資料22－2

KDDI Research

5G以降の時代に向けたセキュリティ標準化

2020年3月18日

株式会社KDDI総合研究所

三宅　優

通信分野におけるセキュリティ標準化活動

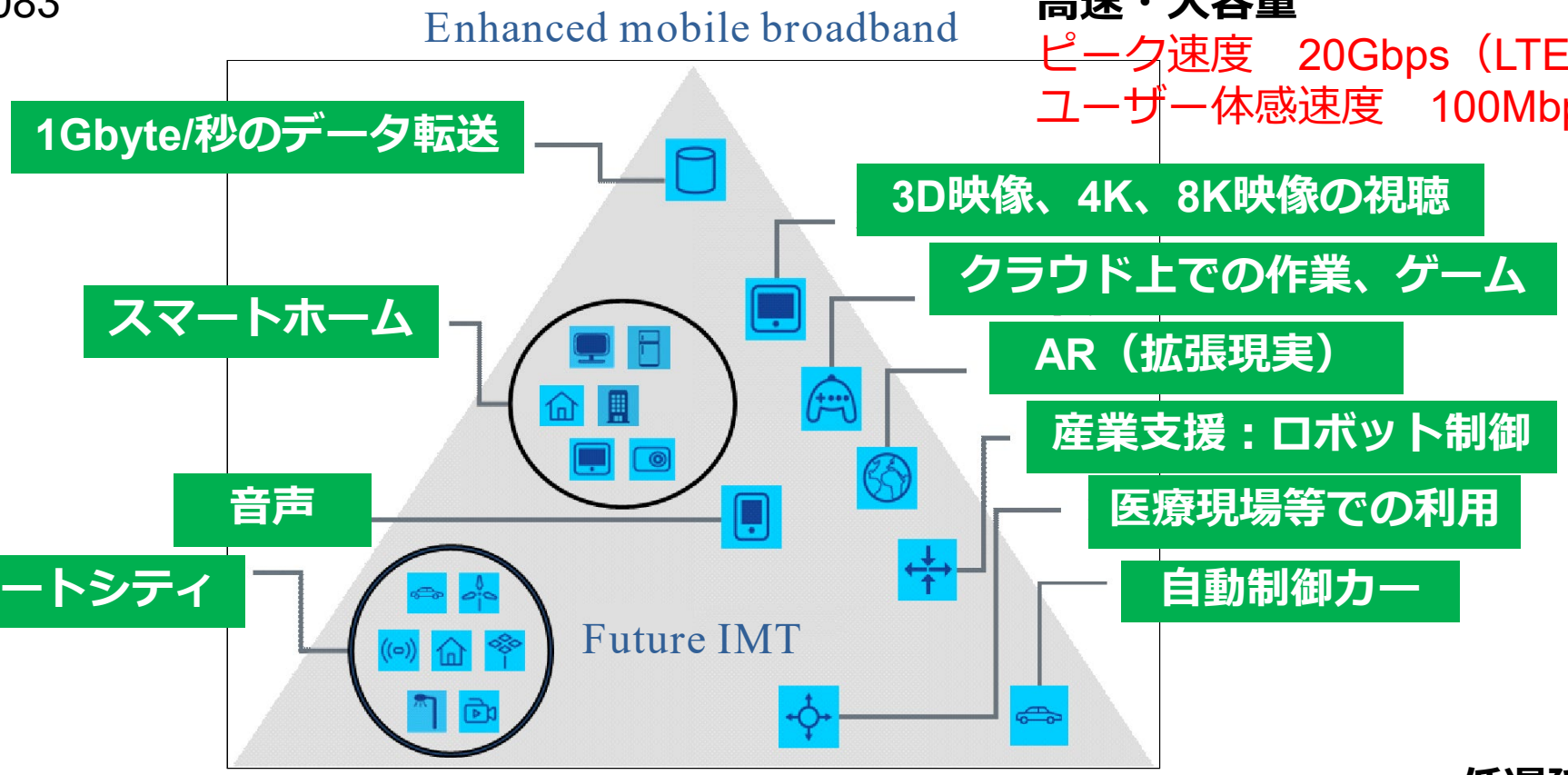
団体名	活動内容
IETF	インターネットに関連するプロトコルのセキュリティ対策・機能、セキュリティプロトコル
3GPP	モバイル通信におけるセキュリティ対策のためのプロトコル、機能
ITU-T	PKI、脆弱性情報管理、サイバーセキュリティ、スパム対策、セキュリティ管理、セキュリティ・アーキテクチャ、ID管理、ITSセキュリティ、DLTセキュリティ
ISO/IEC JTC1	暗号、セキュリティ管理、サイバーセキュリティ、ID管理、プライバシー対策
ETSI	サイバーセキュリティ、モバイルセキュリティ（3GPPと連携）
GSMA	（業界団体）　モバイルセキュリティに関するガイドライン作成、脆弱性情報・対策
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
OASIS	認証・認可方式（SAML/XACML）、サイバー脅威情報の交換（STIX/TAXII）

