

# つながるトラスト

2022年5月20日

富士通株式会社

フェロー データ&セキュリティ研究所長

津田宏 (htsuda@fujitsu.com)



# Our Purpose

わたしたちのパーパスは、  
イノベーションによって社会に  
信頼をもたらし、世界をより  
持続可能にしていくことです。

## トラストの定義として

- 「結果の予想であり、物事がうまく行く可能性が高いと期待すること」(ボツマン, 「Trust」)
- 「相手が期待したとおりに振る舞うと信じる度合い」(Trusted Web協議会)

等ありますが

このプレゼンでは色々な意味で使っていますのでご了承ください

- 真正性、存在証明、改ざん不能、Verifyできること、安全な領域、相互監視、スコアリング、偽情報(Disinformation)、等々

# デジタル時代の新たなリスク

スマホ位置情報、乗降履歴、監視カメラ映像、採用情報、友人関係、等の不適切な利活用、視聴履歴からの個人特定	Personal Data
監視カメラからのDDOS攻撃、Coincheck事件、地図データ誤りによる事故	サイバーフィジカル
パーソナライズによる情報操作(フィルターバブル)、フェイクニュース、ディープフェイク、Disinformation(ウクライナ侵攻)	Disinformation
人種差別、性差差別、硫化水素を発生する商品をリコメンド	倫理
取引先を騙った請求書メール被害が2.9兆円 (ビジネスメール詐欺)	なりすまし
Facebook 5,400億円(米FTC), Amazon 970億円(EU GDPR)	制裁金
AIへの攻撃(Microsoft Tay, 敵対的サンプル, モデルの再構築)	人工知能
越境移転、国外からのアクセス (LINE事件)	経済安全保障

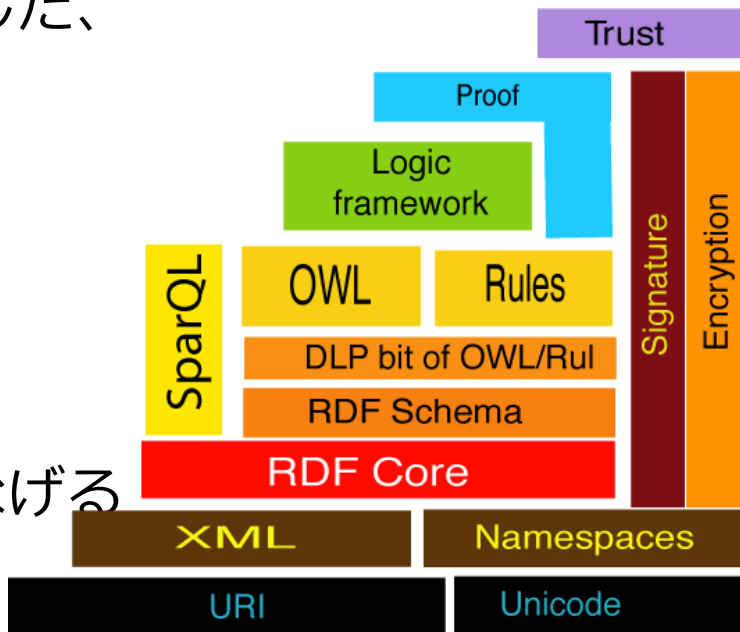
サイバー空間で人やモノ、データがつながる  
その正しさを保証する仕組み = デジタルトラスト が必要に

- ゼロトラストアーキテクチャ (NIST SP800-207等)
  - イントラネットのように信頼できる領域を境界を作って守ることの限界
- ブロックチェーン
  - 分散された信頼 (レイチェル・ボッツマン「Trust」)
  - Decentralized (非中央集権)
- Decentralized Web
  - Trusted Web (内閣官房), DID, Web3
- DFFT : Data Free Flow with Trust
  - 2019.1 ダボス会議にて、Society5.0に向けて安倍首相が提唱
- トラストサービス
  - EUのeIDAS規則(Electronic identification and trust services)
  - デジタルトラスト協議会(JDTF)設立 (2020.8, 2022一般社団法人化)
- 芝麻信用
  - 信用スコアリング
- ニューノーマル
  - 脱ハンコに関する三省ガイドライン

- Tim Berners-Leeが10年たって見直した、(当時の)次世代Web, データのWeb
- コード-> Identifier
  - > メタデータ (RDF)
  - > スキーマ -> オントロジー(OWL)
  - > ルール、推論
  - > トラスト

というプロトコルレイヤでデータをつなげる

- 最上層が「Trust」



W3C, Semantic Web Layer Cake

Trusted Webとか、Webをトラストの観点で根本から見直す時期にきているのでは

## デジタル時代の信頼

- ビジネス取引の安全性やデータの信頼性を保証するためにテクノロジーが重要な役割を果たす
  - ブロックチェーン
  - セキュリティ技術

トラスト1.0



トラスト2.0



トラスト3.0



物々交換 → 国家 → サイバー空間とIdentityの広がり

トラスト 1.0  
人同士のトラスト

トラスト 2.0 中央が保証するトラスト  
(法律・制度)

トラスト 3.0 分散されたトラスト  
テクノロジーによるトラスト

人  
(個人)  
(法人)

口コミ、評判



データ

証文(私的文書)  
石貨に刻む

システム

物々交換

連帯保証人  
銀行保証

クレジットスコア (FICO)  
個人信用情報

署名, サイン  
契約

国民ID  
電子署名, eIDAS

① 信頼の  
デジタイ  
ゼーション  
(Digitization)

内容証明郵便  
公正証書  
会計基準

タイムスタンプ

国による通貨

クレジットカード、電子マネー

SLA, reliability

ソーシャルネットワーク (Uber)

分散型ID (デンティティID)  
情報銀行・本人同意管理/UBI

② 信頼による  
デジタイ  
ゼーション  
(Digitalization)

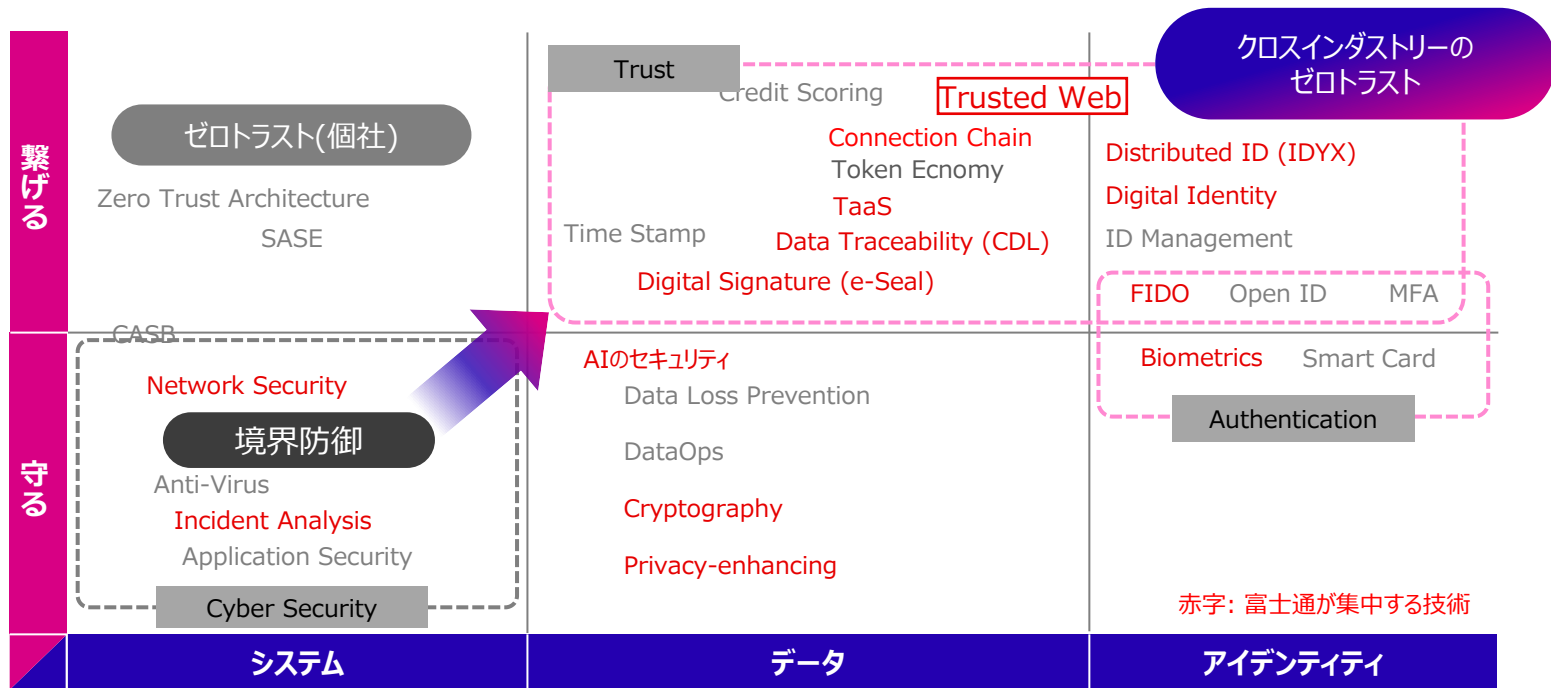
暗号資産 (仮想通貨)  
説明可能

ブロックチェーン

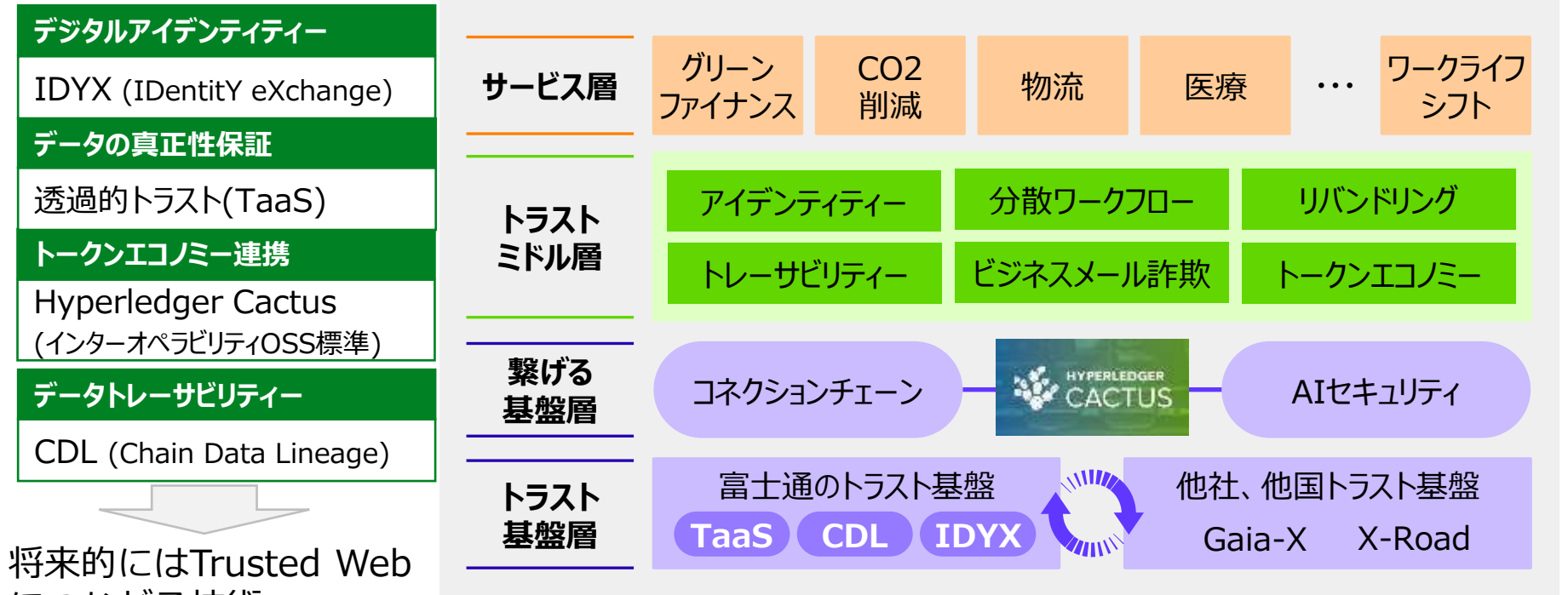


# 狙い: クロスインダストリーのゼロトラストへ

- 境界で守るサイバーセキュリティから、ゼロトラスト(何も信用しない)セキュリティへ
- さらに、クロスインダストリーのゼロトラストへ(相手先、交換データのトラスト)



