WAN 二重化の有効利用

東亜建設工業株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

石倉　正英

1994 年　東亜建設工業入社
　　技術研究所・情報解析研究室
1999 年　同主任研究員
2001 年　情報システム部 社内インフラ担当
2005 年　現在 システムグループ・リーダ
　　社内インフラ・イントラ担当

■ 論文要旨 ■

当社では、災害対策の一環で、昨年、WAN 環境の二重化を図ったが、単なるバックアップ回線として眠らせておくのはもったいない、という発想から、バックアップ用の回線についても通常時はメールの送受信や、夜間の遠隔地オンライン・バックアップ・ルートとして活用し、障害（災害）時には、自動的に一方に通信を集約する仕組みを構築した。

本論では、その構成や採用した技術、利点と問題点等について述べる。

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要とネットワーク環境

当社は明治 41 年創業，大正 9 年設立の総合建設会社である．海上土木，陸上土木，浚渫・埋立，建築工事の請負などを主な事業とし，日本全国，および，東南アジアを中心とした海外にも事業進出を果たしている．

当社のネットワーク構成の概念図を図１に示す。社内の基幹サーバ群は ISP ベンダーのデータセンターにハウジングし，東京本社，全国主要都市に散らばる 11 の支店を IP-VPN によって，また，海外拠点を含めた営業所・作業所約 350 拠点をインターネット VPN、もしくは、SSL-VPN によってネットワーク接続している．

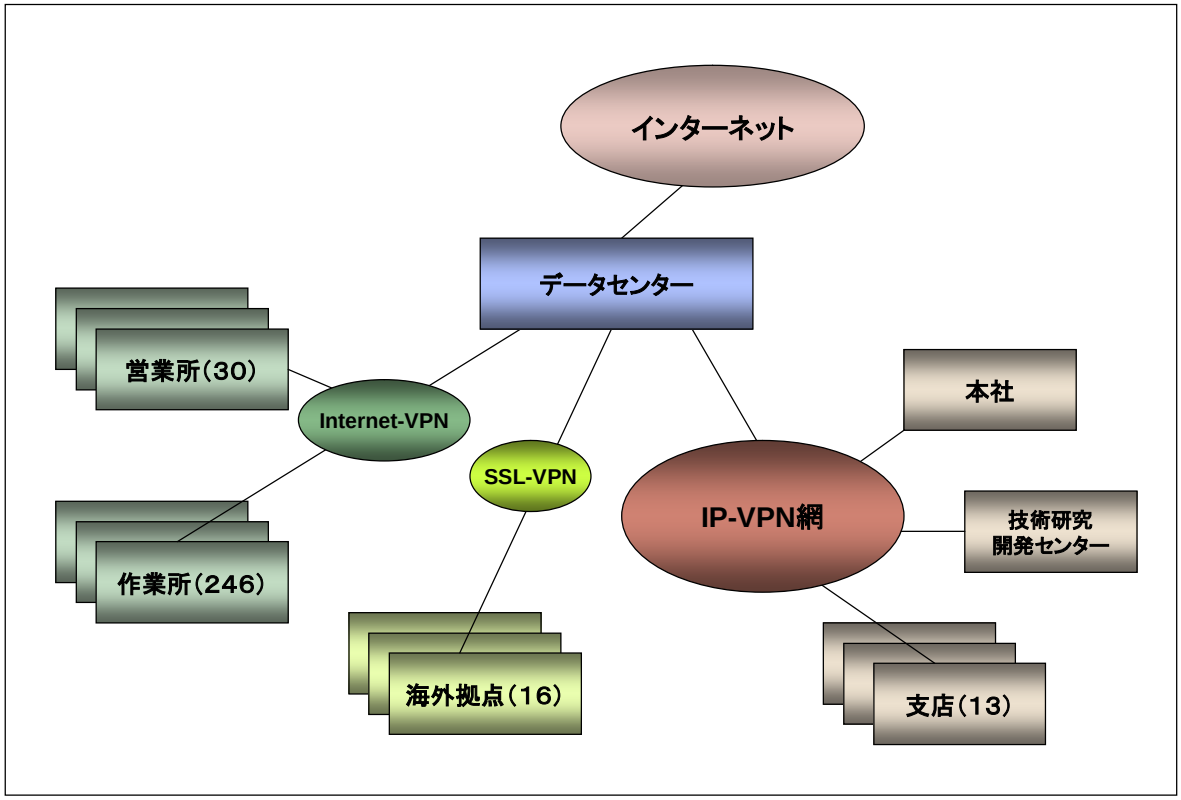


図１　ネットワーク構成概念図

１．２　背景と目的

当社では 2007 年 9 月に事業継続計画「TOA-BCP」を策定した。東京湾北部を震源とする震度 6 弱以上の地震災害を想定し、建設会社の社会的責任から、以下のような基本方針を打ち出している。

・　当社は、首都圏直下型地震など大規模災害発生時には、いつ、いかなる場合においても、社員とその家族の身体・生命・財産の安全の確保、並びに顧客及びインフラの復旧支援を最優先にします。そして、被害を軽減・回避し、経営資源の毀損を防ぐとともに、二次災害の発生防止など緊急対応の適切かつ迅速な遂行を図り、早期の復旧・事業再開に向け全力を傾注します。

