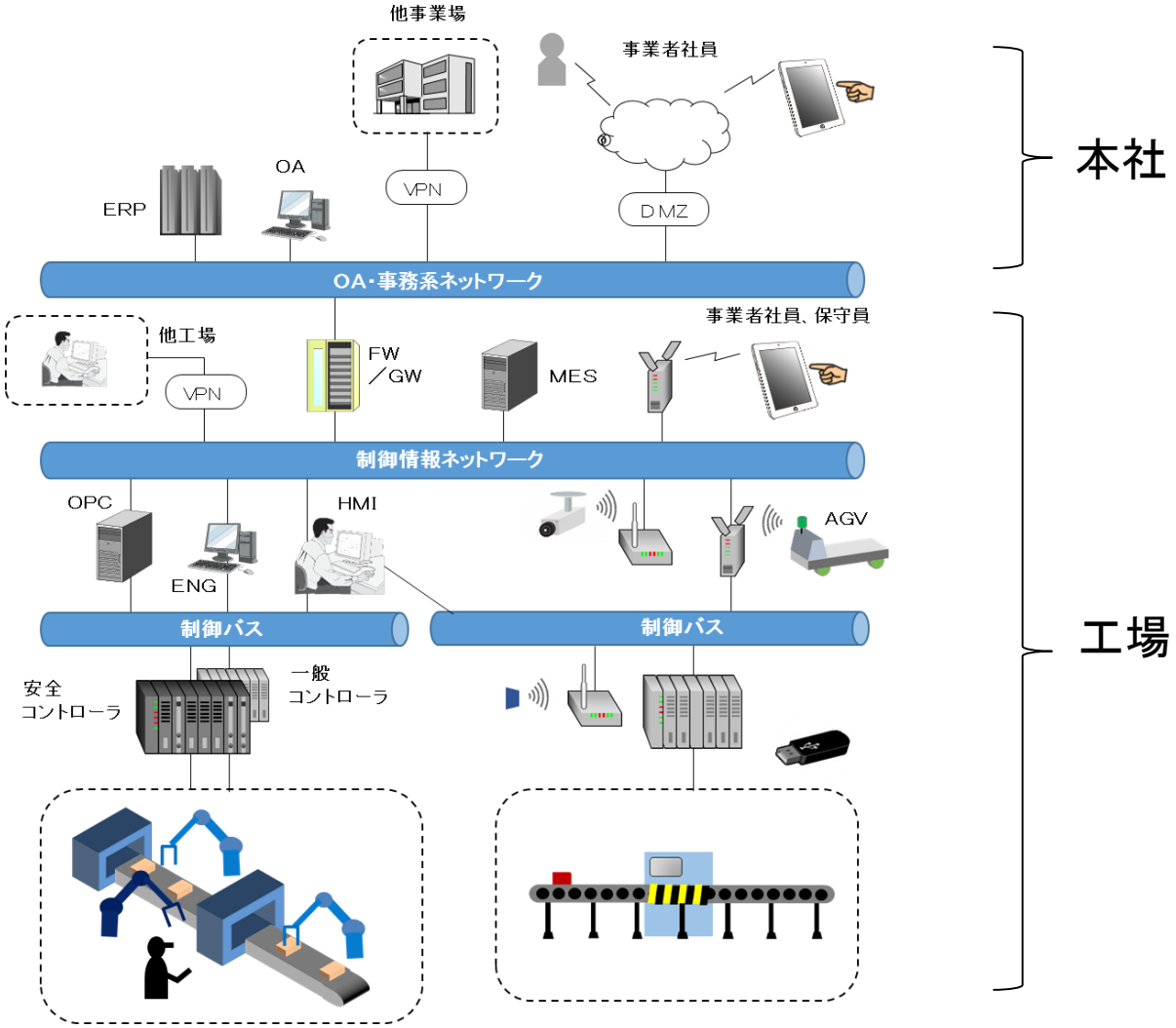
2．労働安全マネジメントシステムの構築
労働安全活動を向上させるための労働安全マネジメントの仕組みの維持向上に努めます。

3．安全衛生に関する目標設定と運用管理の推進
労働災害や職場健康管理の基準を定め、目標達成に向けた労働安全衛生計画を作成、遂行します。

4．健康のための取り組み
当社従業員のこころとからだの健康維持・増進に向けた取り組みを行います。

概要

- 下図のような日本国内の工場内に設けられた産業用ロボット及び生産機器を用い組み立て生産を行うFAシステムです。

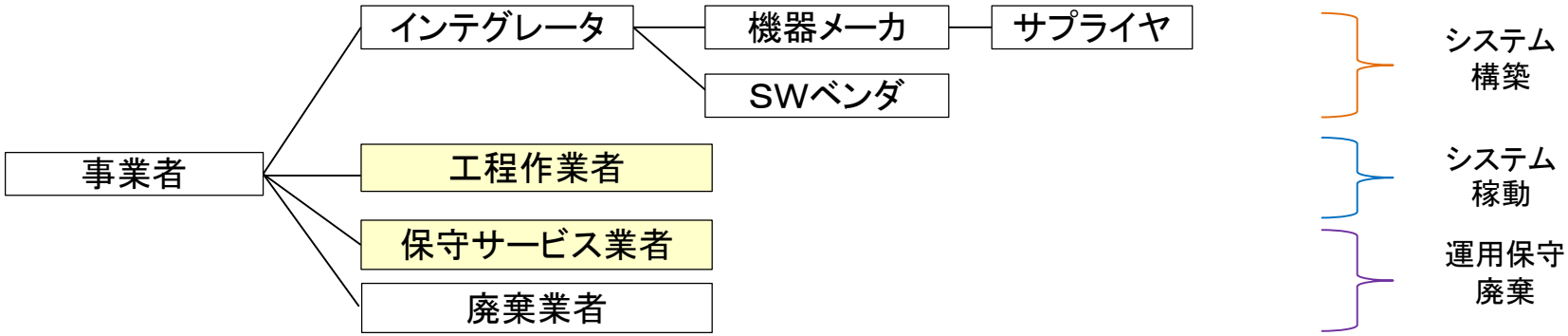


概要 （とりまく事業環境と変化）

- このシステムは従来、工場内で閉じたものでしたが、近年の事業形態の変化により、以下の様な変化が生じてきました。
  - 事業者の基幹情報ネットワークを経由し、事業者社員、保守員などのインターネット経由のアクセスがある。（保守サービス業者による遠隔監視含）
  - 製造工程にはAGV（自動搬送車）による搬送経路も含まれ各種センサーからのデータ送受信が発生している。
  - 事業者社員、保守員などが構内無線を経由してアクセスしている。
- 現状工場内では複数の生産ラインが稼働中です。この既設ラインに隣接して新たな生産ラインを構築することになりました。
- この新設ラインのセーフティ要件は、機能安全に適合済の既設ラインを踏襲しますが、IEC 62443 によるセキュリティ対策の検討が必要になってきました。

関係者

- 検討システムの関係者を以下に示します。本ガイドでは、工程作業者または運用保守業者の保守員が危害に会う可能性があるとします。



関係者	役割	主な関連ﾌｪｰｽﾞ
事業者	工場並びに生産設備システムの保有者	全体
インテグレータ	事業者の要求に従って生産システム全体の設計、供給、製造などを行い、制御インタフェース、制御システムの接続を含む安全戦略を担当　（ISO 11161: 2007参考）	システム構築
機器メーカ	生産設備機器・装置ならびに当該機器・装置をコント ロールするための制御システムを開発、提供する企業	システム構築
SWベンダ	機器・装置に搭載される生産管理、制御プログラムを作成、提供	システム構築
サプライヤ	機器を構成するコンポ、部品を機器メーカに提供する製造業者（HW/SW含む）	システム構築
工程作業者	製造ラインで生産に従事する作業者	システム稼動
保守サービス業者	設備機器の運用保守サービスを事業者から委託される業者	運用・保守
廃棄業者	設備機器の廃棄を事業者から委託される業者	運用・保守・廃棄

