資料6

厚生労働省
機械の無人運転における安全確保等に関する専門家検討会（第1回）

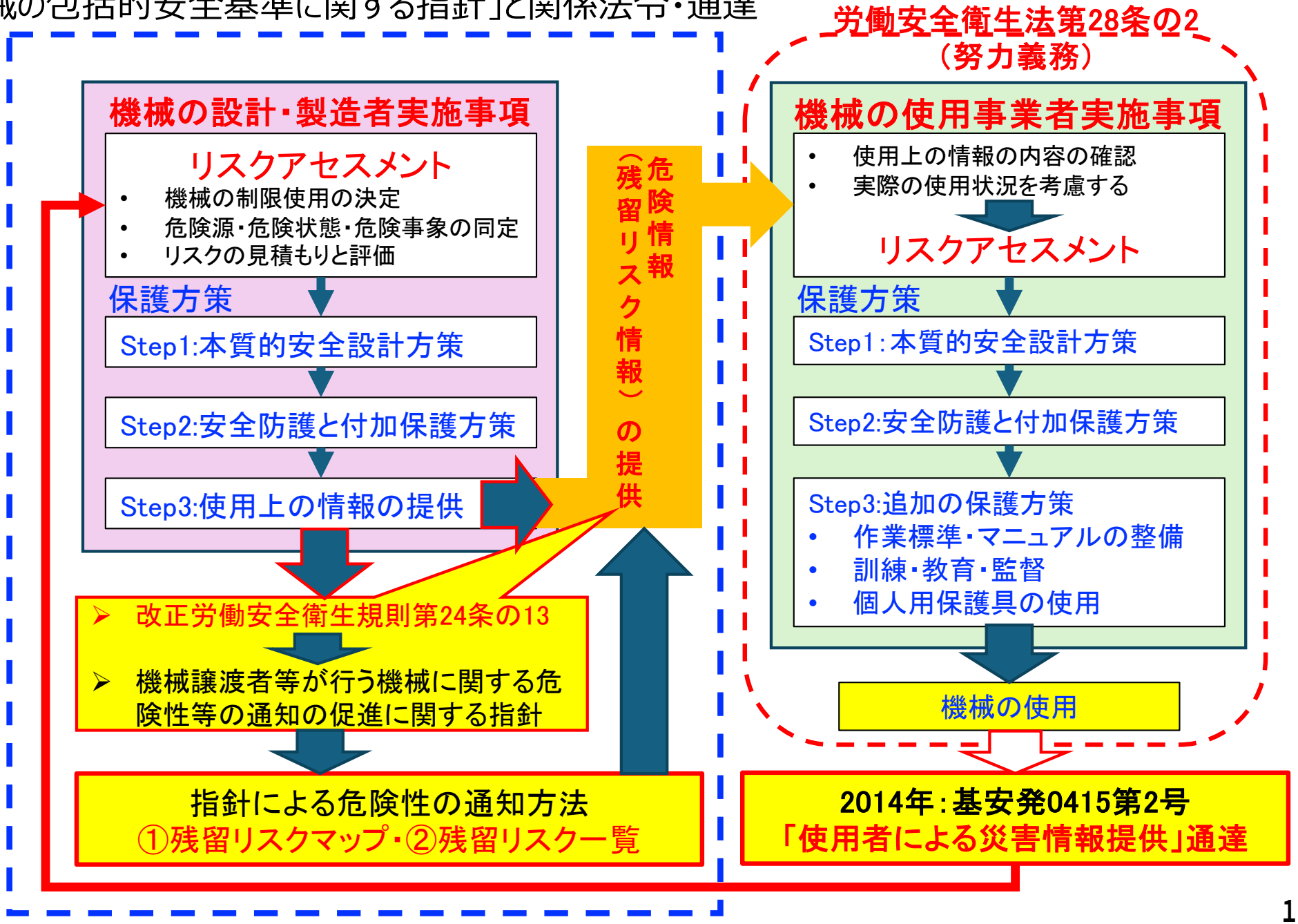
機械の安全確保における機能安全の役割とは

1. 機械設計における機械安全設計と機械使用者との関係
2. 機械設計者による機械安全設計と機能安全設計の概要
3. 機械の安全確保における機械・機能安全関連の技術規格
4. JIS規格における機能安全の適用事例
   （JIS D 6802：2022無人搬送車及び無人搬送車システム安全要求事項及び検証）
5. 機械設計における機能安全設計の考え方

