SINET クラウド接続サービスを用いた 学内サーバ群のパブリッククラウドへの展開

林 豊洋 [1)], 福田 豊 [1)]，佐藤 彰洋 [1)]，中村 豊 [1)]

1) 九州工業大学 情報基盤センター

toyohiro@isc.kyutech.ac.jp

Deployment of on premise servers to the public cloud using SINET cloud connection service

Toyohiro Hayashi[1)], Yutaka Fukuda[1)], Akihiro Satoh[1)], Yutaka Nakamura[1)]

1) Information Science and Technology Center, Kyushu Institute of Technology

概要

本学では，2013 年より学外のクラウドサービスの利用を開始し，電子メールの SaaS での運用，WWW のパブリッククラウドでの集約化等に活用している．仮想サーバを稼働する IaaS については 2019 年度より大規模な契約を行い，本格的な利活用を進めている．IaaS は学内のサーバリソース不足時に早急にリソースが拡大できることが利点であるが，初期状態では学内のネットワーク体系と分離されている．従って，「学内のセキュリティ機器を通過しない」「既存の学内セグメントとして取り扱えない」「学内とパブリッククラウド間に高信頼の通信路を要する」等の課題が，学内サービスのパブリッククラウドへの移行を妨げる要因となっていた．

本学では，これらの課題への対応として，SINET クラウド接続サービスを用いたパブリッククラウドとの専用線接続を実施した．ネットワーク構成としては，学内の既存セグメントと IaaS 内のネットワーク体系をマッピングし，既存セグメントの延伸として扱える形式とした．本構成により，学内システム上で稼働するサーバ群のクラウド移行を促進する．

1 クラウド利活用の状況

本学が整備する情報システムは，そのシステムを提供する部局がそれぞれ調達を実施している．基本的に，事務系・学務系のシステムについては事務局が調達し，教育研究系のシステムについては学部や学科が整備している．また，LMS や大規模仮想基盤等の管理に高度な専門性を有するシステムについては，学習教育センター，情報基盤センター (以降本センターと称する) が調達・運用している．これらのシステムについては，各部局が有する計算機室にて稼働するオンプレミス方式が基本となる．

対して，情報システムやサービスの多様化・高機能化や，高度なセキュリティ対策を持続して実施するためには，クラウドサービスの活用が不可欠となっている．この状況は大学においても同様であり，教職員向け，学生向けを問わず，多くのサービスをクラウドに展開している．

本学におけるクラウドサービスの利活用は，2012 年度に開始した卒業生向けの電子メールサービスが最初であった．これは，SaaS 型の電子メールシステム (Yahoo!メール Academic Edition) であった [1]．その後，SaaS については，Office365 (電子メール (Exchange Online)，オンラインストレージ (Onedrive, Box)，コラボレーションツール（Teams))[2]，会議システム (Teams, WebEX, Zoom) など，順次利用を拡大している．PaaS についても，リスクベース認証に基づく多要素認証 (Azure AD)[3]，WWW サーバ向けのコンテナ (Azure App Service) 等を用いて，セキュリティ強化やアプリケーションの信頼性向上に活用されている．SaaS，PaaS については本学とは異なるネットワークに配置されるため，ネットワークの論理構造，ポリシー，IP アドレスの範囲等が異なる．従って，学内ネットワークとは分離した運用となる (分離されたネットワークで提供可能なサービスのみが利用可能とも換言できる)．

IaaS はパブリッククラウド上に仮想マシンを展開し，自前でアプリケーション等をインストールし，サービスを展開することが可能である．様々な OS のイメージが整備されていること，リソースのサイジ

ングやスケールアップが容易であること，API を用いたシステムの構築や運用が可能なことから，迅速なサービスの展開が可能である．本センターにおいては，2019 年度より Microsoft Azure 上のリソースについて，定められた月額上限金額まで利用可能な契約を行い，IaaS の利活用を開始した．

2 IaaS による学内向けサービス提供に関する課題

本センターでは 2019 年度より，Microsoft Azure 上に仮想サーバを配置し，学内向けサービスの展開を開始した．

本センターが有するオンプレミス内のシステム構成と，Azure 上に構築したシステム構成の関係性を図 1 に示す．

本学の学内ネットワークは，部局やプロジェクトに対して，目的ごとに複数のサブネット (VLAN) を割り当てている．サブネット内の IP アドレスについては，本学に割り当てられたアドレスブロック (グローバル IP アドレス，クラス B，2 つ) を分割し割り当てられる．

