Preserving TCP Connection Across Host Address Changes

名城大学　理工学部　情報工学科
渡邊研究室4年　土井敏樹

- 本資料は下記論文を基にして作成されたものです。文書の正確さは保証できない為、正確な知識を求める方は原文を参照してください。

- 題目
  - Preserving TCP Connections Across Host Address Changes
- 著者
  - Vassilis Prevelakis, Sotiris Ioannidis
- 発行
  - 2006
- 発行所
  - Computer Science Department, Drexel University
  - Computer Science Department, Institute of Technology

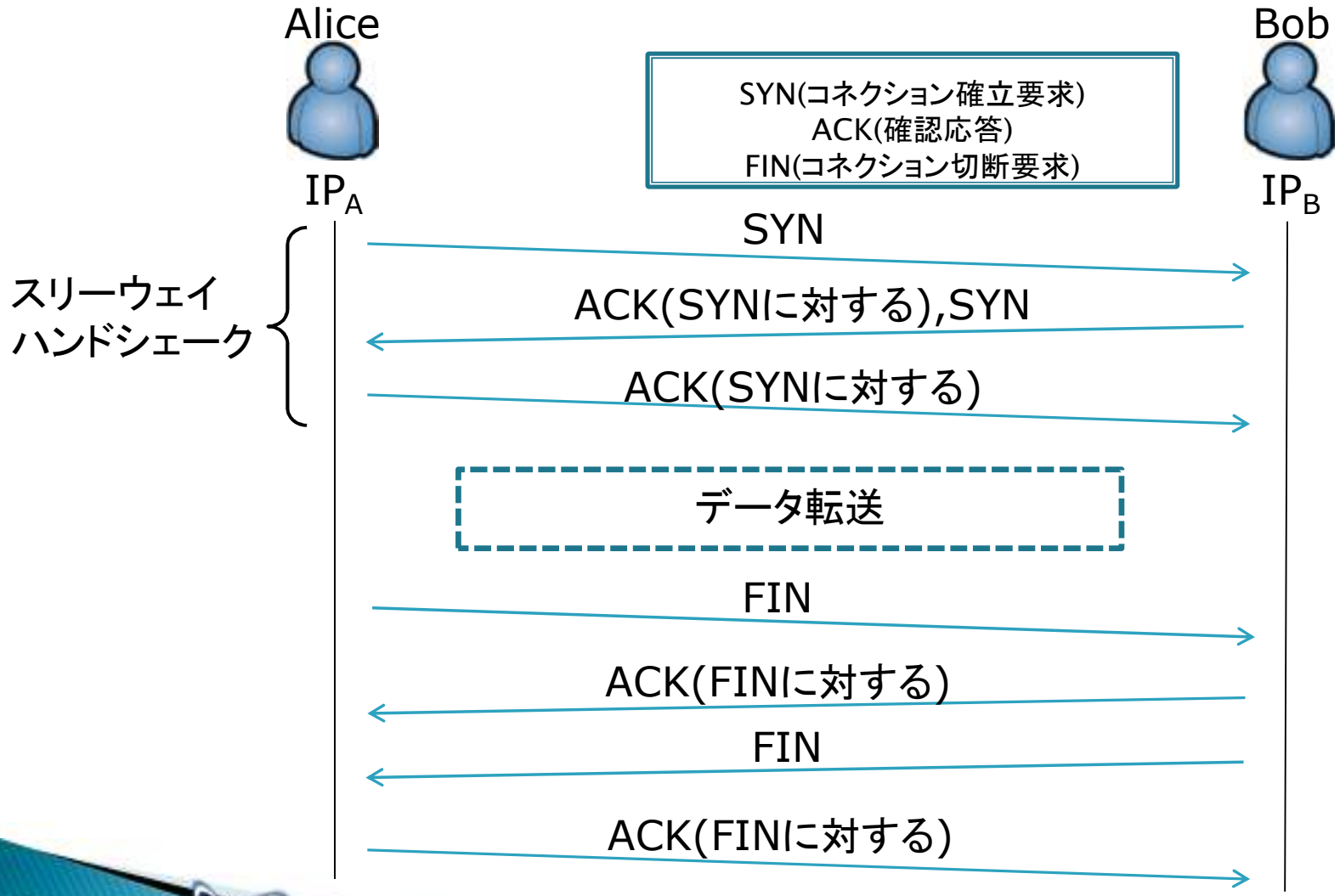
Abstract – アブストラクト

- 今日のインターネット環境では短い接続(short-lived connection)が多くを占める
- 接続の両端ホストのIPアドレス変更が重要
- アドレスの変更とそこからの変更を認識するメカニズムを提案

