スマート安全　PJの進捗報告と今後の方針

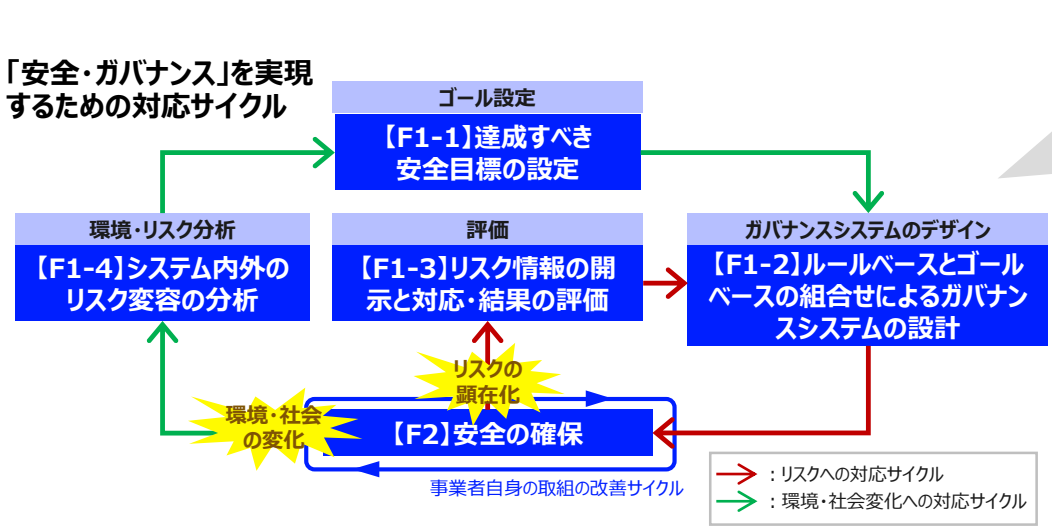
Digital Architecture Design Center

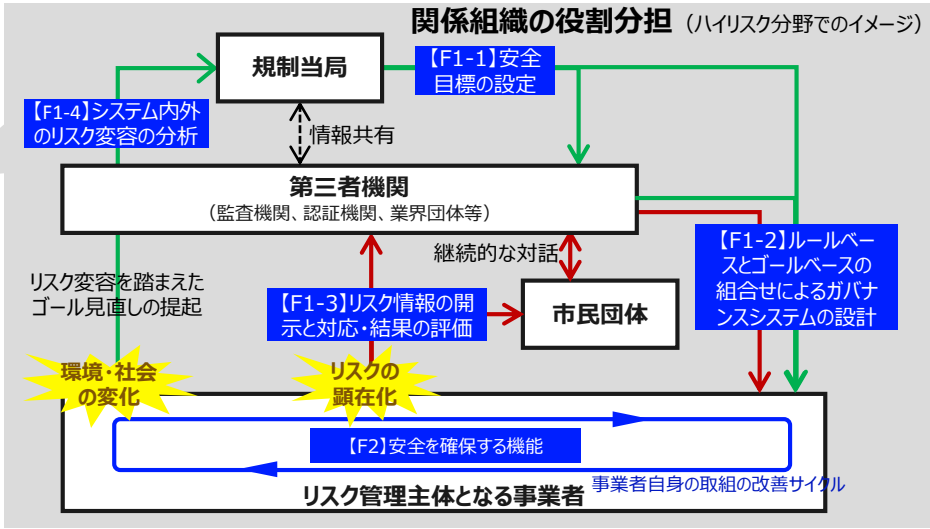
本PJの目的

Ⅰ）人の判断を介在せずデータで制御されるCPS、Ⅱ）連携先が頻繁に変更されうるシステム、Ⅲ）新たな技術革新を取り入れて進化するシステムが、今後実装される中で、このような**新たなリスクや複雑性が増大し、変化が加速したシステム**において、**安全を確保するためのガバナンスの在り方**を検討する。

2020年度の成果

- 複雑で変化の速いシステムに対しては、事前の合意によって定められたプロセス・手段（ルール）とその実行・遵守、という形のみを固持するのではなく、**ゴールに照らしながら動的に手段を選択**し（＝ゴールベース）、**変化に柔軟に対応できるアジャイル型のガバナンス**（＝アジャイル・ガバナンス）が求められる。
- そのためには、事業者の**①「安全確保・維持のための取組」**そのものと、これまで規制当局（あるいは権限委譲された機関）が実施していた取組の適切性の確認や是正等の**②「ガバナンス」**は、互いに情報共有しながら、それぞれ「定期」ではなく**「状況の変化に合わせて都度」行う**必要がある。
- **①②で構成される「安全・ガバナンス」のあるべき姿**の検討にあたり、議論が先行する自動走行等の調査や、具体例としてプラント分野における関係組織の役割分担や関係性を分析した。その結果、**CPSや先進技術の特徴を考慮したリスク評価**や**技術的な基準の策定**など、**安全確保のための一部の機能や責任を第三者機関に分担**することや、**リスクへの対応/環境・社会変化への対応の両方のプロセスを継続的に回す**ことが重要との結論に至った。
- 上記を踏まえ、**「安全・ガバナンス」を実現するための対応サイクル**（左図）と、**関係組織の役割分担**（右図）についての仮説を検討した。なお、複数の分野に適用できるよう抽象度が高い形で検討を行ったため、具体分野に当てはめた仮説の検証は2021年度以降に実施。





今後の方針

まずは、システムの変化が速く連携が複雑になる**自律移動ロボットをユースケース**として、**上記の仮説や効果の検証**を行う。その後、それ以外の複数分野でも検証を行った後、その結果を踏まえて、国際標準化や規制等への反映などの実装の仕方について検討を進める。

