# サイバー安全保障に関する政府の検討状況やサイバーセキュリティに関する国土交通省の取組み

令和６年１２月１３日

国土交通省
大臣官房サイバーセキュリティ・情報化審議官
山下　雄史

# アジェンダ

国土交通省

1．サイバーセキュリティを取り巻く情勢

2．サイバー安全保障に関する政府の検討状況

3．サイバーセキュリティに関する国土交通省の取組

# 1．サイバーセキュリティを取り巻く情勢

# 重要インフラ分野のサイバーセキュリティ情勢



## 国家安全保障戦略（2022年12月閣議決定）（抄）

- **サイバー空間**、海洋、宇宙空間、電磁波領域等において、**自由なアクセスやその活用を妨げるリスクが深刻化**している。特に、**相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている**

- サイバー攻撃による**重要インフラの機能停止や破壊**、他国の選挙への干渉、**身代金の要求**、**機微情報の窃取**等は、**国家を背景とした形**でも平素から行われている。そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、**軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせる ハイブリッド戦が、今後更に洗練された形で実施される可能性が高い**

# 名古屋港コンテナターミナルのシステム障害について

国土交通省

## 名古屋港コンテナターミナル システム障害事案（2023年7月）

- 2023 年 7 月 4 日に名古屋港の 5 つのコンテナターミナル及び集中管理ゲートで運用されている**名古屋港統一ターミナルシステム**（以下「NUTS」という。）**が、ランサムウェアの感染を受けて停止**

## 影響

- **荷役スケジュールに影響が生じた船舶37隻**（NUTSが停止したことによりマニュアル作業で荷役を行なったため最大24 時間程度の遅延が発生）
- **搬入・搬出に影響があったコンテナ約2万本（推計）**
- トヨタ自動車の愛知県と岐阜県にある4つの拠点の稼働停止、アパレルメーカーにおける衣類の入荷遅延等

## 感染経路

- ランサムウェアの感染経路として考えられているのは、以下の3点
  ①指定ユーザのみ利用可能な仮想専用線たる**VPN機器からの侵入**
  ②外部記憶媒体である **USB メモリからの持ち込み**
  ③NUTS と港湾運送事業者間とのネットワーク連携で運用している**NAT変換によるNUTSへの接続からの侵入**

【出典】コンテナターミナルにおける情報セキュリティ対策等検討委員会資料
https://www.mlit.go.jp/kowan/content/001719866.pdf

# 港湾分野における情報セキュリティ対策等の推進のための制度的措置

国土交通省

## 緊急的対策

### 事案発生直後の対策（Ｒ５．７．７～　実施中）

○港湾運送事業者、港湾運営会社、ふ頭会社、港湾管理者を通じて関係事業者に対し、「物流分野における情報セキュリティ確保に係る安全ガイドライン」を参考に必要な対策を講じるよう注意喚起を実施。

### 情報セキュリティ対策等の周知徹底（Ｒ５．９．２９～ 実施中）

○専門家の意見を踏まえた、具体的な情報セキュリティ対策、システム障害発生時の対応策（中間取りまとめ①）を港湾運送事業者に通知し、説明会等により周知の上、取組状況をフォローアップ

➡ **専門家の知見を踏まえた港湾分野における情報セキュリティ対策を事業者に周知徹底**

## 制度的措置

TOS：ターミナルオペレーションシステム

### 港湾運送事業法の観点

○コンテナターミナルにおいて一般港湾運送事業者が使用するTOSについて、①TOSの情報セキュリティ対策の状況を的確に把握し、②TOSの情報セキュリティ対策の強化・底上げを図ることが必要。

○港湾運送事業への参入等に際して審査を受ける必要がある事業計画にTOSの概要や情報セキュリティの確保に関する事項の記載を求める。

➡ **TOSの情報セキュリティ対策の確保状況を国が審査する仕組みの導入** 改正港湾運送事業法施行規則を施行（令和6年3月31日）

### サイバーセキュリティ基本法の観点

○「重要インフラのサイバーセキュリティに係る行動計画」を改定し、重要インフラ分野に「港湾分野」を位置づける方向で検討する。

○コンテナターミナルにおけるTOSを含む港湾分野に焦点を当てた情報セキュリティガイドラインを作成する。

➡ **官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進**

重要インフラ分野に「港湾分野」を位置づけ（令和6年3月8日）

### 経済安全保障の観点

○コンテナターミナルにおいて一般港湾運送事業者に使用されるTOSの機能が停止・低下し、荷役作業に支障が生じた場合、影響が甚大となるおそれがある。

○経済安全保障推進法の趣旨も踏まえ、TOSを使用して役務の提供を行う一般港湾運送事業を経済安全保障推進法の対象事業とすることが必要であると考えられる。

➡ **経済安全保障の観点からも国として積極的に関与** 改正経済安全保障推進法が公布(令和6年5月17日)

【出典】コンテナターミナルにおける情報セキュリティ対策等検討委員会資料
https://www.mlit.go.jp/kowan/content/001843334.pdf

# 我が国におけるサイバー攻撃数の推移

国土交通省

- **サイバー攻撃関連通信**は引き続き増加、2023年は6000億件超（**IPあたり14秒に1回**）
- **ランサムウェア被害**は、2022年上半期以降、**高い水準で推移**

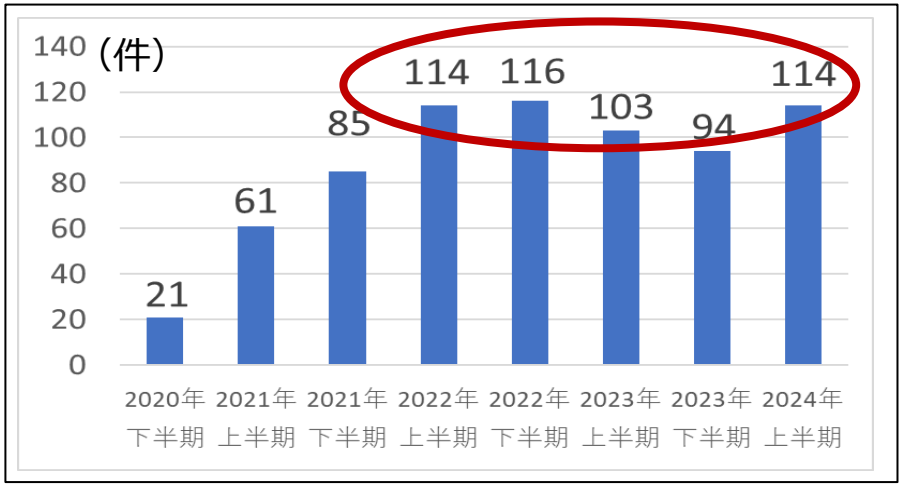
＜NICTERの観測実績(過去10年)＞

| 年 | 年間総観測パケット数 |
|---|---|
| 2014年 | 約　241.0億件 |
| 2015年 | 約　631.6億件 |
| 2016年 | 約1,440　億件 |
| 2017年 | 約1,559　億件 |
| 2018年 | 約2,169　億件 |
| 2019年 | 約3,756　億件 |
| 2020年 | 約5,705　億件 |
| 2021年 | 約5,180　億件 |
| 2022年 | 約5,226　億件 |
| **2023年** | **約6,197　億件** |

