SoE時代のサービスの信頼を支えるクラウドネットワーク運用管理技術

Cloud Network Operation Management Technology to Support Trust of Services in Age of SoE

小口　直樹　　朝永　博　　上野　仁　　青木　泰彦

あらまし

企業と顧客とのつながりを作り，維持し，信頼関係を醸成するためのICTシステムであるSoE（Systems of Engagement）は，組織内の基幹業務を支えるICTシステムであるSoR（Systems of Record）並みの可用性に加え，ビジネスの変化に対応する柔軟性，迅速性が求められる。SoEが提供するサービスがより多くの利用者に使われるためには，利用者の安心感につながるセキュリティや十全性をシステムが満たしていることが不可欠である。しかし，サービス開発者がシステム全体の構成や要件を把握することは一般的に難しく，サービスを改良するたびにそのサービスに応じたセキュリティや性能を考慮して，システムを再設計するのは困難であった。そこで富士通研究所では，このようなサービス開発者でもマルチクラウド環境下で安心なサービスを迅速かつ柔軟に提供できるように，SoEの構築や安定運用を支援する仕組みを開発している。

本稿では，システム全体を把握していないサービス開発者でもセキュアなシステムを構築できるように支援するNaC（Network as Code）技術とネットワークベリフィケーション技術を紹介する。また，SoEシステムにおける障害や性能劣化を早期に認識し，十全性を提供可能とするトラフィック予測技術とアノマリ検知技術を紹介する。

Abstract

Systems of engagement (SoE)—ICT systems for creating and maintaining connections between companies and customers and building trust—are required to offer flexibility and quickness in responding to changes in business, in addition to availability comparable to that of systems of record (SoR), which are ICT systems that support the mission-critical operations in an organization. For services provided by SoE to be used by more users, a system must essentially satisfy the security and integrity requirements that allow for a greater sense of security in users. However, grasping the configuration and requirements of an entire system is generally difficult for service developers, and it was difficult to redesign a system giving considerations to the security and performance based on the service every time improvements were made to the service. Therefore, Fujitsu Laboratories has developed a system of building SoE and supporting stable operations so that such service developers can quickly and flexibly provide a secure service in a multi-cloud environment. This paper presents the Network as Code (NaC) and network verification technologies that assist even those service developers who lack an understanding of the entire system with the construction of a secure system. It also describes traffic prediction and anomaly detection technologies, which promptly recognize any failures and performance degradation in an SoE system to allow for the provision of integrity.

1. まえがき

これまでのICTシステムは，企業の基幹系システムや個人情報を扱うシステムなど，正確かつ安定した動作が求められるものが主流であった。そのため，冗長化を講じた設計や十分なテストがなされた上で，構築・運用されてきた。このようなシステムはSoR（Systems of Record）と呼ばれている。

一方，近年のWeb技術やクラウドを中心とした仮想化・コンテナ技術の進展に伴い，ビジネスの変化も速くなっている。ユーザー満足度を高め，ビジネスを優位に進めるためには，顧客からのフィードバックを素早くシステムに反映し，アップデートし続けられることが必要となる。このようなシステムはSoE（Systems of Engagement）と呼ばれている。

SoEでは，これまでとは異なるシステムの信頼性（Trust）が求められる。ここでのTrustとは，システムがデータ的に安全であるセキュリティのみならず，所定の応答時間や性能を満たす十全性の両方を提供することを指す。[(1)] SoEでは，構成されるシステムに合わせて，これらのTrustを柔軟かつ迅速に提供できる仕組みが求められる。

そのためには，まずサービスを更新するたびにサービスの規模や内容，および提供フェーズに応じて，セキュリティの変更や，他のサービスとのセキュリティの違反（バイオレーション）がないかといった安全性の確保が必要になる。システム全体の構成や要件の把握が難しいサービス開発者でも，簡単かつ柔軟にセキュリティ要件を満たすシステムを構築できる仕組みが必要となる。

