特集論文

クラウド型VPN接続機能：クラウドを利用した汎用機能のコンポーネント化

根岸啓吾*
Keigo Negishi

*三菱電機ビルソリューションズ㈱

Cloud-based VPN Connection Function:
Componentization of Generic Functions Using Cloud Computing

要　旨

“クラウド型Virtual Private Network（VPN）接続機能”は，クラウドコンピューティング技術を活用し，三菱電機ビルソリューションズ㈱（MEBS）稲沢ビルシステム製作所製ビルマネジメント製品（以下“MEBS製システム”という。）のVPN接続機能を汎用的に利用できるようコンポーネント化したものである。クラウド型VPN接続機能が提供可能なサービスとして，“VPN接続サービス”“メール送信サーバーサービス”の二つが挙げられる。VPN接続サービスは“通信経路暗号化機能”“複数拠点(注1)間の通信制御機能”及び“拠点への遠隔接続機能”を備える。メール送信サーバーサービスは“メール送信機能”及び“過剰送信の通知機能”を備える。これらのサービス・機能をMEBS製システムに利用できる汎用機能として開発した。クラウド型VPN接続機能は今後もクラウド上に構築されているシステムである点を生かして，汎用的な機能を取り込みながら，コストや汎用性の面でMEBS製品の価値向上に寄与していく。

（注1）　ここで“拠点”とは，MEBS製システムが納入された，顧客の所有する拠点のことを指す。ただし，1拠点当たりVPNルーターを1台設置する前提とするため，VPNルーターが複数設置された拠点はVPNルーターの台数分の拠点として数える。

1．ま　え　が　き

近年，パブリッククラウドの市場規模が初めて1兆円を超過したが，2026年には4兆円を突破するとの推計(1)(2)が出ている。市場規模の増大に伴い，パブリッククラウド上で提供される機能は年々多様化・高度化している。また，パブリッククラウド上で実現可能な技術が多様化・高度化したことと，提供されるサービスが市場競争によって安価になったことに伴い自社のサービスや製品をクラウド化することで，開発コストや運用コストを低減しようとする動きも活発化している。クラウド型VPN接続機能（**図1**）はこうした動きに追従するとともに，今まで製品ごとに開発されていた汎用機能をどのMEBS製品でも利用可能な形でクラウド上に構築することによって，開発コストの低減ひいては顧客が負担するコストの低減に寄与する。

