JNSA Network Security Forum
2017/1/23

規制、イノベーション、協調：サイバーセキュリティ成熟度向上へのアジェンダ

門林　雄基
奈良先端科学技術大学院大学

規制

- サイバーセキュリティ基本法
- NIS Directive, GDPR（欧州）
- Cybersecurity Information Sharing Act（米国）

- 監督権限と義務の付与
- 予算と人員の裏付け

- 報告義務
  - 政策決定のための基礎データ(状況認識)

段階的規制 vs 一律規制

欧州

- Directive 2009/140/EC, Article 13a (2009)
  - 改正指令にてインシデント報告義務を明記
  - 通信サービス事業者を対象
  - 加盟各国における改正指令の法制化 (2011年から)
- → NIS Directive (2016)

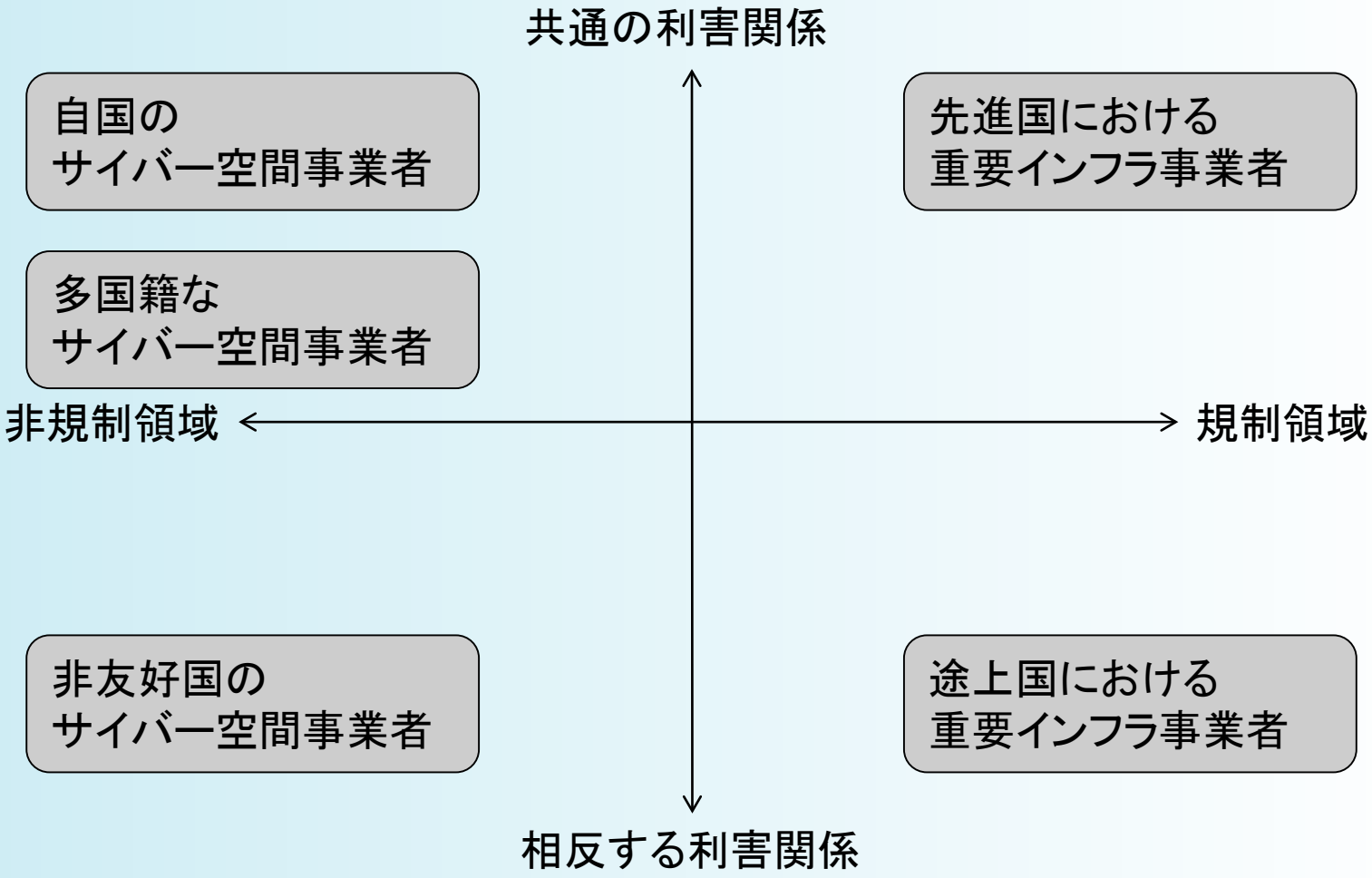
米国

- 州法 → … → 連邦法

日本

- 制度的実験の手法は「特区」のみか

規制、重要インフラ、インターネット経済



規制、重要インフラ、インターネット経済

- 重要インフラ
  - これも定義が社会情勢により変わるが.
  - 例: (米国) 投票システムが重要インフラに.
- サイバー空間事業者および一般企業
  - 重要インフラ諸規制の対象外

- 政府: 規制、ガイドライン以外の政策手段は.
- 民間: 規制が適さないイノベーション領域である
  ことを自ら立証できているか.
- 諸団体: Japan と名乗るからには海外連携し、
  国際的なコンセンサス形成に寄与すべき.

その他の政策的手段

- 税制
  - 控除
  - 減税
- 財政
  - 会計制度上の工夫 ← インフラ老朽化の抑止
  - 減損処理、リスク引当金 ← リスクを会計に反映
  - 災害復旧事業、復興基金 ← セーフティネット
- 金融
  - 証券
  - 債券
- その他

イノベーション

- 人材育成
  - 調整型人材ではなく..
  - 新しい組織、業務フロー、ツール導入、能力開発等
- インセンティブ
  - オープンソース
  - アクセラレータ
- 生産性向上
  - インターオペラビリティ
  - AI
- イノベータの保護
  - バグ報奨金制度
  - 有限責任　(SAFETY Act 等)

協調

- サイバー演習
  - さまざまな形式、さまざまな効能
- マーケットメカニズム
  - メディアに書けない事実（重大事故よりガジェット）
  - 知的労働、価値ある情報への対価
  - 調達形態の多様化（米国式も一つの選択肢に）
- 情報共有
  - 脅威レポート
  - インディケータ (STIX, TAXII)
- トラスト・ネットワーク
  - セプター, ISAC, CSIRT連携
  - 地域のサイバーセキュリティ・クラスタ

アジェンダ：規制

- 規制するのであれば、
  予算と人の裏付けが必須
  - 第190回国会閣法第11号 附帯決議
- 規制を正当化するだけの実効性があるか？
  - アリバイ的に予算投下して政策評価を怠っていないか？
- 萎縮効果の解消
  - Wassenaar arrangement の具体的解釈
  - 他国ではすでに、萎縮効果解消に動いている

アジェンダ：イノベーション

- オープン・データ
- オープン・ソース

- アクセラレータ
  - 海外商材を担いで儲けるモデルではなく.

- 多様なコンペティションの創造

アジェンダ：協調

- 事故調査と事故統計
  - 米国: CIDAR
    (Cyber incident data and analysis repository)
- FUD からファクトへ

- 政策決定の羅針盤としての事故統計

- IT以外の産業分野から信頼を勝ち得るためには
  何をすべきか。

アジェンダ：倫理

- 倫理綱領
  (Code of Ethics)
- 専門家としての行動指針
  (Code of Professional Conduct)