

ブロックチェーンを用いた 分散型認証基盤

2020年11月

名古屋工業大学 情報工学専攻

ネットワーク分野

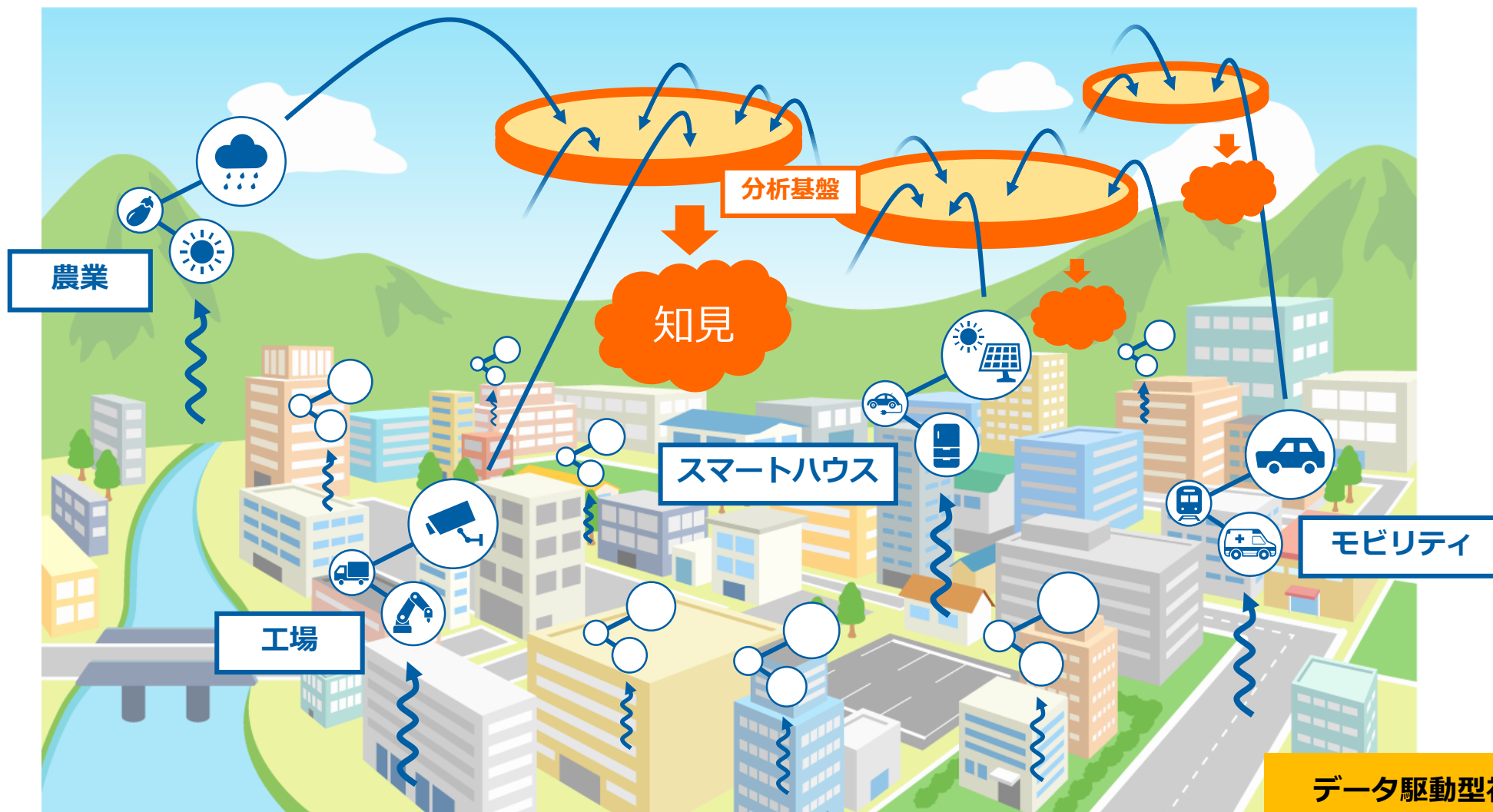
助教 掛井 将平

ビッグデータは社会を映す鏡



IoTにより多種多様なデータが時々刻々と生成されている

ビッグデータは社会を映す鏡

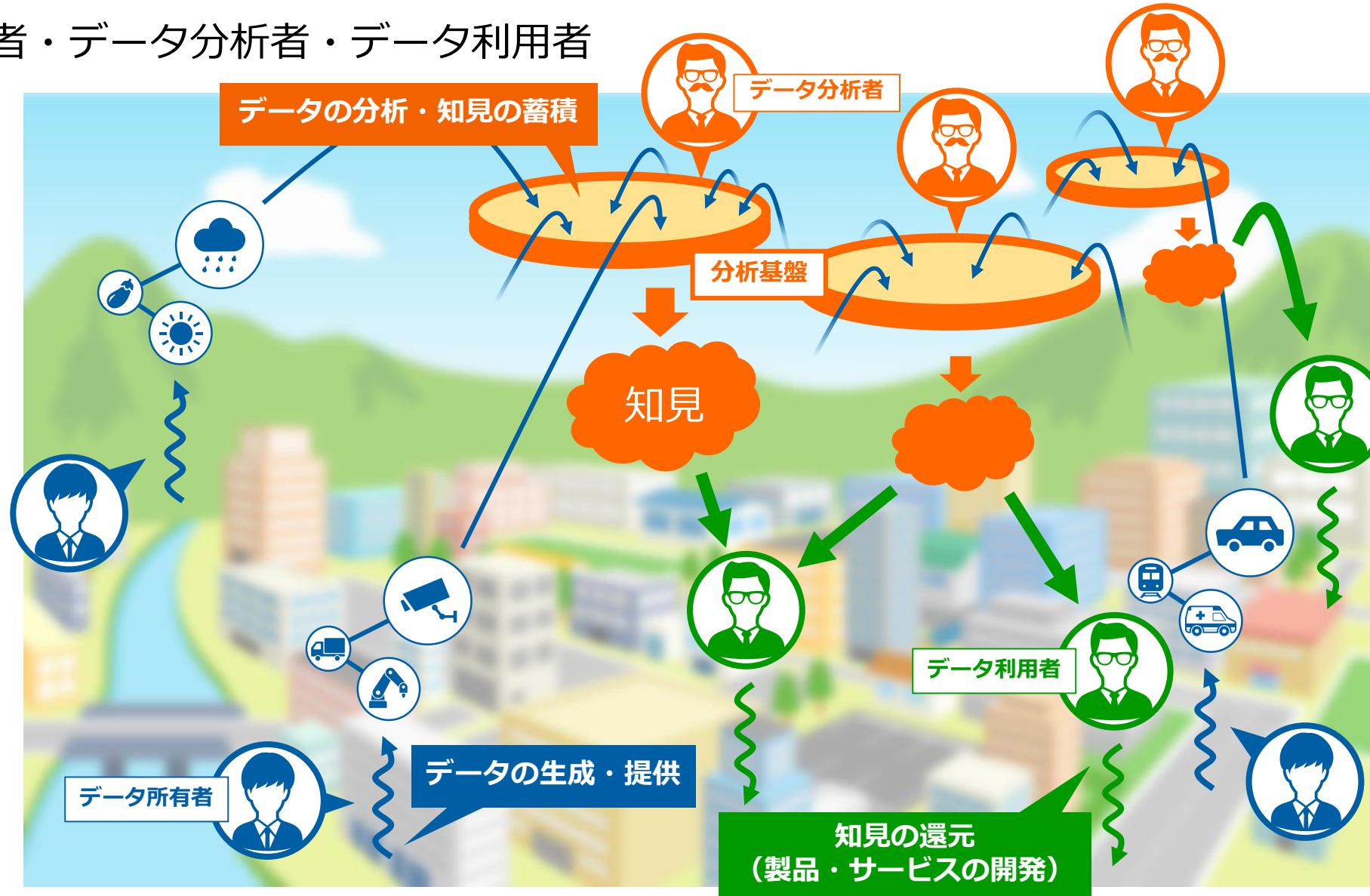


