サイバーセキュリティに関する政府・国土交通省の取組

令和７年１２月１０日

国土交通省
大臣官房政策立案総括審議官
長井　総和

アジェンダ

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取組

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

サイバー攻撃の脅威の増大①

国土交通省

■サイバー攻撃は巧妙化・高度化するとともに、その被害は増加傾向。
質・量両面でサイバー攻撃の脅威は増大。

サイバー攻撃の巧妙化・高度化

公開サーバへの攻撃

ウェブサーバ・外向けサービスへの大量送信　等

エストニア・2007年

ウェブサイト等の停止

↓

IT系システムの侵害

情報システム内部への侵入・暗号化
（主に既知の脆弱性を悪用）

WannaCry・2017年
コロニアルパイプライン・2021年
大阪急性期・総合医療センター・2022年

システム障害
身代金要求

↓

重要インフラ等への侵入・潜伏

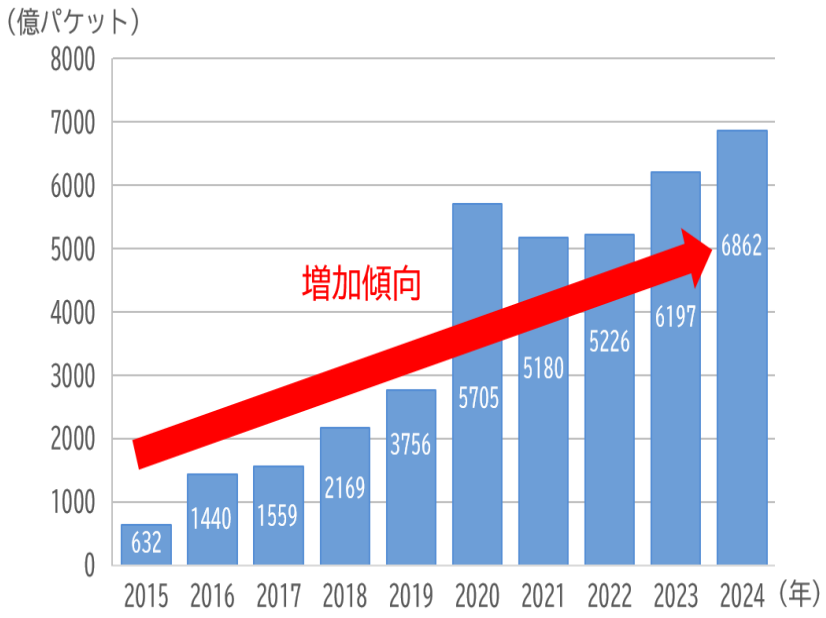
最深部・制御系システムに至る高度な侵入・潜伏
（ゼロデイ脆弱性の活用、システム内寄生戦術など）

ウクライナ・2015年/2022年等
Volt Typhoon・2023年

インフラ機能停止

サイバー攻撃の増大

サイバー攻撃関連通信数（※）



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2024（令和７年２月13日）」を基に作成

※NICTの観測用IPアドレス約29万に届いたパケットの数。

【出典】 内閣官房国家サイバー統括室　第15回サイバーセキュリティ国際シンポジウム講演資料を基に国土交通省で作成

サイバー攻撃の脅威の拡大②

国土交通省

■攻撃の巧妙化・高度化、国家を背景とした攻撃キャンペーン等により、国民生活・経済活動、さらには安全保障に被害が及ぶおそれが顕在化。

■個人・中小企業、さらに委託先等あらゆる主体が攻撃の標的化。

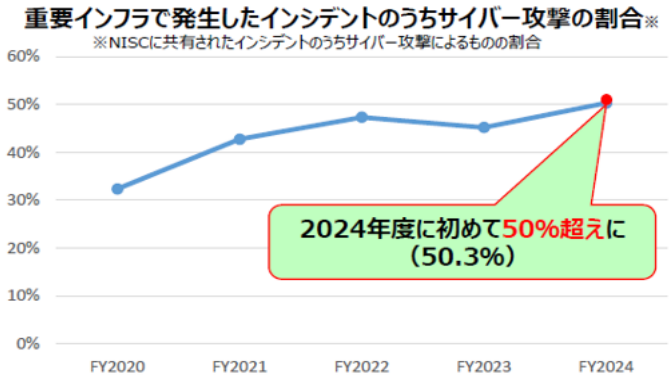
→官民連携の強化、社会全体のサイバーセキュリティ向上が急務

国家背景とされるアクターによる攻撃

・23年、米国は「Volt Typhoon」が国内重要インフラの機能不全を狙い、システム内寄生攻撃等を実施と公表
・19年以降、「Mirror Face」が対日攻撃キャンペーンを実行
・24年「TraderTrailor」が暗号資産窃取

