IoT時代のセキュリティについて

（情報通信審議会　情報通信技術分科会　技術戦略委員会　重点分野WG（第3回）資料）

2015年4月10日

東京工科大学
手塚　悟
tezuka@stf.teu.ac.jp

IoTの到来とセキュリティ上の問題点

問題点①
IoT/M2Mはセキュリティ対策が不十分

□IoT/M2Mシステムではセキュリティ対策のスキームが未整備

●従来のPCベース環境を利用したICTシステムは、Windows、LinuxなどのOSをベース

●供給者責任による脆弱性対策の提供や、ウィルス対策ソフトウェアや脆弱性検査ツールおよび脆弱性情報公開により、セキュリティ対策のスキームが整備

●IoT/M2Mシステムにおいては、そのスキームは未整備

問題点②
サイバー攻撃の対象範囲、影響範囲の拡大

□IoT/M2Mシステムがサイバー攻撃の対象に

●サイバー攻撃の対象は、従来のPCベースの環境にとどまらない

●Android、iOSなどをOSとする環境、さらには組込み機器、制御機器も攻撃対象に

□サイバー攻撃が物理空間にも影響を及ぼす

●重要インフラや自動車等がサイバー攻撃により物理的影響を受ける事態は避けなければならない

セキュリティ対策の方向性

方向性①
IoT/M2Mの特徴を考慮したセキュリティ対策

□現状の脆弱性の洗い出しと、今後のセキュリティ対策

●現状で運用されているIoT/M2Mシステムのセキュリティ点検は急務
●その上で今後、ウェアラブル等のリソース制約のある機器への軽量暗号の実装や
●PC・スマホと異なり常時接続では無いシステム（車など）へのソフトウェアアップデートのためセキュアなプロトコルの整備が必要

