NISC National center of Incident readiness and Strategy for Cybersecurity

資料5-1

安全なIoTシステムの検討に関する今後の進め方について（案）

平成３０年６月

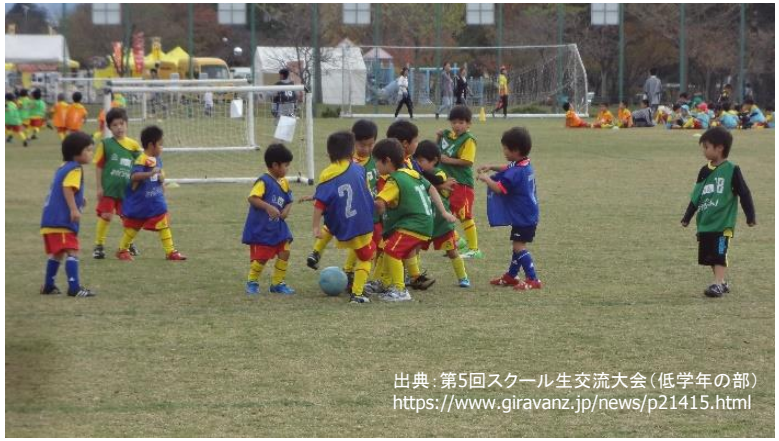
内閣サイバーセキュリティセンター

基本方針

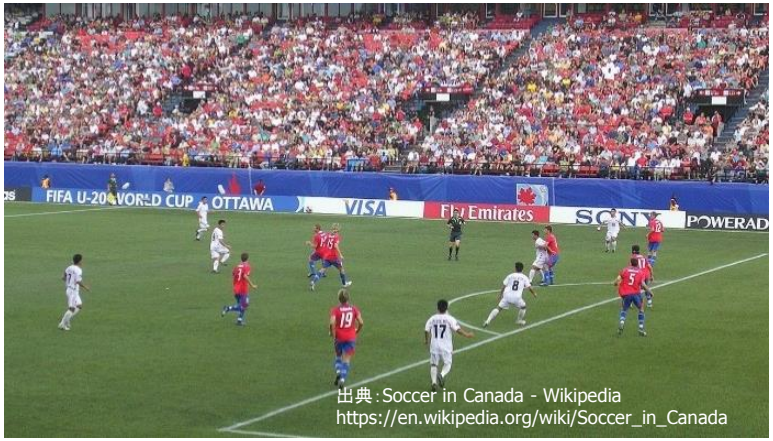
多様な主体が体系的に安全なIoTシステムを効率的に推進していくためには、関係主体間でセキュリティ対策に係る基本理念、目標、方法、期限等についての共通認識を醸成

- 競争領域を除き、官民を含む関係主体間での相互信頼に基づく情報共有
- できるだけ競合を排除
- 相互に力を合わせることを基本
- 各主体の取組をマッピングし、情報共有

