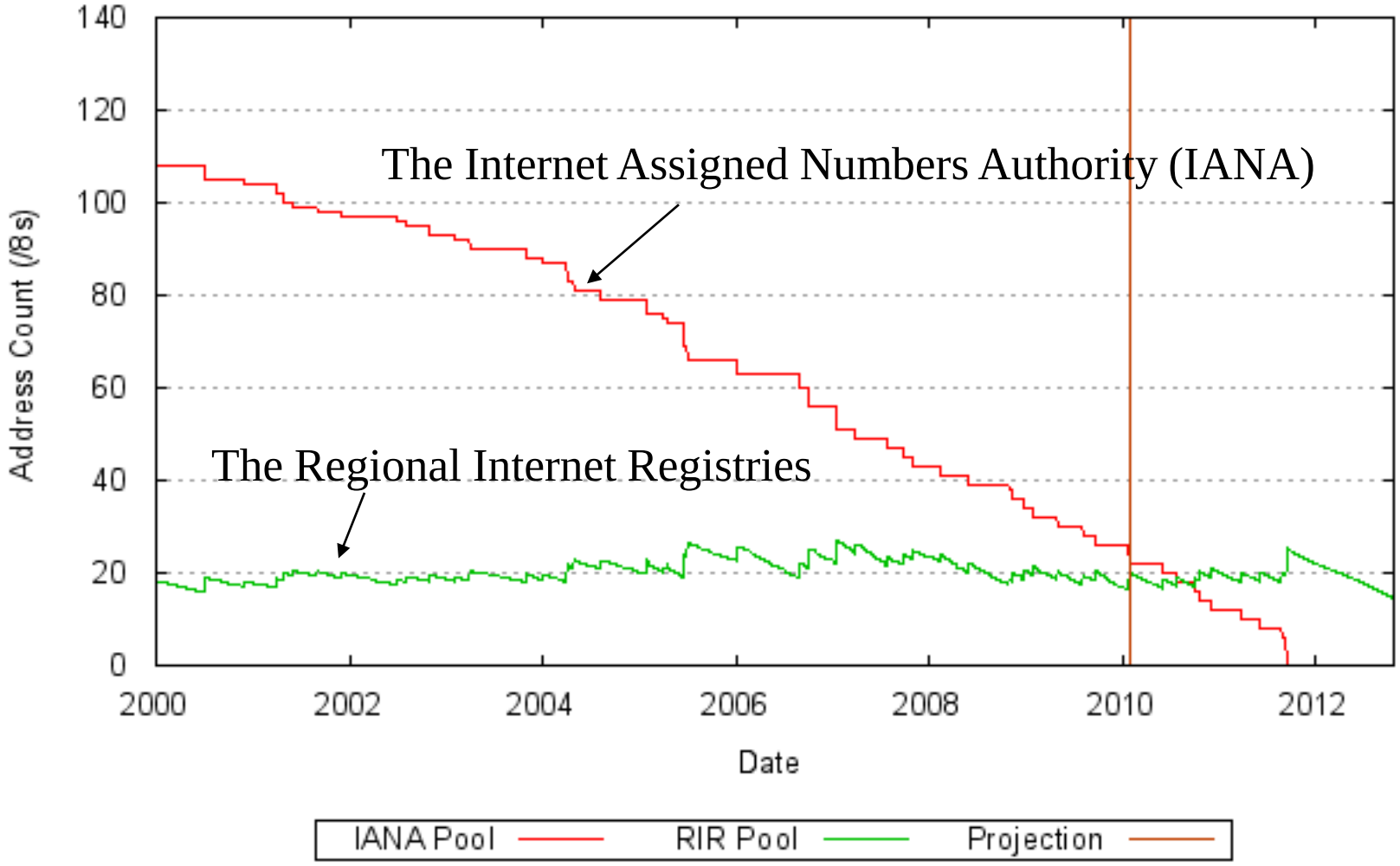
IPv6とセキュリティ

東京電機大学　教授
内閣官房情報セキュリティセンター
情報セキュリティ補佐官
佐々木良一
sasaki@im.dendai.ac.jp

IPv4のIPアドレス枯渇問題



何度も叫ばれてきたが、いよいよ現実の問題に
iPadの普及もこれに拍車を

米国連邦政府の動き

米国　Federal Chief Information Officer　Kundraのメモ（９月２８日）http://www.cio.gov/Documents/IPv6MemoFINAL.pdf

