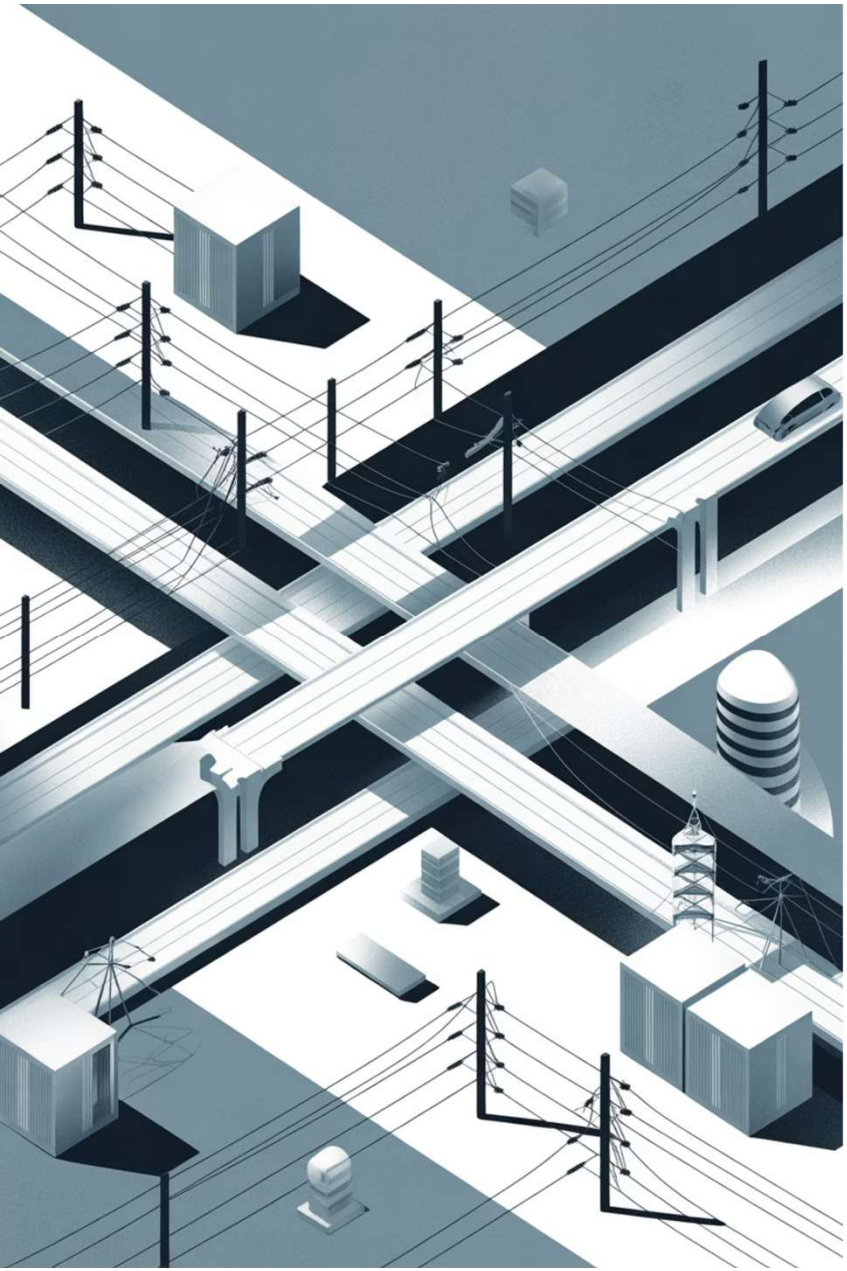


経済安全保障と重要インフラ防護

-米英豪の政策比較と日本への示唆-

京都大学大学院 教授
関山　健

本日の講演概要

01

問題提起

重要インフラ防護（CIP）への国際的関心の高まり

02

国際比較

OECD諸国の傾向と米・英・豪三国の政策分析

03

日本への示唆

国際比較から見えてくる日本の特徴と課題

