クラウド環境での
ネットワーク運用設計のあり方
－網(ネット)で雲(クラウド)をつかまえよう！－

アブストラクト

1. 社会背景とネットワーク管理者の悩み

近年、仮想化技術の進歩、セキュリティおよび耐障害性の向上などにより、いよいよ本格普及期に入ってきたと言われるクラウド。2011 年に発生した東日本大震災は、その流れを一層加速させた。従来クラウドに懐疑的であったユーザー、とりわけ企業経営層におけるクラウドへの注目度はかつてないほどに高まっている。

だが、クラウド化への急速な流れは、ネットワーク管理者に対し、二つの大きな悩みをもたらしている。ひとつはクラウドに繋がるネットワークの運用管理技術が、仮想サーバーのそれと比べてまだ未成熟、ということである。その結果、ネットワーク管理者はクラウドのどこを監視すればよいか、ネットワークリソースをどう配分すればよいか、などを手探りで対応せざるを得ない状況が続いている。

もうひとつは、クラウドの将来像が見えない中で、ネットワークへ投資を進めなければならない、ということである。企業にとってクラウド化に対応したネットワークの構築はもはや必須となってきている。今後も急速に変化するクラウドの将来像がイメージできていないと、いわゆる「使えない」ネットワークを構築してしまうという事態になりかねない。

2. クラウド環境でのネットワークとは(研究対象範囲)

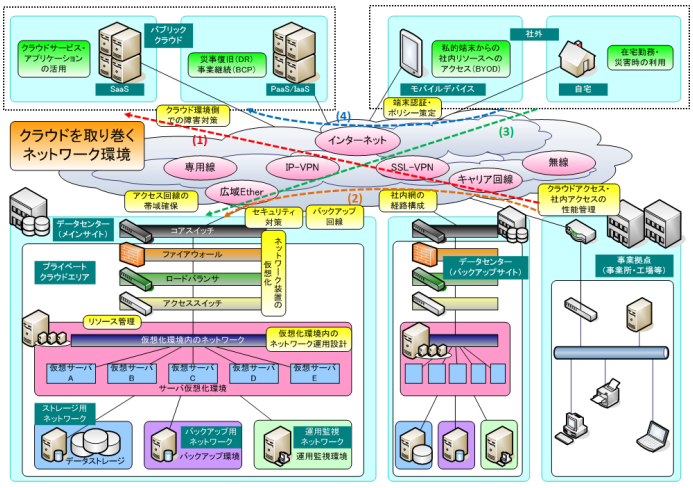
上述したネットワーク管理者の悩みを解決するため、本分科会では、クラウド時代におけるネットワーク管理者の担当範囲を定義した上で、そこで必要となる運用管理技術と将来像(どのようなネットワークを構築しておくべきか)について検討した。具体的には、次の 2 つに分けて検討した。

(A)パブリッククラウドやプライベートクラウドに繋がるネットワーク

(B)プライベートクラウドを構成するネットワーク

(A)はクラウドの外側、(B)はクラウドの内側のネットワークというイメージである。また我々は(A)をさらに 4 つのネットワーク経路に分け、これを「クラウドを取り巻くネットワーク環境」と定義した(図 1)。

図 1 当分科会で定義したクラウドを取り巻くネットワーク環境



左図(1)～(4)の区間を以下に示す。

(1)「社内」⇔「パブリッククラウド」

(2)「社内」⇔「プライベートクラウド」

(3)「社外」⇔「プライベートクラウド」

(4)「社外」⇔「パブリッククラウド」

※ただし、経路(4)は社内のネットワークを通らないため、今回の検討外(企業のネットワーク管理者の管理対象外)とした。

3. クラウド環境でのネットワーク運用設計の課題

クラウドの導入により、ネットワークの特徴や要件が変化すれば、それはネットワーク管理者にとって新たな課題が発生する要因となりうる。

そこでまず、前記(1)～(3)のネットワークについて、クラウド導入時の変化を次の 5 つの観点で分析、整理した。この 5 つは、ネットワーク管理フレームワークである「Open Systems Interconnection (OSI)」の FCAPS モデルを参考にして作成したもので、同一の観点で評価することで各ネットワークの共通課題の有無や、ネットワーク管理者の課題か否か、の分析を比較的容易に実施できた。表 1 に結果を示す。

