TTC技術レポート
Technical Report

# TR-M2M-R3
# oneM2M リリース 3 の構成と解説

Structure and Interpretation of
oneM2M release 3

第 1.0.0 版

2019 年 6 月 28 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

本書は、一般社団法人情報通信技術委員会が著作権を保有しています。
内容の一部又は全部を一般社団法人情報通信技術委員会の許諾を得ることなく複製、転載、改変、転用及びネットワーク上での送信、配布を行うことを禁止します。

－目次－

## はじめに

本レポートはoneM2Mリリース3およびそれらに対応したTTC仕様書の構成と各仕様書間の関係、仕様書のポイントを解説しており、TTC仕様書の理解を助けるために作成されたものである。なお、oneM2Mリリース3の追加や更新がある場合には、適宜、本レポートの改訂を行う。その他の追加・更新の提案等については、TTC oneM2M専門委員会事務局へご連絡をいただきたい。

# 1　oneM2M リリース3の構成

## 1.1　oneM2M リリース３の構成と TTC 仕様書との対応

oneM2M リリース３は、24件の技術仕様書（TS：Technical Specification）および3件の技術報告書（Technical Report)から構成されている。oneM2M Administrative Document ADM-0017 V3.0.0 - oneM2M Release3 Control Document－　に記載されている版(version)の一連の文書で構成されている。これらに対応するTTC仕様書の文書番号とタイトルを表1-1（技術仕様書）及び表1-2（技術報告書）に示す。

表 1-1　oneM2M リリース3の構成と対応するTTC仕様（１）技術仕様書（Technical Specification）

| 仕様番号（*は新規、他は Release2 の改訂） | Title | TTC 仕様書 |
|---|---|---|
| TS-0001[1] | Functional Architecture<br>（機能アーキテクチャ） | V3.13.2 |
| TS-0002[2] | Requirements<br>（要求条件） | V3.1.2 |
| TS-0003[3] | Security Solutions<br>（セキュリティ技術の適用） | V3.10.2 |
| TS-0004[4] | Service Layer Core Protocol<br>（サービス層 API 仕様（共通部）） | V3.11.0 |
| TS-0005[5] | Management Enablement (OMA)<br>（OMA 仕様によるデバイス管理） | V3.4.2 |
| TS-0006[6] | Management enablement (BBF)<br>（BBF 仕様によるデバイス管理） | V3.6.2 |
| TS-0008[7] | CoAP Protocol Binding<br>（サービス層 API 仕様（CoAP 用） | V3.3.1 |
| TS-0009[8] | HTTP Protocol Binding<br>（サービス層 API 仕様（HTTP 用）） | V3.2.0 |
| TS-0010[9] | MQTT protocol binding<br>（サービス層 API 仕様（MQTT 用）） | V3.0.2 |
| TS-0011[10] | Common Terminology<br>（共通用語） | V3.0.2 |
| TS-0012[11] | Base Ontology<br>（ベースオントロジー） | V3.7.3 |
| TS-0014[12] | LWM2M Interworking<br>（LWM2M とのインタワーク） | V3.1.1 |
| TS-0016[13]* | Secure Environment Abstraction<br>（セキュア環境抽象化） | V 3.0.2 |

| | | |
|---|---|---|
| TS-0020[14] | WebSocket Protocol Binding<br>（サービス層 API 仕様（WebSocket 用））| V 3.0.1 |
| TS-0022[15]* | Field Device Configuration<br>（フィールドデバイス構成） | V 3.0.1 |
| TS-0023[16] | Home Appliances Information Model and Mapping<br>（家電用デバイス管理モデルとマッピング） | V 3.7.3 |
| TS-0024[17] | OCF Interworking<br>（OCF とのインタワーク） | V 3.2.2 |
| TS-0026[18]* | 3GPP Interworking<br>（3GPP とのインタワーク） | V3.0.0 |
| TS-0030[19]* | Ontology Based Interworking<br>（オントロジーベースのインタワーク） | V 3.0.3 |
| TS-0031[20]* | Feature Catalogue<br>（フィーチャーカタログ） | V 3.0.0 |
| TS-0032[21]* | MAF and MEF Interface Specification<br>（MAF/MEF インタフェース仕様） | V 3.0.1 |
| TS-0033[22]* | Interworking Framework<br>（インタワークフレームワーク） | V 3.0.0 |
| TS-0034[23]* | Semantics Support<br>（セマンティックスサポート） | V 3.0.0 |
| TS-0035[24]* | OSGi Interworking<br>（OSGi インタワーク） | V 3.0.0 |


[1] TS 0001 - Functional Architecture, V3.13.2
[2] TS 0002 - Requirements, V3.1.2
[3] TS 0003 - Security Solutions, V3.10.2
[4] TS 0004 - Service Layer Core Protocol, V3.11.0
[5] TS-0005 - Management Enablement (OMA), V3.4.2
[6] TS-0006 - Management enablement (BBF), V3.6.2
[7] TS-0008 - CoAP Protocol Binding, V3.3.1
[8] TS 0009 - HTTP Protocol Binding, V3.2.0
[9] TS 0010 - MQTT Protocol Binding, V3.0.2
[10] TS-0011 - Common Terminology, V3.0.2
[11] TS 0012 - Base Ontology, V3.7.3
[12] TS 0014 - LWM2M Interworking, V3.1.1
[13] TS-0016 - Secure Environment Abstraction V3.0.2
[14] TS 0020 - WebSocket Protocol Binding, V3.0.1
[15] TS-0022 - Field Device Configuration, V3.0.1

[16] TS 0023 - Home Appliances Information Model and Mapping, V3.7.3
[17] TS 0024 - OCF Interworking, V3.2.2
[18] TS-0026 - 3GPP Interworking, V3.0.0
[19] TS-0030 - Ontology Based Interworking, V3.0.3
[20] TS-0031 - Feature Catalogue, V3.0.0
[21] TS-0032 - MAF and MEF Interface Specification, V3.0.1
[22] TS-0033 - Interworking Framework, V3.0.0
[23] TS-0034 - Semantics Support, V3.0.0
[24] TS-0035 – OSGi Interworking, V3.0.0

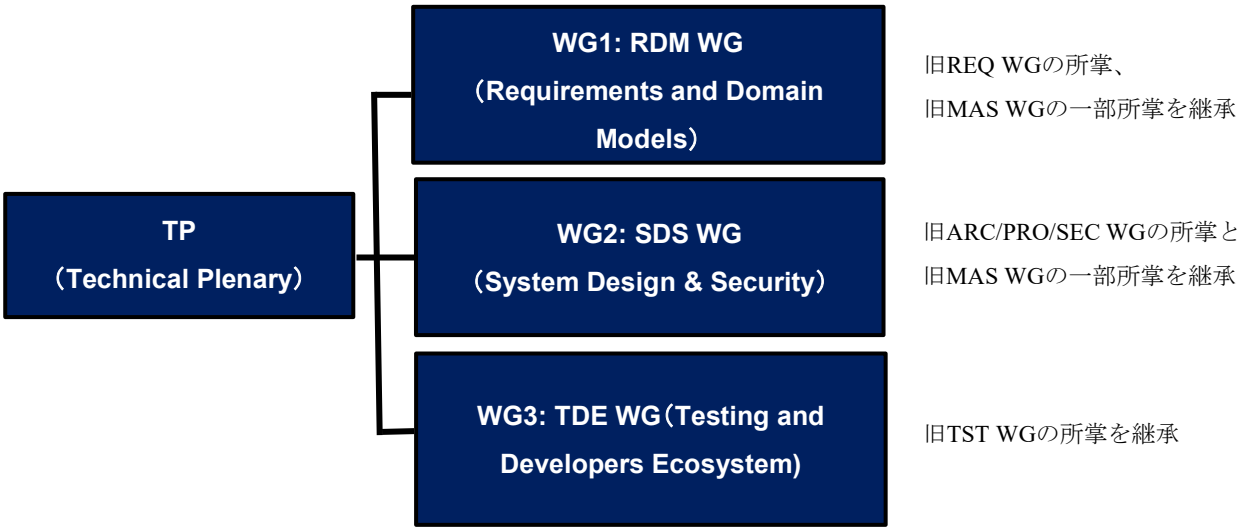
表 2-2　oneM2M リリース3の構成と対応するTTC仕様（２）技術報告書（Technical Report）

| TR番号（*は新規、無印はRelease2の改訂） | Title | TTC仕様書 |
|---|---|---|
| TR-0001[25] | Use Cases Collection<br>（ユースケース集） | V 3.4.2 |
| TR-0026[26]* | Vehicular Domain Enablement<br>（車両ドメインでの使用可能性） | V 3.0.1 |
| TR-0033[27] | Study on Enhanced Semantic Enablement<br>（高度セマンティックの使用可能性に関する研究） | V 3.0.0 |

[25] TR 0001 - Use Cases Collection, V3.4.2
[26] TR 0026 - Vehicular Domain Enablement, V 3.0.1
[27] TR 0033 - Study on Enhanced Semantic Enablement, V 3.0.0

### 1.2　oneM2M WG 構成

oneM2Mでは、2019年2月から、WG構成が下図のように変更になった。旧WGとの関係とともにその構成を示す。



# 2　oneM2M Rel-3の解説

## 2.1 リリース 3 の主なフィーチャー

oneM2M リリース 1（2015 年 1 月）は 10 件の技術仕様書(TS)で構成されていたが、リリース 2（2016 年 8 月）では、そのうち、TS-0008 - CoAP Protocol Binding を除く 9 件の技術仕様書が改訂された他、新たに 8 件の技術仕様書が作成された。また、リリース 2 から、技術仕様書だけでなく、技術報告書（Technical Report）も合わせて発行されることになり、9 件の技術報告書も合せてリリースされた。

リリース 3（2018 年 12 月）では、リリース 2 で発行された仕様書の改訂や強化に加え、新たに加わったフィーチャーとしては、

・異なる M2M/IoT 技術とのインターワーキング・フレームワーク
・他技術との個別インターワーキング仕様の拡張（3GPP Rel15、OPC-UA、OSGi、OCF 等）
・フィールドデバイス構成
・フィーチャーカタログ
・オントロジーベースのインターワーキング
・セマンティックサポート
・セキュア環境の抽象化
・MAF/MEF インタフェース仕様

等が挙げられる。

### 2.1.1　TR-M2M-0001v3.1.1 – ユースケース集

本文書は、様々な oneM2M のインダストリーセグメントから収集されたユースケースが記載されている。これらのユースケースは、相互交流にフォーカスし、潜在要件も含んでいる可能性もある。

ユースケースは、エネルギー、エンタープライズ、ヘルスケア、公共サービス、住まい、小売り、交通輸送、などについて記載されている。

### 2.1.2　TS-M2M-0002v3.1.2 – 要求条件

本仕様書は、oneM2Mに関する情報としての機能的役割モデルおよび強制力のある技術的要求条件を規定する。

#### 2.1.2.1　M2M エコシステムの紹介

M2Mエコシステムとして、ユーザ、アプリケーションサービスプロバイダ、M2Mサービスプロバイダ、ネットワークオペレータの4つの機能的役割を定義している。

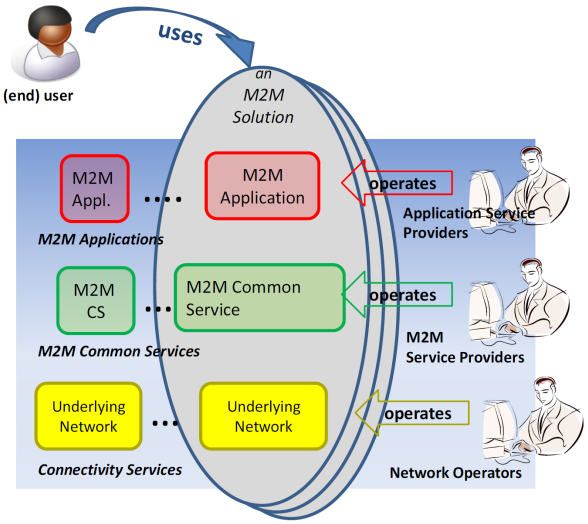



図2-1　M2Mエコシステムでの機能的役割

#### 2.1.2.2 機能的要求条件

M2Mの機能的要求条件を抽出し、下記のとおりに分類している。

- システム要求条件（140件）
- 管理要求条件（19件）
- オントロジー関連の要求条件（17件）
- セマンティックス注釈要求条件（7件）
- セマンティックスクエリ要求条件（1件）
- セマンティックスマッシュアップ要求条件（5件）
- セマンティックス推論要求条件（3件）
- データ分析要求条件（3件）
- セキュリティ要求条件（75件）
- 課金要求条件（7件）
- 運用要求条件（10件）
- 通信要求処理条件（19件）
- LWM2Mとの相互接続に関する要求条件（8件）

#### 2.1.2.3　非機能的要求条件（情報）

RESTfulスタイルを考慮したシステム設計（NFR-001）、および、効率のよいデータ交換が可能なプロトコル使用（NFR-002）の2件を抽出している。

### 2.1.3　TS-M2M-0001v3.15.0 - 機能アーキテクチャ

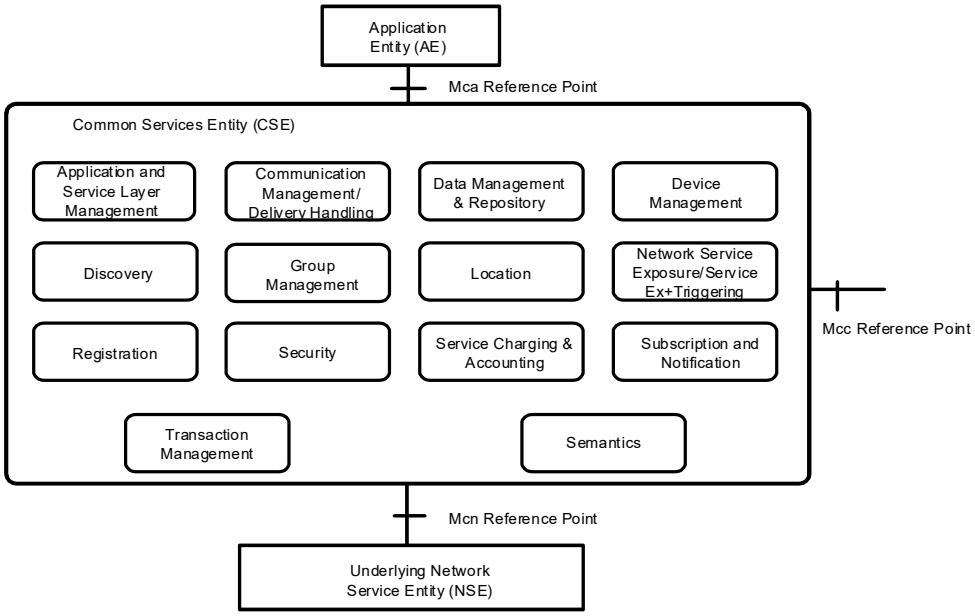
本文書は oneM2M の機能アーキテクチャを規定する文書である。リリース 3 で追加された主な機能について、以下に記載する。

#### 2.1.3.1 Common Services Functions

共通サービス機能を定義した CSF (Common Services Functions)では、Transaction Management と Semantics の 2 つの機能が追加されている。

