KDDI Research

通信分野におけるセキュリティ標準化

2020年3月31日

株式会社KDDI総合研究所

三宅　優

目次

1. セキュリティ標準化の特徴と今後の方向性

セキュリティを取り扱う標準化団体（通信関連）

KDDI Research

分野	団体名	活動内容
ネットワーク	IEEE802	LAN/MANに関わるネットワークプロトコルとそのセキュリティ対策
	IETF	インターネットに関連するプロトコルのセキュリティ対策・機能、セキュリティプロトコル
	ITU-T	PKI、脆弱性情報管理、サイバーセキュリティ、スパム対策、セキュリティ管理、セキュリティ・アーキテクチャ、ID管理、ITSセキュリティ、DLTセキュリティ
	ETSI	サイバーセキュリティ、モバイルセキュリティ（3GPPと連携）
	3GPP	モバイル通信におけるセキュリティ対策のためのプロトコル、機能
	GSMA	（業界団体）　モバイルセキュリティに関するガイドライン作成、脆弱性情報・対策
セキュリティ全般	ISO/IEC JTC1	暗号、セキュリティ管理、サイバーセキュリティ、ID管理、プライバシー対策、ICカード、バイオメトリクス
認証系、Web系	OASIS	認証・認可方式（SAML/XACML）、サイバー脅威情報の交換（STIX/TAXII）
	FIDO	生体認証を含む多要素認証、パスワードレス認証方式
	Open ID Foundation	OpenIDに関わる認証・認可方式の仕様策定、普及促進
	W3C	Web認証、アプリケーションセキュリティ、Web支払い、プライバシー

セキュリティ標準化の項目と特性（通信分野）

KDDI Research

対象項目	実施内容	標準化状況、展開状況
暗号	公開鍵暗号アルゴリズム、共通鍵暗号アルゴリズム	NIST（米国）とISO/IEC JTC1 SC27が中心的に活動。現在は、ポスト量子コンピュータ暗号の検討が進められている。安全性の評価が重要。
セキュリティ管理	ISMS、情報セキュリティ管理、ITセキュリティ評価基準等	ISO/IEC JTC1 SC27が中心的。ITU-T SG17では通信事業者向けISMSを策定。ISMSは、日本では広く利用されている。
プロトコルに対するセキュリティ	インターネットや通信システムで使用されるセキュリティ対策	DNS、BGPのセキュリティ対策等、プロトコルに使用に応じてセキュリティ機能を追加する。方式が標準化されても普及に時間を要することがある。
セキュリティプロトコル	他の通信プロトコルによる通信に対して、暗号化による通信路を提供するもの	SSL/TLS、IPsec等が標準化され、HTTP、メール等の通信の暗号化が可能となっている。アプリレベルで対応する必要はあるが、比較的対応しやすく、広く利用されている。
サイバーセキュリティ対策	脆弱性管理、DDoS攻撃対策、スパムメール対策、等	ITU-Tで脆弱性情報に関する他団体の仕様を順次勧告化した。サイバー攻撃に対して連携するための標準化作成の要望は多く、実現や展開に向けた課題を解決していくことが必要。
認証・認可	認証強化、認証連携、機能追加が行われている	フォーラム系が主体となって標準化が進められている分野。攻撃者に狙われやすく、安全性の強化は常に必要。
ガイドライン	通信システムやサービスのためのセキュリティ対策の指針として作成	GSMA（モバイルシステム）やITU-T SG17（通信機能に対するセキュリティガイドライン）を策定中。対応が必須となっているわけではないので、利用するかどうかは事業者次第。

セキュリティ標準化作業の分類

種類	例	活用状況
セキュリティ機能を中心としたもので共通化が必要なもの	• 暗号アルゴリズム • 認証／認可プロトコル • ICカード	目的・必要性が明確で、広く利用されている
システム、プロトコルを安全にするための仕組み	• 通信プロトコルのセキュリティ対策 • セキュリティアーキテクチャ	既に普及したものに対する対策は導入が進まない可能性あり
セキュリティの取り組みに対する認定（認証）	• ISMS • Common Criteria • 暗号モジュール試験	普及の度合いは、国や分野により違いが大きい
サイバー攻撃対策	• 脆弱性情報管理 • 技術的な攻撃防御対策 • 導入／運用ガイドライン	脆弱性情報管理については広く利用されているが、費用対効果の点から利用が進まない面がある

セキュリティ標準化の課題

KDDI Research

セキュリティ標準化において指摘されるポイント

1.セキュリティの重要性は理解されつつも、セキュリティ機能導入のモチベーションが低い

- セキュリティ機能が無くてもシステム、サービスは動く
- セキュリティ対策にはコストがかかる（費用対効果が分かりにくい）

2.セキュリティが中心となる取り組みでは注目を集めにくい

- システム、サービスをサポートするための仕組みを提供（セキュリティが主役でない）
- 必要な取り組みであるが、新たなマーケットを創出したり、世間から注目を集めることが難しい

3.標準化のタイミングが難しい

- 攻撃のトレンドに応じて必要とされる標準化技術が推移する
- 対抗する取り組みに対して公開する情報の制御が必要となる場合がある

4.各国の政策的な意向を考慮する必要がある

- サイバーセキュリティ関連は、対策の必要性を共有しつつも、情報共有や国際連携を想定した取り組みは各国の考え方やポリシーの違いもあり慎重に検討
- プライバシー関連は、各国・地域の規制が異なる中で、パーソナル情報を扱う企業がそれぞれに対応中

セキュリティ標準化（通信分野）を活性化させるための方向性

KDDI Research

対象例	特徴	方向性
認証・認可プロトコル、暗号	• ニーズがあり広く利用されることが期待される	• サービスの発展や攻撃手法の高度化に応じた取り組みを推進 • 新たな機能でマーケット創出（認証ハードウェア、バイオメトリクス、暗号モジュール、等）
インターネットプロトコルのセキュリティ、通信インフラのセキュリティ	• 現在はセキュリティは必須と考えられているが、取り組みは後回しになる場合もあり	• 他の分野の標準化担当者との交流拡大 • エキスパートの育成
サイバー攻撃対策	• ITUでは途上国からの要望が高い • 標準化の世界では脆弱性管理が中心	• 日本の取り組み（CCC、Active、PRACTICE、ICT-ISAC 情報共有基盤、NOTICE、等）のノウハウ活用、展開 • 主要インフラ分野の脆弱性情報管理の促進
セキュリティレベルの保証	• お墨付きのために利用される • 各種分野あり	• サプライチェーン・セキュリティの必要性に対応 • IoT機器等のセキュリティ基準のように国や分野でそれぞれ検討されているものは、国際標準化が必要
セキュリティレベルの確保、セキュリティ対策指針	• サービスやシステムを開発、運用するための仕様外のセキュリティ対応	• 多機能化、複雑化するシステムのセキュリティ指針としてのガイドライン作成 • ガイドライン活用のための方策の検討
パーソナル情報制御	• パーソナル情報の収集が進む中で各国の基準にも対応した情報管理が求められている	• パーソナル情報を利用したサービス分野の確立と活性化 • パーソナル情報を抱えるプラットフォーマへの対抗

【参考】今後注力すべきセキュリティ標準化分野

項目	方向性	標準化項目（案）
認証、ID管理	• 個人認証の高機能化 • IoTデバイス等のID・認証 • トラスト技術の展開	• 認証高度化、自動化 • デバイスID認証基盤 • トラスト関連技術とその応用の標準化
暗号	• 量子暗号通信 • 耐量子コンピュータ暗号 • 超高速、低遅延アプリ向け	• 量子暗号通信の応用 • 耐量子コンピュータ暗号アルゴリズム • 特殊用途向け暗号アルゴリズム（準同形暗号、秘密分散、等）
通信インフラ	• 新機能機能に対応 • 通信機器、デバイスの安全性対応	• 5Gセキュリティ • Beyond 5G/6Gセキュリティ • サプライチェーン・セキュリティ • 通信機器・デバイス　セキュリティガイドライン
サイバーセキュリティ対策	• 脆弱性、インシデント情報管理 • 運用、管理の強化	• セキュリティ体制ガイドライン • 通信インフラ向けセキュリティガイドライン • セキュリティ情報（IoCや脆弱性情報、ソフトウェア資産情報等）の自動収集・共有・解析基盤 • 運用自動化のセキュリティ
パーソナルデータ管理	• データ利活用の活性化 • 事業者認定制度	• データ流通プラットフォーム • データ利活用事業者のセキュリティ基準 • AIセキュリティ

標準化項目の検討、および、スケジュールについては、各分野の専門家と要協議

（事例）IoTデバイスセキュリティ対策

セキュリティガイドライン（2015年～）

IoT Acceleration Consortium

IoTセキュリティコンソーシアム
総務省・経済産業省（2016年7月）

IoT開発における セキュリティ設計の手引き

IPA（2016年5月）

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS

U.S. DHS（2016年11月）

Baseline Security Recommendations for IoT
in the context of Critical Information Infrastructures

ENISA（2017年11月）

GSMA

GSMA（2016年2月）

IoT Security Guidelines Overview Document
Version 1.0
08 February 2016

国際標準化（2017年～）

ISO/IEC 27030
Guidelines for security and privacy in Internet of Things (IoT)

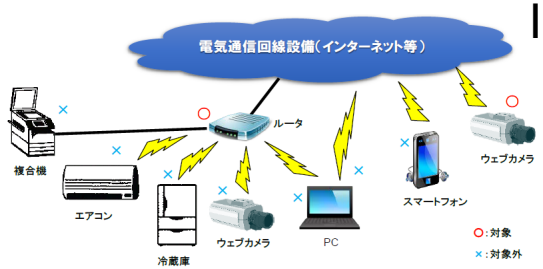
IETF suit
Software Updates for Internet of Things

⇔

ITU-T X. secup-iot
Secure software update for IoT devices

セキュリティ規制（2020年）

英国IoT機器セキュリティ法



IoT技術適合認定（2020年）

?

