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

2019年9月4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

©Advanced IT Corporation 3

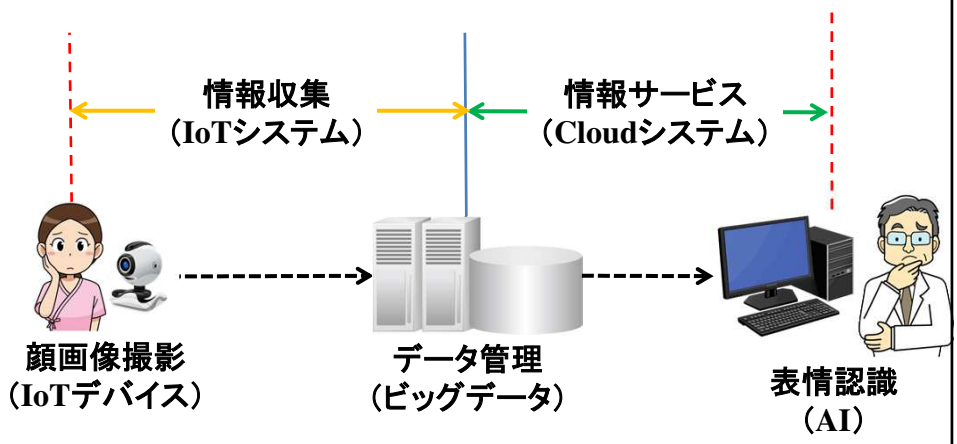
IoTデバイス認証基盤の構築と新AI手法による表情認識の医療介護への応用（IoTAI-PJ）（SCOPE：2018～2020）

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。

©Advanced IT Corporation 4

IoTAI-PJが想定する応用イメージ



©Advanced IT Corporation 5

IoTシステムにおける真正性保証

情報サービス層	リーマン幾何学を用いた新AIによる、敵対学習による誤認識の防止・真正性の高い表情を認識する手法の確立。デバイス層と連携し、要介護施設等で実証実験。
データ管理層	クラウドや組織内における情報漏洩防止のための組織暗号、論理的暗号化状態処理、及び構造化自然言語による秘匿検索に関する研究開発。
ネットワーク層	拡張S/MIMEであるSSMAX コンセプトに基づき、OSI参照モデルのアプリケーション層における、送信デバイス・データの真正性の確保および送信デバイスの匿名性と特定・追跡性の両立が可能な仕組みの提案
デバイス層	重要デバイスへの電子認証の埋め込みと監視・見守りカメラへの実装。

©Advanced IT Corporation 6

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
患者・被介護者の顔画像 データ採取

ゲートウェイ
顔画像データの安全な送信

アグリゲータ
顔画像データの安全な管理

アナライザ
顔画像データによる表情認識

デバイス層
デバイスの真正性を示す鍵ペアの保有

アプリケーション層
使用データの真正性を確認の上の表情認識

実証実験の構成

©Advanced IT Corporation 7

SSMAX構想と基本コンセプト
（Secure and Safe e-Mail Exchange Framework）

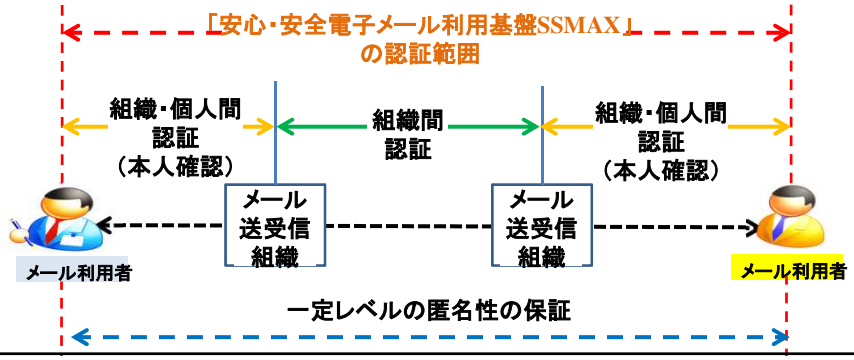
電子メールの真正性および匿名性と特定・追跡性の両立の必要性

真正性：なりすまし・改ざん検知

匿名性：プライバシー保護

特定・追跡性：犯罪・悪用抑止

（標的型攻撃/フィッシング/誹謗・中傷/いじめ）対策



©Advanced IT Corporation 8

安心・安全な電子メール利用基盤SSMAX
研究開発活動の歴史

2016年に研究に着手

2016年10月、コンピュータセキュリティシンポジューム（CSS2016）にて発表
才所敏明，五太子政史，辻井重男，
”標的型メール攻撃に対抗する「組織通信向けS/MIME」”

