認証、許可、アカウンティングコンフィギュレーションガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

認証の設定 3

機能情報の確認 3

認証の設定の前提条件 4

認証の設定に関する制約事項 4

認証の設定に関する情報 4

認証の名前付き方式リスト 4

方式リストとサーバ グループ 5

方式リストの例 6

RADIUS 認可変更について 7

CoA 要求 7

RFC 5176 規定 8

CoA 要求応答コード 9

セッションの識別 9

CoA ACK 応答コード 10

CoA NAK 応答コード 10

CoA 要求コマンド 10

セッション再認証 10

セッションの終了 11

CoA 要求の disable host port 11

CoA 要求の bounce port 11

ドメイン ストリッピング 12

AAA 認証方式を設定する方法 13

AAA を使用したログイン認証の設定 13

イネーブル パスワードによるログイン認証 15

Kerberos によるログイン認証 15

ライン パスワードによるログイン認証 16

ローカル パスワードによるログイン認証 16
group RADIUS によるログイン認証 16
アクセス要求での RADIUS 属性 8 の設定 17
group TACACS によるログイン認証 17
group group-name によるログイン認証 17
AAA を使用した PPP 認証の設定 18
Kerberos による PPP 認証 20
ローカル パスワードによる PPP 認証 20
group RADIUS による PPP 認証 21
アクセス要求での RADIUS 属性 44 の設定 21
group TACACS による PPP 認証 21
group group-name による PPP 認証 21
PPP 要求に対する AAA スケーラビリティの設定 22
AAA を使用した ARAP 認証の設定 22
認可済みゲスト ログインを許可する ARAP 認証 25
ゲスト ログインを許可する ARAP 認証 25
ライン パスワードによる ARAP 認証 25
ローカル パスワードによる ARAP 認証 25
group RADIUS による ARAP 認証 26
group TACACS による ARAP 認証 26
group group-name による ARAP 認証 26
AAA を使用した NASI 認証の設定 27
イネーブル パスワードによる NASI 認証 29
ライン パスワードによる NASI 認証 29
ローカル パスワードによる NASI 認証 29
group RADIUS による NASI 認証 29
group TACACS による NASI 認証 30
group group-name による NASI 認証 30
ログイン入力にかける時間の指定 30
特権レベルでのパスワード保護のイネーブル化 31
パスワード プロンプトに表示するテキストの変更 32
ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにする 32

AAA 認証のメッセージ バナーの設定 33
ログイン バナーの設定 34
Failed-Login バナーの設定 34
AAA パケット オブ ディスコネクトの設定 35
二重認証のイネーブル化 36
二重認証の機能 37
二重認証の設定 38
二重認証後のユーザ プロファイルへのアクセス 39
自動二重認証のイネーブル化 40
自動二重認証の設定 41
自動二重認証のトラブルシューティング 42
RADIUS CoA 用の動的認可サービスの設定 43
bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定 45
サーバ グループ レベルでのドメイン ストリッピングの設定 46
非 AAA 認証方式 47
ライン パスワード保護の設定 47
ユーザ名認証の確立 49
CHAP 認証または PAP 認証の有効化 50
PPP カプセル化の有効化 52
PAP または CHAP のイネーブル化 52
着信認証と発信認証 53
発信 PAP 認証のイネーブル化 54
PAP 認証要求の拒否 54
共通 CHAP パスワードの作成 54
CHAP 認証要求の拒否 55
ピアが認証されるまで CHAP 認証を遅延する 55
MS-CHAP の使用 56
MS-CHAP を使用した PPP 認証の定義 57
認証の例 58
RADIUS 認証の例 58
TACACS 認証の例 60
Kerberos 認証の例 61

AAA スケーラビリティの例 61
例：AAA 認証のログイン バナーおよび Failed-Login バナーの設定 62
AAA パケット オブ ディスコネクト サーバ キーの例 63
二重認証の例 63
二重認証による AAA のローカル ホストの設定例 64
第 1 段階の PPP 認証と認可に関する AAA サーバの設定例 64
第 2 段階の Per-User 認証と認可に関する AAA サーバの設定例 65
TACACS による設定完了の例 65
自動二重認証の例 68
その他の参考資料 70
認証の設定に関する機能情報 72
RADIUS 許可の変更 79
機能情報の確認 79
RADIUS 認可変更に関する情報 80
RADIUS 認可変更について 80
CoA 要求 80
RFC 5176 規定 80
CoA 要求応答コード 82
セッションの識別 82
CoA ACK 応答コード 82
CoA NAK 応答コード 83
CoA 要求コマンド 83
セッション再認証 83
セッションの終了 83
CoA 要求の disable host port 84
CoA 要求の bounce port 84
RADIUS 認可変更の設定方法 85
RADIUS 認可変更の設定 85
bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定 87
RADIUS CoA 用の動的認可サービスの設定 88
RADIUS 認可変更のモニタリングとトラブルシューティング 90
RADIUS 認可変更の設定例 91

例：RADIUS 認可変更の設定 91
例：bounce および disable RADIUS 要求を無視するためのデバイスの設定 91
例：RADIUS CoA 用の動的認可サービスの設定 91
RADIUS 認可変更に関する追加情報 92
RADIUS 認可変更の機能情報 93
AAA 認証のメッセージ バナー 95
機能情報の確認 95
AAA 認証のメッセージ バナーに関する情報 96
AAA 認証のログイン バナーおよび Failed-Login バナー 96
AAA 認証のメッセージ バナーの設定方法 96
AAA 認証のログイン バナーの設定 96
AAA 認証の Failed-Login バナーの設定 97
AAA 認証のメッセージ バナーの設定例 99
例：AAA 認証のログイン バナーおよび Failed-Login バナーの設定 99
AAA 認証のメッセージ バナーに関する追加情報 99
AAA 認証のメッセージ バナーの機能情報 100
サーバ グループ レベルでの AAA ドメイン ストリッピング 103
機能情報の確認 103
サーバ グループ レベルでの AAA ドメイン ストリッピングに関する情報 104
サーバ レベル グループでの AAA ドメイン ストリッピングの設定方法 105
サーバ グループ レベルでのドメイン ストリッピングの設定 105
サーバ グループ レベルでの AAA ドメイン ストリッピングの設定例 106
例：サーバ グループ レベルでの AAA ドメイン ストリッピング 106
その他の参考資料 106
サーバ グループ レベルでの AAA ドメイン ストリッピングの機能情報 108
AAA Double Authentication Secured by Absolute Timeout 109
機能情報の確認 109
AAA Double Authentication Secured by Absolute Timeout の前提条件 110
AAA Double Authentication Secured by Absolute Timeout の制約事項 110
AAA Double Authentication Secured by AbsoluteTimeout に関する情報 110
AAA 二重認証 110
AAA Double Authentication Secured by Absolute Timeout の適用方法 111

AAA Double Authentication Secured by Absolute Timeout の適用 111
AAA Double Authentication Secured by Absolute Timeout の設定例 111
例：RADIUS ユーザ プロファイル 111
例：TACACS ユーザ プロファイル 112
その他の参考資料 114
AAA Double Authentication Secured by AbsoluteTimeout の機能情報 115
AAA RADIUS レコードのスロットリング 117
機能情報の確認 117
AAA RADIUS レコードのスロットリングに関する情報 118
AAA RADIUS レコードのスロットリング機能の利点 118
スロットリング アクセス要求とアカウンティング レコード 118
AAA RADIUS レコードのスロットリングの設定方法 119
アカウンティングおよびアクセス要求パケットのグローバルなスロットリング 119
サーバグループごとのアカウンティングおよびアクセス要求パケットのスロットリング 120
AAA RADIUS レコードのスロットリングの設定例 122
アカウンティングおよびアクセス要求パケットのグローバルなスロットリングの例 122
サーバグループごとのアカウンティングおよびアクセス要求パケットのスロットリングの例 122
その他の参考資料 123
AAA RADIUS レコードのスロットリングの機能情報 124
RADIUS パケット オブ ディスコネクト 127
機能情報の確認 127
RADIUS パケット オブ ディスコネクトの前提条件 128
RADIUS パケット オブ ディスコネクトの制約事項 128
RADIUS パケット オブ ディスコネクトに関する情報 128
POD が必要な場合 128
POD パラメータ 128
RADIUS パケット オブ ディスコネクトの設定方法 129
RADIUS POD の設定 129
トラブルシューティングのヒント 132

RADIUS POD の設定の確認 132
その他の参考資料 132
RADIUS パケット オブ ディスコネクトの機能情報 134
用語集 135
AAA 認可および AAA 認証のキャッシュ 137
機能情報の確認 137
認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の前提条件 138
認可プロファイルおよび認証プロファイルのキャッシュ機能の実装について 138
認可プロファイルおよび認証プロファイルのキャッシュ機能によるネットワーク パフォーマンスの最適化 138
フェールオーバー メカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能 139
認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト 139
認可プロファイルおよび認証プロファイルのキャッシュ機能に関するガイドライン 140
認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための一般的な設定手順 140
認可プロファイルおよび認証プロファイルのキャッシュ機能の実装方法 141
キャッシュ プロファイル グループの作成とキャッシュ処理ルールの定義 141
キャッシュ プロファイル グループ情報を使用する RADIUS および TACACS サーバ グループの定義 144
キャッシュ情報の使用方法を指定するための認可および認証の方式リストの更新 146
認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための設定例 147
ネットワークを最適化するための認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例 147
フェールオーバー メカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例 148
RADIUS 認可変更に関する追加情報 150
認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の機能情報 151
認可の設定 153
機能情報の確認 153
AAA 認可の前提条件 154

認可の設定の概要 154
許可方式の指定リスト 154
AAA 認可方式 155
認可方式 156
方式リストとサーバ グループ 157
AAA 認可タイプ 157
承認タイプ 158
認可の属性値ペア 158
認可の設定方法 158
名前付き方式リストによる AAA 認可の設定 158
グローバル コンフィギュレーション コマンドの認可のディセーブル化 160
リバース Telnet の認可の設定 160
認可設定の例 162
TACACS 認可の例 162
RADIUS 認可の例 162
リバース Telnet 認可の例 163
その他の参考資料 165
認可の設定に関する機能情報 166
アカウンティングの設定 167
機能情報の確認 167
アカウンティングを設定するための前提条件 168
アカウンティングの設定の制約事項 168
アカウンティングの設定に関する情報 168
アカウンティングの方式指定リスト 168
方式リストとサーバ グループ 170
AAA アカウンティング方式 170
アカウンティング レコードの種類 171
アカウンティング方式 171
AAA アカウンティング タイプ 172
ネットワーク アカウンティング 173
EXEC アカウンティング 175
コマンド アカウンティング 176

接続アカウンティング 177

システム アカウンティング 179

リソース アカウンティング 179

AAA リソース失敗終了アカウンティング 179

開始 - 終了レコードの AAA リソース アカウンティング 181

AAA アカウンティングの強化 181

AAA ブロードキャスト アカウンティング 181

AAA セッション MIB 182

アカウンティング属性と値のペア 183

AAA アカウンティングの設定方法 183

名前付き方式リストによる AAA アカウンティングの設定 183

ヌル ユーザ名セッション時のアカウンティング レコード生成の抑制 185

中間アカウンティング レコードの生成 185

定期的アカウンティング レコードを有効化する代替手段の設定 186

中間サービス アカウンティング レコードの生成 187

失敗したログインまたはセッションに対するアカウンティング レコードの生成 188

EXEC-Stop レコードよりも前のアカウンティング NETWORK-Stop レコードの指定 189

スイッチオーバー上のシステム アカウンティング レコードの抑制 189

AAA リソース失敗終了アカウンティングの設定 190

開始 - 終了レコードの AAA リソース アカウンティングの設定 191

AAA ブロードキャスト アカウンティングの設定 191

DNIS による AAA ブロードキャスト アカウンティングの設定 192

AAA セッション MIB の設定 192

AAA サーバが到達不能な場合のルータとのセッションの確立 193

アカウンティングのモニタリング 193

アカウンティングのトラブルシューティング 194

AAA アカウンティングの設定例 194

方式指定リストの設定の例 194

AAA リソース アカウンティングの設定の例 196

AAA ブロードキャスト アカウンティングの設定の例 197

DNIS による AAA ブロードキャスト アカウンティングの設定の例 197

AAA セッション MIB の例 198
その他の参考資料 198
アカウンティングの設定に関する機能情報 199
AAA-SERVER-MIB Set Operation 203
機能情報の確認 203
AAA-SERVER-MIB Set Operation の前提条件 204
AAA-SERVER-MIB Set Operation の制約事項 204
AAA-SERVER-MIB Set Operation に関する情報 204
CISCO-AAA-SERVER-MIB 204
CISCO-AAA-SERVER-MIB Set Operation 204
Configure AAA-SERVER-MIB Set Operation の設定方法 205
RADIUS サーバの設定およびサーバの統計情報の確認 205
AAA-SERVER-MIB Set Operation の設定例 206
RADIUS サーバの設定およびサーバの統計情報の例 206
その他の参考資料 208
AAA-SERVER-MIB Set Operation の機能情報 209
Per VRF AAA 211
Per VRF AAA の前提条件 211
Per VRF AAA の制約事項 212
Per VRF AAA に関する情報 212
Per VRF AAA の機能 212
AAA アカウンティング レコード 213
新しいベンダー固有属性 213
VRF 認識 Framed-Route 219
Per VRF AAA の設定方法 219
Per VRF AAA の設定 219
AAA の設定 219
サーバ グループの設定 220
Per VRF AAA の認証、許可、アカウンティングの設定 221
Per VRF AAA の RADIUS 固有のコマンドの設定 223
Per VRF AAA のインターフェイス固有のコマンドの設定 224
ローカル カスタマー テンプレートを使用した Per VRF AAA の設定 226
AAA の設定 226

サーバ グループの設定 226

Per VRF AAA の認証、許可、アカウンティングの設定 226

ローカル カスタマー テンプレートを使用した Per VRF AAA の認可の設定 226

ローカル カスタマー テンプレートの設定 227

リモート カスタマー テンプレートを使用した Per VRF AAA の設定 229

AAA の設定 229

サーバ グループの設定 230

リモート カスタマー プロファイルを使用した Per VRF AAA の認証の設定 230

リモート カスタマー プロファイルを使用した Per VRF AAA の認可の設定 231

SP RADIUS サーバ上の RADIUS プロファイルの設定 232

VRF ルーティングの設定確認 232

Per VRF AAA 設定のトラブルシューティング 233

Per VRF AAA の設定例 233

Per VRF の設定の例 233

Per VRF AAA の例 233

ローカルで定義されたカスタマー テンプレートを使用した Per VRF AAA の例 234

リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA の例 234

カスタマー テンプレートの例 235

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してローカルで設定されたカスタマー テンプレートの例 235

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してリモートで設定されたカスタマー テンプレートの例 236

AAA アカウンティング終了レコードの例 236

AAA アカウンティング終了レコードと拒否されたコールの例 237

AAA アカウンティング終了レコードと成功したコールの例 239

その他の参考資料 241

Per VRF AAA の機能情報 243

用語集 246

AAA の IPv6 サポート 247

機能情報の確認 247

AAA の IPv6 サポートに関する情報 248

AAA over IPv6 248
IPv6 RADIUS 属性の AAA サポート 248
IPv6 の AAA 属性を使用するための前提条件 248
IPv6 環境での仮想アクセス用の RADIUS ユーザ単位属性 249
IPv6 用の AAA サポートの設定方法 252
DHCPv6 AAA オプションの設定 252
AAA の IPv6 サポートの設定例 254
例：DHCPv6 AAA オプションの設定 254
例：RADIUS の設定 254
その他の参考資料 254
RADIUS over IPv6 の機能情報 256
TACACS+ over IPv6 257
機能情報の確認 257
TACACS+ over IPv6 に関する情報 257
AAA over IPv6 258
IPv6 トランスポートを介した TACACS+ 258
TACACS+ over IPv6 の設定方法 258
IPv6 を介した TACACS+ サーバの設定 258
TACACS+ パケットでの送信元アドレスの指定 260
TACACS+ サーバ グループ オプションの設定 261
TACACS+ over IPv6 の設定例 262
例：IPv6 を介した TACACS+ サーバの設定 262
その他の参考資料 262
TACACS+ over IPv6 の機能情報 264
AAA Dead-Server Detection 267
機能情報の確認 267
AAA Dead-Server Detection の前提条件 268
AAA Dead-Server Detection の制約事項 268
AAA Dead-Server Detection について 268
RADIUS サーバをデッド状態と指定するための条件 268
AAA Dead-Server Detection の設定方法 269
AAA Dead-Server Detection の設定 269
トラブルシューティングのヒント 270

AAA Dead-Server Detection の確認 270
AAA Dead-Server Detection の設定例 271
AAA Dead-Server Detection の設定の例 271
debug aaa dead-criteria transactions コマンドの例 271
show aaa dead-criteria コマンドの例 272
その他の参考資料 272
AAA Dead-Server Detection の機能情報 274
Login Password Retry Lockout 275
MSCHAP バージョン 2 277
機能情報の確認 278
MSCHAP バージョン 2 の前提条件 278
MSCHAP バージョン 2 の制約事項 279
MSCHAP バージョン 2 の概要 279
MSCHAP バージョン 2 の設定方法 279
MSCHAP V2 の認証の設定 279
MSCHAP V2 設定の確認 281
クリプトベースのクライアントのパスワード エージングの設定 282
設定例 284
ローカル認証の設定の例 284
RADIUS 認証の設定の例 284
クリプト認証を使用したパスワード エージングの設定の例 284
その他の参考資料 285
MSCHAP バージョン 2 の機能情報 287
AAA ブロードキャスト アカウンティング - 必須応答サポート 289
機能情報の確認 289
AAA ブロードキャスト アカウンティング - 必須応答サポートの前提条件 290
AAA ブロードキャスト アカウンティング - 必須応答サポートの制約事項 290
AAA ブロードキャスト アカウンティング - 必須応答サポートに関する情報 290
AAA ブロードキャスト アカウンティング 290
ブロードキャスト アカウンティングと待機アカウンティングの同時使用 291
GGSN での AAA ブロードキャスト アカウンティングのサポート方法 292
GGSN でのブロードキャスト アカウンティングと待機アカウンティングの設定 292

AAA ブロードキャスト アカウンティング - 必須応答サポートの設定例 295
AAA ブロードキャスト アカウンティング - 必須応答サポートの例 295
その他の参考資料 296
AAA ブロードキャスト アカウンティング - 必須応答サポートの機能情報 297

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、コンバージドリリースの 1 つのバージョン - Cisco IOS XE 16 - に統合されました。この 1 つのリリースでスイッチングおよびルーティング ポートフォリオのアクセスおよびエッジ製品を幅広くカバーしています。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が、使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

認証の設定

認証は、選択したセキュリティ プロトコルに応じてログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および暗号化などのユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。

- 機能情報の確認，3 ページ
- 認証の設定の前提条件，4 ページ
- 認証の設定に関する制約事項，4 ページ
- 認証の設定に関する情報，4 ページ
- AAA 認証方式を設定する方法，13 ページ
- 非 AAA 認証方式，47 ページ
- 認証の例，58 ページ
- その他の参考資料，70 ページ
- 認証の設定に関する機能情報，72 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

認証の設定の前提条件

認証の Cisco IOS XE ソフトウェア実装は、AAA 認証方式と非認証方式に分かれています。シスコでは、可能であれば AAA セキュリティ サービスを試用して認証を実装することを推奨します。

認証の設定に関する制約事項

設定できる AAA 方式リストの数は 250 です。

認証の設定に関する情報

ここでは、認証方式の名前リストを定義し、このリストをさまざまなインターフェイスに適用して、AAA 認証を設定する方法について説明します。ここでは、RADIUS 認可変更（CoA）を使用した AAA 認証の処理方法についても説明します。

認証の名前付き方式リスト

AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。方式リストには、実行する認証の種類と、実行するシーケンスを定義します。方式リストは特定のインターフェイスに適用され、定義済みの認証方式のいずれかが実行されます。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストとは、ユーザ認証のために照会される認証方式を記載したシーケンシャル リストです。方式リストを使用すると、認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方式が失敗した場合に備えて認証のバックアップ システムを確保できます。Cisco IOS XE ソフトウェアは、ユーザを認証するため、リストに掲載されている最初の方式が使用されます。その方式で応答に失敗した場合、Cisco IOS XE ソフトウェアは、方式リストに掲載されている次の認証方式を選択します。このプロセスは、方式リストのいずれかの認証方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

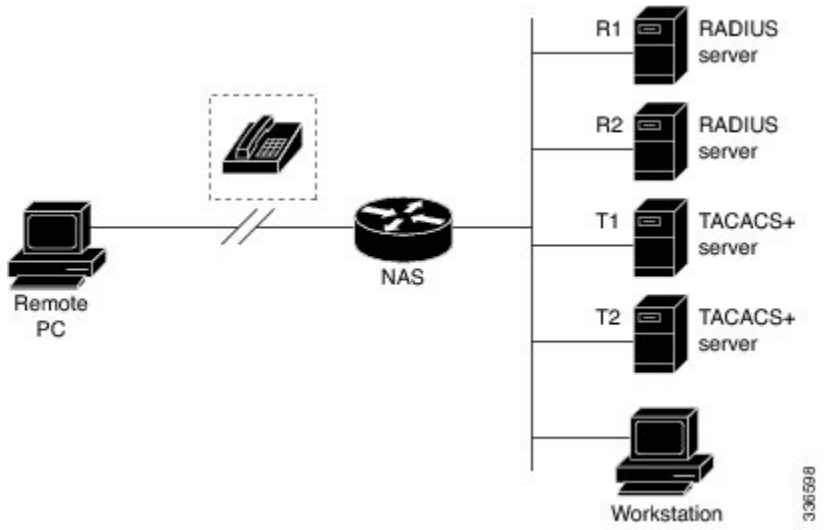
Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にだけ、リストの次の認証方式で認証が試行される、という点が重要です。このサイクルの任意の時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ アクセスの拒否応答が返される場合）、認証プロセスは停止し、その他の認証方式は試行されません。

（注） 設定できる AAA 方式リストの数は 250 です。

方式リストとサーバ グループ

サーバ グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバ ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

図 *1*：一般的な *AAA* ネットワーク設定



サーバ グループを使用して、設定したサーバ ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバ グループを使用すると、R1 および R2 を 1 つのサーバ グループとして定義し、T1 および T2 を別のサーバ グループとして定義できます。また、認証ログインの方式リストに R1 および T1 を指定し、PPP 認証の方式リストに R2 および T2 を指定することもできます。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（認証など）に設定されている場合、設定されている 2 番めのホストエントリは最初のホストエントリのフェールオーバーバックアップとして動作します。この例の場合、最初のホストエントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループの設定および着信番号識別サービス（DNIS）番号に基づくサーバ グループの設定の詳細については、「Configuring RADIUS」または「Configuring TACACS+」の章を参照してください。

方式リストの例

たとえば、システム管理者が、すべてのインターフェイスに同じ認証方式を使用して PPP 接続を認証する、というセキュリティ ソリューションを決定したとします。RADIUS グループでは、まず認証情報のために R1 に接続し、応答がない場合、R2 に接続します。R2 が応答しない場合、TACACS+ グループの T1 に接続し、T1 が応答しない場合、T2 に接続します。すべての指定したサーバが応答しなかった場合、認証はアクセス サーバ自体のローカルユーザ名データベースで行われます。このソリューションを実装するには、システム管理者が次のコマンドを入力してデフォルトの方式リストを作成します。

```
aaa authentication ppp default group radius group tacacs+ local
```

この例では、「default」が方式リストの名前です。この方式リストにプロトコルを含める場合、名前の後に、照会される順で指定します。デフォルトのリストは、すべてのインターフェイスに自動的に適用されます。

リモート ユーザがネットワークにダイヤルインしようとすると、ネットワーク アクセス サーバは、まず R1 に認証情報を照会します。ユーザが R1 から認証されると、R1 からネットワーク アクセス サーバに対して PASS 応答が発行され、ユーザはネットワークにアクセスできるようになります。R1 から FAIL 応答が返されると、ユーザはアクセスを拒否され、セッションは終了します。R1 が応答しない場合、ネットワーク アクセス サーバでは ERROR として処理され、認証情報について R2 に照会されます。このパターンは、ユーザが認証または拒否されるか、セッションが終了するまで、残りの指定した方式について続行されます。

FAIL 応答は ERROR とまったく異なる点に注意してください。FAIL とは、適用可能な認証データベースに含まれる、認証の成功に必要な基準をユーザが満たしていないことを示します。認証は FAIL 応答で終了します。ERROR とは、認証の照会に対してサーバが応答しなかったことを示します。そのため、認証は試行されません。ERROR が検出された場合にだけ、認証方式リストに定義されている次の認証方式が AAA によって選択されます。

たとえば、システム管理者が、1 つのインターフェイス、または一部のインターフェイスにだけ方式リストを適用するとします。この場合、システム管理者は名前付き方式リストを作成し、その名前付きリストを対象のインターフェイスに適用します。次に、システム管理者が、インターフェイス 3 にだけ適用する認証方式を実装する場合の例を示します。

```
aaa authentication ppp default group radius group tacacs+ local
aaa authentication ppp apple group radius group tacacs+ local none
 interface async 3
 ppp authentication chap apple
```

この例では、「apple」が方式リストの名前です。また、この方式リストに含まれるプロトコルは、名前の後に、実行する順で指定されています。方式リストを作成すると、該当するインターフェイスに適用されます。AAA および PPP 認証コマンド両方の方式リスト名（apple）は一致する必要があります。

次の例では、システム管理者がサーバ グループを使用し、PPP 認証の場合は R2 および T2 だけが有効であることを指定します。この場合、管理者は、メンバがそれぞれ R2（172.16.2.7）と T2

（172.16.2.77）であるサーバ グループを定義する必要があります。この例では、RADIUS サーバ グループ「rad2only」は **aaa group server** コマンドを使用して次のように定義されます。

```
aaa group server radius rad2only
 server 172.16.2.7
```

TACACS+ サーバ グループ「tac2only」は、**aaa group server** コマンドを使用して次のように定義されます。

```
aaa group server tacacs+ tac2only
 server 172.16.2.77
```

次に、管理者はサーバ グループを使用して PPP 認証を適用します。この例では、PPP 認証用のデフォルト方式リストは **group rad2only**、**group tac2only**、**local** の順序に従います。

```
aaa authentication ppp default group rad2only group tac2only local
```

RADIUS 認可変更について

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。シスコのソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS CoA 要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、許可、アカウンティング（AAA）またはポリシー サーバからの動的なセッション再設定が可能になります。

次のセッション単位の CoA 要求を使用します。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了
- セキュリティとパスワード
- アカウンティング

CoA 要求

CoA 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。モデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してデバイスでサポートされています。

次の表に、RADIUS 認可変更（CoA）機能でサポートされている IETF 属性を示します。

表 *1*：サポートされている *IETF* 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *2*：*Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）

値	説明
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求の応答コードは、デバイスへコマンドを発行するために使用されます。サポートされているコマンドを「CoA 要求コマンド」に示します。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

属性フィールドは、Cisco ベンダー固有属性（VSA）を送信するために使用します。

セッションの識別

特定のセッションに対する接続解除および CoA 要求の場合、デバイスは次の 1 つまたは複数の属性に基づいてセッションを検出します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id（シスコのベンダー固有属性（VSA））
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、デバイスは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

（注） CoA NAK メッセージは、キーの不一致があるすべての CoA 要求に送信されるわけではありません。メッセージは、クライアントの最初の 3 つの要求にのみ送信されます。その後、そのクライアントからのすべてのパケットがドロップされます。キーの不一致が見つかると、CoA NAK メッセージで送信される応答オーセンティケータはダミーのキー値から計算されます。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なります。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。

CoA 要求コマンド

デバイスでサポートされているコマンドを次の表に示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *3*：デバイスでサポートされる *CoA* 要求コマンド

コマンド	シスコの VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	VSA を必要としない標準の接続解除要求です

セッション再認証

セッション認証を開始するために、認証、許可、アカウンティング（AAA）サーバは、Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は、Cisco:Avpair=“subscriber:command=reauthenticate” の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1*x* によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN（EAPoL）-RequestId メッセージをサーバに送信することで応答します。
- セッションが現在 MAC 認証バイパス（MAB）によって認証されている場合、デバイスはアクセス要求をサーバに送信し、最初に成功した認証で使用したのと同じ ID 属性を渡します。
- デバイスがコマンドを受信した際にセッション認証が実行中である場合は、デバイスはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションの終了

CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。CoA 接続解除要求終了によって、指定したホストのオーセンティケータ ステートマシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

CoA 要求の disable host port

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。デバイスは、セッションを検出すると、ホスティング ポートを無効にし、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブ デバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

RADIUS サーバの CoA disable port コマンドを無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

CoA 要求の bounce port

RADIUS サーバの CoA bounce port が RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「セッション ID」に示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。このセッションがある場合は、デバイスはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

RADIUS サーバの CoA bounce port を無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

ドメイン ストリッピング

radius-server domain-stripping コマンドを使用して、グローバル レベルで受信したユーザ名からドメイン名を削除できます。**radius-server domain-stripping** コマンドを設定すると、「user@example.com」を含むすべての AAA 要求のユーザ名が「user」に再フォーマットされてリモート RADIUS サーバに送信されます。ドメイン名は要求から削除されます。

（注） ドメイン ストリッピングは TACACS 設定では行われません。

AAA ブロードキャスト アカウンティング機能を有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、プライベートおよびパブリック AAA サーバにアカウント情報を送信できます。この機能では、音声アプリケーションによる課金情報も提供されます。

ドメイン ストリッピング機能を使用すると、ドメイン ストリッピングをサーバ グループ レベルで設定できます。

サーバ単位のグループ コンフィギュレーションはグローバル コンフィギュレーションを上書きします。ドメイン ストリッピングが、グローバルではイネーブルではないがサーバ グループでイネーブルになっている場合、そのサーバ グループに対してのみイネーブルになります。また、Virtual Routing and Forwarding（VRF）固有のドメイン ストリッピングがグローバルで設定されていて、別の VRF のドメイン ストリッピングがサーバ グループで設定されている場合、ドメイン ストリッピングは両方の VRF でイネーブルになります。VRF の設定は、サーバグループ コンフィギュレーション モードから取得されます。サーバグループ コンフィギュレーションがグローバル コンフィギュレーション モードでディセーブルになっているが、サーバ グループ コンフィギュレーション モードで使用可能である場合、サーバグループ コンフィギュレーション モードでのすべての設定が適用可能です。

ドメイン ストリッピングおよびブロードキャスト アカウンティングを設定した後で、設定ごとに別個のアカウンティング レコードを作成できます。

AAA 認証方式を設定する方法

（注） **aaanew-model** コマンドを使用して AAA をグローバルにイネーブルにするまで、AAA 機能は使用できません。

この章のコマンドを使用した認証の設定例については、「認証の例」を参照してください。

AAA を使用したログイン認証の設定

AAAセキュリティサービスにより、さまざまなログイン認証方式を容易に実行できるようになります。**aaaauthenticationlogin** コマンドを使用すると、サポートされているログイン認証方式のいずれを使用するかに関係なく、AAA認証がイネーブルになります。**aaaauthenticationlogin** コマンドを使用すると、ログイン時に試行する認証方式リストを 1 つ以上作成できます。これらのリストを適用するには、**loginauthentication** ライン コンフィギュレーション コマンドを使用します。

AAA を使用してログイン認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaanew-model**
2. Router(config)# **aaaauthenticationlogin** {**default** | *list-name*} *method1*[*method2...*]
3. Router(config)# **line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**]
4. Router(config-line)# **loginauthentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaanew-model**	AAA をグローバルにイネーブルにします。
ステップ 2	Router(config)# **aaaauthenticationlogin** {**default** | *list-name*} *method1*[*method2...*]	ローカルな認証リストを作成します。
ステップ 3	Router(config)# **line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**]	認証リストを適用する回線について、ライン コンフィギュレーション モードを開始します。
ステップ 4	Router(config-line)# **loginauthentication** 例： {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。

次の作業

list-name は、作成するリストを指定するときに使用される名前で、文字列を使用できます。method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）TACACS+ サーバでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+ none
```

（注） **none** キーワードを指定すると、すべてのユーザがログイン認証に成功するため、認証のバックアップ方式としてだけ使用してください。

loginauthentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザ認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

次の表に、サポートされるログイン認証方式を示します。

表 *4* : *AAA* 認証ログイン方式

キーワード	説明
enable	認証にイネーブル パスワードを使用します。
krb5	Kerberos 5 を認証に使用します。
krb5-telnet	ルータへの接続に Telnet を使用する場合、Kerberos 5 Telnet 認証プロトコルを使用します。このキーワードを選択する場合、方式リストの最初の方式としてこのキーワードを指定する必要があります。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。

キーワード	説明
none	認証を使用しません。
groupradius	認証にすべての RADIUS サーバのリストを使用します。
grouptacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group*group-name*	認証に **aaagroupserverradius** コマンドまたは **aaagroupservertacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

（注） **login** コマンドによって変更されるのはユーザ名および特権レベルだけであり、シェルは実行されません。したがって、autocommand は実行されません。この状況で autocommand を実行するには、Telnet セッションをルータに復帰（ループバック）させる必要があります。この方法で autocommand 機能を実装する場合は、ルータがセキュアな Telnet セッションを使用するように設定されていることを確認してください。

イネーブル パスワードによるログイン認証

ログイン認証方式としてイネーブル パスワードを指定するには、**enable** *method* キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式としてイネーブル パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default enable
```

ログイン認証方式としてイネーブル パスワードを使用するには、イネーブル パスワードを定義しておく必要があります。イネーブル パスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

Kerberos によるログイン認証

Kerberos による認証は、他のほとんどの認証方式とは異なり、ユーザのパスワードはリモート アクセス サーバに送信されません。ネットワークにログインするリモートユーザは、ユーザ名の指定を求められます。ユーザのエントリがキー発行局（KDC）に存在する場合は、そのユーザのパスワードを含む暗号化されたチケット認可チケット（TGT）が作成され、ルータに送信されます。次に、ユーザにパスワードの入力が求められ、ルータではそのパスワードを含む TGT の復号化が

試行されます。復号化に成功すると、ユーザは認証され、ルータ上にあるユーザのクレデンシャル キャッシュに TGT が保存されます。

krb5 は KINIT プログラムを使用しませんが、ルータに対して認証するために、ユーザが KINIT プログラムを実行して TGT を取得する必要はありません。これは、Cisco IOS XE の Kerberos 実装のログイン手順に KINIT が統合されているためです。

ログイン認証方式として Kerberos を指定するには、**krb5***method* キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として Kerberos を指定するには、次のコマンドを入力します。

```
aaa authentication login default krb5
```

ログイン認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバとの通信をイネーブルにしておく必要があります。Kerberos サーバとの通信を確立する方法の詳細については、「Configuring Kerberos」の章を参照してください。

ライン パスワードによるログイン認証

ログイン認証方式としてライン パスワードを指定するには、**line***method* キーワードを指定して **aaaauthenticationlogin** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式としてライン パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default line
```

ログイン認証方式としてラインパスワードを使用するには、ラインパスワードを定義しておく必要があります。ラインパスワードの定義の詳細については、「ラインパスワード保護の設定」を参照してください。

ローカル パスワードによるログイン認証

Cisco ルータまたはアクセス サーバが認証にローカル ユーザ名データベースを使用するように指定するには、**local***method* キーワードを指定して **aaaauthenticationlogin** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication login default local
```

ローカル ユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS によるログイン認証

ログイン認証方式として RADIUS を指定するには、**group radius** *method* を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

ログイン認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。

アクセス要求での RADIUS 属性 8 の設定

aaaauthenticationlogin コマンドを使用して RADIUS を指定し、NAS から IP アドレスを要求するようにログインホストを設定すると、グローバルコンフィギュレーションモードで **radius-server attribute 8 include-in-access-req** コマンドを使用して、access-request パケットで属性 8（Framed-IP-Address）を送信できます。このコマンドによって、ユーザ認証の前に、NAS から RADIUS サーバに対してユーザ IP アドレスのヒントを提供できます。属性 8 の詳細については、巻末の付録「RADIUS 属性」を参照してください。

group TACACS によるログイン認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** *method* を指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+
```

ログイン認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

group group-name によるログイン認証

ログイン認証方式として使用する RADIUS または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication login** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group loginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *loginrad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group loginrad** を指定するには、次のコマンドを入力します。

```
aaa authentication login default group loginrad
```

ログイン認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

AAA を使用した PPP 認証の設定

多くのユーザは、async または ISDN を介したダイヤルアップでネットワーク アクセス サーバにアクセスします。async または ISDN を介したダイヤルアップは、CLI を完全にバイパスします。その代わり、接続が確立するとすぐにネットワーク プロトコル（PPP や ARA など）が開始されます。

AAA セキュリティ サービスにより、PPP を実行するシリアル インターフェイスに使用できるさまざまな認証方式の実行が容易になります。**aaaauthenticationppp** コマンドを使用すると、サポートされている PPP 認証方式のいずれを使用するかに関係なく、AAA 認証がイネーブルになります。

PPP を使用してシリアル回線に AAA 認証方式を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaanew-model**
2. Router(config)# **aaaauthenticationppp**{**default** | *list-name*} *method1*[*method2...*]
3. Router(config)# **interface***interface-typeinterface-number*
4. Router(config-if)# **pppauthentication** {*protocol1* [*protocol2...*]}[**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**][**optional**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaanew-model**	AAA をグローバルにイネーブルにします。
ステップ 2	Router(config)# **aaaauthenticationppp**{**default** | *list-name*} *method1*[*method2...*]	ローカルな認証リストを作成します。
ステップ 3	Router(config)# **interface***interface-typeinterface-number*	認証リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config-if)# **pppauthentication** {*protocol1* [*protocol2...*]}[**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**][**optional**]	1 つの回線または複数回線に認証リストを適用します。このコマンドの *protocol1* と *protocol2* は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず *protocol1* に指定された最初の認証方式を使用して試行されます。認証に *protocol1* を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。

次の作業

aaaauthenticationppp コマンドを使用して、PPP を介して認証を試行するときに使用する認証方式のリストを 1 つまたは複数作成します。これらのリストは、**pppauthentication** ライン コンフィギュレーション コマンドによって適用されます。

pppauthentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。

たとえば、ユーザ認証のデフォルト方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）TACACS+ サーバでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+ none
```

（注） **none** を指定するとすべてのユーザが認証に成功してログインできるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされるログイン認証方式を示します。

表 *5*：*AAA* 認証 *PPP* 方式

キーワード	説明
if-needed	ユーザが TTY 回線で認証済みの場合、認証しません。
krb5	認証に Kerberos 5 を使用します（PAP 認証にだけ使用できます）。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。

キーワード	説明
groupradius	認証にすべての RADIUS サーバのリストを使用します。
grouptacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group*group-name*	認証に **aaagroupserverradius** コマンドまたは **aaagroupservertacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