IoT機器の安全性を高める次のステップは？

民間団体による任意の取組

分野別セキュリティガイドライン（2016年）

CCDS:
重要生活機器連携セキュリティ協議会

- 車載分野
- オープンPOS分野
- 金融端末分野
- IoT-GW分野

セキュリティ認証（2019年）

CCDS 2019 Security Certification

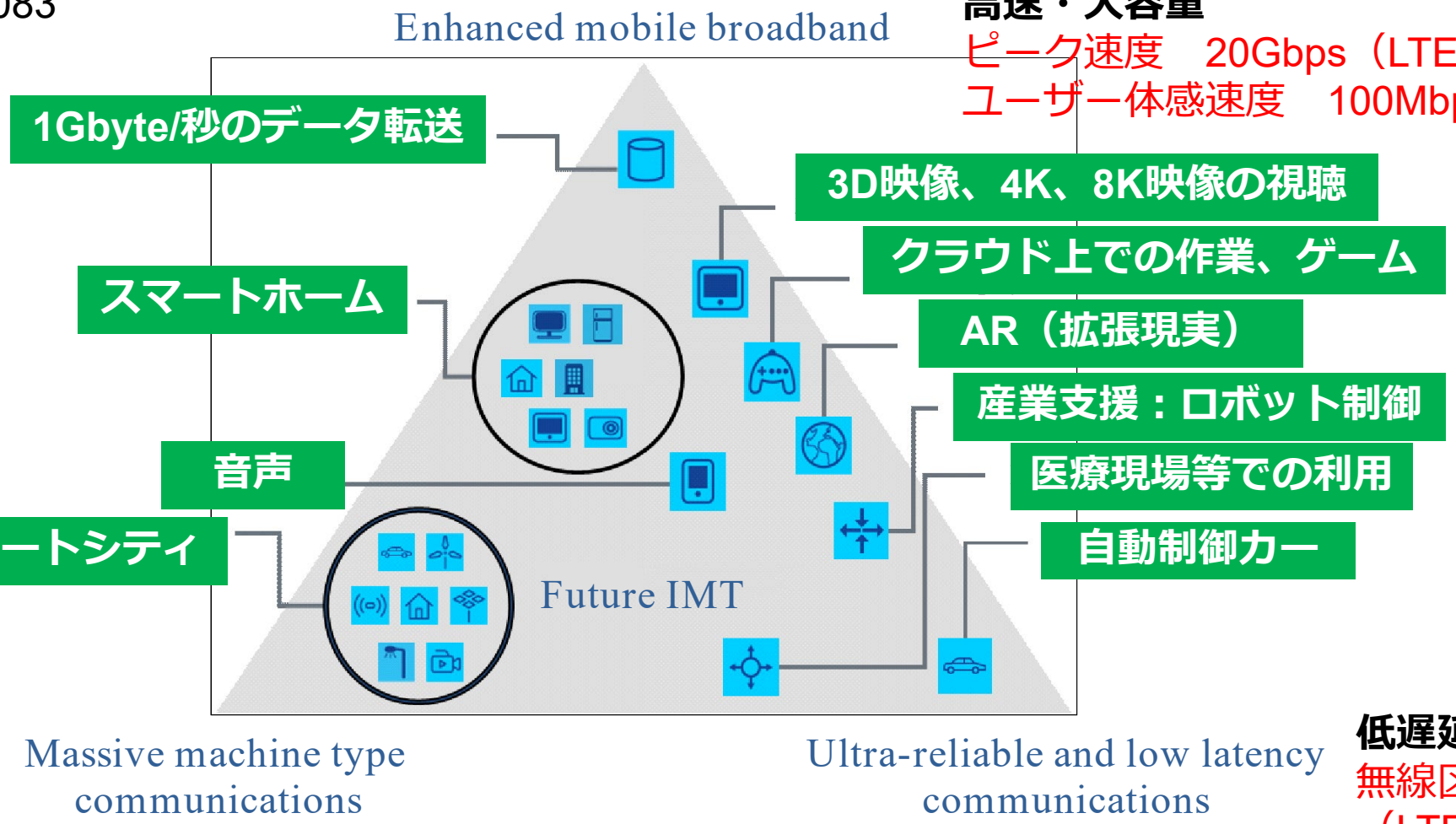
2. 通信分野におけるセキュリティ標準化

通信インフラの移り変わりとセキュリティ

5Gが目指す世界

高速・大容量（eMBB）　多接続（mMTC）　高信頼・低遅延（URLLC）

出展：勧告ITU-R M.2083



高速・大容量
ピーク速度　20Gbps（LTEの20倍）
ユーザー体感速度　100Mbps

多接続
同時接続端末数
100万台/km^2
（LTEの10倍）

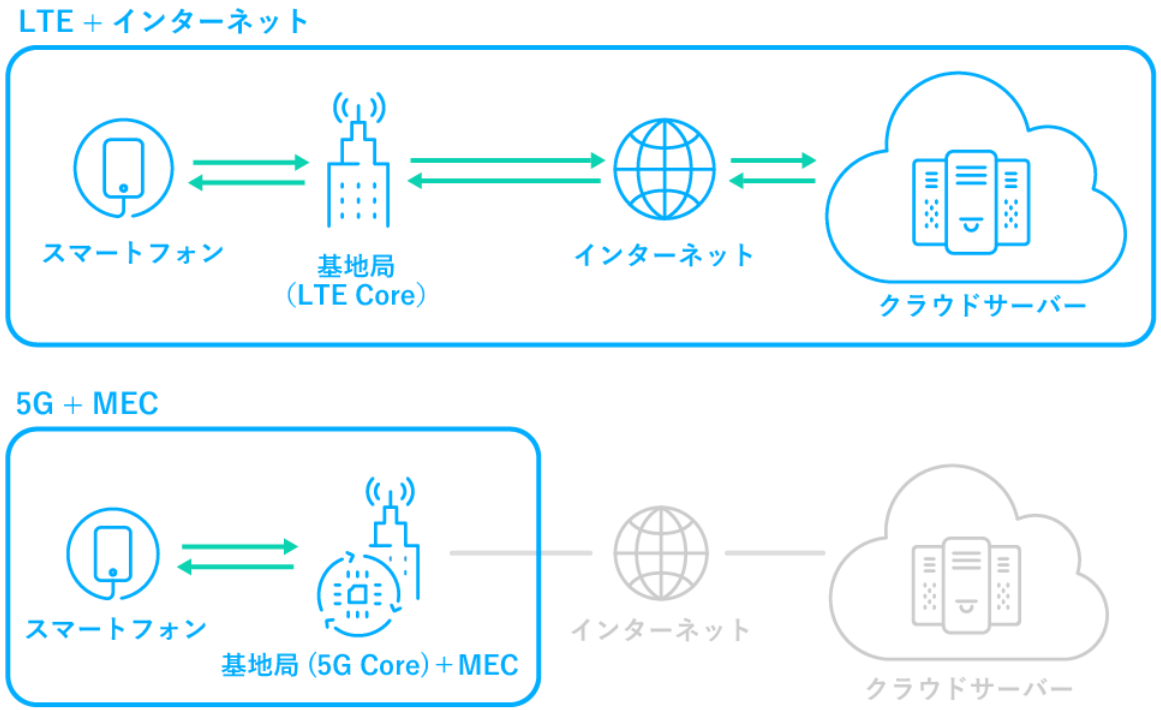
低遅延
無線区間　1ms
（LTEの10分の1）

M.2083-02

通信機能の多様化・複雑化

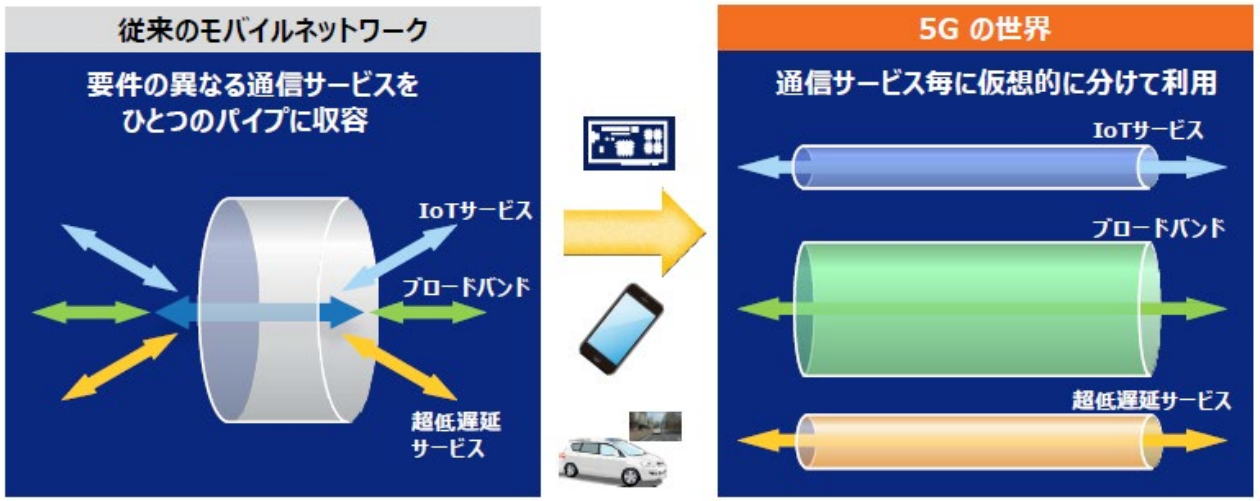
■ MEC (Multi-access dge Computing)

- 端末の近く（エッジ）にサーバを配置し、スマートフォンやIoTデバイスとの通信時間を短縮させるための技術



■ ネットワーク・スライシング

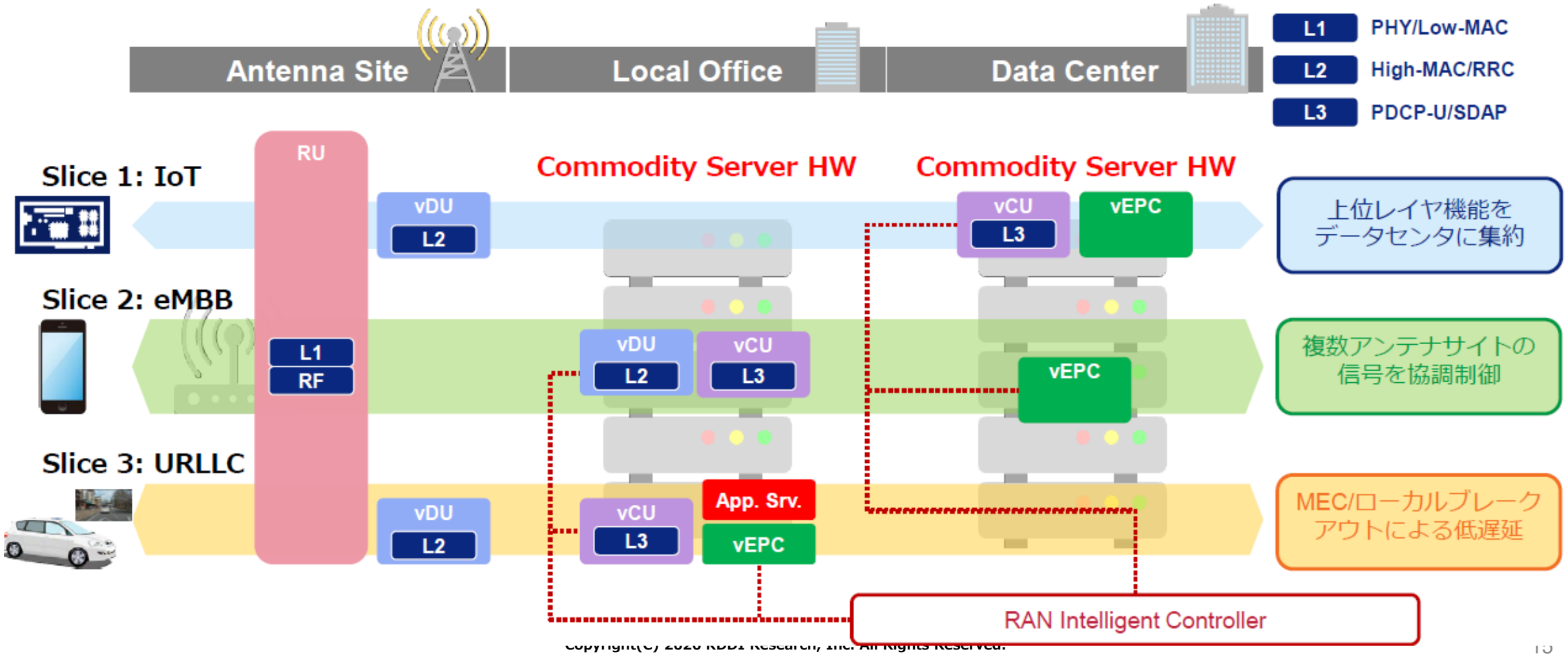
- サービスに応じてオーダーメイドで仮想的なネットワークを提供
- SDN（Software-Defined Networking）、NFV（Network Function Virtualization）等の技術を利用



