IPv6環境における脅威と対策

情報通信研究機構
ネットワークセキュリティ研究所
サイバーセキュリティ研究室
衛藤 将史

自己紹介

- 衛藤 将史
- 情報通信研究機構
  - ネットワークセキュリティ研究所
  - サイバーセキュリティ研究室 主任研究員

- インシデント分析センター nicter

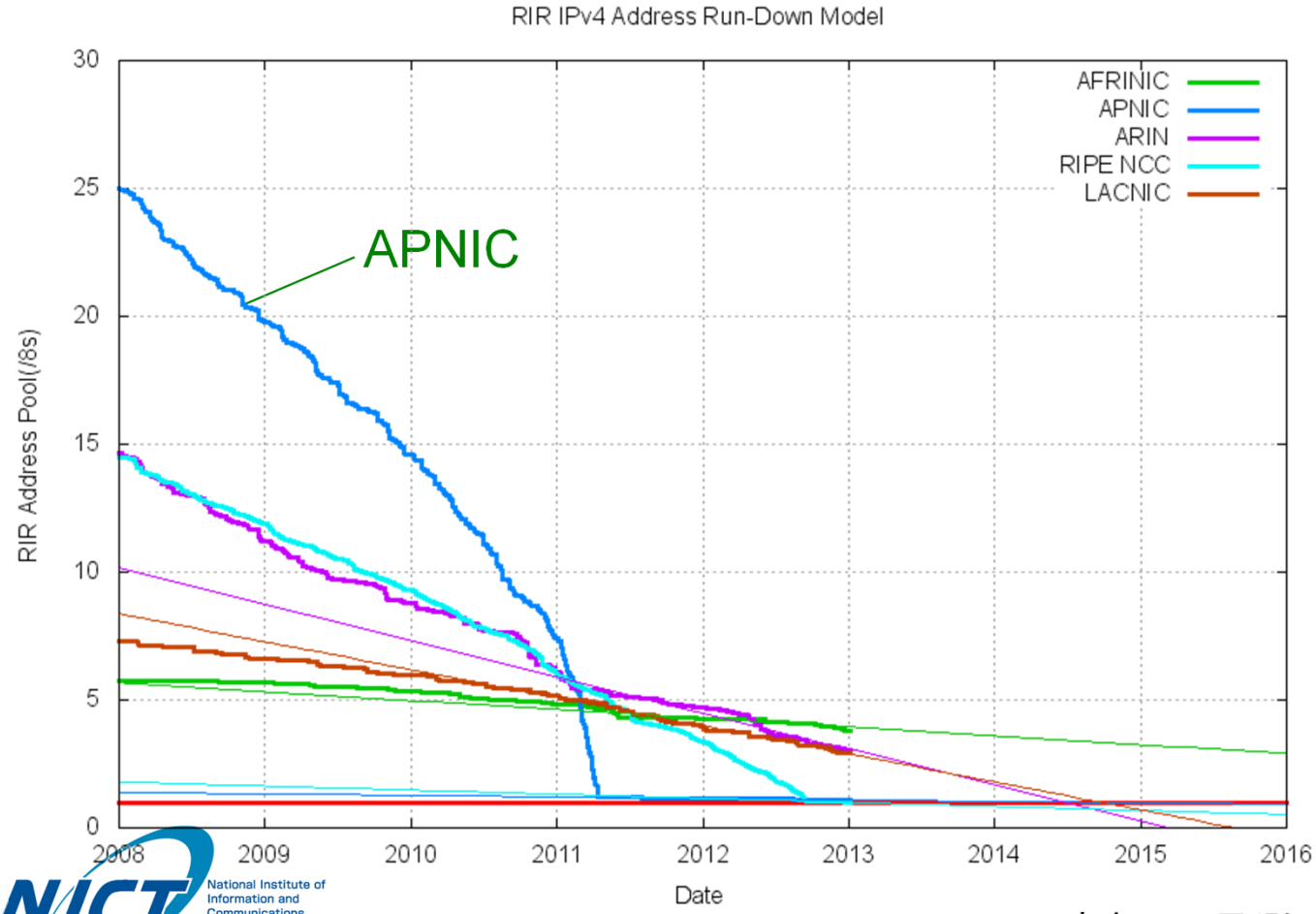
- IPv6 技術検証協議会
  - セキュリティ評価対策検証部会 部会長

背景：IPv6 への移行と課題

IPv4 アドレスの枯渇

- IPv4 アドレス枯渇問題
  - 2011 年～ 2014 年の間に IPv4 アドレスが枯渇
    - ICANN の中央在庫 → 2011/02/03 に枯渇
    - アジア太平洋地域 (APNIC*) の在庫 → 2011/04/15 に枯渇

*APNIC：Asia Pacific Network Information Centre



枯渇時期 (予測)

- APNIC : 2011/04/15
- RIPE/NCC : 2012/09/14
- ARIN : 2014/06/21
- LACNIC : 2014/07/18
- AfriNIC : 2020/11/21

http://www.potaroo.net/tools/ipv4/index.html (2013/1/8 時点での予測)

IP アドレス枯渇問題を放置すると…

- インターネットの普及・拡大が停止
  - × 新規サービス事業者の参入
  - × 個人ユーザのインターネットへの新規加入

- さまざまな IPv4 アドレスの延命措置
  - – NAT : 1 つのアドレスを複数の端末が共同で使用する技術
  - – アドレスの回収と再割り当て : 未使用のアドレスを回収して再利用

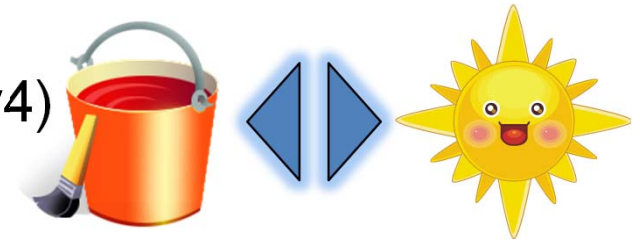
  → その他、数多くの努力が払われてきたが、枯渇は避けられない状況

- 新たな IP アドレス体系を導入する必要性

  → **IPv6 (Internet Protocol version 6)**

IPv6（Internet Protocol version 6）の特徴

- 広大なアドレス空間
  - 128 ビットのアドレス ←→ 32 ビットアドレス (IPv4)
  - IPv4 : IPv6 = バケツの体積 : 太陽の体積
  - 約340澗個（澗 = 10^{36}）



  → 340,282,366,920,938,463,463,374,607,431,768,211,456個
  澗 溝 穣 秭 垓 京 兆 億 万千百十一

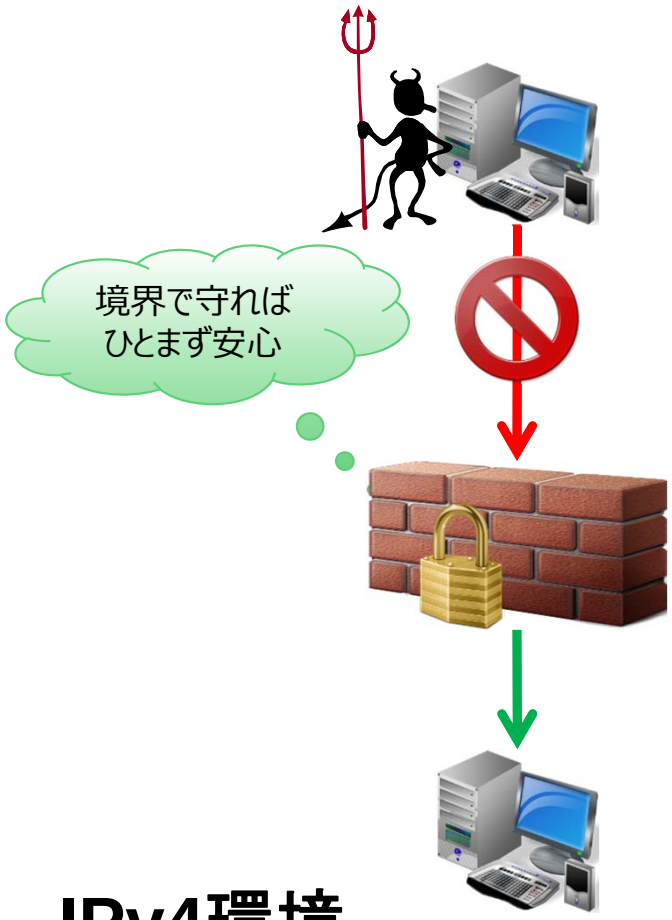
- End-to-End 原理への回帰
  - 豊富なアドレスにより、すべての端末が固有のアドレスを持つことが可能 (＝ どこからでも到達可能) に

- さまざまな新機能
  - アドレス自動設定機能（プラグアンドプレイ）
  - セキュリティ機能や同報通信（マルチキャスト）の標準サポート
  - 柔軟な拡張性による通信品質の向上

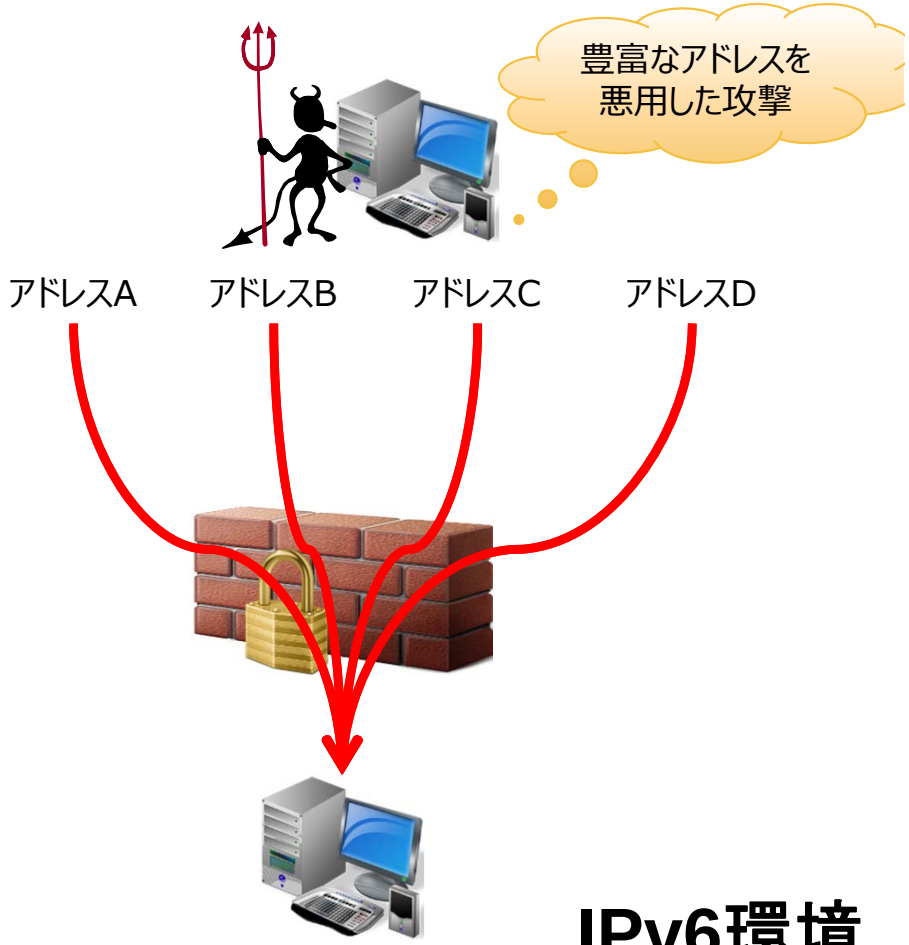
インターネットを取り巻く環境

- IPv6の世界は安全？
  - 定説:
    - End-to-End での暗号化・認証でセキュアに
  - 実際:
    - 自動設定機構に起因する経路詐称などが容易に
    - 膨大なアドレス数を処理できずネットワーク機器が機能不全に
    - 既存のセキュリティ戦略の再検討が必要