他方，クラウドなどの仮想インフラにおいては，様々なSoEが多重化されていることに加え，適切なツールが揃っていないため，サービス開発者が障害箇所や性能劣化の要因を特定することが困難であった。そのため，より早期に障害やリソース不足の要因を特定しこれに対処あるいは回避し，十全性を実現する技術が必要となる。

富士通研究所は，このようなサービス開発者でもマルチクラウド環境下で安心なサービスを迅速かつ柔軟に提供できるように，SoEの構築や安定運用を支援する仕組みを開発している。

本稿では，まずシステム全体を把握していないサービス開発者でもセキュアなシステムを構築できるよう支援する，NaC（Network as Code）技術とネットワークベリフィケーション技術を紹介する。更に，SoEにおける障害や性能劣化を早期に認識し，十全性を提供可能とするクラウドネットワーク分析技術を紹介する。

2. SoEに求められる信頼性

一般的に，SoEは，仮想マシンや仮想ネットワークなどにより構成された仮想インフラ上に，コンテナで構成される様々なマイクロサービスを配置し，これらを仮想ネットワークでつなぎ合わせることで動作するクラウドネイティブなビジネスシステムである。そして，システムの提供・顧客フィードバック・システム修正といった開発サイクルを短期間に繰り返し，顧客に提供するサービスをすみやかに改善していく。サービスの改善には，安全性の確保を目的として，コンピューティングやネットワーク設定に関する広範なノウハウが必要となり，専門のスタッフを用意したり，委託したりするなどコストと時間がかかる作業となる。

3. 信頼レベルに応じて迅速なサービスを提供する仮想ネットワーク構築・検証技術

本章では，信頼レベルに応じてSoEを迅速に構築するNaC技術，および構築したシステムのセキュリティ設定の整合性を担保するネットワークベリフィケーション技術について説明する。

3.1 NaC技術の概要

SoEでは，独立した多数の機能（マイクロサービス）を組み合わせてサービスを構成する。一つのモジュールで構成されたモノリシックなシステムと比べ，各機能を疎結合で構築しておくことで，マイクロサービスごとに適したスピードで進化できるようになる。その結果，システム全体が環境の変化に追従しやすくなる。

一方で，サービス数が増加するだけでなく，各サービスが頻繁に更新されるようになり，更新され

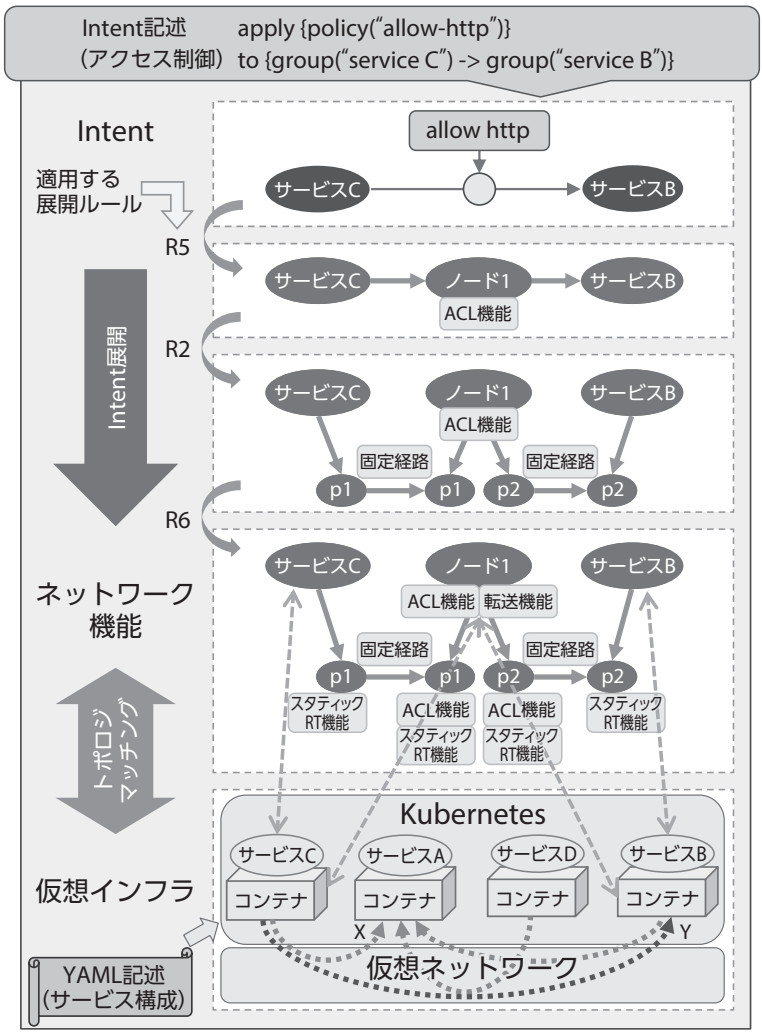
たサービスの実行マシンがその都度決定されるため，頻繁に実行マシンが変わる。そのため，各サービス間を結合する仮想ネットワークでは，マイクロサービス導入の利点である柔軟性やアジリティを阻害しないように，サービス実行マシンの位置に合わせて接続を変える必要がある。

