重要インフラのサイバーセキュリティ対策に係る国土交通省の取り組みについて

令和４年9月26日

国土交通省　サイバーセキュリティ・情報化審議官
髙杉 典弘

「情報セキュリティ」から「サイバーセキュリティ」へ

国土交通省

2000年代当初

- e-Japan戦略(2001.1)
  - IT基本法の成立
  - 「情報通信技術 (IT)を積極的に活用、世界最先端のIT国家となることを目指す」
- 重要インフラの情報セキュリティ対策に係る行動計画(2005.12)
  - 重要インフラの各事業において発生する障害のうち、ITの機能不全が引き起こすものから重要インフラを防護
  - 官民の緊密な連携の下、重要インフラの情報セキュリティ対策を強化

ITの普及
サイバー攻撃の高度化・巧妙化　等

2020年代

- サイバーセキュリティ戦略(2021.9)
  - 業務、製品・サービス等のデジタル化が進む中、**サイバーセキュリティは企業価値に直結する営為**に
  - デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組をあらゆる面で同時に推進
- 重要インフラのサイバーセキュリティに係る行動計画(2022.6)
  - 組織統治の一部としてサイバーセキュリティを組み入れ、**組織全体で対応**

重要インフラ防護に関する法体系

国土交通省

● サイバーセキュリティ基本法

（平成26年法律第104号）
最終改正：令和元年法律第11号

✓ 我が国のサイバーセキュリティ政策に関し、基本理念、**国、事業者等の責務を定める**もの。

● サイバーセキュリティ戦略

（令和３年９月28日閣議決定）

✓ サイバーセキュリティ基本法に基づき策定される**サイバーセキュリティに関する基本的な計画**。
✓ **諸施策の目標及び実施方針を国内外に示す**もの。３年ごとに改定。

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）

✓ **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**。
✓ **国、重要インフラ事業者等が取り組むべき事項を規定**。

行動計画の基本的な考え方

◆ 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、**経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。**特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。

◆ 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。

◆ 重要インフラを取り巻く脅威の変化に適確に対応するため、**サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。**

重要インフラ(全14分野)

- 情報通信
- 金融
- **航空**
- **空港**
- **鉄道**
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- **物流**
- 化学
- クレジット
- 石油

※赤字は国土交通省所管分野

重要インフラ事業者に求められる取り組み

自助

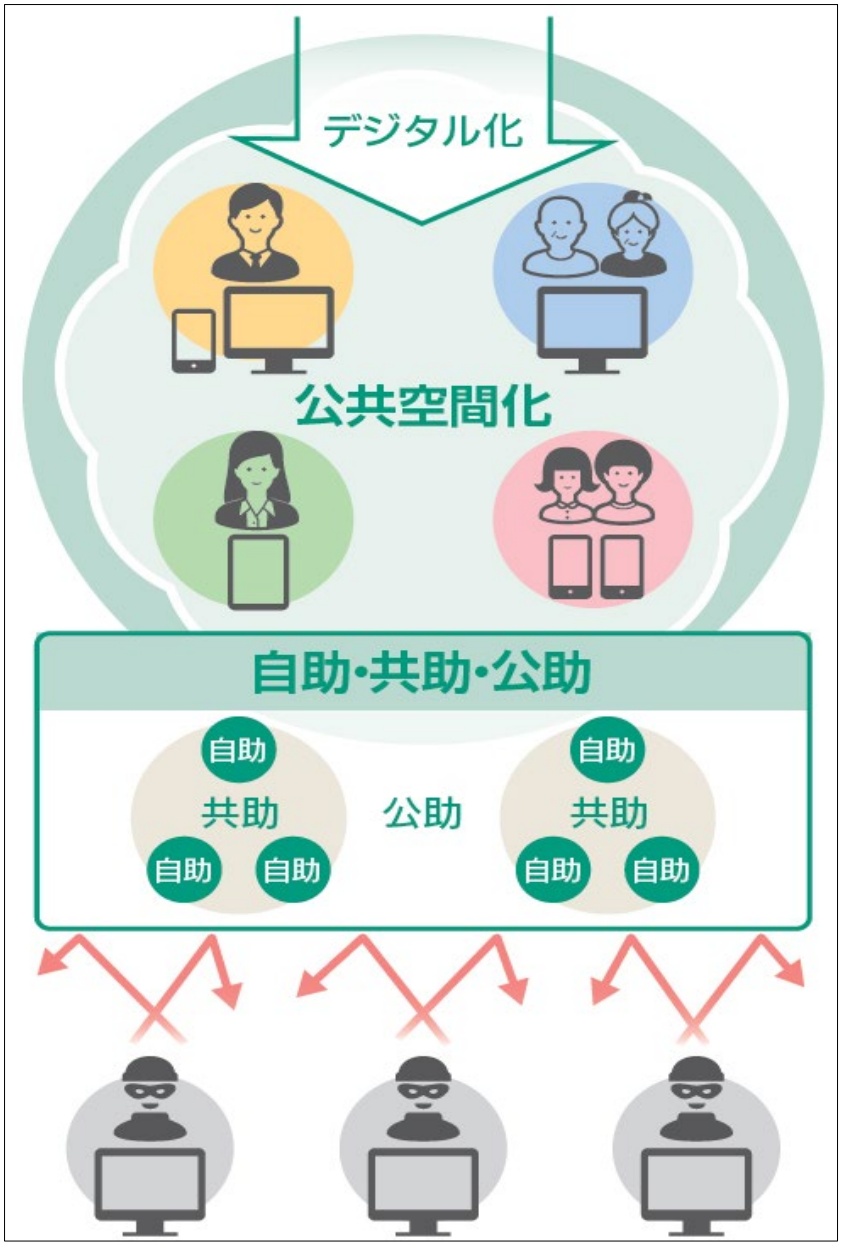
重要インフラサービスを安定的かつ適切に提供するため、自主的かつ積極的なサイバーセキュリティの確保を実施