経済安全保障推進法
「基幹インフラ制度」
2024年5月より開始

電気・ガス・水道・鉄道・通信・運送・金融など
社会基盤の防護が政策課題として浮上

なぜ今、重要インフラ防護なのか

現実の脅威

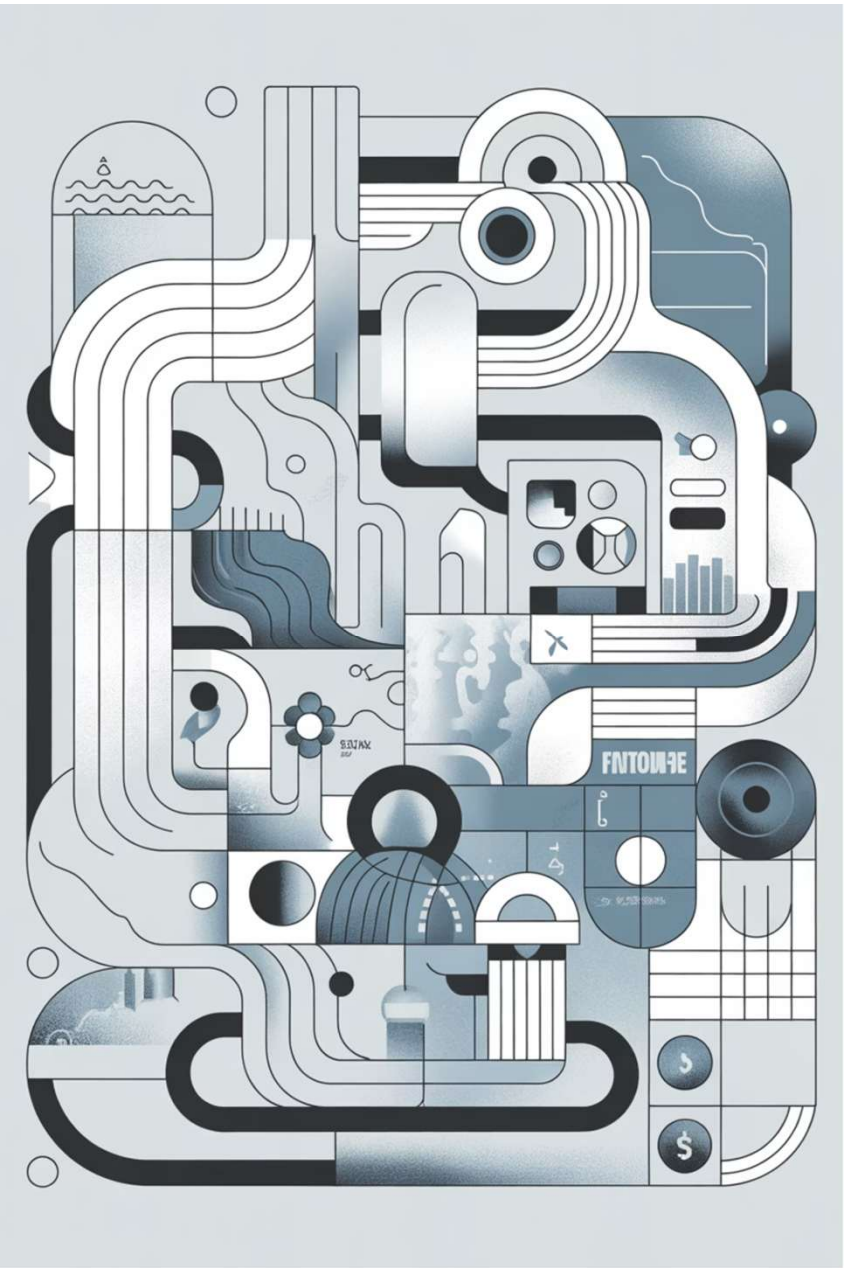
- ウクライナでは重要インフラへの攻撃が現実に発生。
- 中東でもエネルギー施設,水道,データセンターが攻撃対象。