2017年1月、暗号と情報セキュリティシンポジューム（SCIS2017)にて発表
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）」構想”

2017年10月、コンピュータセキュリティシンポジューム2017（CSS2017）にて発表
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）」

2017年11月、暗号と情報セキュリティ研究会 (ISEC)にて発表
才所 敏明，五太子 政史，辻井 重男，”社会的課題「安心・安全な電子メール
利用環境の実現」のための三止揚・MELT-UP の試み”(ISEC2017-54)

2018年9月、情報処理学会論文誌 2018年9月号（Vol.59，No,9）に掲載
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）」悪意のあるメールの根絶とメール内容の確実な保護を目指して“

©Advanced IT Corporation 9

安心・安全なIoTシステムフレームワークSSIoT（Secure and Safe IoT System Framework）

2017年に研究着手

2018年5月、情報処理学会第81回CSEC研究会にて発表

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“

本発表では、SSIoTとして期待される機能の定義および活用可能な既存技術を調査の上、各機能実現における基本的な考え方を提示

SSIoTで実現すべき機能

- **＊IoT機器の保護（被害者にならないために）**
- **＊IoT機器の保護（加害者にならないために）**
- **＊被害・加害の早期の収拾**
- **＊IoT機器の適切な状態の維持**
- **＊IoT機器が送信するデータの保護**

機能実現に活用が可能な既存技術

- **＊PLA（パケットのIPアドレスへのIoTデバイスの署名付与によるパケットの認証）**
- **＊HIP（IoTデバイスの署名付与によるホストIDの認証）**
- **＊組織暗号（IoTデバイスの署名付与による送信デバイス・送信データの認証）**

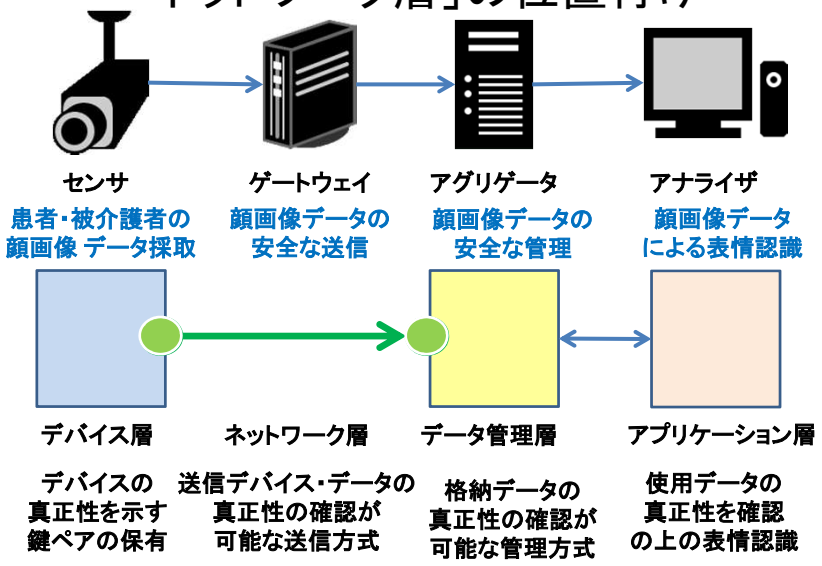
©Advanced IT Corporation 10

OSI参照モデルにおける活用想定技術の適用想定階層

階層	名称	活用想定技術
7	アプリケーション層	SSMAX（組織暗号、他）
6	プレゼンテーション層	
5	セッション層	HIP（Host Identity Protocol） PLA（Packet Level Authentication）
4	トランスポート層	
3	ネットワーク層	
2	データリンク層	
1	物理層	

