国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

高度通信・放送研究開発委託研究

課題 241
高信頼データ流通のための非集中型ネットワーク内ストレージ及びアプリケーションの研究開発

2024年11月12日

国立研究開発法人情報通信研究機構（NICT）
ネットワーク研究所　ネットワークアーキテクチャ研究室

＜ 本件に関する問合せ先 ＞公募担当　E-mail: info-itaku@ml.nict.go.jp

概要

高信頼データ流通のための非集中型ネットワーク内ストレージ及びアプリケーションの研究開発

背景と課題

将来のデータ駆動型社会では膨大な分散データをデータの所有者が管理し、連携させる**自律分散型のデータ流通アーキテクチャ**が必要となる。このアーキテクチャのもとデータの真正性や可用性を向上させるため、ブロックチェーンに代表される分散台帳技術の研究開発が盛んである。ブロックチェーンは、オフチェーンストレージと組み合わせることで大容量のデータを共有可能であるが、既存のオフチェーンストレージは**機密・プライバシーの保護やデータ流通範囲の制限、データアクセス効率の観点で課題**があり、アプリケーション展開上の障壁となっている。

研究開発の目的

当機構では、非集中型データストレージIPFS(InterPlanetary File System)と、属性に基づく暗号処理技術、ICN (Information-Centric Network)技術を組み合わせ、既存オフチェーンストレージの課題を解決する「**NICTセキュアオフチェーンストレージ**」の研究開発を行っている。本研究では、ブロックチェーンとNICTセキュアオフチェーンストレージを用いる**高信頼・高効率の非集中型ネットワーク内ストレージフレームワークを設計・実装し、アプリケーション実証**により有効性を示す。

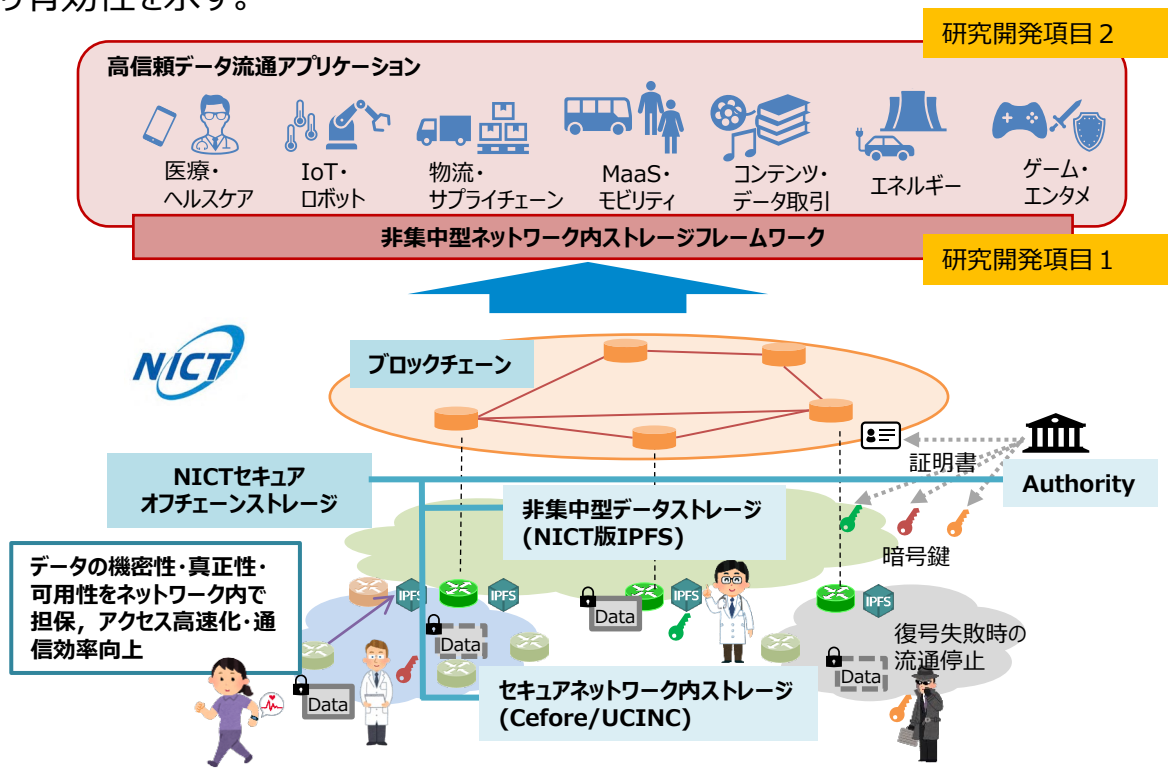
研究開発の内容

研究開発項目１　非集中型ネットワーク内ストレージフレームワークの研究開発

ブロックチェーン、および、NICTセキュアオフチェーンストレージを活用して、高信頼かつ高効率なデータ流通アプリケーションを実現する上で必要な機能（ブロックチェーン上のスマートコントラクトを含む）を、非集中型ネットワーク内ストレージフレームワークとして設計・実装する研究開発を行う。既存アプリケーションやデータ基盤との互換性、法令等との親和性を確保しつつ、アプリケーション共通の基盤となるソフトウェアフレームワークとして設計・実装する 。