Introduction – 序論

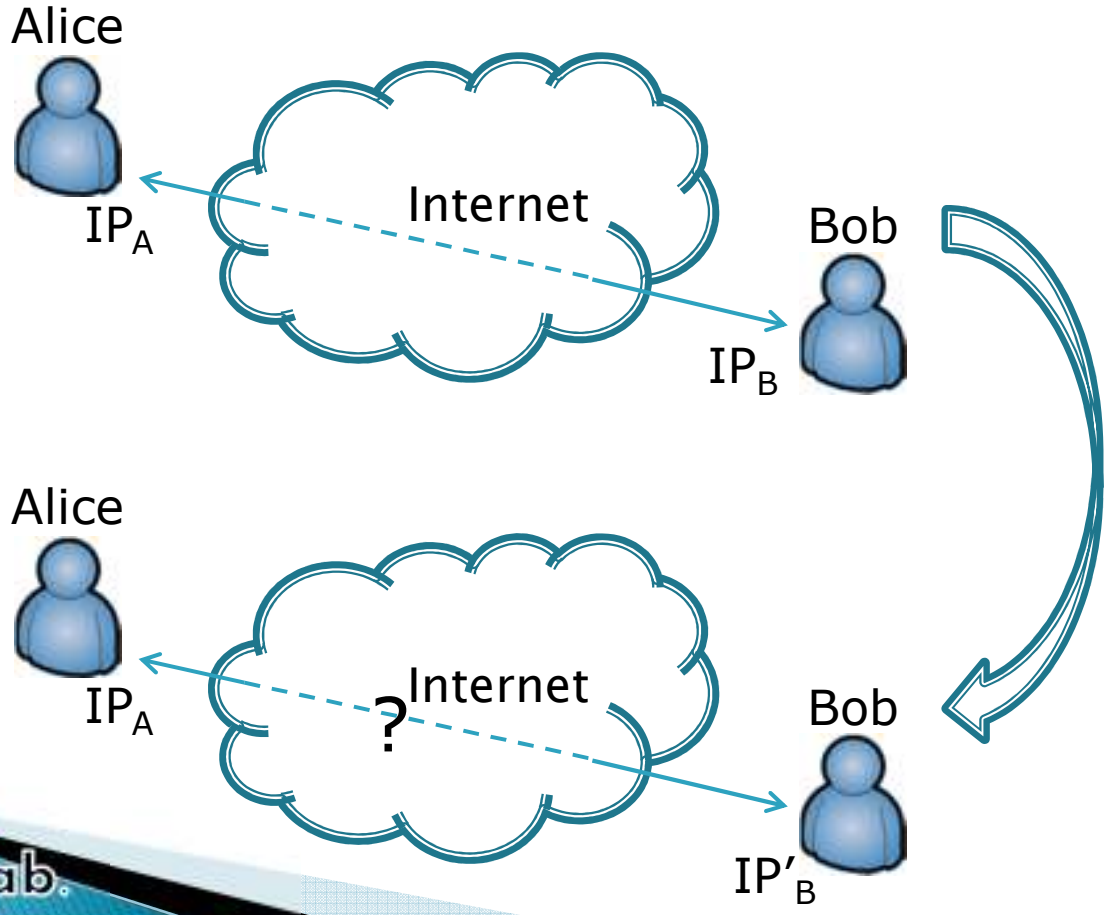
- IPに基づくアプリケーションでは一般的に長期間に渡って同じままであると仮定される
- 固定発信元と宛先IPアドレスに依存
  - 確立された接続(ex.SSHセッション)はアドレス変更に対応できない
  - エンドポイントは接続を継続する必要
- 接続を継続するための提案
- セキュリティ上の影響

TCP Connection – TCP接続



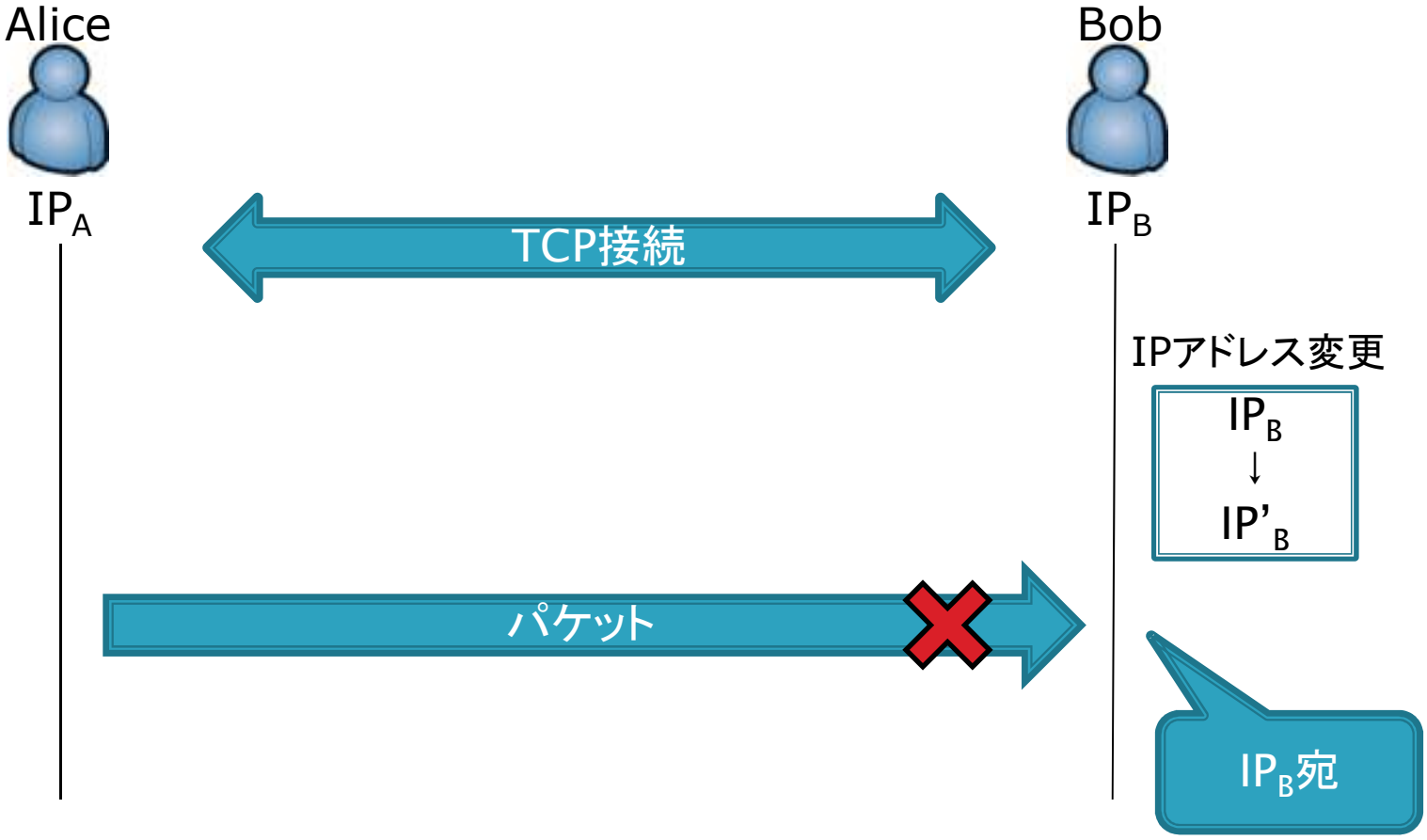
Connection Redirection(1)