©Advanced IT Corporation11

IoTAI-PJにおける「ネットワーク層」の位置付け



©Advanced IT Corporation12

IoTAI-PJ（SCOPE：2018～2020）「ネットワーク層」の研究開発目標と研究開発方針

研究開発目標

拡張S/MIMEであるSSMAX コンセプトに基づき、
OSI参照モデルのアプリケーション層における、
送信デバイス・データの真正性の確保および送信デバイスの匿名性と特定・追跡性の両立が可能な仕組みの提案
（SSDTF：Secure and Safe Data Transfer Framework）

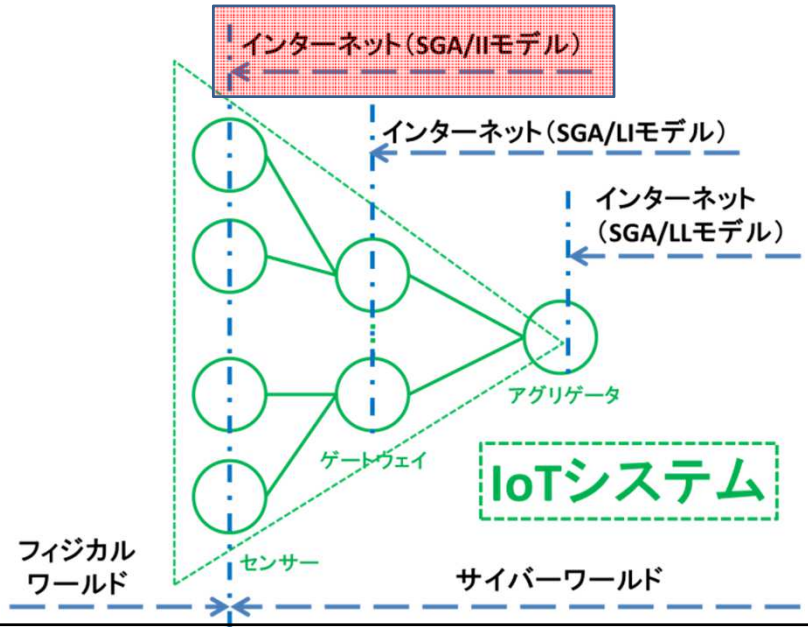
研究開発方針

①SSMAXコンセプトのIoT分野への適用の観点から、SSDTFの研究開発を推進する
②現存する主要なデータ送信プロトコルをベースに、SSDTFの研究開発を推進する

4.IoTAI-PJ：ネットワーク層

©Advanced IT Corporation13

想定するIoTシステム　SGA/IIモデル



5.SSDTF：実現方式

©Advanced IT Corporation14

SSDTF
Secure and Safe Data Transfer Framework

2018年7月、夏のセキュリティシンポジューム in 札幌（CSEC82）にて、発表

才所敏明，辻井重男，“インターネット依存社会における情報送信者・情報送信機器の匿名性と特定・追跡性”

発表概要

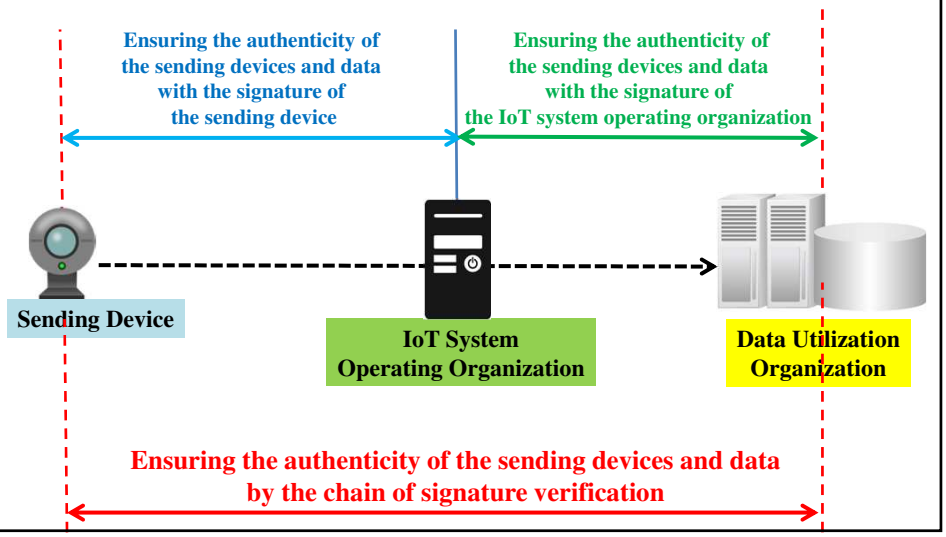
＊IoT機器が情報を送信する場合、送信デバイス・データの真正性保証と共に、匿名性と特定・追跡性の両立の必要性を主張

