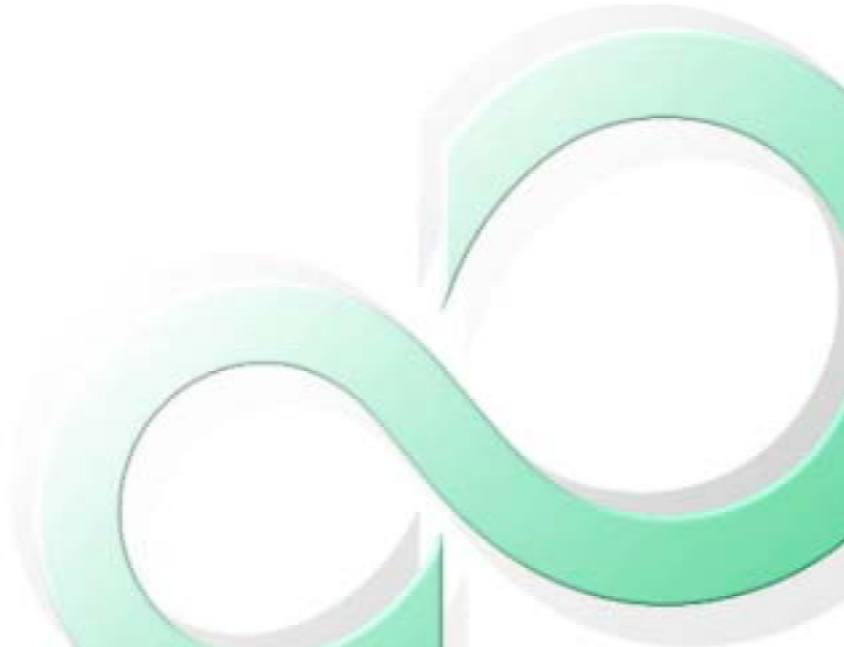
FUJITSU THE POSSIBILITIES ARE INFINITE

Onion Routerの紹介

1. インターネット上の脅威
2. オニオンルータ
3. 弊社の取組み
4. デモ

平成１５年７月１日
富士通プライムソフトテクノロジ
貝沼　達也

１．インターネット上の脅威



インターネット上の脅威

インターネットは公開ネットワーク

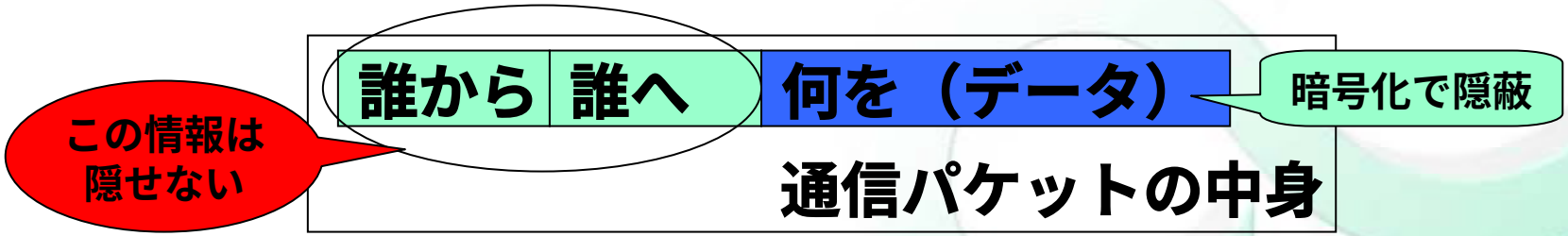
- 誰でも自由に利用が可能

誰かが、通信を“覗き見”しているかもしれない！

秘密情報やプライバシーを守るためには

- SSL等の通信暗号化
- VPN等の第３者の排除

しかし、これらの方法で守れるのはデータのみ！