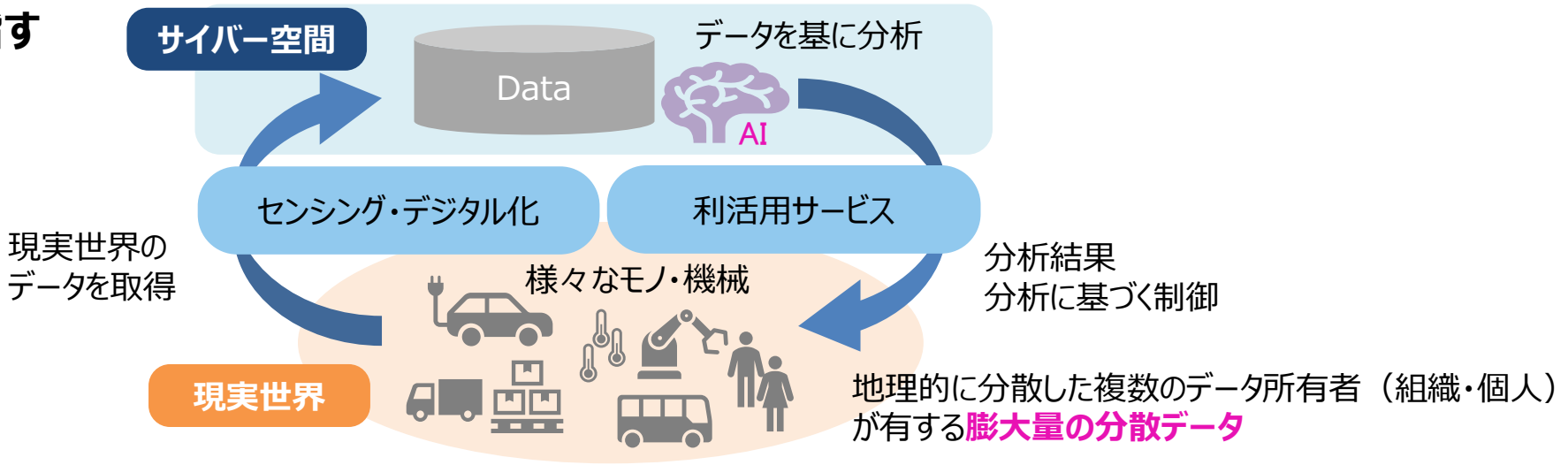
研究開発項目２　高信頼データ流通アプリケーションの研究開発

研究開発項目１の非集中型ネットワーク内ストレージフレームワークを用いたアプリケーション実証を行う。ブロックチェーン、および、オフチェーンストレージを組み合わせたデータ流通が有効となるアプリケーションを一つ以上選択し、動作を実証する。

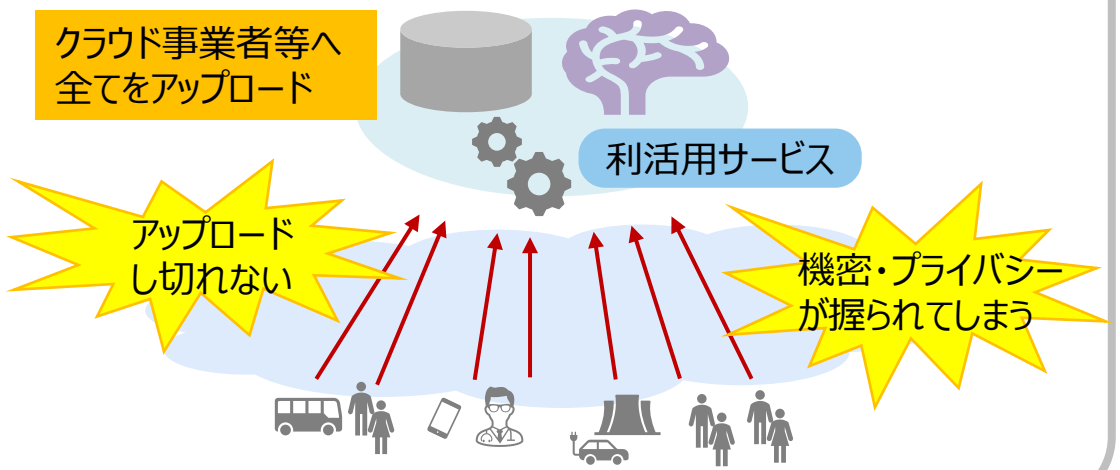


背景

Society5.0が目指すデータ駆動型社会

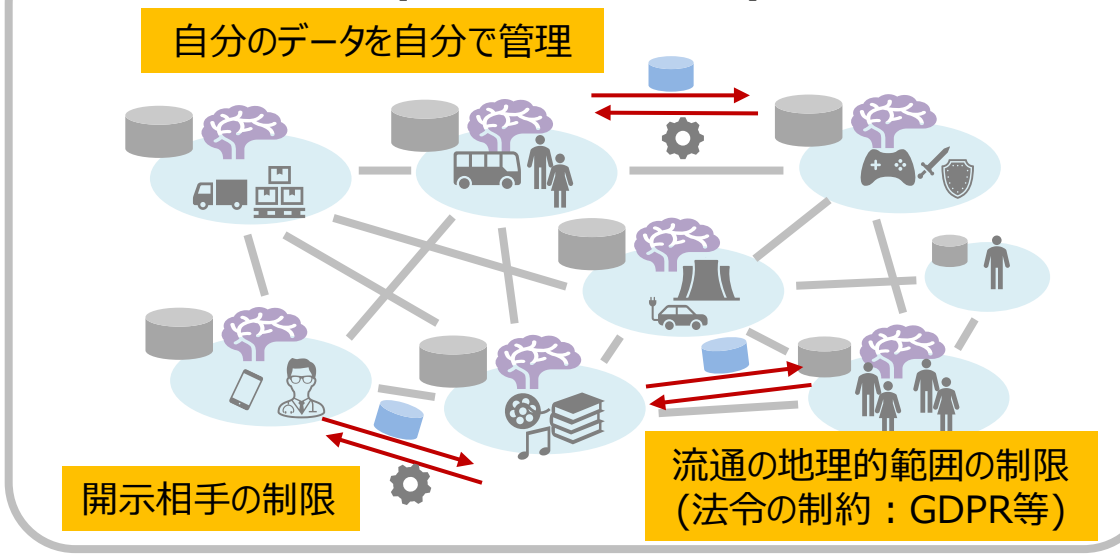


従来のクラウド中心アーキテクチャ（データ総取得型プラットフォームビジネス）



将来の方向性

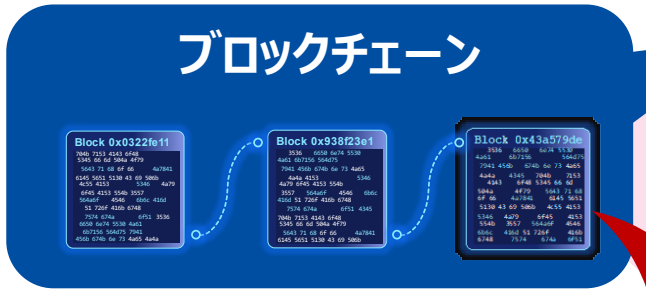
「自律分散型」のデータ流通アーキテクチャ（本委託研究の想定）



ブロックチェーンとオフチェーンストレージ

分散台帳（ブロックチェーン）により「自律分散型」アーキテクチャにおける非改ざん性・真正性を担保

- 非中央集権型
- 検証可能な記録（書き換え不能）
- 検証可能なコード実行
- 組織ではなくシステムを信頼



ブロックチェーンネットワーク

- データが拡散される
- ストレージコスト大

オフチェーンストレージ

ブロックチェーンにはデータのポインタ(ハッシュ値)を保存、データ本体はブロックチェーンと連動した**ブロックチェーン外のストレージ（オフチェーンストレージ）**で管理・流通

