IPv6普及･高度化推進協議会活動アップデート

津国　剛
株式会社三菱総合研究所/IPv6普及･高度化推進協議会

協議会の活動の主体であるWG構成

基本戦略SG

IPv6対応に伴う課題の検討

- サーティフィケーションWG
- IPv4/IPv6共存WG
- セキュリティWG

IPv4枯渇に伴う課題の検討

- IPv4枯渇に係るインターネット新技術導入にむけた検討WG

IPv6の人材育成

- ビジネステストベッドWG
- ビジネスラーニングWG

IPv6ならではの使い方の検討

- FMCv6プラットフォームWG
- デジタル情報家電v6プラットフォームWG

IPv6のプロモーション

- ビジネスエクスチェンジWG

IPv6普及・高度化推進協議会
IPv6 Promotion Council

IPv6家庭用ルータSWG

- 2014.06.19「IPv6家庭用ルータガイドライン第2版とTR-124i2の比較」を公開
  - IPv6家庭用ルータガイドラン第2版(v6pc 2010年7月29日公開)
  - TR-124i2(Functional Requirements for Broadband Residential Gateway Device Issue2)(Broadband Forum 2010年5月発行)
  - 日本の議論と国際的議論との際の明確化、将来的なガイドライン改版時の内容の取り込みを念頭にドキュメントの比較を実施

IPv6家庭用ルータSWG

- 比較内容の例

4 Local Area Networking (LAN)

4.1 General LAN Protocol

Section	Item	Requirements	ガイドラインとの比較
LAN.GEN.	1	The device MAY support SOCKS as defined in IETF RFC 1928 for non-ALG access to the public address.	ガイドラインには記述がないが，対応不要.
LAN.GEN.	2	Both NetBios and Zero Config naming mechanisms MAY be used to populate the DNS tables.	ガイドラインには記述がないが，対応不要.
LAN.GEN.	3	The device MAY act as a NETBIOS master browser for that name service.	ガイドラインには記述がないが，対応不要.
LAN.GEN.	4	The device MUST support multiple subnets being used on the local LAN.	ガイドラインには記述がないが，次版で現在の 3 章に，BBF の MUST 機能として紹介した上で，MAY 機能として記述する.

IPv6導入に起因する問題検討SWG

- 2014.07.11「国内IPv6対応サービス状況チェックで発見された事例について」を公開
  - IPv6対応状況について調査を実施してきた際に発見された事例をもとに、サーバサービス等、外部公開サービスをIPv6に対応させる際に注意すべき点についてまとめたもの
  - 典型的な不具合事例
    - DNS設定の不具合：場合によっては，DNSによる名前解決に失敗し，サービスにアクセスできない
    - Web サービスの不具合：IPv6でのアクセスに失敗する場合がある
    - これらはIPv6に特化した不具合ではないが、「IPv6を導入をきっかけとして発生」したり「IPv6サービスへのアクセスが少ないため発見が遅れた」等がある