ほぼ全ての VLAN が，部局ごとに用意された仮想ファイアウォール (VDOM) に集約される．VDOM は，キャンパス毎に設置されたファイアウォール装置 (Fortigate) 内で稼働する．本センターにおいては，サービスの利用目的に応じて，戸畑・飯塚キャンパス双方に複数のサブネット (VLAN) が割り当てられている．

本センターが利用する Microsoft Azure のテナント上には，本センターのサービス用に作成した仮想ネットワーク (Azure VNET[4]，以降 VNET と称する) と，サービスの利用目的毎に仮想サーバ等の設置を行うためのサブネット (Azure Subnet) を作成している．AVNET 内では，プライベート IP アドレスで構成されたアドレスブロックを割り当て，VNET と外部との境界にて，グローバル IP アドレスとの対応付けが実行される．

2.1 学内向けサービス提供に関する課題

学内ネットワークと VNET 上の仮想ネットワークは，異なる別途のネットワークであるため，学内 - Azure 間は外部との通信として扱われる．

従って，VNET に設置した仮想サーバから，学内ネットワークに設置した機器へ通信を行う際 (例：LDAP 認証に要する通信等) は，学内に設置した機器を外部公開する必要がある．より透過的な通信を行うためには，VNET に Azure VPN 接続を定義し，対象の学内サブネットと VPN 接続 (IPSec) を確立する必要がある [5]．

本センターにおいては，VNET とセンター内のサブネット間に IPSec による拠点間接続を形成している．VNET 側では，特定の Azure Subnet のルートテーブルを編集し，学内機器への通信について VPN を経路として設定する．センター側では特定サブネット内に VPN ルータを設置し，VPN ルータに IPSec および NAT の定義を行い，Azure 側からの通信をセンター内からの通信として取り扱えるよう設定する．

これにより，特定の Azure Subnet → センター内の特定機器が直接通信可能としている．しかし，IPSec を用いることによる通信のオーバーヘッドが生じること，十分な帯域幅が得られないこと生じることが問題となる．また，本センターの VPN 設定では Azure 内 → センター内の特定機器への通信のみを考慮しており，学内全体 - Azure 間の通信は考慮していない．すなわち，「Azure 内に展開した仮想サーバが本学のネットワーク体系として取り扱えない」状況であり，学内サービスの IaaS への展開が進まない要因となっている．

3 SINET クラウド接続サービスを用いた IaaS との専用線接続

3.1 IaaS との専用線接続

学内サービスを IaaS 内へ展開するためには，IPSec による拠点間接続によって生じる通信の安定性の問題と，学内 - IaaS 間の双方向について通信可能であることが求められる．Azure には，ExpressRoute と呼ばれる，専用線接続サービスが存在する [6]．これは，利用者が契約した専用線を Azure と接続し，VNET に設定するゲートウェイ (ExpressRoute ゲートウェイ) と経路制御を行い，利用者側のネットワーク - VNET 間の通信について専用線を用いることができる機能である．VNET から外部ネットワークへの全ての通信を ExpressRoute と定義することにより，全ての通信が利用者側のネットワークを経由するため，利用者側のネットワーク接続形態やセキュリティポリシーに適合させることが可能となる．

ExpressRoute の活用は有用であると認識していたものの，専用線は利用者が調達する必要があり，加えて ExpressRoute とは指定の回線プロバイダーと契約し，マイクロソフト社に指定された拠点までの接続方法を検討する必要がある [7]．