ネットワークインフラの仮想化

■ 仮想化基地局アーキテクチャ

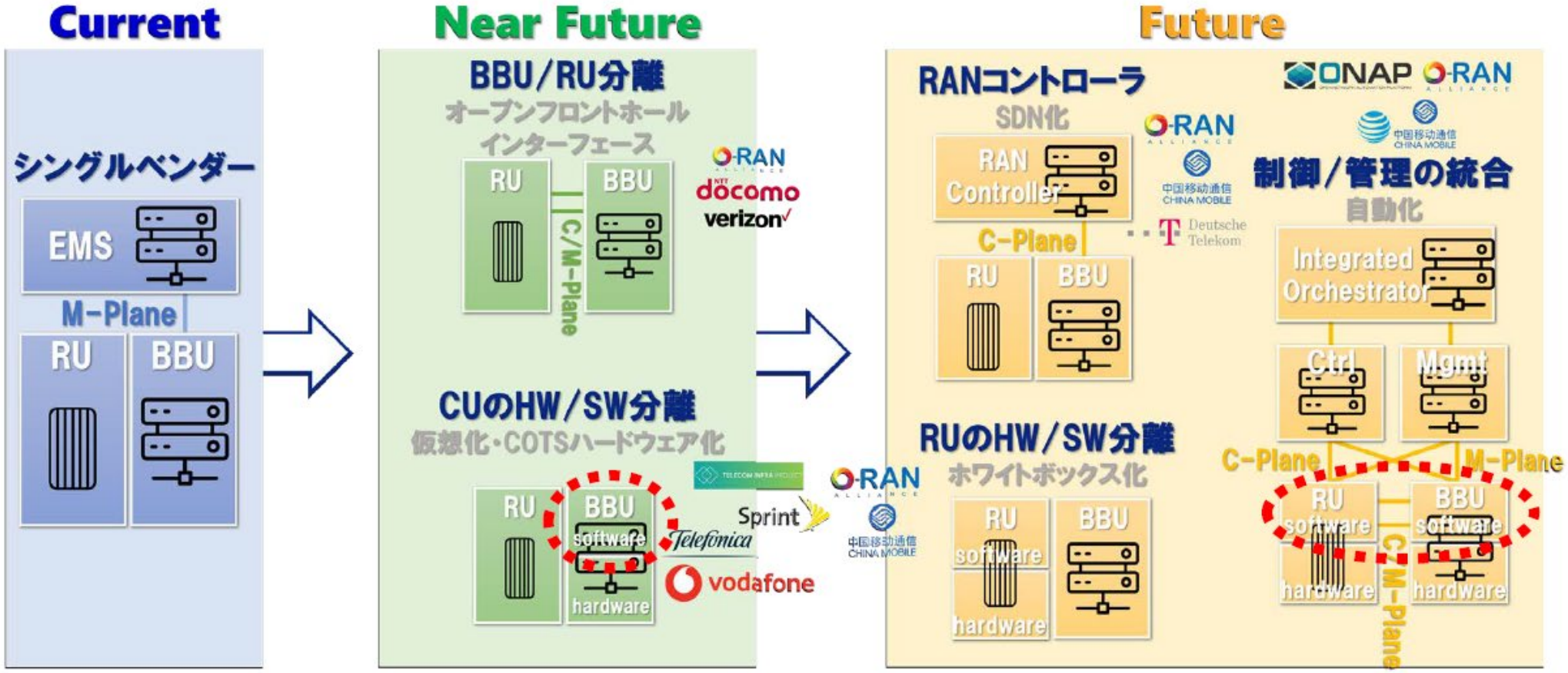
- サービスタイプに応じて基地局機能を配置することにより、論理ネットワーク = スライス を実現



インフラ設備のオープン化

■ 基地局設備（Radio Access Network: RAN）のオープン化

● オープン化・仮想化の流れはクラウド・ネットワークからモバイルまで浸透

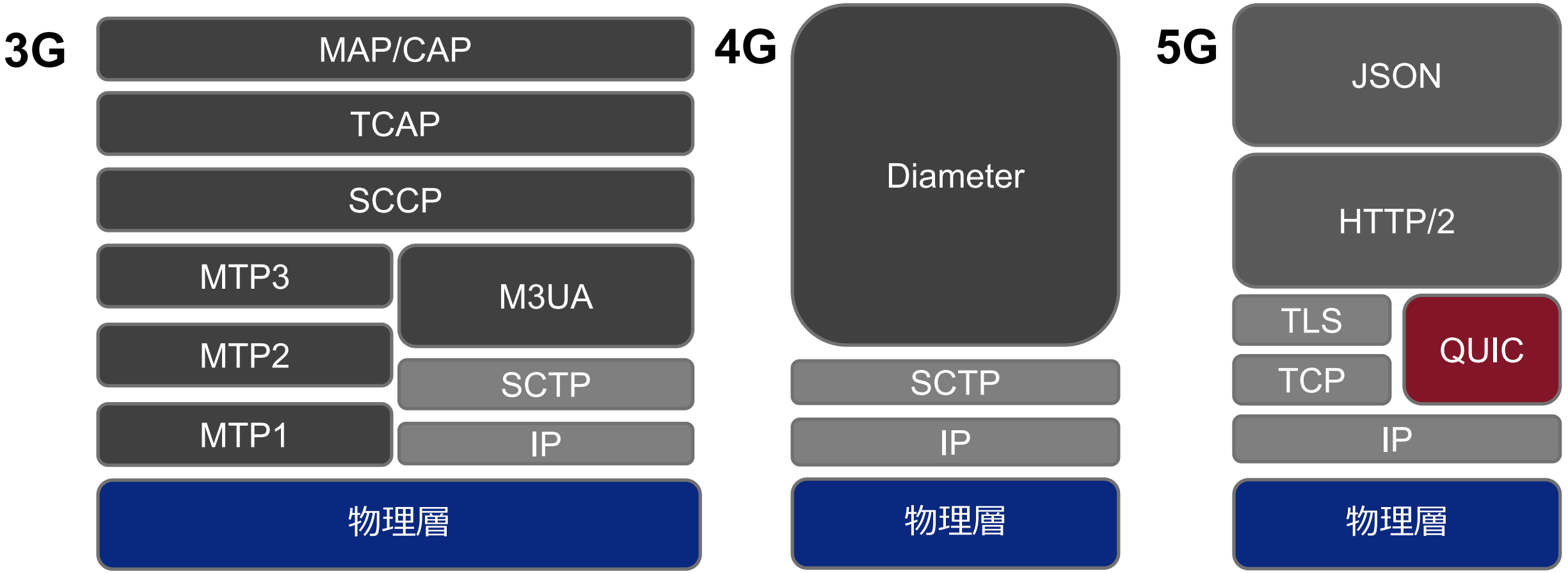


● オープンソースの利用、インタフェースの公開、・・・

汎用プロトコルの利用

■ モバイルネットワークにおけるインターネットプロトコル利用の導入

- 5Gのコアは、SBA（サービスベースアーキテクチャ）の採用により、インターネットベースのプロトコル（HTTPベースのRESTful、JSON）を利用
- 攻撃者にとっては理解しやすいプロトコル、脆弱性の発見も容易になる可能性あり

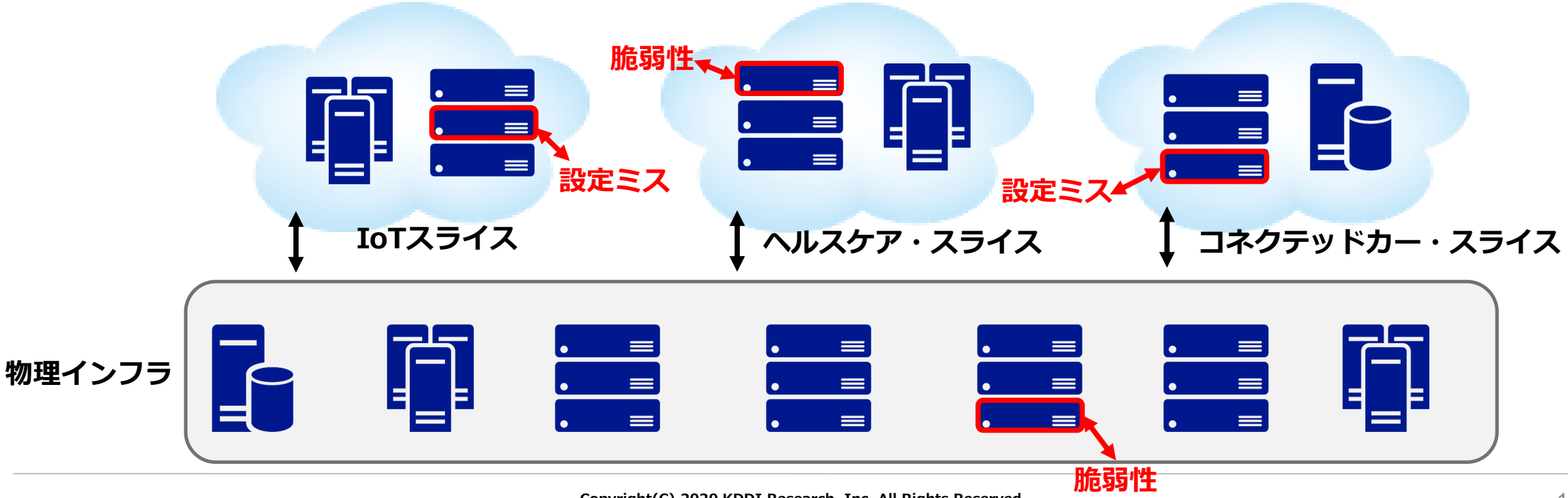


ネットワークの複雑化

- SDN、NFVの導入により、ネットワーク上の機能の追加、ネットワーク構成の変更が容易に
- ネットワークスライシングにより、1つの物理的なネットワーク上に仮想的なネットワークが多数存在

ネットワーク設定の複雑化

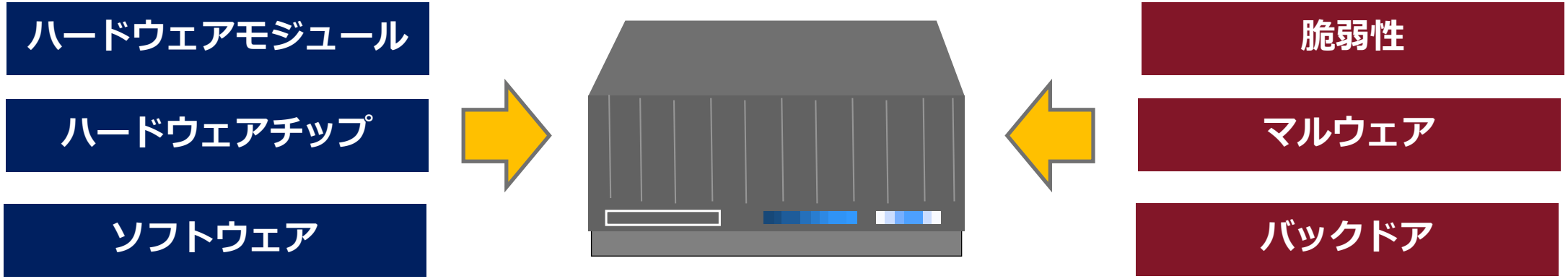
- ネットワークの設定ミス、設定の不整合、脆弱性、等により、攻撃のされるポイントが増加？



