TTC技術レポート
Technical Report

TR-M2M-R2

oneM2Mリリース2の構成と解説

Structure and Interpretation of
oneM2M release 2

第1.0.1版

2017年6月20日制定

一般社団法人
情報通信技術委員会
THE TELECOMMUNICATION TECHNOLOGY COMMITEE

Telecommunication Technology Committee

目　次

＜参考＞

１．　国際勧告等との関連

本技術レポートはoneM2Mで承認されたoneM2M Administrative Document ADM-0011-V-2.0.0 Release 2 Control Document -に準拠している。

２．　改版の履歴

版数	制定日	改版内容
第1.0.0版	2016年11月30日	制定
第1.0.1版	2017年6月20日	誤記修正

３．参照文章

主に、本文内に記載されたドキュメントを参照した。

４．技術レポート作成部門

oneM2M専門委員会 [oneM2M Working Group]

[1] oneM2M はARIB/TTCの登録商標である。

はじめに

本レポートはoneM2Mリリース2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2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。

第1章　oneM2M リリース2の構成

1.1　oneM2M リリース 2 の構成と TTC 仕様書との対応

oneM2M リリース2は、17件の技術仕様書（TS : Technical Specification）および9件の技術報告書（Technical Report）から構成されている。 oneM2M Administrative Document ADM-0011 V2.0.0 - oneM2M Release2 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2の構成と対応するTTC仕様（１）技術仕様書（Technical Specification）

oneM2M 仕様番号	TTC 技術仕様書タイトル	TTC 文書番号･版数
TS-0001[1]	Functional Architecture （機能アーキテクチャ）	TS-M2M-0001v2.10.0
TS-0002[2]	Requirements （要求条件）	TS-M2M-0002v2.7.1
TS-0003[3]	Security Solutions （セキュリティ技術の適用）	TS-M2M-0003v2.4.1
TS-0004[4]	Service Layer Core Protocol （サービス層 API 仕様（共通部））	TS-M2M-0004v2.7.1
TS-0005[5]	Management Enablement (OMA) （OMA 仕様によるデバイス管理）	TS-M2M-0005v2.0.0
TS-0006[6]	Management enablement (BBF) （BBF 仕様によるデバイス管理）	TS-M2M-0006v2.0.1
TS-0007[7]	Service Components （サービスコンポーネント）	TS-M2M-0007v2.0.0
TS-0009[8]	HTTP Protocol Binding （サービス層 API 仕様（HTTP 用））	TS-M2M-0009v.2.6.1
TS-0010[9]	MQTT protocol binding （サービス層 API 仕様（MQTT 用））	TS-M2M-0010v2.4.1
TS-0011[10]	Common Terminology （共通用語）	TS-M2M-0011v2.4.1
TS-0012[11]	Base Ontology （ベースオントロジー）	TS-M2M-0012v2.0.0
TS-0014[12]	LWM2M Interworking （LWM2M とのインターワーク）	TS-M2M-0014v2.0.0
TS-0015[13]	Testing Framework （試験フレームワーク）	TS-M2M-0015v2.0.0
TS-0020[14]	WebSocket Protocol Binding （サービス層 API 仕様（WebSocket 用））	TS-M2M-0020v2.0.0

TS-0021[15]	oneM2M and AllJoyn Interworking （AllJoyn とのインターワーク）	TS-M2M-0021v2.0.0
TS-0023[16]	Home Appliances Information Model and Mapping （家電機器の共通デバイス管理モデル）	TS-M2M-0023v2.0.0
TS-0024[17]	oneM2M and OIC Interworking （OIC とのインターワーク）	TS-M2M-0024v2.0.0

[1] TS 0001 - Functional Architecture, v2.10.0

[2] TS 0002 - Requirements, v2.7.1

[3] TS 0003 - Security Solutions, v2.4.1

[4] TS 0004 - Service Layer Core Protocol, v2.7.1

[5] TS 0005 - Management enablement (OMA), v2.0.0

[6] TS 0006 - Management enablement (BBF), v2.0.1

[7] TS 0007 – Service Component, v2.0.0

[8] TS 0009 - HTTP Protocol Binding, v.2.6.1

[9] TS 0010 - MQTT Protocol Binding, v2.4.1

[10] TS 0011 - Common Terminology, v2.4.1

[11] TS 0012 - Base Ontology, v2.0.0

[12] TS 0014 - LWM2M Interworking, v2.0.0

[13] TS 0015 - Testing Framework, v2.0.0

[14] TS 0020 - WebSocket Protocol Binding, v2.0.0

[15] TS 0021 - oneM2M and AllJoyn Interworking, v2.0.0

[16] TS 0023 - Home Appliances Information Model and Mapping, v2.0.0

[17] TS 0024 - oneM2M and OIC Interworking, v2.0.0

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

oneM2M TR番号	TTC技術レポートタイトル	TTC文書番号・版数
TR-0001[18]	Use Cases Collection （ユースケース集）	TR-M2M-0001v2.4.1
TR-0007[19]	Study on Abstraction and Semantics Enablement （抽象化とセマンティクスの適用性検討）	TR-M2M-0002v2.11.1
TR-0008[20]	Security （セキュリティの検討）	TR-M2M-0008v2.0.0
TR-0012[21]	End-to-End-Security and Group Authentication （エンド・エンド セキュリティとグループ認証）	TR-M2M-0012v.2.0.0
TR-0016[22]	Authorization Architecture and Access Control Policy （認可アーキテクチャとアクセス制御ポリシー）	TR-M2M-0016v2.0.0
TR-0017[23]	Home Domain Abstract Information Model （住宅分野に適用する抽象デバイス管理モデル）	TR-M2M-0017v.2.0.0
TR-0018[24]	Industrial Domain Enablement （産業分野への適用）	TR-M2M-0018v2.0.0
TR-0022[25]	Continuation and Integration of HGI Smart Home activities （HGIにおけるスマートホーム分野の成果の持続と統合）	TR-M2M-0022v2.0.0
TR-0024[26]	3GPP_Rel13_IWK （3GPPリリース13とのインターワーク）	TR-M2M-0024v2.0.0

[18]　TR 0001 - Use Cases Collection, v2.4.1

[19]　TR 0007 - Study on Abstraction and Semantics Enablement, v2.11.1

[20]　TR 0008 - Security, v2.0.0

[21]　TR 0012 - End-to-End-Security and Group Authentication, v2.0.0

[22]　TR 0016 - Authorization Architecture and Access Control Policy, v2.0.0

[23]　TR 0017 - Home Domain Abstract Information Model, v2.0.0

[24]　TR 0018 - Industrial Domain Enablement, v2.0.0

[25]　TR 0022 - Continuation and Integration of HGI Smart Home activities, v2.0.0

[26]　TR 0024 - 3GPP_Rel13_IWK, v2.0.0

1.2　リリース２の主なフィーチャー

oneM2M リリース 1 は 10 件の技術仕様書(TS)で構成されていたが、リリース 2 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、9 件の技術報告書（Technical Report）も合わせて発行されることになった。

リリース 2 の主なフィーチャーとしては、図 1-1 に示す通り、oneM2M と異なる M2M/IoT 技術とのインターワーキング・フレームワーク、セマンティック・インターオペラビリティ・サポート、セキュリティの強化、プロトコルバインディングの強化（WebSocket の追加）、試験フレームワーク、及びをホームドメインや産業ドメインへのサービス展開の検討の６つの特徴から構成されている。

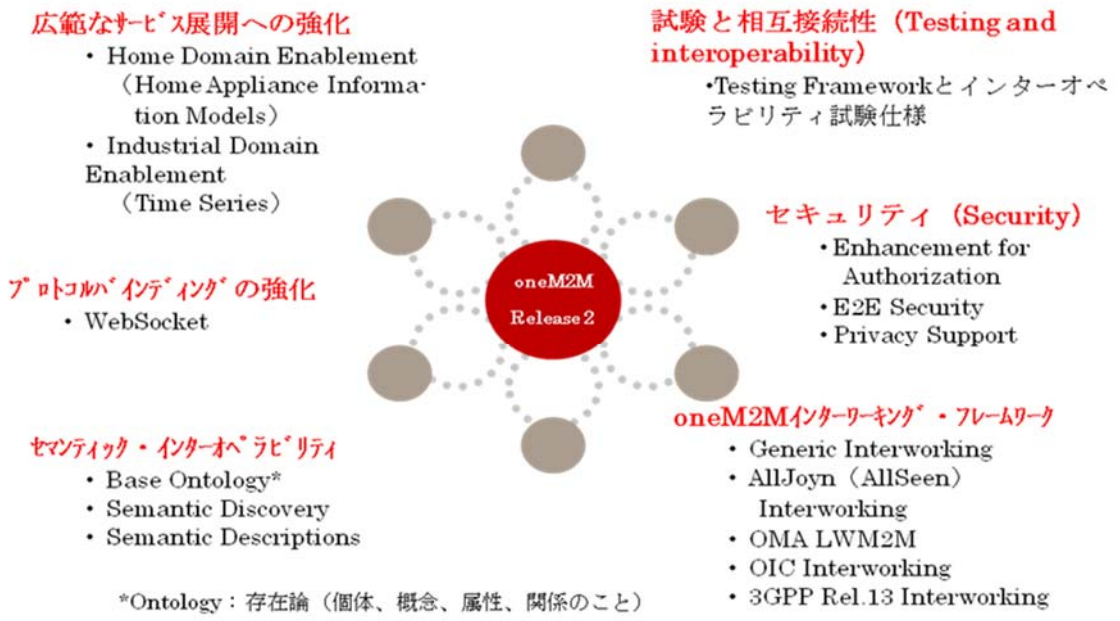


図 1-1　リリース 2 の主なフィーチャー

第2章　oneM2M リリース2の解説

2.1 要求条件とアーキテクチャ

2.1.1　TR-M2M-0001v2.4.1 – 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-0002v2.7.1 – 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。

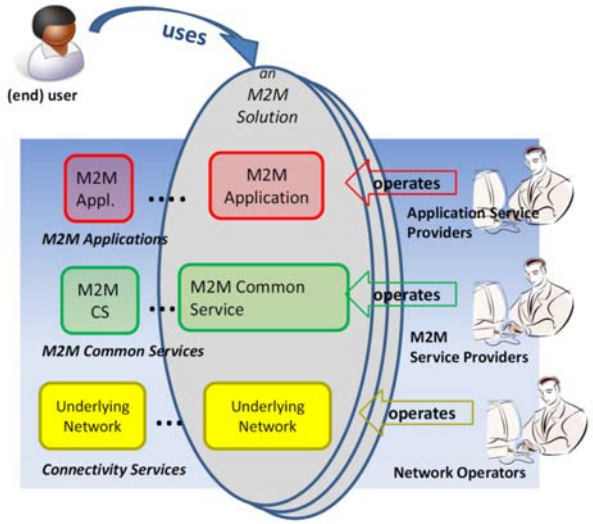


図2-1　M2Mエコシステムでの機能的役割

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（98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（63件）
- 課金要求条件（6件）

- 運用要求条件（10件）
- 通信要求処理条件（15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-0001v2.10.0 - 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 2 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 Dynamic Authorization

Dynamic Authorizationは、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フレームワークである。tokenは、アクセス権、有効期限等の認可情報を伝送するために使用されるリソースで、リリース2で新規追加されている。

本文書では、Dynamic Authorizationパラメータのリソースタイプ<dynamicAuthorizationConsultation>、伝送方法、アーキテクチャを規定しており、Dynamic Authorizationパラメータと関連する処理については、TS-0003 Security Solution、ユースケース、要求条件は、TR-0019 Dynamic Authorizationに記載されている。

2.1.3.2 ESPrim （End-to-End Security of Primitives）

ESPrimは、Originator～Receiver間で相互認証、高い機密性、完全なプロテクション等を提供するため、セキュアなoneM2Mプリミティブに必要なフレームワークを提供する。本文書では、ESPrimオブジェクトの伝送方法を規定している。ESPrimのクレデンシャル管理、データ・プロテクションについては、TS-0003 Security Solutionで規定している。

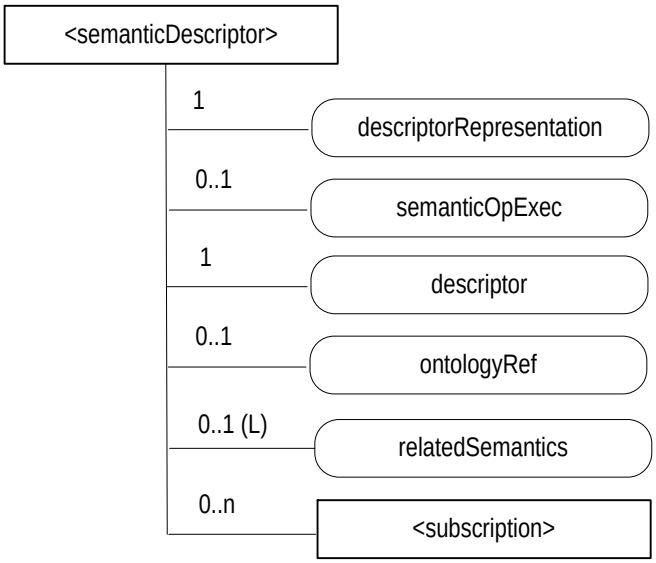
2.1.3.3 ESCertKE (End-to-End Certificate-based Key Establishment)

ESCertKEは、TS-0003で規定しているE2EKeyと呼ばれるシークレットなシメトリック鍵生成で必要となる認証処理のためのエンドエンド間のフレームワークを提供する。

本文書では、ESCertKEメッセージの伝送について規定している。

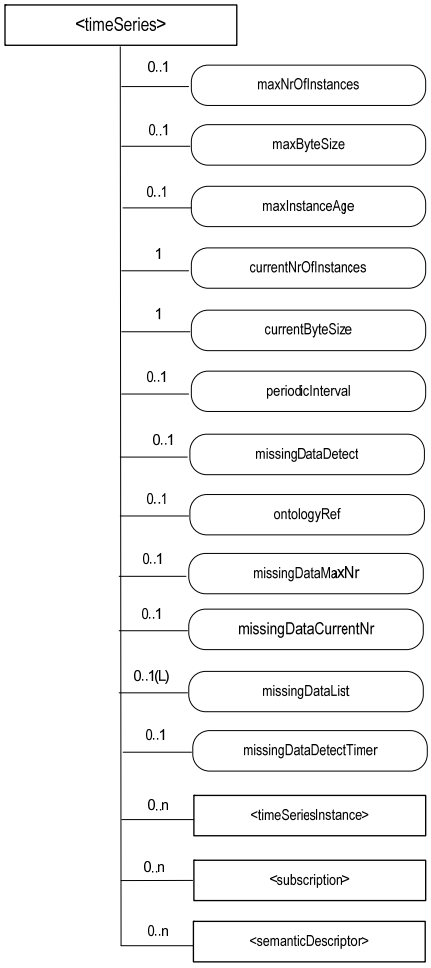
2.1.3.4 semanticDescriptor

リリース 2 では、<semanticDescriptor>リソースを新たに定義している。これにより、リソース内部に、セマンティクス情報を記述することが可能となっている。セマンティック情報は、oneM2M システムのセマンティック機能で使用され、アプリケーションや CSE で利用できる。