Digital Architecture
Design Center

IPA Better Life with IT

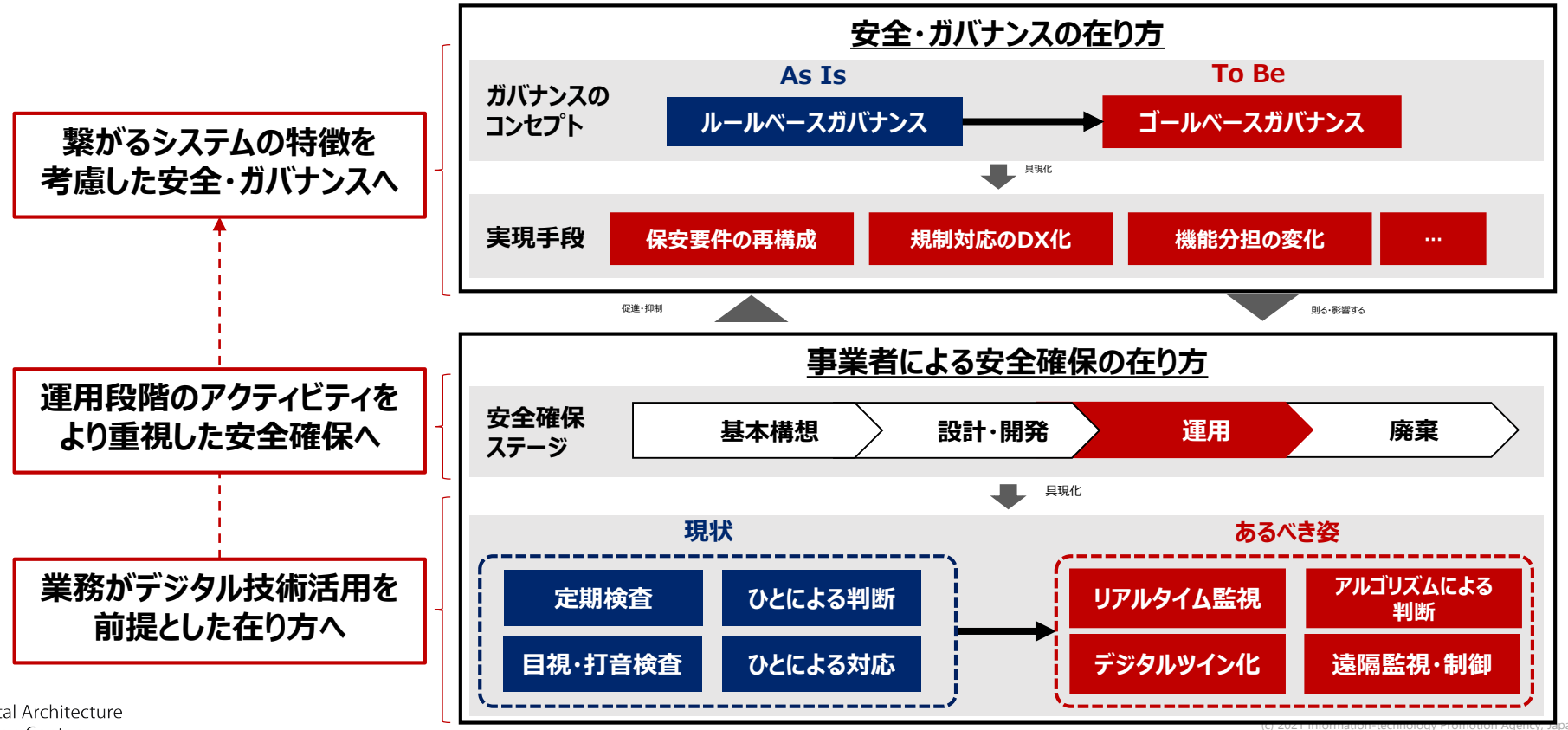
スマート安全PJ中間成果

～Society5.0における安全確保を実現する ガバナンスアーキテクチャのビジョン～

2021年７月
独立行政法人情報処理推進機構（IPA）
デジタルアーキテクチャ・デザインセンター（DADC）

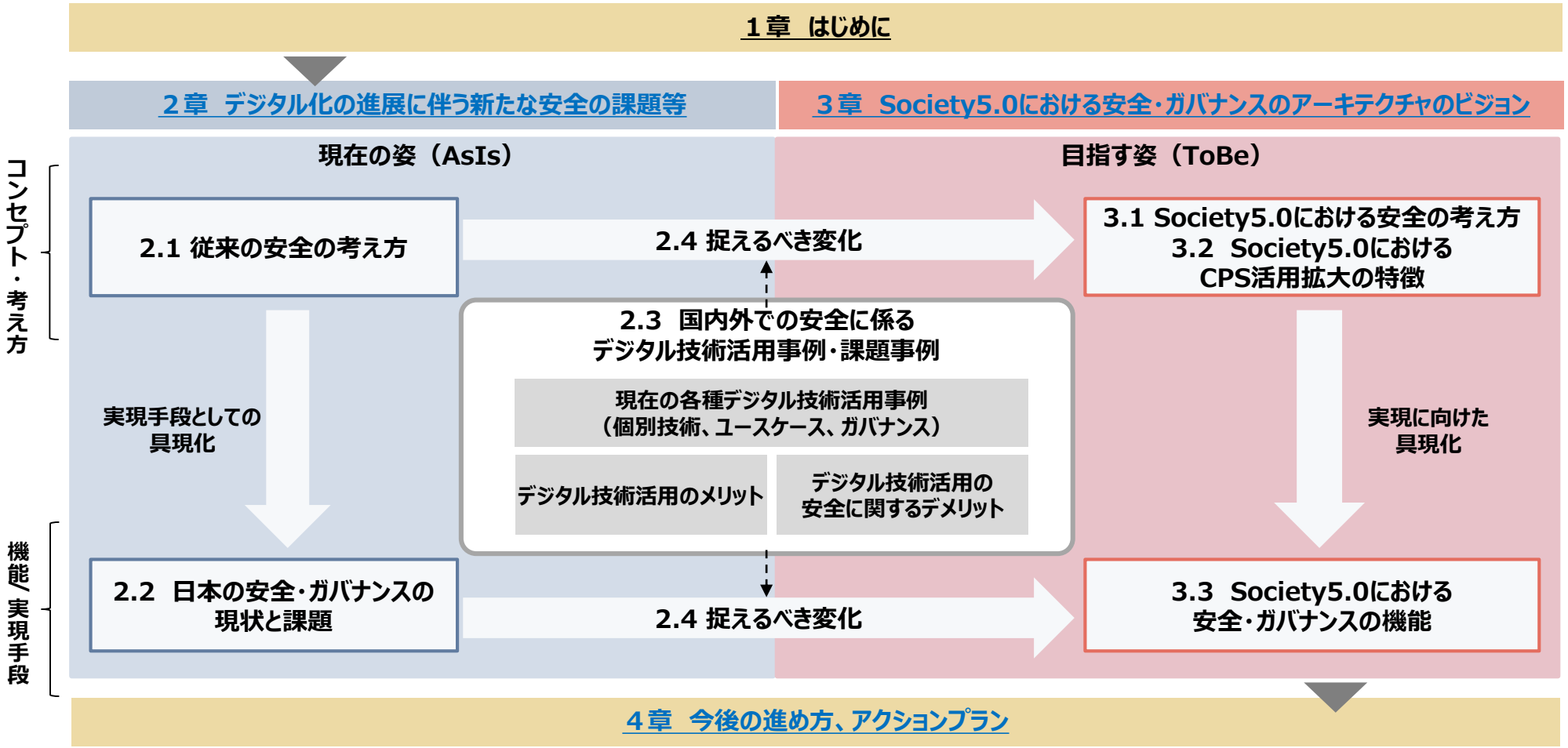
はじめに（１章）

- 経済産業省「GOVERNANCE INNOVATION VER.2: アジャイル・ガバナンスのデザインと実装に向けて」にある通り、複雑で変化の速いデジタル社会において、イノベーションを加速しつつ社会の安全安心を実現するためには、事前の合意によって定められたプロセス・手段（ルール）とその実行・遵守、という形のみを固持するのではなく、ゴールに照らしながら動的に手段を選択し（＝ゴールベース）、変化に柔軟に対応できるアジャイル型のガバナンス（＝アジャイル・ガバナンス）が求められる。
