

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

2020年3月5日

才所敏明* 辻井重男†
セキュアIoTプラットフォーム協議会

*（株）IT企画 †中央大学研究開発機構

説明項目

1.

総務省・SCOPE対応PJ（IoTAI-PJ）および担当課題概要

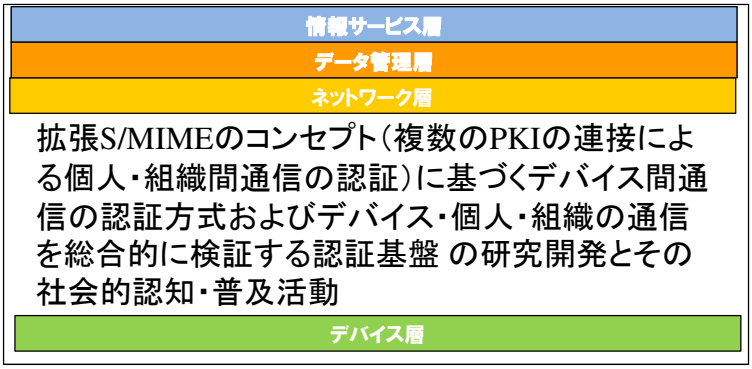
IoTデバイス認証基盤の構築と新AI手法による表情認識の医療介護への応用（IoTAI-PJ）（SCOPE：2018～2020）

本研究は、IoT・Big-Data・AIを支える情報セキュリティ基盤の構築を目指し、電子認証(真正性確認)を軸とした4階層（デバイス層、ネットワーク層、データ管理層、情報サービス層）に対し研究開発／ビジネスモデル構築／社会的普及／ガイドライン・標準化の作成を図る。

また情報サービス層における応用として、要介護者・患者などの医療介護現場に対し、電子認証によりセキュリティを担保したうえでの、リーマン幾何学を用いたAI技術による表情認識システムを確立することを目的とする。

 5

4階層から成る本PJの ネットワーク層の研究目的

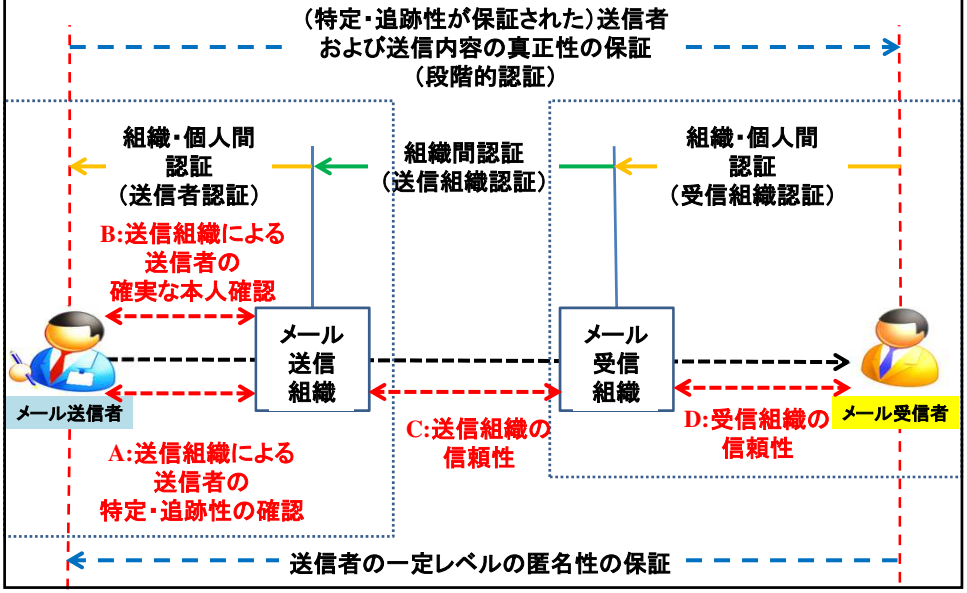


ネットワーク層の目標

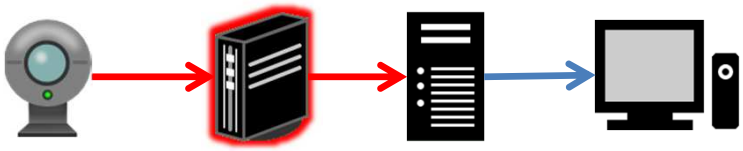
IoTシステムにおける送信機器・送信内容の真正性確保のために、
拡張S/MIMEのコンセプトに基づくIoTシステム向けの認証方式の提案
およびその普及方策の策定を目標とする。

 6

拡張S/MIME（SSMAX）における 送信者・送信内容の認証（真正性保証）方式



SCOPE研究開発課題の全体像と「ネットワーク層」の位置付け



センサ

真正性確認が可能な機器（センサ）によるデータ収集（デバイス層）

データ収集システム

送信機器/送信内容の真正性確認が可能な通信システム（ネットワーク層）

データ管理サーバ

収集データの真正性確認、安全な管理・処理方式（データ管理層）

アナライザ

使用データの真正性確認、応用分野ごとの分析サービス（情報サービス層）

＜理論・方式研究＞ ＜理論・方式研究＞

＜プロトタイプ実装＞ ＜プロトタイプ実装＞

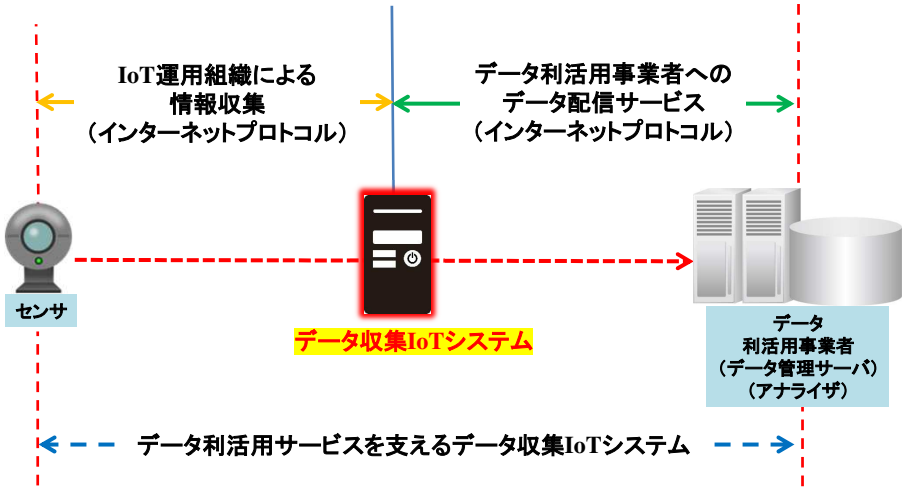
実証実験

5分

2.