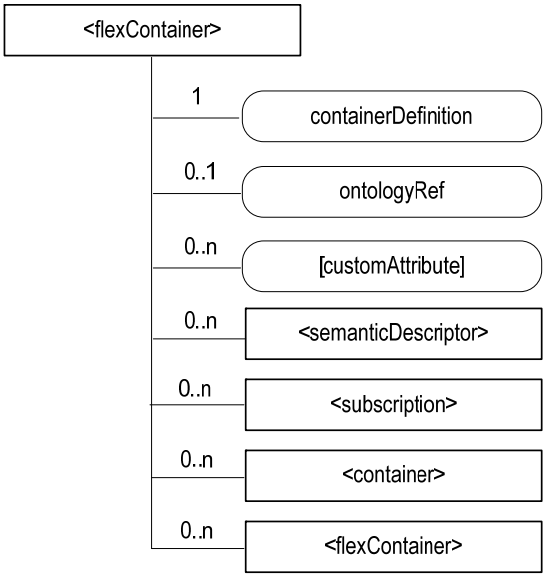
2.1.3.5 timeSeries

timeSeriesは、データ欠損を検出する機能を搭載したリソースで、監視周期間隔、データ生成時刻、データのシーケンス番号を付与することが可能である。定期的に収集される測定データのロギング等、運用監視での利用が想定される。



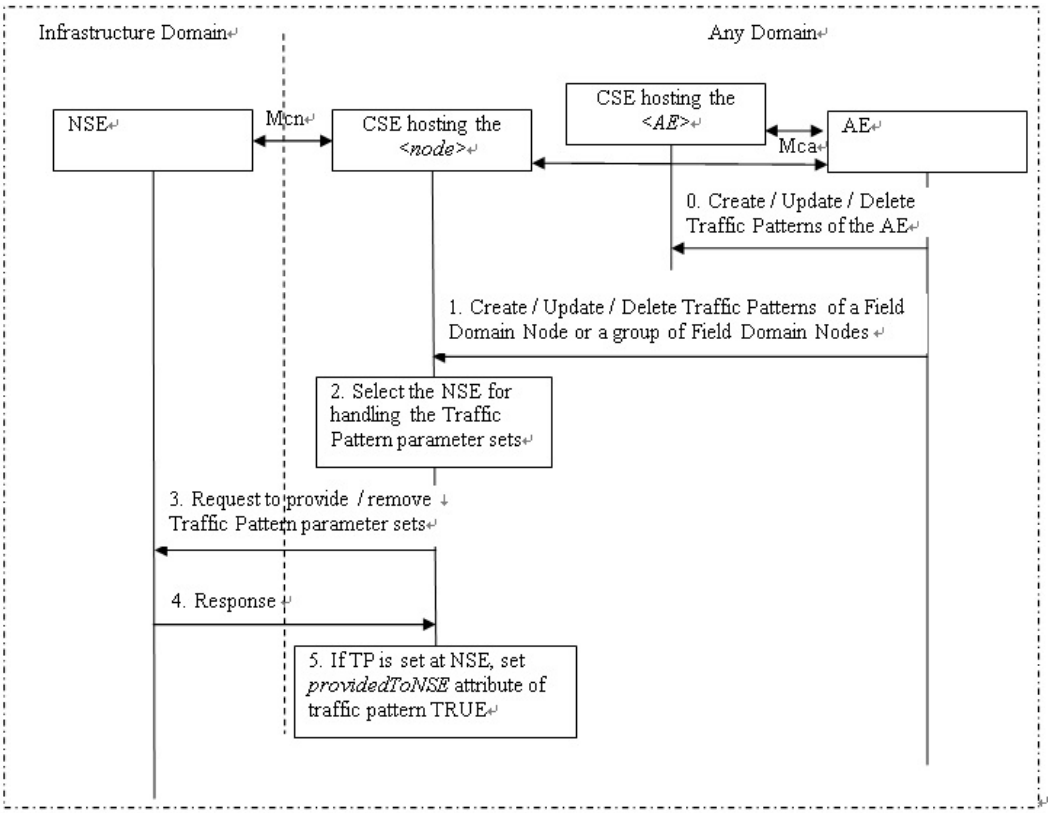
2.1.3.6 flexContainer

flexContainer は、データコンテナの柔軟な specialization を定義することが可能なリソースである。各 specialization 毎の定義（名前、データタイプ）と、本定義を参照する URI を記述することで、フィールド単位で値を格納できる汎用データストレージとして使用することができる。



2.1.3.7 trafficPattern

trafficPattern は、M2M デバイスのトラフィックパターンを、インフラドメインへ通知をすることで、ネットワークのトラフィック量削減を行う機能である。trafficPattern のリソースは、通信が、定周期（5 分間隔等）であるか、オンデマンドか、日時単位（毎週月曜日 13:00-20:00）等を定義している。

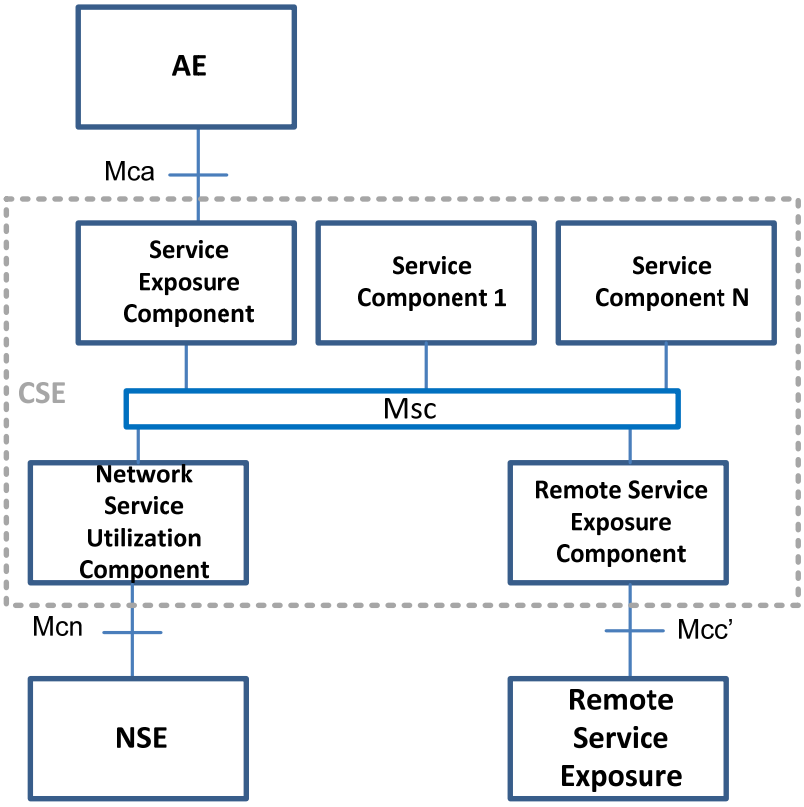


2.1.4　TS-M2M-0007v2.0.0 – サービスコンポーネント

本文書は、M2Mサービスプラットフォームにより提供されるM2Mサービスを規定し、次に、oneM2Mサービスプラットフォームの M2Mサービス機能アーキテクチャの統合や連携について規定し、最後に複雑なビジネスのサービスの範囲内でM2Mサービスをどのように利用するかについて図示して説明する。（注：一般的に、このようなアーキテクチャは、SoA（Service Oriented Architecture）と呼び、TS-0001で規定されるRoA（Resource Oriented Architecture）と区別される。）

2.1.4.1 M2Mサービスアーキテクチャ

本章ではM2M サービスプラットフォーム内で用いられるM2Mサービスのアーキテクチャについて記述する。ここで、M2Mサービスサーキテクチャとは、M2Mアプリケーションやサービスプロバイダに対して提供されるM2Mサービスを規定することにより、M2M機能アーキテクチャを強化する役割を担う。oneM2Mサービスアーキテクチャを下図に示す。



ここで、図の各コンポーネントは、以下の通りの意味を表す。

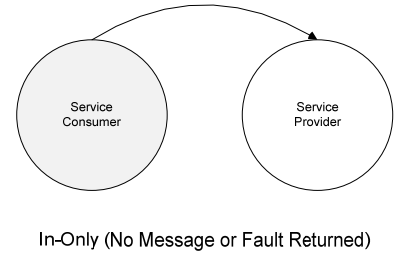
- **Service Exposure Component:** AEに対するM2Mサービス機能を露出する。.
- **Network Service Utilization Component:** NSEのサービス機能を露出する。.
- **Remote Service Exposure Component:** M2M 環境と異なるM2Mサービス機能を露出する。

2.1.4.2 Msc参照点

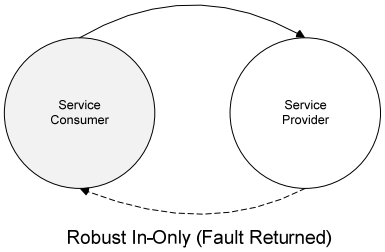
Msc参照点は、異なるサービスコンポーネントのサービス機能（Service Capability）間でのやりとりを規定する固有の参照点のことを示す。

2.1.4.3 メッセージ交換パターン

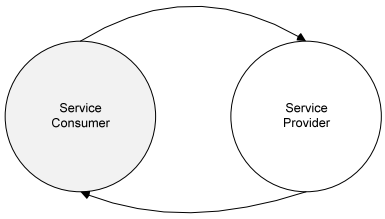
Msc参照点を通じて、M2Mサービスコンポーネント間でやりとりされるメッセージのパターンは、以下の8種類ある。



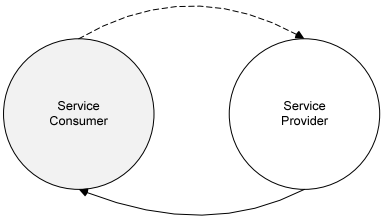
In-Only (No Message or Fault Returned)



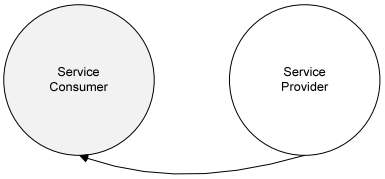
Robust In-Only (Fault Returned)



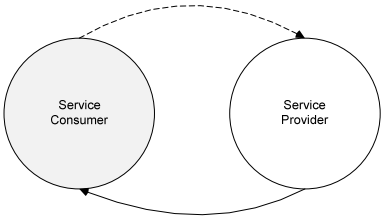
In-Out (Message or Fault Returned)



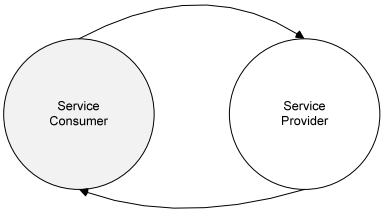
In-Optional-Out (Fault Returned)



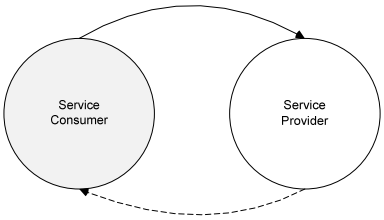
Out-Only (No Message or Fault Returned)



Robust Out-Only (Fault Returned)



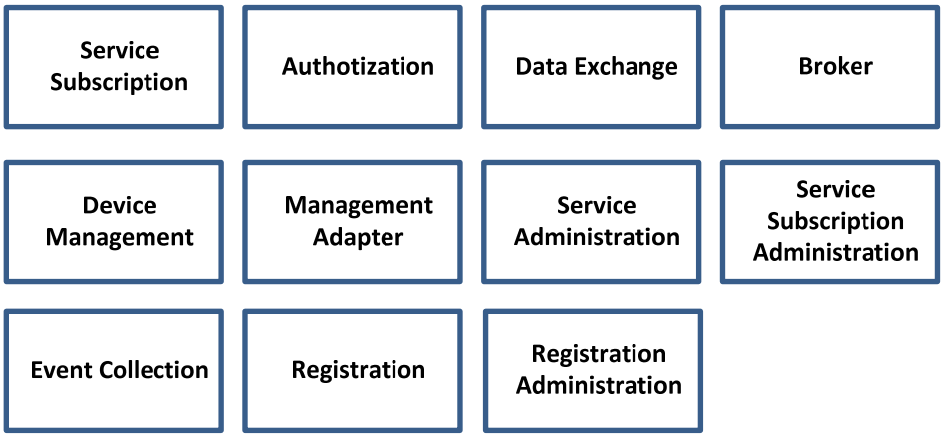
Out-In (Message or Fault Returned)



Out-Optional-In (Fault Returned)

2.1.4.4 M2M サービス

本章では、oneM2Mサービスプラットフォームにより提供されるM2Mサービスについて記述する（下図参照）。



(1) Service Subscription

M2Mサービス機能の有効化、AEのretrieve等のサービスを提供する。

(2) Authorization

サービス機能に対して、Originatorを認可する。

(3) Data Exchange

Mca参照点上で、AE間のペイロードを交換するサービスを提供する。

(4) Broker

Publish-Subscribe-Notifyや Request/ Response データ交換を適用するサービスのこと。

(5) Device Management

Mca参照点上で、デバイス管理する機能をAEに対して提供するサービスのこと。

(6) Management Adaptor

技術に特有の管理サーバの運用に対し、M2Mサービス層の運用を適応させる役割のサービスを提供する。

(7) Service Administration

M2Mサービスとサービスロール、及びサービスロールとM2Mサービス機能（M2M Service Capability）とを関連づけて管理するサービス

(8) Service Subscription Administration

Mca及びMsc参照点上でのM2Mサービスサブスクリプションの機能の維持及びM2Mサービスサブスクリプションに対するM2Mノードやサービスルールの関連付けを行う。

(9) Event Collection

アカウンティングを目的として、イベントを記録する役割のサービスを提供する。

(10) Registration

AEの新規登録、登録のリフレッシュ等を行う。

(11) Registration Administration

AEの登録状態を引き出したり、登録の解除等を行う。

2.1.5　TS-M2M-0011v2.4.1 - 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　TS-M2M-0023v2.0.0 – 家電機器の共通デバイス管理モデル

本文書は、oneM2Mにおける家電機器の共通デバイス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)を活用して規定されている。