データを組み合わせて分析することで
社会の状況をより詳しく知ることができる

▶ 新たな知見の発見

データ駆動型社会を進める3つの主体

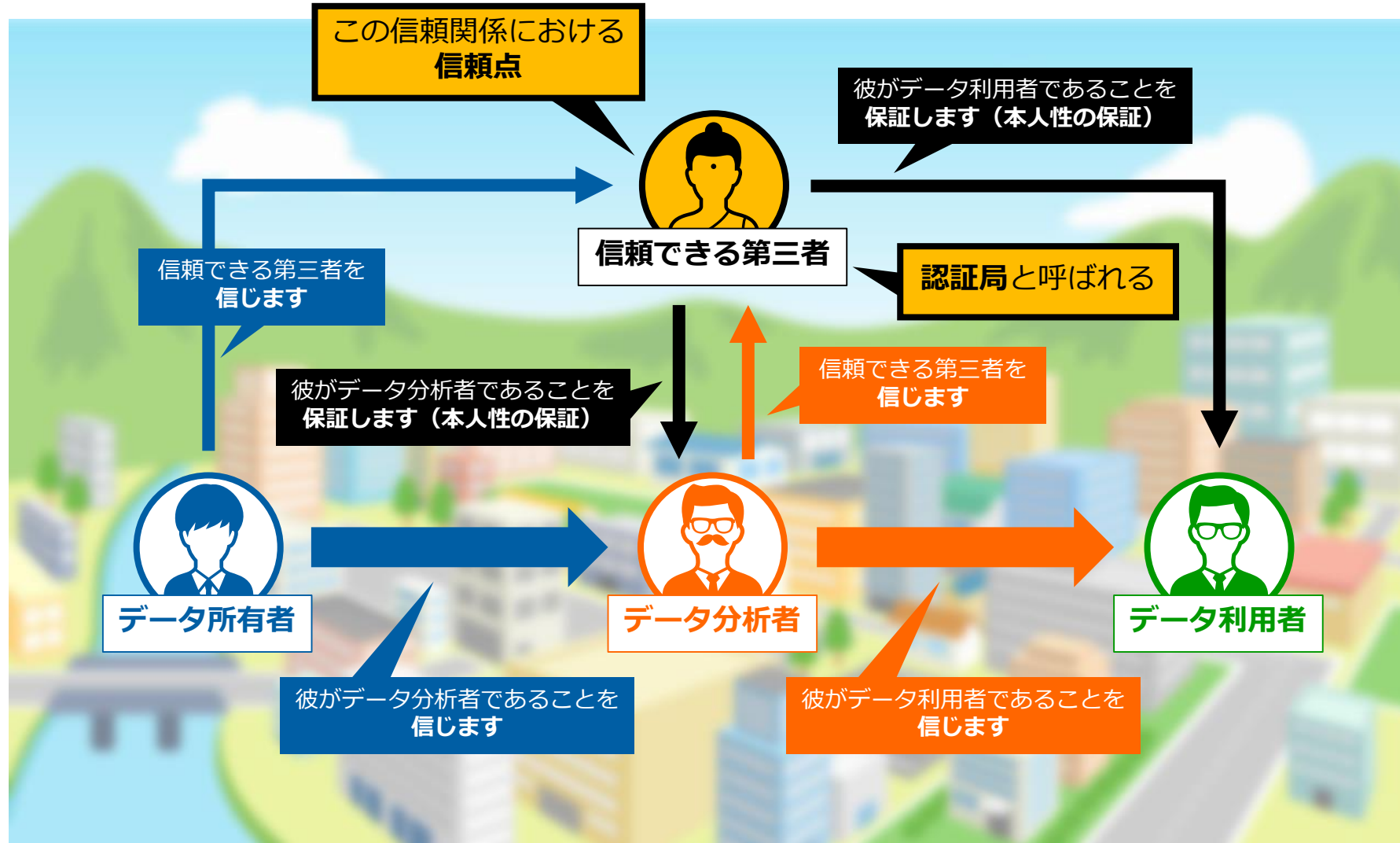
データ所有者・データ分析者・データ利用者



データ所有者・データ分析者・データ利用者の3者の連携が必要不可欠
→ どのようにお互いを信頼し合うか？

