

認証、認可、アカウントिंग

はじめに

この数年、さまざまな新しいアクセス技術の利用者が、ネットワーク利用時間に対して課金するために、認証や課金記録についての手法を模索し続けた結果、認証、認可、およびアカウントिंग (authentication, authorization, and accounting : AAA) の仕組みは劇的に変化しました。

シスコシステムズの提供する、機能豊富で堅牢な AAA 実装は、以下のような幅広いアプリケーション クライアントに対応します。

- 802.11b
- ケーブルおよびDSL
- ダイアルアップ
- ファイアウォール
- GPRS (Gateway General Packet Radio Service) および GGSN (GPRS Support Node)
- IPSec (IP Security)
- MPLS (マルチプロトコル ラベル スイッチング)
- OSP (Open Settlement Protocol)
- PDSN (Packet Data Serving Node)
- 公開キー基盤 (Public Key Infrastructure: PKI)
- SIP (Session Initiation Protocol)
- DCN (Data Communication Network)
- トンネリング
- VoIP (Voice over IP)
- RADIUS (Remote Access Dial-In User Service)

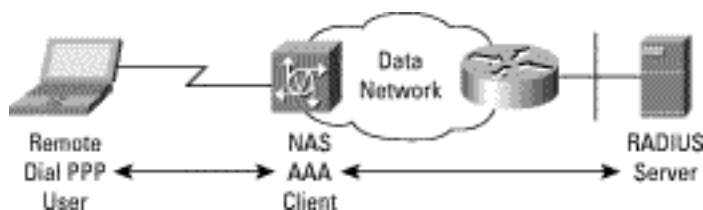
Cisco IOS®ソフトウェアのAAA ネットワーク セキュリティ サービスは、ルータまたはアクセスサーバ上にアクセス制御機能を実装するための基本的なフレームワークを提供します。Cisco IOS AAA は、独立した 3 つのセキュリティ機能を一貫した手法で実装するための構造的なフレームワークです。これにより、認証、認可、およびアカウントング サービスをモジュール形式で実行できます。

Cisco IOS AAA の利点は以下のとおりです。

- 柔軟性と制御能力の強化
- スケーラビリティ
- 標準の認証機能 (RADIUS, TACACS+ [Terminal Access Controller Access Control System Plus], Kerberos)

Cisco IOS AAA クライアントはルータまたは NAS (ネットワーク アクセス サーバ) 上に実装し、あらゆる認証、認可、およびアカウントング機能をローカルに実行できます。大量のデータが保管されるため、このモデルは拡大することはありません。RADIUS プロトコルによって外部サーバの利用が可能になるので、AAA は外部サーバに対し、問い合わせと応答の受信を行えます。RADIUS プロトコルは、クライアント / サーバ モデルに基づきます。Cisco AS5200 アクセスサーバなどの NAS は、RADIUS のクライアントとして機能します。クライアントはユーザ情報を指定の RADIUS サーバに渡し、このサーバから返される応答に従って処理を実行します。RADIUS データベースには、セキュリティ、ネットワークアクセス、および課金記録に関する数千規模のユーザ情報に加え、接続関連の他のデータが保存されます。

図 1:AAA クライアントと RADIUS サーバの関係





AAA サービスの必要性

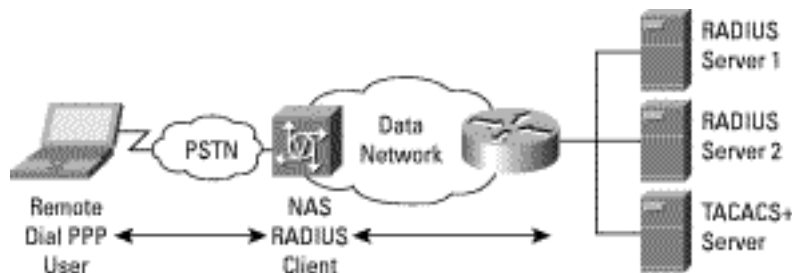
ネットワークにアクセスするユーザのセキュリティと、ユーザ情報を動的に定義してネットワーク資源へのアクセスを取得する機能は、非同期ダイヤルアクセス時代からある手法です。AAA ネットワーク セキュリティ サービスの提供する基本フレームワークを使用すると、ネットワーク管理者は、ネットワークの入口またはネットワーク アクセスサーバ上にアクセス制御機能を実装できます。これは、従来はルータまたはアクセスサーバで実現するしかなかった機能です。認証機能はユーザを識別します。認可機能は、このユーザに許可された機能を判断します。アカウントینگ機能はネットワークの利用時間を監視し、課金データを作成します。

