IPv6とセキュリティ

IPv6サミット 2013

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

IPv6に関する疑問・質問に誰かがもの凄い勢いで答えるパネル

IPv6サミット 2013

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY
1990

IPv6普及への想い

IPv6サミット 2013

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

出演者

コーディネーター：

篠田 陽一

北陸先端科学技術大学院大学 教授
IPv6普及・高度化推進協議会
セキュリティWG 主査

パネリスト：

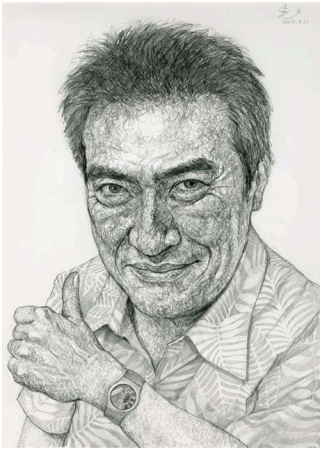
許 先明 ラック

衛藤 将史 情報通信研究機構

加藤 雅彦 日本ネットワークセキュリティ協会 - JNSA

國武 功一 ビーコンエヌシー

Self Introduction



北陸先端科学技術大学院大学（JAIST）
情報科学センター教授
高信頼ネットワークイノベーションセンター（dnic） センター長

StarBED プロジェクト創始者
NICT北陸StarBED技術センター

WIDEプロジェクト 運営評議員

内閣官房情報セキュリティセンター（NISC）
情報セキュリティ補佐官

情報通信研究機構（NICT）
R&Dアドバイザー

宇宙航空研究開発機構（JAXA）
情報化統括補佐

(株)ラック

許 先明

セキュリティオペレータ

いろいろ大変なんすよ が口ぐせ

誰でもそうだと思いつつ、ガイドラインやぐれーとてーぶるへの寄与は、はかり知れないものがある（感謝）

自己紹介

名前/所属：許 先明 / 株式会社ラック サイバー救急センター

本日の立場：セキュリティ・オペレータ

現実には、ネットワーク・仮想化システムの運用を通してセキュリティを保護

IPv6に対する思い

- ある意味での「諦め」と、将来に対する「期待」

1997年から、細々とIPv6普及活動をやって(手伝って)きたが、一般の関心は、IETF IPng WG Interim Meeting(@29/Sep/1999)の時代から大きく変わっていないような気がしている。