Transaction Management CSF は、トランザクションのスケジューリング、トランザクション対象のリソースの lockinng/ unlocking、アトミック・トランザクション、トランザクションの実行、成功したトランザクション結果の引き渡し、失敗したトランザクションのロールバック・廃棄といった機能をサポートする。本 CSF は、Originator によって使用され、Originator は複数の oneM2M リクエスト・プリミティブ・セットで構成されるトランザクションを提供する。

Semantics (SEM) CSF は、アプリケーションに、セマンティック情報を管理することを可能とし、本情報を基にした機能を提供する。これにより、データ/リソースの意味に関連する付加価値機能を提供する。SEM CSF の機能は、セマンティック記述がベースとなり、アノテーション、リソース・フィルタリング、探索、querying、validation、マッシュアップ、reasoning、分析等の機能をサポートする。またセマンティック・コンテンツを取り込むためのアクセス制御機能やオントロジー管理といった機能も提供する。




#### 2.1.3.2 Resource Type

リリース 3 では、以下の新規リソースを規定している。

##### 2.1.3.2.1 authorizationDecision

アクセス制御の決定に関するリソースで、<CSEBase>リソースの子リソースとなる。本リソースが UPDATEリクエストに含まれていたら、Hosting CSEは、TS-0003で規定されているPolicy Decision Point (PDP)として動作する。PDPはアクセス制御ポリシーに従いアクセス制御の決定をし、本リクエストのレスポンスとしてアクセス制御決定の情報を提供する。本リソース用で使用するアトリビュートは、2 つのカテゴリに分類される。decisionとstatusのアトリビュートは、アクセス制御決定のレスポンスを記述するために使用され、これ以外のアトリビュートは、アクセス制御決定のリクエストをするために使用される。

#### 2.1.3.2.2 authorizationPolicy

アクセス制御ポリシーの取得をするためのリソースで、<CSEBase>リソースの子リソースになる。本リソースがUPDATEリクエストに含まれていたら、Hosting CSEは、TS-0003で規定されているPolicy Retrieval Point （PRP)として動作する。PRPはアクセス制御ポリシーを取得し、本リクエストのレスポンスとして取得したアクセス制御ポリシーの情報を提供する。本リソースで使用するアトリビュートは、２つのカテゴリに分類される。combiningAlgorithmとstatusのアトリビュートは、アクセス制御ポリシーのレスポンスを記述するために使用され、これ以外のアトリビュートは、アクセス制御ポリシー取得のリクエストをするために使用される。

#### 2.1.3.2.3 authorizationInformation

アクセス制御情報の取得をするためのリソースで、<CSEBase>リソースの子リソースになる。本リソースがUPDATEリクエストに含まれていたら、Hosting CSEは、TS-0003で規定されているPolicy Information Point （PIP)として動作する。PIPはアクセス制御情報を取得し、本リクエストのレスポンスとして取得したアクセス制御情報を提供する。本リソースで使用する子リソース・アトリビュートは、２つのカテゴリに分類される。<role>リソース、<token>リソース、statusアトリビュートは、アクセス制御情報のレスポンスを記述するために使用され、これ以外のアトリビュートは、アクセス制御情報のリクエストをするために使用される。

#### 2.1.3.2.4 localMulticastGroup

CSEがマルチキャストグループのメンバーであることを明示するために使用する。本リソースは<CSEBase>リソースの子リソースになり、1つの<CSEBase>リソースに複数の<localMulticastGroup>グループが含まれるケースもある。

#### 2.1.3.2.6 AEContactList

IN-CSEの<CSEBase>の子リソースとして生成され、<AEContactListPerCSE>リソースを子リソースに含む。本リソースを使用するCSEの生成・更新・削除があった場合、本CSE は、IN-CSEへNOTIFYリクエストを送信する。

#### 2.1.3.2.7 AEContactListPerCSE

CSEがAE-ID (SP-relative-Resource-IDs of an AE)を参照する場合、AE-IDリスト等の情報を規定。例えば、CSEが、アナウンスメント、notification target、group member ID等を介して、<AE>リソースを参照する場合、本CSEは、IN-CSEへNotificationを送信する。

#### 2.1.3.2.8 transactionMgmt

複数のoneM2Mリクエストprimitiveで構成されるトランザクションの処理の開始・管理をするために使用する。

#### 2.1.3.2.9 transaction

１つのoneM2Mリクエストprimitiveで構成されるトランザクションの処理の開始・管理をするために使用する。本リソースは、oneM2Mトランザクションの対象となる全リソースの子リソースとして生成される（<request>, <delivery>, <transaction>, <transactionMgmt>を除く）。本リソースのCREATEリクエストは、< transactionMgmt >リソースをホストするCSEによって生成されるケースや、個々の<transaction>リソース自身で生成するといった<transactionMgmt>リソースと独立した形で生成するケースもある。

#### 2.1.3.2.10 triggerRequest

デバイス・トリガリングのリクエスト開始時に使用し、IN-CSE上でインスタンスを生成する。本リソース生成が成功した場合、IN-CSEからターゲットとなるデバイス(3GPP UE等)へデバイス・トリガリン

グを開始する結果となる。ペンディングされたリクエストは、本リソースを削除することで取り消される。

#### 2.1.3.2.11 ontologyRepository

<CSEBase>リソースの子リソースとして使用し、oneM2Mシステムの内部・外部のオントロジーを管理・表現するため、1つ以上の<ontology>子リソースを持つ。<ontology>リソース上でCRUDオペレーションを実行するため、明示的なオントロジーが<semanticDescriptor>リソースで参照される場合、本オントロジーは、oneM2Mシステム内での生成、探索、取得、更新、削除のオペレーションで使用する。

本リソースは、AE/CSEからのセマンティクスのValidationリクエストを受信するためのインタフェースとして、子リソース<semanticValidation>リソースが含まれている。

#### 2.1.3.2.12 ontology

< ontologyRepository >リソースの子リソースで、ontologyのrepresentationを保存するために使用する。このrepresentationは、既存ontologyの再利用、外部でのみ利用するontologyのサポート、システム内でインポートされたontologyサポート等の要求条件をふまえ、様々なフォーマットのontology記述を含んでいる。本オントロジー記述は、oneM2Mシステムのセマンティクス関連機能で利用できる。

複数のオントロジー・バージョン、様々なフォーマットでのアクセスを想定し、ontologyFormatアトリビュートは、oneM2MシステムがontologyContent内で利用可能な情報を解釈するため、必要となる情報を提供する。

#### 2.1.3.2.13 semanticValidation

representationを持たない仮想リソースで<ontologyRepositoy>リソースの子リソースに相当する。本リソースは、セマンティクスのvalidationリクエスト（<semanticDescriptor>リソースのvalidationを含む）を受信するためのインタフェースである。

#### 2.1.3.2.14 semanticMashupJobProfile

本リソースはSemantic Mashup Job Profile (SMJP)を表現。SMJPは、特定のマッシュアップ・サービス（入出力パラメータ、メンバー・リソース、マッシュアップ機能等）で要求されるプロファイル・必要情報を記述している。SMJPに記述しているプロファイルを基に、Originatorsは、セマンティック・マッシュアップの結果を生成・保存するセマンティック・マッシュアップを生成する。

#### 2.1.3.2.15 semanticMashupInstance

本リソースは、Semantic Mashup Instance (SMI)を表現。Mashup RequestorとしてCSE/AEはセマンティック・マッシュアップ機能を搭載する別のoneM2M CSEへ<semanticMashupInstance>リソース生成をリクエストできる。各生成された<semanticMashupInstance>リソースは、セマンティック・マッシュアップ・ジョブ・プロファイル（<semanticMashupJobProfile> リソース等）に対応する。言い換えると、<semanticMashupInstance>リソースが、どのようにマッシュアップ・オペレーションを実行するかは、相対する<semanticMashupJobProfile>リソースで規定される。

#### 2.1.3.2.16 mashup

representationを持たない仮想リソースで、<semanticMashupInstance>の子リソースに相当する。RETRIEVEオペレーションが、本リソースへ送信された場合、本リソースは、親リソースとなる<semanticMashupInstance>を基にして.マッシュアップ結果の生成・処理のトリガリングを行う。

#### 2.1.3.2.17 semanticMashupResult

マッシュアップ結果を保存するリソースで、<semanticMashupInstance>の子リソースに相当する。<semanticMashupInstance>上でセマンティック・マッシュアップのオペレーションを行った場合、本リソースはHosting CSEによって自動的に生成される。

#### 2.1.3.2.18 multimediaSession

2つのAEが関与するマルチメディア・セッションについての情報を表現し、<AE>リソースの子リソースとして、Originatorによって生成される。本リソースの生成・更新・削除は、AEがマルチメディア・セッションの管理（セッション確立・切断等）をするためのトリガリングとなる。本リソースで記述されるマルチメディア・セッションは、非oneM2Mプロトコルを使用する2つのAEによって管理される。

#### 2.1.3.2.19 crossResourceSubscription

複数のターゲット・リソースセット（既存<subscription>リソースやサブスクリプション可能なoneM2Mリソース）上で、cross-resourceサブスクリプションを表現。タイムウィンドウ内で指定されたターゲット・リソース数になったときに変更が発生するコンフィギュレーションの場合、Hosting CSEは、cross-resource notificationを生成する。本リソースは、cross-resource notification生成のため、関与するターゲット・リソースを特定する。

#### 2.1.3.2.20 backgroundDataTransfer

IN-CSEがフィールド・ノードのデータ配信管理の為、バックグラウンドデータ配信のネゴシエーションをするためのリクエストで使用する。本リソースのアトリビュートは、バックグラウンドデータ配信の特徴、伝送ポリシー選択のガイダンス、データ伝送に関与するフィールド・ノード情報を提供する。

### 2.1.3.3 Trust Enabling Architecture

#### 2.1.3.3.1 Distributed Authorization

Originator（AE/CSE）が、Hosting CSEのリソースへアクセスするために、tokenを利用したテンポラリなパーミッションを発行するDynamic Authorizationとは異なり、他のCSEにあるアクセス制御ポリシーを利用するフレームワークである。本フレームワークは、Policy Enforcement Point (PEP)、Policy Decision Point (PDP)、Policy Retrieval Point (PRP)、Policy Information Point (PIP)の4つのサブコンポーネントによって構成される。これは、PEP, PRP, PDP, PIPが異なるノードを介して分配されることを意味している。例えば、PEPはASN/MNに配置され、PDPはINに配置されるといったデプロイメントが想定される。本文書では、参照モデルと各サブコンポーネント間のインタラクションの概要を記載しており、詳細は、TS-0003で規定している。

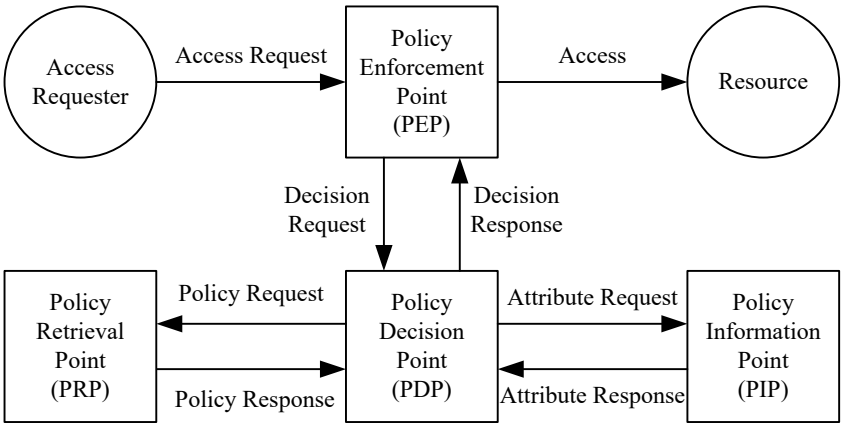



図2.1.3.3.1 Distributed Authorizationの参照モデル

### 2.1.4　TS-M2M-0011v3.0.1 - 共通用語

本文書は、oneM2M仕様書内で参照される専門技術用語、定義、および略語をまとめて記述したものである。oneM2M文書と関連した共通の定義と略語を収集することにより、用語がoneM2M文書で一貫して用いられることを保証する。また、複数文書で使用される技術用語について有用な参照を提供する。

なお、個々のoneM2M技術仕様書には、本文書で示す共通用語以外にそれらの仕様書に特有の定義と略語のための章も存在する。

## 2.2　広範なサービス展開への強化

### 2.2.1　Home Appliances Information Model and Mapping　家電用デバイス管理モデルとマッピング (TS-0023)

本文書は、oneM2Mにおける家電用デバイスの管理モデルを定めたものである。デバイス管理モデルの仕様は、図2.2.1に示すSmart Device Template(SDT) 3.0を活用して規定されている。

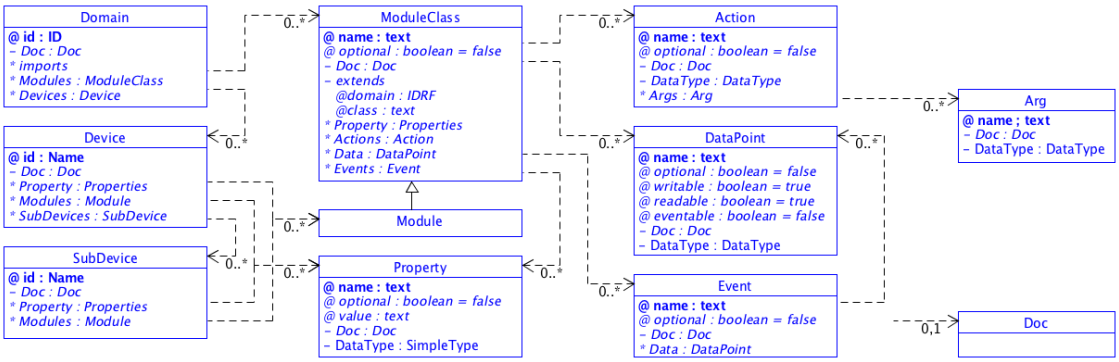



図2.2.1　Smart Device Template 3.0の構成

Open Mobile Alliance (OMA)やOpen Connectivity Foundation (OCF)，ECHONETといった標準化団体は，家電やヘルスケアデバイスに関して独自のデバイスモデルを規定している．そこで，これらのデバイスモデルと容易にインターワーク出来るよう，oneM2Mでも主に家電に関して独自のデバイスモデルを規定した．それがSDTを活用したHome Appliances Information Model (以下デバイス管理モデル)である．

SDTはデバイス管理モデルにおける各クラス間の包含関係を示しており、デバイス管理モデルのひな形と言える。例えばデバイスクラス(Device)を見ると、サブデバイスクラス(SubDevice)と属性クラス(Property)と機能クラス(Module)から成ることが分かる。そして、「AとBという機能クラスから成るデバイスクラスは冷蔵庫デバイスと呼ぶ」というように、各クラスの定義そのものがデバイス管理モデルと呼ばれている。

デバイス管理モデルは、デバイスクラス・サブデバイスクラス・機能クラス・データポイントクラスなどが規定されており、その具体例は表2.2.1の通りである。

表2.2.1　デバイス管理モデルの例

| クラス | 具体例 |
|---|---|
| デバイスクラス(Device) | deviceDishWasher, deviceFreezer, deviceLight等 |
| サブデバイスクラス(SubDevice) | subDeviceCuff, subDevicePowerOutlet |
| 機能クラス(Module) | timer, doorStatus, filterInfo, battery等 |
| データポイントクラス(DataPoint) | targetTimeToStart, voltage, size等 |

