オープンソースソフトウェアで実現するクラウドサービス

クラウドコンピューティングをはじめとするさまざまな分野でオープンソースソフトウェア（OSS）が業界標準となっているが，企業におけるOSSの活用においては，セキュリティポリシーへの適合や運用管理が課題である。
本稿では，SDN技術やChatOps型運用自動化技術によって課題を解決することで，OSSを活用してクラウドサービスを実現する手法を提案する。試作および社内適用によって評価した結果，1年半で約1万8,000個の仮想マシンが生成されるなど，提案手法の有効性を確認した。

木下 順史 | Kinoshita Junji
小澤 洋司 | Ozawa Yoji
阿久根 憲 | Akune Ken
Nazim Sebih

1. はじめに

クラウドコンピューティングやデータ分析，IoT（Internet of Things）などのさまざまな分野でOSS（Open Source Software）が業界標準となっている。デジタルトランスフォーメーションを実現するためには，それらOSSの活用や，顧客協創を通したオープンイノベーションが必要不可欠である。OSSは世界中の開発者や研究者のコミュニティによって開発されており，進化が速く技術的にも高度であるが，商用製品のようなサポートが受けられるとは限らず，ドキュメントが不足している場合もある。よってOSSを使いこなすためには，日頃からOSSの活用やコミュニティへの参画・貢献を実践し，ノウハウの蓄積や人材の育成を行う必要がある。

一方，企業におけるOSS活用には高いハードルがある。昨今のOSSはインターネットサービスとの連携が前提となっており，企業のセキュリティポリシーに準拠できない場合がある。さらに，多種多様で進化の速いOSSを活用するために，それらの運用管理が必要となる。このような課題を解決するために，社内から隔離された環境の構築や手作業での運用管理が行われてきたが，使い勝手が悪く，OSSの活用が進まなかった。

そこで本稿では，SDN[1)]（Software Defined Network）技術やChatOps[2)] による運用自動化技術を用いて課題を解決することで，OSSを活用してクラウドサービスを実現する手法を提案する。さらに，試作および社内適用を行った結果と今後の展望を示す。

2. 企業におけるOSS活用の課題

2.1 既存セキュリティポリシーとのギャップ

昨今のOSSは，インターネット上のソフトウェアリポジトリやWebサービスへの接続を前提とするなど，インターネットサービスとの連携が必要不可欠である。

一方で企業や組織においては，機密情報漏えいやマルウェア感染などのセキュリティ事故を防ぐために，厳格なセキュリティポリシーを規定して社内ネットワークを保護している。特にインターネットサービスとの連携は，ファイアウォールやWebフィルタリング，認証プロキシなどによるアクセス制御や閲覧制限を行うのが一般的である。OSSの中には，そのような厳格なセキュリティポリシーの下での利用を想定していないものがあり，例えばプロキシ環境下で動作しないなどの問題が発生する。

2.2 多種多様なOSSの運用管理

企業や組織において必要となるOSSには多種多様なものがある。例えばIaaS（Infrastructure as a Service）を実現するOpenStack[3), ※1)]や，PaaS（Platform as a Service）を実現するCloud Foundry[4), ※2)]，コード管理のためのGitLab[5), ※3)]，プロジェクト管理のためのRedmine[6)]，継続的インテグレーションのためのJenkins[7), ※4)]，コミュニケーションのためのRocket.Chat[8)]などが挙げられる。日々新しいものが現れ，進化が速く移り変わりが激しい。

一方で企業や組織においては，長期サポートのある商用ソフトウェアや社内独自開発のソフトウェアを中心とした業務システムを構築して運用体制を確立しており，そのような多種多様で移り変わりの激しいOSSを管理しきれないという問題がある。

さらに，OSSの中にはマルチユーザーで利用可能なものや，サーバ仮想化技術やコンテナ技術を用いてマルチテナントで利用可能なものもあり，誰が何をどの程度使っているのかを管理するのが難しい。管理せず放置すると，実際には使用されていない計算機リソースによってコストが増大し，管理されていない計算機リソースから情報が漏えいするなどのセキュリティリスクも増大する。

2.3 従来の取り組み（隔離環境の構築と手動運用）

上述の問題に対処すべく，社内環境から隔離された特別な環境を設けてインターネットサービスとの連携を許可し，特例としてメールベースでの利用申請や台帳管理を行うなどの施策が行われてきた。しかし，このような隔離環境では，社員が日常使用している社内ネットワークからの利用や，社内ネットワークとの間のデータのやり取りができず，社内審査のために利用開始に時間がかかるなど，使い勝手の悪さに起因して利用者の生産性やモチベーションが下がり，結果としてOSSの活用が進まない。