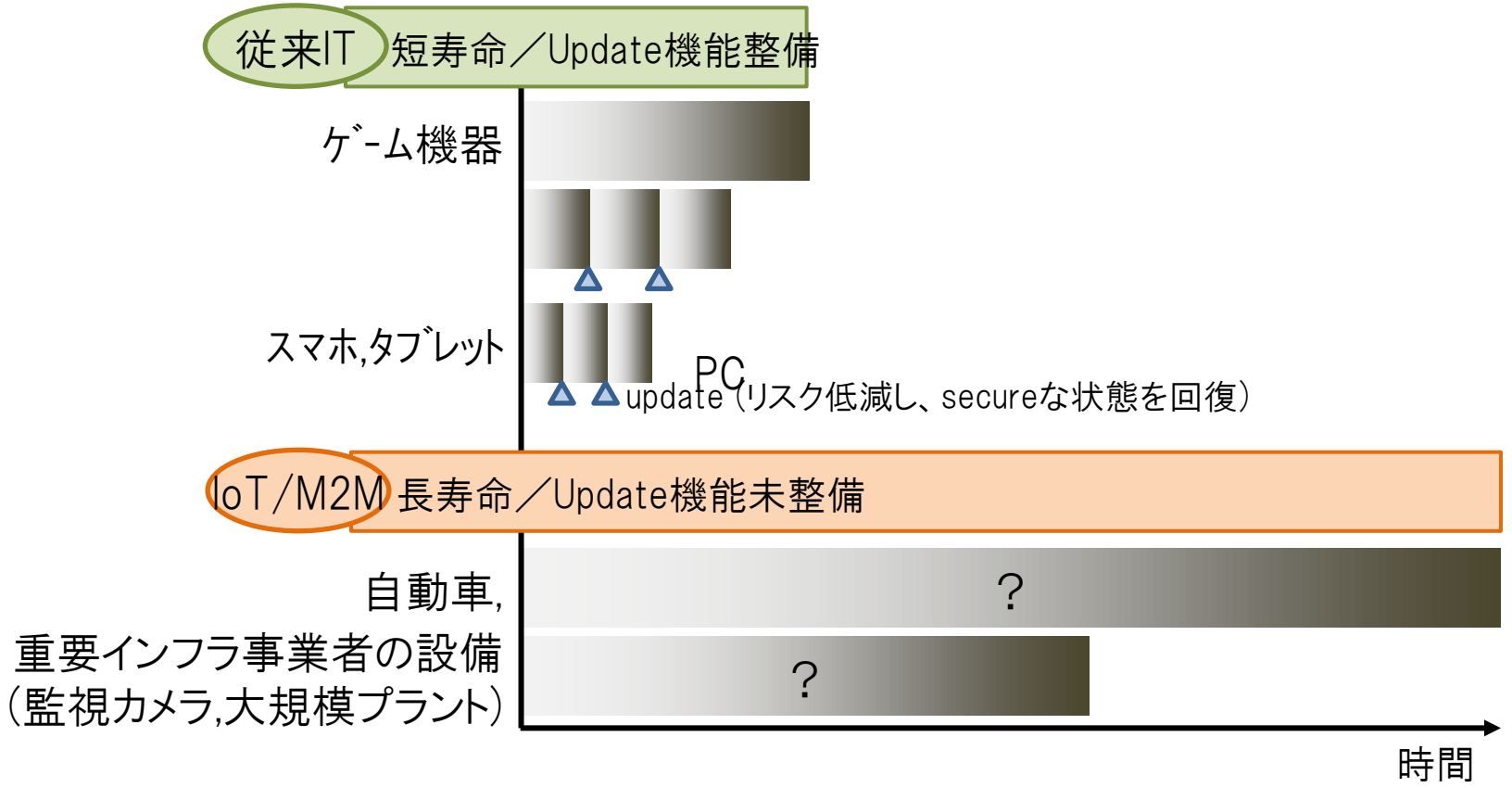
方向性②
情報交換モデルの構築

□対象範囲、影響範囲が拡大する攻撃への対処

●セクショナリズムにとらわれ、断片情報にとらわれていては攻撃を理解できない
●また、サイバー空間のみではなく、物理空間も含めた全体を俯瞰する観点が重要
●攻撃事象だけではなく、いかに予兆を捉えるか
●2020オリ・パラ東京大会も見据えて、国家としての情報交換モデルの構築は急務

