改正個人情報保護法等を踏まえた
プライバシー保護検討タスクフォース（第4回）

Innovative R&D by NTT

IoTプライバシーの技術的考察

2016.4.6

日本電信電話株式会社
NTTセキュアプラットフォーム研究所
高橋克巳

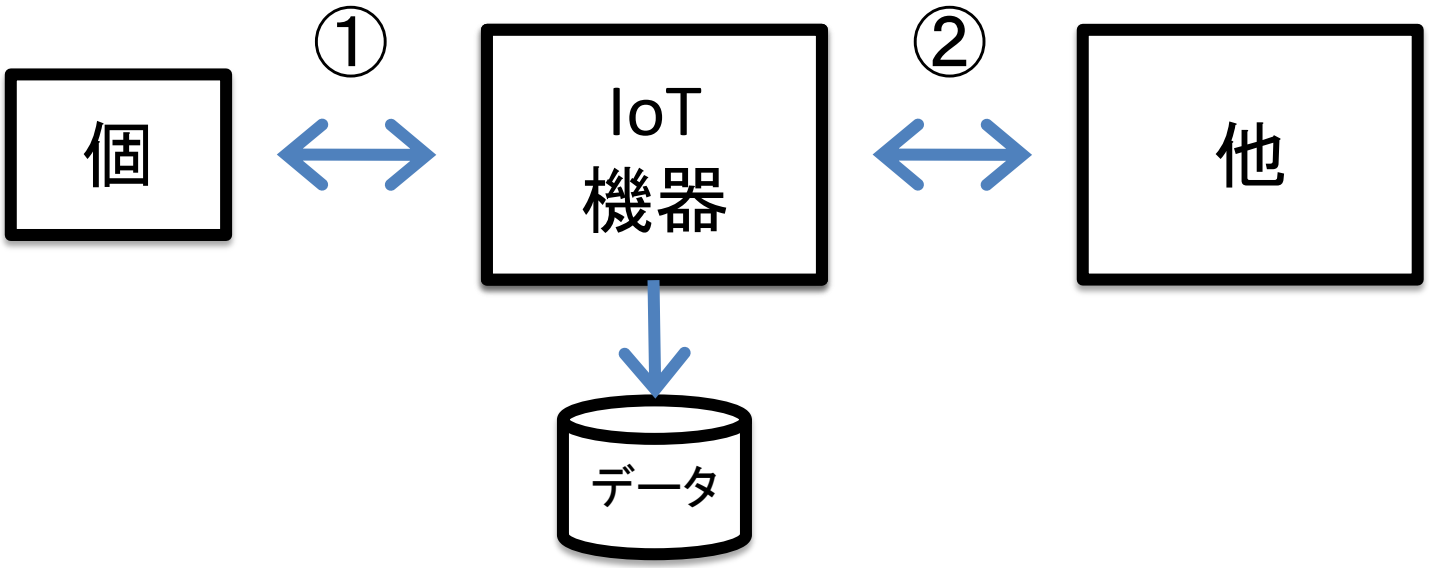
あらまし

- IoTのプライバシー
- IoT機器の保護
- IoTから得られるデータの保護
  ～データプライバシー原則へのあてはめ～
  - 同意
  - 目的の限定とデータ最小化
  - 開示の制限・利用の制限
- IoTにふさわしいプライバシー保護技術
  - 開示の制限・利用の制限

- **IoTのプライバシー**

IoTのプライバシー（仮置き）

- 「IoT機器」から得られるデータによって、個に関する情報がみだりに他に知られないこと
  - ① 個に関する
  - ② みだりに他に



IoTと個の関係（1/2）

- IoT機器と個の関係の例題
  - a.個人の持ち物（例、スマートフォン、ウェアラブル）
  - b.自宅設置機器（例、スマートメーター）
  - c.公共設置機器（例、監視カメラ）
- どのように理解したらよいか
  - 個の単位は個人・家族・組織と多様
    - a. は個人に関する／b. は家族・組織に関する
  - 個人との関係が自明ではないものがある
    - 「個人の何かを記録しているかも」のレベル
    - 《 IoT機器から得られるデータ 》との関係も考える必要が