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）

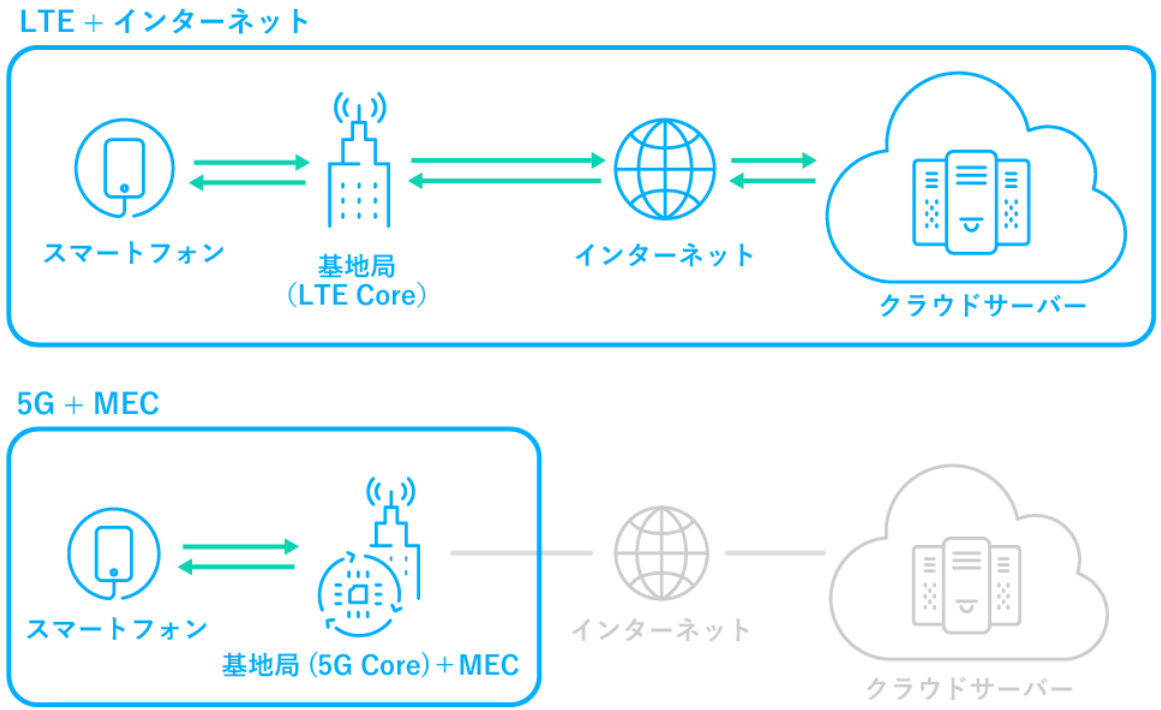
低遅延
無線区間　1ms
（LTEの10分の1）

M.2083-02

通信機能の多様化・複雑化

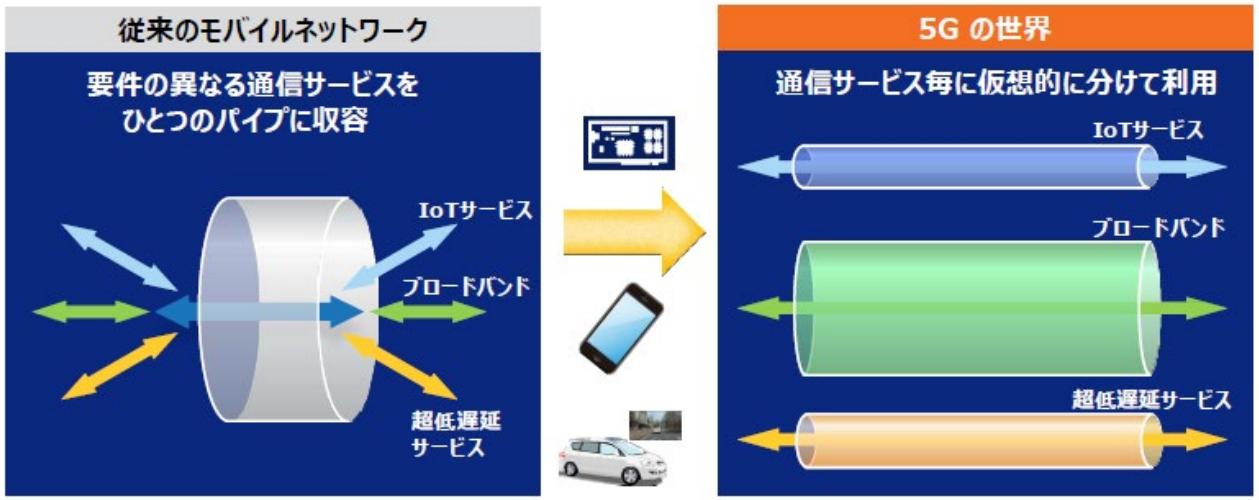
■ MEC (Multi-access Edge Computing)

