TTC技術レポート
Technical Report

TR-M2M-R1v1.0.0

oneM2Mリリース１の構成と解説

Structure and Interpretation of
oneM2M release 1

第1版

2015年3月30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

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。

＜参考＞ 4
はじめに 5
第 1 章　oneM2M リリース 1 の構成 6
1.1　oneM2M リリース 1 の構成と TTC 仕様書との対応 6
1.2　文書間の関係 7
第 2 章　oneM2M リリース 1 の解説 8
2.1　TS-M2M-0002 v1.0.1 - 要求条件 8
2.2　TS-M2M-0001v1.6.1 - 機能アーキテクチャ 9
2.3　TS-M2M-0003 v1.0.1 - セキュリティ技術の適用 10
2.4　TS-M2M-0004 v1.0.1 - サービス層 API 仕様（共通部） 11
2.5　TS-M2M-0005 v1.0.1 - OMA 仕様によるデバイス管理 12
2.6　TS-M2M-0006 v1.0.1 - BBF 仕様によるデバイス管理 15
2.7　TS-M2M-0008 v1.0.1 - サービス層 API 仕様（CoAP 用） 16
2.8　TS-M2M-0009 v1.0.1- サービス層 API 仕様（HTTP 用） 17
2.9　TS-M2M-0010 v1.0.1 - サービス層 API 仕様（MQTT 用） 18
2.10　TS-M2M-0011 v1.2.1 - 共通用語 19
おわりに 20

＜参考＞

１．　国際勧告等との関連

本技術レポートの1.1はoneM2Mで承認されたoneM2M Administrative Document ADM-0008 V1.0.0 - oneM2M Release 1 List of Technical Specifications - 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	2015年3月30日	制定
		改訂 誤記訂正

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1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1の追加や更新がある場合には、適宜、本レポートの改定を行う。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1の構成

1.1　oneM2M リリース 1 の構成と TTC 仕様書との対応

oneM2M リリース1は、oneM2M Administrative Document ADM-0008 V1.0.0 - oneM2M Release 1 List of Technical Specifications – に記載されている版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に示す。

表 1-1　oneM2M リリース1の構成と対応するTTC仕様

	oneM2Mの文書番号とタイトル	TTCの文書番号（版数）とタイトル
1.	TS 0001 - Functional Architecture, [1]	TS-M2M-0001v1.6.1 - 機能アーキテクチャ
2.	TS 0002 - Requirements, [2]	TS-M2M-0002 v1.0.1 - 要求条件
3.	TS 0003 - Security Solutions, [3]	TS-M2M-0003 v1.0.1 - セキュリティ技術の適用
4.	TS 0004 - Service Layer Core Protocol, [4]	TS-M2M-0004 v1.0.1 - サービス層API仕様（共通部）
5.	TS 0005 - Management enablement (OMA), [5]	TS-M2M-0005 v1.0.1 - OMA仕様によるデバイス管理
6.	TS 0006 - Management enablement (BBF), [6]	TS-M2M-0006 v1.0.1 - BBF仕様によるデバイス管理
7.	TS 0008 - CoAP Protocol Binding, [7]	TS-M2M-0008 v1.0.1 - サービス層API仕様（CoAP用）
8.	TS 0009 - HTTP Protocol Binding, [8]	TS-M2M-0009 v1.0.1- サービス層API仕様（HTTP用）
9.	TS 0010 - MQTT Protocol Binding, [9]	TS-M2M-0010 v1.0.1 - サービス層API仕様（MQTT用）
10.	TS 0011 - Common Terminology, [10]	TS-M2M-0011 v1.2.1 - 共通用語

[1] TS 0001 - Functional Architecture, V1.6.1, Jan 2015

[2] TS 0002 - Requirements, V1.0.1, Jan 2015

[3] TS 0003 - Security Solutions, V1.0.1, Jan 2015

[4] TS 0004 - Service Layer Core Protocol, V1.0.1, Jan 2015

[5] TS 0005 - Management enablement (OMA), V1.0.1, Jan 2015

[6] TS 0006 - Management enablement (BBF), V1.0.1, Jan 2015

[7] TS 0008 - CoAP Protocol Binding, V1.0.1, Jan 2015

[8] TS 0009 - HTTP Protocol Binding, V1.0.1, Jan 2015

[9] TS 0010 - MQTT Protocol Binding, V1.0.1, Jan 2015

[10] TS 0011 - Common Terminology, V1.2.1, Jan 2015

1.2　文書間の関係

oneM2M リリース 1 は 10 の技術仕様書(TS)で構成されているが、その開発は Stage 1(要求条件定義)、Stage 2(アーキテクチャ検討-機能セット定義)、Stage 3(プロトコル検討－API 仕様策定)の 3 段階で進められた。