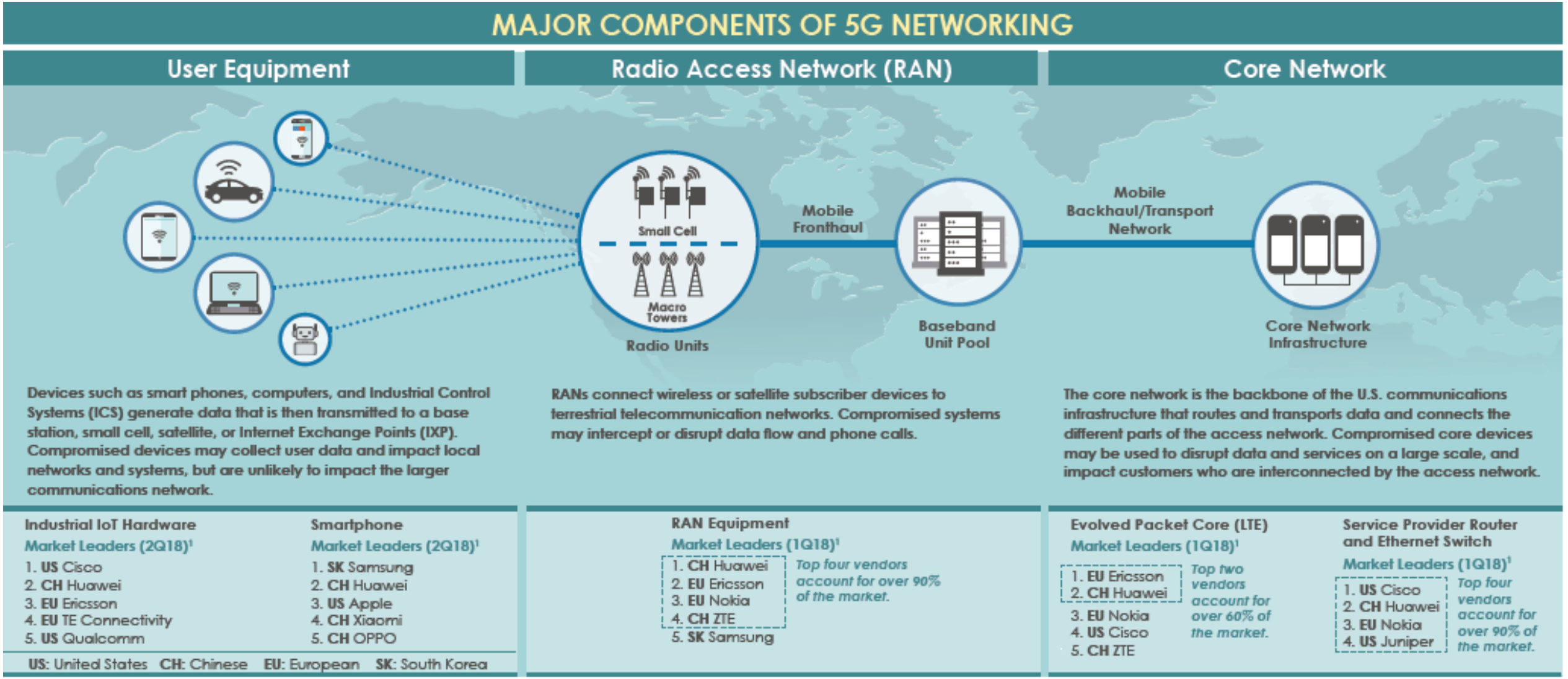
サプライチェーン・リスク

■ サプライチェーン・リスク（内閣サイバーセキュリティセンター　資料より）
- 情報通信機器等の開発や製造過程において、情報の窃取・破壊や、情報システムの停止等の悪意のある機能が組み込まれる懸念
- さらに、納入後においても、情報システムの特徴として、事後的な運用・保守作業により、製造業者等が修正プログラムを適用する等、調達機関が意図しない、不正な変更が行われる可能性

■ ネットワーク機器におけるサプライチェーン・セキュリティ
- ハードウェアが複雑化しするとともに、製造過程で多くの企業が関与
- ネットワーク構築に必要な機器の種類が増大



5Gにおける主要通信機器のシェアの寡占化



米国CISA（Cybersecurity and Infrastructure Security Agency）の資料より

通信インフラの変化によるセキュリティ上の懸念

項目	懸念点
通信機能の多様化	新しい機能の導入の際には仕様上、実装上のセキュリティ脆弱性が発見されやすい。
通信インフラの仮想化	仮想化インフラ自体のセキュリティ対策の強化が必要。通信システムの複雑化による脆弱性管理の複雑化。
インタフェースのオープン化	インタフェース部分の処理の厳格化、セキュリティ対策が必要。
オープンソースの活用	攻撃者がシステムの脆弱性を探しやすくなる。
通信制御機能の外部への公開	信頼関係の確立が必要。監視機能の強化が必要。
汎用プロトコルの利用	攻撃の敷居が下がる。
ネットワークの複雑化	セキュリティ対策が不十分なソフトウェア、ハードウェアが組み込まれる可能性が増える。セキュリティ対策のための機器の導入が難しくなる。攻撃されたことが発見しにくくなる。
サプライチェーン・リスク	品質がばらついたソフトウェア、ハードウェアが製品に使われる可能性がある。

- システム全体的な視点からセキュリティ対策の検討
- セキュリティ対策のガイドライン

次世代通信インフラに向けた
セキュリティ標準化の取り組み

通信インフラの変化に対するセキュリティの取り組み

KDDI Research

■ 課題

- 個々のセキュリティ対策だけではく、全体的な視点からセキュリティ対策が必要
- 事業者ごとにシステム構成が異なることもあり、画一的なセキュリティ対策が困難に
- 複雑化するシステムを把握した上でのセキュリティ対策が必要
- 通信インフラソフトウェア・ハードウェアのセキュリティ対策向上、脆弱性管理の強化

■ サイバーセキュリティ標準化に期待されること

- 通信インフラが複雑化する中で、高いセキュリティレベルを確保
- 通信機能の変化（大容量、低遅延、多接続）に伴う新たなサービス形態や技術の移り変わりに対応して、我が国が強い産業分野を維持、創出する取り組みに注力

次世代の通信インフラに対応したセキュリティ対策

- 仮想化、SDN、NFV、等の新しい技術に対応したセキュリティ
- 通信インフラの変化や新機能を利用した、新たなアプリ・サービスやマーケット分野の創出

（通信）インフラに使用するソフトウェア・ハードウェアのセキュリティ確保

- サプライチェーン・セキュリティ
- ソフトウェア、ハードウェアに対するセキュリティ評価基準
- 脆弱性管理、評価の対象範囲拡大

新規分野・機能でのセキュリティによる優位性確保

- 耐量子コンピュータセキュリティ（暗号等）
- コネクテッド・カー向けセキュリティ
- スマートシティ・セキュリティ
- AI・ビッグデータ利用に関わるセキュリティ、プライバシー保護

次世代の通信インフラに対応したセキュリティ対策

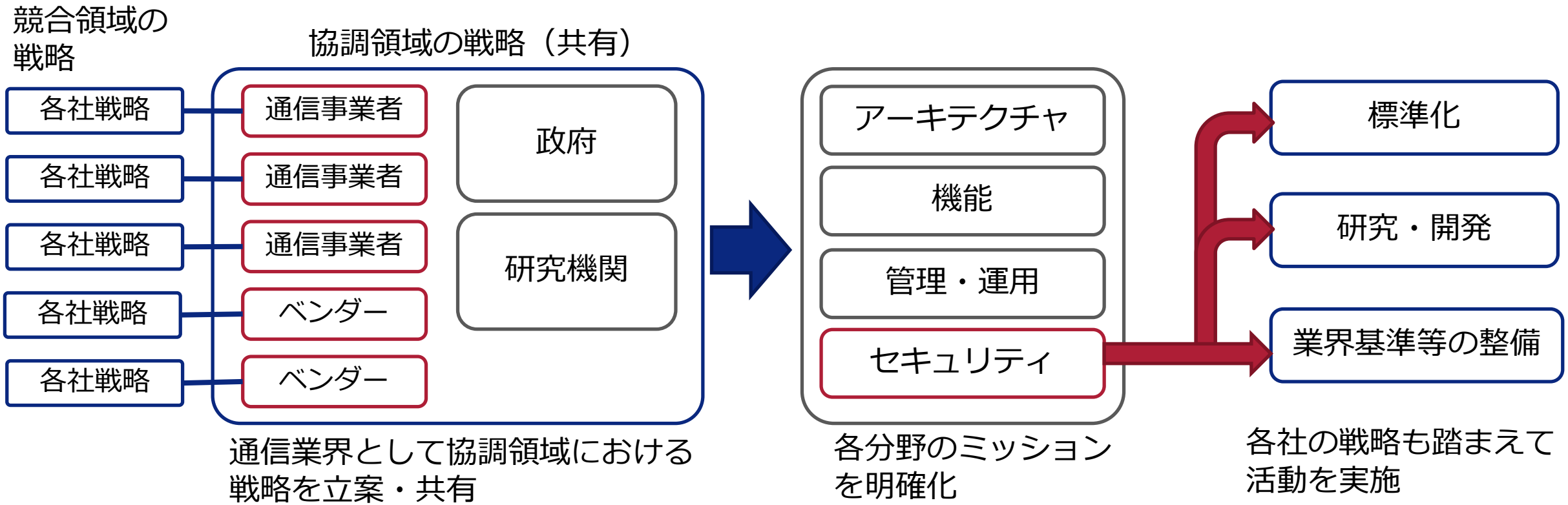
KDDI Research

■ **方向性**

- ネットワーク全体を俯瞰した取り組み
- マーケットを見据えた戦略に沿った活動

→

- 通信サービスにおけるセキュリティレベルの水準確保
- 通信分野における日本としての強みの創出



サイバーセキュリティ分野（通信インフラ）で注力すべき標準化（例）

- **5G・6Gセキュリティ、SDN/NFV/MEC/NWスライシング等の新機能のセキュリティ、クラウド（仮想化基盤）セキュリティ、サプライチェーン・セキュリティ、セキュリティ管理、脆弱性情報の管理、等**

インフラに使用するソフトウェア・ハードウェアのセキュリティ確保

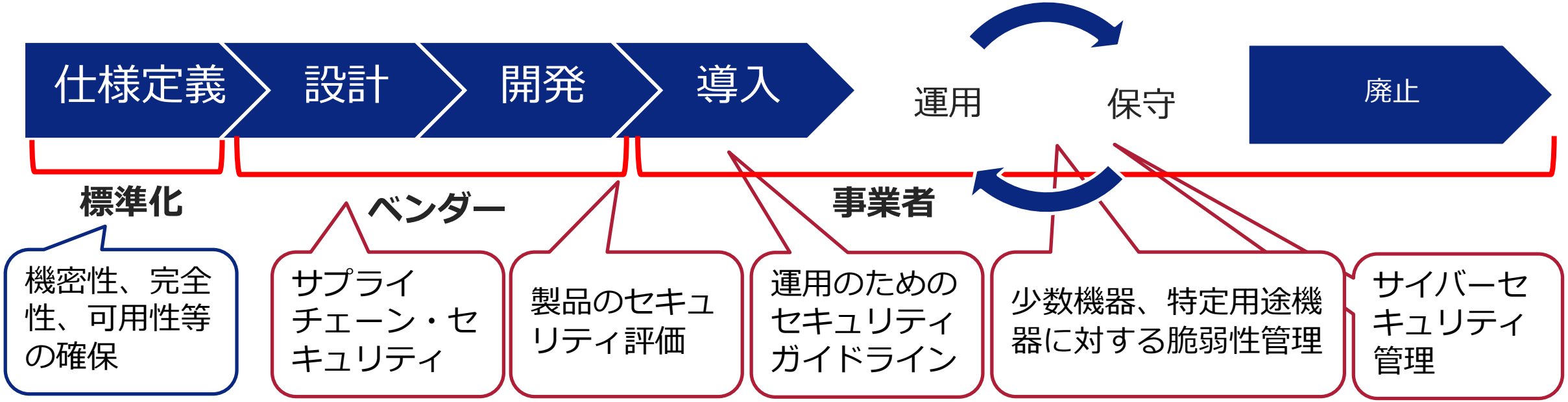
KDDI Research

■ 方向性

- **サプライチェーン・セキュリティの強化**
  - 製造側が受け入れやすい技術的な方式の確立
  - 国際的に統一された方式の展開
- **セキュリティ評価方式・基準の確立**
  - 製品に対するセキュリティ審査基準等の確立
  - セキュリティ・ガイドライン等の制定
- **サイバーセキュリティ情報の管理の対象範囲の拡大**
  - インフラ設備全般に関わる脆弱性情報の管理

