Orchestrating a brighter world NEC

ブロックチェーン技術で Identityをセキュアに扱うためには ～Ethereum ERC725概要説明～

2019年11月26日

日本電気株式会社 金融システム本部
稲垣 正俊

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

目次

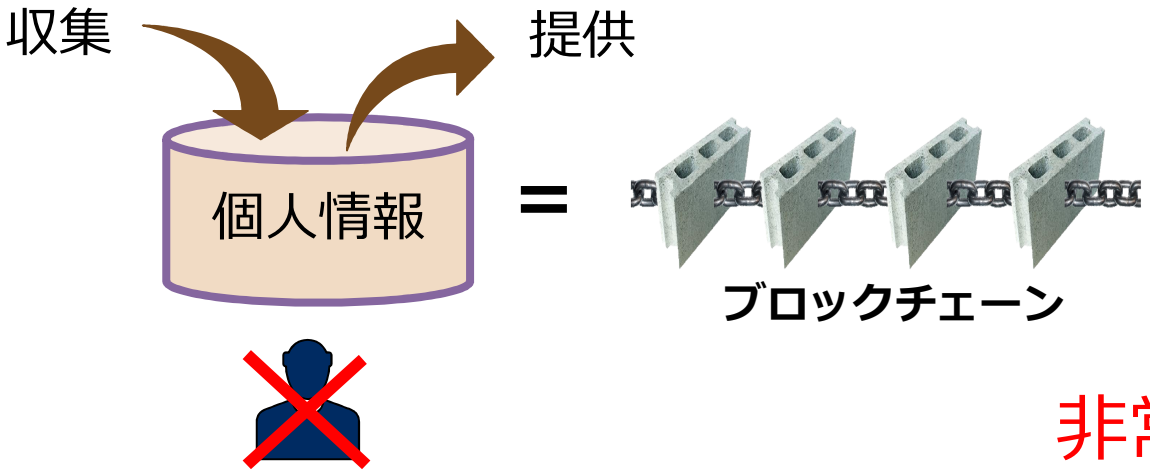
１．ブロックチェーンにおけるアイデンティティ標準化

- ブロックチェーンによる個人情報管理のメリット
- ブロックチェーンを用いた自己主権型アイデンティティの標準化

ブロックチェーンによる個人情報管理のメリット

なぜブロックチェーンに実装する？

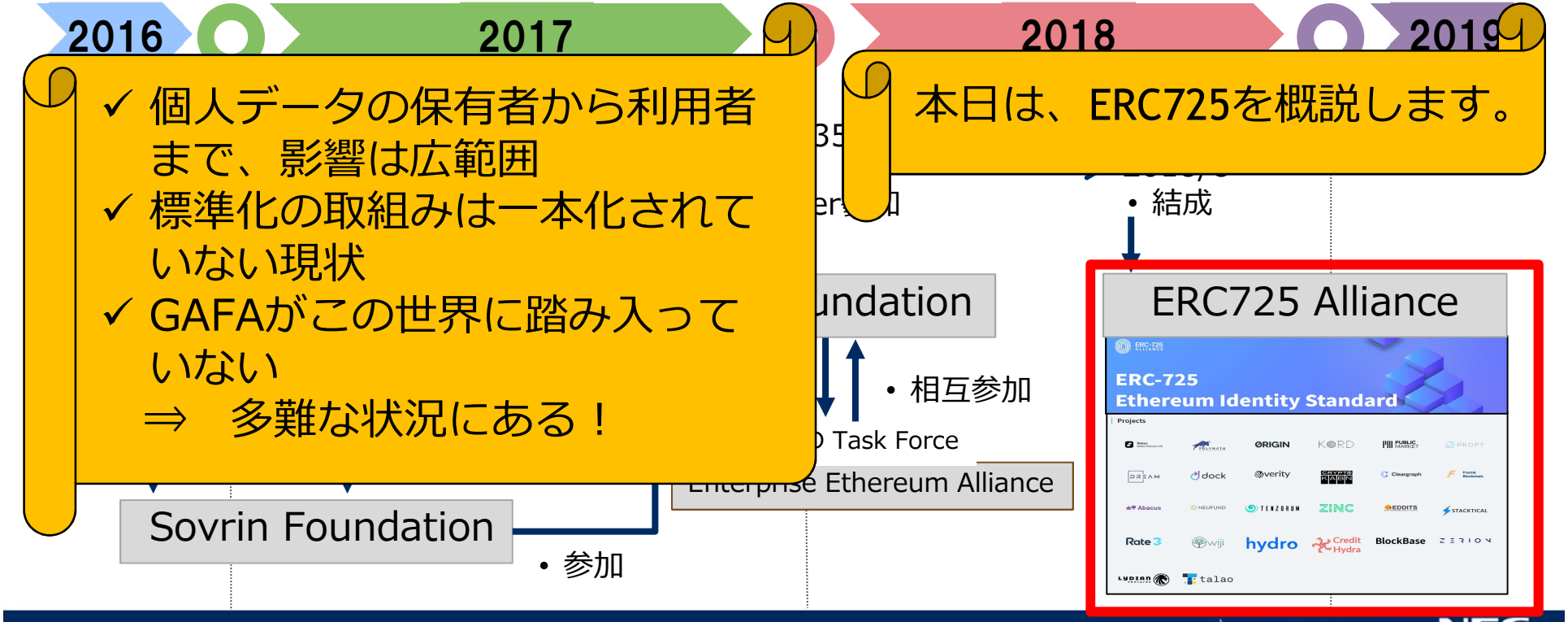
1. 個人情報の扱い（収集、提供の流れ）が完全に記録される
2. 取り込まれた個人情報の改ざん、漏洩の恐れがない
3. ブロックチェーン自体が、「あなたは誰？」の仕組みを必要としている



非常に相性がよい！

ブロックチェーンを用いた自己主権型アイデンティティの標準化

- ERC725、uPort、Hyperledger Indy等の様々な実装方式が存在
- DIFがW3C standards標準化推進、メンバーの取りまとめなど実施



2．ERC725/ERC734/ERC735概要

- ERC725とは？
- ERC725/ERC734/ERC735で使用される用語と具体例
- 健康診断の受診（具体例）
- セキュアに扱うために 削除権 (データの消去)への対応方法

