資料６－３

HITACHI
Inspire the Next

IoTのセキュリティ

2015/4/6

株式会社 日立製作所 研究開発グループ
システムイノベーションセンタ セキュリティ研究部

鍛　忠司

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

1. 本発表でのIoTの定義と分類

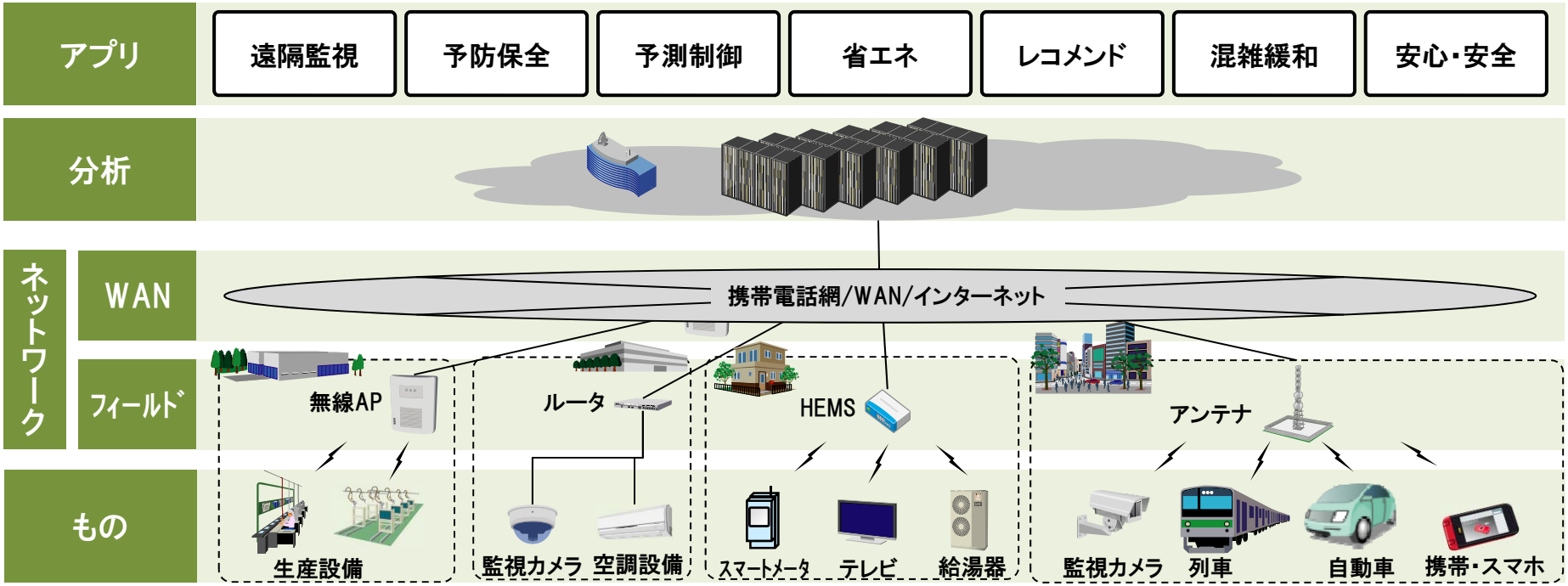
1-1 本発表でのIoTの定義

HITACHI
Inspire the Next

ネットワークに接続された「もの」(Thing)をセンシングし、分析することで新しい価値を生むシステム

監視カメラや携帯電話等、従来からネットワークに接続されていた「もの」に加え、生産設備や空調機器、自動車、列車等、あらゆる「もの」をネットワークに接続し、稼働データを収集、目的に応じた分析を実施

