資料１－１

一部非公開・関係者限り

BCG BOSTON CONSULTING GROUP

令和６年度 シンクタンク機能育成事業の進捗報告

事業項目① 調査研究

安全・安心シンクタンク運営ボード

令和7年 (2025年) 3月17日

内閣府 Cabinet Office

R6/7年度「調査事業」プロジェクト概要

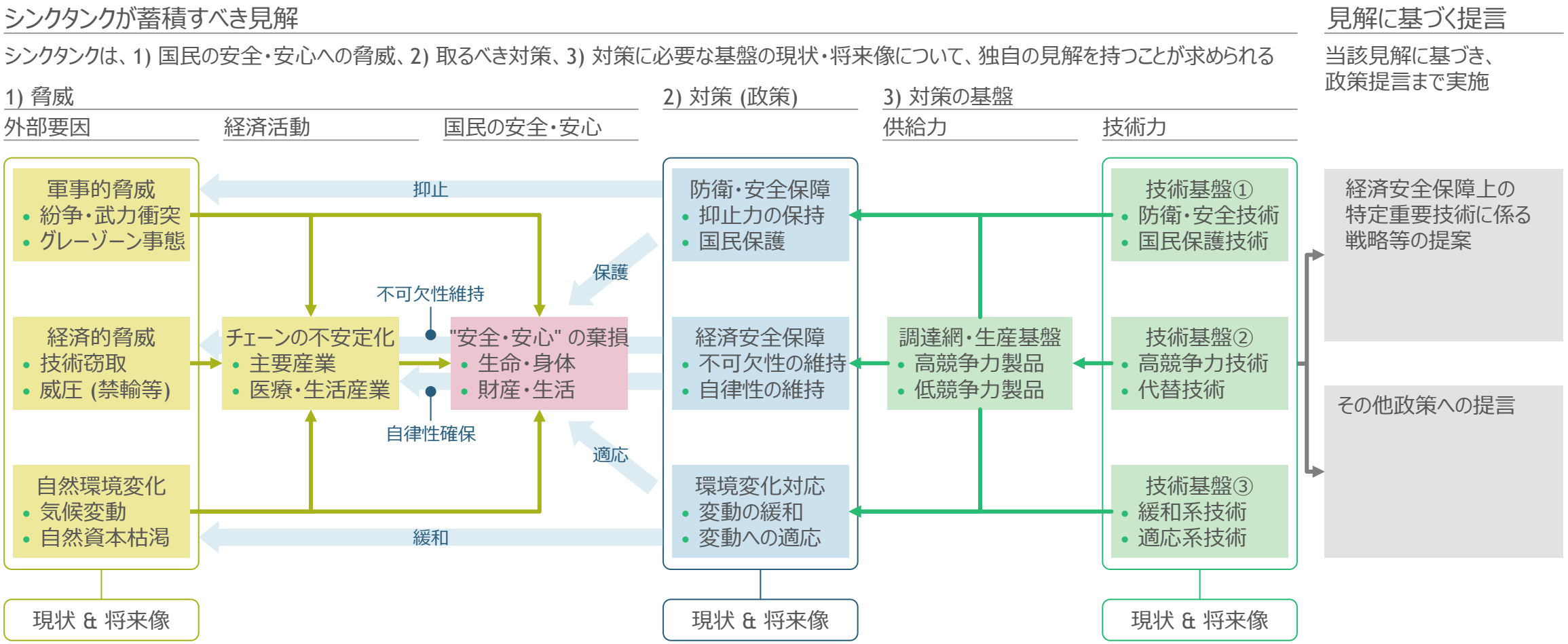
A 「安全・安心シンクタンク」の果たすべき役割と本調査の位置付け

B R6/7年度「調査事業」のプロジェクト設計

- 01 成果物及び調査アプローチ
- 02 関係者及び役割分担
- 03 調査スケジュール
- 04 現時点調査概要

安全・安心シンクタンクは、脅威・対策・技術の3点に独自の見解を持ち、政府に対して、重要技術の研究開発・成果活用に有用な提言等を行う役割を期待されている

「安全・安心シンクタンク」の果たすべき役割 (1/2)



本調査は、シンクタンクの果たすべき役割も踏まえた準備活動・試行的かつ先行的な調査に該当、その知見、並びに手法論を活かすことでスムーズな立ち上げを実現

R6/7年度調査事業の実施項目

R6年度	R7年度	R8年度 (立上げ後) 以降
準備段階としての活動		立上げ後の活動
R6 試行・先行調査	**R7 試行・先行調査**	**承継作業**
• 広範囲調査分析[1)] • 個別調査分析[2)] - 国内外需要動向調査 - 国内外の技術動向調査 - 国際情勢分析 - 統合需給/シナリオ分析（調査・分析手法の開発・検討を含む） [各技術のOCA[3)]分析と、初期的な打ち手の整理]	• 広範囲調査分析 **[発展/精緻化]** • 個別調査分析 **[発展/精緻化]** - 国内外需要動向調査 - 国内外の技術動向調査 - 国際情勢分析 - 統合需給/シナリオ分析（調査・分析手法の開発・検討を含む）**[上記を踏まえ育成アプローチ/アウトプット目標の分析等を精緻化]**	• R6・R7 先行調査の成果物の整理・アーカイブ • 調査・分析手法の承継

本格調査
(経済安全保障上の特定重要技術に係る戦略の提案等)

① **土台としての知見 [発射台]**
- 情報を更新すれば、シンクタンクの事業として先述のミッションを果たすことができる**土台**として活用する **[① 見解の仮説]**

② **依拠できる手法論**
- ① の土台を、どのように更新すればよいか、確立された方法で活動する **[② 分析結果/手法詳細]**

1.特定の分野について、脅威、政策動向、国際情勢等の調査による現在/将来の政策課題・ニーズの明確化、それらの解決等につながり得る技術シーズの特定・動向調査、技術のインパクト評価や経済安全保障の観点も含めた重要度評価、政策オプションの検討・提案
2.幅広い技術領域における新興技術等について、国内外の最新の研究開発動向等の俯瞰的かつ体系的な情報収集・整理・評価等
3. "Own"、"Collaborate"、"Access" の略であり、技術確保に関して、自国で保有するか、他国と連携するか、他国の技術にアクセスしにいくか、という技術確保に必要なアクション