ERC725とは？

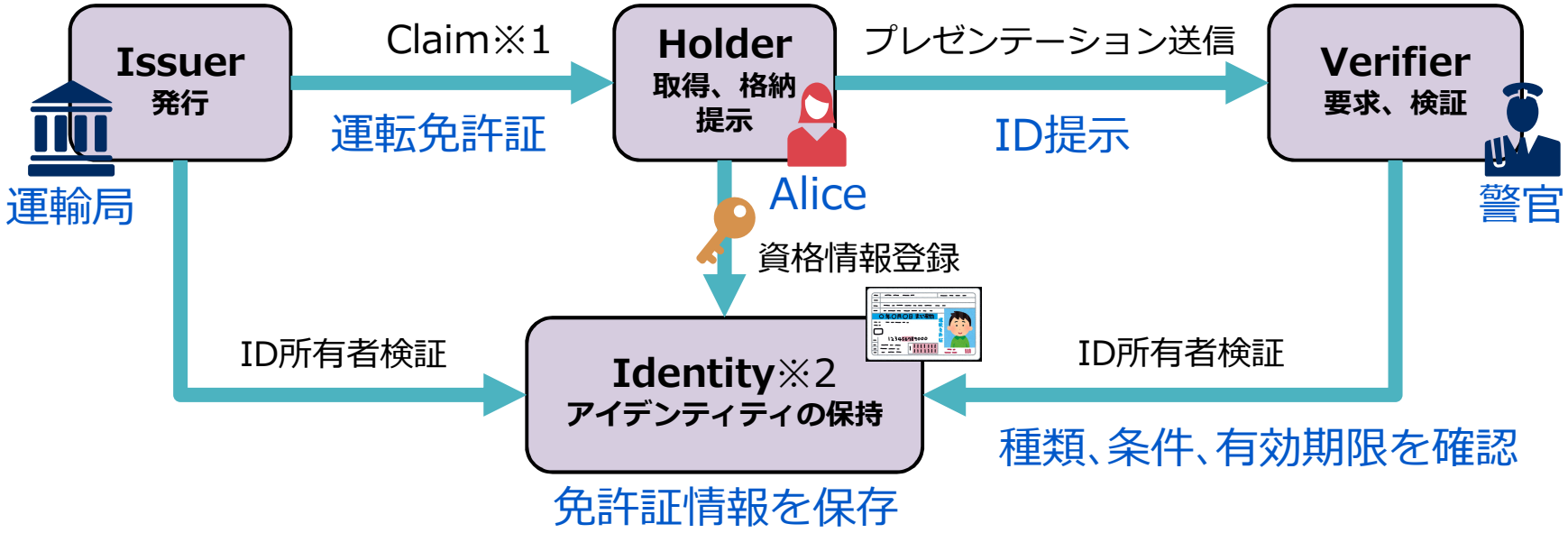
ERC725 とは、

公開鍵暗号を用いてブロックチェーン上で**自己主権型アイデンティティ**を管理するために提案されたEthereumの標準規格案。2017年10月に、ERC20およびWeb3.jsの作成者であるFabian Vogelstellerによって提案された。2018年10月にERC725-v2とERC734の２つの規格案に分割され、最新の規格案は以下の３つから構成されている。

- ERC725-v2: プロキシアカウントの規格
  https://github.com/ethereum/EIPs/issues/725
- ERC734：鍵管理の規格
  https://github.com/ethereum/EIPs/issues/734
- ERC735：Claimホルダーの規格
  https://github.com/ethereum/EIPs/issues/735

