

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、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(39カ月間)
- ◆研究開発予算
- 総額186百万円(令和2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

WP3. 都市間の安全な共有、取引、連携を可能にするハイパーコネクテッドスマートシティプラットフォームアーキテクチャを構築

Secure Marketplaces

Smart City Applications

Smart City Platform

IoT Gateway

IoT Devices

City X, City Y, City Z

デジタルモデル/実定モデル以上

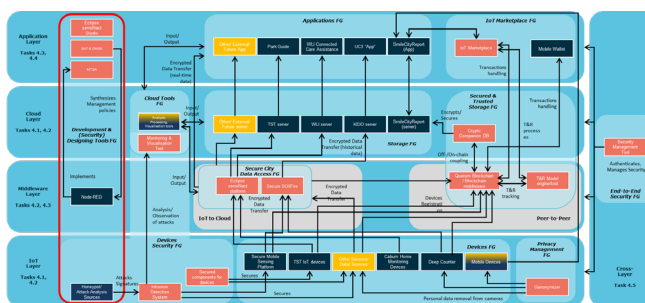
WP1.5. プロジェクト成果の普及展開のためにステークホルダーと連携しデータ保護、ビジネスモデル、コミュニティ形成など多面的な検討、展開を実施

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、プライバシー保護技術
- 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アーキテクチャを構成するアセットを相互に接続し、ユースケース毎の実証シナリオにおいて、どのコンポーネントを活用・実証するかのマッピングを洗練化し、M-Secアーキテクチャを定義した。



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実施し、コロナ禍の状況に合わせ調整を続け、M-Secプラットフォームを活用した実証シナリオを実施、検証をした。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(サンタンデル市)  
スマートシティパークを充実させる安全なIoT
- ユースケース2(サンタンデル市)  
高齢者を見守るセキュリティシステム
- ユースケース3(藤沢市)  
安全/信頼のモバイルセンシングプラットフォーム
- ユースケース4(クロスボーダー)  
感情を表す安全な参加型センシング
- ユースケース5(クロスボーダー)  
スマートシティデータマーケットプレイス



3. 研究開発の成果(続)

Task2.2 M-Sec実証実験の計画・実施、市民参加型の取り組み

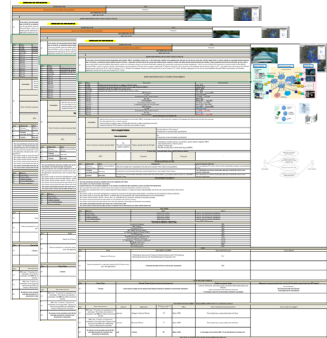
策定した各ユースケースをテスト、検証するため計画、ステークホルダーエンゲージメントプラン、データ管理計画、倫理計画について各パイロット毎に当初の予定からコロナ禍の状況に合わせ再度検討し、フィールドトライアルを実施、検証した。



藤沢市でのフィールドトライアル

Task2.4 システム全体の妥当性確認と評価

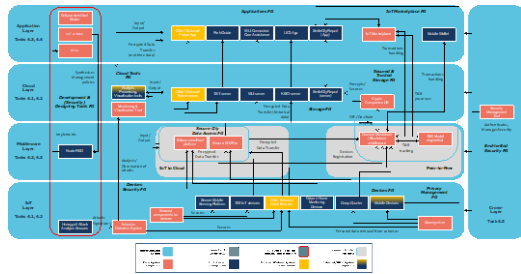
最終年度に実施するパイロットシステムの妥当性確認・評価に向けて、実証シナリオの洗練化に対応して各パイロットで評価するKPIの再検討、洗練化を行った。