R6/7年度「調査事業」プロジェクト概要

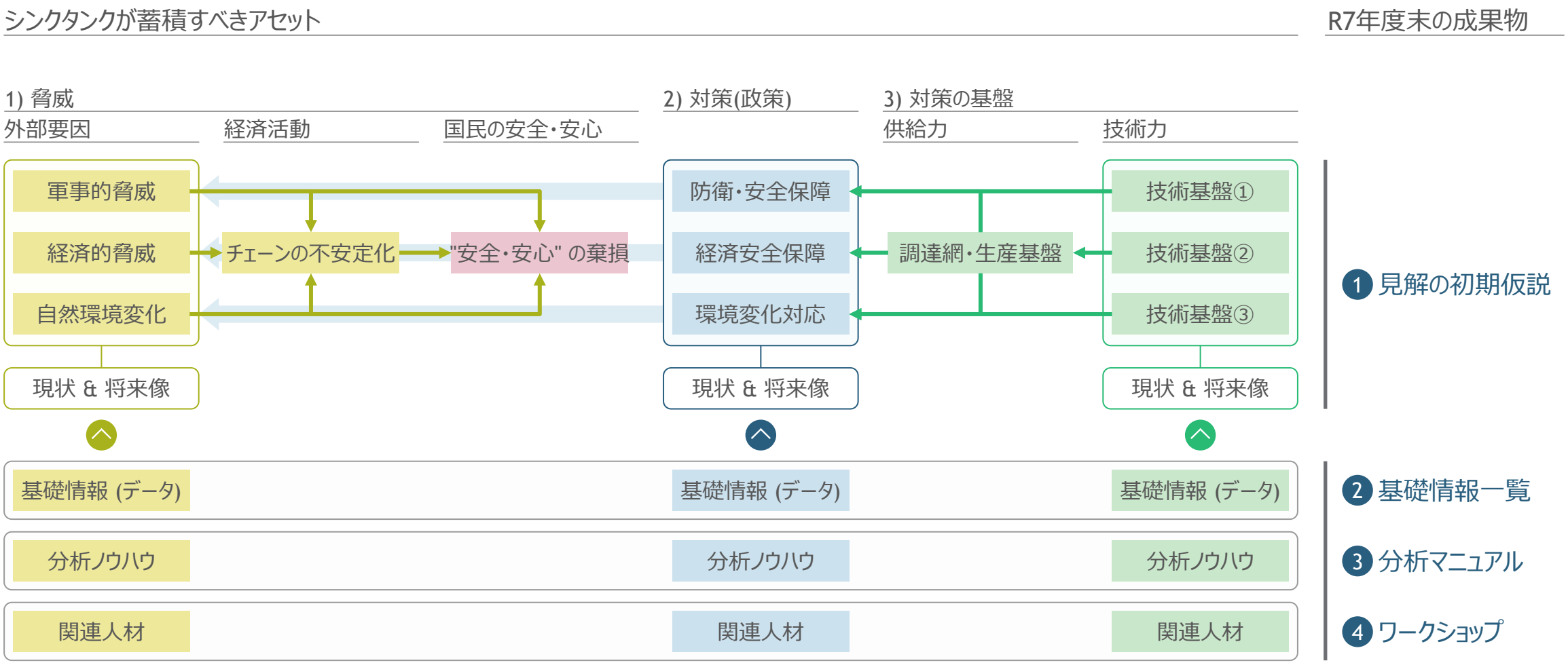
A 「安全・安心シンクタンク」の果たすべき役割と本調査の位置付け

B R6/7年度「調査事業」のプロジェクト設計

- 01 成果物及び調査アプローチ
- 02 関係者及び役割分担
- 03 調査スケジュール
- 04 現時点調査概要

R6/7年度の調査事業では、脅威・対策・技術についてシンクタンクに引き継げる初期仮説とそれを得るために用いた基礎情報、分析手法を整理、ワークショップで若手人材を巻き込む

R6/7年度調査事業の成果物



本調査ではⅠ現在の脅威の動向・政策課題から出発し、Ⅱ将来トレンドを踏まえた脅威のシナリオ及びⅢ注目を集める最先端技術を踏まえ、Ⅳ今後必要となる政策とそれに活用できる技術を整理し、Ⅴ我が国の「安全・安心」確保に向けた重要技術戦略を取りまとめ

調査プロセスの全体像 (1/2)

Ⅰ 脅威の現状・脅威に対する政策課題・対策ニーズの現状

分析ソース/インプット

- 各国政策文章・シンクタンク論考 等
- エキスパートヒアリング

×

Ⅱ 国際情勢のトレンドを踏まえた脅威の将来シナリオ

分析ソース/インプット

- シンクタンク論考 等
- エキスパートヒアリング

Ⅲ 本領域における注目技術の特定・各技術に関する我が国の競争優位性

分析ソース/インプット

- 論文・書誌情報、特許情報
- エキスパートヒアリング

Ⅳ 想定される脅威に対する政策課題の解決に活用し得る技術

分析ソース/インプット

- Ⅰ Ⅱ Ⅲ 検討内容
- エキスパートヒアリング

Ⅴ 5-10年後以降の脅威に向け必要な重要技術戦略

分析ソース/インプット

- Ⅰ Ⅱ Ⅲ Ⅳ 検討内容
- 既存政策・研究開発事業等に関する文献
- エキスパートヒアリング

サイバーセキュリティ、AI、量子、食料安全保障、エネルギーの5テーマを対象に、以下の15項目に沿って具体的な調査・分析を試行的に実施

調査プロセスの全体像 (2/2)

1. "Own"、"Collaborate"、"Access" の略であり、技術確保に関して、自国で保有するか、他国と連携するか、他国の技術にアクセスしにいくか、という技術確保に必要なアクション

各注目技術の競争優位性と脅威・社会課題への活用可能性 (=重要度) から、技術確保の方向性を策定

技術の確保に必要なアクション (OCA – Own、Collaborate、Access) の分類に関する考え方

Own

研究開発から社会実装・商業化に至るまで、我が国が一貫して主導的な役割を担い、高い自律性を確保

- 軍事・経済的な重要度が極めて高く、我が国として戦略的自律性や不可欠性を確保しておくべき技術、又は、重要度が一定程度高く、かつ、既に我が国が非常に高い競争優位性を有する技術へのアクション

Collaborate

我が国が支配的な地位を確立することは困難であるが、研究開発等における目標達成のため、他国と連携

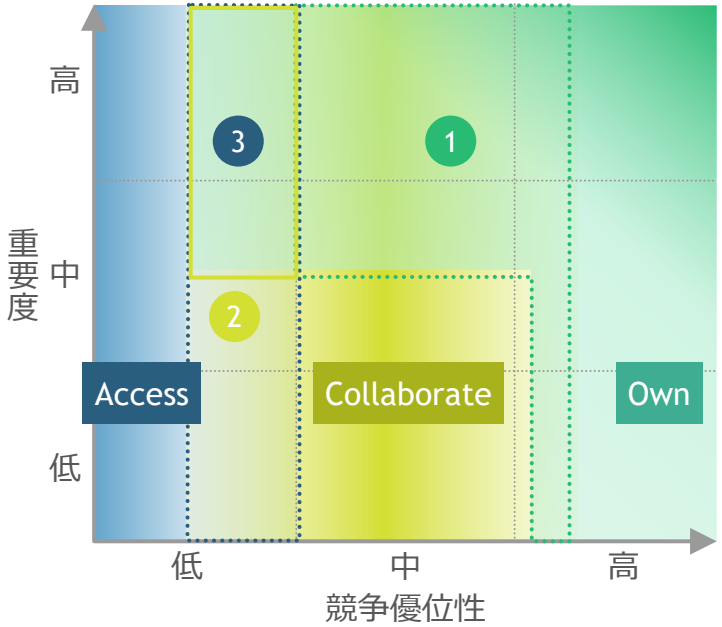
- 我が国が一定以上の競争優位性を有する技術であり、他国 (同盟・同志国等) との協働により、補完的・互恵的な形での研究開発等が可能な技術へのアクション

Access

取引やパートナーシップ等を通じて、他国から技術を獲得

- 我が国の競争優位性が低く、同盟・同志国が既に支配的な地位を確立している技術や、技術成熟度が高く、追加リソースに対して競争優位性の向上が見込めない技術へのアクション

