

ARIB / TTC共催セミナー

M2M標準化最新動向

－ oneM2M技術仕様(初版)の全貌 －

平成26年9月1日

ARIB / TTC

時間	内容	スライド No.
	司会進行 TTC oneM2M専門委員会 副委員長 日本電信電話株式会社 筒井 章博 様	
13:30 - 13:40	開会挨拶 ARIB oneM2M対応ワーキンググループ 主査 株式会社NTTドコモ 井原 武 様	
13:40 - 14:05	oneM2Mの意義と初版技術仕様書の公開について TTC oneM2M専門委員会 委員長 oneM2M Technical Plenary Vice Chair KDDI株式会社 山崎 徳和 様	3~30
14:05 - 14:25	技術仕様(初版)の構成及び概略 日本電気株式会社 小林 中 様	31~46
14:25 - 14:45	Registration - CSEへのAE/CSEの登録手順 - 日本電信電話株式会社 後藤 良則 様	47~55
14:45 - 15:05	コミュニケーションマネジメント&デリバリーハンドリング(CMDH) ARIB oneM2M対応ワーキンググループ 副主査 クアルコムジャパン株式会社 内田 信行 様	56~66
15:05 - 15:20	休憩	
15:20 - 15:40	デバイス・トリガリング及び下位伝送網との連携機能 株式会社NTTドコモ 奥水 敬 様	67~77
15:40 - 16:00	サブスクリプション・マネージメント - Subscription and Notification - 住友電気工業株式会社 平川 満 様	78~87
16:00 - 16:20	M2Mデバイス・マネージメント 株式会社KDDI研究所 服部 雅晴 様	88~95
16:20 - 16:40	M2Mセキュリティ 株式会社日立ソリューションズ 中野 正樹 様	96~104
16:40 - 17:10	サービスレイヤプロトコル oneM2M Protocols Working Group Vice Chair 株式会社富士通研究所 藤本 真吾 様	105~119

oneM2Mの意義と 初版技術仕様書の公開について

KDDI株式会社
山崎 徳和

概要

- 統合M2Mサービス層標準化組織としてoneM2Mが設立(2012/7月)
- 「M2Mサービス層」の要求条件、機能アーキテクチャ、プロトコル/API、セキュリティ等を中心に標準化を検討、Device Aspect(モジュール)に関する取り扱いが課題
- 当初は、各国SDOからの標準化成果がベース(ETSI中心)
- 既存外部仕様(3GPP/3GPP2、OMA、BBF)の利用と協調
- Vertical Industry Segmentからの参加/寄与(Continua、HGI、ESMIG)
- Use Caseやアーキテクチャに関するTR(技術報告書)が完成
- Requirements仕様書(Stage1)が完成('13/10)
- Architecture仕様書(Stage2)が完成('14/08)
- 2014年8月に、初版仕様書リリース(V-2014-08: Stage1/2プロトコル仕様書、デバイス管理仕様書、セキュリティ仕様書を含む)、外部にもコメントを求め、2015年1月に改訂版のリリース予定
- ETSIの協力を得て、本年12月9日に、Initial Release Launch Eventを企画、Continua、ESMIG、HGI、複数ベンダーがデモ実施の方向で調整中
- ここに来て、主要なVerticals(業界団体)にoneM2M仕様への関心の高まり、仕様採用への動きあり

oneM2Mの概要

背景: ETSI TC M2Mが2009年1月にM2Mサービス層標準化を目的として設立されて以来、TIA、CCSA等のSDOやOMA、BBFが同様に標準化を開始し、作業の重複やマーケットの fragmentationの懸念が生じてきた。これを背景に、ETSIの提唱により2011年7月からARIB、ATIS、CCSA、ETSI、TIA、TTA、TTCの7つのTelecom SDOで非公式に、M2M共通の標準化ソリューションを見出すため、M2Mサービス層標準化活動の統合し、グローバルなイニシアティブ設立を検討。2011年12月に設立に向けて基本的合意、2012年1月に「oneM2M」と名称が決定された。2012年7月に正式に発足。

＝組織の概要＝

- 3GPPsと類似の形態 (Legal Entityではなく、各SDOが共同で運営する組織)
- 複数のM2Mアプリケーションに跨る共通のユースケースとアーキテクチャに基づき、第1歩として、「M2Mサービスレイヤ」の仕様書作成を目指す。
- 電気通信系の標準化団体が結集した形だが、各M2Mサービス分野のプレイヤー (Vertical Industry Segment) や他の標準化機関との協調・連携にも積極的に取り組んでいく。

better together



M2Mの機能を標準化することによるベネフィット

1. 多数のプロバイダによる相互運用可能なコンポーネント

大規模
アプリケーション開発
エコシステム

大規模
ハードウェアサプライ
エコシステム

大規模
サービスプロバイダ
エコシステム

2. スケールメリット(規模の経済性)

FCQトレードオフ改善
(Functionality-Cost-Quality)

広がる選択肢

広がるチャンス

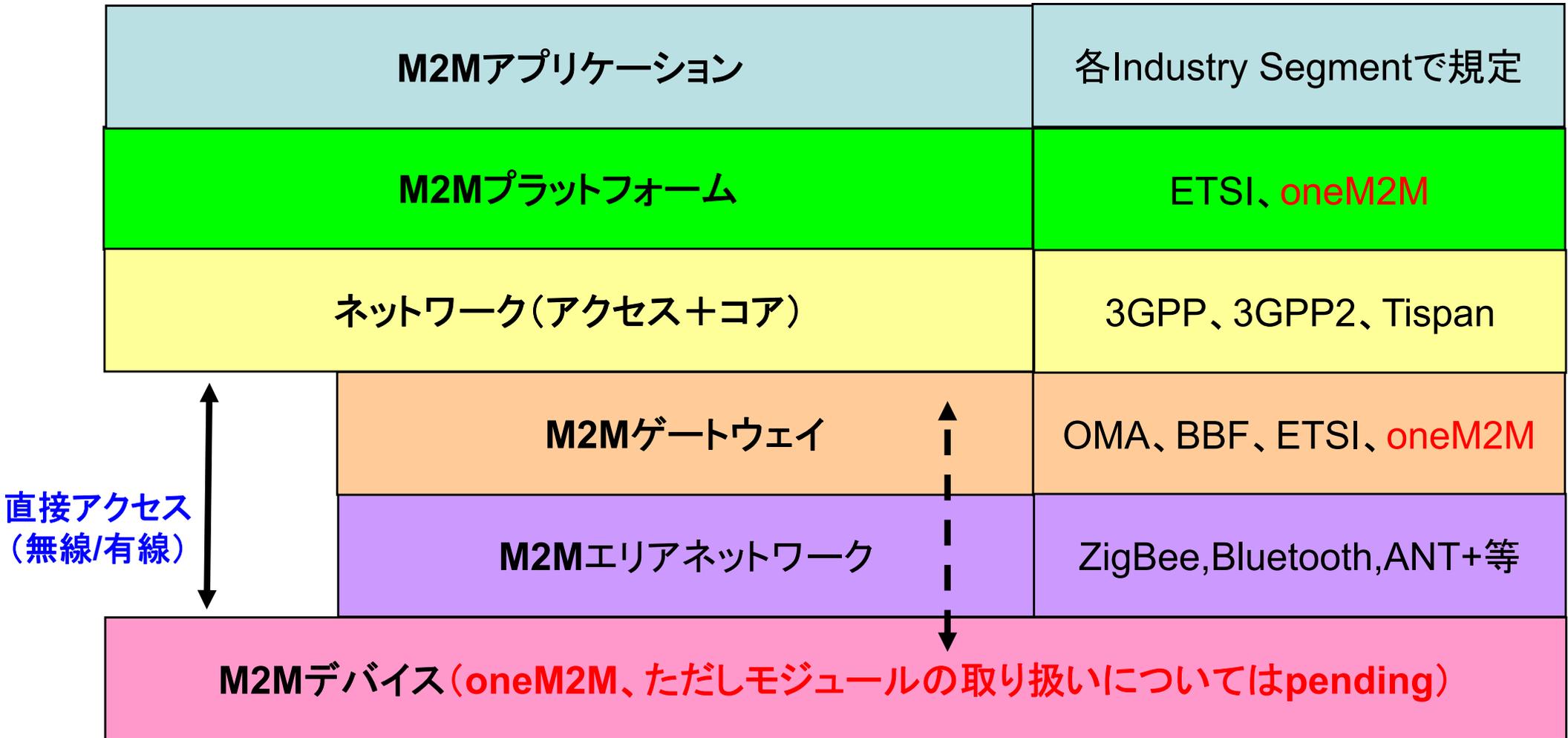
拡張性の向上

M2M市場からの期待

M2Mのレイヤー構造と標準化対応

M2M階層(レイヤ)

標準化



M2Mアプリケーション/デバイスに対し、共通のサービス機能 (Common Service Function) を提供する

→ **共通プラットフォーム機能 (ミドルウェアに相当)**

➤ **リモート・デバイス管理機能**

➤ Configuration (環境設定) やDiagnostics (診断)

➤ **通信管理・接続処理機能**

➤ 基盤ネットワークを信頼性、拡張性を維持しつつ、効率的に利用

➤ **データ管理機能**

➤ M2Mアプリケーション間でのデータ保存と共有やイベント通知

➤ データへのアクセス管理: Who、What、When、Why

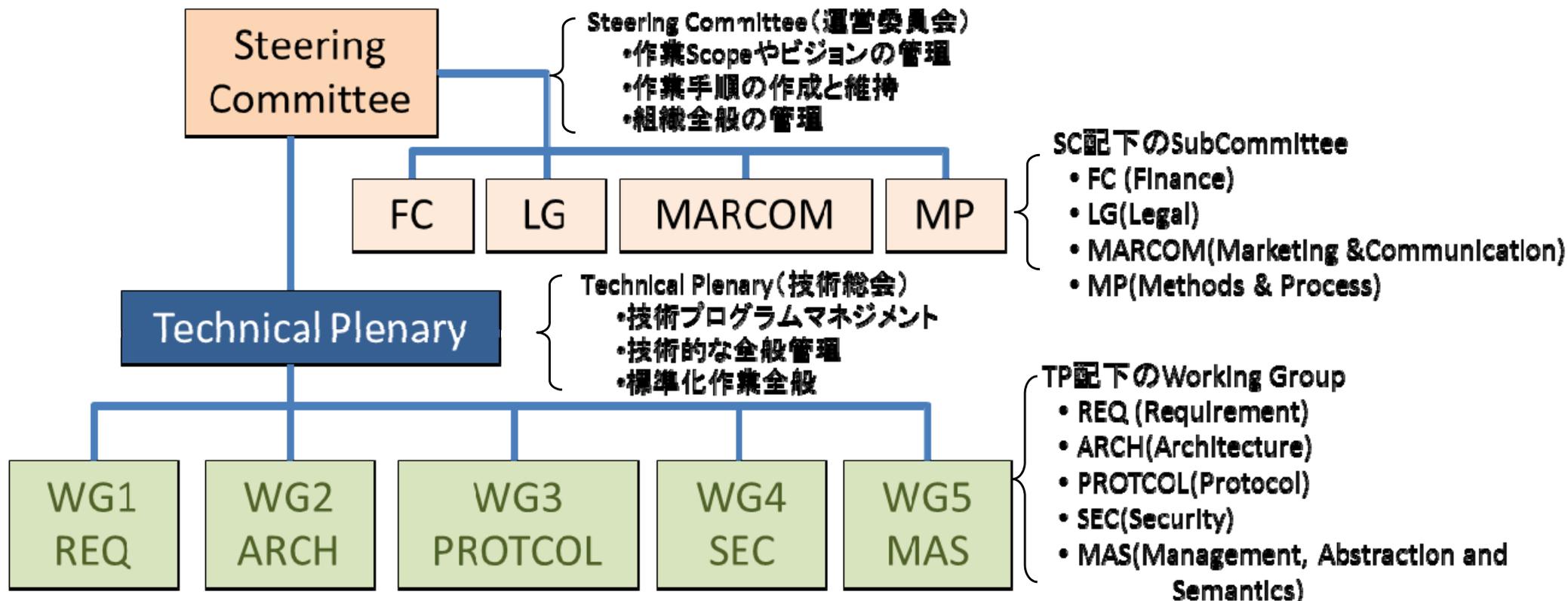
➤ **アプリケーション管理**

➤ **セキュリティ及びアクセス制御機能**

➤ **課金**

➤ **加入管理、等々**

oneM2Mの構成(2014年8月現在)



Technical Plenary Leadership

Chair: Peter Nurse (Qualcomm/TIA)
 Vice Chair: 山崎 徳和 (KDDI/TTC)
 Joachim Koss (Gemalto/ETSI)*
 Yong Chang (Samsung/TTA)
 *8月末退任

Steering Committee Leadership

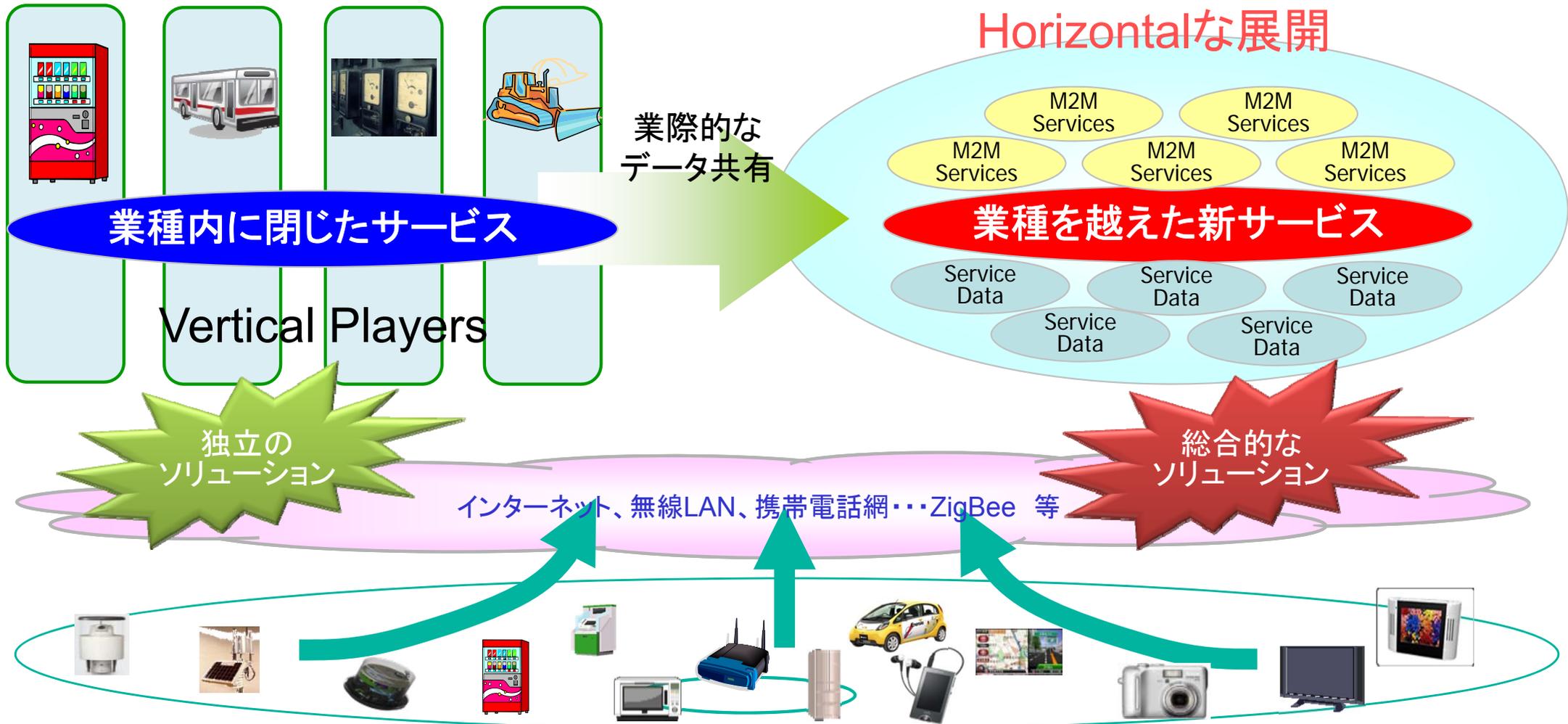
2014/7に選挙実施

Chair: Fran O'brien (Cisco/TIA)
 Vice Chair: Puneet Jain (INTEL/ATIS)
 Enrico Scarrone (Telecom Italia /ETSI)
 Thomas Li (Huawei/CCSA)

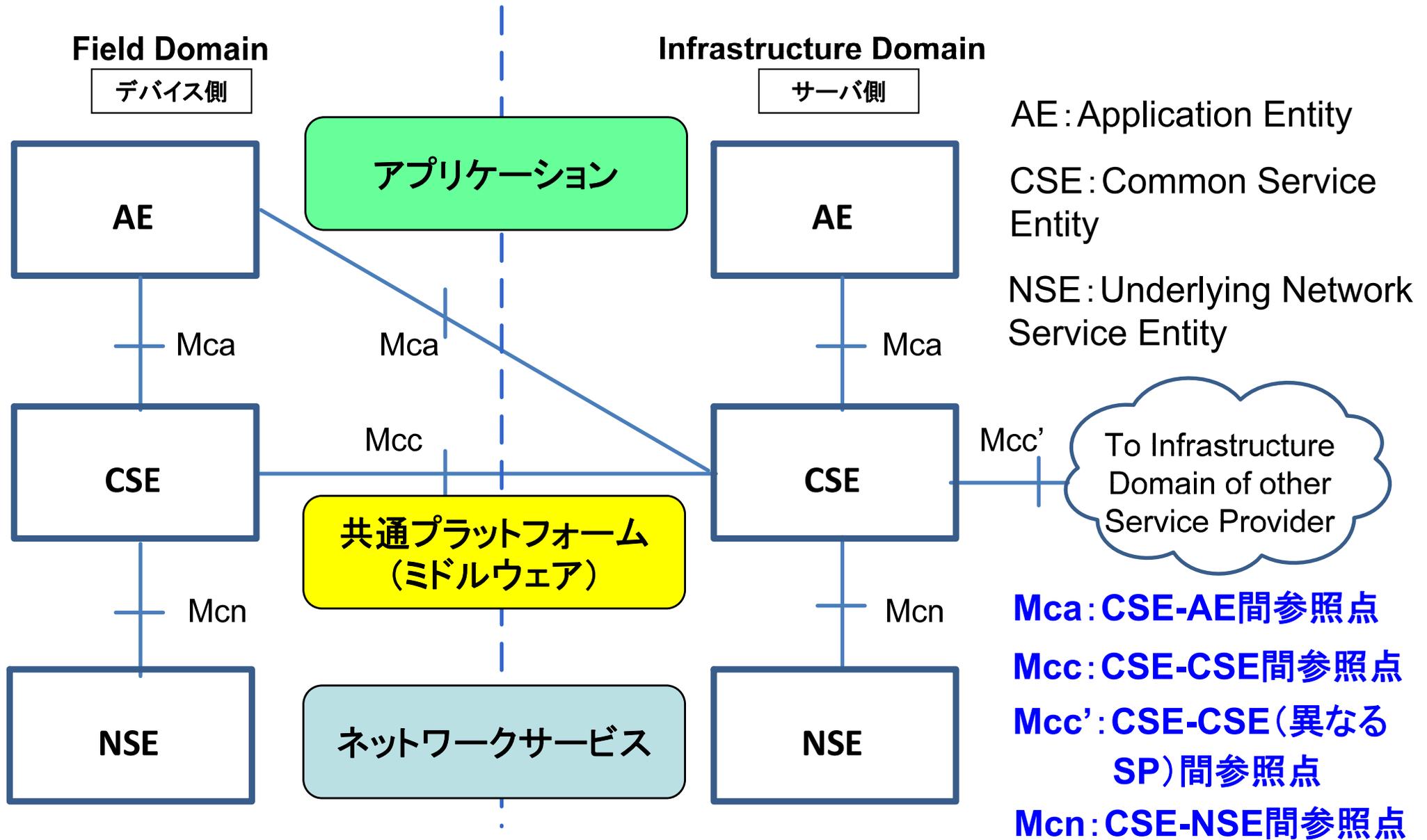
oneM2M標準化の特徴との狙い

oneM2Mが目指すM2M市場構造の変革

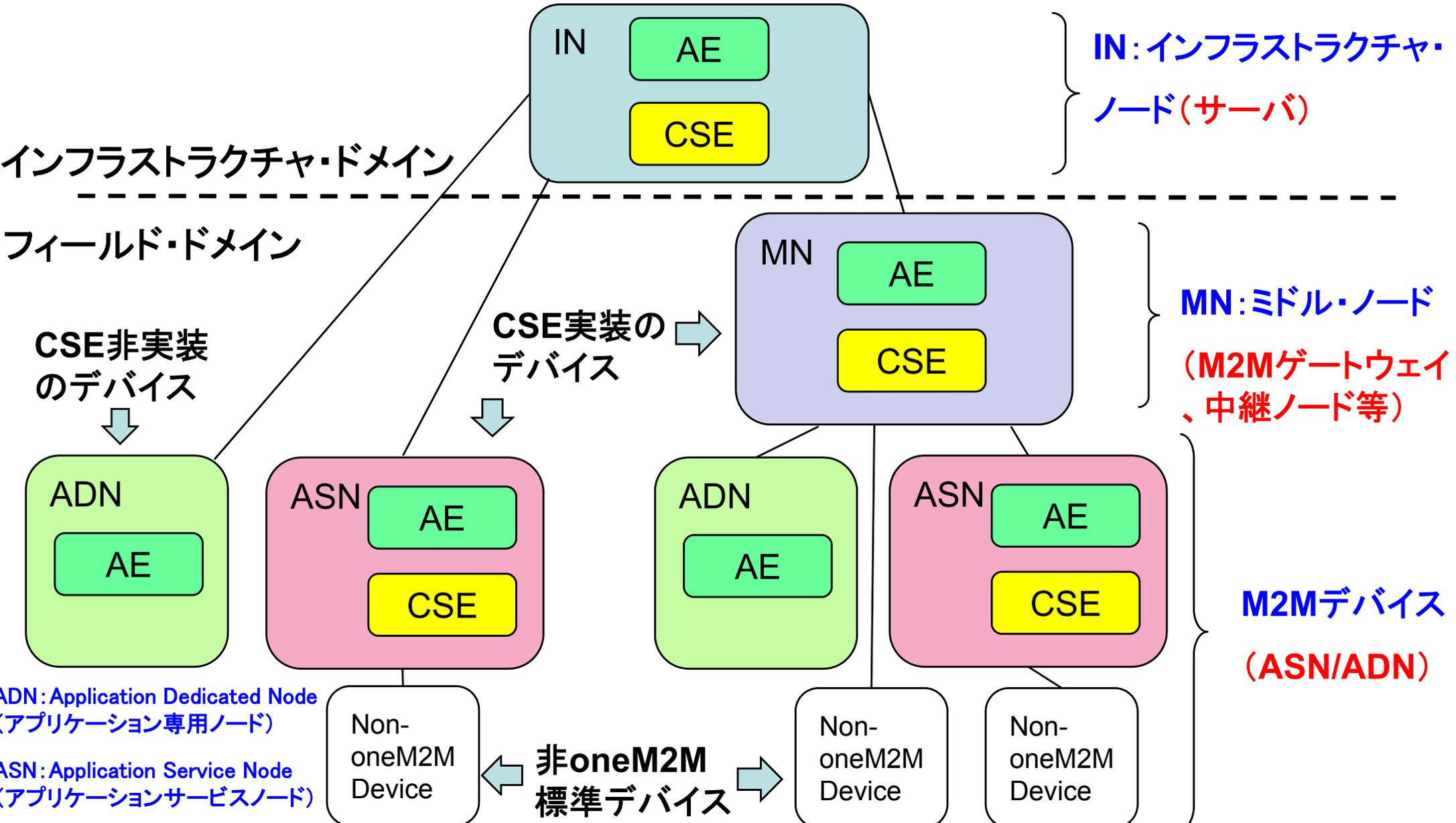
これまで個別に取り扱われてきた「モノ」の情報を、サービス間の境界を越えて、組み合わせたり、再利用することによって、新しいサービスの創造を期待。



oneM2M機能アーキテクチャ



oneM2Mアーキテクチャ(実装イメージ)



IN: インフラストラクチャ・ノード(サーバ)

MN: ミドル・ノード (M2Mゲートウェイ、中継ノード等)

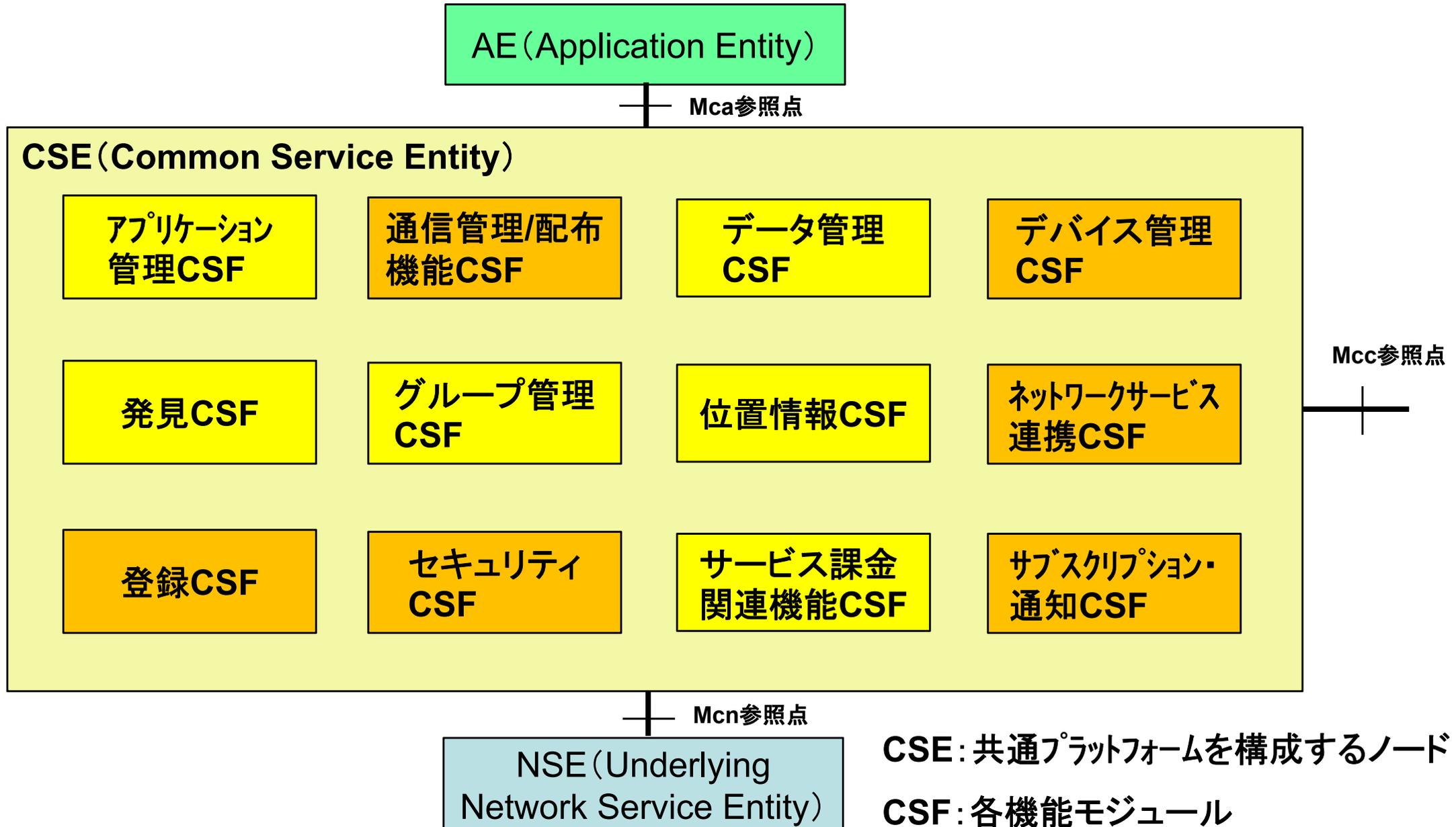
M2Mデバイス (ASN/ADN)