情報システムについては、基本方針の中で以下の二点が明記されている。

・ 通信手段の確保
　本・支店災害対策本部間や社員・顧客等の関係者との通信手段は、インターネット、無線など複数の通信手段を確保する。
・ IT システムのバックアップ
　すべての重要データは、バックアップシステムにより二重化する。

また、関連文書の「大規模災害時における初動対応マニュアル」の中では、次のように明記されている。

・ コンピュータシステムの点検と復旧
　情報システム班（班長：情報システム部長）は、ネットワーク通信、コンピュータシステムの点検を行い、障害が確認された場合には、バックアップシステムへの切り替えやネットワークの復旧を行う。

これを受けて、ディザスタリカバリとして、以下の事項を実施している。

・ 主要サーバをデータセンターに集約
・ 主要拠点ファイルサーバを含め、主要サーバのバックアップデータをテープメディアに取得（日次、過去 5 世代）
・ バックアップサーバは用意せず、重要データのバックアップテープは月 1 で別所保管
・ 各ネットワーク機器、および、主要サーバのシステム復旧マニュアルを整備

このように、データセンターにハウジングすることによりある程度堅牢性を確保できていることと、投資コストにみあわないという理由により、遠隔地にバックアップサーバ（システム）を構築してはいないが、データの保全性という点においては、最低限のディザスタリカバリ環境を築いているといえる。

しかし、昨今の業務にはネットワーク通信が欠かせないものになっている。サーバやデータがきちんと保全されていても、ネットワーク・インフラが止まってしまっては業務継続はままならない。また、TOA-BCP基本方針の「災害時の通信手段の確保」を実現するためにも主要な通信環境の冗長化が必要とされていた。

２．従来の WAN 環境

２．１　構成

図２に従来の WAN 構成を示す。

データセンターを中心としたネットワークで、本社は 3Mbps、主要拠点については 1～2Mbps の専用回線で接続している。このように回線帯域が小さいため、インターネット通信については B フレッツ回線を各拠点に引き込み、通信を振り分けることで、WAN トラフィックを緩和させていた。