そこで，サービスの構築に必要な接続性やアクセス制御，信頼レベルといった，サービス開発者自身の多様な要求をIntent（意図）として記述するだけで，各仮想ネットワークに必要な詳細レベルの機能や設定を自動的に導出する仕組みが，NaCである（図-1）。例えば，あるサービスは特定のサービスからしか利用できない，開発段階なので障害時は停止して良い，といったものがIntentである。これらを示すだけで，コンテナや仮想ネットワークで構成される仮想インフラの構成などを意識せずに，低コストかつ迅速にマイクロサービス間を接続できるようになる。

3. 2 NaCの実現方式

まず，様々な仮想インフラの構成に対応して自動的に設定を導出するために，仮想インフラの構成に依存しない手順（Intent展開）と依存する手順（トポロジマッチング）に処理を分離する（図-1）。

Intent展開とは，Intentからネットワーク機能およびそれらのつながりを導出するフェーズであり，Intentを展開ルールに当てはめることで機能を導出する。ここで，単一の展開ルールでサービス開発者



RT：Route

図-1　NaCの実現方式とユースケース

の多様なIntentに対応しようとすると，ルールが複雑化してしまうという問題がある。そこで，シンプルな展開ルールを複数定義し，Intentに応じて展開に使用するルールをサーチしながら，検出したルール（図-1ではR5，R2，R6）を順次適用して徐々に展開を進めていく。これによって，展開ルールを複雑化することなく，ルールの組み合わせで様々なIntentに対応可能となる。

次に，トポロジマッチングについて図-1下部に示す。Intent展開で導出した機能のつながりと，実際の仮想インフラの構成を照らし合わせ，その機能を実施する構成要素を決定していく。機能配備が決まると，その機能を実現するための設定およびパラメータを導出し，仮想ネットワークに設定を行う。このようにしてIntent展開とトポロジマッチングを進め，ネットワーク設定を自動導出する。

ここで，マイクロサービスのオーケストレーションプラットフォームとしてデファクトスタンダードになりつつあるKubernetesでは，YAMLファイルに記述されたサービスの構成情報に基づいて，コンテナの配備が決定される。更に，依存する各サービス間でAPI（Application Programming Interface）のアクセス制御を行う必要がある。そこで，ここにNaCを用いることで，このアクセス制御をネットワークが満たすべき状態として記述するだけで自動構築できる。

3.3 マイクロサービスでのユースケース

本節では，マイクロサービス環境におけるNaCのユースケースについて述べる。

例えば，サービスAの提供するAPIエンドポイントXに対して，任意のサービスがアクセス可能であり，サービスBの提供するAPIエンドポイントYに対しては，サービスCからのみアクセス可能という状態が，既に記述されていたとする。ここで，サービスCからサービスBへのhttpアクセスを許可したい場合，この状態を図-1に示した吹き出しのようにIntentとして記述する。この記述を基に，NaCがネットワークへの設定を自動導出・設定し，サービスCからサービスBへのhttpアクセスが許可される。