Kerberos による PPP 認証

PPP を実行するインターフェイスで使用する認証方式として Kerberos を指定するには、**krb5***method* キーワードを指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にユーザ認証方式として Kerberos を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default krb5
```

PPP 認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバとの通信をイネーブルにしておく必要があります。Kerberos サーバとの通信を確立する方法の詳細については、「Configuring Kerberos」の章を参照してください。

（注） Kerberos ログイン認証は、PPP PAP 認証とだけ連携します。

ローカル パスワードによる PPP 認証

Cisco ルータまたはアクセス サーバが認証にローカル ユーザ名データベースを使用するように指定するには、*method* キーワード **local** を指定して **aaaauthenticationppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、PPP を実行する回線に使用するユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

ローカル ユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS による PPP 認証

ログイン認証方式として RADIUS を指定するには、**group radius** *method* を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group radius
```

PPP 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。

アクセス要求での RADIUS 属性 44 の設定

groupradius*method* を指定して **aaaauthenticationppp** コマンドを使用してから、ログイン認証方式として RADIUS を指定すると、グローバル コンフィギュレーション モードで **radius-serverattribute44include-in-access-req** コマンドを使用して access-request パケットで属性 44（Acct-Session-ID）を送信するようにデバイスを設定できます。このコマンドによって、RADIUS デーモンはコールを開始から終了まで追跡できます。

group TACACS による PPP 認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** *method* を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+
```

PPP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

group group-name による PPP 認証

ログイン認証方式として使用する RADIUS または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication ppp** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group ppprad** のメンバを最初に定義します。

```
aaa group server radius ppprad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *ppprad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group ppprad** を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group ppprad
```

PPP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

PPP 要求に対する AAA スケーラビリティの設定

ネットワーク アクセス サーバ（NAS）の PPP マネージャによって割り当てられた複数のバックグラウンド プロセスを設定およびモニタして、AAA 認証要求と認可要求に対応できます。AAA スケーラビリティ機能によって、PPP に対する AAA 要求を処理するために使用される複数のプロセスを設定できるようになります。つまり、同時に認証または認可できるユーザ数が増えます。

PPP に対する AAA 要求を処理するために、特定の数のバックグラウンド プロセスを割り当てるには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **aaa processes** *number*	PPP に対する AAA 認証要求および認可要求を処理するために、特定の数のバックグラウンド プロセスを割り当てます。

引数 *number* には、PPP に対する AAA 認証要求と認可要求を処理するために確保するバックグラウンド プロセス数を定義します。また、1 ～ 2147483647 の任意の値を設定できます。PPP マネージャが PPP に対する要求を処理する方法のため、この引数には、同時に認証できる新規ユーザの数も定義します。この引数は、いつでも増減できます。

（注） 追加バックグラウンドプロセスの割り当ては、コストが高くなる可能性があります。PPP に対する AAA 要求を処理できるバックグラウンド プロセスの最小数を設定してください。

AAA を使用した ARAP 認証の設定

aaaauthenticationarap コマンドを使用して、AppleTalk Remote Access Protocol（ARAP）ユーザがデバイスにログインを試行するときに使用する認証方式のリストを 1 つまたは複数作成できます。これらのリストは、**arapauthentication** ライン コンフィギュレーション コマンドで使用されます。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Device(config)# **aaanew-model**
2. Device(config)# **aaaauthenticationarap**
3. Device(config)# **line***number*
4. Device(config-line)# **autoselectarap**
5. Device(config-line)# **autoselectduring-login**
6. Device(config-line)# **arapauthentication***list-name*
7. Device(config-line)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **aaanew-model**	AAA をグローバルにイネーブルにします。
ステップ 2	Device(config)# **aaaauthenticationarap** 例： ARAP ユーザに対する認証をイネーブルにします。	
ステップ 3	Device(config)# **line***number*	（任意）ライン コンフィギュレーション モードに変更します。
ステップ 4	Device(config-line)# **autoselectarap**	（任意）ARAP の自動選択をイネーブルにします。
ステップ 5	Device(config-line)# **autoselectduring-login**	（任意）ユーザ ログイン時に ARAP セッションを自動的に開始します。
ステップ 6	Device(config-line)# **arapauthentication***list-name*	（任意：**default** が **aaaauthenticationarap** コマンドに使用されている場合は不要）回線上の ARAP に対する TACACS+ 認証をイネーブルにします。
ステップ 7	Device(config-line)# **end**	特権 EXEC モードに戻ります。

次の作業

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。*method* 引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

arapauthentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

（注） **none** を指定するとすべてのユーザのログインが認証されるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされるログイン認証方式を示します。

表 *6*：*AAA* 認証 *ARAP* 方式

キーワード	説明
auth-guest	ユーザが EXEC モードにログイン済みの場合にだけ、ゲスト ログインを許可します。
guest	ゲスト ログインを許可します。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
groupradius	認証にすべての RADIUS サーバのリストを使用します。
grouptacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group*group-name*	認証に **aaagroupserverradius** コマンドまたは **aaagroupservertacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

たとえば、ARAP とともに使用するデフォルトの AAA 認証方式リストを作成するには、次のコマンドを使用します。

```
aaa authentication arap default if-needed none
```

ARAP に同じ認証方式リストを作成し、リストに *MIS-access* と名前を付けるには、次のコマンドを入力します。

```
aaa authentication arap MIS-access if-needed none
```

ここでは、次の内容について説明します。

認可済みゲスト ログインを許可する ARAP 認証

ユーザが EXEC にログイン済みの場合にだけ、ゲスト ログインを許可するには、**auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式は ARAP 認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式として、すべての認可済みゲスト ログイン（つまり、EXEC にログイン済みのユーザによるログイン）を許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default auth-guest group radius
```

（注） AAA を初期化すると、デフォルトで ARAP によるゲスト ログインはディセーブルになります。ゲスト ログインを許可するには、**guest** キーワードまたは **auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用する必要があります。

ゲスト ログインを許可する ARAP 認証

ゲスト ログインを許可するには、**guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式は ARAP 認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式としてすべてのゲスト ログインを許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default guest group radius
```

ライン パスワードによる ARAP 認証

認証方式としてライン パスワードを指定するには、*method* キーワード **line** を指定して **aaaauthenticationarap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、ARAP ユーザ認証方式としてライン パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication arap default line
```

ARAP 認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ラインパスワードの定義の詳細については、この章の「ラインパスワード保護の設定」を参照してください。

ローカル パスワードによる ARAP 認証

Cisco ルータまたはアクセス サーバが認証にローカル ユーザ名データベースを使用するように指定するには、*method* キーワード **local** を指定して **aaaauthenticationarap** コマンドを使用します。

たとえば、他の方式リストが定義されていない場合に、ARAPユーザ認証方式としてローカルユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication arap default local
```

ローカル ユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS による ARAP 認証

ARAP 認証方式として RADIUS を指定するには、**group radius** *method* を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group radius
```

ARAP 認証方式として RADIUS を使用する前に、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。

group TACACS による ARAP 認証

ARAP 認証方式として TACACS+ を指定するには、**group tacacs+** *method* を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group tacacs+
```

ARAP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

group group-name による ARAP 認証

ARAP 認証方式として使用する RADIUS または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication arap** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group araprad** のメンバを最初に定義します。

```
aaa group server radius araprad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *araprad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group araprad** を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group araprad
```

ARAP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

AAA を使用した NASI 認証の設定

aaaauthenticationnasi コマンドを使用して、NetWare Asynchronous Services Interface（NASI）ユーザがデバイスにログインを試行するときに使用する認証方式のリストを 1 つまたは複数作成できます。これらのリストは、**nasiauthenticationline** ライン コンフィギュレーション コマンドで使用されます。

AAA を使用して NASI 認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Device(config)# **aaanew-model**
2. Device(config)# **aaaauthenticationnasi**
3. Device(config)# **line***number*
4. Device(config-line)# **nasiauthentication***list-name*
5. Device(config-line)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **aaanew-model**	AAA をグローバルにイネーブルにします。
ステップ 2	Device(config)# **aaaauthenticationnasi** 例：	NASI ユーザに対する認証をイネーブルにします。
ステップ 3	Device(config)# **line***number*	（任意：**default** が **aaaauthenticationnasi** コマンドに使用されている場合は不要）ライン コンフィギュレーション モードを開始します。
ステップ 4	Device(config-line)# **nasiauthentication***list-name*	（任意：**default** が **aaaauthenticationnasi** コマンドに使用されている場合は不要）回線上の NASI に対する認証をイネーブルにします。
ステップ 5	Device(config-line)# **end**	特権 EXEC モードに戻ります。

次の作業

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。*method* 引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

aaaauthenticationnasi コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

（注） **none** を指定するとすべてのユーザのログインが認証されるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされる NASI 認証方式を示します。

表 *7* : ***AAA*** 認証 ***NASI*** 方式

キーワード	説明
enable	認証にイネーブル パスワードを使用します。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。
groupradius	認証にすべての RADIUS サーバのリストを使用します。
grouptacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group*group-name*	認証に **aaagroupserverradius** コマンドまたは **aaagroupservertacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

イネーブル パスワードによる NASI 認証

認証方式としてイネーブル パスワードを指定するには、キーワード **enable** を指定して **aaaauthenticationnasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式としてイネーブル パスワードを指定するには、次のコマンドを使用します。

```
aaa authentication nasi default enable
```

認証方式としてイネーブルパスワードを使用するには、イネーブルパスワードを定義しておく必要があります。イネーブル パスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

ライン パスワードによる NASI 認証

認証方式としてライン パスワードを指定するには、*method* キーワード **line** を指定して **aaaauthenticationnasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASIユーザ認証方式としてラインパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default line
```

NASI 認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ラインパスワードの定義の詳細については、「ラインパスワード保護の設定」を参照してください。

ローカル パスワードによる NASI 認証

Cisco ルータまたはアクセス サーバが認証情報にローカル ユーザ名データベースを使用するように指定するには、*method* キーワード **local** を指定して **aaaauthenticationnasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASIユーザ認証方式としてローカルユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default local
```

ローカル ユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS による NASI 認証

NASI 認証方式として RADIUS を指定するには、**group radius** *method* を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASIユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group radius
```

NASI 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。

group TACACS による NASI 認証

NASI 認証方式として TACACS+ を指定するには、**group tacacs+** *method* キーワードを指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group tacacs+
```

認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

group group-name による NASI 認証

NASI 認証方式として使用する RADIUS または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication nasi** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group nasirad** のメンバを最初に定義します。

```
aaa group server radius nasirad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *nasirad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group nasirad** を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group nasirad
```

NASI 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」の章を参照してください。

ログイン入力にかける時間の指定

timeout login response コマンドを使用すると、ログイン入力（ユーザ名やパスワードなど）がタイムアウトするまでの待機時間を指定できます。デフォルトのログイン値は 30 秒です。**timeout login response** コマンドを使用して、1 ～ 300 秒のタイムアウト値を指定します。30 秒というデフォルトのログイン タイムアウト値を変更するには、ライン コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-line)#` **timeout login response** *seconds*	タイムアウトまでログイン情報を待機する時間を指定します。

特権レベルでのパスワード保護のイネーブル化

ユーザが特権 EXEC コマンド レベルにアクセスできるかどうかを判断するときに使用する一連の認証方式を作成するには、**aaaauthenticationenabledefault** コマンドを使用します。最大 4 つの認証方式を指定できます。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **aaa authentication enable default** *method1* [*method2...*]	特権 EXEC レベルを要求するユーザに対して、ユーザ ID とパスワードのチェックをイネーブルにします。 （注） ルータから RADIUS サーバに送信されたすべての **aaaauthenticationenabledefault** 要求には、ユーザ名「$enab15$」が含まれます。TACACS+ サーバに送信された要求にはログイン認証用に入力されたユーザ名が含まれます。

メソッド引数は、認証アルゴリズムが試行した方式の実際のリストを入力された順に参照します。次の表は、サポートされているイネーブル認証方式を示します。

表 *8*：*AAA* 認証イネーブル デフォルト方式

キーワード	説明
enable	認証にイネーブル パスワードを使用します。
line	認証にライン パスワードを使用します。
none	認証を使用しません。
groupradius	認証にすべての RADIUS ホストのリストを使用します。 （注） RADIUS 方式は、ユーザ名別では機能しません。
grouptacacs+	認証にすべての TACACS+ ホストのリストを使用します。

キーワード	説明
group*group-name*	認証に **aaagroupserverradius** コマンドまたは **aaagroupservertacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

パスワード プロンプトに表示するテキストの変更

Cisco IOS XE ソフトウェアからユーザに対してパスワードの入力を求めるときに表示されるデフォルト テキストを変更するには、**aaa authentication password-prompt** コマンドを使用します。このコマンドによって、イネーブル パスワードと、リモート セキュリティ サーバから提供されていないログイン パスワードのパスワード プロンプトが変更されます。このコマンドの **no** 形式を使用すると、パスワード プロンプトが次のデフォルト値に戻ります。

```
Password:
```

aaa authentication password-prompt コマンドでは、リモートの TACACS+ サーバまたは RADIUS サーバから提供されるダイアログは変更されません。

aaa authentication password-prompt コマンドは、RADIUS をログイン方式として使用するときに機能します。RADIUS サーバに到達不能の場合でも、コマンドで定義されたパスワード プロンプトが表示されます。aaa authentication password-prompt コマンドは、TACACS+ と併用できません。TACACS+ は、NAS に対して、ユーザに表示するパスワードプロンプトを提供します。TACACS+ サーバが到達可能な場合、NAS はそのサーバからパスワード プロンプトを受け取り、aaa authentication password-prompt コマンドで定義したプロンプトではなく、受け取ったプロンプトを使用します。TACACS+ サーバが到達不能の場合、aaa authentication password-prompt コマンドで定義したパスワード プロンプトが使用される可能性があります。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **aaa authentication password-prompt** *text-string*	ユーザにパスワードの入力を求めるときに表示するデフォルト テキストを変更します。

ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにする

次の設定手順では、ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにする方法について説明します。この機能により、RADIUS サーバとの不要なやりとりを回避でき、RADIUS ログの量を少なくすることができます。

（注） **aaa authentication suppress null-username** コマンドを開始できるのは、Cisco IOS XE Release 2.4 です。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaauthenticationsuppressnull-username**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router(config)# configure terminal`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaaauthenticationsuppressnull-username** 例： `Router(config)# aaa authentication suppress null-username`	ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにします。

AAA 認証のメッセージ バナーの設定

AAA は、設定可能でパーソナライズされたログインおよび failed-login バナーの使用をサポートします。ユーザが AAA を使用して認証を受けるシステムにログインする場合、および何らかの理由で認証が失敗した場合に表示されるメッセージ バナーを設定できます。

ログイン バナーの設定

ユーザがログインするときに表示されるメッセージを設定する（デフォルトのログイン メッセージを置き換える）には、次のタスクを実行します。

はじめる前に

ログイン バナーを作成するには、デリミタを設定する必要があります。設定することで、続くテキスト文字列をバナーとして表示する必要があることがシステムに通知されます。次に、テキスト文字列自体を設定する必要があります。デリミタは、バナーの末尾を示すために、テキスト ストリングの末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナー用のテキスト文字列には使用できません。

手順の概要

1. **aaanew-model** Device(config)# **aaanew-model**
2. Device(config)# **aaaauthenticationbanner***delimiterstringdelimiter*
3. Device(config)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**aaanew-model** Device(config)# **aaanew-model**	AAA をイネーブルにします。
ステップ 2	Device(config)# **aaaauthenticationbanner***delimiterstringdelimiter*	パーソナライズされたログイン バナーを作成します。
ステップ 3	Device(config)# **end**	特権 EXEC モードに戻ります。

次の作業

ログイン バナーの設定後、まだ実行していない場合は、AAA を使用した認証の基本設定を完了する必要があります。さまざまな、使用可能な AAA 認証の詳細については、『認証、許可、アカウンティング コンフィギュレーション ガイド』の「認証の設定」を参照してください。

Failed-Login バナーの設定

ユーザ ログインが失敗したときに表示されるメッセージを設定する（デフォルトの failed-login メッセージを置き換える）には、次のタスクを実行します。

はじめる前に

failed-login バナーを作成するには、デリミタを設定する必要があります。設定することで、続くテキスト文字列をバナーとして表示する必要があることがシステムに通知されます。次に、テキスト文字列自体を設定する必要があります。デリミタは、failed-loginバナーの末尾を示すために、テキスト ストリングの末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト ストリングには使用できません。

手順の概要

1. Device(config)# **aaanew-model**
2. Device(config)# **aaaauthenticationfail-message***delimiterstringdelimiter*
3. Device(config)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **aaanew-model**	AAA をイネーブルにします。
ステップ 2	Device(config)# **aaaauthenticationfail-message***delimiterstringdelimiter*	ユーザ ログインが失敗したときに表示されるメッセージを作成します。
ステップ 3	Device(config)# **end**	特権 EXEC モードに戻ります。

次の作業

failed-login バナーの設定後、まだ実行していない場合は、AAA を使用した認証の基本設定を完了する必要があります。さまざまな、使用可能なAAA認証の詳細については、『認証、許可、アカウンティング コンフィギュレーション ガイド』の「認証の設定」を参照してください。

AAA パケット オブ ディスコネクトの設定

特定のセッション属性が指定された場合、パケットオブディスコネクト（POD）によってネットワーク アクセス サーバ（NAS）の接続が終了されます。UNIX ワークステーション上にある POD クライアントでは、AAA から取得したセッション情報を使用して、ネットワーク アクセス サーバで実行されている POD サーバに接続解除パケットを送信します。NAS では、1 つまたは複数の一致するキー属性を含む任意の着信ユーザ セッションを終了します。必要なフィールドがない場合、または完全一致が見つからない場合、要求は拒否されます。

POD を設定するには、グローバル コンフィギュレーション モードで次のタスクを実行します。

手順の概要

1. Router(config)# **aaa accounting network default**
2. Router(config)# **aaa accounting delay-start**
3. Router(config)# **aaa pod server server-key**string
4. Router(config)# **radius-server host** *IP address*non-standard

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa accounting network default** 例： **start-stop radius**	AAA アカウンティング レコードをイネーブルにします。
ステップ 2	Router(config)# **aaa accounting delay-start**	（任意）POD パケットで使用できるように、Framed-IP-Address が割り当てられるまで、開始アカウンティング レコードの生成を遅延します。
ステップ 3	Router(config)# **aaa pod server server-key**string	POD の受信イネーブルにします。
ステップ 4	Router(config)# **radius-server host** *IP address*non-standard	RADIUS のベンダー固有バージョンを使用する RADIUS ホストを宣言します。

二重認証のイネーブル化

シスコのリリースによっては、PPP セッションの認証には、PAP または CHAP のどちらか 1 つの認証方法しか使用できないことがあります。二重認証方式の場合、ネットワーク アクセス権を得るには、リモート ユーザが（CHAP または PAP 認証後に）認証の第 2 段階に合格する必要があります。

この第2段階（「二重」）の認証には、ユーザがパスワードを知っている必要がありますが、ユーザのリモート ホストにパスワードは保存されません。そのため、第 2 段階の認証は、ホストではなくユーザに固有です。その結果、リモート ホストから情報が盗まれた場合でも有効な、追加のセキュリティ レベルが実現します。さらに、ユーザ別にネットワーク特権をカスタマイズできるため、柔軟性も高くなります。

第 2 段階の認証には、CHAP ではサポートされないトークン カードなど、ワンタイム パスワードを使用できます。ワンタイムパスワードを使用している場合、ユーザパスワードが盗まれても盗用者の役に立ちません。

二重認証の機能

二重認証を使用する場合、2 つの認証/認可段階があります。この 2 つの段階は、リモート ユーザがダイヤルインした後、および PPP セッションが開始された後に発生します。

第 1 段階では、ユーザがリモート ホスト名を使用してログインして CHAP（または PAP）がリモート ホストを認証し、次に PPP が AAA とネゴシエートしてリモート ホストを認可します。このプロセスで、リモートホストに関連付けられたネットワーク アクセス特権は、そのユーザに関連付けられます。

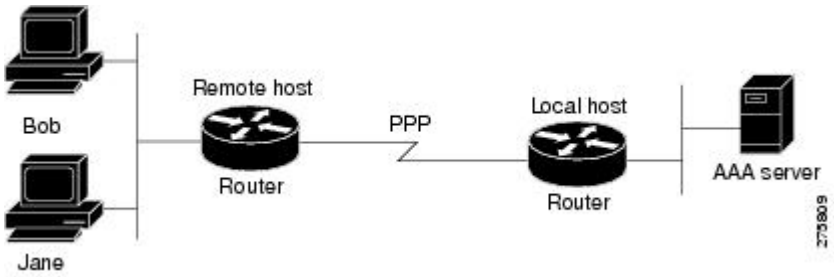
（注） ローカル ホストに対して Telnet 接続だけを許可するように、この第 1 段階ではネットワーク管理者が認可を制限することを推奨します。

第 2 段階では、リモート ユーザが、認証を受けるネットワーク アクセス サーバに対して Telnet を送信する必要があります。リモートユーザがログインする場合、AAA ログイン認証を使用してユーザを認証する必要があります。次に、AAA を使用して最認可を受けるために、**access-profile** コマンドを入力する必要があります。この認可が完了すると、ユーザは二重に認証され、ユーザ別のネットワーク特権に従ってネットワークにアクセスできるようになります。

システム管理者は、セキュリティ サーバで適切なパラメータを設定することで、各認証段階の後にリモート ユーザが保持するネットワーク特権を決定します。二重認証を使用するには、**access-profile** コマンドを発行してアクティブ化する必要があります。

注意 複数のホストがネットワーク アクセス サーバに対して PPP 接続を共有する場合、二重認証によって望ましくない状況が発生することがあります（次の図を参照）。まず、ユーザ Bob が PPP セッションを開始し、ネットワーク アクセス サーバで二重認証をアクティブにした場合（次の図を参照）、Bob の PPP セッションが期限切れになるまで、他のすべてのユーザは Bob と同じネットワーク特権を持つことになります。この問題が発生するのは、PPP セッション時に Bob の認可プロファイルがネットワーク アクセス サーバのインターフェイスに適用され、他のユーザからの PPP トラフィックに Bob が確立した PPP セッションが使用されるためです。第 2 に、Bob が PPP セッションを開始して二重認証をアクティブにし、（Bob の PPP セッションが期限切れになる前に）別のユーザ Jane が **access-profile** コマンドを実行する場合（または、Jane がネットワーク アクセス サーバに Telnet を送信し、**autocommandaccess-profile** が実行された場合）、再認可が発生し、Jane の認可プロファイルがインターフェイスに適用され、Bob のプロファイルは置換されます。その結果、Bob の PPP トラフィックの不通や中止が発生することや、Bob が本来は持っていないレベルの特権が Bob に付与されることがあります。

図 *2*：危険性を伴うトポロジ：複数のホストがネットワーク アクセス サーバに対する *PPP* 接続を共有



二重認証の設定

二重認証を設定するには、次の手順を実行します。

1. **aaa-newmodel** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。AAA をイネーブルにする方法の詳細については、「AAA Overview」を参照してください。
2. **aaaauthentication** コマンドを使用して、ログインおよび ppp 認証方式リストを使用するようにネットワーク アクセス サーバを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaaauthorization** コマンドを使用して、ログイン時の AAA ネットワーク認可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティ プロトコル パラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ の詳細については、「Configuring TACACS+」の章を参照してください。

5 セキュリティ サーバで、ユーザがローカル ホストに接続できるアクセス コントロール リストの AV ペアを使用するには、Telnet 接続を確立する必要があります。

6 （任意）autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモート ユーザは、個人のユーザ プロファイルに関連付けられた権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。

（注） **access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザがローカル ホストに Telnet を送信し、ログインする必要があります。

ユーザ固有の認可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティ サーバでアクセス コントロール リストの AV ペアを設定する場合、有効な AV ペアを使用します。
- リモート ユーザがインターフェイスの既存の認可（第 2 段階の認証/認可の前に存在する認可）を使用し、異なるアクセス コントロール リスト（ACL）を持つようにするには、ユーザ固有の認可定義で ACL AV ペアだけを指定します。この方法は、デフォルトの認可プロファイルを設定してリモート ホストに適用し、ACL はユーザ別に適用する場合などに有効です。
- これらのユーザ固有の認可ステートメントを後でインターフェイスに適用すると、ユーザの認可に使用する **access-profile** コマンドの実行方法によって、既存のインターフェイス設定に追加することや、既存のインターフェイス設定を置き換えることができます。認可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。
- ISDN または Multilink PPP を使用する予定がある場合、ローカル ホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debugaaaper-user** デバッグ コマンドを使用します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

二重認証後のユーザ プロファイルへのアクセス

二重認証で、リモート ユーザがローカル ホスト名を使用してローカル ホストに対する PPP リンクを確立すると、リモート ホストは CHAP（または PAP）認証されます。CHAP（または PAP）認証後、PPP は AAA とネゴシエートして、リモート ホストに関連付けられたネットワーク アクセス特権をユーザに割り当てます（この段階の特権では、ユーザがローカル ホストに接続するには Telnet 接続を必須にするという制限を付けることを推奨します）。

ユーザが二重認証の第 2 段階を開始する必要があり、ローカル ホストに対して Telnet 接続を確立する場合、ユーザは個人のユーザ名とパスワード（CHAP または PAP のユーザ名とパスワードとは異なります）を入力します。この処理の結果、個人のユーザ名/パスワードに従って AAA 認証が発生します。ただし、ローカルホストに関連付けられた初期の権限が有効です。ローカルホストに関連付けられた権限は、**access-profile** コマンドを使用して、ユーザ プロファイルのユーザ用に定義されている権限で置き換えられるか、結合されます。

二重認証後にユーザ プロファイルにアクセスするには、EXEC コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router>` **access-profile** [**merge** | **replace**] [**ignore-sanity-checks**]	二重認証後に、ユーザに関連付けられた権限にアクセスします。

autocommand として実行するように **access-profile** コマンドを設定した場合、リモート ユーザのログイン後に自動的に実行されます。

自動二重認証のイネーブル化

自動二重認証を実装することで、ユーザにとって二重認証プロセスが容易になります。自動二重認証は、二重認証が持つセキュリティ上の利点をすべて備えていますが、リモート ユーザにとってよりシンプルでユーザフレンドリなインターフェイスです。二重認証の場合、ユーザ認証の第 2 レベルは、ユーザがネットワーク アクセス サーバまたはルータに Telnet に送信し、ユーザ名とパスワードを入力したときに完了します。自動二重認証の場合、ユーザがネットワーク アクセス サーバに Telnet を送信する必要はありません。その代わり、ユーザ名とパスワードまたは Personal Identification Number（PIN）の入力を求めるダイアログボックスが表示されます。自動二重認証機能を使用するには、対応するクライアント アプリケーションがリモート ユーザ ホストで実行されている必要があります。

（注） 自動二重認証は、既存の二重認証機能と同様に、Multilink PPP ISDN 接続専用です。自動二重認証は、X.25 や SLIP など他のプロトコルとは併用できません。

自動二重認証は、既存の二重認証機能の強化です。自動二重認証を設定するには、まず次の手順を実行して二重認証を設定する必要があります。

1. **aaa-newmodel** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。
2. **aaaauthentication** コマンドを使用して、ログインおよび ppp 認証方式リストを使用するようにネットワーク アクセス サーバを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaaauthorization** コマンドを使用して、ログイン時の AAA ネットワーク認可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティ プロトコル パラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ の詳細については、「Configuring TACACS+」の章を参照してください。
5. セキュリティ サーバで、ユーザがローカル ホストに接続できるアクセス コントロール リストの AV ペアを使用するには、Telnet 接続を確立する必要があります。

6 autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモート ユーザは、個人のユーザ プロファイルに関連付けられた権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。autocommand の設定方法については、『*CiscoIOS Dial Technologies Command Reference* , Release 12.2』の **autocommand** コマンドを参照してください。

（注） **access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザがローカル ホストに Telnet を送信し、ログインする必要があります。

ユーザ固有の認可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティ サーバでアクセス コントロール リストの AV ペアを設定する場合、有効な AV ペアを使用します。
- リモート ユーザがインターフェイスの既存の認可（第 2 段階の認証/認可の前に存在する認可）を使用し、異なるアクセス コントロール リスト（ACL）を持つようにするには、ユーザ固有の認可定義で ACL AV ペアだけを指定します。この方法は、デフォルトの認可プロファイルを設定してリモート ホストに適用し、ACL はユーザ別に適用する場合などに有効です。
- これらのユーザ固有の認可ステートメントを後でインターフェイスに適用すると、ユーザの認可に使用する **access-profile** コマンドの実行方法によって、既存のインターフェイス設定に追加することや、既存のインターフェイス設定を置き換えることができます。認可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。
- ISDN または Multilink PPP を使用する予定がある場合、ローカル ホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debugaaaper-user** デバッグ コマンドを使用します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

二重認証を設定したら、自動機能を追加できます。

自動二重認証の設定

自動ダブル認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **ip trigger-authentication**
2. 次のいずれかを実行します。
   - Router(config)# **interface bri** *number*
   -
   -
   - Router(config)# **interface serial** *number* **:23**
3. Router(config-if)# **ip trigger-authentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **ip trigger-authentication** 例： ［**timeout** *seconds*］［**port** *number*］	二重認証の自動化をイネーブルにします。
ステップ 2	次のいずれかを実行します。 • Router(config)# **interface bri** *number* • • • Router(config)# **interface serial** *number* **:23**	ISDN BRI インターフェイスまたは ISDN PRI インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Router(config-if)# **ip trigger-authentication**	自動二重認証をインターフェイスに適用します。

自動二重認証のトラブルシューティング

自動二重認証の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **show ip trigger-authentication**
2. Router# **clear ip trigger-authentication**
3. Router# **debug ip trigger-authentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **show ip trigger-authentication**	自動二重認証が試行され、成功または失敗したリモートホストのリストが表示されます。
ステップ 2	Router# **clear ip trigger-authentication**	自動二重認証が試行されたリモートホストのリストをクリアします（これは、**show ip trigger-authentication** コマンドで表示されるテーブルをクリアします）。
ステップ 3	Router# **debug ip trigger-authentication**	自動二重認証に関する **debug** の出力が表示されます。

RADIUS CoA 用の動的認可サービスの設定

次の手順を使用して、動的認可サービスの認証、許可、アカウンティング（AAA）サーバとしてのルータが、入力方向と出力方向でポリシーマップをプッシュするCoA機能をサポートできるようにします。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaserverradiusdynamic-author**
5. **client** {*ip_addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character*| **stripping [right-to-left]**}
7. **port** {*port-num*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaaserverradiusdynamic-author** 例： `Router(config)# aaa server radius dynamic-author`	ローカル AAA サーバを動的認可サービス用にセットアップして、動的認可ローカルサーバコンフィギュレーションモードに入ります。このサービスは、ポリシーマップを入力方向と出力方向にプッシュする CoA 機能をサポートするように有効にする必要があります。このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*ip_addr* | *hostname*} [**server-key** [**0** | **7**] *string*] 例： `Router(config-locsvr-da-radius)#client 192.168.0.5 server-key cisco1`	AAA サーバ クライアントの IP アドレスまたはホスト名を設定します。オプションの **server-key** キーワードと *string* 引数を使用して、クライアント レベルのサーバ キーを設定します。 （注） クライアント レベルでサーバ キーを設定すると、グローバル レベルで設定されたサーバ キーが上書きされます。

ステップ 6	**domain** {**delimiter** *character*| **stripping** **[right-to-left]**}
	
	例：
	
	`Router(config-locsvr-da-radius)# domain stripping right-to-left`
	
	例：
	
	`Router(config-locsvr-da-radius)# domain delimiter @`
		（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。
		
		• **delimiter** キーワードで、ドメイン デリミタを指定します。*character* 引数には、**@**、/、**$**、**%**、\、**#**、または **-** のオプションを指定できます。
		
		• **stripping** キーワードは、着信のユーザ名と、**@** ドメイン デリミタの左側にある名前を比較します。
		
		• **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。

ステップ 7	**port** {*port-num*} 例： `Router(config-locsvr-da-radius)# port 3799`	CoA 要求に UDP ポート 3799 を設定します。

bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定

複数のホストを使用して認証ポートを認証していて、このポートで 1 つのホストに対してフラップする認可変更（CoA）要求があるか、このポートで終了するホスト セッションがある場合、このポート上のその他のホストにも影響があります。したがって、複数のホストを使用して認証されたポートは、フラップの場合に 1 つまたは複数のホストから DHCP の再ネゴシエーションをトリガーします。または、1 つまたは複数のホストについて、セッションをホストする認証ポートを管理的にシャットダウンします。

次の手順を使用して、bounce port コマンドまたは disable port コマンドの形式で RADIUS サーバの認可変更（CoA）要求を無視するようにデバイスを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **authenticationcommandbounce-portignore**
5. **authenticationcommanddisable-portignore**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Device(config)# aaa new-model`	認証、許可、アカウンティング（AAA）をグローバルに有効化します。

	コマンドまたはアクション	目的
ステップ 4	**authenticationcommandbounce-portignore** 例： `Device(config)# authentication command bounce-port ignore`	（任意）RADIUS サーバの bounce port コマンドを無視するようにデバイスを設定します。無視しない場合、認証ポート上でホストがフラップをリンクし、結果として、そのポートに接続する 1 つまたは複数のホストから DHCP 再ネゴシエーションが発生します。
ステップ 5	**authenticationcommanddisable-portignore** 例： `Device(config)# authentication command disable-port ignore`	（任意）RADIUS サーバの CoA disable port コマンドを無視するようにデバイスを設定します。無視しない場合、1 または複数のホストセッションをホストする認証ポートが管理的にシャットダウンされます。 • ポートがシャットダウンされると、セッションも終了します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

サーバ グループ レベルでのドメイン ストリッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *server-name*
4. **domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa group server radius** *server-name* 例： `Device(config)# aaa group server radius rad1`	RADIUS サーバを追加し、サーバ グループ RADIUS コンフィギュレーション モードを開始します。 • *server-name* 引数には、RADIUS サーバ グループ名を指定します。
ステップ 4	**domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*] 例： `Device(config-sg-radius)# domain-stripping delimiter username@example.com`	サーバ グループ レベルでドメイン ストリッピングを設定します。
ステップ 5	**end** 例： `Device(config-sg-radius)# end`	サーバ グループ RADIUS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

非 AAA 認証方式

ライン パスワード保護の設定

このタスクは、パスワードを入力し、パスワード チェック処理を確立することで、端末回線にアクセス コントロールを提供するために使用します。

（注） ライン パスワード保護を設定し、TACACS または拡張 TACACS を設定する場合、TACACS のユーザ名とパスワードの方が、ライン パスワードよりも優先されます。まだセキュリティ ポリシーを実装していない場合、AAA を使用することを推奨します。

手順の概要

1. **enable**
2. **configureterminal**
3. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
4. **password***password*
5. **login**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Router(config)# line console 0`	ライン コンフィギュレーション モードを開始します。
ステップ 4	**password***password* 例： `Router(config-line)# secret word`	回線上の端末または他のデバイスにパスワードを割り当てます。パスワード チェッカでは大文字と小文字が区別され、スペースを使用できます。たとえば、パスワード「Secret」とパスワード「secret」は異なるパスワードです。また、「two words」は有効なパスワードです。
ステップ 5	**login** 例： `Router(config-line)# login`	ログイン時のパスワード チェックをイネーブルにします。 このコマンドの **no** 形式を使用してパスワード チェックをディセーブルにすると、回線パスワード検証をディセーブルにできます。

	コマンドまたはアクション	目的
		（注） **login** コマンドによって変更されるのはユーザ名および特権レベルだけであり、シェルは実行されません。したがって、autocommand は実行されません。この状況で autocommand を実行するには、Telnet セッションをルータに復帰（ループバック）させる必要があります。この方法で autocommand 機能を実装する場合は、ルータがセキュアな Telnet セッションを使用するように設定されていることを確認してください。

ユーザ名認証の確立

ユーザ名ベースの認証システムを作成できます。これは、次のような場合に役立ちます。

- TACACS をサポートしないネットワークに、TACACS のようなユーザ名と暗号化されたパスワード認証システムを提供する場合
- 特殊なケース（たとえば、アクセス リストの確認、パスワードの確認なし、ログイン時の autocommand の実行、「エスケープなし」の状況など）に備えたログインを提供する場合

ユーザ名の認証を確立するには、システム設定の必要に応じて、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. 次のいずれかを実行します。
   - Router(config)# **username***name* [**nopassword** | **password***password* | **password***encryption-typeencryptedpassword*]
   -
   -
   - Router(config)# **username***name* [**access-class***number*]
2. Router(config)# **username***name* [**privilege***level*]
3. Router(config)# **username***name* [**autocommand***command*]
4. Router(config)# **username***name* [**noescape**] [**nohangup**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	次のいずれかを実行します。 • Router(config)# **username***name* [**nopassword** | **password***password* | **password***encryption-typeencryptedpassword*] • • • Router(config)# **username***name* [**access-class***number*]	暗号化されたパスワードを使用してユーザ名認証を確立します。 または （任意）アクセス リストによるユーザ名認証を確立します。
ステップ 2	Router(config)# **username***name* [**privilege***level*]	（任意）ユーザの特権レベルを設定します。
ステップ 3	Router(config)# **username***name* [**autocommand***command*]	（任意）自動実行されるコマンドを指定します。
ステップ 4	Router(config)# **username***name* [**noescape**] [**nohangup**]	（任意）「エスケープなし」のログイン環境を設定します。

次の作業

キーワード **noescape** を指定すると、ユーザは接続先のホストでエスケープ文字を使用できなくなります。**nohangup** 機能を使用すると、autocommand の使用後に接続が解除されません。

注意 **servicepassword-encryption** コマンドをイネーブルにしない限り、設定のパスワードはクリアテキストで表示されます。**servicepassword-encryption** コマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

CHAP 認証または PAP 認証の有効化

インターネット サービス プロバイダー（ISP）のダイヤル ソリューションに使用されている最も一般的なトランスポート プロトコルの 1 つは、ポイントツーポイント プロトコル（PPP）です。従来、リモート ユーザはアクセス サーバにダイヤルインして、PPP セッションを開始していました。PPP のネゴシエート後は、リモート ユーザは ISP ネットワークに接続され、そしてインターネットに接続されます。

ISP はアクセス サーバへの接続を顧客に限定したいため、リモート ユーザはアクセス サーバに対して認証を受けてから、PPP セッションを開始する必要があります。通常、リモート ユーザは、アクセス サーバからのプロンプトに応じてユーザ名とパスワードを入力して、認証を受けます。これは実行可能なソリューションですが、管理が困難で、リモート ユーザにとっても面倒です。

よりよいソリューションは、PPPに組み込まれた認証プロトコルを使用することです。この場合、リモート ユーザはアクセス サーバにダイヤルインし、アクセス サーバと PPP の最小サブセットを開始します。この操作で、ISP のネットワークに対するアクセス権はリモート ユーザに付与されません。単に、アクセス サーバがリモート デバイスと通話できるだけです。

現在、PPP は 2 つの認証プロトコルをサポートします。パスワード認証プロトコル（PAP）およびチャレンジ ハンドシェイク認証プロトコル（CHAP）の 2 つです。いずれも RFC 1334 で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAP または CHAP を介する認証は、サーバからのプロンプトを受けてユーザ名とパスワードを入力する方法と同等です。CHAP の場合、接続の間にリモート ユーザのパスワードは送信されないため、より安全性が高いと考えられます。

（PAP 認証または CHAP 認証の有無に関係なく）PPP はダイヤルアウト ソリューションでもサポートされます。アクセスサーバがダイヤルアウト機能を使用するのは、アクセスサーバからリモート デバイスに対してコールを開始し、PPP などのトランスポート プロトコルを起動しようとするときです。

CHAP と PAP に関する詳細については、『*Cisco IOS XE Dial Technologies Configuration Guide* , Release 2』を参照してください。

（注） CHAP または PAP を使用するには、PPP カプセル化を実行する必要があります。

インターフェイスで CHAP をイネーブルにし、リモート デバイスがそのインターフェイスに接続しようとすると、アクセス サーバからリモートデバイスにCHAPパケットが送信されます。CHAP パケットは、リモート デバイスに応答するように要求または「チャレンジ」します。チャレンジ パケットは、ローカル ルータの ID、ランダム番号、およびホスト名から構成されます。

リモートデバイスは、チャレンジパケットを受信すると、ID、リモートデバイスのパスワード、およびランダム番号を連結し、リモート デバイスのパスワードを使用してすべてを暗号化します。リモート デバイスは、その結果を、暗号化プロセスで使用されたパスワードに関連付けられた名前とともにアクセス サーバに返信します。

アクセスサーバがその応答を受信すると、受信した名前を使用して、ユーザデータベースに保存されているパスワードを取得します。取得したパスワードは、暗号化プロセスで使用されたリモートデバイスと同じパスワードです。アクセスサーバは、新しく取得したパスワードを使用して、連結された情報を暗号化します。その結果が応答パケットで送信された結果と一致する場合、認証は成功です。

CHAP 認証を使用する利点は、リモート デバイスのパスワードがクリア テキストで送信されないことです。結果として、他のデバイスによるパスワード盗用や、ISP のネットワークに対する不正アクセスの取得を回避できます。

CHAP トランザクションが発生するのは、リンクが確立したときだけです。アクセス サーバは、以降のコール中にパスワードを要求しません（ただし、ローカル デバイスは、コール中に他のデバイスからこのような要求があった場合、応答する可能性があります）。

PAP をイネーブルにすると、アクセス サーバに接続しようとするリモート ルータは、認証要求を送信する必要があります。認証要求に指定されているユーザ名とパスワードが受け入れられた場合、Cisco IOS XE ソフトウェアから認証の確認応答が送信されます。

CHAP または PAP をイネーブルにすると、アクセス サーバは、ダイヤルインするリモート デバイスからの認証を必須にするようになります。イネーブルにしたプロトコルをリモート デバイスがサポートしていない場合、コールはドロップされます。

CHAP または PAP を使用するには、次のタスクを実行する必要があります。

1. PPP カプセル化をイネーブルにします。
2. インターフェイスで CHAP または PAP をイネーブルにします。
3. CHAP の場合、認証が必須の各リモート システムについて、ホスト名の認証および秘密（パスワード）を設定します。

PPP カプセル化の有効化

PPP カプセル化をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)#` **encapsulation ppp**	インターフェイスで PPP をイネーブルにします。

PAP または CHAP のイネーブル化

PPP カプセル化として設定されているインターフェイスで、CHAP 認証または PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)#` **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**]	サポートされる認証プロトコルと、使用順序を定義します。このコマンドの *protocol1* と protocol2 は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず *protocol1* に指定された最初の認証方式を使用して試行されます。認証に *protocol1* を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。

インターフェイスで **ppp authentication chap** を設定する場合、そのインターフェイスで PPP 接続を開始するすべての受信コールは、CHAP を使用して認証される必要があります。同様に、**ppp authentication pap** を設定する場合、PPP 接続を開始するすべての受信コールは、PAP を使用して認証される必要があります。**ppp authentication chap pap** を設定する場合、アクセス サーバは、CHAP を使用して PPP セッションを開始するすべての受信を認証しようとします。リモート デバ

イスが CHAP をサポートしない場合、アクセス サーバは PAP を使用してコールを認証しようとします。リモート デバイスが CHAP も PAP もサポートしない場合、認証は失敗し、コールはドロップされます。**ppp authentication pap chap** を設定する場合、アクセス サーバは、PAP を使用して PPP セッションを開始するすべての受信を認証しようとします。リモート デバイスが PAP をサポートしない場合、アクセス サーバは CHAP を使用してコールを認証しようとします。リモート デバイスがいずれのプロトコルもサポートしない場合、認証は失敗し、コールはドロップされます。**callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセス サーバは、リモートデバイスがコールを開始した場合にだけ、リモートデバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA をイネーブルにした場合だけです。TACACS または拡張 TACACS をイネーブルにしている場合は、使用できません。**ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPP は、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPP は、デフォルトに定義されている方式を使用して接続を認証しようとします。**one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイム パスワードをサポートできます。

if-needed キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。**if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモート デバイスがまだ認証されていない場合にだけ、PPP が PAP または CHAP を介してリモートデバイスを認証することを示します。リモートデバイスが、標準のログイン手順で認証を受け、EXEC プロンプトから PPP を開始した場合、**ppp authentication chap if-needed** がインターフェイスで設定されていれば、PPP は CHAP を介して認証しません。

注意 **aaa authentication ppp** コマンドを使用して設定されていない *list-name* を使用する場合、その回線での PPP はディセーブルです。

ローカルルータまたはアクセス サーバが認証を必須とする各リモート システムについて、**username** エントリを追加する方法については、ユーザ名認証の確立, （49 ページ）を参照してください。

着信認証と発信認証

PPP は双方向の認証をサポートしています。通常、リモート デバイスがアクセス サーバにダイヤルインするときは、それが許可されているアクセスであることをリモート デバイスが証明するように、アクセス サーバから要求されます。これは着信認証と呼ばれます。同時に、リモートデバイスは、身元を証明するようにアクセス サーバに要求することもできます。これは発信認証と呼ばれます。また、アクセスサーバは、リモートデバイスに対してコールを開始するときにも、発信認証を実行します。

発信 PAP 認証のイネーブル化

発信 PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)#` **ppp pap sent-username** *username* **password** *password*	発信 PAP 認証をイネーブルにします。

アクセスサーバからリモートデバイスに対してコールを開始する場合は常に、または発信認証のためにリモートデバイスの要求に応答する必要がある場合は、**ppp pap sent-username** コマンドで指定されたユーザ名とパスワードを使用して自身を認証します。

PAP 認証要求の拒否

ピアからの PAP 認証要求を拒否するには（つまり、すべてのコールで PAP 認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)#` **ppp pap refuse**	PAP 認証を要求するピアからの PAP 認証を拒否します。

refuse キーワードが使用されない場合、ルータはピアから受信した PAP 認証チャレンジを拒否しません。

共通 CHAP パスワードの作成

リモート CHAP 認証だけの場合、不明なピアからのチャレンジに対して使用する共通 CHAP シークレット パスワードを作成するように、ルータを設定できます。たとえば、ルータが、新しい（つまり不明な）ルータが追加された、ルータのロータリー（別ベンダー製のルータ、または古いバージョンの Cisco IOS ソフトウェアを実行するルータ）に発信する場合などです。**ppp chap password** コマンドを使用すると、任意のダイヤラ インターフェイスまたは非同期グループ インターフェイスで、複数のユーザ名およびパスワードコンフィギュレーションコマンドをこのコマンドの単一のコピーで置換できます。

ルータのコレクションに発信するルータが、共通の CHAP シークレット パスワードを設定できるようにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)#` **ppp chap password** *secret*	ルータのコレクションに発信するルータが、共通の CHAP シークレット パスワードを設定できるようにします。

CHAP 認証要求の拒否

ピアからの CHAP 認証要求を拒否するには（つまり、すべてのコールで CHAP 認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)#` **ppp chap refuse** [**callin**]	CHAP 認証を要求するピアからの CHAP 認証を拒否します。

callin キーワードが使用されると、ルータは、ピアから受信した CHAP 認証チャレンジへの応答を拒否します。ただし、ルータが送信する CHAP チャレンジに対しては、ピアが応答することを必須とします。

（**ppp pap sent-username** コマンドを使用して）発信 PAP がイネーブルの場合、拒否パケットの認証方式として、PAP が提案されます。

ピアが認証されるまで CHAP 認証を遅延する

ピアがルータから認証を受けるまで、CHAP 認証を要求するピアに対してルータを認証しないように指定するには、インターフェイスコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)#` **ppp chap wait** *secret*	ピアがルータから認証を受けるまで、CHAP 認証を遅延するようにルータを設定します。

このコマンド（デフォルト）により、CHAP 認証を要求するピアがルータの認証を受けてから、ルータがピアの認証を受けるように指定します。**no ppp chap wait** コマンドにより、ルータが認証チャレンジに対して即時に応答するように指定されます。

MS-CHAP の使用

マイクロソフト チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）は、Microsoft バージョンの CHAP であり、RFC 1994 の拡張です。標準バージョンの CHAP と同様に、MS-CHAP は PPP 認証に使用されます。この場合、Microsoft Windows NT または Microsoft Windows 95 を使用する PC と、ネットワーク アクセス サーバとして動作する Cisco デバイスまたはアクセス サーバとの間に認証が発生します。

MS-CHAP と標準の CHAP の違いは次のとおりです。

- MS-CHAP をイネーブルにするには、LCP オプション 3 の Authentication Protocol で、CHAP Algorithm 0x80 をネゴシエートします。
- MS-CHAP 応答パケットは、Microsoft Windows NT 3.5 および 3.51、Microsoft Windows 95、および Microsoft LAN Manager 2.*x* と互換性を持つように設計されたフォーマットです。このフォーマットを使用する場合、オーセンティケータは、クリア パスワードまたは可逆的に暗号化されたパスワードを保存する必要はありません。
- MS-CHAP には、オーセンティケータが制御する認証リトライ メカニズムがあります。
- MS-CHAP には、オーセンティケータが制御するチャレンジ パスワード メカニズムがあります。
- MS-CHAP には、Failure パケット メッセージ フィールドで返される「reason-for failure」コード セットが定義されています。

実装したセキュリティ プロトコルに応じて、AAA セキュリティ サービスの有無にかかわらず、MS-CHAP による PPP 認証を使用できます。AAA をイネーブルにしている場合、MS-CHAP を使用する PPP 認証は、TACACS+ および RADIUS の両方と併用できます。次の表に、RADIUS が MS-CHAP をサポートできるベンダー固有 RADIUS 属性（IETF Attribute 26）を示します。

表 *9*：*MS-CHAP* 用のベンダー固有 *RADIUS* 属性

ベンダー ID 番号	ベンダータイプ 番号	ベンダー固有属性	説明
311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。

ベンダー ID 番号	ベンダータイプ番号	ベンダー固有属性	説明
211	11	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです

MS-CHAP を使用した PPP 認証の定義

MS-CHAP を使用して PPP 認証を定義するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config-if)# **encapsulation ppp**
2. Router(config-if)# **ppp authentication ms-chap** [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config-if)# **encapsulation ppp**	PPP カプセル化をイネーブルにします。
ステップ 2	Router(config-if)# **ppp authentication ms-chap** [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]	MS-CHAP を使用して PPP 認証を定義します。

次の作業

あるインターフェイスで **ppp authentication ms-chap** を設定する場合、PPP 接続を開始するそのインターフェイスに着信するすべてのコールは、MS-CHAP を使用して認証する必要があります。**callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセス サーバは、リモート デバイスがコールを開始した場合にだけ、リモート デバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA をイネーブルにした場合だけです。TACACS または拡張 TACACS をイネーブルにしている場合は、使用できません。**ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPP は、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPP は、デフォルトに定義されている方式を使用し

て接続を認証しようとします。**one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイム パスワードをサポートできます。

if-needed キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。**if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモート デバイスがまだ認証されていない場合にだけ、PPP が MS-CHAP を介してリモートデバイスを認証することを示します。リモートデバイスが、標準のログイン手順で認証を受け、EXEC プロンプトから PPP を開始した場合、**ppp authentication chap if-needed** が設定されていれば、PPP は MS-CHAP を介して認証しません。

（注） MS-CHAP を使用する PPP 認証と、ユーザ名認証を併用する場合、ローカルユーザ名/パスワードデータベースに MS-CHAP シークレットを含める必要があります。ユーザ名認証の詳細については、「ユーザ名認証の確立」の項を参照してください。

認証の例

RADIUS 認証の例

ここでは、RADIUS を使用する 2 つの設定例を紹介します。

次に、RADIUS を使用して認証および認可を行うようにルータを設定する例を示します。