共助

サイバーセキュリティに関する情報共有・分析・対策を企業・分野を超えて連携

公助

基準の策定、演習及び訓練、情報共有等を通じた支援を継続して実施



ISACとその必要性

国土交通省

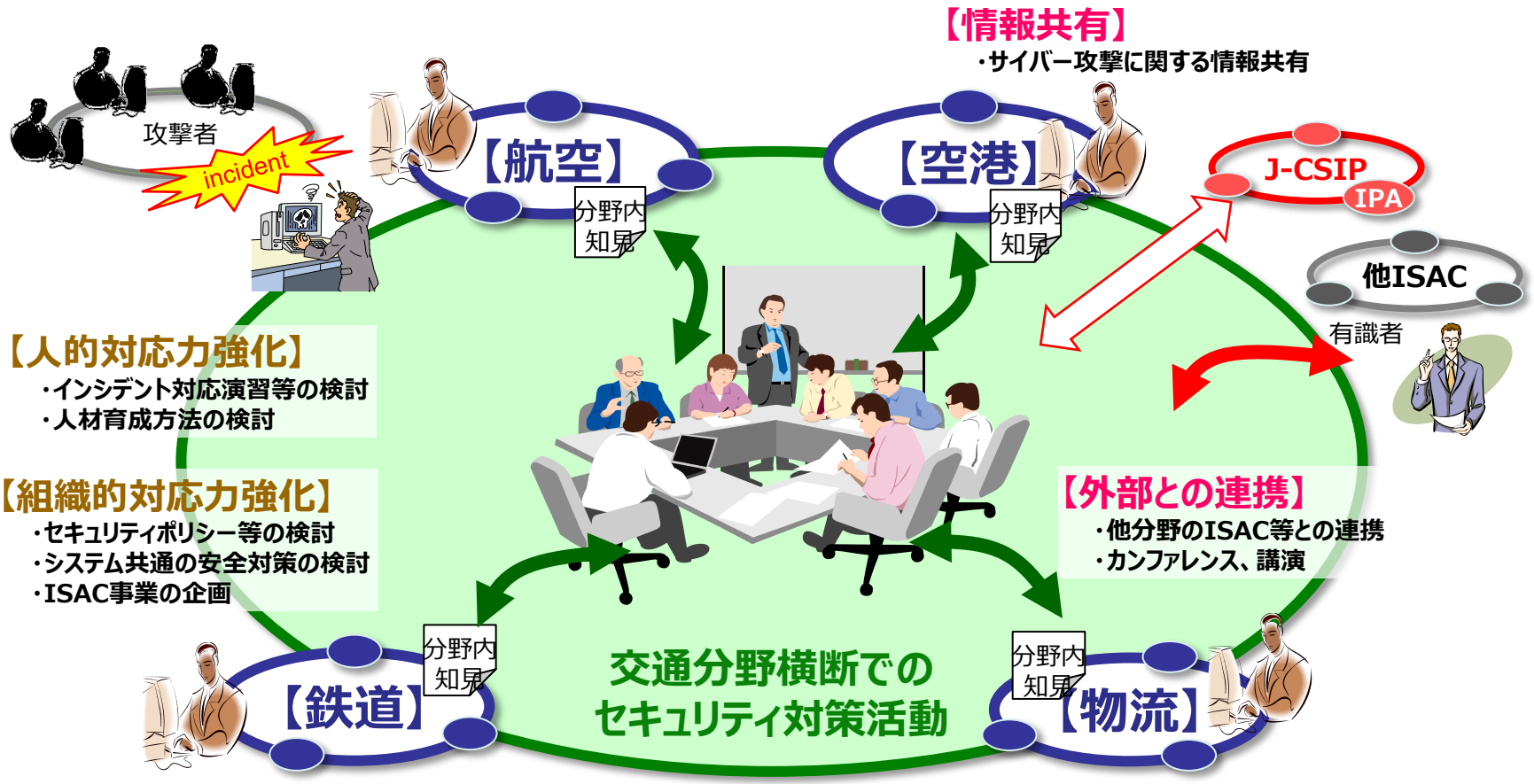
- ＩＳＡＣ（Information Sharing and Analysis Center）：業界内での情報共有・連携の取り組み推進を図る組織
- 人の流れ、物の流れにおいて、各分野で類似のシステムも存在することから、共通の敵となる「サイバー攻撃者」に対して、**分野横断での情報を共有・分析し、共助していく組織として「交通ISAC」が効果的。**