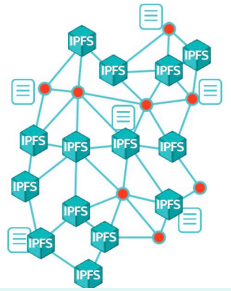
オフチェーンストレージネットワーク

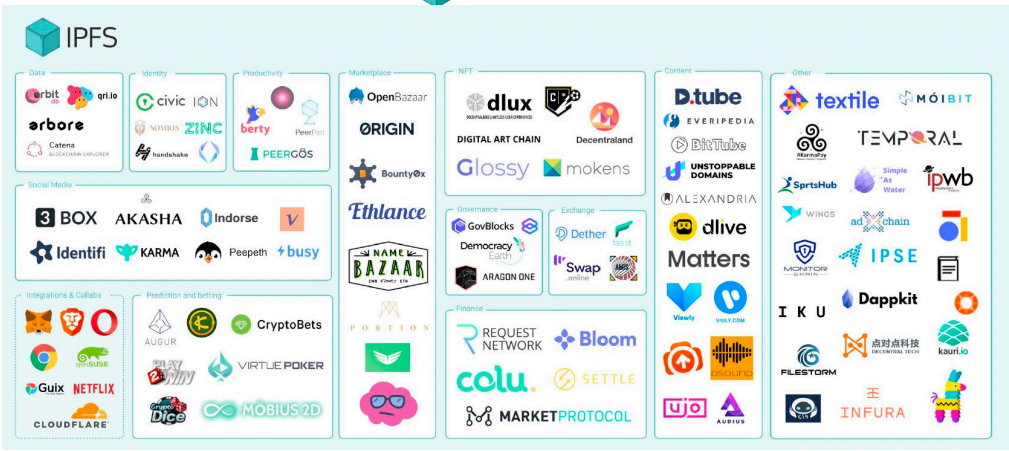
- データの制御可能
- ストレージコスト削減

関連動向

ブロックチェーン関連の技術の進展にともない、分散型・非集中型のシステム構成によるデータ連携技術に対する注目が高まっており、いずれの国においても技術の主導権を握るべく研究開発が盛ん。オフチェーンストレージとしてはIPFSがデファクト標準的に用いられている。

- **オフチェーンストレージの実装・実現方式**
  - IPFS (Inter-Planetary File System) [Trautwein 2022]
  - ヘルスケア向け適用手法 [Esposito 2018]
  - 識別子管理手法 [Shuaib 2023]
  - アクセス制御方法 [Ugobane 2018]
- **IPFS関連研究**
  - 効率的なストレージ構成方法 [Chen 2017]
  - Webアプリケーションとしての性能向上方法 [Le 2021]
- **分野横断データ連携プラットフォーム**
  - EU Horizon Europe TRUSTEE プロジェクト（2022-）





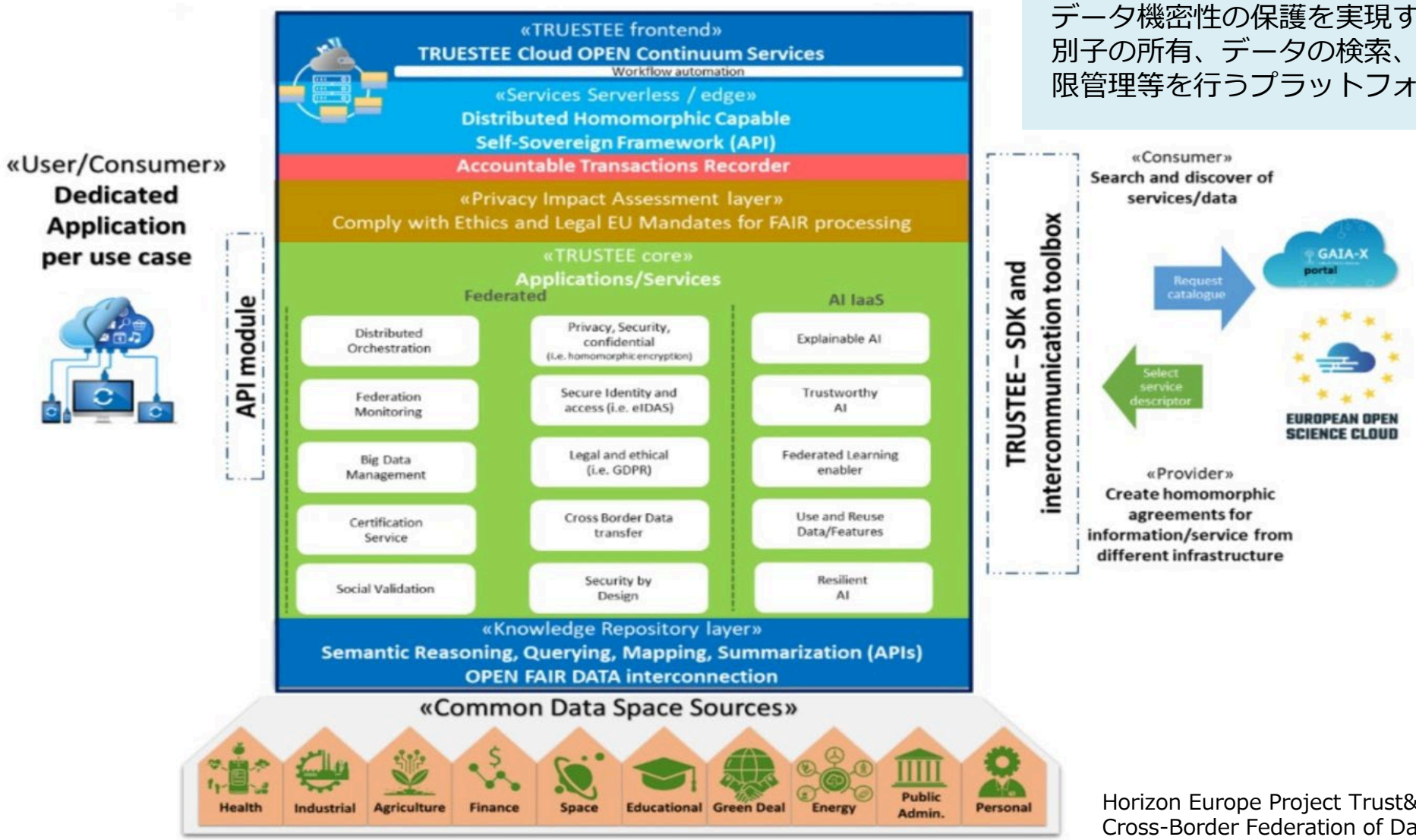
IPFSの課題
- 機密保持・流通範囲の制限は不可：全てオープン前提
- 遅延が大きい： データ取得時の問い合わせ先多数
- 攻撃耐性が低い： Eclipse Attack に対する脆弱性

