



ブロックチェーンで世界を簡単に。

ブロックチェーンID“bPassport”概要と活用事例 ～DIDとの関係～

株式会社 bitFlyer Blockchain
金光 碧

2020年12月3日

目次

1. 当社のブロックチェーン“miyabi”の概要
 2. 当社のブロックチェーンID“bPassport”の概要
 3. 当社のブロックチェーンID“bPassport”と
W3Cにより定義されたDIDの関係
- Appendix. “bPassport”活用事例

注：

当社のブロックチェーンID「bPassport」は「分散ID」「SSI」であり、仕組み、事例をご説明させて頂いた後、W3CによるDIDとの定義との関係、W3Cにより定義されたDIDにおいてブロックチェーンを使うメリット、デメリットについてお話しさせていただきます。

「bPassport」はW3Cにより定義されたDIDの規格には準拠予定ですが、アーキテクチャはW3CのDIDの定義にマッチしていると当社では考えています。

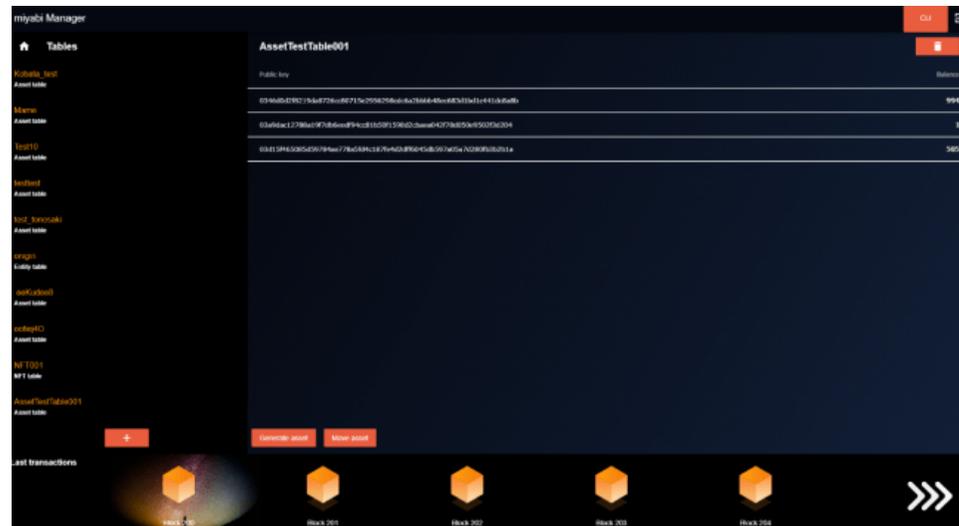
当社のブロックチェーン“miyabi”の概要

独自開発プライベートブロックチェーンmiyabi

bitFlyer Blockchainはプライベートブロックチェーンmiyabiを開発し本番環境で運用しております。
データがすぐに確定するというファイナリティを有し、また単一障害点を排除したBCで秒間4000トランザクション以上は世界最速だと言えます。

ブロックチェーンの五大利点

- ① ビザンチン耐性 (BFT)
- ② 改ざん耐性
- ③ 高可用性 (単一障害点の排除)
- ④ アドレス (公開鍵) による疎結合の容易さ
- ⑤ エンタープライズ間でのデータ共有の容易さ



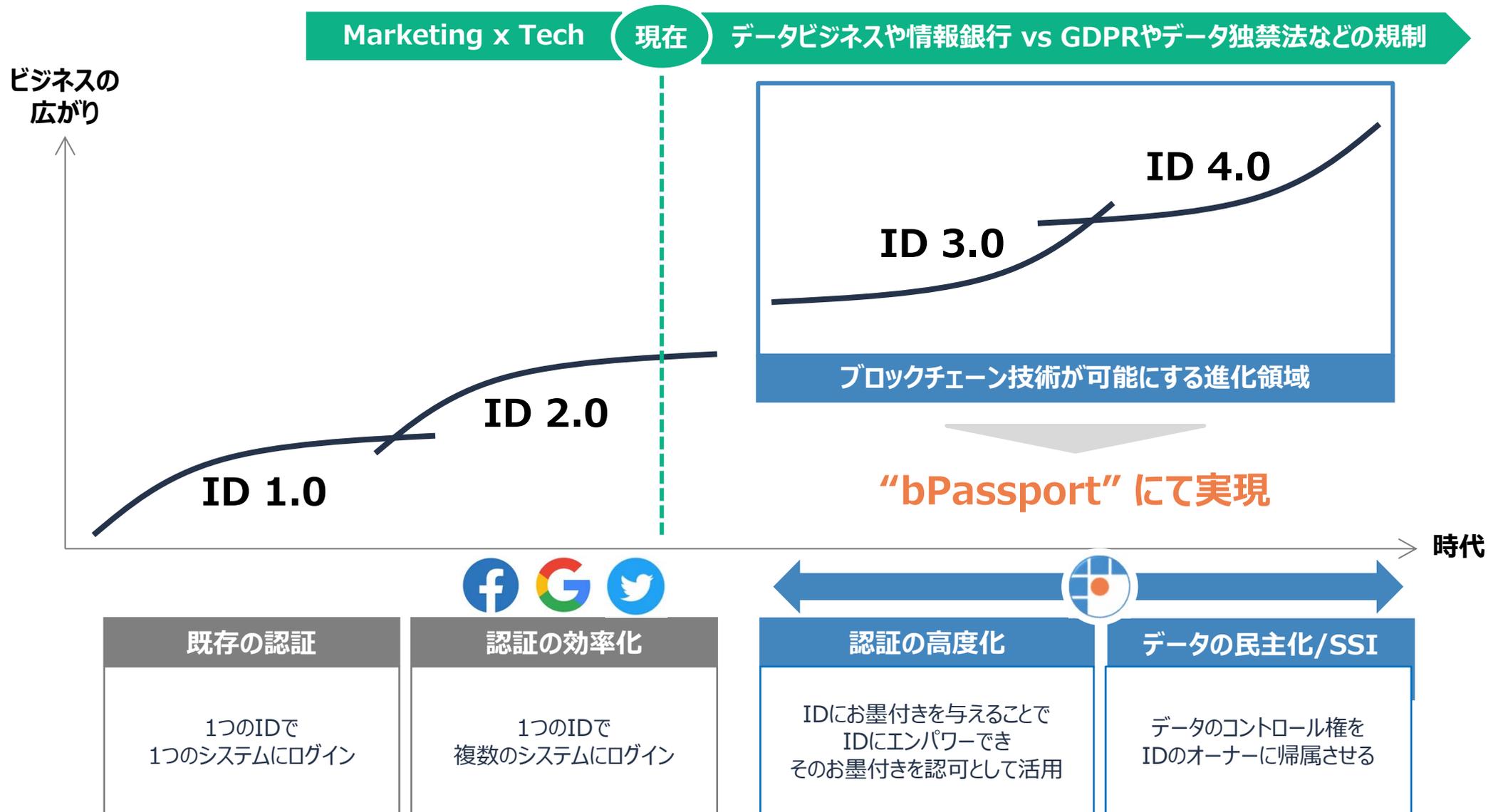
miyabiはタブレットでも稼働



当社のブロックチェーンID“bPassport”の概要

IDの進化論

ID にブロックチェーン技術に応用した ID3.0 / 4.0 の領域では、ID2.0 の世界とは非連続な領域にあるビジネスが創出され、ID へのエンパワーやユーザー自身によるデータコントロールが可能となります。



個人情報流通の将来像

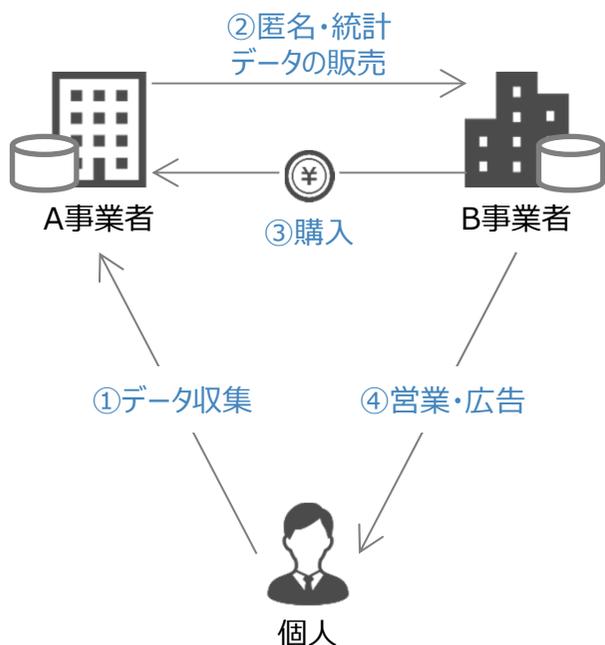
これまでは個人の意思に関係なく事業者間で消費者情報の流通が行われていましたが、今後は情報銀行・情報信託や個人主権型IDサービスにより、個人の意思で情報流通のコントロールが可能となっていくと考えています。

