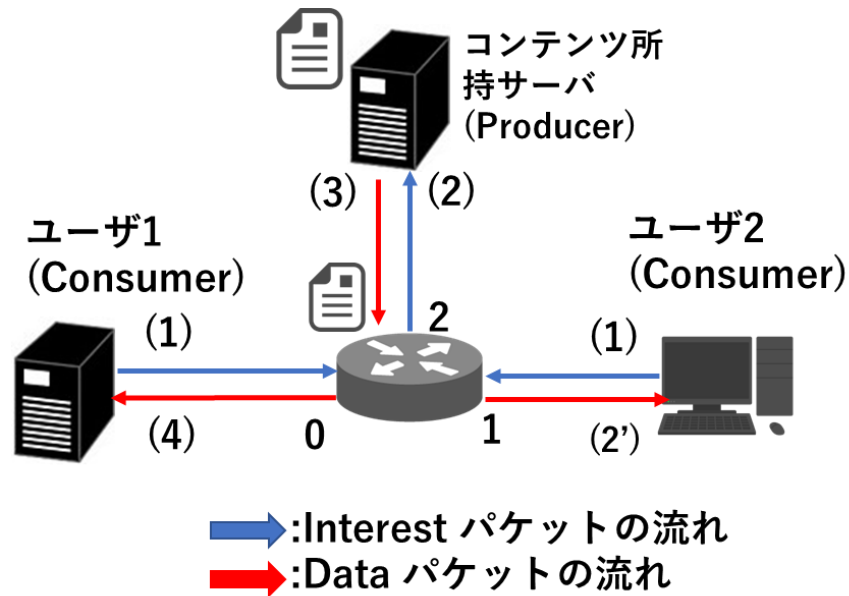


CCNにおけるスマートコントラクトを用いた 経路構築及び名前解決サービスの実現

生井 青伊† 大坐 畠 智† 山本 嶺†

† 電気通信大学 大学院 情報理工学研究科 情報学専攻

研究背景



- **CCN**(Content-Centric Networking)[1]
 - コンテンツの識別子にコンテンツ自体の名前を利用したネットワーク
 - FIB(Forwarding Information Base)エントリの増大が課題[2]
- **NRS**(Name Resolution Service)
 - 人気が高いコンテンツをオンデマンド対応
 - 常設するFIBエントリの削減

[1] 福田 健一伊藤 章,“ICN が切り開く次世代ネットワークアーキテクチャー (特集 研究開発最前線) – (進化する ICT システム 運用・データ利活用技術),” Fujitsu,vol.66,no.5, pp.53–61,sep 2015. <https://ci.nii.ac.jp/naid/40020594124/>

[2] A. Detti, M. Pomposini, N. Blefari-Melazzi, and S. Salsano. Supporting the web with an information centric network that routes by name. Computer Networks, Vol. 56, No. 17, pp. 3705– 3722, 2012.

研究背景

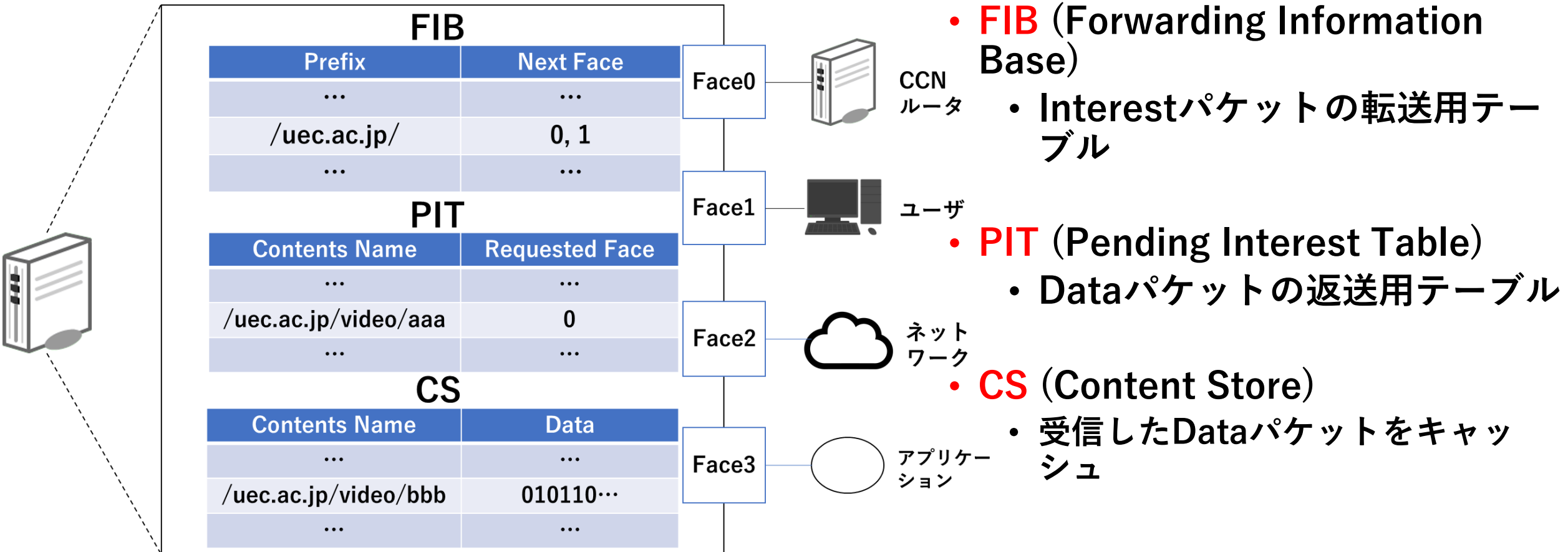
- SDNコントローラを用いたFlowアップデート [3][4]
- URLに変換し、IPの通信でコンテンツ取得 [5]
 - 課題：常設するFIBとNRSを両方の構築・管理の実現
- CCNのルーティングテーブル構築とNRSを提供する分散型
のアプリケーション作成
 - スマートコントラクトを利用した情報集積・共有
 - コンテンツの情報、ネットワークの接続情報の登録
 - 優先度の高いFIBエントリの作成
 - 人気の低いコンテンツへのオンデマンド対応機能を提供

[3]M. Vahlenkamp, F. Schneider, D. Kutscher and J. Seedorf, "Enabling ICN in IP networks using SDN," 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, Germany, 2013, pp. 1-2