- 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

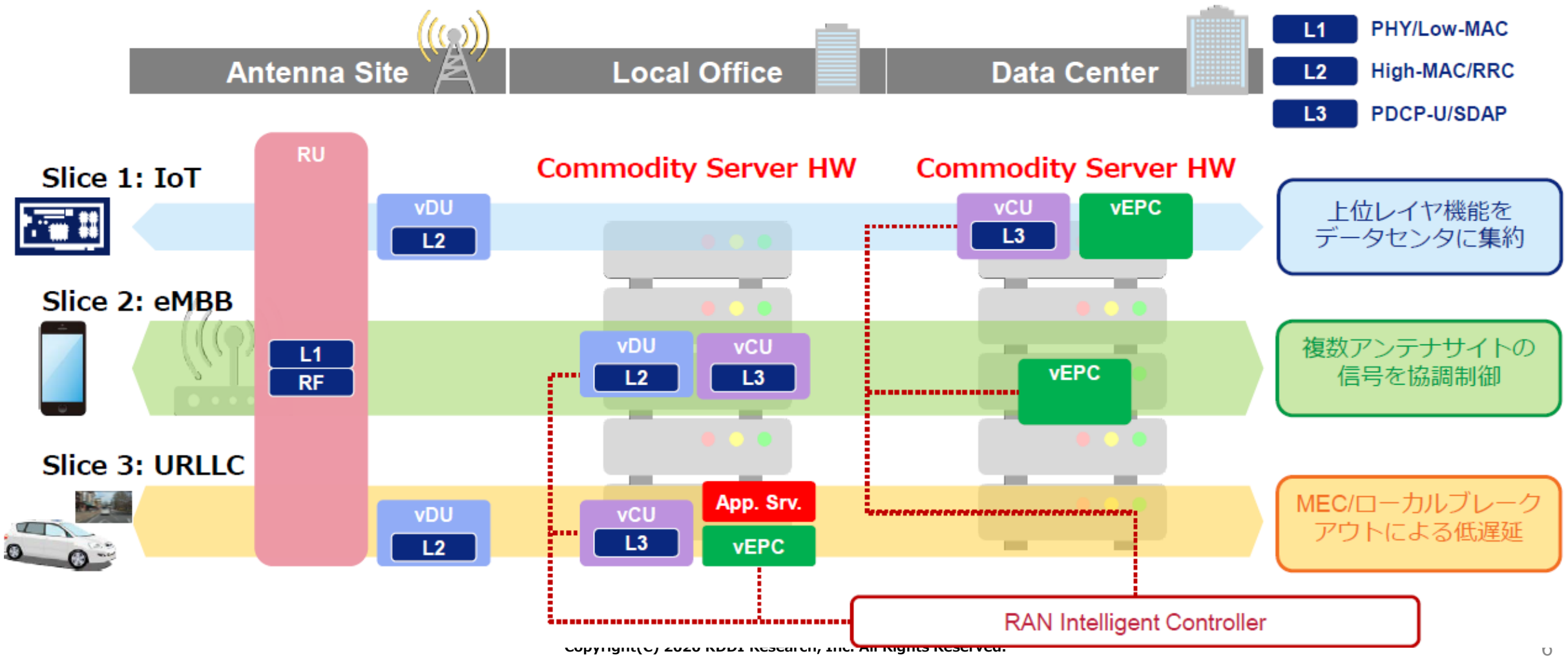
- サービスに応じてオーダーメイドで仮想的なネットワークを提供
- SDN（Software-Defined Networking）、NFV（Network Function Virtualization）等の技術を利用



