

ワーキンググループ1 活動報告

佐古 和恵

NEC

ワーキンググループ1 (WG1) 「分散PDS」のシステムモデルを検討

「分散PDS」により個人が事業者と直接的関係を結ぶ基本モデルとその関係を仲介するメディアを基本モデルに付加した拡張モデルのアーキテクチャを設計

(<http://www.ducr.u-tokyo.ac.jp/jp/research/dbd-conso/index.html>より)

WG1(all time)メンバーリスト(28)

- アンリツ
 - 小熊
 - 安鳶
 - 渡邊
 - 尾坪
 - 秋山
 - 吉田
- シナジーマーケティング
 - 木虎
 - 藤井
 - 安松
 - 織田
- 日本IBM
 - 黒木
 - 宮田
 - 篠崎
 - 篠原
 - 青木
- インテージ
 - 伊藤
- DNP
 - 栃原
 - 土屋
 - 松山
- 大学・事務局
 - 橋田先生
 - 中川先生
 - 飯山先生
 - 笥先生
 - 奥貫先生
 - 加藤先生
- NEC
 - 佐古
 - 竹之内
 - 若目田

日時	名称	場所	内容
2015/2/5 15:00 ～17:20	第1回WG1	東京大学産学連携プラザ2階 大会議室	【議論】 WG1で議論するテーマについて
2015/3/2 15:30 ～17:30	第2回WG1	東京大学産学連携プラザ2階 2AB会議室	【議論】 学会発表先について、橋田先生のPLRについての説明と質疑
2015/3/23 15:30 ～17:30	第3回WG1	東京大学 工学部2号館31A会 議室	【議論】 DICOMO 発表申し込み内容について、ユースケースについて、システムアーキテク チャについて
2015/4/13 15:30 ～17:30	第4回WG1	東京大学産学連携プラザ2階 2AB会議室	【議論】 ユースケースについて、論文目次について
2015/4/21 10:30 ～12:00	第5回WG1	東京大学 工学部 2号館 3F 33B1	【議論】 DICOMO発表論文執筆の割り当てについて、掲載ユースケースの絞り込み
2015/5/8 15:30 ～17:30	第6回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 持ち寄った論文記述について
2015/6/9 10:00 ～12:00	第7回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 DICOMO論文まとめ中に議論した課題の見直し、標準化要件の検討、進捗状況の 確認
2015/7/2 14:00 ～16:00	第8回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 DICOMOプレゼン資料について、電子母子手帳 柏市のヒアリング、提案システム アーキテクチャとPLRの対応について
2015/7/14 10:30 ～12:30	第9回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 DICOMOプレゼンについての報告、PLRにおけるID管理とデータ共有方法について
2015/7/29 10:30 ～12:30	第10回WG1	東京大学工学部2号館 3階 電気 系会議室 1C 33A	【議論】 成果のまとめ方について、今後明確にしたいことの持ち寄り
2015/8/17 15:00 ～17:00	第11回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 名簿管理アプリとPLRにおける安全なデータ共有方法について、標準化へのアプ ローチについて、分散PDSの標準化を考えるにあたって、検討すべき要件の整理
2015/8/28 10:30～ 12:30	第12回WG1	東京大学 産学連携プラザ 2階 201 会議室	【議論】 報告書執筆項目と分担について

