資料 2

PPM説明資料

2016. 04. 21

KDDI研究所　田中俊昭

資料概要

- プライバシーポリシーマネージャー(PPM)概要
- PPMの適用事例　HEMS実証プロジェクト
- PPM標準化状況
- 社会実装に向けた課題

プライバシーポリシーマネージャー(PPM)とは

パーソナルデータ提供のためのポリシ管理を行い、
利用者自らがデータの提供をコントロールできる機能を提供

サービスごとに個別に利用規約に同意する必要があり面倒
利用規約がわかりにくい
自分のどの情報がいつ取られるかわからない

特定の企業にだけ情報を公開することができます

企業Bのサービスには住所の情報が必要ですがどうしますか？

管理・確認

同意

公開する個人情報

メール ✓

住所 ✓

TEL

では、企業Bにだけ住所を公開します

PPM

■利用規約のわかりやすい表示

■サービス利用時の提供情報の管理
（プライバシー情報）

利用者に代わり、個人情報の管理
設定情報提供の履歴を可視化

などをPPMが代行

要求

通知

企業A：電力見える化

必要な個人情報

メール ✓

住所

要求

通知

企業B：見守りサービス

必要な個人情報

メール ✓

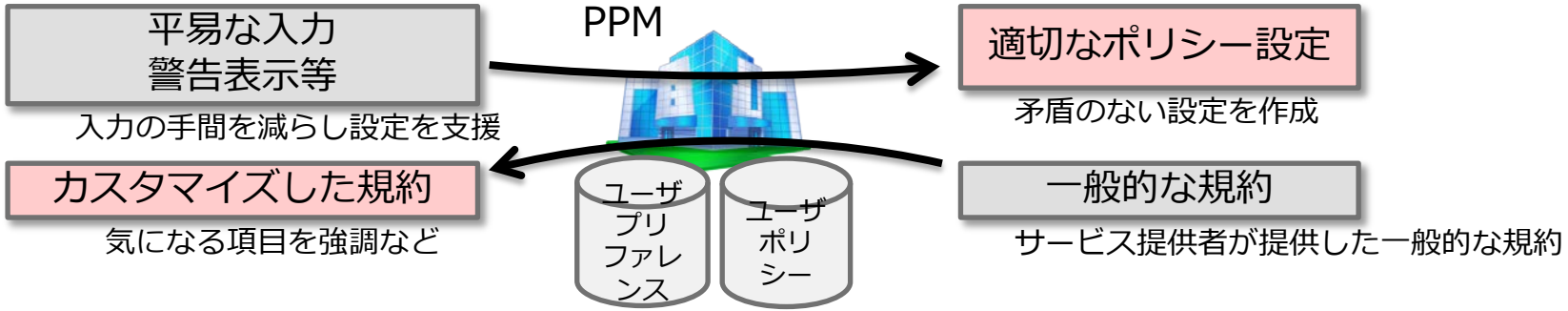
住所 ✓

利用者に信頼されるためのプライバシー課題とPPMの機能

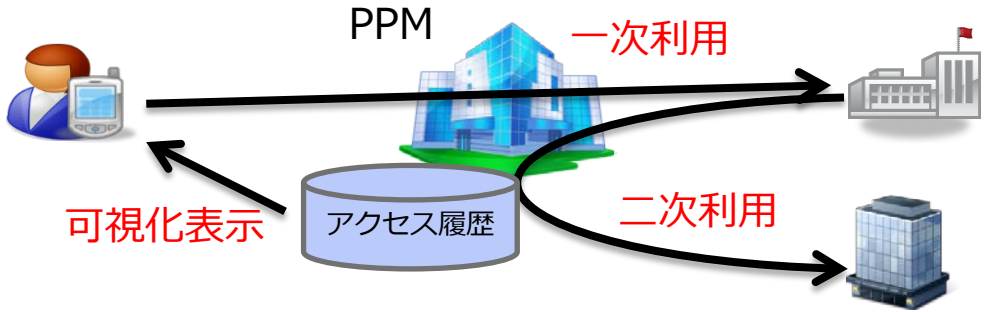
課題	PPMの機能
＜有効な同意を取る＞ （納得して同意してもらう） ※再同意を含む	わかり易い規約表示を含めた共通インターフェースを提供し同意取得を代行
＜第三者提供の透明性確保＞	データ提供履歴をPPMが保管しておき、ユーザに対して「見える化」する機能を提供
＜削除プロセスの確立＞	データ提供履歴を使ってデータ取得事業者に削除依頼を行う機能を提供