また，多種多様なOSSや，生成・破棄が繰り返される仮想マシンやコンテナ，それらが行うさまざまな通信プロトコルなどを手動で台帳管理するのは困難である。結果として運用が形骸化し，運用ミスや管理漏れなどが発生しやすい。

3. OSSで実現するクラウドサービス

従来手法の課題を解決するために，SDN技術やChatOpsによる運用自動化により，社内外と連携可能，かつ迅速に利用可能なプライベートクラウドとしてOSS活用環境を実現する（**図1**参照）。

3.1 SDN技術を用いた社内外との連携技術

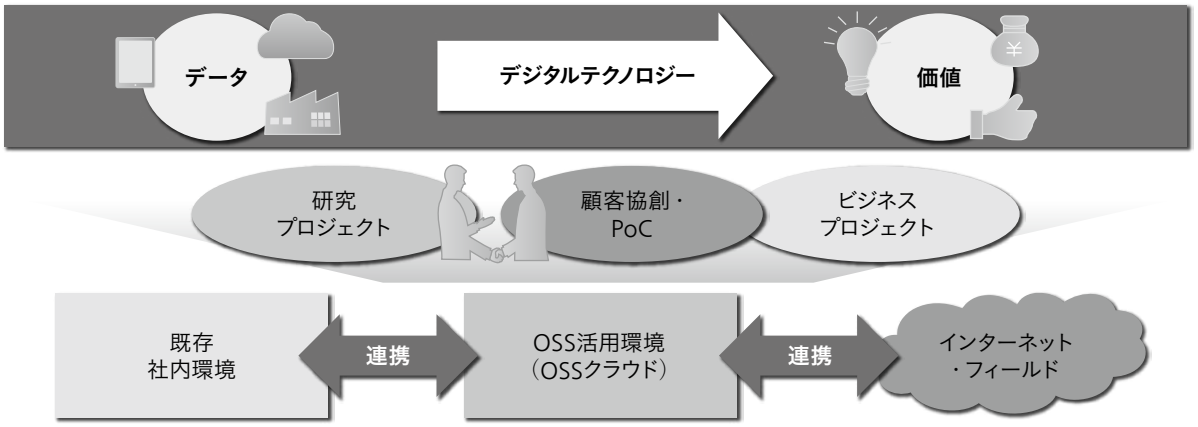
隔離環境に起因する課題を解決すべく，OSS活用のためのプライベートクラウドを社内ネットワークとインターネットの間のDMZ（Demilitarized Zone）領域に設け，利用者やプロジェクトなどのテナント間をVXLAN［Virtual Extensible LAN（Local Area Network）］[9)]などのネットワーク仮想化技術を用いて論理分離する。また，DMZを構成するファイアウォールをSDN制御することで，社内外とのセキュアかつオンデマンドでの連携を実現する（**図2**参照）。

DMZ環境に設置することで，社内ネットワークからのプライベートクラウド利用，およびプライベートクラ

※1) OpenStackは，米国とその他の国におけるOpen Stack Foundationの登録商標または商標である。
※2) Cloud Foundryは，CloudFoundry.org Foundationの米国および各国での登録商標または商標である。
※3) GitLabは，Gitlab BVの米国およびその他の国における登録商標または商標である。
※4) Jenkinsは，Software in the Public Interest, Inc.の登録商標である。

図1｜OSSクラウド

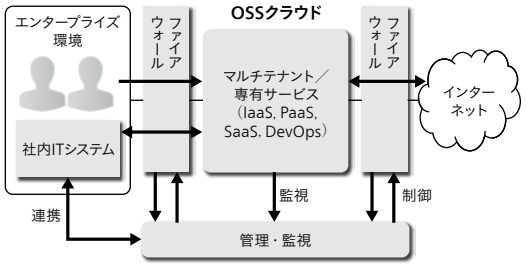
社内外と連携可能なプライベートクラウドとしてOSS活用環境を設置し，OSS活用や顧客協創を通したオープンイノベーションを実現する。



注：略語説明
PoC（Proof of Concept），OSS（Open Source Software）

図2｜SDN技術を用いた社内外との連携技術

社内外と連携可能なプライベートクラウドとしてOSS活用環境を設置し，社内認証基盤と連携して個人粒度での通信監視および制御を実施した。



注：略語説明
IaaS（Infrastructure as a Service），PaaS（Platform as a Service），SaaS（Software as a Service）

