



Multi-layered Security Technologies

for hyper-connected
smart cities

ハイパーコネクテッド社会のための
マルチレイヤーセキュリティ技術の研究開発



A EU-Japan collaboration

Funded by European Commission and NICT^{*1}

2020年8月28日
日本ITU協会 第89回情報通信研究会

東日本電信電話株式会社
道口恵子

^{*1} National Institute of Information and Communications Technology in Japan



Table of Contents

1. M-Sec is... (プロジェクト概要)
2. Use Cases (ユースケース)
3. Challenges (課題／悩みごと)

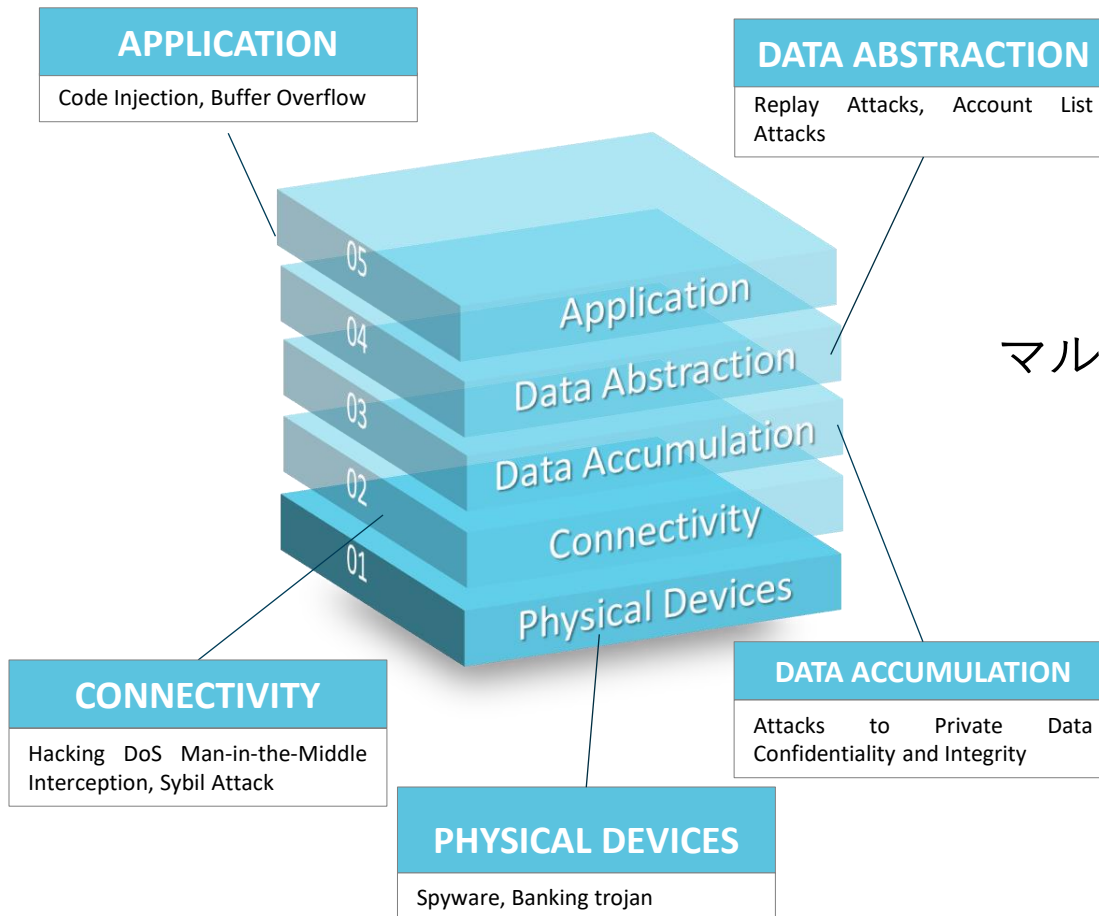


M-SEC IS...