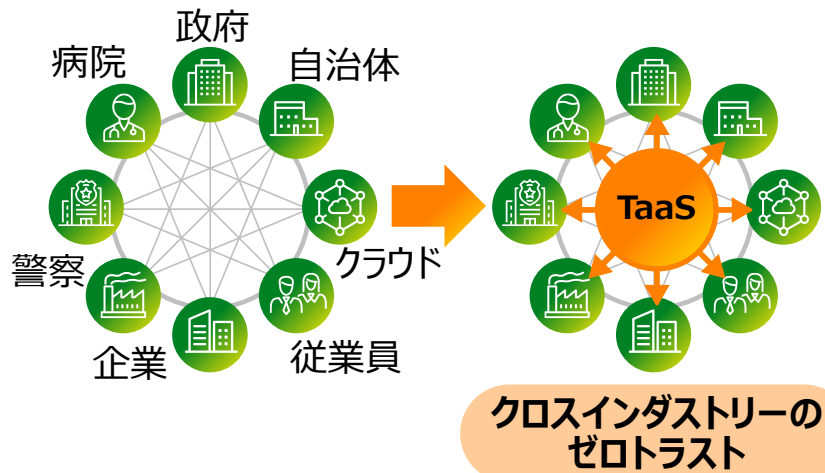
## 人・データ・プロセス・AIの信頼の上に、クロスインダストリーのDXを実現



## TaaS: Trust as a Service

クラウド間でデータの真正性を保証

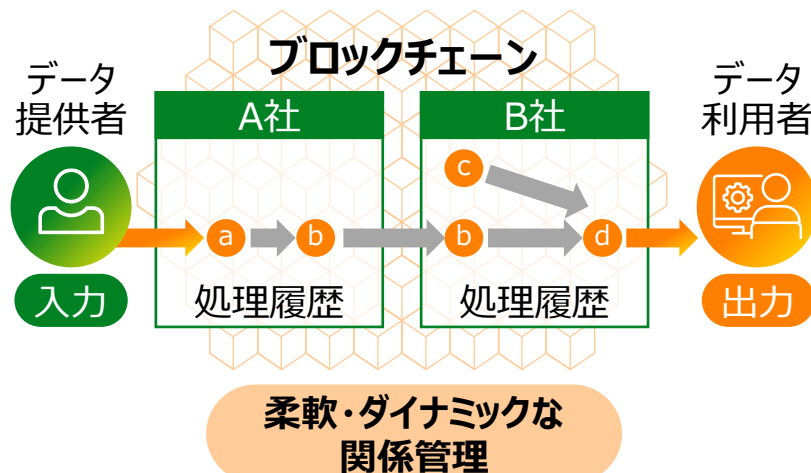
- 異なるクラウド間でビジネスデータの真正性を確保
- ビジネスメール詐欺のリスクを排除し、ハンコレスによる複数企業の安全なコラボレーションを可能に
- デジタルトラスト協議会でルール形成をリード



## CDL: Chain Data Lineage

データのトレーサビリティ

- 各社が持つモノの流通・加工の履歴データをエンド-エンドでトレース
- 様々な組織が柔軟につながるデータのサプライチェーンで、AIで利用するデータの出元の正しさを常に確認



# 1. 「人」をつなげる: IDYX

# デジタルアイデンティティの現状

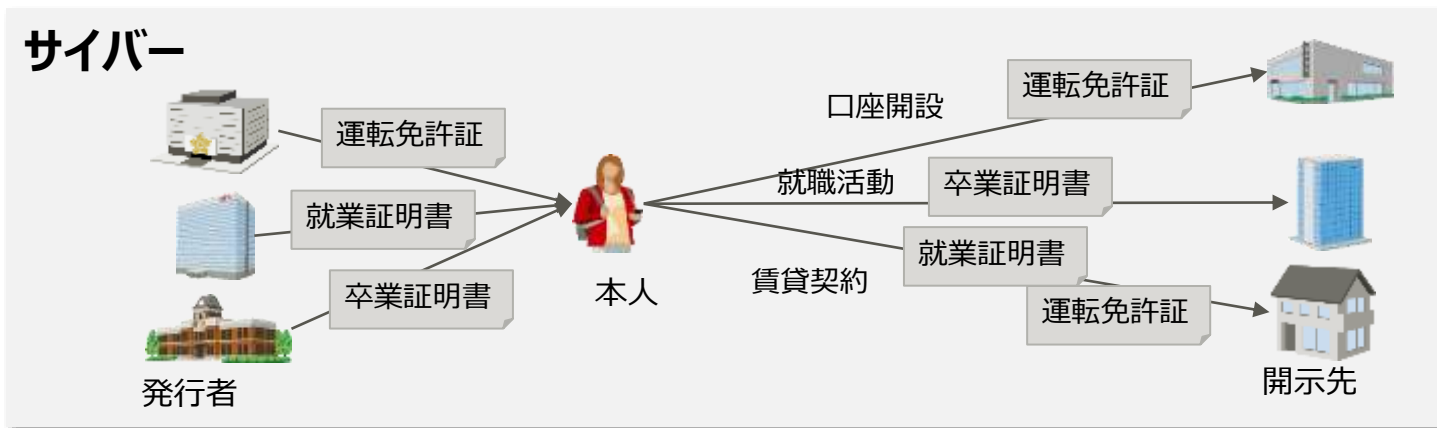
自身で管理するデジタルアイデンティティを、さまざまなサービスに自由に開示・証明できるようになりつつある。