※ ERCとは、Ethereum Improvement Proposals (EIPs)の分類の１つで、アプリケーション層の提案がこのコードに分類されている。

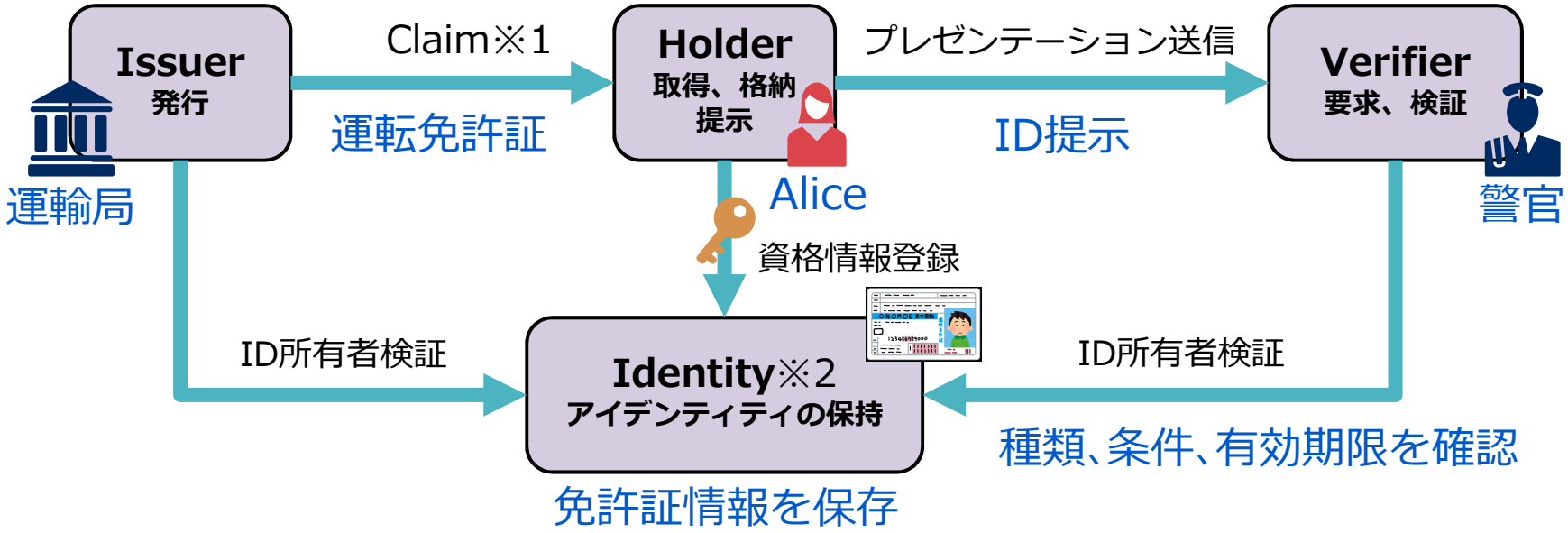
ERC725/ERC734/ERC735で使用される用語と例



- **Claim**（免許証、卒業証書など）は、
  - ✓ **Issuer**（学校、企業、政府など）が発行
  - ✓ **Holder**（学生、従業員、顧客など）が保持
  - ✓ **Verifier**（企業、公共機関、webサイトなど）に提示

