経済安全保障上の重要政策に関する提言

令和 5 年 3 月 28 日
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

国家安全保障戦略が新たに決定された。初版となる同戦略は、第二次安倍政権の発足に伴い積極的平和主義を基本理念として策定されたが、爾来、加速度的に厳しさを増す安全保障環境に対応するため、同戦略に基づき様々な政策が実行され、大きな成果を得てきた。一方で、国際政治の不安定化と、産業構造の複雑化やテクノロジーの高度化が相まって、安全保障のすそ野が劇的に広がり、経済分野を含めた多岐の分野にわたる安全保障を国家として整合的に確保する必要性が増していた。

特に中国が軍民融合で先端技術開発を進める一方で、米国は安全保障を理由に経済分野の政策運用の厳格化を進めており、日本を含む第三国への影響が拡大する事態となっている。日本は、自由で開かれたインド太平洋構想に代表されるように、自由かつルールベースの国際秩序を希求し、各国の橋渡しの役割を担いつつ国際連携強化を模索しているが、未曽有の環境変化に対処する能力を持たなければならない。初版の国家安全保障戦略でも、そうした時代の到来をある程度予想し経済分野の対応の必要性を謳っていたが、より体系的な戦略が必要となっていた。

自民党経済安全保障推進本部（以下、経済安保本部）は、こうした認識に基づき、累次にわたる提言で、国家安全保障戦略への経済安全保障視点の反映や「経済安全保障戦略」の策定を求めてきた。今回の新たな国家安全保障戦略の決定で、経済安全保障が明記されたことは大きな一歩として評価するものであるが、一方で、経済安全保障分野は民間が主たる担い手になること、従って政府と民間の対話と協調が今まで以上に重要であること、に鑑み、潜脱を許さない限りにおいて、より具体的な経済安全保障戦略を可及的速やかに策定することを求めるものである。

新たな国家安全保障戦略の目標を達成するためには、具体的な政策の実行が必要不可欠である。経済安保本部は、これまで多岐にわたる具体的な政策の実行を政府に求めてきたが、その中でも特に重要なものとして、（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、を求めてきた。本提言は、主にこの3点につき、それぞれについて具体的な実装の方向性に関する提言を行うものである（今後も進捗を見て適宜提言する）。

（1）いわゆる「セキュリティ・クリアランス（SC）」制度の導入

（課題認識）

国民の生存若しくは国民生活や経済活動に重大な影響を及ぼし得る物資や技術など、経済安全保障に関わるものを含め、重要な情報を保全し、情報を取り扱う者の適性を評価し認証を与えるいわゆるSC制度の整備は、先進諸外国では既に整備されており、わが国も経済安全保障情報の流出を防ぐ意味でも、また情報保全の取組における国際的整合性や実質的同等性の観点からも、焦眉の急を告ぐ課題である。

（具体例）

例えば米国などでは、テロ対策の意識の高まりから重要な施設への受け入れを厳格化しており（例えばBSL4施設）、日本人研究者がそれらへのアクセスを制限され研究参画機会を逸している可能性は否定できない。また、同志国政府によって我が国産業界に対して共同事業開発の打診があったとしても、SC制度がない以上参画し難い状況が生まれ、実質的にビジネスチャンスを逸している可能性もある。

（国際連携）

いわゆるファイブアイズと呼ばれる同盟国・同志国間では、SC制度を含む情報保全制度全体の実質的同等性を踏まえ、need-to-know ベースで相互に必要な情報をスムーズに共有することで、国際共同事業やサイバーセキュリティなど経済安全保障分野を含め、オペレーションを共同で実施し得る体制を構築しているものと思われ、結果的に同盟強化にも資するものとなっていると考えられる。

（現状の制度）

一方、日本では、防衛・外交・特定有害活動（スパイ）・テロという、いわば伝統的な安全保障分野については、特定秘密保護法によって、対象情報の指定と管理やSC付与について、罰則付きの制度で担保しているが、対象情報の機微性の程度と分野等が限定されている。

（民間ニーズ）

こうした背景により、産業界や有識者から、「機微情報をいかにして守るか。国際協力の拡大に備え、他国と同等の効果を有する制度とすることが重要」[1]、「機微技術に関する国際共同研究開発に我が国企業が参加できないという指摘もあり、産業保全に関する今後の対応について検討すべき」[2]、「相手国から信頼されるに足る、実効性のある情報保全制度の導入を目指すべきである」[3]、「民間保有の機微技術や情報に関して、きちんとした適性評価制度を持っているとは言いがたい」[4]、「（制度の）導入に賛成する回答が78．7％に達した。（中略）最先端の技術へのアクセスにおいて大きく後れをとっている可能性を想定したい」[5]、など、経済安全保障分野でのSC制度や情報保全制度全般の改善を求める声が出ている。昨年5月に成立した経済安全保障推進法の審議では、与

[1] 2020年8月　自民党新国際秩序形成戦略本部　経団連ヒアリング資料
[2] 2019年10月　産業構造審議会通商・貿易分科会安全保障貿易管理小委員会中間報告
[3] 2022年2月　経団連「経済安全保障法制に関する意見―有識者会議提言を踏まえてー」
[4] 2022年9月　読売新聞　地球を読む　安保の新領域　技術窃取の試み　常態化…　北村滋
[5] 2023年2月6日　「日本の経済安全保障」主要100社が答えた実情　地経学研究所　鈴木均