増加傾向

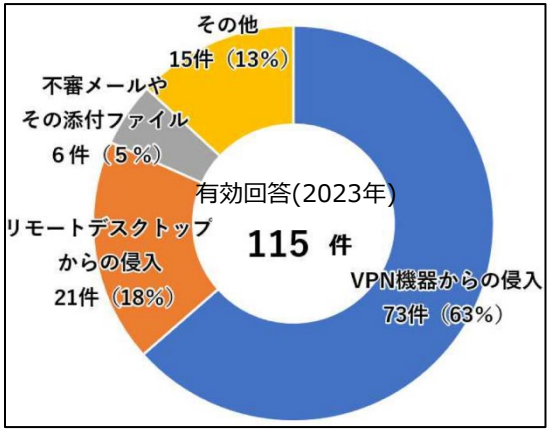
【出典】国立研究開発法人 情報通信研究機構 NICTER 観測レポート2023
https://csl.nict.go.jp/report/NICTER_report_2023.pdf

＜警察へのランサムウェア被害報告件数＞




＜感染経路＞

・**テレワーク等に利用される機器等の脆弱性**や、**強度の弱い認証情報**等を利用して侵入したと考えられるものが約82%を占める。




【出典】警察庁　令和６上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

# 諸外国の重要インフラに対するサイバー攻撃事例

国土交通省

| 時期 | 国/地域 | 産業 | 攻撃/被害 |
|---|---|---|---|
| 2016年12月 | ウクライナ | エネルギー | ・マルウェア「Industroyer」への感染<br>・大規模停電が発生 |
| 2017年５月 | 全世界 | 医療、空港、通信、鉄道等 | ・ランサムウェア「WannaCry」への感染<br>・世界規模で拡大。英国では、多数の病院で電子カルテや病理診断システムが使用不能 |
| 同　　６月 | ウクライナ、欧米等 | 銀行、メディア、エネルギー、医療等 | ・ランサムウェアに偽装したワイパー型マルウェア「NotPetya」への感染<br>・マルウェアは自己増殖機能を有しており、世界規模で拡大 |
| 同　　11月 | 中東 | エネルギー | ・マルウェア「Triton」への感染<br>・石油化学プラントが停止 |
| 2020年12月 | 全世界 | 政府等 | ・SolarWinds社が提供するネットワーク監視ソフトウェアに、正規のアップデートを通じてマルウェアが仕込まれ、感染が拡大（サプライチェーン攻撃）<br>・米政府機関を含む約18,000の組織に影響。多くの組織で情報窃取等の被害が確認 |
| 2021年5月 | 米国 | エネルギー | ・ランサムウェアへの感染<br>・米石油パイプライン最大手のコロニアル・パイプラインが全ての業務を停止 |
| 2022年2月 | ウクライナ、欧州等 | 通信 | ・ワイパー型のマルウェアへの感染<br>・ウクライナを始めとして欧州各国で衛星通信の利用が不可能に |
| 同　　4月 | ウクライナ | エネルギー | ・マルウェア「Industroyer２」への感染<br>・高圧変電所への攻撃などが確認されたが大規模停電には至らず |
| 同　　10月 | ウクライナ | エネルギー | ・ウクライナの変電所が攻撃を受け、停電が発生 |
| 2023年12月 | ウクライナ | 通信 | ・キーウスター社が攻撃を受け、2400万のユーザーが携帯電話を使用できない状態に<br>・個人情報・位置情報・テレグラムアカウント窃取・SMS傍受が行われた可能性 |

【出典】各種報道等

# ウクライナに対する主なサイバー攻撃



## 侵略開始前

- ロシアは、**侵略1年以上前**から、ウクライナの政府機関や重要インフラの**情報システムに侵入し、攻撃準備**
- **侵略開始1月程度前**から、**破壊的なサイバー攻撃**を開始
- **侵略前日**には、約300システムを対象とした**大規模な破壊的サイバー攻撃**を実施

## 2022年２月　衛星通信に対する攻撃

- 2022年2月、米社が提供する**衛星通信サービスが利用不能**に
- ウクライナ国内に限らず、ドイツの風力発電所等にも影響が拡大

## 2022年４月　高圧変電所に対する攻撃

- 2016年の攻撃に用いられたマルウェアの亜種（Industroyer2）による**高圧変電所への攻撃**
- ウクライナ政府のコンピュータ緊急対応チーム（CERT-UA）等の支援により、**大規模停電には至らず**

## 2022年10月　変電所に対する攻撃

- 2022年10月、ウクライナの変電所が攻撃を受け、**停電が発生**（攻撃者は**6月までにはシステム侵入**）
- 侵入先の正規ツールを悪用する**「現地調達型の攻撃」(Living-Off-The-Land)**により、変電所のブレーカーを遮断（ミサイル攻撃と同時に停電）。その後、マルウェアを展開し、システムを破壊。

【出典】各種報道等

# 最近のサイバー攻撃の動向（事前配置(pre-positioning)活動）

国土交通省

2023年５月、**ファイブ・アイズ５か国**は、中国背景とされるサイバー攻撃グループ **Volt Typhoon** について、注意喚起。

- 有事における機能不全を念頭に、**重要インフラへの事前のアクセス確保（pre-positioning）**を目的としたサイバー攻撃が発生
- **長期間の潜伏**に必要な、**高度な検知回避能力**
  - ネットワーク機器の脆弱性を突いて侵入。ゼロデイ脆弱性も悪用
  - マルウェアを使わず、**正規ユーザーになりすまし、正規ツールを駆使（Living-Off-The-Land）**
  - 侵入痕跡となる**ログの消去**　等
- 米国においては、本土及び島嶼部の米軍基地にサービスを提供する**重要インフラ（通信、エネルギー、水道など）への攻撃の脅威**が高まっている