ADN: Application Dedicated Node (アプリケーション専用ノード)

ASN: Application Service Node (アプリケーションサービスノード)

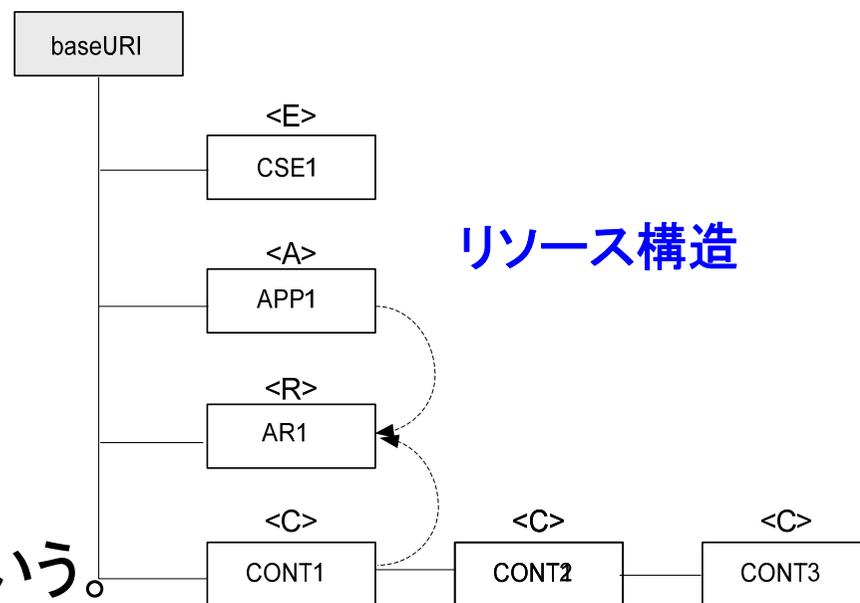
非oneM2M標準デバイス

共通プラットフォームの各種機能(CSF)



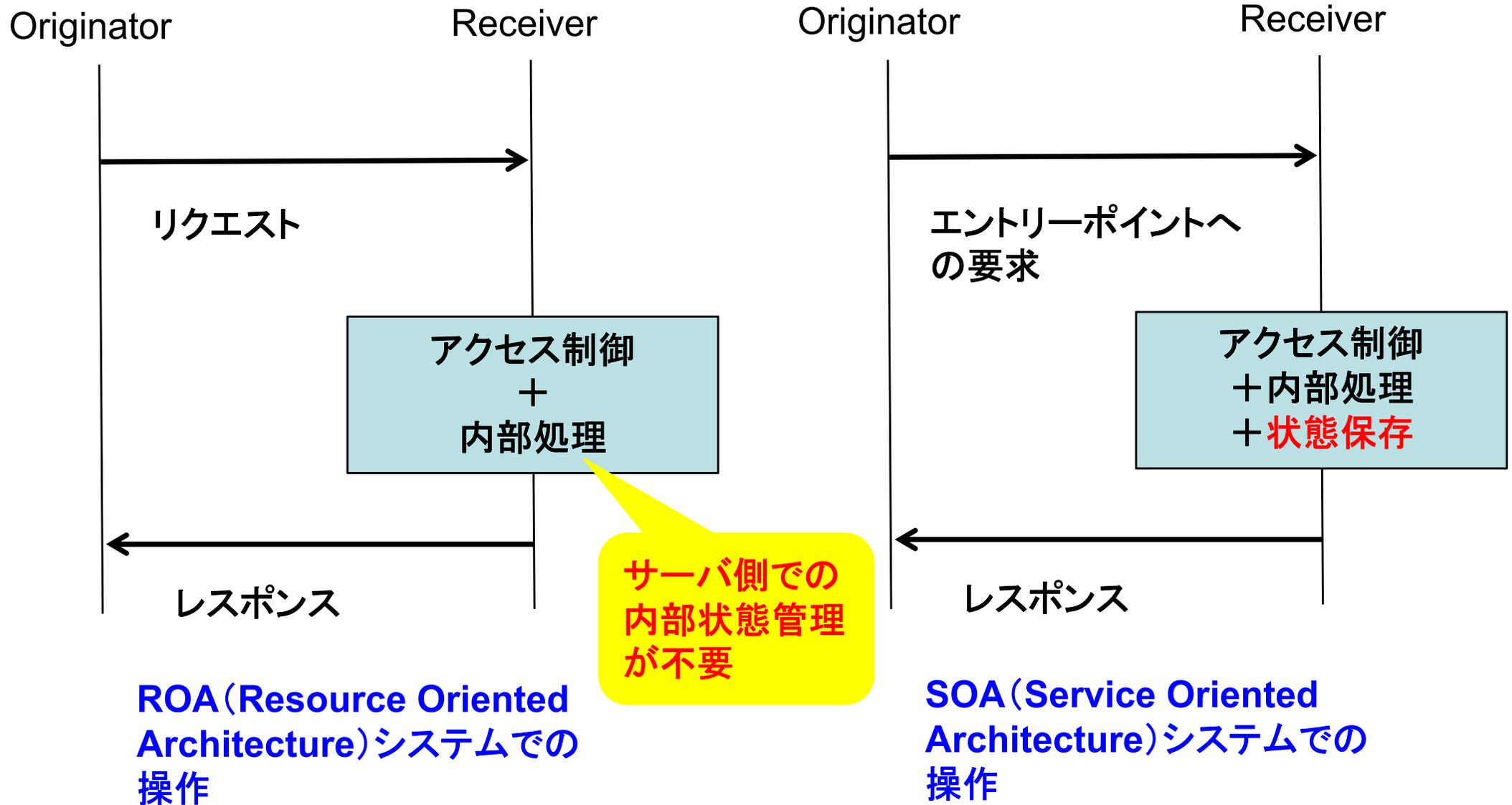
ROA: リソース管理とRESTful構造

- M2Mで取り扱われるシステムの利用やデバイス制御のために交換される情報はすべてユニークなアドレスを持つ**リソース**として規定。
- **Web設計思想のひとつであるRESTful*構造を採用。**
 - URIを指定することによりリソースを容易に参照できる。処理に必要なパラメータ（設定値、測定値等）はリソースを介して授受され、CSFで定義された処理毎に、これらのパラメータの読み書きが可能。
 - **Stateless**な操作が可能でサーバ側で内部状態を管理しないため、スケーラビリティが向上しシステム規模の拡張が容易。負荷分散が可能、故障に強いシステム構成。
 - メッセージ構造がシンプル、**Web系のプロトコル**との親和性が高い。
- **簡単なoperation (CRUD + notify; 後述)の採用で処理の簡素化。**
- **このようなアーキテクチャ設計指針をROA (Resource Oriented Architecture) という。**

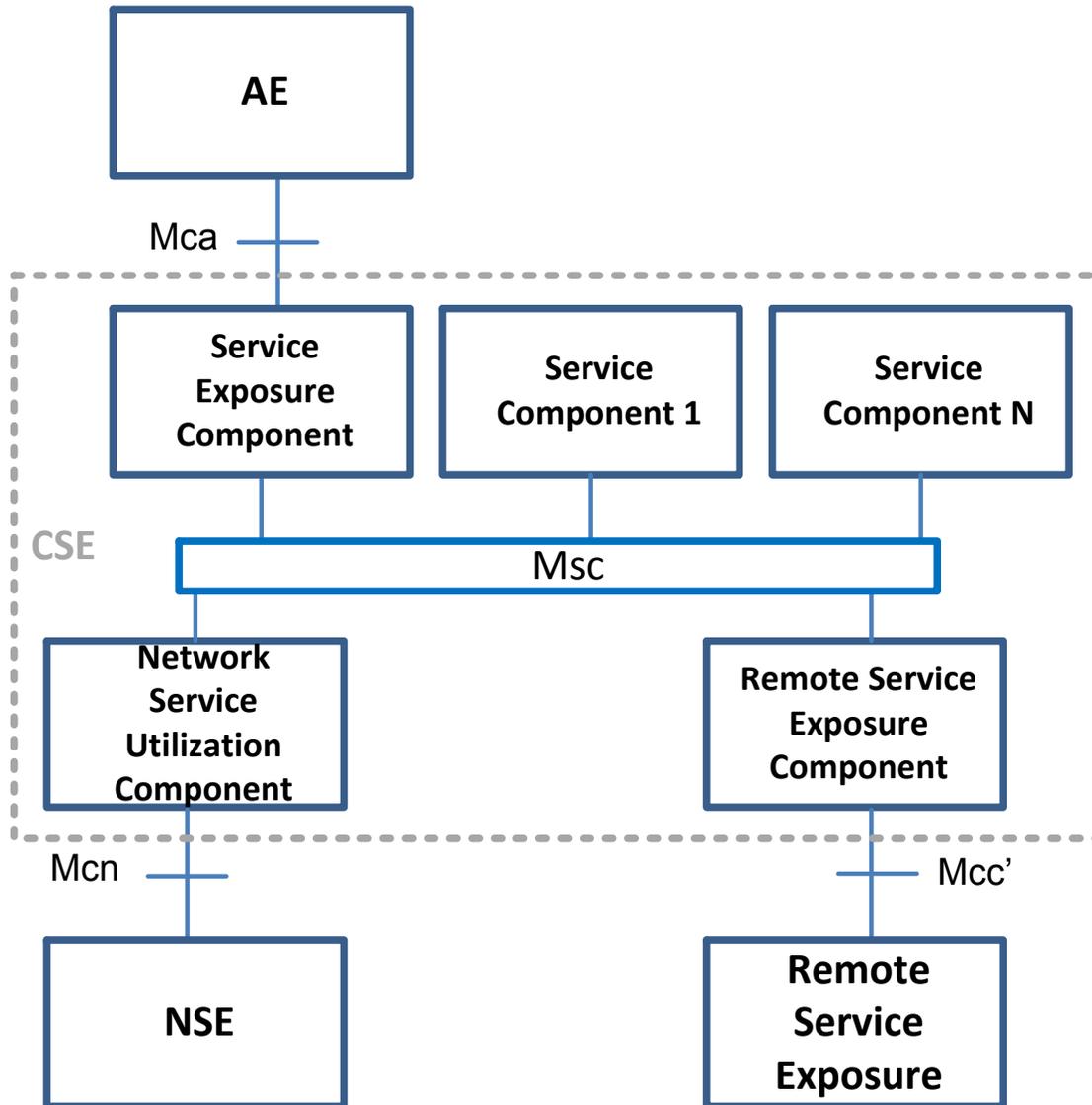


*REST: REpresentational State Transfer

参考: ROAとSOA



参考 : Service Component Architecture (SCA)



- ・ROAとは異なり、CSEを実際の **Service Component**ベース(ソフトウェアモジュール)で構成し、各サービス間のInterworkを行い易くするとともに、ユーザに対して、その機能(**Functionality**)を露出させ、どのようなサービスが可能なのかについてわかり易い構成となる (**SOA: Service Oriented Architecture**の要素の導入)

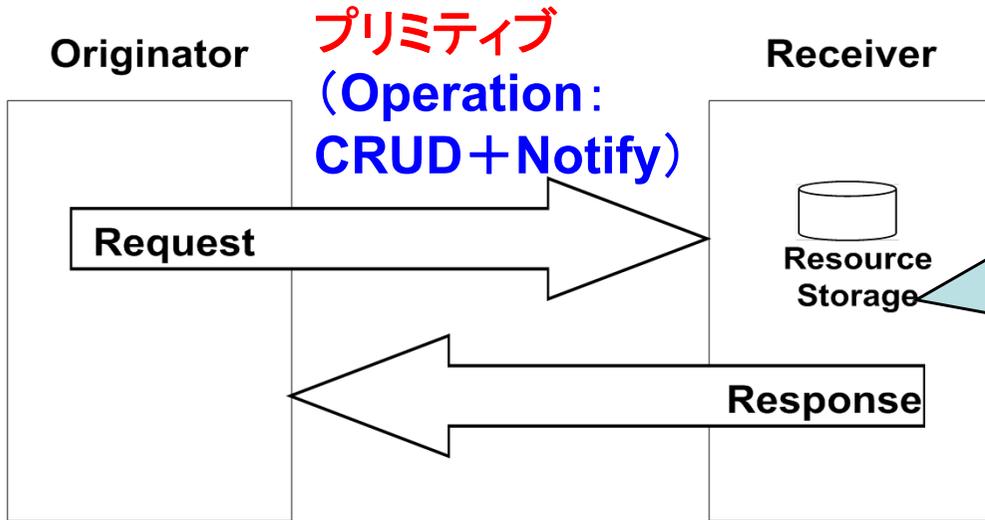
- ・フレキシブルなサービスの追加が可能のため、既存のベンダーソリューションの統合が行い易いところがメリットか

- ・提案元: ALU、Ericsson、Verizon、AT&T、ZTE、LGE、Orange

- ・次期リリースに向け策定中

Mca/Mcc上の通信メッセージフロー

- M2Mデータ交換用の通信フローについては、**Mca**および**Mcc**参照点上のフローを規定。

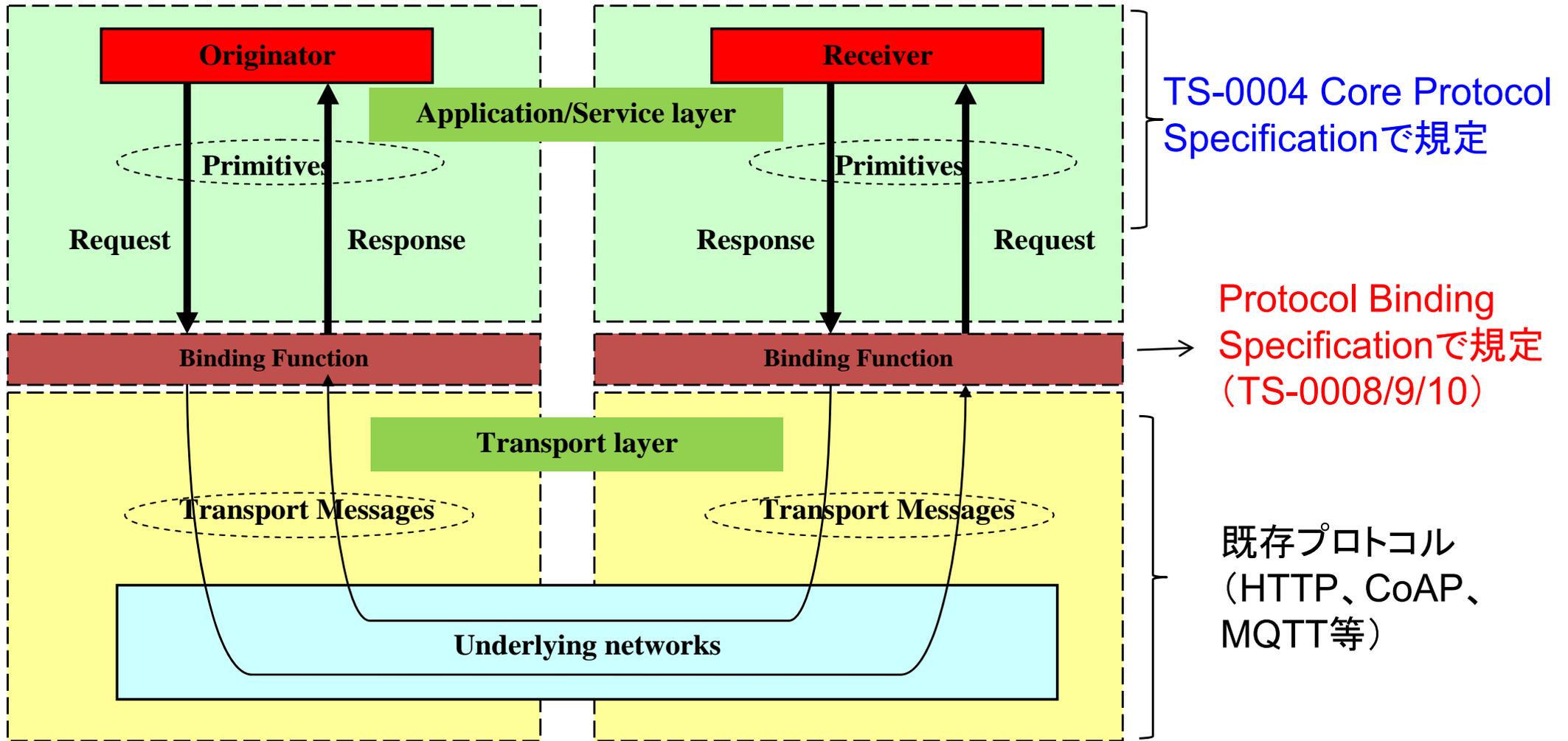


- 基本的には、**Request**と**Response**のプリミティブで規定。
- アプリケーションおよびCSEのいずれかからリクエストを開始できることが前提。
- アクセス制御及び状態の保存を指示(内部状態をサーバ側に持たない)

- **Mcn**上のフロー(CSE/Underlying Network間)については、アプリや通信事業者による既存のメッセージングサービスやOMA、GSMA等のNetwork API、3GPP MTCでのインターワーキングやセキュリティを参照する予定。

Operation	用途
Create	リソース情報の登録
Retrieve	リソース情報の参照
Update	登録済リソースの変更
Delete	リソース情報の開放
Notify	メッセージ送信

Mca/Mcc上のメッセージ伝送



Primitives: Request/Response, OperationはCRUD+Notifyで規定、binding機能により、transport layer message (HTTP、CoAP、MQTT等)にマッピングされる。

1. 共通プラットフォーム(CSE)は、各分野のアプリに共通に必要な機能をAPIにより提供(様々な分野に使い回し可能)

➤通信事業者やベンダーがプラットフォーム事業者となりCSEを提供すれば、M2Mサービス事業者はアプリとデバイスのみでビジネスが可能 ⇒ **ビジネスコスト低減により参入障壁が低下**

2. アクセス非依存

➤移動網、固定網を問わずUnderlying Networkにindependentなサービス層仕様

➤3GPP等と連携し、oneM2Mからの要求を反映

3. 既存M2Mプロトコルに対応、相互接続性を保証

➤多様なニーズを想定し、oneM2Mコアプロトコル(TS-0004)を規定し、共通データモデル(M2Mリソース)を介して異なるプロトコルを利用した相互接続を想定 ⇒ **スモールスタートが可能**

➤このため利用頻度の高い通信プロトコルについて、RESTful操作を定義したプロトコル・バインディングを仕様化し、異なるベンダー間の相互接続性を保証(当初は、HTTP、CoAP、MQTTの既存プロトコルへのバインディングを規定)

4. サービス層セキュリティや課金等を考慮

➤M2Mシステムに対する脅威分析、セキュリティサーキテクチャの検討

5. 既存ベンダーソリューションとのインターワークを想定

➤ROAをベースにSOAの要素を取り入れたSCA(Service Component Architecture)も検討、フレキシブルなサービス追加が可能で、既存ベンダーソリューションの統合が行い易い

6. M2Mデータの再利用や流通を可能とするセマンティックスの仕様化の検討

➤異なるインダストリー間での**データ利用の促進、新規ビジネスの創生**

初版技術仕様書 (V-2014-08)の公開

oneM2M標準化作業の流れ

- ① Use Case(ユースケース) TR(Technical Report; 技術報告書) の作成 (Potential Requirements含む) **初版2013年10月に完成**
- ↓
- ② Requirements(要求条件) TS(Technical Specification; 技術仕様書) の作成: **Stage1(初版リリース用'13年10月に承認)**
- ↓
- ③ Architecture(アーキテクチャ) TS の作成: **Stage2(初版リリース用、'14年2月凍結、6月承認、8月発行済み)**
- ↓
- ④ Protocol(プロトコル)等TSの作成: **Stage3(当初、'13年末完成目途だったが、Stage2の遅れで、'14年8月に凍結)**

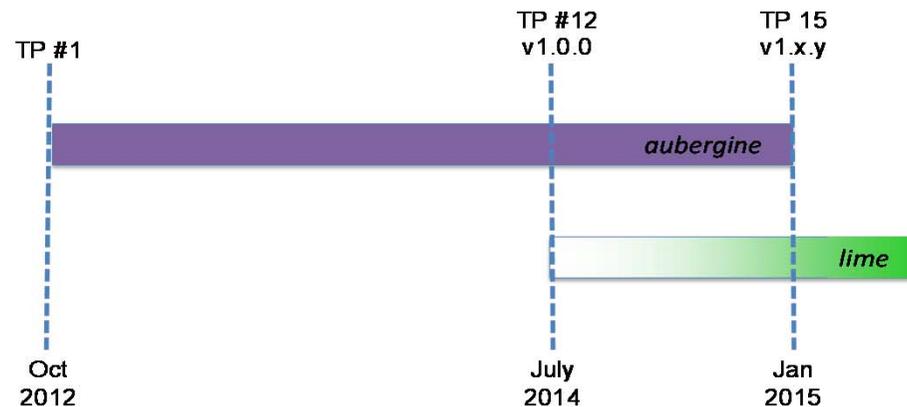
その他、セキュリティTS、デバイス・マネジメントTSを含めて、**2014年8月に初版となる V-2014-08版を公開、その後、内外からコメントを募集し、完成度を高め、2015年1月に改訂版を発行予定。**

また、各種技術報告書(TR:Technical Report)を、数件発行済/予定。

初版リリースと次期リリース

- 初版リリース用V-2014-08パッケージ(aubergine; 9件(次ページ))をTP#12 (2014年8月)で承認し、公開。
 - TP#12とTP#15 (2015年1月)の間は、Stage3の作業にフォーカスする。
 - V-2014-08に対しては、PT2やnonメンバからも広くコメントを募集。
 - TP#15の時点でそれまでに承認されたCR(Change Request)を反映し、V-2015-01パッケージを承認し、発行する。
 - リリースの対象はTS(Technical Specification)のみ、TR(Technical Report)は対象外。

- 次期リリース(lime)に関する新たなWIIは、TP#15まではStage-1とセキュリティ関連のNon-normativeなもののみ受け付ける(準備期間)。TP#15以降は完全に次期リリース作業に入る。



§7.6.1 of Method of Work includes:

An easy to remember name shall be associated to the Release (e.g. the year, a colour, or a fancy name).
aubergine and *lime* are placeholders for those names that are not yet agreed.