日時	名称	場所	内容
2015/2/5 15:00 ～17:20	第1回WG1	東京大学産学連携プラザ2階 大会議室	【議論】 WG1で議論するテーマについて
2015/3/2 15:30 ～17:30	第2回WG1	東京大学産学連携プラザ2階 2AB会議室	【議論】 WG1で議論するテーマについて
2015/3/23 15:30 ～17:30	第3回WG1	東京大学 工学部2号館31A会 議室	【議論】 WG1で議論するテーマについて
2015/4/13 15:30 ～17:30	第4回WG1	東京大学産学連携プラザ2階 2AB会議室	【議論】 WG1で議論するテーマについて
2015/4/21 10:30 ～12:00	第5回WG1	東京大学 工学部 2号館 3F 33B1	【議論】 DICOMO発表論文執筆の割り当てについて、掲載ユースケースの絞り込み
2015/5/8 15:30 ～17:30	第6回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 持ち寄った論文記述について
2015/6/9 10:00 ～12:00	第7回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 DICOMO論文まとめ中に議論した課題の見直し、標準化要件の検討、進捗状況の 確認
2015/7/2 14:00 ～16:00	第8回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 DICOMO論文まとめ中に議論した課題の見直し、標準化要件の検討、進捗状況の 確認
2015/7/14 10:30 ～12:30	第9回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 DICOMO論文まとめ中に議論した課題の見直し、標準化要件の検討、進捗状況の 確認
2015/7/29 10:30 ～12:30	第10回WG1	東京大学工学部2号館 3階 電気 系会議室 1C 33A	【議論】 DICOMO論文まとめ中に議論した課題の見直し、標準化要件の検討、進捗状況の 確認
2015/8/17 15:00 ～17:00	第11回WG1	東京大学 産学連携プラザ 2階 2AB 会議室	【議論】 名簿管理アプリとPLRにおける安全なデータ共有方法について、標準化へのアプ ローチについて、分散PDSの標準化を考えるにあたって、検討すべき要件の整理
2015/8/28 10:30～ 12:30	第12回WG1	東京大学 産学連携プラザ 2階 201 会議室	【議論】 報告書執筆項目と分担について

に加えて、電話会議
3,4回

WG1のメーリングリス
トの
総流量 589通！

ワーキンググループ1 (WG1) 「分散PDS」のシステムモデルを検討

「分散PDS」により個人が事業者と直接的関係を結ぶ基本モデルとその関係を仲介するメディアを基本モデルに付加した拡張モデルのアーキテクチャを設計

(<http://www.ducr.u-tokyo.ac.jp/jp/research/dbd-conso/index.html>より)

成果

- 「分散PDS」により個人が事業者と直接的関係を結ぶ基本モデルのアーキテクチャを設計
- その構想をDICOMO2015(安比高原)にて発表
- PLRと対比し、過不足を検討
- PLRにおける安全なデータ共有方式を議論
- 今後、分散PDSの標準化を検討するにあたって、考慮すべき要件を整理
- 「メディエータ」はサービスプロバイダの一形態(マッチングサービス)として詳細検討は割愛

論文：個人情報データを本人が管理するPDSシステムモデル —「集めないビッグデータコンソーシアム」における検討報告—

個人情報データを本人が管理する PDS システムモデル —「集めないビッグデータコンソーシアム」における検討報告—

青木孝裕¹ 秋山智宏² 坂山裕³ 伊藤直之⁴ 小原康之⁵ 森田朝美⁶ 加藤綾子⁷
木虎直樹⁸ 黒木信彦¹ 佐古和恵¹ 竹之内隆夫¹ 中川裕志¹ 橋田浩一¹
藤井絵美子¹ 松山純² 宮田智博¹ 安松健⁹

概要：個人が自らデータを蓄積・管理し、かつ事業者等が個人情報を利用できる仕組みが必要であるが、それを実現するツールはまだ十分に普及しているとはいえない。本報告では、個人情報等を本人(または代理人)が管理し、データの利用を本人同意に基きさせる PDS (Personal Data Store) のシステムモデルを検討する。具体的には、ユースケースを踏まえながら PDS の必要十分条件を検討し、現地で実証可能な機能とシステムモデルを提示する。なお、本報告は「集めないビッグデータ」コンソーシアムのシステムモデル検討 WG の検討内容をまとめたものである。

System Model for Personal Data Store(PDS) Managed by Individuals - Report from DBD Consortium -

Takahiro AOKI¹ Tomohiro AKIYAMA² Hiroshi IYAMA³ Naoyuki ITO⁴
Yasuyuki OGUMA⁵ Asami ORITA⁶ Ayako KATO⁷ Naoki KITORA⁸
Nobuhiko KUROKI¹ Kazuo SAKO¹ Takao TAKENOCHI¹ Hiroshi NAKAGAWA¹
Koiti HASIDA¹ Emiko FUJII¹ Len MATSUYAMA² Tomohiro MIYATA¹
Ken YASUMATSU⁹