PPMの特徴

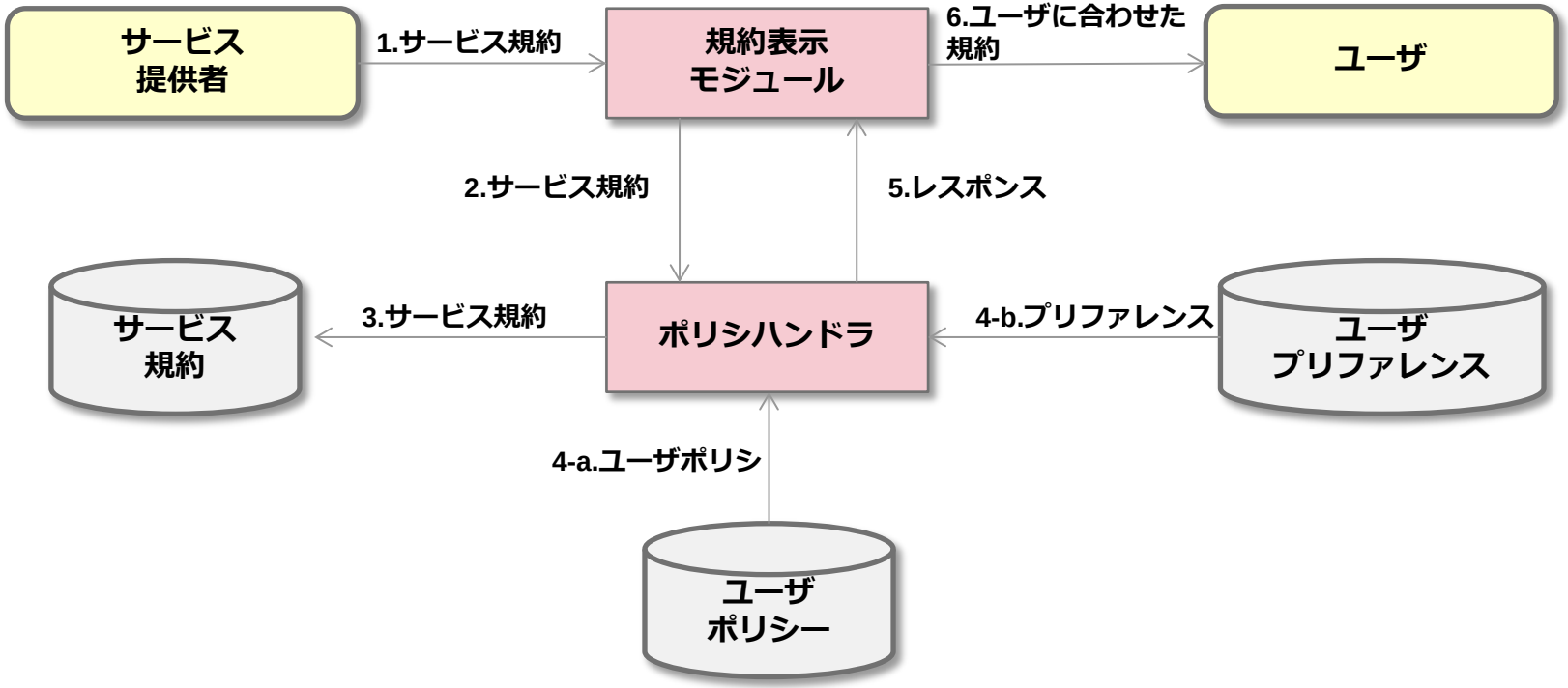
■ ユーザ支援機能：ポリシー設定の簡素化・サービス規約表示を最適化



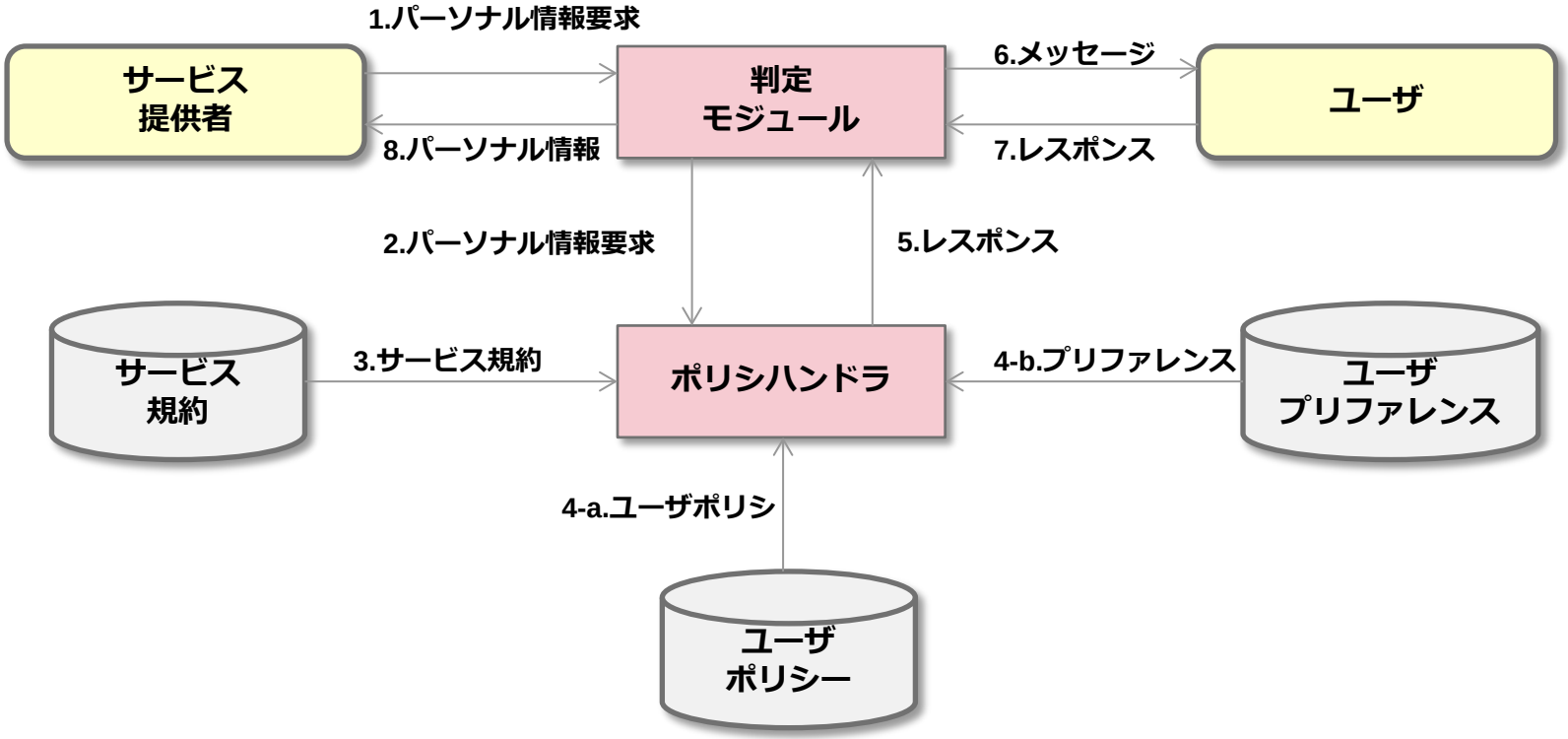
■ 可視化機能：パーソナルデータの利用状況を見える化・削除機能の提供



データフローモデル(初回サービス利用時)



データフローモデル（パーソナル情報要求時）



ユーザポリシー、プリファレンスの例

- 位置情報を要求する規約が提示されたときに、それをポップアップで通知
- 位置情報に関する規約を優先して表示
- 外部モジュールに関する箇所を強調
- 枠の色を変えるなど

ユーザポリシー