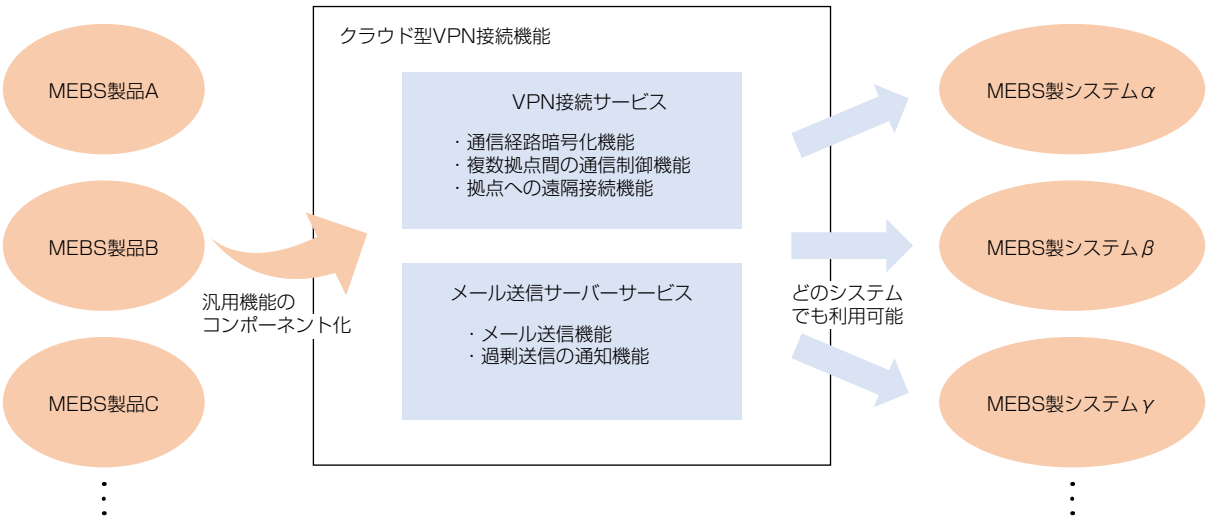


図1．クラウド型VPN接続機能の概念図

本稿では，始めにクラウド型VPN接続機能のシステム構成と特長を述べる。次に，具体的なサービスとして，VPN接続サービスとメール送信サーバーサービスについて述べて，最後にクラウド型VPN接続機能の今後の展望を示す。

