マルチドメイン環境における汎用AAA基盤の設計と実装

Design and Implementation of a Universal AAA Infrastructure in Multi-domain Environments

横路隆　平岡達也*　寺岡文男
慶應義塾大学大学院理工学研究科

概要

インターネット上でサービスを提供する際にはユーザの認証・権限付与・課金情報管理が不可欠であり，これを AAA (Authentication, Authorization and Accounting) と呼ぶ．様々なネットワークサービスが存在する状況でユーザ情報が分散して扱われた場合，ユーザは多数のアカウントを管理する必要があり，サービス提供者は各サービス毎に AAA システムを構築および保守運用する必要がある．これはユーザとサービス提供者の双方に対する大きな負担である．そのため様々なサービスに対して AAA 機能を提供するための統一的な基盤が必要とされているが，既存の AAA システムでは十分な AAA 機能を提供することはできず，また柔軟性，汎用性に欠ける．そこで本論文では，インターネット上の様々なサービスに対して共通のインタフェースを通して柔軟な AAA 機能を提供する汎用 AAA 基盤を提案する．またサービスの一例として汎用 AAA 基盤をセキュアマルチキャストシステムに適用し，システムの AAA 処理にかかる時間を計測することによってその有効性を検証することができた．

1　はじめに

インターネット上ではさまざまなサービスが提供されている．最も基本的なインターネットサービスはインターネットへの接続サービスである．ユーザがインターネットに接続する際，ISP (Internet Service Provider) はこのユーザが正しいユーザであることを認証し (authentication)、このユーザにインターネット接続を行う権利を付与し (authorization)，このユーザによるネットワーク資源の利用状況を把握する (accounting) 必要がある．この一連の処理を AAA (Authentication, Authorization, and Accounting) と呼ぶ．一方、インターネットは複数の管理ドメイン (e.g., ISP) から構成されるマルチドメイン環境であり，ユーザは通常 1 つの ISP と契約するものと考えられる．ここではユーザが契約を結んでいるドメインを “ホームドメイン” と呼び，ホームドメイン と提携関係にあるドメインを “提携ドメイン” と呼ぶこととする．ユーザがホームドメインにおいてインターネット接続を要求した場合はこのユーザに対する AAA 処理はホームドメイン内で行われるので問題はない．しかし，ユーザが提携ドメインにおいてインターネット接続を要求した場合，提携ドメインにはこのユーザの AAA 処理に必要となる情報がないため，提携ドメインはユーザのホームドメインと連携して AAA 処理を行う必要がある．すなわち，マルチドメイン環境に適応した AAA 基盤が必要となる．IETF (Internet Engineering Task Force) ではマルチドメイン環境に適応した AAA プロトコルとして Diameter[1] が標準化されている．さらにインターネット接続や Mobile IPv4 利用のための Diameter アプリケーションが定義されている [2][3]．一方，インターネット上にはインターネット接続サービスや Mobile IPv4 の利用以外にも帯域保証サービスやコンテンツ配信サービスなどさまざまなサービスが考えられる。しかし，サービスごとに個別のメッセージを定義してそれ専用のアプリケーションプログラムを作成していては効率が悪い．

そこで本論文では，マルチドメイン環境に適応した汎用 AAA 基盤を提案する．本汎用 AAA 基盤はネットワークサービスごとに異なる部分を隠蔽し，ネットワークサービスを提供するアプリケーションプログラムに対して統一的なインタフェースを提供する．その結果，ネットワークサービスを提供するアプリケーションプログラムはサービス 種類に関わらずに統一的に AAA 処理を行うことができるようになる．本汎用 AAA 基盤は AAA のバックエンドプロトコルとして Diameter を利用し，フロントエンドプロトコルとして PANA[4] を利用している．本論文では本汎用 AAA 基盤の設計，プロトタイプの実装、基本性能の測定，セキュアマルチキャストへの適用について述べる．

2　IETF の AAA モデル

1 章で述べたように，インターネット上でサービスを提供するための必要条件として, ユーザの認証, サービス利用権限の確認・付与, サービス利用情報の収集の一連の処理の実現が挙げられる．これら 3 つの機能を持つシステムを AAA システムと定義する．AAA システムは通常，各機能

