資料4－4

IPv6化に伴う セキュリティ環境変化と その影響について

力武　健次
情報通信研究機構 インシデント対策グループ

2008年1月31日

総務省「次世代の情報セキュリティ政策に関する研究会」発表原稿

発表内容概要

- IPv6化は移行ではなく追加である
- IPv6導入に伴う新しい脅威
- IPv6インターネットから見たNGN
- IPv4/IPv6の分断から統合へ
- 接続機器の多様化に伴うリスク
- IPsec義務化への対応

IPv6化は移行ではなく新規追加

- IPv4にIPv6が追加される
  - 違うプロトコルであり，移行はできない
  - 既存IPv4ネットワークは引き続き存在する
- IPv4/IPv6の両プロトコルへの対応が必要
  - 脆弱性も両プロトコルにまたがるようになる
  - IPv4の脆弱性はそのまま残る
  - IPv6では新たな脅威の可能性がある

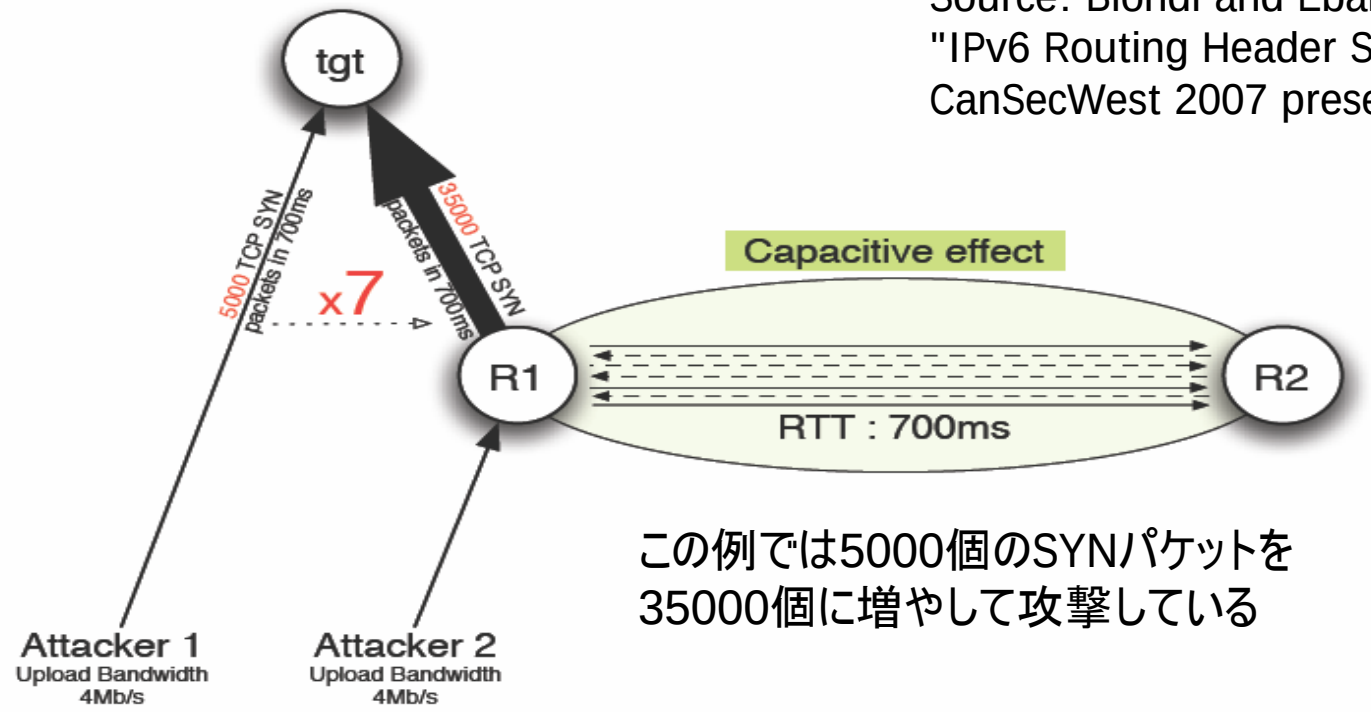
IPv6化に伴う新しい脅威（1）

- 一番の問題はプロトコルの検証不足
  - 例: Routing Header 0 (RH0)問題
    - 各パケットの通過経路を任意の段数指定できるため，DoS攻撃等に使うことができる
    - →仕様廃止へ（RFC5095，2007年12月）
  - 実はIPv4でも1997年にadvisoryがあった
    - A simple TCP spoofing attack
    - http://seclists.org/bugtraq/1997/Feb/0036.html

RH0の攻撃例

IPv6 prerequisite
All about Routing Header extension
Security implications
Solutions and workaround
Advanced Network Discovery
Bypassing filtering devices
DoS
Defeating Anycast

Capacitive effect
A flux capacitor



Source: Biondi and Ebalard,
"IPv6 Routing Header Security",
CanSecWest 2007 presentation

この例では5000個のSYNパケットを
35000個に増やして攻撃している

EADS

P. Biondi / A. Ebalard — IPv6 Routing Header Security. — 36/57

IPv6化に伴う新しい脅威（2）

- IPv4になかった新機能による問題
  - IPv6では任意個数のオプションヘッダが付く