委託先・サプライチェーンへの攻撃

・22年、取引先への攻撃により、大手自動車メーカーの国内全工場が一時操業停止
・22年、委託先の給食事業者を経由した攻撃により、病院が通常診療を一時停止



【出典】 内閣官房国家サイバー統括室HP　サイバーセキュリティ戦略本部　第1回会合資料を基に国土交通省で作成

日本企業に対するサイバー攻撃事例

国土交通省

アサヒグループホールディングス　システム障害事案（2025年9月）

- 2025 年 9 月 29 日、ランサムウェアによるサイバー攻撃を受け、国内の業務システムが停止。

影響等

- 国内の受注・出荷システム、物流システム、コールセンター業務が停止。
- 国内約30工場で一時操業停止。ビール・飲料の出荷が大幅に遅延。

アスクル株式会社　システム障害事案（2025年10月）

- 2025 年 10 月 19 日、ランサムウェアによるサイバー攻撃を受け、基幹システムの一部が暗号化。

影響等

- 法人向け通販「ASKUL」、個人向け「LOHACO」、物流子会社「ASKUL LOGIST」の業務停止。
- 顧客問い合わせ情報や仕入先情報の一部流出

【出典】各種報道等

国内交通インフラに対するサイバー攻撃事例

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が、ランサムウェアの感染を受けて停止**
- **荷役スケジュールに影響が生じた船舶37隻**（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）**

【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

とびしま
【名古屋港「飛島ふ頭」南側コンテナターミナル】

【写真出典】
国土交通省 中部地方整備局
名古屋港湾事務所　公式 X

日本航空 ネットワーク障害事案（2024年12月）

- 2024年12月26日、**DDoS攻撃により、社外システムと通信しているシステム**（飛行計画システム等）**で不具合**が発生
- 国内線に**５便の欠航**、**国際線11便**（最大遅延幅４時間02分）、**国内線60便**（最大遅延幅１時間26分）**に遅延**が発生

【出典】日本航空HP

2. サイバー安全保障に関する政府の取組

サイバーセキュリティ対策（交通インフラ関係概観）

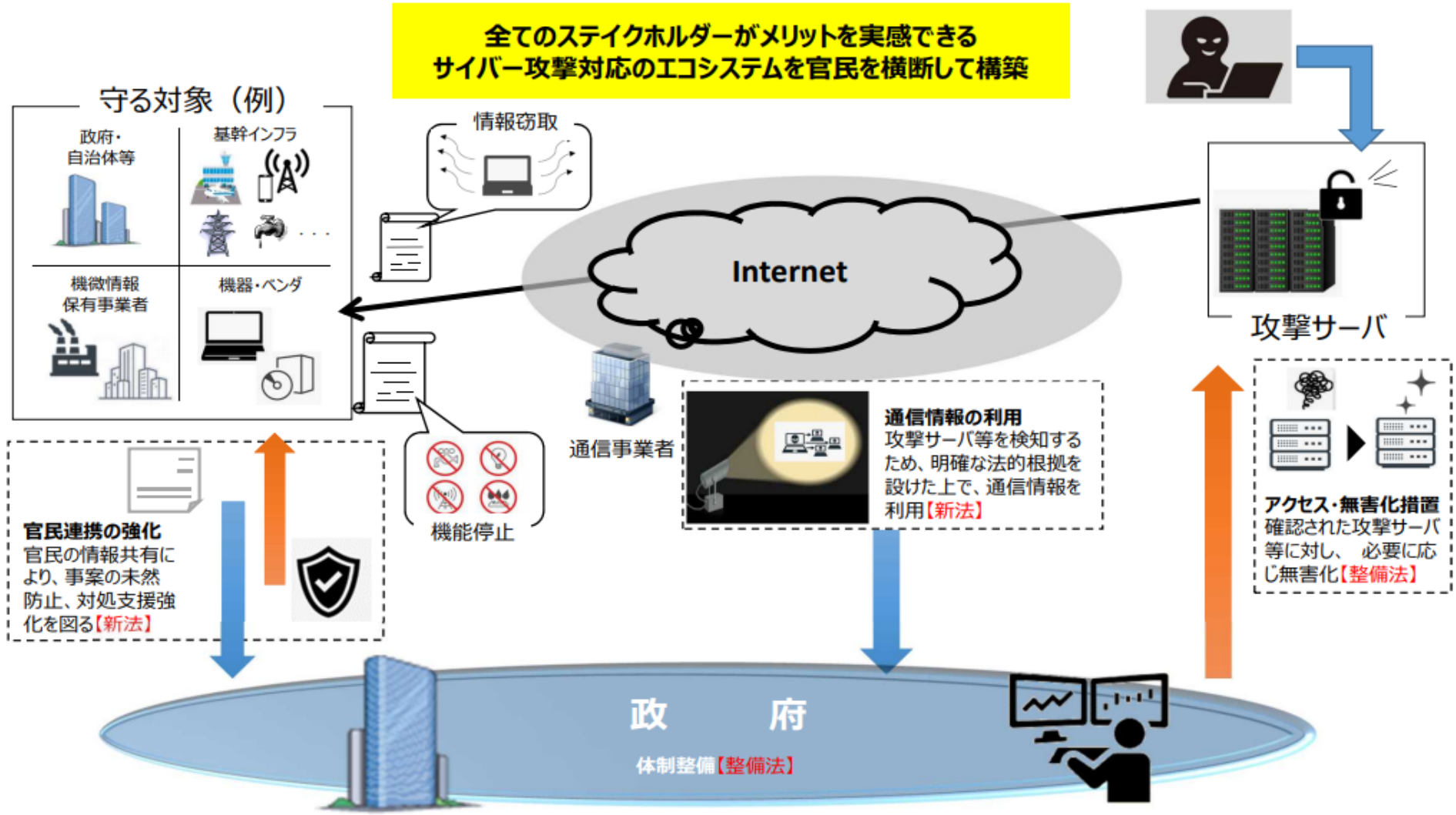
国土交通省

法律	サイバーセキュリティ基本法	サイバー対処能力強化法（同整備法）	経済安全保障推進法
目的	サイバーセキュリティに関する施策の総合的かつ効率的な推進	国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれのある国等の重要電子計算機に対する不正な行為による被害の防止	安全保障の確保に関する経済施策の総合的かつ効果的な推進
基本方針等	サイバーセキュリティ戦略	基本方針	基本方針
インフラ関係施策	行動計画 分野別ガイドライン	①官民連携の強化 ②通信情報の利用 ③攻撃者のサーバ等への侵入・無害化	重要設備の導入・維持管理等の委託の事前審査等

