



# 交通ISAC 活動状況と設立にむけた取り組みについて

2019年11月7日

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長  
大嶋 孝友

ANAシステムズ株式会社  
品質・セキュリティ管理部  
エグゼクティブ・マネージャー  
阿部 恒一

1. 我が国におけるサイバーセキュリティの現状
2. ISACとその必要性
3. 交通ISAC創設に向けて
4. 交通ISACを仮運用した効果
5. 持続可能な交通ISACへ
6. 交通ISAC入会案内

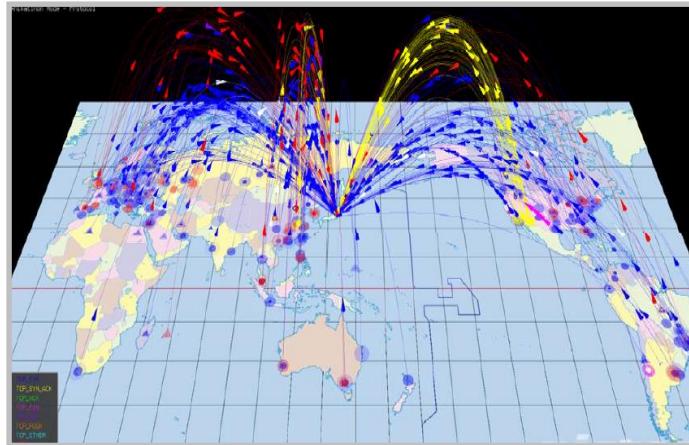
# 1. 我が国におけるサイバーセキュリティの現状

---

# 1. 我が国におけるサイバーセキュリティの現状 (1/5)

- 日本に対するサイバー攻撃は増加の一途を辿っている。NICT(情報通信研究機構)の調査によると、2018年度は約2121億件もの攻撃が行われた可能性がある。

＜攻撃の様子を可視化＞



【出典】[http://www.soumu.go.jp/main\\_content/000467154.pdf](http://www.soumu.go.jp/main_content/000467154.pdf)

＜攻撃の観測イメージ＞



【出典】<http://www.nict.go.jp/cyber/research.html>

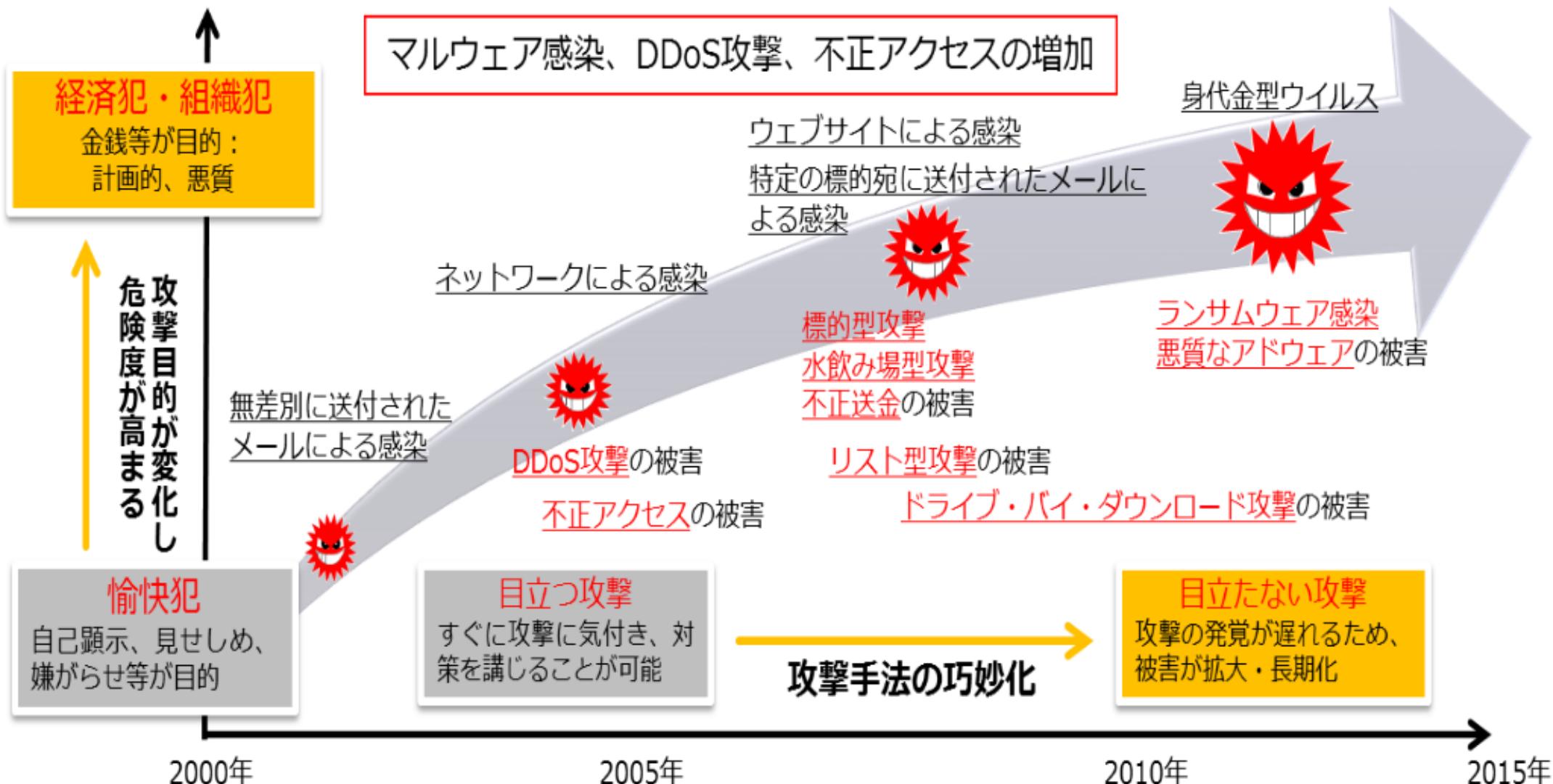
＜観測の実績＞

年	年間総観測パケット数
2005年	約3.1億件
2006年	約8.1億件
2007年	約19.9億件
2008年	約22.9億件
2009年	約35.7億件
2010年	約56.5億件
2011年	約45.4億件
2012年	約77.8億件
2013年	約128.8億件
2014年	約256.6億件
2015年	約545.1億件
2016年	約1281億件
2017年	約1504億件
2018年	約2121億件

【出典】<https://www.nict.go.jp/press/2019/02/06-1.html>

着実な  
増加傾向

# 1. 我が国におけるサイバーセキュリティの現状（2/5）



【出典】サイバーセキュリティ政策の最新動向（総務省）

## 国内事例

- 2015年6月：**日本年金機構**の職員が利用する端末がマルウェアに感染し、年金加入者に関する情報約125万件が流出した。（**標的型攻撃**）
- 2015年10月：**金融庁**の注意喚起を装ったフィッシングサイトを確認、国内銀行のセキュリティを向上させるためと称して、口座番号、パスワード、第二認証などの情報を騙し取られる恐れ。（**フィッシング攻撃**）
- 2015年11月：**東京五輪組織委員会**のホームページにサイバー攻撃、約12時間閲覧不能。（**DDoS攻撃**）
- 2016年6月：**i.JTB(JTBのグループ会社)**の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（**標的型攻撃**）
- 2017年5月：国内（**行政、民間企業、病院等**）において、**WannaCry**による被害が確認。企業内のシステム停止などの障害が発生した。（**ランサムウェア**）

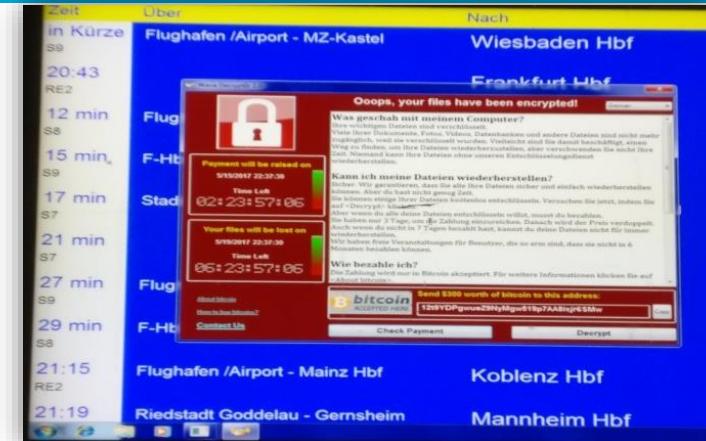
## 海外事例

- 2015年4月：**フランスのテレビネットワークTV5 Monde**がサイバー攻撃を受け、放送が一時中断。（**標的型攻撃**）
- 2015年6月：**米国的人事管理局（OPM）**が不正にアクセスされ、政府職員の個人情報が流出。（**不正アクセス**）
- 2015年12月：**ウクライナの電力会社**のシステムがマルウェアに感染し、停電が発生。（**標的型攻撃**）
- 2016年10月：**米国のDny社**のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生。（**DDoS攻撃**）
- 2017年5月：世界各国（**アメリカ、イギリス、中国、ロシア等**）で**WannaCry**の感染被害が発生。行政、民間企業、医療等の多くの組織に影響を及ぼした。（**ランサムウェア**）

