インターネット数理科学第13回

～P2Pテクノロジーと今後の展望～

2007年1月25日

株式会社インターネット総合研究所代表取締役所長
東京大学大学院数理科学研究科客員教授

藤原　洋

目　　次

1．P2P技術の世界

P2Pとは？

IRI
Ubilabs Innovations

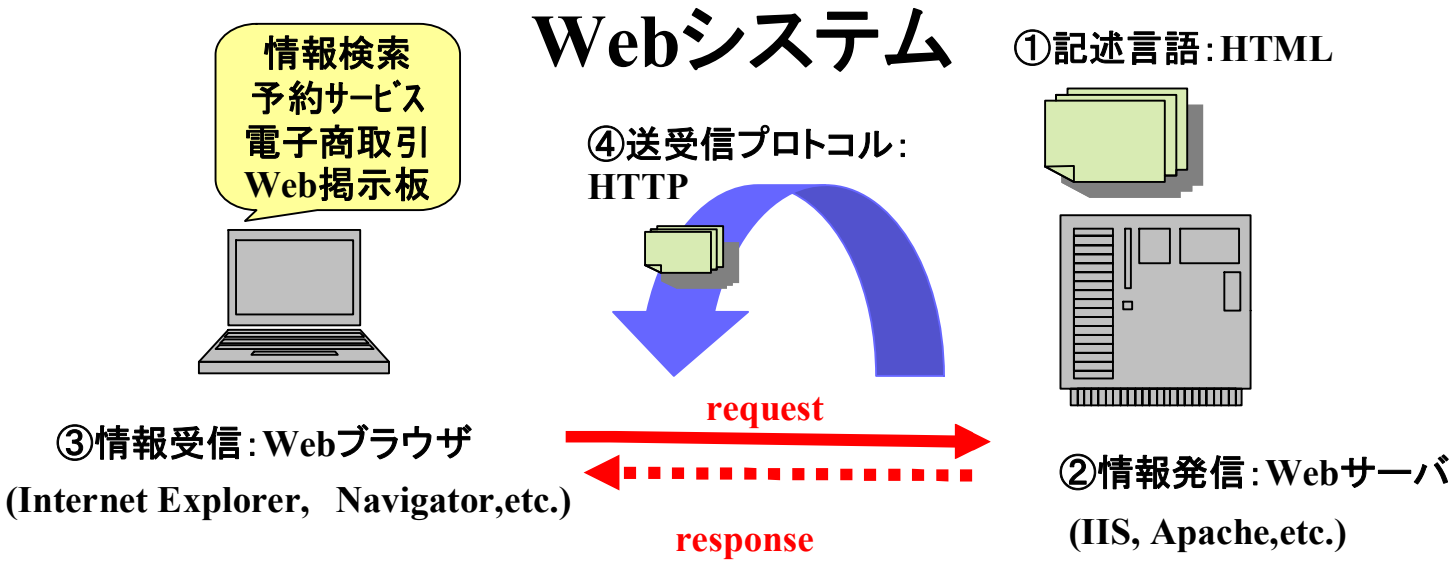
P2P＝Peer to Peer

Peer とは同等の人、対等の人、同僚、友人、仲間

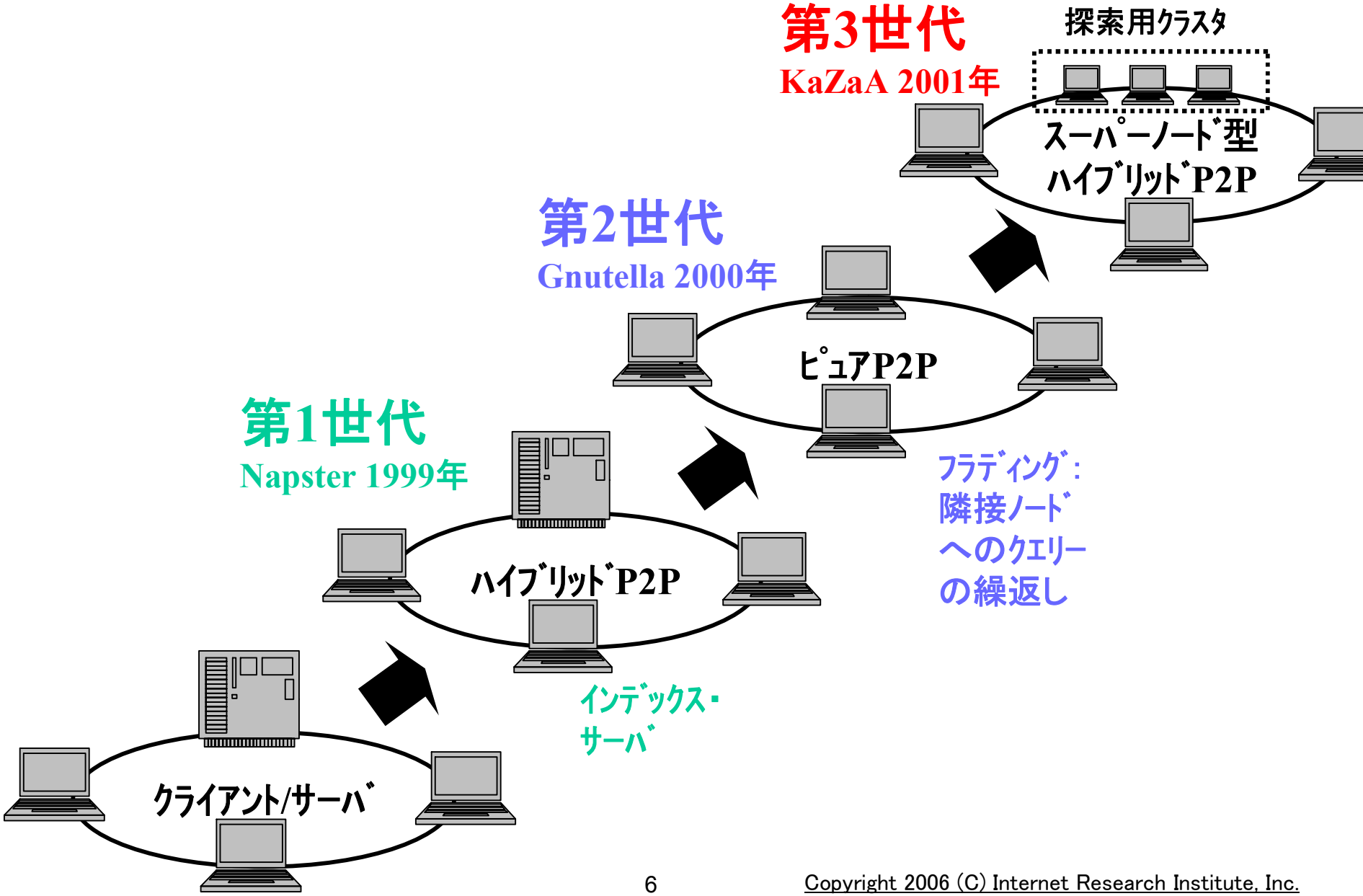
対立概念：　P2Pシステム　⇔ｸﾗｲｱﾝﾄ/ｻｰﾊﾞｼｽﾃﾑ

ｸﾗｲｱﾝﾄ/ｻｰﾊﾞｼｽﾃﾑの例＝World Wide Web

WebとP2Pとの相違



P2Pの発展経緯



P2P技術の概要

IRI
Ubilabs Innovations

1．ハイブリッドP2P（Napster：音楽MP3ファイル交換訴訟に)

・データの場所を探索するインデックス・サーバ

・データアクセスはサーバに集中しない

・Napster：　Shawn Fanning(Northeastern Univ.学生)が開発

2．ピュアP2P（Gnutella：米Nullsoft社、サービス主体不明で未訴訟)

・データの場所を探索するフラディング技術

・隣接ノードへ探索クエリーを発行（TTL：Time to Live/ Gnutella＝7)