検討対象IoTシステム・サービスおよびSSDTF構想

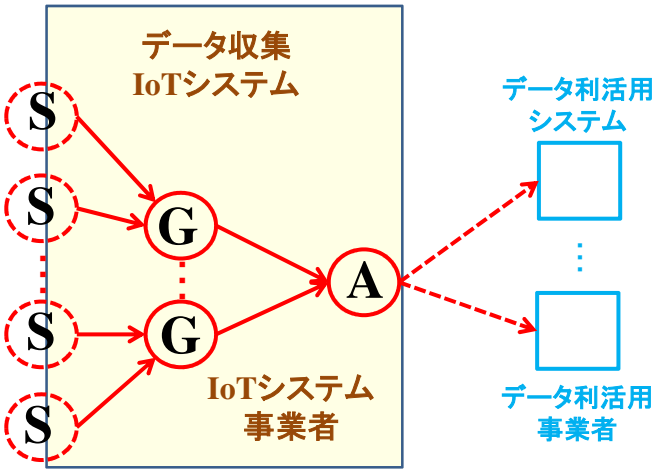
データ収集IoTサービスモデル/システム



「ネットワーク層」の対象範囲

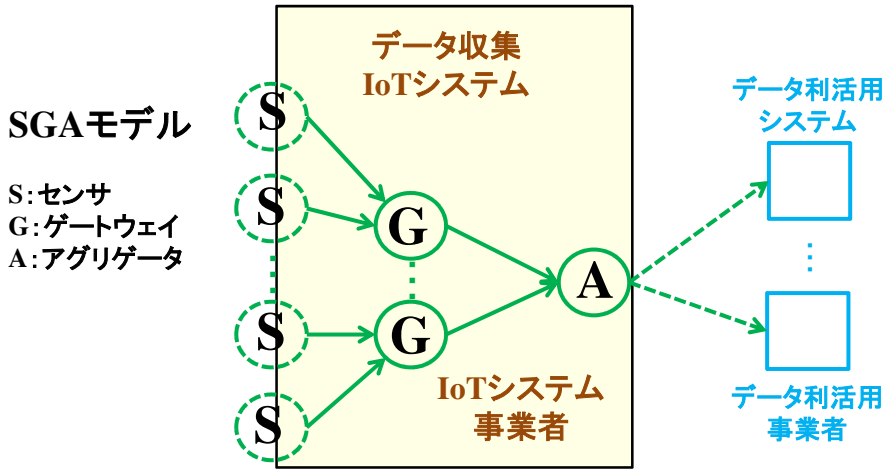
SGAモデル

S：センサ
G：ゲートウェイ
A：アグリゲータ



➔IoT向けの安心・安全なデータ転送フレームワーク
SSDTF（Secure and Safe Data Transfer Framework）

データ収集IoTシステムにおける ネットワーク層研究の目標



➔SSMAXのコンセプトに基づき、OSIのアプリケーション層上での SSDTF（Secure and Safe Data Transfer Framework）構想策定

SSDTF構想で実現を目指す機能

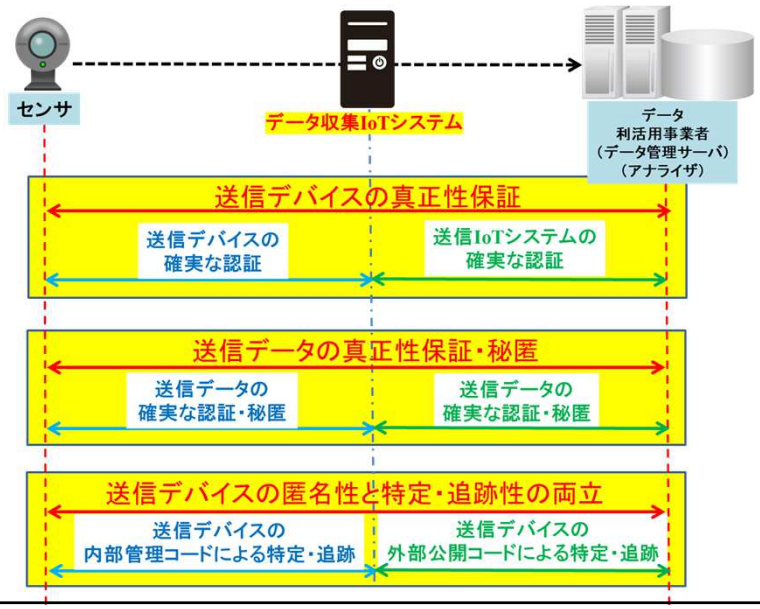
（1）送信デバイスの真正性保証

（2）送信データの真正性保証

（3）送信データの秘匿

（4）送信デバイスの匿名性（秘匿）および特定・追跡性の両立

SSDTF構想で実現を目指す機能

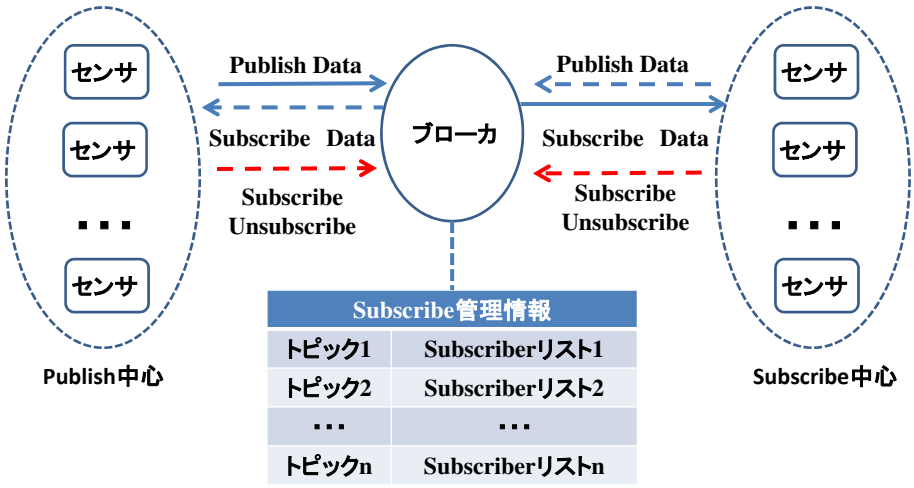


10分

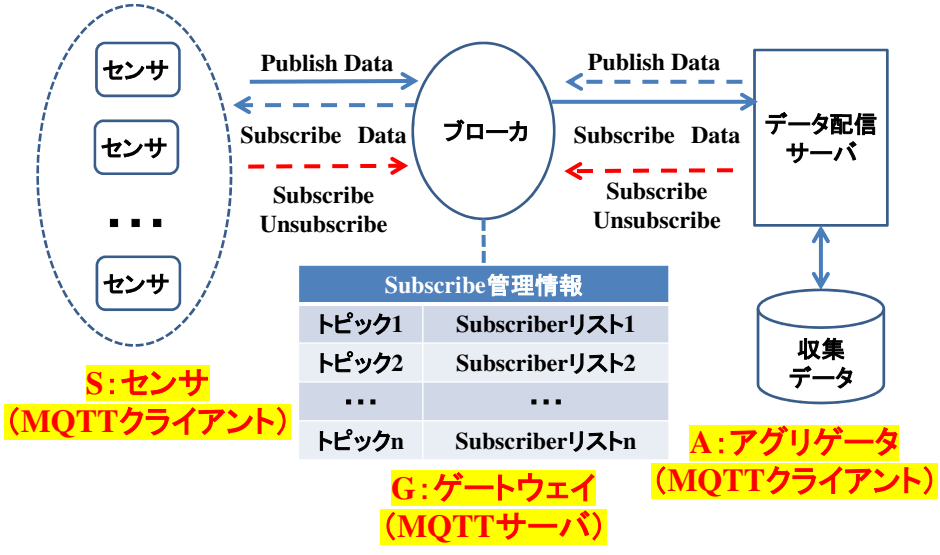
3.