# 1. 我が国におけるサイバーセキュリティの現状（4/5）



<WannaCry感染画面>



<ドイツ空港の電子掲示板がWannaCryに感染した様子>

## ● WannaCry概要

世界150カ国30万台以上（国内約600カ所、2000台以上）のコンピュータに感染。  
感染したコンピュータのデータを暗号化し、使用不能にして、身代金としてビットコインを要求。

## ● 攻撃方法

マイクロソフト製品の脆弱性(MS17-010)を利用して侵入し、データの暗号化を行う。

## ● 被害企業

- Telefonica (スペイン携帯会社) 、Renault (フランス自動車メーカー) 、  
Deutsche (ドイツ鉄道) …等

## ● 対策

- マイクロソフトがリリースしたセキュリティ更新プログラムMS17-010を適用する。
- 重要なデータはバックアップする。

## 物理的破壊(停止)目的 <= 実際の物理的攻撃



### 重要インフラへ物理的破壊、停止、混乱目的のサイバー攻撃

- 制御系装置（遠心分離機）の破壊
- 電力設備への攻撃による大規模停電
- 銀行ATMの停止
- 鉄道会社の切符券売機の停止
- ダムの制御システムへの不正侵入

#### ビジネスの「可用性」を脅かすサイバー攻撃

- サイバー攻撃は、従来、大規模データ漏洩など、情報資産の機密性を脅かすリスクだと考えられてきた。しかし、2017年5月に世界規模で発生したWannaCryというランサムウェアは、工場の操業停止など、事業の継続を困難に陥れた。
- この事例から、サイバー攻撃は、機密性の問題を引き起こす以外に、**可用性を脅かすリスク**でもあると認識されるようになった。**ビジネスに与える影響は、可用性の侵害のほうが深刻な場合もある。**

## 2. ISACとその必要性 ～なぜ交通ISACなのか～

---

### 現状認識と将来像 (サイバー空間と実空間の一体化に伴う脅威の深刻化)

#### 策定の趣旨・背景

【サイバー空間と実空間の一体化、活動空間の拡張】

【(2015年戦略策定時) 連接融合情報社会の到来】

～実空間のヒト・モノがネットワークに連接され、  
実空間とサイバー空間の融合が高度に深化～



### 国民が安全で安心して暮らせる社会の実現

#### 1 国民・社会を守るための取組

- 「積極的サイバー防衛」の構築  
(脅威情報の共有・活用の促進、脆弱性情報の提供等)
- サイバー犯罪への対策

#### 2 官民一体となった 重要インフラの防護

- 重要インフラ行動計画に基づく取組の推進
- 地方公共団体の取組強化

#### 3 政府機関等における セキュリティ強化・充実

- 情報システムの状態のリアルタイム管理の強化  
(新たな統一基準群に基づく取組等)

#### 4 大学等における安全・安心な 教育・研究環境の確保

- 各層別研修及び実践的な訓練・演習の実施

#### 5 2020年東京大会と その後を見据えた取組

- サイバーセキュリティ対処調整センターの構築

#### 6 従来の枠を超えた 情報共有・連携体制の構築

- 多様な主体の情報共有・連携の推進

#### 7 大規模サイバー攻撃事態等への 対処態勢強化

- サイバー空間と実空間の双方の危機管理に挑むため  
の対処態勢の強化

- 「情報共有体制の強化」については、情報セキュリティの動向が刻々と変化する昨今、重要インフラ事業者等が高いセキュリティ水準を保ち続けるには、**単独で取り組む情報セキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組む必要がある。**
- 現在、NISCをはじめとする政府機関や民間において、以下のような情報共有体制が活動している。

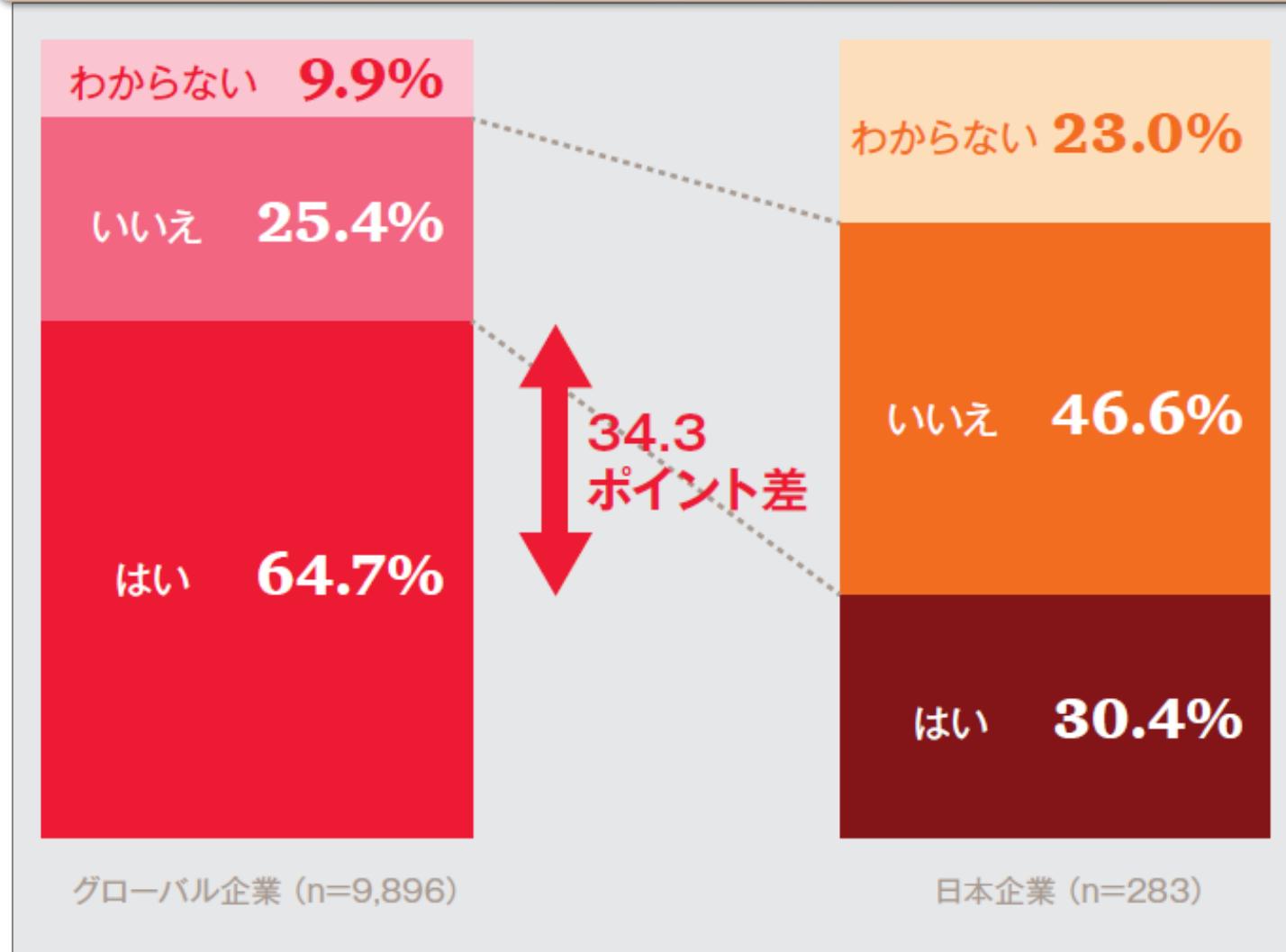
- サイバーセキュリティ協議会
- 早期警戒情報の提供システム「CISTA」（JPCERT/CC）  
※CISTA : Collective Intelligence Station for Trusted Advocates
- 「重要インフラの情報セキュリティ対策に係る第4次行動計画」に基づく情報共有体制（NISC）
- サイバー情報共有イニシアティブ「J-CSIP」（IPA）  
※J-CSIP : Initiative for Cyber Security Information sharing Partnership of Japan
- 日本サイバー犯罪対策センター（JC3）による情報共有
- ICT-ISAC、金融ISAC、電力ISAC等（民間事業者）  
※ISAC : Information Sharing and Analysis Center

- セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。

サイバーセキュリティ経営の重要10項目	
1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
2	サイバーセキュリティリスク管理体制の構築
3	サイバーセキュリティ対策のための資源（予算、人材等）確保
4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
5	サイバーセキュリティリスクに対応するための仕組み構築
6	サイバーセキュリティ対策におけるPDCAサイクルの実施
7	インシデント発生時の緊急対応体制の整備
8	インシデントによる被害に備えた復旧体制の整備
9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