・ Gnutella：　Justin Frankel とTom Perpper

3．スーパーノード型ハイブリッドP2P（蘭FastTrack社）

・データの場所を探索するスーパーノード・クラスター

・一般/スーパー・ノード数割合＝一定

・ライセンスビジネス⇒Skypeが利用

P2Pの特長

IRI
Ubilabs Innovations

1. 冗長性： 全ノードがバックアップ機能）

2. 拡張性： アクセス集中がない

3. オーバーレイ機能： セグメント境界の意識不要

4. 非同期アクセス機能： ローカル・データ処理機能

5. オフラインアクセス機能： 同上

6. アドホック構成： 参加者同士の合意で参加が成立

P2Pを支えるオーバーレイ・ネットワーク技術

IRI Ubilabs Innovations

1. 下位のネットワークレイヤ（IP）を抽象化する

2. IPレイヤ（IP）：ルータ、スイッチ、ファイアウォール
などでセグメント化され、セグメント間のノード同士の
直接接続は通常は不可

3. 通常のアクセス：サーバ名/フォルダ名/ファイル名
【データの所在は、固定的に】
⇒データを複数ノードに分散設置し同一IDでアクセス
⇒位置透過技術

P2P技術の社会的影響

IRI Ubilabs Innovations

1. 個人利用では「インターネットの匿名性」と連動

⇒情報を匿名で入手可能

⇒情報の入手経路が特定困難

⇒P2Pファイル交換による違法コピーが流行

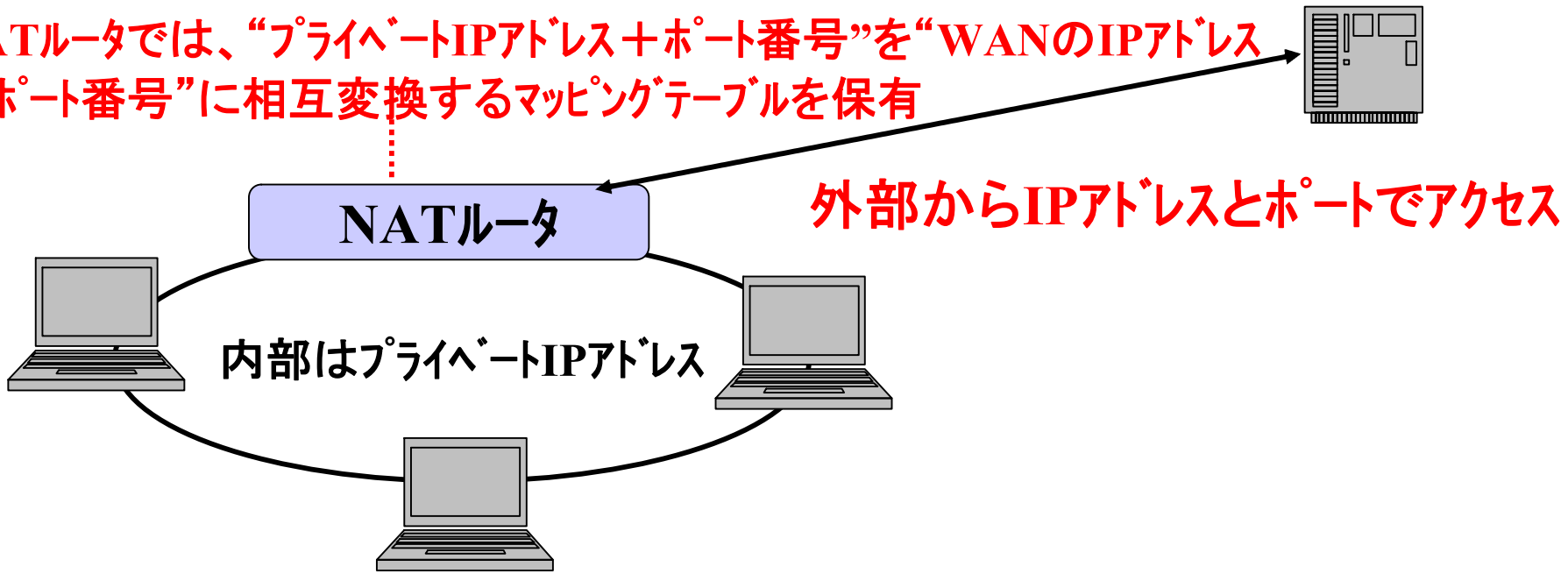
2. ビジネス利用では新たな可能性が増大

⇒Groove社のP2Pグループウェア：サーバ不要の企業横断型情報共有環境

⇒Kontik社、BitTorrent社のP2P型CDN (Contents Delivery Network)

2. NAT/ファイアウォール透過技術

UPnP (Universal Plug and Play)方式



もともとUPnP

Microsoftによって提唱されたTCP/IPベースのホームネットワーク向けのプロトコル仕様でMicrosoft、Intel、Compaq、IBMなどが参加した「UPnP Forum」で仕様策定。

UPnPは、IPアドレスや名前解決を行なうサーバの有無でConfigured型とAdHoc型に分類。Configured型のUPnPネットワークではDHCP、DNSディレクトリサービスなどが稼働するサーバによって、機器が認識され、通信が可能となる。

一方、サーバのないAdHoc型のUPnPネットワークでは、デバイスのネットワークへの参加を自動的に検出する「SSDP(Simple Service Discovery Protocol)、DHCPサーバがなくても自動的に重複しないプライベートIPアドレスを割り当てる「Automatic Private IP Addressing」、デバイスの名前解決と階層状の管理を行う「Multicast Name Resolution」などが適用される。

UDP Hole Punching/STUN方式

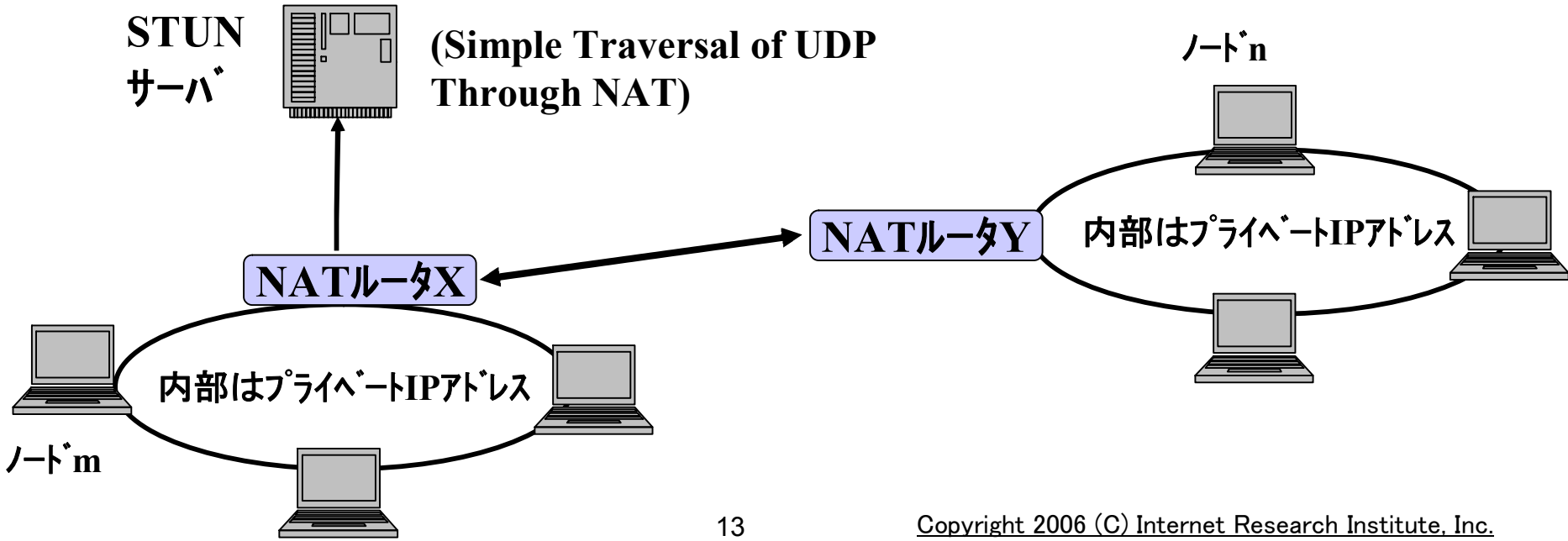
①ﾉｰﾄﾞmは、STUNｻｰﾊﾞから自らのWANのIPｱﾄﾞﾚｽ＋ﾎﾟｰﾄ番号取得しﾉｰﾄﾞnへ通知