W3Cの定義では、
※1：verifiable credential
※2：Identity Registry

ERC725/ERC734/ERC735で使用される用語と例

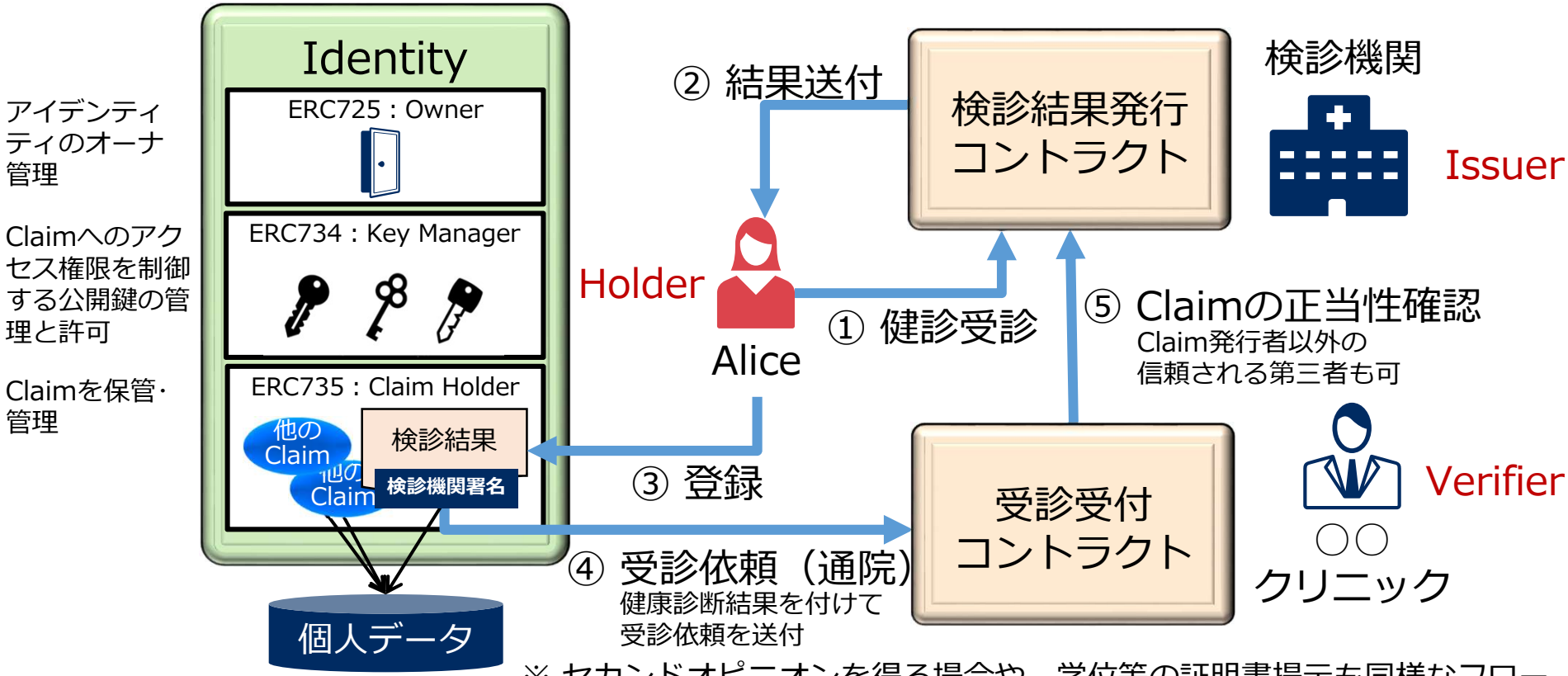


- **Identity**は、
  - ✓ 対象は不定（個人、企業、物、イベント、・・・）
  - ✓ Claimを格納・管理
  - ✓ １対象に複数Identityが可（医療関連、金融関連、・・・）
  - ✓ 実体はスマートコントラクト（Identityごとに１コントラクト）

W3Cの定義では、
※1：verifiable credential
※2：Identity Registry

健康診断の受診（具体例） Aliceが健康診断結果を掛かり付けのクリニックに提示

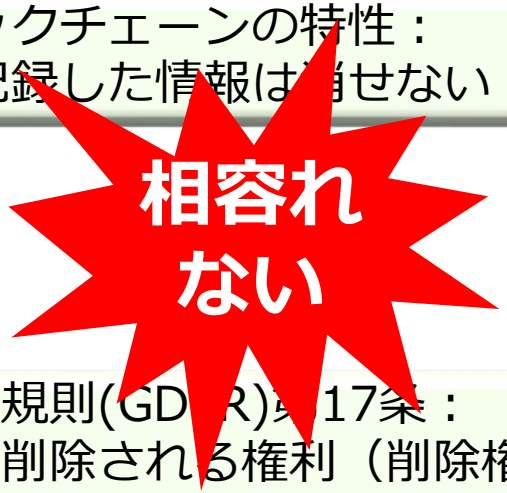
