

# DID技術動向

2021.3.4

# | 目次

1. 自己紹介
2. DID技術動向（ERC725）
3. DIDの今後
4. おまけ：興味を持ったきっかけ

# 自己紹介：こんにちは！

שלום!



## 須田 隆太郎 (すだ りゅうたろう)

- ✓ 東京大学工学部 計数工学科3年 (推薦入学)
- ✓ CO.NECT東大ブロックチェーン学生起業家支援プログラム4期
- ✓ IDやERC725規格の研究開発を行っています。
- ✓ 2021年1月よりCougerでインターン中

その他の活動：

- Red Bull Basement 2020日本代表
- MAKERS UNIVERSITY 6期生



# | この1年考えてきたこと

正しい情報を載せた人が  
評価される仕組み作り

# | この1年考えてきたこと

正しい情報を載せた人が  
評価される仕組み作り

# | この1年考えてきたこと



# 情報の正確さの要素



1. 改ざん耐性
2. 正確さへのインセンティブ
3. 第三者による再評価

# 身元保証に必要な条件とは



1. 改ざん耐性
2. 身元の検証可能性
3. 個人情報面のセキュリティ



# ブロックチェーンにできること



情報の正確さ

1. 改ざん耐性
2. 正確さへのインセンティブ
3. 第三者による再評価



PoW, PoS



Token

情報提供者の  
身元

1. 改ざん耐性
2. 身元の検証可能性
3. 個人情報面のセキュリティ

# ブロックチェーンにできること



1. 改ざん耐性



PoW, PoS

2. 正確さへのインセンティブ



Token

3. 第三者による再評価

1. 改ざん耐性

2. 身元の検証可能性

3. 個人情報面のセキュリティ



スマートコントラクトで  
実現できないか？

# | アイデンティティとは？

身元確認は全て **請求する・される**



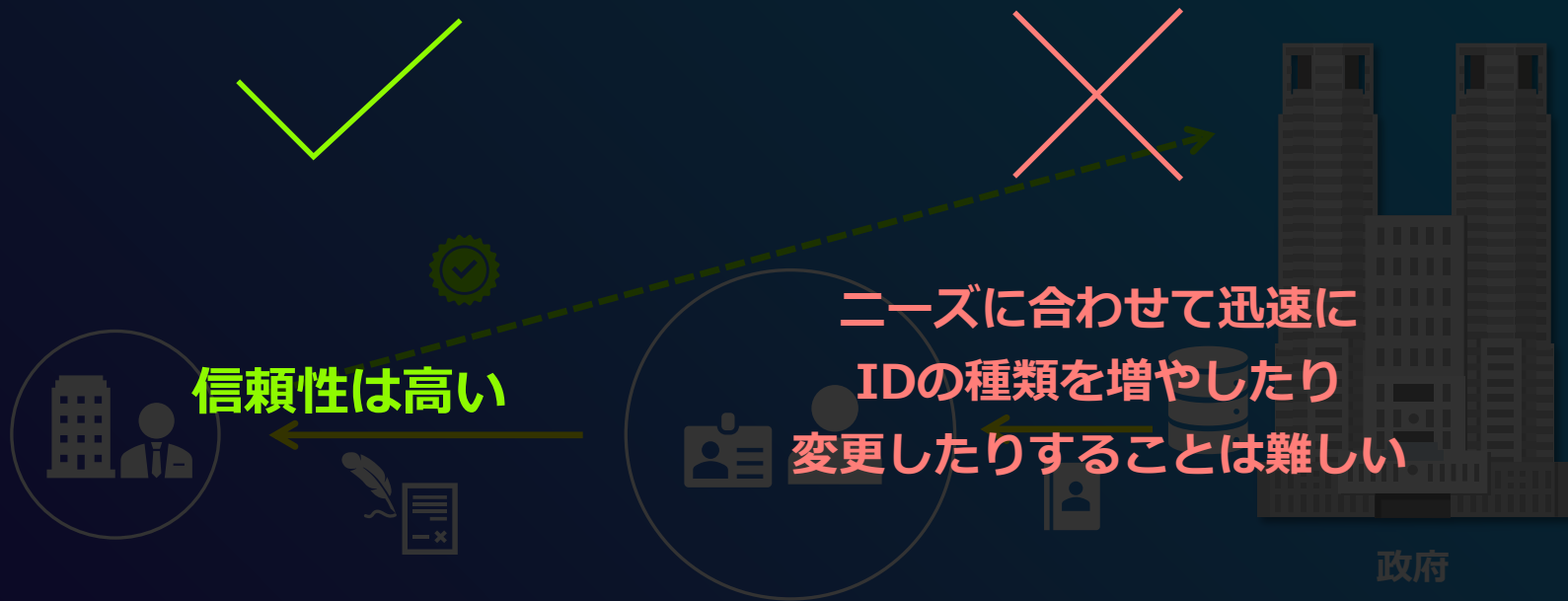
# 中央集権的なアイデンティティ

信頼の根拠は政府などの中央組織



# 中央集権的なアイデンティティ

信頼の根拠は政府などの中央組織



# | 分散型アイデンティティ (DID) とは？

**ERC: Identity**



<https://www.slideshare.net/FabianVogelsteller/erc-725-identity>

# | ERC725とは

- ERC725: Ethereum上でDIDを実現することを目的として2017年10月にFabian Vogelstellerによって提案された規格.
  - FabianはEthereumの初期からのデベロッパーであり、ERC20トークン規格の発案者でもある.
  - 現在同氏は、ICOのためのプラットフォーム"LUKSO"のファウンダーとして活動中
- ERC725を用いたEthereum Identity 標準化の動きがあり、30を超えるプロジェクトが正式に参加している (ERC725Alliance) .
- 一方、提案から3年以上が経過したが、一般ユーザ向けサービスレベルにはまだ浸透していないのではないか.
  - 例えば、gitcoinのユーザ認証では「github連携でユーザ登録 → ウォレット選択 → grant支援」の流れ
  - 同プラットフォームは、C.R.E.A.M.のグラント資金の調達でも用いられた.