信頼できる第三者による信頼関係の橋渡し

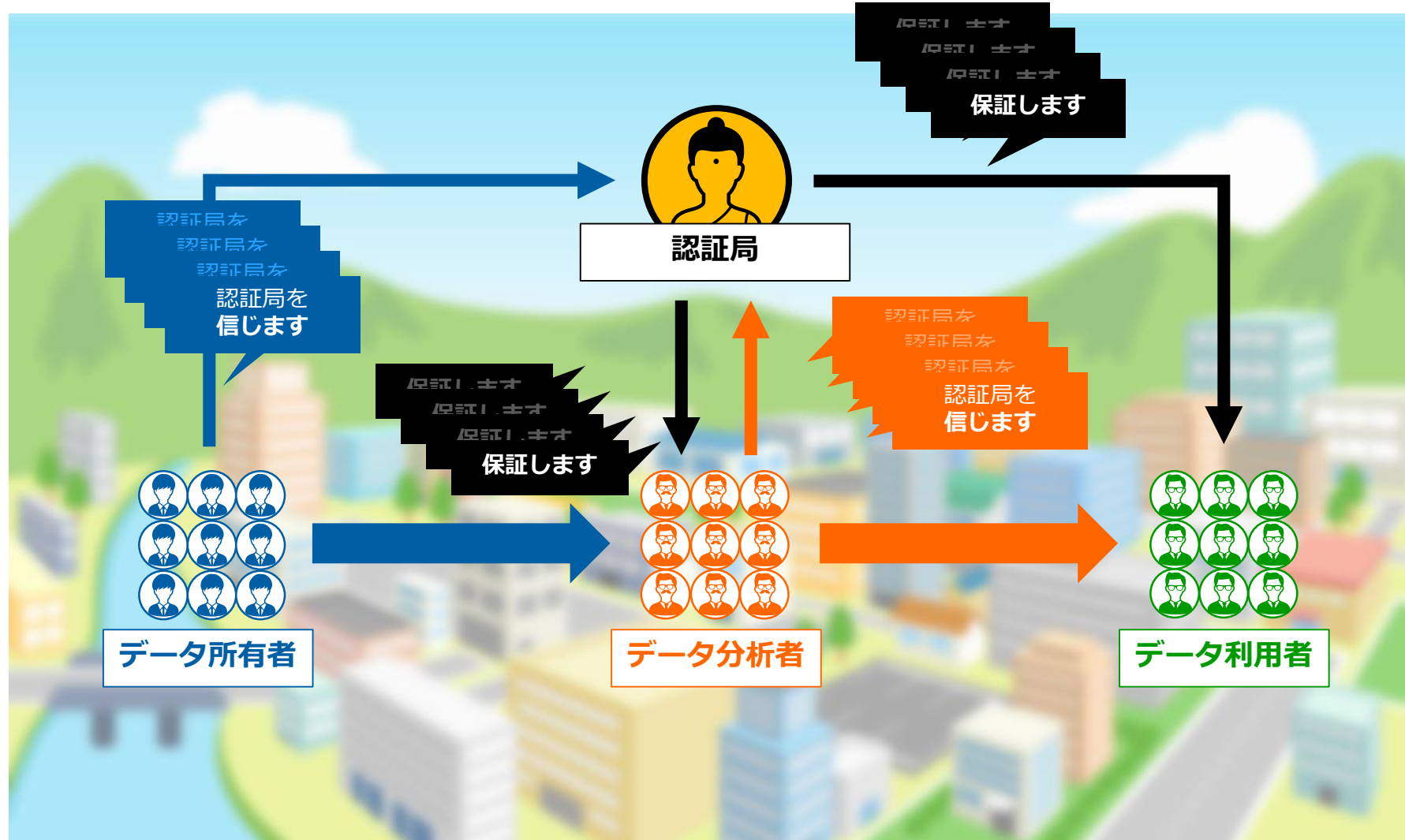
既存の公開鍵基盤の例



お互いに面識が無くとも，信頼できる第三者を信頼点として相手の本人性を確認することができる

信頼できる第三者による信頼関係の橋渡し

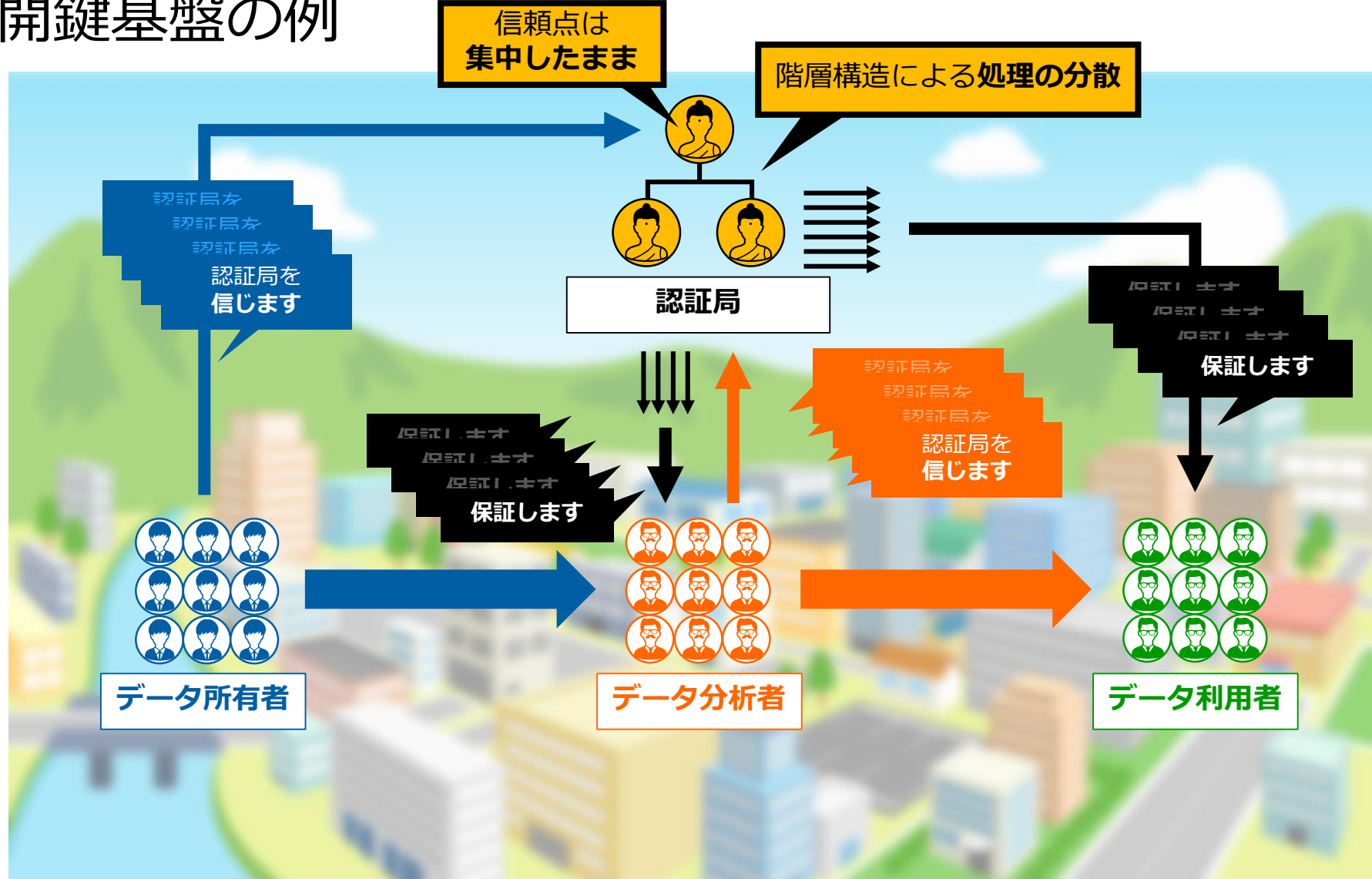
既存の公開鍵基盤の例



信頼関係の橋渡しをすればするほど、
