真贋の判定こそはモノ層からサービス層まで貫く理念（2019年2月23日、26日）

SCOPE研究開発課題
“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”

「ネットワーク層」

2019年2月26日
才所敏明（（株）IT企画）
toshiaki.saisho@advanced-it.co.jp
セキュアIoTプラットフォーム協議会
中央大学研究開発機構

 1

ご説明項目一覧

1．本研究開発で活用するこれまでの研究開発活動・成果概要（4分）
- 1．1　SSMAX
- 1．2　SSIoT

2．SCOPE研究開発課題における
「ネットワーク層」の位置付け・研究開発目標（3分）

3．平成30年度の「ネットワーク層」の成果目標・具体的成果（10分）
- 3．1　段階的開発・普及戦略の策定
- 3．2　研究対象IoTシステムモデルの選定、
送信デバイス（IoT機器）・送信データの真正性確保方式、
および匿名性と特定・追跡性の両立の仕組みの素案策定
- 3．3　IoTシステム向けデータ送信プロトコルの予備調査結果

4．次年度以降の研究開発計画と最終目標（3分）

 2

1．本研究開発で活用する
これまでの研究開発活動・成果概要（4分）

1.1　SSMAX（安心・安全な電子メール利用基盤）
（1）SSMAX構想と基本コンセプト
（2）活動状況・成果

1.2　SSIoT（安心・安全なIoTシステムフレームワーク）
（1）問題提起、活動状況・成果

 3

1.1　SSMAX（安心・安全な電子メール利用基盤）
（1）SSMAX構想と基本コンセプト

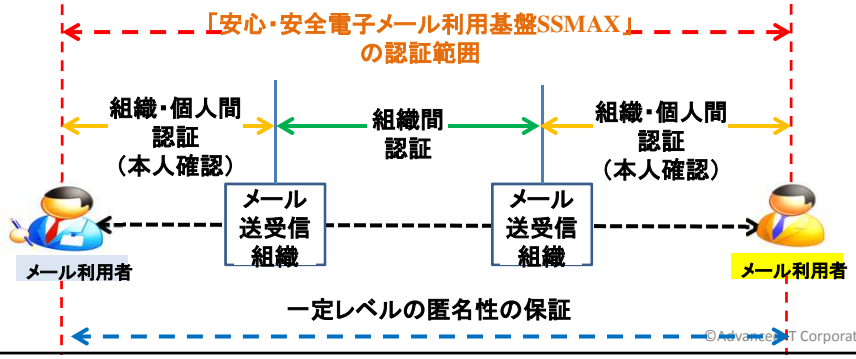
電子メールの真正性および匿名性と特定・追跡性の両立の必要性

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



 4

1.1 SSMAX（安心・安全な電子メール利用基盤）
（2）活動状況・成果

＊2016年より4件の学会発表実施、段階的にSSMAXの構想を具体化。

＊SSMAXの技術仕様、他の対策に対するSSMAXの優位性、
SSMAXの社会実装上の課題と克服方策等を下記論文に掲載。

情報処理学会論文誌 2018年9月号（ Vol.59, No,9）, 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“（2018年9月15日発行）

＊今後は、SSMAXの試作・検証、実証実験等の機会をとらえ、
我が国が世界に先駆け、安心・安全な電子メール利用基盤を
構築・整備し、我が国の産業や国民の生活を支える安定した
基礎的・共通的コミュニケーション基盤の確立を目指したい。

1.2 SSIoT（安心・安全なIoTシステムフレームワーク）
（1）問題提起、活動状況・成果

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機器が送信するデータの保護
- ＊IoT機器の保護（加害者にならないために）
- ＊IoT機器の適切な状態を維持するために
- ＊被害・加害を早期に収拾させるために

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デバイス署名付与によるパケット認証）
- ＊HIP（IoTデバイスのIDとIoTデバイス署名付与によるホスト認証）
- ＊組織暗号（IoTデバイスが収集した情報の安全な送信）

