ITU-TにおけるIoTセキュリティ標準化

ーITU-T SG17を中心にー

中尾　康二

情報通信研究機構（NICT） 主管研究員

横浜国大　客員教授

内閣官房　NISC　サイバーセキュリティ参与

ITU-T SG17
Security

SG17 – ミッション

- 情報通信技術（ICTs）の利用における信頼性と安全性の構築は、ITUの最優先課題の一つである。
- IMT-2020/5G以降（６Gを含む）のセキュリティ、IoT、スマートシティ、DLT（仮想通貨関連）、クラウド技術を含むビッグデータ解析、ITS（インテリジェント交通システム）、人工知能（AI）や量子関連技術に関するセキュリティの視点での多種多様な革新的な技術を用いて、ネットワーク、アプリケーション、サービスなどの多様な資産を保護するための技術的、組織的、物理的対策を検討するのがSG17である。
- 新たな安全保障上の脅威（サイバーテロ等を含む）に適切に対処するための新たなセキュリティアプローチに取り組んでいる。
- すなわち、SG17では、枯れた技術内容（十分に実証された）の国際規格化だけではなく、新しい視点からみたセキュリティ技術の国際標準化にも積極的に取り組んでおり、革新的な技術の早期共有化や相互参照化を進めている。

Study Group 17 における議長、副議長の方々

Mr Samir ABDELGAWAD
Egypt

Mr Heung Youl YOUM
Korea (Republic of)

Mr Gökhan EVREN
Turkey

Mr Yutaka MIYAKE
Japan

Ms Lia MOLINARI
Argentina

Mr Greg Ratta
USA

Mr Arnaud Taddei
UK

Ms Wala TURKI LATROUS Tunisia

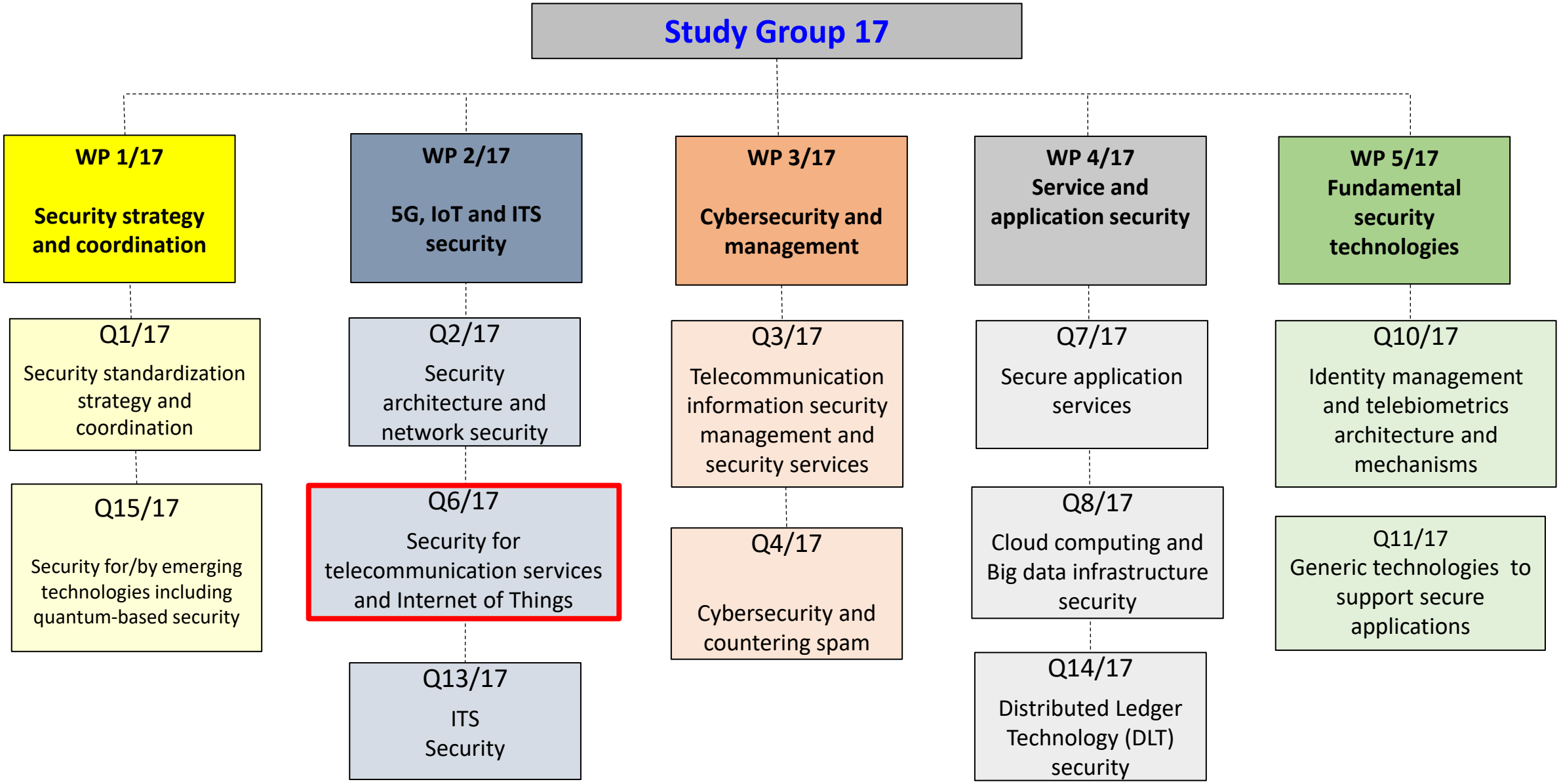
Mr Liang WEI
P.R. China

SG17参加国 （主な参加国：CJK+US/UKなど）

SG17におけるワーキンググループの構成

- **WP 1　Security strategy and coordination**
  - Q1/17　Security standardization strategy and coordination
  - Q15/17　Security for/by emerging technologies including quantum-based security
- **WP 2　5G, IoT and ITS security**
  - Q2/17　Security architecture and network security
  - Q6/17　Security for telecommunication services and Internet of Things
  - Q13/17　Intelligent transport system (ITS) security
- **WP 3　Cybersecurity and management**
  - Q3/17　Telecommunication information security management and security services
  - Q4/17　Cybersecurity and countering spam
- **WP 4　Service and application security**
  - Q7/17　Secure application services
  - Q8/17　Cloud computing and Big data infrastructure security
  - Q14/17　Distributed Ledger Technology (DLT) security
- **WP 5　Fundamental security technologies**
  - Q10/17　Identity management and telebiometrics architecture and mechanisms
  - Q11/17　Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications

ITU-T SG17の構造・構成



Study Group 17における主なトピック

Technical solution toolkit for trust

Identity management and tele-biometrics

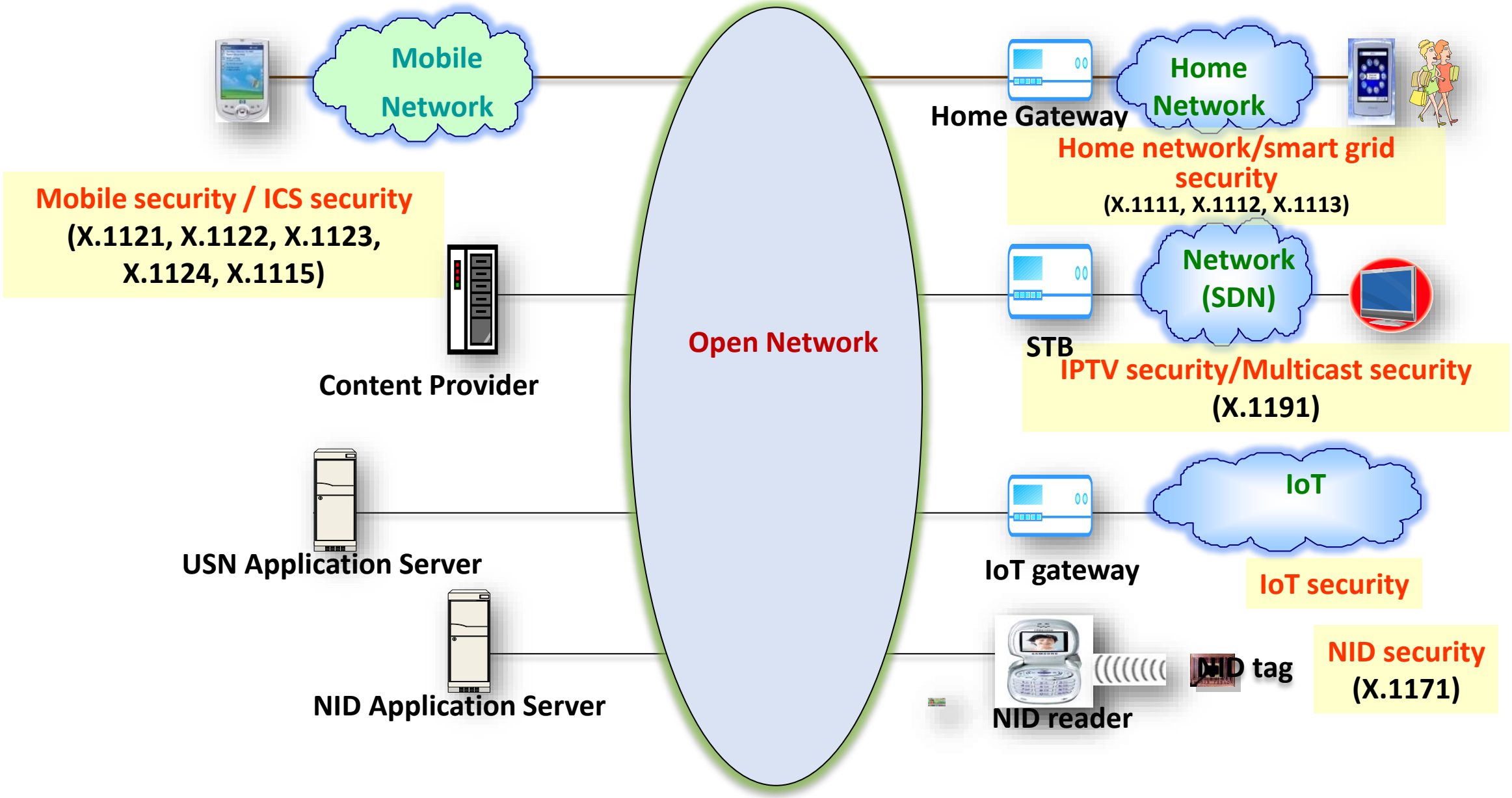
Application security solutions

IoT

5G/B5G (6G)

Security management

Question 6/17 – スコープ



SG17 課題6におけるIoT 国際標準文書

- X.1352: Security requirements for Internet of things devices and gateway
- X.1353 (draft): Security methodology for zero-touch Deployment in massive IoT based on blockchain
- X.1361: Security framework for the Internet of things based on the gateway model
- X.1362: Simple encryption procedure for Internet of things (IoT) environments
- X.1363: Technical framework of personally identifiable information handling system in Internet of things environment
- X.1364: Security requirements and framework for narrowband Internet of things
- X.1365: Security methodology for the use of identity-based cryptography in support of Internet of things (IoT) services over telecommunication networks
- X.1366: Aggregate message authentication schemes for Internet of things environment
- X.1367: Standard format for Internet of things error logs for security incident operations
- X.1368: Secure firmware or software update for Internet of things devices
- X.1369: Security requirements for IoT service platform
- TR.ba-io t： Broadcast authentication scheme for IoT system

X.1361：Security framework for the Internet of things based on the gateway model

スコープ：

この勧告は、セキュリティゲートウェイを使用したモノのインターネット（IoT）のためのセキュリティフレームワークを記述している。

具体的には、IoT環境におけるセキュリティ脅威と課題を分析し、これらのセキュリティ脅威と課題に対処し緩和する能力について記述している。IoTのセキュリティ脅威と課題を緩和し対処するために、どのセキュリティ能力が必要かを決定するためのフレームワーク手法が提供されている。

この勧告の焦点は、セキュリティゲートウェイを使用するIoTセキュリティ能力にあり、管理面ではなく技術面に焦点を当て、[b-ITU-T Y.4401]に記述された参照モデルを考慮する。

[ITU-T Y.4401]：Recommendation ITU-T Y.4401/Y.2068 (2015), Functional framework and capabilities of the Internet of things.