・位置情報の利用は禁止する

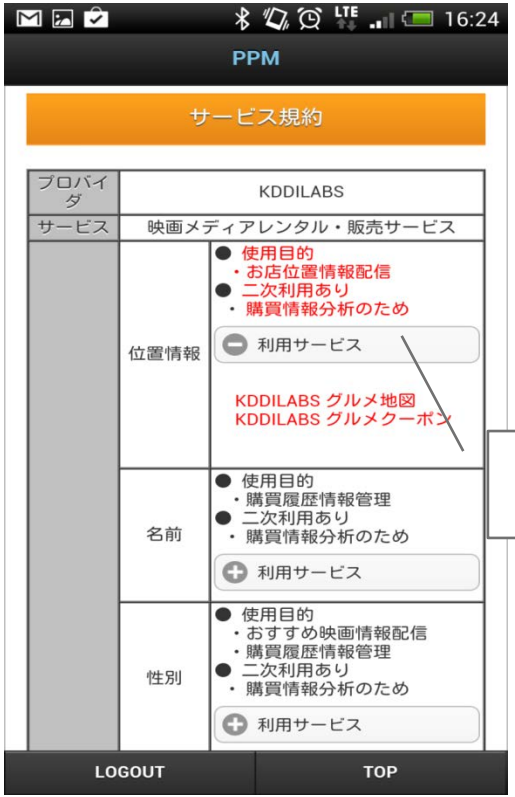
ユーザプリファレンス

・利用を禁止しているパーソナル情報が要求された場合、規約合意時に強調して通知する
・位置情報に関する規約は優先して表示する
・外部モジュールによる取得に関しては強調して表示する

プロバイダ	KDDI	
サービス	クーポンサービス	
取得情報	位置情報	・近くの店舗情報の提供に利用 ・自動的に取得 ・ぐるなびにサービス品質向上のために二次利用 ・外部モジュールは利用しない
	メールアドレス	・ダイレクトメールの送信に利用 ・自動的に取得 ・二次利用しない ・外部モジュールは利用しない
問い合わせ先	abc.xyz@kddi.com	