【出典】PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024.2) 等

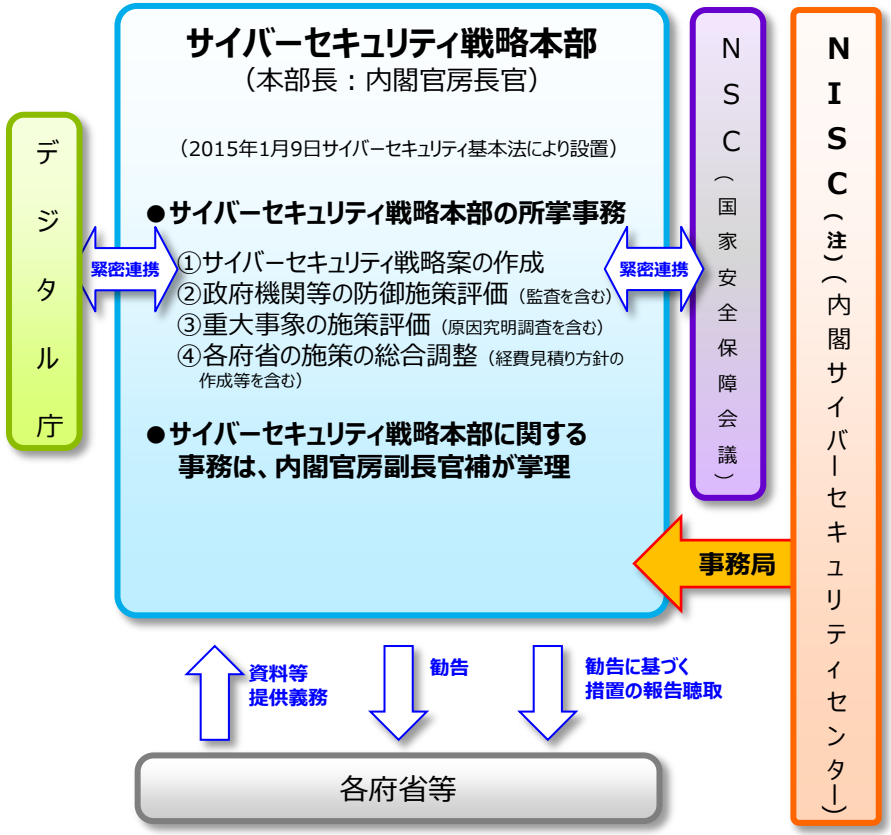
# 2. サイバー安全保障に関する政府の検討状況

# サイバーセキュリティ対策の推進

国土交通省

- 我が国のサイバーセキュリティに関する施策を総合的かつ効果的に推進するための法律「サイバーセキュリティ基本法」が2014年11月に成立
- 同法の規定に基づき、政府のサイバーセキュリティ政策の基本的な方向性を示す「サイバーセキュリティ戦略」が平成2015年9月、2018年7月、2021年9月に閣議決定（基本的に３年に１度改定）

## (1)サイバーセキュリティ対策の推進体制




（注）英名称：National center of Incident readiness and Strategy for Cybersecurity

## (2)サイバーセキュリティ対策に係る政府の方針

**サイバーセキュリティ基本法**（2014年11月12日法律第104号）
- サイバーセキュリティ戦略の策定
- 国の行政機関、独立行政法人及び重要インフラ事業者におけるサイバーセキュリティの確保
  - ・サイバーセキュリティに関する統一的な基準の策定・評価（監査）
  - ・情報システムの不正な活動の監視・分析
  - ・サイバーセキュリティに関する演習・訓練
- サイバーセキュリティ戦略本部の設置

**（2016年改正）**
- 国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を独立行政法人等まで拡大

**（2018年改正）**
- サイバーセキュリティ協議会を新設

**サイバーセキュリティ戦略**（2021年9月28日閣議決定）
- 経済社会の活力の向上及び持続的発展
  - ・経営層の意識改革等
- 国民が安全で安心して暮らせるデジタル社会の実現
  - ・国民・社会を守るためのサイバーセキュリティ環境の提供等
- 国際社会の平和・安定及び我が国の安全保障への寄与
  - ・「自由、公正かつ安全なサイバー空間」の確保等
- 横断的施策
  - ・研究開発の推進、人材の確保、育成、活躍推進等
- 推進体制
  - ・「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

# 国家安全保障戦略（2022年12月閣議決定）（抄）（能動的サイバー防御 関係部分）

国土交通省

- **武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入**する。そのために、…以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。

(ア) 重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

(イ) **国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

(ウ) **国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

- …これらの取組を実現・促進するために、内閣官房サイバーセキュリティセンター(ＮＩＳＣ)を発展的に改組し、サイバー安全保障分野を一元的に総合調整する新たな組織を設置する。そして、**これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備**、運用の強化**を図る**。

# 能動的サイバー防御体制のイメージ

国土交通省

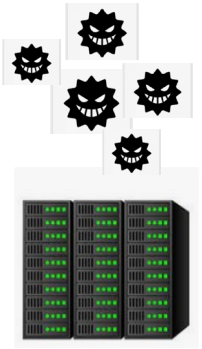
**「国民生活の基盤をなす経済活動」や「社会の安定性」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。**

全てのステークホルダーがメリットを実感できる
サイバー攻撃対応のエコシステムを
官民を横断して構築

守る対象（例）


Internet

攻撃者



通信事業者

(ア) **官民連携の強化**
官民の情報共有により、事案の未然防止、対処支援強化を図る

(イ) **通信情報の活用**
攻撃サーバ等を検知するため、明確な法的根拠を設けた上で、通信情報を活用

(ウ) **アクセス・無害化措置**
確認された攻撃サーバ等に対し、必要に応じ無害化

政　　府

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議資料
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html

# サイバー安全保障分野での対応能力の向上に向けた有識者会議

国土交通省

## 目的

- 「国家安全保障戦略」（2022年12月16日閣議決定）に基づき、**サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる**べく、当該分野における新たな取組の実現のために必要となる法制度の整備等について検討を行うため、**サイバー安全保障分野での対応能力の向上に向けた有識者会議を開催**する。

## 開催実績

- **令和6年6月7日　第1回**
  - ・サイバー安全保障分野での対応能力の向上に向けた有識者会議について　等
- **令和6年7月8日　第2回**
  - ・日本経済団体連合会、経済同友会、日本商工会議所のヒアリング　等
- **令和6年8月6日　第3回**
  - ・これまでの議論の整理　等
- **令和6年11月29日　第4回（提言書のとりまとめ）**
  - ・サイバー安全保障分野での対応能力の向上に向けた提言（案）　等

サイバー安全保障分野での対応能力の向上に向けた有識者会議　構成員

（五十音順）

| | |
|---|---|
| 上沼　紫野 | LM 虎ノ門南法律事務所弁護士 |
| 遠藤　信博 | 日本電気株式会社特別顧問 |
| 落合　陽一 | 筑波大学デジタルネイチャー開発研究センター長/准教授 |
| 川口　貴久 | 東京海上ディーアール株式会社主席研究員 |
| 川添　雄彦 | 日本電信電話株式会社代表取締役副社長 副社長執行役員<br>一般社団法人 電気通信事業者協会参与<br>一般社団法人 ICT-ISAC 理事 |
| 酒井　啓亘 | 早稲田大学法学学術院教授 |
| 佐々江　賢一郎 | 公益財団法人 日本国際問題研究所理事長 |
| 宍戸　常寿 | 東京大学大学院法学政治学研究科教授 |
| 篠田　佳奈 | 株式会社 BLUE 代表取締役 |
| 辻　伸弘 | SB テクノロジー株式会社プリンシパルセキュリティリサーチャー |
| 土屋　大洋 | 慶應義塾大学大学院政策・メディア研究科教授 |
| 野口　貴公美 | 一橋大学副学長、法学研究科教授 |
| 丸谷　浩史 | 株式会社日本経済新聞社常務執行役員 大阪本社代表 |
| 村井　純 | 慶應義塾大学教授 |
| 山岡　裕明 | 八雲法律事務所弁護士 |
| 山口　寿一 | 株式会社読売新聞グループ本社代表取締役社長 |
| 吉岡　克成 | 横浜国立大学大学院環境情報研究院/先端科学高等研究院教授 |

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議資料
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html

