

事前資料

v1.02

共存/移行技術と P2P対戦ゲームの相性

2012/7/5

株式会社コナミデジタルエンタテインメント 佐藤 良

事前資料のお品書き

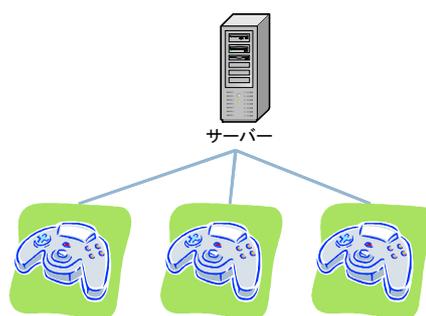
1

1. オンラインゲームの通信方式
2. P2P対戦ゲームの通信方式
3. 共存/移行技術との相性
4. RFC 4787
5. WIDE合宿での検証

オンラインゲームの通信方式

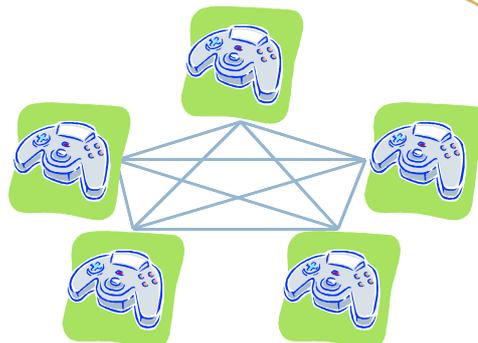
… クライアント/サーバ型

- ☒ ソーシャルコンテンツ、MMORPGなどで利用される基本的な構成
- ☒ よくある3-tierシステム



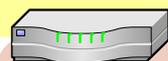
… P2P型

- ☒ 低遅延を必要とする対戦ゲームなどで利用される構成
 - ☒ IP電話と似たシステム
- ☆こちらについて取り上げます



P2P対戦ゲームの登場人物

