SPSM

サイバーセキュリティを考慮したプロセス安全マネジメントフレームワーク

田邊雅幸

ストラトジックPSM研究会代表/横浜国立大学IMS客員教授

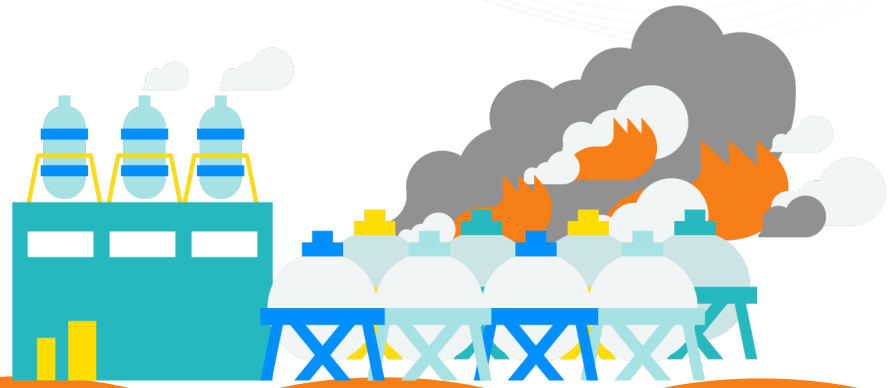
OUTLINE

1. はじめに
2. リスクベースアプローチ
3. CSリスクマネジメント
4. CS機能要求管理
5. PSとCS組織
6. おわりに

はじめに

課題と社会変化

プラント災害



熟練技術者の退職

省人化

高経年劣化

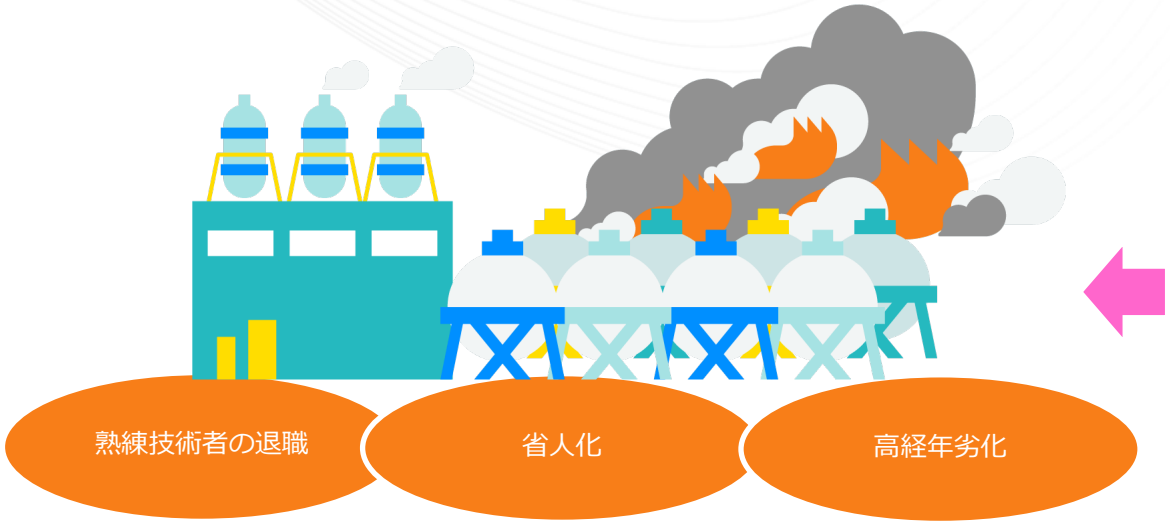
社会の変化

スマートデバイス

リスクベース
アプローチ

研究の背景

プラント災害



熟練技術者の退職

省人化

高経年劣化

社会の変化

スマートデバイス

リスクベース
アプローチ

サイバー攻撃

ストラトジックPSM研究会

横浜国立大学先端科学高等研究院(IAS)を母体とした、産官学の有志によるリスクベースのPSM効果的導入手法の研究会。2020年より活動開始。

成果物

提言書
(https://ias.ynu.ac.jp/news/20210527_spsm2020/spsm_proposal2020.pdf)

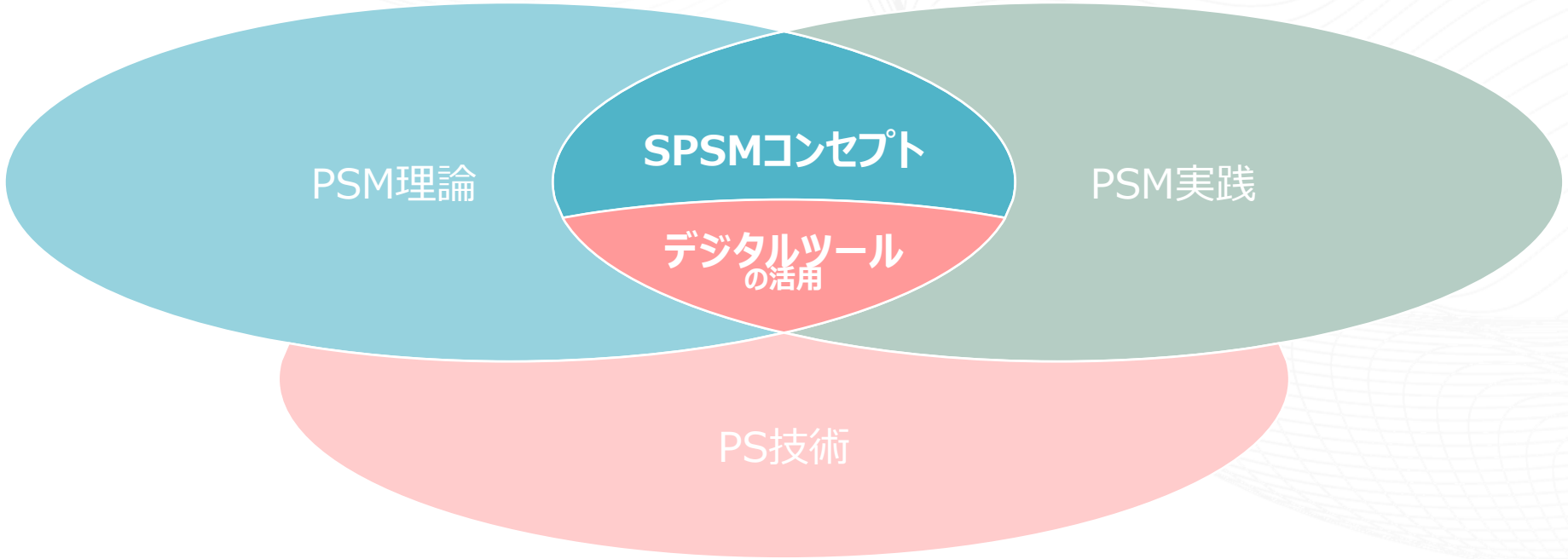
自律型高度保安導入ガイドライン
(https://www.anshin.ynu.ac.jp/activityreport/activityreport-890/)