重要インフラへの攻撃は、もはや仮定の話ではない。

分析の枠組み

OECD諸国の全体的傾向を踏まえつつ、
特に米英豪に焦点を当て、
その政策的特徴を解説。

そのうえで日本と比較、特徴と課題を考察。



重要インフラとは何か

定　義

社会経済・国家安全保障に
不可欠なシステム、資産、
施設、ネットワーク

対象分野

電力・ガス・水道・通信・
交通・金融・医療・食料・
政府情報システム　など

影響範囲

停止・破壊時は生命・安全・政治的安定、国家主権に影響

重要インフラ防護の歴史的背景

1990年代：物理的施設の保護 → 2000年代以降：**機能維持**へ政策目的が転換

2001年～

9.11・ロンドン爆破テロ
→ 国家安全保障への組み込み

1

2

気候変動・SARS・COVID-19
→ 非軍事リスクの顕在化

IT化・デジタル化による相互依存深化
→ 連鎖的機能障害リスク

3

OECD諸国の定義

加盟28カ国を調査（2019年）

約半数
経済・社会的福祉の観点のみで定義（例：スイス）

残り半数
国家安全保障の観点も含めて定義

- ファイブ・アイズ（米英加豪NZ）の共通定義：
  「国家安全保障・経済安全保障・繁栄・健康・安全に不可欠なサービスを提供するシステム、資産、施設、またはネットワーク」

出所）OECD (2019), Good Governance for Critical Infrastructure Resilience

OECD諸国の重要インフラ対象セクター

	AUS	AUT	BEL	CAN	CHE	CHL	CZE	DEU	ESP	EST	FIN	FRA	GBR	GRC	IRL	ISL	ISR	ITA	KOR	LAT	LUX	MEX	NLD	NOR	NZL	POL	PRT	SVK	SVN	SWE	TUR	USA
Energy	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Nuclear sector				●			●		●			●	●				●		●				●	●									●
ICT	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Transportation	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Water	●	●	●	●	●		●	●	●	●	●	●	●				●		●	●	●		●	●	●	●		●				●
Dams & flood defence	●					●	●					●			●	●		●	●	●		●	●	●					●		●	●
Food supply & dist.	●	●		●	●		●	●	●		●	●	●				●				●			●		●				●	●	●
Health	●	●	●	●	●	●	●	●	●	●	●	●	●				●		●	●	●			●		●		●		●	●	●
Finance & banking	●	●	●	●	●		●	●	●	●	●	●	●				●		●	●	●		●	●		●		●		●	●	●
Government		●		●	●		●	●	●			●	●				●		●	●	●			●		●				●		●
Public safety	●	●		●	●		●	●	●				●				●			●	●		●	●						●		●
Law enforcement		●				●		●				●	●				●			●	●		●	●								
Chemical industry	●	●			●				●		●	●	●				●			●	●		●	●		●		●				●
Space sector			●						●			●	●																			
Defence industry	●										●	●	●				●			●												●
Critical manufacturing				●							●	●					●							●							●	●
Other		●	●					●	●	●	●	●	●				●		●	●	●		●	●	●	●				●	●	●