本発表におけるIoTのリファレンス構成



AP:アクセスポイント　HEMS:ホームエネルギー管理システム

1-2 IoTの分類

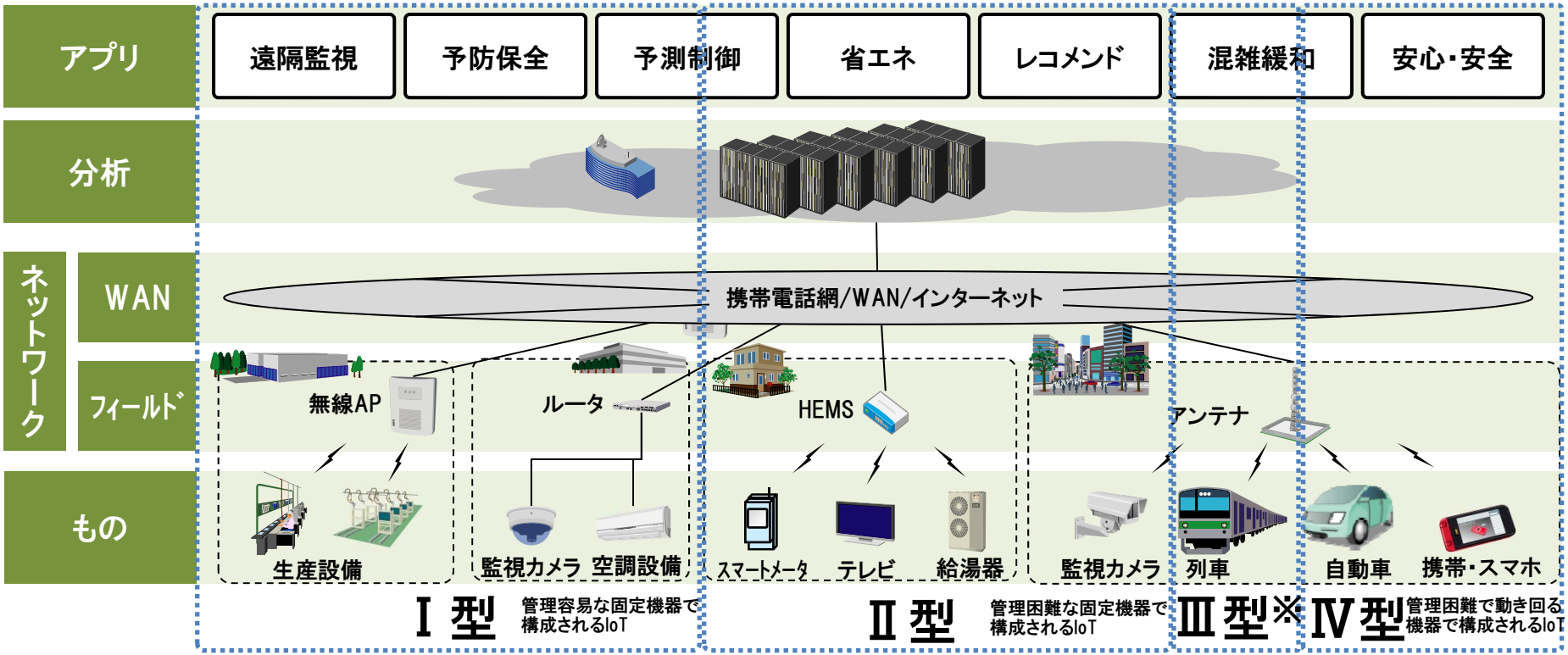
HITACHI
Inspire the Next

「もの」のガバナンスとモビリティの観点でIoTを分類

■ガバナンス：「もの」が管理容易か否か
（個人宅設置/個人所有の「もの」は管理困難）
■モビリティ：　「もの」は固定か、動き回るか

ガバナンス ＼ モビリティ	なし	あり
あり	Ⅰ型	Ⅲ型
なし	Ⅱ型	Ⅳ型

IoTの分類



AP:アクセスポイント　HEMS:ホームエネルギー管理システム

※　管理容易だが動き回る機器で構成されるIoT

HITACHI
Inspire the Next

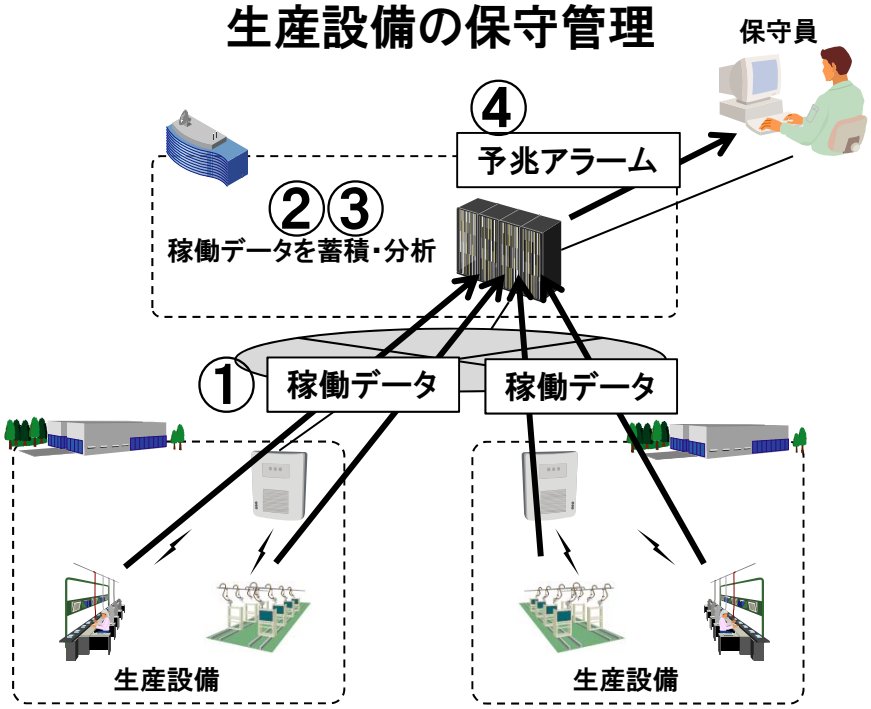
2. IoTのユースケース例

2-1 Ⅰ型の例：生産設備の保守管理

HITACHI
Inspire the Next

生産設備の稼働データの分析に基づく事前保守により計画外停止を回避

「もの」	生産設備
ネットワーク	工場内ネットワーク、企業情報ネットワーク
分析	機械学習による稼働状態の変調検出
新しい価値	予防保全



【課題】