2023年より法人化（横国大発ベンチャー）。
社会人向けのプロセスセーフティエンジニア実践教育の提供、およびリスクベースアプローチ導入のための各種サポート。

2024年よりサイバーセキュリティとPSMの統合について議論

ストラトジックPSM(SPSM)コンセプト

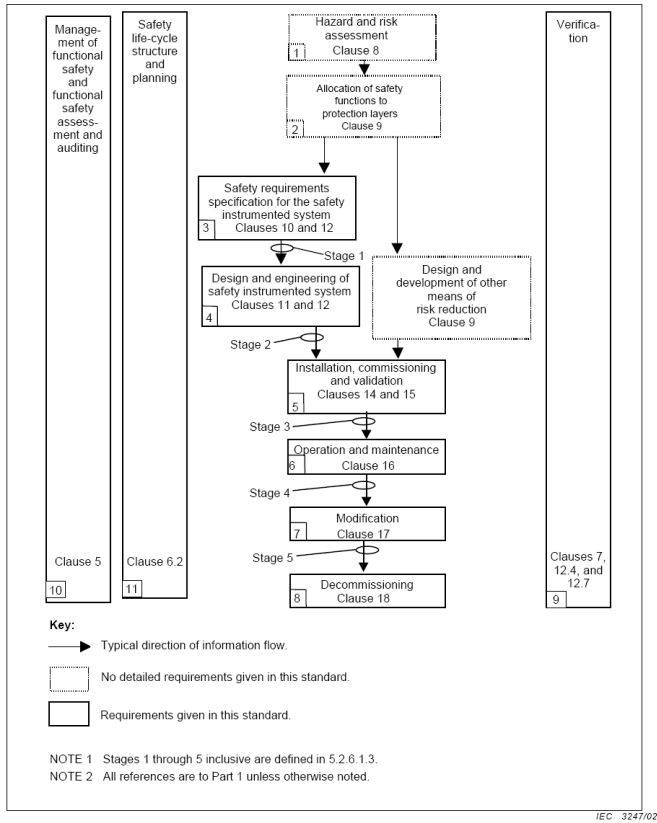
SPSM:PSMの戦略的導入のためのコンセプト



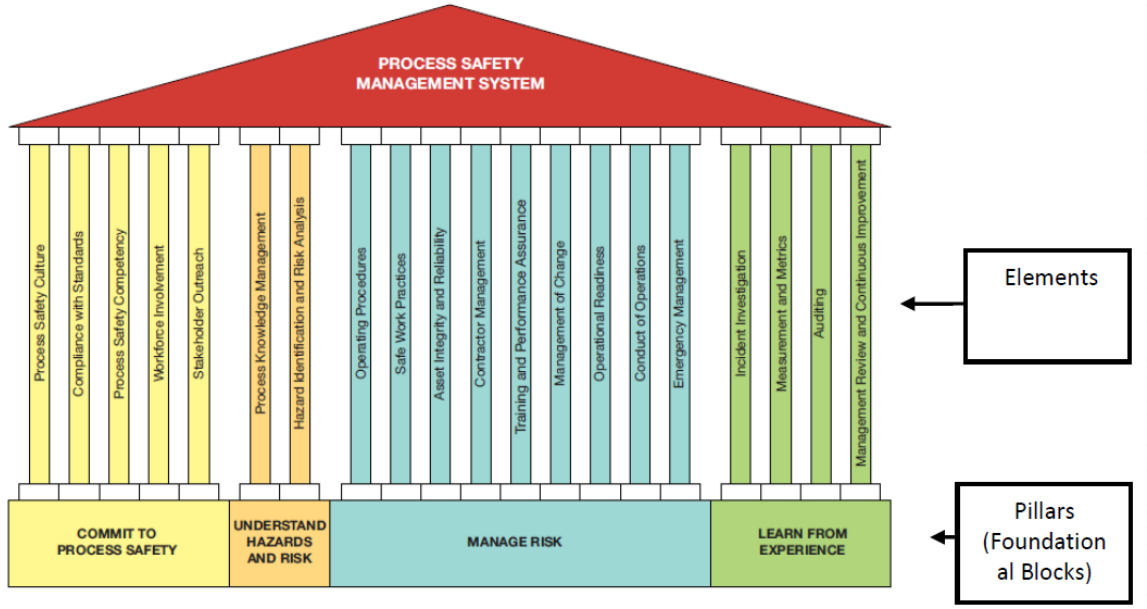
リスクベースアプローチ

ライフサイクルマネジメントとRBPS20エレメント

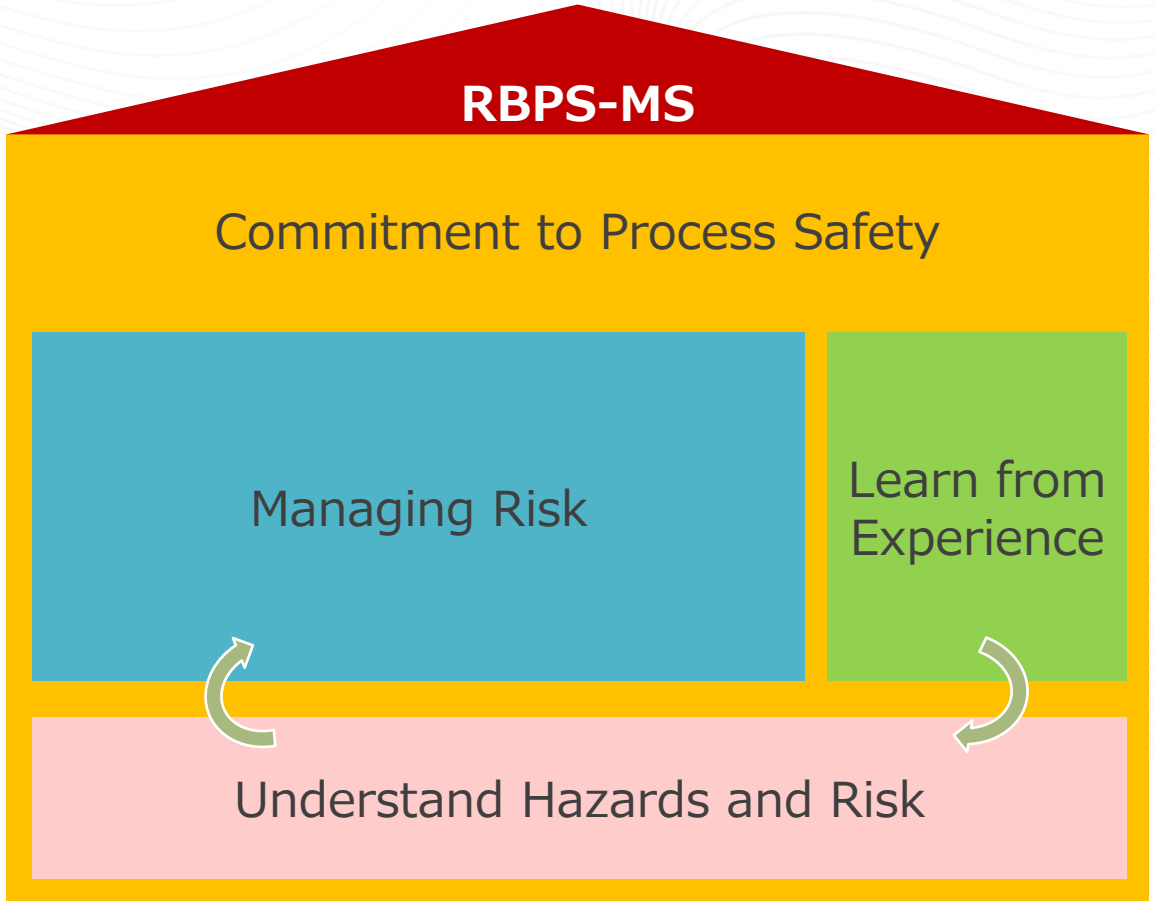
IEC61508/61511
ライフサイクルマネジメント



CCPS Guidelines for Risk Based Process Safety
RBPS 20エレメント



RBPS20エレメントモデル



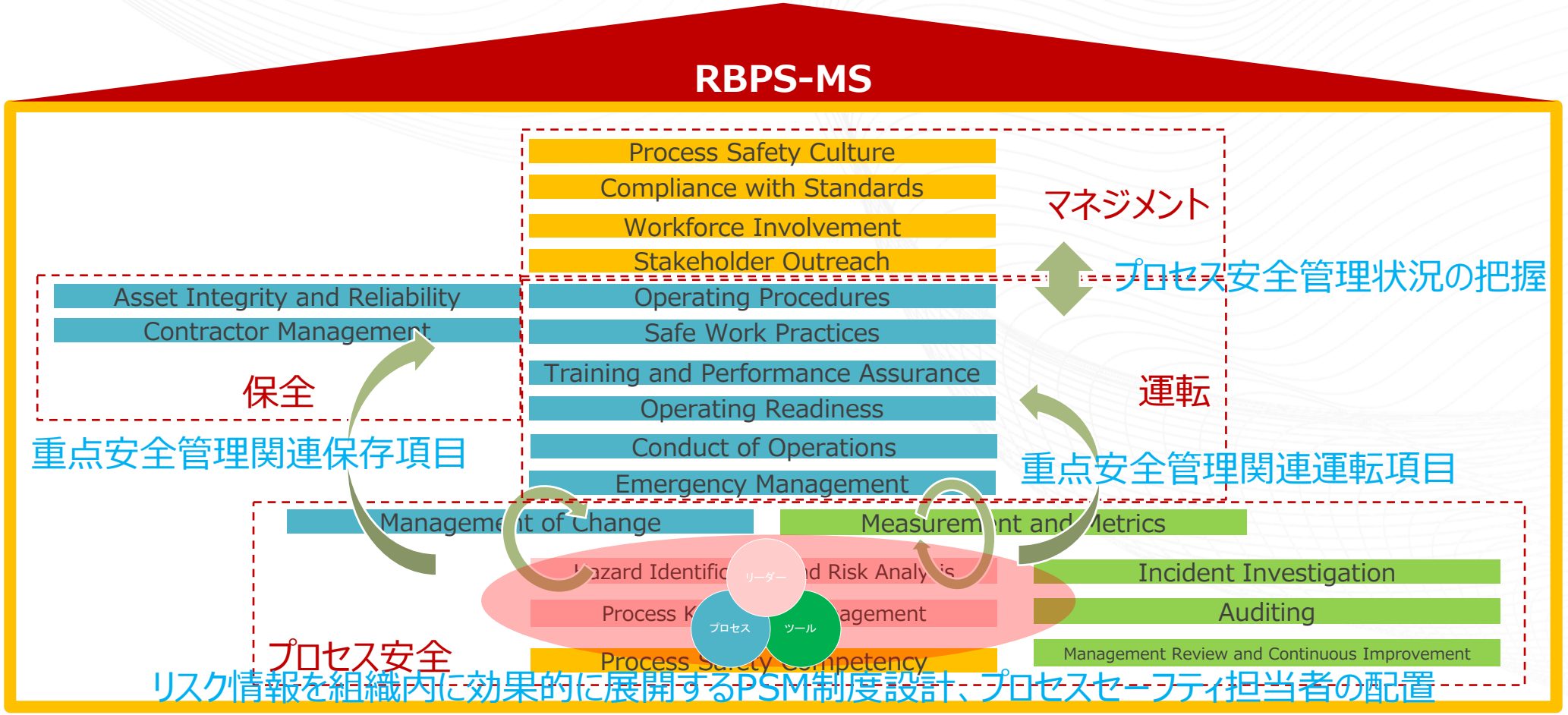
- Operating Procedures
- Safe Work Practices
- Asset Integrity and Reliability
- Contractor Management
- Training and Performance Assurance
- Management of Change
- Operating Readiness
- Conduct of Operations
- Emergency Management

- Process Safety Culture
- Compliance with Standards
- Process Safety Competency
- Workforce Involvement
- Stakeholder Outreach

- Incident Investigation
- Measurement and Metrics
- Auditing
- Management Review and Continuous Improvement

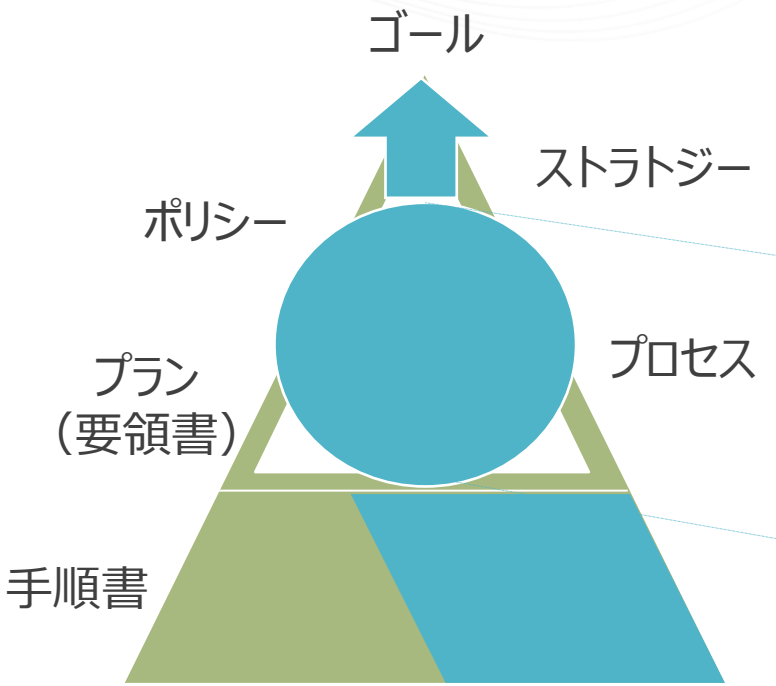
- Process Knowledge Management
- Hazard Identification and Risk Analysis