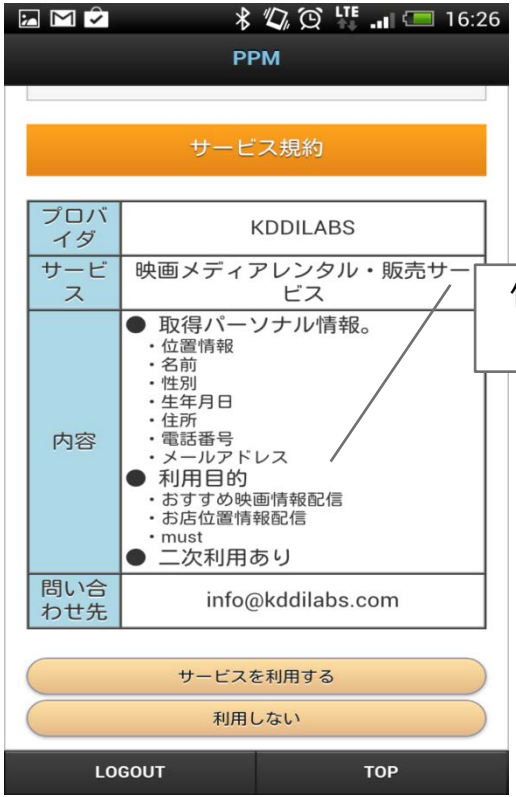
わかり易い規約表示の例

詳細に表示する設定の場合



項目ごとに使用目的を表示

簡素に表示する設定の場合



使用目的をまとめて表示

有効な同意を得るための工夫の例（iエネコンソーシアムの検討事例）

■ 規約を理解しやすくする支援機能

- 要約版プライバシーポリシーの作成
- ラベル表示、アイコン表示の併用

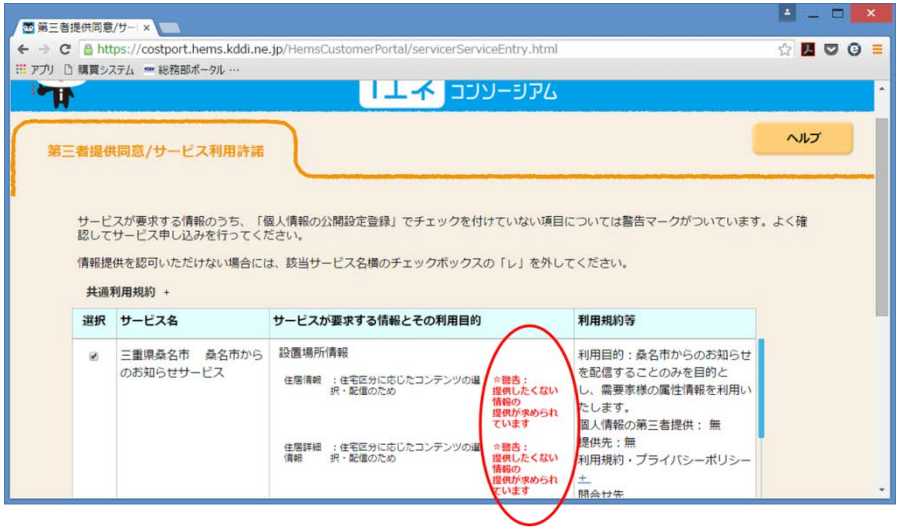
ラベル

	情報区分	取り扱いデータ・情報名
顧客情報	個人情報	氏名、住所、電話番号、メールアドレス など
	世帯情報	世帯情報（住宅種別、住宅取得区分、間取り、部屋割りなど）
	家族構成	家族構成、年齢
	顧客属性	性別、職業、所得、趣味 など
HEMSデータ	機器情報	機器ID、設置情報
	LIVE情報	動作情報 （HEMSによって検出した、家電、設備などの動作に関する情報）
	累積情報	電力量測定値（HEMS機器によって収集した電力量の積算値）
利用	第三者提供	第三者提供の有無

