資料４

経済安全保障法制に関する有識者会議
基幹インフラに関する検討会合
第一回資料

令和３年12月10日

基幹インフラ機能への妨害防止に関する新しい仕組みの検討の背景

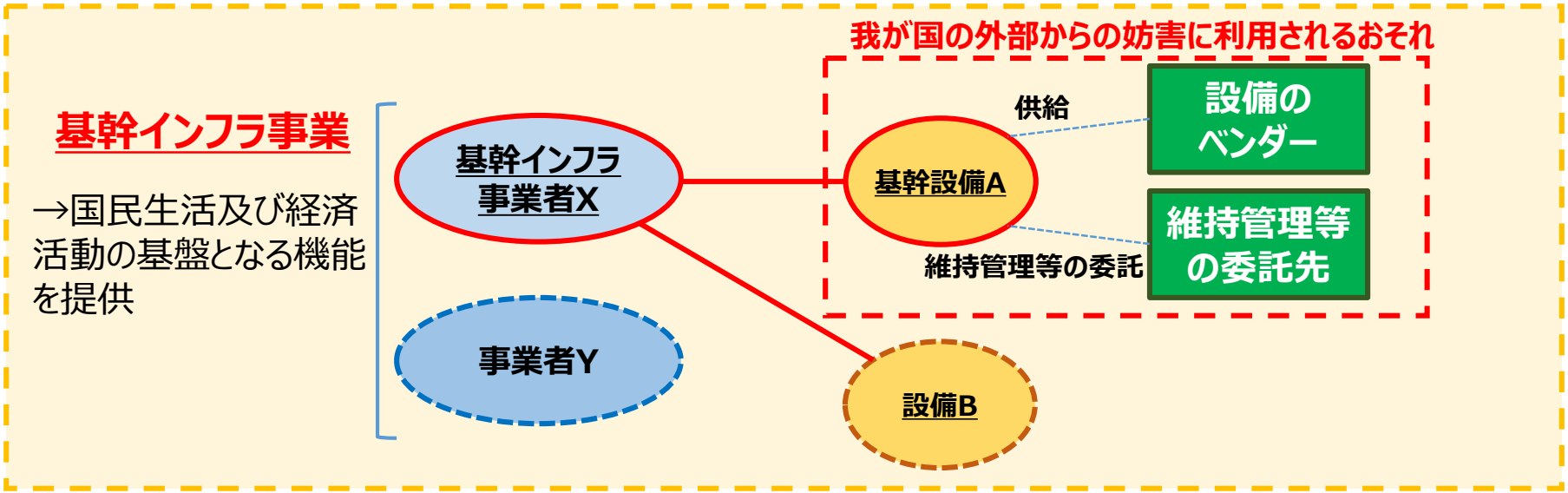
現状認識

- 世界各国において、基幹インフラ事業を対象とするサイバー攻撃により大きな社会的混乱が引き起こされる事案が多数発生。
- 我が国においても基幹インフラ事業者を含む民間企業等が対象となったとされるサイバー攻撃事案が発生しており、これら事案の中には外国政府の関与した可能性が高いと評価されている例も存在。
- 基幹インフラ事業者が果たす重要な役務の安定的な提供を妨害しようとする**我が国の外部にある主体**が、基幹インフラ事業者への設備の供給や設備の維持管理等の委託先（供給事業者）に影響を及ぼすことができる場合は、例えば、供給事業者が供給し、又は維持管理等を行う**基幹設備に不正な機能を埋め込む**ことや、**当該設備の脆弱性などの情報を把握**することなどが可能。

基幹インフラ機能への妨害防止に関する新しい仕組みの検討の背景

基幹インフラに係る安全保障上の課題

- 現状認識を踏まえると、**基幹設備を利用したインフラ機能に対する妨害行為が発生するおそれ。**



現行制度の課題

- 一方で、我が国の基幹インフラ事業を規律する**既存の業法等は、我が国の外部から行われる妨害行為を未然に防止することを目的としていない。**
- そのため、現行制度においては、設備の導入や維持管理等の委託といった通常のビジネス活動に起因するリスクに対して、そのような目的から対応することは出来ない。

基幹インフラ機能への妨害防止に関する新制度の必要性

- 有識者からのご意見や、我が国が直面する現状と課題に照らすと、**基幹インフラ機能の維持等に係る安全性・信頼性を確保するため**には、**基幹インフラ事業者が導入する基幹設備等を利用した外部からの妨害リスクを未然に防止するための何らかの仕組み**が必要と考えられる。

