令和元年度研究開発成果概要図 （目標・成果と今後の研究計画）

採択番号：19501

１．研究課題・受託者・研究開発期間・研究開発予算

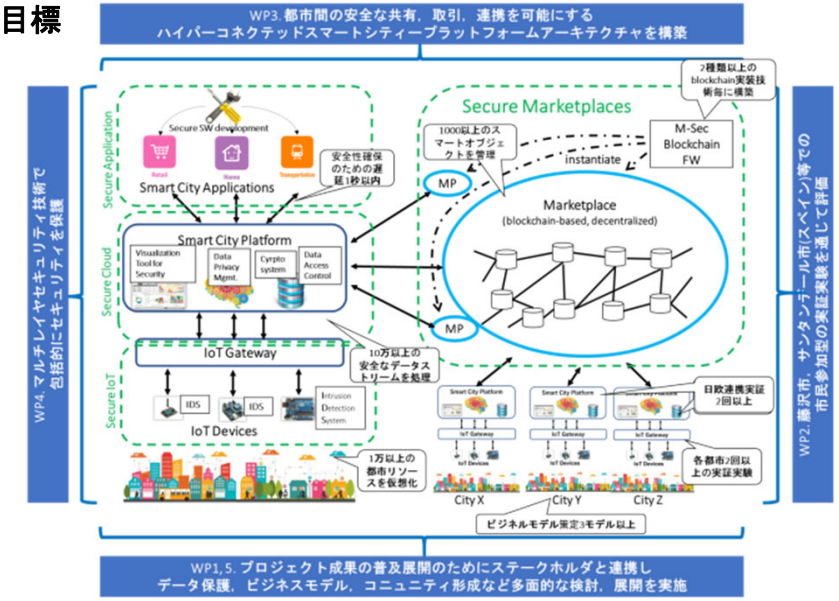
◆研究開発課題名 ：欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発
◆副題 ：ブロックチェーン・ビッグデータ・クラウド及びIoTを使用したハイパーコネクテッドスマートシティを実現するマルチレイヤセキュリティ技術
◆ Acronym ：M-Sec
◆実施機関 ：東日本電信電話株式会社＜代表研究者＞、学校法人慶應義塾 慶應義塾大学SFC研究所、国立大学法人横浜国立大学、大学共同利用機関法人情報・システム研究機構、学校法人早稲田大学、株式会社エヌ・ティ・ティ・データ経営研究所
◆研究開発期間：平成30年度～令和3年度（36ヶ月）
◆研究開発予算：総額186百万円（令和元年度 62百万円）

２．研究開発の目標

・ハイパーコネクテッド社会を構成するIoTデバイス、クラウドシステム、及びそれらを介して流通するデータの機密性、完全性、及び可用性を向上させるために、多層にわたってそれらを実現するM-Secアーキテクチャの研究開発を行う。さらにこれらを基礎としてデータマーケットプレイスを構築し、その上での実社会データ流通・取引と、新産業創出を促進する。

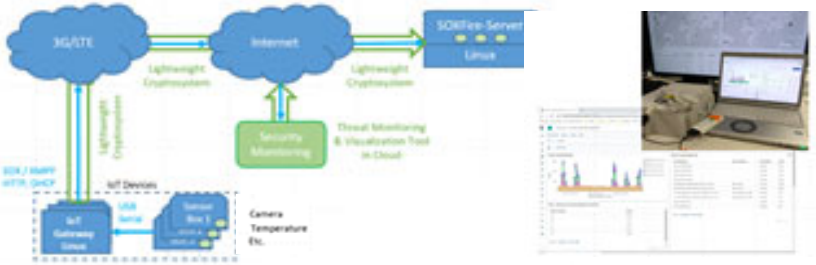
３．研究開発の成果

プロジェクト目標



ブロックチェーン・ビッグデータ・クラウド及びIoTを使用したハイパーコネクテッドスマートシティを実現するマルチレイヤセキュリティ技術（M-Sec)の研究開発として、具体的には以下の5つの社会的および技術的目標をもってプロジェクトを推進する。
①新たな分散(decentralized) IoTアーキテクチャ
②人やモノ、サービス同士のシームレスで自律的かつセキュアなインタラクション技術
③新たなセキュリティ、トラスト、プライバシ保護技術
④分散IoTエコシステムのリファレンス実装
⑤社会的インパクトの最大化