重要度・競争優位性に基づいた大枠としての分類



技術毎の定性的な判断

- 重要度が高いものであっても、我が国として主導的・支配的役割を確立することが困難な場合には、OwnではなくCollaborateやAccessとなることがあり得る
- 我が国の競争優位性が低い場合であっても、非同盟・同志国が支配的地位を確立している場合には、同盟・同志国との協働 (Collaborate) を通じ、競争優位性の向上を図ることもあり得る

Source: UK Government. (2021). Defence and Security Industrial Strategy (DSIS): A strategic approach to the UK's defence and security industrial sectors.; BCG分析;

R6/7年度「調査事業」プロジェクト概要

A 「安全・安心シンクタンク」の果たすべき役割と本調査の位置付け

B R6/7年度「調査事業」のプロジェクト設計

- 01 成果物及び調査アプローチ
- 02 関係者及び役割分担
- 03 調査スケジュール
- 04 現時点調査概要

本事業の関係者及び役割分担の整理

(注) 敬称略

調査内容 (再掲)

広範囲調査分析

個別調査分析

- 国内外需要動向調査
- 国内外の技術動向調査
- 国際情勢分析
- 統合需給/シナリオ分析
  （調査・分析手法の開発・検討を含む）
  [各技術のOCA分析と、初期的な打ち手の整理]

実施者

内閣府 Cabinet Office

BCG

CRDS 研究開発戦略センター Center for Research and Development Strategy

「広範囲調査分析」を一部担当

中央大学

「個別調査分析」の一部調査を担当

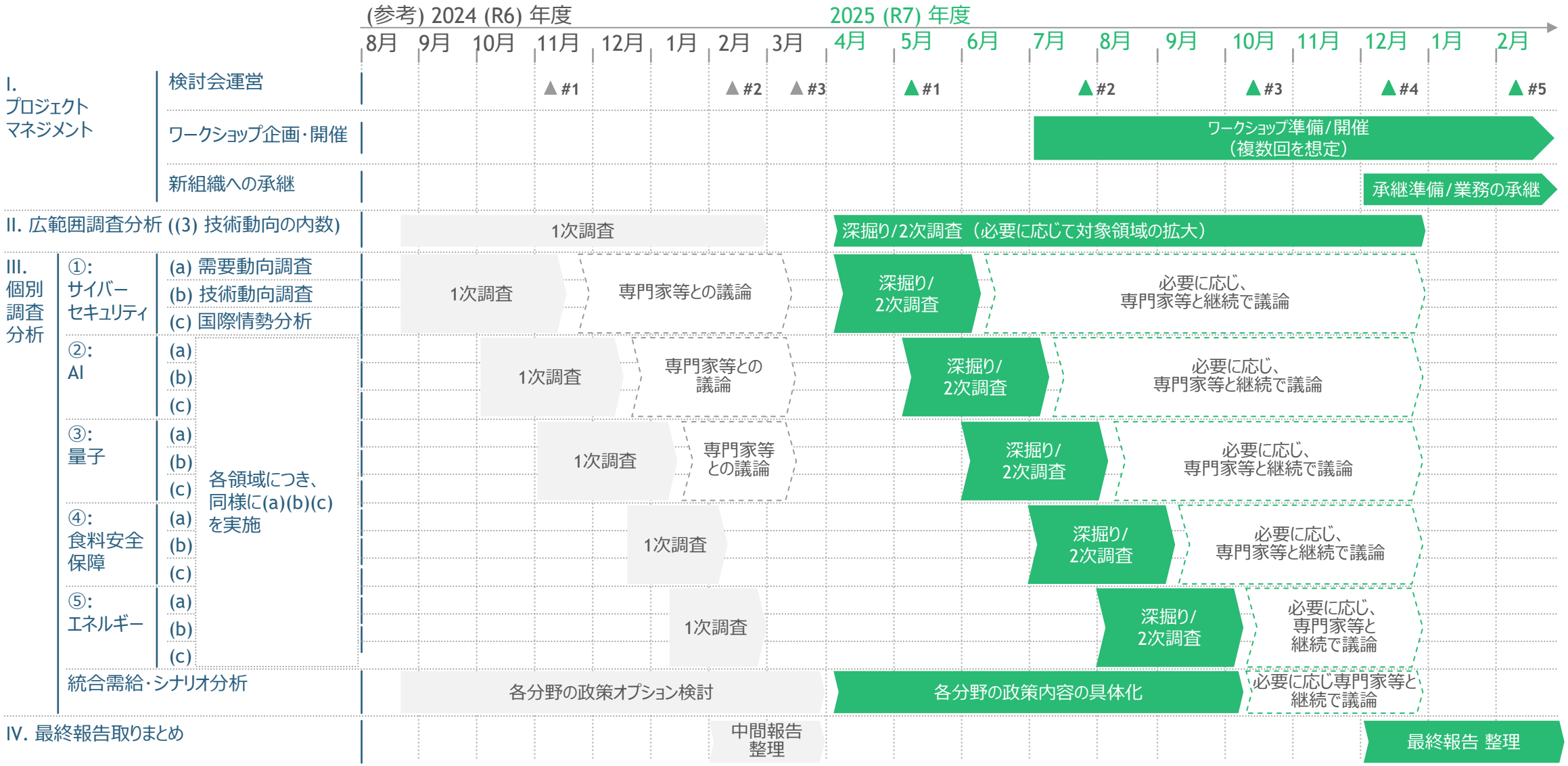
R6/7年度「調査事業」プロジェクト概要

A 「安全・安心シンクタンク」の果たすべき役割と本調査の位置付け

B R6/7年度「調査事業」のプロジェクト設計

- 01 成果物及び調査アプローチ
- 02 関係者及び役割分担
- 03 調査スケジュール
- 04 現時点調査概要

R7年度 事業実施計画 (現時点想定)



R6/7年度「調査事業」プロジェクト概要

A 「安全・安心シンクタンク」の果たすべき役割と本調査の位置付け

B R6/7年度「調査事業」のプロジェクト設計

- 01 成果物及び調査アプローチ
- 02 関係者及び役割分担
- 03 調査スケジュール
- 04 現時点調査概要

広範囲調査分析

CRDS 研究開発戦略センター
Center for Research and Development Strategy

国立研究開発法人科学技術振興機構

概要版

我が国における先端・重要な研究開発領域の特定に関する試行分析 中間報告書（2024年度）

2025年3月17日

JST研究開発戦略センター(CRDS)

調査方法（全体像）

(1) 対象分野の選定

- 調査対象の研究開発領域の選定
  - **129領域**
  - 内閣府指定の特定20領域との紐付け

(2) 対象分野の評価

- 論文、特許定量分析・スコア化
  - **論文**：論文数およびTop10%論文数のシェアをスコア化（1-5点）
  - **特許**：Patent Asset Index（PAI）のシェアをスコア化（1-5点）

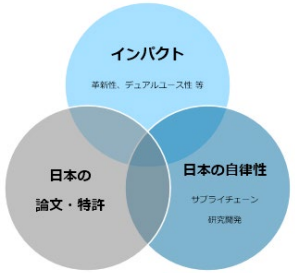
- 研究開発領域のインパクトを定性分析・スコア化
  - **革新性**　（1-5点）
  - **汎用性**　（1-5点）
  - **デュアルユース性**　（1-5点）
  - **公共性**　（1-5点）
  - **自律性**　（1-5点）