リアル



アイデンティティ = ID + 属性  
物理的な証明書を自由に利用  
名前や年齢、信用などの属性を証明

サイバー

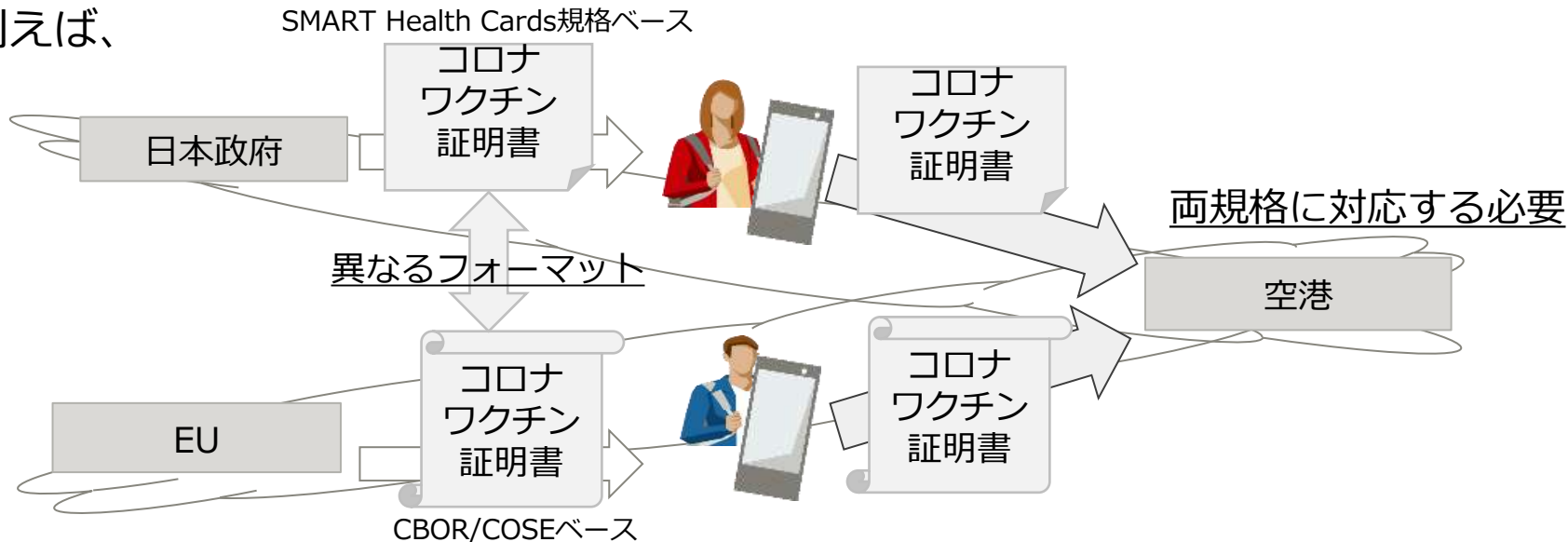


リアルでの手続きをデジタル化し、効率化することが可能

# デジタルアイデンティティ：課題

アイデンティティをデジタル化するための技術標準化が進められている  
しかし、さまざまなフォーマット・プロトコルが併存するのが実態

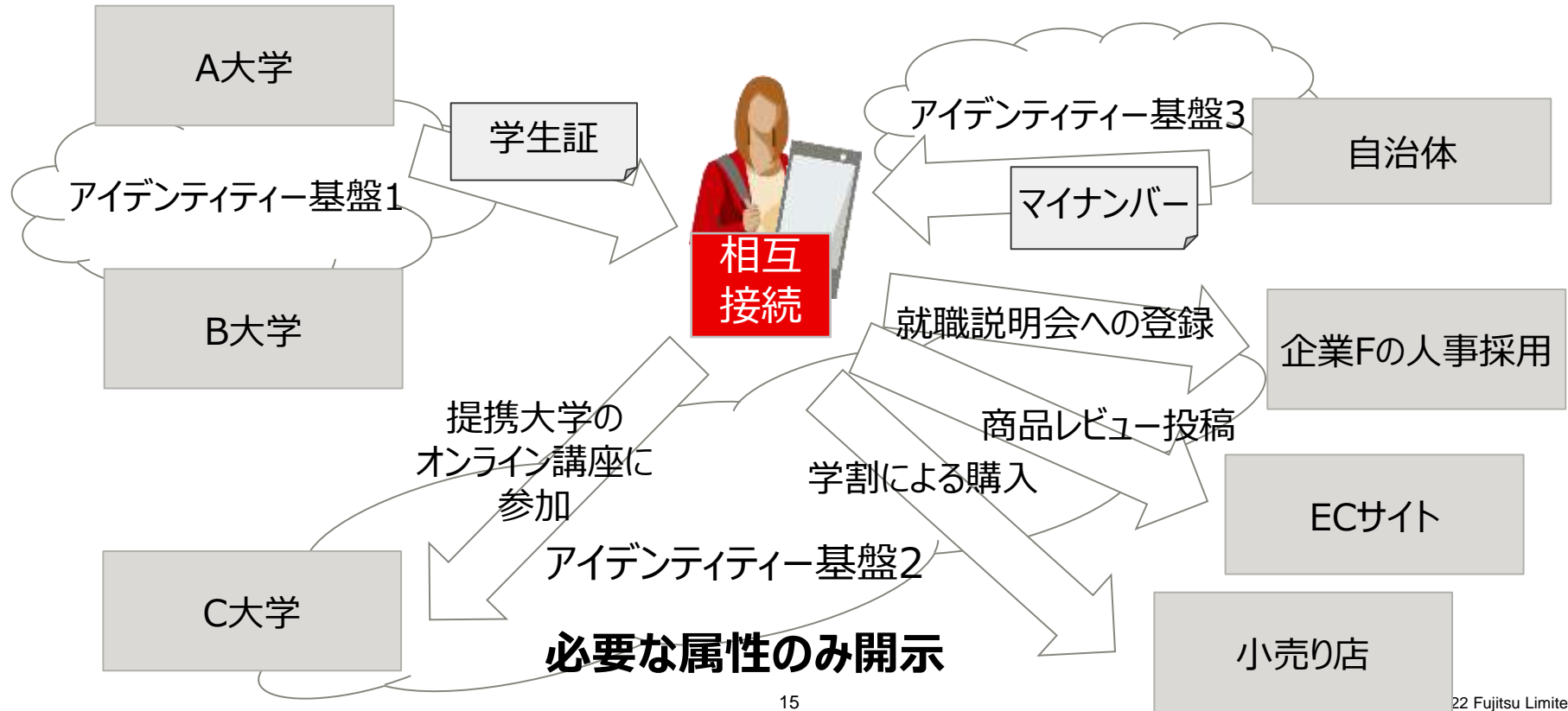
例えば、



組織やサービスを跨いでアイデンティティを扱うには、  
複数フォーマット・プロトコルへの対応必要

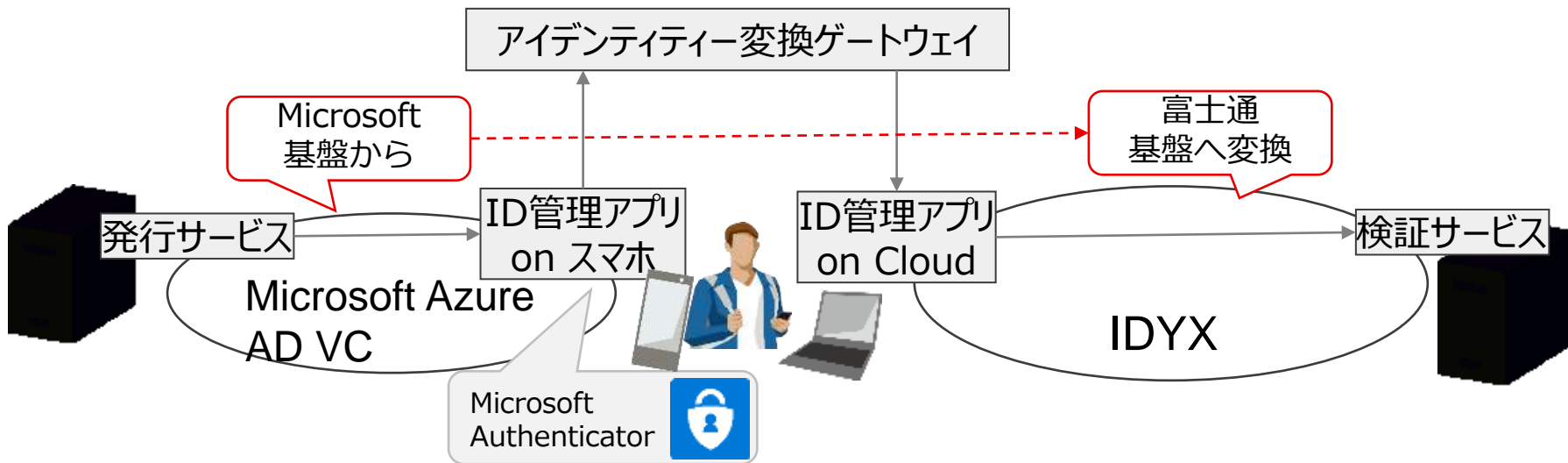
# デジタルアイデンティティ：目指す世界

○ある組織で管理される証明書を組織やサービスを跨いで活用



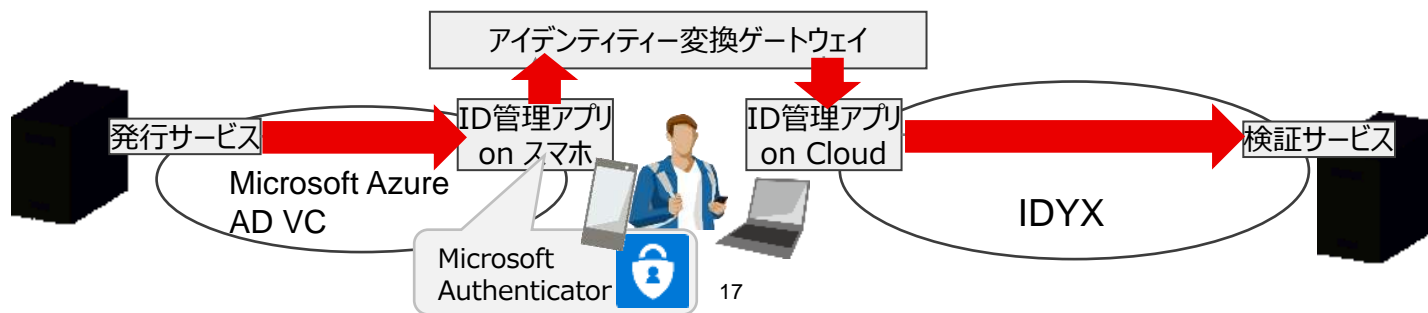
○アイデンティティ変換ゲートウェイを開発

→ 検証サービスは、複数フォーマット・プロトコルへの対応不要

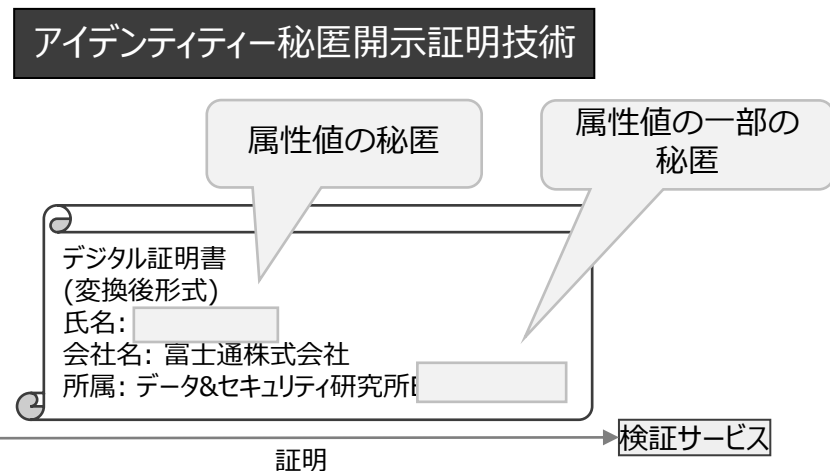
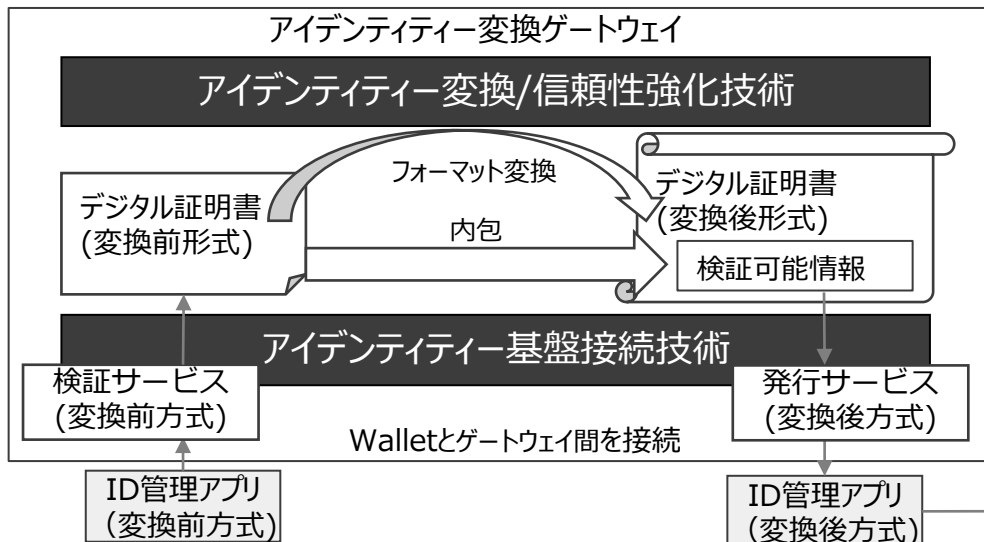


Microsoft方式のID基盤 と富士通のID基盤 IDYX を接続

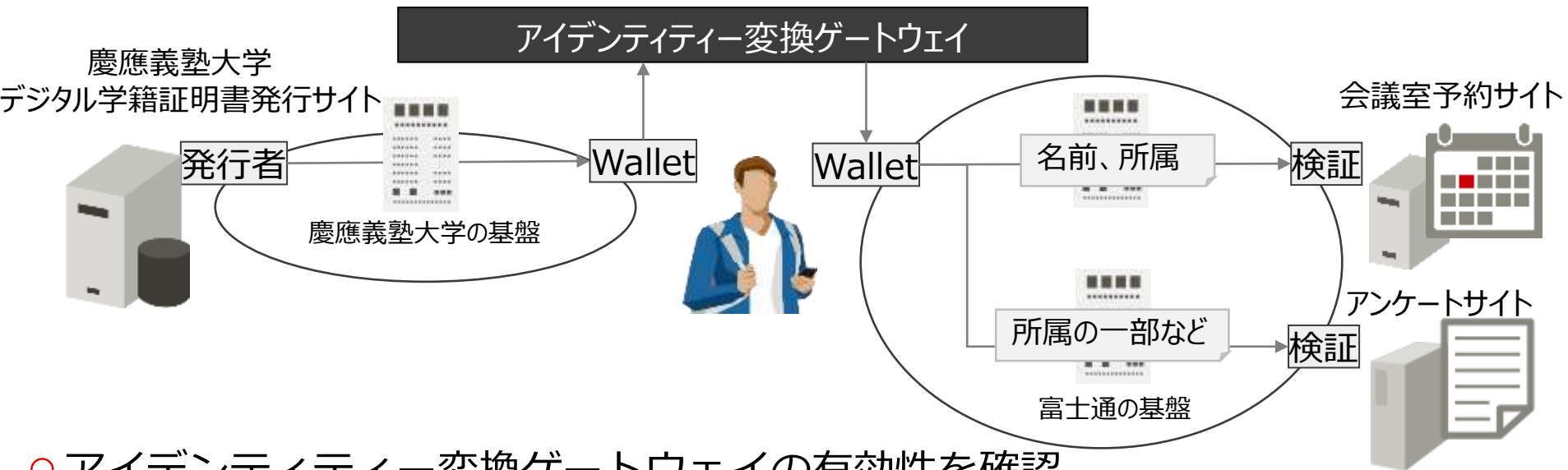




- アイデンティティ基盤接続技術
  - 変換前方式の検証プロトコル/変換後方式の発行プロトコルで接続することで、ID管理アプリの機能追加が不要
- アイデンティティ変換技術/信頼性強化技術
  - 変換前のID証明書の正当性を検証した上で情報を抽出、変換後形式でID証明書を構成して署名
  - 変換前のID証明書を内包して検証可能情報を継承することで、変換時の不整合を検出可能に
- アイデンティティ秘匿開示証明技術
  - ID証明書に含まれる属性値の一部のみを開示・証明を可能にすることで、自身の異なる見せ方が可能



