2025年03月21日

国土交通省総合政策局国際政策課　御中

米国のインフラ分野における サイバーセキュリティ関連政策等の 動向に係る調査等業務 公開用・概要版

WASHINGTON | CORE

報告書の構成

本調査事業では、米国のインフラ分野におけるサイバーセキュリティ関連政策、米国のISACの取組、自国内生産の動向・政策、その他経済安全保障分野の動向・政策に焦点を当てて調査を行い、結果を報告書にとりまとめた。本編は、報告書の概要をまとめたものである

報告書の構成

1 米国のインフラ分野におけるサイバー攻撃の事例及び政策の調査

6つの分野
- 航空・空港
- 鉄道
- 運送(コネクテッドカー等)
- 港湾・運送 (船舶)
- 水道
- ダム

×

- 1) サイバーセキュリティの脅威・事例
  - 脅威の実態
  - 攻撃事例
- 2) サイバーセキュリティ関係省庁
- 3) サイバー攻撃事案発生への備え
  - 規制
  - 戦略・ガイドライン
  - 資金提供プログラム等
  - 啓発活動

分野横断的な規則

2 インフラ分野の米国のISACの取組に関する調査

1) 米国のインフラ分野におけるISACの概要

2) 7つのISACの ①組織の概要、③活動状況、③米国政府との連携

7つのISAC: 航空 / 海上輸送システム / 不動産 / 地上輸送 / 公共交通・高速バス / 自動車 / 水

3 米国のインフラ分野における自国内生産の政策に係る調査

1) 米国のインフラ分野の自国内生産に係る動向・政策

2) 連邦政府による主な政策の動向

3) WTOルールに係る動向

4 米国のインフラ分野におけるその他経済安全保障分野に係る調査

1) 対米外国投資委員会による経済安全保障のための取引規制

2) 海底ケーブルにおけるサイバーセキュリティ強化のための取組

3) 海上輸送分野における政策

4) 特定企業等を排除する規制

5 今後の方向性

1) 今後国土交通省が取り組むべき施策の方向性

2) 日本国内のISACの取組の方向性

3) 本邦企業の海外インフラ展開にあたって留意すべき点・海外インフラ展開の案件開拓の可能性

航空・空港分野

サイバーセキュリティの脅威の実態

- 航空・空港会社は、毎年何百万人もの旅客や貨物の輸送データを処理している
  - 顧客の個人識別情報: 氏名、住所、パスポート番号など
  - 支払情報: クレジットカード情報などの金融データ
  - 従業員データ: 職員の個人情報や業務データ
  - 生体認証情報: 顔認証、指紋認証データなど
- 国際航空機関（International Civil Aviation Organization: ICAO）は、2023年11月に「サイバーセキュリティ・レジリエンス・シンポジウム(Cybersecurity and Resilience Symposium)」を開催し、以下のリスクを指摘
  - 乗客データの漏洩: 氏名、住所、パスポート番号が含まれる情報の流出
  - フライトの欠航や遅延: 運行への影響
  - 乗り継ぎ便への影響: 旅行全体の混乱
  - 経済的な損害: 企業の収益への影響や補償コストの増加
  - 壊滅的な事故のリスク: サイバー攻撃による航空機事故や墜落の可能性
- 空港施設の複雑なシステム構成が、セキュリティ上のリスクとなる
  - 発券端末や自動手荷物預け機
  - Wi-Fiネットワークや駐車場の出入庫管理システム
  - 職員の認証システム
- 航空・空港業界が直面する主なサイバー脅威
  - ランサムウェア攻撃: システムを暗号化し、身代金を要求する攻撃
  - ハッキング: システム侵入やデータ盗難
- 米国における航空分野へのサイバー攻撃は世界最多であり、2023年には7件の事例が報告された

関係省庁

- 連邦航空局（FAA）
- 運輸保安局（TSA）
- サイバー・インフラセキュリティ庁(CISA)

サイバー攻撃事案発生への備え

規制

- 緊急セキュリティ指令（Security Directive on an Emergency Basis）
- 勧告通達119-1A（Advisory Circular：AC）：「航空機ネットワーク・セキュリティ・プログラムの運用認可 (Operational Authorization of Aircraft Network Security Program)」
- 機器、システム、ネットワークの情報セキュリティ保護に関する規則案（Notice of Proposed Rulemaking：Equipment, Systems, and Network Information Security Protection）