- 生産設備に組み込まれた機能がアラームを発信 → 故障寸前のため即時に停止が必要
- オペレータの経験・勘が重要

【動作概要】
①生産設備から稼働データを収集
②収集した稼働データを蓄積
③稼働データを分析し、初期の異常を検知
④保守員に予兆アラームを発信

【想定効果】
- 故障停止の2週間以上前に異常を検知（過去の実績データでの実証実験による）
- 故障の3日前に事前保守を計画、実行可能

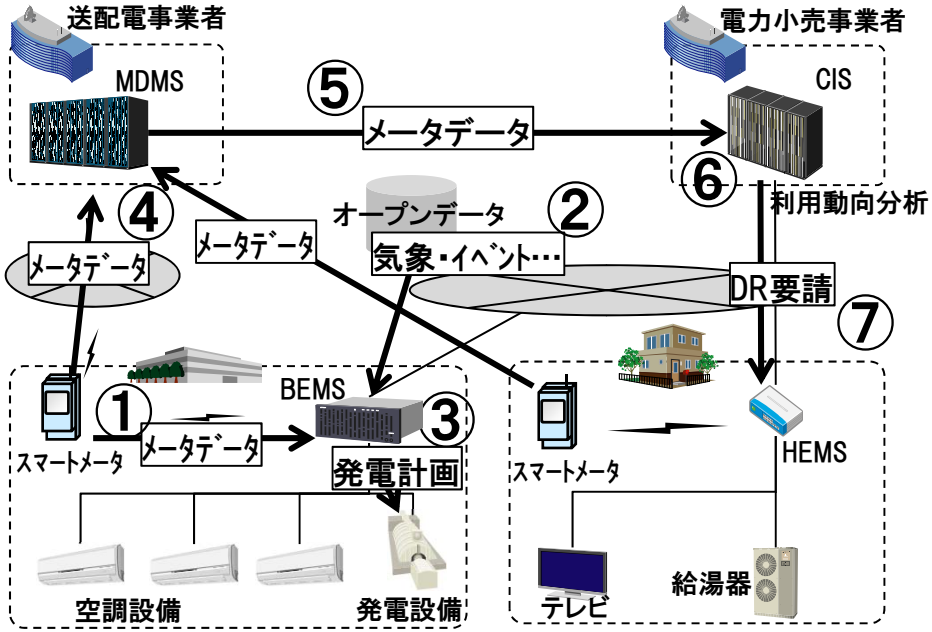
2-2 II型の例：エネルギー需要推定

HITACHI
Inspire the Next

スマートメータから収集したデータを分析、エネルギー需要を推定

「もの」	スマートメータ
ネットワーク	LAN、アドホック型無線通信ネットワーク、企業間通信網
分析	メータデータのクラスタ分析等
新しい価値	エネルギー需要推定

エネルギー需要推定



【課題】
- エネルギーの効率的な利用

【動作概要】
①スマートメータからメータデータを収集
②気象情報等をオープンデータから収集
③エネルギー需要を推定し、発電計画を策定
④スマートメータからメータデータを収集
⑤収集したメータデータを小売事業者に配信
⑥料金計算と同時に、需要家の利用動向を分析
⑦DR等を組み合わせ、効率的に電力を調達