X.1361の目次

脅威

要求事項

セキュリティ能力

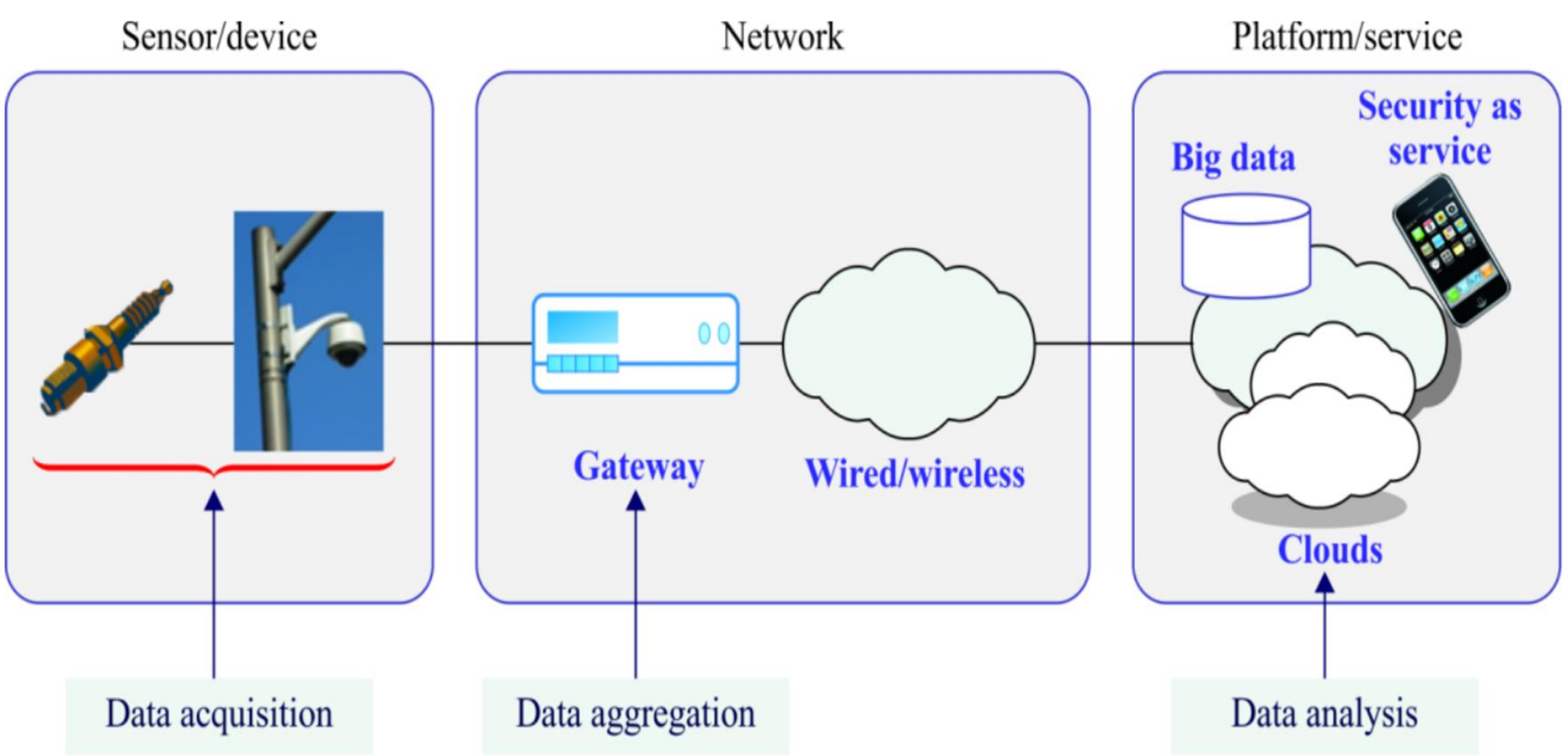


Figure 1 – IoT functional architecture (simplified)

脅威

8 Security threats to the Internet of things

8.1 Security threats to IoT sensors/devices

Sensor/device-specific threats:

– Device capture: Refers to a

機器の盗難、鍵の紛失

its keys lost.

– Sinkhole attack: Refers to an attack in which a compromised device attracts communication traffic to form a black hole or introduce selective forwarding. In a sinkhole attack, an intruder compromises a device or i

シンクホール攻撃：トラヒックを別のルートに流す攻撃

launch a sinkhole attack. neighbouring nodes based achieved, the compromised device will launch an attack. Sinkhole attacks are a type of network-layer attack where a compromised device sends fake routing information to its neighbours to attract network traffic to itself. Due to ad hoc networks and the many-to-one communication patterns of wireless networks where many nodes send data to a single base station, wireless networks are particularly vulnerable to sinkhole attacks. Based on communication flows in a wireless network, a sinkhole does not need to target all nodes in the networ

Sybil攻撃：攻撃者が複数のアカウント、ノード、コンピュータを作ってネットワークを支配しようとする攻撃

– Sybil attac ble identities. ck

International Telecommunication Union

要求事項

ITU-T Y.2066

(06/2014)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

---

Common requirements of the Internet of things

要求事項：目次

8.8 セキュリティとプライバシー要件

- 通信セキュリティ
- データ管理セキュリティ
- サービスプロビジョニングセキュリティ
- ポリシー統合と技術
- 相互認証・認可
- セキュリティ監査

10.3 Security capabilities for gateways

セキュリティ能力の例

The gateway should include:

- an intrusion detection system (IDS)/intrusion prevention system (IPS) capability;
- a key management capability;
- a capability for performing secure configuration;
- a cryptographic algorithm negotiation capability;
- a capability to encrypt data and in some cases signalling, control and management plane data with IoT devices and components in the data center to mitigate the security concerns to confidentiality of data transmitted through wireless networks;
- an integrity capability of data transmitted through wireless networks by using appropriate integrity protection schemes to provide assurances that user data or signalling, control or management data has not been tampered with or altered;
- an availability capability to handle DoS attacks ranging from using secure source coding techniques, source code analysis testing and vulnerability testing, to using a network or host-based IDS/IPS;
- an authentication capability of the origin of the data or of identities of the IoT sensors/devices and of administrators and maintenance personnel of the sensor networks;
- an access control capability to ensure that only authorized personnel or devices are allowed

X.1367 : Standard format for Internet of things (IoT) error logs for security incident operations

スコープ：

本勧告は、エッジデバイスが発行するエラーログ情報を標準エラーログ形式に変換するために、 syslog [b-IETF RFC 5424] などのプロトコルペイロードに配置できる Internet of Things (IoT) エラーログの標準エラー形式を規定する。

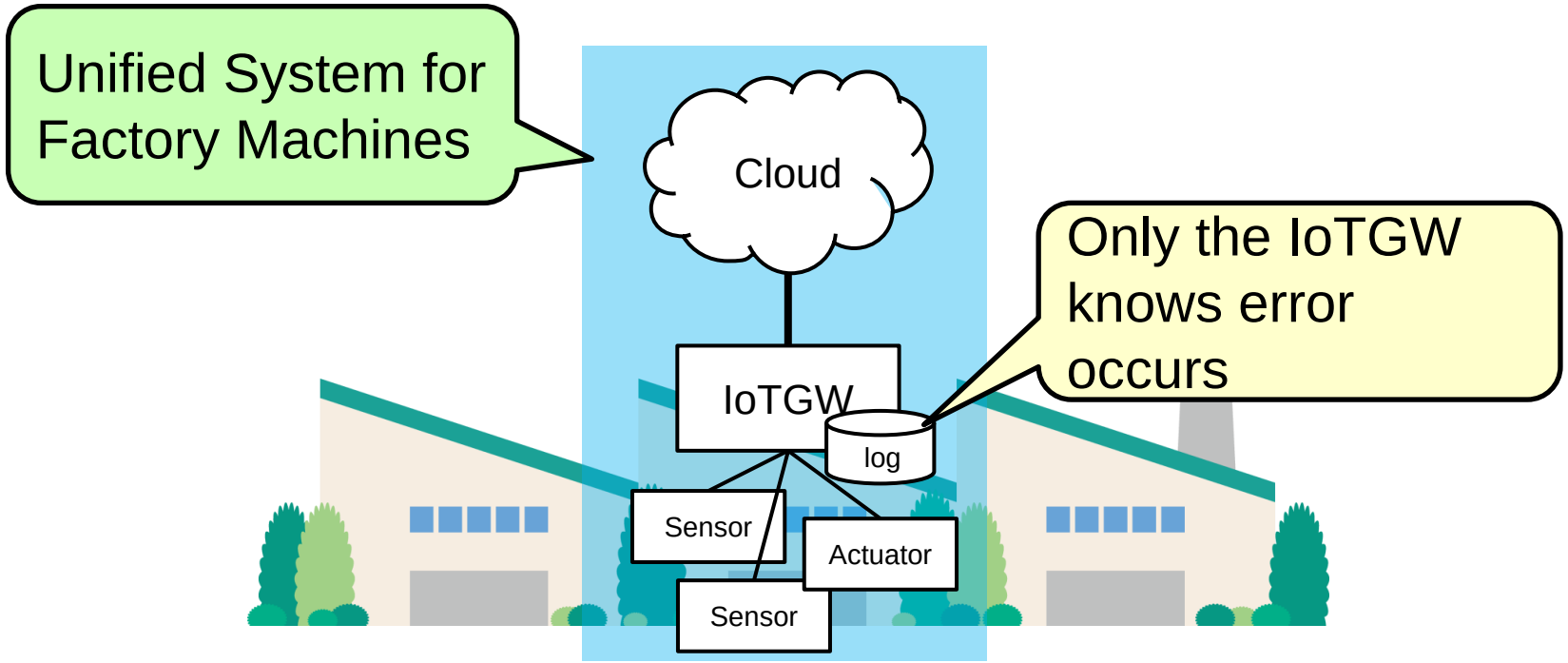
この勧告はまた、エッジデバイスメーカー間のエラーコードの互換性の欠如を解決するために、標準化されたエラーコードテーブルを規定する。この勧告は、エッジデバイスの製造業者間のエラーコードの互換性の欠如を解決するために、標準化されたエラーコードテーブルも規定している。その結果、コンピュータネットワークやIoTエッジデバイスのネットワークにおけるセキュリティインシデント ネットワークとIoT エッジデバイスのネットワークを統合的に管理することができる。