NOT JUST ANOTHER EU-JP PROJECT



Multi-Layerd Security Technologies for Hyper-Connected Smart City



ハイパーコネクテッド社会のための
マルチレイヤーセキュリティ技術の研究開発



M-Sec goals

M-Secプロジェクトの主な目的はハイパーコネクテッドスマートシティを保証する**マルチレイヤセキュリティ技術**を研究、開発、展開、実証すること、また、ブロックチェーン、ビッグデータ、クラウド、IoTのセキュリティを活用した革新的なプラットフォームを通じてIoTのステークホルダーが革新的なスマートシティアプリケーションを構築することを可能にすること

We use innovative technologies in our smart city solutions



Cloud



IoT



Device level



Big Data
security



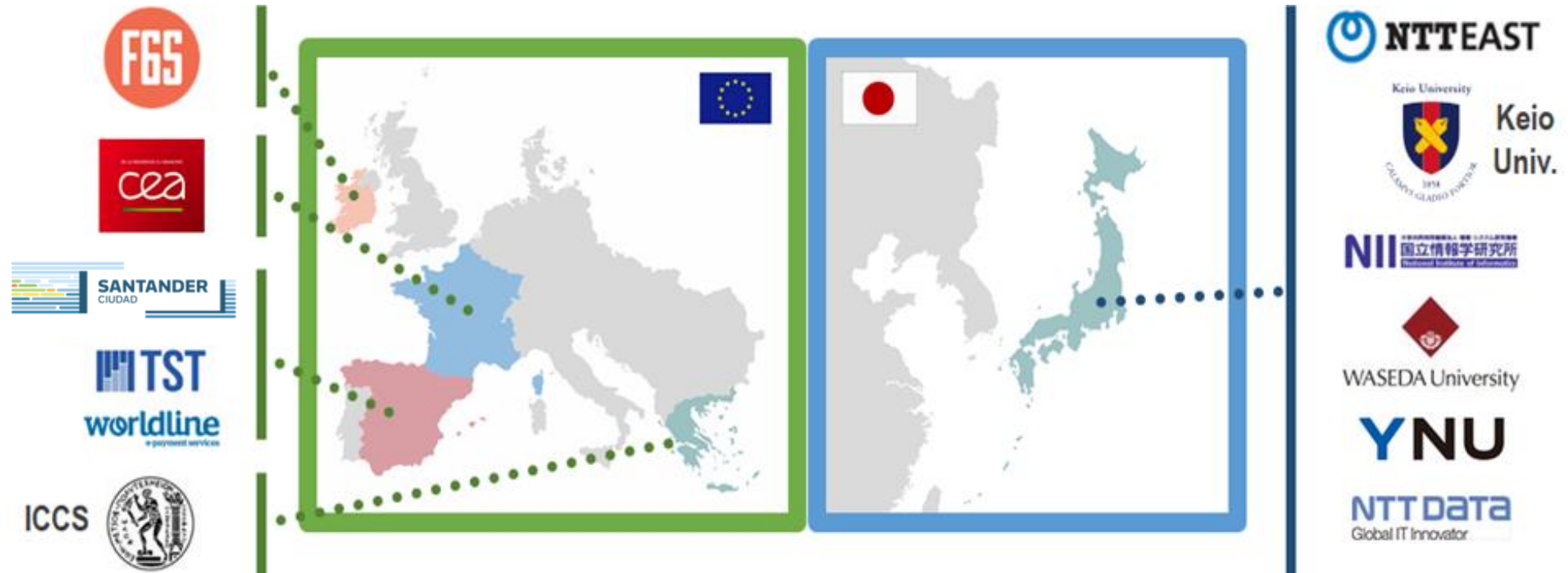
Blockchains



End to End
security

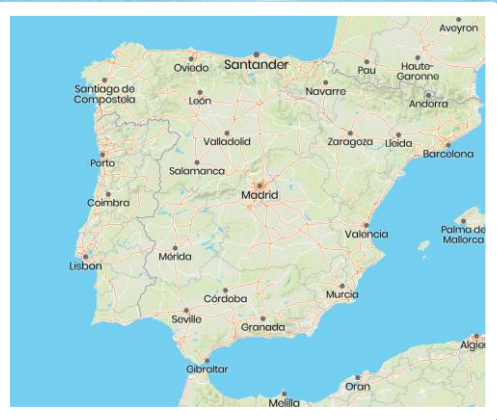


M-Sec Consortium as a whole





