IoTセキュリティの社会実装における課題抽出

セコム株式会社 IS研究所
○国井 裕樹　　伊達 浩行　　伊藤 忠彦

アウトライン

[概要]

IoTセキュリティセキュリティとしての暗号技術の社会実装に向けた実装要件の導出を行った

- 研究背景
- 研究課題
- 研究内容
  - 標準規格・ガイドライン調査
  - ユースケース検討
  - IoT機器への暗号技術の実装要件

研究背景

- IoT機器への脅威の増大
  - MiraiによるWebカメラへの侵入
  - ホテルのスマートキーがランサムウェア感染
  - Jeep Cherokeeへのリモート操作実演
  - インシュリンポンプの脆弱性発覚

- セキュリティ技術の普及がICTほどに進んでいない
  - 幅広い機器（低リソース、電池駆動、小型）
  - 非機能要件であるセキュリティとコストメリット

研究課題

- IoT機器へのセキュリティ技術の実装が普及するための要件を抽出する
  - 特にセキュリティ技術の基礎となる暗号技術に着目
  - 暗号技術がIoT機器に社会実装されるための実装要件を検討

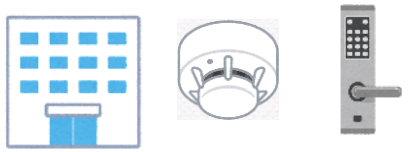
研究内容

1. 検討対象分野の選定
2. 各分野のセキュリティ標準・ガイドライン調査
3. 各分野のユースケース検討
4. 社会実装への要件抽出

検討対象分野の選定

- 多様なIoT分野全般を検討対象とるのは困難
- 下記基準に従い分野を選定

項目	説明
システムの複雑さ	複数のメーカーから調達された機器で構成される
相互接続の有無	他者が運用するシステムと相互に接続する
人命・資産への影響	人命・資産へクリティカルに影響する

① 防犯カメラ	② ビル管理/データセンタ	③ 自動車	④ ヘルスケア機器
			

トラストを構築する暗号技術

システムの複雑性受容、コネクタビリティ、
安全性確保のための本質技術としてのセキュリティ

トラスト：
コミュニケーションの相手、情報、システムなどが正しいと判断できる状態にあること

IoT機器において、上記の概念およびそれらを達成する機能のためのセキュリティには「暗号技術」が本質的に必要になる

検討対象分野におけるセキュリティの現状

- 暗号技術を含むセキュリティがどの程度、各分野において利用されているかを調査
- 相場観および使われ方、考え方を分析

- 調査方法
  - 業界標準となるような国際標準や国内外のガイドライン
    - 防犯カメラ
    - ビル管理システム・データセンター
    - 自動車
    - ヘルスケア機器

標準・ガイドライン調査

防犯カメラ	ビル管理/データセンタ	自動車	ヘルスケア機器
ONVIF TLS	BACnet	IEEE1609.2 楕円	DICOM TLS
PSIA TLS	LonWorks	ETSI TS 103 097 楕円	血液透析装置に関する通信共通プロトコル 記述なし
日本防犯設備協会ガイドライン 記述なし	Ubiquitous Green Community Control Network TLS	700MHz帯安全運転支援システム構築 セキュリティガイドライン 楕円	医療情報システムの安全管理に関するガイドライン TLS
BSI TLS	ECHONET	ITU-T X.1373 TLS	医療品、医療機器等の品質、有効性及び安全性の確保等に関する法律 記述なし
NIST TLS	日本計装工業会 計装マニュアル 記述なし	EVITA 楕円	IHE TLS
	建物設備システム リファレンスガイド 記述なし	TPM Automotive Thin 楕円	MDS2

IEEE1609.2

- 車車間通信 (V2V)や路車間通信等 (V2I) のネットワーク層およびトランスポート層のセキュリティ標準
- 最新版はIEEE1609.2-2016
- 通信メッセージのセキュリティのためにメッセージフォーマット、電子署名の付与、PKIの利用などがあげられている
- 実運用で必要なスペック等も議論が進んでいる

<table>
<tr><td colspan="2">SAE J2735/SAE J2945.1</td><td>AppIF</td></tr>
<tr><td rowspan="2">IEEE 1609.2
(Security)</td><td rowspan="2">IEEE 1609.3</td><td>TCP/UDP</td></tr>
<tr><td>IPv6</td></tr>
<tr><td colspan="2">IEEE 802.2/IEEE 1609.3</td><td>LLC</td></tr>
<tr><td colspan="2">IEEE 802.11p/IEEE 1609.4</td><td>MAC</td></tr>
<tr><td colspan="2">IEEE 802.11p</td><td>PHY</td></tr>
</table>

