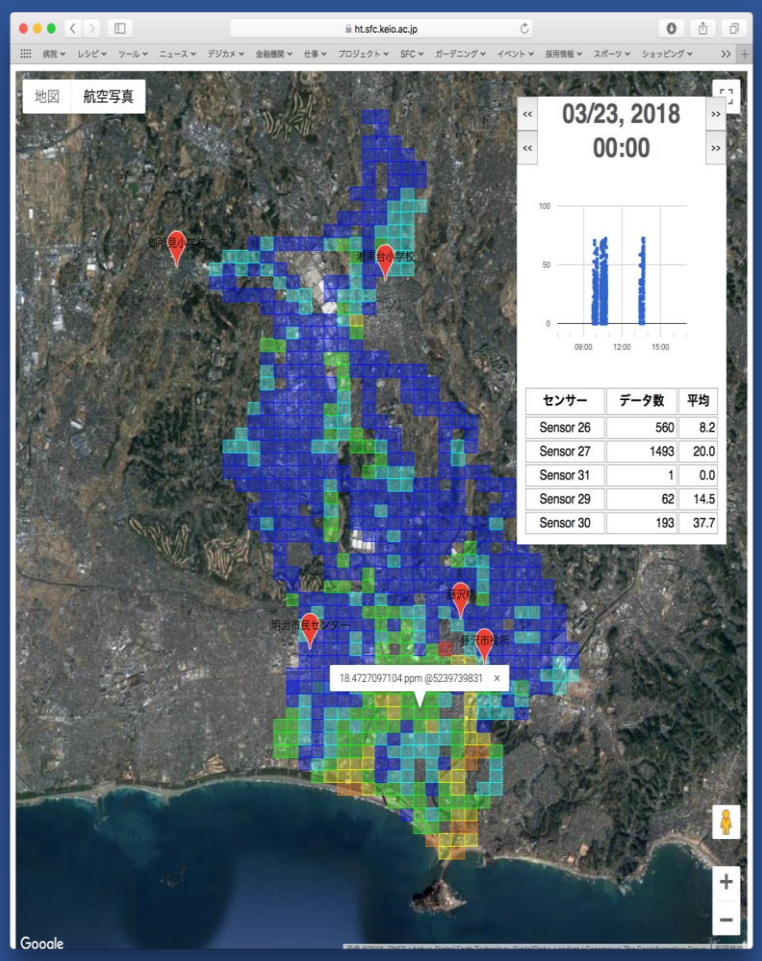
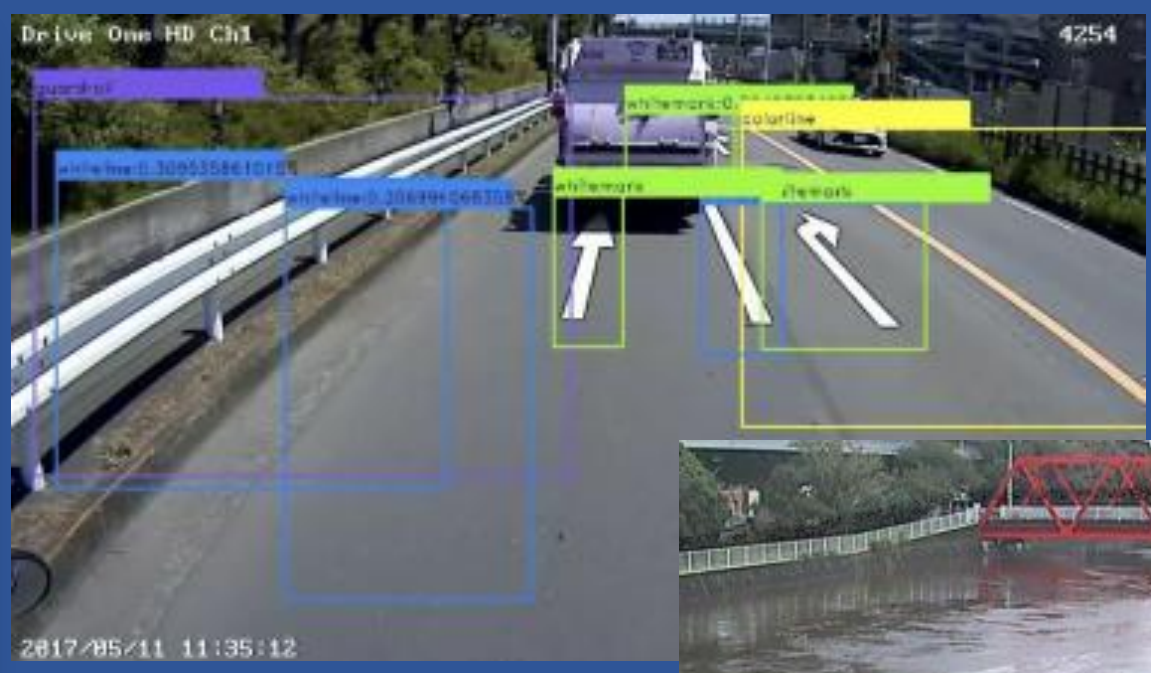
M-Sec