野党からSC制度創設を求める声が相次ぎ、附帯決議に記されたことは記憶に新しい[6]。

（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」とされた。本SC提言はその具体的内容を提言するものである。

（制度のスコープ及び実装の方向性）

- 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SC制度を含む情報保全制度とすること。
- SC制度は、サイバーセキュリティ（CS）面での情報保全とも密接不可分の関係にあるため、整合性を十分に確保すること。
- 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を進めること。
- 産業界等からのニーズを踏まえるべく新たに設置した有識者会議において、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。その際、法律名称も本提案の趣旨目的が包含されるものにすること。

（情報区分）

- 対象となる情報区分として、現行の機密性3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すること（表1のA～E）。
- 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し、必要な制度設計を講じること。
- 情報区分Dは重要インフラ事業者等を念頭に、事業者とも協議を十分に重ね、国際的に均衡のとれる必要な範囲で限定的に設定し担保すること。
- 情報区分Eについては、ガイドラインを設定するなど、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とすること。

（情報分野）

- 対象となる分野は、経済安全保障に関連した事業に関わる情報など、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すること。

（情報区分設計と対象情報特定）

- 各省庁において保護すべき情報を特定し、内閣官房において情報区分の詳細設計を行うこと。

---

[6] 経済安全保障推進法・衆議院附帯決議第14項「国際共同研究の円滑な推進も念頭に、我が国の技術的優位性を確保、維持するため、情報を取り扱う者の適性について、民間人も含め認証を行う制度の構築を検討した上で、法制上の措置を含めて、必要な措置を講ずること。」（参議院附帯決議も同旨）

なお、表1は現行の情報区分や分野の概略を便宜上示したものである。

➢

（情報保全及びSC制度）

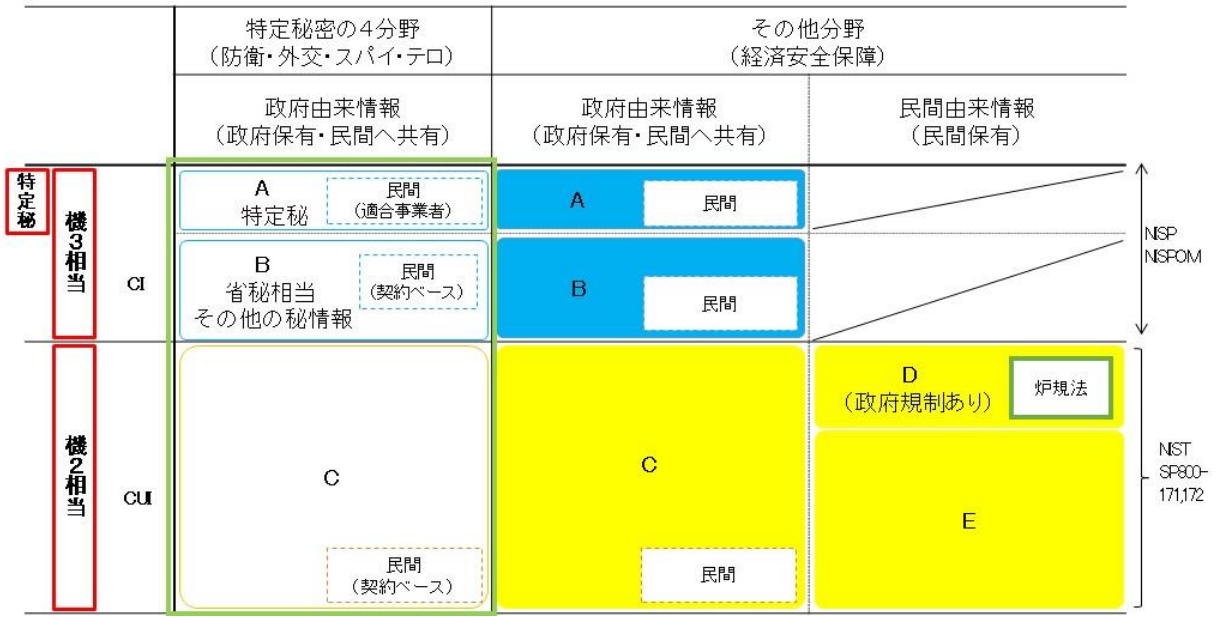
- 詳細設計された情報区分に応じた、情報アクセス権限（SCレベル）の段階設定、応分の罰則制度設計、本人同意を前提としたバックグラウンドチェック（BC）の対象範囲と調査深度の詳細設計を行うこと。
- CS分野も含め、同盟国・同志国との実質的同等性の観点も踏まえた制度整備を図ること。
- SC付与は、属人的で「ポータブル」な運用とすること。
- 民間事業者の負担となる領域では合理的な範囲内で支援制度を検討すること。