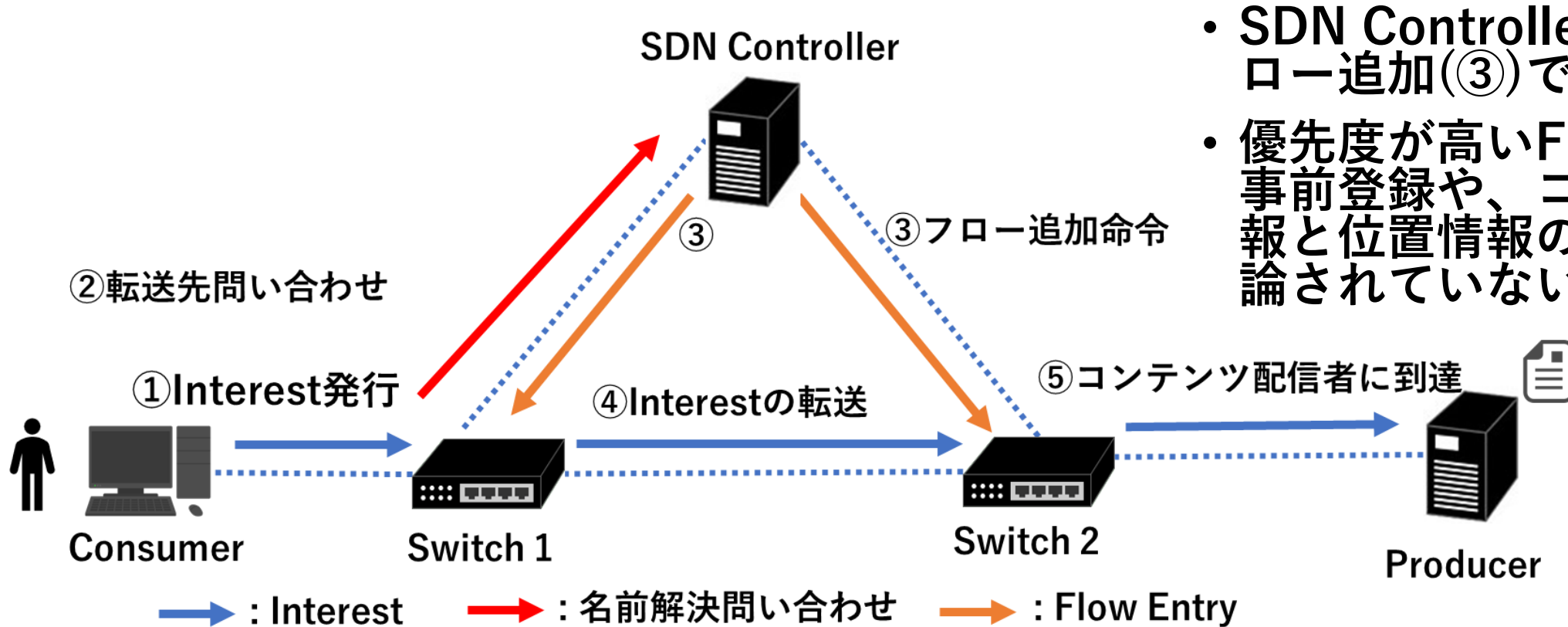
[4]A. F. R. Trajano and M. P. Fernandez, "ContentSDN: A Content-Based Transparent Proxy Architecture in Software-Defined Networking," 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 2016, pp. 532-539

[5]J. Hong, T. -W. You and Y. -G. Hong, "Name resolution service for CCN," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2017, pp. 1276-1279

関連研究：CCNルータ内のデータ構造



先行研究：SDNコントローラを用いたNRS[3][4]

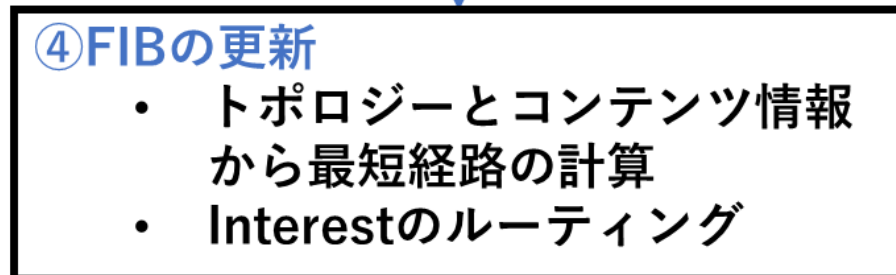
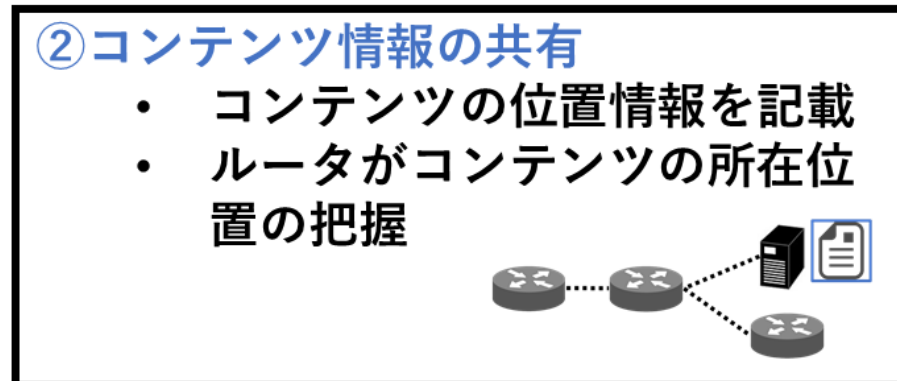
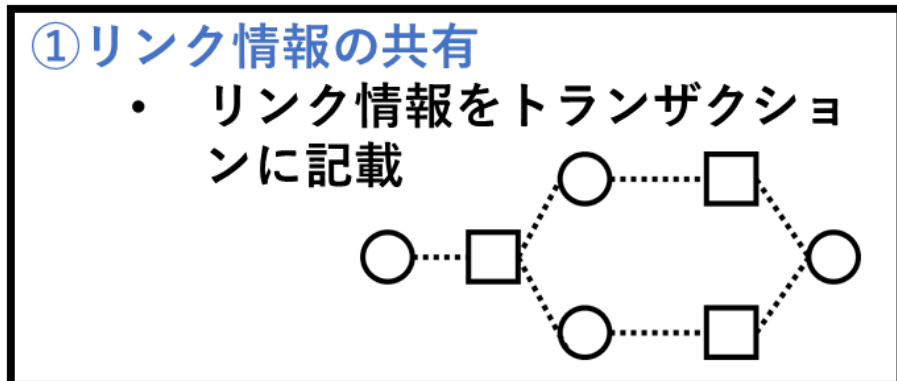


- SDN Controllerによるフロー追加(③)で実現
- 優先度が高いFIBエントリの事前登録や、コンテンツ情報と位置情報の紐づけは議論されていない

[3] M. Vahlenkamp, F. Schneider, D. Kutscher and J. Seedorf, "Enabling ICN in IP networks using SDN," 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, Germany, 2013, pp. 1-2

[4] A. F. R. Trajano and M. P. Fernandez, "ContentSDN: A Content-Based Transparent Proxy Architecture in Software-Defined Networking," 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 2016, pp. 532-539

先行研究：ブロックチェーンを用いたCCNのFIB構築[6]



③各トランザクションを
ブロックチェーンで共有

- コンテンツの位置情報はネットワークが認知 → Interestに位置情報を加えなくて良い
- 課題：すべてのルータがブロックチェーンを持っている前提

課題と解決アプローチ

• 解決する先行研究の課題

1. CCN内で利用できるルーティングテーブル構築・NRSの両方提供
2. ブロックチェーン所持によるルータの要件の高さ

• 解決アプローチ

1. FIBを動的に構築・管理する分散型アプリケーションの実装
 - スマートコントラクトを用いてリンク情報とコンテンツ情報を集約
 - 優先順位が高いコンテンツ：定期的なFIB構築命令
 - 優先順位が低いコンテンツ：NRSで対応
2. Ethereumノードと通常CCNルータ情報交換機能の実装
 - CCN通信で実装
 - 通常CCNルータのストレージ要件を抑えることが可能
 - Ethereumの同期機能によりネットワーク全体で同じデータ取得可能