「本当の意味で切羽詰まらないとIPv6の利用者は増えないのだろう」という意味で「諦めて」いる

IPv4アドレスの不足はじわじわと現実に影響を及ぼし始めている。

従って「望むと望まざるとに関わらずIPv6に対応しなければならなくなる」という実感を持っているし、その意味で将来に「期待」もしている

LAC

(独) 情報通信研究機構

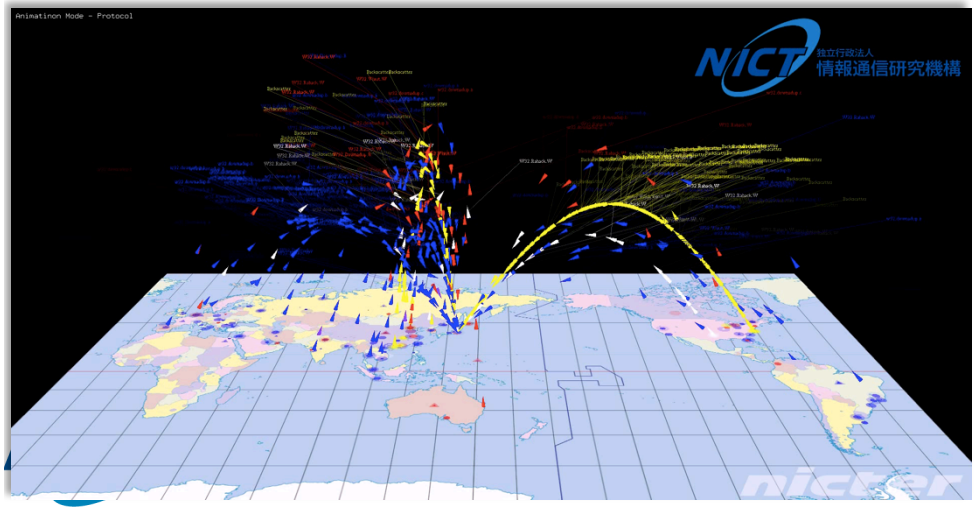
衛藤 将史

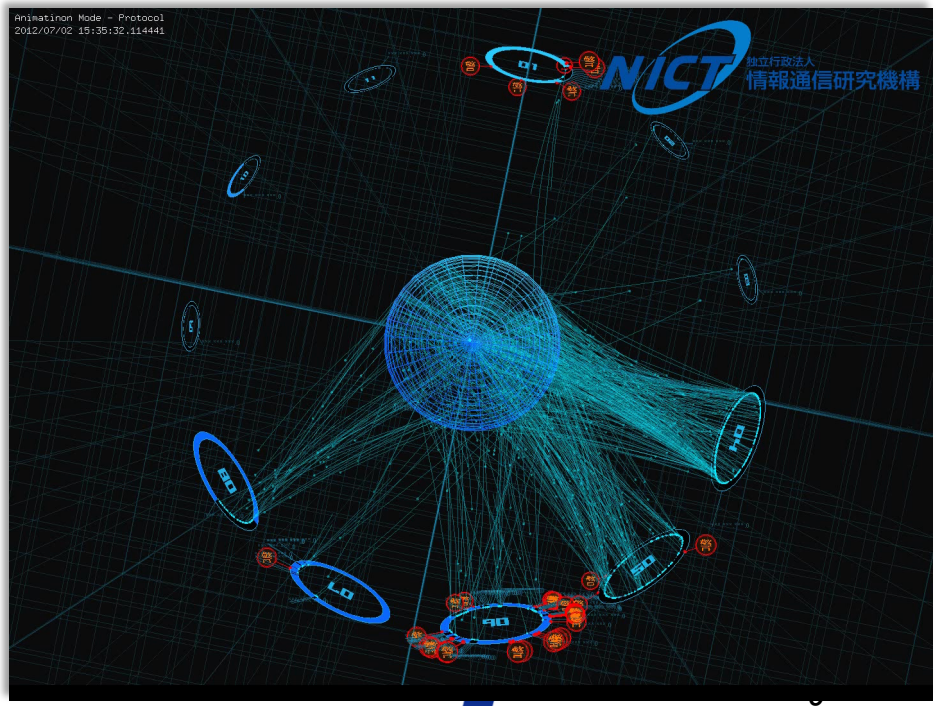
ネットワークセキュリティ研究者

バックエンド(mio)と共に、頼んだ仕事は着実にこなす、頼れる存在

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
- インシデント対策センター 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





nicter
Network Incident Analysis Center for Tactical Emergency Response

IPv6 への思い

同　情

– IPv4 : Internet 創生期からの積み重ね
– IPv6 : いきなり実戦投入

(NPO) 日本ネットワークセキュリティ協会

加藤 雅彦

業界団体の中のひと

詳細は本人から

自己紹介

- **氏名・所属**
  - 加藤雅彦
  - NPO 日本ネットワークセキュリティ協会 調査研究部会長

- **業務経験**
  - **運用業務**
    - ユーザ系企業でのインターネット、イントラネット環境の運用（前職）
    - フォレンジック対応、セキュリティインシデント対応
    - クラウドサービスの品質セキュリティ管理
  - **設計構築業務**
    - オープン系システムのインテグレーション
  - **セキュリティサービス業務**
    - 脆弱性検査サービス（ネットワーク、Webアプリケーション、データベース）の企画、開発、運営