日本国内の主なISAC組織

一般社団法人　交通ISACの活動

国土交通省

- ◆ 一般社団法人交通ISAC　（英文表示：Transportation ISAC JAPAN）
- ◆ 令和２年４月１日設立
- ◆ 現在の会員数　88団体(R4.7.1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

1. 各社における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**
2. 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**
3. 国からの**情報提供**
4. インシデント発生時における国や各社等との**情報共有**（トラフィックの変化など被害状況や対応策が相談できる）
5. その他、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
   例：保険会社からサイバー保険に関する説明

特に、昨今のサイバーセキュリティを取り巻く情勢から上記活動は極めて有意義

【参考】９月７日(水)

- 東京メトロや大阪メトロのホームページが一時的に閲覧しづらい状況が発生。
- 鉄道の運行に支障は生じず、７日中にホームページの閲覧が可能な状態に復旧。

経営層がとるべきサイバーセキュリティ対策　10か条

国土交通省

【出典】一般財団法人　運輸総合研究所HPより

1　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

サイバーセキュリティリスクの重要性について取締役会等の経営会議において協議・分析し、その結果に基づき、経営層が共通した認識の下で意思決定を行う。

2　サイバーセキュリティリスクに関する検討組織を設置する。

経営層が情報を分析して施策に反映させるために専門の検討機能を組織し、自社におけるサイバーセキュリティリスクの評価を行う。評価結果を経営会議におけるインプット資料として活用して経営方針を立案し、予算確保等、対策推進のための社内資産を確保する。

3　危機管理を統括する既存部門とCSIRTの連携を強化する。

経営リスクとサイバーセキュリティリスクを統括管理するために組織連携を強化する。サイバー攻撃が発生した際のシナリオを事業継続計画に含め、その発動の際には、危機管理を統括する既存部門と CSIRT が連携するよう組織を整備する。

4　PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。

情報セキュリティの改善活動を統括する立場として、橋渡し人材を主体とする PDCA サイクルを実施する組織を発足し、経営層として直接進捗を確認する。最新動向、世間のインシデント状況、自社の対応状況等を踏まえて、重視するサイバーセキュリティリスクへの対応状況について定期的に報告を受ける。報告をもとに、経営層が重視するサイバーセキュリティリスクへの対応状況を確認する。

5　経営層として情報共有に努める。

経営層が関与することの組織的な効果を踏まえ、サイバーセキュリティリスクに関わる情報共有に努める。

6　危機管理コミュニケーション力を高める。

危機が発生した際に適切な情報開示ができるよう、危機管理コミュニケーション力を高める。経営層自身が適切な有事対応できるよう、平時より能力を高める。

7　有事に備えた現場担当者教育を強化する。

サイバー攻撃等の有事に備えて、日頃から現場担当者・管理者の教育を行い、体制を強化する。攻撃を最初に検知するのは現場担当者であり、これを踏まえた教育を行う。

8　監査機能を積極活用する。

経営層が重視するサイバーセキュリティリスクに対応した対策を確実に実施するために、システム監査やセキュリティ監査等の監査機能を積極的に活用する。監査を忌避する風潮を打破し、ガバナンス強化の仕組みとしての活用を図る。