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

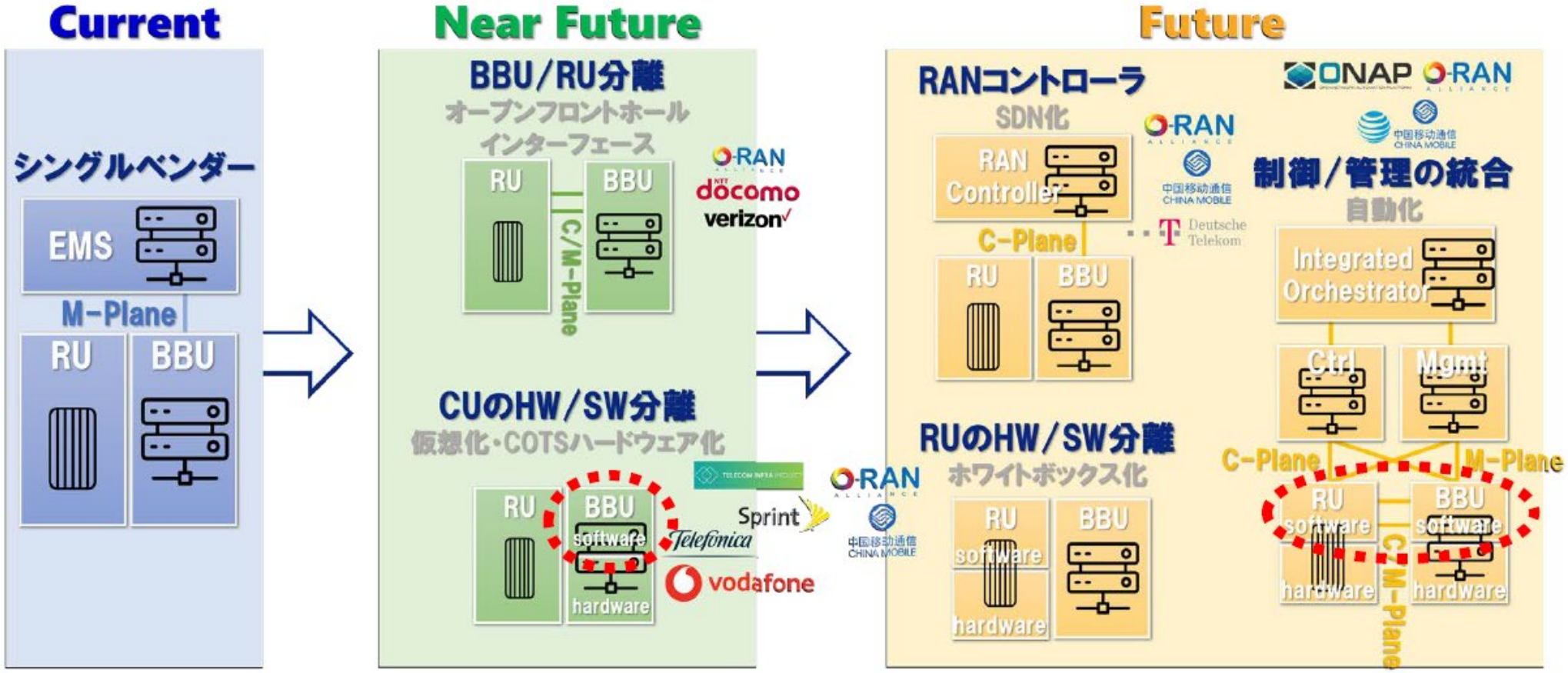
- サービスタイプに応じて基地局機能を配置することにより、論理ネットワーク = スライス を実現