ウドとインターネットサービスとの連携を両立する一方，社内ネットワークとインターネットサービス間の直接的な連携を抑止できる。

また，プライベートクラウドを社内認証基盤などの既存社内運用管理システムと連携させる。これにより，社員が既存のIDを用いてOSSを使い始められるとともに，社員のIDや組織情報，属性情報と，プライベートクラウド上の利用リソース，およびネットワーク通信を関連付けることができる。それらの関連付けを利用し，個人粒度での通信の利用状況監視や異常検知を行い，監視結果や検知結果を基に社内ネットワークとプライベートクラウド，プライベートクラウドとインターネット間のファイアウォールをSDN制御することで，個人粒度でのアクセス制御や監査を行う。

通信の異常検知においては，近年HTTPS（Hypertext Transfer Protocol Secure）などの普及によって暗号化通信が増加しており[10), 11)]，さらにそれら一般的なWebプロトコル上で双方向通信が行われることから，通信パケットのペイロードを分析することが難しくなっている。そこで，通信の統計情報を基にした通信の挙動分析を行うことで，暗号化の有無にかかわらず通信の異常検知を行う。

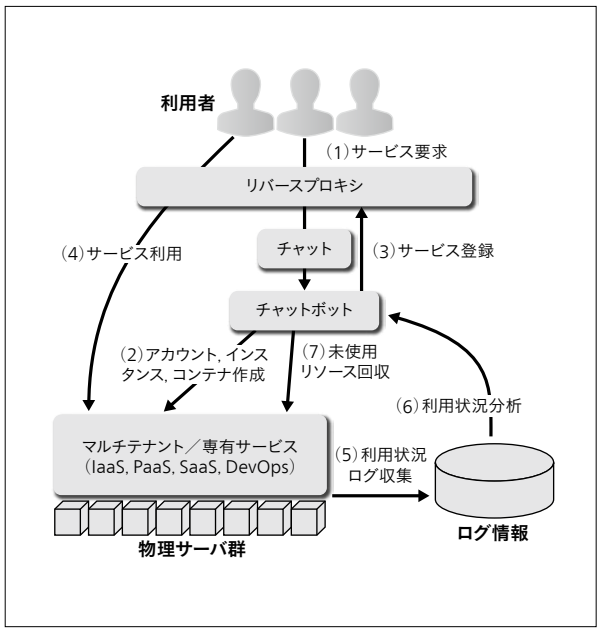
3.2 ChatOpsによる運用自動化技術

手動運用に起因する課題を解決すべく，ChatOpsによる多種多様なOSSの利用および運用自動化を行う。具体的には，社員がチャット上で，チャットボットと呼ばれるソフトウェアに対話形式で各種OSSの利用開始や停止を要求し，要求を踏まえてチャットボットが各種OSSのAPI（Application Programming Interface）と連携してアカウントやインスタンス，コンテナ，プロジェクトなどを作成することで，セルフサービスかつオンデマンドでの利用を実現する（**図3**参照）。

ChatOps形式にすることで，社員が迅速に各種OSSを利用開始できるとともに，チャット上でそれらOSSの活用ノウハウや関連情報の共有をシームレスに実施することができ，利用者間での問題解決やコラボレーションの促進につながる。

また，チャットにログインした社員のIDや組織情報，属性情報と，各種OSSやプライベートクラウド上のアカウント，リソースを関連付けることで，個人粒度での利用状況の計測および管理を行う。さらに，計測した利用状況を基に，実際には使用していない計算機リソースの

図3｜ChatOpsによる運用自動化技術
チャットボットによりサービス利用を自動化し，未使用リソースを削除する。



自動検出および自動回収を行う。

未使用リソースの自動検出においては，利用者によってOSSの種類やバージョン，システム構成，ワークロードが異なるため，閾（しきい）値による使用有無の判定は困難である。そこで，機械学習を用いて判定を行う。

4. 試作および今後の展望

前章で示した解決方式の有効性を評価すべく，日立の研究開発部門とIT部門が協力し，OSSを活用する環境をプライベートクラウドとして社内に構築するとともに，2015年9月に社内サービスとして公開した（以下，「OSSクラウド」と記す。）。OSSクラウドそれ自体も，OSS活用のノウハウを蓄積すべく，すべてOSSを活用して実装した。具体的にはIaaS環境としてOpenStack，PaaS環境としてCloud Foundry，DevOps環境としてGitLabやRedmine，Jenkins，Rocket.Chatなどを提供し，それらすべてをChatOpsで利用可能とした。ChatOps実現にあたっては，チャットボットのOSSフレームワークであるHubot [12), ※5)] を用いた。