自己主権型アイデンティティは、ERC725/ERC734/RC735の組合わせで実現される。



※ セカンドオピニオンを得る場合や、学位等の証明書提示も同様なフロー

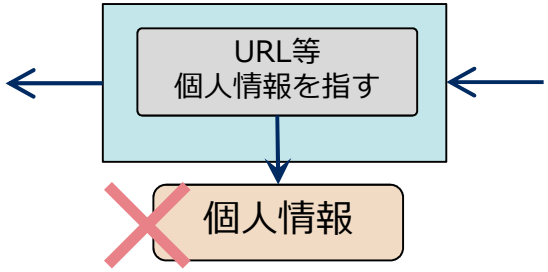
セキュアに扱うために　削除権 (データの消去)への対応方法

ブロックチェーンの特性：
一旦記録した情報は消せない



一般データ保護規則(GDPR)第17条：
忘れられそして削除される権利（削除権）
データ主体は、管理者に個人データの消去、および個人データのさらなる拡散防止を求める権利を有する。

セキュアに扱うために　削除権 (データの消去)への対応方法

	オフチェーン方式
方式	ブロックチェーンにはURLのみを書き、個人情報は外部ファイルに保存
データ配置と対応	Blockchain 
課題など	↑ ↑ ↑ ↑ 個人情報保護法だけなら、これらも通用？ （努力の跡が見られる！）