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

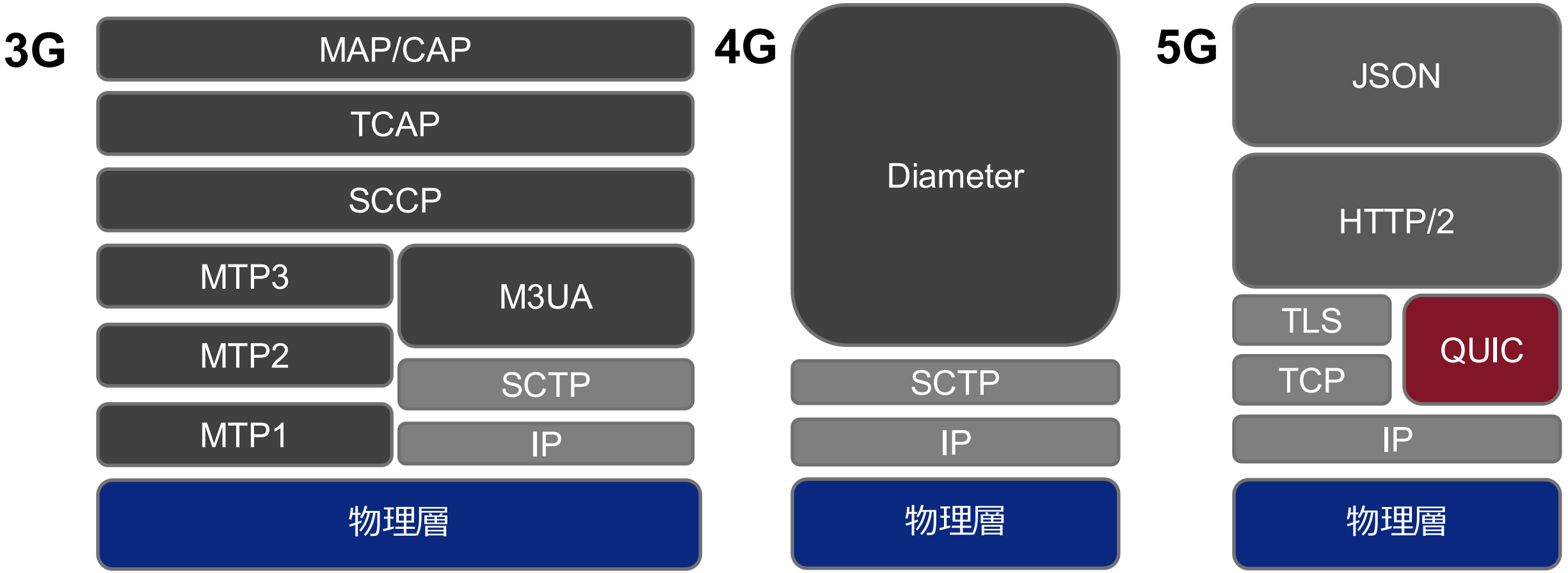


- オープンソースの利用、インタフェースの公開、・・・

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

