

①新しい仕組みの必要性／②どのような仕組みが必要か

- ✓ 安全保障の観点から、基幹インフラのサービス提供へのリスクに対処できるよう、設備や維持管理の委託の状況を政府が把握できる新しい仕組みが必要。
- ✓ 設備へのサイバー攻撃を防止するには、内部に脆弱性を仕込まれ、被害が出てからでは遅いため、設備の導入の際、事前に供給者などに問題がないか確認するという考え方が重要。アップデートや維持管理に関与する委託先の確認も検討すべき。
- ✓ 設備のサプライチェーンを包括的に見る必要がある。
- ✓ 他方、事業者ごとに分散的に対応をしても時間がかかるので、民間の努力に加えて、国が包括的に確認できる仕組みが必要。
- ✓ 事業者にとっての予見可能性の観点からは、導入後に政府が問題を指摘する仕組みではなく、事前審査を行う仕組みとせざるを得ない。

③経済活動の自由と国家及び国民の安全の両立

- ✓ 国家・国民の安全と事業者の経済活動の自由との間でバランスが必要。
- ✓ 規制対象となる事業、事業者、設備等について対象を絞ることが重要。
- ✓ 諸外国の審査基準も参考とし、審査基準を可能な限り明確にすべき。
- ✓ 事業者の事業判断が遅れないよう、政府における審査は可能な限り速やかに行うべき。
- ✓ 我が国だけでこのような取組みを進めるのではなく、国際的な動向も見定めるべき。
- ✓ 国際法との整合性が必要。

④守るべき基幹インフラ事業の考え方／⑤守るべき基幹インフラ事業者の考え方

- ✓ 安定供給が脅かされた場合に、国民の生存に支障をきたすものや、国民生活や経済活動に広範囲・大規模な混乱が生ずるもの等に対象事業を限定すべき。
- ✓ 対象事業者は、規模等により限定すべきであり、特に中小企業に規制を課すのは慎重になるべき。
- ✓ 対象事業者は絞ることを前提としつつ、ネットワーク全体への影響や競争の公正性も念頭に検討することが必要。