9　サイバーセキュリティリスクへの取組について積極的な情報開示に努める。

株主や投資家等を含め、多様な利害関係者に向け、サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

10　自社のセキュリティ水準の将来目標を定め、目標達成や進捗状況を管理する。

中長期の事業計画と整合したサイバーセキュリティ対策を計画し、実行する。自社が目標とする中長期のセキュリティ水準を定め、目標達成や進捗状況を内部監査の実施を通じて確認する。

参考：「サイバーセキュリティお助け隊サービス」制度

国土交通省

制度概要

➢ **中小企業**に対するサイバー攻撃への対処に不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすことが確認されたサービスを独立行政法人情報処理推進機構(IPA)が登録・公表

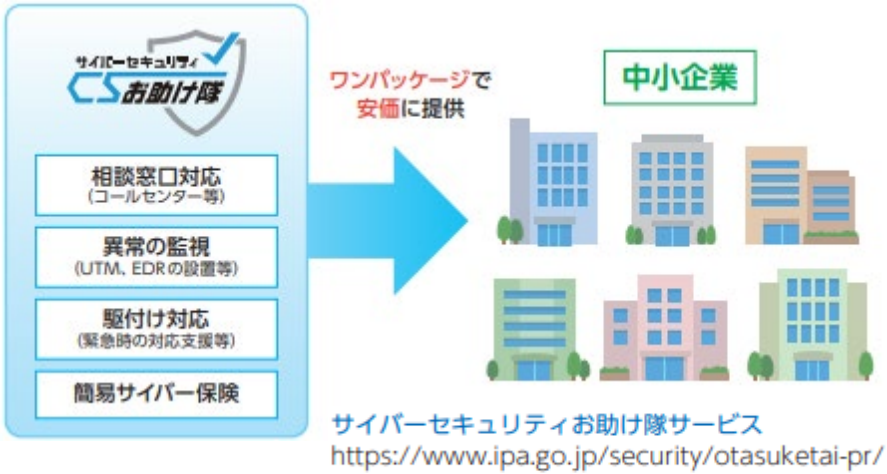
サービスのイメージ

「見守り」「駆け付け」「保険」など中小企業のセキュリティ対策に
不可欠なサービスをワンパッケージで安価に提供

見守り
（異常の監視）
24時間265日監視
挙動や問題のある攻撃を検知し
あなたのPCとネットワークを守ります。

駆け付け
問題が発生したときに、
地域のIT事業者等が
駆け付け対応します。
（リモート支援の場合あり）

保　険
簡易サイバー保険で、
駆け付け支援等インシデント
対応時に突発的に発生する
各種コストが補償されます。



サイバーセキュリティお助け隊サービス
https://www.ipa.go.jp/security/otasuketai-pr/

登録サービスリスト(2022年4月時点)

	サービス名	事業者名
1	商工会議所サイバーセキュリティお助け隊サービス	大阪商工会議所
2	防検サイバー	ＭＳ＆ＡＤインターリスク総研株式会社
3	PCセキュリティみまもりパック	株式会社ＰＦＵ
4	EDR運用監視サービス「ミハルとマモル」	株式会社ＡＧＥＳＴ
5	SOMPO SHERIFF（標準プラン）	ＳＯＭＰＯリスクマネジメント株式会社
6	ランサムガード	株式会社アイティフォー
7	オフィスSOCおうちSOC	富士ソフト株式会社
8	セキュリティ見守りサービス「＆セキュリティ＋」	株式会社ＢＣＣ
9	CBM ネットワーク監視サービス	中部事務機株式会社
10	中部電力ミライズ サイバー対策支援サービス	中部電力ミライズ株式会社
11	ＣＳＰサイバーガード	セントラル警備保障株式会社
12	PCお助けパック　PC定期侵害調査プラン	沖電グローバルシステムズ株式会社

https://www.ipa.go.jp/security/otasuketai-pr/

【出典】独立行政法人情報処理推進機構HPより

ご清聴いただき
ありがとうございました

【連絡先】
国土交通省総合政策局情報政策課サイバーセキュリティ対策室
電話（直通）：０３－５２５３－８３４１
Ｅ－ｍａｉｌ：hqt-csirt＊gxb.mlit.go.jp
（送信時は＊を@に変換いただくようお願いします）