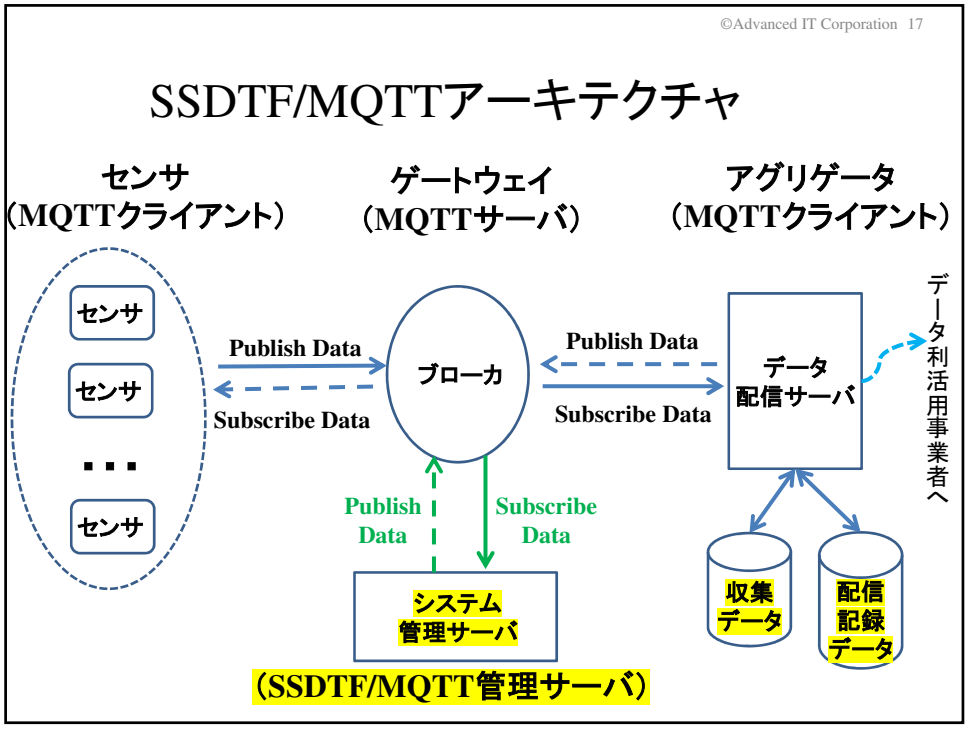
SSDTFの
MQTT上での実現方式

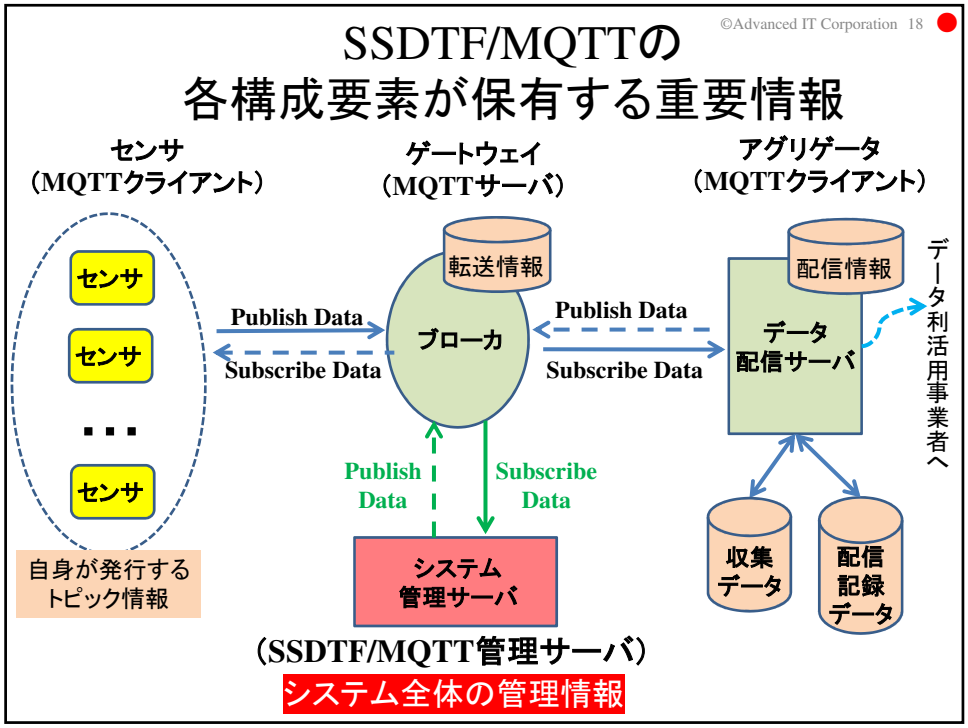
SSDTF適用検討対象MQTTのアーキテクチャ



MQTTアーキテクチャとSGAモデルの対応付け



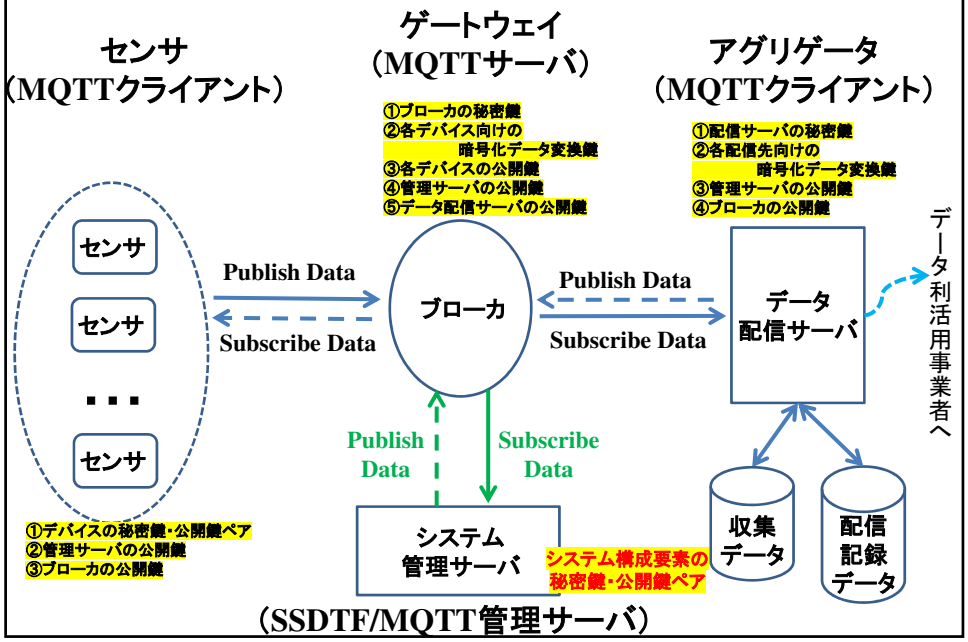

©Advanced IT Corporation 17
SSDTF/MQTTアーキテクチャ
センサ
（MQTTクライアント）
ゲートウェイ
（MQTTサーバ）
アグリゲータ
（MQTTクライアント）
センサ
センサ
センサ
Publish Data
Subscribe Data
ブローカ
Publish Data
Subscribe Data
データ
配信サーバ
データ利活用事業者へ
Publish
Data
Subscribe
Data
システム
管理サーバ
収集
データ
配信
記録
データ
（SSDTF/MQTT管理サーバ）


©Advanced IT Corporation 18
SSDTF/MQTTの
各構成要素が保有する重要情報
センサ
（MQTTクライアント）
ゲートウェイ
（MQTTサーバ）
アグリゲータ
（MQTTクライアント）
センサ
センサ
センサ
自身が発行する
トピック情報
転送情報
Publish Data
Subscribe Data
ブローカ
Publish Data
Subscribe Data
配信情報
データ
配信サーバ
データ利活用事業者へ
Publish
Data
Subscribe
Data
システム
管理サーバ
収集
データ
配信
記録
データ
（SSDTF/MQTT管理サーバ）
システム全体の管理情報

SSDTF/MQTTにおいて実現できる セキュリティ機能

(1)送信デバイスの真正性保証
　公開鍵暗号、チャレンジ/レスポンス方式による
　　送信デバイスの真正性保証
　　受信デバイスの真正性保証
(2)送信データの真正性保証
　公開鍵暗号を利用した送信データへの署名付与・検証による
　　送信データの真正性保証（非改ざん性保証）
　　送信デバイスの真正性保証
(3)送信データの秘匿
　公開鍵暗号を利用した送信データの暗号化による漏洩防止（秘匿）