グローバルIPアドレス

STUN
サーバロビー
サーバ

BBルータ



BBルータ



プライベートIPアドレス

P2P対戦ゲームのフロー

6

1. NAT/Firewall
特性調査

2. マッチメイキング

3. P2P通信開始

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

NAT/Firewall特性調査

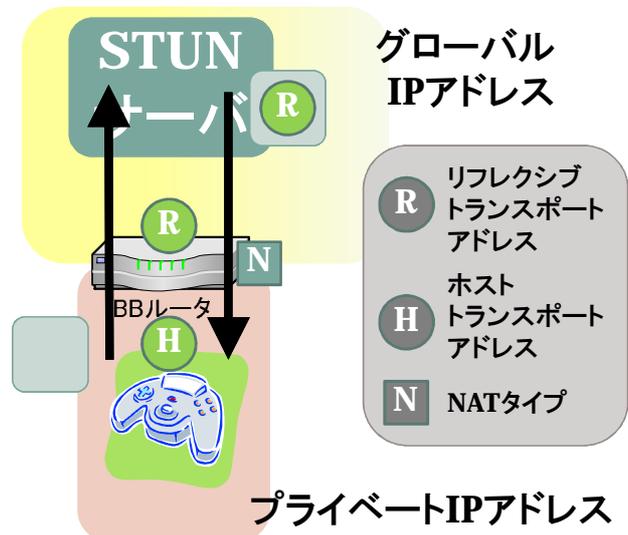
7

.. 大前提

- ✧ P2P対戦ゲームの通信にはUDPを使用する

.. STUNプロトコルで調査

- ✧ リフレクシブトランスポートアドレスの調査
- ✧ NATタイプ(マッピング/フィルタリング特性)をクライアント側で判定

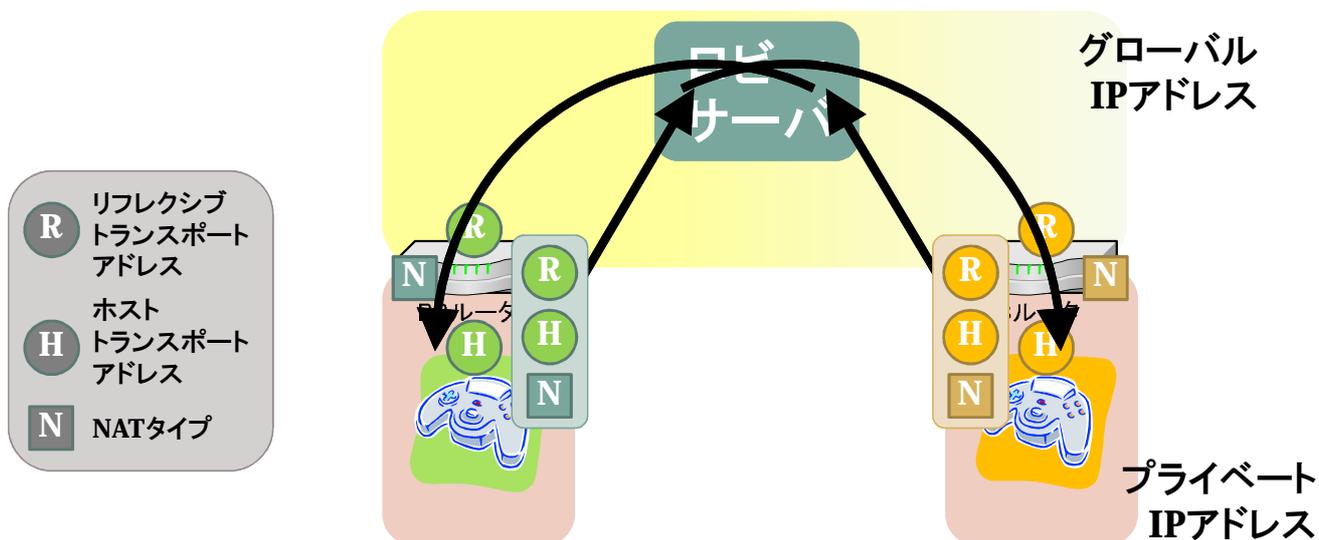


©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

マッチメイキング

8

