P2P SIP解説

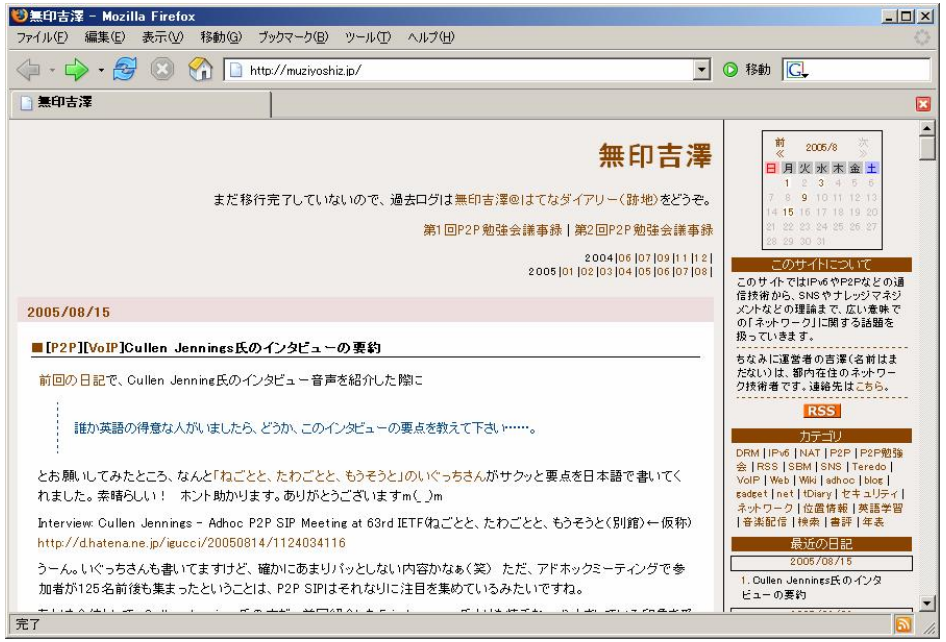
2005/9/3

吉澤

http://muziyoshiz.jp/

自己紹介

- **無印吉澤**
  http://muziyoshiz.jp/



“P2P”と“SIP”

- P2P (Peer-to-Peer)
  - Peer = 「仲間、同等の人」
  - 中央サーバの機能を、個人のPCに分散する技術
  - Napster, Gnutella等のファイル共有ソフトで注目
- SIP (Session Initiation Protocol)
  - IP電話 (VoIP) を実現する標準プロトコルの1つ
  - SIPサーバがアドレス登録、呼び出しの機能を提供

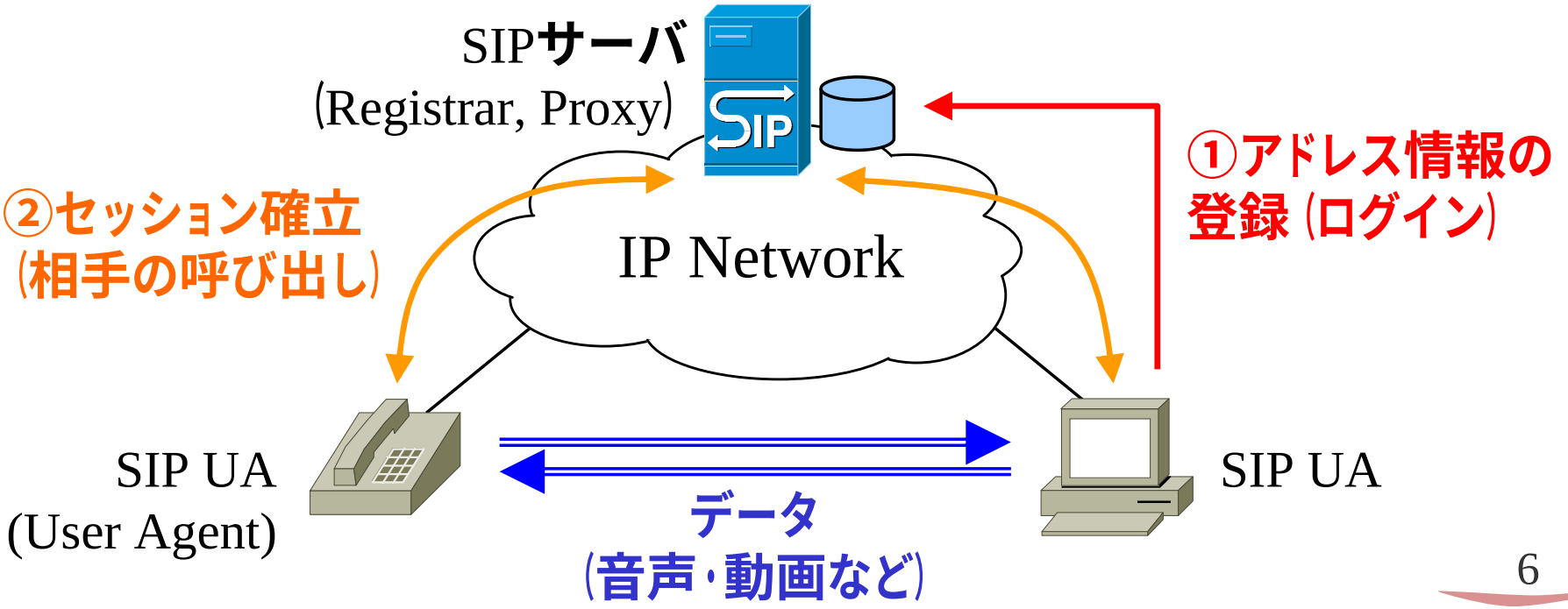
- P2P SIP
  - SIPサーバの機能を分散し、拡張性、耐障害性を向上
  - オープンなプロトコル、既存のSIP技術を流用可能

目次

目次

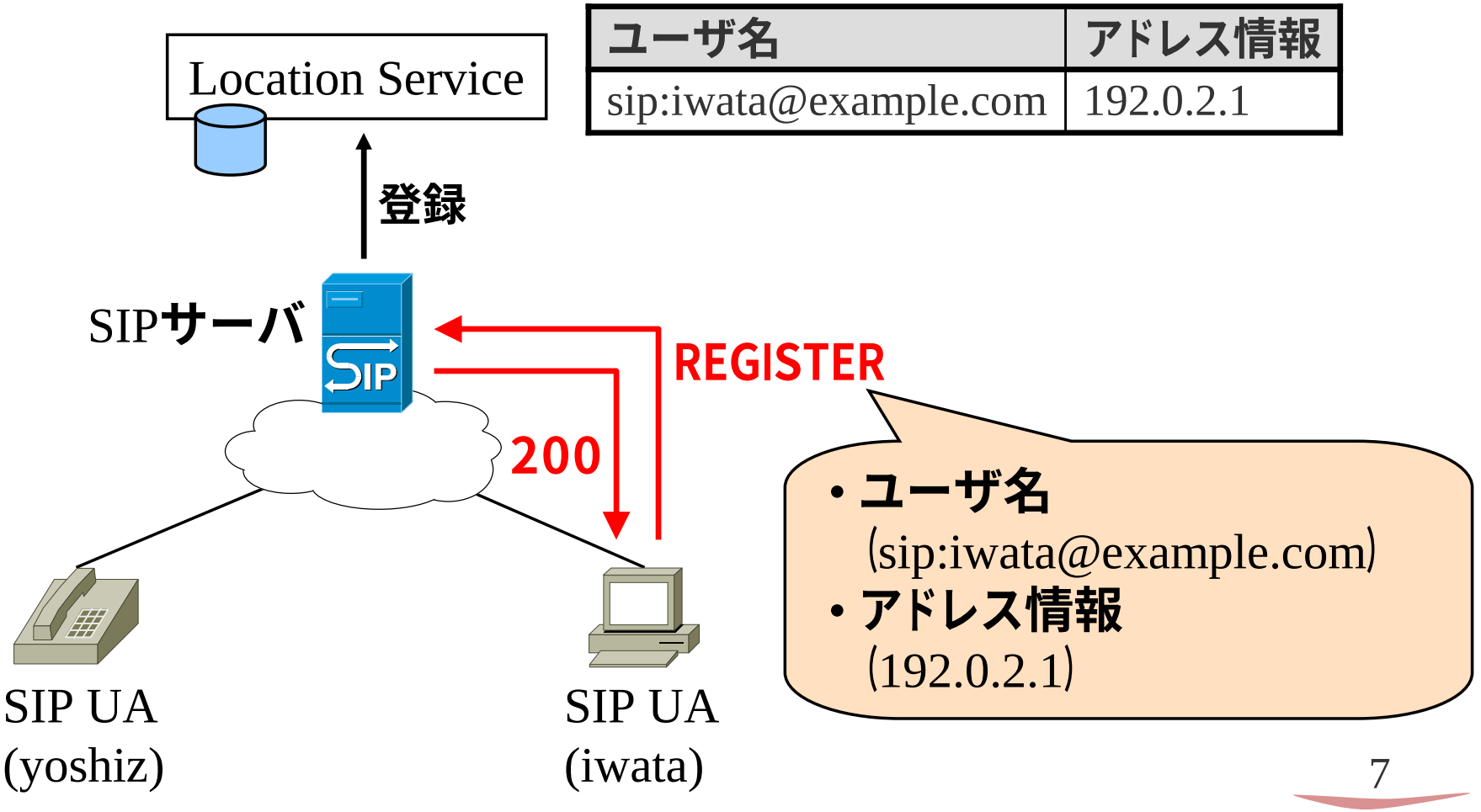
SIP(Session Initiation Protocol)