- 学生を被験者として、大学の提供するMicrosoft方式のデジタル学籍証明書をIDYXと連携する複数のサービスで利用する実証実験を実施



- アイデンティティ変換ゲートウェイの有効性を確認
  - 学籍証明書の名前・所属などを使って会議室予約サイトの認証に利用
  - 学籍証明書の情報の一部の情報のみを選択して開示して、アンケートへ回答

# 慶應スモールリサーチラボ設立 (4/14プレス)

## 共同研究拠点「トラステッド・インターネット・アーキテクチャ・ラボ」の概要

### 研究期間：

○ 2022年4月 ～2025年3月

### 研究内容：

- 本共同研究拠点では、個人や企業の活動と安全を確保し、安心してデジタル社会の構築を再構築することを目指します。
- インターネットの運用が開始された時点では備わっていない認証や認可、ウェブページでの個人情報取得のみの合意のクリックといった追加的な要素の組み合わせでの実現を、個人や企業の安心と安全を確保するためのメカニズムを開発やアーキテクチャーの設計について、グローバルな視点で研究していきます。

### 体制：

- 代表 中村 修 (慶應義塾大学環境情報学部 教授)
- 副代表 村井 純 (慶應義塾大学 教授)
- 副代表 鈴木 茂哉 (慶應義塾大学大学院政策・メディア研究科 特任教授)
- 慶應義塾大学SFC研究所と富士通の研究員 約20名

PRESS RELEASE

2022年4月14日  
慶應義塾大学SFC研究所  
富士通株式会社

## 学籍証明書のデジタルアイデンティティを相互連携 利用する実証実験を実施

企業や大学、自治体が発行する属性情報を個人が安心して活用し、  
様々な人や組織が協調できる社会の実現に向けて

慶應義塾大学SFC研究所<sup>(注1)</sup>と富士通株式会社<sup>(注2)</sup>（以下富士通）は、個人がデジタルで管理する自身の属性情報（デジタルアイデンティティ）を組織やサービスを越えて活用できるデジタル社会の実現に向けて、異なるアイデンティティ基盤を相互接続して自己主権型で連携利用する実証実験を2022年3月17日から4月12日まで実施し、国内で初めて有効性を確認しました。

本実証実験では、慶應義塾大学の次世代デジタルアイデンティティ基盤<sup>(注3)</sup>から実験的に発行したデジタル学籍証明書を、富士通が開発したアイデンティティ交換プラットフォーム<sup>(注4)</sup>で連携した上で、学生が富士通の「IDYX (IDentity exchange)」<sup>(注5)</sup>と連携する各種オンラインサービスごとに必要な属性情報を異なる見せ方で開示できることを証明しました。この仕組みが実用化すれば、企業や大学、自治体が発行する個人の属性情報を、利用者自身が様々なサービスに連携利用できるため、例えば、大学が発行した学生情報を、就職活動や卒業後のリクルーティング、また、旅行会社の学生割引サービスに活用するなど、デジタルアイデンティティによる利便性の向上が期待できます。

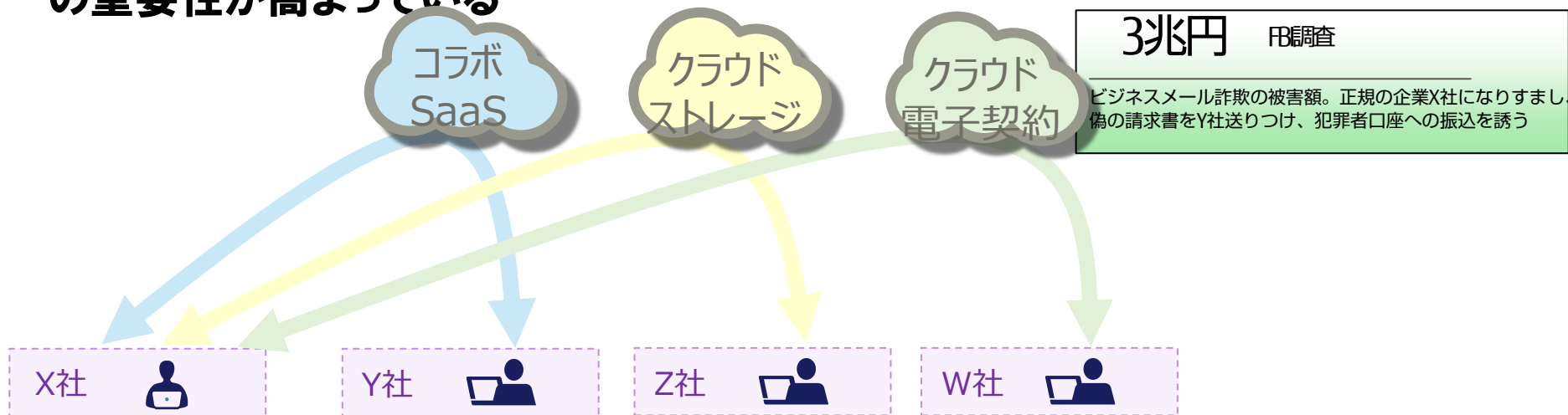
なお、慶應義塾大学SFC研究所と富士通は、本実証実験の成果も生かし、デジタルアイデンティティを軸にインターネット上で信頼性を担保できるアーキテクチャ設計や技術開発を行う共同研究拠点「トラステッド・インターネット・アーキテクチャ・ラボ」を2022年4月に慶應義塾大学（湘南藤沢キャンパス）内に新設しました。

<https://pr.fujitsu.com/jp/news/2022/04/14.html>

## 2. 「データ」をつなげる①： 透過的トラスト(TaaS)

# デジタルが主の働き方へ

- ニューノーマル、メタバース → **デジタルインフラ**を利用した業務形態が**標準**に  
(デジタルオフィス・ファースト)
- **全てデジタルでビジネスを行うため、デジタルトラスト**(人・データの真正性の保証)の重要性が高まっている



取引相手・業務ごとに様々なクラウドサービスを使い分けながら  
いかにデジタルトラストを確保していくか

## ○これまで：**デジタル署名**

- 従業員ICカードなど

## ○ユーザーの**利便性に課題**

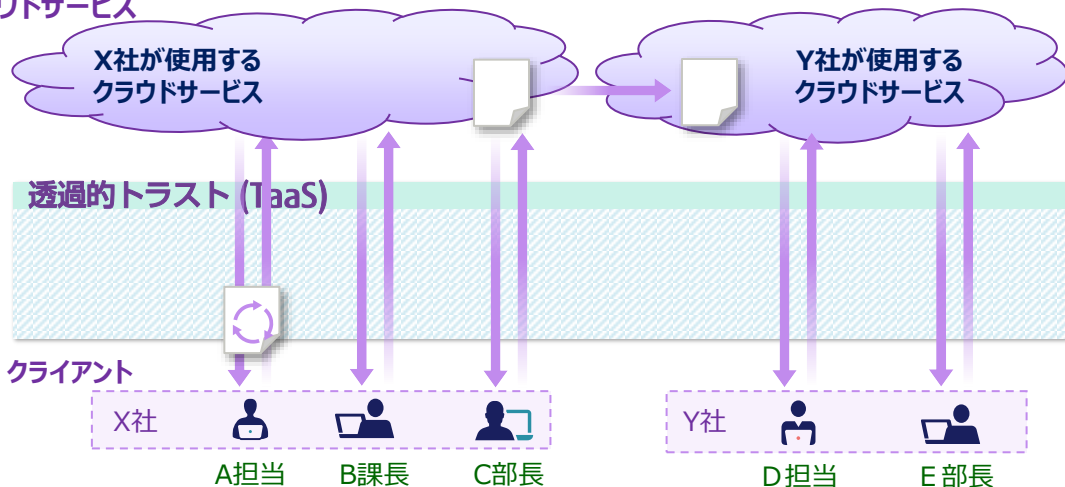
- 署名用の秘密鍵の**嚴重な管理**
- 署名サービスにログインし、手動で明示的にデジタル署名を付与するなどの**作業負担**が発生します



ユーザビリティの高いデジタルトラストが求められる

- **普段使っているクラウドサービス** (Box、OneDrive等) を使いながら、なりすましを防いだ**ビジネスコラボレーション環境**を作れる
  - クラウドサービスと**独立して**、**ビジネスデータへのデジタル署名付与**や、**組織をまたいだ業務プロセス**(承認ワークフロー)の保証を実現

クラウドサービス



TaaSによりクラウドサービスを活用した**信頼なビジネスコラボ**が可能に  
(中央集権型→分散型)