自己紹介

- **業務経験**
  - **研究開発**
    - ネットワークシステムにおけるセキュリティの定量評価に関する研究
  - **各種渉外活動**
    - NPO 日本ネットワークセキュリティ協会幹事、調査研究部会長
    - 日本セキュリティオペレーション事業者協議会 運営委員
    - 日本クラウドセキュリティアライアンス 幹事
    - 内閣官房情報セキュリティセンター WG委員
    - 経済産業省 クラウドセキュリティガイドライン作成メンバー
    - ASPIC クラウドサービス利用者の権利保護の在り方委員会委員
    - 情報処理推進機構 脅威と対策WG 委員、ITサービス継続WG委員
    - 日本セキュリティ監査協会 WG委員
    - JIPDEC　情報化白書2012 「クラウドコンピューティングのセキュリティ」執筆
    - その他、各種セミナー講演、大学等での集中講義 等

本日の立ち位置と、v6に対するもっとも大きな思い

- **本日の立ち位置**
  - セキュリティ業界団体の人
    - ですが、業界団体の代表ではありません
    - 個人的な意見として発言します
  - v6ド素人

- **v6に対するもっとも大きな思い**

痺れ（思いじゃないけど）

新しい攻撃とか事件とか起きると思うと痺れる
サポートの手間が増えたりすると思うと痺れる
v6来るといってなかなか来ないので痺れが切れる

(株) ビーコンエヌシー
國武 功一

IPv6ホスティング対応したが仕事にならないと悩む

なにやってる人？

- 1997-2000年 ISPでネットワーク屋さん
- 2001-2003年 ネットワークコンサル屋さん
- 2003-2008年 Webアプリ開発屋さん
- 2008年-　　データセンター屋さん

そんなことしつつ

- コミュニティ活動/スタッフなど

2007年
　JANOG19　Publicity, 司会
2006年
　JANOG17　Program Committee Co-Chairs
2005年
　JANOG15　Steering Committee Co-Chairs
2004年
　JANOG13　Local Arrangement
2003年
　JANOG12　Local Arrangement
　JANOG11　Publicity
2002年
　JANOG10　Publicity Co-Chairs
　JANOG9　Publicity, Logger
2000年
　USAGI Project / 2000年10月発足 - 2008年3月 活動完了
1999年
　JANOG5　Logger

そんなことしつつ

- 雑誌・ウェブ記事など
  - 2012年
    - atmarkIT (@IT) 2011/7/19
  - 2009年
    - 日経コミュニケーション2009年10月15日号
    - 日経NETWORK 2009年06月号
  - 2006年
    - オープンソースマガジン(OSM) 2006年 08月号
    - UNIX magazine 2006年7月号
  - 2003年
    - 5分で分かるIPv6プログラミング / 2003年6月
    - IPv6 magazine No.5
    - モバイル機器からWebDAVを使う / 2003年4月
    - Linux Magazine, 2003年1月号
  - 2002年
    - TCP/IPをマスターしよう
  - 2001年
    - IPv6 Journal ステータスレポート
    - Linux Magazine, 2001年8月号
    - Linux Magazine, 2001年6月号

そんなことしつつ

- 講演/インタビュー等

2012年
- 「Inetrnet Week 2012」[D3] IP Meeting 2012～人のチカラ、インターネットのチカラ～
- 「Inetrnet Week 2012」[H3] IPv6 ハンズオン サーバ編
- IPv6サーバ編（座学＋ハンズオン）
- IPv6サーバ基礎編

2011年
- IPv6対応への道しるべ(インタビュー協力)

2010年
- Internet Week 2010
- IPv6サーバ基礎編(沖縄)
- IPv6サーバ基礎編(広島)
- IPv6ハンズオンセミナー/IPv6 サーバ基礎編
- JANOG25