＜対応指示＞

・2012年度末までに連邦政府の外部サービス（web、メール、DNS、　ISP等）をnative IPv6対応にすること。

・2014年度末までにクライアントアプリ（外部サービスにつながるもの）　をnative IPv6対応にすること。

・2010年10月30日までに、各省はIPv6移行責任者を定め米国行政管理予算局に提出すること。

IPv6のIPv4に勝るメリットは？

1. 膨大なアドレス数
2. すべての機器にグローバルアドレスを割り当てることが可能なので、NATが不要
3. IPSecが標準実装されたことにより、セキュリティが向上
4. フラグアンドプレイにより、設定不要でネットワークに繋がること
5. ヘッダが固定長なので、通信が高速

IPv6の登場

「IPv6はIPSecが標準実装されたことにより、セキュリティが向上する」といわれているが

IPSecで実現できるのは主に通信路暗号の機能だけ

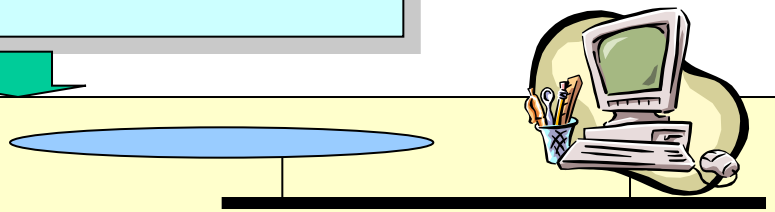
セキュリティを守るためにはこれだけでは不十分

DDoS攻撃などはIPSecがあっても防止できない

しかも、IPv4とIPv6共存状態ではセキュリティ上、ディペンダビリティ上のいろいろな問題が

IPv6におけるセキュリティ課題の整理

攻撃手段
DoS、侵入、不正アクセス、なりすまし、通信傍受



影響対象

ネットワーク、アプリケーション、ノード（サーバ／端末）

（1）仕様上の問題、実装上の問題

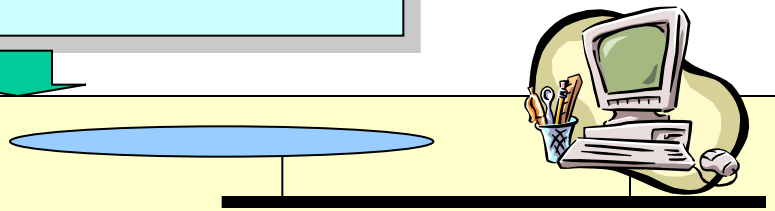
（2）IPv6単体での問題、IPv4,v6共存下における問題

（3）セキュリティ固有の問題、ディペンダビリティと関連する問題

下線がより重要になる問題