出所）OECD (2019), Good Governance for Critical Infrastructure Resilience

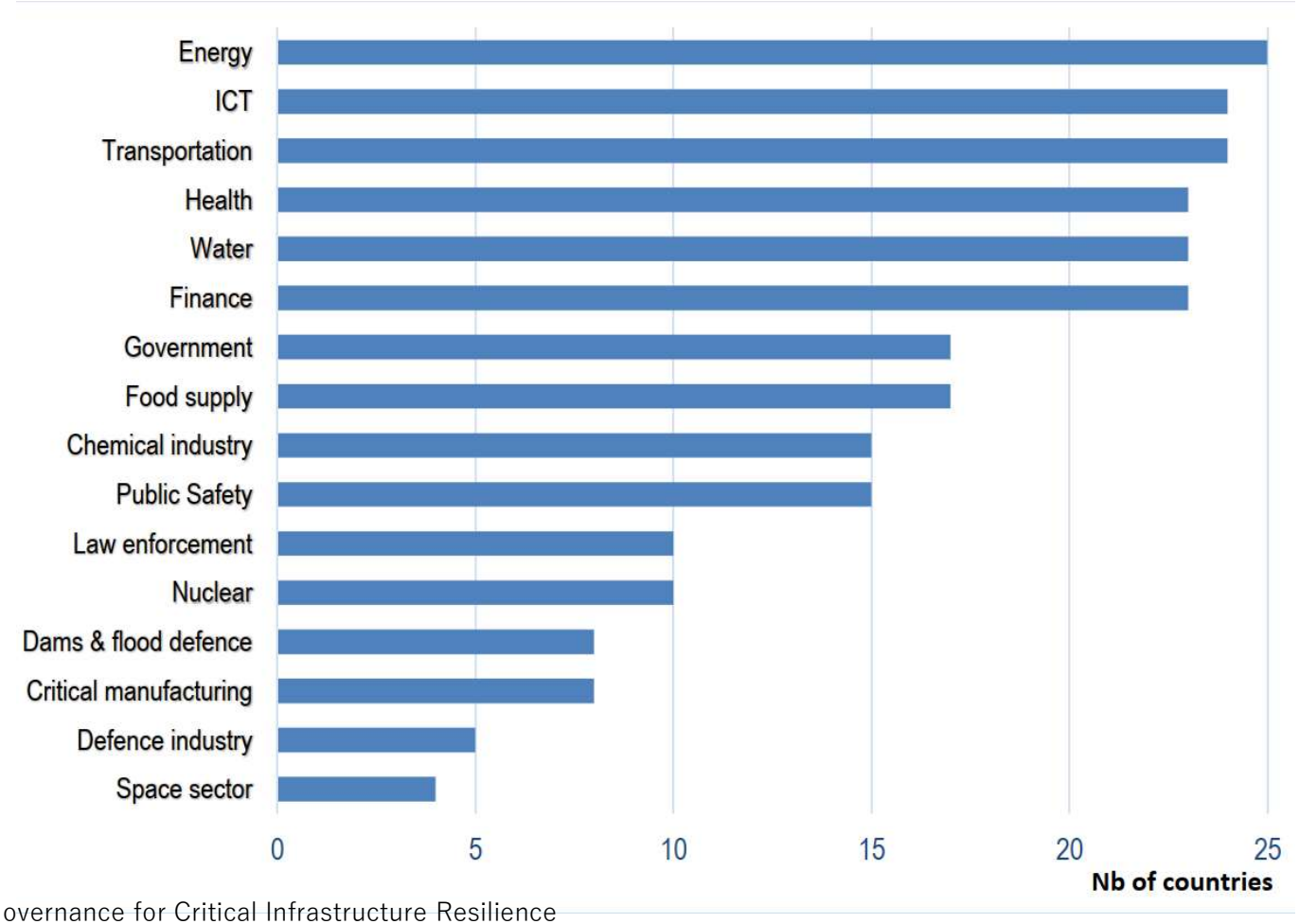
→ **米国**：
*16*分野（最多水準）

→ **ポルトガル**：
電力・通信の*2*セクターのみ

→ **日本**：
*15*分野（ 国際的に幅広い部類）

OECD諸国の重要インフラ対象セクター

情報通信、エネルギー、金融、医 療、運輸、水道の６分野は、多くのOECD諸国が重要インフラと認識