- そのためには、事業者の①「安全確保・維持のための取組」そのものと、これまで規制当局（あるいは権限委譲された機関）が実施していた取組の適切性の確認や是正等の②「ガバナンス」は、互いに情報共有しながら、それぞれ「定期」ではなく「状況の変化に合わせて都度」行う必要がある。
- スマート安全PJでは、①②から構成される「安全・ガバナンス」についてアーキテクチャのビジョン検討及び構成要素の具体化を実施した。下図に示す3層目の安全確保の手段を単に人からデジタル技術に置き換えることだけでなく、Society5.0に適した安全確保の在り方を考慮してガバナンスの本質的な変革を行うこと目指す。



取組の全体像（初年度の目的と成果の骨子）

- 初年度の目的として、成果を発信することでSociety5.0における安全・ガバナンスに係る課題意識及び未来像を共有し、示したアーキテクチャのビジョンを実践するためにステークホルダーとの連携体制を構築することを掲げ、以下に取り組んだ。
- 我が国の現行ガバナンスの課題分析、先行事例（自動運転、医療機器等の他の産業分野）調査を踏まえて、Society5.0に向けて安全・ガバナンスはどのように変化すべきかを捉えた（第2章）。その上で、Society5.0における安全・ガバナンスのアーキテクチャのビジョンを共有し（第3章）、その実装に向けてDADCの今後の進め方、アクションプランを共有・提案した（第4章）。