    - 最大個数の規定は実装依存
      - 例: FreeBSD: 50個→15個に（RH0問題対応）
        - src/sys/netinet6/in6_proto.c 1.42で追加
  - 新規オプション例: Jumbo Payload option
    - 64Kバイト超パケットを利用可能（RFC2675）
    - Linux 2.6で脆弱性（CVE-2008-0352）

IPv6化に伴う新しい脅威（3）

- 自動設定によるplug-and-play化
  - RAには認証の仕組みがない
  - →端末認証でのアクセス管理が必要
    - DHCPv6, SENDなどの普及を促していく
- マルチキャストの多用による複雑化
  - 物理網を越えたグループの形成が可能
    - →VPN等と同様のアクセス管理が必要

IPv6化に伴う新しい脅威（4）

グローバルアドレスの一般化

どの機器もサーバになり得る環境の復活

→踏み台にされる危険の増大

プレフィクスと利用者の対応付けが容易になる

→個人情報とプライバシーの保護対策が必要

匿名に近いアドレスが使えるようになる

→アクセス制御が複雑になり不正につながる

IPv6化に伴う脅威への対応（1）

- プロトコルスタックの検証作業は個人ベース
  - RH0問題は数名の技術者のみで対応
  - その他研究課題としての成果はあるが…
    - Google Summer of Code 2006の一課題
      - BSDCan 2007 "Securing IPv6 on FreeBSD"
      - ND，マルチキャスト周辺のバグを多数発見
- 研究だけでなく実用化のための対応を!
  - コード検証を網羅的かつ詳細に行う必要あり

IPv6化に伴う脅威への対応（2）

IPv6普及・高度化推進協議会の文書

2005年IPv6移行ガイドライン セキュリティ編

仕様書ベースの脅威分析と対応を示している

今後特に注目を要するであろう点

1. 機器とアドレスの対応が「1対多数」になる
2. デュアルスタック機器が増加する
3. 組み込み機器が増加する

IPv6化に伴う脅威への対応（3）

- 機器とアドレスの対応が1対1でなくなる
  - 単一アドレスで機器は識別できなくなる
  - 「複数アドレスの集合」と機器との対応づけ
    - IDSやファイアウォールの設定原則の変更
    - 従来の侵入情報収集手法は効果が下がる
- 攻撃者の検出回避行動で性能が低下
  - 経路表の複雑度が大幅に増加する可能性

出典：小柏伸夫，衛藤将史，中尾康二，「IPv6環境における攻撃検出回避とその対策」，SCIS2008シンポジウム，論文2C1-3.