2025年11月26日

1. 機械設備における機械安全設計と機械使用者との関係

「機械の包括的安全基準に関する指針」と関係法令・通達



厚生労働省　第１４次災害防止計画（2023年～2027年）

ウ 製造業対策

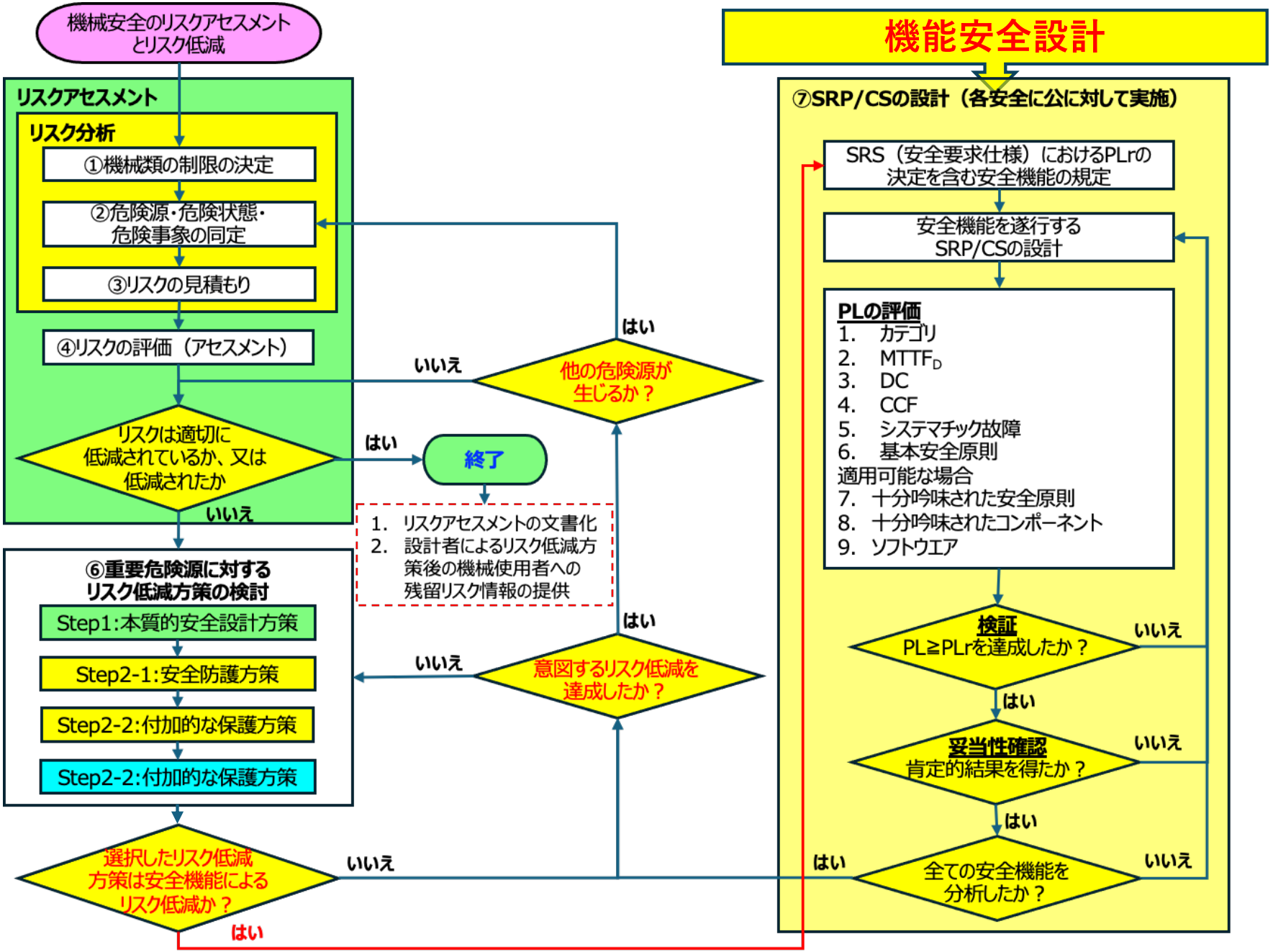
（ア）労働者の協力を得て、事業者が取り組むこと

- 「はさまれ・巻き込まれ」等による労働災害の危険性の高い機械等については、製 造者（メーカー）、使用者（ユーザー）それぞれにおいてリスクアセスメントを実 施し、労働災害の防止を図ることが重要であることから、**「機械の包括的な安全基 準に関する指針」**（平成 19 年 7 月 31 日付け基発第 0731001 号）**に基づき、使用者 においてもリスクアセスメントが適切に実施できるよう、製造者は、製造時のリス クアセスメントを実施しても残留するリスク情報を、機械等の使用者へ確実に提供** する。
- **機能安全の推進により機械等の安全水準を向上**させ、合理的な代替措置により安全対策を推進する。