Stage1 は WG1 が活動の中心であったが、Stage 2 以降の活動では WG1 から WG5 までのすべての WG のメンバーが、それぞれの得意分野で協力しあって、主担当となった技術文書のとりまとめを行って Release-1 技術仕様書が完成した。（図 1-1）

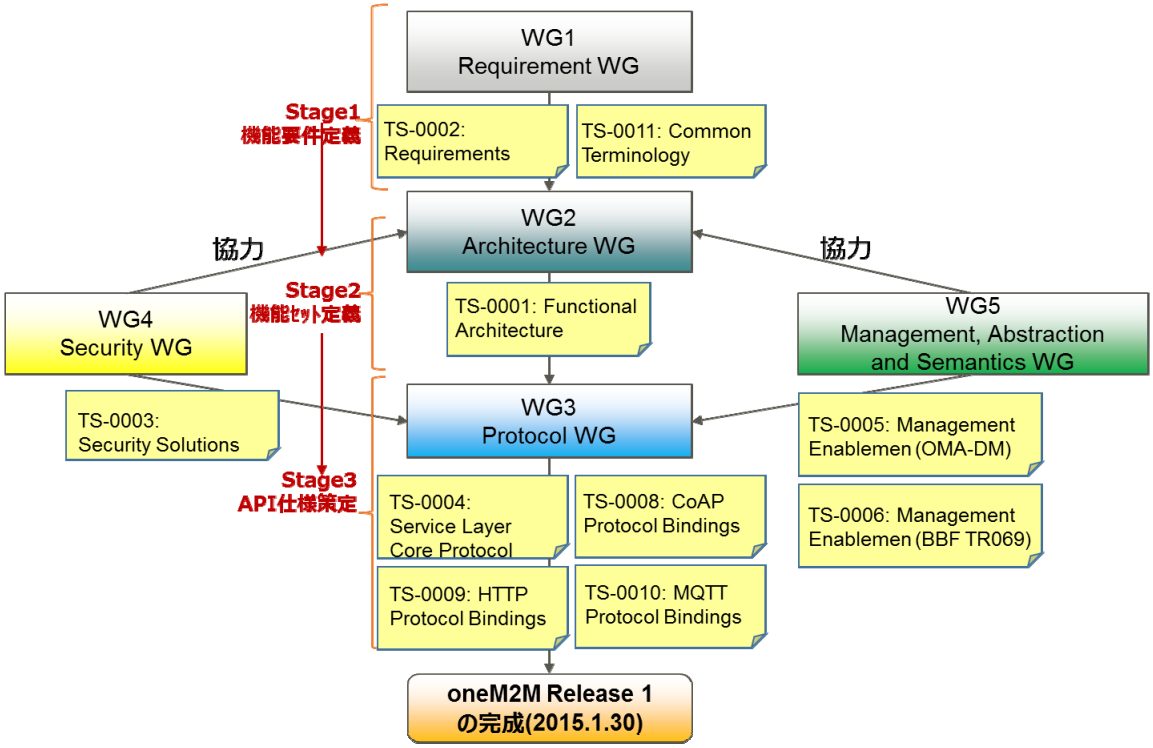

図 1-1　技術仕様書と WG の活動

第2章　oneM2M リリース1の解説

2.1　TS-M2M-0002 v1.0.1 - 要求条件

本文書は、oneM2Mにおける機能要求条件をとりまとめたものである。ユースケース文書（TR-0001）に掲載された33件のユースケースに記載されているPotential Requirementsから要求条件として取りまとめられた144件の項目が下記の通り規定されている。各要求条件では、掲載された項目数とそのうちA:リリース１において標準化された項目数、B:一部標準化された項目数及びC:標準化が行われなかった項目数を再掲した。