IPv6におけるセキュリティ課題の整理

攻撃手段
DoS、侵入、不正アクセス、なりすまし、通信傍受



影響対象

ネットワーク、アプリケーション、ノード（サーバ／端末）

（1）仕様上の問題、実装上の問題

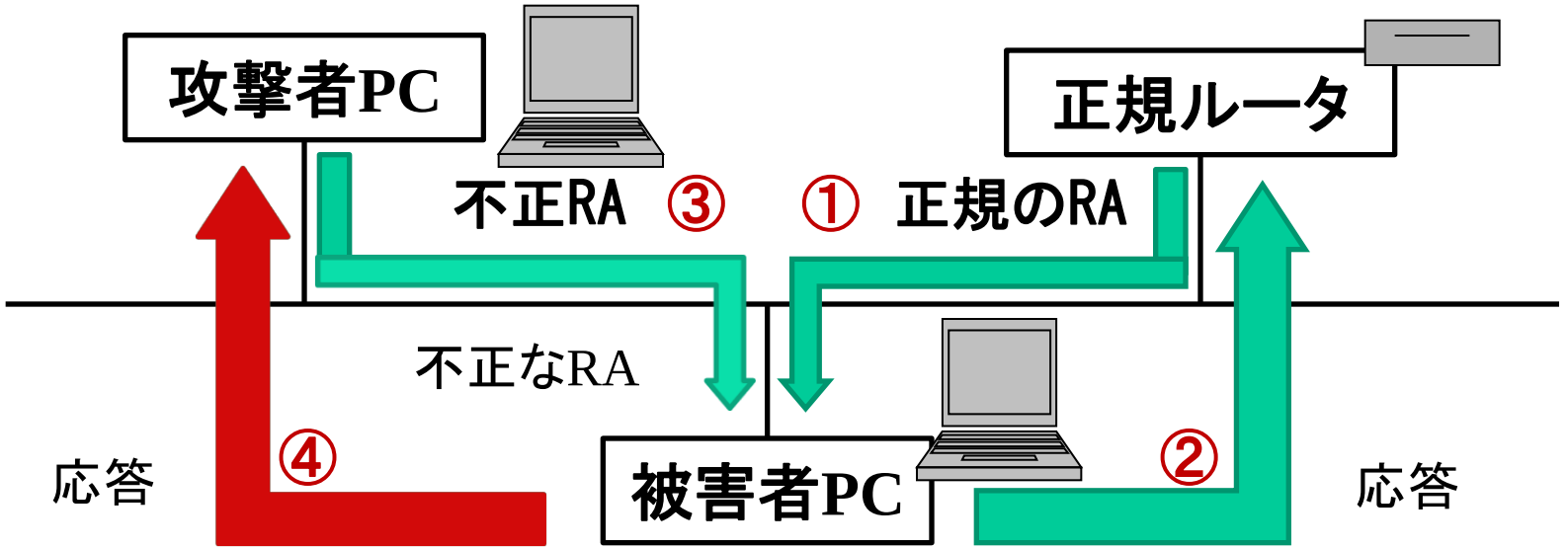
（2）IPv6単体での問題、IPv4,v6共存下における問題

（3）セキュリティ固有の問題、ディペンダビリティと関連する問題

IPv6単体での問題の一例

不正RA

正規のルータへの成りすまし

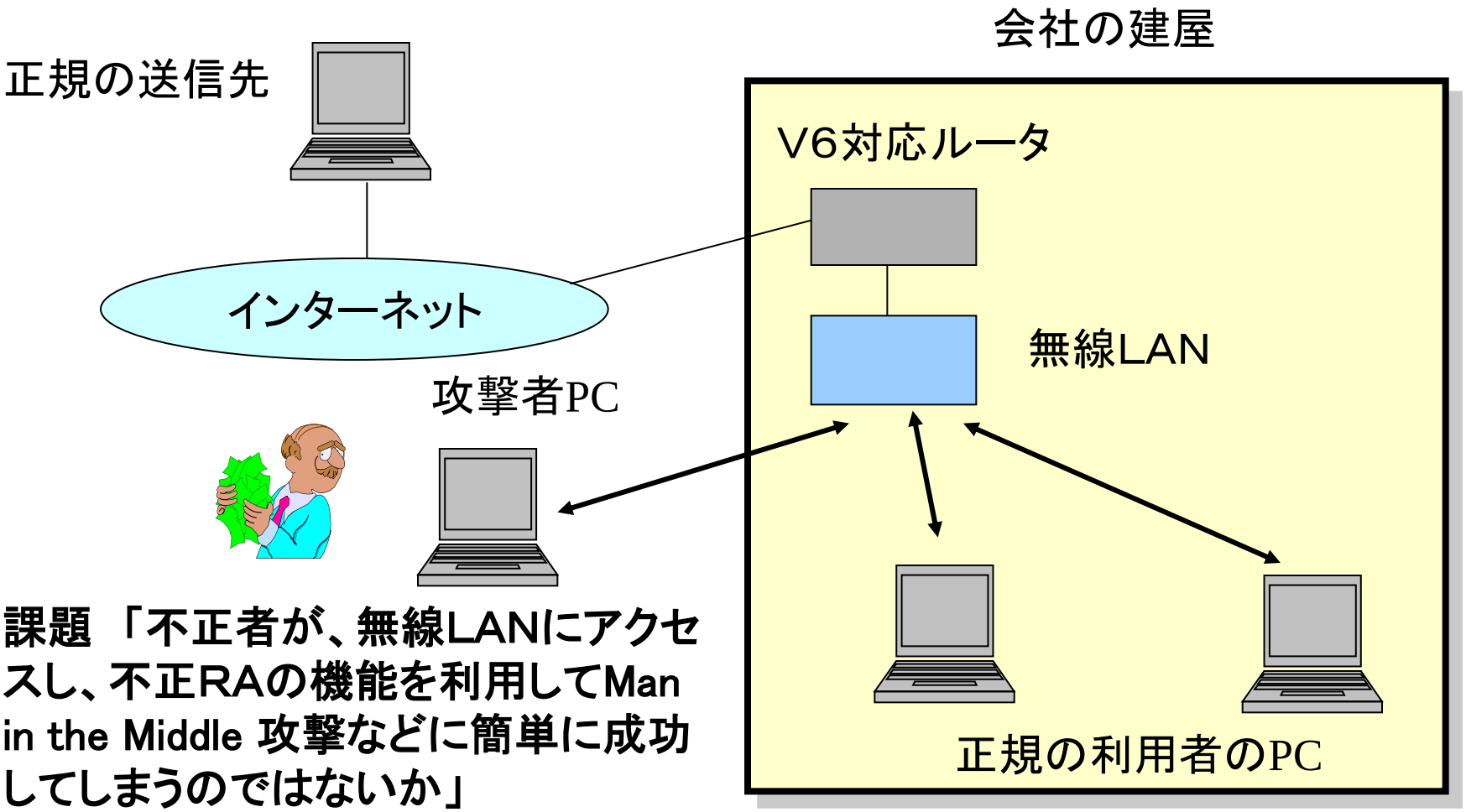


①によるアドレス生成
③によるアドレス生成

RA : Router Advertisement

＜IPv6では1つのPCで複数のアドレスを用いうる＞

東京電機大学での実験（1）