出所）OECD (2019), Good Governance for Critical Infrastructure Resilience

重要インフラへの脅威

自然災害・事故

- 暴風・地震・洪水による損壊
- 人的ミス・設備劣化による産業事故

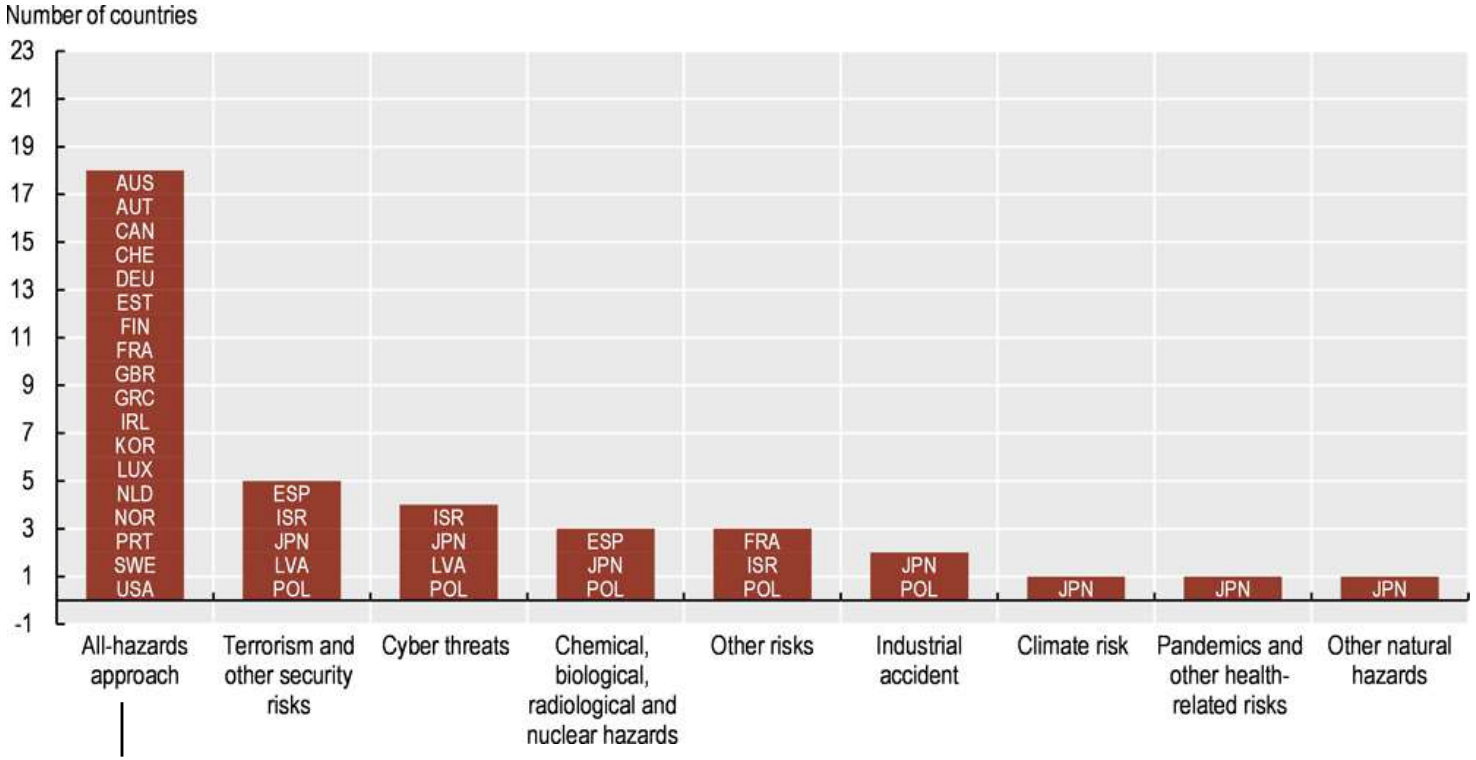
国内外からの物理的攻撃

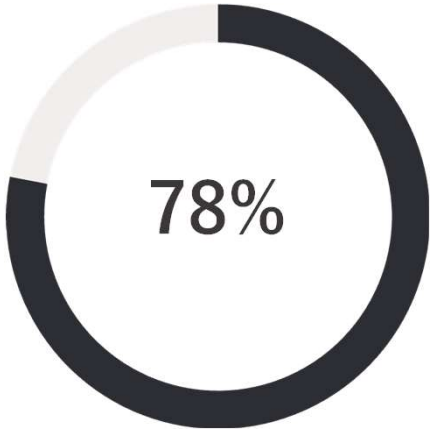
テロ、反社会勢力、外国勢力など

サイバー攻撃

- 電力網への侵入（2015年ウクライナ停電）