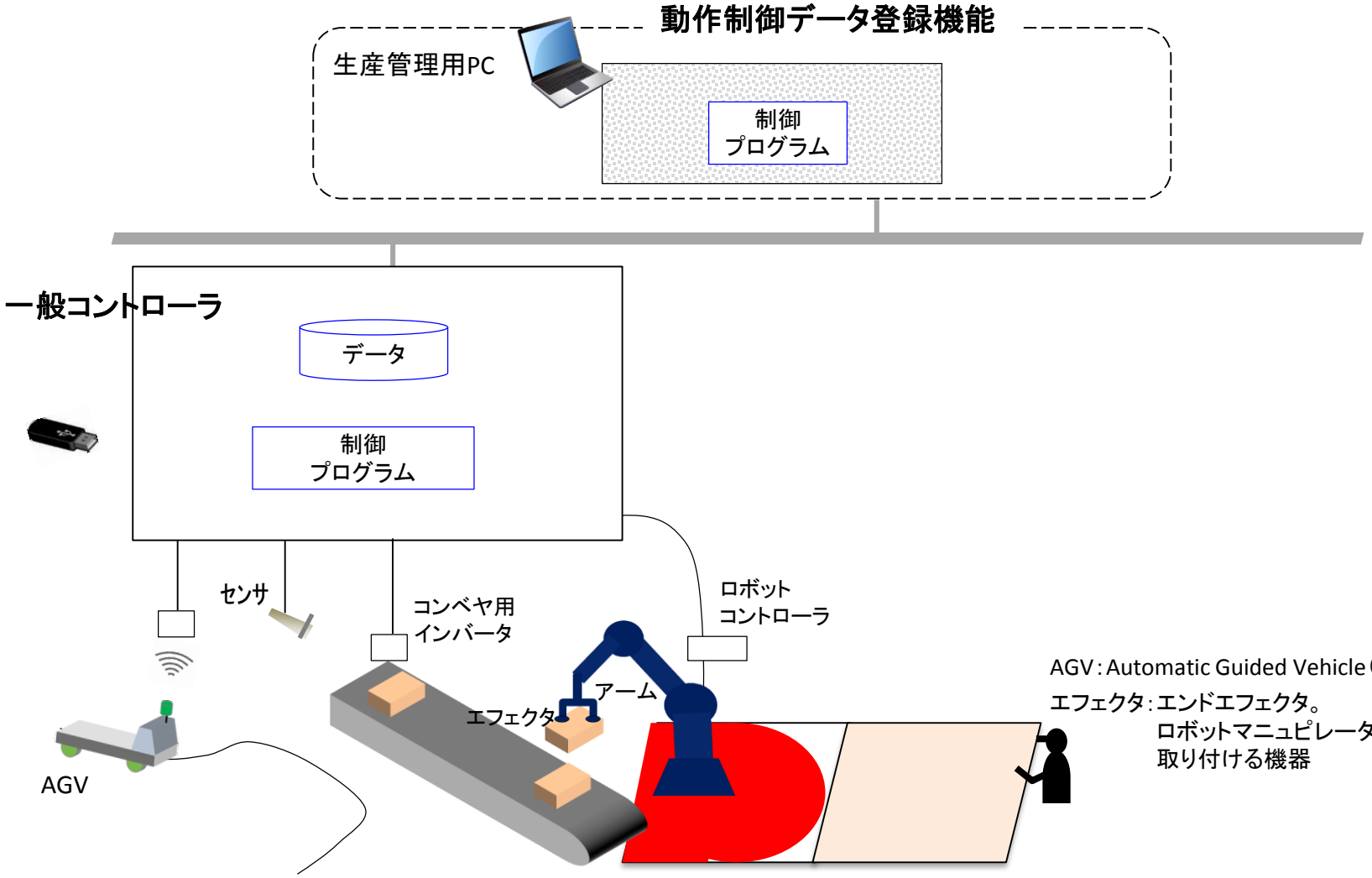
ライフサイクル

検討システムのライフサイクルとその関係者は以下の通りです。

フェーズ		概要	関係者
企画	引き合い 見積もり 受注	インテグレータは、事業者と契約内容について合意し、契約する。 性能、機能、納期、コスト、規制・法令など	事業者、インテグレータ
設計	システム基本設計	インテグレータは、契約に基づき、システムの構成などシステムの基本設計を行う。	インテグレータ
	サブシステム設計	インテグレータおよびインテグレータから設計を請け負った業者は、システム基本設計に基づき、サブシステムの設計を行う。ソフトウェアの開発、ハードウェアの開発を伴う場合はソフトウェア・ハードウェアの設計も含む。	インテグレータ、機器メーカ、サプライヤ、SWベンダ
製造	サブシステム製造ための調達	インテグレータおよびインテグレータから設計を請け負った業者は、サブシステムを構成するソフトウェア、ハードウェアを調達する。	インテグレータ、機器メーカ、サプライヤ、SWベンダ
	サブシステム製造	インテグレータおよびインテグレータから製造を請け負った業者は、サブシステムを製造する。ソフトウェア・ハードウェアの開発を伴う場合はソフトウェア・ハードウェアの製造も含む。	インテグレータ、機器メーカ、サプライヤ、SWベンダ
	サブシステム試験	インテグレータおよびインテグレータから製造を請け負った業者は、サブシステムが設計通りであることを試験する。	インテグレータ
	総合試験のための調達	インテグレータは、サブシステムを組み合わせるためのソフトウェア・ハードウェアを調達する。	インテグレータ、機器メーカ、サプライヤ、SWベンダ
	総合試験	インテグレータおよびインテグレータから製造を請け負った業者は、サブシステムを組み合わせ、システム基本設計通りであることを試験する。	インテグレータ、機器メーカ、HWサプライヤ、SWベンダ
	顧客立会検査	インテグレータは、顧客立会いの下、契約に基づく試験を行う。	事業者、インテグレータ
据え付け	出荷	インテグレータおよびインテグレータから請け負った輸送業者は、製造した製品・システムを輸送する。	インテグレータ、輸送業者
	設置のための調達	事業者およびインテグレータは、設置するための機器を調達する。	事業者（事業者から委託を受けた業者を含む）、インテグレータ
	設置・据え付け	インテグレータは、使用場所に設置・据え付ける。	インテグレータ
	試験、引き渡し	インテグレータは、契約の引き渡し条件に基づき、試験する。	事業者、インテグレータ
運用	定常運用	事業者および事業者から運用を請け負った業者は、運転マニュアルに基づいて、システムの運用を行う。	事業者、保守サービス業者
	非常時運用	事業者および事業者と契約している業者は、システム異常からの復旧を行う。	事業者（施設管理、情シスなど）、事業者と契約している保守サービス業者（含セキュリティコンサルなど）
	保守・点検	事業者あるいは事業者と契約しているサービス業者は、システムの保守作業を行う。修理・調整が必要な製品は、サプライヤーに修理・調整に出す。交換が必要な製品はサプライヤーから調達する。	事業者（施設管理部署、情シスなど）、保守サービス業者、機器メーカ
	拡張・リニューアル	システムを拡張する。システムあるいはシステムの一部を入れ替える。	事業者、保守サービス業者、インテグレータ、代理店など
廃棄		事業者から委託された廃棄業者はシステムを廃棄する。	事業者、廃棄業者

安全対策の経緯 （安全対策前の構成）

- 安全対策が施される前のロボット近辺の状態を以下に示します。
  この状態から次頁以降の手順で安全分析が実施されます。



AGV：Automatic Guided Vehicle（無人搬送車）
エフェクタ：エンドエフェクタ。
ロボットマニュピレータの先端に
取り付ける機器

安全対策の経緯　（安全制御システムの安全分析）

- 安全制御システムの安全リスクアセスメントは、機械の構造・機能仕様の他、誰がどのように使うのか、保全作業なども含めて検討システムに潜む危険源を洗い出します。その危険源によって発生しうる危害の大きさとその発生確率から、その危険源ごとのリスクを推定します。
  ここでは下表のように分析されています。

部位	危険源	危険事象	被害程度	暴露頻度	回避可能性	リスクレベル
エフェクタ	挟まれ	エフェクタが衝突する	軽傷	頻繁	不可	SIL2
アーム	挟まれ	関節部に指を挟まれる	重傷	頻繁	可	SIL2
アーム	衝突	アーム（エフェクタ）が衝突する	軽傷	頻繁	不可	SIL2
コンベア	巻き込まれ	コンベヤに手指を巻き込まれる	重傷	時々	不可	SIL2
コンベア モータ・インバータ	感電	通電部に接触して感電	軽傷	まれ	不可	SIL1

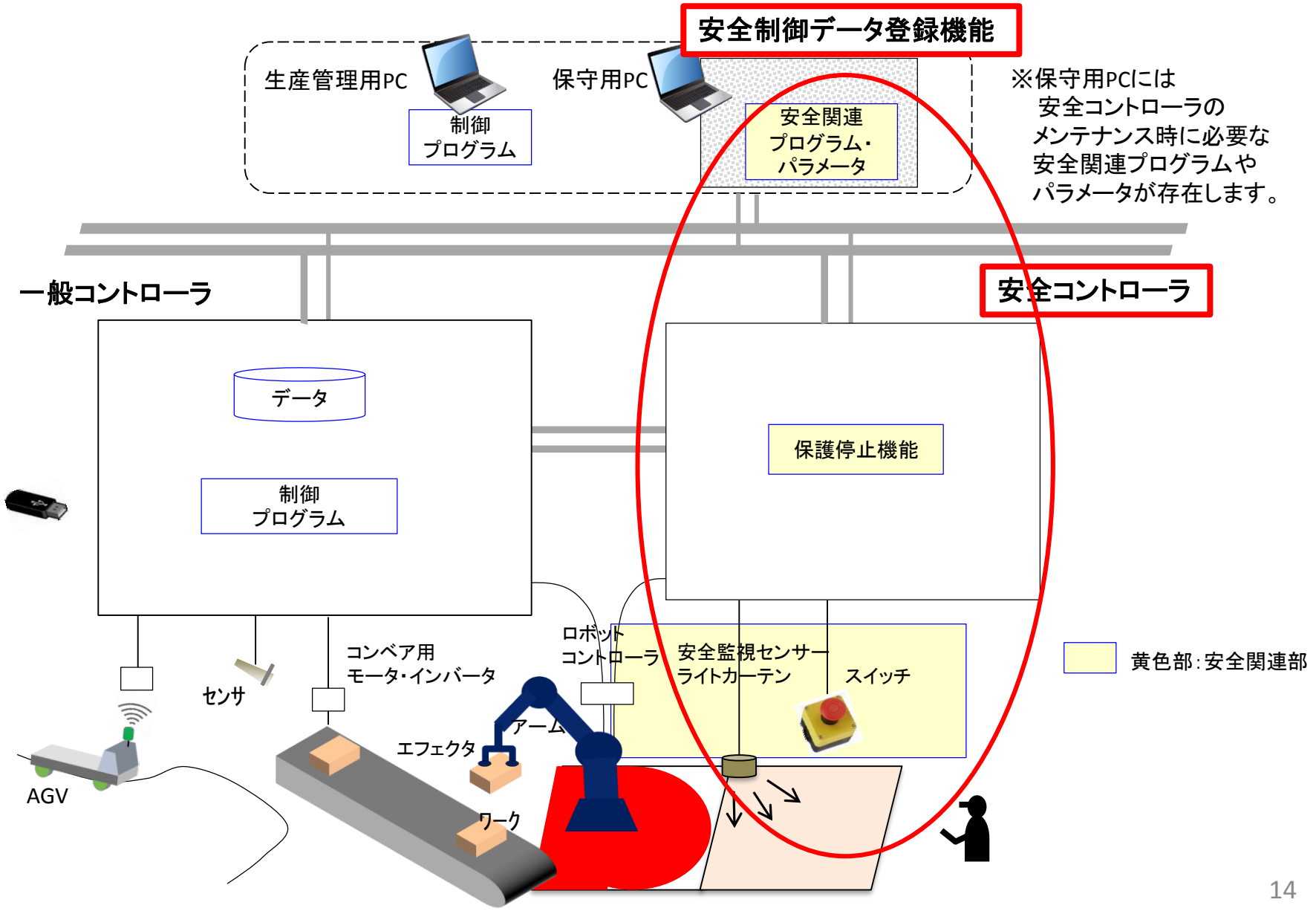
※リスクレベルにはSIL（ISO 61508 電気・電子・プログラマブル電子（E/E/PE）安全関連システム 安全度水準。（SIL1，SIL2，SIL3，SIL4））と、
PLr（ISO 13849-1　機械類の安全性−制御システムの安全関連部−第1部：設計のための一般原則 から 要求パフォーマンスレベル）がある。
PLr=dがSIL2、PLr=eがSIL3に相当する

安全対策の経緯　（安全システム仕様）

- ロボットは工程作業者との協働作業を行うため、防護柵で囲まない構成です。
- コンベアの危険区域に工程作業者が進入すると、機械を非常停止します。
- ロボットの稼働空間に人が進入すると、レーザースキャナが進入検知し、ロボットを減速運転します。さらに、ロボットの危険区域に人が進入すると、ロボットを保護停止します。これにより、ロボットの危険源のリスクを低減します。
- ロボットの減速運転、保護停止機能は、協働作業ロボットの安全機能として規格適合(ISO 10218-1)が必要です。ここでは、安全センサ（ライトカーテン、レーザースキャナ、非常停止スイッチ）の入力を安全コントローラが判断してロボットの安全機能を実行します。
- 以降の図では**保護停止機能**のみ記載します。
- リスクレベルSIL2，SIL3については、安全対策を実施し、SIL1以下に低減することが求められます。

部位	危険源	危険事象	安全対策	安全機能（安全コントローラ）	被害程度	暴露頻度	回避可能性	リスクレベル
エフェクタ	挟まれ	エフェクタが衝突する	進入検知して減速	・安全状態監視 **・保護停止機能** ・非常停止機能	なし	頻繁	可	―
アーム	挟まれ	関節部に指を挟まれる	進入検知して停止		軽傷	頻繁	可	SIL1
アーム	衝突	アーム（エフェクタ）が衝突する	進入検知して減速		軽傷	頻繁	可	SIL1
コンベア	巻き込まれ	コンベヤに手指を巻き込まれる	進入検知して停止		なし	時々	不可	―

安全対策の経緯　（安全対策後の構成）



デフォルトのセキュリティ機能

- 既存の安全コントローラは、セキュリティ分析を実施していません。
  但し、独自に下記のセキュリティ機能が実装済です。
  - 認証機能
    ネットワーク経由でのログイン時ならびに、データ登録装置など外部機器を直接接続する際のID/PW認証機能
  - 権限管理
    パラメータやデータ変更者、グループの設定管理機能
  - ログ機能
    ネットワークアクセス、環境変更、操作情報の自動記録機能

- 事業者は現状、下記のような対応は実施しています。
  - 情報システム部門が存在し、スタッフへのセキュリティ教育が実施されている
  - 事務系システムと制御系システムはファイヤウォールで分離されている
  - 保守を委託する企業の選定においては、自社セキュリティ基準を遵守させている