信頼できる第三者による本人性保証の処理の負担が増加

信頼できる第三者による信頼関係の橋渡し

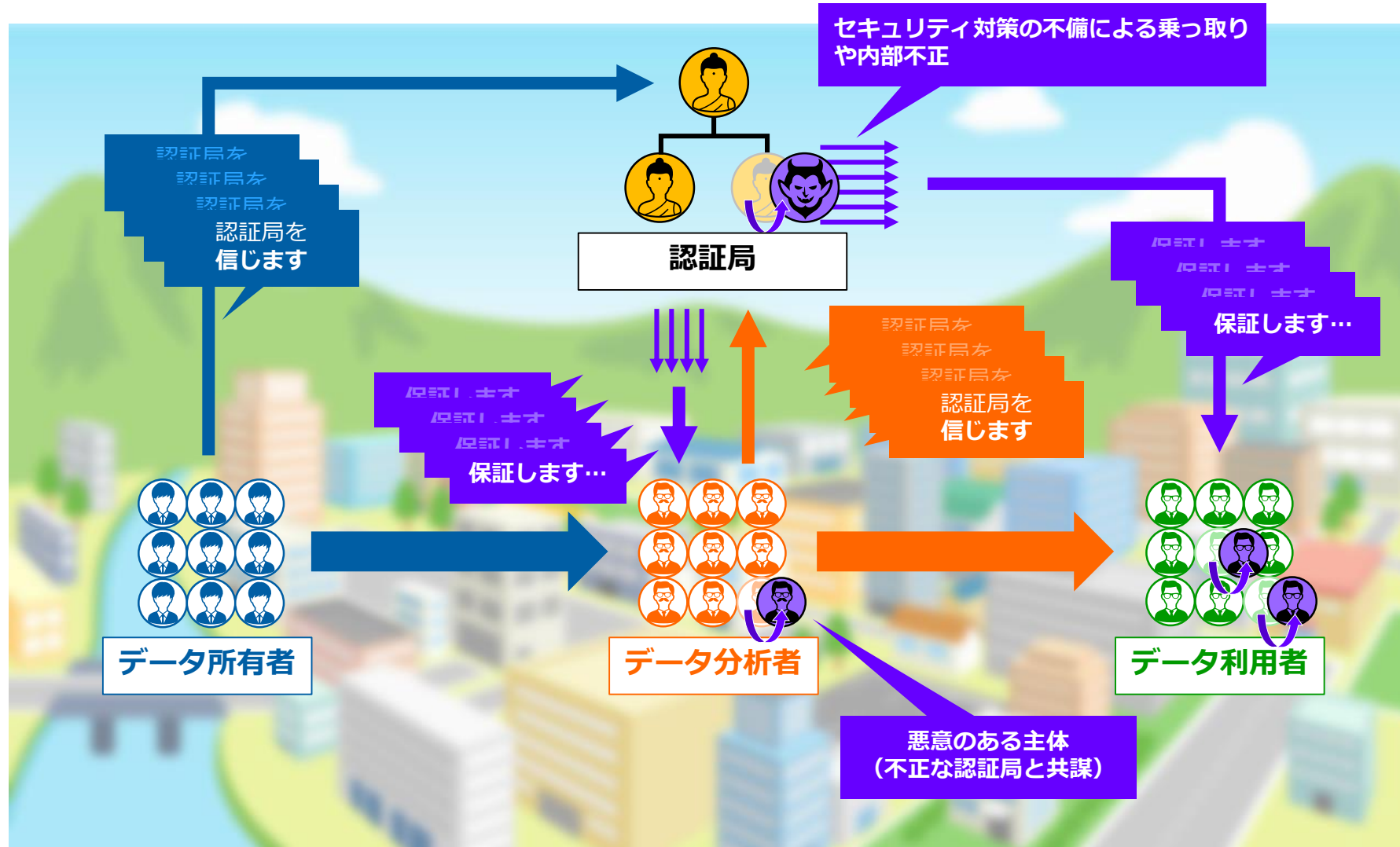
既存の公開鍵基盤の例



本人性の保証を下位の認証局に委任
→ 本人性保証の処理負荷が分散される

信頼できる第三者による信頼関係の橋渡し

本研究における問題意識

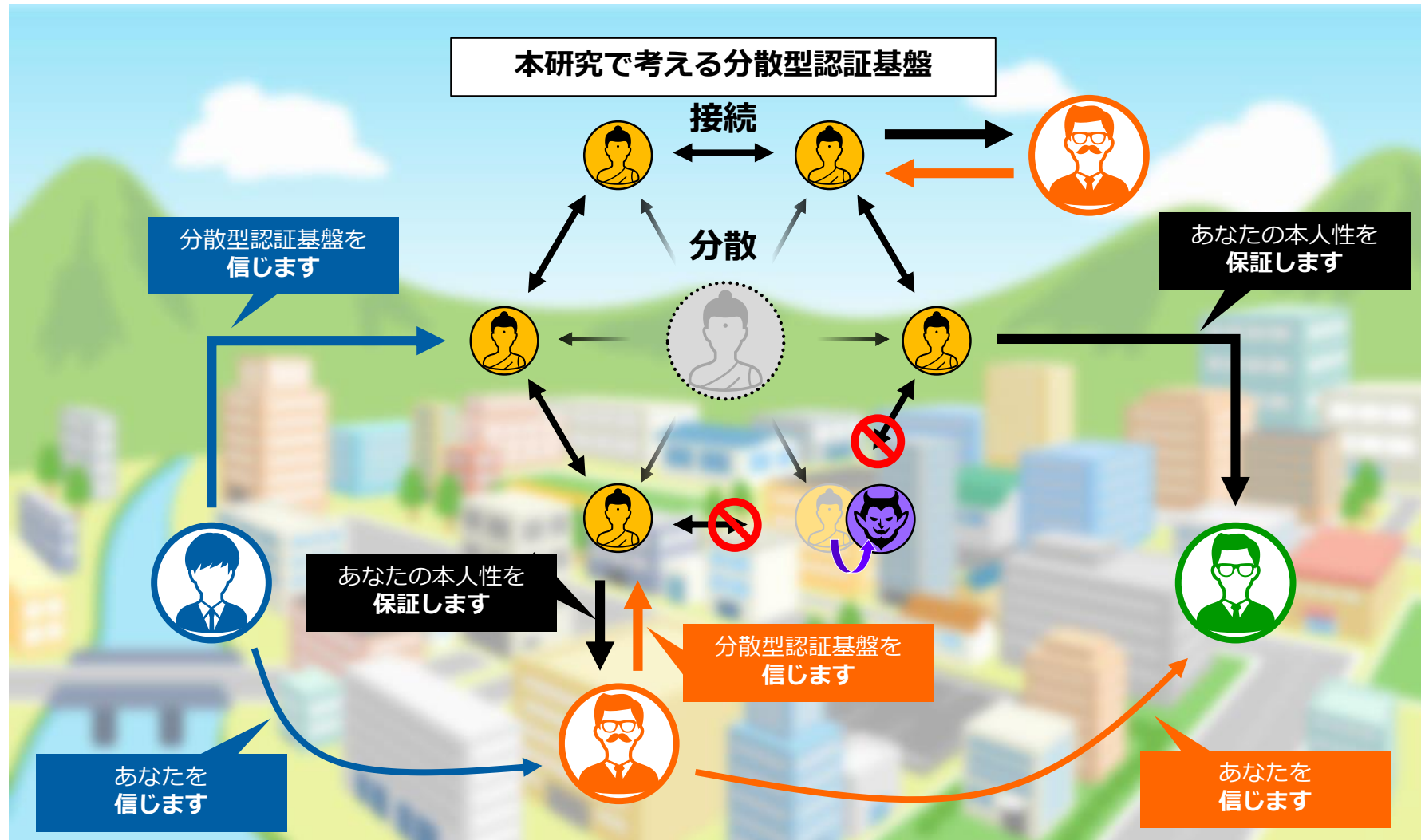