```
aaa authentication login radius-login group radius local
aaa authentication ppp radius-ppp if-needed group radius
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
line 3
login authentication radius-login
interface serial 0
ppp authentication radius-ppp
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- aaa authentication login radius-login group radius local コマンドを実行すると、ルータは、ログイン プロンプトで認証に RADIUS を使用するように設定されます。RADIUS がエラーを返すと、ユーザはローカル データベースを使用して認証されます。
- aaa authentication ppp radius-ppp if-needed group radius コマンドを実行すると、ユーザがまだログインしていない場合、Cisco IOS XE ソフトウェアは CHAP または PAP による PPP 認証を使用するように設定されます。EXEC 施設がユーザを認証すると、PPP 認証は実行されません。
- aaa authorization exec default group radius if-authenticated コマンドを実行すると、autocommand や特権レベルなど、EXEC 認可時に使用される情報について、RADIUS データベースに照会されます。ただし、ユーザの認証が成功した場合にだけ、権限が付与されます。
- aaa authorization network default group radius コマンドを実行すると、ネットワーク認可、アドレス割り当て、および他のアクセス リストについて RADIUS に照会されます。

- **login authentication radius-login** コマンドを使用すると、ライン 3 について radius-login 方式リストがイネーブルになります。
- **ppp authentication radius-ppp** コマンドを使用すると、シリアル インターフェイス 0 について radius-ppp 方式リストがイネーブルになります。

次に、ユーザ名とパスワードの入力を求め、その内容を確認し、ユーザの EXEC レベルを認可し、特権レベル 2 の認可方式として指定するように、ルータを設定する例を示します。この例では、ユーザ名プロンプトにローカル ユーザ名を入力すると、そのユーザ名が認証に使用されます。

ローカル データベースを使用してユーザが認証されると、RADIUS 認証からのデータは保存されないため、RADIUS を使用する EXEC 認可は失敗します。また、この方式リストではローカル データベースを使用して autocommand を検索します。autocommand がない場合、ユーザは EXEC ユーザになります。次に、ユーザが特権レベル 2 に設定されているコマンドを発行しようとすると、TACACS+ を使用してコマンドの認可が試行されます。

```
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa authorization command 2 default group tacacs+ if-authenticated
radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- aaa authentication login default group radius local コマンドにより、RADIUS（RADIUS が応答しない場合はルータのローカル ユーザ データベース）がユーザ名およびパスワードを確認するように指定します。
- aaa authorization exec default group radius local コマンドにより、RADIUS を使用してユーザが認証される場合、ユーザの EXEC レベルの設定に RADIUS 認証情報を使用するように指定します。RADIUS 情報が使用されない場合、このコマンドにより、EXEC 認可にローカル ユーザ データベースが使用されるように指定します。
- aaa authorization command 2 default group tacacs+ if-authenticated コマンドにより、すでにユーザの認証が成功している場合、特権レベル 2 に設定されているコマンドに TACACS+ 認可を指定します。
- radius-server host 172.16.71.146 auth-port 1645 acct-port 1646 コマンドにより、RADIUS サーバ ホストの IP アドレス、認証要求の UDP 宛先ポート、およびアカウンティング要求の UDP 宛先ポートを指定します。
- radius-server attribute 44 include-in-access-req コマンドにより、access-request パケットで RADIUS 属性 44（Acct-Session-ID）を送信します。
- radius-server attribute 8 include-in-access-req コマンドにより、access-request パケットで RADIUS 属性 8（Framed-IP-Address）を送信します。

TACACS 認証の例

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
aaa new-model
aaa authentication ppp test group tacacs+ local
interface serial 0
ppp authentication chap pap test
tacacs-server host 192.0.2.3
tacacs-server key goaway
```

この TACACS+ 認証設定のサンプル行は、次のように定義されます。

- **aaanew-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaaauthentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「test」を定義します。キーワード **grouptacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **interface** コマンドにより、回線を選択します。
- **pppauthentication** コマンドにより、この回線に test 方式リストを適用します。
- **tacacs-serverhost** コマンドにより、TACACS+ デーモンが 192.0.2.3 という IP アドレスを持っていると指定します。
- **tacacs-serverkey** コマンドにより、共有暗号キーを「goaway」に定義します。

次に、PPP に AAA 認証を設定する例を示します。

```
aaa authentication ppp default if-needed group tacacs+ local
```

この例のキーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合、PPP は不要なので、スキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、認証が TACACS+ を介して実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
aaa authentication ppp MIS-access if-needed group tacacs+ local
interface serial 0
ppp authentication pap MIS-access
```

この例では、リストはどのインターフェイスにも適用されないため（自動的にすべてのインターフェイスに適用されるデフォルト リストとは異なります）、管理者は **interface** コマンドを使用して、この認証スキームを適用するインターフェイスを選択する必要があります。次に、管理者は **ppp authentication** コマンドを使用して、選択したインターフェイスにこの方式リストを適用する必要があります。

Kerberos 認証の例

ログイン認証方式として Kerberos を指定するには、次のコマンドを使用します。

```
aaa authentication login default krb5
```

PPP に Kerberos 認証を指定するには、次のコマンドを使用します。

```
aaa authentication ppp default krb5
```

AAA スケーラビリティの例

次に、セキュリティ プロトコルとして RADIUS による AAA を使用する一般的なセキュリティ設定例を示します。この例では、ネットワーク アクセス サーバは、16 バックアップ プロセスを割り当てて PPP に対する AAA 要求を処理するように設定されています。

```
aaa new-model
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authentication login admins local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa processes 16
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication pap dialins
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **radius-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** コマンドは、ネットワーク アクセス サーバと RADIUS サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **radius-server configure-nas** コマンドは、デバイスが最初に起動したときに、Cisco ルータまたはアクセス サーバがスタティック ルートと IP プール定義について RADIUS サーバに照会するように定義します。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP パスワード認証プロトコル（PAP）認証での発信元の身元確認に使用されます。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。

- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドで、PPP の使用状況を追跡します。
- **aaa processes** コマンドにより、PPP に対する AAA 要求を処理するために 16 バックグラウンド プロセスを割り当てます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるようにします。
- **autoselect during-login** コマンドを使用して、Return キーを押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に「admins」方式リストを適用します。
- **modem dialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。
- **interface group-async** コマンドは非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定したインターフェイスに適用します。

例：AAA 認証のログイン バナーおよび Failed-Login バナーの設定

次に、ユーザがシステムにログインするときに表示されるログイン バナー（この場合、「Unauthorized Access Prohibited」というフレーズ）を設定する例を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
```

次の例では、ユーザがシステムにログインしようとして失敗すると表示される Failed-Login バナー（この場合、「Failed login.Try again」というフレーズ）を設定する方法を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーおよび Failed-Login バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

AAA パケット オブ ディスコネクト サーバ キーの例

次に、パケット オブ ディスコネクト（POD）を設定する例を示します。その結果、特定のセッション属性が指定されると、ネットワーク アクセス サーバ（NAS）の接続が終了します。

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
aaa pod server server-key xyz123
radius-server host 192.0.2.3 non-standard
radius-server key rad123
```

二重認証の例

ここでは、二重認証に使用できる設定例を示します。実際のネットワークおよびセキュリティ要件によっては、この例とは大幅に異なる可能性があります。

（注） 設定例には、特定の IP アドレスと他の特定の情報が含まれます。この情報は説明のための例であり、実際の設定には異なる IP アドレス、異なるユーザ名とパスワード、異なる認可ステートメントを使用します。

二重認証による AAA のローカル ホストの設定例

次の 2 つの例では、PPP とログイン認証、およびネットワークと EXEC 認可に AAA を使用するようにローカル ホストを設定する方法を示します。例はそれぞれ RADIUS の例と TACACS+ の例です。

いずれの例でも、先頭の 3 行で AAA を設定し、特定のサーバを AAA サーバとして設定しています。続く 2 行で PPP およびログイン認証に AAA を設定し、最後の 2 行でネットワークおよび EXEC 認可を設定します。最後の行が必要なのは、**access-profile** コマンドを autocommand として実行する場合だけです。

次に、RADIUS AAA サーバを使用するデバイス設定の例を示します。

```
aaa new-model
radius-server host secureserver
radius-server key myradiuskey
aaa authentication ppp default group radius
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization exec default group radius
```

次に、TACACS+ サーバを使用するデバイス設定の例を示します。

```
aaa new-model
tacacs-server host security
tacacs-server key mytacacskey
aaa authentication ppp default group tacacs+
aaa authentication login default group tacacs+
aaa authorization network default group tacacs+
aaa authorization exec default group tacacs+
```

第 1 段階の PPP 認証と認可に関する AAA サーバの設定例

次に、AAA サーバでの設定例を示します。また、RADIUS 用の AAA 設定例の一部を示します。

TACACS+ サーバも同様に設定できます（「TACACS による設定完了の例」を参照してください）。

この例では、二重認証の第 1 段階で CHAP によって認証される「hostx」というリモート ホストに関する認証/認可を定義します。ACL AV ペアは、リモート ホストによる Telnet 接続をローカル ホストに制限しています。ローカル ホストの IP アドレスは 10.0.0.2 です。

次に、RADIUS 用の AAA サーバの設定例を一部示します。

```
hostx   Password = "welcome"
        User-Service-Type = Framed-User,
        Framed-Protocol = PPP,
        cisco-avpair = "lcp:interface-config=ip unnumbered fastethernet 0",
        cisco-avpair = "ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet",
        cisco-avpair = "ip:inacl#4=deny icmp any any",
        cisco-avpair = "ip:route#5=10.0.0.0 255.0.0.0",
        cisco-avpair = "ip:route#6=10.10.0.0 255.0.0.0",
        cisco-avpair = "ipx:inacl#3=deny any"
```

第 2 段階の Per-User 認証と認可に関する AAA サーバの設定例

ここでは、RADIUS サーバでの AAA 設定例の一部を示します。これらの設定では、ユーザ名が「patuser」のユーザ（Pat）の認証と認可を定義します。このユーザは、二重認証の第 2 段階でユーザ認証されます。

TACACS+ サーバも同様に設定できます（「TACACS による設定完了の例」を参照してください）。

3 つの例は、**access-profile** コマンドの 3 つの各形式で使用できる RADIUS AAA 設定の例を示します。

最初の例は、**access-profile** コマンドのデフォルト フォーム（キーワードなし）で機能する AAA 設定例の一部を示します。1 つの ACL AV ペアのみが定義されます。また、この例では autocommand として **access-profile** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any host 10.0.0.2 eq telnet",
          cisco-avpair = "ip:inacl#4=deny icmp any any"
```

2 番めの例は、**access-profile** コマンドの **access-profile merge** 形式で機能する AAA 設定例の一部を示します。また、この例では autocommand として **access-profile merge** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile merge"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any any"
          cisco-avpair = "ip:route=10.0.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.1.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.2.0.0 255.255.0.0"
```

3 番めの例は、**access-profile** コマンドの **access-profile replace** 形式で機能する AAA 設定例の一部を示します。また、この例では autocommand として **access-profile replace** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile replace"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any any",
          cisco-avpair = "ip:inacl#4=permit icmp any any",
          cisco-avpair = "ip:route=10.10.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.11.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.12.0.0 255.255.0.0"
```

TACACS による設定完了の例

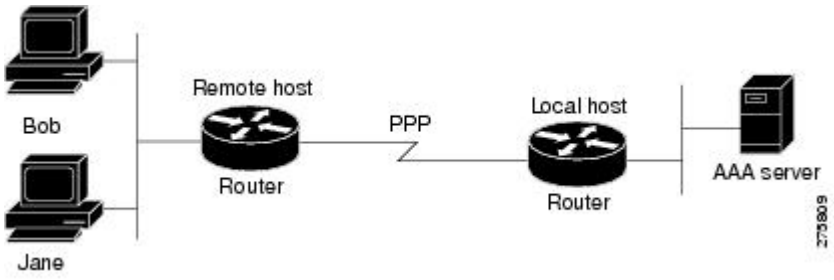
この例では、リモート ホスト（二重認証の第 1 段階で使用）および特定のユーザ（二重認証の第 2 段階で使用）の両方向けの、TACACS+ 認可プロファイルの設定を示します。この TACACS+ の例には、前の RADIUS の例とほぼ同じ設定情報が使用されます。

この設定例は、リモート ホスト「hostx」および 3 ユーザ（ユーザ名が「pat_default」、「pat_merge」、および「pat_replace」）の TACACS+ サーバ上にある認証/認可プロファイルを示

します。これら 3 つのユーザ名の設定は、**access-profile** コマンドの 3 種類のフォームに対応する異なる設定を示しています。また、3 つのユーザ設定は、**access-profile** コマンドの各形式について autocommand の設定方法も示しています。

次の図に、トポロジを示します。図の後に、TACACS+ 設定ファイルの例を示します。

図 *3*：二重認証のトポロジ例



この設定例は、リモート ホスト「hostx」および 3 ユーザ（ユーザ名が「pat_default」、「pat_merge」、および「pat_replace」）の TACACS+ サーバ上にある認証/認可プロファイルを示します。

```
key = "mytacacskey"
default authorization = permit
#-----------------------------Remote Host (BRI)-------------------------
#
# This allows the remote host to be authenticated by the local host
# during fist-stage authentication, and provides the remote host
# authorization profile.
#
#-----------------------------------------------------------------------
user = hostx
{
    login = cleartext "welcome"
    chap = cleartext "welcome"
    service = ppp protocol = lcp {
                interface-config="ip unnumbered fastethernet 0"
    }
    service = ppp protocol = ip {
            # It is important to have the hash sign and some string after
            # it. This indicates to the NAS that you have a per-user
            # config.
            inacl#3="permit tcp any 172.21.114.0 0.0.0.255 eq telnet"
            inacl#4="deny icmp any any"
            route#5="10.0.0.0 255.0.0.0"
            route#6="10.10.0.0 255.0.0.0"
    }
    service = ppp protocol = ipx {
            # see previous comment about the hash sign and string, in protocol = ip
            inacl#3="deny any"
    }
}
#------------------- "access-profile" default user "only acls" ------------------
#
# Without arguments, access-profile removes any access-lists it can find
# in the old configuration (both per-user and per-interface), and makes sure
# that the new profile contains ONLY access-list definitions.
#
#-------------------------------------------------------------------------------
user = pat_default
{
        login = cleartext "welcome"
        chap = cleartext "welcome"
```

```
        service = exec
        {
                # This is the autocommand that executes when pat_default logs in.
                autocmd = “access-profile”
        }
        service = ppp protocol = ip {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any host 10.0.0.2 eq telnet”
                inacl#4=”deny icmp any any”
        }
        service = ppp protocol = ipx {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
#--------------------- “access-profile merge” user ---------------------------
#
# With the 'merge' option, first all old access-lists are removed (as before),
# but then (almost) all AV pairs are uploaded and installed. This will allow
# for uploading any custom static routes, sap-filters, and so on, that the user
# may need in his or her profile. This needs to be used with care, as it leaves
# open the possibility of conflicting configurations.
#
#-------------------------------------------------------------------------------
user = pat_merge
{
        login = cleartext “welcome”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_merge logs in.
                autocmd = “access-profile merge”
        }
        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any any”
                route#2=”10.0.0.0 255.255.0.0"
                route#3=”10.1.0.0 255.255.0.0"
                route#4=”10.2.0.0 255.255.0.0"
        }
        service = ppp protocol = ipx
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
#--------------------- “access-profile replace” user ----------------------------
#
# With the 'replace' option, ALL old configuration is removed and ALL new
# configuration is installed.
#
# One caveat: access-profile checks the new configuration for address-pool and
# address AV pairs. As addresses cannot be renegotiated at this point, the
# command will fail (and complain) when it encounters such an AV pair.
# Such AV pairs are considered to be “invalid” for this context.
#-------------------------------------------------------------------------------
user = pat_replace
{
```

```
        login = cleartex
t
“
welcome
”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_replace logs in.
                autocmd = “access-profile replace”
        }
        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any any”
                inacl#4=”permit icmp any any”
                route#2=”10.10.0.0 255.255.0.0"
                route#3=”10.11.0.0 255.255.0.0"
                route#4=”10.12.0.0 255.255.0.0"
        }
        service = ppp protocol = ipx
        {
                # put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
```

自動二重認証の例

次に、自動二重認証が設定された設定ファイル全体の例を示します。自動二重認証に適用されるコンフィギュレーション コマンドは、2 つのアスタリスク（**）を使用した記述よりも優先されます。

```
Current configuration:
!
version 11.3
no service password-encryption
!
hostname myrouter
!
!
! **The following AAA commands are used to configure double authentication:
!
! **The following command enables AAA:
aaa new-model
! **The following command enables user authentication via the RADIUS AAA server:
!
aaa authentication login default none
aaa authentication ppp default group radius
! **The following command causes the remote user’s authorization profile to be
! downloaded from the AAA server to the router when required:
!
aaa authorization network default group radius
!
enable password mypassword
!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name example.com
```

```
ip name-server 172.16.2.75
!
!
interface FastEthernet0/0/0
 ip address 172.21.127.186 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 no keepalive
 ntp disable
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered loopback0
 no ip route-cache
 no ip mroute-cache
!
! **The following command specifies that device authentication occurs via PPP CHAP:
 ppp authentication chap
!
router eigrp 109
 network 172.21.0.0
 no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
dialer-list 1 protocol ip permit
no cdp run
! **The following command defines where the TACACS+ AAA server is:
tacacs-server host 172.16.57.35 port 1049
tacacs-server timeout 90
! **The following command defines the key to use with TACACS+ traffic (required):
tacacs-server key mytacacskey
snmp-server community public RO
!
line con 0
 exec-timeout 0 0
 login authentication console
line aux 0
 transport input all
line vty 0 4
 exec-timeout 0 0
 password lab
!
end
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドで、PPP の使用状況を追跡します。

- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP パスワード認証プロトコル（PAP）認証での発信元の身元確認に使用されます。
- **radius-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** コマンドは、ネットワーク アクセス サーバと RADIUS サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **interface group-async** コマンドは非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **ppp authentication ms-chap dialins** コマンドは PPP 認証方式として MS-CHAP を選択し、特定のインターフェイスに「dialins」方式リストを適用します。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるようにします。
- **autoselect during-login** コマンドを使用して、Return キーを押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に「admins」方式リストを適用します。
- **modem dialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

その他の参考資料

ここでは、認証の設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
許可	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring Authorization」
アカウンティング	『*Cisco IOS XE Security Configuration Guide: Securing User Service* , Release 2』の「Configuring Accounting」

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1334	PPP 認証プロトコル
RFC 2433	「Microsoft PPP CHAP Extensions」
RFC 2903	「*Generic AAA Architecture*」
RFC 2904	「*AAA Authorization Framework*」
RFC 2906	「*AAA Authorization Requirements*」
RFC 2989	「*Criteria for Evaluating AAA Protocols for Network Access*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

認証の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：認証の設定に関する機能情報

機能名	リリース	機能情報
AAA 方式リストの拡張	Cisco IOS XE Release 2.1	この機能を使用すると、認証、許可、アカウンティングのフォールバック方式を有効にすることができます。フォールバック方式では、RADIUS または TACACS+ サーバまたは、場合によってはローカル データベースのグループ化の試行が行われます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaaauthenticationppp**。
AAA のユーザ別スケーラビリティ	Cisco IOS XE Release 2.3	AAA のユーザ別スケーラビリティ機能では、**ipvrf** および **ipunnumbered** コマンド向けに 2 つの RADIUS VSA がサポートされています。優れた拡張性を達成するために完全な VA インターフェイスの代わりに指定されている場合は、サブバーチャル アクセス インターフェイスを作成します。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

機能名	リリース	機能情報
チャレンジ ハンドシェイク認証プロトコル（CHAP）	Cisco IOS XE Release 2.1	現在、PPP は 2 つの認証プロトコルをサポートします。パスワード認証プロトコル（PAP）およびチャレンジ ハンドシェイク認証プロトコル（CHAP）の 2 つです。いずれも RFC 1334 で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAP または CHAP を介する認証は、サーバからのプロンプトを受けてユーザ名とパスワードを入力する方法と同等です。CHAP の場合、接続の間にリモートユーザのパスワードは送信されないため、より安全性が高いと考えられます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。 **pppauthentication**、**pppchappassword**、**pppchaprefuse**。

機能名	リリース	機能情報
サーバ グループ レベルでのドメイン ストリッピング	Cisco IOS XE Release 3.4S	ドメイン ストリッピング機能を使用すると、ドメイン ストリッピングをサーバ グループ レベルで設定できます。サーバ単位のグループ コンフィギュレーションはグローバル コンフィギュレーションを上書きします。 この機能に関する詳細については、次の各項を参照してください。 • ドメイン ストリッピング • サーバ グループ レベルでのドメイン ストリッピングの設定 次のコマンドが導入されました。**domain-stripping**。
二重認証	Cisco IOS XE Release 2.1	Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaaauthentication**、**aaaauthorization**、**access-profile**。
AAA 認証のメッセージ バナー	Cisco IOS XE Release 2.1	Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaaauthenticationbanner**。

機能名	リリース	機能情報
MS-CHAP バージョン 1	Cisco IOS XE Release 2.1	マイクロソフト チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）は、Microsoft バージョンの CHAP であり、RFC 1994 の拡張です。標準バージョンの CHAP と同様に、MS-CHAP は PPP 認証に使用されます。この場合、Microsoft Windows NT または Microsoft Windows 95 を使用する PC と、ネットワーク アクセス サーバとして動作する Cisco ルータまたはアクセス サーバとの間に認証が発生します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。 **pppauthentication**。

機能名	リリース	機能情報
Password Authentication Protocol（PAP）	Cisco IOS XE Release 2.1	現在、PPP は 2 つの認証プロトコルをサポートします。パスワード認証プロトコル（PAP）およびチャレンジ ハンドシェイク認証プロトコル（CHAP）の 2 つです。いずれも RFC 1334 で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAP または CHAP を介する認証は、サーバからのプロンプトを受けてユーザ名とパスワードを入力する方法と同等です。CHAP の場合、接続の間にリモートユーザのパスワードは送信されないため、より安全性が高いと考えられます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**pppauthentication**、**ppppapsent-username**、**ppppaprefuse**。
RADIUS：ユーザ名が空のアクセス要求を送信しないようにする CLI	Cisco IOS XE Release 2.4	この認証機能によって、ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにします。この機能により、RADIUS サーバとの不要なやりとりを回避でき、RADIUS ログの量を少なくすることができます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入されました。**aaaauthenticationsuppressnull-username**。

第 3 章

RADIUS 許可の変更

RADIUS 認可変更（CoA）機能は、認証、許可、アカウンティング（AAA）セッションの属性を、セッション認証後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は Cisco Secure Access Control Server（ACS）などの AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーを適用することができます。

- 機能情報の確認，79 ページ
- RADIUS 認可変更に関する情報，80 ページ
- RADIUS 認可変更の設定方法，85 ページ
- RADIUS 認可変更の設定例，91 ページ
- RADIUS 認可変更に関する追加情報，92 ページ
- RADIUS 認可変更の機能情報，93 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

RADIUS 認可変更に関する情報

RADIUS 認可変更について

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。シスコのソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS CoA 要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、許可、アカウンティング（AAA）またはポリシー サーバからの動的なセッション再設定が可能になります。

次のセッション単位の CoA 要求を使用します。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了
- セキュリティとパスワード
- アカウンティング

CoA 要求

CoA 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。モデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してデバイスでサポートされています。

次の表に、RADIUS 認可変更（CoA）機能でサポートされている IETF 属性を示します。

表 *11*：サポートされている *IETF* 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *12*：*Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー

値	説明
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求の応答コードは、デバイスへコマンドを発行するために使用されます。サポートされているコマンドを「CoA 要求コマンド」に示します。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

属性フィールドは、Cisco ベンダー固有属性（VSA）を送信するために使用します。

セッションの識別

特定のセッションに対する接続解除および CoA 要求の場合、デバイスは次の 1 つまたは複数の属性に基づいてセッションを検出します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id（シスコのベンダー固有属性（VSA））
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、デバイスは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

（注） CoA NAK メッセージは、キーの不一致があるすべての CoA 要求に送信されるわけではありません。メッセージは、クライアントの最初の 3 つの要求にのみ送信されます。その後、そのクライアントからのすべてのパケットがドロップされます。キーの不一致が見つかると、CoA NAK メッセージで送信される応答オーセンティケータはダミーのキー値から計算されます。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なります。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。

CoA 要求コマンド

デバイスでサポートされているコマンドを次の表に示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *13*：デバイスでサポートされる *CoA* 要求コマンド

コマンド	シスコの VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	VSA を必要としない標準の接続解除要求です

セッション再認証

セッション認証を開始するために、認証、許可、アカウンティング（AAA）サーバは、Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は、Cisco:Avpair=“subscriber:command=reauthenticate” の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1*x* によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN（EAPoL）-RequestId メッセージをサーバに送信することで応答します。
- セッションが現在 MAC 認証バイパス（MAB）によって認証されている場合、デバイスはアクセス要求をサーバに送信し、最初に成功した認証で使用したのと同じ ID 属性を渡します。
- デバイスがコマンドを受信した際にセッション認証が実行中である場合は、デバイスはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションの終了

CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。CoA 接続解除要求終了によって、指定したホストのオーセンティケータ ステートマシンが再初期化されま

すが、ホストのネットワークへのアクセスは制限されません。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

CoA 要求の disable host port

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。デバイスは、セッションを検出すると、ホスティング ポートを無効にし、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブ デバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

RADIUS サーバの CoA disable port コマンドを無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

CoA 要求の bounce port

RADIUS サーバの CoA bounce port が RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「セッション ID」に示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。こ

のセッションがある場合は、デバイスはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

RADIUS サーバの CoA bounce port を無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

RADIUS 認可変更の設定方法

RADIUS 認可変更の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf***vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port***port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	認証、許可、アカウンティング（AAA）をグローバルに有効化します。