SECURE AND TRUSTWORTHY MOBILE SENSING PLATFORM

Environment Monitoring





Environment monitoring is one of the major tasks of local government. Better serving citizens with live environment data contributes to wellbeing of the society. This use case illustrates how environment monitoring data can be captured from the real world, handled in the cloud system, and delivered to citizens securely.

Environment sensing data, namely sensor data and camera images, are encrypted so that they are not tampered. IoT devices and cloud systems are monitored to protect them from malicious attackers.

The data is, in case they are provided to applications in an open fashion, disseminated through the data marketplace leveraging the Blockchain mechanism. In all, data authenticity, data security, IoT device security, and cloud systems security are achieved to ensure secure and trustworthy environment sensing and data dissemination. The data is provided to (1) city government in encrypted form and (2) a number of applications via the marketplace.

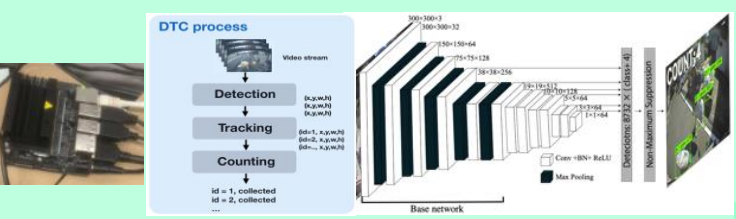
Multi-layered Security Technologies for hyper-connected smart cities

A EU-Japan collaboration

SECURE & TRUSTWOTHY MOBILE SENSING PLATFORM

DETECTING ENVIRONMENT DATA BY GURBAGE TRUCKS RUNNING AROUND THE CITY
SENSORIZER THAT CAN HANDLE EVERYTHING AS SENSOR DATA
FLEXIBLE AND SCALABLE DATA DISTRIBUTION PLATFORM “SOXFire”
BASED ON SECURE DATA HANDLING TECHNOLOGIES