*現 野村総合研究所

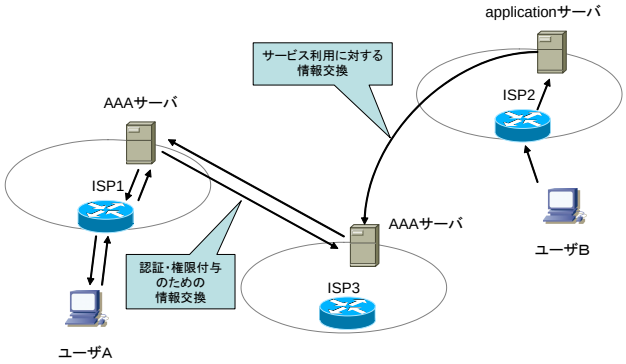

図 1: マルチドメイン環境における AAA システム

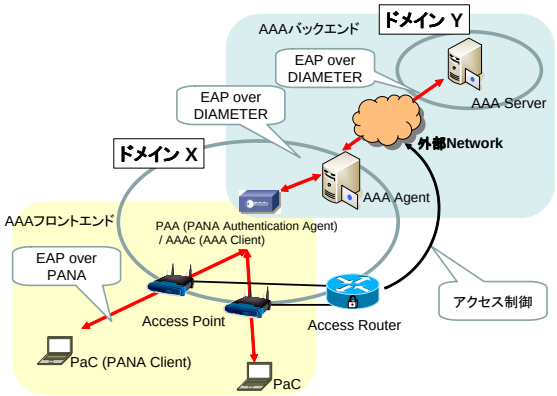

図 2: Diameter と PANA を用いた AAA システム

を持つ複数のモジュールにより構成されるシステムである．マルチドメイン環境における AAA システムは図 1 のようになる．

図 1 が示すように，AAA システムは AAA バックエンドと AAA フロントエンド 2 つに大きく分けることができる．AAA バックエンドはサービスに対し AAA 機能を提供するために必要な情報を交換するための基盤であり，ユーザは AAA フロントエンドを通して要求するサービスへの要求や，サービスに対する AAA を行うために必要な情報を渡す．ここでは，PANA と Diameter を使用した場合について説明する．このモデルでは，AAA フロントエンドに PANA を，AAA バックエンドに Diameter を用いる．このモデル図を図 2 に示す．

Diameter を用いることによる大きな利点は，マルチドメイン環境を標準サポートしている点である．Diameter は RADIUS[7] の後継プロトコルで，マルチドメイン環境を想定して設計されている．また，RADIUS と比較して通信の信頼性，End-to-End のメッセージ確認，Failover，メッセージのセキュリティなどの点においても優れており，RADIUS からの移行や RADIUS との共存などもサポートしている．さらに，Diameter では IPsec[8] や TLS を使用することにより，標準で End-to-End のセキュリティが保証されており，マルチドメイン環境においても ISP 間の通信の保護に TLS を用いてセキュリティを確保することが可能である．

PANA を用いることによる大きな利点は，トランスポート層で認証情報を転送するため，下位層のメディア構成に依存せずに認証を行うことができるという点である．またアクセスポイントと認証モジュールが分離可能であるため，アクセスポイントはアクセスポイントの機能のみを行い，その先の PANA Authentication Agent (PAA) でアクセス制御を行うことができる．そのため，アクセスポイント設置や管理のコストを削減することが可能である点も利点として挙げられる．また，認証エージェント (PAA) とアクセスコントロールを行うモジュール (EP) を分離することができるため，用途に適した柔軟なネットワーク構成が可能となる．

このように，Diameter と PANA を組み合わせることにより，マルチドメインに対応した柔軟で拡張性のある AAA システムを構築することが可能である．しかし，この PANA と Diamter のモデルはネットワークアクセス制御のためのモデルであり，基本的にはそれ以外の用途については考慮されていない．そのため，Mobile IP などその他の用途については別途 Diameter Application という形でメッセージや処理手順を定義する必要がある．すると，たとえばセキュアなマルチキャストコンテンツ配信のような新しいネットワークサービスが登場するたびに，サービス提供者は新しい Diameter Application を設計し実装しなければならない．

しかし，サービスの種類によらすサービスを提供するにあたってサービス提供者が必要とすることは，ユーザの認証，権限付与，資源利用状況の把握，すなわち AAA である．そこで本論文ではサービスの種類によらずに必要となる AAA 機能を汎用基盤として構築し，サービス提供者およびサービス利用者に統一的なインタフェースを提供することを目的とする．

3 関連研究

3.1 Service Oriented AAA

Service Oriented AAA (SOAAA)[5] はサービス利用者に対して統一的なインタフェースを提供する AAA 基盤である。SOAAA のアーキテクチャを図 3 に示す。

AAA server はユーザ情報やサービスのポリシーなどの管理と AAA 処理を行い，Network Access Serve (NAS) はユーザがネットワークに接続する際にユーザの ID を特定し，その後のユーザ情報管理を行う．SOAAA の特徴として，サービス提供サーバに対して AAA 基盤を利用するためのインタフェースを提供するために，AAA Agent が定義されている．SOAAA ではユーザが認証されると AAA server によって証明書が発行され，サービス提供サーバと NAS に保存される．これ以降ユーザが各サービスを利用する際には，毎回 NAS とサービス提供サーバ間で証明書の確認が行われ，AAA Agent のインタフェースによってポリシーに沿った課金情報の収集が行われる．しかし，SOAAA ではサービスの種別毎に AAA サーバで定義されたポリシー

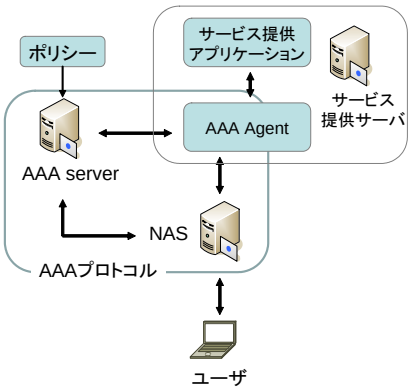

図 3: SOAAA アーキテクチャ

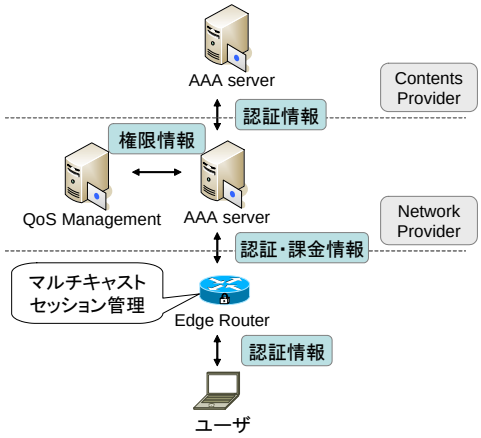

図 4: マルチキャストコンテンツ配信のための AAA フレームワーク

のみ用いることが可能であるため，各サービス毎に個別のポリシーを適用することが困難である．そのため，サービスの柔軟な権限付与，アカウンティングを行うことが出来ない．またマルチドメイン環境での使用が想定されていないため，汎用的な基盤として用いることは難しい．

