VPNとホストの実行環境を統合するパーソナルネットワーク

光来健一* 廣津登志夫* 佐藤孝治*
明石修* 福田健介* 菅原俊治* 千葉滋**

*NTT未来ねっと研究所

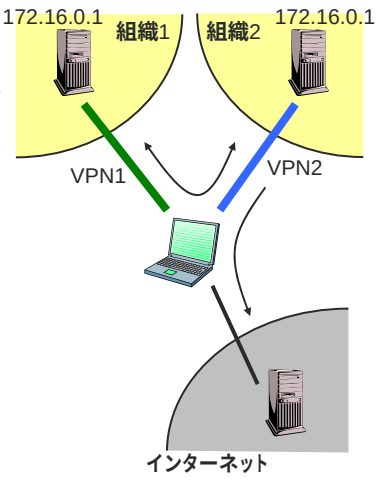
**東京工業大学

複数のネットワークの同時利用

- VPNの普及
  - 管理者によるLAN間接続だけでなく、ユーザによるリモートアクセスに
    - IPsec road warrior、ssh port forwarding
  - 仮想的なLANに見せかける
  - インターネット上で情報の漏洩を防ぐ
- 複数のネットワークを使う機会が増加
  - LANと複数のVPN

複数のネットワークを扱うホストの問題

- 名前空間の衝突
  - 各ネットワークのIPアドレスやホスト名が重なるかも
- VPNからの情報漏洩
  - 他のネットワークに機密情報が流れるかもしれない
    - ホスト上のプロセスやファイルシステムを介して

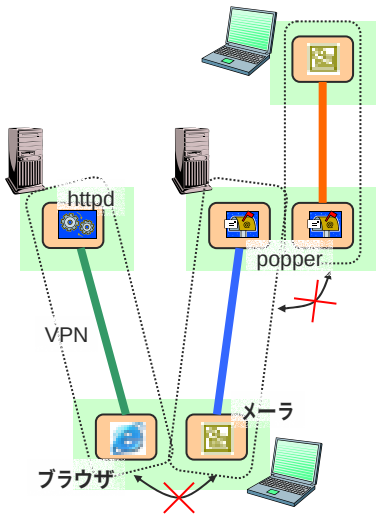


ネットワークの排他制御の必要性

- 従来のOSはネットワークを排他的に利用できなかった
  - 名前空間が1つしか提供されていない
  - プロセスには全てのネットワークが見える
- IPが重ならないように運用し、データの流れに注意を払う必要があった
  - LAN間接続のVPNではネットワークは1つだったので問題なかった

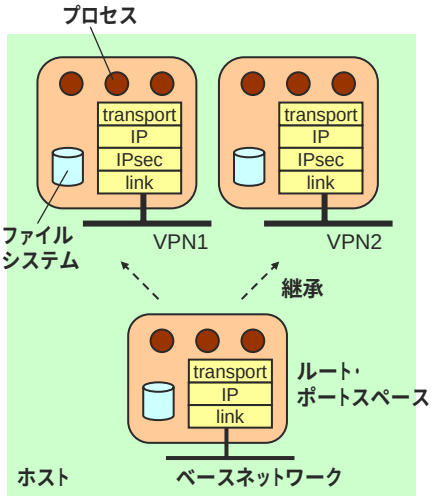
パーソナルネットワーク

- VPNとホストの実行環境を統合
  - プロセスとVPNを結びつける
- 独立したネットワーク
  - 独自の名前空間を持つ
    - ベースネットワークと同じIPアドレスも使える
  - 情報の流れを制限できる
    - 機密情報を外に漏らさない



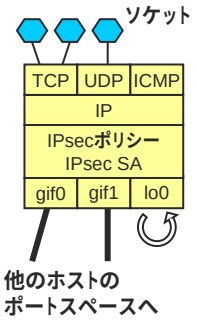
ポートスペース

- VPN毎に分離された実行環境
  - ネットワークとファイルシステムの空間を分離
  - ユーザプログラムはそのまま動かせる
- 継承
  - 親の実行環境の一部を利用できる
  - ユーザが作り易くなる



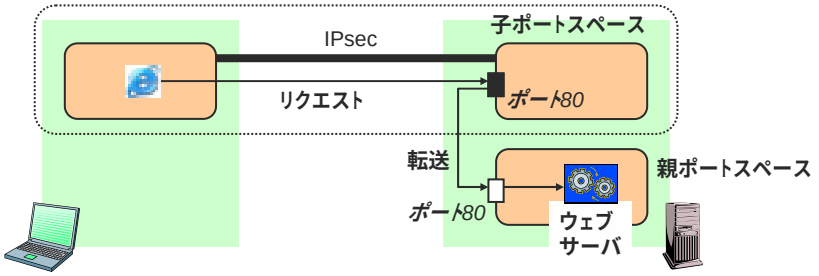
ネットワーク空間の多重化

- ポートスペースは以下の空間を独自管理
  - ネットワークインタフェース空間
    - VPNの出入り口
  - IPsec空間
    - VPNの設定
  - IP空間
    - IPの設定とルーティングテーブル
  - トランスポート空間
    - ポートへのソケットのバインド