②ﾉｰﾄﾞnは、ﾉｰﾄﾞmへUDPﾊﾟｹｯﾄを送信：NATﾙｰﾀY内ﾃｰﾌﾞﾙにm-Y-Xが追加

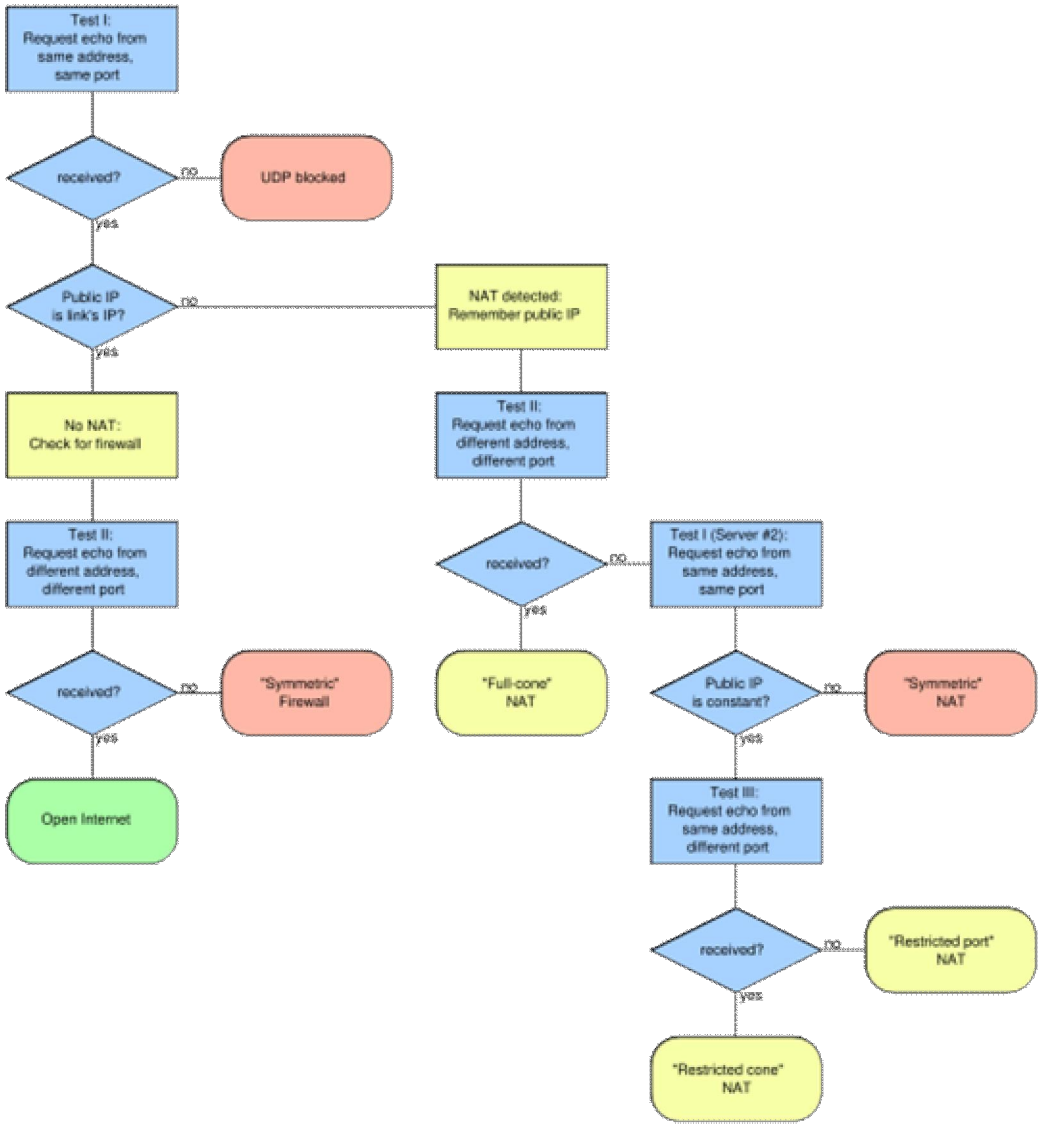
③NATﾙｰﾀX内ﾃｰﾌﾞﾙにﾙｰﾀYからのﾊﾟｹｯﾄ・ｴﾝﾄﾘがなく受けつけない

④ﾉｰﾄﾞmは、同様にﾉｰﾄﾞnのWANのIPｱﾄﾞﾚｽ＋ﾎﾟｰﾄ番号取得し、UDPﾊﾟｹｯﾄを送信、②でY内ﾃｰﾌﾞﾙにX-Y-nが追加され、NATﾙｰﾀYで変換されﾉｰﾄﾞnに到達。

*UDPでは、しばらく外部からWANのIPｱﾄﾞﾚｽ＋ﾎﾟｰﾄ番号に届いたUDPﾊﾟｹｯﾄは内部ﾉｰﾄﾞへ到達。
ﾉｰﾄﾞmが外向きに出したﾊﾟｹｯﾄでﾉｰﾄﾞnからのUDPﾊﾟｹｯﾄは届く＝UDP Hole Punching