AsIs

ToBe

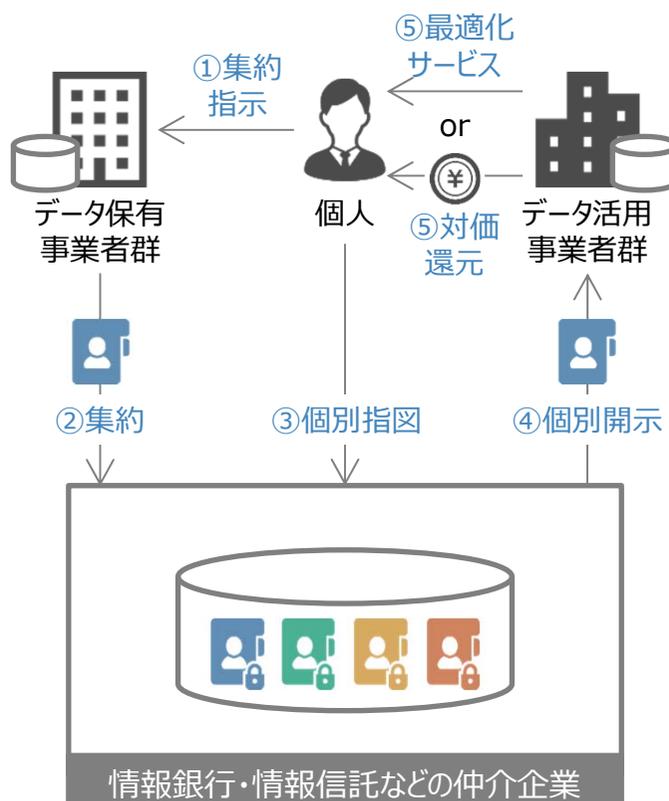
事業者間のダイレクト流通

事業者間のデータ授受を個人が認識しておらず
本人が希望しない営業や広告などが発生



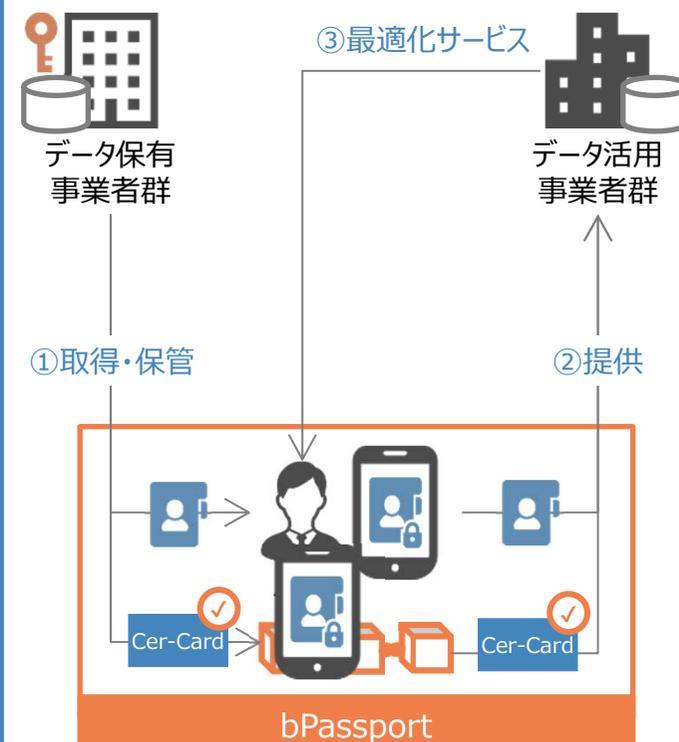
情報銀行・情報信託

個人が自らの意思で情報の流通先を決める
情報管理や開示先コントロールは仲介企業が実施



個人主権型IDサービス (SSI)

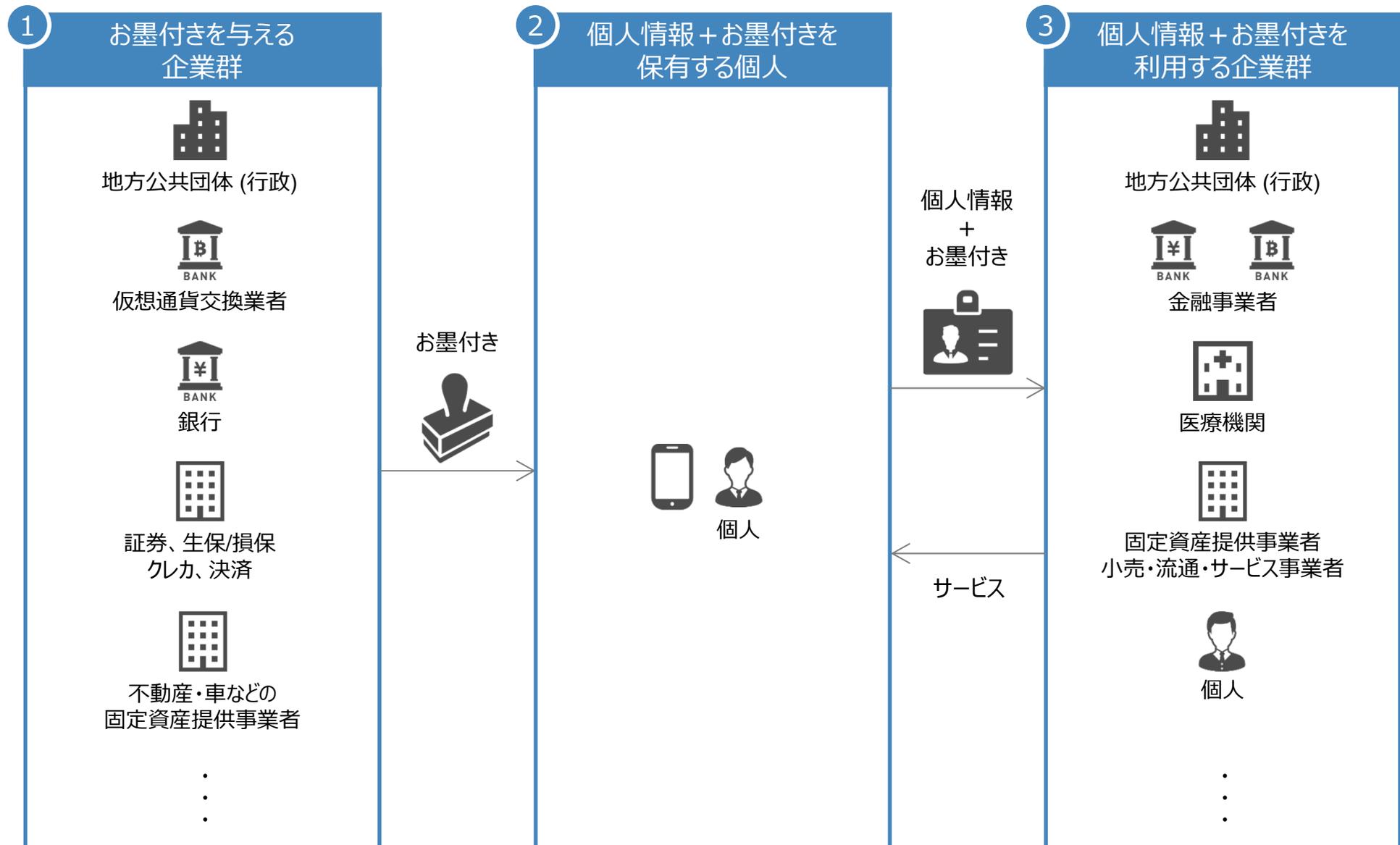
個人が自身の情報を取得・保管し、提供先を決める
データ保有企業のCertも渡せるため真正性を保証