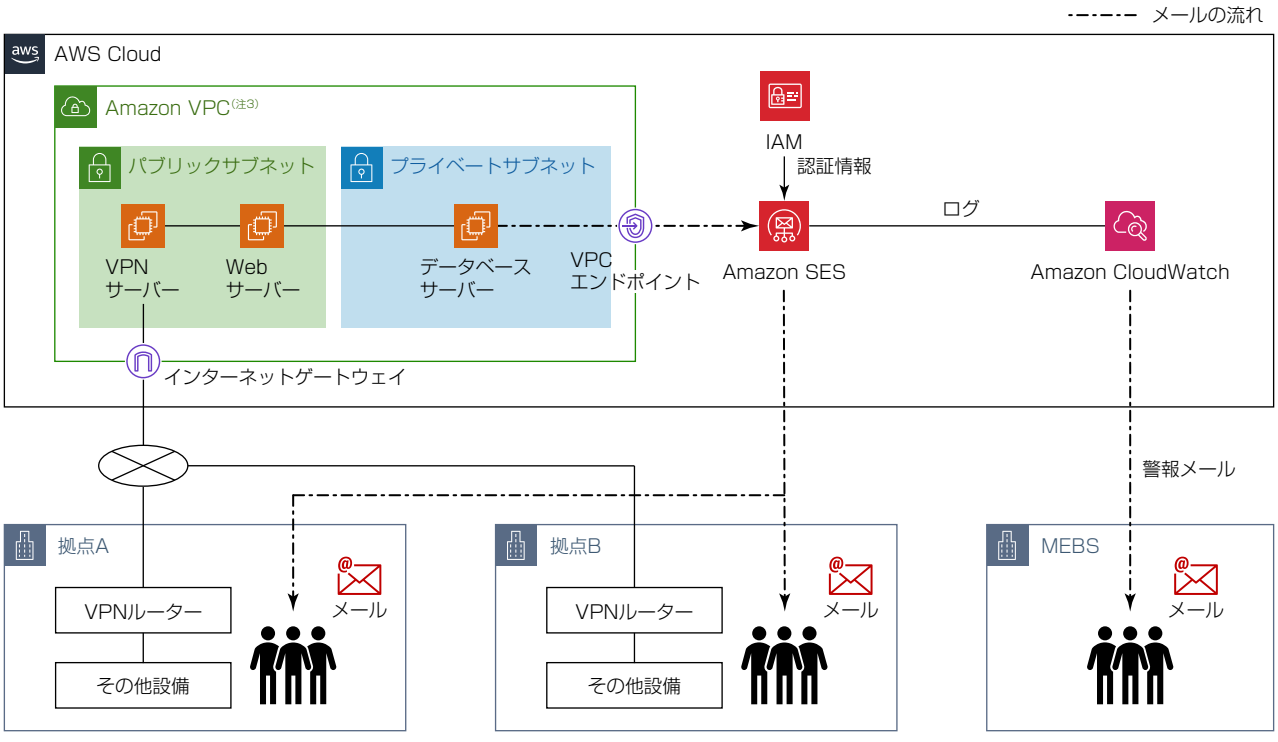
2. クラウド型VPN接続機能のシステム構成

この章では，クラウド型VPN接続機能のシステム構成を述べた上で，その特長について述べる。

2.1 システム構成

図2にクラウド型VPN接続機能の持つ二つのサービスのシステム構成を示す。クラウド型VPN接続機能はインターネット回線を利用して，AWS(Amazon Web Services)(注2)上に構築されたシステムである。クラウド型VPN接続機能を利用するMEBS製システムがそのシステム内の拠点間で通信する必要がある場合に，外部ネットワーク上の通信経路暗号化を提供する。また，MEBS製システムが外部へメールを送信する必要がある場合，メール送信サーバーを提供する。クラウド型VPN接続機能で接続される各拠点には3G通信モジュール内蔵VPNルーター(以下“VPNルーター”という。)が設置されており，VPNルーターのLAN側に接続された設備とクラウド上のサーバーを接続する。クラウド型VPN接続機能は，クラウド上にあるデータベースサーバーやWebサーバーの前段にVPNサーバーを構築することによって，これらと各拠点に設置された設備の通信経路を暗号化する。また，拠点が複数存在する場合では，拠点間通信の制御も実施する。さらに，VPNルーターのLAN側に接続された設備又はクラウド上のサーバーがメールを送信する場合，AWSのAmazon SES(以下“SES”という。)を利用することによって，設備が接続するメール送信サーバーを提供する。

(注2)　AWS，Amazon Web Servicesは，Amazon Technologies, Inc.の登録商標である。



(注3)　Amazon VPCは，Amazon Technologies, Inc.の登録商標である。
VPC：Virtual Private Cloud，SES：Simple Email Service

図2．クラウド型VPN接続のシステム構成

2.2 システム構成上の特長

クラウド型VPN接続機能は，汎用機能をクラウド上に構築することによって，当該の汎用機能を利用するシステムごとに構築しなければならなかったという従来の課題を解決している。例えば，従来製品ではVPN接続機能を実装しよう

と考えた場合，高額なVPNサーバーを構築するか，又は，パブリッククラウドのVPN接続サービスを利用する必要があった。パブリッククラウドのVPN接続サービスを利用する場合，拠点間の通信制御を実施するためには，別途中継サーバーも構築する必要がある。また，メール送信機能を実装しようと考えた場合，別途，高額なメール送信サーバーを構築する必要があった。この場合，システムに改善や改修が発生したとすると，メールサーバーも改修する必要がある可能性があり，保守員が現地を訪れる必要がある点や顧客との日程調整が必要な点から保守性・経済性を損なっていた。さらに，VPNサーバーやメール送信サーバーのような物理サーバーは導入時の初期費用が高額であり，顧客の負担も大きかった。

一方で，クラウド型VPN接続機能はクラウド上に構築されているため，システムの改修等が発生した場合でもローカルコントローラーやローカルサーバーに手を加える必要はなく，遠隔作業によって改善点をスムーズに顧客へと提供できる点で優れている。さらに，従来必要であった高額なVPNサーバーの導入費用や割高なVPN接続サービスの利用料が不要になり，安価な月額費用だけで安全な通信経路を提供可能である。

3. クラウド型VPN接続機能のサービスと特長

この章では，クラウド型VPN接続機能のサービスとして挙げた“VPN接続サービス”と“メール送信サーバーサービス”の２点について，それぞれの機能と特長を述べる。

3.1　VPN接続サービス

VPN接続サービスの機能と特長を述べる。

3.1.1　VPN接続サービスの機能

VPN接続サービスは“通信経路暗号化機能”“複数拠点間の通信制御機能”“拠点への遠隔接続機能”の三つの機能を持つ。

まず通信経路暗号化機能では，AWS上にAmazon EC2(注4)というサービスを利用して仮想のLinux(注5)サーバーを構築し，そこにオープンソースのVPNソフトウエアであるstrongSwanを動作させることで，L3-VPNであるIPsec(Security Architecture for Internet Protocol) VPNを使用し，VPNルーター-VPNサーバー間の通信をAES(Advanced Encryption Standard)暗号化する。

また拠点間の通信制御機能では，顧客が複数の拠点を所有していた場合に，その各拠点間のIP(Internet Protocol)アドレスベースでのアクセス制御を実施する。