処理を委任することで
不正を行う認証局の存在のリスクが増加

悪意のある主体が信頼関係
に入り込む

分散型認証基盤による信頼関係の橋渡し

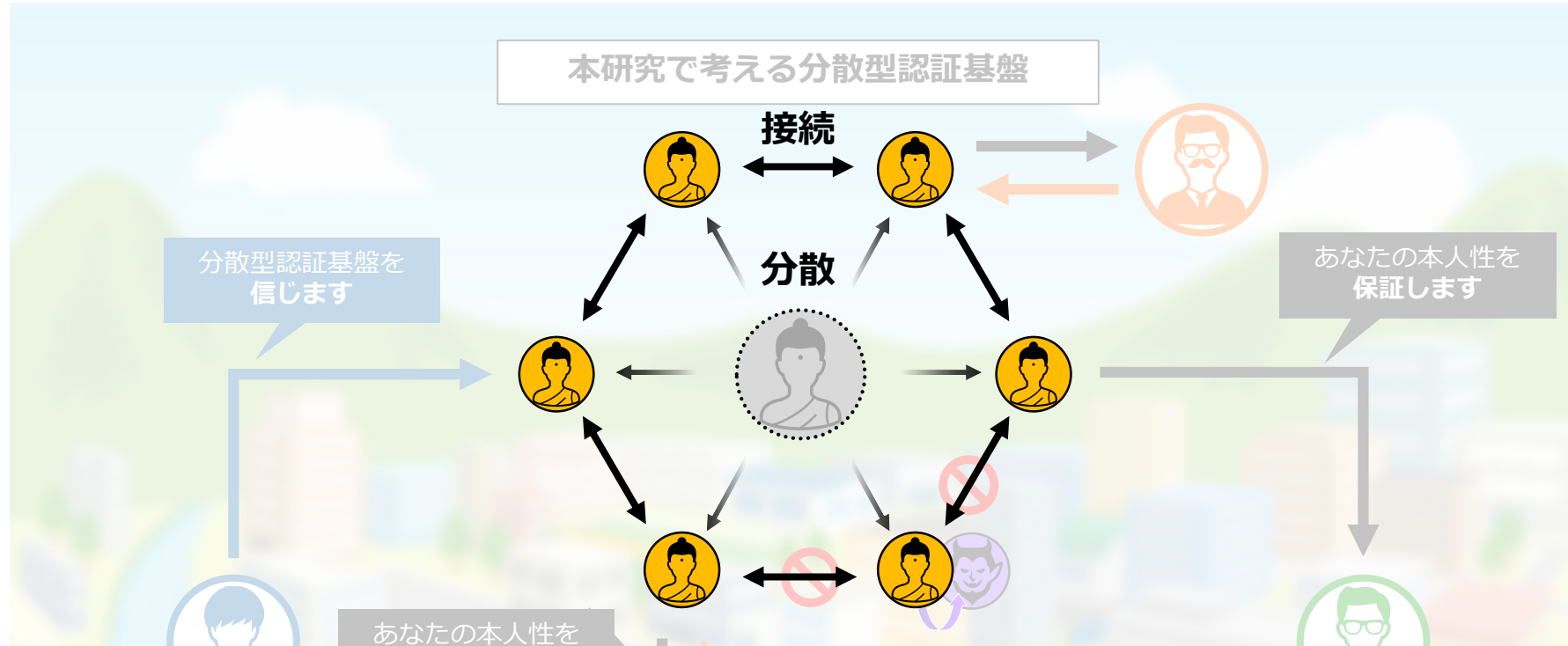
本研究の目標



認証局の信頼点を分散しつつ、統一された評価手法に基づいて
信頼点を相互に接続するシステムの開発

分散型認証基盤による信頼関係の橋渡し