IPv6 環境におけるセキュリティ上の課題



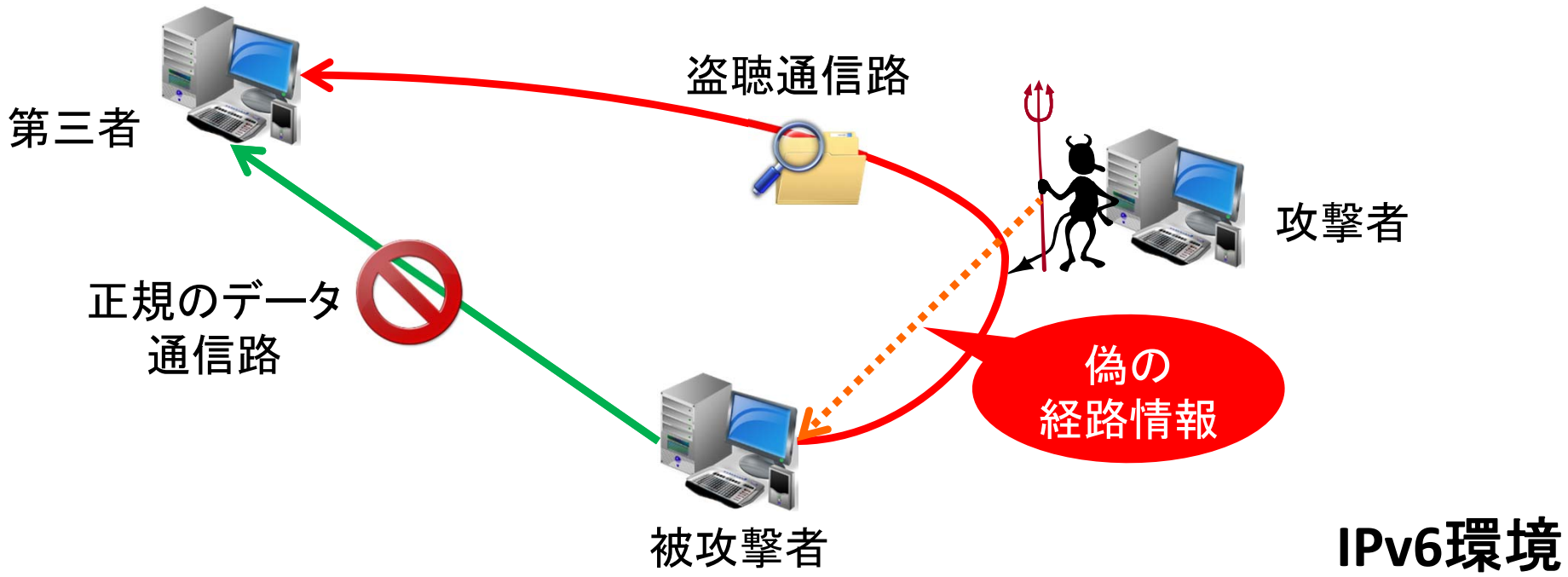
IPv4環境



IPv6環境

セキュリティ上の課題の一例 ～ 自動設定機能の弊害 ～

- IPv6 のプラグアンドプレイ機能 (自動設定機能) を悪用したデータの盗聴



脅威リスト (1)

- ✓ **詐称した近隣要請広告（NS/NA）メッセージを用いて通信を妨害（シナリオ 4）**
- ✓ **RH0（Route Type 0）を用いて通信を妨害（シナリオ 7）**
- ✓ **OSPFv3を用いて通信を妨害（シナリオ 12）**
- ✓ **近隣キャッシュ（Neighbor Cache）を溢れさせることによる通信の妨害（シナリオ 18）**
- ✓ **P2Pリンクを用いて通信を妨害（シナリオ 22）**
- ✓ **6to4を用いて通信を妨害（シナリオ 23）**
- ✓ **Multicast Listener Discovery（MLD）を用いて通信を妨害（シナリオ 27、28）**
- ✓ **大量のセッションを作成してNAT66（NAT64）の状態テーブルを枯渇させる（シナリオ30）**
- ✓ **MACアドレスの異なる大量のパケットを送信してスイッチのFDBを枯渇させる（シナリオ33）**
- – マルウェアに感染したTeredoサーバを用いて通信を妨害
- – 中間者攻撃によるバインディング管理鍵の入手及び移動ノードへのなりすまし
- – EUI64を用いてインターフェースIDを構成しているIPv6アドレスからのMACアドレス抽出
- – 不変のインターフェースIDを用いているIPv6アドレスを使用している端末に対し、複数NWへの接続を追跡
- – 暗号化されていないバインディングメッセージからのバインディング情報搾取
- – HIP Base Exchange の盗聴による両端ノードのIPアドレスとHost Identifyの取得
- – HIP UPDATE メッセージの盗聴による送信元IPアドレスとHIT（Host Identify Tag）の取得
- – RAを盗聴しによるMACアドレスの取得
- – リンク内のリンクローカルアドレス独占による他ホストのリンクローカルアドレス取得の阻害
- – MACアドレスのcompany_id特定による可変アドレス空間24ビットに対するスキャン行為

脅威リスト (2)

- ✓ 不正なジャンボペイロードを用いて通信を妨害 (シナリオ 1)
- ✓ 不正なフラグメントパケットを用いて通信を妨害 (シナリオ 2)
- ✓ Pad1オプションを用いて通信を妨害 (シナリオ 3)
- ✓ 詐称したルータ広告(RA)メッセージを用いて通信を妨害及び盗聴 (シナリオ 5、10、11)
- ✓ 詐称したICMPリダイレクトメッセージを用いて通信を妨害及び盗聴 (シナリオ 8、9)
- ✓ 不正なDADを用いてIPv6アドレスの取得を妨害 (シナリオ 13、14)
- ✓ マルチキャストアドレスを用いてネットワークに関する情報を収集 (シナリオ 16)
- ✓ 詐称したマルチキャストパケットを用いて通信を妨害 (シナリオ 17)
- ✓ DHCPv6を用いて通信を盗聴 (シナリオ 19)
- ✓ DHCPv6 Solicitメッセージを用いて通信を妨害 (シナリオ 20、21)
- ✓ 脆弱性攻撃ツールを用いてIPv6ホストを攻撃 (シナリオ 25)
- ✓ MTU機能を悪用して通信を妨害 (シナリオ 26)
- ✓ 不正なルータ広告(RA)メッセージを用いて通信を妨害および盗聴する(シナリオ31・35・37・38)
- ✓ マルチキャストDNSを使用して虚偽の情報を送信する(シナリオ34)
- ✓ Anycast DNSを使用して虚偽の情報を送信する(シナリオ36)
- ✓ 虚偽のDHCPv6サーバで広告した虚偽のDNSサーバから大量のAAAAレコードを送信してアプリケーショントラフィックを妨害する(シナリオ39)
- ✓ ファジングにより、対象機器のIPv6スタックの脆弱性を検出する(シナリオ40)
- – RSVPによる不正な帯域予約によりサービスを妨害
- – 多重カプセル化により負荷を増大させサービスを妨害
- – 偽造RAの送信によるデフォルトルータなりすまし及びサービス妨害
- – 悪意を持ったルータからの無意味なRIPng経路広告によるリンク内の帯域負荷
- – 特定のリンクローカルやエリアを指定し、意図的に無意味なOSPFv3 LSAを大量にフラッドすることによるDoS攻撃

脅威リスト (3)

- ✓ **オーバーラップしたフラグメントパケットを用いてファイアウォールを無効化 (シナリオ 6)**
- ✓ **マルチリンク化によるIDS回避 (シナリオ 15)**
- ✓ **経路の非対称性を利用してIDSを回避 (シナリオ 24)**
- ✓ **IPv6 通信によるリモートエクスプロイト攻撃 (シナリオ 29)**
- ✓ **大量のセッションを作成してファイアウォールのテーブルを枯渇させる(シナリオ32)**
- – バックドアを待ち受けるグローバルアドレスの変更によるセキュリティデバイスの回避
- – 感染システムのIPsec暗号化利用によるセキュリティデバイスの回避

さまざまな課題が存在
- 誰が対策を行えばよいか
- どのような対策が有効か
- 優先的に対策すべき課題は？

脅威の体系化

- 分類軸1: IPv6 固有かIPv6 / IPv4 共通の課題か
  - IPv6/IPv4 共通の問題 → 既存ネットワーク(IPv4)の対応策を参考に
  - IPv6 固有の問題 → 新たな対策が必要

- 分類軸2:対策方法による分類
  - プロトコルの改善による対策 → SDO(標準化団体) へ
  - 運用による対策 → NOG (Network Operators Group)、SIer へ
  - 実装の改善による対策 → 各ベンダへ

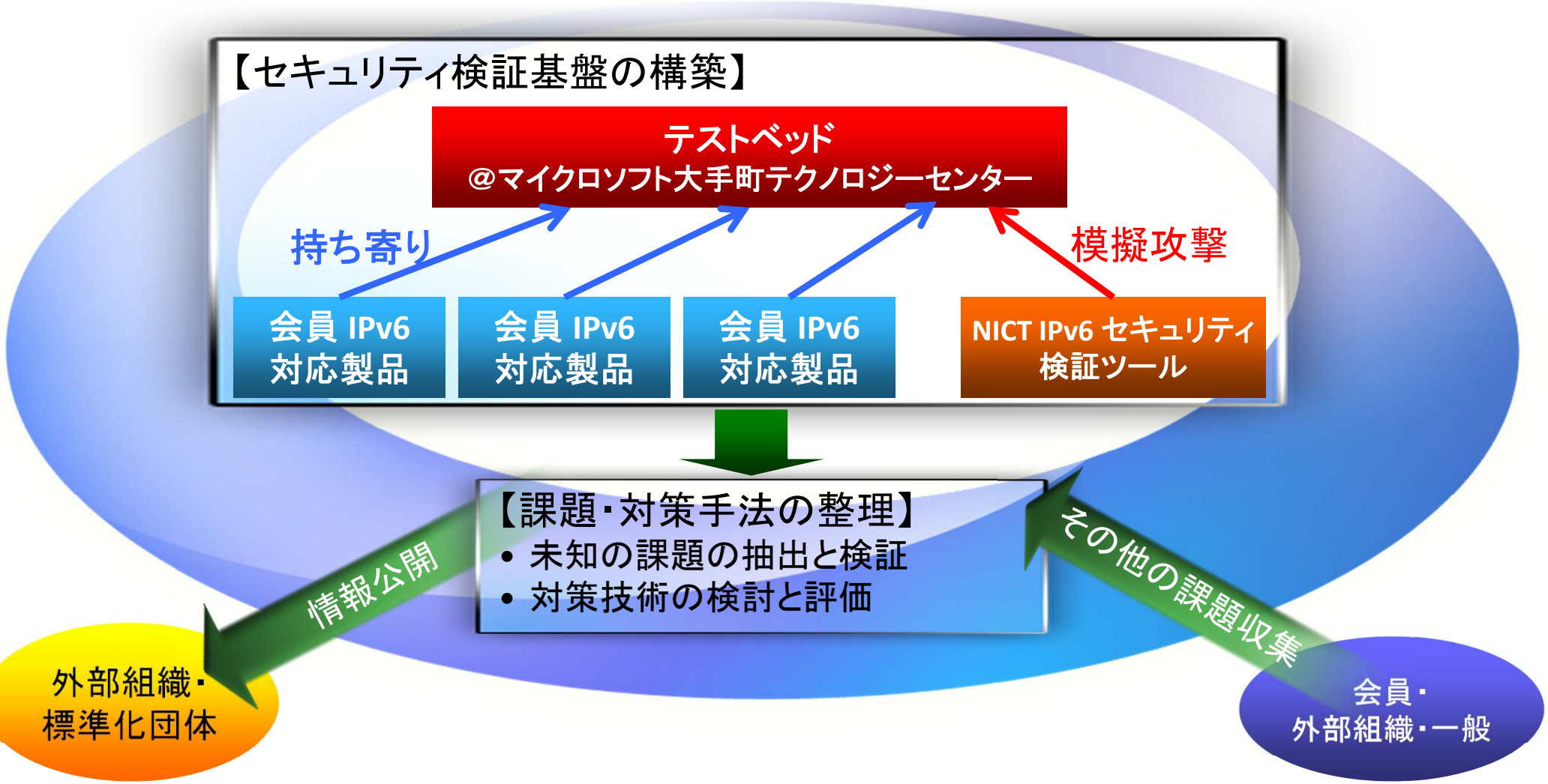
- 分類軸3:攻撃対象による分類
  - エンドノードに対する問題
  - ネットワーク機器に対する問題
  - セキュリティデバイスに対する問題