ユースケースの検討

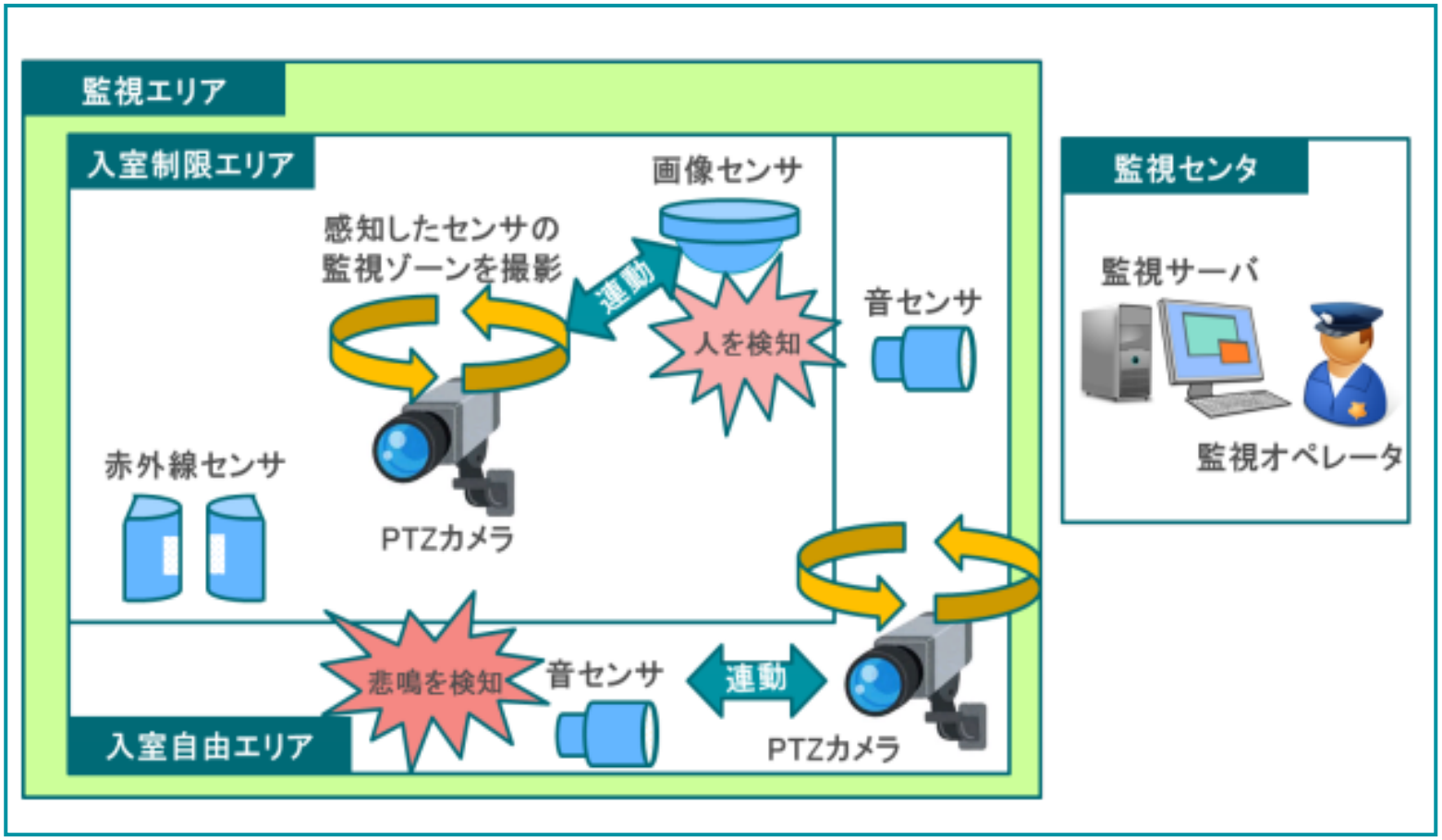
各分野におけるセキュリティの標準化等の調査
→ それぞれ存在一定程度存在

システムの複雑性受容、コネクタビリティ、
安全性確保のための本質技術としてのセキュリティ

IoTシステムにおいて「つながること」が本質的になるような価値になるシステムを考案。

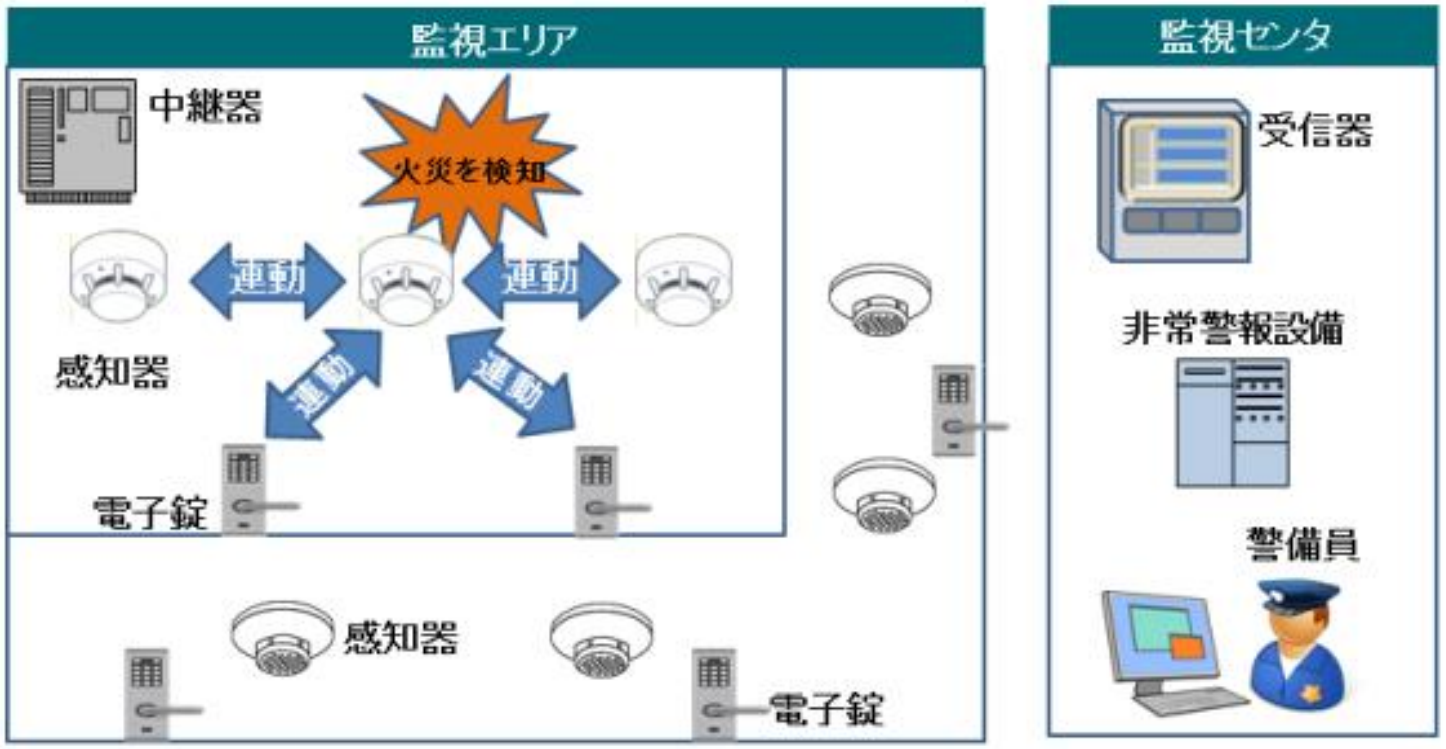
そこへの実装要件を導き出すことで社会実装への要件を導出

ユースケース：防犯カメラ



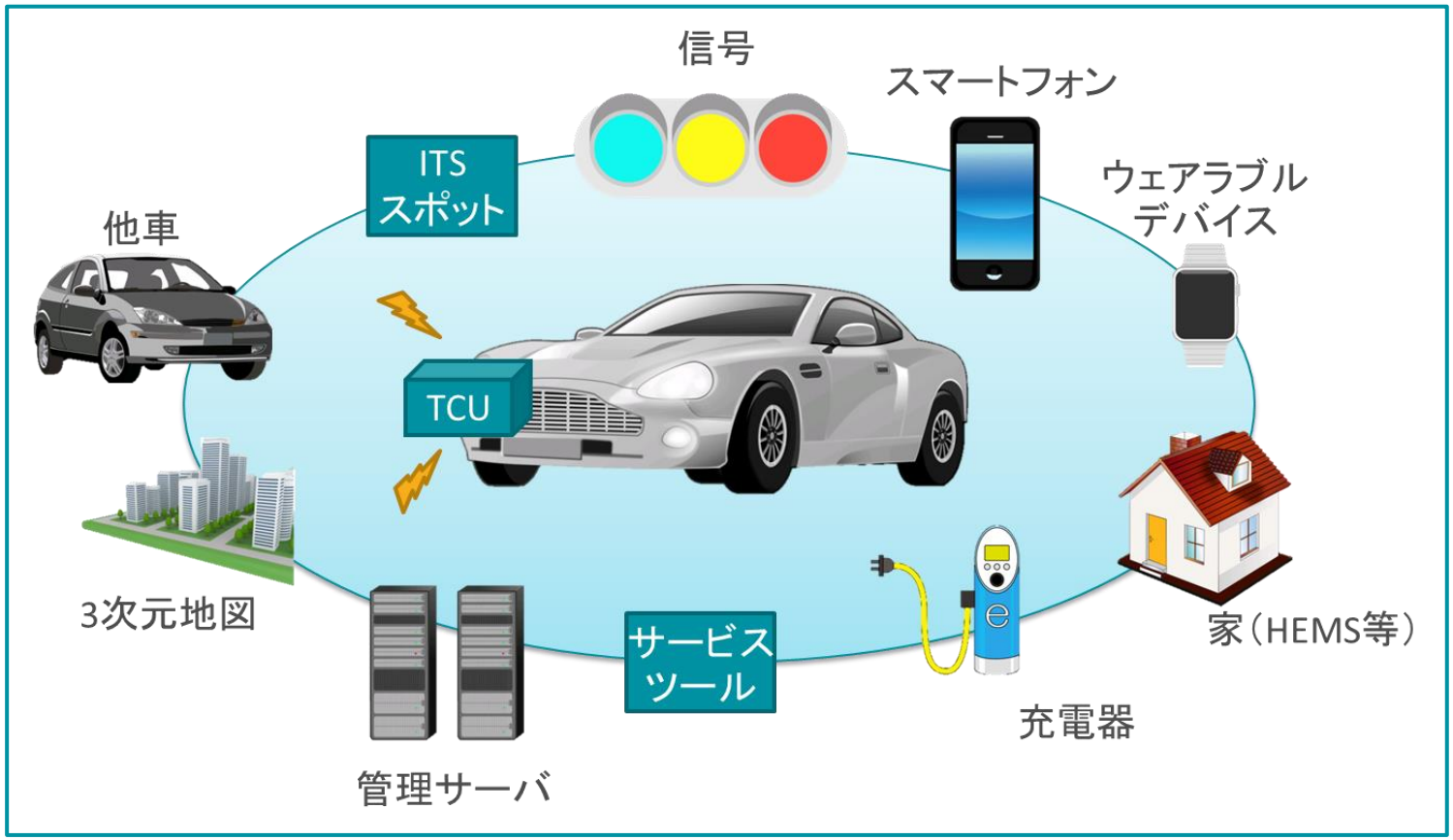
PTZカメラと各センサの連動