STUNアルゴリズム

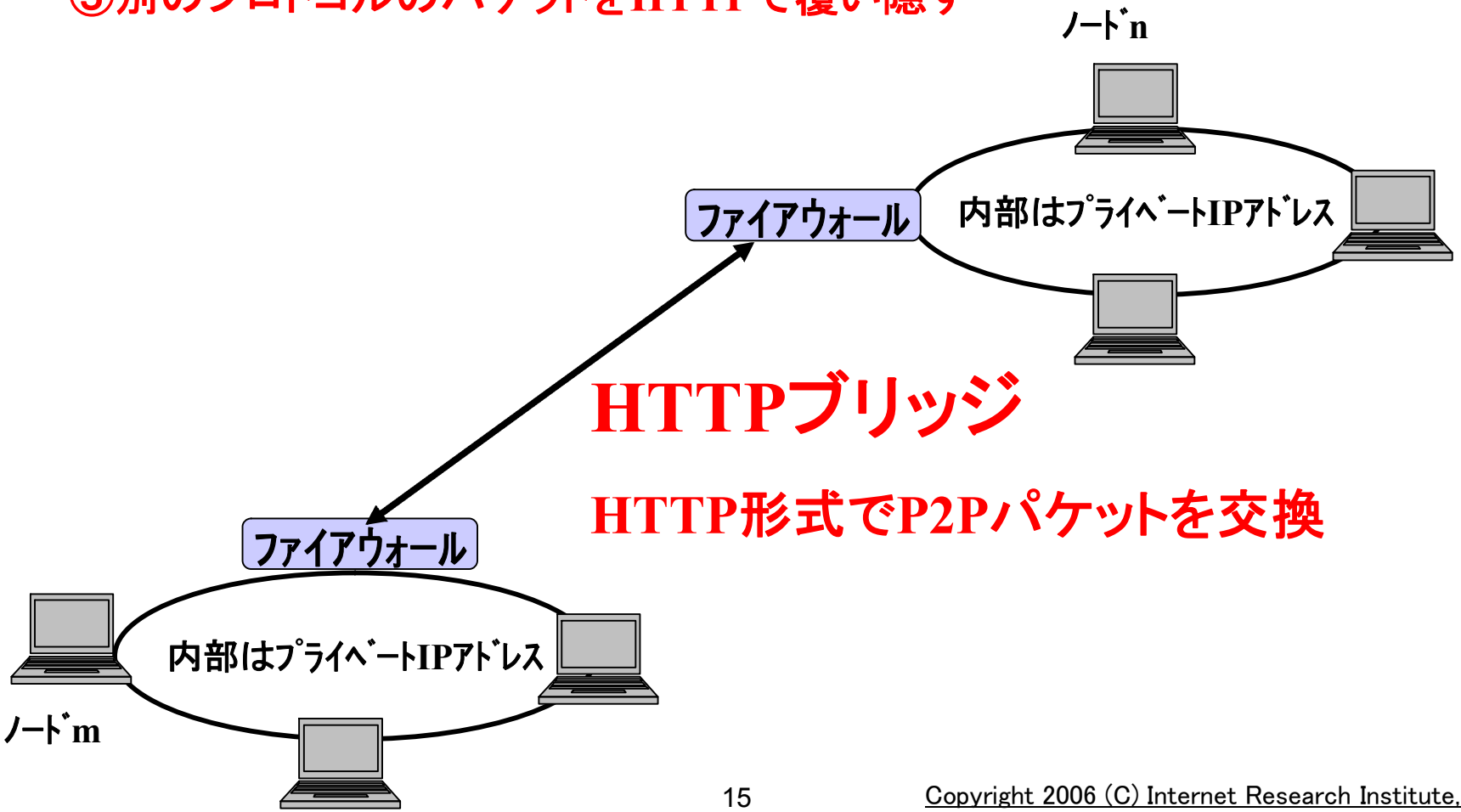


HTTPカプセル方式

①ファイアウォールのパケットフィルタリングによる排除

②Webアクセス専用の80番HTTP用ポートのみ可能

③別のプロトコルのパケットをHTTPで覆い隠す



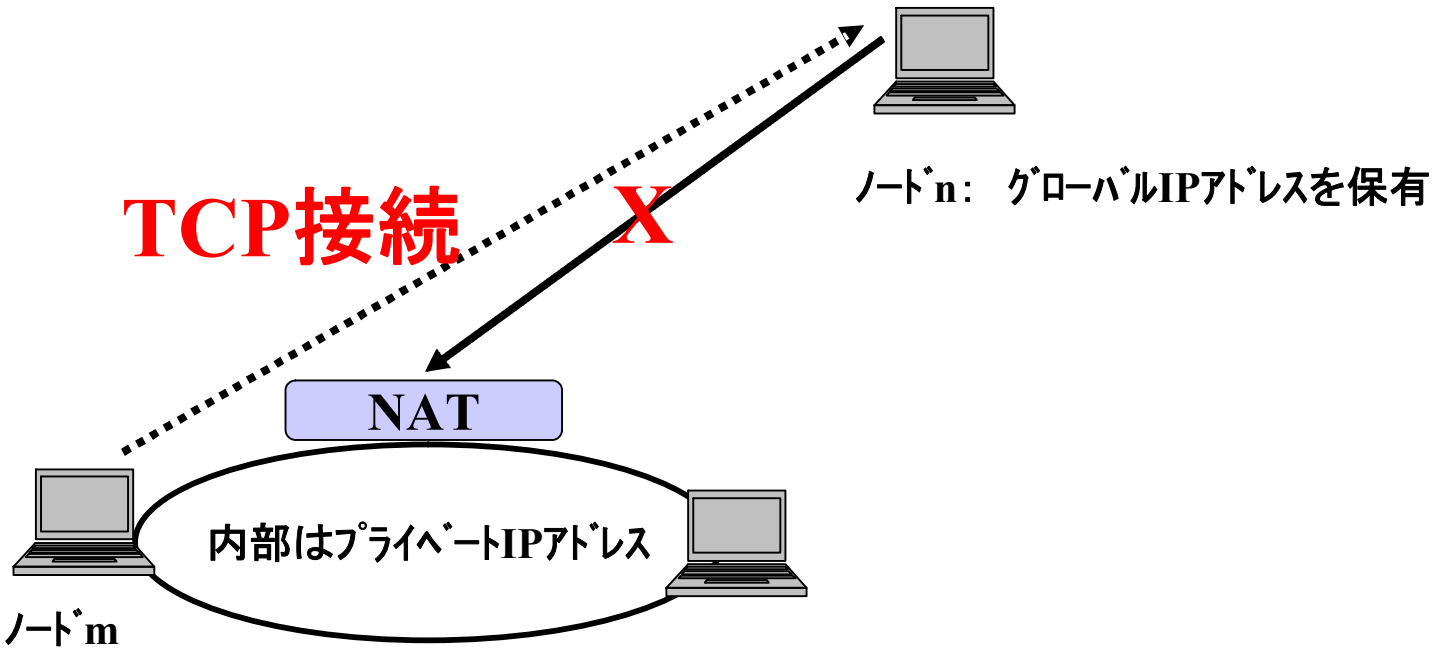
コネックション・リバーサル方式

①ﾉｰﾄﾞnがNATの先のﾉｰﾄﾞmへアクセスする時P2Pアクセス不可

②ﾉｰﾄﾞmへ外向きにTCP接続を基本ネットワークを用いて要求

③ﾉｰﾄﾞmは、外向きにTCP接続が確立し、nからmへの通信も可能

*Napster、Gnutellaでも採用

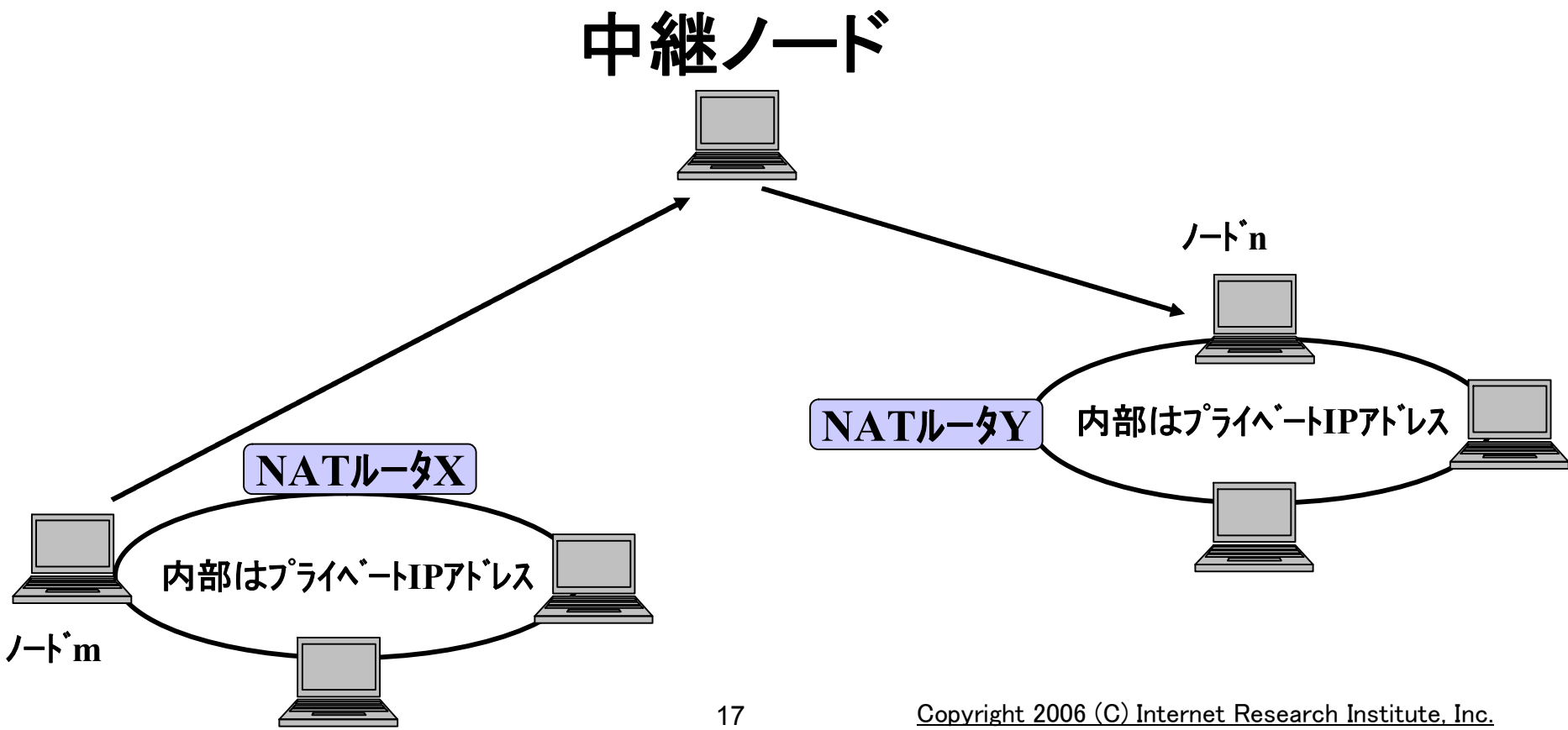


リレー方式

①ﾉｰﾄﾞmとﾉｰﾄﾞnとは中継ノードを経由する（蓄積はしない）

②専用中継ノードと一般ノードを中継ノードに用いる場合がある

③KaZaAとSkypeは一般ノードが中継ノードになる



3. ノード探索技術

ノード探索技術(1)

