TR-M2M-0012v2.0.0

oneM2M 技術レポート －エンド・エンド セキュリティとグループ認証－

oneM2M Technical Report －oneM2M End-to-End Security and Group Authentication－

サマリ（和文）：

アブストラクト：

本文書は、エンド・エンド セキュリティとグループ認証に関する技術報告書である。

目次：　章立てを記載

１章　所掌範囲（目的）

本文書は、エンド・エンド セキュリティとグループ認証を実現する際に必要なセキュリティの特徴やメカニズムについて、分析および取りうる選択肢について説明したものである。

２章　引用文献

３章　定義、略語と頭字語

４章　表記法

５章　ユースケース

エンド・エンド セキュリティおよびグループ認証を適用すべきユースケースが記載されている。

６章　候補アーキテクチャ

静的なグループ認証の候補となるアーキテクチャの説明。エンド・エンド セキュリティのフレームワークの説明。

７章　利用可能な選択肢

エンド・エンド セキュリティとグループ認証を実現するために、実現可能なアーキテクチャについて記述されている。また、オブジェクトベースのセキュリティや暗号方式などのセキュリティに関する技術的な選択肢に対して、機密性、完全性、否認防止などのセキュリティ要件から、利用すべき組み合わせについて記述されている。

８章　Release2 におけるエンド・エンド セキュリティと論理的理由

Release2 におけるエンド・エンド セキュリティは、以下の 4 つで構成されている。

- エンド・エンドのデータのセキュリティ
- エンド・エンドのプリミティブのセキュリティ
- 証明書ベースの鍵交換
- MAF（M2M 認証機能）を用いたフレームワーク

付則 A（情報）エンド・エンドのデータのセキュリティの必要性

エンド・エンドのデータのセキュリティの必要性を２つの例を用いて記述されている。中継点に悪意のある CSE がある場合は、エンド・エンドでデータを保護しないとセキュリティリスクが生じる。

付則 B（情報）遠隔検証のユースケース

遠隔検証のユースケースにおいて、oneM2m の技術仕様に必要な要件について整理されている

サマリ（英文）：

Abstract:

Technical Report of oneM2M End to End Security and Group Authentication

Scope:

The present document provides options and analyses for the security features and mechanisms providing end-to-end security and group authentication for oneM2M.

The scope of this technical report includes use cases, threat analyses, high level architecture, generic requirements, available options, evaluation of options, and detailed procedures for executing end-to-end security and group authentication.