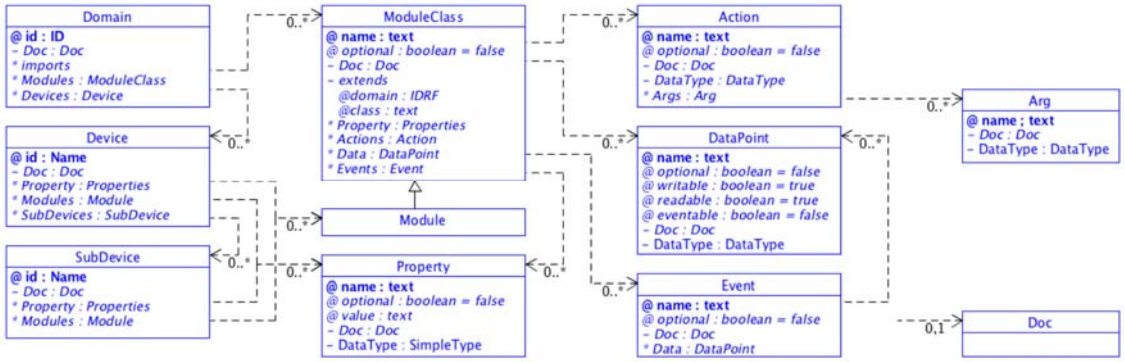


図2.2.1　Smart Device Templateの構成

共通デバイス管理モデルは、13種類の機種(Device Model)、41種類の機能(ModuleClass)として分類されており、各機種・機能の定義とこれらの定義に用いられる列挙型(Enumeration type)やデバイス属性(Property)についても規定されている。

表　2.2.1 共通デバイス管理モデルの構成

要素	具体例	項目数
ModuleClass(機能)	battery、binarySwitch、clock、doorStatus等	**41**
Device Model(機種)	AirConditioner、ClothesWasher等	**13**
Enumeration Type(列挙型)	deviceType、supportedModes等	**10**
Universal and Common Properties (共通デバイス属性)	DeviceSerialNum、DeviceModelName等	**18**

この共通デバイス管理モデルについて、oneM2Mシステムで用いるためのリソース規定についても示されている。<flexContainer>リソースの運用規定という形で規定されており、SDTにおける各要素でリソース規程ルール、各リソースのshortname、containerDefinitionの属性値、XSD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。

2.2.2　TR-M2M-0017v2.0.0 – 住宅分野に適用する抽象デバイス管理モデル

本文書では、住宅分野に適用する抽象デバイス管理モデルを定義し、住宅分野向けの oneM2M プラットフォームで動作する API を提供している。

■抽象デバイス管理モデルの紹介

以下の抽象デバイス管理モデルを紹介している。

・AllJoyn の Information model

・Apple 社の HomeKit

・HGI の SmartHome Device Template（SDT）

・ECHONET Consortium の ECHONET/ECHONET Lite

・OIC（Open Interconnect Consortium）

■抽象デバイス管理モデルのデザインに関する方針

OIC 以外の上記モデルの共通方針・'Service'を規定する場合の方針・モデル統合方針・SDT をそのまま採用する方針の 4 つの方針を説明している。

○方針 1. OIC 以外のデバイス管理モデルの方針

・各デバイスタイプはそれぞれに抽象デバイス管理モデルを持つ。

・ベンダ依存の機能は定義されない Characteristic を必要とする。

・共通の Characteristic は記述に重複がないようにする。

・家庭用機器は一つ以上の Characteristic を持つ。

・'Characteristic' はあらかじめ定義されたデバイス特性を規定する、共通かつデバイス依存な特性であり、全てのデバイスの記述重複を防ぐ。

・'Device' は TV や冷蔵庫といった実際の家庭用機器を表し、一つ以上のあらかじめ定義された Characteristic を持つ。

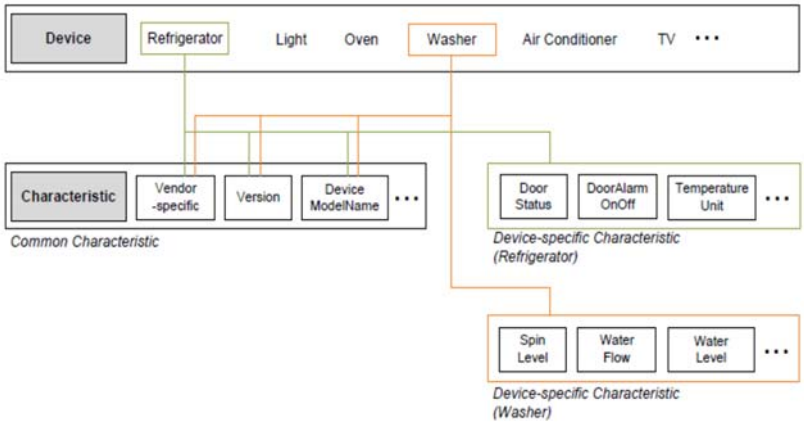


図 2.2.2-1. 方針 1 に基づいた抽象デバイス管理モデル

○方針 2. 一つ以上の特性を持つ'Service'を規定する場合の方針

・各デバイスタイプはそれぞれに抽象デバイス管理モデルを持つ。

・家庭用機器は一つ以上の Service を持つ。

・Service は common・shared・device-specific の 3 つのタイプに分けられる。

・Common Service は記述の重複を防ぐために必要。

・Shared Service は再利用によるリソース効率化に必要。

・Device-specific Service は特定デバイスの特定機能のサポートに必要。

・Service は一つ以上のあらかじめ定義された Characteristic を持つ。

・Characteristic は attribute も behavior も表せる。

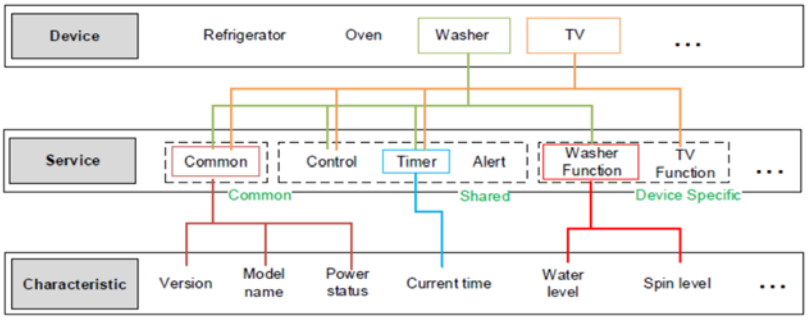


図 2.2.2-2. 方針 2 に基づいた抽象デバイス管理モデル

○方針 3. AllJoyn と SDT のコンセプトを参考に、モデル統合を目指した方針

・’Sub-device’ をサポートする。

・デバイス属性を表す’Device characteristic’ を規定する.

・’Service’ は、’Method’・‘Service characteristic’・‘Event’ を持つ。

・各家庭機器はそれぞれに抽象デバイス管理モデルを持つ。

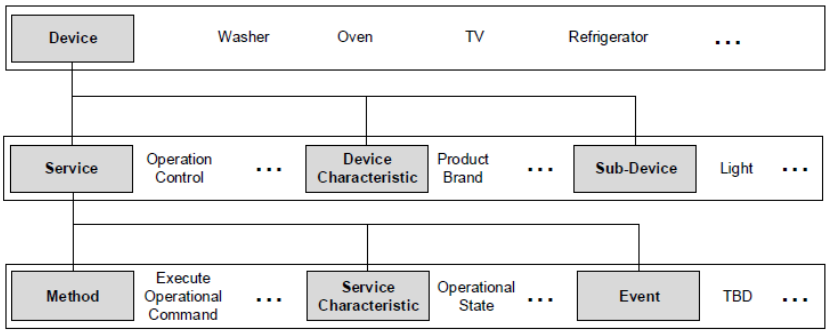


図 2.2.2-3. 方針 3 に基づいた抽象デバイス管理モデル

〇方針 4. SDT をそのまま oneM2M のデバイス管理モデルとして規定する方針

■上記方針に基づいた抽象管理モデルの具体例

上記の 4 つの方針に基づいた場合の各属性の記述方法について、冷蔵庫などを具体例にして述べている。

■デバイス管理モデルを oneM2M で表す方法

専用のリソースタイプを使用する方法と、既存の container / contentInstance リソースタイプを使用する方法の 2 種類の方法を記載している。

2.2.3　TR-M2M-0022v2.0.0 –　HGI におけるスマートホーム分野の成果の持続と統合

HGI(Home Gateway Initiative)はSmart Home Task Forceを設けて、スマートホームのためのゲートウェイについて、各種検討を実施してきた。HGIの活動終了に伴って、oneM2MではHGIにおけるスマートホーム分野の検討成果をoneM2Mの活動に統合することとし、HGI側での成果について概要を取りまとめたのが本文書である。

HGIの成果として、図2.2.3-1に示すSmart Home Gatewayのアーキテクチャ仕様(HGI-RD036)、Smart Device Template、無線通信方式に対する要求仕様(HGI-RD039)、ゲートウェイ上のOpen platformの要求仕様(HGI-RD048)が紹介されている。

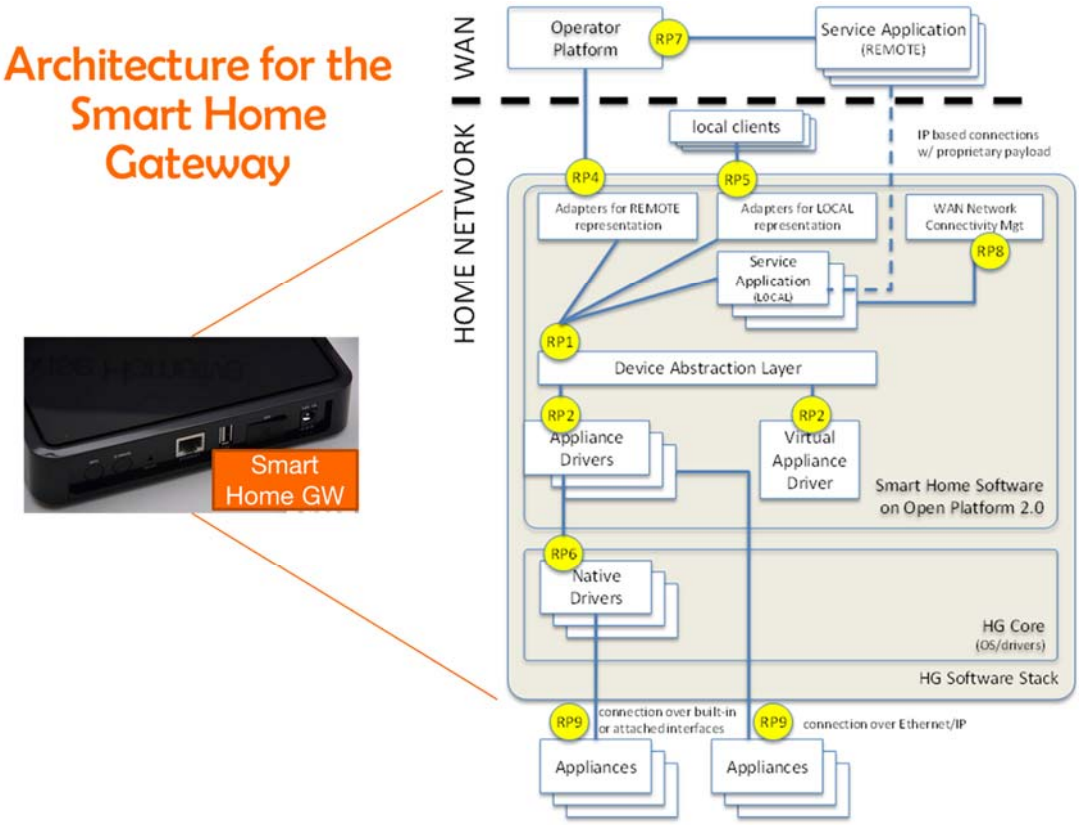


図2.2.3-1　Smart Home Gatewayのアーキテクチャと参照点

これらに基いて、Smart Homeのアーキテクチャについては、TS-0001におけるFunctional Architectureとの対応関係が示されている。また、Smart Device Templateについては、TS-0023で活用されており、oneM2Mシステムで用いるためのリソース規定への発展している。

2.2.4　TR-M2M-0018v2.0.0 –　産業分野への適用

本文書は、産業分野のユースケースと、そのユースケースを実現するために必要となる要求事項をまとめたものである。さらに、将来のoneM2M仕様拡張で必要となる技術作業を見極めるものでもある。

2.2.4.1 産業分野の概要

産業分野におけるアーキテクチャ例を図2-xに示す。M2Mシステムにより工場は製造サービスと接続される。工場内のゲートウェイがデータを収集し、管理センター内の製造サービスへ送信する。その後、製造サービス内の異なる管理モジュールが動作して、その処理結果が工場へと送り返される。

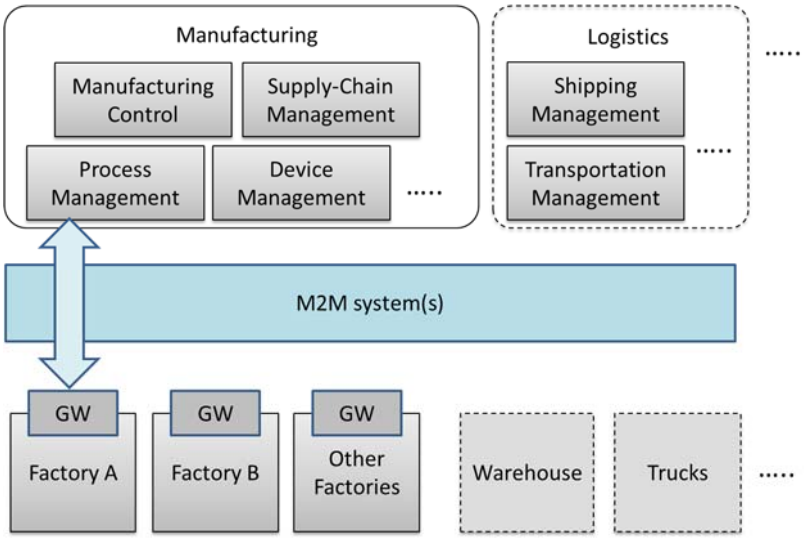


図2.2.4-1　産業分野におけるアーキテクチャ

2.2.4.2 ユースケース

本文書では、下記のユースケースについて記載する。

- 工場におけるオンデマンドデータ収集
- データ収集モニタリング
- 工場間におけるデータプロセス
- 航空機の製造および保守
- リアルタイムデータ収集
- 産業分野におけるデータ暗号化
- 産業分野におけるQoS/QoIモニタリング