フラッディング

●バケツリレー

●探索クエリー:情報保有ノードへ到達すると来たルートを帰る

●帰りルートのノードに保有場所をキャッシュ記憶する

●同一クエリーを再転送しない

●TTL (Time To Live)を設定

●カテゴリーリスト作成し一括してクエリー発行

ノード探索技術(2)【DHT方式】

IRI Ubilabs Innovations

- 情報保有ノード固定方式の欠点

  ⇒フラッディング(大規模化困難)

  インデックスサーバ方式(負荷集中)

- DHT (Distributed Hash Table:分散ﾊｯｼｭﾃｰﾌﾞﾙ)登場
- Hash値＝一方向性変換で得られる固定長値
- Hash関数:あるデータが与えられた場合にそのデータを代表する数値を得る操作、又は、その様な数値を得るための関数のこと。
- Hash値は、元データとHash関数が同一なら同値
- DHT探索:Hash値を求めHash値と情報所在のﾏｯﾋﾟﾝｸﾞ

ノード探索技術(3)【DHT方式】

IRI Ubilabs Innovations

- DHT (Distributed Hash Table:分散ﾊｯｼｭﾃｰﾌﾞﾙ)方式
  ハイブリッドP2P方式と同様にデータ追加時に登録必要
- 登録:　Hash値と情報保存場所の組
- 登録先:　複数が分散配置(固定でない)
- インデックスノード:複数の分散配置された管轄の領域のHash値と所在場所ﾃｰﾌﾞﾙを保有
- 情報保有ノード:対象データのHash値に近いHash値を持つインデックスノードに登録する

ノード探索技術(4)【DHT方式】

IRI
Ubilabs Innovations

- DHT (Distributed Hash Table:分散ﾊｯｼｭﾃｰﾌﾞﾙ)方式における探索はインデックスノードへのアクセスで開始
- インデックスノード中で最もHash値の近いHash値を持つノードへクエリーを発行
- 該インデックスノードが管轄でない時更にHash値の近いインデックスノードへクエリーを転送(繰り返す)
- 対数的に収束： 100万ノードで20回
- フラッディングのように発散せず効率的

4. P2Pルーティング技術

P2Pルーティング技術（1）

IRI
Ubilabs Innovations

インテリジェント・ルーティング

- FastTrack社が実装
- Skype（IP電話）の基本
- 常に複数のルーティングパスを保持
- 通話中でもより広帯域パスを見つけて切替
- 耐ネットワーク障害性に優れる

P2Pルーティング技術（2）

オニオン・ルーティング

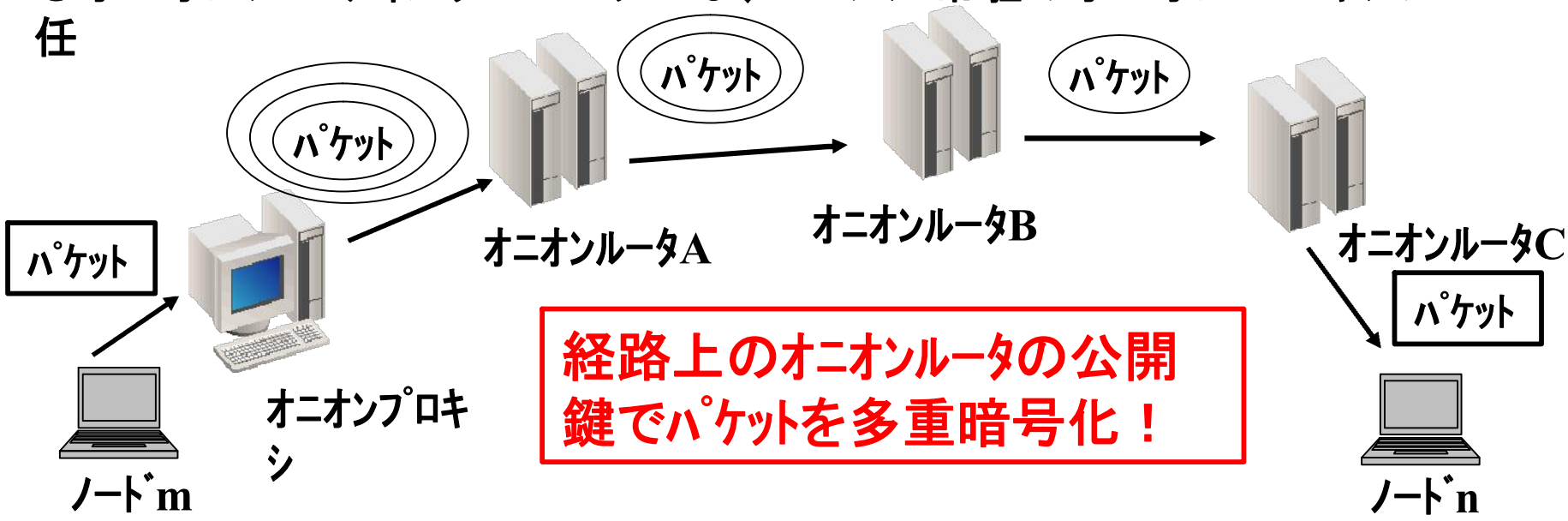
●TCP通信路を暗号化

●IPアドレス部も含めて暗号化

●何重にも皮を被せた暗号化＝オニオン

●オニオンルータ＝1ペアのPKI（公開鍵基盤）の公開鍵と秘密鍵を保有

●オニオンルーティング・ユーザーは、ローカル常駐のオニオンプロキシに一任



5. P2Pアプリケーション技術

同期型P2Pアプリケーション(Skype)(1)

IRI Ubilabs Innovations

- コミュニケーション相手が同時刻に通信
- 一定時間内の転送速度確保が重要
- 遅延防止技術が重要
- 代表例:Skype

  ルクセンブルグのSkype Technologies社
- ごく小規模の管理ノードだけで機能
- 利用者のPCが構成するP2Pネットワーク

同期型P2Pアプリケーション(Skype)(2)