- ロビーサーバを介して、お互いのアドレス情報を交換する

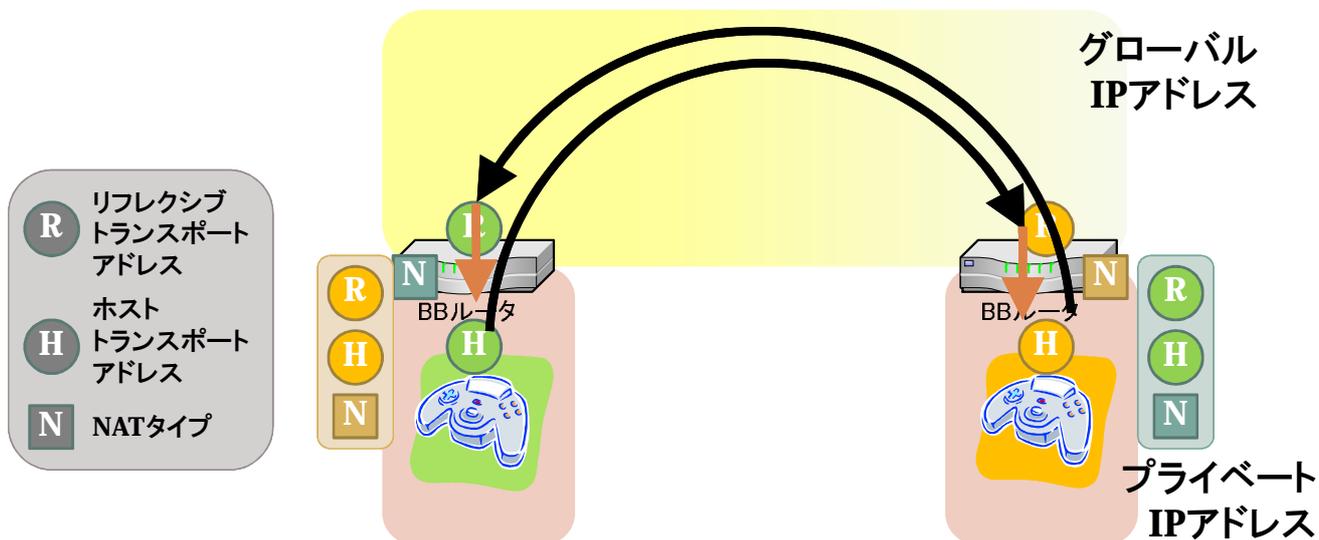


©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

P2P通信開始

9

- 相手のリフレクシブトランスポートアドレスに送信すると、内側に届く

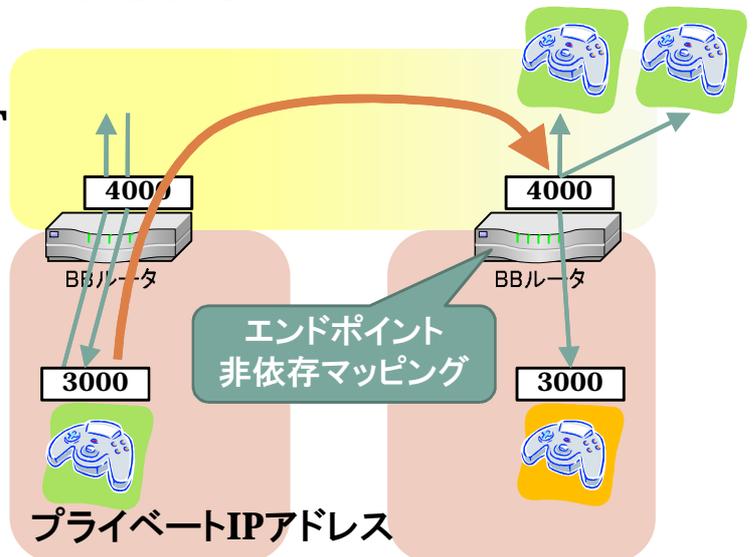


©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

NAT越えできるケース： エンドポイント非依存マッピング

10

- 同一送信元ポートからの通信で、外側ポート番号が相手によらず同一となるタイプ
- EIMと略す
- 旧呼称：コーンNAT



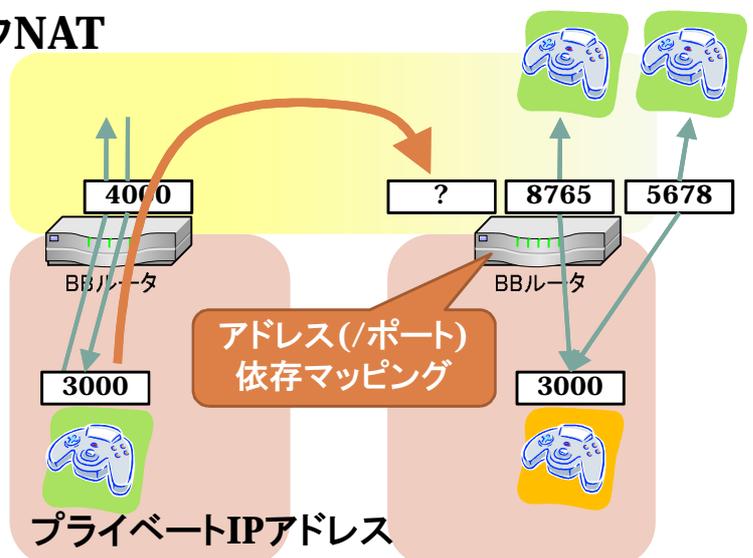
©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