3.2 マルチキャストコンテンツ CDN のフレームワーク

文献 [6] はマルチキャストを利用したコンテンツ配信のための AAA フレームワークを提案している。このフレームワークを図 4 に示す。

このフレームワークでは，Contents Provider(CP)，Network Provider(NP)，ユーザによってコンテンツ配信ネットワークが構成され，ユーザが一つのネットワークプロバイダ (NP)，複数のコンテンツプロバイダと契約する前提となっている．ユーザが Edge Router に接続要求を行うと，認証が行われて結果に応じた権限付与が行われる．認証については，CP，NP のどちらで行う方法も定義されている．サービスの利用が開始されると，NP によって QoS 制御が行われ，また Edge Router がマルチキャストグループへ

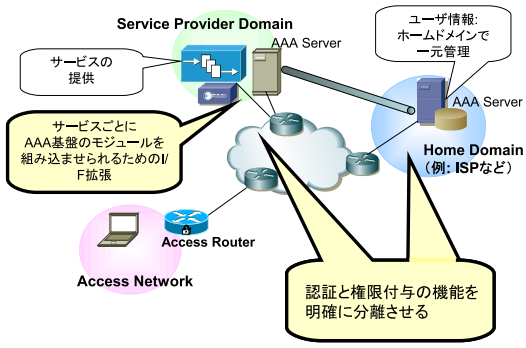

図 5: 汎用 AAA 基盤のアーキテクチャ

の参加，離脱状況を NP の AAA サーバへ報告することによって，課金情報収集が行われる．

しかしこの AAA フレームワークは，マルチキャストコンテンツ配信サービスに特化していることと具体的に使用する AAA プロトコルが明記されていないことから，このままでは様々なサービスに適用する汎用基盤を設計することは難しい．

3.3 汎用 AAA 基盤の必要性

以上では，関連研究として SOAAA 及びマルチキャストコンテンツ配信のための AAA フレームワークを取り上げたが，どちらもネットワークアクセスまで含めた汎用的なサービスに対する統一的な AAA 基盤として使用するには不十分である．ユーザが様々なネットワークサービスで共通のアカウントを使用し，サービス提供者が各サービスに対して新たに AAA システムを構築することなく十分な AAA 機能を実現するために，統一的な汎用 AAA 基盤が必要となる．そこで，汎用 AAA 基盤には以下の点が要求される．

・マルチドメインに対応していること
・AAA 機能を全て備えていること
・サービスに対し統一的なインタフェースを提供すること
・容易に拡張可能であること

4 汎用 AAA 基盤の設計

本論文では，2 章で述べたマルチドメインに対応したネットワークアクセスに特化した AAA システムを拡張し，汎用的なネットワークサービスを利用する際の共通 AAA システムとして使用可能にすることを目的とする．

4.1 汎用 AAA 基盤のアーキテクチャ

提案アーキテクチャを図 5 に示す．

マルチドメイン環境では，認証はドメインをまたがって行われる．しかし，権限付与や課金情報収集は各サービスがそれぞれのポリシーに従って行うべきである．そのため，認証と権限付与に関して明確な分離が要求される．そこで，

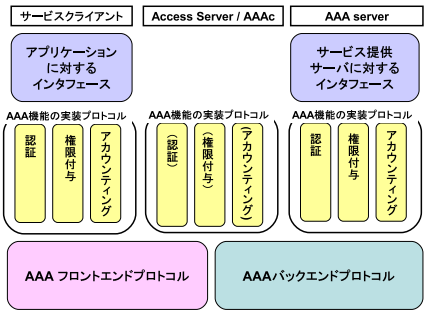

図 6: 汎用 AAA 基盤アーキテクチャの階層

本アーキテクチャでは，図 6 に示したように，AAA 基盤から各サービス提供サーバ，サービスクライアントに対するインタフェースを提供し，また認証と権限付与，課金情報収集の明確な分離を行い，様々なプロトコルの組み合わせを用いた認証と権限付与を可能にする．そしてこれらの各プロトコルをまとめて，AAA 機能の実装プロトコルとしてカプセル化し，上位アプリケーションに対するインタフェースを提供する．

4.2 上位アプリケーションへのインタフェース

汎用 AAA 基盤においては，共通の基盤を各サービスから利用する必要があるため，サービスクライアントとサービス提供サーバから AAA 基盤を利用するためのインタフェースを定義する必要がある．これにより，各サービス提供サーバはそのインタフェースを利用することによって AAA の機能を自身に実装することなく利用できるようになる．

汎用 AAA 基盤では，このインタフェースを HTTP や SMTP のようなテキストベースでやり取りされるコマンドによって定義する．このコマンド群は大きく分けて 4 種のメッセージから成る．