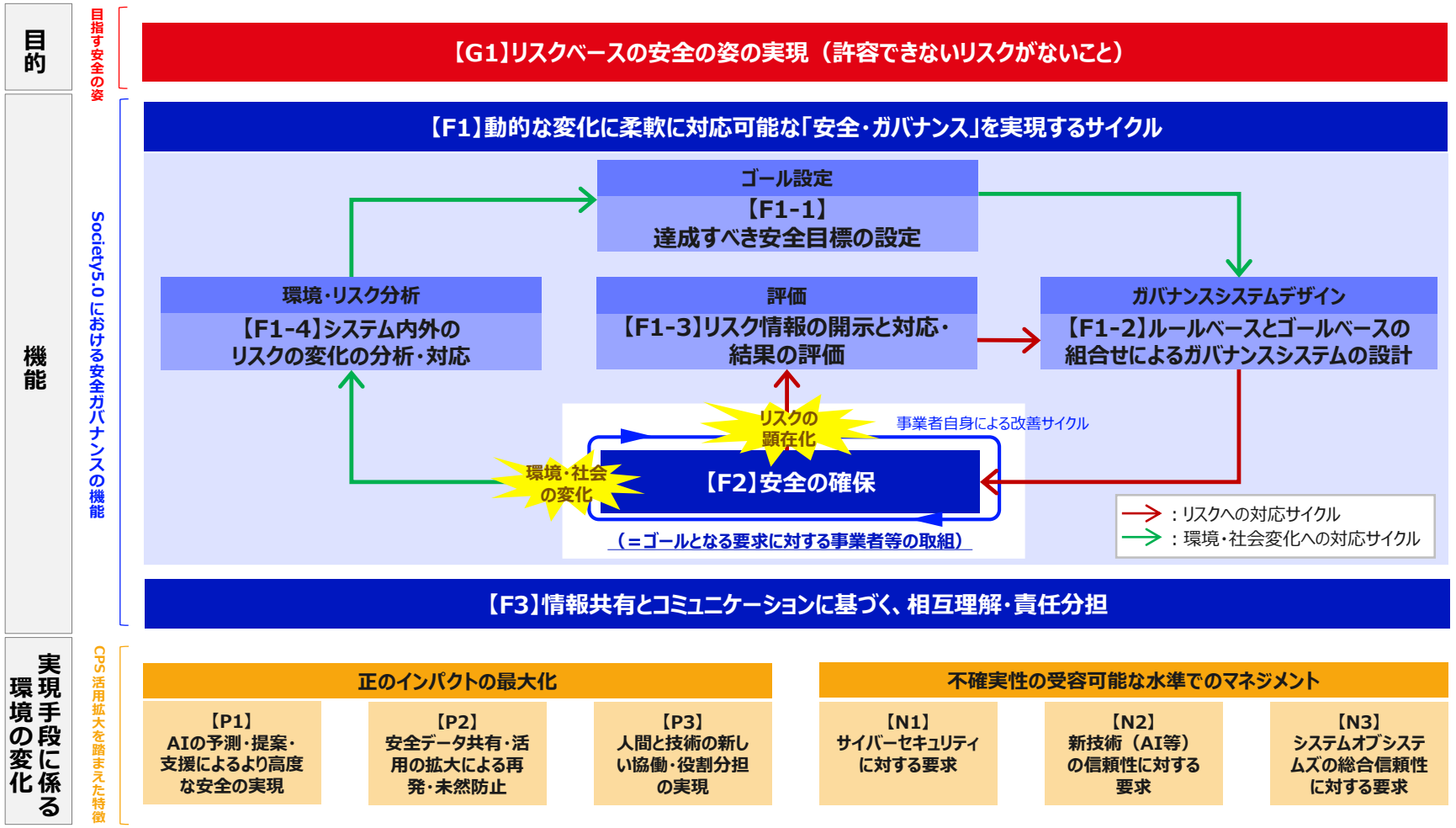
課題・論点を踏まえ捉えるべき変化（報告書2.2～2.4章）

- プラント保安分野をユースケースとした机上調査（高圧ガス保安法についてアーキテクチャ分析等を実施）及び、分野横断的なヒアリング調査（安全に係る学識者、プラント分野、自動車産業、電気産業等の事業者（安全管理、DX担当者）等から合計30名程度を対象にした個別/合同ヒアリングを基に意見の構造化を実施）を通し、日本の安全・ガバナンスに係る課題の構造化を実施した。
- 技術・分野別調査結果より、先進技術による安全に係る課題を整理した。その整理を基に、安全性向上が望める部分がある反面、技術によって新たなリスクが生じることや、そのリスクへの対応に対する課題、その課題への対応に必要となる安全・ガバナンスのビジョンの方向性（下図参照）を考察した。

	日本の安全・ガバナンスの現状の課題	先進技術による安全に係る課題	分野横断的な安全・ガバナンスのビジョン
安全の考え方	絶対安全思想/ゼロリスク志向により、新技術活用や事業者のより高度な安全を実現するための**自主的な取組が停滞**	高度化するシステム（CPS）に対してはAIやリアルタイムデータ活用等の**先進技術による高度な安全確保の実施が合理的**	先進技術活用のベネフィットを享受するために、リスクの存在を認め共生することが前提に **➡【G1】リスクベースの安全の姿の実現**
法制度・ガバナンス	技術革新や繋がるシステムによるリスク変化等を鑑みず、（単体システムに対する）**一律の安全レベルを要求する硬直的なガバナンス**	技術・システムの継続的な変化と法整備の**スピード・考慮事項の違いによる法規制の穴の存在**	技術・システムに係るリスクの変化への柔軟な対応をシステム全体として運用中も行えるガバナンスが必要に **➡【F1】動的な変化に柔軟に対応可能な「安全・ガバナンス」を実現するサイクル**
組織・技術・設備の管理	危険事象の再発防止の徹底により、問題発生の度に追加され**複雑化した手段を縛る安全規制**	AI等の新技術やサイバー空間との接続により、**事前にリスクを特定することや、リスク管理方法を予め規定することが困難に**	リスク・社会変化に合わせて合理的に安全を達成できるよう、ゴールベースとルールベースの組合せによるガバナンスシステムとそれに応じた事業者役割が必要に **➡【F2】安全の確保**
相互理解・説明責任	多様なステークホルダーに対してリスクに係る説明責任を果たすことによる**合意形成の仕組みの欠如**	ステークホルダー間の情報共有や危険事象発生時の責任の在り方を考慮した**社会的受容性の確立が必要**	新技術のリスクに対してステークホルダーとの相互理解と責任分担を行う機能が必要に **➡【F3】情報共有とコミュニケーションに基づく、相互理解・責任分担**

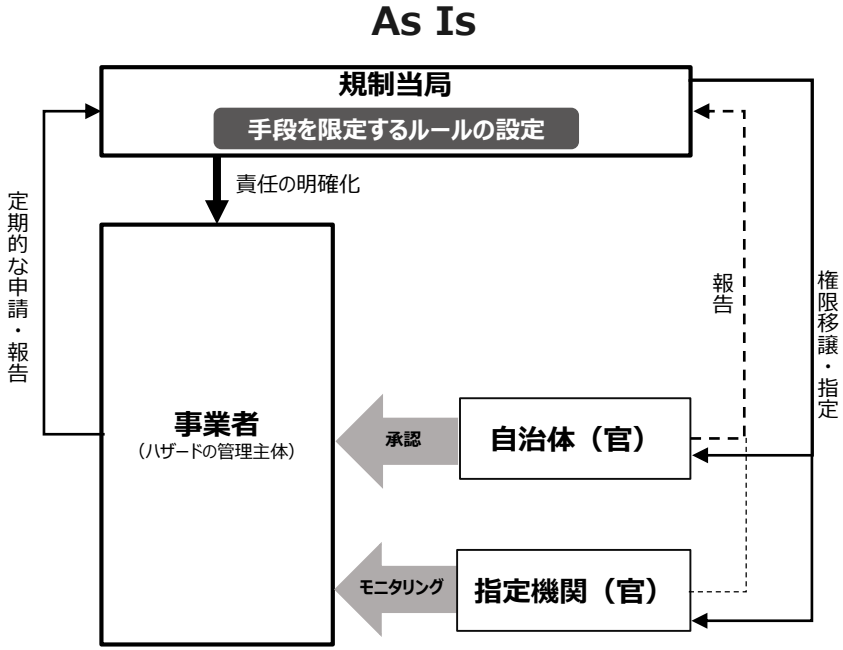
安全・ガバナンスのアーキテクチャのビジョン（報告書3章）

- 経済産業省「GOVERNANCE INNOVATION VER.2: アジャイル・ガバナンスのデザインと実装に向けて」で提唱されている、「ゴール設定」「システムデザイン」「運用（＝図中「安全を確保する機能」）」「説明」「評価」「改善」といったサイクルを多様なステークホルダーで継続的かつ高速に回転させるアジャイル・ガバナンスについて、安全に特化した切り口でガバナンスの構成要素のそれぞれを複数の分野に汎用的に適用できるよう具体化を実施した。
- Society5.0における安全・ガバナンスのアーキテクチャは、目的である「リスクベースの安全の実現」と、実現手段となるCPSの特徴を考慮したガバナンスの目的である「正のインパクトの最大化」及び「不確実性の受容可能な水準でのマネジメント」を実現するための機能設計が必要ではないか。