戦略・ガイドライン等

- FAAサイバーセキュリティ戦略（FAA Cybersecurity Strategy）
- 商業用無人航空機システム（UAS）の運用におけるサイバーセキュリティのベストプラクティス（Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs)）
- サイバーセキュリティガイダンス：中国製UAS（Cybersecurity Guidance：Chinese-Manufactured UAS）

資金提供プログラム等

- 州及び地方のサイバーセキュリティ補助金プログラム (State and Local Cybersecurity Grant Program)

啓発活動

- サイバーセキュリティ啓発シンポジウム（Cybersecurity Awareness Symposium）
- Be Air Aware™プログラム

鉄道分野

サイバーセキュリティの脅威の実態

- 鉄道制御システムの現状と課題
  - 多くの鉄道制御システムは数十年前に設計されたものであり、セキュリティ機能が組み込まれていないことが多い
  - 部分的なシステムの更新が困難であり、古い設計がサイバー脆弱性に繋がっている
  - 多様なサプライチェーンや複数の運行事業者が異なるセキュリティ慣行を持つことが、脆弱性を生じさせる要因となっている
- デジタル技術の統合による利点
  - 重要な運用技術（OT）とモノのインターネット（IoT）ソリューションの統合が進んでおり、運行スケジュールの精密化や運営効率の向上が実現
  - PTC（Positive Train Control）システム: 列車同士の衝突や速度超過、誤操作による脱線を防ぐ重要な制御システム
  - PTCシステムがIoT技術に統合されることで、リアルタイムでのデータ交換や運行状況の監視が可能となり、運行の安全性と効率性がさらに向上している
- デジタル技術の導入による課題:デジタル技術の導入に伴い、サイバー脅威のリスクが拡大
  - ITとOTシステムの融合により、攻撃対象となる領域が広がり、新たな脆弱性が生まれている
  - 過去5年間で鉄道業界へのサイバー攻撃は220%以上増加しており、業界全体に深刻な影響を与えている
- 鉄道業界における防御戦略
  - ネットワークの細分化による被害箇所の分離、厳格なアクセス制御、侵入検知システムの導入、インシデント対応計画の策定、従業員教育など、多層的な防御戦略を採用

関係省庁

- 連邦公共交通局(FTA)
- 連邦鉄道局(FRA)
- 運輸保安局(TSA)
- サイバー・インフラセキュリティ庁(CISA)

サイバー攻撃事案発生への備え

規制

- セキュリティ指令（Security Directive）1580-21-01A・1582-21-01A
- セキュリティ指令（Security Directive）1580-21-01C・セキュリティ指令1582-21-01C
- 地上サイバーリスク管理の強化に関する規則案（Notice of Proposed Rulemaking：Enhancing Surface Cyber Risk Management）

戦略・ガイドライン等

- 技術報告書「接続された鉄道のサイバーセキュリティリスク管理（Cyber Security Risk Management for Connected Railroads）」
- 技術報告書「PTC通信：サイバーセキュリティ技術レビューと運用コンセプト（PTC Communications: Cybersecurity Technology Review and Concept of Operations）」

資金提供プログラム等

- 州及び地方のサイバーセキュリティ補助金プログラム（State and Local Cybersecurity Grant Program）
- 統合鉄道インフラ・安全改善（CRISI）プログラム（Consolidated Rail Infrastructure and Safety Improvements (CRISI) Program）
- 市街化区域フォーミュラ・プログラム（Urbanized Area Formula Program）