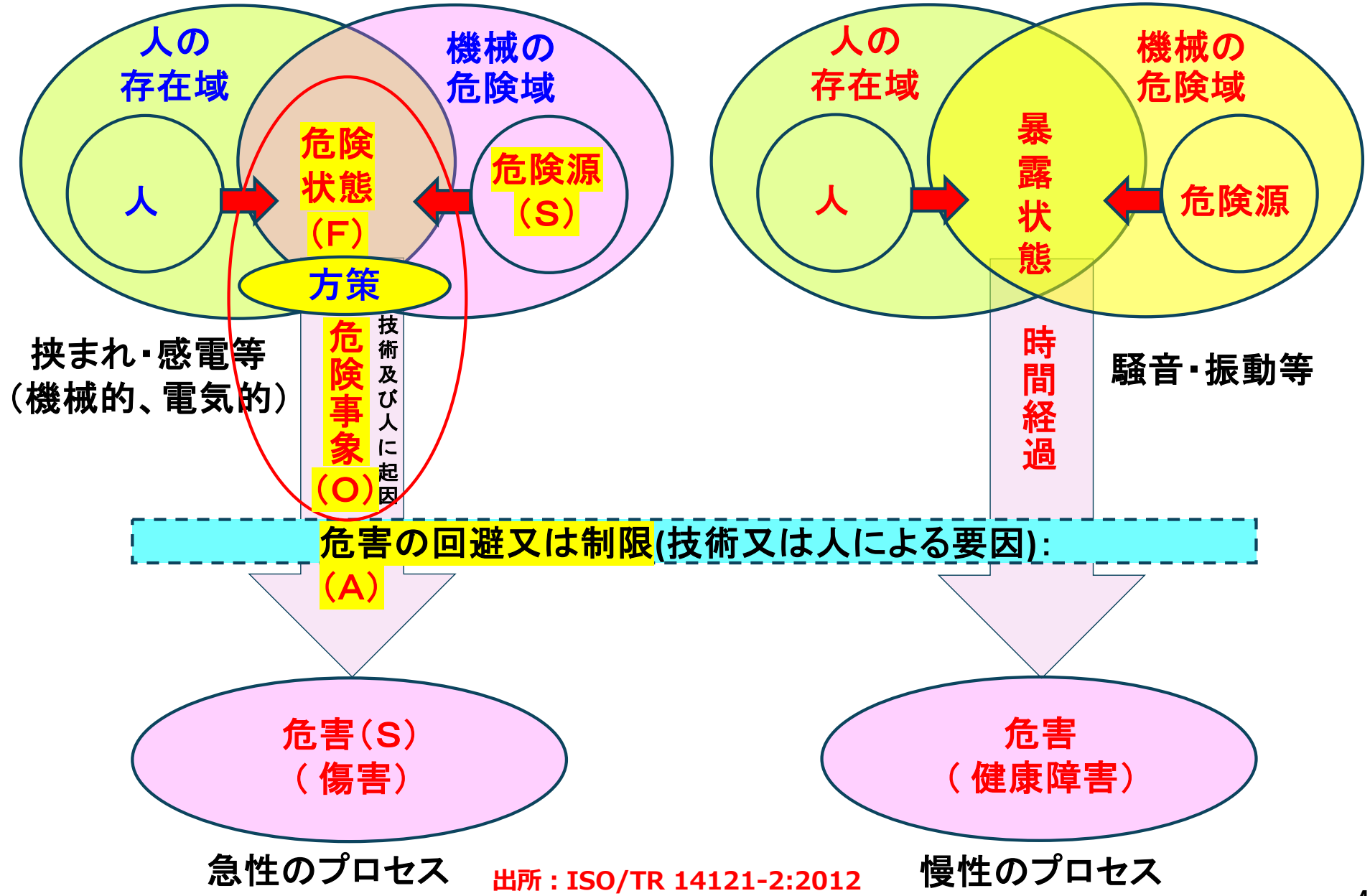
（イ）（ア）の達成に向けて国等が取り組むこと

- 製造業で使用される機械等について、技術の進展に対応するよう、**国際的な安全規格と整合を図る等、安全基準（ボイラー構造規格等）の見直し**を行う。
- 作業手順の理解や危険への感受性を高めるためのＶＲの活用について、より安全に 資するものとなるよう要件を検討する。
- **機能安全を有する機械を活用し**、危険な作業を信頼性の高い技術を有する機械等で 置き換えることを通じて、**現場の作業者が労働災害に被災するリスクを低減させる 取組を推進**する。

2. 機械安全設計と機能安全設計の概要



危険域_危険源_危険状態_危険事象_危害の考え方
危害の発生プロセス(危害の発生条件)



出所：ISO/TR 14121-2:2012

機械安全：リスクアセスメント実施の基本方針

用語	ISO 12100(JIS B9700)の定義 【設計のための一般原則- リスクアセスメント及びリスク低減 】
危険源 (hazard)	危害を引き起こす潜在的根源
危険状態 (hazardous situation)	人が少なくとも一つの危険源に暴露される状況。
危険事象 (hazardous event)	危害を起こし得る事象
危害(harm)	身体的傷害又は健康障害
リスク見積 評価 リスク(risk)	危害の発生確率と危害のひどさとの組合せ
許容不可の場合 保護方策 (protective measure)	リスク低減を達成することを意図した方策。 • **設計者による方策（3ステップメソッド）** **【1:本質的安全設計方策、2:安全防護及び付加保護方策、3:使用上の情報】** • **使用者による方策**【組織(安全作業手順，監督，作業許可システム)，追加安全防護物の準備及び使用,保護具の使用，訓練】
安全機能 (safety function)	故障がリスクの増加に直ちにつながるような機械の機能 **→一般的に制御システムによりリスク低減方策と考えて良い。**

リスクアセスメント

危険源から危害発生に至るシナリオ及び危害の内容がわかる様にまとめる。

危害発生のプロセスとリスク低減方策の考え方

危険源

人

危険状態

1：本質的安全設計方策
- 危険源除去:閉塞金型等・
- 危険状態排除：外部作業、自動化等

2：危険源への暴露の排除・低減
- 隔離による方策：固定ガード(ガード構造・安全距離）・施錠式インタロック付ガード（ガード＋制御システム）等
- 停止による方策：検知保護装置・開放停止型インタロックガード