表　2-1 要求条件の分類

要求条件	概要	項目数	内訳A	内訳B	内訳C
OSR（システム全般に関する要求条件）	M2Mシステムにおけるアプリケーション、デバイス/ゲートウェイ、ネットワーク等に関する要件	**75**	46	8	21
MGR（管理に関する要求条件）	M2Mゲートウェイ/デバイス管理、M2Mエリアネットワーク関連の要件	**16**	15	1	0
ABR（抽象化に関する要求条件）	M2Mデータの情報モデル化、仮想デバイスに関する要件	**3**	0	0	3
SMR（セマンティック化に関する要求条件）	M2Mデータのセマンティック記述に関する要件	**7**	0	0	7
SER（セキュリティに関する要求条件）	M2Mシステムにおけるセキュリティ要件	**26**	18	7	1
CHG（課金に関する要求条件）	M2Mシステムにおける課金情報の収集や記録、ビリング等に関する要件	**6**	1	1	4
OPR（運用に関する要求条件）	M2Mアプリケーションに対する監視、診断、管理、実行等に関する要件）	**6**	3	0	3
CRPR（通信要求処理に関する要求条件）	M2Mデバイス/M2Mゲートウェイ/インフラ・ドメイン間の通信の設定・処理に関する要件	**5**	4	1	0
NFR（機能要件以外の要求条件）	Continua Health Allianceのサービス支援のための要件等	**2**	2	0	0
合計		**144**	89	18	39

注：内訳A：リリース１で標準化が完了した要求条件の項目数
　　内訳B：リリース１で一部標準化された要求条件の項目数
　　内訳C：リリース１で標準化が行われなかった要求条件の項目数

2.2　TS-M2M-0001v1.6.1 - 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。oneM2Mのアーキテクチャは以下の図2-1に示されているようにアプリケーション・エンティティAE(Application Entity)，共通サービス・エンティティCSE(Common Service Entity)，ネットワークサービス・エンティティNSE(Network Service Entity)で構成されている。このうちCSEがoneM2Mにおける標準化の中心である。これらのエンティティを接続する参照点としてMca、Mcc、Mcc’、Mcnが規定されている。また、AE、CSE、NSEを搭載した機器のことをノードと呼ぶ。フィールド・ドメイン（Field Domain）はM2Mデバイス、M2Mゲートウェイ、センサ・アクチュエータ、M2Mエリアネットワークからなる。インフラストラクチャ・ドメイン（Infrastructure Domain）はアプリケーションインフラストラクチャおよびM2Mサービスインフラストラクチャからなる。Mcc’は、他のサービスプロバイダのインフラストラクチャ・ドメインのCSEとの間の参照点である。