啓発活動

- 交通機関を対象としたウェビナーの開催

運送（コネクテッドカー等）分野

サイバーセキュリティの脅威の実態

- V2X技術の発展とサイバー脅威の増加
  - 車両とさまざまなもの（自動車同士、自動車と道路周辺のインフラ機器など）との通信や連携を行う技術であるV2X（Vehicle to X）が発展
  - V2X技術を搭載したコネクテッドカーや自動運転車へのサイバー脅威が増加
- 電気自動車（EV）の普及に伴う新たなリスク
  - EVの増加に伴い、EV用電源設備やEV用充電インフラのエコシステム全体におけるサイバーセキュリティリスクが増加しており、攻撃者は以下のような攻撃を試みる可能性がある：
    - ユーザーデータへの不正アクセス
    - 充電の中断
    - 電力網を遮断させるためのネットワーク侵入
- 自動車に対するサイバー攻撃の増加
  - 全世界で報告された自動車に対するサイバー攻撃件数は、2017年以降増加
  - 2023年には295件のサイバー攻撃が報告され、そのうち95%は遠隔で操作されたもの
- サイバー攻撃の主な攻撃ベクトル
  - 2023年に報告されたサイバー攻撃の攻撃ベクトル（攻撃者がネットワークやシステムに侵入する方法）のうち、最も多かったもの：
    - テレマティクスとクラウド（43.0%）：車両盗難時の追跡機能や位置情報・走行履歴の把握・管理などを行う通信システムであるテレマティクスと、車両データを管理・保存するクラウドシステムへの攻撃

関係省庁

- 連邦公共交通局(FTA)
- 商務省(DOC)
- サイバー・インフラセキュリティ庁(CISA)
- 高速道路庁(FHWA)
- 米国運輸省道路交通安全局(NHTSA)
- エネルギー省サイバーセキュリティ・エネルギーセキュリティ・緊急対応局及びエネルギー・運輸合同事務所

サイバー攻撃事案発生への備え

規制

- 情報通信技術とサービス・サプライチェーンの確保:コネクテッドカーに関する最終規則（Final Rule : Securing the Information and Communications Technology and Services Supply Chain : Connected Vehicles）

戦略・ガイドライン等

- 近代的自動車のためのサイバーセキュリティ・ベストプラクティス（Cybersecurity Best Practices for Modern Vehicles）
- サイバーセキュリティと高度道路交通システム・ベストプラクティスガイド（Cybersecurity and Intelligent Transportation Systems – A Best Practice Guide）
- 輸送サイバーセキュリティインシデント対応と管理フレームワーク（Transportation Cybersecurity Incident Response and Management Framework）
- 自律型地上車両セキュリティガイド（Autonomous Ground Vehicle Security Guide）
- 近代的自動車の安全性のためのサイバーセキュリティ・ベストプラクティス（Cybersecurity Best Practices for the Safety of Modern Vehicles）
- 交通機関向けサイバーセキュリティ評価ツール（Cybersecurity Assessment Tool for Transit）
- EV充電インフラ調達のためのサイバーセキュリティに関連する模範条項（Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements）
- DOEサイバーセキュリティ戦略（Cybersecurity Strategy）
- 小規模な高度道路交通システムチームのためのサイバーセキュリティ・ウォーゲーム（Cybersecurity Wargames for Small Intelligent Transportation Systems Teams）
- 運輸業界のサイバーセキュリティに関するリソース（Transportation Cybersecurity Resources）

資金提供プログラム等

- 州及び地方のサイバーセキュリティ補助金プログラム（State and Local Cybersecurity Grant Program）
- 市街化区域フォーミュラ・プログラム（Urbanized Area Formula Program）
- 裁量補助金プログラム（Discretionary Grant Program）

啓発活動

- 車両サイバーセキュリティ訓練カリキュラムのパイロットテスト（Vehicle Cybersecurity Training Curriculum Pilot Testing）

港湾・運送（船舶）分野

サイバーセキュリティの脅威の実態

- 地政学的緊張の高まりによるサイバー脅威の急増
  - 近年、地政学的な緊張の高まりにより、サイバー脅威が急増
  - サイバー攻撃の影響は港湾だけでなく、造船会社、ITプロバイダー、ベンダーにも及ぶ
- サイバー攻撃がもたらす影響
  - 海運・港湾業務の中断
  - 安全対策やシステム、船舶の通信・航行システムへの侵害
  - 貨物の盗難とそれに伴う経済的損失
  - 安全システムや航行、通信の混乱による船舶事故
- 2023年におけるサイバーインシデントの発生状況
  - オランダ・NHLステンデ応用科学大学の研究によると、2023年には全世界で少なくとも64件のサイバーインシデントが発生
  - これらのインシデントの多くは欧州と北米大西洋岸で発生
  - 紅海、ペルシャ湾、東シナ海でもインシデントが確認されている
- 国家主体による攻撃の割合
  - 攻撃の約80%は国家主体によるものであり、主な攻撃者はロシア、中国、北朝鮮、イランである
- デジタル領域におけるセキュリティ対策の不十分さ
  - 港湾・海運セクターはこれまで物理的なセキュリティ対策を行ってきたため、デジタル領域におけるセキュリティ対策が十分に整っているとは言い難い
- 船舶のデジタル化による新たな脅威
  - 船舶のデジタル化が進み、地球低軌道衛星によって海上でインターネット機器が広範に使用可能となった
  - 船舶のソフトウェア・アップデート・システムに対するサイバー攻撃が増加しており、海運事業者にとって大きな懸念となっている