# サイバー安全保障分野での対応能力の向上に向けた提言

国土交通省

## （１）官民連携の強化

- **国家をも背景とした高度なサイバー攻撃への懸念の拡大**、デジタルトランスフォーメーションの進展を踏まえると、**官のみ・民のみでのサイバーセキュリティ確保は困難**。インフラ機能など社会全体の強靭性を高めるため、**産業界をサイバー安全保障政策の「顧客」としても位置づけ**、政府が率先して情報提供し、**官民双方向の情報共有を促進**すべき。

- 高度な侵入・潜伏能力を備えた攻撃に対し事業者が具体的行動を取れるよう、専門的なアナリスト向けの技術情報に加え、**経営層が判断を下す際に必要な、攻撃の背景や目的なども共有**されるべき。情報共有枠組みの設置や、クリアランス制度の活用等により、情報管理と共有を両立する仕組みを構築すべき。

- これらの取組を効果的に進めるため、システム開発等を担う**ベンダとの連携を深める**べき。脆弱性情報の提供やサポート期限の明示など、**ベンダが利用者とリスクコミュニケーションを行う**べき旨を法的責務として位置づけるべき。

- 経済安保推進法の**基幹インフラ事業者によるインシデント報告を義務化**するほか、その**保有する重要機器の機種名等の届出**を求め、攻撃関連情報の迅速な提供や、ベンダに対する必要な対応の要請ができる仕組みを整えるべき。基幹インフラ事業者以外についても、インシデント報告を条件に情報共有枠組みへの参画を認めるべき。**被害組織の負担軽減と政府の対応迅速化**を図るため、**報告先や様式の一元化、簡素化**等を進めるべき。

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議（第4回）
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai4/siryou1-1.pdf

# 各国における高度な攻撃に対する支援・情報提供（参考）

国土交通省

- ✓ 各国とも、これまで、**各業界の自主的情報共有の促進**や、**攻撃検知に必要な指標の提供**※1を実施
- ✓ 一方、海外では、**情報提供を政府の役割として明確化**。高度な侵入・潜伏能力を備えた攻撃に対し、事業者等が具体的行動を取りやすいよう、セキュリティクリアランスも活用し、インテリジェンス情報等に基づく**脅威ハンティングの支援**※2や、攻撃背景など**経営層の意思決定に有用な情報提供**も実施

※1 攻撃検知に必要な指標：攻撃者のIPアドレスやマルウェアのハッシュ値などのインディケータ情報

※2 脅威ハンティング：未知の脆弱性の悪用やマルウェアを用いない攻撃は、指標の一致・不一致では検知困難。このため、侵入を前提に、システムの作動状況から侵害の痕跡を探索する「脅威ハンティング」が必要となるが、標的組織や攻撃手法などの情報がないと、処理量が膨大となり、効果的探索は困難。

## 【国内外におけるこれまでの取組】

### 業界ごとの情報共有促進

- ✓ 2000年頃から、業界ごとの情報共有のため、ISAC※3の設置を促進
- ✓ 国内では、2002年のテレコムISACを皮切りに、重要インフラ各分野で導入

### 多様な主体の情報共有促進

- ✓ 官民の情報共有を促進するため、2019年にｻｲﾊﾞｰｾｷｭﾘﾃｨ協議会を設置。必要に応じ、国家公務員法相当の守秘義務も適用。

### 自動インディケータ共有（AIS※4, 2016年）

- ✓ 攻撃者のIPアドレスやマルウェアのハッシュ値等を、参加者間で機械可読な形でリアルタイムに共有
- ✓ 「ｻｲﾊﾞｰｾｷｭﾘﾃｨ情報共有法」に基づく取組
- ✓ 攻撃の背景情報が含まれないと、対策に活かしづらいとの指摘もあり

＋

## 【海外における更なる取組】

### 政府の役割として位置づけられた「情報提供のあり方」

- ✓ 「具体的な行動に結びつく情報の適時の共有は、機密性のあるものを含め、事業者等によるリスク管理に不可欠」【米：重要インフラに係る国家安全保障覚書（NSM-22, 2024年）】
- ✓ 「事業者等が具体的な行動を取れるような規模と頻度で脅威情報を提供」【英：国家サイバー戦略（2022年）】
- ✓ 「政府は、専門知識と機密情報源へのアクセスを活用し、事業者等による高度なサイバー脅威への対処を支援」【豪州サイバーセキュリティ戦略（2023年）】

### 脅威ハンティング部門設置（2021年）

- ✓ センサ検知情報やインテリジェンス情報等を元に、民間企業等にアウトリーチし、脅威発見・対処・分析等の支援を行う
- ✓ 技術者に限らず経営層用の情報も発信

### Industry100（2017年）

- ✓ NCSC※5と産業界との人的交流枠組み
- ✓ セキュリティクリアランスを求めた上で、非常勤として民間企業の専門家が出向

### 官民ｻｲﾊﾞｰｾｷｭﾘﾃｨ協力枠組み（JCDC, 2021年）

- ✓ 政府機関とセキュリティベンダ、ビッグ・テック等が連携し、情報共有

### サイバー脅威情報共有枠組み（CTIS, 2021年）

- ✓ ｲﾝﾃﾞｨｹｰﾀの自動共有に加え、参加者が専門家に相談し、助言を得ることも可能

※3ISAC: Information Sharing and Analysis Center ※4AIS: Automated Indicator Sharing ※5 NCSC: National Cyber Security Centre

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議資料

# 各国における政府の情報提供・対処支援を支える制度（参考）



- ✓ 日本では、重要インフラ行動計画のもと、個別業法に基づき所管省庁に報告されたインシデントについて、**各所管省庁を経由する形で内閣サイバーセキュリティセンター(NISC)に集約**
- ✓ 主要国では、業界・業種を超えた、政府の対処・情報収集能力を支えるための**サイバー対応組織の一元化**や、重要インフラ事業者に対する**インシデント報告の義務化**が進められている
- ✓ その際、**報告先集約化による負担軽減**や、**情報の取扱いについて報告者の意向を反映**する仕組みを整備する例もあり

【国内におけるこれまでの取組】

**内閣サイバーセキュリティセンター**(NISC)

- ✓ 内閣官房情報セキュリティセンター(2005年設置)を起源とし、サイバーセキュリティ基本法の制定を契機に改組(2015年)
- ✓ 内閣補助事務として、サイバーセキュリティ関係省庁間の総合調整を担当

**重要インフラのサイバーセキュリティに係る行動計画**(サイバーセキュリティ戦略本部決定)※

- ✓ インシデント発生時の情報集約等をルール化。重要インフラ事業者は、所管省庁を経由してNISCに報告する旨を規定
- ✓ ただし、情報流通経路が多層的となり、業界を跨いだ攻撃発生時の迅速な情報共有は困難
- ✓ また、報告の法的根拠は各業法であり、業法がない業種については、本行動計画のみが根拠

【海外における更なる取組】

**サイバーセキュリティ・インフラ保安庁**(CISA, 2018年)

- ✓ 国土安全保障省下に設置
- ✓ インシデント対処や関係省庁との調整を担う

**重要インフラサイバーインシデント報告法**(CIRCIA法, 2022年)

- ✓ 重要インフラ事業者に対し、インシデント発生から72時間以内のCISAへの報告を求める
- ✓ CISAが報告を関係省庁と共有。事業者の負担に配慮
- ✓ 細則はCISAが作成中