●ビジネスモデル

・P2Pだけの通信＝無料

・Skype～PSTN(公衆電話網)＝有料

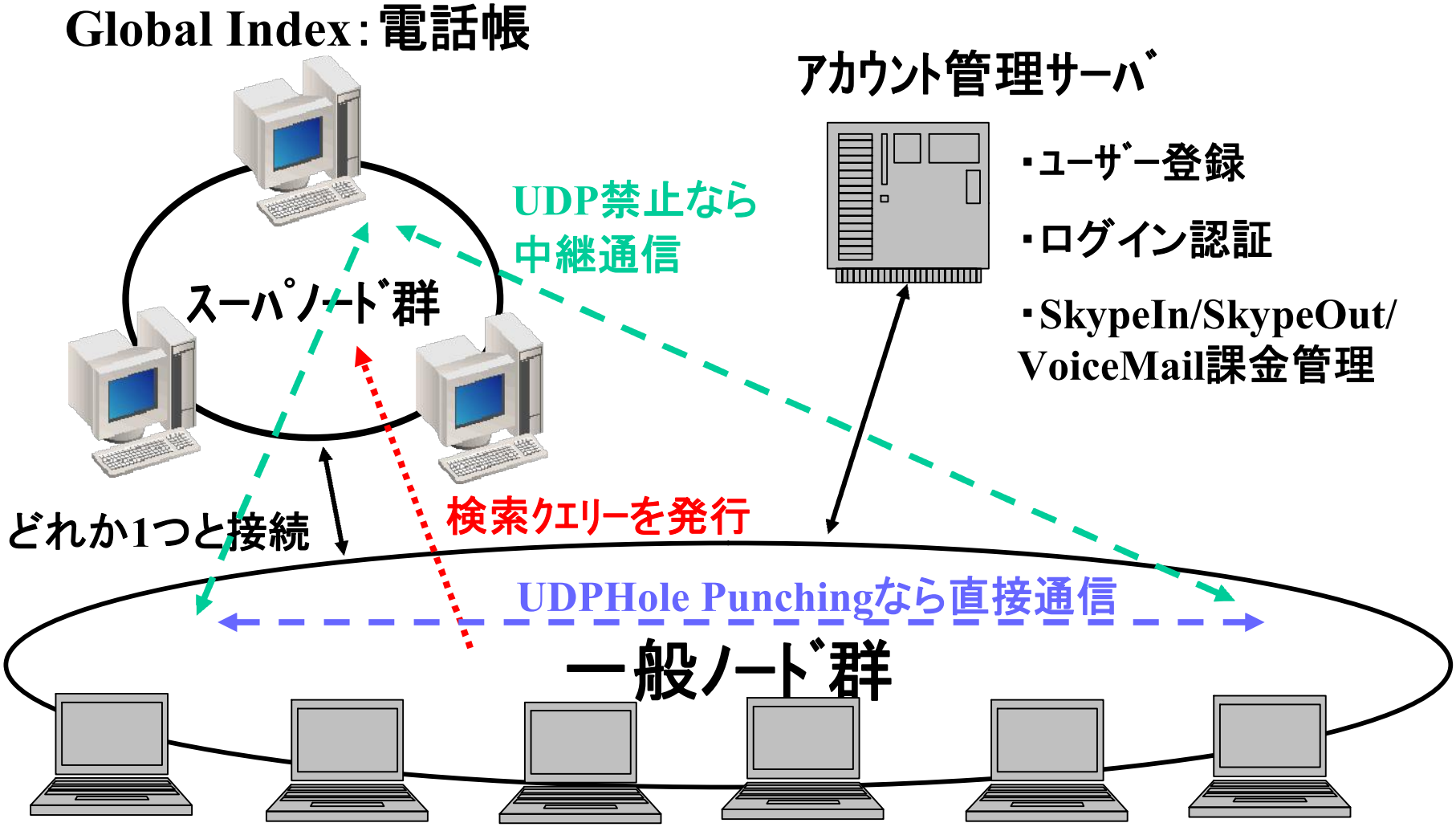
⇒ SkypeIn, SkypeOut

・VoiceMail＝有料

●P2Pによるサービス＝無料

●追加設備によるサービス＝有料

同期型P2Pアプリケーション(Skype)(3)



Skypeのスーパーノードの条件

- P2P実現のための中継ﾉｰﾄﾞ
- 一般ﾉｰﾄﾞからの初期接続
- Global Indexの提供

- UDPﾊﾟｹｯﾄ/内向きTCPﾊﾟｹｯﾄの通過可
- 高性能
- 高速回線
- ｸﾞﾛｰﾊﾞﾙIPアドレス
- 連続稼動

非同期型P2Pアプリケーション（1）

IRI
Ubilabs Innovations

●利用者にとって同時刻ではない利用形態

●ローカルにデータ保有

●サービス形態としては大きく2つある

①不特定多数の一般消費者向け

②特定グループのビジネス向け

●典型例が2つある

①CDN (Contents Delivery Network)

②　ファイル交換

非同期型P2Pアプリケーション（CDN）（1）

IRI Ubilabs Innovations

●CDN (Contents Delivery Network)

- 動画像を中心とした大容量配信
- センターサーバからの配信型ではトラフィック集中がボトルネック
- P2P型ではスケーラビリティが高い
- パッケージメディアの代替として

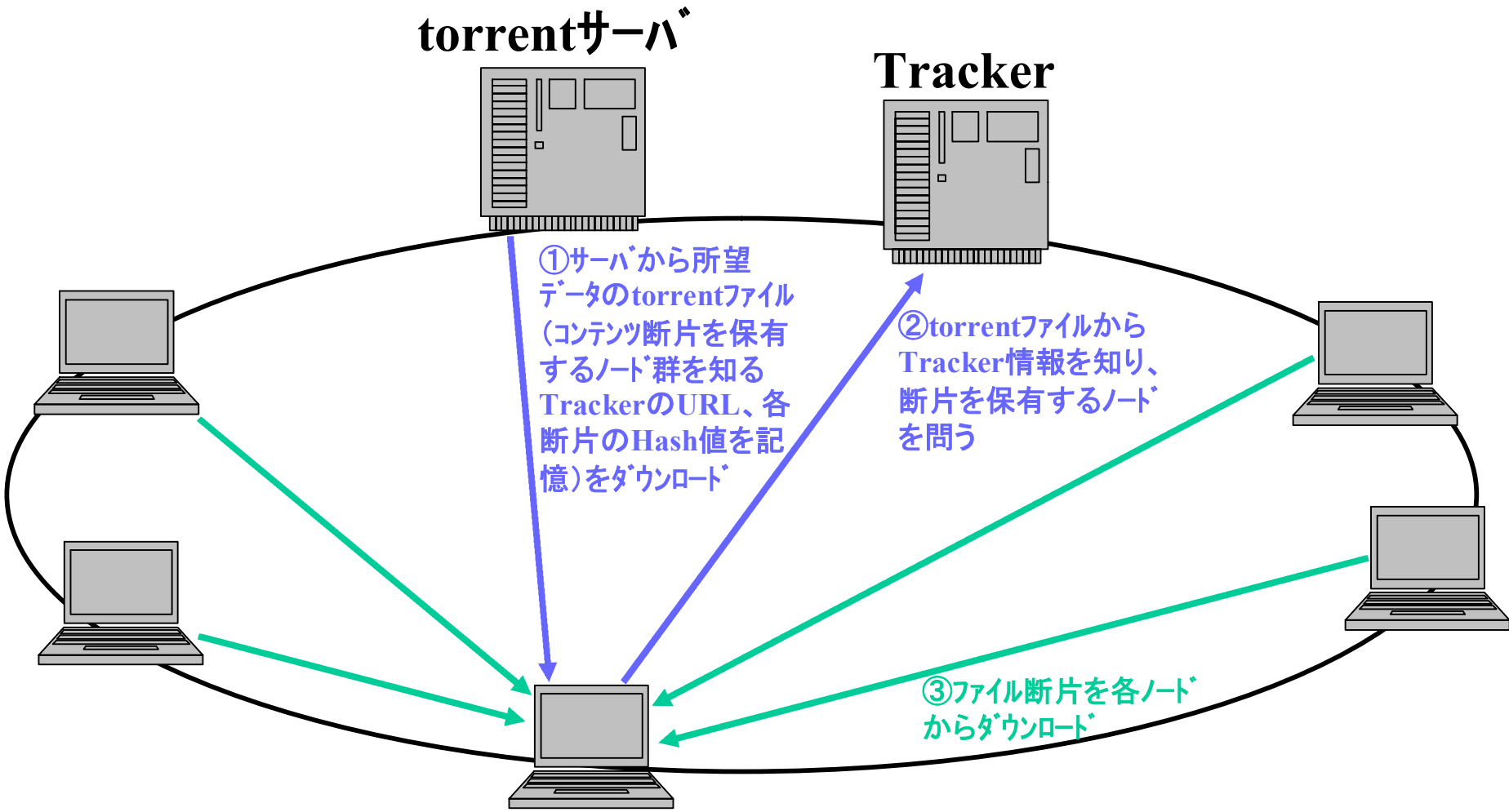
非同期型P2Pアプリケーション（CDN）（2）

IRI Ubilabs Innovations

●BitTorrent

- Bram Cohenが開発
- 大容量ファイルを分割し断片をノード間で通信
- 所望のコンテンツ入手時に断片を集めると同時に保有コンテンツを他ノードへ送る
- 人気コンテンツの断片保有率が上昇し効率向上
- インターネット上に散在するtorrentファイルの検索サービスを実施

非同期型P2Pアプリケーション（CDN）（3）



非同期型P2Pアプリケーション（CDN）（4）

IRI Ubilabs Innovations

●Kontiki DMS (Delivery Management System)

・大容量ファイルを分割し断片をノード間で通信

・クライアントにSecure Delivery Plug-Inをインストール

⇒ Kontiki DMS によるダウンロード可

・該当コンテンツを保有するノード群が各断片を送信

・BitTorrentにない特徴：

①ファイル断片要求コマンドの暗号化

②著作権保護（他社のDRMと連携）

③Kontiki社と契約要

非同期型P2Pアプリケーション（Groove）（1）

IRI Ubilabs Innovations

●Groove社 (Groove Virtual Office)