など検討する。

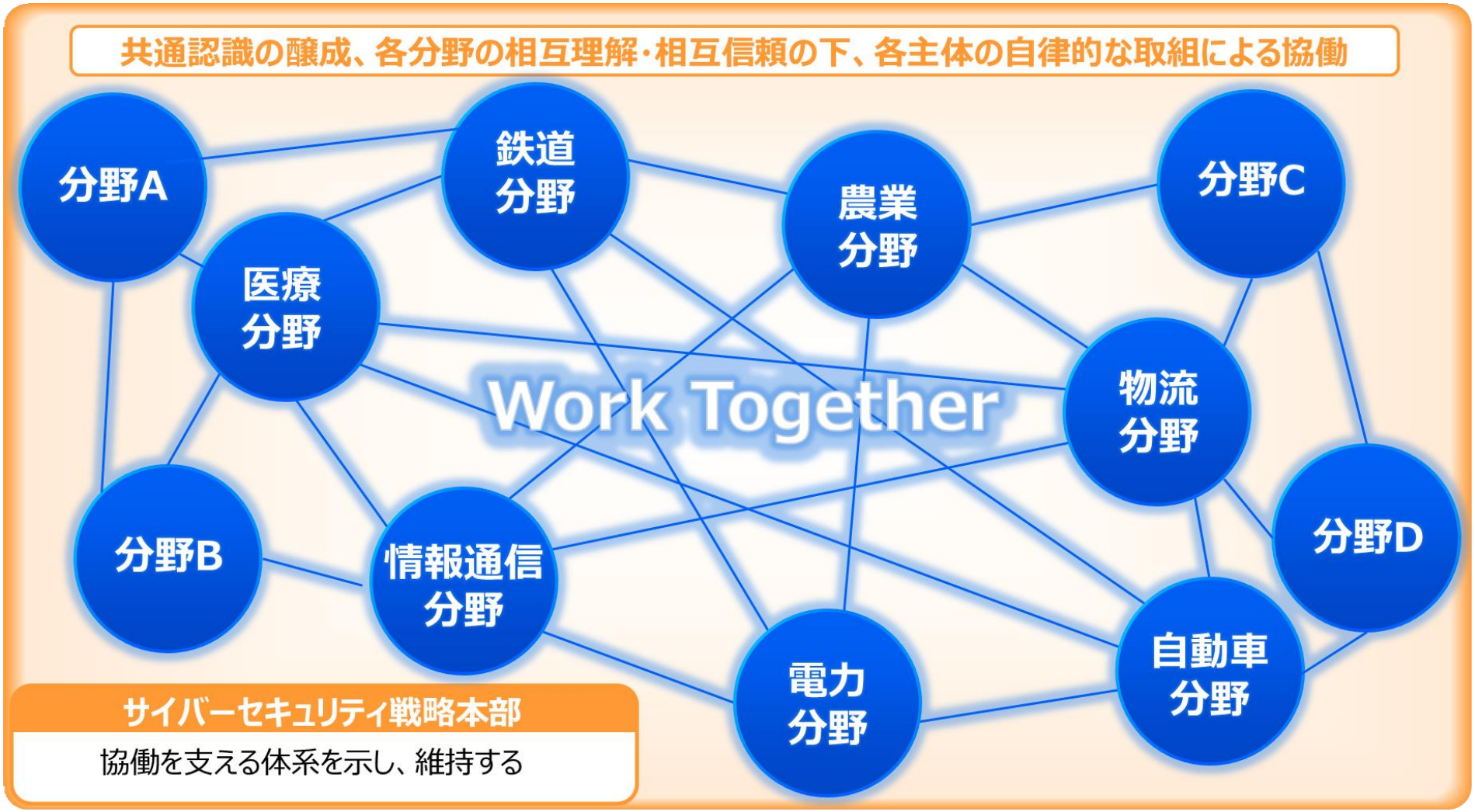


出典：第5回スクール生交流大会（低学年の部）
https://www.giravanz.jp/news/p21415.html



出典：Soccer in Canada - Wikipedia
https://en.wikipedia.org/wiki/Soccer_in_Canada

1. 各産業分野とNISCの役割のイメージ



2. これまでの検討の経緯

平成27年

- ９月：サイバーセキュリティ戦略の策定
- 秋　：総務省・経済産業省がIoTセキュリティガイドラインの検討開始

平成28年

- ６月：安全なIoTシステムのセキュリティに関する一般的枠組の意見募集
- ７月：総務省・経済産業省がIoTセキュリティガイドラインを策定
- ８月：安全なIoTシステムのセキュリティに関する一般的枠組の策定

平成29年

- ３月：官民の有識者による「安全なIoTシステムの創出に向けた意見交換会を発足」

平成30年

- ３月：４回にわたる意見交換会の開催を経て、その成果のとりまとめ文書（素案）を提示
- ４月：関係省庁調整会合（準備会合）

3. 趣旨・目的

IoTはさまざまなモノ（機器）が連接することによる新たな価値の創造

セキュリティレベルや物理的安全性等の基準が異なるモノがつながることによる新たな脅威

基本方針：
IoTシステムによる新たな価値の創造を実現するため、競争領域を除き、官民を含む関係主体間での相互信頼に基づく情報共有によって、できるだけ競合を排除し、相互に力を合わせていく

当面の取組：
関係各府省庁の
①実現したい項目
②それに必要な検討分野
③それらの見える化（マッピング）
④各府省庁の連携体制の在り方
をスケジュール感を含め検討し、今年度第二四半期を目途にアクションプランとして整理

4. アクションプランにおける分野・項目の整理

応用分野
（項目）IoTの脆弱性対策、IoTシステムに関わるサプライチェーンリスク対策、
産業分野別の課題

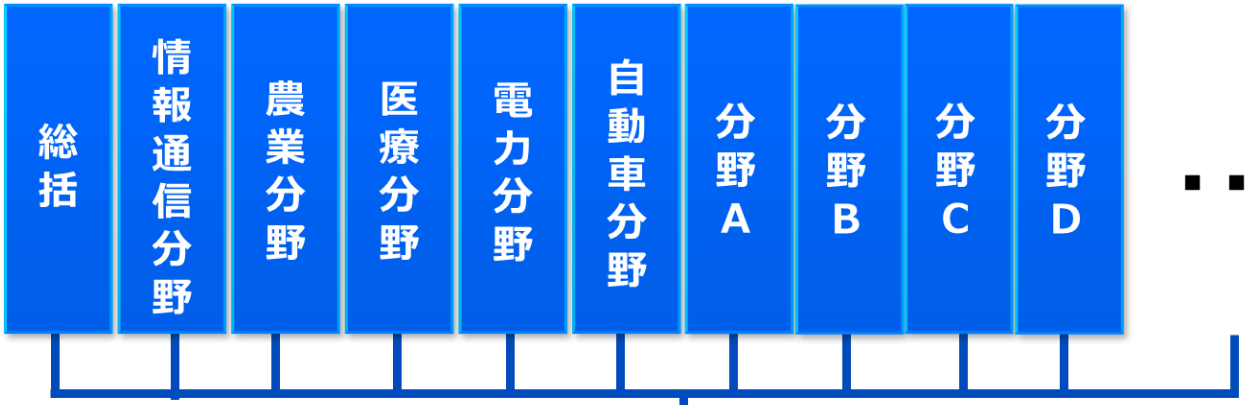
標準化分野
（項目）国際基準戦略
IoTプラットフォームの標準化

法令分野
（項目）財産上の責任分界点、
データ利活用、プライバシー（P）

基礎分野
（項目）範囲・定義・カテゴリー、機器の物理安全対策、CIAと強靭性・信頼性

5. 検討体制（案）

各分野の所管省庁等が中心となって検討



関係省庁が中心となって検討
（事務局：NISC）

関係省庁調整会合
（各分野におけるサイバーセキュリティの取組について共通認識の醸成や情報共有などの総合調整を行う会合）

安全なIoTシステム創出のためのセキュリティWG
（有識者、産業界、関係省庁等が出席し、方向性を検討するためのWG）

サイバーセキュリティ戦略本部

※例示した分野は、イメージ