実証都市：神奈川県藤沢市

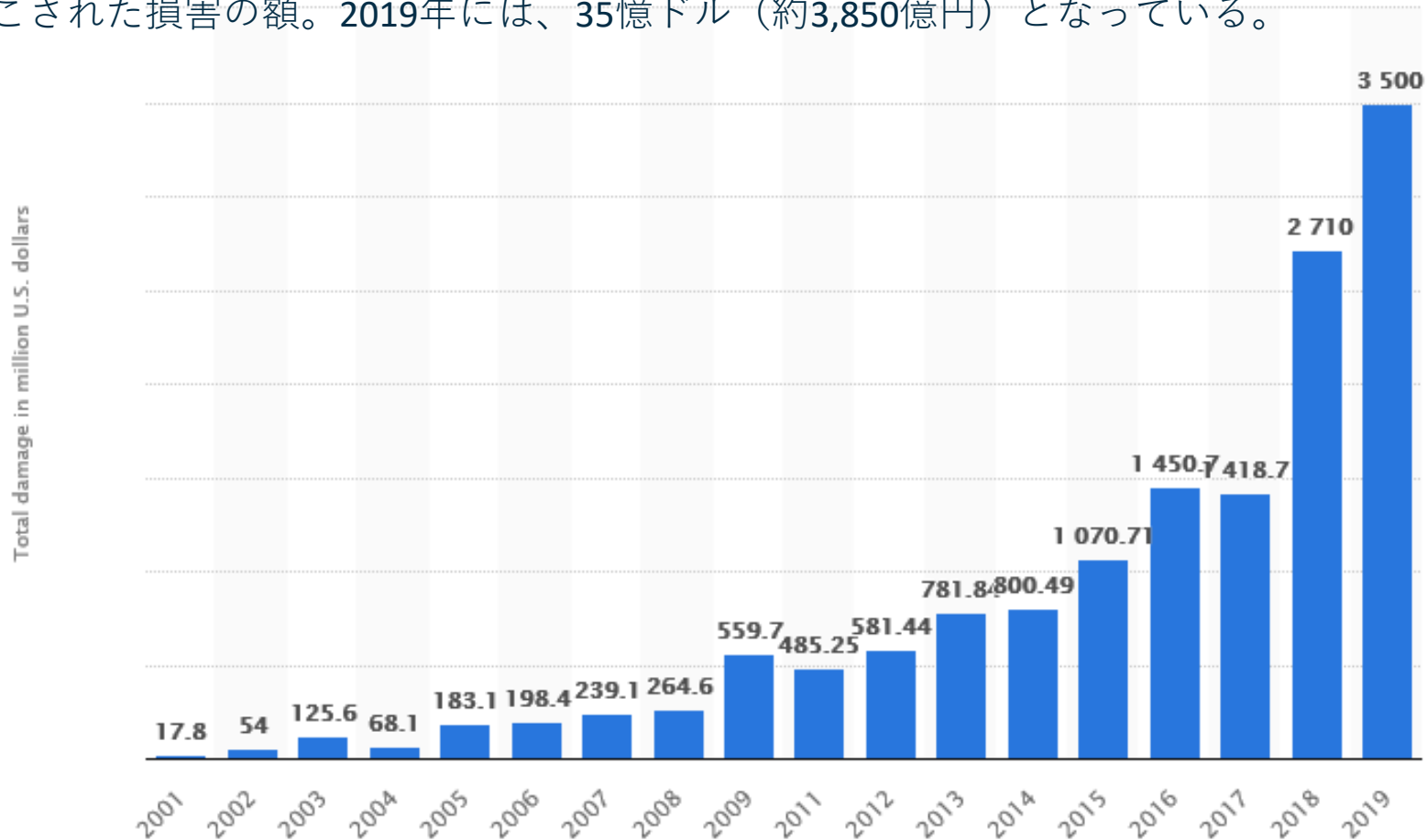


実証都市：スペイン サンタンデル市



Total Damage Caused by Reported Cyber Crime in the US

2001年から2019年にIC3（米国政府Internet Crime Complaint Center）に報告されたサイバー犯罪によって引き起こされた損害の額。2019年には、35憶ドル（約3,850億円）となっている。





セキュリティ10大脅威

昨年	個人	順位	組織	昨年
1位 ^(*1)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者への被害	3位	ランサムウェアによる被害	2位
NEW	メール等を使った脅迫詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT機器の不適切な管理	10位	不注意による情報漏えい	12位

「情報セキュリティ10大脅威 2019」は、2018年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約120名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したもの

