報告

秘密保護法廃止へ！実行委員会
院内集会　2023.11.6

経済安保法「改正」とセキュリティ・クリアランス法制化の狙い

セキュリティクリアランス＝SC

井原　聰（東北大学名誉教授）

１．経済安全保障推進法
特徴と問題点

経済安保の枠組み

経済安保法の枠組みと主な問題点

提言の主な柱			条	主な内容と問題点等	主な措置
第1章　総則			1 ～ 5	目的、基本方針	・安全保障を確保するため合理的に必要と認められる限度において行わなければならない
戦略的自律性	柱1 第2章	サプライチェーン多元化・強靭化	6~48	基本指針　特定物資の管理・支援・統制（半導体、蓄電池、医薬品、パラジウム、クラウド、肥料、船舶関係等）官民癒着・忖度、事業者への天下り、アメと鞭の危険性	・国民の生存や、国民生活・経済活動に甚大な影響のある物資 ・事業者の計画の認定・支援措置、規制
	柱2 第3章	基幹インフラ供給・確保	49~59	基本指針　特定社会基盤事業（①電気、②ガス，③石油，④水道，⑤鉄道，⑥貨物自動車運送，⑦外航貨物，⑧航空，⑨空港，⑩電気通信，⑪放送，⑫郵便，⑬金融，⑭クレジットカード）特定重要設備の管理・統制、官民癒着・忖度、事業者への天下り、アメと鞭の危険性	・重要設備の導入・維持管理等の委託の事前審査 ・勧告・命令 等を措置
戦略的不可欠性	柱3 第4章	技術基盤	60~64	基本指針　特定重要技術の定義なし（先端技術の研究開発、機微技術の研究開発）罰則付き研究協議会・シンクタンク等による研究情報管理、研究の遂行管理、官民伴走→社会実装（軍民）、国費による先端技術研究は監視の対象となりうる。研究の自由・発表の自由の制約が起こりうる。	・先端的な重要技術の研究開発の促進 ・官民伴走支援のための協議会設置、調査研究業務の委託（シンクタンク） 等を措置。
	柱4 第5章	特許非公開	65~85	基本指針　秘密特許（特許の非公開）恣意的運用の危険性、研究の自由・発表の自由の制約が起こりうる。	・安全保障上機微な発明の特許出願 ・非公開指定 ・外国出願の制限
	第6章	雑則	86~91		
	第7章	罰則	92~99	第15条、第19条、第20条、第22条、第37条、第38条、第40条、第47条、第48条、第50条、第52条、第54条、第58条、第62条、第63条、第64条、第67条、第70条、第73条、第74条、第77条、第78条、第80条、第84条、第92条、第94条　（計26ヶ条に罰則規定あり）	
附則			1~11		
附帯決議			1~17		

経済安保法、基本方針・基本指針等から井原作成

経済安全保障推進法の主な枠組み

提言の主な柱		条番号	主な内容
第1章　総則		1～5	目的、基本方針
戦略的自律性	第2章　サプライチェーン	6~48	レアアース・半導体など特定物資の管理統制
	第3章　基幹インフラ	49~59	電気・ガス事業など14業種の管理統制
戦略的不可欠性	第4章　技術基盤	60~64	先端技術の研究開発、機微技術の研究開発
	第5章　特許非公開	65~85	秘密特許
第6章　雑則		86~91	
第7章　罰則		92~99	26カ条の罰則規定
附則		1~11	

経済統制

軍事動員

安全保障特別重要技術育成プログラム

２．安全保障重要技術育成プログラム（Kプロ）という名の軍事技術開発

重要技術のリストアップ

重要な先端技術に対する構造的な理解

様々な場（領域）で活用され得る、我が国にとって重要な先端技術を如何に見定めるか。

重要な先端技術の例

- ○ バイオ技術
- ○ 医療・公衆衛生技術（ゲノム学含む）
- ○ 人工知能・機械学習技術
- ○ 先端コンピューティング技術
- ○ マイクロプロセッサ・半導体技術
- ○ データ科学・分析・蓄積・運用技術
- ○ 先端エンジニアリング・製造技術
- ○ ロボット工学
- ○ 量子情報科学
- ○ 先端監視・測位・センサー技術
- ○ 脳コンピュータ・インターフェース技術
- ○ 先端エネルギー・蓄エネルギー技術
- ○ 高度情報通信・ネットワーク技術
- ○ サイバーセキュリティ技術
- ○ 宇宙関連技術
- ○ 海洋関連技術
- ○ 輸送技術
- ○ 極超音速
- ○ 化学・生物・放射性物質及び核(CBRN)
- ○ 先端材料科学

（順不同）

「米国重要・振興技術(CET)国家戦略」（2020年10月公表）を基礎に、内閣府シンクタンク機能の試行事業の幅広調査において示された技術分野

場としての領域（社会や人の活動等が関わる領域）

- ・ 海洋領域
- ・ 宇宙・航空領域
- ・ 領域横断（サイバー空間領域）
  - *領域横断には、エネルギー・半導体等の確保（[illegible]）等、人の経済安全保障と関[illegible]
- ・ バイオ領域

先端軍事領域

（参考）
○科学技術イノベーション基本計画（R3.3閣議決定）において、レジリエントで安全・安心な社会の構築の観点から、**具体的な取組を要する領域として例示**されたもの
- サイバー空間におけるセキュリティの確保
- 新たな生物学的な脅威への対応
- 宇宙・海洋分野等の安全・安心への脅威への対応
- 分野横断的な視点から安全・安心確保のため「知る」「育てる」「生かす」「守る」の取組の強化

○第二百七回国会における岸田内閣総理大臣所信表明演説「国が、五千億円規模に向けた基金を設け、**人工知能・量子・ライフサイエンス・宇宙・海洋**といった世界の未来にとって不可欠な分野における研究開発投資を後押しします。」令和3年12月6日

（参考）
米国重要・新興技術国家戦略に示された19の技術分野
(Critical and Emerging Technology, CET2022)

- ○ 先端コンピューティング
- ○ 先端ｴﾝｼﾞﾆｱﾘﾝｸﾞ素材
- ○ 先端ガスタービンエンジン技術
- ○ 先端製造
- ○ 先端ネットワーク化センサ・管理
- ○ 先端原子力技術
- ○ 人工知能
- ○ 自律システム・ロボティクス
- ○ バイオ技術
- ○ 通信・ネットワーク技術
- ○ 指向性エネルギー
- ○ 金融技術
- ○ ﾋｭｰﾏﾝ・ﾏｼﾝ・ｲﾝﾀｰﾌｪｰｽ
- ○ 極超音速
- ○ ﾈｯﾄﾜｰｸ化ｾﾝｻｰ・ｾﾝｼﾝｸﾞ
- ○ 量子情報科学
- ○ 再生可能エネルギー・貯蔵
- ○ 半導体及びﾏｲｸﾛｴﾚｸﾄﾛﾆｸｽ
- ○ 宇宙技術・システム

「米国重要・振興技術(CET)国家戦略」2020

出典：「経済安全保障関係 「経済安全保障重要技術育成プログラムにかかる研究開発ビジョン検討WG」の検討結果について（報告）」「第1回経済安全保障重要技術育成プログラムに係るプログラム会議」

重要技術の意味

米国：安全保障技術※ （軍事技術）

※田上靖「米国輸出管理改革法の新基本技術(Emerging and Foundational Technologies)新規制 及び CISTEC パブコメの概要」（安全保障貿易情報センター（CISTEC），2019

デュアルとは

デュアル（マルチ）とその意味

- デュアル技術 → 米国防総省の技術力低下を補完する民用技術を spin on するための戦略※
- デュアル技術開発研究の成果

→ 軍用・民用

→ 軍用になると民用に規制

※Schmitt, Roland W., "Export Controls: Balancing Technological Innovation and National Security",Issues in Science and Technology.1984

経済安全保障推進法案の国会審議における論点等③

（参考）４分野ごとの論点

（技術）

- ■ 多義性を有する先端的な重要技術の育成の必要性（米欧中の投資額と比較し、日本の投資額は明らかに少ない）
- ■ 官民協議会やシンクタンクと、自由な研究活動との関係
  - ➢ 守秘義務の対象や運用方法
  - ➢ 研究成果の公開について
- ■ 軍事技術開発への研究者の動員