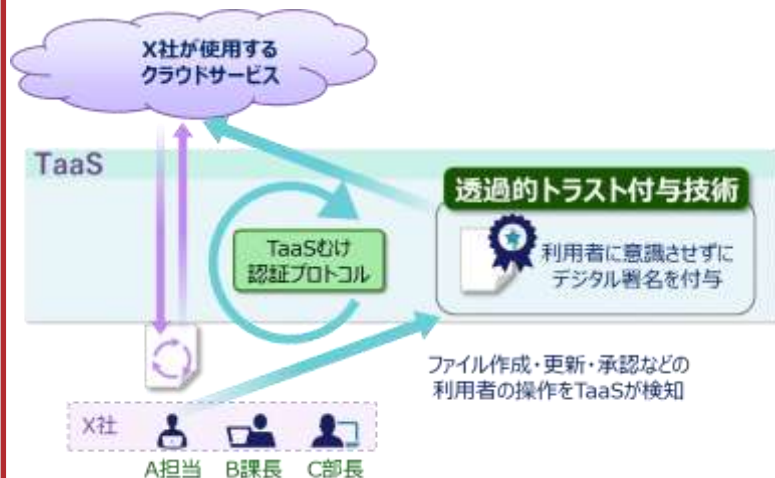


# TaaSを実現する透過的トラスト技術

2020.10.6 プレスリリース  
ビジネスデータの真正性を保証する  
デジタルトラスト仲介技術を開発

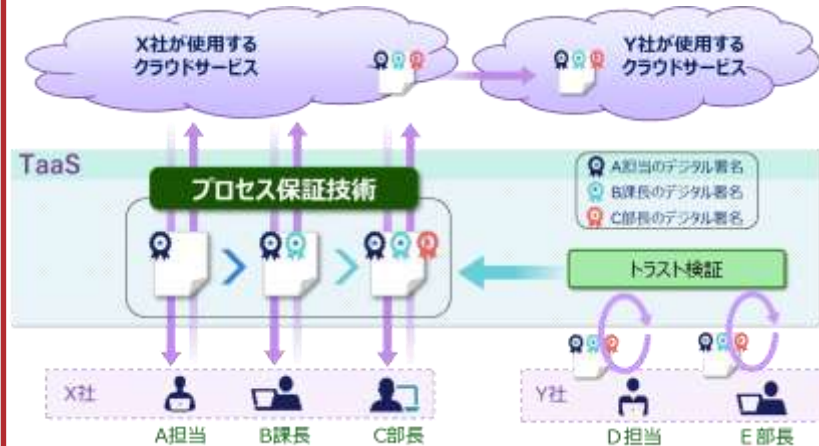
FUJITSU

## ① 透過的トラスト技術



TaaSはサービスと利用者間に入り  
**利用者に意識させずに**  
デジタル署名の付与を仲介

## ② プロセス保証技術

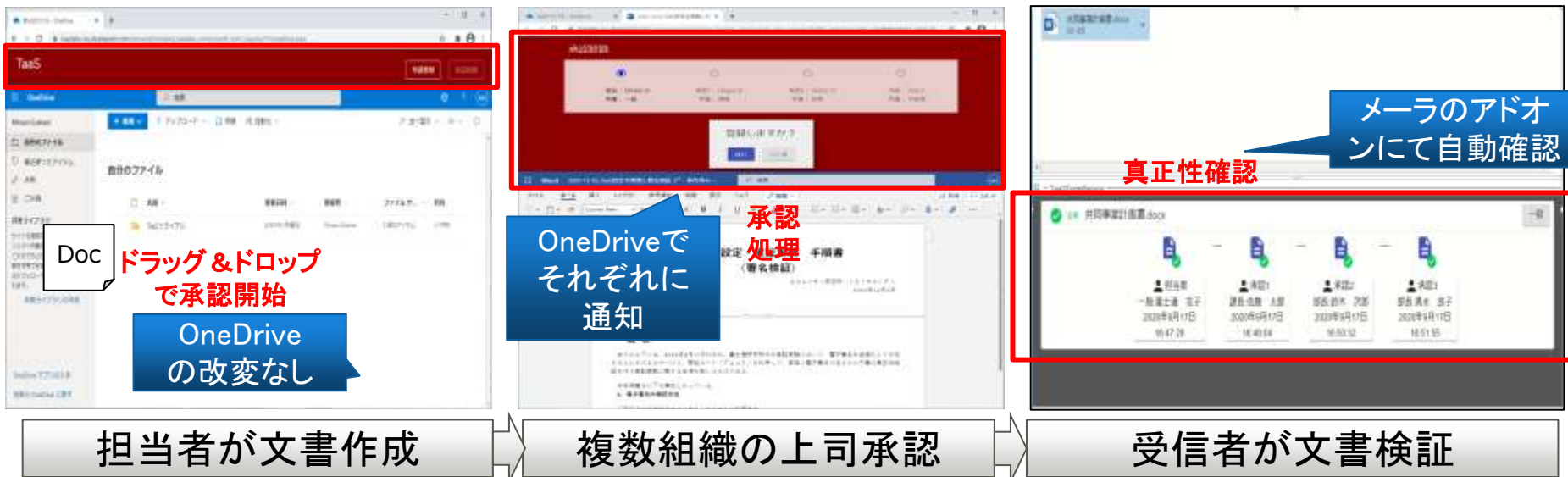


データの生成過程を見える化し、組織  
を跨いだ**業務プロセス**の真正性を保証

# 利用シーン① 組織をまたがる文書の真正性確認

説明動画

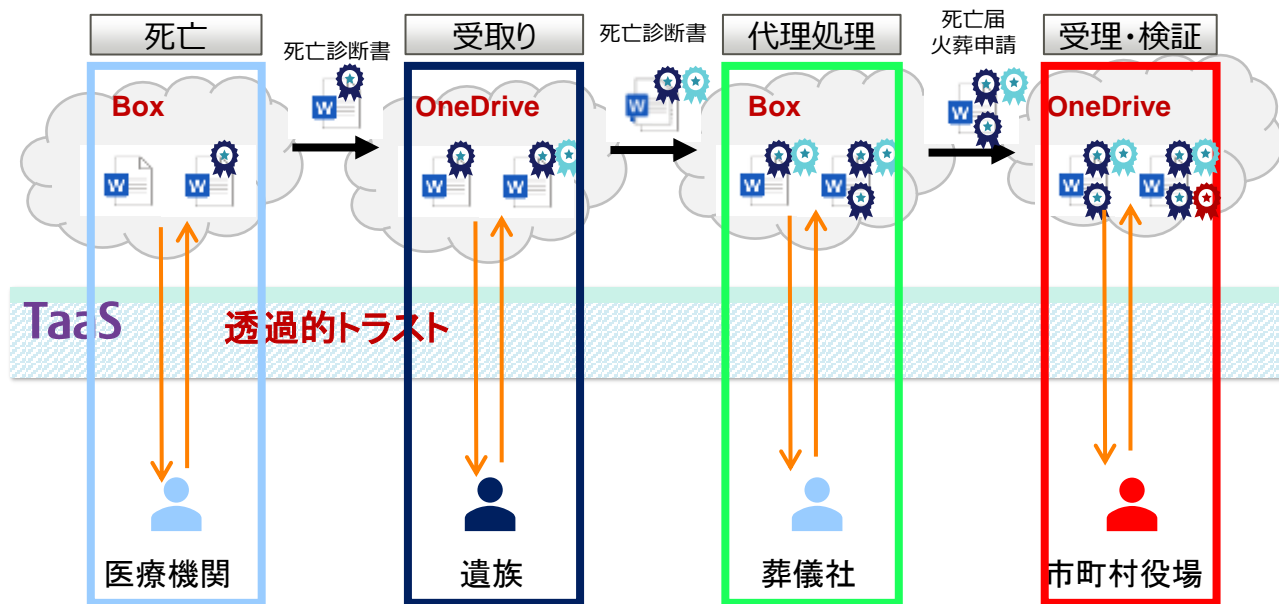
- アドホックに複数組織をまたいだ業務にTaaSを活用
  - BoxやOneDrive上の文書に、統一UXでデジタル署名や承認フローを付与
  - メールで文書を受け取った参加者が**真正性** (eシール相当) をTaaSで確認



普段のクラウドとメールで、文書の真正性を確認できる

# 利用シーン② クラウドをまたがったアドホックなワークフロー

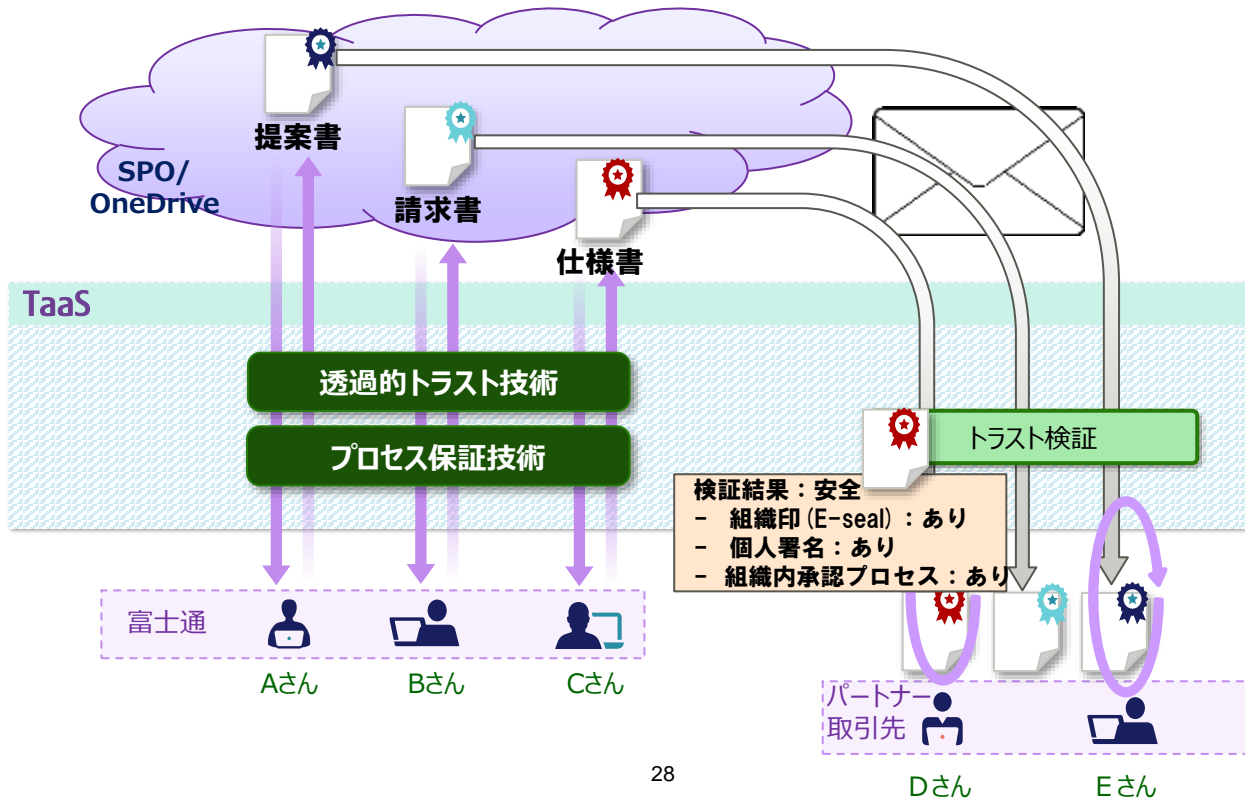
- 複数組織をまたがる文書によるコラボレーション(例: 死亡届)
- 複数関係者がワークフローに沿って承認手続きしたことを保証



紙で行っていた手続きが、普段の電子文書・クラウド・メールでできるように

# 利用シーン③ ビジネスメール詐欺の無い組織間ネットワークの構築

## ■ 富士通から取引先に送られる**全てのデータ**の真正性を確認可能



## デジタル・トラスト協議会 ～TaaS / コンセプト～

**【現在】**ゼロトラスト環境下、手続き等の業務や、そのデータ交換が行われている。  
・送られてきたデータやメールは正しいのか？  
・相手は信頼できる人なのか？



**【将来】**  
安全、かつシンプルな繋がり(人/企業/クラウド間等)を実現する環境の実現



- 脱ハンコ
- 非対面手続・業務効率化
- デジタル証左
- ワンスオンリー
- サプライチェーンデジタル化
- ビジネスメール詐欺対策
- オンライン融資
- ゼロトラストセキュリティ

・慶應・手塚教授先生が設立(2020/8/27)、電子データの信頼性を確保するためのデジタルトラストを民間利用するための課題整理・政府省庁への提言を行う場を提供。(2020/8/25 日経朝刊に記事が掲載)

- ・富士通研究所が提唱したTaaSをデジタルトラスト実現のコアコンセプトとして位置付け、民間普及促進
- ・ベンダー企業(N, H, F, T, セイコー、セコムなど)、ユーザー企業(みずほ情報総研、SMBCなど)30社以上が参加(2020.10.15)
- ・内閣府、法務省、総務省、経産省、金融庁、国税庁がオブザーバー参加



# 帝国DBとのeシール実証(3/31)

## ○帝国データバンク様と富士通(CPS事)間でのプレスリリースを発表

○透過的トラスト/TaaS技術は「富士通のデジタルトラスト仲介技術」として記載

### 富士通と帝国データバンク、国内初となる「日本版eシール」の社会実装に向けた実証実験を開始

「日本版eシール」を伴う実業務を想定した検証環境の構築と複数企業間での受け渡し

富士通株式会社(本社:東京都港区、代表取締役社長:時田隆仁、以下、富士通)と株式会社帝国データバンク(本社:東京都港区、代表取締役社長:後藤信夫、以下、TDB)は、コロナ禍でより一層需要が高まるデジタル文書の受け渡しにおいて発行元企業の真正性を証明する技術「日本版eシール」(注1)の社会実装に向け、国内初となるトラストプラットフォーム(注2)を構築した実証実験を2022年3月1日から約7か月間行います。