※上記のほか、サイバーセキュリティに関係する法律としては、デジタル社会形成基本法、不正アクセス禁止法、電子署名法、個人情報保護法等がある。

能動的サイバー防御に係る法制度の全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」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。



【出典】 内閣官房HP サイバー対処能力強化法及び同整備法説明資料 より

サイバー対処能力強化法※1及び同整備法※2

国土交通省

●国家安全保障戦略（令和4年12月16日閣議決定）では、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との目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISC※3の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置**　等の実現に向け検討を進めるとされた。

●令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

総　則　□　目的規定、基本方針等　（第１章）

官 民 連 携　（強化法）

- □　基幹インフラ事業者による
  - ・　導入した一定の電子計算機の届出
  - ・　インシデント報告

  （第２章）
- □　情報共有・対策のための協議会の設置　（第９章）
- □　脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用　（強化法）

- □　基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- □　（同意によらない）通信情報の取得　（第４章、第６章）
- □　自動的な方法による機械的情報の選別の実施　（第22条、第35条）
- □　関係行政機関の分析への協力　（第27条）
- □　取得した通信情報の取扱制限　（第５章）
- □　独立機関による事前審査・継続的検査　等（第10章）

→　□　分析情報・脆弱性情報の提供等　←（第８章）

アクセス・無害化措置　（整備法）

- □　重大な危害を防止するための警察による無害化措置
- □　独立機関の事前承認・警察庁長官等の指揮　等（警察官職務執行法改正）
- □　内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- □　自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等　（整備法）

- □　サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- □　内閣サイバー官の新設（内閣法改正）　等

7月1日から施行

施行期日　公布の日（令和7年5月23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　等

※1　重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）

※2　重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）

※3　内閣サイバーセキュリティセンター（令和７年７月１日に国家サイバー統括室（NCO）に改組）

【出典】　国家サイバー統括室HP　サイバーセキュリティ推進専門家会議　第1回会合資料を基に国土交通省で作成

サイバー対処能力強化法に基づく「基本方針」の策定に向けて

国土交通省

第１節　本法による各種措置を行うこととなった背景・経緯

サイバー脅威は国民生活・経済活動を脅かす**まさに災害のような存在**

- ○ 昨今、国家を背景としたサイバー攻撃が行われるなどサイバー分野における安全保障の確保が切迫した課題に。
- ○ 攻撃の巧妙化・高度化が進み、サイバー攻撃関連通信数も増加傾向にあり、質・量両面でサイバー攻撃の脅威は増大。
- ○ あらゆる主体がサイバー攻撃のリスクに晒され、一主体に対する攻撃による被害の影響が社会全体にまで波及するおそれ。

⇒「**国家安全保障戦略**」（令和４年12月国家安全保障会議及び閣議決定）では、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こととした。これに基づき、**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**が開催され、令和６年11月に提言を取りまとめ。

⇒ 令和７年２月、当該提言に基づく法律案が国会に提出され、国会での審議を経て、①**官民連携の強化**及び**通信情報の利用**に係る制度の導入を内容とする**サイバー対処能力強化法**、及び②アクセス・無害化措置に係る制度の導入等を内容とする同整備法が成立し、同年５月23日に公布。

○ 法の段階的な施行を経て、基本方針に基づき効果的かつ適正に制度の運用を図ることを通じ、**関係機関・関係者が一体となってサイバー脅威に対する我が国のサイバー対処能力を強化**する必要。