- あるホストのIPアドレスが変わり、2ホスト間の通信が中断されてしまう



Connection Redirection(2)

- リダイレクト・・・接続先を変更する事



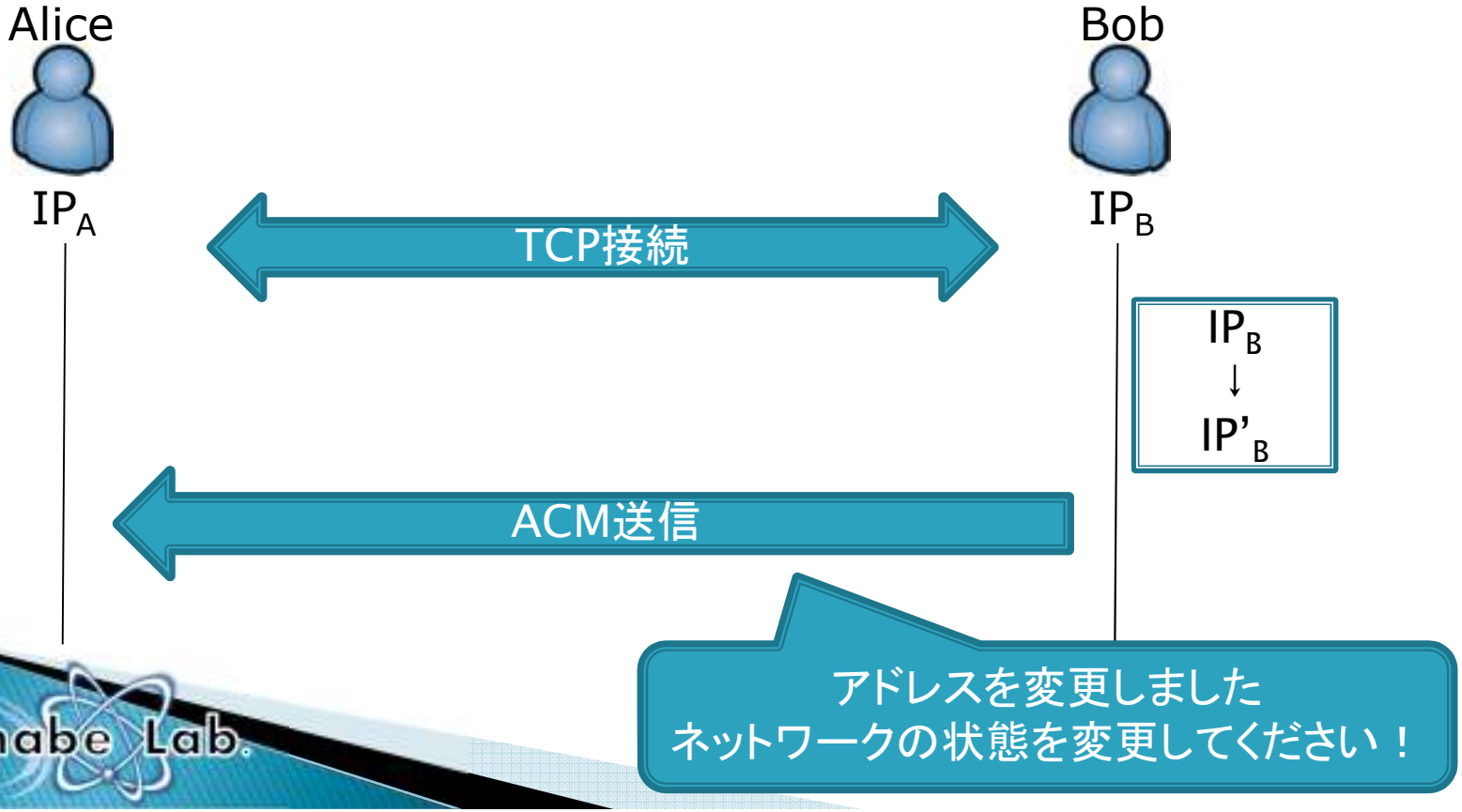
起こりうる現象

- ICMPエラー(アドレス到達不可能)
  - 宛先アドレスが変更されている為到達不可能
- パケットが失われる
  - 宛先アドレスがないので途中でパケットが失われてしまう
    ⇒Aliceは接続がタイムアウトするまで待ち状態
- TCP RST
  - RST・・・TCP接続を中断したい場合などに送信されるパケット
  - 受信した側では接続要求が拒否されたと認識
    ⇒現在のTCP接続を破棄または強制終了

ACM(Address Change Message)の使用

ACM(Address Change Message)