プロジェクトの成果



M-Secを構成するすべてのレイヤにおいて、セキュリティを担保するための技術設計及びプロトタイプの実装を行った。

プロジェクトの成果

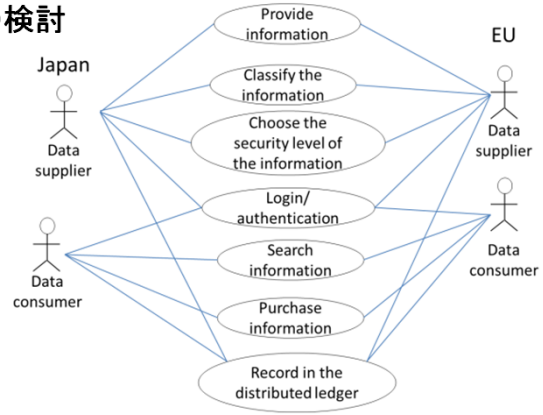
日欧それぞれの実証都市において、ユースケースに基づき実証実験を計画・調整し、M-Secが掲げる5つの社会的及び技術的目標と各ユースケースとの対応付けを行い、アプリケーション等の技術的要素の開発を進めた。主な実証実験の内容は以下の通りである。

ユースケース1（サンタンデール市）
スマートシティ向けのマルチレイヤセキュリティを備えた信頼性の高いIoTデバイス
ユースケース2（サンタンデール市）
健康的な独居高齢者のための在宅モニタリングと遠隔支援
ユースケース3（藤沢市）
自動車／参加型／仮想センシング技術による安全で信頼できる都市環境モニタリング

ユースケース4（藤沢市）
安全で信頼できるハイパーコネクテッド市民ケア
ユースケース5（クロスボーダー）
効果的な意思決定を実現するIoTサービスマーケットプレース
ユースケース6（クロスボーダー）
市民参加型センシング

Task2.1 M-Secユースケースの検討

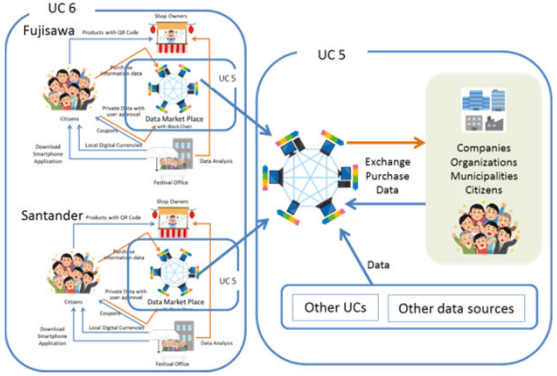
日欧それぞれの実証都市においてその地域のステークホルダー及び住民の課題分析結果から、どのようなデータを扱い、それらをどのように保護するかを考慮したユースケースの最新化を行った。



ユースケース5のUML図

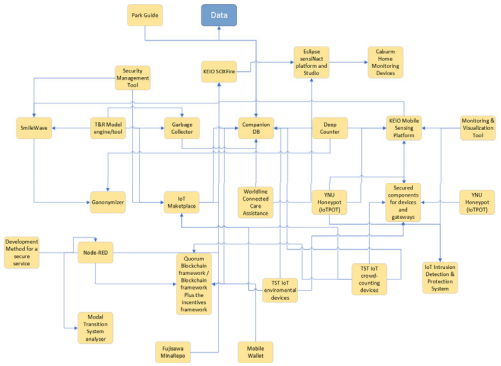
Task2.2 M-Sec実証実験の計画・実施、市民参加型の取り組み

策定した各ユースケースをテスト、検証するための計画、ステークホルダーエンゲージメントプラン、データ管理計画、倫理計画について各パイロット毎に検討し、フィールドトライアルを実施するうえでの調整を行った。



Crossborder ユースケースのイメージ

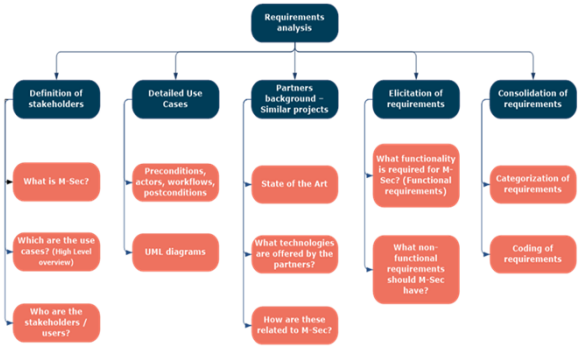
Task2.3 技術統合



M-SECの技術統合概観図

各タスクで研究開発を行う要素技術（アセット）を取りまとめ、各ユースケースで現在および今後行う技術間の統合を整理し、全体としてM-Secアーキテクチャを構成した。

Task3.1 システムレベル及びユーザレベルの要求の分析

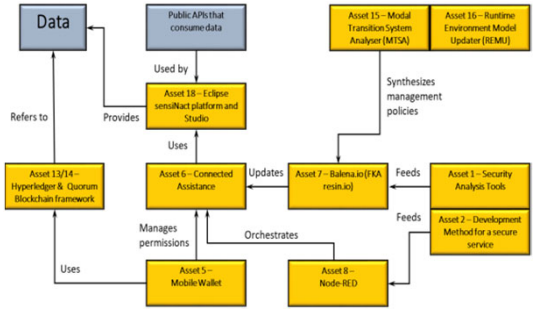


M-Sec要求分析のMethodology

M-SecユースケースとパイロットのWP2でのさらなる分析・検討に沿って，初版で取りまとめたM-Secフレームワークの機能要件とセキュリティ等の非機能要件の分析・検討をさらに進めた。