関係省庁

- 米国沿岸警備隊（USCG）
- 連邦海事局（MARAD）
- 国防総省（DOD）
- サイバー・インフラセキュリティ庁（CISA）

サイバー攻撃事案発生への備え

規制

- 2002年海上輸送保安法（Maritime Transportation Security Act：MTSA）
- 米国の船舶、港湾、臨海施設の保護に関する規則の改正に関する大統領令（Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States）
- 2023年海上輸送改革法案（Ocean Shipping Reform Act of 2023）
- 海上輸送システムにおけるサイバーセキュリティに関する最終規則（Final Rule：Cybersecurity in the Marine Transportation System）

戦略・ガイドライン等

- 航行及び船舶検査に関する回章（Navigation and Vessel Inspection Circular：NVIC）01-20「海上輸送安全法（MTSA）規制対象施設におけるサイバーリスク対応ガイドライン（Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities）」
- 港湾施設サイバーセキュリティリスク・インフォグラフィック（Port Facility Cybersecurity Risks Infographic）
- 海運サイバーセキュリティ評価ガイド（Maritime Cybersecurity Assessment and Annex Guide：MCAAG）
- 勧告（Advisory）「港湾の脆弱性－外国の敵対勢力による技術的、物理的、サイバー的影響（Maritime Port Vulnerabilities - Foreign Adversarial Technological, Physical, and Cyber Influence）」
- 海上輸送システムレジリエンス評価ガイド（Marine Transportation System Resilience Assessment Guide：MTS Guide）
- MARAD戦略計画2022～2026会計年度（MARAD Strategic Plan FY 2022－2026）

資金提供プログラム等

- 州及び地方のサイバーセキュリティ補助金プログラム（State and Local Cybersecurity Grant Program）

啓発活動

- 沿岸警備隊海事産業サイバーセキュリティリソースウェブサイト（The Coast Guard Maritime Industry Cybersecurity Resource website）

水道分野

サイバーセキュリティの脅威の実態

- 上下水道システムを標的としたサイバー攻撃の増加
  - 上下水道システムは、浄水場、配水ネットワーク、廃水施設を制御・監視するSCADA（Supervisory Control and Data Acquisition）システムへの依存度を高めている
  - SCADAシステムは効率性を向上させる一方で、サイバー攻撃に対して脆弱である
- SCADAシステムへの不正アクセスによるリスク
  - 攻撃者がSCADAシステムに不正アクセスし、ポンプや薬品注入システムの操作、水量調節の変更を行えば、水の供給が中断される、水質が悪化する、水量が超過するなどの問題が発生するリスクがある
  - 公衆に重大な健康リスクをもたらすほか、多額の金銭的損失を引き起こす可能性がある
- EPAによるサイバーセキュリティ脆弱性の検査結果
  - 環境保護庁（EPA）は2024年10月、3,300人以上にサービスを提供する全米の飲料水システムを対象にサイバーセキュリティの脆弱性を検査した
  - 検査対象は1,062の飲料水システム（全米で1億9,300万人以上にサービスを提供）であり、そのうち70%以上がサイバーセキュリティ要件を完全に満たしていないことが判明した
  - 合計約2,660万人に飲料水を供給する97の飲料水システムが「極めて高（critical）」または「高（high）」リスクのサイバーセキュリティ脆弱性を有していると評価された（脆弱性は「極めて高」「高」「中」「低」の4段階で評価）
- 水道分野におけるサイバー攻撃の影響
  - EPAは、水道分野におけるサイバー攻撃が以下の影響を及ぼす可能性があると警鐘を鳴らしている：
    - 公衆衛生への影響
    - 公共サービスの混乱
    - サイバー犯罪者による従業員や顧客情報への不正アクセス

関係省庁

環境保護庁
(Environmental Protection Agency：EPA)