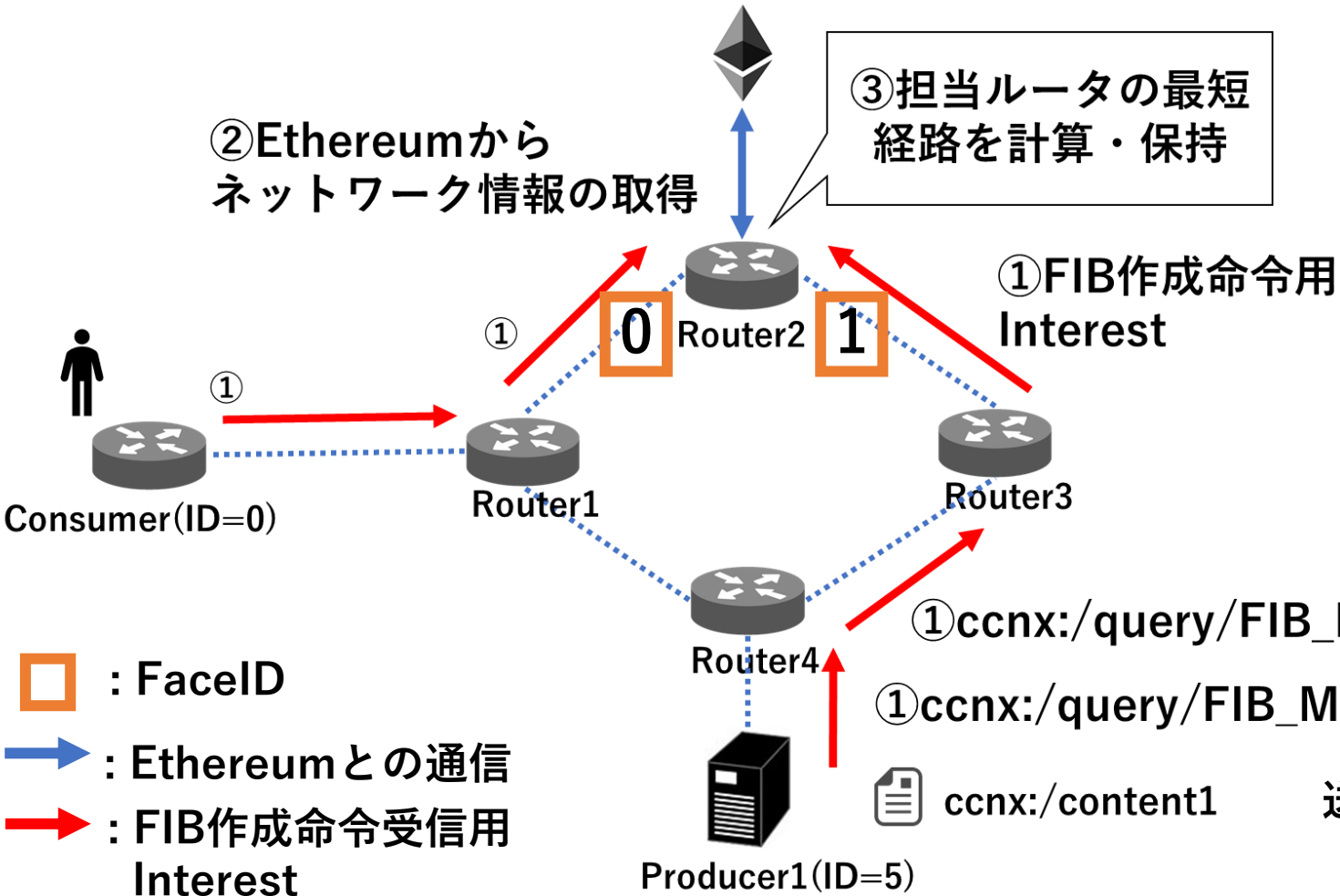
提案手法 -概要-

- スマートコントラクトを用いた情報共有
 - Ethereum上に各種情報共有用のスマートコントラクトをデプロイ
 - ルータの接続情報、所有しているコンテンツの情報を登録
 - 利点:分散されたアプリで各種情報とルータIDの自動管理可能
 - コンテンツ名に位置情報を添付せずにコンテンツ要求可能
- FIBの構築とNRSの提供
 - CCNアーキテクチャとしてNICT開発のCefore[7]を利用
 - NRSの構築
 - Dijkstra法による最短経路情報の計算
 - 問い合わせ → 最短経路のルータに**FIB作成命令送信**
 - 各ルータが必要な情報に対してFIBの更新
 - 経路情報と優先度が高いコンテンツ情報を定期的に取得

[7] 電子情報通信学会情報指向ネットワーク技術特別研究専門委員会, “ICN/CCN 通信を実現するソフトウェアプラットフォーム cefore,”
参照日:2023/9/9 https://www.ieice.org/cs/icn/?page_id=1208

提案手法：NRSの実装(1/2)

- 定期的に行う事前準備処理



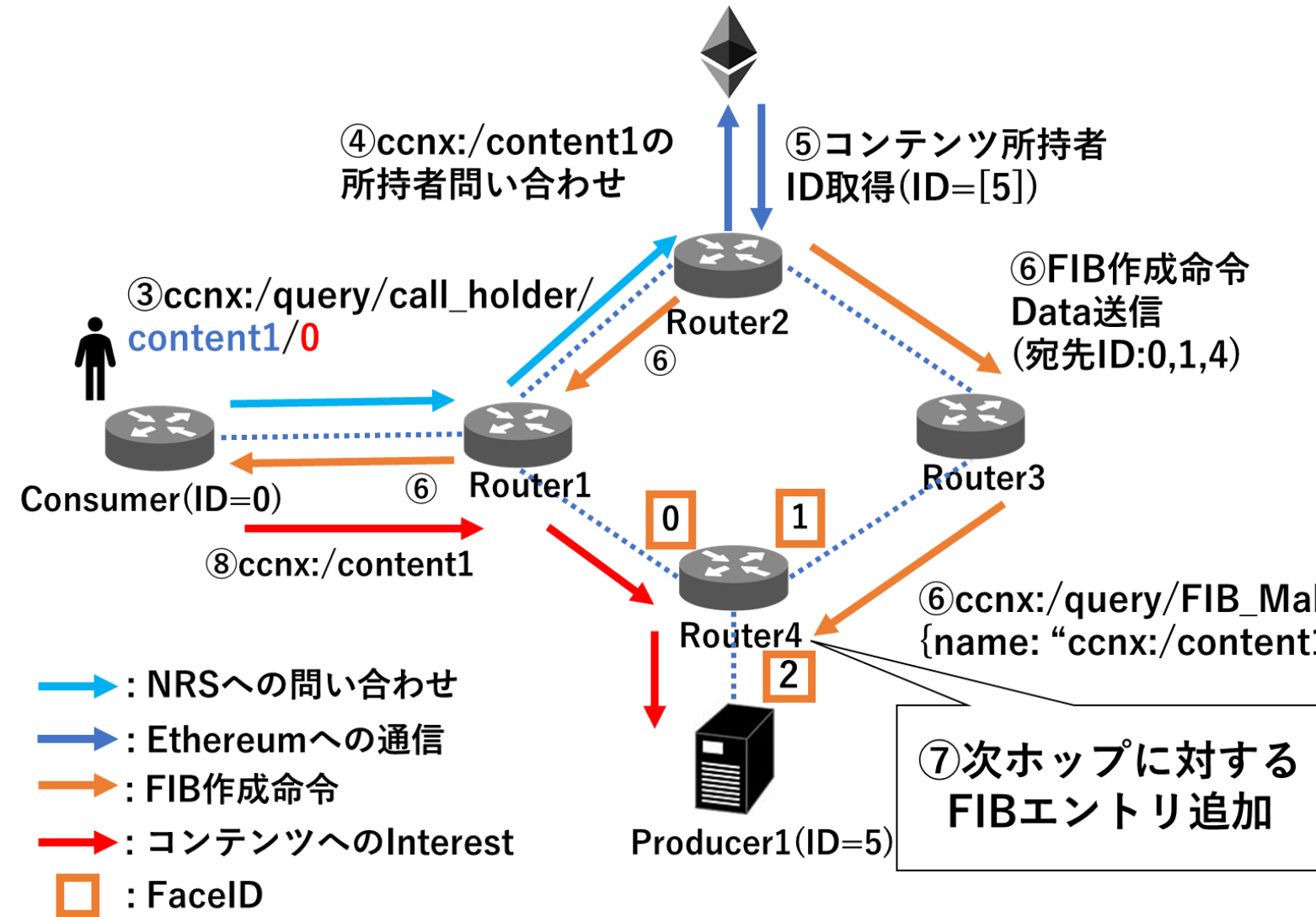
Router2のPIT (①で生成)