（特許）

- ■ 経済活動やイノベーションとの両立
  - ➢ 対象技術分野について
  - ➢ 保全指定前の離脱について
  - ➢ 補償について
- ■ 弁理士の関与

軍事技術開発への
研究者の動員

4

出典「経済安全保障推進法の審議・今後の課題等について」（内閣官房 経済安全保障法制準備室、2022.7.25

軍事研究への囲い込み

軍事研究への囲い込み
ー研究の自由・発表の自由の侵害ー

橋本和仁
JST理事長
JST　HPより

上山隆大
CSTI常任議員
JCSTIHPより

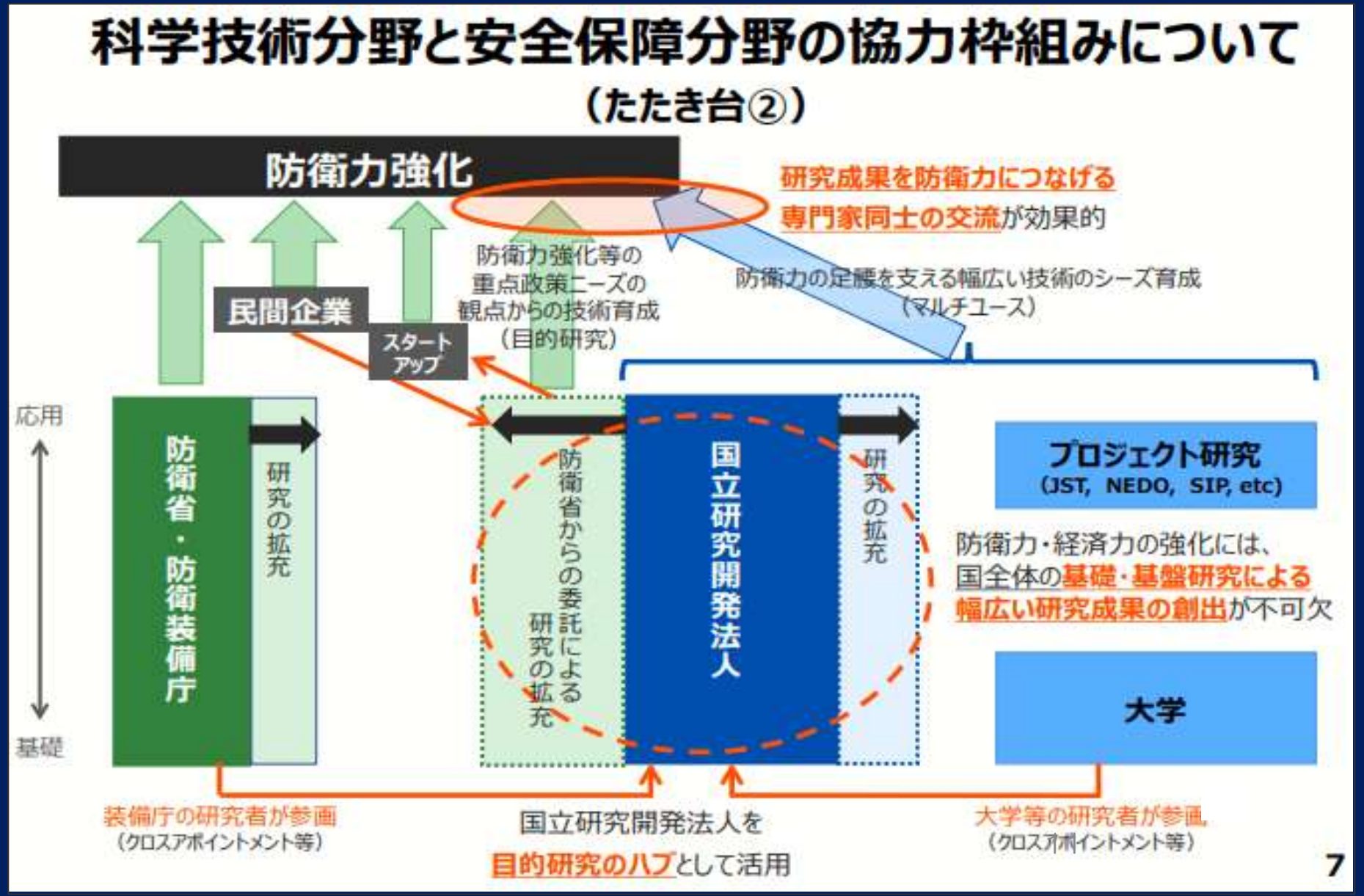
資料４

総合的な防衛体制の強化に資する
科学技術分野の研究開発に向けて
（橋本委員・上山委員　提出資料）

■甘利グループ■
橋本和仁科学技術振興機構理事長（JST）
上山隆大総合科学技術・イノベーション会議常勤議員（CSTI）

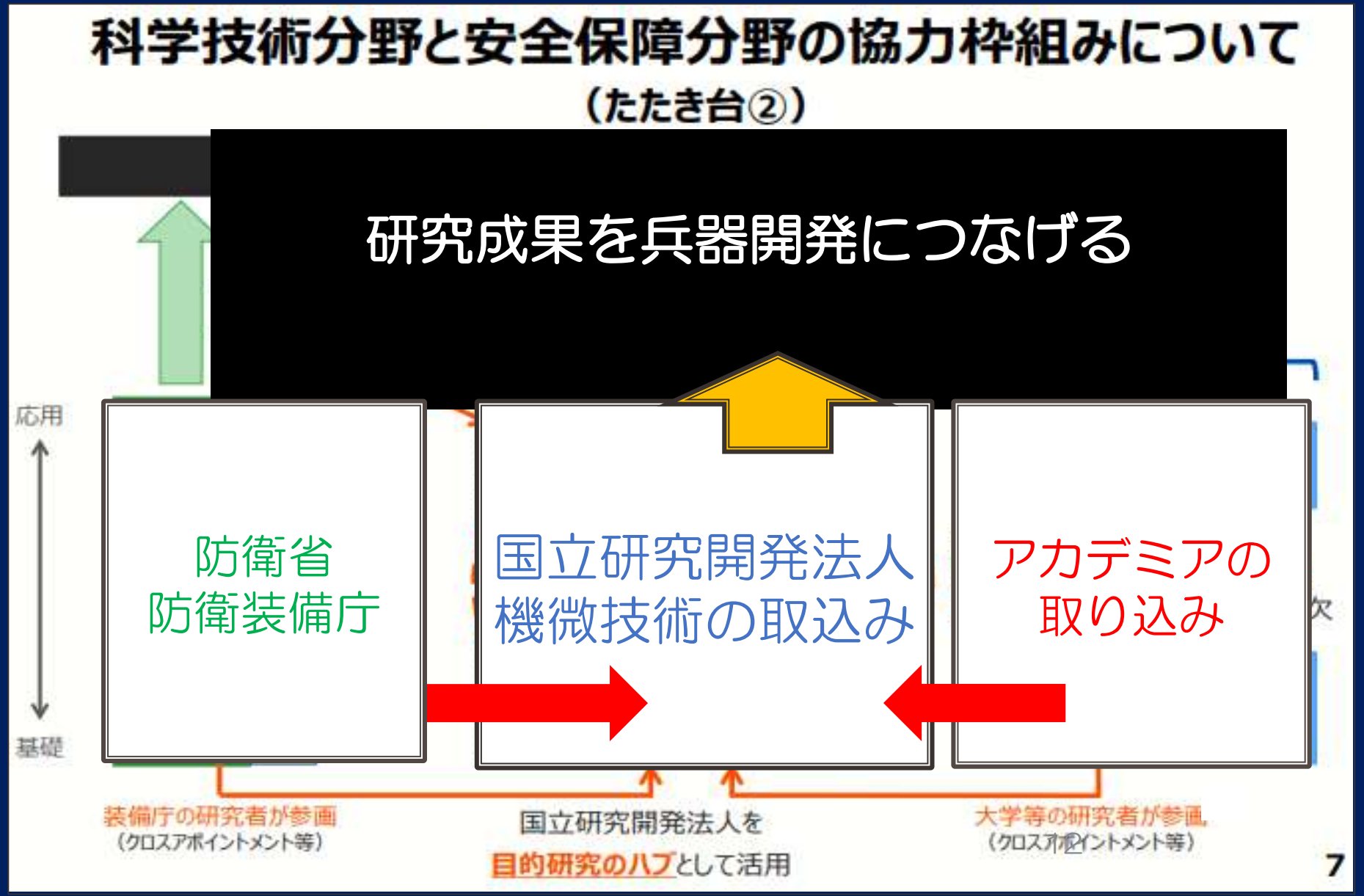
出典「経済安全保障推進法の審議・今後の課題等について」（内閣官房 経済安全保障法制準備室、2022.7.25