最後に拠点への遠隔接続機能では，遠隔地に存在する顧客の拠点へ，調整作業のためMEBSから接続することを可能にする。このとき，VPNルーターの持つモバイル回線機能を利用することで，ネットワーク回線が敷設されていない拠点でも外部からのアクセスも可能にしている。

（注４）　Amazon EC2は，Amazon Technologies, Inc.の登録商標である。
（注５）　Linuxは，Linus Torvalds氏の登録商標である。

3.1.2　VPN接続サービスの特長

VPN接続サービスでは，オープンソースソフトウエアを利用することによって，開発負荷を軽減している。

また，顧客が拠点に敷設している回線では一般に固定IPアドレスが付帯していないことを鑑みて，VPNサーバーに固定IPアドレスを付与し，VPNルーター側をVPN接続の起点としている。これによって顧客に固定IPアドレスを新たに取得させることなく，VPN接続サービスの提供を実現している。

さらに，顧客が複数の拠点を持つ場合，拠点同士での通信を実施したいケースや，反対に特定の拠点同士では通信を実施したくないケースが発生する。しかし，VPNの機能では，クライアント同士の通信の制御はできないため，このケースでは，VPNサーバーのOSであるLinuxに実装されているファイアウォール機能であるiptablesを利用することで拠点間の通信制御を実現している。

最後に，拠点への遠隔接続機能では，実際に拠点へ赴くことなく，VPNルーターのファームウエアのアップデートや設定値の変更，ログファイルの取得等が可能である。また，VPNルーター自体だけでなく，そのLAN側に接続されたシステムへ接続し，設定を施すことも可能である。これに加えて，VPNルーターの持つモバイル回線機能と拠点への遠隔

通信機能を合わせることによって(注6)，従来であればネットワーク回線が敷設される前の拠点で不可能であった，ネットワークを利用するシステムの施工や調整作業を可能にしている。

(注６)　モバイル回線を利用した拠点への遠隔接続機能は，無線特有の不安定性等を鑑みて，工事・調整用途でだけ利用を許可する。

3. 2　メール送信サーバーサービス

この章では，メール送信サーバーサービスの機能と特長について述べる。

3. 2. 1　メール送信サーバーサービスの機能

メール送信サーバーサービスは“メール送信機能”と“過剰送信の通知機能”の二つの機能を持つ。まずメール送信機能では，その名前のとおり，MEBS製システムに対してメールを送信するためのSMTP(Simple Mail Transfer Protocol)サーバーを提供する。また過剰送信の通知機能では，メールの送信数が事前に設定した値を超えていないか監視し，超えた場合はMEBSの担当者へ通知が送られる。

3. 2. 2　メール送信サーバーサービスの特長

メール送信サーバーサービスでは，SESに備えられているSMTPエンドポイントを利用してメールの送信を実現している。ここで，メール送信機能を提供する上で避けられないのがエラーメールである。このサービスでは，エラーメールが発生した場合，Return-Pathと呼ばれるメールヘッダの一部に返信先のメールアドレスを記載することで，記載したメールアドレスへとエラーメールが返信される仕組みを提供している。これによって，送信エラーが発生した場合にも，送信者がそのエラーに気が付くことができる。

また，過剰送信の通知機能によって，不正アクセス等による認証情報の流出を原因とするメール送信サーバーの踏み台利用を検知するとともに，SESの１日当たりのメール送信上限数に到達していないかを監視している。

4．今後の展望

VPN接続サービスは，**図３**に示すように，VPNサーバー二重化による通信の冗長化を含めた機能の拡張を検討している。

図３に示した構成で，平時はLVS(Linux Virtual Server)という，Linux OSに搭載されたロードバランサーを利用することで，待機サーバーとの間で負荷分散を図る。これによって，待機系サーバーが稼働していない時間を減らし，コス