(3) ロングリストの作成

- 各分析項目のスコアで研究開発領域をスクリーニング
  - 論文・特許
  - 革新性
  - 汎用性
  - デュアルユース性
  - 公共性
  - 自律性

  各20領域程度

- 掛け合わせ分析



- リスト化（ロングリスト）

(4) 報告書

- 目次

1．調査概要
(1) 背景・目的
(2) 前回の取組概要と示唆
(3) 前回の取組での主な課題と対応
2．調査方法
(1) 対象分野の選定
(2) 対象分野の評価
(3) ロングリストの作成
3．諸外国の状況
4．調査結果
(1) 各評価項目の調査結果
(2) 集計結果
(3) 掛け合わせ分析
5．考察と今後の課題

参考資料
個票
参考文献

調査方法

論文・特許による評価

■ 論文データのスコア化

１．論文シェアの計算

- 対象： CRDSの定める129研究開発領域の全論文シェアおよびTop10%論文シェア
  - 全論文シェア：論文数÷当該領域論文数の合計
  - トップ10%論文シェア：Top10%論文数÷当該領域論文数の合計
- 対象期間： 2014年 - 2023年
- データソース：Elsevier

2 スコア付与の基準

- 全論文シェア及びトップ10%論文シェアについて、それぞれのデータの分布等を総合的に判断し、得点付与のシェア閾値を設定。

3 スコア計算及び集計

- １で算出した論文シェアを２の閾値に当てはめ、スコア化。

■ 特許データのスコア化

１．特許PAI値シェアの計算

- 対象： CRDSの定める129研究開発領域の特許のPAI値
- 各国の各領域の特許PAI値についてシェアを計算（ある国の～領域におけるPAI値÷全ての国の～領域におけるPAI合計値）。
- 対象期間： 2014年 - 2023年
- データソース：PatentSight

2 スコア付与の基準

- 1で算出したデータの分布等を総合的に判断し、得点付与のシェア閾値を設定。

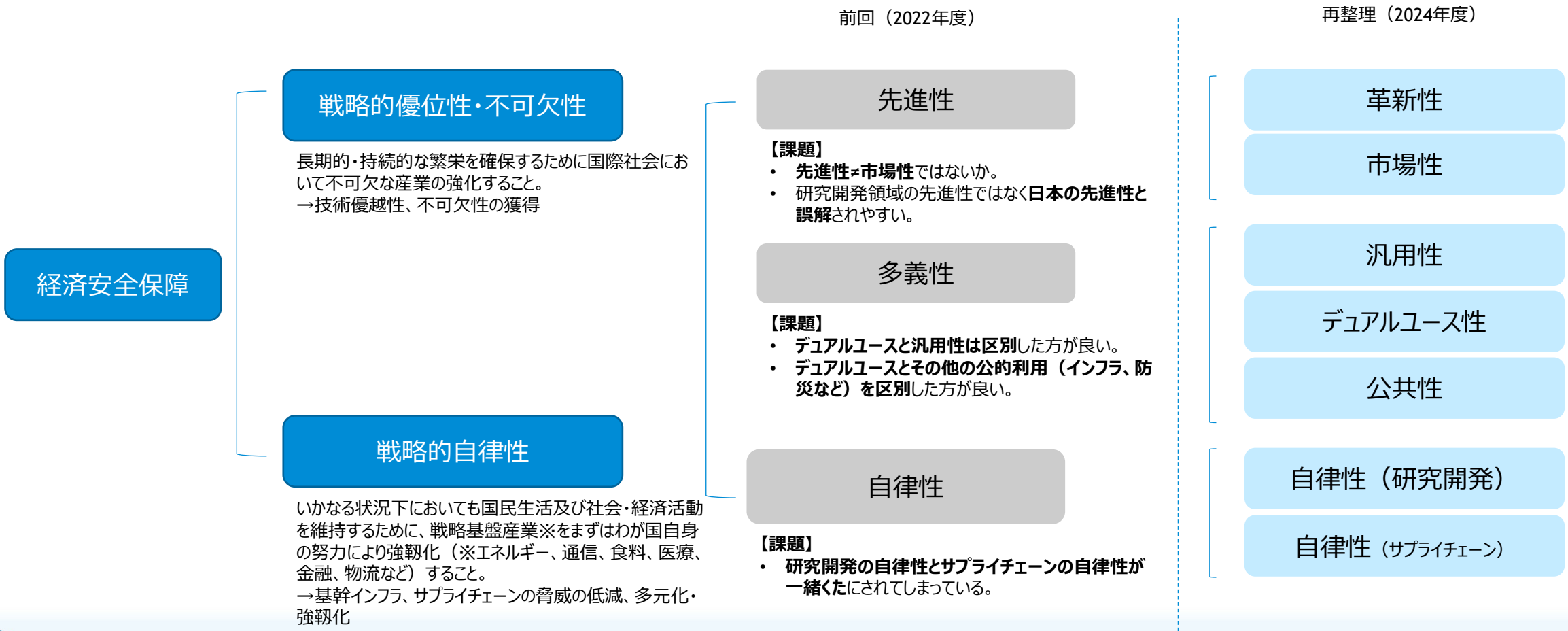
3 スコア計算及び集計

- １で算出した数値を２の閾値に当てはめ、スコア化。

調査方法

研究開発領域のインパクトに関する定性評価

- 2022年度は経済安全保障の目的を政策文書等から「戦略的優位性・不可欠性」「戦略的自律性」とし、それらに資する研究開発領域を検討するための評価観点として「先進性」「多義性」「自律性」を設定。
- 2022年度実施の際に出た課題から今般においては、以下7項目（「革新性」「市場性」「汎用性」「デュアルユース性」「公共性」「自律性（研究開発／サプライチェーン）」に再整理した。



調査方法

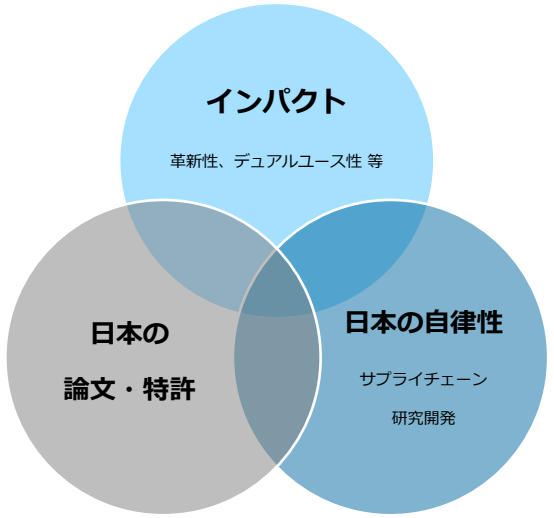
ロングリストの作成

- 論文、特許、インパクト評価で高い／低いスコアのもの20程度スクリーニングする。
- 日本の論文・特許、日本の自律性のスコアとインパクト評価のスコア掛け合わせ、ロングリストの作成を検討。

スクリーニング

論文・特許　スコアが高い	20領域程度
革新性　スコアが高い	20領域程度
汎用性　スコアが高い	20領域程度
デュアルユース性　スコアが高い	20領域程度
公共性　　スコアが高い	20領域程度
自律性（研究開発）　スコアが低い	20領域程度
自律性（サプライチェーン）　スコアが低い	20領域程度