SPSMモデルによるRBPS20エレメントの実行力向上

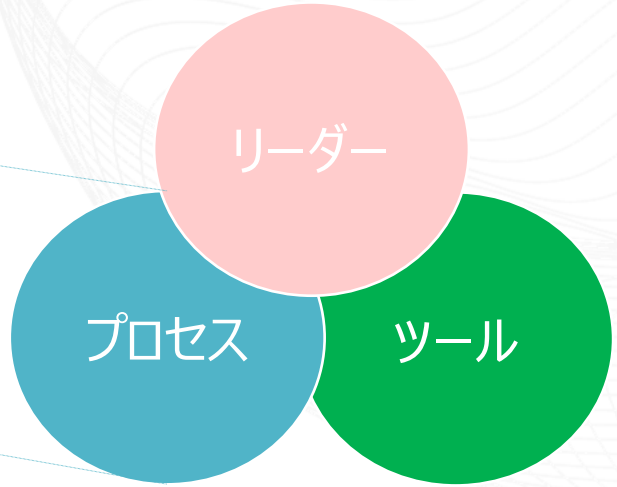


ストラトジックPSMモデル

図書＆プロセスベース融合型MS

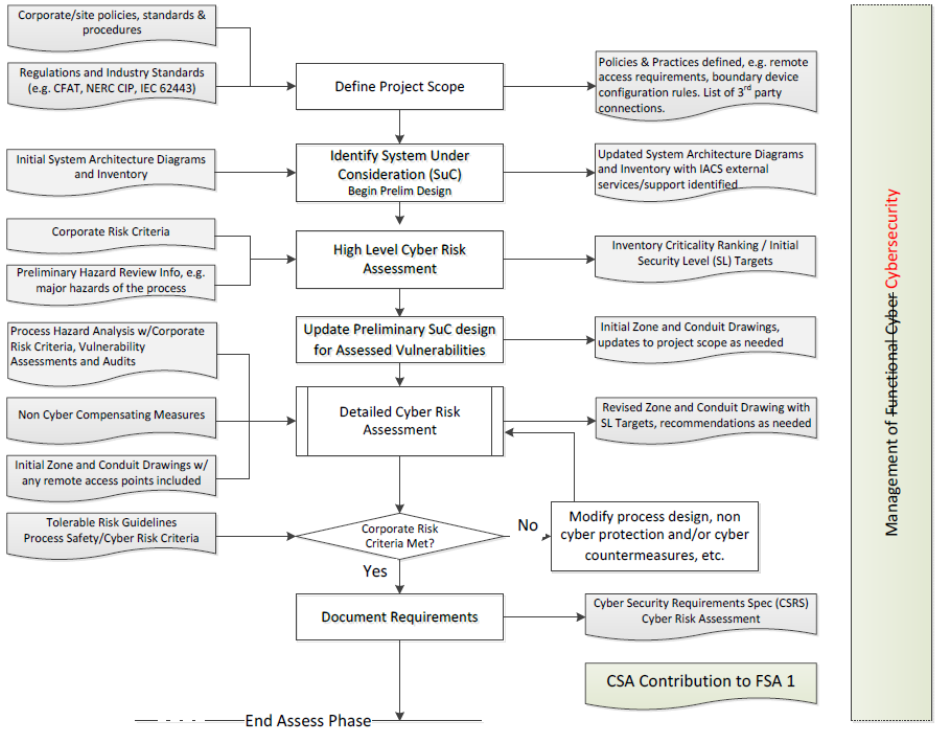


プロセスを効果的に回すため
リーダーによる牽引 と ツールによるサポート

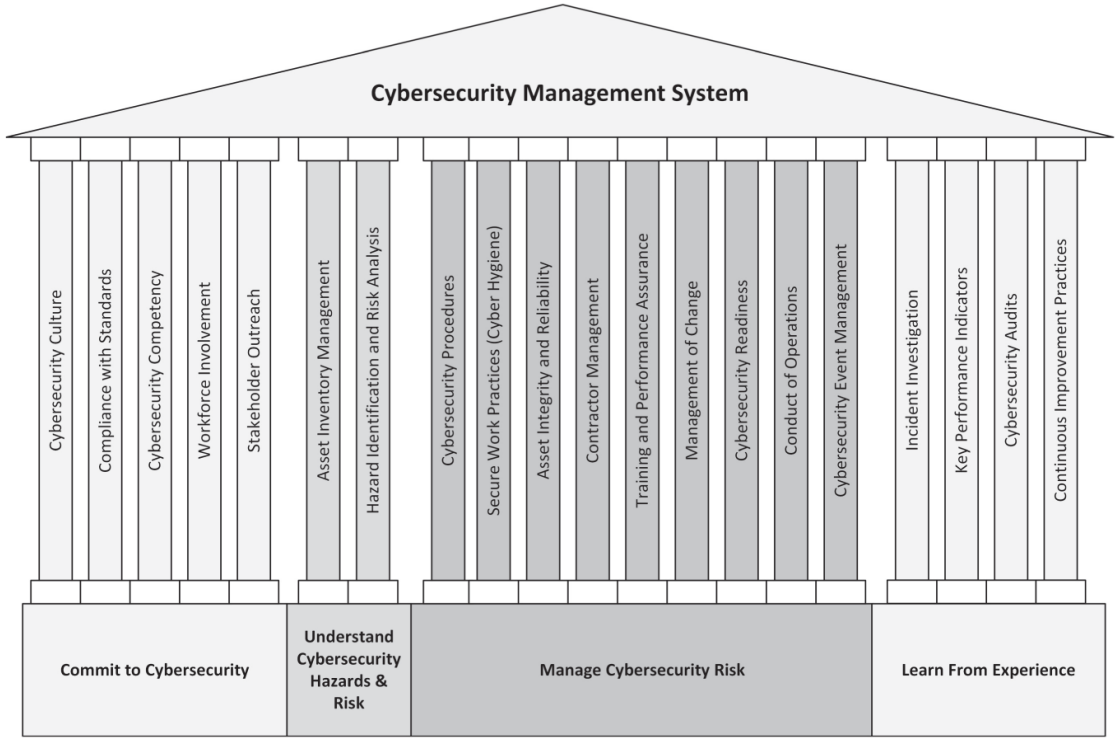


CSライフサイクルマネジメントとCS20エレメント

ISA TR84.00.09 Cybersecurity Related to the Functional Safety Lifecycle

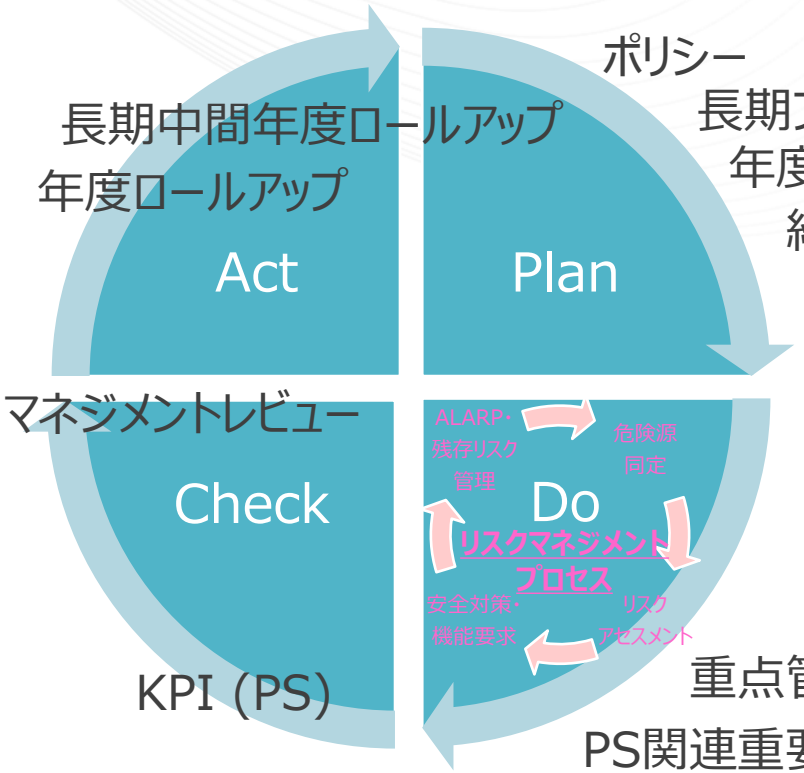


CCPS Managing Cybersecurity in the Process Industries: A Risk-based Approach



CSリスクマネジメント

RBPSマネジメントシステム



長期中間年度ロールアップ
年度ロールアップ

ポリシー
長期プラン（例：5年）
年度プラン
組織・制度
コンピテンシーマネジメントプラン

マネジメントレビュー

リスクプロファイル
レイアウト：HAZID
自然災害：HAZID
プロセス：HAZOP、LOPA
非定常作業：手順HAZOP
作業詳細：JHA

KPI（PS）

重点管理項目(PS重要業務の把握)
PS関連重要操業項目(作業許可・変更管理など)
意思決定/ALARP

監査(適合性/有効性)