START コマンド
セッションのスタート時や認証，権限付与など各フェーズの開始時に使用される．

SET コマンド
ユーザ情報やサービス情報など，セッションに対して値をセットする際に使用される．

REQ コマンド
サービスのレジストレーションや権限付与などの要求を行う場合に使用される．

ANS コマンド
上記の各メッセージに対する返信として使用される．ANS のみが ACK として使用される他，補足情報を含むこともある．

次に，具体的なコマンドの例のうち主要なものと含まれる値を表 1 に示す．SET AUTH コマンドは，サービス

表 1: コマンドの例

コマンド	値
SET AUTH	destrealm, username
START SERVICE_SESSION	serviceID
REQ REG_SERVICE	serviceID
ANS AUTH	sessionID, Key

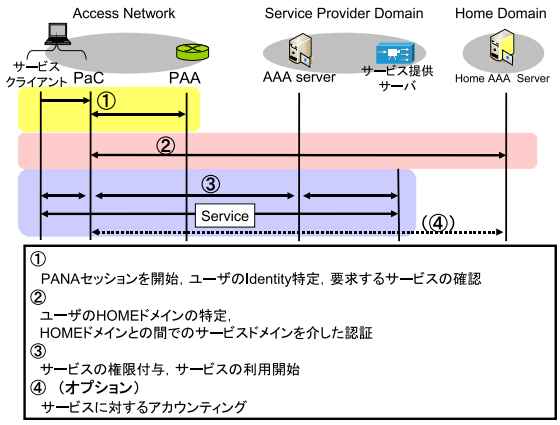

図 7: 提案アーキテクチャの動作

クライアントが認証要求を行う際にサービス提供ドメイン (dstrealm) とクライアント名 (username) を PaC に登録するために用いる．また，START SERVICE_SESSION コマンドはユーザが利用したいサービスの開始要求を行う際にその ID (serviceID) を AAA 基盤に通知するために用い，REQ REG_SERVICE コマンドは，サービス提供サーバが AAA 基盤にサービスを登録する際にその ID (serviceID) を登録するために用いる．ANS AUTH コマンドは，AAA 基盤で認証が終了した際に AAA 基盤がサービスクライアントにその結果を通達するために用いる．

4.3 汎用 AAA 基盤の動作

次に，この提案モデルにおける動作について，図 7 を用いて説明する．なお，文中の番号は図 7 に対応している．

1. まず，ユーザは自分が受けたいサービスがある場合にその ServiceID を取得する．ServiceID の取得方法は本論文の範囲外とするが，Web ページ上において XML 形式で公開されているなど様々なケースが考えられる．サービスクライアントはまず，PaC (PANA Client) に対して要求するサービスが使用するユーザ情報を伝える．これを受け取った PaC は PAA (PANA Authentication Agent) と PANA セッションを開始し，PAA に対してこのユーザの Identity を伝えるとともに，要求するサービスが提供されているサービスドメイン名を伝える．
2. PAA は PaC より伝えられたユーザの要求するサービ

スドメイン名に基づいて，そのサービスドメインの AAA サーバ (AAAse) に接続し，サービスに対する要求があったことをユーザの Identity と共に伝える．これを受け取った AAAse はその Identity よりユーザのホームドメインを判断し，ホームドメインの AAA サーバである AAAh に接続し，認証要求を行う．これ以降，例えば認証プロトコルとして EAP を用いるシステムであった場合，PaC と AAAh 間で EAP メッセージを PANA 及び Diameter 上でやり取りして認証を行うことになるが，これはすべて AAAse を経由して行うことになる．これにより AAAse はその認証の経緯や結果を知ることが出来る．ただし，EAP には End-to-End のセキュリティがあるため，AAAse はあくまで認証の結果や経緯を知ることができるだけで，ユーザの秘密情報を得ることはできない．

3. 認証が成功すると，サービスクライアントは認証時と同様に PaC を通して利用したいサービスの ServiceID を AAAse に要求する．これにより，サービスクライアントとサービス提供サーバ間で権限付与が行われる．この権限付与プロトコルは各サービスで異なるものを利用することができる．また，AAA 基盤上に権限付与の機能を実装させることも可能である．サービスクライアントとサービス提供サーバ間で権限付与のためのプロトコルが動作する場合には，AAA 基盤はこれを End-to-End で中継するだけであるが，AAA 基盤のセキュアパスをそのまま利用できるという利点がある．そして，ここで権限付与が行われるとサービスが利用可能となる．

4. 課金が行われる場合には，権限付与の終了時に AAAse から AAAh へ課金情報やサービスの使用状況の情報が渡される．その他に一定の使用時間単位ごとに課金される場合には，AAAse と PaC 間，またはサービス提供サーバとサービスクライアント間でタイムアウト時間をあらかじめ定めておき，タイムアウト時間に達した時にそれ以降もサービス利用を継続するかどうかの確認を行い，その情報を AAAh に伝えることでアカウンティングを行う．また，更に細やかなアカウンティング情報を取得する場合には PAA または PaC に対してアカウンティング情報を採取し，それを AAAse または直接 AAAh に対してフィードバックするように命令することで可能となる．

次に，ネットワークアクセスに特化した AAA システムを拡張し，汎用的なネットワークサービスを利用することができるようにするための AAA システムの拡張点について述べる．汎用 AAA 基盤では，認証と権限付与，アカウンティングの明確な分離を行うことで，各サービスがそれぞれのポリシーに従った権限付与や課金情報管理を行うことができる必要がある．そこで認証と権限付与を分離するために PANA および Diameter の拡張が必要となる．具体的には，そのような権限付与のためのプロトコルにおけるメッセージを運ぶための AVP，そしてその AVP 群をやり取りするためのコマンドを定義する．