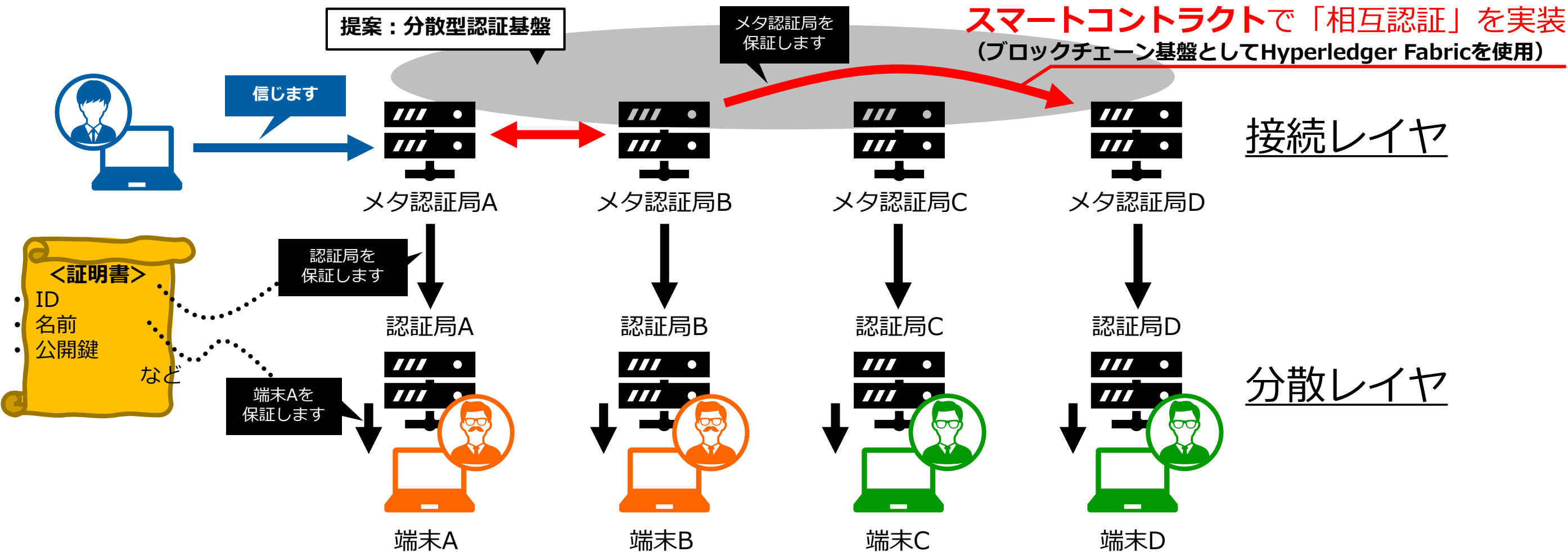
本研究の目標



★本研究の新規なところ

認証局を相互に接続（相互認証）する仕組みはあるが、各認証局の独自の基準で実施するしかなかった → 現実的に利用できるシチュエーションが限られていた
本研究では、ブロックチェーンを利用することで、同一の基準で相互認証できる枠組みを示した → 相互認証のより汎用的な利用が期待できる