実証実験では、富士通のデジタルトラスト仲介技術とTDBの保有する企業の存在証明に関するナレッジを用いて「日本版eシール」を付与するトラストプラットフォームを構築し、実業務で想定されるデジタル文書の受け渡しの「日本版eシール」を付与し、その有用性を検証します。

本取り組みを通じて、両社は「日本版eシール」の社会実装に向けた方式検討、課題の抽出を推進します。

なお、本実証実験のeシールは「eシールに係る指針」(注3)で定義されているレベル1程度を想定しています。

#### 【背景】

現在、デジタル文書の真正性証明には「電子署名」や「PDFパスワード」などにより、文書作成者の証明や文書自体の改ざん防止が行われています。これらの方式では文書作成者個人の証明や改ざん防止は可能であっても、企業・組織が発した文書であるという法人による真正性証明ができないという課題があります。さらに、文書のデジタル化の必要性がコロナ禍で急速に高まりを見せたこともあり、迅速な社会実装に向けて、両社による本取り組みの開始に至りました。

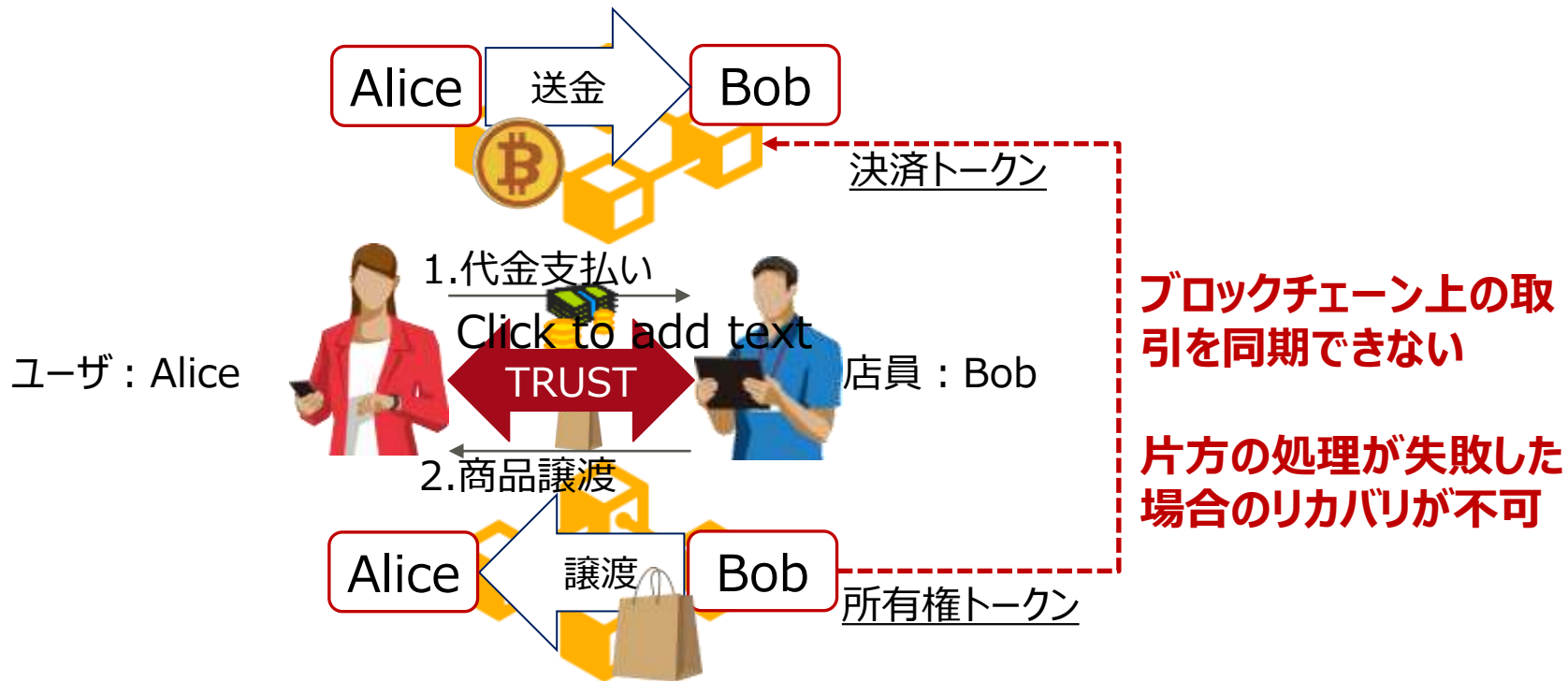
## 想定スケジュール・ロードマップ

### スケジュール/ロードマップ



# 3. データ(トークン)をつなげる②: ConnectionChain/Hyperledger Cactus

# 課題：異なるブロックチェーンをつなげるには

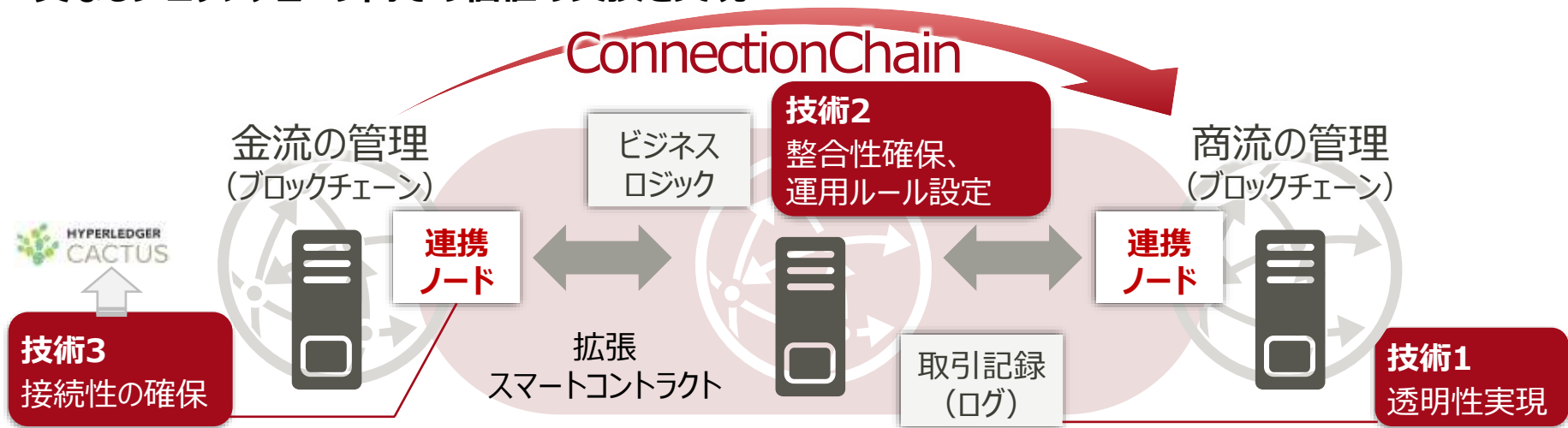


複数のDLTを対象にした高度な状況判断と、エラーリカバリ機能が必要



# トークン台帳を連携させる技術：ConnectionChain

- ✓ ブロックチェーン「で」つなげる技術
- ✓ 異なるブロックチェーン間での価値の交換を実現



- 【技術1：拡張スマートコントラクト】システムを跨ぐ取引を証拠性を担保したまま台帳管理し、透明性を実現
- 【技術2：マルチシナリオ機能】運用ルールをスクリプトで設定可能とすることで、既存サービスを特定顧客向けにカスタマイズする等、自在な運用ルール設定が可能。複数サービス間での処理の整合性も確保
- 【技術3：BC操作抽象化】ブロックチェーン操作の抽象化で接続機能を部品化。様々なBC基盤と接続可能

# OSS活動: Hyperledger CACTUS

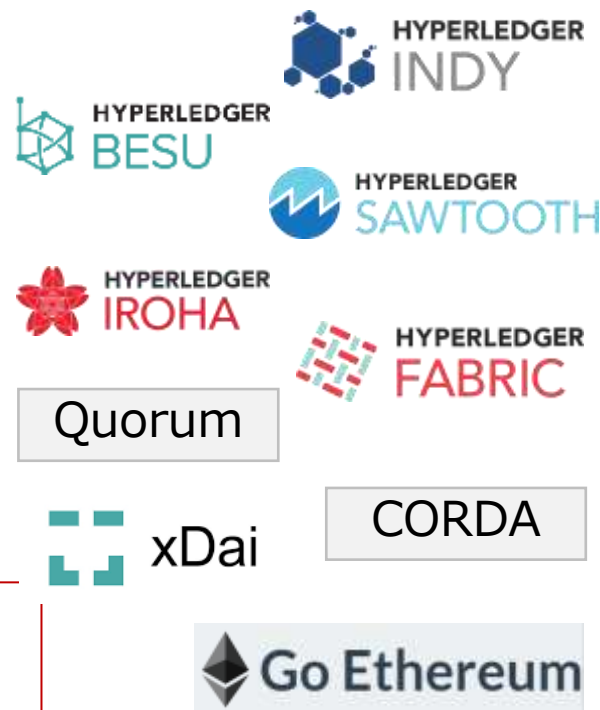


Hyperledger Landscape  
<https://landscape.hyperledger.org/projects>

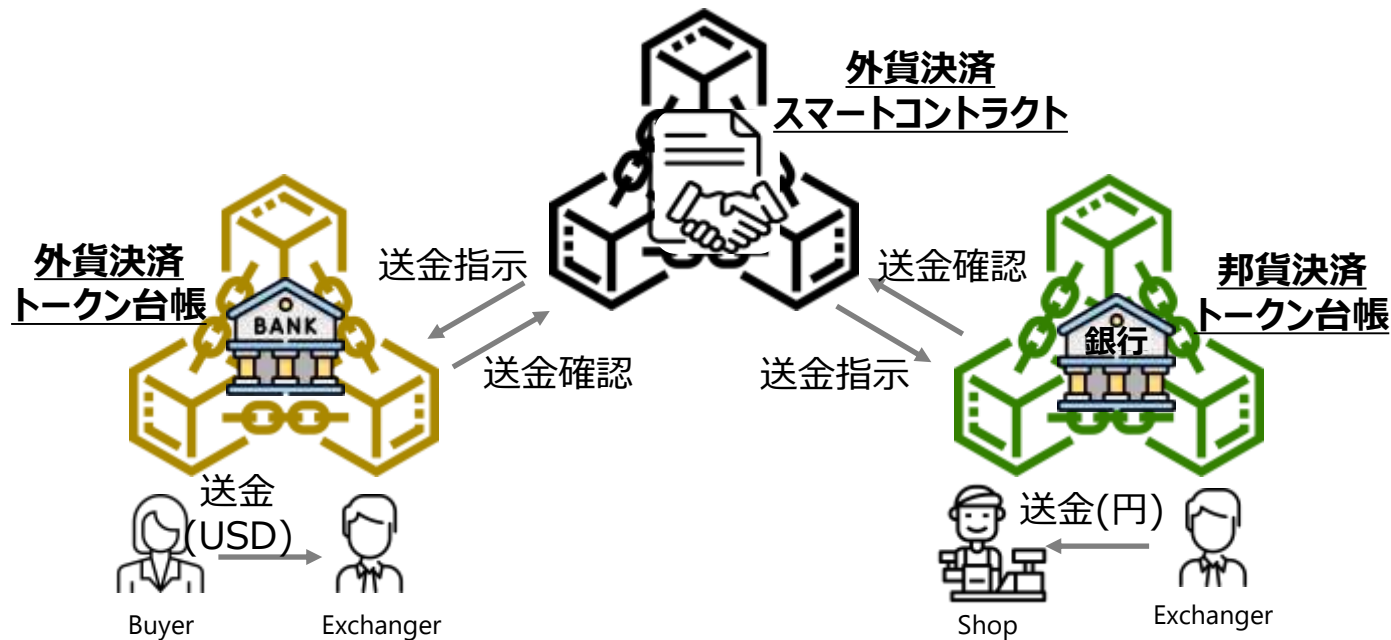
2022年3月に  
Hyperledger Cactus  
V1.0をリリース