本勧告は、JNSAからの提案

提案の背景
Multiple IoT eco systemsへの流れ(0)

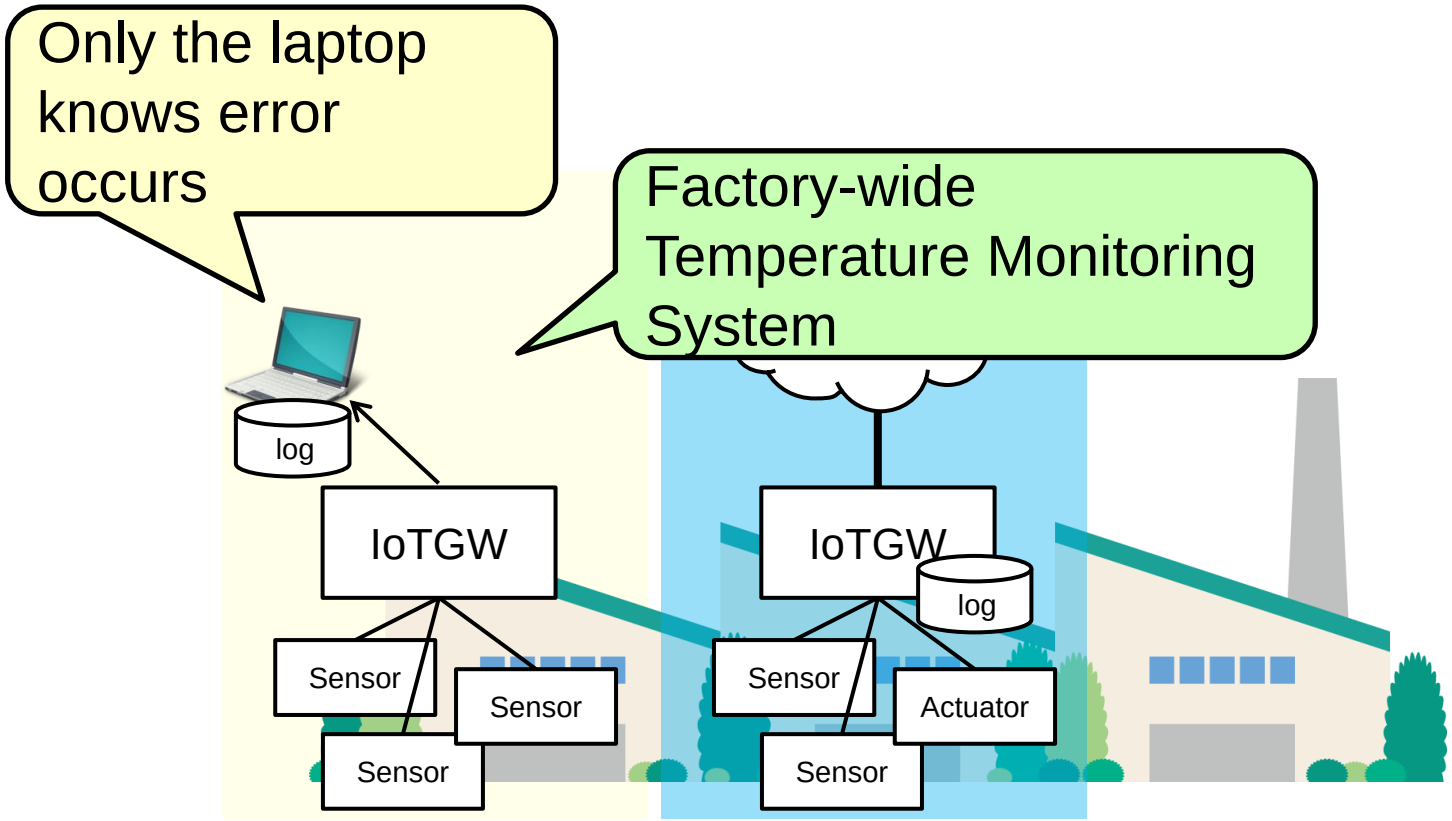
提案の背景
Multiple IoT eco systemsへの流れ(1)

- First IoT eco system is installed



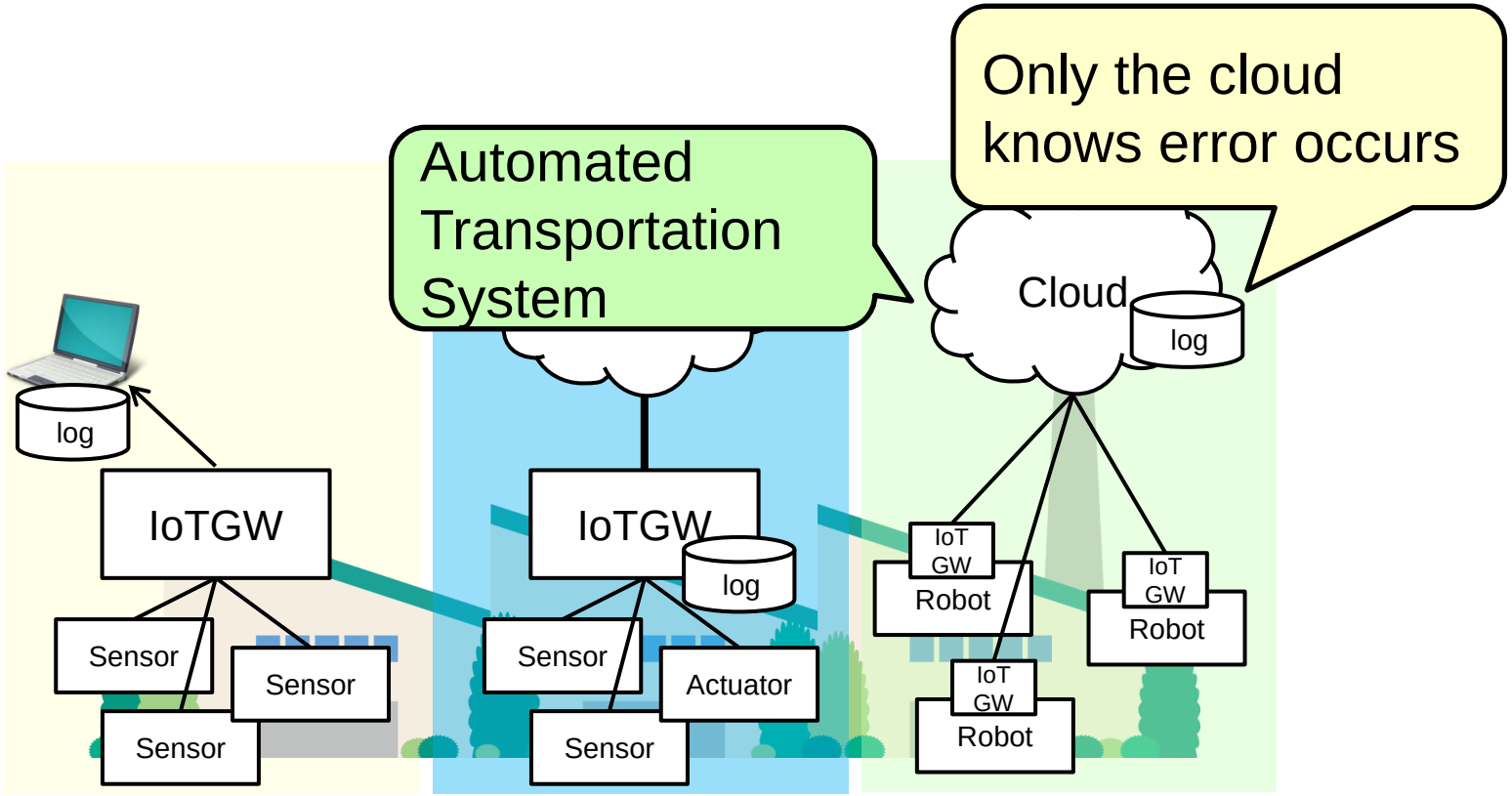
提案の背景
Multiple IoT eco systemsへの流れ(2)