1. はじめに

ビッグデータ時代において、個人に紐づくデータに関して本人同意を得ながら、事業者等が個人情報を利用できる仕組みを確立することが社会的急務となっている。そこで、東京大学の「集めないビッグデータ」コンソーシアムでは、個人情報の管理と意思決定を個人に帰属させた技術的・社会的モデルの構築を目指し、2014 年 10 月より、2つのワーキンググループ(WG)体制で、システムモデルと社会受容性の両面から PDS (Personal Data Store) に関する検討を進めている。

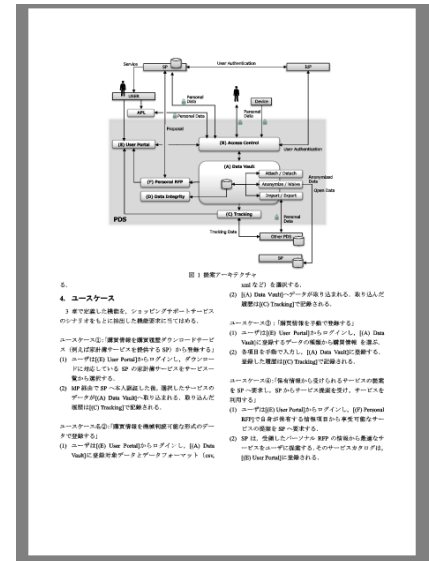
PDS とは、個人が自分のデータを電子的に蓄積・保管し、他者と共有・活用する仕組み[1]である。個人を軸にデータが蓄積・管理され、データの表示や提供の範囲等を個人が決定できる仕組みが普及すれば、本人の意思がより適切に反映されたデータ利用が可能となる。また、事業者等が個人情報を含む膨大なデータを抱え込むことによって生じるリスクも低減することができる。

プライバシーと個人情報保護、パーソナルデータ流通に係る国際的な動向[2][3][4][5]や、企業の国際競争力向上などの観点から、このような仕組みを日本でも導入することの社会的要請と意義は非常に高い。しかしながら新たな技術的・社会的モデルを実現するためには課題も多く、さまざまな見地から議論をしておかねばならない。そこで、「集めないビッグデータ」コンソーシアムの社会受容性検討 WG では、複数の事業者等が個人データを共有して地域コミュニティ等で活用する際の社会モデルについて、ルールや制度設計の観点から検討を行っている。システムモデル検討 WG では、技術的な側面から PDS のアーキテクチャ構築を目指し、議論を進めている。本稿は同コンソーシアムのシステムモデル検討 WG に基づく検討報告である。本報告を通じて、我々個人情報の適切な管理と流通の促進に向けて貢献することを目指している。

- 1 日本アイ・ビー・エム IBM Japan
- 2 アシラエンジニアリング Asira Engineering
- 3 東京大学 The University of Tokyo
- 4 インテラジ INTAGE
- 5 アシラ Asira
- 6 システムマーケティング Strategy Marketing
- 7 文政大学 Bunkei University
- 8 NEC NEC
- 9 大日本印刷 Dai Nippon Printing