サイバー対処能力強化法

第２節　制度の基本的な考え方

法に基づく各般の施策を実施することにより、以下①～③の機能を**抜本的に強化**

① 情報の収集

通信情報の利用

（ア）当事者協定
（イ）同意によらず通信情報を利用する措置（外外通信目的送信措置等）

官民連携の強化

（ウ）特定重要電子計算機の届出義務
（エ）特定侵害事象等の報告義務
（オ）協議会の枠組

② 情報の整理・分析

- (ア)～(オ)の制度に基づき収集した情報
- その他の手法により取得した情報

↓ 整理・分析（情報のデータベース化、照合等）

次の情報をそれぞれ作成：

- 総合整理分析情報
- 提供用総合整理分析情報
- 周知等用総合整理分析情報

③ 情報の提供

作成した総合整理分析情報等を被害防止等に役立てるため、次の者に適切に提供

- 行政機関等
- 外国の政府等
- 協議会の構成員
- 特別社会基盤事業者
- 電子計算機を使用する者
- 電子計算機等供給者

法に基づく上記の各施策について、以下を**施策の駆動力の両輪**として制度運用を図る。

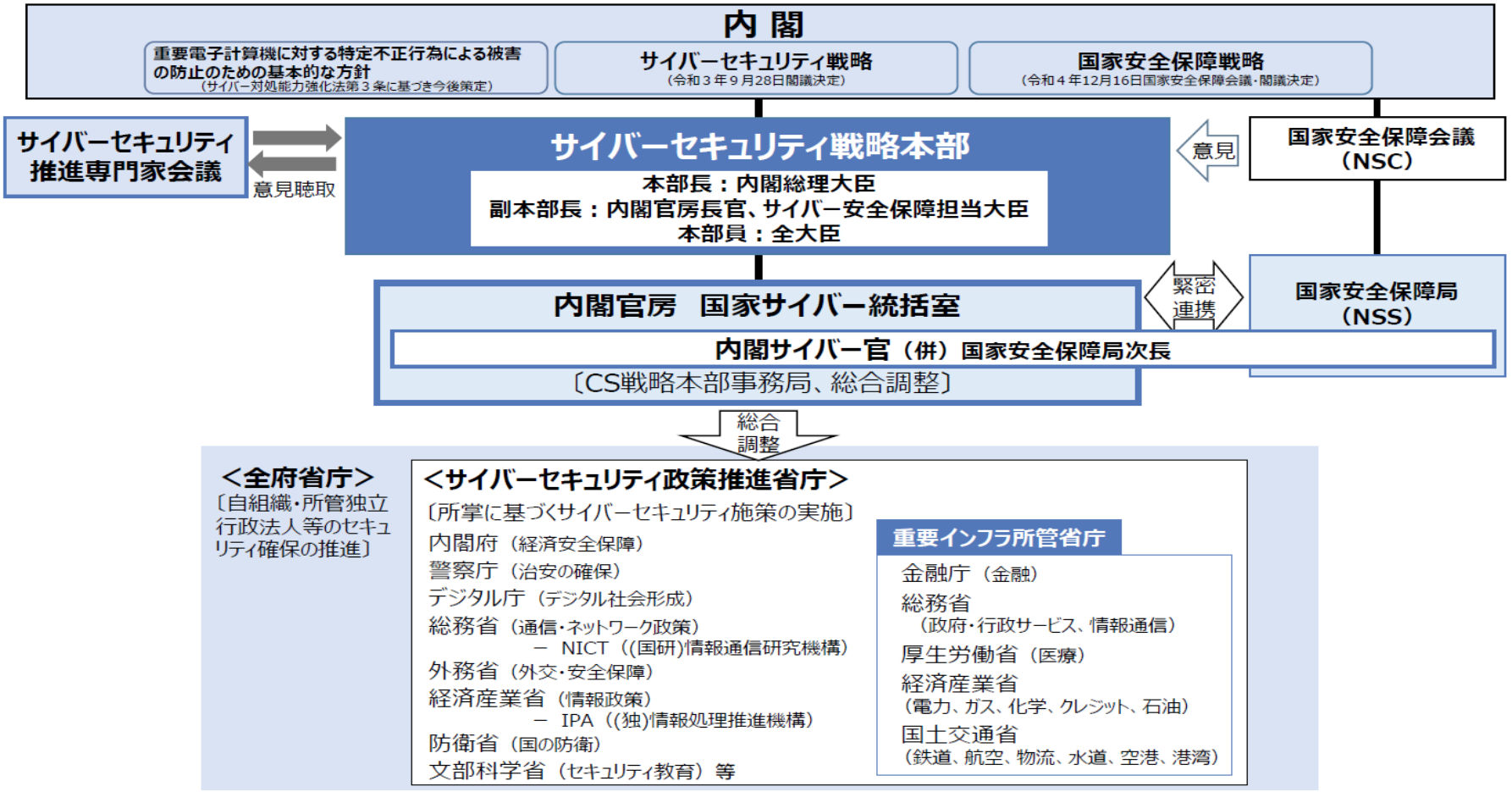
(1) 当該**施策が適切に機能**することにより法目的を効果的かつ効率的に達成
(2) 当該**施策に係る事務を適正に実施**

⇒ **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

【出典】 国家サイバー統括室HP　サイバー対処能力強化法の施行等に関する有識者会議　第4回会合資料より

サイバー対処能力強化法及び同整備法を踏まえた体制強化等

- 新たに内閣総理大臣をトップとし全閣僚をメンバーとするサイバーセキュリティ戦略本部の強化
- 新たなサイバーセキュリティ戦略の策定



【出典】 内閣官房国家サイバー統括室HP　サイバーセキュリティ戦略本部　第1回会合資料　より

新たな「サイバーセキュリティ戦略」（案）の全体像

国土交通省

○ **「国家安全保障戦略」**及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に、**取るべき諸施策の目標や実施方針を内外に示す。

基本的な考え方

○ サイバー空間は、経済社会の持続的な発展、自由主義、民主主義、文化発展を支える基盤。

○ 法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「５つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

（※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」）

情勢認識

- 厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大
- 社会全体のデジタル化の進展とサイバー脅威の増大
- AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

施策の方向性

1 深刻化するサイバー脅威に対する防御・抑止

- 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来からの施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要インフラ事業者・地方公共団体等の対策強化

サプライチェーン全体のレジリエンス確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

サイバー犯罪対策

3 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

・産学官を通じたサイバー人材の確保・育成
・国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術(AI、量子技術等)への対応・取組