IoTと個の関係（2/2）

《IoT機器から得られるデータ》と個の関係

- 形式から個との関係の有無がわかるか？
  - 記名データ
  - 「IDのある」データ（例、端末ID）
  - さがすと「ID相当がある」データ（例、監視カメラ画像の顔）
  - 長期間貯めると個人が見えてくるデータ（例、移動履歴）

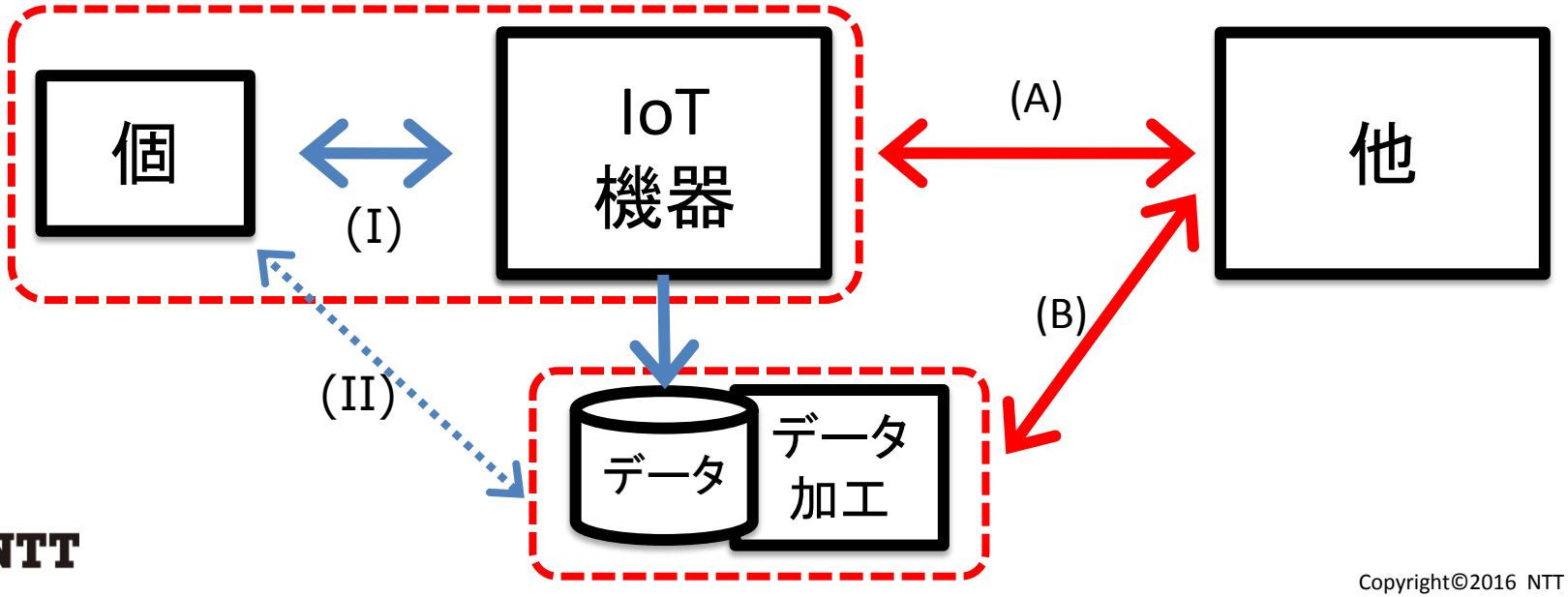
  ★パーソナルデータの個人識別性の問題と同等
- 内容から個との関係の有無がわかるか？
  - センサーデータ（例、加速度データ）
  - 行動データ（例、歩数データ）

  ★センサーデータも解釈（データ加工）をすると行動データに

  ★内容だけで個との関係の有無を議論することは困難

IoTのプライバシー（一旦まとめると）

- (A) IoT機器の保護、(B) IoT機器から得られるデータの保護、どちらも必要
- 個との関係の有無の判断は単純でない
  - (I) IoT機器と個との関係
  - (II) 分析されたデータと個との関係