Step 1　事業者のセキュリティ検討

Step0　安全設計経緯の確認

Step1　事業者のセキュリティ検討

入力	アクティビティ	成果物
・事業継続計画（BCP）資料 ・安全基本方針・計画 ・安全要求、他	1-1 セキュリティ方針・計画の策定、SuC＊識別	・セキュリティ方針・計画 ・セキュリティ検討範囲（Suc）
・検討システム仕様・構成図・設計書 ・状態遷移、データフロー他	1-2 セキュリティリスク分析 ・事業者による資産明確化 ・ZC（ゾーン・コンジット）分割 ・保護資産の抽出 ・影響度・発生可能性評価 ・セキュリティ要求の抽出	資産一覧 分析結果（ATA他） 保護資産一覧 セキュリティ要求
	1-3 セーフティへの影響確認	セーフティへの影響確認結果

Step2　インテグレータのセキュリティ検討

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

*) SuC（System under Consideration ）：セキュリティ検討対象システム

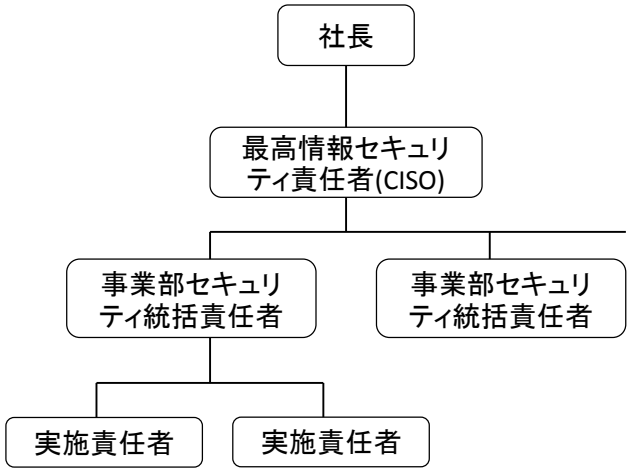
セキュリティ方針・計画の策定

■事業者は情報セキュリティ対応には取り組んでいます。（次頁方針参照）
一方、制御系セキュリティ対応はその重要性を理解し、システム構築に必要となる十分なコンピテンシを確保します。

■事業者では検討システムのセキュリティ推進にあたり、下記事項の重要性を認識し、外部企業・組織を含めた対応計画を検討しています。

【体制】
- 各組織の権限、事業所・工場責任者のコンピテンシーならびに所掌責任の定義
- 教育・研修：全社員向け、階層別教育ならびにセキュリティ担当者向け教育
- 体制構築スケジュール

【セキュリティマネジメント】
- マネジメントプロセス定義、管理
- セキュリティガイドライン
  セキュリティ設計・実装方針、V&Vの作成、運用、問題管理、更新（含むパッチ）管理
  セキュリティ監査要領、文書化　など



セキュリティ方針・計画の策定

■事業者では以下のような情報セキュリティ方針が運用されており、保守契約に基づき、ソフトウェアアップデートサービスを受けています。

当社は、当社基本理念に基づき、お客様に安全性の高い製品を提供するとともに、ネットワークの脆弱性に起因するサイバー攻撃に対応するため、情報セキュリティマネジメントシステムを構築し、お客様の信頼を得られるよう、セキュリティレベルの向上に努めます。

【セキュリティ基本方針】

●セキュリティ体制の構築
社内に情報セキュリティの責任体制を設け、インシデントレスポンスを含めたリスクマネジメントを行います。

●安全、安心な製品・サービスの提供
当社事業において、情報セキュリティ対策を講じることにより安全で安心な製品・サービスを提供します。

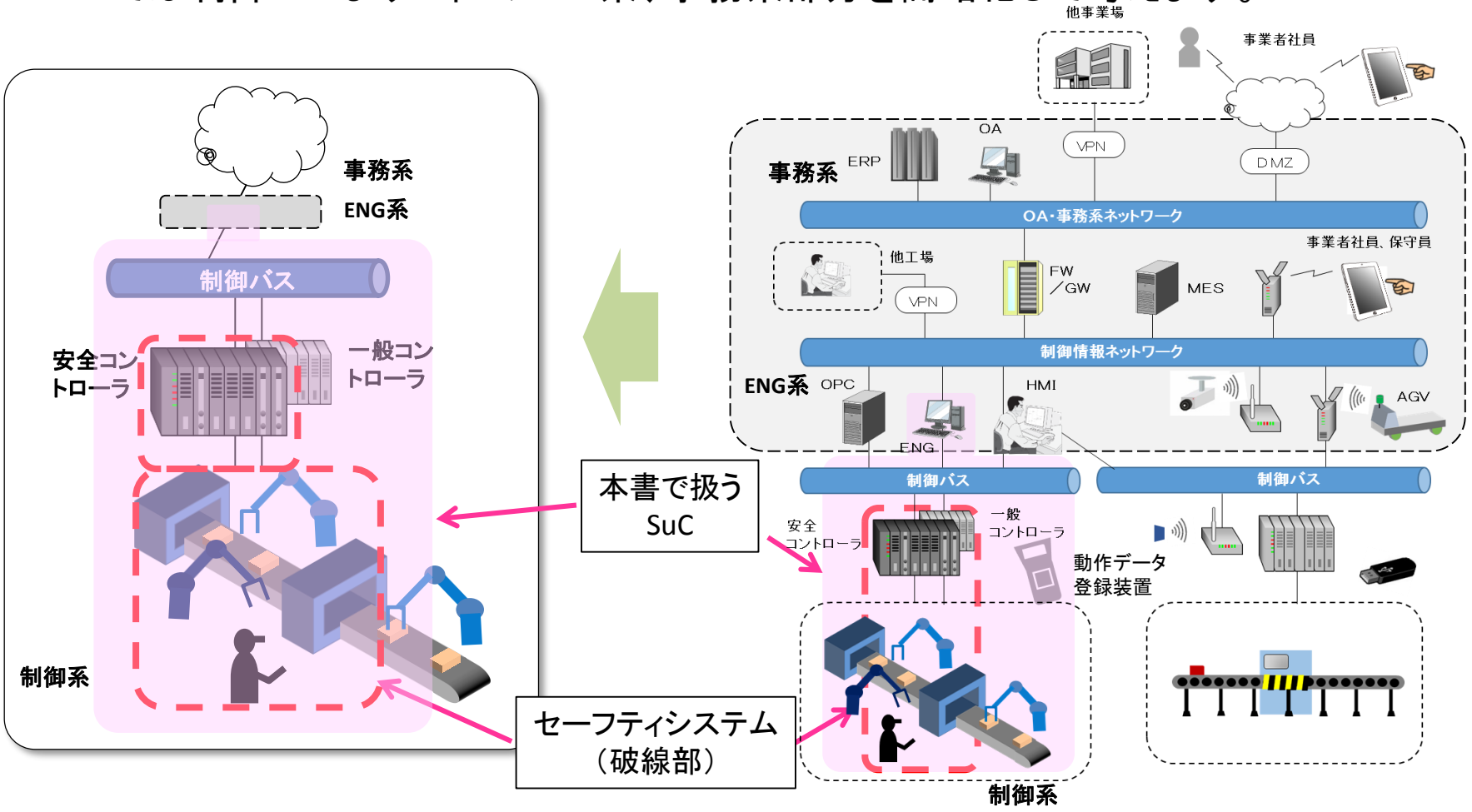
●情報資産・人的資産の保護と継続的管理
当社の扱う情報資産を適切に管理し、要員の安全ならびに要員が保有する知的財産の保護に努めます。

●法令遵守
情報セキュリティに関係する法令、指針及びその他社会的規範を遵守します。

●教育・訓練
当社役員、従業員に対して情報セキュリティの意識向上を図り、教育・訓練を行います。

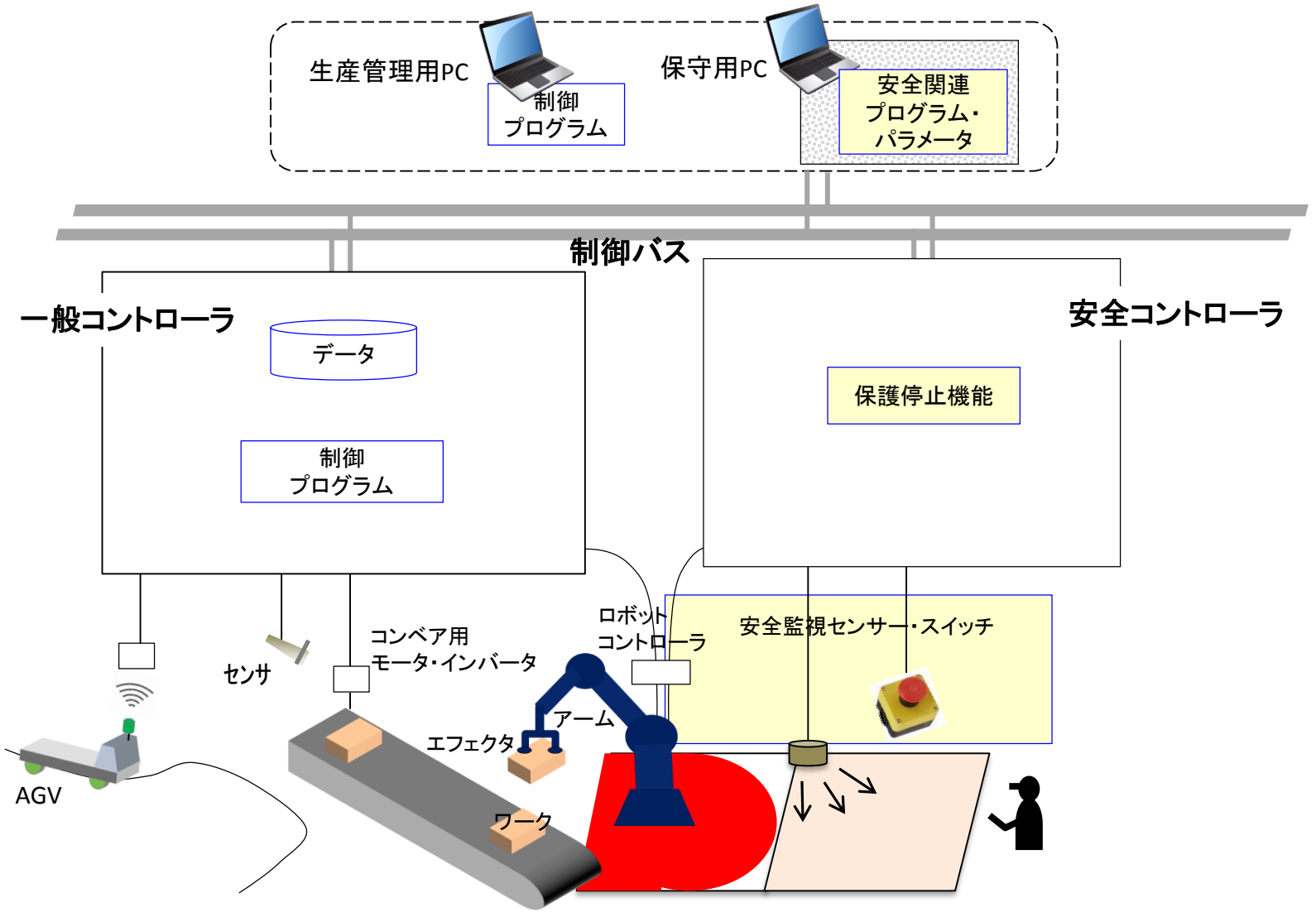
SuC識別

■セーフティシステムのバウンダリ（境界）と共に、本書で扱うセキュリティ検討システム（以下SuC部分）を示しています。
ここでは制御バスより上位のENG系、事務系部分を簡略化して考えます。