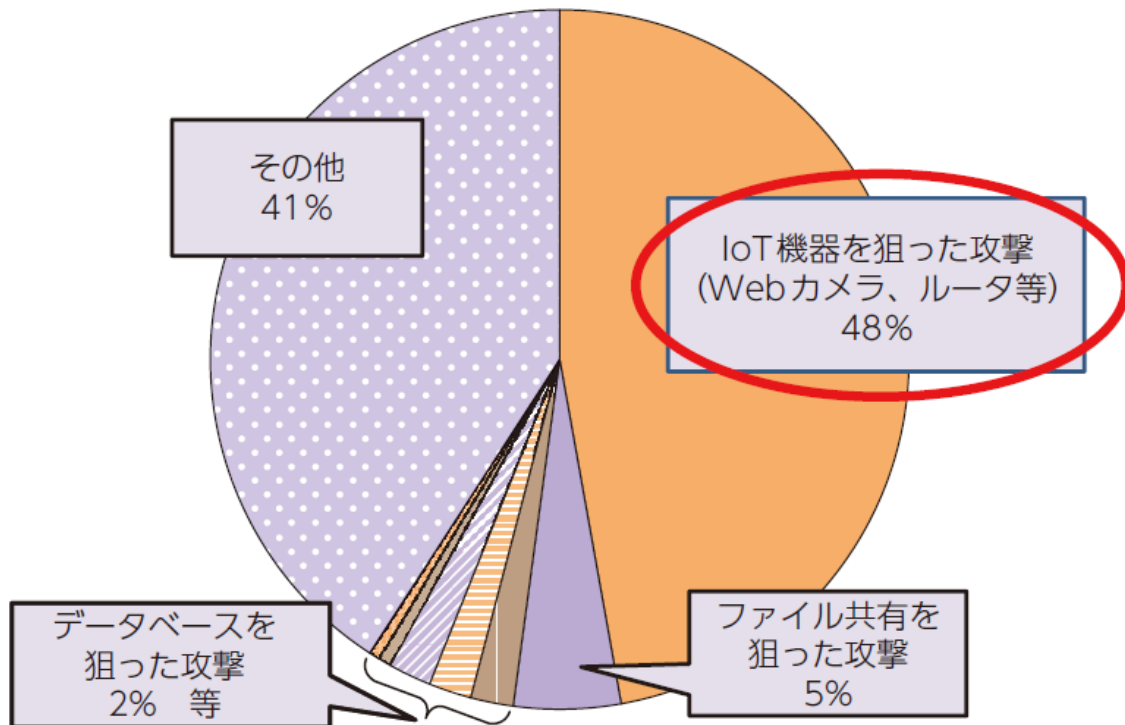
(*1) クレジットカード被害の増加とフィッシング手口の多様化に鑑み、2018年個人1位の「インターネットバンキングやクレジットカード情報等の不正利用」を本年から、①インターネットバンキングの不正利用、②クレジットカード情報の不正利用、③仮想通貨交換所を狙った攻撃、④仮想通貨採掘に加担させる手口、⑤フィッシングによる個人情報等の詐取、に分割。

情報処理通信機構 情報セキュリティ10大脅威 2019より <https://www.ipa.go.jp/security/vuln/10threats2019.html>



Attacks towards IoT Devices

約半数がIoT機器を狙った攻撃



NICTが運用するサイバー攻撃観測網（NICTER）が2018年（平成30年）に観測したサイバー攻撃パケット2,121億パケットのうち、約半数がIoT機器を狙ったものであるという結果が示されている

- * 1 NICTERで観測されたパケットのうち、サービスの種類（ポート番号）ごとに割合の多い上位から30位までを分析したもの。
- * 2 IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。



M-SEC USE CASES

AND THEIR SUBTLETIES



List of Use Cases

	Titles	City
Use Case 1 Pilot 1	Secured IoT devices to enrich strolls across smart city parks スマートシティパークを充実させる安全なIoT	Santander
Use Case 2 Pilot 2	Home Monitoring Security System for ageing people 高齢者を見守るセキュリティシステム	Santander
Use Case 3 Pilot 3	Secure and Trustworthy Mobile Sensing Platform 安全/信頼のモバイルセンシングプラットフォーム	Fujisawa
Use Case 4 Pilot 4	Secure Affective Participatory Sensing of City Events (cross-border) 感情を表す安全な参加型センシング	Fujisawa & Santander
Use Case 5 Pilot 5	Smart City Data Marketplace with secure Multi-layer Technologies スマートシティデータのマーケットプレイス	Fujisawa & Santander



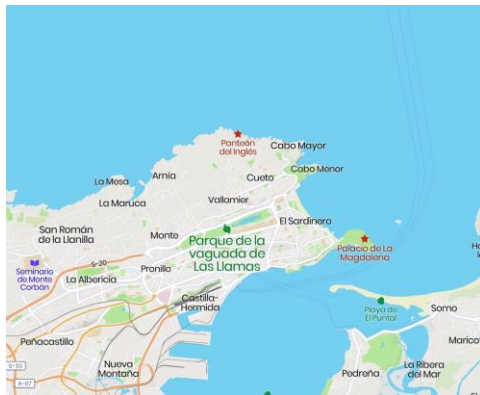


USE CASE 1

SECURED IOT DEVICES TO ENRICH STROLLS ACROSS SMART CITY PARKS



Lovely view of Las Llamas Park in **Santander**



**Pilot will be implemented
starting August '20**

スマートシティパークを充実させる安全なIoT

サンタnder市内の公園にIoTセンサーを設置し、騒音や人の混雑状況など、市民が快適に公園を利用するために役立つ情報の収集、その情報をWebアプリにより提供する。