＊SSMAXと同等の「連結可能匿名化」による実現可能性を提示

©Advanced IT Corporation 15

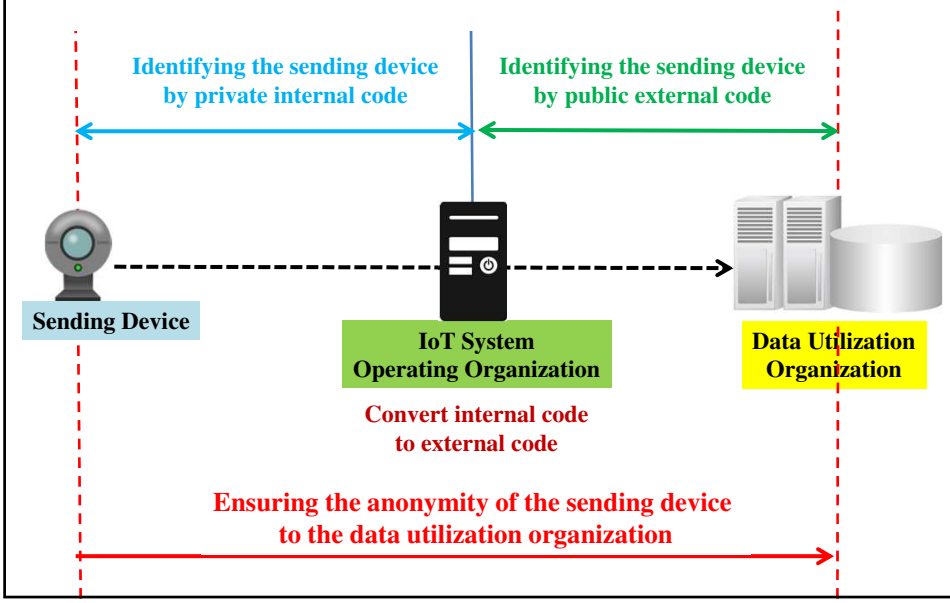
(1)Authenticity assurance at the network layer

a: Authenticity of the sending device (spoofed device detection)
b: Authenticity of the received data (tampered data detection)