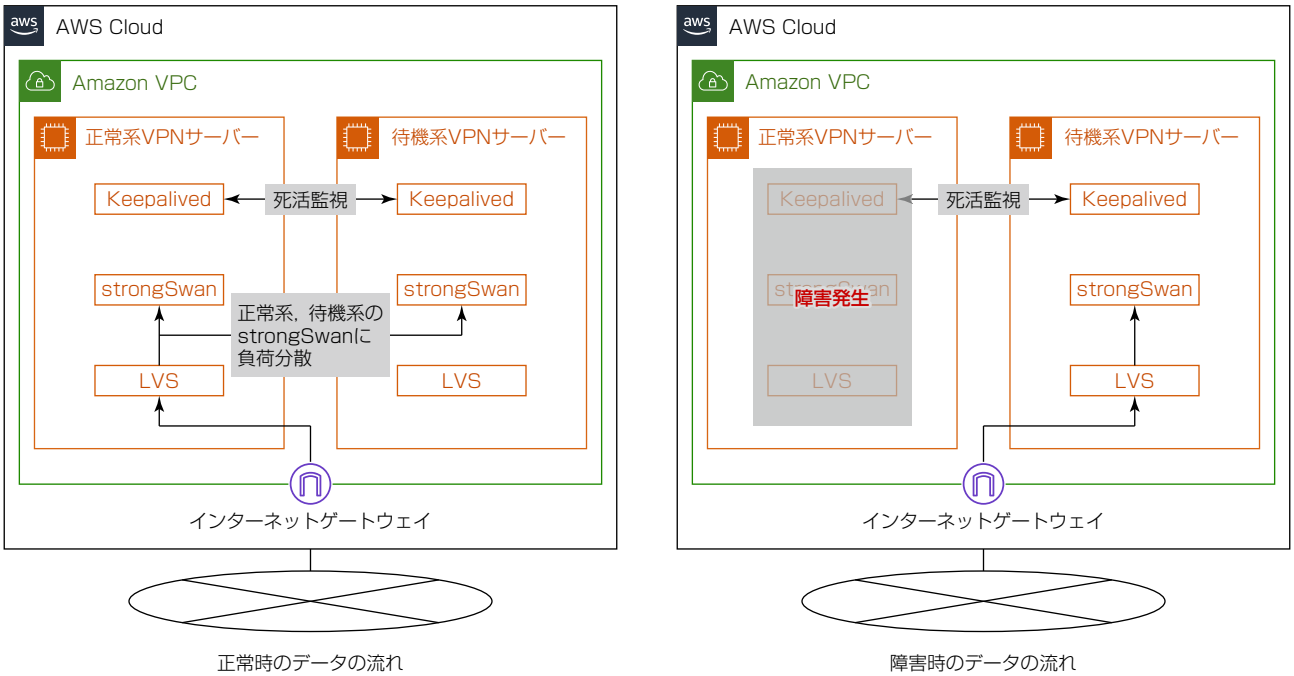


図３．VPN接続サービス冗長化検討

ト面での無駄を削減している。また，常に待機系サーバーを起動しておくことによって，切替え時に待機系サーバーが起動するまでの時間を短縮している。さらに，**図3**に示した構成で，同一サブネット上のルーター装置間での冗長化を実現するプロトコルであるVRRP(Virtual Router Redundancy Protocol)をLinux上で実装したモジュールのKeepalivedを利用することによって，正常系と待機系のVPNサーバー間での死活監視を実施する。この死活監視によって，正常系のサーバーに問題が発生した場合は即座に待機系のサーバーだけでの運用に切り替えることができ，システムの稼働を維持することが可能である。

5. むすび

クラウド型VPN接続機能の持つサービスである，安全な通信経路と通信の制御を提供するVPN接続サービスと，新規開発不要でメールの送信機能を提供するメール送信サーバーサービス，及びその機能と将来展望について述べた。クラウド型VPN接続機能は今後も自社製品向けの汎用的な機能を取り込んで，製品及び運用コスト・開発コストの両面から製品の価値向上を支えていく。

参考文献

(1) ㈱MM総研：パブリッククラウドの国内市場は1兆円を突破（2021）
https://www.m2ri.jp/release/detail.html?id=500
(2) IDC Corporate：国内パブリッククラウドサービス市場予測を発表（2022）
https://www.idc.com/getdoc.jsp?containerId=prJPJ49684222