サイバー・インフラセキュリティ庁
(CISA)

サイバー攻撃事案発生への備え

規制

- 2022年重要インフラ向けサイバーインシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act of 2022：CIRCIA）

戦略・ガイドライン等

- 上下水道システムにおけるサイバーセキュリティ向上に関するEPAのガイダンス（EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems）
- 上下水道システム部門向けインシデント対応ガイド（Incident Response Guide for Water and Wastewater Systems Sector）
- 水道システムの安全性を確保するためのトップ・サイバー・アクション（Top Cyber Actions for Securing Water Systems）
- インターネットに露出したHMIが上下水道システムにもたらすサイバーセキュリティ上のリスク（Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems）

資金提供プログラム等

- 州及び地方のサイバーセキュリティ補助金プログラム（State and Local Cybersecurity Grant Program）
- クリーンウォーター州回転基金（Clean Water State Revolving Fund：CWSRF）
- 中規模・大規模飲料水システムのインフラレジリエンスと持続可能性プログラム（Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program）

啓発活動

- EPA水分野サイバーセキュリティ評価プログラム（EPA's Water Sector Cybersecurity Evaluation Program）
- サイバーセキュリティ訓練（Cybersecurity Training）

ダム分野

サイバーセキュリティの脅威の実態

- サイバー攻撃の潜在的な影響
  - 米国のダム分野では、2013年以降、公開情報では、サイバー攻撃事例は報告されていない
  - しかし、ダムをターゲットにしたサイバー攻撃は以下のような広範な影響をもたらす可能性がある：
    - 停電や洪水の発生
    - 水供給の停止
    - 施設及び流域コミュニティの安全性の低下
    - 経済的打撃
  - これらのリスクを踏まえ、サイバーセキュリティの強化が重要視されている
- 米国におけるダムの所有状況
  - 米国には9万基以上のダムが存在する
  - そのうち約65%は民間所有、約31%は連邦政府や州政府などの政府所有である
  - 米国連邦エネルギー規制委員会（FERC）は、約2,500基の水力発電用ダム（全ダム数の3%）を監督している
- 統一的な規制の欠如
  - 米国では、大半のダムが州や地方自治体、または民間の管理下にあるため、統一された規制が存在しないことが課題となっている
  - FERCの監督を受けるダムにおいても、資金不足や人員不足がセキュリティ対策の実施を妨げている

関係省庁

米陸軍工兵隊（USACE）

米国連邦エネルギー規制委員会(FERC)

サイバー・インフラセキュリティ庁(CISA)

サイバー攻撃事案発生への備え

規制

- 連邦エネルギー規制委員会ダム安全・検査部門水力発電プロジェクトのFERCセキュリティプログラム改訂版3A（Federal Energy Regulatory Commission Division of Dam Safety and Inspections FERC Security Program for Hydropower Projects Revision 3A）
- セキュリティ・レター（Security Letter）

戦略・ガイドライン等

- ダム分野サイバーセキュリティフレームワーク実施ガイド（Dams Sector Cybersecurity Framework Implementation Guide）
- ダム部門危機管理ハンドブック（Dams Sector Crisis Management Handbook）
- ダム部門サイバーセキュリティ能力成熟度モデル（Dams Sector Cybersecurity Capability Maturity Model：Dams-C2M2）
- ダム部門サイバーセキュリティ能力成熟度モデル実施ガイド（Dams Sector Cybersecurity Capability Maturity Model (C2M2) Implementation Guide）

資金提供プログラム等

- 州及び地方のサイバーセキュリティ補助金プログラム（State and Local Cybersecurity Grant Program）

啓発活動

- FERC-D2SIセキュリティブランチウェビナー（FERC-D2SI Security Branch Webinar）
- セキュリティ計画サンプル（Sample Security Plan）
- 国土安全保障情報ネットワーク－重要インフラ・ダムポータル（Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Dams Portal）

2022年重要インフラ向けサイバーインシデント報告法(2025年発効予定)
(Cyber Incident Reporting for Critical Infrastructure Act of 2022 : CIRCIA)

米国では、2022年3月、重要インフラにおけるサイバー攻撃事案に係る法整備や情報共有について規定する「2022年重要インフラ向けサイバーインシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act of 2022 : CIRCIA）」が制定された。2024年3月29日には、同法施行に向けた規則案が発表された。2025年10月に規則が最終化され、発効する予定である