AAA 情報は通常、外部データベース、または RADIUS、TACACS+ といったリモートサーバ上に保存されます。この情報は、アクセスサーバまたはルータ上にローカルに保存することもできます。RADIUS、TACACS+ などのリモート セキュリティ サーバは、対になった属性値 (attribute-value:AV ペア) を関連付けることで、ユーザ固有の権限を割り当てます。AV ペアは、適切なユーザにアクセス権限を定義する機能です。すべての認可手段は、AAA によって定義する必要があります。

従来の AAA 利用方法

図 2 は AAA の従来の使用方法、つまりダイヤルアップ PPP (Point-to-Point Protocol) 接続ユーザに対する認証やアカウント記録を維持する仕組みを示します。この実装においてユーザは、データネットワーク エッジにあるいずれかの NAS のポートに対応付けられた電話番号をダイヤルします。ユーザ ID とパスワードが設定されている場合は、サーバは NAS データベースをローカルに検索するか、あるいは設定済みの RADIUS サーバに問い合わせを送り、ネットワークへのアクセスを許可するか拒否するかを判断します。許可されたユーザであれば、通常 RADIUS サーバは設定値または AV ペアを NAS に送ります。これにより、このユーザに許可されているサービスタイプが決定されます。

図 2: 従来の AAA 実装





VoIP プリペイド課金ソリューション

シスコのプリペイド課金 VoIP 実装(図 3)は、音声ゲートウェイと課金アプリケーションとの間で、RADIUS プロトコルを使用して AAA 情報をやり取りします。

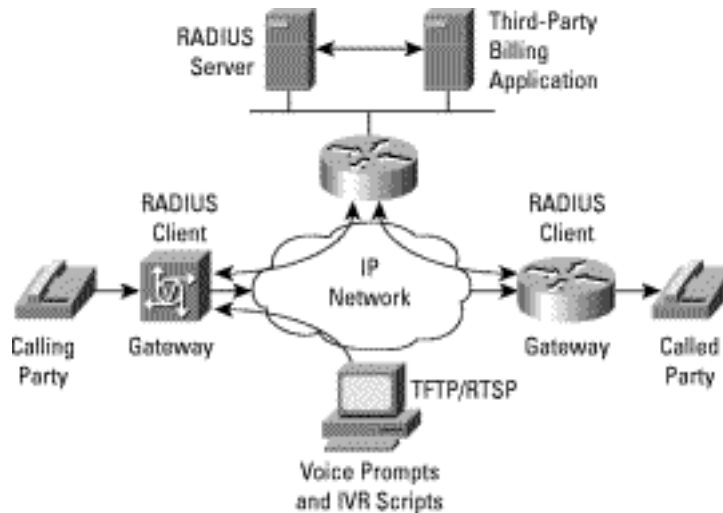
こうしたプリペイドサービスが対象とする市場は、旅行者、移住、移動端末利用者層(軍関係者など)のほか、信用履歴の制限により、自宅に個人電話を引くための他の手段を持たない人々です。こうしたすべてのユーザは、スーパーマーケットや他の多くの小売店で購入可能なプラスチックの通話カードを使用するだけで、長距離または国際通話をどんな場所からでもすぐに利用できるようになります。

シスコの分散型 VoIP プリペイド通話ソリューションを実装するには、サービスプロバイダー ネットワーク内のすべての音声ゲートウェイが、プリペイド IVR(Interactive

Voice Response: 自動音声応答)スクリプトを実行する必要があります。このスクリプトと言語選択機能を各ゲートウェイに保存し、そこから実行されるようにします。プリペイド IVR スクリプトは、通話者に対してどのオーディオ プロンプトを起動するかを判断します。また、受話器(ハンドセット)によって入力され、各ゲートウェイで DTMF (Dual-Tone Multifrequency) 検知によって抽出された通話者の応答を収集します。時間を計り、通話を終了する仕組みも VoIP ゲートウェイから実行されます。これにより、許可された時間が経過した時点で通話を確実に切断できます。