コンテンツ名	送信元Face
ccnx:/query/FIB_Make/0	0
ccnx:/query/FIB_Make/1	0
ccnx:/query/FIB_Make/4	1
⋮	⋮

Consumerからの最短経路(③で計算)

宛先ルータID	最短経路
2	[0, 1, 2]
5	[0, 1, 4, 5]
⋮	⋮

NRSの実装(2/2)

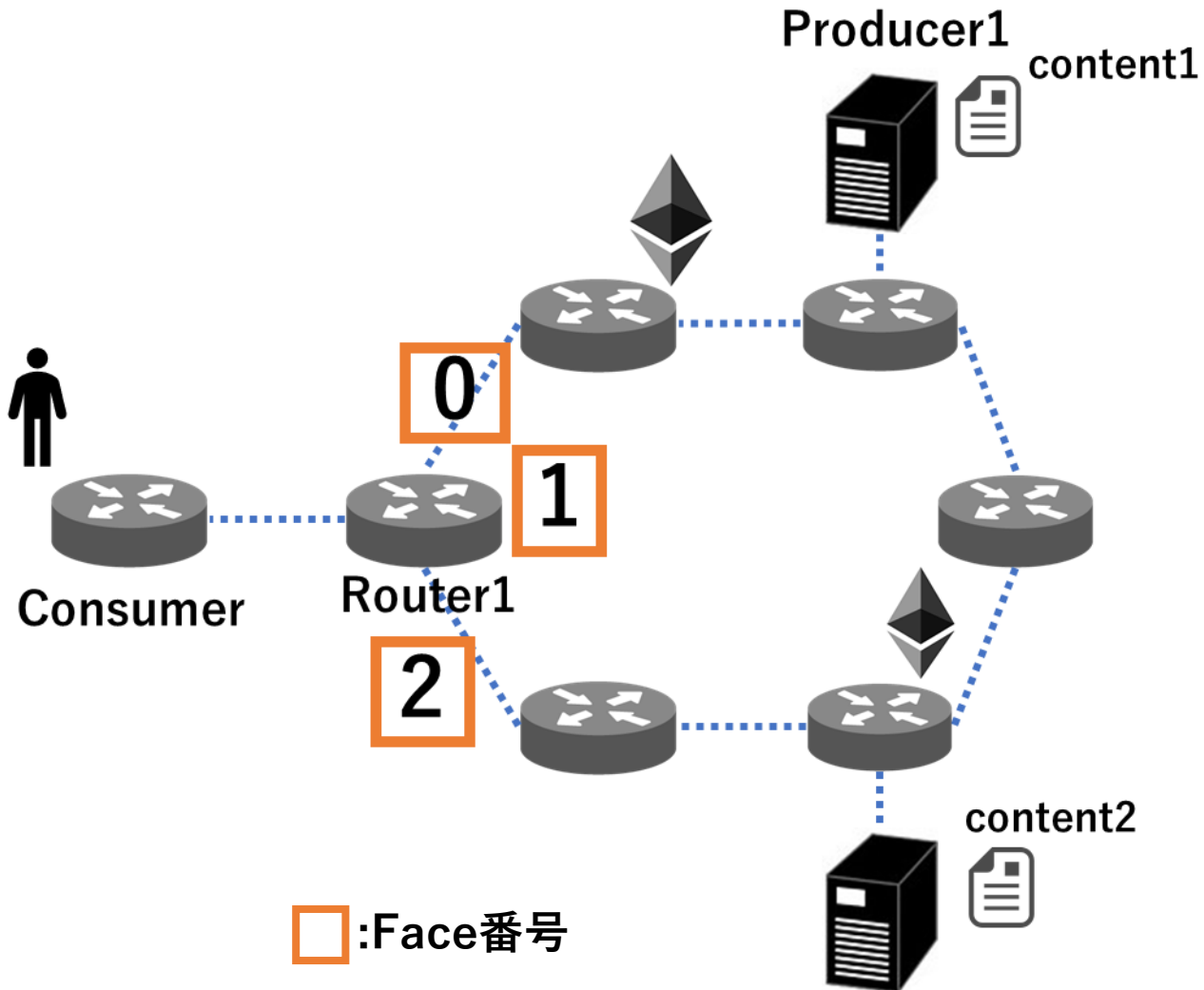


- NRSへの問い合わせ情報(③)
 - 青字: コンテンツ名
 - 赤字: 送信元ID
- 送信元IDとコンテンツ所持者から最短経路を決定
- 対象ルータへFIB作成Interest送信(⑥)
- Prefixと次ルータのFaceIDをFIBエントリに追加(⑦)