※Cer-Card : 様々なデータ保有事業者群から与えられる「お墨付き」

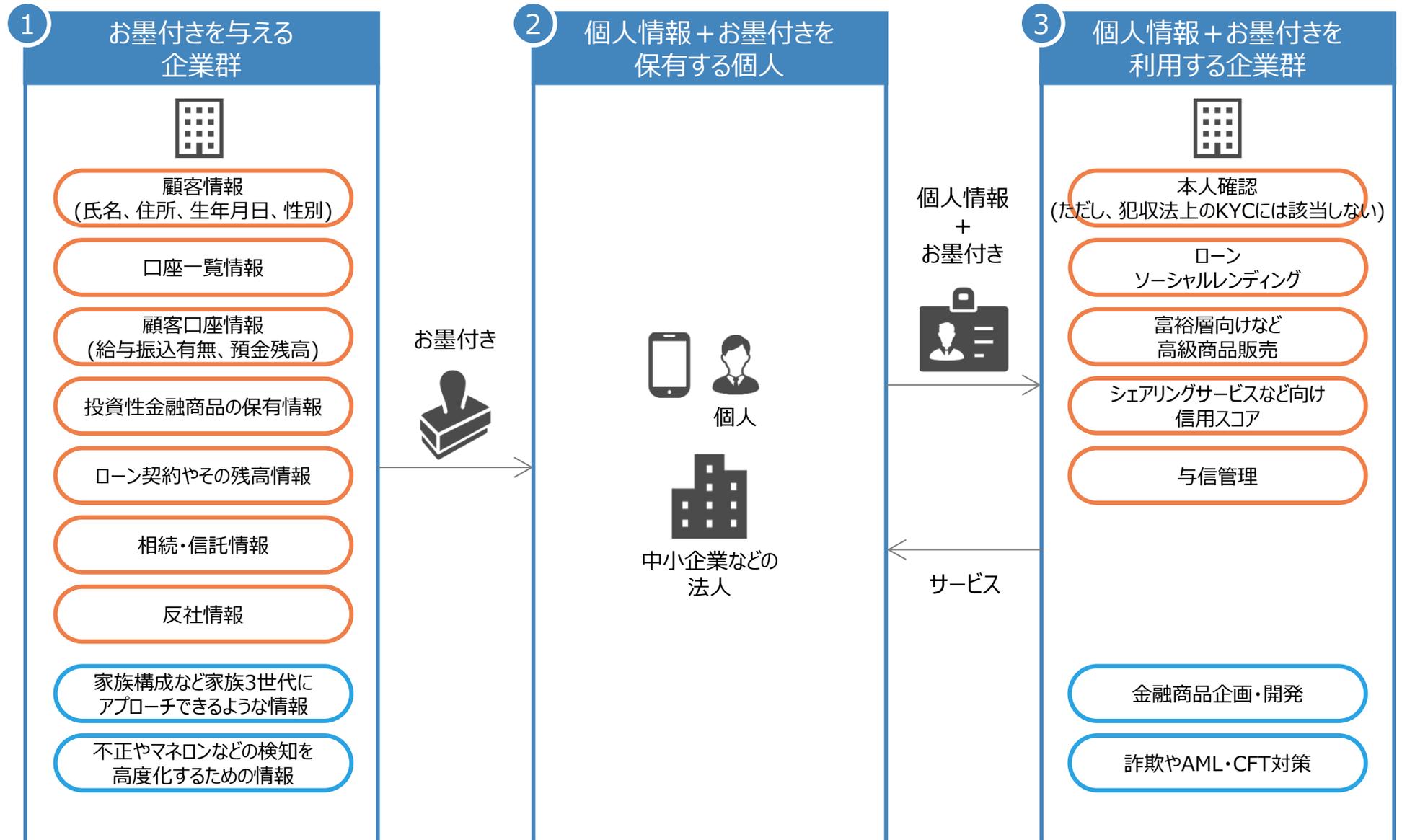
bPassport のサービススキーム (現時点の想定)

bPassport では、本人確認済みなどのお墨付きを企業からもらい、個人のコントロールでその情報を別の企業に提供することで、簡単にサービス提供を受けることができるスキームを想定しています。