センサデータなどの動的データはデータポイントクラス(DataPoint)に格納され、データポイントクラスを自分で持てないデバイスクラスは、データポイントクラスを自分で持てる機能クラスを最低一つは持たないと動的データを持てないことになる。一方、製造番号などの静的データは属性クラス(Property)に格納され、属性クラスを自分で持てるデバイスクラスは機能クラスを持たなくても静的データは持てる。なお、静的データの項目は様々なデバイス間で共通しているため、全デバイスクラスの共通属性クラス(Common Property)が規定されている（Common Property自体の記載はTS-0001）。

このデバイス管理モデルをoneM2Mリソースにマッピングする方法について、本文書では<flexContainer>リソースの運用規定という形で規定されている。各クラスのshortnameやcontainerDefinitionの属性値、XSDの定義が含まれている。また、SDTの各要素について、oneM2M Base Ontologyとのマッピングについても示されている。さらに，先述したOMAやOCFの独自データモデルとのインターワーク方法についても，本文書に規定されている．

### 2.2.2　TR-M2M-0026v3.0.1 – 車両領域への適用性

現在の oneM2M システムが車両領域においていかに適用されるかを検証すると共に、将来の oneM2M リリースが本領域向けにサポートするであろう拡張機能の検討を含んでいる。また、車両領域のユースケースやそれらに付随する潜在的な要求条件も分析している。

ITS のような車両分野のアーキテクチャを開発するため、多くの国際組織が本領域に関わる技術や標準化を議論している。

表 2.2.2-1 車両領域標準

| No | Organization | Sector | Focus point | Major topics |
|---|---|---|---|---|
| 1 | ISO | TC204, TC22 | ITS services | Cooperative System, In-vehicular gateway |
| 2 | ITU-T | SG16 | Telecommunication | Vehicle Gateway Platform, Communication protocol |
| 3 | ETSI | TC ITS | Network system, Radio Technique | Cooperative ITS, DSRC |
| 4 | W3C | Automotive WG | Web services | Web-API for vehicles |
| 5 | ITU-R | SG5/WP5A | Wireless communication | V2V/V2I communication (DSRC) |
| 6 | IEEE | 802.11p + P1609 | Wireless communication | V2V/V2I communication (DSRC) |
| 7 | 3GPP | - | Wireless communication | V2V/V2I communication (Cellular) |

本文書に記述している車両領域の M2M アーキテクチャは、自動車メーカーやサプライヤーのみならず、通信事業者や政府までも含んだ広い範囲の協調を加速し、結果として安全性、快適性、エコ親和性を発展させることになる。リファレンスアーキテクチャ例を図 2.2.2-1 に示す。

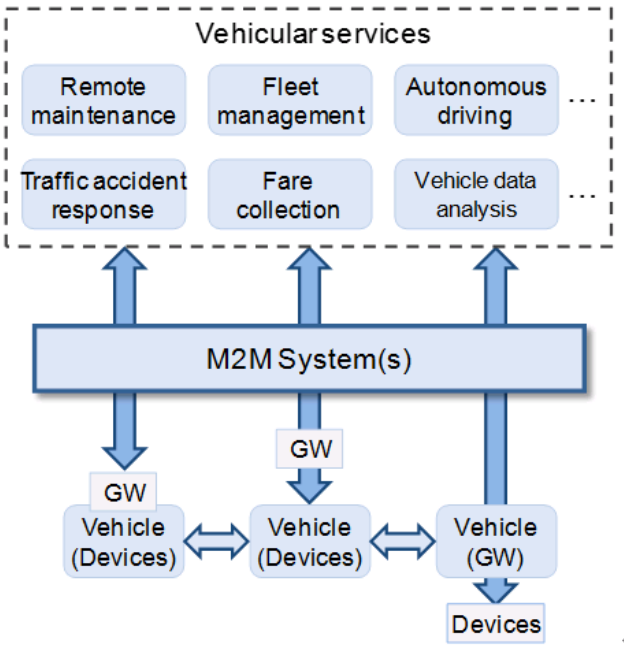



図2.2.2-1 車両領域アーキテクチャ

車両領域のユースケースとして以下が記述されている。車両診断＆メンテナンス、リモートメンテナンス、交通事故情報収集、フリートマネジメント、ETCサービス、タクシー広告、車両データサービス、自動運転、車両データワイプサービス、ジオフェンスに基づく車両管理、車両ECU向けのセキュアなOTAファームウェア更新、自動車/自転車シェアサービス、スマートパーキング、レジストレーション不要の車両情報広報、車両位置情報プライバシー保護、車両分野サービスの継続性、最適速度推奨、自動運転。

上記ユースケースから71の潜在的な要求条件が導かれ、四つのハイレベルアーキテクチャタイプがマッピングされた。

適用に向けた課題は、地理位置情報、処理遅延、レジストレーション管理、セキュリティ、クロスリソース起因のイベント対応、加入者データアグリゲーション等であり、AE 接続情報の維持－IN-CSE が全 CSE へ通知、AE 接続情報の維持－IN-CSE が影響のある CSE へ通知、AE/CSE が複数リソースの同時変化による自動通知に加入、M2M GW のような中間ノードの加入者要求グループ化/アグリケーションによるメッセージ処理負荷軽減、セキュアなチャネルの確立、ハードウェアセキュリティ部材等が解決のアプローチである。

## 2.3 プロトコルバインディングの強化

### 2.3.1 TS-M2M-0004v3.10.1 - サービス層 API 仕様（共通部）

本文書では、oneM2M に準拠するシステム、M2M アプリケーション、及び他の M2M システムのための通信プロトコル（API仕様共通部）を規定している。また、oneM2M で定義される参照点に対応するための共通データフォーマット、AE/CSE間でのメッセージシーケンスも規定している。

APIの呼び出しは、呼び出す側を “Originator”、呼び出される側を “Receiver”として、 TS-M2M-0001で規定されているoneM2Mリソース・アドレスに対するCRUD(Create/Retrieve/Update/Delete)操作を行う。このCRUD操作にリソース操作を伴わないメッセージ交換のみを行うためのNotify操作を合わせた “CRUD+N操作”をGeneric Procedureとして説明している。 さらに、Generic Procedureに含まれる個別の内部処理については、Common Procedureとして別途詳細を説明する構成となっている。

oneM2M Message Primitive(リクエストとレスポンス)によるメッセージングはシステム内部の仮想的なやりとりであり、実際の通信は “Protocol Binding”仕様 (リリース1ではHTTP、CoAP、MQTT向けがある)で規定される通信プロトコルへのマッピング形で実現される。

これは、M2M通信プラットフォームでは多種多様なデバイスの併用を想定し、Protocol Bindingを定義すればデバイスがサポートする様々なプロトコルの特性を最大限に活かした連携を可能にするためである。

上記の目的を達成するために、API呼び出しにおけるパラメータの項目と型を揃える必要があり、TS-0004では単純型/複合型/列挙型のデータ型定義をW3CのXSD(XML Schema Description)仕様を使って定義している(TS-0004の添付ファイル: XSDbudle-v2_7_1.zip)。

XSDで定義されたデータ型は、プロトコルメッセージ上ではXSDを元にしてXMLまたはJSON(Javascript Object Notation)形式のデータとしてやりとりされるが、転送データサイズを低減するため最大3文字の“shortname”に置き換えて表現する。これらの変換ルールはXML版が”XML serialization”、JSON版が “JSON serialization”として説明されている。

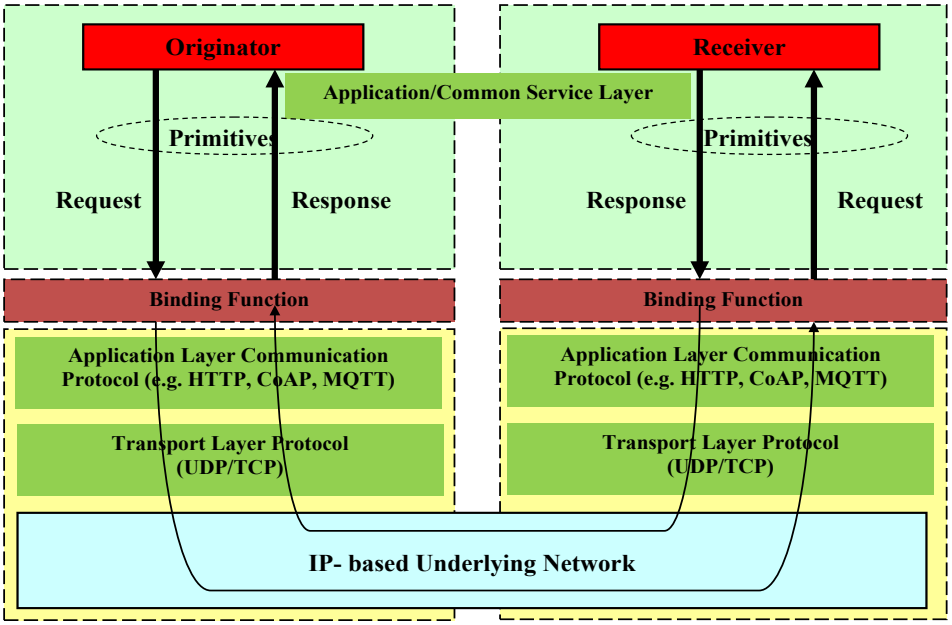



図 1.3.1-1　Request/Response プリミティブ通信のマッピング例

Version 3 では主に下記の追加等がなされた。

- Data type の追加等
- Semantic query の追加
- Resource Type の追加等
- Multicast group procedures の追加
- Mcn procedure の追加

### 2.3.2 TS-M2M-0008v3.3.0- サービス層 API 仕様（CoAP 用）

本文書ではoneM2M準拠システムで用いられる通信プロトコルのうちRESTful CoAPに関するプロトコルについて、以下を規定している。

- oneM2Mプロトコルプリミティブタイプ とCoAPメッセージとの対応
- oneM2Mレスポンスステータスコード（成功／不成功）とCoAPレスポンスコードとの対応
- oneM2Mパラメータ依存でのCoAPクライアント／サーバの動作の定義

#### 2.3.2.1 概要

CoAPレイヤに必要な特性とメッセージフォーマット等が記載されている。
必要な主な特性は下記の通り。

- 4 バイトのバイナリ CoAP メッセージヘッダは IETF RFC 7252 の 3 章に定義される
- Confirmable (CON)、Acknowledgement (ACK)、Reset (RST) メッセージをサポートしなければならない
- GET、PUT、POST、DELETE 方法をサポートしなければならない
- oneM2M レスポンス状態コードパラメータマッピングのため、CoAP レスポンスコードをサポートしなければならない
- Uri-Host、Uri-Port、Uri-Path、Uri-Query をサポートしなければならない
- ペイロードのメディタタイプを示すため、Content-Type オプションが用いられなければならない

CoAPのメッセージフォーマットは以下の通り。

- CoAP メッセージは一つの UDP データグラムのデータセクションを占める
- CoAP メッセージフォーマットは 4 バイトの固定長ヘッダをサポートする
- 固定サイズヘッダに、0～8 バイト長のトークン値が続く
- トークン値に、ゼロ個以上の TLV フォーマットの CoAP オプションが続く
- CoAP オプションに、ペイロード部分が続く

#### 2.3.2.2 CoAP メッセージマッピング

CoAPメッセージとoneM2Mプリミティブとのマッピングは以下の場合に適用される。

- Originatorがリクエストプリミティブを送信するとき
- ReceiverがCoAPメッセージを受信するとき
- Receiverがレスポンスプリミティブを送信するとき
- OriginatorがCoAPメッセージを受信するとき

oneM2Mプリミティブパラメータが、CoAPリクエスト/レスポンスメッセージを構成するために、対応するCoAPメッセージフィールドにどのようにマッピングされるかを規定している。

#### 2.3.2.3 セキュリティ面での配慮

CoAPは認可/認証のためのプロトコルプリミティブを持たないため、HTTPと同様である。

### 2.3.3　TS-M2M-0009v3.2.0- サービス層 API 仕様（HTTP 用）

本文書ではoneM2M準拠システムで用いられる通信プロトコルのうちRESTful HTTPに関するプロトコルについて、以下を規定している。

- oneM2Mプロトコルプリミティブタイプと HTTP方式との対応
- oneM2Mレスポンスステータスコード（成功／不成功）とHTTPレスポンスコードとの対応
- oneM2MリソースとHTTPリソースの対応

#### 2.3.3.1 概要

oneM2Mのリクエスト／レスポンスプリミティブパラメータはそれぞれ、HTTPのリクエスト／レスポンスメッセージにマッピングできる。マッピングの例を図2.3.3-1に示す。AEはHTTPクライアントとしての役割を、MN-CSE（AEのRegister）はHTTP Proxy Serverとしての役割を、IN-CSEとMN-CSE（リソースホスト）はHTTPサーバとしての役割を果たす。

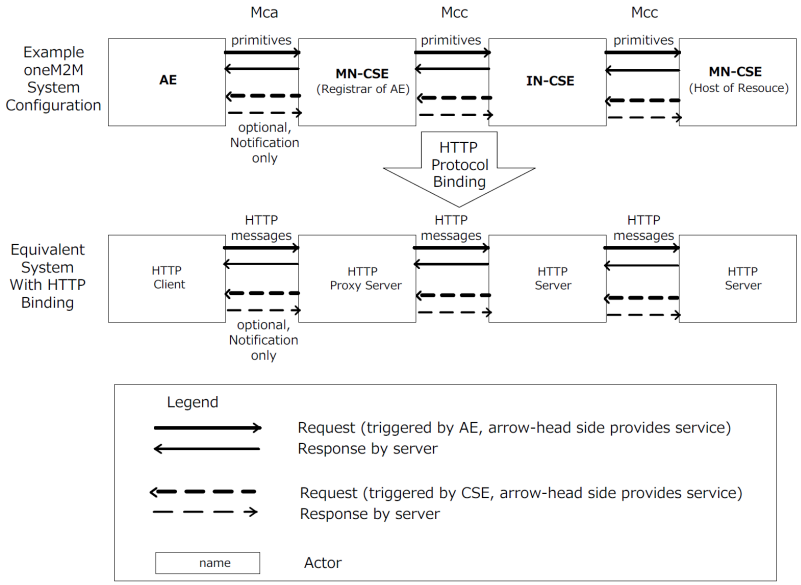



図2.3.3-1　oneM2MエンティティとHTTPクライアント／サーバとの対応関係

一つのリクエストプリミティブは一つのHTTPリクエストメッセージに、一つのレスポンスプリミティブは一つのHTTPレスポンスメッセージにマッピングされる。

#### 2.3.3.2 HTTP メッセージマッピング

oneM2MプリミティブとHTTPメッセージとのマッピングは以下の場合に適用される。

- Originatorがリクエストプリミティブを送信するとき
- Receiverがリクエストプリミティブを受信するとき
- Receiverがレスポンスプリミティブを送信するとき
- Originatorがレスポンスプリミティブを受信するとき

oneM2Mプリミティブパラメータが、対応するHTTPメッセージにどのようにマッピングされるかを、リクエストライン、ステータスライン、ヘッダ、メッセージ本文、メッセージルーティングについて規定している。