- **IoT機器の保護**

IoT機器の保護（セキュリティ）

Innovative R&D by NTT

- 情報セキュリティのCIA
  - 機密性（Confidentiality）
  - 完全性（Integrity）
  - 可用性（Availability）
- IoTのプライバシーへのあてはめ
  - 機密性：IoT機器からみだりにデータがもれない
  - 完全性：IoT機器がでたらめなデータを出さない
  - 可用性：IoT機器がいつでもデータを出してくれる
- IoTのプライバシーのためには機密性の確保が最も重要　⇒　IoT機器へのアクセス制限
  - 業務によっては完全性と可用性も必要に

NTT

- **IoTから得られるデータの保護**
  ～データプライバシー原則へのあてはめ～
  同意
  目的の限定とデータ最小化
  開示の制限・利用の制限

IoTから得られるデータの保護
～データプライバシー原則へのあてはめ～

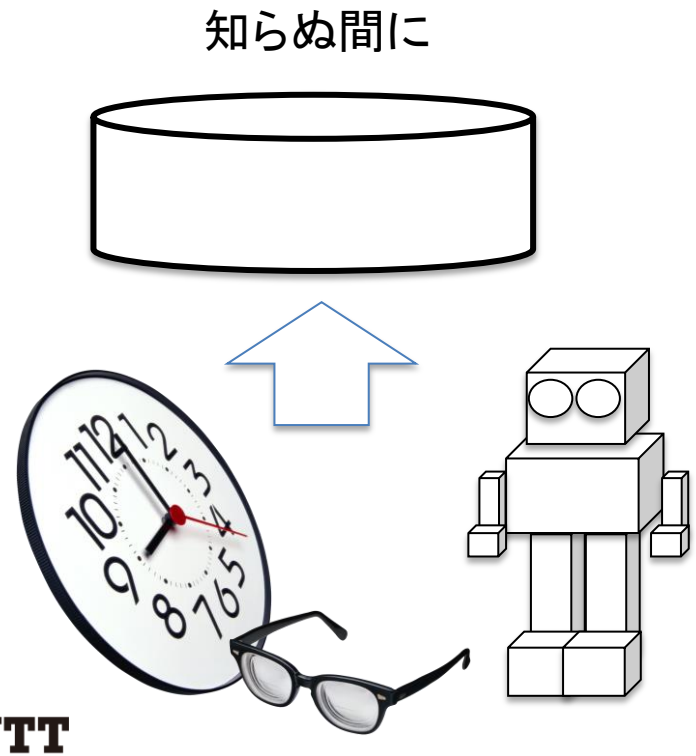
Innovative R&D by NTT

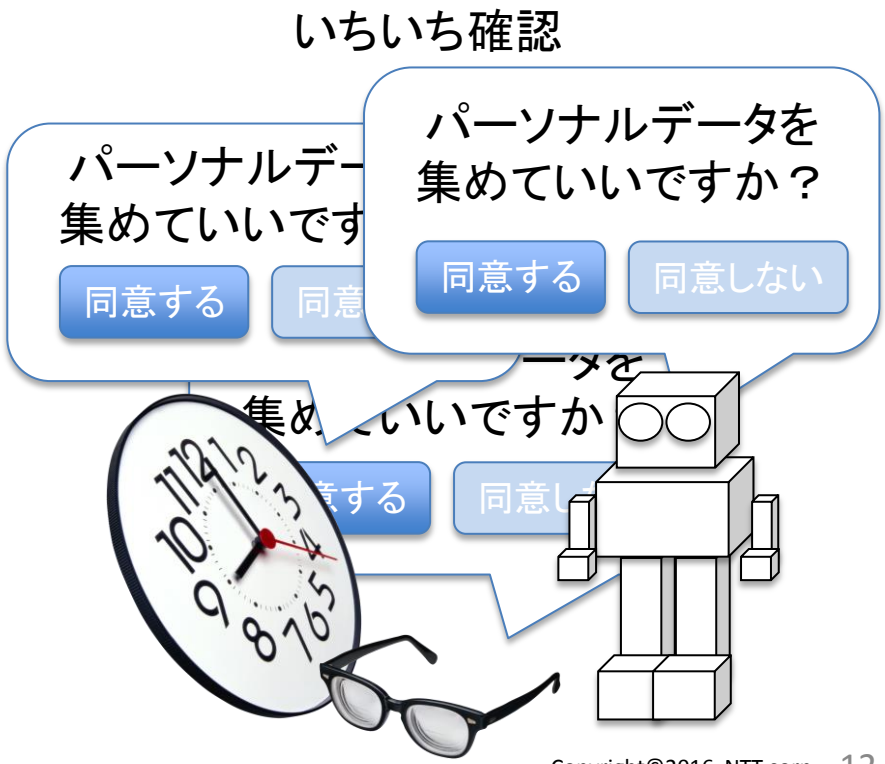
1. 同意と選択
2. 目的の正当性と明確化
3. 収集の制限
4. データ最小化
5. 利用、保管、公開の制限
6. 精度と品質
7. 公開性、透明性と通知
8. 個人参加とアクセス
9. 説明責任
10. 情報セキュリティ
11. プライバシー・コンプライアンス