VII（Virtual Intranet over Internet）の実現可能性

2. SCOPE研究開発課題

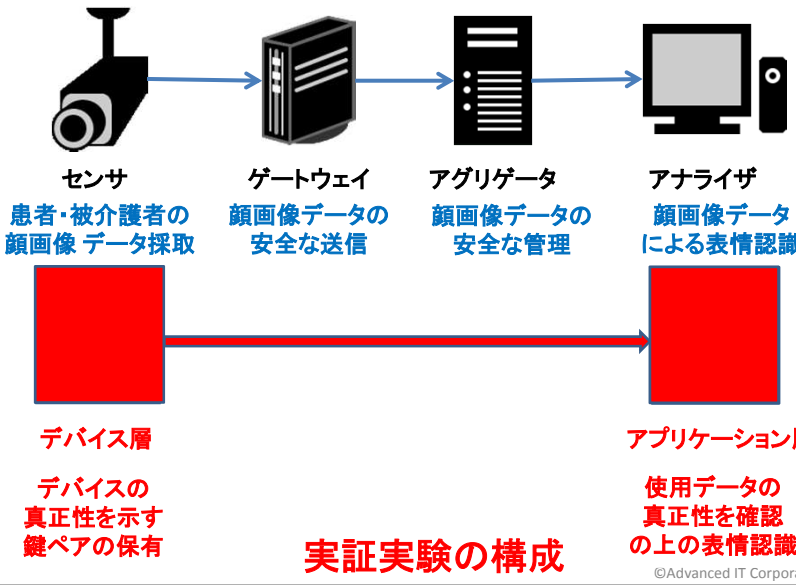
“IoTデバイス認証基盤の構築と
新AI手法による表情認識の医療介護への応用”

「ネットワーク層」の位置付け・研究開発目標（3分）

（1）SCOPE研究開発課題の
全体像と「ネットワーク層」の位置付け

（2）「ネットワーク層」の
研究開発目標と研究開発方針

（1）SCOPE研究開発課題の全体像と「ネットワーク層」の位置付け



実証実験の構成

（2）「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

①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・データの真正性確保のための仕組みの提案
（SSDTF：Secure and Safe Data Transfer Framework）

②SSMAXおよびSSDTFを包含する
組織・個人・IoT を対象とする認証方式全体の枠組を検討・提案

研究開発方針

①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

②SSMAX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

3．平成30年度の「ネットワーク層」の成果目標・具体的成果（10分）

3．1　段階的開発・普及戦略策定（案）

SSDTF（Secure and Safe Data Transfer Framework）構想が対象

（1）段階的開発戦略：構想策定戦略、具体的開発戦略

（2）段階的普及戦略：社会認知促進戦略、具体的実装促進戦略

3．2　構想策定戦略に基づく具体的研究開発成果

（1）研究対象IoTシステムモデルの選定

（2）送信デバイス・データの真正性確保方式（素案）

（3）匿名性と特定・追跡性の両立の仕組み（素案）

（4）IoTシステム向けデータ送信プロトコル（予備調査）

3．1　段階的開発・普及戦略（案）

段階的開発戦略：

①IoTシステム向け認証方式の“構想策定戦略”

本研究期間中にIoTシステム向けの認証方式の基本構想策定

学会発表等を通じ、認証方式に関する専門家との意見交換実施

②IoTシステム向け認証方式の“具体的開発戦略”

本研究期間終了後、具体的開発のためのPJ立ち上げを期待

具体的開発は、普及戦略を担うIoTシステムベンダの参画が必須

段階的普及戦略

①IoTシステム向け認証方式の“社会認知促進戦略”

本研究期間中から、公開シンポジュームによる説明等を通じ、

新たな認証方式の具体的開発や社会実装の国民的合意形成へ

②IoTシステム向け認証方式の“具体的実装促進戦略”

