# 経済安全保障推進法に基づく制度とサイバーセキュリティに関する国土交通省の取組

令和5年11月20日

国土交通省
大臣官房政策立案総括審議官
池光　崇

# アジェンダ



１．最近のサイバー攻撃関係事案

２．サイバーセキュリティに関する国土交通省の取組

# 名古屋港へのサイバー攻撃①(事案の概要)

国土交通省

- 今年7月、ランサムウェア感染により、名古屋港統一ターミナルシステム(NUTS)が機能停止
- この結果、トヨタ自動車における4つの部品組立拠点が一時操業停止するなどの影響が発生
- 事態覚知(7/4 6:30機能停止)から全ターミナル再開(7/6 18:15)まで59時間45分を要した

出典：読売夕刊
(7月5日 11面)

名古屋港にサイバー攻撃か
コンテナ搬出入停止

名古屋港のコンテナターミナルでシステム障害が発生し、4日朝からコンテナの搬出入が停止していることがわかった。港湾運送事業者でつくる名古屋港運協会（名古屋市港区）は5日、身代金要求型ウイルス「ランサムウェア」の攻撃だと原因と発表した。

愛知県警がサイバー攻撃の疑いがあるとみて捜査している。5日も終日、荷物の搬出入は行われないという。

同協会によると、障害が発生しているのは、港湾の6時半頃に発生した。協会側は5日午後6時頃までにシステムの復旧を図り、6日午前8時半頃からの搬出入作業の再開を目指すとしている。

名古屋港は自動車などを

年3月に一新したばかりだった。

システム障害は4日午前

トヨタ　愛知と岐阜４つの部品組立拠点停止へ

07月06日　18時15分

サイバー攻撃によるシステム障害で名古屋港でのコンテナの積み降ろしができなくなっていた影響で、トヨタ自動車は海外の完成車工場に送る部品を組み立てる愛知県と岐阜県の合わせて４つの拠点について、７日の稼働を停止することを決めました。

コンテナの積み降ろしは一部再開しているものの、トヨタでは物流の正常化には時間がかかる見通しのため稼働停止を決めたとしています。
海外の完成車工場には部品の在庫があることから、今のところ車の生産自体に影響はないとしています。

出典：NHK(7月6日)



名古屋港　各ターミナル等の機能と位置関係

出典：名古屋港運協会HP

# 名古屋港へのサイバー攻撃②(国土交通省における対応：検討委員会の設置)

国土交通省

- 有識者から成る「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」を立ち上げ、名古屋港で発生した事案の検証等を行うとともに、コンテナターミナルの運営に関する基幹的な情報システムに必要な情報セキュリティ対策、サイバーセキュリティ政策及び経済安全保障政策における港湾の位置付け等の整理・検討を実施中

**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 委員名簿**

| | | |
|---|---|---|
| 有識者 | 岩井 博樹 | 株式会社サイント 代表取締役 |
| | 小野 憲司 | 京都大学経営管理大学院 客員教授 |
| | 北尾 辰也 | 国土交通省最高情報セキュリティアドバイザー |
| | 椎木 孝斉 | 一般社団法人JPCERTコーディネーションセンター 理事 |
| | 柴崎 隆一 | 東京大学大学院工学系研究科レジリエンス工学研究センター 准教授 |
| 関係事業者等 | 北田 彰 | 商船港運株式会社 取締役執行役員(神戸国際コンテナターミナル) |
| | 木村 伸児 | 三菱倉庫株式会社 取締役常務執行役員(港湾運送事業者) |
| | 長山 達哉 | 静岡県交通基盤部 港湾局長(港湾管理者) |
| | 名村 悦郎 | 一般社団法人日本港運協会 理事 |
| | 人見 伸也 | 横浜川崎国際港湾株式会社 代表取締役社長(港湾運営会社連絡協議会 会長) |
| 行政関係者 | 紺野 博行 | 内閣官房内閣サイバーセキュリティセンター 内閣参事官 |
| | 田島 聖一 | 国土交通省総合政策局 情報政策課長 |
| | 稲田 雅裕 | 国土交通省港湾局長 |
| オブザーバー | 田中 博 | 内閣官房国家安全保障局<br>内閣府政策統括官（経済安全保障担当）付参事官（特定社会基盤役務担当） |

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/001633535.pdf

検討スケジュール

○第１回検討委員会(令和5年7月31日)
- 名古屋港におけるシステム障害の原因及び対応策の分析
- システムを運用する名古屋港運協会等からのヒアリング
- ヒアリングを踏まえての情報セキュリティ対策に関する議論

○第２回検討委員会(令和5年9月29日)
- 中間とりまとめ①(情報セキュリティ対策、システム障害発生時の対応策)
- サイバーセキュリティ政策及び経済安全保障政策における港湾の位置づけについての議論

○第３回検討委員会(令和5年11月下旬)
- 中間とりまとめ②(サイバーセキュリティ政策及び経済安全保障政策における港湾の位置づけ)
- 中間とりまとめ①を踏まえての対応についての議論