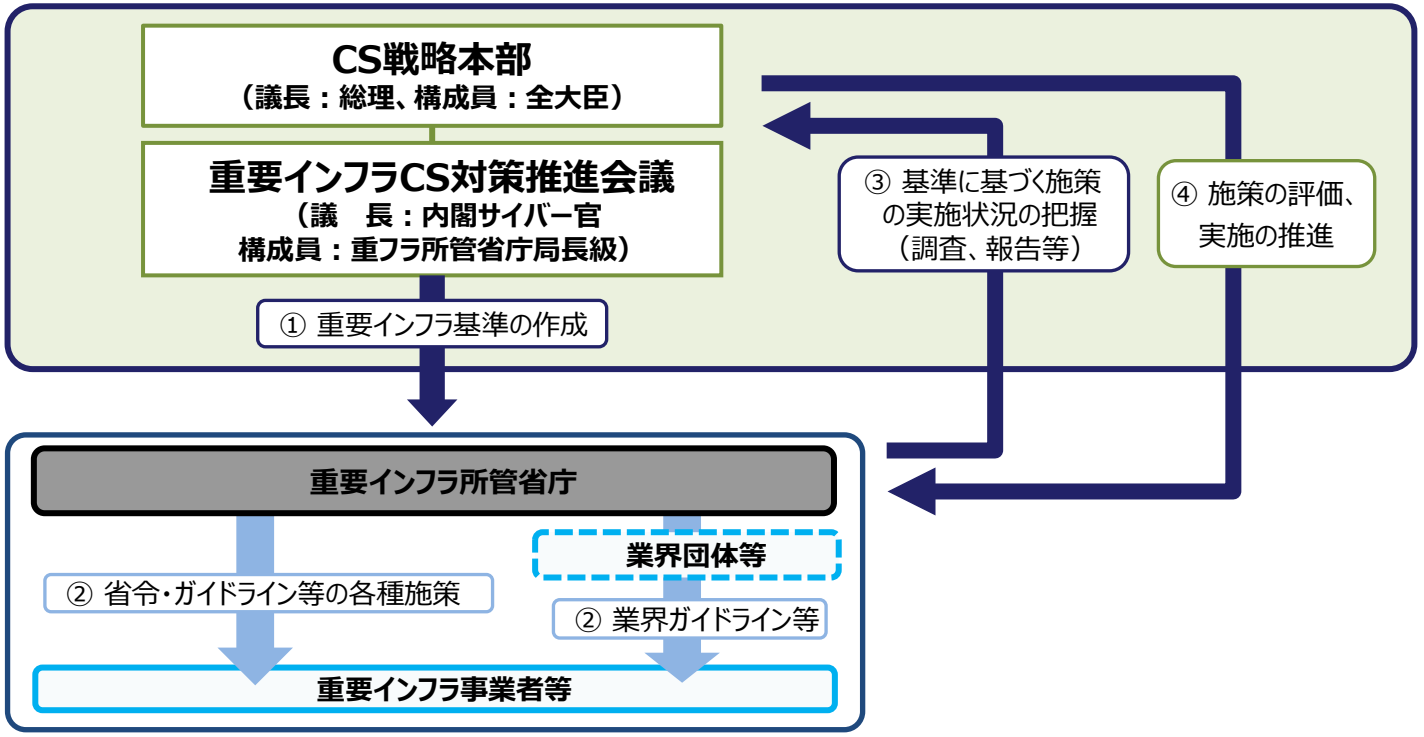
官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進
これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す。

【出典】 国家サイバー統括室HP サイバーセキュリティ推進専門家会議 第２回会合資料 より

重要インフラ統一基準の策定

国土交通省

- 改正サイバーセキュリティ基本法第26条第１項第３号の規定に基づき、CS戦略本部は、重要インフラのサイバーセキュリティ対策強化を図るため、重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成（来年度中）や、当該基準に基づく施策の評価を行う。



サイバーセキュリティ基本法
第二十六条　本部は、次に掲げる事務をつかさどる。
三　重要社会基盤事業者等におけるサイバーセキュリティの確保に関して**国の行政機関が実施する施策の基準の作成（当該基準の作成のための重要社会基盤事業者等におけるサイバーセキュ リティの確保の状況の調査を含む。）**及び**当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進**に関すること。
六　前各号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

【出典】内閣官房国家サイバー統括室HP　重要インフラサイバーセキュリティ対策推進会議　第２回会合資料　より

訓練、演習の実施（全分野一斉演習の例）

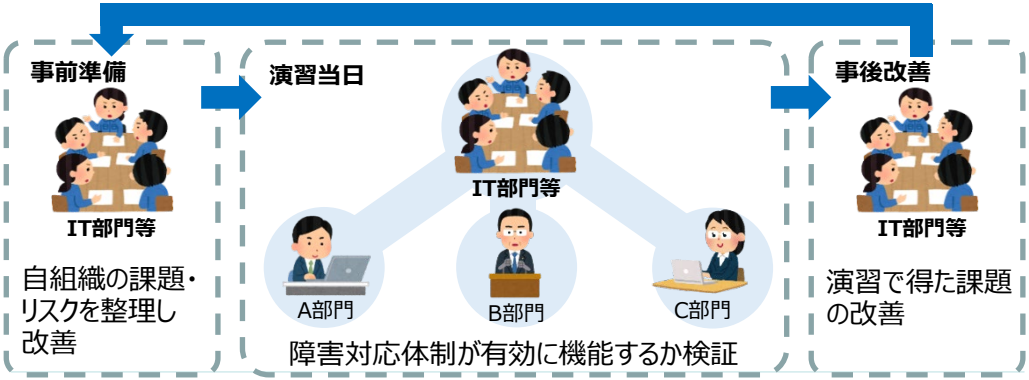
国土交通省

①演習の目的

全分野一斉演習は、「重要インフラのサイバーセキュリティに係る行動計画（以下、重要インフラ行動計画という）」の主要5施策のうち「防護基盤の強化」の「障害対応体制の有効性検証」に位置付けられ、以下の目的として実施するものである。