サイバー攻撃に関するリスクプロファイルを把握できればリスクベースPSMと統合できるのでは？

操業管理への展開イメージ

対象の決定および
基本情報の収集

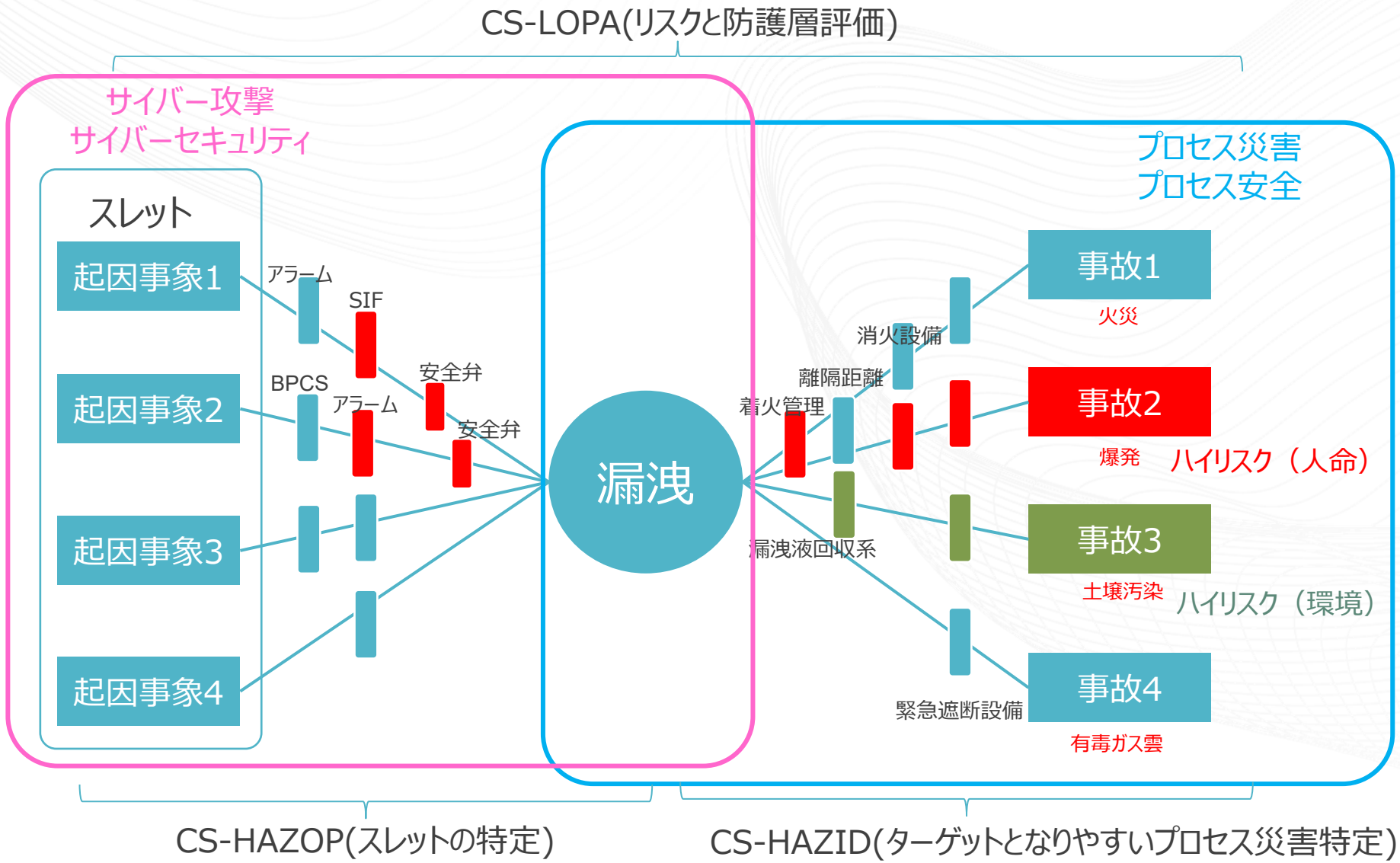
CS-PHA実施

CS-HAZOP実施

CS-LOPA実施

セキュリティレベル(SL)
および機能要求決定

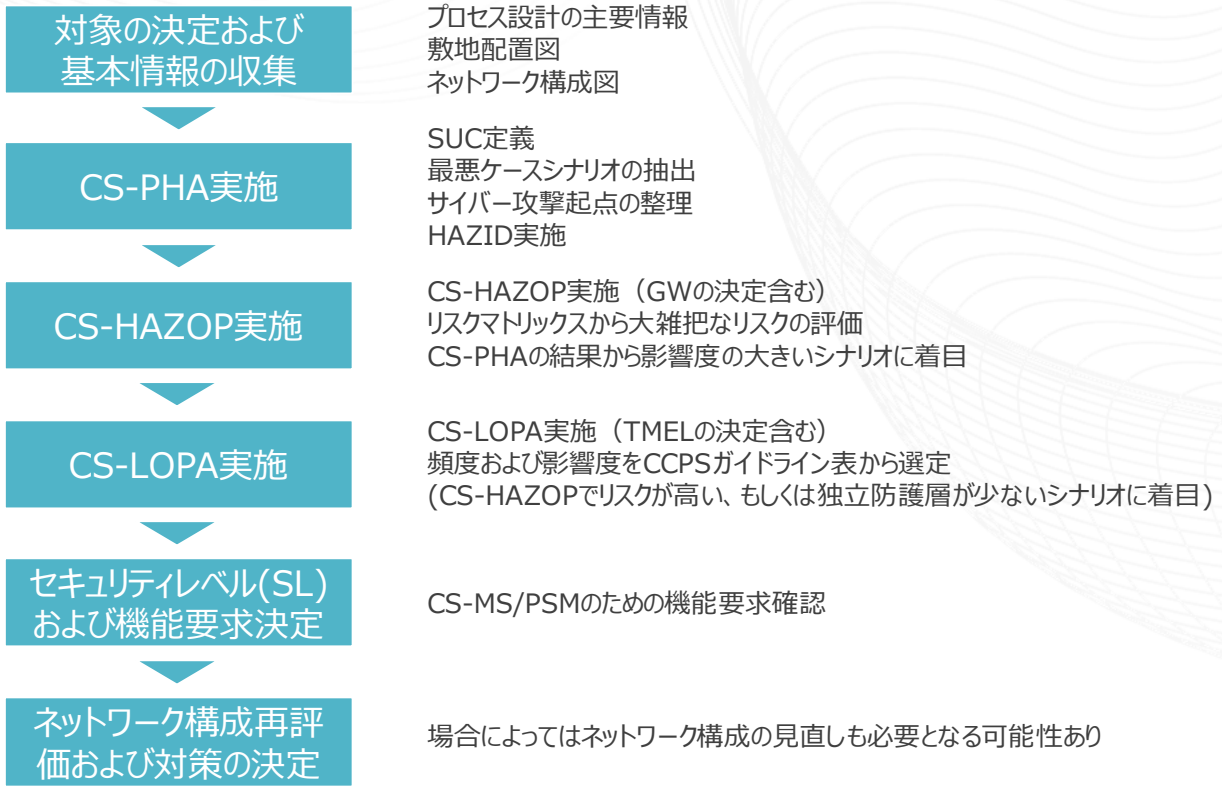
CSリスクアセスメントの位置づけ



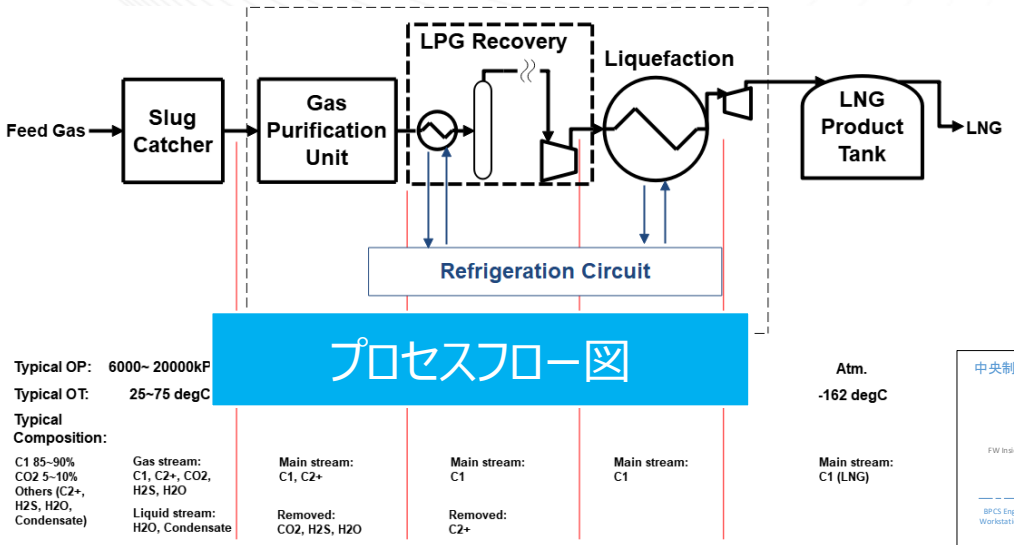
CS-PHA/HAZOP/LOPAの流れ

CSリスクアセスメントは以下2つの参考文献をもとに実施；

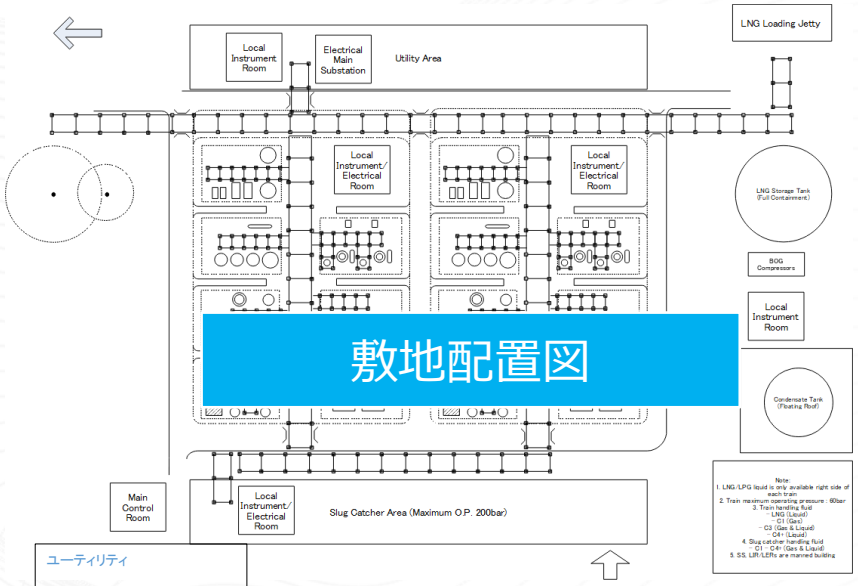
CCPS, Managing cybersecurity in the process industries - a risk based approach
ISA TR84.00.09, Cybersecurity related to the functional safety lifecycle