軍事研究への囲い込み



出典：https://www.cas.go.jp/jp/seisaku/boueiryoku_kaigi/dai2/siryou4.pdf

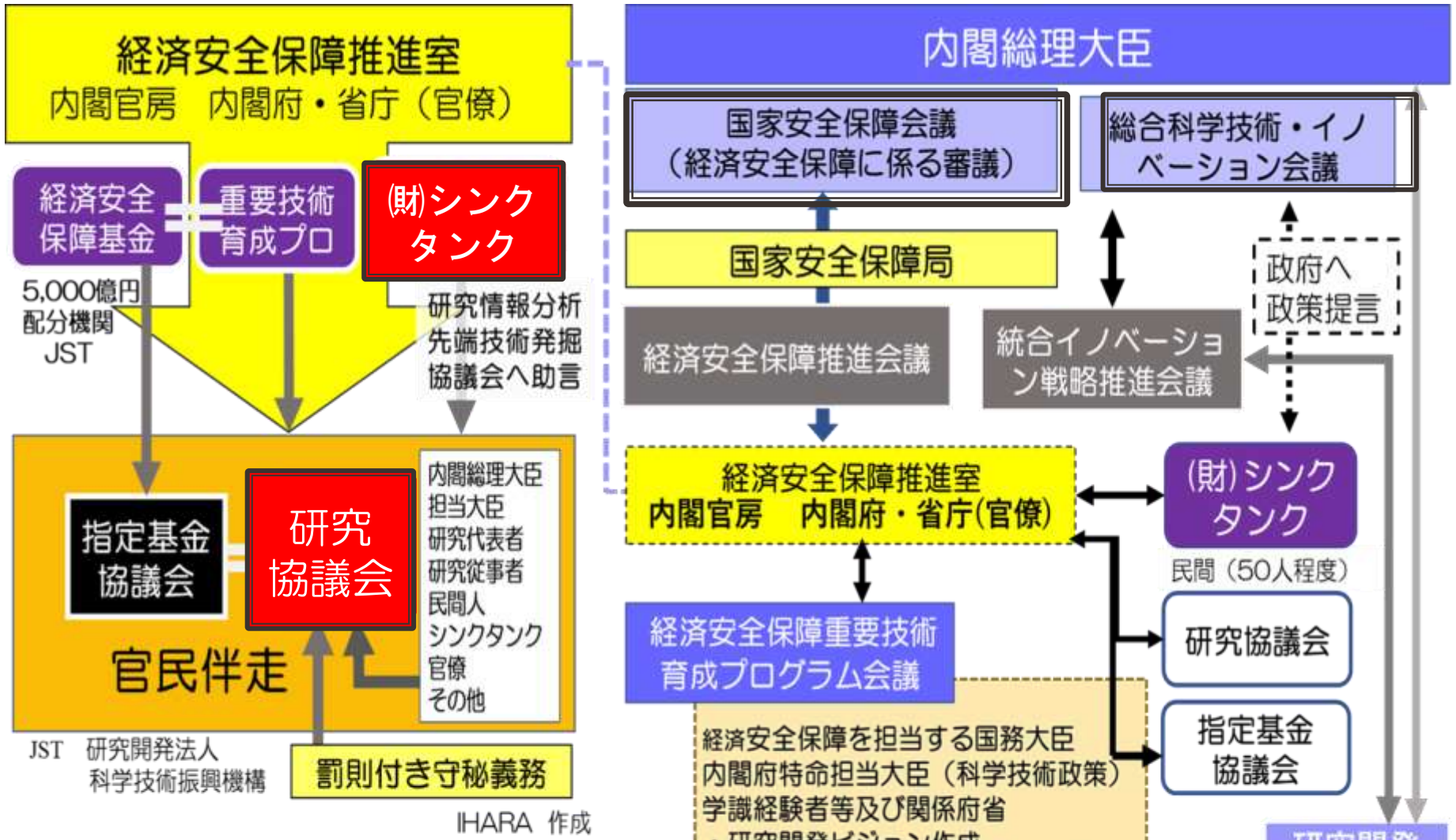
軍事研究への囲い込み



出典：https://www.cas.go.jp/jp/seisaku/boueiryoku_kaigi/dai2/siryou4.pdf

研究協議会・シンクタンク

罰則付き守秘義務付き秘密情報の提供と官民伴走



シンクタンクの役割

- 先端研究の調査と研究
- 政府への政策提言
- 若年研究者養成
- 内外の優れた研究に目を光らせる
- 研究課題の選定
- プロジェクトの選定機能
- 大学や研究機関のハブになる
- 米国のRAND研究所のように博士号を出せる組織に

3「経済安全保障上の重要政策に関する提言」

（2023.3.28、自由民主党
政務調査会
経済安全保障推進本部
安全保障調査会
サイバーセキュリティ対策本部
デジタル社会推進本部

「経済安全保障上の重要政策に関する提言」

【提言の目的】国家安全保障戦略では「経済安全保障分野における新たなセキュリティ・クリアランス制度の創設の検討に関する議論も踏まえつつ、情報保全のための体制の更なる強化を図る」とされ、本ＳＣ提言はその具体的内容を提言するものである。

（１）セキュリティ・クリアランス（ＳＣ）制度の導入
（２）サイバーセキュリティ（ＣＳ）の確保
（３）経済インテリジェンス（ＥＩ）の強化

（１）いわゆる「セキュリティ・クリアランス（SC）」制度の導入

提言の目的	• 新たな国家安全保障戦略では、「経済安全保障分野における新たなセキュリティ・クリアランス制度の創設の検討に関する議論も踏まえつつ、情報保全のための体制の更なる強化を図る」とされており、その具体的内容を提言するもの
制度のスコープ	• 経済安全保障等の分野での国際共同事業や研究・開発等の円滑な実施を可能とするため、同盟国・同志国の情報保全のレベルや産業界等からのニーズも踏まえ、国際的整合性や実質的同等性の観点にも沿うセキュリティ・クリアランス制度を含む情報保全制度とする • サイバーセキュリティ面での情報保全とも整合性を十分に確保 • 包括的な情報保全制度を整備するため、特定秘密保護制度との関係の整理も含め検討 • 新たに設置した有識者会議（2023年2月22日に第1回会合を開催）において、今後１年程度を目途に可能な限り速やかに検討を進め結論を得た上で、法改正及び体制整備等を行うこと
情報区分（下表を参照）	• 機密性３情報を中心として、必要に応じて機密性２に相当する政府保有及び民間保有の情報を検討 • 情報区分AやBの民間関連部分では、施設のクリアランス等の必要性についても検討 • 情報区分Dは、重要インフラ事業者等を念頭に、事業者とも協議を重ね必要な範囲で限定的に設定 • 情報区分Eは、ガイドラインの設定など、経済合理性とイノベーション創出の観点で合理的な運用を前提
情報分野	• 経済安全保障分野を中心とし、情報保全措置を実施する必要性の範囲と外縁を設定
情報保全及びセキュリティ・クリアランス制度	• 情報区分に応じたアクセス権の段階設定と応分の罰則制度、本人同意を前提としたバックグラウンドチェックの対象範囲と調査深度を設計 • セキュリティ・クリアランスの付与は、属人的でポータブルな運用とする • 民間事業者の負担となる領域では、合理的な範囲内で支援制度を検討
体制整備	• セキュリティ・クリアランスを含む情報保全にあたり、政府一体となって十分な体制を整備

現行の情報区分と分野及び保全措置

情報区分	情報帰属	狭義安全保障	経済安保
A）CI）特定秘（機３）	政府	実施	未手当
B）CI）特定秘以外の機３相当	政府	契約単位で実施あり	未手当
C）CUI）機２相当	政府	契約単位で実施あり	未手当
D）CUI相当）機２相当（規制付）	民間	契約単位で実施あり	炉規法
E）CUI相当）機２相当	民間	国家制度なし（企業独自）	