- First IoT eco system is installed
- Second IoT eco system is installed



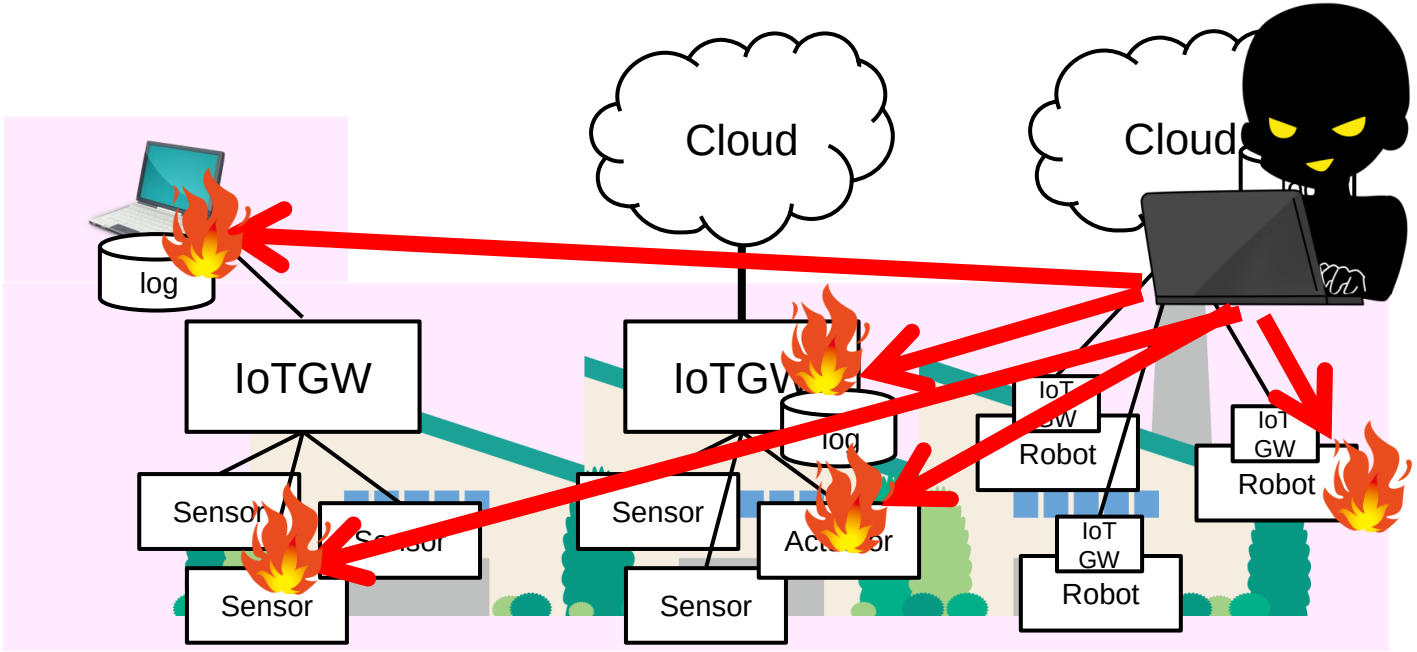
提案の背景
Multiple IoT eco systemsへの流れ(3)

- First IoT eco system is installed
- Second IoT eco system is installed
- Third IoT eco system is installed



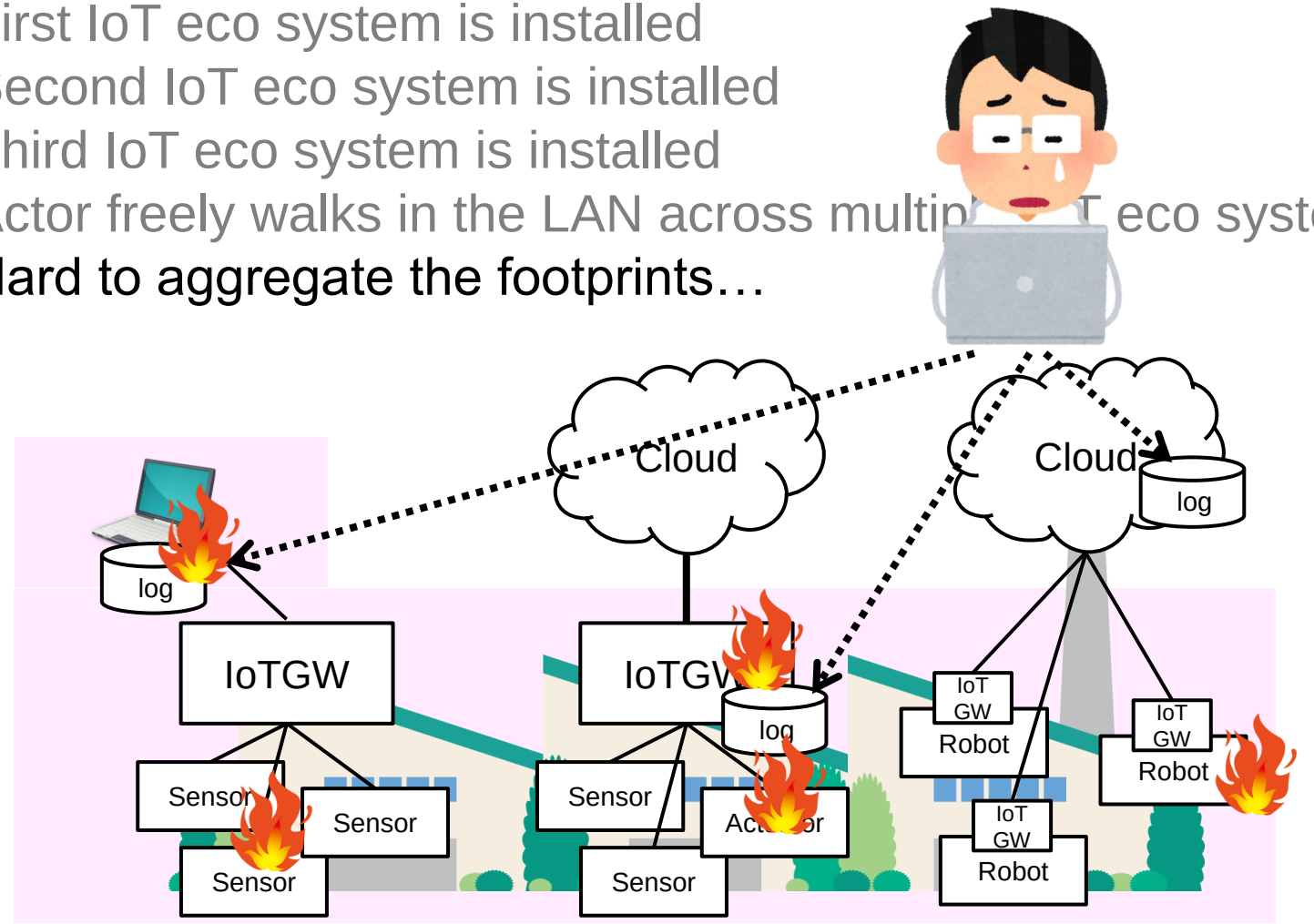
提案の背景
Multiple IoT eco systemsへの流れ(4)