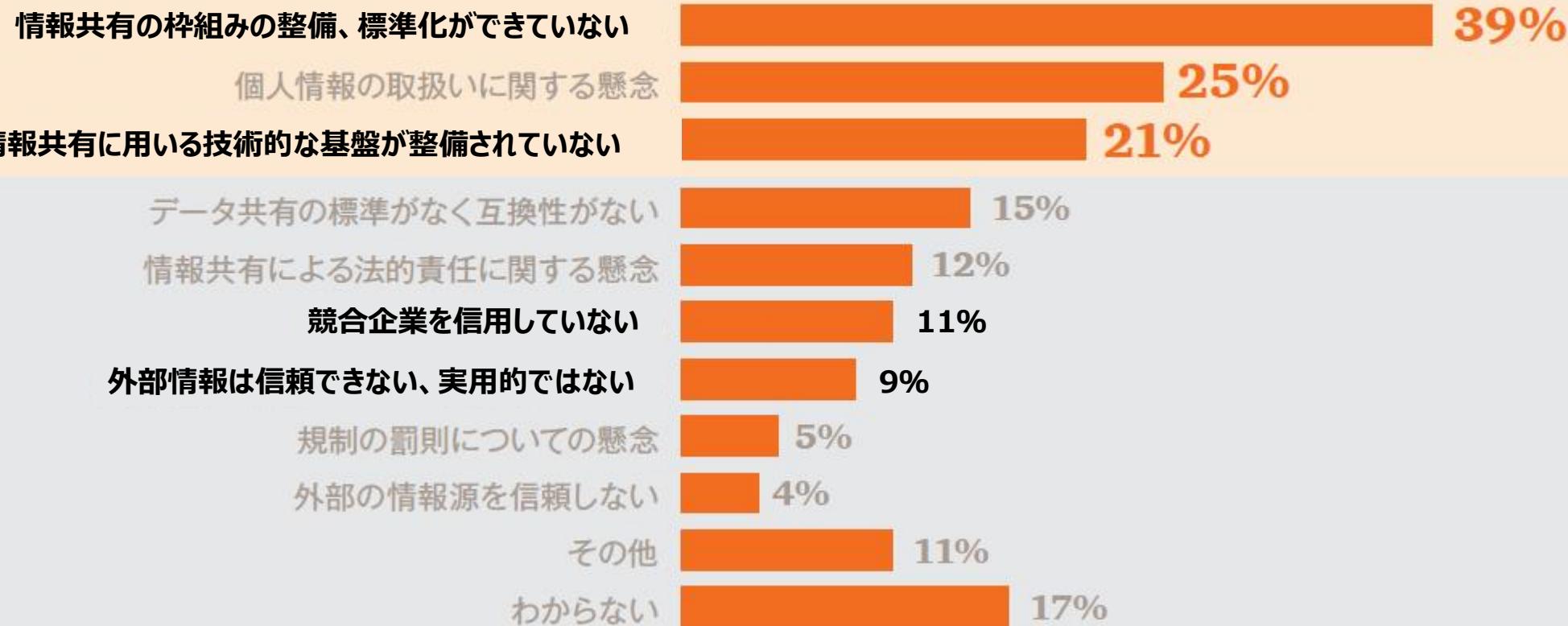
【出典】サイバーセキュリティ経営ガイドライン（情報処理推進機構）

### 他組織とサイバーリスクに関する情報共有を行っているか？



### 他組織と情報共有を行わない理由

(n=132)  
日本企業のみ

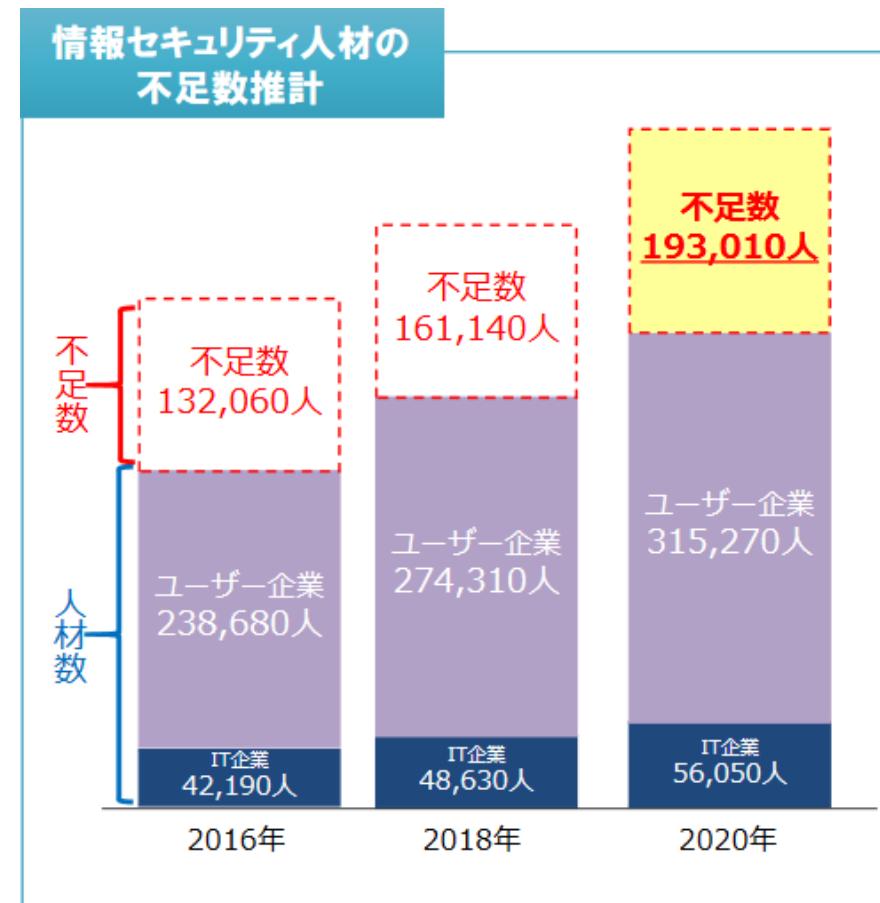


(複数回答、回答率の降順)

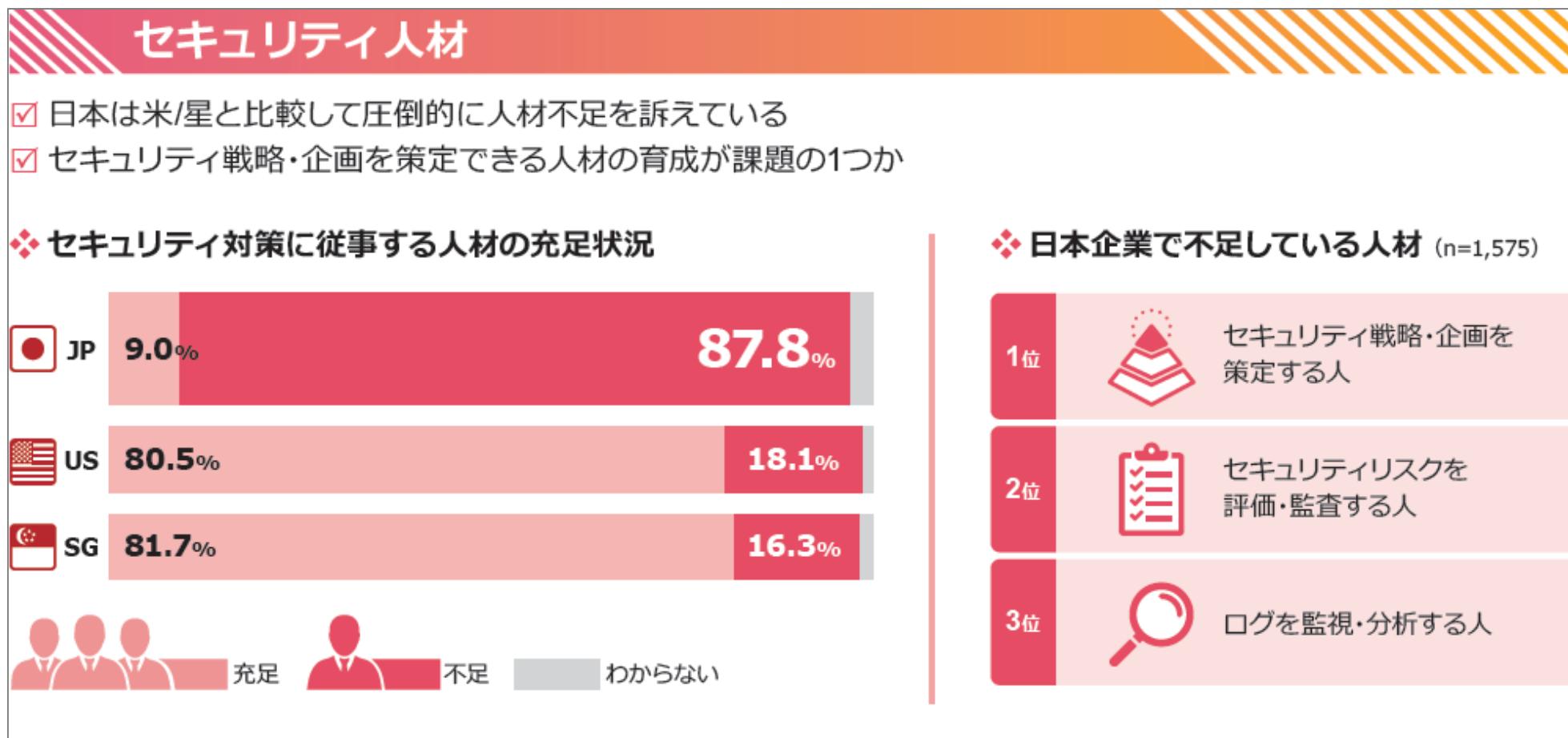
【出典】サイバーセキュリティの転換と変革 (PwC)