（注）
CI: Classified Information
CUI: Controlled Unclassified Information

「経済安全保障上の重要政策に関する提言　（概要）」自民党

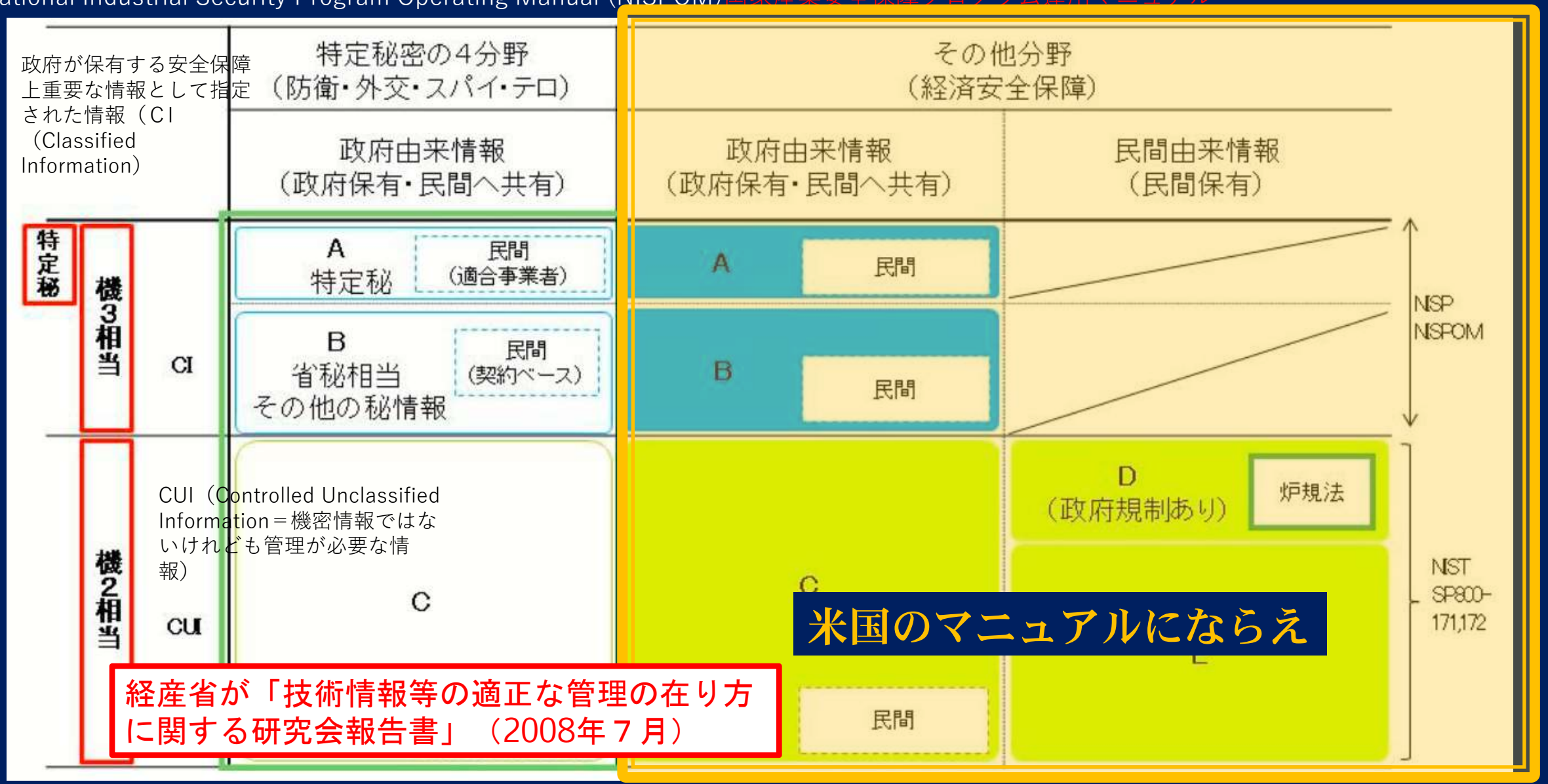
SC制度の導入

目的・ねらい
- 経済安保にSC制度創設
- 包括的情報保全
- 一年以内に

情報区分
- 秘→機密・極秘・秘
- 取扱注意

政府一体
体制整備

National Industrial Security Program Operating Manual (NISPOM)国家産業安全保障プログラム運用マニュアル

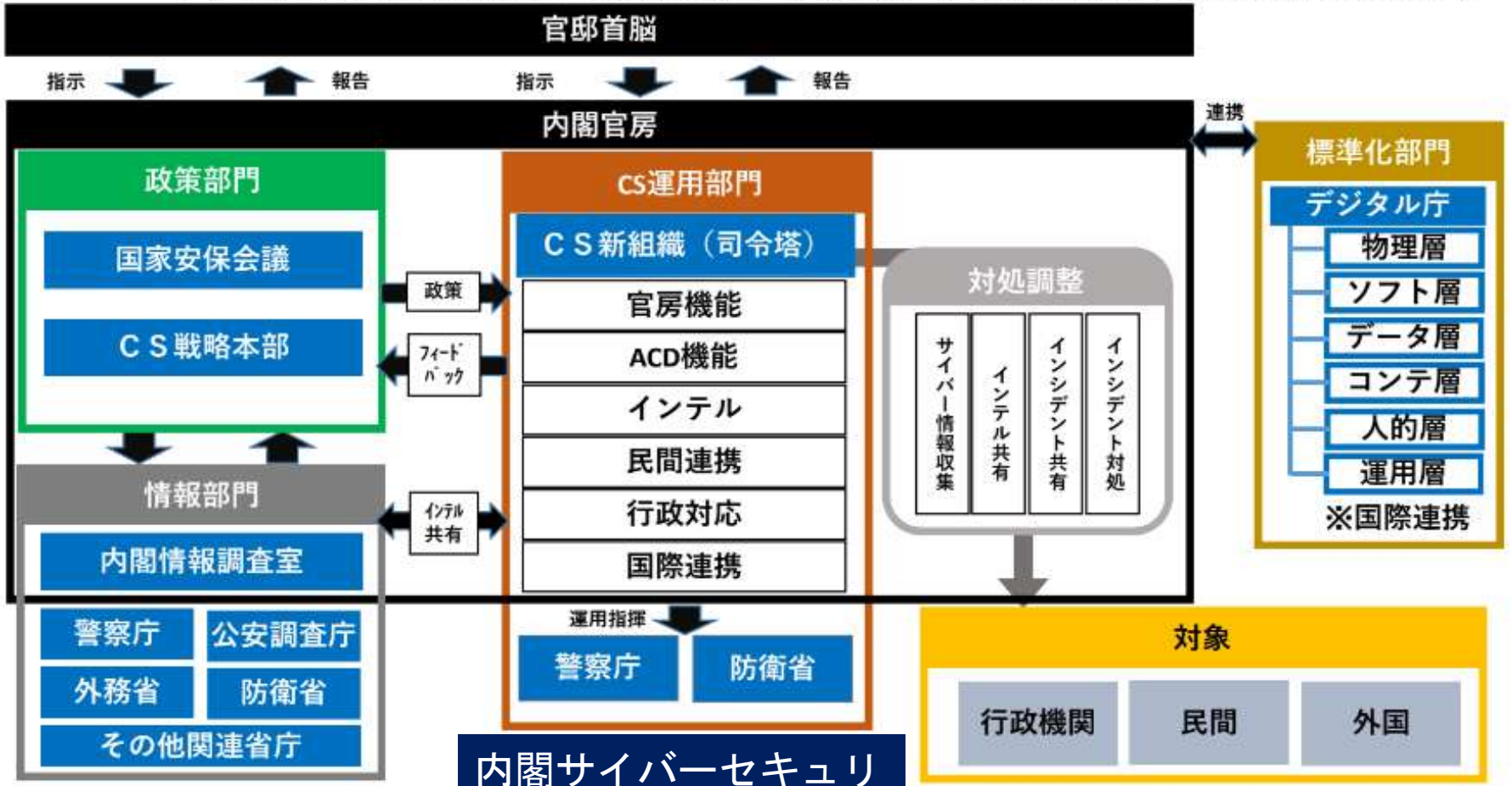


米国国立標準技術研究所（NIST: National Institute of Standards and Technology）

SP800シリーズ（SP: Special Publications）とFIPS（Federal Information Processing Standards)

（2）サイバーセキュリティー（CS）の確保

提言の目的	• 新たな国家安全保障戦略では、能動的サイバー防御の導入、サイバー安全保障分野における情報収集・分析能力の強化、新組織の設置、必要な法制度の整備が明記された。本提言は、その具体化に関し骨格を提言するもの
取組のスコープ	• 平時有事に関わらず、あらゆる状況を対象とした能動的サイバー防御（ACD)を含む、包括的ＣＳ対策とすること • 多様な主体とのインシデント情報共有、インテリジェンス情報共有、共同オペレーションを可能とする制度とすること
政府の体制	• NISCは発展的改組し、CS戦略本部の事務機能とは別に、全く新しい実運用機能を内閣官房に設置すること • ACD機能・民間及び行政セクターのCS対策機能・インテリジェンス収集分析共有機能、官房機能等を設置すること