IPv6導入に起因する問題検討SWG

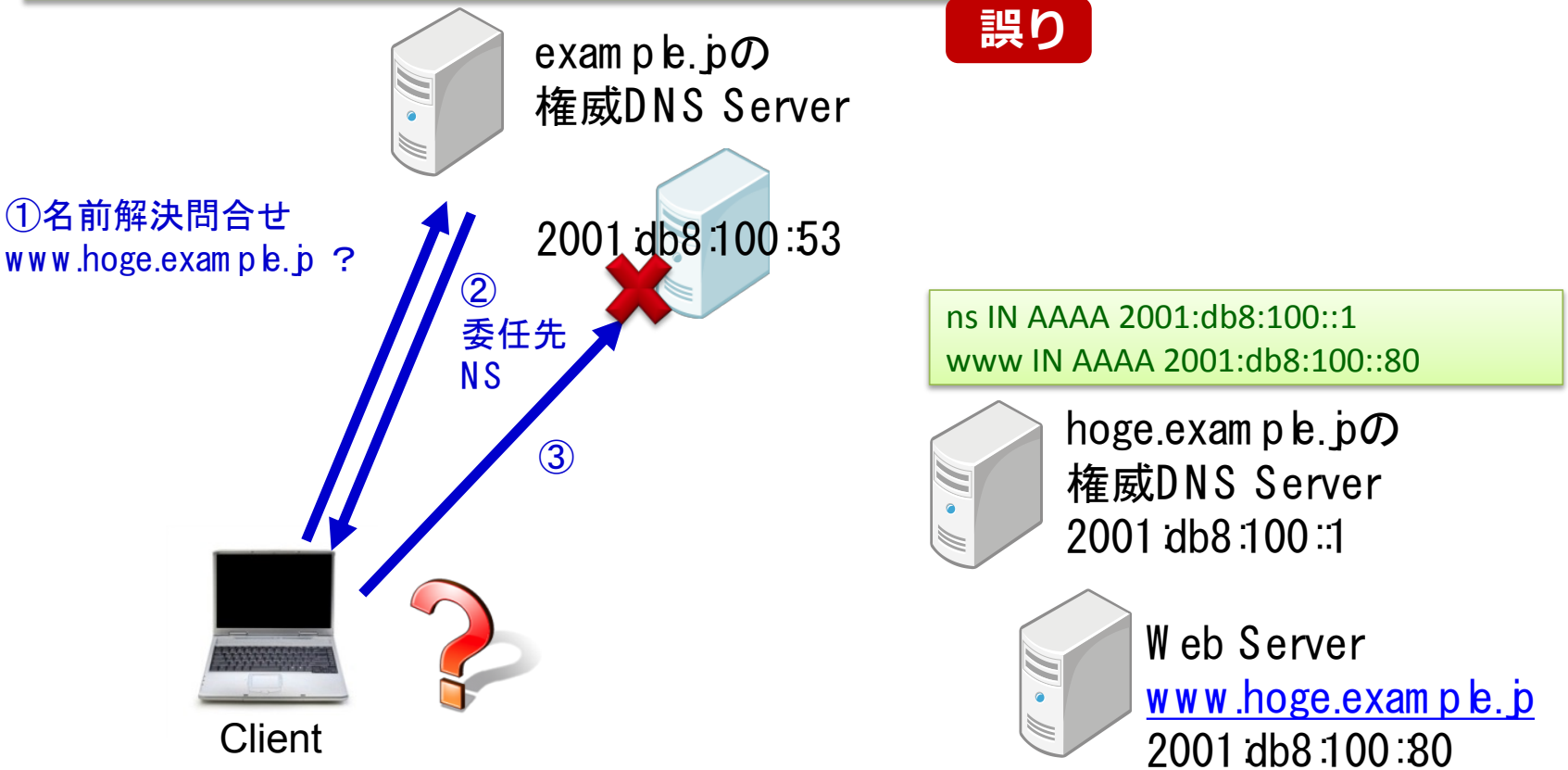
- 実際の不具合の例（事例１）
  - ネームサーバのグルー(glue) AAAA のIPv6アドレスと，ゾーンファイル中の AAAAレコードのIPv6アドレスが違っている．
    - レジストリ等，上位ドメインの DNS への登録情報と，権威サーバでの設定情報が整合していない．
    - 本事例は，IPv4のみの環境でも同等のことが発生しうる．
  - 想定される影響
    - ネームサーバ のグルーに書かれているDNSサーバにアクセスできない場合，当該ドメインと通信できない可能性がある（実装に依存）．
    - ドメイン乗っ取りの原因になる可能性がある．
  - 検証方法（例）
    - http://dnscheck.jp/ によりチェックする ．
  - その他
    - IPv6導入時，グルーレコードや，権威サーバの情報にAAAAアドレス記述が追加されることがある．この場合，整合性を取るべき情報が増えること，IPv6普及段階では，追加した情報に対するアクセスが少なく，結果として不具合の発見が遅れることなどが想定される．

IPv6導入に起因する問題検討SWG

- 実際の不具合の例（事例１）

hoge.example.jp NS ns.hoge.example.jp
ns.hoge.example.jp IN AAAA 2001:db8:100::53

誤り



IPv6導入に起因する問題検討SWG

- 不具合確認のための参考情報

http://dnscheck.jp/

参考2： telnet コマンドを利用した動作確認の例

サービスごとの動作確認例を示す. アンダーラインの行が入力行となる.