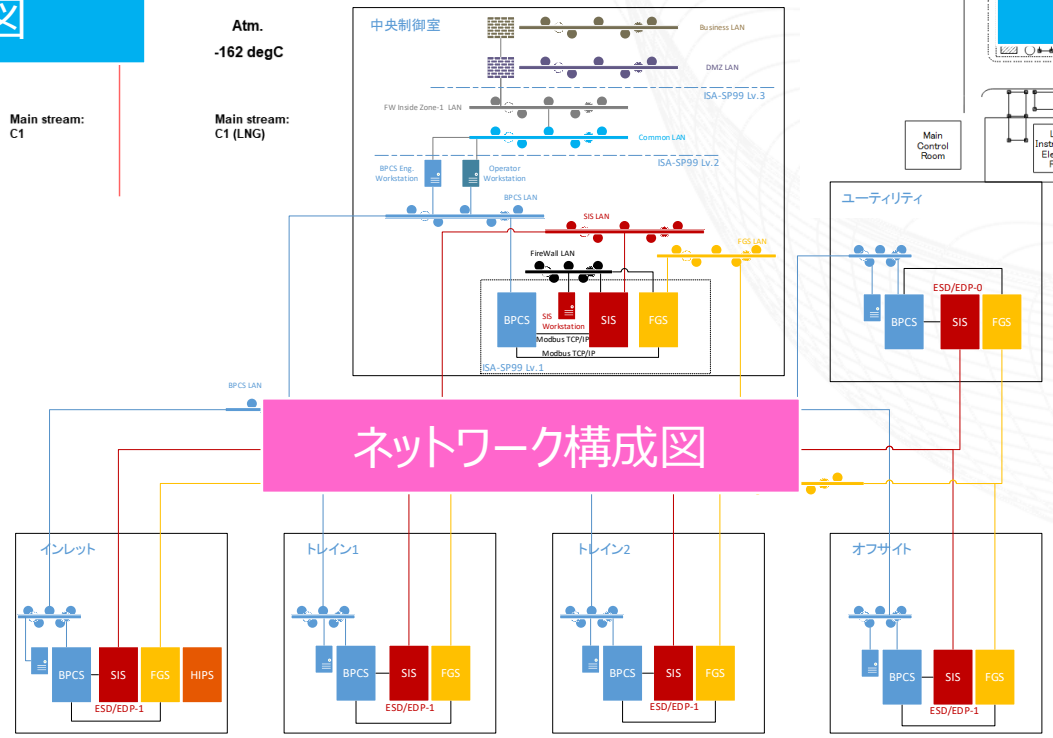
ベースラインデータの収集



プロセスフロー図



敷地配置図

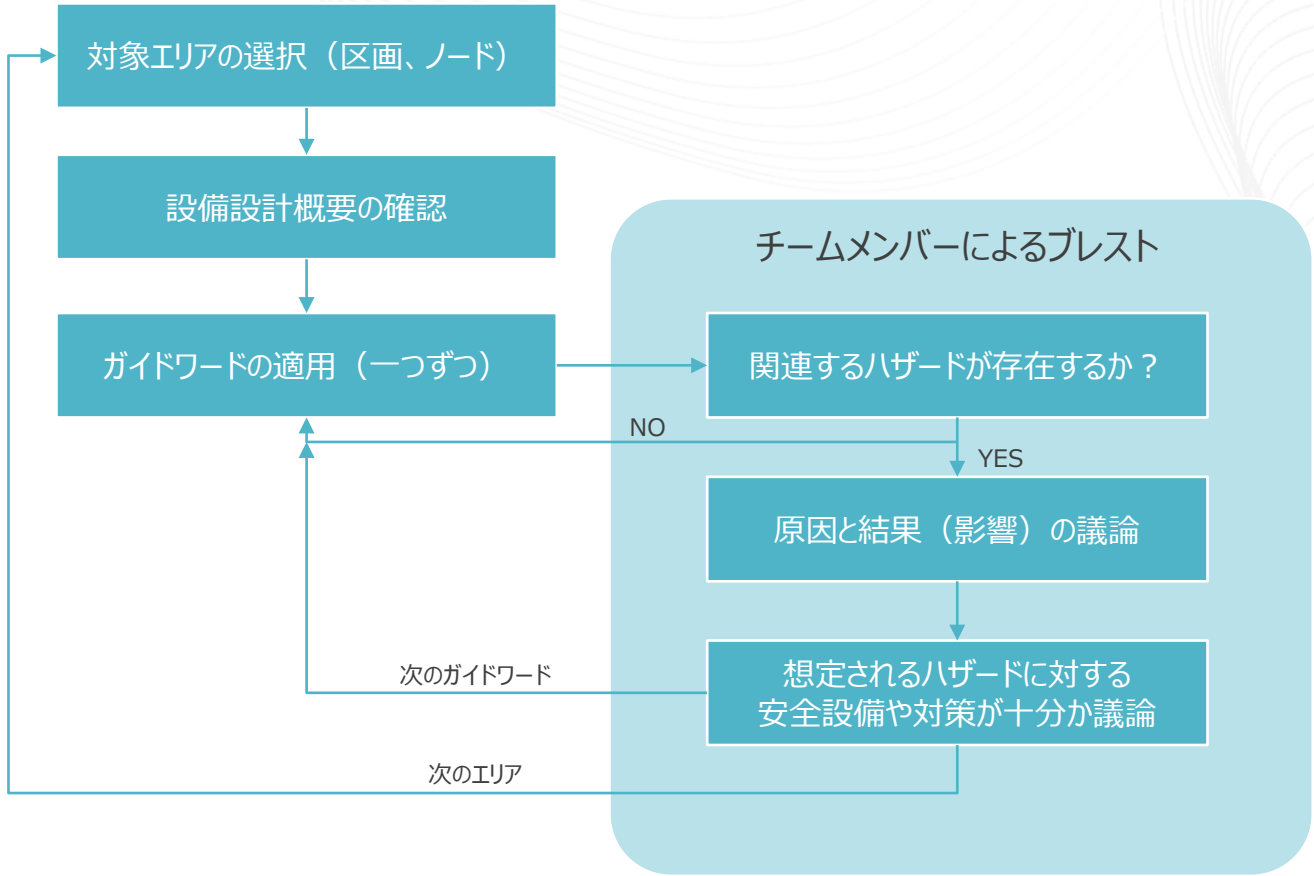


ネットワーク構成図

SUC(System Under Consideration)

No.	SUC	物理的ロケーション・アクセスポイント	補足
1	運転支援・モデル予測用外部PC	セキュリティゾーン外のPC	BPCSへの設定値変更可能
2	BPCSネットワークブロック	中央制御室BPCSエンジニアリングワークステーション	
		中央制御室BPCSオペレータワークステーション	
		中央制御室BPCS PLC（キャビネット室）	
		インレット計器室BPCSエンジニアリングワークステーション	中央制御室より人の目が減る
		インレット計器室BPCS PLC（キャビネット室）	中央制御室より人の目が減る
		トレイン1計器室BPCSエンジニアリングワークステーション	中央制御室より人の目が減る
		トレイン1計器室BPCS PLC（キャビネット室）	中央制御室より人の目が減る
		…	
		BPCS-SIS間リンクの物理的遮断	SISループの一部機能を殺せる
3	SISネットワークブロック	中央制御室 SIS ワークステーション	SISワークステーションからFGSも殺せる
		中央制御室SIS PLC（キャビネット室）	同じ中央制御室キャビネット室に入っているものは同時に他ブロックと同時に攻撃可能であることも考慮する
		インレット計器室SIS PLC（キャビネット室）	
		トレイン1計器室SIS PLC（キャビネット室）	
		…	
4	FGSネットワークブロック		
5	HIPS PLC		
6	1～5のうち時間差を持っての順次複数攻撃なポイント		

HAZID手法



ハザードタイプ	HAZIDガイドワード例
プロセスハザード	プロセス漏洩,漏洩後の着火(ガス), 漏洩後の着火(LPGなど),プロセス漏洩(全般), フレアリング, 大気ベント, ドレイン, サンプリング
サイバーアタック（CS-PHA用に追加）	プロセス設計範囲からの逸脱, 主要機器の損傷, 安全装置の無効化, 機能の喪失, 大量漏洩, 誤動作, ドミノイベント, 死傷事故, 経済損失, 環境汚染

CS-HAZOP手順

スタート

(1) SUCの選定

(2) SUC設計意図の説明

(3) ガイドワードの適用（該当するずれに関して適用）

(4) 可能性のある起因事象（Threat）の抽出

(5) Threatによる影響・結果を議論　（サイバー攻撃による最悪想定事故シナリオの抽出）

(6) 最悪想定事故シナリオに対する安全装置・対策の抽出（OTとIT防護分けて挙げると良い）

(7) リスクの評価を行う

(8) 必要に応じて勧告を挙げる

(9) 手順(3) - (8)を想定されるすべてのガイドワードに繰り返す

(10) 次のSUCに移り手順(1) - (8)を繰り返す

終了

No.	HAZOPガイドワード例
1	ソーシャル・エンジニアリング（フィッシング、スピアフィッシングなど）
2	通信（例：サービス妨害、マン・イン・ザ・ミドル）
3	サプライチェーン（例：サービスプロバイダの侵害）
4	物理的アクセス（例：無防備なワークステーションへのログオン）
5	ソフトウェア（例：既知のソフトウェアの脆弱性の悪用）
6	ハードウェア（例：安全でないポートへのUSB接続）

CS-LOPA手法

目標リスク値までのギャップが1(もしくは0.1)以上(すなわちこれ以上のリスク削減は必要なし)

LOPA比率(すなわちPFD)

事故シナリオの目標リスク削減値

$$LOPA\ Ratio\ (Safety) = \frac{TMEL}{ICL \times PFD_{PS1} \times PFD_{PS2} \times PFD_{CS1} \times PFD_{CS2} \ldots \times VFi \times VFp.}$$

起因事象の頻度

安全装置の故障確率
(PS, CSそれぞれ加味)

着火確率
(火災・爆発の場合)

人の存在確率

各数値パラメータに関しては“CCPS Managing Cybersecurity in the Process Industries: A Risk-based Approach”に例示されているので参照のこと