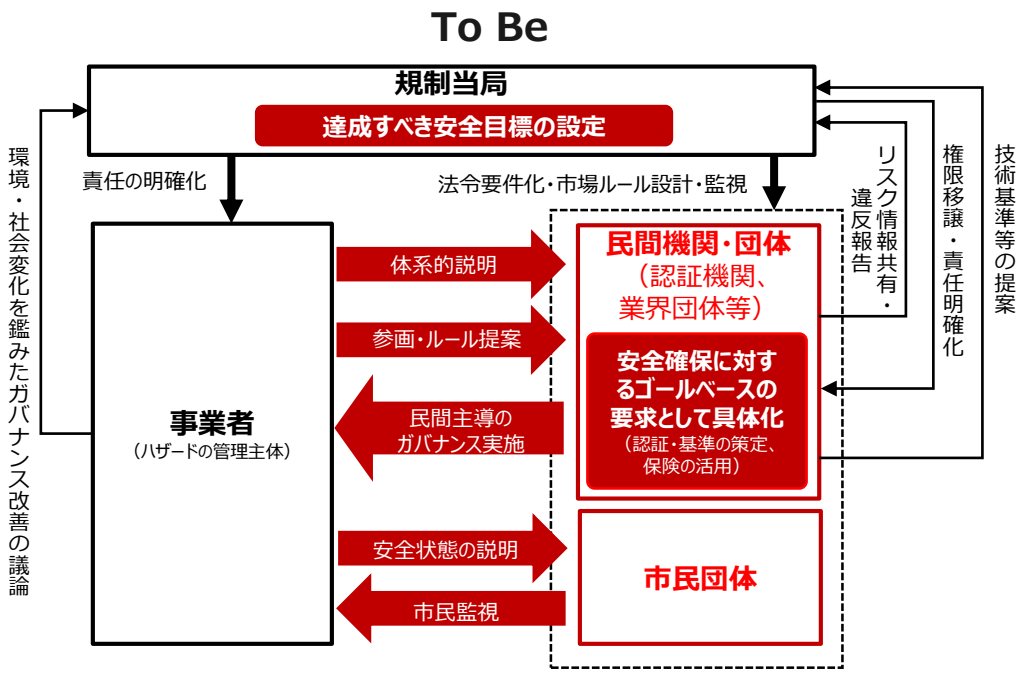


安全・ガバナンスのアーキテクチャのビジョン（報告書3章）
－F1：動的な変化に柔軟に対応可能な「安全・ガバナンス」を実現するサイクル－

- Society5.0における先進技術活用のベネフィットを享受・活用するためには、残留リスクの存在を認め受容・共生することが前提となる。その際、安全とは危険が一切存在しないという絶対安全思想を前提とし、社会的なリスクの顕在化時には説明責任が政府に強く求められ、再発防止の徹底に傾注しがちであった従来のガバナンスから、リスクベースの安全を志向したうえで、ガバナンスの在り方を設計する必要がある。
- 柔軟な修正が困難な手段や行為を制限する法規制から、リスクや社会の変化に応じて事業者が合理的に安全を達成できるよう、「安全確保に対するゴールベースの要求」をルールとして実装する必要がある。（下図イメージ）
  - ✓ 「定期的な目視検査を実施することを要求する」ルールベースから、「リスクに基づく管理を適切に行うことを要求する」ゴールベースの法規制とし、**事業者の裁量を拡大**
  - ✓ ガバナンスシステムにおける各民間企業が健全に機能を果たしていることを国が裏支え・監視する機能（リスク情報の真正性を評価する第三者機関認定等）を担い、リアルタイムデータ等を活用したリスクアセスメントを可能とすることで、**より迅速な改善サイクルを回す仕組み**に
  - ✓ ルール設計の段階から民間事業者が関与することで、民間事業者の持つ**先進技術に係る知見・ノウハウを効果的にルールに組込む**ことが可能に
- さらに、変化し続ける技術や社会システムのリスクについて柔軟に対応し、常に変化に応じて設定したゴールを見直していくことが求められるため、「動的な変化に柔軟に対応できるガバナンス」が必要となる（前頁のF1参照）。



組織の役割分担（イメージ）



組織の役割分担（イメージ）

安全・ガバナンスのアーキテクチャのビジョン（報告書3章）
－F2：安全の確保－

- 危険事象が発生した際の事象の進展シナリオは、従来のフィジカルシステムによる影響が中心的に検討されていたシナリオから、サイバーシステムによる波及影響の割合が拡大することとなる。そのため、CPSにおいて想定すべき危険事象のシナリオ及びその影響を低減するための方策は、従来のフィジカルシステムとは大きく異なることを前提とする必要がある。
- CPSの安全を実現する機能として、①CPS全体及び構成要素の安全度合いを評価する機能（下図の【A】、【B】、【C】）と②アカウンタビリティを果たすための機能（下図【D】）、③コンテクストの変化を捉え対応するための機能（下図の【E】）の3点に着目した。

課題：CPSではこれまで危険とみなされていないものが危険源（unknown）となる
・他システム（別の事業者のシステム）からの異常/正常な動作までもが、自システムに影響しうる
・物理システムをサイバー空間でつなげることで、サイバー空間からのセキュリティの問題が物理システムの安全に影響しうる
等