B フレッツ回線の障害時には、クライアント側で WAN 側にルートを変更することで、インターネット通信が復旧する冗長化を図っていた。

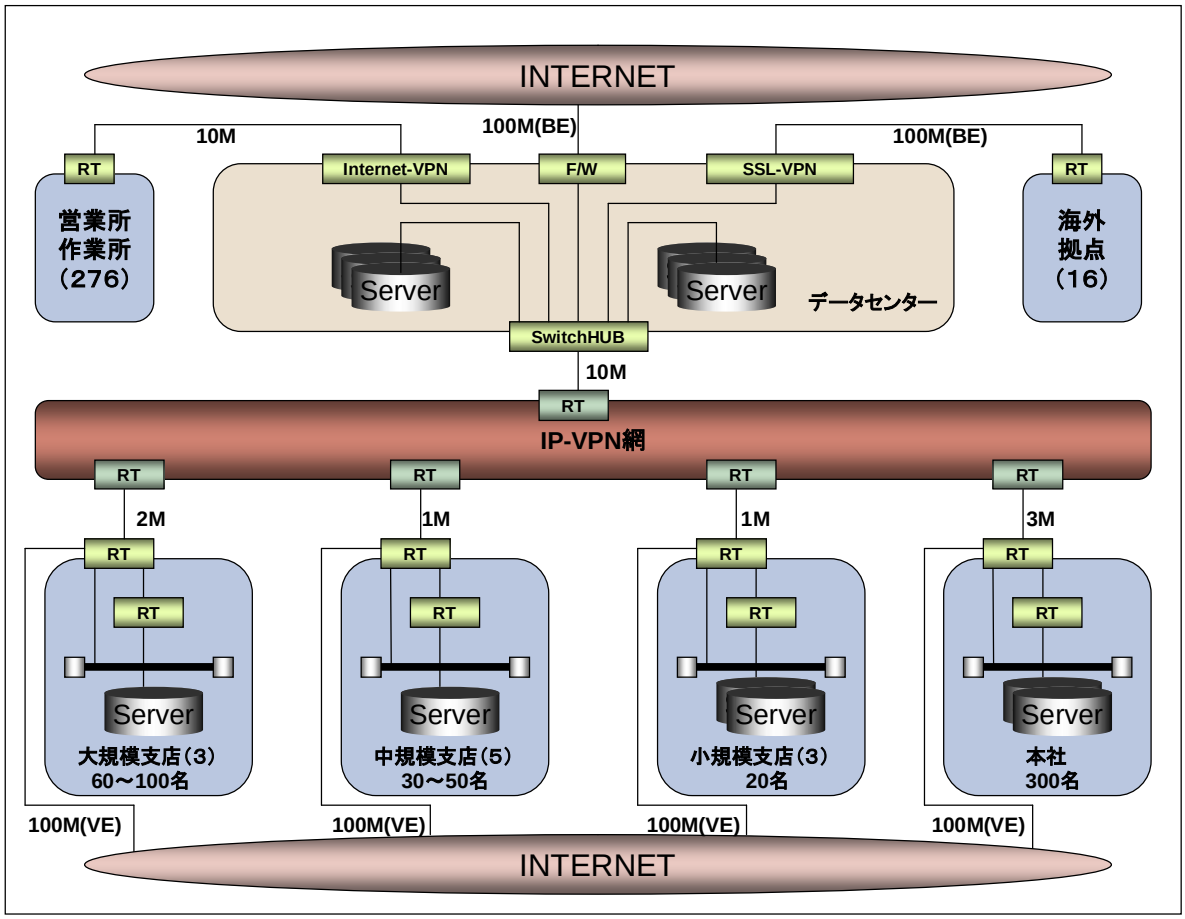


図２　従来の WAN 構成

２．２　問題点

従来の WAN 構成では、各主要拠点のインターネット通信のみ冗長化が図られていたが、クライアント PC 上のインターネット・エクスプローラの設定をユーザ側で設定変更（プロキシ設定）する必要があった。また、本来重要である WAN 側通信の回線障害については冗長化がなされていなかった。

セキュリティ面では、各拠点からのインターネット通信経路に簡易的なファイアーウォール（兼ルータ）を設置していたが、フィルタリング等の設定が甘く、かつ、メンテナンスに手数がかかっていた。

使用実感としても、インターネットのアクセス速度に比べて、WAN 回線の細さゆえに、社内通信の遅さが目立ち、ユーザの不満も大きかった。また、その割に速度保証型回線のため運用コストが高かった。

３．WAN の二重化

３．１　基本方針とスケジュール

当初、BCP の観点から WAN 冗長化の検討を開始したが、単に非常時のみ使用するバック

アップ回線を用意するだけではもったいない、という発想から、従来の WAN 構成上の問題点もこの際に改善するべく、以下のような基本方針を立てた。

- 通常時もバックアップ回線を有効利用し、WAN トラフィックを緩和する。
- 片側の網や回線、もしくは、ネットワーク機器の障害時には自動的に、もう片側に通信を移管させ、ノンストップに近い運用を実現する。その際、ユーザサイドの設定変更を伴わないようにする。
- インターネット通信におけるフィルタリング等のセキュリティを高め、統一的に管理できるようにする。
- 運用コストを現行レベルにとどめる。

このプロジェクトのスケジュールを表１に示す。当初、弊社の夏期休暇期間である 8 月中旬を切り替えターゲットと設定していたが、回線工事が間に合わない拠点等があり、一部 9 月に実施したところもあった。このように切り替え時期が拠点ごとに異なるため、旧 WAN 環境との併存に問題がないか、および、通信の振り分けの妥当性等を判断するため、7 月初旬に２つのパイロット拠点（東京・千葉）を先行して切り替え、一月程度の運用状況をモニタリングする期間を設けた。その結果、特に問題は発生せず、以降の拠点切り替えがスムーズに実施できた。

表１　WAN 二重化スケジュール

項目		4月		5月				6月				7月				8月				9月			
要件定義		■	■	■																			
基本設計					■	■																	
詳細設計							■	■	■														
機器設定										■	■		■	■	■	■							
事前テスト										■	■		■	■	■	■							
回線工事	データセンター							■															
	各拠点									■	■	■								■	■		
切り替え	データセンター										■												
	東京(パイロット)											■											
	千葉(パイロット)											■											
	北陸																■						
	大阪																■						
	中国																■						
	四国																■						
	九州																■						
	技術センター																■						
	本社																	■					
	北海道																	■					
	名古屋																				■		
	横浜																					■	
	東北																					■	
旧回線撤去																							■

３．２　構成

二重化後の物理的 WAN 構成を図３に、各拠点の回線帯域を表２に示す。

各拠点の足回りとしては、メイン回線には光の専用回線、バックアップ回線にはベストエフォート式の ADSL 回線を採用した。また、両網を Layer2 化することで、従来の運用コストとほぼ同じランニングコストを実現した。

インターネット通信も WAN を経由することで、データセンターでのフィルタリング等の一元管理を実現し、セキュリティレベルを高めた。また、全社のインターネット通信が集