Router4のFIB

Prefix	FaceID
ccnx:/query	1
<u>ccnx:/content1</u>	<u>2</u>

提案手法 FIBの構築

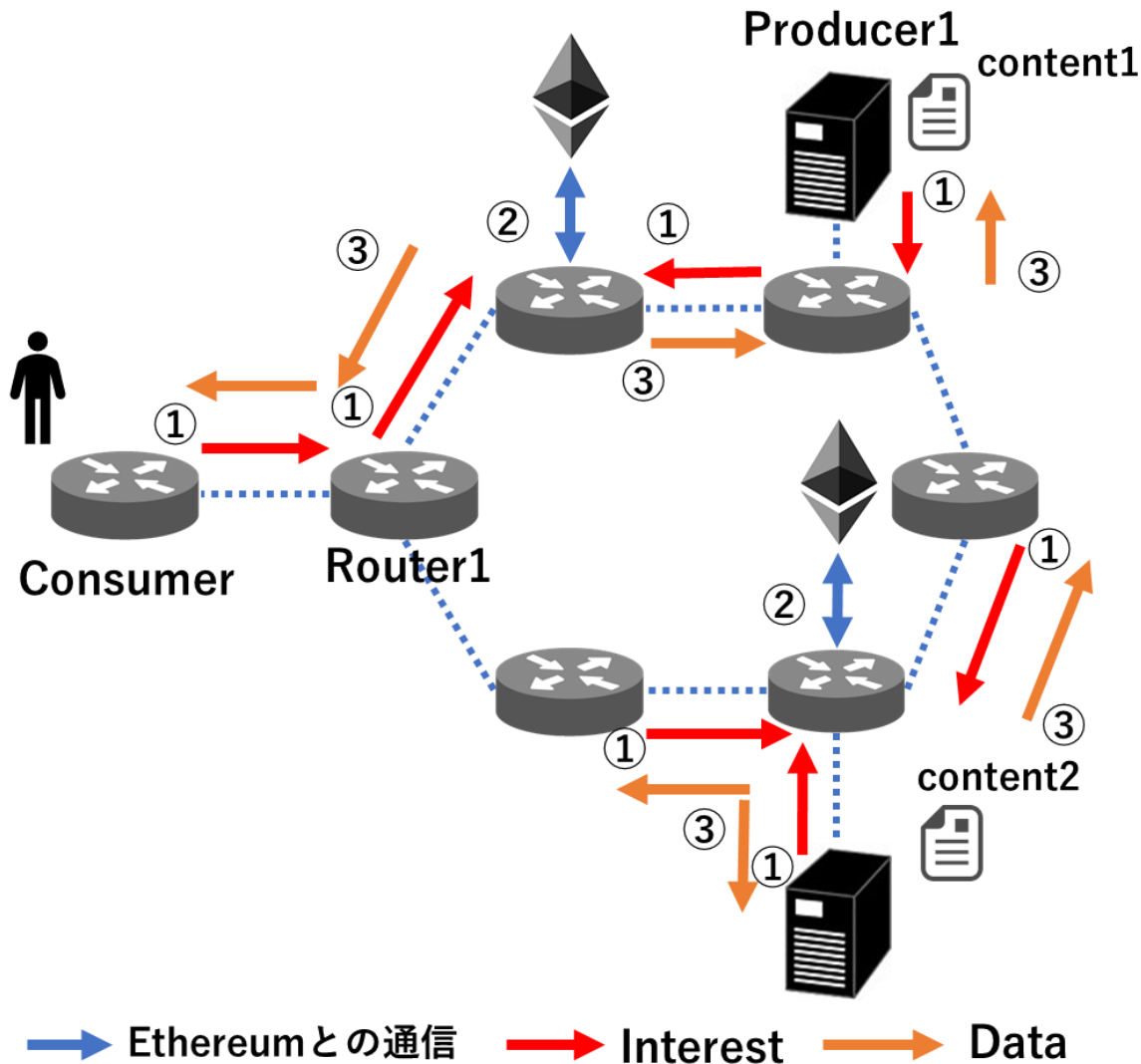


- 左図のようなトポロジーで説明
 - Ethereumへの問い合わせPrefix (ccnx:/query)もコンテンツ扱い
 - 優先度の高いPrefix
 - ccnx:/query, ccnx:/content2
 - 隣接しているルータの把握可能
 - 接続時にはccnx:/queryのみ仮登録

Router1のFIB

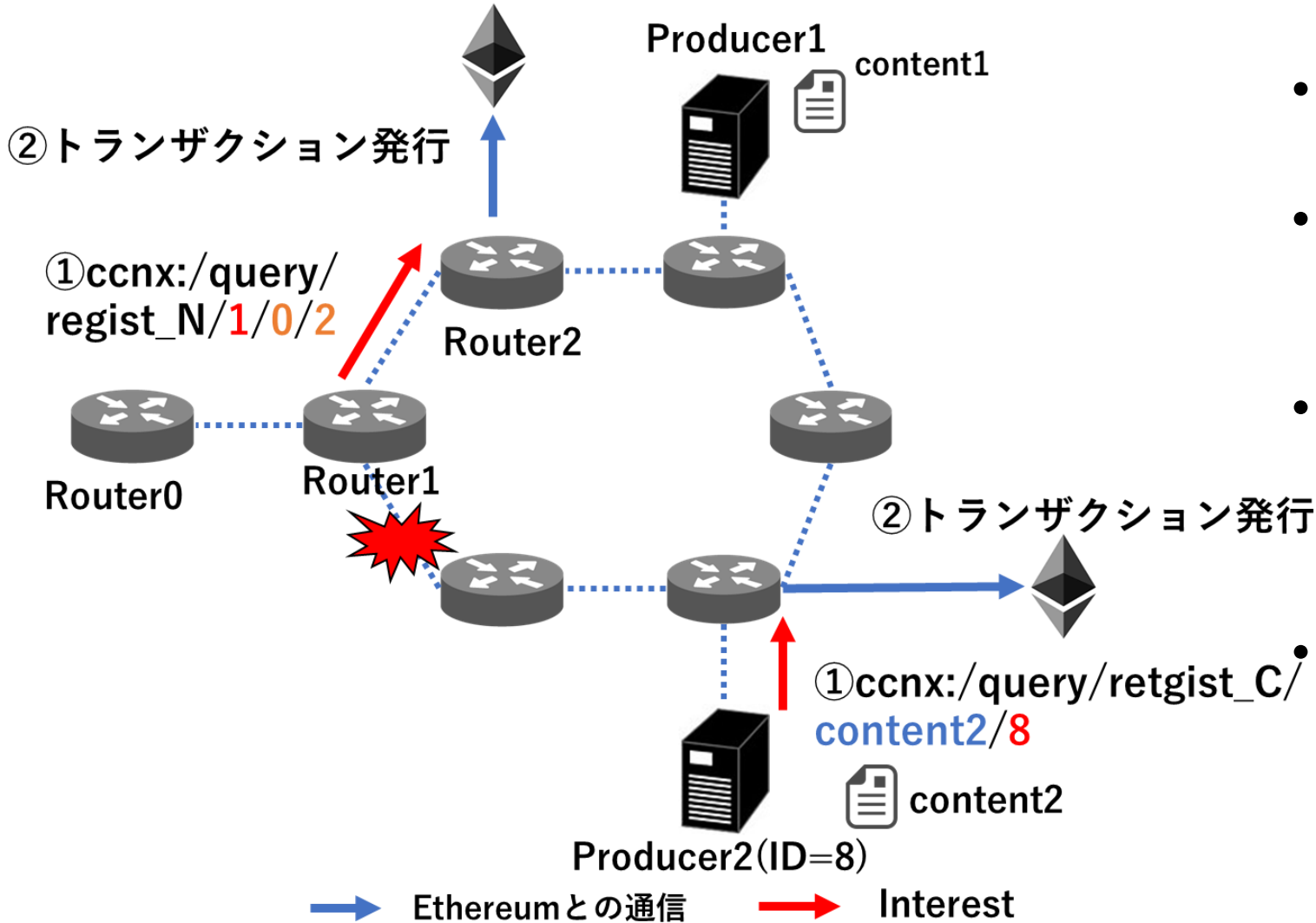
Prefix	Face番号
ccnx:/query	0
ccnx:/content2	2
⋮	⋮

FIBの構築手法(FIBの更新)



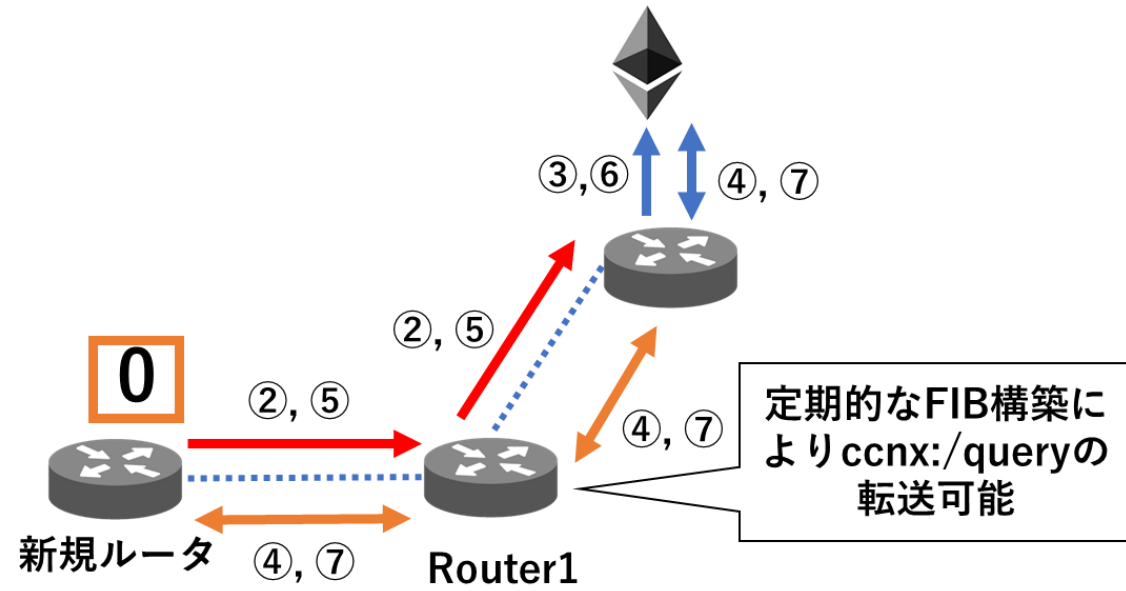
- ① Ethereumノードからの情報を受け取る用のInterestを定期的に送信
 - A) 優先度が高いコンテンツ情報
 - ccnx:/query/content_first
 - B) ネットワーク情報
 - ccnx:/query/network
- ② Ethereumノードは定期的にスマートコントラクトへ情報要求
- ③ ①で作成したPITへData(A, B)送信
- ④ それぞれのルータがBよりDijkstra法を用いた最短経路計算
- ⑤ ④とAからFIBのアップデート