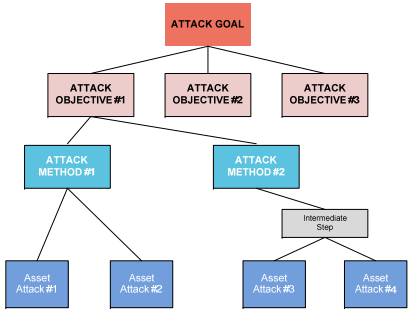
Task3.2 M-Secアーキテクチャ

各ユースケース毎にアーキテクチャに基づいたアセット間相互作用による実現方法を分析した。
その結果に基づき初期アーキテクチャの洗練化を実施した。



ユースケースを実現するアセット間相互作用

Task3.3 ハイパーコネクテッドスマートシティの要素技術

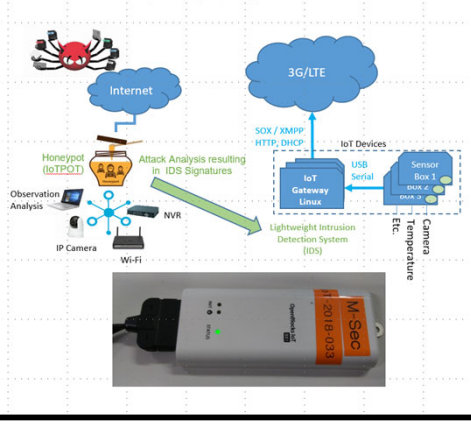


脅威/攻撃の整理に用いるツリー概念テンプレート

ハイパーコネクテッドスマートシティにおける、特にセキュリティの観点でのリスク分析を行った。欧州側研究機関とも連携し、ユースケースを具体的に念頭に置いた上でエッジ側、クラウド側、エンドツーエンドのデータ流通におけるリスクを、網羅的に整理・検討した。

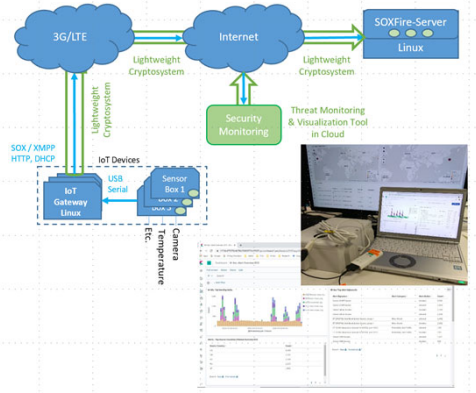
3. 研究開発の成果（続）

Task4.1 IoTセキュリティ



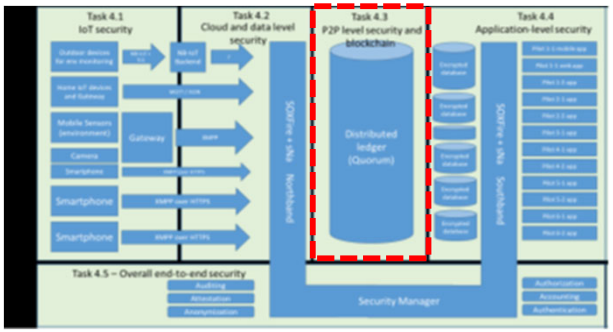
IoT機器向けの小型軽量なIDS (Intrusion Detection System) の設計、プロトタイプの実装を行った。
ハニーポットで得られた攻撃パターンを分析してシグネチャを作成、それを用いてIoTデバイスで外部からの侵入、攻撃を検出する機能を持つ。

Task4.2 クラウドおよびデータレベルセキュリティ



軽量な暗号化技術を用いて、IoTデバイスとクラウドの間で行われる通信の安全性を確保する技術と、センサで観測された攻撃通信の集約・可視化を行う技術（Visualization Tool for Security）の設計、プロトタイプ実装を行った。

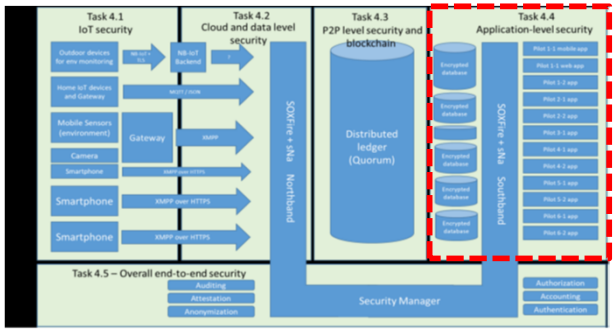
Task4.3 P2Pレベルのセキュリティとブロックチェーン



M-Secフレームワークの P2Pレベルのセキュリティとブロックチェーンについて、“Blockchain Framework and Middleware Services”と“IoT Marketplace”デモの設計・実装を行った。