- IETF（Internet Engineering Task Force）**が標準化**
- **単純で、拡張性の高いIP電話プロトコル**
  - HTTP**に似たテキストベースの呼制御メッセージ**
  - **セッション確立の手順が単純**



SIPサーバの機能

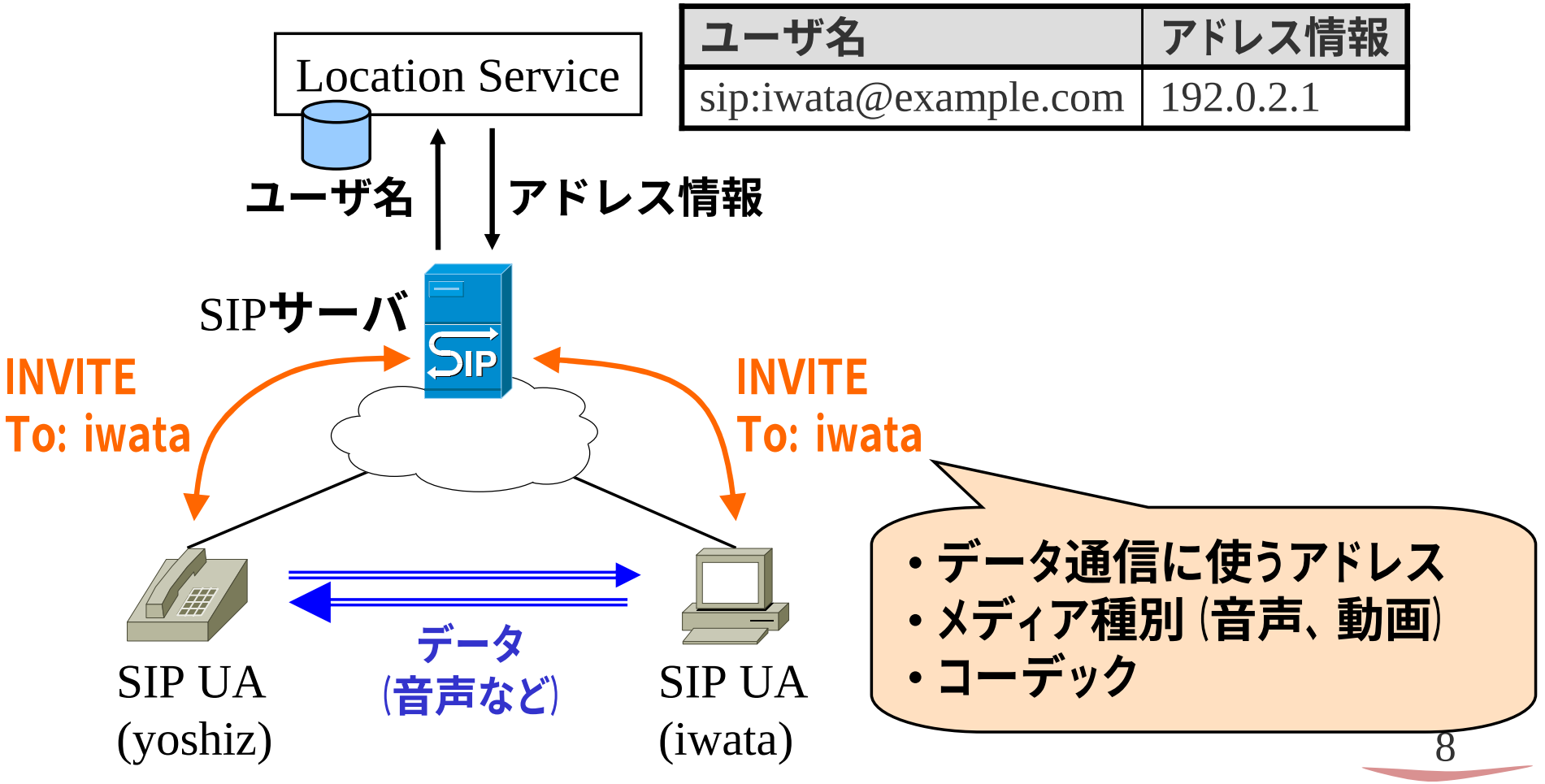
① アドレス情報の登録（ログイン）



ユーザ名	アドレス情報
sip:iwata@example.com	192.0.2.1

SIPサーバの機能

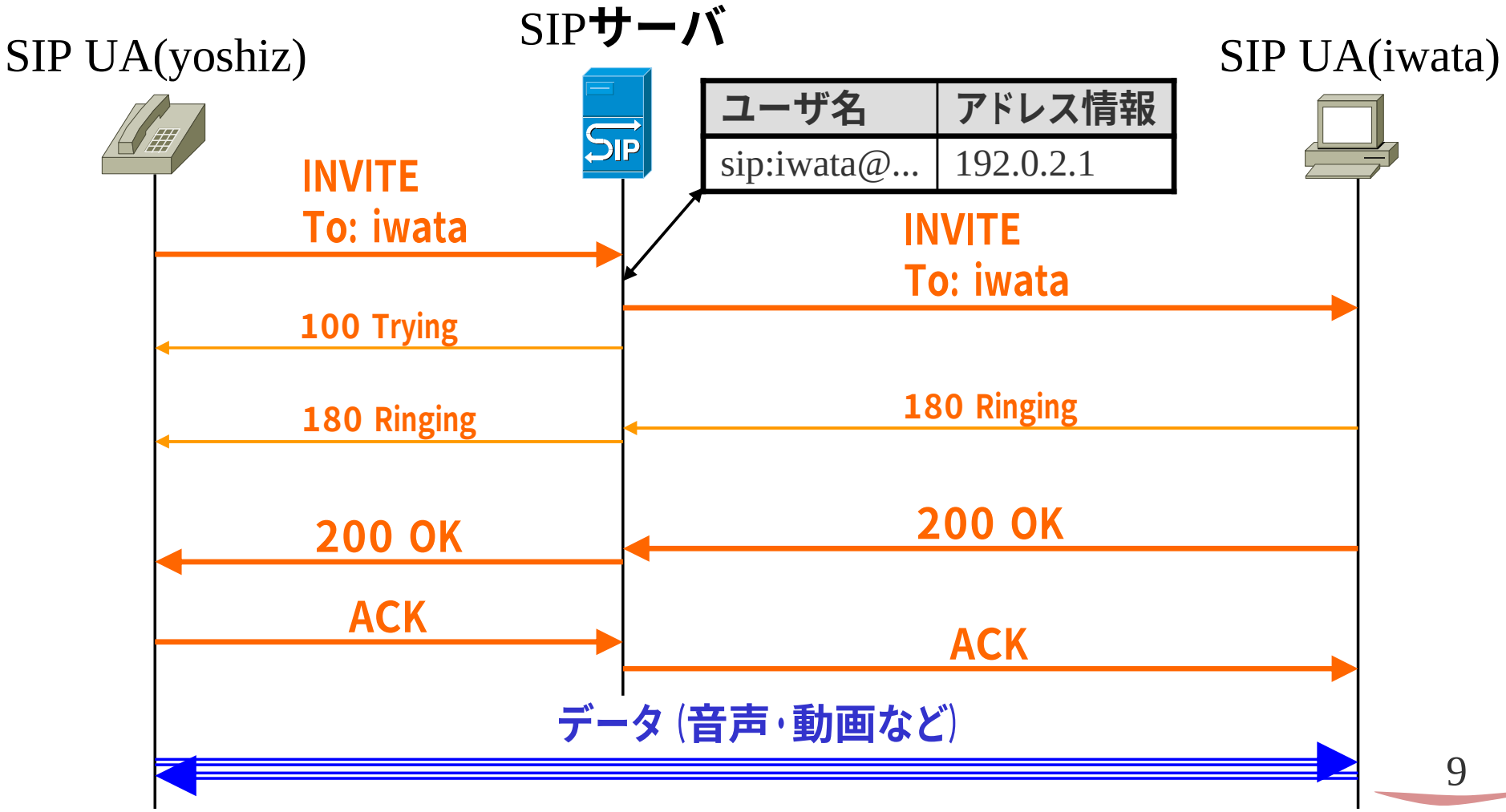
② セッション確立（相手の呼び出し）



ユーザ名	アドレス情報
sip:iwata@example.com	192.0.2.1

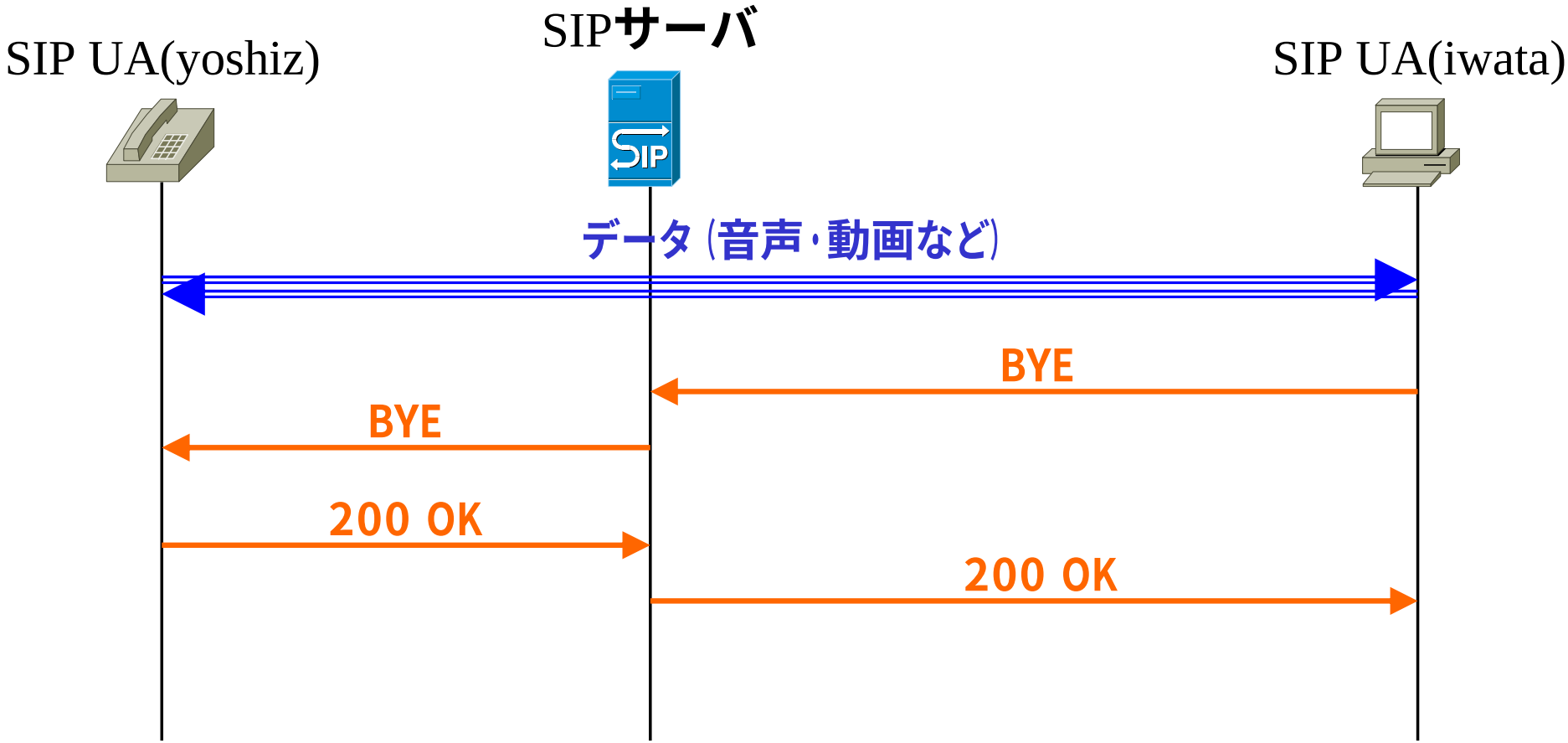
SIPの基本シーケンス