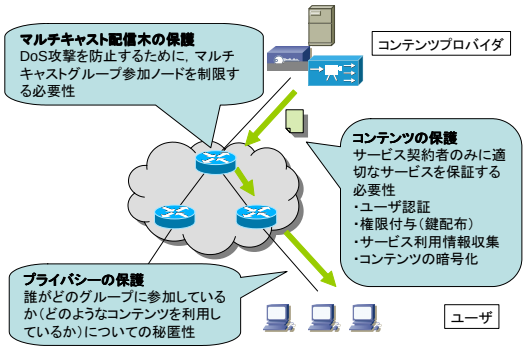

図 8: コンテンツ配信サービスに求められる機能

5 セキュアマルチキャストへの適用

2011 年の地上デジタル放送への完全移行に伴い，今後はテレビ番組もインターネットを介して配信されることが予想される．その際，非常に多くの受信者に効率よくコンテンツ配信を行うには，IP マルチキャストが利用されるものと思われる．そこで本論文が提案する汎用 AAA 基盤によってセキュアなマルチキャストコンテンツ配信が可能であるかを検証する．

IP マルチキャストを用いたコンテンツ配信サービスを実現する際には，セキュリティ上図 8 に示すコンテンツの保護，マルチキャスト配信木の保護，プライバシーの保護の 3 つを実現することが求められる．

これらの機能を実装していない場合，コンテンツの盗聴，不正なユーザのマルチキャストグループへの参加，不正な送信者によるマルチキャストグループへのパケットの送信，ユーザ情報の流出などの危険性がある．本論文ではこれら 3 つの機能の中のコンテンツの保護について焦点を当てる．コンテンツの保護とは，サービスの契約者のみが適切なサービスを受けられることを保証してサービスの非契約者によるコンテンツの不正利用を防止することである．そのためには，マルチキャストグループに参加する際のユーザの認証，契約サービスに対する権限付与，コンテンツの暗号化，コンテンツを復号するための安全な鍵配布が必要である．そこで，マルチキャストを用いたコンテンツ配信モデルに汎用 AAA 基盤を適用することによってコンテンツの保護を実現する．権限付与のプロトコルとしては，リアルタイムマルチメディア通信のための安全な鍵交換プロトコルである MIKEY (Multimedia Internet KEYing)[9] を用いる．

5.1 MIKEY

MIKEY とは，peer-to-peer，あるいは一対多，多対多のリアルタイムマルチメディア通信において Secure Realtime Transport Protocol (SRTP) のようなセキュリティプロトコルによって用いられる，安全に鍵をやりとりするための鍵管理プロトコルである．MIKEY では TEK Generation Key (TGK) と呼ばれる鍵をセキュリティプロトコルに対し

て提供し，これがデータの暗号鍵である Traffic Encryption Key (TEK) を生成するための鍵となる．また MIKEY ではセキュリティプロトコルにおける各暗号化コンテンツ (CSB: Crypto SessionBundle) は暗号化ストリーム (CS: Crypto Session) をまとめたものとして定義され，それぞれには CSB ID，CS ID という識別番号がつけられる．これらの情報やその他のポリシーは鍵配布サーバから安全な方法を用いて送信され，コンテンツ配信サーバとコンテンツ利用者との間で TGK の共有が可能となる．TEK は，TGK のほかに鍵の送信側，受信側で共有された CS ID や CSB ID，タイムスタンプ，乱数を用いて生成される．各パラメータは MIKEY パケットのヘッダに含まれ，鍵の送信者と受信者で共有されるため，送信者と受信者で同一の TEK を生成することができる．

MIKEY では様々な種類の鍵を用いる方法が定義されているが，本論文では TGK を暗号化するための鍵として送信者−受信者間で共有されるセッションキーを共有鍵として使うため，共有鍵を用いた方式を用いる．また MIKEY を権限付与プロトコルとして使用する場合，受信者から鍵要求を行うメッセージが必要となるが，MIKEY の鍵要求メッセージは共有鍵方式では定義されていない．公開鍵方式における鍵要求メッセージの拡張は MIKEY-RSA-R[10] に定義されているため，これと同様に，MIKEY における鍵要求メッセージを共有鍵方式においても定義する．

5.2 シーケンス

次に，汎用 AAA 基盤を適用したセキュアマルチキャストシステムのシーケンスを示す．次のような認証，権限付与の流れに沿って安全なサービス提供を実現する．

1. コンテンツプロバイダによるサービス登録手続き
2. AAA システムによるユーザの認証手続き
3. サービスセッションの開始手続き
4. ユーザに対する権限付与手続き
5. サービス開始．ユーザがマルチキャストグループに参加し，コンテンツ利用を開始する

以下では，それぞれの項目について詳細を説明する．

5.2.1 サービス登録

コンテンツ配信サービスの提供を開始するにあたり，サービス提供サーバは自身の提供するサービスを自身のドメイン内の AAA サーバに登録しておく必要がある．これは，同一ドメイン内の AAA サーバにおいて各サービスを一意に識別する必要があるためである．サービス登録の様子を図 9 に示す．

まず，サービスクライアントであるサービス提供サーバは START SERVER SESSION コマンドを AAA サーバに送信する．これはサービス提供サーバが AAA サーバに一意に識別される必要があることから，AAA サーバとの間にセッションを開始するためのものである．START SERVER SESSION コマンドを受け取った AAA サーバは，サービス提供サーバに対して同ドメイン内で一意となる ServerID を割り当ててこれを通知するとともに，ここでサービス提供サーバとのセッションを開始する．セッションが開始されると，サービス提供サーバは次にサービスの登録を行う．サービス提供サーバは利用するサービスの ServiceID を含んだ AAA サーバに送信し，登録が正しく行われた場合には「ANS OK」によって通知される．サービスの登録はサービスごとに行われ，登録要求は複数回行うことができる．