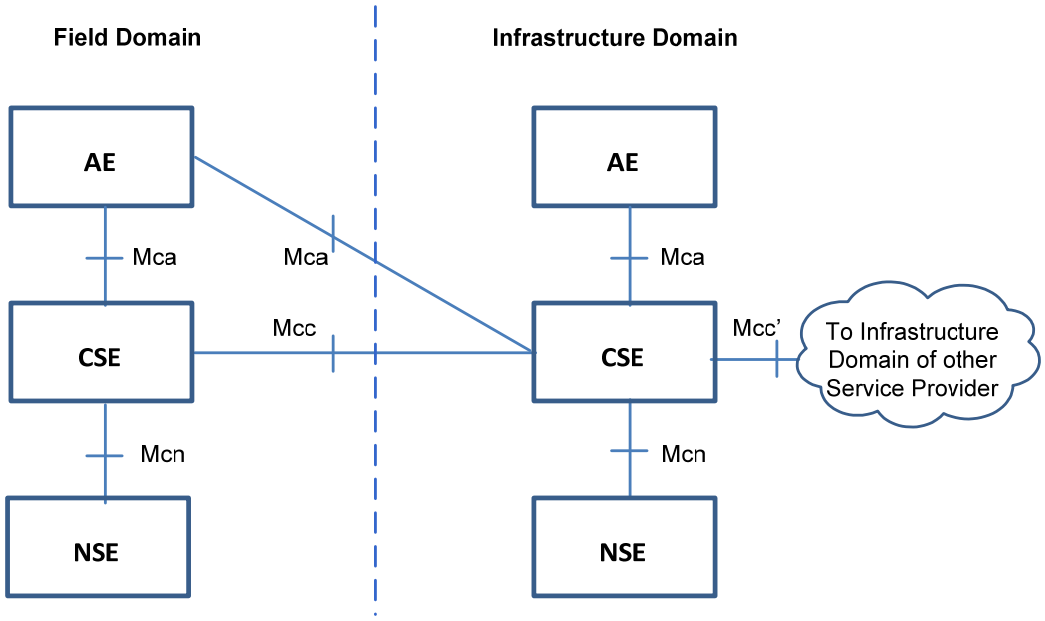

図2-1　oneM2Mの機能アーキテクチャ

CSEの内部には以下の12個の共通サービス機能（CSF, Common Service Functions）が定義されている。

- アプリケーション及びサービス層管理（Application and Service Layer Management）
  AE, CSEを管理する機能。設定、故障対応、アップグレードなど。
- 通信管理／配布管理（Communication Management and Delivery Handling）
  送信タイミングの管理、メッセージのバッファなど
- データ管理及び蓄積（Data Management and Repository）
  データの収集、蓄積、フォーマット変換など
- デバイス管理（Device Management）
  M2Mゲートウェイ、デバイスなどの管理
- 発見（Discovery）
  アプリケーション、サービスの検索
- グループ管理（Group Management）
  グループに関連する要求を取り扱う機能。
- 位置情報（Location）

位置を利用したサービスのための位置情報の管理。

- ネットワークサービス連携（Network Service Exposure, Service Execution and Triggering）
  Mcn参照点を介してネットワークサービス機能にアクセスするためにUnderlying Networkとの通信を管理する機能
- 登録（Registration）
  CSEにAE及び他のCSEを登録する機能
- セキュリティ（Security）
  ID管理、アクセス制御などセキュリティ管理
- サービス課金及び管理（Service Charging and Accounting）
  課金管理を行う機能
- サブスクリプション及び通知（Subscription and Notification）
  メッセージの発行、通知、通知予約を行う機能

また、本書はサービスプロバイダ、AE、CSE、ノードなどに割り当てられるID、参照点における信号のフロー、リソース（Resource）と属性（Attribute）と呼ばれるデータ構造及びデータの操作方法などについても記述されている。