公的資金によるパイロットPJ推進、IoT減税等の税制面の施策を展開

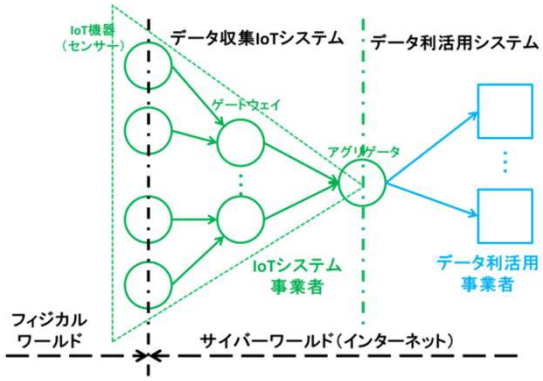
IoT/IoTシステムの脆弱性やその脆弱性に起因する事故・事件の

法的責任の明確化等の法制度面の施策を展開

3．2　構想策定戦略に基づく具体的研究開発成果
（1）研究対象IoTシステムモデルの選定

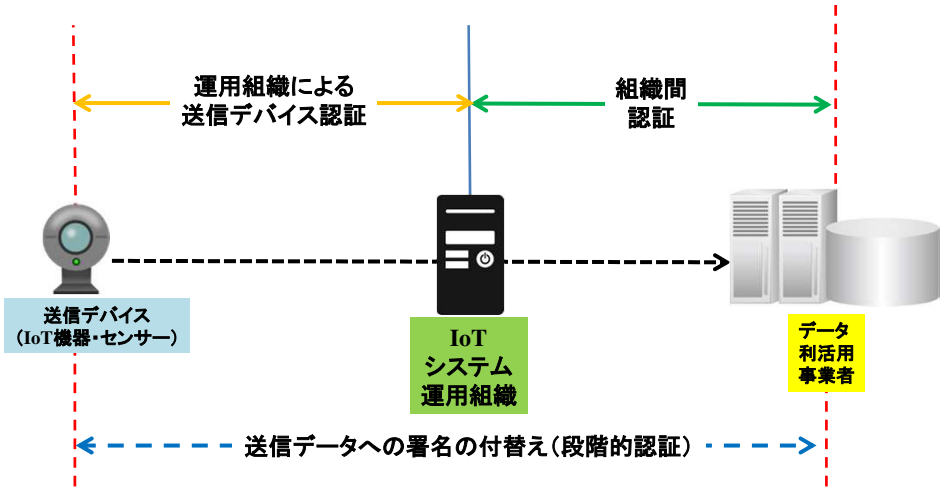
①シンプルな構成のデータ収集IoTシステム、具体的にはセンサー、ゲートウェイ、アグリゲータから構成されるIoTシステムを対象。