　送信デバイスは暗号化に管理サーバの公開鍵の利用、
　ブローカおよび配信サーバによる受信デバイス向けに暗号化鍵の付け替えにより
　　ブローカおよび配信サーバでのデータ漏洩リスクの低減
　　第三者入手よるデータ入手は困難
　　配信先/受信デバイス向けに想定外のデータ配信リスクは残存
(4)送信デバイスの匿名性と特定・追跡性の両立
　配信サーバでの送信デバイスの内部IDの外部IDへの変換による匿名性保証
　配信サーバでの内部ID/外部ID対応表の管理による特定・追跡性保証

各構成要素が保有する鍵情報（例）



4.

SSDTF/MQTTの基本通信手順

送受信デバイス認証
パケットフロー（クライアント←→ブローカ）

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 −−>	クライアントIDの確認			
				CONNACT <−−				
（1）サーバ（ブローカ）の署名の確認				PUBLISH <−−	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	DIS CONNECT −−>				
		○	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 −−>	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	○		

送信データ認証＋送信データ秘匿 パケットフロー（クライアント➔ブローカ）

クライアント（センサ）	パケット	サーバ（ブローカ）		
（1）PUBLISHパケットをサーバ（ブローカ）へ送信 ①送信データを サーバ（ブローカ）の公開鍵により暗号化 ②固定ヘッダ、可変ヘッダ、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 （2）送信データを一時的に保存 （受信確認後に破棄）	PUBLISH －－＞	ペイロード内の署名を確認		
PUBLISHパケットの再送 または 管理サーバへ通報	PUBLISH ＜－－	確認結果	どちらか× 両方とも○	署名エラーまたはメッセージエラーであることを連絡 送信データに対応する処理を実行＜別途定義＞