SuC識別

■事業者にて把握、理解しうる範囲で検討システムの構成を確認します。



事業者による資産明確化

- 前掲図に対応する資産リストを作成します。
  各コントローラ上で動作するソフトウェアはコントローラに包含されています。

分類	ゾーン	内容
情報資産（論理的資産）	ENG系	動作制御データ登録機能
	制御系	一般コントローラの機器制御機能
		安全コントローラの安全機能
機能資産	ー	生産計画通りに製造が継続できる
		:
物理資産	ENG系	生産管理用PC、保守用PC
		HMIシステム
		:
	ネットワーク	制御バス他
	制御系	産業用ロボット
		一般コントローラ
		安全コントローラ
		ロボットコントローラ
		安全監視センサー・スイッチ
人的資産	ー	作業者、保守員の命、身体
		ロボット教示方法
		保守・メンテナンス方法
		:

ZC（ゾーン、コンジット）分割

- 識別されたSuCに対してZC（ゾーン、コンジット）分割を行います。

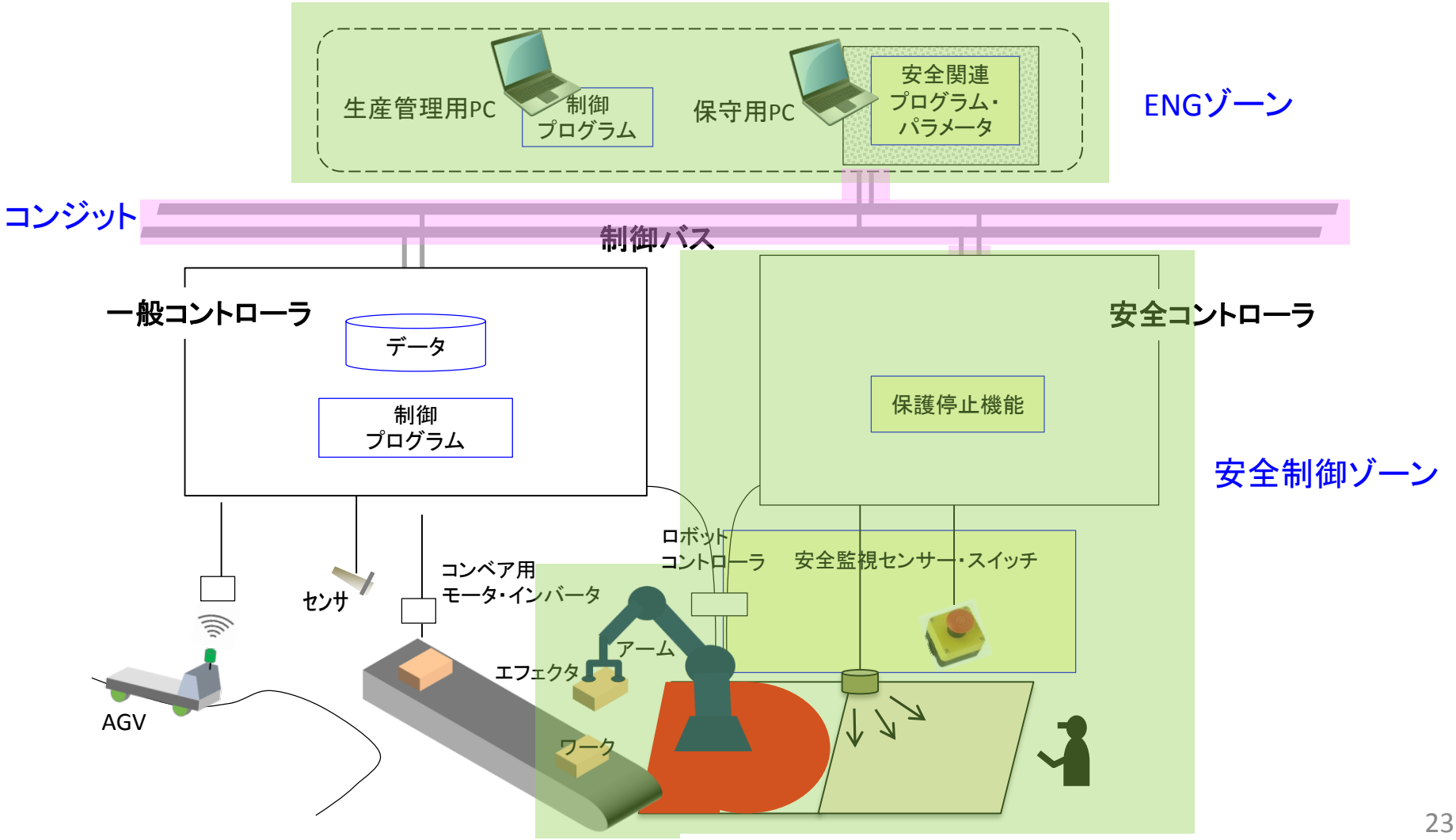
- 分割は、保護すべき資産の重要性、運用機能、物理的または論理的な配置、必要最小限のアクセス、組織の基準等に基づいて行われます。

- 制御用の装置、システムは事務系、ENG系のものとは別のゾーンとして分割します。また、安全系システムは非安全系システムとは別のゾーンとして分割します。

- 一時的に接続される端末装置、無線機器、信頼できないネットワークからアクセスされる機器は別のゾーンとします。

ZC（ゾーン、コンジット）分割

本検討システムでは、下記のように分割しています。
制御系は一般系と安全系を分け、下図では安全制御ゾーンのみを示しています。

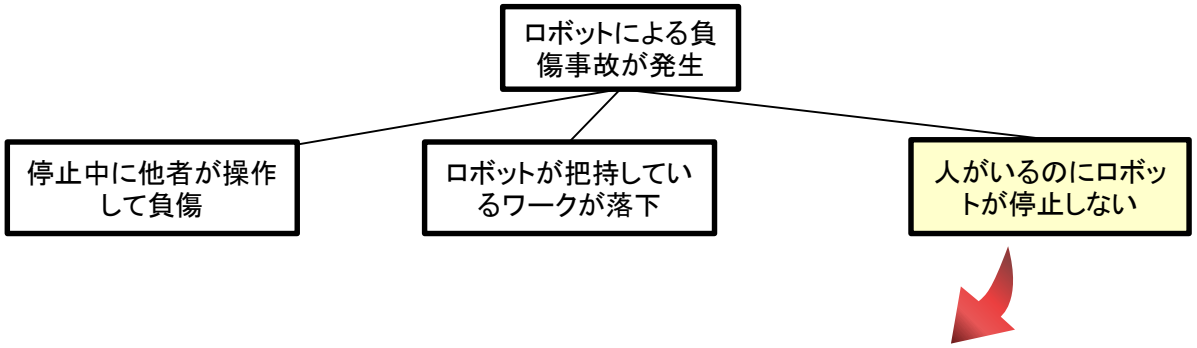


保護資産の抽出

- 抽出されている資産のうち、セキュリティ攻撃から保護すべき重要度の高い資産を抽出します。
  （「制御システムのセキュリティリスク分析ガイド」（IPAセキュリティセンター）を参照）

- セーフティな制御システムでは、HSE（H:健康、S：安全性、E:環境への影響）＋AIC(A:可用性、I:完全性、C：機密性）が重要です。
  （本書では安全性(S)部分以外の記述は省略しています）

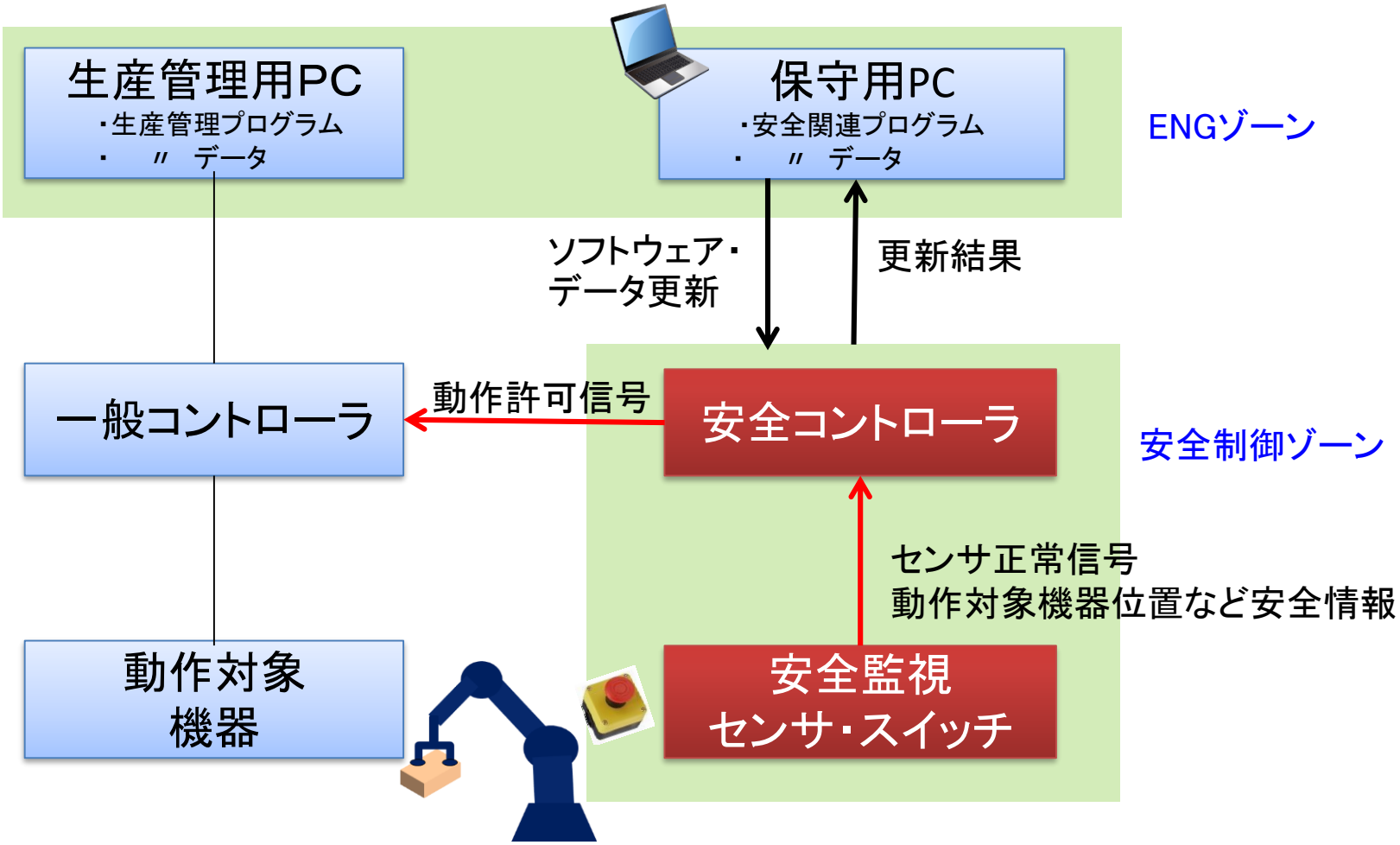
- 工程作業者の死傷を最上位とし、本書では相互の関係性の表記に優れるATA（攻撃ツリー分析）を用いたリスク分析により、以下の結果になりました。



