Continuous Security Protection by Selection Technology for Trustworthy Connection

FUJITSU LIMITED

Continuous security protection in the application of the selection technology for trustworthy connection to the local government subsidy project is introduced.

Application Area

Semiconductor / Packaging	IoT	ICT vendor
Manufacturer	Infrastructure	Distribution
Local Government	Building / Smart City	

Technology Features

■ Homogenizing security measures for local government project networks

- Automated threat detection, analysis/visualization, and primary countermeasures at each company's site participating in the subsidy project
- Automate deployment to other companies participating in the subsidy project, and homogenize measures for the entire system

Effects

■ Preventing delays in the implementation of subsidies due to increased security damage

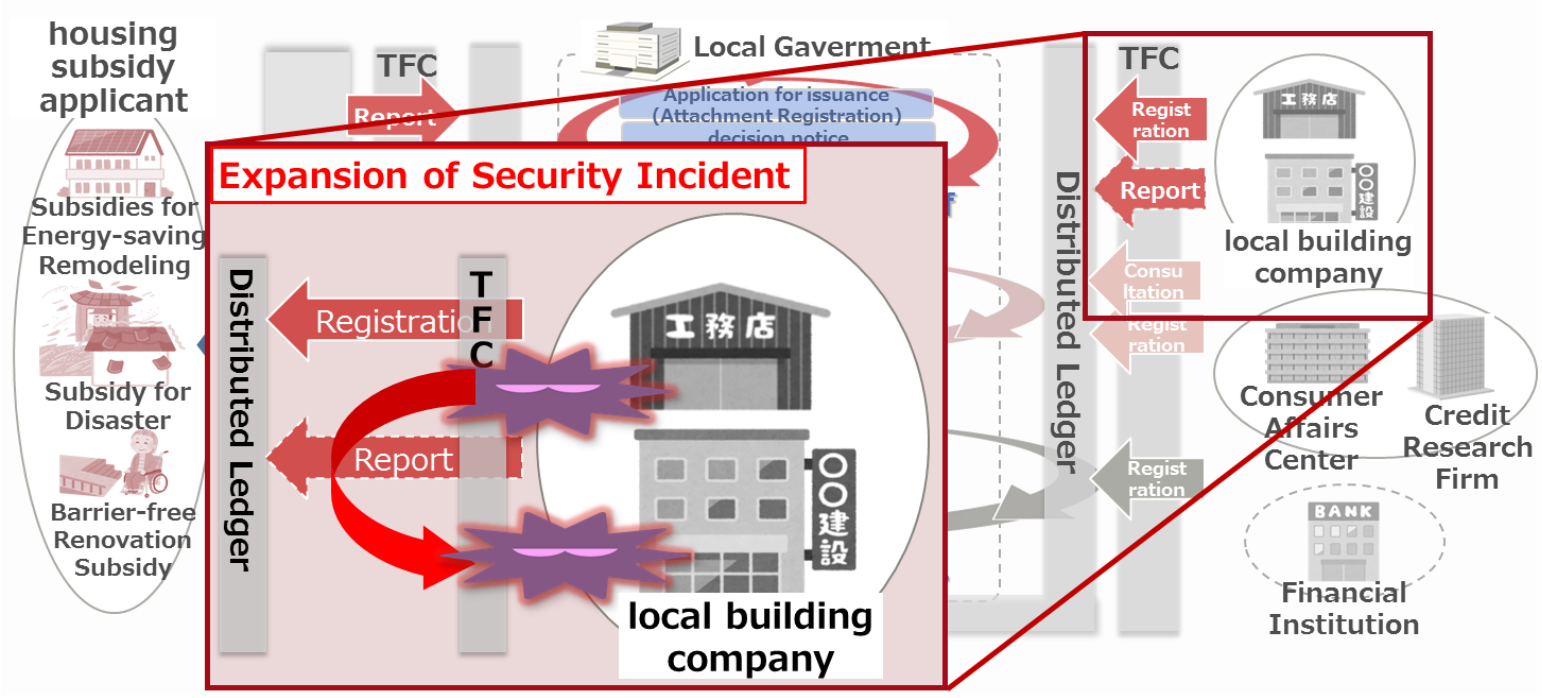
- Prevent the spread of threats by automatically deploying and applying security threat countermeasures to the entire data distribution network related to subsidy applications
- Preventing delays in procurement of parts and materials, extension of construction period, and delay in provision of subsidies due to security damage at building companies, etc.

Use case

■ Housing subsidy project

【present】 There is no mechanism for sharing security damage and threat information among subsidy project participants, and security measures are implemented to each company individually. If the damage spreads from the companies with weak measures, in the worst case, the subsidy project will be stopped.