○第４回検討委員会(令和6年年明け)
- 最終とりまとめ

# 名古屋港へのサイバー攻撃③(国土交通省における対応：検討委員会での中間とりまとめ（概要）)

国土交通省

## 課題等

**【主な問題点】**

- 保守作業に利用する外部接続部分のセキュリティ対策が見落とされていた
  → 一般ユーザ向けのセキュリティ対策のみでなく、保守等に潜むリスクのセキュリティ対策も講じる必要がある

- 原因調査、システム復旧の両方の面において、バックアップが直近3日分と不足していた
  → プログラム等、更新頻度が低く必要性が高いデータについては、より長期間のバックアップを取る必要がある

**【主な評価点】**

- 日頃よりセキュリティ研修等を通じて愛知県警と名古屋港運協会との関係を構築しており、事案発生時の相談、対応がスムーズに実施できていた

- 事案発生後、早急に関係者を招集し、復旧までの間、意思決定機関として機能していた。特に、復旧を最優先すると判断したことにより、事案発生から丸2日半という短期間で復旧できた

## 対策

**【ターミナルオペレーションシステムに必要な対策】**

- セキュリティ対策を検討するために、システムの機器構成、ネットワーク構成、外部との接続状況等を把握すること

- ウイルスの潜伏期間を考慮し、バックアップは直近のもののみではなく、数週間前のものを含めて複数保存すること

**【コンテナターミナルの運用に必要な体制】**

- 情報セキュリティ対策の推進の責任者として最高情報セキュリティ責任者を指定し、情報セキュリティ対策を推進する上での最終決定権及び責任を持つこと

- サイバー攻撃が発生した場合に備え、被害の拡大防止、システム障害復旧、原因調査等に必要な報告や対応の手順等を予め整理しておくこと

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より作成
（https://www.mlit.go.jp/kowan/content/001633535.pdf）

# 政府機関のメールセキュリティ製品の脆弱性を突かれたサイバー攻撃

国土交通省

- 今年8月、内閣サイバーセキュリティセンター（NISC）、気象庁、気象研究所において、メールセキュリティ製品の脆弱性を突かれたサイバー攻撃によるメール流出の可能性を公表
- 具体的には、外部からのメールを受信するメールシステムが攻撃を受け、メールデータの一部が流出した可能性が確認されたもの
- メーカーからの脆弱性公表は今年5月。全世界では少なくとも昨年10月以降サイバー攻撃を受けていたと推定

朝日新聞
(東京/Tokyo)
35面
20230805(土)

## NISCにサイバー攻撃 5000人情報流出か

### 攻撃、気象庁にも

政府の内閣サイバーセキュリティセンター（NISC）は4日、電子メールシステムがサイバー攻撃を受け、約5千人分の個人情報を含むメールのデータが外部に流出した可能性があると発表した。NISCと取引のある民間企業や協力組織が被害を受けた可能性があるという。

発表によると、流出した可能性があるのは、昨年10月から今年6月までの間に、インターネットを経由してNISCとメールのやりとりをした個人や組織のメール。該当者約5千人には4日までにメールで通知した。政府の個人情報保護委員会には報告済みという。

電子メールシステムを構成する機器に対する不正な通信の痕跡が6月13日に見つかり、調査していた。NISCは政府のサイバーセキュリティー戦略の推進を担い、省庁など政府機関のセキュリティー監視も行う。

気象庁も4日、同庁と気象研究所の電子メール関連機器に不正な通信の痕跡が見つかったと発表した。昨年6月から今年5月にかけて外部から送られてきたメールデータの一部が流出した可能性がある。

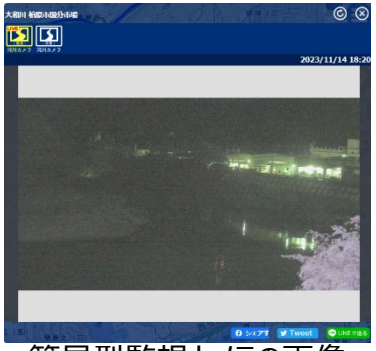
（編集委員・須藤龍也）

# 国土交通省　簡易型河川監視カメラへのサイバー攻撃

国土交通省

- 今年1月、国土交通省地方整備局が管理する簡易型河川監視カメラへの不正アクセス事案が発生
- 初期パスワードが変更されないまま運用、通常運用と異なる通信量の大幅な増加を観測したことで事案が発覚

| | 簡易型河川監視カメラ  |
|---|---|
| 回線の接続形態 | モバイル回線(インターネット経由)接続 |
| 設置条件 | 太陽電池等で稼働可能 |
| 監視の形態 | 5分ごとに静止画を伝送 |
| 夜間撮影 | 月明かり程度の明るさの撮影が可能 |
| カメラの機能 | ズーム、首振り機能なし(定点撮影に特化) |
| 監視の状況 | 画像集約サーバ経由の閲覧が必要 |
| 導入費用(カメラ本体) | 30万円以下 |

簡易型監視カメラの画像
(上段は平常時、下段は表示時点での最新画像)

# 「経済安全保障」関係事案の発生と取組の必要性

国土交通省

## 我が国でも、サイバーセキュリティにかかる事案が相次いで確認

事例１(個人情報の大規模流出)