（体制整備）

- SC 制度を含めた情報保全制度を実施するにあたり、政府一体となって十分な体制整備を行うこと。

表1. 現行の情報区分と分野及び保全措置（脚注参照[7]）

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）	



[7] CI)Classified Info.、CUI)Controlled Unclassified Info.、機密性3）特別防衛秘密や外交文書の機密・極秘・秘など、機密性2）犯罪・治安・個人情報など不開示対象となりうるもの、A,B)cf.NISP，C,D)cf.NIST SP800-171/172、C，D，E）CUI若しくはCUI相当の情報には、米国を参考にすれば、重要インフラ関連、輸出管理、金融、インテル、国際協定、法執行、天然・文化資源、原子力、個人情報、政府調達、営業秘密情報、統計、税、輸送などが入り得ると想定。

(2) サイバーセキュリティ(CS)の確保

(課題認識)

サイバー攻撃の規模・烈度が劇的に増大しており、手法も複雑化・多様化している。経済活動や国民生活に対して甚大な影響を及ぼしかねず、経済安全保障の観点で極めて深刻な状況となっている。例えばロシアの侵略行動で明らかになったように、武力攻撃事態に至る前の段階において、軍事目的達成手段の一環として烈度の高いサイバー攻撃が本格的に行われるようになっており、政府機関・重要インフラ・基幹産業等のサーバデータ窃取・改竄、運用妨害・無力化など、国の安全を揺るがしかねない事態に発展するケースもある。

(ACDの必要性)

サイバー攻撃は、その匿名性・非対称性・越境性などから攻撃側が圧倒的に有利とされる。攻撃者は悪意のないサーバを踏み台にして攻撃をしかけてくる可能性などもあり、発信源隠匿・偽装は容易である。こうした中、従前の受動的防御―パッシブ・サイバー・ディフェンス(PCD)による対策には限界があり、攻撃者のアトリビューションや無力化、攻撃の影響の軽減等を含め、攻撃前の事前予防から事後対処まで能動的防御―アクティブ・サイバー・ディフェンス(ACD)によらなければ到底対抗できない。

(多様主体との連携)

また、そもそもCS対策は、インシデント情報の共有の意味でも、インテリジェンス情報の共有の意味でも、共同オペレーションの意味でも、諸外国との連携協力が不可欠となる。そのためには前述のSC制度を含む包括的な情報保全体制の整備が必要となる。また、ACDを含め、諸外国と実質的に同等の機能を有するCS体制を構築し、それにより技術力の獲得・向上を図り、国際連携を促進するメカニズムを構築する必要がある。また、民間企業や大学など、民間の多様な主体との連携協力も最重要課題の一つである。インシデント情報を常時共有し、経済安全保障上のリスクが顕在化する前に対処できる能力の構築が必要である。

(民間ニーズ)

こうしたサイバー分野の後進性については、産業界からも指摘がなされており、例えば経団連は、経済安保本部会合の場で、米国がNIST標準により、インシデント防止からインシデント対処まで幅広くCS対策を実施していることに触れ、現状の日本のCS対策の実施範囲の狭さを指摘している[8]。

(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、能動的サイバー防御の実施のための体制整備が謳われ、新組織の設置、必要な法制度の整備が明記された。本CS提言は、その具体化に関し、ACDの実施等を中心に必要な体制と機能の骨格を提言するものである。