- **ベンダー、事業者の負担を軽減する仕組みの導入**
- **認証ビジネス（安全性評価、セキュリティ監査）**
- **安全性が確保された製品による他社との差別化**
- **セキュリティ対策コストの削減**
- **事業者等のセキュリティレベル向上**

Cyber Defense Center
（ITU-T）



新規分野・機能でのセキュリティによる優位性確保

KDDI Research

■ 方向性

- **今後出現し、利活用が広がると考えられる機能、サービスに対するセキュリティ対策技術の開発**
- **知財確保と標準化展開、適用のルール化**

量子コンピュータの出現

- 暗号アルゴリズムの危殆化
- 耐量子コンピュータ暗号の実現

新暗号アルゴリズム（NIST、ISO/IEC）

量子暗号通信（ITU-T）

スマートシティ

- 様々な種類のIoT機器の展開
- 大規模セキュリティ管理、プライバシー保護

ITU-T SG17,SG20

oneM2M

ID管理・認証

データ流通

コネクテッド・カー時代

- 車両等がネットに接続
- 車両に対する攻撃経路のセキュリティ対策

ITU-T SG17

UNECE WP29

ISO TC204

ISO TC22

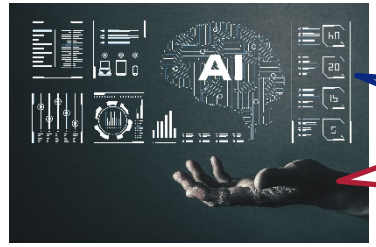
通信セキュリティの確保

遠隔セキュリティ監査

ID管理・認証

AI、ビッグデータ

- AIエンジンへの攻撃、プライバシー情報の漏洩
- 不正なデータ入力対策、不正なデータ利用の防止



ISO/IEC JTC1 SC42

IEEE

AIエンジンの信頼性確保

AIの適正利用

巨大マーケットでのシェア確保

3. データ流通分野におけるプライバシー保護（PPM: Privacy Preference Manager）

PPM概要

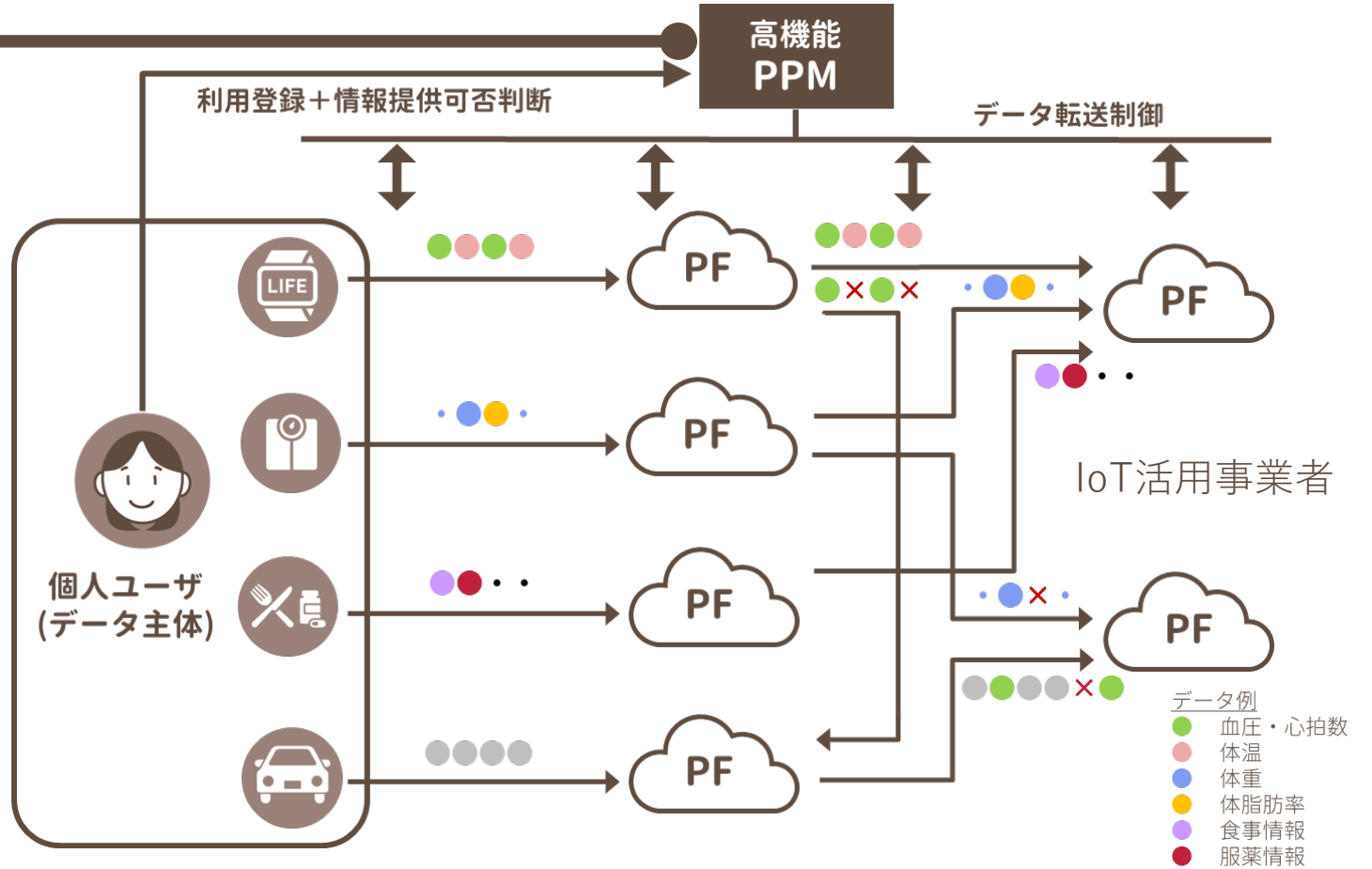
- パーソナルデータに関する同意取得・制御の一元化
- 各種パーソナルデータと多様なサービスPFに対応
- 「プライバシー保護」と「利活用・流通性」(利便性）の両立を実現