**豪州サイバーセキュリティセンター**(ACSC, 2014年)

- ✓ 通信情報局(ASD)下に設置、政府内の関係部門を順次統合

**重要インフラ保安法**(SOCI法, 2021・2022年改正)

- ✓ 重要インフラ事業者に対し、重大インシデント発生から12時間以内のACSCへの報告を求める
- ✓ 重要システム保有者には、システム状態の定期報告等を求めることが可能

**国家サイバーセキュリティセンター**(NCSC, 2016年)

- ✓ 政府内の関係部門を政府通信本部(GCHQ)下に統合し設置

**ネットワーク情報システム規則**(NIS, 2018年)

- ✓ 基幹サービス事業者等に対し、サービス継続に重大な影響を及ぼすインシデントの報告義務を課す

※インシデント情報について、所管省庁を通じて内閣官房に集約する旨は、行動計画の前身となる「重要インフラのサイバーテロ対策に係る特別行動計画(2000年)」から記載

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議資料

# サイバー安全保障分野での対応能力の向上に向けた提言



## （２）情報通信の利用

- **先進主要国は国家安保の観点からサイバー攻撃対策のため事前に対象を特定せず一定量の通信情報を収集し、分析**。我が国でも、重大なサイバー攻撃対策のため、**一定の条件下での通信情報の利用を検討すべき**。
- **国外が関係する通信**は分析の必要が特に高い。まず、①**外外通信(国内を経由し伝送される国外から国外への通信)は先進主要国と同等の方法の分析が必要**。加えて、 ②攻撃は国外からなされ、また、国内から攻撃元への通信が行われるといった状況を踏まえ、**外内通信(国外から国内への通信）及び内外通信(国内から国外への通信)**についても、被害の未然防止のために必要な分析をできるようにしておくべき。
- **コミュニケーションの本質的内容**に関わる情報は特に**分析する必要があるとは言えない**。**機械的にデータを選別し検索条件等で絞る等の工夫が必要**。
- **通信の秘密**であっても法律により**公共の福祉**のために**必要かつ合理的な制限**を受ける。先進主要国を参考に明確で詳細なルールとなるよう考慮し、緻密な法制度を作るべき。その際、**取得及び情報処理のプロセス**について**独立機関の監督**が重要。
- なお、**通信当事者の有効な同意**がある場合の**通信情報の利用**は、同意がない場合とは**異なる内容の制度により実施することも可能**であると考えられる。その際、制度により、**基幹インフラ事業者の協議の義務化等で、必要に応じ、同意を促すことが考えられる**。
- 性質上**非公開とすべき範囲はある**が**適切な情報公開**は行われるべき。**公開困難な部分を独立機関の監督で補う**べき。

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議（第4回）
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai4/siryou1-1.pdf

# 各国政府による通信情報の利用を許容する法律の例（参考）



主要国では、一定の条件の下、安全保障上の必要性等がある場合に、政府による通信情報の利用を許容する法律が整備されている。

| | 英国 | ドイツ | 米国 | 豪州 |
|---|---|---|---|---|
| 主な対象通信 | 海外関連通信（英諸島外の個人による送受信される通信） | 外国の電気通信 | 国外所在の非米国人（の通信） | 外国の通信（国外で送受信される通信） |
| 通信情報の取得要件 | ・安全保障上の必要性又は重大犯罪の検知等の必要性（取得目的のリストは首相がレビュー） | ・安全保障上の必要性<br>・重大な危険分野（マルウェアによる国際的犯罪・テロ・国家攻撃、重要インフラに対する脅威等）に関する情報の入手のために必要 | 外国インテリジェンス情報（外国勢力等の活動・安保関連情報）の収集のために必要 | ・安全保障上の必要性<br>・外国インテリジェンス情報（外国組織等の能力・意図・活動に関する情報）の収集のために必要 |
| 取得した情報を分析できる範囲 | ・必要性・比例性のある分析に限定<br>・国内通信内容の分析を原則禁止 | ・私生活の中核的領域の分析を禁止<br>・自国民等の個人データの分析を原則禁止 | ・米国人関連情報の分析は必要最小限 | ・国内通信記録は原則廃棄 |
| その他利用制限 | ・閲覧・複製・開示は最小限 | ・外部提供可能な場合を法令上限定 | ・裁判での証拠としての利用を原則禁止 | ・裁判での証拠としての利用を原則禁止 |
| 独立機関の監督 | あり | あり | あり | あり |
| 法令名 | 調査権限法 | 連邦情報庁法 | 外国情報監視法 | 電気通信（傍受及びアクセス）法 |

※1 上記の制度は、主要国において、個別具体的な調査対象を事前に特定せず、通信情報を調査できる法的枠組の例。
（これら以外に存在しないという趣旨ではない）
※2 公表済の各国法令の条文を参照して作成。各国政府の確認を経たものではなく、また、各国政府による対策の実態まで示すものではない。

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議（第3回）
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/siryou5-2.pdf

# サイバー安全保障分野での対応能力の向上に向けた提言



## （３）アクセス・無害化

- **サイバー攻撃の特徴**（①危険の認知の困難性、②意図次第でいつでも攻撃可能、③被害の瞬時拡散性）**を踏まえ**、**被害防止を目的**としたアクセス・無害化を行う権限は、**緊急性を意識**し、**事象や状況の変化に応じて臨機応変かつ即時に対処可能な制度にすべき**。こうした措置は、比例原則を遵守し、必要な範囲で実施されるものとする必要。その際、執行のシステム等を含め、従前から機能してきた**警察官職務執行法を参考**としつつ、その**適正な実施を確保するための検討を行うべき**。
- 平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるサイバー攻撃の特性から、**武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度**とすべき。
- アクセス・無害化の措置の性格、既存の法執行システムとの接合性等を踏まえ、**権限の執行主体**は、**警察や防衛省・自衛隊**とし、その能力等を十全に活用すべき。**まずは警察が**、**公共の秩序維持の観点から特に必要がある場合には自衛隊**がこれに加わり、共同で実効的に措置を**実施できるような制度とすべき**。
- 権限行使の対象は、**国の安全や国民の生命・身体・財産に深く関わる国、重要インフラ、事態発生時等に自衛隊等の活動が依存するインフラ**等へのサイバー攻撃に重点を置く一方、必要性が認められる場合に適切に権限行使できる仕組みとすべき。
- 国際法との関係では、他国の主権侵害に当たる行為をあらかじめ確定しておくことは困難。他国の主権侵害に当たる場合の違法性阻却事由としては、実務上は対抗措置法理より**緊急状態法理の方が援用**しやすいものと考えられるが、国際法上許容される範囲内でアクセス・無害化が行われるような仕組みを検討すべき。

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議（第4回）
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai4/siryou1-1.pdf

# サイバー安全保障分野での対応能力の向上に向けた提言

国土交通省

## （４）横断的課題

- 脅威の深刻化に対し、**普段から対策の強化・備えが重要**であり、**サイバーセキュリティ戦略本部の構成等を見直す**とともに、**NISCの発展的改組**に当たり政府の司令塔として強力な情報収集・分析、対処調整の機能を有する組織とすべき。