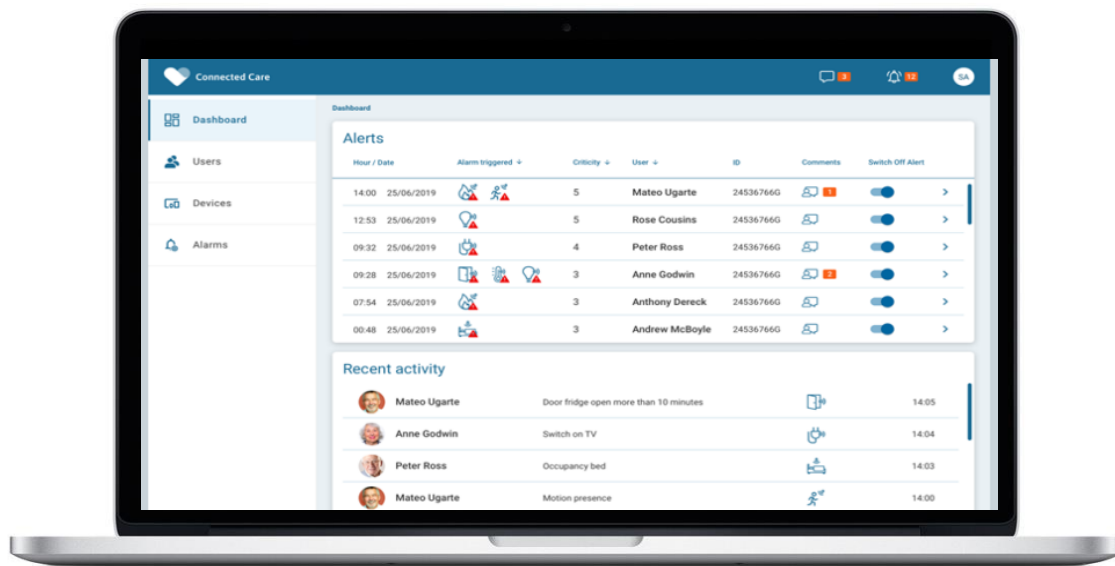
Webアプリを使用すると、ユーザーは公園の状況を確認することができる。さらに、自治体もこの情報を活用することにより、園内のサービス向上につなげる

これらのデータが正しく、安全な環境で取り扱えるかを検証する。



USE CASE 2

HOME MONITORING SECURITY SYSTEM FOR AGEING PEOPLE



Connected Care Dashboard

高齢者を見守るセキュリティシステム

コネクテッドケアは、独居高齢者を対象とした遠隔支援サービスプロバイダー向けのリモートホームアクティビティー監視システムである。

高齢者の自宅にて設置されたセンサーにより、対象者の活動を監視し、支援が必要かどうかの意思決定をサポートする。それらの関連するセンサー、健康機器などが安全な環境で活用できるかを実証する。

Pilot will be implemented from August 20'-October 20'



USE CASE 3

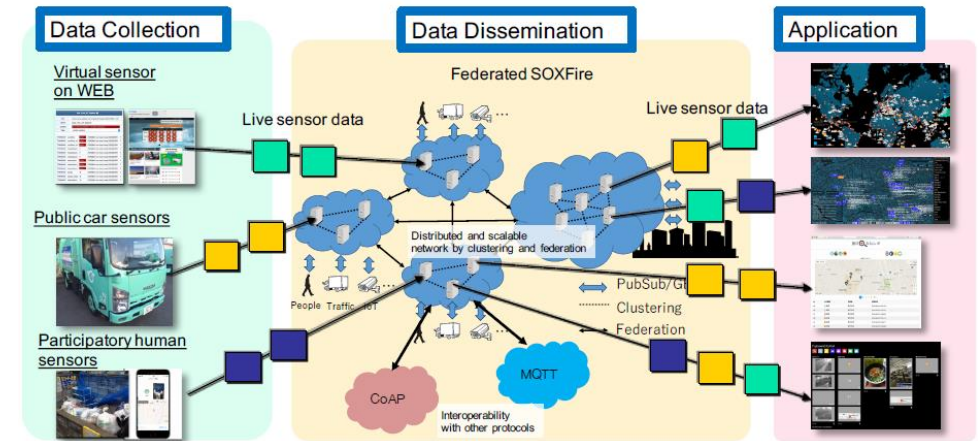
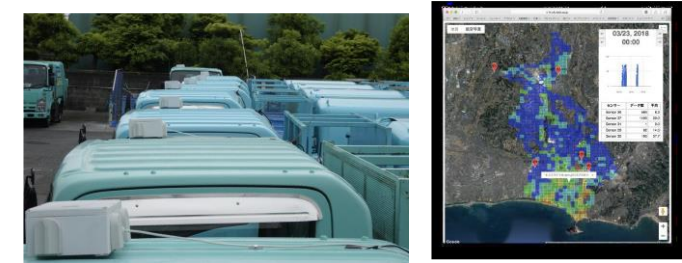
SECURE AND TRUSTWORTHY ENVIRONMENT MONITORING