これによって，ビジネスや環境の変化に応じたSoEを即座に実現できる。

3.4 ネットワークベリフィケーション技術の課題

本技術は，仮想ネットワーク内に複数配置されるルータやファイアーウォールの中継テーブル，あるいはAccess Control List（ACL）と呼ばれるフィルターの内容を収集し，システム全体の整合性を検証する技術である。

ACLは基本的に，5タプル（Source IP, Source Port，Destination IP，Destination Port，Protocol）で表現される。ここで，Source IPとSource PortはTCPまたはUDPプロトコルを用いた通信における送信元アプリケーションのIPアドレスおよびポート番号，Destination IPとDestination Portは送信先アプリケーションのIPアドレスおよびポート番号，ProtocolはTCPかUDPかを識別するプロトコル番号を表す。

大規模な仮想インフラ上にサービスを構築した場合，システム内に含まれる複数のファイアーウォールにACLを設定する必要がある。その際，複数のファイアーウォールにおいて設定の整合性が取れていないと，マイクロサービス間で通信ができなかったり，サービスが危険にさらされたりする可能性がある。

また，様々なサービスが仮想インフラに多重化されている場合，異なるサービス開発者が矛盾するIntent設定を行う可能性がある。その際，各開発者は，自分の開発したサービスで生じる通信が各ファイアーウォールを通過できるように，ACLを設定する必要がある。しかし，ほかの開発者のACL設定と矛盾する内容で既存設定を上書きしてしまうと，ほかのサービスを阻害する可能性がある。

例えば，図-2において，開発者＃1が，サービスで生じる通信＃1（セッション＃1）が通過できるようにファイアーウォールFW1，FW2にそれぞれACL11，ACL12を設定したとする。それを知らずに，開発者＃2が，サービスで生じる通信＃2（セッション＃2）が通過できるようにFW2，FW3にそれぞれACL21，ACL22を設定してしまう可能性がある。その結果，ACL21がACL12と矛盾した設定である場合，セッション＃1が通過できなくなってしまう可能性がある。このように，システムの中に多数のファイアーウォールがあり，様々なサービス