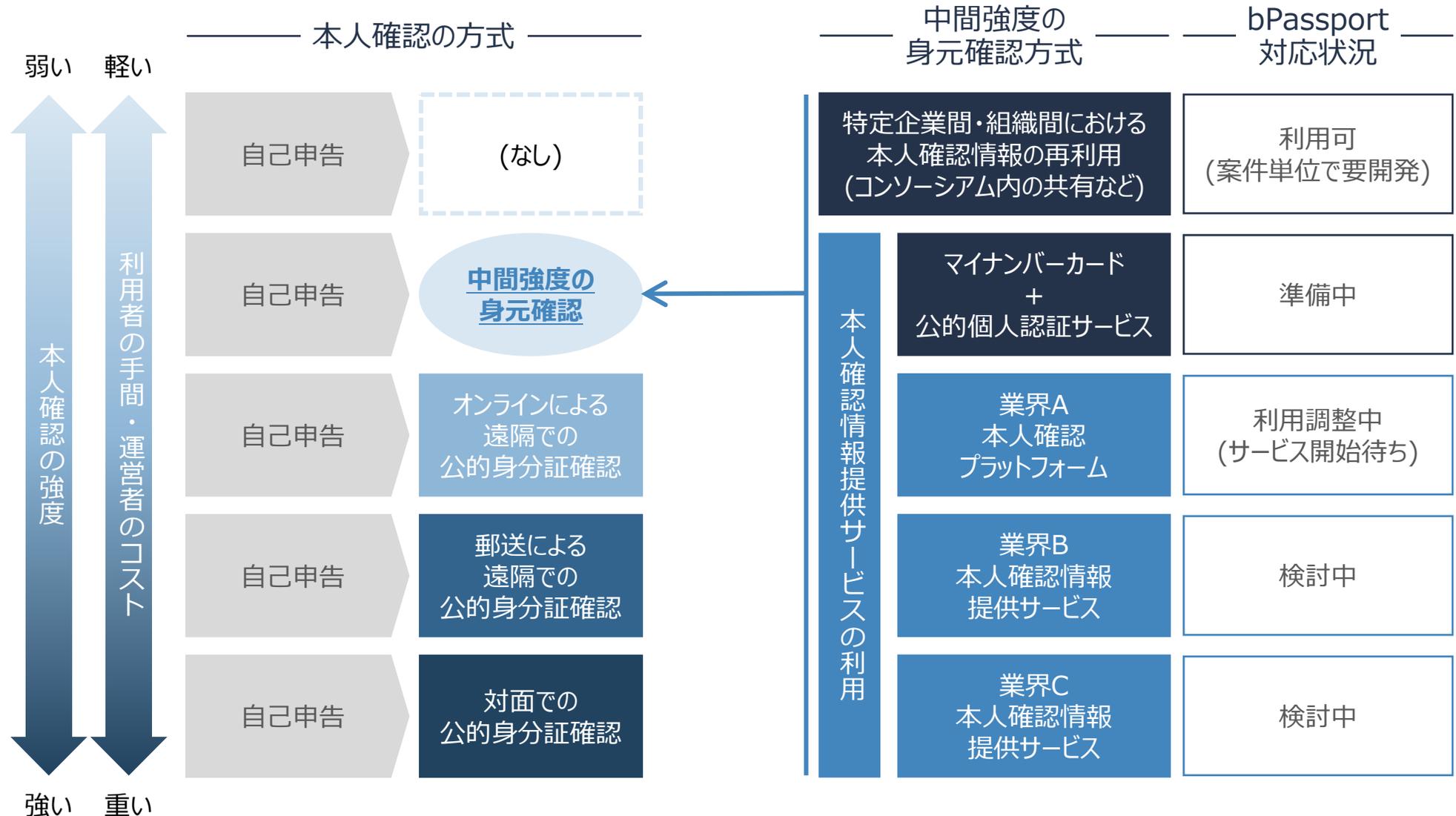
bPassport の可能性

下記①および③の企業によって実現されるユースケースは変わりますが、その一例を以下に記載します。



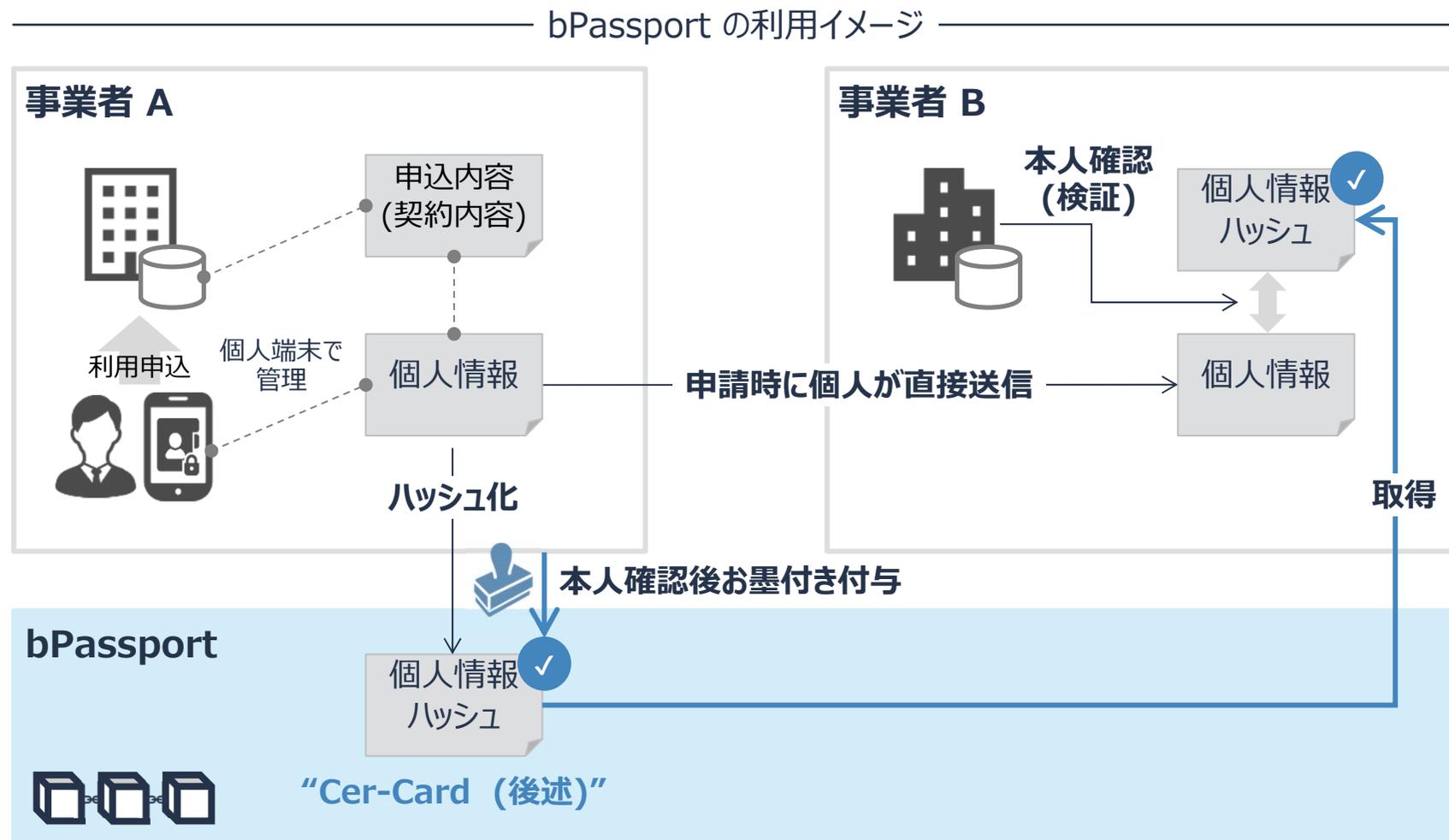
中間強度の身元確認方式への対応

本人確認の方式には、自己申告のみ～対面での公的身分証確認までが存在。近年、「中間強度の身元確認」として、身元確認結果を再利用する方式が検討されていますが、bPassport はこの方式に該当します。



bPassport の利用イメージ

事業者Aにて、ユーザーがサービス利用申込を行う際に、ユーザーが入力した個人情報（本人確認の対象データ）をハッシュ化。事業者Aは本人確認の結果がOKであれば、そのハッシュにお墨付きを添えて bPassport に登録。次に、事業者Bのサービスに加入するケースでは、ユーザーが自身の端末で管理している個人情報を事業者Bに送信し、事業者Bは、その内容と bPassport から取得した Cer-Card を突合する方法でサービス提供可否を判定。