未解決

参考：TRUSTEE

ブロックチェーンと準同型暗号を使用してデータの自己主権とデータ機密性の保護を実現するプロジェクト。ユーザによる識別子の所有、データの検索、情報の選択的な開示、ユーザの権限管理等を行うプラットフォームの実現を目指している。

TRUSTEE



Horizon Europe Project Trust&Privacy Preserving Computing Platform for Cross-Border Federation of Data (TRUSTEE), (GA 101070214).

本委託研究の目的

目的

機密・プライバシーの保護、データ流通の地理的範囲を制限する機能を有する**信頼性の高い非集中型ネットワーク内ストレージを世界に先駆けて実装、アプリケーション実証**を行う

IPFSの課題

- 機密保持・流通範囲の制限は不可
  - 全てオープン前提
- 遅延が大きい
  - データ取得時の問い合わせ先多数
- 攻撃耐性が低い
  - Eclipse Attack に対する脆弱性

未解決

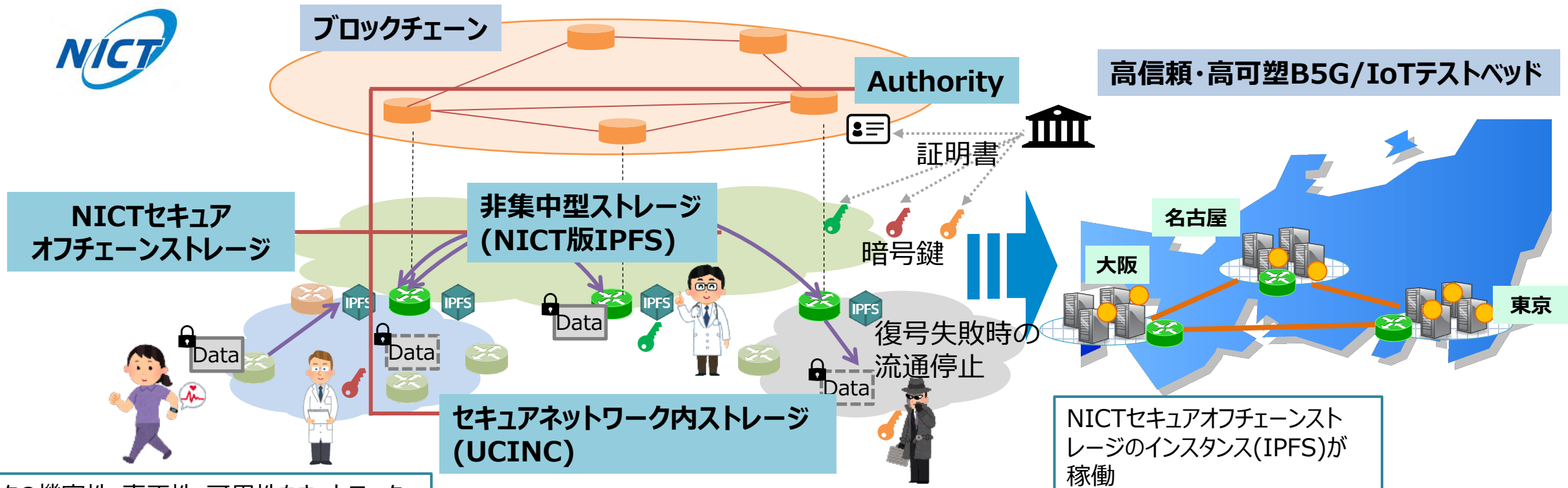
本研究の前提

「**NICTセキュアオフチェーンストレージ**」
IPFS + ICN + CP-ABE

- 属性（「医師」「NICT職員」等)に応じた暗号化
- データ流通をネットワークレベルで制御
- ネットワーク内キャッシュ活用等による低遅延化
- Eclipse Attack耐性が高いネットワーク構成方式

NICTセキュアオフチェーンストレージ

NICTが保有するであるセキュアネットワーク内ストレージ機能、オフチェーンストレージネットワーク構成方式を実装した**非集中型データストレージ(IPFS)、セキュアネットワーク内ストレージ(UCINC)**（後述）を含むNICT独自のセキュアなオフチェーンストレージ。高信頼・高可塑B5G/IoTテストベッド上で2025 1Qより稼働予定。