内閣サイバーセキュリティセンターNISC廃止

CSの確立

サイバセキュリティ官邸への権限集中

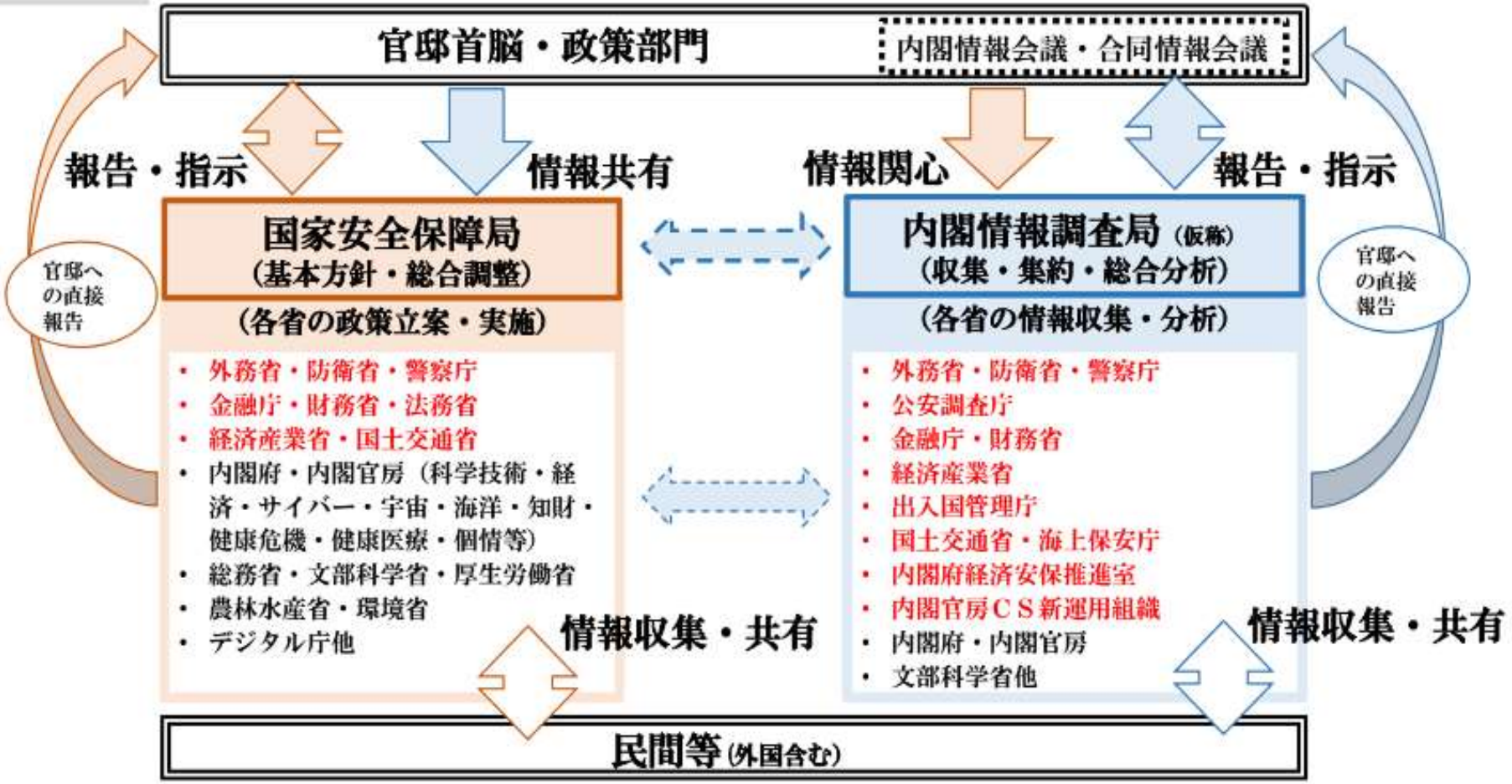
■秘→

- 機密
- 極秘
- 秘
- 取扱注意

●常時あらゆる情報対象
●能動的サイバー防御
●インシデント、インテル情報共有

（３）経済インテリジェンス（EI）の強化

提言の目的	• 新たな国家安全保障戦略では、人的情報を含む多様な情報源に関する情報収集能力を大幅に強化することが謳われており、本提言は、経済安全保障の分野を中心に、その具体的内容を提言するもの
取組のスコープ	①情報部門（ＣＩＲＯ及び各省庁等）と政策部門（ＮＳＳ及び各省庁等）の間のＥＩエコシステムの強化（インテリジェンス・サイクル稼働体制）、②ＮＳＳを中心とした政策部門の強化、③ＣＩＲＯを中心とした集約分析機能の強化、④各省庁の収集分析機能の強化、⑤官民若しくは国際の共同対処を念頭においた情報共有メカニズムの強化、⑥官民ビッグデータを活用した情報収集分析、サイバー空間のインテリジェンス、ディスインフォメーションといった新たな分野への対応、⑦ガバナンス、⑧人材育成・採用の各側面で改善に取り組むこと。



EIの強化

●経済安保中心の人的情報・多様な情報取集
●国家安全保障局中心
●内閣情報調査室
→内閣情報調査局

４　経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議

資料

第7回経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議

事務局説明資料

令和５年10月11日
内閣官房

中間論点

中間論点整理の概要

新たな制度の方向性	**政府が保有する安全保障上重要な情報として指定された情報(CI(Classified Information))を念頭に置いた制度** **主要国との間で通用する実効性のある制度、必要となる国際的な枠組みの検討** **政府横断的・分野横断的な制度の検討**
具体的な制度の方向性	**経済安全保障上重要な情報の指定の範囲** • 経済関係省庁等も含めて政府内で議論を深め、特定秘密保護法の４分野との整理も含め検討 • 情報の機微度に応じて単層構造から複層構造化、柔軟かつ機動的な情報の指定・解除の検討 **信頼性の確認（評価）とそのための調査** • 情報保全の効果を毀損しない範囲で効率性を追求 • 調査結果の一定のポータビリティ性（調査結果が一定期間、組織や部署を超えて有効であること）の確保 **産業保全(民間事業者等に対する情報保全)** • 政府からCIの共有を受ける意思を示した民間事業者等について、防衛産業と同様、調査や保全体制の確認など厳格な対応を適用 **プライバシー等との関係** • 信頼性確認のための調査は、丁寧な手順を踏んだ本人の同意を得ることが大前提。その際、信頼性確認のために収集された情報の適切な管理が必須 • プライバシーや労働法令との関係を十分踏まえ適切な形で整理 **官民の体制整備** • 政府において情報保全を適切に実施するための必要な体制整備の在り方の検討 • 民間事業者等における保全の取組みに対する支援の在り方の検討
その他	**CI以外の重要な情報の取扱い** • 必要に応じ、信頼性の確認のための調査も含め、CIほど厳格ではないが、一定の保全措置を講ずる必要性を検討 • 環境整備を行う場合には、民間事業者等任せにせず、政府が明確な指針等を示していくことの妥当性も含め検討 • 既存の関連制度との関係も踏まえつつ、望ましい情報保全の在り方を検討 **信頼性の確認に係る理解の促進**

同盟国・同志国との通用性

経済安保法にビルトイン

産業統制の強化

CI以外の重要情報の定義なし、秘密扱いの拡大

基本骨格

新しい制度の基本的な骨格

□ 経済安保上の重要情報を保全するための制度として検討していくにあたり、その基本的な骨格は下記のようになるのではないか。

① 経済安全保障上の重要な情報の秘密指定・指定解除

- 政府が保有する情報の指定、有効期間の設定、指定解除　　等

※ 政府が外部から受領した情報については、秘密指定の効果は原保有者に及ばない。

② 経済安全保障上の重要な情報の管理・提供ルール

- 保管及び外部提供のルール
- 当該情報を取り扱う個人及び事業者に対する信頼性確認（クリアランス）
- 信頼性確認のための一元的調査機関　　等

③ 罰則

- 漏えいや不正取得に関する罰則　　等

（注）このほか、プライバシー、同意拒否者等の処遇等や経済安保上の重要情報に準ずる重要な情報の取り扱いについて議論が必要。

3

経済安保上の重要情報

セキュリティ・クリアランス

罰則と監視

秘密階層

経済安全保障上の重要な情報のイメージ

□ 経済安保上の重要情報とは、Top Secret及びSecretレベルだけではなく、Confidentialレベルもカバーする、下記のようなイメージになるのではないか。

①防衛
②外交
③スパイ防止
　特定有害活動
④テロ防止

例えば
⑤特定重要物質
⑥サイバーセキュリティ・インテリジェンス
⑦基盤インフラ
⑧先端機微技術・デュアル技術
⑨秘密特許関係

（※）Confidential級については、行政文書の管理に関するガイドラインに基づき、各府省庁において保全措置がとられている。

4

重要情報

経済安全保障上重要な情報の候補

□ 各省庁において現時点で経済安全保障上の重要な情報に関連するとしている情報は、概ね次の類型のうち機密性が高い情報であると考えられる。

サイバー関連情報
■ サイバー脅威・対策等に関する情報

規制制度関連情報
■ 審査等にかかる検討・分析に関する情報

調査・分析・研究開発関連情報
■ 産業・技術戦略、サプライチェーン上の脆弱性等に関する情報

国際協力関連情報
■ 国際的な共同研究開発に関する情報

（注）上記には、特定秘密保護法上の別表に該当し得ると思われる情報も含まれており、今後関係省庁の協力も得ながら事務局にて要精査。

□ 「経済安全保障上重要な情報を指定していくに当たっては、我が国として真に守るべき政府が保有する情報に限定し、そこに厳重な鍵をかける」という基本的な考え方（中間論点整理）を踏まえ、制度化に当たって、対象となる情報の範囲を適切に画していくために、一定の考え方の下で情報を整理していくべきではないか。