約されるため、データセンターのインターネット・アクセス回線を１Gbps のベスト・エフォート型の回線に切り替えた。

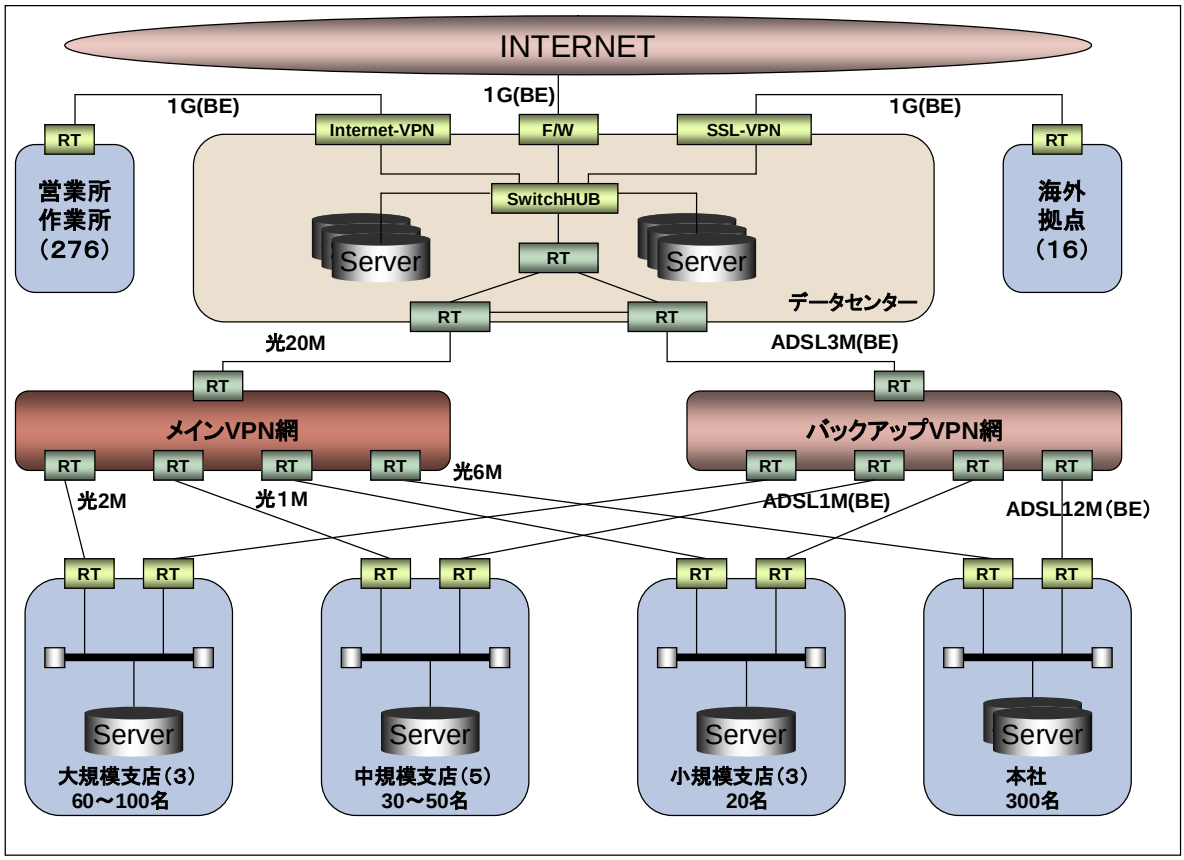


図３　二重化後の WAN 構成

表２　各拠点の回線帯域

拠点名	人数規模	メイン回線	バックアップ回線 （ベストエフォート）
本社	300	6Mbps	12Mbps（128Kbps保証）
北海道支店	30	1Mbps	1Mbps
東北支店	50	1Mbps	1Mbps
千葉支店	20	1Mbps	1Mbps
東京支店・国際事業部	100	2Mbps	1Mbps
横浜支店	60	2Mbps	1Mbps
北陸支店	20	1Mbps	1Mbps
名古屋支店	50	1Mbps	1Mbps
大阪支店	60	2Mbps	1Mbps
中国支店	50	1Mbps	1Mbps
四国支店	20	1Mbps	1Mbps
九州支店	50	1Mbps	1Mbps
データセンター		20Mbps	3Mbps

特に構成人数が多く、通信量のオーバーフローが発生していた本社についてはメイン回線を３Mbps から６Mbps に増速した。

また、各拠点のルータは既存のものを流用することでコストダウンを図った。

３．３　バックアップ回線の有効利用

通信の振り分けイメージを図４に示す。

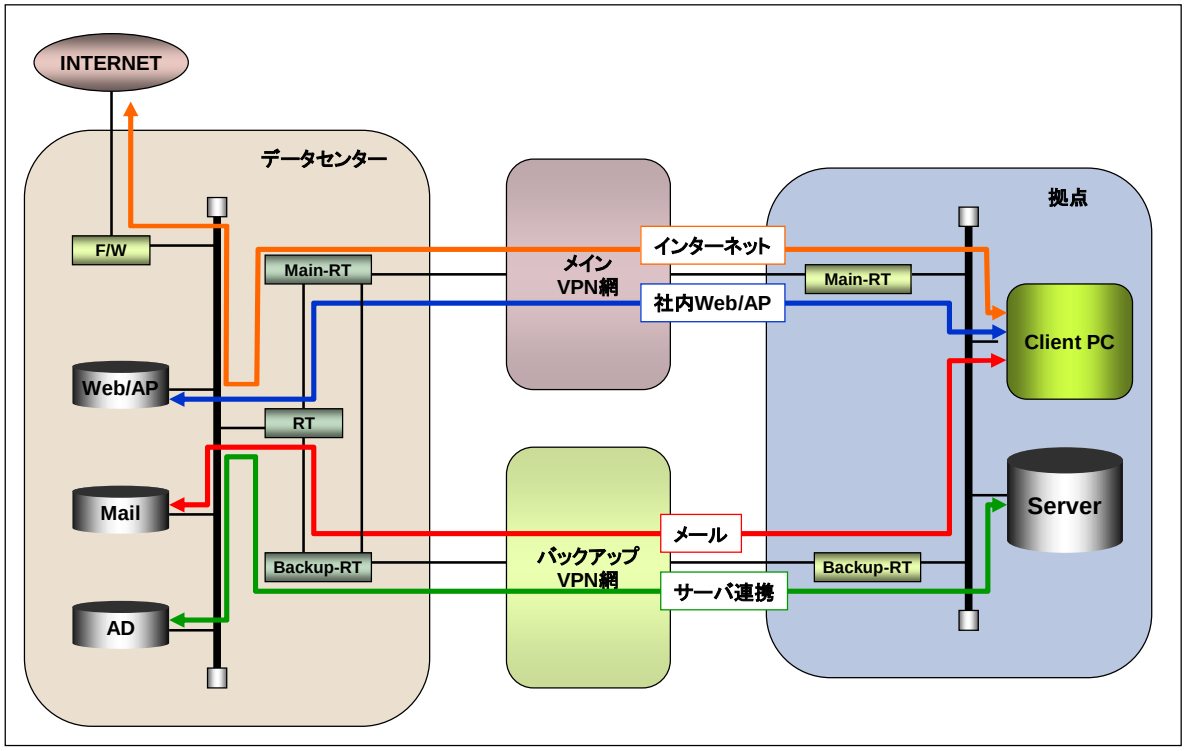


図４　通信の振り分けイメージ

通常時は、業務アプリケーションやイントラ HP、インターネット通信についてはメイン回線を使用し、メールアプリケーションとバッチ系の処理（サーバ間連携等）についてはバックアップ回線を使用するように、ポリシー・ベース・ルーティング（※１）の技術を利用して環境を構築した。このように振り分けた理由としては、ユーザの体感レスポンスの部分を重視したためである。すなわち、レスポンスタイムの早さが求められる Web インターフェースの業務アプリケーションや、社内外 HP の閲覧には早く、かつ、安定したメイン回線をあてがい、メールやサーバ間のバックグラウンドでの連携やバッチ処理等のユーザからレスポンスタイムの早さを求められない通信についてはバックアップ回線をあてがうように設計した。

また、バックアップ回線を使用して、各拠点に置かれているファイルサーバのオンライン・バックアップも実現した。オンライン・バックアップの仕組みにはマイクロソフト社の DFS（分散ファイル・システム：Distributed File System）を利用している。一回目のコピーはフル・データとなるため、小規模拠点以外はバックアップテープを搬送してベースを築き、その後の差分情報をバックアップ回線を用いて行うようにした。

※１　ポリシー・ベース・ルーティング(Policy Based Routing)

送信元アドレス、宛先アドレス、優先順位、ポート番号などの条件に基づいてトラフィックをルーティングする技術。合致するポリシーが見つからない場合、パケットはポリシー・ベース・ルーティングでは拒否され、宛先に基づいて通常通りにルーティングされる。

３．２　冗長化の仕組み

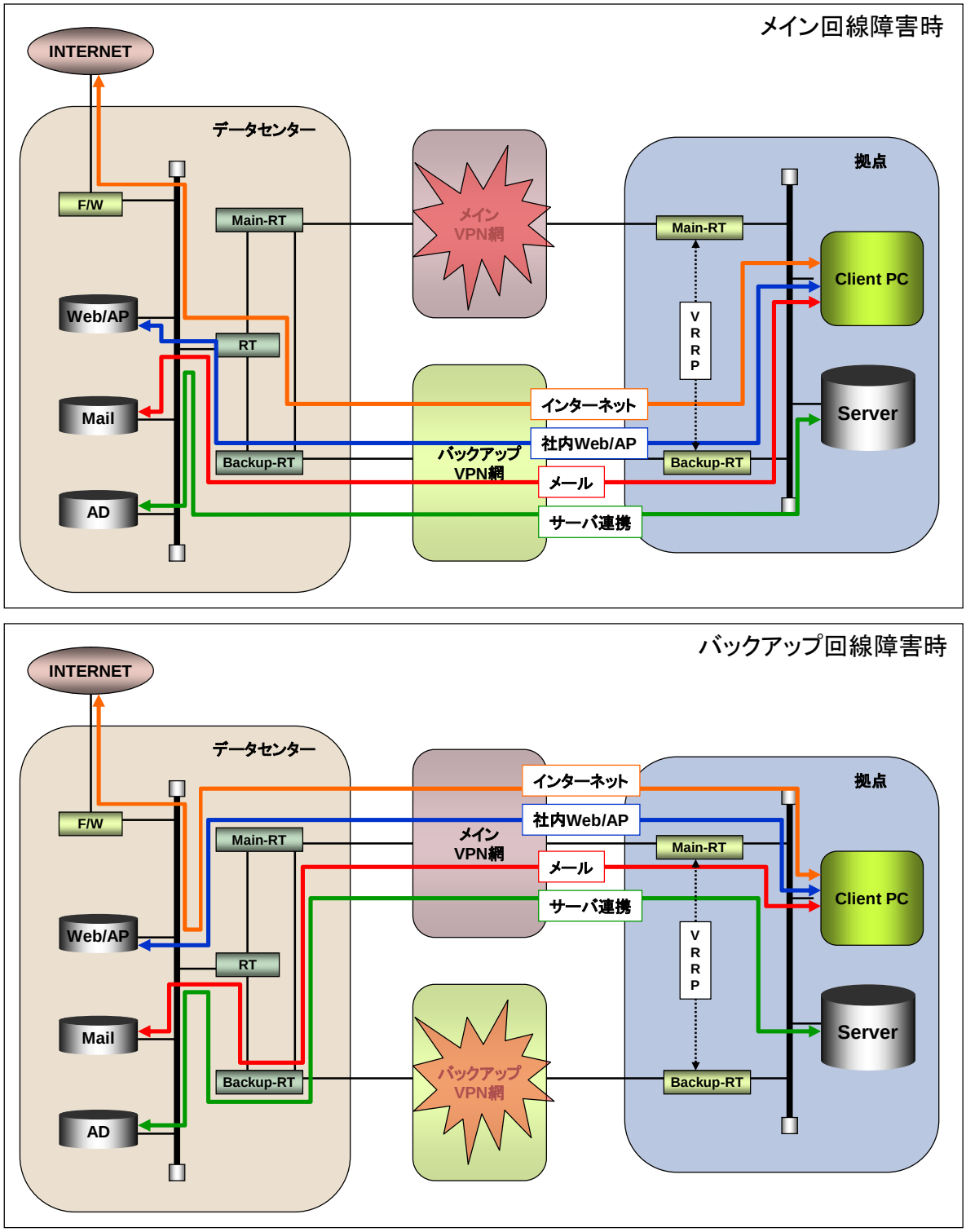


図５　障害時の切り替えイメージ

片側回線の障害時における切り替えのイメージを図５に示す。

WAN ルーティング・プロトコルに RIP（※２）を使用することで、メイン／バックアップ網内のルートの切り替えを自動的に行えるようにした。

データセンター内もルーティング・プロトコルに RIP を使用することでセンター内のル

ート切り替えも自動的に行えるようにした。
拠点内は VRRP（※３）、および、フローティング・スタティック(※４)を使用することで、拠点内ルータの障害時の自動切り替えを実現した。

※２　RIP(Routing Information Protocol)
Distance Vector Algorithm というアルゴリズムを用いて、隣接ホストと動的に経路を交換し、目的ネットワークにたどり着くまでに経由するであろうルータをホップ数という値で数値化し、最短となる経路を決定する。
同一ホップ数の経路は、2 経路までを有効経路として採用し、固定のメトリック値を付与する事により、優先する経路を制御する事が可能。

※３　VRRP（Virtual Router Redundancy Protocol ）
仮想的な IP アドレスと MAC アドレスを共有することで、複数のルータを単一の仮想ルータとして機能させることができる。マスター側の機器でインターフェース障害や機器障害が発生した場合に、スタンバイ側機器が仮想 IP アドレスと MAC アドレスを引き継ぎ、アクティブなルータとして動作する。

※４　フローティング・スタティック（Flowting Static）
通常スタティック・ルートが最も優先されるが、スタティック・ルートのアドミニストレーティブ・ディスタンス値を変えることで、この優先順位を変更することができる。例えば、RIP で学習した経路とスタティック・ルートの両方を使える環境で、スタティック・ルートのアドミニストレーティブ・ディスタンス値を RIP よりも大きく設定しておくと、RIP で学習した経路が優先的にルーティング・テーブルへ適用されることとなる。
しかし、RIP で適用されたルートがダウンした場合にはスタティック・ルートがルーティング・テーブルに適用されることとなり、ルーティングに使用される。これをフローティング・スタティックと呼ぶ。

４．結果と考察

４．１　可用性・セキュリティの向上

今回の WAN 二重化によって、ネットワーク通信のディザスタリカバリ環境が構築できたと共に、障害時の可用性の向上も果たせた。これは回線や網の障害だけではなく、ルータ等の拠点内機器やネットワークの障害においても有効であった。二重化後、バックアップ回線や拠点内ネットワーク機器の障害が二回ほど発生したが、いずれも数十秒程度で自動切り替えがなされ、ユーザへの影響を最小限にとどめることができた。
また、インターネット通信をデータセンター経由に集約できたため、フィルタリング等の一元管理が実現でき、セキュリティの統一性とレベルアップを果たすことができた。
ただし、インターネット通信に関しては、従来ブロードバンド（B フレッツ）で直に通信できていた環境に比べ、絶対的にアクセス速度が下がったため、切り替え当初は、ユーザからの不満の声も多く聞かれた。

４．２　通信量の比較

二重化前後の大規模支店の通信量の比較を図６に、小規模支店を図７に示す。いずれも、決算業務など通信の傾向を合わせるために、二重化前は 2007 年～2008 年、二重化後は 2008 年～2009 年の９月～3 月のデータを元に作成した。

インターネット通信がメイン回線に乗った分、全体的にメイン回線の通信量が増えているが、その分メール通信等をバックアップ回線に振り分けているため、帯域に対しては余裕のある通信量となっている。