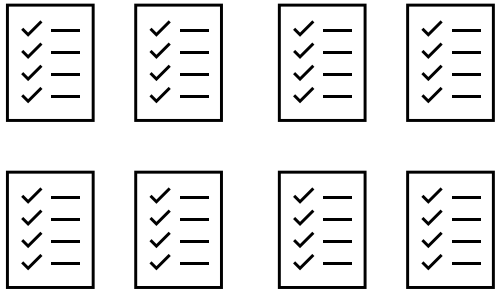
掛け合わせ分析



ロングリスト

（例）
日本の論文・特許　高 × インパクト　高
日本の自律性　低　　× インパクト　高

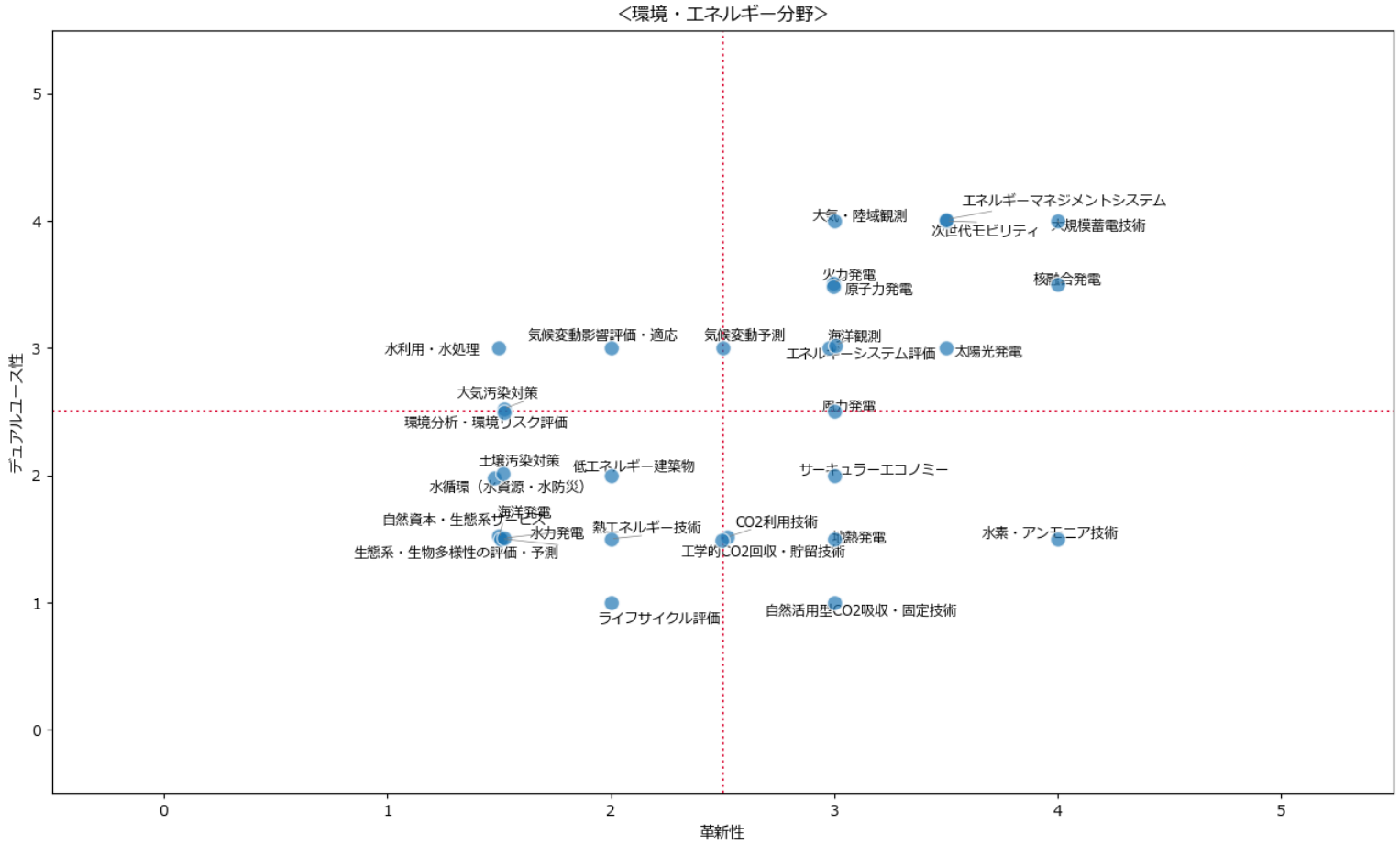
・研究開発領域 A
・研究開発領域 B
・研究開発領域 C ・・・・



調査結果

掛け合わせ分析（環境・エネルギー分野）

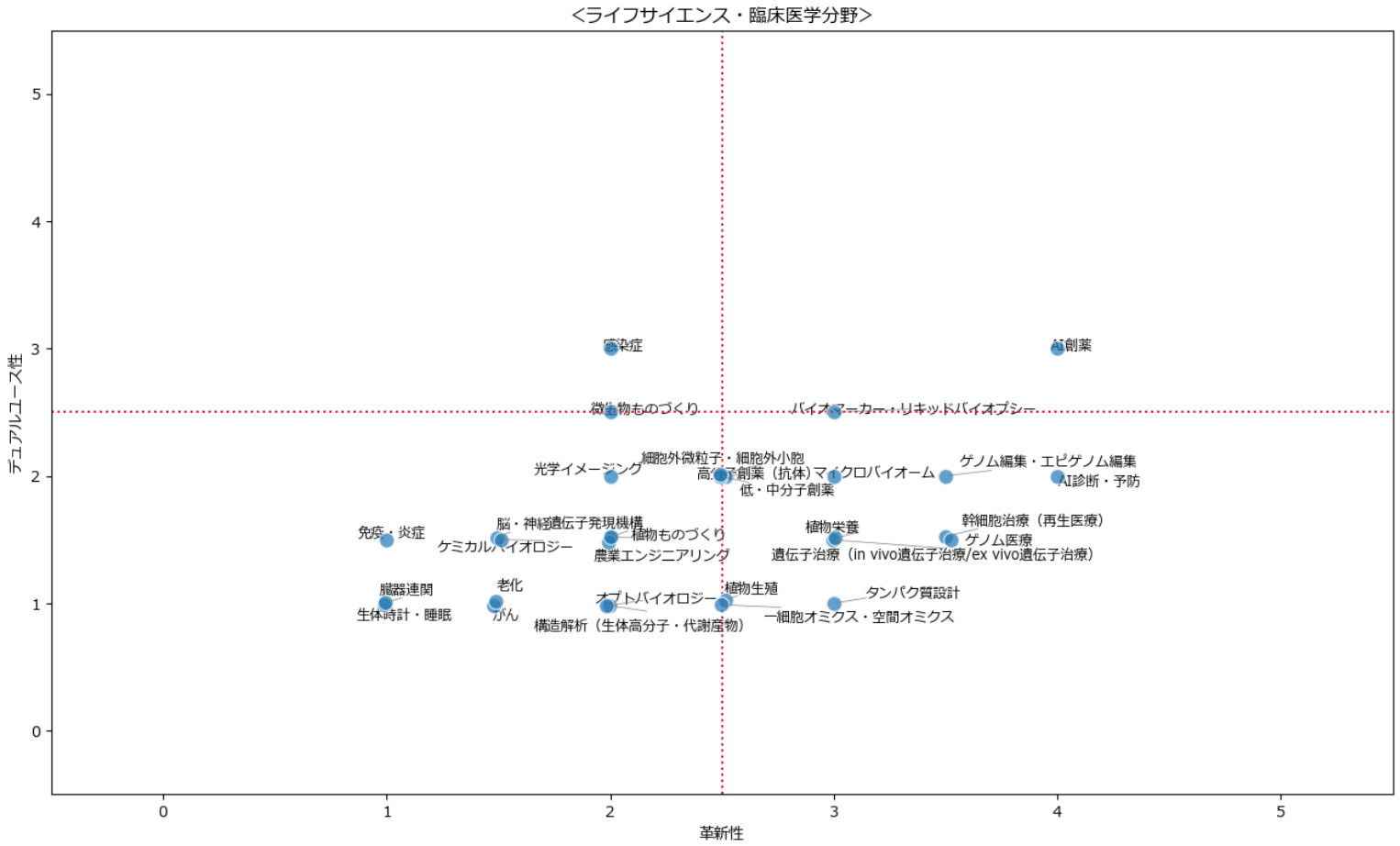
■ 革新性 × デュアルユース性



調査結果

掛け合わせ分析（ライフサイエンス・臨床医学分野）

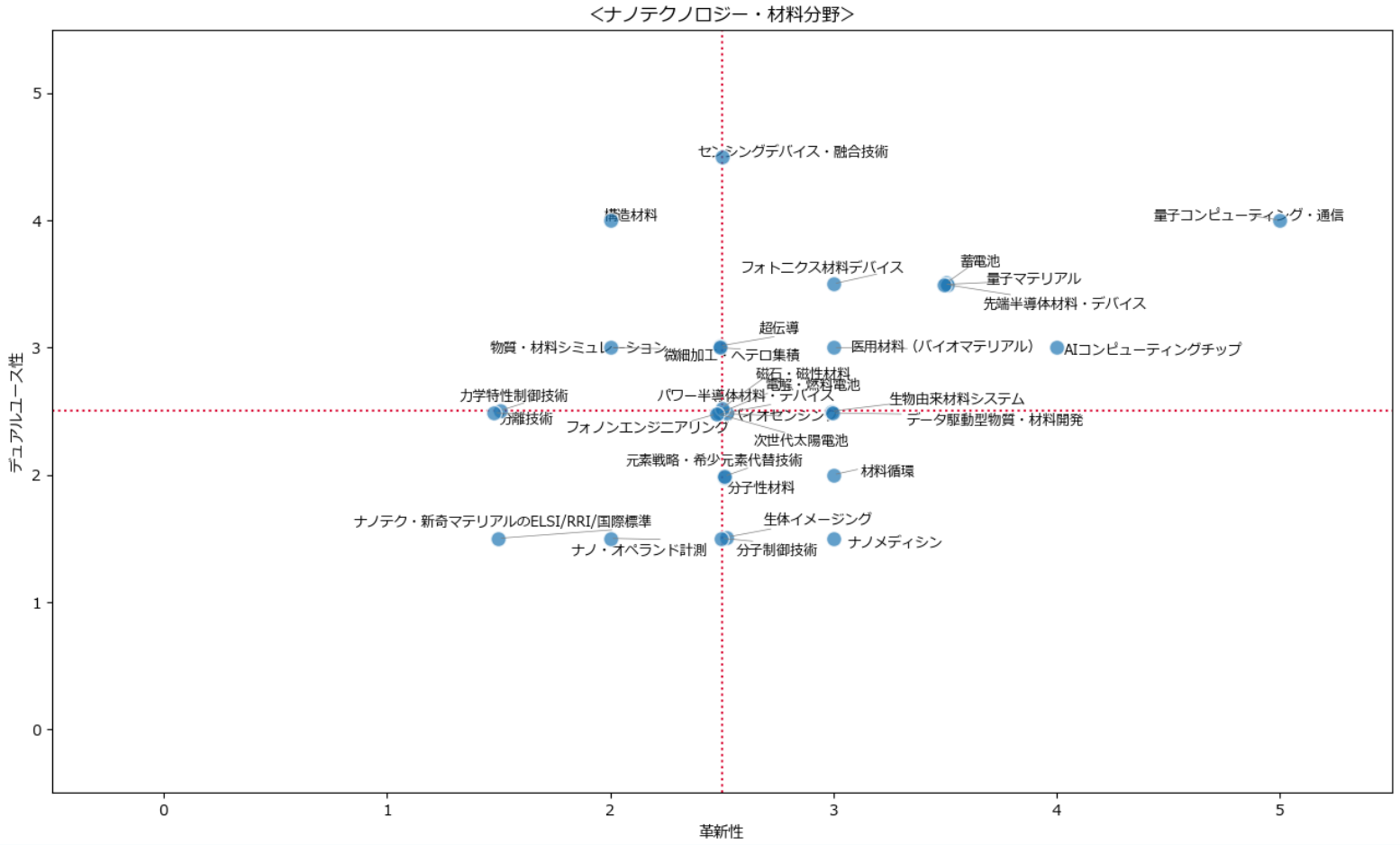
■ 革新性 × デュアルユース性



調査結果

掛け合わせ分析（ナノテクノロジー・材料分野）

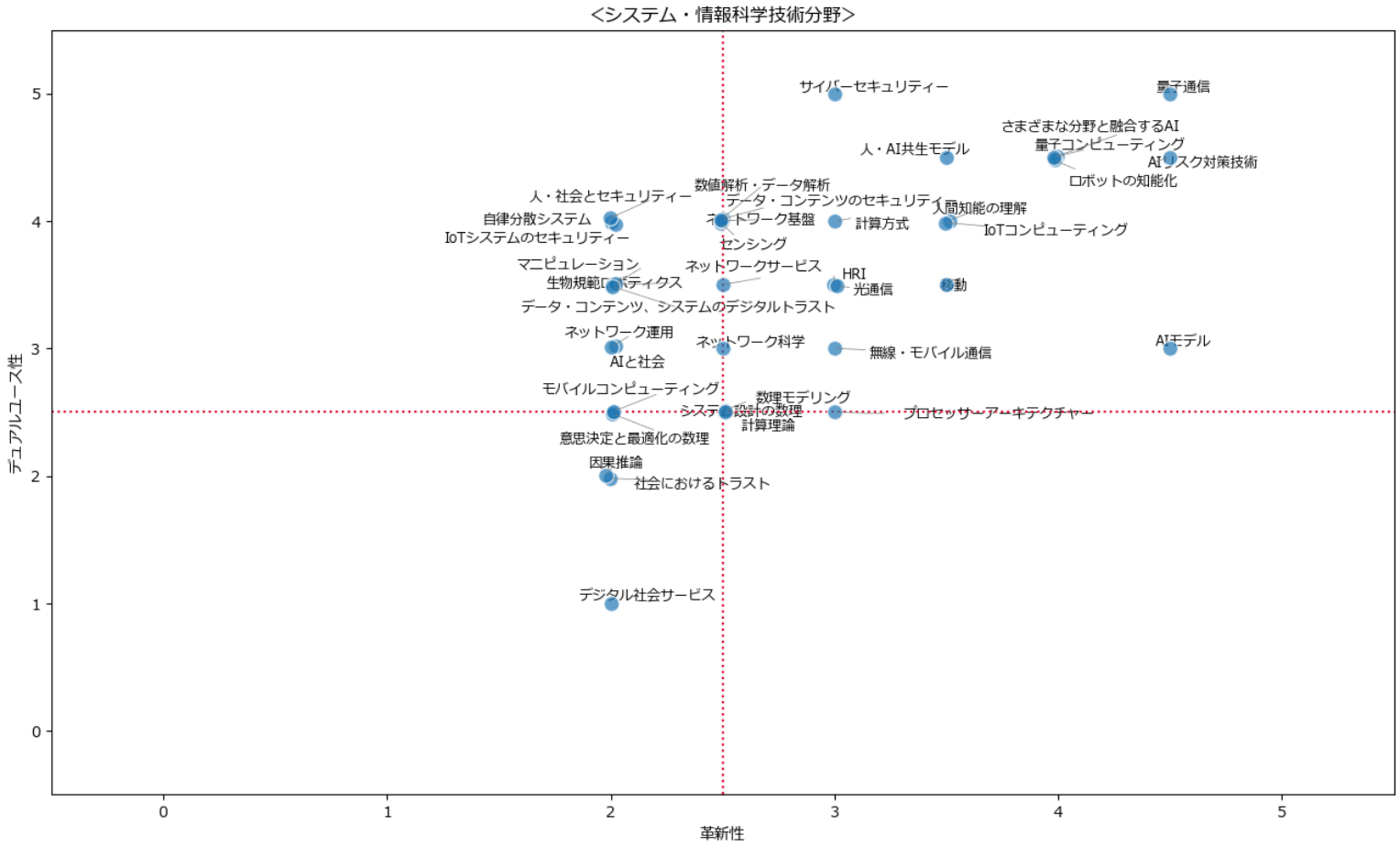
■ 革新性 × デュアルユース性



調査結果

掛け合わせ分析（システム・情報科学技術分野）

■ 革新性 × デュアルユース性



個別調査分析
(以降、全て3月時点版)

本事業における個別調査分析の対象は、「サイバーセキュリティ」「量子」「AI」「食料安全保障」「エネルギー」の5テーマとし、以下の通り定義

調査範囲の対象・定義

	サイバーセキュリティ	AI	量子	食料安全保障	エネルギー
定義	デジタル情報の漏えい・改ざん・または利用の防止等に関する措置 (特に技術)	データに基づき、自律的/半自律的に「識別・分類」「予測」「分析・判断」「生成」を行う技術	量子特有の性質を活用する先端技術	食料の安定的供給と国民による食料の入手に関する措置 (特に技術)	エネルギーを安定的かつ合理的な価格で確保する措置 (特に技術)
備考	偽誤情報は調査対象に含める 電磁戦等は対象外とする	対象となる「脅威」は、AIが解決する脅威とし、もらたすリスクについても別途分析する	対象となる「脅威」は、量子が解決する脅威とし、もらたすリスクについても別途分析する	生産から加工、流通、消費等へとつながる食分野の新しい技術であるフードテックを含む	-

個別調査分析
「サイバーセキュリティ」概要・抜粋