- 分類軸4:解決策の有無による分類

IPv6 技術検証協議会の設立

IPv6 技術検証協議会の設立

IPv6 技術検証協議会 (2010 年 7 月)



会員企業(12企業・組織)

NTT

SoftBank

Designing The Future KDDI

NICT 独立行政法人 情報通信研究機構

paloalto NETWORKS

デジタルライフ、もっと快適に BUFFALO

BROCADE

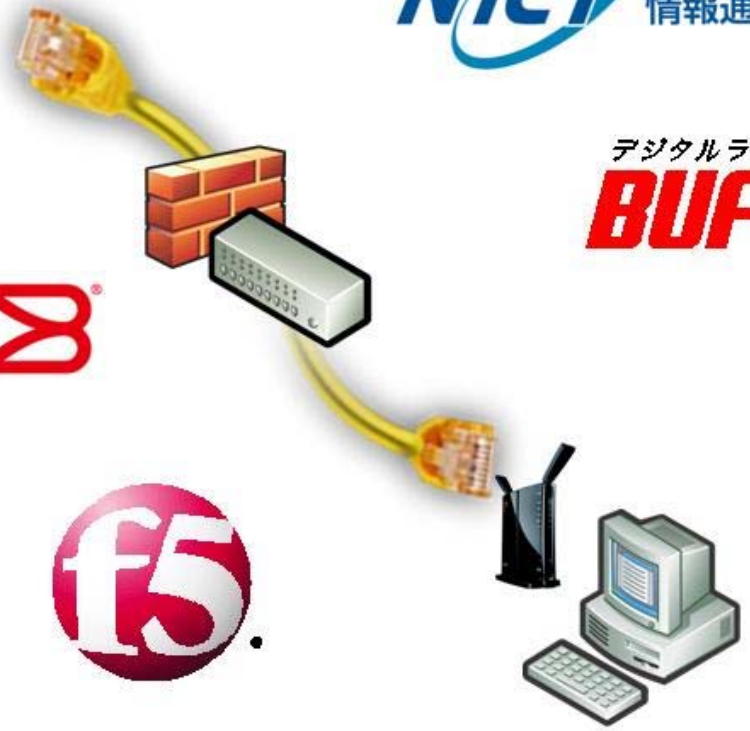
Microsoft

THALES

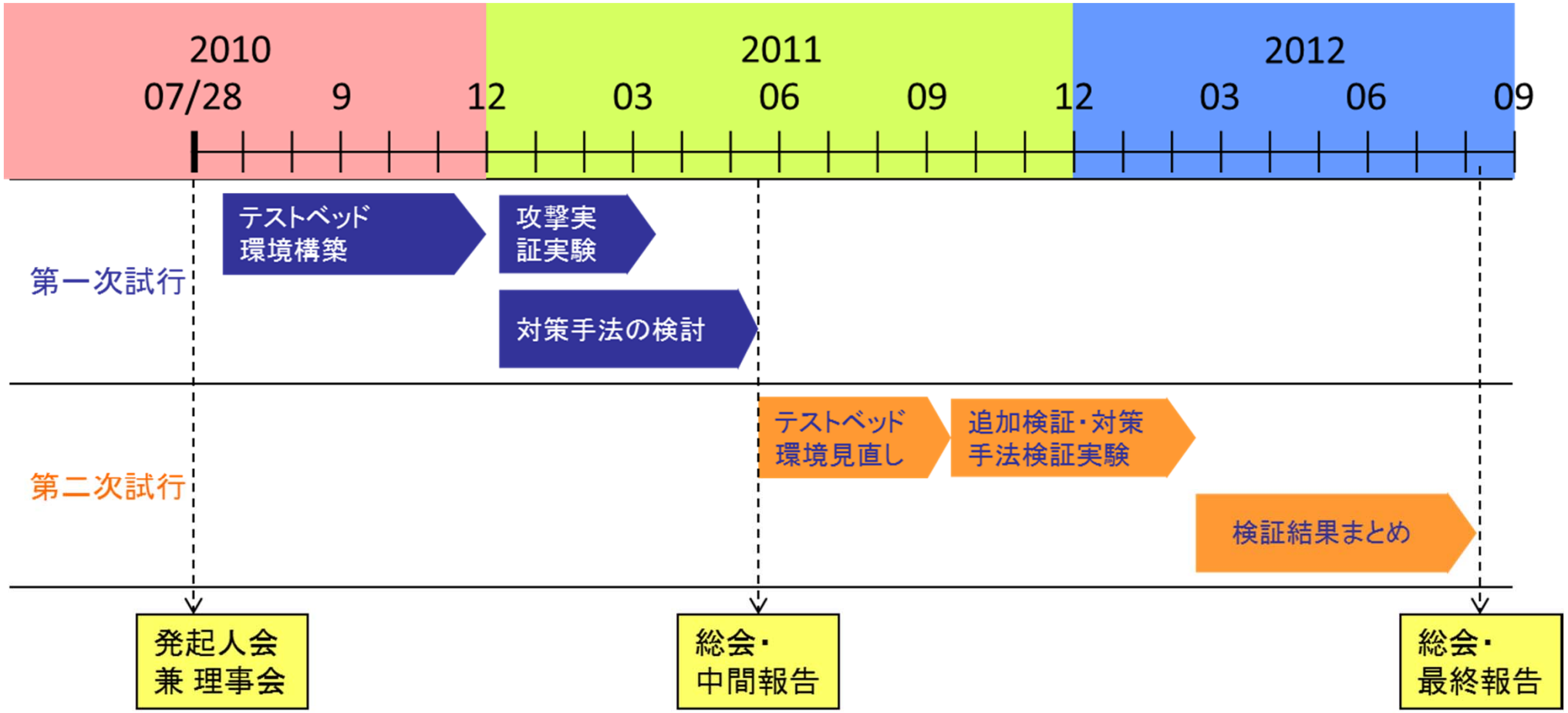
f5

東陽テクニカ

BlueCoat



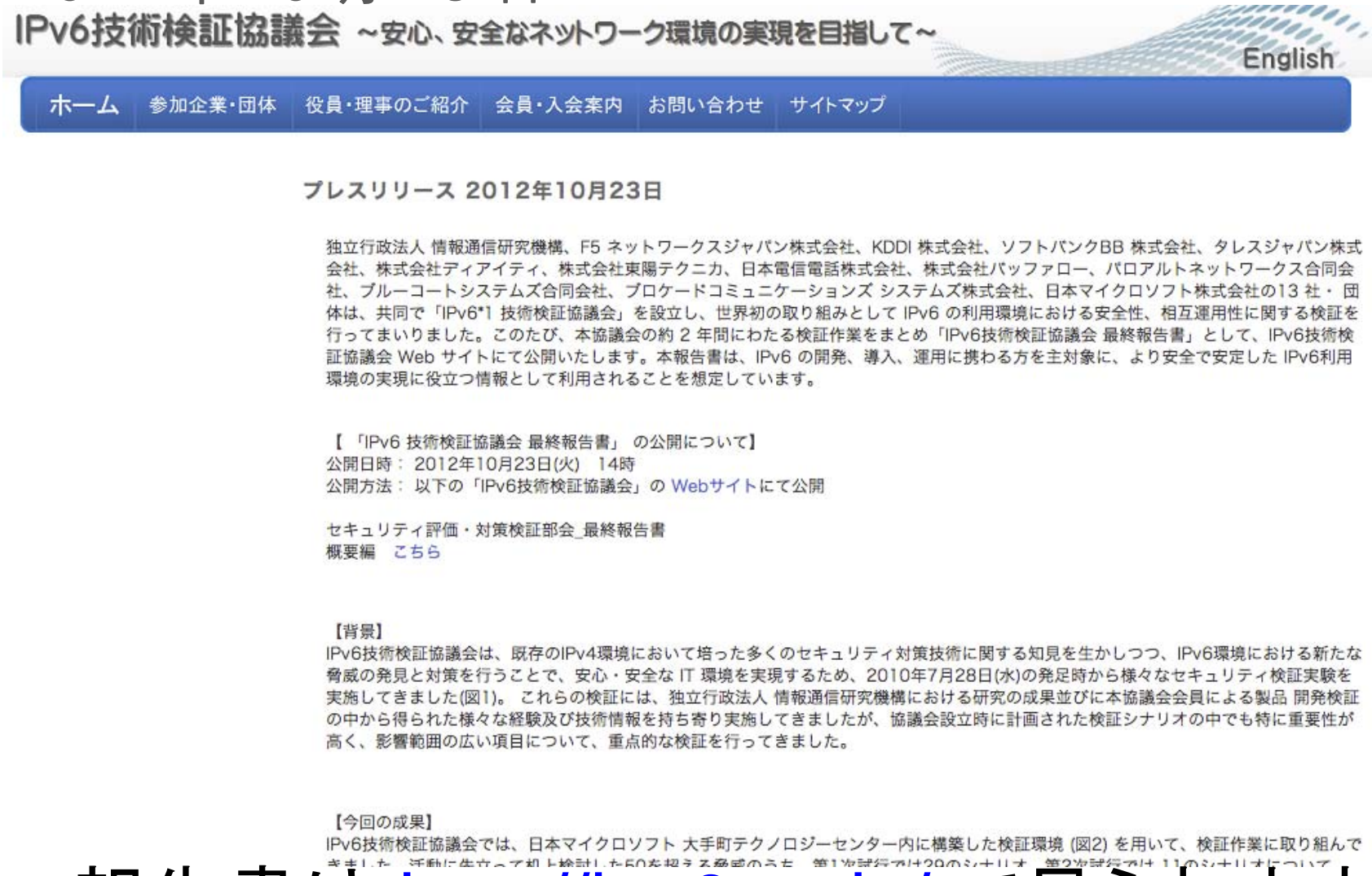
ロードマップ



第一次試行：テストベッド環境構築と攻撃の実証実験
および対策手法の検討
第二次試行：テストベッド環境の見直しと対策手法の導入
および検証実験 → まとめ

IPv6 技術検証協議会 最終報告書

2012 年 10 月 23 日



IPv6技術検証協議会 ～安心、安全なネットワーク環境の実現を目指して～

English

ホーム | 参加企業・団体 | 役員・理事のご紹介 | 会員・入会案内 | お問い合わせ | サイトマップ

プレスリリース 2012年10月23日

独立行政法人 情報通信研究機構、F5 ネットワークスジャパン株式会社、KDDI 株式会社、ソフトバンクBB 株式会社、タレスジャパン株式会社、株式会社ディアイティ、株式会社東陽テクニカ、日本電信電話株式会社、株式会社バッファロー、パロアルトネットワークス合同会社、ブルーコートシステムズ合同会社、ブロケードコミュニケーションズ システムズ株式会社、日本マイクロソフト株式会社の13 社・ 団体は、共同で「IPv6*1 技術検証協議会」を設立し、世界初の取り組みとして IPv6 の利用環境における安全性、相互運用性に関する検証を行ってまいりました。このたび、本協議会の約 2 年間にわたる検証作業をまとめ「IPv6技術検証協議会 最終報告書」として、IPv6技術検証協議会 Web サイトにて公開いたします。本報告書は、IPv6 の開発、導入、運用に携わる方を主対象に、より安全で安定した IPv6利用環境の実現に役立つ情報として利用されることを想定しています。

【 「IPv6 技術検証協議会 最終報告書」 の公開について】
公開日時： 2012年10月23日(火) 14時
公開方法： 以下の「IPv6技術検証協議会」の Webサイトにて公開