②センサーとゲートウェイ間、ゲートウェイとアグリゲータ間のネットワークとしてはインターネットを利用。



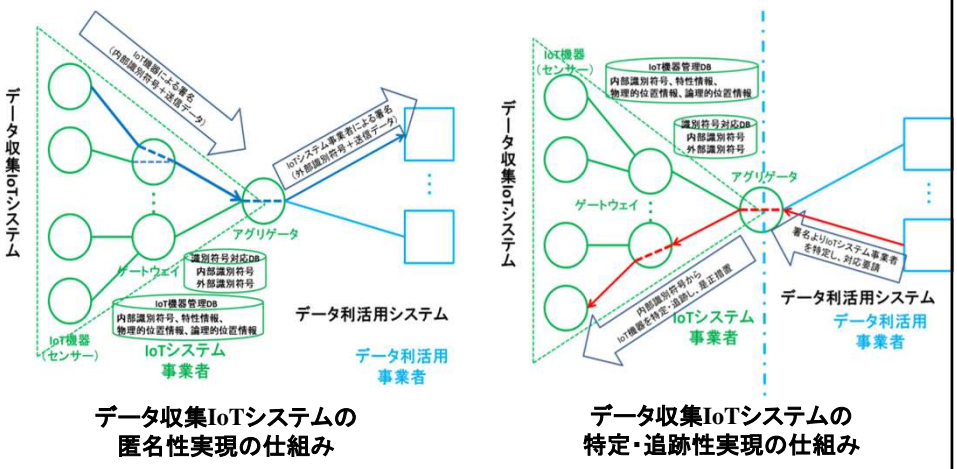
研究開発対象としたデータ収集IoTシステムの構成（SGA/IIモデル）

3．2　構想策定戦略に基づく具体的研究開発成果
（2）送信デバイス・データの真正性確保方式（素案）



 13

3．2　構想策定戦略に基づく具体的研究開発成果
（3）匿名性と特定・追跡性の両立の仕組み（素案）



データ収集IoTシステムの
匿名性実現の仕組み

データ収集IoTシステムの
特定・追跡性実現の仕組み

送信デバイスIDの置換え（連結可能匿名化）

 14

３．２　構想策定戦略に基づく具体的研究開発成果
（４）IoTシステム向けデータ送信プロトコル

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）

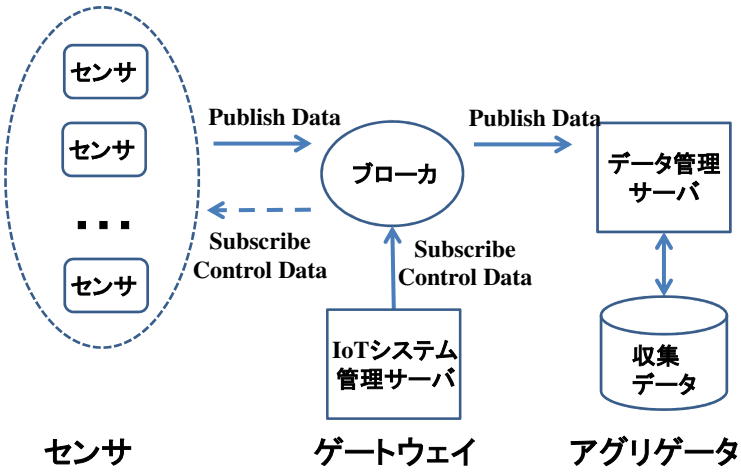
CoAP（Constrained Application Protocol）　IETFでRFC（8ビットコントローラ/ネットワーク（6LoWPAN）を対象、HTTPとのインタフェース）

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

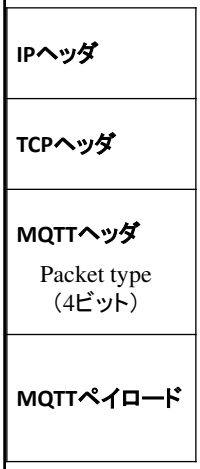
MQTT（Message Queueing Telemetry Transport）　OASISが標準化（IBMが90年代にテレメトリ用の軽いプロトコルとして開発、IoTのデータ送信の標準プロトコルとして注目されている）

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）

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



MQTTパケットの内容



Packet Type	名称	機能
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 クライアントID（ユーザ名） （1～23バイトの文字列） パスワード（0～65535バイトのバイナリ）
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
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

MQTTのセキュリティ　送信デバイス認証機能

（1）サーバ（ブローカ）による
クライアント（センサおよびデータ管理サーバ群）認証機能

①CONNECTパケットのペイロードに指定されたクライアントID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）

②CONNECTパケットのペイロードのクライアントID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）

注1：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）クライアントによるサーバ認証機能➔無い
注1：TLS利用時には、サーバ認証が可能

MQTTのセキュリティ　送信データ認証機能

（1）送信データの改ざん検知機能

標準では用意されていないが、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

注1：TLS利用時には、ネットワーク上のメッセージの改ざん検知は可能

（2）送信データの秘匿機能

標準では用意されていないが、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1：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

注2：TLS利用時には、ネットワーク上のメッセージの暗号化は可能

MQTTのセキュリティ機能に関する考察

（1）セキュリティは、TLSに依存する部分が多い。

➔ ネットワーク上のセキュリティのみで、
ネットワークの接続点が脆弱となる

（2）通信路のセキュリティのみではなく、
通信情報のセキュリティも必要

➔ TLSのセキュリティ機能のみでは不十分

（3）MQTTへのSSMAXコンセプトの組込みのための検討課題

①CONNECTパケットにおける
クライアント認証プロセスの変更可能性

②サーバ認証の実現方法

③複数データ管理サーバ（クライアント）の場合の対応方法

４．次年度以降の研究開発計画と成果目標（3分）

2019年度：

(1)IoTシステムモデル/IoT向け
データ送信プロトコルの詳細調査

(2)送信デバイス/データ認証のためのSSDTF素案策定
（真正性確保および匿名性と特定・追跡性の両立の
構想実現方式案の作成）

2020年度：

(1)送信デバイス/データ認証のための
SSDTF基本仕様とりまとめ

(2)組織・個人・IoT を対象とする
認証方式全体の枠組を検討・提案

SCOPE研究開発課題 “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”

「ネットワーク層」の研究開発目標

①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・データの真正性確保のための仕組みの提案
（SSDTF：Secure and Safe Data Transfer Framework）

②SSMAXおよびSSDTFを包含する
組織・個人・IoT を対象とする認証方式全体の枠組を検討・提案

終

ご清聴、ありがとうございました！