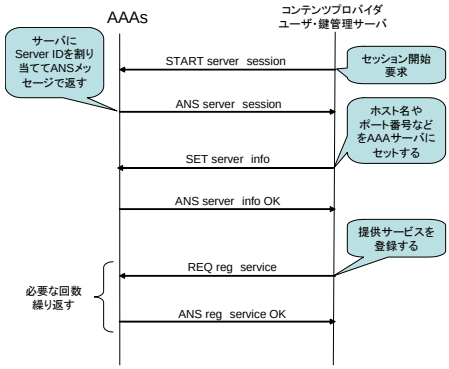

図 9: サービス登録

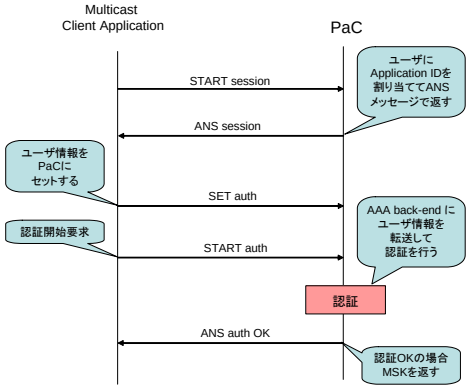

図 10: 認証

5.2.2 認証

次に，ユーザがコンテンツ配信サービスを利用しようとする際の認証の流れを説明する．この様子を図 10 に示す．

まず，サービスクライアントであるアプリケーションは START SESSION コマンドを PaC に送信する．これはサービスクライアントが PaC に一意に識別される必要があることから，PaC との間にセッションを開始するためのものである．START SESSION コマンドを受け取った PaC はサービスクライアントに対して同ホスト内で一意となる Application ID を割り当て，これを通知するとともに，ここでサービスクライアントとのセッションを開始する．PaC から Application ID を受け取ったサービスクライアントは，自身に割り当てられた Application ID と共にユーザ名やパ

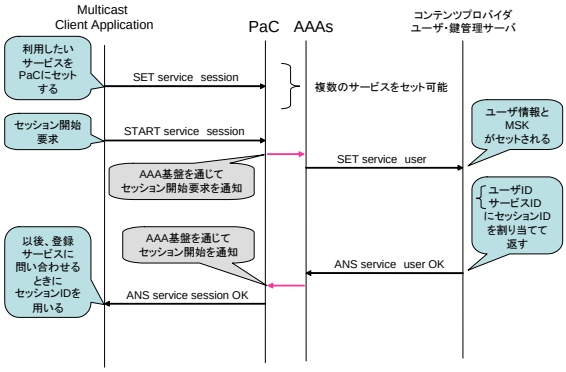

図 11: サービスセッション開始

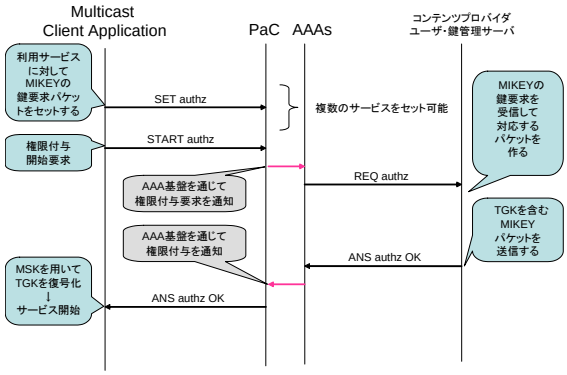

図 12: 権限付与

スワードまたは証明書と共に，利用するサービスプロバイダドメインを PaC に通知する．これを受け取った PaC は Application ID からそのサービスクライアントのセッションを識別し，該当するセッションに通知された値をセットする．その後サービスクライアントが START AUTH コマンドを送信すると，セットされたユーザ情報が AAA 基盤に通知され，ユーザの認証が行われる．

無事に AAA システムで認証が完了すると PaC に認証完了が通知され，PaC はサービスユーザセッションに記憶された Application ID からクライアントアプリケーションを特定し，そのアプリケーションに対して「ANS AUTH OK」コマンドを送信することで認証の成功と共に Master Session Key(MSK) を通知する．MSK は後にサービス提供サーバにも通知され，クライアントアプリケーションとサービス提供サーバとの間の共有鍵として用いられる．

5.2.3 サービスセッション開始

認証が完了すると，ここからサービスクライアントは利用するサービスの要求を行う．この様子を図 11 に示す．

まずサービスクライアントは，「SET SERVICE SESSION」コマンドを用いて PaC に対して要求するサービスを通知する．これを受けた PaC はサービスユーザセッションに各サービスを登録する．ここで，サービスは複数登録することが可能である．次に「START SERVICE SESSION」コマンドをアプリケーションが送信すると，PaC は AAA サーバにサービスクライアントに対するサービスセッションの開始を要求する．AAA サーバはこれを受けとると，サービスユーザセッションに該当するサービスクライアントが要求している ServiceID を記憶すると共に，その ServiceID が指し示すサービス提供サーバに対して「SET SERVICE USER」コマンドを用いてあるユーザに対するサービスセッションの開始を通知する．また，この際にユーザ情報と共に該当するサービスクライアントの MSK も通知する．このとき通知される MSK が，サービスクライアントとサービス提供サーバの間での共有鍵として用いられる．サービス提供サーバは通知されたユーザに対してサービスごとのセッションを開始して，必要であればユーザに対してセッションを識別するための SessionID を割り当て，これを AAA サーバに対して「ANS SERVICE USER」コマンドを用いて通知する．SessionID は以降のサービス管理を安全に行うために用いられる．AAA 基盤を通じてこのコマンドが PaC まで伝えられると，PaC は「ANS SESSION USER」コマンドによってサービスクライアントに対してサービス提供サーバから割り当てられた SessionID を通知する．以上の流れによって，サービスクライアントとサービス提供サーバ間でサービスセッションが開始される．