初版リリース仕様書パッケージ

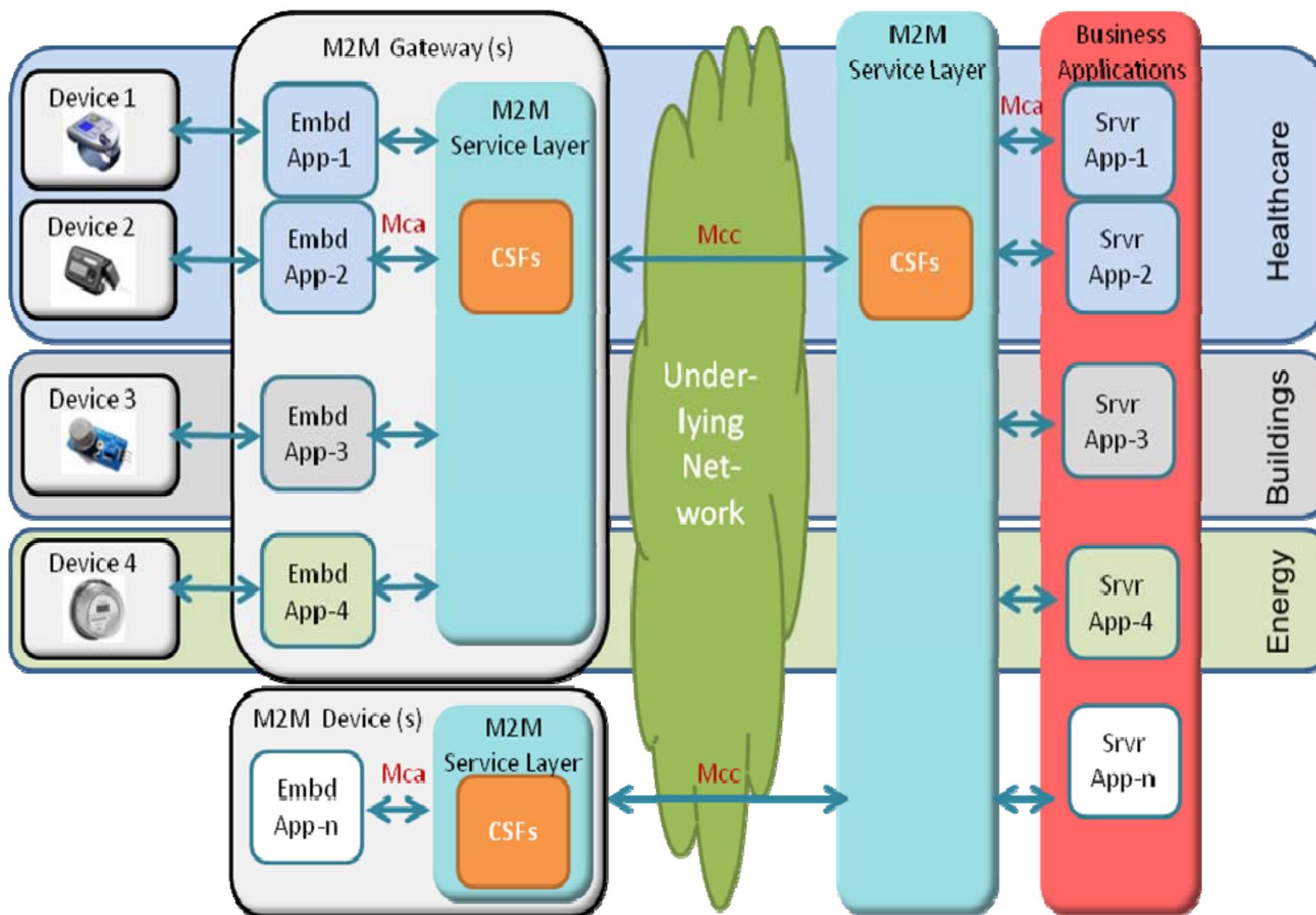
緑色が公開された仕様書

Deliverable	Version	Is Trigger?
TR 0001 - oneM2M Use Case collection	1.0.0	
TR 0002 - Part 1: Analysis of the architectures proposed for consideration by oneM2M	1.0.0	
TR 0003 - Part 2 Study for the merging of architectures proposed for consideration by oneM2M	1.0.0	
TR 0004 - Definitions and Acronyms[1] (定義と略語) ⇒ TS-0011に変更して承認	1.0.0	√
TR 0005 - Roles and Focus Areas	1.0.0	
TR 0006 - Study of Management Capability Enablement Technologies for Consideration by oneM2M	1.0.0	
TR 0007 - oneM2M Abstraction and Semantics Capability Enablement	1.0.0	
TR 0008 - Analysis of Security Solutions for the oneM2M System	1.0.0	
TR 0009 - oneM2M Protocol Analysis	1.0.0	
TR 0010 - oneM2M Device / Gateway Classification	1.0.0	
TR 0011 - MQTT Protocol Interworking Study	1.0.0	
TS 0001 - M2M Architecture (Stage2: アーキテクチャ仕様書)	1.0.0	√
TS 0002 - M2M Requirements (Stage 1: 要求条件仕様書)	1.0.0	√
TS 0003 - oneM2M Security Solutions (セキュリティ仕様書)	1.0.0	√
TS 0004 - oneM2M Protocol Technical Specification (プロトコル仕様書)	1.0.0	√
TS 0005 - oneM2M Management Enablement (OMA) (OMAデバイス管理技術の利用)	1.0.0	‡
TS 0006 - oneM2M Management Enablement (BBF) (BBFデバイス管理技術の利用)	1.0.0	‡
TS 0007 - oneM2M Service Components	1.0.0	
TS 0008 - CoAP Protocol Binding Technical Specification (CoAPプロトコルのバインディング)	1.0.0	†
TS 0009 - HTTP Protocol Binding Technical Specification (HTTPプロトコルのバインディング)	1.0.0	†
TS 0010 - MQTT Protocol Binding Technical Specification (MQTTプロトコルのバインディング)	1.0.0	†
† approval of at least one of TS 0008, TS 009, or TS 010 constitutes a trigger event. ‡ approval of at least one of TS 0005 or TS 0006 constitutes a trigger event.		

Initial Release Launch Event

- oneM2Mの活動と成果のアピールのためにLaunch Eventを企画
- 2014年12月9日(火)に実施、ETSI M2M Workshop(12/9-11、ソフィアアンティポリス)と共催
 - AMは、講演(oneM2Mの紹介や各仕様に関する説明)
 - PMは、デモンストレーション中心(Continua、ESMIG等やその他のベンダー)
- 関連スケジュール
 - 7/8 デモ用Tender発出(~9/30:デモ詳細締め切り)
 - 7/28 Communication/roll-out planの作成
 - 9/2 Agendaと講演者決定
 - 10/6 デモ用Agendaと講演者決定

Demonstrationの構成案



oneM2M次期リリースの展望

- **新世代M2Mコンソーシアム**がPartner Type 2として参加
 - OMA、Continua、HGI、BBFに続いて5団体目のPT2の加入
- **IEEE SA (Standards Association)**が参加を検討
 - Wi-SUN(IEEE 802.15.4)が協調・連携を視野に入れ活動
- **TSDSI (Telecommunications Standards Development Society, India)**がSC#19/TP#12に参加、正式参加を検討
 - M2M Communication WG ChairがTP#12に参加
- **欧州CEN/CENELEC**がSC#19/TP#12に参加、正式参加を検討
 - CEN(欧州標準化機関)/CENELEC(欧州電気標準化機関)は、ETSIとともに、EC(欧州委員会)からの指令を受け、スマート・グリッド、スマート・メータ等の標準化を推進

次期リリースへの期待

- 2015年1月～次期リリース向け作業の開始
- 想定される内容
 - SCA (Service Component Architecture)
 - セマンティックス (Semantics) 仕様書の作成
 - デバイス関連の標準化 (M2Mデバイス/ゲートウェイの分類、モジュール)
 - 新たなユースケースの収集 (Verticalsからの入力を期待)
 - コンフォーマンステスト仕様 (テストケース等の作成)
 - Home Domain Enablement

技術仕様(初版)の構成及び概略

日本電気株式会社

小林 中

技術仕様(初版)一覧

9件の仕様書がCandidate Releaseされた。

パブリックコメントが募集されている。(募集は2014年11月1日迄。)

(仕様書ダウンロードURL、コメント用テンプレート、問合せ先等の詳細は以下URLに情報あり)

仕様書番号	タイトル	リリース年月
TS 0001	M2M Architecture	2014-08
TS 0002	M2M Requirements	2014-08
TS 0003	oneM2M Security Solutions	2014-08
TS 0004	oneM2M Protocol Technical Specification	2014-08
TS 0005	oneM2M Management Enablement (OMA)	2014-08
TS 0006	oneM2M Management Enablement (BBF)	2014-08
TS 0008	CoAP Protocol Binding Technical Specification	2014-08
TS 0009	HTTP Protocol Binding Technical Specification	2014-08
TS 0011	Definitions and Acronyms	2014-08

Candidate Release仕様書のURL:

http://www.onem2m.org/candidate_release/

- スコープ(第1章)
 - エンドツーエンドでの下位伝送網の技術とは独立したサービス層にフォーカスしたoneM2M機能アーキテクチャ、機能エンティティ、エンティティ間の通信参照点の役割や振る舞いを定義
- アーキテクチャモデル(第5章)
 - 一般的なコンセプトでのレイヤーモデル(アプリケーション層、共通サービス層、ネットワーク層)、機能アーキテクチャ上のエンティティ(AE、CSE、NSE)と参照点(Mca、Mcc、Mcn、Mcc'、Mch)を定義
- oneM2Mアーキテクチャでサポートされる構成(第6章)
 - ノードの定義(IN、MN、ASN、ADN)、oneM2Mでサポート可能なノードとエンティティおよび参照点の間の関係を図を使って説明、共通サービスエンティティ(CSE)でサポートされる12の共通サービス機能(CSF)の役割を定義、他にセキュリティアспект、M2Mサービスプロバイダー内の通信におけるエンティティ間登録の組合せパターン、M2Mサービスプロバイダー間の通信における一般的な通信手順、M2Mサービスサブスクリプションなどの説明

- M2M 識別とアドレッシング (第7章)
 - M2Mシステムで使用する12の識別子を定義
- 参照点の記述とフロー (第8章)
- リソース管理 (第9章)
 - oneM2Mシステムにおけるリソースの概念 (全てのエンティティとデータはリソースで表現)
- 情報フロー (第10章)
 - McaとMcc/Mcc'参照点における操作毎 (Create、Retrieve、Update、Delete、Notify) の一般手順
- 信頼を可能にするアーキテクチャ (第11章)
 - 信頼を可能にするアーキテクチャとして、M2M登録機能、M2M認証機能、M2M認可機能の大きく3機能に分類
- 情報の記録 (第12章)

➤ 附属文書(参照文書、標準文書)

- Annex A 各共通サービス機能(CSF)とTS 0002で定義した要求条件との対応表
- Annex B oneM2Mシステムと3GPP MTC Release 11仕様の下位ネットワークとの相互接続に関連したMTCコンセプト、通信モデルなどの参考情報、ASN/MN-CSE起動による接続性確立手順、IN-CSE起動による3GPP定義Tsp参照点を通じた接続性確立手順などの説明
- Annex C oneM2Mシステムと3GPP2 MTC仕様の下位ネットワークとの相互接続に関連したMTCコンセプト、通信モデルなどの参考情報、3GPP2定義Tsp参照点を通じたデバイストリガー手順、SMSを使ったデバイストリガー機能などの説明
- 標準文書 ➤ Annex D oneM2Mのデバイス管理機能として、<mgmtObj>リソースのインスタンス詳細を定義
- Annex E CSEにおける最低限のリソース設定の内容を整理
- Annex F 既存の非oneM2Mソリューション／プロトコルとの相互接続或いは統合に関する考察と幾つかのアイデア
- Annex G M2Mサービス大別、サービスロールと関連リソースのまとめ表
- Annex H ITU-T, ISO/IECなどによるオブジェクトIDベースのM2MデバイスIDの概要

- 機能要件定義の標準仕様であり、次の分類毎に合計142の要件を定義。
 - システム全体に関わる要件: 72件 (OSR-001~072)
 - デバイス管理機能に関する要件: 17件 (MGR-001~017)
 - デバイス／データの抽象化とセマンティック: 10件 (ABR-001~003、SMR-001~007)
 - セキュリティ関連の要件: 26件 (SER-001~026)
 - 課金関連の要件: 6件 (CHG-001~006)
 - 運用関連の要件: 6件 (OPR-001~006)
 - 通信リクエスト処理に関する要件: 5件 (CRPR-001~005)
- その他
 - 非機能要件: 2件 (NFR-001,002)
- 記載された要件全てが初版で標準化された訳ではない。初版で標準化された要件がわかるように明記予定。

- セキュリティアーキテクチャ(第5章)
 - 3つの層(セキュリティ機能層、セキュリティ環境抽象層、セキュア環境層)の定義、設計原則、識別と認証、認可、ID管理、およびoneM2M全体アーキテクチャとの関係などの概要説明。
- セキュリティサービスとインタラクション(第6章)
 - oneM2Mイベントとセキュリティの統合、特にレイヤ間の関係作り、登録フェーズおよび運用フェーズにおけるハイレベルなセキュリティシーケンス、セキュリティ機能層における各セキュリティサービス(アクセス管理、サービス認可、セキュリティ証明の管理、ID保護、機微データの扱い、トラスト可能セキュリティ機能)の説明、セキュア環境抽象層におけるプロテクションレベルなど説明
- 認可(第7章)
- セキュリティフレームワーク(第8章)
- セキュリティフレームワークにおける手順とパラメータ(第9章)
- プロトコルとアルゴリズムの詳細(第10章)

➤ 附属の標準文書

- Annex D oneM2MサービスサポートのためのUICCセキュリティフレームワーク
- Annex F 位置ベースアクセス制御のための位置情報取得方法

➤ 附属の参照文書

- Annex A 3GPP GBAとの用語のマッピング
- Annex B 一般的な相互認証メカニズム
- Annex C 特定のセキュリティ環境技術に関連したセキュリティプロトコル
- Annex E M2Mサービスサポートのための厳密なUICCフレームワーク
- Annex G アクセス制御決定リクエスト

- プロトコル設計の原則と要求条件(第5章)
 - Mca/Mcc/Mcc'参照点におけるデータタイプ定義、基本的な構成要素(Primitives)の定義、およびXMLとスキーマ定義を提供するが、具体的なプロトコルへのバインディングは別書扱い。デバイス管理関連も定義。
 - Mcn参照点におけるデバイストリガと位置情報取得もAnnexで定義。
 - 設計原則としては、RESTful APIとし、スケーラビリティ、拡張性、効率性が求められる。
- oneM2MプロトコルとAPIの概要(第6章)
 - 通信プロトコルメッセージのためのデータ表現方法(各共通データタイプ、各メッセージパラメータデータタイプ、各リソースデータタイプ)、正常/準正常手順に関連したステータスコードなどを提供。

➤ oneM2Mリソース種別 (第7章)

- 各種リソース操作別 (Create, Retrieve, Update, Delete, Notify)、参照点別 (Mca, Mcc)、リクエストとレスポンス毎の各パラメータプリミティブ一覧、および各サービス手順における発信エンティティと受信エンティティのステップ毎の説明。

➤ 附属の標準文書

➤ Annex A リソースアトリビュート一覧

- リソースタイプとデータ名、略称、データタイプ、デフォルト値、取り得る値の制限などの情報。

➤ Annex B 3GPPデバイストリガの情報

➤ Annex D <mgmtObj>リソースインスタンスの詳細定義

➤ Annex G 位置情報リクエストの情報

➤ Annex H CMDHメッセージ処理

➤ 附属の参照文書

➤ Annex C XMLの例

➤ Annex E リソースへのアクセス手順

- Blocking方法(Ackなし)とNon-Blocking方法(Ackあり)

➤ Annex F oneM2MリソースタイプXSD定義ガイドライン

➤ Annex I oneM2Mリソース種別記述のテンプレート(7章用)

- oneM2MサービスレイヤとOMA DM技術との間のプロトコル変換とマッピングを定義
- OMA DM 1.3と OMA DM 2.0に対応(第5章)
 - 基本データタイプのマッピング、IDのマッピング、各種リソースのマッピング、管理手順のマッピング、DMサーバーとの連携、新しい管理オブジェクトなどを定義。
- OMA Lightweight M2M 1.0に対応(第6章)
 - 基本データタイプのマッピング、IDのマッピング、各種リソースのマッピング、管理手順のマッピング、新しい管理オブジェクトなどを定義。

- oneM2M管理リソースとBBF TR-181i2定義のデータモデル間のマッピング手順を定義
 - 基本データタイプのマッピング(第5章)
 - IDのマッピング(第6章)
 - リソースのマッピング(第7章)
 - 管理手順のマッピング(第8章)
 - サーバーとの連携(第9章)
 - 新しい管理技術固有のリソース(第10章)

- oneM2Mシステムで利用される通信プロトコルの内、CoAP (Constrained Application Protocol) プロトコル固有の部分を定義
- 概要 (第5章)
 - 要求機能、メッセージフォーマット、レスポンスのキャッシュ機能、複数リクエスト-レスポンスペアのブロック化機能
- oneM2Mプロトコルマッピング (第6章)
 - プリミティブのマッピング、オプションとクエリ文字列の構成、応答コードのマッピング、CSEにおけるリソースへのアクセス (Blockingケース、Non-Blocking非同期ケース、Non-Blocking同期ケース)などを定義
- セキュリティの考慮 (第7章)

- oneM2Mシステムで利用される通信プロトコルの内、RESTful HTTPバインディング固有の部分を定義
- 概要(第5章)
- HTTPメッセージマッピング(第6章)
 - Request-Lineのマッピング、Status-Lineのマッピング、各種Header Fieldsのマッピング、Message-bodyのマッピング
- セキュリティの考慮(第7章)

- oneM2Mシステム仕様書で使用される各種用語(第3章)と略語(第4章)の説明(アルファベット順)
- 例) 本セミナーの為に説明を翻訳
 - 3.2節 A
 - Access Control Attributes (アクセス制御アトリビュート)
 - アクセス制御のために査定されるルールとなり得る発信者・ターゲットリソース・環境などのパラメータのセット
 - 発信者のアクセス制御アトリビュートの例ではrole(役割)があり、環境のアクセス制御アトリビュートの例ではtime(時刻)、day(日付)、IP addressがあり、ターゲットリソースのアクセス制御アトリビュートの例ではcreation time(リソース生成時間)などがある。
 - 3.4節 C
 - Common Services Entity (共通サービスエンティティ)
 - M2M環境における共通サービス機能のセットの具体化を表す実体。尚、この様な共通サービス機能は、参照点を通して他のエンティティに提供される。
- 4.19節 R
 - RBAC (Role Based Access Control)
 - 役割ベースアクセス制御

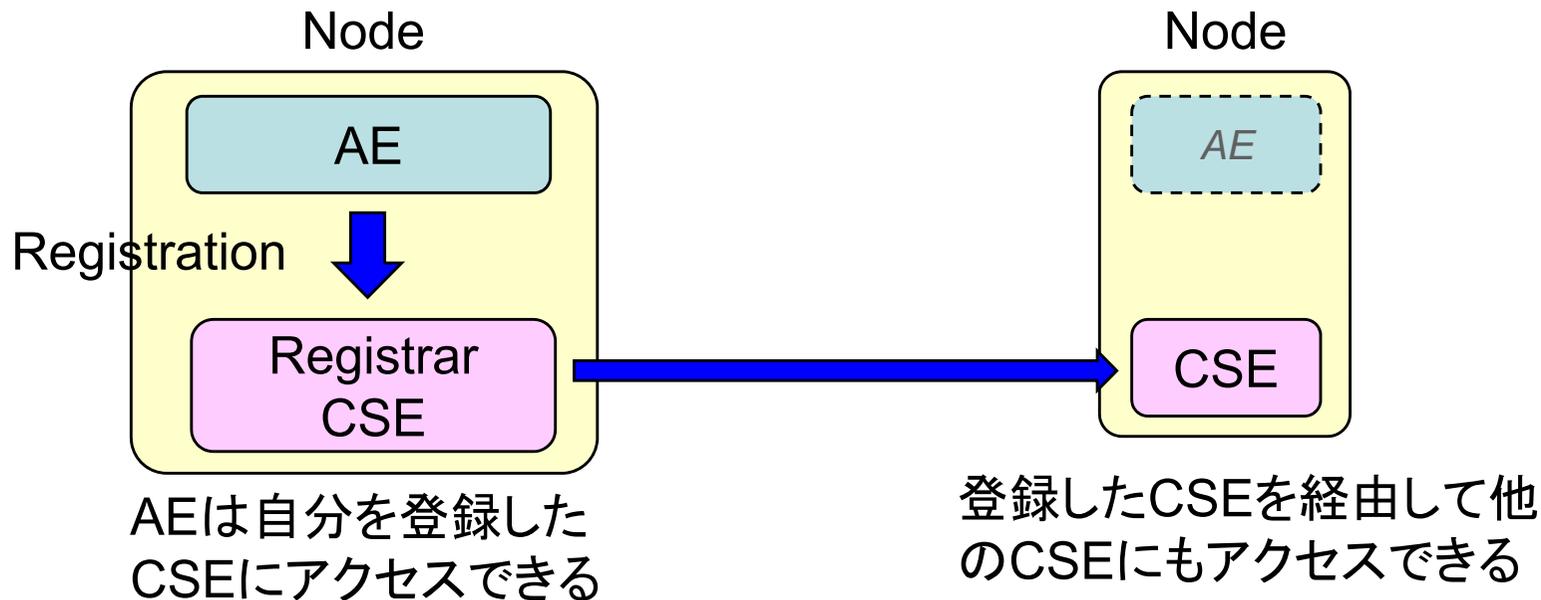
Registration

- CSEへのAE/CSEの登録手順 -

日本電信電話株式会社
後藤 良則

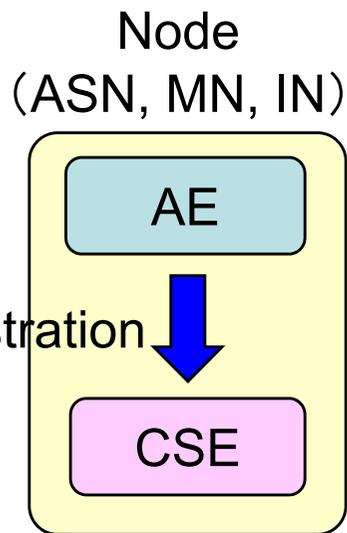
Registrationとは？

- CSEにAEや他のCSEを登録すること。登録することでAEやCSEはRegistrar CSEのサービスを利用できる。
- また、Registrar CSEを経由して他のCSEのリソースにアクセスできるようになる。

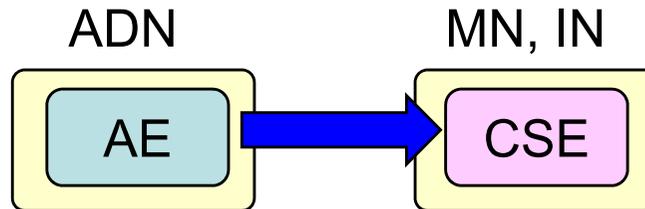


Registrationのパターン

- AE/CSEのCSEへの登録にはいくつかのパターンがある。基本的にAE/CSEは直近のCSEに登録し、下流のノードのCSEは上流のノードのCSEに登録していく。