Keio Mobile Sensing



Real time Deep Learning on Edge device

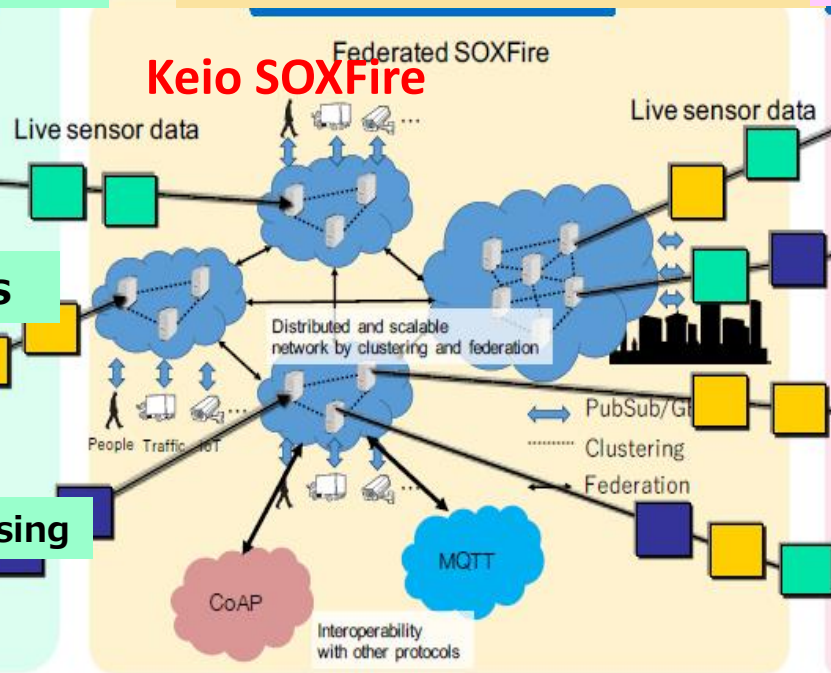
① Collect Data

Web Data

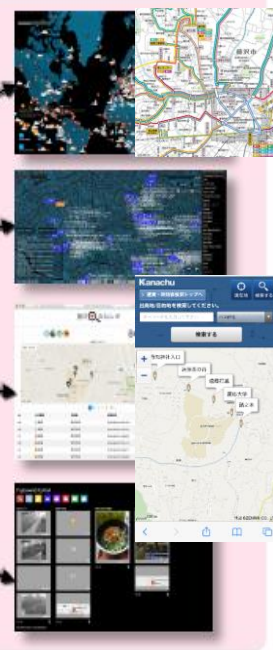
IoT Sensors

Participatory Sensing

② Deliver effectively



③Value



M-Sec End-to-end Security Protection

security monitoring, stealth security, encryption, an advance authentication mechanism

With this "Keio SOXFire" as the core, UC3 uses not only information from IoT sensors and edge devices, but also scraped Web data and various information input from smartphones as participatory sensing as if it were sensor data. And M-Sec's End-to-End Security technology enables these data to be shared safely, securely, flexibly and scalable between global cities.

M-SEC AS A SOLUTION TO THE GREAT CHALLENGE IN PRIVACY & SECURITY

・Secure Mobile Sensing Platform

In this use case, the environment sensing data from the garbage truck is input, and **Secure SOXFire**, which is a secure data distribution platform, is used as the core to provide **Secure Mobile Sensing Platform** as a secure data distribution core for smart cities.

・Secure Edge Device Processing

By avoiding uploading image data to the cloud as much as possible, advanced image processing including deep learning can **be processed on the edge device side** without unnecessary uploading of privacy data. In this use case, the **Deep Counter**, which automatically counts the discharged garbage, is a specific example.

・Multi-Layerd Security

The IoT devices (sensors), the cloud system (servers of a sensor data exchange platform), and applications consuming sensor data streams included in the mobile sensing platform are extended with **Multi-Layerd security** mechanisms.

・Blockchain-ready system

The data generated by the whole service, properly encrypted, is complemented by blockchain-related features available to users through the web application.

・A Marketplace to monetize anonymous data

Data that is not personal or sensitive is sent automatically to the M-Sec Marketplace prepared to provide a secure IoT data exchange environment. This Marketplace includes a Trust&Reputation component capable to evaluate the actual content being shared.

Multi-layered Security Technologies for hyper-connected smart cities

A EU-Japan collaboration

UNIQUE VALUE PROPOSITION

Flexible Sensor Network Everything as a sensor

Friendly (no technical skills required)

Scalable

System Resilience

End to End Security

FOR WHOM MAY BE USEFUL?

Are you an IoT Provider and want to partner to expand your business?