アイコン

■ 誤った判断をしないための支援機能

- ユーザが設定した基本ポリシーに従って注意すべき点をハイライト



明示的に提供を許可する情報にチェックを付ける必要はない。
許可していない情報には警告メッセージが表示される。

データ提供履歴表示機能の例

アクセス履歴の検索機能

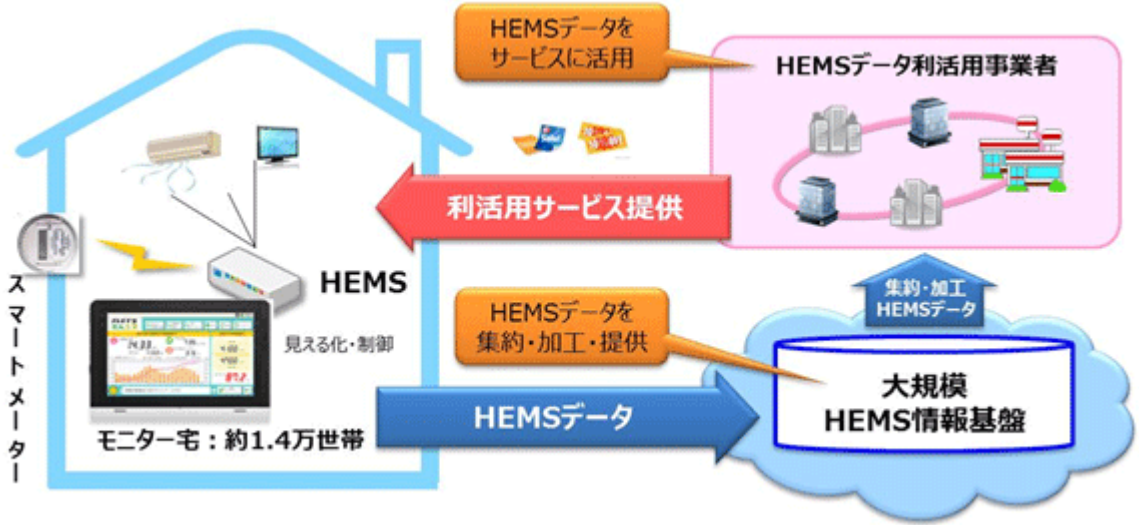
アクセス履歴の表示

※PPMはパーソナルデータ自体は持たず、アクセス履歴のみ蓄積する

HEMS実証プロジェクト実施概要

■「大規模HEMS情報基盤整備事業」　経産省の実証プロジェクト

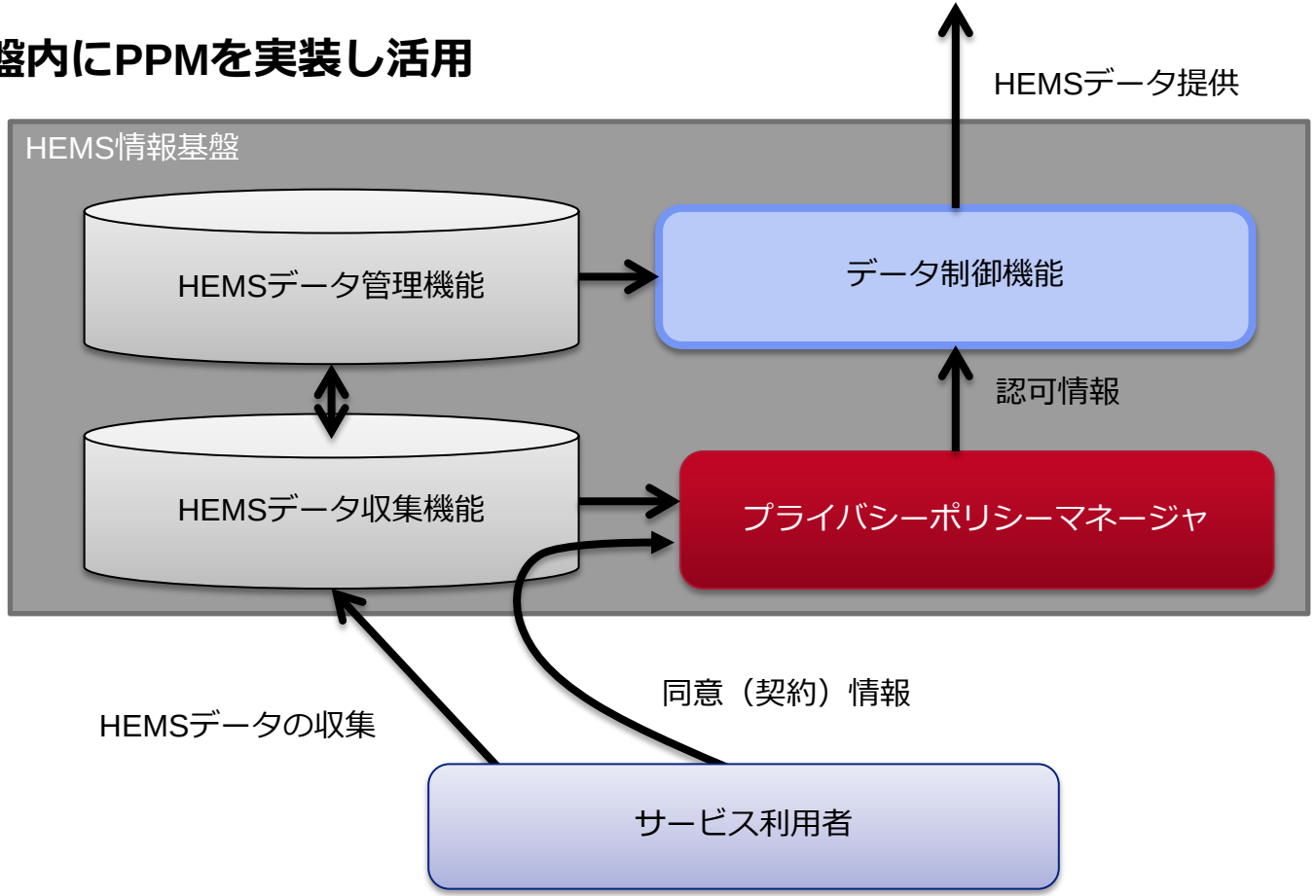
- **目的：**
  - HEMSの普及による省エネ・ピーク対策に貢献するとともに、電力データを活用した新しいサービスによるより便利で快適な社会の実現を目指す
    - » 大規模HEMS情報基盤の構築
    - » 大規模HEMS情報基盤の標準化検討
    - » プライバシーに配慮した電力利用データの利活用環境の検討
- **実施期間：**
  - 2014年9月～2016年3月
- **参加企業：iエネ　コンソーシアム**
  - 幹事会社
    - » 東日本電信電話（株）
    - » KDDI　（株）
    - » ソフトバンクBB（株）
    - » パナソニック（株）
  - 参加企業　約20社
- **実証規模：**
  - 約14000世帯のモニタを対象



http://news.kddi.com/kddi/corporate/newsrelease/2014/08/28/626.html

HEMS実証プロジェクトのおける組み込み事例

■ HEMS情報基盤内にPPMを実装し活用



oneM2MにおけるPPM標準化活動の背景と目的

■ oneM2Mについて

- 7つのSDO（標準化開発機構）がM2Mの標準を策定する目的で設立した標準化団体
  - ７つのSDO：ARIB, TTC（日本）, CCSA（中国）, TTA（韓国）, ATIS, TIA（米国）, ETSI（欧州）
  - 現在はインドのTSDSIが加わり8団体
- ESTIのM2M技術委員会（2009年2月設置）をもとに6つのSDOの協力を得て、大きな国際標準を目指して設立（2012年7月）
- 多くの通信キャリア、通信機器メーカ、チップベンダなどが参加