2009年
- IPv6ハンズオンセミナー（IPv6オペレータ育成プログラム）/ 予定
- Internet Week 2009 クラウドの虚像と実像」～クラウドの本質を正しく理解する3時間～ パネルディスカッション
- Internet Week 2009仮想化DAY IaaSセッション
- Internet Week 2009仮想化DAY パネルディスカッション
- IPv6ハンズオンセミナー（IPv6オペレータ育成プログラム）
- Interop Conference 2009
- Interop Tokyo 2009
- 日本UNIXユーザ会勉強会

2008年
- Virtualized Infrastructures Workshop [02]
- InternetWeek 2008
- NEC C&Cフォーラム
- Virtualized Infrastructures Workshop [01]

2007年
- NEC 2007年データセンターソリューションセミナー

2006年
- JANOG18
- Interop 2006 Tokyo

2005年
- Internet Week 2005
- JANOG16

2003年
- 第57回IETF報告会

2002年
- Networld+Interop 2002 ビギナーズセミナー

2000年
- JANOG6

その他

Twitter : @kunitake 

IPv6の活動：USAGI Project, 他社技術支援、IPv4アドレス枯渇対応タスクフォース、各種雑誌記事など

最近のお仕事：問題が起きたら、お客様へ謝りに行ったり、障害報告書書いたりしてます。楽しいことしたいです

IPv6提供サービス

- CDN（他者様サービスとの組み合わせ）
- インターネット接続サービス
- ファイアウォール
- ロードバランサー
- WAF(Web Application Firewall・フルスペック）
- サーバホスティング（Linux, Windows)
  - 仮想、物理
- 各種運用サービス

IPv6、自社への展開

- Webサーバ
- SMTP
- 社内システム（チケット管理システムなど）

〒163-0241 東京都新宿区西新宿二丁目6番1号 新宿住友ビル41F
TEL：03-3342-1135 FAX：03-3342-1136 http://www.benc.jp/

IPv6への思い

憂鬱

〒163-0241 東京都新宿区西新宿二丁目6番1号 新宿住友ビル41F
TEL:03-3342-1135 FAX:03-3342-1136 http://www.benc.jp/

セキュリティWGの活動

- ガイドライン
  - IPv6対応セキュリティガイドライン(2012.09)
- ガイドラインの拡張
  - データセンター・ホスティング向けに拡充の予定だが・・・
- SP800-119
  Guidelines for the Secure Deployment of IPv6抄訳
  (WIP)
- v6ぐれーとてーぶる (WIP)
  - イマココ

v6普及って・・・

v6グレートテーブル (WIP)

- セキュリティWGの現状仕事の一部
  - v6におけるセキュリティ上のさまざまな懸念が、別の問題に帰着する、あるいはv6固有の問題ではないことが多いことから、知られている問題および解を列挙することが必要。
- テーブルエントリ
  - 固有ID、カテゴリ、セグメント、v6固有、問題の名前、問題の概要、問題定義への参照、解への参照
- 現在75エントリ
  - v4/v6共通の問題が多い
  - 明確な解が与えられていない問題も多い
  - v4/v6のインタラクションが起きる箇所での問題の存在

問題認識

個人的に思うIPv6の問題点は

仕様上の問題が多い　(I/F IDが64bitあることによる問題等)