2.3　プロトコルバインディングの強化

2.3.1　TS-M2M-0004v2.7.1 - 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。

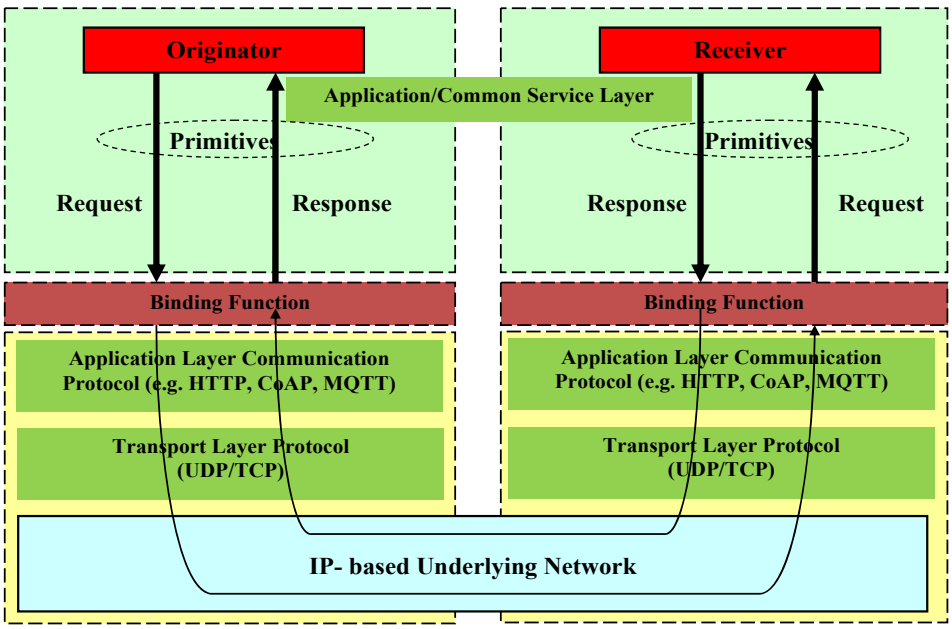


図 3.3.1-1　Request/Response プリミティブ通信のマッピング例

2.3.2 TS-M2M-0009v2.6.1- 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

2.3.2.1 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2.3.2-1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。

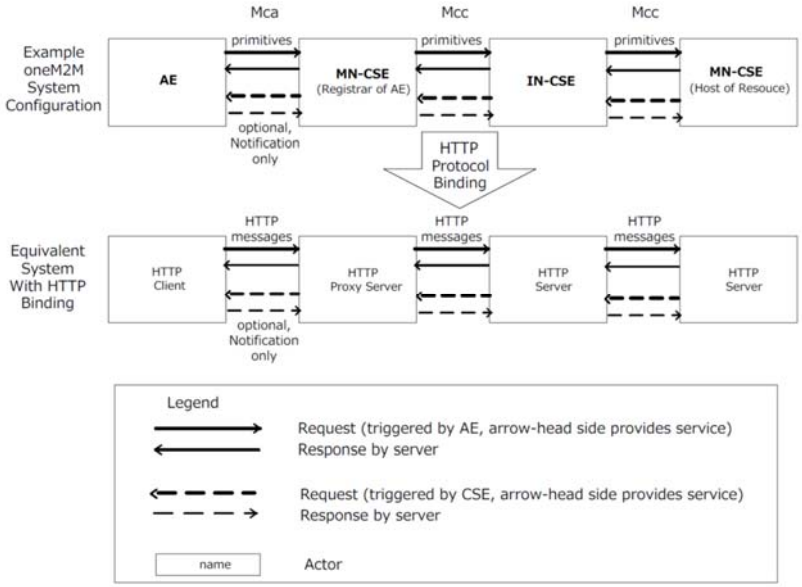


図2.3.2-1　oneM2MエンティティとHTTPクライアント／サーバとの対応関係

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。

2.3.2.2 HTTPメッセージマッピング

HTTP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。

2.3.2.3 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。

2.3.3　TS-M2M-0010v2.4.1 - 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

2.3.3.1 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。

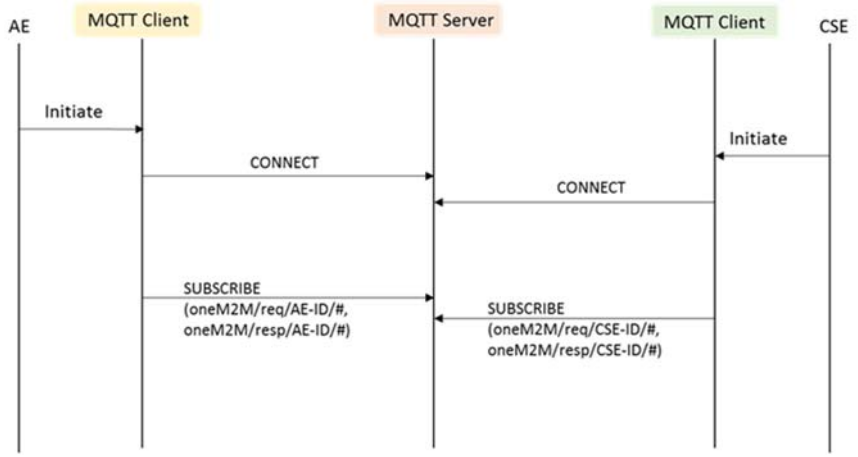


図2.3.3-1　MQTT対応での起動手順

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。

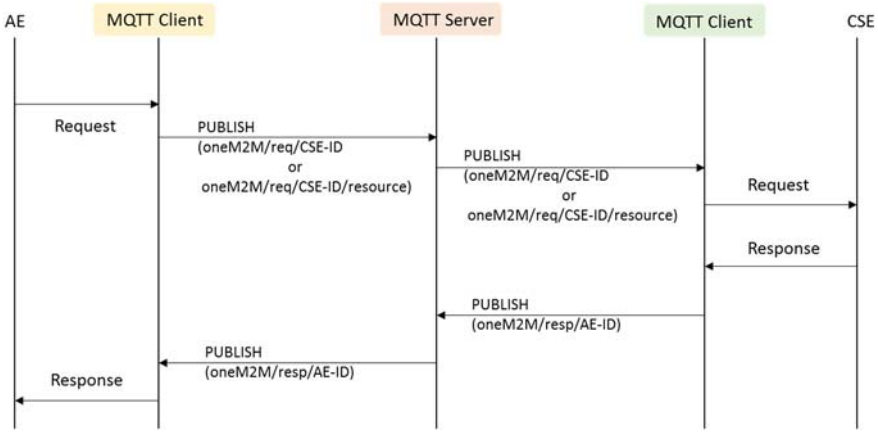


図2.3.3-2　MQTTによるリクエスト／レスポンスメッセージ送受信

2.3.3.2 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。

2.3.4 TS-M2M-0020v1.0.0 – 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。

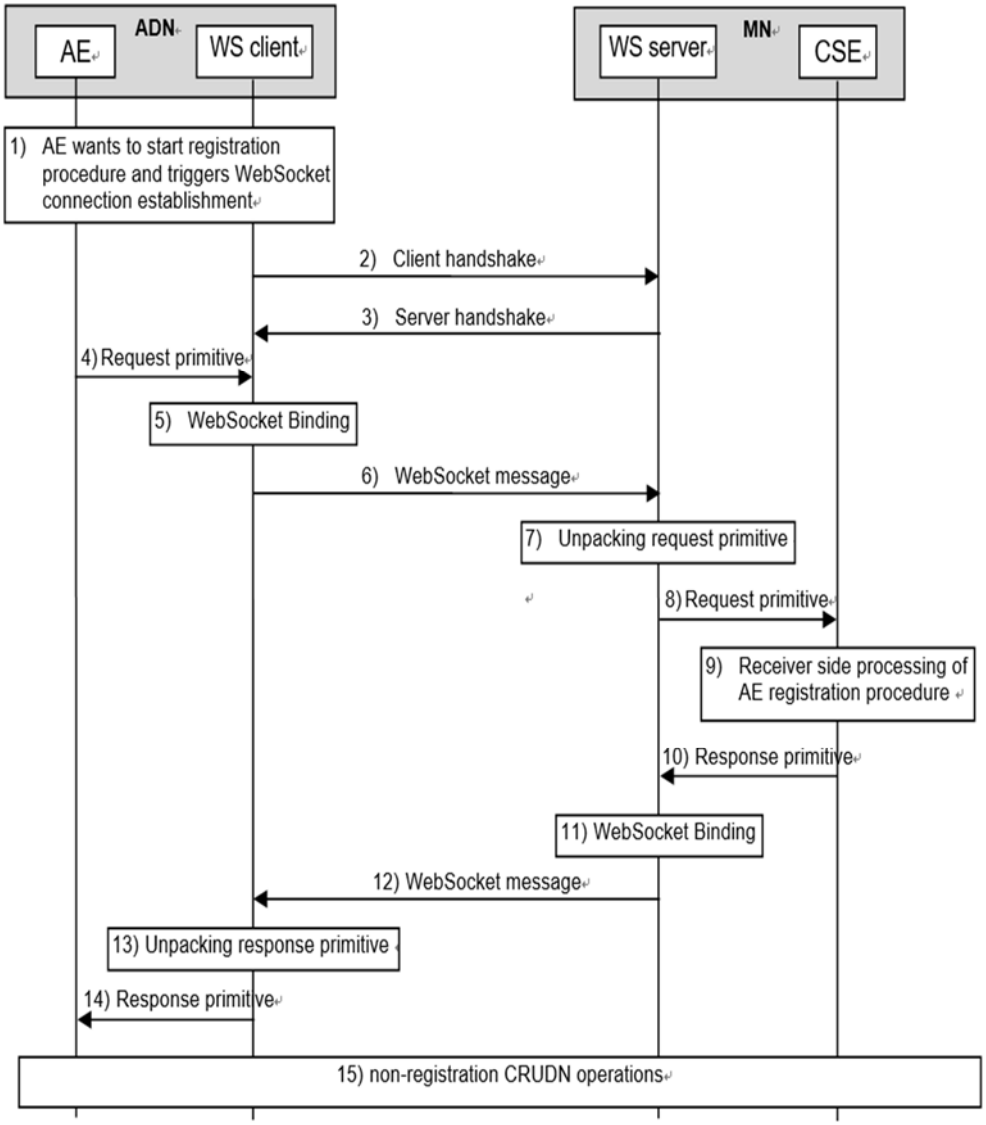


図 2.3.4-1 WebSocket バインディングのメッセージフローの一例

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。

2.4　セマンティック・インターオペラビリティ

2.4.1　TS-M2M-0012v2.0.0 - 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、汎用インタワーキングの Flex Container のリソースタイプへと詳細説明する構成になっている。

2.4.2　TR-M2M-0007v2.11.1 - 抽象化とセマンティクスの適用性検討

本文書では、oneM2Mにおいて抽象化とセマンティクス機能を実現するために利用され得る最新技術の収集と分析結果を報告している。オントロジー、セマンティクス、抽象化技術を検討している他の標準化団体・業界団体で議論されている用語と事例、oneM2M Partner Type 1からoneM2Mに移管される関連技術、およびoneM2M Partner Type 2からの情報提供が含まれる。

oneM2Mアーキテクチャとプロトコルにおいて、収集した技術とソリューションが抽象化とセマンティクス機能実現のために活用できるかについての分析結果が記載されている。

抽象化については、ETSI M2M、HGIで検討されている既存技術が紹介されている。セマンティクスについては、ETSI M2M、OGC SWE、W3C SSNで検討されている技術が紹介されている。これらを踏まえ、oneM2Mにおいて抽象化とセマンティクスをサポートするために必要となるであろう要求条件、モデル、アーキテクチャの検討結果が報告されている。

2.5　インターワーキング・フレームワーク

2.5.1　TS-M2M-0005v2.0.0 - 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）。

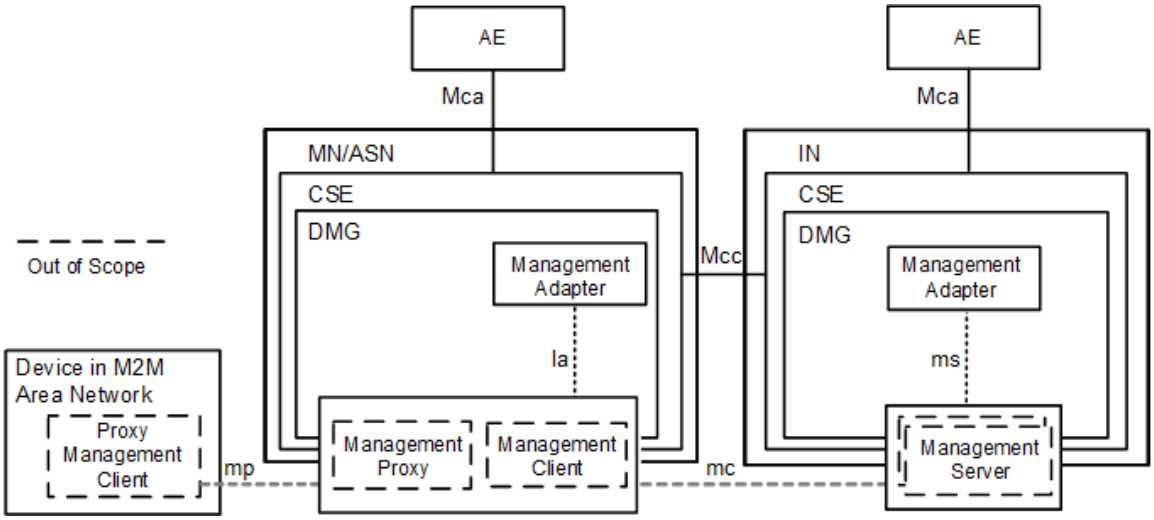


図 3.5.1-1　デバイス管理アーキテクチャ

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

- 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。）

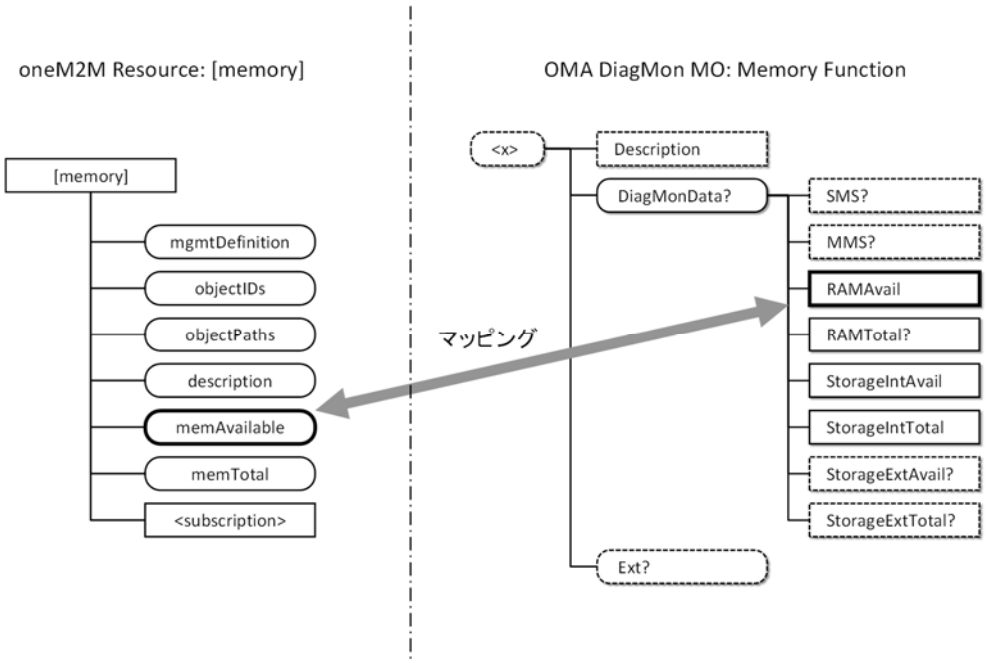


図2.5.1-2　oneM2MリソースとOMA DM MOとの対応関係（例）

2.5.2　TS-M2M-0006v2.0.1 - BBF 仕様によるデバイス管理

本文書では、既存デバイス管理技術として Broadband Forum (BBF) TR-069: CPE WAN Management Protocol (CWMP)　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。

