Design and Implementation of Secure IPv6 Communication Architecture using Non-negotiated Specific Service Addresses

大阪大学 大学院情報科学研究科
村田研究室
西田　和生

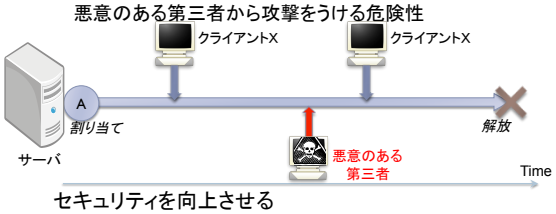
1

従来の通信方式

- 従来の通信は IP アドレスをノードに対して割り当て
  - IP アドレスはノードが有効な間、同じものを使用

→高いセキュリティを実現することはできない

- IPアドレス情報の公開、スキャンにより特定され、悪意のある第三者から攻撃をうける危険性



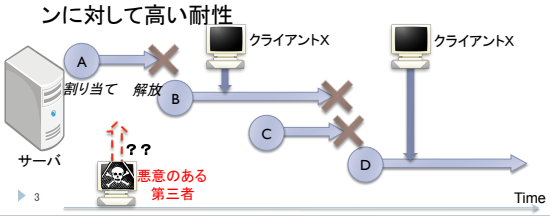
セキュリティを向上させる
Unified Multiplex 通信アーキテクチャを提案[4]

[4] H.Kitamura,S.Ata,andM.Murata "IPv6 ephemeral addresses," Internet Draft draft-kitamura-ipv6-ephemeral-address-01, July 2009.

2

Unified Multiplex 通信アーキテクチャ (Unified 通信)の概要

- ノードは同じアドレスを使い続けるのではなく、セッションごとにアドレスを変更
  - アドレスの有効期間は短い
  - 接続が開始されると対象ホスト以外から接続不可能
- IPv6の広大なアドレス空間を利用することでスキャンに対して高い耐性



3

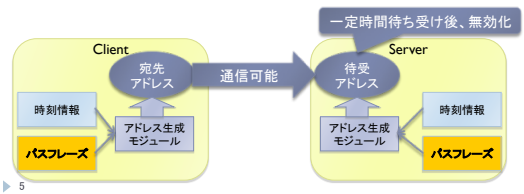
研究の目的

- 短い時間で変化するサーバの待受アドレスをクライアントが安全に知る機構が必要
  - **第三者に知られることなく、サーバ、クライアント間で通信するためのアドレスを決定するための機構**
  - **導入の容易性を考えエンドノードへの更新のみで実現可能な機構**
- 新たな非交渉型アドレス決定機構を提案
- 提案手法の動作確認のため設計し、実装

4

非交渉型待受アドレス決定機構の概要

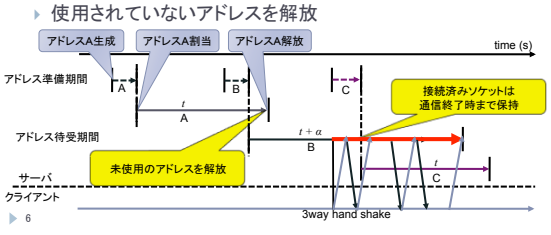
- サーバ、クライアント間でアドレス生成情報を同期させ、同一アドレスを生成
  1. サーバ、クライアントはパスフレーズを事前に共有
  2. サーバはパスフレーズ＋時刻情報によりアドレスを生成
  3. クライアントはパスフレーズ＋時刻情報によりサーバと同じアドレスを生成することで通信可能



5

非交渉型待受アドレス決定機構の設計 (サーバ側)

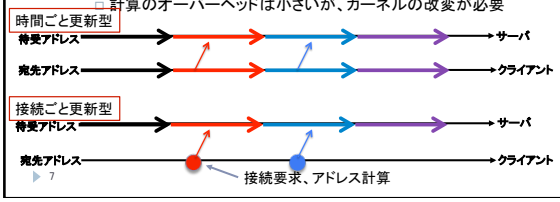
- クライアントごとに異なる待受アドレスを生成
- 一定期間ごとに待受アドレスを更新
  - 新しいアドレスを生成
  - 待受プロセスに割り当て
  - 使用されていないアドレスを解放



6

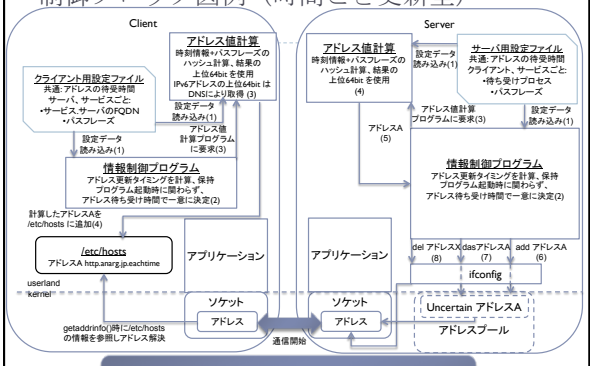
非交渉型待受アドレス決定機構の設計（クライアント側）

- 一定時間ごとに変動するサーバの待受アドレスを計算
  - 時間ごと更新型
    - 一定時間ごとにサーバのアドレスを計算
    - 計算のオーバーヘッドが大きいが、実装は容易
  - 接続ごと更新型
    - クライアントが接続する直前にサーバのアドレスを計算
    - 計算のオーバーヘッドは小さいが、カーネルの改変が必要



7

制御ブロック図例（時間ごと更新型）



8

時間ごと更新型を実装し、動作を確認

まとめと今後の課題

- 短い時間で変化するサーバの待受アドレスをクライアントが安全に知る機構を提案
  - 非交渉型待受アドレス決定法の設計、実装仕様策定
    - 時間ごと更新型決定法は実装、動作確認済み
  - 第三者に知られることなくサーバ、クライアント間で待ち受けアドレスを共有可能
  - 安全にサービスを利用することが可能
- 今後の課題
  - 接続ごと更新型アドレス決定法の実装、動作確認

9