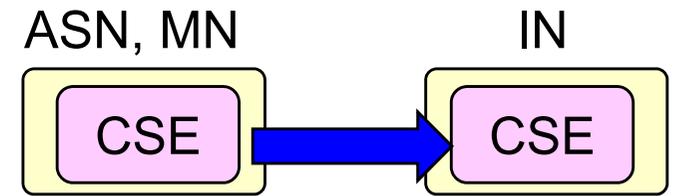


AEを搭載するnodeにCSEがある場合にはAEをローカルに登録



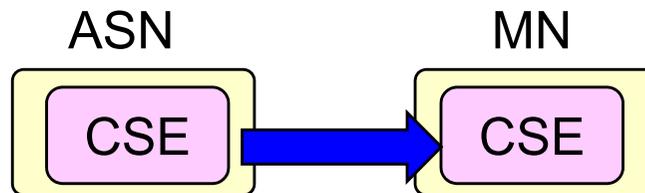
Registration

ADNに搭載されているAEはMNかINのCSEに登録



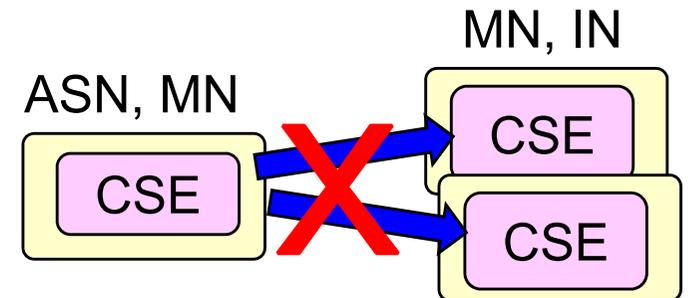
Registration

ASN, MNのCSEはINのCSEへ登録



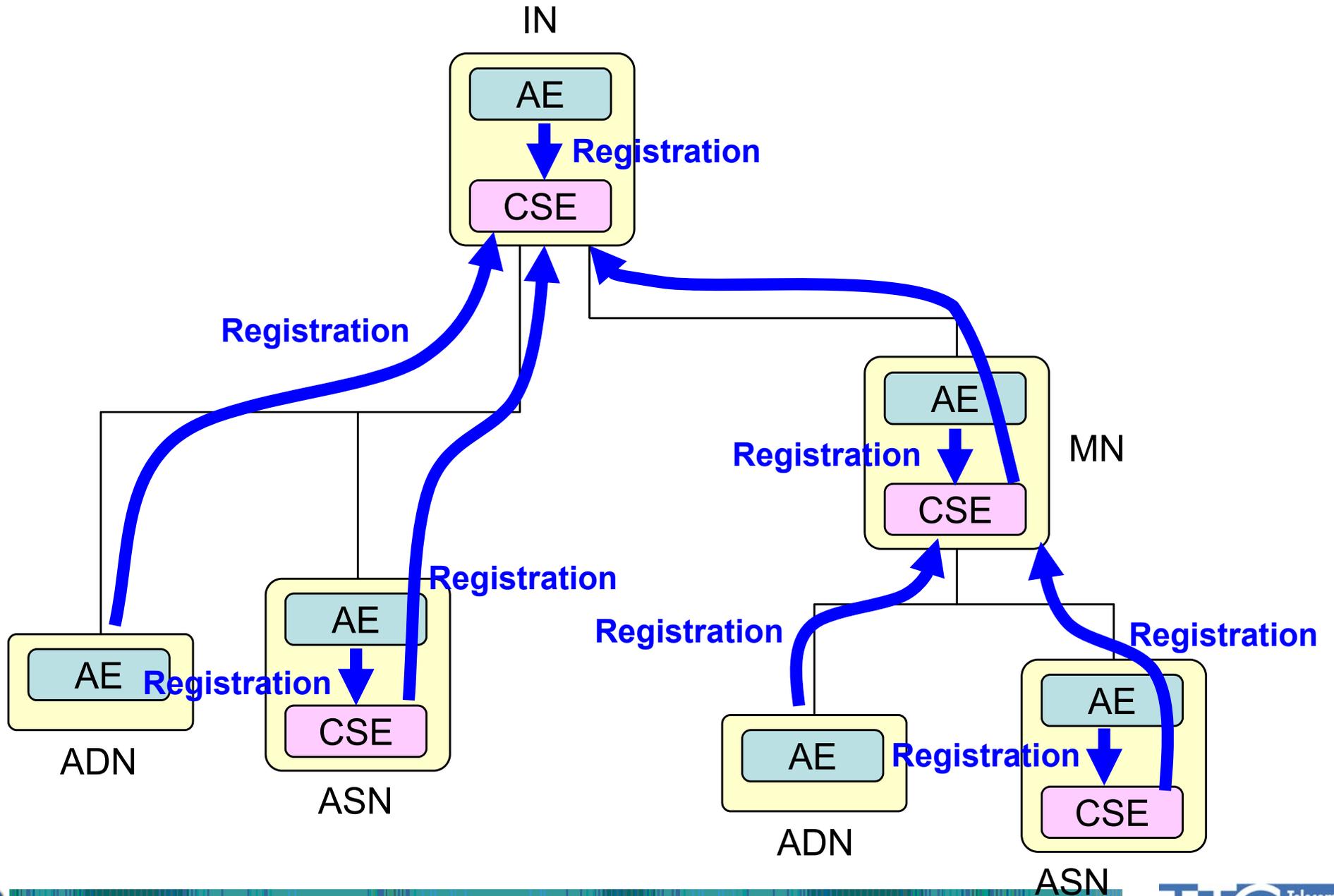
Registration

ASNに搭載されているCSEはMNのCSEに登録



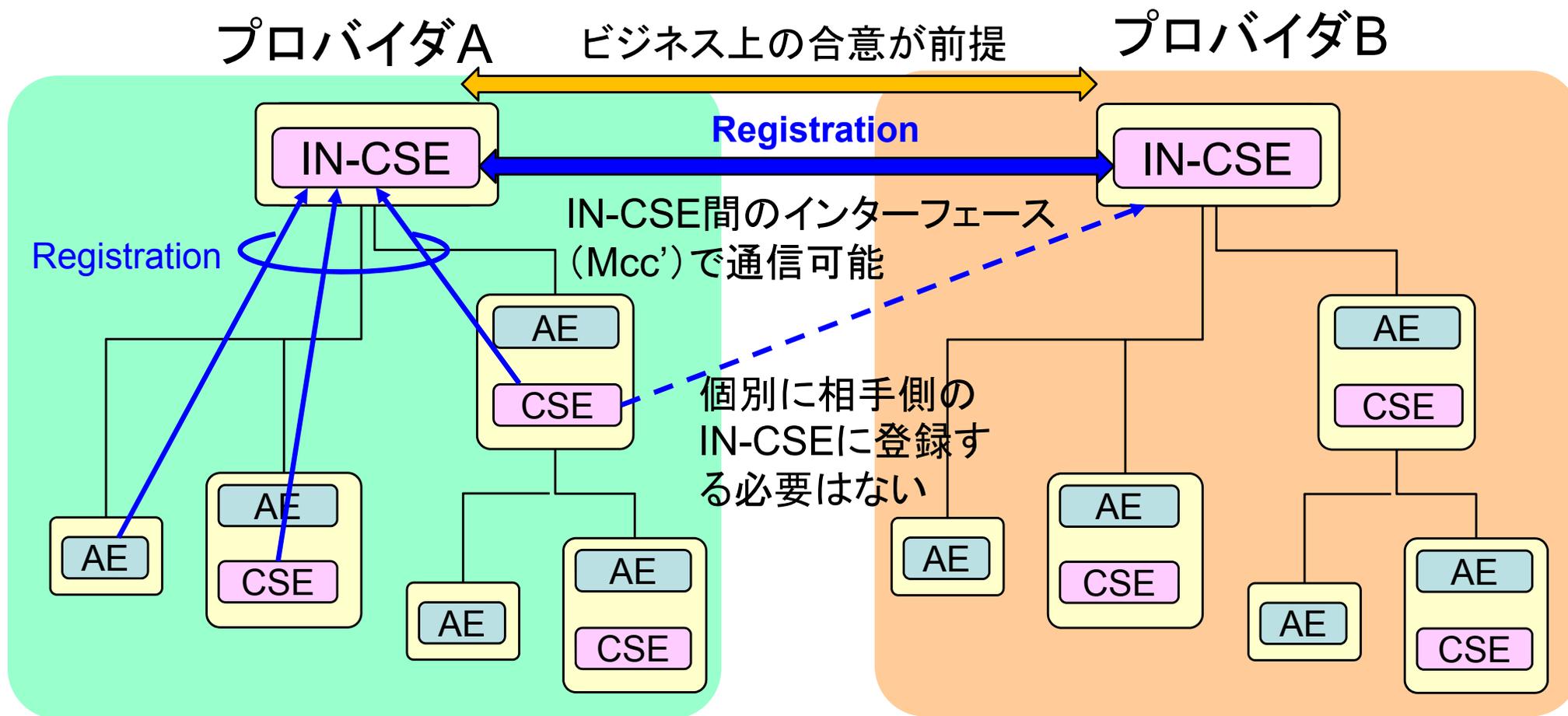
AEやCSEを複数のCSEに登録することはできない

Registrationのパターン



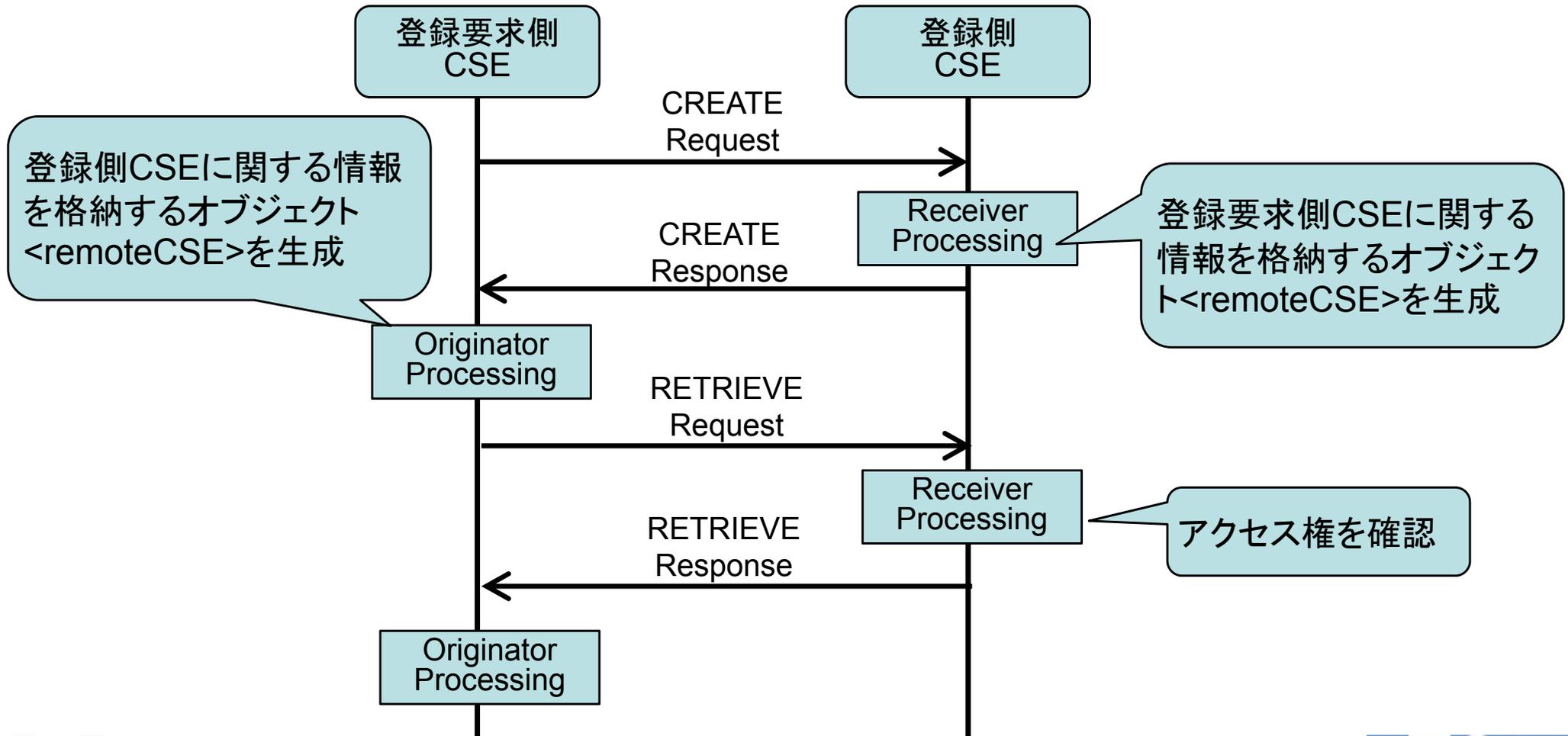
Registration: inter Service Provider

- AE/CSEは直近のCSEへ登録することで、その先のCSEへもアクセス可能。必要なリソースが他のプロバイダのCSEにある場合でも自分のプロバイダのIN-CSEを経由してアクセス可能になる。



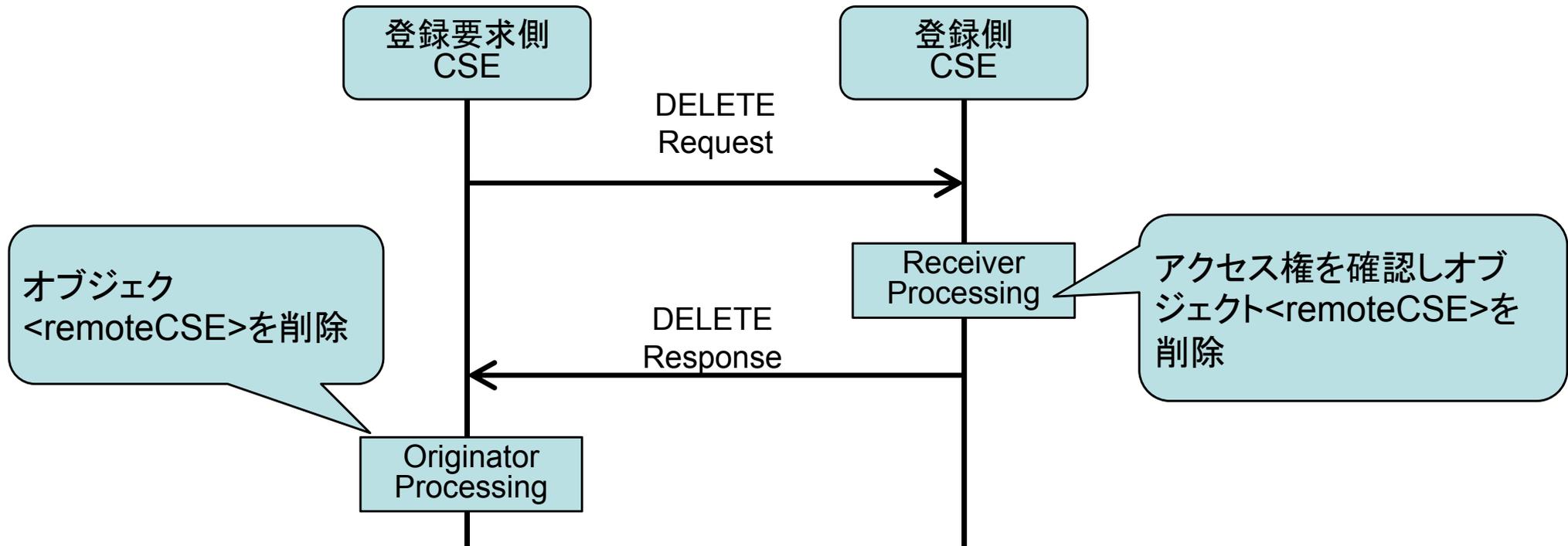
Registrationの手順 (CSE間の場合)

- CSEのRegistrationにより双方のリソースに<remoteCSE>オブジェクトを生成。登録要求はMN、ASNなどfield domain側から開始(プロバイダ間を除く)。



Deregistrationの手順 (CSE間の場合)

- Deregistrationは登録時に生成した<remoteCSE>を削除する手順。



まとめ

- AEやCSEは他のCSEに登録することで登録先のCSEとの情報を交換することができるようになる。また、登録先のCSEを経由して更にその先のCSEにもアクセスできる。
- CSEへの登録は直近のCSEへ行うのが基本。下流のノードのCSEから順次上流のノードに登録しIN-CSEに至る。
- プロバイダ間のCSEの登録はIN-CSE間で行われ、これによりMcc'を経由したプロバイダ間での情報のやり取りが可能になる。

Reference

- TS-0001 oneM2M Functional Architecture Baseline
 - 6.2.9 Registration
 - 6.4 Intra-M2M SP Communication
 - 6.5 Inter-M2M SP Communication
 - 10.1 Basic Procedures
 - 10.2 Resource Type-Specific Procedures

コミュニケーションマネジメント & デリバリーハンドリング (CMDH)

クアルコムジャパン株式会社
内田 信行

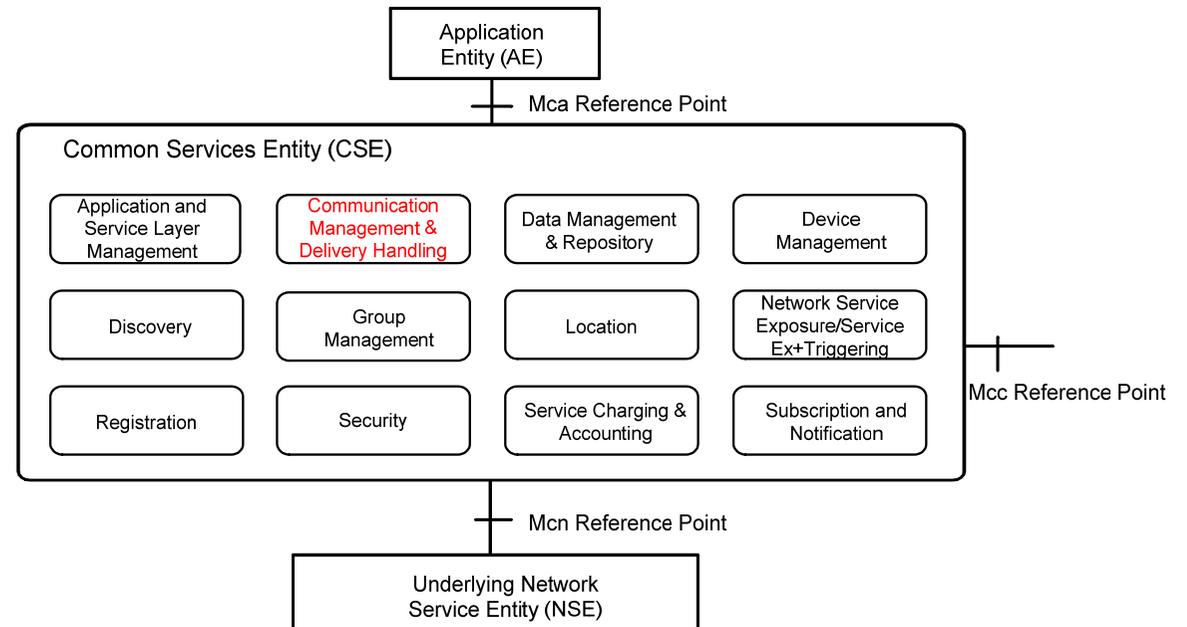
1. CMDHとは？
2. CMDHによるデータ転送の例
3. CMDH関連パラメータとポリシー
4. CMDHによるメリット
5. まとめ

➤ 参考

- Reference & Abbreviations

CMDHとは？

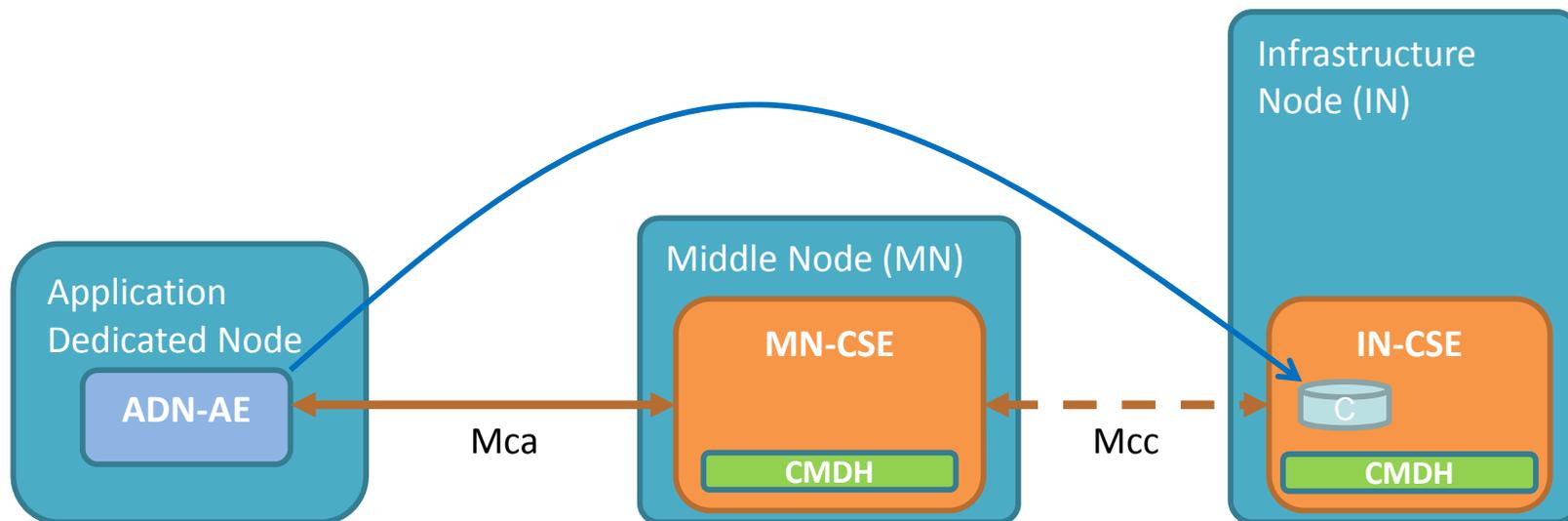
- 通信管理および配信処理に関わる機能を提供
 - 他のノードとの通信管理
 - 下位伝送網の選択 (LAN, WLAN, 3G, 4G etc.)
 - 転送スケジューリングおよびバッファリング
 - 少量データの一括転送



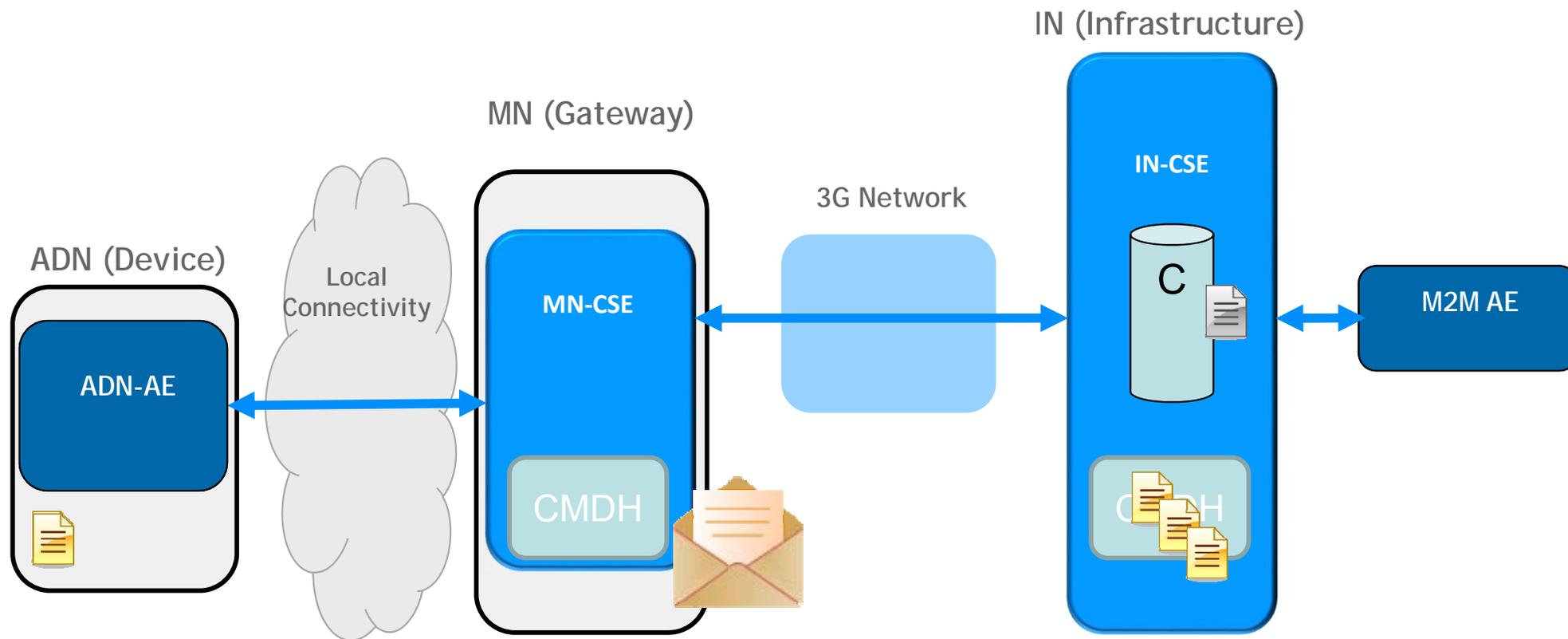
CMDHによるデータ転送の例①

➤ 前提条件

- ADNのアプリケーションがリモートリソースへアクセス
(eg. 温度センサからのデータを定期的にINへ更新)
- ADNとMNはローカルエリア常時接続
- MNとINは無線ワイドアエリア接続でオフライン状態



CMDHによるデータ転送の例②



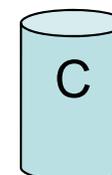
IN-CSEがM2M AEに対して、新規データの通知を行う

個別のリクエスト(UPDATE処理)を実施

Update //IN/C, ec = 3, rqt = 4am

MNのポリシー設定: ec=3 => 2amから5amにのみ転送

MN-CSEはADNからのリクエストを受領し、バッファリング



02:00 am
ストレージ

- リクエストに含むことのできるCMDH関連パラメータ
 - ec (event category)
 - CMDHポリシーに対応しているイベント処理設定
 - 定義済みカテゴリ: immediate, bestEffort, latest
 - rqt (request message expiration timestamp)
 - リクエスト有効時間
 - rset (result message expiration timestamp)
 - リザルト有効時間
 - oet (operation execution time)
 - オペレーション実施時間
 - rp (response persistence)
 - レスポンス保持時間
 - da (delivery aggregation)
 - 一括転送許容フラグ

参照資料: [1], Section 8.1.2

CMDHポリシー①

- CSEを持つノードに予めプロビジョニングされ、CMDH処理の詳細を決めるためのポリシー
- 以下の4つの要素から構成
 - Default
 - リクエストにCMDH関連パラメータが設定されていなかった場合に適用されるデフォルト値
 - Limit
 - CMDH関連パラメータのリミットを定義
 - Network Usage Rules
 - 下位伝送網を使用するための条件(使用時間帯、バックオフ値、データ量)
 - Buffering Rules
 - 許容されるバッファサイズやストレージの優先度

参照資料: [1], Annex D.12

CMDHポリシー②

Request Defaults

Scope	Context Condition	Parameter	Default Value
RequestOrigin	Applicable Context Condition	ec	0..N
		rqet	{duration}
		rset	{duration}
		oet	{duration}
		rp	{duration}
		da	On / Off

Request Limits

Scope	Context Condition	Parameter	Limit Value
RequestOrigin	Applicable Context Condition	ec	[N..M, X, Z ...]
		rqet	{duration range}
		rset	{duration range}
		oet	{duration range}
		rp	{duration range}
		da	[On Off On/Off]

Network Usage Rules

Event category / NW / Conditions	Rule	Value
0..N, <targetNetwork/scope>	schedule	<schedule>
	backOff	{back-off rule}
	minReqVolume	{data volume}

Buffering Rules

Event category	Rule	Value
0..N	maxBuffer	{data volume}
	Storage Priority	P

CMDHによるメリット

- 少量データを個別転送するとオーバーヘッドが大きくなるが、一括転送すれば下位伝送網を効率的に使用できる。
- 即時性を要さないアプリケーションデータはバッファリングし、トラフィックの少ない時間帯にスケジューリングすることにより、通信費用を低くすることが可能。
- 複数の下位伝送網が使用可能な場合、伝送網を選択できる。
- M2Mのオペレーションコストを下げる事が可能に！

まとめ

- CMDHは通信管理および配信処理機能を提供
- CMDHパラメータやポリシーに基づくきめ細かな処理設定が可能
- 少量データの一括転送、下位伝送網の選択およびスケジューリングによって、常時接続ではない環境で効果を発揮
- M2Mのオペレーションコスト削減に寄与

[1] **oneM2M TS-0001 V-2014-08** oneM2M Functional Architecture

http://www.onem2m.org/candidate_release/TS-0001-oneM2M-Functional-Architecture-V-2014-08.pdf

[2] **oneM2M TS-0004 V-2014-08** oneM2M Service Layer Protocol Core Specification

http://www.onem2m.org/candidate_release/TS-0004-CoreProtocol-V-2014-08.pdf

- ADN: Application Dedicated Node
- AE: Application Entity
- CMDH: Communication Management and Delivery Handling
- CSE: Common Service Entity
- IN-CSE: Infrastructure Node CSE
- M2M : Machine To Machine
- MN-CSE: Middle Node CSE

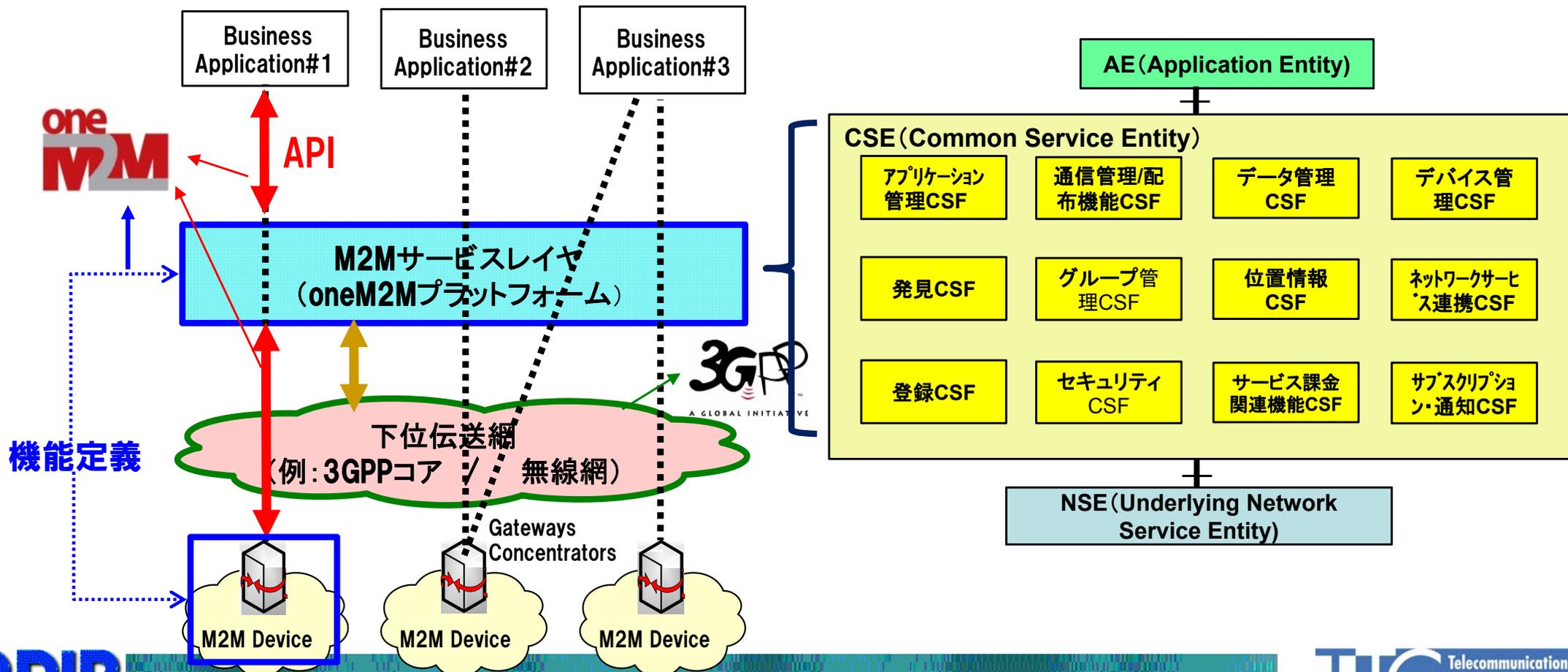
デバイス・トリガリング及び下位伝送網 との連携(インターワーキング)機能

株式会社NTTドコモ
輿水 敬

アウトライン (お伝えしたい骨子)