NAT越えしにくいケース①： アドレス(/ポート)依存マッピング

11

- 通信相手によって外側ポート番号が変わるタイプ
- A(P)DMと略す
- 旧呼称：シンメトリックNAT

- 対A(P)DMだと、受信するまで、送信先が決められない
- A(P)DM対A(P)DMでは、お互い送信先が定まらないので、基本的にP2P通信不可

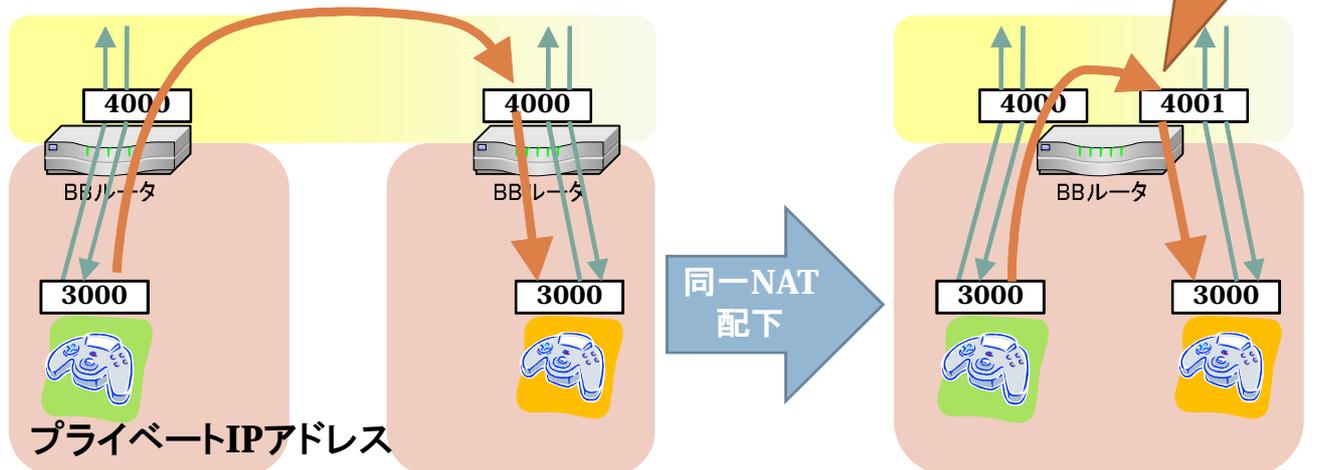


©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

NAT越えしにくいケース②: ヘアピン

12

- … 同一NAT配下でマッチメイクすると起こる
- … **ヘアピン出来ないBBルータが多い**
 - ☒ ローカルIPで通信するようにすれば良い

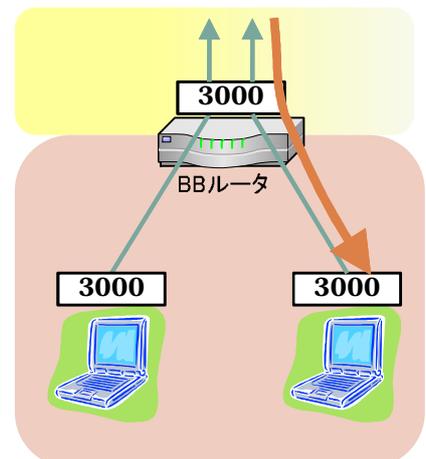


©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

NAT越えしにくいケース③: ポート多重

13

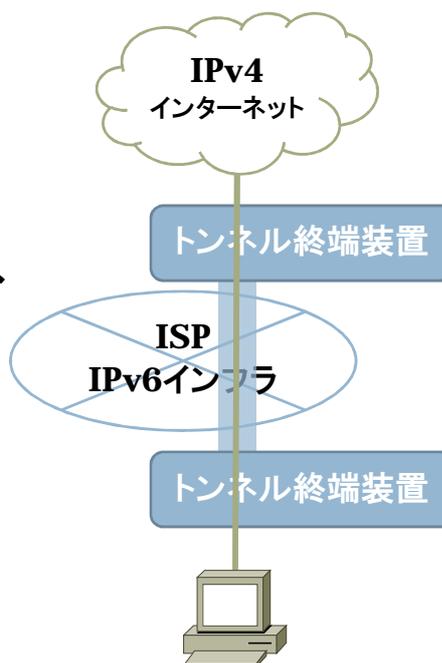
- … 内側・外側に同じポート番号を割り当てるタイプ
- … 最後に送信した方にレスポンスを届ける
- … ポート多重では、同一NAT配下で2台以上でP2P通信不可
- … 家庭ならまだしも、マンションやISPでこのNAT挙動を提供してはならない！