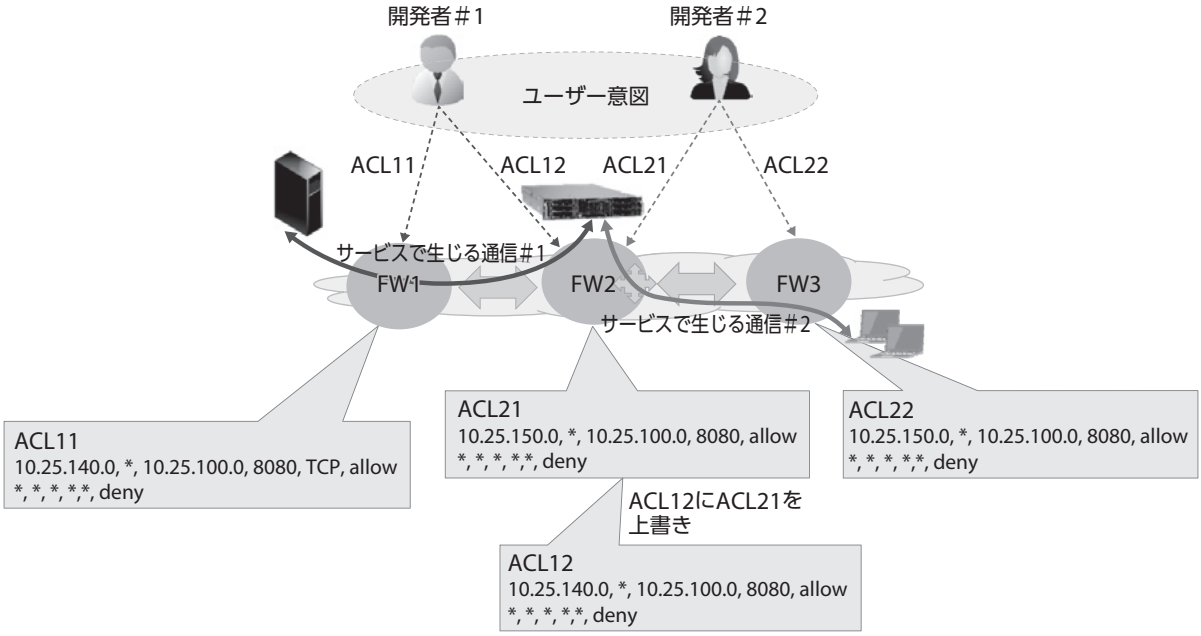


図-2　ファイアーウォール設定の課題

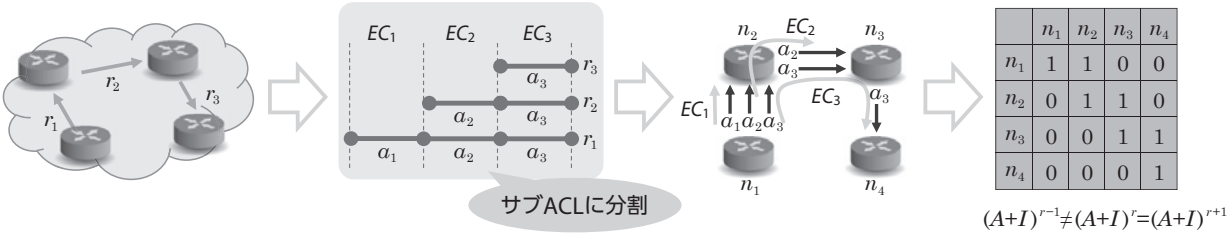


図-3　ネットワークベリフィケーション技術の仕組み

で生じる通信が通過できるようにしている場合，人間がこれらのルール間の整合性，重複，矛盾を全てチェックすることは困難である。

こうした課題に対して，本技術はネットワークやシステムの設定が正しいかどうかを数学的に検証し，あらゆるパケットの振る舞いを予測する。具体的には，以下を行う（図-3）。

(1) ネットワーク内のデバイスから設定情報（ACL）を収集する。
(2) 全てのACLを，アドレス範囲が重複しない互いに素なアドレス範囲（Equivalence Class：EC）に相当するサブACLに分割する。
(3) サブACLを使ってシステム内の全ACLをフォワーディンググラフとして表す。
(4) フォワーディンググラフを行列で表現し，可到達行列を演算することで到達性の不整合をチェックする。

以上を設定変更が行われるたびにリアルタイムに演算することで，実際にパケットが流れる前に設定の矛盾を見つけることが可能になる。

4. クラウドネットワーク分析技術

本章では，SoE時代に不可欠な，サービス提供者の要件に応じた十全性を提供可能にする，クラウドネットワークの分析技術について述べる。

4.1 基本的な考え方

サービスを安定稼動させるためには，仮想マシン（VM）やVM間を接続する仮想ネットワークの振る舞いに加え，VMで稼動するコンテナの振る舞いなども用いて，障害要因を早期に特定し，切り分けることが重要となってくる。特に今後，システムの大規模化やクラウドサービスの多様化が進むにつれて，従来のような計測パラメータごとの固定のしきい値設定，あるいは熟練した運用者のノウハウに基づく監視では対応できなくなることが予想される。そのため，VMや仮想ネットワークなどから収集されるリアルタイムデータに対して，機械学習などのAI（人工知能）技術を活用したシステムやネットワーク運用管理の高度化が期待されている。

サービスの安定稼動を妨げる要因には，運用者による設定ミス，ソフトウェアバグの顕在化，ハードウェア故障などの不具合が考えられるが，全てのコンポーネントの振る舞いを常時監視することは難しい。しかし，例えばあるコンポーネントがスローダウンすると，サービスとしてのレスポンス低下やトラフィック急減として現れる。このように，各コンポーネントの異常はサービスレベルの通信異常となって顕在化すると考え，サービスおよび仮想ネットワークに対して，トラフィック予測技術およびトラフィックアノマリ検知技術を適用する。