■ oneM2MでのPPM標準化活動の背景と目的

- oneM2Mにおけるプライバシー情報保護機構の必要性
  - プライバシー情報の保護の重要性は認識されていたが、情報を管理する視点での議論はされていなかった。KDDIの提案から、本分野の議論が活性化した。
- PPMをoneM2Mのエコシステム内で利用できるようにする
  - PPMをoneM2Mの仕様の一部として組み込むことで、oneM2Mに準拠したエコシステムが普及した場合に負荷なくPPMを組み込むことができ、PPMの普及を期待することができる。

oneM2MにおけるPPM標準化活動状況

■ PPM標準化に向けた経緯

■ oneM2MでのPPM標準化活動における成果

- **PPMを外部認可機能としてoneM2Mで新規に定義**
  - oneM2Mのアーキテクチャを使用したPPMのアーキテクチャをセキュリティ仕様書に反映
  - Release2の文書として記載される見込み（Normative、ただし実装方法はInformativeまたは範囲外）
- **PPMによる制御を実現するためにoneM2Mの制御機能を拡張**
  - PPMを用いた制御をoneM2Mで利用できるようにアクセスコントロール機能の拡張
  - Release2の文書として記載される見込み（Normative）

PPMをoneM2Mで利用可能にする大きな一歩

oneM2MにおけるPPM標準化に関わる諸外国の反応

■ Distributed Authorizationとの連携

- Datang社（中国）が提案していたDistributed Authorizationの活用先としてPPMが適しているため、連携して機能仕様を検討することとなった。

■ Terms and Conditions Mark-up Language（TACML）の提案とPPMとの連携

- PPMの提案に対応して、British Telecom社（BT、英国）がTerms and Conditions Mark-up Language（TACML）を提案。PPMとの連携を前提に、利用規約をマークアップ言語で記述して、PPMによるアクセス制御に必要となるプレファレンスの設定に利用することを想定。

■ PPMに対する寄書

- Gemalto社（フランス）、BT社（英国）から、PPMの標準化文書更新に関する寄書が提出されている。KDDI以外の組織からもPPMの標準化に貢献している。

■ CPDP（Computers, Privacy and Data Protection）におけるPPMの紹介

- プライバシー保護に関する国際会議であるCPDP2016（2016年1月、ブリュッセルにて開催）において、フランステレコム（フランス）からoneM2Mにおけるセキュリティ、プライバシーの取り組みの説明があり、そこで、PPMが紹介された。

IoT特有のプライバシー課題とPPMの適用

- **IoT/M2M特有のプライバシーに関わる検討課題**

✓ **データ提供判断の自動化**
  ✓ IoT/M2Mデバイスから送出されるデータの提供可否の判断は、ユーザの介在なしに行われる場合が多い。

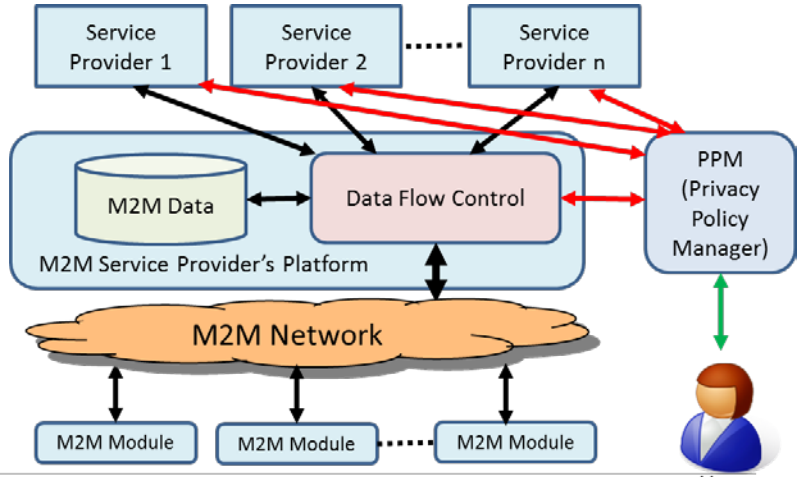
✓ **データ送信の不透明性**
  ✓ IoT/M2Mデバイスは自動でデータ送信を行うケースが多いため、ユーザがどのようなデータが送られているかわからない、という不安感がある。