# | ERC: Identityの考え方



**Keys**

公開鍵



**Execution**

実行

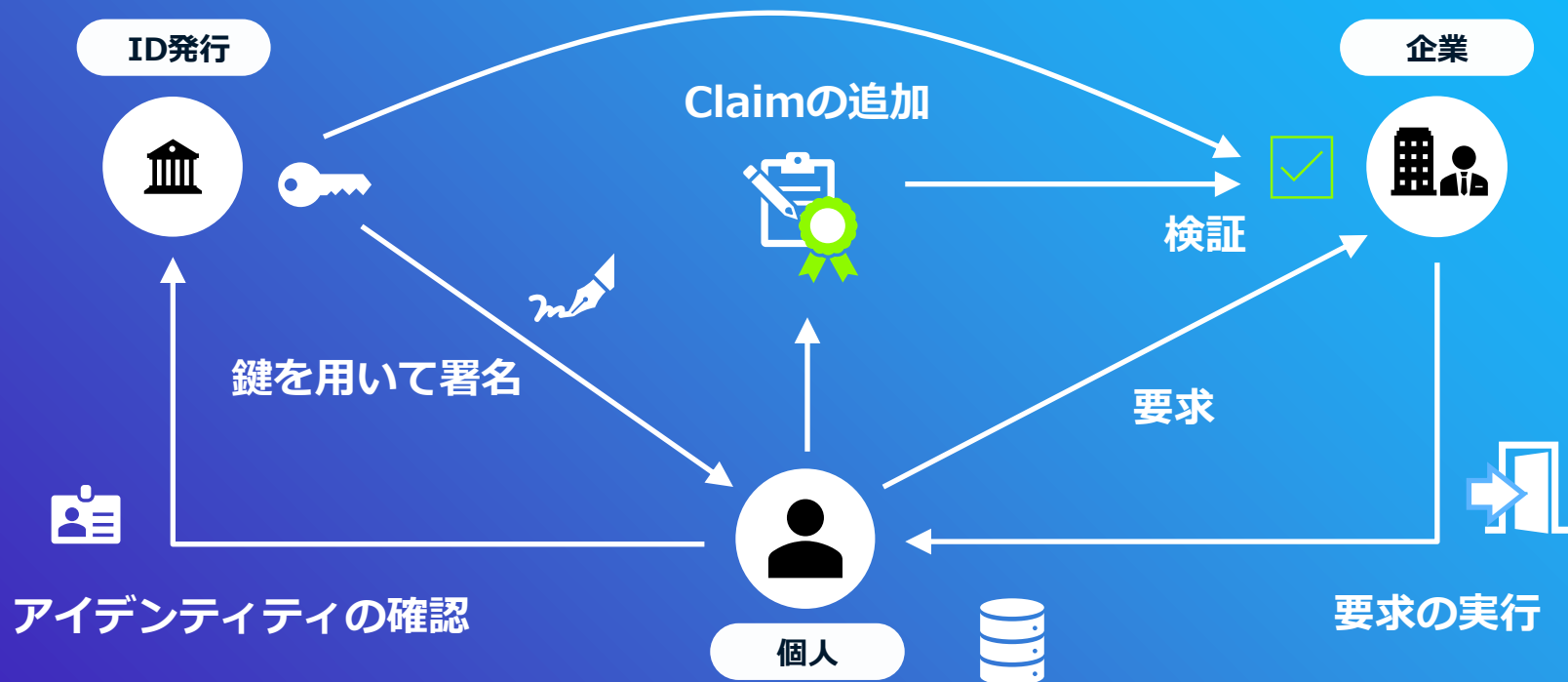


**Claims**

請求



# ERC: Identity の仕組み