- 全ての場合において接続は失われる
  ⇒再確立の必要性
  ⇒ACM(Address Change Message)の使用



ACMのパケットフォーマット

古い送信元IP	新しい送信元IP	宛先IP	送信元ポート	宛先ポート	認証	ナンス

- Nonce(ナンス)
  - 文字列または数字列
  - ハッシュを用いた認証でなりすましを防ぐ為に使用される

- Bob–Alice間の全ての確立された接続に影響を与える場合
- 特定のTCP接続にのみ適用される場合

  ⇒全てのTCP接続に個々のACMを送る必要性

ACMの問題点

TCP接続をリダイレクトする為に使用

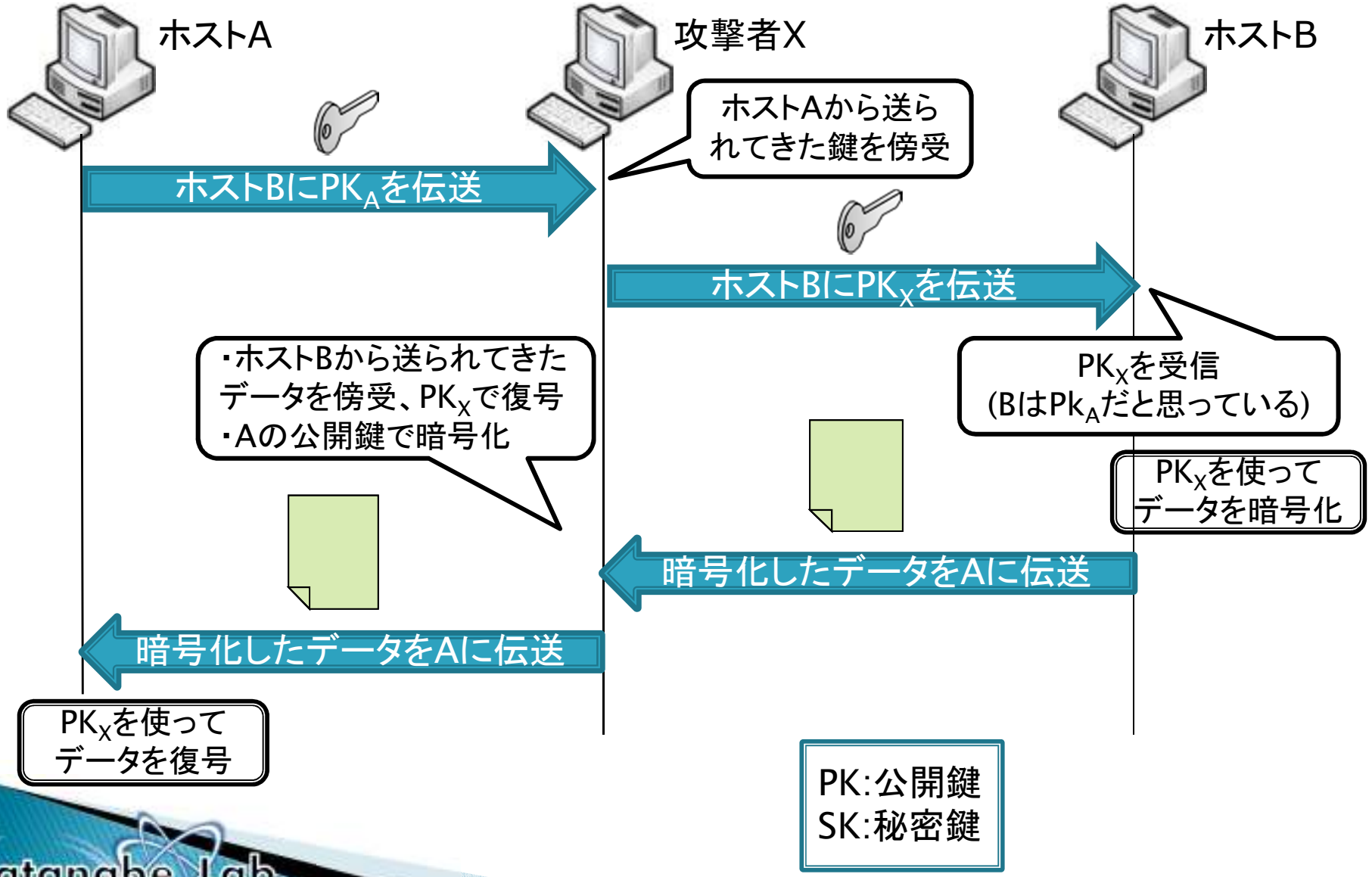
既存の接続のハイジャックに使用される可能性

パケットインジェクション攻撃
データ改竄攻撃

Packet Injection

- 攻撃者がACMをホストに送信する
  - 送信されたホストは通信相手のアドレスが変わったと認識
  - Injection・・・注入
- 通信チャネル上で傍受する攻撃者には簡単
  - ネットワークトラフィックを監視することが簡単である無線ネットワーク上は特に心配
- 攻撃者が推測できないようなシーケンス番号の使用
  - 初期値はスリーウェイハンドシェイクでランダムに決定
  - 分割されたデータごとにつけられる番号