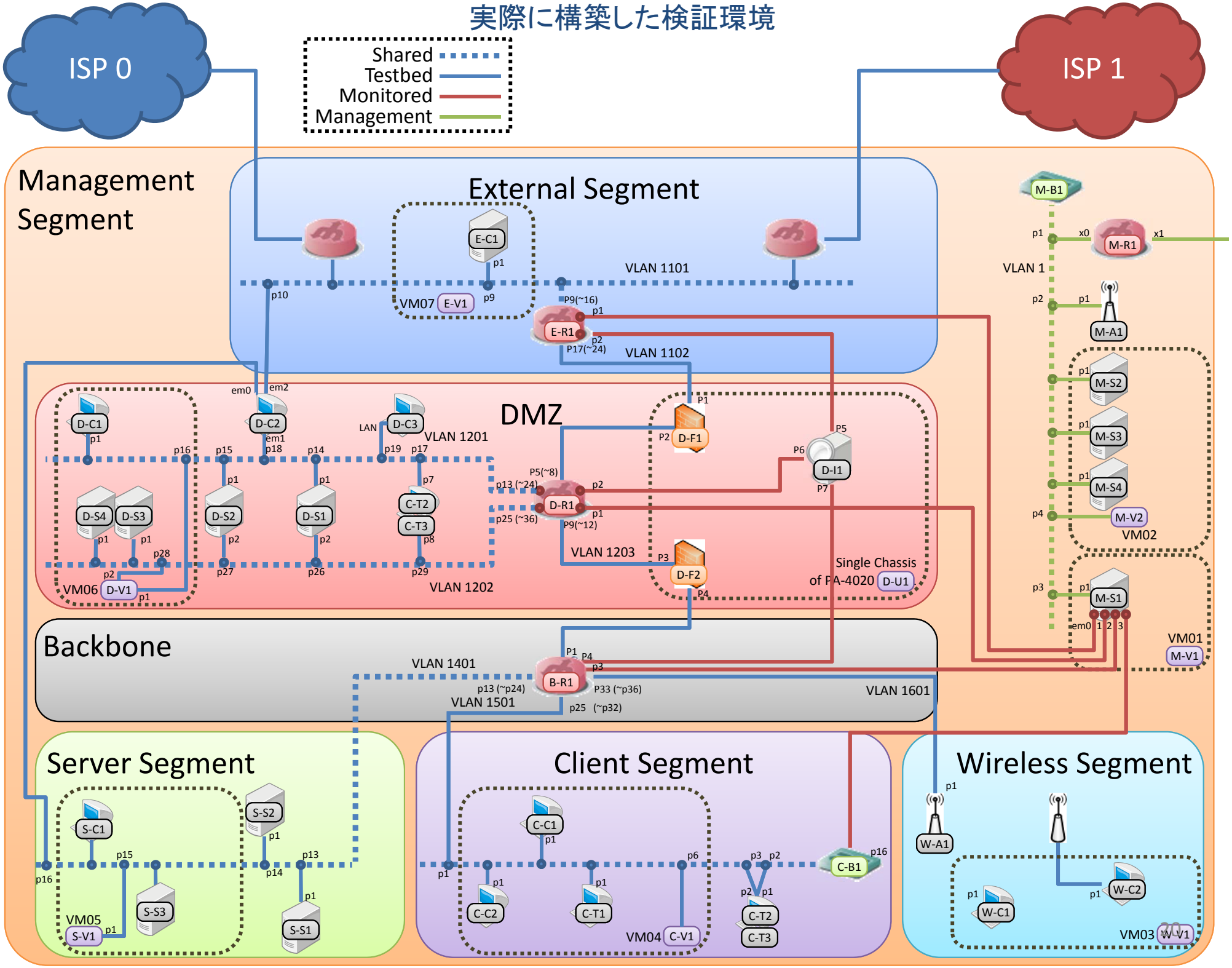
セキュリティ評価・対策検証部会_最終報告書
概要編 こちら

【背景】
IPv6技術検証協議会は、既存のIPv4環境において培った多くのセキュリティ対策技術に関する知見を生かしつつ、IPv6環境における新たな脅威の発見と対策を行うことで、安心・安全な IT 環境を実現するため、2010年7月28日(水)の発足時から様々なセキュリティ検証実験を実施してきました(図1)。 これらの検証には、独立行政法人 情報通信研究機構における研究の成果並びに本協議会会員による製品 開発検証の中から得られた様々な経験及び技術情報を持ち寄り実施してきましたが、協議会設立時に計画された検証シナリオの中でも特に重要性が高く、影響範囲の広い項目について、重点的な検証を行ってきました。

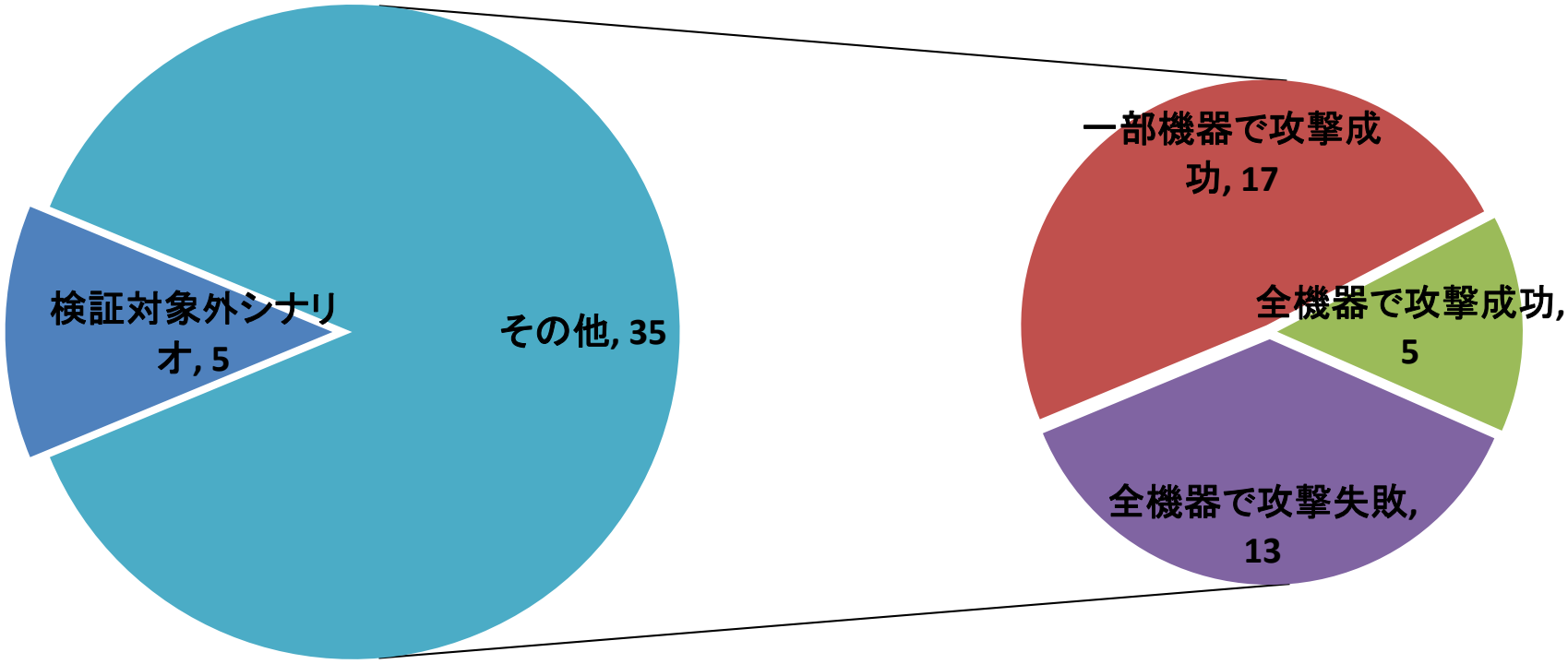
【今回の成果】
IPv6技術検証協議会では、日本マイクロソフト 大手町テクノロジーセンター内に構築した検証環境 (図2) を用いて、検証作業に取り組んで

報告書は http://ipv6tvc.jp/ で見られます

IPv6技術検証協議会の活動


実際に構築した検証環境
ISP 0
ISP 1
Shared
Testbed
Monitored
Management
Management Segment
External Segment
E-C1
VM07 E-V1
VLAN 1101
E-R1
VLAN 1102
DMZ
D-C1
D-C2
D-C3
LAN
VLAN 1201
D-S4
D-S3
D-S2
D-S1
C-T2
C-T3
VM06 D-V1
VLAN 1202
D-F1
D-I1
D-R1
VLAN 1203
D-F2
Single Chassis of PA-4020 D-U1
Backbone
VLAN 1401
B-R1
VLAN 1501
VLAN 1601
Server Segment
S-C1
S-S2
S-S3
S-S1
VM05 S-V1
Client Segment
C-C1
C-C2
C-T1
VM04 C-V1
C-B1
C-T2
C-T3
Wireless Segment
W-A1
W-C1
W-C2
VM03 W-V1
M-B1
M-R1
VLAN 1
M-A1
M-S2
M-S3
M-S4
M-V2
VM02
M-S1
VM01 M-V1

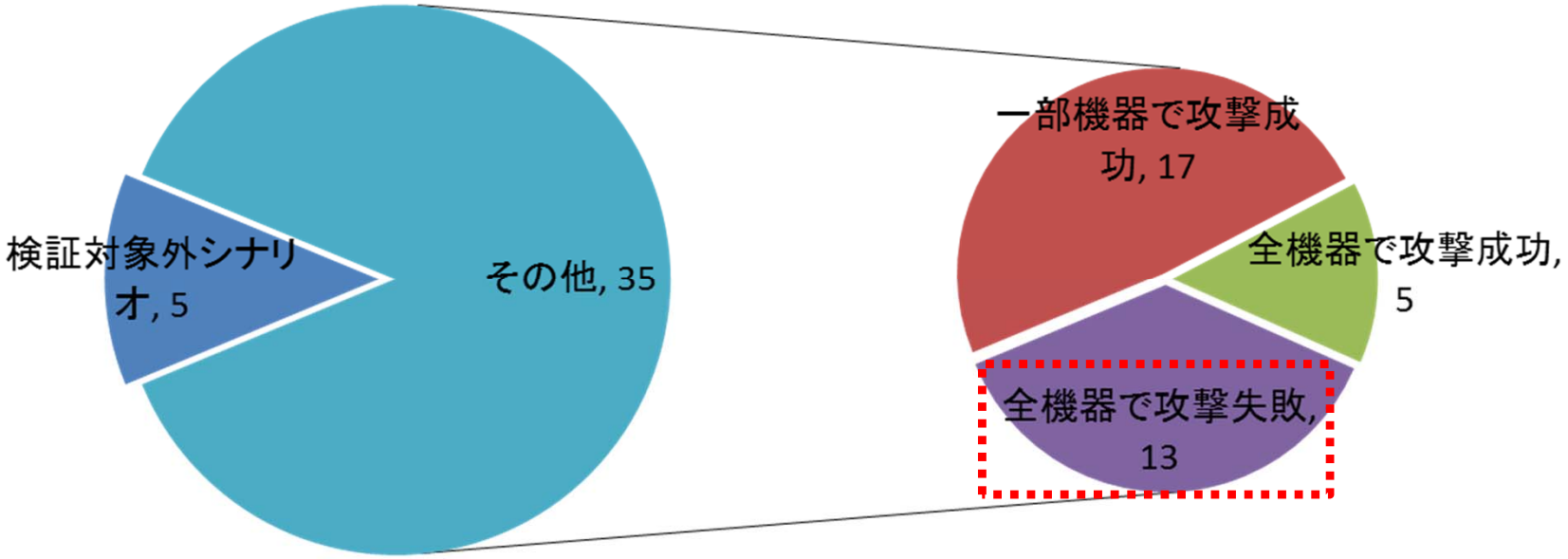
検証結果の概要



全 40 シナリオ
(うち 35 シナリオが実施対象に)

実施 35 シナリオの
検証結果の内訳

対象機器の全てで攻撃が失敗したシナリオ (1)