# ERC: Identity の仕組み



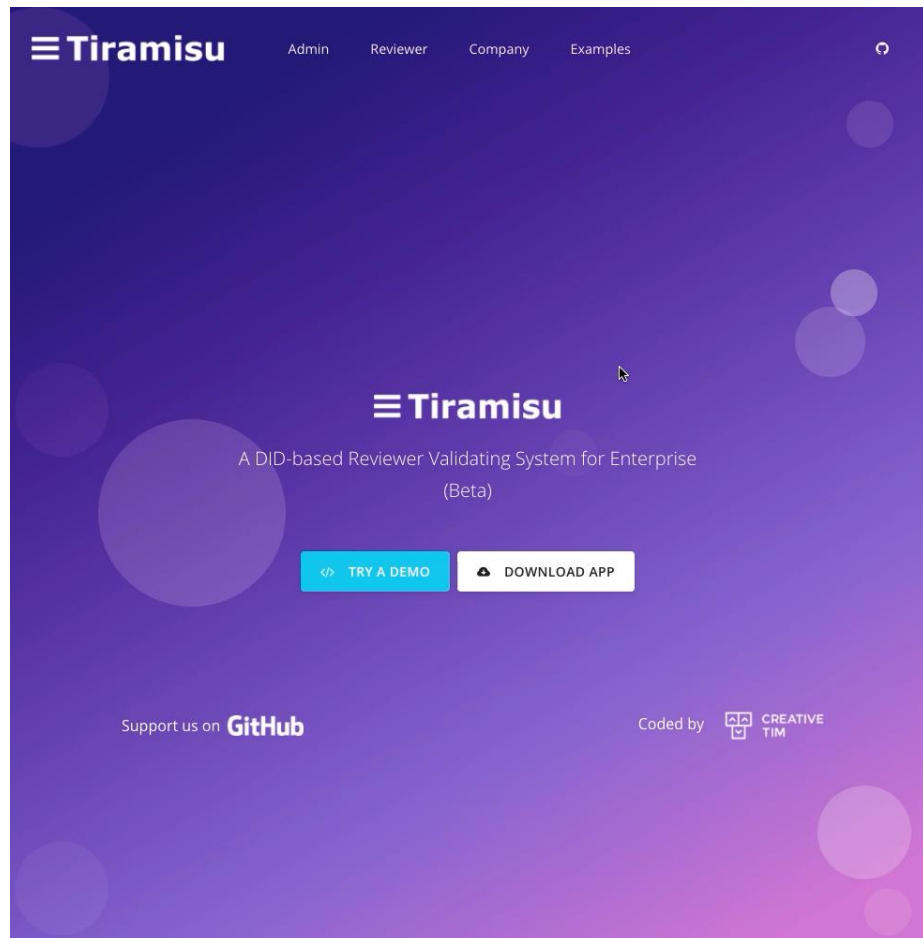
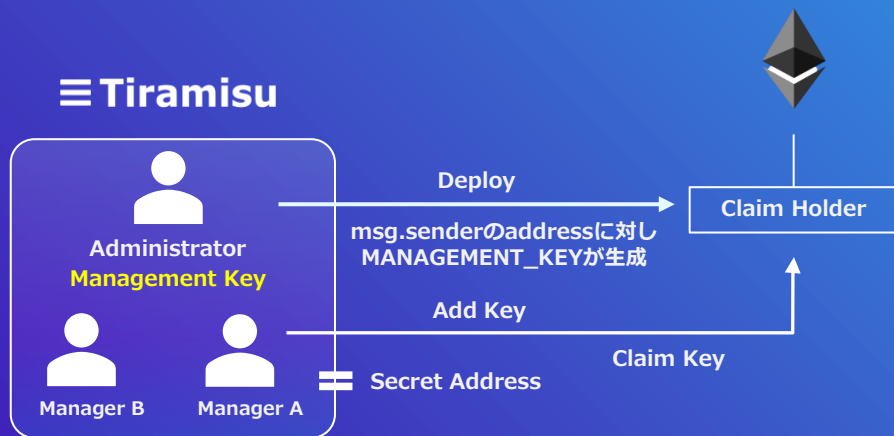
# 分散型IDを用いた レビュアー認証とトークン報酬 プラットフォーム