ISO/IEC 29100:2011 Privacy framework
（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

同意

- IoTでは従来方法による同意取得が困難な場合も
  - 図は同意のあてはめの両極端な例
- 現実的かつ有意な確認の仕組みが必要
- IoTのポテンシャル的には 権限委譲やトラスト に至る問題



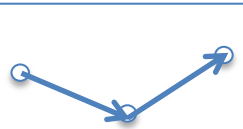
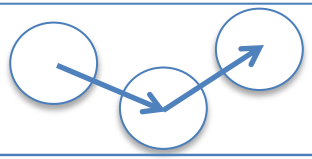


目的の限定とデータ最小化

- プライバシー原則
  - 『データ収集の目的を明確にして、その達成に必要最小限のデータだけを集めなさい』
- IoTで現実に起きていること
  - 研究開発の目的限定／目的表現の難しさ
  - データに新たな価値が発見されたときの対応
  - データの限定取得の技術的難しさ（コスト）
    - 例、画像（アナログデータ）から目的以外のデータの「映り込み」を削除することにはコストがかかる

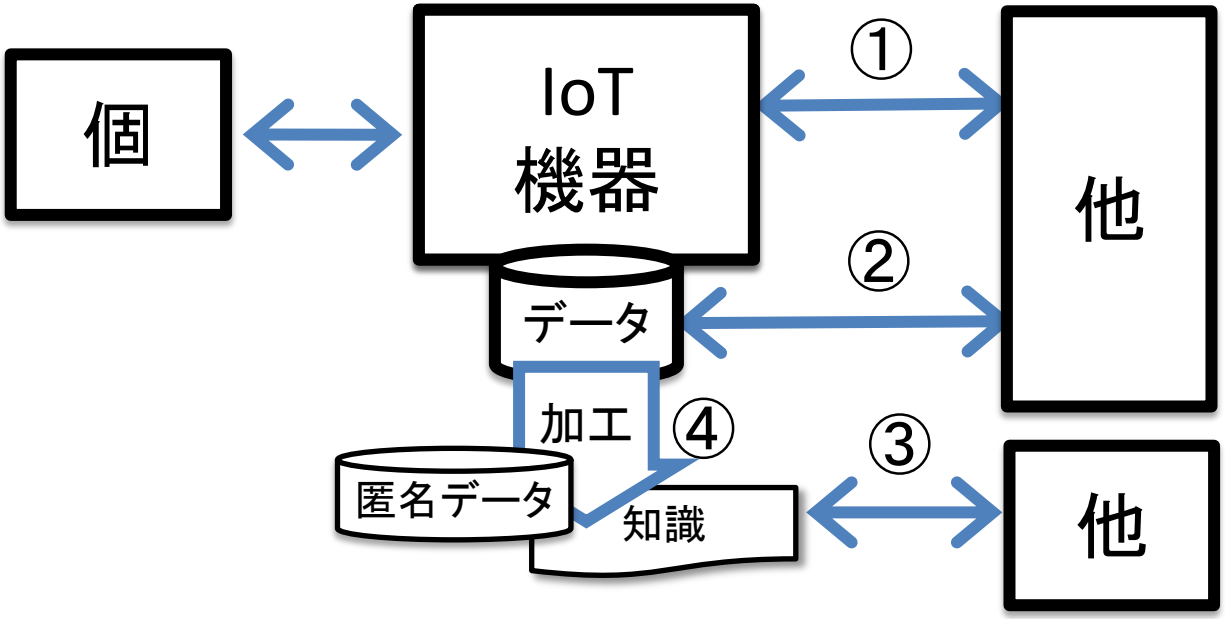
データ最小化（Data Minimization）

- データ最小化のパラメーターの例
  1. レコード数（集める機器数を制限する）
  2. 属性種（集める属性の種類を制限する）
  3. 属性粒度（集める属性の粒度を粗くする）
  4. 属性数（集める履歴の期間を制限する）
  5. 属性頻度（集める履歴の時間間隔を長くする）
- 位置情報の最小化の例