この規則案では、ダム、輸送システム、上下水道システムを含む16の重要インフラ分野に関わる事業体（30万社以上が該当）に対し、「対象事業体が経験する重大なサイバーインシデント」が発生したと認識してから72時間以内、ランサムウェア攻撃に対する身代金を支払ってから24時間以内にCISAに報告することを義務付けている

米国の事業体は、サイバー攻撃のうちランサムウェアの被害を受ける可能性が最も高く、2023年の全サイバー攻撃の47%を占めている

この規則案については、負担義務が大きい、定義が曖昧などの理由で、業界からの反対の声も大きい

概要

制定	2022年3月
目的	重要インフラ事業体（30万社以上）に **重大なサイバーインシデント** の迅速な報告を義務付ける
対象	航空、海事、輸送システム、上下水道など16の重要インフラ
発効	最終規則発効日: 2025年10月予定

目的
- 重大なサイバーインシデントが発生したと認識してから72時間以内
- ランサムウェア攻撃に対する身代金を支払ってから24時間以内

→ CISAに報告

定義
1. 情報システムやネットワークの機密性、完全性、または可用性の重大な損失
2. 営業や操業に従事する能力、または商品もしくはサービス提供能力の中断
3. 業務システム及びプロセスの安全性及び回復力への深刻な影響
4. サードパーティによる情報システムまたはネットワーク、またはその中に含まれる非公開情報への不正アクセス

ISAC

米国では、各業種においてサイバーセキュリティ分野の業界内での連携に向けたISACが存在し、業種特有の問題に取り組んでいる。例えば、インシデントの情報共有、ベストプラクティス、次世代人材の開発などに取り組み、業界としてのサイバーセキュリティーの向上を目指している

各業種のISAC	組織概要	活動内容
航空ISAC	2014年にメリーランド州アナポリスを拠点として設立され、よりレジリエンスの高いグローバルな航空輸送ネットワークを実現することを目的としている。航空ISACとそのメンバーは、脅威情報の共有とベストプラクティスを通じて、サイバーリスクの予防、検出、対応、修復のために協力している	①情報共有・分析 ②ベストプラクティスの開発 ③知識向上のためのイベント等の開催 ④パートナーシップの強化
海上輸送システムISAC	2020年2月に米国を拠点とする海事重要インフラの利害関係者グループによって設立。利害関係者間においてタイムリーで実用的なサイバー脅威情報を共有するための調整において中心的な役割を担っている。情報共有と分析の取組としては、利害関係者が潜在的なサイバーインシデントを防止及び/または最小化するために利用できるIT、OT、IoTシステムに関連する情報の共有に重点を置いている	①情報共有 ②トレーニング及び意識向上 ③イベントの開催
不動産ISAC	2014年にワシントンD.C.で設立され、不動産業界におけるサイバーセキュリティの脅威と脆弱性に関する情報を共有・分析することを目的とし、業界特有のセキュリティリスクに対する意識向上と連携強化を図る役割を担っている	①情報共有 ②分析とアラート ③コラボレーション
地上輸送ISAC	2002年にワシントンD.C.で設立され、トラック輸送及び貨物鉄道業界を対象に、サイバーセキュリティ態勢を強化することを目的に活動している。メンバーが輸送セクターに特有のセキュリティ上の課題に対して、十分な情報に基づいた意思決定を行い、サイバー及び物理的脅威の両方を軽減し、新たな懸念、技術、傾向を探り、地上輸送業界全体のセキュリティ態勢を強化できるよう支援している	①コミュニティの支援 ②情報共有 ③専門的な分析と支援
公共交通・高速バスISAC	2004年にワシントンD.C.で設立され、米国公共交通協会（American Public Transportation Association：APTA）が運営している。公共交通システムの運営者や業界関係者を対象に、セキュリティ対策を支援することを目的として、物理的及びサイバーセキュリティの脅威、脆弱性、解決策に関する情報やアドバイザーサービスを提供している	①コミュニティの支援 ②情報共有 ③専門的な分析の提供
自動車ISAC	ゼネラルモーターズ（GM）、フォード、トヨタなど14社の自動車メーカーによって2015年8月に設立された。コネクテッドカーのサイバーセキュリティに対処するためのグローバルな情報共有コミュニティとして、2016年1月に本格運用を開始し、サイバー脅威や脆弱性、インシデントに関する情報を共有、追跡、分析するための中央ハブとして重要な役割を担う	①情報共有 ②インテリジェンス・レポート作成 ③ワークショップ・イベントの実施 ④ベストプラクティス・ガイドの開発
水ISAC	2001年にワシントンD.C.で設立され、水道及び下水処理分野のセキュリティ強化を目的とし、サイバー攻撃や物理的脅威に関する情報を収集・分析し、業界全体のサイバーセキュリティ強化に向けた取組を行っている	①情報収集と分析 ②ツールの提供 ③教育と情報提供