FIBの構築手法(情報登録)



- トランザクションを発光してもらうための**特殊Interest送信**
- 各種情報の登録
 - Ethereumノードへパケット転送(①)
 - トランザクションの発行(②)
- 新規コンテンツ発生
 - ccnx:/query/regist_C/
<コンテンツ名>/<自身のルータID>
- ネットワーク情報の更新
 - ccnx:/query/regist_N/
<自身のルータID>/<隣接ルータID列>

新規ルータ登録



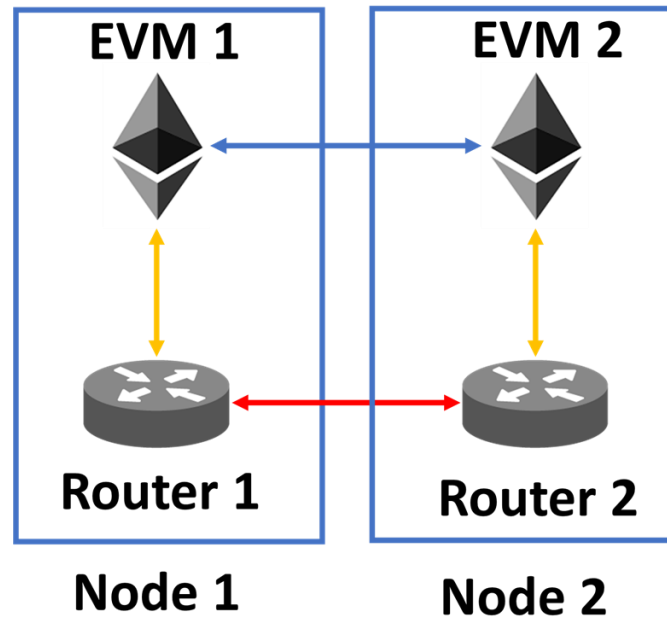
→ Ethereumとの通信
 → 情報登録Interest
 → Interest/Data交換

ConsumerのFIB(①)		ConsumerのFIB(⑧)	
Prefix	Face番号	Prefix	Face番号
ccnx:/query	0	ccnx:/query	0
		ccnx:/content1	0

最近傍のEthereumノード用にアップデート

- ① 隣接ルータへ情報登録を行うためのFIB作成
- ② **ルータ登録用Interest**を送信
 - ccnx:/query/regist_R/<IPアドレス>
- ③ ルータ登録トランザクションを発行
 - スマートコントラクト上で自動的にID付け
- ④ ルータIDの取得
- ⑤ 自身の隣接配列情報登録用Interestを発行
- ⑥ 隣接配列登録トランザクション発行
- ⑦ FIB構築に必要な情報取得
- ⑧ FIB構築
 - ①で作成したccnx/queryに対してもアップデート

EthereumとCCNの構成



↔ Ethereum同期通信

↔ 情報登録&取得

↔ CCN通信

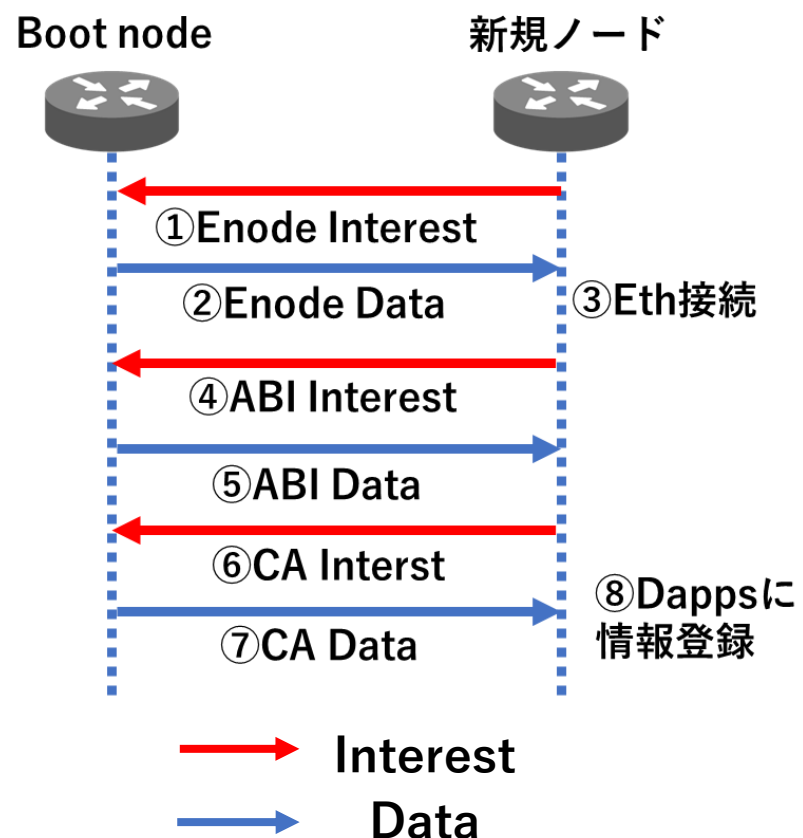
- **Ethereum同期通信**
 - P2Pでブロックのやり取り
 - Ethereum同士の接続にEnodeアドレス情報が必要
- **スマートコントラクトとの情報交換**
 - Web3.py[8]の利用
 - PythonプログラムからEthereumノードへの通信
 - HTTP通信を利用
- **CCN通信**
 - Ceforeとcefpyco[9]を用いたCCN通信

[8]Ethereum Foundation, “web3.py stable” 参照日2023/10/28 <https://web3py.readthedocs.io/en/stable/index.html#>

[9]大岡 睦, 朝枝 仁. “Cefpyco : Cefore アプリケーション開発用 Python パッケージ” 参照日:2023/10/29.

