

# 精選接続技術による安全性維持

富士通株式会社

精選接続技術の自治体補助金事業への適用における安全性維持について紹介する

適用領域

半導体・実装

IoT

ICTバンダー

製造

インフラ

流通

自治体行政

ビル・スマートシティ

## 技術の特長

### ■ 自治体事業ネットワークのセキュリティ対策を均質化

- ・補助金事業に参加する各事業者サイトにおいて脅威検知、分析/可視化、一次対策までの一連の処理を自動化
- ・補助金事業に参加している他の事業者にも自動的に展開し、システム全体の対策を均質化

## 導入効果

### ■ セキュリティ被害拡大による補助金事業の実行停滞を防止

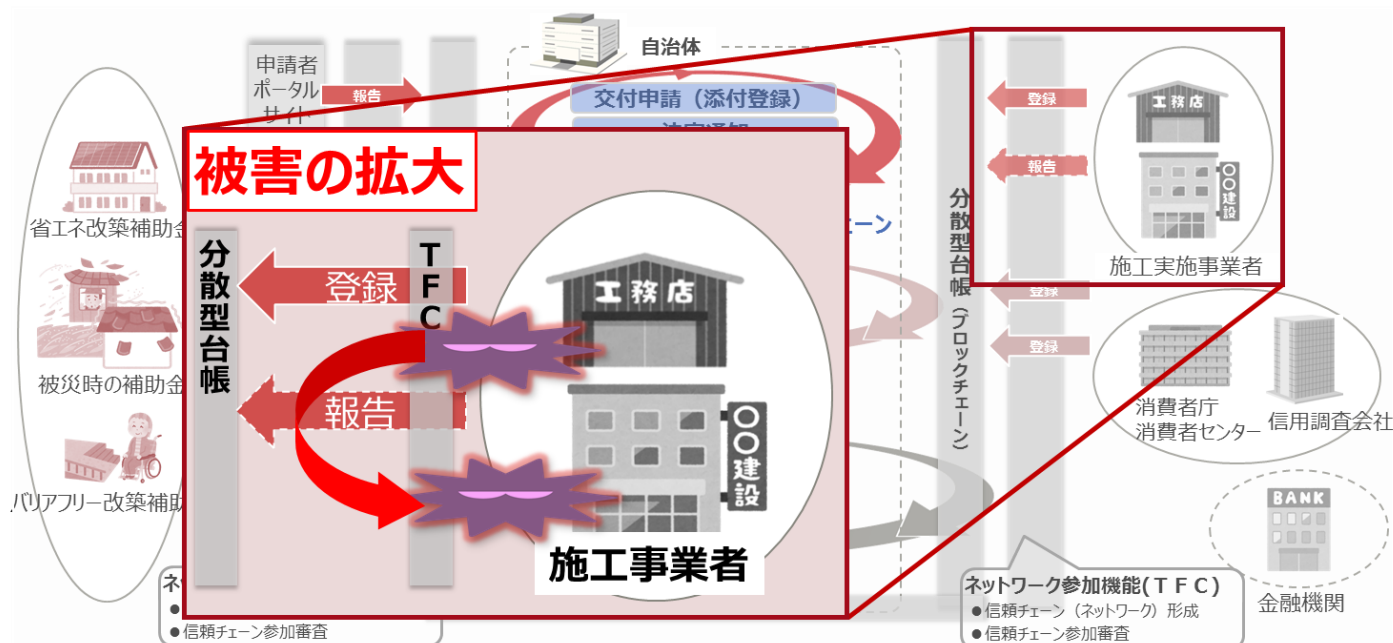
- ・補助金申請に関わるデータ流通ネットワーク全体へのセキュリティ脅威対策の自動展開・適用により脅威拡大を防止
- ・施工事業者等におけるセキュリティ被害発生による部材調達遅れ、工期延伸、しいては補助金交付の遅れなどを防止

## ユースケース

### ■ 住宅補助金事業

【現状】 補助金事業参加事業者間でセキュリティ被害や脅威情報を共有する仕組みが無く、セキュリティ対策は各事業者毎にバラバラで、対策が脆弱な事業者から被害が拡大蔓延した場合、最悪、補助金事業が停止