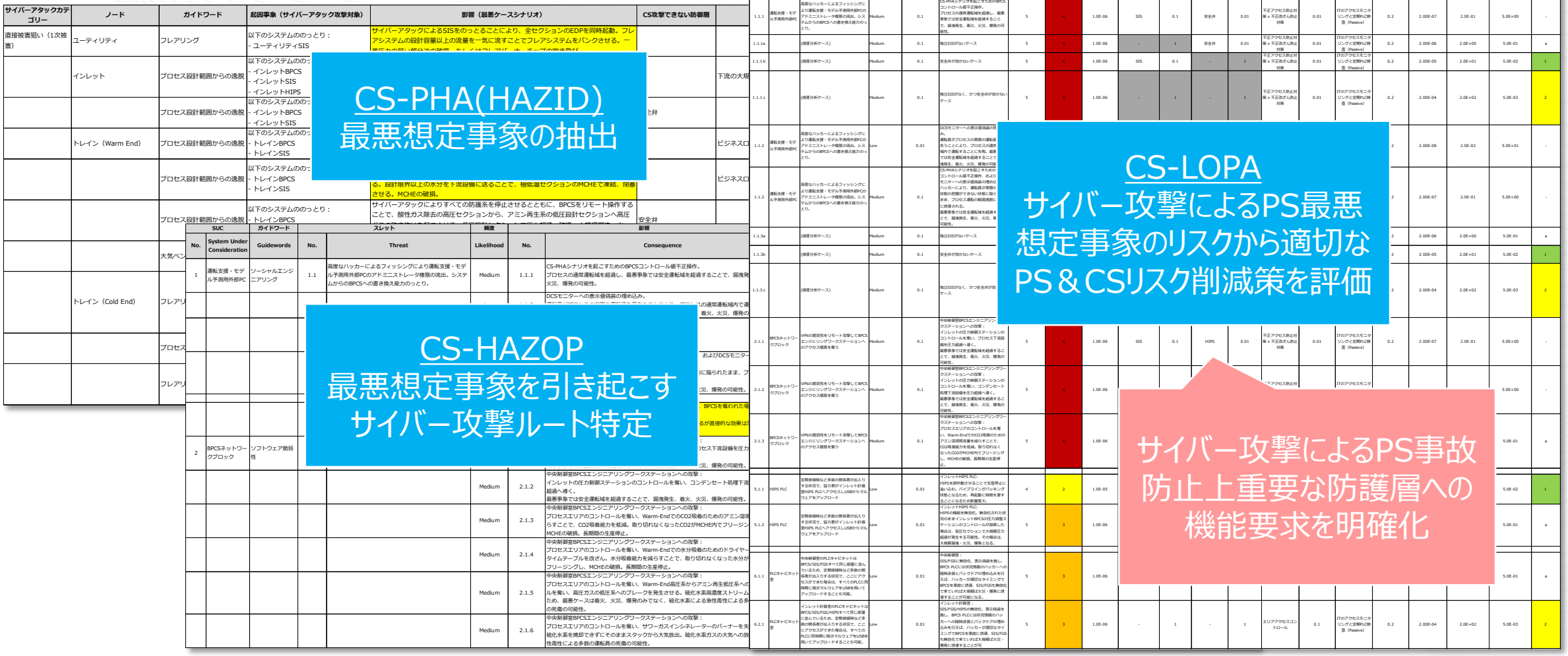
CS-PHA/CS-HAZOP/CS-LOPAアウトプット

CS-PHA(HAZID)
最悪想定事象の抽出

CS-HAZOP
最悪想定事象を引き起こす
サイバー攻撃ルート特定

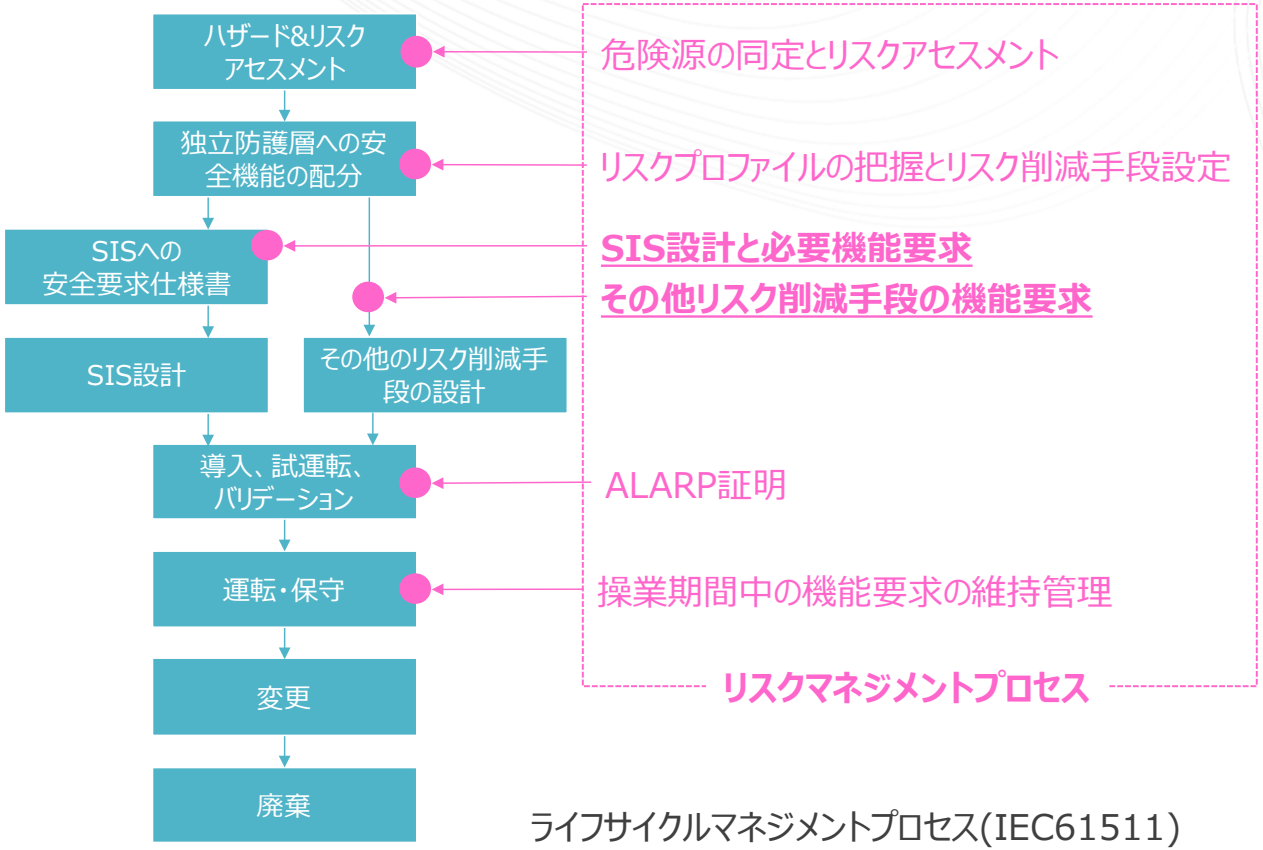
CS-LOPA
サイバー攻撃によるPS最悪
想定事象のリスクから適切な
PS＆CSリスク削減策を評価

サイバー攻撃によるPS事故
防止上重要な防護層への
機能要求を明確化

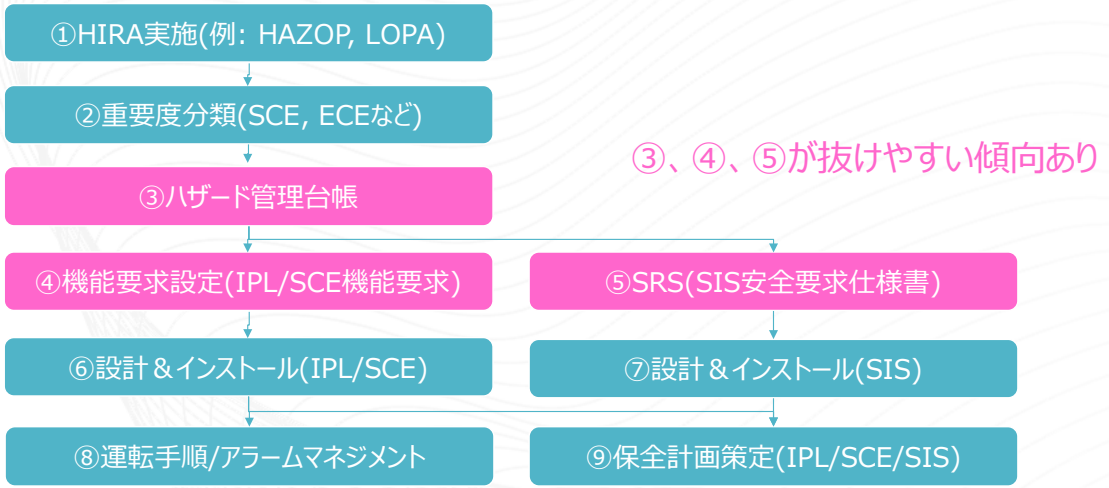


CS機能要求管理

技術的要件定義の重要性



ライフサイクルマネジメントプロセス(IEC61511)



③、④、⑤が抜けやすい傾向あり

セキュリティレベル

Severity Level	Tolerable Frequency （TMEL）	Attributes
1	1.00 E-2/ yr.	セキュリティ防護に関する特別な要求なし
2	1.00 E-3/ yr.	何気ないもしくは偶然の侵害からの保護を対象とする。 4～8時間の間、攻撃を遅らせるか拒否できる対策と検知能力を持つこと。
3	1.00 E-4/ yr.	少ないリソース、一般レベルのスキル、低モチベーションの攻撃者の単純な手段による意図的な侵害から保護することを対象とする。 対策と検知の有効性により、攻撃を数日間遅らせるか拒否できる対策と検知能力を持つこと。 セキュリティレベル 1 よりもリスク低減係数（RRF）が桁違いに向上することが必要。
4	1.00 E-5/ yr.	中程度のリソース、IACS固有のスキル及び中程度のモチベーションの攻撃者の洗練された手段を用いた意図的な侵害からの保護を対象とする。 数日から数週間の期間、攻撃を遅らせるか拒否することができる対策と検知能力を持つこと。 セキュリティレベル2によりもリスク低減係数（RRF）の桁違いに向上することが必要。
5	1.00 E-6/ yr.	広範なリソース、IACS固有のスキル、高いモチベーションを持つ攻撃者による洗練された手段を用いた意図的な侵害からの保護を対象とする。 数週間から数ヶ月の期間、攻撃を遅らせるか拒否することができる対策と検知能力を持つこと。 セキュリティレベル3よりもリスク低減係数（RRF）が桁違いに向上することが必要。

CSMS 20エレメント

CSMS 20 Elements	CSMS 20エレメント	PSMに導入すべき要件
Cybersecurity Culture	サイバーセキュリティ文化	CS起因によるPS事故シナリオ防止の重大さの理解醸成のためのコミットメント。ポリシーの整備。
Compliance with Standards	規格類への遵守	CCPSガイドラインやISAなどガイドライン・規格類の認知とPSMとの関連性理解。
Cybersecurity Competency	サイバーセキュリティコンピテンシー	CS対応組織設計と能力要件の担保（教育システム構築）。
Workforce Involvement	従業員の参画	従業員が積極的にCSを高める行動を取るように教育・啓蒙。
Stakeholder Outreach	ステークホルダーアウトリーチ	PSMに関する規制庁や業界団体とCS対応方法について連携。
Asset Inventory Management	資材在庫管理	不正なアクセスを防止する。
Hazard Identification and Risk Assessment	危険源の同定とリスク解析	CS-PHA/CS-HAZOP/CS-LOPAを実施し、CSMSへの管理要件を定義する。
Cybersecurity Procedures	サイバーセキュリティ手順	CS-PSに関連する手順の整備。HIRA手順。PSM関連手順へのCS要素追加。
Secure Work Practices (Cyber Hygiene)	確実な業務習慣（CS慣行）	CS-PS事故防止のための業務習慣ベストプラクティスの整備。
Asset Integrity and Reliability	設備の健全性と信頼性	ITネットワークにぶら下がる設備の保全。
Contractor Management	協力会社の管理	サイバーアタックを媒介する可能性もあるためCS管理を徹底。
Training and Performance Assurance	トレーニングとパフォーマンスの保証	IT-OT間の連携トレーニング。
Management of Change	変更管理	特にネットワーク関連の設備変更や、新規IoT技術導入でゾーン外からのアクセスが増える際はリスクアセス要。
Cybersecurity Readiness	サイバーセキュリティレディネス	PSSRの確認事項へCS関連項目を追加する。
Conduct of Operations	操業の実行	HIRAから定まる要件をもとにIT-OT間の連携業務を定義し確実にCS業務を遂行する。
Cybersecurity Event Management	サイバーセキュリティ事象管理	CSイベント発生時の対応体制整備。
Incident Investigation	事故調査	CS事故調査体制整備。
Key Performance Indicator	キーパフォーマンスインディケーター	CSイベントに特化したKPI整備。
Cybersecurity Audits	サイバーセキュリティ監査	監査へのCS事項の追加。
Continuous Improvement Practices	継続的改善の慣習	PSMで設定したCS事項の定期的確認とPSM/CSMプログラムの改善。