	コマンドまたはアクション	目的
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ダイナミック許可ローカル サーバ コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外すRADIUSクライアントを指定します。デバイスを AAA サーバとして設定し、外部ポリシー サーバとの連携を可能にする。
ステップ 5	**client** {*ip-address* | *name* [**vrf***vrf-name*]} **server-key** [**0** | **7**] *string* 例： `Device(config-locsvr-da-radius)# client 10.0.0.1`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 6	**port***port-number* 例： `Device(config-locsvr-da-radius)# port 3799`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。 （注） パケット オブ ディスコネクトのデフォルト ポートは 1700 です。ACS 5.1 と相互運用するためには、ポート 3799 が必要です。
ステップ 7	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-locsvr-da-radius)# auth-type all`	デバイスがRADIUSクライアントに使用する許可のタイプを指定します。クライアントは、認証用に設定された属性と一致していなければなりません。
ステップ 8	**ignore session-key** 例： `Device(config-locsvr-da-radius)# ignore session-key`	（オプション）セッション キーを無視するようにデバイスを設定します。
ステップ 9	**ignore server-key** 例： `Device(config-locsvr-da-radius)# ignore server-key`	（オプション）サーバ キーを無視するようにデバイスを設定します。
ステップ 10	**exit** 例： `Device(config-locsvr-da-radius)# exit`	グローバル コンフィギュレーション モードに戻ります。

bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定

複数のホストを使用して認証ポートを認証していて、このポートで 1 つのホストに対してフラップする認可変更（CoA）要求があるか、このポートで終了するホスト セッションがある場合、このポート上のその他のホストにも影響があります。したがって、複数のホストを使用して認証されたポートは、フラップの場合に 1 つまたは複数のホストから DHCP の再ネゴシエーションをトリガーします。または、1 つまたは複数のホストについて、セッションをホストする認証ポートを管理的にシャットダウンします。

次の手順を使用して、bounce port コマンドまたは disable port コマンドの形式で RADIUS サーバの認可変更（CoA）要求を無視するようにデバイスを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **authenticationcommandbounce-portignore**
5. **authenticationcommanddisable-portignore**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Device(config)# aaa new-model`	認証、許可、アカウンティング（AAA）をグローバルに有効化します。

	コマンドまたはアクション	目的
ステップ 4	**authenticationcommandbounce-portignore** 例： `Device(config)# authentication command bounce-port ignore`	（任意）RADIUS サーバの bounce port コマンドを無視するようにデバイスを設定します。無視しない場合、認証ポート上でホストがフラップをリンクし、結果として、そのポートに接続する 1 つまたは複数のホストから DHCP 再ネゴシエーションが発生します。
ステップ 5	**authenticationcommanddisable-portignore** 例： `Device(config)# authentication command disable-port ignore`	（任意）RADIUS サーバの CoA disable port コマンドを無視するようにデバイスを設定します。無視しない場合、1 または複数のホストセッションをホストする認証ポートが管理的にシャットダウンされます。 • ポートがシャットダウンされると、セッションも終了します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

RADIUS CoA 用の動的認可サービスの設定

次の手順を実行して、動的許可サービスの認証、許可、アカウンティング（AAA）サーバとしてデバイスを有効にします。このサービスは、入力方向と出力方向でポリシー マップをプッシュする認可変更（CoA）機能をサポートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter***character* | **stripping** | [**right-to-left**]}
7. **port***port-num*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ローカル AAA サーバを動的認可サービス用にセットアップして、動的認可ローカル サーバ コンフィギュレーション モードに入ります。このサービスは、ポリシーマップを入力方向と出力方向にプッシュする CoA 機能をサポートするように有効にする必要があります。 • このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*] 例： `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	AAA サーバ クライアントの IP アドレスまたはホスト名を設定します。 • オプションの **server-key** キーワードと *string* 引数を使用して、クライアント レベルのサーバ キーを設定します。 （注） クライアント レベルでサーバ キーを設定すると、グローバル レベルで設定されたサーバ キーが上書きされます。
ステップ 6	**domain** {**delimiter***character* | **stripping** | [**right-to-left**]} 例： `Device(config-locsvr-da-radius)# domain stripping right-to-left`	（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。 • **delimiter** キーワードで、ドメインデリミタを指定します。*character* 引数には、**@**、/、**$**、**%**、\、**#**、または **-** のオプションを指定できます。 • **stripping** キーワードは、着信のユーザ名と、**@** ドメインデリミタの左側にある名前を比較します。 • **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。

	コマンドまたはアクション	目的
ステップ 7	**port***port-num* 例： `Device(config-locsvr-da-radius)# port 3799`	CoA 要求に UDP ポートを設定します。
ステップ 8	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。

RADIUS 認可変更のモニタリングとトラブルシューティング

RADIUS 認可変更機能のモニタリングおよび問題を解決するために、次のコマンドを使用できます。

表 *14*：*RADIUS* 認可変更のモニタリングとトラブルシューティング

コマンド	目的
debug aaa coa	CoA 処理のデバッグ情報を表示します。
debug aaa pod	パケット オブ ディスコネクト（POD）パケットに関連するデバッグ メッセージを表示します。
debug radius	RADIUS 関連の情報を表示します。
show aaa attributes protocol radius	認証、許可、アカウンティング（AAA）属性番号と対応する AAA 属性名のマッピングを表示します。

RADIUS 認可変更の設定例

例：RADIUS 認可変更の設定

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.0.0.1
Device(config-locsvr-da-radius)# server-key cisco123
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# auth-type all
Device(config-locsvr-da-radius)# ignore session-key
Device(config-locsvr-da-radius)# ignore server-key
Device(config-locsvr-da-radius)# end
```

例：bounce および disable RADIUS 要求を無視するためのデバイスの設定

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# authentication command bounce-port ignore
Device(config)# authentication command disable-port ignore
Device(config)# end
```

例：RADIUS CoA 用の動的認可サービスの設定

次に、認証、許可、アカウンティング（AAA）サーバとしてのデバイスが、入力方向と出力方向でポリシー マップをプッシュする認可変更（CoA）機能をサポートするように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1
Device(config-locsvr-da-radius)# domain delimiter @
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# end
```

RADIUS 認可変更に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA の設定	『認証、許可、アカウンティング コンフィギュレーション ガイド』

標準および RFC

標準/RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 5176	「*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS 認可変更の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *15*：*RADIUS* 認可変更の機能情報

機能名	リリース	機能情報
RADIUS 許可の変更		RADIUS 認可変更（CoA）機能は、AAA セッションの属性をセッション認証後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザグループのポリシーに変更がある場合、管理者は Cisco Secure Access Control Server（ACS）などの AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーを適用することができます。 次のコマンドが導入または変更されました。**aaa server radius dynamic-author**、**authentication command bounce-port ignore**、および **authentication command disable-port ignore**。

第 4 章

AAA 認証のメッセージ バナー

AAA 認証のメッセージ バナー機能は、ユーザ認証のためにパーソナライズされたログイン バナーおよび failed-login バナーを設定するために使用されます。ユーザが認証、許可、アカウンティング（AAA）を使用して認証を受けるシステムにログインする場合に認証が失敗すると、メッセージ バナーが表示されます。

- 機能情報の確認，95 ページ
- AAA 認証のメッセージ バナーに関する情報，96 ページ
- AAA 認証のメッセージ バナーの設定方法，96 ページ
- AAA 認証のメッセージ バナーの設定例，99 ページ
- AAA 認証のメッセージ バナーに関する追加情報，99 ページ
- AAA 認証のメッセージ バナーの機能情報，100 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA 認証のメッセージ バナーに関する情報

AAA 認証のログイン バナーおよび Failed-Login バナー

ログインバナーおよびfailed-loginバナーは、認証、許可、およびアカウンティング（AAA）認証用のバナーとして表示する必要があるテキスト文字列そのものをシステムに通知するデリミタを使用します。デリミタは、ログイン バナーまたはfailed-loginバナーの末尾を示すために、テキスト文字列の末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナー用のテキスト文字列には使用できません。

ログイン バナーまたは failed-login バナーには、最大 2996 文字を表示できます。

AAA 認証のメッセージ バナーの設定方法

AAA 認証のログイン バナーの設定

次の作業を行って、ユーザがログインするときに表示されるバナーを設定します（デフォルトのログイン メッセージを置き換えます）。ログイン バナーをディセーブルにするには、**no aaa authentication banner** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner** *delimiter-string delimiter*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaa authentication banner** *delimiter-string delimiter* 例： `Device(config)# aaa authentication banner *Unauthorized Access Prohibited*`	パーソナライズされたログインバナーを作成します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

AAA 認証の Failed-Login バナーの設定

次の作業を行って、ユーザ ログインが失敗したときに表示される faild-login バナーを設定します（デフォルトのメッセージを failed-login に置き換えます）。failed-login バナーをディセーブルにするには、**no aaa authentication fail-message** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner** *delimiter-string delimiter*
5. **aaa authentication fail-message** *delimiter-string delimiter*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに開始します。
ステップ 4	**aaa authentication banner** *delimiter-string delimiter* 例： `Device(config)# aaa authentication banner *Unauthorized Access Prohibited*`	パーソナライズされたログインバナーを作成します。
ステップ 5	**aaa authentication fail-message** *delimiter-string delimiter* 例： `Device(config)# aaa authentication fail-message *Failed login. Try again*`	ユーザログインが失敗したときに表示されるメッセージを作成します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

AAA 認証のメッセージ バナーの設定例

例：AAA 認証のログイン バナーおよび Failed-Login バナーの設定

次に、ユーザがシステムにログインするときに表示されるログイン バナー（この場合、「Unauthorized Access Prohibited」というフレーズ）を設定する例を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
```

次の例では、ユーザがシステムにログインしようとして失敗すると表示される Failed-Login バナー（この場合、「Failed login.Try again」というフレーズ）を設定する方法を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーおよび Failed-Login バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

AAA 認証のメッセージ バナーに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA の設定	『認証、許可、アカウンティング コンフィギュレーション ガイド』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AAA 認証のメッセージ バナーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *16*：*AAA* 認証のメッセージ バナーの機能情報

機能名	リリース	機能情報
AAA 認証のメッセージ バナー		AAA 認証のメッセージ バナー機能により、ユーザ認証のためにパーソナライズされたログイン バナーおよび failed-login バナーを設定できます。ユーザが認証、許可、アカウンティング（AAA）を使用して認証を受けるシステムにログインする場合に認証が失敗すると、メッセージ バナーが表示されます。 次のコマンドが導入または変更されました。**aaa authentication banner**、 **aaa authentication fail-message**、 および **aaa new-model**。

第 5 章

サーバ グループ レベルでの AAA ドメイン ストリッピング

サーバ グループ レベルでの AAA ドメイン ストリッピング機能を使用すると、ドメイン ストリッピングをサーバ グループ レベルで設定できます。

- 機能情報の確認，103 ページ
- サーバ グループ レベルでの AAA ドメイン ストリッピングに関する情報，104 ページ
- サーバ レベル グループでの AAA ドメイン ストリッピングの設定方法，105 ページ
- サーバ グループ レベルでの AAA ドメイン ストリッピングの設定例，106 ページ
- その他の参考資料，106 ページ
- サーバ グループ レベルでの AAA ドメイン ストリッピングの機能情報，108 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

サーバ グループ レベルでの AAA ドメイン ストリッピングに関する情報

radius-server domain-stripping コマンドを使用して、グローバル レベルで受信したユーザ名からドメイン名を削除できます。**radius-server domain-stripping** コマンドを設定すると、「user@example.com」を含むすべての AAA 要求のユーザ名が「user」に再フォーマットされてリモート RADIUS サーバに送信されます。ドメイン名は要求から削除されます。

（注） ドメイン ストリッピングは TACACS 設定では行われません。

AAA ブロードキャスト アカウンティング機能を有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、プライベートおよびパブリック AAA サーバにアカウント情報を送信できます。この機能では、音声アプリケーションによる課金情報も提供されます。

サーバ グループ RADIUS コンフィギュレーション モードで **domain-stripping** コマンドを使用すると、ドメイン ストリッピングをサーバ グループ レベルで設定できます。サーバ単位のグループ コンフィギュレーションはグローバル コンフィギュレーションを上書きします。ドメイン ストリッピングが、グローバルではイネーブルではないがサーバ グループでイネーブルになっている場合、そのサーバ グループに対してのみイネーブルになります。また、Virtual Routing and Forwarding（VRF）固有のドメイン ストリッピングがグローバルで設定されていて、別の VRF のドメイン ストリッピングがサーバ グループで設定されている場合、ドメイン ストリッピングは両方の VRF でイネーブルになります。VRF の設定は、サーバグループ コンフィギュレーション モードから取得されます。サーバグループ コンフィギュレーションがグローバル コンフィギュレーション モードでディセーブルになっているが、サーバ グループ コンフィギュレーション モードで使用可能である場合、サーバグループ コンフィギュレーション モードでのすべての設定が適用可能です。

ドメイン ストリッピングおよびブロードキャスト アカウンティングを設定した後で、設定ごとに別個のアカウンティング レコードを作成できます。

サーバ レベル グループでの AAA ドメイン ストリッピングの設定方法

サーバ グループ レベルでのドメイン ストリッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *server-name*
5. **domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa group server radius** *server-name* 例： `Device(config)# aaa group server radius rad1`	RADIUS サーバを追加し、サーバ グループ RADIUS コンフィギュレーション モードを開始します。 • *server-name* 引数には、RADIUS サーバ グループ名を指定します。
ステップ 5	**domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*]	サーバ グループ レベルでドメイン ストリッピングを設定します。

	コマンドまたはアクション	目的
	例： `Device(config-sg-radius)# domain-stripping delimiter username@example.com`	
ステップ 6	**end** 例： `Device(config-sg-radius)# end`	サーバ グループ RADIUS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サーバ グループ レベルでの AAA ドメイン ストリッピングの設定例

例：サーバ グループ レベルでの AAA ドメイン ストリッピング

次に、サーバ グループ レベルでのドメイン ストリッピング設定の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# domain-stripping right-to-left delimiter @$/
Device(config-sg-radius)# end
```

その他の参考資料

ここでは、認証の設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
許可	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring Authorization」
アカウンティング	『*Cisco IOS XE Security Configuration Guide: Securing User Service* , Release 2』の「Configuring Accounting」

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1334	PPP 認証プロトコル
RFC 2433	「Microsoft PPP CHAP Extensions」
RFC 2903	「*Generic AAA Architecture*」
RFC 2904	「*AAA Authorization Framework*」
RFC 2906	「*AAA Authorization Requirements*」
RFC 2989	「*Criteria for Evaluating AAA Protocols for Network Access*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

サーバ グループ レベルでの AAA ドメイン ストリッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *17*：サーバ グループ レベルでの *AAA* ドメイン ストリッピングの機能情報

機能名	リリース	機能情報
サーバ グループ レベルでの AAA ドメイン ストリッピング	Cisco IOS XE Release 3.4S	サーバ グループ レベルでの AAA ドメインストリッピング機能を使用すると、ドメインストリッピングをサーバグループ レベルで設定できます。 次のコマンドが導入されました。**domain-stripping**。

第 6 章

AAA Double Authentication Secured by Absolute Timeout

AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。この機能は、サービス プロバイダーにより認可されたネットワークへの接続を最適化し、不要なセッションが接続されないようにすることで、ネットワークへのアクセス全体のセキュリティを高めます。

- 機能情報の確認，109 ページ
- AAA Double Authentication Secured by Absolute Timeout の前提条件，110 ページ
- AAA Double Authentication Secured by Absolute Timeout の制約事項，110 ページ
- AAA Double Authentication Secured by AbsoluteTimeout に関する情報，110 ページ
- AAA Double Authentication Secured by Absolute Timeout の適用方法，111 ページ
- AAA Double Authentication Secured by Absolute Timeout の設定例，111 ページ
- その他の参考資料，114 ページ
- AAA Double Authentication Secured by AbsoluteTimeout の機能情報，115 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA Double Authentication Secured by Absolute Timeout の前提条件

- Cisco RADIUS サーバまたは TACACS+ サーバにアクセスできる必要があります。また、RADIUS または TACACS+ の設定方法を十分に理解していることが必要です。
- 認証、許可、アカウンティング（AAA）の設定方法および AAA 自動二重認証の有効化方法を十分理解していることが必要です。

AAA Double Authentication Secured by Absolute Timeout の制約事項

- AAA Double Authentication Secured by Absolute Timeout 機能は、PPP 接続専用です。自動二重認証は、X.25 やシリアル ライン インターネット プロトコル（SLIP）などの他のプロトコルとともに使用することはできません。
- TACACS+ サーバが使用されている場合、パフォーマンスにわずかに影響することがあります。ただし、RADIUS サーバが使用されている場合は、パフォーマンスへの影響はありません。

AAA Double Authentication Secured by AbsoluteTimeout に関する情報

AAA 二重認証

ホストのユーザ名とパスワードを使用して最初の認証を渡すために、AAA 二重認証メカニズムを使用します。2 回目の認証は、チャレンジ ハンドシェイク認証プロトコル（CHAP）またはパスワード認証プロトコル（PAP）認証の後で行われますが、このときはログイン ユーザ名とそのパスワードが使用されます。最初の認証では、PPPセッションタイムアウトがローカルまたはリモートで設定されていれば、PPPセッションタイムアウトがバーチャルアクセスインターフェイスに適用されます。

AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。ユーザ単位のセッション タイムアウトは、一般的な絶対タイムアウト値よりも優先されるほか、カスタマイズすることが可能です。このメカニズムの動作原理は、二重認証のユーザ単位のアクセス コントロール リスト（ACL）と同じです。

AAA Double Authentication Secured by Absolute Timeout の適用方法

AAA Double Authentication Secured by Absolute Timeout の適用

絶対タイムアウトを適用するために、リンク コントロール プロトコル（LCP）のユーザ単位の属性としてログイン ユーザ プロファイルでセッション タイムアウトを設定する必要があります。AAA 二重認証を有効にするには、**access-profile** コマンドを使用します。このコマンドは、PPP セッション中にインターフェイスにユーザ単位の認可属性を適用するために使用されます。**access-profile** コマンドを使用する前に、LCP のユーザ単位の属性（セッション タイムアウトなど）を再度認可してから、ネットワーク制御プロトコル（NCP）を再度認可して、ACL やルートなどの他の必要な条件を適用します。「AAA Double Authentication Secured by Absolute Timeout の例」を参照してください。

（注） TACACS+ ユーザ プロファイルのタイムアウト設定は、RADIUS ユーザ プロファイルの設定とは異なります。RADIUS プロファイルでは、autocommand の **access-profile** とともに 1 つのセッション タイムアウトだけが設定されています。このタイムアウトは EXEC セッションおよび PPP セッションにそれぞれ適用されます。TACACS+ では、タイムアウトはサービス タイプ「exec」および「ppp」（LCP）下で設定し、EXEC セッションと PPP セッションに適用する必要があります。タイムアウトをサービス タイプ「ppp」下でのみ設定すると、そのタイムアウト値は EXEC 認可で使用できず、EXEC セッションに適用されません。

AAA Double Authentication Secured by Absolute Timeout の設定例

例：RADIUS ユーザ プロファイル

次の出力例は、RADIUS ユーザ プロファイルが適用されていることと、AAA 二重認証が絶対タイムアウトによって保護されていることを示しています。

```
aaapbx2 Password = "password1",
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Session-Timeout = 180,
 Idle-Timeout = 180000,
 cisco-avpair = "ip:inacl#1=permit tcp any any eq telnet"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_default Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile",
```

```
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_merge Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile merge",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
broker_replace Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile replace",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
```

例：TACACS ユーザ プロファイル

次の出力例は、TACACS+ ユーザ プロファイルが適用されていることと、AAA 二重認証が絶対タイムアウトによって保護されていることを示しています。

リモート ホスト認証

次に、最初の段階の認証でリモート ホストがローカル ホストによって認証され、リモート ホストの認可プロファイルが提供される例を示します。

```
user = aaapbx2
 chap = cleartext Cisco
 pap = cleartext cisco
 login = cleartext cisco
 service = ppp protocol = lcp
  idletime = 3000
  timeout = 3
 service = ppp protocol = ip
  inacl#1="permit tcp any any eq telnet"
 service = ppp protocol = ipx
```

引数のない access-profile コマンドの使用

引数を何も付けずに **access-profile** コマンドを実行すると、古い設定（ユーザ単位およびインターフェイス単位）で見つかったアクセスリストがすべて削除され、アクセスリストの定義のみが新しいプロファイルに存在する状態になります。

```
user = broker_default
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile"
! This is the autocommand that executes when broker_default logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
```

```
! installed prior to the creation of this user profile)!
  inacl#1="permit tcp any any"
  inacl#2="permit icmp host 10.0.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

merge キーワードを指定した access-profile コマンドの使用

access-profile コマンドの **merge** キーワードを使用して、すべての古いアクセス リストを削除すると、属性と値（AV）のペアのアップロードおよびインストールが許可されます。**merge** キーワードを使用すると、カスタムのスタティック ルート、Service Advertisement Protocol（SAP）フィルタ、プロファイルに必要になることがある他の要件をアップロードできます。**merge** キーワードは競合する設定のあらゆる要素を未処理のままにするため、注意して設定してください。

```
user = broker_merge
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile merge"
! This is the autocommand that executes when broker_merge logs in.
  timeout = 6
 service = ppp protocol = lcp
 timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.4.0.0 255.0.0.0"
  route#2="10.5.0.0 255.0.0.0"
  route#3="10.6.0.0 255.0.0.0"
  inacl#5="permit tcp any any"
  inacl#6="permit icmp host 10.60.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

replace キーワードを指定した access-profile コマンドの使用

access-profile コマンドに **replace** キーワードを指定して実行すると、古い設定がすべて削除され、新しい設定がインストールされます。

（注） **access-profile** コマンドを設定すると、アドレス プールとアドレスと AV のペアについて新しい設定がチェックされます。この時点でアドレスは再ネゴシエートできないため、このコマンドはそのようなアドレスと AV のペアを検出すると正常に動作しません。

```
user = broker_replace
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile replace"
! This is the autocommand that executes when broker_replace logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
```

```
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.7.0.0 255.0.0.0"
  route#2="10.8.0.0 255.0.0.0"
  route#3="10.9.0.0 255.0.0.0"
  inacl#4="permit tcp any any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

（注） TACACS+ ユーザ プロファイルのタイムアウト設定は、RADIUS ユーザ プロファイルの設定とは異なります。RADIUS プロファイルでは、autocommand の **access-profile** とともに 1 つのセッション タイムアウトだけが設定されています。このタイムアウトは EXEC セッションおよび PPP セッションに適用されます。TACACS+ ユーザ プロファイルでは、タイムアウトはサービス タイプ「exec」および「ppp」（LCP）下で設定し、EXEC セッションと PPP セッションにそれぞれ適用する必要があります。タイムアウトをサービス タイプ「ppp」下でのみ設定すると、そのタイムアウト値は EXEC 認可で使用できず、EXEC セッションに適用されません。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AAA Double Authentication Secured by AbsoluteTimeout の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *18*：*AAA Double Authentication Secured by AbsoluteTimeout* の機能情報

機能名	リリース	機能情報
AAA Double Authentication Secured by Absolute Timeout		AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。この機能では、サービス プロバイダーによるネットワークへの接続を認可された接続のみに最適化し、不要なセッションが接続されないようにすることで、ネットワークへのアクセス全体のセキュリティを高めます。

第 7 章

AAA RADIUS レコードのスロットリング

Throttling of AAA (RADIUS) Records 機能は、RADIUS サーバに送信されるアクセス（認証および認可）およびアカウンティング レコードのスロットリングをサポートします。この機能により、ユーザは ルータから RADIUS サーバに対して生成されるレコードの突然のバーストへの対応に十分な帯域幅がない場合などに、適切なスロットリング レートを設定して、ネットワークの輻輳や不安定さを防ぐことができます。

- 機能情報の確認，117 ページ
- AAA RADIUS レコードのスロットリングに関する情報，118 ページ
- AAA RADIUS レコードのスロットリングの設定方法，119 ページ
- AAA RADIUS レコードのスロットリングの設定例，122 ページ
- その他の参考資料，123 ページ
- AAA RADIUS レコードのスロットリングの機能情報，124 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA RADIUS レコードのスロットリングに関する情報

AAA RADIUS レコードのスロットリング機能の利点

RADIUS クライアントとして機能するネットワーク アクセス サーバ（NAS）は、アカウンティングまたはアクセス要求のバーストを生成し、重大なネットワーク輻輳を生じさせたり、RADIUS サーバに RADIUS トラフィックのバーストによる過負荷を生じさせる場合があります。複数の NAS で RADIUS サーバとのやり取りがあると、この問題が悪化する可能性があります。

次の条件は、RADIUS トラフィックの突然のバーストをトリガーします。

- すべての加入者セッションを順にダウン状態にし、各加入者へのアカウンティング要求を生成するインターフェイス フラップ。
- 前項で説明されているシナリオなど、スイッチオーバーで停止しなかったすべてのセッションに開始レコードを生成する ハイアベイラビリティ（HA）プログラム。

帯域幅が不十分であったり、RADIUS サーバの応答が遅い場合に、多数の要求が生成されると、ネットワークが不安定になる場合があります。ユーザデータグラムプロトコル（UDP）トランスポート層および RADIUS プロトコルには、フロー制御メカニズムがありません。この機能で提供されるスロットリング メカニズムは、これらの問題へのソリューションを提供します。

スロットリング アクセス要求とアカウンティング レコード

Throttling of AAA (RADIUS) Records 機能には、NAS レベルでパケットを制御するメカニズム（フロー制御）が導入されています。これにより、RADIUS サーバのパフォーマンスが向上しました。

特定の用途があるため、アクセス要求とアカウンティング レコードは別々に処理する必要があります。アクセス要求パケットは時間依存ですが、アカウンティング レコードパケットは時間依存ではありません。

- アクセス要求への応答が適切なタイミングでクライアントに返されない場合、プロトコルまたはユーザはタイムアウトし、デバイスの伝送レートが影響を受けます。
- アカウンティング レコード パケットは、リアルタイム クリティカルではありません。

同じサーバでしきい値を設定する場合、時間依存のアクセス要求パケットを扱うしきい値を優先し、アカウンティング レコード パケットにはより低次のしきい値を配置することが重要です。

インターネット サービス プロバイダー（ISP）がアクセス要求とアカウンティング レコードに個別の RADIUS サーバを使用していて、アカウンティング レコードのスロットリングのみが必要な場合もあります。

変更点

- Throttling of AAA (RADIUS) Records は、デフォルトではディセーブルです。

- スロットリング機能は、グローバルにまたはサーバ グループ レベルで設定できます。

AAA RADIUS レコードのスロットリングの設定方法

ここでは、グローバルおよびサーバ グループの両方の RADIUS サーバに送信されるアクセス（認証および認可）およびアカウンティング レコードのスロットリングを設定する方法について説明します。

server-group コンフィギュレーションは、特定のサーバ グループのスロットリングのイネーブル化またはディセーブル化、およびそのサーバ グループのしきい値の指定に使用されます。

（注） server-group コンフィギュレーションは、設定された任意のグローバル コンフィギュレーションを上書きします。

アカウンティングおよびアクセス要求パケットのグローバルなスロットリング

アカウンティングおよびアクセス要求パケットのグローバルなスロットリングを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-serverthrottle{accounting***threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**radius-serverthrottle**{**accounting***threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]} 例： `Router(config)# radius-server throttle accounting 100 access 200 access-timeout 2`	アカウンティングおよびアクセス要求パケットにグローバルなスロットリングを設定します。 この例では次のようになります。 • アカウンティングのしきい値（範囲は 0 ～ 65536）を 100 に、アクセスのしきい値を 200 に設定します。 （注） デフォルトのしきい値は 0 です（スロットリングはディセーブル）。 • トランザクションごとのタイムアウト回数の値（範囲は 1 ～ 10）を 2 に設定します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

サーバグループごとのアカウンティングおよびアクセス要求パケットのスロットリング

次の server-group コンフィギュレーションは、指定されたサーバ グループのイネーブル化またはディセーブル化、およびそのサーバ グループへのしきい値の指定に使用できます。

server-groupアカウンティングおよびアクセス要求パケットのスロットリングを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaagroupserverradius***server-group-name*
4. **throttle** {[**accounting***threshold*] [**access***threshold* [**access-timeout***number-of-timeouts*]]}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaagroupserverradius***server-group-name* 例： `Device(config)# aaa group server radius myservergroup`	server-group コンフィギュレーション モードを開始します。
ステップ 4	**throttle** {[**accounting***threshold*] [**access***threshold* [**access-timeout***number-of-timeouts*]]} 例： `Device(config-sg-radius)# throttle accounting 100 access 200 access-timeout 2`	アカウンティングおよびアクセス要求パケットに指定された server-group のスロットリング値を設定します。 この例では次のようになります。 • アカウンティングのしきい値（範囲は 0 ～ 65536）を 100 に、アクセスのしきい値を 200 に設定します。 （注） デフォルトのしきい値は 0 です（スロットリングはディセーブル）。 • トランザクションごとのタイムアウト回数の値（範囲は 1 ～ 10）を 2 に設定します。
ステップ 5	**exit** 例： `Device(config-sg-radius)# exit`	server-group コンフィギュレーション モードを終了します。

AAA RADIUS レコードのスロットリングの設定例

アカウンティングおよびアクセス要求パケットのグローバルなスロットリングの例

次に、サーバに送信するアカウンティング要求の回数を 100 に制限する方法の例を示します。

```
enable
configure terminal
radius-server throttle accounting 100
```

次に、サーバに送信するアクセス要求パケットの回数を 200 に制限し、トランザクションごとに許可されるタイムアウトの回数を 2 に設定する方法の例を示します。

```
enable
configure terminal
radius-server throttle access 200
radius-server throttle access 200 access-timeout 2
```

次に、アカウンティングおよびアクセス要求パケットの両方のスロットリングを設定する例を示します。

```
enable
configure terminal
radius-server throttle accounting 100 access 200
```

サーバグループごとのアカウンティングおよびアクセス要求パケットのスロットリングの例

次に、server-group-A に送信するアカウンティング要求の回数を 100 に制限する方法の例を示します。

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100
```

次に、server-group-A に送信するアクセス要求パケットの回数を 200 に制限し、トランザクションごとに許可されるタイムアウトの回数を 2 に設定する方法の例を示します。

```
enable
configure terminal
aaa group server radius server-group-A
throttle access 200 access-timeout 2
```

次に、server-group-A のアカウンティングおよびアクセス要求パケットの両方のスロットリングを設定する例を示します。

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100 access 200
```

その他の参考資料

ここでは、Throttling of AAA (RADIUS) Records 機能に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

AAA RADIUS レコードのスロットリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *19* : ***AAA***（***RADIUS***）レコードのスロットリングの機能情報

機能名	リリース	機能情報
AAA（RADIUS）レコードのスロットリング	Cisco IOS XE Release 2.1	Throttling of AAA (RADIUS) Records 機能は、RADIUS サーバに送信されるアクセス（認証および認可）およびアカウンティング レコードのスロットリングをサポートします。この機能により、ユーザは Cisco IOS XE ルータから RADIUS サーバに対して生成されるレコードの突然のバーストへの対応に十分な帯域幅がない場合などに、適切なスロットリングレートを設定して、ネットワークの輻輳や不安定さを防ぐことができます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドがこの機能で導入または変更されました。**radius-serverthrottle**、**throttle**

第 8 章

RADIUS パケット オブ ディスコネクト

RADIUS パケット オブ ディスコネクト機能は、接続された音声コールを終了させるために使用します。

- 機能情報の確認，127 ページ
- RADIUS パケット オブ ディスコネクトの前提条件，128 ページ
- RADIUS パケット オブ ディスコネクトの制約事項，128 ページ
- RADIUS パケット オブ ディスコネクトに関する情報，128 ページ
- RADIUS パケット オブ ディスコネクトの設定方法，129 ページ
- その他の参考資料，132 ページ
- RADIUS パケット オブ ディスコネクトの機能情報，134 ページ
- 用語集，135 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

RADIUS パケット オブ ディスコネクトの前提条件

『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』で説明されているように、AAA を設定します。

RADIUS パケット オブ ディスコネクトの制約事項

以下により、適切に一致する識別情報の通知が行われる必要があります。

- 課金サーバとゲートウェイの設定
- ゲートウェイのオリジナル アカウンティング開始要求
- サーバの POD 要求

RADIUS パケット オブ ディスコネクトに関する情報

パケット オブ ディスコネクト（PoD）は RADIUS access_request パケットであり、RADIUS access_accept パケットによりセッションが承認された後、認証するエージェント サーバがユーザを接続解除するときに使用されるようになっています。

POD が必要な場合

POD が必要な場合としては、少なくとも次の 2 つの状況が考えられます。

- 不正使用の検出。これは、コールを承認後でなければ実行できません。価格構造が複雑でコールを受け入れる前に最大セッション期間を推定できない。ある種のディスカウントが適用されるか、複数のユーザが同じサブスクリプションを同時に使用している場合が、これに当てはまります。
- 認可されていないサーバからユーザが切断されるのを防ぐには、PODパケットを発行する認可エージェントが パケット オブ ディスコネクト要求に 3 つのパラメータを含める必要があります。接続解除されるコールに対して、すべてのパラメータは、ゲートウェイの期待値と一致している必要があります。パラメータが一致しないと、ゲートウェイはパケット オブ ディスコネクトのパケットを破棄し、エージェントにNACK（否定応答）メッセージを送信します。

POD パラメータ

POD には次のパラメータがあります。

- このコールに対してゲートウェイから受信されたものと同じ内容の h323-conf-id ベンダー固有属性（VSA）
- 対象の区間に対してゲートウェイから受信されたものと同じ内容の h323-call-origin VSA。
- POD 要求の *authentication* フィールドで伝送される 16 バイトの MD5 ハッシュ値。
- Cisco IOS XE ソフトウェアは、RFC 3576 の『*Dynamic Authorization Extensions to RADIUS*』（POD を介してサポートされるディスコネクト メッセージ（DM）および認可変更（CoA）の両方を公式にサポートするために RADIUS 標準を拡張）に基づいて POD コード 50 を音声 POD 要求のコード値として割り当てます。

RFC 3576 では、以下の POD コードを指定します。

-
  - 40：切断要求
  - 41：切断：ACK
  - 42：切断：NAK
  - 43：CoA 要求
  - 44：CoA-ACK
  - 45：CoA-NAK

RADIUS パケット オブ ディスコネクトの設定方法

RADIUS POD の設定

次のタスクを使用して、RADIUS POD を設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string*
4. Router# **end**
5. Router# **show running-configuration**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string*
	
	例：
	
	`Router(config)#` **aaa pod server server-key xyz123**
		次のような特定のセッション属性が提供されると、インバウンド ユーザ セッションを切断できます。
		
		• **port***port-number*：（任意）POD 要求に使用されるネットワーク アクセス サーバのユーザデータグラム プロトコル（UDP）ポート。デフォルト値は 1700 です。
		
		• **auth-type**：（任意）セッションの切断に必要な認証の種類。
		
		  • **any**：POD パケット内で送信されたすべての属性と一致するセッションが切断されます。POD パケットには、4 つのキー属性（user-name、framed-IP-address、session-ID、session-key）の 1 つまたは複数が含まれることがあります。
		
		  • **all**：4 つの主要属性のすべてに一致するセッションだけが切断されます。**all** はデフォルトです。
		
		  • **session-key**：一致する session-key 属性を持つセッションが切断されます。他のすべての属性は無視されます。
		
		• **server-key**：共有秘密テキスト ストリングを設定します。
		
		• *encryption-type*：（任意）直後のテキストが暗号化されるかどうか、および暗号化される場合は使用される暗号化タイプを定義する 1 桁の数字。定義されている暗号化タイプは、0（直後のテキストは暗号化されない）および7（テキストはシスコが定義した暗号化アルゴリズムを使用して暗号化される）です。
		
		• *string*：ネットワーク アクセス サーバとクライアント ワークステーション間で共有される事前共有キー。この事前共有キーは、両方のシステムで同じである必要があります。

	コマンドまたはアクション	目的
ステップ 4	Router# **end**	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 5	Router# **show running-configuration**
	
	例：
	`Router#` **show running-configuration**
	
	例：
	`!`
	
	例：
	`aaa authentication login h323 group radius`
	
	例：
	`aaa authorization exec h323 group radius`
	
	例：
	`aaa accounting update newinfo`
	
	例：
	`aaa accounting connection h323 start-stop group radius`
	
	例：
	`aaa pod server server-key cisco`
	
	例：
	`aaa session-id common`
	
	例：
	`!`
		ゲートウェイが特権EXECモードで正しく設定されていることを確認します。

トラブルシューティングのヒント

AAA Dead-Server Detection を設定したら、**show running-config** コマンドを使用して、その設定を確認してください。この確認が特に重要になるのは、**no** 形式の **radius-server dead-criteria** コマンドを使用している場合です。**show running-config** コマンドの出力は、**radius-server dead-criteria** コマンドを使用して設定した「Dead Criteria Details」フィールドと同じ値を示している必要があります。

RADIUS POD の設定の確認

RADIUS POD 設定を確認するには、次の例に示すように **show running configuration** 特権 EXEC コマンドを使用します。

```
Router# show running-configuration
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting update newinfo
aaa accounting connection h323 start-stop group radius
aaa pod server server-key cisco
aaa session-id common
.
.
.
```

その他の参考資料

次の項で、RADIUS パケット オブ ディスコネクト機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA	『*Cisco IOS XE Security Configuration Guide, Securing User Services*, Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
CLI Configuration	『*Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『*Remote Authentication Dial-in User Service*』
RFC 3576	『*Dynamic Authorization Extensions to RADIUS*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS パケット オブ ディスコネクトの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *20*：***RADIUS*** パケット オブ ディスコネクトの機能情報

機能名	リリース	機能情報
RADIUS パケット オブ ディスコネクト	Cisco IOS XE Release 2.1	RADIUS パケット オブ ディスコネクト機能は、接続された音声コールを終了させるために使用します。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービスルータに導入されました。 次のコマンドが導入または変更されました。**aaapodserver**、**debugaaapod**。

用語集

AAA：認証、許可、アカウンティング。セキュリティ サービスのフレームワークであり、ユーザの身元確認（認証）、リモートアクセスコントロール（許可）、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信（アカウンティング）の方式を定めています。

L2TP：Layer 2 Tunnel Protocol。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

PE：プロバイダー エッジ。サービス プロバイダー ネットワークのエッジ上のネットワーキング デバイス。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：バーチャル プライベート ネットワーク リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

VRF：Virtual Route Forwarding。最初は、ルータにグローバルのデフォルト ルーティング/フォワーディング テーブルは 1 つしかありません。VRF は、複数の分離されたルーティング/フォワーディ