資産			重要度
人的資産	ー	作業者、保守員の命、身体	◎
		ロボット教示方法	
		保守・メンテナンス方法	

影響度・発生可能性評価（脅威メカニズムの識別）

- 影響度ならびに発生可能性が高いと考えられる作業者の死傷につながるメカニズムが抽出されます。ここではソフトウェアやデータ更新時に正しく更新できないリスクが識別されています。



セキュリティ要求の抽出、セーフティの影響確認

- 前述の検討に基づき、事業者のセキュリティ要求項目が提示されます。

分類	ゾーン	内容	重要度
物理資産・情報資産	ENGゾーン	生産管理用PC、保守用PC	○
	安全制御ゾーン	産業用ロボット、教示装置	◎
		安全コントローラ	◎
		安全監視センサー・スイッチ	◎
人的資産	ー	作業者、保守員の命、身体	◎

HSE+AICの観点でのセキュリティ要求

事業者のセキュリティ要求項目	
工程作業者の死傷を生じさせないこと	安全性（S）
故意や過失などによる生産システムの停止を防止し、許可された利用者が必要なときに必要な情報にアクセス可能であることを確実にすること	可用性（A）
生産システムの情報・データが常に完全であることを保証すること。許可されていない利用者によってデータを改ざんまたは破壊されるのを防ぐこと	完全性（I）
生産に関わる情報には許可された利用者のみアクセス可能とすること	機密性（C）

- セキュリティ分析の結果作成されたセキュリティ要求項目に基づき、既存 のセーフティシステムに与える影響を検討します。
- 本書では、セキュリティ要求項目がインテグレータに対して提示されます。

Step 2　インテグレータのセキュリティ検討

Step1 事業者のセキュリティ検討

Step2　インテグレータのセキュリティ検討

入力	アクティビティ	成果物
・検討システム 仕様・構成図・設計書 ・状態遷移、データフロー 他		
・セキュリティ方針・計画 ・セキュリティ検討範囲（Suc）	2-1　事業者からの要求事項の確認 ・事業者セキュリティ要求事項の確認 ・システム構成の詳細化	詳細資産一覧
資産一覧		
・安全要求仕様（SRS） ・分析結果（FMEDA）、 他		
分析結果（ATA他）	2-2　セキュリティリスク分析 ・セキュリティリスク分析の手順 ・インテグレータによる保護資産の抽出 ・脅威の識別 ・脆弱性の識別 ・被害内容の確認	保護資産一覧（詳細）
保護資産一覧		・分析結果（脅威分析表） ・セキュリティ要求仕様 ・セキュリティリスクレベル
セキュリティ要求		
システム、機器の脆弱性情報		
セーフティへの影響確認結果	2-3 リスク評価 ・評価指標 ・リスクレベルの求め方 ・リスクレベルの決定	セーフティへの影響確認結果

Step3 セキュリティ対策の立案と残存リスク評価

＜入力・成果物の区分＞

一般要求事項　セーフティ　セキュリティ

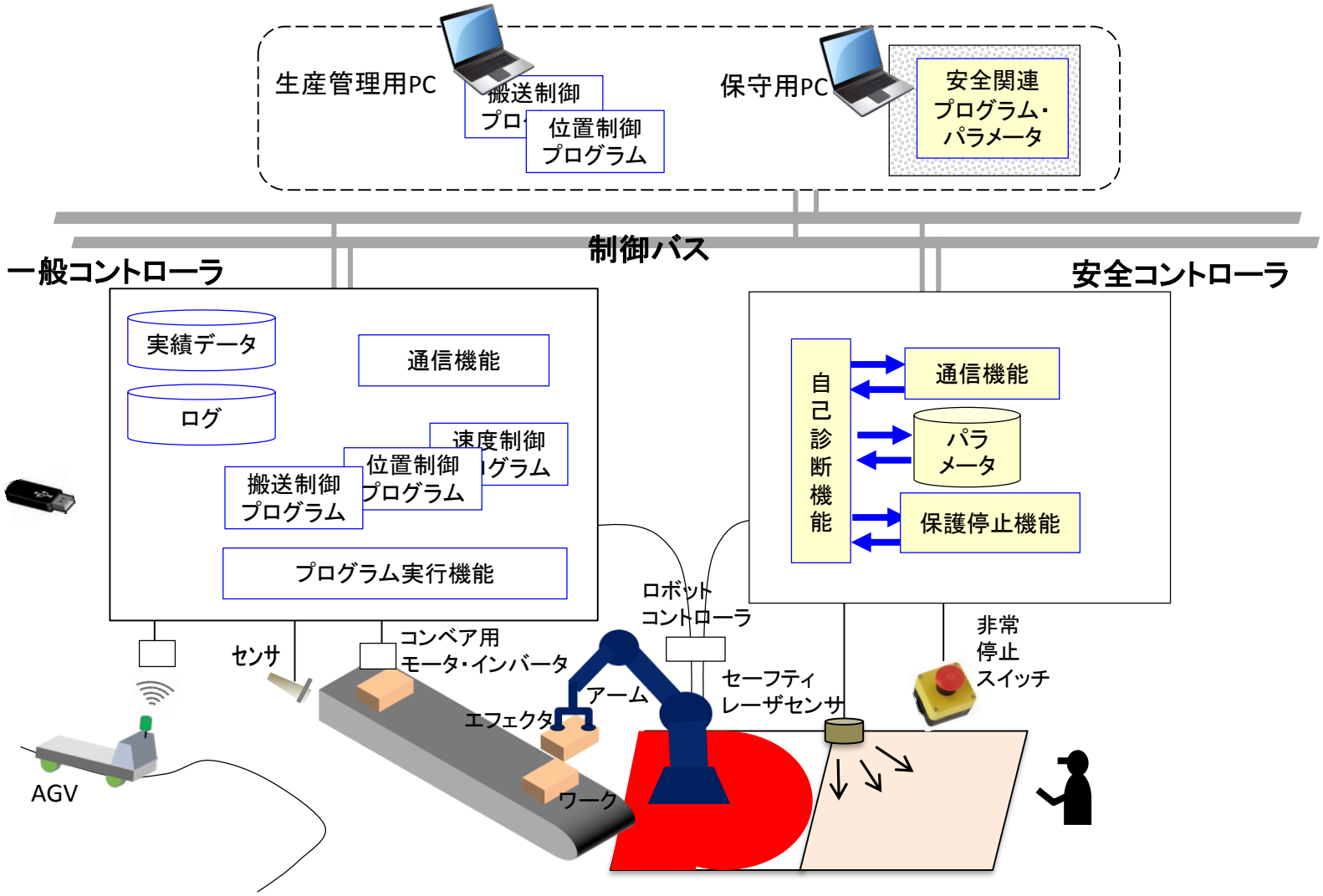
事業者セキュリティ要求事項の確認

- 事業者で作成済のセキュリティ方針、計画をインプットとし事業者のセキュリティ要求を確認します。
- 下記の施策は既知事例情報等も参考し、事業者とインテグレータで検討の上定められます。

事業者のセキュリティ要求項目		施策
工程作業者の死傷を生じさせないこと	安全性（S）	労働安全の徹底
故意や過失などによる生産システムの停止を防止し、許可された利用者が必要なときに必要な情報にアクセス可能であることを確実にすること	可用性（A）	ユーザIDとPW管理、従業員カードによる入場管理
生産システムの情報・データが常に完全であることを保証すること。許可されていない利用者によってデータを改ざんまたは破壊されるのを防ぐこと	完全性（I）	現場で使用する機器管理、ウィルスパッチ適用
生産に関わる情報には許可された利用者のみアクセス可能とすること	機密性（C）	ユーザIDとPW管理

システム構成の詳細化

■インテグレータがコントローラの機能構成を下図のように詳細化します。



セキュリティリスク分析の手順

- 作成された詳細構成に基づき、インテグレータは以下の手順に従ってセキュリティ分析を進めます。

セキュリティリスク分析の手順

抽出・検討項目		備考	
保護資産の抽出		インテグレータによる保護資産の抽出	
脅威の識別		脅威の分類（通信妨害、不正アクセス、改ざん、脆弱性利用・・）	
脆弱性の識別		事業リスクにつながる事象・事業者セキュリティ要求からの逸脱	
被害内容の確認		脅威事象発生時の被害内容	
リスク評価*1	影響度	3段階のレベルで分類	高中低
	発生可能性	3段階のレベルで分類	高中低
	リスクレベル	3段階のレベルで分類	高中低

＊1）本書では、セーフティも含めたリスク評価とするため、Step2-3にて実施しています。

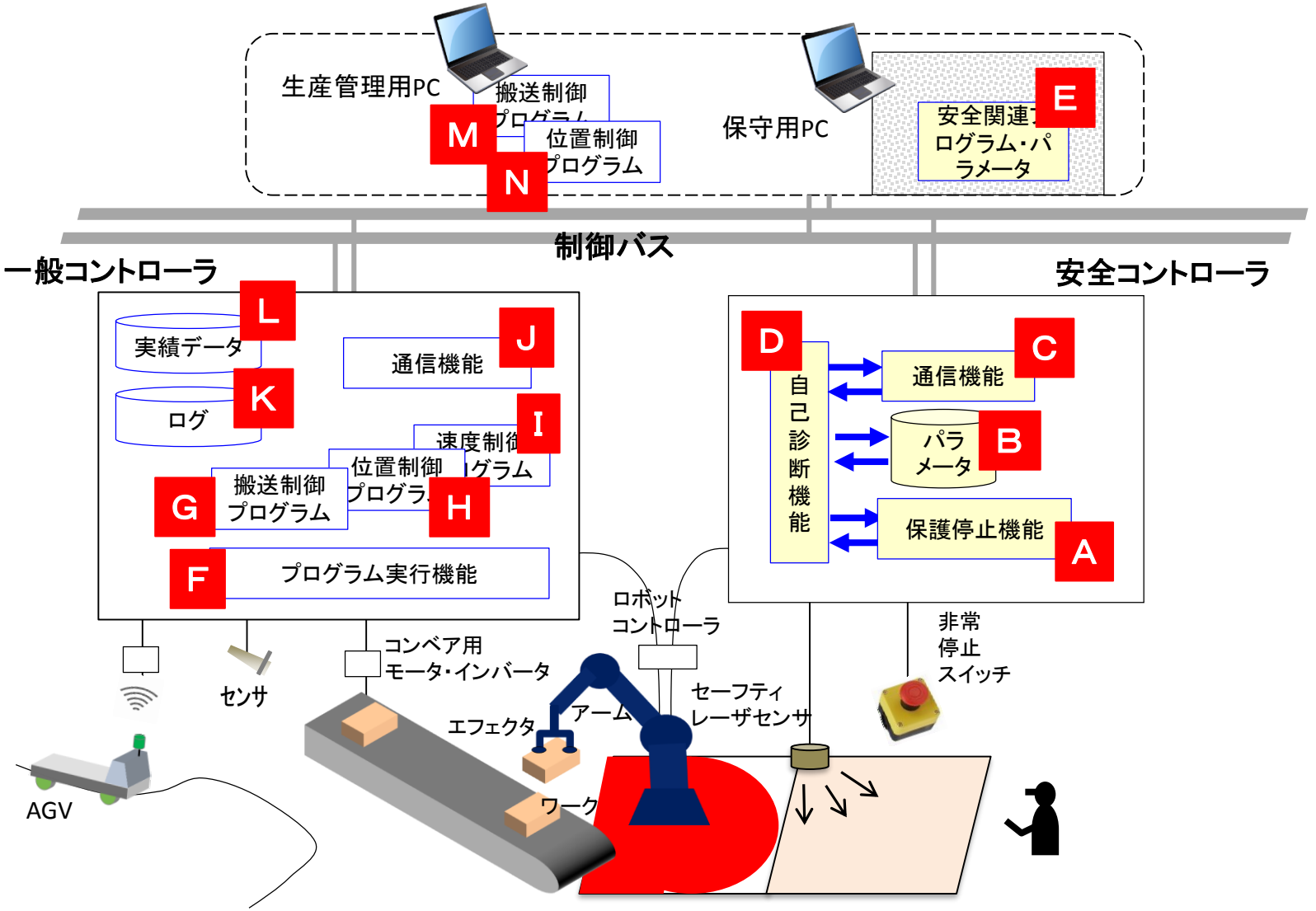
インテグレータによる保護資産の抽出

- 事業者から提示されている保護資産と詳細化したシステム構成に基づいてインテグレータの視点、知識に基づいて保護資産を抽出します。

- 検討システムの重要度や公開済の脆弱性情報などによって、攻撃者の攻撃動機も異なってきます。保護資産抽出の際に、もし攻撃の動機を含めて検討することが可能であれば、その点もあわせて考慮します。