- セッション確立時



SIPの基本シーケンス

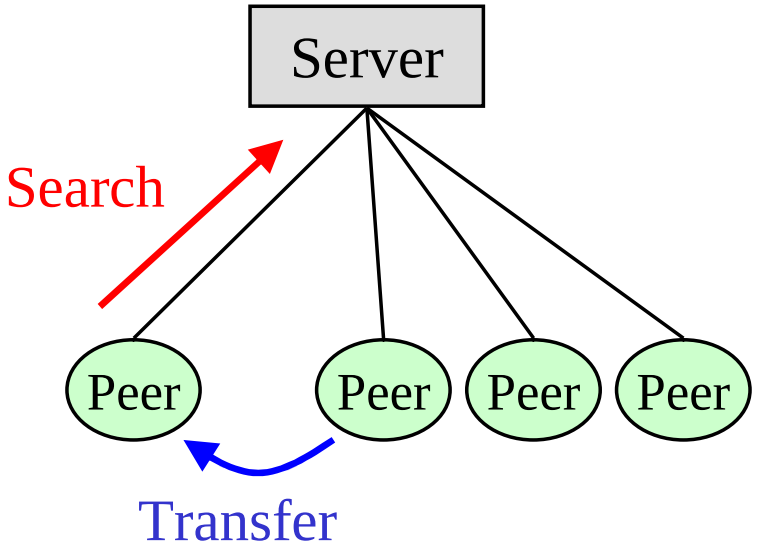
- セッション終了時



目次

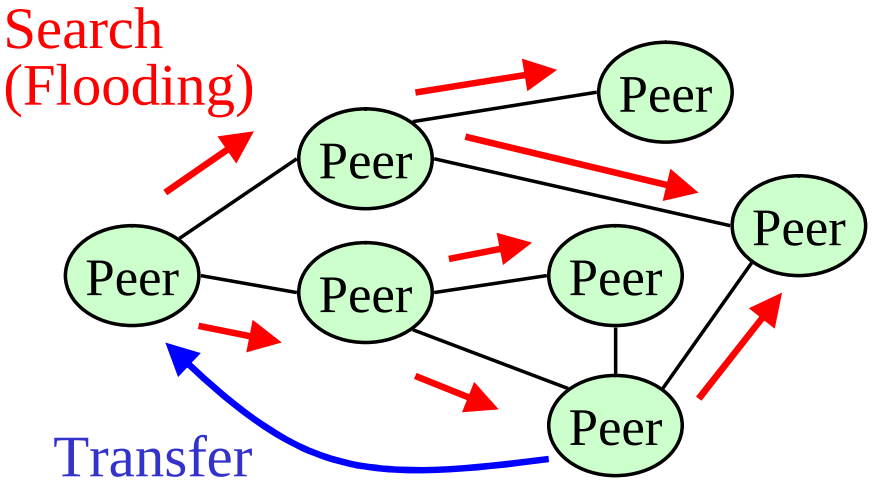
初期のP2P技術

Hybrid P2P
(ex. Napster)



- **サーバが単一障害点**
  (Single Point of Failure)

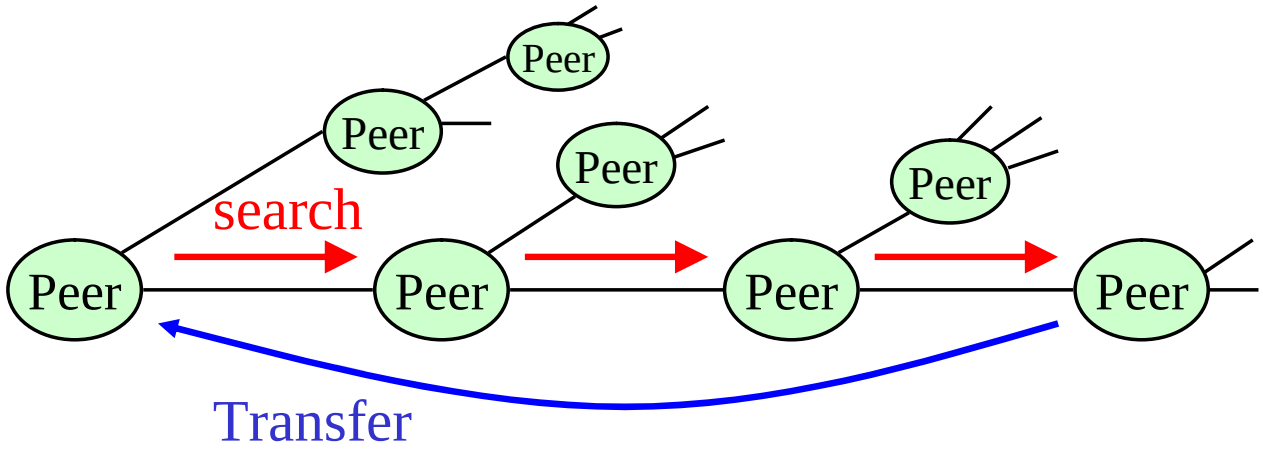
Pure P2P
(ex. Gnutella, Freenet, Winny)



- **ノード数が増加すると、検索メッセージ数が急増**
- **検索がどれくらいで終わるか保証できない**

DHT(Distributed Hash Table)

DHT
(ex. Chord, CAN, Pastry, Tapestryなどのアルゴリズム)