# Demo

## 1. セットアップ 鍵の登録

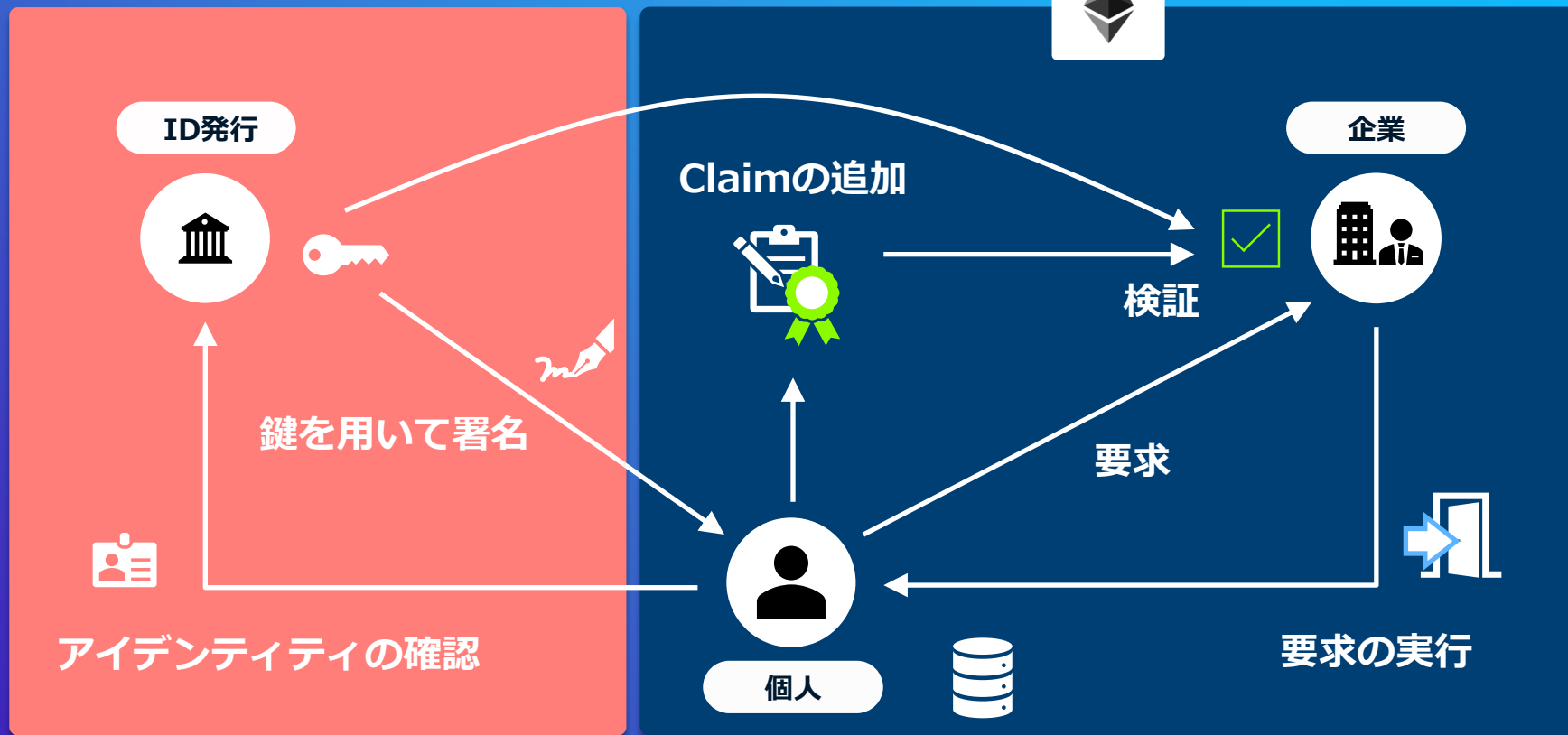
役割に応じて複数の鍵を登録可能



# | ERC725 まとめ

1. ERC725は「鍵」「署名」「要求」
2. アイデンティティの実態は「ある所望の関数が実行できる」ということ
3. 課題：大元のIDチェックはオフチェーン

# ERC: Identity の仕組み




# | ERC725の変遷とこれから

1. ERC725の現状
2. ERC725の課題に関する考察
3. IoT領域における応用可能性について

# | ERC725 v2 の提案

## ERC: Proxy Account #725

 Open frozeman opened this issue on Oct 3, 2017 · 272 comments



frozeman commented on Oct 3, 2017 · edited

Contributor



```
eip: <to be assigned>
title: ERC-725 Smart Contract Based Account
author: Fabian Vogelsteller <fabian@lukso.network>, Tyler Yasaka (@tyleryasaka)
discussions-to: https://github.com/ethereum/EIPs/issues/725
status: Draft
type: Standards Track
category: ERC
requires: ERC165, ERC173, ERC1271 (optional)
created: 2017-10-02
updated: 2020-07-02
```

This is the new 725 v2 standard, that is radically different from [ERC 725 v1](#). ERC 725 v1 is be moved to [#734](#) as a new key manager standard.