富士通はCACTUSプロジェクトの設立に関わり、アーキ設計やソースコード開発でOSSコミュニティに貢献しています  
(参考: [Forbes Blockchain 50 \(2020\)](#) にも掲載)

## CACTUS supports

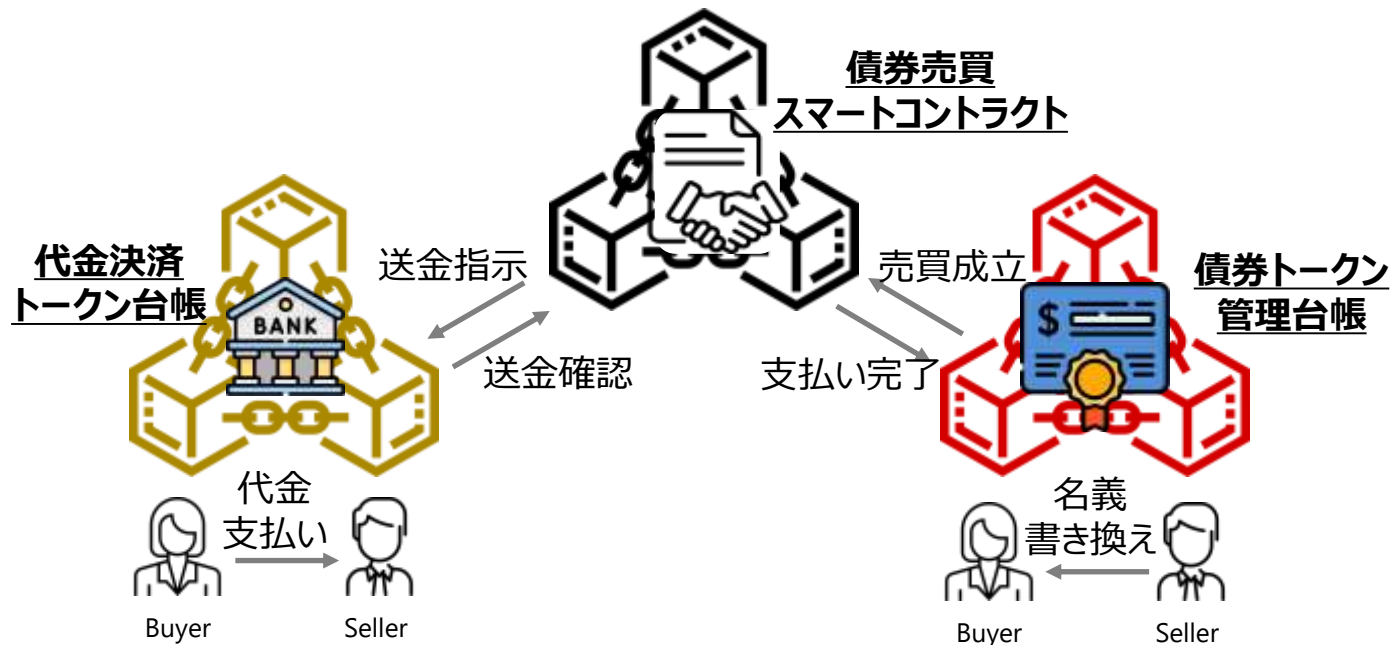


# 実証実験①：外国人旅行者向け決済



仲介者(Exchanger)が居れば同じブロックチェーンに参加する必要はない

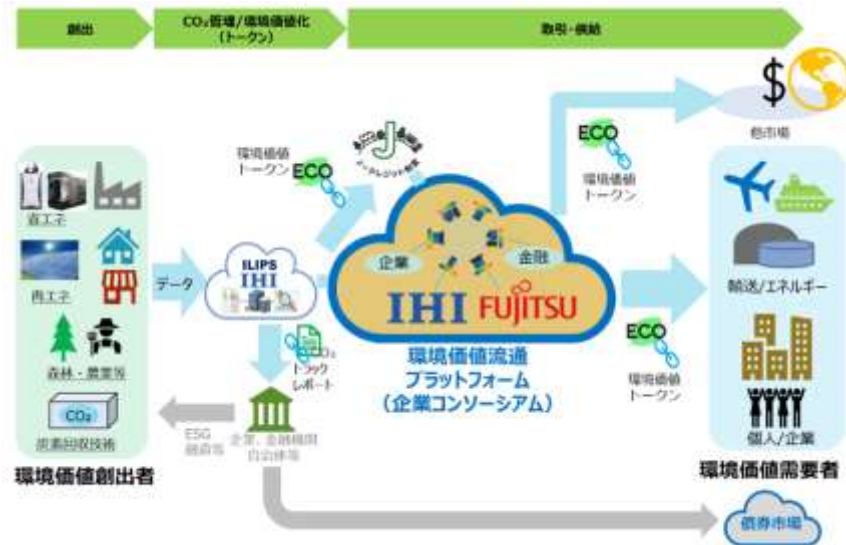
# 実証実験②：デジタル債券の売買



代金の支払いと名義書き換えを統一された処理ロジックで自動実行

## ○ブロックチェーン技術を活用した新たな環境価値流通プラットフォームの実現に向けた共同事業プロジェクトを開始（2022/04/12プレスリリース）

- IHIと富士通は、新たな環境価値取引エコシステムの市場活性化を目指した共同事業プロジェクトを開始
- 異なるブロックチェーン同士を安全に相互接続する「ConnectionChain」を活用して、世界各国の企業が創出するCO2削減量などの環境価値の効率的な流通を目指す

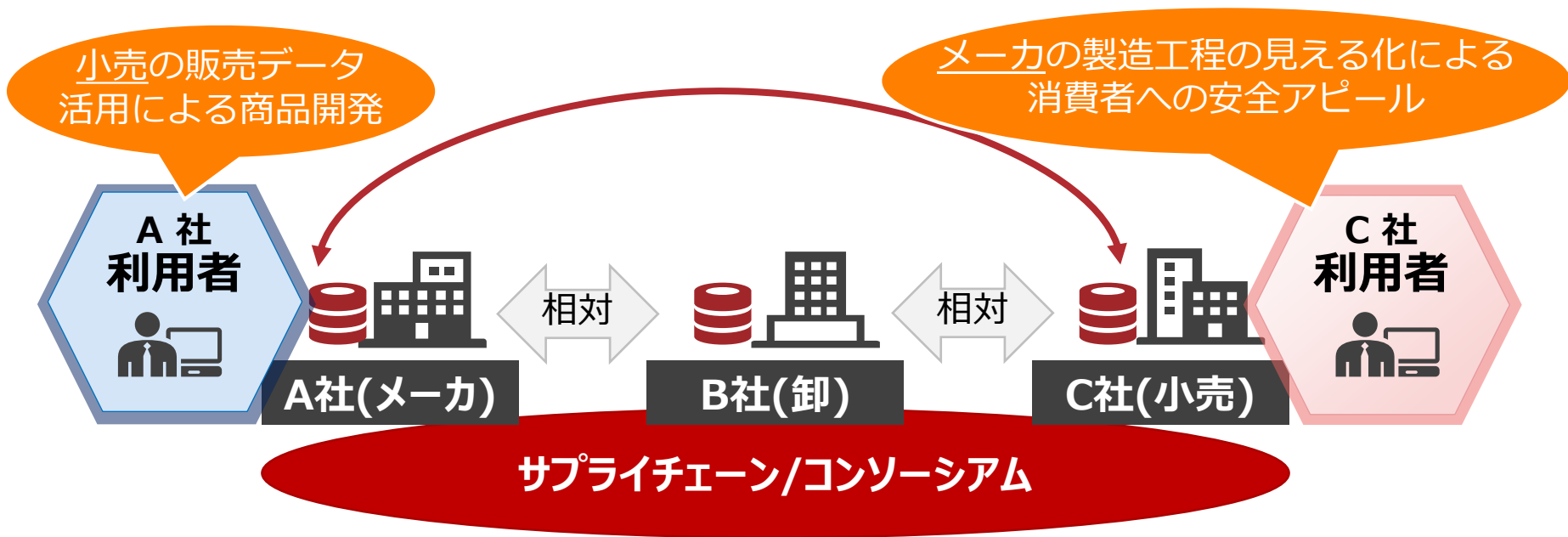


新たな環境価値流通プラットフォームを活用した市場のイメージ

## 4. プロセスをつなげる： CDL (Chain Data Lineage)

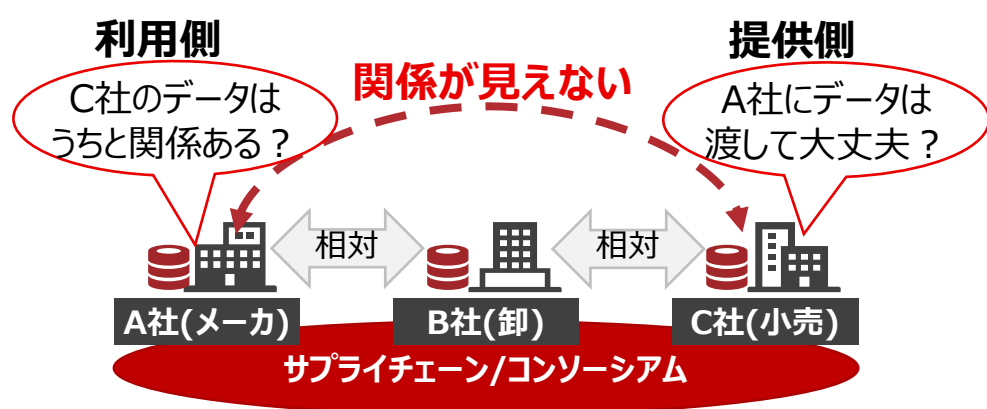
# 今後の企業を跨ぐデータ連携

- 今後のDXの1つとして、サプライチェーン上の相対する企業とのデータ交換だけでなく、それを越えた企業とのデータ連携がカギ
  - 例. 小売の販売データによるメーカーでの顧客ニーズに沿った商品開発

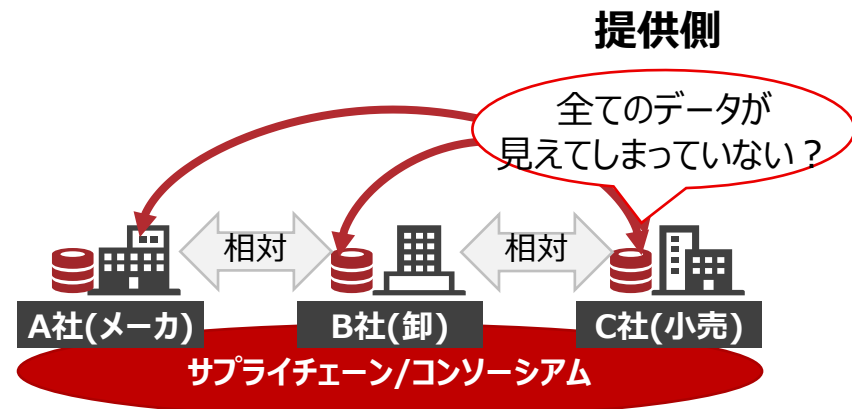


# 企業を跨ぐデータ連携の課題

- ① 相対企業から先の企業との関係性が見えず、データ連携が進まない
  - データ提供側：関係性が見えないと、相手へのデータ提供は不安
  - データ利用側：関係性が見えないと、相手データの有効性・信頼性が不明
- ② データ連携において企業間をつなげるのみでは、つないだ先に自社のデータが丸見え