保護方策の不足、不適切、不具合

危険事象の低減・危険回避検討

危険事象の発生

回避の失敗

危害

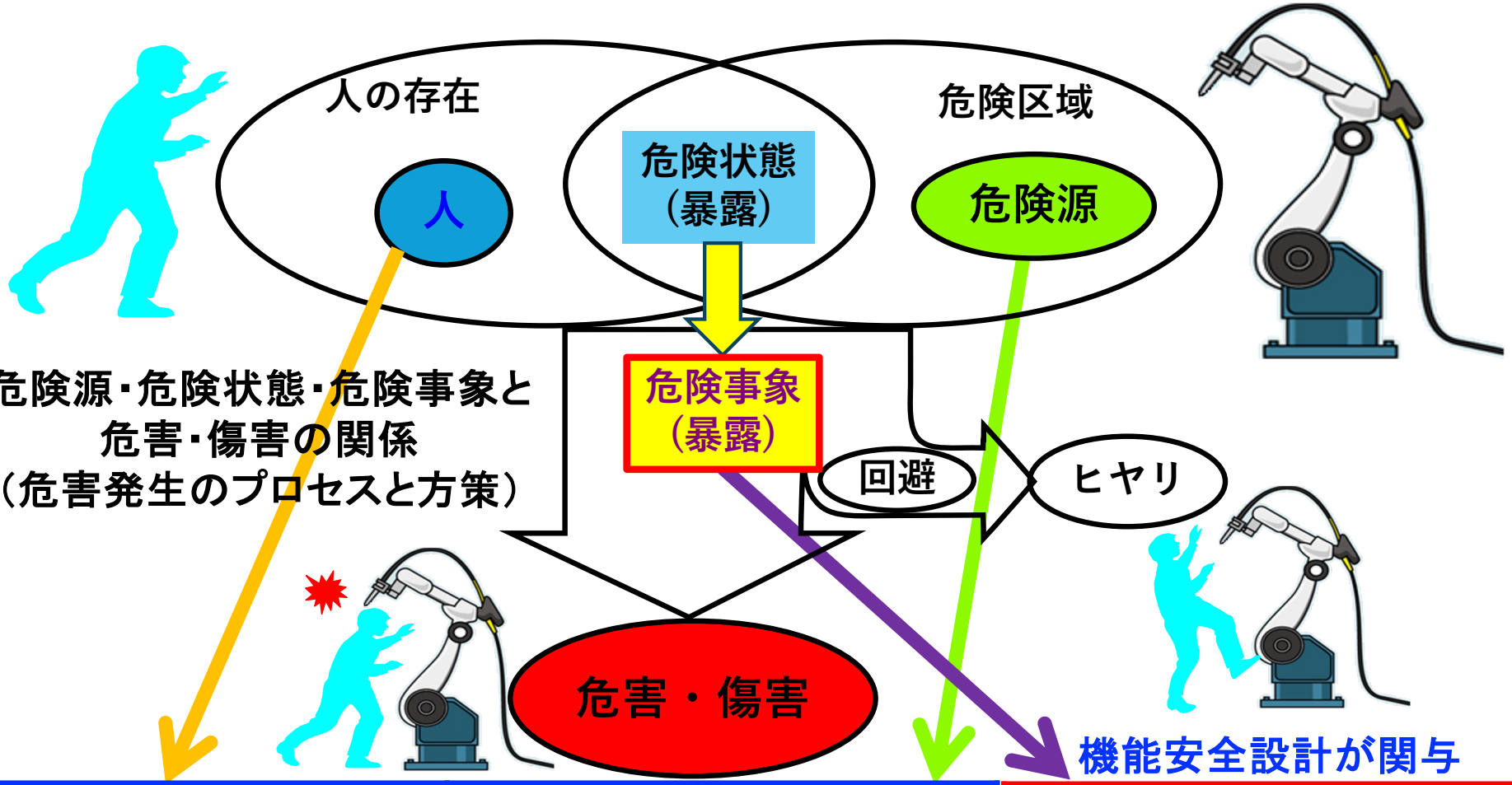
3：危険事象の低減
- **構造：安全防護の取り付け、構造の規格適合等**
- **確率：光線式安全装置・インタロック等の保護装置等、制御システム(PL/SIL・等による機能安全設計)の適用**

→【危険側故障発生確率（PFH)の低減】

4：事故回避(制限）の実施
- **段取・メンテナンス：**【モード・速度制限・イネーブルSW等による事故回避】・使用上の情報（警報・信号・銘板等）

リスク（R） は **危害の酷さ（S）** と **暴露の頻度・時間（F）**、**危険事象の発生確率（Q）**、**事故回避又は制限の可能性（P）** の組合せ（関数）