インテグレータによる保護資産の抽出

以下抽出された保護資産を示します。保護資産にA～Nのラベル付けされています。



インテグレータによる保護資産の抽出

■下表は抽出された資産を安全性との関係を含めたリストです。

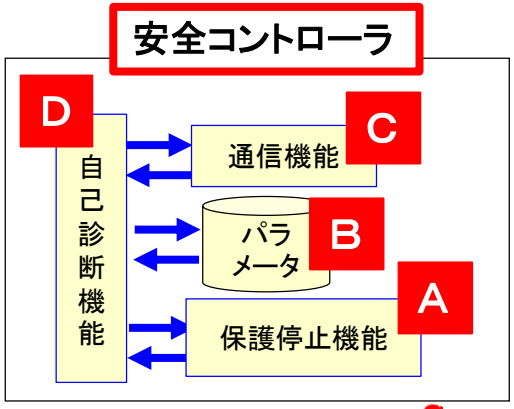
資産			安全関連*1
情報資産	E	安全関連プログラム・パラメータ	◎
	–	センサーデータ(ワーク位置等)	
	L	実績データ(製造数量、トレンド等)	
	K	ログデータ(リモートアクセス、稼働、停止、教示、警報、故障、非常停止、操作等)	
	F	プログラム実行機能	
	J	通信機能	
	I	速度制御プログラム	
	N・H	位置制御プログラム	
	M・G	搬送制御プログラム	
	–	ユーザ認証機能(ID/PW)	
	–	権限管理機能	
	A	保護停止機能	◎
	B	安全コントローラパラメータ	◎
	C	安全コントローラ通信機能	◎
	D	安全コントローラ自己診断機能	◎
		ロボットコントローラ	

資産		安全関連*1
機能資産	生産計画通りに製造が継続できる	
	所定の品質を維持できる	
	:	
物理資産	安全コントローラ	◎
	教示装置	◎
	産業用ロボット	◎
	セーフティレーザセンサ	◎
	非常停止スイッチ	◎
	イネーブルスイッチ	◎
	通信機器(ルータ等)	
	通信機器(無線アクセスポイント等)	
	一般コントローラ	
	生産管理用PC	
	保守用PC	◎
	マテハン用センサ	
人的資産	作業者、保守員の命、身体	
	ロボット教示方法	
	保守・メンテナンス方法	

＊1)安全関連:◎有(例:安全機能の実装)

インテグレータによる保護資産の抽出

- 前掲一覧から、標的となりえる重要な保護資産を分析シートに記入します。
  ここでは安全コントローラ部分を示しています。



No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure	
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容
1	情報	安全コントローラ	A:保護停止機能								
2			B:パラメータ								
3			C:通信機能								
4			D:自己診断機能								

脅威の識別

- 攻撃手段を遂行するために行われる脅威を抽出します。Step1-2で事業者が行ったように、HSE＋AICの観点で抽出し、分析シートへ記入します。
  （本書ではS（安全性）に関わる部分以外は記述省略しています）

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure	
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容
1	情報	安全コントローラ	A:保護停止機能								
2			B:パラメータ								
3			C:通信機能								
4			D:自己診断機能								

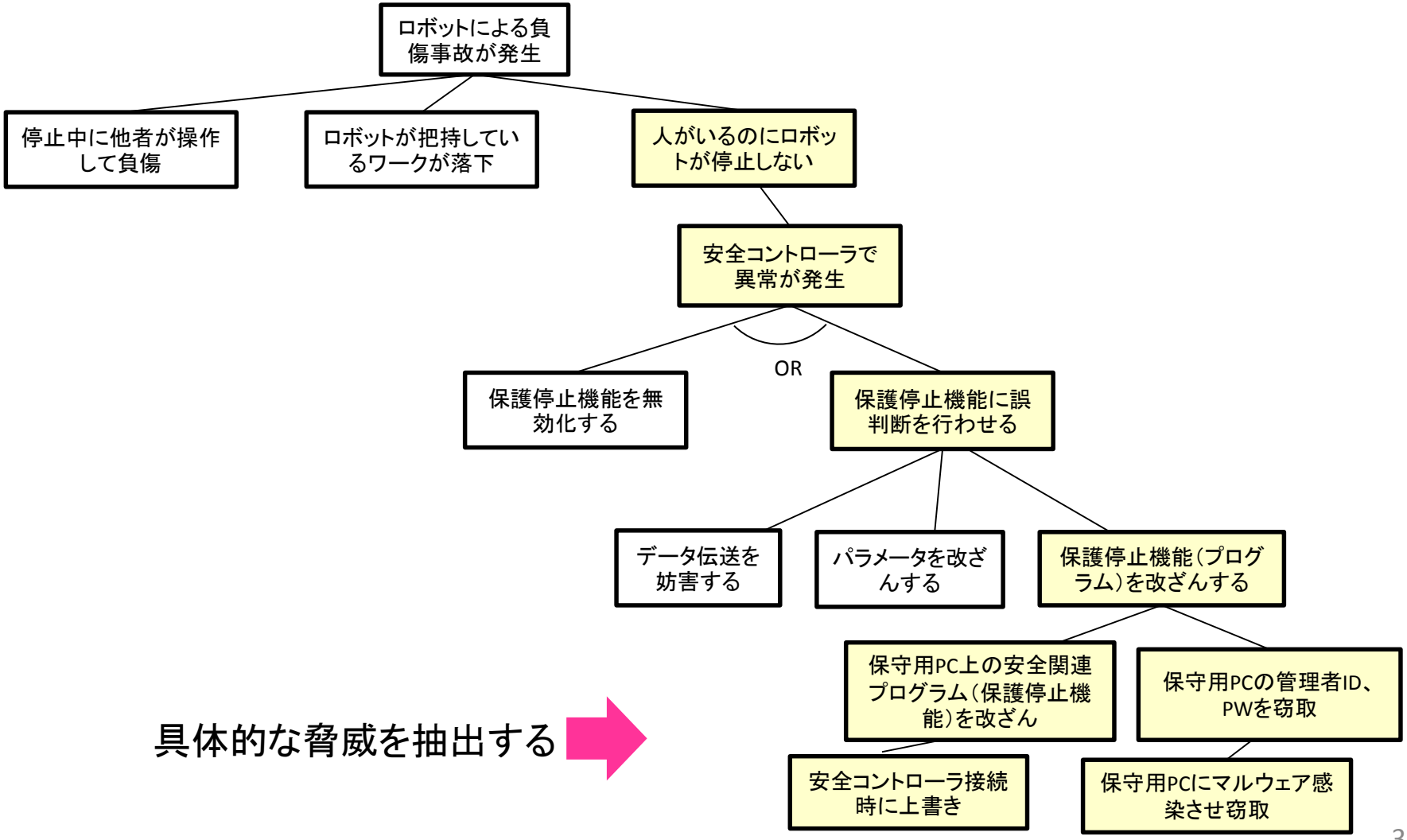
脅威の識別 （脅威の観点例）

■セキュリティ脅威を導き出す際の観点例を以下に示します。

通信妨害	
輻輳	DoS攻撃
遮断	物理的に切断（ケーブル切断）
電波妨害	遮蔽物設置、同一周波数帯使用し通信妨害
不正アクセス	
盗聴	情報が傍受・窃取され盗用、悪用される
情報窃取	ID/PW情報、データ、設定情報等窃取
機能・サービスの低下、停止	情報の書換、削除等により機能が低下・停止
改ざん	
不正データ設定	不正なシステム設定値に変更される
不正コマンド・メッセージ発行	正しくないコマンド、メッセージを送信し不正動作をさせる
ログ消去・喪失	操作履歴を消去、改ざんし追跡不能状態にする
脆弱性利用	
脆弱性露見	脆弱性を悪用される
不正中継	悪意のあるアクセスの踏み台として利用される
物理的脅威	
盗難・紛失	機器、装置が盗み出される
破壊	機器、装置が破壊され動作不能になる
保守・廃棄時の窃取	保守作業、廃棄時に機器から不正に情報を取出す
誤操作	
誤操作、・設定	操作者の誤った操作、設定による脅威の発現
ウィルス感染	
ウィルス感染	ウィルス感染した機器、記憶媒体により感染する脅威

脅威の識別

- 想定された攻撃のパターンを具体化する攻撃手段を想定しながら、前掲の脅威の観点例等を参考にして、脅威を抽出します。



脅威の識別

- 攻撃手段を遂行するために行われる脅威を抽出します。Step1-2で事業者が行ったように、HSE＋AICの観点で抽出し、分析シートへ記入します。
  （本書ではS（安全性）に関わる部分以外は記述省略しています）

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure	
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容
1	情報	安全コントローラ	A:保護停止機能	保護停止機能プログラムを不正に書き換える							
2			B:パラメータ	パラメータが改ざんされる							
3			C:通信機能	盗聴							
4			D:自己診断機能	機能停止							

「脅威の観点」を参照

脆弱性の識別

- 脆弱性には「人に潜在するもの」「ソフトウェアを含む機器に潜在するもの」「経路（インタフェース）に潜在するもの」があり、業務等を含む運用に関する内容も含まれます。

- 通常運転中か、メンテナンス作業中であるか等によっても脆弱性が異なる場合もあると考えられますので、識別においては運転の状況も考慮します。

- 事業者のセキュリティ要求を念頭に、重要資産に脅威となりうる脆弱性を網羅的に識別します。この際、影響度、発生可能性の高低を意識して識別を行うと、重要度に鑑みた優先付けができます。