サイバーセキュリティ領域における脅威の構造

サイバーセキュリティ領域における脅威の増加

対象の多様化・複雑化

デジタルサービス
(行政・非対面サービス等のデジタル化が進むことで範囲が拡大)

情報提供・取引サービス (例: Webニュース、ECサイト)	オンライン投票
遠隔医療	ロボティクス利用

...

インフラ
(重要・通信・生活インフラ等のデジタル化が進むことで範囲が拡大)

既存インフラ (例: 行政インフラ、決済システム)	防衛システムを含む重要インフラ
海底ケーブル・衛星	メタバース

...

技術 (技術の脆弱性により、範囲が拡大)

古典技術 (例: 古典計算機、4/5G)	量子
AI	5G・6G

...

ヒト (ヒトの感覚がICT空間に接続され、範囲が拡大)

インプランタブルデバイス	人工臓器
ウェアラブルデバイス	

...

脅威アクターの多様化

外部

国家	(競合) 企業	個人	組織犯罪グループ
過激派グループ・テロリスト	ハッカー・ハッキンググループ	不正なサプライヤー・ベンダ・パートナー	

内部

企業・組織に不満を持つ従業員
非意図的な個人・企業 (脅迫等を含む)

手段の高度化・巧妙化

基本的なハッキング

パスワード推測	バッファオーバーフロー
セッションハイジャック	スニッフィング
トロイの木馬	ウイルス・ワーム

自動化・大規模化

DDoS攻撃	クロスサイトスクリプティング
SQLインジェクション	フィッシング
ボットネット	スパイウェア

多様化・複雑化

ゼロデイ攻撃	重要インフラ攻撃
サプライチェーン攻撃	ランサムウェア
ファイルレスマルウェア	ダブルエクストーション/ノーウェアランサム
クリプトジャッキング	
ICS/OT攻撃	SNS情報操作

新技術の悪用による巧妙化

量子コンピュータによる暗号解読	
AIフィッシング	ディープフェイクなりすまし

Source: Information Security Incorporated、BCG分析

本調査では、サイバーセキュリティ領域における脅威を、軍事・政治的脅威、経済・社会的脅威という2つの軸に基づき、4つの項目に分類

調査アプローチ

軍事・政治的脅威

1. サイバー領域における軍事力強化の競争激化