- 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 におけるマネジメント・リソースと、BBF TR-181 デバイスデータモデルとの対応関係（7章）(表2.5.2-1に対応づけられるリソースを示す。)
- 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）
- IN-CSEとマネジメント・サーバとのやり取り（9章）
  （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。）

表 2.5.2-1　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
一般的なmgmtObj	deviceInfo, memory, battery, areaNwkInfo, areaNwkDeviceInfo, deviceCapability, firmware, software, reboot
CMDH関連	cmdhPolicy, activeCmdhPolicy, cmdhDefaults, cmdhDefEcValue, cmdhEcDefParamValues, cmdhLimits, cmdhNetworkAccessRules, cmdhNwAccessRule, cmdhBuffer
RPCサポート関連	mgmtCmd, execInstance

2.5.3 TS-M2M-0021v2.0.0 - AllJoyn とのインターワーク

本文書は、AllJoynアプリケーションとoneM2Mエンティティがサービスを相互に提供、消費するために必要となるoneM2MとAllJoynのインターワキング技術を規定している。非oneM2Mシステムとのインターワキングについては、TS-0001の付則Fに記述されているIPE（インターワキングプロキシアプリケーションエンティティ）と呼ばれる特別なアプリケーションエンティティを使用する。AllJoynインターワーキングリファレンスモデルを図2.5.3-1に示す。

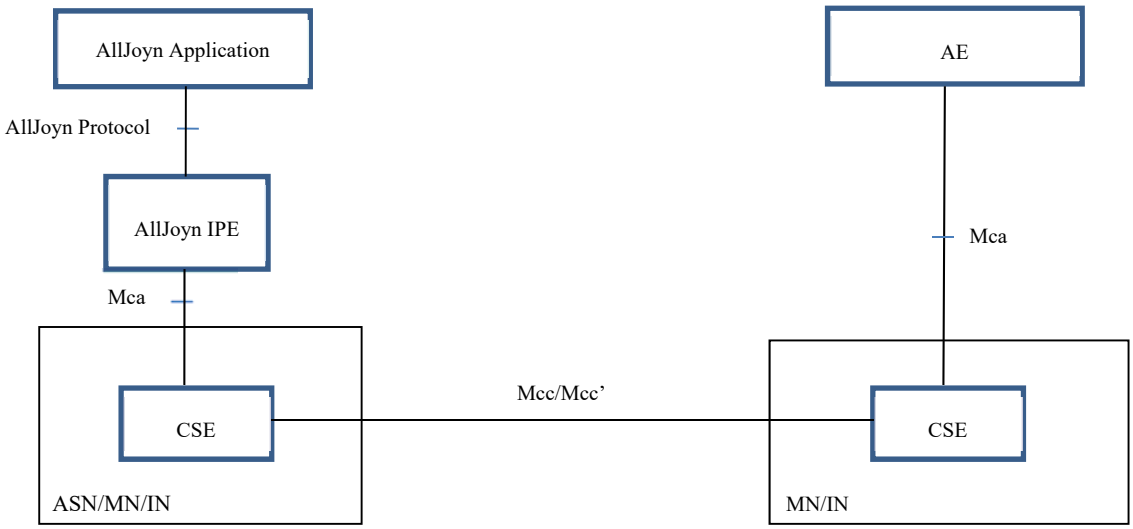


図2.5.3-1 AllJoynインターワキングリファレンスモデル

AllJoyn IPEは、oneM2MのAEとAllJoynアプリケーションによって構成されており、AllJoynのサービスはIPEによってoneM2Mリソースへのマッピングが行われ、Mca参照点を通してCSEに公開・格納される。他のoneM2Mエンティティへインターワーキング機能を提供するために、IPEは通常のAEと同様に、CSEへの登録が必要である。また、IPEはAllJoynアプリケーションとして、他のAllJoynアプリケーションとAllJoynプロトコルを使用して、やりとりを行う。

AllJoynのサービスは、oneM2Mの<flexContainer>リソースを用いたAllJoynに特化したリソースとして、マッピングが行われる。AllJoynインターワキングのために、以下のリソースが定義されている。

- svcObjWrapper
- svcFwWrapper
- allJoynApp
- allJoynSvcObject
- allJoynInterface
- allJoynMethod
- allJoynMethodCall
- allJoynProperty

2.5.4 TS-M2M-0024v2.0.0 - OIC とのインターワーク

本仕様書は、oneM2MとOICのインターワキング技術を規定する。非oneM2Mシステムとのインターワキングについては、TS-0001の付則Fに記述されているIPE（インターワキングプロキシアプリケーションエンティティ）と呼ばれる特別なアプリケーションエンティティを使用する。OICインターワーキング リファレンスモデルを図2.5.4-1に示す。

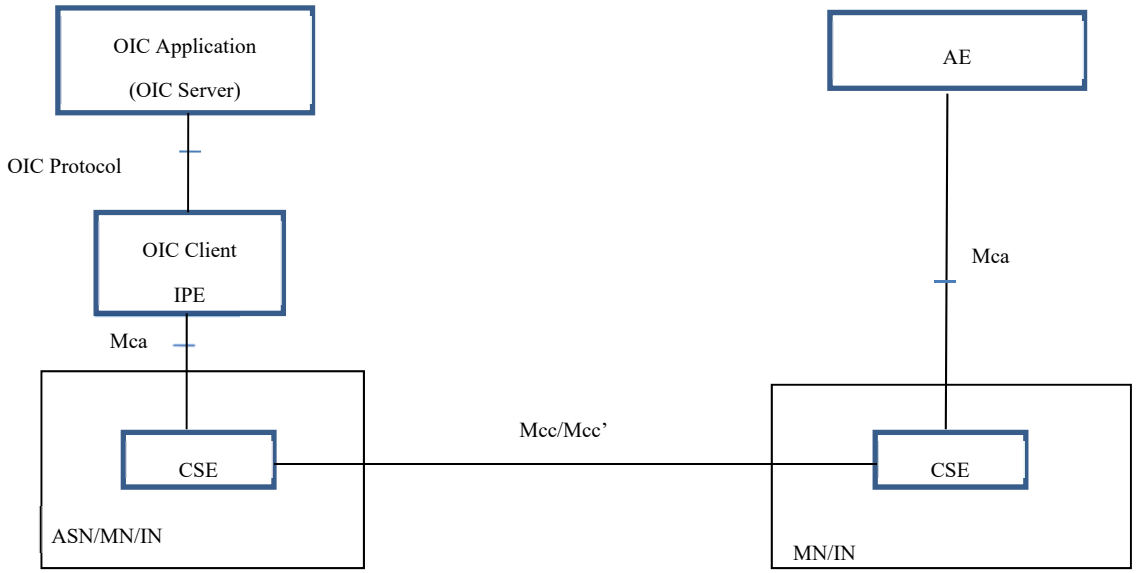


図2.5.4-1 OICインターワキングリファレンスモデル

OIC IPEは、oneM2MのAEとOICクライアントによって構成されている。OICプロトコルにおいて、IPEはOICサーバーとやりとりを行うOICクライアントの役割を担い、各OICサーバーはそれぞれAEのインスタンスとしてIPEに作成・保持される。本仕様書では<container>リソースを使用した透過的インターワーキングがサポートされている。透過的インターワーキングでは、oneM2M AEがOICで定義されているリソースデータモデルを理解していることが前提であり、<container>リソースにはOICのリソースがそのまま符号化されて格納される。本仕様書では、oneM2M AEからOICデバイスを制御することを想定しており、OIC側からはoneM2Mのアプリケーションへのアクセスはできない一方向のインターワーキングである。

2.5.5 TS-M2M-0014v2.0.0 – LWM2Mとのインターワーク

本文書は、ASN/IN/MN CSE と LWM2M エンドポイントとの間をつなぐ、M2M サービス・レイヤのインターワーキング機能を規定したものである。以下のインターワーキング・シナリオを実現するため、oneM2M TS-0001 付録 F にて割り出されたアーキテクチャが用いられている。

- LWM2M エンドポイントと M2M アプリケーションとの間のコンテンツ共有リソース内で、エンコードされた LWM2M オブジェクトとコマンドを透過的に移送するインターワーキング
- LWM2M エンドポイント内の LWM2M オブジェクトを、M2M アプリケーションが用いるセマンティクスに対応するコンテンツ共有リソースに全てマッピングする形のインターワーキング

LWM2M リファレンスモデルは、oneM2M TS-0001 の機能アーキテクチャのリファレンスモデルを流用し

LWM2M の IPE を介して接続される。

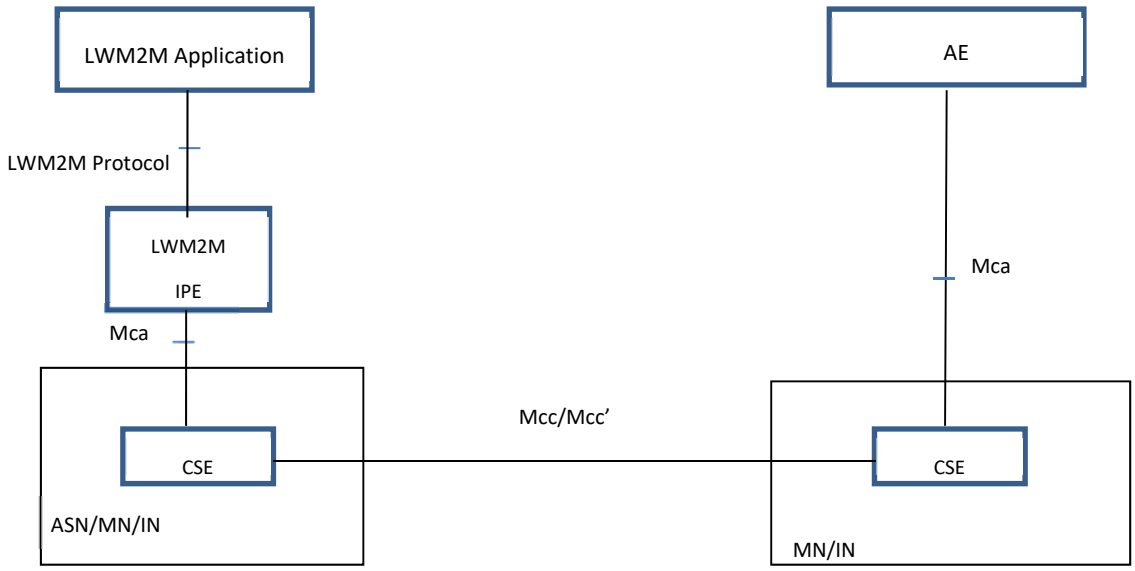


図2.5.5-1 LWM2Mインターワーキングリファレンスモデル

2.5.6 TR-M2M-0024v2.0.0 – 3GPP リリース 13 とのインターワーク

本文書は、TS 23.682 V13.2.0 で定義されているサービス・ケイパビリティ・エクスポージャーに関する 3GPP Rel-13 アーキテクチャと oneM2M アーキテクチャとの間のインターワーキングについて検討したものである。

3GPP リリース 13 では、Machine Type Communication (MTC) の文脈で 3GPP 網の一部機能をサードパーティに開示する Service Capability Exposure Function (SCEF) が定義されている。本文書では、この SCEF と oneM2M IN-CSE との関係を検討し、インターワーキングのアーキクチャとして以下が挙げられている。

A) oneM2M IN-CSE の Network Service Exposure, Service Execution and Triggering (NSSE) CSF が SCEF として動作するケース（図 2.5.6-1）

B) oneM2M IN-CSE かサードパーティとして、OMA API などの標準 API を通して SCEF にアクセスするケース（図 2.5.6-2）

C) 両者を組み合わせたハイブリッド・モード

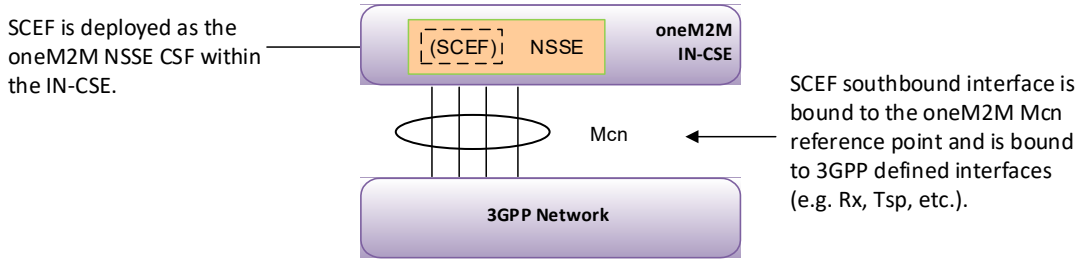


図 2.5.6-1　neM2M interworking with a 3GPP underlying network via 3GPP Reference Points