- 検討システムを構成する購入品についても、既知のものについては機器メーカからの提供情報により把握します。

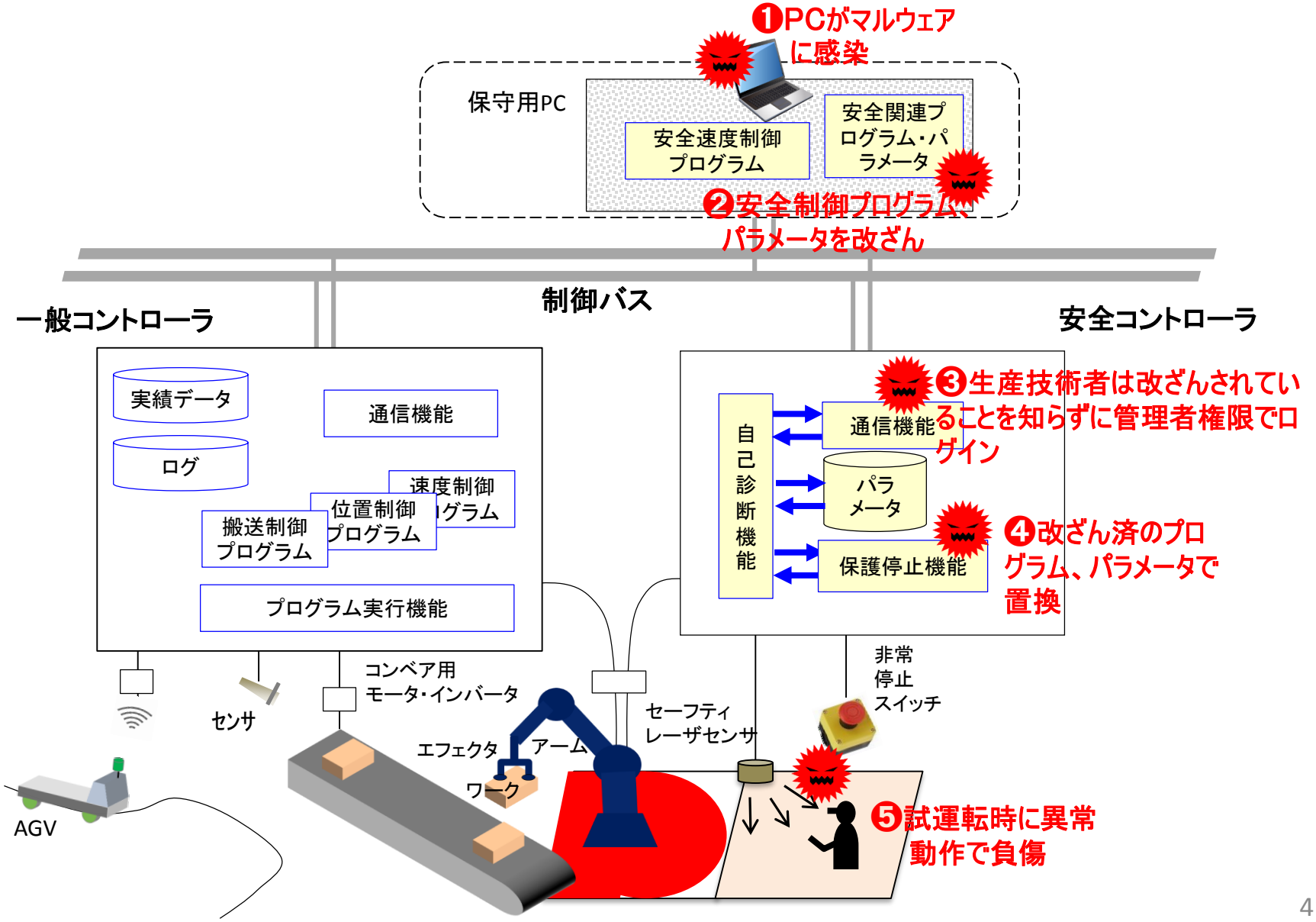
- 脆弱性の識別は、その脆弱性をついた脅威による被害とその発生頻度が客観的に評価できるレベルで行います。

脆弱性の識別

- 事業者のセキュリティ要求に逸脱すると考えられる事項を、弱点（脆弱性）とみなして抽出し、分析シートに記入します。

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure	
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容
1	情報	安全コントローラ	A：保護停止機能	保護停止機能プログラムを不正に書き換える	ウィルス対策管理がずさんな保守用PC						
					無線（旧Wi-Fi機器）						
					：						
2			B：パラメータ	パラメータが改ざんされる	ウィルス対策管理がずさんな保守用PC						
					無線（旧Wi-Fi機器）						
					：						
3			C：通信機能	盗聴	施錠していないHUB						
4			D：自己診断機能	機能停止	ウィルス対策管理がずさんな保守用PC						
			：								

被害内容の確認


❶PCがマルウェアに感染
保守用PC
安全速度制御プログラム
安全関連プログラム・パラメータ
❷安全制御プログラムのパラメータを改ざん
制御バス
一般コントローラ
安全コントローラ
実績データ
ログ
通信機能
速度制御プログラム
位置制御プログラム
搬送制御プログラム
プログラム実行機能
自己診断機能
通信機能
パラメータ
保護停止機能
❸生産技術者は改ざんされていることを知らずに管理者権限でログイン
❹改ざん済のプログラム、パラメータで置換
コンベア用モータ・インバータ
センサ
非常停止スイッチ
セーフティレーザセンサ
エフェクタ
アーム
ワーク
AGV
❺試運転時に異常動作で負傷

被害内容の確認

ここでは、安全コントローラ内の保護停止機能が、攻撃を受けた場合のシナリオを一例として示しています。

❶悪意を持った第三者が、保守用PCにウィルスを感染させます。
保守用PCはウィルス対策の一環で定期的にパッチを適用していますが、この時はその間隔が空いてしまい、最新状態となっていませんでした。
しかし、生産技術者はあまり気にせずに使用することにしました。

❷悪意ある第三者は安全コントローラの制御プログラム、パラメータメンテナンスの機会を狙い、事前に保護停止機能モジュールとパラメータを改ざんします。

❸生産技術者は管理者権限でログインします。

❹悪意ある第三者によって改ざんされている保護停止機能モジュールとパラメータで、安全コントローラの情報を更新します。

❺試運転時に保護停止機能が正しく動作せず、ロボットが停止せずそばにいた作業者が負傷します。

被害内容の確認

■ロボットが停止しない結果、作業者が負傷が発生します。

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure	
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容
1	情報	安全コントローラ	A:保護停止機能	保護停止機能プログラムを不正に書き換える	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷					
					無線(旧Wi-Fi機器)						
					:						
2			B:パラメータ	パラメータが改ざんされる	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷					
					無線(旧Wi-Fi機器)						
					:						
3			C:通信機能	盗聴	施錠していないHUB	制御情報の暴露					
4			D:自己診断機能	機能停止	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷					
			:								

評価指標

- 被害内容の影響度ならびに発生可能性を3段階で評価します。（次頁参照）
  - 影響度：被害の大きさ
  - 発生可能性：その事象の起こしやすさ
  - リスクレベル：影響度と発生可能性からリスクレベルを決定

- リスクレベルが「高」「中」に対して、セキュリティ対策が必要であるとします。

- ここでは、リスクが高いと識別された脅威が、以下に示すようにセーフティに影響を与えるかという観点も含めます。

【例】
- そのセキュリティリスクの発生可能性が高く、かつ単独でも発生するとセーフティ機能が著しく低下もしくは停止する
- そのセキュリティリスクが他要因と組み合わされて発生するとセーフティ機能が著しく低下もしくは停止する

リスクレベルの求め方

リスクレベル	発生可能性		
	高	中	低
影響度 高	高	高	中
影響度 中	高	中	低
影響度 低	中	低	低

発生可能性	説明
高	今後1年以内に発生する可能性が高い脅威、脆弱性
中	今後10年以内に発生する可能性が高い脅威、脆弱性
低	これまで発生したことがなく発生する可能性がほとんどないと考えられ脅威、脆弱性

影響度	事業継続性計画作成		情報セキュリティ			産業活動の安全性		環境的安全性	全国的な影響
	1サイトでの製造停止	複数サイトでの製造停止	コスト（百万$)	法的	公衆の信頼	サイト内の人	サイト外の人	環境	基盤・サービス
高	>7日	>1日	>500	重い刑事犯罪	ブランドイメージ喪失	死亡	死亡or重大な地域ｲﾝｼﾃﾞﾝﾄ	国家・地域機関から召喚	複数事業分野への影響or地域ｻｰﾋﾞｽ大規模中断
中	>2日	>1時間	>5	軽い刑事犯罪	顧客信頼喪失	休職or重傷	苦情or地域社会へ影響	地域機関から召喚	1社の規模を超える事業分野へ影響可能性
低	<1日	<1時間	<5	なし	なし	応急手当	苦情なし	小規模かつ限定的	同上

人の安全性

※安全性に関わる事業リスクとして、本書では「工程作業者の負傷・死亡」に注目して分析を進めます

リスクレベルの決定

- セキュリティ脅威の発生可能性と発生時の影響度の基準に基づき評価し、セキュリティリスクレベルを決定します。

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure	
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容
1	情報	安全コントローラ	A:保護停止機能	不正に書き換える	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷	高	高	高		
					無線(旧Wi-Fi機器)		高	高	高		
					:						
2			B:パラメータ	パラメータが改ざんされる	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷	高	高	高		
					無線(旧Wi-Fi機器)		高	高	高		
					:						
3			C:通信機能	盗聴	施錠していないHUB	制御情報の暴露	高	中	高		
4			D:自己診断機能	機能停止	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷	高	高	高		
			:								

Step 3　セキュリティ対策の立案と残存リスク評価

Step2　インテグレータのセキュリティ検討

Step3 セキュリティ対策の立案と残存リスク評価

入力		アクティビティ	成果物
・検討システム 仕様・構成図・設計書 ・状態遷移、データフロー他	保護資産一覧 システム、機器の脆弱性情報	3-1セキュリティ対策の立案 ・対策の立案と残存リスク評価	セキュリティ対策 ・分析結果（脅威分析表） ・セキュリティ要求仕様 ・セキュリティリスクレベル
・安全基本方針・計画 ・安全要求、他	・分析結果（脅威分析表） ・セキュリティ要求仕様 ・セキュリティレベル	3-2セーフティへの影響確認 ・確認事項 ・影響有無の確認	セーフティへの影響確認結果
・安全要求仕様（SRS） ・分析結果（FMEDA）、他			

Step4　全妥当性確認

＜入力・成果物の区分＞

一般要求事項　セーフティ　セキュリティ

対策の立案と残存リスク評価

- 特定されたセキュリティ脅威への対策を運用環境条件を含め立案します。
- リスク対策にはセキュリティ機能の追加、マネジメントによるもの、脆弱性の排除などがあります。一般的なセキュリティ対策を次頁に示します。
- 立案された対策によって新たなセキュリティリスクが生じないかを再確認し、全体的に許容レベルまで低減できることを確認し、対策後のリスク評価を記入します。

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure				対策後のリスク評価			セーフティへの影響
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容	脅威・脆弱性の再確認・結果		影響度	可能性	リスクレベル	
1	情報	安全コントローラ	A:保護停止機能	不正に書き換える	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷	高	高	高	防御（初期）	パッチ適用をダブルチェック	脆弱性情報公開によるゼロデイ攻撃	無	高	低	無	
										防御（初期）	接続認証						
					無線（旧Wi-Fi機器）		高	高	高	防御（初期）	メッセージ認証						