著者17名

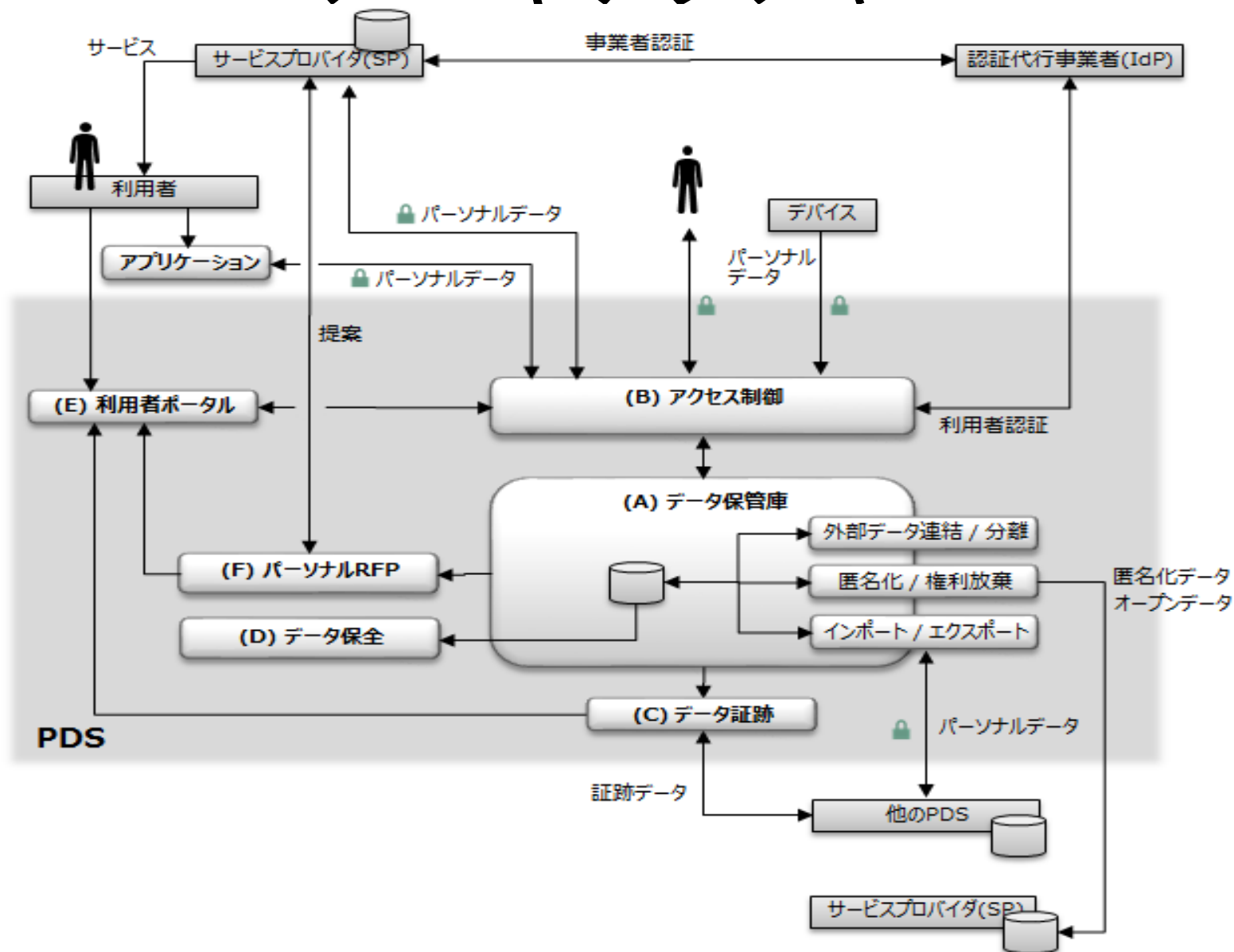
9組織



- 図 1 システムアーキテクチャ
- 1 ユーザー認証
 - 2 ユーザープロファイル
 - 3 サービス認証
 - 4 サービスプロファイル
 - 5 サービス認証
 - 6 サービスプロファイル
 - 7 サービス認証
 - 8 サービスプロファイル
 - 9 サービス認証
 - 10 サービスプロファイル
 - 11 サービス認証
 - 12 サービスプロファイル
 - 13 サービス認証
 - 14 サービスプロファイル
 - 15 サービス認証
 - 16 サービスプロファイル
 - 17 サービス認証