PPM*

複数のPFを対象とし
パーソナルデータの提供に関して個人ユーザからの同意取得を効率的に行い、その同意内容に基づきデータの転送を制御する仕組み

* Privacy Preference Managerの略

新たなライフ/ワーク・スタイルを
生活者がスマートに実現可能に

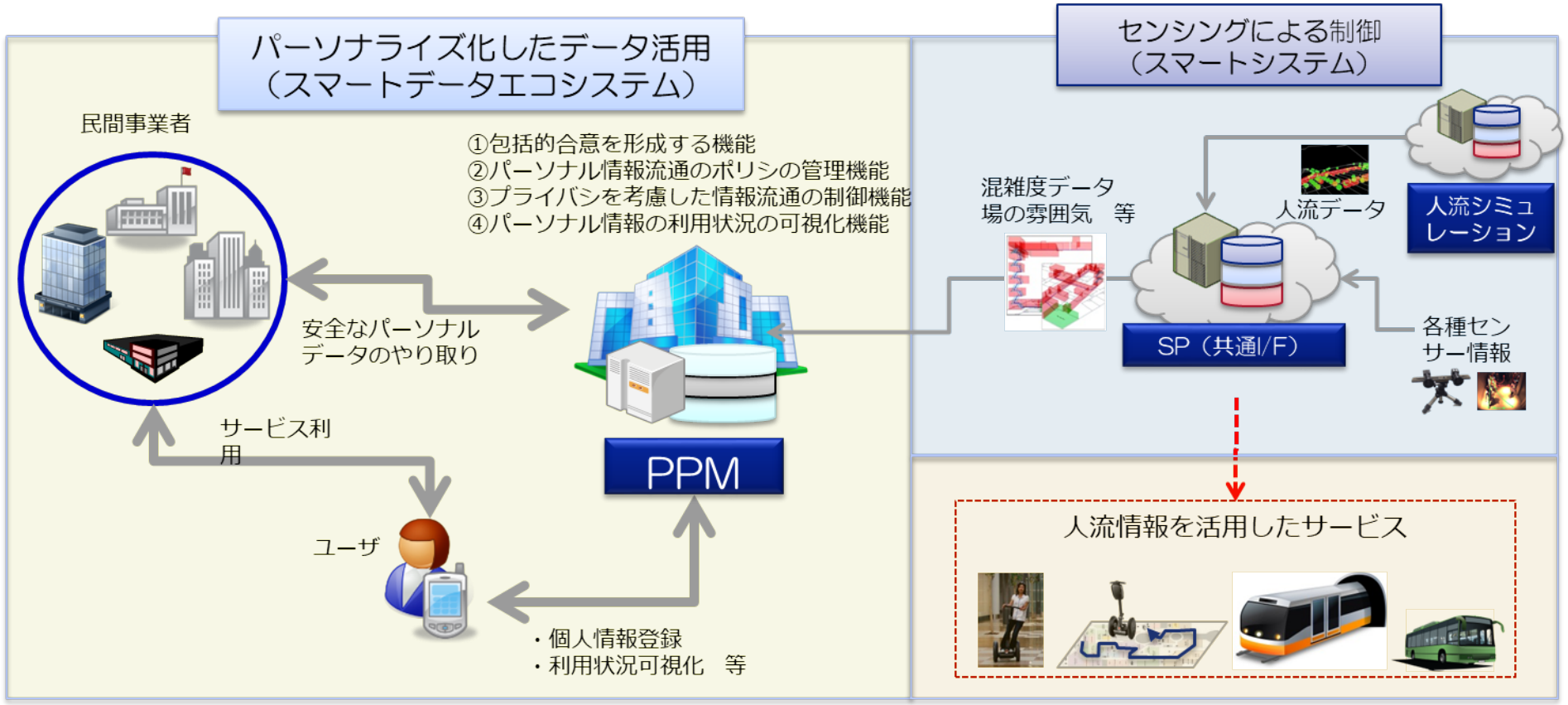


PPMに関連する取り組み（スマートデータエコシステム）

■ 「IT融合による新社会システムの開発・実証プロジェクト」

NEDOの実証プロジェクト

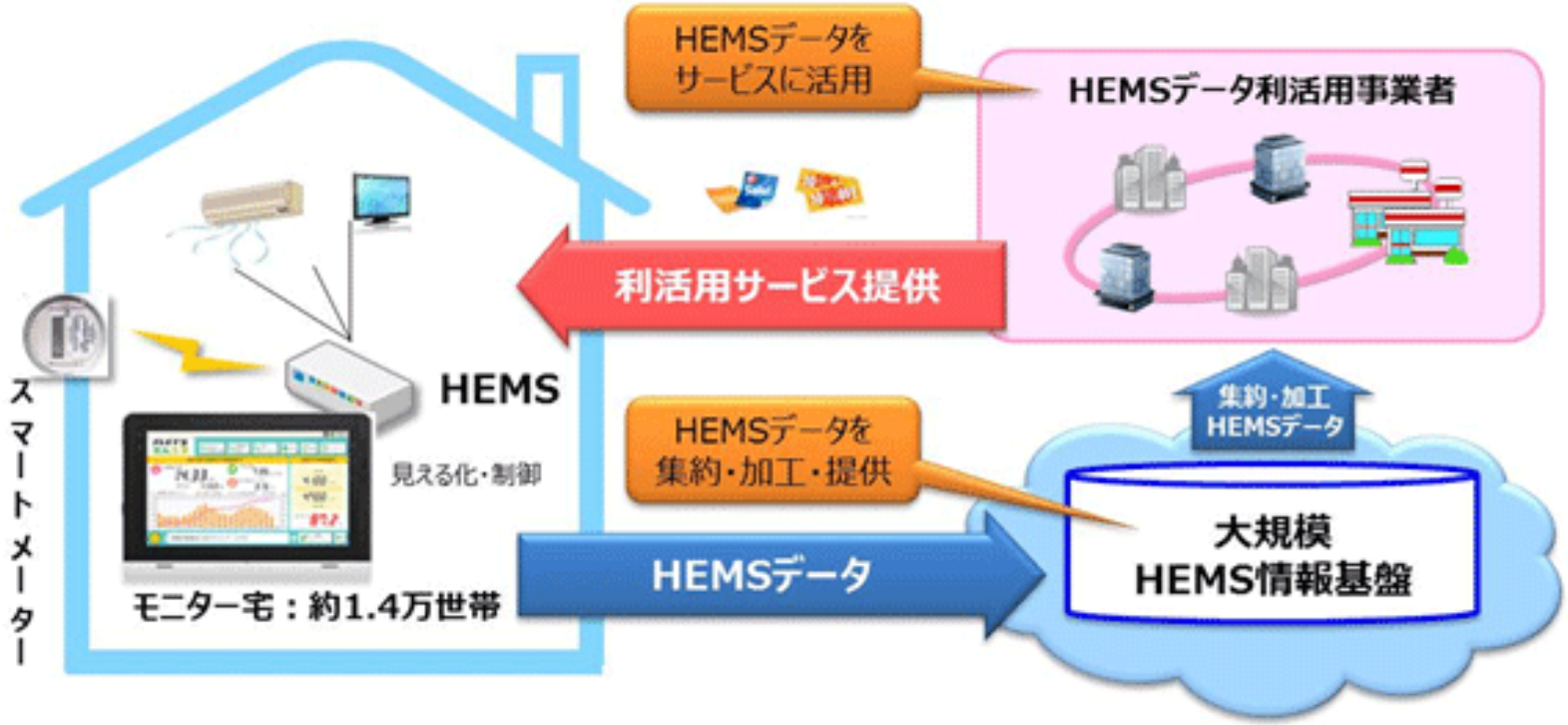
- **目的：**人の属性、場所、時間情報等に応じたコンテンツ等と融合する新しいパーソナルモビリティシェアリングシステムの開発
- **期間：**2012年から2013年
- **場所：**二子玉川ライズ（終了）



PPMに関連する取り組み（HEMS実証プロジェクト実施概要）

■ 大規模HEMS情報基盤整備事業」　経産省の実証プロジェクト

- 目的：
  - HEMSの普及による省エネ・ピーク対策に貢献するとともに、電力データを活用した新しいサービスによるより便利で快適な社会の実現を目指す
    - 大規模HEMS情報基盤の構築
    - 大規模HEMS情報基盤の標準化検討
    - PPMを用いたプライバシーに配慮した電力利用データの利活用
- 実施期間：
  - 2014年9月～2016年3月
- 参加企業：iエネ　コンソーシアム
  - 幹事会社
    - 東日本電信電話（株）
    - KDDI（株）
    - ソフトバンクBB（株）
    - パナソニック（株）
  - 参加企業　約20社
- 実証規模：
  - 約14000世帯のモニタを対象

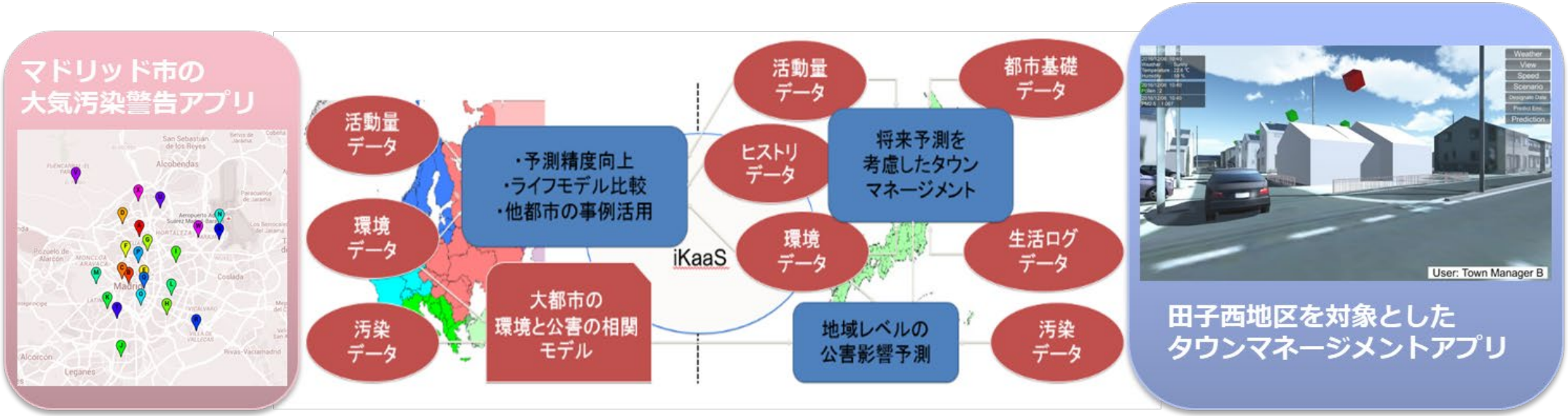


PPMに関連する取り組み（スマートシティ実証プロジェクト実施概要）

■ 「戦略的情報通信研究開発推進事業（国際標準獲得型）」

総務省の研究開発プロジェクト

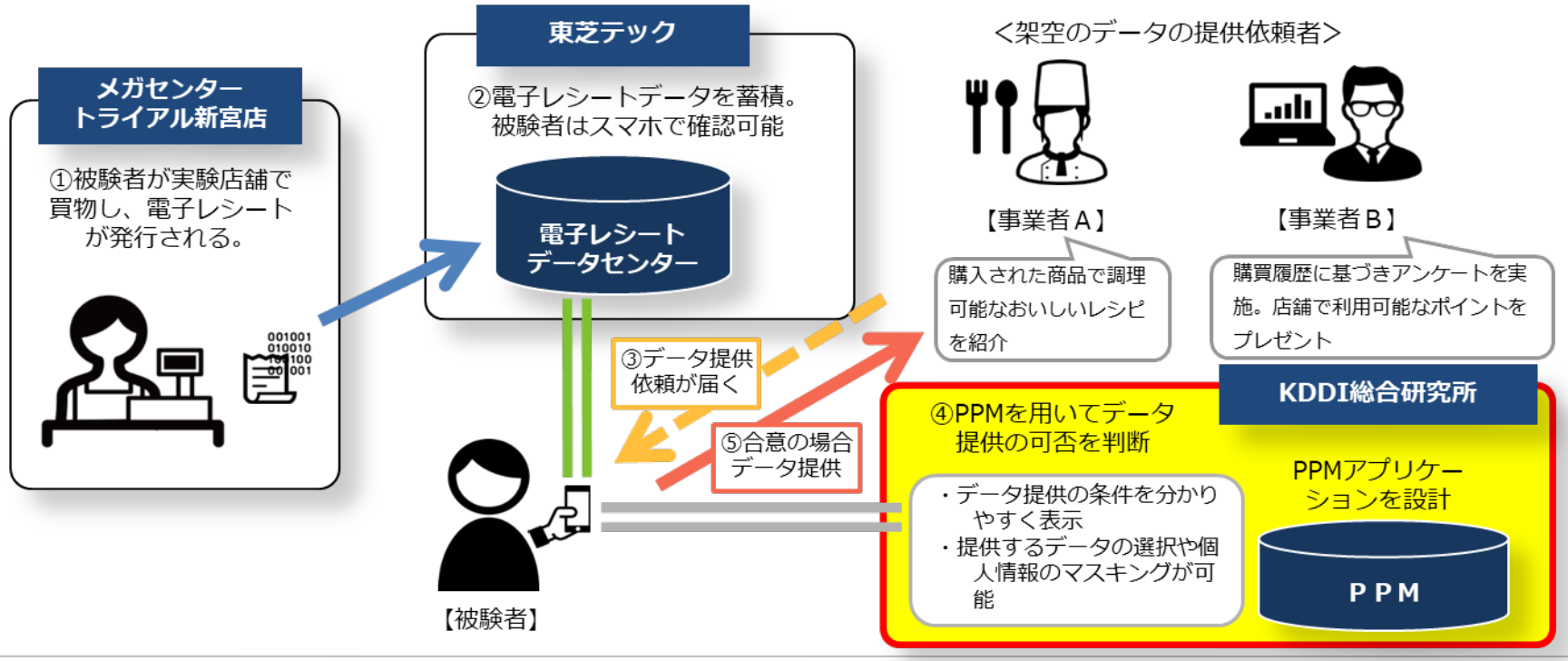
- 目的：スマートシティにおいて、プライバシに配慮したIoTデータ利活用を実現するためのプラットフォーム機能の検討並びに実証、および関連技術の国際標準化
- 実施期間：2014年10月～2017年9月
- 実証環境：マドリッド市（スペイン）ならびに仙台市田子西地区
- PPMの活用：プラットフォーム機能としてデータ提供を制御、クロスボーダー（越境）データ提供に対応



PPMに関連する取り組み（電子レシートシステム実証事業の実施概要）

■「平成28年度IoT推進のための新産業モデル創出基盤整備事業」経産省の実証プロジェクト

- **目的**：個人を起点に購買履歴を管理するシステムの標準化に向けた課題整理
- **期間**：2016年12月から2017年3月まで
- **場所**：ディスカウントストア「トライアル」メガセンタートライアル新宮店
- **参加企業**：トライアルカンパニー、東芝テック、KDDI総合研究所、インテージ、大日本印刷