経済安全保障法制に関する有識者会議 第１回（令和3年11月26日）及び議事要旨から抜粋

２．今後取組を強化する上で、法制上の手当てを講ずることによりまず取り組むべき分野

サプライチェーン：国民生活や産業に重大な影響が及ぶ状況を回避すべく、重要物資や原材料のサプライチェーンを強靭化

基幹インフラ：基幹インフラ機能の維持等に係る安全性・信頼性を確保

官民技術協力：官民が連携し、技術情報を共有・活用することにより、先端的な重要技術を育成・支援する枠組み

特許非公開：イノベーションの促進との両立を図りつつ特許非公開化の措置を講じて機微な発明の流出を防止

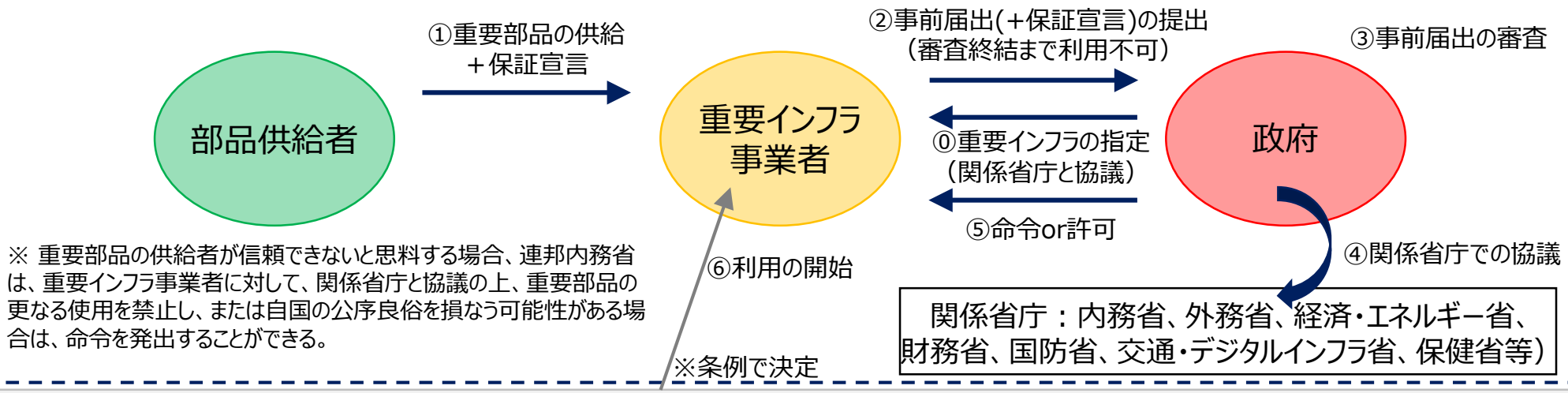
＜有識者からの主なコメント＞

- 政府には強い決意でこの政策を進めていただきたい。経済安全保障政策は、法律分野だけではなく、運用面での取組が極めて重要。
- 基幹インフラに関しては、経済効率性の原則の中でこれまで運営されてきたと認識。経済安全保障という観点は、こうした効率性の流れの中に一つの大きな軸を入れるものと捉えている。これまで技術基準や提供義務等に基づき対応してきたが、技術進歩の中で適切に対応できてきたかを振り返る必要。
- 企業は数年先を見通して投資を行うものであり、事業の予見可能性が非常に大事である。政府には、安全保障の観点から何をしてはいけないかというレッドラインを明確に示していただくことが、事業の予見可能性を確保する上で非常に重要。
- 我が国は、国際社会における法の支配の実現を基本方針としており、経済安全保障政策も国際法と整合的に行うことで、国際社会の理解も得られ、結果として様々な政策が成功することにつながる。

海外事例①（ドイツ「ITセキュリティ法2.0」）

- 2021年5月、連邦大統領の署名を経て、「情報技術システムのセキュリティを高めるための第2の法律（ITセキュリティ法2.0）」が発効。本法により、情報技術安全庁（BSI）法や電気通信法、エネルギー産業法等を改正。
- BSI法において、重要インフラ運用者は、インフラに係る重要部品の使用を開始しようとする場合、事前に政府に通知する義務が規定されている。政府部内での協議を踏まえて審査を行い、自国の公共の秩序や安全が損なわれる可能性がある場合には、命令を発することができる。
- 通知に際して、重要部品についての信頼性（重要部品が重要インフラセキュリティ・機能性等を阻害する技術的特性を有さないこと）を製造業者が保証した宣言を添付する必要がある。審査に際して、以下の点などを考慮する：
  1. 製造者が第三国政府（その他の政府機関や軍隊を含む）に直接または間接的に支配されていること。
  2. 製造者が自国、EU、NATO等の加盟国・機関の公序良俗や治安に悪影響を及ぼす活動を行っていること。
  3. 重要部品の使用が、自国、EU、NATOの安全保障政策の目的に合致していること。