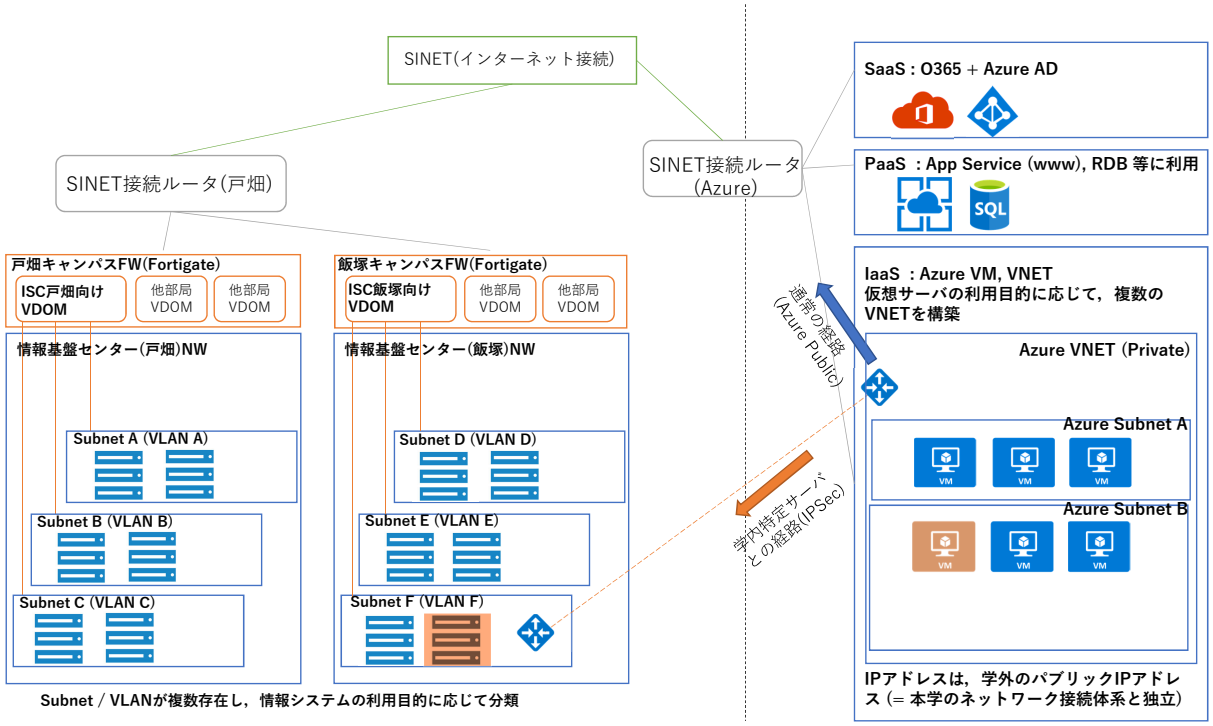

図 1　システム構成の関係性 (オンプレミス，パブリッククラウド)

専用線や ExpressRoute に対応した回線プロバイダーについては調達金額が高額となること，また利用者側と Azure 間は冗長化を持たせた経路を設定する必要があり，設置調整が煩雑であることが課題であった．

これらの課題に対しては，SINET 加入機関向けに整備された 2 つのサービスを組み合わせ活用することにより専用線接続が実現する．一点目は，国立情報学研究所が運用する SINET5[*1]の一機能となる SINET クラウド接続サービスであり，前述の「専用線」に相当する [8]．SINET クラウド接続サービスは，加入機関とクラウド提供事業者間の L2VPN 接続が提供される．従って，本学が希望する VLAN ID を用いて，本学とマイクロソフト社が指定する機材間が L2 で接続される．

二点目は，日本マイクロソフト株式会社が提供する「SINET-Azure 接続サービス」である．これは，前述の回線プロバイダー (本学向けには 1Gpbs の帯域幅が割当) および BGP ルータが提供されるサービスとなる．SINET-Azure 接続サービスが提供する BGP ルータには，SINET クラウド接続サービス (本学側) と，ExpressRoute が接続される．

上記のサービスを組み合わせ，SINET クラウド接続サービスを接続する本学側の機材と，ExpressRoute ゲートウェイの経路設定を行うことにより，学内ネットワーク - VNET 間が専用線にて学外に出ることなく L3 接続される (図 2)．

なお，これらのサービスは大学に対しては無償で提供頂いており，IaaS の利活用に大変有用である[*2]．

3.2　学内ネットワークと IaaS との接続形態

VNET 内に割り当てるネットワークアドレスによって，学内ネットワークと VNET 間の接続形態が異なる．

VNET の運用形態として，IaaS 専用のネットワークアドレスを割り当てる方法が考えられる．Azure では，VNET に対してグローバル IP アドレス空間の割り当てが可能であるため，本学が管理する任意のサブネット (グローバル IP アドレス) を VNET(および Azure Subnet) に割り当てることにより，「Express-Route 上の学内グローバル IP アドレスを持つセグメント」が構成できる (図 3)．この方式は，クラウド上にサービスを配置するセグメントを新規に設置し，新規サービスを配置する，あるいは既存の学内セグメントに配置されたサービスは順次移行する運用に適していると考えられる．