Simple Summary

<https://github.com/ethereum/EIPs/issues/725>




# | ERC725 : v1→v2

1. v1よりも包括的な枠組みを目指す
2. 他のスマートコントラクトを実行したりデプロイしたりできる
3. スマートコントラクト=ID →「実行できる（アクセスできる）」ということがIDの証明
4. 2つのサブコントラクトからなる
  - ERC725X: 他のスマートコントラクトにアクセス（execute, deploy）
  - ERC725Y: コントラクトオーナーが任意のデータを登録可能

# | ERC725 v2 の提案

## ERC: Proxy Account #725

 Open frozeman opened this issue on Oct 3, 2017 · 272 comments



frozeman commented on Oct 3, 2017 · edited

Contributor  ...

```
eip: <to be assigned>
title: ERC-725 Smart Contract Based Account
author: Fabian Vogelsteller <fabian@lukso.network>, Tyler Yasaka (@tyleryasaka)
discussions-to: https://github.com/ethereum/EIPs/issues/725
status: Draft
type: Standards Track
category: ERC
requires: ERC165, ERC173, ERC1271 (optional)
created: 2017-10-02
updated: 2020-07-02
```

This is the new 725 v2 standard, that is radically different from **ERC 725 v1**. ERC 725 v1 is be moved to **#734** as a new key manager standard.