単一の信頼点を分散させるのではなく、 多数の信頼点が分散・相互接続する分散型認証基盤の提案

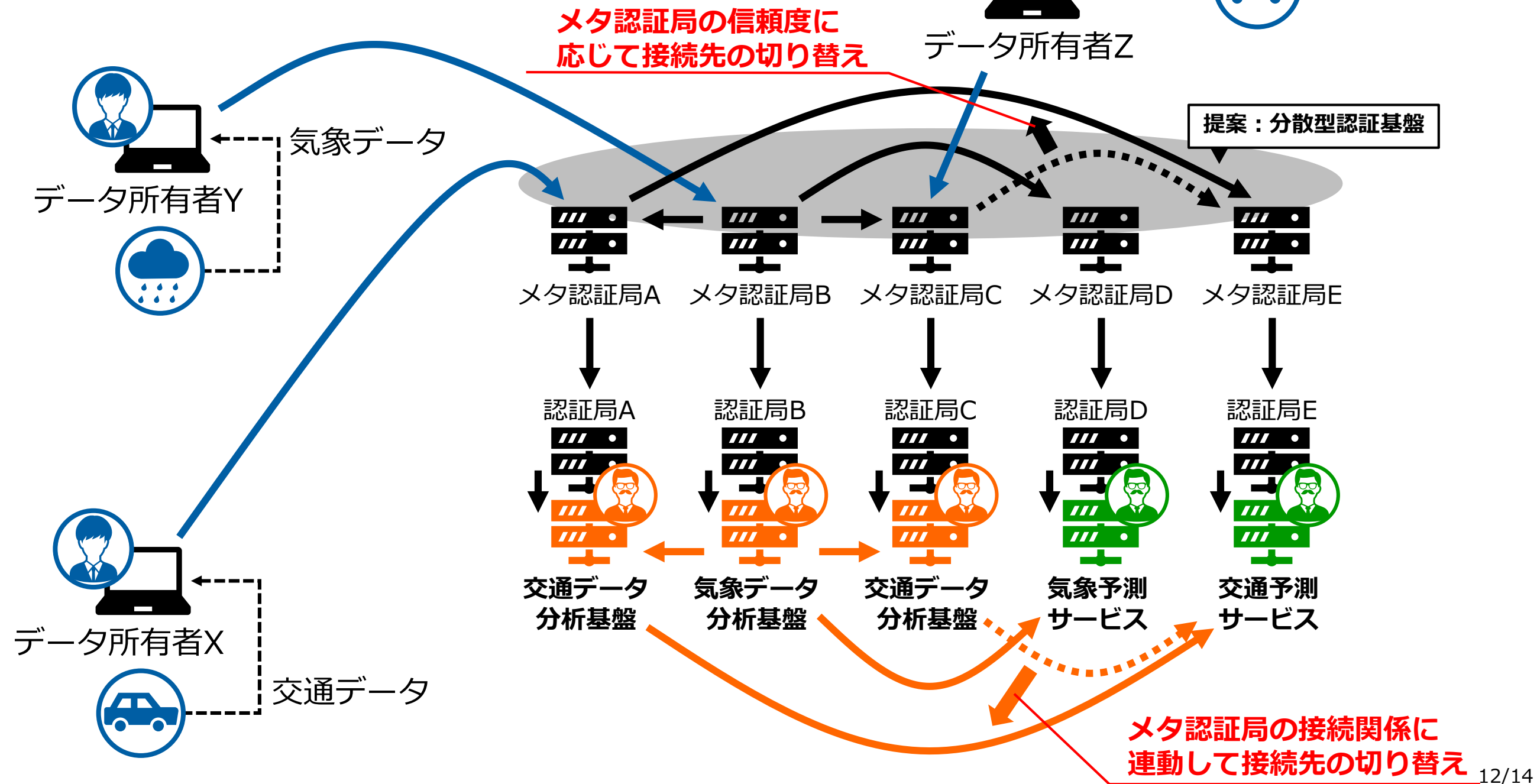


相互認証に関わる処理をスマートコントラクトで実装

→ ブロックチェーン上で証明書の発行履歴を公開 (透明性)