- First IoT eco system is installed
- Second IoT eco system is installed
- Third IoT eco system is installed
- Actor freely walks in the LAN across multiple IoT eco systems



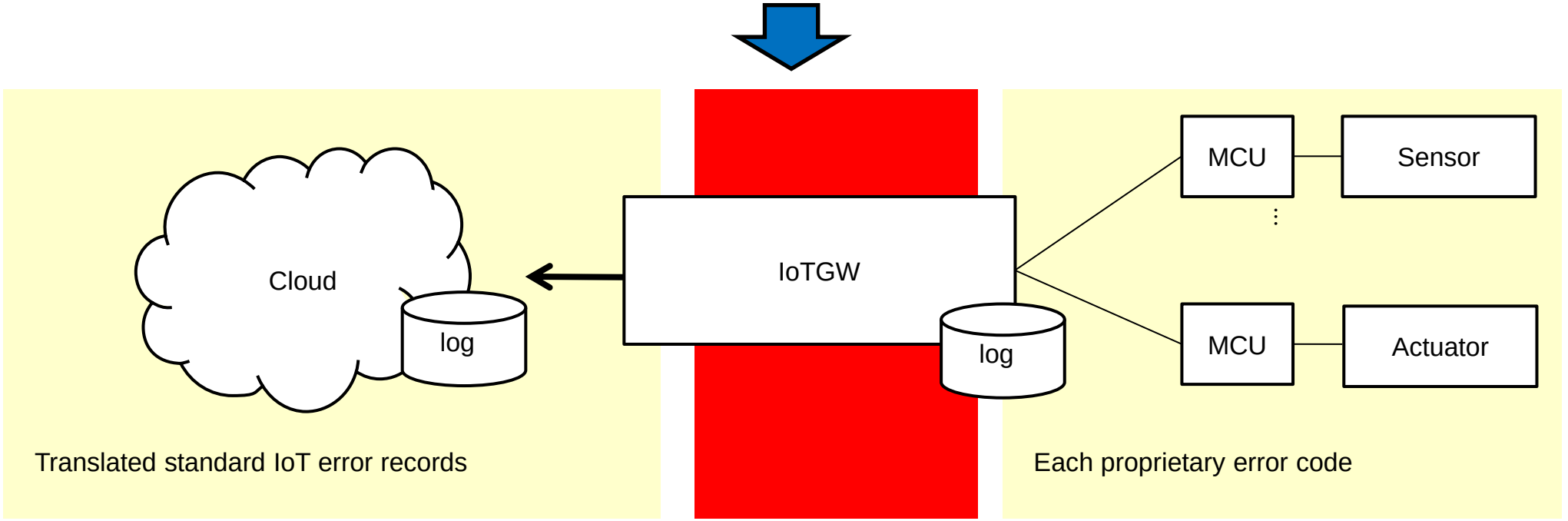
提案の背景
Multiple IoT eco systemsへの流れ(5)

- First IoT eco system is installed
- Second IoT eco system is installed
- Third IoT eco system is installed
- Actor freely walks in the LAN across multiple IoT eco system
- Hard to aggregate the footprints…



「IoTシステムにおけるセキュリティログをどのように扱うか」を解決する勧告化提案

- IoT-GWがIoTエッジ機器からエラーコードを収集する
- IoT-GWが、それぞれのエラーコードをJSONかXMLのエラーコードに統一的に変換する
- IoT-GWは、共通的なエラーコードを他システムと共有することが可能となる



Error code and error message

(This annex forms an integral part of this Recommendation.)

Error code and error message are specified in Table A.1.

エラーコードのイメージ

Table A.1 – Error code and error message

Code	Message	Description
	No Error (0x00-0x0F)	
0x00	No Error	No error occurs.
	Communication (0x10-0x1F)	
0x10	No Response	No response even though the request requires any responses.
0x11	Communication Failed	Some problems for failing communication.
0x12	Link Down	A network interface link is down.
0x1E	Extended Reasons	Prefix code for extended reasons.
0x1F	Other Communication Reasons	Other reasons related to communication.
	Security (0x20-0x2F)	
0x20	Authentication Failed	Some problems of the authentication.
0x21	Certification Failed	Some problems of the certification.
0x22	Encryption Failed	Some problems of the encryption.
0x23	Authorization Failed	Some problems of the authorization.
0x2E	Extended Reasons	Prefix code for extended reasons.
0x2F	Other Security Reasons	Other reasons related to the authentication, the certification, the encryption or the authorization

X.1368：Secure firmware or software update for Internet of things devices

スコープ：
本勧告は、この勧告では、ファームウェアまたはソフトウェア（FW/SW）を安全に更新するための基本的なモデルおよび手順を規定する。
また、IoT の FW/SW の更新に関する要件と能力についても記述している。
本勧告は、FW の更新に焦点を当てるが、IoT 機器の他のあらゆる SW の更新に適用可能である。

連携：[b-IETF suit] IETF (2021). Software updates for the internet of things (suit), version 7.26.0. [viewed 2021- 02-19] at: https://datatracker.ietf.org/wg/suit/about/