©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

IPv6・IPv4共存/移行技術

- … IPv4を提供する方式
 - ☒ プロトコル変換
 - ☒ トンネル(カプセル化)
- … これらを行う過程で、**IPv4 NAT**したり、**フィルタ**されたり、**フラグメントの取り扱いが不十分**だったりする**実装**や**コンフィギュレーション**がある
- … **P2P対戦ゲームが動作するためには、RFC 4787に準拠**していれば良い



RFC 4787

- … NATのユニキャストUDPに関する挙動の要件
- … NATの特性モデルが定義されている
- … 要件が14項目ある

RFC 4787のNAT特性モデル

18

マッピング特性

マッピング生成規則

- 通信相手に依らず同一
- アドレス依存
- アドレス/ポート依存

マッピング有効時間

マッピングタイマー

リフレッシュ方向

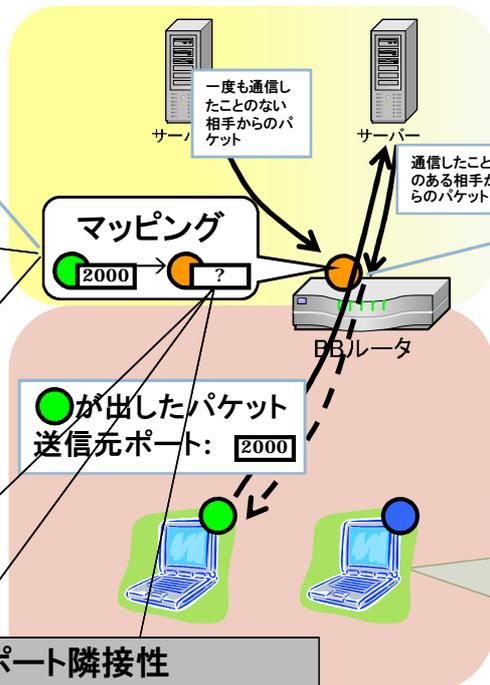
- 外向き
- 内向き
- どちらでも

ポート割り当て規則

- ポート番号維持
- ポート番号多重
- ポート番号維持無し

ポートパリティ

ポート隣接性



フィルタリング特性

- 通信相手に依らず通過
- アドレス依存
- アドレス/ポート依存

NAT配下に複数の端末がある場合、マッピング特性はより複雑になる

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

RFC 4787の要件(1/6)

19

- .. **REQ-1: NATは、“エンドポイント非依存マッピング”の挙動でなければならない(MUST)。**
- .. **REQ-2: NATは“ペア”の“IPアドレスプーリング”の挙動を持つことが推奨される(RECOMMENDED)。**この要件が、IPアドレスプーリングをサポートしないNATsに適用できないことに注意すること。
- .. **REQ-3: NATは“ポート多重”の“ポート割り当て”の挙動があってはならない(MUST NOT)。**
 - ✧ ホストの送信元ポートが範囲0~1023であったなら、NATの送信元ポートは同じ範囲であることが推奨される(RECOMMENDED)。ホストの送信元ポートが範囲1024~65535であったなら、NATの送信元ポートはその範囲にあることが推奨される(RECOMMENDED)。

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

RFC 4787の要件(2/6)

20

- … REQ-4: NATは“ポートパリティ維持”に“Yes”の挙動を持つことが推奨される(RECOMMENDED)。
- … REQ-5: REQ-5aを適用しない場合、NAT UDPマッピングタイマーは、2分未満で期限が切れてはならない(MUST NOT)。
 - a. ウェルノウンポート範囲(ポート0~1023)の特定の宛先ポートに関して、NATはその特定のポート上で動作しているIANAに登録されたアプリケーションに特有のより短いUDPマッピングタイマーであってもよい(MAY)。
 - b. NAT UDPマッピングタイマー値を設定可能にしてもよい(MAY)。
 - c. NAT UDPマッピングタイマーは5分以上のデフォルト値が推奨される(RECOMMENDED)。