本委託研究の研究開発項目

研究開発項目１　非集中型ネットワーク内ストレージフレームワークの研究開発

研究開発項目２にて実証するアプリケーションで活用可能とする非集中型ネットワーク内ストレージのフレームワークを研究開発する。**ブロックチェーン、および、NICTセキュアオフチェーンストレージを活用**し、高信頼かつ高効率なデータ流通アプリケーションを実現する上で必要な機能（ブロックチェーン上のスマートコントラクトを含む）を、**ソフトウェアフレームワークとして設計・実装**する研究開発を行う。

研究開発項目２　高信頼データ流通アプリケーションの研究開発

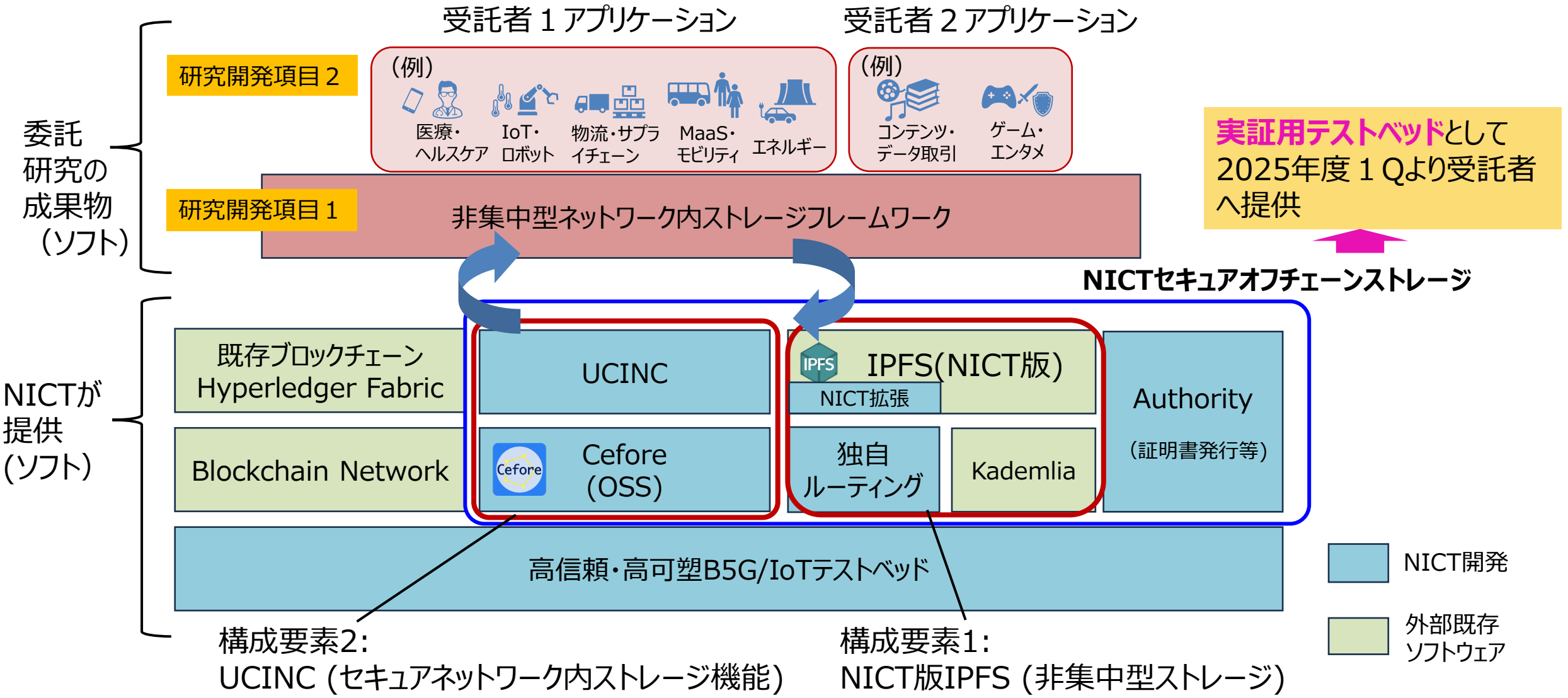
研究開発項目１の非集中型ネットワーク内ストレージフレームワークを用いて、**具体的なアプリケーションを実装し、実証**を行う。受託者は、ブロックチェーン、および、オフチェーンストレージを組み合わせたデータ流通が有効となるアプリケーションを一つ以上選択し、動作を実証する。[…] **受託者が既に有している、あるいは、既存のアプリケーションを改造しても良い。**

チャレンジングな要素

- 安全性・プライバシーを維持する計算処理方法
  アプリケーションがNICTセキュアオフチェーンストレージから取得するデータの安全性、プライバシーを維持しつつ、アプリケーション固有の計算処理を実行する方法
- 性能の確保
  NICTセキュアオフチェーンストレージが有するキャッシュ機能等の利点を活かし、高い応答性能やスループットを実現可能とするアプリケーションデータ制御（検索、処理、送受信などを含む）方法