・関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげていくこと
・重要インフラ行動計画の他施策に資すること

障害対応体制の有効性検証



②演習の日時、形態、参加者

- 日時：2025年11月12日（水）　13:00～17:00
- 形態：机上演習（集合会場及びオンライン（自職場、自宅等））
- 参加者：内閣官房国家サイバー統括室（NCO）、重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）、重要インフラ事業者等（15分野）、セプター（15分野21セプター）、サイバーセキュリティ関係機関

【出典】 内閣官房国家サイバー統括室HP　重要インフラ専門調査会　第34回会合資料を基に国土交通省で作成
【障害対応体制の有効性検証図　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」 行動計画の取組⑤：防護基盤の強化　より

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①

国土交通省

複雑化・巧妙化するサイバー攻撃に対し、国交省、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。

① 国土交通省における対策

- 関係規定等の整備　：国土交通省情報セキュリティポリシー等の関係規定を整備
- システム管理・脆弱性対応等　：専門家による個々のシステムの脆弱性解消支援、情報システム台帳を活用した省内システムの一元的管理（予定）、リスク情報の収集・分析等
- 監査等の実施　：省内の情報システム及びその管理運用に対する監査（内閣官房国家サイバー統括室（NCO）によるものを含む。）等
- インシデント対応　：対応チーム（CSIRT注1）による初動対応、影響調査、原因究明、再発防止対策支援
- 人材育成・教育訓練　：計画に基づく人材確保・育成、役割別（CSIRT、幹部、担当者）研修、標的型メール訓練、自己点検の実施等

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。
○内閣官房 国家サイバー統括室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。
○ 各法人が策定する情報セキュリティ対策推進計画の助言及び把握。

（注1）Computer Security Incidents Response Team：情報セキュリティに係るインシデントに対処するための体制のこと。当省においてはサイバーセキュリティ対策室に設置。

国土交通省におけるサイバーセキュリティ対策②（事業者関係）

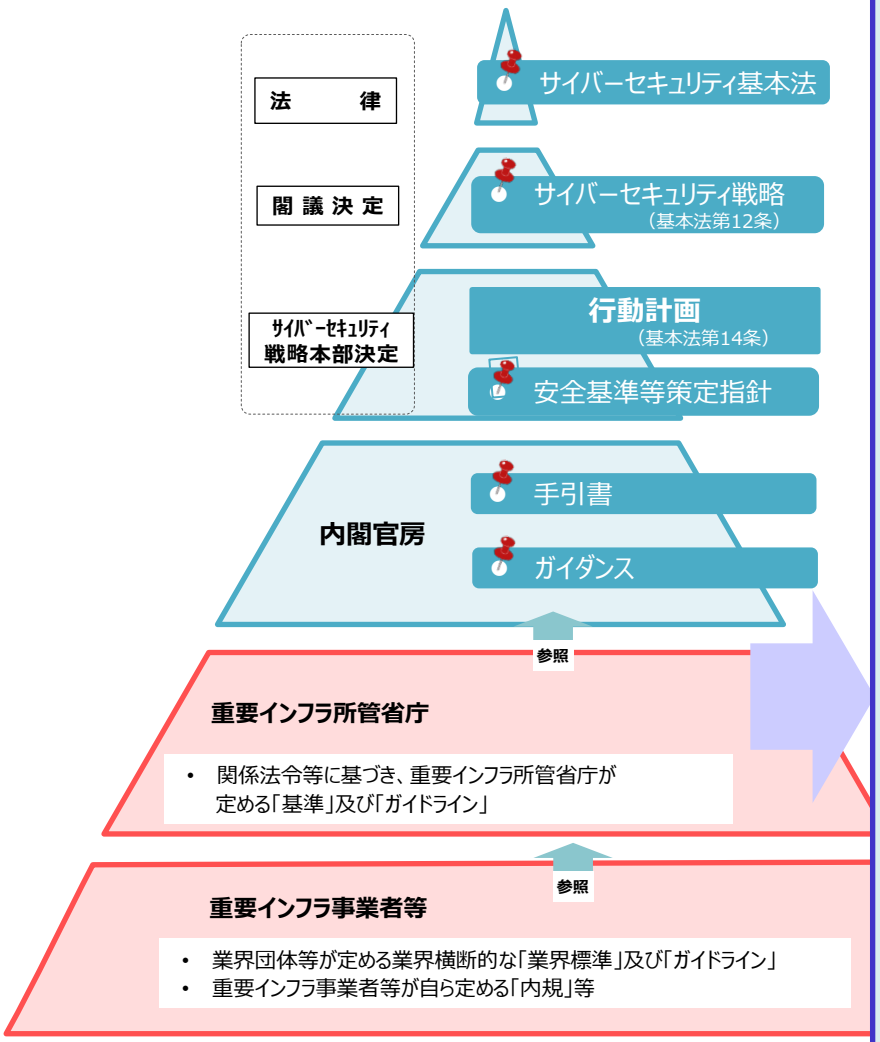
- 国土交通省では、**重要インフラ15分野のうち6分野、約1,400事業者を所管**
- **官民が一体**となって**重要インフラのサイバーセキュリティの確保に向けた取組**を推進