©Advanced IT Corporation 16

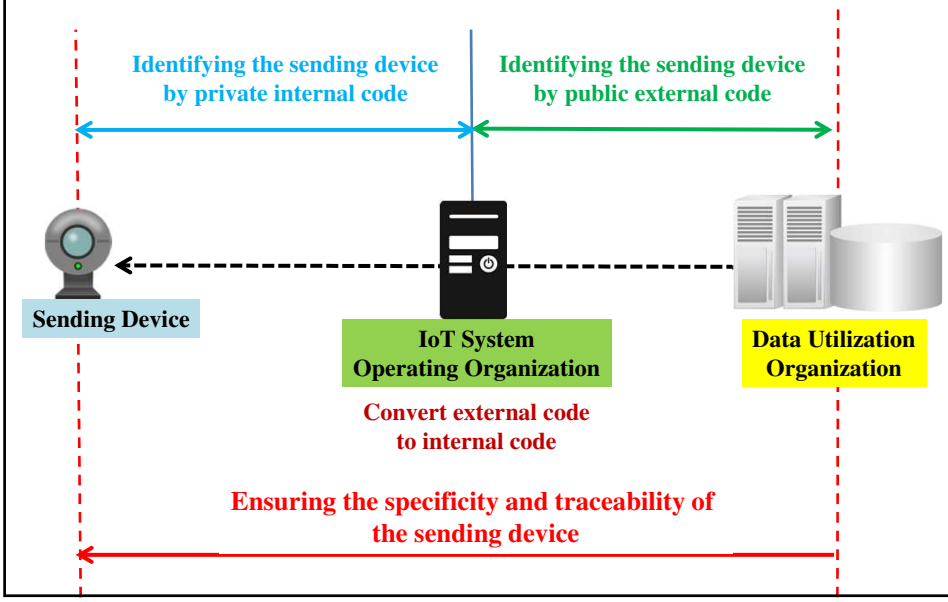
(2)Anonymity of the sending device



5.SSDTF：実現方式

©Advanced IT Corporation 17

(3)Specificity and traceability of the sending device



6.SSDTF：実装方式

©Advanced IT Corporation 18

既存のプロトコルをベースにSSDTF仕様を検討

Protocol	Transport	Security	Architecture
AMQP	TCP	TLS/SSL	Publish/Subscribe
CoAP	UDP	DTLS	Request/Response
DDS	UDP(TCP)	DTLS(TLS)	Publish/Subscribe
MQTT	TCP	TLS/SSL	Publish/Subscribe
REST	HTTP	HTPPS	Request/Response

主要なIoT向けデータ送信プロトコル

AMQP（Advanced Message Queueing Protocol） OASISが標準化（もともと、AMQPコンソーシアムが金融・企業向けのメッセージ標準として定義）

CoAP（Constrained Application Protocol） IETFでRFC（8ビットコントローラ/ネットワーク（6LoWPAN）を対象、HTTPとのインタフェース）

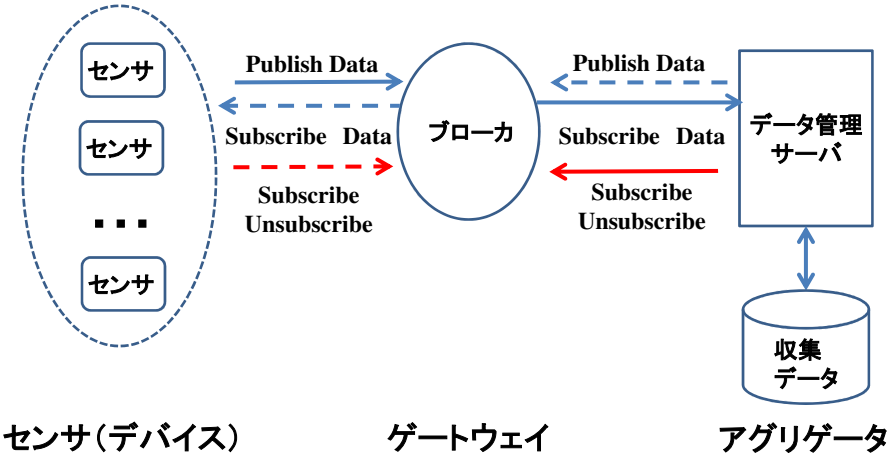
DDS（Data Distribution Service） Object Management Groupで標準化

MQTT（Message Queueing Telemetry Transport） OASISが標準化（IBMが90年代にテレメトリ用の軽いプロトコルとして開発、IoTのデータ送信の標準プロトコルとして注目されている）

REST（Representational State Transfer） IETFでRFC（HTTP プロトコルの作成者の1人Roy Fieldingが提案、主にWorld Wide Web とHTTP に適用）

©Advanced IT Corporation 19

MQTTアーキテクチャ(Publish/Subscribe)とSGA/IIモデルとの対応



©Advanced IT Corporation 20

MQTTパケットの内容

	Packet Type	名称	機能
IPヘッダ			
TCPヘッダ			
MQTT ヘッダ Packet type (4ビット)	1	CONNECT	センサがブローカに接続要求 ペイロードに以下の情報を格納 それぞれ65535バイトまで可能 クライアントID ユーザ名 パスワード
	3	PUBLISH	メッセージを発行 ヘッダにトピック名(文字列) ペイロードにメッセージを格納
MQTT ペイロード	8	SUBSCRIBE	受け取るメッセージのトピックを通知 ペイロードにトピック名の一覧を格納

©Advanced IT Corporation21

MQTTのセキュリティ
アプリケーション層における送信デバイス認証

（1）CONNECTパケットのペイロードに指定されるユーザ名および
パスワードによりクライアント認証機能を実装可能（標準）
注：認証情報を格納しているペイロードの暗号化が必要
独自にペイロードの暗号化機能の実装が必要
（TLS利用時には、通信路上ではペイロードも暗号化）

（2）CONNECTパケットのペイロードに指定されるユーザ名および
パスワードの領域を利用し、独自の認証機能の組込みが可能
（LDAP [RFC4511] および OAuth [RFC6749] の利用も可）