安全/信頼のモバイルセンシングプラットフォーム

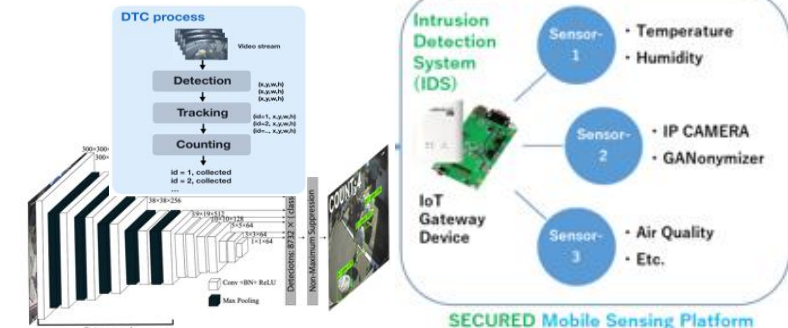
神奈川県藤沢市の清掃車に環境データを測定するセンサーを取り付け、環境データ（空気の質、温度/湿度、ごみの処分量、障害のない道路標識など）を視覚化できるアプリケーション実装の実証をする。

スマートシティのプラットフォーム上で都市データを共有するためには、プライバシー保護とセキュリティ保証のメカニズムが不可欠だが、既存のプラットフォームでは依然としてプライバシー保護とセキュリティ保証に問題がある。

プライバシーを保護するため、画像データからプライバシー情報を自動的に削除できるGANonymizerを活用や、IoTデバイスとクラウド間の暗号化メカニズム（TLS）、クラウド内の高度な認証メカニズム、さらに、エンドツーエンドのセンサーデータストリーム配信は、軽量の暗号化メカニズムによって保護される。



Privacy protected and Secured enhanced by M-Sec assets



USE CASE 4



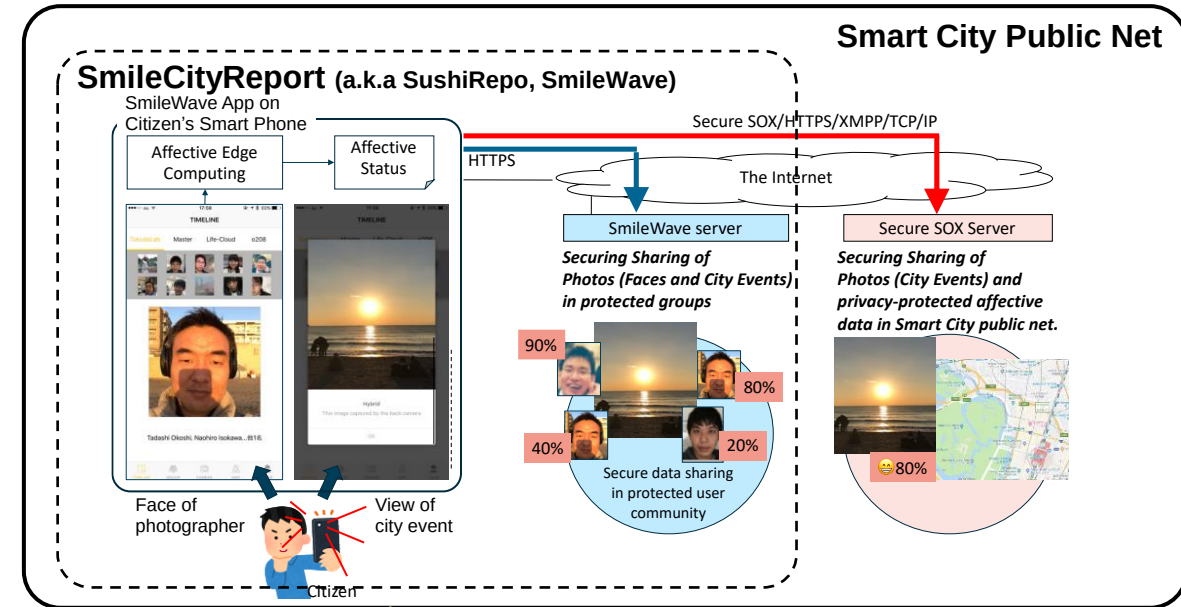
SECURE AFFECTIVE PARTICIPATORY SENSING OF CITY EVENT (Crossborder)