X.1388 目次

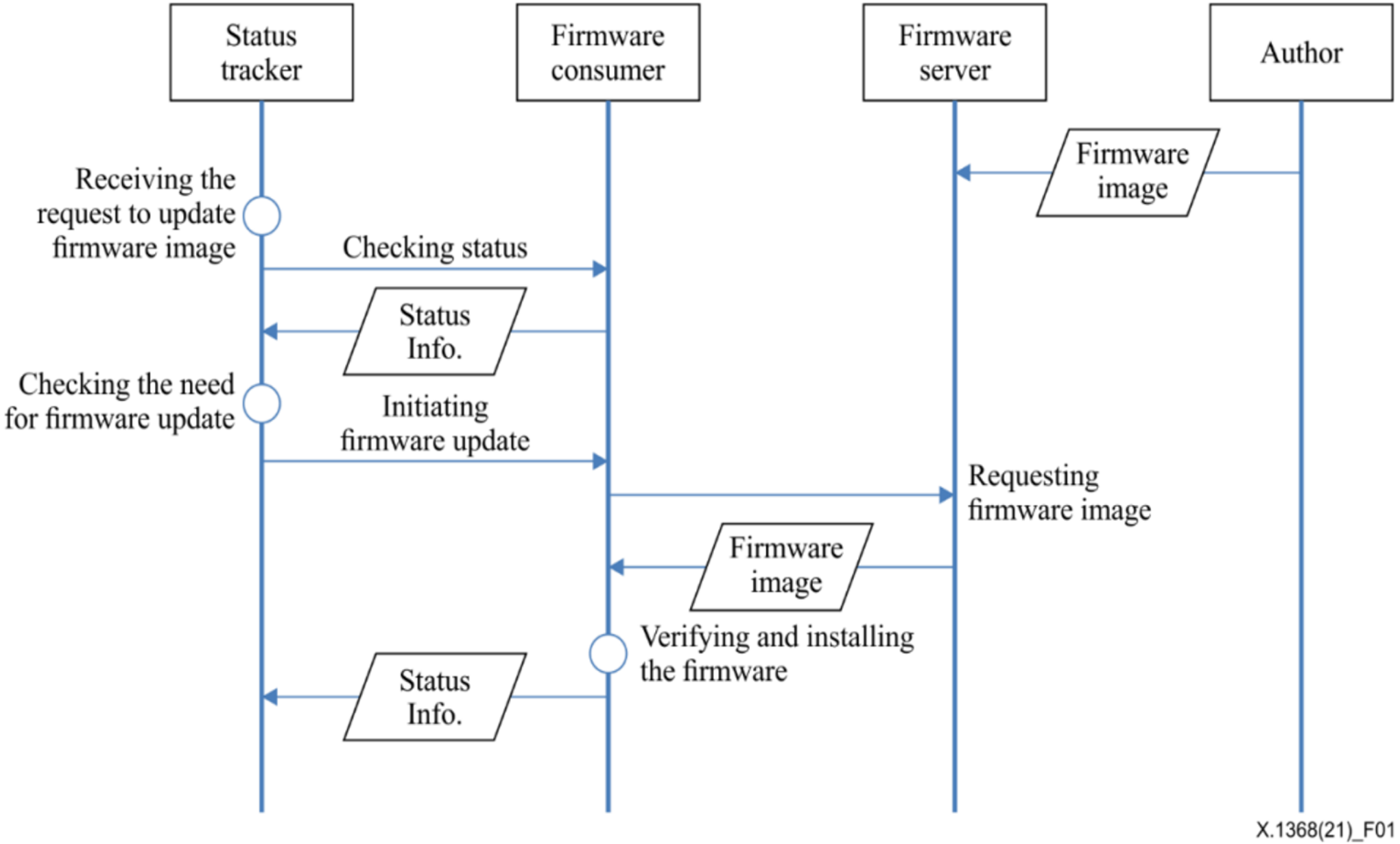


Figure 1 – Protocol procedure

TR.ba-iot: Broadcast authentication scheme for IoT system

スコープ：
本TR（技術文書）では、BA（Broadcast Authentication）システムの対象となる任意のIoT機器の部分集合を指定し、IoT機器を安全に制御するためのコマンドを放送することで、安全な遠隔操作システムを実現する放送認証のスキームを提供する。

TR化への背景：
本内容は、「勧告化」を想定した提案を実施していたが、米国からの提案で、「内容が技術的過ぎるため、技術文書と当面して検討を進め、内容の精査を途中段階で実施し、必要があれば、勧告に切り替えるべき」との提案があり、それが合意された。

Broadcast Authentication Scheme for IoT System

Junji Shikata, Yokohama National University, Japan (invited expert)

Koji Nakao, NICT, Japan

Proposal: Broadcast authentication scheme

Proposed scheme

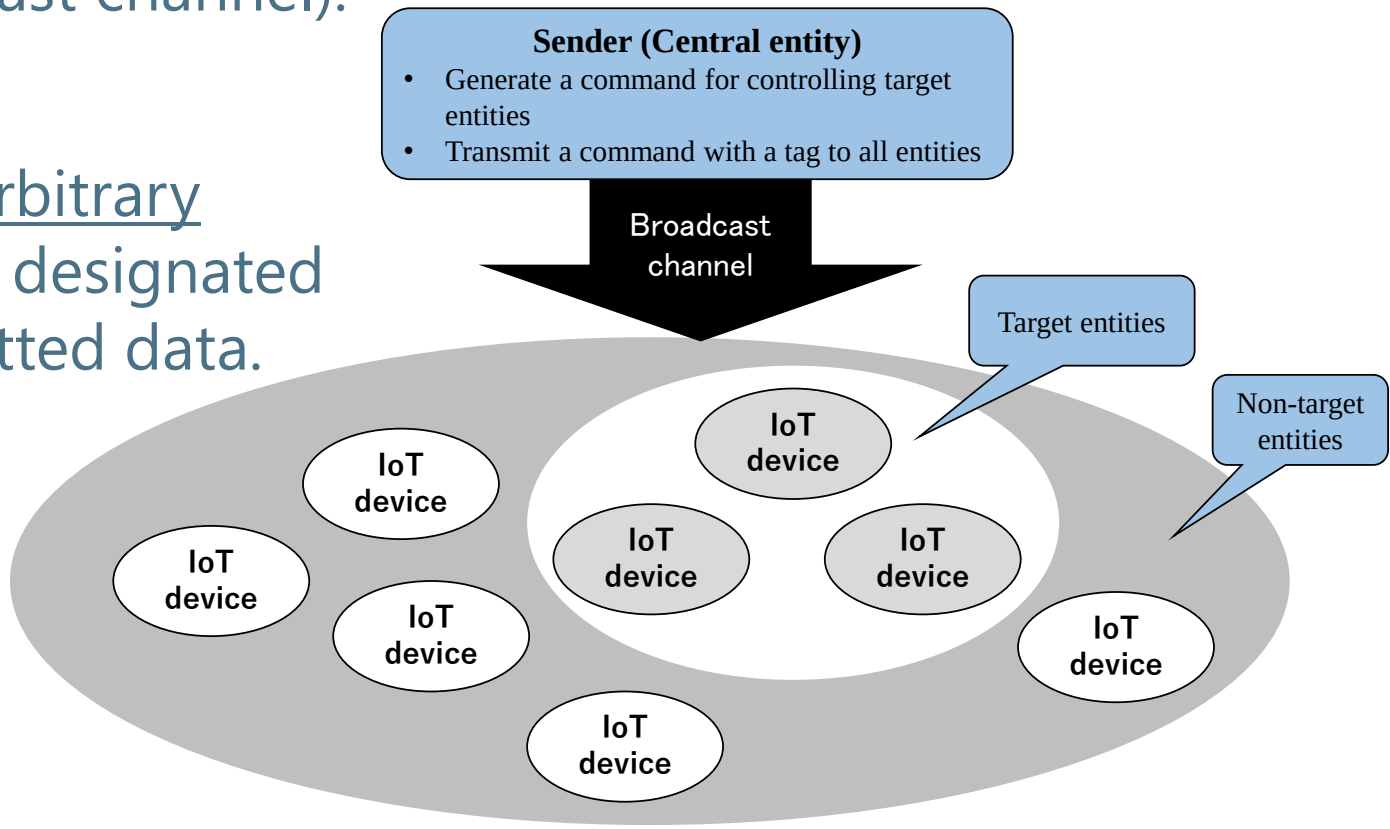
A central entity (i.e., a sender) remotely and simultaneously can control many and arbitrary target entities (i.e., IoT devices) via a one-to-many communication channel (i.e., broadcast channel).