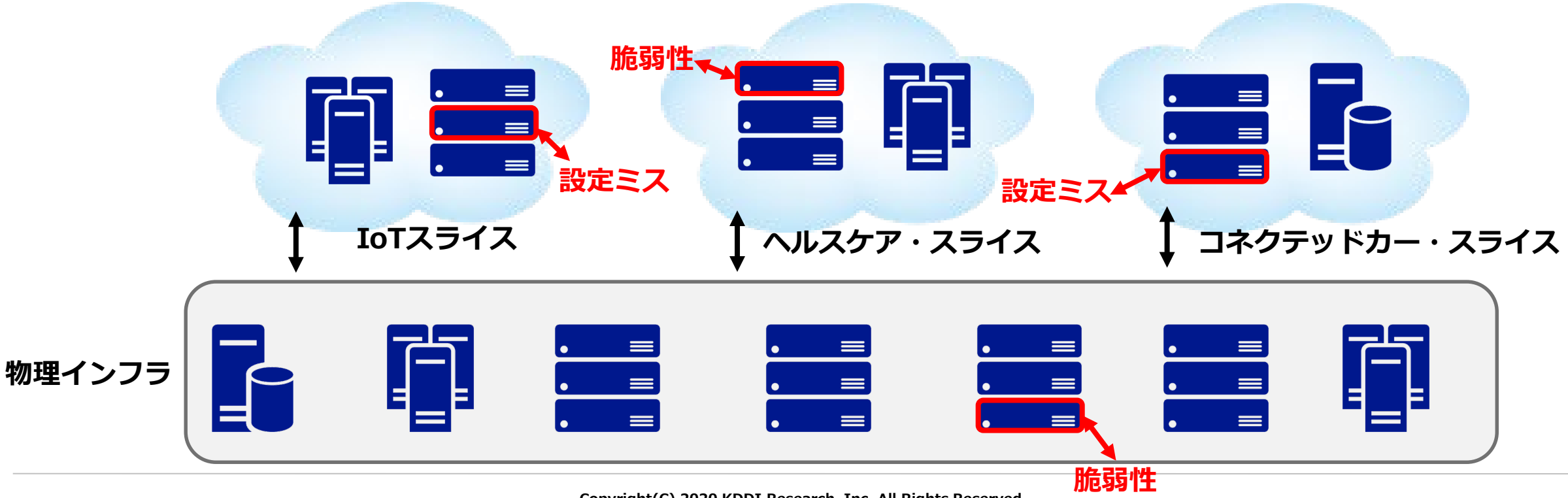


ネットワークの複雑化

- 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

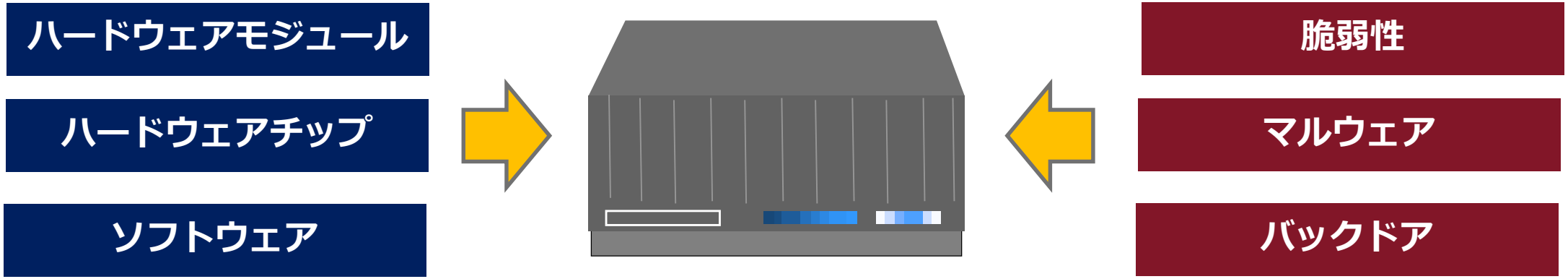
- ネットワークの設定ミス、設定の不整合、脆弱性、等により、攻撃のされるポイントが増加？