→ 認証局を二層構造にすることで、端末利用者の個人情報公開されることを防ぐ

実用化のイメージ



実用化に向けた課題

★現状

Hyperledger Fabricを用いた実装・
概念実証

→ 静的なパラメータに基づいたメタ
認証局の相互接続

★今後

評価指標のさらなる検討

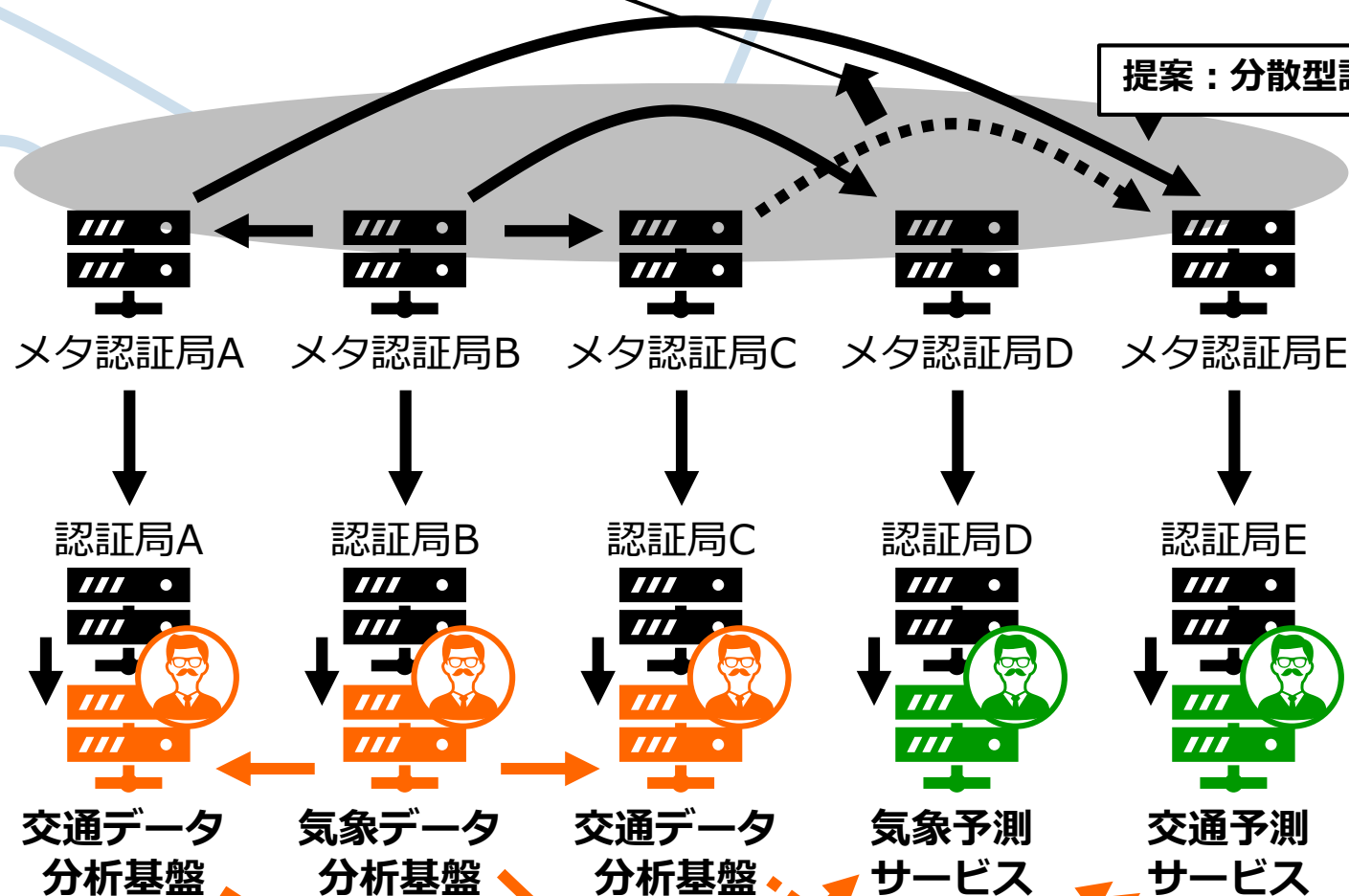
メタ認証局の信頼度を動的に測る手法
の検討

メタ認証局の信頼度
に応じて接続先の切り替え

データ所有者Z

交通
データ

提案：分散型認証基盤



メタ認証局の接続関係に
連動して接続先の切り替え

求める連携先とメッセージ

- 今後の検討について、以下の二点が重要な要素
 - － ①提案基盤を適用する領域に特化した指標の検討
 - － ②認証局の運用方法とセキュリティ侵害の関連の調査
- データ収集の仕組みをお持ちの企業（①）、認証局の運用に関する知見をお持ちの企業（②）の力をお借りしたい

データ収集基盤と分析基盤，データ利用者をその信頼度に応じて緩やかに接続できる仕組みを確立することが本研究の目的である。データから真に新たな知見を得るには，真に雑多なデータの収集が必要であり，そのためには，三者の独立性が重要である。この三者の安全な連携を支える基盤を考案することでデータ駆動型社会に貢献したい。



本技術に関する情報

試作品の状況

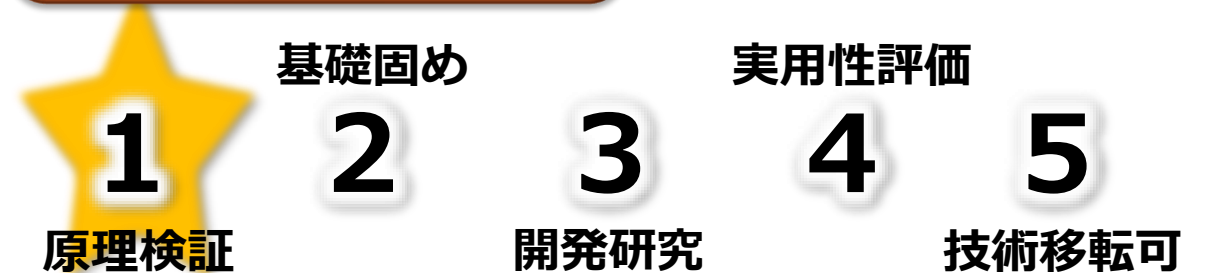
無し

※提供の際は諸手続が必要となるため、問合せ先までご連絡願います。

文献・特許の情報

- Shohei Kakei, Yoshiaki Shiraishi, Masami Mohri, Toru Nakamura, Masayuki Hashimoto and Shoichi Saito, "Cross-Certification Towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric," in IEEE Access, vol. 8, pp. 135742-135757, 2020, doi: 10.1109/ACCESS.2020.3011137. 著者名, 雑誌名, vol., page (発行西暦年)

研究フェーズ



【お問合せ】

名古屋工業大学 産学官金連携機構

〒466-8555 名古屋市昭和区御器所町字木市29番

TEL:052-735-5627 FAX:052-735-5542

E-mail: nitfair@adm.nitech.ac.jp

URL: <https://technofair.web.nitech.ac.jp/>