ング テーブルとして表示でき、ユーザのルートには別のユーザのルートとの相互関係はありません。

第 9 章

AAA 認可および AAA 認証のキャッシュ

AAA 認可キャッシュ機能および AAA 認証のキャッシュ機能を使用すると、設定した一連のユーザ プロファイルまたはサービス プロファイルの認可応答と認証応答をキャッシュに格納することができます。このため、認可応答および認証応答から返されるユーザ プロファイルとサービス プロファイルを複数のソースから照会できるようになり、オフロード サーバだけに依存する必要がなくなるので、パフォーマンスとネットワークの信頼性レベルが向上します。また、この機能のフェールオーバー メカニズムにより、ネットワークの RADIUS サーバまたは TACACS+ サーバが認可応答や認証応答を返せなくなっても、ネットワークのユーザや管理者は引き続きネットワークにアクセスできます。

- 機能情報の確認，137 ページ
- 認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の前提条件，138 ページ
- 認可プロファイルおよび認証プロファイルのキャッシュ機能の実装について，138 ページ
- 認可プロファイルおよび認証プロファイルのキャッシュ機能の実装方法，141 ページ
- 認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための設定例，147 ページ
- RADIUS 認可変更に関する追加情報，150 ページ
- 認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の機能情報，151 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の前提条件

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装には、次の前提条件が適用されます。

- プロファイル キャッシュ機能の実装方法を理解している必要があります。つまり、ネットワークのパフォーマンス向上させたり、ネットワークの認証（RADIUS）サーバや認可（TACACS+）サーバが使用できなくなった場合にフェールオーバーを実行したりするためにプロファイルがどのようにキャッシュされるかを理解している必要があります。
- RADIUS サーバ グループと TACACS+ サーバ グループがすでに設定されている必要があります。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装について

認可プロファイルおよび認証プロファイルのキャッシュ機能によるネットワーク パフォーマンスの最適化

RADIUS クライアントおよび TACACS+ クライアントは Cisco ルータ上で稼働し、ユーザ認証およびネットワーク サービス アクセスに関するすべての情報を保持する中央の RADIUS サーバまたは TACACS+ サーバへ認証要求を送信します。ルータはオフロードの RADIUS サーバまたは TACACS+ サーバと通信してコールを認証した後、ポリシーまたはサービスをそのコールに適用する必要があります。認証、許可、アカウンティング（AAA）アカウンティングと異なり、AAA 認証および AAA 認可はブロッキング手順です。つまり、コールの認証中および認可中は、コール セットアップは進行しません。したがって、そのような認証要求または認可要求が、ルータから RADIUS オフロード サーバまたは TACACS+ サーバに渡されて処理される時間と、そのサーバからルータに渡されて処理される時間は、コール セットアップの処理に必要な時間に直に影響します。転送中の通信の問題、オフロードサーバの利用率、その他のさまざまな要因が、コールセットアップのパフォーマンスを大幅に低下させるのは、AAA 認証および AAA 認可の手順に原因があります。この問題がさらに顕著になるのは、複数の AAA 認証および AAA 認可が 1 つのコールまたはセッションに必要になるときです。

この問題の解決策は、そのような認証要求の影響を最小限にすることです。そのために、ルータで特定のユーザの認証応答および認可応答をキャッシュに格納して、要求をオフロード サーバに

何度も送信する必要をなくします。このプロファイルキャッシュ機能により、コールセットアップ時間が大幅に短縮されます。また、プロファイル キャッシュ機能によってネットワークの信頼性レベルが上がります。これは、認証応答および認可応答から返されるユーザ プロファイルやサービスプロファイルを複数のソースから照会できるようになり、オフロードサーバだけに依存する必要がなくなるためです。

このようにパフォーマンスを最適化するためには、ユーザがルータから認証されるときに AAA キャッシュ プロファイルが最初に照会されるように認証方式リストを設定する必要があります。詳細については、「認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト」を参照してください。

フェールオーバーメカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能

何らかの理由で、RADIUS サーバまたは TACACS+ サーバが認証応答および認可応答を返せない場合、ネットワークのユーザおよび管理者はネットワークから締め出されることがあります。プロファイルのキャッシング機能により、認証フェーズを完了しなくてもユーザ名の承認が可能になります。たとえば、ユーザ名が user100@example.com でパスワードが secretpassword1 のユーザは、正規表現「.*@example.com」を使用してプロファイル キャッシュに格納されます。ユーザ名が user101@example.com で、パスワードが secretpassword2 である別のユーザもまた、同じ正規表現を使用して格納できます。「.*@example.com」プロファイルのユーザの数が何千にもなる可能性があるため、個人のパスワードを使用して各ユーザの認証を行うのは現実的ではありません。このため、認証はディセーブル化され、各ユーザは単にキャッシュに格納されている共通のアクセス応答の認証プロファイルにアクセスします。

Challenge Handshake Authentication Protocol（CHAP）、Microsoft チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）、または拡張認証プロトコル（EAP）などの、クライアントと AAA オフロードサーバの間で暗号化されたパスワードを使用する高度なセキュリティ メカニズムを使用する場合に、同じ理論が当てはまります。認証プロファイルを処理するために、これらの一意で、安全なユーザ名とパスワードのプロファイルを許可するには、認証をバイパスします。

このフェールオーバー機能を利用するためには、ユーザがルータから認証されるときにキャッシュ サーバ グループが最後に照会されるように認証および認可の方式リストを設定する必要があります。詳細については、「認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト」を参照してください。

認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト

方式リストとは、ユーザ認証のために照会される認証方式を記載したシーケンシャル リストです。サポートされているのは、ローカル（ローカルのデータベースを使用）、なし（なにも実行しない）、RADIUS サーバ グループ、または TACACS+ サーバ グループなどの方式です。通常は、複数の方式を方式リストに設定できます。 ソフトウェアは、ユーザを認証するため、リストに掲載されている最初の方式が使用されます。その方式で応答に失敗した場合、ソフトウェアは、

方式リストに掲載されている次の認証方式を選択します。この処理は、リストのいずれかの認証方式で正常に通信できるか、方式リストで定義されているすべての方式を試行するまで続行されます。

ネットワークのパフォーマンスを最適化したり、プロファイルキャッシング機能を使用してフェールオーバー機能を有効にするには、方式リストの認証および認可の方式の順序を変更します。ネットワーク パフォーマンスを最適化するためには、キャッシュ サーバ グループが方式リストで最初に検出されるようにします。フェールオーバー機能を有効にするためには、キャッシュ サーバ グループが方式リストで最後に検出されるようにします。

認可プロファイルおよび認証プロファイルのキャッシュ機能に関するガイドライン

特定のアクセス ポイント（POP）の特定のルータで、認証および認可を要求できるユーザ名とプロファイルの数は相当な数になることがあるため、ユーザ名とプロファイルをすべてキャッシュするのは現実的ではありません。このため、ユーザ名およびプロファイルのうち、一般的に使用されるものや、一般的な認証応答や認可応答を共有するものだけをキャッシングに使用するように設定する必要があります。ドメイン ベースのサービス プロファイルに加え、America Online（AOL）のコールに使用される aolip や aolnet などの一般的に使用されるユーザ名や、公衆電話交換網（PSTN）のコールを、ネットワークに接続されたストレージデバイスに接続するのに使用される事前認証の着信番号識別サービス（DNIS）番号はいずれも、認証および認可のキャッシュ機能の効果が現れるユーザ名とプロファイルの例です。

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための一般的な設定手順

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するには、次の手順を行います。

1. キャッシュ プロファイル グループを作成し、各グループのキャッシュに格納する情報についてのルールを定義します。

ユーザ名に正確に一致するエントリ、正規表現に一致するエントリ、またはすべての認証要求および認可要求をキャッシュに格納することを指定します。

1. 新しく定義したキャッシュ グループを参照するようにサーバ グループを更新します。
2. キャッシュに格納された情報を使用してネットワークのパフォーマンスを最適化したり、フェールオーバー メカニズムを有効にしたりするように認証または認可の方式リストを更新します。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装方法

キャッシュ プロファイル グループの作成とキャッシュ処理ルールの定義

次の作業を行って、キャッシュプロファイルグループを作成し、そのグループのキャッシュに格納する情報についてのルールを定義して、キャッシュ プロファイルのエントリの確認と管理を行います。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaacacheprofile***group-name*
5. **profile***name*[**no-auth**]
6. 手順 4 のプロファイル グループに追加する各ユーザ名に対して手順 5 を繰り返します。
7. **regexp***matchexpression*{**any**| **only**}[**no-auth**]
8. 手順 4 で定義されたキャッシュ プロファイル グループに追加する各正規表現に対して手順 7 を繰り返します。
9. **all**[**no-auth**]
10. **end**
11. **showaaacachegroup***name*
12. **clearaaacachegroup***name*{**profile** *name*| **all**}
13. **debugaaacachegroup**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	AAA アクセスコントロールモデルをイネーブルにします。
ステップ 4	**aaacacheprofile***group-name* 例： `Router(config)# aaa cache profile networkusers@companyname`	認証および認可のキャッシュ プロファイル サーバ グループを定義し、プロファイルマップコンフィギュレーションモードを開始します。
ステップ 5	**profile***name*[**no-auth**] 例： `Router(config-profile-map# profile networkuser1 no-auth`	ユーザ名の一致に基づいて個々の認証および認可プロファイルのキャッシュを作成します。 • *name* 引数は、認証または認可のサービス要求によって照会されるユーザ名と正確に一致する必要があります。 • **no-auth** キーワードを使用して、このユーザの認証をバイパスします。
ステップ 6	手順 4 のプロファイル グループに追加する各ユーザ名に対して手順 5 を繰り返します。	--
ステップ 7	**regexp***matchexpression*{**any**|**only**}[**no-auth**] 例： `Router(config-profile-map)# regexp .*@example.com any no-auth`	（任意）正規表現に基づいて、一致するエントリをキャッシュ プロファイル グループに作成します。 • **any** キーワードを使用すると、正規表現に一致する一意のユーザ名がすべて保存されます。 • **only** キーワードを使用すると、正規表現に一致するすべてのユーザ名に対して 1 つのプロファイルエントリのみがキャッシュされます。 • **no-auth** キーワードを使用して、このユーザまたは一連のユーザの認証をバイパスします。 • 正規表現のプロファイルグループ内のエントリの数が何千にもなる可能性があるため、そして各要求の検証を正規表現に対して行うと時間がかかる場合があるた

	コマンドまたはアクション	目的
		め、キャッシュ プロファイル グループで正規表現を使用することは推奨されません。
ステップ 8	手順4で定義されたキャッシュ プロファイル グループに追加する各正規表現に対して手順 7 を繰り返します。	--
ステップ 9	**all**[**no-auth**] 例： `Router(config-profile-map)# all no-auth`	（任意）認証要求および認可要求をすべてキャッシュに格納することを指定します。 • **all** コマンドは、特定のサービス認可要求に対して使用しますが、認証要求を処理するときは使用しないでください。
ステップ 10	**end** 例： `Router(config-profile-map)# end`	特権 EXEC モードに戻ります。
ステップ 11	**showaaacachegroup***name* 例： `Router# show aaa cache group networkusers@companyname`	（任意）指定したグループのすべてのキャッシュ エントリを表示します。
ステップ 12	**clearaaacachegroup***name*{**profile** *name*| **all**} 例： `Router# clear aaa cache group networkusers@companyname profile networkuser1`	（任意）キャッシュの 1 つまたはすべてのエントリをクリアします。
ステップ 13	**debugaaacachegroup** 例： `Router# debug aaa cache group`	（任意）キャッシュに格納されているエントリのデバッグ情報を表示します。

キャッシュ プロファイル グループ情報を使用する RADIUS および TACACS サーバ グループの定義

このタスクを実行して、RADIUS および TACACS+ サーバ グループが各キャッシュ プロファイル グループに保存されている情報をどのように使用するかを定義します。

はじめる前に

RADIUS サーバ グループと TACACS+ サーバ グループが作成されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaagroupserverradius***group-name*or**aaa group server tacacs+** *group-name*
5. **cacheauthorizationprofile***name*
6. **cacheauthenticationprofile***name*
7. **cacheexpiry***hours*{**enforce failover**}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaagroupserverradius***group-name*or**aaa group server tacacs+** *group-name* 例： `Router(config)# aaa group server radius networkusers@companyname`	RADIUS サーバ グループ コンフィギュレーション モードを開始します。 • TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** *group-name* コマンドを使用します。
ステップ 5	**cacheauthorizationprofile***name* 例： `Router(config-sg-radius)# cache authorization profile networkusers@companyname`	この RADIUS または TACACS+ サーバ グループのプロファイルのネットワーク ユーザで認可のキャッシュ処理ルールをアクティブにします。 • このコマンドの *name* 引数は、AAA キャッシュ プロファイル グループ名です。
ステップ 6	**cacheauthenticationprofile***name* 例： `Router(config-sq-radius)# cache authentication profile networkusers@companyname`	この RADIUS または TACACS+ サーバ グループのプロファイルのネットワーク ユーザで認証のキャッシュ処理ルールをアクティブにします。
ステップ 7	**cacheexpiry***hours*{**enforce** **failover**} 例： `Router(config-sq-radius)# cache expiry 240 failover`	（オプション）キャッシュ プロファイルのエントリが期限切れになる（古くなる）までの時間を設定します。 • **enforce** キーワードは、期限切れになったキャッシュ プロファイルのエントリを再使用しないことを指定するときに使用します。 • **failover** キーワードは、他のすべての方式でユーザを認証および認可できなかった場合にキャッシュ プロファイルの期限切れのエントリを使用することを指定するときに使用します。
ステップ 8	**end** 例： `Router(config-sg-radius)# end`	特権 EXEC モードに戻ります。

キャッシュ情報の使用方法を指定するための認可および認証の方式リストの更新

次の作業を行って、認可および認証のキャッシュ情報を使用するように認可および認証の方式リストを更新します。

はじめる前に

方式リストをすでに定義している必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaauthorization** {**network** | **exec** | **commands** *level* | **reverse-access**| **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
5. **aaaauthenticationppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaaauthenticationlogin**{**default** | *list-name*} *method1* [*method2...*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaaauthorization** {**network** | **exec** | **commands** *level* | **reverse-access**| **configuration**} {**default** | *list-name*} [*method1* [*method2...*]] 例： `Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname`	AAA 認可を有効にし、指定した機能にユーザがアクセスしたときに使用される認可方式を定義する方式リストを作成します。
ステップ 5	**aaaauthenticationppp** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname`	PPP が実行されているシリアルインターフェイスで使用する 1 つまたは複数の認証方式を指定します。
ステップ 6	**aaaauthenticationlogin** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication login default cache adminusers group adminusers`	ログイン時の認証を設定します。
ステップ 7	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための設定例

ネットワークを最適化するための認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例

次の設定例について説明します。

- ネットワーク上のすべての管理者名を含むキャッシュ プロファイル グループ adminusers を定義し、すべてのログイン セッションと exec セッションに使用するデフォルトのリストとして設定します。
- RADIUS サーバ グループの新しいキャッシュ処理ルールをアクティブにします。
- 新しいキャッシュ プロファイル グループを認証および認可の方式リストに追加し、このキャッシュ プロファイル グループが最初に照会されるように方式の順序を変更します。

```
configure terminal
 aaa new-model
 ! Define aaa cache profile groups and the rules for what information is saved to cache.
 aaa cache profile admin_users
 profile adminuser1
 profile adminuser2
 profile adminuser3
 profile adminuser4
 profile adminuser5
 exit
 ! Define server groups that use the cache information in each profile group.
 aaa group server radius admins@companyname.com
 cache authorization profile admin_users
 cache authentication profile admin_users
 ! Update authentication and authorization method lists to specify how profile groups and
server groups are used.
 aaa authentication login default cache admins@companyname.com group admins@companyname.com
 aaa authorization exec default cache admins@companyname.com group admins@companyname.com
 end
```

フェールオーバーメカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例

次の設定例について説明します。

- RADIUS サーバまたは TACACS+ サーバが万一使用できなくなった場合でも、管理者が引き続きネットワークにアクセスできるように、ネットワーク上のすべての管理者を含むキャッシュ プロファイル グループ admin_users を作成します。
- RADIUS サーバまたは TACACS+ サーバが万一使用できなくなった場合でも、ABC という会社のユーザがネットワークの使用を認可されるように、ネットワーク上のこれらのユーザをすべて含むキャッシュ プロファイル グループ abc_users を作成します。

- RADIUS サーバの各プロファイル グループの新しいキャッシュ処理ルールをアクティブにします。
- 新しいキャッシュ プロファイル グループを認証および認可の方式リストに追加し、このキャッシュ プロファイル グループが最後に照会されるように方式の順序を変更します。

```
configure terminal
 aaa new-model
 ! Define aaa cache profile groups and the rules for what information is saved to cache.
 aaa cache profile admin_users
 profile admin1
 profile admin2
 profile admin3
 exit
 aaa cache profile abcusers
 profile .*@example.com only no-auth
 exit
 ! Define server groups that use the cache information in each cache profile group.
 aaa group server tacacs+ admins@companyname.com
 server 10.1.1.1
 server 10.20.1.1
 cache authentication profile admin_users
 cache authorization profile admin_users
 exit
 aaa group server radius abcusers@example.com
 server 172.16.1.1
 server 172.20.1.1
 cache authentication profile abcusers
 cache authorization profile abcusers
 exit
 ! Update authentication and authorization method lists to specify how cache is used.
 aaa authentication login default cache admins@companyname.com group admins@companyname.com
 aaa authorization exec default cache admins@companyname.com group admins@companyname.com
 aaa authentication ppp default group abcusers@example.com cache abcusers@example.com
 aaa authorization network default group abcusers@example.com cache abcusers@example.com
 end
```

RADIUS 認可変更に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA の設定	『認証、許可、アカウンティング コンフィギュレーション ガイド』

標準および RFC

標準/RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 5176	「*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *21*：認証プロファイルおよび認可プロファイルのキャッシュ機能の実装の機能情報

機能名	リリース	機能情報
AAA 認可および AAA 認証のキャッシュ	Cisco IOS XE Release 2.3	この機能により、ネットワークのパフォーマンスが最適化されるほか、RADIUS サーバまたは TACACS+ サーバが何らかの理由で使用できなくなった場合のフェールオーバー メカニズムが確立されます。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaaauthenticationlogin**、**aaaauthenticationppp**、**aaaauthorization**、**aaacacheprofile**、**all**（プロファイル マップ設定）、**cacheauthenticationprofile**（サーバ グループ設定）、**cacheauthorizationprofile**（サーバ グループ設定）、**cacheexpiry**（サーバ グループ設定）、**clearaaacachegroup**、**debugaaacachegroup**、**profile**（プロファイルマップ設定）、**regexp**（プロファイル マップ設定）、**showaaacachegroup**。

第 10 章

認可の設定

AAA 認可を使用すると、ユーザが利用できるサービスを制限できます。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバはユーザのプロファイルから取得した情報を使用して、ユーザの設定を設定します。このプロファイルは、ローカル ユーザ データベースまたはセキュリティ サーバにあります。認可が完了すると、ユーザ プロファイルの情報で許可されているサービスであれば、ユーザは要求したサービスに対するアクセス権を付与されます。

- 機能情報の確認，153 ページ
- AAA 認可の前提条件，154 ページ
- 認可の設定の概要，154 ページ
- 認可の設定方法，158 ページ
- 認可設定の例，162 ページ
- その他の参考資料，165 ページ
- 認可の設定に関する機能情報，166 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA 認可の前提条件

名前付き方式リストを使用して認証を設定する前に、まず、次のタスクを実行する必要があります。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- AAA 認証を設定します。一般的に、認可は認証後に実行し、認証が適切に動作することに依存します。AAA 認証の設定方法については、「認証の設定」モジュールを参照してください。
- RADIUS または TACACS+ 認可を発行している場合、RADIUS または TACACS+ セキュリティ サーバの特性を定義します。シスコのネットワーク アクセス サーバを設定して RADIUS セキュリティ サーバと通信する方法の詳細については、「Configuring RADIUS」の章を参照してください。シスコのネットワーク アクセス サーバを設定して TACACS+ セキュリティ サーバと通信する方法の詳細については、「Configuring TACACS+」モジュールを参照してください。
- ローカル認可を発行している場合、**username** コマンドを使用して、特定のユーザに関連付けられている権限を定義します。**username** コマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

認可の設定の概要

許可方式の指定リスト

許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、順に照会する認可方式（RADIUS または TACACS+ など）を記述した指定リストです。方式リストを使用すると、許可に使用するセキュリティ プロトコルを 1 つ以上指定できるため、最初の方式が失敗した場合のバックアップ システムを確保できます。Cisco IOS XE ソフトウェアでは、特定のネットワーク サービスについてユーザを許可するために最初の方式が使用されます。その方式が応答しない場合、リストの次の方式が選択されます。このプロセスは、リストのいずれかの認可方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の許可方式が試行されます。このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ サービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許可方式は試行されません。

方式リストは、要求した認可タイプに固有です。

- Commands：ユーザが実行する EXEC モード コマンドに適用されます。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- EXEC：ユーザ EXEC ターミナル セッションに関連付けられた属性に適用されます。
- Network：ネットワーク接続に適用されます。これには、PPP、SLIP、または ARAP 接続が含まれます。
- Reverse Access：リバース Telnet セッションに適用されます。

方式の指定リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。方式リストを指定せずに、特定の許可タイプ用の **aaa authorization** コマンドが発行されると、方式リストが明示的に定義されている場合を除いて、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます。（定義済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、デフォルトでローカル認可が実行されます。

AAA 認可方式

AAA は 5 種類の認可方式をサポートしています。

- TACACS+：ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと認可情報を交換します。TACACS+ 認可は、属性値ペアを関連付けることでユーザに特定の権限を定義します。属性ペアは適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。
- If-Authenticated：ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- None：ネットワーク アクセス サーバは、認可情報を要求しません。認可は、この回線/インターフェイスで実行されません。
- Local：ルータまたはアクセス サーバは、**username** コマンドの定義に従って、ローカル データベースに問い合わせて、たとえばユーザに固有の権限を認可します。ローカルデータベースを介して制御できるのは、一部の機能だけです。
- RADIUS：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの認可情報を要求します。RADIUS認可では、属性を関連付けることでユーザに固有の権限を定義します。属性は適切なユーザとともに RADIUS サーバ上のデータベースに保存されます。

（注） CSCuc32663 では、パスワードおよび認可ログは、TACACS+、LDAP、または RADIUS セキュリティ サーバへ送信される前にマスクされます。マスクされていない情報を TACACS+、LDAP、または RADIUS セキュリティ サーバに送信するには、**aaa authorization commands visible-keys** コマンドを使用します。

認可方式

ネットワーク アクセス サーバから TACACS+ セキュリティ サーバを介して認可情報を要求するには、**grouptacacs+***method* キーワードを指定して **aaaauthorization** コマンドを使用します。TACACS+ セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring TACACS+」の章を参照してください。TACACS+ サーバが、PPP や ARA などのネットワーク サービスの使用を認可できるようにする例については、「TACACS 認可の例」を参照してください。

ユーザが認証済みであれば、要求した機能へのアクセスを許可するには、**if-authenticated***method* キーワードを指定して **aaaauthorization** コマンドを使用します。この方式を選択する場合、すべての要求した機能は、認証済みユーザに自動的に許可されます。

特定のインターフェイスまたは回線から認可を実行したくない場合があります。指定した回線またはインターフェイスで認可動作を停止するには、**none***method* キーワードを使用します。この方式を選択すると、すべてのアクションについて認可はディセーブルになります。

ローカル認可を選択するには（つまり、ルータまたはアクセス サーバがローカル ユーザ データベースに問い合わせて、ユーザが使用可能な機能を決定する場合）、**local***method* キーワードを指定して **aaaauthorization** コマンドを使用します。ローカル認可に関連する機能は、**username** グローバルコンフィギュレーションコマンドを使用して定義します。許可されている機能のリストについては、「認証の設定」の章を参照してください。

ネットワーク アクセス サーバから RADIUS セキュリティ サーバを介して認可を要求するには、**radius***method* キーワードを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」の章を参照してください。

ネットワーク アクセス サーバから RADIUS セキュリティ サーバを介して認可情報を要求するには、**groupradius***method* キーワードを指定して **aaaauthorization** コマンドを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」の章を参照してください。RADIUS サーバがサービスを認可できるようにする例については、「RADIUS 認可の例」を参照してください。

（注） SLIP の認可方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、認可のデフォルト設定が適用されます。

方式リストとサーバ グループ

サーバ グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバ ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

サーバ グループを使用して、設定したサーバ ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバ グループを使用すると、R1 および R2 を別のサーバ グループとして定義し、T1 および T2 を別のサーバ グループとして定義できます。つまり、R1 と T1 を方式リストに指定できるか、または R2 と T2 を方式リストに指定できます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（認可など）に設定されている場合、設定されている 2 番めのホストエントリは最初のホストエントリのフェールオーバーバックアップとして動作します。この例の場合、最初のホストエントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループの設定および DNIS 番号に基づくサーバ グループの設定の詳細については、「Configuring RADIUS」または「Configuring TACACS+」の章を参照してください。

AAA 認可タイプ

Cisco IOS XE ソフトウェアは、5 種類の認可をサポートしています。

- Commands：ユーザが実行する EXEC モード コマンドに適用されます。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- EXEC：ユーザ EXEC ターミナル セッションに関連付けられた属性に適用されます。
- Network：ネットワーク接続に適用されます。これには、PPP、SLIP、または ARAP 接続が含まれます。
- Reverse Access：リバース Telnet セッションに適用されます。
- Configuration：AAA サーバからのコンフィギュレーションのダウンロードに適用されます。
- IP Mobile：IP モバイル サービスの認可に適用されます。

承認タイプ

名前付き認可方式リストは、指定される認可の種類によって変わります。

ユーザ別に固有のセキュリティ ポリシーを適用する認可をイネーブルにする方式リストを作成するには、auth-proxy キーワードを使用します。認証プロキシ機能の詳細については、このガイドの「Traffic Filtering and Firewalls」の部の「Configuring Authentication Proxy」を参照してください。

すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP などのプロトコル）について認可をイネーブルにする方式リストを作成するには、**network** キーワードを使用します。

ユーザが EXEC シェルを実行できるかどうかを認可で決定できるように方式リストを作成するには、**exec** キーワードを使用します。

特定の特権レベルに関連付けられた個々の EXEC コマンドについて認可をイネーブルにする方式リストを作成するには、**commands** キーワードを使用します。これにより、指定されたコマンドレベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

リバース Telnet 機能について認可をイネーブルにする方式リストを作成するには、**reverse-access** キーワードを使用します。

Cisco IOS XE ソフトウェアでサポートされている認可のタイプの詳細については、「AAA 認可タイプ」を参照してください。

認可の属性値ペア

RADIUS および TACACS+ の認可はいずれも、セキュリティ サーバのデータベースに保存されている属性を処理することで、ユーザに固有の権限を定義します。RADIUS と TACACS+ のいずれも、属性はセキュリティ サーバに定義され、ユーザに関連付けられ、ユーザの接続に適用されるネットワーク アクセス サーバに送信されます。

サポートされる RADIUS 属性のリストについては、「RADIUS 属性の概要および RADIUS IETF 属性」の章を参照してください。サポートされる TACACS+ の AV ペアのリストについては、「Configuring TACACS+」の章を参照してください。

認可の設定方法

この章のコマンドを使用した認可の設定例については、「認可の設定例」を参照してください。

名前付き方式リストによる AAA 認可の設定

名前付き方式リストを使用して AAA 認可を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]
2. 次のいずれかを実行します。
   - Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
   -
   -
   - Router(config)# **interface** *interface-type interface-number*
3. 次のいずれかを実行します。
   - Router(config-line)# **authorization**{**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}
   -
   -
   - Router(config-line)# **ppp authorization**{**default** | *list-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]	特定の認可タイプの認可方式リストを作成し、認可をイネーブルにします。
ステップ 2	次のいずれかを実行します。 • Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] • • • Router(config)# **interface** *interface-type interface-number*	認可方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。 または、認可方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを実行します。 • Router(config-line)# **authorization**{**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*} • • • Router(config-line)# **ppp authorization**{**default** | *list-name*}	1 つの回線または複数回線に認可リストを適用します。 または、1 つのインターフェイスまたは複数インターフェイスに認可リストを適用します。

グローバル コンフィギュレーション コマンドの認可のディセーブル化

commands キーワードを指定して **aaaauthorization** コマンドを使用すると、その特権レベルに関連付けられているすべての EXEC モード コマンド（グローバル コンフィギュレーション コマンドを含む）に対して認可が試行されます。一部の EXEC レベル コマンドと同じコンフィギュレーション コマンドもあるため、認可プロセスが混乱する可能性があります。**noaaaauthorizationconfig-commands** を使用すると、ネットワーク アクセス サーバがコンフィギュレーション コマンド認可の試行を停止します。

すべてのグローバル コンフィギュレーション コマンドについて AAA 認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Device(config)#` **no aaa authorization config-commands**	すべてのグローバル コンフィギュレーション コマンドについて認可をディセーブルにします。

コンソール上で AAA 認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

（注） デフォルトでコンソールの AAA 認可はディセーブルです。コンソールで AAA 認可がイネーブルの場合、AAA コンフィギュレーション段階で **no aaa authorization console** コマンドを設定してディセーブルにします。ユーザ認証用のコンソールでは AAA をディセーブルにする必要があります。

コマンド	目的
`Device(config)#` **no aaa authorization console**	コンソールでの認証を無効にします。

リバース Telnet の認可の設定

Telnet は、リモート ターミナル接続に使用される標準ターミナル エミュレーション プロトコルです。通常、ネットワーク アクセス サーバに（主にダイヤルアップ接続経由で）ログインし、Telnet を使用してそのネットワーク アクセス サーバから他のネットワーク デバイスにアクセスします。ただし、場合によっては、リバース Telnet セッションを確立する必要があります。リバース Telnet

セッションでは、反対方向の Telnet 接続（つまり、ネットワーク内部から、ネットワーク周辺にあるネットワーク アクセス サーバに対する接続）が確立されます。その接続によって、ネットワーク アクセス サーバに接続しているモデムや他のデバイスへのアクセスを取得します。リバース Telnet は、ユーザがネットワーク アクセス サーバに接続されているモデム ポートに Telnet を送信できるようにすることで、ユーザにダイヤルアウト機能を提供します。

リバース Telnet を介してアクセスできるポートのアクセス権を制御することが重要です。適切に制御しないと、たとえば、不正ユーザがモデムに自由にアクセスし、着信コールをトラップして迂回させたり、不正な宛先にコールを送信したりする可能性があります。

リバース Telnet 時の認証は、Telnet 用の標準の AAA ログイン手順を介して実行されます。通常、Telnet またはリバース Telnet セッションを確立するには、ユーザはユーザ名とパスワードを指定する必要があります。リバース Telnet 認可は、認証に加えて認可を必須にすることで、追加（任意）レベルのセキュリティを提供します。リバース Telnet 認可をイネーブルにすることで、標準の Telnet ログイン手順を介してユーザ認証を完了した後に、RADIUS または TACACS+ を使用して、そのユーザが非同期ポートにリバース Telnet アクセスを実行できるかどうかを認可できます。

リバース Telnet 認可には次の利点があります。

- リバース Telnet アクティビティを実行しているユーザに、リバース Telnet を使用して特定の非同期ポートにアクセスする権限を付与することで、追加レベルの保護を実現しています。
- リバース Telnet 認可を管理できる（アクセス リスト以外の）代替方式があります。

ネットワーク アクセス サーバが TACACS+ または RADIUS サーバからの認可情報を要求するように設定してから、ユーザによるリバース Telnet セッションの確立を許可するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **aaa authorization reverse-access** *method1* [*method2* ...]	ネットワーク アクセス サーバが認可情報を要求するように設定してから、ユーザによるリバース Telnet セッションの確立を許可します。

この機能によって、ネットワーク アクセス サーバは、セキュリティ サーバ（RADIUS または TACACS+）からリバース Telnet 認可情報を要求できます。セキュリティ サーバ上のユーザに固有のリバース Telnet 特権を設定する必要があります。

認可設定の例

TACACS 認可の例

次に、TACACS+ サーバを使用して、PPP や ARA などのネットワーク サービスの使用を認可する例を示します。TACACS+ サーバが使用不能の場合、または認可プロセス中にエラーが発生した場合、フォールバック方式（none）はすべての認可要求を許可することです。

```
aaa authorization network default group tacacs+ none
```

次に、TACACS+ を使用してネットワークの認可を許可する例を示します。

```
aaa authorization network default group tacacs+
```

次に、同じ認可を提供し、「*mci*」と「*att*」というアドレス プールも作成する例を示します。

```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255
```

これらのアドレス プールは、TACACS デーモンによって選択できます。デーモンの設定例を次に示します。

```
user = mci_customer1 {
    login = cleartext "some password"
    service = ppp protocol = ip {
        addr-pool=mci
    }
}
user = att_customer1 {
    login = cleartext "some other password"
    service = ppp protocol = ip {
        addr-pool=att
     }
```

RADIUS 認可の例

次に、RADIUS を使用して認可を行うようにルータを設定する方法の例を示します。

```
aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key
```

この RADIUS 認可設定のサンプル行は、次のように定義されます。

- **aaa authorization exec default group radius if-authenticated** コマンドで、ネットワーク アクセス サーバが RADIUS サーバに接続して、ユーザのログイン時にユーザが EXEC シェルを起動する権限があるかどうかを決定するように設定します。ネットワーク アクセス サーバが RADIUS サーバに接続するときにエラーが発生した場合、フォールバック方式は CLI の開始を許可することあり、ユーザが適切に認証されると行われます。

返される RADIUS 情報を使用して、その接続に適用される autocommand または接続アクセス リストを指定できます。

- **aaa authorization network default group radius** コマンドで、RADIUS を経由でネットワーク認可を設定します。この操作は、アドレス割り当ての管理、アクセス リストのアプリケーション、および他の多様なユーザ別の数量に使用できます。

（注） この例ではフォールバック方式を指定していないため、何らかの理由で認可に失敗すると、RADIUS サーバからの応答はありません。

リバース Telnet 認可の例

次に、ネットワーク アクセス サーバが TACACS+ セキュリティ サーバから認可情報を要求してから、ユーザによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

この TACACS+ リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA をイネーブルにします。
- **aaa authentication login default group tacacs+** コマンドで、ログイン時のユーザ認証のデフォルト方式として TACACS+ を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group tacacs+** コマンドで、ユーザ認可の方式として TACACS+ を指定します。
- **tacacs-server host** コマンドで、TACACS+ サーバを指定します。
- **tacacs-server timeout** コマンドで、ネットワーク アクセス サーバが TACACS+ サーバの応答を待機する期間を設定します。
- **tacacs-server key** コマンドで、ネットワーク アクセス サーバと TACACS+ デーモン間のすべての TACACS+ 通信に使用される暗号キーを定義します。

次に、ネットワーク アクセス サーバ「maple」上のポート tty2、およびネットワーク アクセス サーバ「oak」上のポート tty5 に対するリバース Telnet アクセス権をユーザ pat に付与する汎用の TACACS+ サーバを設定する例を示します。

```
user = pat
  login = cleartext lab
  service = raccess {
    port#1 = maple/tty2
    port#2 = oak/tty5
```

（注） この例では、「maple」と「oak」には、DNS 名またはエイリアスではなく、ネットワーク アクセス サーバのホスト名が設定されています。

次に、TACACS+ サーバ（CiscoSecure）を設定して、ユーザ pat にリバース Telnet アクセス権を付与する例を示します。

```
user = pat
profile_id = 90
profile_cycle = 1
member = Tacacs_Users
service=shell {
default cmd=permit
}
service=raccess {
allow "c2511e0" "tty1" ".*"
refuse ".*" ".*" ".*"
password = clear "goaway"
```

（注） CiscoSecure は、バージョン 2.1(*x*)～ バージョン 2.2(1) のコマンドライン インターフェイスを使用して、リバース Telnet だけをサポートしています。

空の「service=raccess {}」句は、リバース Telnet のネットワーク アクセス サーバ ポートに対して無条件のアクセス権をユーザに許可しています。「service=raccess」句が存在しない場合、ユーザはリバース Telnet のすべてのポートに対してアクセスを拒否されます。

TACACS+ の設定の詳細については、「Configuring TACACS」の章を参照してください。CiscoSecure の設定の詳細については、『*CiscoSecure Access Control Server User Guide*』の version 2.1(2) 以降を参照してください。

次に、ネットワーク アクセス サーバが RADIUS セキュリティ サーバから認可を要求してから、ユーザによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key go away
auth-port 1645 acct-port 1646
```

この RADIUS リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA をイネーブルにします。
- **aaa authentication login default group radius** コマンドで、ログイン時のユーザ認証のデフォルト方式として RADIUS を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group radius** コマンドで、ユーザ認可の方式として RADIUS を指定します。
- **radius-server host** コマンドで、RADIUS サーバを指定します。
- **radius-server key** コマンドで、ネットワーク アクセス サーバと RADIUS デーモン間のすべての RADIUS 通信に使用される暗号キーを定義します。

次に、ネットワーク アクセス サーバ「maple」上のポート tty2 で、ユーザ「pat」にリバース Telnet アクセス権を付与する RADIUS サーバに要求を送信する例を示します。