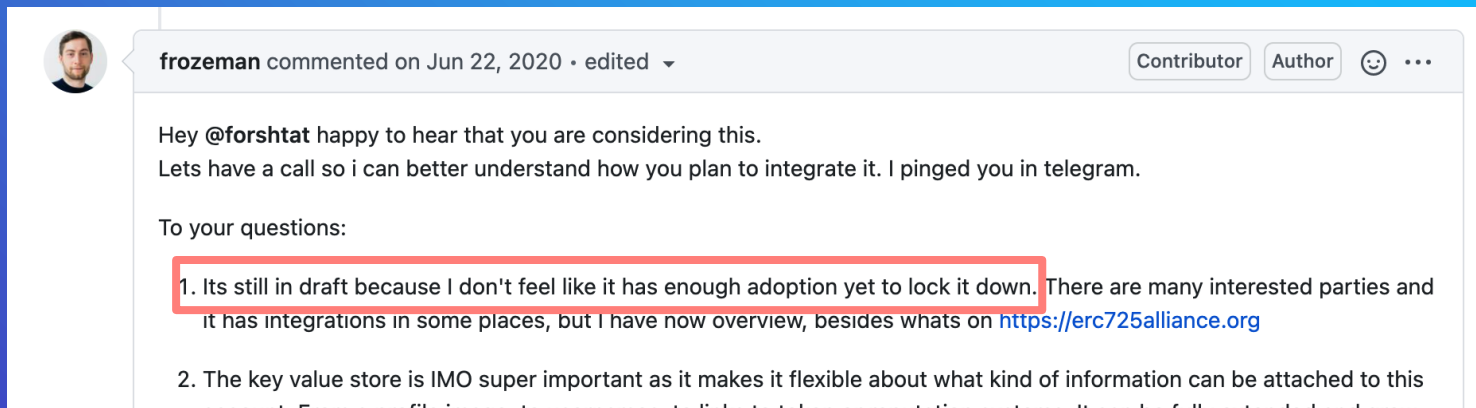
Simple Summary

<https://github.com/ethereum/EIPs/issues/725>

# | ERC725の現状と課題

1. Fabian自身がDraftに満足していない
2. LUKSOあつてのERC725
3. メタトランザクションが難しい（拡張は可能か？）

# | Fabian自身がDraftに満足していない



- 一方で、大枠は固まったとしている。
- npmでERC725のパッケージが公開(2020.11月) (ベータ版)
- 上記がLUKSOのテスト版でも使われている(LUKSOのgitリポジトリ)

# | LUKSOあつてのERC725

## LUKSO

LUKSO . . . 消費財（物理的なもの・デジタルのもの両方）の  
透明性を高めるための標準・解決策を提供する  
ブロックチェーン・インフラ（売買プラットフォーム）

# About LUKSO

LUKSO The Blockchain for new digital lifestyle is created by former Ethereum Developer Fabian Vogelsteller, author of ERC20 and web3.js - both of which are the foundation for today's #DeFi protocols. Together with brand architect Marjorie Hernandez, he is building the platform for the next wave of mainstream Blockchain applications.

## The Founders



Fabian Vogelsteller



Marjorie Hernandez

## The Advisors

<https://lukso.network/about>

*All members of the advisory board are acting on their own behalf and not in the name of their companies.*



**Daniel Heaf**

Nike

Vice President Digital

[Linkedin](#)



**Dr. Berndt Hauptkorn**

CHANEL

President of Europe

[Linkedin](#)



**Eric Pfrunder**

Former Artistic Director of  
Fashion Image at CHANEL

[Say Who](#)



**Rajeev Aikkara**

Burberry

Vice President -  
Digital Technology

[Linkedin](#)



# メタトランザクションが難しい (拡張は可能か?)

- GSN (Gas Station Network) では `msg.sender` ではなく20バイトの `msg.data` という変数が、証明された sender アドレスとして扱われる。
- しかし、ERC725で `execute` や `setData` を実行できるのは `msg.sender` だけの作りになっている。