2.3 TS-M2M-0003 v1.0.1 - 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。図 2-2 にハイレベルセキュリティアーキテクチャを示す。

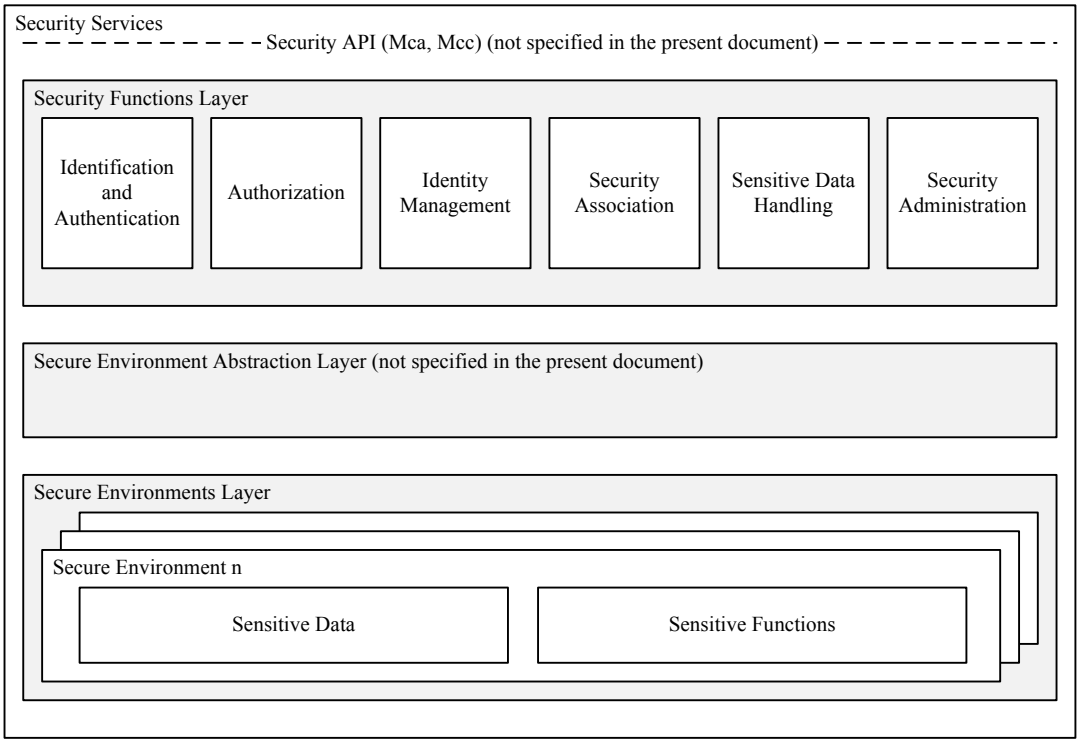

図2-2 ハイレベルセキュリティアーキテクチャ

本文書では、M2M システムを展開する上で重要となる以下のソリューションについて主に取り扱う。

① リモートセキュリティプロビジョニング： M2M サービスを使用するにあたり、フィールドドメイン

のエンティティと M2M サービスプロバイダの持つ M2M 認証機能のセキュリティアソシエーションを確立するため、最低限必要な情報（セキュリティクレデンシャル、識別子など）を事前に提供する必要がある。このために以下の３種類のリモートセキュリティプロビジョニングフレームワーク（RSPF）がサポートされている。

(ア) Provisioned Symmetric Enrollee Key RSPF

(イ) Certificate-based RSPF

(ウ) GBA-based RSPF

② セキュリティアソシエーション： M2M サービスは CSE によって、AE や他の CSE へ提供されるが、不正アクセスから保護するため、エンティティ相互に識別および認証されなければならない。この相互認証によって、Mca や Mcc 参照点におけるメッセージを保護するための暗号化およびインテグリティを提供することが可能になる。本文書では多種多様な M2M の展開シナリオへ対応するため、３種類のセキュリティアソシエーション確立フレームワーク（SAEF）がサポートされている。

(ア) Provisioned Symmetric Key SAEF

(イ) Certificate-based SAEF

(ウ) M2M Authentication Function-based SAEF

③ アクセス制御： アクセスを許容されているエンティティのみが、リソースへアクセスできる状態を確保する必要がある。本文書ではアクセスコントロールポリシーによるアクセス制御メカニズムを規定している。

2.4 TS-M2M-0004 v1.0.1 - 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/Retrive/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-v1_0_0.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。

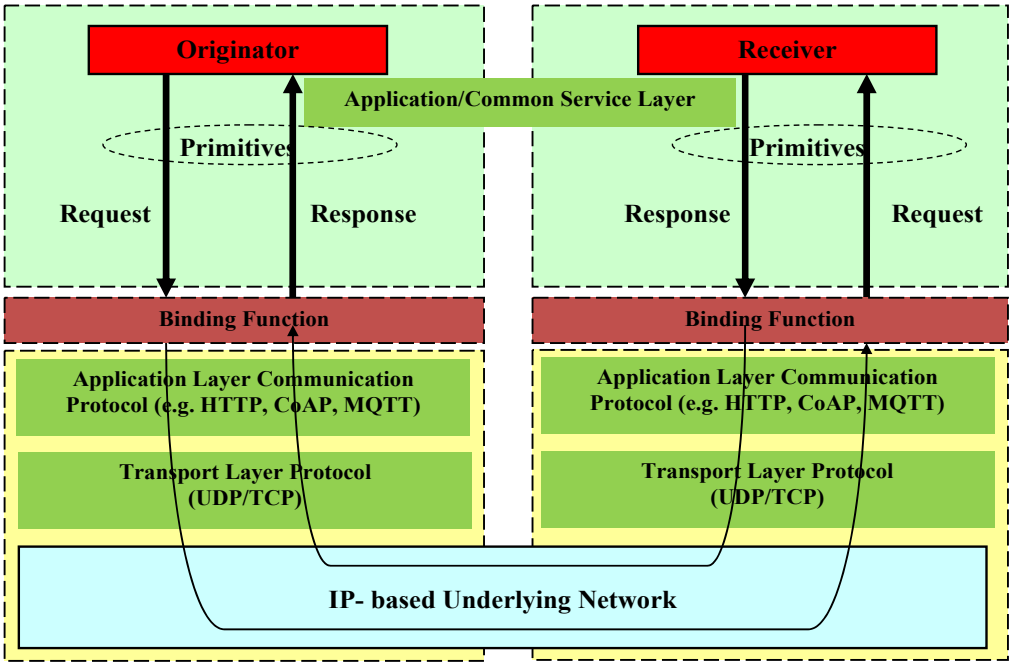

図 2-3　Request/Response プリミティブ通信のマッピング例

2.5　TS-M2M-0005 v1.0.1 - 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2-4である。図2-1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）。