✓ **データ所有権の確認**
  ✓ IoT/M2Mでは、デバイスの所有者とデータの所有者が異なるケースがある。

- **PPMの導入による効果**

・ユーザが、事前にデータ提供の可否を設定でき、事後にデータの削除ができる
・データ提供履歴を可視化できる
・提供されるデータに対してデータ所有者を指定できる

PPMの機能は、IoT特有のプライバシ課題を解決する上で有効



社会実装に向けた課題

■ 技術面

- サービス提供者から見たデータ提供IFの共通仕様策定
- ポータルサイトの機能要件の策定とガイドライン化
- プライバシーポリシー記述の標準化

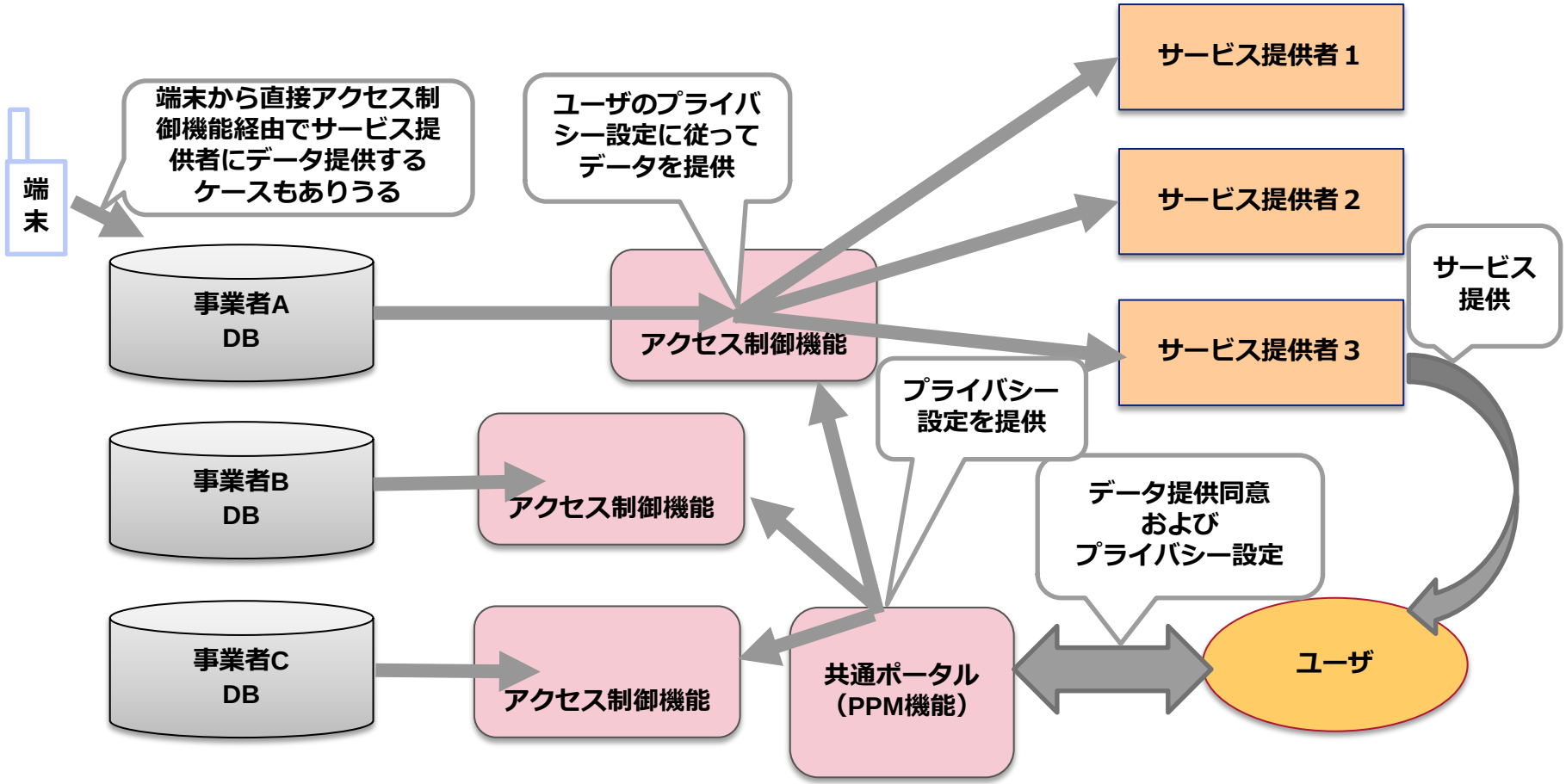
■ 制度面

- ポータルサイト(PPM)とアクセス制御機能の運用ガイドライン策定

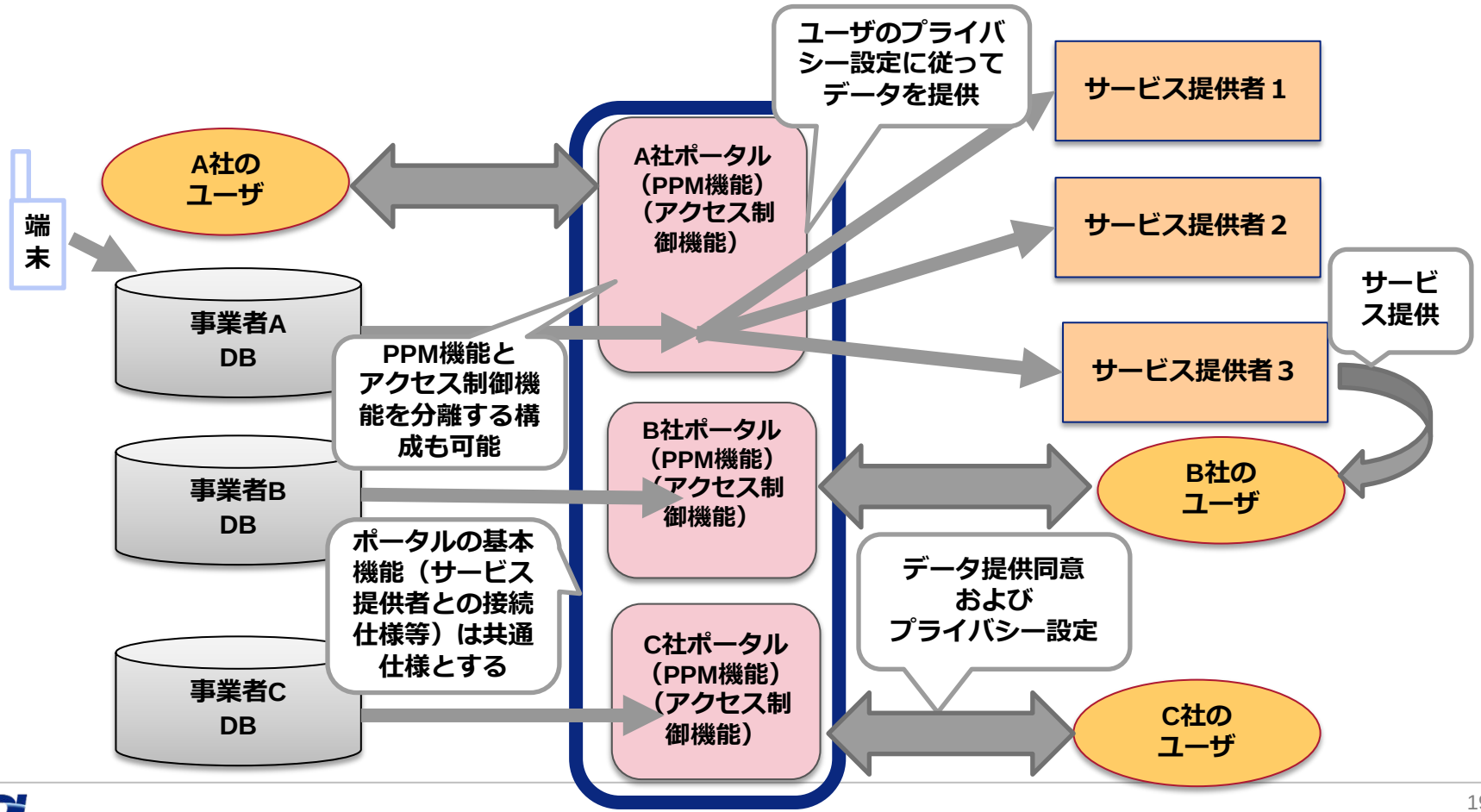
■ その他

- 実証による有効性検証とユーザ受容性の確認
- 持続可能なビジネススキームの構築（PPMの運用コストの確保）

社会実装のモデル：共通ポータル型



社会実装のモデル：個別管理型



PPMの通信事業への適用例

■ 適用先