SMTP (port 25/tcp)

```
% telnet 2001:db8::25 25
Trying 2001:db8::25...
Connected to 2001:db8::25.
Escape character is '^]'.
220 mail.example.jp ESMTP Postfix
helo example.jp
250 mail.example.jp
mail from: test@example.com
250 2.1.0 Ok
rcpt to: test@example.jp
250 2.1.5 Ok
2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: test mail

test
.
250 2.0.0 Ok: queued as 051B22F5CAB
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

http (port 80/tcp)

```
% telnet 2001:db8::80 80
Trying 2001:db8::80...
Connected to 2001:db8::80.
Escape character is '^]'.
GET / HTTP/1.1
host: www.example.jp

HTTP/1.1 200 OK
        :       :
```

Pop (port 110/tcp)

```
% telnet 2001:db8::25 110
Trying 2001:db8::25...
Connected to 2001:db8::25.
Escape character is '^]'.
+OK Dovecot ready.
user test
+OK
pass testpass
+OK Logged in.
```

参考3： openssl コマンドを利用した動作確認の例

アンダーラインの行が入力行となる.

- SSL/TLS通信のチェック
  - https

```
% openssl s_client -connect "[2001:db8::80]:443"
        :       :
GET / HTTP/1.1
host: www.example.jp

HTTP/1.1 200 OK
        :       :
```

  - smtp, pop, imap等は2種類のハンドシェーク
    - ✓ いきなりSSL/TLS開始
    - ✓ plaintextで接続し、STARTTLSコマンド開始

```
% openssl s_client -connect "[2001:db8::25]:25"

% openssl s_client -connect "[2001:db8::25]:25" -starttls smtp

% openssl s_client -connect "[2001:db8::25]:110"