既存アプリケーションやデータ基盤との互換性、法令等との適合性を確保しつつ、アプリケーション共通の基盤となるソフトウェアフレームワークとして設計・実装

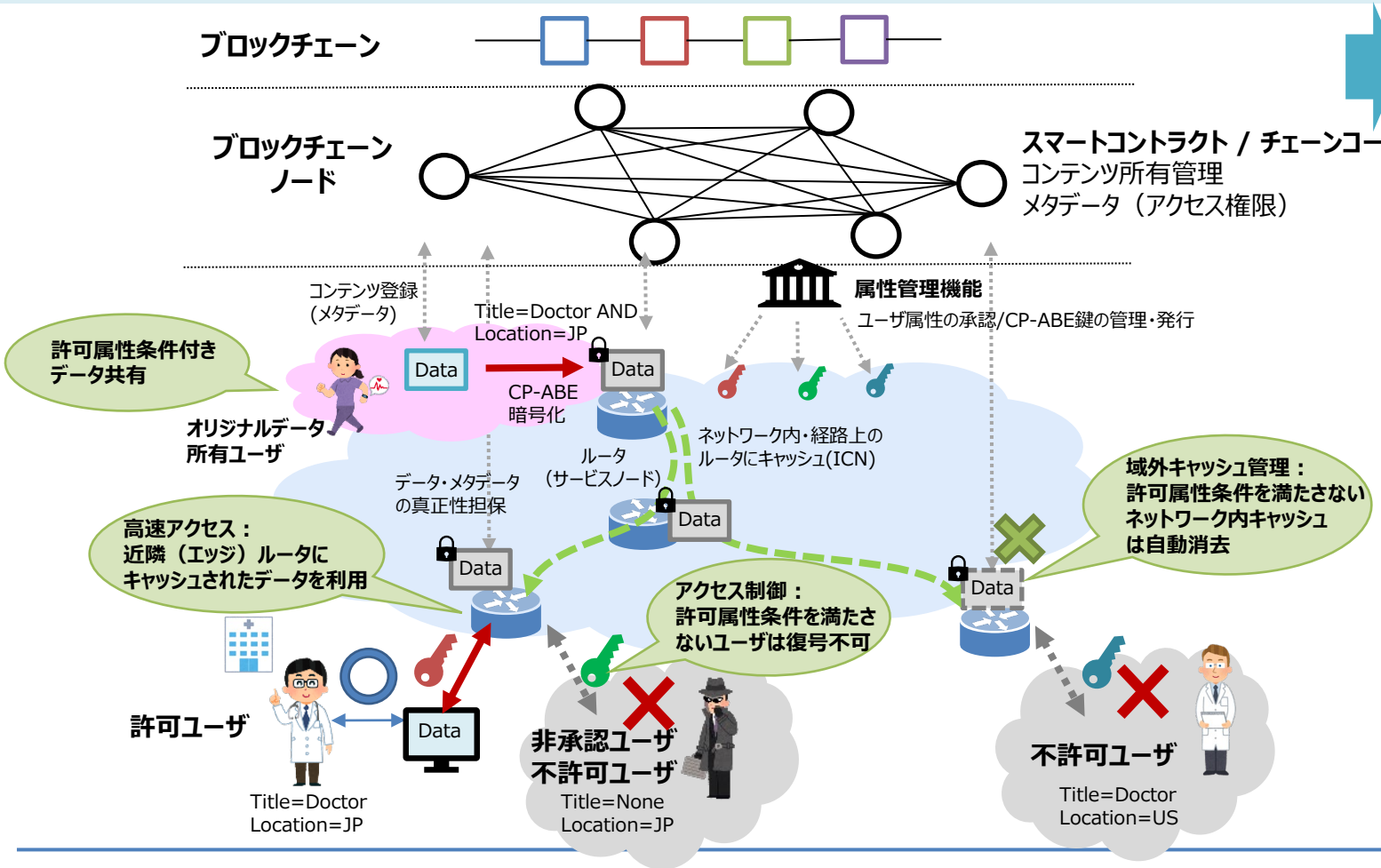
全体ソフトウェア構成


受託者１アプリケーション
受託者２アプリケーション
委託
研究の
成果物
（ソフト）
研究開発項目２
（例）
医療・
ヘルスケア
IoT・
ロボット
物流・サプラ
イチェーン
MaaS・
モビリティ
エネルギー
（例）
コンテンツ・
データ取引
ゲーム・
エンタメ
実証用テストベッドとして
2025年度１Qより受託者
へ提供
研究開発項目１
非集中型ネットワーク内ストレージフレームワーク
NICTセキュアオフチェーンストレージ
NICTが
提供
(ソフト)
既存ブロックチェーン
Hyperledger Fabric
UCINC
IPFS
IPFS(NICT版)
NICT拡張
Authority
（証明書発行等）
Blockchain Network
Cefore
Cefore
(OSS)
独自
ルーティング
Kademlia
高信頼・高可塑B5G/IoTテストベッド
NICT開発
外部既存
ソフトウェア
構成要素2:
UCINC (セキュアネットワーク内ストレージ機能)
構成要素1:
NICT版IPFS (非集中型ストレージ)

NICT提供機能１：セキュアネットワーク内ストレージ機能 UCINC

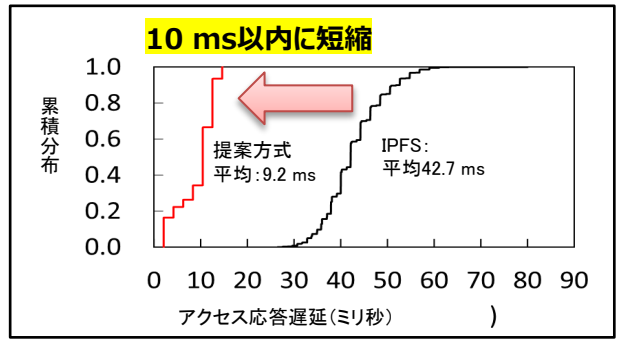
ネットワークレイヤ機能の連携により「流通の地理的範囲の制限」に対応可能。ブロックチェーンで管理されたデータへのアクセスを安全かつ高速に行えるネットワーク内ストレージ機能としてソフトウェア開発

- 高速アクセス：Cefore(ICN)機能を内包、ネットワーク内キャッシュにより**アクセスの低遅延化**，データ送信元/NWの負荷削減
- アクセス制御：**属性暗号(CP-ABE)**を用いてアクセス権限に応じた機密性を維持
- 流通範囲制限：許可されたネットワーク外でデータ（キャッシュ）しない機能により**流通の地理的範囲を制限**