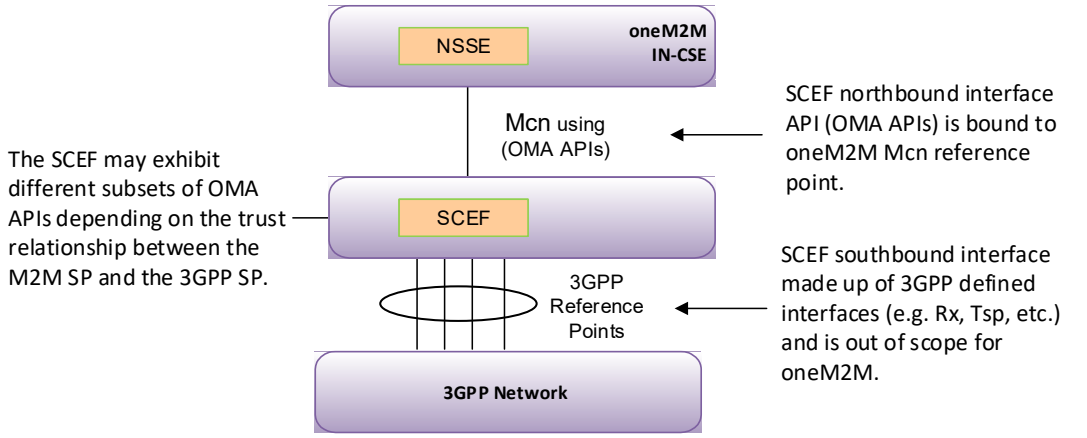


図 2.5.6-2　oneM2M interworking with a 3GPP underlying network via OMA API

本文書ではさらに、SCEF がサポートする以下の機能について、oneM2M IN-CSE を含めた動作フローや関連パラメータ等が検討されている。

- Configuration of Device Triggering Recall/Replace
- Configuration of Traffic Patterns
- Configuration of Background Data Transfers
- Support for Group Messaging
- Support for Network status report

2.6　セキュリティ

2.6.1　TR-M2M-0008v2.0.0 - セキュリティの検討

本文書では、oneM2Mシステムのセキュリティ機能を検討する前提として、各種セキュリティサービスへの機能要件の抽出や、想定される脅威について説明している。

以下のセキュリティ関連機能を、一般的な機能要件と特定の脅威への対策として提案している：

- **大切な情報を保存するためのセキュア・データストレージ**
- **大切な情報を操作するための機能**
- **通信内容を保護するための接続手段**

また、本文書ではセキュリティ・ドメインの安全性を脅かす様々なリスクについて、想定ユースケースにおける想定被害を、被害が想定されるシステム構成要素ごとに深刻度を考慮して抽出し、リストアップしている。

本文書でのセキュリティ関連機能の抽出と脅威分析の結果として、Security CSFは以下で示される階層構造を持ったセキュリティ機能群として定義された。

Security Functions Layer: Mca, Mcc 参照点で利用されるセキュリティ機能群。(AE/CSEの)識別(Identification)、認証(Authentication)、認可(Authorization)、セキュリティ・コンテキストの紐づけ(Security Association)、大切な情報の保管(Secure Data Handling)、セキュリティ機能の制御(Security Administration)からなる。

Secure Environment Abstraction Layer: 短命鍵の生成や、データ暗号化/復号化、電子署名の生成/検証、認証用秘密情報の生成/保存/読み出しなどの(Security Functions Layerが提供するセキュリティ)機能を提供する。

Secure Environments Layer: 前記のSecure Environment Abstraction Layerが提供する機能を提供する実体で、Abstraction Layerより低レイヤーの処理であるSE機能(鍵データ/運用ポリシーの管理機能、データの暗号化保存機能など)を提供する。

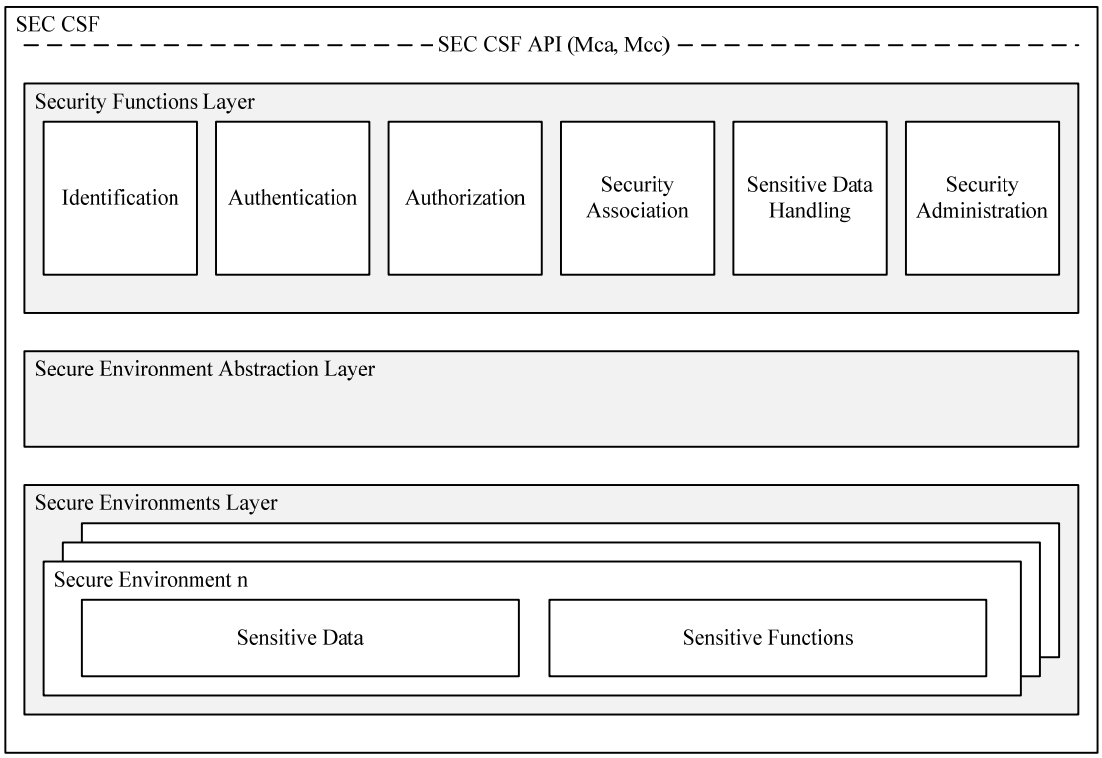


図2.6.1-1：セキュリティCSFの概略

2.6.2　TS-M2M-0003v2.4.1 - セキュリティ技術の適用

本文書は、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 2 で追加された主な機能について、以下に記載する。

2.6.2.1 Dynamic Authorization

Dynamic Authorization は、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フレームワークである。

ユースケース、要求条件は、TR-0019 Dynamic Authorizationに記載されている。また本文書では、Originator～Hosting CSE間のDynamic Authorizationパラメータと関連する処理について規定している。またDynamic Authorizationパラメータの伝送は、TS-0001 Functional Architecture、TS-0004 Service Layer Core Protocol Specificationで規定している。

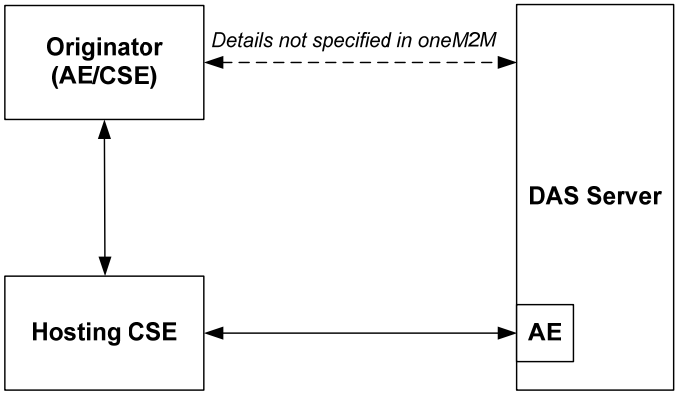


図2.6.2-1: Dynamic Authorization参照モデル

認可情報を伝送する Token は、以下に示す通り、Version、tokenID、issuer、holder、有効期限（notBefore,notAfter）、permissions 等から構成される。

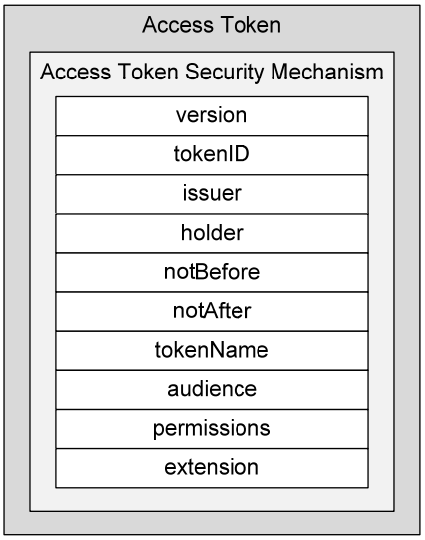


図2.6.2-2 Tokenの構造

2.6.2.2 Role Based Access Control

oneM2M システムにおける Role Based Access Control アーキテクチャの概要を下図に記載する。Oringinator は、Authorization Authority を介して、Role/Token Repository に保存されている<role>/<token>リソースを取得し、必要なロールを取得し、Hosting CSE へのアクセスを行う。

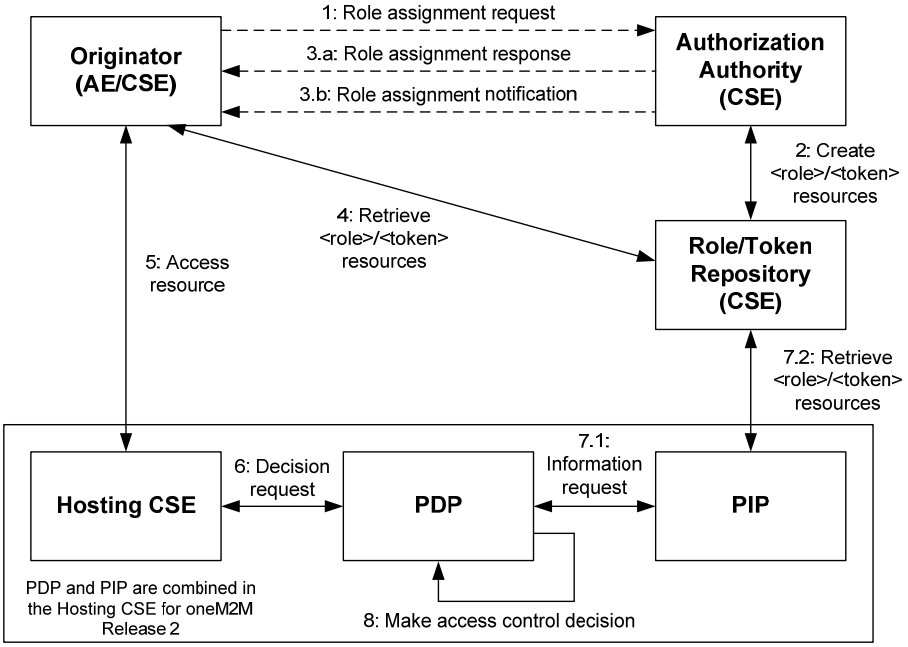


図2.6.2-3 Role based Access Controlアーキテクチャ

2.6.2.3 ESPrim （End-to-End Security of Primitives）

ESPrimは、Originator～Receiver間で相互認証、高い機密性、完全なプロテクション等を提供するため、セキュアなoneM2Mプリミティブに必要なフレームワークを提供する。

本文書は、ESPrimのクレデンシャル管理、データ・プロテクションを規定しており、ESPrimオブジェクトの伝送方法については、TS-0001 Functional_Architectureで規定している。

また利用できるユースケース、要求条件は、TR-0012 End-to-End-Security and Group Authenticationに記載している。

2.6.2.4 ESData（End-to-End Security of Data）

ESDataは、oneM2M参照点を使用して伝送されるプロテクション・データに必要となるフレームワークを提供する。このプロテクション・データは、ESData Payloadと呼ばれ、属性値（<contentInstance>リソースのcontent属性値等）、またはプリミティブ・パラメータから構成される。

利用できるユースケース、要求条件は、TR-0012 End-to-End-Security and Group Authenticationに記載している。

2.6.2.5 Remote Security Frameworks for End-to-End Security

本章では、エンティティが、TEF(Trust Enabler Function)を使用して、End-to-Endのセキュリティを提供するフレームワークを記載している。下図は、TEFを介したリモートレジストレーション、プロビジョニングのシーケンス概要を示している。

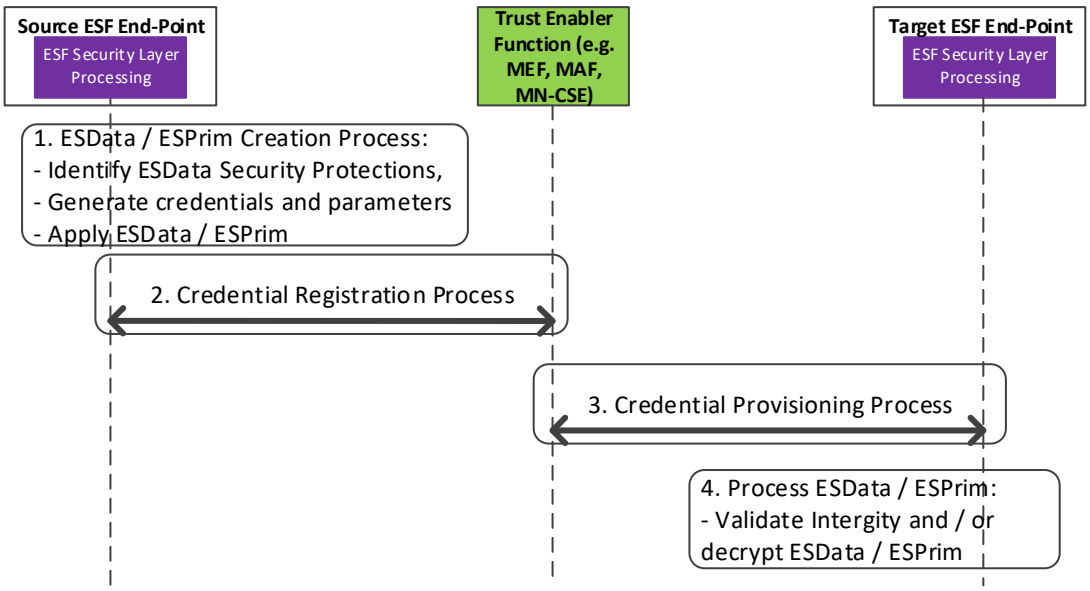


図2.6.2-4 TEFを使用したEnd-to-End Remote Securityのシーケンス概要

2.6.2.6 ESCertKE (End-to-End Certificate-based Key Establishment)

ESCertKEは、E2EKeyと呼ばれるシークレットなシメトリック鍵生成で必要となる認証処理のためのエンド・エンド間のフレームワークを提供する。

本文書では、ESCertKEメッセージ、ESCertKEと関連する処理を規定している。利用できるユースケースと要求条件は、TR-0012 End-to-End-Security and Group Authentication に記載している。またESCertKEメッセージの伝送は、TS-0001 Functional_Architectureで規定している。