2015年、日本年金機構職員がメールに添付されたマルウェア付きファイルを開封した結果、PCが外部から遠隔操作され、加入者の個人情報約125万件が流出。

事例２(安全保障に影響を及ぼすデータの流出)

2019年に発生した三菱電機の事案について、外部に流出した可能性のある防衛関連情報のファイル約2万件のうち、安全保障への影響を及ぼすおそれのあるデータが約60件含まれていたことが2020年に判明。

事例3(情報共有ツールを経由したデータの窃取)

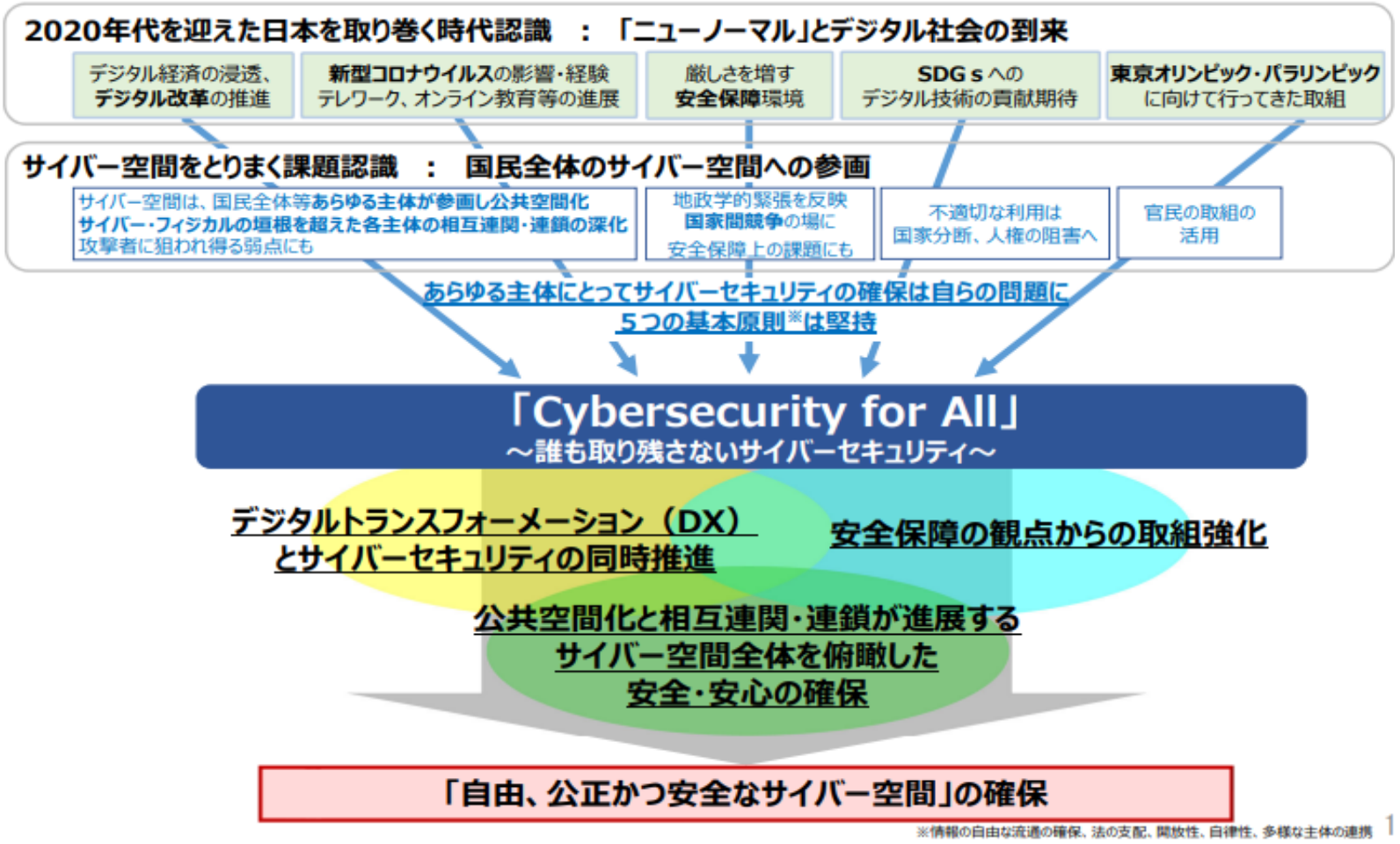
2021年、富士通が提供する情報共有ツール(ProjectWEB)に対するサイバー攻撃が発覚。後に、同ツールを利用する100以上の組織(国土交通省も含む)から個人情報を含むデータが窃取されたことが判明。

- 経済のグローバル化や技術革新によるデジタル化の進展は、企業の経済活動や大学などの研究活動を国内で完結させることが現実的ではない現代において、大きなリスクにもなり得る
- 我が国から技術・データ等が流出した場合、大量破壊兵器等の研究・開発に転用されるおそれや企業に対する信頼の低下、我が国企業や大学等における技術的優位性の喪失に伴う国際的な競争力の低下にもつながりかねず、その経済的損失は計り知れない
- 各国は、自国の優位性を確保するために機微な技術・データ・製品等の獲得に向けた動きを活発化
- 国益を守るため、各国は規制や取締りを強化