感情を表す安全な参加型センシング

特定のテーマ（都市のスポット、美食など）の写真を交換できるアプリケーション「SmileCityReport」を使用して、市民の感情的な情報と都市の情報を安全に共有する可能性を、サントアンデルおよび藤沢で検証する。

既存のスマートシティプラットフォームでは、プライバシー保護やセキュリティ保護の観点から、市民が情報交換や安心して参加できる環境の実現が難しい。

本実証では、プライバシー保護されたモバイル参加型センシングプラットフォームを開発、市民が近隣（都市）の情報や特定のテーマに沿った写真などを、感情的なステータス情報を添付して共有することにより、情報の活用を促進できるかを検証する。これらの情報は、適切なプライバシー保護メカニズムによって市民のコミュニティ間で安全に共有される。



USE CASE 5



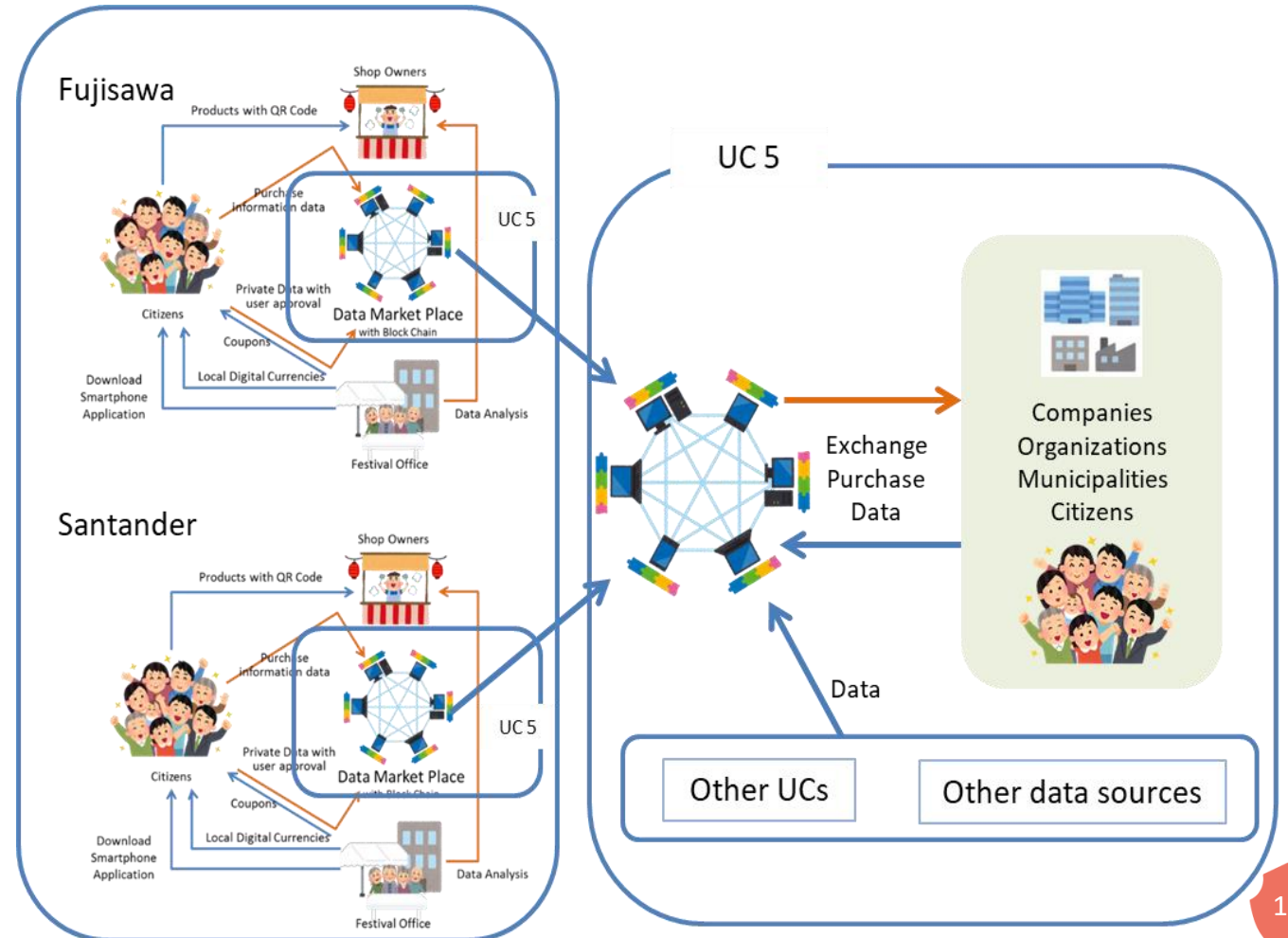
Smart City Data Marketplace with secure Multi-layer Technologies (Crossborder)