	max	minimize	例
属性粒度			1m単位 → 100m
属性数			5地点 → 3地点
属性頻度			30分毎 → 1時間

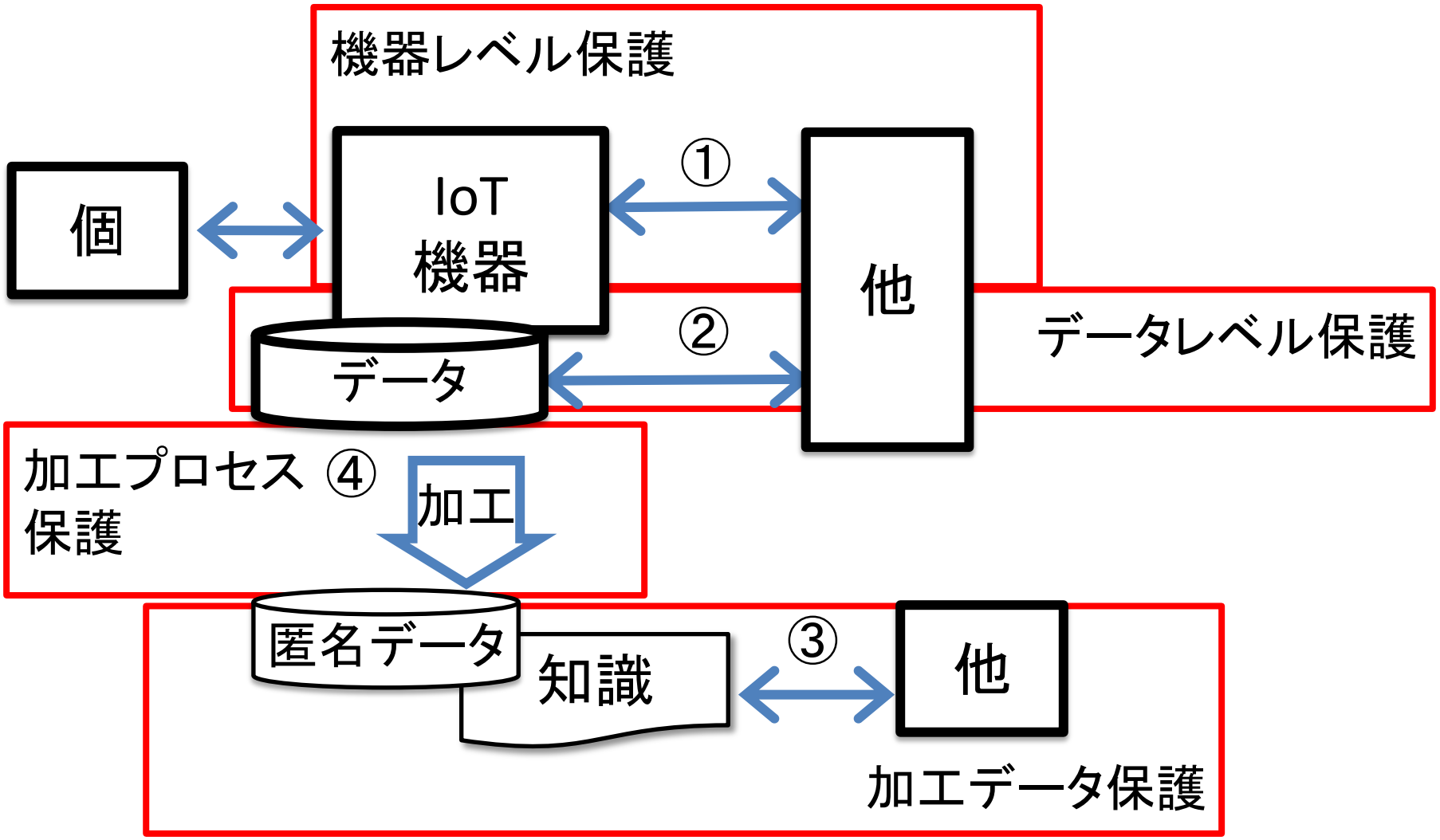
開示の制限・利用の制限

① IoT機器に対して正当な他者だけがアクセスできる
② IoT機器からのデータを正当な他者だけが受け取ることができる
③ IoT機器からのデータを加工して得られた匿名データや知識から個のプライバシーがもれない
④ IoT機器からのデータの加工処理で個のプライバシーがもれない