# サイバーセキュリティ対策の概要

国土交通省

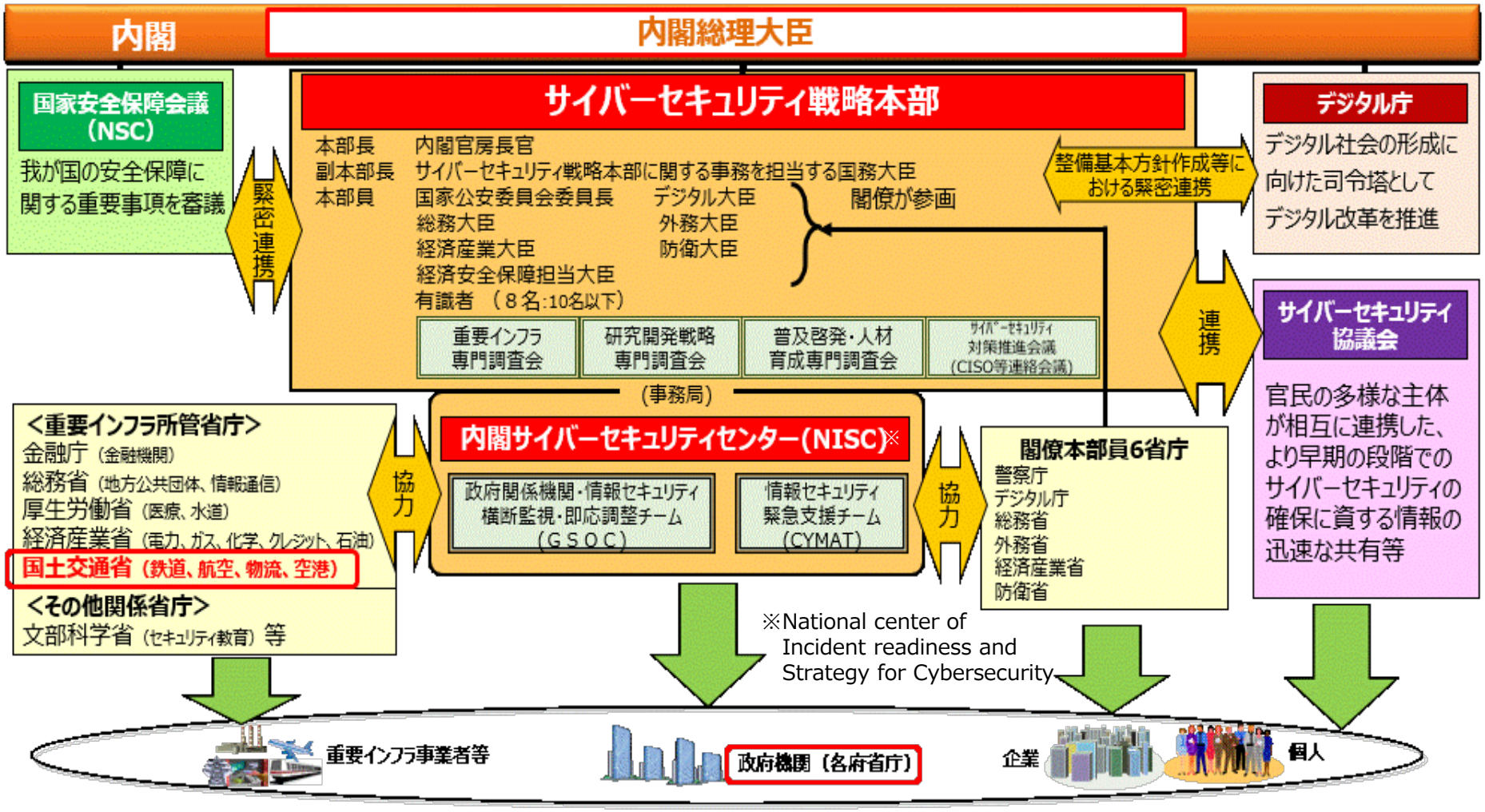
| | |
|---|---|
| サイバーセキュリティ基本法<br>(平成26年11月成立) | 我が国のサイバーセキュリティに関する施策を総合的かつ効果的に推進するための法律 |
| サイバーセキュリティ戦略<br>(3年に1度改定、令和3年9月閣議決定) | サイバーセキュリティ基本法に基づき、政府のサイバーセキュリティ政策の基本的な方向性を示すもの |




出典：内閣サイバーセキュリティセンターHP(サイバーセキュリティ戦略の概要)
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf

# サイバーセキュリティに関する政府の推進体制

国土交通省




【出典】我が国のサイバーセキュリティ戦略について（令和4年6月）　NISC作成資料

# 経済安全保障に関する政府の推進体制

国土交通省

- 国家安全保障局が司令塔となり、関係行政機関が相互に協力して安全保障の確保に関する経済施策を総合的かつ効果的に推進
- 我が国の安全保障に関する重要事項については、国家安全保障会議での審議を経る