・Lotus Notesの開発者Ray Ozzieが開発

・Lotus Notesの欠点（社外との情報共有不可）

⇒ ファイアウォール透過技術

・アプリケーションが情報を直接授受

・社外とも情報共有

非同期型P2Pアプリケーション（Groove）（2）

IRI
Ubilabs Innovations

グループウェア

ファイル共有
予定表
掲示板

基本機能レイヤ

プレゼンス（ユーザーの情報）
アラート （各種お知らせ）
パーソナル（VoIP、IM、チャット）

同期レイヤ

ファイアウォール透過機能
オフライン支援（ﾃﾞｰﾀの一時預かり等）
帯域効率の向上
PKI認証/暗号化/ディジタル署名

6. Winnyとファイル交換の世界

P2Pファイル共有ソフトの概要

IRI Ubilabs Innovations

1．第1世代（Napster：音楽MP3ファイル交換訴訟に）

・データの場所を探索するインデックス・サーバ

・データアクセスはサーバに集中しない

・Napster：　Shawn Fanning(Northeastern Univ.学生)が開発

2．第2世代（Gnutella：米Nullsoft社、サービス主体不明で未訴訟）

・データの場所を探索するフラディング技術

・隣接ノードへ探索クエリーを発行（TTL：Time to Live/ Gnutella＝7）

・ Gnutella：　Justin Frankel とTom Perpper

3．第3世代（Freenet、Winny）

・ノードの発見とファイル検索＝ピュアP2P方式を採用

・ファイルシステムにキャッシュ（一時貯蔵所）

・匿名性の向上

Winnyの設計思想

IRI
Ubilabs Innovations

1. 匿名性 ： 情報の第1発信者を隠すことでプライバシー保護

2. ファイルの共有効率が良い ： 欲しい情報ができるだけ早く
獲得可能

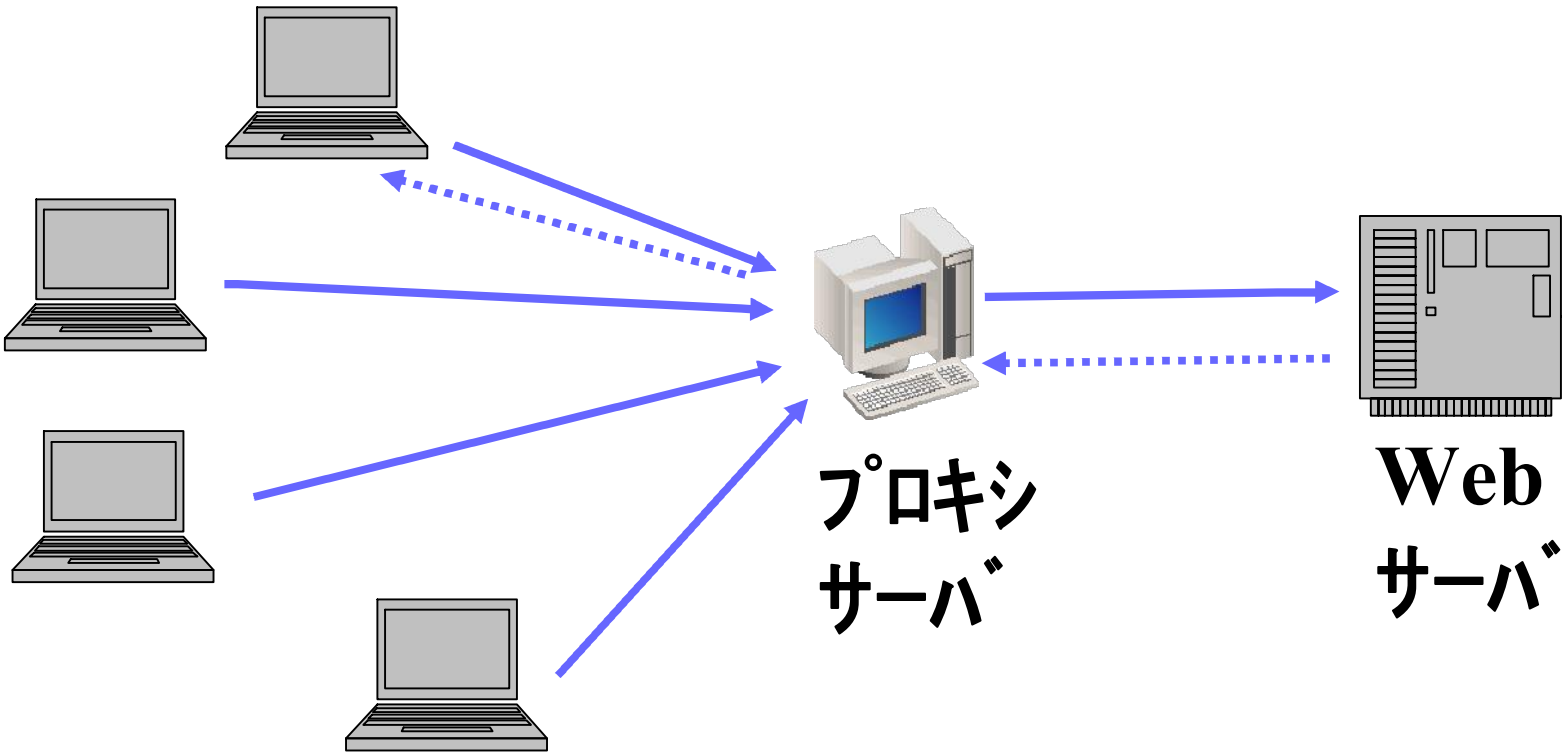
3. Windowsネイティブプログラムである ： パフォーマンス重視
（インタプリタ/仮想マシンを除外）

Winnyの基本となるプロキシ技術

IRI
Ubilabs Innovations

1. 匿名機構としてのプロキシ　：　中継ノード越えのIPアドレス

2. キャッシュ機構としてのプロキシ　：　他クライアントからの要求



Winnyの開発過程

IRI
Ubilabs Innovations

2002年4月1日	Winny開発宣言
5月6日	Winny1のβ1公開
7月25日	Winny1のβ18.0　簡易BBS機能
12月30日	Winny1の正式版公開
2003年4月7日	Winny公開サイト閉鎖
4月9日	Winny2開発宣言
5月5日	Winny2のβ1公開
11月27日	Winny2のBBSで予告した著作物放流後
	公開した2名逮捕⇒警察の家宅捜査
	Winny2 β7.1で中止
2004年5月10日	Winny開発者著作権違反幇助の疑い

Winnyの操作手順

IRI
Ubilabs Innovations

1．Winnyのネットワーク接続

Winny起動⇒ネットワーク内のオンラインの他ノード接続

＊初期起動時だけ接続先ノード情報をサイトから入手要

2．ファイル公開

空フォルダ準備⇒アップロードフォルダ指定

⇒公開ファイルをコピー⇒フォルダ情報タブ「再チェック」クリック

3．目的ファイルの探索

検索テキストボックスへ探索ファイル名入力

⇒「検索」クリック⇒ファイル一覧表登場

4．ファイルのダウンロード

ファイル一覧表から所望のファイルをダブルクリック

Winnyのネットワーク

1. ピュアP2P型
2. Winnyノード相互接続で築いたアプリケーションによるネットワーク
3. ノードの参加/離脱は頻繁
4. Winny起動で接続維持： 検索リンク＋転送リンク
5. 高速接続ノード＝上流 ⇒ 低速接続ノード＝下流

ファイル公開からダウンロード(1)

1. 公開ファイルをアップロードフォルダに置く

   ⇒フォルダのキーと本体を生成

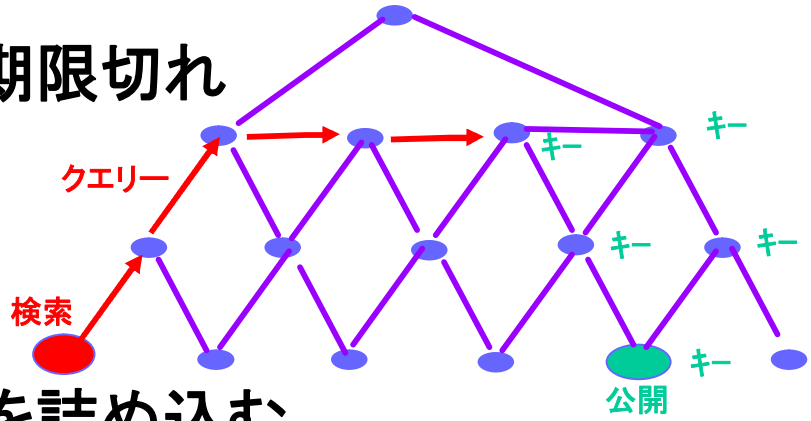
   ⇒キー:ファイル要約情報、ファイル名・大きさ、更新時刻

   ファイル識別のファイルID(Hash値:128ビットMD5)