ESCertKEのメッセージフローを以下に示す。

2.6.3 TR-M2M-0012v2.0.0 - エンド・エンドセキュリティとグループ認証

本文書は、エンドツーエンドでプリミティブとデータの秘匿及び完全性などを保証する仕組みと、グループ認証の仕組みについて記述された技術報告書である。Release1ではトランスポート層やインターネット層のセキュリティについては規定されているが、アプリケーション層のセキュリティについては規定されていない。本文書では、アプリケーション層でのエンドツーエンドセキュリティについて、ユースケース、関連技術の紹介、Release2に向けたoneM2Mアーキテクチャへの適用について記述されている。

2.6.3.1 ユースケース

エンドツーエンドセキュリティとグループ認証に関して、以下のユースケースが紹介されている。

- エンドツーエンドでの秘密情報の共有
- スタティックなグループ認証（例：スマートメータ）
- ダイナミックなグループ認証（例：遠隔での自動車管理）
- セキュアなグループ間の通信
- エンドツーエンドでの認証
- エンドツーエンドでのメッセージ認証
- エンドツーエンドでのデータの完全性検証

2.6.3.2　関連技術の紹介

エンドツーエンドセキュリティにおいて、既存のアプリケーション層のセキュリティであるオブジェクトベースセキュリティについて、以下の例の紹介が記述されている。

- Secure/Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP
- XML Signature and XML Encryption
- JSON Object Signing and Encryption (JOSE)

グループ認証に関しては、図2.6.3-1に示すスタティックなグループを想定した場合について次の3つ段階に分けて説明をしている。

1. Inner Group Authentication

グループ内のエンティティ（ASN、ADN）とMNが、TLSを用いて相互認証及びセキュアチャネルの確立を行う。

2. Outer Group Authentication

MNがグループの代表として振る舞い、TLSを用いてINと相互認証及びセキュアチャネルの確立を行う。

3. Group Security Association Handshake

事前共有されている情報を用いてグループ内のエンティティ（ASN、ADN）とINでコネクション鍵の共有を行う。

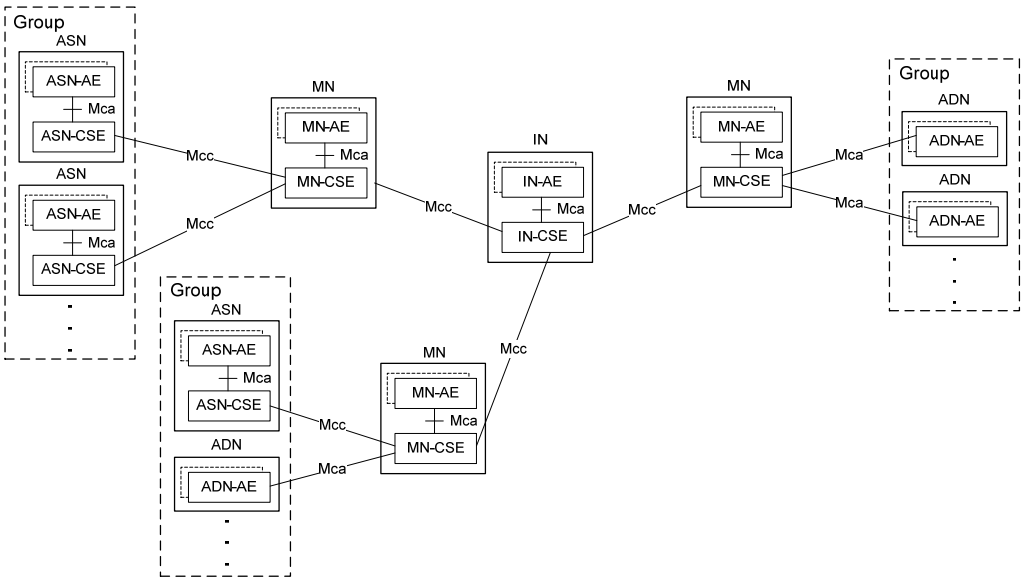


図2.6.3-1 スタティックなグループ認証におけるアーキテクチャ

2.6.3-3　Release2に向けたエンドツーエンドセキュリティ

エンドツーエンドセキュリティに関しては、本文書では以下の4つが規定されており、それぞれがRelease2の機能として規定されている（TS-0001, TS-0003, TS-0004に規定）。

- End-to-End Security of Data (ESData)

ペイロード部分の暗号化

- End-to-End Security of Primitives (ESPrim)

oneM2Mのプリミティブ部分の暗号化

- End-to-End Security Certificate-based Key Establishment (ESCertKE)

証明書を用いたEnd-to-End Securityで使用する共通鍵の共有

□ Generic MAF Security Frameworks

エンティティ間の認証にMAF (M2M Authentication Function)を使用し、エンティティ間の共通鍵の共有をMAF経由で行う方式

2.6.4 TR-M2M-0016v2.0.0 - 認可アーキテクチャーとアクセス制御ポリシー

本文書は、認可に関するアーキテクチャと認可に使用するアクセス制御ポリシーについて記述された技術報告書である。Release1においては、リソースを保持するCSEがアクセス制御ポリシーを持ち、認可を行なっていたが、本文書では、Release2に向けて認可機能の拡張を目的とし、外部のCSEで認可できるアーキテクチャについて記述されている。

2.6.4.1 認可アーキテクチャ

図2.6.4-1に認可アーキテクチャの概要を示す。認可においては、PEP、PDP、PRP、PIPの4つの機能に分割される。

- PEP: リソースへのアクセスに対して、アクセス制御の判断をするためのリクエストを行い、得られたアクセス制御の結果を適用する。
- PDP: アクセス制御のリクエストに対して、アクセス制御の判断に必要な情報を PDP と PIP から取得し、アクセス制御の結果を PEP に出力する。
- PRP: リソースに対応するアクセス制御ポリシーを取得し、PDP に送信する。
- PIP: アクセス制御の判断に必要な、リソースや Requester に関する情報を PDP に送信する。

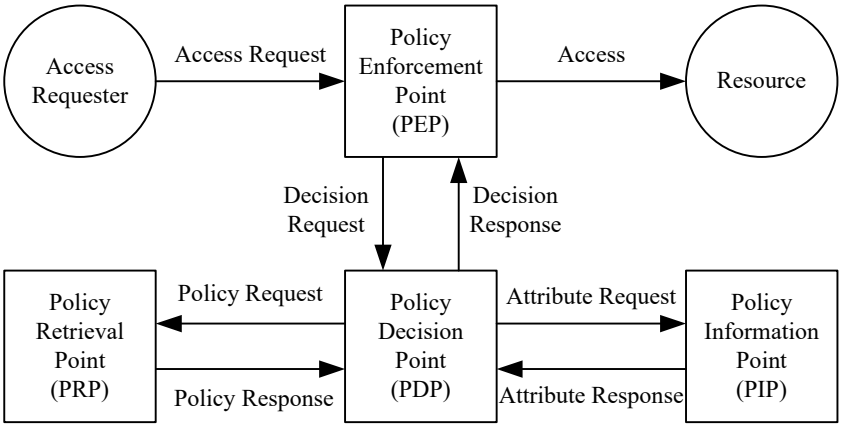


図2.6.4-1：認可アーキテクチャの概要

2.6.4.2 Distributed Authorization

図2.6.4-2にDistributed Authorizationの例を示す。PEP=Device1、PDP=M2M Gateway、PRP=M2M Server 1、PIP=M2M Server 2と対応しており、認可の機能が異なるエンティティに分散されている。この方式は、Release2では規定されていない。

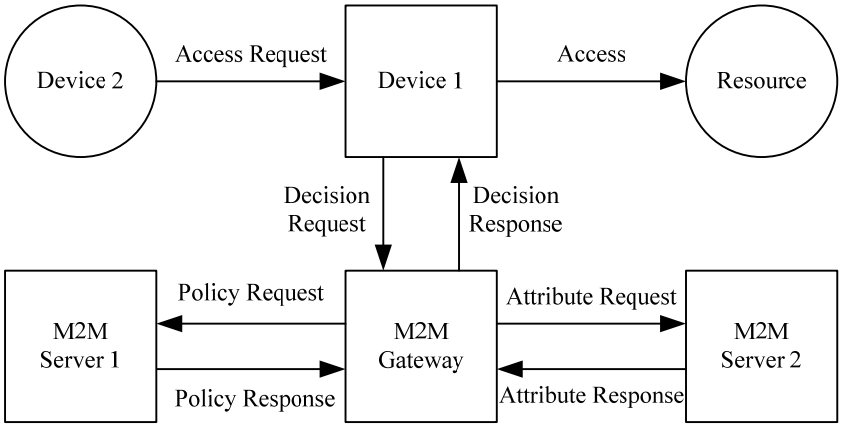


図2.6.4-2：Distributed Authorizationの例

2.6.4.3 Role Base Access Control

図2.6.4-3にRole Base Access Control (RBAC) の概要を示す。RBACでは個人やエンティティごとにアクセス権限を割り当てるのではなく、個人やエンティティに役割(Role)を割り当て、Roleに対してアクセス権限を割り当てる。この方式は、Release2に規定されている。

RBACにおいてはデータの要素として、users (USERS)、 roles (ROLES)、operations (OPS)、objects (OBS)、permissions (PRMS) の5つが規定されている。また、SESSIONSではuserとuserに割り当てられているroleのセットがマッピングされている。Static Separation of Duty (SSD)及びDynamic Separation of Duty （DSD）では、ユーザへのroleの割り当てやSESSIONSへのroleの追加及び削除に関して管理を行う。

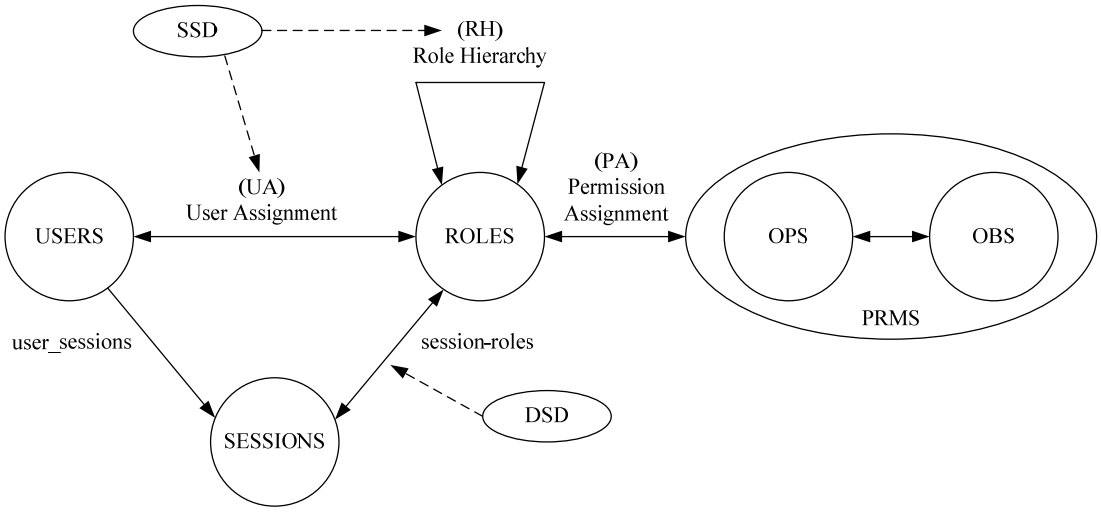


図2.6.4-3：Role Base Access Controlの概要

2.6.4-4 アクセス制御ポリシー言語

既存のアクセス制御ポリシー言語としてOASISで定義されているeXtensible Access Control Markup Langiage (XACML)について調査を行なっている。図2.6.4-4にXACMLによるポリシーの構造を示す。

本文書では、XACMLは標準化されたアクセス制御言語である点と、属性ベースのアクセス制御ポリシーに適している点から、oneM2Mシステムでの利用を推奨している。

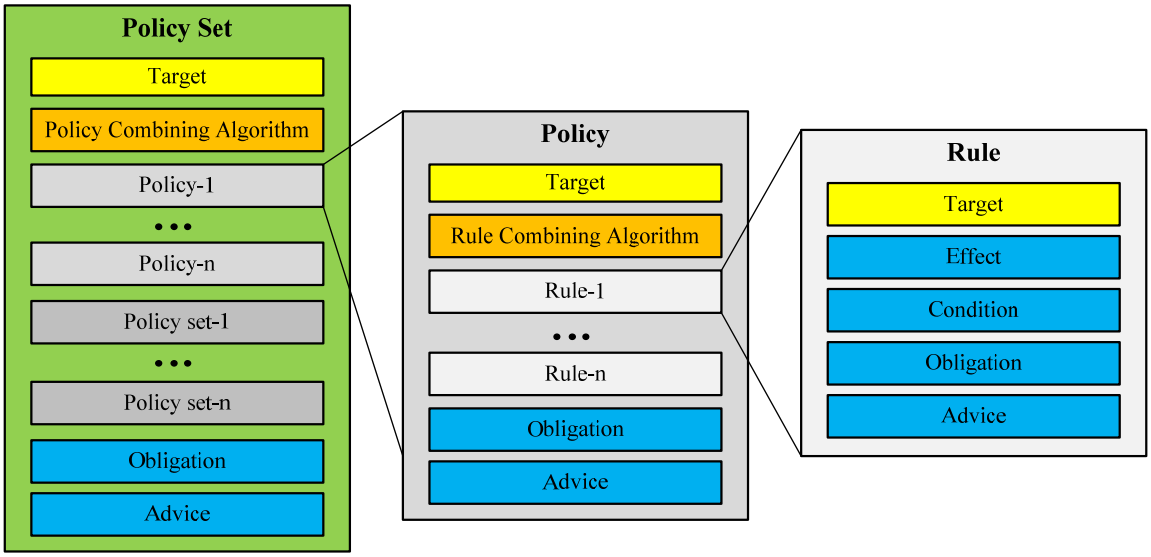


図2.6.4-4：XACMLによるポリシーの構造

2.7　試験と相互接続性

2.7.1　TS-M2M-0015v2.0.0 -試験フレームワーク

本文書は，oneM2M標準のための規格適合性試験および相互接続生試験の戦略，テストシステム，結果として作られるテスト仕様の開発の方法論を定義する試験フレームワークを規定する．

試験フレームワークの全体を図2.7.1-1に示す．基本となる仕様書(TS-0001, TS-0004など)と試験方法論，規格適合性試験仕様，相互接続生試験仕様とのやりとりが示されている．