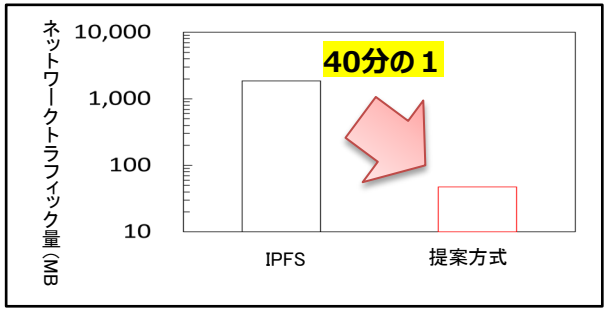


データの機密性・真正性をネットワーク内で担保，アクセス高速化・通信効率向上

応答遅延

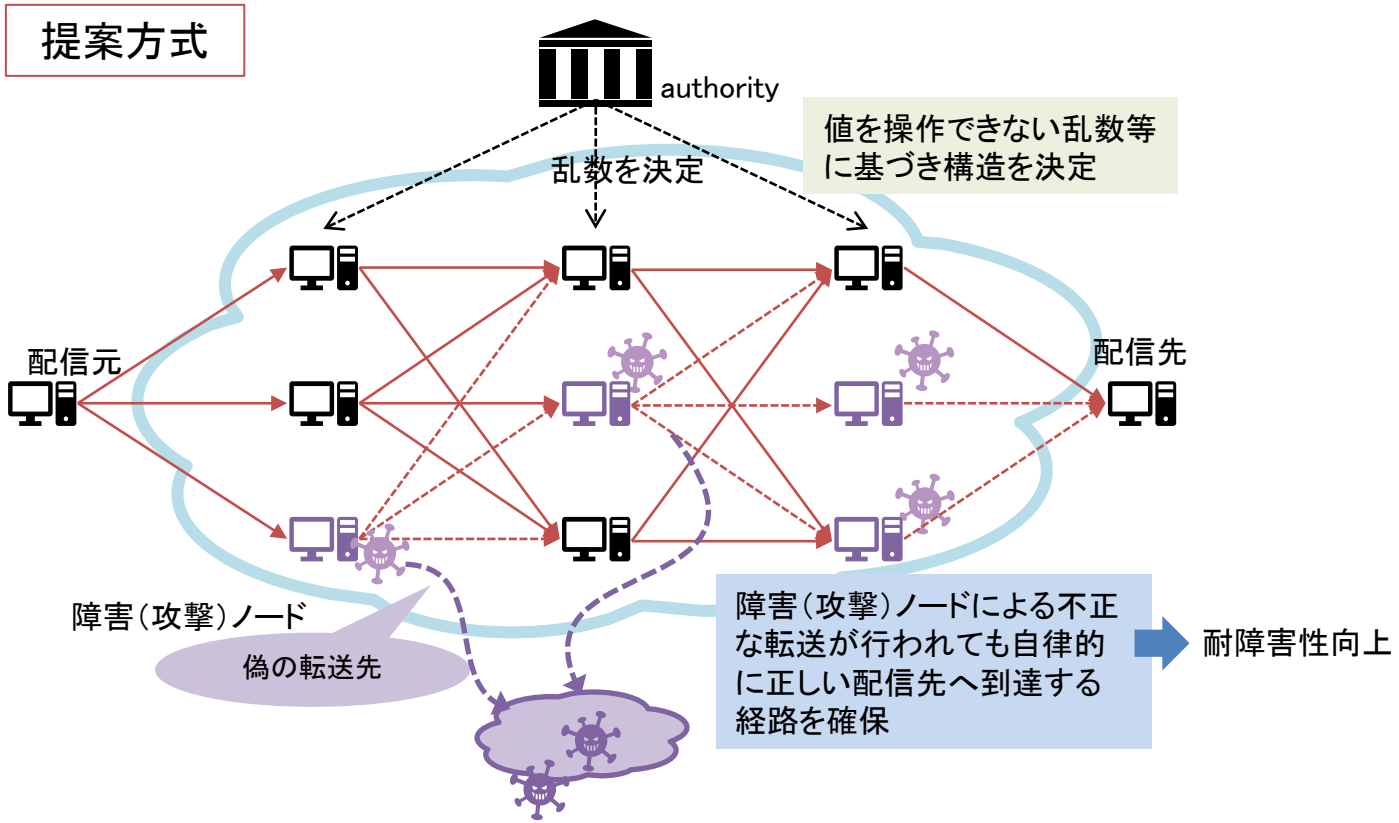


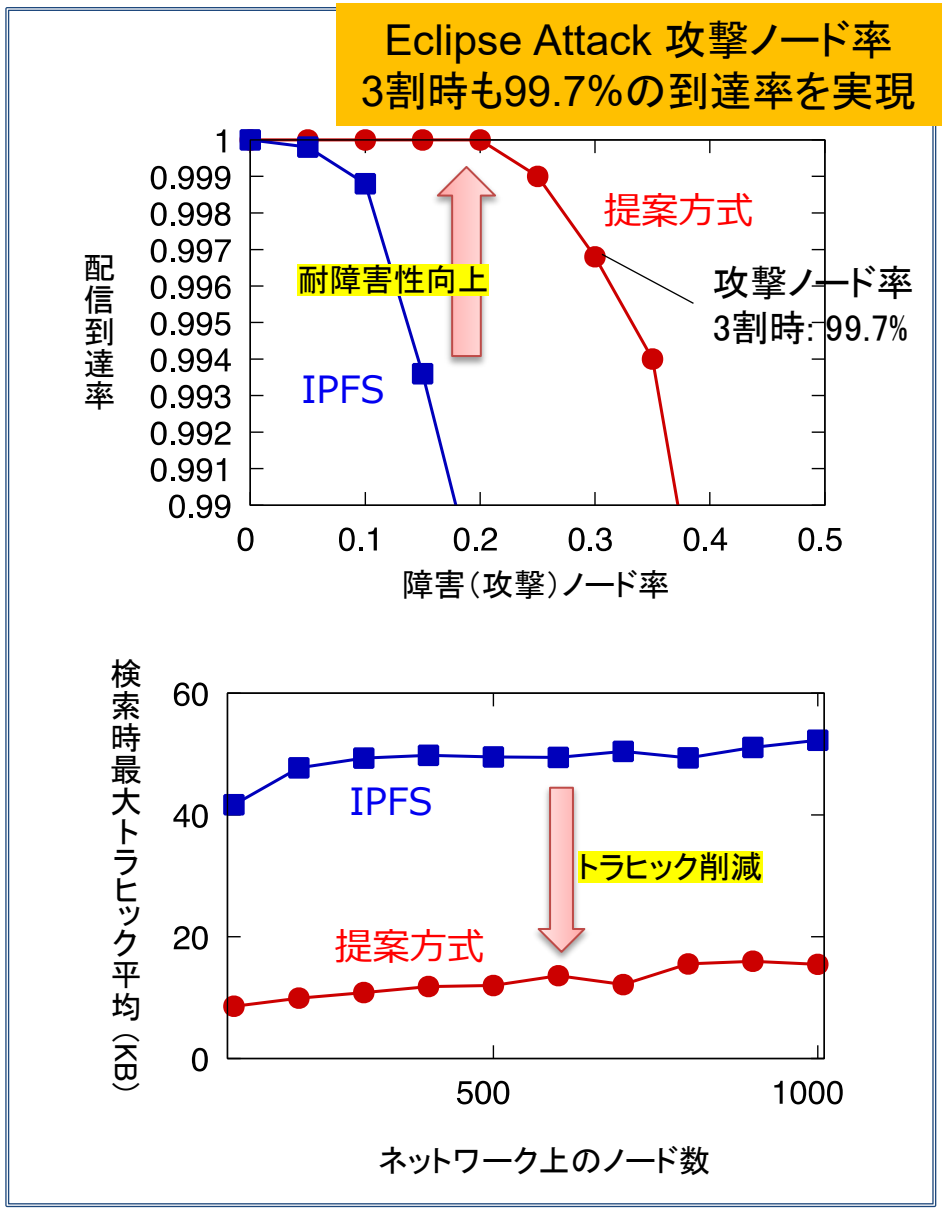
ネットワークトラフィック量



NICT提供機能２：NICT版IPFS

NICT版IPFS：既存 IPFS が前提とする Kademlia の課題の一つ Eclipse Attack 脆弱性への対策を含む信頼性向上方式を提案、IPFSのルーティングレイヤに適用。
NICT版IPFSは、**IPFSの標準的なAPIによるデータアクセスが可能。**





アウトプット目標

研究開発項目１ 非集中型ネットワーク内ストレージフレームワークの研究開発

- 研究開発項目１のフレームワークによって、属性暗号機能およびデータ流通範囲制御機能を利用した**アプリケーションを開発可能であることを示す**こと。
- CP-ABEにより暗号化されたオフチェーンデータの取得要求を行ってから、アプリケーションとして表示完了するまでにかかる応答時間が、**実証用テストベッド上で100ms以内となることを示す**こと。あるいは、達成できることを論理的に示すこと。

認知・知覚情報処理の要求値

研究開発項目２ 高信頼データ流通アプリケーションの研究開発

- 受託者が選択したアプリケーションの動作を確認すること。当機構が提供する実証用テストベッド上で動作するHyperledger Fabric、IPFS、UCINC、およびAuthorityと接続した研究開発項目１のフレームワークを用いて、受託者開発の**アプリケーションの動作を確認**すること。
- ユーザが持つ権限、および、その変化に応じてアプリケーション上で実行できるデータの操作（表示・更新等）も変化することをデモンストレーションにより示すこと。
- **10以上のユーザ（または組織）が、1000以上のデータを収容**し、連携するアプリケーションの実証を行うこと。
- アプリケーションとして利便性高くわかりやすいインタフェースを実現すること。**アプリケーションのユーザビリティや受容性**をアンケートや定量評価により評価・報告すること。

アウトカム目標

2027年　研究開発項目１のフレームワークのソフトウェア、および、受託者開発のアプリケーションの**開発版リリース**。受託者開発のアプリケーション以外の分野の企業間データ連携サービスへの適用性を実証。

2028年　研究開発項目１のフレームワークのソフトウェア、および、受託者開発のアプリケーションの**商用版リリース**。商用サービスの実施にあたっては、**非集中型ネットワーク内ストレージ、および、受託者開発のアプリケーションの管理・運用を受託者にて実施**する前提とする。