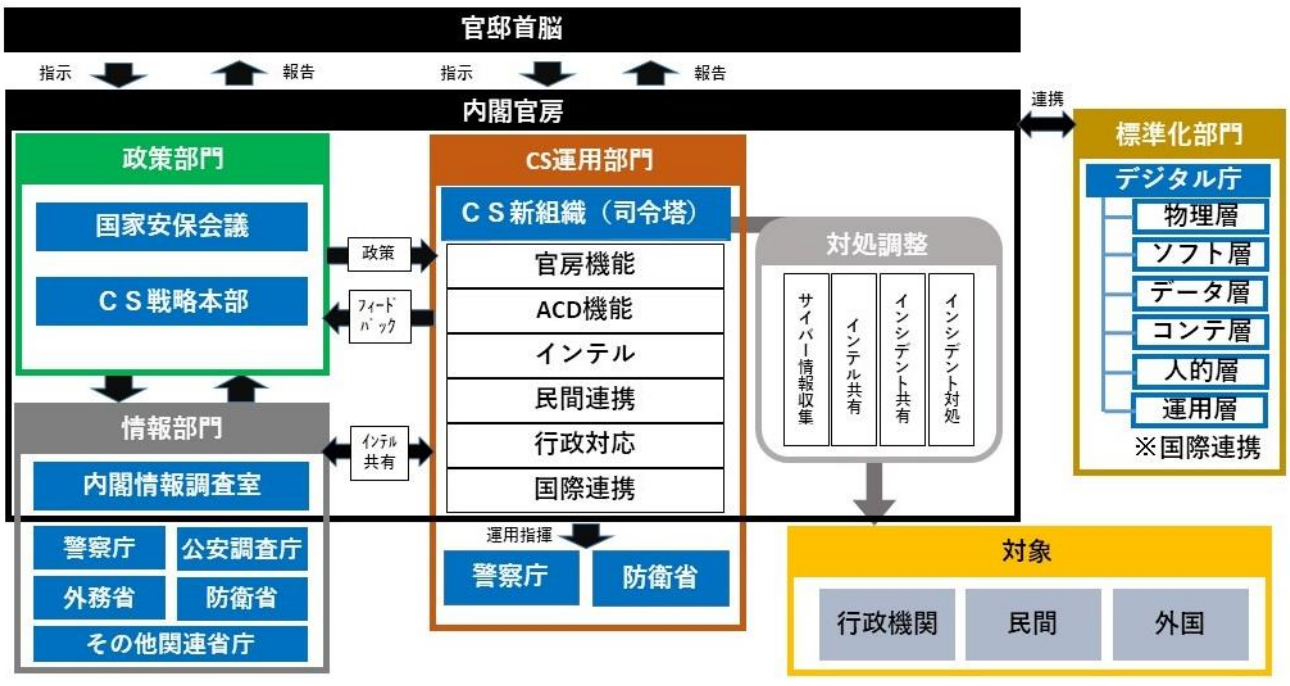
[8] 2020年8月　自民党新国際秩序形成戦略本部　経団連ヒアリング資料

（制度のスコープ及び実装の方向性）

- 有事平時に関わらず、インシデントの事前予防から事後対処までのあらゆる状況を対象とし、攻撃者のアトリビューションや無力化、攻撃の影響の軽減等のフルスペックのACDを含む、包括的CS対策の実施権限を実効的に担保する制度とすること。
- 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の共有、共同オペレーションを可能とする実施権限を実効的に担保する制度とすること。
- CSは、情報保全制度とも密接不可分の関係にあるため、整合性を十分に確保すること。

（政府の体制・ガバナンス）

- 内閣サイバーセキュリティセンター（NISC）は発展的に改組し、CS戦略本部の事務機能（政策企画立案調整）とは別に、全く新しく実運用機能を内閣官房に設置すること。
- 新組織は、ACDの実施機能、民間及び行政セクターのCS対処機能、インテリジェンス収集分析共有機能、官房機能等を設置し、実効的な権限を付与すること。
- その他、CS分野の政策の一元的な総合調整機能、国際連携の推進等に関する一元的な司令塔機能を整備すること。
- 新組織には、必要に応じて本提言のSCを含む情報保全制度を適用すること。
- 新組織は、拡大インテリジェンスコミュニティに加えること。
- 新組織と、関連組織のCS戦略本部（CS政策司令塔）、NSS（国家安全保障司令塔）、デジタル社会推進会議（標準化を含むデジタル政策司令塔）との関係については、政策と運用の適切な連携を念頭に置き、関係を整理すること。
- 防衛省・自衛隊及び警察庁等については、それぞれの目的に応じたACD実施が可能となるよう制度設計を行うこと。
- ガバナンス体制を構築し、制度的に担保すること。



（アクティブ・サイバー・ディフェンス（ACD）機能）

- ACDに関する実施権限などの法整備[9]、既存関連法令との関係整理[10]を含め、有識者会議を設置するなどして十分に審議を行い、実効的な実施権限を担保する制度を整備すること。国内と国外のそれぞれに対するACD実施について、違法性阻却その他の法的正当化の必要性も含め、国際法や国内法の制約に対する法的整理を早急に行うこと。ACDの機能としては、下記を検討すること。
  - 攻撃者が悪用するサーバの探知のための情報収集
  - 攻撃を防ぐための手段
  - サイバー・インテリジェンス収集分析
  - 民間セクターのインシデント調査・支援・対処調整
    官民情報共有等の連携強化

（インテリジェンス機能）

- 関係諸機関とのインテリジェンス共有
- サイバー・インテリジェンス収集集約分析

（民間セクターCS強化機能）

- 民間セクター向けのセキュリティ標準群[11]の見直し
- 民間セクターのCS強化、
  経済安保推進法を通じた基幹インフラ防護やサプライチェーン強靱化
- 民間における情報保全の枠組み強化
- 民間セクターのインシデント調査・支援・対処調整（再掲）
  官民情報共有等の連携強化（再掲）

（行政セクターCS強化機能）

- 行政セクター向けのセキュリティ標準群の見直し
- 行政セクターのIT調達や運用等の検査・継続的アセスメント[12]
- 最新のセキュリティ技術の導入推進

（CS人材の強化）

- 官民CS人材の育成施策の強化

---

9 警察官職務執行法の法理をベースとしつつ、サイバー空間の警察権を担保する新しい制度を創設することが考えられる。

10 攻撃者の処罰に関する法律として、「刑法」「不正アクセス禁止法」「不正競争防止法」、事業者等に義務を課す法律として、「サイバーセキュリティ基本法」「経済安全保障推進法」「電気通信事業法、その他の事業法」「個人情報保護法」「会社法」の他、国際条約等がある。

11 物理層（技術・管理・運用等）、ソフト層（SBOM等）、データ層（情報区分とSC等）、コンテンツ層（偽情報対応等）、人的層（SC等）、運用ガバナンス層、国際連携層の各層での検討が考えうる。