#### 2.3.3.3 セキュリティ面での配慮

HTTPリクエストメッセージでの認証、トランスポートレイヤセキュリティについて記述している。

### 2.3.4　TS-M2M-0010v3.0.0 - サービス層 API 仕様（MQTT 用）

本文書ではoneM2M準拠システムで用いられる通信プロトコルのうちMQTTをトランスポートプロトコルに使う場合の仕様を規定している。

MQTTプロトコル用のMcaインタフェースとMccインタフェースにおけるプリミティブ通信(メッセージ・フロー)について以下を規定している。

1) CSE/AEのMQTTシステムへの接続手順
2) Originator(CSE/AE)によるリクエスト送信時のMQTTメッセージ作成･送信手順
3) oneM2Mリクエストの受信先となるReceiver側の準備手順
4) Receiverによるレスポンス送信時のMQTTメッセージ作成･送信手順

#### 2.3.4.1 プロトコル対応

図2.3.3-1に示すようにAE/CSEは､AE-ID/CSE-IDをMQTTクライアントに送ることでMQTT対応プロセスを起動する。MQTT クライアントはリクエストを受信した後、MQTT サーバに接続する。

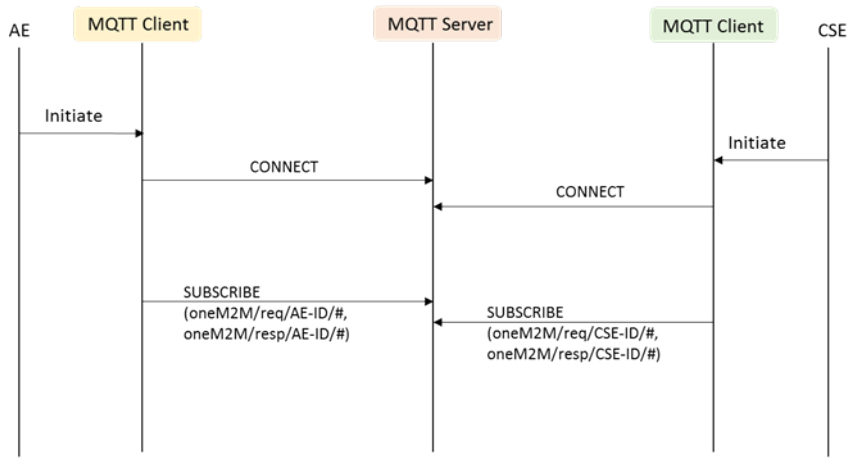



図2.3.3-1　MQTT対応での起動手順

AEとCSE間でoneM2MのMca参照点経由でリクエスト／レスポンスメッセージ送受信をMQTTにより行う場合の例を図2.3.3-2に示す。

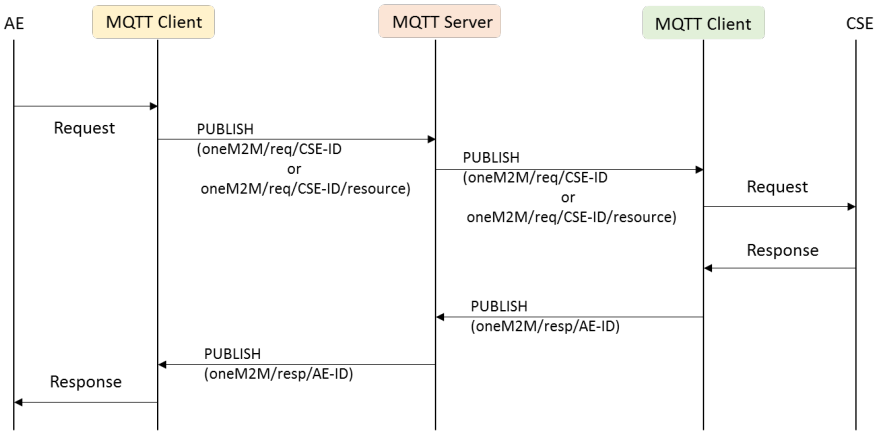



図2.3.3-2　MQTTによるリクエスト／レスポンスメッセージ送受信

#### 2.3.4.2 セキュリティ

MQTTサーバは接続するときにクライアント(CSEとAE)を認証する。クライアントは相互に認証せずにMQTTサーバを使用する。認可、認証、MQTTによる認可について規定している。

### 2.3.5 TS-M2M-0020v3.0.0 – サービス層 API 仕様（WebSocket 用）

本文書では、oneM2M 準拠システムで用いられる通信プロトコルでWebSocket Protocolをトランスポートプロトコルに使う場合の仕様を規定している。

WebSocketプロトコルは、ファイヤウォールやNATが存在するネットワークであっても双方向の通信を可能にするプロトコルで、WebSocketバインディングを使えば、oneM2Mのプリミティブ・メッセージはクライアント/サーバの区別なく双方向で送受信できる。

以下の図では、WebSocketの確立からoneM2Mメッセージの送受信が行えるようになるまでの処理フローの一例を説明している。

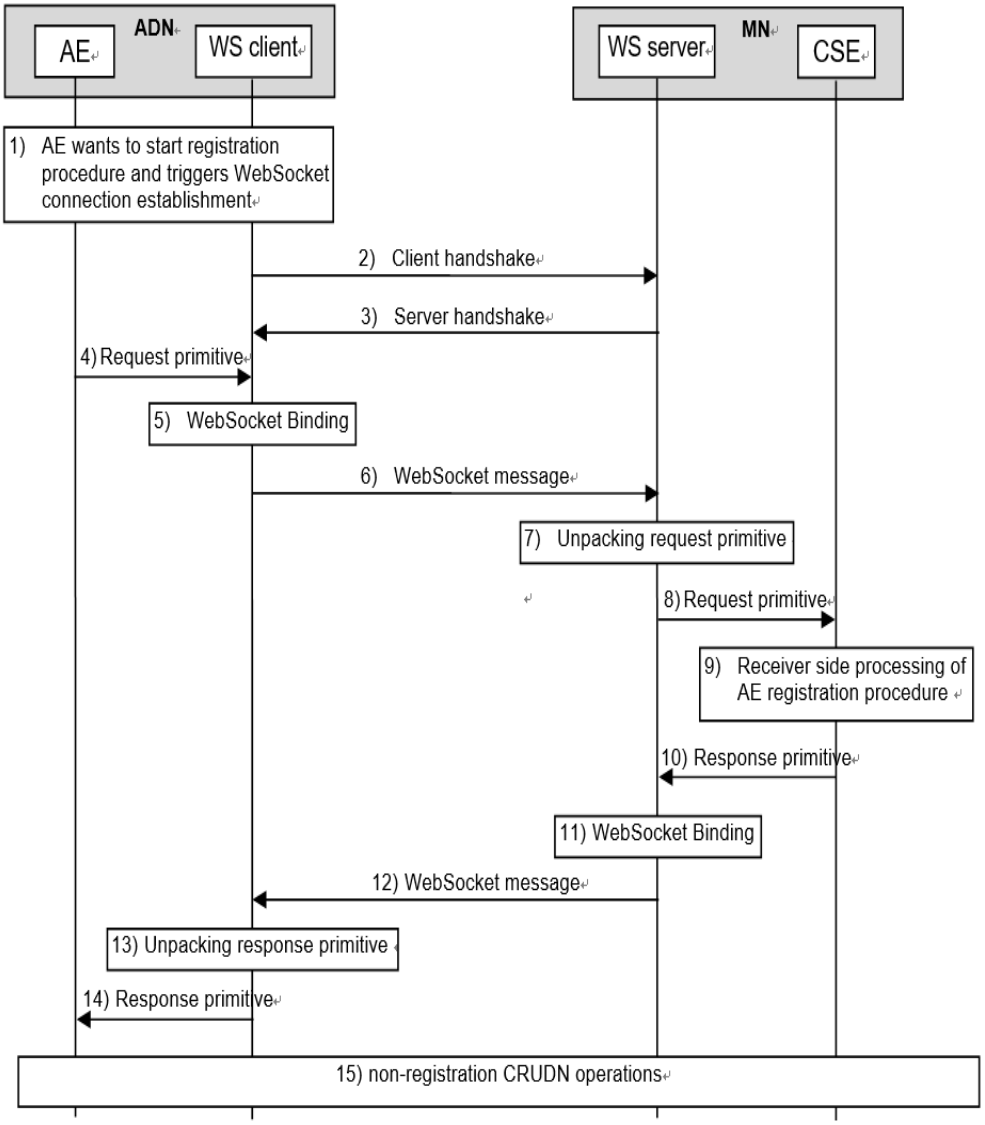



図 2.3.4-1 WebSocket バインディングのメッセージフローの一例

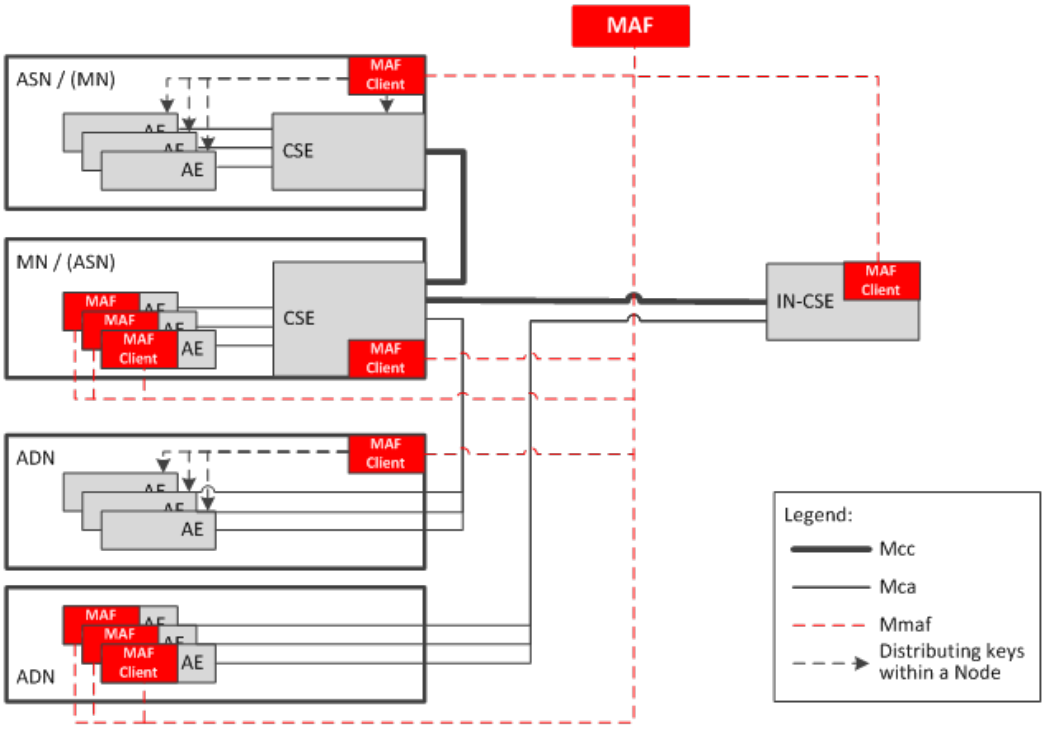
なお、WebSocketバインディングでは、プリミティブ・メッセージのシリアライゼーション形式としてRel-1までにあったXML、JSONテキストに加え、バイナリ表現でJSONデータの転送効率を向上させたCBORエンコーディングもサポートしている。

### 2.3.6　TS-M2M-0032 v.3.0.0　MAF/MEF インターフェース仕様書

・MAFインターフェースは、MAF機能を搭載したMAFクライアント同士を容易に相互接続できるようにするためのMCC/MCAリファレンスポイントを簡素化したものである。

MAFクライアントは、oneM2Mのノード(ADN, ASN, IN, MN等), CSEあるいはAEにそれぞれ実装されMAF間同士が相互接続される

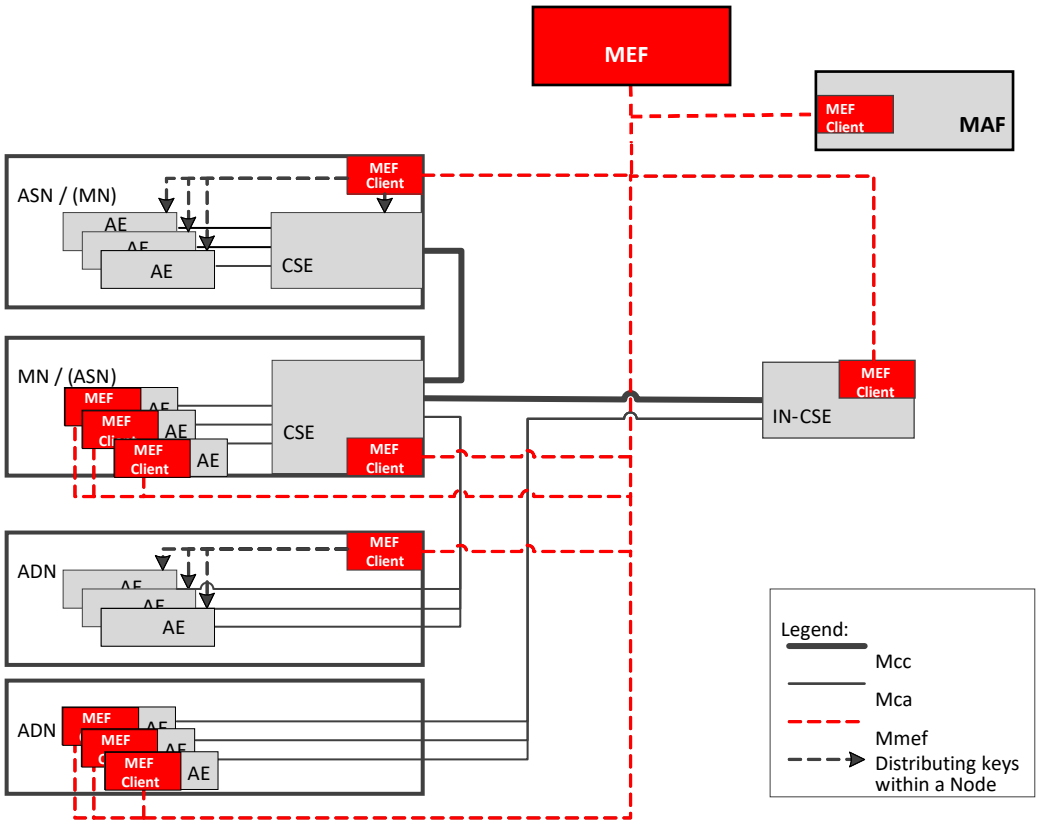
MAFクライアントとMAF間のレファレンスポイントMAFの定義を図に示す。




・MEFインターフェースは、oneM2Mリモート・セキュリティ・アーキテクチャで、oneM2M TS-0003[2]の6.1.2.1節にフレーワークが規定されている。

MAFと同様にMEF機能とMEFクライアントから構成されるMCC/MCAリファレンスポイントであり、MEFクライアントはoneM2Mノード(ADN, ASN, IN or MN), CSE,AEがMEF経由で相互接続される。MEFインターフェースには1)Pre-Provisioned Symmetric Key RSPF, 2)Certificate-Based RSPF,　3)GBA-based RSPFが規定されている。