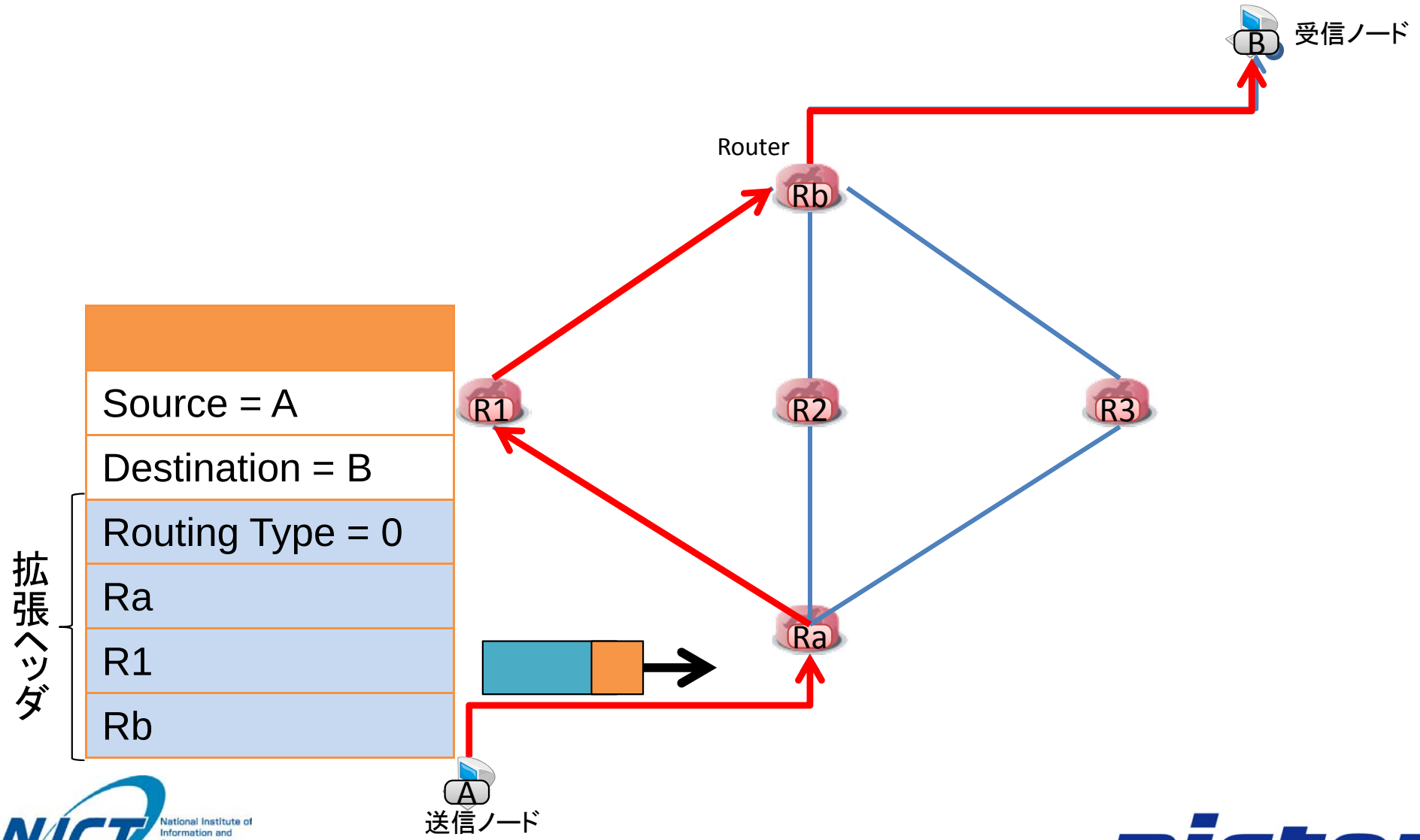


- 全ての機器で攻撃が失敗したシナリオ（13件）
  - 特殊な経路情報（RH0：Router Type 0）を使用したパケットを大量に送信してトラフィックを妨害する
  - 不正なジャンボペイロードオプションを指定したパケットを大量に送付し通信を妨害する
  - オーバーラップしたフラグメントパケットを送付することでファイアウォールを無効化する
  - 詐称したICMPv6リダイレクトを送信してユーザトラフィックを攻撃ノードに誘導する
  - 詐称したICMPv6リダイレクトを送信してユーザトラフィックを妨害する
  - マルチキャストルーティングデーモンに対してDoSを行う
- 原因：RFC*によって既に無効とされている、または実装や運用によって回避可能なシナリオであったため

*RFC（Request For Comments）：インターネットの通信規約等の仕様文書

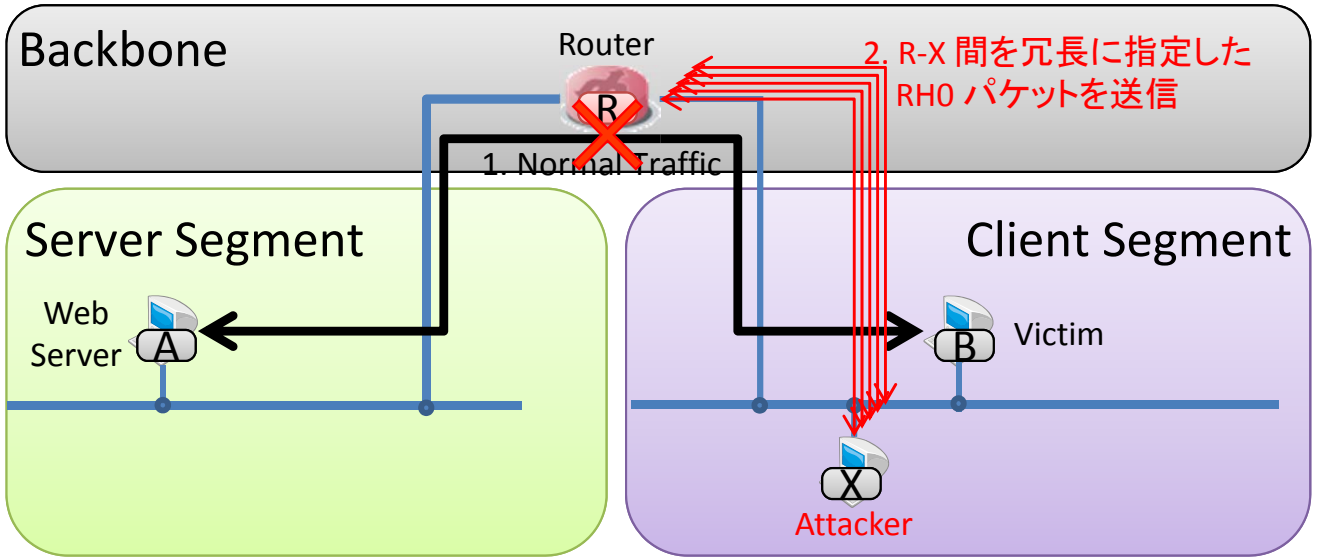
Routing Header Type 0

- IPv4 におけるソースルーティング。送信者が宛先までの経路を送信パケットの拡張ヘッダに記述することで、パケットが転送される経路を明示的に指定することができる。



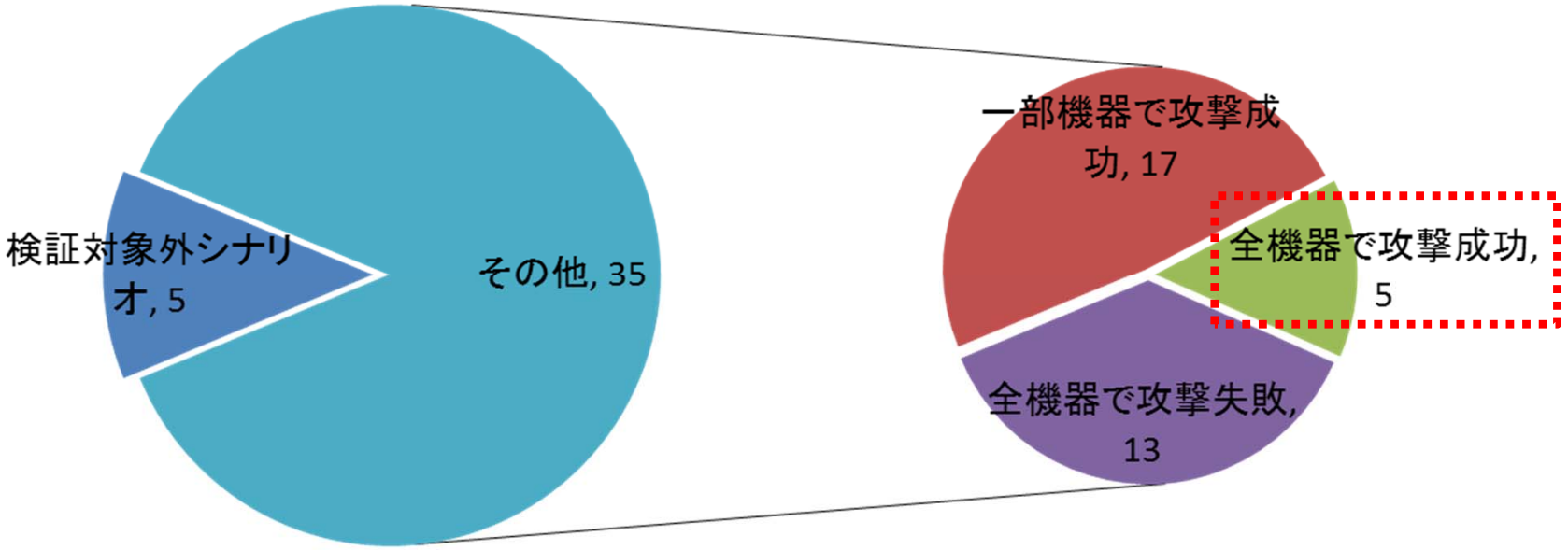
対象機器の全てで攻撃が失敗したシナリオ (2)

- 特殊な経路情報(RH0:Routing Header Type 0)を使用したパケットを大量に送信してトラフィックを妨害する



- 攻撃概要
  - 攻撃ノードXから境界ルータに、RH0ヘッダを使用したパケットを大量に送信する
- 想定される攻撃の効果
  - RH0ヘッダを使用したパケットが、攻撃ノードXと境界ルータの間を往復し続けることで通信の帯域を占領し、正常な通信を妨害する
- 考察
  - RH0 は RFC5095 において無効化するよう標準化されているが、今回の検証では評価対象となったすべてのシステムがこの RFC に準拠していることが確認された

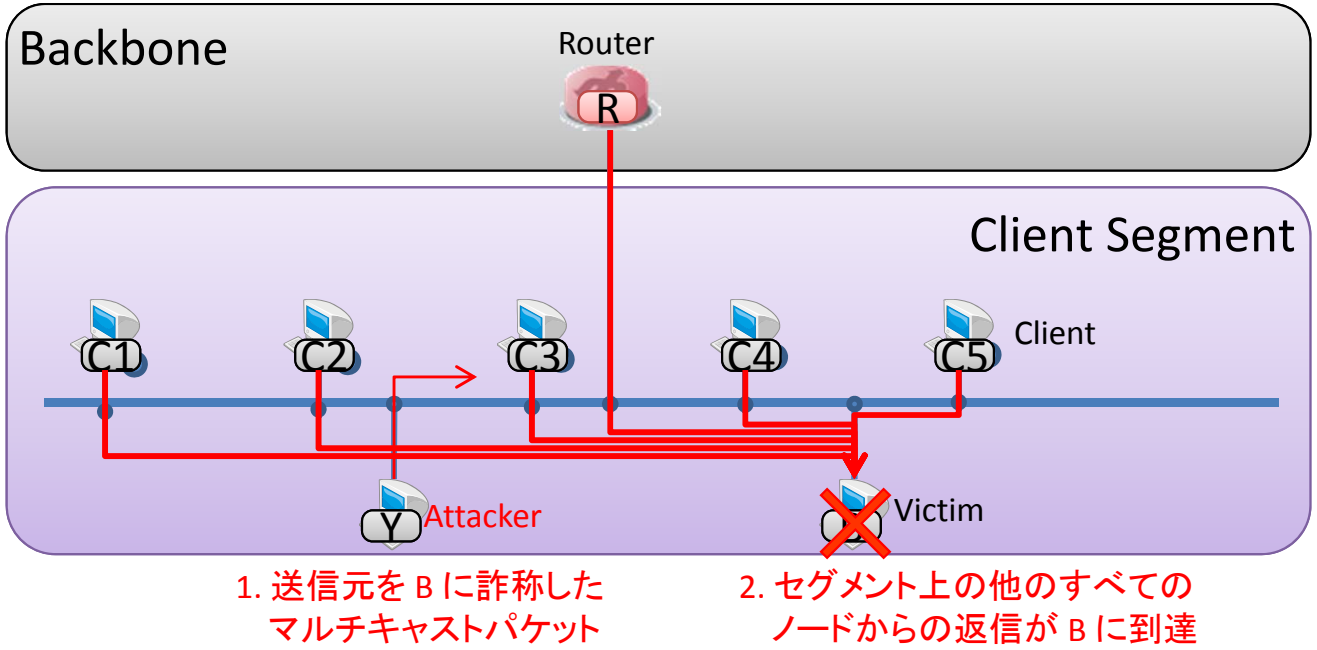
対象機器の全てで攻撃が成功したシナリオ (1)