man in the middle attack – 中間者攻撃

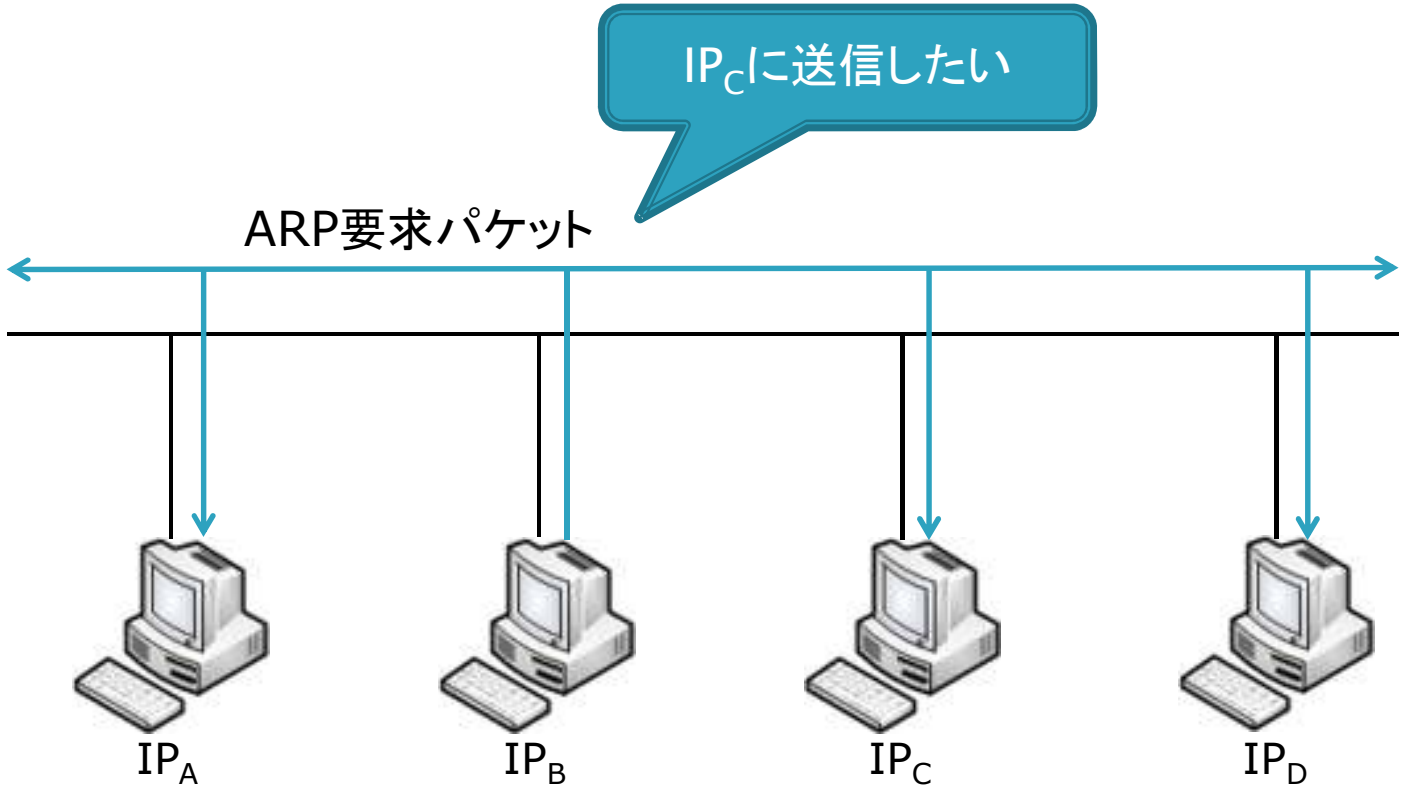


man in the middle attack – 中間者攻撃

- 2ホスト間で交換されるパケットを検査・変更できる
- ACMを守るために共通鍵を使用する
  - セッション中に鍵を送信　⇒　攻撃者が傍受・変更できる
    ⇒前もって鍵を交換する
    ⇒第三者機関を利用する
- 攻撃者と被害者が同じLAN内にあると一般的に困難
  - ARPスプーフィングの使用
    ⇒攻撃者を介してトラフィックが流れるのを許可

ARP Spoofing(1) – ARPとは

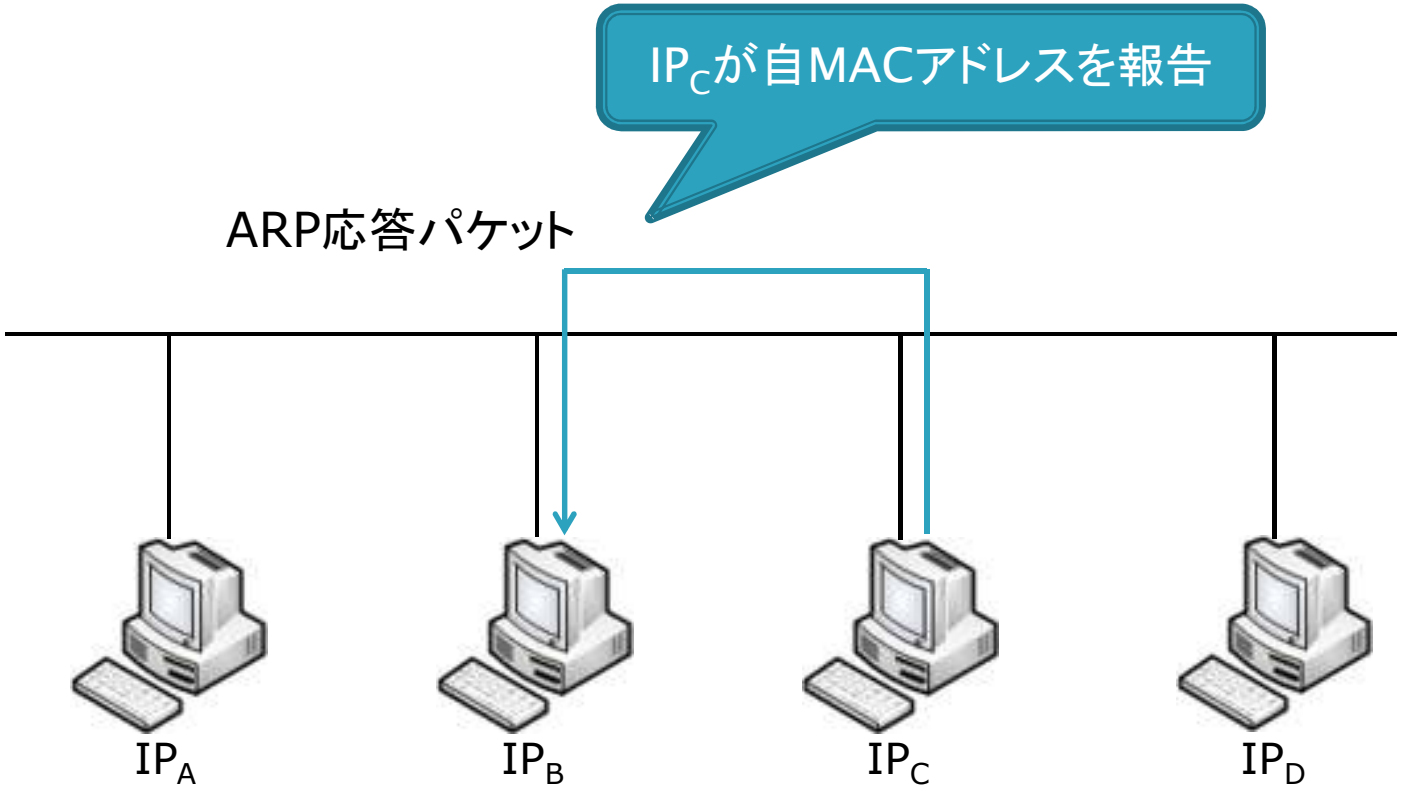
ホストBからホストCへの通信の場合



Watanabe Lab.