国家間の戦争/非正規戦において、サイバー空間を重要な戦闘領域と認識、**各国（特に非同盟・同志国）が戦力拡充に注力**

2. ハイブリッド戦/グレーゾーン事態の拡大

通信・重要インフラシステム等へのサイバー攻撃や、**偽誤情報の流布**が主要な戦闘手段の一つとなり、有事における国民生活への影響が甚大化

社会・経済的脅威

3. 重要インフラ等に対するサイバー攻撃の激化

製品・サービスの生産ライン停止や、**知的財産/顧客データ**等の競争力の源泉が甚大な被害を受ける

- 重要インフラシステム等をターゲットとするサイバー攻撃が増加

4. 対個人や中小企業等へのサイバー犯罪等による影響拡大

社会・経済全体のデジタル化の進展等を通じ、市民生活において**サイバー攻撃/犯罪に対する脆弱性**が増大

- 個人や中小企業等を狙ったサイバー犯罪等が増加・巧妙化

Note: 本資料においては、各用語を次の定義とする;
サイバー戦: 国家を主体としたサイバー空間における武力衝突
ハイブリッド戦: 軍事と非軍事の境界を意図的に曖昧にした手法を指し、例えばサイバー攻撃による通信・重要インフラの妨害、インターネットやメディアを通じた偽情報の流布等による影響工作を複合的に用いた手法が挙げられる
グレーゾーン事態: 純然たる平時でも有事でもない幅広い状況を指し、例えば国家間において、領土、主権、海洋を含む経済権益等について主張の対立があり、少なくとも一方の当事者が、武力攻撃に当たらない範囲で、実力組織等を用いて、問題にかかわる地域において頻繁にプレゼンスを示すこと等により、現状の変更を試み、自国の主張・要求の受入れを強要しようとする行為が挙げられる
サイバー攻撃: 重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバーテロ (重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの) や、情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取するサイバーインテリジェンス (サイバーエスピオナージ)
サイバー犯罪: 不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