## 国家安全保障会議

「国家安全保障」に関する重要事項を審議する機関

**議長**　内閣総理大臣
**議員**　国務大臣等

緊密連携

## 経済安全保障推進会議

社会経済構造の変化、国際情勢の複雑化等により、安全保障の裾野が経済分野に急速に拡大する中、経済安全保障の取組を強化・推進

**議長**　内閣総理大臣
**副議長**　経済安全保障担当大臣、内閣官房長官
**構成員**　内閣総理大臣が指名する国務大臣

## 内閣官房の他の機関

・内閣官房副長官補（事態対処・危機管理担当）付
・内閣サイバーセキュリティセンター（NISC）
・内閣情報調査室　など

連携 緊密

(事務局)

## 内閣官房 国家安全保障局 (NSS)※

・国家安全保障会議を恒常的にサポートする事務局

・国家安全保障に関する経済政策等の基本方針・重要事項に関する企画立案・総合調整

・緊急事態への対処に当たり、国家安全保障に関する経済政策等の観点から必要な提言を実施　等

※National Security Secretariat

## 経済安全保障法制に関する有識者会議

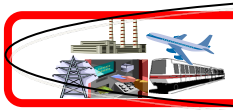
経済安全保障担当大臣の下に開催され、以下の４つの制度に関して有識者の意見を聴く

- 重要物資の安定的な供給の確保に関する制度
- 基幹インフラ役務の安定的な供給の確保に関する制度
- 先端的な重要技術の開発支援に関する制度
- 特許出願の非公開に関する制度

協力

**<関係省庁>**（）は基幹インフラの所管する分野

金融庁（金融機関）
総務省（電気通信、放送、郵便）
厚生労働省（水道）
経済産業省（電気、ガス、石油、クレジット）
国土交通省（鉄道、貨物自動車運送、外航貨物、航空、空港）
など



基幹インフラ事業者

その他事業者

出典：内閣官房国家安全保障局HPを参考に国土交通省において作成

# 経済安全保障推進法制の概要

国土交通省

## 経済安全保障推進法(令和4年法律第43号)
(経済政策を一体的に講ずることによる安全保障の確保の推進に関する法律)

| ４つの柱 | 重要物資の安定的な供給の確保に関する制度 | 基幹インフラ役務の安定的な供給の確保に関する制度 | 先端的な重要技術の開発支援に関する制度 | 特許出願の非公開に関する制度 |
|---|---|---|---|---|
| 対象領域 | 半導体、蓄電池、重要鉱物、工作機械・産業用ロボット、船舶部品など | 電気、ガス、水道、情報通信、放送、金融、クレジットカード、運輸、郵便など | 宇宙、海洋、量子、AI、バイオなどの分野における先端的な重要技術 | 原子力関連技術、航空機等の偽装・隠ぺい技術など |
| 概要 | • 国民の生存や国民生活・経済活動に甚大な影響のある物資(半導体や重要鉱物など)の安定供給の確保のため、「特定重要物資」を指定<br>• 供給確保計画の認定を受けた民間事業者には資金支援を行い、民間の取組では不足の場合には、政府が対策(備蓄など)を実施 | • 特定社会基盤事業14分野の重要設備(機器、ソフトウェア、クラウドサービスなど)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ことを防止するため、重要設備の導入・維持管理などの委託先を事前審査し、勧告・命令などを可能にする | • 安全保障上重要な先端技術の研究開発の促進と成果活用のため、資金支援や官民での情報共有を行う協議会を設置<br>• 対象技術はシンクタンクなどによる調査で不断に見直し | • 安全保障上機微な発明の技術流出を防止するため、出願後の審査で必要と認められた場合には出願内容を非公開化し、特許の実施（対象物又は対象技術を使った物の生産）を制限<br>• 審査対象技術の外国出願を制限<br>• 発明の実施が許可されず被った損害に対する補償の規定あり |

出典：経済安全保障推進法及び同法に基づく制度の基本指針を基に国土交通省において作成

# 重要インフラ事業者と基幹インフラ事業者の関係

国土交通省

## 重要インフラ事業者(サイバーセキュリティ基本法)

- 国民生活及び経済活動の基盤であって、その機能が停止または低下した場合に国民生活または経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者

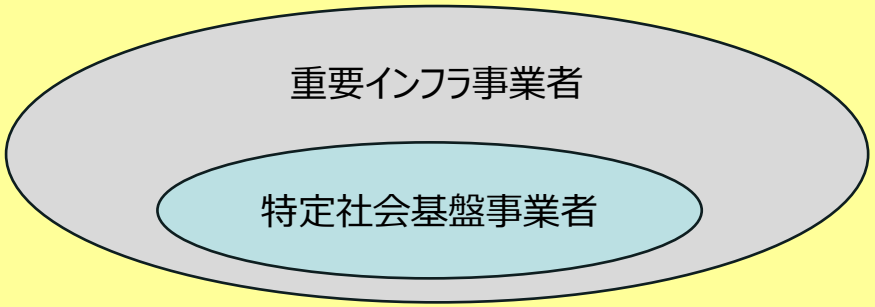
| 重要インフラ(全14分野) | 基幹インフラ(全14分野) |
|---|---|
| ●情報通信 | ●電気通信 |
| ●金融 | ●金融 |
| ●**航空** | ●**航空** |
| ●**空港** | ●**空港** |
| ●**鉄道** | ●**鉄道** |
| ●電力 | ●電気 |
| ●ガス | ●ガス |
| ●政府・行政サービス | ●水道 |
| ●医療 | ●放送 |
| ●水道 | ●**貨物自動車運送** |
| ●**物流** | ●**外航貨物** |
| ●化学 | ●郵便 |
| ●クレジット | ●クレジット |
| ●石油 | ●石油 |