実証シナリオごとのKPI

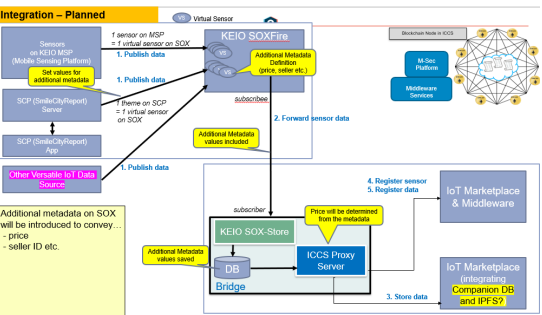
Task3.2 M-Secアーキテクチャ

初期のM-Secアーキテクチャに対して実証シナリオ毎に対応を検討、洗練化することでM-Secアーキテクチャを定義した。



M-Secアーキテクチャ

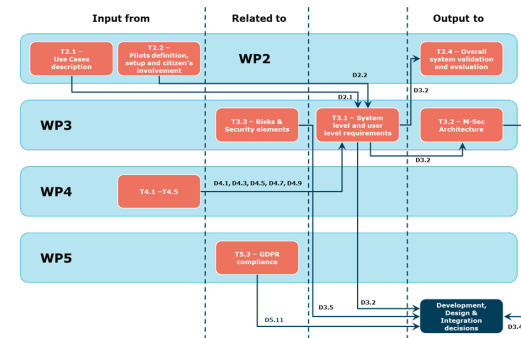
Task2.3 技術統合



M-SecソリューションとMarketPlaceのインテグレーション

各タスクで研究開発を行う要素技術を取りまとめ、全体としてM-Secアーキテクチャを構成した。特にUC3ではYNUのセキュリティ技術、ICCSのMarketPlaceとの連携により、M-Secプロジェクトとしての全体アーキテクチャ実現に貢献した。

Task3.1 システムレベル及びユーザーレベルの要求の分析



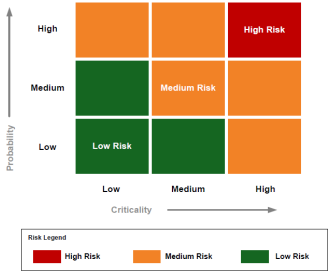
M-Sec要求分析と他のTaskとの関連

M-Secプラットフォーム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、他のWPのTaskと連携してさらに進め、システムレベル及びユーザーレベルの要求の最終版の取りまとめを完了した。

Task3.3 ハイパーコネクテッドスマートシティの要素技術

| RISK RATING | RISK   | ACTION REQUIRED                                               |
|-------------|--------|---------------------------------------------------------------|
| 1-3         | LOW    | ACCEPT RISK                                                   |
| 4-10        | MEDIUM | MANAGE BY ROUTINE PROCEDURES AND EXISTING POLICIES/PROCEDURES |
| 11-20       | HIGH   | ACTION REQUIRED                                               |

A visual representation of these Risk Bands is depicted in Figure 3.

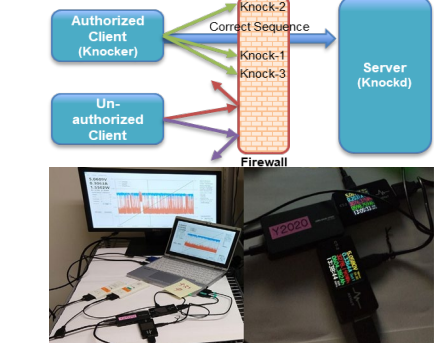


Risk Bands

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の結果をTST, YNUと連携して報告書D3.5としてまとめた。リスク分析を行うにあたっては欧州側研究機関とも連携し、特にユースケースを具体的に念頭に置いた視点からエッジ側、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検討した。

3. 研究開発の成果(続)

Task4.1 IoTセキュリティ



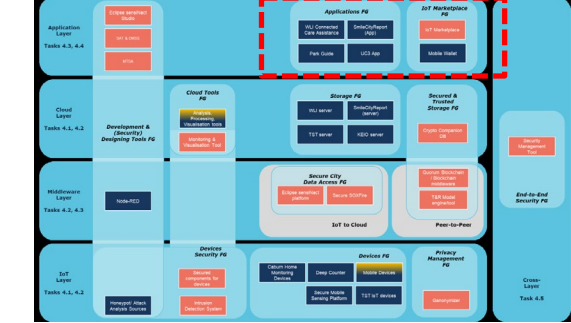
Port knocking methodologyと研究室での実験

藤沢市でのPilot-1では、攻撃通信の90%以上をブロックするというUse-Case3目標(D2.3.2)を達成した。更に攻撃通信の完全ブロックを目指し、ステルスセキュリティ機能を介して安全なリモートアクセスを追加してセキュリティを強化する手法を開発した。この機能は、ポートを非表示に保ち、正しいシークレットログインシーケンスを受信したときにのみポートを開くもので、Pilot-2で適用評価する。

