資料２６－１

平成24年度
IPv4アドレスの枯渇に伴う情報セキュリティ等の課題への対応に関する実証実験の請負　結果報告
（IPv4アドレス共有技術導入に係る諸課題とその対策）

NTTコミュニケーションズ株式会社
先端IPアーキテクチャセンタ
宮川　晋
2013年7月1日

目的と概要

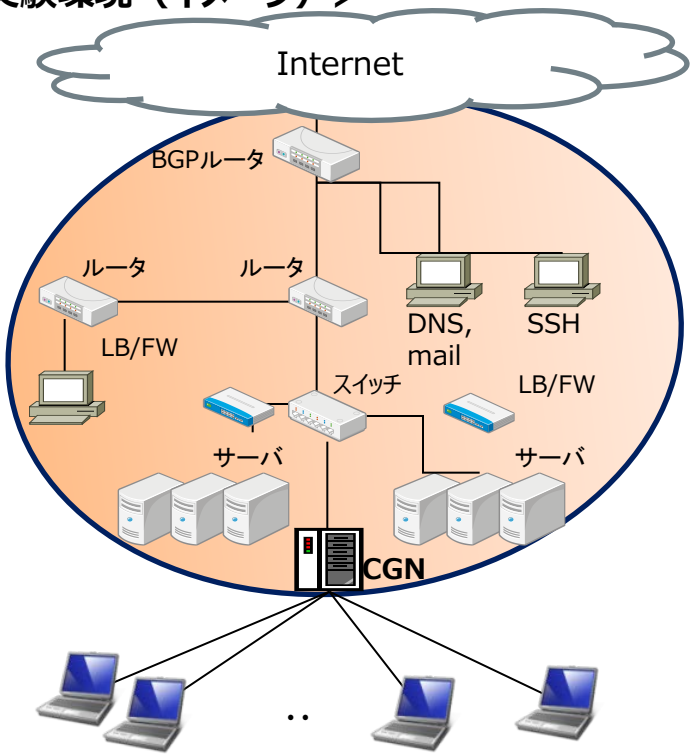
実証実験の背景・課題

■アドレス需要が旺盛な事業者は、1年から2年分程度のIPv4アドレス在庫しか確保していないと言われ、IPv4の後継規格であるIPv6の導入を急ぐとともに、IPv4アドレスの共有環境を検討せざるを得ない状況に直面している。

■IPv4アドレスの共有環境に関しては、運用、情報セキュリティ対策等に係るノウハウが十分に蓄積・共有されておらず、これまでの情報セキュリティ対策が機能しなくなる等の問題や、アプリケーション等に予期しない問題を引き起こすおそれがあることが指摘されている。

IPv4アドレス共有技術 ⇒ **CGN（Career Grade Nat）：一つのグローバルIPv4アドレスを複数のユーザで共有する技術**

＜実証実験環境（イメージ）＞



＜調査・実証実験内容＞

(1) アドレス共有技術の導入における情報セキュリティ確保に係る課題への対処

(2) アドレス共有技術の導入におけるログ情報の取得・管理に係る課題への対処

(3) アドレス共有技術によるセッション数制限の最適化及び新技術（Webソケット）導入の効果

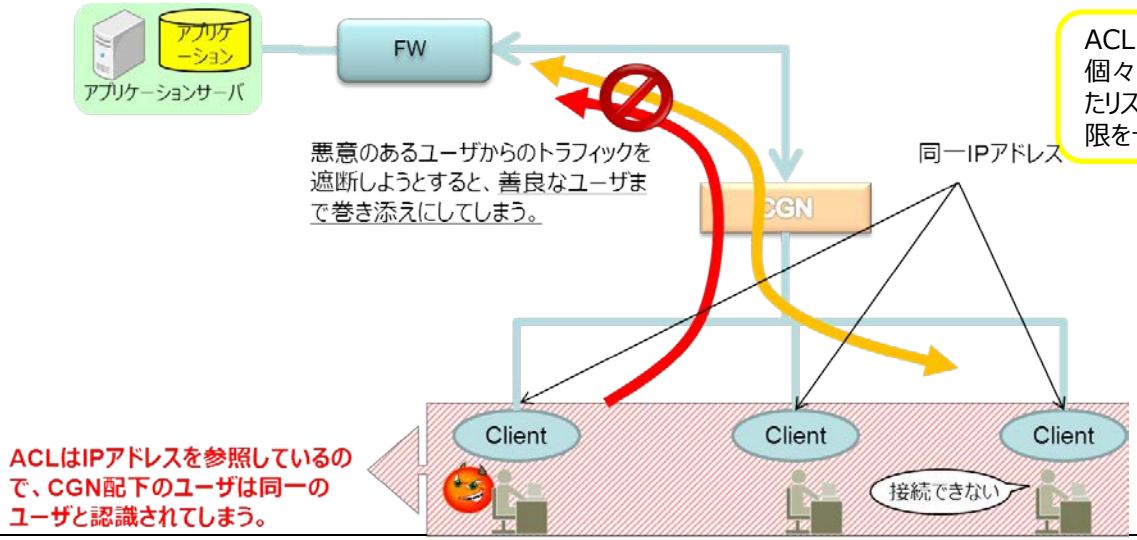
(4) アドレス共有技術（CGN）の導入範囲（配置箇所、数量等）の最適化

(5) アドレス共有技術の導入におけるアプリケーションへの影響への対処

結果報告　(1) アドレス共有技術の導入における情報セキュリティ確保に係る課題への対処

課題(1)　アドレス共有技術の導入における情報セキュリティ確保

一つのグローバルIPv4アドレスを共有している複数ユーザのうちの一人が攻撃を仕掛けた場合、そのIPアドレスからの通信を遮断すると、善良なユーザまで巻き添えにしてしまうため、結果としてACL利用による情報セキュリティ対策ができなくなるという問題がある。



ACL（Access Control List）：アクセス制御リスト
個々のネットワーク利用者が持つアクセス権限等を列挙したリスト。ネットワーク上に存在する機器や情報の利用権限を一元管理するために導入される

実証内容

CGN配下のユーザに**ホストID**[*]という識別子を付与することで、ユーザごとのアクセス制御が可能となるかの検証を実施。

[*] クライアントの識別子。CGNからインターネットに向かう通信上において本識別子を付与して利用する。
本検証用に、試作のホストID処理機能及びFW機能を持ったCGN（セキュリティ強化版CGN）を用意し、検証を実施。

結果・考察

CGNにおいてホストIDを付与することにより、インターネットに存在するサーバにおいて、**ユーザの判別が可能**となることが証明された。
これにより、悪意のあるユーザと善良なユーザを区別でき、悪意のあるユーザのみの通信を遮断するなどの情報セキュリティ対策を講じることが可能となる。

結果報告　(2) アドレス共有技術の導入におけるログ情報の取得・管理に係る課題への対処

課題(2) アドレス共有技術の導入におけるログ情報の取得・管理（ログ管理コストの増大）

従来、CGNで取得・管理すべきログはIPアドレスのみであったが、ホストIDによるセキュリティ対策を講じた場合、IPアドレス以外にも、ホストIDやソースポート番号のログを取得・管理することが必要となるため、ログ情報が膨大となる。

→ 事業者は取得・管理すべきログ情報の増大により、**ログ情報の取得及び管理に多大なコストがかかることが懸念**されている。

実証内容

NATテーブルの割当・消去、データ通信の開始・終了、送信先アドレス・ポート情報といったログ情報について、実証により具体的なデータ量を把握するとともに、不必要なログの削減やログ形式の工夫によるログのデータ量の削減効果について検証を実施。

結果・考察

すべてのログ情報を取得する場合のログデータ量を100%としたときに、削減手法を利用したケース毎の割合を、以下の表に示す。

（１）NATテーブルの割当・消去
（２）データ通信の開始・終了
（３）送信先アドレス・ポート情報

＜参考＞
ユーザ規模1.6万人のうち25%のユーザが400セッションの通信を”1回”行ったと仮定した際の総量は720Mbpsとなる。
（※(注)本検証下における結果）

ログ対象・形式	説明	Ratio
Full Logging	全てのログを取得する場合	100%
Case1：Compact Option	IPアドレス・ポート番号の形式を16進数表記にするなど、表記上を工夫	78%
Case2：Remove include-destination	(3)送信先アドレス・ポート情報を取得しない	96%
Case3：Remove Log-session	(2)データ通信の開始・終了情報を取得しない	44%
Case1＋Case2＋Case3	上記の3つの手法を組み合わせた場合	32%

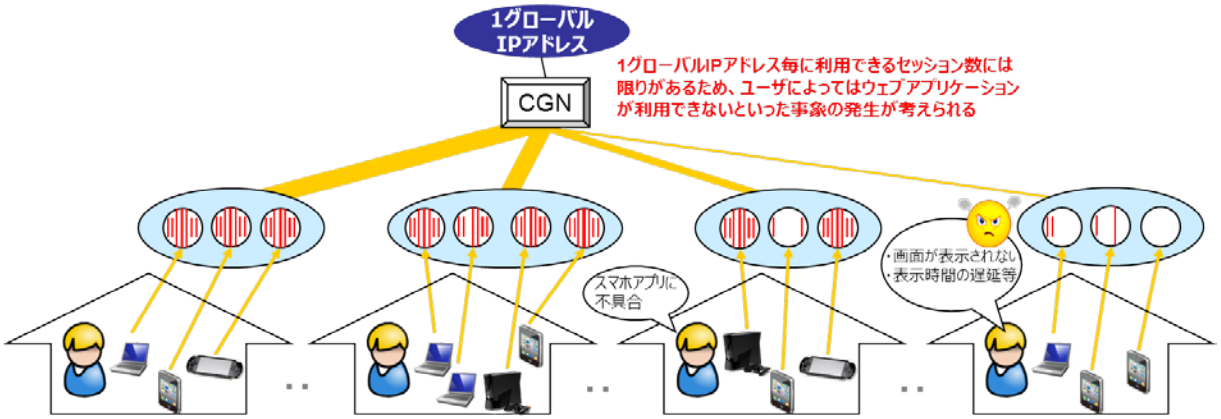
32%に削減する手法を確立

上記より、個別のユーザを識別するためのログデータ量を最大32%に削減することが可能となった。

結果報告　(3) アドレス共有技術によるセッション数制限の最適化及び新技術（Webソケット）導入の効果

課題(3) アドレス共有技術によるセッション数制限の最適化及び新技術（Webソケット）導入の効果

1グローバルIPアドレス当たり、張れるTCPセッション数が限られているから、ISP等において同時セッション数を制限する等の対策が行われることが想定される。



実証内容

・1ユーザ当たりに**必要なセッション数**について検証を実施。
・また、セッション数の削減に効果があると思われる**Webソケットの有効性**について検証を実施。

Webソケットとは
サーバとクライアント間で、複数のセッションを張ることなく、
１セッションで双方向の高速通信を可能とする技術

結果・考察

検証結果より、1ユーザ当たりに必要なセッション数は**1000程度**であることが判明した。

	Web mail	映像/テレビ系	ポータル	EC	blog	検索	Online game
平均TCPセッション数	65	83	36	45	61	8	95

	Online Banking	Twitter	Facebook	iTunes	Cloud	IM	VoIP
平均TCPセッション数	20	33	51	20	29	66	18

また、**Webソケットを利用することにより、TCPセッション数の削減に効果があることが明らかとなった（TCPセッション数＝1）。**
しかし、遅延やロス発生等の環境によってパフォーマンスが著しく低下する（末尾参考に検証結果の表を記載）ことが判明したため、サービス性の向上を図るため更なる検証が必要である。

NTT Communications　Global ICT Partner
Innovative. Reliable. Seamless.

結果報告　(4) アドレス共有技術（CGN）の導入範囲（配置箇所、数量等）の最適化

課題(4) アドレス共有技術（CGN）の導入範囲（配置箇所、数量等）の最適化

アドレス共有技術（CGN）の導入にあたっては、コスト等を勘案しつつ配置箇所や数量を決定する必要がある。導入可能なポイントは多岐に渡り、現在のところ有効的かつ効率的な配置場所や数量等が決まっていない。

実証内容

実証実験環境で、実際にCGNの配置を変更し、ISP規模ごとに**最適なCGNの個数や、配置**を明らかにするため検証を実施。

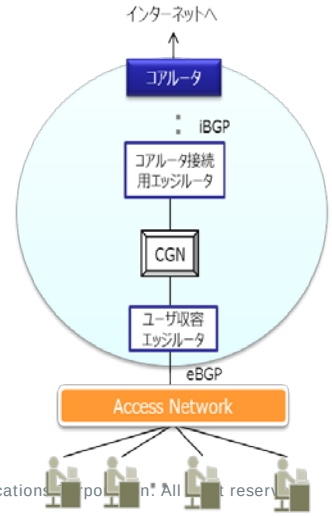
結果・考察

本検証環境では、**一般的な性能のCGNの単体性能限界値として、約16万ユーザ（同時接続セッション数：16,368,000セッション）**であることを明らかとした。ISP規模毎のCGNの個数（Min）は以下の表に示すとおりである。また、検証結果より得られた推奨構成もあわせて示す。

ISP規模	検証想定数			CGN数（Min構成）
	契約者数	アクティブユーザ数	最大セッション数	
小規模ISP	10,000	2,500	1,000,000	1台
中規模ISP	100,000	25,000	10,000,000	1台
大規模ISP	1,000,000	250,000	100,000,000	7台

＜参考＞
契約者に対して
Active率：25%
同時セッション数:400
として算出

＜推奨構成＞



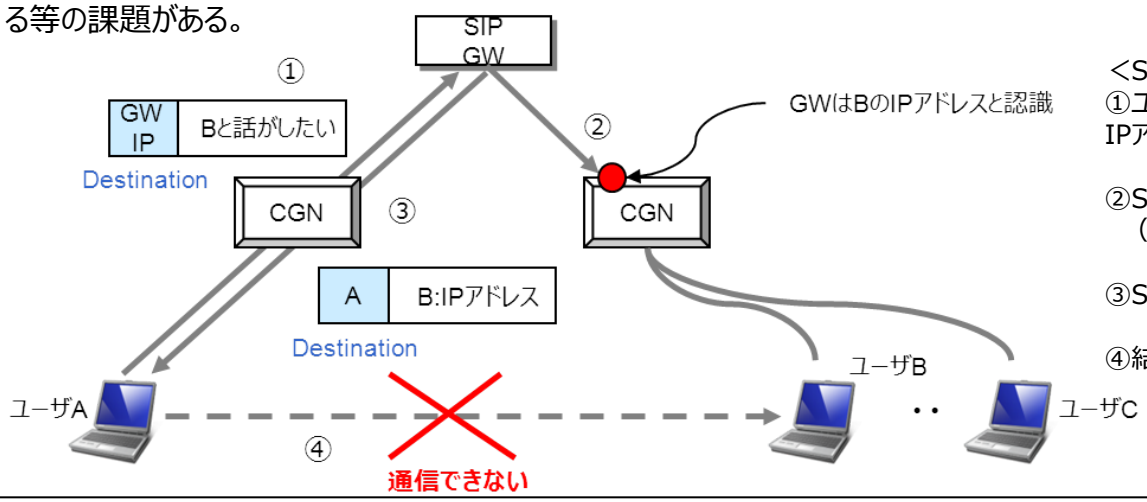
CGNはユーザ収容エッジルータとコアルータ接続用エッジルータの間に設置
また、冗長構成をとることができるよう**CGNはエッジルータ毎に設置**

・CGNでeBGPを動作させる必要はなし
・iBGPピアを分断させることもない

結果報告　(5) アドレス共有技術の導入におけるアプリケーションへの影響への対処

課題(5) アドレス共有技術の導入におけるアプリケーションへの影響への対処

IPv4アドレス共有技術（CGN）の導入により、VPN系サービス、P2Pサービス、SIPベースのアプリケーションの提供に制限が生じるおそれがある等の課題がある。



＜SIP系サービスの場合＞
①ユーザＡはユーザBと通信を行うため、SIP GWにユーザBのIPアドレスを問い合わせる

②SIP GWはCGNのIPアドレスをユーザBのものと認識
（CGN配下には多数のユーザがぶら下がっている）

③SIP GWはユーザAに誤ったIPアドレスを通知

④結果として、ユーザAとユーザＢは通信が出来ない。

検証内容

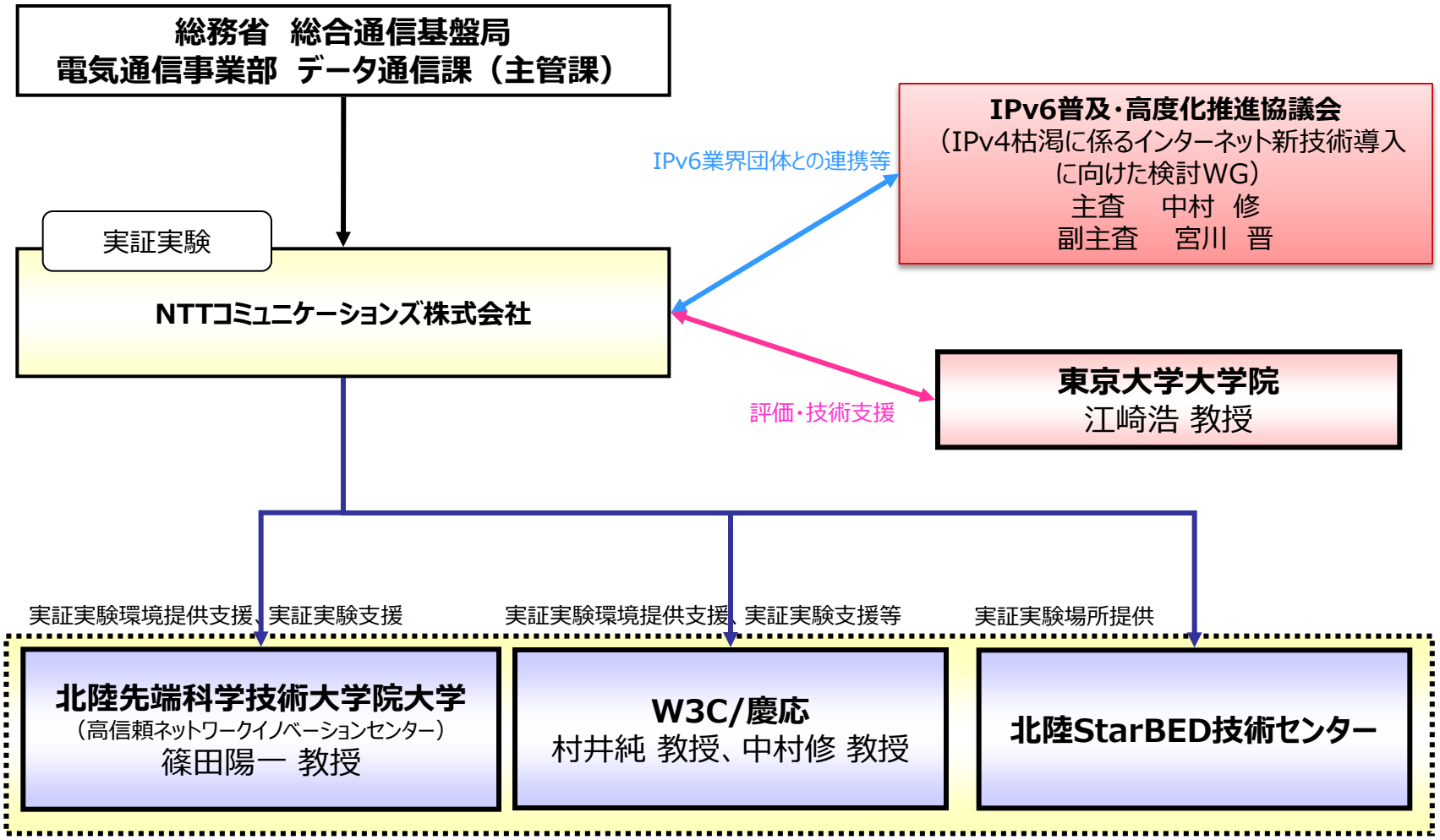
CGNを導入した本実証実験下で、STUNやTURNといった技術を利用し、SIPなど**各アプリケーションに対する有効性について検証を実施。**

結果・考察

CGN側、アプリケーション側それぞれに表に挙げた技術を実装することで、VPN系サービス、P2Pサービス、SIPベースのアプリケーションをCGNを導入した環境でも利用が可能であることを、検証より明らかとした。