<https://www.ieice.org/~icn/wp-content/uploads/2020/09/a-ooka2019ICN-cefpyco.pdf>

Ethereumノード接続手順



- **CCN通信を利用したスマートコントラクト利用のための事前準備通信**
 - Ethereum同士の接続(①～③)
 - Enodeアドレスの交換
 - スマートコントラクトにアクセスするための情報交換(④～⑧)
 - ABI(Application Binary Interface)
 - 異なるハードウェア間でプログラムを共有するための規約
 - CA(Contract Address)
 - スマートコントラクトのブロックチェーン上の位置情報
- ↓
- **Ethereumが同期し、ルータがスマートコントラクトにアクセス可能**

評価実験

1. Ethereumノードの数を制限することによる効果

- Ethereumが生成するブロックサイズの確認
- CCNノードのストレージ要件への影響調査

2. NRSで最短経路のFIBが構築できていることの確認

- 2つのトポロジーを用いてコンテンツ取得遅延の評価

仮想ルータの設定

OS	Ubuntu 18.04.3 LTS
メモリ	8.0GB
プロセッサ数	4
その他の機能	Cefore-0.8.3a
	cefpyco-0.6.0
	Python 3.9.7

Ethereumの設定

クライアント	Geth 1.12.0-stable
コンセンサス アルゴリズム	Proof of Authority
ブロック生成速度	1秒に1個生成

評価実験1

- ルータ上にEthereumを稼働させ、各種トランザクションを送信した際のブロックサイズの検証
 - 実験a
 - 1000回トランザクションを送信した際の平均ブロックサイズを検証
 - 対象
 - スマートコントラクトの利用無し
 - コンテンツ情報登録(所持者1,2)
 - ルータ情報登録
 - 実験b
 - 隣接配列(ネットワーク情報)登録時のブロックサイズ検証
 - ルータの数を1~10個まで変化
 - 100個のトランザクションを送信した際の平均ブロックサイズの測定

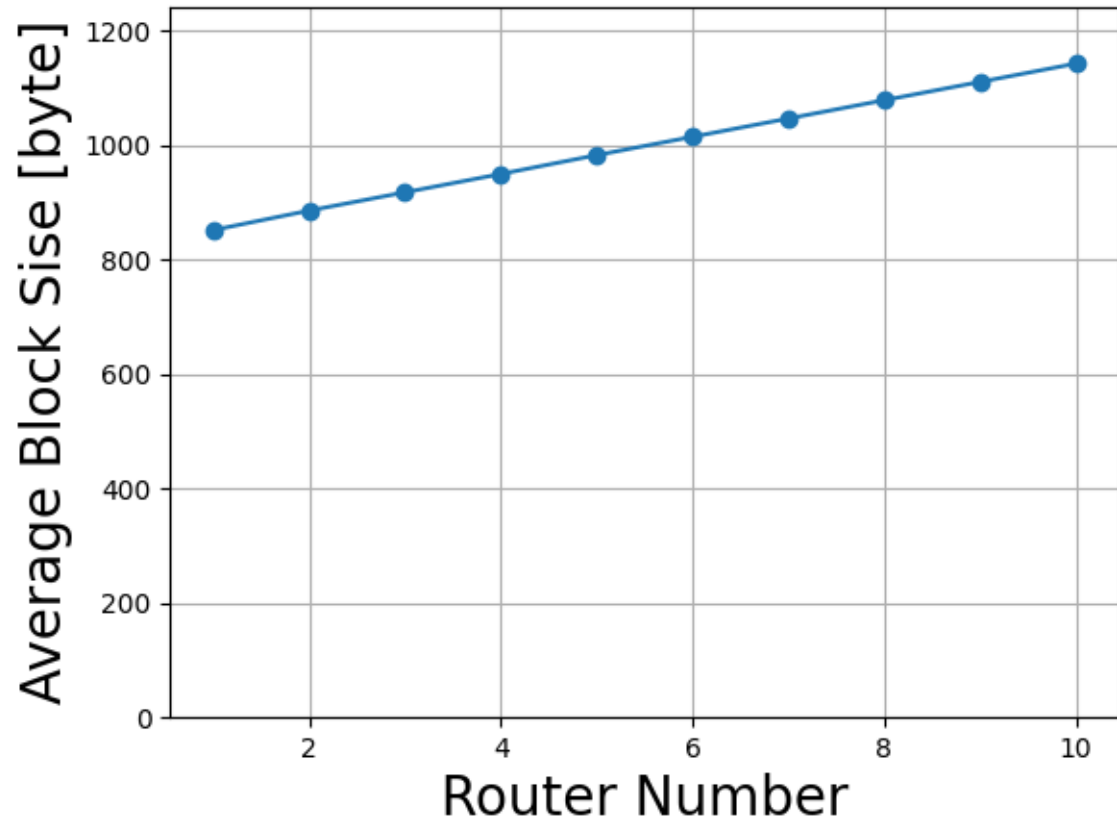
実験結果1a

格納トランザクションごとの平均ブロックサイズ

格納トランザクション	平均ブロックサイズ[byte]
利用なし	609
コンテンツ情報(所持者数1)	919
コンテンツ情報(所持者数2)	950
ルータ情報	821

- 各種登録におけるブロックサイズの平均値
 - スマートコントラクトを利用しなくてもブロックが生成
 - 1つ1つのブロックのサイズは大きくない
- ブロックチェーンの途中消去は不可能
- 能力が高いルータにEthereum稼働を任せただ方が良い

実験結果1b

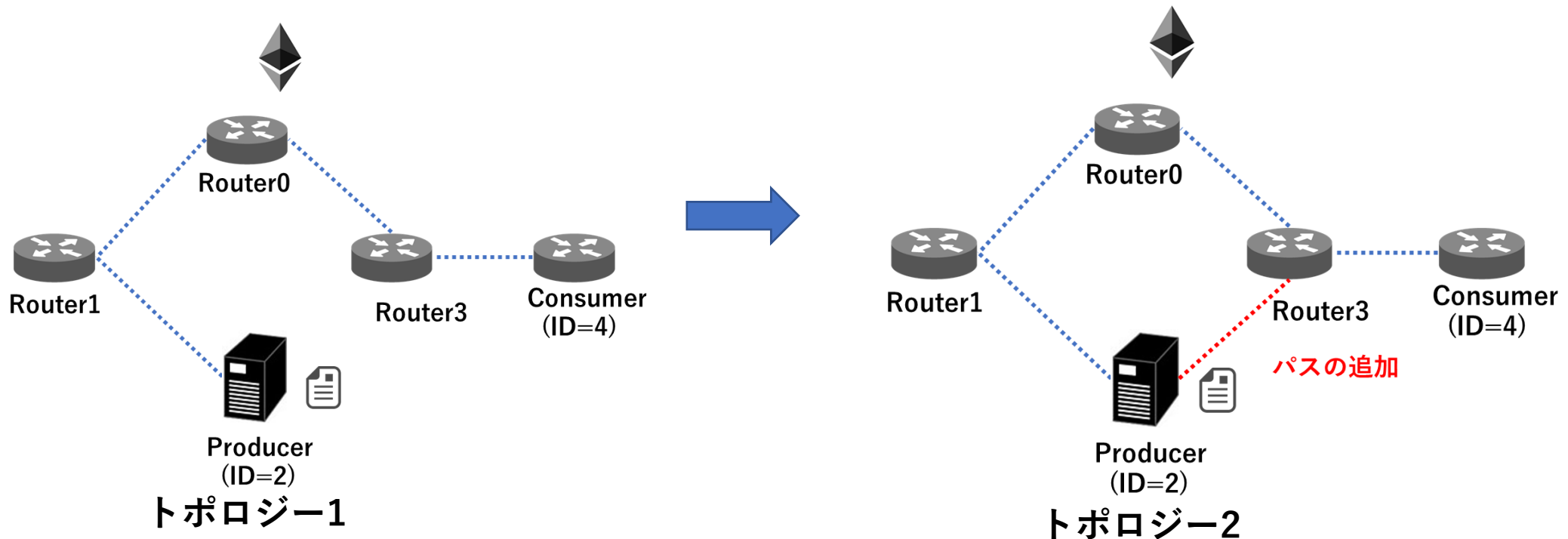


ルータの数と隣接配列登録時のブロックサイズの関係

- 登録ルータ数を変化した際の隣接配列登録時のブロックサイズの変化
 - ルータの数が増加することによりブロックサイズの増加
 - 大規模なネットワークの実装時はストレージ要件の増大
 - 登録時のブロックサイズの増加
 - ネットワーク情報更新回数の増加