12 例えば米国会計検査院（GAO）は定期的に行政システム及び運用のアセスメントを行っている。

➢ 民間の高度CS人材の政府での活用推進

(3)経済インテリジェンス(EI)の強化

(現状認識)

経済安全保障上の静的[13]及び動的[14]なリスクを的確に管理し対応するためには、民間企業や大学等を含む官民が国内外に保有する専門性の高い幅広い分野の情報(経済的威圧の政策情報、研究・技術・資源等の特性情報、貿易・投資・市場・商取引等の経済情報、人的・物的・資金的・知的・制度的な資本情報を含む有形無形の情報)を、輻輳的に収集、分析、集約、共有する必要がある。そのためには、政府内でEI情報収集の意義・目的等の共有を図る必要があるほか(経済安全保障戦略策定の意義の一つ)、各省庁のEI収集分析能力、政策部門(国家安全保障局(NSS)及び各省庁等)及び情報部門(内閣情報調査室(CIRO)及び各省庁等)の集約分析共有能力等、を強化した上で、インテリジェンス・サイクルが確実に稼働するEIエコシステムを構築するなど、従来の枠に捉われない体制及び機能の抜本強化が必要となる。

(NSS等の課題)

静的リスク管理については、平時より、NSSが中心となって各省庁からEI情報を集約分析、政策企画立案及び総合調整を行っている他、各省庁も独自に取り組んでいるが、現時点では後述のように省庁によっては経済安全保障に対する意識や対応に温度差があるほか所管省庁が明確でない場合もあるため、各省庁からのEI情報の集約が必ずしも合理的に図れていない。EI情報に関するNSSの政策機能を更に強化し、より積極的に情報部門に情報関心を示す必要がある。また、国家安全保障上の動的リスクが顕在化した際の対処については、事態室が初動の司令塔機能を担うとされているが、特に経済安全保障上の動的リスクを含む場合は、政府が一体的な初動対処を有効に行うためのEI情報の一元的集約は十分とは言えない。

(各省庁の課題)

一方で、拡大インテリジェンスコミュニティ関係省庁[15]は、所掌の範囲内で独自に情報の収集分析に取り組んでいるが、EI情報の分野は幅広く専門性も高いため、抜本的な体制強化が必要であるほか、経済安全保障政策の一体的な推進の必要からNSSやCIROとのより積極的な連携が必要である。また、それ以外の各省庁については、そもそも国家安全保障戦略上の問題意識が全ての省庁で共有されているわけではなく、前例がない未経験のリスク対応には消極的な傾向が見られる場合や、省庁内部で政策企画立案から実施までのインテリジェンス・サイクルが十分に稼働していないためEI情報が集約されていない場合など、省庁間での意識や対応に温度差やズレがある。また、国際的なEI情報収集のための人的情報収集活動が決定的に脆弱である。

(CIROの課題)

---

13 直ちに顕在化する蓋然性は低いものの、我が国に与える影響が大きく、事前に能動的に対処が必要なリスク。被害を未然に防ぐためのアクティブ・リスク・マネジメントとしての政策企画立案が必要。

14 現に何らかの影響がでており、その時点で受動的に対処が必要なリスク。起きた被害の拡大を防止し復旧するためのパッシブ・リスク・マネジメントとしての政策企画立案が必要。

15 警察・外務・防衛・公安調査・財務・金融・経済産業・海上保安の各8省庁

CIROは内閣の情報部門を司る機関であるが、Ⓐ各省庁との関係では連絡調整のみを行うこととされており[16]、情報集約が合理的に行われにくい構造にある。逆にⒷ政策部門が積極的にCIROを活用しているとは言い難い。更に、Ⓒ拡大インテリジェンスコミュニティの所掌範囲に関心が集中しており、それ以外を所掌する各省庁からの情報集約が十分でない上、Ⓓ各省庁所管の各機関からの直接のEI集約も十分でなく、また、Ⓔ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についても不十分であるといった課題がある。

（EIの抜本的強化）

経済安全保障分野のインテリジェンス能力の向上は、産業界や有識者からも指摘[17]があり、経済安全保障上の未曽有の環境変化に対処していくため、EI能力の抜本的強化を強く政府に求めるものである。

（提言の目的）

新たな国家安全保障戦略では、こうした観点に基づき、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た。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である。