CPS/SoSとして繋がると、従来のロジックが通用しない。そこで…

危険源に対するリスク対応のための機能

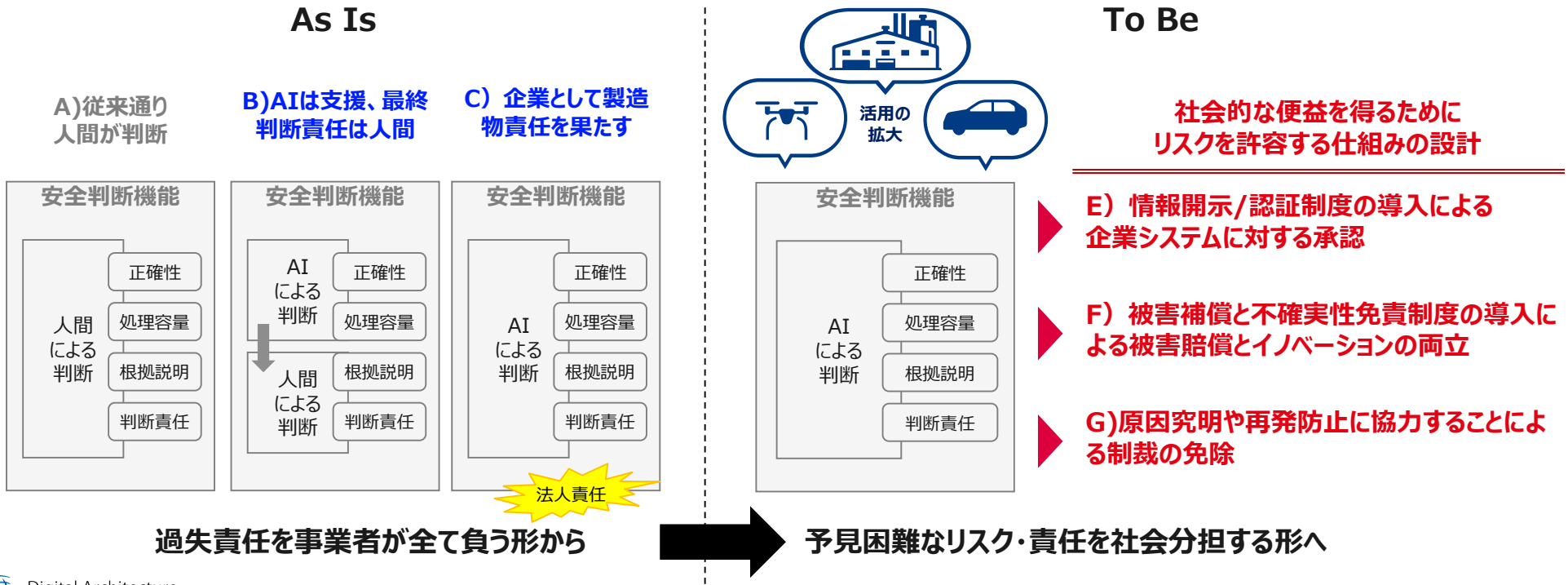
設計段階	①危険事象シナリオの特定・リスク評価・対策	● 新技術活用によるサイバーからの影響や他システムからの影響があると、危険事象シナリオの特定が困難となる。さらに自システムが他システムに与える影響が分からず、リスクの評価が単一システムではできない。 ⇒【A】複数システム間の関係性・波及影響を評価する機能、 【B】新技術要素（AI等）の信頼性を評価する機能の検討の必要性
	②安全防御の設計・対策	● ①の危険事象シナリオの特定・リスク評価ができないと、効果的な防御層の設計が困難となる。特にサイバーからのセキュリティの問題が物理システムの安全に影響し得るため、サイバー空間からの影響を考慮することが重要に。 ⇒【C】サイバーセキュリティの信頼性と防護機能を評価する機能の検討の必要性
	③意思決定とアカウンタビリティへの対応	● アカウンタビリティは、単一システム及びその管理主体のみでは対応しきれないこととなる。さらに、繋がることで単一システムのアカウンタビリティを果たすことも困難となる。 ⇒【D】CPSにおけるアカウンタビリティを果たすための機能の検討の必要性
危険事象		
運用段階	④緊急時対応による被害の局限化	● システムが繋がることで単一システムだけでは危険事象発生の際の被害の大きさを予測することが困難となり、各システムの管理主体のみではシステム内外の変化に対応することや被害の拡大を抑制することができない。 ⇒【E】コンテクストの変化を捉え、対応するための機能の検討の必要性