## 2. ISACとその必要性 ～なぜ交通ISACなのか？～ (7/13)

- 2016年時点で情報セキュリティ人材が**13.2万人不足**と推計。**2020年には、19.3万人に増加すると見込まれている。**
- 中小企業（従業員数5人～99人、100人～299人）では、2016年時点で最大15.6万人不足と推計。



- サイバー攻撃は日々高度化・巧妙化しており、これに対応して防御策等の戦略も高度化していくことが求められている。
- 一方で情報セキュリティ対策に従事する人材は不足している。



- 日本の多くの企業・組織ではセキュリティ対策はコストと捉えられ、セキュリティ対策の実施について経営層の理解を得られない状況である。

### セキュリティ対策

- 対策実施のきっかけ1位は、日本は自社のセキュリティインシデントであり、米/星は経営層の指示であった
- 担当者として最も対応に困っていることは、日本は対策実施・有事対応が、米/星は情報収集・共有が上位となつた

#### ❖ セキュリティ対策の実施のきっかけや理由

1位 自社のセキュリティインシデント



JP

1位 経営層のトップダウン指示



US SG

#### ❖ セキュリティ担当者として最も対応に困っていること



JP



US



SG

1位

自社セキュリティ対策の遅れ  
(最新技術・動向の未反映)



セキュリティ対策のトレンド・他社動向の把握

2位

セキュリティインシデント発生時の緊急対応

セキュリティ脅威・事故に関する情報収集と関係者共有

3位

サイバー攻撃の高度化への対応

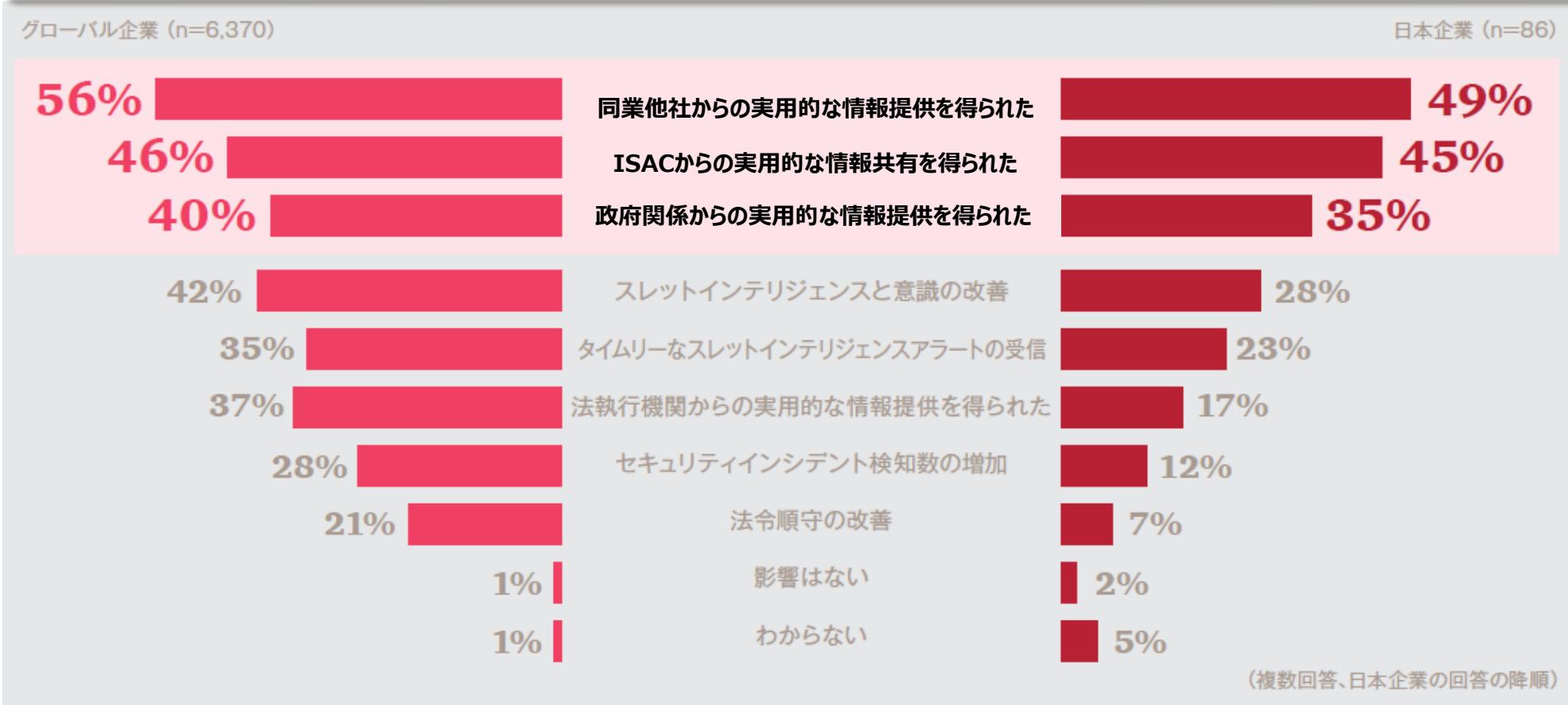
サイバー攻撃の高度化への対応

セキュリティインシデント発生時の緊急対応

## 2. ISACとその必要性 ~なぜ交通ISACなのか?~ (10/13)

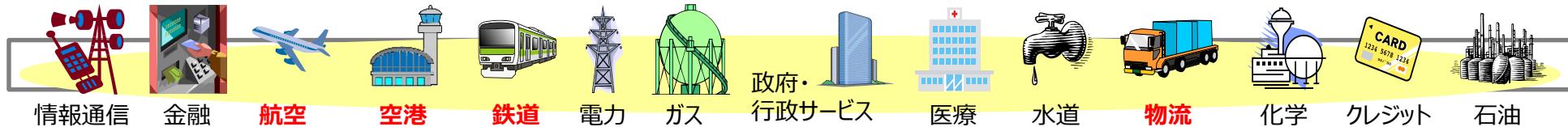
- 他社の事例や取り組みを知ることで、自社取り組みのレベルやポジショニングを確認・把握
- 最新動向や対策を知ることで、業界を取り巻く課題、環境変化等について共通理解を醸成
- 各社の情報・知見を持ち寄ることで、自社課題解決の方法や方向性を協同検討

### 情報共有による自組織へのメリット



## 2. ISACとその必要性 ~なぜ交通ISACなのか?~ (11/13)

### ● 重要インフラの情報セキュリティ対策に係る第4次行動計画 (2018年7月25日サイバーセキュリティ戦略本部改定)



#### 航空

- ・運航システム
- ・予約・搭乗システム
- ・整備システム
- ・貨物システム



#### 鉄道

- ・列車運行管理システム
- ・電力管理システム
- ・座席予約システム



#### 空港

- ・警戒警備・監視システム
- ・フライトインフォメーションシステム
- ・バゲージハンドリングシステム



#### 物流

- ・集配管理システム
- ・貨物追跡システム
- ・倉庫管理システム



## 2. ISACとその必要性 ~なぜ交通ISACなのか?~ (12/13)

- サイバー攻撃による被害が深刻化する中、サイバー空間における**攻撃者優位の状況**も背景に、**サイバー空間と実空間の一体化の進展により被害が拡大する可能性**がある。

