RENAネットワークサービスを実現するプラットフォーム技術

日本電信電話株式会社
レゾナントネットワークプロジェクト
直井　邦彰

日本電信電話株式会社
レゾナントネットワークプロジェクト
小林　透

あらまし

サービス/ネットワーク制御プラットフォームは、サービスアプリケーションとコア転送網の中間に位置し、RENAのコンセプトを実現する上で、キーとなる役割を担っている。ここでは、サービス/ネットワーク制御プラットフォームの位置づけ、提供すべき機能とその実現技術、アーキテクチャ概要について紹介する。

サービス/ネットワーク制御プラットフォームの重要性

サービス/ネットワーク制御プラットフォームは、RENAの特徴であるエンド・ツー・エンド型の高度の接続（リアルタイムコネクティビティ）や、品質、セキュリティが保証された信頼性の高いネットワークを実現する上で中核となる共通機能や複数のサービスを連携させるために必要な機能を提供する[1]。

これにより、サービス開発のコスト削減、ならびに複数のサービスを利用者毎のニーズに応じて自由に連携させるネットワークサービス基盤の提供が可能となる。

サービス/ネットワーク制御プラットフォームの位置づけ

サービス/ネットワーク制御プラットフォームは、双方向エンドエンドリアルタイム通信やコンテンツ配信などのRENA上で実現されるサービスアプリケーションとコア転送網の間に位置し、下位レイヤーの転送機能を制御することによって、RENAの特徴であるコネクティビティ、品質制御、セキュリティ、ユーザビリティの各機能を上位アプリケーションに提供する。また、サービス連携に必要な基本機能を提供することで、RENA上での新しいサービスやビジネス開発の容易化を可能にする（図1）。

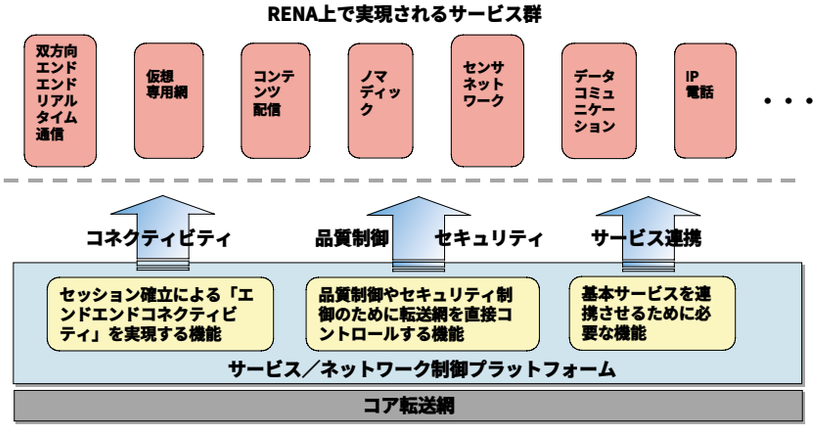

図1　サービス／ネットワーク制御プラットフォームの位置付け

サービス/ネットワーク制御プラットフォームが提供すべき機能概要については、表1に示した通りである。

プレゼンス、位置情報管理、セッション制御の各機能は、つなぎたい相手の状況や意向に合わせて、確実なリアルタイムコネクティビティを

実現するための基本機能である。セキュリティ管理、ネットワーク装置制御機能は、ユーザネットワーク内のホームGWやコア転送網内のエッジノード、コアノードを制御することによって、エンド・ツー・エンドでの通信内容の秘匿化やサービス種別、ユーザー要望に基づくマルチグレードの品質制御などを実現する。