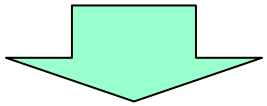
匿名通信路の必要性

●誰と誰が通信しているか推測される可能性

●誰が何をしようとしているか推測される可能性

例）“かつら”や美容整形に関連したWebサイトにアクセス

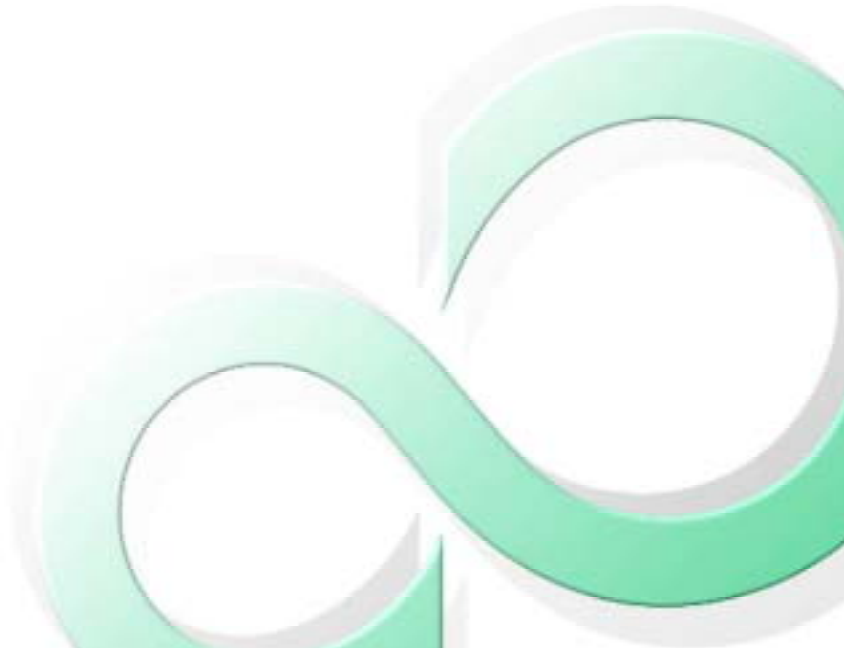
→個人の身体的特徴や悩み事が推測される可能性がある



データだけでなく、通信者も隠蔽したい！！

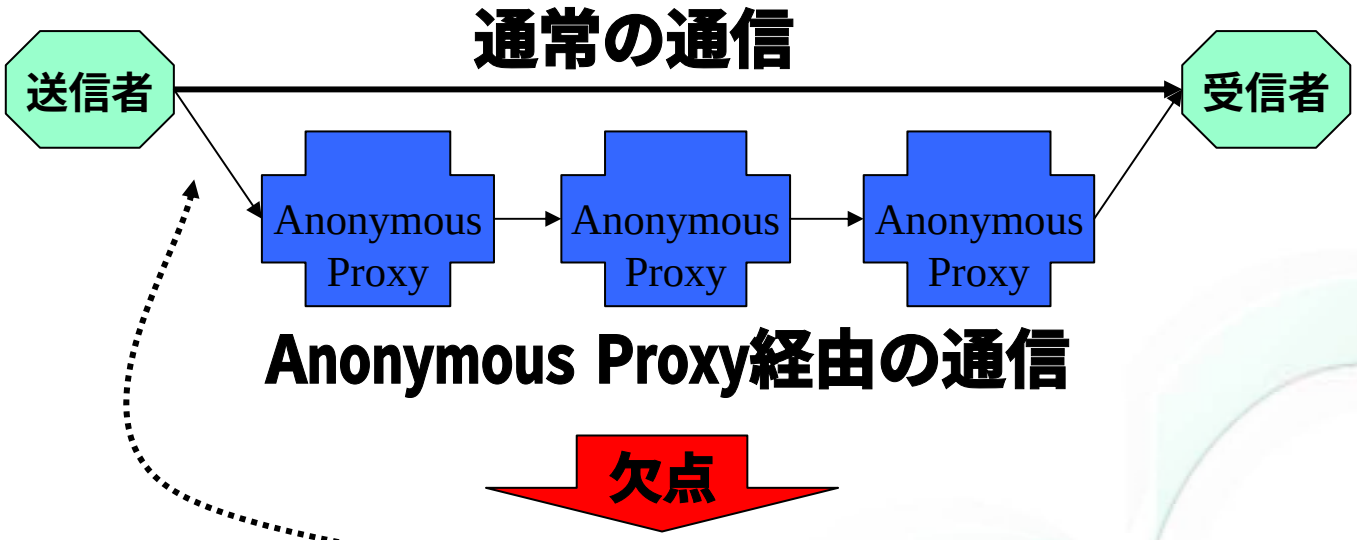
これを解決するのがAnonymous Proxyという考え方

２．オニオンルータ



Anonymous Proxyの考え方

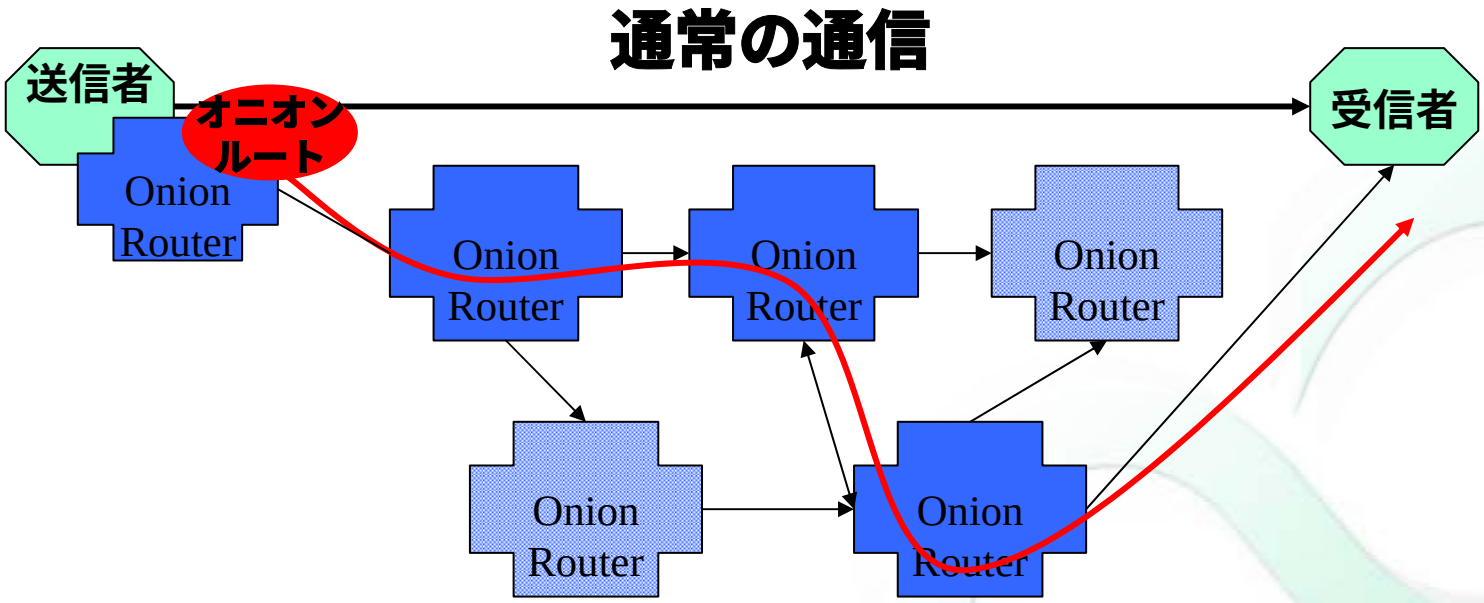