- 通信事業者がサービス事業者に対して提供するID認証サービスにおいて、サービス事業者に提供するユーザの属性情報の提供の制御に適用する。

■ 現状

- 通信事業者によるID認証サービス（auID、GSMA Mobile Connect、等）において、通信事業者からサービス事業者に提供されるユーザの属性情報のユーザに対してその都度確認してから、提供。
- サービスに年齢制限がある場合の年齢確認等に活用。

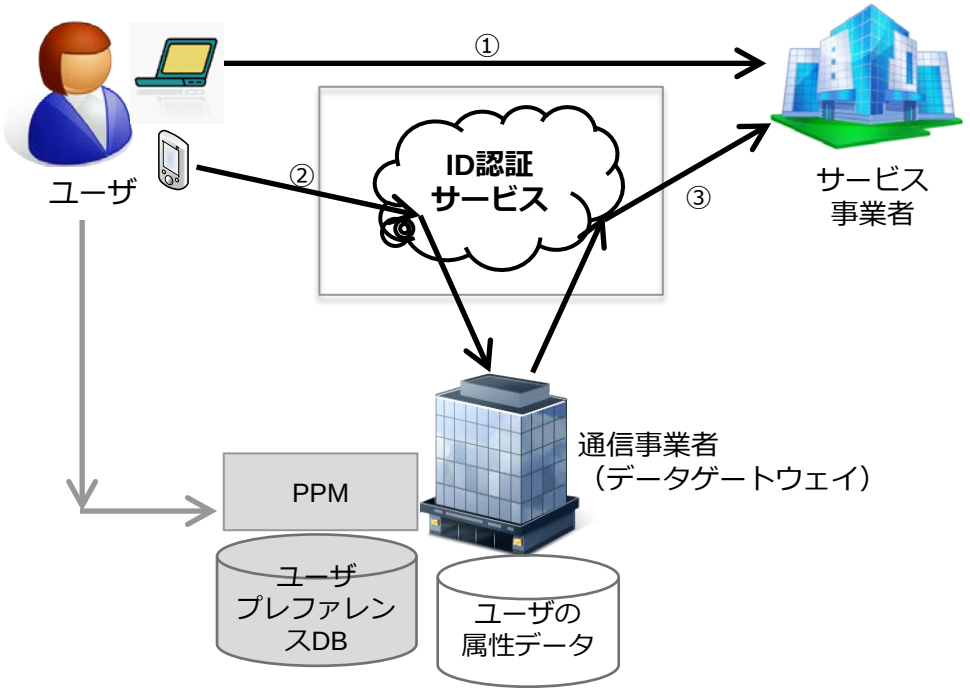
■ 課題

- サービスを利用するたびに、同意確認が求められる。
- 提供される属性データの種類が増えると、同意の手間が増える。

■ PPMの適用によるメリット

- ユーザがあらかじめプレファレンスとして属性状況の提供を定義することにより、属性情報提供による同意取得の手間が省ける。
- 属性情報の種類を増やすことができる。例えば、信用情報（支払い状況、等）や行動履歴（位置情報等のリアルタイムデータ）の活用により、新たなサービスが創出される可能性が高くなる。

認証サービスにおける属性情報の提供




Designing The Future
KDDI