MEFクライアントとMEF間のリファレンスポイントMAFの定義を図に示す。




## 2.4　セマンティック・インターオペラビリティ

### 2.4.1　TS-M2M-0012 v3.7.3 – 基本オントロジー

oneM2M 基本オントロジーは、oneM2M で取り扱うデータのセマンティクスを特定するための基本的なフレームワークを構成する。セマンティクスインターワーキングを実現するために、その概念のサブクラスが他団体により定義されることが期待される。特に、（エリアネットワークやデバイス等の）非 oneM2M システムとのインターワーキングの促進が望まれる。

oneM2M の基本オントロジーの概要説明から始まり、その中では、導入する動機や目的、外部オントロジーとの利用、オントロジーが見抜くもの、エリアネットワークとのインターワーキングのため利用が記載されている。

その後は、クラスとプロパティの表現、外部オントロジーのインスタンス化、汎用インターワーキング IPE を用いた通信の機能仕様、汎用インターワーキングの Flex Container のリソースタイプと詳細説明する構成になっている。

### 2.4.2　Ontology Based Interworking　オントロジーベースのインターワーク　(TS-0030)

本文書では，前章で紹介したoneM2M Base Ontologyを用いたインターワークの方法を規定している．oneM2M仕様においてだけではなく，一般的にオントロジーとは概念体系と訳され，イメージ図としてはノ

ードとノードを繋ぐ矢印によって構成されたグラフが用いられることが多い．例えば，「A（主語）はB（目的語）をCする（述語）」という関係があるときは「A→B」と表され，Cは矢印である．このように，主語・目的語・述語を用いてノード間の関係性を表現する技術をセマンティクスと呼ぶ．

オントロジーベースのインターワークでは，セマンティクスが不可欠である．本文書ではoneM2M Base Ontology以外にZigBeeやSAREFといった外部規格のオントロジー同士のインターワーク方法が紹介されているが，その際もセマンティクスによってオントロジー同士を融合させている．

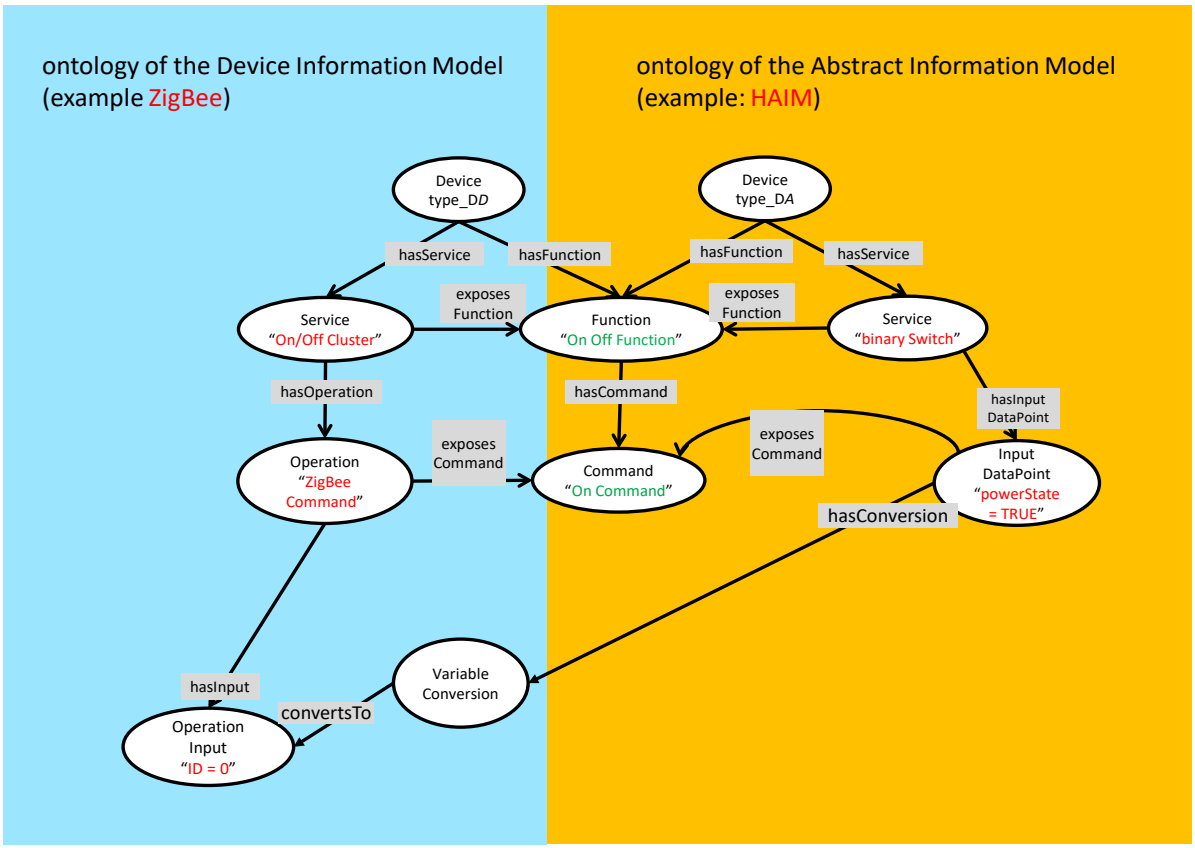



Figure 1: Ontologies relations

本文書では，オントロジーやセマンティクスの概説の後に，oneM2Mのプロキシである IPEがoneM2M Base Ontologyの各クラスをoneM2Mリソースとして表現する手順の説明がある．そして，その表現の際に使用するXSDが最後に示されている．

### 2.4.3 Semantics Support　セマンティクスのサポート　(TS-0034)

本文書では，13個あるCSFの一つであるセマンティクス（SEM）CSFの使い方を規定している．

セマンティクスには，主に9つのoneM2Mリソースが関与している．9つのoneM2Mリソースとは，<semanticDescriptor>，<semanticFanOutPoint>，<semanticMashupJobProfile>，<semanticMashupInstance>，<mashup>，<semanticMashupResult>，<ontologyRepository>，<ontology>，<semanticValidation>であり，本文書はこれらのCRUD手順を規定している．

また，上記9つのリソースを使うとどのような機能が実現できるかについても説明している．一般的な機能であるアクセス制御機能をはじめ，セマンティクスによってしか実現できない，意味による検索機能やオントロジー構築機能に関する規定もある．

### 2.4.4　Study on Enhanced Semantics Enablement　拡張セマンティクス適用の検討　(TR-0033)

本文書は，上記TS-0034を具体的な電文例を交えながら詳細に説明した技術文書である．上記で紹介したセマンティクスに関連しているoneM2Mリソースについて，各リソースの属性に何を書けばよいかの具体例を電文の図やイメージ図を用いて示し，セマンティクス機能を実現するにあたっての各リソースの役割を説明している．

さらに，オントロジー自体をセマンティックレイヤー，<semanticDescriptor>などのoneM2Mリソースをデータレイヤーと呼び，両レイヤーがそれぞれセマンティックを用いた要求文を受け取った場合のフローの違いを図解しており，Ontology Based Interworkingにおいて有益な説明となっている．

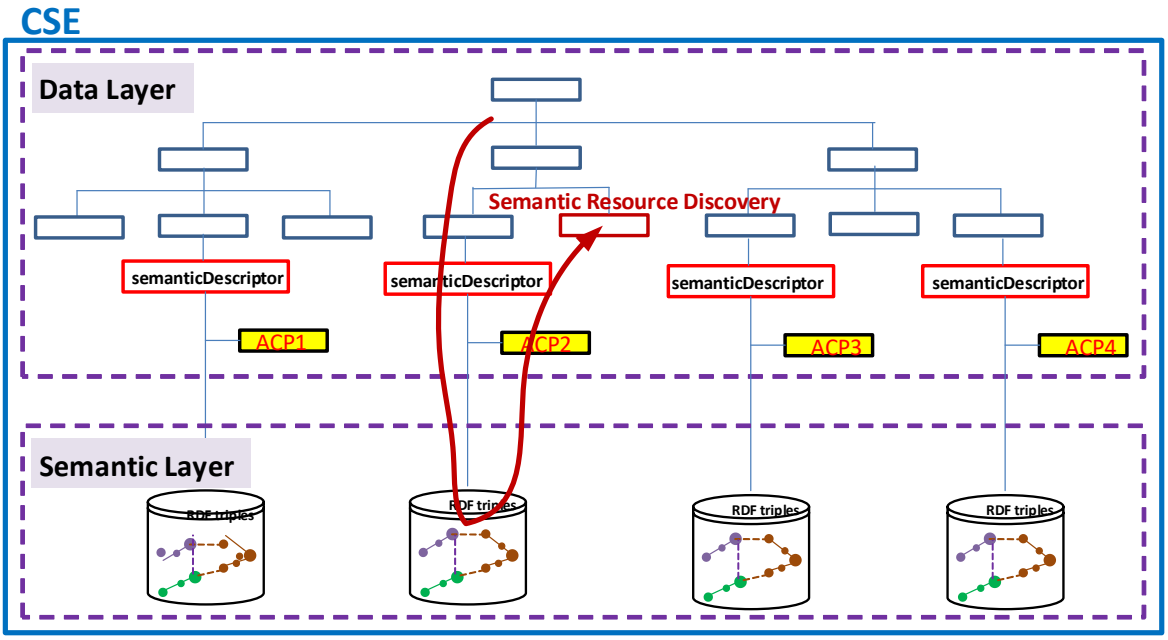
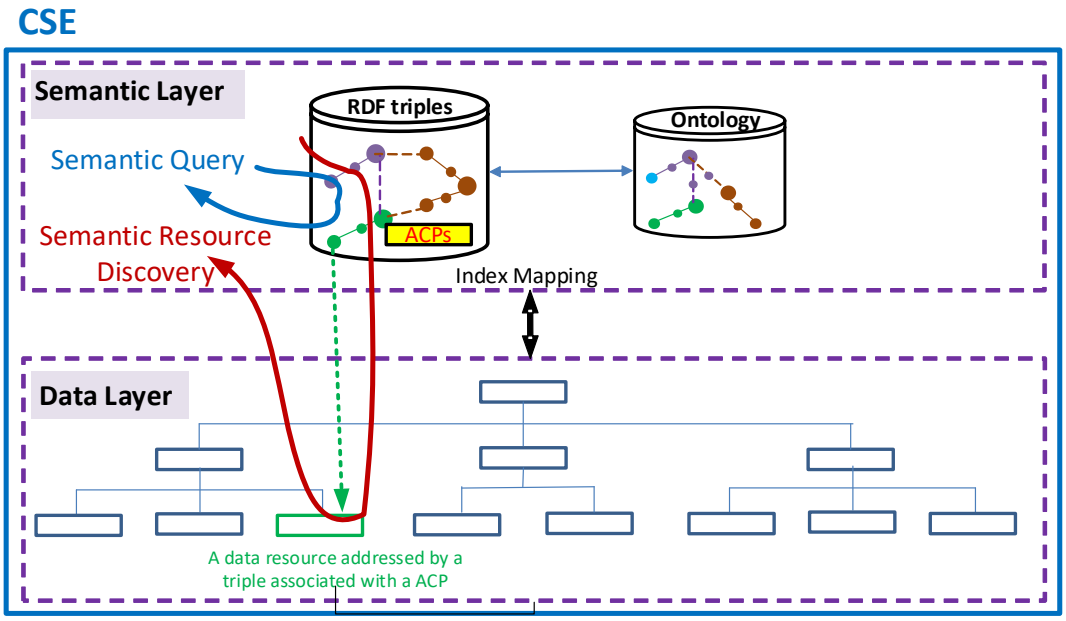
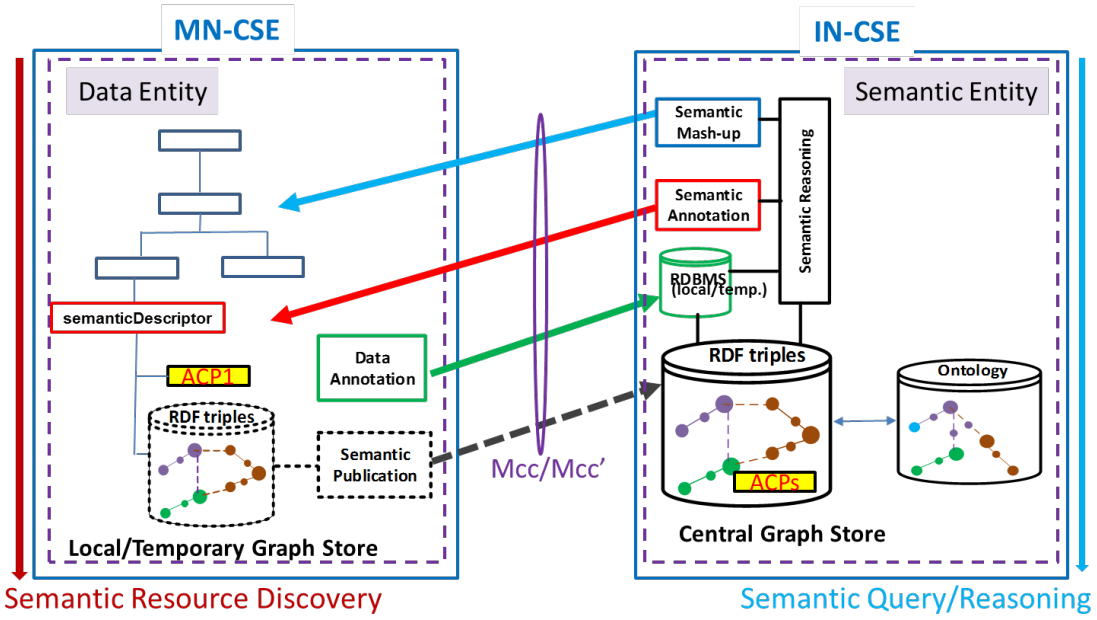



Figure 7.4.2.1-1: Hierarchically layered structure - controlled by the data layer






セマンティクスによってしか実現できない機能については先に紹介したTS-0034とほぼ同等の説明が載っている．

## 2.5 oneM2M インターワーキング・フレームワーク

### 2.5.1 Interworking Framework インターワークのフレームワーク (TS-0033)

インターワークはターゲットとするレイヤごとに下記の3種類に分けられる．

1. コネクションレイヤのインターワーク
   Wifi や 3GPP など通信プロトコルの違いを吸収することによるインターワーク
2. リソースフレームワークレイヤのインターワーク
   データ型，スキーマ，シリアライゼーションをそろえることによるインターワーク．
3. 情報モデルレイヤのインターワーク
   データ構造や語彙をそろえることによるインターワーク

これらのうち，本文書では 3. 情報モデルレイヤのインターワーク について述べており，非oneM2Mシステムをどのようにしてone M2Mリソースタイプで表すかを説明している．

AEの一種であるInterworking Proxy Entity(IPE)は，非oneM2Mシステム内のデバイスやアプリケーション，サービス等をoneM2Mリソースタイプとして表現し，そのリソースのCREATEリクエストをCSEに送ることによって，非oneM2MシステムとoneM2Mシステム間のインターワークが可能となる．本文書では，そのIPEの働きを概説するとともに，非oneM2Mシステム内のデバイスやアプリケーション，サービスを表現するoneM2Mリソースを具体的に示している．

