2F-02

SSDTF（IoT 向け安心・安全データ転送フレームワーク）およびMQTT における実現方式の提案・考察

才所 敏明†‡　　辻井 重男†

Toshiaki Saisho　Shigeo Tsujii

1.はじめに

SSDTF（Secure and Safe Data Transfer Framework）は、総務省の重点領域型研究開発推進事業（SCOPE）にて委託された「IoT デバイス認証基盤の構築と新 AI 手法による表情認識の医療介護への応用についての研究開発」（以下、IoTAI-PJ と略記）の一環として研究を進めている IoT 向けの安心・安全なデータ転送フレームワークである。データ転送時の送信デバイス/データの真正性保証を OSI のアプリケーション層での実現を目指している。筆者らが別途推進中の研究“安心・安全電子メール利用基盤 SSMAX”（[3]）の成果であるメール送信者及び送信メールの真正性保証の仕組みを IoT システムへ適用することにより SSDTF の実現を目指す予定である。

2.研究対象 IoT システムモデル

本研究ではデータ収集 IoT サービスモデルを対象とし、IoT システムを構成するデバイス間のネットワークはすべてインターネットプロトコルを使用しているものとしている（図 1）

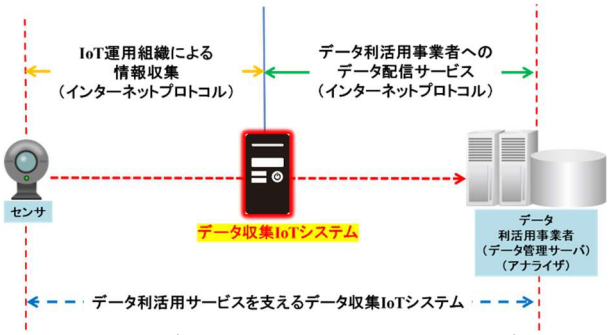

図 1　データ収集 IoT サービスモデル

また、データ収集 IoT システムは、センサ/ゲートウェイ/アグリゲータの 3 層から構成されているものとする（図 2）。データ収集 IoT サービスモデルを対象とするネットワーク層の研究は、図 2 に示すデータ収集 IoT システムを構成するデバイスおよびデバイス間の通信を対象とし、送信デバイス・データの真正性確保を可能とする仕組み、SSDTF（Secure and Safe Data Transfer Framework）、の提案を目標としている。

Proposal of SSDTF（Secure and Safe Data Transfer Framework） and it's realization method in MQTT

†セキュア IoT プラットフォーム協議会
Secure IoT Platform Consortium
‡ Mail:toshiaki.saisho@advanced-it.co.jp

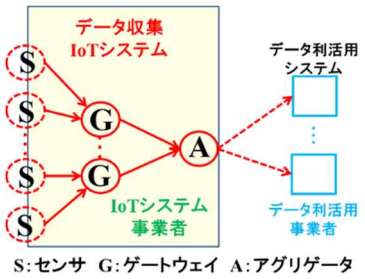

図 2　データ収集 IoT システム構成(SGA)モデル
（赤色表示部分が研究対象範囲）

3．SSDTF 概要

SSDTF では、IoTAI-PJ にて期待される送信デバイス/データの真正性保証を含む以下の機能を実現する仕組みの提案を目指している。

①送受信デバイスの真正性確認
　送信デバイスに加え、受信デバイスも認証
②送信データの真正性確認
　送信データの非改ざん性の確認
③送信データの秘匿
　送信データの漏洩防止
④送信デバイスの匿名性と特定・追跡性の両立
　送信デバイスの IoT システム外に対する匿名性維持と、送信データの不具合時の送信デバイスの特定。追跡性の確保

4.SSDTF/MQTT

SSDTF/MQTT は、SSDTF の機能・仕組みを代表的な IoT 向けデータ転送プロトコルである MQTT の仕様の範囲で実現する MQTT である。

4．1　MQTT アーキテクチャと SGA モデル

図 3 に、MQTT の基本的アーキテクチャ、および、この MQTT アーキテクチャと本研究で想定している IoT システム構成（SGA）モデルとの対応を示している。

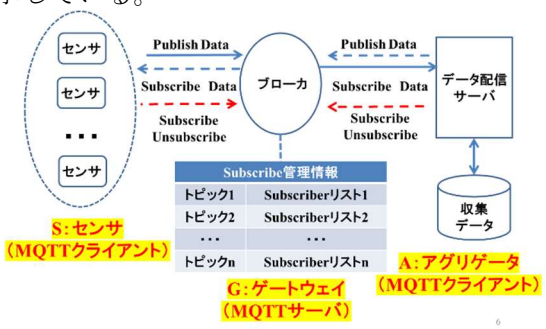

図 3　MQTT アーキテクチャと SGA モデルの対応

4．2　SSDTF/MQTT アーキテクチャ

SSDTF/MQTT では、MQTT にシステム管理サーバを加えた構成を想定している（図 4）。システム管理サーバは、データ収集にかかわる運用処理は担当せず、システム全体の管理情報の維持・更新の担当を想定している。