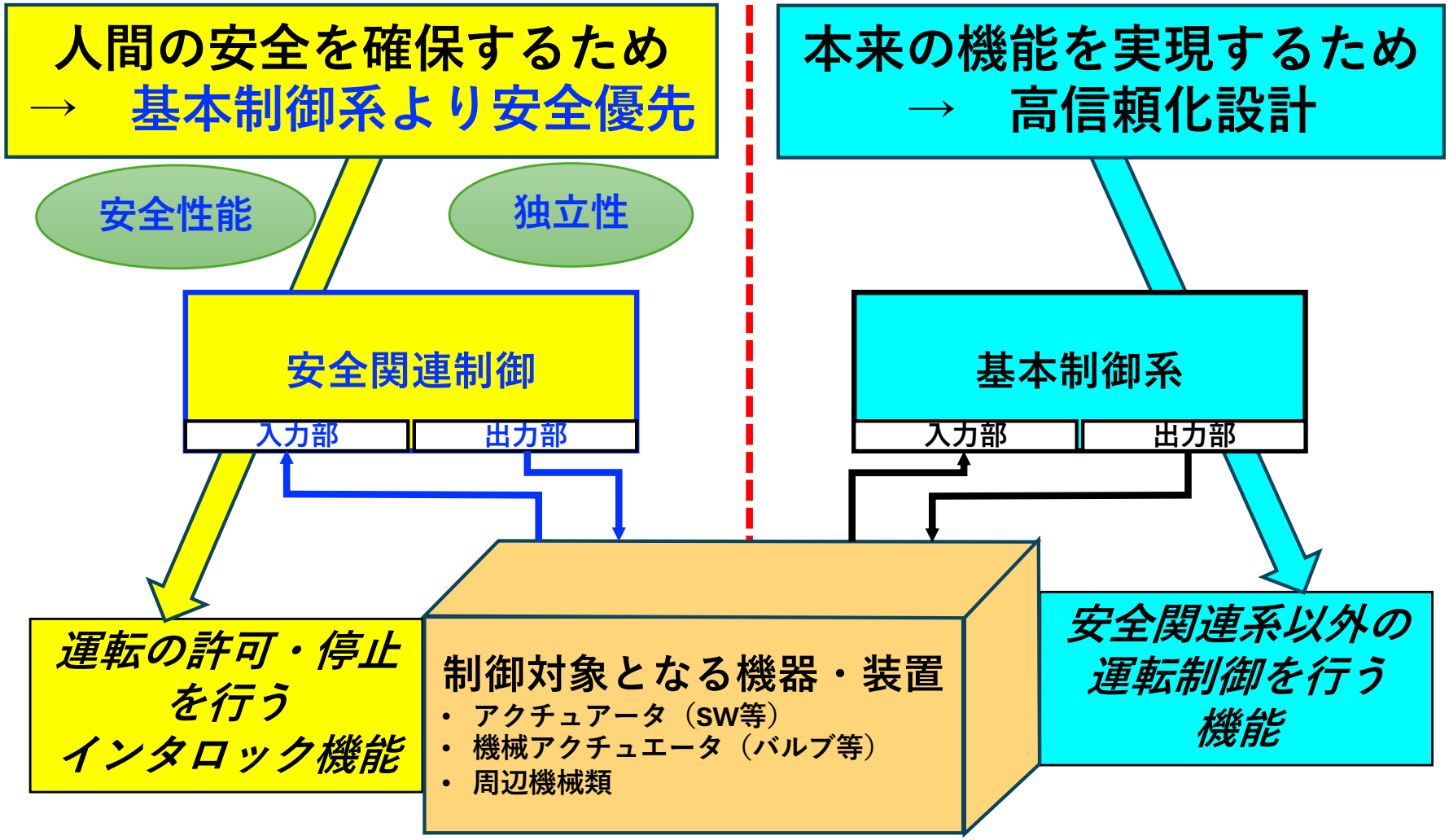
危害発生のプロセスとリスク低減・機能安全の役割



危険状態となる作業の排除	危険源の除去・低減	危険事象発生確率の低減
危険区域内の作業を廃止する、あるいは危険区域外からの作業とする	危険源の除去、または危害が及ばないエネルギーに低減する	人間工学考慮や信頼性向上により機械や人が“異常”とならないようにする／確率を下げる

制御システムの安全関連部の構成

平成２８年度厚生労働省委託　機能安全を活用した機械設備の安全対策の推進事業　機能安全テキスト　P27　より



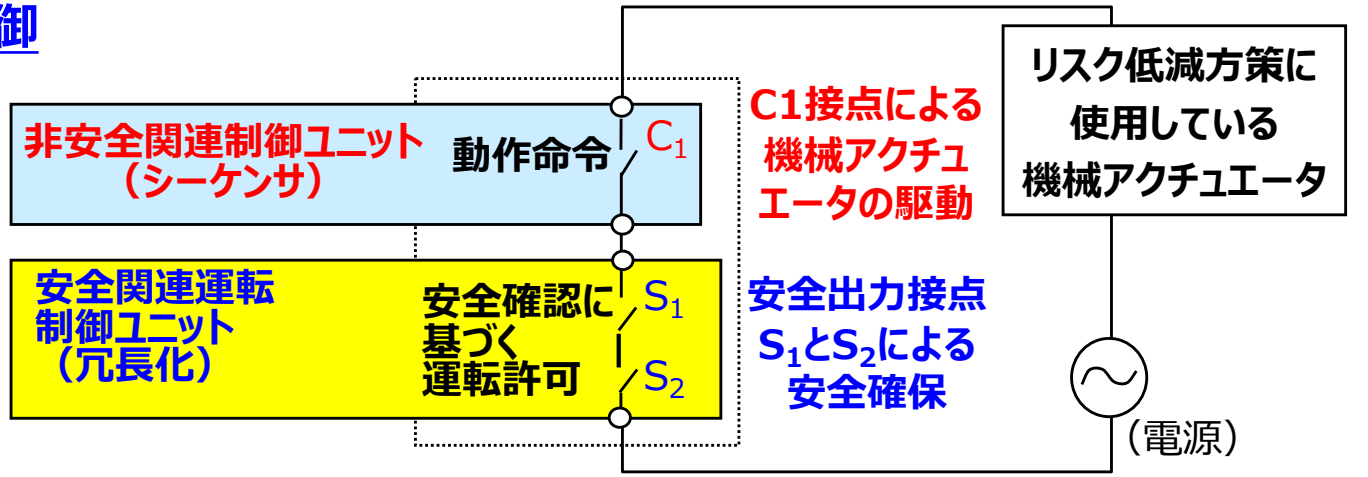
制御システムの安全関連部の制御構成例

制御システムの安全関連部の要求事項適合のための達成手段

1. 制御システムの安全関連部への適用が認められている機器の使用
2. 安全関連部の基本制御系からの分離/独立は、基本安全原則
3. 安全関連部への冗長化技術等の採用（リスクに合わせた制御カテゴリの採用）
4. ISO 13849-1に基づくリスクに合わせた信頼性設計（$MTTF_D$/DC/CCF等）