5.3 権限付与

サービスセッションが開始されると，次はサービスクライアントに対する権限付与が行われる．この様子を図 12 に示す．提案システムでは，MIKEY の TGK を各サービスに対する権限としてサービスクライアントに付与する．

まず，クライアントアプリケーションは受け取った MSK を共有鍵として MIKEY の鍵要求メッセージを作成し，「SET AUTHZ」コマンドでこれを PaC に対して通知した後,「START AUTHZ」コマンドにて権限付与を要求する．これを受け取った PaC は通知されたサービス情報を，サービスクライアント情報とともに AAA 基盤へ通知し，サービス提供ドメインの AAA サーバまで通知される．AAA サーバはこれを受け取ると，受け取ったサービスクライアントの権限付与のための情報を「REQ AUTHZ」コマンドによりサービス提供サーバに伝える．サービス提供サーバはこれに対して「ANS AUTHZ OK」コマンドを返すと同時に MSK を用いて暗号化した TGK を含む MIKEY パケットを AAA サーバへ送信する．このパケットは AAA 基盤を通じて PaC まで届けられ，これを受け取った PaC では「ANS AUTHZ OK」コマンドを用いてクライアントアプリケーションに対してパケットを届ける．

サービスクライアントは TGK を含む MIKEY メッセージを受け取ると，サービス提供サーバとの間で共有されている MSK を用いてメッセージの中から TGK を復号化して取り出す．TGK を入手できた場合，対応するコンテンツ配信サービスを提供しているマルチキャストグループに

表 2: 実装環境

項目	内容
OS	FreeBSD 5.4-Release (KAME 適用), FreeBSD 6.2-Release
言語	C 言語

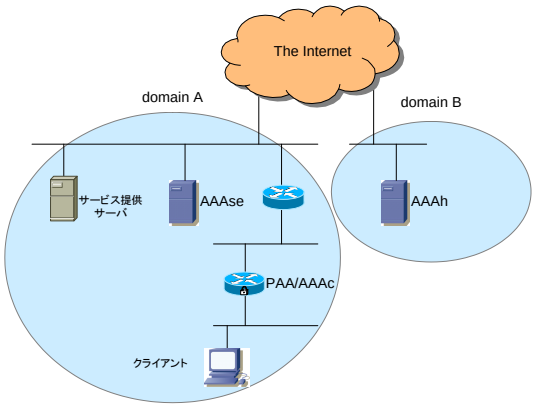

図 13: 実験環境

参加し，マルチキャストパケットを受信する．もしこの時点で TGK を正しく入手できているならば，サービスクライアントは TEK を生成して正しくコンテンツを復号化し，利用を開始することができる．

6 実装と評価

本論文では，汎用 AAA 基盤を適用したセキュアマルチキャストシステムの実装，評価を行った．

6.1 実装環境

まずは本システムの実装環境を表 2 に示す．

実装は FreeBSD 5.4-Release に KAME と呼ばれるパッチを当てたものまたは FreeBSD 6.2-Release の 2 つのオペレーションシステム上で開発および動作確認を行った．FreeBSD 5.4 を用いた理由は，KAME が FreeBSD 5.4 までの対応となっているからである．なお，開発は全て C 言語を利用して行った．

次に評価を行った際の環境について説明する．実験は図 13 に示すネットワーク上で行った．

ここで，以下ではサービス提供ドメインの AAA サーバを AAAse と表記する．図の左側のネットワークは図の右側のネットワークとはまったく異なるネットワークであり，それぞれのネットワークを仮想的な ISP として実験を行った．またなるべく実環境に近い条件で実験を行うため，各 AAA サーバ間での通信はすべて IPsec により暗号化されるよう設定した．実験に使用した各マシンのスペックを表 3 に示す．

表 3: 実験に使用したマシンのスペック

マシン	CPU	メモリ
クライアント	Intel Pentium M processor 1.60MHz	1GB
PAA/AAAc	VIA C3 800 MHz	512MB
AAAse	Intel Celeron 2.53GHz	1GB
AAAh	Intel Celeron 2.53GHz	1GB
サービス提供サーバ	VIA C3 800 MHz	512MB

表 4: 各ノード間の RTT

区間	IPsec 適用前	IPsec 適用後
クライアント/PaC - PAA/AAAc 間	0.330 msec	-
PAA/AAAc - AAAse 間	0.402 msec	0.661 msec
AAAse - AAAh 間	2.948 msec	3.189 msec
AAAse - サービス提供サーバ 間	0.363 msec	-