Are you the Municipal Service and want to provide innovative secure solutions for citizens?

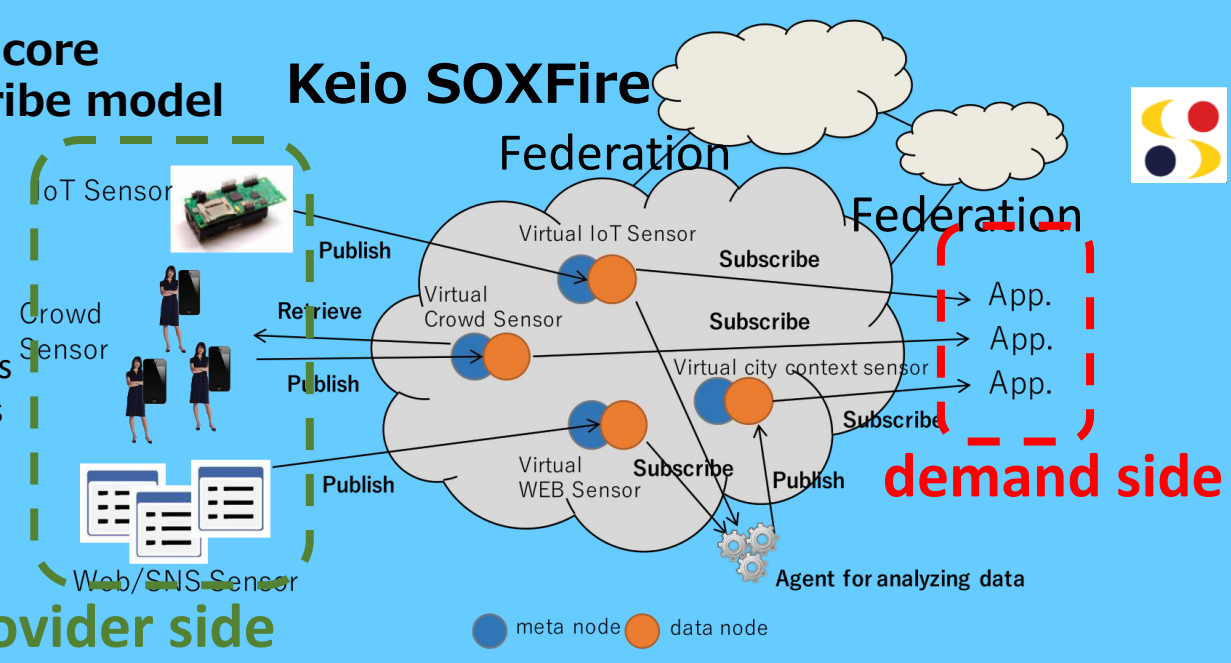
Are you a citizen and want to know more about how these types of solutions can help on your daily life?

PILOT TESTIMONY

"Keio SOXFire" is not a sensor network that is conscious of the other party like the conventional IoT system, but it enables matching between the data provider side and the data demand side without being conscious of the other party. It is possible to build a platform for horizontally deployed smart cities that enables data sharing between truly global cities.

IoT data matching core based on publish subscribe model

- ✓ Coping with various physical/virtual sensors
- ✓ Providing unified APIs for various languages
- ✓ Flexible Data Sharing



http://www.sfcity.jp

ABOUT M-SEC

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).

The M-Sec consortium is a strong partnership of leading European and Japanese universities and research centers as well as companies in the area of Big Data, IoT, Cloud Computing, Blockchain and all of them have an extensive experience in smart city related projects.

The overall M-Sec consortium is made of 12 partners, 6 from 4 different European countries (France, Spain, Greece, Ireland) and 6 from Japan.

One of the main results of the project is based on providing a set of components that provide security and integrity of data traffic, end to end, from the device to the Cloud and to the application in a secure and transparent way, with a modular approach for the IoT and Smart City domain.