スマートシティデータのマーケットプレイス

様々なデータが、GDPR/APPIのルールに従いながら、データの機密性、正確性、プライバシー保護が担保された環境で取引できるような、データマーケットプレイスを構築、サンタンデル、藤沢両都市で、その有効性を検証する。

インターネットの発達に伴い、サイバー攻撃はますます複雑化・高度化しており、スマートシティにとって国間の安全なデータ配信方法の提供は不可欠な課題である。

このユースケースでは、ネット上でのデータ取引に関わるすべてのレイヤーにおいて、セキュリティを担保することにより、市民、企業、自治体などといったユーザーが安心してデータの売買ができる環境の構築を目指す。





Challenges

WHAT WE ARE FACING



課題

1. 言葉や文化の壁

- ✓ お互い訛りがあって聞き取りづらい、考え方がわからない

2. 成果の普及展開が難しい

- ✓ ビジネスモデル

3. コロナ禍で、

- ✓ F2Fミーティングができない

- ✓ 実証実験ができない

- ◆ 藤沢実証では、ちょいのみフェスティバルとの連携により参加者を集めようとしていたが、コロナの影響でフェスティバル自体が実施されず、実証延期が続いている。スペインも同じ。
- ◆ オフラインでの実証アイデアを模索中。



Do you want to know more?



<https://www.msecproject.eu/>



....and don't forget to follow us on



linkedin.com/company/msecproject

M-Sec
Internet · Barcelona, Barcelona · 41 seguidores

Registrarse

Ver los 4 empleados en LinkedIn →

Inicio

Acerca de

Empleos

Personas

Videos

Anuncios

Todo Imágenes Documentos Videos Ordenar por: Principales

M-Sec
41 seguidores
1 semana ·

Coimbra Sustainability Summit online event is coming closer!

The online summit will explore growth opportunities at the intersection of technology and innovation ecosystems. ... ver más

Ver traducción

Your dream job is closer than you think

See jobs

Linked in

SUSTAINABLE GROWTH AT THE INTERSECTION OF TECHNOLOGY AND INNOVATION ECOSYSTEMS



[@MSecProject](https://twitter.com/MSecProject)

M-Sec
Improving the security and connectivity of smart cities

Follow

M-Sec Project
@MSecProject

An EU-Japan collaboration 🇪🇺 🇯🇵 empowering researchers/govs/ businesses/citizens to create #IoT #BigData #Cloud tech & improve well-being in #smartcities. #H2020

📍 EU + Japan 📅 Joined September 2018

757 Following 727 Followers

Tweets Tweets & replies Media Likes

M-Sec Project Retweeted

TST / IoT solutions @TSTsistemas · Apr 29

Cuarta reunión plenaria de @MSecProject, esta vez por vía telemática. El encuentro ha servido para evaluar el impacto de la Covid-19 en la ejecución de los casos de uso del proyecto, y sus correspondientes pilotos 📝 Crónica en nuestro blog tst-sistemas.es/la-covid-19-pr...



Multi-layered
Security
Technologies
for hyper-connected
smart cities

Thank you!



www.msecproject.eu



www.f6s.com/iot



[@MSecProject](https://twitter.com/MSecProject)



linkedin.com/company/msecproject

Worldline



TST



NTTEAST



YNU



NTT DATA
Trusted Global Innovator

The M-Sec project is jointly funded by the European Union's Horizon 2020 research and innovation programme (contract No. 814917) and by the Commissioned Research of National Institute of Information and Communications Technology (NICT), JAPAN (contract No. 19501).