アドレス管理、顧客ID管理、認証、課金管理の各機能は、RENAサービスのユーザビリティを向上させる共通機能及び、サービスを連携させるために必要な機能を提供する。

ここでは、RENAの大きな特徴であるリアルタイムコネクティビティ機能、セキュリティ管理機能、ネットワーク装置制御機能、認証機能について紹介する。

表１　サービス／ネットワーク制御プラットフォーム提供機能構成

PF提供機能	機能概要
プレゼンス	接続可能な相手の表示、接続したい相手の現在の状態表示
位置情報管理	モビリティを考慮したユーザーや端末の位置情報管理
セッション制御	モビリティを含めたエンドエンドコネクションの確立 発信者のアクセス環境、端末種別と、着信相手のアクセス環境、端末種別が異なった状況でのコネクションの確立
セキュリティ管理	ＮＡＴ／ＦｉｒｅＷａｌｌを越えたコネクション確立 セキュアな通信路および信号路セッションの確立 ネットワーク自体がＤＤｏＳ攻撃を防御
ネットワーク装置制御	サービス種別やユーザー要望に基いたネットワーク品質の制御
アドレス管理	ネットワークで利用するアドレスの払出し管理と変換
顧客ID管理	サービスを提供するために必要な顧客情報の一元管理
認証	ユーザー認証および端末認証による不正アクセス防止 シングルサインオン認証による上位サービスとの連携
課金管理	個々のサービスの利用料徴収のための課金に必要な各種ＣＤＲの収集とバンドル課金、複数サービス連携課金

NAT: Network Address Translation DDos: Distributed Denial of Service ,CDR:Call Detail Record

リアルタイムコネクティビティ機能

RENAにおいては、ユーザーによって、利用している端末種別、アクセス網種別、利用したいメディア（音声、映像・音声、テキストなど）、品質条件、セキュリティ条件、利用場所、ネットワーク利用状況などが異なることを想定している。そのような環境下で、確実な接続を実現するためには、種々の情報を元にネゴシエーションを行うことで、その時々の状況に応じたリアルタイムコネクティビティを提供する必要がある（図２）。例えば、つなぎたい相手が、現在、外出中で、ホットスポットにおける狭帯域の無線LAN環境とPDAしか使えない場合でも、相手のアクセス環境や端末処理能力に合わせた柔軟な接続を可能とする。このように、サービス／ネットワーク制御プラットフォームは、プレゼンスなどのユーザー管理情報を元に、その時々のネットワーク条件やユーザー要望を最大限考慮して、アクセス網やコア転送網を直接制御することによって、エンド・ツー・エンド型のリアルタイムなコミュニケーションを実現する。