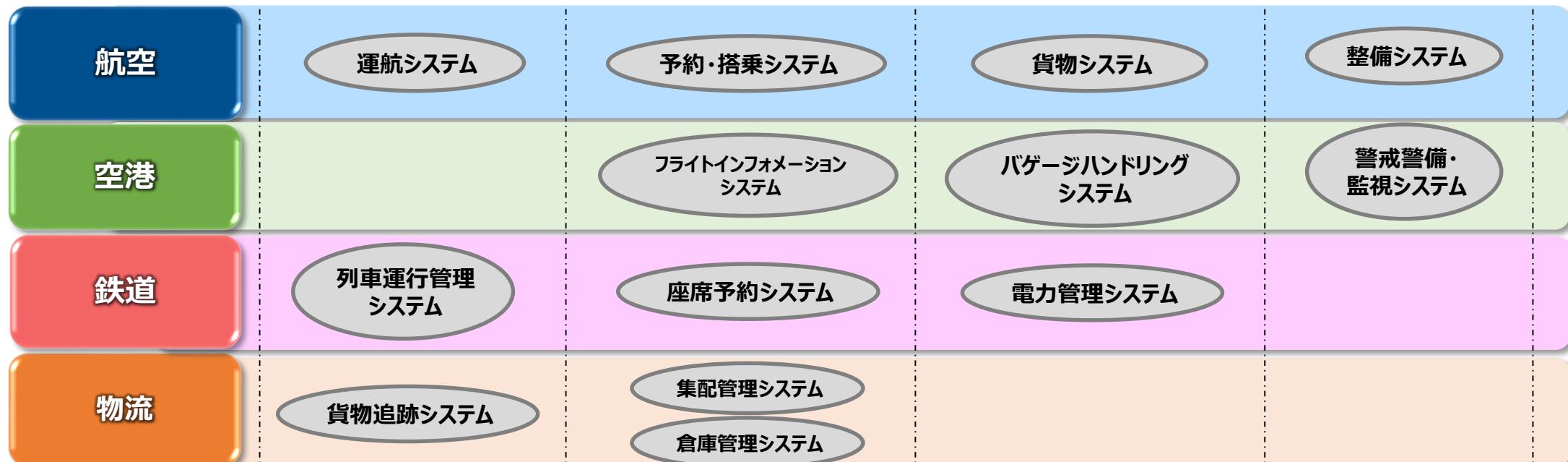
**攻撃者** ~時間・場所の無制約、  
低コストかつ豊富な手段~



**防御側** ~限られた資源、脆弱性の完全除去  
は不可能、攻撃者特定困難~



**集団防御**



## 2. ISACとその必要性 ~なぜ交通ISACなのか?~ (13/13)

運輸・交通事業者における  
サイバーセキュリティ人材不足

サイバー空間と実空間の一体化の進展

国民生活における利便性向上

サイバー攻撃における被害の拡大の懸念

鉄道 運行管理システム 相互乗り入れの増加

空港や変電所 遠隔監視システムの増加

その他 OT系でクローズドシステム



各種システムは分野を問わず  
IT系の汎用技術を用いて  
いるものも多い。

日本の企業は、システムインテグレーターにサイバーセキュリティ業務を外部委託する傾向あり

いつ、誰とサイバーセキュリティ情報  
を共有すべきか判断できる人  
材が事業者側（ユーザー側）で  
不足している

人の流れ、物の流れにおいて、各分野において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」を創設していくことが効果的!!!



### 3. 交通ISAC創設に向けて

---

### 3. 交通ISAC創設に向けて（1/10）

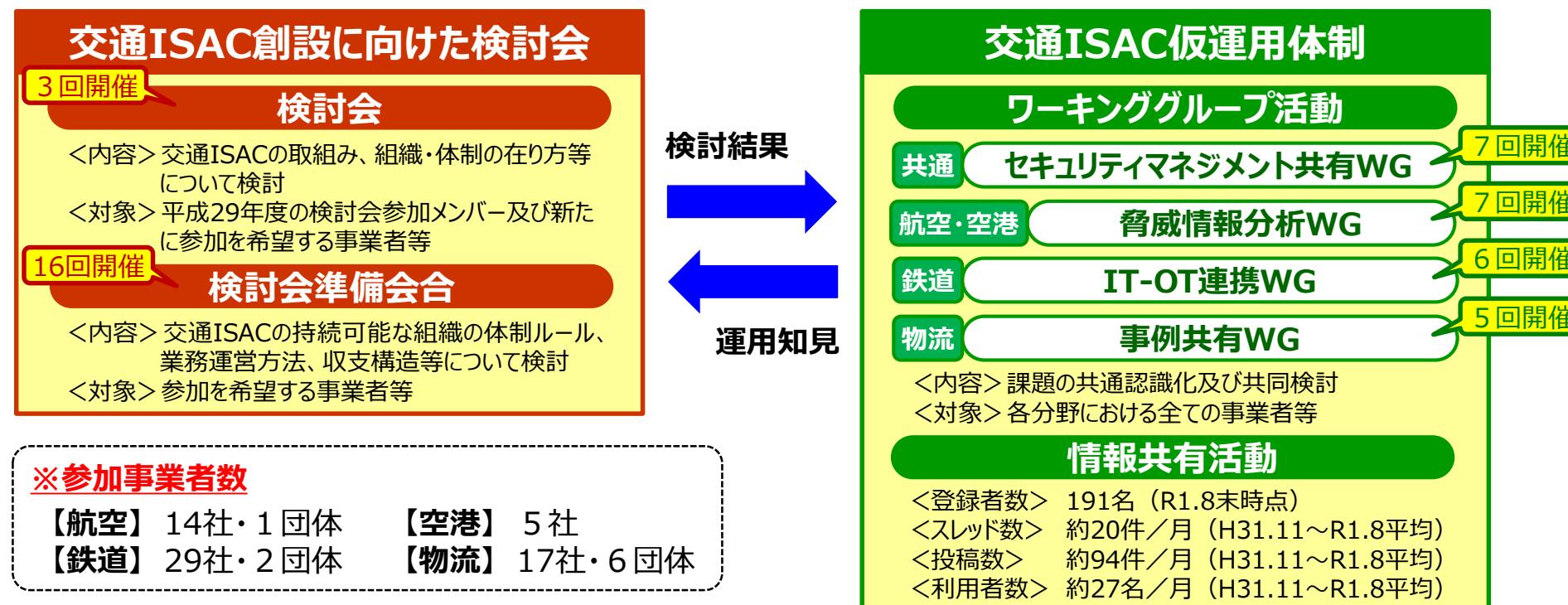
- 交通ISACの「創設に向けた検討会」及び「仮運用体制」の両輪で推進。

#### ➤ 交通ISAC創設に向けた検討会

- ✓ 平成29年7月に設置以降、交通ISACの持続可能な在り方等について検討。
- ✓ 平成31年3月の第3回会合において、交通ISACを一般社団法人として創設することを目指して検討を進めていくことに合意。

#### ➤ 交通ISAC仮運用体制

- ✓ 平成30年4月にワーキンググループ活動を、同年9月にSIGNALシステムを使用した情報共有活動を開始し、交通ISACの有用性及び実効性について検証。





ANAシステムズ株式会社  
品質・セキュリティ管理部  
ANAグループ情報セキュリティセンター  
ASY-CSIRT  
エグゼクティブマネージャー



Certified SIM3 Auditor  
阿部恭一

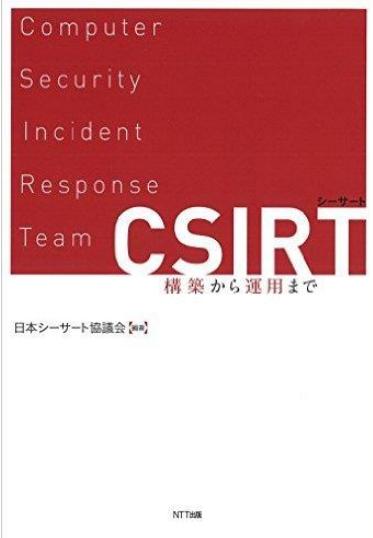
Open CSIRT  
Foundation

## ＜外部団体メンバー＞

日本シーサート協議会：シーサート人材WG、机上訓練SWG、トレーニングSWG  
日本ネットワークセキュリティ協会：情報セキュリティ知識分野（SecBoK）改訂委員  
国際化サイバーセキュリティ学 C y s e c 講師  
産業サイバーセキュリティセンター 中核人材育成プログラム講師  
経済産業省 セキュリティサービス審査登録制度に関する有識者検討会 委員  
交通ISAC セキュリティマネージメント共有WG 主査  
IPAモデル契約見直し セキュリティ検討委員

## ＜外部講演2019年度～＞

I S A C国際会議  
日独セキュリティフォーラム  
損保ジャパン サイバーセキュリティセミナー  
ガートナー セキュリティ & リスク・マネジメント サミット 2019  
マイナビセミナー 巧妙化するサイバー攻撃に向けて  
JUAS 企業リスク研究会  
サイバーセキュリティフォーラム 2019  
新聞社・通信社CSIRT連絡会  
スミセイ情報企業セミナー  
CSIRT北九州協議会