プリペイド通話課金アプリケーションは、通話者の全記録の保持、通話者の認証、通話の課金と認可を行い、通話の終了時には、通話者のカードの残高を更新します。

図 3:AAA を使用した VoIP プリペイド通話ソリューション



RADIUS プロトコル

RADIUS は、ネットワーク アクセス サーバのベンダー数社が採用するプロトコルであり、ISP (インターネット サービス プロバイダー) を含む幅広い顧客層に支持されています。シスコは Access Registrar (AR) やアクセスコントロールサーバ (ACS) など、いくつかの RADIUS サーバ実装をサポートしています。

RADIUS プロトコルは、NAS と RADIUS 認証サーバとの間で、認証、認可、および設定情報をやり取りします。RADIUS プロトコルによって運ばれる要求と応答は、RADIUS 属性と呼ばれます。この属性は、ユーザ名やサービスタイプなどを表します。これらは、RADIUS サーバがユーザを認証し、これらのユーザに対して認可ネットワークを確立するために必要となる情報を提供します。また、RADIUS プロトコルは NAS と RADIUS アカウンティングサーバとの間で、アカウンティング情報のやり取りも行います。

DIAMETER プロトコル

DIAMETER は、次世代 AAA サーバに対する IETF (Internet Engineering Task Force) の新フレームワークです。DIAMETER に関する要件は、Mobile IP ROAMOPS (ローミング処理) TR45.6 作業グループによって規定されています。DIAMETER はまた、ネットワーク資源に対する認証または認可機能の提供、あるいはネットワーク資源の利用(音声通話など) に対する課金のためのアカウントینگ取得機能が必要となる場面において、他の技術によっても定義されます。

DIAMETER の基本プロトコルは、Mobile-IP、NASREQ、および ROAMOPS に対する AAA フレームワークを提供します。DIAMETER プロトコルは、RADIUS モデル内の欠陥には対処しません。DIAMETER は RADIUS プロトコルと同じデータユニットは使用しませんが、RADIUS と下位互換を保つことで、円滑な移行を促進します。DIAMETER と RADIUS の主要な違いは、DIAMETER ではピアツーピアで多様なメッセージを交換できる点です。



DIAMETER RFC は、次のように規定しています。
 「DIAMETER の基本概念は、AAA サービスを新たなアクセス技術に提供できるような、拡張可能な基本プロトコルの提供である。このプロトコルは現時点では、従来の PPP においても、あるいは ROAMOPS モデルや Mobile-IP を考慮した環境においても、インターネットアクセスのみに関係する。」

現時点では、Cisco IOS ソフトウェアは DIAMETER をサポートしていません。

DIAMETER の利点

特徴	DIAMETER によるサポート
ピアツーピアによる双方向通信	• プッシュ型およびプル型のアプリケーションモデルまたはアーキテクチャを実現 (RADIUS は単方向)
高い効率性	• 効率性を高める 32 ビット VSA のサポート (RADIUS = 8 ビット) • より多くのペンディング AAA 要求の処理 • ハードウェアプロセッサの新技术を利用した 32 ビット配置
卓越した信頼性と可用性	• AAA クライアント / サーバの送信 / 受信確認による要求受信 • 障害またはペンディング障害を通知する「キープアライブ」メッセージのサポート
安全性	• 暗号化による認証のリプレイ攻撃防止

RADIUS と DIAMETER の違い

DIAMETER プロトコルは、RADIUS との下位互換性があります。DIAMETER は次世代 AAA プロトコルであり、RADIUS の持つ以下の欠点を補います。

特徴	RADIUS の欠点	DIAMETER の改良点
属性データの厳格な制限	属性ヘッダ内のデータフィールド長として 1 バイトのみを予約 (最大 255)	データフィールド長として 2 バイトを予約 (最大 16,535)
非効率な再送アルゴリズム	再送の識別用に 1 バイトのみを識別子フィールドとして予約。これにより、待機可能な要求数が制限されます (最大 : 255)	同機能に 4 バイトを予約 (最大 : 2 ³²)
サーバへのフロー制御不可	UDP (User Datagram Protocol) による処理であり、UDP フローを制御する標準スキームを持たない	UDP パケットフローを制御するスキーム (ウィンドウイングスキーム)
エンドツーエンドのメッセージ確認	要求を発したクライアントは、成功またはエラーを通知する応答を期待しますが、サーバが適切に要求を受け取ったかどうかを確認できません。	クライアントは、サーバによる確実なエラー通知、および要求の受信確認を期待できます。