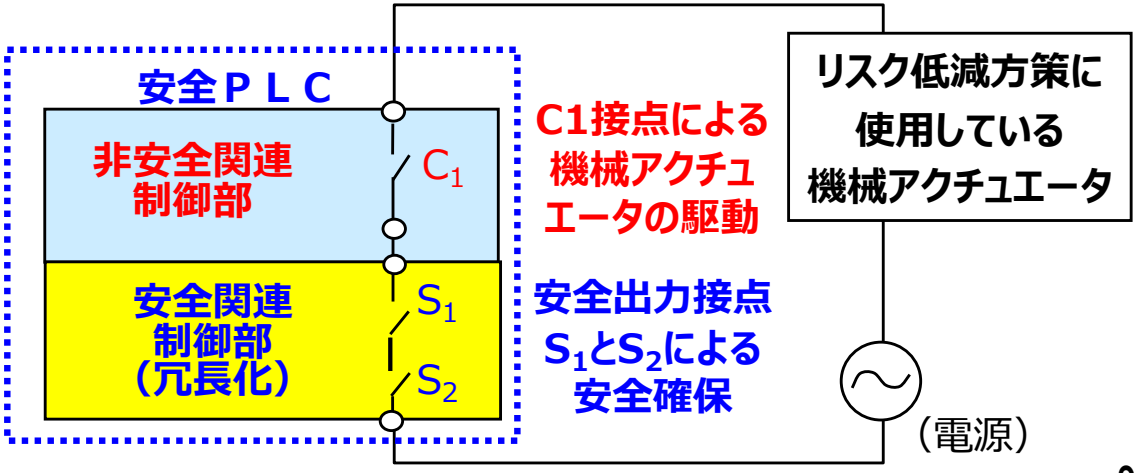
安全リレーユニットによる制御

安全関連部の分離独立が
第三者によって認証された
安全リレーユニットの使用

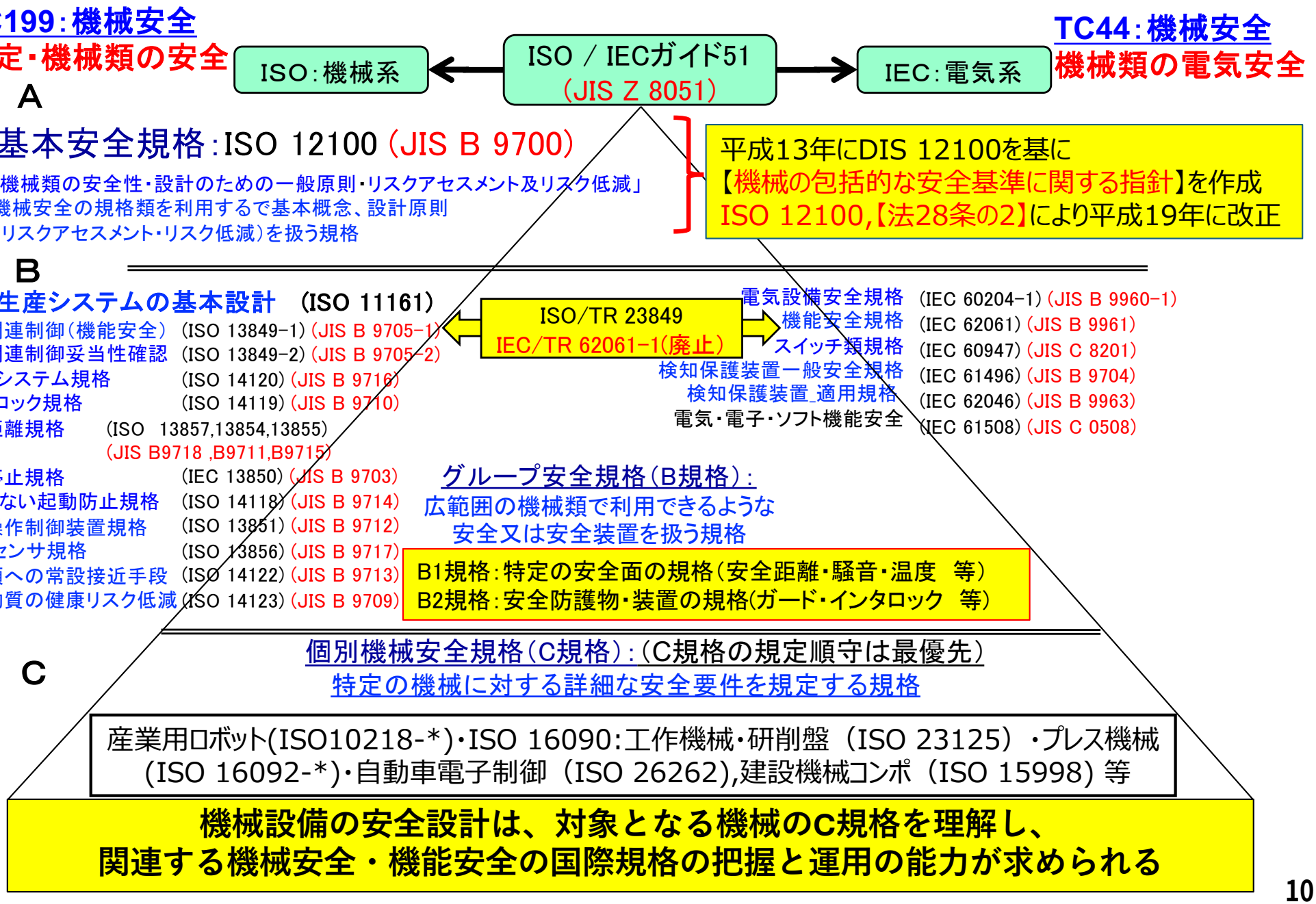


安全PLC制御・安全コントローラ

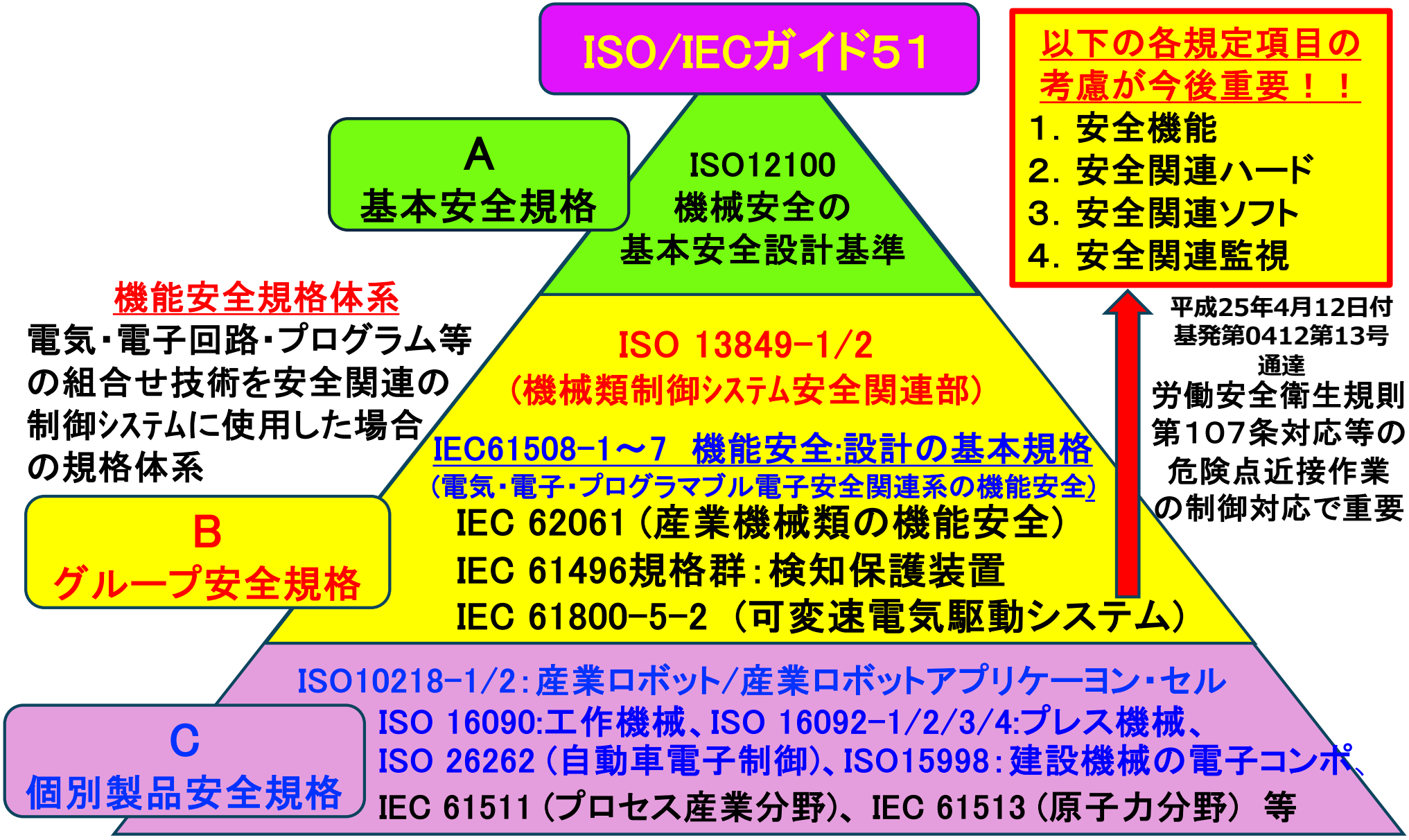
安全関連部の分離独立が
第三者によって認証された
機器（PLC・コントローラ等)の使用



3. 機械の安全確保における機械・機能安全関連の技術規格



機能安全に関連する国際規格体系



4．JIS規格における機能安全の適用事例