[*1] 2021 年度末に切り替え予定の SINET6 においても，継続して提供される

[*2] Azure の機能である ExpressRoute と ExpressRoute ゲートウェイについては，これまで通りの利用料金が生じる

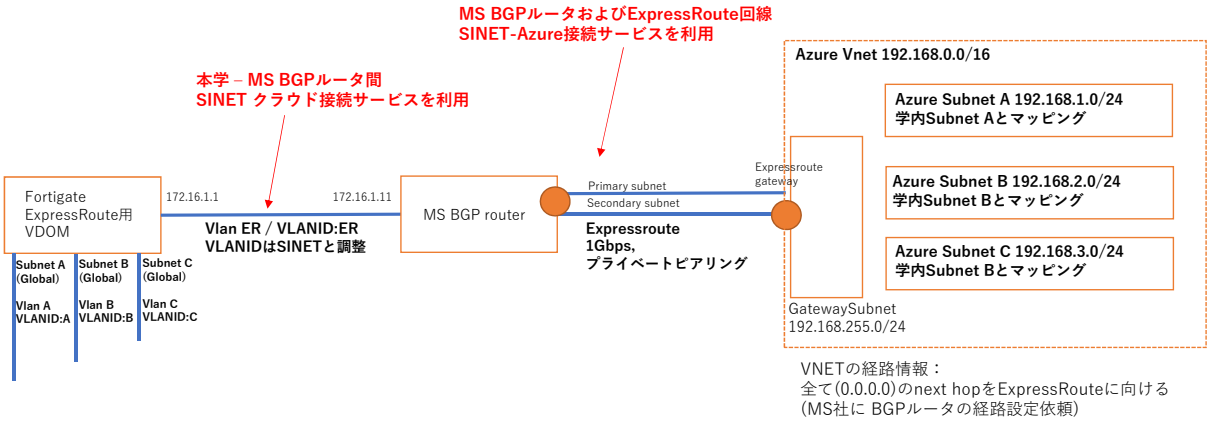

図 2　SINET クラウド接続サービスを用いた IaaS との専用線接続

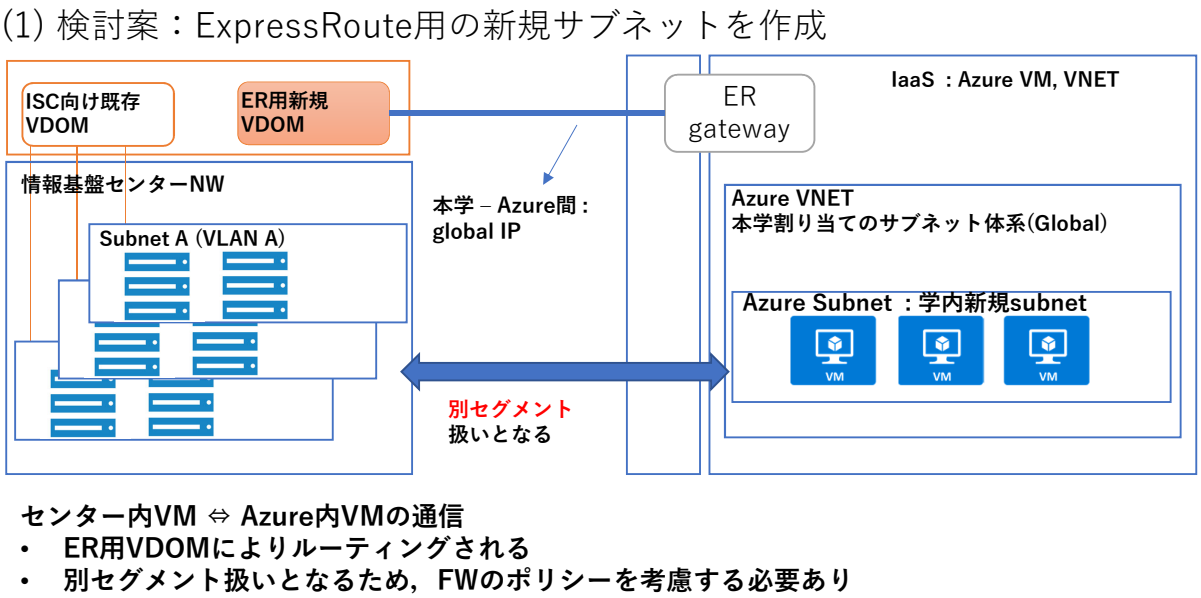

図 3　VNET 内への学内グローバル IP アドレスの割り当て

前述の IaaS 専用のネットワークアドレスを割り当てる方法は，VNET 内が学内のネットワークアドレス体系であり，学内 - VNET 間の経路の設定も直感的である．しかし，既存セグメント内の一部のサービスのみを IaaS 上のセグメントに移設するような状況においては，サービスを構成するサーバ群の IP アドレスが変更となる点や，別セグメントとの通信に構成が変更される．別セグメントとの通信を考慮するためには，ファイアウォール装置によるアクセス許可等のポリシーを適切に追加・更新する必要がある．本センターは既にサービス用の複数のサブネットを有しているため，ポリシーの書き換えは困難な作業となる．

従って本センターにおいては，VNET を既存セグメントの延伸として取り扱える形態を検討した．VNET からの外部への全ての通信を ExpressRoute 経由に出来ることと，本学側のファイアウォール装置を経由できる性質を利用し，ファイアウォール装置が持つ機能を組み合わせることにより，既存セグメントの延伸の形態を実現する (図 4)．