※**赤字**は国土交通省所管分野、水道分野は令和6年度より当省が所管

## 特定社会基盤事業者(経済安全保障推進法)

- 国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもののうち、以下①または②のいずれかに当てはまる役務を提供する事業に絞り込み、事業規模や代替可能性を考慮した上で事業者を指定
  - ① 国民生活又は経済活動が依存しており、その利用を欠くと経済・社会秩序の平穏を損なう事態が生じ得る役務
  - ② 国民の生存に不可欠で代替が困難な役務

### 対象事業者(対象範囲)のイメージ



# 重要インフラ事業者と対象となる重要システム例

国土交通省

## 別紙1 対象となる重要インフラ事業者等と重要システム例

| 重要インフラ分野 | | 対象となる重要インフラ事業者等(注1) | 対象となる重要システム例(注2) |
|---|---|---|---|
| 情報通信 | | ・主要な電気通信事業者<br>・主要な地上基幹放送事業者<br>・主要なケーブルテレビ事業者 | ・ネットワークシステム<br>・オペレーションサポートシステム<br>・編成・運行システム |
| 金融 | 銀行等<br>生命保険<br>損害保険<br>証券<br>資金決済 | ・銀行、信用金庫、信用組合、労働金庫、農業協同組合等<br>・資金清算機関<br>・電子債権記録機関<br>・生命保険<br>・損害保険<br>・証券会社<br>・金融商品取引所<br>・振替機関<br>・金融商品取引清算機関<br>・主要な資金移動業者<br>・主要な前払式支払手段(第三者型)発行者　等 | ・勘定系システム<br>・資金証券系システム<br>・国際系システム<br>・対外接続系システム<br>・金融機関相互ネットワークシステム<br>・電子債権記録機関システム<br>・保険業務システム<br>・証券取引システム<br>・取引所システム<br>・振替システム<br>・清算システム |
| 航空 | | ・主たる定期航空運送事業者 | ・運航システム<br>・予約・搭乗システム<br>・整備システム<br>・貨物システム |
| 空港 | | ・主要な空港・空港ビル事業者 | ・警戒警備・監視システム<br>・フライトインフォメーションシステム<br>・バゲージハンドリングシステム |
| 鉄道 | | ・JR各社及び大手民間鉄道事業者等の主要な鉄道事業者 | ・列車運行管理システム<br>・電力管理システム<br>・座席予約システム |
| 電力 | | ・一般送配電事業者、主要な発電事業者　等 | ・電力制御システム<br>・スマートメーターシステム |
| ガス | | ・主要なガス事業者 | ・プラント制御システム<br>・遠隔監視・制御システム |
| 政府・行政サービス | | ・地方公共団体 | ・地方公共団体の情報システム |
| 医療 | | ・医療機関<br>（ただし、小規模なものを除く。） | ・診療録等管理システム<br>・診療業務支援システム<br>・地域医療支援システム |
| 水道 | | ・水道事業者及び水道用水供給事業者<br>（ただし、小規模なものを除く。） | ・水道施設や水道水の監視システム<br>・水道施設の制御システム |
| 物流 | | ・大手物流事業者 | ・集配管理システム<br>・貨物追跡システム<br>・倉庫管理システム |
| 化学 | | ・主要な石油化学事業者 | ・プラント制御システム |
| クレジット | | ・主要なクレジットカード会社<br>・主要な決済代行業者<br>・指定信用情報機関　等 | ・クレジット(包括信用購入あつせん及び二月払購入あつせん)に係る決済システム<br>・信用情報提供・収集システム |
| 石油 | | ・信用情報提供・収集システム | ・受発注システム<br>・生産管理システム<br>・生産出荷システム |

注1 ここに掲げているものは、重点的に対策を実施すべき重要インフラ事業者等であり、行動計画の見直しの際に、事業環境の変化及びITへの依存度の進展等を踏まえ、対象とするものの見直しを行う。
注2 ここに掲げているものは、例であり全てではない。

※**赤枠**は国土交通省所管分野、水道分野は令和6年度より当省が所管



出典：「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４年６月策定）より抜粋

# 重要インフラ事業者のサイバーセキュリティ強化関係の国土交通省の取組

国土交通省

- 政府では、「サイバーセキュリティ戦略」（令和３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」（令和４年６月１７日サイバーセキュリティ戦略本部決定）を策定
- 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（航空、空港、鉄道、物流)毎に「情報セキュリティ確保に係る安全ガイドライン」を策定（平成３１年３月２９日）
- 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