- **重要インフラのレジリエンス強化のため、行政が達成すべきと考えるセキュリティ水準を示し、常に見直しを図る制度**とするとともに、政府機関等についても**国産技術を用いたセキュリティ対策を推進**し、**実効性を確保する仕組み**を設けるべき。

- 政府主導でセキュリティ人材の定義の可視化を行い、関係省庁の人材の在り方の検討を含め、非技術者の巻き込みや人材のインセンティブに資する**人材育成・確保の各種方策を自ら実践**しながら、**官民の人材交流を強化**すべき。

- **サプライチェーンを構成する中小企業等のセキュリティ**について、**意識啓発や支援拡充、対策水準等を検討**すべき。

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議（第4回）
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai4/siryou1-1.pdf

# 中小企業における対策強化（参考）

国土交通省

✓ 中小企業においてもセキュリティ対策を強化するため、**対策実施に役立つガイドラインの提供**、セキュリティ対策の**ワンパッケージサービス（「サイバーセキュリティお助け隊」）の導入促進**などを実施。

## 中小企業の情報セキュリティ対策ガイドライン（第3.1版 2023年4月）

中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、を実践する際の手順や手法をまとめたもの。
付録としてクラウドサービスの安全利用やセキュリティインシデント対応に関する手引きなどがある。

**中小企業の情報セキュリティ対策ガイドライン**


**経営者向けの解説** — **経営者が認識すべき３原則と実施すべき重要７項目**を解説

**実践者向けの解説** — 企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

**付録6、8:クラウドサービス安全利用の手引き、セキュリティインシデント対応手引き**



## 「SECURITY ACTION」

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。30万者を超える中小企業が宣言。

★一つ星


**情報セキュリティ５か条に取り組む**

★★二つ星


**情報セキュリティ自社診断を実施し、基本方針を策定**

## サイバーセキュリティお助け隊サービス

相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など各種サービス内容を要件としてまとめた基準を満たすワンパッケージサービス。（2024年４月時点で40事業者）

サイバーセキュリティ お助け隊

IT導入補助金「セキュリティ推進枠」で導入を支援

【出典】サイバー安全保障分野での対応能力の向上に向けた有識者会議資料

# 「能動的サイバー防御」法整備の動き



**11/29　サイバー安全保障分野での対応能力の向上に向けた有識者会議**

「サイバー安全保障分野での対応能力の向上に向けた提言」をとりまとめ

**11/29　石破総理大臣　有識者会議での発言**

「サイバー対応能力の向上はますます急を要する課題だ。可能なかぎり早期に関連法案をまとめてもらいたい」

**11/29　橘官房副長官　記者会見での発言**

「わが国のサイバー対応能力の向上は、現在の安全保障環境に鑑みるとますます急を要する課題であり、有識者会議からの提言を踏まえ可能なかぎり早期に法案を示せるよう検討を加速していきたい。国民や与野党から広く理解を得られるよう政府の考え方を丁寧に説明していく」

**11/29　石破総理大臣　所信表明演説での発言**

「サイバー攻撃の脅威は差し迫った課題であり、有識者会議の提言も踏まえ、サイバー安全保障分野での対応能力を向上させるための法案を、可能な限り早期に国会に提出するべく、検討をさらに加速します」

# 3. サイバーセキュリティに関する国土交通省の取組

# 国土交通省におけるサイバーセキュリティ対策及び個人情報保護

国土交通省

近年、複雑化・巧妙化するサイバー攻撃に対して、国土交通省、所管独立行政法人及び重要インフラ分野におけるサイバーセキュリティ対策を推進。また、個人情報保護法に基づく措置を実施

## 1．サイバーセキュリティ対策

### ① 国土交通省における対策

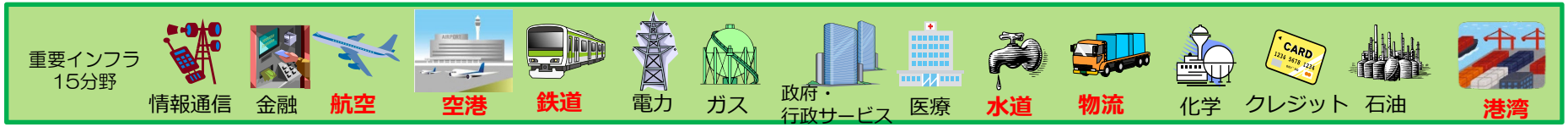
○ セキュリティ規程の整備　：国土交通省情報セキュリティポリシーを中心とした省内セキュリティ関係規程の整備
○ 情報システムのセキュリティ強化：インターネット接続の制限及びインターネット分離による無害化等
○ 情報セキュリティ監査　：省内情報システムやセキュリティ関係規程等に対する内部監査・外部監査の実施、NISCによるマネジメント監査及びペネトレーションテストへの協力
○ 教育・訓練　：情報セキュリティ対策の自己点検・研修の実施、CSIRT訓練・研修への参加、本省職員への研修の実施
○ 人材育成　：「国土交通省セキュリティ・IT人材確保・育成計画」の作成

### ② 当省所管の独立行政法人（15法人）における対策

○独立行政法人CISO連絡会議を開催し、所管独法におけるセキュリティ対策を促進。
○ NISCによる独立行政法人に対する情報セキュリティ監査への協力。

### ③ 当省所管の重要インフラ分野（航空、空港、鉄道、水道、物流、港湾）における対策

○「重要インフラのサイバーセキュリティに係る行動計画」（令和6年3月サイバーセキュリティ戦略本部改定）に基づき、重要インフラ分野として「航空」、「空港」、「鉄道」、「水道」、「物流」、「港湾」を含む15分野を特定。




○ NISC主催の全分野一斉演習に参加・協力し、障害発生時における重要インフラ防護能力の維持・向上を促進。

### ④ 経済安全保障推進法の基幹インフラ（鉄道、貨物自動車運送、外航海運、航空、空港、水道、港湾運送）への対応

○ 経済安全保障推進法の規定に基づき、国に指定された基幹インフラ事業者が特定重要設備（新幹線、航空のシステム等）の導入・維持管理等の委託をする際の事前審査を国土交通省が担当。

## 2．　個人情報の保護

○ 個人情報保護委員会等と連携し、個人情報保護法に基づく対策（国土交通省保有個人情報等管理規程の整備、個人情報漏えい対策、個人情報監査、　個人情報に係る自己点検・研修、開示請求の決定、審査請求の裁決等）の実施。

# 重要インフラのサイバーセキュリティに係る行動計画の概要

（2022年6月17日サイバーセキュリティ戦略本部改定）

国土交通省

## 官民連携による重要インフラ防護の推進

- 重要インフラ防護に係る基本的な枠組みを定めた政府と重要インフラ事業者との官民共通の行動計画
- 重要インフラサービスの継続的提供を不確かなものとするサイバー攻撃等をリスクとして捉え、リスクを許容範囲内に抑制
- 重要インフラサービス障害に備えた体制を整備し、障害発生時の迅速な復旧を図る