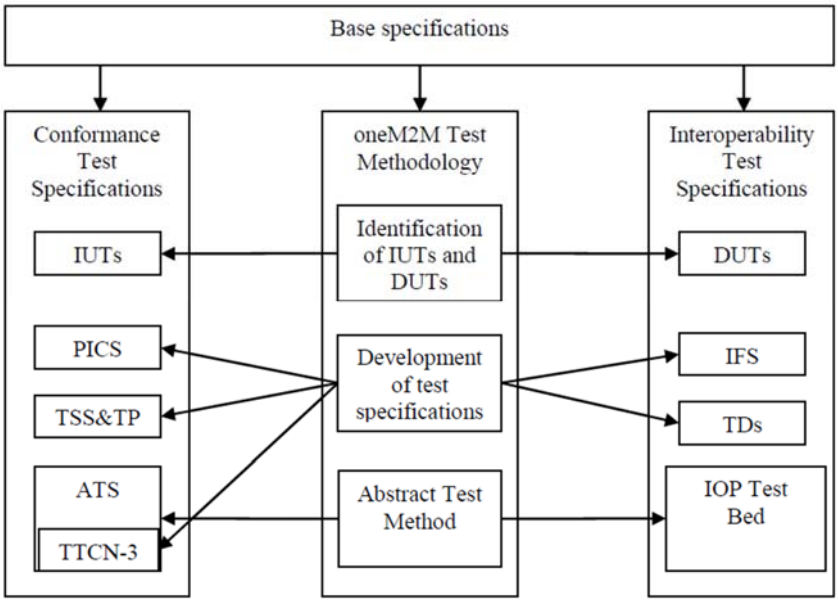


図2.7.1-1 oneM2M試験フレームワーク

表 2.7.1-1 oneM2M 試験フレームワーク中の略語

略語	原文	日本語訳または説明
IUT	Implementation Under Test	テスト対象となる実装
PICS	Protocol Implementation Conformance Statement	プロトコル実装適合性明細書
TSS	Test Suite Structure	テストスイート構造
TP	Test Purpose	テストの目的
ATS	Abstract Test Suite	抽象テストスイート
TTCN-3	Testing and Test Control Notation version 3	試験用プログラム言語
DUT	Device Under Test	テスト対象となるデバイス
IFS	Interoperable Features Statement	相互接続特性明細書
TD	Test Description	テスト記述
IOP	Interoperability	相互接続性

表2.7.1-2にテストスイート構造の例を示す．対象デバイス，テストする機能，テストのカテゴリ（正常系/異常系）などの要素から構成されている．

表 2.7.1-2 テストスイート構造の例

TP/<root>/<gr>/<sgr>/<xx>/<nnn>		
<root> = root	oneM2M	oneM2M
<gr> = group	AE	Application Entity
	CSE	Common Services Entity
<sgr> = sub- group	REG	Registration
	DMR	Data Management and Repository
	SUB	Subscription and Notification
	GMG	Group Management
	DIS	Discovery
	LOC	Location
	DMG	Device Management
	CMDH	Communication Management and Delivery Handling
	SEC	Security
<xx> = type of testing	BI	Invalid Behaviour tests
	BO	Inopportune Behaviour tests
	BV	Valid Behaviour tests
<nnn> = sequential number		001 to 999

テスト目的は，期待されるテストの振る舞いの記述であり，通常，定型化されない口語で記載される．oneM2Mではテスト目的の明確化，可読性の向上のため，テンプレート（表2.7.1-3）を決めている．

表 2.7.1-3 テスト目的のためのテンプレート

TP Id		
Test objective		
Reference		
Config Id		
PICS Selection		
Initial conditions		
Expected behaviour	Test events	Direction
	when { }	IUT ← AE
	then { }	IUT → AE

規格適合性試験に用いる抽象プロトコルテスターの概念を図2.7.1-2に示す．oneM2Mでは，OSIのアプリケーション層プロトコルとして，HTTP, CoAPまたは，MQTTが用いられる．このプロトコルに依存しない形のPDUをやり取りする形でテストを記述することで，効率的にテストを記述することができる．

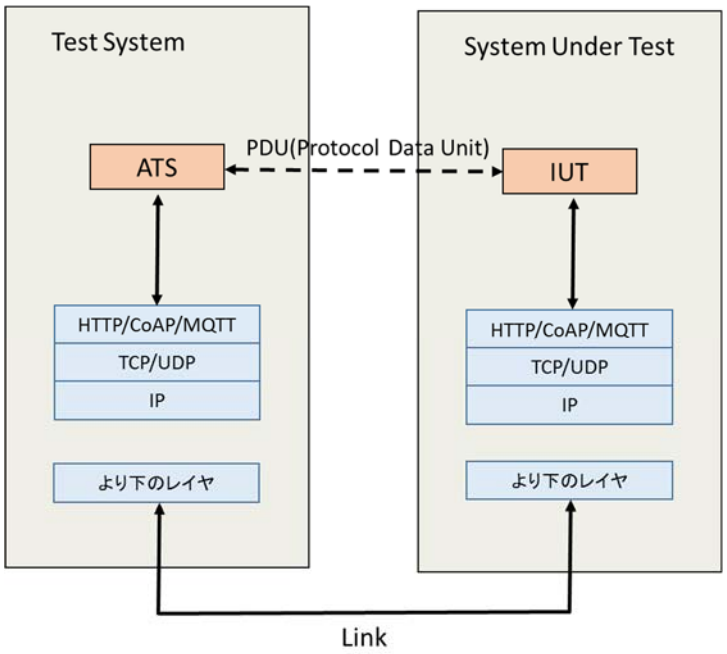


図 2.7.1-2 oneM2M のための抽象プロトコルテスター

2.8　アプリケーション開発ガイド

2.8.1　TR-M2M-0025v1.0.0 - アプリケーション開発ガイド

本文書は、oneM2Mアプリケーション開発者が各種oneM2M仕様書を参照する前に、oneM2M仕様の全体像を把握可能とする事を目的としている。簡単なユースケースを例に、 oneM2Mアーキテクチャへのマッピングや信号フロー、信号コーディング、実装といった一連の開発手順がまとめられている。

2.8.1.1 ユースケース例

本ガイドで解説する内容は、図2.8.1-1に示す『ライトの遠隔制御』のユースケースをベースとしている。

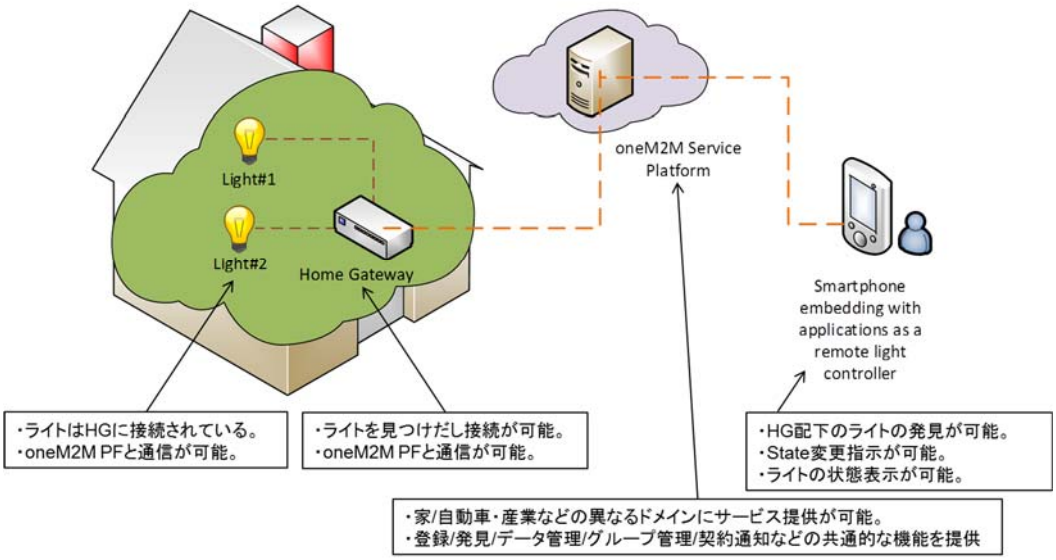


図2.8.1-1　本ガイドで扱うユースケース例：ライトの遠隔制御

2.8.1.2 アーキテクチャおよび信号フロー例

ユースケースに対応したoneM2Mアーキテクチャへのマッピングおよび、登録手順や発見手順等の複数の信号フローがわかりやすく解説されている。

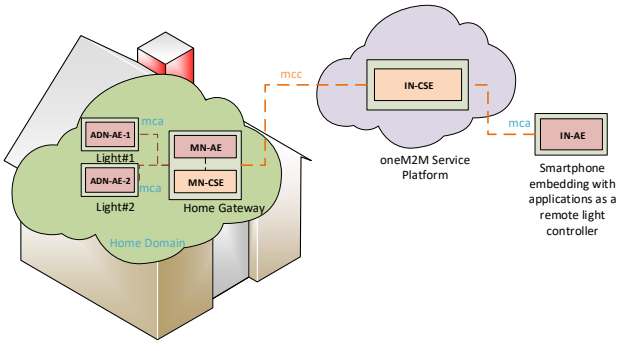


図2.8.1-2　ライトの遠隔制御におけるアーキテクチャ

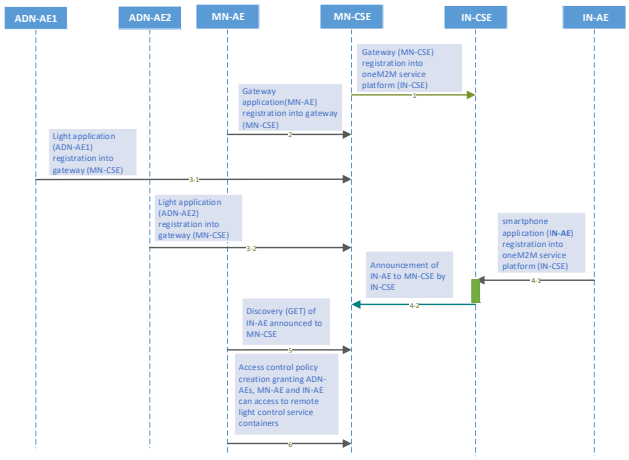


図2.8.1-3　信号フロー（例：登録手順）

2.8.1.3 実装時に考慮する設定値例

oneM2M共通および本ユースケースに特化した前提条件が示されている。さらに、ユースケースに対応したHTTPレイヤの具体的な設定値を示しており、汎用的なHTTPプロトコル上の実装レベルの考慮点が理解可能となる。

第３章　おわりに

2016年8月にリリース2として発行された17件の技術仕様書及び9件の技術報告書では、2015年1月に完成したリリース1仕様書（10件のうち9件）の改訂と、概ね6分野にわたる新たなフィーチャーの追加が行われた。

次期リリース（リリース3）は、現時点では、2016年10月から2017年10月までを作業目標期間とされており、以下の3項目にフォーカスして策定が進められることを合意している。

(1) Work Track 1：Market Adoption

これまで作成してきた仕様書（リリース1及びリリース2）により、M2M/IoTに必要な共通機能や他のIoT技術とインターワークするためのしくみ、セマンティック・インターオペラビリティ、セキィリティ＆プライバシー、テスト用フレームワークと試験仕様等が完成した。次期リリースでは、これらの技術が市場により採用されることを促進するために、どのような標準化活動が必要かについてフォーカスし、以下の項目を中心に検討する。

① これまでに策定した仕様の修正や若干の機能の高度化
② oneM2M技術の採用や容易なインプリを行うための、ガイドライン・仕様書の開発または強化、及びベストプラクティス文書の作成
③ 試験仕様
④ リリース2で積み残した文書で完成の近い文書の策定促進

(2) Work Track 2：IIoT（Industrial IoT）やSmart City

⑤ クルマ分野を含むIIoT（Industrial IoT）やSmart Cityに関するサービス展開を睨んだ検討及びその分野の技術専門家へのアピール
⑥ クルマ分野を含むIIoT（Industrial IoT）やSmart Cityに関する改善及び要求条件の追加
⑦ 同分野の新規フィーチャーに関する検討（技術報告書の作成）

(3) Work Track 3：将来技術分野

AI（人工知能）、ビッグデータの解析技術等、将来技術に関する検討

次期リリースの内容としては、以下のような作業項目（Work Item）が候補として挙げられている。

WI 番号	タイトル	概要
WI-0046	Vehicular domain enablement	Vehicularドメインにおけるユースケース、要求条件、アーキテクチャの分析
WI-0047	DDS usage in oneM2M system	DDSとのインターワーキング、プロトコルバインディング
WI-0048	OSGi Interworking	OSGiとのインターワーキング
WI-0049	Maintenance of oneM2M Release 1 and 2　(REL1&2_MNT)	Release1、2のエディトリアルな修正
WI-0050	Small Technical enhancements of oneM2M Release 3(REL3_STE)	Release2のフィーチャに関する小規模な機能の高度化のための修正
WI-0051	Security Functions Conformance Testing	セキュリティ機能に関するコンフォーマンステスト仕様の作成

WI-0052	LWM2M DM &Interworking Enhancements	リリース２のOMA Light Weight M2M インターワーキングの強化
WI-0053	Rel-3 Enhancements on Semantic Support	リリース２で開発したSemantic Supportの強化(Release3)
WI-0054	Developers guide series	アプリ開発者を支援するためのガイドブックの作成
WI-0055	Product Profiles & Feature Catalog	oneM2M仕様準拠のプロダクト開発者に理解しやすいように、機能セット、テストケース、パラメータとリソースの関係等を記載したカタログの作成。
WI-0056	Evolution of Proximal IoT Interworking	OCF、AllSeen、ZigBee 等の Proximal 技術とのインターワーキングの機能の強化
WI-0057	TEF Interface	セキュリティ関連の Trust Enabling Function （TEF）M2M Enrolment Function （MEF） M2M Authorization Function （MAF）の規定
WI-0058	Interworking with Cellular IoTnetwork features (Cellular IoT IWK)	3GPP Rel.13,14（LPWA 等）とのインターワーキング
WI-0059	OPC-UA Interworking	Industrial Domain の情報モデルである OPC-UA （OPC Unified Architecture）とのインターワーキング
WI-0060	Interoperability testing Release 2	リリース２仕様に関する Interoperability（相互接続性）テストの作成
WI-0061	Distributed Authorization	oneM2M の認可方式 Distributed Authorization の規定
WI-0062	Service Layer Forwarding	相互接続性試験の際に判明した件に基づき、複数の CSE の連携の際に必要な要求等の情報を forward して機能させる取り組み
WI-0063	Release3 Enhancements on Base Ontology & Generic Interworking	リリース２で開発した Generic Interworking の強化（オントロジー等）。
WI-0064	Adaptation of oneM2M for Smart City	oneM2M 技術の Smart City への適用
WI-0065	Trust Management in oneM2M	oneM2M における Trust Management の検討