- 公開ネットワーク上に専用のプロキシサーバを複数設置
- 送信者から受信者へ幾つかのプロキシサーバを中継して送信
- プロキシはアプリプロトコルヘッダから個人特定情報を削除



- ネット上で受信者は公開（特に初段… で個人特定情報が漏洩）
- ルートが固定　→　攻撃の対象が固定
　　→　匿名性強度を送信者が制御できず

オニオンルータ

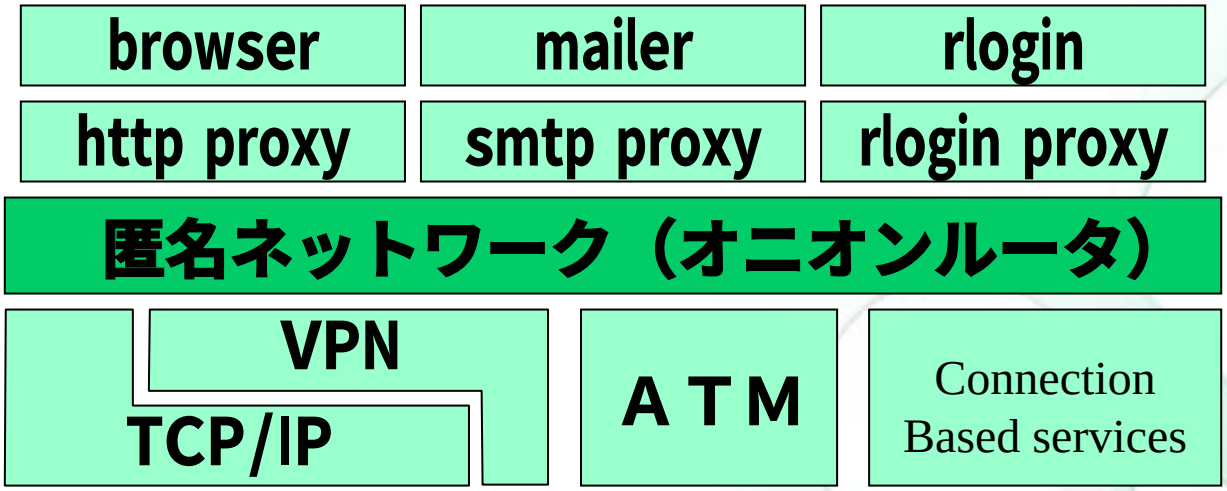
- Anonymous Proxyの一種。オニオンルータと呼ぶ。
- 送信ノードのオニオンルータがプロキシサーバを選択してルート制御
- ルートはプロキシサーバの公開鍵で多重に暗号化（オニオンルート）
- 米国の軍事研究所ＮＲＬ(Naval Research Lab.)の技術