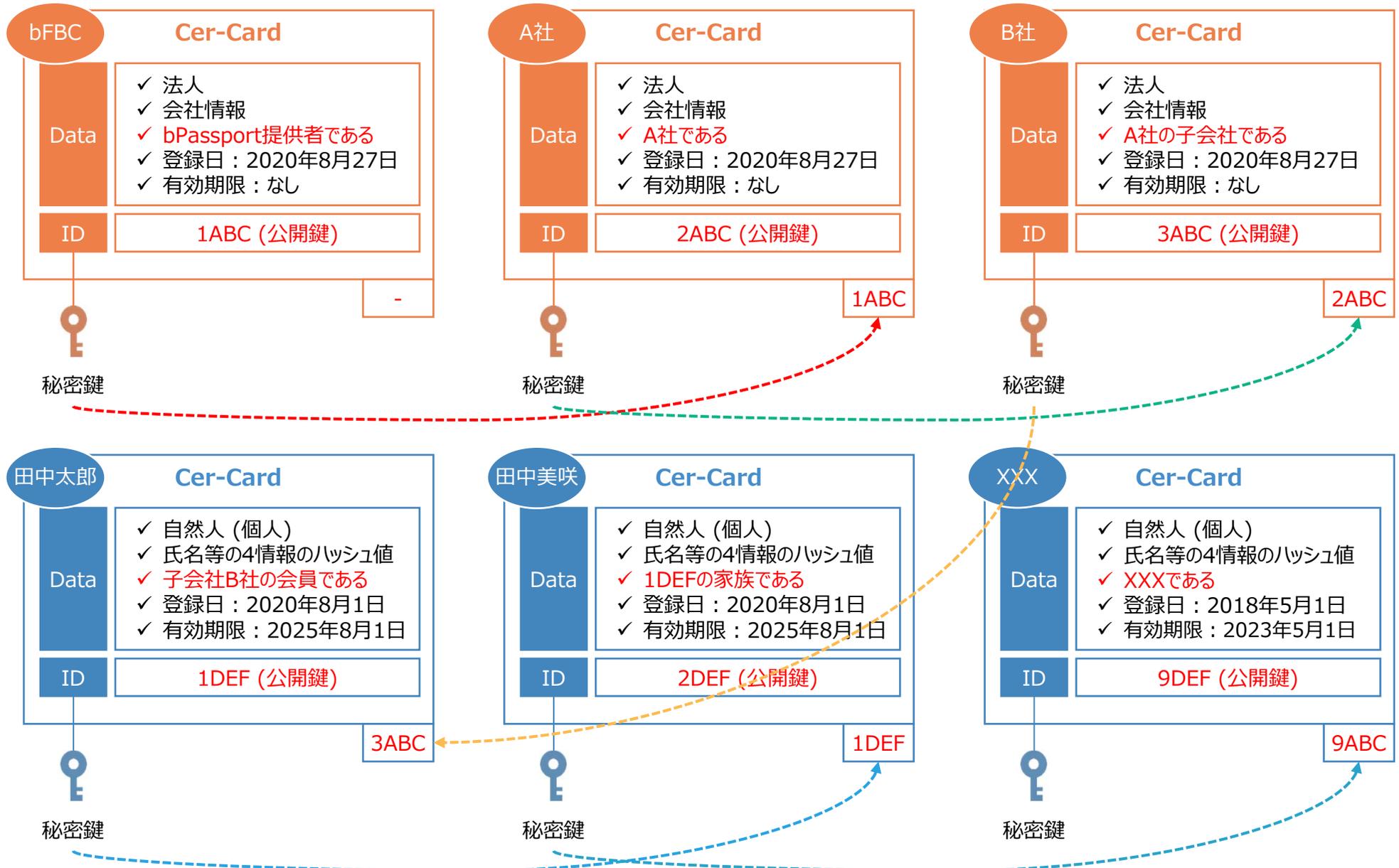
【凡例】

法人

自然人

Cer-Card が表現するIDの属性

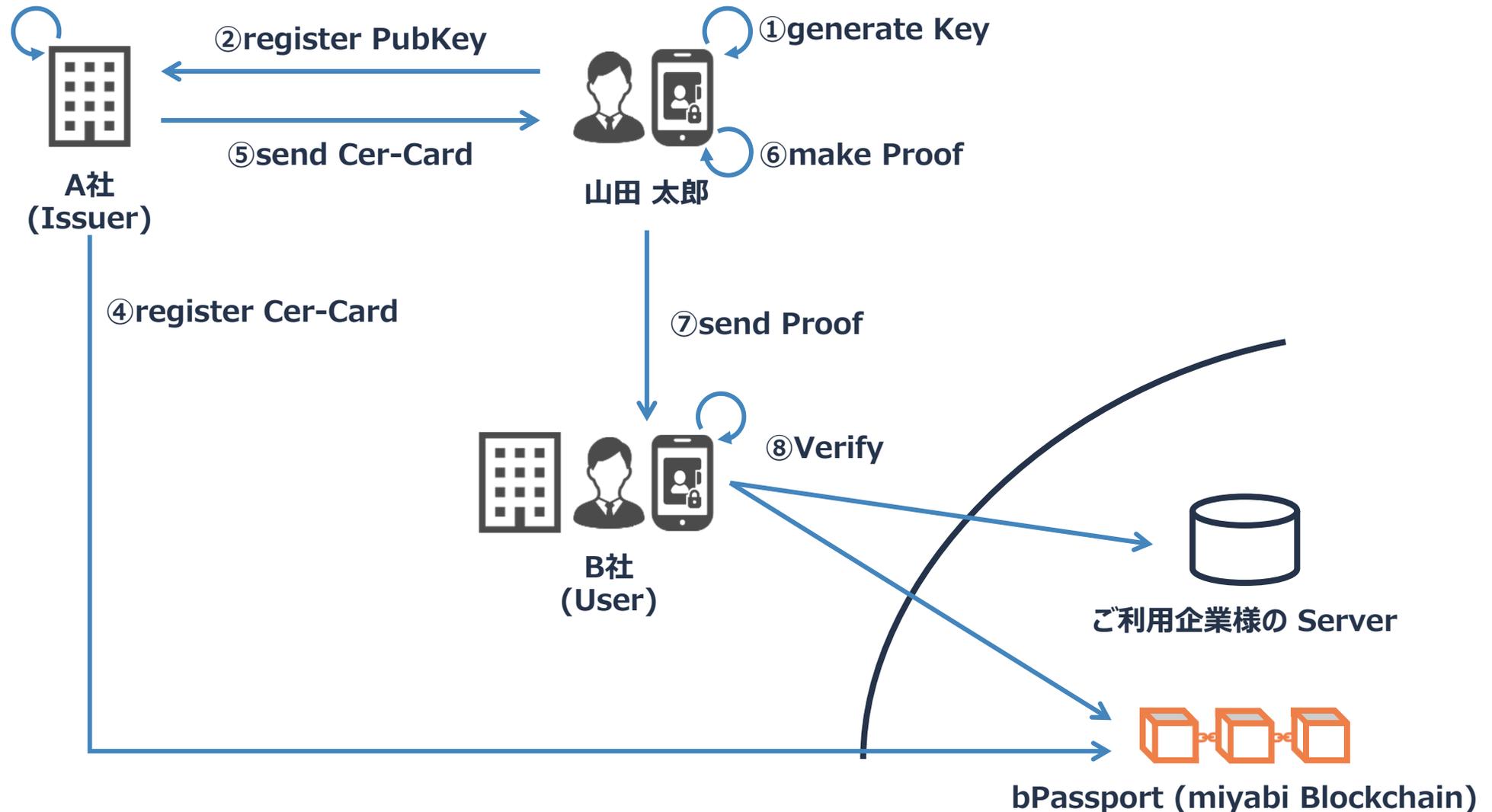
bPassport の機能であるお墨付き “Cer-Card” により、そのIDの属性や行動特性を表現することが可能となります。



Cer-Cardの作成から検証までのイメージ

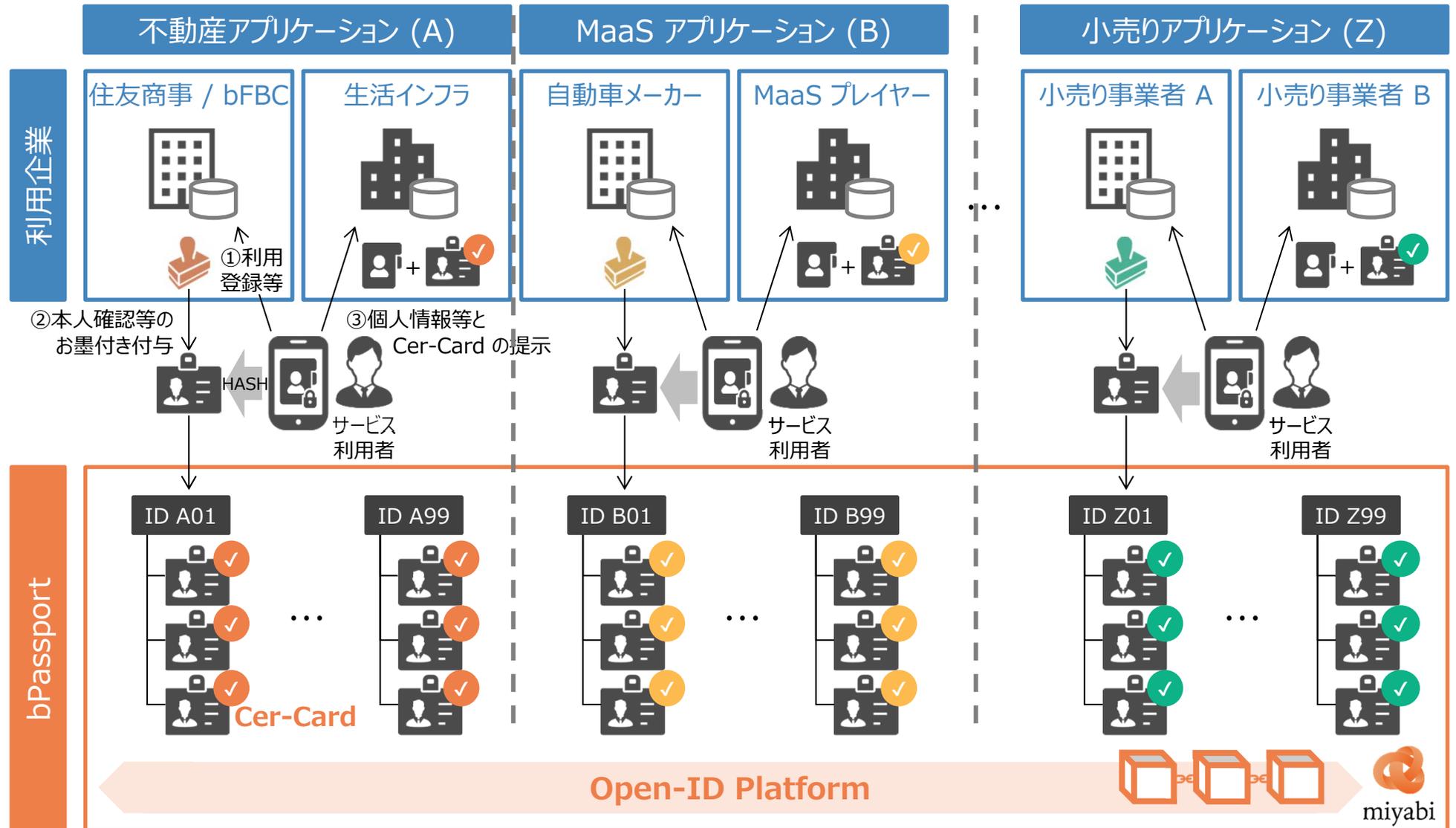
山田太郎がA社から Cer-Card (KYC済みであるお墨付きなど) を発行してもらい、中間強度の身元確認を行いたい、B社に提出します。B社は山田太郎から渡された個人情報 + Cer-Cardを検証し、サービスを提供します。

