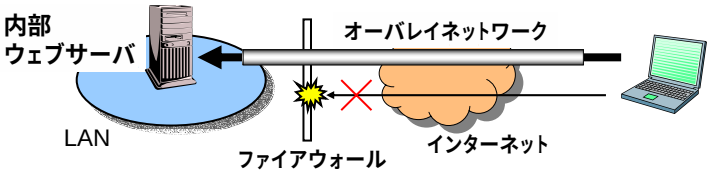
複数のオーバレイネットワークを制御するためのプライベートなネットワーク環境

光来健一*　廣津登志夫*　佐藤孝治*
明石修*　菅原俊治*　千葉滋**

*NTT未来ねっと研究所
**東京工業大学

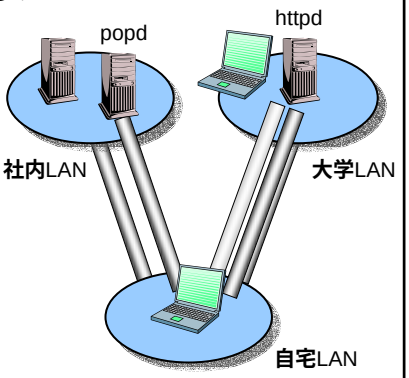
オーバレイネットワーク

- ユーザがLANを外から使う機会が増加
  - ファイアウォール等が問題
- オーバレイネットワークが使われている
  - ベースネットワーク上の仮想ネットワーク
    - 例：VPN、sshポートフォワーディング
    - 1つの機能：ファイアウォール越え



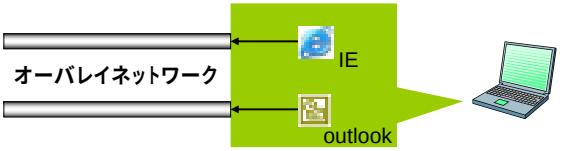
オーバレイネットワークの使い分け

- 状況に応じてオーバレイネットワークを作り、使い分けられるようにしたい
  - LAN毎
    - 内部情報を漏らさない
  - ホスト毎
    - 攻撃の被害を減らす
  - データの重要度毎
    - 重要でないデータは暗号化しない、など
  - ユーザ毎



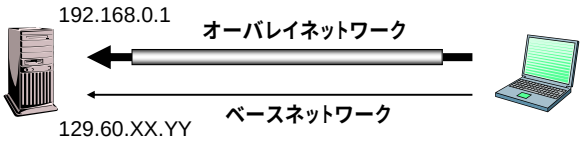
複数のオーバレイネットワークの制御

- 従来のOSは複数のオーバレイネットワークをうまく使い分けられていない
  - システム内でフラットな名前空間を使っている
    - プライベートIPアドレスを割当て (IPsec)
    - 特定のポートを割当て (sshポートフォワーディング)
  - アクセスを制限できない
    - 使い分けはユーザとアプリケーションに依存



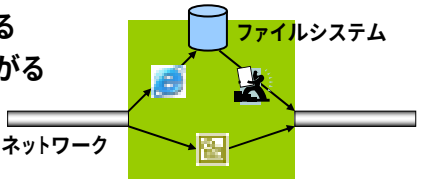
利便性の問題

- アクセスするホストの名前によってオーバレイネットワークを使い分ける必要がある
  - オーバレイネットワーク毎にホストに名前がつく
    - ホスト名、IPアドレス、ポート番号など
  - ユーザの負担になる
    - ベースネットワークと同じ名前でアクセスできない
    - 設定ファイルの書き換えが必要になる



安全性の問題

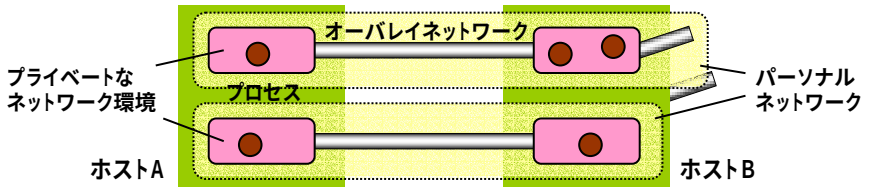
- ユーザはホスト上の全てのオーバレイネットワークを使えてしまう
  - プロセスやファイルシステムを介して、オーバレイネットワーク間で影響が伝播する
    - 機密情報が漏れる
    - 攻撃の影響が拡がる