4.2 アーキテクチャー

提案手法のシステムアーキテクチャーを図-4に示す。コンテナを含むサービスの品質情報については，OSS（Open Source Software）であるIstioコントローラ[(2)] から取得し，サービスの応答時間およびその変動を算出する。また，ネットワークの品質情報については，富士通研究所が開発したトレースパケット抽出部とパケット性能分析サーバを用いて，パケットのロス率やトラフィック量を算出する。トレースパケット抽出部は，仮想ネットワークからキャプチャしたパケットをリアルタイムにサービスごとにグルーピングし，サービスごとパケットDBに格納する機能を提供する。パケット性能分析サーバは，パケットの応答遅延やパケットロス率などを算出する機能を提供するものである。そして，統合性能分析部はサービスの品質情報とネットワー

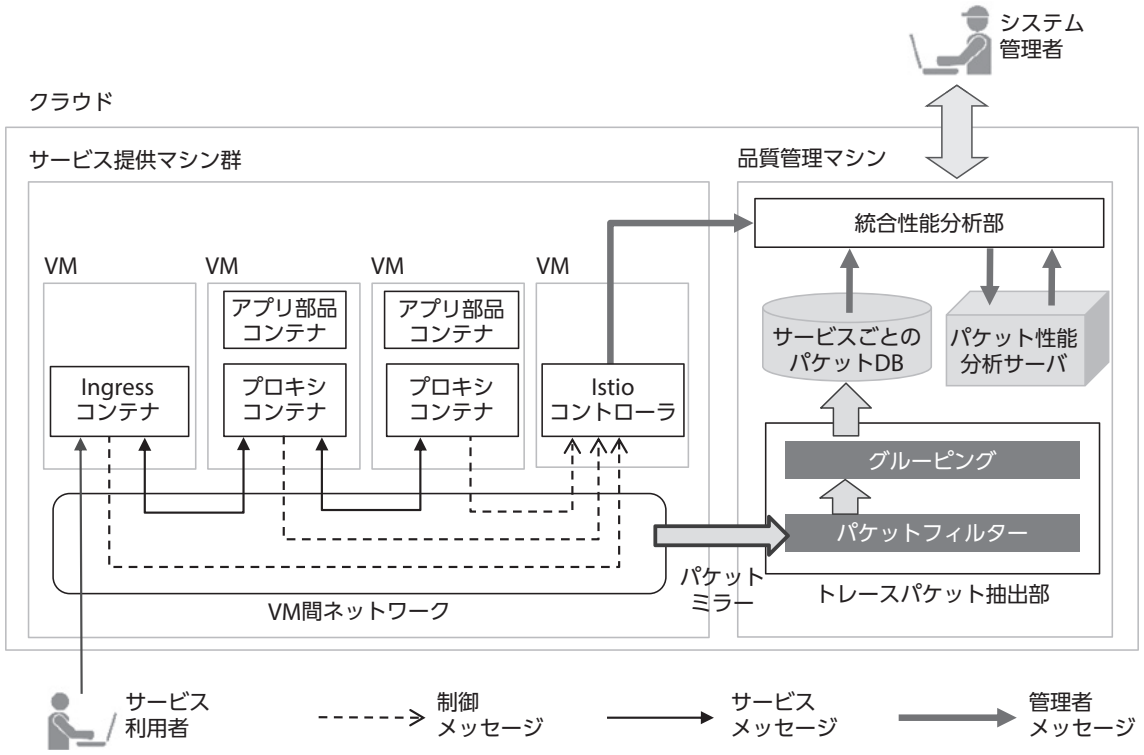


図-4　提案システムアーキテクチャー

クの品質情報の両方を集約し，次節で示すようなトラフィック予測やアノマリ分析の機能を提供する。このように，サービスとネットワークという種類の異なる品質情報を収集・算出する機能と，それらを統合した全体分析を行う機能を分離しておくことで，新たな分析手段の追加，拡張を容易にするアーキテクチャーとした。

4.3 トラフィック予測技術

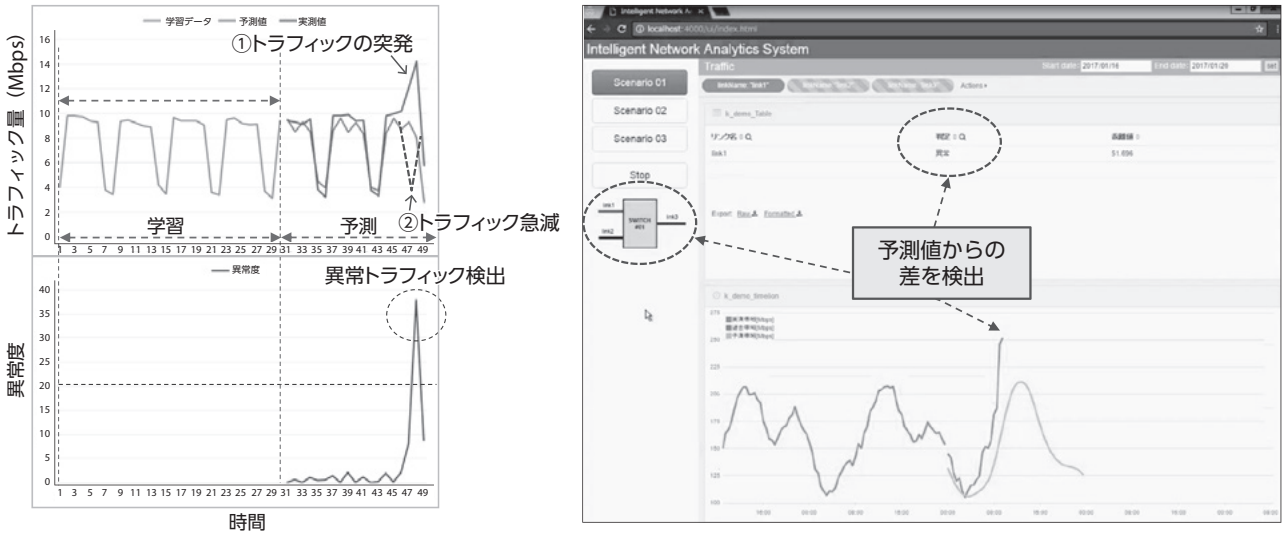
本節では，仮想ネットワークを対象に高精度なトラフィック変化検知を実現する手段として，ARIMA（Autoregressive Moving Average Model）モデルを活用したトラフィック予測技術について紹介する。この技術では，まずトラフィックのように時間変化する観測対象に対して，過去の時系列データの自己相関や移動平均から，周期パターンおよびそのトレンドをモデル化する。次に，将来時刻に対する自己回帰予測を行い，その予測と実測との差分を判定することで，変化を検知する。(3)

今回開発したモデルから予測したトラフィックと，トラフィック予測との差から検出したトラフィック異常の結果を，図-5に示す。図-5（a）は，予測したトラフィックと実際のトラフィックとの差を異常度として示している。また図-5（b）は，この異常度をGUI上に表記した例である。このように，通常と異なる振る舞いを素早く検知できるようにすることで，VMやコンテナの再配備などをいち早く推奨できるようになる。

4.4 トラフィックアノマリ検知技術

異常検知の手法には，前節で述べた時系列データに対する手法のほか，パケットキャプチャデータなど，ある計測値における分布の変化に着目することによって，通常と異なる状態を検出する手法もある。このようなパケットキャプチャなどの計測値監視を，サービスやVM，VM間ネットワークに適用するためには，熟練した仮想インフラの運用スキルが必要となる。そのため，サービス開発者にとって多大な時間を要する困難な作業となる。

そこで富士通研究所は，外れ構造検知技術(4) を応用したトラフィックアノマリ検知技術を開発した。具体的には，仮想アプライアンスとして提供されるパケットキャプチャ機能から得たログデータにこの技術を適用し，通常のネットワーク動作とは異なる挙動を示すログデータを検出する。異常度ランキングを基にしたキャプチャデータの分析結果およびその統計情報のGUIを，図-6に示す。この図では，開発した技術により異常度が最も高いと検出されたパケットキャプチャデータの集合（クラスタ）について，拠点Aと拠点Bでそれぞれ実際にとらえてい



（a）予測値と実測値との差　　（b）異常度の表記例

図-5　トラフィック予測事例

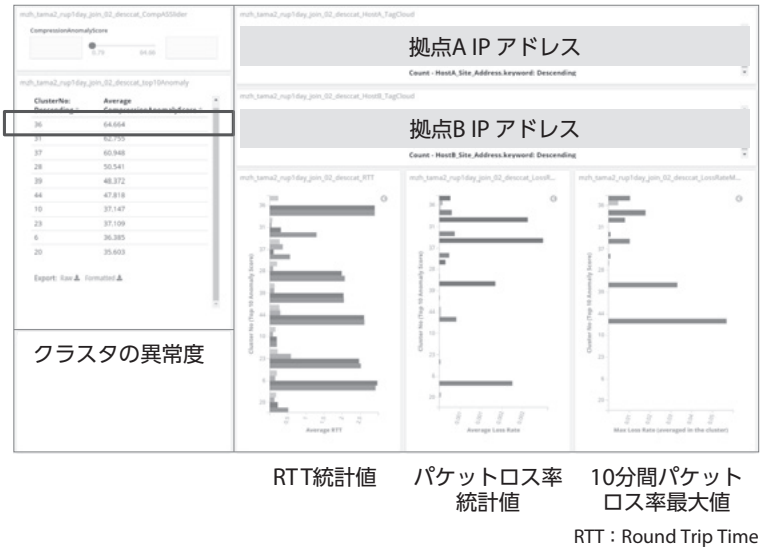


図-6　アノマリ検知GUI

る事象を，測定データとして可視化している。

これによって，システム全体を把握していないサービス開発者が，特定の障害要因を探るために，膨大なキャプチャデータの中を細かく調べることなく，サービス影響につながるログを優先的に分析可能となる。そして，異常が発生している可能性のあるリソースを回避したシステムの作り直しなどが可能となる。

5. むすび

本稿では，SoE時代において，システム全体の構成や要件の把握が困難なサービス開発者でも，簡単に安心なサービスを構築・運用できるよう支援する技術について述べた。具体的には，マルチクラウドに跨がって仮想ネットワークを迅速に構築するNaC技術と仮想ネットワークを検証するネットワークベリフィケーション技術，NaCが構築した仮想ネットワークの異常検知から要因特定までを行うトラフィック予測・アノマリ分析技術について紹介した。

今後は，「お客様の業務の特性すなわちトランザクション保証重視か，処理スループット重視かなどの特性」と，「お客様が必要とする信頼性の高さ」に応じ，これらの技術を適切に組み合わせて簡単に提供することも想定している。これらの技術を，機械学習などのAI（人工知能）技術も活用した次世代型のサービス運用プラットフォーム（スイート）として発展させ，2020年度の提供を目指していく。

参考文献

(1) 宮西洋太郎ほか：“情報システムの「安心性」評価モデルの提案”．信学技報，Vol.116，No.200，SWIM2016-9，p.15-22，2016年8月．
(2) Istio.
https://istio.io/
(3) S. Yamashita et al.：Analytics Framework for AI-based Network Operation and Management. IEICE ソサエティ大会（2017）．
(4) 丸橋弘治ほか：外れ構造検知：大規模離散値データの圧縮による集団アノマリの発見．DEIM Forum（2017）．
https://db-event.jpn.org/deim2017/papers/64.pdf

著者紹介

小口　直樹（おぐち　なおき）
（株）富士通研究所
サービスビジネス開発運用・ユニット
マルチクラウド環境におけるSoEシステム運用に関する研究業務に従事。

朝永　博（ともなが　ひろし）
（株）富士通研究所
サービスビジネス開発運用・ユニット
マルチクラウド環境における仮想リソース分析に関する研究開発に従事。

上野　仁（うえの　ひとし）
（株）富士通研究所
サービスビジネス開発運用・ユニット
マルチクラウド環境におけるサービス品質分析に関する研究業務に従事。

青木　泰彦（あおき　やすひこ）
富士通（株）
ネットワークプロダクト事業本部
Beyond 5G/6G時代に向けたネットワークアーキテクチャーに関する研究に従事。