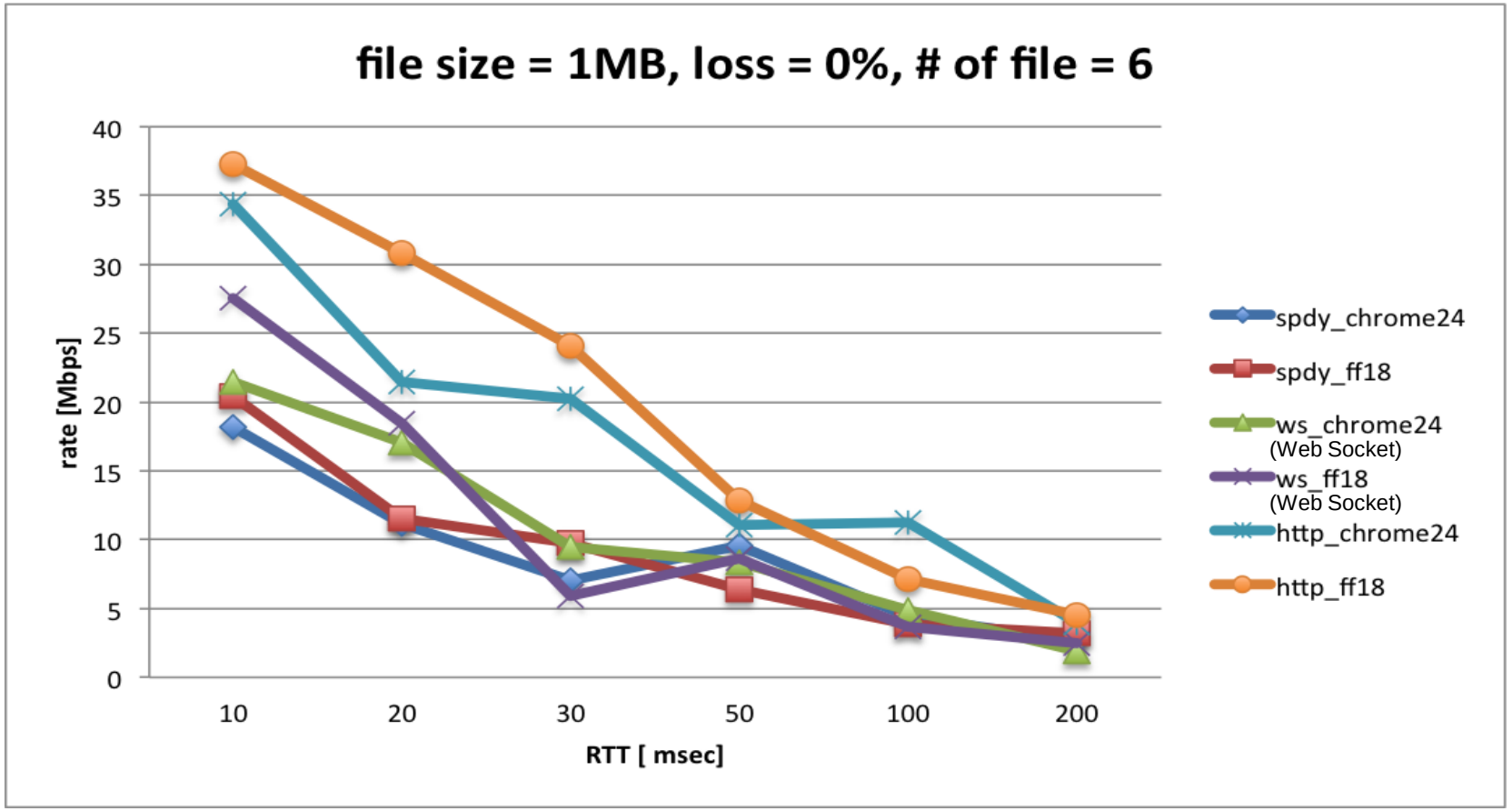
	VPN型	P2P型	SIP型
CGN側対策実装	ALG	Fullcone NAT	ALG
アプリケーション側対策実装	IPsec NATトラバーサル(UDPカプセル)	STUN/UDP hole punching TURN	TURN

（参考）実施体制



（参考）Webソケット検証

Windows7、ファイルサイズ1MB、パケットロス率1%、同時ダウンロード数6においてブラウザ及び遅延を変動させた。



SPDY：Webページの表示を高速化するためのプロトコル