Azure 側では，VNET 側にプライベート IP アドレスを割り当て，VNET から外部への通信は全て ExpressRoute を経由するよう経路を設定する．この設定により，IaaS 上に展開された仮想マシン等はプライベート IP アドレスを持ち，通信は本学側のファイアウォール装置 (本学では Fortigate VDOM にて構築) を経由する．

VDOM は ExpressRoute との通信用に新たに作成し (以降，ER VDOM と称する)，延伸したいセグメント群の VLAN と ExpressRoute への VLAN(SINET クラウド接続サービス経由で Azure に到達) を収容

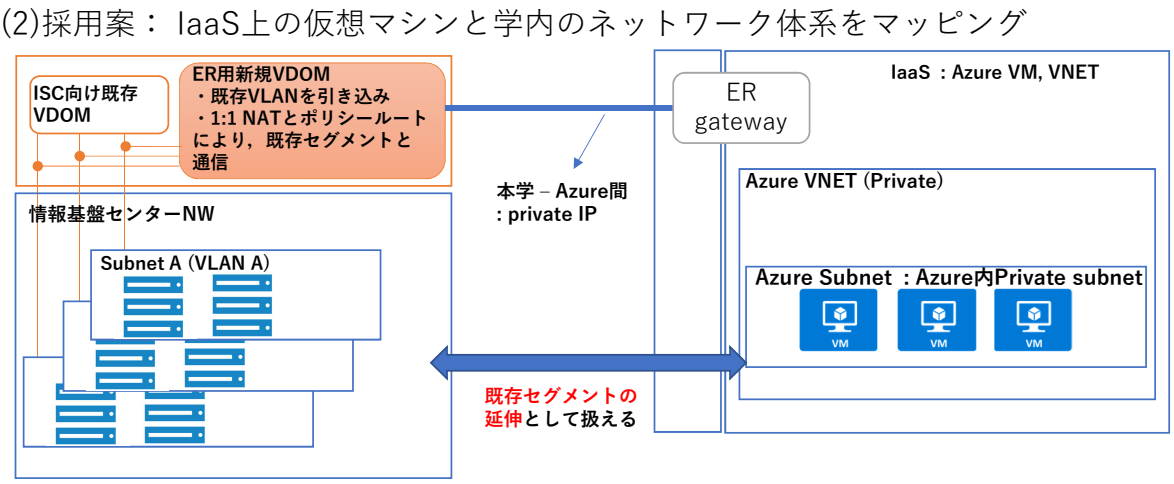

図 4　VNET への学内既存セグメントの延伸

する．ER VDOM において，VNET 内の仮想マシンと，既存セグメント上のグローバル IP アドレスの 1:1 マッピング (バーチャル IP，1:1 NAT) を行う．

利用したい既存セグメントが複数存在する場合においても，

1. VNET 内の Azure Subnet を複数作成し，学内 VLAN A,B,C - Azure Subnet A,B,C のように 1:1 の対応関係とする
2. ER VDOM のポリシールート機能を用いて，Azure Subnet のソース IP を手掛かりとして，対応する既存セグメント内のゲートウェイへ経路を設定する

ことにより収容可能となる [9][10].