米国のインフラ分野における自国内生産の政策概要

背景

米政権の方針

目的
- 国内製造業の振興
- 雇用創出
- 経済成長

- 連邦政府調達品に関し国産品を優遇する措置「バイ・アメリカン法（1933年制定）」に基づき、国内生産要件を設定・強化し、インフラ政策において「メイド・イン・アメリカ」の実現を目指す
- バイデン政権は、2021年1月、バイ・アメリカン法条項の運用を強化する大統領令に署名し、自国の製造業を優遇する姿勢を表明

主な政策

インフラ投資・雇用法（BIL法, 2021年11月成立）

- 道路、橋、港湾、空港、鉄道などのインフラ整備を行う
- BIL法の一部として「ビルド・アメリカ・バイ・アメリカ法（BABA）」を制定。連邦資金援助を受けるプロジェクトで使用されるすべての鉄鋼、製造製品、建設資材を米国内で生産することを義務化

国内生産要件の強化

- 2022年3月：DOD、GSA、NASAが鉄鋼などの国内生産割合を55%→60%に引き上げることを発表（2024年に65%、2029年に75%へ引き上げ）
- 2024年10月：FARが国内生産要件から除外されている国内で入手できない109の物品を見直し、うち70品目を除外リストから削除することを提案
- 2025年1月：FHWAが高速道路プロジェクトにおける要件の全面適用を発表

国内生産の推進

国内生産が推進されている主な製品

- EV・その他電子機器等に使用されるバッテリー
- 高速道路
- 高速鉄道
- 船舶
- 港湾クレーン

造船業の推進

法律
- 2023年米国造船活性化法（Energizing American Shipbuilding Act of 2023）
- 2020年メイド・イン・アメリカ造船法（Made in America Shipbuilding Act of 2020）

同盟国との連携
- 米国は造船能力の強化のため、特に韓国や日本との提携を模索している
- 韓国のハンファグループ（Hanwha Group）は2024年12月、フィリー造船所（Philly Shipyard）を1億ドルで買収

国際的批判（WTO関連の問題）

- 中国 2024年、IRA（インフレ抑制法）の税額控除要件がWTO規則違反として、WTOの紛争解決手続きに基づく協議を要請
- EU IRAの税額控除要件に含まれる現地調達要件を批判し、WTOの紛争解決手続きに基づく協議の要請を検討

米国のインフラ分野におけるその他経済安全保障分野に係る動向・政策

米国では、重要インフラを特定国から保護することを目的として、法律の制定や行政命令の発出、連邦政府機関による規制、関税、外資の監視など、さまざまな対策が講じられている

主な規制・取組

対米外国投資委員会(CFIUS)による経済安全保障のための取引規制

- 外国人による米国への投資や特定の不動産取引を対象に、それらの取引が米国の国家安全保障に与える影響を調査
- 財務省（USDT）は2024年11月、CFIUSよる手続きや罰則、執行権限を強化するための最終規則を発表

海底ケーブルにおけるサイバーセキュリティ強化のための取組

- 2020年4月、大統領令により、省庁間組織チーム・テレコム（Team Telecom）を設立。米連邦通信委員会（FCC）の通信ライセンス審査に関する助言を提供
- 外国企業による米通信インフラへの投資審査や、海底ケーブルの陸揚げ許可申請の審査、国家安全保障リスクの評価などを実施

海上輸送分野における政策

商船法(Merchant Marine Act of 1920、通称ジョーンズ法(Jones Act))