**→国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する**

## 行動計画で求められる国が取り組むべき事項

- 重要インフラ事業者の安全基準等の整備にあたって、情報セキュリティ対策の水準等を定めた安全ガイドラインを作成
- 重要インフラサービス障害対応時の状況を把握するほか、重要インフラ事業者へ脆弱性情報を共有
- 分野横断演習のシナリオ、実施方法、検証課題等の企画、分野横断演習の実施の協力　等

## 行動計画で国、重要インフラ事業者等が取り組むべき事項の「5本の柱」

### 障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

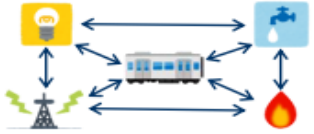
### 安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

### 情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

### リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

### 防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

# 「国土交通省所管重要インフラにおける情報セキュリティ確保に係るガイドライン」の改定

国土交通省

- 政府では、「サイバーセキュリティ戦略」（2021年９月２８日閣議決定）を踏まえ、重要インフラ防護に係る基本的な枠組みを定めた「重要インフラのサイバーセキュリティに係る行動計画」（2022年６月17日サイバーセキュリティ戦略本部決定、2024年３月８日戦略本部改定）を改定
- 国土交通省では、本行動計画を踏まえ、重要インフラ事業者自らが規定するセキュリティ対策の指針となるよう、**重要インフラ分野毎**（航空、空港、鉄道、物流、港湾）**に「情報セキュリティ確保に係る安全ガイドライン（2024年4月）」を改定**
- 安全ガイドラインでは、重要インフラ事業者における**情報セキュリティに係るリスクへの必要な備えや、有事の際の適切な対処等を規定**

## 安全ガイドラインにおいて重要インフラ事業者に求めている基本的な内容

**今回改定で追加**

- 最高情報セキュリティ責任者は、重要インフラ防護の目的、目指す方向、情報セキュリティ対策にて守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を情報セキュリティ方針として規定すること
- 最高情報セキュリティ責任者は、情報セキュリティインシデントに備えた体制の整備を行うこと
- 必要な情報のバックアップを取得し、同じ重要インフラサービス障害で同時に被災しない場所に保存することはもとより、特に重要な業務を支える情報システムについては、バックアップシステムを整備すること
- 情報を保存することにより発生するリスクに対応するため、情報の管理方法、保存期間等について、保存する情報の格付けに応じた適切な対策を講ずること　等

【出典】国土交通省HP　情報セキュリティ関連
https://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

# 重要インフラ分野の事業法におけるサイバーセキュリティ対策の規定状況

国土交通省

| 重要インフラ分野 | | | 事業法 | サイバーセキュリティ対策の規定・規律内容(注) |
|---|---|---|---|---|
| 事業法あり | 情報通信 | （電気通信） | 電気通信事業法 | ・設備の技術基準への適合・維持<br>・**管理規程の策定・届出（情報セキュリティの方針・対策を含む。）**<br>・利用者情報の取扱い状況のリスク評価 |
| | | （放送） | 放送法 | ・設備の技術基準への適合・維持<br>（設備の技術適合義務の１つとして）　**サイバーセキュリティの確保** |
| | | （ケーブルテレビ） | | |
| | （電力・ガス） | 電　力 | 電気事業法 | ・電気設備の技術基準への適合・維持<br>（設備の技術適合義務の１つとして）　**サイバーセキュリティの確保**<br>・保安規程の策定・届出 |
| | | ガ　ス | ガス事業法 | ・**保安規程の策定・届出（サイバーセキュリティの確保を含む。）** |
| | 医　療 | | 医療法 | ・（病院等管理者の遵守事項の１つとして）**サイバーセキュリティの確保** |
| | 金融 | （銀行） | 銀行法 | ・情報の適正な取扱いその他の健全かつ適切な運営の確保 |
| | | （生保・損保） | 保険業法 | |
| | | （証券） | 金融商品取引法 | ・業務管理体制の整備 |
| | | （資金決済） | 資金決済法 | ・情報の安全管理のための措置 |
| | クレジット | | 割賦販売法 | ・クレジットカード番号等の適切な管理 |
| | 水　道 | | 水道法 | ・（施設の技術適合義務の１つとして）　**サイバーセキュリティの確保** |
| | （運輸） | 航　空 | 航空法 | **＜法令に基づく対応を検討＞** |
| | | 空　港 | | |
| | | 鉄　道 | 鉄道事業法 | |
| | | 物　流 | 貨物自動車運送事業法等 | |
| | | 港　湾 | 港湾運送事業法 | ・事業の許可の申請（2024年3月31日施行）**サイバーセキュリティの確保** |
| 事業法なし | 政府・行政（自治体） | | ― ― ― | ― ― ― |
| | 化　学 | | | |
| | 石　油 | | | |

注：2023年12月時点調べ（港湾分野を除く）。**青字**は、法令に「サイバーセキュリティ」の言及があるもの（言及は全て省令レベル）。記載されている規律内容のうち、「サイバーセキュリティ」に言及のないものは、各省庁において「サイバーセキュリティ対策」が含まれていると解釈しているもの。

# 基幹インフラの安定的な提供の確保に関する制度の概要

国土交通省

- 基幹インフラの重要設備が役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、国が一定の基準のもと、**基幹インフラ事業（特定社会基盤事業）・事業者（特定社会基盤事業者）を指定**し、国が定めた重要設備（特定重要設備）の導入・維持管理等の委託をしようとする際には、**事前に国に届出を行い、審査を受ける制度**を構築。昨年11月に法を施行し、2024 年５月17日から制度運用開始。
- 国は、届け出られた計画書に係る特定重要設備が、我が国の外部から行われる妨害行為の手段として使用されるおそれが大きいと認めるときは、当該計画書を届け出た者に対し、妨害行為を防止するため必要な措置を講じた上で重要設備の導入等を行うこと等を勧告（命令）できる。

## 制度のスキーム


⑴ **対象事業**…現在法律で次の１５分野を外縁として規定。それぞれの分野について、必要な範囲に細分化し**政令**で絞り込む。

| | | | | |
|---|---|---|---|---|
| 1.電気 | 2.ガス | 3.石油 | 4.水道 | 5.鉄道 |
| 6.貨物自動車運送 | 7.外航海運 | 8.港湾運送（※） | 9.航空 | 10.空港 |
| 11.電気通信 | 12.放送 | 13.郵便 | 14.金融 | 15.クレジットカード |

⑵ **対象事業者（特定社会基盤事業者）**…絞り込んだ事業ごとに、事業所管大臣が、**省令**で基準を作成し、該当する者を**告示**で指定。

（※）2024 年５月17日、港湾運送分野を追加する改正法が公布。公布日から起算して１年６月を超えない範囲内において政令で定める日から施行

# 中小企業に向けた取組

国土交通省

## ～国土交通省所管事業者における情報セキュリティ対策の自己点検チェックリストの改定～

- サイバー攻撃手法の巧妙化、悪質化などにより事業に悪影響を及ぼすリスクは高まっており、重要インフラ事業者ではない事業者についても、自主的にサイバーセキュリティ確保に取組が必要
- 国土交通省では、鉄道、バス、バスターミナル、タクシー、宿泊施設、フェリー・旅客船及び空港・空港ビルの７分野を対象に、自組織のセキュリティ対策を自己点検できるチェックリスト（2021年4月）を改定
- 上記7分野に加え、航空、港湾、倉庫、トラック及び上水道も対象分野に加えた**自己点検チェックリストを2024年度末までに改定予定**
- 国土交通省所管事業者の情報セキュリティを確保するためのさらなる支援のあり方を検討するため、**所管事業者のセキュリティ対策状況及び必要としている支援内容について、アンケート調査及びヒアリングを実施予定**