項目	内容	備考
1	ユーザー認証	ユーザー認証を行うための機能
2	ユーザープロファイル	ユーザープロファイルの管理を行うための機能
3	サービス認証	サービス認証を行うための機能
4	サービスプロファイル	サービスプロファイルの管理を行うための機能
5	サービス認証	サービス認証を行うための機能
6	サービスプロファイル	サービスプロファイルの管理を行うための機能
7	サービス認証	サービス認証を行うための機能
8	サービスプロファイル	サービスプロファイルの管理を行うための機能
9	サービス認証	サービス認証を行うための機能
10	サービスプロファイル	サービスプロファイルの管理を行うための機能
11	サービス認証	サービス認証を行うための機能
12	サービスプロファイル	サービスプロファイルの管理を行うための機能
13	サービス認証	サービス認証を行うための機能
14	サービスプロファイル	サービスプロファイルの管理を行うための機能
15	サービス認証	サービス認証を行うための機能
16	サービスプロファイル	サービスプロファイルの管理を行うための機能
17	サービス認証	サービス認証を行うための機能

アーキテクチャ

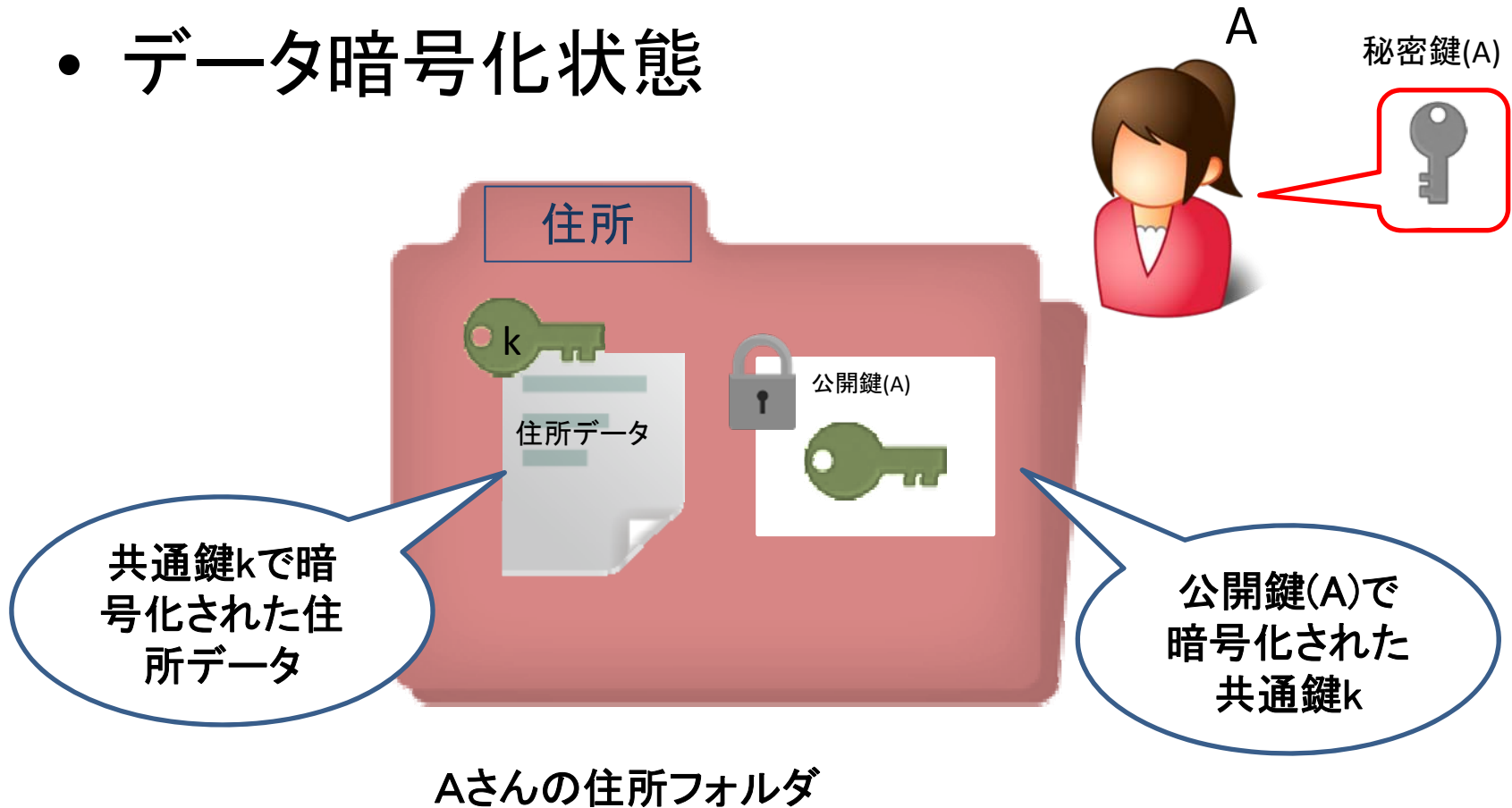


活動概要

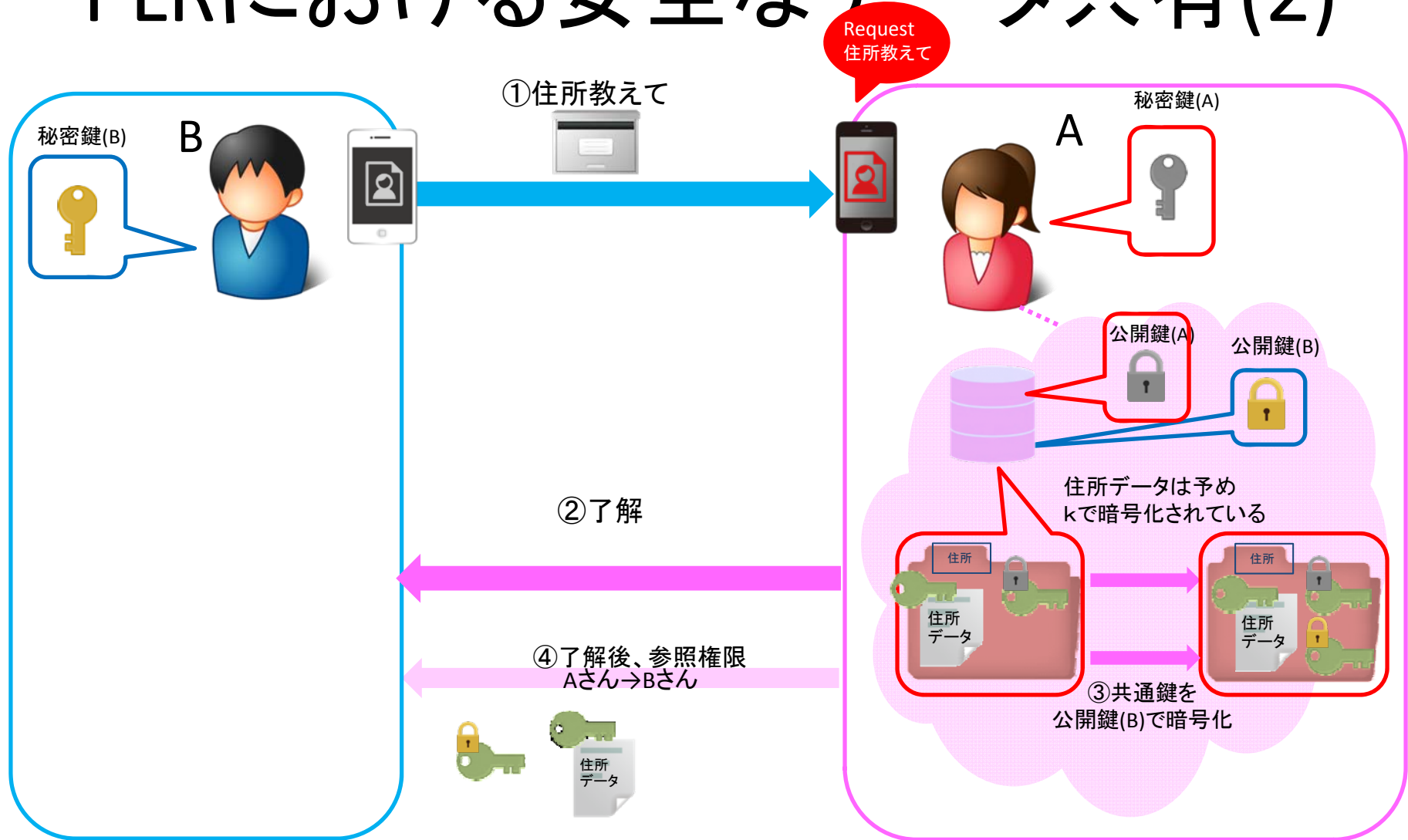
- WG1活動2月スタート
- 3月末 論文タイトル、著者リストの決定、論文目次案策定(検討項目案)
- 4月末 要件の明確化、論文執筆(締切5/15)
- 5月末 アーキテクチャ策定開始、
- 6月末 プレゼン資料準備(発表7月上旬)
- 7月末 PLRとの対応検討
- 8月末 標準化に向けた要件整理
- 9月末 全体まとめ、発表先検討