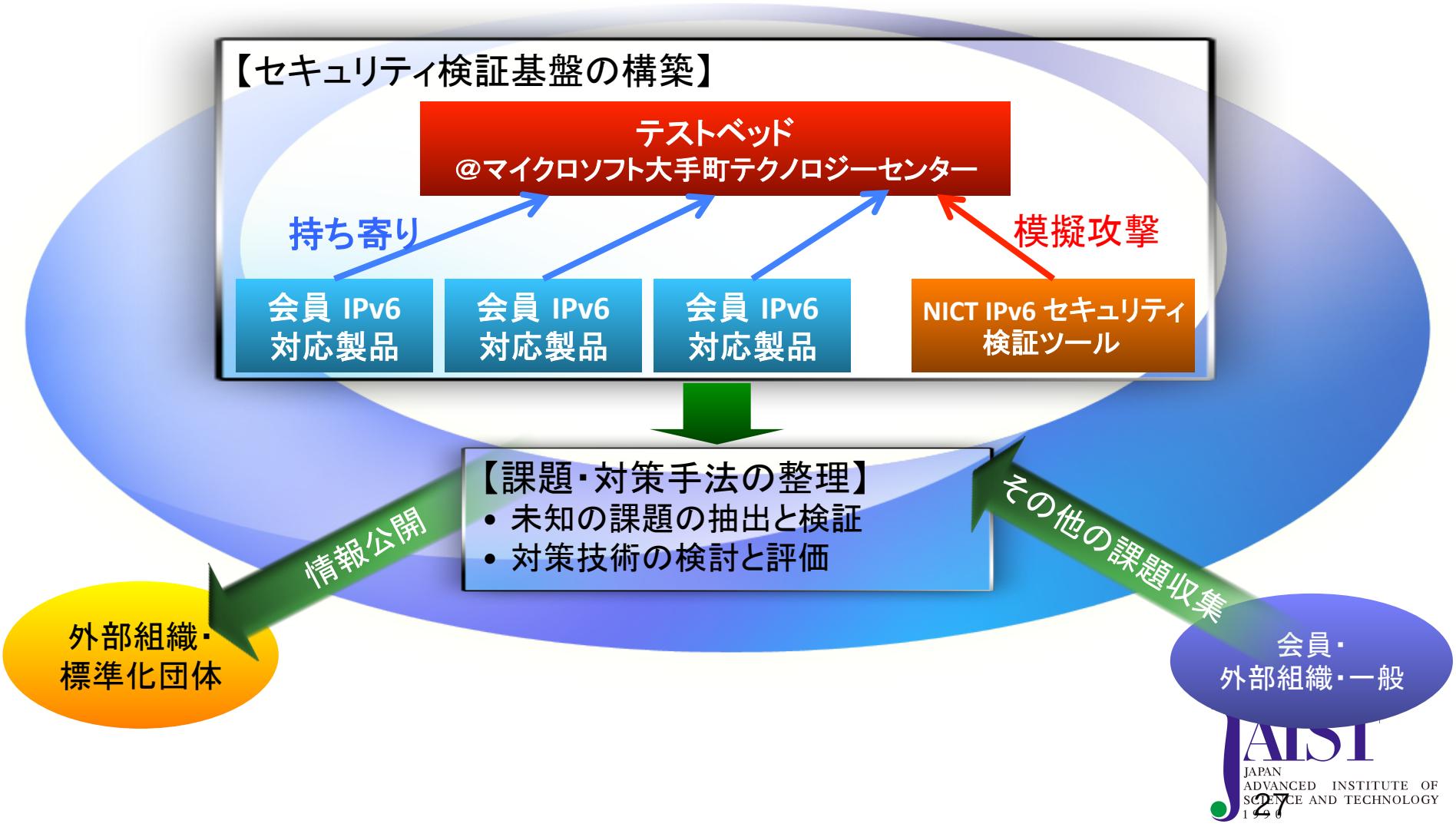
結局アプリケーション対応が多い

といわざるを得ないこと