  - ホストを共有している他のユーザや攻撃者にも使われる

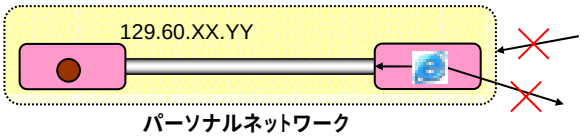
パーソナルネットワークの提案

- パーソナルネットワークとは？
  - ネットワークの仮想化 ＋ ホストの仮想化
    - オーバレイネットワーク
    - プライベートなネットワーク環境
  - オーバレイネットワークを完全に独立させる
    - 特定のネットワーク環境からしかアクセスできない
    - プロセスは1つのネットワーク環境に属する



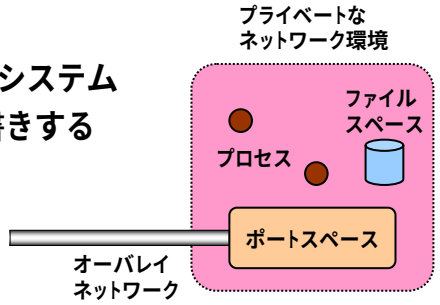
パーソナルネットワークの利点

- プロセスに見える唯一のネットワーク
  - プロセスはオーバレイネットワークの使い分けを意識しなくてよい
- 他のパーソナルネットワークから独立
  - ベースネットワークと同じIPアドレスを使える
  - 機密情報を漏らしたり、外部から攻撃されたりすることはない



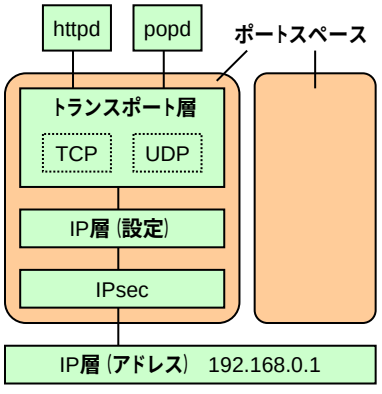
プライベートなネットワーク環境

- ポートスペース
  - 仮想的なネットワーク空間
  - プロセスと特定のオーバレイネットワークを結びつける
- ファイルスペース
  - 仮想的なファイルシステム
  - プロセスの読み書きするデータを隔離する



ポートスペース

- 1つのIPアドレスに対応するネットワーク空間を多重化した空間



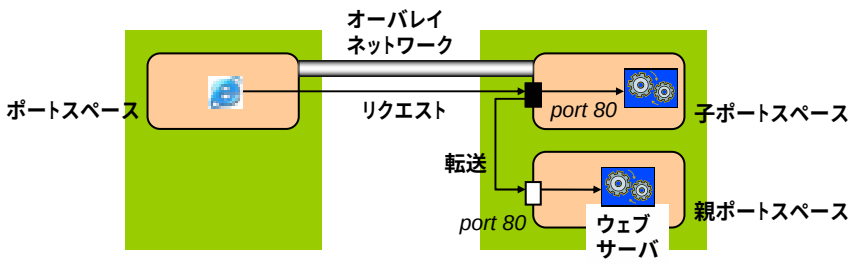
- IPアドレス毎に保持されていた情報を管理
  - ルーティング情報
  - サービスのバインド情報
- IPsecを個別に管理
  - 特定のオーバレイネットワークとバインドする

ポートスペースの特徴

- 新しいIPアドレスを必要としない
  - IPsecのレベルでポートスペースを振り分ける
- 互いに独立している
  - ポートスペースは全て同じIPアドレスを持つので、互いに直接アクセスできない
- ユーザが自由に使える
  - ネットワーク設定、サービスの立ち上げ
- 親ポートスペースを継承できる
  - ユーザが簡単にセットアップできる

ポートスペースの継承

- 親ポートスペースの状態を引き継げる
  - ネットワーク設定 (ルーティング等)
  - 提供されているサービス
- 設定やサービスの上書き、隠蔽もできる

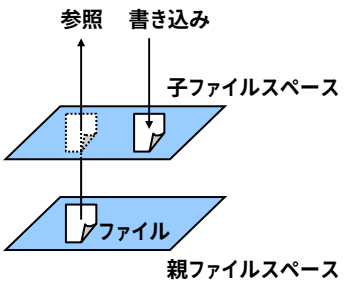


ファイルスペース

- ファイルシステムを多重化した空間
  - ファイル、ディレクトリ、マウント状態を管理
  - 互いに独立している
    - プロセスは1つのファイルスペースにしかアクセスできない
  - 親ファイルスペースを継承できる
    - 一からファイルシステムを作成する必要がない