③make Cer-Card



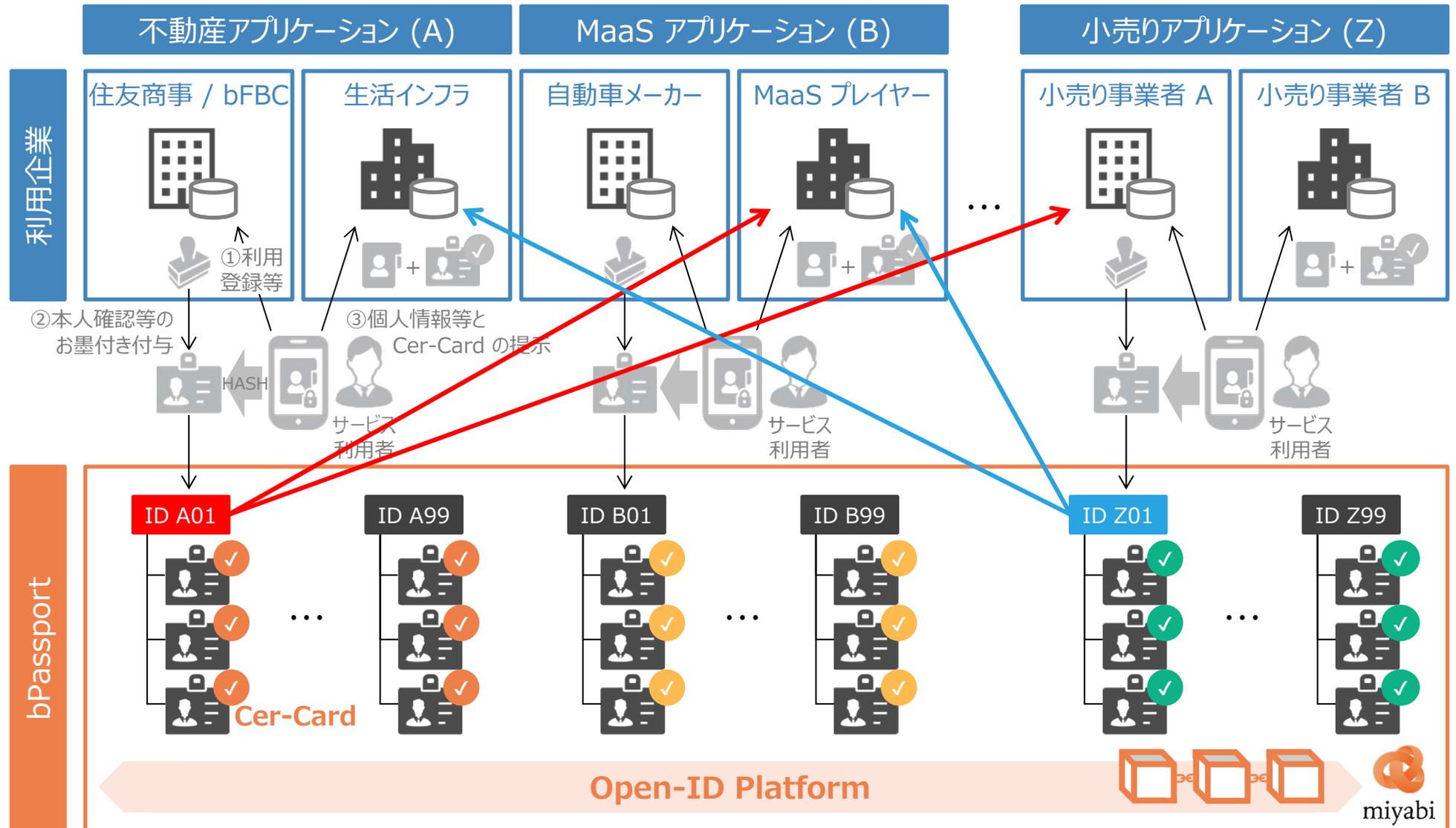
bPassport の構想 (現時点)

bPassport は Open-ID であり、サービス横断での認証機能、ユーザーの本人確認やサービス適合性判断向け認可機能を提供します。現時点ではアプリケーション間でお墨付き情報をやりとりできる、という形になっています。



bPassport の構想 (将来)

初期は各プラットフォーム内に所属する利用企業間の ID連携となりますが、将来的にはプラットフォーム間で相互送客などの契約を行うことにより、プラットフォーム間を跨るID連携が可能となり、各社サービスのスケールをサポートします。



bPassport の企画・開発状況

①他社との共同ビジネス、②当社単独サービスのそれぞれについて、bPassport を活用した事業・サービスの企画・開発を推進中。来年前半をターゲットに商用展開を目指し、bPassport 自体も開発を推進中。

プロジェクト/プロダクト (提供主体)

bitFlyer Blockchainと住友商事、不動産契約の効率化に向け
業界初級
ブロックチェーンを活用した不動産契約の効率化、署名・契約管理
2020年6月22日 17:30



不動産プラットフォーム
(住友商事 × bitFlyer Blockchain)

DX プロジェクト
(大手小売業者様)

bVote
(bitFlyer Blockchain)

中間強度の身元確認 (KYC)
(bitFlyer Blockchain)

概要

ユースケース

1

他社との
共同ビジネス

- 賃貸に関わる個人・法人向けに、物件確認、申込・契約、保証、送客に係るサービスを提供
- 将来的には不動産業に限らず、幅広い領域で多様なサービスが接続エコシステムを目指す

- 電子契約における本人証明
- 賃貸契約後の電気やガスの申込簡略化

- ID共通化構想に対して、bPassportを活用
- 各組織間でのIDを共通化し、付加価値の高いデータを取得しながら、顧客により良いサービスを提供

- 会員登録簡略化
- デジタル会員証の提示

2

当社単独
サービス

- bPassportでオンラインでの本人性を担保することで、投票者のなりすましを防止する投票システム
- bitFlyer Holdingsの株主総会で利用 (2020年6月に開催)

- 投票におけるなりすまし防止

- 日本においては手間がかかる身元確認 (例えば対面での公的身分証明書の確認) か、簡易だが自己申告の情報で信頼性の低い身分確認手法しか広まっていない
- 適度に簡易で信頼性のある身分確認方法が求められており、bPassportで解決できないかを企画中

- 身元確認の効率化

当社のブロックチェーンID“bPassport”とW3Cにより定義されたDIDの関係

W3Cの定義するDIDとbPassportの関係

W3Cのによる標準規格DIDのアーキテクチャに対し、当社のbPassportのアーキテクチャは以下のように対応しています。bPassportはW3CのDIDの規格にも準拠する予定です。

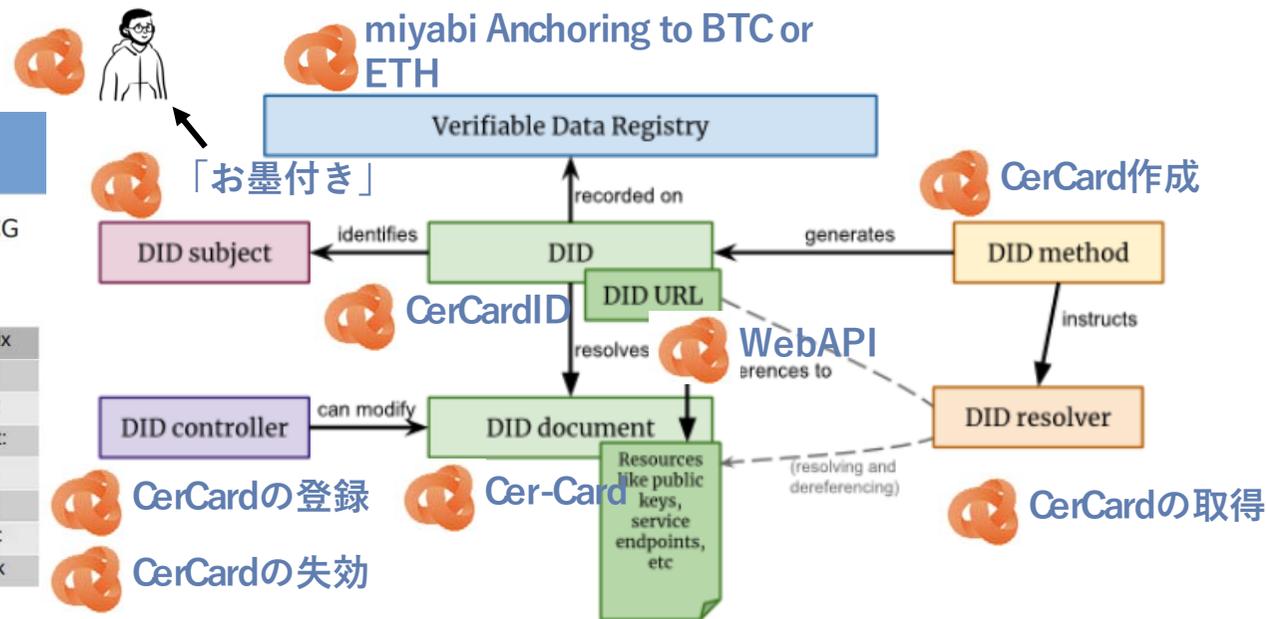
W3Cの定義するDID及びアーキテクチャ、bPassportとの比較



Decentralized IDentifiers (DIDs)