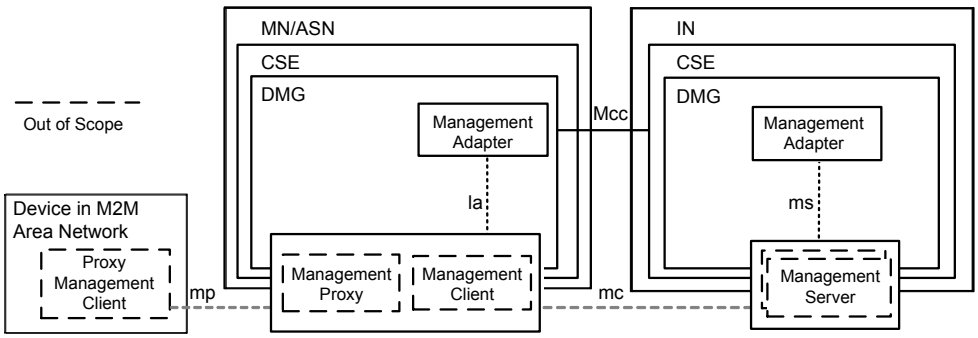

図 2-4　デバイス管理アーキテクチャ

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）
  - 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。）

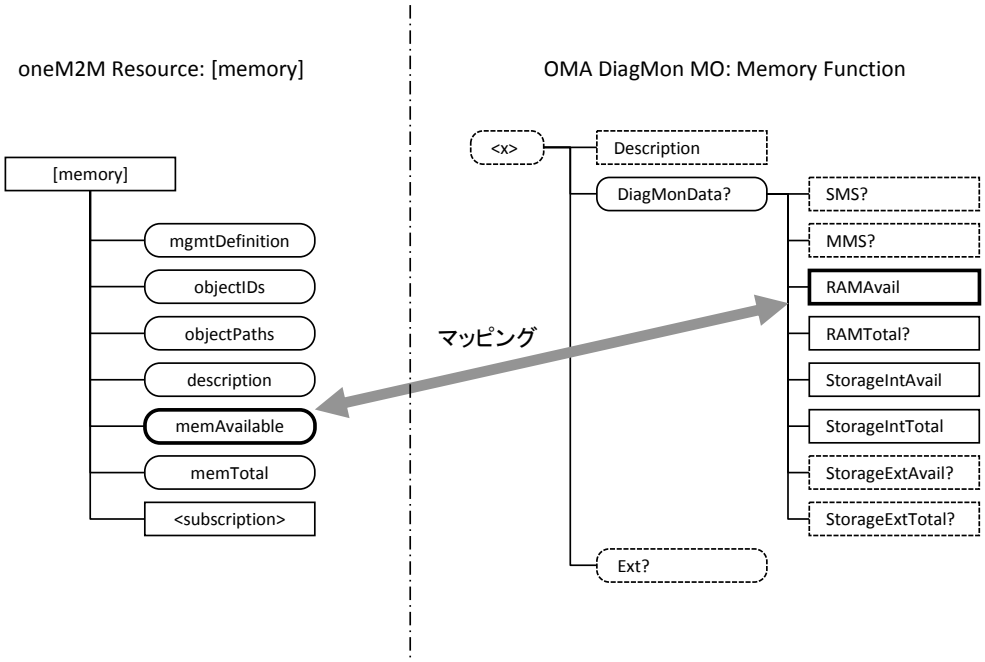

図2-5　oneM2MリソースとOMA DM MOとの対応関係（例）

2.6　TS-M2M-0006 v1.0.1 - 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、以下の内容を規定している。

- 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
- oneM2M におけるマネジメント・リソース<mgmtObj>と、BBF TR-181 デバイスデータモデルとの対応関係
- 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
- 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TR-181データモデルの内容
  （cmdhPolicyに関しては既存のTR-181データモデルに対応するものがないため、新たに定義する。具体的にはts-0006-1-1-0.xmlを参照。）

2.7　TS-M2M-0008 v1.0.1 - 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プリミティブと CoAPメッセージとの対応
- oneM2Mレスポンスステータスコードと CoAPレスポンスコードとの対応
- oneM2Mのパラメータに対応したCoAPのクライアントとサーバの動作の定義

2.7.1 概要

oneM2Mに対応するためにCoAPでサポートすべき機能を明記し、プロトコル対応で使われるメッセージフォーマットなど、CoAPの機能を紹介している。

2.7.2 CoAPメッセージマッピング

AEまたはCSEがoneM2Mプリミティブを CoAPメッセージに、または CoAPメッセージを oneM2Mプリミティブに対応させるときは、下記のどちらかが要求される。