【適用後】 脅威情報、対策をシステム全体で共有し、対策の全体への自動適用によりセキュリティ被害拡散を抑止、全体の安全性とセキュリティ耐性を向上



自治体事業に参加している事業者毎にセキュリティ脅威を検知・対策し、システム全体に自動展開し、システム内のセキュリティ対策を均質化

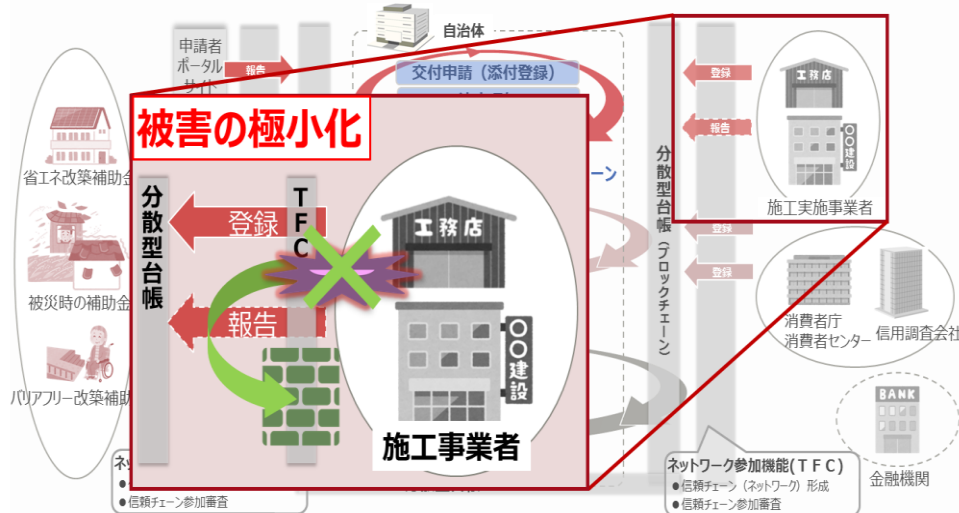
# 精選接続技術による安全性維持

富士通株式会社

## 技術内容

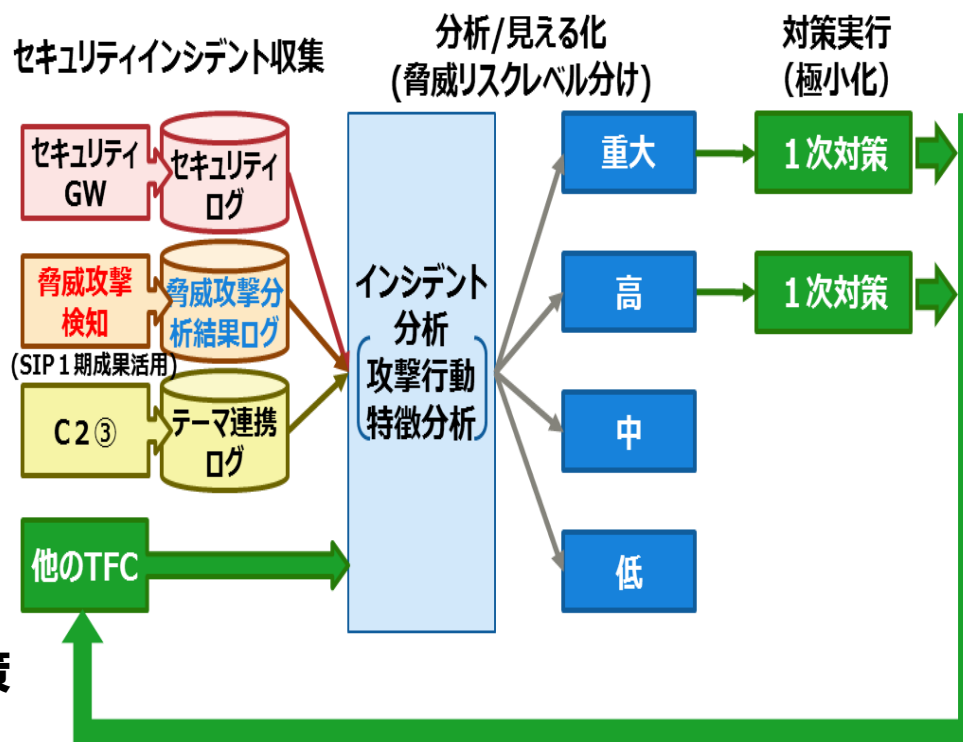
### ■ 安全性維持の考え方

- 参加事業者サイト毎にネットワークアクセス動作を基に脅威の危険度を算定
- 危険度の高いアクセス動作を検知した場合、事前設定された対策を適用
- 検知した脅威、対策を他事業者サイトに通知
- 各サイトでは、通知内容を基に対策を適用し、システム全体に対策が展開され、セキュリティ対策を均質化



### ■ 安全性維持の具体的な技術

- セキュリティインシデント収集 (ログ収集)
  - セキュリティGW (市販)
  - 脅威検知 (パケットキャプチャによるアクセスログ)
  - 外部連携 (テーマ連携など、外部通知ログ)
- 分析/見える化 (脅威リスクレベル分け)
  - 攻撃行動特徴分析
  - (ネットワーク上の活動を活動フェーズに分けた行動モデルを基にした危険度を算出)
- 対策実行 (極小化)
  - 危険度が高い場合、1次対策 (対象通信遮断等) を自動適用し被害を極小化
  - 脅威情報を他のTFCに展開し、全TFCで対策を自動適用



### ■ 開発技術の役割、効果

補助金事業の課題	開発技術と効果
• 補助金事業に参加する組織の情報を保護	• セキュリティ対策適用の均質化によるシステム全体の情報保護
• セキュリティ脅威によるシステム全系停止の防止	• システム全系への脅威拡大防止策適用、対策底上げによる全系停止の防止

## 問い合わせ先

富士通株式会社  
 キャリア事業本部 NTTソリューション事業部  
 Email: contact-sip2021b2@cs.jp.fujitsu.com