特徴	RADIUS の欠点	DIAMETER の改良点
無通知のパケット破棄	期待された情報を保持しないパケット、またはエラーのあるパケットは、通知されことなく破棄されます。このように何の応答もないと、クライアントはサーバがダウンしているとみなして処理を進めてしまう恐れがあります。この場合、クライアントはセカンダリサーバ宛にパケットの送信を試みます。	サーバはエラーメッセージの送信により、クライアントに問題の発生を通知できます。
サーバがフェイルオーバーをサポートしない	サーバには、稼働の中止、または現在稼働中であることを通知する手段がありません。	キープアライブメッセージと、サーバが一定期間ダウンすることを伝えるメッセージをサポート
認証リプレイ攻撃	PPP CHAP を使用すると、すべての RADIUS クライアントはチャレンジ / レスポンスの流れを生成できます。これは、チェーン内のどの RADIUS クライアントまたはプロキシサーバでも傍受できます。したがって、別の RADIUS クライアントがこのチャレンジ / レスポンスの流れを、任意の時点でリプレイする可能性があります (RADIUS 拡張でも、EAP プロトコルによってこの問題の一部解決が可能)	チャレンジ / レスポンス属性を、エンドツーエンドの暗号化および認証によって安全化
ホップ間セキュリティ	ホップ間セキュリティのみをサポート。送信元を追跡できないデータであれば、どのホップでもこれを簡単に変更できます。	エンドツーエンドのセキュリティをサポート。これにより、通知もなくデータが変更されないことを保証できます。
ユーザ独自のコマンドがサポートされない	ベンダー独自の属性はサポートされますが、ベンダー独自のコマンドはサポートされません。	ベンダー独自のコマンドコードをサポート
高負荷の処理コスト	配置要件がないため、ほとんどのプロセッサに不要な負荷を与えます。	32 ビット配置要件を持ち、ほとんどのプロセッサが効率よく処理を行えます。

まとめ

Cisco IOS AAA サービスは、昔からの遺産（レガシー）を従来のデータダイヤル技術市場と共有し、この市場にも適用可能な属性とサービスを持つことを、多数の技術グループからも認められています。

評価すべき重要な点は、現在の RADIUS プロトコル実装を、どのような実用サービスで利用できるのかということです。現在の新たな世界に適合させようと、本来 RADIUS 向けではない新機能を改良することは避けるべきです。多くの新しい技術は、RADIUS の豊富な機能だけでなく、次世代 AAA プロトコルである DIAMETER の柔軟性と堅牢性を兼ね備えた、安全性および信頼性の高いピアツーピアのフレームワークを必要としています。

詳細について

詳細な技術情報については、『RADIUS Support in Cisco IOS Software』またはシスコの設定に関する関連文書を参照してください。

AAA 関連 Web サイト：

<http://www.in.cisco.com/ios/security/aaa.shtml>

参考文献

RADIUS IETF 標準 RFC

RADIUS プロトコル仕様は、認証、アカウントティング、および拡張機能に関する以下の RFC で構成されます。

- RFC 2865 - Remote Authentication Dial In User Service (RADIUS) (obsoletes RFC 2138)
- RFC 2866 - RADIUS Accounting (obsoletes RFC 2139)
- RFC 2867 - RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868 - RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 - RADIUS Extensions
- DRAFT RFC - Introduction to Accounting Management
- DRAFT RFC - Accounting Attributes and Record Formats

- DRAFT RFC - Criteria for Evaluating AAA Protocols for Network Access
- DRAFT RFC - Criteria for Evaluating NAS Protocols
- DRAFT RFC - Network Access Server Requirements Next Generation (NASREQNG) NAS Model
- DRAFT RFC - Network Access Servers Requirements: Extended RADIUS Practices

DIAMETER RFC

DIAMETER プロトコル仕様は、ベースプロトコルや拡張仕様、または Mobile IP、MIB などのアプリケーションに関する各種の IETF 草案で構成されます。

<http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-07.txt>

<http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-nasreq-07.txt>

<http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-mobileip-07.txt>

<http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-cms-sec-02.txt>

<http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-api-01.txt>

<http://search.ietf.org/internet-drafts/draft-koehler-aaa-DIAMETER-base-protocol-mib-01.txt>

<http://search.ietf.org/internet-drafts/draft-le-aaa-DIAMETER-mobileipv6-00.txt>

<http://search.ietf.org/rfc/rfc2002.txt>



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先