（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。

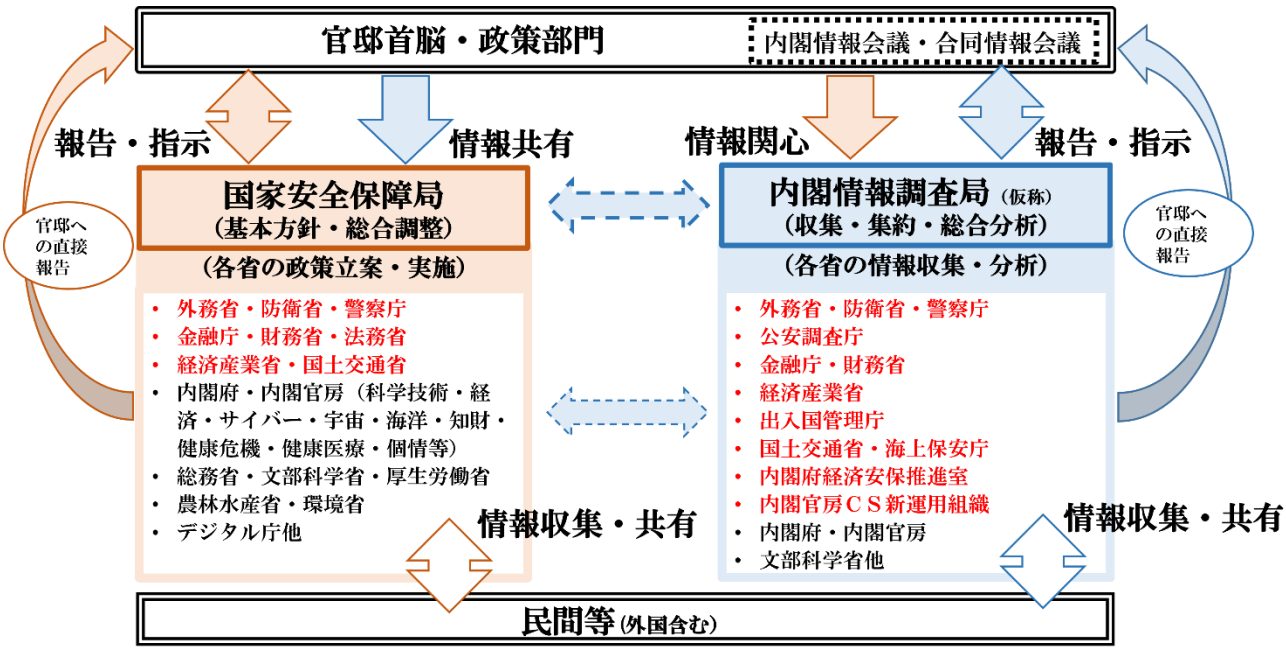
（取組の方向性について）

- 政策の実効性を担保するには、一般的に制度・運用・意識が必要とされるが、EI能力の強化は特に意識によるところが大きく、政府全体で意識共有を図ること。
- CS及びSC制度との整合性の確保を念頭に取り組むこと。
- NSS及びCIROが中心となって、EIエコシステム及び収集・集約・分析・共有の各機能の体制・能力強化に向けた全体設計を行うこと。その際、各省庁は積極的にNSS及びCIROに協力すること。また自らのEI能力向上を図ること。

① EIエコシステム構築

16 CIROは内閣官房組織令に基づき設置された組織で、連絡調整のみを行うこととされている。
17 例えば、「情報と国家―憲政史上最長の政権を支えたインテリジェンスの原点」（北村滋）、2022年2月の経団連「経済安全保障法制に関する意見―有識者会議提言を踏まえてー」がある。

NSS及びCIROは、各省庁と協力して、政策部門の情報部門への情報関心の提示の在り方、情報部門のEI情報の収集・集約・分析の在り方、情報部門の政策部門への情報伝達及び共有の在り方、各省庁が取り組むべき静的及び動的な経済安全保障リスクのEI情報の範囲、対象とすべき分野と活動（対外活動・対内活動・人的活動・サイバー活動等）、EI情報に関する人的活動の在り方、所管政府系機関との連携の在り方、各省庁と民間（所管する業界団体や物品役務調達先等）との連携の在り方、地方自治体との連携の在り方、同志国との国際連携の在り方、などをはじめ、EIエコシステムの強化に向けた取組の具体化を図ること。



② 政策部門の機能強化

（NSS）

情報部門の活動は政策部門からの情報関心の適切な提示を前提とする側面があることを踏まえ、NSSは、総合的かつ機動的な政策立案の必要から内閣官房に設置されている経済安全保障重点課題検討会議[18]などのほか、CIROも積極的に活用し、各省庁に対するリスクシナリオを含む情報関心の提示・情報集約分析・対処企画立案といった政策企画立案の運用機能の抜本強化を図ること。特にディスインフォメーションを含む新たな分野の情報を活用した戦略コミュニケーションや戦略的情報発信を含む能動的な対処能力の強化を進めること。また、動的リスクに対しては、当該検討会議にワーキングチームを設置するなど、機動的かつ柔軟な開催を可能とすること。

18 NSS経済班を事務局としたリスク情報収集・分析・集約及び政策企画立案と総合調整のための会議体で、経済安全保障担当大臣を議長とする、NSS、CIRO、外務省、防衛省、警察庁、公安調査庁、宇宙開発戦略推進事務局、NISC、デジタル庁、CSTI、財務省、金融庁、経済産業省、国土交通省、文部科学省、総務省、厚生労働省、農林水産省等、の関係局長級の会議。

（各省庁）

各省庁は、政府全体のEIエコシステム強化を念頭に、経済安全保障担当官を設置した上で、経済安全保障に係る政策部門の機能を強化し、各省庁組織内部でのローカルなEIエコシステムの構築を図ること。