オニオンルータの特徴

- 双方向のリアルタイム通信
- アプリケーションプロトコルに非依存

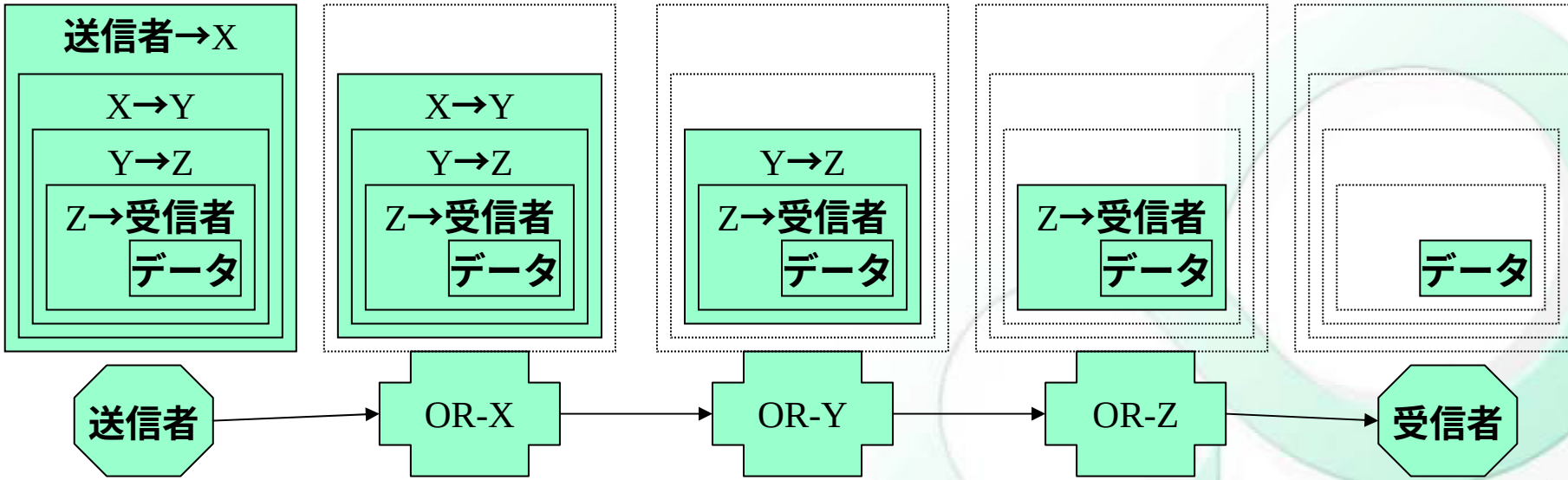
  ←アプリプロトコルヘッダの匿名性対処にはプロキシが必要
- stateless プロキシ（セッションを維持しない）
- 全てのオニオンルータが結託すると匿名性が暴かれる
- ルーティング途中で動的にルート変更ができない



どうやって通信者を隠蔽するか

公開暗号方式を利用した暗号処理

- “たまねぎ”構造によるパケット隠蔽
- 送信者は受信者の公開鍵でパケットを暗号化
- 受信者は自分の秘密鍵でパケットを復号
- 復号したデータの情報を元にパケットを中継
- オニオンルータ自身にもデータの通信者は不明



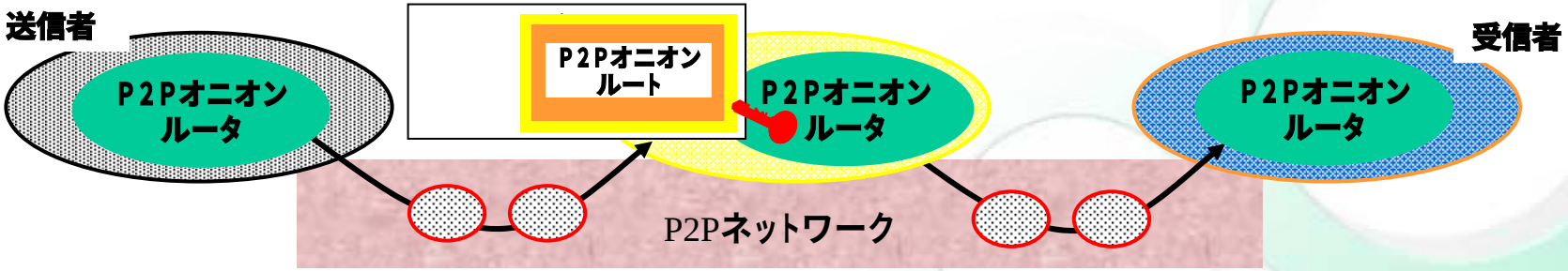
３．弊社の取組み

個人情報を匿名的に共有

- 平成14-15年度ＩＰＡ委託研究の成果。東大今井研との共同研究
- 個人情報を匿名的に共有するネットワーク。中央サーバを廃することで、危険を分散し、堅牢性を確保する。
- 特許出願中