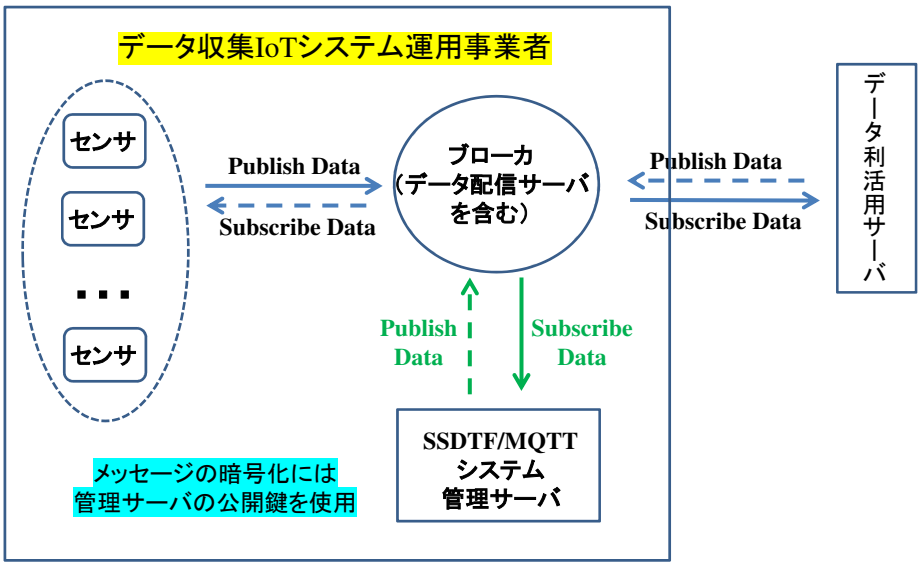
送信データ認証＋送信データ秘匿 パケットフロー（ブローカ➔クライエント）

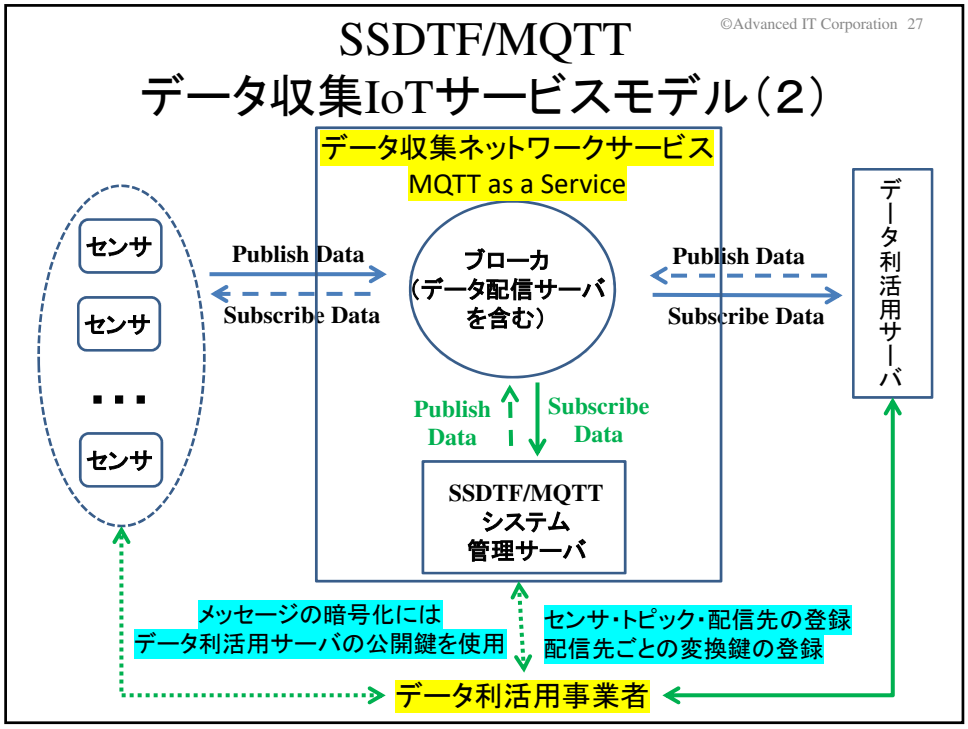
サーバ（ブローカ）	メッセージ	クライアント（データ配信サーバ）		
（1）メッセージ・トピックのサブスクライバへ 受信データを送信 ①暗号化されている受信データは、 各サブスクライバへの変換鍵を使用し、 各サブスクライバ向け暗号化データへ変更 ②固定ヘッダ、可変ヘッダ、 暗号化された送信データ、 クライアントID全体への署名を作成し、 ペイロードの最後に署名を添付	PUBLISH －－＞	ペイロード内の署名を確認		
PUBLISHパケットの再送 または 管理サーバへ通報	PUBLISH ＜－－	確認結果	× ○	署名エラーおよび再送が必要なことを連絡 送信データに 対応する処理を実行 ＜別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

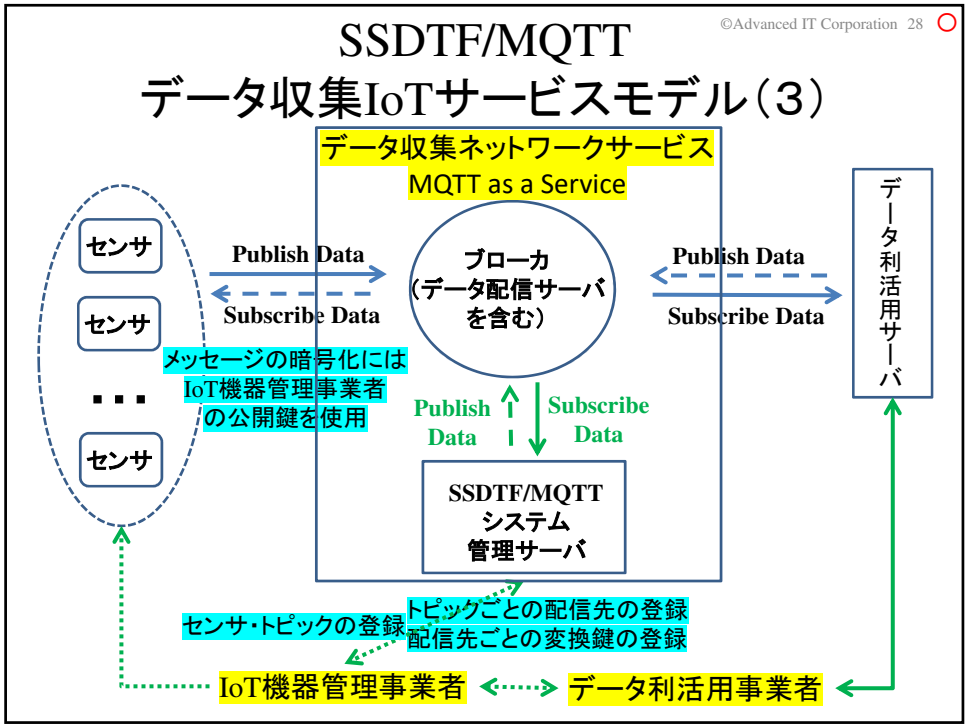
5.

SSDTF/MQTTの各種データ収集IoTサービスモデルに対する適用可能性

SSDTF/MQTT データ収集IoTサービスモデル（1）




SSDTF/MQTT
データ収集IoTサービスモデル（2）
©Advanced IT Corporation 27
データ収集ネットワークサービス
MQTT as a Service
センサ
センサ
センサ
Publish Data
Subscribe Data
ブローカ
（データ配信サーバ
を含む）
Publish Data
Subscribe Data
データ利活用サーバ
Publish Data
Subscribe Data
SSDTF/MQTT
システム
管理サーバ
メッセージの暗号化には
データ利活用サーバの公開鍵を使用
センサ・トピック・配信先の登録
配信先ごとの変換鍵の登録
データ利活用事業者


SSDTF/MQTT
データ収集IoTサービスモデル（3）
©Advanced IT Corporation 28
データ収集ネットワークサービス
MQTT as a Service
センサ
センサ
センサ
Publish Data
Subscribe Data
ブローカ
（データ配信サーバ
を含む）
Publish Data
Subscribe Data
データ利活用サーバ
メッセージの暗号化には
IoT機器管理事業者
の公開鍵を使用
Publish Data
Subscribe Data
SSDTF/MQTT
システム
管理サーバ
センサ・トピックの登録
トピックごとの配信先の登録
配信先ごとの変換鍵の登録
IoT機器管理事業者
データ利活用事業者

6.

類似する研究の概要と SSDTF/MQTTとの関係

調査した類似研究論文一覧

①Secure MQTT for Internet of Things (IoT)

https://ieeexplore.ieee.org/document/7280018

②HOW TO AUTHENTICATE MQTT SESSIONS WITHOUT CHANNEL- AND BROKER SECURITY

https://arxiv.org/pdf/1904.00389.pdf

③Securing MQTT protocol in IoT by payload Encryption Technique & Digital Signature

https://www.researchgate.net/publication/335328286_Securing_MQTT_protocol_in_IoT_by_payload_Encryption_Technique_Digital_Signature

④LIGHTWEIGHT SECURE SCHEME FOR IOT-CLOUD CONVERGENCE BASED ON ELLIPTIC CURVE

http://www.jatit.org/volumes/Vol97No1/13Vol97No1.pdf

送信デバイスの真正性保証

類似研究	提案内容	補足説明
①	ー （対象外）	
②	送信デバイス認証	シュノアの非対話ゼロ知識証明 クライアントIDはクライアントの秘密xのg^x
③	ー （対象外）	
④	送信デバイス・ブローカ相互認証	楕円曲線離散対数問題および一方向性関数を利用した独自方式 通信情報からの送信デバイスの特定は不可 相互認証に6パスが必要
SSDTF/MQTT	送信デバイス・ブローカ相互認証	公開鍵暗号（楕円エルガマル暗号等） チャレンジ/レスポンス方式