- AEが CoAP クライアントの能力を持ち、CoAP サーバ能力も提供するか、
- CSEが CoAP クライアントとサーバ両方の能力を持つ

基本的に一つのoneM2Mリクエストプリミティブは一つの CoAPリクエストメッセージに、一つのoneM2Mレスポンスプリミティブは一つの CoAPレスポンスメッセージにマッピングされる。図2-6にAE登録手順の CoAPマッピングの例を示す。

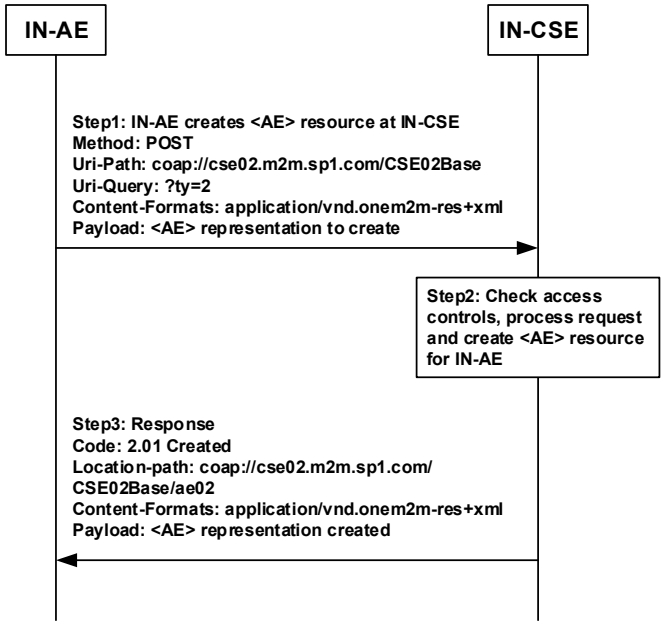

図2-6 対応の例－AE登録

oneM2Mパラメータのプリミティブが CoAPメッセージのどこにマッピングされるか、レスポンスタイプ別(Blocking、Non-Blocking非同期、Non-Blocking同期)の CoAPの動作、キャッシングのマッピング規則、ブロック転送の使用について規定している。

2.7.3 セキュリティ面の配慮

セキュリティ面から配慮すべき項目について記述している。

2.8　TS-M2M-0009 v1.0.1- 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

2.8.1 概要

oneM2Mのプリミティブパラメータは 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。AEはHTTPクライアントの能力を，CSEはHTTPクライアントとサーバ両方の能力を持つと仮定している。マッピングの例を図2-7に示す。