構成：

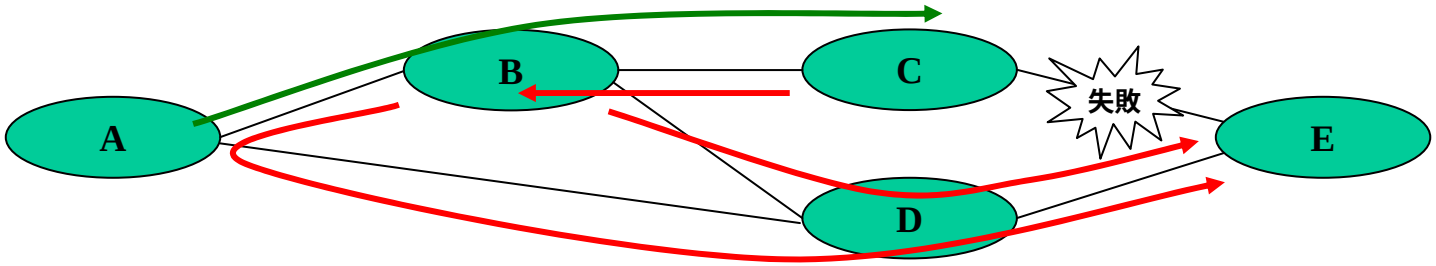
- オニオンルータで匿名ネットワークを構成
- Ｐ２Ｐネットワーク上の任意のノードがオニオンルータに。鍵の分散
- 個人情報を分散共有。エージェントがオニオンルーティングして検索