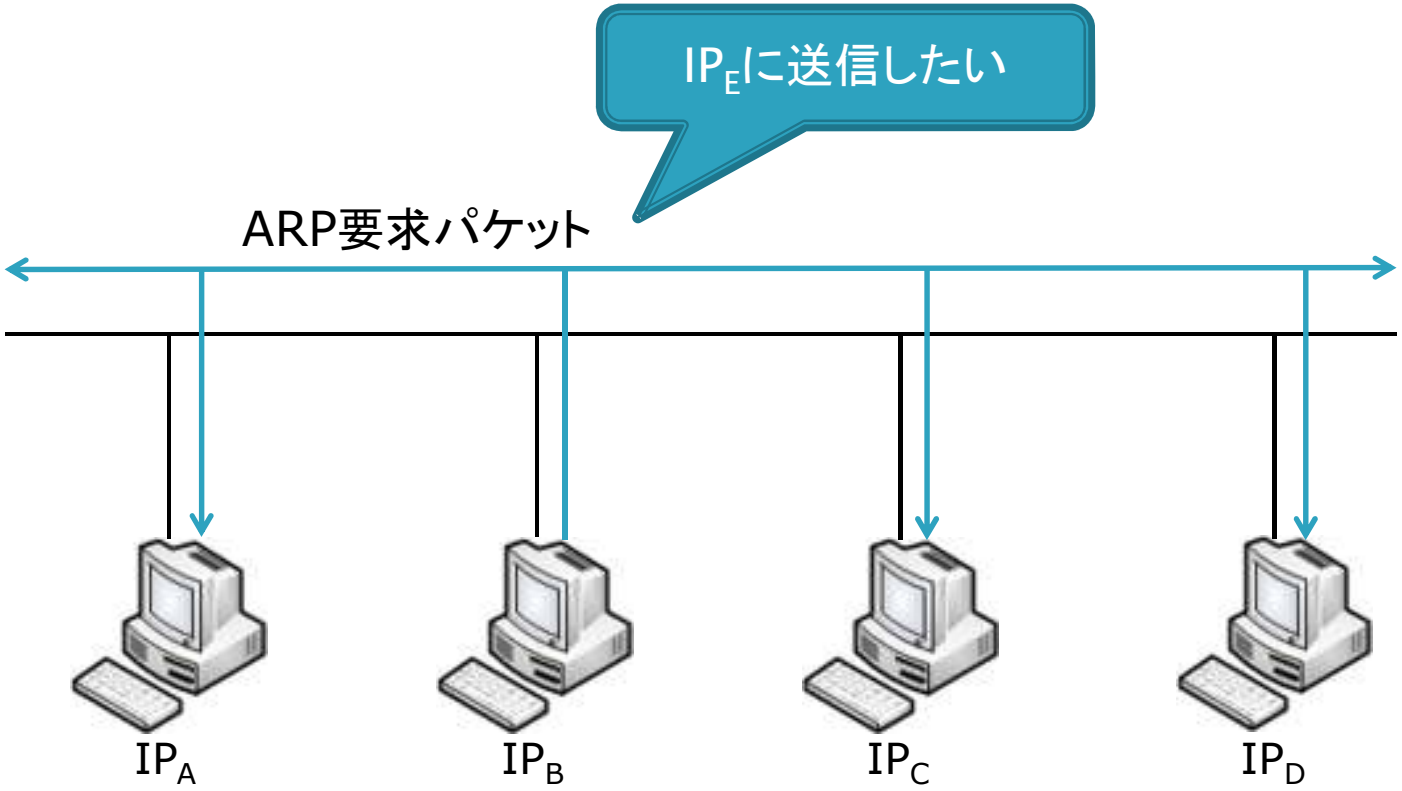
ARP Spoofing(2) – ARPとは

ホストBからホストCへの通信の場合

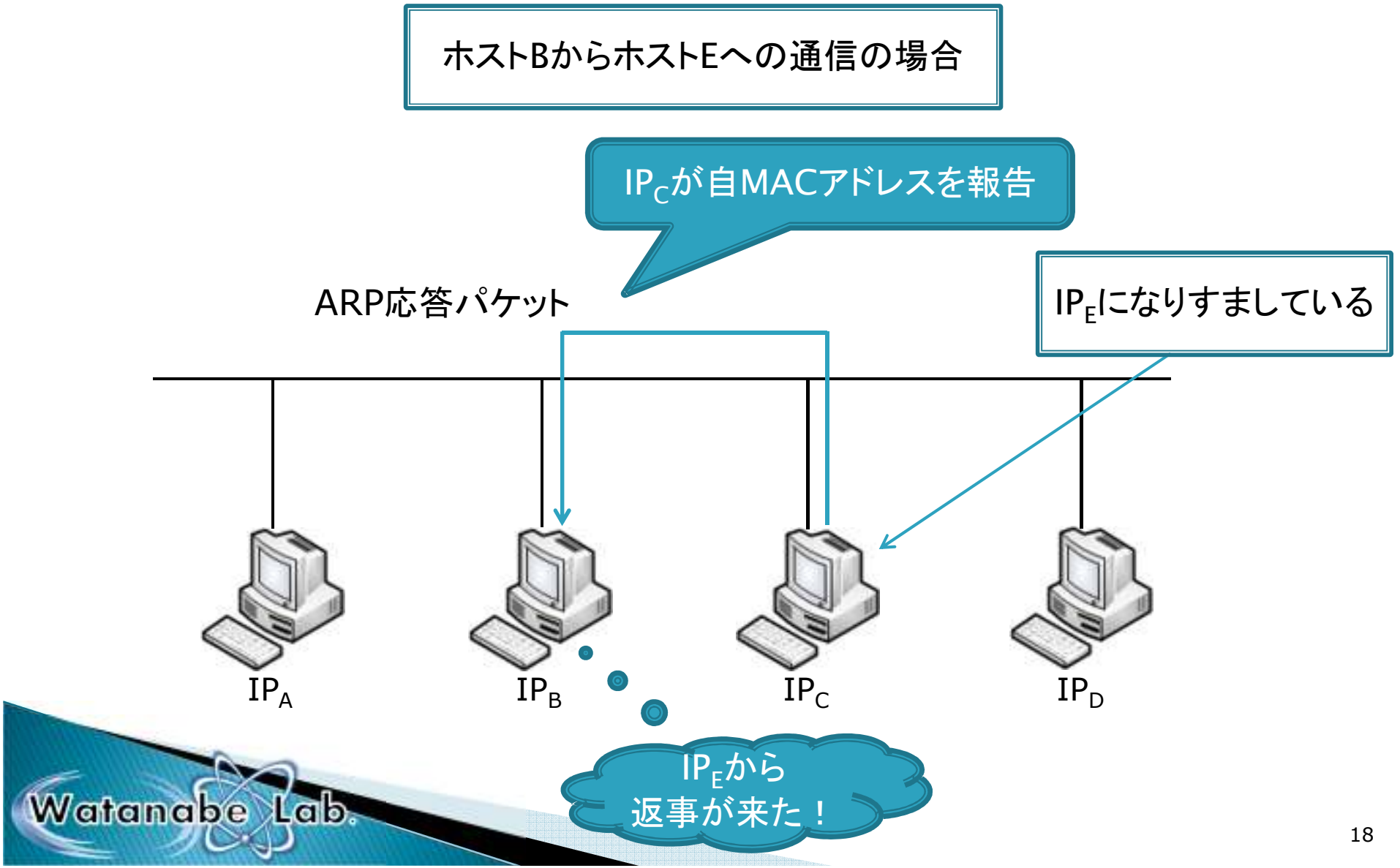


ARP Spoofing(3) – ARPの悪用

ホストBからホストEへの通信の場合



ARP Spoofing(4) – ARPの悪用



Global vs. local redirects – ACM使用方法

- Global
  - 2ホスト間の全てのアクティブなセッションに適用される単一のリダイレクトリクエストを送る
  - リダイレクトリクエストを認証する為の、セッション開始時に確立したトークンを使用可
- Local Redirect
  - 個別の接続毎にACMを送る
  - 接続上で盗聴ができない場合は以下の事は出来ないと予測
    - 正しい組み合わせを予測
    - 全ての可能な組み合わせを試すことによって総当たり攻撃を仕掛ける(探査空間が大きいので)

Global vs. local redirects

- 盗聴者問題を解決できない
  - ⇒平文(in the clear)でトークンを送らない
  - ⇒トークン確立の為にDH鍵交換を使う
- DH(Diffie-Hellman)鍵交換
  - 安全でない通信路を使って秘密鍵を送受信する鍵交換方式
  - 中間者攻撃に対し脆弱
  - DoS攻撃に利用されてしまう可能性
    - DH鍵交換を繰り返し実行する事によって