送信データの真正性保証

類似研究	提案内容	補足説明
①	ー （対象外）	
②	ー （対象外）	
③	公開鍵暗号による署名をPayloadへ	公開鍵暗号を利用した送信データへの署名付与・検証 タイムスタンプの有用性にも言及
④	Payloadを利用した独自方式による真正性保証・秘匿のためのプロトコル	楕円曲線離散対数問題および一方向性関数を利用した独自方式 通信情報からの送信デバイスの特定は不可 3パスで送信デバイスからブローカへ ブローカから受信デバイスへは1パス
SSDTF/MQTT	公開鍵暗号による署名をPayloadへ	公開鍵暗号を利用した送信データへの署名付与・検証

送信データの秘匿

類似研究	提案内容	補足説明
①	トピックごとにPublishデータを暗号化しPayloadへ	属性ベース暗号 ブローカは信頼できる第三者であることが必要 SPUBLISHという独自のコマンドを追加 多数のクライアントへの暗号化同報が可能
②	ー （対象外）	
③	Publishデータを暗号化しPayloadへ	ブローカによる復号方式、End-to-End暗号化方式の両方に言及
④	Payloadを利用した独自方式による真正性保証・秘匿	楕円曲線離散対数問題および一方向性関数を利用した独自方式 通信情報からの送信デバイスの特定は不可 3パスで送信デバイスからブローカへ ブローカから受信デバイスへは1パス
SSDTF/MQTT	Publishデータを暗号化しPayloadへ	送信デバイスは管理サーバの公開鍵による暗号化 ブローカおよび配信サーバによる受信先向けに暗号化鍵の付け替えにより、ブローカおよび配信サーバでのデータ漏洩リスクの低減

送信デバイスの匿名性と特定・追跡性の両立

類似研究	提案内容	補足説明
①	ー （対象外）	
②	ー （対象外）	
③	ー （対象外）	
④	ー （対象外）	
SSDTF/MQTT	送信デバイスの内部管理コードと外部公開コードの分離	連結可能匿名化 （データ配信サーバにおける内部管理コードと外部公開コードの対応表の管理）

Keychain
MQTT通信規格にブロックチェーンで暗号化と対改ざん性を実現

合同会社Keychain（2016年設立） 代表者：Jonathan Hope

DPI：Data Provenance Infrastructure

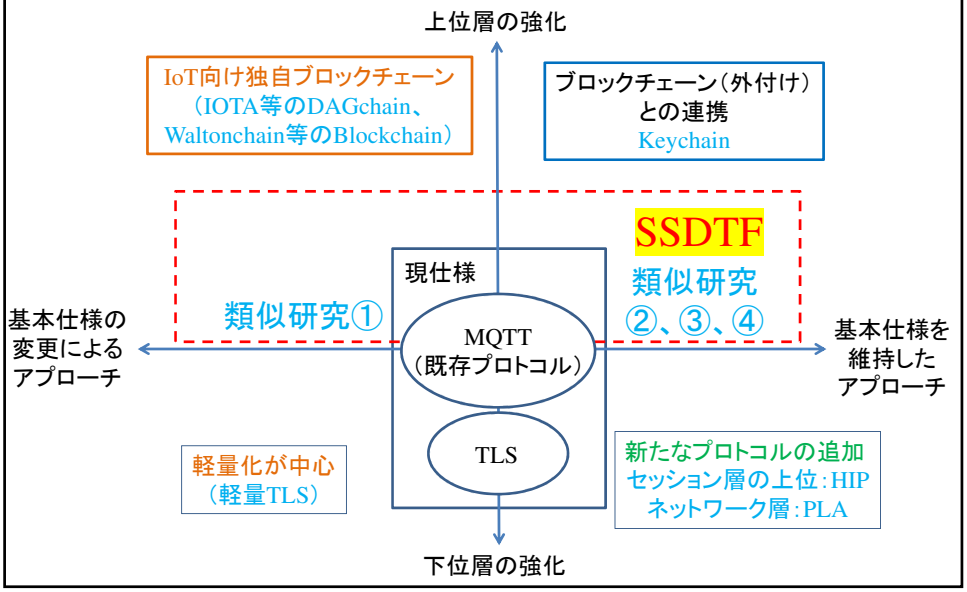
1. マシン・デバイスごとのIdentity生成・管理
2. End-to-end 暗号化通信
3. デジタル署名
4. デバイスの鍵更新および相手への更新情報通知
5. 多数のデバイス・参加者間でのセキュア通信

「DPIを活用し、MQTT通信規格上で、IoTデバイスが発するデータの暗号化、対改ざん性、および双方・多対多デバイス認証を実現」

主要な類似研究論文の対象

	①	②	③	④	SSDTF
送信デバイスの真正性保証	―	送信デバイス認証	―	相互認証	相互認証
送信データの真正性保証	―	―	公開鍵暗号による署名	独自方式による真正性保証	公開鍵暗号による署名
送信データの秘匿	トピックの受信デバイス向け暗号化	―	ブローカによる復号・再暗号化	ブローカによる復号せず再暗号化	ブローカによる復号せず再暗号化
送信デバイスの匿名性と特定・追跡性の両立	―	―	―	―	連結可能匿名化

MQTTにおける セキュリティ強化策分類



15分

7.

おわりに

SSDTF/MQTTで実現を目指す セキュリティ機能

(1)送信デバイスの真正性保証
　公開鍵暗号、チャレンジ/レスポンス方式による
　　送信・受信デバイスの真正性保証
(2)送信データの真正性保証
　公開鍵暗号を利用した送信データへの署名付与・検証による
　　送信データの真正性保証（非改ざん性保証）
　　送信デバイスの真正性保証
(3)送信データの秘匿
　公開鍵暗号を利用した送信データの暗号化による漏洩防止（秘匿）
　ブローカでは復号せずの再暗号化による暗号化データの転送
(4)送信デバイスの匿名性と特定・追跡性の両立
　配信サーバでの送信デバイスの内部IDの外部IDへの変換による匿名性保証
　配信サーバでの内部ID/外部ID対応表の管理による特定・追跡性保証