オニオンルータの改良

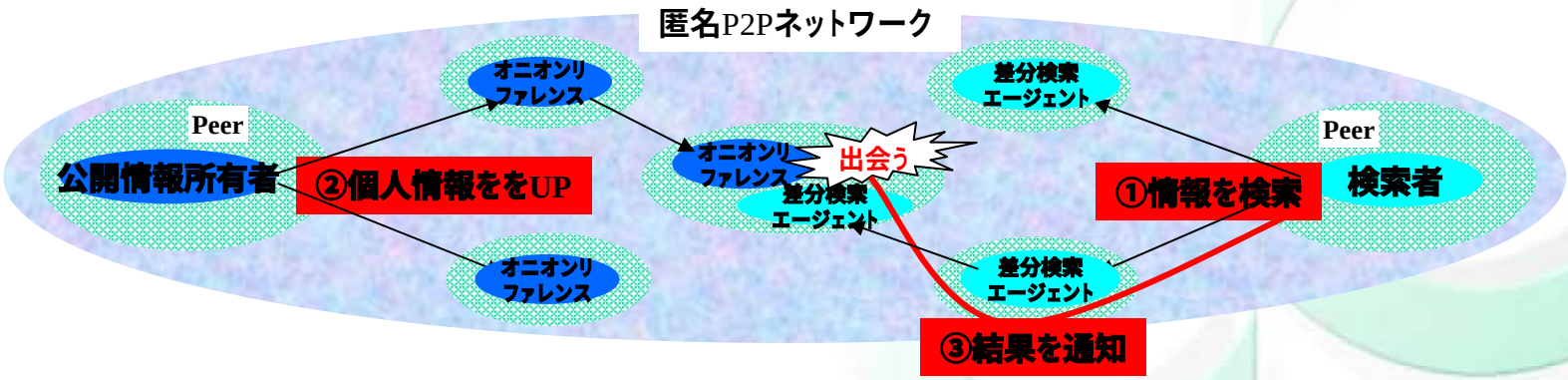
- **Ｐ２Ｐネットワークの不安定性とオニオンルーティングを両立**

  匿名的なルート探索プロトコル、及び、バックトラック可能オニオンで解決



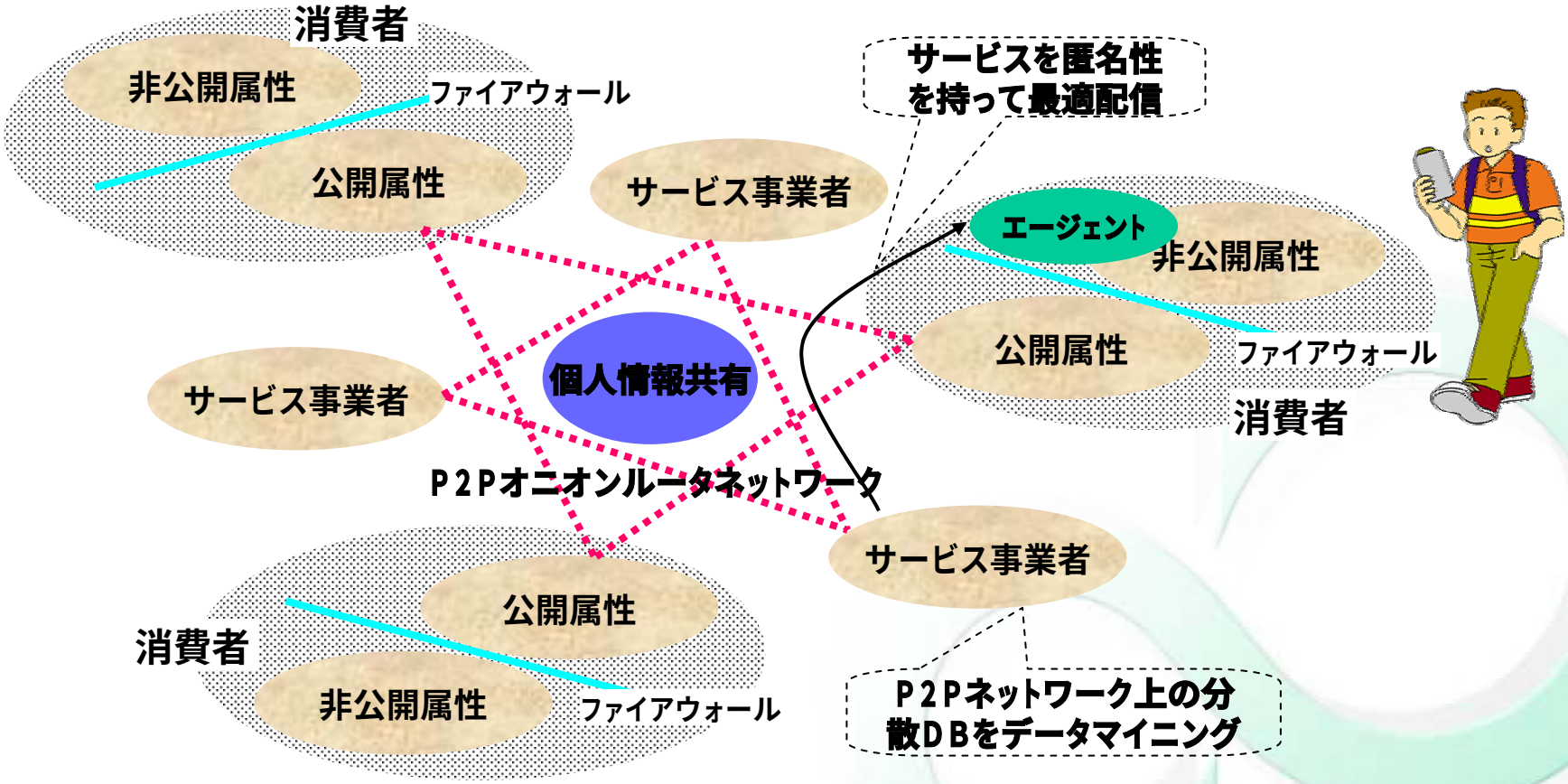
- **検索の非効率性を改善**

  個人情報をネット上にキャッシュ（オニオンルートで所有者を参照：オニオンリファレンス）。検索エージェントもキャッシュし、差分を検索する。

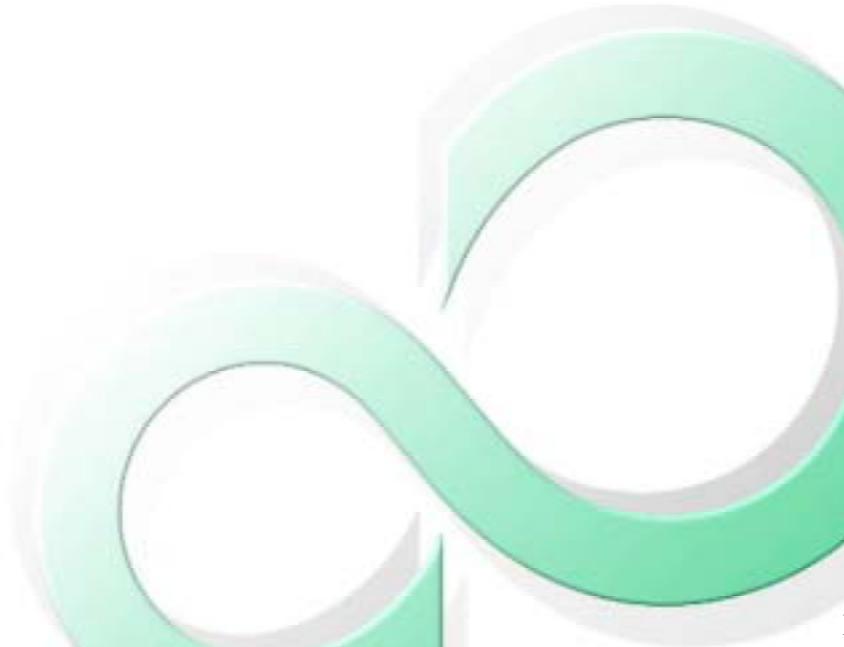


個人情報保護活用プラットホーム

サービス事業者と消費者は、**匿名性をもって**相互の公開データを授受する。非公開データを利用するサービスは、消費者の**firewall内に**エージェントとして訪問し、サービスを提供する。