- 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

# 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

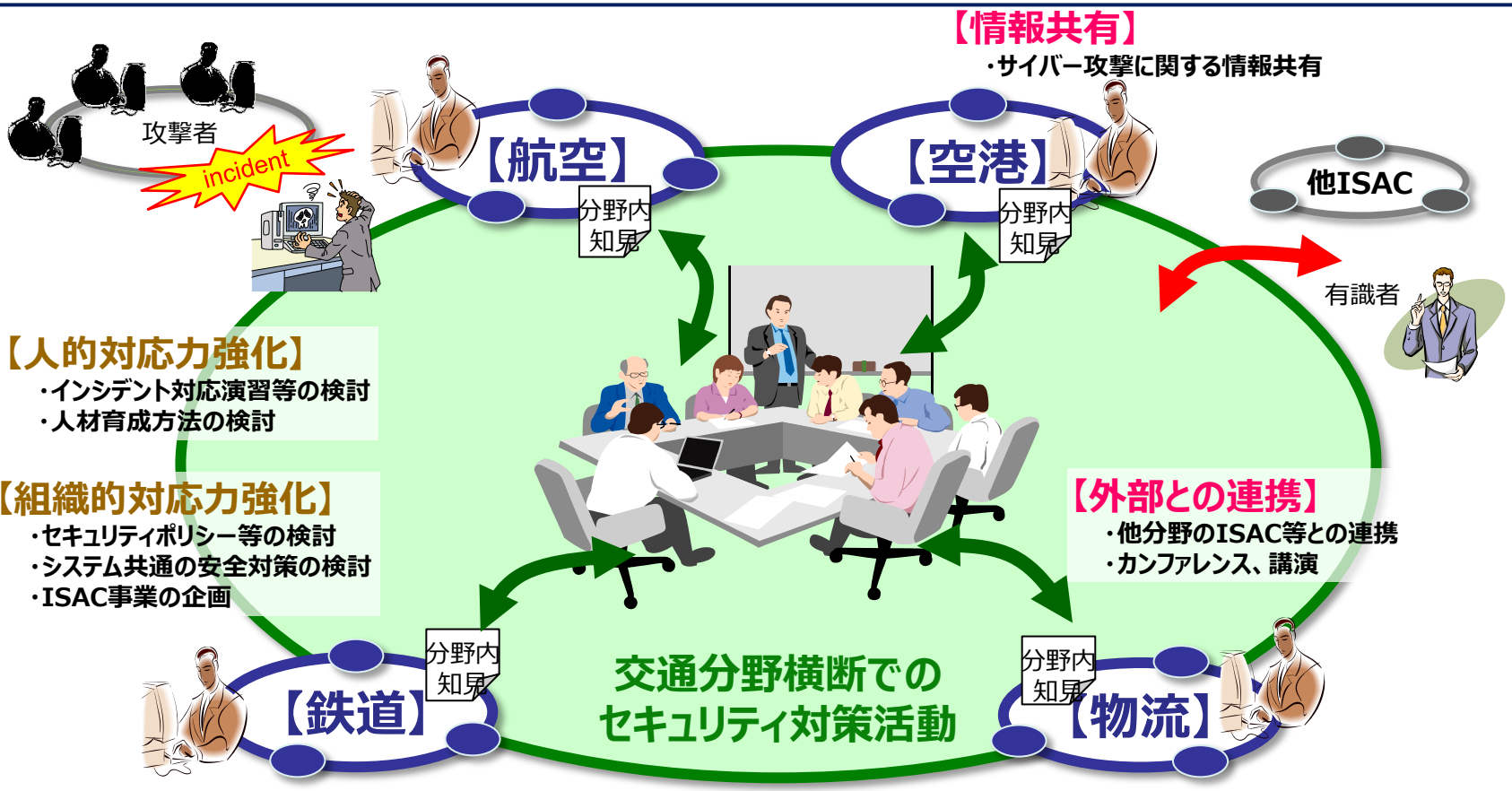
## 交通ISACでの対応

- 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

# 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:88団体(R5.6.23現在【正会員67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



# 交通ＩＳＡＣの主な活動例

国土交通省

- セキュリティ対策情報(体制、規模、技術的内容等)についての情報交換
  - ✓ ChatGPTの企業利用や社内セキュリティ規程整備状況等について情報交換

- セキュリティベンダーからのサイバー攻撃や対策に係る最新情報の入手
  - ✓ 具体の攻撃事案について、事案全体を調査・整理した資料の共有
  - ✓ ランサムウェア感染について、最新の攻撃手法や対策等についての情報共有

- 国からの情報提供
  - ✓ 関係事業者へのサイバー攻撃等に関する情報提供のほか、交通ISAC会員向け情報共有ツールを用いたサイバー攻撃等に関する情報の提供

- インシデント発生時における国や各社等との情報共有
  - ✓ 他社の被害情報(攻撃元IPアドレス情報やトラフィック変化情報など)を参考に、自社における被害状況把握や対応策検討に活用