- #1: oneM2Mトリガリング機能と下位伝送網連携
 - 必要性・ねらい、留意点、M2M端末の特徴
- #2: 3GPPのMTC関連機能概要
 - Rel-11のMTC基盤を例とした下位伝送網
- #3: トリガリング機能方式の紹介・仕組み
 - 実際の方式紹介・特徴・ソリューションの重視点
- #4: まとめ/将来拡張
 - Rel-11から今後に向けて、更なる機能改善の可能性

- oneM2Mと3GPP下位伝送網のIWG(全体像)・ねらい
- 青い部分が、oneM2Mで検討されている、M2Mサービスレイヤ(oneM2MサービスPF)
- その下の下位伝送網(例:3GPP網)は、アンダーレイNWと呼ばれる
- 上下で機能があるだけでなく、しっかりとした相互接続性・インターワーク能力が必要



- デバイス・トリガリング、インターワーク機能のねらい・留意点
 - oneM2Mサービス・プラットフォーム[1]と伝達網である3GPP_MTCアンダレイNW[2]とのインターワーキング(相互連携)を実現する技術方式。
 - oneM2Mサービス・プラットフォームの機能は伝達網と一体となった組として機能すべきで、この様なインターワークは必須の機能であると考える。

デバイストリガリング方式の留意点

- 1) IN-CSEでM2M-UEのステート(電源断、接続済、ドーマント)を考慮し着信挙動を変化
 - 2) M2M-UEは上記ステート変更が発生する場合は、更新ステートをIN-CSEに送信する
 - 3) 保持するM2M-UEステート情報及び、AEからの着信コンテンツをIN-CSEが勘案し、トリガリングメッセージの動作と含める情報を決定し着信動作を実行
- この様な動作方式により、oneM2M-PFはUEのステート状態に応じ、適切な着信手順を動作する事が可能、多様な目的に沿った制御、高信頼性動作が実現可能に。

M2M/IoT/MTC端末の特徴とデバイス・プロキシ コンセプト(重要な概念)

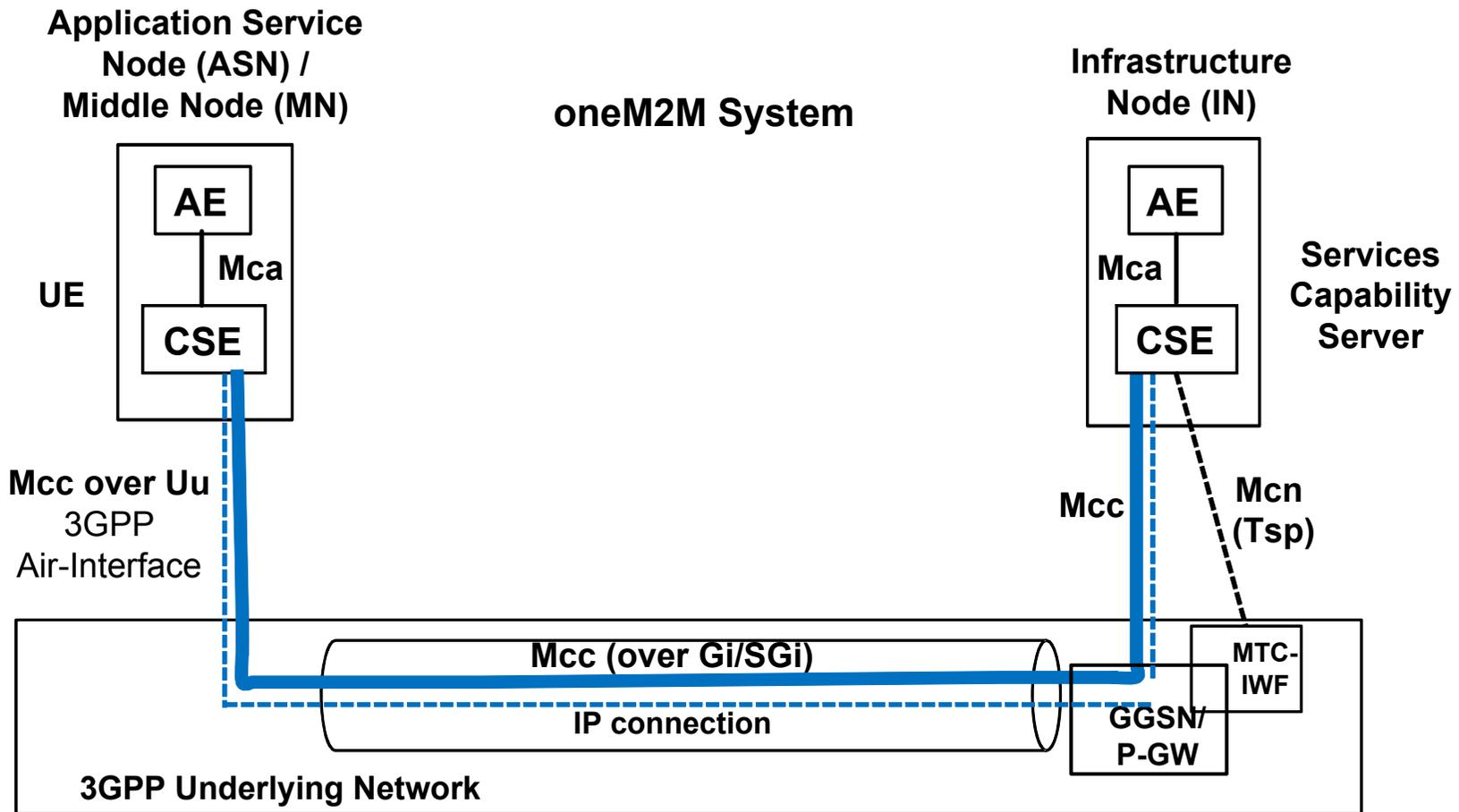
- **M2M端末の特徴** :殆ど寝ている、小容量の時々通信、小電源、小さく多数
- **デバイス・プロキシ**:この様な特徴のエンド端末の代理をさせるコンセプト
 - The Sensor Proxy (i.e., MTC-device-Proxy) represents on behalf of physical device nodes.
 - This enables MTC-devices stay still sleep and power-off mode even if the Clients sends a push request. Because of this mechanism, the concept of REST can be realized and MTC-GW need to work for this function.

(M2M communications, Boswarthink, Elloumi, et.al., Wiley[3]からの抜粋です、転用禁止)

#2: 3GPPのMTC関連機能概要(1/2)

➤ oneM2M-PFと3GPP下位伝送網のつながり(機能全体像)

oneM2M TS-0001[1], Annex B.4



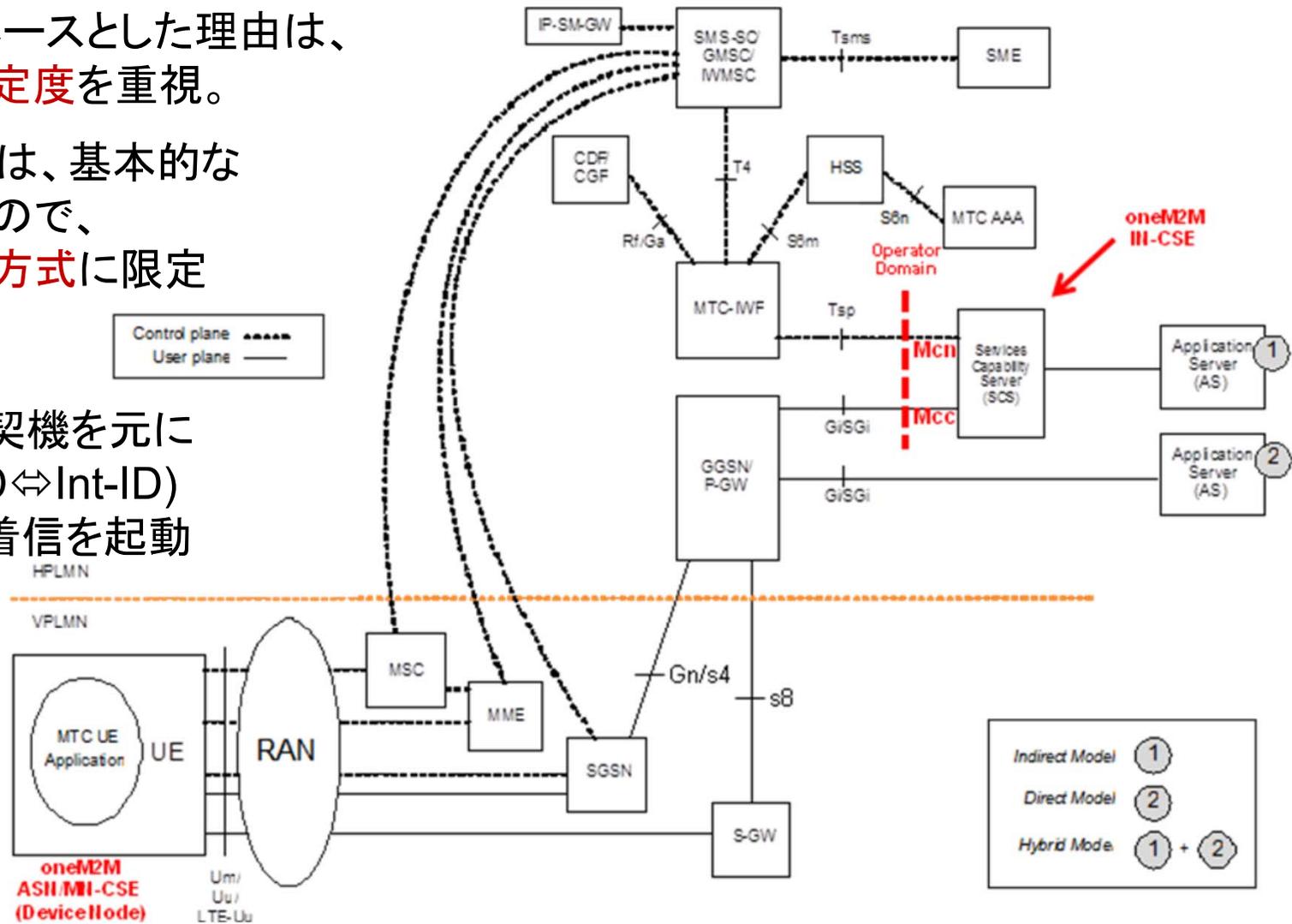
#2: 3GPPのMTC関連機能概要(2/2)

➤ Rel-11のMTC基盤例とした下位伝送網 (TS 23.682 v11.5.0)[2]

☆Rel-11のNWをベースとした理由は、機能の**完成度**や**安定度**を重視。

☆従って能力としては、基本的なMTC機能のみですので、トリガリングは**SMS方式**に限定

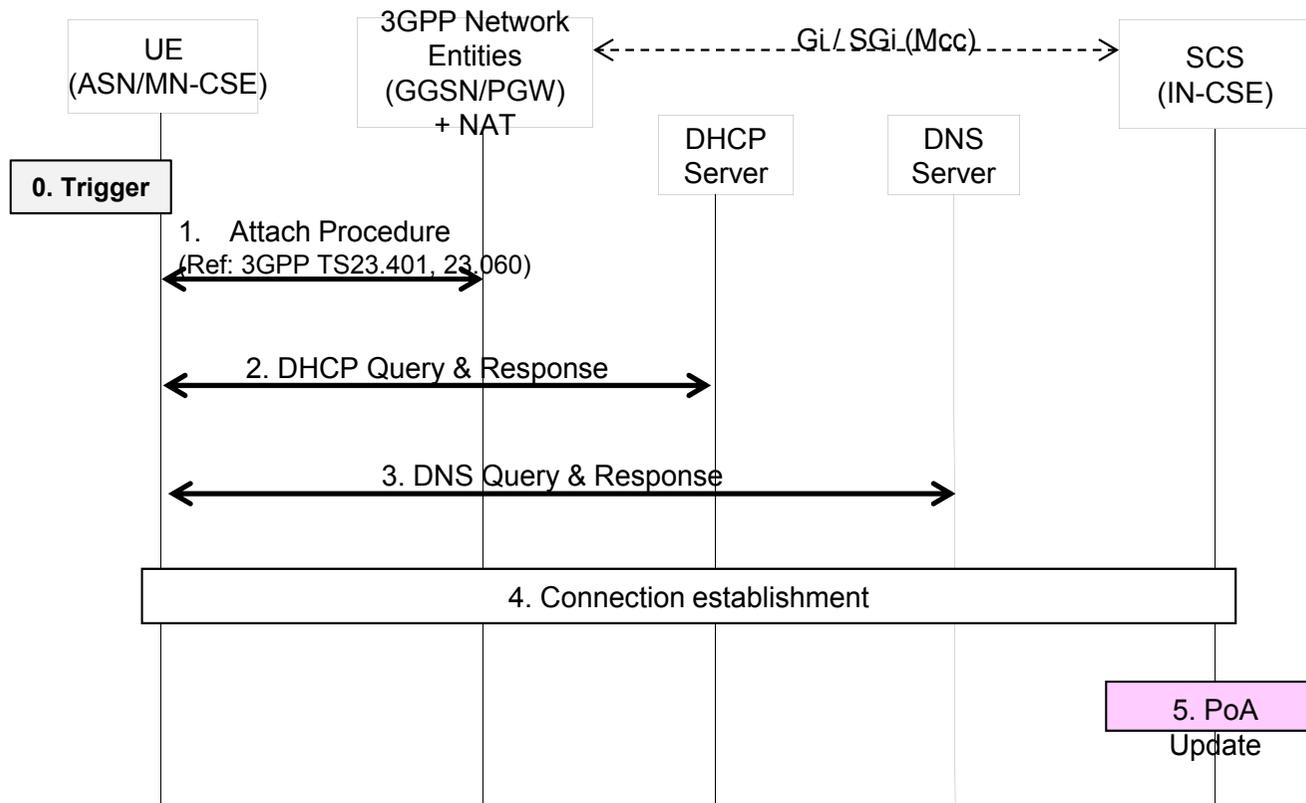
☆SCSからの着信契機を元に**MTC-IWF**が(Ext-ID⇔Int-ID)変換、その後SMS着信を起動



#3:トリガリング機能方式の紹介・仕組み(1/2)

端末側からのIN-CSEへのコネクション形成手順 (UE initiated)[1] B.6.1.1

- UE(ASN-CSE)からIN-CSEにこのアタッチ手順を経てUEの宛先アドレスを登録させる。IN-CSEでは、UEを特定できるID(M2M-Ext-ID)とこの端末の宛先アドレスの組をIN-CSEに保持。
- UEステート状態(例えば電源断、ドーマントステート等)の変化時、IN-CSEに通知。IN-CSEではこのステート(接続中含)も保持し、その後のIN-AEからの着信コンテンツも勘案し、着信挙動を選択させる手順が工夫の部分。

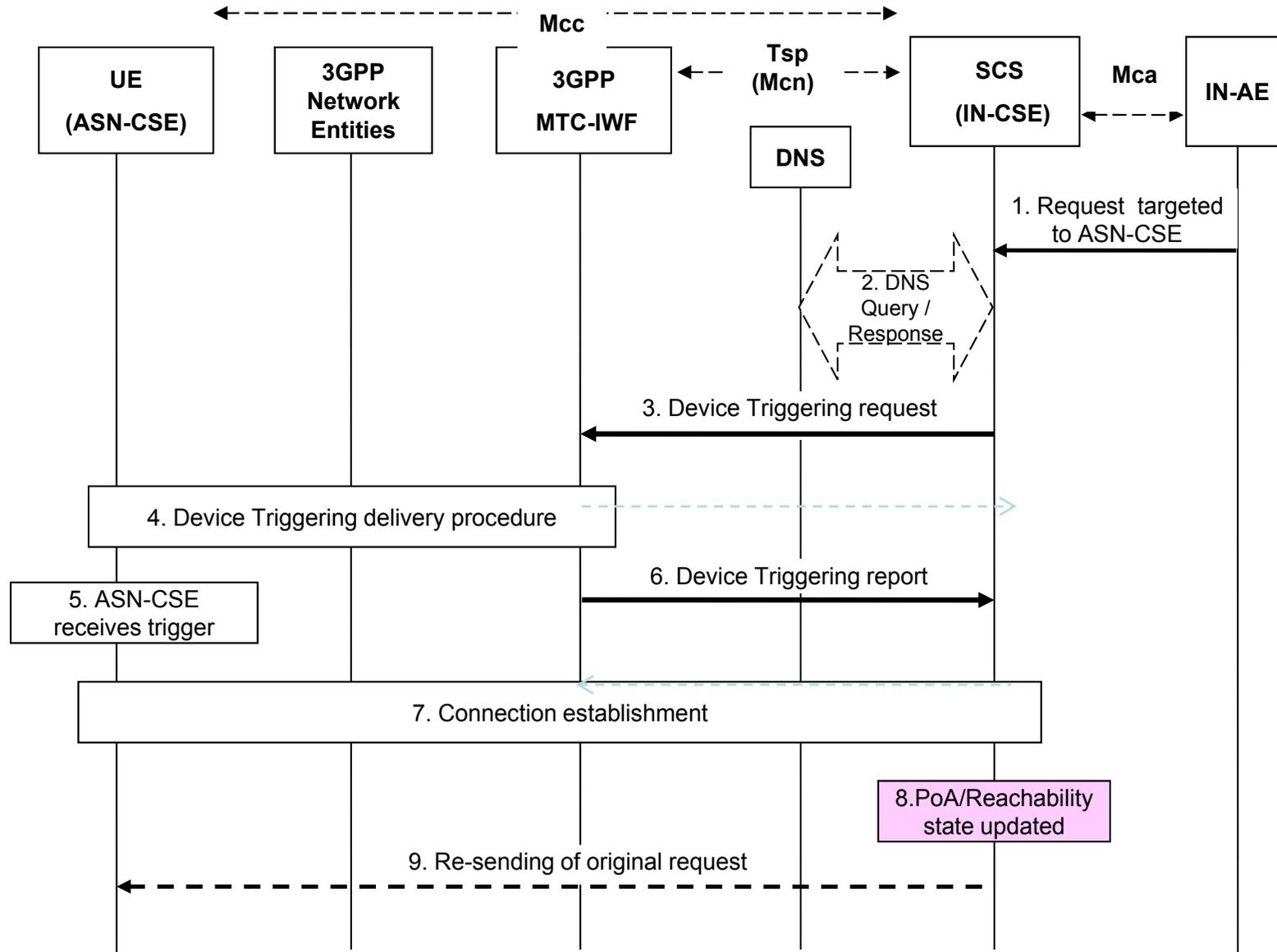


UEのステート状態(例えば電源断、ドーマントステート等)が変わった場合には、IN-CSEに通知(step4に含)。IN-CSEでは、このステート(接続中含)を保持し、着信動作を選択する。

IN-CSEにおいて各UE-IDとその初期宛先アドレスの組を保持させる(@REG/NSE-CSE)

#3:トリガリング機能方式の紹介・仕組み(2/2)

➤ IN-CSE から端末への コネクション形成手順 (NW Initiated) [1] B.6.1.2



➤ まとめ

- oneM2Mと3GPP_MTC網を例とした、**デバイス・トリガリング手法**と、**インターワークの手順、ねらい、特徴等**を説明しました。
- Rel-1では、この様に**oneM2M-PF**と下位伝送網とが**一体**となりかつ、**連携**の取れた利用が可能になっています。

➤ 将来拡張

- 今後は、3GPP網の機能拡張も進み、より一層の連携が高まるものと考えます。例えば、
- 3GPP_Rel-13のAESE, MTC_Groupe, MTC_Monte等も有用な機能と考えています。
- また、トリガリング手法もSMSから多様なトリガリング手法が使える可能性も残しており、一層の機能連携を通し**より利便性の高い、M2Mサービス提供基盤**となる事を、期待しています。

- [1] **oneM2M TS-0001 v1.1.0**, oneM2M Functional Architecture, 2014-Aug-04, ARC-2014-1518.
- [2] **3GPP TS 23.682 v11.5.0**, September 2013, Architecture enhancements to facilitate communications with packet data networks and applications, R11.
- [3] **M2M Communications**, David Boswarthck, Omar Elloumi, Oliver Hersent, 2012 WILEY

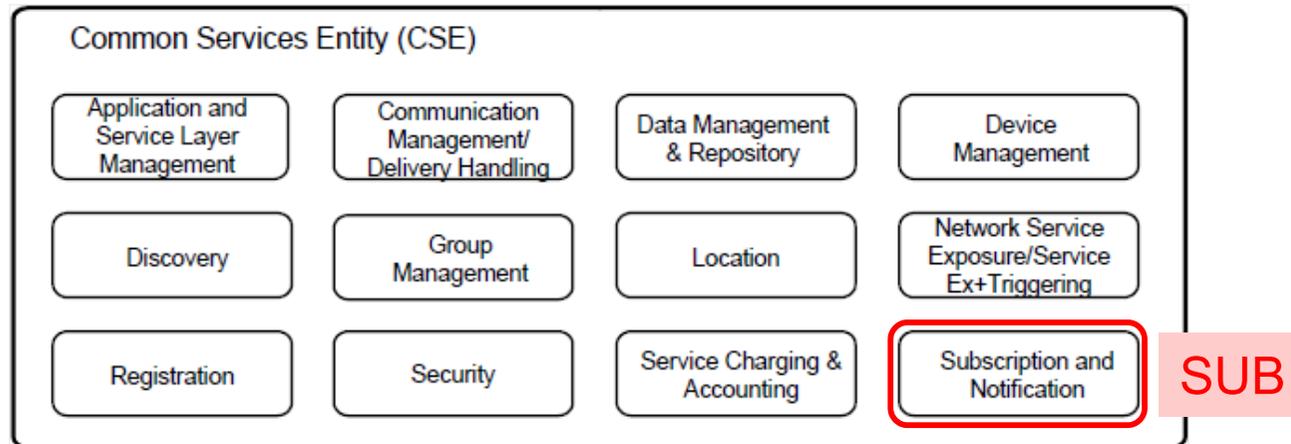
- M2M : Machine To Machine
- MTC : Machine Type Communications
- IoT : Internet Of Things
- REST : Representational State Transfer
- IN-CSE: Infrastructure Node CSE
- CSE: Common Service Entity
- AE: Application Entity

サブスクリプション・マネージメント - Subscription and Notification -

住友電気工業株式会社
平川 満

サブスクリプション・マネージメント

- CSF: SUB (Subscription and Notification)
- サブスクリプションに関する機能を提供
 - 監視したいリソースへの加入と停止に関する管理
 - アクセス制御ポリシーに従って管理
 - 監視中のリソースに変更があった場合に通知
 - 通知ポリシー(オプション)に従って通知



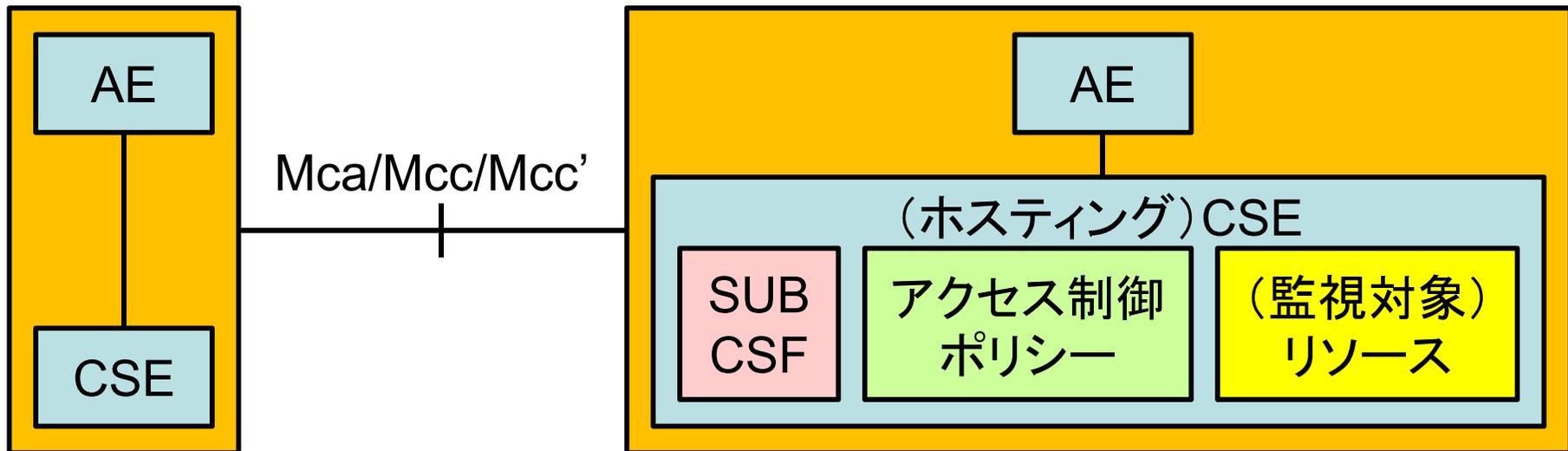
- 監視するリソース: URI でaddressing できるもの
 - センサデータ, 状態, 画像...
- 具体的な例
 - オフィスビルの温度データやstatus
 - 温度データそのもの, ある閾値を超えた場合のWarning
 - 河川の水位
 - 不審者検知カメラ画像

oneM2Mでは, どのM2Mユースケースにおいても不可欠となる
Subscription and Notification 機能を共通サービスとしてプラット
フォーム化 ⇒ アプリ追加時の実装負荷を軽減