IoT/M2Mの特徴を考慮したセキュリティ対策（例）

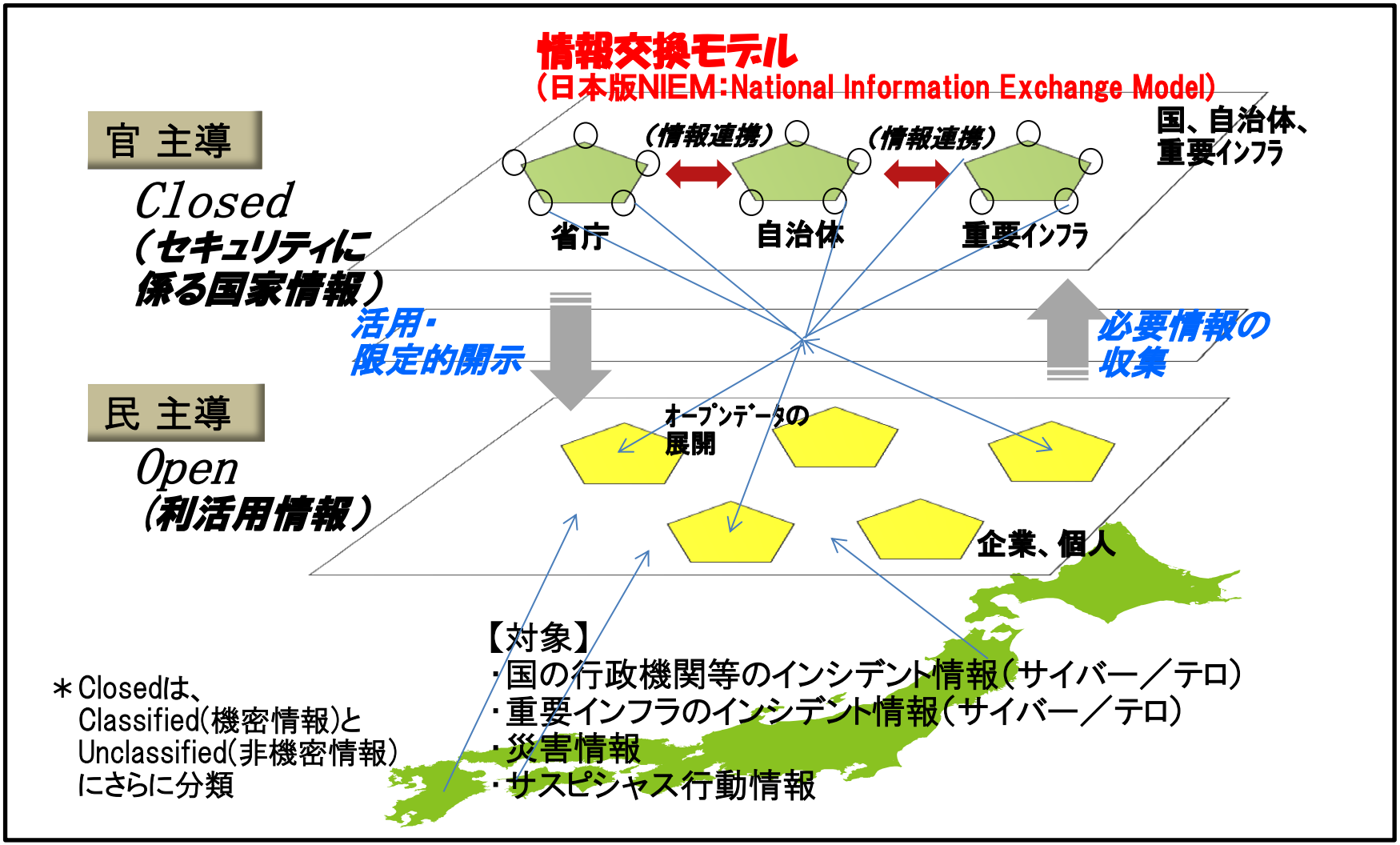
IoT/M2MをUpdatableとする技術、枠組みの整備など



IoT/M2Mシステム向けにソフトウェアや暗号鍵の更新を行うための
セキュア通信プロトコルの開発が重要

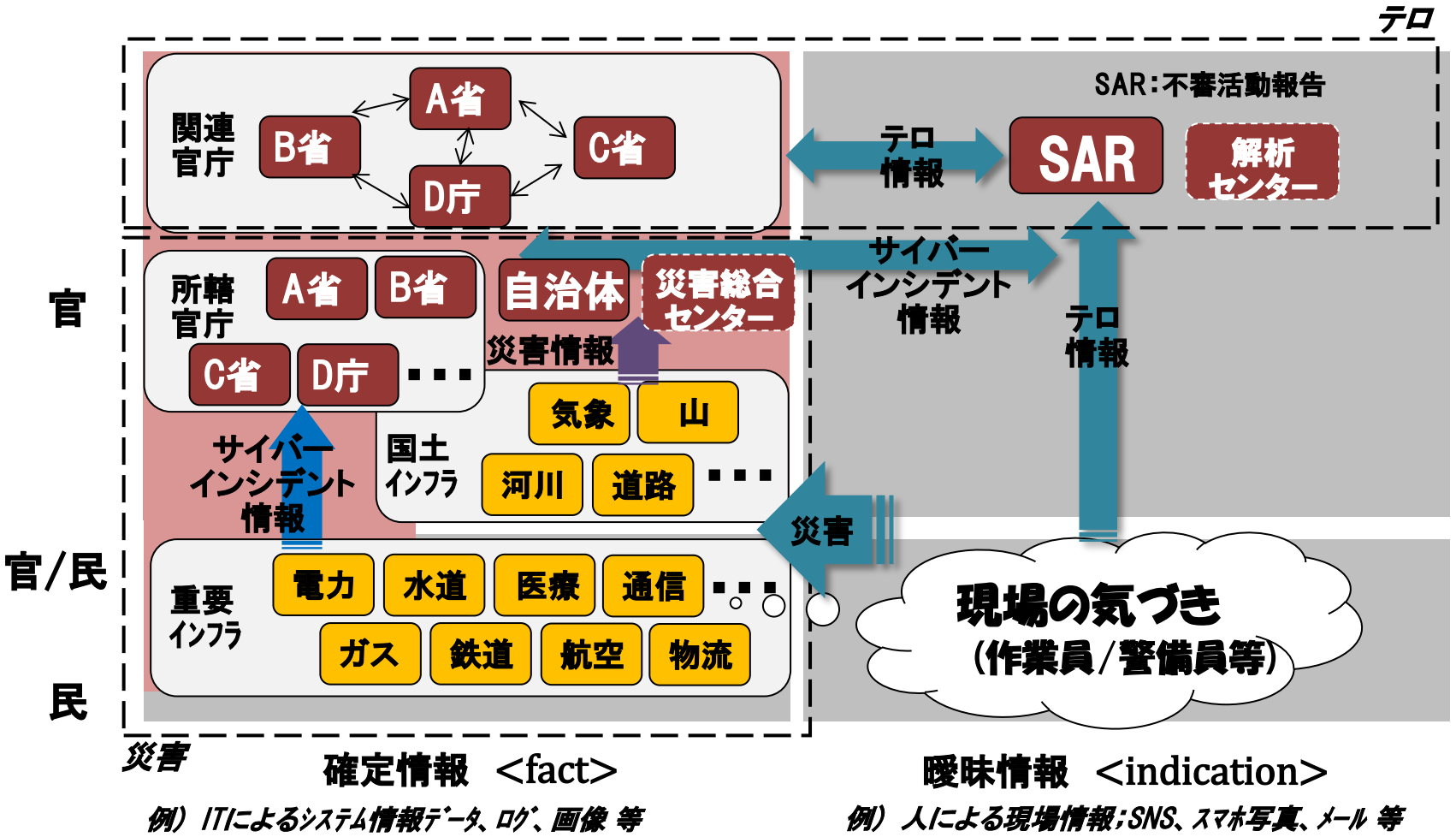
情報交換モデルの構築

サイバー攻撃の全容を把握するために
国家における情報交換モデルの構築を図る



緊急対応を踏まえた「平時における」情報共有の在り方

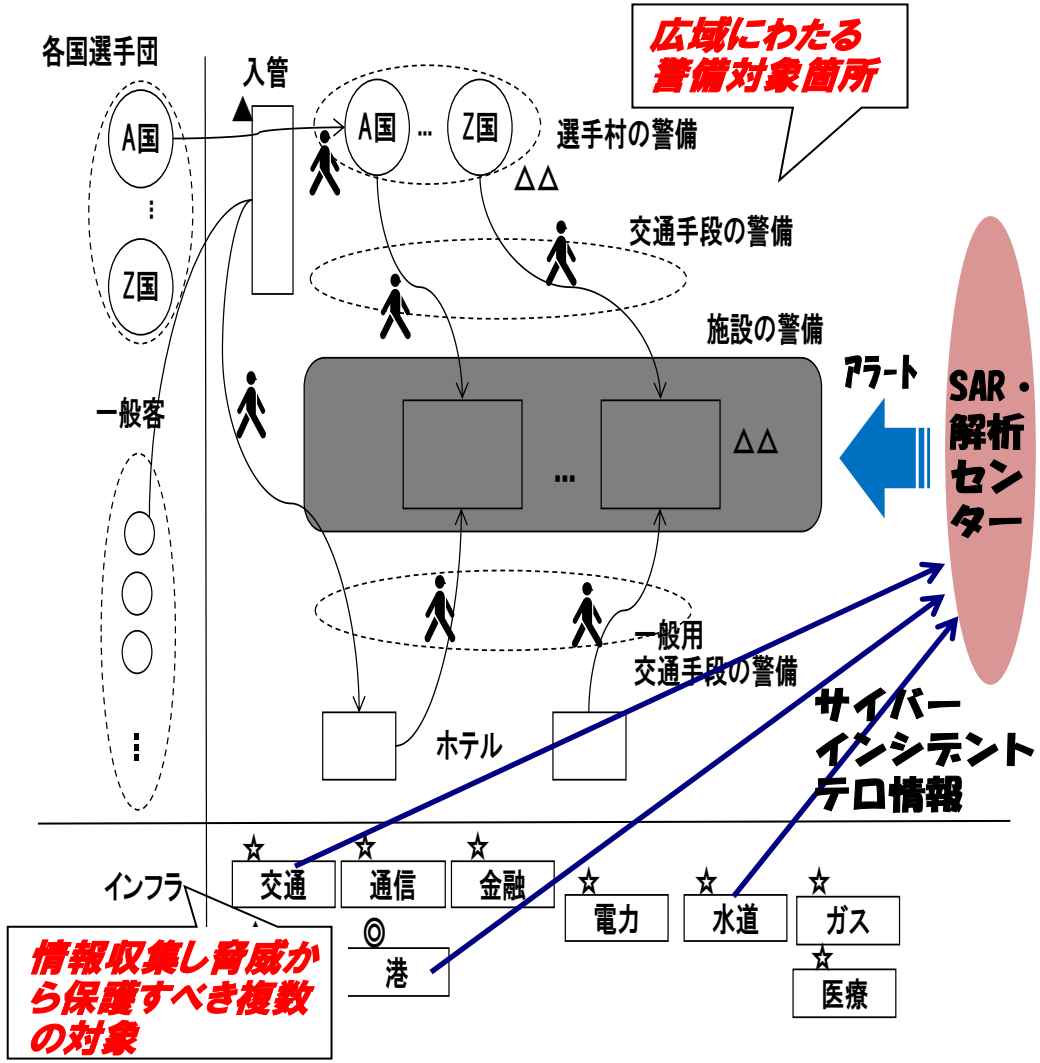