また、サーバ間連携にバックアップ回線を使用しているため、各拠点ファイルサーバのデータセンターへのオンライン差分バックアップを、夜間だけでなく、平日の日中に同期を取ることも可能になっている。バックアップ間隔を小さくできるため、差分のデータ量が減り、ネットワーク・トラフィックに与える負荷も軽減できていると推測される。

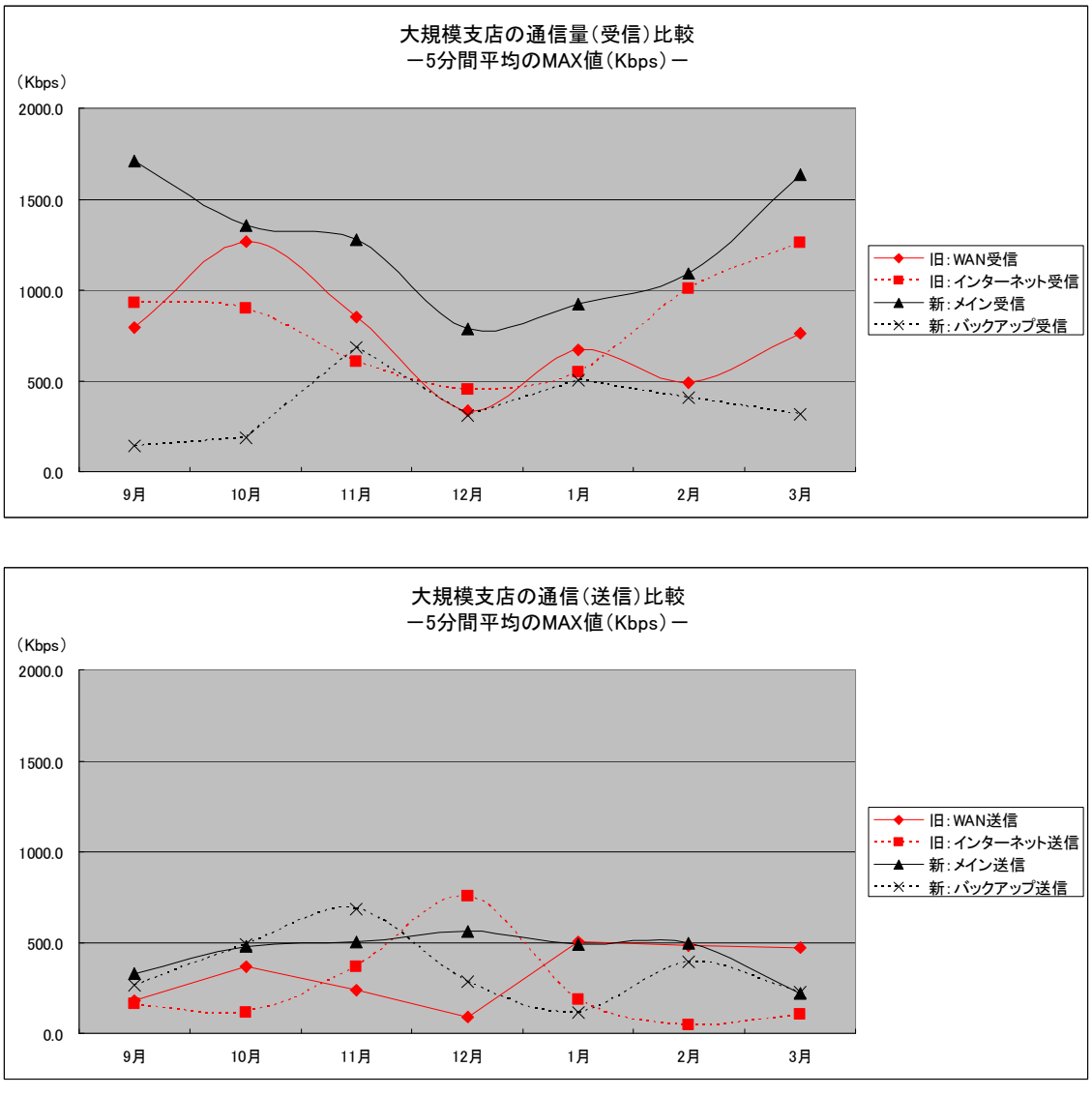
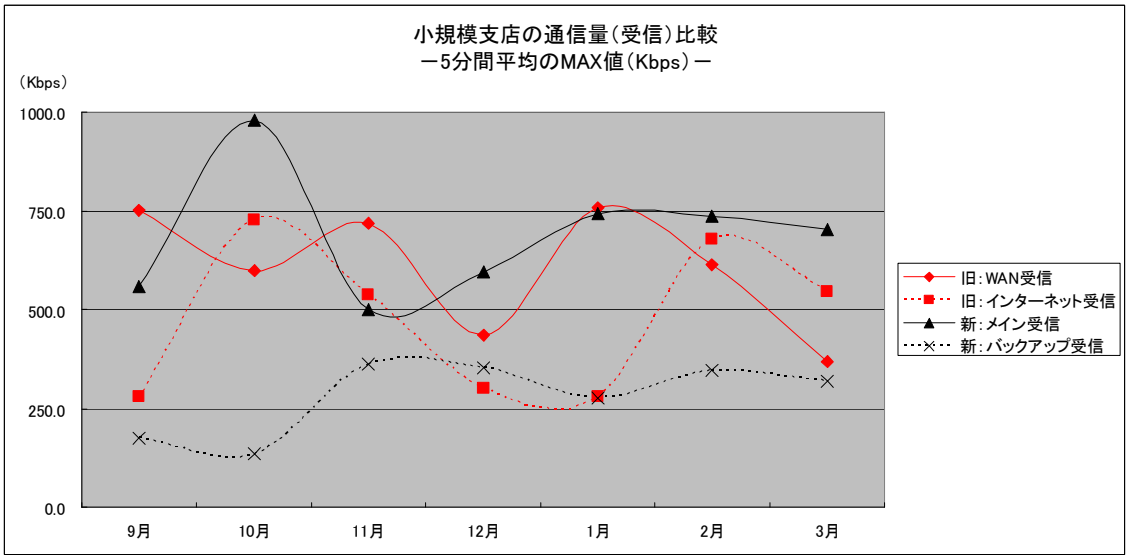