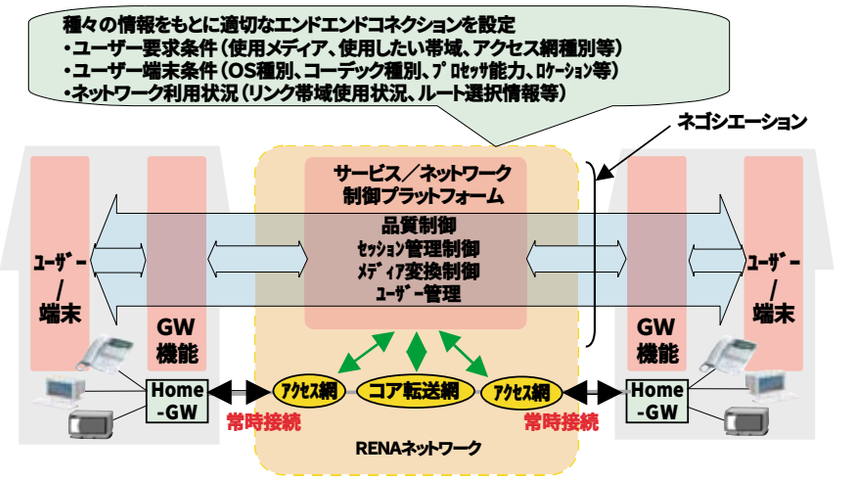

図２　リアルタイムコネクティビティ

セキュリティ管理機能

セキュリティ管理では、様々なネットワークへの不正アクセス、盗聴、改竄、 DDos攻撃(2)などに対する各種対策機能を提供する。

IPベースのエンド・ツー・エンドのコミュニケーションにおいては、特に、成りすましや改竄、情報漏洩に対する不安が大きいことが指

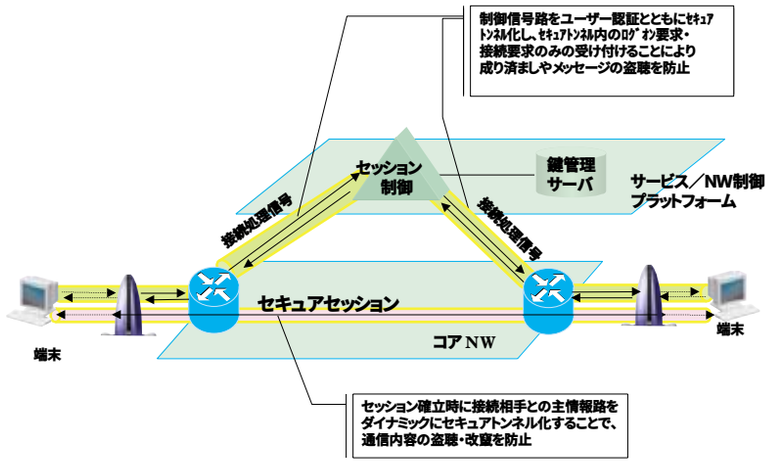

図３　エンド・ツー・エンドセキュアセッション技術

摘されている。そこで、セッション毎に、セキュアなシグナリングを用いてセッションを確立することで、成りすましの防止や、通信内容の秘匿化を実現する機能（ダイナミックエンドエンドセキュアセッション技術）を提供している（図３）。

これは、発着各端末とセッション制御サーバ間の制御信号路をセキュアトンネル化し、セキュアトンネル内でそれぞれ認証を行うことで、成りすましを防止する。このように、セッション制御サーバ経由でセッション接続を行うことで、エンドユーザー間で直接やりとりを行うことなく、相互認証が可能となる。

また、セッション確立時に、セッション制御サーバから暗号鍵を配布し、接続相手との主情報をダイナミックにセキュアトンネル化することで通信内容の秘匿化を実現している。

通常、エンド・ツー・エンドで暗号通信を行う場合は、事前に暗号鍵を交換しておく必要があるため、特定対地間、あるいは、特定相手とし か通信内容の秘匿化が実現できなかったが、本機能により不特定多数のユーザー間で、通信内容の秘匿化が実現可能となる。

インターネット上でサービスを提供しているサーバや端末に対して、トラフィックを集中的に送ることで負荷をかけ、正規ユーザーに提供するサービスをさまたげるDos（Denial of Service：サービス妨害）攻撃や、インターネット上の無防備なサーバを操って複数台から同時に送信するDDos（Distributed Dos：分散サービス妨害）攻撃を行うハッカーやクラッカーの出現により、安全な電子社会が最近脅かされている。それらへの対策がMovingFirewall技術である（図４）。

本技術の特徴は、２つある。１つ目は、攻撃に対応して、対処プログラムが動的に移動するということである。

MovingFirewall装置は、Dos攻撃を検出すると攻撃防御プログラムを攻撃元に近い箇所へ分散させて配置し、攻撃抑止が実行される。これにより、被害を局所的に抑えることが可能となる。２つ目は、正規ユーザーの通信を保護するということである。サーバへのトラフィックの分析を行い、正規・容疑・攻撃トラヒックの３つに分けて、疑わしさに応じてデータ転送量を制御する。これにより、攻撃への対処を行いながらも正規ユーザーの通信を保護することが可能となる。

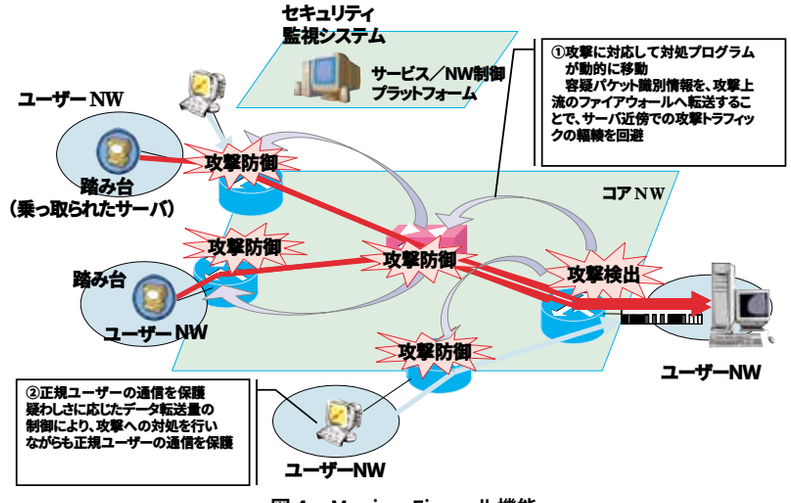

図４　Moving Firewall 機能

ネットワーク装置制御機能

ここでは、ネットワーク装置制御機能の中で、QoS制御に関する機能について説明する。

一般的に、QoS制御は転送系の技術として、RSVP（Resource ReSerVation Protocol）やMPLS（Multi Protocol Label Switching）による帯域確保技術などが提案されている。こうしたQoS制御の際には、転送系装置に対して、優先識別情報の扱いやリソース確保の指示が必要である。