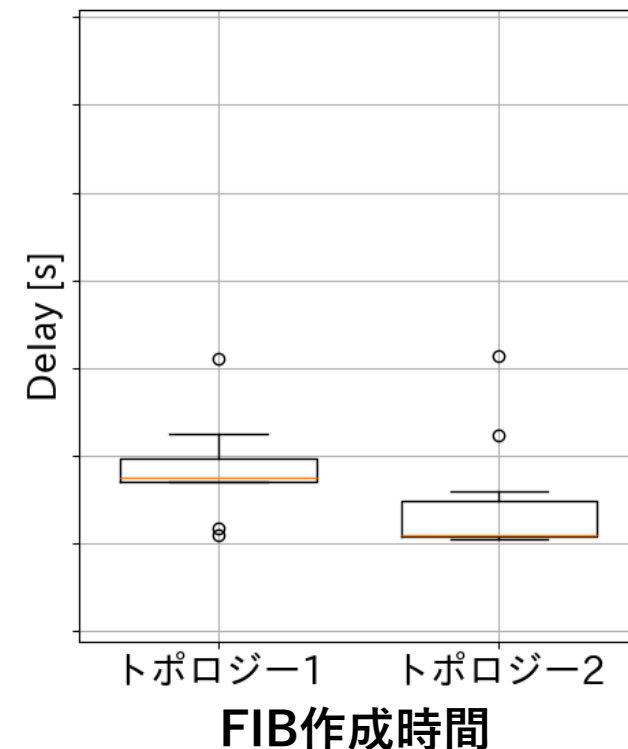
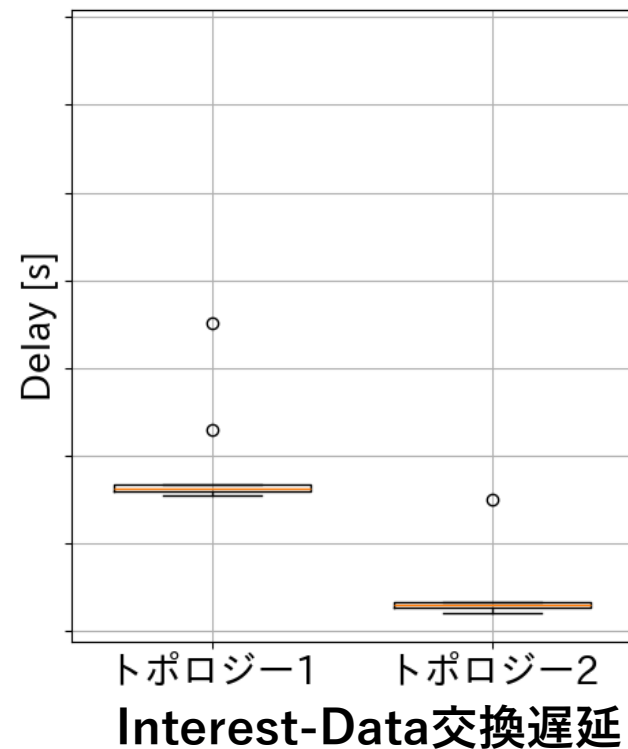
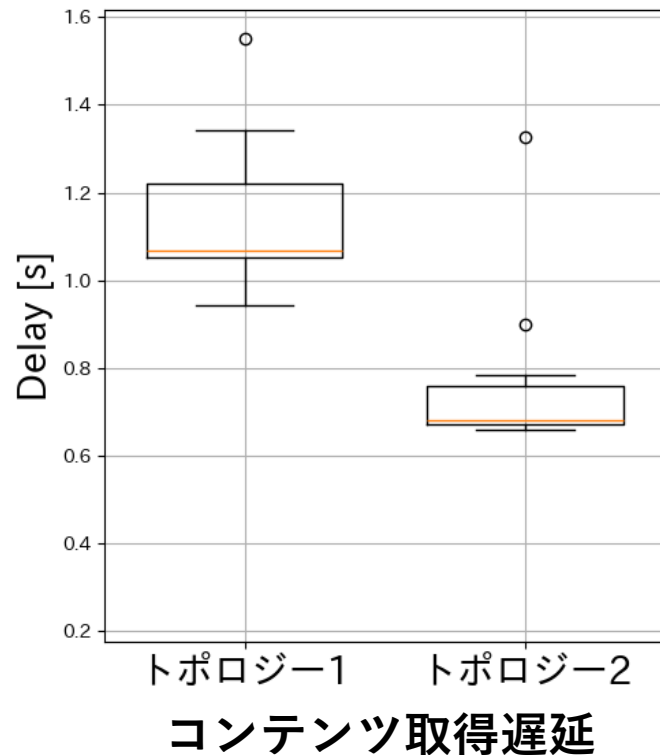
評価実験2

- 2つのトポロジーで評価
 - トポロジー1 : Consumer – Producer間が4ホップ
 - トポロジー2 : Producer – Router3の間にパス追加
 - それぞれ10回コンテンツ取得にかかる遅延を測定



結果2

- トポロジー2の方が遅延が小さい
 - 最短経路を通るためのFIB作成成功
- FIBの作成時間には大きな差がない
 - 今回はConsumerとEthereumの距離は変更していない



まとめと今後の課題

- CCNにおけるInterestのフォワーディングテーブルであるFIBの動的な構築とNRS構築手法の説明
 - ブロックチェーンを用いた手法のルータ要件を回避するために、Ethereumを持たないノードとの通信を実装
 - コンテンツ取得遅延を計測し、最短経路を通るようにFIBが作成可能
- 課題
 - NRSの配置場所を変えることによるコンテンツ取得遅延
 - コンテンツの優先度の決定方式をスマートコントラクト上に実装
 - グローバルネットワークでも実装できるような仕組みの考案

参考文献

- [1] 福田 健一・伊藤 章, “ICN が切り開く次世代ネットワークアーキテクチャー (特集 研究開発最前線) – (進化する ICT システム運用・データ利活用技術),” Fujitsu, vol.66, no.5, pp.53–61, sep 2015. <https://ci.nii.ac.jp/naid/40020594124/>
- [2] A. Detti, M. Pomposini, N. Blefari-Melazzi, and S. Salsano. Supporting the web with an information centric network that routes by name. Computer Networks, Vol. 56, No. 17, pp. 3705– 3722, 2012.
- [3] M. Vahlenkamp, F. Schneider, D. Kutscher and J. Seedorf, "Enabling ICN in IP networks using SDN," 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, Germany, 2013, pp. 1-2
- [4] A. F. R. Trajano and M. P. Fernandez, "ContentSDN: A Content-Based Transparent Proxy Architecture in Software-Defined Networking," 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crańs-Montana, Switzerland, 2016, pp. 532-539
- [5] J. Hong, T. -W. You and Y. -G. Hong, "Name resolution service for CCN," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2017, pp. 1276-1279
- [6] Shuichi Tokunaga, Rei Nakagawa, Satoshi Ohzahata, Ryo Yamamoto, and Toshihiko Kato. A content registration method for ccn routers with blockchain. In 2020 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), pp. 1–2, 2020
- [7] 電子情報通信学会情報指向ネットワーク技術特別研究専門委員会, “ICN/CCN 通信を実現するソフトウェアプラットフォーム cefore,” 参照日 2023/9/9 https://www.ieice.org/cs/icn/?page_id=1208
- [8] Ethereum Foundation, “web3.py” 参照日2023/10/28 <https://web3py.readthedocs.io/en/stable/index.html#>
- [9] 大岡 睦, 朝枝 仁. “Cefpyco : Cefore アプリケーション開発用 Python パッケージ” 参照日:2023/10/29. <https://www.ieice.org/~icn/wp-content/uploads/2020/09/a-ooka2019ICN-cefpyco.pdf>