重要インフラ所管省庁

国土交通省	金融庁	厚生労働省	総務省	経済産業省
				
［航空、空港、鉄道、水道、物流、 港湾］	［金融］	［医療］	［情報通信、行政］	［電力、ガス、化学、クレジット、石油］

国土交通省の取組［①情報セキュリティ確保に係るガイドライン］

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**
- 中小を含む事業者向けに**「情報セキュリティ対策チェックリスト」**を作成

【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」
行動計画②：安全基準等の整備及び浸透を基に国土交通省で作成

【出典】国土交通省HP　情報セキュリティ関連

（参考）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

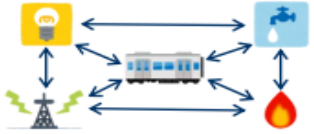
安全基準等の整備及び浸透

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

国土交通省の取組［②事業法体系におけるサイバーセキュリティの明確化］

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 ・**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。）** ・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 （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 （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** ・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	・重要インフラ事業者等に対する**サイバーセキュリティの確保**を規定（予定）
		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。

国土交通省の取組［③ASM］

- オープンソース情報を収集・分析することで、所管重要インフラ事業者※1を対象としたASM※2を実施
- さらに得られた情報から個別事業者の評価レポートを作成

※1 航空、空港、鉄道、水道、物流、港湾分野
※2 Attack Surface Management

国土交通省 サイバーセキュリティ対策室

- リスクレーティング実施
- 優先的に支援が必要となる事業者を選定
- 推奨される対策措置の検討
- 分野ごとの傾向を分析

・レーティング結果展開
・緊急性の高いものは速やかな対策を促す

国土交通省 分野所管部局

省内6部局

- 所管分野の傾向を把握
- 安全ガイドライン等の改善に活用

所管重要インフラ事業者等

6分野 約1,400事業

- セキュリティ上の弱点を把握し、事前対策の実施やレジリエンス改善を図る
- レーティング結果を経営層への説明に活用

国土交通省の取組［④SNSモニタリング］

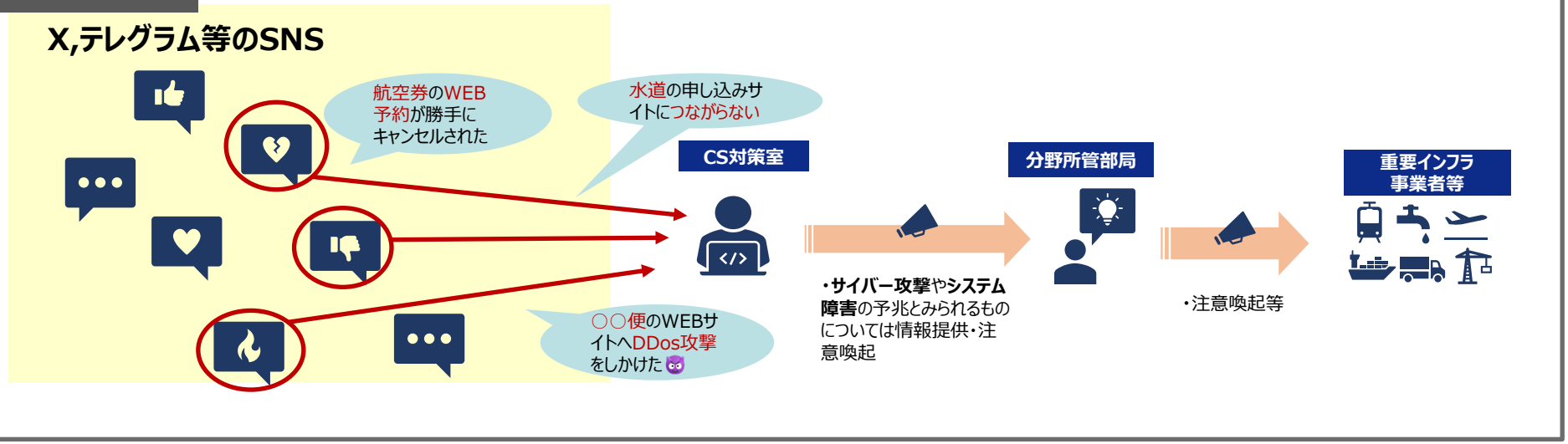
国土交通省

- SNSモニタリングによりインシデント予兆をいち早くキャッチ
- プロアクティブな対策を支援

◘ 国土交通省においてSNSを常時モニタリングし、インシデントの予兆と考えられる情報を速やかに提供する**SNSモニタリング及び情報提供サービス**を実施

◘ 本サービスは、所管重要インフラ事業者等に関係するSNSユーザの投稿を収集し、**システム障害**や**サイバー攻撃**の予兆と推定されるものをピックアップし、国土交通省内関係者及び該当する事業者へ**共有・注意喚起**を図ることにより、サイバーセキュリティインシデントへの事前対処を促すもの