2. キー:拡散、一定時間後有効期限切れ

3. ファイル検索:

   検索クエリーを上流ノードへ



   ⇒クエリーは条件合えばキーを詰め込む

   ⇒隣接ノードへ転送⇒検索元ノード:経由ノードで得たキーのリスト入手

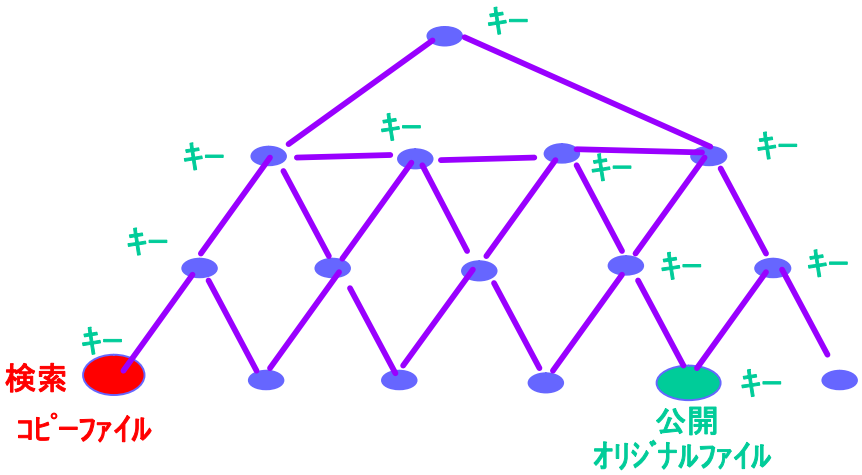
   ⇒クエリ通過道のノードに収集キーがコピーされる

ファイル公開からダウンロード(2)

4. ファイル転送　：　定期的にキーを受信し、検索で収集したキーからファイル選択するとダウンロードを開始
ファイルは暗号化したキャッシュファイル形式
⇒転送完了後:オリジナルファイル形式へ

5. ダウンロードファイル公開　：　定期的なキー交換で拡散

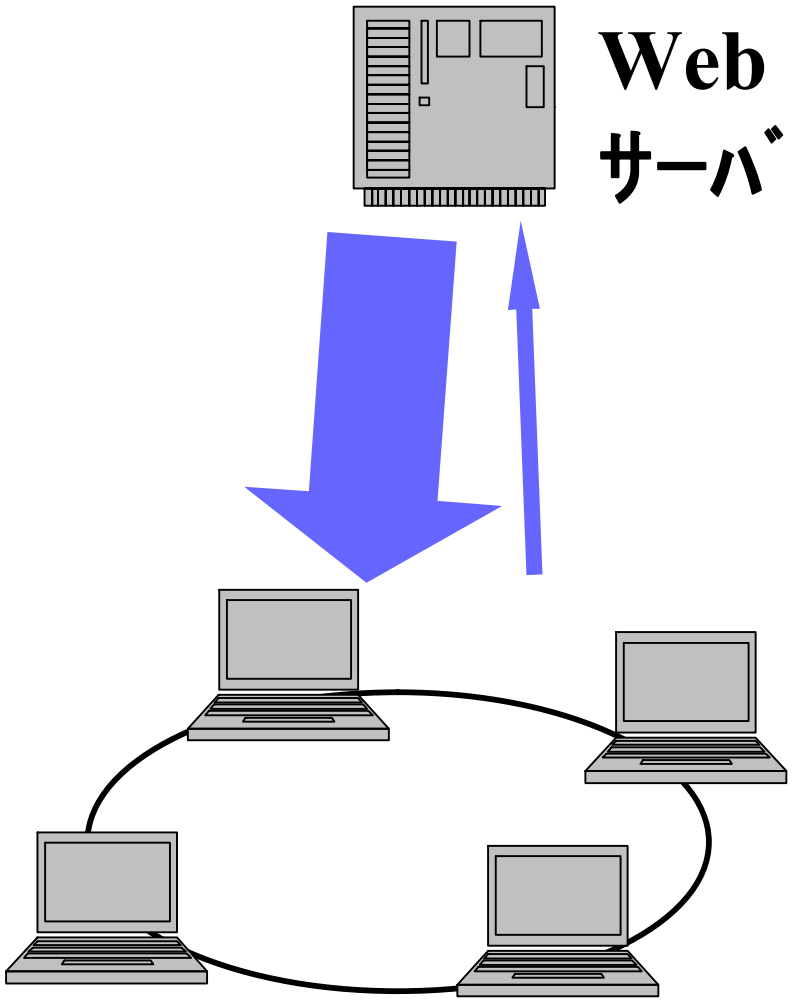
6. 別のノードからのダウンロード:　一次情報か二次情報かは、判別不可



おわりに

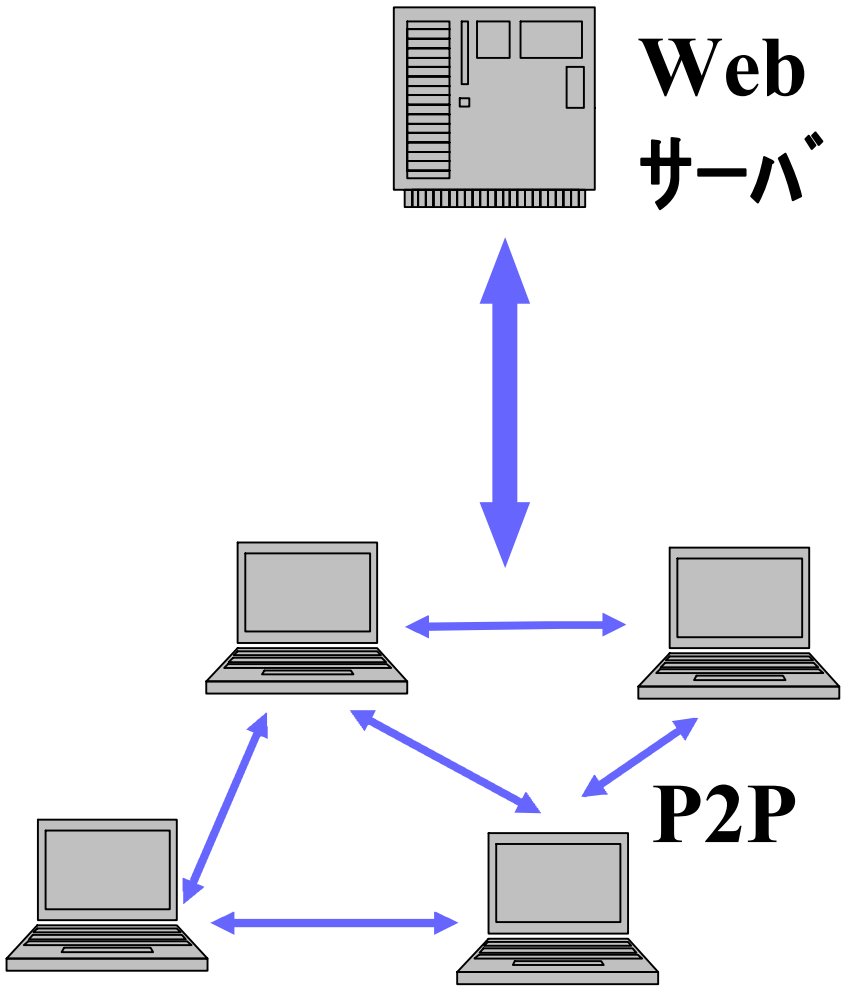
●現在のインターネット

＝非対称トラフィック



●今後のインターネット

＝対称トラフィックへ



ご清聴ありがとうございました