監視範囲の広範化とコストメリットの両立

ユースケース：ビル管理/データセンタ



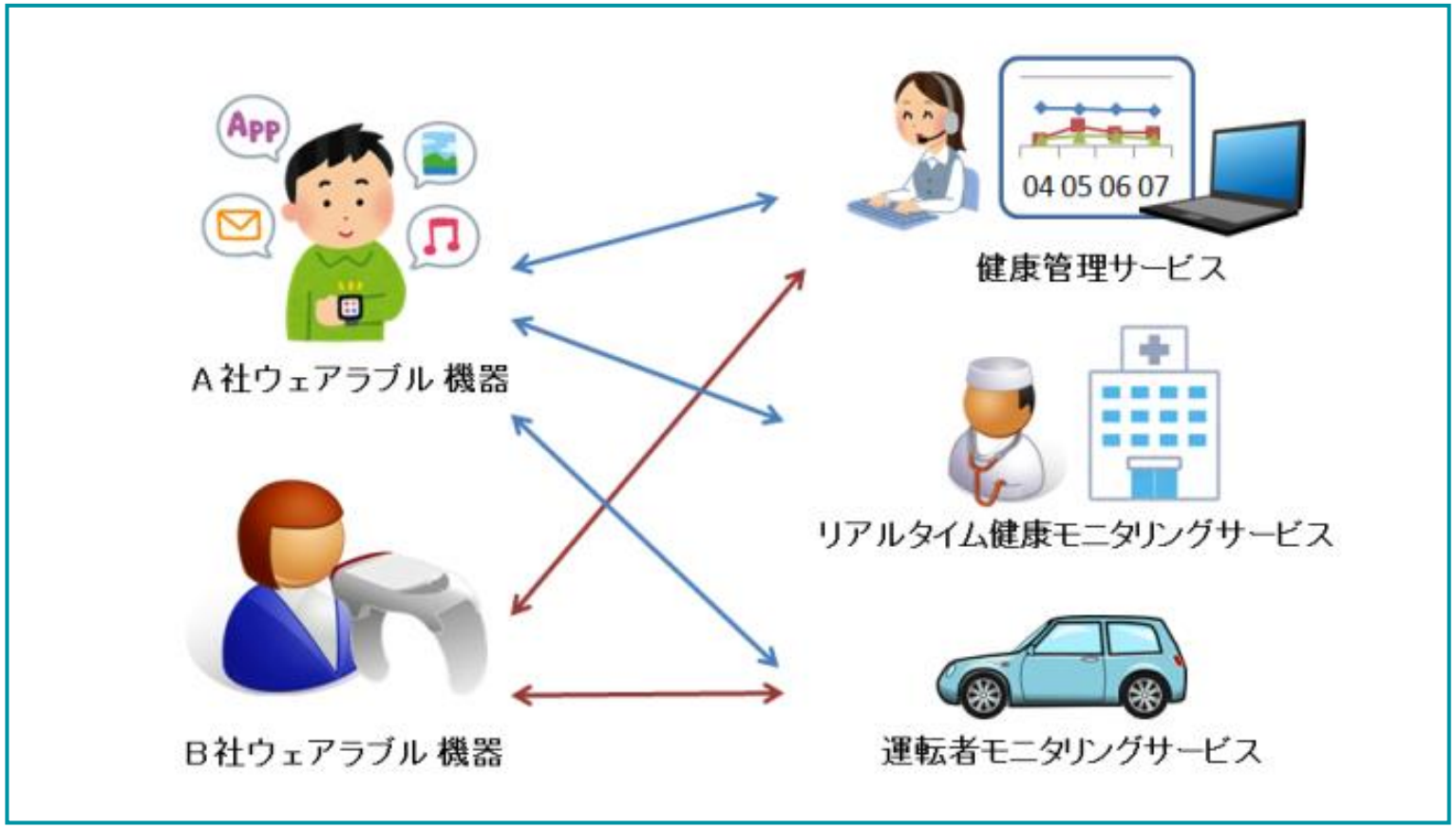
防災センサと電子錠の連動
検知精度の向上とシステムの可用性向上

ユースケース：自動車



V2V・V2I・V2X（自動車と様々なものの通信）
世界中で検討が進んでいる

ユースケース：ヘルスケア機器



ヘルスケア機器と複数サービスの連携
ユーザーへの選択肢提供と利便性向上

暗号技術の実装要件の検討

システム開発・システム運用の観点での条件

- 実装コスト
  ソフトウェア実装：実装簡便性、鍵の秘匿化
  ハードウェア実装：調達容易性、低価格
- 運用コスト
  導入コストと保守コストとのトレードオフ
  サプライチェーン全般での対応
- スケーラビリティ
  普及時の膨大な処理量への対応
  運用コストへの影響

IoTセキュリティの社会実装における課題抽出

要件	説明
公開鍵暗号の利用	普及数と複数ベンダをまたがるセキュリティを考慮 共通鍵暗号での鍵共有スケーラビリティ両立の困難性 PKI(Public Key Infrastructure)の利用が効果的
軽量性（省電力性）	リソースに限りのあるデバイスでの動作を想定 メインの計算処理・メモリ・バッテリへの影響を考慮 電源がある場合でも省電力化は重要
高速性	多数の機器の通信時のボトルネックにならないこと メッセージの正当性検証などはスケーラビリティに重要
物理攻撃への耐性	機器のライフサイクル全般に渡っての鍵管理 リバースエンジニアリング等への耐性 サプライチェーン全般（製造・流通等）での攻撃対策

おわりに

IoT システムにおける本来の価値を最大化するために必要なセキュリティ技術としての暗号技術が、どのようなシステムやサービスで社会実装されうるのか、そこにどのような要件が必要なのかを調査・検討し、4つの要件を示した。

なお、本研究の一部は、総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（ＳＩＰ）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されている。