また，SDN技術を用いた社内外との連携技術やChatOpsによる運用自動化技術についても試作を行い，OSSクラウドに適用した。

2015年7月～2017年2月におけるOSSクラウド上での仮想マシンの生成数の推移を**図4**に示す。2015年9月にプライベートクラウドとして社内公開して以降，急速に利用が増加しており，2017年2月時点で累計約1万8,000個の仮想マシンが生成された。仮想マシン以外にも，社内の数百人が利用し，数百のプロジェクトが生成され，そのうち37%のプロジェクトが複数部署にまたがるコラボレーションプロジェクトであるなど，提案手法によってOSS活用を促進できていることを確認した。

提案方式の試作および社内適用結果を踏まえ，Lumadaへの展開を始めとして，今後は開発技術の事業適用をめざす。

5. おわりに

既存のセキュリティポリシーとのギャップや多種多様なOSSの運用管理など，企業においてOSSを活用するうえでの課題を，SDN技術やChatOpsによる運用自動化技術によって解決し，OSSの活用を促進するクラウド

※5) Hubotは，GitHub, Inc.の商標である。

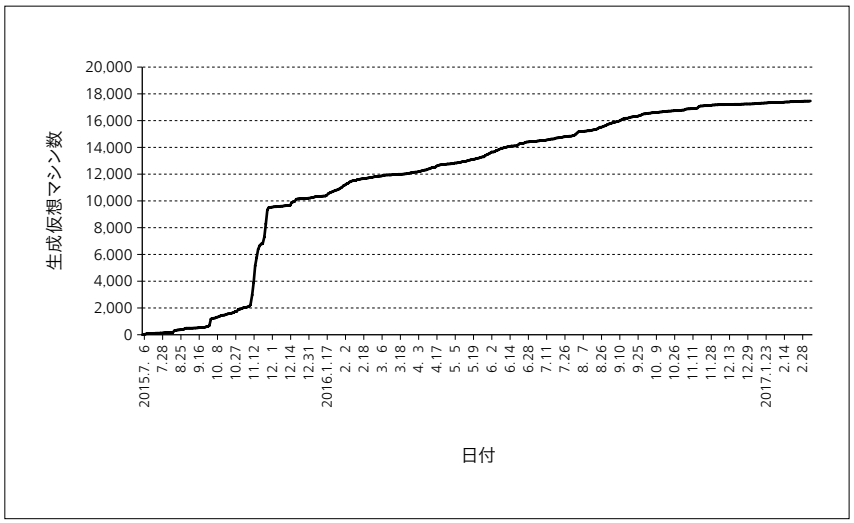


図4｜OSSクラウド上での生成仮想マシン数の推移
2015年7月～2017年2月の期間にOSSクラウド上で作成された仮想マシン数の推移を示す。

サービスを実現する手法を提案した。また，試作および社内での適用を通して提案手法の有効性を確認した。

今後は顧客協創を通したオープンイノベーションに適用し，顧客のデジタルトランスフォーメーションを実現する。

参考文献など

1）E. Haleplidis (Ed), et al.: Software-Defined Networking (SDN): Layers and Architecture Terminology, IRTF, RFC7426 (2015.1), https://tools.ietf.org/html/rfc7426

2）Rubyfuza, ChatOps at GitHub - Jesse Newland, https://www.youtube.com/watch?v=NST3u-GjjFw

3）OpenStack, The OpenStack Foundation, https://www.openstack.org/

4）Cloud Foundry, The Cloud Foundry Foundation, https://www.cloudfoundry.org/

5）GitLab, https://about.gitlab.com/

6）Redmine, http://www.redmine.org/

7）Jenkins, https://jenkins.io/

8）Rocket.Chat, https://rocket.chat/

9）M. Mahalingam, et al.: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, IS, RFC7348 (2014.8), https://tools.ietf.org/html/rfc7348

10）HTTPS as a ranking signal, Google Online Security Blog, http://googleonlinesecurity.blogspot.jp/2014/08/https-as-ranking-signal_6.html

11）GoogleでのHTTPSへの対応, https://www.google.com/transparencyreport/https

12）Hubot, https://hubot.github.com/

執筆者紹介

木下 順史
日立製作所 研究開発グループ 情報通信イノベーションセンタ
クラウド研究部 所属
現在，OSSを用いたクラウド運用管理技術の研究に従事

小澤 洋司
日立製作所 研究開発グループ 情報通信イノベーションセンタ
クラウド研究部 所属
現在，OSSを用いたクラウド運用管理技術の研究に従事
電子情報通信学会会員

阿久根 憲
日立製作所 研究開発グループ 情報通信イノベーションセンタ
クラウド研究部 所属
現在，OSSを用いたクラウド運用管理技術の研究に従事
電子情報通信学会会員

Nazim Sebih
日立製作所 研究開発グループ 情報通信イノベーションセンタ
クラウド研究部 所属（執筆時）
OSSを用いたクラウド運用管理技術の研究に従事