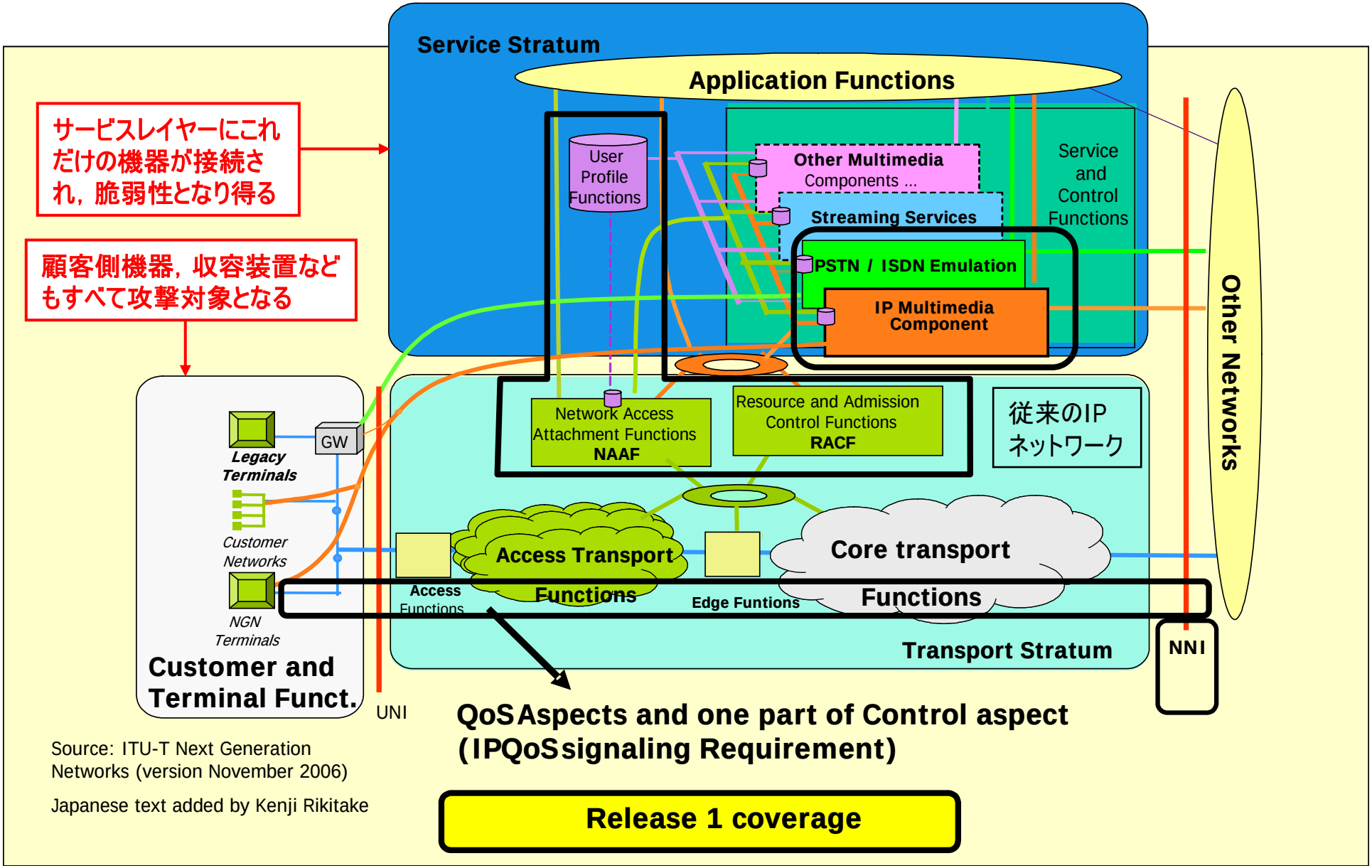
IPv6インターネットから見たNGN(1)

- NGNではIPv6はキャリア内が前提
  - NGN＝IPv6の閉域網＋IPv4のアクセス線
    - （NTT地域会社の申請用仕様書）
- 現実にはISPの基幹部は既に一部IPv6
  - 例: NTT西日本は地域IPv6網を提供
    - 問題: IPv6での外部到達性が提供できない
      - NTT法の制限，NGNの帯域保証との矛盾