そこで、RENAでは、サービス／ネットワーク制御プラットフォームの中に、転送系と連携してセッション単位にQoS制御を実現する機能をもたせている。

具体的な機能については、複数の方式があるが、ここでは、リソース集中管理QoS制御方式について紹介する（図５）。

この方式では、事前に収集したコア転送網、アクセス網からネットワーク状態やルーティング情報をベースとして、ネットワーク内の全リンクの空きリソースを帯域管理サーバにおいて集中的な管理を行う。その後、セッション制御サーバと帯域管理サーバが連携することによって、セッション接続要求毎に、要求されたネットワークリソースを割り当てることが可能かどうかを判定する。

このように、リソース集中管理QoS制御方式は、ネットワークリソースの利用状況をダイナミックに集中管理する機能をサービス／ネットワーク制御プラットフォームにもたせることで、厳密なエンド・ツー・エンドQoSを保証しようというものである。

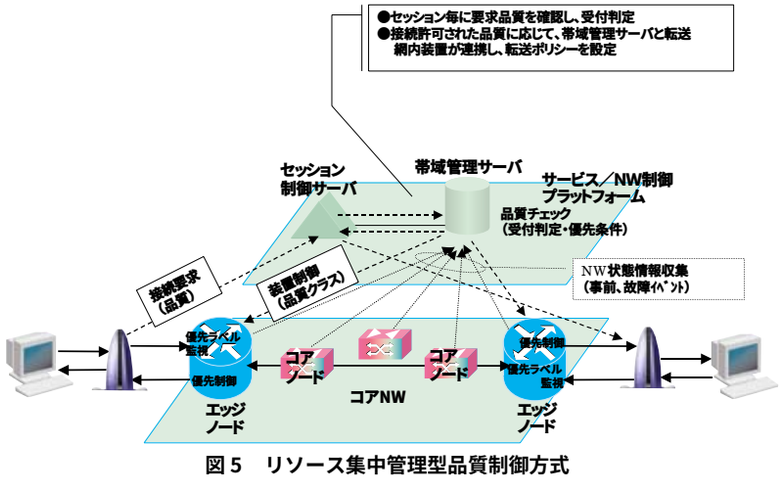

図５　リソース集中管理型品質制御方式

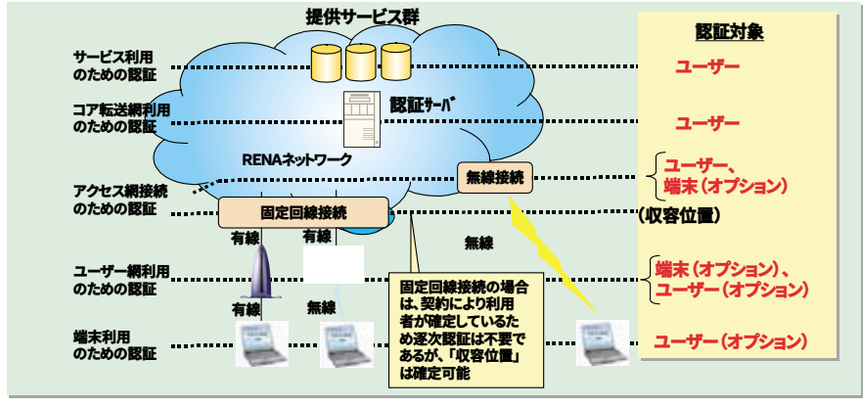

図６　認証フェーズ毎の認証対象

セッション制御サーバと連携した帯域管理サーバをサービス／ネットワーク制御プラットフォーム内に集約して実装し、転送系の優先制御機能を用いてQoSを実現する方式とすることで、転送系装置のすべてに高度なQoS機能を実装する必要が無いため、コスト面、実現容易性の面でメリットがある。