```
Username = "pat"
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=maple/tty2"
```

構文「raccess:port=any/any」で、リバース Telnet のネットワーク アクセス サーバ ポートに対して無条件のアクセス権をユーザに許可します。「raccess:port={*nasname* }/{*tty number* }」句がユーザ プロファイルにない場合、ユーザはすべてのポートでリバース Telnet へのアクセスを拒否されます。

RADIUS の設定の詳細については、「Configuring RADIUS」の章を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

認可の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *22*：認可の設定に関する機能情報

機能名	リリース	機能情報
AAA 認可およびアカウンティングの名前付き方式リスト	Cisco IOS XE Release 2.1	許可メソッドリストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、シーケンスで照会される認可方式（RADIUS または TACACS+ など）を説明する単なる名前付きリストです。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 11 章

アカウンティングの設定

AAA アカウンティング機能を使用すると、ユーザがアクセスするサービス、およびユーザが消費するネットワーク リソース量を追跡できます。AAAアカウンティングをイネーブルにすると、ネットワーク アクセス サーバから TACACS+ または RADIUS セキュリティ サーバ（実装しているセキュリティ手法によって異なります）に対して、アカウンティング レコードの形式でユーザ アクティビティがレポートされます。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを分析して、ネットワーク管理、クライアント課金、および監査に利用できます。

- 機能情報の確認，167 ページ
- アカウンティングを設定するための前提条件，168 ページ
- アカウンティングの設定の制約事項，168 ページ
- アカウンティングの設定に関する情報，168 ページ
- AAA アカウンティングの設定方法，183 ページ
- AAA アカウンティングの設定例，194 ページ
- その他の参考資料，198 ページ
- アカウンティングの設定に関する機能情報，199 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

アカウンティングを設定するための前提条件

次のタスクを実行してから、名前付き方式リストを使用してアカウンティングを設定します。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- RADIUS または TACACS+ 認可が発行されている場合、RADIUS または TACACS+ セキュリティ サーバの特性を定義します。シスコのネットワーク アクセス サーバを設定して RADIUS セキュリティ サーバと通信する方法の詳細については、「Configuring RADIUS」の章を参照してください。シスコのネットワーク アクセス サーバを設定して TACACS+ セキュリティ サーバと通信する方法の詳細については、「Configuring TACACS+」の章を参照してください。

アカウンティングの設定の制約事項

AAA アカウンティング機能には次の制限があります。

- アカウンティング情報は、最大 4 台の AAA サーバに同時送信できます。
- Service Selection Gateway（SSG）制限：SSG システムの場合、**aaa accounting network broadcast** コマンドを実行すると、**start-stop** アカウンティング レコードのみがブロードキャストされます。**ssg accounting interval** コマンドを使用して中間アカウンティング レコードを設定する場合、中間アカウンティング レコードは、設定したデフォルト RADIUS サーバにのみ送信されます。

アカウンティングの設定に関する情報

アカウンティングの方式指定リスト

認証および認可方式リストと同様に、アカウンティングの方式リストには、アカウンティングの実行方法とその方式を実行するシーケンスが定義されています。

アカウンティングの方式指定リストには、特定のセキュリティ プロトコルを指定し、アカウンティング サービスの特定の行またはインターフェイスに使用できます。唯一の例外はデフォルトの方式リスト（偶然に「default」と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、順に照会するアカウンティング方式（RADIUS、TACACS+ など）を記述する指定リストです。方式リストでは、アカウンティングに 1 つまたは複数のセキュリティ プロトコルを指定できます。そのため、最初の方式が失敗した場合にアカウンティングのバックアップ システムを確保できます。Cisco IOS XE ソフトウェアでは、方式リストのうち、アカウンティングをサポートする最初の方式が使用されます。その方式が応答しない場合、方式リストの次のアカウン

ティング方式が選択されます。このプロセスは、リストのいずれかのアカウンティング方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次のアカウンティング方式でアカウンティングが試行されます。このサイクルの任意の時点でアカウンティングが失敗した場合（つまり、セキュリティ サーバからユーザ アクセスの拒否応答が返される場合）、アカウンティング プロセスは停止し、その他のアカウンティング方式は試行されません。

アカウンティング方式リストは、要求されるアカウンティングの種類によって変わります。AAA は、次の 6 種類のアカウンティングをサポートしています。

- Network：パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。
- EXEC：ネットワーク アクセス サーバのユーザ EXEC ターミナル セッションに関する情報を提供します。
- Command：ユーザが発行する EXEC モード コマンドに関する情報を提供します。コマンド アカウンティングは、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、アカウンティング レコードを生成します。
- Connection：Telnet、ローカルエリア トランスポート（LAT）、TN3270、パケット アセンブラ/ディスアセンブラ（PAD）、rlogin などのネットワーク アクセス サーバから行われたすべてのアウトバンド接続に関する情報を出力します。
- System：システム レベルのイベントに関する情報を提供します。
- Resource：ユーザ認証に成功したコールの「開始」および「終了」レコードを提供します。また、認証に失敗したコールの「終了」レコードを提供します。

（注） システム アカウンティングは、名前付きアカウンティング リストを使用しません。システム アカウンティングのデフォルト リストだけを定義できます。

方式指定リストが作成されると、指定したアカウンティング タイプのアカウンティング方式のリストが定義されます。

アカウンティング方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。方式リストを指定せずに、特定の認可タイプ用の **aaa accounting** コマンドが発行されると、方式リストが明示的に定義されている場合を除き、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます。（定義済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、アカウンティングは実行されません。

ここでは、次の内容について説明します。

方式リストとサーバ グループ

サーバ グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバ ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 は RADIUS サーバのグループから構成されます。T1 と T2 は TACACS+ サーバのグループから構成されます。

Cisco IOS XE ソフトウェアでは、RADIUS および TACACS+ サーバ設定はグローバルです。サーバ グループを使用して、設定済みのサーバ ホストのサブセットを指定できます。このようなサーバ グループは、特定のサービスに使用できます。たとえば、サーバ グループを使用すると、R1 と R2 を個別のサーバ グループ（SG1 と SG2）として定義し、T1 と T2 を個別のサーバ グループ（SG3 と SG4）として定義できます。つまり、R1 と T1（SG1 と SG3）を方式リストに指定できるか、または R2 と T2（SG2 と SG4）を方式リストに指定できます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この場合、最初のホストエントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じ装置上でアカウンティング サービス用に設定されている 2 番めのホスト エントリを試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

DNIS 番号に基づくサーバ グループの設定およびサーバ グループの設定の詳細については、『*Cisco IOS XE Security Configuration Guide: Securing User Services* Release 2』の「Configuring RADIUS」または「Configuring TACACS+」を参照してください。

AAA アカウンティング方式

Cisco IOS XE はアカウンティングについて次の 2 つの方式をサポートします。

- TACACS+：ネットワーク アクセス サーバは、アカウンティング レコードの形式で TACACS+ セキュリティ サーバに対してユーザ アクティビティを報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。
- RADIUS：ネットワーク アクセス サーバは、アカウンティング レコードの形式で RADIUS セキュリティ サーバに対してユーザ アクティビティを報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。

（注） CSCuc32663 では、パスワードおよびアカウンティング ログは、TACACS+ または RADIUS セキュリティ サーバへ送信される前にマスクされます。マスクされていない情報を TACACS+ または RADIUS セキュリティ サーバに送信するには、**aaa accounting commands visible-keys** コマンドを使用します。

アカウンティング レコードの種類

最小限のアカウンティングの場合、**stop-only** キーワードを使用します。このキーワードによって、要求されたユーザプロセスの終了時に、終了レコードアカウンティング通知を送信するように、指定した方式（RADIUS または TACACS+）に指示します。詳細なアカウンティング情報が必要な場合、**start-stop** キーワードを使用して、要求されたイベントの開始時には開始アカウンティング通知、そのイベントの終了時には修理用アカウンティング通知を送信します。この回線またはインターフェイスですべてのアカウンティング アクティビティを終了するには、**none** キーワードを使用します。

アカウンティング方式

次の表に、サポートされるアカウンティング キーワードを示します。

表 *23*：*AAA* アカウンティング方式

キーワード	説明
groupradius	アカウンティングにすべての RADIUS サーバのリストを使用します。
grouptacacs+	アカウンティングにすべての TACACS+ サーバのリストを使用します。
group group-name	*group-name* サーバ グループで定義したように、アカウンティングのための RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にのみ使用されます。他のすべての方式がエラーを返しても、認証に成功したことを指定するには、コマンドで追加の方式を指定します。たとえば、TACACS+ 認証がエラーを返す場合に認証のバックアップ方式として RADIUS を指定する acct_tac1 という方式リストを作成するには、次のコマンドを入力します。

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

指定リストが **aaa accounting** コマンドで指定されていない場合に使用するデフォルト リストを作成するには、**default** キーワードの後に、デフォルトの状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザ認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa accounting network default stop-only group radius
```

AAA アカウンティングは、次の方式をサポートします。

- **grouptacacs**：ネットワーク アクセス サーバからアカウンティング情報を TACACS+ セキュリティ サーバに送信するようにするには、**grouptacacs+***method* キーワードを使用します。
- **groupradius**：ネットワーク アクセス サーバからアカウンティング情報を RADIUS セキュリティ サーバに送信するようにするには、**groupradius***method* キーワードを使用します。

（注） SLIP のアカウンティング方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、アカウンティングのデフォルト設定が適用されます。

- **group***group-name*：RADIUS または TACACS+ サーバのサブセットを指定して、アカウンティング方式として使用するには、**group***group-name* 方式を指定して **aaaaccounting** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaagroupserver** コマンドを使用します。たとえば、**aaagroupserver** コマンドを使用して、**grouploginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *loginrad* のメンバとして指定されます。

他の方式リストが定義されていない場合、ネットワーク アカウンティングの方式として **grouploginrad** を指定するには、次のコマンドを入力します。

```
aaa accounting network default start-stop group loginrad
```

アカウンティング方式としてグループ名を使用するには、事前に RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにする必要があります。

AAA アカウンティング タイプ

名前付きアカウンティング方式リストは、指定したタイプのアカウンティングに固有です。

- **network**：すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP などのプロトコル）について認可をイネーブルにする方式リストを作成するには、**network** キーワー

ドを使用します。たとえば、ARAP（ネットワーク）セッションにアカウント情報を提供する方式リストを作成するには、**arap** キーワードを使用します。

- **exec**：ネットワーク アクセス サーバ上のユーザ EXEC ターミナル セッションに関するアカウンティング レコード（ユーザ名、日付、開始時刻、終了時刻など）を提供する方式リストを作成するには、**exec** キーワードを使用します。
- **commands**：特定の特権レベルに関連付けられた特定の EXEC コマンドに関するアカウンティング情報を提供する方式リストを作成するには、**commands** キーワードを使用します。
- **connection**：ネットワーク アクセス サーバから開始されるすべての発信接続について、アカウンティング情報を提供する方式リストを作成するには、**connection** キーワードを使用します。
- resource：ユーザ認証に成功したコールまたは認証に失敗したコールのアカウンティング レコードを提供する方式リストを作成します。

（注） システム アカウンティングは、名前付き方式リストをサポートしません。

ネットワーク アカウンティング

ネットワーク アカウンティングは、パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。

次に、EXEC セッションを介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:44:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:45:00 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

```
Wed Jun 27 04:47:46 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Input-Octets = 3075
        Acct-Output-Octets = 167
        Acct-Input-Packets = 39
        Acct-Output-Packets = 9
        Acct-Session-Time = 171
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:48:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “408”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

次に、最初に EXEC セッションを開始した PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:00:35 2001 172.16.25.15    username1   tty4    562/4327528     starttask_id=28
      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15    username1   tty4 562/4327528     starttask_id=30
     addr=10.1.1.1   service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15    username1   tty4    408/4327528     update
task_id=30      addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=30
       addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1   bytes_in=2844
  bytes_out=1682  paks_in=36      paks_out=24     elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=28
       service=shell   elapsed_time=57
```

（注） アカウンティング パケット レコードの正確なフォーマットは、セキュリティ サーバ デーモンに応じて変わります。

次に、autoselect を介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:30:52 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 3
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000B”
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
```

```
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:36:49 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 3
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Framed-IP-Address = "10.1.1.1"
        Acct-Input-Octets = 8630
        Acct-Output-Octets = 5722
        Acct-Input-Packets = 94
        Acct-Output-Packets = 64
        Acct-Session-Time = 357
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、autoselect を介して着信する PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:02:19 2001 172.16.25.15    username1   Async5  562/4327528     starttask_id=35
      service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15    username1   Async5  562/4327528     update
task_id=35      service=ppp     protocol=ip     addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15    username1   Async5  562/4327528     stoptask_id=35
       service=ppp     protocol=ip     addr=10.1.1.2   bytes_in=3366   bytes_out=2149
  paks_in=42      paks_out=28     elapsed_time=164
```

EXEC アカウンティング

EXEC アカウンティングは、ネットワーク アクセス サーバ上にあるユーザ EXEC ターミナル セッション（ユーザ シェル）に関する情報を提供します。たとえば、ユーザ名、日付、開始時刻と終了時刻、アクセス サーバの IP アドレス、および（ダイヤルイン ユーザの場合）発信元の電話番号などです。

次に、ダイヤルイン ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:26:23 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:27:25 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
```

```
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Session-Time = 62
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、ダイヤルイン ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=2       service=shell
Wed Jun 27 04:08:55 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=2       service=shell   elapsed_time=1354
```

次に、Telnet ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:48:32 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Session-Time = 14
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、Telnet ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:06:53 2001        172.16.25.15    username1   tty26   10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001        172.16.25.15    username1   tty26   10.68.202.158
stoptask_id=41       service=shell   elapsed_time=9
```

コマンド アカウンティング

コマンドアカウンティングは、ネットワーク アクセス サーバで実行される各特権レベルの EXEC シェル コマンドに関する情報を提供します。各コマンド アカウンティング レコードには、その特権レベルで実行されるコマンド、各コマンドが実行された日時、および実行したユーザのリストが含まれます。

次に、特権レベル 1 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:47 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=3       service=shell   priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001        172.16.25.15    username1   tty3    5622329430/4327528
```

```
stop     task_id=4       service=shell   priv-lvl=1      cmd=show interfaces <cr>
Wed Jun 27 03:47:03 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=5       service=shell   priv-lvl=1      cmd=show ip route <cr>
```

次に、特権レベル 15 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:17 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=6       service=shell   priv-lvl=15     cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=7       service=shell   priv-lvl=15     cmd=interface GigabitEthernet0/0/0
 <cr>
Wed Jun 27 03:47:29 2001        172.16.25.15    username1   tty3    56223294304327528  stop
     task_id=8       service=shell   priv-lvl=15     cmd=ip address 10.1.1.1 255.255.255.0
 <cr>
```

（注） シスコの RADIUS 実装は、コマンド アカウンティングをサポートしていません。

接続アカウンティング

接続アカウンティングは、Telnet、LAT、TN3270、PAD、rlogin などのネットワーク アクセス サーバから行われるすべての発信接続に関する情報を提供します。

次に、発信 Telnet 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:28:00 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "00000008"
        Login-Service = Telnet
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:28:39 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "00000008"
        Login-Service = Telnet
        Login-IP-Host = "10.68.202.158"
        Acct-Input-Octets = 10774
        Acct-Output-Octets = 112
        Acct-Input-Packets = 91
        Acct-Output-Packets = 99
        Acct-Session-Time = 39
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、発信 Telnet 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:43 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=10     service=connection     protocol=telnet addr=10.68.202.158 cmd=telnet
 username1-sun
Wed Jun 27 03:48:38 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=10     service=connection     protocol=telnet addr=10.68.202.158 cmd=telnet
 username1-sun    bytes_in=4467   bytes_out=96    paks_in=61     paks_out=72 elapsed_time=55
```

次に、発信 rlogin 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:29:48 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Input-Octets = 18686
        Acct-Output-Octets = 86
        Acct-Input-Packets = 90
        Acct-Output-Packets = 68
        Acct-Session-Time = 22
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、発信 rlogin 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:48:46 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=12     service=connection     protocol=rlogin addr=10.68.202.158 cmd=rlogin
 username1-sun /user username1
Wed Jun 27 03:51:37 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=12     service=connection     protocol=rlogin addr=10.68.202.158 cmd=rlogin
 username1-sun /user username1 bytes_in=659926 bytes_out=138   paks_in=2378    paks_
out=1251        elapsed_time=171
```

次に、発信 LAT 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:53:06 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
VAX
Wed Jun 27 03:54:15 2001        172.16.25.15    username1   tty3    5622329430/4327528
```

```
stop     task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
VAX  bytes_in=0      bytes_out=0     paks_in=0      paks_out=0      elapsed_time=6
```

システム アカウンティング

システムアカウンティングは、すべてのシステムレベルイベント（たとえば、システムのリブート時やアカウンティングのオン/オフ時）に関する情報を提供します。

次のアカウンティング レコードは、AAA アカウンティングがオフになったことを示す一般的な TACACS+ システム アカウンティング レコード サーバを示します。

```
Wed Jun 27 03:55:32 2001        172.16.25.15    unknown unknown unknown start   task_id=25
   service=system  event=sys_acct  reason=reconfigure
```

（注） アカウンティング パケット レコードの正確なフォーマットは、TACACS+ デーモンに応じて変わります。

次のアカウンティング レコードは、AAA アカウンティングがオンになったことを示す TACACS+ システム アカウンティング レコードを示します。

```
Wed Jun 27 03:55:22 2001        172.16.25.15    unknown unknown unknown stop    task_id=23
   service=system  event=sys_acct  reason=reconfigure
```

システム リソースを測定する追加のタスクについては、他の Cisco IOS XE ソフトウェア コンフィギュレーションガイドを参照してください。たとえば、IPアカウンティングタスクについては、『*CiscoIOS XE Application Services Configuration Guide,* Release 2』の「Configuring IP Services」を参照してください。

リソース アカウンティング

シスコが採用している AAA アカウンティングでは、ユーザ認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。ユーザ認証の一部として認証に失敗したコールの「終了」レコードを生成する追加機能もサポートされます。このようなレコードは、ネットワークを管理およびモニタするアカウンティング レコードを採用する場合に必要です。

ここでは、次の内容について説明します。

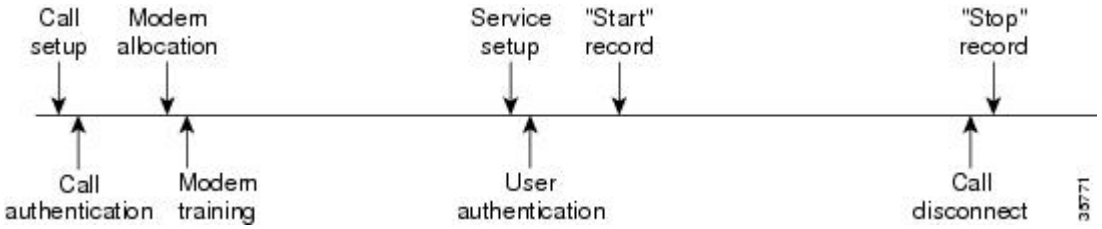
AAA リソース失敗終了アカウンティング

AAA リソース失敗終了アカウンティングの前には、コール設定シーケンスのユーザ認証段階に到達できなかったコールについて、アカウンティング レコードを提供する方式がありませんでした。このようなレコードは、ネットワークおよびその卸売りの顧客を管理およびモニタするアカウンティング レコードを採用する場合に必要です。

この機能によって、ユーザ認証に到達しなかったコールの「終了」アカウンティング レコードが生成されます。「終了」レコードは、コール設定の時点から生成されます。ユーザ認証に成功したすべてのコールは、従来と同様に動作します。つまり、追加のアカウンティング レコードは確認されません。

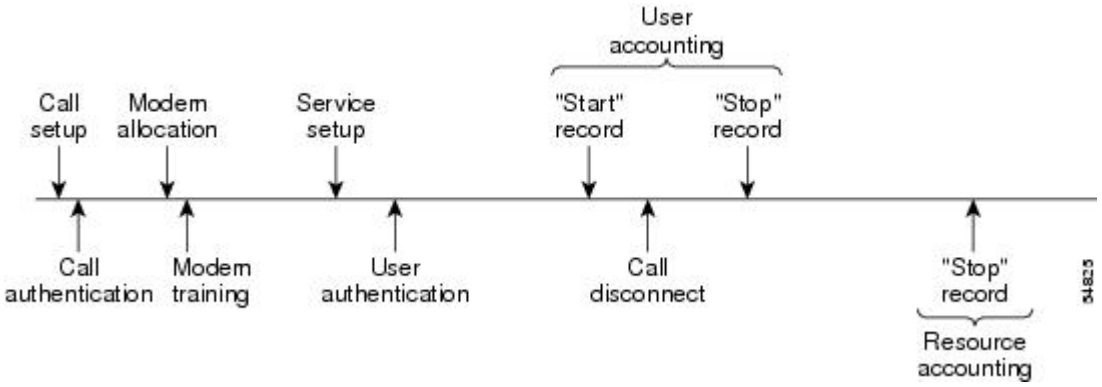
次の図に、通常のコールフローで、AAA リソース失敗終了アカウンティングをイネーブルにしていないコール シーケンスを示します。

図 *4*：通常のフローで *AAA* リソース失敗終了アカウンティングをイネーブルにしていないモデム ダイヤルイン コール設定シーケンス



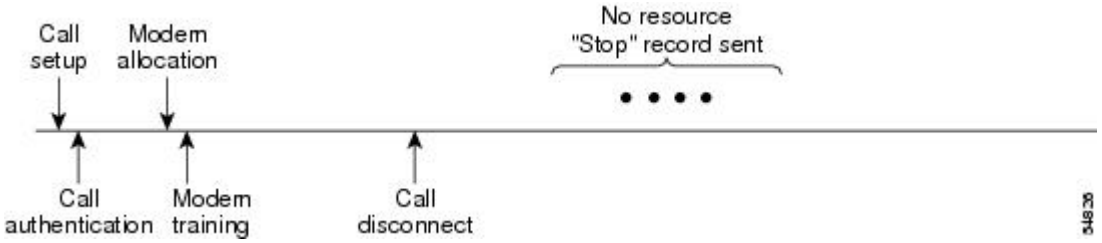
次の図に、通常のコールフローで、AAA リソース失敗終了アカウンティングをイネーブルにしたコール シーケンスを示します。

図 *5*：通常のフローで *AAA* リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



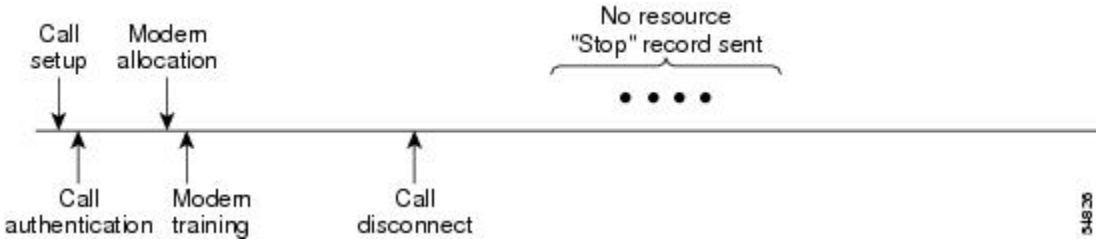
次の図に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしたコール設定シーケンスを示します。

図 *6*：ユーザ認証前にコールの接続解除が発生し、*AAA* リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



次の図に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしていないコール設定シーケンスを示します。

図 *7*：ユーザ認証前にコールの接続解除が発生し、*AAA* リソース失敗終了アカウンティングをイネーブルにしていないモデム ダイヤルイン コール設定シーケンス



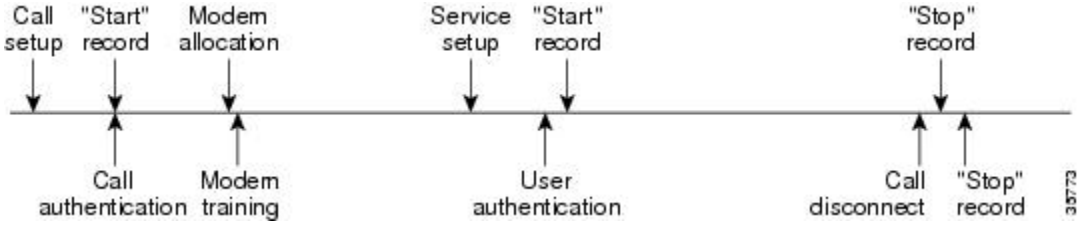
開始 - 終了レコードの AAA リソース アカウンティング

開始 - 終了レコードの AAA リソース アカウンティングは、各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートしています。この機能は、アカウンティング レコードなどを報告するデータの発信元の 1 つから、卸売りの顧客を管理およびモニタするために使用できます。

この機能を使用すると、コール設定およびコールの接続解除の「開始 - 終了」アカウンティング レコードは、デバイスに対するリソース接続の進行状況を追跡します。個別のユーザ認証「開始 - 終了」アカウンティング レコードが、ユーザ管理の進行状況を追跡します。これら 2 セットのアカウンティング レコードは、そのコールで固有のセッション ID を使用して相互リンクされます。

次の図は、AAA リソース開始 - 終了アカウンティングをイネーブルにしたコール設定シーケンスを示します。

図 *8*：リソース開始 - 終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



AAA アカウンティングの強化

AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同

時にブロードキャストすることが可能です。この機能を使用すると、サービス プロバイダーは自社使用のプライベート AAA サーバやエンドユーザの AAA サーバにアカウンティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバグループは、他のグループとは関係なく、フェールオーバーの場合のバックアップ サーバを定義できます。

したがって、サービス プロバイダーとそのエンド ユーザは、アカウンティング サーバに異なるプロトコル（RADIUS または TACACS+）を使用できます。また、サービス プロバイダーとそのエンド ユーザは、それぞれ単独でバックアップ サーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバー シーケンスを持つ個別のグループを介して、冗長的なアカウンティング情報を単独で管理できます。

AAA セッション MIB

ユーザが AAA セッション MIB 機能を使用すると、簡易ネットワーク管理プロトコル（SNMP）を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告される AAA アカウンティング情報に直接関連付けることができます。AAA セッション MIB は、次の情報を提供します。

- 各 AAA 機能の統計情報（show radius statistics コマンドと併用する場合）
- AAA 機能を提供するサーバのステータス
- 外部 AAA サーバの ID
- （アイドル時間などの）リアルタイム情報（アクティブ コールを終了するかどうかを評価する SNMP ネットワークが使用する追加基準を提供します）

次の表に、認証済みクライアントと AAA セッション MIB 機能との接続をモニタおよび終了するために使用できる SNMP ユーザエンド データ オブジェクトを示します。

表 *24*：*SNMP* エンドユーザ データ オブジェクト

フィールド	説明
SessionId	AAA アカウンティング プロトコルに使用されるセッション ID（RADIUS 属性 44（Acct-Session-ID）から報告される値と同じ）
UserId	ユーザ ログイン ID または（ログインが使用できない場合）長さがゼロの文字列
IpAddr	セッションの IP アドレスまたは（IP アドレスが適用されない場合、または使用できない場合）0.0.0.0
IdleTime	セッションがアイドルになってからの経過時間

Disconnect	そのクライアントとの接続を解除するために使用されるセッション終了オブジェクト
CallId	コール トラッカー レコードが保存した、このアカウンティング セッションに対応するエントリ インデックス

次の表に、システム別に SNMP を使用する AAA セッション MIB 機能から提供される AAA の概要情報を示します。

表 *25*：*SNMP AAA* セッションの概要

フィールド	説明
ActiveTableEntries	現在アクティブなセッションの数
ActiveTableHighWaterMark	システムが最後に再インストールされてからの接続セッションの最大数
TotalSessions	システムが最後に再インストールされてからのセッションの合計数
DisconnectedSessions	システムが最後に再インストールされてから接続解除されたセッションの合計数

アカウンティング属性と値のペア

ネットワーク アクセス サーバは、TACACS+ 属性と値（AV）のペアまたは RADIUS 属性（実装しているセキュリティ方式によって異なります）に定義されたアカウンティング機能を監視します。

AAA アカウンティングの設定方法

名前付き方式リストによる AAA アカウンティングの設定

名前付き方式リストを使用して AAA アカウンティングを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]
2. 次のいずれかを実行します。
   - Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
   -
   -
   -
3. 次のいずれかを実行します。
   - Router(config-line)# **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*}
   -
   -
   -

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]	アカウンティング方式リストを作成し、アカウンティングをイネーブルにします。引数 *list-name* は、作成したリストに名前を付けるときに使用される文字列です。
ステップ 2	次のいずれかを実行します。 • Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] • • • 例： `Router(config)#` **interface** *interface-type interface-number*	アカウンティング方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。 または アカウンティング方式リストを適用するインターフェイスについて、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを実行します。 • Router(config-line)# **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*} • •	1 つの回線または複数回線にアカウンティング方式リストを適用します。 または 1 つのインターフェイスまたは複数インターフェイスにアカウンティング方式リストを適用します。

	コマンドまたはアクション	目的
	• 例： `Router(config-if)#` **ppp accounting** {**default** | *list-name*}	

次の作業

（注） システム アカウンティングは、名前付き方式リストを使用しません。システム アカウンティングの場合、デフォルトの方式リストだけを定義します。

ヌル ユーザ名セッション時のアカウンティング レコード生成の抑制

AAA アカウンティングをアクティブにすると、Cisco IOS XE ソフトウェアは、システム上にあるすべてのユーザにアカウンティング レコードを発行します。このとき、プロトコル変換のためにユーザ名文字列がヌルのユーザも含まれます。この例では、**aaa authentication login** *method-list* **none** コマンドが適用される回線で着信するユーザです。関連付けられているユーザ名がないセッションについて、アカウンティング レコードが生成されないようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting suppress null-username**	ユーザ名文字列がヌルのユーザについて、アカウンティング レコードが生成されないようにします。

中間アカウンティング レコードの生成

アカウンティング サーバに定期的な中間アカウンティング レコードを送信できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting update** [**newinfo**] [**periodic**] `number`	アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

aaa accounting update コマンドをアクティブにすると、Cisco IOS XE ソフトウェアは、システム上のすべてのユーザに中間アカウンティング レコードを発行します。**newinfo** キーワードを使用した場合は、レポートする新しいアカウンティング情報が発生するたびに、中間アカウンティング レコードがアカウンティング サーバに送信されます。たとえば、インターネット プロトコル コントロール プロトコル（IPCP）がリモート ピアとの IP アドレスのネゴシエーションを完了したときにこれが発生します。中間アカウンティング レコードには、リモート ピアに使用されるネゴシエート済み IP アドレスが含まれます。

キーワード **periodic** を指定して **aaa accounting update** コマンドを使用すると、中間アカウンティング レコードが引数番号によって定義されたように定期的に送信されます。中間アカウンティング レコードには、中間アカウンティング レコードが送信される時間までに、そのユーザについて記録されたすべてのアカウンティング情報が含まれます。

注意 多数のユーザがネットワークにログインしている場合、**aaa accounting update periodic** コマンドを使用すると、重度の輻輳が発生する可能性があります。

定期的アカウンティング レコードを有効化する代替手段の設定

次の代替手段を使用して、アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにできます。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaaccountingnetworkdefault**
4. **action-type** {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaaccountingnetworkdefault** 例： `Router(config)# aaa accounting network default`	すべてのネットワーク関連のサービス要求のデフォルトのアカウンティングを設定し、アカウンティング方式リストのコンフィギュレーション モードを開始します。

ステップ 4	**action-type** {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}
	
	例：
	
	`Router(cfg-acct-mlist)# action-type start-stop`
	
	例：
	
	`periodic interval 5`
		アカウンティング レコードに対して実行されるアクションのタイプを指定します。
		• （任意）periodic キーワードは、定期的なアカウンティング アクションを示します。
		• interval キーワードは、定期的なアカウンティング間隔を指定します。
		• value 引数は、アカウンティング更新レコードの間隔を指定します（分単位）。
		• disable キーワードは、定期的なアカウンティングをディセーブルにします。

ステップ 5	**exit** 例： `Router(cfg-acct-mlist)# exit`	グローバル コンフィギュレーション モードに戻ります。

中間サービス アカウンティング レコードの生成

このタスクを実行して、サブスクライバに対する定期的な間隔での中間サービス アカウンティング レコードの生成をイネーブルにします。

はじめる前に

ユーザ サービス プロファイルの RADIUS 属性 85 は設定済みの中間の間隔値よりも常に優先されます。RADIUS 属性 85 は、ユーザ サービス プロファイル内にある必要があります。詳細については、RADIUS 属性の概要および RADIUS IETF 属性の機能のドキュメントを参照してください。

（注） RADIUS 属性 85 がユーザ サービス プロファイル内にない場合、中間アカウンティング レコードの生成で設定された中間の間隔値がサービスの中間アカウンティング レコードに使用されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **subscriberserviceaccountinginterim-interval***minutes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**subscriberserviceaccountinginterim-interval***minutes* 例： `Router(config)# subscriber service accounting interim-interval 10`	サブスクライバに対する定期的な間隔での中間サービス アカウンティング レコードの生成をイネーブルにします。*minutes* 引数は、アカウンティング更新レコードを送信する定期的な間隔を 1 ～ 71582 分で示します。

失敗したログインまたはセッションに対するアカウンティングレコードの生成

AAA アカウンティングをアクティブにすると、Cisco IOS XE ソフトウェアは、ログイン認証に失敗したシステム ユーザ、またはログイン認証には成功しても何らかの理由で PPP ネゴシエーションに失敗したユーザのアカウンティング レコードを生成しません。

ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザについて、アカウンティング終了レコードを生成するように指定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting send stop-record authentication failure**	ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザについて、「終了」レコードを生成します。

EXEC-Stop レコードよりも前のアカウンティング NETWORK-Stop レコードの指定

EXEC 終了セッションを開始する PPP ユーザの場合、EXEC-stop レコードの前に、NETWORK レコードを生成するように指定できます。特定のサービスについて顧客に課金する場合など、状況によっては、ネットワークの開始レコードと終了レコードを一緒に保持する方が望ましいことがあります。その際、基本的に、EXEC の開始メッセージと終了メッセージのフレームワーク内に「ネスト」にします。たとえば、PPP を使用するユーザ ダイヤルインによって、EXEC-start、NETWORK-start、EXEC-stop、NETWORK-stop というレコードを作成できます。ネットワーク アカウンティング レコードをネストにすることで、NETWORK-stop レコードは NETWORK-start メッセージ（EXEC-start、NETWORK-start、NETWORK-stop、EXEC-stop）に従います。

ユーザ セッションのアカウンティング レコードをネストするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting nested**	ネットワーク アカウンティング レコードをネストします。

スイッチオーバー上のシステム アカウンティング レコードの抑制

スイッチオーバー中のシステムアカウンティングオンおよびアカウンティングオフメッセージを抑制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting redundancy suppress system-records**	スイッチオーバー中のシステムアカウンティング レコードを抑制します。

AAA リソース失敗終了アカウンティングの設定

リソース失敗終了アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting resource** *method-list* **stop-failure group** *server-group*	ユーザ認証に到達しないコールについて、「終了」レコードを生成します。 （注） AAA リソース失敗終了アカウンティング機能を設定する前に、アカウンティングを設定するための前提条件,（168 ページ）に記載されている作業を実行し、ネットワーク アクセス サーバ上で SNMP をイネーブルにしてください。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で SNMP をイネーブルにする方法の詳細については、『Cisco IOS XE Network Management Configuration Guide』の「Configuring SNMP Support」の章を参照してください。

開始 - 終了レコードの AAA リソース アカウンティングの設定

開始 - 終了レコードのフル リソース アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting resource** *method-list* **start-stop group** *server-group*	各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートします。 （注） この機能を設定する前に、アカウンティングを設定するための前提条件,（168 ページ）に記載されている作業を実行し、ネットワーク アクセス サーバ上で SNMP をイネーブルにしてください。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で SNMP をイネーブルにする方法の詳細については、『Cisco IOS XE Network Management Configuration Guide, Release 2』の「Configuring SNMP Support」の章を参照してください。

AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。このコマンドは、**broadcast** キーワードを使用できるように変更されました。

コマンドまたはアクション	目的
`Router(config)#` **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] *method1* [*method2...*]	複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。

DNIS による AAA ブロードキャスト アカウンティングの設定

DNIS による AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa dnis map accounting network** コマンドを使用します。このコマンドは、**broadcast** キーワードおよび複数のサーバ グループを使用できるように変更されました。

コマンドまたはアクション	目的
`Router(config)#` **aaa dnis map** *dnis-number* **accounting network** ［**start-stop** ｜ **stop-only** ｜ **none**］［**broadcast**］ *method1* ［*method2*...］	DNIS によるアカウンティングの設定を許可します。このコマンドは、グローバルの **aaa accounting** コマンドよりも優先されます。 複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。

AAA セッション MIB の設定

次のタスクは、次の AAA セッション MIB 機能の設定よりも前に実行する必要があります。

- SNMP を設定します。SNMP については、『Cisco IOS XE Network Management Configuration Guide』の「Configuring SNMP Support」の章を参照してください。
- AAA を設定します。
- RADIUS または TACACS+ サーバの特性を定義します。

（注） SNMP を多用すると、全体のシステム パフォーマンスに影響が出る可能性があります。そのため、この機能を使用するときに、通常のネットワーク管理パフォーマンスを考慮する必要があります。

AAA セッション MIB を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **aaa session-mib disconnect**	SNMP を使用して、認証済みクライアント接続をモニタおよび終了します。 コールを終了するには、disconnect キーワードを使用します。

AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとの間にコンソールセッションを確立するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)#` **no aaa accounting system guarantee-first**	**aaa accounting system guarantee-first** コマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。 状況によっては、システムの再ロードが完了するまで（3 分よりも長くかかる可能性があります）、ユーザがコンソールまたは Telnet 接続でセッションを開始できない可能性があります。この問題を解決するには、**no aaa accounting system guarantee-first** コマンドを使用します。

アカウンティングのモニタリング

RADIUS または TACACS+ アカウンティングの場合、特定の **show** コマンドは存在しません。ログインしているユーザに関する情報を表示するアカウンティング レコードを取得するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router#` **show accounting**	ネットワークでアクティブなアカウント可能なイベントの表示を許可し、アカウンティング サーバでデータが損失した場合に情報を収集できます。

アカウンティングのトラブルシューティング

アカウンティング情報の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router#` **debug aaa accounting**	説明の義務があるイベントが発生したときに、その情報を表示します。

AAA アカウンティングの設定例

方式指定リストの設定の例

次に、RADIUS サーバから AAA サービスを提供するために Cisco AS5200（AAA および RADIUS セキュリティ サーバとの通信で有効）を設定する例を示します。RADIUS サーバが応答に失敗すると、認証情報と認可情報についてローカル データベースへの照会が行われ、アカウンティング サービスは TACACS+ サーバによって処理されます。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network network1 group radius local
aaa accounting network network2 start-stop group radius group tacacs+
username root password ALongPassword
tacacs-server host 172.31.255.0
tacacs-server key goaway
radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization network1
 ppp accounting network2
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaanew-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaaauthenticationloginadminslocal** コマンドは、ログイン認証に方式リスト「admins」を定義します。
- **aaaauthenticationpppdialinsgroupradiuslocal** コマンドで、最初に RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。

- **aaaauthorizationnetworknetwork1groupradiuslocal** コマンドで、「network1」というネットワーク認可方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS 認可を使用するように指定します。RADIUS サーバが応答に失敗すると、ローカル ネットワークの認可が実行されます。
- **aaaaccountingnetworknetwork2start-stopgroupradiusgrouptacacs+** コマンドで、「network2」というネットワーク アカウンティング方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS アカウンティング サービス（この場合、特定のイベントに対する開始レコードと終了イベント）を使用するように指定します。RADIUS サーバが応答に失敗すると、アカウンティングサービスは TACACS+ サーバによって処理されます。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP パスワード認証プロトコル（PAP）認証での発信元の身元確認に使用されます。
- **tacacs-serverhost** コマンドは TACACS+ サーバ ホストの名前を定義します。
- **tacacs-serverkey** コマンドは、ネットワーク アクセス サーバと TACACS+ サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **radius-serverhost** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-serverkey** コマンドは、ネットワーク アクセス サーバと RADIUS サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **interfacegroup-async** コマンドは非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulationppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **pppauthenticationchapdialins** コマンドは ppp 認証方式としてチャレンジ ハンドシェイク認証プロトコル（CHAP）を選択し、特定のインターフェイスに「dialins」方式リストを適用します。
- **pppauthorizationnetwork1** コマンドによって、blue1 ネットワーク認可方式リストは指定したインターフェイスに適用されます。
- **pppaccountingnetwork2** コマンドによって、red1 ネットワーク アカウンティング方式リストは指定したインターフェイスに適用されます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselectppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS XE ソフトウェアを設定します。
- **autoselectduring-login** コマンドを使用して、Return キーを押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **loginauthenticationadmins** コマンドは、ログイン認証に admins 方式リストを適用します。