【applied】 Sharing threat information and countermeasures throughout the system, automatically applying countermeasures throughout the system to prevent the spread of security damage, and improving overall security and security resilience



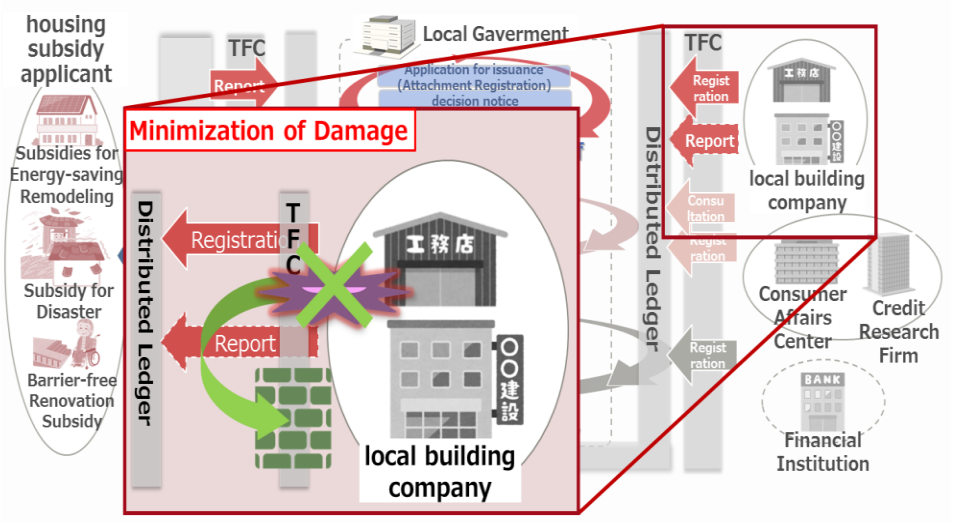
Continuous Security Protection by Selection Technology for Trustworthy Connection

FUJITSU LIMITED

Technology Description

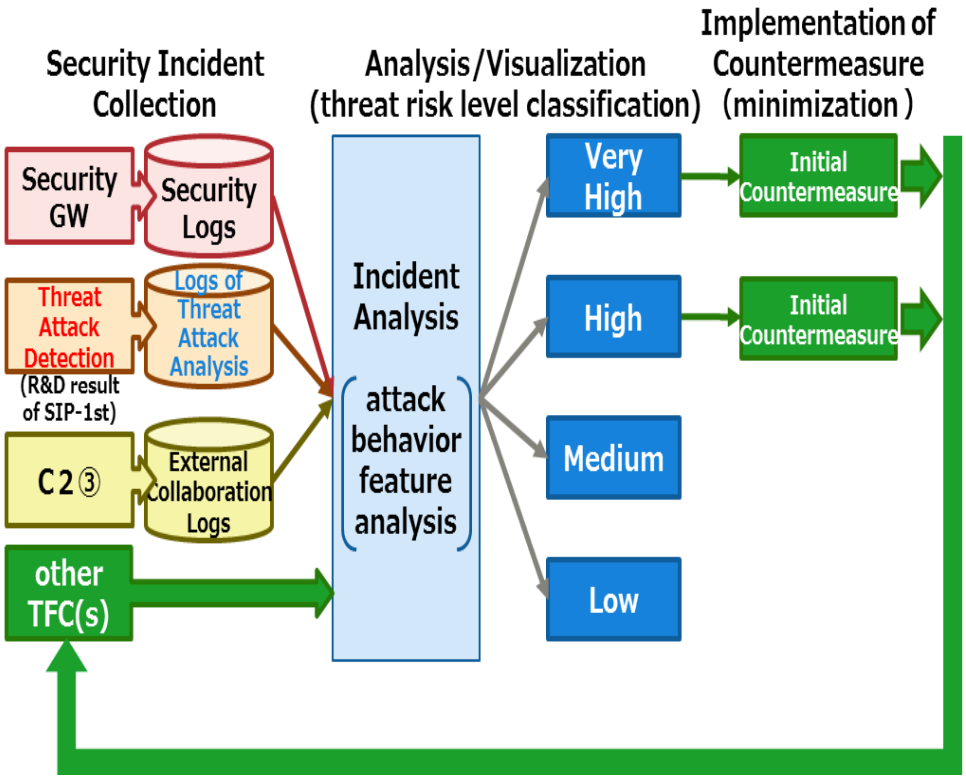
■ Approach to continuous security protection

- Calculate threat risk based on network access behavior at each participating site
- When a high-risk access action is detected, a preset measure is applied
- Notify other company sites of detected threats and countermeasures
- Each site applies countermeasures based on the content of the notification, develops countermeasures throughout the system, and homogenizes security measures



■ Specific technologies for continuous security protection

- Security Incident Collection (Log Collection)
  - Security GW (commercial product)
  - Threat detection (Access log with packet capture)
  - External collaboration (External notification log such as theme collaboration)
- Analysis/Visualization (threat risk level classification)
  - Attack Behavior Characteristic Analysis
  - (Calculate risk based on an action model that divides network activities into activity phases)
- Implementation of countermeasures (minimization)
  - Minimize damage by automatically applying primary measures (Disconnection of targeted communications, etc.) when the risk is high
  - Deploy threat information to other TFCs and automatically apply countermeasures to all TFCs



■ Roles and effects of development technologies

Issue of the subsidy project	Development technologies and effects
•Protects information on companies participating in subsidy project	•Information protection of the entire system by homogenizing the application of security measures
•Preventing system outages due to security threats	•To apply measures to prevent the spread of threats to all systems, and to prevent the suspension of all systems by raising the level of countermeasures

Contact

NTT Solution Div., Telecom Business Unit
FUJITSU LIMITED
Email:contact-sip2021b2@cs.jp.fujitsu.com

内閣府 Cabinet Office
NEDO
SIP Cross-ministerial Strategic Innovation Promotion Program