- Developed at Rebooting-the-Web-of-Trust workshop and W3C Credentials CG
- Persistent, dereference-able, cryptographically verifiable identifiers
- Registered in a blockchain or other decentralized network
- did:sov:3k9dg356wdcj5gf2k9bw8kfg7a**
- Modular specification using "methods":
- did:sov, did:btcr, did:v1, did:uport, ...**
- Can be pairwise unique for each relationship
- Resolution: DID → DID Document
 - Set of public keys
 - Set of service endpoints

Method	DID Prefix
Sovrin	did:sov:
Bitcoin	did:btcr:
uPort	did:uport:
VeresOne	did:v1:
IPFS	did:ipid:
IPDB	did:ipdb:
Blockstack	did:stack



bPassportの思想とW3C規格

- 当社のブロックチェーンIDサービスbPassportではDIDのサブジェクトを「お墨付き」にすることで個人と特定のIDを結びつけることを回避している
 - ID自体から個人が特定されてしまうことを回避 (IDが特定されることはSSIの精神と反する)
- bPassportはW3Cが定義するDIDの規格にも準拠する予定
 - 外の世界のDIDとも連携できる (インターオペラビリティ) 可能性を追求

W3Cの定義するDIDにおいてBlockchainを使うメリットとデメリット

W3Cの定義するDIDにおいてBlockchainを使うメリットとデメリットについては以下のように考えられます。

メリット

- Data Registry/DID/DID documentの耐改ざん性
- Blockchainであれば既存のセキュリティー対策を必要としない（ビットコインはTCP/IPそのまま通信している）
- 特定の管理人がいないことがDIDの定義。レガシーシステムはすべからず管理人がいるので定義を満たせないのではないか？ Blockchainには特定の管理人がなく動き続けているという実績がある
- 秘密鍵を持っている人が管理するので個人情報が必要以上に開示されるリスクが減る

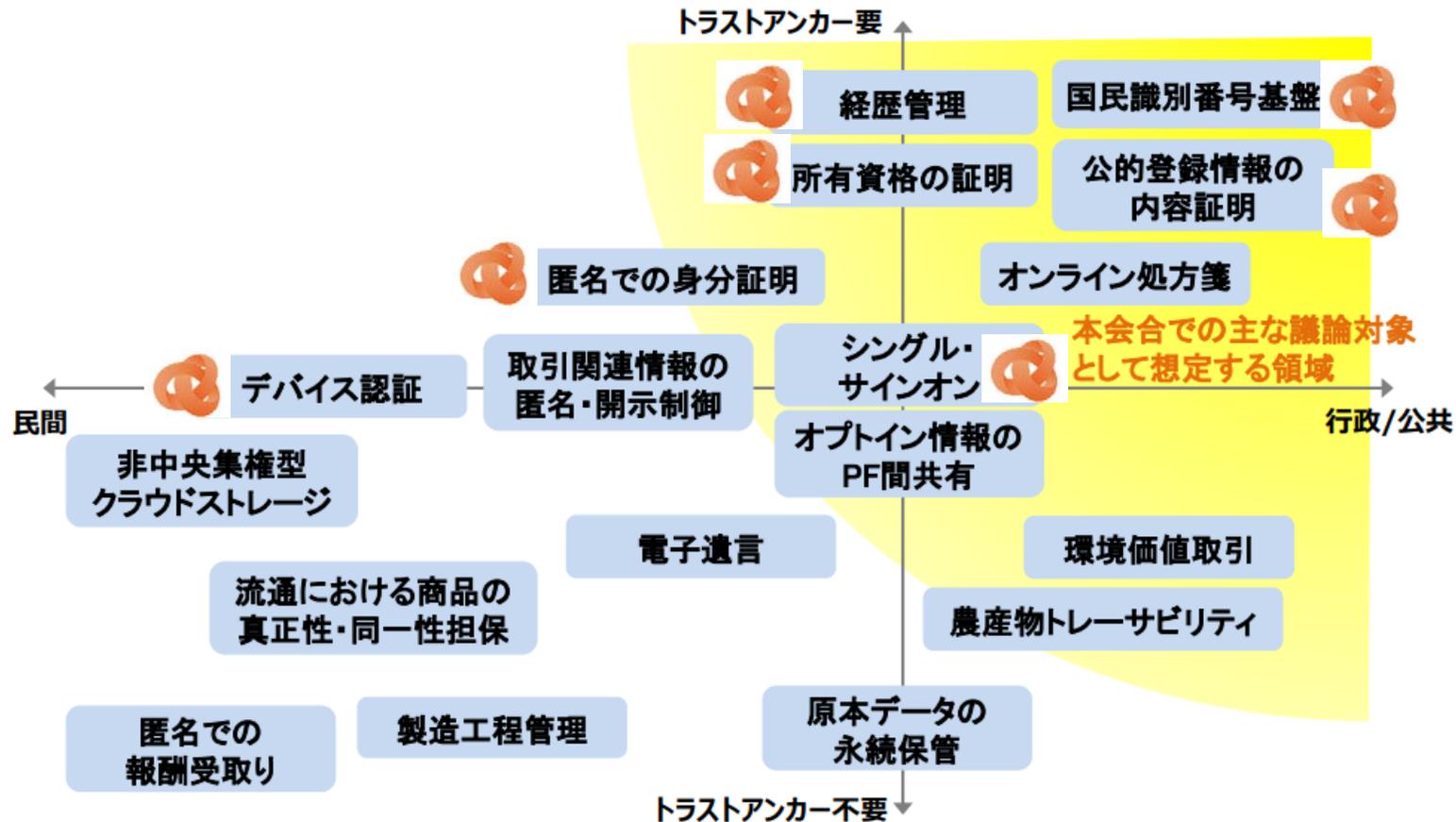
デメリット

- DID Documentの厳密な信頼性検証のためにはVerifierが都度分散台帳上の全ブロックヘッダーを検証する必要があると考えられる（ただしこれは既存RDBでも同様の課題）
- 利用可能なBlockchain製品の選択肢が少ない
- Blockchain製品はまだインターオペラビリティを実現していないので相互接続しづらい
- 機器にIDを振った場合に大量のトランザクションをBCで処理しきれるか？

当社のbPassportでカバーするユースケース

現状bPassportでカバーするユースケースは以下。行政／公共のトラストアンカーが必要なユースケースにおいてすでに実績を有しています。

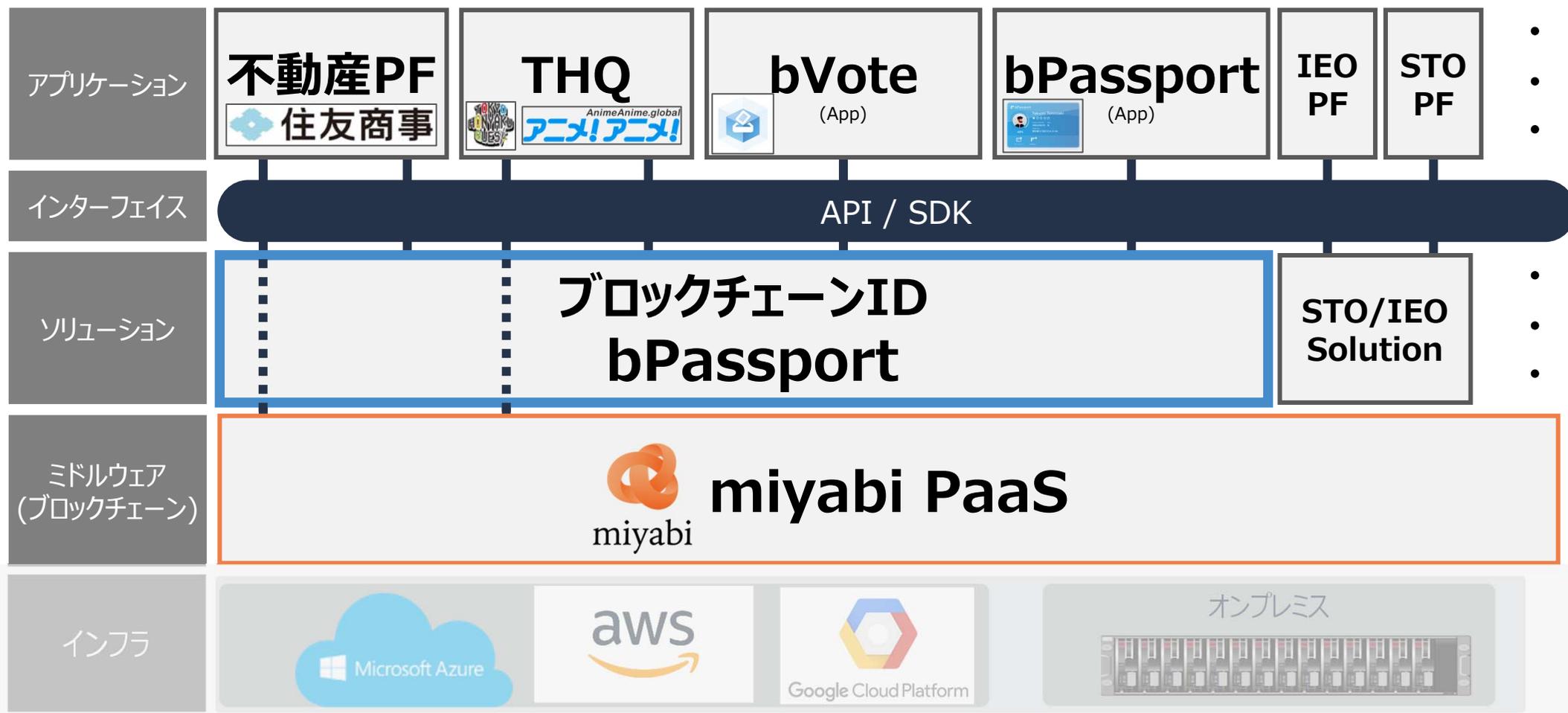
DIDのユースケースと位置付け(例)