※上記A～Eはあくまで2020年度に着眼したポイント及び仮説であり、今後更なる検証を行い、その他の論点も継続して検討する

安全・ガバナンスのアーキテクチャのビジョン（報告書3章）
－F3:情報共有とコミュニケーションに基づく、合意形成・責任分担－

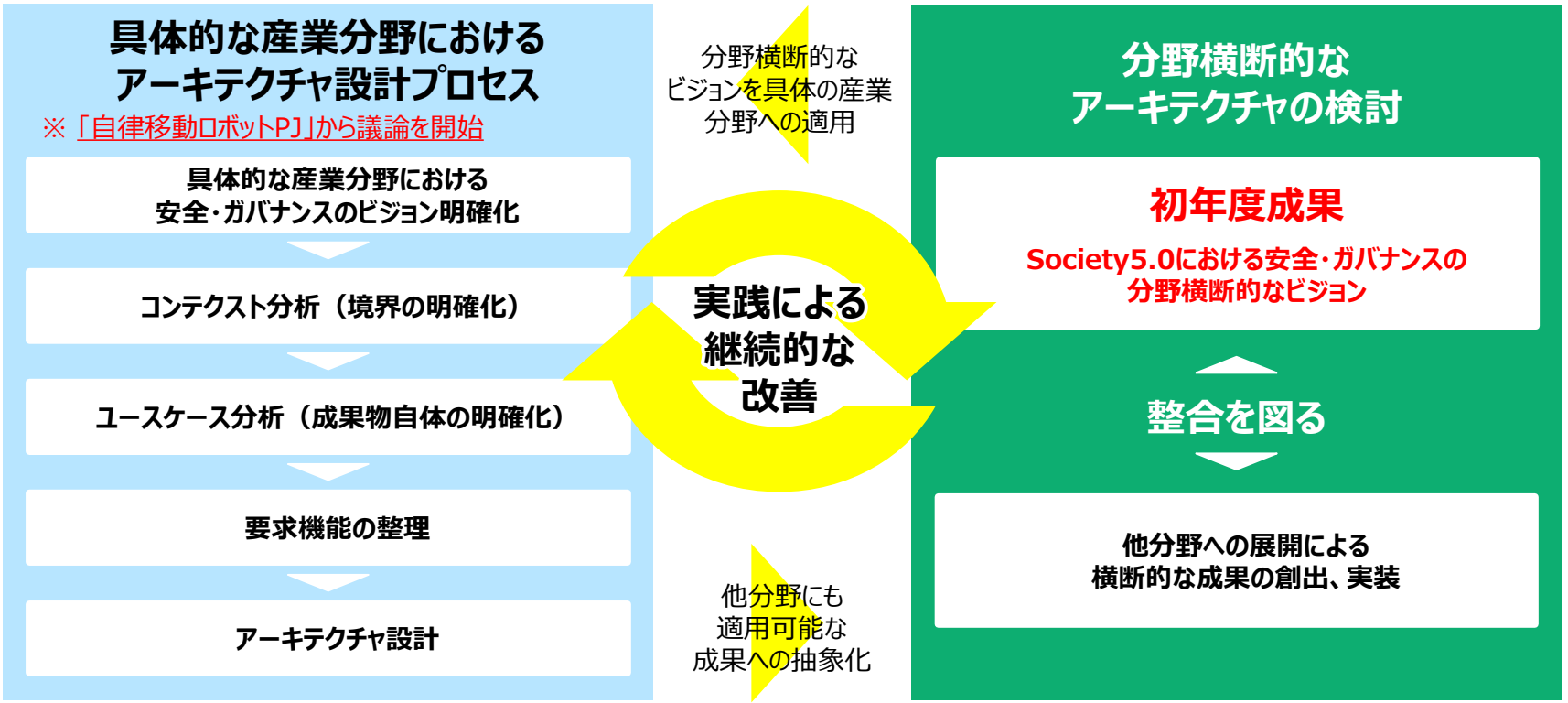
- 新技術は安全面に関しても不確実性を持ち得るものであるが、新技術によるベネフィットを社会的に享受するためには、不確実なもの全てを否定するのではなく、それらを適正に評価して社会実装を進めることが必要である。つまり、AI等に代表される不確実性を完全に排除できない新たな技術の導入のためには、社会全体でその不確実性を認識し、許容し、責任を分担するための仕組みを設計していくことが重要となる。
- 例えば、認証制度・制裁制度を背景とする事業者（群）による適切なリスクマネジメントの担保と、被害救済制度の導入などを含めて、社会的なリスク分担のあり方の検討が必要となる。下図の整理を有識者との議論に基づきDADCにおける仮説として検討しており、今後、具体的な分野での実践を通し検証していく予定。
- 社会全体での安全の実現のためには、不具合データの蓄積・共有が必要であり、失敗経験を社会に還元すること、再発防止に協力することによる制裁の免除（※）等、法律、社会規範の柔軟な改革が求められる。また、安全性を守ることへの社会的受容性の担保や安全教育も必要となる。※ 訴追延期合意といい、事故が生じた場合に、情報提供と損害賠償を行い、合理的なリスクの発現に過ぎないことを証明するか、製品・開発体制の改善を約束する場合には、検察官が訴追を延期することを合意する仕組みを組み込んでいくことが専門家間で議論されている

※参考）JSTニュース 2019年5月 https://www.jst.go.jp/pr/jst-news/backnumber/2019/201905/pdf/2019_05_p08-11.pdf



今後の進め方（報告書4章）

- 具体的な産業分野/ユースケースにおけるアーキテクチャ設計を通し、初年度の成果であるSociety5.0における安全・ガバナンスのアーキテクチャの分野横断的なビジョンの検証・改善を実施し、さらに、分野横断的なビジョンの改善及びリファレンスアーキテクチャ/アーキテクチャフレームワークの開発を目指す。
- 初年度の活動を通じて得られた以下2点の示唆を踏まえ、今後の取組を進めていく。
  - ✓ 国内の足下の課題から着手し、積み重ねられた安全に係る考え方を含むシステムをどうSociety5.0に適したものにしていくのか、システムのCPS化した姿を具体化したうえで、新たな安全・ガバナンスの実装・転換の在り方を検討することがポイント。
  - ✓ 新興の産業分野・ビジネス（よりオープンに進化的につながるシステム）を主な対象として、安全を競争力に繋げるための安全評価の仕組み・仕掛けの提案が重要。
- まずは、DADCで推進されているPJ（自律移動システム等）を事例とし、安全に特化したガバナンスのアーキテクチャについて検討を継続する。平行して、様々な分野で実用可能な成果を発信していくために、実践（適用・検証）すべき適切な複数の具体分野を特定する。



【参考】Society5.0における安全・ガバナンスのイメージ（1/2）

- 提案したアーキテクチャのビジョンに基づくガバナンス機能を実装した場合に、具体的にどのようなガバナンスモデルになるかというイメージをプラント分野をユースケースとして検討し、各産業分野のステークホルダーが実装に向けたイメージを持ちやすくするための考え方や具体事例を提示した。（次頁参照）
- 提案する官民連携のガバナンス（リスクベースの安全の志向、安全確保に対するゴールベースの要求、アジャイルガバナンス）を実装するためには、民間主導のルール設計や認証機能（ゴールを達成しているか適合性評価を実施する等）を担う組織が必要となる。
- 他方で、現状の我が国では、そのような能力・スキルを持つ主体が不足しており、その機能をどの様に社会的に実装していくかが課題となることが本分析を通して示唆として得られた。