【「ITセキュリティ法2.0」における重要インフラに関する機器の審査スキーム】



※ 重要部品の供給者が信頼できないと思料する場合、連邦内務省は、重要インフラ事業者に対して、関係省庁と協議の上、重要部品の更なる使用を禁止し、または自国の公序良俗を損なう可能性がある場合は、命令を発出することができる。

エネルギー（電力供給、ガス供給、一般消費者への燃料供給等）、水関係（飲料水供給、排水処理等）、食品供給、ICT（音声とデータの伝送、データの保存と処理等）、医療（医療行為、生命を直接維持する医療機器、処方薬・血液・血漿濃縮液の提供、研究診断）、金融・保険（現金供給、カード決済、伝統的決済、証券・デリバティブの清算・決済、保険サービス）、交通・運輸（航空・鉄道・内陸水路・海上輸送・道路輸送・物流等の旅客・貨物輸送）

海外事例②（米国「ICTSの販売・利用制限に係る大統領令」）

- 2019年5月15日、トランプ前大統領は、国家緊急経済権限法（IEEPA）に基づき、「外国敵対者」との情報通信技術・サービス（ICTS）に関する取引を禁止する大統領令(EO13873)に署名。
- 2021年1月19日、商務省が暫定最終規則を発表し、3月22日に発効。「外国敵対者」及びその支配下の企業とのICTS取引について、審査手続きを定めた。
- 一方で、商務省は、事業者の予見可能性を担保する観点から、事前承認制度案を検討中。

大統領令の概要(情報通信技術・サービスサプライチェーンの安全性を確保する大統領令(EO13873))

米国内の個人・民間企業による以下の取引（**調達、輸入、設置等**）を禁止。

◆ **「外国敵対者」影響下にある個人・団体によって設計・開発・製造・供給される ICT機器・サービス**に係る

- 米国の**ICT機器・サービスに係る事業**活動に悪影響を与える取引
- 米国の**重要インフラ・デジタル経済のセキュリティ**に深刻な悪影響を与える取引
- その他の米国の**安全保障**に深刻な脅威を与える取引

「外国敵対者」※1 及びその配下企業

関係省庁の審査（事前/中/後）
- **商務長官の要請**または**申請**による。
- ２審制、180日以内に最終決定（許可/条件付き許可/不許可）

対象となる情報通信技術・サービス（ICTS）：
重要インフラ※2関連、**通信**関連、大量※3の米国人の**機微個人情報**関連、大量※3に米国に販売される**家庭用通信・モニタリング機器**、米国人に広く※3使用される**接続・通信ソフトウェア**、**AI・機械学習**、**量子暗号**、**量子コンピュータ**、**ドローン**、**自律システム**、**応用ロボティクス**関連

米国人・米国企業
（米国司法権に服する者）

※1 「米国の国家安全保障等に顕著に反する長期的な傾向又は深刻な行為に関与したと商務長官が判断する外国政府又は外国の個人・法人」（EO13873）
※2 大統領指令21（2013）に定められた「重要インフラ」（化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急サービス、エネルギー、金融、食料・農業、政府施設、ヘルスケア・公衆衛生、情報技術、原子力、輸送システム、上下水システム）およびその下位分野
※3 いずれも閾値は「100万（件・単位・人）を超えるもの」として設定。

ご議論いただきたい事項

① 政府が基幹インフラ機能の維持等に係る安全性・信頼性を確保するために新しい仕組みを創設する必要はあるか。

② 世界各国においてサイバー攻撃を通じた基幹インフラ機能に対する妨害行為が発生している現状、我が国の基幹インフラに係る現行制度、及び他国の立法例を踏まえると、基幹インフラ機能の維持等に係る安全性・信頼性を確保するためには、どのような仕組みが必要となるのか。

③ 契約自由の原則の下、基幹インフラ事業者の経済活動の自由を過度に制約することは望ましくないが、新しい仕組みにおいて、そのような考えと「国家及び国民の安全」とをどのように両立していけばよいのか。

④ 守るべき基幹インフラ事業をどのような考え方で特定していくか。

⑤ 守るべき基幹インフラ事業者をどのような考え方で特定していくか。