JIS D 6802：2022無人搬送車及び無人搬送車システム安全要求事項及び検証

無人搬送車及び無人搬送車システムの制御システムの安全関連部

- **労働災害防止のために必要措置として最低限，表2に記載するパフォーマンスレベル（以下，PL という。）への適合が、求められる。**　（ JIS B 9705-1:2019 の適用）
- **車両に対して実施する制御システムの安全関連部のPLを決定するためには、**質量と運動エネルギーとを考慮に入れた**リスクアセスメントの結果**を適用することが可能である。

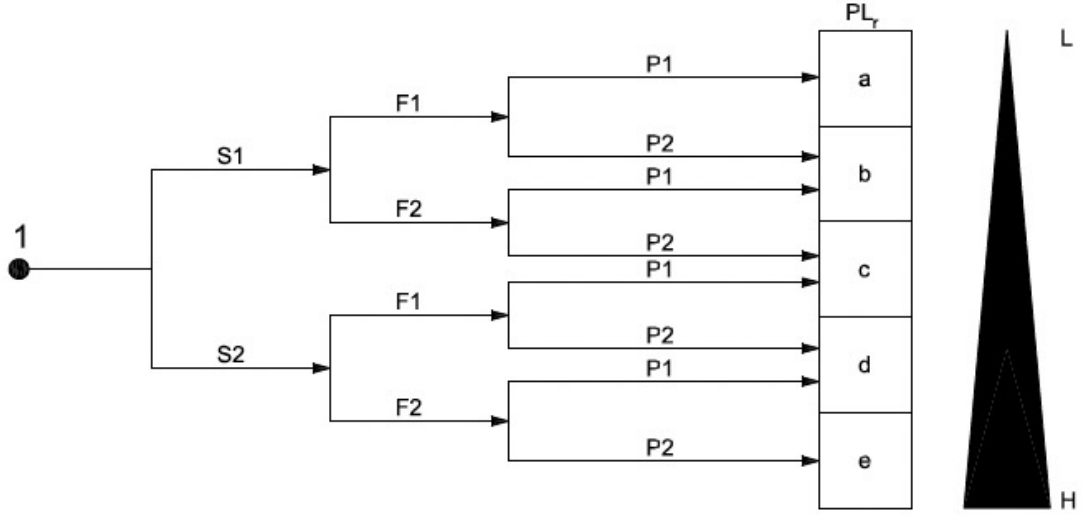
表２．JIS B 9505-1:2019による制御システムの安全関連部の最小PL　（抜粋）