研究開発項目1の非集中型ネットワーク内ストレージフレームワークを**20以上のデータ連携サービスに適用**。

2030年　欧米のブロックチェーン・IPFSを活用する**データ連携技術（例：Horizon Europe の TRUSTEE）との接続**。

研究開発期間・予算額等

採択件数

1件

研究開発期間

2年間（2025年度（4月1日または契約締結日）～2026年9月30日）

予算額

2025年度：総額50百万円（上限）
2026年度：総額25百万円（上限）

提案の予算額の調整を行った上で採択する提案を決定する場合がある。

研究開発体制

単独の提案も可能であるが、産学官連携等による複数の実施主体からなる体制とすること。
選択するアプリケーション分野の商用サービスを実施している、あるいは、実施する予定がある企業が受託者として参加する体制とすること。

留意点など

- 受託者は、当機構が開発したNICTセキュアオフチェーンストレージを構成するソフトウェアを、研究開発期間中は**無償で利用することができる**。
- NICTセキュアオフチェーンストレージのデータへ、IPFSおよびUCINC**両方のインターフェース**を用いてアクセスするアプリケーションソフトウェアを実装すること。
- 本委託の成果となる非集中型ネットワーク内ストレージフレームワークのソフトウェアは、**可能な限りオープンソース公開**すること。
- 本委託にて開発する非集中型ネットワーク内ストレージフレームワークのインターフェースや機能について複数の**受託者間で調整**を行う可能性がある。
- **外部のIPFSのデータを標準的なAPIを用いて取り込む**機能を有すること。連携が可能であることを、研究開発項目２の実証において示すこと。
- IPFS、UCINC、Cefore、Authorityの各機能要素は、基本的に当機構より提供または貸与されるソフトウェアを用いること。Hyperledger Fabricは、オープンソースソフトウェアとして公開されているのでそれを用い […] 品質担保や課題解決のために**必要であれば、各機能要素を改良・拡張する**こと。また、各機能要素は当機構と協議の上、**独自の実装に置き換えても良い**。
- NICTセキュアオフチェーンストレージのソフトウェアの改良・拡張を受託者にて行なった場合、**変更箇所のプログラムソースは可能な限り当機構へ提供**するものとする。
- 委託研究後のシステム・運用体制の構築を含めた**事業化等の内容を明確に示す**こと
- 2026年度については、機構の次期中長期目標の状況によっては、**実施スケジュールや実施内容等の変更、調整が必要となる場合がある**ことをあらかじめご了承ください。

ご応募をお待ちしております

公募期間

2024年10月31日（木）～ 2024年12月6日（金）正午