※ W3CにおけるDID及びVCのユースケース文書、本会合で紹介された事例を参考に内閣官房IT総合戦略室にて作成
(参考) W3C "Use Cases and Requirements for Decentralized Identifiers," W3C Working Draft 02 September 2020
W3C "Verifiable Credentials Use Cases," W3C Working Group Note 24 September 2019

Appendix : bPassport利用事例

ブロックチェーンレイヤーから アプリケーションレイヤーまで幅広にサービス展開



住友商事様との共同事業

bitFlyer Blockchainと住友商事、不動産契約の効率化に向け業務提携

ブロックチェーンmiyabi活用しアプリで賃貸契約の申込・審査・契約を電子化

日下 弘樹 2019年7月23日 17:50

ツイート リスト B! 3 Pocket 1

いいね! 9 シェア



業務提携を発表し握手を交わすbitFlyer Blockchain・代表取締役の加納裕三氏（写真左）と住友商事株式会社・不動産投資開発事業部長の中本昭人氏（写真右）

日本経済新聞

朝刊・夕刊 ストーリー

トップ 速報 経済・金融 政治 ビジネス マーケット テクノロジー 国際 オピニオン スポーツ 社会・暮らし

速報 > プレスリリース > 記事

プレスリリース

企業名 | 産業 住友商事 | 商社・サービス

住友商事とbitFlyer Blockchain、不動産賃貸契約プラットフォームの共同開発に向けて業務提携

2019/7/23 16:10

保存 共有 印刷 共有 ツイート f その他

発表日:2019年7月23日

不動産賃貸契約プラットフォームの共同開発に向けた業務提携について

住友商事株式会社（本社:東京都千代田区、代表取締役 社長執行役員CEO:兵頭 誠之、以下「住友商事」）と株式会社 bitFlyer Blockchain（本社:東京都港区、代表取締役:加納裕三、以下「bitFlyer Blockchain」）は、スマートコントラクト機能を備えたブロックチェーン（注1）「miyabi」（注2）を活用し、住宅の賃貸契約を電子化した上で、物件の内見予約から契約までを行えるプラットフォームの共同開発に向けて業務提携しました。

現在、住宅の賃貸契約においては、貸主、管理会社、仲介会社および借主の間の対面でのコミュニケーションやFAX・郵送による契約締結プロセスなど多大な労力を要しています。我が国の労働人口の減少や昨今の働き方改革といった社会背景を踏まえ、不動産業界でも業務効率化が喫緊の課題となっており、革新的なテクノロジーを活用した業務効率化の実現に期待が高まっています。



住友商事



bitFlyer Blockchain

物件内見

① 申込・審査

② 賃貸契約・
保証契約

③ 保険契約

④ 生活インフラ契約

不動産管理・
仲介会社
(9社)

EPOS CARD

MS&AD

PinT

Orico
株式会社オリコフォルトインシュア

三井住友海上

エネルギー・フロンティア
TOKYO GAS

NICIGAS
ニチガス

J:COM

0123 アート引越センター
アートコーポレーション株式会社

アップル引越センター

2020年10月28日

25社が参加し

プレ商用サービスを開始

賃貸・引っ越し・ガス...スマホで一括契約 25社参加
【イブニングスクープ】

全記事一覧 [+フォローする](#)
2020年10月27日 18:00 (有料会員限定)

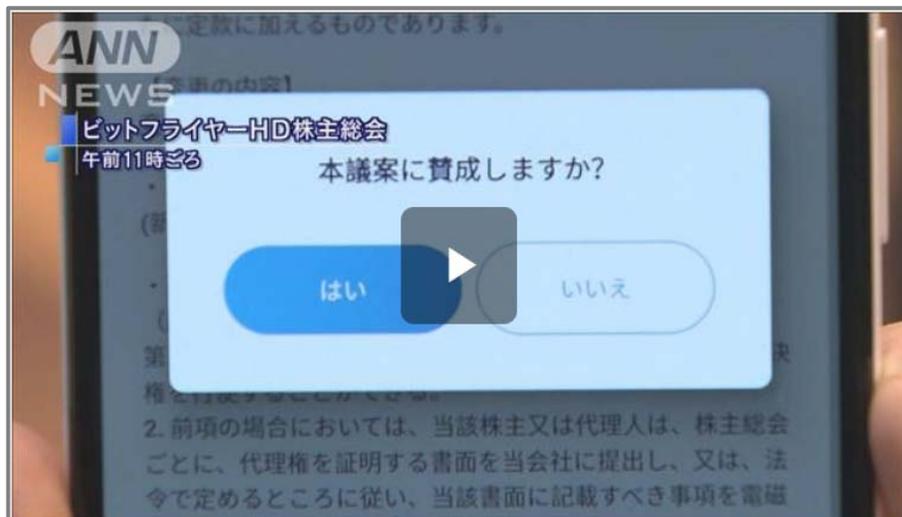
保存



アートコーポレーションなどに転用し併って必要になるサービスを提供する企業が電子化計画に賛同する

住友商事とビットフライヤーブロックチェーン（東京・港）が手がける不動産賃貸契約の電子化プロジェクトに三井住友海上火災保険や東京ガスなど25社が加わるのが分かった。物件の申し込みから、電力やガスなど生活インフラの契約までをスマートフォン上で完結できるサービスを2021年春に始める。

bVoteによるオンライン株主総会を実施



ANN NEWS
ビットフライヤーHD株主総会
午前11時ごろ

本議案に賛成しますか?

はい いいえ

26日は多くの企業が株主総会を開く集中日です。今年は新型コロナウイルス感染予防のため「3つの密」を防ぐ取り組みが広がり、様変わりしています。

IT企業の株主総会では株主がテレビ会議のシステムを使って出席できるようにし、議案への賛否もスマートフォンのアプリで投票できるようにしました。新型コロナウイルスの感染予防のため、今年は多くの企業が株主に対してできるだけ会場には来ないように呼び掛け、郵送やネットで議決権を行使するよう求めています。また、会場に来た株主に渡す「お土産」を廃止する企業も相次いでいます。ただ、経営陣と株主が直接対話する機会が減ることに懸念の声も出ています。

テレビ朝日「ANN ニュース」のほか
テレビ東京「モーニングサテライト」など地上波で紹介

記事出典) [テレ朝ニュース「きょう株主総会の集中日 3密対策で新様式に」](#) / ITmedia

「改ざん不能だけでなく、透明性を保証できる。投票の集計開票作業は会社側が行うが、しばしば株主と会社側の利害は対立するからだ」（加納氏）



bitFlyer Blockchainの加納裕三社長

bVoteが投票結果を書き込むブロックチェーンはプライベート・ブロックチェーンだが、外部から閲覧できるようにも設定できる。誰がどんな投票を行ったかは暗号化されており、改ざんはできないため、会社側が集計結果を操作することはできない。

ITmedia / CNET Japan / JBpress / コインデスクや
海外メディアなどにも多数掲載

Tokyo Honyaku Questのご紹介 (全体像)



フィギュア

トークンエコノミーを実現



感謝・賞賛