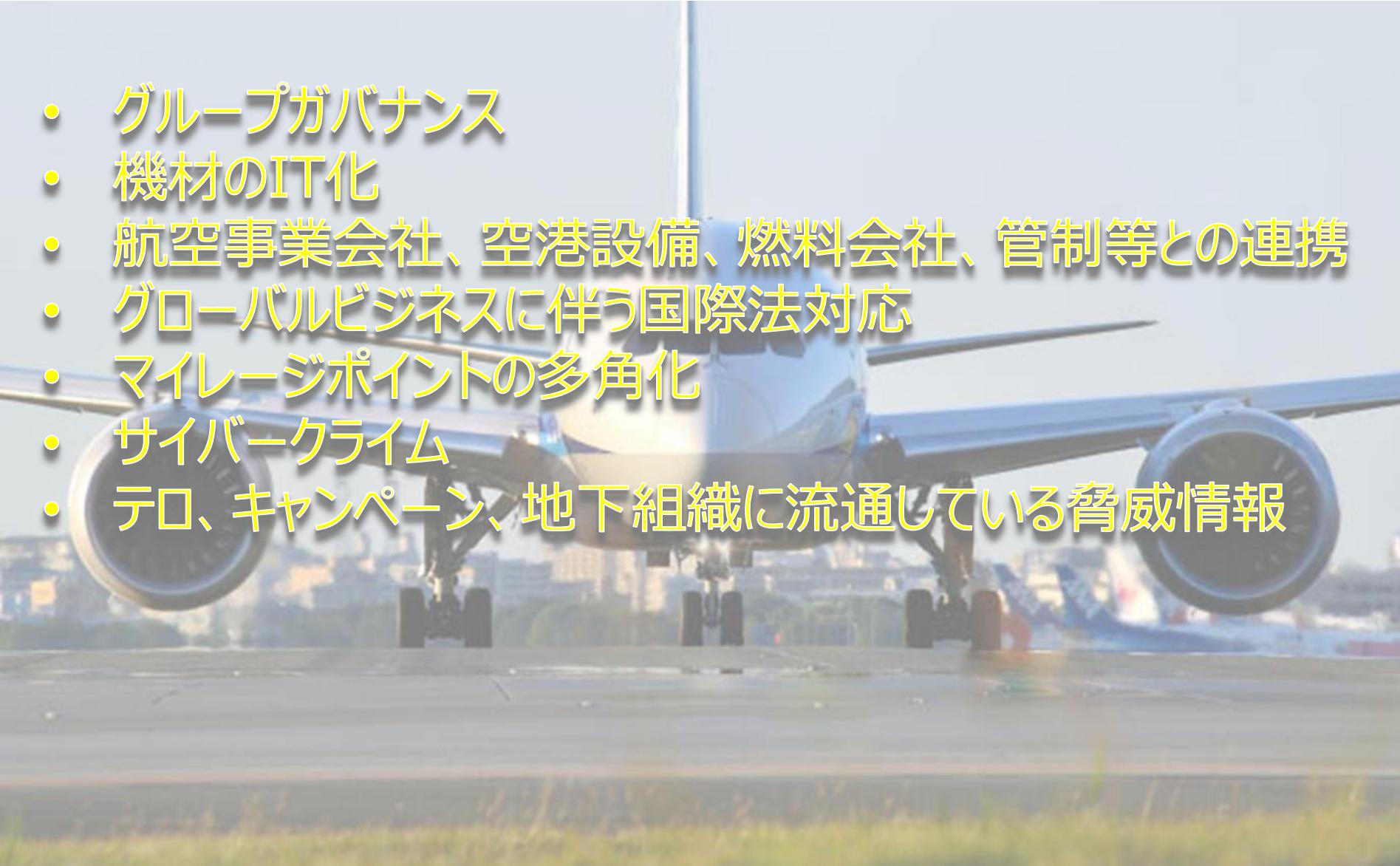
NTT出版「CSIRT 構築から運用まで」



ITMedia CSIRT小説「側線」  
2018/6月～12月まで連載

## 航空

- グループガバナンス
- 機材のIT化
- 航空事業会社、空港設備、燃料会社、管制等との連携
- グローバルビジネスに伴う国際法対応
- マイレージポイントの多角化
- サイバークライム
- テロ、キャンペーン、地下組織に流通している脅威情報

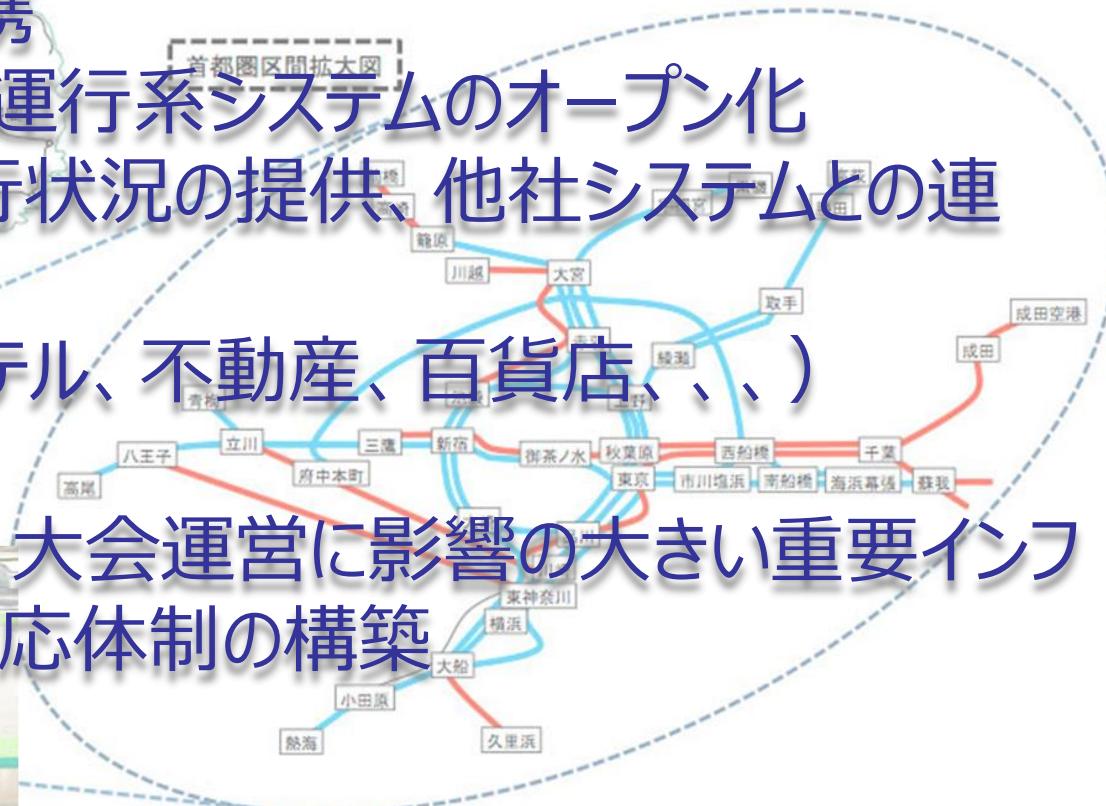
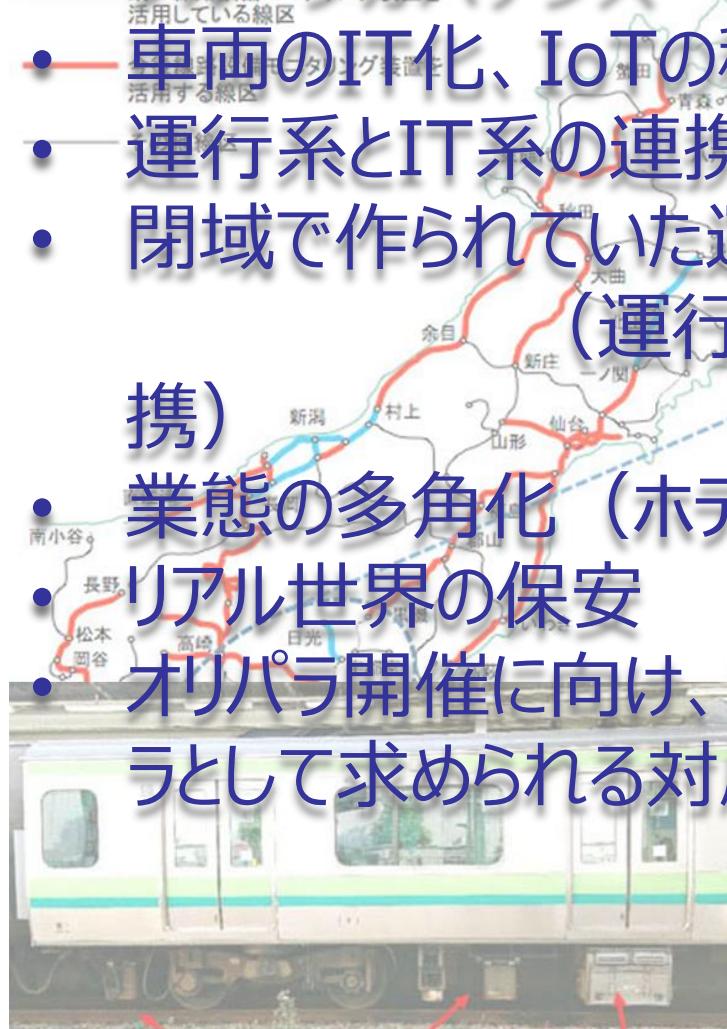