認証機能

正当な利用者かどうかを判定するための認証種別としては、利用する端末を特定する「端末認証」、利用する人を特定する「ユーザー認証」がある。

「端末認証」は、主に無線接続の場合にセキュリティの観点から厳密に接続可能な端末を限定したいという場合に有効であるが、それ以外のケースでは、ユーザーの利便性を考慮すると端末によらず（種別、自己所有・他者所有）にネットワークサー

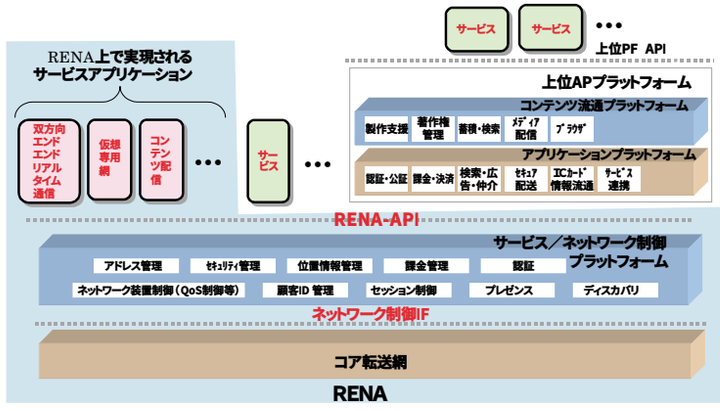

図７　サービス／ネットワーク制御プラットフォーム構成

ビスを享受できることが望ましい。従って、端末によらない「ユーザー認証」を実施することを基本方針とし、「端末認証」は、オプションとして必要に応じてユーザー認証と併用とする。これらの関係を図６に示す。また、ユーザーの利便性を考慮してアクセス網認証の結果を上位サービスの認証にも適用する垂直方向のシングルサインオンを実現する。

RENAでは必要に応じて公開鍵の暗号方式を適用し、セキュリティを確保する。

サービス／ネットワーク制御プラットフォームアーキテクチャ

サービス／ネットワーク制御プラットフォームは、２つのインタフェースを持つ（図７）。１つは、コア転送網に対するネットワーク制御インタフェースであり、もう１つは、RENA上で実現されるサービスアプリケーションや上位アプリケーションプラットフォームに対するRENAアプリケーションインタフェース（RENA-API）である。

ネットワーク制御インタフェースは、コネクティビティ、品質制御、セキュリティの各機能を上位サービスアプリケーションに提供するために、コア転送網内のエッジノードやコアノードを制御するインタフェースである。サービス／ネットワーク制御プラットフォームとコア転送網との間にインタフェースを定義し、それらの間の機能分担を明確にすることによって、それぞれ独立した機能拡張や装置更改によるネットワークの高度化が可能になる。

アプリケーションインタフェースは、RENAの特徴を活かしたサービスアプリケーションの開発効率化やサービス間の連携、市販サービスアプリケーションの利用を可能とするインタフェースである。

アプリケーションインタフェースは、サービスアプリケーションばかりでなく、上位アプリケーションプラットフォームにも提供されることで、RENAの特徴にさらなる付加価値をつける上位アプリケーションプラットフォームの構築や新しいプラットフォームビジネスも可能としている。

コア転送網とサービスアプリケーションの間に、サービス／ネットワーク制御プラットフォームを位置づけて、上位サービスアプリケーションや上位アプリケーションプラットフォームにRENA-APIを提供することで、例えば、将来、ネットワーク装置の光ノード化などによりコア転送網の広帯域化が図られたとしても、上位のサービスアプリケーションやアプリケーションプラットフォームに影響を与えることなく、広帯域サービスを提供できるようになる。

今後の展望

RENAにおけるサービス／ネットワーク制御プラットフォームの位置づけと、主要な機能、アーキテクチャの概要について説明した。今後は、マーケットニーズをベースにして、確実なエンドエンドコネクション、マルチグレード品質メニュー、高度なセキュリティ／プライバシー保護、キャリアグレードのスケーラビリティと信頼性などに関する各機能を段階的にサービス／ネットワーク制御プラットフォームへ実装していく予定である。

■ 参考文献

（１）和田、“”光”新世代ビジョン－ブロードバンドでレゾナントコミュニケーションの世界へ－“、NTT技術ジャーナル、Vol.15、No.2、pp.6-17、2003
（２）吉田、“情報セキュリティ応用技術、”NTT技術ジャーナル、Vol.14、No.8、pp.16-19、2002