M-Secの全体構成図（P2Pのレベルセキュリティとブロックチェーン）

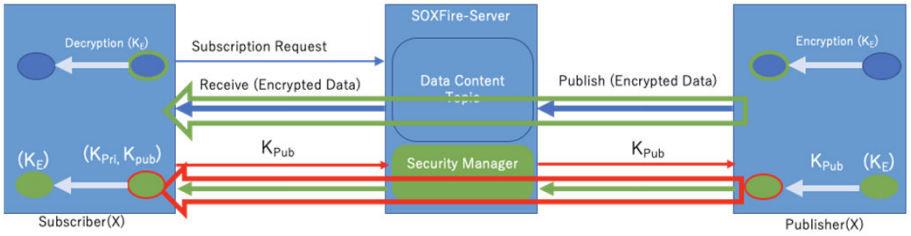
Task4.4 アプリケーションレベルのセキュリティ



M-Secフレームワークのアプリケーションレベルのセキュリティについて、“the Crypto Companion Database”と“Security Analysis Tool”デモの設計・実装を行った。

M-Secの全体構成図（アプリケーションンレベルセキュリティ）

Task4.5 エンド-エンドセキュリティ



Publish/subscribeに基づくセンサデータ流通基盤を介したエンドツーエンドの通信において、データ流通基盤に対する機密性を確保するため、publisherがsubscriberとの暗号鍵を用いて、送信データを暗号化する技術を研究開発した。

４．特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	標準化提案	プレスリリース 報道	展示会	受賞・表彰
0 (0)	0 (0)	7 (6)	41 (23)	0 (0)	1 (0)	2 (0)	0 (0)

※成果数は累計件数、(　)内は当該年度の件数です。

(1)標準化、利活用、GDPR遵守、コミュニティ形成、持続可能性関連活動について

標準化

標準化団体へのM-Sec紹介について欧州側と連携しながら適切な団体に対して効果的な提案活動を進める検討を行った。

利活用及び知財

M-Secソリューションの市場での活用方法および妥当性について検討した。競合機関及び製品の市場分析草案を実施し、それらから当プロジェクト成果物の強みと弱みを検討した。

GDPR遵守

GDPRの定義・分析に基づき、日本での個人情報保護法との相関関係を導き日本企業へのガイドライン策定への課題や、blockchainに関わるGDPR法規則の調査事項等を整理した。

コミュニティ形成、持続可能性関連活動

日本国内のコミュニティ活動として、「地域IoTと情報力研究コンソーシアム」の活動を継続推進した。

第3回シンポジウム開催、健康情報コンソーシアムとの合同シンポジウム、勉強会を開催(勉強会4回、WG3回)

(2)業界・一般に向けた発表・討論の実施

以下のように、業界・一般に向けた発表を実施した。

- 2019年9月13日 「第1回ブロックチェーンセキュリティ(BSEC)研究会」にて「M-Sec:ブロックチェーンを利用したハイパーコネクテッドスマートシティの研究開発」の講演を実施。
- 2020年1月23日 「第21回　クラウドセキュリティ研究会&海外展開研究会(サイバーセキュリティにおけるグローバル対応(国際連携、標準化))」にて、「Multi-layered Security Technologies for hyper-connected smart cities」の講演を実施。
- 2020年2月19日 「The 2nd International Workshop on Big data, cloud, and IoT technologies for smart cities (IWBigDataCity2020)」にて、「Big Data, Cloud and IoT Technologies for Smart Cities: The M-Sec project paradigm – objectives, current status and related future research topics」の発表を実施。

５．今後の研究開発計画

これまでに得られた日欧の技術的な成果を、今後の実証実験での活用や個々の技術要素間の連携により、さらに洗練、進化させ、実用化を目指した取り組みを行う。また、実証協力自治体である藤沢市及び関連する機関からのフィードバック等により得られた教訓を踏まえ、新たな課題の解決につながるようなプラットフォームやアプリケーション等の技術的要素の開発を進める。さらに、日欧連携実証であるクロスボーダー実証を計画・実施し、技術的要素の成果や効果、汎用性について評価を行っていく。

６．外国の実施機関

Worldline Iberia SA (スペイン)＜代表研究者＞、National Technical University of Atene(ギリシャ)、CEA-LETI(フランス)、F6S Network Limited(アイルランド)、Tecnologías, Servicios Telemáticos y Sistemas, S.A. (スペイン) 、Santander市(スペイン)