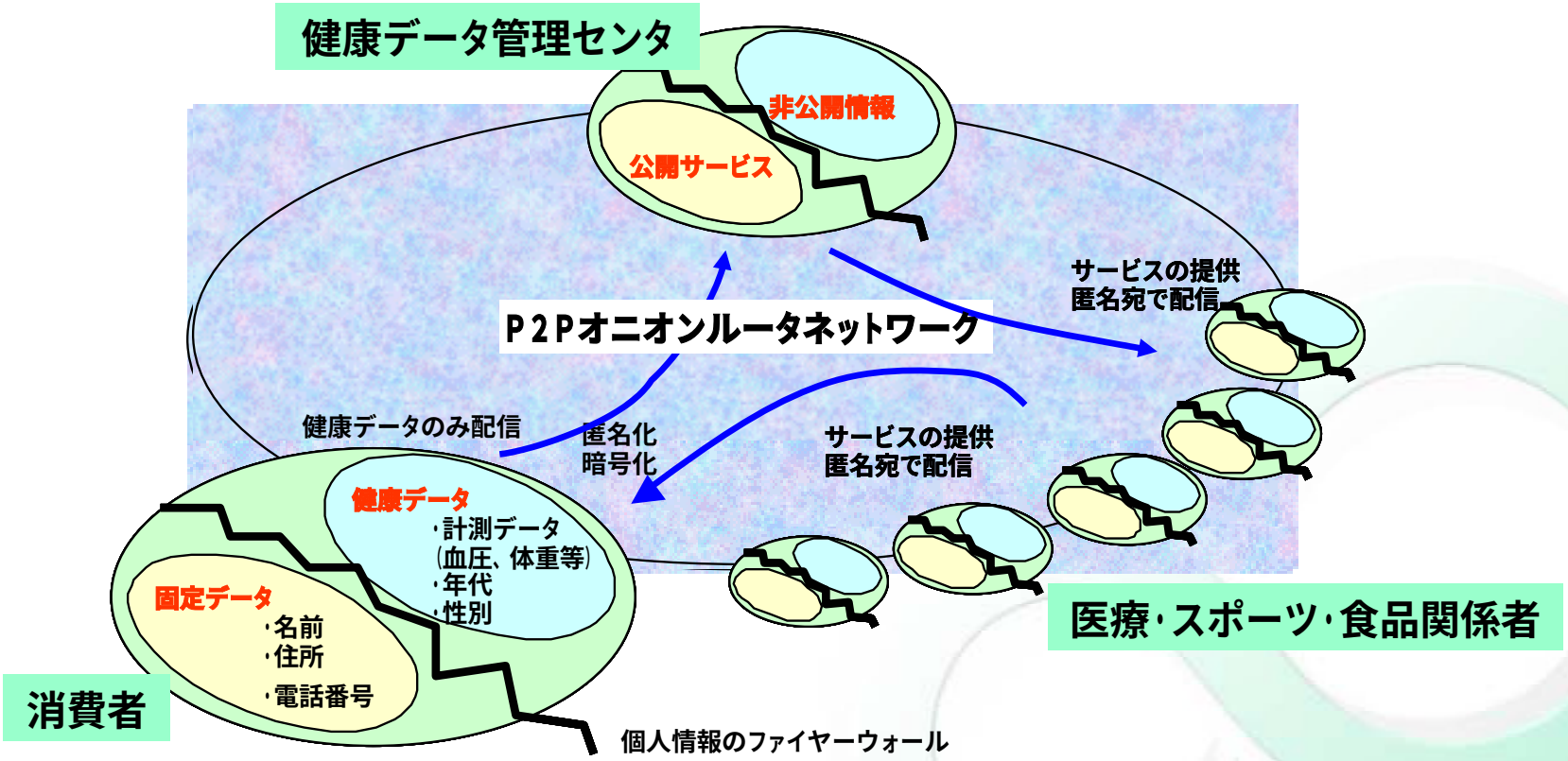


４．デモンストレーション



ヘルスケアサービスのデモ

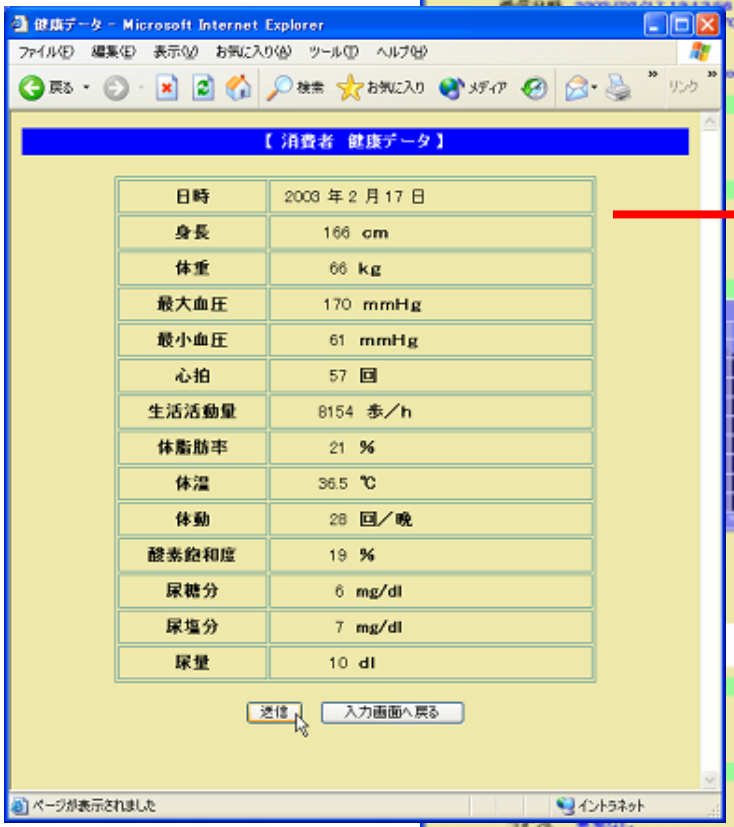
- 健康データのみがネット上に流れ、医療サービスに利用される