SUC管理台帳（簡易な機能要求管理）

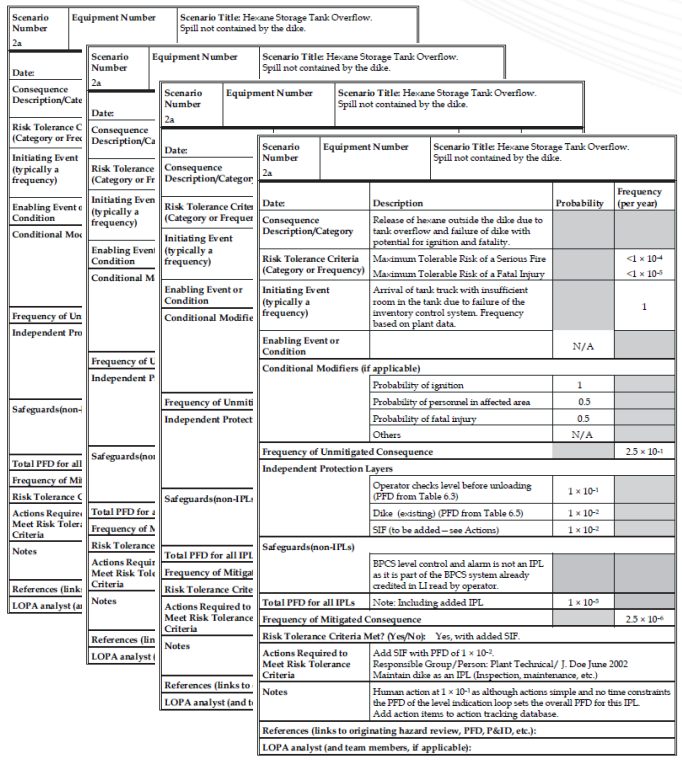
CS-HAZOP SUC		サイバーアタック想定			独立防護層へのリスクアロケーション						残存リスク	管理要件
		物理的ロケーション・アクセスポイント	起因事象	影響	アラーム・ITエンジニア/運転員の対応	安全弁	SIS	アクセスコントロール	不正アクセス防止対策 x 不正改ざん防止対策	ITアクセス管理・定期PLC検査	SL	
1	運転支援・モデル予測用外部PC	セキュリティゾーン外のPC	高度なハッカーによるフィッシングにより運転支援・モデル予測用外部PCのアドミニストレータ権限の流出。システムからのBPCSへの書き換え能力のっとり。	CS-PHAシナリオを起こすためのBPCSコントロール値不正操作。プロセスの通常運転域を超過し、最悪事象では安全運転域を超過することで、漏洩発生、着火、火災、爆発の可能性。	-	0.01	0.1	-	0.01	0.2	1	PS系独立防護層の管理はPSMでの管理要件に従う。 不正アクセス防止対策および不正改ざん防止対策は定期的にアップデートすること（white list） ITアクセスの不正ログインモニタリングは常時実施。OT側との連携方法を明確に定義すること。 PLC検査は最低月1回は実施すること。
2	BPCSネットワークブロック	中央制御室BPCSエンジニアリングワークステーション										
		中央制御室BPCSオペレータワークステーション										
		中央制御室BPCS PLC（キャビネット室）										

実施において工夫は必要なものの、
CSリスクアセスメントを行うことで
サイバー攻撃によるプロセス災害のリスクと
その防護層および管理要件を明確化できる

- セキュリティエリア外の運転支援システムなどもターゲットとなる可能性
- 本質安全・安全弁などサイバーで落とされない手段の価値が高まる
- PS防護層が脆弱なところがねらい目

リスクマネジメントデジタルツールの活用

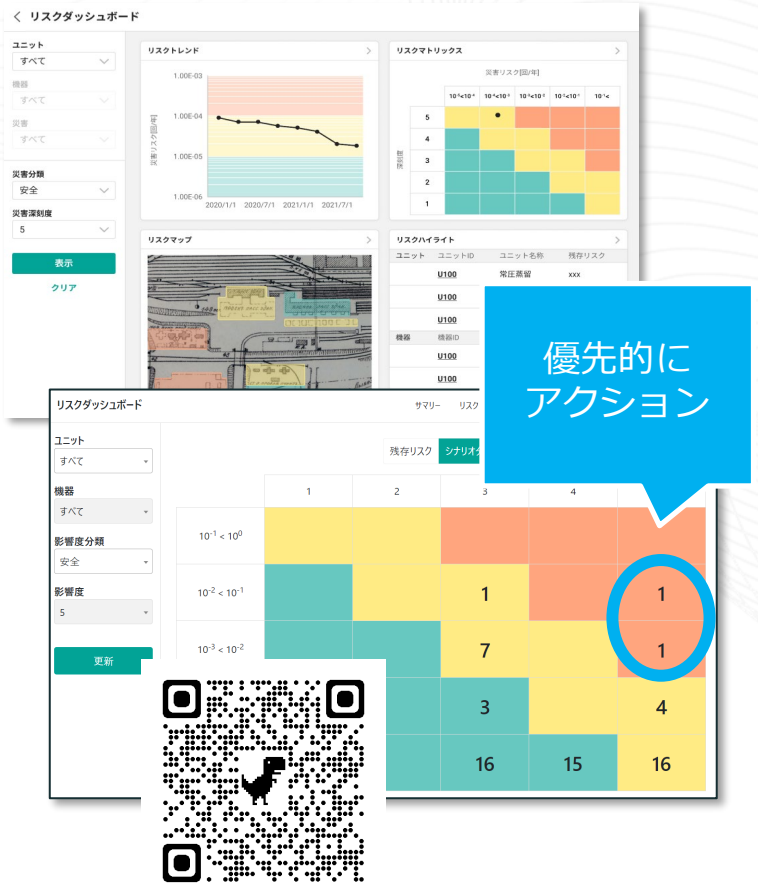
ローカルフォルダのワークシート



Scenario Number 2a	Equipment Number	Scenario Title: Hexane Storage Tank Overflow. Spill not contained by the dike.

Date:	Description	Probability	Frequency (per year)
Consequence Description/Category	Release of hexane outside the dike due to tank overflow and failure of dike with potential for ignition and fatality.		
Risk Tolerance Criteria (Category or Frequency)	Maximum Tolerable Risk of a Serious Fire Maximum Tolerable Risk of a Fatal Injury		$<1 \times 10^{-4}$ $<1 \times 10^{-5}$
Initiating Event (typically a frequency)	Arrival of tank truck with insufficient room in the tank due to failure of the inventory control system. Frequency based on plant data.		1
Enabling Event or Condition		N/A	
Conditional Modifiers (if applicable)			
	Probability of ignition	1	
	Probability of personnel in affected area	0.5	
	Probability of fatal injury	0.5	
	Others	N/A	
Frequency of Unmitigated Consequence			2.5×10^{-1}
Independent Protection Layers			
	Operator checks level before unloading (PFD from Table 6.3)	1×10^{-1}	
	Dike (existing) (PFD from Table 6.5)	1×10^{-2}	
	SIF (to be added – see Actions)	1×10^{-2}	
Safeguards(non-IPLs)	BPCS level control and alarm is not an IPL as it is part of the BPCS system already credited in LI read by operator.		
Total PFD for all IPLs	Note: Including added IPL	1×10^{-5}	
Frequency of Mitigated Consequence			2.5×10^{-6}
Risk Tolerance Criteria Met? (Yes/No): Yes, with added SIF.			
Actions Required to Meet Risk Tolerance Criteria	Add SIF with PFD of 1×10^{-2}. Responsible Group/Person: Plant Technical/ J. Doe June 2002 Maintain dike as an IPL (Inspection, maintenance, etc.)		
Notes	Human action at 1×10^{-1} as although actions simple and no time constraints the PFD of the level indication loop sets the overall PFD for this IPL. Add action items to action tracking database.		
References (links to originating hazard review, PFD, P&ID, etc.):			
LOPA analyst (and team members, if applicable):			