- **IoTにふさわしいプライバシー保護技術（開示の制限・利用の制限の課題解決）**

IoTにふさわしいプライバシー保護技術（開示の制限・利用の制限の課題解決）



① 機器レベル保護

- 認証で機器レベル保護
  - –不当な他者にデータを開示しないこと（認証）
  - –他者に必要以上のデータを開示しないこと（匿名認証）
- 公開鍵系の高機能暗号（楕円曲線暗号）で高度な制御が

IoT機器認証のプライバシー保護の2つのケース

サーバとしてのIoT機器

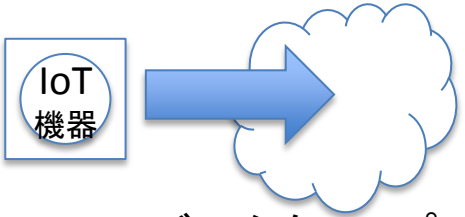
（IoT機器がクライアントを認証）

データを回答

- 適切な他者にのみデータを回答したい
- オープンかつ不特定のクライアントに対する認証が必要
- IoTで動く公開鍵ベースの認証

クライアントとしてのIoT機器

（クラウドがIoT機器を認証）

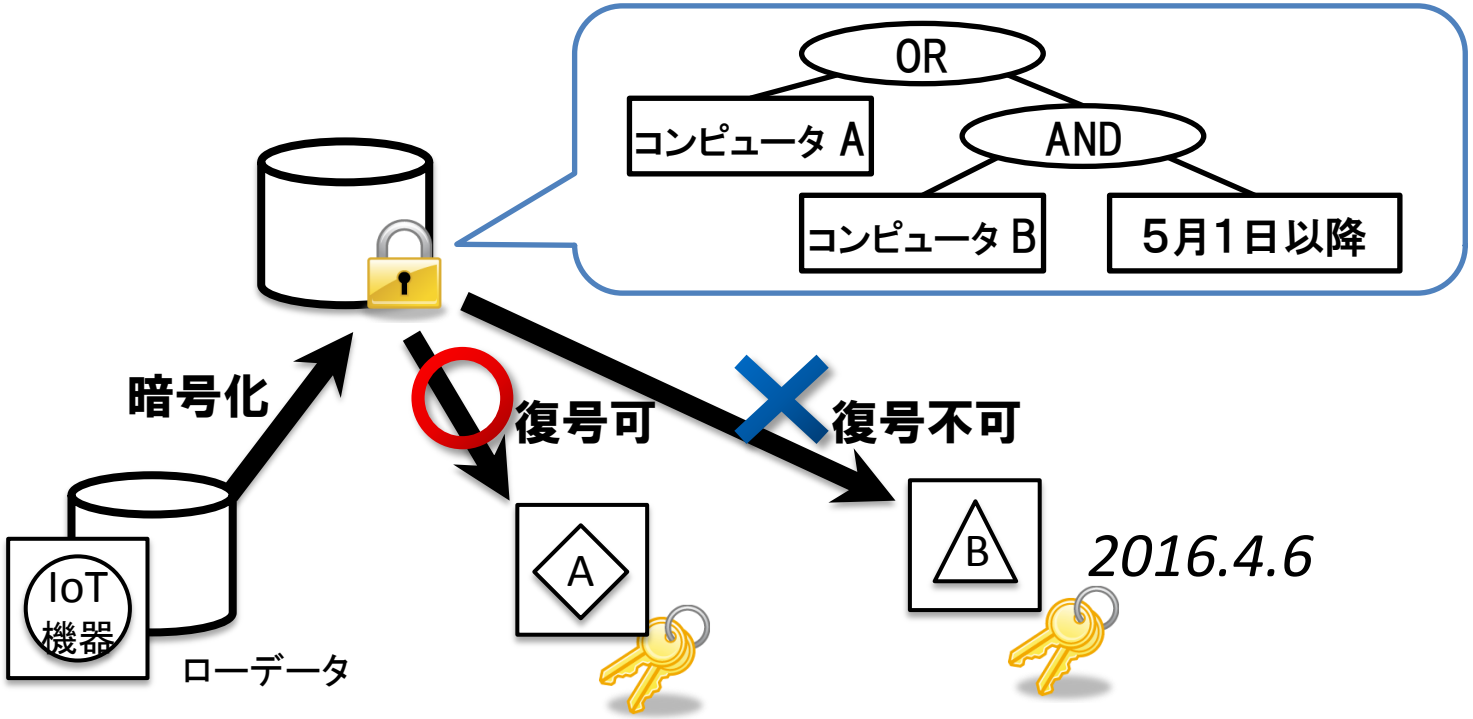


データをアップロード

- 匿名でデータだけアップロードしたい
- 匿名認証
  - 端末の証明書 (ID) を見せずに、メンバーであることを証明する暗号プロトコル

② データレベル保護

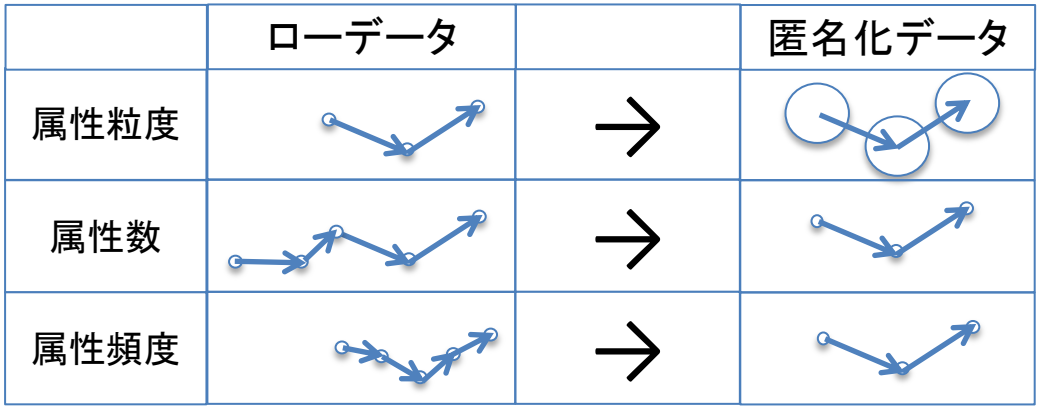
- 暗号でデータを保護
  - IoT機器から得られるデータを暗号化し、そのデータに開示制御機構を埋め込む
- 図の例
  - ローデータに開示条件を設定して暗号化
  - コンピュータA または B で5月1日以降の場合開示される