➔ SSDTFにおける「送信デバイスの真正性保証」に活用を検討

©Advanced IT Corporation22

MQTTのセキュリティ
アプリケーション層における送信データ認証

（1）標準では用意されておらず、送信データの改ざん検知機能は無い
注：TLS利用時には、通信路上のメッセージの改ざん検知は可能

（2）PUBLISHパケットのペイロードにメッセージのメッセージ認証コード
または署名を格納することによる改ざん検知は可能

➔ SSDTFにおける「送信データの真正性保証」に活用を検討

©Advanced IT Corporation23

MQTTのセキュリティ
アプリケーション層における送信データ秘匿

（1）標準では用意されておらず、送信データの秘匿機能は無い

注：TLS利用時には、通信路上のメッセージの暗号化は可能

（2）独自に暗号化したメッセージを
PUBLISHパケットのペイロードに格納することは可能

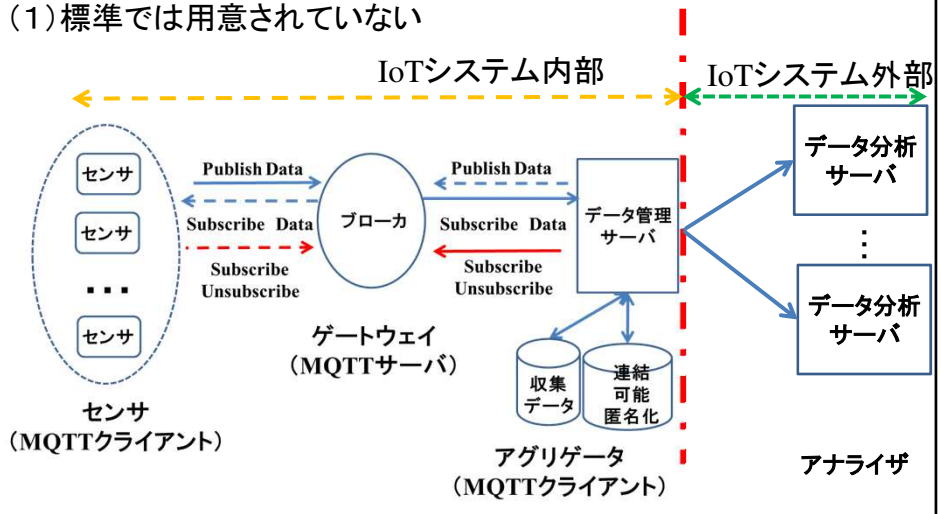
注：PUBLISHパケットのヘッダに格納されている
トピック名の暗号化は不可能

➔ SSDTFにおける「送信データの秘匿」に活用を検討
➔ トピック名の暗号化ができないことの影響の検討
➔ End-to-Endの秘匿実現可能性を検討（組織暗号）

©Advanced IT Corporation24

MQTTのセキュリティ
送信デバイスの匿名性と特定・追跡性

（1）標準では用意されていない



7.おわりに

©Advanced IT Corporation25

まとめ（1/2）

（1）「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）」

①IoTAI-PJにおけるネットワーク層の研究開発目標

拡張S/MIMEであるSSMAX コンセプトに基づき、
OSI参照モデルのアプリケーション層における、
送信デバイス・データの真正性の確保および送信デバイスの
匿名性と特定・追跡性の両立が可能な仕組みの提案➔SSDTF

②先行研究SSIoT、SSMAXの内容・成果

メール送信者・メール内容の真正性保証方式
メール送信者の匿名性と特定・追跡性の両立方式

7.おわりに

©Advanced IT Corporation26

まとめ（2/2）

（2）SSDTF実現方式および実装方式の考察結果

①IoTシステムにおける真正性保証および匿名性と特定・追跡性の両立の実現方式の提案

署名チェーンによる真正性保証方式
連結可能匿名性による匿名性と特定・追跡性の両立方式

②既存のプロトコルMQTTにおけるSSDTF機能

現仕様の拡張性を利用し、SSDTF機能実装の見通し確認
対象機能：送信デバイス認証、送信データ認証、
送信データ秘匿、匿名性と特定・追跡性の両立

©Advanced IT Corporation27

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。

©Advanced IT Corporation28

終

（ご清聴、ありがとうございました。）