### 2.5.2 TS-M2M-0005v3.4.0 - OMA 仕様によるデバイス管理

oneM2Mアーキテクチャにおけるアプリケーション・エンティティ（AE）は、デバイス管理に関わる特定のプロトコルやデータモデルについての知識がなくとも、CSEのデバイス管理機能（DMG CSF）を用いることで、Middle Node（MN）（例えばM2Mゲートウェイ）や、Application Service Node（ASN）およびApplication Dedicated Node（ADN）（例えばM2Mデバイス）に当たるデバイスの機能を管理することができ

る。このときDMG CSFは、Mcc参照点を通した各種「マネジメント・リソース」の操作に加えて、既存のデバイス管理技術（TR-069、OMA DM、LWM2M など）を利用することもできる。

この様子を表したのが図2.5.1-1である。oneM2M機能アーキテクチャで示されるとおりInfrastructure Node（IN）CSEと、MNまたはASNのCSEとはMcc参照点で結ばれている。ここで既存のデバイス管理技術は、マネジメント・サーバ、マネジメント・クライアント、およびその間の**mc**参照点によって構成され、それ自体はoneM2M仕様の範囲外である（破線で示されている）。

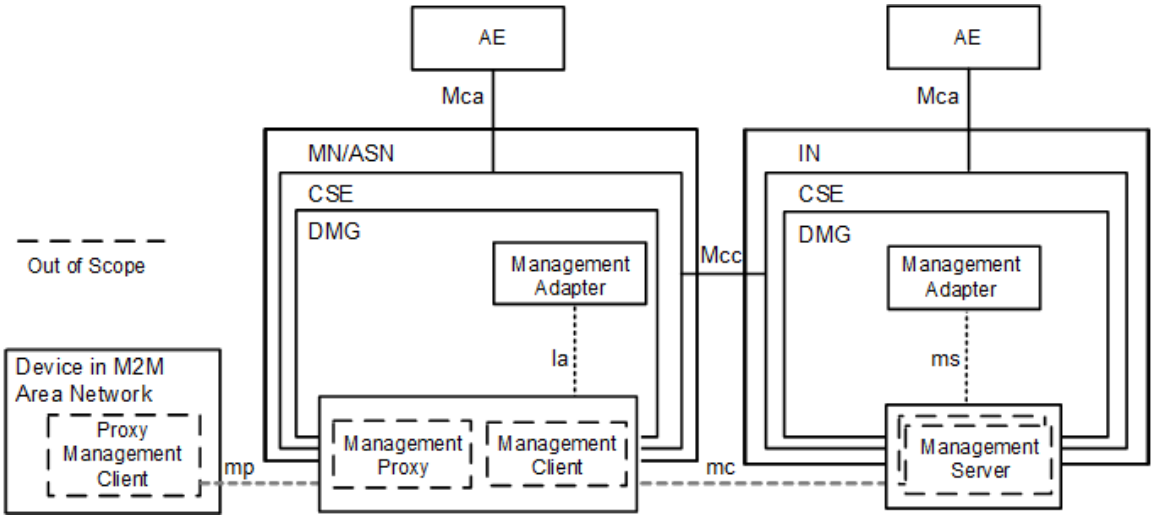



図 3.5.1-1　デバイス管理アーキテクチャ

既存のデバイス管理技術を用いてMN、ASNおよびADNを管理する場合、INのDMG CSFは、他CSEあるいはAEから受けた関連リクエストを、当該デバイス管理技術のコマンドへと適宜変換し、mc参照点を通してMN、ASNおよびADNへと送信する。またMN、ASNおよびADNから受け取ったレスポンスを逆方向に変換し、コマンドの実行結果をリクエスト送信元のCSEあるいはAEに返す。この変換・適合を行うために、DMGはマネジメント・アダプタ（MA）という機能コンポーネントを備える。INのDMG内にあるMAは、**ms**インターフェースを通してDMGと管理サーバとを適合させる。一方、MNおよびASNのDMG内にあるMAは、**Ia**インターフェースを通してDMGと管理クライアントとの間でプロトコルやデータモデルの変換・適合を担う。

本文書では、既存デバイス管理技術として Open Mobile Alliance（OMA）Device Management（DM）あるいは Lightweight M2M（LWM2M）を用いる際に必要となる、以下の内容を規定している。

- oneM2M と OMA DMおよび LWM2M における、基本データ型と識別子の対応関係
- oneM2M におけるマネジメント・リソース<mgmtObj>と、OMA DM Management Object（MO）および LWM2M Object との対応関係（図2.5.1-2）
  - oneM2Mにおける[firmware] [battery] といったリソースの各属性が、OMA DM 1.2/1.3/2.0における、どの MO の、どのノードに対応するか
  - oneM2Mにおける[firmware] [battery] といったリソースの各属性が、OMA LWM2Mにおける、どの Object の、どのリソースに対応するか

  Version 3 では、TS-0022に規定される屋外端末のリソースに関する対応関係、また、LWM2M Objectに対応するマネジメント・リソース<mgmtObj>が定義されていない場合のガイドライン等が追加された

- oneM2M における各プリミティブと、OMA DM および LWM2M の各コマンドとの対応関係。またプリミティブやコマンドのレスポンスに含まれる各ステータス・コードの対応関係
- IN-CSE (MA)とマネジメント・サーバとの、やり取り
  （セッション確立、リクエスト／レスポンス／ノティフィケーションの相互変換など。）
- oneM2MのcmdhPolicyリソースに対応する、新たなOMA DM MOおよびLWM2M Objectの内容
  （cmdhPolicyに関しては既存のMOやObjectに対応するものがないため、TS-M2M-0005で新たに定義する。）

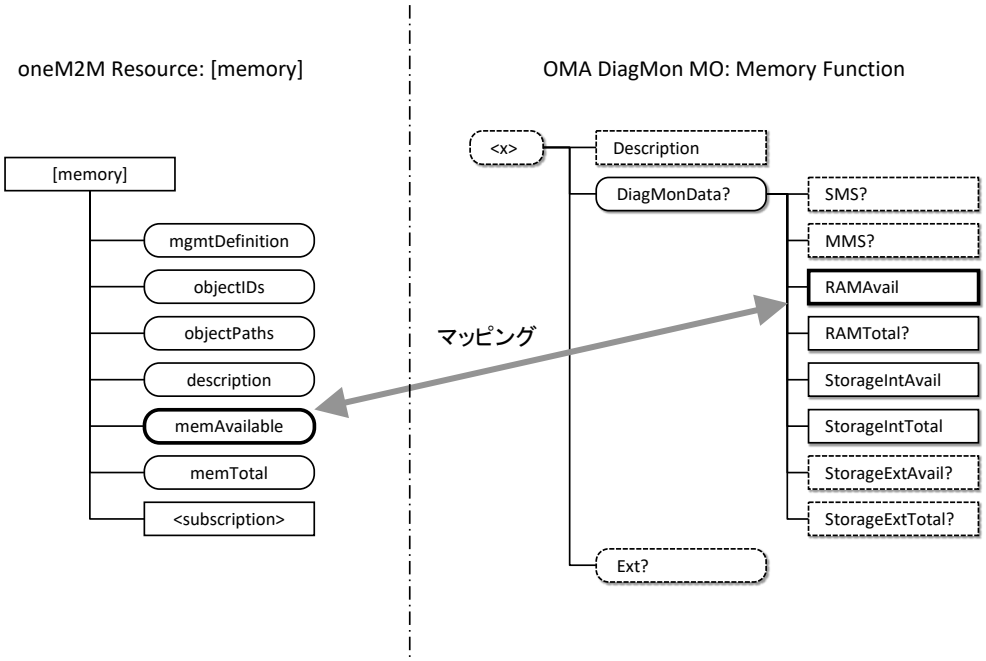



図2.5.1-2　oneM2MリソースとOMA DM MOとの対応関係（例）

### 2.5.3　Management enablement (BBF)　BBF 仕様によるデバイス管理　(TS-0006)

本文書ではoneM2Mシステムにおいて，既存デバイス管理技術として Broadband Forum (BBF) TR-069, TR-106, TR-181を用いる際に必要となるマッピングやサーバ間のやりとりを規定している．規定項目は下記の通りである．

- oneM2M と BBF TR-069およびTR-106 における，基本データ型と識別子の対応関係（5章, 6章）
- oneM2M リソースと，BBF TR-181におけるオブジェクトやパラメータとの対応関係（7章）(表2.5.2-1参照)
- oneM2Mリソースと，BBF TR-069における遠隔操作機能との対応関係（7章）（表2.5.2-1参照）
- oneM2M における各プリミティブと，BBF TR-069における各 Remote Procedure Call (RPC) との対応関係．またプリミティブや RPC のレスポンスに含まれる各ステータス・コードの対応関係（8章）
- oneM2MにおけるIN-CSEと，BBF TR-069におけるAuto-Configuration Server (ACS) とのやり取り（9章）

表2.5.3-1　対応付けられるoneM2Mリソース

| 分類 | 対応付けられるoneM2Mリソース |
|---|---|
| <mgmtObj>の一般的なspecializations | deviceInfo, memory, battery, areaNwkInfo, areaNwkDeviceInfo, eventlog, deviceCapability, firmware, software, reboot, registration, dataCollection |
| <mgmtObj> の CMDH 関連 specializations | cmdhPolicy, activeCmdhPolicy, cmdhDefaults, cmdhDefEcValue, cmdhEcDefParamValues, cmdhLimits, cmdhNetworkAccessRules, cmdhNwAccessRule, cmdhBuffer |
| RPCサポート関連のoneM2Mリソース | mgmtCmd, execInstance |

### 2.5.5　LWM2M Interworking　LWM2M とのインターワーク　(TS-0014)

本文書は、oneM2M エンティティと LWM2M エンドポイント間のインターワーキング方法を 3 パターン規定しており，それぞれのパターンにおいてどの oneM2M リソースに LWM2M オブジェクトのどの情報を入力すればよいかを説明している。3 パターンのインターワーキング方法は下記の通りである．

1. oneM2M で規定されている Content Sharing Resource（本文書内では <container> と <contentInstance>)によって LWM2M オブジェクトを包括して(encapsulate)表現する．
2. セマンティクス情報を表すことができる oneM2M リソース（本文書内では<contentInstance>）に LWM2M オブジェクトのセマンティクス情報をマッピングする．
3. <mgmtObj>に LWM2M オブジェクトを 1 対 1 の関係になるようにマッピングする．

なお，上記3パターンに共通している規定は，LWM2Mエンドポイントを有するM2Mアプリケーションは <AE>，LWM2Mエンドポイントを有するM2Mデバイスは<node>で表すという点である．

### 2.5.6　TS-M2M-0024 v3.2.2 - OCF とのインターワーク

本仕様書(oneM2M TS-0033[5])は、インフォメーション・モデル・レイヤーおける OCF デバイスとのインターワーク、および oneM2M システムにおけるリソース・インスタンスと OCF 拡張機能を実行方法とその実装を規定している。

インフォメーション・モデルの規定は、次のそれぞれの仕様書に記載されている。

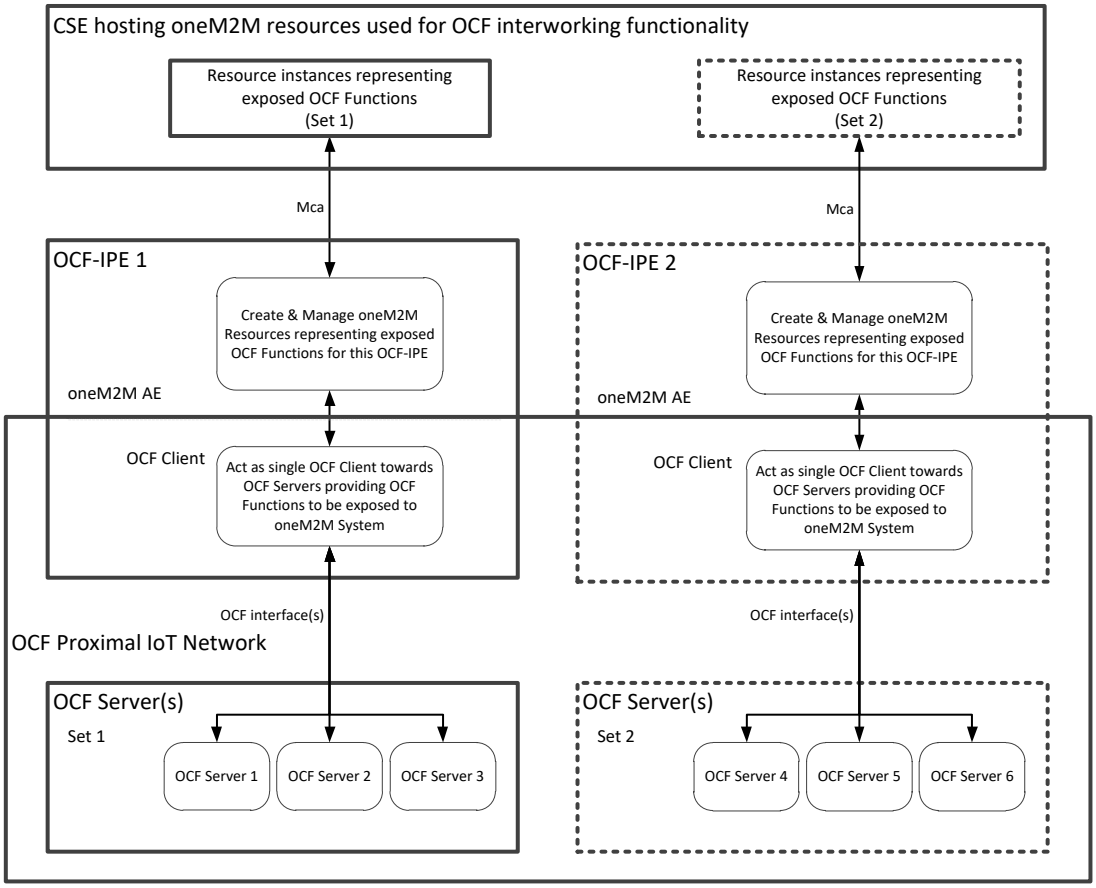
oneM2M TS-0023 [6].

OCF Device-Specification-V1.3.0 [8].