【想定効果】
- 需要パターンに合わせた発電計画や調達計画を策定

BEMS：ビルエネルギー管理システム　CIS：需要家情報管理システム　DR：デマンドレスポンス　MDMS：メータデータ管理システム
HEMS：ホームエネルギー管理システム

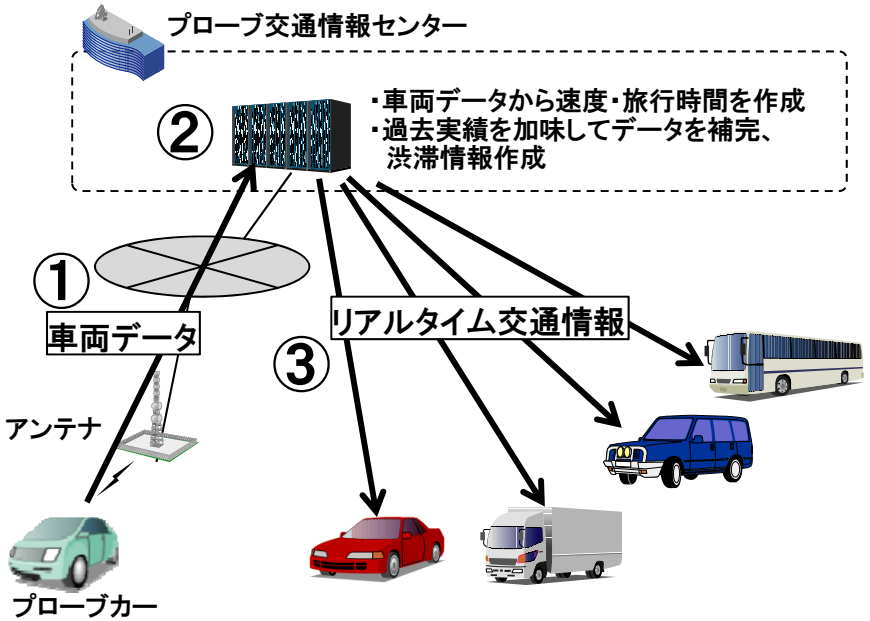
2-3 Ⅳ型の例：交通情報作成

HITACHI
Inspire the Next

プローブカーが発信した車両情報を分析、交通情報として配信

「もの」	自動車
ネットワーク	携帯電話網、無線通信網、放送網
分析	過去実績を加味した欠損データの補完
新しい価値	渋滞回避

交通情報配信



【課題】
- 路上インフラに依存しない、交通情報の提供

【動作概要】
①プローブカーから車両ﾃﾞｰﾀ(時刻・位置)を収集
②車両データから地点の速度・旅行時間を作成
③過去実績をもとに、速度・旅行時間を補完し、精度向上
④放送などにより、リアルタイムに交通情報として配信

【想定効果】
- 少ないプローブカーの情報から交通情報を作成可能→リアルタイムな配信が可能

BEMS:ビルエネルギー管理システム　CIS:需要家情報管理システム　DR:デマンドレスポンス　MDMS:メータデータ管理システム
HEMS:ホームエネルギー管理システム

2-4 社会インフラ/制御システムがIoTでやりたいこと

HITACHI
Inspire the Next

フィードバック制御から予測(フィードフォワード)制御への移行

さまざまな「もの」から得られるセンシングデータ、過去の実績やオープンデータなどを組み合わせて分析することで**将来を予測**し、事前対策で**影響を最小化/局所化**する

HITACHI
Inspire the Next

3. IoTセキュリティの課題と要件

3-1 IoTに想定されるリスク

HITACHI
Inspire the Next

社会インフラ/制御システムがIoTでやりたいこと

さまざまな「もの」から得られるセンシングデータ、過去の実績やオープンデータなどを組み合わせて分析することで**将来を予測**し、事前対策で**影響を最小化/局所化**する

IoTに想定されるリスク

- 将来の予測を間違わせ、影響を増大/拡大する
- IoTの機能を不正利用することで、サービス提供を妨害する

リスクの原因例

項番	事象	原因	原因の原因	原因の原因の原因
1			事前対策が妨害される	
2			事前対策が遅延する	-
3	影響が最小化/局所化できない	事前対策が取れない	影響が予測できない	情報が不足している
4			影響と対策の対応が間違っている	-
5				センシングデータが間違っている
6				過去実績が間違っている
7				オープンデータが間違っている
8	影響が増大/拡大する	事前対策が間違っている	間違った影響予測をしている	影響予測の処理方法が間違っている
9	サービス提供が妨害される	IoTの機能が不正利用される	セキュリティ対策を行っていない	-