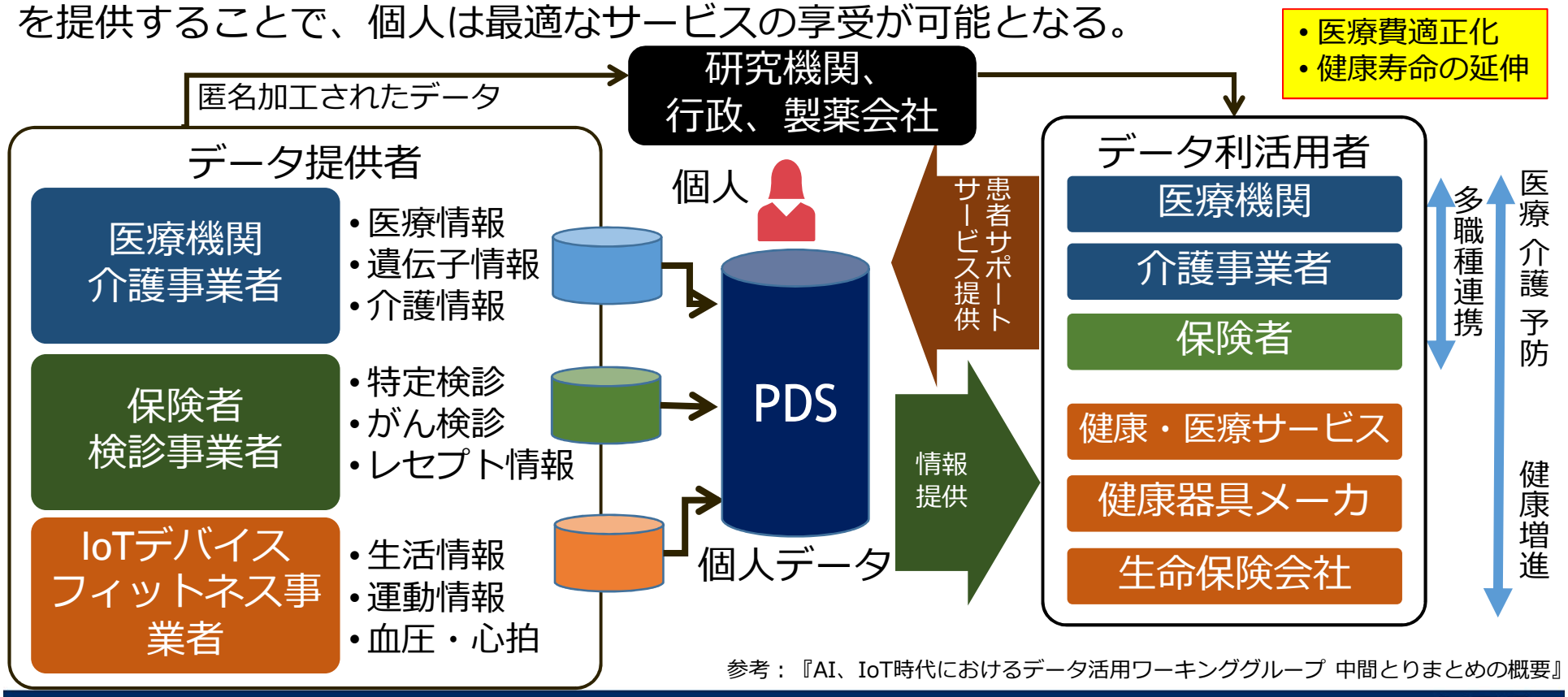
参考：https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most