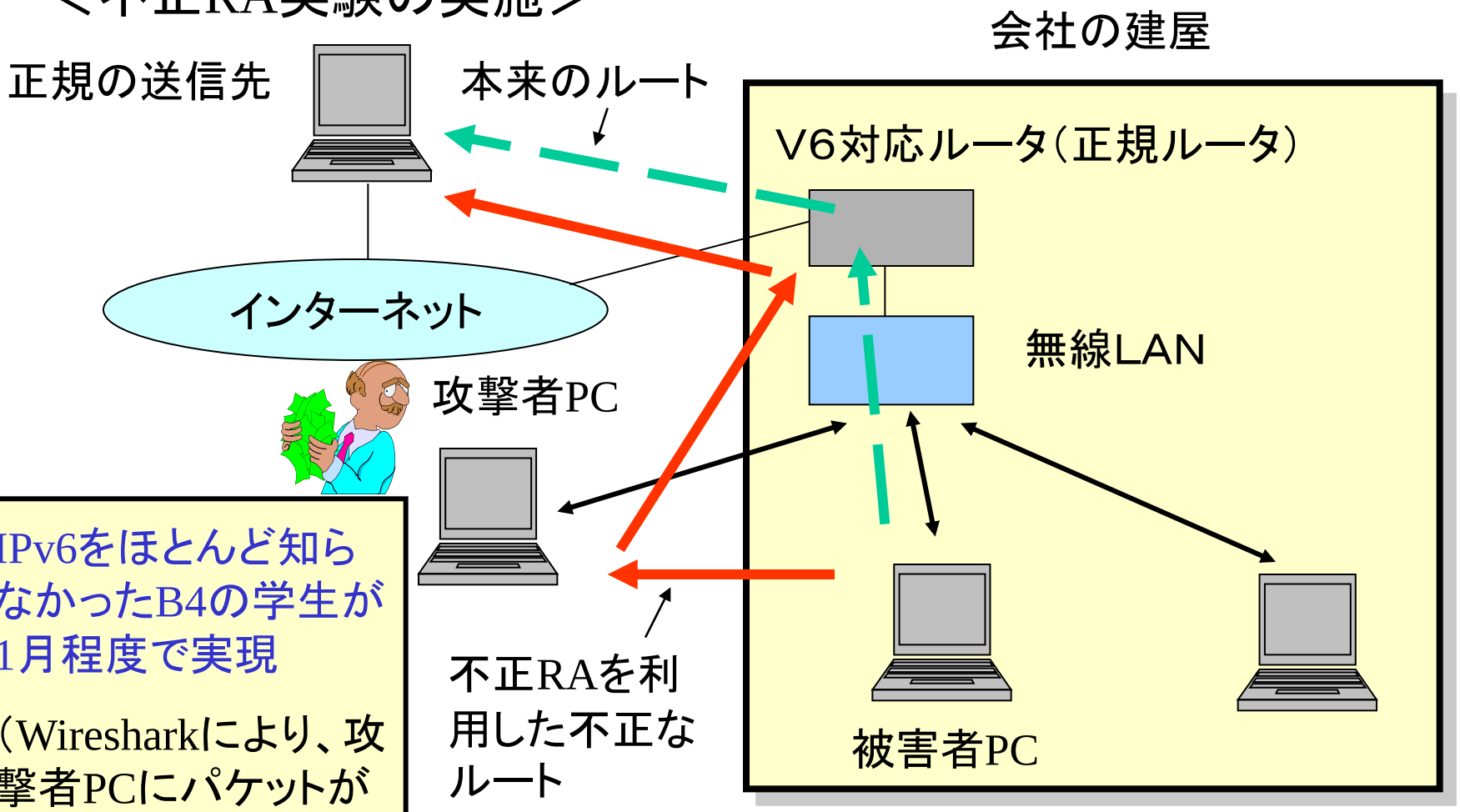


課題 「不正者が、無線LANにアクセスし、不正RAの機能を利用してMan in the Middle 攻撃などに簡単に成功してしまうのではないか」
WEPを使っていれば、無線LANへのアクセスは容易。不正RAは？

RA : Router Advertisement
WEP: Wired Equivalent Privacy

東京電機大学での実験(2)

＜不正RA実験の実施＞

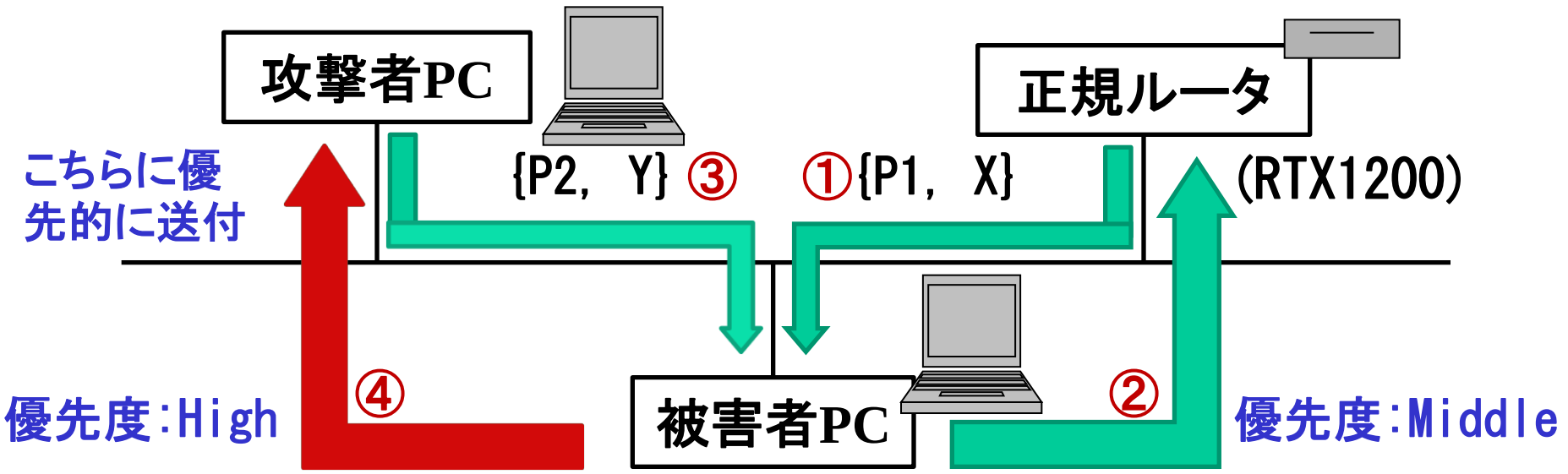


IPv6をほとんど知らなかったB4の学生が1月程度で実現

(Wiresharkにより、攻撃者PCにパケットが送られていることを確認)

RA : Router Advertisement

東京電機大学での実験(3)