表 1　クラウドを取り巻くネットワーク環境の課題分析結果

【分析の観点】
① セキュリティ
② 構成管理
③ 障害対策
④ 性能管理
⑤ リソース管理

【分析結果】

管理対象ﾈｯﾄﾜｰｸ	①	②	③	④	⑤
(1)社内⇔ﾊﾟﾌﾞﾘｯｸ	△	△	○	○	○
(2)社内⇔ﾌﾟﾗｲﾍﾞｰﾄ	×	○	○	○	○
(3)社外⇔ﾌﾟﾗｲﾍﾞｰﾄ	○	○	×	○	○

・○･･･変化がありネットワーク管理者の課題である
・△･･･変化はあるがネットワーク管理者の課題でない
・×･･･変化なし

次に、プライベートクラウドを構成するネットワークにおいても同様の分析を実施した。その結果、ネットワーク管理者にとって次の 2 つ、(1)サーバーとネットワークの境界の曖昧化によるサーバー管理者とのやり取り(交渉ごと)の増加、(2)仮想ネットワーク装置(仮想アプライアンス)の監視や帯域などのリソース配分の複雑化が、それぞれ課題となる、ということがわかった。

4. 検討結果(前記課題に対する対策)

前記課題に関して LS 研参加各社を中心に行ったアンケートを利用し、現状あまり認識されていない、または認識されているが対策が不十分と思われる課題について、その対策方法を、クラウドを先行的に進めている企業の取り組みや最新の技術動向の調査をもとに検討した。対策のポイントを表 2 に示す。

表 2 クラウド環境におけるネットワーク対策のポイント

管理対象ﾈｯﾄﾜｰｸ	観点	対策ポイント
(1)社内⇔ﾊﾟﾌﾞﾘｯｸ	③	接続サービス(網)の選択、可用性確保
	④	帯域の確保(インターネット出口の回線増強、多重化)
	⑤	帯域制御装置の活用(有効な配置と上位レイヤーでの制御)
(2)社内⇔ﾌﾟﾗｲﾍﾞｰﾄ	②	運用ルールの標準化、最新化(ツール導入の検討)
	③	回線の選択、可用性確保
	④	帯域拡張サービスの選択、WAN高速化装置の導入検討
	⑤	帯域制御装置の活用(有効な配置と上位レイヤーでの制御)
(3)社外⇔ﾌﾟﾗｲﾍﾞｰﾄ	①	MDM(MobileDeviceManagement)、検疫の実施
	②	運用フローの確立、端末認証、本人認証
	④	帯域の確保(インターネット出口の回線増強、多重化)
	⑤	帯域制御装置の活用(有効な配置と上位レイヤーでの制御)
ﾌﾟﾗｲﾍﾞｰﾄｸﾗｳﾄﾞ内ﾈｯﾄﾜｰｸ	②	サーバー管理者とのやりとりの定型化、ヒアリングシート作成
	④	インフラ全般をトータルで管理できる機器、ツールの導入

5. まとめ

クラウド環境を導入することで、コスト削減を目的のひとつとしていたにも関わらずサーバーとネットワークの境界が曖昧となりネットワーク管理にかかるコストが増える傾向にある。また、様々なパブリッククラウドサービスおよびモバイル機器の普及がどのように企業ネットワークを構築すればよいかという検討を難しくしている。今回、我々がクラウド先駆者の動向や最新の技術調査をもとに検討・抽出した対策ポイントを抑えつつ、企業ネットワークの運用および設計を進めていただくことで、これらの問題が軽減できると考えている。