PLRにおける安全なデータ共有(1)

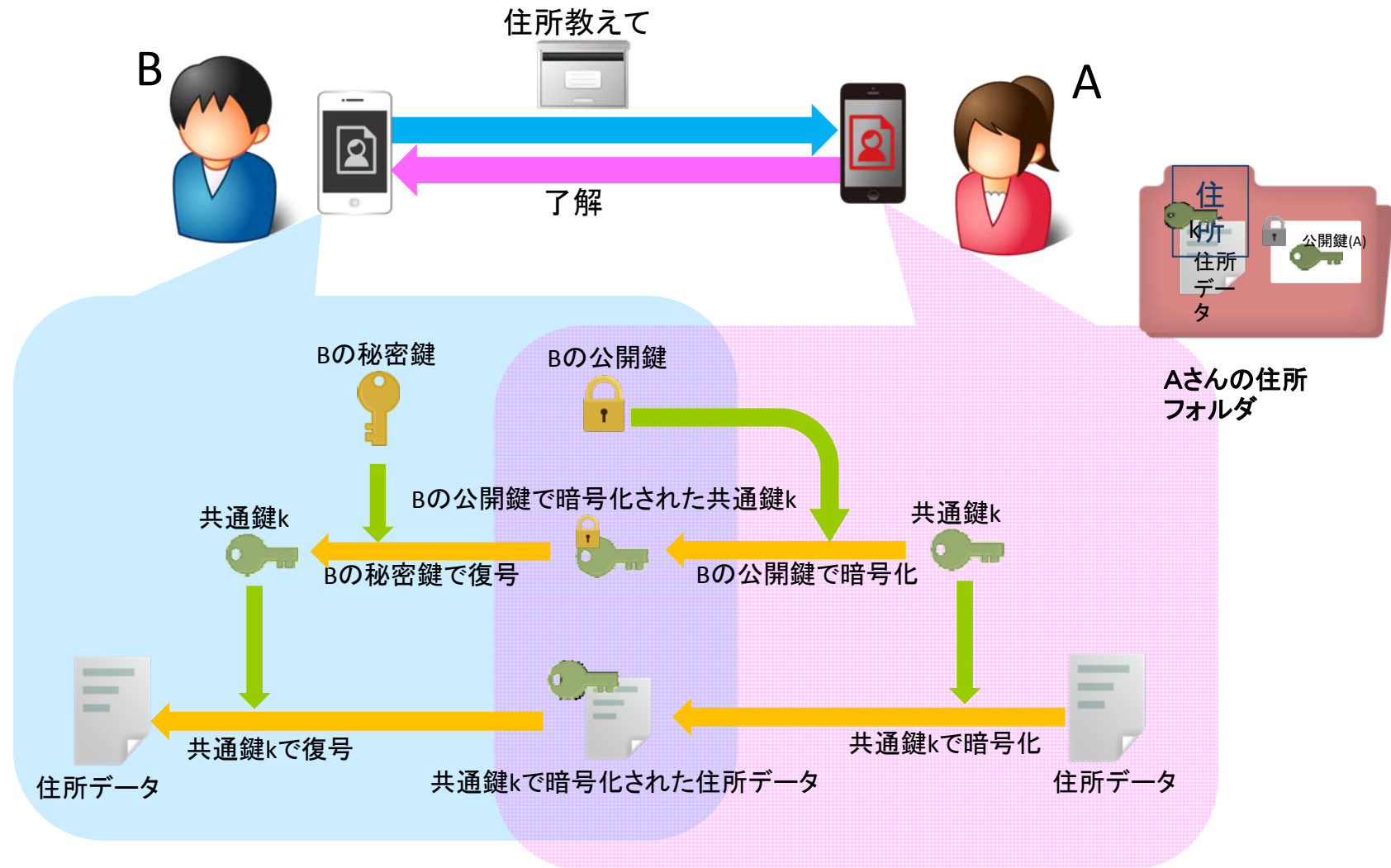
- データ暗号化状態



PLRにおける安全なデータ共有(2)



共有ができる理由



今後考慮すべき要件

- **汎用性**: 多種のパーソナルデータを統合的に扱える
 - － 1つの業界に特定されないこと
 - － 異なる機微度の情報を扱えること
 - － 情報の意味を互いに理解しあえること
- **継続性**: 個人の一生および複数の世代にわたり継続的に利用できる
 - － ハードウェア・ファームウェアの改版に対応する手立てが考慮されていること
- **互換性**: 多くの事業者が参画できる
 - － 新たなサービスを創り出しやすいOpen性も確保すること
 - － さまざまなプラットフォームで利用できること
- **信頼確保**: 個人(利用者)による自己情報コントロールが可能である
 - － VRM(Vendr Relationship Management)を実現する基本機能が備わっていること
- **安全性**: パーソナルデータの漏洩や不正な利用を防げる
 - － 個人認証、企業認証の確保
 - － データ信憑性の確保
 - － サイバー攻撃への耐性(悪意者からのアクセスを排除できること)

積み残し課題

- 「メディエータ」はサービスプロバイダの一形態（マッチングサービス）として詳細検討は割愛
- 「データ開示条件」の構造化には未着手

まとめ

- 「分散PDS」により個人が事業者と直接的関係を結ぶ基本モデルのアーキテクチャを設計した