課題①：不透明な関係では連携が進まない



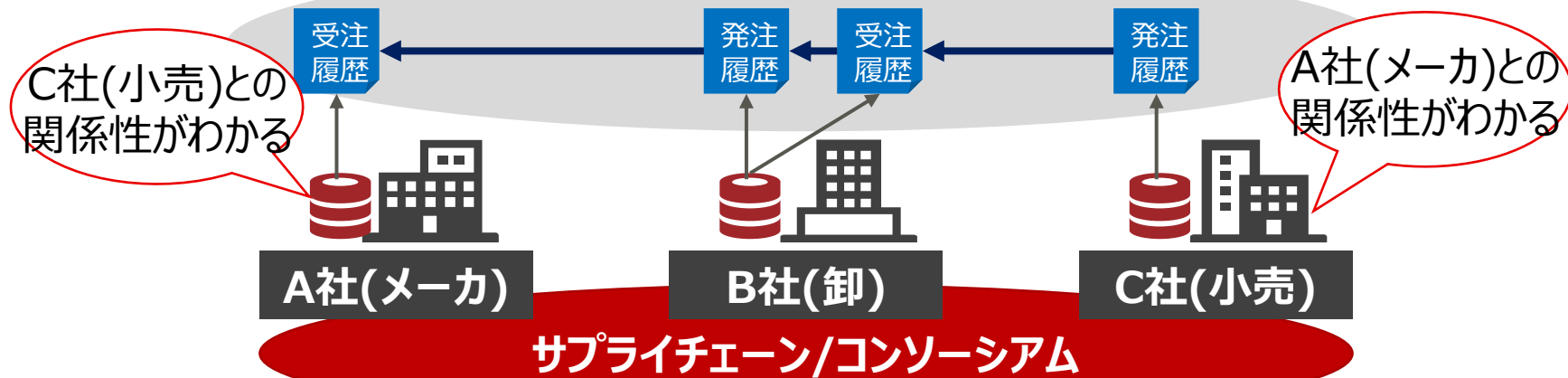
課題②：単なる接続ではデータが丸見え



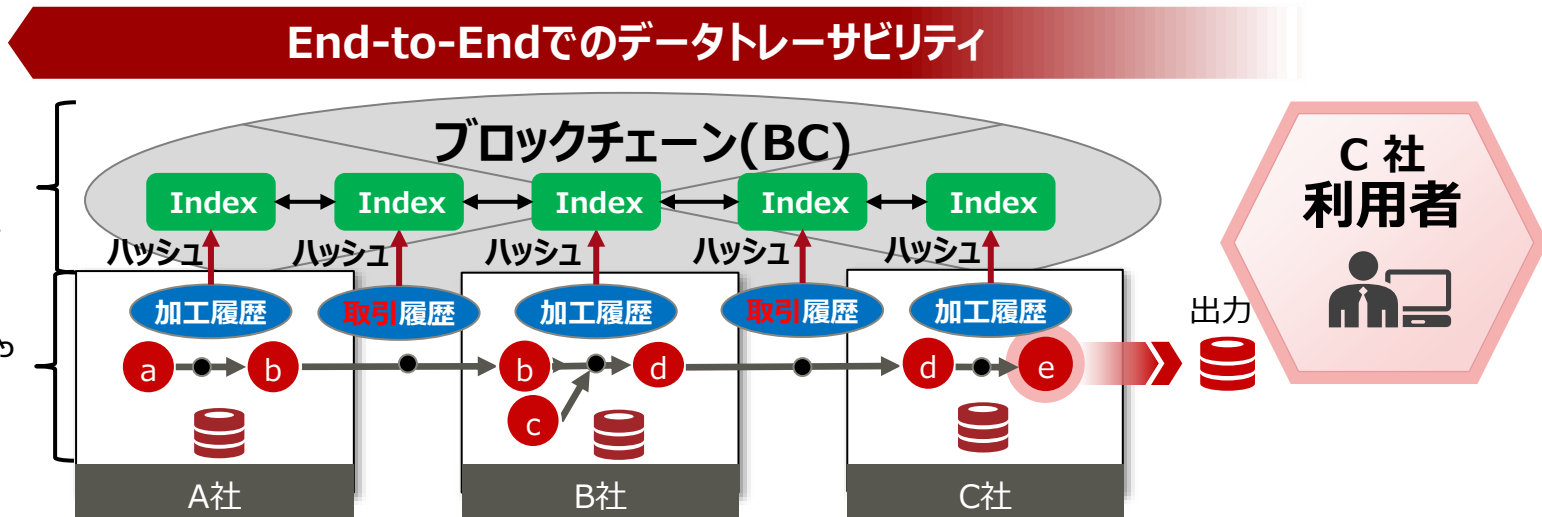
# Chain Data Lineage(データ来歴管理)

- サプライチェーン上でのモノの流通の履歴や受発注の取引履歴を、相対する企業を超えてEnd-to-Endの一気通貫で見える化
- 履歴の繋がりからサプライチェーン全体の取引関係を確認し、その後に履歴の関連付く企業固有データを提供企業のコントロールで安全に交換

サプライチェーン上の履歴を基点に、企業間のデータ利活用を促進



- 企業毎の履歴を、組織を跨いで連結管理。双方向でのEnd-to-Endの追跡を実現
- 耐改ざん性と透明性を提供するブロックチェーンによるグローバルな履歴管理と、機密性の高いローカルな履歴やデータの個社管理をハッシュで連携
  - 個社管理の履歴やデータをアクセス制御で守りながら、それらの真正性をブロックチェーンで担保

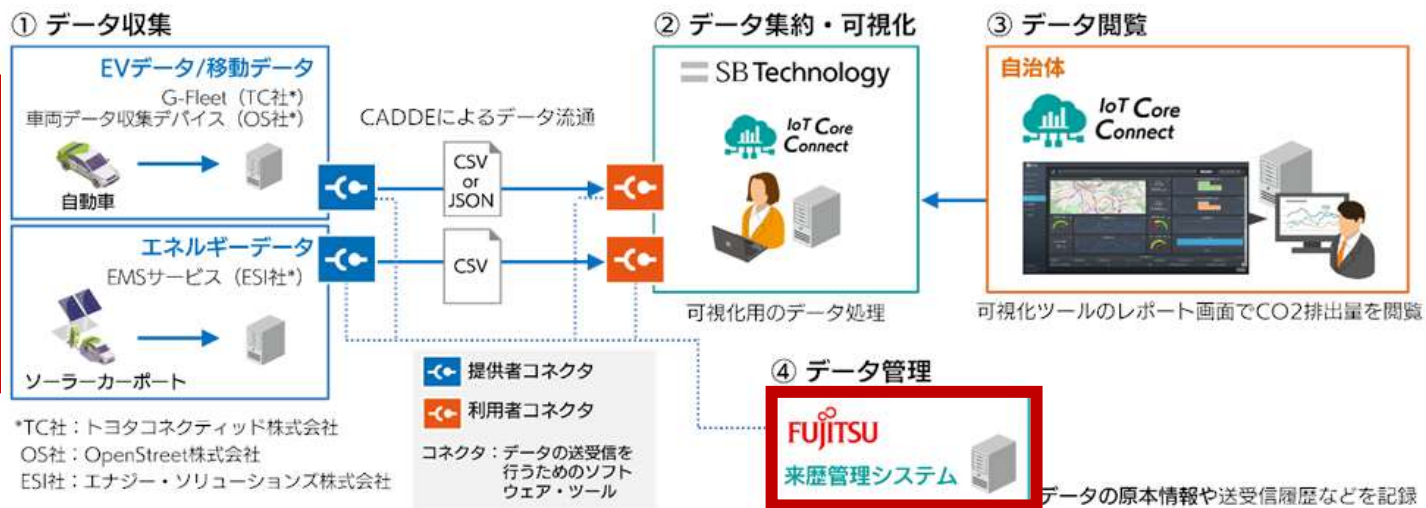


※個社管理：製造工程の履歴，含有化学物質データ等，特定の企業・シーンにのみ開示する履歴やデータ

# 適用事例：SIP実証実験での来歴管理の活用(3/31ブレス)

- SIP分野間データ連携基盤コネクタ(CADDE)に来歴管理システムを組み込み
- 4自治体の公用車(EV車)の走行実績データを2ヶ月間収集・活用し、自治体(データ利用者)、サービス事業者、自動車メーカー(データ提供者)でデータを流通
- 自治体はCO2排出量を確認可能、自動車メーカーは提供データがどこで利用されているかを確認可能

提供データの流通先を複数組織をまたがって確認可能



富士通参加箇所

この成果は、内閣府が実施し国立研究開発法人新エネルギー・産業技術総合開発機構 (NEDO)が管理法人を務める「戦略的イノベーション創造プログラム (SIP) 第2期/ビッグデータ・AIを活用したサイバー空間基盤技術」(JPNP18013) の結果得られたものです。

- ビジネスでつながることが前提によるリスク
- クロスインダストリーでDXを実現するために必要なトラスト関連技術をご紹介します
  - 人: IDYX(DID連携)
  - データ: 透過的トラスト (TaaS), ConnectionChain
  - プロセス: CDL
- メールやWebなどつながる基本的な仕組みがTrustにならないといけない時期にきています。Trusted Webのような、トラストを内在したWebの仕組みづくりに期待

- ConnectionChain, Cactus
  - ブロックチェーン同士を安全につなげるセキュリティ技術を開発  
<https://pr.fujitsu.com/jp/news/2017/11/15.html>
  - 富士通研究所とアクセンチュア、安心かつ確実な異なるブロックチェーン連携を共同で加速  
<https://pr.fujitsu.com/jp/news/2020/05/15.html>
  - ブロックチェーン技術を活用した新たな環境価値流通プラットフォームの実現に向けた共同事業プロジェクトを開始 (富士通、IHI) [ConnectionChain/Cactus] (2022/4/12)
- IDYX
  - オンラインの取引相手の信用を判断可能にするアイデンティティー流通技術を開発  
<https://pr.fujitsu.com/jp/news/2019/07/4.html>
  - デジタル決済時代に、個人データを安心して活用できる社会をつくる (JCB様)  
<https://www.fujitsu.com/jp/about/resources/case-studies/trends/cs-202004-jcb.html>
  - 学籍証明書のデジタルアイデンティティーを相互連携利用する実証実験を実施 (慶応大) 2022/4/14
- CDL
  - 自治体におけるゼロカーボンシティ施策の推進に向けた実証実験を実施、EV公用車の走行情報など多様なデータを活用しCO2削減量を可視化 (SIP国プロ) [CDL] (2022/3/31)
- その他
  - 高度かつ安全なAI利用の実現に向け、イスラエルの研究拠点にて富士通とベングリオン大学が共同研究を開始
  - 「デジタルトラスト」 津田(富士通研) PC Webzine 2020.2  
<https://www.pc-webzine.com/entry/2020/02/post-344.html>

Thank you