- プレイヤー
 - サブスクライバ: AEまたはCSE
 - ホスト: (ホスティング)CSE
 - SUB CSF, アクセス制御ポリシー
 - (監視対象)リソース ※下図ではホスティングCSEの中

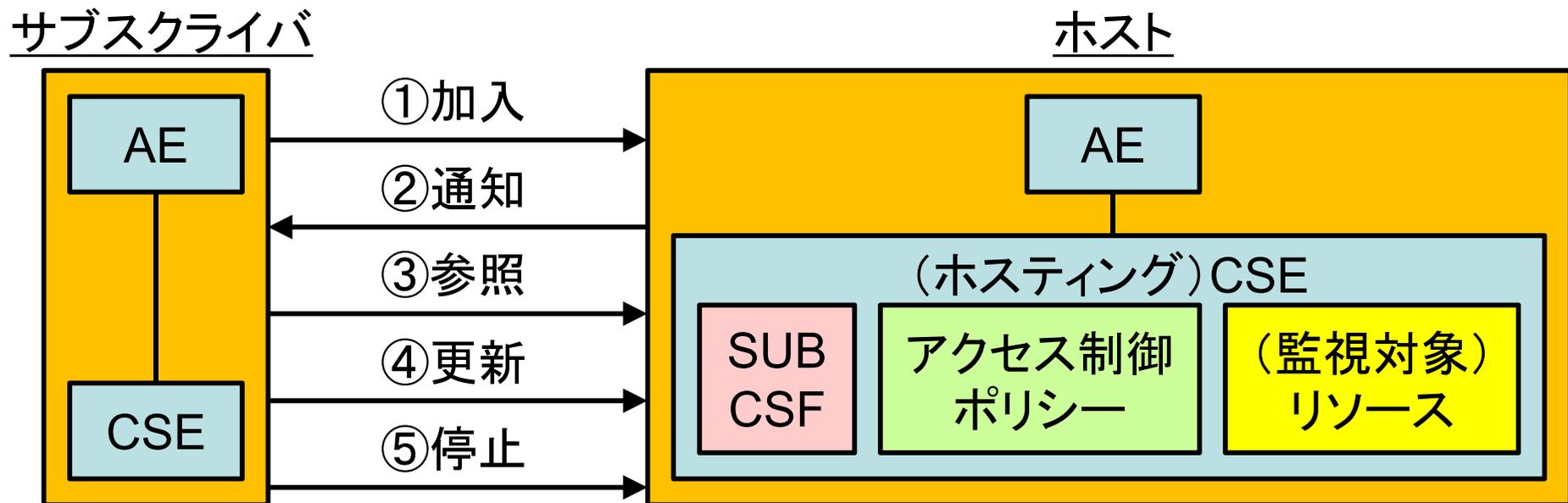
サブスクライバ

ホスト



基本的な処理フロー

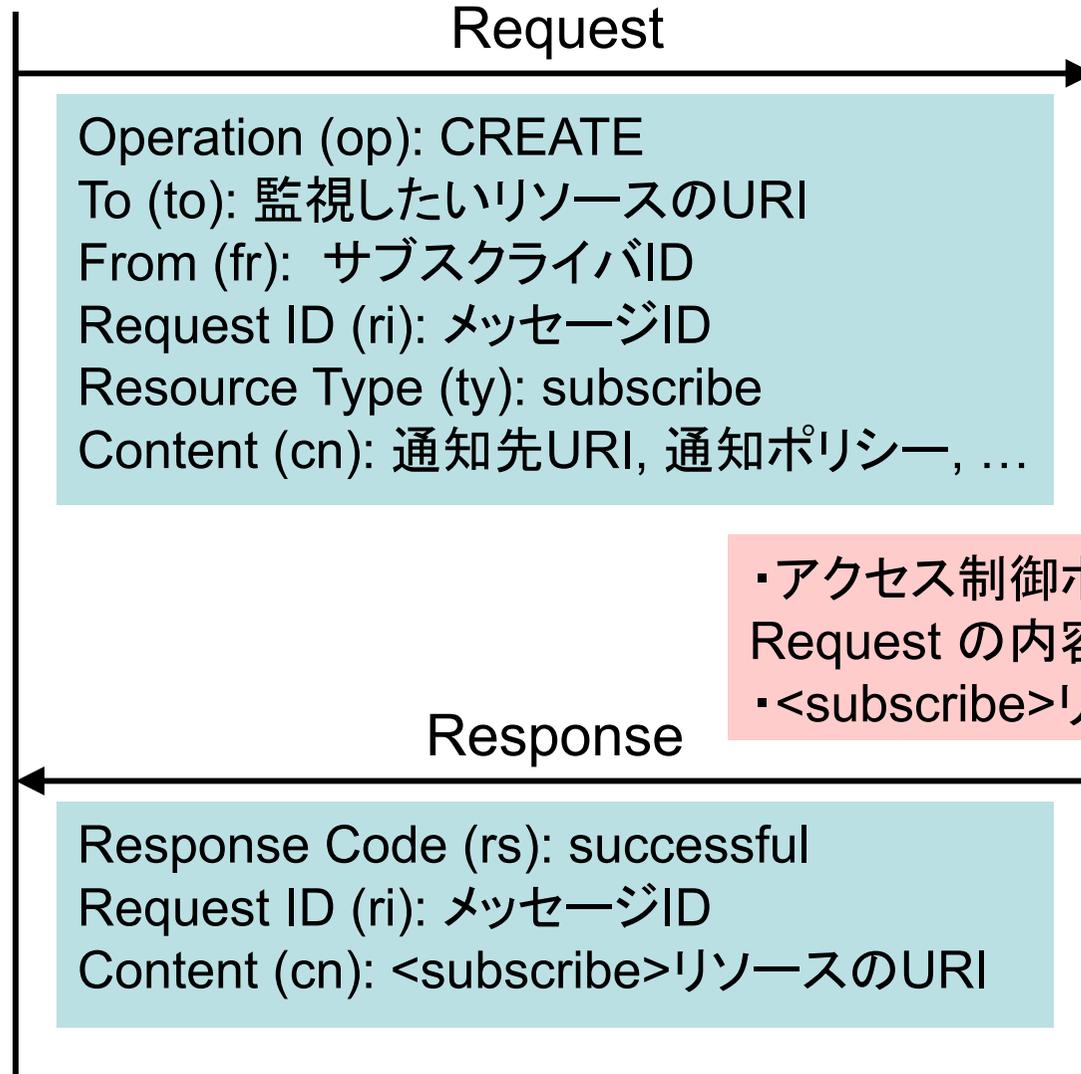
- ① 加入：監視したいリソースへの加入を要求 (CREATE)
- ② 通知：リソースに変更があった場合に通知 (NOTIFY)
- ③ 参照：リソースの情報を参照 (RETRIEVE)
- ④ 更新：リソースに対する更新 (UPDATE) ※例: 監視期間の延長
- ⑤ 停止：サービス停止を要求 (DELETE)



①加入の正常処理フロー

サブスクライバ

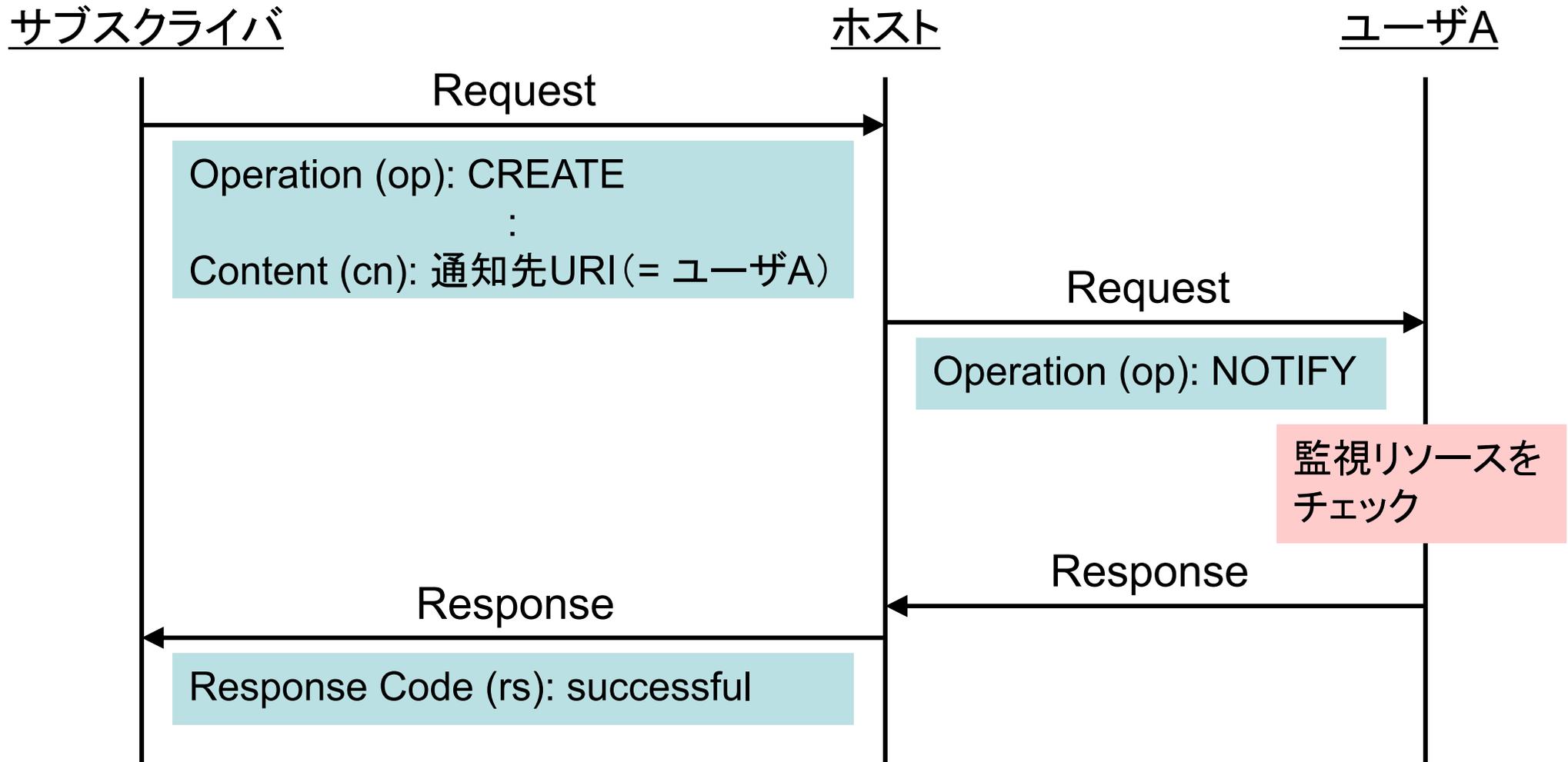
ホスト



- ・アクセス制御ポリシーに従って Request の内容をチェック
- ・<subscribe>リソースを生成

①加入の正常処理フロー(続き)

➤ 通知先URI ≠ サブスクライバの場合



➤ 属性の設定は一部を除いてオプション

属性 (Attributes)	概要
<i>notificationCriteria</i>	通知イベント発生時, 本属性に合致する通知のみ送信
<i>expirationCounter</i>	通知ごとに減少するカウンタ。ゼロになったらリソースを削除
<i>notificationURI</i>	通知先のリスト
<i>batchNotify</i>	一時的に通知をストアしておくか否かを指定
<i>rateLimit</i>	特定の時間範囲における通知回数を制限するか否かを指定
<i>pendingNotification</i>	コネクションレス時の通知メカニズムを指定
<i>notificationStoragePriority</i>	メモリに保持する購読リソースの優先度を指定
<i>latestNotify</i>	通知が貯まっている場合に最新通知のみ必要か否かを指定
<i>notificationDeliveryPriority</i>	通知の送信に関する優先度を指定
<i>notificationEventCat</i>	通知イベントの分類

Notification処理の例

(例) “pendingNotification”

pendingNotification

何らかの理由でコネクションが切断し、その再接続された場合の処理

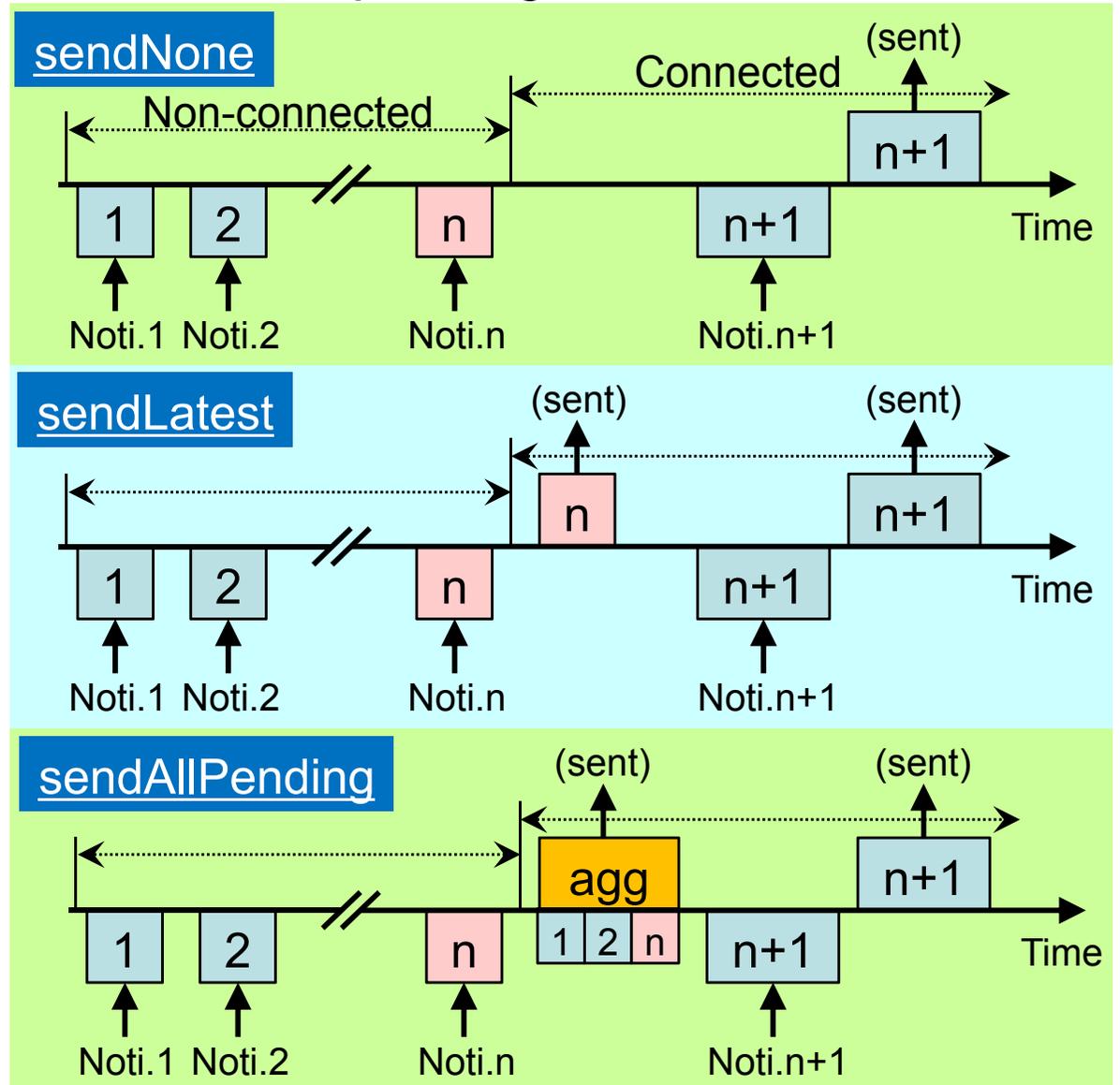
sendNone: 切断時に発生した通知は送信しない(メモリから削除)

sendLatest: 切断時に発生した通知のうち最新の通知のみ送信

sendAllPending: 切断時に発生した通知をすべて集約して送信

※通知に関する処理の詳細は
TS-0004-CoreProtocol-V-2014-08.pdf の“7.4 Notification definition and procedures”を参照のこと

用途や状況に応じてNotificationに関する複数のパラメータを最適設定することで、M2Mトラフィックの削減や通知メッセージの到達性改善を実現



まとめ

- oneM2MではあらゆるM2Mユースケースに不可欠となるリソース監視・通知機能を共通サービス機能としてプラットフォーム化
- 複数のNotification系パラメータによりM2Mトラフィック削減やメッセージ到達性改善を実現
- 参考ドキュメント
 - TS-0001-oneM2M-Functional-Architecture-V-2014-8.pdf
 - TS-0004-CoreProtocol-V-2014-08.pdf

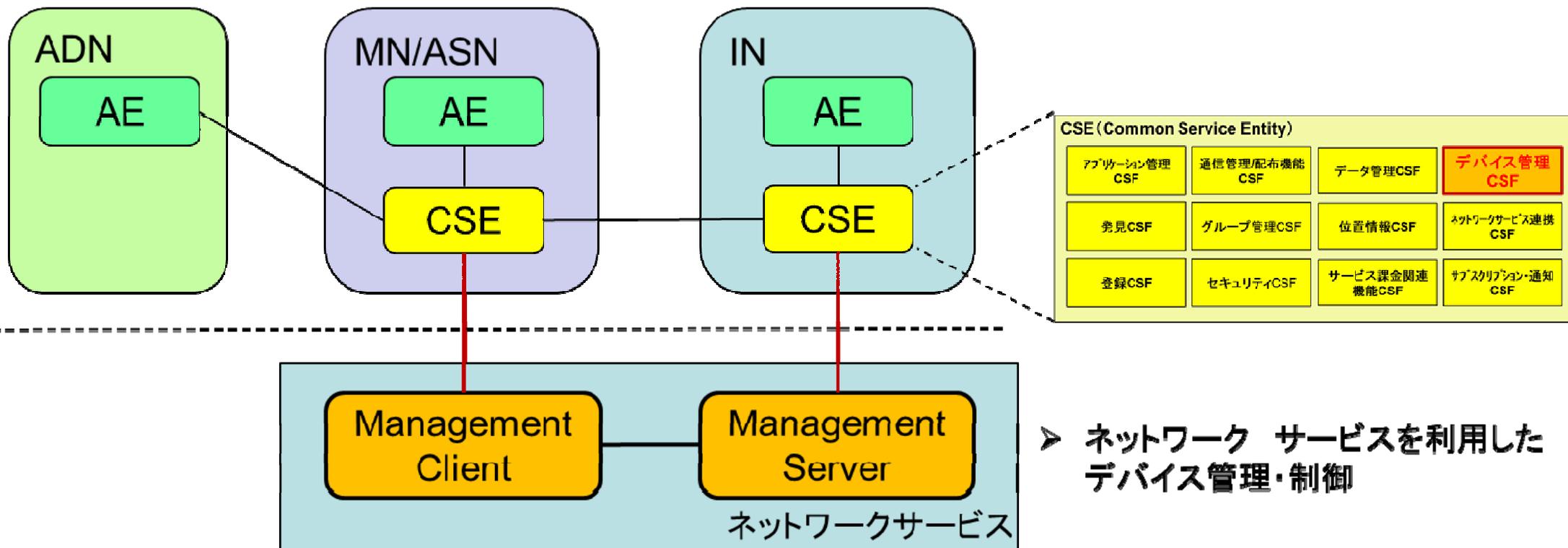
http://www.onem2m.org/candidate_release/index.cfm

M2Mデバイス・マネージメント

株式会社KDDI研究所
服部 雅晴

➤ デバイス・マネージメントの全体像

- oneM2Mサービスレイヤでは、デバイス管理CSFを規定 [TS 0001]
- デバイス管理CSFから別の標準化団体(OMA/BBF)のデバイス管理プロトコル(OMA-DM/TR-069)によるネットワークサービスを利用 [TS 0005, TS 0006]



➤ デバイス・マネージメントのねらい

- AEが複数のデバイス管理プロトコル(OMA-DM/TR-069)を、個々のプロトコルを理解することなく、利用してデバイスを管理・制御
 - データモデルおよび制御コマンドを表現するリソースを仕様化[TS 0001]
 - 個々のプロトコルとのマッピングを仕様化[TS 0005, TS 0006]
- oneM2Mのデバイス・マネージメント機能により、サービスプロバイダは統一されたインタフェースで、複数のデバイス管理プロトコルを利用したデバイスの管理・制御が可能になる

▪ 6.2.4 → Device Management

▪ 6.2.4.1 → General Concepts

- The Device Management (DMG) CSF provides management of device capabilities on MNs (e.g. M2M Gateways), ASNs and ADNs (e.g. M2M Devices), as well as devices that reside within an M2M Area Network. Application Entities (AE) can manage the device capabilities on those Nodes by using the services provided by the DMG CSF alleviating the need for the AE to have knowledge of the management technology specific protocols or data models. While the AE does not require an understanding of the management technology specific protocols or data models, this information is provided to the AE so that an AE can utilize this information for administrative purposes (e.g. diagnostics, troubleshooting).

デバイス管理プロトコル

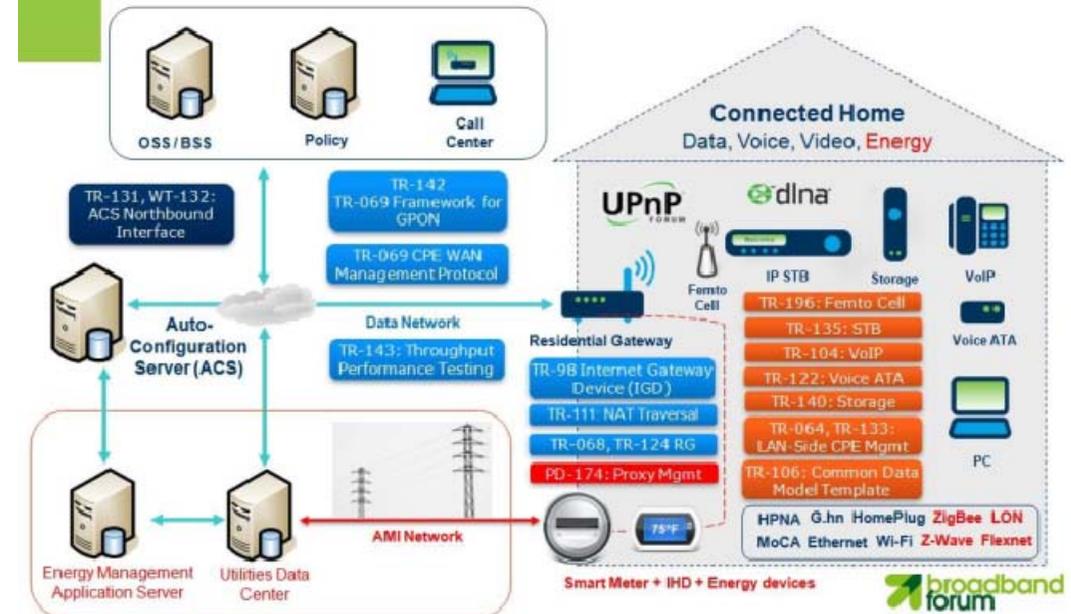
➤ 各標準化団体によるデバイス管理プロトコル(oneM2M対象プロトコル)

標準化団体	デバイス管理プロトコル	対象技術仕様書
OMA	OMA-DM 1.3 OMA-DM 2.0 OMA-DM LWM2M	TS 0005
BBF	TR-069	TS 0006

OMA-DM



TR-069

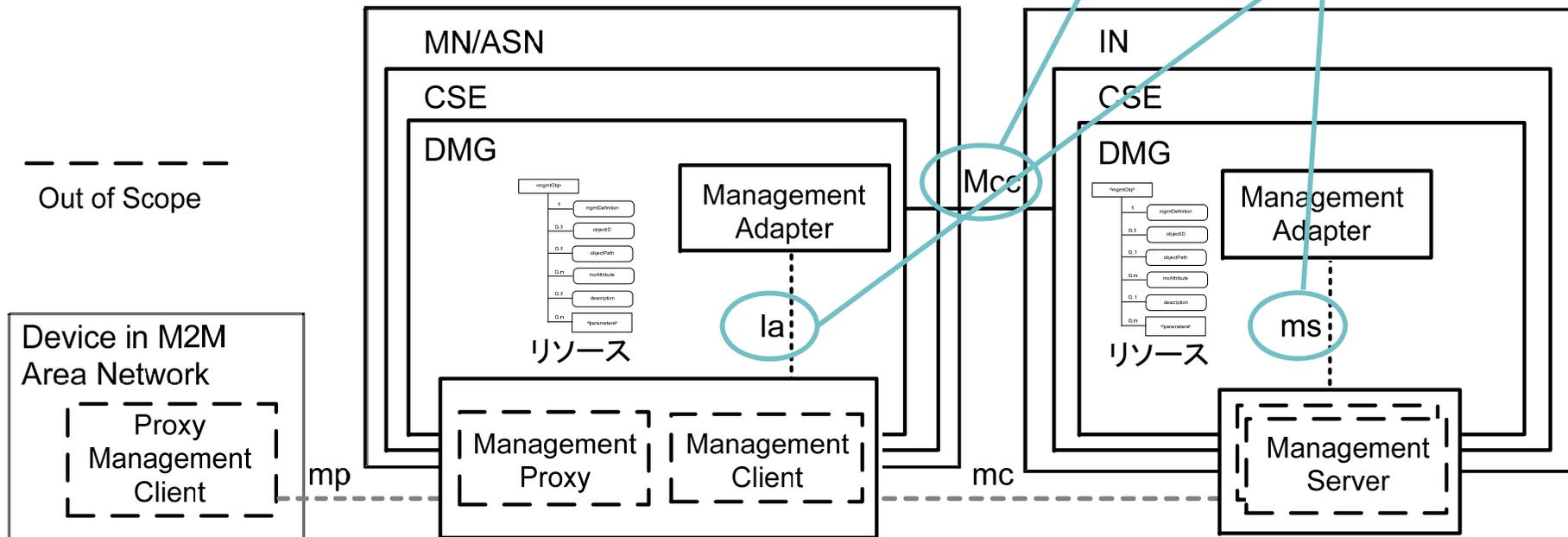


M2Mデバイス・マネージメント仕様

- デバイス・マネージメントのアーキテクチャ
 - デバイス管理CSF (DMG CSF) の定義
 - デバイス管理プロトコルとのインタフェースの定義
 - ms: Management Serverとのインタフェース
 - la: Management Clientとのインタフェース
 - リソースの定義 (次スライド)