% openssl s_client -connect "[2001:db8::25]:110" -starttls pop3
```

アプリケーションのIPv6対応検討SWG

- 2014.06.10「アプリケーションのIPv6対応ガイドラインWebアプリケーション編(案)」のパブリックコメント実施
  - IPv4/IPv6共存期を前提としたアプリケーション開発についての情報整理を行い、アプリケーション開発者に向けた情報発信と情報共有のためのドキュメントの取りまとめを実施
  - 「アプリケーションのIPv6対応ガイドライン 基礎編」（2012.12.05公開）の続編として、Webアプリケーションの IPv6対応についてまとめたもの

アプリケーションのIPv6対応検討SWG

- 主な記載内容
  - 3. アプリケーション開発におけるIPv6対応
  - 4. IPv6対応のプログラミング言語と実行環境を使用する
  - 5. Webアプリケーションにおける通信処理のIPv6対応
    - 5.1 IPv6アドレスの名前解決
    - 5.2 通信の試行順序
    - 5.3 フォールバックとその解決
  - 6. データとしてIPv6アドレスを扱う箇所の対応
    - 6.1 データベースへの格納
    - 6.2 ログ出力への影響
    - 6.3 Webフォームへの入力
    - 6.4 IPv6アドレスの検索や整列
  - 7. その他の考慮事項
    - 7.1 DMZのIPv6対応方式とWebアプリケーションがアクセス元IPアドレスを取得する方法
    - 7.2 WebページへのIPアドレスの埋め込み

基本的理念

項目別の留意点

IPv6企業ネットワーク導入SWG

- 企業ネットワークへのIPv6導入シナリオの策定、企業・自治体・SIer/NIerなどへのIPv6普及戦略の検討
  - 個々のトピックについて各回で議論を実施
    - グローバル企業のIPv6対応
    - 国内外のIPv6対応状況
    - IPv6対応端末がIPv4onlyネットワークに入り込むリスク
    - フォールバック問題の現在の状況
    - モバイルのIPv6対応状況とフォールバック問題
    - 情報システム部門の一括アウトソースによる中小企業の一斉IPv6化
  - IPv6企業ネットワーク導入ガイドラインに向けた、検討内容の整理の実施
    - IPv6の積極利用のモチベーション
    - フォールバック問題
    - 意識しないIPv6端末のリスク

アクセス網IPv6サービス導入検討SWG

- アクセス網におけるIPv6普及状況を四半期ごとに算定し公開

■ フレッツ光ネクストのIPv6普及率

フレッツ光ネクストのIPv6の普及率 =
((1)IPoE契約数 + (2)PPPoE実測契約数) / (3)フレッツ光ネクスト総契約数

	NGN IPv6契約数	NGN 契約数	NGN IPv6普及率