イメージ



国土交通省の取組［⑤駆けつけ支援］

国土交通省

➢**重要インフラ事業者にサイバーセキュリティに関する重大な事象が発生等した場合、専門的知見を有する職員等を現地に派遣**

□「国家安全保障戦略（2022年12月16日閣議決定）」において、我が国が優先する戦略的アプローチの一つとしてサイバー安全保障分野での対応能力向上が求められている。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の導入や、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、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**するなどの取組が求められている

□重要インフラ事業者にサイバーセキュリティに関する重大な事象が発生等した場合、**専門的知見を有する職員等を現地に派遣**し、「インシデントアドバイザー」の観点から、重要インフラ事業者が実施する事案の内容の把握・分析、被害拡大防止の措置、早期の原因究明、対応方針や再発防止策の対処の支援を実施

国土交通省の取組［⑥交通ISACとの連携］

国土交通省

（一社）交通ISACと連携・協力し、サイバー攻撃等に関する情報共有網の拡充・人材育成を支援

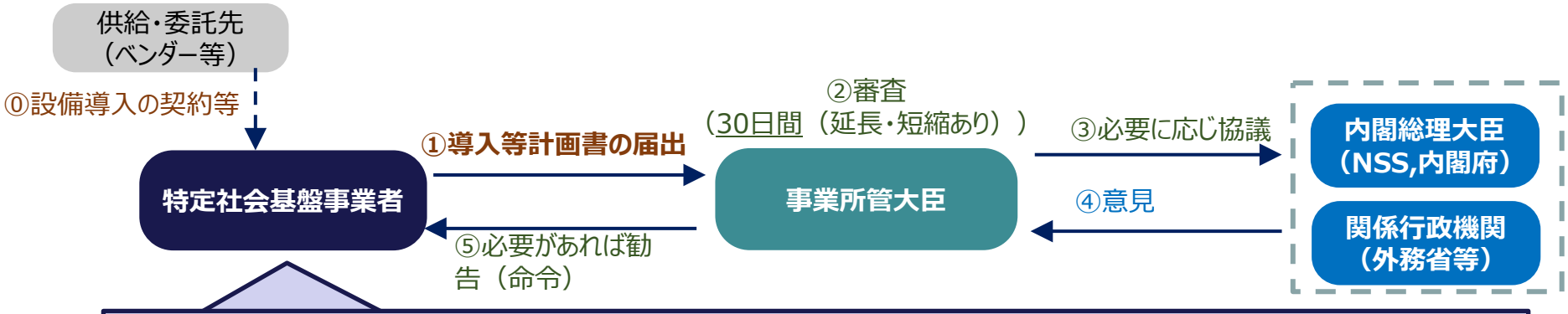
組織概要		
	設立日	2020年４月１日
	会員企業	鉄道、航空、空港、物流分野の大手事業者　９７団体 【2025年10月21日現在】 （うち、正会員70団体、賛助会員16団体、オブザーバー会員11団体）
	設立目的	サイバー攻撃等に対する交通・運輸分野全体の集団防御力の向上に資する活動を推進することで、我が国における交通・運輸サービス全体の安全・安心の向上に寄与する。
	活動内容	・参画事業者間で共通の課題に対し、協同で解決策を検討 ・インシデント等の情報を参画事業者間で展開し、対策を共有 ※国もオブザーバーとして、攻撃者に関する情報や最新のセキュリティ動向等を共有

国土交通省の取組［⑦経済安保法に基づく事前審査］

国土交通省

- 基幹インフラサービスの安定的な提供の妨害を防止するため、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、重要な設備の導入・維持管理等の委託をする際には、**事前に国に届出を行い、審査を受ける制度**を導入。本年４月には港湾分野を追加指定。
- 国土交通省において、港湾等７分野の業者を担当。

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。

【出典】 内閣官房　基幹インフラ役務の安定的な提供の確保に関する制度の概要資料について（詳細版）を基に国土交通省で作成

（参考）経済安全保障推進法基幹インフラ制度　港湾運送分野追加

○ **令和５年７月の名古屋港のサイバー攻撃事案の発生**を受け、港湾運送役務の安定的な提供の確保を図るため、特定社会基盤事業として**一般港湾運送事業を追加する法改正**を令和６年に行い、**令和７年４月１日に施行。**

○ 国土交通省において、**令和７年５月１日**に特定社会基盤事業者として**32者を指定。**６月間の経過措置期間を経て、**令和７年11月２日より届出義務の適用開始。**

対象分野（法律）／特定社会基盤事業の指定（政令）	特定社会基盤事業者の指定基準（省令）	特定重要設備（省令）
一般港湾運送事業	**年間コンテナ取扱量が80万個（TEU※）以上の港湾**のコンテナターミナルでコンテナ荷役を行う者 ※TEU：20フィートのコンテナに換算したコンテナ取扱量 •コンテナ取扱量の多い5港湾を対象に設定 ※京浜港（東京港、川崎港、横浜港） 名古屋港、大阪港、神戸港、博多港 •日本全体のコンテナ取扱量の約3/4をカバー	**ターミナルオペレーションシステム（TOS）** ※対象となる港湾において使用するものに限る。 ターミナルオペレーションシステムとは、コンテナターミナルにおいて、以下を総合的に行う情報処理システム ①船舶へのコンテナの積込に関する計画の作成 ②コンテナの配置計画の作成 ③コンテナの配置の状況の管理

【出典】 内閣官房HP　経済安全保障法制に関する有識者会議　第12回資料　より

ご静聴ありがとうございました