3．ユースケース

- 医療・介護・ヘルスケア分野でのユースケース
- ERC725を使用したプロジェクトでのユースケース

医療・介護・ヘルスケア分野でのユースケース

生涯に渡り個人の医療・健康情報が管理可能となり、また医療・介護事業者等にデータを提供することで、個人は最適なサービスの享受が可能となる。



参考：『AI、IoT時代におけるデータ活用ワーキンググループ 中間とりまとめの概要』

ERC725を使用したプロジェクトのユースケース

ERC725Allianceの“ERC 725 Use Cases”から抜粋翻訳

Project名	説明
Origin	Origin Protocolは、ERC725をOriginのユーザーIDの基盤として使用。 ERC725は、将来、他のプロジェクトやDappsとの相互運用性を最大化するために選択された。
Caelum Labs	Caelum Labsは、ERC725をEthereumベースのブロックチェーンの基本的なローカル/ナショナルIDシステムとして使用する予定。 主な目標は、それを使用して、人々、企業、行政の間の信頼を確立すること。
Hydro	Hydroは、Identity管理を含むdApp開発プロセスの側面を促進･改善するためのプラットフォーム層を提供することを計画し、アプリケーションの特定のニーズを満たすことができる他のID標準とともに、ERC725の標準実装を提供することを計画。
LydianID	LydianVenturesは、いくつかのプロジェクトでERC725 / 735のIDと証明を使用し、ID管理DappとしてLydianIDを作成。 LydianIDは現在、他の人と認証を共有できる学生の研究をブロックチェーンで認証するために、学術機関によって使用されている。

https://github.com/ERC725Alliance/erc725/blob/master/docs/use-cases.md

４．課題

- ERC725/ERC734/ERC735の課題

ERC725/ERC734/ERC735の課題

- 本規格はIdentity管理としてシンプルな仕様となっていて、『システム』として採用するためには検討すべき周辺事項が多数存在する。
- この規格がEthereumをベースに作られているので、他のプロダクトで作成されたIdentity管理と互換性がない。
- DID(Decentralized Identifier)への集約（ERC725はメソッドの１つ）が可能か、今後の展開の先行きは不透明。

付録

- ERC725を理解するには
- ERC734：鍵の構造
- ERC735：Claim情報の構造

ERC725を理解するには

以下の記事が理解を深める助けとなる。

1. Origin Identity Playground
   ERC725/735コード事例と活用サンプルアプリ
   - https://github.com/OriginProtocol/origin-playground

2. First impressions with ERC 725 and ERC 735—identity and claims
   上記のコードを用いたもう一つの活用サンプルアプリ
   - https://hackernoon.com/first-impressions-with-erc-725-and-erc-735-identity-and-claims-4a87ff2509c9

3. A Companion Guide to “First impressions with ERC 725 and ERC 735 - identity and claims” (Part 1)～ (Part 3)
   上記サイトの詳細説明
   - https://medium.com/@kctheservant/a-companion-guide-to-first-impressions-with-erc-725-and-erc-735-identity-and-claims-part-1-51b53603cfc0

ERC734：鍵の構造

ERC734において、鍵の構造は以下のように定められている。

```
struct Key {
    uint256[] purposes;
    uint256 keyType;
    bytes32 key;
}
```

- purposes ：
  キーの用途（例　1 = MANAGEMENT、2 = EXECUTION）
- keyType ：
  キーのタイプ（例　1 = ECDSA、2 = RSA）
- key：
  公開鍵

※ Purpose、KeyTypeは、開発者による拡張定義も可。

ERC735：Claim情報の構造

ERC735において、Claimの構造は以下のように定められている。

```
struct Claim {
        uint256 claimType;
        uint256 scheme;
        address issuer;
        bytes signature;
        bytes data;
        string uri;
    }
```

- claimType：
  Claimの種類（例　1＝biometric, 2＝residenceなど）
- scheme　：
  このClaimがどのように処理されるべきかについての
  スキーム（例　1=ECDSA, 2=RSAなど）
- issuer：
  発行者のIdentityコントラクトアドレス
- signature：
  Claim発行者がこのIdentityに対してClaimを発行したと
  証明する署名
- data：
  外部にあるClaim実データのハッシュ、またはSchemeに
  基づく実データ
- uri：
  Claim実データの置き場所（例　HTTPリンク, IPFSハッシュなど）


Orchestrating a brighter world
NEC