IPv6インターネットから見たNGN(2)

- NGNからIPv6インターネットは使えるか?
  - (IPv4)PPPoEではアクセス線のみで不十分
  - 本質的解決: マルチプレフィクスによる制御
    - 複数プレフィクス割当で外部と内部を分離
    - IPv6ネイティブ接続で高速化
- 問題: インターネット同様の脆弱性が発生
  - サービスストラタムすべてが攻撃対象になる

NGN Release 1がもたらすもの



Source: ITU-T Next Generation Networks (version November 2006)

Japanese text added by Kenji Rikitake

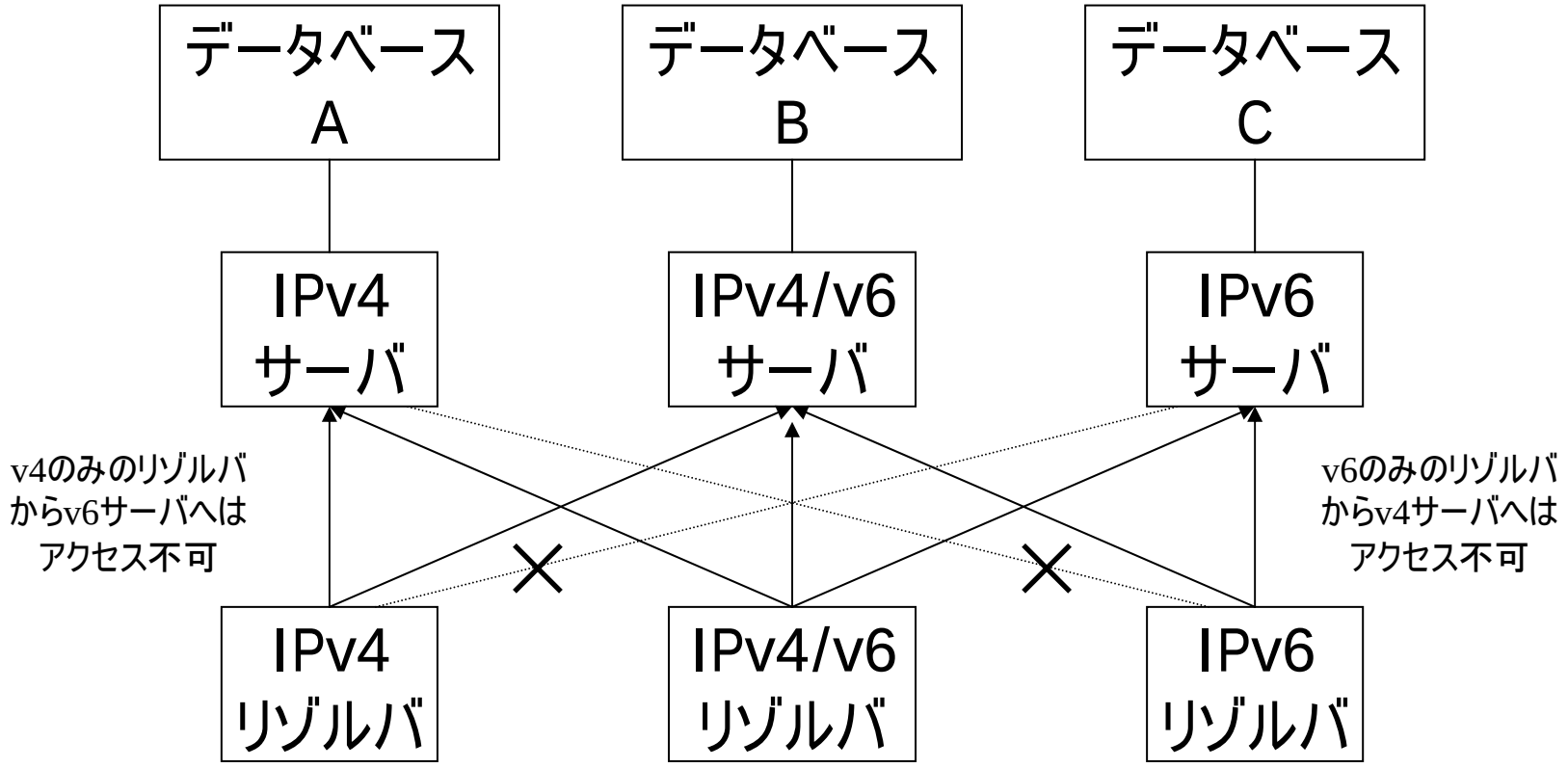
IPv4/IPv6の分断から統合へ（1）

- 初めは新規技術の導入で相互接続
  - プロトコル間中継が前提の技術開発が必要
    - 例: 大規模（毎秒数百万～数十億）同時接続数を可能にするIPv4-IPv6間プロキシ
      - 対象はWebやメールなどの基幹サービス
      - TLSなどアプリケーション暗号化の対応も必要
  - クライアントもv4/v6/両方の3種類を想定
    - どちらから見ても同じように使えることが必要

IPv4/IPv6の分断から統合へ（2）

必須基盤のDNSに関する問題点

IPv4単一からIPv4/IPv6併用環境に対応する技術が必要
以下のデータベースA/B/Cで同じ内容が見えなければならない
IPv4/IPv6片方しか見えないリゾルバでも不自由があってはならない



接続機器の多様化に伴うリスク(1)

脆弱性が多様化

携帯端末，情報家電，社会基盤(電気・水道・ガスなど)のインターネット化が始まっている

PCとの成り立ちの違いを考慮する必要がある

- ●組み込み機器はハード・ソフト共に利用できるシステム資源が限られており，PCとは全く異なる理由や傾向の脆弱性が見つかっている(＝攻撃は容易)