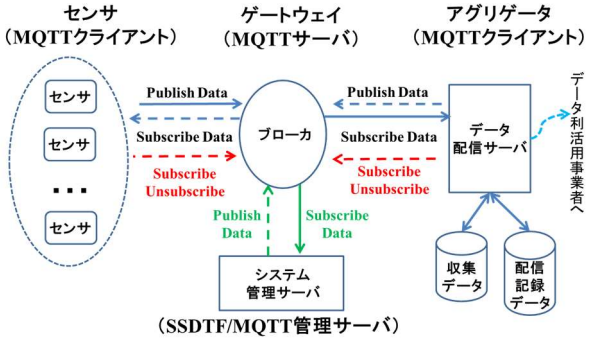

図 4　SSDTF/MQTT アーキテクチャ

4．3「送受信デバイスの真正性確認」実現方式

クライアント（センサ、データ管理サーバ等）	パケット	サーバ（ブローカ）
（1）User Nameフラグ、Passwordフラグの指定 （2）クライアントIDの指定 （3）User Nameの代わりに生成した乱数を指定	CONNECT ーー>	クライアントIDの確認
	CONNACT <ーー	
（1）サーバ（ブローカ）の署名の確認	PUBLISH <ーー	User Nameとして指定された乱数文字列および新たに生成した乱数文字列を送信データとし、PUBLISHパケットへ署名を付加
確認結果 ×	サーバ（ブローカ）との接続をクローズ	DISCONNECT ーー>	
確認結果 ○	新たな乱数文字列を送信データとし、PUBLISHパケットへ署名を付加	PUBLISH ーー>	クライアント（センサ）の署名確認
		クライアント（センサ）との接続をクローズ × 確認結果
		通信開始 ○ 確認結果

図 5　SSDTF/MQTT の送受信デバイス認証機能

4．4「送信データの真正性確認」および「送信データの秘匿」の実現方式

サーバ（ブローカ）	メッセージ	クライアント（データ配信サーバ）
（1）メッセージ・トピックのサブスクライバへ受信データを送信 ①暗号化されている受信データは、各サブスクライバへの変換鍵を使用し、各サブスクライバ向け暗号化データへ変更 ②固定ヘッダ、可変ヘッダ、暗号化された送信データ、クライアントID全体への署名を作成し、ペイロードの最後に署名を添付	PUBLISH ーー>	ペイロード内の署名を確認
PUBLISHパケットの再送または 管理サーバへ通達	PUBLISH <ーー	確認結果 × 署名エラーおよび再送が必要なことを連絡
		確認結果 ○ 送信データに対応する処理を実行＜別途定義＞

図 6　SSDTF/MQTT の送信データの真正性確認および秘匿（クライアント-サーバ間）

サーバ（ブローカ）	メッセージ	クライアント（データ配信サーバ）
（1）メッセージ・トピックのサブスクライバへ受信データを送信 ①暗号化されている受信データは、各サブスクライバへの変換鍵を使用し、各サブスクライバ向け暗号化データへ変更 ②固定ヘッダ、可変ヘッダ、暗号化された送信データ、クライアントID全体への署名を作成し、ペイロードの最後に署名を添付	PUBLISH ーー>	ペイロード内の署名を確認
PUBLISHパケットの再送または 管理サーバへ通達	PUBLISH <ーー	確認結果 × 署名エラーおよび再送が必要なことを連絡
		確認結果 ○ 送信データに対応する処理を実行＜別途定義＞

図 7　SSDTF/MQTT の送信データ真正性確認および秘匿（サーバ-クライアント間）

4．5「送信デバイスの匿名性と特定・追跡性の両立」実現方式

SSDTS/MQTT では、データ利活用事業者への契約ベースのデータ配信を担当するデータ配信サーバを MQTT のクライアントの一つとして運用することを想定している。

配信サーバでは、送信デバイス（ブローカ）/データの真正性確認の後、配信サーバ向けに暗号化されている送信データを個々のデータ利活用業者向けに暗号化された送信データに変換、クライアント ID を内部識別符号から外部識別符号に置き換え、全体に対する配信サーバの署名を付与し、データ利活用事業者へ送信することを想定している。

謝辞

本研究は，総務省「戦略的情報通信研究開発推進事業 SCOPE（受付番号：181603006）」にて、セキュア IoT プラットフォーム協議会及び中央大学のチームが採択を受けた「IoT デバイス認証基盤の構築と新 AI 手法による表情認識の医療介護への応用についての研究開発」の活動の一環として行ったものである。

参考文献

[1] 才所敏明，辻井重男，” IoT システムにおける送信デバイス・データの真正性確保に関する考察”，FIT2019（2019）.
[2] 才所敏明，辻井重男，”安心・安全な IoT システム(SSIoT)に関する考察”，CSEC81（2018）.
[3] 才所敏明，五太子政史，辻井重男，”「安心・安全電子メール利用基盤（SSMAX）」，情報処理学会論文誌 59 巻 9 月号(2018).
[4] 才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男，”組織暗号の構成と社会的実装－個人情報の安全な利活用を目指して－”，情報処理学会誌論文誌 56 巻 9 月号(2016)