- 米国が戦争や国家緊急事態に際し海軍の補助部隊として機能する強力な商船隊を維持することを目的として制定
- 米国の水域内及び米国の港間の海上貿易を規制

海事安全保障プログラム(Maritime Security Program：MSP)

- 軍事的に有用な商船の船団を維持することを目的として制定
- 国家緊急事態時にDODに即座に提供される
- 米国籍船舶であることなと、特定の基準が定められている

米国の繁栄と安全保障のための造船業と港湾施設法案(SHIPS for America Act)

- 外国船への依存を減らし、米国のサプライチェーンを強化することを目的として提案
- 10年以内に米国人船員が搭乗する米国建造かつ米国籍の国際船隊を250隻増加することなどを提案

通商法第301条に基づく中国への措置案

- USTRは、2025年2月、海事・物流・造船分野における中国の独占的な慣行は、米国の通商を脅かすものであるとし、通商法第301条に基づく措置案を発表
- 米国の港湾に入港する中国の船舶運航事業者や中国製の船舶の運航事業者などに対し、入港手数料を課すことを提案

中国製クレーンに対する措置

- USCGは、2024年2月、中国製クレーンの所有者・運営者に対するサイバーリスク管理措置を規定する措置を発表
- 中国製のクレーンは、世界市場で最大のシェアを占め、米国港湾のクレーンの約80%を占める
- これらのクレーンは遠隔地から不正アクセスされる可能性が高い

特定企業等を排除する規制

- エンティティリスト(Entity List)
  - 産業安全保障局(BIS)は、米国の国家安全保障や外交政策上の利益に反する活動を行う事業体をリストにして公開している
- 中国軍事企業リスト(Chinese Military Companies: CMC)
  - DODは、中国に拠点を置き、米国で直接または間接的に事業を展開し、中国軍と関連があるとみなされる中国企業をまとめたリストを公開している

今後の方向性

今後国土交通省が取り組むべき施策の方向性

米国の先進事例調査の深化

- 最新の規制やガイドライン等の動向をフォローする
- 米国の監査体制の実態（人員、監査内容など）を調査する
- 実際に攻撃を受けた米公共機関を対象に、ヒアリングや現場視察等を通じて調査し、ベストプラクティスを得る

日米間の情報共有の強化

- サイバー脅威に関する情報やサイバーセキュリティのベストプラクティスの共有を促進する
- 日米間の情報共有を促進する仕組みを整備する

官民連携の強化

- 重要インフラのサイバーセキュリティの強化に向け、官民が一体となって取組を推進していく

日本国内のISACの取組の方向性

官民の連携体制及び活動内容の強化

- 既存のISACの取組を強化するとともに、米国で先行するISACの取組を参考にする
- 米国の各ISACへのヒアリングや現地視察等の調査を実施することで、日本のISACの取組の参考となる詳細情報を得る
- 日本のISACと政府機関の連携体制及び活動内容の強化を図っていく

日米ISACの連携

- 日本のISACが米国の関連ISACと連携することは効果的であると考えられる
- 日本のISACが米国側のサイバーセキュリティに係る最新情報やベストプラクティスなどを習得することで、日本の関係業界における能力向上が図られる

ISACの役割・機能の明確化

- ISACとセプター（CEPTOAR）のすみ分けを明確にし、両者の連携体制等を検討する

本邦企業の海外インフラ展開にあたって留意すべき点・海外インフラ展開の案件開拓の可能性

米国のインフラ分野における自国内生産の政策に対する施策の方向性

免除措置の活用と動向のフォロー

- 免除措置を活用する
- 免除措置解除後に向けた備えをする

二国間協議

- 米国との二国間調達協定の交渉・締結を視野に入れる

経済安全保障上のビジネス展開の可能性

同盟国との連携強化を見据えたビジネス展開

- 本邦企業は、米企業のものづくりのパートナーとして活躍できる可能性がある
- 米国の他国との連携強化に向けた動向をフォロー
- 政府関係者等との対話を継続する

規制の遵守

- 米国の各分野の規制・ガイドラインを十分に理解し、遵守する

トランプ政権におけるインフラ政策の動向のフォロー

政策転換のフォローと多様なインフラプロジェクトへの参画の検討

- 政策の変更・中止や新たな政策の動きについて情報収集し、政策の転換に注意を払う
- 連邦資金によるインフラプロジェクトに依存することなく、多様なプロジェクトへの参画を検討する