図６　大規模支店の通信量の比較



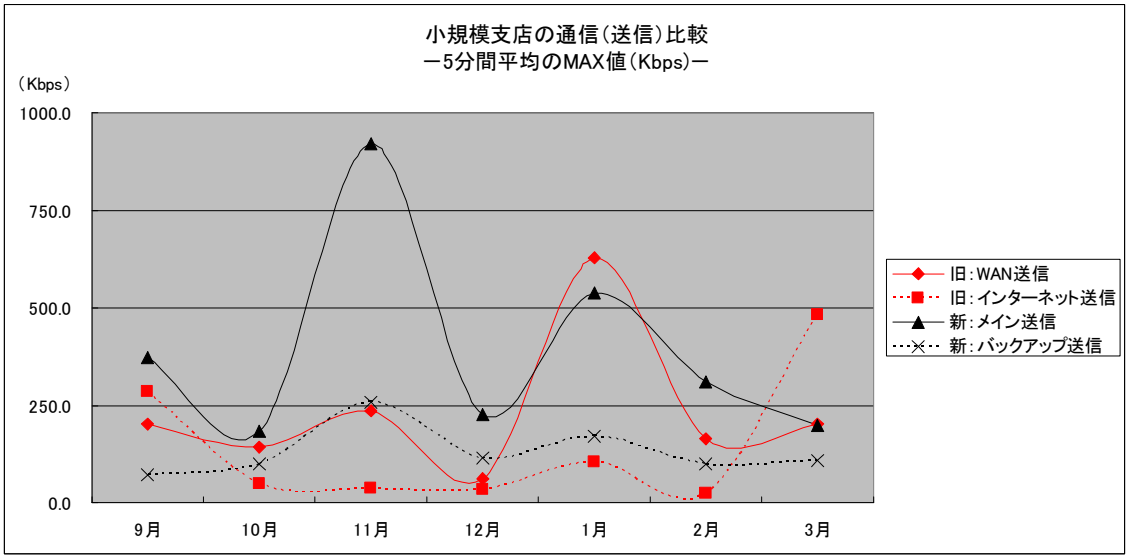


図７　小規模支店の通信量の比較

一般的にオンラインでの遠隔地バックアップの仕組み構築には回線の増速や別立てなど、高額の投資が必要とされるイメージがあったが、ADSL レベルのバックアップ回線を有効利用することで、十分安価に実運用に耐えうる環境を構築できたと思う。このように、大きな初期投資もなく、かつ、従来と変わらない運用コストで、通信環境の二重化に加え、データの保全性の向上をも果たすことができた。こういった数値化しにくい面でのコストメリットも大きいと思われる。

５．今後の課題

従来は回線品質と運用コストとの兼ね合いから、細くて高額な通信回線を使用することを余儀なくされていた。しかし、今回二重化を行い、かつ、通常時も通信内容によって自動的に振り分ける環境を構築してみて、メインの通信回線についてもベストエフォート型の安く広帯域な回線を使用しても問題がないのではないか、という実感を得た。また、フ

ファイルサイズが巨大化している昨今、そういったファイルの WAN 越えでの共有のニーズも高まってきている。これらを鑑みて、次のステップとしては、メイン／バックアップ回線のベストエフォート型ブロードバンド回線への切り替えが、今後の課題となると思われる。

また、ポリシー・ベース・ルーティングによる通信内容の振り分けに一部弊害が出ている。これは、特定のサーバに対する通信をバックアップ回線に振り分けるため、特に拠点間を異動した社員の帯同した PC 等から、他拠点サーバに何らかの通信が発生する場合には、それらの通信がバックアップ回線を通ることになり、トラフィックを圧迫することがある。こういった不都合を緩和するためにも、細かなルーティングのチューニングが必要と考えられる。

６．おわりに

今回の WAN 二重化はディザスタリカバリの実装だけにとどまらず、可用性の向上や、今後のネットワークの方向性を指し示す大きな一歩となった。末筆ながら、このプロジェクトのスムーズな進行、および、当初のイメージ通りの環境構築にご尽力いただいた関係諸氏に厚くお礼申し上げたい。