6.2 評価・考察

本論文で提案した汎用 AAA 基盤を適用したセキュアマルチキャストシステムにおいて，サービス開始までの各ステップの処理にかかる時間を測定した．

認証処理にかかる時間の測定は，図 10 のシーケンス通りに認証を行った際の，クライアントが PaC に START AUTH メッセージを送信した時点からクライアントが ANS AUTH を受信した時点までの時間を測定した．セッション開始処理にかかる時間の測定は，図 11 のシーケンス通りにセッション開始処理を行った際の，クライアントが PaC に START SERVICE_SESSION メッセージを送信してセッション開始要求がはじまった時点からクライアントが ANS SERVICE_SESSION を受信した時点までの時間を測定した．また権限付与処理にかかる時間の測定は，図 12 のシーケンス通りに権限付与を行った際のクライアントが PaC に START AUTHZ メッセージを送信して PaC で権限付与要求がはじまった時点からクライアントが ANS AUTHZ を受信した時点までの時間を測定した．

まず各ノード間の Round-Trip Time (RTT) を表 4 に示す．

次に，各処理にかかった時間を表 5 に示し，サービス開始までに各ノードでかかった処理時間の内訳を表 6 に示す．

認証処理は他の処理に比べて多く時間が費やされた．これは，認証処理ではネットワーク的に遠い位置にある AAAse と AAAh が通信する必要があることと，認証処理のシーケンスが複雑でありバックエンドのノードが多くのメッセー

表 5: 各処理の処理時間

処理	処理時間 (ms)
認証	29.45
サービスセッション開始	6.67
権限付与	6.70
合計	42.82

表 6: サービス開始までの各ノードの処理時間

ノード (区間)	処理時間 (ms)
PaC	3.78
PAA/AAAc	15.23
AAAse	4.83
AAAh	1.44
ServiceProviderApp	1.62
PaC-PAA/AAAc 間の RTT	2.31 (7RTT)
PAA/AAAc-AAAse 間の RTT	3.31 (5RTT)
AAAse-AAAh 間の RTT	9.57 (3RTT)
AAAse-ServiceProvider 間の RTT	0.73 (1RTT)
合計	42.82

ジを交換する必要があるためである．さらに RTT の合計に占める AAAse - AAAh 間の RTT の割合が大きいため，特に AAAse - AAAh 間の距離が離れているほど認証完了に時間がかかることがわかる．AAAh の認証情報の複製をネットワーク的に分散して配置することによってボトルネックを解消できると考えられるが，複製を配置するドメイン同士に強い信頼関係がある必要がある．またサービスセッション開始処理，権限付与処理では AAAse と AAAh が通信する必要はないため，ネットワーク上の距離的なボトルネックは存在しなかった．汎用 AAA 基盤ではシングルサインオンでサービスが利用可能であるので，認証処理に要する時間はサービスセッション開始処理，権限付与処理に要する時間と比較して重要でないと考えられる．よって，本システムは十分実用的であると言える．

また，今回は一例としてセキュアマルチキャストシステムに汎用 AAA 基盤を適用したが，その他にも QoS などのサービスに対しても汎用 AAA 基盤を適用できると考えられる．

7 結論

本論文では，インターネット上の様々なサービスに対して，ユーザ及びサービス提供サーバへのインタフェースを定義し，更に認証プロトコル，権限付与プロトコル，アカウンティングプロトコルを分離して使うためのフレームワークを提案し，プロトタイプ実装を行った．また，ネットワークサービスの一例として汎用 AAA 基盤を適用したセキュアマルチキャストシステムを設計，実装し，評価した．その結果，本提案システムは従来の AAA システムでは不可能であった統一的な汎用 AAA 基盤として機能し，本システムを用いることで様々なサービスのクライアント及びサービス提供サーバに容易かつ十分な AAA 機能を提供できると結論づけられた．

参考文献

[1] P.Calhoun, J.Loughney, E.Guttman, G.Zorn and J.Arkko. Diameter Base Protocol. RFC 3588, *IETF*, Sep. 2003.

[2] P. Calhoun, T. Johansson, C. Perkins and P. McCann. Diameter Mobile IPv4 Application. RFC 4004, *IETF*, Aug. 2005.

[3] P. Calhoun, D. Spence and D. Mitton. Diameter Network Access Server Application. RFC 4005, *IETF*, Aug. 2005.

[4] P.Jayaraman, R. Lopez, Y.Ohba (Ed.), M. Parthasarathy and A.Yegin. Protocol for Carrying Authentication for Network Access (PANA) Framework. RFC 5193, *IETF*, May. 2008.

[5] Rui He, Man Yuan, Jianping Hu, Hong Zhang, Zhigang Kan and Jian Ma. A Novel Service-Oriented AAA Architecture. International Symposium on Personal,lndoor and Mobile Radio Communication Proceedings, *IEEE*, Sep. 2003.

[6] Hiroaki Satou, Hiroshi Ohta, Jun Nishikido and Tsunemasa Hayashi. Authentication, Authorization and Accounting Framework for Multicast Content Delivery. 2005 Asia-Pacific Conference on Communications, *IEEE*, Oct. 2005.

[7] C.Rigney, S.Willens, A.Rubens and W.Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865, *IETF*, Jun. 2000.

[8] S.Kent and K.Seo. Security Architecture for the Internet Protocol. RFC 4301, *IETF*, Dec. 2005.

[9] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman. MIKEY: Multimedia Internet KEYing. RFC 3830, *IETF*, Aug. 2004.

[10] D. Ignjatic, Polycom, L. Dondeti, QUALCOMM, F. Audet, P. Lin, Nortel. MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY). RFC 4738, *IETF*, Nov. 2006.