□ 例えば、国家及び国民の安全を支える我が国の経済的な基盤の保護に関する情報が対象になると整理することが考えられるか。

5

■サイバー関連

■監視制度
　クリアランス審査
　監視システム

■先進技術
　サプライチェーン

■国際協力

秘密保護法とSC制度(案)比較

		特定秘密保護法	セキュリティ・クリアランスの法制化
法律	成立年	2013年12月6日	2024年？
	施行年	2014年12月10日	2024年？
機密範囲	対象領域	①防衛、②外交、③特定有害活動防止、④テロ防止	①②③④+経済安保情報、AI・宇宙・サイバーの技術分野
	秘密区分	単一（特定秘密）	Top Secret機密、Secret極秘、Confidential秘
適格性評価	適性評価の特徴	統一の基準で各行政機関が実施	分野横断、調査機能の集約、効率化
	評価対象	個人：公務員、一部の民間企業従事者	個人・施設：公務員、研究者・技術者、民間企業従者
			同盟国・同志国との同等性確保　米国のシステムを採用
	評価基準	本人 ①特定有害活動とテロリズムとの関　係②犯罪等の経歴　③情報通信関係の非違歴　④薬物の濫用　⑤精神疾患　⑥飲酒の性癖　⑦金融の信用状態、経済状態　⑧知人の連絡先等	本人 ①テロ等・政府転覆活動の関与　②外国との関係　③犯罪歴　④民事訴訟歴　⑤情報通信関係の非違歴　⑥薬物の濫用　⑦精神の健康状態　⑧飲酒の性癖　⑨金融・経済の信用状態　⑩知人の連絡先等
		家族・同居人・上司・隣人 氏名・生年月日・国籍・住所	上司・知人・同居人・隣人等 氏名・生年月日・住所・社会保障番号等
		本人の同意が必要	本人の同意が必要

「日本のセキュリティ・クリアランス―求められる企業の経済安全保障対応」総合政策研究部　准主任研究員　鈴木 智也を参考に加筆修正
https://www.nli-research.co.jp/report/detail/id=75927?pno=2&site=nli

5　経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議

資料３

経済安全保障分野における
セキュリティ・クリアランス制度等に関する有識者会議

令和５年２月22日
内閣官房

（別紙）

経済安全保障分野におけるセキュリティ・クリアランス制度等に関する

経済安全保障分野におけるセキュリティクリアランス制度に関する有識者一覧　(2023.2.24)

氏　名	現　　職	元職等
梅津 英明	森・濱田松本法律事務所 パートナー弁護士	経済安保辣腕弁護士
北村 滋	北村エコノミックセキュリティ 代表	元警察官僚、元国家安全保障局長 経済安保推進、SC推進
久貝 卓	日本商工会議所 常務理事	財界
小柴 満信	経済同友会 副代表幹事	財界
境田 正樹	TMI総合法律事務所 パートナー弁護士	元東大理事、元スポーツ審議会委員
鈴木 一人	東京大学公共政策大学院 教授　　座長代理	経産安保法推進論者
富田 珠代	日本労働組合総連合会 総合政策推進局総合局長	自動車総連、金融審議委員
永野 秀雄	法政大学人間環境学部 教授	秘密保護法賛成・チェック機関の創設
原 一郎	一般社団法人 日本経済団体連合会 常務理事	財界
細川 昌彦	明星大学経営学部 教授	元経産省貿易管理部長
渡部 俊也	東京大学未来ビジョン研究センター 教　座長	知財学会会長・産学連携
	（第1回有識者会議資料より）	（井原作成）

細川　昌彦　　明星大学経営学部 教授

渡部　俊也　　東京大学未来ビジョン研究センター 教授

経済安全保障の観点からの情報保全の強化の必要性①

第4回経済安全保障推進会議資料

□ 経済安全保障推進法の附帯決議や国家安全保障戦略を踏まえ、セキュリティ・クリアランスを含む我が国の情報保全の強化に向けた検討を進める必要。

経済安全保障推進法の附帯決議

衆議院内閣委員

十四　国際共

取り扱う者の

含めて、必要

参議院内閣委員

二十一　国際

を取り扱う者の

を含めて必要な措置を講ずること。

附帯決議：民間人も含めた認証制度
国家安全保障戦略：情報保全の強化
主要国、産業界：ニーズを踏まえる

国家安全保障戦略（令和4年12月16日 国家安全保障会議決定・閣議決定）

Ⅵ 我が国が優先する戦略的なアプローチ

2 戦略的なアプローチとそれを構成する主な方策

(5) 自主的な経済的繁栄を実現するための経済安全保障政策の促進

エ （前略）また、**主要国の情報保全の在り方や産業界等のニーズも踏まえ、セキュリティ・クリアランスを含む我が国の情報保全の強化に向けた検討を進める。**

セキュリティ・クリアランス有識者会議
「中間論点整理（骨子）」

1．セキュリティ・クリアランス制度に関する必要性
2．新たな制度の方向性
3．具体的な方向性
4．その他

（2023年６月6日

地方公務員法
自衛隊法
外為法
特許法
労働法
…

経済安保法

我が国の情報保全の枠組みの例

□ 我が国では、政府・民間それぞれが持つ機微な情報の保護について様々な場面・態様に応じた枠組みが存在。

	枠組み	概要
政府が持つ情報	国家公務員法	■ **職務上知ることのできた秘密**を守る義務（守秘義務）について規定　※漏えい時の罰則あり
	情報公開法	■ 行政文書の開示請求があった際、不開示となる情報の類型（国の安全、犯罪の予防など）を規定
	公文書管理制度	■「行政文書の管理に関するガイドライン」において、秘密文書（特定秘密以外の公表しないこととされている情報が記録された行政文書のうち秘密保全を要する行政文書（**極秘文書・秘文書**））の管理等について規定
	特定秘密保護法	■ 我が国の安全保障に関する情報のうち特に秘匿することが必要であるもの（**特定秘密**）の保護について規定 ※特定秘密の取扱者に対する適性評価、漏えい時の罰則あり
	防衛上の情報保全	■ 日米相互防衛援助協定等に伴う秘密保護法に掲げる米国から供与された装備品等の性能等（**特別防衛秘密**）の保護について規定 ■ 国の安全又は利益に関わる事項であって、関係職員以外に知らせてはならないもの（**秘**）の保護について規定 ※いずれも秘密取扱い資格の確認、漏えい時の罰則あり（現在提出中の法案において契約事業者が取扱う装備品等秘密に係る守秘義務についても規定）
	安全保障貿易管理	■ 国際的な平和及び安全の維持を妨げることとなると認められる特定の**貨物**の輸出や**技術**の提供を行おうとする者に対し、外為法に基づき許可取得を義務付け　※罰則あり
民間が持つ情報	不正競争防止法	■ 事業者が持つ秘密情報（**営業秘密**）が不正に持ち出された場合等の法的保護について規定　※罰則あり
	技術情報管理認証制度	■ 事業者が保有する**機微技術情報**（研究成果、事業活動に有用な情報等）の適切な管理を担保し流出を防止するため、技術等情報を適切に管理している事業者を産業競争力強化法に基づき認証
	原子炉等規制法	■ **特定核燃料物質の防護に関する秘密**について、原子力事業者・従業員等に対する守秘義務を規定。信頼性確認を行った上で秘密を業務上知り得る者を指定するなどの防護措置を講じることを原子力事業者等に義務付け ※守秘義務違反及び防護措置に係る是正命令違反に対する罰則あり

5

１．セキュリティ・クリアランス制度に関する必要性

■主要国と異なり、同法（特定秘密保護法）では政府が特定秘密として指定できる情報の範囲が、防衛、外交、特定有害活動、テロの４分野に限定。経済安全保障に関する情報は必ずしも保全の対象でない。
■経済関係省庁や防衛産業を超えた民間における情報保全強化が必要。
■機微な情報を扱う者について信頼性の確認を行う必要があるほか、情報保全全般が米国等主要国との間でも認められる必要がある。
■企業からのニーズ

２ 新たな制度の方向性

（１）ＣＩを念頭に置いた制度
（２）主要国との間で通用する実効性のある制度
（３）政府横断的・分野横断的な制度の検討
　　セキュリティ・クリアランス制度に関
　　する必要性

CI：機密情報（Classified Information）

３　具体的な方向性

（１）情報指定の範囲ＣＩを念頭に置いた制度
（２）信頼性の確認（評価）とそのための調査
（３）産業保全（民間事業者等に対する情報保全）
（４）プライバシー等との関係
（５）情報保全を適切に実施するための官民の体制整備
（６）ＣＩ以外の重要な情報の扱い
　　CI以外とは米国における管理された非格付け情報
　　CUI:（Controlled Unclassified Information）
（７）信頼性の確認に係る理解の促進