ネットワークサービスの継承

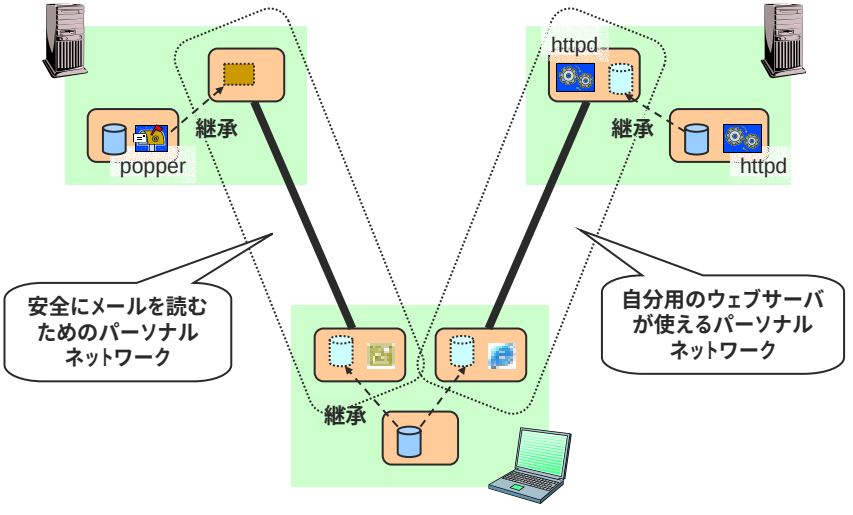
- 親ポートスペースで提供されているサービスを継承
  - サービスの上書き、隠蔽もできる



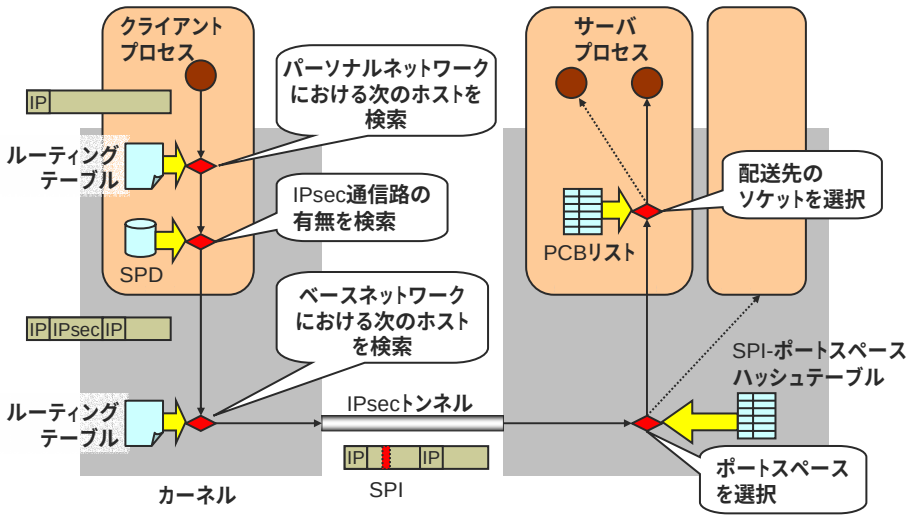
ファイルシステム空間の多重化

- ポートスペース毎に独自のファイルシステムを提供
  - プロセスは他のポートスペースのファイルシステムにアクセスできない
- ファイルシステムの継承
  - 親ポートスペースのファイルシステムを参照
  - 変更は子ポートスペースのファイルシステムへ