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

RFC 4787の要件(3/6)

21

- … REQ-6: NATマッピングリフレッシュ方向は、“NAT外向きリフレッシュの挙動”に“True”を持たなければならない(MUST)。
 - a. NATマッピングリフレッシュ方向は、“NAT内向きリフレッシュの挙動”に“True”を持ってもよい(MAY)。
- … REQ-7: 外側IPインタフェースを動的に設定することができるNAT装置は、(1) 外側ネットワークと衝突しないIPアドレス群を内側ネットワークが使用することを自動的に保証する、もしくは、(2) IPアドレス群が内側ネットワークと数値的に衝突する全ての内側ノードと全ての外側ノード間でトラフィックを変換・転送することができる、のいずれかでなければならない(MUST)。

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

RFC 4787の要件(4/6)

22

- .. REQ-8: アプリケーション透過性が最も重要であれば、NATは“エンドポイント非依存フィルタリング”の挙動であることが推奨される(RECOMMENDED)。より厳しいフィルタリングの挙動が最も重要であれば、NATは“アドレス依存フィルタリング”の挙動であることが推奨される(RECOMMENDED)。
 - a. フィルタリングの挙動は、NATの管理者が設定可能なオプションであってもよい(MAY)。
- .. REQ-9: NATは“ヘアピンング”をサポートしなければならない(MUST)。
 - a. NATのヘアピンングの挙動は、“外側送信元IPアドレス /ポート”でなければならない(MUST)。

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

RFC 4787の要件(5/6)

23

- .. REQ-10: UNSAFのNAT越えメカニズムとの干渉を排除するためとUDP通信の完全性保護を出来るようにするために、UDPベースプロトコルのNAT ALGsを切る必要がある(SHOULD)。ALGを定義する将来のスタンダードトラック仕様書は、それらが規定値を定めるALGsを推薦するためにこれを更新することができる。
 - ❖ NATがALGsを含んでいるなら、NATの管理者が各ALGを別々に有効、無効に出来るようにすることが推奨される(RECOMMENDED)。
- .. REQ-11: NATは一意に定まる挙動を持たなければならない(MUST)。すなわち、それはどの時点でも、あるいはどんな特定の条件下でも、NAT変換やフィルタリングの挙動を変えてはならない(MUST NOT)。
- .. REQ-12: どんな種類のICMPメッセージを受け取っても、NATマッピングを消去してはならない(MUST NOT)。
 - ❖ NATのデフォルト設定は、それらの送信元IPアドレスに基づいてICMPメッセージをフィルタしないほうがよい(SHOULD NOT)。
 - ❖ NATがICMP Destination Unreachableメッセージをサポートすることを推奨する(RECOMMENDED)。

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

RFC 4787の要件(6/6)

24

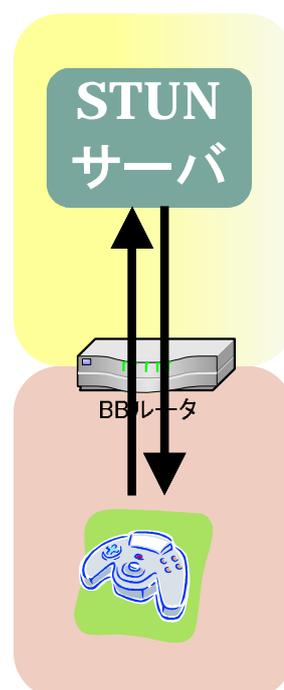
- .. REQ-13: 内側IPアドレスで受信したパケットがDF=1だったならば、NATは、ホストへICMPメッセージの“フラグメント化が必要だったが、DFがセットされている”を返送しなければならない(MUST).
 - a. パケットがDF=0であるならば、NATはパケットをフラグメント化し
なければならない(MUST)、順番にフラグメントを送る必要がある
(SHOULD)。
- .. REQ-14: NATは、正しい順序とばらばらの順序のフラグメントを受信することをサポートしなければならない(MUST)、つまり、“非順序フラグメントを受信する”の挙動を持たなければならない(MUST).
 - a. NATの非順序フラグメント処理メカニズムは、フラグメント化ベースのDoS攻撃が、順序が正しくフラグメント化していないIPパケットを処理するNATの能力を落とさないように、設計しなければならない(MUST)。