- 2 種類以上のシステムを対象に実施されたシナリオのうち、すべてのシステムにおいて攻撃が成立したシナリオ（5 件）
  - 送信元を詐称したマルチキャストパケットを送信し、パケットの増幅攻撃を行う
  - 詐称した経路情報を送信してユーザトラフィックを攻撃ノードに誘導する
  - アドレスを詐称した隣接情報をルータに送付してトラフィックを妨害する
  - 詐称した経路情報を送信してユーザトラフィックを妨害する
  - DHCPv6 サーバから虚偽の情報を送付することによる中間者攻撃
- 原因：RFC に準拠して正しく実装されていれば必ず攻撃が成立

対象機器の全てで攻撃が成功したシナリオ (2)

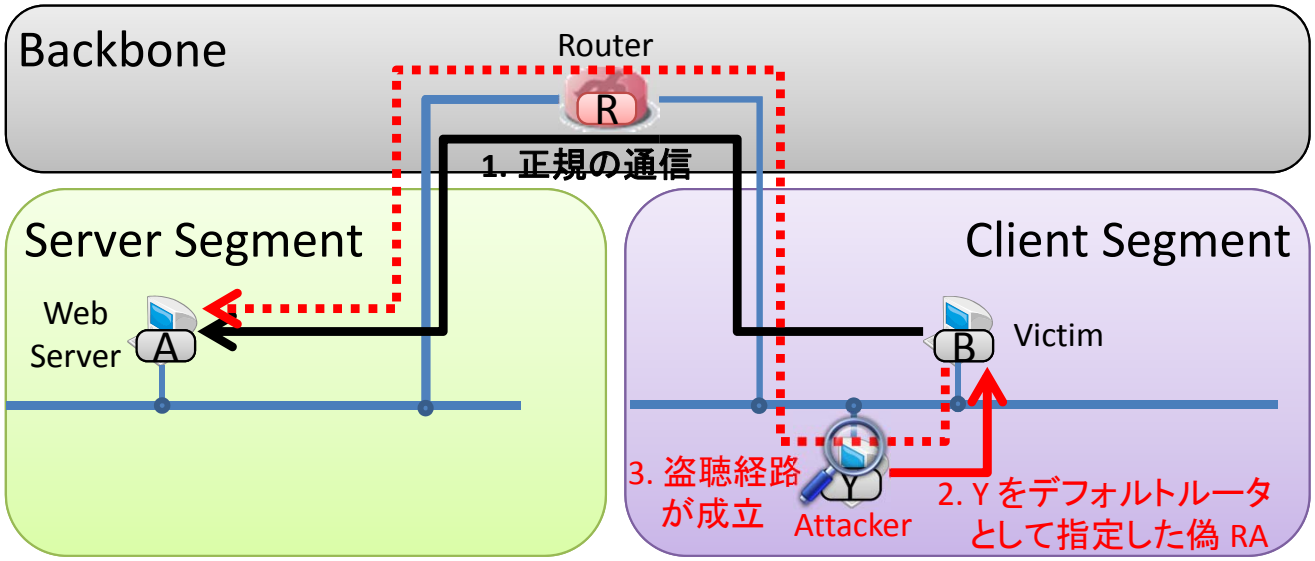
- 送信元を詐称した同報通信用のパケット（マルチキャストパケット）を送信し、パケットの増幅攻撃を行う



- 攻撃概要
  - 攻撃ノードYから送信元アドレスをユーザーノードBに詐称した、不正なヘッダを持つマルチキャストパケット (ff02::1 宛) を送信する。
- 想定される攻撃の効果
  - マルチキャストパケットに対する大量のICMP エラーメッセージ(ICMP Parameter Problem) がユーザーノードBに送信される
- 考察
  - ローカルの全てのノード宛(ff02::1) のマルチキャストパケットの処理についてはRFCにおいて規定されている。それぞれの機器は RFC に準拠した機能を実装しているが、結果的にこれが攻撃の成立に繋がっている。

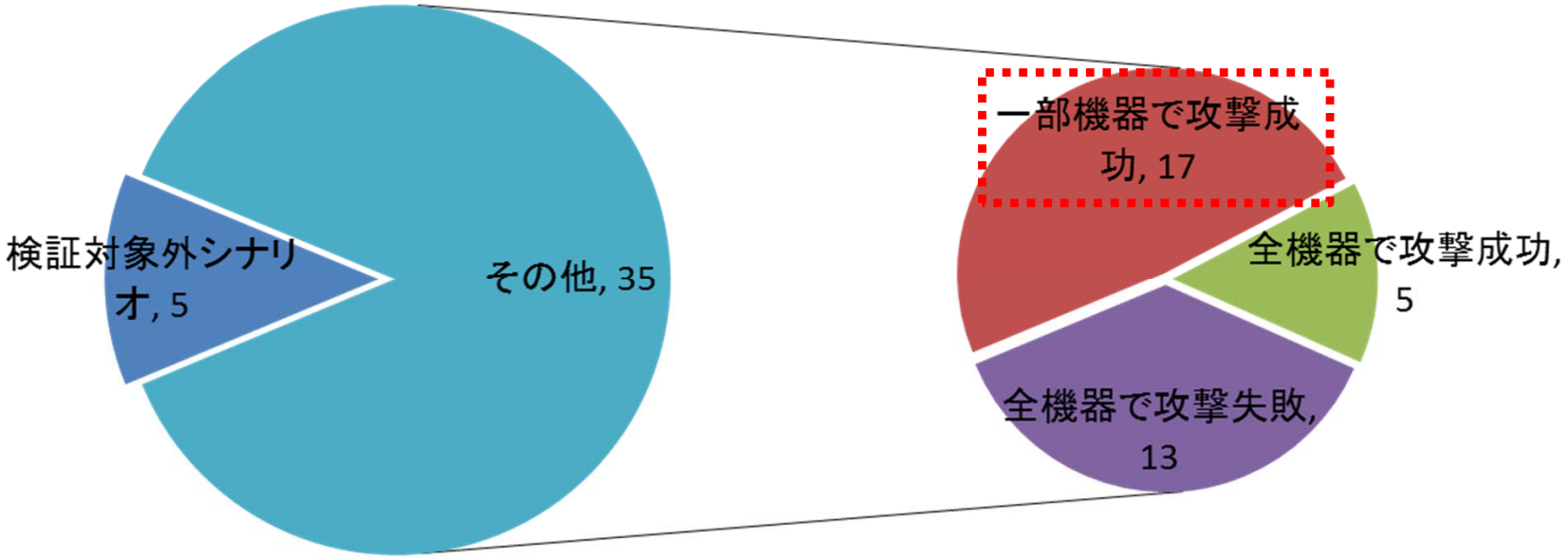
対象機器の全てで攻撃が成功したシナリオ (3)

- 詐称した経路情報 (RA:Router Advertisment) を送信してユーザトラフィックを攻撃ノードに誘導する



- 攻撃概要
  - 攻撃ノードYが、デフォルトルータとして攻撃ノードYを指定したRAをユーザーノードBに送付する
- 想定される攻撃の効果
  - ユーザーノードB（例：エンドユーザーのPC）からユーザーノードA（例えば、Webサーバ）へのパケットが攻撃ノードYを経由するため、攻撃者がパケットを盗聴・改ざん可能になる
- 考察
  - 本攻撃が行われてもユーザーノードAとBが通信可能であり、攻撃を検知し難い。また、暗号化されていない通信が盗聴されるリスクは、IPv4にも存在する。

一部の機器で攻撃が成功したシナリオ (1)