③ 情報集約分析機能の強化

（NSS情報集約分析の機能強化）

NSSは、政策立案のためのEI情報集約分析機能を強化すること（②再掲）

（CIRO設置根拠及び権限の明確化）

CIROは、内閣の情報収集・集約及び分析等を司る機関であるが、より効果的に機能させるための方策を講じること。内閣法を改正し、内閣情報調査局（仮称）とすることや、各省庁または各省庁所管の政府系機関から必要な範囲で直接EI情報を集約できる仕組みの創設などが考えられる。

（CIRO体制強化）

CIROは、専門性が高く幅広い分野のEI情報を収集・集約分析するため、国際情勢の知見に加え、産業構造や企業経営、国際金融や貿易、原子力を含む科学技術やその動向、更には各国の技術開発・保有の状況や犯罪事例等に関する知見等を有する職員の拡充を図ること。

（CIROの政策部門との連携強化）

CIROは、EI情報収集・集約・分析をより合理的に進めるため、拡大インテリジェンスコミュニティのみならず経済安全保障に関係する各省庁や本提言にあるCS新組織及び内閣府経済安全保障推進室と積極的に連携すること。また、各省庁の情報保全体制整備、継続的な教育・研修への協力を行うこと。各省庁に情報関心を提示しても必要な情報が収集できない場合には、各省庁に積極的に協力を求める仕組みを構築すること。

（CIRO新たな分野への対応）

CIROは、後述するEIに関する官民ビッグデータ、サイバー空間上の情報、ディスインフォメーション等の新たな分野の情報に関する収集・集約・分析の能力構築を図ること。同時に、NSSとともに、各省庁によるOSINT機能等の総合調整、機能分担・統合化等の検討も行うこと。サイバー空間のEI能力については、本提言にあるCS新組織との連携を念頭におくこと。

（拡大インテリジェンスコミュニティ）

CS新組織及び内閣府経済安全保障推進室を、拡大インテリジェンスコミュニティに加えること。

④ 情報収集分析機能の強化

（各省庁各機関の取組）

拡大インテリジェンスコミュニティ関係省庁のみならず各省庁及び各省所管機関は、政府全体のEIエコシステム強化を念頭に、経済安全保障担当官を設置した上で、NSS及びCIROとの連携を強化し、更に本経済安保本部が累次に亘り提言を重ねてきた内容の実施を図り、それに必要なEI収集分析の機能及び体制の強化を図ること。特に人的情報収集体制の強化を図ること。また、既存関連法のみで十分なEI情報の収集が可能かどうか検討すること。

各省庁等の経済安全保障担当官は、NSS及びCIROを含む関係省庁と連携しつつ、所管政策を踏まえ、経済安全保障政策を推進する上で必要・有益なEI情報の収集分析を行うこと。

特に下記の事項に留意すること。

- 公安調査庁は、国内外の諸機関との協力関係を一層強化するとともに、我が国の脆弱性及び優位性に係る我が国内外における懸念国の動向や機微技術・先端技術・重要インフラ・重要物資サプライチェーン・重要土地等に関する情報の収集分析に全力を上げ、そのために必要な体制構築に万全を期すこと。サイバー空間やディスインフォメーション等の新たな分野の情報収集分析を更に強化すること。収集分析した情報は、NSS や CIRO などの政策部門及び情報部門や法執行機関、関係府省庁と共有すること。
- 警察庁は、諸外国政府等による違法な情報収集活動等の取り締まりを推進するとともに、捜査を含む各種警察活動に万全を尽くすこと。その過程で得られた情報を、NSSやCIROなど政策部門及び情報部門に必要な限り十分に共有し、経済安全保障の一体的な推進に繋げること。加えて、上記の公安調査庁の項で掲げた内容と同様の取り組みを行うこと。
- 外務省は、経済安全保障政策室のEI情報収集及び省内EI情報集約及び分析体制を着実に整備すること。主要な在外公館における経済安全保障担当官の設置、他省庁と連携した諸外国在京大使館との連携等を図ること。
- 防衛省は、情報本部の体制を強化すること。サイバー空間やディスインフォメーションなど新たな分野のEI情報収集分析の取り組みを含めNSSやCIROと連携をなお一層強化すること。外務省と協力し防衛駐在官の増員を図ること。更に、防衛装備品サプライチェーンリスクの把握に努めること。
- 経済産業省（資源エネルギー庁、特許庁、中小企業庁を含む）は、JETRO等の在外活動機関の体制強化を検討すること。また、貿易管理部門以外の個別産業からエネルギー・デジタルを含めた省内EI情報の集約を積極的に図るとともに、NSSと密接に連携して経済安全保障政策の一体的運用に努めること。外為法に基づく貿易管理に万全を尽すこと。
- 財務省は、マネロン・テロ資金供与・拡散金融対策にかかる内外の関係機関との更なる調整の強化、関係金融機関等に対する検査・監督上の対応、外為法の投資審査・事後モニタリングの強化等のための体制強化を図ること。輸出通関・関税情報の収集に注力し、経済安全保障情報分析センターを強化するなど、必要な体制を整備すること。国際協力銀行等の在外活動機関の体制強化を検討すること。国際銀行間資金決済等に関する情報収集に注力すること。
- 金融庁は、経済安全保障室の体制を確実に整備すること。特にサードパーティも含めた金融機関等のシステムのリスクに係るEI情報を積極的に収集すること。マネロン・テロ資金供与・