非 oneM2M システムとのインターワーキングについては、TS-0001 の付則 F に記載の IPE(Interworking Proxy Application Entities）と呼ばれる Application Entities を使用する。

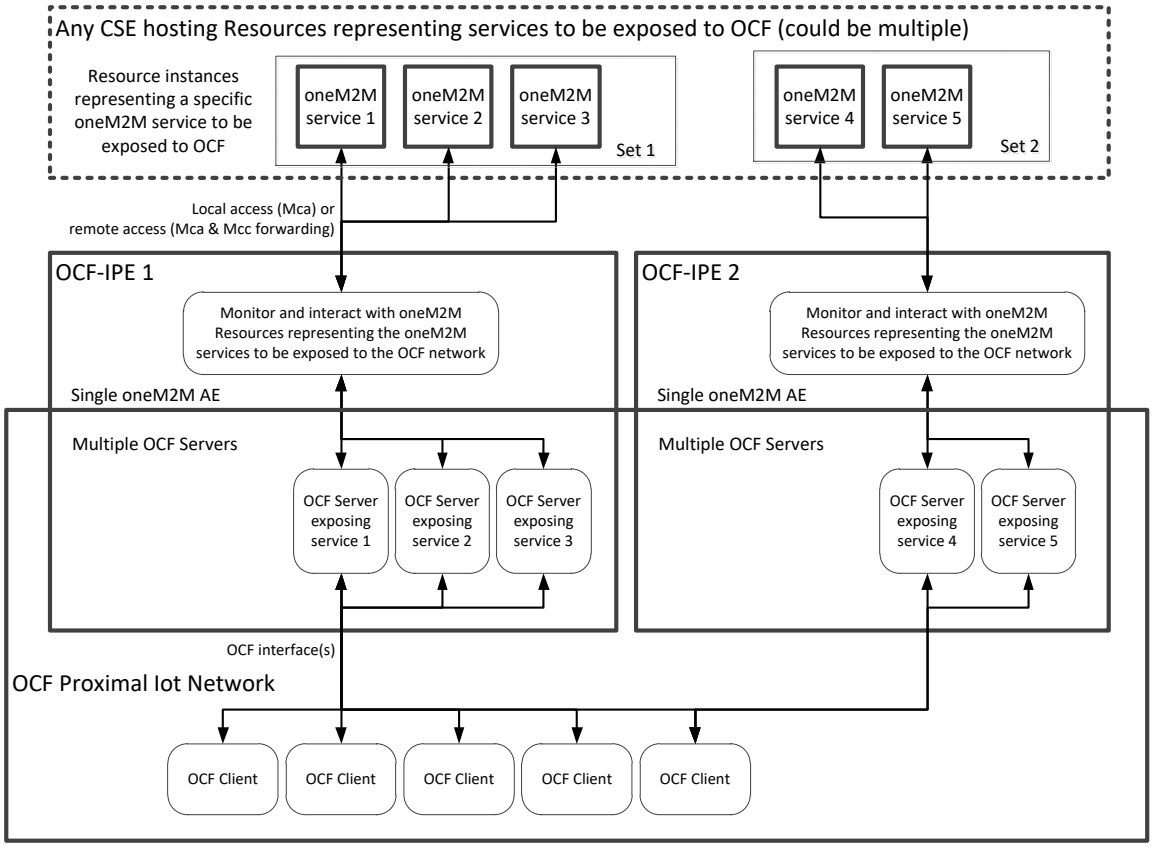
OCF とのインターワークには、OCF-IPE として次図の通り使用する。

OCF から oneM2M へのインターワーク・アーキテクチャを下図に示す。




: Summary of Interworking Architecture for Exposure OCF → oneM2M

oneM2M から OCF へのインターワーク・アーキテクチャを下図に示す。




: Summary of Interworking Architecture for Exposure oneM2M → OCF

### 2.5.7　TS-M2M-0026v3.13.2 - 3GPP とのインタワーク（TS-0026）

本文書はoneM2M サービス層と3GPP下位ネットワーク間とのインタワーキングを規定する文書である。

#### 2.5.7.1　3GPP インタワーキングの oneM2M アーキテクチャ

本文書では、3GPPインタワーキングとセルラーIoT機能をサポートするための基本アーキテクチャを紹介している。またoneM2Mシステムが、3GPPリリース10～15で追加されたIoT関連機能・サービスを、どのように活用するか記述している。規定している機能・サービスは、IN-CSEやUEをホストするAND-AE, MN-CSE, ASN-CSEによって利用されると想定。3GPPトラスト・ドメインは以下3つのインタフェースを提供する。

- SGiインタフェースを介したSCS/ASとのIPベースのデータプレーン通信
- TSPインタフェースを介したMTCインタワーキング機能
- Restful APIベースのT8インタフェースを介したサービス・ケイパビリティ開示機能（SCEF）

T8インタフェースは、SCEF～IN-CSE間でインタラクションするためのリソース・手順を定義しているAPIセットである。本APIのアーキテクチャレベル、プロトコルレベルの規定は、3GPP TS23.682、3GPP TS29.122で夫々定義している。本文書では、T8 APIを介して、IN-CSEがSCEFとインタワークをする方法を定義している。またIN-CSEで、個々のリクエスト・レスポンスの設定・送信・受信するための方法を定義している。

またIN-CSEによる、T8 HTTPプロトコル・バインディング、JSONメッセージ・エンコーディングを使用したT8リクエスト・レスポンズの生成・処理方法を定義している。

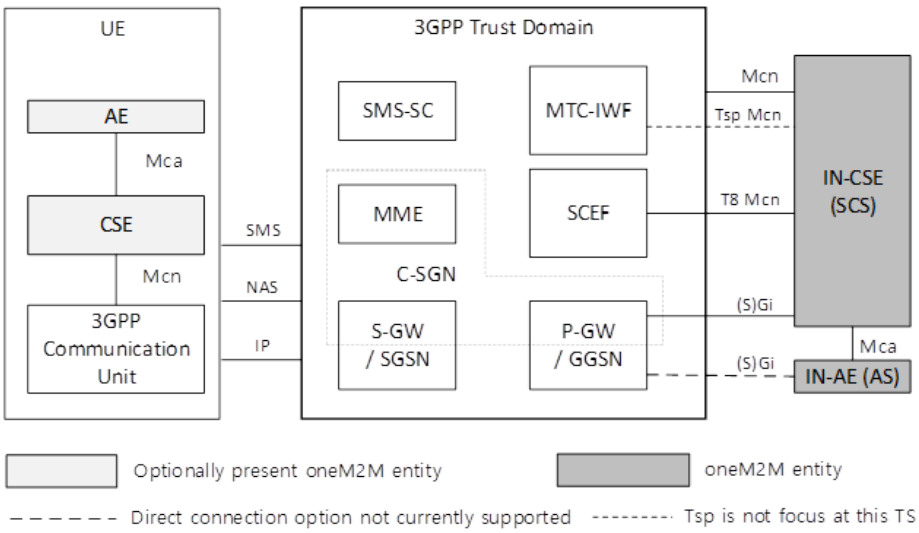



図2.5.7.1-1　3GPPインタワーキング・アーキテクチャ

### 2.5.7.2　コネクティビティ確立

IN-CSEでの下位ネットワークのベアラ確立・探索完了後、ADN-AE, ASN/MN-CSEとIN-CSEは、通信を開始する。そしてデータは、3GPP Gi/SGiインタフェースを介して、下位ネットワークのIPレイヤ上でoneM2Mエンティティ間を通過する。図2.5.7.2-1は、ADN-AE, ASN/MN-CSEとIN-CSE間のコネクティビティを記述している。

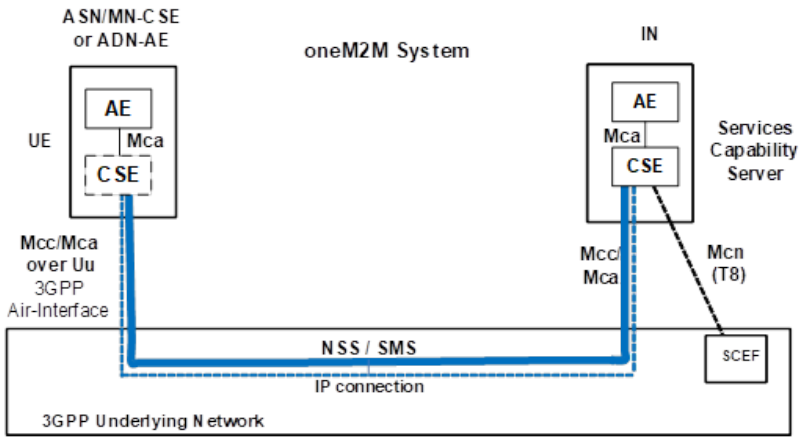



図2.5.7.2-1　ADN-AE, ASN/MN-CSEとIN-CSE間のコネクティビティ

### 2.5.7.3　3GPP インタワーキングの API

本文書では、以下8つの3GPP APIとのインタワークを規定している。

#### 2.5.7.3.1　non-IP data delivery(NIDD)

NIDDは、3GPP Release 15で標準化されたIPを使用しないC-Planeを用いたデータ伝送技術で、センサーデータ等、小容量のデータを、セキュアに効率よく伝送することができる。oneM2M TS-0026では、①NIDDデータ送受信前の設定手順、②IN-CSEからのNIDDデータ送信手順、③UEデバイスからのNIDDデータ送信手順を規定している。

#### 2.5.7.3.2 モニタリング・イベント

デバイスのステータスをIN-CSEへ通知するために使用する。oneM2M　Release 3では、3GPPで規定している8つのイベント・タイプの内、以下7つをサポートしており、本文書では、下記イベント・タイプとのインタワーキングの手順を記載している。

- UE Availability after DDN Failure：DDN 障害から復帰した時のデバイスの Availability 通知
- UE Communication Failure：デバイスとの通信失敗時の通知
- UE Loss of Connectivity：デバイスがスリープ・モード等により通信できない期間の通知
- Detecting Change of IMSI-IMEI(SV) Association：デバイスの IMSI(国際移動体加入者識別番号)/IMEI(国際移動体装置識別番号)変更時の通知
- Roaming Status：デバイスのローミング先が変更となった場合の通知
- UE Reachability Monitoring：デバイスが、PSM や eDRX 等の省電力機能を使用する場合、デバイスの Reachability を通知するために使用する。

#### 2.5.7.3.3 デバイス・トリガリング

デバイスのコネクション確立、デバイス登録、デバイスのIPアドレス更新等で使用する。本文書では、IN-AE/CSEからのデバイス・トリガリングの手順を規定している。

#### 2.5.7.3.4 トラフィック・パターン通知

デバイスの通信パターンを3GPPネットワークへ通知することにより、トラフィック最適化を行う。本文書では、IN-CSEで、oneM2Mのトラフィック・パターンのアトリビュートを3GPPのAPIのアトリビュートに変換し、3GPP SCEFへ通知をする手順（Create/Udpdate/Delete）を記載している。

#### 2.5.7.3.5 MBMS (Multimedia Broadcast Multicast Service)

クラウドから特定エリア内のデバイス群へ、マルチキャストでデータ配信をする場合に使用する。本文書では、<group>リソースを用いたMBMSグループの生成、グループメッセージ配信の手順を規定している。

#### 2.5.7.3.6 ネットワーク・ステータス・レポート

3GPP無線基地局の輻輳レベルを通知するために使用する。本文書では、ネットワーク・ステータス・レポートのSubscription、無線基地局輻輳時のNotifiationの手順を規定している。

#### 2.5.7.3.7 バックグラウンド・データ配信

トラフィックの輻輳状態に応じてデータを効率よく配信するために用いられる。IN-CSEでは、配信時間、デバイス数、デバイスが配信するデータ量、配信するエリア等の設定情報をSCEFへ送信する。SCEFでは、3GPP内部エンティティから取得した利用可能なポリシー情報リストをIN-CSEへ返信する。IN-CSEでは、SCEFから入手したポリシー情報リストからポリシーを選択（選択方法は実装依存）し、SCEFへ送信する

#### 2.5.7.3.8 ネットワーク・パラメータ設定

デバイスが、PSMやeDRX等の省電力機能を使用する場合、IN-CSEで、デバイスのスリープ時間、アクティブ時間等のパラメータを設定する。これにより、3GPPネットワークのトラフィックの状況に応じて設定をカスタマイズして、ネットワーク・リソース利用の最適化を図ることができる。

### 2.5.8 TR-M2M-0035-v3.0.0 – OSGi とのインターワーク

OSGi フレームワークに準拠するデバイス、あるいはゲートウェイと oneM2M システムとの間のインターワーキングに関する原則とガイドラインの規程である。oneM2M リソースへの要求を行うことで、アプリケーションは OSGi デバイス、あるいはゲートウェイが提供するサービスへのアクセスが可能になる。

OSGiインターワーキングとはOSGiベースのデバイス、あるいはゲートウェイが提供するサービスとoneM2Mエンティティ（AE/CSE）との間のインターワークのことである。OSGiサービスはOSGi が定義するDAL (Device Abstraction Layer)サービス、SDT (Smart Device Template)サービス、DMT (device management tree)管理者サービス等を含む。

oneM2M-OSGi IPEバンドルがインターワーキングを担い、OSGiベースのデバイス、あるいはゲートウェイがCSEバンドルを提供する場合には、IPEは内部でCSEバンドルとやり取りする。OSGiベースのデバイス、あるいはゲートウェイは、Mca/Mcc参照ポイントを通じて他のoneM2Mエンティティとやり取りする。OSGiベースのデバイス、あるいはゲートウェイがCSEバンドルを提供しない場合には、IPEはネットワークインタフェースを通じてCSEとやり取りする。

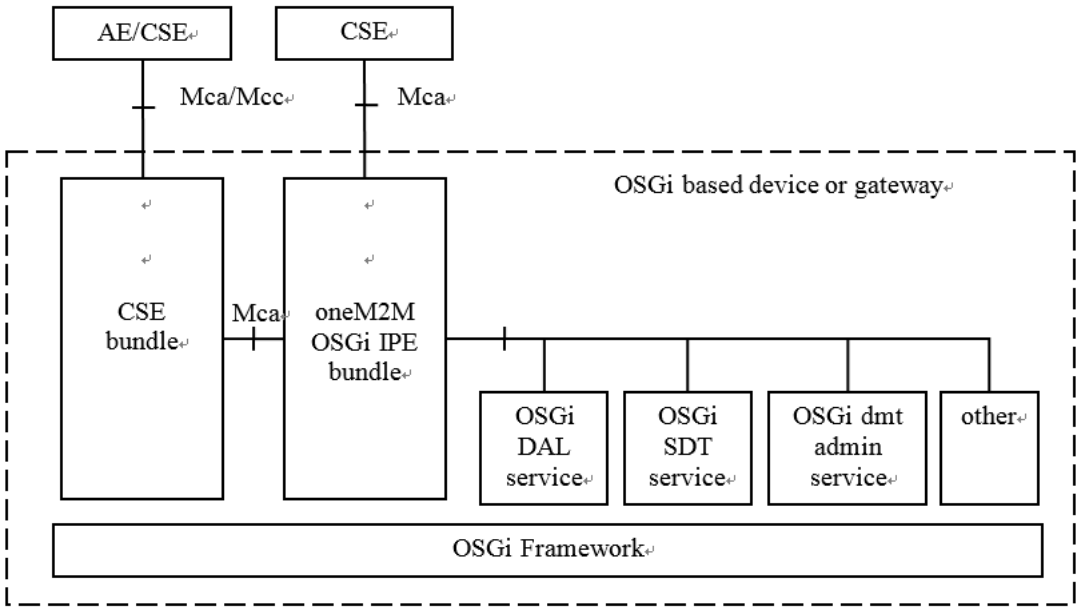



図 2.5.8-1　OSGi Interworking Architecture

OSGi DALとのマッピング：

OSGi DALにより定義されるデバイスサービスとoneM2M NoDNへのマッピング（<flexContainer>リソースと<node>リソースで表される）/ デバイスサービスの手順

OSGiファンクションサービスとTS-0023で規定されたmoduleClassに対応する<flexContainer>リソースへのマップ / ファンクションサービスの手順

## 2.6　セキュリティ

### 2.6.1　TS-M2M-0003 セキュリティ技術の適用

本文書は、IoT/M2Mシステムに適用可能なセキュリティソリューションについて規定している。
リリース3で追加された主な機能について、以下に記載する。

#### 2.6.1.1 Distributed Authorization

Distributed Authorizationは、認可の構成要素であるPEP（Policy Enforcement Point）、PDP（Policy Decision Point）、PRP（Policy Retrieval Point）およびPIP（Policy Information Point）が異なるCSEに存在する場合に、