クラウド上のリスク情報

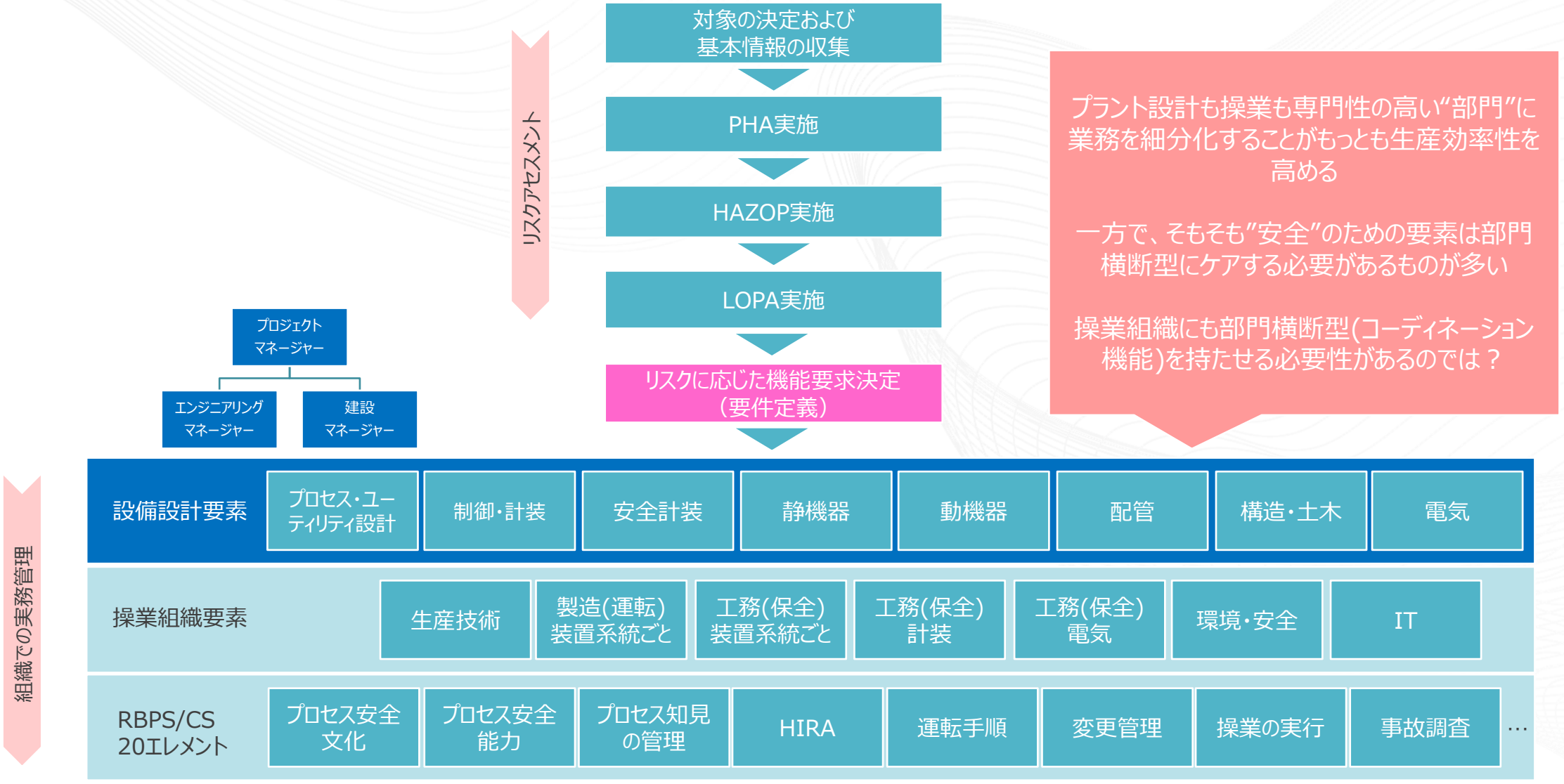


RBPS20エレメントでの活用

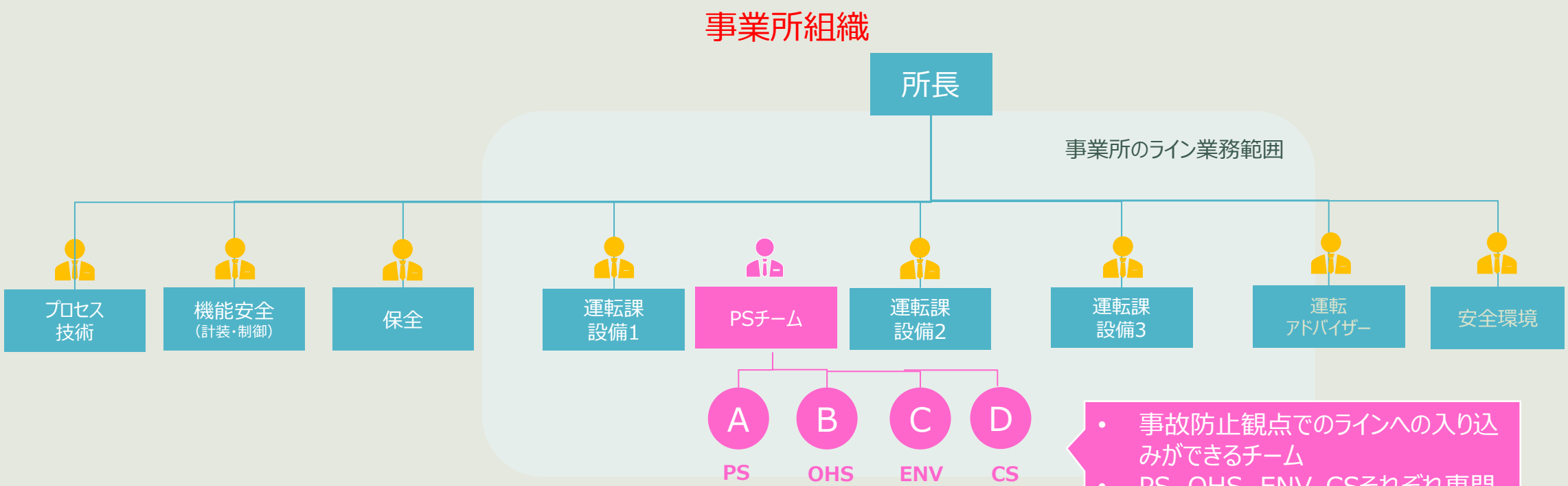
- 高リスク項目のALARP判断
- 重要アラーム発報時手順(手順&訓練)
- 事故起因機器と安全装置の健全性と信頼性
- 変更管理や作業許可審査時のリスク変化の定量的確認
- 具体的なプロセス災害に対する緊急時対応(計画&訓練)

PSとCS組織

RAから操業管理への展開イメージ(PS全般)



CSも考慮したPSチーム構成イメージ



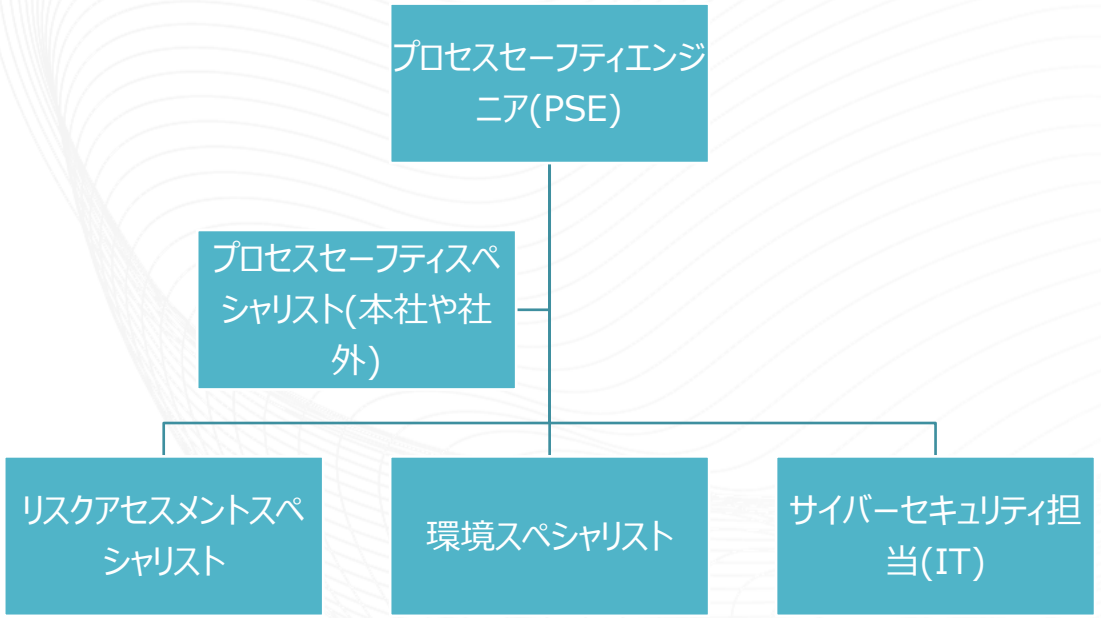
PSチーム編成検討

PSEの重要性は高まっているが、世界的にもリスクアセスメント技術の進化・分化が進んでおり”PSE”の中にさらにスペシャリティができてきている。

PSE職務も必要コンピテンシーの広がりに合わせてPSチームとして対応していくことが現実的ではないか。

この流れに従い、PSチームにCS担当を配員しIT-OT間の連携を強化することが望ましい。

IT-OT間の技術の壁は高い。IT-OT間の通訳ができる人材育成が必要。



おわりに

CSを考慮したPSMの導入

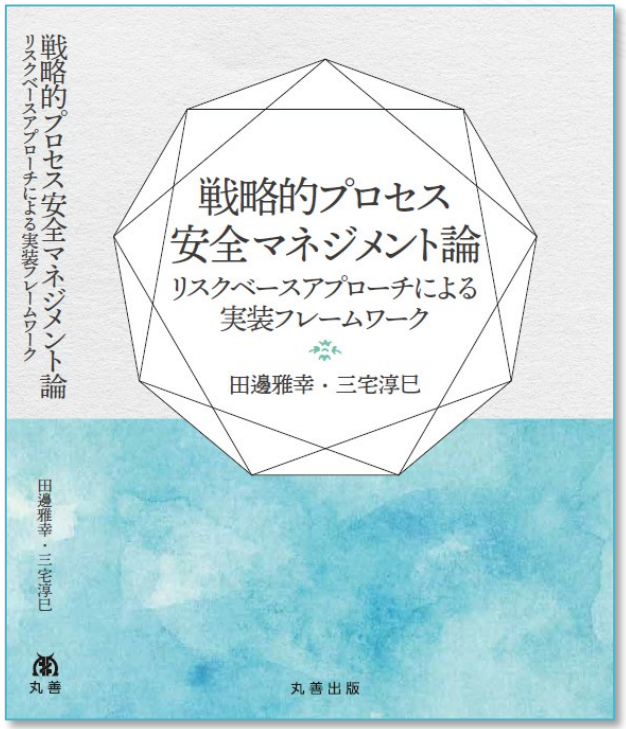
リスクベースアプローチを採用するプロセス安全マネジメントシステムを構築することで組織のプロセス安全力の継続的改善につながることが期待される

プロセス災害を狙ったサイバー攻撃を対象としたサイバーセキュリティリスクアセスメントを実施することで、同じリスクベースプロセス安全マネジメントシステムにのせることが可能となる

これからのプロセス安全グループは広範な専門性をカバーするため複数のスペシャリストからなるチームで対応することも重要となってくる

SPSMラーニング

戦略的PSM論（丸善出版）



SPSM概論コース

なぜリスク？なぜプロセス安全？

SPSM基礎コース

業界の、世界の、ベストプラクティス

SPSMスペシャリストコース

実践フレームワークと実践スキル