ファイルスペースの継承

- ファイルをコピー・オン・ライトで子ファイルスペースにコピーすることができる
  - 親ファイルスペースのファイルを参照できる
  - ファイルへの書き込みは子ファイルスペースに
    - 以降の参照は子ファイルスペースから

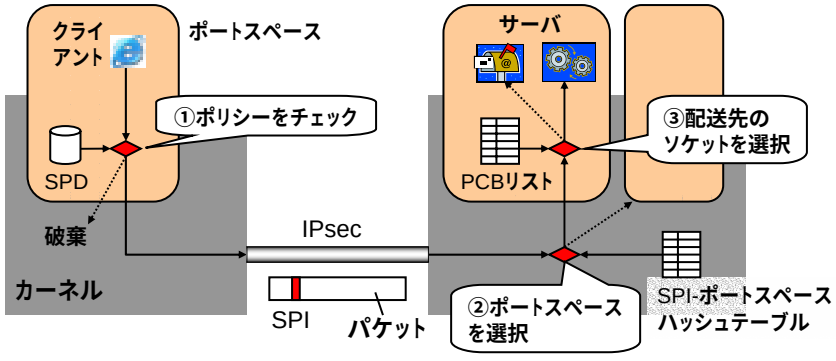


ポートスペースの実装

- FreeBSD 4.5をベースに開発
- mkportspaceシステムコールにより作成
  - 発行したプロセスとその子孫が所属
- カーネル内の以下のデータベースを管理
  - PCBリスト
    - ポートへのソケットのバインド情報など
  - IPsecセキュリティポリシー
  - ルーティングテーブル

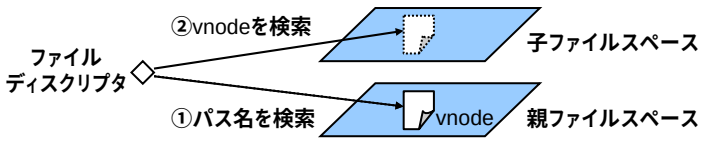
ポートスペース間通信

- IPsecのSPIを介して2つのポートスペースをバインドする
  - SPI：IPsecを識別するためのID



ファイルスペースの実装

- ユニオンファイルシステムを利用してファイルスペースの継承を実装
  - mount -t union /.filespace/1 /
- mkportspaceシステムコールで同時に作成
  - 既にオープンされているファイルの参照先を子ファイルスペース上のvnodeに付け替える



実験

- ポートスペースのオーバヘッドを調べた
  - TCP/IPの往復のレイテンシを測定
    - 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（サービスを継承）
- 実験環境
  - PC（PentiumIII-S 1.4GHz, メモリ512MB） 2台
  - 100baseTのイーサネットで接続
  - トランスポートモードのIPsec
    - 暗号化と認証にはNULLアルゴリズム

実験結果

	μsec
ベースネットワーク＋IPsec	131.3
パーソナルネットワーク	131.1
パーソナルネットワーク（継承あり）	131.0

- パケットを適切なポートスペースに配送するオーバヘッドはほとんどない
- サービスを継承することによるオーバヘッドもほとんどない

関連研究

- パーソナルVPN [Uzaki'02]
  - ユーザ単位でVPNへのアクセスを制限する
  - 目的のホストまで複数のVPNを結合できる
- リソーススペース[廣津'00]
  - VLANとの連携によりネットワークを多重化し、使い分けを強制できる
- jail / UML / VMware / Palladium[Microsoft]
  - 仮想的な環境を一から構築する
  - ネットワークとの統合はされていない

まとめ

- パーソナルネットワークを提案した
  - ユーザが複数のオーバレイネットワークを容易にかつ安全に使い分けられる
    - 各オーバレイネットワークを独立させる
  - ＯＳがプライベートなネットワーク環境を提供する
    - ポートスペース
    - ファイルスペース

今後の課題

- パーソナルネットワークの構成に制約をつけられるようにする
  - 現在はユーザの努力に任されている
- ＯＳによるリソース管理を見直す
  - プライベートなネットワーク環境の作成者には擬似的に管理者の権限を与えたい