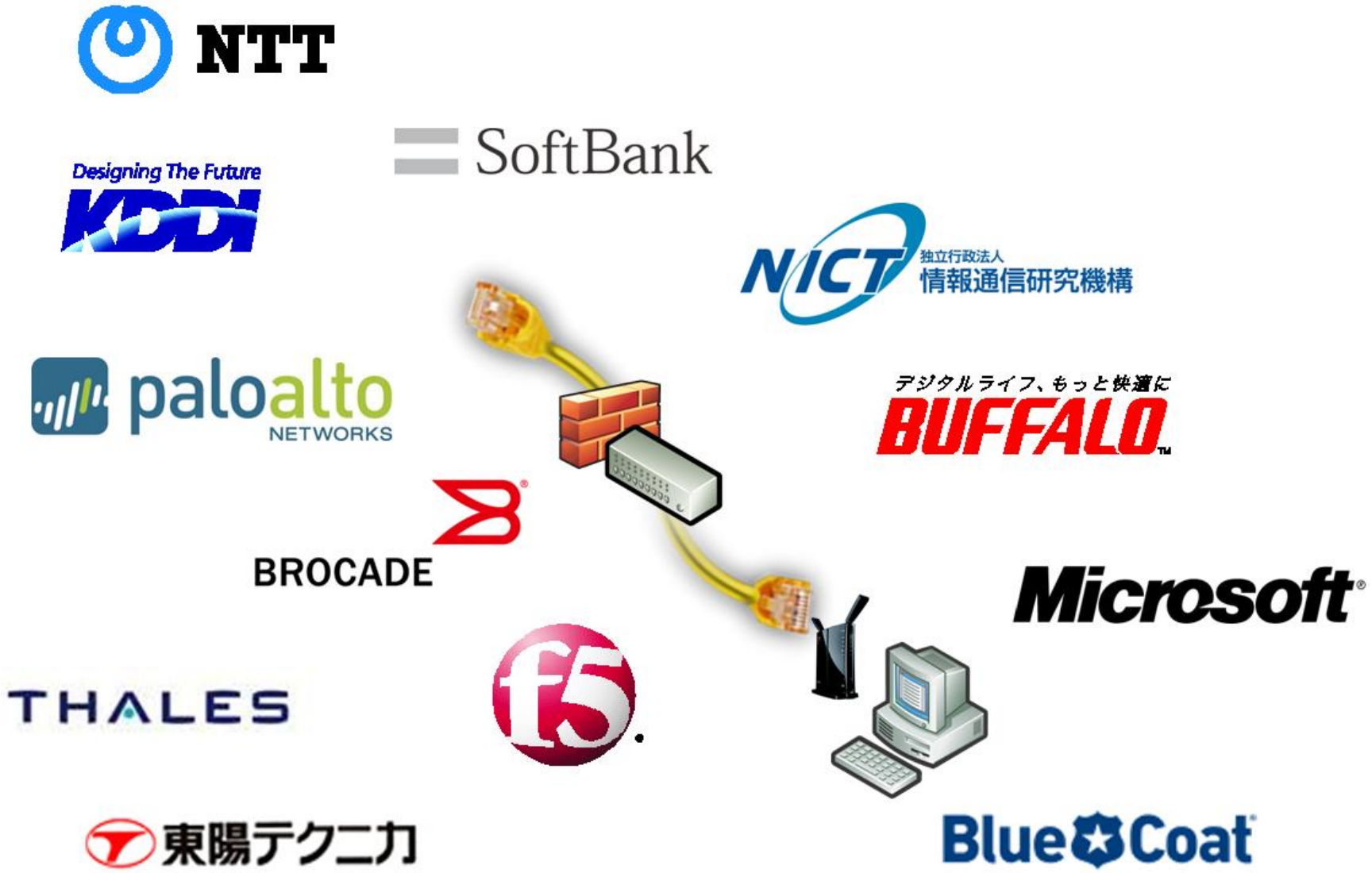
JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