拡散金融対策のための体制強化を図ること。暗号資産取引情報等の収集に注力すること。

- 海上保安庁は、体制拡充とEI情報収集分析に努めること。NSS及びCIROとの連携を強化すること。
- 上記以外の拡大インテリジェンスコミュニティ以外の省庁は、EIの情報を扱うことに留意し、体制拡充と所管政策に関するEI情報収集分析に積極的に努めること。NSS及びCIROとの連携を強化すること。
- 特に、出入国在留管理庁等の所管行政に関する情報収集分析・関係機関との情報共有を既に推進している各省庁は、EI情報の観点からも、その取組強化に努めること。
- 特に、内閣府は、経済安全保障に係るシンクタンクを速やかに設置すること。安全保障、科学技術、防災、海洋、重要土地、宇宙活動、国境離島、知的財産、経済財政、健康医療、原子力等、重要なEI情報を扱うことに留意し、体制拡充と情報収集分析に積極的に務めること。
- また、文部科学省は、内閣府と協力しつつ、所管する大学や研究機関において、外国からの不当な影響によって研究環境基盤が損なわれないよう、国費研究については、現行の研究インテグリティの取り組みを尚一層推進し、不断の見直しを行うこと。それ以外の研究についても、国際的に信頼性のある研究環境を構築するため、例えば諸外国の貿易管理上のエンティティ―リストに係る取引が行われないよう関係法令を遵守することとともに、個別の契約に配慮しつつ、資金や共同研究者や関係事業者などの研究活動に関する情報の公開を大学ガバナンスコード改革等を通じて促し、また研究インテグリティに関わる情報を積極的に収集するよう促すこと。

（人的情報収集）

NSS及びCIROは、上記各省庁の取組とは別に、関係省庁と協力し、EI 情報収集の人的活動を強化するため、可及的速やかに体制整備を行うこと。

⑤ 官民連携及び国際連携のための情報共有メカニズムの構築

各省庁は、民間の経済安全保障に関する意識醸成の取組、民間がリスク情報に接した場合の相談窓口の設置、民間への政府側からのアウトリーチによる情報収集、などの重要な取組について、CIRO、警察庁、公安調査庁等と連携して推進すること。

NSS及びCIROは、関係省庁と連携し、経済安全保障に関する極めて重大なリスク情報に関して、民間から政府へ、また政府から民間への適切な情報の共有が確実に行われるよう、情報共有基盤構築のための制度検討を行うこと。同様に、同志国政府・産業界・研究機関との国際連携を推進するための情報共有体制を強化すること。

CIROは、各種業界団体の代表者とのネットワーキングやワークショップ等を実施するなど、民間との連携に関する各種プログラムを実施すること。更に、インテル官庁における民間人材、民間ツ

ールの積極的な活用を検討すること。

⑥ 新たな分野への対応

EIは、既存の手法だけでは限界があることに鑑み[19]、NSSは、CIRO及び各省庁と連携し、官民ビッグデータによる総合的分析（オール・ソース・アナリシス）と意思決定への活用のメカニズム構築を検討すること。また、NSS及びCIROは、本提言で示したCS新組織と連携し、サイバー空間及びディスインフォメーション情報の収集集約分析に努めること。

⑦ ガバナンス

EIは、伝統的インテリジェンス情報よりも専門性が高く幅広い分野を扱う必要があるため、EIの特性に鑑みて、十分に審議してガバナンス体制を強化すること。また、本提言で示したSC制度を含む情報保全制度の着実な構築を行うこと（SC再掲）。

⑧ 人材育成・採用

各省庁各機関は、経済安全保障担当官を設置した上で（再掲）、EI収集分析に必要な人材の育成・採用を積極的に図ること。インテリジェンス研究や教育が充実している有志国への留学・出向・国際学会参加などに積極的に取り組むこと。

（4）経済安全保障戦略の策定

政府と民間及び国際社会との連携及び意識共有のため、潜脱を許さない限りにおいて、具体的な経済安全保障の戦略を可及的速やかに策定すること。同内容の提言が複数回提出されていることに十分留意すること。その際、本提言に関わるものも含め、①官民連携の在り方と、民間の役割や責務及び取組の指針、②国際連携の在り方と、関係者の取組の指針、③各省庁や政府系機関及び地方自治体の役割や責務及び取組の指針、となるよう努めること。特に、民間の取組は、企業自体の持続可能性と企業統治を支える重要な要素であり、その取組が市場から評価されるような環境を醸成するよう努めること（例えばコーポレートガバナンスコードへの反映など[20]）。

19 米国では既に今世紀初頭にビッグデータを活用したインテリジェンス技術獲得に挑戦しており、InQTelのプログラムで政府向けインテリジェンス企業を生み出し、現在では民生分野にも進出を果たし、これらは世界有数のビッグデータ分析企業となっている。

20 自民党金融調査会は、企業の情報開示に関する提言（令和4年3月29日）で「経済安全保障の観点を踏まえ各企業にサプライチェーンの脆弱性の最小化を促す開示の在り方」検討を政府に求めている。