2012.12	67,000	8,127,000	0.8%
2013.03	121,000	8,595,000	1.4%
2013.06	182,000	9,094,000	2.0%
2013.09	235,000	9,506,000	2.5%
2013.12	287,000	10,741,000	2.7%
2014.03	357,000	11,301,000	3.2%
2014.06	426,000	13,588,000	3.1%
2014.09	613,000	15,805,000	3.9%

注:実際の普及率よりも値が低く出る(算出方法(2)参照)

参考)フレッツ光ネクスト以外のネットワークのIPv6普及率

	KDDI AUひかり	CTCコミュファ光
2012.12	55%	24%
2013.03	61%	29%
2013.06	63%	36%
2013.09	65%	40%
2013.12	66%	44%
2014.03	67%	48%
2014.06	68%	53%
2014.09	99%	58%

アクセス網IPv6サービス導入検討SWG

- IPv6普及に関する最新情報の共有
  - (1)OCN：7月30日より一部都道府県にてひかり電話ルーターでのインターネット(IPv6 PPPoE)接続への対応を開始
    詳細は http://www.ntt.com/release/monthNEWS/detail/20140725_2.html
  - (2)So-net：7月より順次ひかり電話ルーターからのIPv6インターネット接続を標準で対応
    詳細は　http://www.so-net.ne.jp/option/others/ipv6/
  - (3)BBIX：2012年8月よりIPv6 IPoE+IPv4ハイブリッドサービスを提供
  - (4)インターネットマルチフィード：transixサービス IPv4インターネット接続オプションサービス
    http://www.mfeed.ad.jp/press/2014/20141001-1.html
  - (5)韓国のSK Telecom：IPv6を提供開始した
    http://www.whowired.com/news/articleView.html?idxno=404401
  - 最新情報の共有は議事録の公開で広く一般向けにも行っていく

IPv4枯渇に係るインターネット新技術導入にむけた検討WG

- IPv4アドレス共有技術に関する技術課題の検討を実施
  - 今年度検討する新たな課題（10/17）
    - CGNによるDNSキャッシュポイゾニング対策弱体化への対応
    - IPv4アドレス共有時の送信者特定（ポートロギングの必要性）

IPv4枯渇に係るインターネット新技術導入にむけた検討WG

- CGNによるDNSキャッシュポイゾニング対策弱体化への対応
  - DNSキャッシュポイゾニング対策としてSource port randomization（キャッシュサーバから権威サーバへ問い合わせを広範囲なポートからランダムに選択）がある