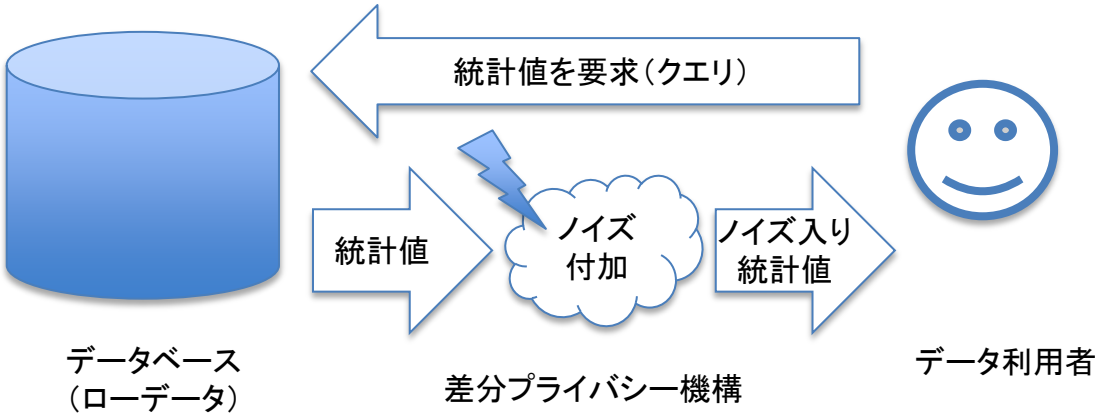
③ 加工データ保護

- 匿名化や「ノイズ」で加工データを保護
- IoT機器（周辺）でデータをプライバシーが守られた形式に加工する

- データ（系列）の匿名化
  - –位置情報の匿名化の例
  - –特定個のデータを識別できないよう、データを抽象化する
  - –粒度を1mから100mに粗くする
  - –地点数を5から3に短くする
  - –頻度を30分から1時間にまびく

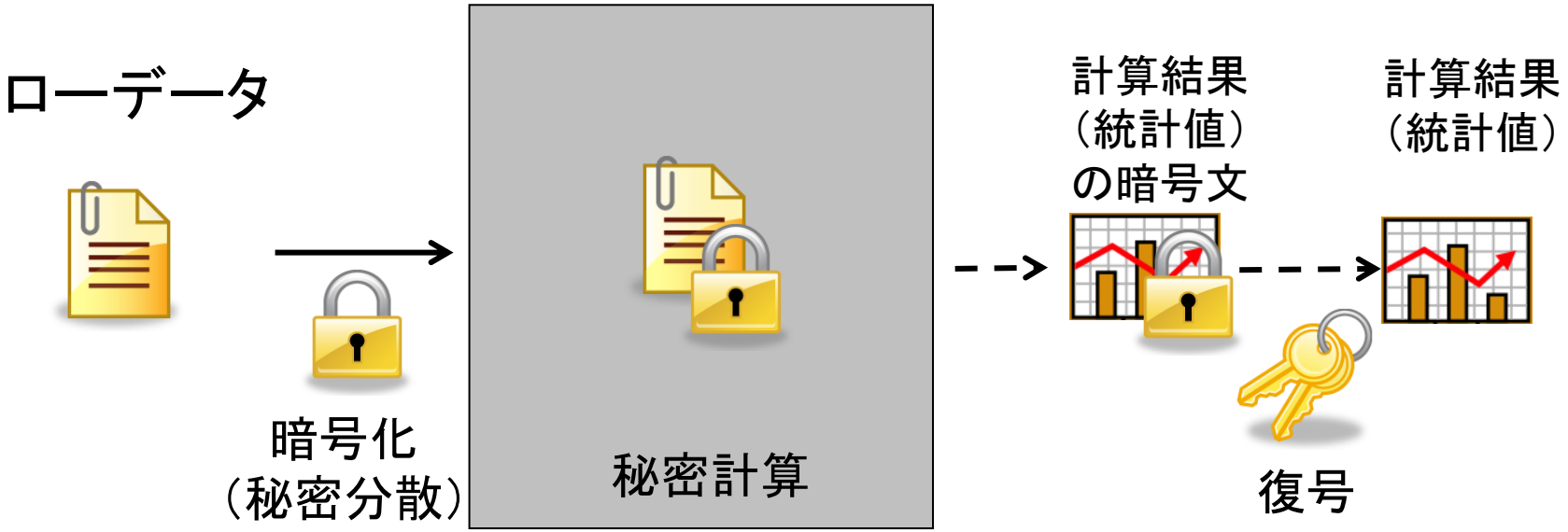


- 分析結果の保護
  - –統計値の保護の例（差分プライバシー）
  - –特定個のデータを識別できないよう、統計値にノイズを入れる
  - –『ある個のデータがあっても無くても、結果に（ほとんど）差がない』ようにする



④ 加工プロセス保護

- 暗号（秘密計算）で加工プロセスを保護
- IoT機器周辺の生々しいデータの安全管理
- 秘密計算（計算結果のみ開示）
  - データを暗号化して保存
  - データを暗号したまま計算
  - 計算結果の暗号文を出力



まとめ

- IoTプライバシーを以下の2観点から考察
  - IoT機器の保護
  - IoTから得られるデータの保護
- IoTにふさわしいと考えられるプライバシー保護技術を分野をしぼって解説
  - 開示の制限・利用の制限の課題解決
  - 楕円曲線暗号などの高度な暗号の利用によるIoTプライバシーの課題解決を提案