  ⇒2つの技術によってこの問題を解決

Global vs. local redirects

- 長いセッションの高い交渉(expensive negotiation)を制限する
  - ⇒長い接続がいくつも起こることの内容に制限する

- 以前のセッションから許可情報(allows information)を使う
  - SSHに使う認証メカニズムに似ている
  - 2ホスト間で最初の接続が行われた時にホスト鍵を転送
  - 認証手順に両ホストは含むが個々の接続は含まない
    ⇒オーバーヘッドを減らすことが可能

まとめ

- TCP接続が通信しているホストのアドレス変更を生き残る事が出来るシステムを提案

- 提案に対するハイジャックや中間者攻撃について解説

参考文献

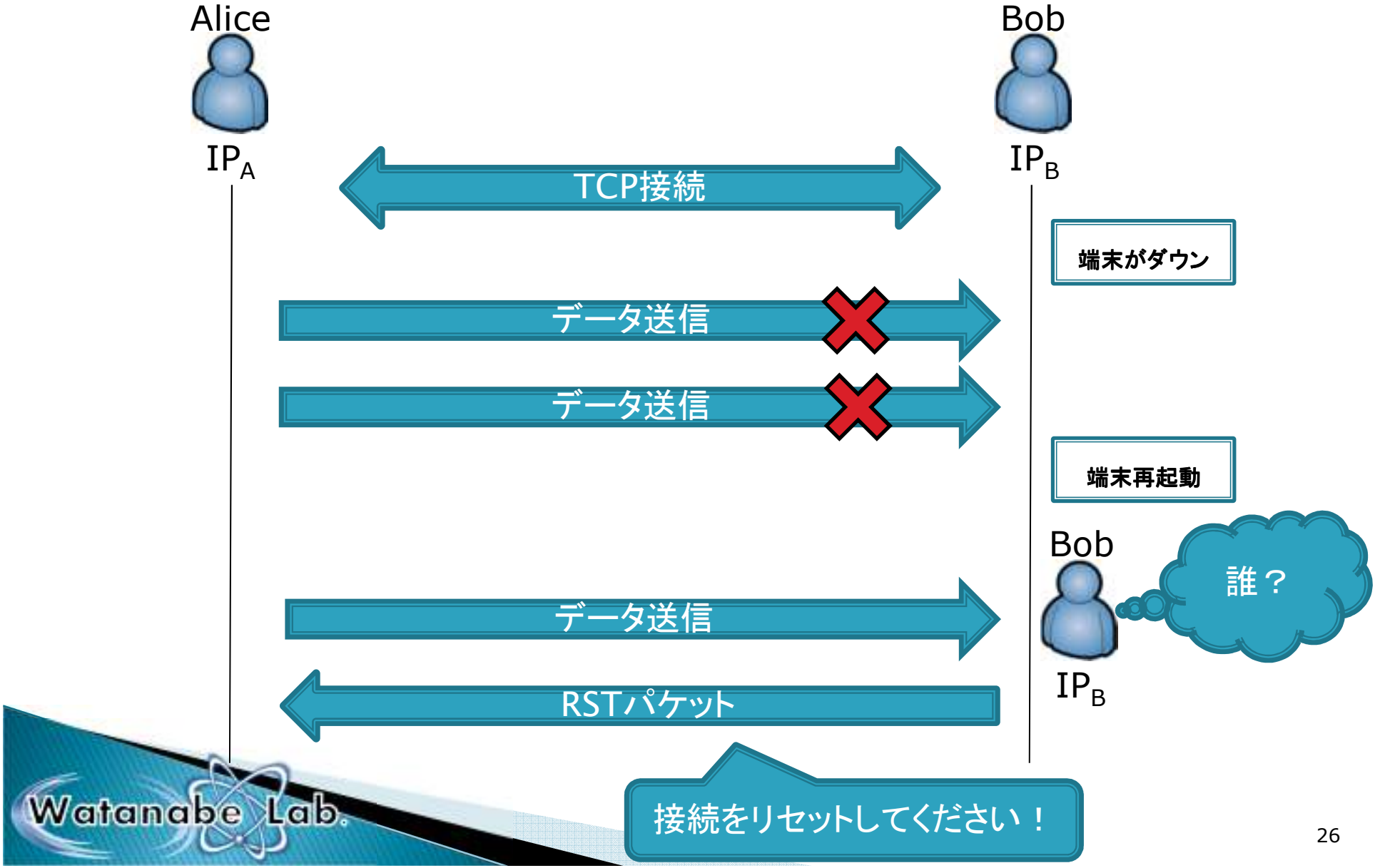
- ARPスプーフィング
  - http://itpro.nikkeibp.co.jp/article/Keyword/20080819/312977/
  - http://herald.jugem.jp/?eid=67
- TCP RST
  - http://www.7key.jp/nw/tcpip/tcp/rst.html
- ICMP
  - http://www.tef-room.net/main/icmp.html
- 中間者攻撃
  - http://ewords.jp/w/E4B8ADE99693E88085E694BBE69283.html