IoTAI-PJにおけるネットワーク層の今後の活動

（1）SSDTF 構想のMQTT 上での具現化方式
　　SSDTF/MQTT の基本仕様策定

（2）IoTデバイスおよび人が情報を発信する際の
　　認証の枠組みの総合的整理

（3）関連研究の調査・分析による
　　SSDTF構想の独自性・特徴等の整理

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。

終

（ご清聴、ありがとうございました。）

（付録1）SSDTF構想の目標

（1）送信デバイスの真正性保証

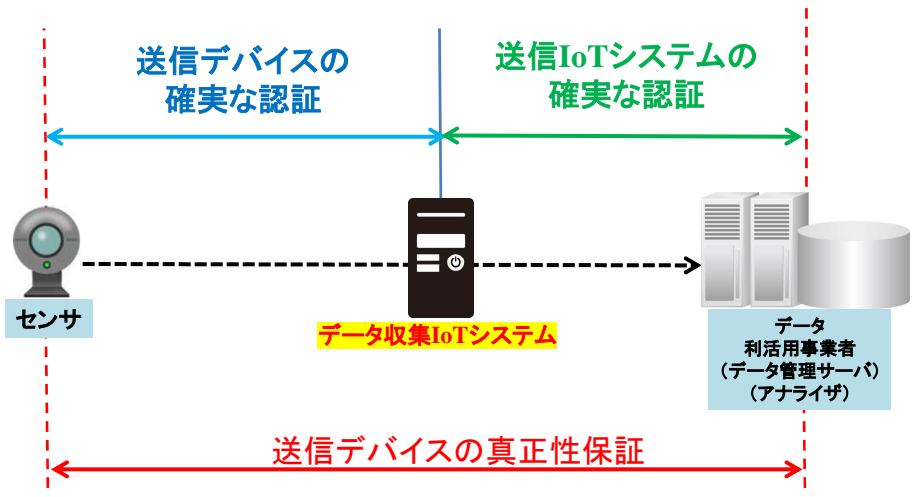
（2）送信データの真正性保証

（3）送信データの秘匿

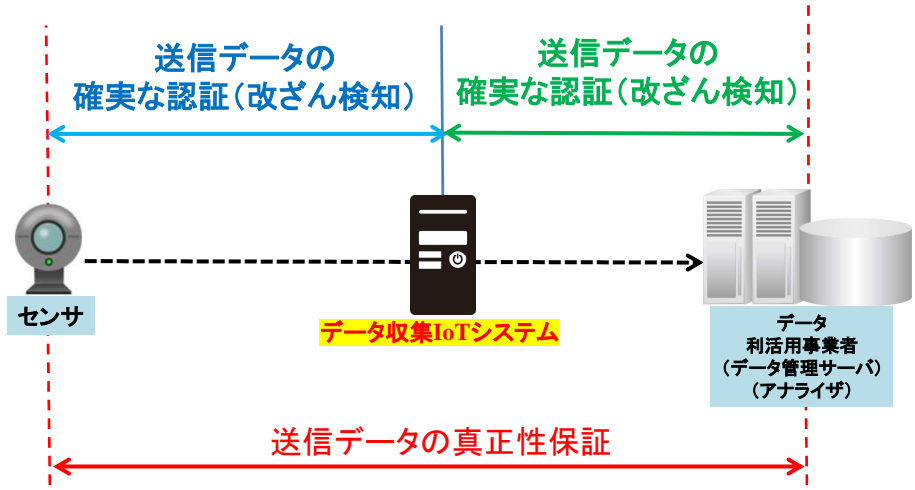
（4）送信デバイスの匿名性

（5）送信デバイスの特定・追跡性

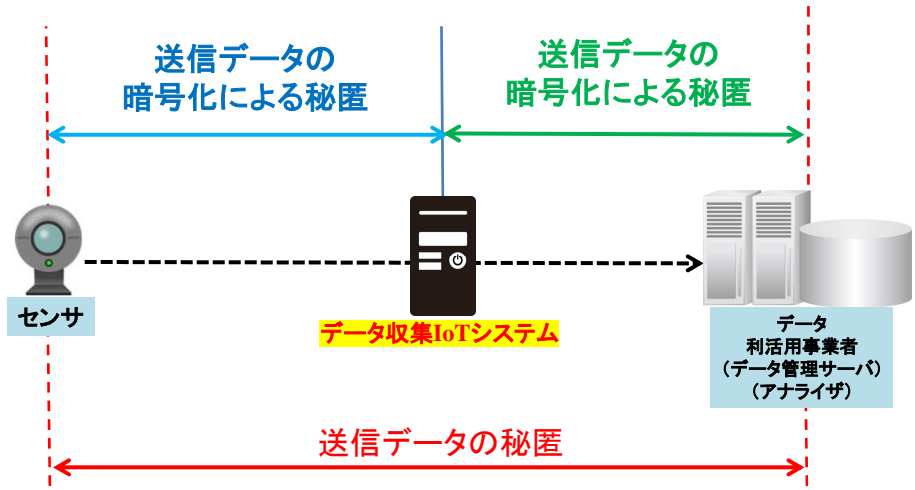
（1）送信デバイスの真正性保証



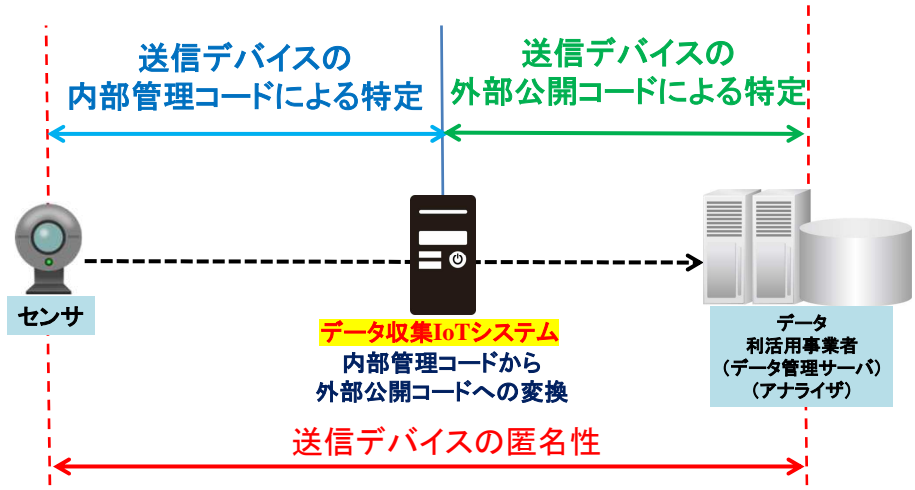
（2）送信データの真正性保証



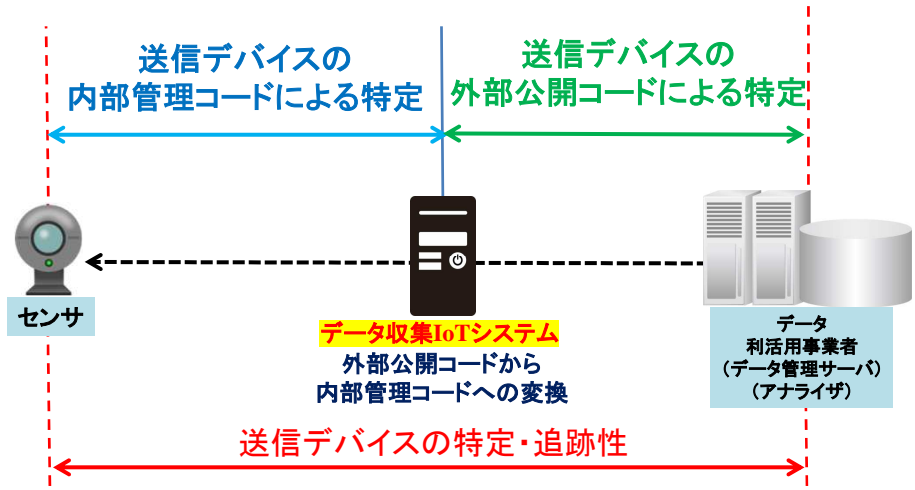
（3）送信データの秘匿



(4)送信デバイスの匿名性



(5)送信デバイスの特定・追跡性



（付録2）類似研究論文一覧

①Secure MQTT for Internet of Things (IoT)