サイバーセキュリティ領域に影響する国際情勢のトレンドを幅広く特定

個別トレンド (xx: 各シナリオの共通前提 xx: シナリオで分岐)		個別トレンドと当該領域との関連性	蓋然性	影響度
Societal (社会)	国家・行政におけるデジタル化の進展	サイバー攻撃対象の増加、セキュリティ対策の政策的支援や義務化	高	高
	情報価値の向上・保護の強化	データの誤用や流出によるセキュリティリスクの増大	高	中
	セキュリティリテラシーの向上	個人のリテラシー向上による詐欺や攻撃被害の予防・減少	中	中
Technological (技術)	特化型人工知能研究・実装	超高速ハッキングなどサイバー攻撃特化型AIと防御特化型AIとの攻防	高	中
	汎用人工知能の完成	自律的な攻撃の実現、汎用人工知能同士のサイバー攻防	低	高
	ネットワーク接続・自動化技術(5G/6G等)の進展	インターネット接続デバイスの増加でIoTテロなどの被害増加	高	高
	AR・VR・MR・XR等デジタル空間の拡張技術の進展	拡張技術の悪用による新たなセキュリティリスクの増大	中	中
	人間機能拡張・デジタル融合技術の進展	ロボティクスやBMIへのハッキングによる不正操作リスクの増大	高	高
	ブロックチェーン技術の普及・進展	サイバーセキュリティへのブロックチェーン技術の活用拡大	高	中
	IoT技術の活用拡大	IoT接続機器のセキュリティ更新の遅れやボットネット攻撃などの脅威拡大	中	高
	量子研究の進展	現代暗号の危殆化による根本的なセキュリティリスクの増大	中	高
	モビリティ技術 (自動運転・ドローン等) の進展・活用拡大	自動運転車やドローンへのハッキング・不正操作のリスクの増大	高	中
Economical (経済)	テックジャイアントの影響力拡大	セキュリティ技術開発の独占・寡占、情報流通への影響	中	中
	経済活動の非対面化・デジタル化	個人デバイスから経済全体へ伝播するなどサイバー攻撃の威力・被害が増大	高	高
	インフラデジタル化・複雑化	基幹サーバへのサイバー攻撃による経済活動への影響の拡大	高	高
Political (政治)	地政学対立の激化	グレーゾーン事態としてのサイバー攻撃やサプライチェーンリスクの増加	中	高
	各国内政の不安定化	国際協力の分断によるセキュリティの脆弱化・サイバー脅威の増大	低	高
	国際協力の進展	サイバーセキュリティでの安全保障協力体制の構築	中	中
	テロ組織など非国家犯罪組織の伸長	一定の組織力・資金力を持った組織によるサイバー攻撃の活発化	中	中
Demographical (人口)	先進国における少子高齢化の進行	サイバー攻撃におけるリテラシーの世代間格差の加速	高	中
	先進国における地方過疎の進行	設備の老朽化等によるサイバーセキュリティの格差拡大	中	中

STEEPED (Societal=社会、Technoloical=技術、Economical=経済、Environmental=環境、Political=政治、Ethical=倫理、Demographical=人口) のフレームワークに基づき分類;
Source: BCGメガトレンド; BCG分析

本領域における注目技術について、学術論文・専門家ヒアリング等幅広いソースをもとに調査・取りまとめ、29の技術を特定

サイバーセキュリティ領域における注目技術

理論

- 暗号化
  - 安全性の向上
    - 1 耐量子計算機暗号
    - 2 情報理論的暗号
    - 3 量子鍵配送
  - 機能の拡充
    - 4 軽量暗号
    - 5 属性ベース暗号
- 秘匿処理・モデル共有
  - 6 完全準同型暗号
  - 7 マルチパーティ計算
  - 8 連合学習
  - 9 ゼロ知識証明
- 難読化
  - 10 統計的開示抑制
  - 11 コード難読化

実装

		Identify	Protect	Detect	Respond	Recover
セキュリティ領域技術		12 アーティファクト分析	15 バイオメトリクス認証	20 電子署名 (オリジネーター・プロファイル)		24 デジタルフォレンジック
		13 アタックサーファスマネジメント	16 PUF (Physical Unclonable Function)	21 電子透かし		
		14 ペネトレーションテスト	17 TEE (Trusted Execution Environment)	22 エンドースメント情報分析		
			18 RASP (Runtime Application Self-Protection)	23 デセプション		
			19 移動標的防御			
新技術の活用	AI	25 脅威インテリジェンス[1)]	26 脅威ハンティング[1)]	27 UEBA (User Entity Behavior Analytics)	28 SOAR (Security Orchestration Automation Response)	
	ブロックチェーン	29 分散型ID				

1. 本分析では、受動的な情報収集のみならず、アトリビューションを含む能動的活用までを包含した概念として扱う; Note: サイバーセキュリティ対策はRespond, Recoverの後段においては技術以外の解決(組織ガバナンス等) 等も重要となり、技術要素が薄まる。また、近年着目されている "Usable Security" (セキュリティシステムのUIの利用のしやすさ、等)については個別技術の上位概念と整理

Source: Web of science、2023-2027 Strategic Technology Roadmap: Version 5 (CISA)、2023.03.08 Emerging privacy-enhancing technologies Current regulatory and policy approaches (OECD)

Disclaimer

The services and materials provided by Boston Consulting Group (BCG) are subject to BCG's Standard Terms (a copy of which is available upon request) or such other agreement as may have been previously executed by BCG. BCG does not provide legal, accounting, or tax advice. The Client is responsible for obtaining independent advice concerning these matters. This advice may affect the guidance given by BCG. Further, BCG has made no undertaking to update these materials after the date hereof, notwithstanding that such information may become outdated or inaccurate.

The materials contained in this presentation are designed for the sole use by the board of directors or senior management of the Client and solely for the limited purposes described in the presentation. The materials shall not be copied or given to any person or entity other than the Client ("Third Party") without the prior written consent of BCG. These materials serve only as the focus for discussion; they are incomplete without the accompanying oral commentary and may not be relied on as a stand-alone document. Further, Third Parties may not, and it is unreasonable for any Third Party to, rely on these materials for any purpose whatsoever. To the fullest extent permitted by law (and except to the extent otherwise agreed in a signed writing by BCG), BCG shall have no liability whatsoever to any Third Party, and any Third Party hereby waives any rights and claims it may have at any time against BCG with regard to the services, this presentation, or other materials, including the accuracy or completeness thereof. Receipt and review of this document shall be deemed agreement with and consideration for the foregoing.

BCG does not provide fairness opinions or valuations of market transactions, and these materials should not be relied on or construed as such. Further, the financial evaluations, projected market and financial information, and conclusions contained in these materials are based upon standard valuation methodologies, are not definitive forecasts, and are not guaranteed by BCG. BCG has used public and/or confidential data and assumptions provided to BCG by the Client. BCG has not independently verified the data and assumptions used in these analyses. Changes in the underlying data or operating assumptions will clearly impact the analyses and conclusions.


BCG
BOSTON
CONSULTING
GROUP
bcg.com