本方式により，VNET 上の仮想マシン等は学内の既存セグメントに配置されたものとして振る舞われる．VNET 内の仮想マシン間においても既存セグメントに割り当てたグローバル IP アドレスを用いて通信可能である[*3]．従って，既存セグメント間のアクセス許可等のポリシーを維持したまま，IaaS への仮想マシン等の展開が可能となる．

3.3　既存セグメントと Azure Subnet のマッピング設定例

ここでは，図 2 の接続形態を例として，学内の 2 セグメントを VNET 上の 2 つの Azure Subnet に延伸する場合の設定例を示す．主要なパラメータは図 5 の通りである．

なお，設定例にて用いるファイアウォール装置は Fortinet 社の Fortigate シリーズを想定しており，仮想ファイアウォール (VDOM 機能) 上に設定を行うものとする．

学内セグメントA (Subnet A)	グローバルIPアドレス(1.1.1.0/24) VLAN ID A ゲートウェイIPアドレス 1.1.1.1
学内セグメントB (Subnet B)	グローバルIPアドレス(1.1.2.0/24) VLAN ID B ゲートウェイIPアドレス 1.1.2.1
学内 – MS BGPルータ間	プライベートIPアドレス(/29) VLAN ID ER MS BGPルータIPアドレス 172.16.1.1
ExpressRoute接続用VDOM	VDOM名 ER VDOM 収容VLAN VLAN ID A,B,ER
Azure VNETのアドレス空間	192.168.0.0/16
Azure Subnet A	プライベートIPアドレス(192.168.1.0/24) 全ての外部への経路をExpressRouteへ向ける **学内セグメントAと対応付け**
Azure Subnet B	プライベートIPアドレス(192.168.2.0/24) 全ての外部への経路をExpressRouteへ向ける **学内セグメントBと対応付け**
IPアドレス対応付け1	学内セグメントA 1.1.1.10 Azure Subnet A 192.168.1.2
IPアドレス対応付け2	学内セグメントB 1.1.2.10 Azure Subnet B 192.168.2.3

図 5　VNET へのセグメント延伸設定例 (パラメータ)

学内セグメント - Azure Subnet の対応付けには，学内セグメント毎のデフォルトゲートウェイの設定，ポリシールートの設定，NAT ポリシーの設定を要する．上記設定後，学内セグメント内の IP アドレス - Azure Subnet 内の仮想マシン等の対応付けには，バーチャル IP の定義，1:1NAT 向けのポリシーの設定を要する．