Task4.2 クラウドおよびデータレベルセキュリティ



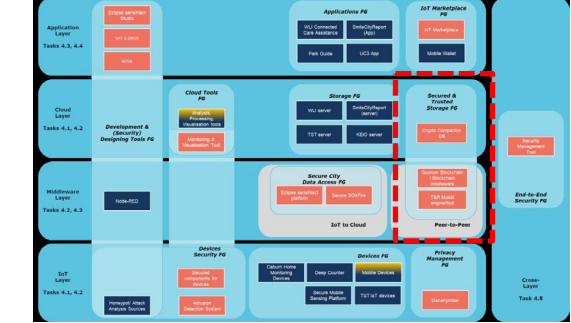
Task4.4 アプリケーションレベルのセキュリティ



M-Secフレームワーク階層毎の構成(アプリケーションレベルセキュリティ)

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、“IoT Marketplace”, “Modal System Transition Analyzer”及び“Security Analysis Tool”の設計・実装を完了した。

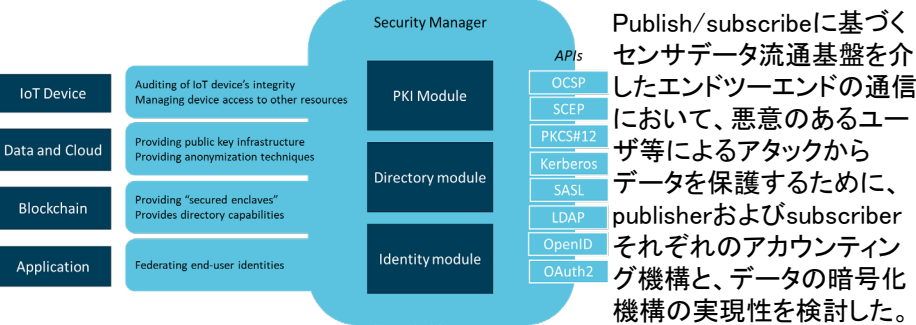
Task4.3 P2Pレベルのセキュリティとブロックチェーン



M-Secフレームワーク階層毎の構成(P2Pのレベル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”の設計・実装を完了した。

Task4.5 エンド-エンドセキュリティ



M-Secの各レイヤの取組みを持つセキュリティ・マネージャーのアーキテクチャ

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、悪意のあるユーザ等によるアタックからデータを保護するために、publisherおよびsubscriberそれぞれのアカウントング機構と、データの暗号化機構の実現性を検討した。

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・採択 | プレスリリース<br>報道 | 展示会      | 受賞・表彰    |
|----------|----------|-----------|------------|----------|---------------|----------|----------|
| 0<br>(0) | 0<br>(0) | 12<br>(5) | 56<br>(14) | 0<br>(0) | 1<br>(0)      | 4<br>(2) | 0<br>(0) |

(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 ※成果数は累計件数、( )内は当該年度の件数です。

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や紹介を行った。

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。特に中小規模で競合となり得るIoTプラットフォーム及び提供企業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、クロスボーダーユースケースに関わる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。

コンソメンバーと具体的に連携してコロナ対策として藤沢市内の飲食店10店舗にCO2センサーを設置し、来年度に向けた実証の準備を実施した。

(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。

- 2020年5月22日 「Coimbra Sustainability Summit」にて、「M-Secプロジェクト」について講演を実施。
- 2020年7月27日 「地域IoTと情報力研究コンソーシアム」にて、「M-Secの紹介」と「IoTにおけるサイバー攻撃の最新動向とその対策について」講演を実施。
- 2020年8月26日 「第89回情報通信研究会」にて、「M-Secの紹介」と「IoTにおけるサイバー攻撃の最新動向とその対策について」講演を実施。
- 2020年11月25日 「GDPR & APPI: regulatory challenges in modern smart cities」にて、GDPRとAPPIの相互認証及び差異について講演を実施。
- 2021年1月 ITU協会のオンライン月刊誌「ITUジャーナル」へ「M-Secプロジェクトの紹介」を寄稿

5. 今後の研究開発計画

これまでの実証実験で得られたデータの分析を行い、各実証実験にマッピングされた日欧の技術要素間の連携が円滑に機能して利用されているかを検証するとともにクロスボーダー実証を実施し、成果や効果、汎用性について評価を行う。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、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をさらに洗練、進化させ、実用化を目指した取り組みを行う。

6. 外国の実施機関

Worldline Iberia SA (スペイン)、National Technical University of Athens (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)