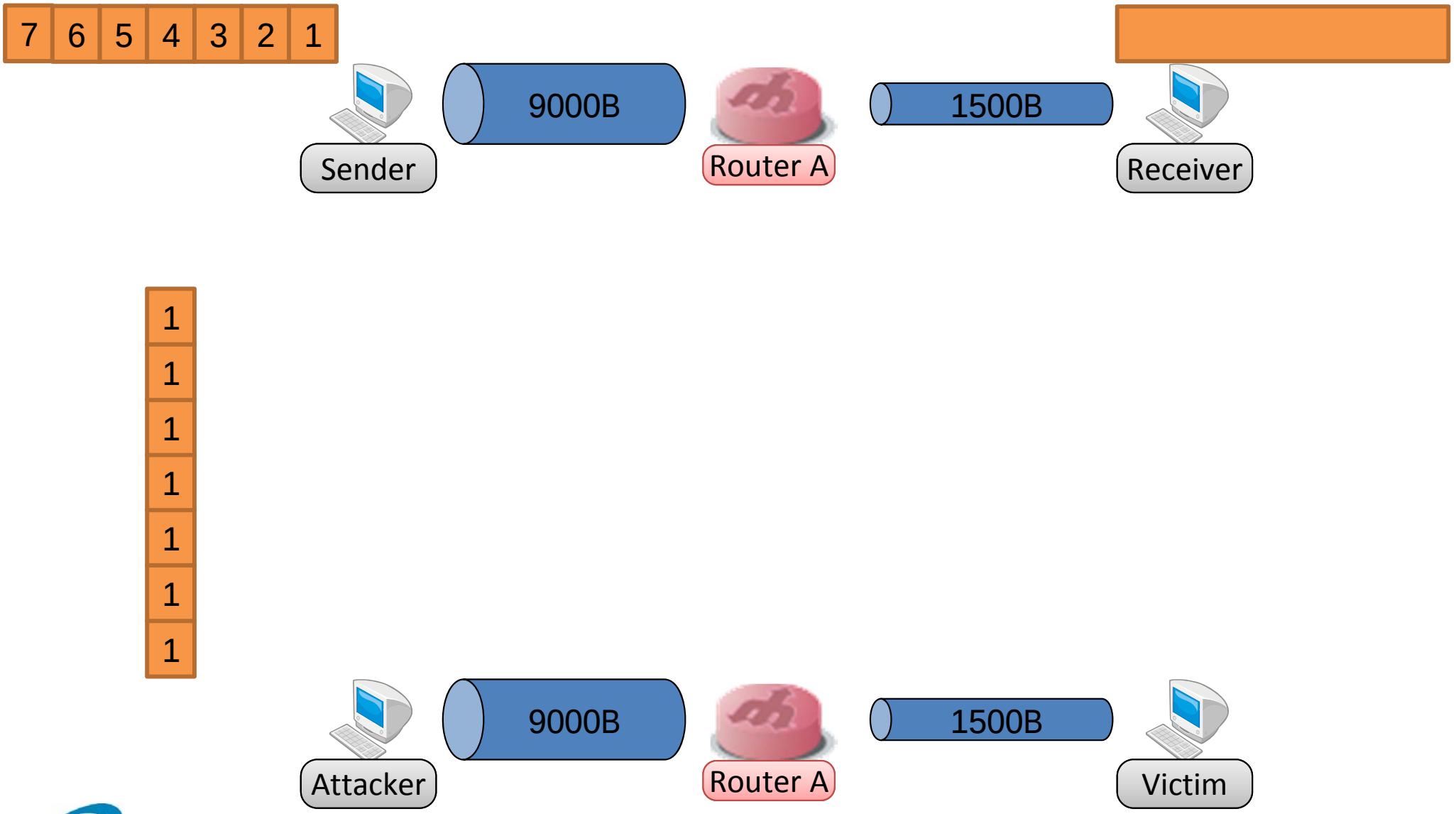


- 検証対象シナリオのうち 1 つ以上のシステムで攻撃が成立し、かつそれ以外のシステムで攻撃が失敗したもの

→ 一部の機器で成功した攻撃シナリオ（17 件）

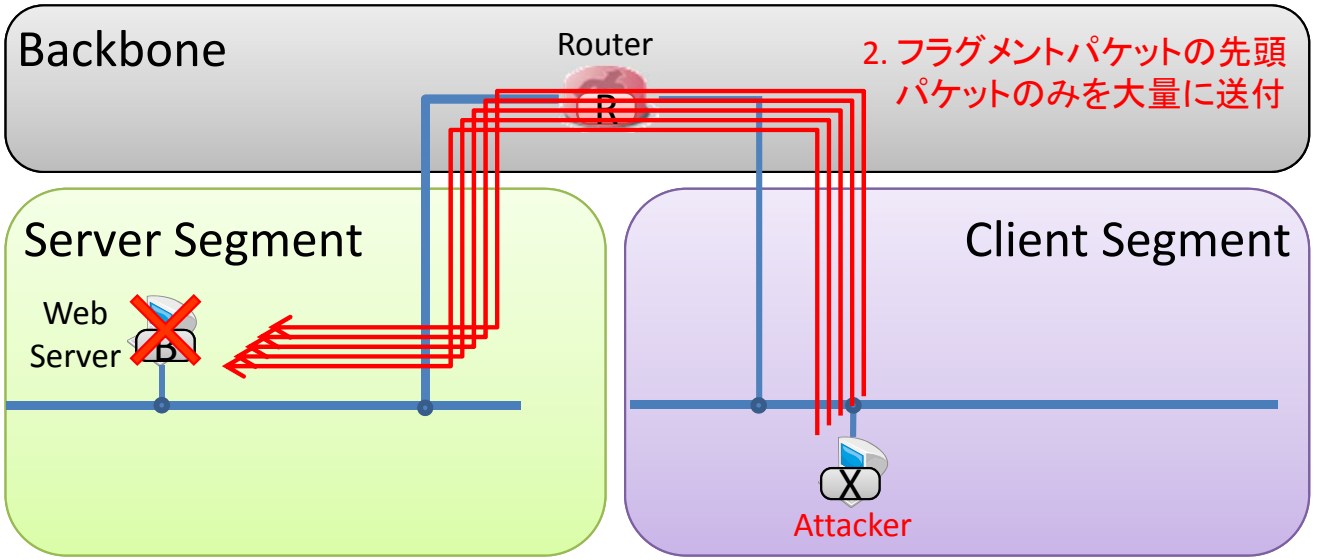
  - 小さく分割されたパケット（フラグメントパケット）の先頭パケットのみを大量に送付し通信を妨害する
  - 大量のDHCPv6 によるアドレス取得を実施し、DHCPv6サービスのアドレスプールを枯渇させる
  - など

IP フラグメンテーション



一部の機器で攻撃が成功したシナリオ (2)

- 小さく分割されたパケット（フラグメントパケット）の先頭パケットのみを大量に送付し通信を妨害する

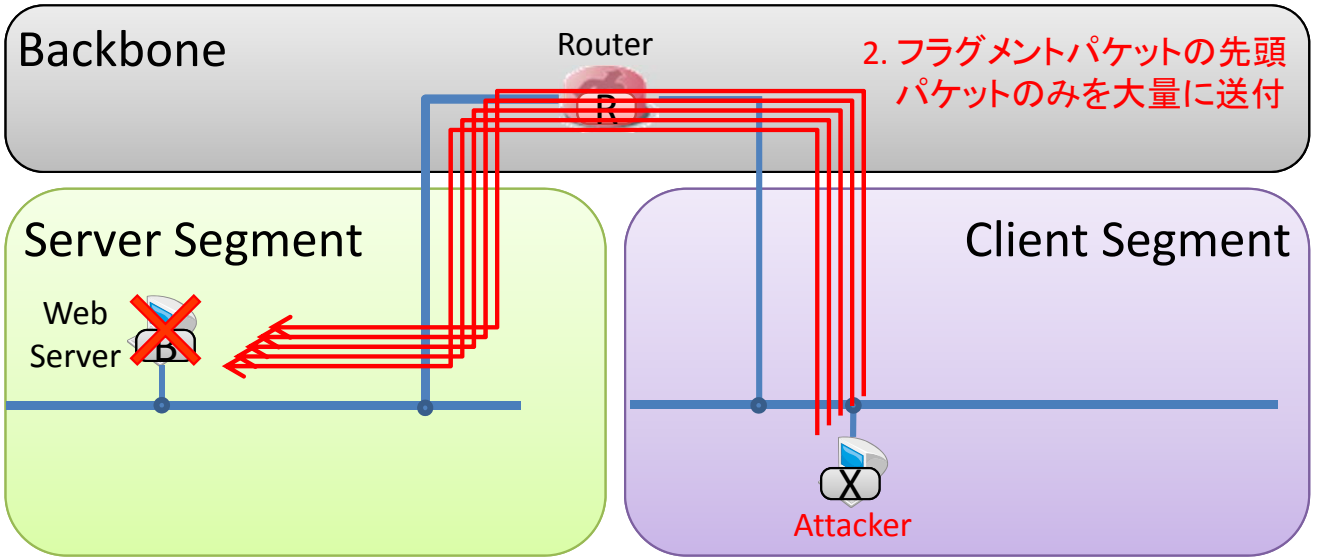


- 攻撃概要
  - 攻撃ノードXからノードBにフラグメントパケットの先頭パケットを大量に送信
- 想定される攻撃の効果
  - ユーザーノードBが誤動作を引き起こす
- 考察
  - 攻撃により、3 社中2 社の機器では、システムの再起動や、パケット（HTTPトラフィック）の送受信不能に陥った。
  - フラグメントパケットから元のパケットを復元するために、各フラグメントパケットをメモリに保持し続けた結果、CPUやメモリ資源が枯渇したと考えられる

対策手法の検討

Rate Limit による対策 (1)

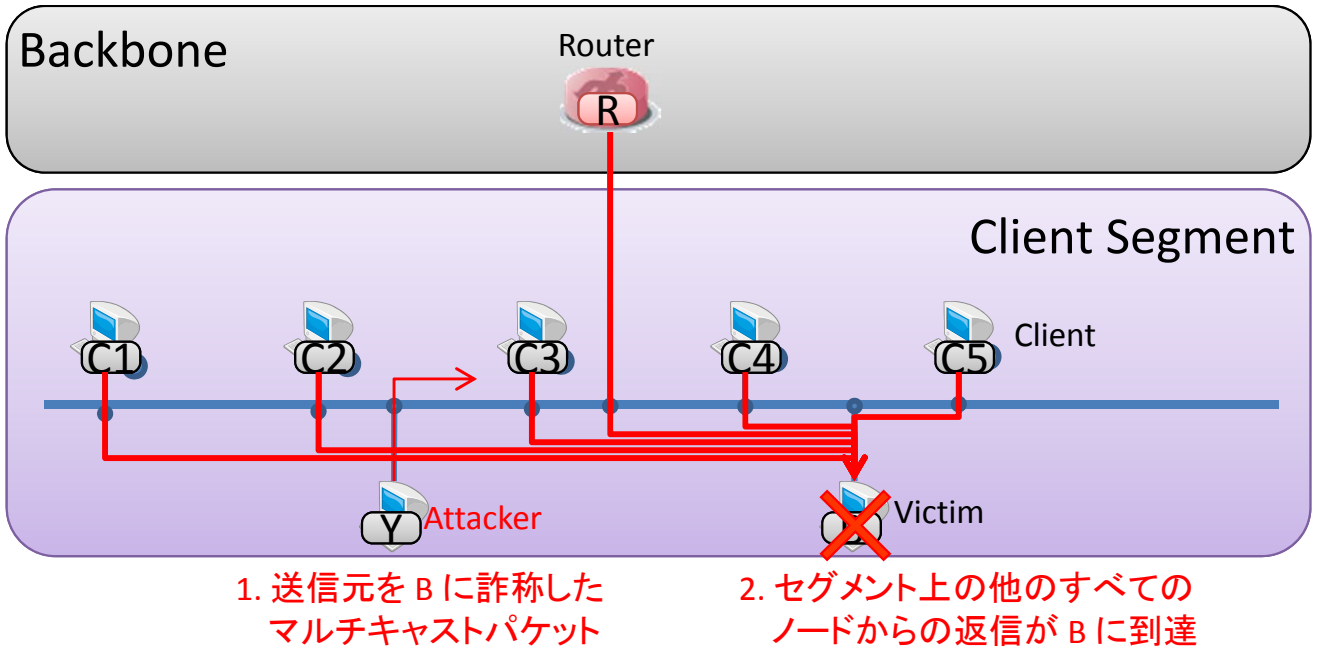
- 小さく分割されたパケット（フラグメントパケット）の先頭パケットのみを大量に送付し通信を妨害する



- 対策案
  - 案1）単一のホストから受信するフラグメントパケットの数に上限（Rate Limit）を設定する（例えば、単位時間あたり最大1,000パケットとする）。
  - 案2）単一のホストから大量にフラグメントパケットの先頭パケットを受信した場合、それらを不正なパケットであると判定するロジックを導入する。

Rate Limit による対策 (2)

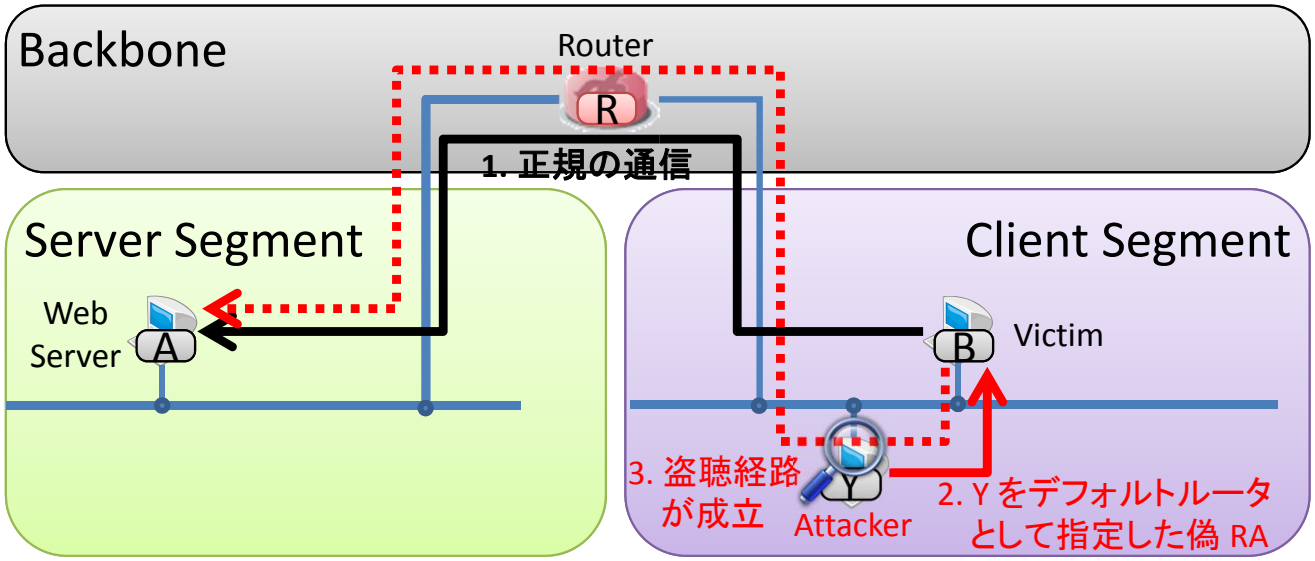
- 送信元を詐称したマルチキャストパケットを送信し、パケットの増幅攻撃を行う



- 攻撃の特徴
  - マルチキャストパケットを受信した各ノードがそれぞれエラーメッセージを返信することで、攻撃対象となったユーザーノードBに大量のパケットが届く。
- 対策案
  - ICMP に対する Rate Limit を設定することにより、返答の頻度を制限する。