これらの構成要素を相互接続するためのフレームワークである。本フレームワークにより、リソースが保管されているCSE（Hosting CSE）とは異なるCSEにあるアクセス制御ポリシーを用いて、リソースに対するアクセス制御を行うことが可能となる。また、本フレームワークを実現するために、3つのリソース（<authorizationDecision>, <authorizationPolicy>, <authorizationInformation>）が新規に定義されている。

#### 2.6.1.1.1 アクセス制御判定結果の取得

Hosting CSEとは異なるCSEにあるPDPにアクセスし、アクセス制御結果を受け取ることができる（Figure 1）。Mode aは、PDPへのアクセス制御結果のリクエストとそのレスポンスを示しており、UPDATEの操作により行われる。Mode bは、PDPがPRPやPIPにアクセス制御判定結果の生成に必要な情報を取得し、アクセス制御結果を生成することを示している。

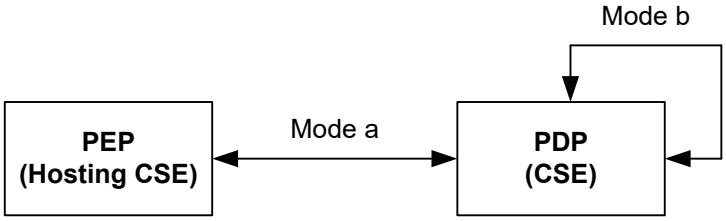



Figure 2　PDP へのアクセス

#### 2.6.1.1.2 アクセス制御ポリシーの取得

PDPは異なるCSEにあるPRPにアクセスし、アクセス制御ポリシーを受け取ることができる（Figure 2）。Mode cは、PRPへのアクセス制御ポリシーのリクエストとそのレスポンスを示しており、UPDATEの操作により行われる。Mode dは、異なるCSEにある他のPRPへのアクセス制御ポリシーのリクエストとそのレスポンスを示している。

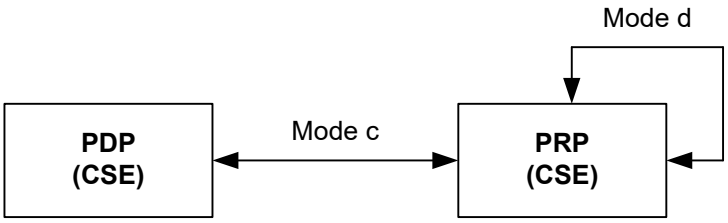



Figure 3　PRP へのアクセス

#### 2.6.1.1.3 アクセス制御情報の取得

PDPは異なるCSEにあるPIPにアクセスし、アクセス制御情報を受け取ることができる（Figure 3）。Mode eは、PIPへのアクセス制御情報のリクエストとそのレスポンスを示しており、UPDATEの操作により行われる。Mode fは、異なるCSEにある他のPIPへのアクセス制御情報のリクエストとレスポンスを示している。

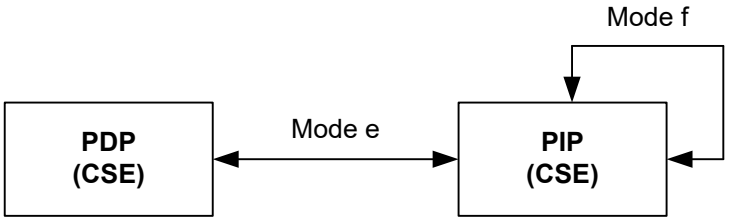



Figure 4　PIP へのアクセス

#### 2.6.2　Secure Environment Abstraction　セキュア領域の抽象化　（TS-0016）

本仕様書は、Release 3にて新規に発行された仕様書である。セキュリティ技術の適用　(TS-0003)で定義されている様々なセキュア領域の実装に対して、抽象化されたインターフェースや構造が定義されている。（セキュア領域：機密データの保管や、暗号化や復号などのセキュリティ機能を安全に実施するための高度なセキュリティを確保した領域）

##### 2.6.2.1 セキュア領域の抽象的アーキテクチャ

フィールドデバイスにおけるセキュア領域とCSEやAEとの関係をFigure 1に示す。セキュア領域は、CSEやAEと独立して定義されており、セキュア領域とCSEの参照ポイントは、Mcsとして定義されている。また、CSEやAEでセキュア領域の特性を利用したセンシティブな処理やセンシティブなデータの保管などを利用するために、CSEやAEの一部をセキュア領域内に配置することができる。

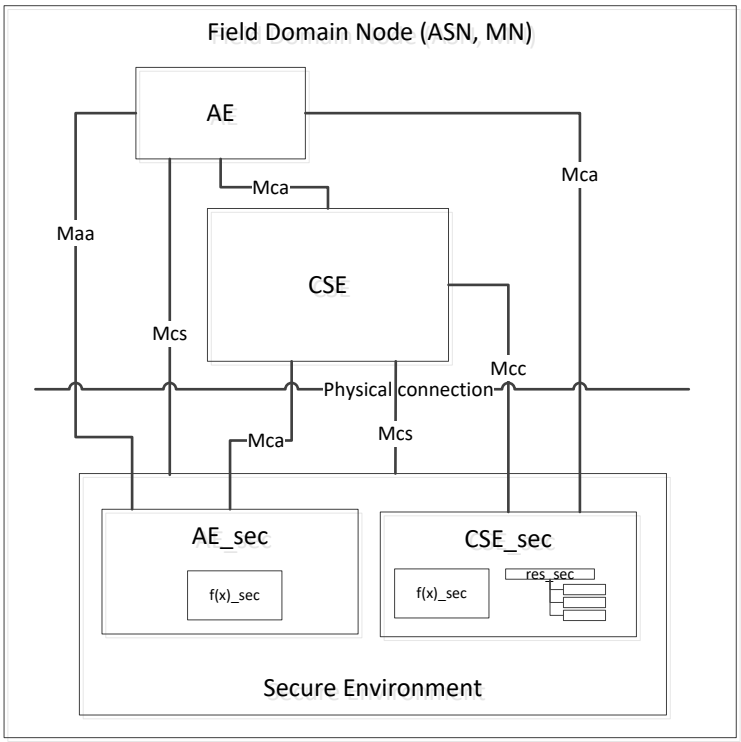



Figure 5　フィールドデバイスにおけるセキュア領域アーキテクチャ

#### 2.6.2.2 セキュア領域

セキュア領域は特徴によって、3 つのセキュリティレベルで定義されている。

- レベル 3
  耐タンパー性があり、リモートによる攻撃にも耐性があるハードウェアレベルで独立しているセキュリティ領域（例：GlobalPlatform eSE）
- レベル 2
  リモートによる攻撃に耐性はあるが、物理的な攻撃に対する保護までは対象に入っていないハードウェア内に統合されているセキュア領域（例：GlobalPlatform TEE）
- レベル 1
  セキュリティの高いソフトウェア設計などのソフトウェアベースのセキュリティ領域（例：White Box Cryptography）

#### 2.6.2.3 論理的抽象化—Mcs 参照ポイント

セキュア領域にアクセスするためには、Mcs 参照ポイントを通じてリクエストを送信する。本章では、Mcs 参照ポイントを使用するために必要な以下の項目について定義を行なっている。

- M2M-SE-ID（セキュア領域の識別子）
- ネームスペースとデータタイプ
- Mcs 独自のリソースタイプ（TS-0001 に定義されていないリソース）
  - algorithmSpecificParameter
  - cipher
  - connectionInstance
  - hash
  - identity
  - Rand
  - secureConnection
  - sensitiveDataObject
  - SEReboot
  - SE
  - signature

#### 2.6.2.4 物理インターフェース

セキュア領域への物理的なインターフェースは、oneM2M で定義しない。GlobalPlatform などで定義された仕様を用いる。

#### 2.6.2.5 Mcs 参照ポイントにおけるリソースタイプの定義

Mcs 独自のリソースやアトリビュートの列挙型の定義が記載されている。

#### 2.6.2.6 Mcs 参照ポイントにおける省略名

Mcs 独自のリソースやアトリビュートの省略名の定義が記載されている。

## 2.7 試験と相互接続性

### 2.7.1 Feature Catalogue (TS-0031)

本文書は，oneM2M仕様で規定されている技術的な特徴をFeatureとしてIDを振り定義している。また，類似するFeatureをFeature Setとしてまとめ， Functionが備えるべきFeature Setを示している．Functionが最も大きい単位で，次いでFeature Setがあり，最小単位はFeatureである．Featureはサポートされるone M2Mエンティティごとに3種類に分けられていて，CSEとAEがともにサポートしているFeatureであるGE，CSEがサポートしているFeature群であるCE，AEがサポートしているFeature群であるAEが規定されている．これら3種類の分類項目はEntityと呼ばれている．

最小単位のFeatureは，{Entityの略語}/{Functionの略語}/{Feature Setのシリアルナンバー}/{Feature のシリアルナンバー}によって決まるIDで表される（例：GE/GEN/00002/00003）．

Featureよりも一段階大きい単位であるFeature Setは2～10個ほどのFeatureで構成されており，「AEの登録」などoneM2M特有の機能を表している．

最大単位のFunctionは1~5個ほどのFeature Setで構成されており，「検索」など汎用的なM2Mサービスの機能を表している．

## 2.8 アプリケーション開発ガイド

### 2.8.1 TS-M2M-0022v3.0.1 – フィールド装置設定

装置内のAEやCSEがレジストラやホスティングCSEとの間でM2Mサービスレイヤオペレーションを確立するためには、フィールド領域(例：ADN、ASN/MN)の装置を前もって設定し、維持管理するアーキテクチャ、リソース、手順が必要である。リソースと手順は、AEあるいはCSEがM2Mサービスレイヤオペレーションを開始するのに必要なレジストラCSEやホスティングCSEに関する情報を含んでいる。

装置がM2Mサービスレイヤオペレーションを確立するために、フィールド領域のASN/MNやADNノードを設定する際、基本的にはTS-0001、TS-0003に従う。

フィールド領域にあるリモートAEやCSEがM2Mサービスレイヤオペレーションを確立するのに必要な情報の伝達にはTS-0001を用いる。Configuration AEについても加わっている。

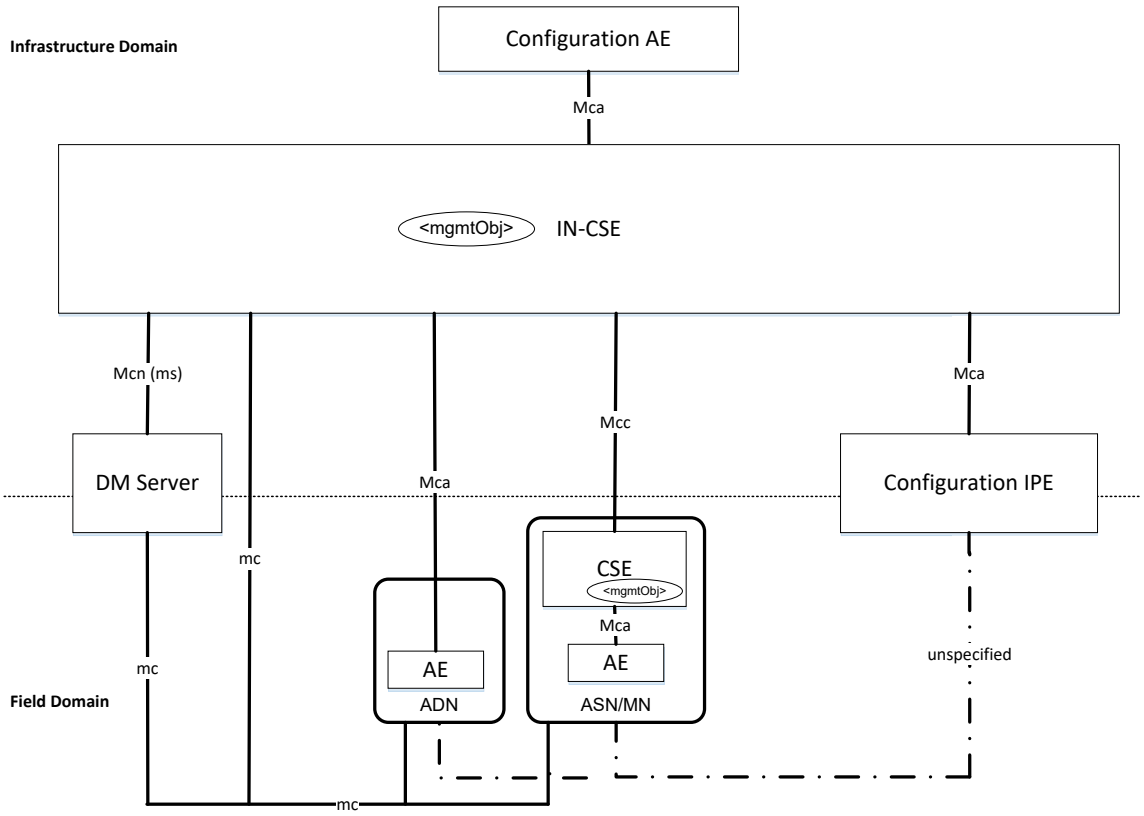



図2.8.1-1　ASN/MNおよびADNノードの設定に関するアーキテクチャ

リソースについては、M2Mサービスレイヤオペレーションを確立するために、フィールド領域のADNやASN/MNノード上のAEやCSE設定に<mgmtObj>リソースを用いる。

またホスティングCSE内<mgmtObj>リソースのライフサイクル(フィールド装置設定手順)は、Configuration AEからの提供、あるいはホスティングCSEの探索で始まる。

## 3　おわりに（次期リリースへの展望）

次期リリース（リリース４）の策定作業は、2018年から開始され、Stage１（要求条件）に関しては、2019年5月にフリーズとなる予定で進められている。Stage2/3のフリーズは2019年から2020年にかけて実施され、そのリリース４のRatification（リリースの承認）は、2020年末までに行われる見込みである。

リリース４では、他技術とのインターワーク技術の策定として、3GPP Rel.15、W3C WoT（Web of Things）、Global Platform、DDS、Modbus等とのインターワークが追加され、oneM2M仕様をベースとしたCross Sectorでの連携や他の技術とのインターワークのための技術基盤が益々充実することが期待される。また、oneM2MにおけるTrust Managementや分散型認証の検討が行われ、セキュリティ関連の技術仕様が機能強化されることが想定される。さらに、ヘテロジニアスIDサービスのoneM2Mへの適用の検討や「oneM2M Service Subscribers and Users」として、oneM2M技術におけるユーザの概念の導入検討が推進することが望まれる。加えて、「Lightweight oneM2M Services」として、oneM2M仕様の複雑性を低減し、より軽量な機能提供が推進することが期待される。そのほかに、3GPPインタワーク技術のAPI拡張（3GPP V2X、Session QoS等）やEdge/Fog Computing技術のoneM2Mへの導入等の検討、クルマ分野/製造業分野/Smart City分野へのoneM2M技術の適用に関する更なる検討、「Disaster Alert Service Enabler (DASE)」としての災害警報サービス分野への導入、oneM2M APIの開発者向けガイドの作成等の作業が進められ、益々oneM2Mの適用分野の拡張や機能の強化が図られる予定である。