現行

調査事項（法律）

①特定有害活動及びテロリズムとの関係に関する事項

②犯罪及び懲戒の経歴に関する事項

③情報の取扱いに係る非違の経歴に関する事項

④薬物の濫用及び影響に関する事項

⑤精神疾患に関する事項

⑥飲酒についての節度に関する事項

⑦信用状態その他の経済的な状況に関する事項

※①には、家族（配偶者・父母・子・兄弟姉妹、配偶者の父母及び子）及び同居人の氏名・生年月日・国籍・住所を含む

調査の実施（運用基準）

●本人による質問票
○必要に応じ旅券の写し等
●上司等の本人をよく知る者による調査票

↓ 疑問が生じた場合

○上司、同僚その他知人への質問
○人事管理情報による確認
○本人に対する面接

↓ これらを行っても疑問が解消されない場合

○公務所・公私の団体への照会

現行

特定秘密の指定の状況等

2 特定秘密の取扱いの業務を行うことができる者の数

行政機関の職員等の数

○ 適性評価の結果、特定秘密の取扱いの業務を行うことができる行政機関の職員等の数は、令和元年以降概ね約13万人で推移

○ 令和３年末時点における内訳は、内閣官房885人、警察庁3,558人、公安調査庁245人、外務省1,229人、防衛省122,282人、防衛装備庁890人。経済官庁は、総務省73人、財務省219人、経産省144人。

適合事業者の従業者の数

○ 適性評価の結果、特定秘密の取扱いの業務を行うことができる適合事業者[illegible]和元年以降概ね約3,000人台で推移。

○ 令和３年末時点における内訳は、内閣官房1,060人、外務省38人、文部科学省20人、防衛省952人、防衛装備庁1,374人。

※特定秘密の取扱いの業務を行うことができる者の数。()内は内数で適合事業者の従業者数を指す。

行政機関名	令和３年末	行政機関名	令和３年末	行政機関名	令和３年末	行政機関名	令和３年末
内閣官房	1,945 (1,060)	法務省	23 (0)	水産庁	52 (0)	防衛省	123,234 (952)
内閣法制局	3 (0)	入管庁	36 (0)	経済産業省	144 (0)	防衛装備庁	2,264 (1,374)
内閣府	107 (0)	公安調査庁	245 (0)	エネ庁	14 (0)	合計	134,297 (3,444)
警察庁	3,558 (0)	外務省	1,267 (38)	国土交通省	100 (0)		
金融庁	9 (0)	財務省	219 (0)	気象庁	12 (0)		
消費者庁	16 (0)	文部科学省	97 (20)	海上保安庁	754 (0)		

9

指定者13万人
防衛省12万人

「経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議」2023.5.26資料より

SC有識者会議のSCの定義

指定する

SCとは「国家における情報保全措置の一環として、
①政府が保有する安全保障上重要な情報を指定することを前提に、
②当該情報にアクセスする必要がある者（政府職員及び必要に応じ民間の者）に対して政府による調査を実施し、当該者の信頼性を確認した上でアクセス権を付与する制度、
③特別の情報管理ルールを定め、当該情報を漏洩した場合には厳罰を科すことが通例」

（「SC有識者会議」（第2回資料）

監視システムが付随する

適正評価の基本的考え方

ア 情報を自ら漏らすような活動に関わることがないか
イ 情報を漏らすよう働き掛けを受けた場合に、これに応じるおそれが高い状態にないか
ウ 情報を適正に管理することができるか
エ 規範を遵守して行動することができるか
オ 自己を律して行動することができるか
カ 職務の遂行に必要な注意力を有しているか
キ 職務に対し、誠実に取り組むことができるか

内面の自由の侵害の危険性

「特定秘密の指定及びその解除並びに適性評価の実施に関し統一的な運用を図るための基準」p.30　より

■一特定有害活動（公になっていない情報のうちその漏えいが我が国の安全保障に支障を与えるおそれがあるものを取得するための活動、核兵器、軍用の化学製剤若しくは細菌製剤若しくはこれらの散布のための装置若しくはこれらを運搬することができるロケット若しくは無人航空機又はこれらの開発、製造、使用若しくは貯蔵のために用いられるおそれが特に大きいと認められる物を輸出し、又は輸入するための活動その他の活動であって、外国の利益を図る目的で行われ、かつ、我が国及び国民の安全を著しく害し、又は害するおそれのあるものをいう。別表第３号において同じ。）及びテロリズム（政治上その他の主義主張に基づき、国家若しくは他人にこれを強要し、又は社会に不安若しくは恐怖を与える目的で人を殺傷し、又は重要な施設その他の物を破壊するための活動をいう。同表第４号において同じ。）との関係に関する事項（評価対象者の家族（配偶者（婚姻の届出をしていないが、事実上婚姻関係と同様の事情にある者を含む。以下この号において同じ。）、父母、子及び兄弟姉妹並びにこれらの者以外の配偶者の父母及び子をい　う。以下この号において同じ。）及び同居人（家族を除く。）の氏名、生年月日、国籍（過去に有していた国籍を含む。）及び住所を含む。）
■二犯罪及び懲戒の経歴に関する事項
■三情報の取扱いに係る非違の経歴に関する事項
■四薬物の濫用及び影響に関する事項
■五精神疾患に関する事項
■六飲酒についての節度に関する事項
■七信用状態その他の経済的な状況に関する事項

「特定秘密の指定及びその解除並びに適性評価の実施に関し統一的な運用を図るための基準」p.30　より

研究インテグリティの確保に係る対応について

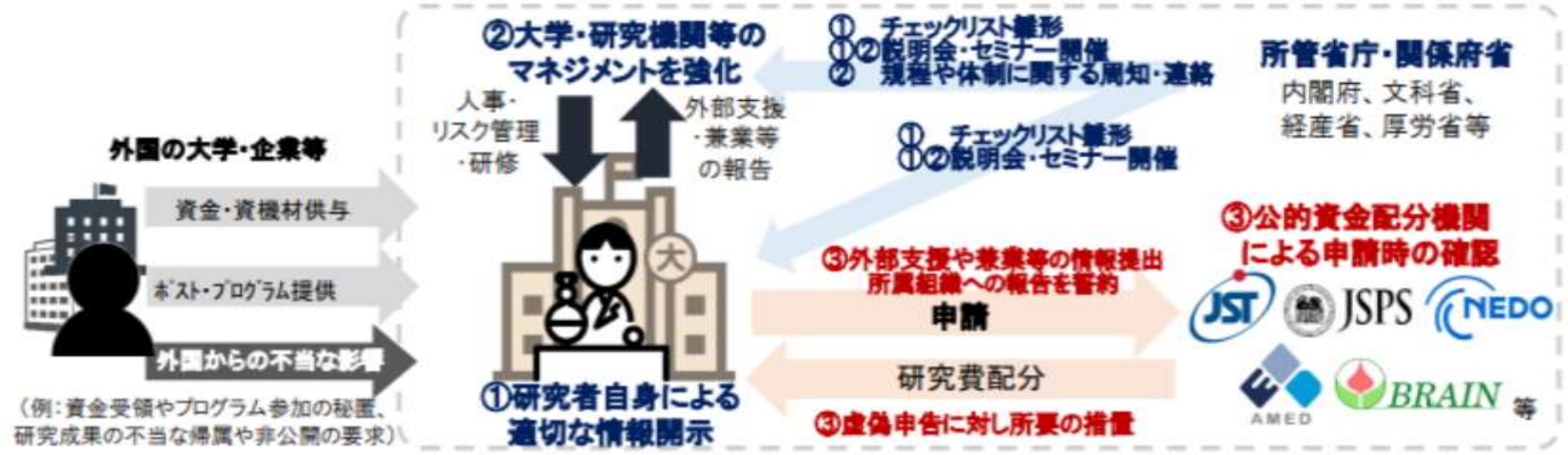
政府としての対応方針（2021年4月27日統合イノベーション戦略推進会議で決定）

※大学・資金配分機関の専門家等から構成された有識者検討会の提言（2021年3月公表）を踏まえた方針

①研究者自身による適切な情報開示
- 研究者、所属機関向けのチェックリスト雛形を作成、公表・配布【内、文科等】
- 研究者、所属機関等への説明会・セミナーを開催【内、文科等】

②大学・研究機関等のマネジメントを強化
- 研究者、所属機関等への説明会・セミナーを開催【内、文科等】
- 関係の規程や体制の整備に関する周知・連絡【所管省庁】
  （→ 令和4年度中にフォローアップを実施）

③公的資金配分機関による申請時の確認
- 競争的研究資金に関するガイドライン等を年内早期に改定【内、関係省庁】
  - 国外も含む外部からの支援や兼業等の情報の提出、所属機関への適切な報告の誓約を求める
  - 利益相反・責務相反に関する規程の整備の重要性を明示、必要に応じて状況確認
  - 虚偽申告に対し、公表、不採択・採択取消し、研究費返還、5年間の応募制限
    （2022年度の公募から反映）



研究インテグリティの確保

- ●研究者の情報開示
- ●競争的研究資金の申請時の確認

6　米国のSC制度と科学者

米国のSC制度　大統領令　1

【原爆開発】
クラウス・フックス、ローゼンバーグ夫妻事件
1951 年以降は軍事研究以外に機密指定を拡大
【機密指定】
大統領令第 13526 号 （2009年：オバマ大統領）
「国家安全保障に関連する科学的，技術的又は経済的事項に関する情報」（第14 条(ｅ)）
連邦政府は，研究内容がこの大統領令に該当する場合，研究は機密指定を受け，これに従事する 研究者はセキュリティクリアランスの取得が必要 .