3-2 IoTのセキュリティ要件

HITACHI
Inspire the Next

IoTのセキュリティ要件例

項番	問題	要件
1	事前対策が妨害される	セキュリティアーキテクチャの立案/実装/実施
2	事前対策が遅延する	運用員の訓練、等
3	情報が不足している	データの可用性の確保
4	影響と対策の対応が間違っている	リスク分析に基づく対策の立案/実装/実施
5		「もの」の保護 ○
6		不正な「もの」の排除 ○
7	センシングデータが間違っている	センシングデータの通信路の保護 ○
8	過去実績が間違っている	蓄積データの保護
9		信頼できるオープンデータの利用 ○
10		オープンデータ提供源の保護 ○
11	オープンデータが間違っている	オープンデータの通信路の保護 ○
12	影響予測の処理方法が間違っている	予測機能の保護
13	セキュリティ対策を行っていない	リスク分析に基づく対策の立案/実装/実施 ○

3-3 IoTセキュリティの課題(１)

HITACHI
Inspire the Next

IoTのセキュリティ要件

- センシングデータの生成源(「もの」)と通信路を保護する
- オープンデータの生成源と通信路を保護する

なぜ大変なのか？

- データの利用者とデータ生成源の所有者/管理者が異なる
- (Ⅱ型/Ⅳ型は)データ生成源の管理が困難
- (Ⅲ型/Ⅳ型は)機器が動き回る

各ユースケースでのデータ発生源と所有者/管理者/設置場所

ユースケース	データ	データ利用者	データ生成源	所有者/管理者	設置場所
生産設備の保守管理	生産設備の稼働データ	•保守会社 •本社	生産設備	各工場	各工場
エネルギー需要推定	メータデータ	•ビル管理会社 •電力小売事業者	スマートメータ	送配電事業者	需要家宅
	気象、イベント情報		オープンデータ	外部組織	インターネット
交通情報配信	車両データ	プローブ交通情報センター	•自家用車 •商用車	•個人 •企業	不定

3-4 IoTセキュリティの課題(２)