- 企業活動におけるサイバーセキュリティ上の有益な情報共有
  - ✓ 損害保険会社を講師に招き、サイバー保険に関する説明会を実施

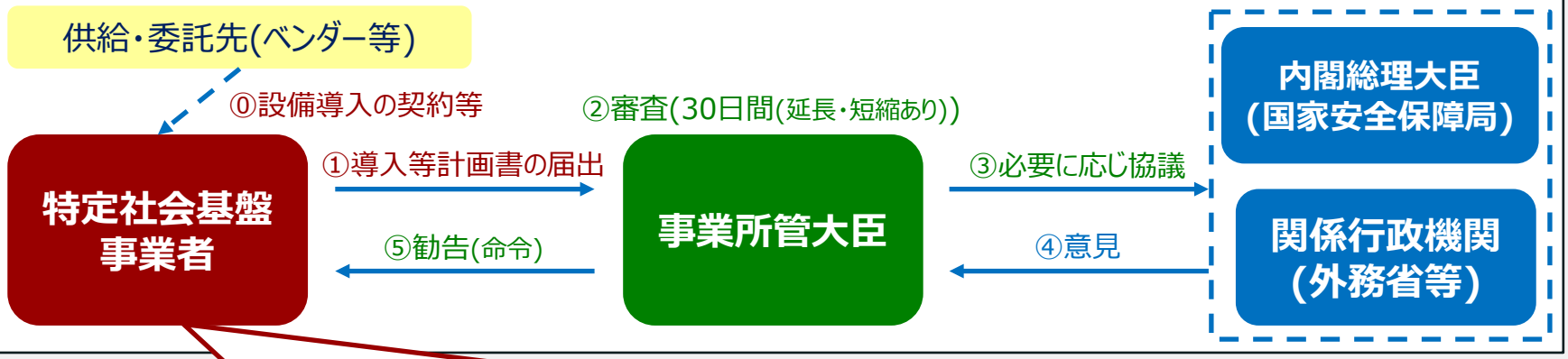
# 基幹インフラ役務の安定的な提供の確保に関する制度(概要)

国土交通省

## 趣旨

- 基幹インフラ役務(電気・ガス・水道等)の安定的な提供の確保は安全保障上重要
- 基幹インフラの重要設備は、サイバー攻撃等による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おそれあり
- 基幹インフラの重要設備が我が国の外部から行われる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、重要設備の導入・維持管理等の委託を事前に審査
- 国土交通省においても、審査体制強化のための体制整備(定員要求)を実施中
- 本制度は、令和6年5月17日より開始

## 制度のスキーム




(1) 対象事業 ※桃色塗りは交通分野、水道分野は令和6年度から当省所管

| | | | | |
|---|---|---|---|---|
| 電気 | ガス | 石油 | 水道 | 鉄道 |
| 貨物自動車運送 | 外航貨物 | 航空 | 空港 | 電気通信 |
| 放送 | 郵便 | 金融 | クレジットカード | |

(2) 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

# 基幹インフラに関する規制対象事業、事業者、特定重要設備

国土交通省

R5.11.17公表

| 対象分野/特定社会基盤事業の指定 | | 特定社会基盤事業者 | 指定基準 | 特定重要設備 |
|---|---|---|---|---|
| 鉄道 | 第一種鉄道事業 | 北海道旅客鉄道株式会社<br>東日本旅客鉄道株式会社<br>東海旅客鉄道株式会社<br>西日本旅客鉄道株式会社<br>九州旅客鉄道株式会社 | 旅客営業キロ：1,000km以上<br>※新幹線を運行している会社 | 列車運行管理システム<br>※列車運行のため重要な進路制御を集中的に行うことから対象 |
| 貨物自動車運送 | 一般貨物自動車運送事業 | 日本通運株式会社<br>佐川急便株式会社<br>ヤマト運輸株式会社 | 実車キロ、輸送トン、車両数のシェア：<br>いずれも5%以上　かつ　全国に営業所を設置 | 輸配送管理システム<br>※配送される貨物の中央管理を司ることから対象 |
| 外航海運 | 貨物定期航路事業 | 日本郵船株式会社<br>株式会社商船三井<br>川崎汽船株式会社 | 輸送量、運航隻数のシェア：<br>いずれも10%以上 | 荷役管理システム<br>※貨物の積卸に必要な配置計画を一元作成することから対象 |
| | 不定期航路事業 | | | |
| 航空 | 国際航空運送事業 | 全日本空輸株式会社<br>日本航空株式会社 | いずれかの事業の特定本邦航空運送事業者における運航回数：全体のシェア25%以上 | 飛行計画作成システム<br>※航空機の運航に不可欠な飛行計画を作成することから対象 |
| | 国内定期航空運送事業 | | | |
| 空港 | 空港の設置及び管理を行う事業 | 成田国際空港株式会社<br>新関西国際空港株式会社<br>関西エアポート株式会社<br>福岡国際空港株式会社<br>北海道エアポート株式会社<br>中部国際空港株式会社 | 年間旅客数：1,000万人以上　かつ<br>国際航空輸送網又は国内航空輸送網の拠点となる空港を管理・運営<br>(国管理空港は指定対象外) | 飛行場灯火定電流調整装置システム<br>※航空機の安全な離着陸を援助する灯火の制御を司ることから対象 |
| | 空港に係る公共施設等運営事業 | | | |

# ご静聴ありがとうございました