パーソナルネットワークの例

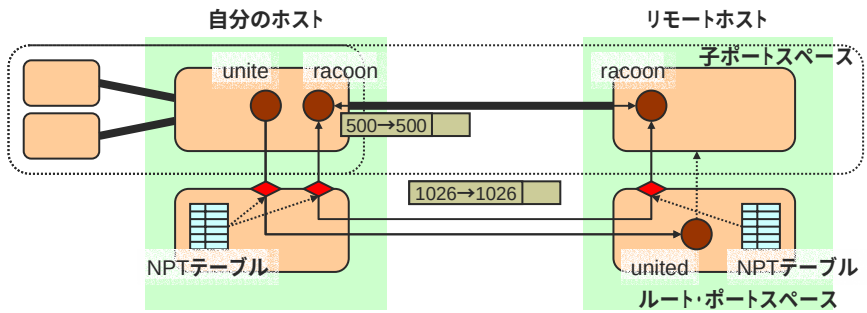


ポートスペース間の通信



パーソナルネットワークの作成: unite

- 自分のホストにリモートホストを結合



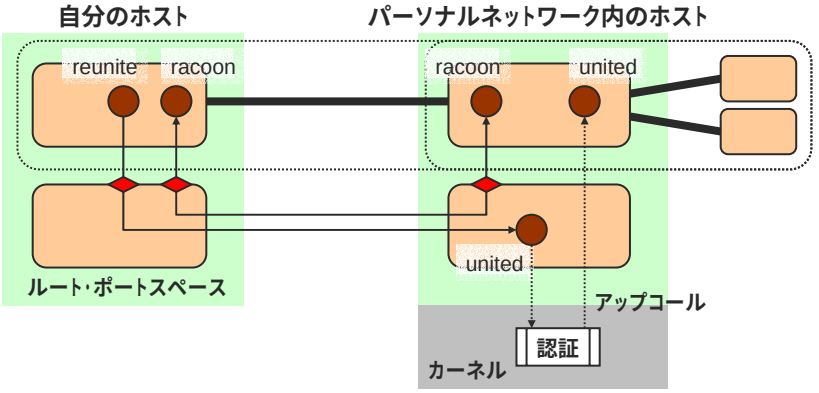
ネットワーク・ポート・トランスレーション (NPT)

親ポートスペースの通信路を使って通信

親子間でポート番号をつけかえる

パーソナルネットワークへの参加：reunite

- パーソナルネットワークに外部から加わる



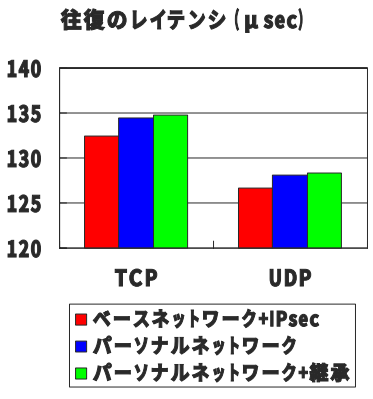
実装

- ポートスペースをFreeBSD 4.7に実装
  - ネットワーク空間の多重化
    - ネットワークに関するデータベースをポートスペース毎に管理
  - ファイルシステムの多重化
    - 継承なし：chrootをベース
    - 継承あり：unionファイルシステムをベース

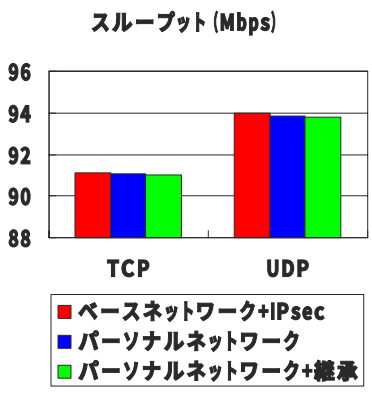
実験

- ポートスペースのオーバヘッドを調べた
  - ベンチマークプログラム：netperf、ab
    - ベースネットワーク＋IPsec
    - パーソナルネットワーク
    - パーソナルネットワーク＋継承
  - 実験環境
    - PC (PentiumIII-S 1.4GHz)　2台
    - 100baseTのイーサネットで接続
    - IPsecの暗号化と認証はなし

実験結果：netperf

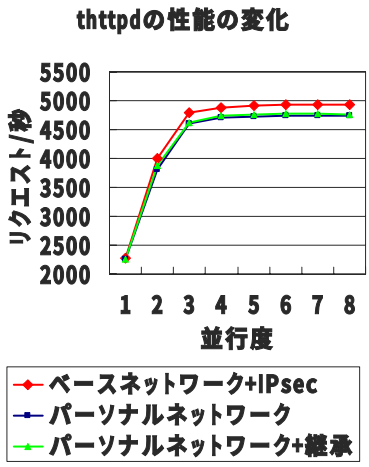


1.5%のレイテンシ増大



0.1%のスループット低下

実験結果：ab



- 並行度1では性能低下は1.1%
- 並行度が増すと性能低下は3.9%に

関連研究：仮想OS

- jail、VMware
  - 既存の環境の上に仮想的な環境を作る
    - 既存の環境の名前空間を汚染する
    - 既存の環境からアクセスできる
- ネットワーク・スタックの仮想化 [Zec'02]
  - ポートスペースのネットワーク多重化と同じ
    - 継承はない

ネットワークからは複数のホストに見える

関連研究：仮想ネットワーク

- 仮想インターネット [Touch et al.'02]
  - 仮想ネットワーク毎にホストに実行環境を作る
  - 実行環境の間でルーティング
- パーソナルVPN [宇崎ら'02]
  - 特定のユーザからのみ利用できるVPNを作れるようにする
- VNAP [廣津ら'00]
  - VLANによって通信を分類し、ホストの特定の実行環境と結びつける

まとめと今後の課題

- パーソナルネットワークを提案した
  - VPNとホストの実行環境（ポートスペース）を統合する
    - 名前空間の衝突を防ぐ
    - 情報の流れを制御する
- 今後の課題
  - パーソナルネットワーク間の情報のやりとり
  - パーソナルネットワーク毎のQoS