デバイス管理・制御の結果を
リソース操作で受けて同期

デバイス管理プロトコルと
リソース同期・コマンド制御



MNを介した
間接的なデバイス管理・制御

Mcn経由のデバイス管理プロトコル
によるデバイス管理・制御

M2Mデバイス・マネージメント仕様

➤ デバイス・マネージメントのリソース

➤ 2種類のリソース(<mgmtObj>と<mgmtCmd>)の定義

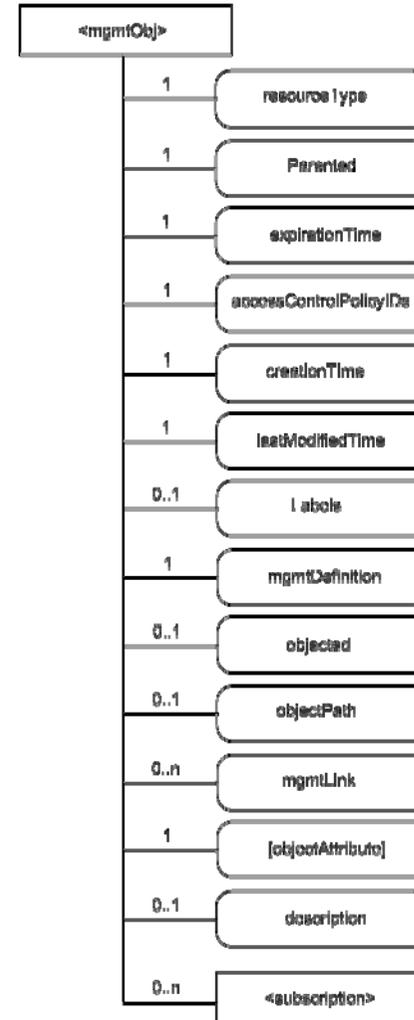
<mgmtObj>リソース

- デバイスの設定値の設定/参照を行うためのリソース
- 個々のManagement Object(TR069/OMA-DMでそれぞれ定義)がマッピングされ、これを直接操作

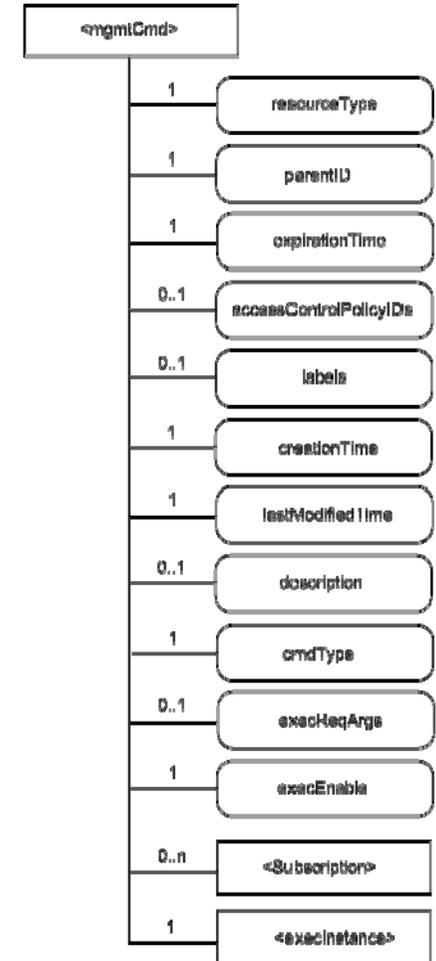
<mgmtCmd>リソース

- OMA-DM/TR-069の制御コマンドを実行するためのリソース
- <cmdType>で制御コマンドを指定し、<execEnable>で制御を指示、実行結果は<execInstances>から取得

<mgmtObj>リソース

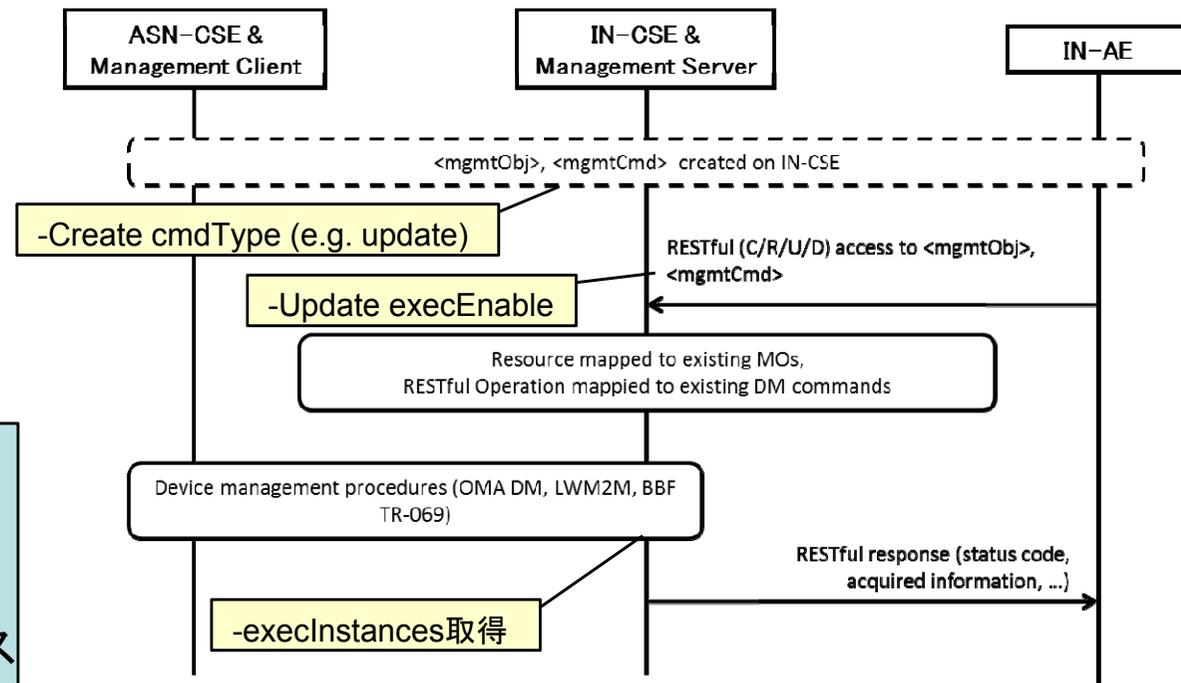
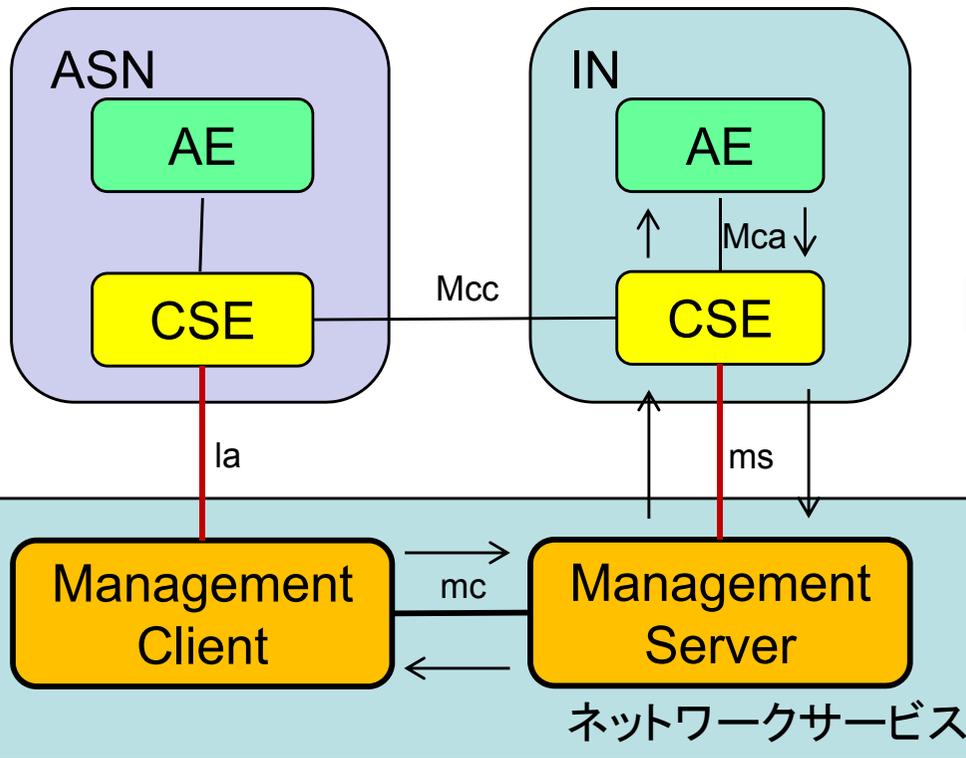


<mgmtCmd>リソース



M2Mデバイス・マネージメント実施例

- M2Mアプリ(AE)からのファームウェア アップデート
 - <mgmtCmd>を利用することにより、AEからはREST形式でデバイスの制御を実行可能
 - DMG CSFを含むCSEにてREST操作をデバイス管理プロトコルの制御コマンドに変換



まとめ

- oneM2Mサービスレイヤでデバイス管理CSFを規定し、複数のデバイス管理プロトコル(OMA-DM/TR-069)を利用して、デバイスを管理・制御する
- oneM2Mのデバイス・マネージメント機能により、サービスプロバイダは統一されたインタフェースで、複数のデバイス管理プロトコルを利用したデバイスの管理・制御が可能になる

M2Mセキュリティ

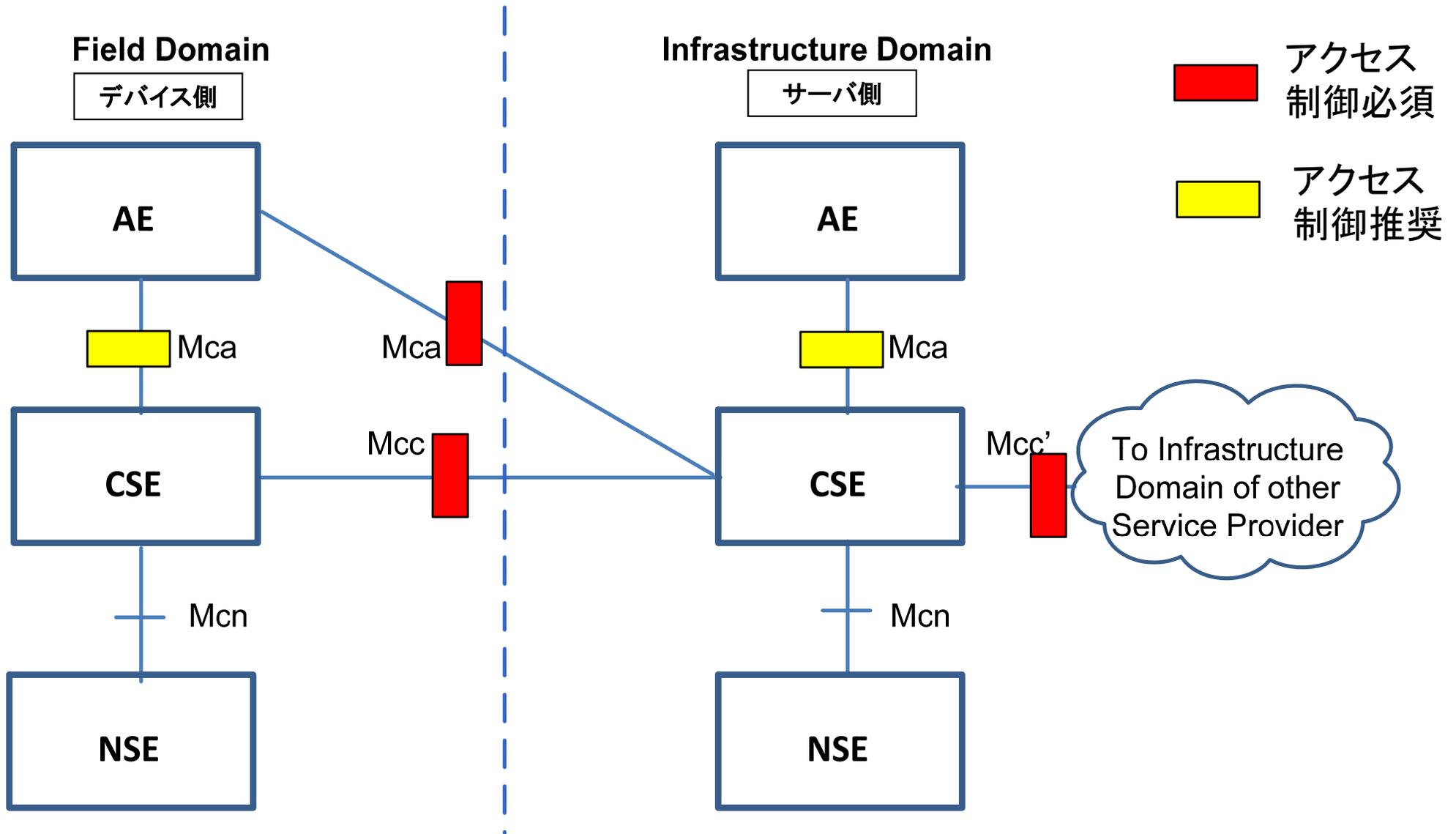
株式会社日立ソリューションズ
中野 正樹

セキュリティCSF

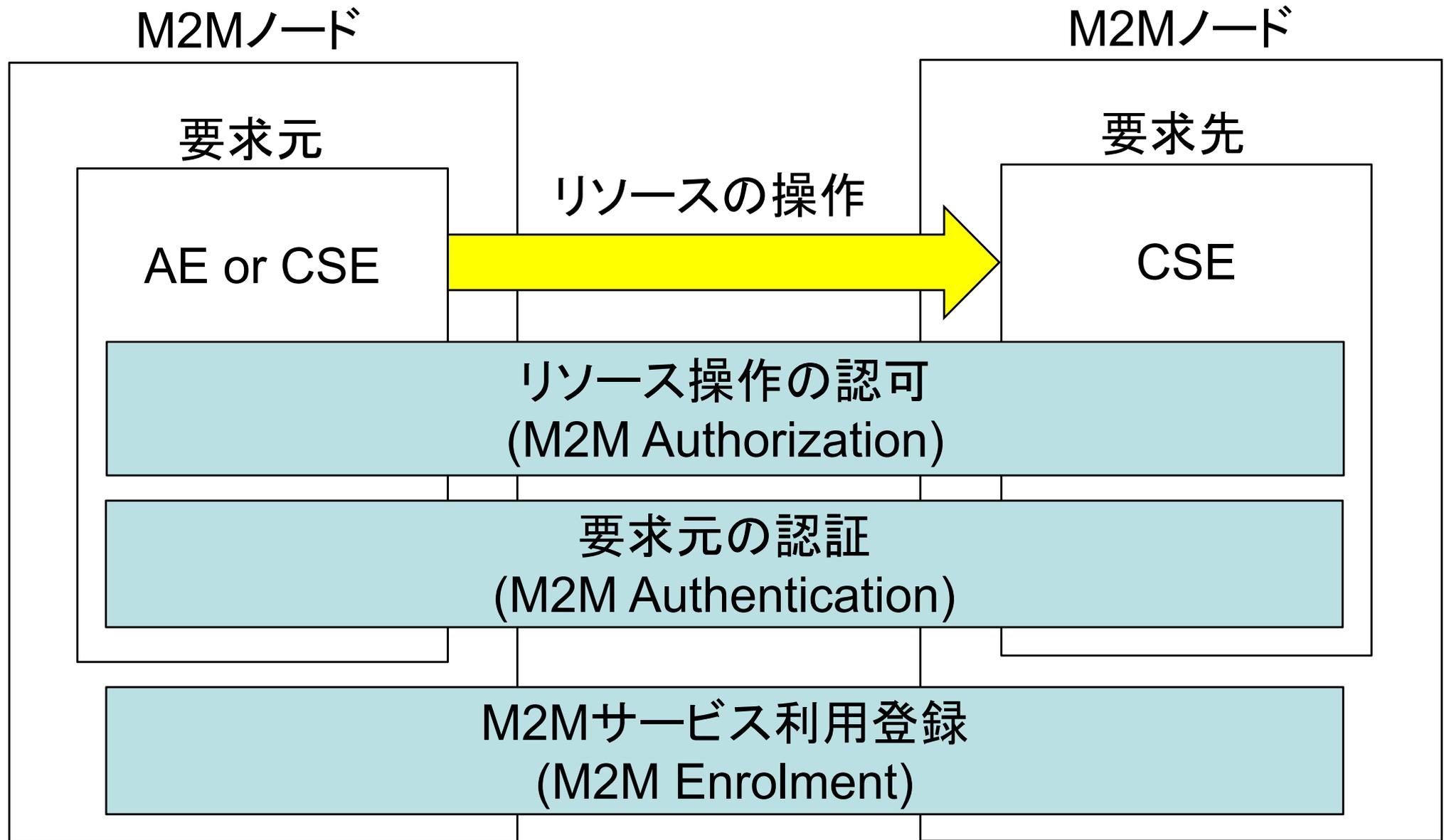
- 共通サービスとしてセキュリティ機能を提供
 - アプリケーション開発を効率化可能

機能項目	提供機能
アクセス制御	<ul style="list-style-type: none"> ・認証 ・操作の認可
安全な通信路の確立	<ul style="list-style-type: none"> ・M2Mノード間での安全な通信路の確立
セキュリティ運用	<ul style="list-style-type: none"> ・セキュリティ設定情報のリモート配布 ・セキュリティ情報管理
機密データ処理	<ul style="list-style-type: none"> ・機密データ保護 ・安全なストレージ
ID保護	<ul style="list-style-type: none"> ・IDを匿名化し、一時的なIDを提供

M2Mサービスのアクセス制御



リソース操作時のセキュリティ確立



セキュリティの確立手順

- M2Mサービス接続時のセキュリティを確立
 - M2M Enrolment
 - M2Mノードを登録し、M2Mサービスを利用可能にする機能
 - M2M Authentication
 - CSE及びAEを認証し、安全な通信路を確立する機能
 - M2M Authorization
 - リソースへのアクセスを認可する機能

M2M Enrolment

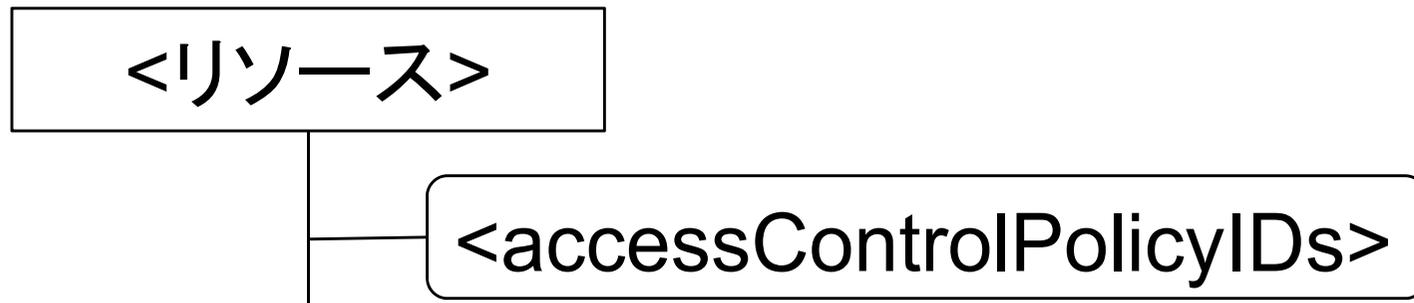
- M2Mノード情報をM2Mサービスプロバイダへ登録
- セキュリティ確立用の情報をM2Mノードへ設定
 - Pre-provisioning
 - 事前に情報をM2Mノードに設定(M2M機器出荷時等)
 - Remote provisioning
 - リモートで情報をM2Mノードに設定
 - Provisioned Symmetric Enrollee Key
 - Certificate-Based
 - GBA-based

M2M Authentication

- AE/CSEのM2Mサービスへの接続を認証し、安全な通信路を確立
 - サポートする認証方式
 - Provisioned M2M Secure Connection Key
 - 共通鍵の事前設定
 - Certificate-Based
 - TLS/DTLSによる認証
 - M2M Authentication Function (MAF)
 - 第3者のMAF(認証サーバ)による認証
 - GBA-based
 - 3GPP Generic Bootstrap Architectureによる認証

M2M Authorization

- 要求元AE/CSEに応じてリソース操作を認可
- 各リソースはアクセス制御ポリシーを指定する
<accessControlPolicyIDs>属性を保持



- アクセス制御ポリシーで認可対象を定義
 - 要求元: SCE-ID/AE-ID等
 - 環境: 時間、場所、IPアドレスを指定可能
 - 操作: CREATE、UPDATE等の操作

まとめ

- セキュリティ機能を共通サービスとして提供
 - 安全な通信を行うM2Mアプリケーションの開発が容易化
 - 多様なセキュリティ要件に全て対応出来る訳ではないが、基本機能が予め用意されているのは大きな利点

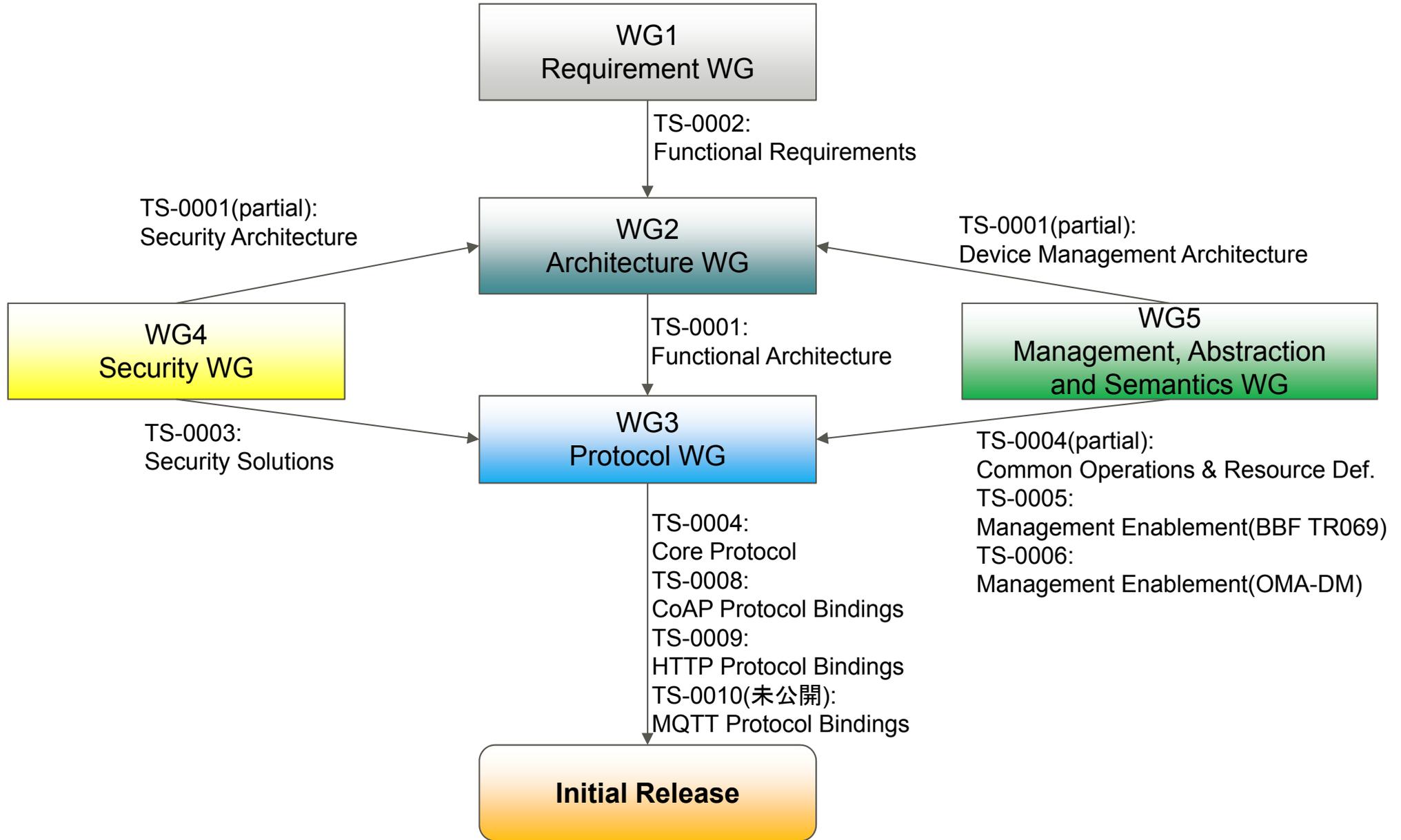
サービスレイヤプロトコル

株式会社富士通研究所

藤本 真吾

- データ型の定義
 - MIME Type: プロトコルメッセージの型を定義
 - Common Type: 単純型/複合型のデータ型を定義
 - Resource Type Definition: 属性値型の選択
- 抽象化された通信プロトコル
 - Generic Procedures: Originator/Receiverの処理手順
 - Common Operations: モジュール化された共通処理
- プロトコルバインディング
 - Initial ReleaseではHTTPとCoAPを公開(MQTTは保留)
 - リソース操作に必要な手順を定義(≠1対1マッピング)