■ 災害、テロ対策を代表例として情報共有をシミュレート



「現場の動き」を定常情報で裏付けし、予兆を検知し、現場へ指示

SAR：Suspicious Activity Report

東京オリンピックを例とした警備上の課題



異なる組織群による連合体

東京オリンピックにおけるセキュリティ要員の内訳		
公的機関	○警察官	21,000
	●緊急サービス（消防隊，救急隊）	6,000
	◎海上保安官	850
民間機関	△民間警備員	14,000
	△セキュリティボランティア	9,000
計		50,850

対象人員が相当に大規模

＜課題＞

テロ対策に必要な情報が共有できず実効ある対応・指示を出す事が困難

情報共有の為のアーキテクチャやデータ交換時の標準手順が必要

① 現場を含めた情報を如何に収集するか　② 収集した情報を如何に分析するか
③ 有用情報を如何に共有し活用するか

NICTに期待すること

国研としての研究開発能力の維持

- NICTは我が国を代表する研究開発機関
- ナショナルセキュリティの観点で、セキュリティ分野の研究開発能力の維持
- 暗号等の基礎的研究分野における研究開発能力の維持も極めて重要

国研としてのリーダーシップの発揮

- 国研としてリーダーシップを発揮
- 民間のイノベーションを創出する触媒としての働きも期待したい