HITACHI
Inspire the Next

IoTのセキュリティ要件

セキュリティ対策の実施

なぜ大変なのか？

設計当初には想定していない使い方をしようとしている

**制御システム/社会インフラシステムの多くは、
稼働データを蓄積して分析するという利用を想定せずに
設計・構築されている**

セキュリティ対策するには一から設計をやり直さなければならないかもしれない・・・
セキュリティ対策すると、性能要件を満足できないかもしれない・・・

既存のセキュリティ標準もIoTを考慮して作っていない

Webシステムのセキュリティ対策の多くは、不正「者」に対する対策

3-5 IoTセキュリティの要件

HITACHI
Inspire the Next

IoTセキュリティの要件①

「もの」を合理的なコストで保護できること

IoTセキュリティの要件②

センシングデータ/オープンデータの信憑性が確認できること

IoTセキュリティの要件③

運用による対策は最低限にとどめること

IoTセキュリティの要件④

セキュリティ対策が段階的に拡張/更新できること

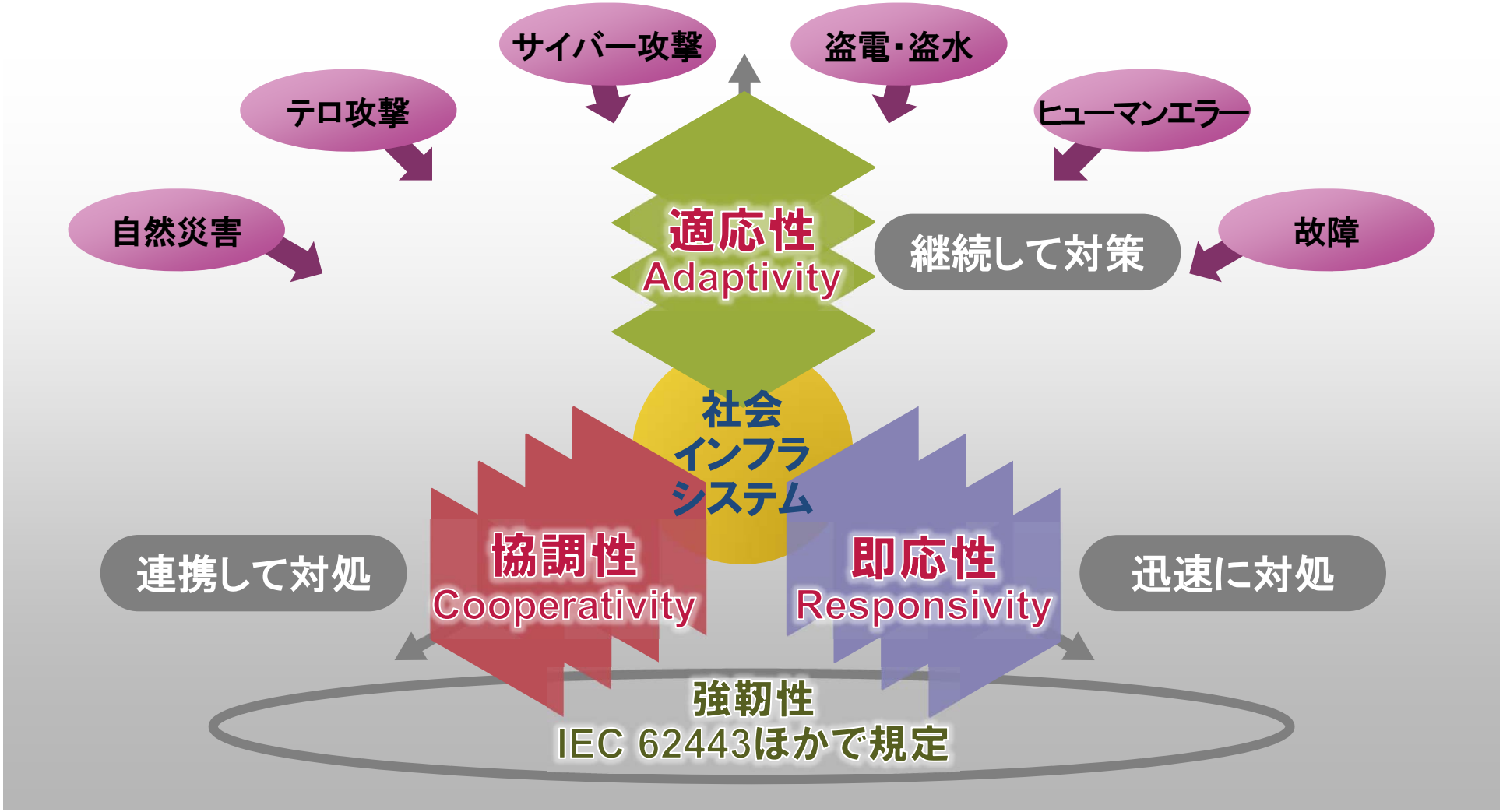
IoTセキュリティの要件⑤

IoTへの適合性が評価・検証されたセキュリティ標準を使うこと

3-6 日立の社会インフラセキュリティコンセプト

HITACHI
Inspire the Next

H-ARC コンセプト　システムとしての強靭性に加え、システムとして必要となる適応、即応、協調の3つの軸で対応



HITACHI
Inspire the Next

4. まとめ

4. まとめ

HITACHI
Inspire the Next

□ 本発表におけるIoT

ネットワークに接続された「もの」(Thing)をセンシングし、分析することで新しい価値を生むシステム

さまざまな「もの」から得られるセンシングデータ、過去の実績やオープンデータなどを組み合わせて分析することで将来を予測し、事前対策で影響を最小化/局所化する

□ IoTセキュリティの課題

- ✓ データの利用者とデータ生成源の所有者/管理者が異なる
- ✓ データ生成源が動き回ったり、設置場所の制約から管理が困難
- ✓ 設計当初には想定していない使い方をしようとしている

□ IoTセキュリティの要件

- ✓ 「もの」を合理的なコストで保護できること
- ✓ センシングデータ/オープンデータの信憑性が確認できること
- ✓ 運用による対策は最低限にとどめること
- ✓ セキュリティ対策が段階的に拡張/更新できること
- ✓ IoTへの適合性が評価・検証されたセキュリティ標準を使うこと

HITACHI
Inspire the Next

END

IoTのセキュリティ

2015/4/6

株式会社 日立製作所 研究開発グループ
システムイノベーションセンタ セキュリティ研究部

鍛　忠司

HITACHI

Inspire the Next