IPv6 技術検証協議会の設立

2010 年 7 月

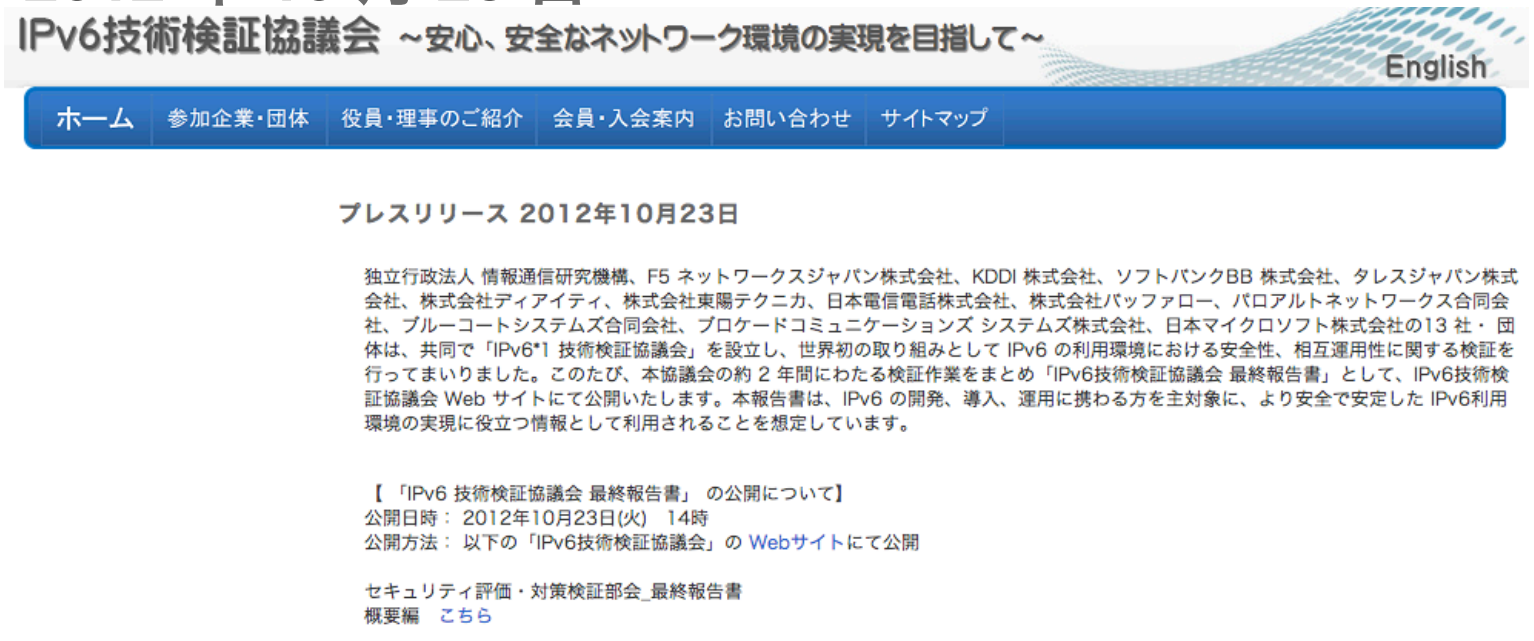


会員企業（12企業・組織）


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

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

National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

脅威の整理 (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

脅威の整理 (2)

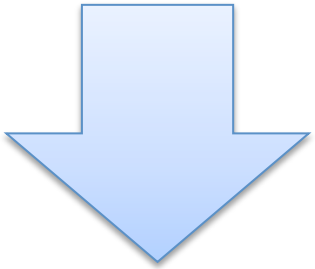
- ✓ 不正なジャンボペイロードを用いて通信を妨害 (シナリオ 1)
- ✓ 不正なフラグメントパケットを用いて通信を妨害 (シナリオ 2)
- ✓ Pad1オプションを用いて通信を妨害 (シナリオ 3)
- ✓ 詐称したルータ広告(RA)メッセージを用いて通信を妨害及び盗聴 (シナリオ 5、10、11)
- ✓ 詐称したICMPリダイレクトメッセージを用いて通信を妨害及び盗聴 (シナリオ 8、9)
- ✓ 不正なDADを用いてIPv6アドレスの取得を妨害 (シナリオ 13、14)
- ✓ マルチキャストアドレスを用いてネットワークに関する情報を収集 (シナリオ 16)
- ✓ 詐称したマルチ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

脅威の整理 (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
- ✓ 大量のセッション
- – バックドアを待ち
- – 感染システムの