- **modemdialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

showaccounting コマンドを使用すると、前述の設定に関する出力が次のように生成されます。

```
Active Accounted actions on tty1, User username2 Priv 1
 Task ID 5, Network Accounting record, 00:00:52 Elapsed
 task_id=5 service=ppp protocol=ip address=10.0.0.98
```

次の表に、前述の出力に含まれるフィールドについて説明します。

表 *26*：*show accounting* のフィールドの説明

フィールド	説明
Active Accounted actions on	ユーザがログインに使用する端末回線またはインターフェイス名
User	ユーザの ID。
Priv	ユーザの特権レベル。
Task ID	各アカウンティングセッションの固有識別情報
Accounting Record	アカウンティング セッション タイプ
Elapsed	このセッション タイプの期間（hh:mm:ss）
attribute=value	このアカウンティングセッションに関連付けられている AV ペア

AAA リソース アカウンティングの設定の例

次に、リソース失敗終了アカウンティング、および 開始 - 終了レコード機能のリソース アカウンティングを設定する例を示します。

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method
 to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all start-stop
 accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to
 use for all start-stop accounting services.
```

```
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

AAA ブロードキャスト アカウンティングの設定の例

次に、グローバル **aaa accounting** コマンドを使用して、ブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

broadcast キーワードによって、ネットワーク接続に関する「開始」および「終了」アカウンティング レコードが、グループ isp ではサーバ 10.0.0.1 に、グループ isp_customer ではサーバ 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

DNIS による AAA ブロードキャスト アカウンティングの設定の例

次に、グローバル **aaa dnis map accounting network** コマンドを使用して、DNIS によるブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

broadcast キーワードによって、DNIS 番号 7777 のネットワーク接続コールに関する「開始」および「終了」アカウンティング レコードが、グループ isp ではサーバ 10.0.0.1 に、グループ isp_customer ではサーバ 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

AAA セッション MIB の例

次に、AAA セッション MIB 機能を設定して、PPP ユーザの認証済みクライアント接続を解除する例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

その他の参考資料

ここでは、アカウンティングの設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
SNMP の設定	『*Cisco IOS XE Network Management Configuration Guide*』
SNMP コマンド	『*Cisco IOS Network Management Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
RADIUS の設定	RADIUS の設定
TACACS+ の設定	TACACS+ の設定
IP サービスの設定	『*Cisco IOS XE Application Services Configuration Guide*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
• CISCO-AAA-SESSION-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

アカウンティングの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *27*：アカウンティングの設定に関する機能情報

機能名	リリース	機能情報
AAA ブロードキャスト アカウンティング	Cisco IOS XE Release 2.1	AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaaaccounting**。
AAA セッション MIB	Cisco IOS XE Release 2.1	ユーザが AAA セッション MIB 機能を使用すると、簡易ネットワーク管理プロトコル（SNMP）を使用して自身の認証済みクライアント接続をモニタおよび終了できます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaasession-mibdisconnect**。

機能名	リリース	機能情報
接続アカウンティング	Cisco IOS XE Release 2.1	接続アカウンティングは、Telnet、ローカルエリア トランスポート（LAT）、TN3270、Packet Assembler/disassembler（PAD）、rlogin など、ネットワーク アクセス サーバからの発信接続すべてに関する情報を提供します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。
AAA 中間アカウンティング	Cisco IOS XE Release 2.4	AAA 中間アカウンティングにより、レポートする必要がある新しいアカウンティング情報が発生するたびに、または定期的に、アカウンティング サーバに中間アカウンティング レコードを送信できます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaaaccountingupdate** および **subscriberserviceaccountinginterim-interval**。

第 12 章

AAA-SERVER-MIB Set Operation

AAA-SERVER-MIB Set Operation 機能により、CISCO-AAA-SERVER-MIB を使用して認証、許可、アカウンティング（AAA）サーバを設定する機能を拡張できます。この機能を使用すると、次のことができます。

- 新しい AAA サーバを作成または追加する。
- CISCO-AAA-SERVER-MIB で「KEY」を修正する。
- AAA サーバの設定を削除する。

- 機能情報の確認，203 ページ
- AAA-SERVER-MIB Set Operation の前提条件，204 ページ
- AAA-SERVER-MIB Set Operation の制約事項，204 ページ
- AAA-SERVER-MIB Set Operation に関する情報，204 ページ
- Configure AAA-SERVER-MIB Set Operation の設定方法，205 ページ
- AAA-SERVER-MIB Set Operation の設定例，206 ページ
- その他の参考資料，208 ページ
- AAA-SERVER-MIB Set Operation の機能情報，209 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA-SERVER-MIB Set Operation の前提条件

AAA がルータで有効になっている必要があります。つまり、**aaa new-model** コマンドが設定されている必要があります。この設定が行われていない場合、SET 操作は失敗します。

AAA-SERVER-MIB Set Operation の制約事項

現時点では、CISCO SNMP SET 操作は RADIUS プロトコルに対してのみサポートされています。このため、追加、修正、削除できるのはグローバル コンフィギュレーション モードの RADIUS サーバだけです。

AAA-SERVER-MIB Set Operation に関する情報

CISCO-AAA-SERVER-MIB

CISCO-AAA-SERVER-MIB により、サーバ自体と AAA サーバの動作、および外部サーバとの AAA 通信の両方の状態が統計情報に反映されます。CISCO-AAA-SERVER-MIB からは次の情報が得られます。

- 各 AAA 動作の統計情報
- AAA 機能を使用できるようになっているサーバのステータス
- 外部 AAA サーバの ID

CISCO-AAA-SERVER-MIB Set Operation

Cisco IOS XE Release 2.1 では、CISCO-AAA-SERVER-MIB は GET と SET 両方の操作をサポートしています。SET 操作を使用すると、次の作業を行うことができます。

- 新しい AAA サーバを作成または追加する。
- CISCO-AAA-SERVER-MIB で KEY を修正する。この「秘密キー」は、ネットワーク アクセス サーバ（NAS）および AAA サーバに存在する AAA サーバへの接続をセキュリティ保護するために使用されます。
- AAA サーバの設定を削除する。

Configure AAA-SERVER-MIB Set Operation の設定方法

この機能を使用するに当たって、特別な設定は必要ありません。簡易ネットワーク管理プロトコル（SNMP）フレームワークを使用して MIB を管理できます。SNMP の設定については、「追加情報」を参照してください。

RADIUS サーバの設定およびサーバの統計情報の確認

RADIUS サーバの設定やサーバの統計情報は、次の手順を実行することで確認できます。

手順の概要

1. **enable**
2. **showrunning-config|includeradius-serverhost**
3. **showaaaservers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showrunning-config|includeradius-serverhost** 例： `Router# show running-config | include radius-server host`	グローバルコンフィギュレーションモードで設定されている RADIUS サーバをすべて表示します。
ステップ 3	**showaaaservers** 例： `Router# show aaa servers`	認証、許可、アカウンティング（AAA）サーバとの間で送受信された要求の数に関するデータを表示します。

AAA-SERVER-MIB Set Operation の設定例

RADIUS サーバの設定およびサーバの統計情報の例

次の出力例は、SET 操作の前と後の RADIUS サーバの設定およびサーバの統計情報を示しています。

SET 操作の前

```
Router# show running-config | include radius-server host
! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

サーバの統計情報

```
Router# show aaa servers
RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 2
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 5m
RADIUS: id 3, priority 2, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 5s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 3m
```

RADIUS サーバの設定と統計情報をチェックする SNMP GET 操作

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
```

```
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
aaa-server5:/users/smetri>
```

SNMP Set オペレーション

RADIUS サーバのキーが変更されています。また、インデックス「1」が使用されています。このインデックスは、エントリの追加、削除、修正に使用されるワイルドカードとして機能します。

```
Change the key for server 1:=>
aaa-server5:/users/smetri>  setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```

SET 操作の後

上記の SNMP SET 操作後、ルータの設定が変更されます。SET 操作後の出力を次に示します。

```
Router# show running-config | include radius-server host
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
! The following line shows a change in the key value to “king.”
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king
```

```
Router# show aaa servers
RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
認証コマンド	『*Cisco IOS Security Command Reference*』
IEEE 802.1x-Flexible Authentication	『*Securing User Services Configuration Library*』

MIB

MIB	MIB のリンク
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3580	「*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AAA-SERVER-MIB Set Operation の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *28*：*AAA-SERVER-MIB Set Operation* の機能情報

機能名	リリース	機能情報
AAA-SERVER-MIB Set Operation	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービスルータで導入されました。

第 13 章

Per VRF AAA

Per VRF AAA 機能により、ISP は、認証、許可、アカウンティング（AAA）サービスをバーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスに基づいて区分して、カスタマーに独自の AAA サービスの一部を制御させることができます。

サーバ グループのサーバ リストは、グローバル コンフィギュレーションでのホストへの参照に加えて、プライベート サーバの定義を含めるために拡張されています。このため、カスタマー サーバとグローバル サービス プロバイダーのサーバに同時にアクセスできます。

Cisco IOS XE Release 2.4 以降のリリースでは、ローカルまたはリモートで保存したカスタマー テンプレートを使用し、カスタマー テンプレートに保存された情報に基づいて、AAA サービスを実行できます。この機能は、Dynamic Per VRF AAA 機能と呼ばれています。

- Per VRF AAA の前提条件，211 ページ
- Per VRF AAA の制約事項，212 ページ
- Per VRF AAA に関する情報，212 ページ
- Per VRF AAA の設定方法，219 ページ
- Per VRF AAA の設定例，233 ページ
- その他の参考資料，241 ページ
- Per VRF AAA の機能情報，243 ページ
- 用語集，246 ページ

Per VRF AAA の前提条件

Per VRF AAA 機能を設定する前に、AAA をイネーブルにする必要があります。詳細については、6 ページの「Per VRF AAA の設定方法」を参照してください。

Per VRF AAA の制約事項

- この機能は、RADIUS サーバについてのみサポートされています。
- すべての機能について、ネットワーク アクセス サーバ（NAS）と AAA サーバとの間で一貫性が必要なため、サーバ グループごとの設定ではなく、Per VRF を設定したら、動作パラメータを定義する必要があります。
- ローカルまたはリモートでカスタマーテンプレートを設定する機能は、Cisco IOS XE Release 2.4 以降のリリースでのみ使用できます。

Per VRF AAA に関する情報

Per VRF AAA 機能を使用する場合、AAA サービスを VRF インスタンスに基づいたものにできます。この機能により、プロバイダー エッジ（PE）または仮想ホーム ゲートウェイ（VHG）で、カスタマーのバーチャル プライベート ネットワーク（VPN）に関連付けられたカスタマーの RADIUS サーバと RADIUS プロキシを経由せずに直接通信できます。RADIUS プロキシを使用する必要がないため、ISP は、VPN による提供サービスをより効率的に拡張でき、カスタマーにさらに柔軟性を提供できます。

Per VRF AAA の機能

カスタマーごとに AAA をサポートするには、一部の AAA 機能をで VRF を認識させる必要があります。つまり、ISP は、AAA サーバ グループ、方式リスト、システム アカウンティング、およびプロトコル固有のパラメータなどの動作パラメータを定義し、これらのパラメータを特定の VRF インスタンスにバインドできる必要があります。動作パラメータの定義とバインディングには、次の 1 つ以上の方式が使用できます。

- バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）：特定のカスタマーに設定されたに仮想テンプレートまたはダイヤラ インターフェイス。
- ローカルで定義されたカスタマー テンプレート：カスタマーの定義による Per VPN。カスタマー テンプレートは、ローカルで VHG に保存されます。この方式は、ドメイン名または着信番号識別サービス（DNIS）に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。
- リモートで定義されたカスタマーテンプレート：RADIUS プロファイルでサービス プロバイダーの AAA サーバに保存された、カスタマーの定義による Per VPN。この方式は、ドメイン名または DNIS に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。

（注） ローカルまたはリモートで定義されたカスタマー テンプレートを設定する機能は、Cisco IOS XE Release 2.4 以降のリリースでのみ使用できます。

AAA アカウンティング レコード

シスコが採用している AAA アカウンティングでは、ユーザ認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。開始レコードと終了レコードは、ユーザがアカウンティング レコードを使用してネットワークを管理およびモニタするために必要です。

新しいベンダー固有属性

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（VSA）属性 26 を使用してベンダー固有の情報を伝達する方法が規定されています。属性 26 は VSA をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。

シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は「cisco-avpair」）です。値は、次の形式のストリングです。

```
protocol : attribute sep value *
```

「protocol」は、特定の認可タイプに使用するシスコの「protocol」属性の値です。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。「sep」は、必須の属性の場合は「=」、任意指定の属性の場合は「*」です。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

次の表に、現在 Per VRF AAA でサポートされている VSA の概要を示します。

表 *29*：*Per VRF AAA* でサポートされる *VSA*

VSA 名	値の種類	説明
（注） 別の拡張子が明示的に記述されている場合を除き、各 VSA には VSA 名の前に拡張子「template:」が必要です。		

VSA 名	値の種類	説明
account-delay	string	この VSA は「on」にする必要があります。この VSA の機能は、カスタマー テンプレートの **aaaaccountingdelay-start** コマンドと同じです。
account-send-stop	string	この VSA は「on」にする必要があります。この VSA の機能は、**failure** キーワードを指定した **aaaaccountingsendstop-recordauthentication** コマンドと同じです。
account-send-success-remote	string	この VSA は「on」にする必要があります。この VSA の機能は、**success** キーワードを指定した **aaaaccountingsendstop-recordauthentication** コマンドと同じです。
attr-44	string	この VSA は「access-req」にする必要があります。この VSA の機能は、**radius-serverattribute44include-in-access-req** コマンドと同じです。
ip-addr	string	この VSA は、IP アドレスを指定します。その後に、ルータが独自の IP アドレスを示すために使用するマスク、およびクライアントとのネゴシエーションのマスクが続きます。例：ip-addr=192.168.202.169 255.255.255.255。
ip-unnumbered	string	この VSA は、ルータ上のインターフェイスの名前を指定します。この VSA の機能は、「Loopback 0」などのインターフェイス名を指定する **ipunnumbered** コマンドと同じです。

VSA 名	値の種類	説明
ip-vrf	string	この VSA は、エンドユーザのパケットに使用する VRF を指定します。この VRF 名は、**ipvrfforwarding** コマンドを使用してルータに使用する名前に一致させる必要があります。
peer-ip-pool	string	この VSA は、ピアに割り当てられるアドレスの IP アドレスプールの名前を指定します。このプールは、**iplocalpool** コマンドを使用して設定するか、RADIUS 経由で自動的にダウンロード可能にする必要があります。
ppp-acct-list	string	この VSA は、PPP セッションに使用するアカウンティング方式リストを定義します。 VSA 構文は次のとおりです。「ppp-acct-list=[start-stop | stop-only | none] group X [group Y] [broadcast]」これは、**aaaaccountingnetworkmylist** コマンド機能と等しくなります。 ユーザは、start-stop、stop-only、または none オプションを少なくとも 1 つ指定する必要があります。start-stop または stop-only を指定した場合、ユーザは少なくとも 1 つ、ただし 4 つ以内のグループ引数を指定する必要があります。各グループ名は、整数で構成する必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。各グループが指定されると、ユーザはブロードキャスト オプションを指定できます。

VSA 名	値の種類	説明
ppp-authen-list	string	この VSA は、PPP セッションで使用する認証方式リスト、および複数の方式が指定されている場合は、方式を使用する順序を定義します。 VSA 構文は次のとおりです。「ppp-authen-list=[groupX | local | local-case | none | if-needed]」これは、**aaaauthenticationpppmylist** コマンド機能と等しくなります。 ユーザは少なくとも 1 つ、ただし 4 つ以内の認証方式を指定する必要があります。サーバ グループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。
ppp-authen-type	string	この VSA を使用すると、エンドユーザは、pap、chap、eap、ms-chap、ms-chap-v2、any のいずれかの認証タイプ、または使用可能なタイプをスペースで区切って、少なくとも 1 つの認証タイプを指定できます。 エンド ユーザは、この VSA で指定された方式のみを使用して、ログインが許可されます。 PPP は属性で提示された順序で、これらの認証方式を試行します。

VSA 名	値の種類	説明
ppp-author-list	string	この VSA は、PPP セッションに使用する認可方式リストを定義します。使用する方式と順序を示します。 VSA 構文は次のとおりです。「ppp-author-list=[groupX] [local] [if-authenticated] [none]」これは、**aaaauthorizationnetworkmylist** コマンド機能に等しくなります。 ユーザは少なくとも 1 つ、ただし 4 つ以内の認可方式を指定する必要があります。サーバ グループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。
（注） RADIUS VSA（rad-serv、rad-serv-filter、rad-serv-source-if、および rad-serv-vrf）は、VSA 名の前にプレフィックス「aaa:」が必要です。		

VSA 名	値の種類	説明
rad-serv	string	この VSA は、サーバのグループとともに、IP アドレス、キー、タイムアウト、およびサーバの再送信回数を示します。 VSA 構文は次のとおりです。「rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W]」IP アドレス以外、すべてのパラメータはオプションで、任意の順序で発行できます。オプションのパラメータが指定されていない場合、デフォルト値が使用されます。 キーには、スペースを含めることはできません。「retransmit V」の「V」は、1 ～ 100 の値で、「timeout W」の「W」は 1 ～ 1000 の値です。
rad-serv-filter	string	VSA 構文は次のとおりです。「rad-serv-filter=authorization | accounting-request | reply-accept | reject-filtername」filtername は **radius-serverattributelistfiltername** コマンドを使用して定義する必要があります。 （注） この VSA は、Cisco IOS XE Release 2.3 以降のリリースでサポートされています。
rad-serv-source-if	string	この VSA は、RADIUS パケットの送信に使用するインターフェイスの名前を指定します。指定されたインターフェイスは、ルータ上に設定されたインターフェイスと一致する必要があります。

VSA 名	値の種類	説明
rad-serv-vrf	string	この VSA は、RADIUS パケットの送信に使用する VRF の名前を指定します。VRF 名は、**ipvrfforwarding** コマンドを使用して指定された名前と一致する必要があります。

VRF 認識 Framed-Route

Cisco IOS XE Release 2.3 以降では、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、VRF 認識 framed-route をサポートしています。この機能のサポートを有効にするために必要な設定はありません。framed-route は自動的に検出されます。framed-route がインターフェイスに関連付けられた VRF の一部である場合、ルートは適宜適用されます。

Per VRF AAA の設定方法

Per VRF AAA の設定

AAA の設定

AAA をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。

サーバ グループの設定

サーバ グループを設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaagroupserverradius***groupname*
5. **server-private***ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaagroupserverradius***groupname* 例： `Router(config)# aaa group server radius v2.44.com`	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。server-group コンフィギュレーション モードを開始します。
ステップ 5	**server-private***ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] 例： `Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww`	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。 （注） プライベート サーバ パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。
ステップ 6	**exit** 例： `Router(config-sg-radius)# exit`	server-group コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

Per VRF AAA の認証、許可、アカウンティングの設定

Per VRF AAA の認証、許可、アカウンティングを設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaauthenticationppp**{**default** | *list-name*} *method1* [*method2...*]
5. **aaaauthorization**{**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**}{**default** | *list-name*} *method1* [*method2...*]
6. **aaaaccountingsystemdefault**[**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
7. **aaaaccountingdelay-start**[**vrf** *vrf-name*]
8. **aaaaccountingsendstop-recordauthentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaaauthenticationppp**{**default**	*list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com`	PPP を実行しているシリアルインターフェイス上で使用する 1 つ以上の AAA 認証方式を指定します。
ステップ 5	**aaaauthorization**{**network**	**exec**	**commands** *level*	**reverse-access**	**configuration**}{**default**	*list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com`	ネットワークへのユーザアクセスを制限するパラメータを設定します。

	コマンドまたはアクション	目的
ステップ 6	**aaaaccountingsystemdefault**[**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* 例： `Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com`	課金、またはRADIUSを使用する際のセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。
ステップ 7	**aaaaccountingdelay-start**[**vrf** *vrf-name*] 例： `Router(config)# aaa acounting delay-start vrf v2.44.com`	ユーザの IP アドレスが確立されるまで、アカウンティング開始レコードの生成を表示します。
ステップ 8	**aaaaccountingsendstop-recordauthentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*] 例： `Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com`	アカウンティング終了レコードを生成します。 **failure** キーワードを使用すると、認証中に拒否されたコールに対する「終了」レコードが送信されます。 **success** キーワードを使用すると、次のいずれかの基準を満たすコールに対して、「終了」レコードが送信されます。 • コールが終了したときに、リモート AAA サーバによって認証されるコール。 • リモート AAA サーバによって認証されず、開始レコードが送信されたコール。 • 正常に確立され、「stop-only」**aaa accounting** 設定で終了したコール。 （注） **success** および **remote-server** キーワードは、Cisco IOS XE Release 2.4 以降のリリースで使用できます。

Per VRF AAA の RADIUS 固有のコマンドの設定

Per VRF AAA の RADIUS 固有のコマンドを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipradiussource-interface***subinterface-name* [**vrf** *vrf-name*]
4. **radius-serverattribute44include-in-access-req** [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ipradiussource-interface***subinterface-name* [**vrf** *vrf-name*] 例： `Router(config)# ip radius source-interface loopback55`	すべての発信 RADIUS パケットに対して、RADIUS に指定されたインターフェイスの IP アドレスを強制的に使用させ、Per VRF に基づいて仕様をイネーブルにします。
ステップ 4	**radius-serverattribute44include-in-access-req** [**vrf** *vrf-name*] 例： `Router(config)# radius-server attribute 44 include-in-access-req vrf v2.44.com`	ユーザ認証前に、アクセス要求パケットで、RADIUS 属性 44 を送信し、Per VRF に基づいて仕様を有効にします。

Per VRF AAA のインターフェイス固有のコマンドの設定

Per VRF AAA のインターフェイス固有のコマンドを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*[*name-tag*]
4. **ipvrfforwarding***vrf-name*
5. **pppauthentication** {*protocol1* [*protocol2...*]}*listname*
6. **pppauthorization***list-name*
7. **pppaccountingdefault**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber*[*name-tag*] 例： `Router(config)# interface loopback11`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipvrfforwarding***vrf-name* 例： `Router(config-if)# ip vrf forwarding v2.44.com`	インターフェイスと VRF を関連付けます。
ステップ 5	**pppauthentication** {*protocol1* [*protocol2...*]}*listname* 例： `Router(config-if)# ppp authentication chap callin V2_44_com`	チャレンジ ハンドシェイク認証プロトコル（CHAP）およびパスワード認証プロトコル（PAP）のいずれかまたは両方をイネーブルにし、CHAP および PAP 認証がインターフェイスで選択される順序を指定します。

	コマンドまたはアクション	目的
ステップ 6	**pppauthorization***list-name* 例： `Router(config-if)# ppp authorization V2_44_com`	選択したインターフェイスで、AAA 認可をイネーブルにします。
ステップ 7	**pppaccountingdefault** 例： `Router(config-if)# ppp accounting default`	選択したインターフェイスで、AAA アカウンティングサービスをイネーブルにします。
ステップ 8	**exit** 例： `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の設定

AAA の設定

「Per VRF AAA の設定」で説明する作業を実行します。

サーバ グループの設定

「サーバ グループの設定」で説明する作業を実行します。

Per VRF AAA の認証、許可、アカウンティングの設定

「Per VRF AAA の認証、許可、アカウンティングの設定」で説明する作業を実行します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の認可の設定

ローカルテンプレートを使用した Per VRF AAA の認可を設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaauthorizationtemplate**
4. **aaaauthorizationnetworkdefaultlocal**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaauthorizationtemplate** 例： `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaaauthorizationnetworkdefaultlocal** 例： `Router(config)# aaa authorization network default local`	ローカルを認可のデフォルト方式として指定します。

ローカル カスタマー テンプレートの設定

ローカル カスタマー テンプレートを設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnsearch-orderdomain**
4. **template***name*[**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]
5. **peerdefaultipaddresspool***pool-name*
6. **pppauthentication** {*protocol1* [*protocol2...*]}[**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
7. **pppauthorization** [**default** | *list-name*]
8. **aaaaccounting**{**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnsearch-orderdomain** 例： `Router (config)# vpdn search-order domain`	ドメインに基づいてプロファイルを検索します。
ステップ 4	**template***name*[**default**	**exit**	**multilink**	**no**	**peer**	**ppp**] 例： `Router (config)# template v2.44.com`	カスタマー プロファイル テンプレートを作成し、受信先のカスタマーに関連する一意の名前を割り当てます。 テンプレート コンフィギュレーション モードを開始します。 （注） ステップ 5、6、および 7 はオプションです。カスタマー アプリケーション要件に適した **multilink**、**peer**、および **ppp** キーワードを入力します。

	コマンドまたはアクション	目的
ステップ 5	**peerdefaultipaddresspool***pool-name* 例： `Router(config-template)# peer default ip address pool v2_44_com_pool`	（任意）このテンプレートの添付先のカスタマー プロファイルが、指定した名前のローカル IP アドレス プールを使用するように指定します。
ステップ 6	**pppauthentication** {*protocol1* [*protocol2...*]}[**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] 例： `Router(config-template)# ppp authentication chap`	（任意）PPP リンク認証方式を設定します。
ステップ 7	**pppauthorization** [**default** | *list-name*] 例： `Router(config-template)# ppp authorization v2_44_com`	（任意）PPP リンク認可方式を設定します。
ステップ 8	**aaaaccounting**{**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* 例： `Router(config-template)# aaa accounting v2_44_com`	（任意）指定したカスタマー プロファイルで、AAA 動作パラメータをイネーブルにします。
ステップ 9	**exit** 例： `Router(config-template)# exit`	テンプレート コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

リモート カスタマー テンプレートを使用した Per VRF AAA の設定

AAA の設定

「Per VRF AAA の設定」で説明する作業を実行します。

サーバ グループの設定

「サーバ グループの設定」で説明する作業を実行します。

リモート カスタマー プロファイルを使用した Per VRF AAA の認証の設定

リモート カスタマー プロファイルを使用した Per VRF AAA の認証を設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaauthenticationppp**{**default** | *list-name*} *method1* [*method2...*]
4. **aaaauthorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaauthenticationppp**{**default**	*list-name*} *method1* [*method2...*] 例： `Router(config)# ppp authentication ppp default group radius`	PPP を実行するシリアル インターフェイス上で使用する 1 つ以上の認証、許可、アカウンティング（AAA）認証方式を指定します。
ステップ 4	**aaaauthorization** {**network**	**exec**	**commands** *level*	**reverse-access**	**configuration**} {**default**	*list-name*} [[*method1* [*method2...*] 例： `Router(config)# aaa authorization network default group sp`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。

リモート カスタマー プロファイルを使用した Per VRF AAA の認可の設定

リモート カスタマー プロファイルを使用した Per VRF AAA の認可を設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaauthorizationtemplate**
4. **aaaauthorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaauthorizationtemplate** 例： `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaaauthorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] 例： `Router(config)# aaa authorization network default sp`	認可のデフォルト方式として指定されたサーバグループを指定します。

SP RADIUS サーバ上の RADIUS プロファイルの設定

サービス プロバイダー（SP）RADIUS サーバ上で RADIUS プロファイルを設定します。RADIUS プロファイルを更新する方法の例については、「リモート RADIUS カスタマーテンプレートを使用した Per VRF AAA の例」を参照してください。

VRF ルーティングの設定確認

VRF のルーティング設定を確認するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. show ip route vrf *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	show ip route vrf *vrf-name* 例： `Router(config)# show ip route vrf northvrf`	VRF に関連付けられた IP ルーティング テーブルを表示します。

Per VRF AAA 設定のトラブルシューティング

Per VRF AAA 機能の問題を解決するには、EXEC モードで次のコマンドを少なくとも 1 つ使用します。

コマンド	目的
`Router#` **debug aaa accounting**	説明の義務があるイベントが発生したときに、その情報を表示します。
`Router#` **debug aaa authentication**	AAA 認証に関する情報を表示します。
`Router#` **debug aaa authorization**	AAA 認可に関する情報を表示します。
`Router#` **debug ppp negotiation**	PPP を実装するインターネットワークでのトラフィックおよび交換に関する情報を表示します。
`Router#` **debug radius**	RADIUS 関連の情報を表示します。
`Router#` **debug vpdn event**	VPN の通常のトンネルの確立、またはシャットダウンの一部であるレイヤ 2 プロトコル（L2TP）のエラーおよびイベントを表示します。
`Router#` **debug vpdn error**	VPN のデバッグ トレースを表示します。

Per VRF AAA の設定例

Per VRF の設定の例

Per VRF AAA の例

次に、関連付けられたプライベート サーバで AAA サーバ グループを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
```

```
aaa accounting delay-start vrf v1.55.com
aaa accounting send stop-record authentication failure vrf v1.55.com
aaa group server radius v1.55.com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding v1.55.com
ip radius source-interface loopback55
radius-server attribute 44 include-in-access-req vrf v1.55.com
```

ローカルで定義されたカスタマー テンプレートを使用した Per VRF AAA の例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、ローカルで定義されたカスタマー テンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa authorization network default local
aaa authorization template
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa group server radius V1_55_com
  server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
  ip vrf forwarding V1.55.com
template V1.55.com
  peer default ip address pool V1_55_com_pool
  ppp authentication chap callin V1_55_com
  ppp authorization V1_55_com
  ppp accounting V1_55_com
  aaa accounting delay-start
  aaa accounting send stop-record authentication failure
  radius-server attribute 44 include-in-access-req
  ip vrf forwarding v1.55.com
  ip radius source-interface Loopback55
```

リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA の例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、SP RADIUS サーバ上にリモートで定義したカスタマーテンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp
aaa group server radius sp
   server 10.3.3.3
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646 key sp_key
```

次の RADIUS サーバ プロファイルは、SP RADIUS サーバ上で設定されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

カスタマー テンプレートの例

RADIUSAttributeScreeningおよびブロードキャストアカウンティングを使用してローカルで設定されたカスタマー テンプレートの例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにローカルで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authentication ppp V1_55_com group V1_55_com
aaa authorization template
aaa authorization network default local group radius
aaa authorization network V1_55_com group V1_55_com
aaa accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server
aaa group server radius SP_AAA_server
 server 10.10.100.7 auth-port 1645 acct-port 1646
aaa group server radius V1_55_com
 server-private 10.10.132.4 auth-port 1645 acct-port 1646
 authorization accept min-author
 accounting accept usage-only
 ip vrf forwarding V1.55.com
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
template V1.55.com
 peer default ip address pool V1.55-pool
 ppp authentication chap callin V1_55_com
 ppp authorization V1_55_com
 ppp accounting V1_55_com
 aaa accounting delay-start
 aaa accounting send stop-record authentication failure
 radius-server attribute 44 include-in-access-req
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 ip vrf forwarding V1.55.com
 ip unnumbered Loopback55
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
ip radius source-interface Loopback0
ip radius source-interface Loopback55 vrf V1.55.com
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
radius-server host 10.10.100.7 auth-port 1645 acct-port 1646 key ww
radius-server host 10.10.132.4 auth-port 1645 acct-port 1646 key ww
```

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してリモートで設定されたカスタマー テンプレートの例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにリモートで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authorization template
aaa authorization network default local group radius
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 no ip address
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

カスタマー テンプレートは、v1.55.com の RADIUS サーバ プロファイルとして保存されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "aaa:rad-serv#2=10.10.100.7 key ww"
cisco-avpair = "aaa:rad-serv-source-if#2=Loopback 0"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1 group 2 broadcast"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "aaa:rad-serv-filter#1=authorization accept min-author"
cisco-avpair = "aaa:rad-serv-filter#1=accounting accept usage-only"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

AAA アカウンティング終了レコードの例

次に、**start-stop** または **stop-only** キーワードを指定して **aaaaccounting** コマンドを発行したときに、「終了」レコードの生成を制御する **aaaaccountingsendstop-recordauthentication** コマンドを設定する方法を示す、AAA アカウンティング終了レコードの例を示します。

（注） **success** および **remote-server** キーワードは、Cisco IOS XE Release 2.4 以降のリリースで使用できます。

AAA アカウンティング終了レコードと拒否されたコールの例

次に、**aaa accounting send stop-record authentication** コマンドを **success** キーワードを指定して発行した場合に、認証中に拒否されたコールに関する「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius
Router#
*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                              [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                    [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 172.19.192.238:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
```

```
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=10.0.0.2"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
172.19.192.238:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                    [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                    [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                     [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                  [9]
```

```
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                      [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

AAA アカウンティング終了レコードと成功したコールの例

次に、**aaa accounting send stop-record authentication** コマンドを **failure** キーワードを指定して発行した場合に、成功したコールに関する「開始」および「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa

.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
```

```
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 10.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                     [2]
```

```
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

その他の参考資料

ここでは、Per VRF AAA に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
サーバ グループの設定	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring RADIUS」の章
RADIUS 属性スクリーニング	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「RADIUS Attribute Value Screening」の章
ブロードキャスト アカウンティングの設定	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring Accounting」の章
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
Cisco IOS Switching Services コマンド	『*Cisco IOS IP Switching Command Reference*』
マルチプロトコル ラベル スイッチングの設定	『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*, Release 2』
仮想テンプレートの設定	『*Cisco IOS XE Dial Technologies Configuration Guide*, Release 2』の「Virtual Templates and Profiles」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Per VRF AAA の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *30*：*Per VRF AAA* の機能情報

機能名	リリース	機能情報
Per VRF AAA	Cisco IOS XE Release 2.1	Per VRF AAA 機能により、バーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスに基づいた、認証、許可、アカウンティング（AAA）が行えます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaaaccounting**、**aaaaccountingdelay-start**、**ipradiussource-interface**、**server-private**（**RADIUS**）、**ipvrfforwarding**（**server-group**）、**radius-serverdomain-stripping**、**aaaauthorizationtemplate**。
RADIUS Per-VRF サーバ グループ	Cisco IOS XE Release 2.1	RADIUS Per-VRF サーバ グループ機能を使用して、インターネット サービス プロバイダー（ISP）は、Virtual Route Forwarding（VRF）に基づいて RADIUS サーバ グループを分割できます。つまり、VRF に属する RADIUS サーバ グループを定義することができます。この機能は、「aaa: rad-serv-vrf」の VSA によってサポートされています。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**ipvrfforwarding**。

機能名	リリース	機能情報
Attribute Filtering Per-Domain and VRF Aware Framed-Routes	Cisco IOS XE Release 2.3	Attribute Filtering Per-Domain and VRF Aware Framed-Routes 機能により、ドメイン単位の属性フィルタリングおよび VRF 認識 Framed-Route が可能です。これにより「aaa:rad-serv-filter」の VSA のサポートが追加されます。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。
AAA CLI レコード停止機能拡張	Cisco IOS XE Release 2.4	AAA CLI レコード停止機能拡張機能により、AAA サーバから Access Accept を受信する場合にのみアカウンティング終了レコードが送信されます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。 **aaaaccountingsendstop-recordauthentication**。
Dynamic Per VRF AAA	Cisco IOS XE Release 2.4	Dynamic Per VRF AAA 機能により、ローカルまたはリモートで保存したカスタマーテンプレートを使用し、カスタマー テンプレートに保存された情報に基づいて、AAA サービスを実行できます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

AAA：認証、許可、アカウンティング。セキュリティ サービスのフレームワークであり、ユーザの身元確認（認証）、リモートアクセスコントロール（許可）、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信（アカウンティング）の方式を定めています。

L2TP：Layer 2 Tunnel Protocol。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

PE：プロバイダー エッジ。サービス プロバイダー ネットワークのエッジ上のネットワーキング デバイス。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：バーチャル プライベート ネットワーク リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

VRF：Virtual Route Forwarding。最初は、ルータにグローバルのデフォルト ルーティング/フォワーディング テーブルは 1 つしかありません。VRF は、複数の分離されたルーティング/フォワーディング テーブルとして表示でき、ユーザのルートには別のユーザのルートとの相互関係はありません。

第 14 章

AAA の IPv6 サポート

IPv6 用の認証、許可、アカウンティング（AAA）サポートは RFC 3162 に準拠しています。このモジュールでは、IPv6 用の AAA オプションの設定方法を示します。

- 機能情報の確認，247 ページ
- AAA の IPv6 サポートに関する情報，248 ページ
- IPv6 用の AAA サポートの設定方法，252 ページ
- AAA の IPv6 サポートの設定例，254 ページ
- その他の参考資料，254 ページ
- RADIUS over IPv6 の機能情報，256 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA の IPv6 サポートに関する情報

AAA over IPv6

ベンダー固有属性（VSA）を使用して、IPv6 を介して認証、許可、アカウンティング（AAA）をサポートします。Cisco VSA は、inacl、outacl、prefix、および route です。

AAA プロトコルを使用して、プレフィックス プールおよびプール名を設定できます。お客様は、シスコ デバイスと通信するために IPv6 RADIUS サーバまたは TACACS+ サーバを導入できます。

IPv6 RADIUS 属性の AAA サポート

RFC 3162 で説明されているように、IPv6 では次の RADIUS 属性がサポートされます。

- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Login-IPv6-Host

IPv6 では、次の RADIUS 属性がサポートされます。

- Delegated-IPv6-Prefix（RFC 4818）
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route

上記の属性は、RADIUS サーバで設定して、アクセス サーバにダウンロードして、ここでアクセス接続に適用できます。

IPv6 の AAA 属性を使用するための前提条件

IPv6 の AAA 属性は RFC 3162 に準拠しており、RFC 3162 をサポートできる RADIUS サーバを必要とします。

IPv6 環境での仮想アクセス用の RADIUS ユーザ単位属性

仮想アクセスでは次の IPv6 RADIUS 属性がサポートされ、属性と値（AV）のペアとして使用できます。

- Delegated-IPv6-Prefix
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route
- Login-IPv6-Host

Delegated-IPv6-Prefix

Delegated-IPv6-Prefix 属性は、ネットワークで使用されるユーザに委任される IPv6 プレフィックスを示します。この属性は、RADIUS サーバと委託デバイスの間の DHCP プレフィックス委任中に使用されます。DHCP バージョン 6（DHCPv6）サーバをホストするネットワーク アクセス サーバ（NAS）は、委託デバイスとして動作できます。

次に、Delegated-IPv6-Prefix 属性を使用する例を示します。

```
ipv6:delegated-prefix=2001:DB8::/64
```