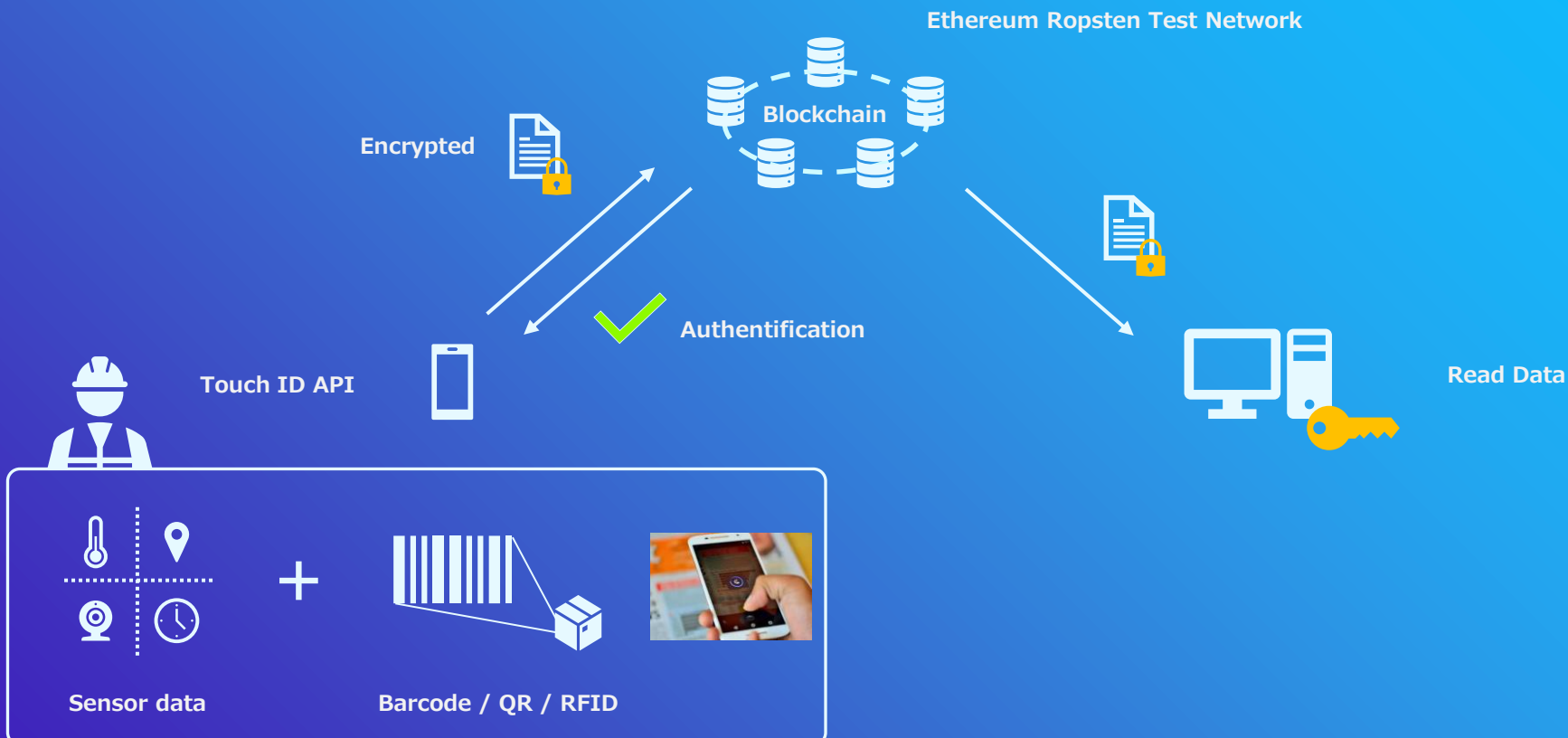
# | ERC725の変遷とこれから

1. ERC725の現状

2. ERC725の課題に関する考察

3. IoT領域における応用可能性について

# IoT領域への応用



## 品質検査の認証とトラッキング

## 検査のコストと不正リスク②

品質・検査偽装の発生原因として

「収益追求・コスト削減」を挙げた企業が最も多く  
また最大のリスクとして「取引先の信頼失墜による  
売り上げの減少」を挙げた企業が多かった。

不正対応においてAI（人工知能）を活用することが期待されているものの、現時点で実際に活用されている事例は少ない。

KPMGの調査（2019年）で不正予防・発見のためにAIの活用が「有効」と回答した企業が約半数を占めた。一方、AIの不正対応分野における有効性を「不明」と回答した企業も4割程度あった。これは現時点では具体的なAIの活用事例が乏しい状況にあるためと考えられ、実際に不正対策としてAIを導入済みの企業は2%にとどまった。