技術文書間の関係



プロトコル仕様の成り立ち

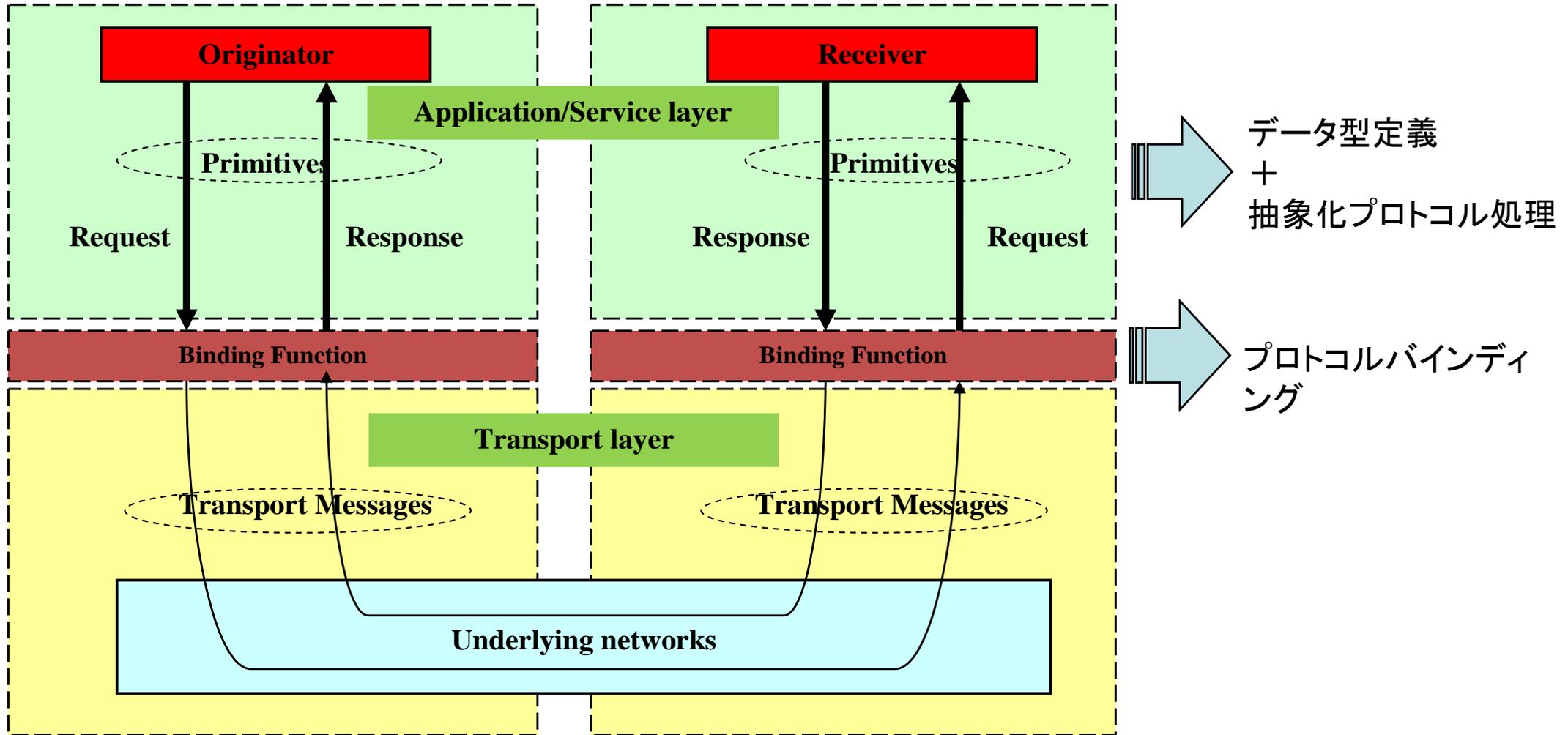
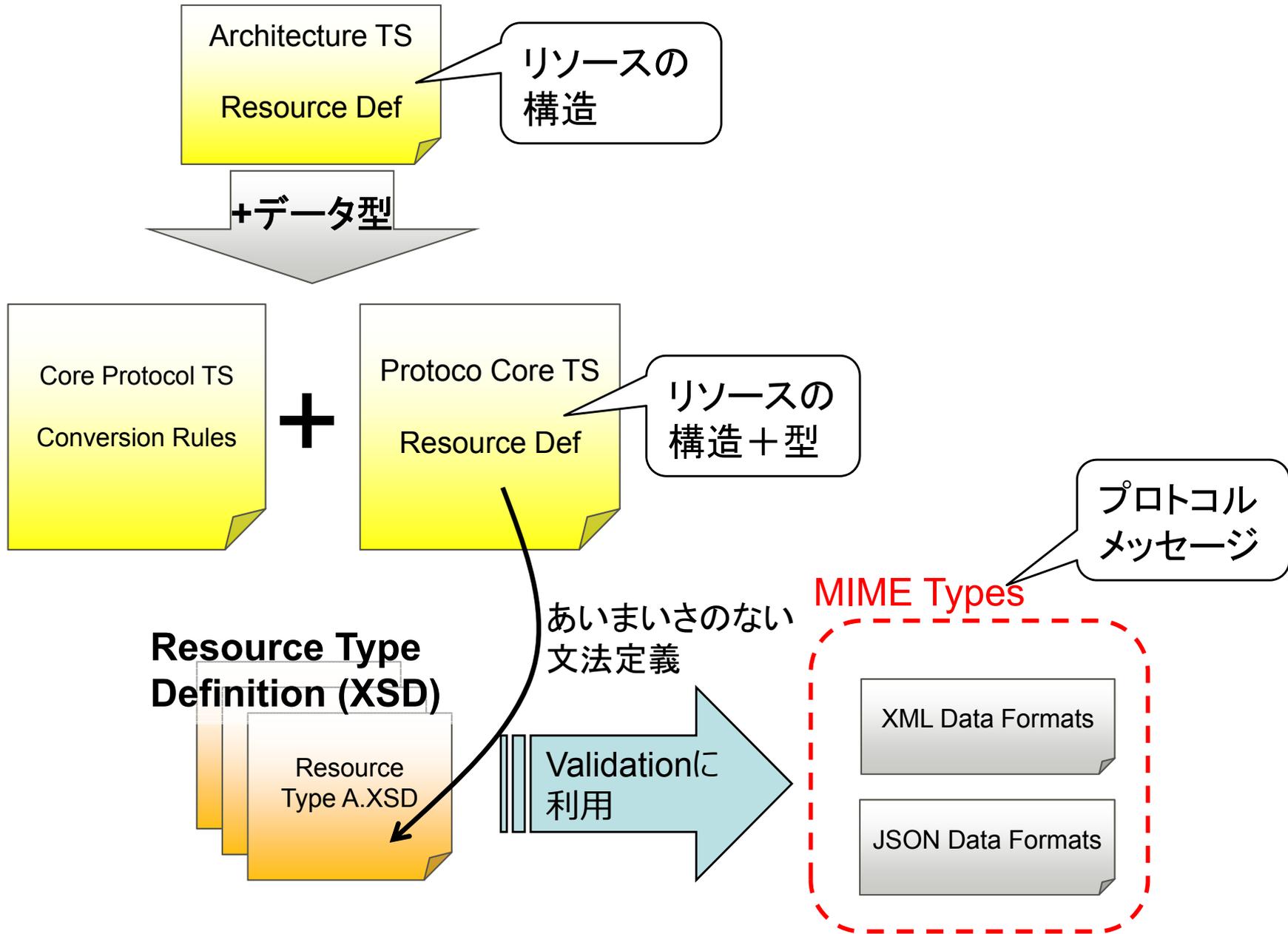


Figure 5.3.1-1: Primitive overview

データフォーマット定義の関係



➤ 概要

- RESTの流儀に従ってMIMEタイプ駆動型の処理
- 'vnd.onem2m-'のプリフィックスを仕様(登録予定)
- 初版リリースではXMLデータ型のみ
(可能ならJSONデータ型も)
- MIMEデータ型は3種類(今後追加の可能性あり)
 - application/vnd.onem2m-resource-data+xml
 - application/vnd.onem2m-response-status+xml
 - application/vnd.onem2m-partial-updates+xml

Common Type: 共通データ型の定義

- NormativeテキストとXSD記述で曖昧さを排除
 - Simple型: XSDの基本データ型+oneM2Mで制限
 - Enumerated型: 整数表現や、文字列の選択肢を規定
 - Complex型: 構造を持ったXMLデータを規定

XSD type name	Type Name	Examples	Description
m2m:networkaccessIdentifier	Network Access Identifier	user@realm	The networkaccessIdentifier is a standard way of identifying users who request access to a network as specified at IETF RFC 4282 [18].

XSD type name	Element	Element Data Type	Description
m2m: externalID	accessId	m2m:networkaccessIdentifier	The identifier of the node for the underlying network provider. In 3GPP case, the accessId is mapped to External Identifier as specified in TS 23.003 [17].
	MSISDN	xs: string	The identifier of the node as specified in TS 23.003 [17]

データ型定義の例

Resource Type Definitions (7.3.x)

- アーキ文書(TS-0001)との重複を避け(システム内部の振舞いには触れずに)外部仕様(API)を既定
- Introduction: attribute/child resourceの型を定義
- Operation: リソース特有の振舞いと、想定されるエラー種類についての規定

7.3.2.2.1. Create

Originator:

The <CSEBase> resource shall not be created via API.

Receiver: The Receiver shall execute the following steps in order.

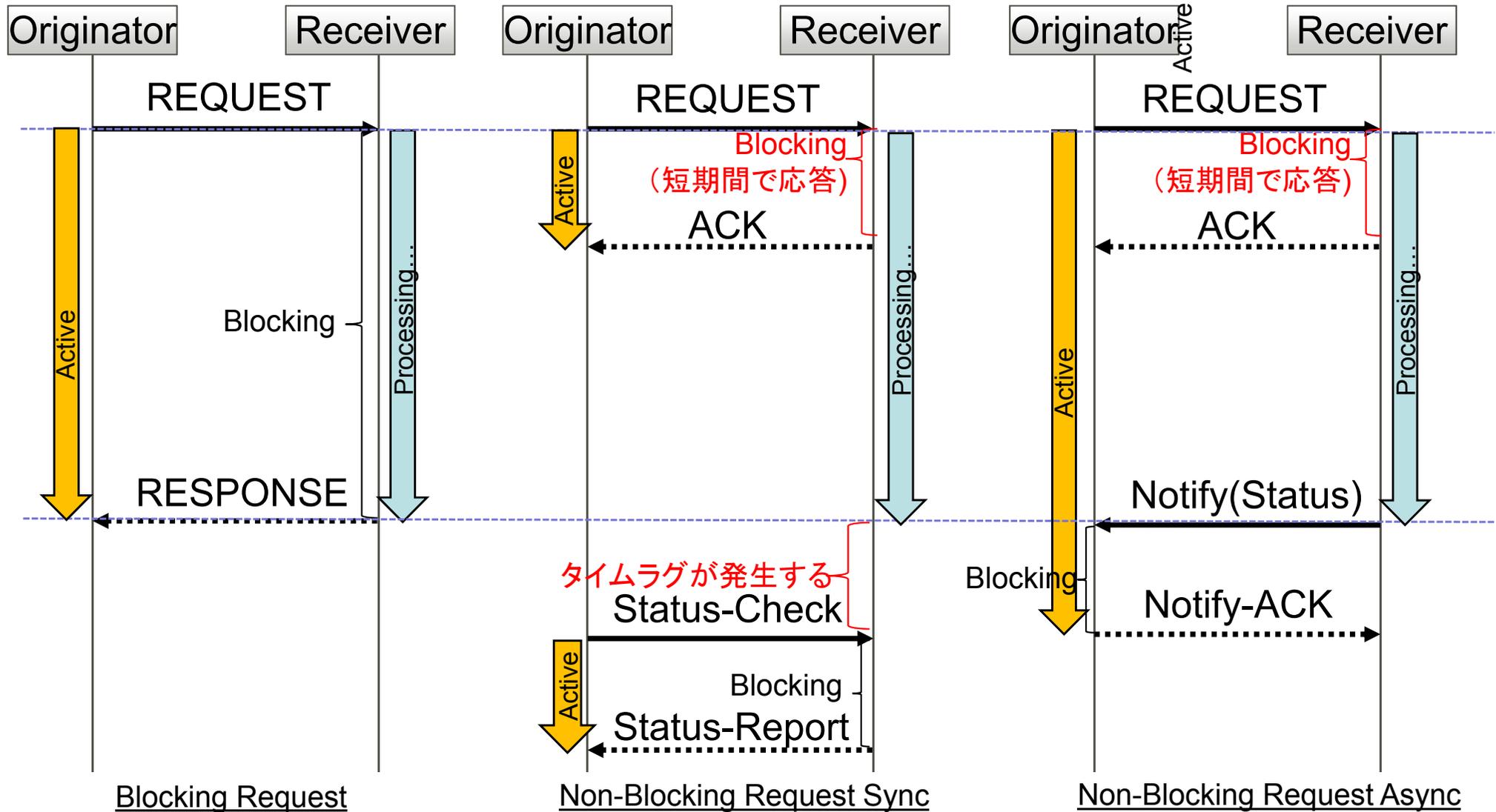
- Rev-C-Rq-1.0 "Create an unsuccessful Response" with responseCode TBD (Method not allowed)
- Rev-C-Rq-2.0 "Send Response primitive".

リソース特有の振舞いをCommon Procedureをベースに説明(後述)

想定されるエラー種類

Resource Type Definitionの例(clause 7.3.2 CSEBase)

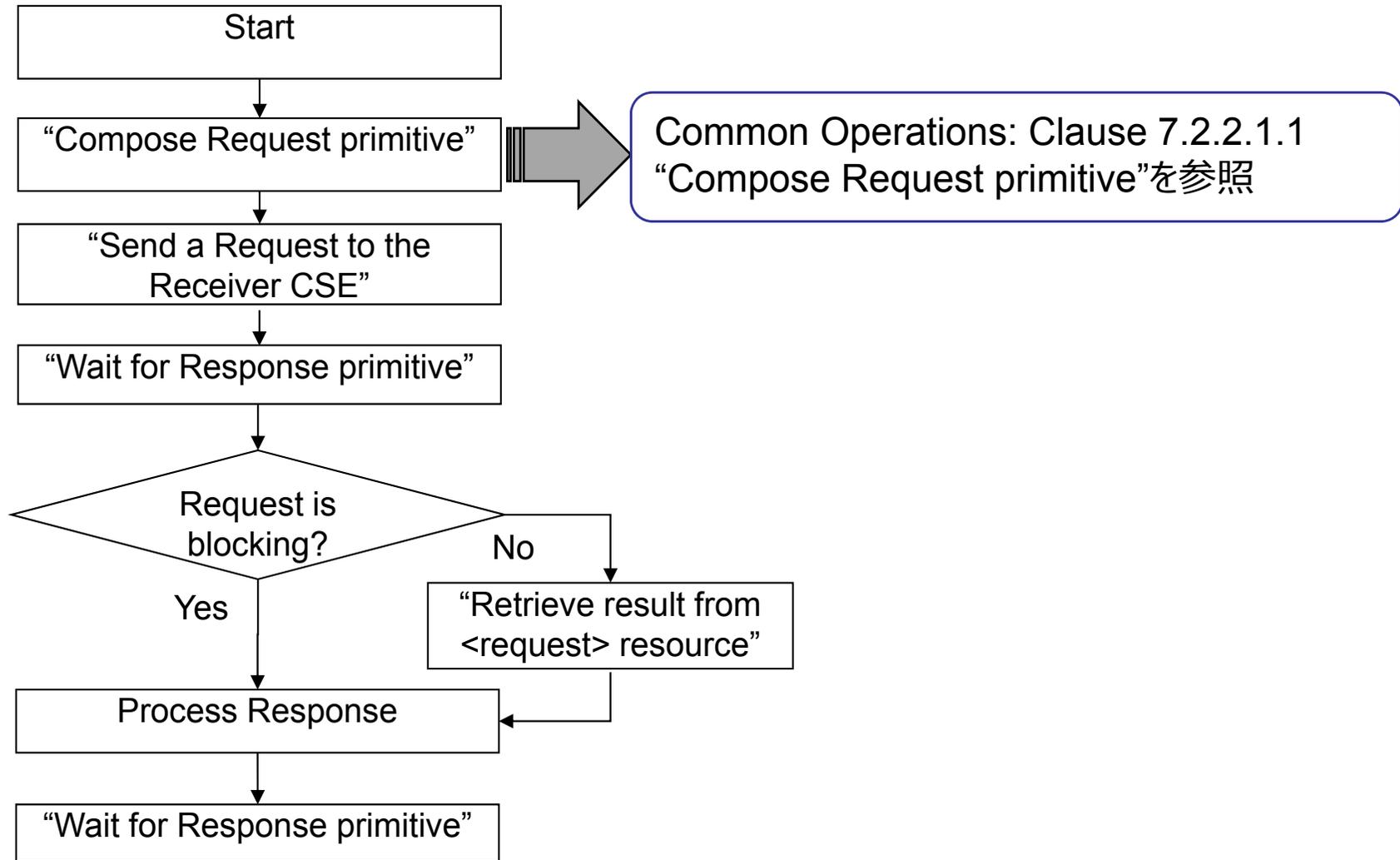
抽象化プロトコル: 通信の基本形



NAT経路のアクセスで便利

応答が速くスリープ時に好適

完全非同期処理モデル



7.2.1.2.1. Generic Resource Request Procedure for Originator

- リソースに依存しない処理をモジュール化
- リソース依存の処理で差異を説明する基になる

7.2.2.1.1. Compose Request primitive

The originator shall compose a Request message that shall be mapped to a specific protocol.

The Request shall include the "fr" and "to" to indicate the identifier of the originator of the request and the targeted receiver of the request.

The Request shall include the other attributes in case needed depend on the resource the request is addressing.

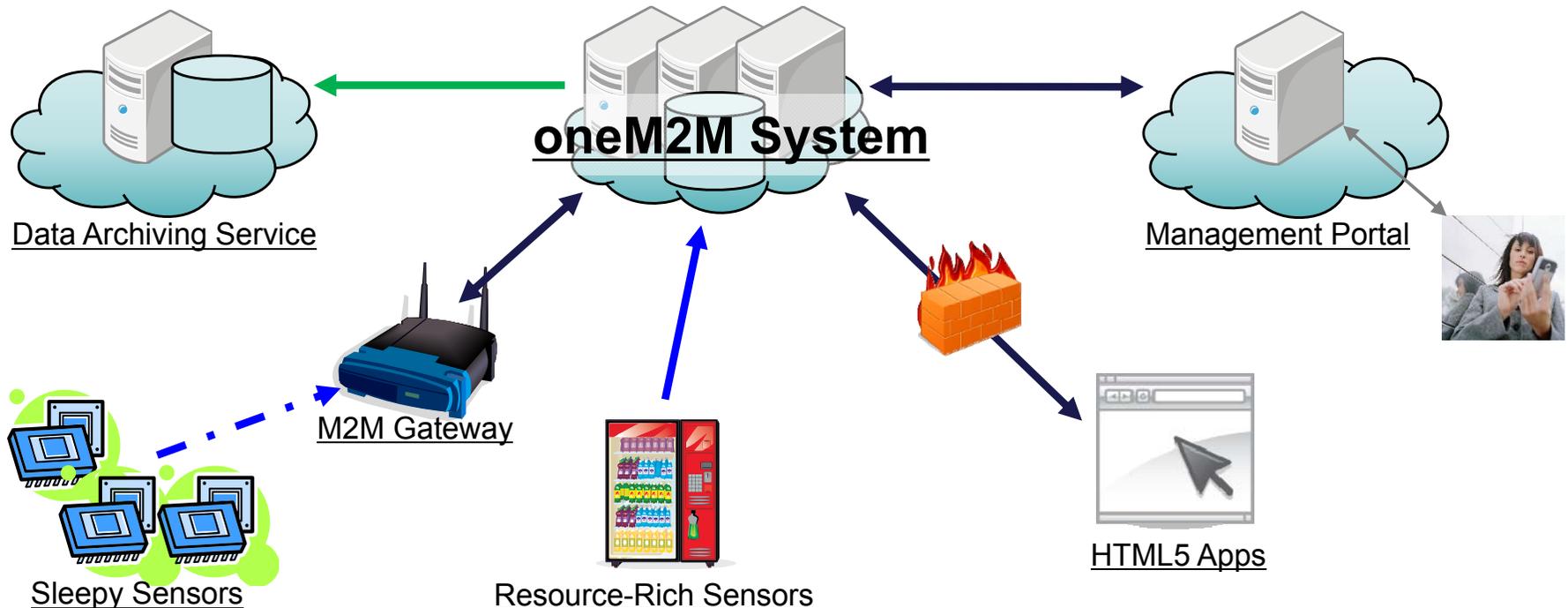
When including a resource representation in the request indication for create and update, the originator shall take into account the validation rules as specified in "Check validity for resource representation for create" and "Check validity for resource representation for update" respectively.

プロトコル・バインディング

- oneM2Mシステムの接続先は多岐に渡るので、
‘one-fits-all’なプロトコルは存在しない

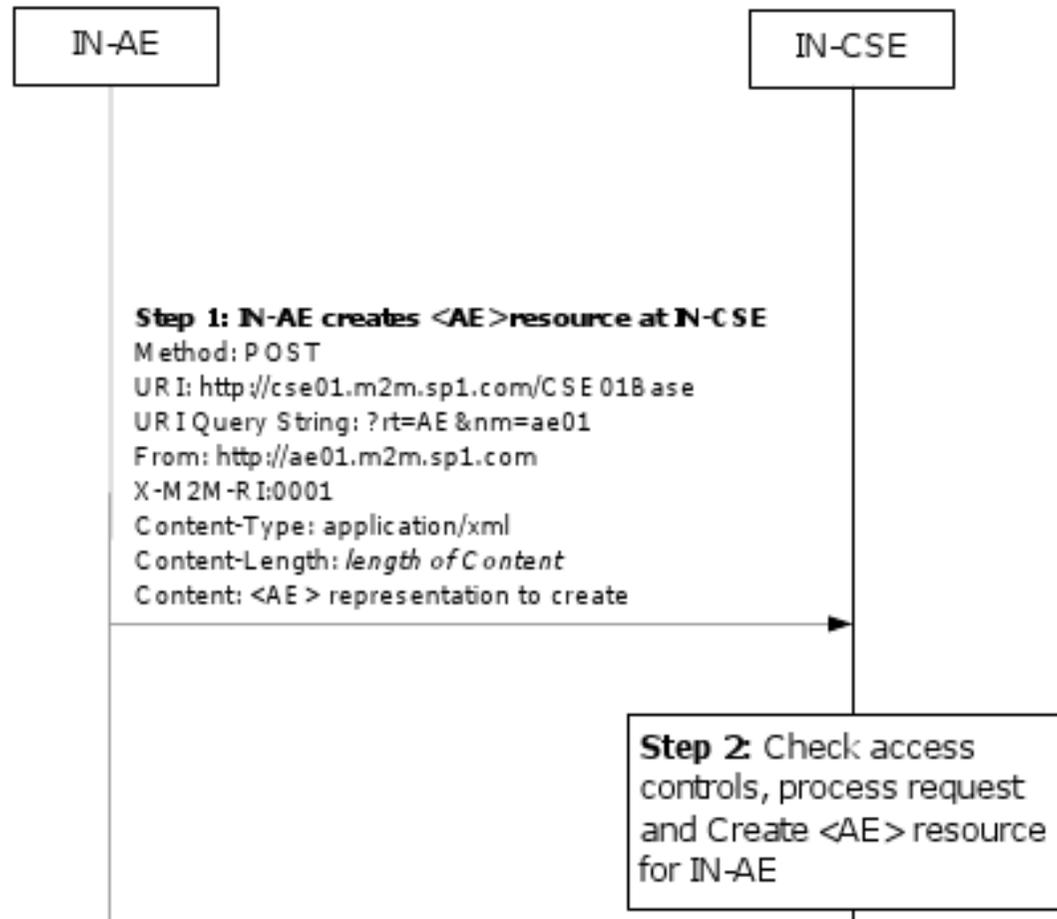


通信レイヤの差異を‘Protocol Binding’で吸収するアプローチ



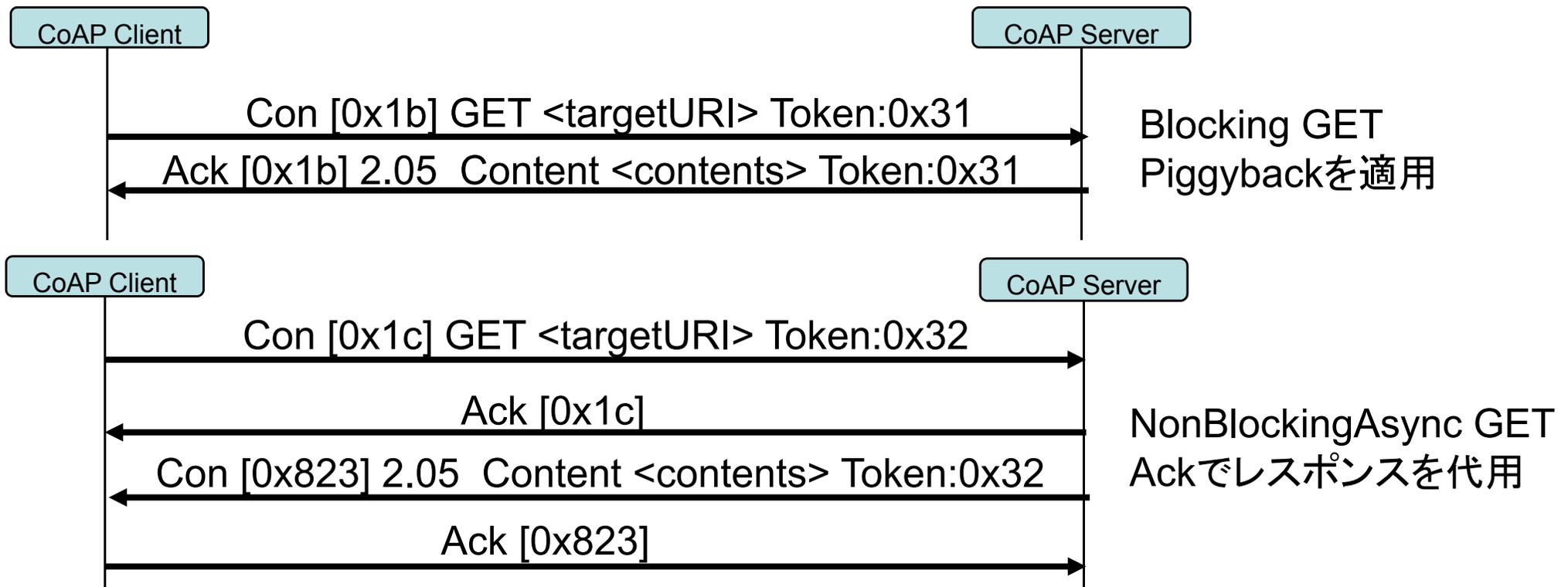
HTTP-REST Binding

- 拡張ヘッダの利用を極力さけ、標準ヘッダを活用
- 制御パラメータはQuery-Stringで指定



CoAP Binding

- 発行直後のRFC7252に準拠
- マッピングはHTTPのマッピングを踏襲
+メッセージレベルの最適化



- データ型定義、抽象化されたプロトコル、プロトコル
バインディングについて概要を説明
- 「これで完成！」ではないが、Stage 3の議論で
Stage 2でのあいまいさが判明し修正、という良い
フィードバックができています
- TP#15までに問題点を解決し、きちんと動作する仕
様に仕上げていく予定

ご清聴ありがとうございました。