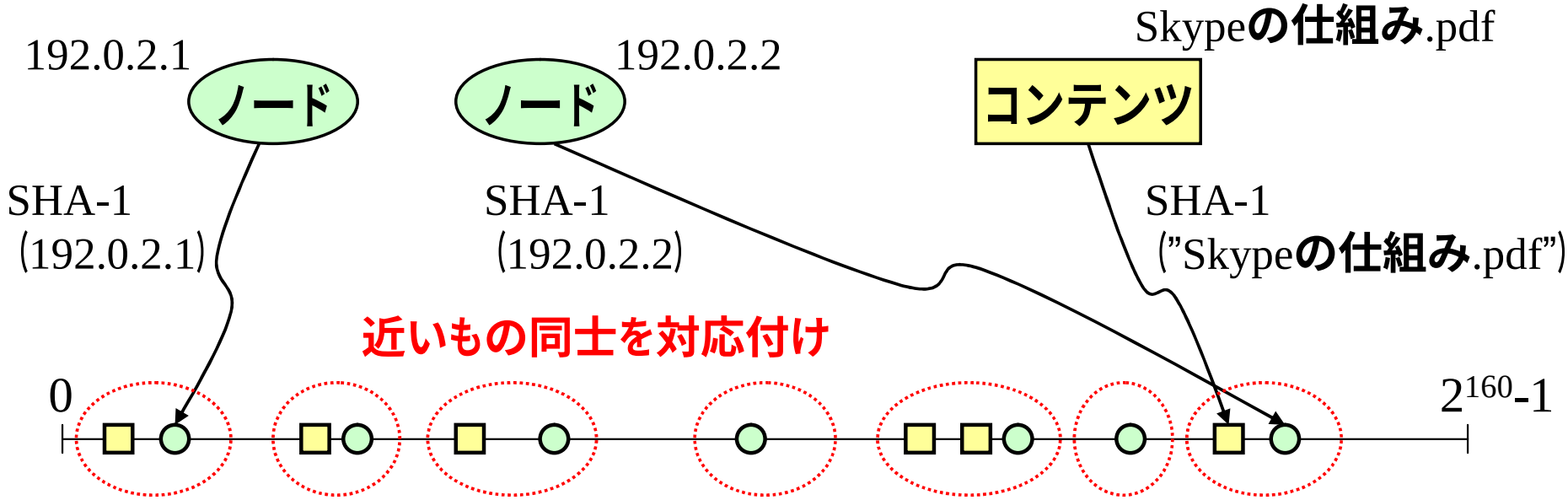


- ノード数が増加しても、検索メッセージ数は急増しない
- コンテンツが存在しない場合、それが明確に分かる
  - 平均探索数は、DHTアルゴリズムに依存
    例：Chordの場合はO(logN)　(Nはノード数)

DHTの特徴

- **特徴1**
  ハッシュ関数を用いて、ノードとコンテンツを対応付け

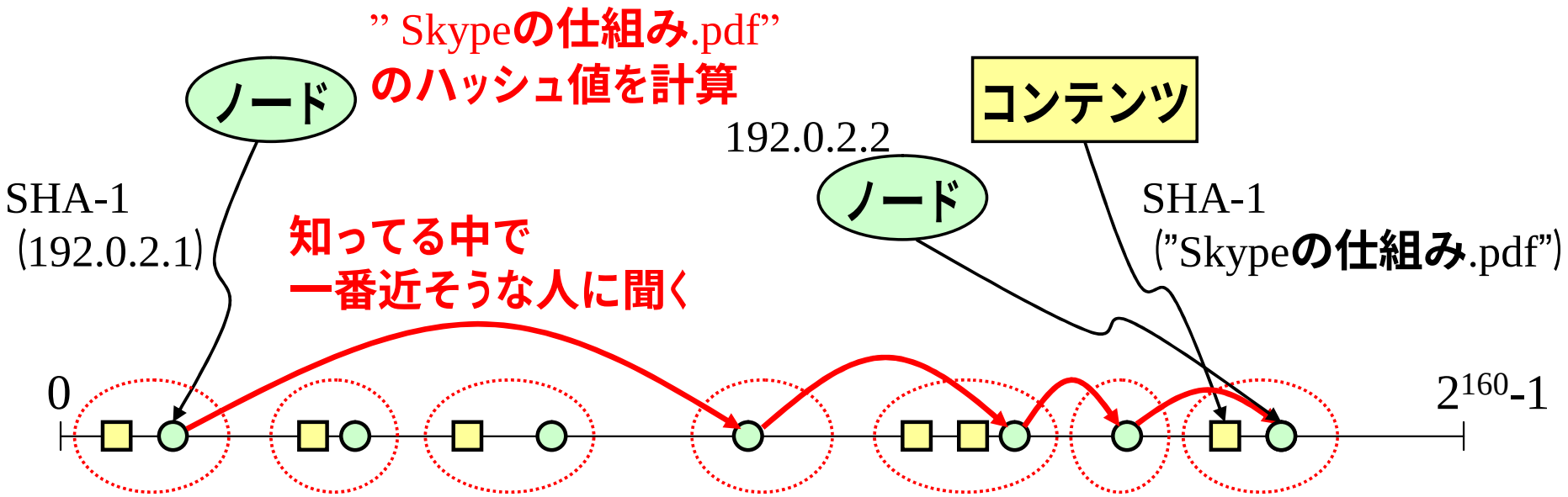
  ※ハッシュ関数
  文字列などのデータを与えると、決まった範囲の値を返す関数
  （例：SHA-1は、返り値が160ビットなので0～ 2^{160}-1の範囲）