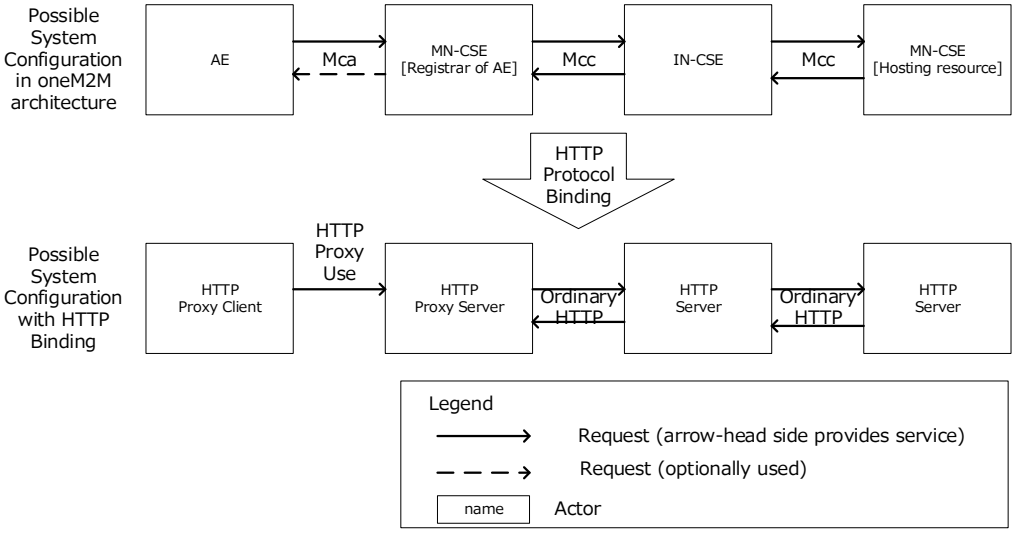

図2-7 AE/CSEとHTTPクライアント／サーバのマッピング例

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。

2.8.2 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。

2.8.3 セキュリティ面での配慮

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。

2.9　TS-M2M-0010 v1.0.1 - 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

2.9.1 プロトコル対応

図2-8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。

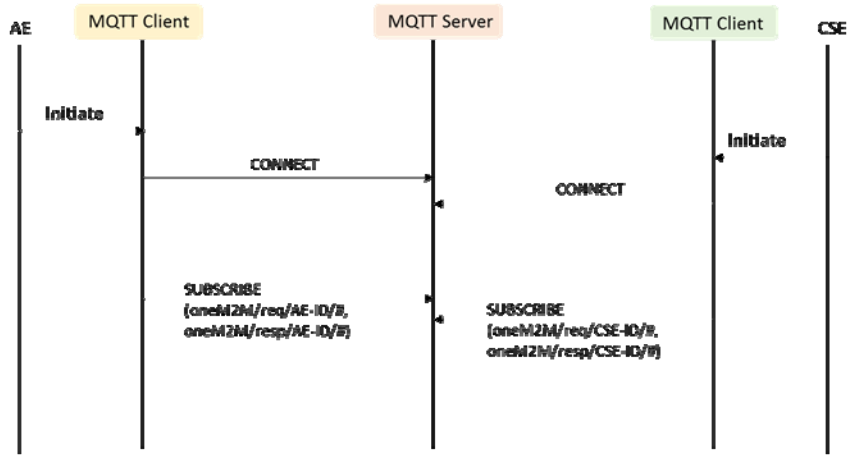

図2-8　MQTT対応での起動手順

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2-9に示す。

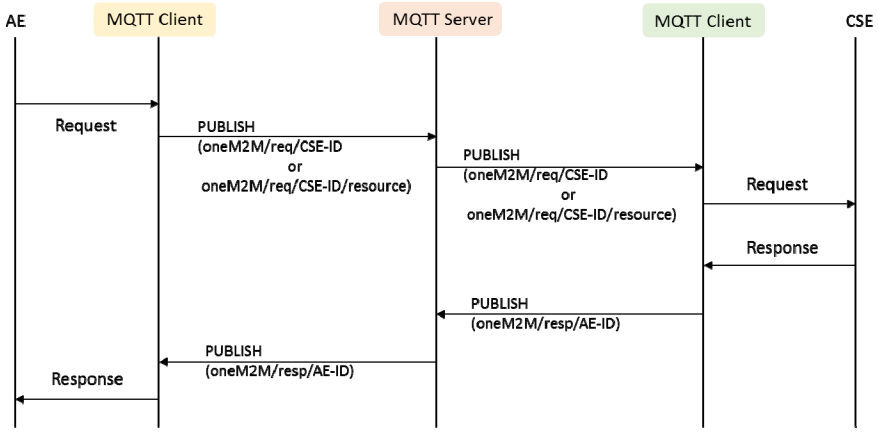

図2-9　MQTTによるリクエスト／レスポンスメッセージ送受信

2.9.2 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。

2.10　TS-M2M-0011 v1.2.1 - 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。

おわりに

2015年1月に発行された10件の技術仕様書（リリース１）は、oneM2Mから初めてリリースされた技術仕様書であり、oneM2Mシステムを展開するのに、必要最低限の技術が盛り込まれていると謳われている。しかし、2.1に示した通り、要求条件のいくつかについては、機能アーキテクチャ仕様書(TS-0001)やその他の仕様書に反映されていない項目が多数残されているのが現状である。

次期リリースは、現時点では、2015年1月から2016年5月までを作業目標期間とされており、リリース１に積み残した要求条件や新たな機能要求が追加されることが見込まれている。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-0011 - Service Component Architecture
WI-0015 - oneM2M Use Case Continuation
WI-0016 - End-to-End Security and Group Authentication
WI-0017 - Home Domain Enablement
WI-0018 - oneM2M and AllJoyn Interworking
WI-0019 - Dynamic Authorization for IoT
WI-0020 - Service Layer API
WI-0021 - Secure Environment Abstraction
WI-0022 - Interoperability Testing
WI-0023 - Authorization Architecture and Access Control Policy
WI-0024 - LWM2M Interworking
WI-0025 - Generic Interworking
WI-0026 - Efficient Communications
WI-0027 - Testing Framework
WI-0028 - Industrial Domain Enablement

これらの作業項目等から、優先順位付け等により次期リリースの内容が決定されていることになっている。