参考文献

- Nonceについて
  - http://www.wdic.org/w/WDIC/%E3%83%8A%E3%83%B3%E3%82%B9

END

補足資料 – TCP RST – TCP Reset



補足資料 – 用語(1)

- ISP(Internet Services Provider)
  - インターネット接続業者
  - 各種回線を通じて顧客である企業や家庭のコンピュータをインターネットに接続する
- Node
  - ネットワークを構成する一つ一つの要素の事
  - ex.コンピュータ、ハブ、ルータ等通信機器
- Stack
  - データ構造の一種
  - 最後に入力したデータが先に出力される特徴

補足資料 – 用語(2)

- Packet
  - コンピュータ通信において送信元アドレスなどの制御情報を付加された小さなデータの纏まりの事
  - データをパケットに分割して送受信する通信方式をパケット通信と呼ぶ
- Diffie–Hellman鍵交換(DH法)
  - 公開鍵暗号が考案される以前の1976年に考案
  - 安全でない通信経路を使って秘密鍵を安全に送受信するための鍵交換方式
  - 秘密鍵その物では無く乱数と秘密鍵から生成した公開情報を送受信
  - 中間者攻撃には弱い

補足資料 – 用語(3)

- Overhead
  - 何らかの処理を進める際に間接的に必要となる処理
  - またそれにより発生する負荷の大きさ
  - 処理に時間がかかるようになるなどシステムの負荷になる物
- BSD(Berkeley Software Distribution)
  - UNIX系OS
- OpenBSD
  - UNIXライクなOS
  - BSD系OSのうち高いセキュリティ性を持つのが特徴

補足資料 – 用語(5)

- Kernel
  - OSの基本機能を実装したソフトウェア
  - OSの中核部分
  - 提供している機能
    - アプリケーションソフトや周辺機器の監視
    - ディスクやメモリなどの資源の管理
    - 割り込み処理
    - プロセス間通信
- Host
  - ネットワークを介して別の機器やコンピュータサービスや処理能力などを提供するコンピュータ

補足資料 – 用語(6)

- RemoteHost
  - ネットワークを介して接続した先の機器
- LocalHost
  - 現在使用しているシステム、自分の操作しているコンピュータ
  - IPアドレス：127.0.0.1
- MobileIPv6
  - IPv6の拡張機能
  - 移動通信中でも同じIPアドレスを使って途切れる事無く通信を継続するための仕組み
  - 移動通信ノード – (ホームエージェント)– 通信相手

補足資料 – 用語(7)

- DHCP(Dynamic Host Configuration Protocol)
  - インターネットなどのネットワークに一時的に接続するPCに、IPアドレスなど必要な情報を自動的に割り当てる
  - 接続していたPCが通信を切断すると、自動的にアドレスなどを回収して新たに接続してきた他のPCに割り当てる
- Traffic
  - 音声や文書、画像などのデジタルデータ
  - ネットワーク上を移動する
- Transaction
  - 関連する複数の処理を一つの処理単位として纏めたもの

補足資料 – 用語(8)

- Time Stamp
  - 電子データの作成や更新などが行われた日時を示す情報
  - コンピュータの内蔵時計に依存し、必ずしも正確ではない
- Negotiation
  - 2台の機器が通信を確立する際に、通信速度などの情報を相互に交換しながら通信設定を決定していく事
  - 殆どのデータ通信では何らかのネゴシエーションが必要
- Integrity Check
  - 完全性チェック
  - 元の状態と一致しているかのチェック

補足資料 – 用語(9)

- ARP Spoofing(Address Resolution Protocol –)
  - ARPの仕組みを悪用した攻撃
- SSH(Secure Shell)
  - ネットワークを介して別のコンピュータにログインしたり、他のマシンへファイルを移動したりする為のプログラム
  - ネットワーク上を流れるデータは暗号化される
- ICMP(Internet Control Message Protocol)
  - プロトコルの一種
  - データが届かないor障害があったときに使用
  - pingに使われている

補足資料 – 用語(10)

- Endpoint
  - ネットワークに接続されたパソコンやPDA、携帯電話などの
    ネットワーク端末の総称