RA Guard による対策

- 詐称した経路情報（RA：Router Advertisment）を送信してユーザトラフィックを攻撃ノードに誘導する



- 攻撃の特徴
  - パケットが攻撃ノードYを経由するような不正な経路情報（RA）を攻撃対象に送付
- 対策案
  - RA を悪用した攻撃については、RA Guard (RFC6105) を用いて**正規のルータのみしか RA を広告できない**ことをL2 レベルで担保することが有効

対策手法のまとめ

- 不正な経路情報による攻撃（Neighbour Discovery Protocolの悪用）
  - 対策）RA Guard（RFC6105）に対応した機器の導入
  - 対策）SeND (RFC3971)に対応した機器の導入

- DoS系の攻撃
  - 対策）特定のパケット (ICMP multicast など) に Rate Limit を設定
  - 対策）特定のパケットを破棄

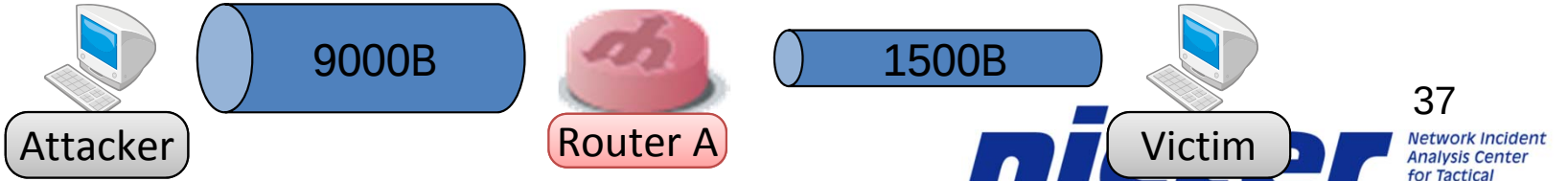
- 特殊な通信路を用いた攻撃
  - 対策）カプセル化を解除した上で検査を行う
  - 対策）SCTP（Stream Control Transmission Protocol）では適切にセッションを再構成した上で検査を行う

  ※ ただし、通信路が暗号化されている場合には、別の対策が必要

まとめ

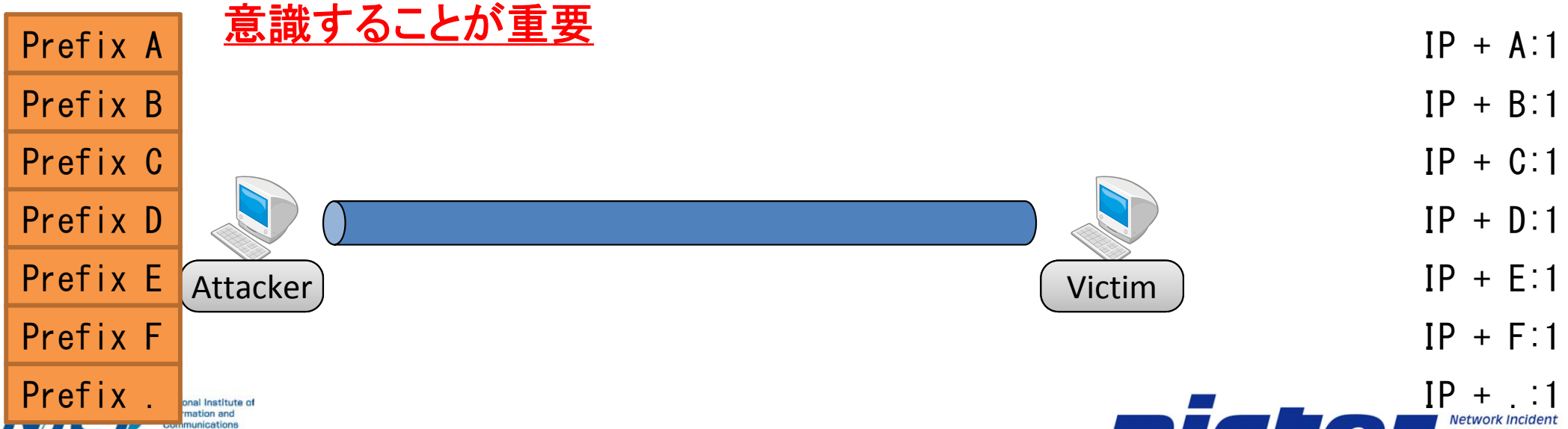
IPv6 実装上の注意点

- IP フラグメントの先頭パケットのみを大量に送付
  → ネットワーク機器がすべての通信の送受信不能に陥った
  → コンソール画面からの操作も不能に
- 原因
  – フラグメンテーションパケット保持用の一時記憶領域のサイズに適切な制限をかけていなかった
  – **特に IPv6 においては、すべての一時記憶領域に対して一定の制限を行うこと**



IPv6 実装上の注意点

- ルータになりすまし、大量のprefixを広告して端末のプレフィックステーブルを枯渇させる (シナリオ 31)
  - → CPU負荷が高くなり、操作/通信に障害が発生する。
  - → 攻撃終了後も100%のままである。
  - → 攻撃終了後もCPU100%で、アドレスの確認作業などの操作が不可能な状態。
- 原因
  - 端末が保持できる IP アドレス数を制限していなかった
  - **RA を悪用すると様々なバリエーションの攻撃が可能となる点を強く意識することが重要**



IPv6 固有の課題かIPv4 / IPv6 共通の課題か

IPv6 固有の脅威

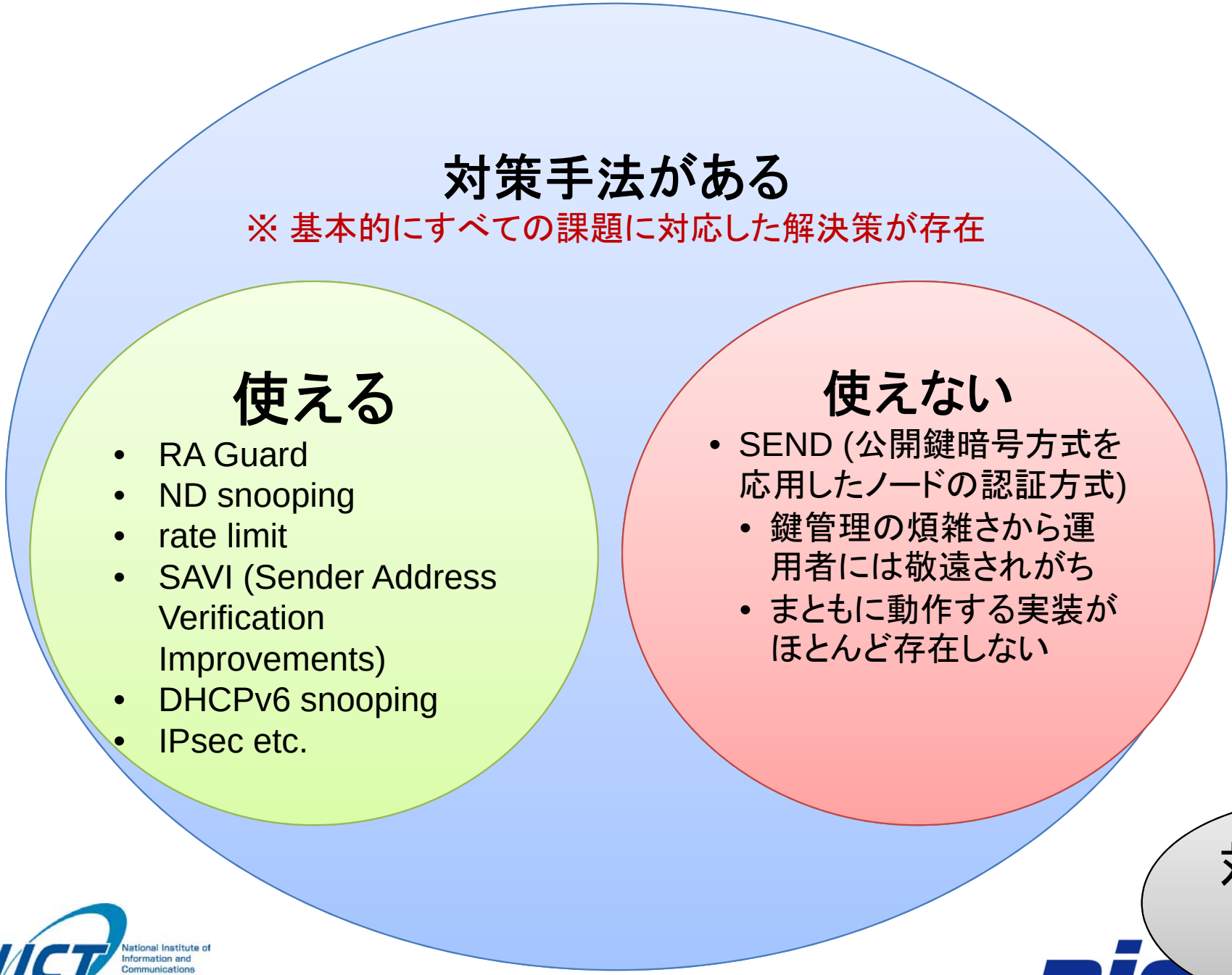
- RA, DAD 等、IPv6 の新機能を悪用した攻撃
- P2P リンクでのループ等、膨大なアドレス数を悪用した攻撃
- トンネルの悪用、など IPv6 への移行技術を悪用した攻撃

IPv4/IPv6 共通の脅威

- NDP / ARP / DHCP による中間者攻撃
- DoS 攻撃、など

※ DoS 攻撃系はv4/v6 共通
※ IPv6 ではアドレス数の増加による影響大

対策手法の有無について



対策手法が無い

ネットワーク管理者が意識すべき点

「IPv6 対応」≠「IPv6 への移行」

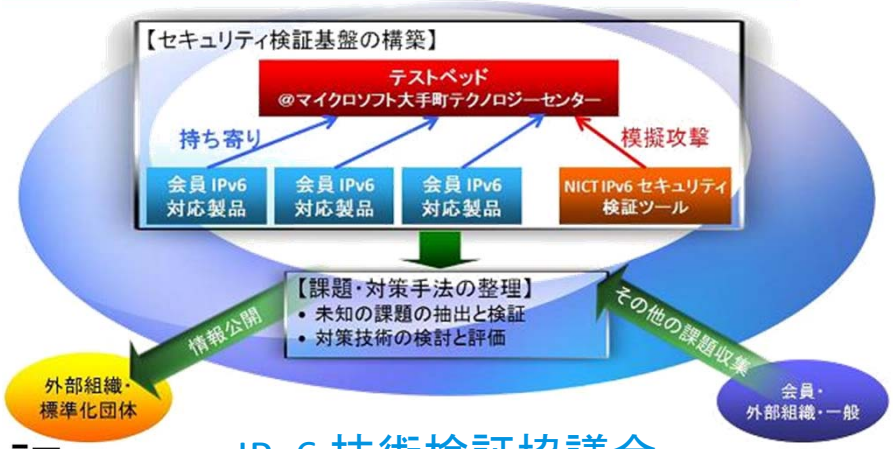
- IPv4 ネットワークが直ぐになくなるわけではない
  （対外接続しないネットワーク等では、IPv4のまま使用される可能性がある）
- 既存の IPv4 ネットワークに IPv6 ネットワークを追加して運用

- 二重のネットワーク運用
  - 3つの視点での考慮が必要
    - IPv4 ネットワーク
    - IPv6 ネットワーク
    - デュアル (パラレル) スタック・ネットワーク（IPv4/v6の両方に対応）

- IPv4 だけのネットワーク運用との相違点を把握することが重要

おわりに

- IPv6 セキュリティの検討
  - セキュリティ上の課題が数多く存在



IPv6 技術検証協議会

- IPv6 技術検証協議会の取り組み
  - 実証実験を通じて会員企業の IPv6 対応製品のセキュリティ対応状況を検証
  - 具体的な対策手法の導出とその有効性の検証
  - 活動報告書の一般公開

- まとめ
  - 脅威の数は多いが、そのすべてについて対策手法が存在
    - 実装者、運用者向けの啓蒙、標準化等が重要
    - より使いやすい、効果的な対策手法を提供していくことが必要
  - IPv4 から継続した脅威も多く存在
    - IPv4 におけるノウハウを応用することも可能