  - CGN等で例えば65536ポートのうち1024ポートを1ユーザに割り当てると、ランダマイズのレンジが64分の1に、逆に1アドレスにDNSキャッシュが存在する可能性は64倍に

    → 攻撃可能性は4096（64x64）倍に

  - 商用のCGNの対策の有無／どのような対策が可能か／携帯のDNSは大丈夫か

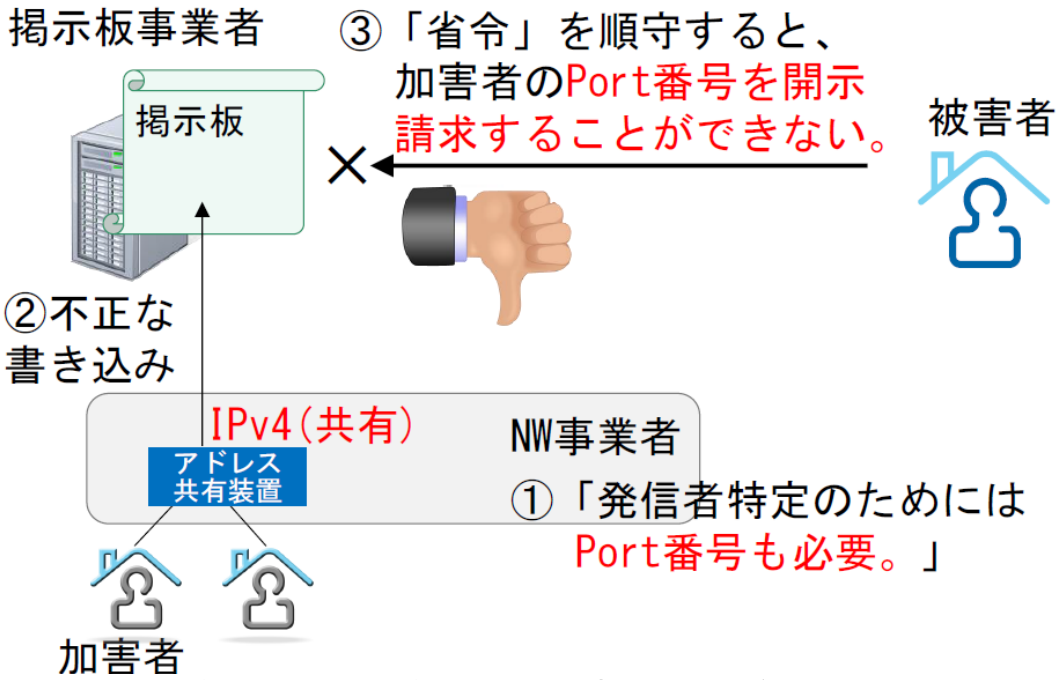
    → StarPORTE設備を用いて検証予定

    来年の3月までにまとめる予定

IPv4枯渇に係るインターネット新技術導入にむけた検討WG

- IPv4アドレス共有時の送信者特定（ポートロギングの必要性）
  - 1アドレスを復数のエンドユーザがシェアするので、サーバ事業者（サービス事業者）はポート番号まで把握する必要が出る

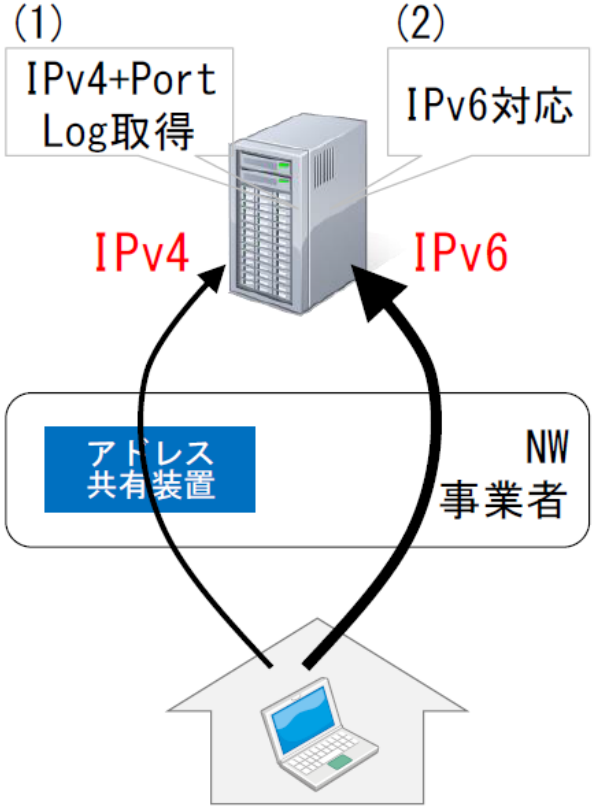
↓　しかし



出典：IPv4アドレス共有時の送信者特定～省令とサーバ運用～　JPNE　中川あきら氏

IPv4枯渇に係るインターネット新技術導入にむけた検討WG

- IPv4アドレス共有時の送信者特定（ポートロギングの必要性）
  - 今後必要となるアクション



サーバ・F/W等の管理者は点検が必要ではないか。

(1) Port番号もLog取得できているか、又は取得するべきかどうか。

(2) IPアドレスのみで送信者を特定するために、IPv6対応して、IPv6側に多くのトラフィックを逃すべきかどうか。(*)

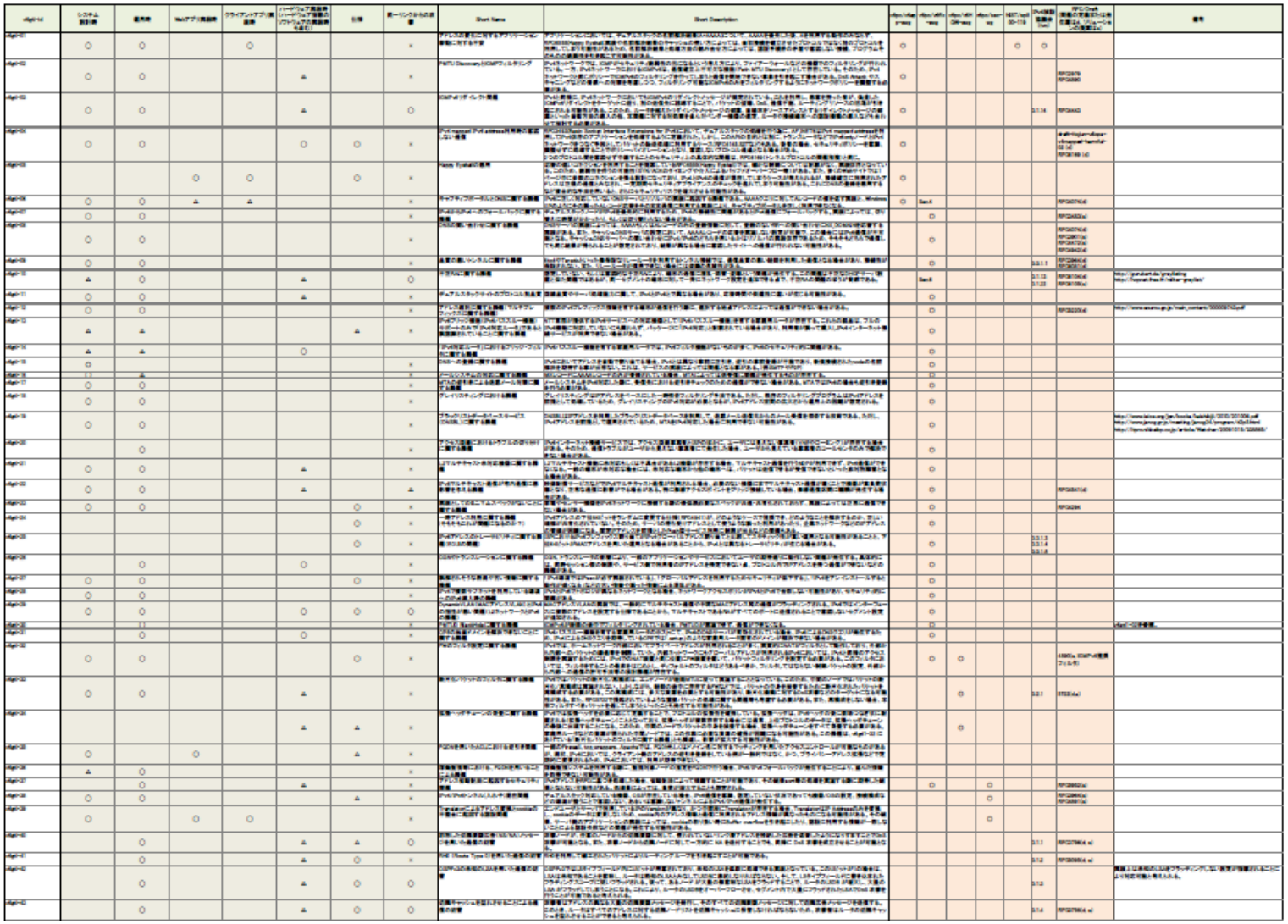
(*) IPv4アドレスを共有している各国のNW事業者はIPv6対応している確率が高い！

出典：IPv4アドレス共有時の送信者特定～省令とサーバ運用～　JPNE　中川あきら氏

セキュリティWG

- 2014.04.16 IPv6対応セキュリティ課題整理「IPv6 Security List of Considerations（6SLoC）（Ver1.0-cfc）」を公開
  - 比較対象
    - IPv6普及・高度化推進協議会／アプリケーションのIPv6対応検討SWG
    - IPv6普及・高度化推進協議会／IPv6導入に起因する問題検討SWG
    - IPv6普及・高度化推進協議会／IPv6家庭用ルータSWG
    - IPv6普及・高度化推進協議会／セキュリティWG
    - NIST／SP800-119
    - IPv6検証協議会
    - RFC/Draft
  - 課題として関連する場面
    - システム設計時
    - 運用時
    - Webアプリ実装時
    - クライアントアプリ実装時
    - ハードウェア実装時
    - 仕様
    - （同一リンクからの攻撃）

セキュリティWG



サーティフィケーションWG