設定例に基づき，「学内セグメント - Azure Subnet の対応付け」「IP アドレス対応付け 1」「IP アドレス対

[*3] ただし，VNET と ER VDOM 間を往復する

応付け 2」を行う際の設定内容を図 6 に示す．

Azure行き，学内セグメント毎の デフォルトゲートウェイ設定	192.168.0.0 gateway 172.16.1.1 dev vlan ER #to Azure 0.0.0.0 gateway 1.1.1.1 dev vlan A #VLAN A 0.0.0.0 gateway 1.1.2.1 dev vlan B # VLAN B
ポリシールートの設定 (Azure Subnet毎に デフォルトゲートウェイを振り分け)	# VNET内の仮想マシン同士で，学内IPを用いて通信するための折り返し設定 In vlan ER, src 192.168.0.0/16, dst 192.168.0.0/16 -> out vlan ER, gw 0.0.0.0 # Azure Subnet Aから学内への通信時，vlan Aを経由し，vlan Aの gwに転送 In vlan ER, src 192.168.1.0/24 -> out vlan A, gw 0.0.0.0 # Azure Subnet Bから学内への通信時，vlan Bを経由し，vlan Bの gwに転送 In vlan ER, src 192.168.2.0/24 -> out vlan B, gw 0.0.0.0
NATポリシーの設定 (Azure → 学内セグメント通過の際に， 学内IPアドレスに付け替え)	# Azureから vlan Aに向かう際に，学内IPにNAT From vlan ER, To vlan A, srcip all, dstip all, nat on # Azureから vlan Bに向かう際に，学内IPにNAT From vlan ER, To vlan B, srcip all, dstip all, nat on
IPアドレス対応付け1 学内セグメントA 1.1.1.10 Azure Subnet A 192.168.1.2 (学内 1.1.1.10 ⇔ Azure 192.168.1.2)	[バーチャルIP] 名称：VIP:VIP1 / 1.1.1.10 と 192.168.1.2をマッピング [NATポリシー] # バーチャルIPを用いて，Azure内仮想マシンに転送 From vlan A, To vlan ER, srcip all, dst VIP:VIP1, nat OFF # Azure内から着信した際，学内IPに付け替えて転送 From vlan ER, To vlan A, srcip all, dst VIP:VIP1, nat ON
IPアドレス対応付け2 学内セグメントB 1.1.2.10 Azure Subnet B 192.168.2.3 (学内 1.1.2.10 ⇔ Azure 192.168.2.3)	[バーチャルIP] 名称：VIP:VIP2 / 1.1.2.10 と 192.168.2.3をマッピング [NATポリシー] # バーチャルIPを用いて，Azure内仮想マシンに転送 From vlan B, To vlan ER, srcip all, dst VIP:VIP2, nat OFF # Azure内から着信した際，学内IPに付け替えて転送 From vlan ER, To vlan B, srcip all, dst VIP:VIP2, nat ON

図 6　VNET へのセグメント延伸設定例 (VDOM への機能設定)

3.4　他部局テナントとの専用線接続の共有

ExpressRoute は Azure のテナントに関連付くため，同一テナント内の VNET に対しては，ExpressRoute ゲートウェイを作成・回線をリンクすることにより利用可能となる [11].

本稿で言及する Azure テナントは，本センターのみが利用しており，他部局の仮想マシン等は別テナントに存在している．

別テナントが学内と ExpressRoute による専用線接続を行う際，別途 SINET クラウド接続サービスと SINET-Azure サービスを契約し，他部局向けの VDOM を構築する方法が挙げられる．別途構築する際，新たに回線契約を実施する必要があることや，ExpressRoute の利用料金が同様に発生することから，構築期間，設備，費用面等の課題がある．

対して，ExpressRoute には，回線を共有し，別テナントの VNET に接続する機能を有している．回線所有者 (本センター) が承認キーを作成し，回線ユーザー (別部局) と共有することにより，別テナントの Express ゲートウェイへ接続可能となる (図 7)．本学においては回線を共有する方式で，事務職員向けの WVD(仮想デスクトップ) 接続を ExpressRoute 経由としている．

節で述べたセグメントの延伸を行う際は，VNET 内の IP アドレスに応じてポリシールートを行うため，別テナントの VNET に割り当てられたネットワークアドレスが重複していないことが，回線を共有可能な条件となる．また，ExpressRoute の帯域を共有するため，多数のテナントと共有する場合，帯域幅が十分であるか留意する必要がある．

4　まとめ

本稿では，学内サービスの IaaS への展開に際して，検討すべき事項と本学における解決策について言及した．IaaS 上に仮想サーバ等を展開した場合，ネットワーク構成が学内と独立したものとなるため，通信が学内のセキュリティ機器を経由しないことや，学内セグメントとして取り扱えないことが課題となる．本学では，SINET クラウド接続サービスと専用線接続機能 (Azure ExpresRoute) を活用し，学内とパブリッククラウド (Microsoft Azure) 間を直接通信できる構成とした．更に，IaaS 上の仮想ネットワーク (Azure VNET) を既存の学内セグメントの延伸として取り扱るよう，ネットワーク及びファイアウォール装置を構成した．加えて，ExpressRoute の持つ回線共有機能を活用し，他部局のテナントを同一の回線で学内に収容した．本稿では，本学が採用したネットワーク構成やファイアウォール装置の設定例を掲載しており，これらのノウハウが大学における IaaS 利活用の一助になれば幸いである．

参考文献

[1] 林 豊洋，本学における生涯メールサービスの提供について，九州工業大学情報科学センター広報第 26 号，2014.

[2] 林 豊洋，甲斐 郷子，九州工業大学における生涯メールサービスの移行，大学 ICT 推進協議会 2017 年度年次大会，2017.