DHTの特徴

- **特徴2**
  局所的な知識を持つノードが協調動作して探索
  （近くの情報は細かく、遠くの情報はおおざっぱに）

例：192.0.2.1のノードがファイル名”Skypeの仕組み.pdf”を検索

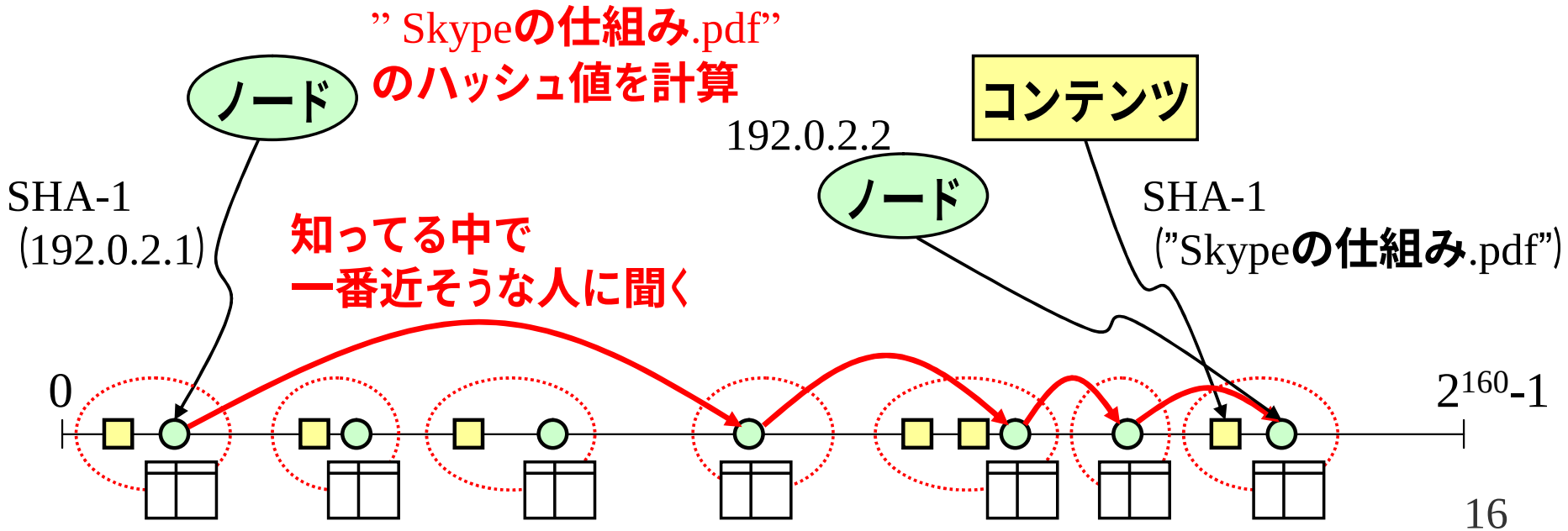


DHTの特徴

- **特徴2**
  局所的
  (近くの

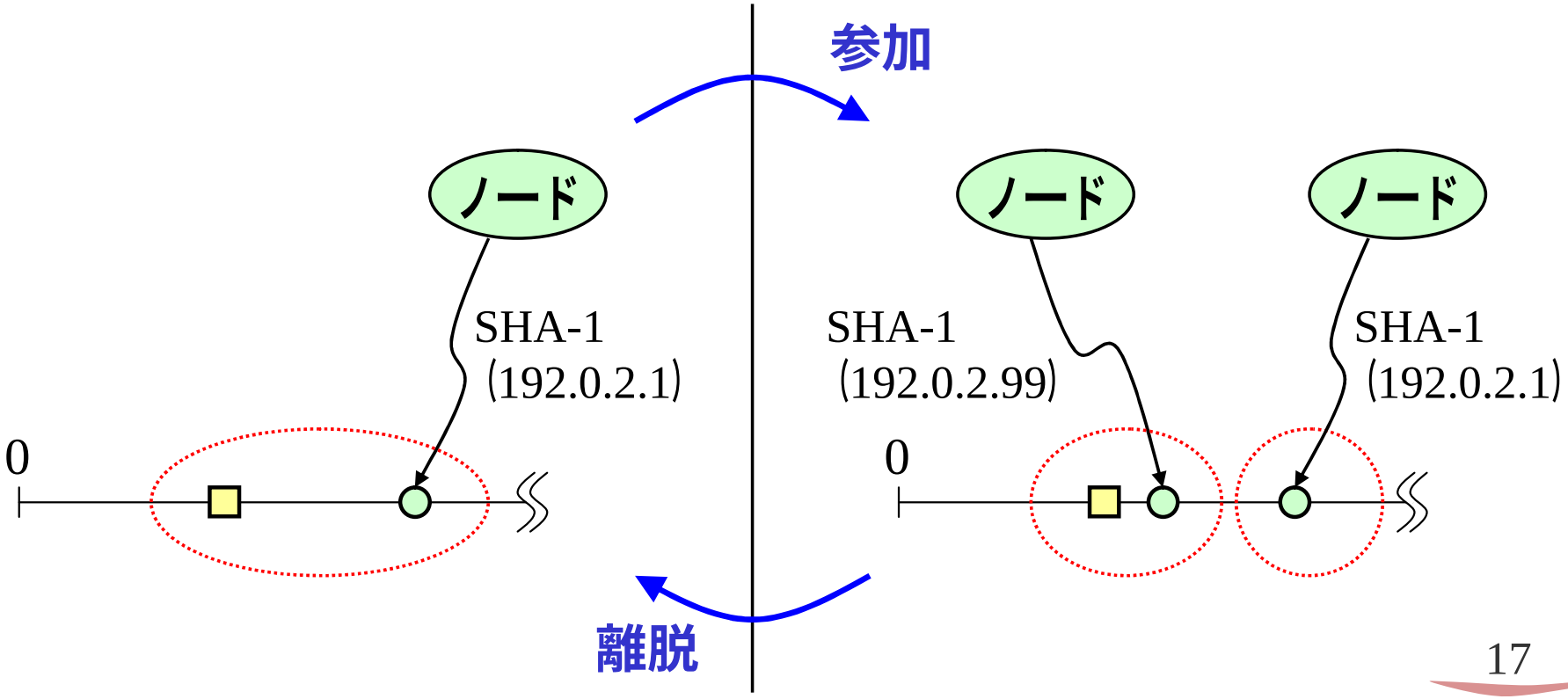
例：192.

- **ハッシュ値とノードの関係を表すテーブルを管理**
  →分散ハッシュテーブル
- **検索結果はコンテンツ** or **その位置情報**
- **名前が厳密に一致していないと検索失敗**



DHTの特徴

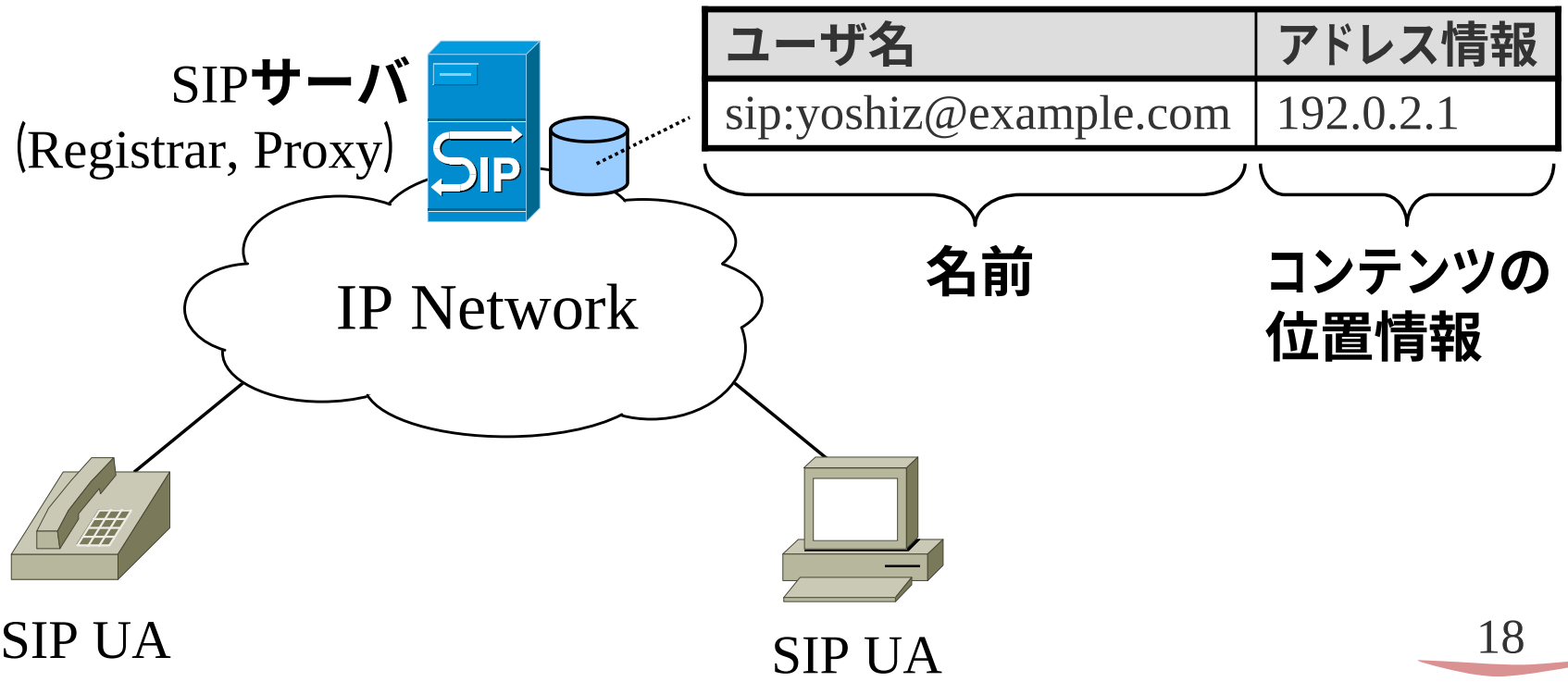
- **特徴3**
  ノードの参加、離脱時に、コンテンツの引き継ぎと近隣ノードのハッシュテーブル更新が必要



SIPとDHT

- SIP（VoIP）**に必要なのは、単純な名前解決**
- **リアルタイム通信のため、名前解決の速度が重要**

→ DHT**は、**SIP**の**Location Service**に適している**



目次

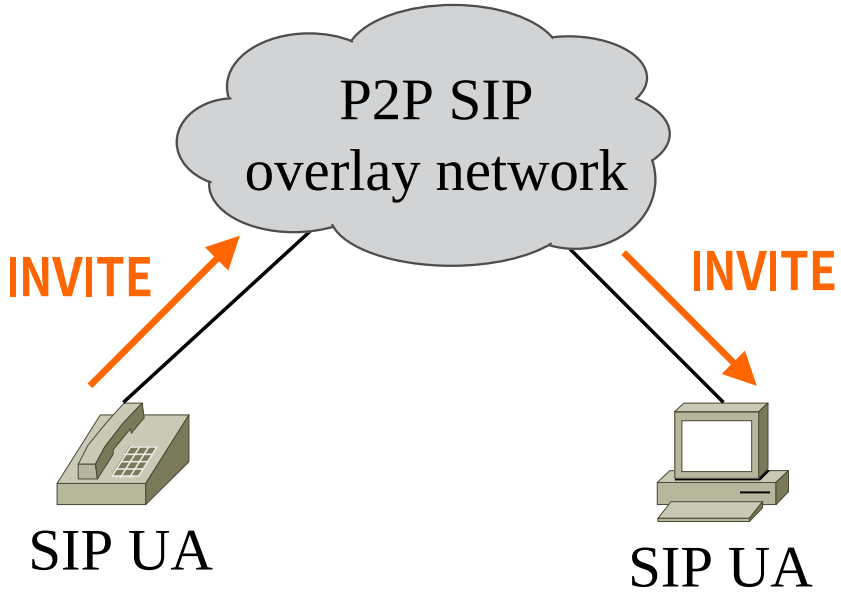
P2P SIPに関する提案

- P2P SIPのモデル
  - P2P over SIP
    - D. A. Bryan(College of William and Mary)
    - K. Singh and H. Schlzrinne(Columbia University)
  - SIP using P2P
    - A. Johnstons(MCI)

- 最初の論文は2003年12月（P2P over SIPの提案）
- 2005年初頭からIETFのSIPPING WGで議論が活発化

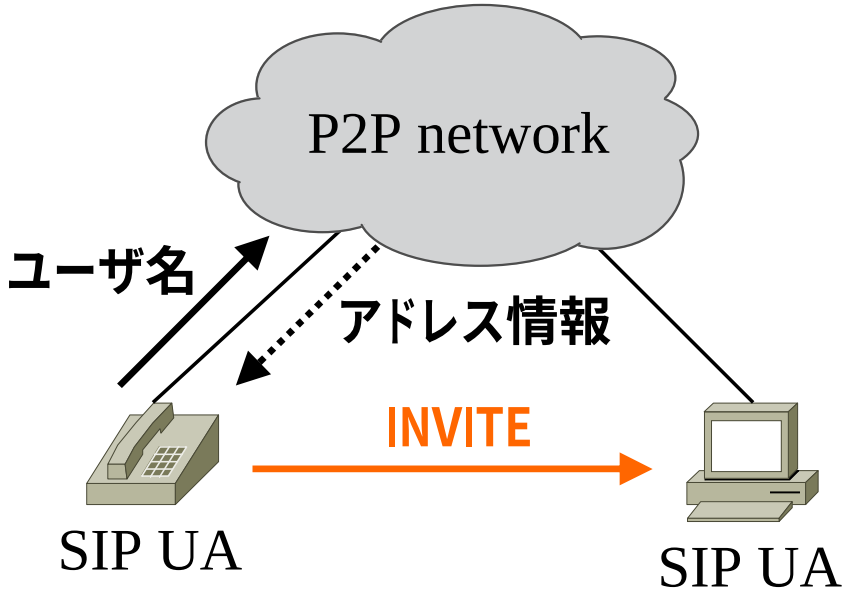
P2P SIPのモデル

P2P over SIP



- SIPメッセージを用いて
  P2Pプロトコルを実装
- Chord over SIPの提案あり

SIP using P2P

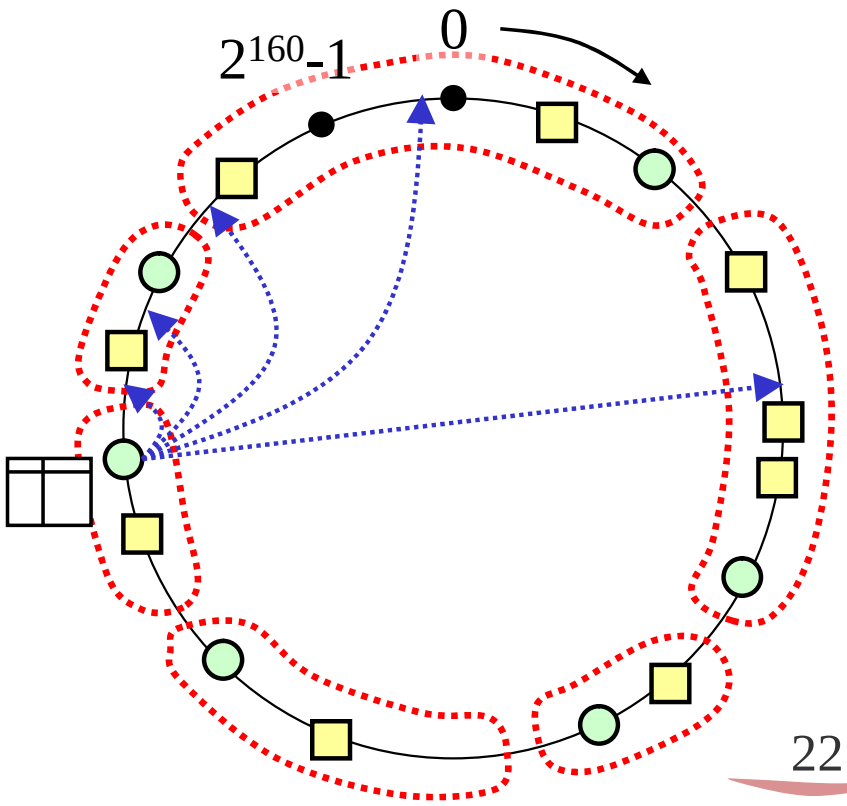


- SIPのLocation Serviceのみ
  P2Pプロトコルで置き換え

Chord

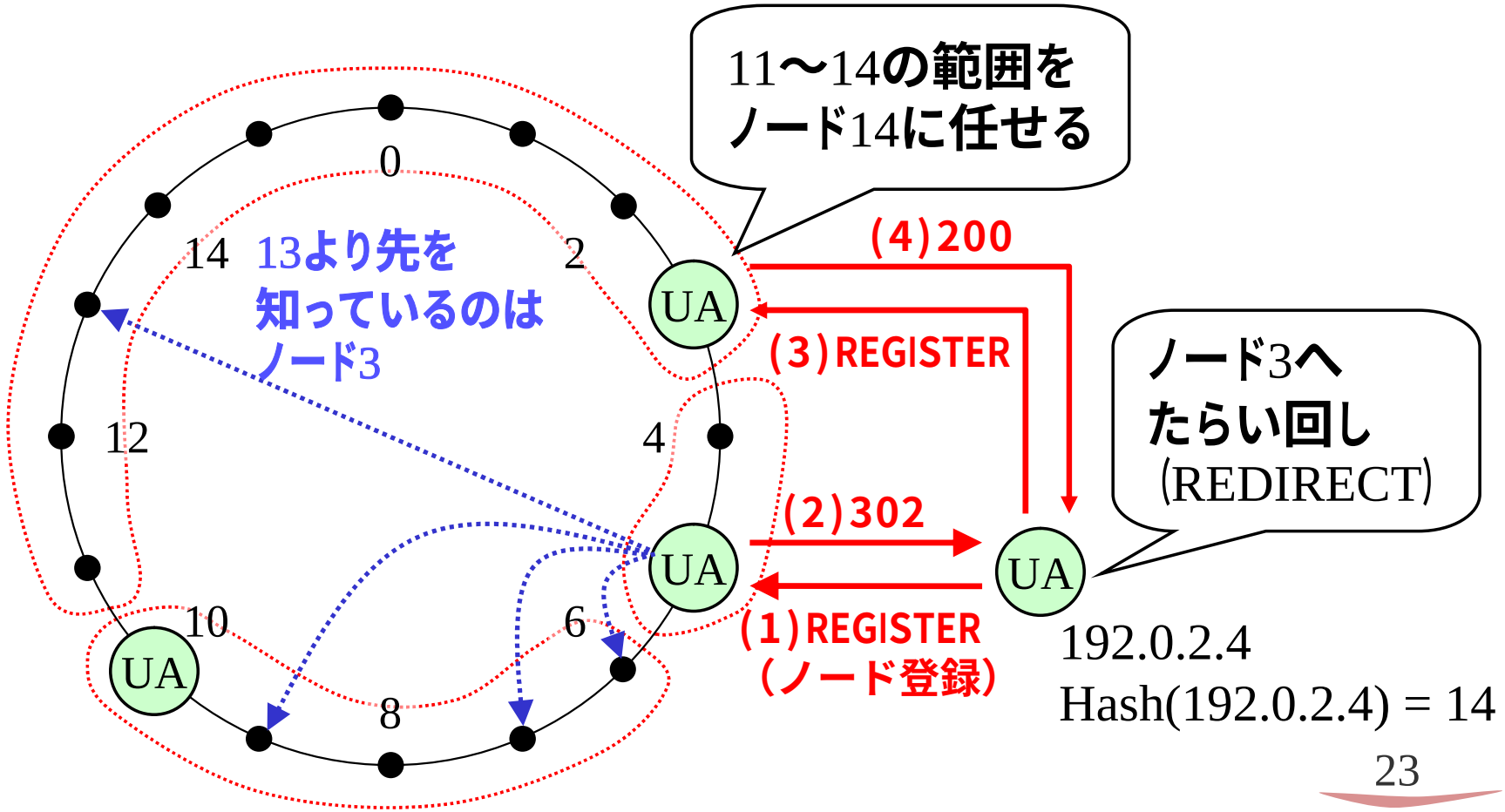
- 一次元座標をリングにした、比較的単純なDHT
  - ハッシュ関数はSHA-1 (Secure Hash Algorithm 1) を使用
- 2001年に発表 (同時期にCAN,Pastry,Tapestryも)

- ハッシュ値が自ノードより小さいコンテンツを管理
- $2^0, 2^1, ..., 2^{m-1}$だけ先の座標を管理しているノードを事前に調べておく
  (mはハッシュ値のビット数)
  → “finger table”



P2P over SIPの動作

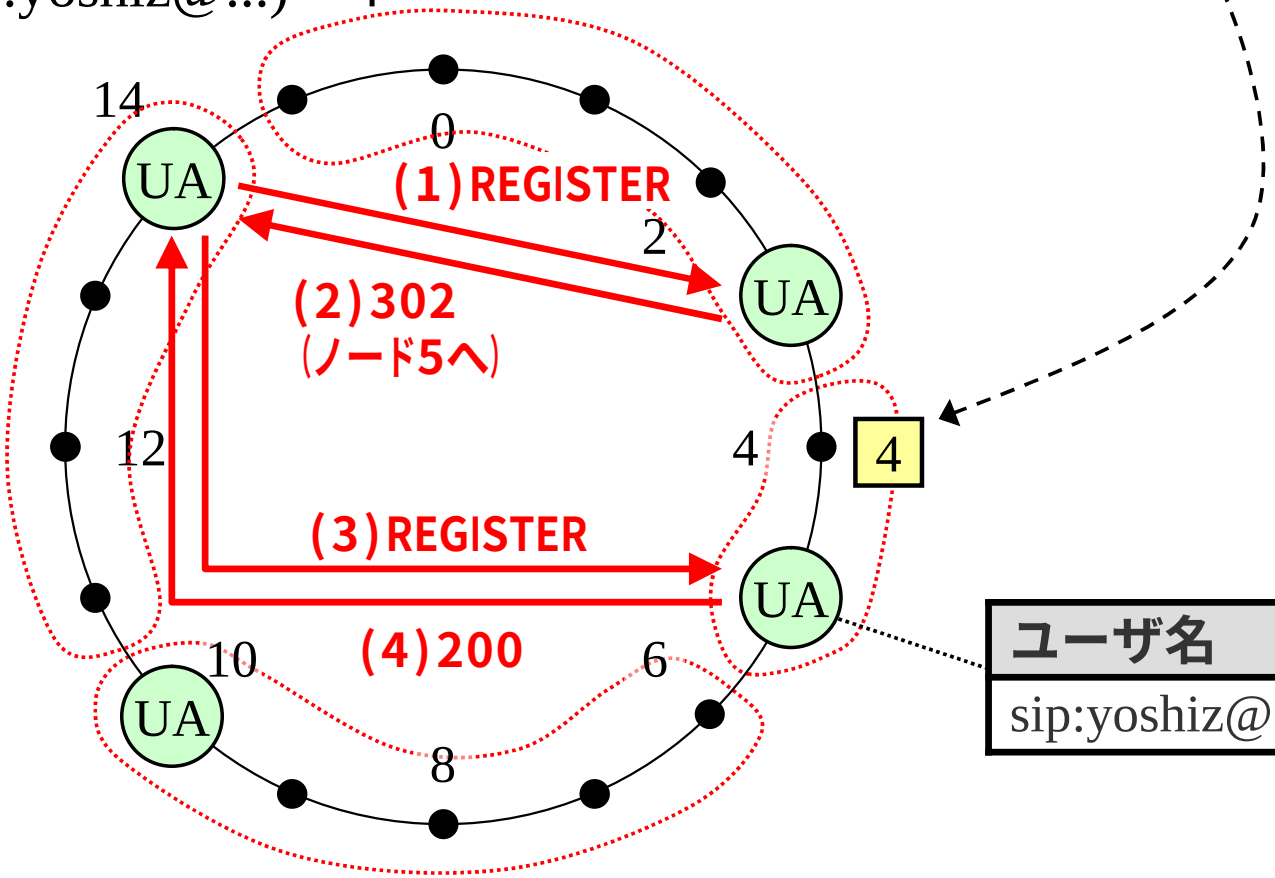
① P2P (Chord) ネットワークへの参加
(ハッシュ値が0～15の範囲の動作例)



P2P over SIPの動作

② アドレス情報の登録

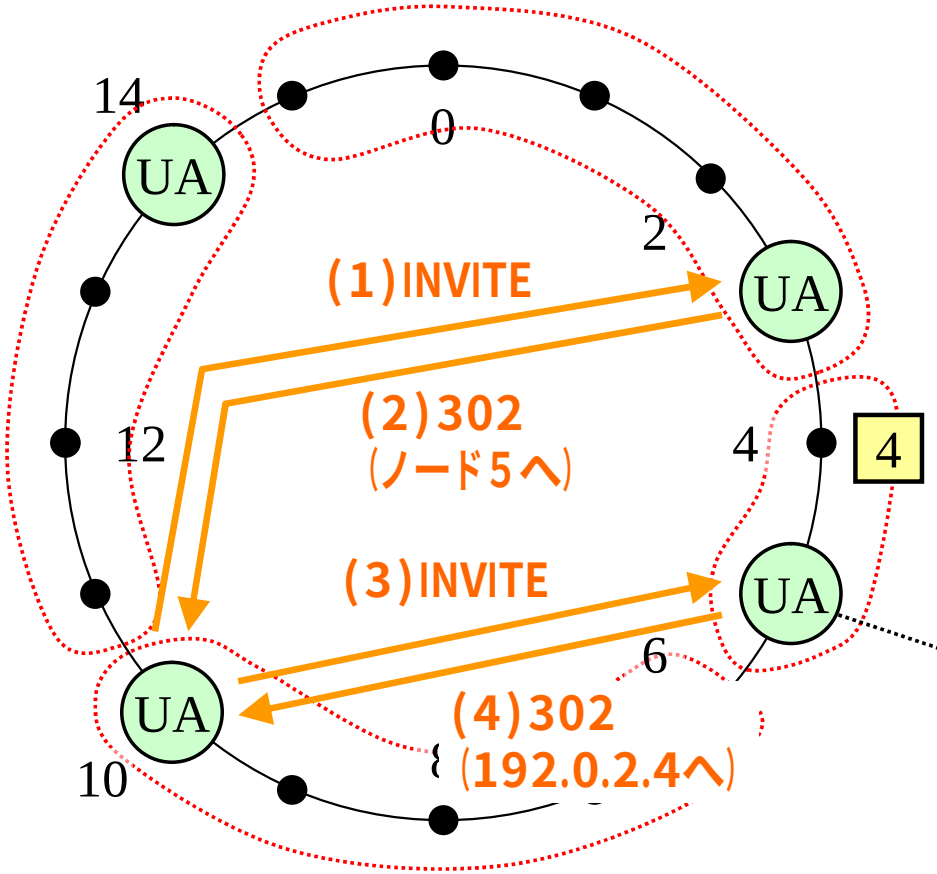
sip:yoshiz@example.com
Hash(sip:yoshiz@...) = 4



ユーザ名	アドレス情報
sip:yoshiz@...	192.0.2.4

P2P over SIPの動作

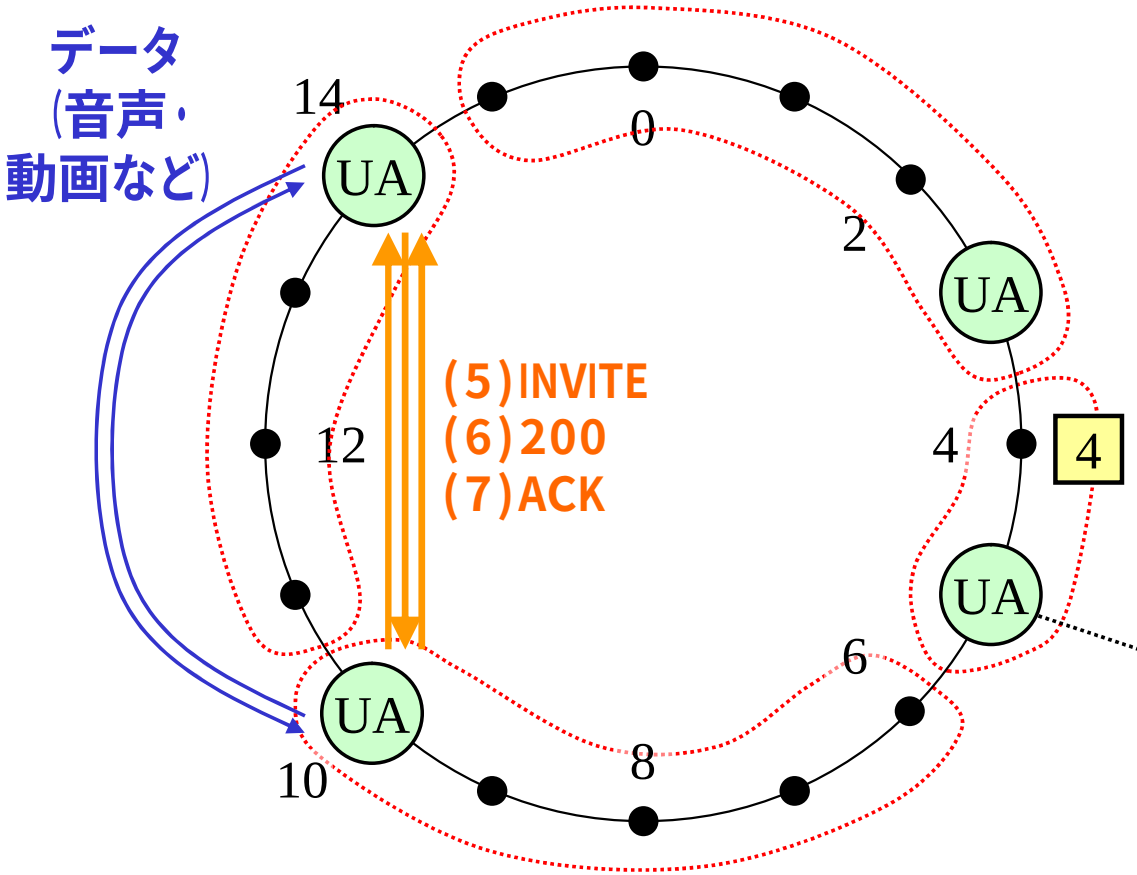
③ セッションの確立
（ノード10からsip:yoshiz@example.comを呼び出し）



ユーザ名	アドレス情報
sip:yoshiz@...	192.0.2.4

P2P over SIPの動作

③ セッションの確立
（ノード10からsip:yoshiz@example.comを呼び出し）



ユーザ名	アドレス情報
sip:yokota@...	192.0.2.4

SIP using P2P

- 具体的な提案はまだ
- P2P over SIPを推奨しない理由
  - SIP独自である
    - このようなLocation Serviceは、SIP以外にも応用できる
  - REGISTER本来の意味と違う
    - REGISTERは本来RegistrarとSIP UAの間でのみ使われる
    - REGISTERのリダイレクトは一般的でない
      (REGISTERの中継を許すことによるセキュリティの問題)
  - SIPによるメッセージ転送はオーバヘッドが高い
    - テキストメッセージ
    - トランザクション状態の管理

その他の提案

- Industrial-Strength P2P SIP (Nimcat Networks)
  - P2P SIPへの要求
  - 既存のVoIPと同等のサービスを提供するために必要な機能
    - 異機種ネットワークのサポート
    - 不在端末への呼び出し (call forwarding, voicemail)
    - ネットワークを複数のゾーンに分割
    - ネットワーク管理機能の提供
    - セキュリティ
  - P2P LayerとSIP Layerは分離すべき

目次

P2P SIPの課題

- 技術的な課題
  - ユーザ名の一意性
  - セキュリティ
  - NAT越え
- ビジネス的な課題
  - P2P SIPの適用先

ユーザ名の一意性

- 同じ名前のユーザが複数存在する可能性

- ユーザ名の割り当て
  - ユーザ名 (SIP URI) の重複を防ぐためには、名前空間を管理する権威 (Naming Authority) が必要
- ユーザ名の認証
  - ログイン時に、そのユーザ名を使う権利があるかどうかを認証するための認証機関 (Certificate Authority) が必要
  - ログイン後も、他ユーザへの成りすましを防ぐ仕組み

セキュリティ

- メッセージ（DHT, SIP）の経路上に悪意あるノード
  - DoS攻撃
    - メッセージを破棄、または正しくないノードへ転送
  - 成りすまし
  - メディアデータ（音声、動画など）の盗聴
  - 通信履歴の監視（call forwarding含む）
  - voicemailの覗き見

- SPIT（Spam over Internet Telephony）

セキュリティ(対策案)

- DoS攻撃
  - 悪意あるノードを排除する仕組みを持つDHTアルゴリズム(リアルタイム通信に適した評判システム)
  - 任意の座標に侵入できないハッシュ値の計算方法
- 成りすまし、メディアデータの盗聴、voicemailの覗き見
  - 1回目の通話で自己署名証明書を配布(例:SSH)
  - S/MIME、SRTP等で暗号化
- 通信履歴の監視
  - Freenetのような匿名化技術でメッセージの送信者を隠す(?)
- SPIT(Spam over Internet Telephony)
  - ホワイトリスト、ブラックリスト
  - ユーザ名を頻繁に変えられる環境では対処が難しい

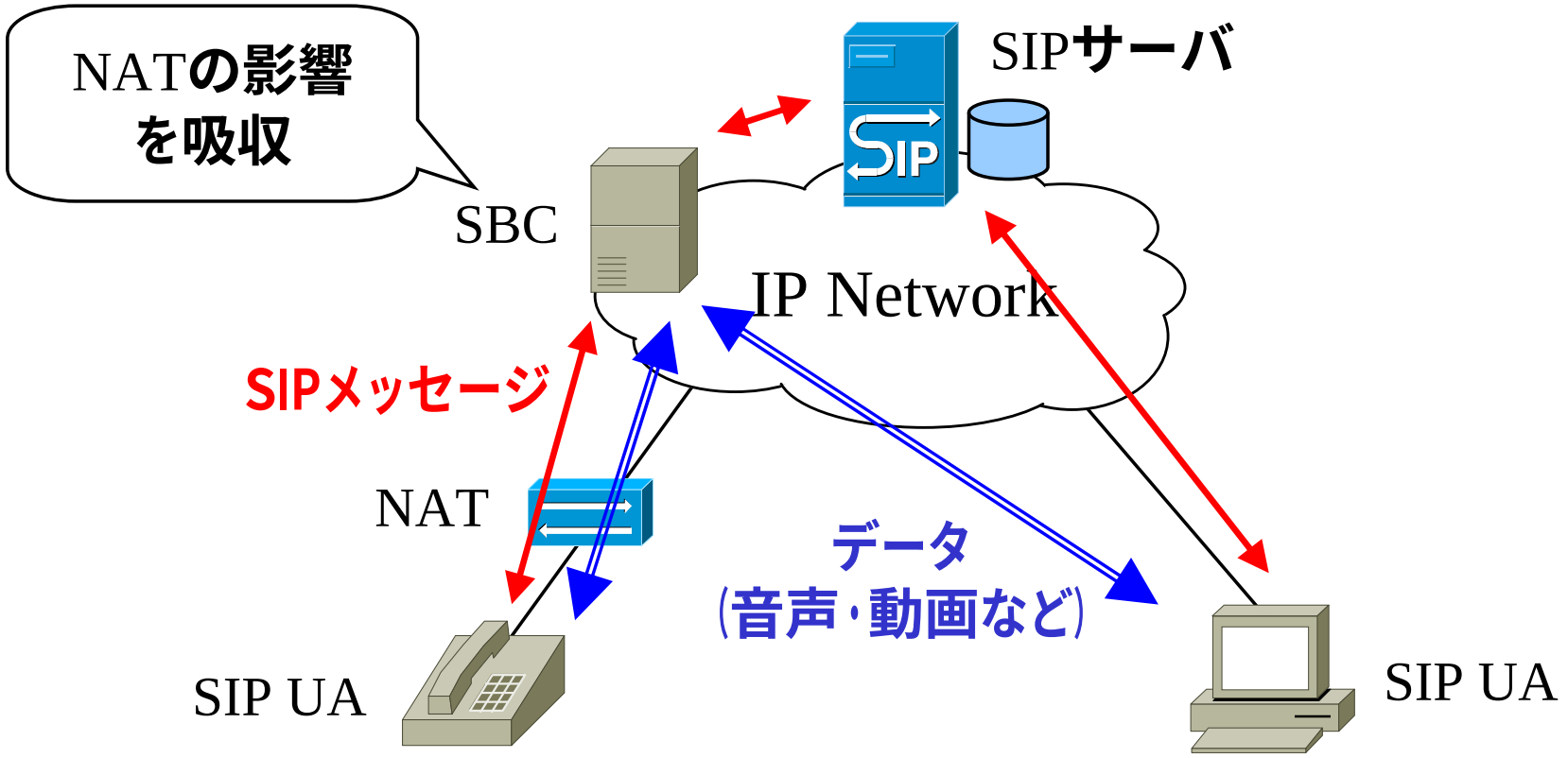
NAT越え

- Skypeのように、他のピアをNAT越えに使う技術は IETFでは提案されていない（SIP、P2P SIP）

- 標準のNAT越え技術
  - UPnP(Universal Plug and Play)
  - STUN(Simple Traversal of UDP through NATs)
  - TURN(Traversal Using Relay NAT)
  - ICE(Interactive Connectivity Establishment)
- P2P通信を試みて、ダメならサーバによるパケット中継 →Google Talkはこのあたりの技術を併用？

SIPにおけるNAT越え

- **専用機器を利用**
  - SIP ALG（Application Level Gateway）
  - SBC（Session Border Controller）



P2P SIPの適用先

- 小規模ネットワーク（家庭内、中小企業）
  - サーバが不要
  - ネットワークに電話機を挿すだけで自動設定
- 大規模ネットワーク（テロ、災害時）
  - 中央サーバと分断された際に、アドホックネットワークを構築
  - 非常時だけの利用で普及する？　SIP機器に組み込み？

- 大規模ネットワーク（コンシューマ向け）
  - Skype, Google Talk(with Gizmo)等と競争？

企業向けP2P VoIP製品

- Nimcat Networks
  - NimX：組み込みP2P VoIPソフトウェア
  - NimXを採用した電話機（Aastra Technologies Ltd.）
  - ネットワーク管理ソフトを無償配布している
    - ボイスメールの通知ソフト
    - nimXシステムをWebブラウザから管理するソフト

- Popular Telephony
  - PeerioBiz：P2P VoIPソフトウェア
  - 過去、Peerio GNUP（VoIPソフトに電話番号）で少し話題に
  - Teledex（サービス業向けPBXベンダ）と戦略的提携関係を結んで製品開発（2005.3）

P2P SIPの可能性

- P2P SIPの標準化
  - 63th IETF peer-to-peer SIP adhoc meeting（2005.8）
  - WG化は未定だが、P2P SIPのMLが作られ、次回（11月）のIETFに向けて議論を進める

- 実用的なP2P VoIPをオープンなプロトコルで再現
  - Naming AuthorityやCertificate Authorityを持ったP2P VoIPの実現方法には、まだ不明な点が多い
  - Skype：ログイン時にサーバが認証
  - 企業向けP2P VoIP：証明書ベースで周囲のピアが認証（？）
  - ビジネス面は不明だが、研究としては有意義

まとめ

- SIPにP2P技術（特にDHT）を適用して、サーバをなくす試みが注目を集めている→P2P SIP
- SIPのユーザ名-IPアドレス解決（Location Service）を、DHTで実装することで拡張性を実現
- P2P over SIPモデルのプロトタイプ実装が存在する（ChordというDHTを利用）
- P2P VoIPは有用だが、内部動作はまだ不明な点が多く、オープンな研究はこれから