P1によるアドレス生成
P2によるアドレス生成

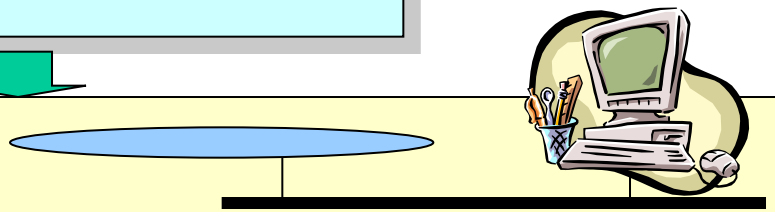
RA : Router Advertisement

＜V6では1つのPCで複数のアドレスを用いうる＞

IPv4の不正DHCP攻撃と同じ結果になるが、難しいタイミングアタックを使わなくても「優先度」を使うことにより比較的容易に実現可能であることが判明

IPv6におけるセキュリティ課題の整理

攻撃手段
DoS、侵入、不正アクセス、なりすまし、通信傍受



影響対象

ネットワーク、アプリケーション、ノード（サーバ／端末）

（1）仕様上の問題、実装上の問題

（2）IPv6単体での問題、IPv4,v6共存下における問題

（3）セキュリティ固有の問題、ディペンダビリティと関連する問題

下線がより重要になる問題

IPv4とv6の共存

- IPv4とv6の両方の機能を有する状態をデュアルスタックという
- デュアルスタックには、ネットワークのデュアルスタックとサーバやPCのデュアルスタックがある
- WINDOWS/VistaやWINDIWS/7はすでにv6対応機能も実装されている
- ネットワークのデュアルスタックは、V4/v6トランスレータを用いる方式と、v4ネットワークにv6をトンネリングさせる方式、v6ネットワークにv4をトンネリングさせる方式がありうる
- ネットワークのデュアルスタックは、2011年3月のNGNのIPv6サービスの開始により発生すると言われている

デュアルスタックの問題の分類

＜デュアルスタック下ではいろいろな問題が生じうる＞

（1）デュアルスタックにすることによりうまく機能しなくなる問題

（例）サーバ上のアプリがv4くくりつけのプログラムになっていて、v6で動かそうとしてもうまく動かない

（2）デュアルスタックで動くが、v4用のセキュリティ対策をうとうとするとv6で機能障害が起こる問題

（例）IPv4のセキュリティ用にICMPのフィルタリングをするとIPv6が動かなくなる

共存環境下でのクリティカルな問題

1. セキュリティ問題の本質はあまり変化しないだろう

2. しかし、運用の要請と作業量はIPv4,v6の2倍ではなく場合によってはIPv4->v6, IPv6->v4を含め4倍まで膨らむだろう

3. この状態でディペンダビリティが失われると障害きりわけに4倍の知識が必要となり、コミュニケーションロスなどにより再立ち上げに膨大な時間がかかる可能性がある

4. このディペンダビリティを失わせるセキュリティ攻撃が巧妙に行われるとサイバーテロともいうべき状態を発生させうるので国としても早めの対応が必要

IPv6セキュリティ問題を検討中の組織

- IPv4アドレス枯渇対応タスクフォース（総務省、IPv6普及・高度化推進委員会、インターネット協会、JNSA，WIDEなどが加盟）
- 日本セキュリティ事業者連絡協議会（ISOG-J ）
- IPv6技術検証協議会
- NTTなどのプロバイダー　ほか

＜ネットワーク系企業の対応は進んでいるが、コンピュータ系企業の検討が十分進み知識や技術が共有されているのだろうか。
また、各省庁や地方自治体は対応できるのか＞


END

興味を持つきっかけ

2010年1月27日に行われたNSF2009に出席し、「IPv6導入でセキュリティはどう変わるか」をみてIPv6セキュリティ対応の必要性を認識

1. 大元隆志著「IPv4アドレス枯渇対策とIPv6導入」 リックテレコム、2009
2. 佐藤友治「IPv6導入でセキュリティはどう変わるか」NSF2009（JNSA）
3. 北口善明「IPv6のセキュリティ」NSF2009（ JNSA ）
4. 許先明「security事業者とIPv6対応」NSF2009（ JNSA ）
5. 宮川晋「大規模NAT技術とIPv6」電子情報通信学会誌，Vol.93,No.2，pp145-150（2010年2月） 他

米国連邦政府の動き

米国　Federal Chief Information Officer　Kundraのメモ（９月２８日）http://www.cio.gov/Documents/IPv6MemoFINAL.pdf

＜目的＞
クラウド、スマートグリッド等による連邦政府ITシステムの近代化
NAT依存による複雑さの低減と透明性の確保
end-to-endにおけるユビキタスでセキュアなシステムの実現
将来のインターネットサービスの拡張性の確保

＜対応＞
・2012年度末までに連邦政府の外部サービス（web、メール、DNS、　ISP等）をnative IPv6対応にすること。
・2014年度末までにクライアントアプリ（外部サービスにつながるもの）　をnative IPv6対応にすること。
・2010年10月30日までに、各省はIPv6移行責任者を定め米国行政管理予算局に提出すること。