- 消費者と医療サービスは匿名的に双方向コミュニケーション

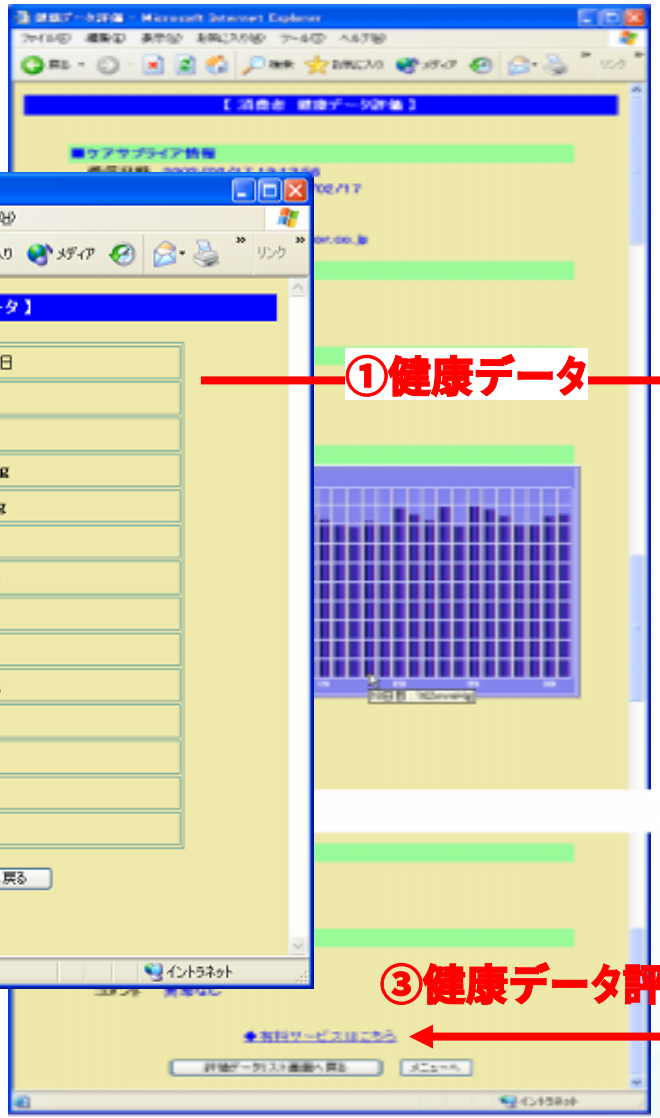


デモ画面

消費者画面

健康データ管理センター画面





①健康データ

②健康データ解析結果

③健康データ評価結果

ヘルスケアサービス事業者