Feature of the scheme

- Allow the sender to designate an arbitrary subset of receivers so that only the designated receivers check integrity of transmitted data.

Security

- Completeness
- Integrity
- Anonymity (optional)



Constructions of (Anonymous) BA

- MAC-based Anonymous BA Construction
- DS-based Non-Anonymous BA Construction

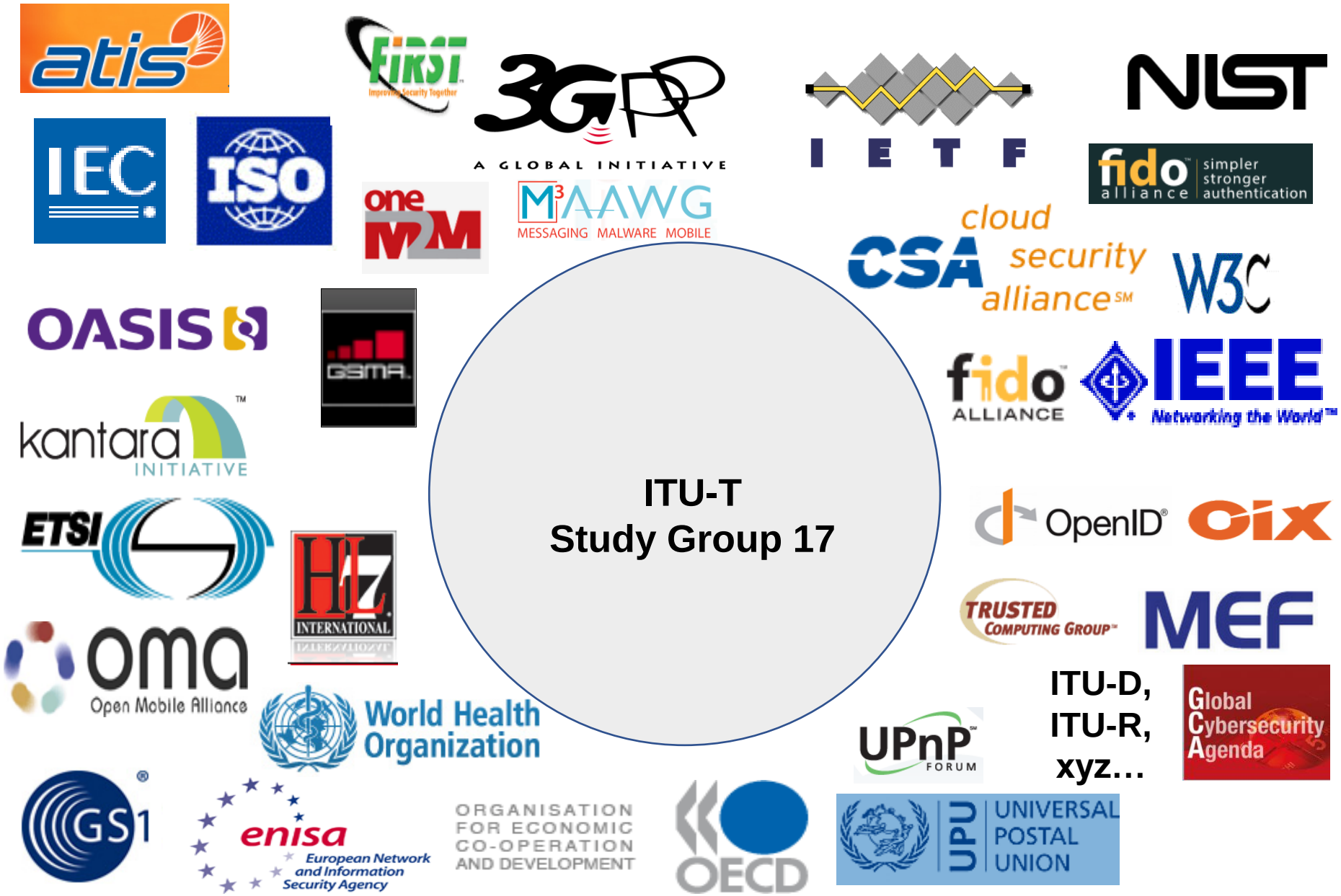
[Note] MAC: Message Authentication Code

DS: Digital Signature scheme

Construction	Security	Features
MAC-based Anonymous BA Construction	Completeness Integrity Anonymity	効率的な実行が可能だが、データサイズは制御対象機器の数に比例する
DS-based Non-Anonymous BA Construction	Completeness Integrity	データサイズが被制御機器数に依存せず、データサイズ圧縮率と制御時の誤検知確率（非対象機器がコマンドを受け付ける可能性）のトレードオフが可能なため、柔軟なパラメータ設定が可能。

Completeness（完全性）：証明者の主張が真であるならば、検証者はその主張の正しさを高確率で検証できること

ITU-T SG17が連携している標準化関連団体



ITU-T SG 20

Internet of things (IoT) and smart cities and communities (SC&C)

SG 20の概要

- ITU-T SG20は、IoTとそのアプリケーション、およびスマートシティとコミュニティの実装に共通に合意されたガイダンスを提供するITU-T勧告を策定する。SG20の活動は、IoT、デジタルツイン、人工知能などの分野のソリューションによって実現される都市部と農村部の両方におけるデジタルトランスフォーメーションをサポートする。
- SG20が開発する標準規格は、IoTの協調的な展開を可能にし、相互運用性、ビッグデータ、さまざまなIoTシステムをサポートするためのアーキテクチャのフレームワークと要件に関連するIoT実装の課題に対応する。また、IoT導入の要件を定めるSG20標準は、スマートシティやコミュニティがIoTシステムやスマートシティプラットフォームの効率を高め、データのサイロ化を解消し、さまざまな業種間でのシームレスなデータ共有を促進し、データ処理・管理能力を向上させるのに役立つ。
- IoTやスマートシティ、コミュニティの標準化作業をより円滑に進めるため、SG20はIoTやスマートシティ、コミュニティの共通用語について、すべての関係者と緊密に連携して取り組んでいる。SG20規格は、スマートシティとコミュニティがIoTの最新のセキュリティとプライバシー要件を満たすのを支援する。・・・

まとめ

- ITU-T SG17は、ITU全体の中で「セキュリティ」の勧告化を推進している唯一の検討グループであり、他の国際規格化団体などとの連携を進めている。（SG間は。。。）
- 特に、セキュリティの枠組み、要求事項、ユースケースや応用に特化したセキュリティ技術の検討を推進している。
- ISOよりハードルは低く、提案内容を規格化しやすいと評価できるが、最近の多様な新課題の提案にチェックをかけるため、新規課題の成立については、そのReviewが強化されている。
- 近年、多くの女性参加者も増加しており（特に中国から）、広い世代の専門家が集まりつつある。

SAFE :
Security is Absolutely First Everywhere

Thank you very much
for your attention!