さまざまな課題が雑多に存在

- 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？



- 分類軸の提案
- 40 項目の課題に適用
- 根源的な問題について考察

分類軸の提案

- 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

分類軸 1: IPv6 固有の課題かIPv4 / IPv6 共通の課題か

	IPv6 固有	IPv4 / IPv6 共通
シナリオ	1、3、5、7、10、11、13、14、16、23、24、31、35、37、38	2、4、6、8、9、15、17、18、19、20、21、22、25、26、27、28、30、32、33、34、36、39
主な脅威	• RA, DAD • P2P リンクでのループ • トンネルの悪用、など	• NDP / ARP / DHCP による中間者攻撃 • DoS 攻撃、など
考察	• IPv6 で新たに導入されたプロトコルやアドレス増、IPv4 からの移行技術に起因する課題が多い	• DoS 系の攻撃は v4/v6 共通 • IPv6 ではアドレス数の増加による影響も大きい

分類軸 2 :対策方法による分類

	プロトコル	実装	運用	その他
シナリオ	7、17	1 ～ 24、 26～ 28、 30 ～ 40	3、5、8 ～ 11、 16、17、19 ～ 21、23 ～ 25、 28、34、36、39	29
主な脅威	• ICMP Parameter Problem による DoS	• DoS 攻撃系	• DoS 攻撃系 • NDP / ARP / DHCP による中間者攻撃	• ファジングツールを用いた攻撃
考察	• ICMP Parameter Problem への応答は任意にすべき	• レートリミットを適用できる実装を意識すべき	• 802.1x 等の認証により不要なノードは L2 で切断すべき • 通信路暗号化	• 必要に応じてファジングツールを用いた検証を行う

分類軸 3 :攻撃対象の機器にもとづく分類

	エンドノード	ネットワーク機器	セキュリティ機器
シナリオ	4、7、12、18、22、23、27、28、30、33	1、2、3、5、8 ～ 11、13、14、16、17、19、20、21、25、26、31、34 ～ 40	6、15、24、29、32
主な脅威	• RA 等による中間者攻撃 • OS のアドレス付与メカニズムを悪用した攻撃	• ルータ、スイッチに対する DoS	• FW, IDS すり抜け

分類軸 4: 解決策の有無

- 現状で解決策のあるもの/ないもの
  - 基本的に全て解決策はある
  - ある & 使える
    - RA Guard
    - ND snooping
    - rate limit
    - SAVI (Sender Address Verification Improvements)
    - DHCPv6 snooping
    - IPsec etc.
  - ある & 使えない / 使われていない
    - SEND (公開鍵暗号方式を応用したノードの認証方式)
      → 鍵管理の煩雑さから運用者には敬遠されがち
      → まともに動作する実装がほとんど存在しない

v6普及における問題点

- コスト
  - 結局v6とv4の混在環境の構築運用が現実で手間（コスト）が増える
- リスク
  - v6にしたら安全になるわけでもなく、運用上のリスクが増える

普及を妨げてるもの

- フォールバック問題
  - ホスティングを提供する立場としては、IPv6に対応することで、コンテンツ配信に問題が発生する可能性を増やしてしまう
  - さらに品質への要求が高まっている現状、これは許容しずらい
- リスクを説明しきれない
  - IPv6に対応することも、しないこともリスク。
  - リスクを取ることに対するリターンとは？
- 運用経験の欠如

真のv6普及に向けて

- 「関係ない」を見直しプレイヤー間の「壁」を取り払う
  - 「独立」あるいは「透過」の思い込みや幻想を捨てる。
  - 「移行・共存」はデュアルスタックがあれば問題ない」の幻想
    - プロトコルエンジニア v.s. インテグレータ・オペレータ
  - 「わが社のサービスはv6 readyです」
    - プロバイダ v.s. ユーザ
    - ユーザのネットワーク構成や機能の実現の仕方は想像以上に複雑である
- 共存・移行を腰を据えて行う覚悟と環境
  - 複雑で大規模なネットワークにおける実例を積み重ねる
  - 新しい技術の導入への共存・移行の対応