### 3. 交通ISAC創設に向けて (3/10)

## 鉄道

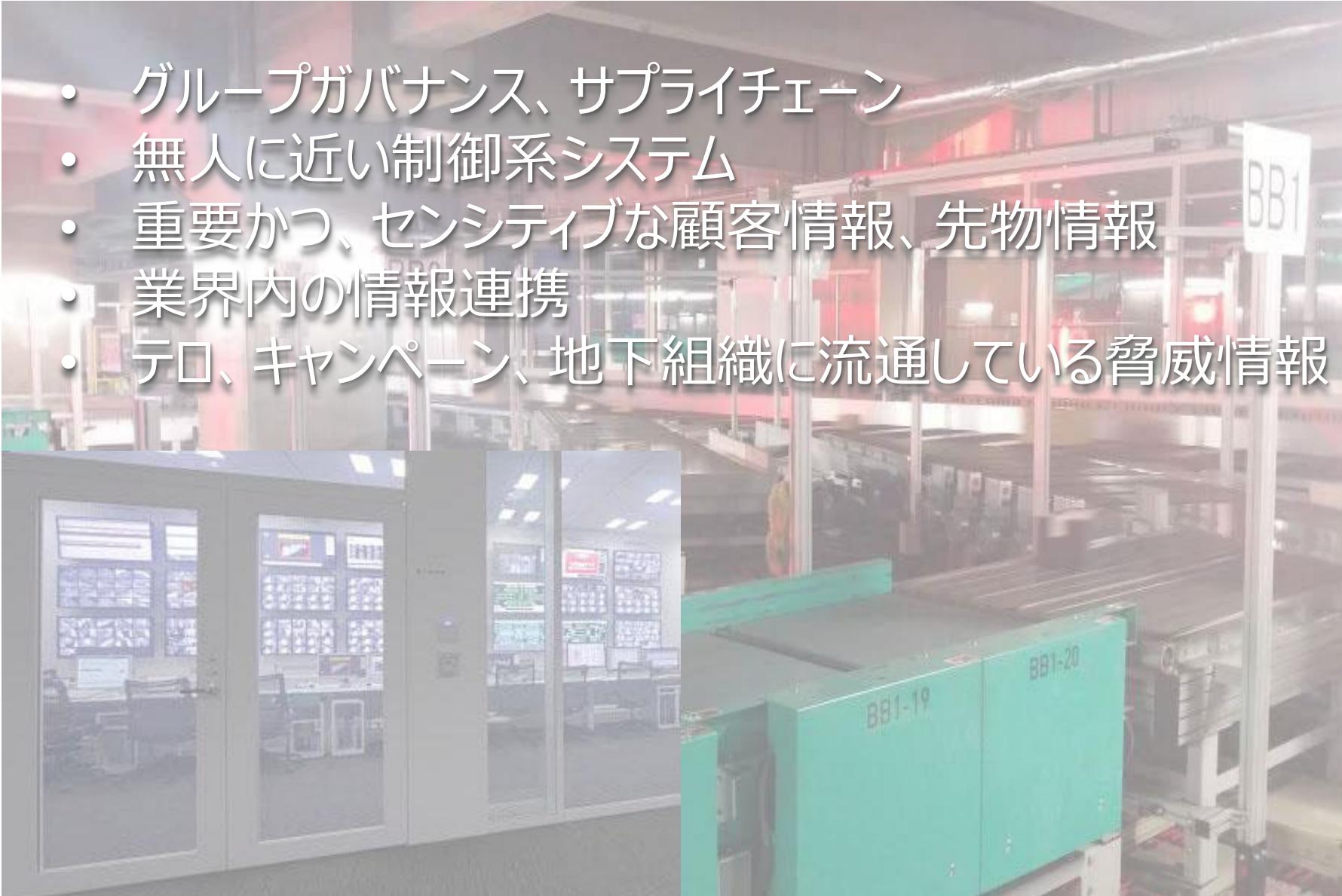
線路設備モニタリング装置導入線区

- ・ グループガバナンス
- ・ 車両のIT化、IoTの積極活用
- ・ 運行系とIT系の連携
- ・ 閉域で作られていた運行系システムのオープン化  
(運行状況の提供、他社システムとの連携)
- ・ 業態の多角化 (ホテル、不動産、百貨店、、、)
- ・ リアル世界の保安
- ・ オリパラ開催に向け、大会運営に影響の大きい重要インフラとして求められる対応体制の構築



## 物流

- グループガバナンス、サプライチェーン
- 無人に近い制御系システム
- 重要かつ、センシティブな顧客情報、先物情報
- 業界内の情報連携
- テロ、キャンペーン、地下組織に流通している脅威情報



## 何を共有すべきか

### -予防に役立つ情報

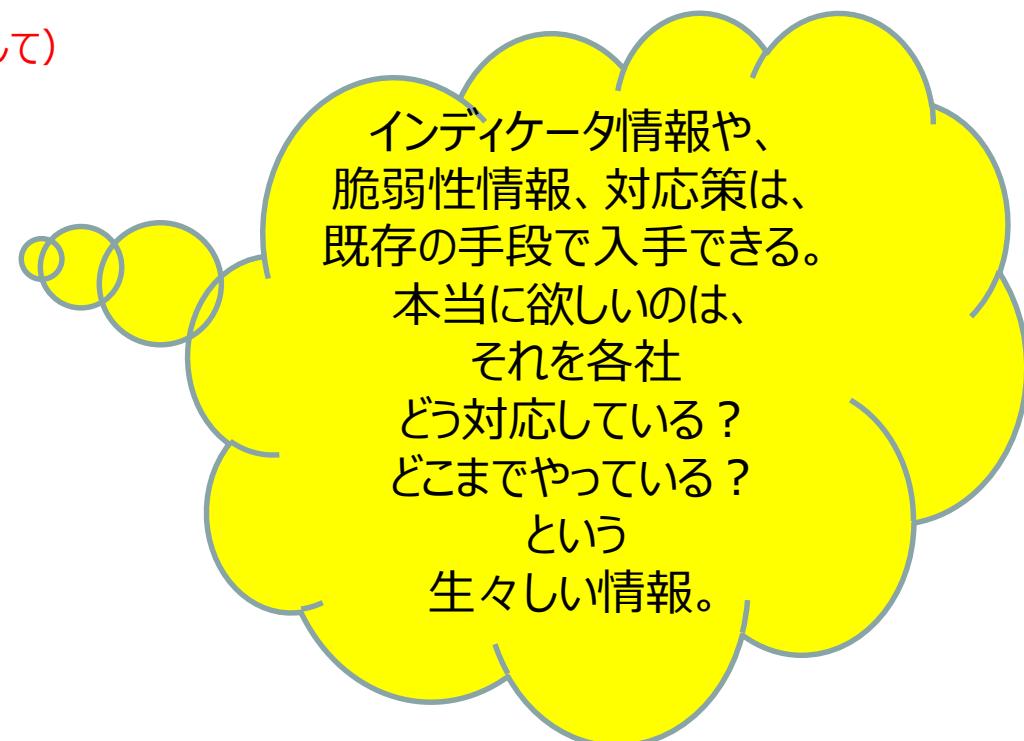
- ✓ 事件・事故事例
- ✓ 各種インディケーター情報
- ✓ 脆弱性情報と対応策
- ✓ 攻撃の最新手法
- ✓ 犯罪者の背景（攻撃を受ける確率判断として）
- ✓ 自社に関する地下組織流通情報（将来攻撃を受ける可能性として）

### -インシデント発生時に役立つ情報

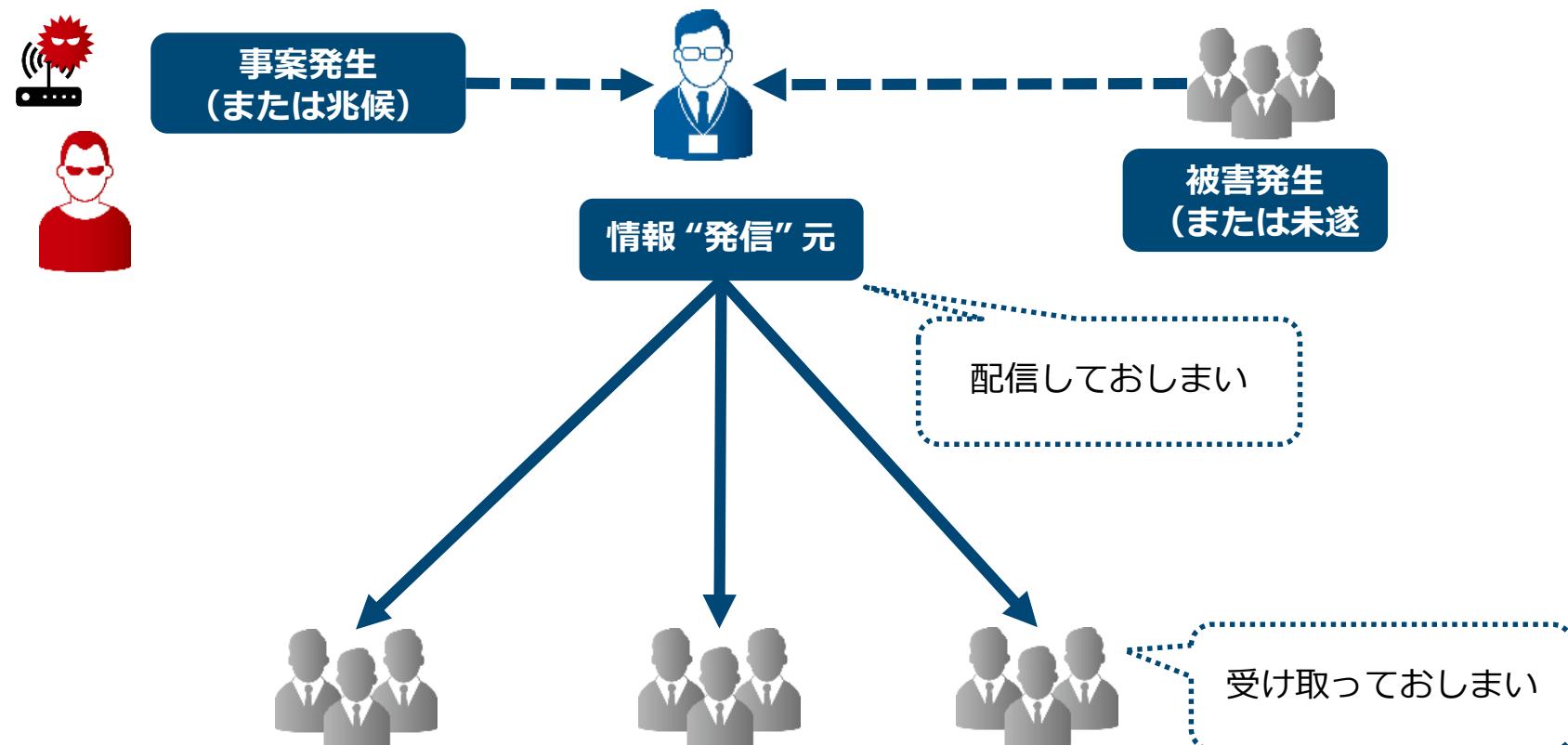
- ✓ 対応・対処方法
- ✓ 各種インディケーター情報
- ✓ 攻撃の最新手法
- ✓ 気づかぬ被害状況の指摘
- ✓ 犯罪者の背景（攻撃の目的の判断として）