この規格内の箇条	項目No.	この規格の相互参照	安全機能（又は安全機能部分）の説明	主なリスク	注記	最小要求PL
4.2 ブレーキシステム	1	**4.2**	ブレーキシステム制御	**人との衝突**	速機能を制御する。	d
4.3 速度制御	3	**4.3**	速度超過検出システ ム（速度＞車両定格速 度）	**人との衝突** 人検出が速度超過のた め効率的に行えない。	車両速度が最大定格速度を 超えないよう監視する。故障 時には，非常停止が作動しなければならない。	c
4.8.2人検出システム	16	**4.8.2.1**	走行方向での人の検出に伴う車両停止	**人との衝突**	経路内での人の検出後，車両を保護停止。	d
4.9 運転モード	23	**4.9.2.3**	乗車を意図した乗員が意図した位置に留 まっていることの検出	**人の転落又は切断**	乗員が意図した位置を離れ た場合，車両は，保護停止を開始しなければならない。	d
A.2.4.3 隔離区域内へのアクセス	29	**A.2.4.3 a)**	周囲防護	**人との衝突**	停止のための人検出手段	d

5. 機械設備における機能安全設計の考え方

■ 機械安全のリスクアセスメント結果で制御システムでのリスク低減を検討する場合の性能レベルの決定

JIS B 9705-1リスクに対する制御システムの安全関連部要求性能（PLr）の決定



S:傷害のひどさ
- S1:軽傷(通常、回復可能)
- S2:重傷(通常、回復不可能)及び死亡

F:危険源にさらされる頻度又は時間
- F1:低頻度(累積された暴露時間が作業時間の1/20を超えず、かつ頻度が15分に1回を超えない)
- F2:高頻度(F１以外)

P：危険源回避の可能性
- P1:回避可(危険状態が発生して、その状態が認知でき、かつ事故を回避する又はその効果を顕著に低減するための現実的機会が存在する場合)
- P2:回避不可(P１以外)

■ 機能安全設計は、システム構成「I入力-L論理-O出力」の各PFHの合計で妥当性評価を実施

ISO:PL(パフォーマンスレベル) JIS B 9705-1	PFH(1時間当たりの危険側故障確率:1/h) PLとSILの共通評価パラメータ	IEC:SIL(安全度水準) JIS C 0508･JIS B 9961
a	$10^{-4}>PFH\geq10^{-5}$	None
b	$10^{-5}>PFH\geq3x10^{-6}$	1
c	$3x10^{-6}>PFH\geq10^{-6}$	1
d	$10^{-6}>PFH\geq10^{-7}$	2
e	$10^{-7}>PFH\geq10^{-8}$	3
機械安全で適用しない	$10^{-8}>PFH\geq10^{-9}$	4

機能安全設計の設計評価パラメータ

機能安全設計の設計評価

①SRP/CSのカテゴリ：構造的配置
2006年以前の評価基準

＋

2006年以降に追加された設計評価の基準

障害検出及び／又はこれらの 信頼性による達成内容で評価

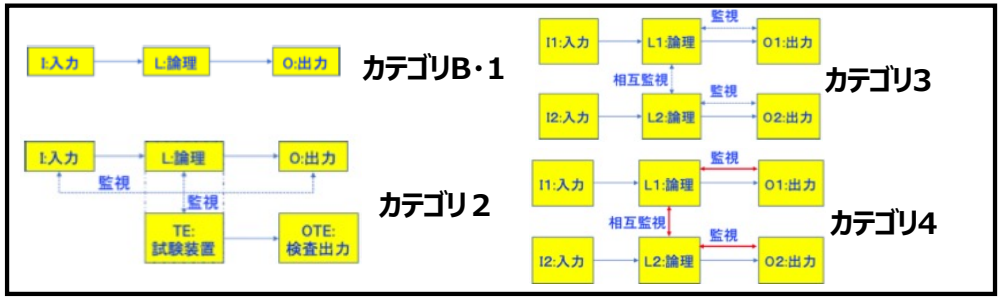
評価を明確化

信頼性による安全性能評価

②SRP/CSの$MTTF_D$
SRP/CSの平均危険側故障時間（年）

③SRP/CSのDC_{AVG}
SRP/CSの平均診断カバー率（%）

④SRP/CSのCCF
SRP/CSの共通原因故障評価（点）



各チャネル（入力･論理･出力）の$MTTF_D$の分類	
分類	**範囲**
受入れ不可	**0 年 ≤ $MTTF_D$ < 3 年**
Low:低	**3 年 ≤ $MTTF_D$ < 10 年**
Medium:中	**10 年 ≤ $MTTF_D$ < 30 年**
High:高	**30 年 ≤ $MTTF_D$ ≤ 100 年**
カテゴリ4のみ	**30 年 ≤ $MTTF_D$ ≤ 2,500 年**

診断カバー率 $DC(\%) = \dfrac{\text{検出できる危険側故障}}{\text{全危険側故障}}$

***DC*　（診断カバー率）**	
分類	**範囲**
無	***DC* < 60%**
Low:低	**60% ≤ *DC* < 90%**
Medium:中	**90% ≤ *DC* < 99%**
High:高	**99% ≤ *DC***

CCFの評価は、JIS B 9705-1附属書Fの共通原因故障に対する方策レベルで評価する。

以　上