- ランサムウェア（2017年欧州）
- ハードウェアのバックドア

OECD諸国の重要インフラ政策アプローチ





包括的アプローチ採用
調査対象23カ国中18カ国

包括的アプローチ：あらゆる脅威を念頭に、重要インフラの**機能維持**に重点

- **日本はこの78%に含まれない。テロ・サイバー・自然災害などに個別対応する体系**
  これが日本の重要インフラ防護政策の大きな課題

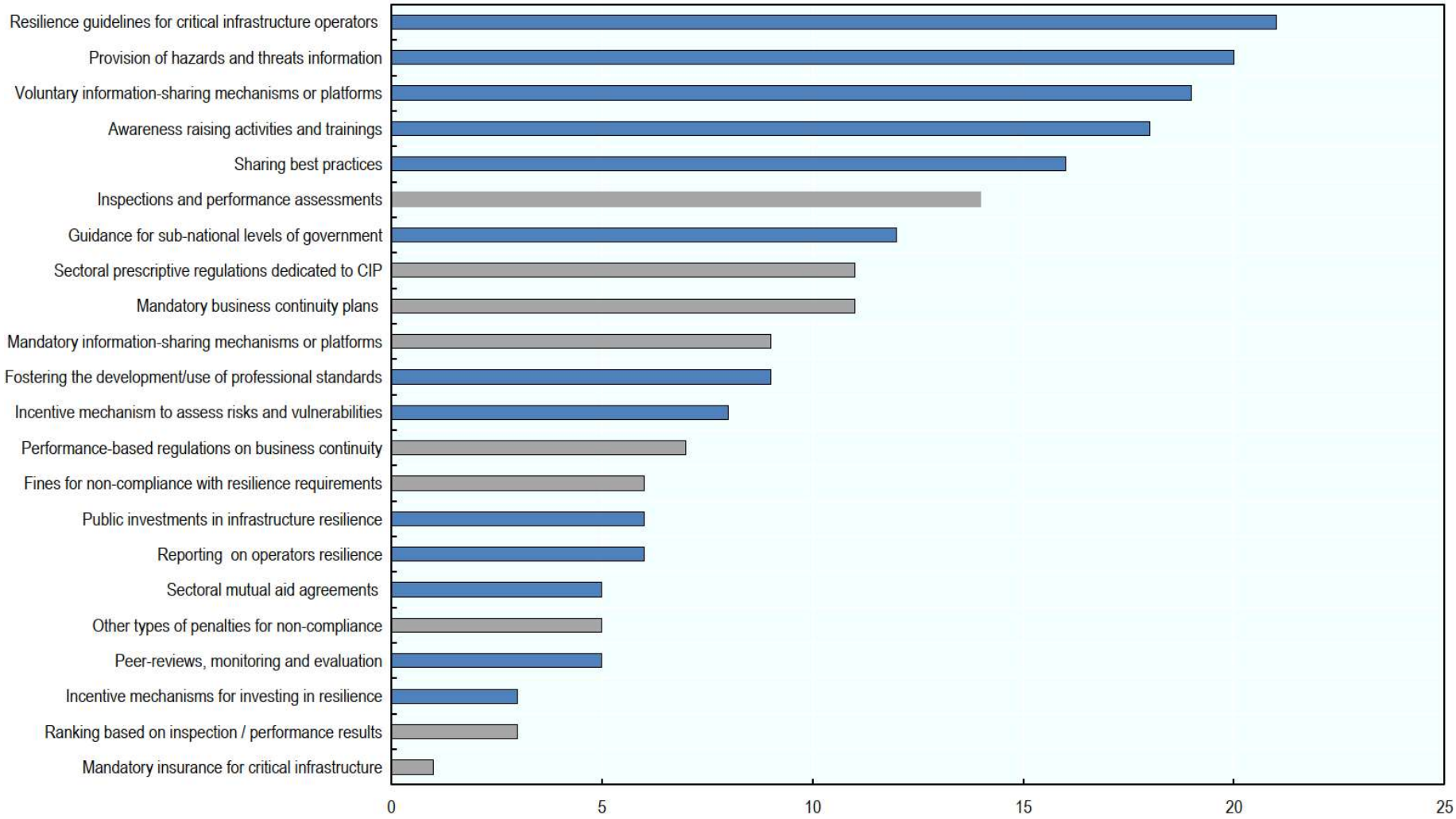
出所）OECD (2025), Government at a Glance 2025