[3] 林 豊洋，福田 豊，佐藤 彰洋，大橋 健，Office365 を用いたメールサービスに対するセキュリティ向上対策 - ログ監視，認証基盤の強化 -，学術情報処理研究，24 巻 1 号 （頁 104 ～ 115），2020.

[4] Microsoft，Microsoft Azure - Virtual Network，https://docs.microsoft.com/ja-jp/azure/virtual-network/

[5] Microsoft，Azure Portal でサイト間接続を作成する，https://docs.microsoft.com/ja-jp/azure/vpn-gateway/tutorial-site-to-site-portal

[6] Microsoft，Azure ExpressRoute とは，https://docs.microsoft.com/ja-jp/azure/expressroute/expressroute-introduction

[7] Microsoft，ExpressRoute パートナーとピアリングの場所，https://docs.microsoft.com/ja-jp/azure/expressroute/expressroute-locations-providers#global-commercial-azure

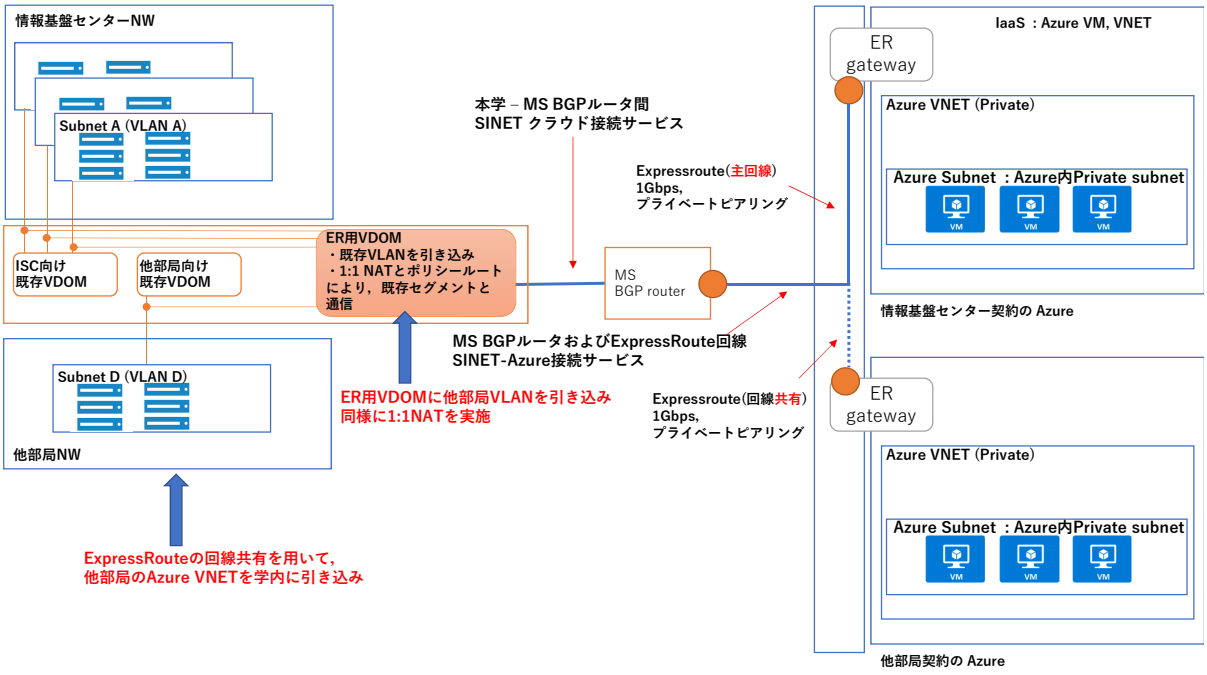

図 7　他部局テナントとの ExpressRoute 回線の共有

[8] 国立情報学研究所，SINET クラウド接続サービス，
https://www.sinet.ad.jp/connect_service/service/cloud_connection

[9] Fortinet，Technical Note：Configuration example of Policy Based Routing and VIP for SMTP services in Dual Wan scenario，
https://kb.fortinet.com/kb/viewContent.do?externalId=FD31240

[10] Fortinet，Technical Note: How to access natted server internally with Public IP address：Loopback policy，
https://kb.fortinet.com/kb/viewContent.do?externalId=FD36657

[11] Microsoft，VNet を回線に接続する - 異なるサブスクリプション，
https://docs.microsoft.com/ja-jp/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager