将来ネットワークアーキテクチャの具現化に向けた取り組み

5G/IoT（Internet of Things）時代には，社会基盤サービスの取込み，端末・トラフィックの大爆発，AI（人工知能）によるスマート化などさまざまなネットワークインパクトが予測されておりネットワークアーキテクチャの変革が求められています．本稿では，それらのインパクトを解決するあるべきネットワーク像を検討し，そのアーキテクチャと重要要素を具体化しPoC（Proof of Concept）による技術検証を行ったのでその取り組みについて紹介します．

安川 正祥[†1] /佐藤 裕昭[†2] /弘田 武志[†1]
東條 琢也[†1] /遠藤 乾市[†1] /笠原 康信[†3]
鈴木 裕志[†2]

NTTネットワーク基盤技術研究所[†1]
NTTネットワークサービスシステム研究所[†2]
NTTアクセスサービスシステム研究所[†3]

5つの要素技術

NTT研究所では5G/IoT（Internet of Things）本格時代を見据え，B2B2Xビジネスも含めた今後の社会基盤を担うことになるネットワークインフラのアーキテクチャと実現要素技術の検討を進めています．

本稿では，以下の５つの要素技術について報告します．

① 5Gトランスポートとして，自動運転や遠隔工場制御などの複数の社会インフラ基盤やIoTなどの新たなデジタルサービスを収容し，複数の事業者に特性の違う論理的なサービス網を切り出すことができる「ネットワークスライス技術」

② クラウド事業者が簡易なカタログをチューニングすることでクラウドアプリケーションとネットワークアプリケーションを連携させるサービスを自動生成できる「クラウドネイティブSDx（Software Defined Anything）* 制御技術」

③ サービスの迅速な提供とネットワーク全体でのリソース最適化を実現するためのIPレイヤと伝送レイヤをSDN（Software Defined Networking）コントローラから統合的に制御する「マルチレイヤSDN制御技術」

④ 5Gトランスポートを実現するうえで重要となる4K/8K，AR（Augmented Reality）/VR（Virtual Reality）に代表される高精細・高臨場の映像コンテンツを経済的かつ高品質に配信する「CDN（Contents Delivery Network）技術」

⑤ DDoS（Distributed Denial of Service）攻撃など大規模化・多様化するサイバー攻撃に対処するためにセキュリティの脅威情報をネットワーク事業者間で事前に取得・展開することによる攻撃の予防的な防御や，複数のネットワークのセキュリティ機能を連携させることによる検知・防御機能の強化を実現する「大規模化・多様化するサイバー攻撃に対処するネットワーク連携対処技術」

ネットワークスライス技術

ネットワークスライシングは，5G時代のネットワーク構成技術として，大容量パケット転送技術，超低遅延データセンタ接続技術と並ぶ主要な革新技術です．ネットワークスライシングは，サーバやルータなどの物理設備（物理資源）を仮想的に分割可能な資源（仮想サーバ，仮想リンク，仮想ネットワーク機能等）として管理し，それら仮想資源を組み合わせた仮想網（スライス）を共有物理設備上に構成する技術です（**図１**）．従来のVPN（Virtual Private Network）や仮想ルータ（Virtual Router）と異なる特長は，仮想回線だけではなく，仮想サーバ，仮想ネットワーク機能，仮想上位アプリケーション機能，仮想OSS（Operation Support Systems）/BSS（Business Support Systems）を柔軟に組み合わせ，プログラム制御可能なエンドエンドネットワークをクラウドサービス並みの即時性で構成できる点です．スライス使用者は，物理網の機能，階梯構成，運用ルールにとらわれず，ネットワーク機能や制御プロトコルを自由に選択し，自由な経路制御が可能です．

極端な例では，IoT事業者による非イーサネット，非IPの使用や，コンテンツ配信事業者による国際標準では

＊ SDx：ITインフラの資源（サーバ，ストレージ，ネットワーク等）をソフトウェアから制御する技術の総称．

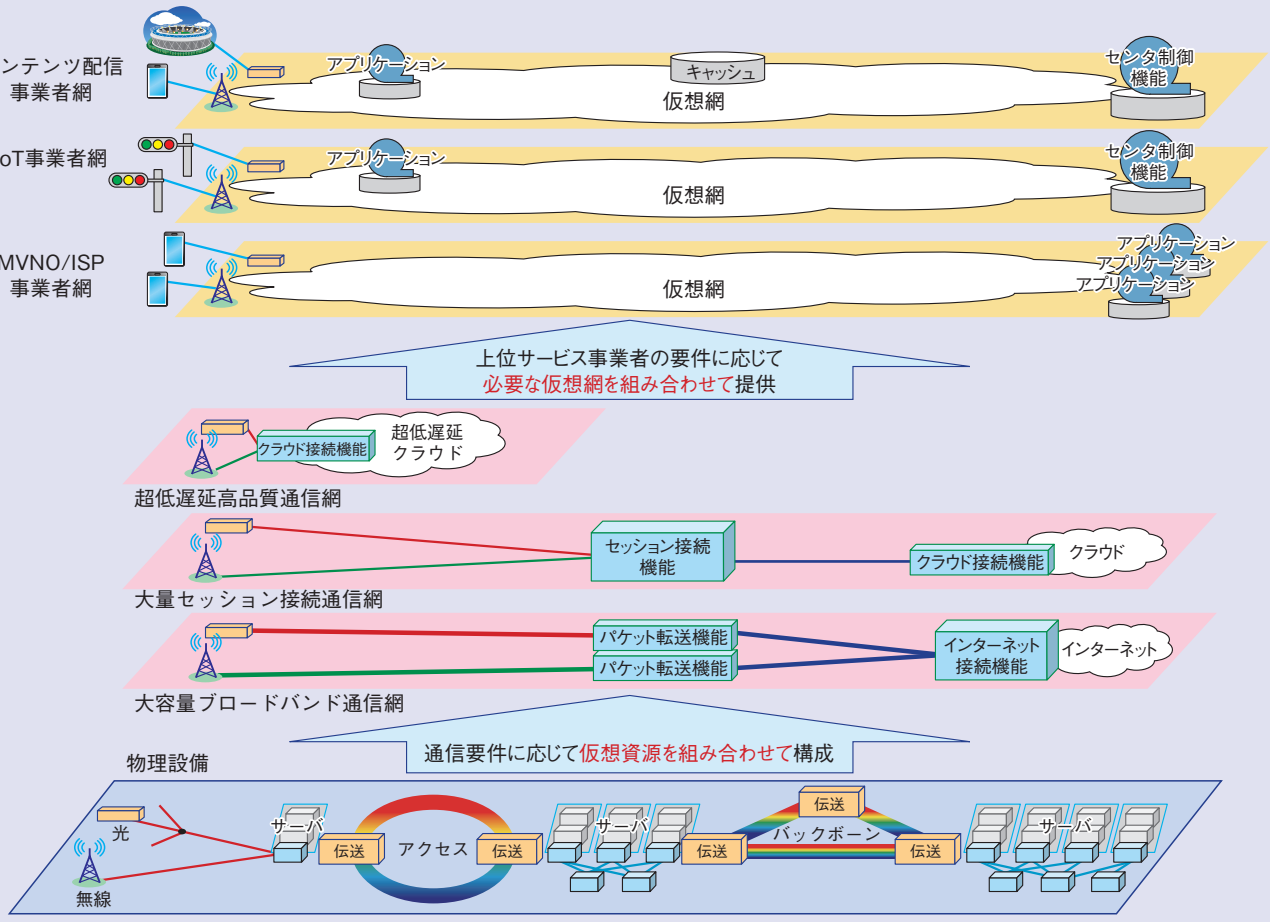

図1　ネットワークスライス

ない独自ルーチング制御プロトコルの使用，独自のQoS（Quality of Service）ポリシー運用も可能となります．

ネットワークスライシングの用途としては，5Gネットワークのように多様な通信要件を同一物理設備上で実現するケースや，上位サービス事業者にプログラム制御可能な仮想資源を提供するケースが考えられます．

多様な通信要件実現の観点では，5Gの国際標準で議論されている3分類，大容量ブロードバンド通信（4K/8K映像配信等），大量セッション接続通信（IoT等），超低遅延高品質通信（AR，自動運転等）をそれぞれ実現する仮想網構成法を検討しています（図1）．

例えば，大容量ブロードバンド通信網では，大部分のトラフィックがインターネットから転送されるため，インターネット接続点をルートとしたツリー構造でパケット転送機能を配備するのが効率的です．大量セッション接続通信網では，大量セッション発生場所にセッション接続機能を大量配備することが効果的です．超低遅延高品質通信網では，遅延条件に適合する範囲のデータセンタに接続するために，アクセス近傍に超低遅延のクラウドを配備することが有効です．

上位サービス事業者に仮想資源を提供する観点では，ISP（Internet Service Provider）用，MVNO（Mobile Virtual Network Operator）用などの主な用途の機能をフルセットにしたエンドエンド仮想網を提供する場合（NSaaS: Network Slicing as a Service），上位サービス事業者によるカスタマイズや組合せが可能な仮想網基盤として提供する場合（NPaaS：Network slicing Platform as a Service），仮想サーバや仮想リンクなどを個別提供する場合（NIaaS: Network slicing Infrastructure as a Service）の3種類を検討しています．

例えば，MVNOやISPはNSaaSを利用して，仮想OSS/BSSも含めたフルセットの仮想通信事業者設備を調達し，独自の加入者向けWeb UI等のみでビジネスが可能となります．またコンテンツ配信事業者はNPaaSを利用し，東京，名古屋，札幌などライブ会場の移動に合わせて，コンテンツ配信者独自の映像加工，配信機能をライブ会場直近のビルに配備するなど，遅延条件を満たす仮想コンテンツ配信網を日単位，週単位に構成することも可能になります．このようなネットワークスライス技術の国際標準化や202X年の商用化に向けて，NTT研究所では，スライス管理技術，スライスゲートウェイ技術，スライスアイソレーション技術，テレメトリスライス監視制御技術等の研究開発に取り組んでいます．

■スライス管理技術

スライス管理技術では，管理系を設備事業者，スライス提供事業者，スライス運用事業者（上位サービス事業者）の3レイヤにモデル化し，レイヤ間のAPI（Application Programming Interface）を検討しています（**図2**）．設備事業者は，ネットワーク設備やデータセンタ設備を所有し，仮想リンク（回線帯域等），仮想サーバ（CPU能力等）等の資源プールとして管理します．スライス提供事業者は設備事業者からAPI経由で仮想資源を調達し，スライスを構成します．この3レイヤモデルは実運用では単純水平分業とは限らず，スライス提供事業者が自設備の仮想資源と他者設備の仮想資源を組み合わせて，自他設備意識せず一括プログラム制御するなどのあらゆる実構成も考慮し，APIを検討しています．また，API上位のスライス提供事業者，スライス運用事業者からスライス単位の運用監視，分析情報収集等をプログラム制御するため，テレメトリ技術のネットワークスライシング適用法を検討しています．

■スライスゲートウェイ技術

スライスゲートウェイ技術は，スライス提供者間スライス接続やスライス

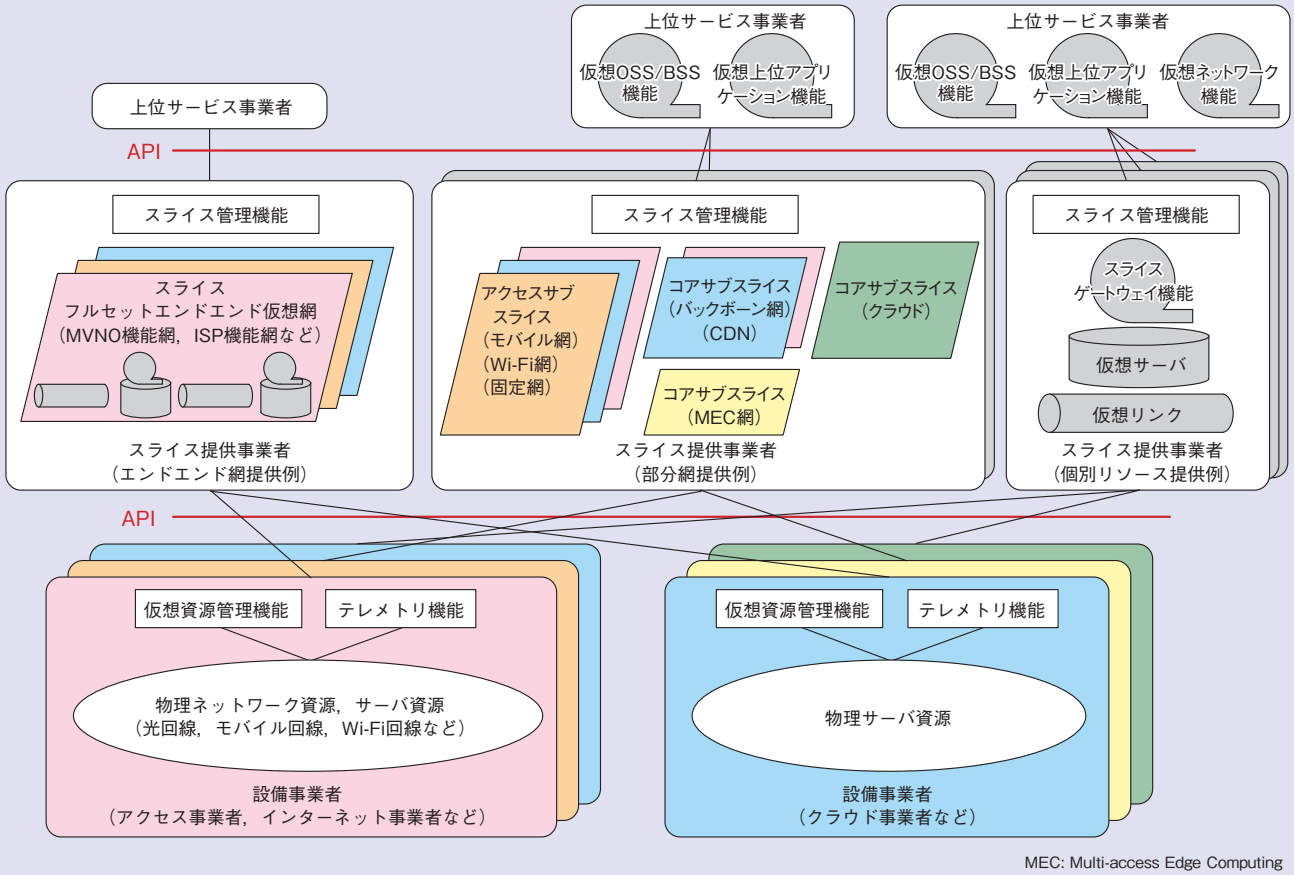

図2　ネットワークスライスモデル

提供者内部のサブスライス間接続に使用します．スライス接続ポリシーに基づきパケットを適切なスライス（あるいはサブスライス）に転送するため，スライス管理機能やスライスアクセス認証機能とパケット転送機能との連携技術を検討しています．また次に説明するスライスアイソレーションのエッジ機能も備えています．

■スライスアイソレーション技術

スライスアイソレーション技術は，リンク区間だけでなく，サーバ内部含めてエンドエンドでトラフィックフローをスライス単位に分離する技術です．将来的な目標は，スライス間が完全非干渉で，他スライスのトラフィック輻輳，機能故障やソフトウェアバグ等に全く影響されないことですが，現在の仮想化技術では困難で，QoS優先制御程度の「緩い」アイソレーションから，仮想リンク帯域や仮想サーバのCPUコア等を確定することで，ある程度の非干渉性を確保する「厳密な」アイソレーションまで実現法を検討しています．特に仮想リンクのプロトコルについては，ベースとして，VxLAN（Virtual eXtensible Local Area Network），MPLS（Multi-Protocol Label Switching），SR（Segment Routing）等の，多数フローを分離可能な国際標準プロトコルが挙げられ，NTT研究所では，これらのプロトコルにアイソレーションに必要な要件を加味したプロトコルの国際標準化をめざしています．

クラウドネイティブSDx制御技術

クラウドネイティブSDx制御技術はネットワークサービスを単独で提供するのではなく，ネットワークやクラウド環境，さらにはサービス提供のためのアプリケーションまでを含めて，エンド・ツー・エンドで自動的に制御することにより，サービス提供を容易かつ迅速に提供するための技術です（**図3**）．

従来のネットワークサービスはサービス利用者とサービス提供者をつなぐだけの機能にとどまっていました．現在ではさまざまなサービス提供者がクラウド環境上で多様なサービスを提供

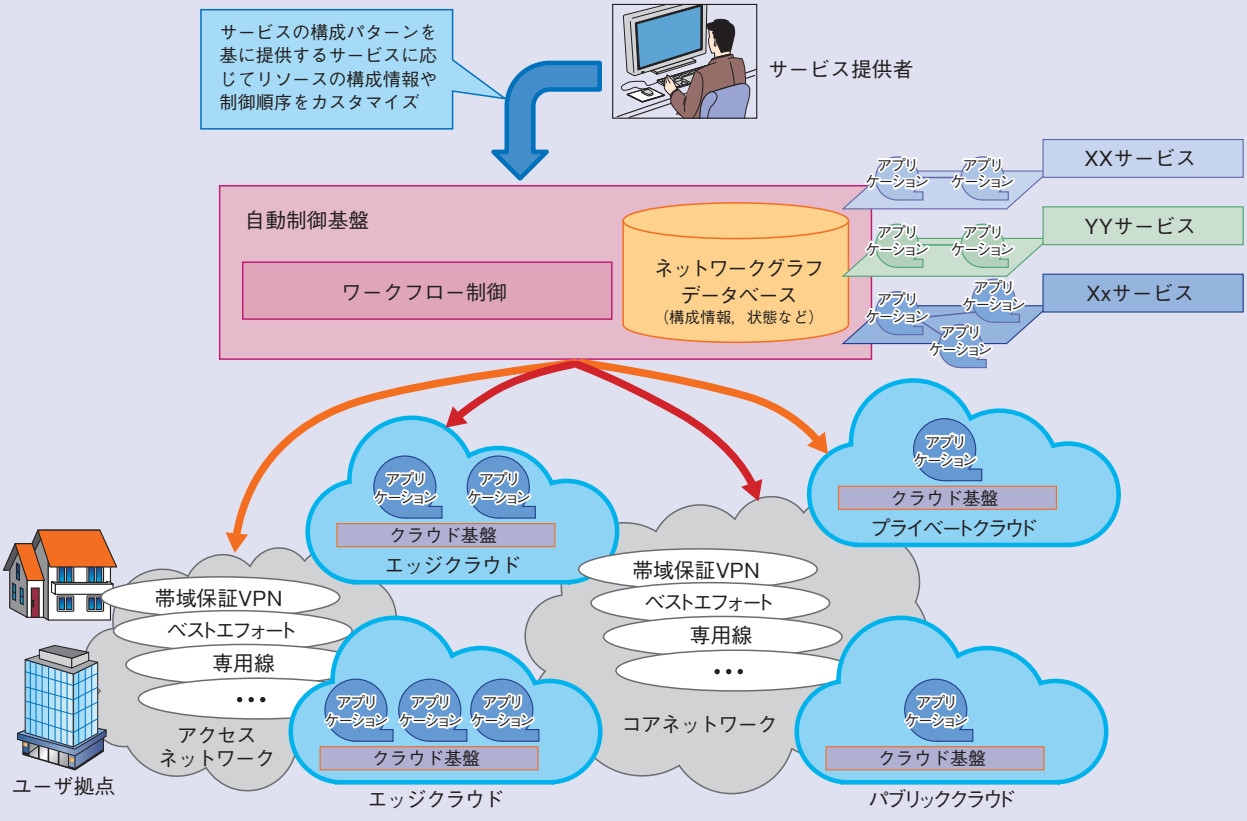

図3　クラウドネイティブSDx制御技術

しています．しかし，クラウド基盤がネットワークと連携できていないことがサービスの迅速な提供の妨げになってきています．そこでネットワークが提供するさまざまな機能と，サービス提供者の利用するクラウド環境やアプリケーションまでをまとめて扱えるようにすることで迅速なサービス提供の実現をめざします．この実現には，サービスを提供するための資源（ネットワーク，クラウド上のリソース等）に対する設定を自動的に行う仕組みと，それを支えるためのリソース情報の管理が必要となります．自動化の仕組みはクラウド環境で利用されているワークフローやクラウド環境制御等，さまざまな技術を基にネットワークの制御も含めてサービスの構成パターンとして提供し，サービス提供者が自身のサービスに応じてカスタマイズできるようにするなど，使いやすいかたちで提供することを検討しています．また，さまざまなリソースを連携させて自動制御するためには制御対象がどのようなもので，それぞれがどういう状態にあり，どういう順序で設定すべきかなどの情報を適切に管理できる必要があります．そこで，個々のサービスや物理的な装置等に依存することなく，さまざまな制御対象を統一して扱うことを可能とするため，制御対象のモデル化と，全体の構成情報や状態を管理するための管理方法について検討を進めています．

現在検討しているモデル化と構成管理方法を確立し，自動制御の仕組みに組み込むことで，サービスに必要なリソースを一元管理し，自動制御を可能とする制御基盤を実現していきます．

マルチレイヤSDN制御技術

サービスの迅速な提供とネットワーク全体でのリソース最適化を実現するために，マルチレイヤSDN制御技術を検討しています．

マルチレイヤSDN制御では，IPレイヤと伝送レイヤをSDNコントローラから統合的に制御することで，ルータや伝送装置に必要な設定を同時に行い，IP-VPNやイーサネット専用線等の異なるサービス種別のパスをSDNコントローラからオンデマンドで提供することができます（**図4**）．このようなサービスの迅速な提供に加えて，5G時代にはさまざまなサービスレベルが必要になることを見据えて，品質・信頼性のグレード化の方式を検討

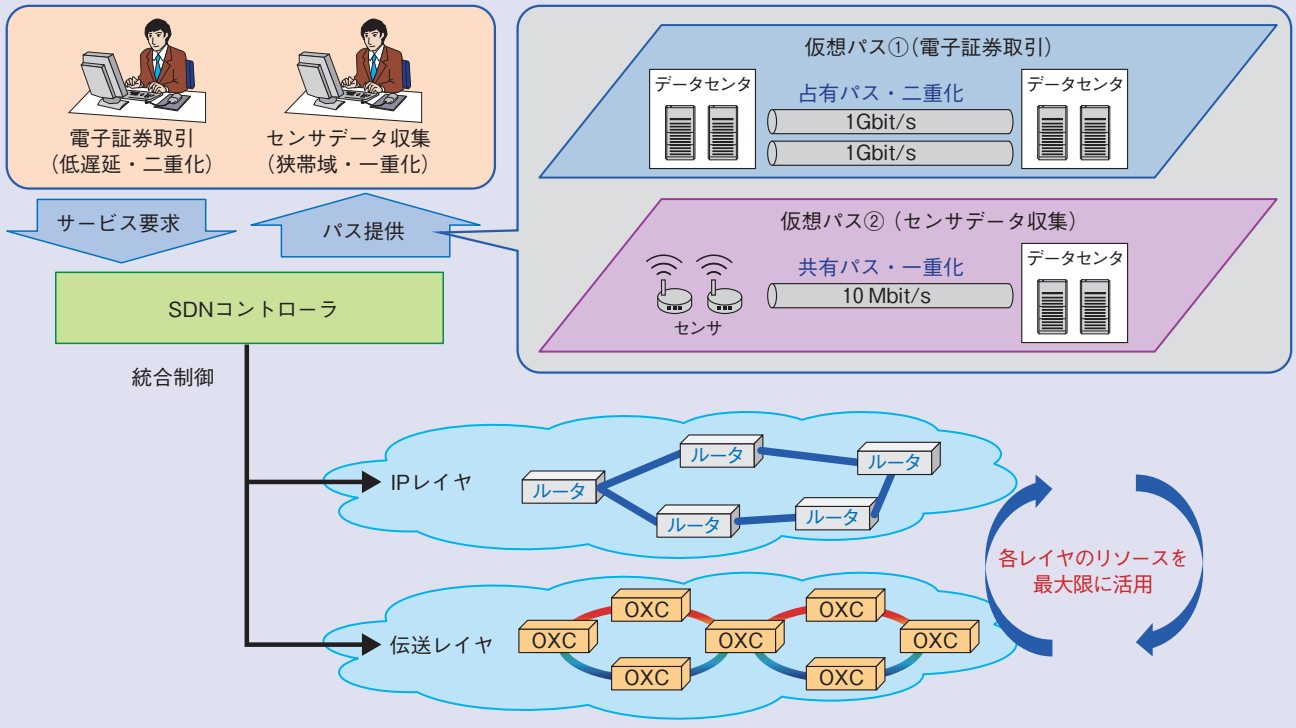

図4　マルチレイヤSDN制御技術

しています[1].

具体的には，①SDN制御に適したSRによるIPレイヤでの経路制御とプロテクションの実現，②光波長スイッチによる伝送レイヤでの経路制御とリストレーションの実現，③ストリーミング・テレメトリ技術を用いたネットワーク状態のリアルタイム監視，④断片化した光波長を再整理する光波長デフラグを検討しています（**図5**）．これらの要素技術を組み合わせることで，品質・信頼性のグレード化を実現するとともに，SDNコントローラがネットワークの状態に応じて，自律的にIPレイヤと伝送レイヤを制御し，ネットワーク全体でリソースを最大限に活用する新たなネットワークの運用をめざしています．現在，オープンソースSDNコントローラのONOS（Open Network Operating System）をベースに，図5に示すコントローラ機能のプロトタイプ実装を行い，技術検証を行いながら，マルチレイヤSDN制御の技術確立に取り組んでいます．

CDN技術

4K/8K，AR/VRに代表される高精細・高臨場の次世代映像コンテンツを経済的かつ高品質に配信するため，CDN技術を検討しています（**図6**）．この技術は，「映像QoE（Quality of Experience）制御・配信設計技術」「リアルタイム大容量配信技術」「状態可視化技術」の3つの特徴があります．

■映像QoE制御・配信設計技術

映像QoE制御・配信設計技術は，QoEに基づいた経済的な映像コンテンツ配信を実現します．ネットワーク上の各種装置やアプリケーション，端末で測定した情報を用いて推定したQoEや視聴状態，サーバやネットワーク等の設備リソース状態に基づいて，QoEと設備リソースのバランスが最適となるように，配信サーバと配信レートを選択する制御（サーバ・コンテンツナビ）と，視聴者の加入サービス等に応じたトラフィック制御，制御と連動したコンテンツ・キャッシュ配備を実施することで，QoEの維持と効率的な設備利用を実現します．

■リアルタイム大容量配信技術

リアルタイム大容量配信技術は，大規模なライブ映像の効率的かつ安定的な配信を実現します．通常，配信サーバと端末間はHTTPベースのユニキャスト通信であり，ライブ配信等により視聴要求が集中すると，配信サーバおよびネットワークの負荷が大幅に増大します．そこで，配信サーバおよび端末はユニキャスト通信のままネット

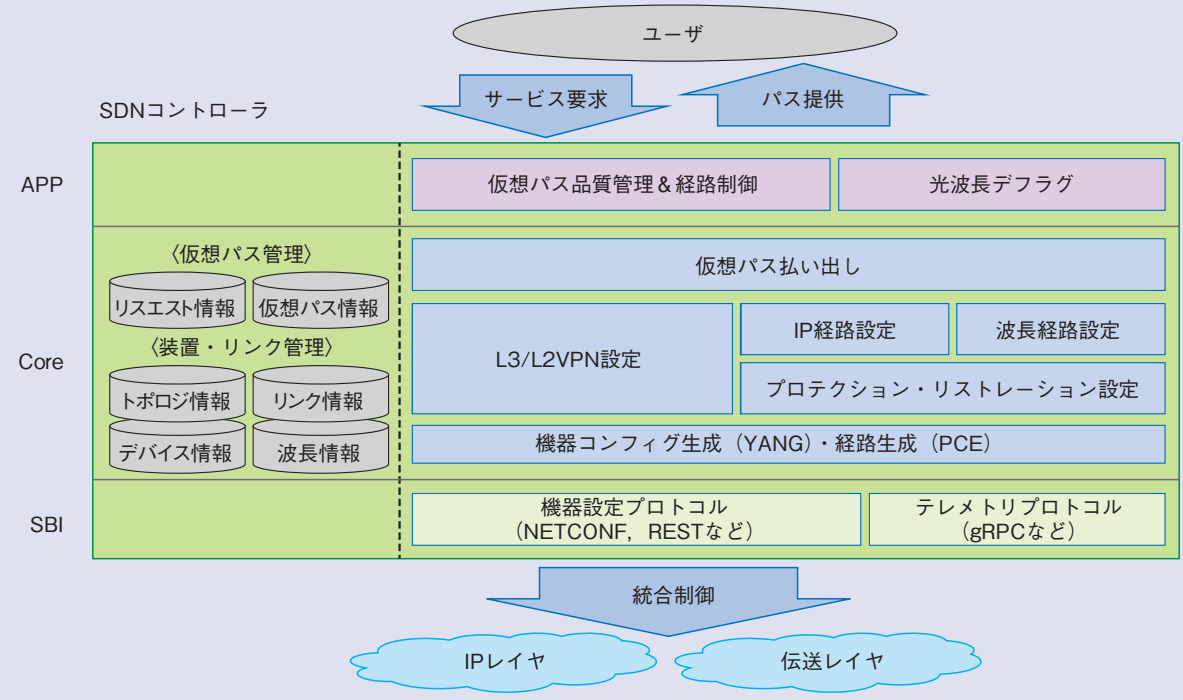

図5　マルチレイヤSDN制御の要素技術

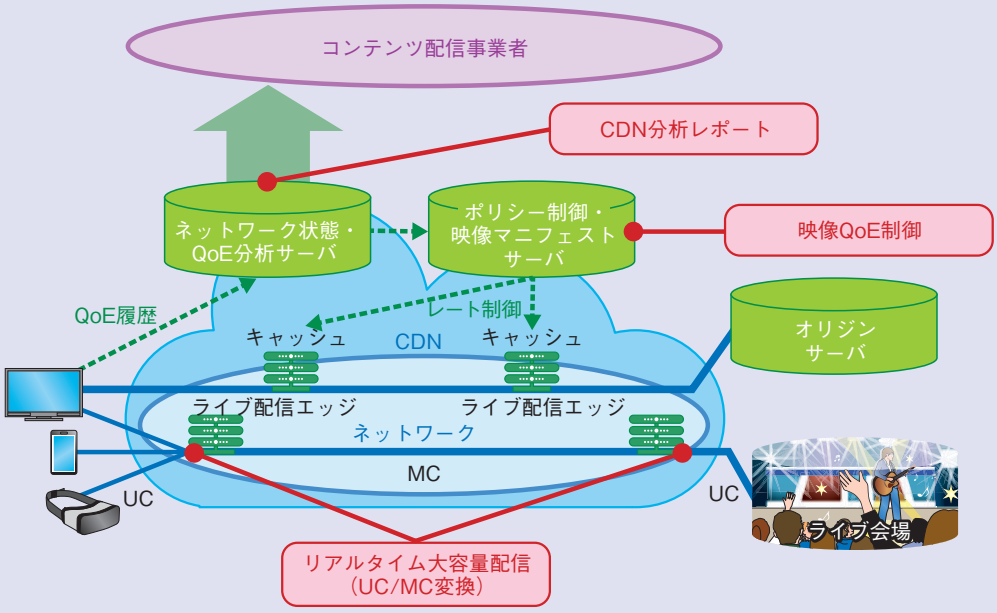

図 6　CDN技術

ワーク区間のみマルチキャスト通信〔UC (Unicast) /MC (Multicast) 変換〕にて配信し，同一ライブ映像の重複配信を回避することで，配信事業者のサーバ等を含む設備利用効率の向上と安定配信を実現します．

■状態可視化技術

状態可視化技術は，ネットワーク上の各種装置やアプリケーション，端末で測定・蓄積した情報から配信状態，QoE，視聴行動（映像の再生・停止，シーク，離脱等）を推定・可視化して，コンテンツ配信事業者へ提供します．これにより，視聴者のコンテンツ視聴特性が把握可能となり，配信事業者のコンテンツ配備業務の効率化が期待できます．

これらの技術により，キャリアの持つネットワーク基盤とその管理情報を活かした高性能で経済的なCDN基盤の実現をめざします．

大規模化・多様化するサイバー攻撃に対処するネットワーク間連携対処技術

近年，DDoS攻撃が大規模化し，またマルウェアも多様化する中で性能面や機能面で単一のネットワークでの効率的な対処が難しくなってきています．このような状況に対して，セキュリティの脅威情報をネットワーク事業者間で事前に取得・展開することによる攻撃の予防的な防御や，複数のネットワークのセキュリティ機能を連携させることによる検知・防御機能の強化が重要となります．本取り組みでは，サイバー攻撃に対するネットワークの防御力強化に向けて，「事前防御の高度化」「DDoS攻撃防御機構の大容量化」「マルウェア感染検知・防御機構の高度化」の実現をめざしています（**図 7**）．

■事前防御の高度化

事前防御の高度化に関しては，これまでの外部機関からの脅威情報取得に加え，フロー情報などネットワークで取得可能な情報を活用することで迅速・正確に脅威情報を生成し，ネットワーク間で連携する技術を検討しています．この技術確立により，DNSのブラックリストを拡充するなど事前防御の高度化を実現することができます．

■DDoS攻撃防御機構の大容量化

DDoS攻撃防御機構の大容量化に関しては，攻撃経路上の複数ネットワークの防御機能が適切に連携できるよう，各ネットワークの防御機能のリソース限界を考慮したDDoS攻撃トラフィック分散方式を検討しています．本方式により，単一ネットワークでの対処と比較し圧倒的な帯域の攻撃に対する防御を実現することができます．