### 現行の自己点検チェックリストの主な質問項目

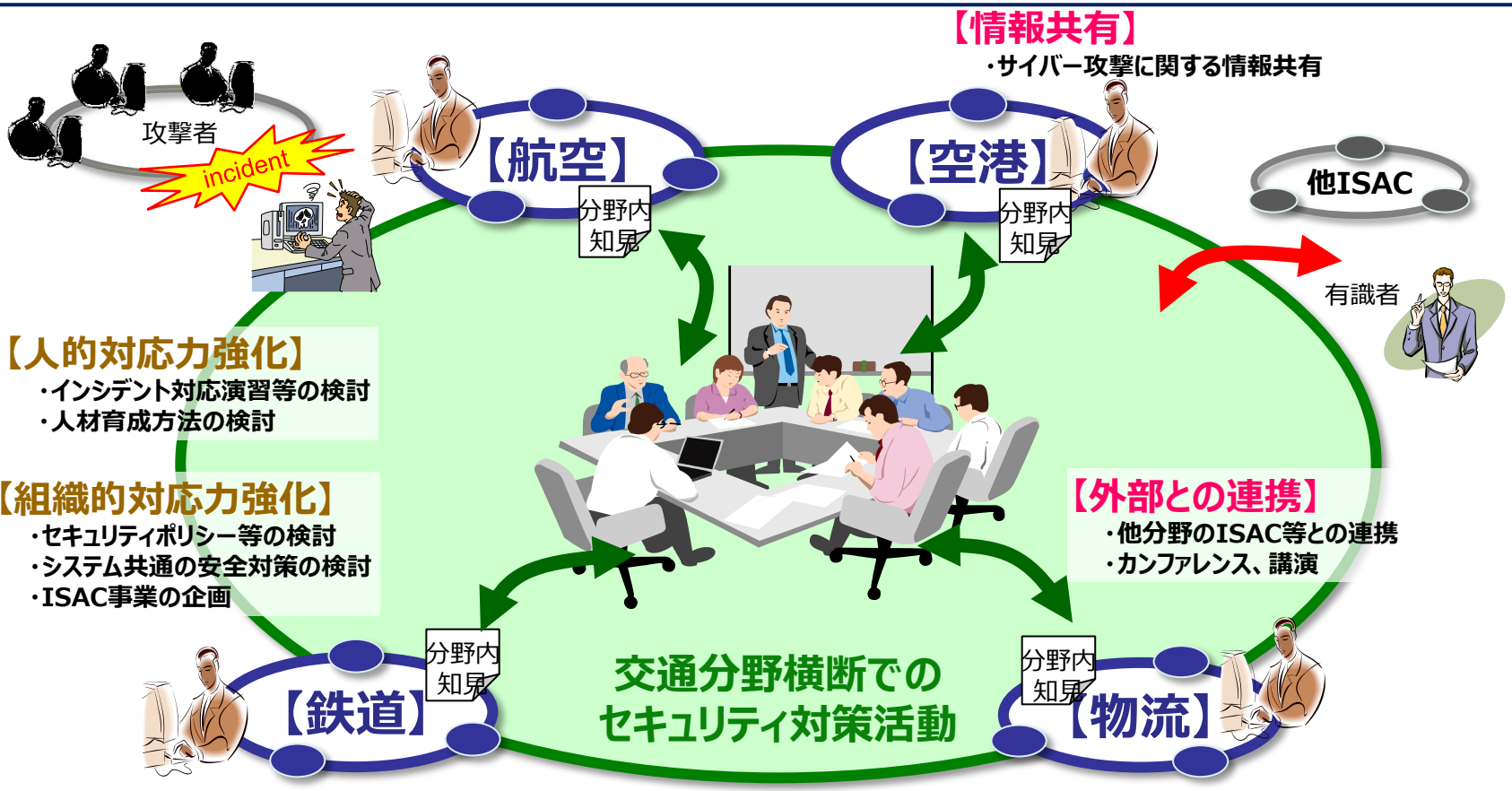
- Wi-Fi のセキュリティ対策：Wi-Fi 管理者パスワードを設定などアクセス制御を実施している
- ホームページのセキュリティ対策：ファイアウォールによる通信の適切なフィルタリングをしている
- 組織のセキュリティ対策：経営者が組織全体のセキュリティリスクに関する対応方針を策定している
- 重要システムのセキュリティ対策：システムで取り扱うデータをバックアップしている　等

【出典】国土交通省HP　情報セキュリティ関連
https://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

# 一般社団法人 交通ISACの概要

国土交通省

- 名称:一般社団法人交通ISAC
  (英文表示：Transportation Information Sharing and Analysis Center JAPAN)
- 設立:令和2年4月1日
- 会員数:87団体(R6.6.1現在【正会員66団体、賛助会員11団体、オブザーバー会員10団体】)
- 航空・空港・鉄道・物流の重要インフラ事業者等が中心となり、**サイバーセキュリティに関する情報共有・分析・対策を連携して行う体制**として設立



# 重要インフラに係るインシデント発生時等における国土交通省の取組

国土交通省

- 「重要インフラのサイバーセキュリティに係る行動計画」に基づき、NISCから提供される脆弱性情報等について、**重要インフラ事業者への情報提供**を実施
- インシデント発生時など**迅速な情報提供**が求められる際には、上記に加え、**交通ISAC**の取組も活用して**情報共有**を実施

## 事案発生時の例

- 令和4年9月7日、東京メトロ、大阪メトロ、e-Gov等一部の政府系Webサイト、ニコニコ動画、JCBブランドサイト、mixi等でアクセスしづらい状況が発生
  (親ロシア派ハッカー集団が日本国内WebサイトへのDDoS攻撃※を行ったとの声明を発表)
  →関係事業者への情報提供に加え、交通ISAC情報共有システムも活用

※Distributed Denial of Serviceの略：Webサーバなどに、複数のコンピュータから大量のパケットを送りつけることで、正常なサービス提供を妨げる行為

## 交通ISACでの対応

- 交通ISAC内で、各社(航空・空港・鉄道・物流問わず)が自社状況について情報共有
  - ✓ ハッカー集団が攻撃対象としてTelegramに投稿したWebサイトの一覧
  - ✓ 各社における影響(トラフィック増大の有無などの状況を監視)
  - ✓ その他、復旧状況や他の情報システムへの影響　等
- 金融ISACとの連携(相互の情報共有)
- セキュリティベンダー(交通ISAC賛助会員)から、後日、事案全体を調査・整理した資料が共有

# ご静聴ありがとうございました