PPMに関連する取り組み（複数事業者による IoT デバイス／プラットフォーム等の連携技術）

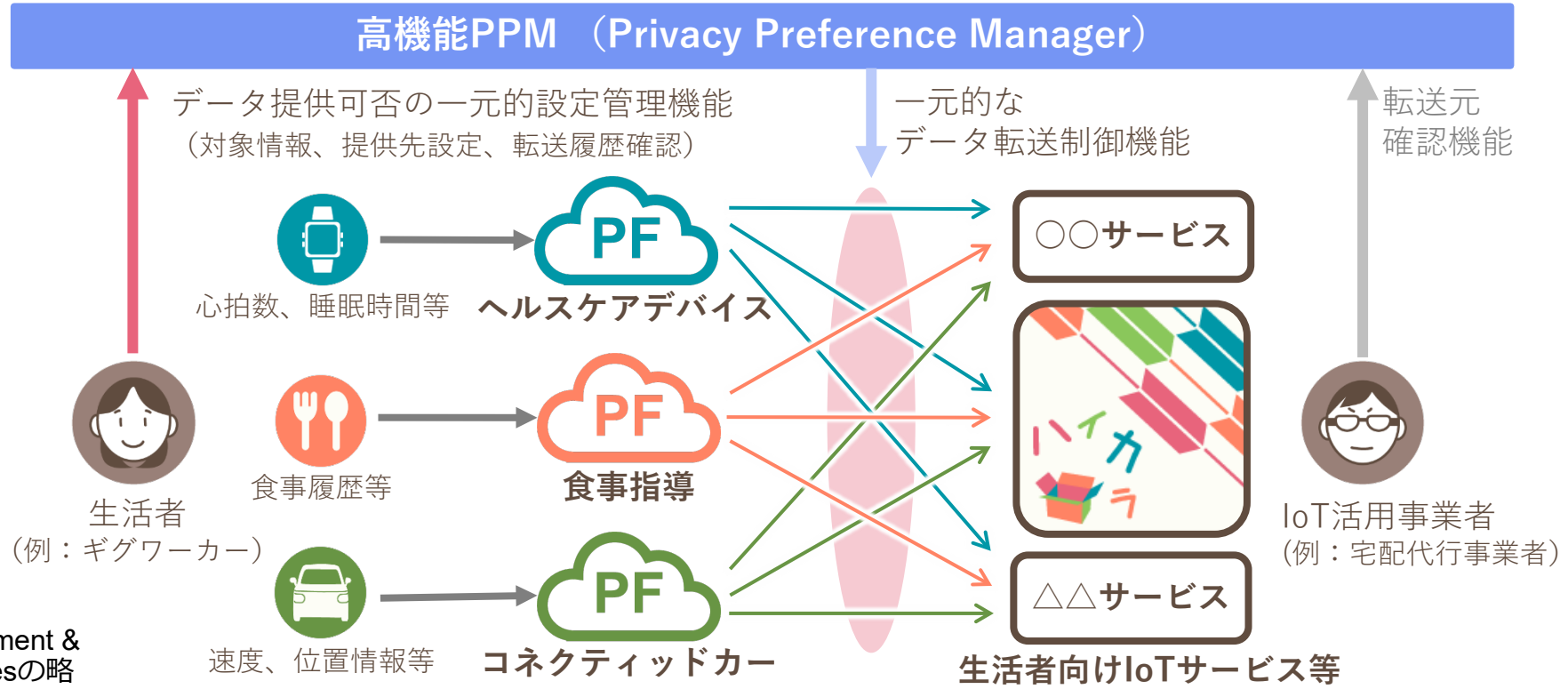
KDDI Research

■ 総務省「IoT/BD/AI 情報通信プラットフォーム」社会実装推進事業課題Ⅲ 研究開発プロジェクト

- **目的：**IoT デバイス／プラットフォーム等の連携技術の確立と３つ以上の事業分野での相互接続検証
  期間：2017年6月から2020年3月まで
- **取組対象：**生体情報を中心とした個人向けIoTサービス基盤の開発・実証（PARMMIT*1）
- **実証実験参加企業：**PARMMIT協議会メンバー24社*2

PARMMITによる サービスイメージの一例

自分の健康状態に合わせた
作業負担の最適化



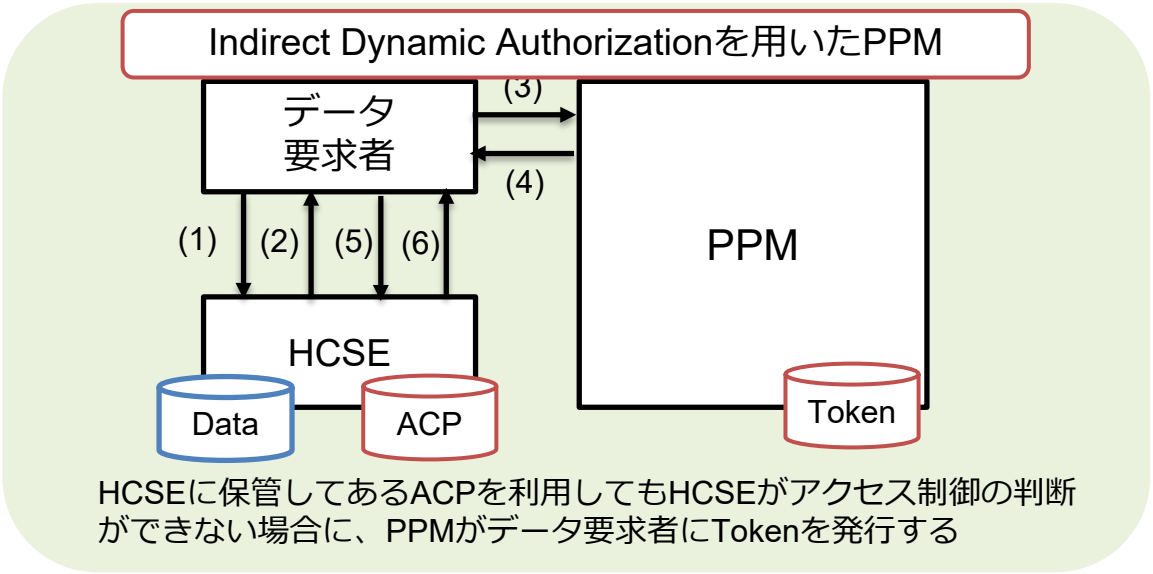
*1 Personal data Access Recording Management & Multi-platform Interconnection Technologiesの略

*2 https://rp.kddi-research.jp/parmmit/contents/about_parmmit/

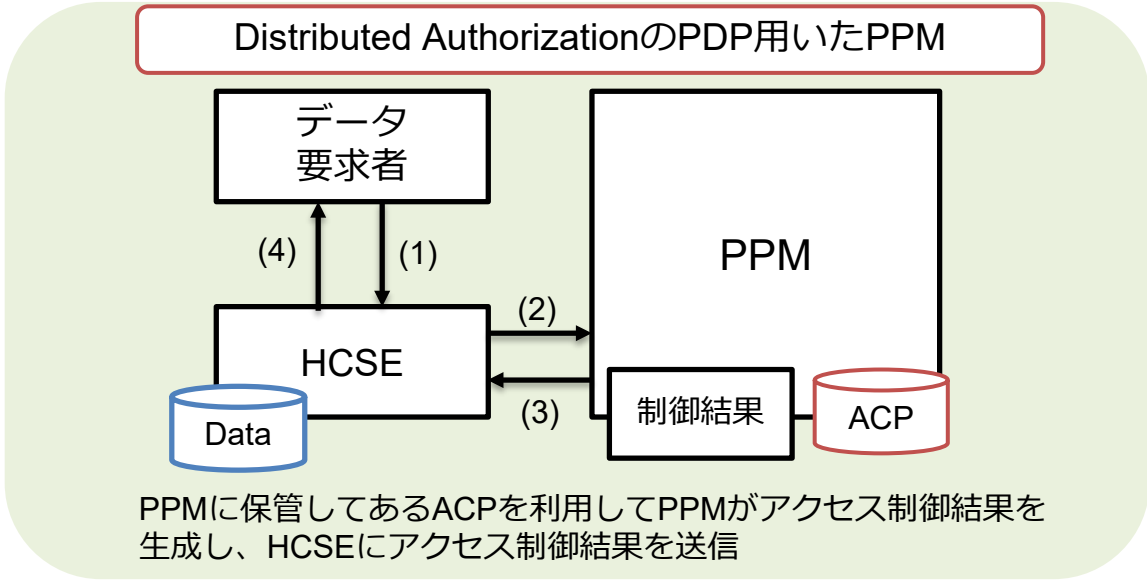
PPMに関連する標準化（oneM2M）

■ 概要

- PPMを実装するためのアクセス制御機構を、TS-0003: Security Solutionsの1項目として標準化
- サブスクライバーID、ユーザIDの概念をoneM2Mに追加



HCSEに保管してあるACPを利用してもHCSEがアクセス制御の判断ができない場合に、PPMがデータ要求者にTokenを発行する



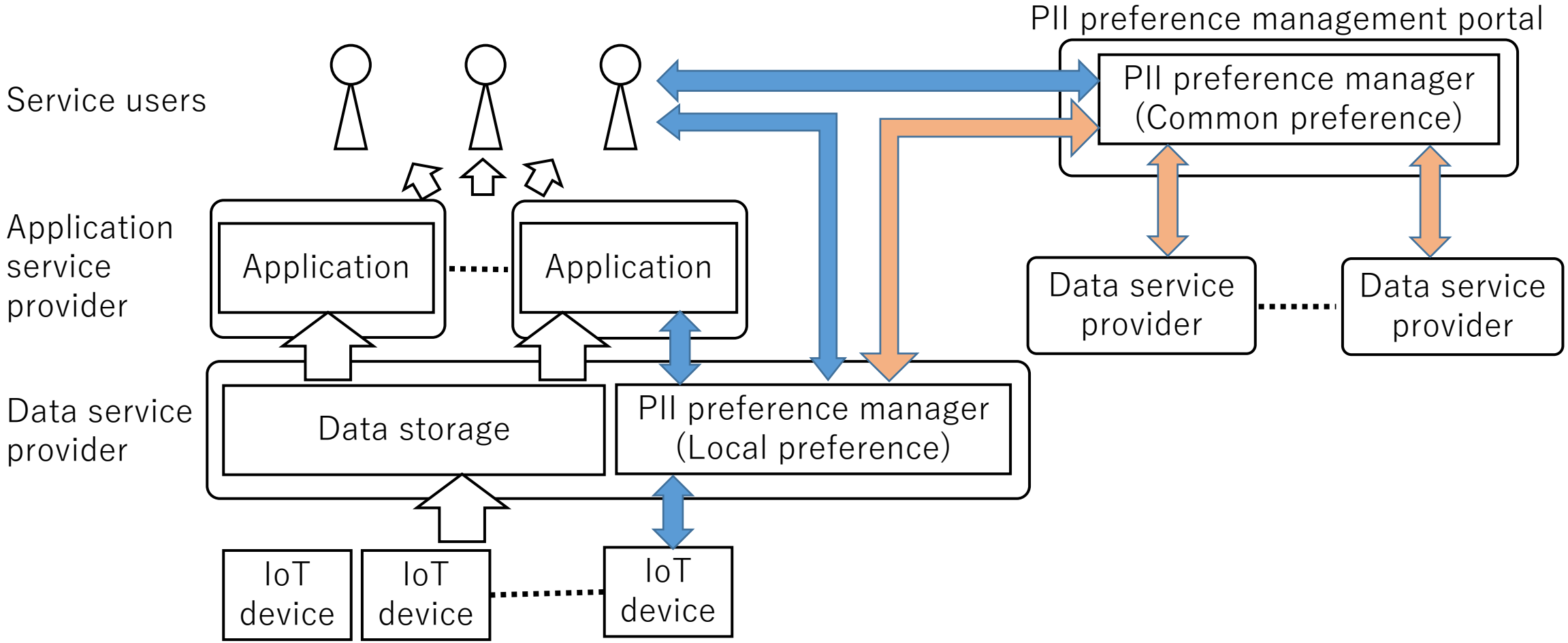
PPMに保管してあるACPを利用してPPMがアクセス制御結果を生成し、HCSEにアクセス制御結果を送信