■マルウェア感染検知・防御機構の高度化

マルウェア感染検知・防御機構の高度化に関しては，情報漏洩等を防ぐた

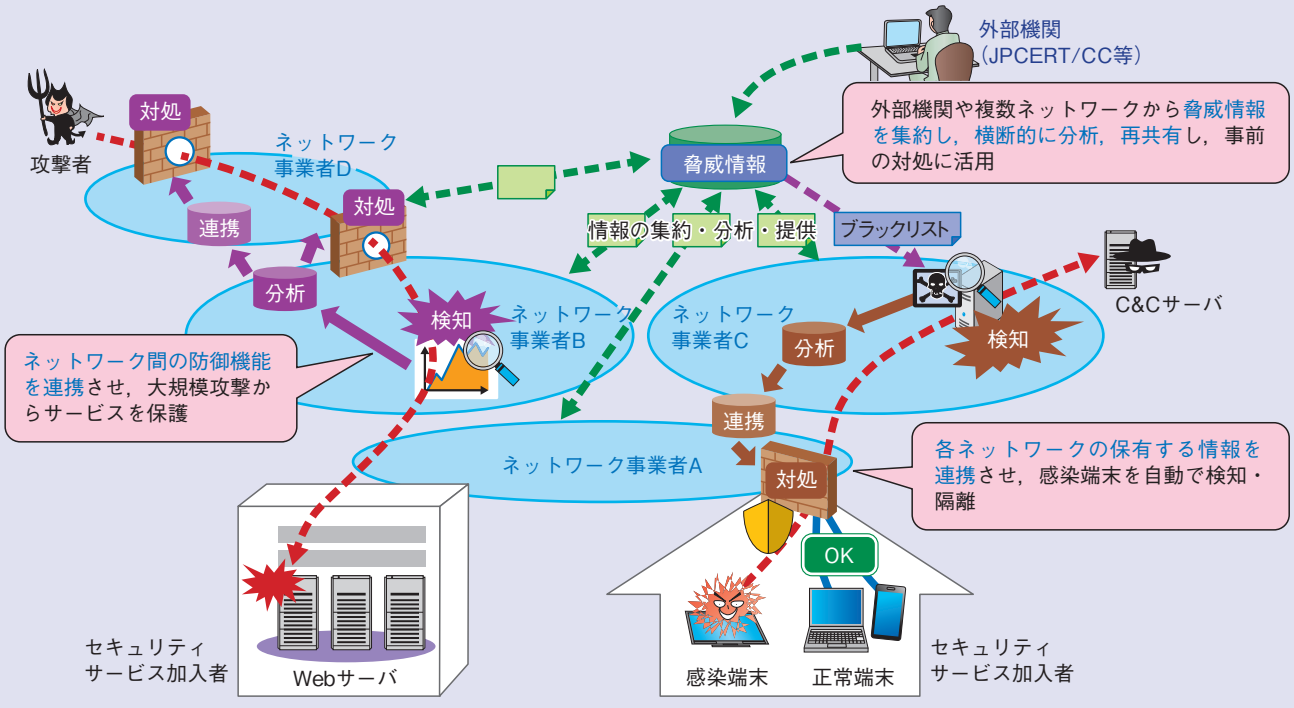

図７　大規模化・多様化するサイバー攻撃に対処するネットワーク間連携対処技術

めに感染端末を迅速・的確に検知・隔離する必要があります．しかし，DNSを備えマルウェアの代表的な振る舞い（C&Cサーバへのアクセス）を検知可能なネットワークと，端末を収容しているネットワークが異なる場合，いずれも単体では隔離困難になります．そこで，ネットワーク間で検知情報や端末の収容情報を連携し感染端末のみ迅速・的確に隔離する方式を検討しています．

本取り組みでは複数ネットワークの機能や情報を連携させてサイバー攻撃を検知・対処する仕組みの確立を推進しています．今後は商用ネットワークで技術を評価し，実用化に向けた課題の洗い出しやシステムの具現化を加速させていきます．

今後の展開

将来ネットワーク技術として，「ネットワークスライス」「クラウドネイティブSDx」「マルチレイヤSDN制御」「CDN」「大規模化・多様化するサイバー攻撃に対処するネットワーク連携対処」技術について検討結果を解説しました．今後は，PoC（Proof of Concept）による技術検証を進め，要素技術としての完成度を高めるとともに，全体アーキテクチャに仕上げていきます．

■参考文献

(1) T. Tojo, T. Matsukawa, S. Okada, S. Arai, and S. Yasukawa: “Multi-level Reliability Architecture for Network Slicing in Metro Networks,” IEEE LANMAN 2017, Osaka, Japan, June 2017.

(後列左から) 安川 正祥/ 佐藤 裕昭/ 弘田 武志/ 東條 琢也
(前列左から) 鈴木 裕志/ 笠原 康信/ 遠藤 乾市

5G/IoT時代のクラウド・ネットワーク・端末環境が融合して映像・セキュリティ・社会インフラ等のさまざまなサービスがネットワーク上で実現される世界をめざし，必要なネットワークアーキテクチャ技術の研究開発に取り組んでいきます．

◆問い合わせ先

NTTネットワーク基盤技術研究所
ネットワークアーキテクチャ技術革新SEプロジェクト
202Xネットワークアーキテクチャ SEグループ
TEL　0422-59-2684
FAX　0422-59-6364
E-mail　yasukawa.seisho@lab.ntt.co.jp