重要インフラ防護の政策目的

1990年代：物理的保護が主眼

→　現代：**機能維持**が主眼。国・自治体・民間事業者など複数ステークホルダーの協力が不可欠

OECD諸国の重要インフラ防護政策手段



出所）OECD (2019), Good Governance for Critical Infrastructure Resilience

OECD諸国の政策手段と今後の課題

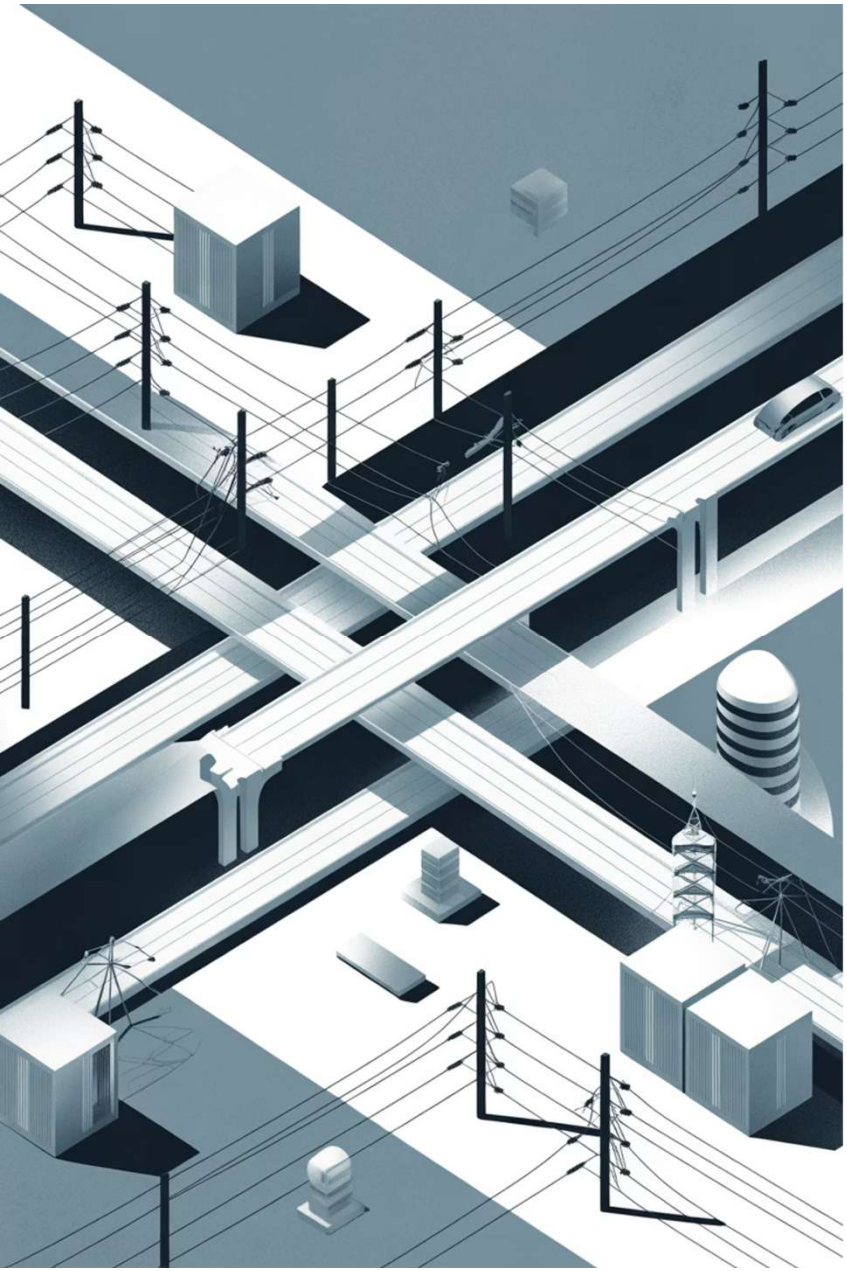
現在の主な政策手段

- 自治体向けガイダンス・研修・情報提供
- 民間事業者向け指針公表・情報共有
- 自主的取り組みの促進が主軸

今後の方向性

- → 最低限の共通安全基準の設定
- → より義務的・強制的アプローチへの移行
- → インフラ保険の加入義務付け（要研究）

情報共有・信頼醸成だけでは万全を期せない。
最低限の共通安全基準など、より義務的、強制的なアプローチが必要。



米英豪の重要インフラ防護政策

ファイブ・アイズ（米・英・豪・加・NZ）は
重要インフラの定義を共有しつつ、
防護政策にはそれぞれ異なる特徴がある。

米国の重要インフラ防護政策

転換点：2001年

同時多発テロ → DHS設立。民間インフラへの非国家主体による攻撃リスクを認識。

PPD-21（2013）→ NSM-22（2024）

共有責任・リスクベース・官民協働を中核概念とする「国家レジリエンス政策」へ。

CIRCIA（2022）

民間事業者にサイバーインシデント報告を義務化。
政府が集約データから脅威を特定・対策へ反映。

- 特徴：民間事業者が機能維持の第一次責任主体。政府は規制・支援・情報ハブの役割。

英国の重要インフラ防護政策

CPNI設立（2007）

官民インフラ事業者へ、諜報・テロ・サイバー脅威に対するセキュリティ助言・計画支援を提供。

規範主導型モデル

政府が達成基準を提示
→ 事業者が自律的に対応・自己評価。

サイバーセキュリティ・レジリエンス法（審議中）

成立すれば広範な組織にセキュリティ義務・インシデント報告義務が課される。

豪州の重要インフラ防護政策

規制の強化の経緯

2003年

官民情報共有ネットワーク

2018年

重要インフラ安全保障法

2024年

新サイバーセキュリティ法

ランサムウェア報告義務・
Cyber Incident Review Board

現行制度の特徴

リスク管理計画（CIRMP）の策定・遵守・報告を義務化

背景：中国との関係緊張化、防衛と経済の一体化