米国のSC制度　大統領令　２

- 「連邦政府の直接雇用者、民間請負業者の個人が秘密情報を取り扱う適性があることを政府が認定すること」
- 「連邦政府の職員もしくは連邦政府と連携する民間事業者の資格」　need-to-know

１）機密指定制度

２）大統領令 第12968号（クリン トン大統領）　1995．８
　　第13526号（オバマ大統領）　2009.12

３）申請に三つのランク
　（Top Secret機密、Secret極秘、Confidential秘）

出典：「セキュリティー・クリアランス・プロセスよくある質問」米国議会調査局
https://crsreports.congress.gov/product/pdf/R/R43216/7

米国のSC制度と研究者　①

①科学技術の発展に研究成果の自由な発表やオープンな研究環境が不可欠
②明らかに国家安全保障と関係のない基礎的な研究の機密指定を禁止
③研究成果が研究コミュニティ内で広く公表・共有されるものを「基礎的研究（ Fundamental Research ）」と定義し，その成果は原則として政府による公開制限を受 けない
④大学では機密指定された研究を一般のキャンパス内で行うことを禁止

米国のSC制度と研究者　②

⑤物理的に隔離された研究施設でSCを受けた研究者，管理者，建物で研究実施
⑥研究成果の公開の制限
⑦業績評価の機会がなくなる1982年全米科学アカデミー等が設置した**研究者委員会**が提言
機密指定とキャンパス外研究施設使用
2000年代多発テロ事件を契機に生物化学兵器（炭そ菌）など生命科学が機密指定バイオテロ対策

米国が導入している制度の概要

機密情報の区分	• Top Secret（トップ・シークレット） • Secret（シークレット） • Confidential（コンフィデンシャル）
機密情報の対象	❶ 軍事計画・兵器システムまたは軍の運用 ❷ 外国政府情報 ❸ インテリジェンス活動や情報源、暗号など ❹ 機密情報源を含む連邦政府の外交関係または対外活動 ❺ 国家安全保障に関連する**科学的・技術的・経済的事項** ❻ 核物質または核施設の防護策のための政府プログラム ❼ 国家安全保障に関連するシステム、設備、インフラ、防護サービスなどの脆弱性または能力 ❽ 大量破壊兵器の開発など
資格付与対象者	原則として米国市民である政府職員など。政府との契約などにより機密情報に触れる場合、民間人にもクリアランスが付与されうる
人物調査の質問例	• 氏名 • 住所 • 家族情報 • 海外渡航歴 • 精神状態、薬物使用歴、飲酒状況など • 税金滞納、破産歴、ギャンブルなどの経済状況 • テロ組織への関与

（注）内閣府作成の資料による

日経新聞2023.7.28 https://www.nikkei.com/article/DGXZQOUA196PB0Z10C23A7000000/

7　米国にならうSCの法制化

急がれるSC制度化のわけ

経済の多元化・強靭化と称して…

- 日米兵器共同開発・日米兵器及び兵器体系のシームレス化対応
- 米国からの強い要求（日米安全保障協議委員会２+２）

日本のSC制度の方向

■機密レベル３段階　米国同様⇒機密・極秘・秘（ / CUI）
■特定秘密保護法を本格的SC制度へ転換
- 対象者の拡大（民間人・研究者・技術者・事業者・SC保有者の上司及び管理者）
- 研究者の発表の自由はく奪、研究環境の隔離
  ⇒防衛研究所・シンクタンク、DARPA型研究所が受け皿
- 特定秘密の拡大
  ⑤特定重要物質・サイバーセキュリティ・インテリジェンス
  ⑥基盤インフラ
  ⑦先端機微技術・デュアル技術
  ⑧秘密特許関係等々

8　おわりに
ー企業は急いでいるか

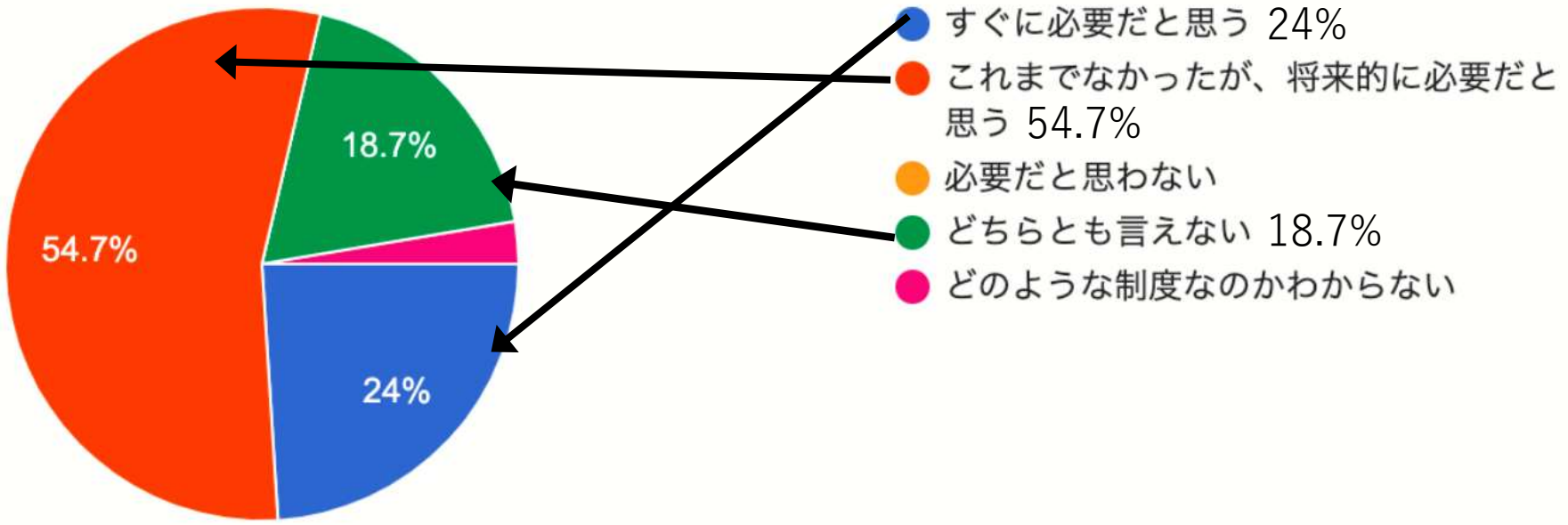
『東洋経済』SC制度は喫緊の課題」

東洋経済Web　2月６日「日本の経済安全保障」主要100社が答えた実状」

https://toyokeizai.net/articles/-/650258?page=3より作成

https://apinitiative.org/GaleyudaTuFo/wp-content/uploads/2023/02/100%E7%A4%BE%E3%82%A2%E3%83%B3%E3%82%B1%E3%83%BC%E3%83%88%E5%85%A8%E4%BD%93%E7%89%88-2.pdf

13.　日本にセキュリティ・クリアランス制度が必要だと思いますか。(75 件の回答)



https://apinitiative.org/GaleyudaTuFo/wp-content/uploads/2023/02/100%E7%A4%BE%E3%82%A2%E3%83%B3%E3%82%B1%E3%83%BC%E3%83%88%E5%85%A8%E4%BD%93%E7%89%88-2.pdf

14.　日本に現状セキュリティ・クリアランス制度がないことにより、参画することのできなかった案件や会議などはありますか。当てはまるもの全てをお選びください。(71 件の回答)

これまでなかったが、将来的に参画できないことが予想される	56.3%
これまでもなく、今後も特に想定されない	40.8%
他国の企業と組んで他国政府のプロジェクトに参画できない	1.4%
他国の政府が行う事業に入札できない	0%
他国企業との共同研究に参加できない	0%

https://apinitiative.org/GaleyudaTuFo/wp-content/uploads/2023/02/100%E7%A4%BE%E3%82%A2%E3%83%B3%E3%82%B1%E3%83%BC%E3%83%88%E5%85%A8%E4%BD%93%E7%89%88-2.pdf

ご清聴
ありがとう
ございました