- ●開発手順がPCのように共通化されていないため，機器ごとに異なる対応を取らなければならない

接続機器の多様化に伴うリスク(2)

- ソフトウェア利用機器すべてに対応が必要
  - 安全な更新などの制御手段の提供
    - 迅速対応のためには自動的に行えることが必要
    - →更新用の安全なプロトコルの開発が必要
    - 更新手段は攻撃者にも利用される恐れがある
    - →最低限IPsec+PKIベースにする必要がある
  - 危険な機器をネットワークから排除できるか?
    - 切り離すための技術開発が必要
    - 同様に法的なリコール同様の手順を定める必要

IPsec義務化への対応

- 公開鍵による認証の一般化
  - Web以外での積極的な導入への対応
- 暗号化通信の一般化
  - 暗号化通信の解読傍受に関する技術的な検証と法的倫理的妥当性の検討が必要
  - 現状の鍵交換プロトコルも，利用者の一般化に伴う規模増大への対策が必要

IPv6化に向けた技術開発（1）

- NGNとIPv6インターネットの直接接続
  - 安全な閉域サービスと網間サービスを両立するためのアクセス管理技術
  - NGN運用機器の脆弱性管理技術
- IPv6基礎技術の安全性検証
  - プロトコルスタックの全コード試験と検証
  - IPv6固有機能の実証試験による検証

IPv6化に向けた技術開発（2）

- IPv6という新ネットワークの追加を前提とした，IPv4と併存する状況への対応
  - IPv4/IPv6アプリを統一的に扱う技術
  - IPv4/IPv6片方で両方が使える技術
- 多様な利用機器への脆弱性対応
  - 機器ソフトウェアの安全な更新技術
  - 危険な機器を切り離すための技術

IPv6化に向けた技術開発(3)

- IPsecによる認証や暗号化に対応できる技術的・社会的・法的基盤の整備
  - 暗号技術的なIPsecの強度の検証
  - IPsecで使うための社会的PKIの整備
  - 仮にIPsec通信を傍受する必要が生じた場合，その法的な線引きと必要な作業量の確定を可能にする技術的根拠の確立

ご清聴ありがとうございました