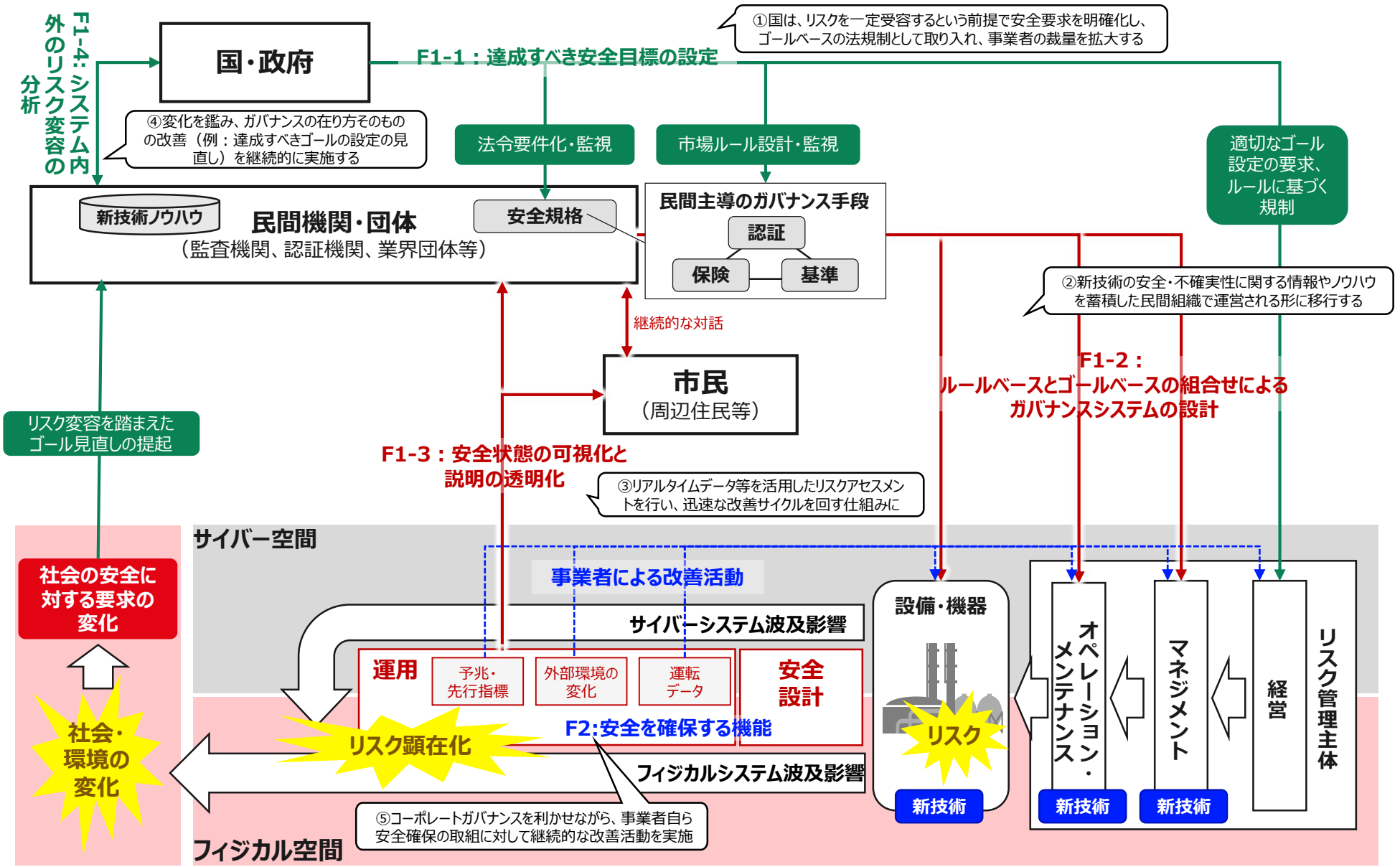
✓ 欧米の認証機関の担う機能のアーキテクチャ分析から抽出された以下の機能をどう解釈し、リスク分配や責任分担と併せて我が国のいずれの主体にその機能を割り当てることができるのかを検討する必要がある。

① 認証する機能
② 地域横断的・分野横断的な知見を獲得する機能
③ 技術支援により知見を事業者へ展開する機能
④ （認証機関自身の）技術支援力を強化する機能
⑤ 規格を開発する機能
⑥ 作成した規格を普及する機能
⑦ 技術的な信頼を獲得する機能　等

✓ そのためには、例えば以下が今後の検討課題であると考えられる。

① 社会制度の設計：権限の付与の在り方や基盤となる仕組み・ルールの設計
② 社会的な能力強化：類似の機能を持つ既存の組織の能力強化や新たな機関創出・人材育成
③ ビジネス・エコシステムの形成：認証・規格・保険を組み合わせにより民間主導のガバナンスを回すをビジネスとして持続的にどう成り立たせることができるか

【参考】Society5.0における安全・ガバナンスのイメージ（2/2）



【参考】Society5.0における安全・ガバナンスのイメージ（2/2）解説

＜イメージ図（前頁）の解説＞

- ✓ 国は、当初設定した安全目標が達成されているかを確認する**ゴールベースの法規制を取り入れ**、第三者認証機関等を活用しながら**事業者の裁量を拡大**し、リスクや社会・技術の変化に応じて**事業者が合理的に安全を達成可能な形へと移行**する。（①:F1-1）
- ✓ 国を中心に、外部環境や外部システムの様々な状況変化（脅威の発生、脆弱性の変更、仕様の変更、など）を鑑み、ガバナンスの在り方そのものの改善（例：達成すべきゴールの設定の見直し）を継続的に実施する。（④：F1-4参照）
- ✓ ガバナンスを可能な限り、**新技術の安全・不確実性に関する情報やノウハウを蓄積した民間組織で運営される形に移行**することを目指す。民間組織で機能する構造とすることで動的な変化に柔軟に対応できるガバナンスモデルの構築・運用が可能となる。リスクに関わる様々な主体がともに互いの活動や情報を確認し、それに応じてガバナンスを構成する要員として主体的に活動することが望まれる。**市民も「安全の達成状況の可視化・説明の透明化」を通して公開される情報に基づきガバナンスに関与する役割を担う**。（②:F1-2参照）
- ✓ ガバナンスシステムにおける**各民間企業が健全に機能を果たしていることを国が裏支え・監視する機能**（リスク情報の真正性を評価する第三者機関認定等）を担い、リアルタイムデータ等を活用したリスクアセスメントを可能とすることで、**迅速な改善サイクルを回す仕組み**となる。（③:F1-3参照）
- ✓ リスク管理主体である事業者は、**コーポレートガバナンスを利かせながら、事業者自ら安全確保の取組に対して継続的な改善活動を実施**する。（⑤：F2を参照）