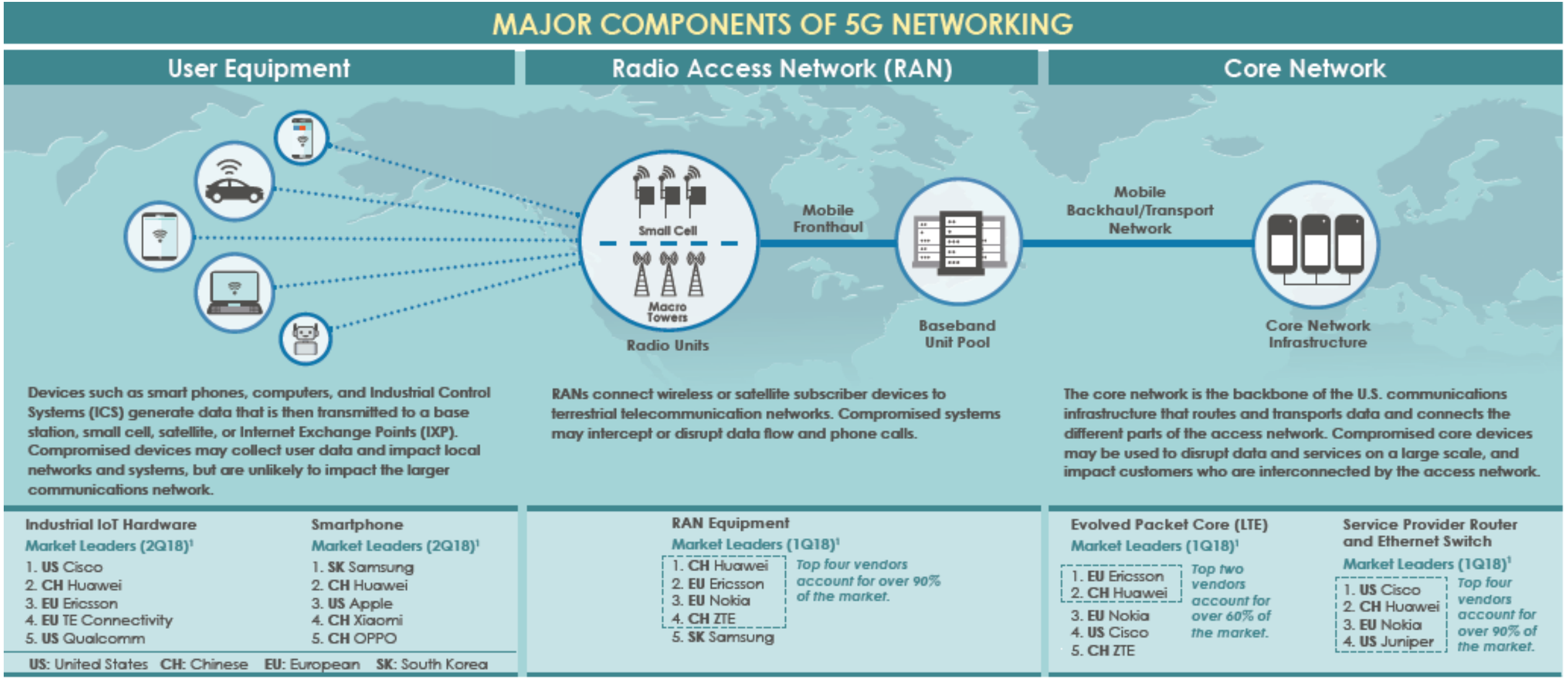
サプライチェーン・リスク

■ 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

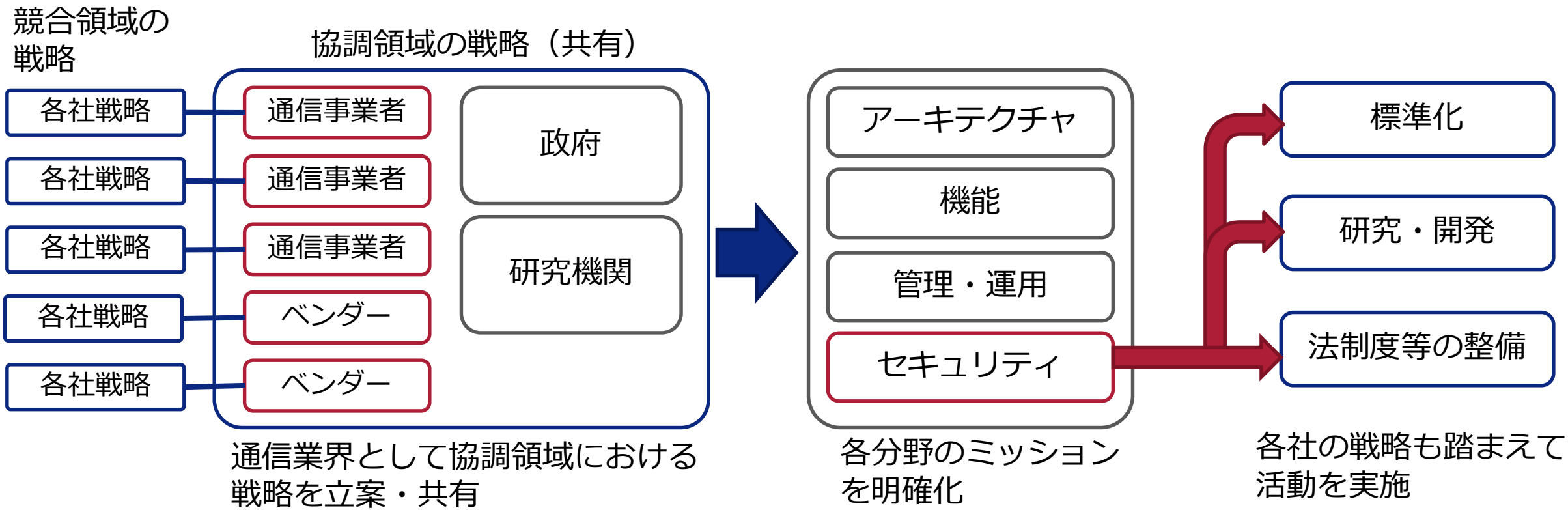
KDDI Research

■ **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