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

RFC 4787準拠の検証方法

25

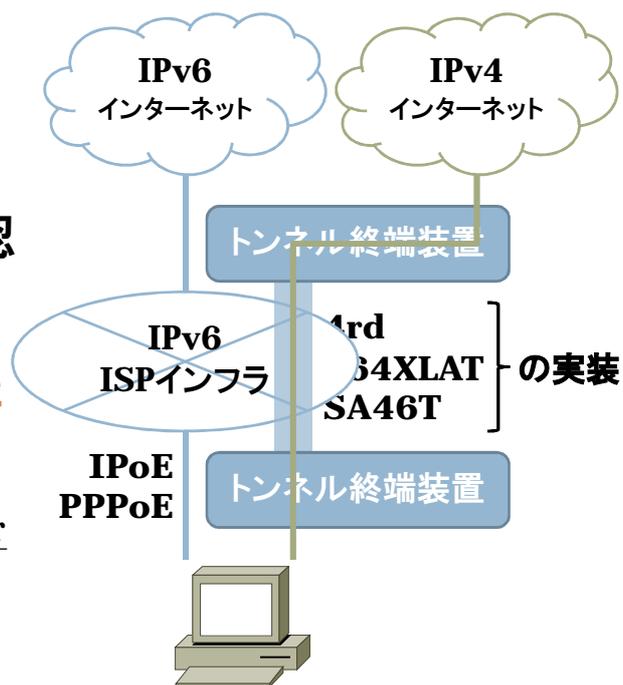
- .. STUN(RFC 5389, 5780)を使用する
- .. 検証できること
 - ☒ STUNクライアント1台
 - n REQ-1(, 2), 4, 5, 6, 8(, 9)(, 10)(, 11)
 - ☒ STUNクライアント2台(or IPアドレス2つ)
 - n REQ-2, 3, 7(2), 9
- .. 検証できないこと、しにくいこと
 - ☒ REQ-7(1), 10, 11, 12, 13, 14



©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

WIDE合宿での検証

- .. 検証内容
 - ☒ 会場のIPv6およびIPv4ネットワークで、P2P対戦ゲームが動作するか確認
- .. 結果
 - ☒ 色々と**問題が検出された**
- .. 詳細
 - ☒ <http://tools.ietf.org/html/draft-hazeyama-widencamp-ipv6-only-experience-01>



使用したクライアント: NTL

28

- .. 弊社製IPv6対応NAT越えライブラリ
 - ☒ STUNクライアント機能
 - n RFC 5389, 5780準拠+KONAMI拡張
 - ☒ TURN(パケット中継)クライアント機能
 - n RFC 5766準拠
 - ☒ UDPホールパンチング機能
 - ☒ トランスポート自動選択/フォールバック機能

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

(参考)KONAMI拡張STUN

29

- .. STUNアトリビュート0x9000
 - ☒ ソースポートを固定した場合の誤判定防止機能
 - n もう少し詳しい解説
 - n <http://www.siprop.org/ja/2.0/index.php?%B3%AB%C8%AF%2F%A5%B3%A5%DF%A5%E5%A5%CB%A5%C6%A5%A3%A1%BC%2F%CA%D9%B6%AF%B2%F1%2F2008%2F06%2F27>
 - ☒ DFビットの制御
 - ☒ レスponseパケットサイズの制御
- .. 検証できること
 - ☒ UPnPと組み合わせたの検証
 - ☒ UDPを用いたPath MTU discovery

©2012 Konami Digital Entertainment Co., Ltd. 2012/7/5

続きは会場で！

30



@ryo_sato