### -経営陣への説明・自社のベンチマークとして役立つ情報

- ✓ 世間で起きている事象の解説
- ✓ 他社のセキュリティ対策状況
- ✓ 他社の法令対応の対策状況
- ✓ 情報の運用方法、キュレート手法



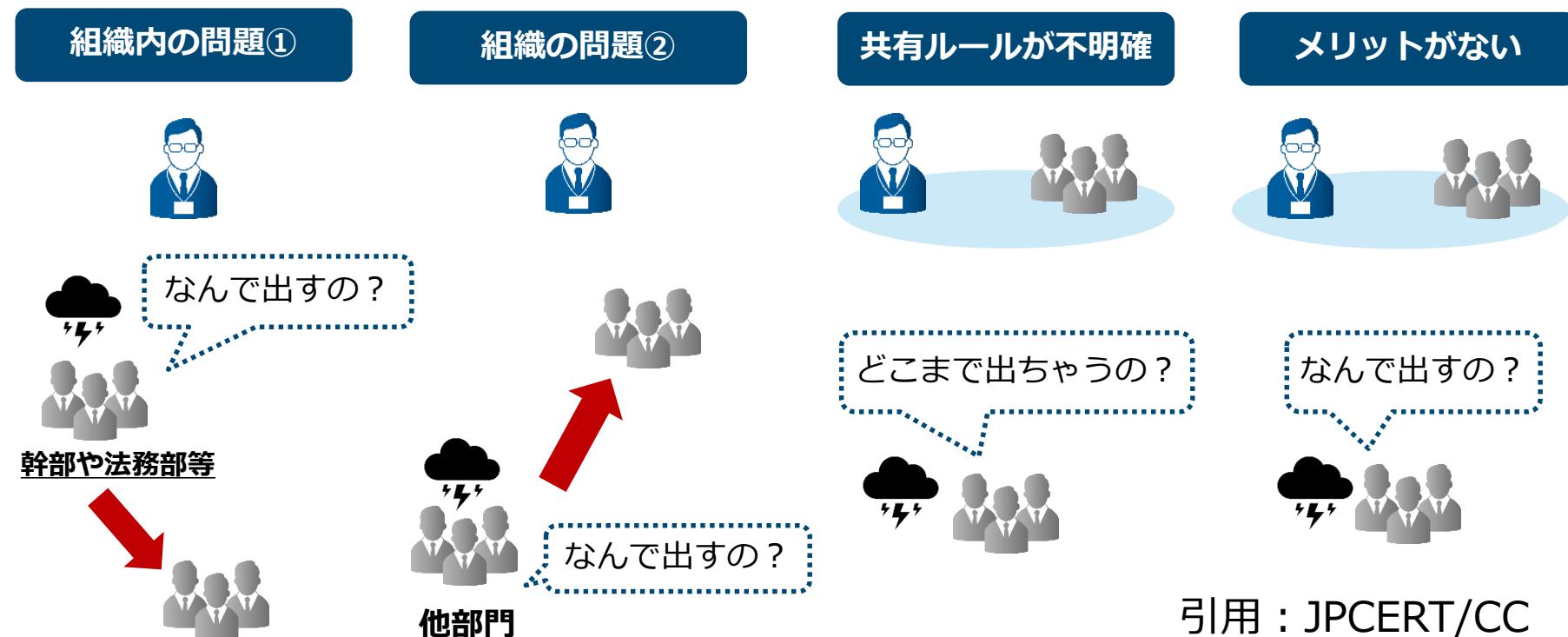
## なぜ、共有できないのか、なにが課題なのか



引用：JPCERT/CC

## なぜ「情報提供」できないのか

- 各社の「動機」のほかに阻害要因がそれぞれ存在する
- 各社、各分野毎にそれぞれの阻害要因がある
- 一方で、情報共有活動側の問題（ルール不足、とりまとめ組織の能力的・立場的問題）もある



引用：JPCERT/CC

- 情報は隠すべきもの？
  - インシデントが起きてることは知られたくない。  
=> なんとか社内で収めたい。
- ノウハウの流出？
  - 社内の知識を公開するなんてもってのほか！
- 波風を立てたくない？
  - 変に目立つと攻撃対象となるのでは！

### 3. 交通ISAC創設に向けて (9/10)

- 情報は隠すべきもの？
  - インシデントが起きてることは知られるたくない。  
=> なんとか社内で隠したい。  
*社内知識だけで解決できる  
単純なインシデントは少なくなっています。*
- ノウハウの流出？
  - 社内の知識を公開するのももってのほか！  
*ただのりばかりでは信用が得られません。  
ただのりばかりでは信用が得られません。  
ギブ＆テークが原理原則。*
- 波風を立てたくない？
  - 変に目立つと攻撃対象となるのです！  
*ブラフであっても、敵は攻撃の優先順位  
を下げます。*

#### ★集団防衛

敵はエコシステムを構築し、効率的、かつ、  
効果的に攻撃を仕掛けてくる。

もはや、企業単独で戦い、守れる状況ではない。

## 4. 交通ISACを仮運用した効果 ～情報共有から共助へ。急勾配克服のスイッチバック～

---

- もう一度考えよう。交通ISACの価値とは？
  - 情報共有だけなら業界内でいままで行っている。
  - ベンダーをメンバーに加えることに抵抗がある。
  - 会費に見合った効果はあるのか？
  - リード、主査はだれができるのか？OT部門を巻き込むには？
- まずは試行として、Online、Offline両方でスマールスタート。
  - SIGNALでの情報共有、相談
  - WGでの情報共有、相談

## 試行の効果

- Onlineでの効果

- 最初は投稿は極少。インディケーター情報など。自社の情報は出さない期間が続く。
- 転機は自社でのインシデント発生。各社から対応方法の知恵が集まりだす。
- この成功体験が引き金となって各社から事例が集まりだす。知恵も結集される。ベンダーからもアドバイスが集まつてくる。
- 赤裸々な事例が集まつてくる。
- **単なる情報共有から共助にレベルアップし、集団防御の形が見えてくる。**

- Offlineでの効果

- WGでのfacetofaceの会議
- 「ここだけのハナシ」、で信頼感が醸成される。WGで集まつた異業界システムの接点が見えてくる。
- 赤裸々な事例が集まつてくる。
- お互いのレベルの理解がOnlineにも反映され、活発になる。
- 今までの業界を超えた共助が実現され、人的ネットワークの広がりを見せる。  
**各個社での人材不足の課題に対して、相談相手が格段に増える。**

## 5. 持続可能な交通ISACへ ～一般社団法人設立への道～

---

## 設立趣意

### 交通ISACの設立

#### ● 目的

➤ 交通・運輸分野の事業者等がサイバーセキュリティに関する広範な連携・協力を行うことにより、サイバー攻撃等に対する分野横断的な集団防御力の向上に資する活動を推進し、もって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。

#### ● 運営形態

➤ 交通ISACが実施する事業の安定性及び持続性を確保するとともに、組織としての社会的信用性及び公益性の維持・向上を図るため、一般社団法人（非営利型）の法人格を取得して運営する。

## 事業内容

- 当面の間、現行の仮運用体制と同様、ワーキンググループ活動及びSIGNALを使用した情報共有活動の2つをメインとする。  

将来的には
- 法人設立後、**交通ISACの在るべき姿を整理・検討の上**、事業の安定性及び持続性並びにそれに必要な財政基盤を確保しつつ、段階的に事業を拡充していく。



# 5. 持続可能な交通ISACへ～一般社団法人設立への道～(4/4)

## 組織体制



## 6. 交通ISAC入会案内 ～TAKE OFF !～

---

日本の動脈を守る！



ご清聴、ありがとうございました