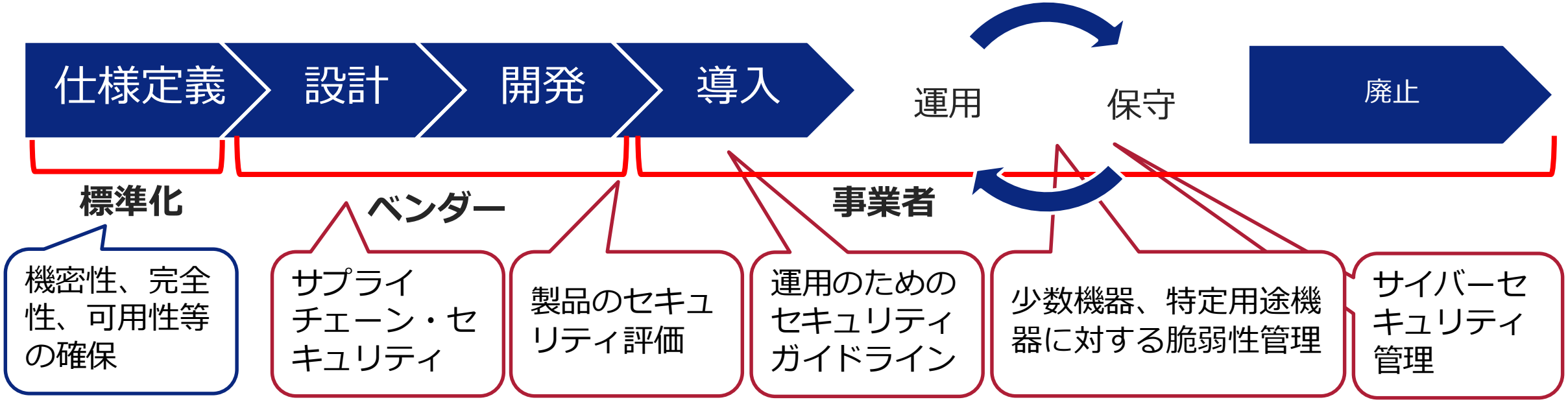
KDDI Research

■ 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

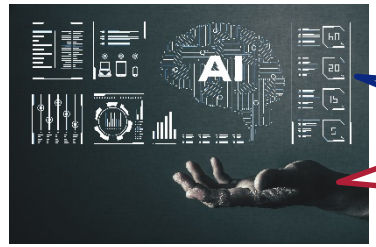
遠隔セキュリティ監査

ID管理・認証

巨大マーケットでのシェア確保

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

KDDI Research