→ 重要インフラへの脅威認識の高まり

米英より規制色が強い「国家主導型モデル」

米英豪 三国比較まとめ

共通点：
①重要インフラの定義・範囲を共有
②国家安全保障の観点から防護
③機能維持の一次責任は事業者

1	2	3
米国	英国	豪州
協調的規制モデル 事業者の自主対策 ＋ 連邦政府への報告義務	**規範主導型モデル** 政府が基準を提示 → 事業者が自律対応,自己評価	**国家主導型モデル** 計画策定・遵守・報告を 事業者に義務化

日本の重要インフラ政策

1 **災害対策基本法（1961）**

「指定公共機関」（約100機関）に防災業務計画・応急対策を義務化。

2 **サイバーセキュリティ基本法（2014）**

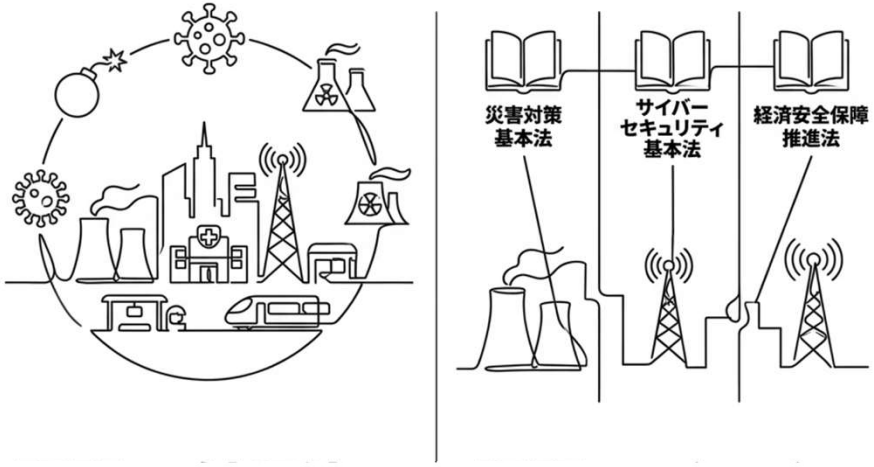
15分野の「重要社会基盤事業者」が対象。
自主的なセキュリティ対策は**努力義務**にとどまる。

3 **経済安全保障推進法（2022制定・2024運用）**

15業種の「基幹インフラ」約250社を「特定社会基盤事業者」に指定。
重要設備の導入・委託に**事前届出・審査制度**を導入。
「重要設備」が「海外からの妨害行為の手段」として使用されることを防止。

統一的な重要インフラ政策・統括官庁は存在しない

国際比較から見た日本の課題



<u>課題①：射程外の脅威</u>

物理テロ・パンデミック・産業事故など、
自然災害でもサイバーでもない脅威への統一基準・
ルールが存在しない。

<u>課題②：バラバラな政策対応</u>

電気・ガス・鉄道など同一セクターに対し、
異なる法律が異なる対象・義務を規定。
全体として効率的・効果的な体系とは言い難い。

多くのOECD諸国は**あらゆる脅威を考慮した包括的アプローチ**で機能維持政策を整備している。

国際比較から見た日本への示唆

統一的な法体系・統括官庁の設置

脅威の種類を問わず機能維持を図る
統一政策枠組みの構築

共通安全基準の設定

英国型：インフラ所有者・運営者が
最低限満たすべき基準を政府が提示

迅速な情報集約・機能回復

米英型：インシデント発生時に政府
へ迅速に情報集約、連鎖停止を防止

事業者の自発的BCP策定

事業者には有事でもサービス継続の社会的責務

サイバーセキュリティ保険の活用

米国の加入率約30%（医療・教育は約50%）に対し、
日本は7～8%。保険活用・義務化も要検討。

出所）https://www.ntt-rm.co.jp/topics/column/a28