- PLRにおける安全なデータ共有方式を議論した
- 今後、分散PDSの標準化を検討するにあたって、考慮すべき要件を整理した
- 「メディエータ」はサービスプロバイダの一形態（マッチングサービス）として詳細検討は割愛

おまけ FAQ(1/3)

- 「集めないビッグデータ」は集めているのではないですか？
 - 現状の、企業が個人のデータを「集めている」状態へのアンチテーゼである。個人が個人のデータをそれぞれ集める。

おまけ FAQ(2/3)

- 集めた個人のデータの実体はどこにあるのですか？
 - 実装依存だと思われる。個人のスマホにあってもよいし、PLRのように外部クラウドサービスにあってもよいし、PDSを提供するサービスプロバイダが管理するかもしれない。もしかしたら秘密分散技術を使って、複数のクラウドサービスに分散されて存在していることも考えられる。

おまけ FAQ(3/3)

- ということができたら「個人が管理する」状態になるのですか？
 - まさにWG内で繰り返し論じられてきた質問だが、明確な線引きはできなかった。
 - たとえば、パソコンに入っているデータは「個人が管理している」と言えるのか？OSの会社が勝手にクラウドに転送している場合には？
 - データにポータビリティがあって、プロトコルにオープン性があって、「管理できていない」と思えた時に、別のプロバイダやソフトウェアに乗り換えることができることではないか。(私見)
 - 少なくとも、データの使用許可の権限を本人が持っているということが必須
 - 本人がデータを「消去」できることも重要
 - データの「所有」の概念とともに、オーブンプロブレム