収益追求・コスト削減が優先され、  
品質保証の確保が後回しになっていた

58%



### 製造業の品質・検査偽装がもたらす最大のリスク



<https://home.kpmg/jp/ja/home/insights/2019/03/fraud-survey-6.html>

# 課題

## 無資格検査の発覚が続く航空機部品業界

ジャムコは2019年3月26日、航空機内装品を製造する事業において不適切な検査が行われていたと発表した。また同社と製造子会社の宮崎ジャムコの2社で判明し、無資格者による検査や受入検査の未実施があった。

ブロックチェーンが保証するのは、あくまでもブロックチェーンに登録された情報入力された情報自体が間違っていれば、元も子もない

そして現在はデータの中継者となる「人間の公正性（データを正しく入力したか）」を客観的に担保する仕組みがなく、その確認作業も人間が実施している。

[https://monoist.atmarkit.co.jp/mn/articles/1903/29/news010\\_2.html](https://monoist.atmarkit.co.jp/mn/articles/1903/29/news010_2.html)

製造マネジメントニュース：

### 航空機部品業界にも検査不正の波、ジャムコがシートなど不適切検査

🕒 2019年03月27日 09時00分 公開

[松本貴志, MONOist]



<https://monoist.atmarkit.co.jp/mn/articles/1903/27/news045.html>

# 製造業の「検査」に着目しトラッキングを行う

部品検査・品質検査は、各事業所間で繰り返し行われる。

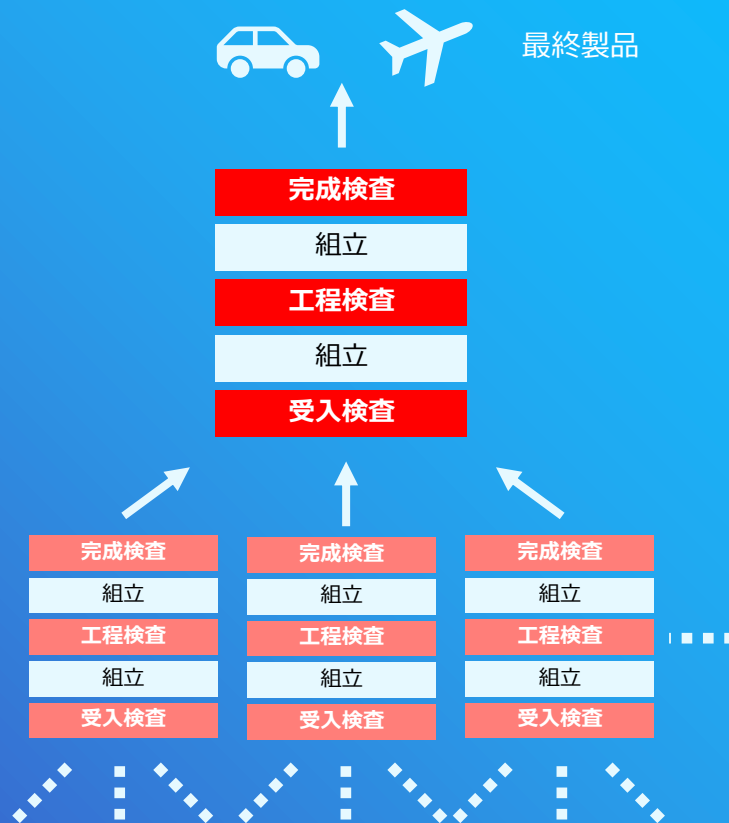
## 1. 繰り返し検査が必要

→ コスト削減の余地あり

## 2. 検査済を保証する仕組みや規格が不足

## 3. 人の手による検査で不正が起きやすい

## 4. 検査漏れの情報が上にあがりにくい



# | ありがとうございました