対策後のリスク評価を追加

対策の立案と残存リスク評価 （分類例）

■セキュリティ対策の分類は以下の内容に基づきます。

用途・目的		説明	対策例
防御	初期侵入段階	攻撃の最上流（初期段階）における、外部との接続点を介したネットワーク経由の攻撃、あるいはシステム（サーバ・操作端末・機器等）設置場所への攻撃者の物理的侵入を防止する目的で実装される対策。 また、攻撃者（内部犯行者を含む）による、システム（サーバ・操作端末・機器等）への不正ログイン等を防止する目的で実装される対策。	ファイアウォール（FW）、IPS、 アンチウイルス、 パッチ適用、脆弱性回避、 通信相手の認証、操作者認証、 入退管理
	内部侵攻・ 拡散段階	システム（サーバ・操作端末・機器等）への侵入を果たした攻撃者（人間あるいは不正プログラム）による、内部の情報収集や侵入範囲拡大（侵入したシステム内部での拡大及び他のシステムへの拡散）を防止する目的で実装される対策。	セグメント分割／ゾーニング、 APT対策ツール、 アクセス制御、 ホワイトリストによるプロセスの起動制限
	目的遂行段階	「情報窃取」「データ改ざん」「制御乗っ取り」「システム破壊」等、攻撃者による最終目的の実現を防止する目的で実装される対策	重要操作の承認、 データ暗号化、データ署名、 フェールセーフ設計
検知		攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策。	IDS、アンチウイルス、APT対策ツール、 統合ログ管理システム、 機器異常検知、機器死活監視、 入退管理、侵入センサ
被害把握		攻撃の成功による被害や影響範囲の把握を目的に実装される対策。あるいは、監査における証跡提示のため、攻撃内容の詳細の把握等を目的に実装される対策	ログ収集・分析、 統合ログ管理システム
事業継続		攻撃の成功による被害を最小限に留めるために実装される対策。あるいは、サービスの継続、被害の早期復旧を実現することを目的に実装される対策	データバックアップ、冗長化、 暗号鍵更新、 フェールセーフ設計

出典：IPA/ISEC　制御システムのセキュリティリスク分析ガイドから

確認事項

- セキュリティ対策が安全関連システムの機能、性能に影響を与えておらず、安全機能がセキュリティ対策によって効果的に保護されているかを評価します。

- セキュリティ対策の実装がシステムハザードを発生させないことを確認します。

  例：情報システムではウィルス感染時、通信路遮断が基本対応になりますが、セーフティシステムでは所定の手続きに基づかない通信途絶は非安全状態と判断され、意図しないプラント停止を引き起こす可能性もあります。

- セキュリティ対策の実装が安全機能を低下、あるいは無効化させないことを確認します。

  例：構成によっては、通信データの暗号・復号処理オーバヘッドが安全機能の応答性に影響を与える可能性もあります。

- 安全機能がセキュリティ対策をバイパスしていないか確認します。

影響有無の確認

■考案されたセキュリティ対策の全てに対して、セーフティ機能に影響していないかを確認し、影響がありそうなものをリストアップします。

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure				対策後のリスク評価			セーフティへの影響
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容	脅威・脆弱性の再確認・結果		影響度	可能性	リスクレベル	
1	情報	安全コントローラ	A:保護停止機能	不正に書き換える	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷	高	高	高	防御（初期）	パッチ適用をダブルチェック	脆弱性情報公開によるゼロデイ攻撃	無	高	低	無	ー（非該当）
										防御（初期）	接続認証						
					無線（旧Wi-Fi機器）		高	高	高	防御（初期）	メッセージ認証						

この時点で該当しないものは除外

セキュリティ対策のうちセーフティ機能に影響しそうなものをリストアップ

＜セーフティ影響度確認リスト＊＞

対策	安全要求:				対策後のSIL
	安全機能		影響	判定	
接続認証	保護停止	機能動作			
		性能(＜50ms)			

＊本ガイドでは「確認リスト」としていますが、セーフティ対応時に構築済のトレーサビリティシステムの変更管理機能等を活用すると、効率的に行うことができます。

影響有無の確認

- リスト化された各項目について、機器メーカ等含め詳細にセーフティ影響分析を行いその結果をフィードバックします。
- 検討の結果セーフティに影響がある場合、Step3-1に戻りセキュリティ対策を見直して検討を繰り返します。

対策	安全要求：				対策後のSIL
	安全機能		影響	判定	
接続認証	保護停止	機能動作	正常／異常	○	SIL1
		性能（50ms）	45ms	○	SIL1

検討の結果全て満たすと判定され、影響無

No	資産 Asset			脅威 Threat	脆弱性 Vulnerability	被害内容	リスク評価			対策 Security Measure			対策後のリスク評価			セーフティへの影響
	種類	名称	標的 Target				影響度	可能性	リスクレベル	分類	内容	脅威・脆弱性の再確認・結果	影響度	可能性	リスクレベル	
1	情報	安全コントローラ	A：保護停止機能	不正に書き換える	ウィルス対策管理がずさんな保守用PC	ロボット停止せず作業者負傷	高	高	高	防御（初期）	パッチ適用をダブルチェック	脆弱性情報公開によるゼロデイ攻撃 無	高	低	無	ー（非該当）
										防御（初期）	接続認証					無
					無線（旧Wi-Fi機器）		高	高	高	防御（初期）	メッセージ認証					無

Step 4　全妥当性確認

Step3 セキュリティ対策の立案と残存リスク評価

Step4　全妥当性確認

入力

- ・安全基本方針・計画
- ・安全要求、他
- ・安全要求仕様（SRS）
- ・分析結果（FMEDA）、他
- セーフティへの影響確認結果
- ・検討システム仕様・構成図・設計書
- ・状態遷移、データフロー他
- セキュリティ対策
- ・分析結果（脅威分析表）
- ・セキュリティ要求仕様
- ・セキュリティレベル

アクティビティ

- ・安全妥当性確認
- ・セキュリティ妥当性確認

成果物

- セーフティ妥当性確認結果
- セキュリティ妥当性確認結果

Step5　運用・保守・修理

＜入力・成果物の区分＞

一般要求事項　セーフティ　セキュリティ

安全妥当性確認／セキュリティ妥当性確認

- 事業者はセキュリティ対策が実装された製品・サブシステムを含む全システムが、事業者のセーフティ要求を満たしているか（SILへの適合性）を確認します。

- 成果物レビューならびにサブシステムを連結させた全体的ペネトレーションテストやロバスト性テスト等でセキュリティの妥当性（セキュリティレベルSLへの適合性）を確認します。

- サブシステムのセーフティ、セキュリティ機能で可能な項目は、本ステップに先立ちインテグレータ、機器メーカにて妥当性確認が行われたとしています。

事業者のセキュリティ要求項目		施策
工程作業者の死傷を生じさせないこと	安全性（S）	労働安全の徹底
故意や過失などによる生産システムの停止を防止し、許可された利用者が必要なときに必要な情報にアクセス可能であることを確実にすること	可用性（A）	ユーザIDとPW管理、 従業員カードによる入場管理
生産システムの情報・データが常に完全であることを保証すること。許可されていない利用者によってデータを改ざんまたは破壊されるのを防ぐこと	完全性（I）	現場で使用する機器管理、 ウィルスパッチ適用
生産に関わる情報には許可された利用者のみアクセス可能とすること	機密性（C）	ユーザIDとPW管理

Step 5　運用・保守・修理

Step4　全妥当性確認

Step5　運用・保守・修理

入力	アクティビティ	成果物
・安全基本方針・計画 ・安全要求、他	・セキュリティ対応計画の立案と実施 ・継続的メンテナンスの実施	・現時点での運用・保守計画・手順書
・セキュリティ方針・計画 ・セキュリティ検討範囲（Suc）		運用・保守 セーフティへの影響 確認結果
・2回目以降は、現時点での運用・保守計画・手順書		

＜入力・成果物の区分＞
一般要求事項　セーフティ　セキュリティ

セキュリティ対応計画の立案と実施

- 本ステップでセーフティに加え、セキュリティ対策の実装により新たに追加、変更される運用、保守に関わる内容を確認します。

- セキュリティインシデントが生じた際の対処、定期的な脆弱性情報の確認及び情報確認時の対応手順等を定めた対応計画を検討、立案します。

- 新たな脆弱性が発見された場合に必要な措置（パッチ適用手順等）を既存のセーフティシステムの運用・保守に組み入れ、あるいは関連付け、運用体系を更新します。

- セキュリティ対応に関わるドキュメントを、既存ドキュメント（保守計画書、操作手順書、メンテナンスマニュアル等）に追加、変更あるいは関係づけします。

- セキュリティ対応活動を日々の運用の中で継続し、対処内容・ドキュメントをメンテナンスします。

セキュリティ対応計画の立案と実施 （実施例）

■本例では以下の対策がなされたとします。

運用	内容
入退出管理	工場サーバ室、工程ライン入退出者のセキュリティ管理要件の追加
インシデントレスポンス体制構築	CSIRT体制（要員の訓練含）の追加
アプリケーション管理	ホワイトリストによるPLC、HMI装置上の制御アプリケーション管理
通信サービス	TCP/IP上の不要な通信サービス（Telnet他）の制限
通信トラフィック監視	工場内制御・情報LAN上のパケット収集＆挙動監視
機器・装置監視	機器ID導入し、接続時の認証機構を追加

保守・修理	内容（★＝インシデントレスポンス ドキュメント例）
機器稼働リモートメンテナンス	機器メーカ、保守会社の保守要件（★遠隔監視保守仕様書）
オンライン交換	機器メーカ、保守会社の保守要件（★オンライン保守要領書）
パッチ適用	セキュリティパッチ適用改訂 ダブルチェックルール追加 （★セキュリティパッチ適用手順書）

コンピテンシ	内容
生産管理・オペレータ	セキュリティ教育受講者であること、当該システムのセキュリティ知識があること、認定許可者であること　などの要件規程追加
製造セキュリティ専門員	セキュリティインシデントへの適切な判断・対処を行うことができる専門要員の規定と監査、体制見直し

継続的メンテナンスの実施 （セキュリティパッチ適用例）

- 下図はセキュリティパッチ運用手順を新たに定めた場合、既存のセーフティ保守計画書に関係づけを行っている例を示しています。

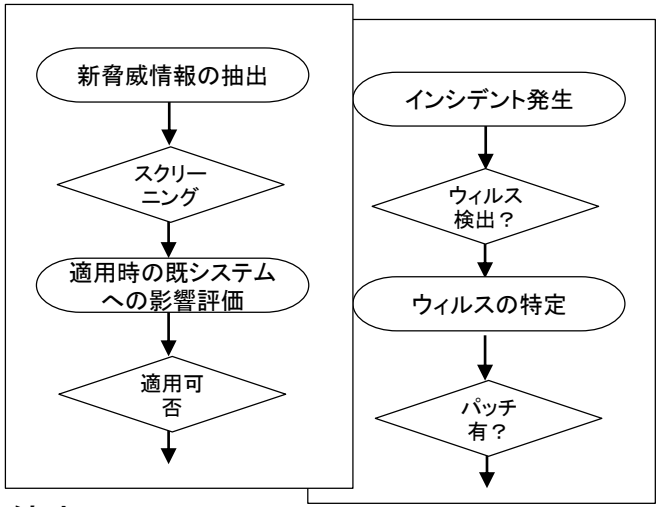
セーフティ保守計画書（既存）

1. 目的
2. 適用対象製品・システム
3. 機器故障時の交換、修理
4. 部品・コンポーネント改廃時対応手順
5. ソフトウェアプログラムのアップデートについて
6. 定期点検
7. 保守体制

関連付け
（図書番号参照）

セキュリティパッチ適用手順書（新規）

1. 目的
2. 適用対象製品・システム
4. 脆弱性の識別
   ・情報源
   ・検出方法
5. 適用検討手順



6. 体制

制御システム セーフティ・セキュリティ要件検討ガイド
– ケーススタディ編 –

2018年3月　第1版発行

独立行政法人情報処理推進機構(IPA) 技術本部 ソフトウェア高信頼化センター(SEC)
〒113-6591
東京都文京区本駒込2丁目28番8号　文京グリーンコートセンターオフィス16階
https://www.ipa.go.jp/sec/index.html