

ICNにおける個別鍵配送を用いたアクセス制御方式

1. 研究の背景

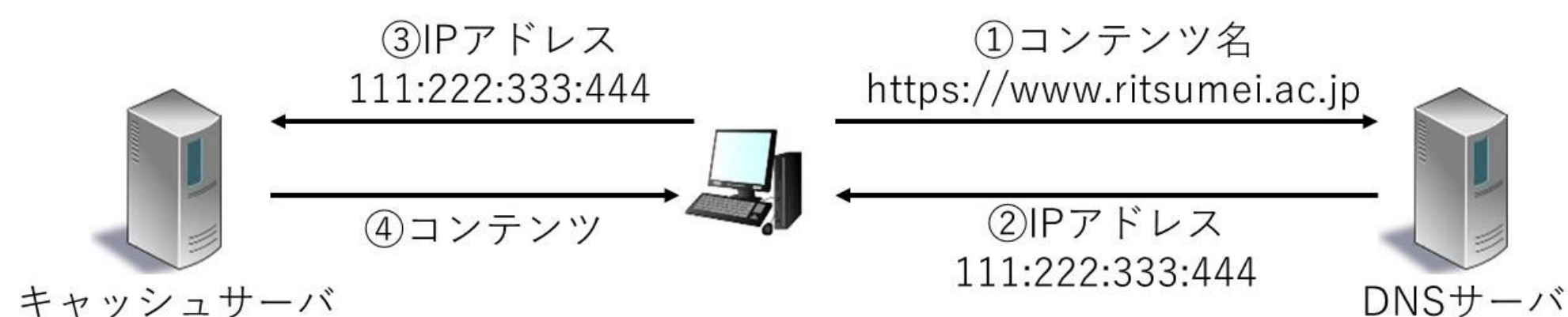
■ 現在のIPネットワーク

■ Domain Name System (DNS)

- コンテンツの名前をDNSサーバに問い合わせることでIPアドレスを取得(名前解決)

■ Content Delivery Network (CDN)

- 要求ユーザの位置に基づき、近くに存在するキャッシュサーバからコンテンツを配信



■ IoTでの問題点

- コンテンツ名が温度や位置情報といった曖昧な名称になるためDNSサーバによるIPアドレス解決が困難

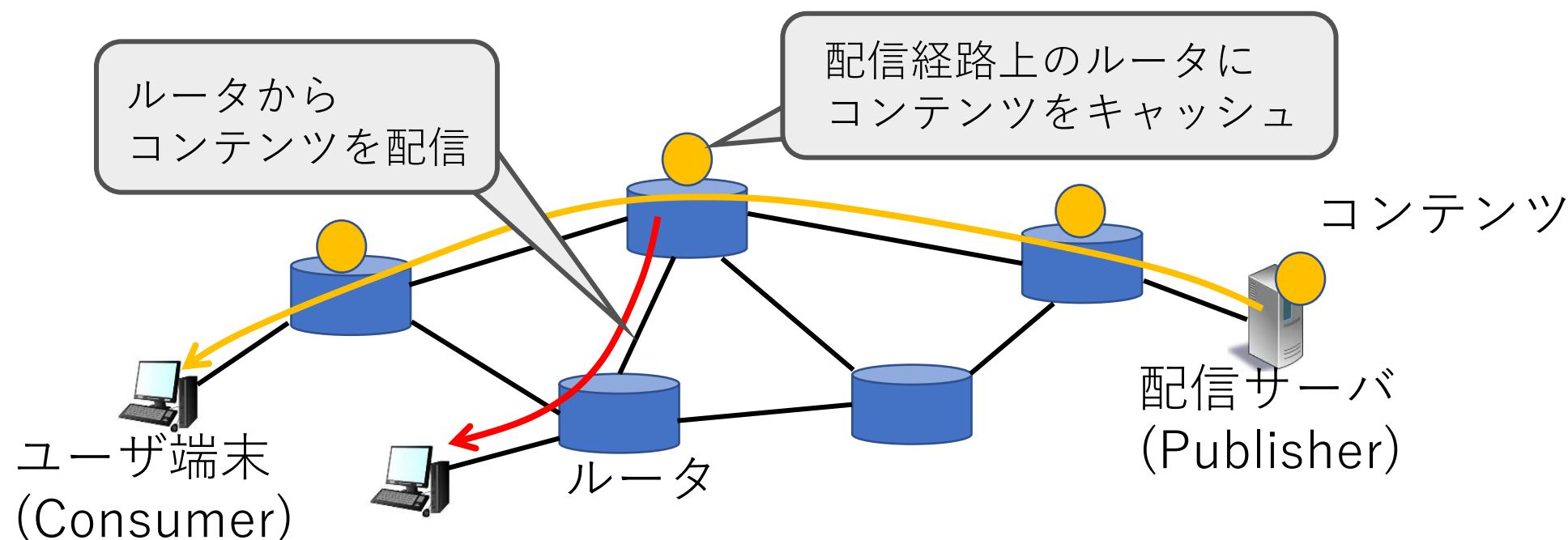
■ 情報指向ネットワーク (ICN: Information-Centric Networking)

■ コンテンツ名によるルーティング

- DNSによる名前解決が不要

■ ルータがコンテンツをキャッシュ

- 他ユーザからの要求も、コンテンツのあるサーバまで到達せずに取得



■ アクセス制御の問題点

- コンテンツがルータ上にあるため、コンテンツ要求を行っても配信サーバへたどり着く前にコンテンツが配信
- IPネットワークのように**配信サーバ上でアクセス制御を行うことが困難**

研究の目的

- ICNで配信サーバでのアクセス制御を行う手法の提案

2. 提案方式の特徴

■ コンテンツ単位でアクセス制御

- 要求されたコンテンツ毎にアクセス制御を行うため各コンテンツを各々異なる共通鍵で暗号化

■ CPF (Cache Permission Flag)

- コンテンツのキャッシュ可否を指定できるフラグ

■ 初回Interest

- コンテンツ要求前に事前に送る要求
- CPFを利用することで常に配信サーバまで到達

■ アクセス制御

- 初回Interestにより配信サーバに到達し、ユーザ認証

■ コンテンツ鍵の配布

- 初回Interestの応答パケットでの要求コンテンツの鍵を配布

3. 提案方式の動作

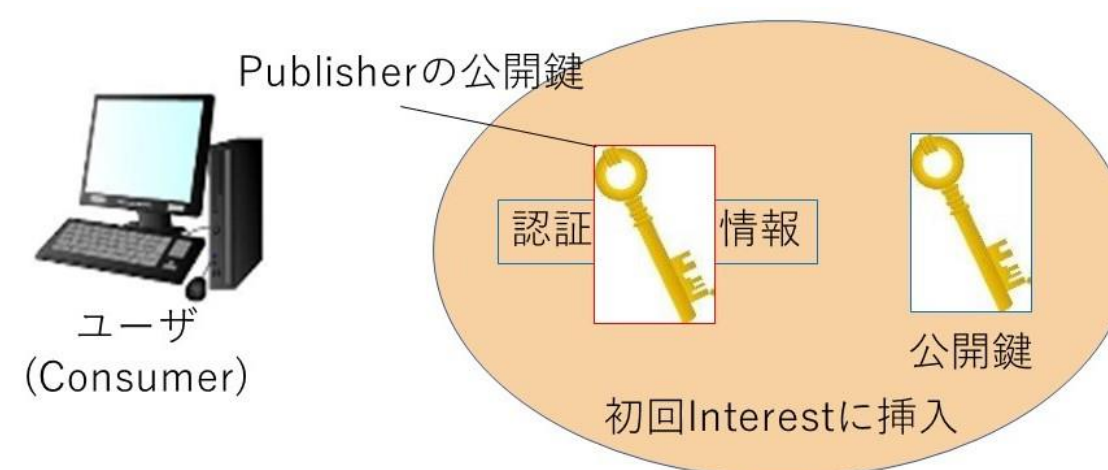
■ 配信サーバ側の準備

- 公開鍵と秘密鍵、各コンテンツ用の共通鍵の用意



■ ユーザ側の準備

- 初回Interestに自身を認証してもらうための情報の挿入
- 初回Interestに自身の公開鍵の挿入

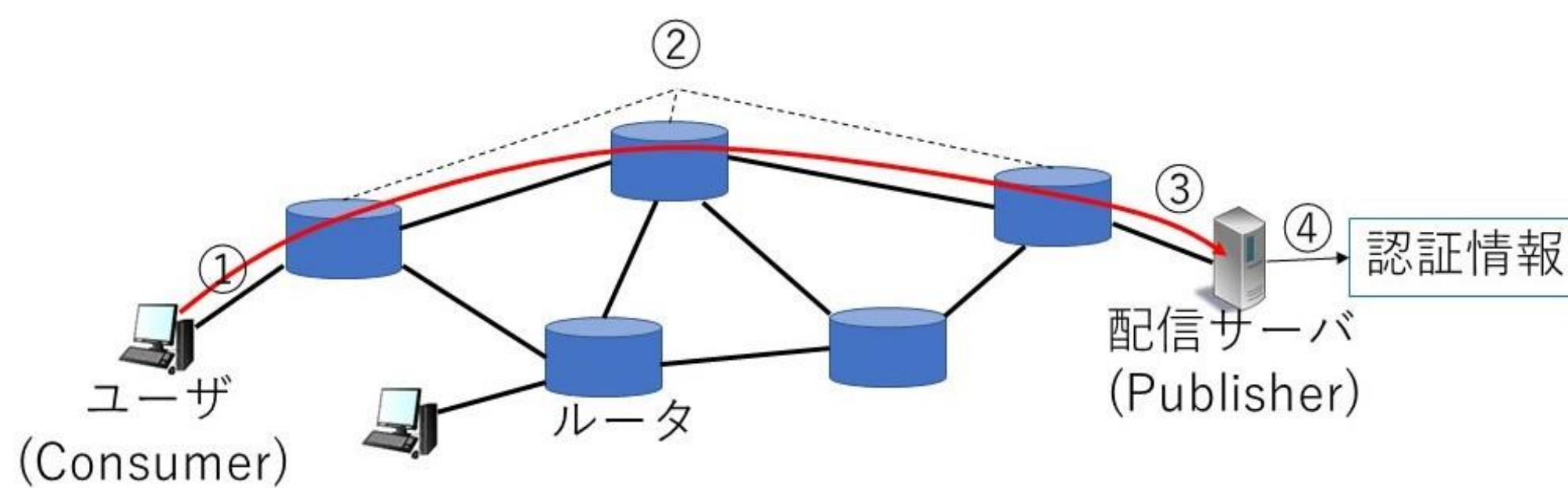


①ユーザは初回Interestを送信

②初回Interestの応答コンテンツはルータ上に存在しない

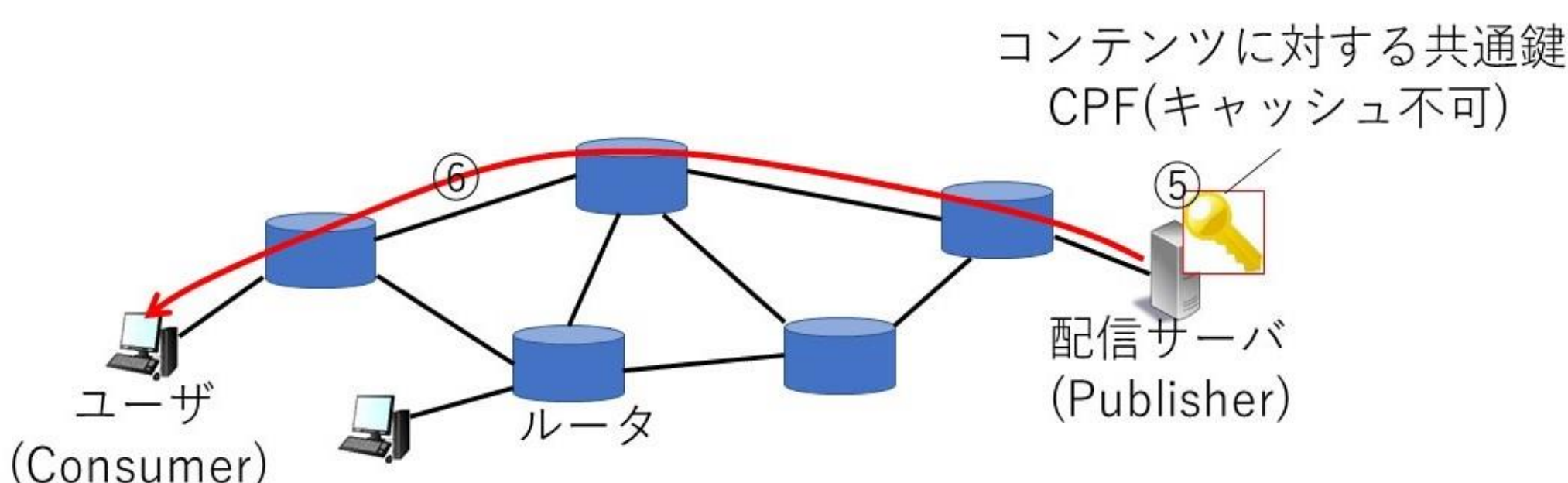
③配信サーバへ到達

④配信サーバで要求ユーザの認証



⑤配信サーバが要求されたコンテンツに対応する共通鍵をCPFをキャッシュしないように設定し返送

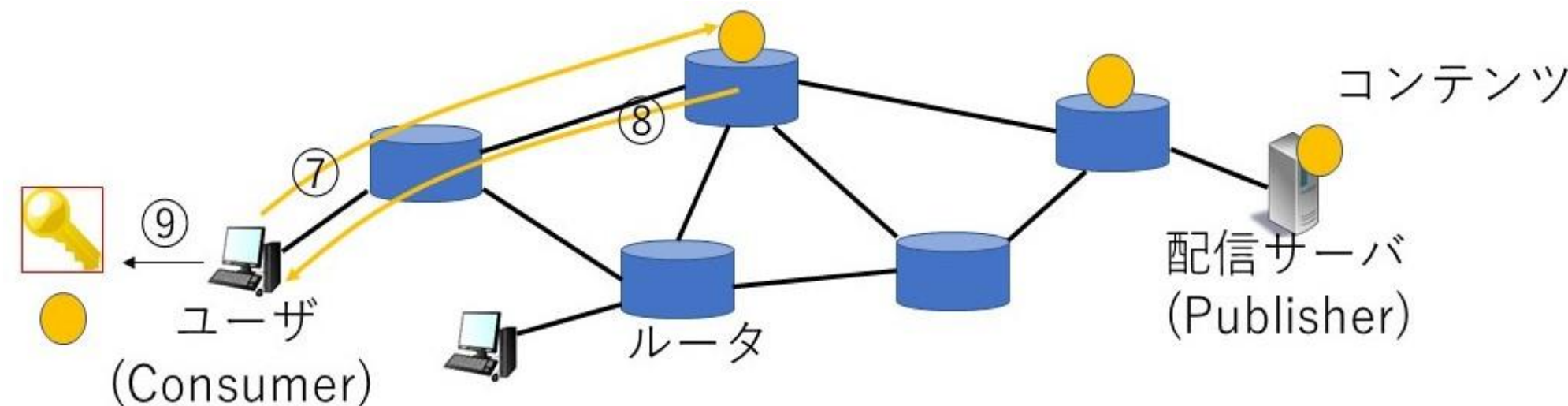
⑥ルータ上に共通鍵がキャッシュされずにユーザへ到達



⑦コンテンツ要求のためのInterest送信

⑧コンテンツがルータ(もしくは配信サーバ)から返送

⑨コンテンツを復号



4. 今後の予定

- 実際のネットワークポロジを作成しシミュレーション評価