https://ieeexplore.ieee.org/document/7280018

②HOW TO AUTHENTICATE MQTT SESSIONS WITHOUT CHANNEL- AND BROKER SECURITY

https://arxiv.org/pdf/1904.00389.pdf

③Securing MQTT protocol in IoT by payload Encryption Technique & Digital Signature

https://www.researchgate.net/publication/335328286_Securing_MQTT_protocol_in_IoT_by_payload_Encryption_Technique_Digital_Signature

④LIGHTWEIGHT SECURE SCHEME FOR IOT-CLOUD CONVERGENCE BASED ON ELLIPTIC CURVE

http://www.jatit.org/volumes/Vol97No1/13Vol97No1.pdf

類似研究①
Secure MQTT for Internet of Things (IoT)

（1）MQTTおよびMQTT-SN（センサーネットワーク向け）のセキュアなバージョンであるSMQTTおよびSMQTT-SNの提案

（2）SSL/TLSに依存しない、MQTTのためのスケーラブルでライトウェイトかつロバストなセキュリティ機能の楕円曲線上のABE（属性ベース暗号）による実現方式（送信デバイスはABEによる1回の暗号化により同一メッセージの多数のデバイスへの秘匿通信が可能）

https://ieeexplore.ieee.org/document/7280018

類似研究①とSSDTF/MQTTの関係

（1）SSDTFではデータ収集IoTシステムを対象としているため、送信デバイス（センサ）が送信するメッセージは、ブローカ経由、そう多くない配信サーバへ送信されることを想定（SSDTFでは、多数のデバイスへの同報通信は想定していない）

（2）但し、SSDTFにおいても管理サーバからの多数のデバイスへの同一メッセージの一斉送信が必要なケースは存在。例えば、管理サーバの公開鍵の更新等（現状は、特定のトピックのメッセージとして管理サーバが更新情報をPUBLISH、ブローカがサブスクライバとして指定されたデバイスごとに暗号鍵付け替え・署名付与しPUBLISHすることを想定）

類似研究②
HOW TO AUTHENTICATE MQTT SESSIONS WITHOUT CHANNEL- AND BROKER SECURITY

（1）MQTTの認証機能の脆弱性からセッションハイジャック等のリスクを指摘、シュノアの非対話型ゼロ知識認証スキームを使用した認証方式を提案。

（2）一般の認証方式の場合に必要となる、ブローカによる事前のセッティング/管理のための、別チャンネルを通した操作や、デバイスとブローカによる秘密の共有が不要。（ClientIDとしてg^xを選定し、xの保有をゼロ知識証明で検証）

（3）求められるブローカのセキュリティレベルを、“fully trusted”から“honest but curious”へ下げることが可能。（ブローカが他のデバイスの秘密の情報を保有しない。）

https://arxiv.org/pdf/1904.00389.pdf

類似研究②とSSDTF/MQTTの関係

（1）SSDTFでは、デバイスは公開鍵暗号による署名のための秘密鍵の保有を前提としており、この秘密鍵を利用したチャレンジ/レスポンス方式の認証を採用予定。研究②で示されたゼロ知識証明利用の可否については別途検討予定。

（2）SSDTFにおいても、ブローカおよび配信サーバには送信データ（メッセージ）の復号権限を与える必要はなく、ブローカおよび配信サーバのセキュリティレベルは“honest but curious”へ下げることが可能。

類似研究③
Securing MQTT protocol in IoT by payload Encryption Technique & Digital Signature

（1）暗号化による送信データ（メッセージ）の秘匿、署名によるインテグリティの検証方式を提案

（2）暗号化にはトピックごとの暗号鍵を使用。署名には送信デバイスの秘密鍵を使用。送信データは、トピックごとの復号鍵を所有する受信デバイスのみが復号可能。

Https://www.researchgate.net/publication/335328286_Securing_MQTT_protocol_in_IoT_by_payload_Encryption_Technique_Digital_Signature

類似研究③とSSDTF/MQTTの関係

（1）トピックごとの暗号鍵により暗号化し、受信デバイスはそのトピックの復号鍵により復号する仕組みによりEnd-To-Endの暗号化を提案しているが、SSDTFでも管理サーバの公開鍵による暗号化、ブローカおよび配信サーバにおける鍵の付け替えにより、End-To-Endの暗号化を実現している（研究③の方式では、送信デバイス側も受信デバイス側も、トピックごとの暗号鍵や復号鍵を管理する必要となる）

（2）SSDTF/MQTTでは、管理サーバがIoTシステムを構成する全てのデバイスの秘密鍵を保有し、運用・管理を行うモデルを想定しているが、AmazonやGoogleが展開しているMQTTクラウドサービス（MQTT as a Service）を利用する場合は、デバイスの秘密鍵の管理方式を工夫する必要がある

類似研究④
LIGHTWEIGHT SECURE SCHEME FOR IOT-CLOUD CONVERGENCE BASED ON ELLIPTIC CURVE

（1）デバイス登録時には、デバイスがSubscribeするトピック情報を加味し鍵ペアが生成され、デバイスへ格納される。ブローカも、鍵ペアを生成し格納。デバイスがブローカへログイン時に、ECCポイントの乗算及び排他的論理和を利用した相互認証方式を提案。SSL/TLSよりパフォーマンスが良い相互認証方式であることを主張。

（2）Publishするデバイスは、その都度、デバイスの認証を行う方式。認証成功後、改めてPublisherはECCポイントの乗算及び排他的論理和を利用したメッセージの暗号化を行い、Publishする方式。

http://www.jatit.org/volumes/Vol97No1/13Vol97No1.pdf

類似研究④とSSDTF/MQTTの関係

（1）デバイス登録時に、デバイスがSubscribeするトピック情報を加味した鍵ペアの生成が一つの特徴（トピックごとの暗号化方式）

（2）ECCポイントの乗算及び排他的論理和を利用した相互認証方式は、署名により相互認証を行うSSDTFに比べ、計算負荷は小さいことが想定される

（3）ECCポイントの乗算及び排他的論理和を利用した独自の暗号化も“軽量”ではあるが、安全性の確認が必要（論文では示されていない）

（4）SSDTF/MQTTの一つの特徴である、ブローカにおける鍵の付け替え、と同等の機能を本研究でも想定している模様（本論文では方式の詳細は不明。詳細入手次第、検討要）

終

（付録　最終ページ）