oneM2Mでサポートしている2種類の認可方式に対して、PPMに設定された情報に基づてアクセス制御を行う歩式を標準化

PPMに関連する標準化（ITU-T SG17、進行中）

■ 概要

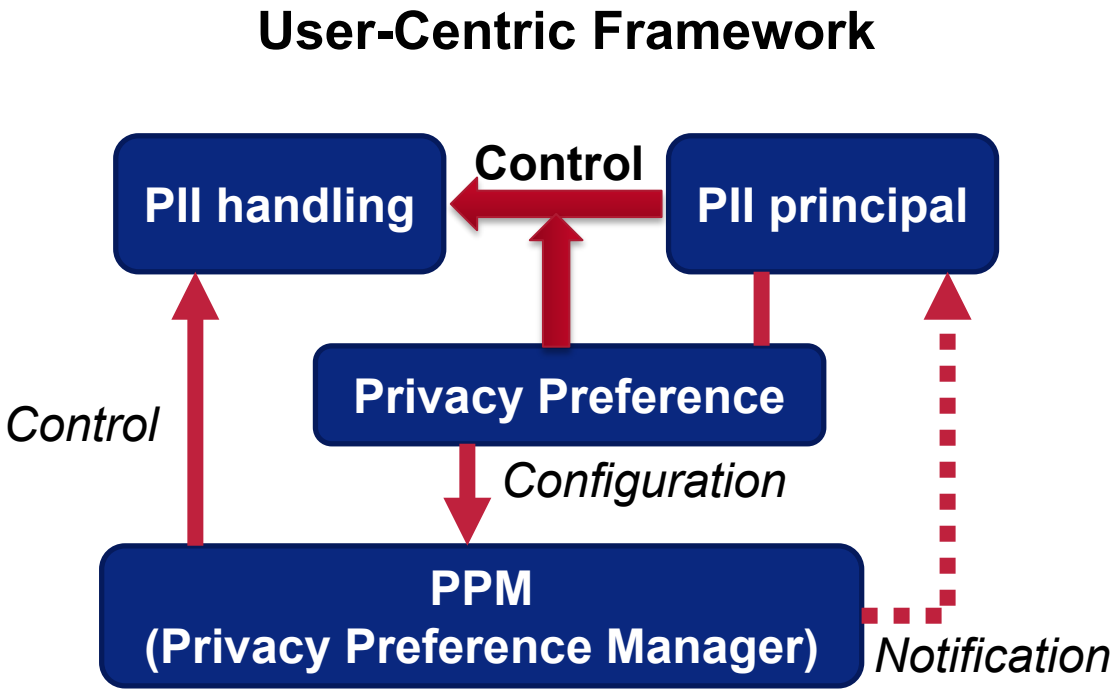
- IoT環境において、事業者間でPIIデータを流通させる場合の原則と、PIIデータ流通ためのフレームワークを規程

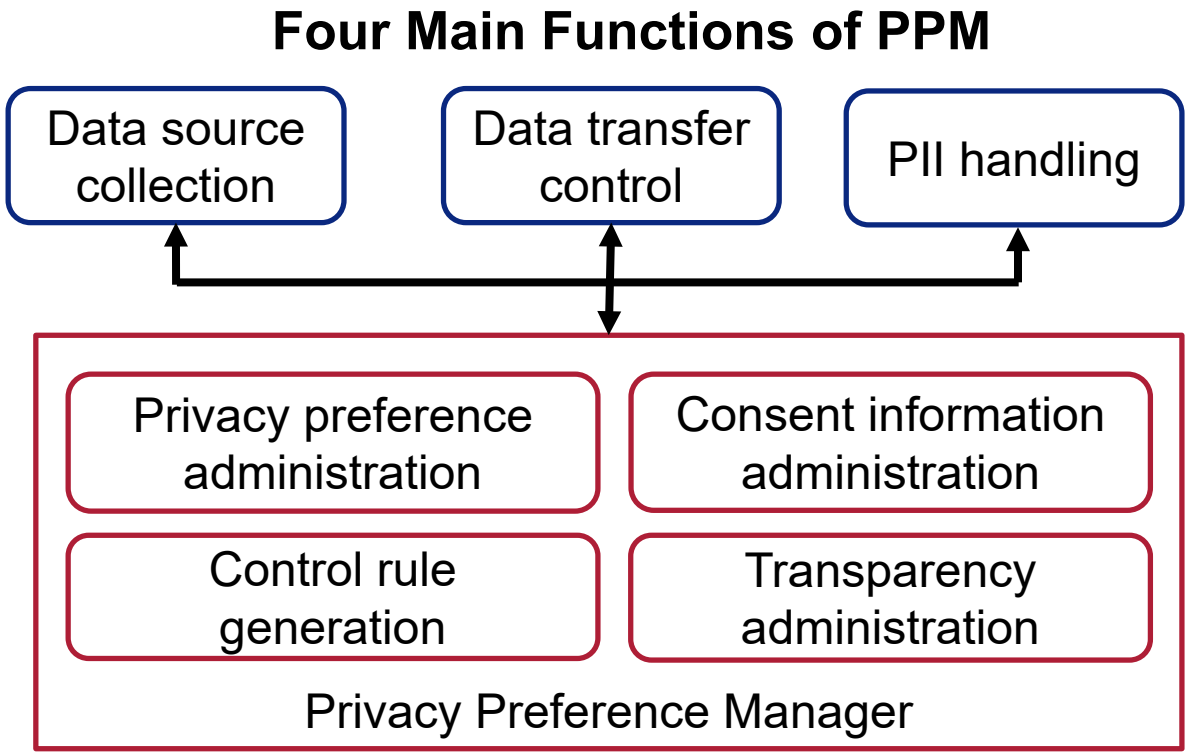


PPMに関連する標準化（ISO/IEC JTC1 SC27、進行中）

■ 概要

- ユーザ主体によるPersonal Identifiable Information（PII）のコントロールを行うフレームワークを規定
- 上記フレームワークを実現するコンポーネントとして、Privacy Preference Manager（PPM）を規定
- PPMの基本要件、機能要件、UI要件、運用要件、等を規定



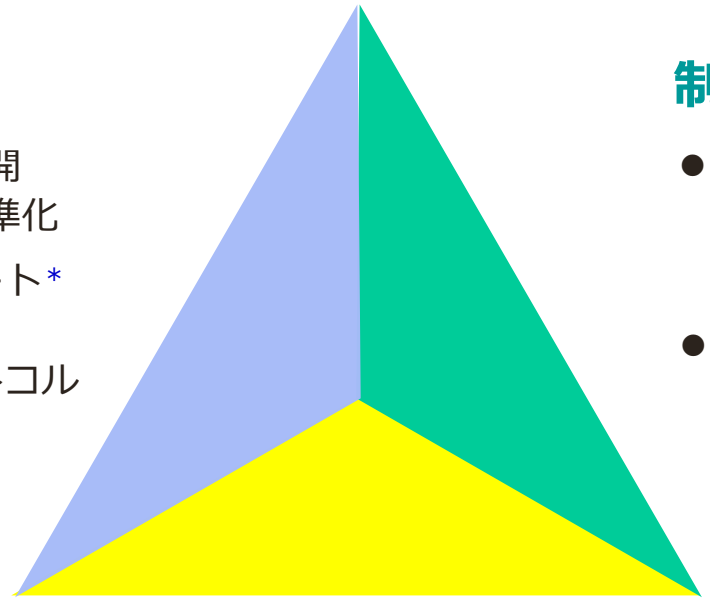


今後の社会実装に向けて

運用技術の共通化・標準化

- 非中央集権型オープンマーケットを展開していくための産業横断的共通化・標準化
  - ✓ データ名称等の語彙とアトリビュート*
  - ✓ サービス約款Mark-up Language
  - ✓ 事業者間ネゴシエーション・プロトコル
- 多省庁／諸外国との協調連携

  例えば、非中央集権型データ流通市場を実現する高機能PPM商用版の国際規格化・OSS化など



制度的整理

- 社会的信用を確保するための高機能PPM機能／事業者の認定制度
  - ✓ 社会的責任／担保
- 運用基準の共通化・遵守事項の明確化
  - ✓ ユーザビリティ／アクセシビリティ
  - ✓ 本人同意によらない個人情報の適正な取得
  - ✓ データ活用サービス本位にならない運用基準
  - ✓ 情報提供可否設定データのポータビリティ（ロックイン回避）など

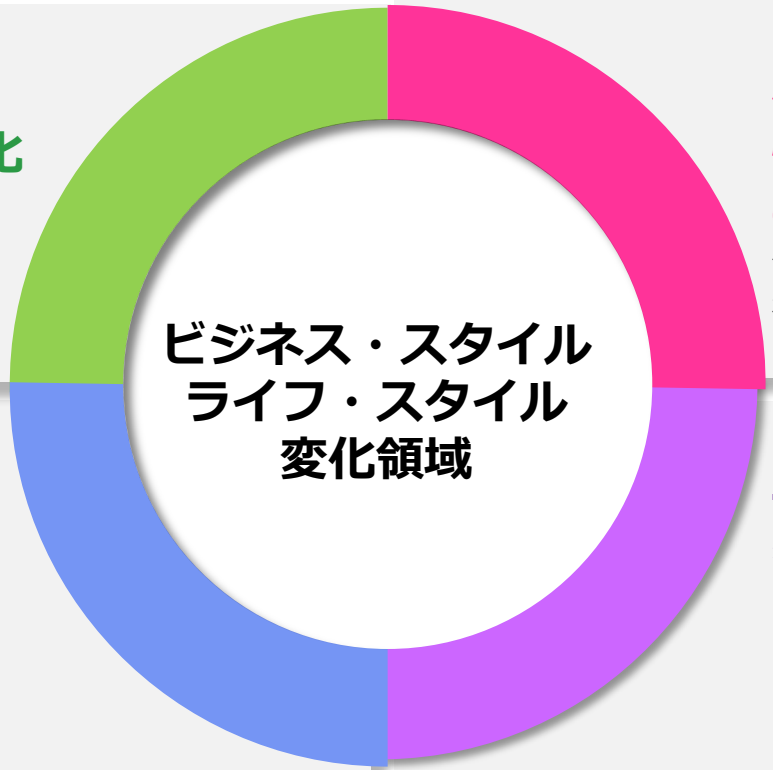
社会実装ロードマップの策定

- PPM／APPM費用負担の軽減策
- データ流通の源泉であるデータ一次取得者のデータ提供インセンティブと責務
- 高機能PPMの協調領域と競争領域の明確化
- 高機能PPM実装ガイドライン
  ～単一サイロでの非標準PPM運用から
  マルチPF運用高機能PPMへの移行シナリオ等

＊データ名称／IDは、以下を考慮し、利用頻度の高いデータ項目（常用データ）については、業界横断で名称／IDを統一しておくことが望ましい。アトリビュート定義も同様。
1．一次取得者と二次利用者との項目名の対応づけ
2．マイデフォルト選好と各事業者との項目名の対応づけ

新技術だけではなく業界横断で取り組んでいくことが肝要

APPMによるIoTプラットフォーム連携がもたらす新たな価値



データ・マーケットの非中央集権化・オープン化
巨大プラットフォーマによるデータ市場から分散型・非中央集権型市場へ（ロックイン回避）

個人による情報コントローラビリティの確立
全ての同意とこれらによる情報制御の一元管理が新たなスタイルへ

ビジネス・スタイル
ライフ・スタイル
変化領域

トラスティッドなリアルタイム転送による安全・安心感の向上
救急救命など緊急対応に用いるリアルタイム・データに対するトラスト機能は社会・生活をより安全に、安心できるものへ

データの異業種間多次元融合の促進
- ✓ 個人のリアルタイムデータ／ビッグデータ・統計データ
- ✓ 社会・環境のリアルタイム／ビッグデータ・統計データ

これらによる、その人、そのとき、その状況と経過に適応したサービス展開の促進

APPMはデータ駆動型社会におけるOSの一部

KDDI Research