（注） この属性では Cisco VSA 形式はサポートされません。この属性を Cisco VSA 形式でユーザ プロファイルに追加しようとすると、RADIUS サーバの応答に失敗します。この属性に使用するのは IETF 属性形式のみです。

Delegated-IPv6-Prefix-Pool

Delegated-IPv6-Prefix-Pool 属性は、プレフィックスが選択され、デバイスに委任されるプレフィックス プールの名前を示します。

プレフィックス委任は IPv6 プレフィックスを委任するための DHCPv6 オプションです。プレフィックス委任には、プレフィックスを選択し、それを要求側のデバイスに一時的に割り当てる委託デバイスが関与します。委任デバイスは、プレフィックスを選択するために多くの戦略を使用しま

す。1 つの方法では、デバイス上でローカルに定義されている名前のプレフィックス プールからプレフィックスを選択します。

Delegated-IPv6-Prefix-Pool 属性は、割り当てられたプレフィックス プールの名前を示します。RADIUS サーバは、この属性を使用して、DHCPv6 サーバをホスティングして、委託デバイスとして動作する NAS にプレフィックス プールの名前を知らせます。

ネットワークで、DHCPv6 プレフィックス委任と ICMPv6 ステートレス アドレス自動設定を共に使用してもかまいません。この場合、Delegated-IPv6-Prefix-Pool 属性と Framed-IPv6-Pool 属性の両方を同じパケット内に含めることができます。曖昧さを回避するために、Delegated-IPv6-Prefix-Pool を DHCPv6 委任で使用されるプレフィックス プールの認可およびアカウンティングに制限して、Framed-IPv6-Pool 属性を SLAAC で使用されるプレフィックス プールの認可およびアカウンティングに使用する必要があります。

次に、アドレス プレフィックスが pool1 という名前のプールから選択される例を示します。プレフィックス プール pool1は、Delegated-IPv6-Prefix-Pool 属性を使用して、RADIUS サーバから委託デバイスにダウンロードされます。次にデバイスは、このプレフィックスプールからアドレスプレフィックス 2001:DB8::/64 を選択します。

```
Cisco:Cisco-AVpair = “ipv6:delegated-ipv6-pool = pool1”
!
ipv6 dhcp pool pool1
address prefix 2001:DB8::/64
!
```

DNS-Server-IPv6-Address

DNS-Server-IPv6-Address 属性は、ドメイン ネーム システム（DNS）サーバの IPv6 アドレスを示します。DHCPv6 サーバは、DNS サーバの IPv6 アドレスを持つホストを設定できます。DNS サーバの IPv6 アドレスを、ICMPv6 デバイスからルータ アドバタイズメント メッセージを使用してホストに伝送することもできます。

NAS は、ホストからの DHCPv6 要求を処理する DHCPv6 サーバをホストすることがあります。また NAS は、ルータ アドバタイズメント メッセージを提供するデバイスとして機能することもあります。したがって、この属性は DNS サーバの IPv6 アドレスを NAS に提供するために使用されます。

NAS がホストに複数の再帰 DNS サーバを通知する必要がある場合、この属性を NAS からホストに送信される Access-Accept パケットに複数回含めることができます。

次に、DNS-Server-IPv6-Address 属性を使用して DNS サーバの IPv6 アドレスを定義する例を示します。

```
Cisco:Cisco-AVpair = "ipv6:ipv6-dns-servers-addr=2001:DB8::"
```

Framed-Interface-Id

Framed-Interface-Id 属性は、ユーザ用に設定する IPv6 インターフェイス ID を示します。

この属性は、Interface-Identifier オプションの IPv6 制御プロトコル（IPv6CP）ネゴシエーション中に使用されます。ネゴシエーションに成功すると、NAS はこの属性を使用して、推奨される IPv6 インターフェイス識別子を Access-Request パケットを使用して RADIUS サーバに知らせます。この属性は、Access-Accept パケットで使用されることもあります。

Framed-IPv6-Pool

Framed-IPv6-Pool 属性は、ユーザに IPv6 プレフィックスを割り当てるために使用するプールの名前を示します。このプールは、デバイスでローカルに定義するか、プールをダウンロードできる RADIUS サーバで定義する必要があります。

Framed-IPv6-Prefix

Framed-IPv6-Prefix 属性は、ユーザ用に設定する IPv6 プレフィックス（および対応するルート）を示します。そのため、この属性は Cisco VSA と同じ機能を実行し、仮想アクセスのみに使用されます。NAS はこの属性を使用して、推奨される IPv6 プレフィックスを Access-Request パケットを使用して RADIUS サーバに知らせます。この属性は Access-Accept で使用されることもあり、これらのパケットで複数回出現することがあります。NAS では、プレフィックスの対応ルートが作成されます。

この属性は、Neighbor Discovery Protocol のルータ アドバタイズメント メッセージでアドバタイズするプレフィックスを指定するために、ユーザによって使用されます。

この属性は DHCPv6 プレフィックス委任にも使用でき、RADIUS サーバのユーザ用には別のプロファイルを作成する必要があります。この別のプロファイルに関連付けられたユーザ名には、サフィックス「-dhcpv6」が付いています。

Framed-IPv6-Prefix 属性の処理は、この別のプロファイルとユーザの通常のプロファイルでは異なります。NAS がルータ アドバタイズメント メッセージを使用してプレフィックスを送信する必要がある場合、プレフィックスは、ユーザの通常のプロファイルの Framed-IPv6-Prefix 属性に配置されます。NAS がリモートユーザのネットワークにプレフィックスを委任する必要がある場合、プレフィックスはユーザの別のプロファイルの Framed-IPv6-Prefix 属性に配置されます。

（注） この属性では、RADIUS IETF 属性形式と Cisco VSA 形式がサポートされます。

Framed-IPv6-Route

Framed-IPv6-Route 属性は、NAS のユーザ用に設定されるルーティング情報を示します。この属性は Cisco VSA と同じ機能を実行します。属性の値は文字列であり、**ipv6 route** コマンドを使用して指定します。

IPv6 ACL

IPv6 ACL 属性は、完全な IPv6 アクセス リストを指定するために使用されます。アクセス リストの一意の名前が自動的に生成されます。アクセス リストは、各ユーザがログアウトしたときに削除されます。インターフェイス上の以前のアクセス リストが再適用されます。

inacl 属性と outacl 属性を使用すると、デバイスに特定の既存のアクセス リストを設定できます。次に、番号 1 で識別されるアクセス リストを定義する例を示します。

```
cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:outacl#1=deny 2001:DB8::/10",
```

IPv6_DNS_Servers

IPv6_DNS_Servers 属性は、最大 2 つの DNS サーバ アドレスを DHCPv6 サーバに送信するために使用されます。DNS サーバ アドレスは、インターフェイス DHCPv6 サブブロックに保存され、DHCPv6 プールの他の設定よりも優先されます。この属性は、AAA の開始および終了通知に対して返される属性にも含まれます。

IPv6 Pool

IPv6 Pool 属性は、RADIUS 認証の IPv6 プロトコルをサポートするために IPv4 アドレス プール属性を拡張します。この属性は、プレフィックスの選択元の NAS 上のローカル プールの名前を指定します。そして PPP を設定するときとプロトコルを IPv6 と指定するときに使用されます。アドレス プールはローカル プーリングで使用でき、NAS 上に事前に設定されたローカル プールの名前を指定します。

IPv6 Prefix#

IPv6 Prefix# 属性は、Neighbor Discovery Protocol のルータ アドバタイズメント メッセージでアドバタイズするプレフィックスを示します。この属性が使用されている場合は、対応するルート（ユーザ単位のスタティック ルートとしてマークされています）が、特定のプレフィックスのルーティング情報ベース（RIB）テーブルにインストールされます。

次に、アドバタイズするプレフィックスを指定する例を示します。

```
cisco-avpair = "ipv6:prefix#1=2001:DB8::/64",
cisco-avpair = "ipv6:prefix#2=2001:DB8::/64",
```

IPv6 Route

IPv6 Route 属性は、ユーザ用のスタティック ルートを指定するために使用されます。スタティック ルートが適切なのは、シスコのソフトウェアが宛先へのルートを動的に作成できない場合です。スタティック ルートの作成の詳細については、**ipv6route** コマンドを参照してください。

次に、スタティック ルートの定義で IPv6 route 属性を使用する例を示します。

```
cisco-avpair = "ipv6:route#1=2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:route#2=2001:DB8:cc00:2::/48",
```

Login-IPv6-Host

Login-IPv6-Host 属性は、Login-Service 属性が含まれている場合のユーザの接続先のホストの IPv6 アドレスを示します。NAS は、あるホストの使用を推奨する RADIUS サーバとの通信のために、Access-Request パケット内の Login-IPv6-Host 属性を使用します。

IPv6 用の AAA サポートの設定方法

DHCPv6 AAA オプションの設定

次のタスクを実行して、AAA サーバからプレフィックスを取得するオプションを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6dhcppool***pool-name*
4. **prefix-delegation aaa** [**method-list***method-list*] [*lifetime*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6dhcppool***pool-name* 例： `Device(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、IPv6 DHCP プール コンフィギュレーション モードを開始します。
ステップ 4	**prefix-delegation aaa** [**method-list***method-list*] [*lifetime*] 例： `Device(config-dhcpv6)# prefix-delegation aaa method-list list1`	プレフィックスを AAA サーバから取得することを指定します。
ステップ 5	**end** 例： `Device(config-dhcpv6)# end`	IPv6 DHCP プール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AAA の IPv6 サポートの設定例

例：DHCPv6 AAA オプションの設定

次に、AAA サーバからプレフィックスを取得する DHCPv6 オプションを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# prefix-delegation aaa method-list list1
Device(config-dhcpv6)# end
```

例：RADIUS の設定

次の RADIUS 設定例は、スタティック ルートを確立するための AV ペアの定義を示します。

```
campus1 Auth-Type = Local, Password = "mypassword"
                User-Service-Type = Framed-User,
                Framed-Protocol = PPP,
                cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:1::/64 any",
                cisco-avpair = "ipv6:route=2001:DB8:2::/64",
                cisco-avpair = "ipv6:route=2001:DB8:3::/64",
                cisco-avpair = "ipv6:prefix=2001:DB8:2::/64 0 0 onlink autoconfig",
                cisco-avpair = "ipv6:prefix=2001:DB8:3::/64 0 0 onlink autoconfig",
                cisco-avpair = "ip:route=10.0.0.0 255.0.0.0",
```

その他の参考資料

ここでは、認可機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
認可コマンド	『*Cisco IOS Security Command Reference*』
RADIUS	「RADIUS の設定」機能モジュール。
LDAP	「RADIUS の設定」機能モジュール。
RADIUS 属性	「RADIUS 属性の概要および RADIUS IETF 属性」機能モジュール。
TACACS+	「Configuring TACACS+」機能モジュール。
TACACS+ 属性値ペア	「TACACS+ Attribute-Value Pairs」機能モジュール。

関連項目	マニュアル タイトル
認証	「認証の設定」機能モジュール
認証プロキシ	「Configuring Authentication Proxy」機能モジュール。

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS over IPv6 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *31*：***RADIUS over IPv6*** の機能情報

機能名	リリース	機能情報
RADIUS over IPv6	15.1(1)SY	RFC 3162 に定義されている RADIUS 属性。

第 15 章

TACACS+ over IPv6

IPv6 サーバは、TACACS+ と共に使用するよう設定できます。

- 機能情報の確認，257 ページ
- TACACS+ over IPv6 に関する情報，257 ページ
- TACACS+ over IPv6 の設定方法，258 ページ
- TACACS+ over IPv6 の設定例，262 ページ
- その他の参考資料，262 ページ
- TACACS+ over IPv6 の機能情報，264 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

TACACS+ over IPv6 に関する情報

Terminal Access Controller Access Control System（TACACS+）セキュリティ プロトコルはユーザの検証を集中的に行います。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。デバイスに設定した TACACS+ 機能を有効にするには、その前に、TACACS+ サーバにアクセスして TACACS+ サーバを設定する必要があります。

TACACS+では、認証、許可、アカウンティングの各ファシリティを個別に提供します。TACACS+を使用すると、単一のアクセス コントロール サーバ（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）を個別に提供できます。各サービスは固有のデータベースにアソシエートされており、デーモンの機能に応じて、そのサーバまたはネットワーク上で使用可能な他のサービスを利用できます。

AAA over IPv6

ベンダー固有属性（VSA）を使用して、IPv6を介して認証、許可、アカウンティング（AAA）をサポートします。Cisco VSA は、inacl、outacl、prefix、および route です。

AAAプロトコルを使用して、プレフィックスプールおよびプール名を設定できます。お客様は、シスコ デバイスと通信するためにIPv6 RADIUS サーバまたはTACACS+ サーバを導入できます。

IPv6 トランスポートを介した TACACS+

IPv6 サーバは、TACACS+ を使用するよう設定できます。IPv4 または IPv6 アドレスの代わりに名前を使用して、TACACS+ を使用するよう IPv6 と IPv4 の両方のサーバを設定できます。

TACACS+ over IPv6 の設定方法

IPv6 を介した TACACS+ サーバの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **tacacsserver***name*
4. **addressipv6***ipv6-address*
5. **key** [**0** | **7**] *key-string*
6. **port** [*number*
7. **send-nat-address**
8. **single-connection**
9. **timeout***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**tacacsserver***name* 例： `Device(config)# tacacs server server1`	IPv6 に対して TACACS+ サーバを設定して、TACACS+ サーバ コンフィギュレーション モードを開始します。
ステップ 4	**addressipv6***ipv6-address* 例： `Device(config-server-tacacs)# address ipv6 2001:DB8:3333:4::5`	TACACS+ サーバの IPv6 アドレスを設定します。
ステップ 5	**key** [**0** | **7**] *key-string* 例： `Device(config-server-tacacs)# key 0 key1`	TACACS+ サーバでサーバ単位の暗号キーを設定します。
ステップ 6	**port** [*number* 例： `Device(config-server-tacacs)# port 12`	TACACS+接続に使用する TCP ポートを指定します。
ステップ 7	**send-nat-address** 例： `Device(config-server-tacacs)# send-nat-address`	クライアントの NAT 後のアドレスを TACACS+ サーバに送信します。

	コマンドまたはアクション	目的
ステップ 8	**single-connection** 例： `Device(config-server-tacacs)# single-connection`	単一の TCP 接続を使用してすべての TACACS パケットを同じサーバに送信できるようにします。
ステップ 9	**timeout***seconds* 例： `Device(config-server-tacacs)# timeout 10`	指定された TACACS サーバからの応答を待機する時間を設定します。

TACACS+ パケットでの送信元アドレスの指定

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6tacacssource-interface***typenumber*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ipv6tacacssource-interface***typenumber* 例： `Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0`	TACACS+ パケットで送信元アドレスに使用するインターフェイスを指定します。

TACACS+ サーバ グループ オプションの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **aaagroupservertacacs+***group-name*
4. **servername***server-name*
5. **server-private**{*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port***port-number*] [**timeout***seconds*] [**key** [**0** | **7**] *string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaagroupservertacacs+***group-name* 例： `Device(config)# aaa group server tacacs+ group1`	各種の TACACS+ サーバ ホストを別個のリストと別個の方式にグループ化します。
ステップ 4	**servername***server-name* 例： `Device(config-sg-tacacs+)# server name server1`	IPv6 TACACS+ サーバを指定します。
ステップ 5	**server-private**{*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port***port-number*] [**timeout***seconds*] [**key** [**0** | **7**] *string*]	グループ サーバに対するプライベート TACACS+ サーバの IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
	例： `Device(config-sg-tacacs+)# server-private 2001:DB8:3333:4::5 port 19 key key1`	

TACACS+ over IPv6 の設定例

例：IPv6 を介した TACACS+ サーバの設定

```
Device# show tacacs

            Tacacs+ Server:          server1
            Server Address:          FE80::200:F8FF:FE21:67CF
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
           Socket Timeouts:          0
   Failed Connect Attempts:          0
        Total Packets Sent:          0
        Total Packets Recv:          0
```

その他の参考資料

ここでは、MSCHAP バージョン 2 の機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
PPP インターフェイスの設定	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」
シスコのネットワーキング装置の設定および管理に必要なタスクとコマンドの説明	『*Cisco IOS Dial Technologies Command Reference*』
IOS セキュリティ コマンドの一覧	『*Cisco IOS Security Command Reference*』
AAA を使用した PPP 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T』の「Configuring Authentication」モジュールの「Configuring PPP Authentication Using AAA」

関連項目	マニュアル タイトル
RADIUS 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』の「Configuring RADIUS」モジュール

標準

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1661	ポイントツーポイント プロトコル（*PPP*）
RFC 2548	『*Microsoft Vendor-specific RADIUS Attributes*』
RFC 2759	「*Microsoft PPP CHAP Extensions, Version 2*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

TACACS+ over IPv6 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *32*：***TACACS+ over IPv6*** の機能情報

機能名	リリース	機能情報
TACACS+ over IPv6	Cisco IOS XE Release 3.2S	TACACS+ over IPv6 がサポートされます。 次のコマンドが導入または変更されました。**aaa group server tacacs+**、**address ipv6**（**TACACS+**）、**ipv6 tacacs source-interface**、**key**（**TACACS+**）、**port**（**TACACS+**）、**send-nat-address**、**server name**（**IPv6 TACACS+**）、**server-private**（**TACACS+**）、**single-connection**、**tacacs server**、**timeout**（**TACACS+**）。

第 16 章

AAA Dead-Server Detection

AAA Dead-Server Detection 機能を使用すると、RADIUS サーバをデッド状態と指定するための条件を設定できます。条件が明示的に設定されていない場合は、条件は未処理のトランザクションの数に基づいて動的に計算されます。この機能を使用すると、デッドタイムが短くなり、パケット処理が高速になります。

- 機能情報の確認，267 ページ
- AAA Dead-Server Detection の前提条件，268 ページ
- AAA Dead-Server Detection の制約事項，268 ページ
- AAA Dead-Server Detection について，268 ページ
- AAA Dead-Server Detection の設定方法，269 ページ
- AAA Dead-Server Detection の設定例，271 ページ
- その他の参考資料，272 ページ
- AAA Dead-Server Detection の機能情報，274 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA Dead-Server Detection の前提条件

- RADIUS サーバにアクセスできる必要があります。
- RADIUS サーバの設定方法を十分理解していることが必要です。
- 認証、許可、アカウンティング（AAA）の設定方法を十分理解していることが必要です。
- あるサーバをデッド状態と指定するためには、まず **radius-server deadtime** コマンドを設定する必要があります。このコマンドを設定していない場合は、サーバをデッド状態と指定するための条件に適合していても、サーバは「アップ」状態になります。

AAA Dead-Server Detection の制約事項

- サーバがデッド状態と指定されるまでにルータで発生する必要がある連続タイムアウト回数には、最初の転送は含まれません。つまり、再転送の回数のみがカウントされます。

AAA Dead-Server Detection について

RADIUS サーバをデッド状態と指定するための条件

AAA Dead-Server Detection 機能を使用すると、RADIUS サーバをデッド状態と指定するための条件を決定できます。つまり、ルータが RADIUS サーバから有効なパケットを最後に受け取ってから RADIUS サーバがデッド状態と指定されるまでに経過する必要がある最低時間を秒単位で設定することができます。ルータの起動後にパケットを受信せずにタイムアウトになった場合は、この時間の条件は満たされたものとして処理されます。

さらに、RADIUS サーバがデッド状態と指定されるまでにルータで発生する必要がある連続タイムアウト回数を設定することもできます。サーバが認証とアカウンティングの両方を実行する場合、両方の種類のパケットがこの回数に含まれます。正しく作成されていないパケットは、タイムアウトになっているものとしてカウントされます。カウントされるのは再転送だけで、最初の転送はカウントされません。（タイムアウトになるたびに再転送が 1 回行われることになります）。

（注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

RADIUS Dead-Server Detection を設定すると、応答を停止している RADIUS サーバが即時検出されます。また、サーバが「動きが鈍い」（応答が遅い）状態になっているときに誤ってデッド状態と指定されなくなるほか、デッド状態からライブ状態になってすぐにまたデッド状態になる現象

を回避できます。この未応答 RADIUS サーバの即時検出、動きが鈍いサーバの誤検出の回避、デッド状態とライブ状態を繰り返す現象の回避が有効になると、デッドタイムが短くなり、パケット処理が高速になります。

AAA Dead-Server Detection の設定方法

AAA Dead-Server Detection の設定

AAA Dead-Server Detection を設定する手順は、次のとおりです。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **radius-serverdeadtime***minutes*
5. **radius-serverdead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router (config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**radius-serverdeadtime***minutes* 例： `Router (config)# radius-server deadtime 5`	いくつかのサーバが使用不能になったときの RADIUS サーバの応答時間を短くし、使用不能になったサーバがすぐにスキップされるようにします。

	コマンドまたはアクション	目的
ステップ 5	**radius-serverdead-criteria** [**time** *seconds*] [**tries** *number-of-tries*] 例： `Router (config)# radius-server dead-criteria time 5 tries 4`	RADIUS サーバをデッド状態と指定するための条件のいずれかまたは両方を、指定した定数で適用します。

トラブルシューティングのヒント

AAA Dead-Server Detection を設定したら、**show running-config** コマンドを使用して、その設定を確認してください。この確認が特に重要になるのは、**no** 形式の **radius-server dead-criteria** コマンドを使用している場合です。**show running-config** コマンドの出力は、**radius-server dead-criteria** コマンドを使用して設定した「Dead Criteria Details」フィールドと同じ値を示している必要があります。

AAA Dead-Server Detection の確認

AAA Dead-Server Detection の設定を確認する手順は、次のとおりです。**show** コマンドと **debug** コマンドは、どの順序で使用してもかまいません。

手順の概要

1. **enable**
2. **debugaaadead-criteriatransactions**
3. **showaaadead-criteria**
4. **showaaaservers** [**private** | **public**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**debugaaadead-criteriatransactions** 例： `Router# debug aaa dead-criteria transactions`	デッド条件の AAA トランザクションの値を表示します。
ステップ 3	**showaaadead-criteria** 例： `Router# show aaa dead-criteria`	AAA サーバのデッド条件に関する情報を表示します。
ステップ 4	**showaaaservers** [**private** | **public**] 例： `Router# show aaa server private`	パブリックおよびプライベートのすべての認証、許可、アカウンティング（AAA）RADIUS サーバとの間で送受信されたパケットのステータスと数を表示します。 • **private** キーワードを付けると、プライベート AAA サーバのみについて表示されます。 • **public** キーワードを付けると、パブリック AAA サーバのみについて表示されます。

AAA Dead-Server Detection の設定例

AAA Dead-Server Detection の設定の例

次の例では、5 秒後および 4 回の試行後にルータがデッド状態と見なされます。

```
Router (config)# aaa new-model
Router (config)# radius-server deadtime 5
Router (config)# radius-server dead-criteria time 5 tries 4
```

debug aaa dead-criteria transactions コマンドの例

次の出力例は、特定のサーバ グループのデッド条件のトランザクションに関する情報を示しています。

```
Router# debug aaa dead-criteria transactions
AAA Transaction debugs debugging is on
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 22, Current Max Tries: 22
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 25s, Current Max
Interval: 25s
```

```
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transactions: 6, Current Max
Transactions: 6
```

show aaa dead-criteria コマンドの例

次の出力例は、IP アドレス 172.19.192.80 の RADIUS サーバに対してデッド サーバ検出に関する情報が要求されたことを示しています。

```
Router# show aaa dead-criteria radius 172.19.192.80 radius
RADIUS Server Dead Criteria:
============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

その他の参考資料

ここでは、AAA Dead-Server Detection 機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
RADIUS の設定	「RADIUS の設定」機能モジュール。
AAA の設定	認証の設定
	認可の設定
	アカウンティングの設定
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『*Remote Authentication Dial In User Service (RADIUS)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

AAA Dead-Server Detection の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *33*：***AAA Dead-Server Detection*** の機能情報

機能名	リリース	機能情報
AAA Dead-Server Detection	Cisco IOS XE Release 3.9S	RADIUS サーバをデッド状態と指定するための条件を設定できます。 次のコマンドが導入または変更されました。 **debugaaadead-criteriatransactions**、**radius-serverdead-criteria**、**showaaadead-criteria**、**showaaaservers**。

第 17 章

Login Password Retry Lockout

Login Password Retry Lockout 機能により、システム管理者はユーザによるログイン試行が設定した回数失敗すると、ローカルの認証、許可、アカウンティング（AAA）ユーザアカウントをロックアウトできます。

第 18 章

MSCHAP バージョン 2

Cisco IOS リリース 12.2(2)XB5 で導入された MSCHAP バージョン 2 機能を使用すると、Cisco ルータは、Microsoft Windows オペレーティング システムを使用するコンピュータとネットワーク アクセス サーバ（NAS）間の PPP 接続にマイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン 2（MSCHAP V2）の認証を使用できます。

Cisco IOS リリース 12.4(6)T では、MSCHAP V2 が新機能をサポートするようになりました。これを MSCHAPv2 のパスワード エージングの AAA でのサポートと呼びます。Cisco IOS リリース 12.4(6)T よりも前のバージョンでは、パスワード認証プロトコル（PAP）ベースのクライアントが認証、許可、アカウンティング（AAA）サブシステムにユーザ名とパスワードの値を送信すると、AAA が RADIUS サーバへの認証要求を生成していました。パスワードが失効している場合は、RADIUS サーバにより認証失敗のメッセージが返信されますが、認証が失敗した理由は AAA サブシステムには渡されていませんでした。そのため、認証が失敗したためにユーザはアクセスを拒否されますが、アクセスが拒否された理由は通知されませんでした。

Cisco IOS リリース 12.4(6)T で使用可能になったパスワード エージング機能は、パスワードが失効したことをクリプトベースのクライアントに通知し、ユーザがパスワードを変更するための一般的な方法を提供します。パスワード エージング機能では、クリプトベースのクライアントのみをサポートします。

- 機能情報の確認，278 ページ
- MSCHAP バージョン 2 の前提条件，278 ページ
- MSCHAP バージョン 2 の制約事項，279 ページ
- MSCHAP バージョン 2 の概要，279 ページ
- MSCHAP バージョン 2 の設定方法，279 ページ
- 設定例，284 ページ
- その他の参考資料，285 ページ
- MSCHAP バージョン 2 の機能情報，287 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

MSCHAP バージョン 2 の前提条件

- **interface** コマンドを使用してインターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
- **encapsulation** コマンドを使用して、PPP をカプセル化するためのインターフェイスを設定します。
- クライアントのオペレーティング システムが MSCHAP V2 のすべての機能をサポートしていることを確認してください。
- Cisco IOS リリース 12.4(6)T のパスワード エージング機能は、クリプトベースのクライアントの RADIUS 認証のみをサポートします。
- RADIUS サーバが送信する認証失敗属性を MSCHAP バージョン 2 機能が正しく解釈していることを確認するには、**pppmax-bad-auth** コマンドを設定し、認証のリトライ回数を 2 回以上に設定する必要があります。

また、**radiusservervsasendauthentication** コマンドを設定し、RADIUS クライアントがベンダー固有属性をRADIUSサーバに送信できるようにする必要があります。パスワード変更機能は、RADIUS 認証のみでサポートされています。

- Microsoft Windows 2000、Microsoft Windows XP、および Microsoft Windows NT のオペレーティング システムには、パスワード変更機能の動作を妨げる既知の注意事項があります。次の URL で Microsoft のパッチをダウンロードする必要があります。

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770

これらのタスクの実行の詳細については、『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」を参照してください。RADIUS サーバで認証を設定する必要があります。RADIUS サーバでの RADIUS 認証の設定の詳細については、ベンダー固有のマニュアルを参照してください。

MSCHAP バージョン 2 の制約事項

- MSCHAP V2 の認証は、MSCHAP V1 の認証と互換性がありません。
- パスワード変更オプションはRADIUS認証のみでサポートされており、ローカル認証では使用できません。

MSCHAP バージョン 2 の概要

MSCHAP V2 の認証は、Microsoft Windows 2000 オペレーティング システムが使用するデフォルトの認証方式です。この認証方式をサポートする Cisco ルータを使用すると、Microsoft Windows 2000 オペレーティング システムのユーザは、クライアントで認証方式を設定せずにリモートの PPP セッションを確立できます。

MSCHAP V2 の認証では、MSCHAP V1 または標準の CHAP 認証では使用できない追加機能が導入されました。それは、パスワードの変更機能です。パスワード変更機能を使用すると、パスワードが失効したことを RADIUS サーバがレポートした場合に、クライアントがアカウントのパスワードを変更できます。

（注） MSCHAP V2 の認証は更新バージョンの MSCHAP です。これは、MSCHAP バージョン 1（V1）と似ていますが、互換性はありません。MSCHAP V2 では、ピアとパスワード変更機能の間の相互認証が導入されました。

MSCHAP バージョン 2 の設定方法

MSCHAP V2 の認証の設定

ローカル認証または RADIUS 認証で MSCHAP V2 認証を受け入れるように NAS を設定し、RADIUS 認証の認証失敗属性およびベンダー固有の RADIUS 属性を適切に解釈できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-servervsasendauthentication**
4. **interface***typenumber*
5. **pppmax-bad-auth***number*
6. **pppauthenticationms-chap-v2**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-servervsasendauthentication** 例： `Device(config)# radius-server vsa send authentication`	ベンダー固有属性を認識して使用するように NAS を設定します。
ステップ 4	**interface***typenumber* 例： `Device(config)# interface Gigabitethernet 1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**pppmax-bad-auth***number* 例： `Device(config-if)# ppp max-bad-auth 2`	認証が失敗した直後、または指定された認証のリトライ回数の範囲内である場合にはリセットするように、ポイント ツーポイント インターフェイスを設定します。 • *number* 引数のデフォルト値は 0 秒（即座に実行）です。 • 範囲は 0 ～ 255 です。

	コマンドまたはアクション	目的
		（注） NAS が認証失敗属性を解釈できるように、*number* 引数の値には最低でも 2 を設定する必要があります。
ステップ 6	**pppauthenticationms-chap-v2** 例： `Device(config-if)# ppp authentication ms-chap-v2`	NAS で MSCHAP V2 認証をイネーブルにします。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

MSCHAP V2 設定の確認

MSCHAP バージョン 2 機能が正しく設定されているかどうかを確認するには、次の手順を実行します。

手順の概要

1. **showrunning-configinterface***typenumber*
2. **debugpppnegotiation**
3. **debugpppauthentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showrunning-configinterface***typenumber* 例： `Device# show running-config interface Asynch65`	MSCHAP V2 の設定が、指定されたインターフェイスの認証方式であることを確認します。
ステップ 2	**debugpppnegotiation** 例： `Device# debug ppp negotiation`	MSCHAP V2 のネゴシエーションが成功していることを確認します。

	コマンドまたはアクション	目的
ステップ 3	**debugpppauthentication** 例： `Device# debug ppp authentication`	MSCHAP V2 認証が成功していることを確認します。

クリプトベースのクライアントのパスワード エージングの設定

AAA セキュリティ サービスにより、さまざまなログイン認証方式を容易に実行できるようになります。**aaaauthenticationlogin** コマンドを使用すると、サポートされているログイン認証方式のいずれを使用するかに関係なく、AAA 認証がイネーブルになります。**aaaauthenticationlogin** コマンドを使用すると、ログイン時に試行する認証方式リストを 1 つ以上作成できます。これらのリストを適用するには、**loginauthentication** ライン コンフィギュレーション コマンドを使用します。

RADIUS サーバが新しいパスワードを要求すると、AAA はクリプトクライアントにクエリーを実行し、今度はユーザに新しいパスワードを入力するように求めます。

クリプトベースのクライアントにログイン認証とパスワード エージングを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

（注） AAA のパスワード失効インフラストラクチャは、パスワードが失効したことを Easy VPN に通知し、ユーザがパスワードを変更するための一般的な方法を提供します。RADIUS サーバのドメイン削除機能と AAA のパスワード失効のサポートをうまく組み合わせて使用してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaauthenticationlogin** {**default** | *list-name*} **passwd-expiry***method1* [*method2...*]
5. **cryptomap***map-name***clientauthenticationlist***list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**aaanew-model** 例： `Device(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaaauthenticationlogin** {**default** | *list-name*} **passwd-expiry***method1* [*method2...*] 例： `Device(config)# aaa authentication login userauthen passwd-expiry group radius`	ローカルの認証リストでクリプトベースのクライアントのパスワードエージングをイネーブルにします。
ステップ 5	**cryptomap***map-name***clientauthenticationlist***list-name* 例： 例： `Device(config)# crypto map clientmap client authentication list userauthen`	既存のクリプトマップで、ユーザ認証（認証方式のリスト）を設定します。

設定例

ローカル認証の設定の例

次の例では、非同期インターフェイスに PPP を設定し、ローカルで MSCHAP V2 認証をイネーブルにします。

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  username client password secret
```

RADIUS 認証の設定の例

次の例では、非同期インターフェイスに PPP を設定し、RADIUS を使用して MSCHAP V2 認証をイネーブルにします。

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

クリプト認証を使用したパスワード エージングの設定の例

次の例では、クリプトベースのクライアントを持つ AAA を使用して、パスワード エージングを設定します。

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group 3000client
 key cisco123
 dns 10.1.1.10
 wins 10.1.1.20
 domain cisco.com
 pool ippool
```

```
 acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
 set transform-set myset
!
crypto map clientmap client authentication list userauthen
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
!
end
```

その他の参考資料

ここでは、MSCHAP バージョン 2 の機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
PPP インターフェイスの設定	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」
シスコのネットワーキング装置の設定および管理に必要なタスクとコマンドの説明	『*Cisco IOS Dial Technologies Command Reference*』
IOS セキュリティ コマンドの一覧	『*Cisco IOS Security Command Reference*』
AAA を使用した PPP 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T』の「Configuring Authentication」モジュールの「Configuring PPP Authentication Using AAA」
RADIUS 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』の「Configuring RADIUS」モジュール

標準

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1661	ポイントツーポイント プロトコル（*PPP*）
RFC 2548	『*Microsoft Vendor-specific RADIUS Attributes*』
RFC 2759	「*Microsoft PPP CHAP Extensions, Version 2*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

MSCHAP バージョン 2 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *34*：*MSCHAP* バージョン *2* の機能情報

機能名	リリース	機能情報
MSCHAP バージョン 2	Cisco IOS XE Release 3.9S	MSCHAP バージョン 2 機能を使用すると、Cisco ルータは、Microsoft Windows オペレーティング システムを使用するコンピュータとネットワーク アクセス サーバ（NAS）間の PPP 接続にマイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン2（MSCHAP V2）の認証を使用できます。 次のコマンドが導入または変更されました。**aaaauthenticationlogin**、および **pppauthenticationms-chap-v2**。

第 19 章

AAA ブロードキャスト アカウンティング - 必須応答サポート

AAA ブロードキャスト アカウンティング - 必須応答サポート機能は、ゲートウェイ GPRS サポート ノード（GGSN）を介して各サーバ グループでのブロードキャスト アカウンティングをサポートするメカニズムを実現します。GGSN は、General Packet Radio Service（GPRS）のワイヤレス データ ネットワークと、インターネットやプライベート ネットワークなどその他のネットワーク間のゲートウェイとして動作します。

- 機能情報の確認，289 ページ
- AAA ブロードキャスト アカウンティング - 必須応答サポートの前提条件，290 ページ
- AAA ブロードキャスト アカウンティング - 必須応答サポートの制約事項，290 ページ
- AAA ブロードキャスト アカウンティング - 必須応答サポートに関する情報，290 ページ
- GGSN での AAA ブロードキャスト アカウンティングのサポート方法，292 ページ
- AAA ブロードキャスト アカウンティング - 必須応答サポートの設定例，295 ページ
- その他の参考資料，296 ページ
- AAA ブロードキャスト アカウンティング - 必須応答サポートの機能情報，297 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AAA ブロードキャスト アカウンティング - 必須応答サポートの前提条件

GGSN を設定するための準備作業の詳細については、『Cisco GGSN Release 8.0 Configuration Guide』を参照してください。

AAA ブロードキャスト アカウンティング - 必須応答サポートの制約事項

アカウンティング情報は、最大 10 台の AAA サーバに同時に送信することができます。

AAA ブロードキャスト アカウンティング - 必須応答サポートに関する情報

AAA ブロードキャスト アカウンティング - 必須応答サポート機能により、最大 10 個のサーバ グループ（方式）を方式リストで設定することができます。次の項では、GGSN をサポートするために使用される AAA アカウンティングの種類について説明します。

AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の認証、許可、アカウンティング（AAA）サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービス プロバイダーは自社使用のプライベート AAA サーバやエンドユーザの AAA サーバにアカウンティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

RADIUS サーバまたは TACACS+ サーバのサーバ グループ間でブロードキャストを実行できるほか、他のグループと関係なく、サーバ グループごとにフェールオーバー用のバックアップ サーバを定義できます。フェールオーバーは、複数のサーバがサーバ グループで定義されているときに発生する可能性のある処理で、サーバ グループの 1 番目のサーバに情報が送信されたとき、このサーバが使用できなくなっていれば、サーバ グループの次のサーバに情報が送信されるプロセスを指しています。このプロセスは、情報がサーバ グループ内の 1 つのサーバに正常に送信されるまで、またはサーバ グループ内の使用可能なサーバのリストがなくなるまで続きます。

ブロードキャストアカウンティングと待機アカウンティングの同時使用

Cisco GGSN リリース 8.0 以降では、ブロードキャスト アカウンティングと待機アカウンティングが一緒に動作するように設定できます。待機アカウンティング機能はアクセスポイント ネーム（APN）レベルで設定されるのに対し、ブロードキャスト アカウンティングは AAA 方式レベルで指定されます。

ブロードキャストアカウンティングでは、開始、停止、中間の各アカウンティング レコードが方式リストで設定されているすべてのサーバ グループに送信されます。サーバ グループ内では、アカウンティング レコードは最初のアクティブなサーバに送信されます。アクティブ サーバに到達できない場合、アカウンティング レコードはグループの次のサーバに送信されます。

さらに、方式リストの 1 つまたは複数のサーバ グループを「必須」と設定することができます。これは、そのサーバ グループのサーバがアカウンティング開始メッセージに応答する必要があるということです。APN レベルの待機アカウンティングを有効にすると、パケット データ プロトコル（PDP）コンテキストが確立される前に、すべての必須サーバ グループからのアカウンティング応答が受信されるようになります。

ブロードキャスト アカウンティングと待機アカウンティングを同時に使用することの利点は、次のとおりです。

- アカウンティング レコードが複数のサーバに送信されます。エントリが作成されると、ユーザはさまざまなサービスの使用を開始できます。
- 冗長性を確保するため、複数の AAA サーバにレコードが送信されます。
- PDP コンテキストの確立は、すべての必須サーバが有効なアカウンティング開始レコードを受信したときにのみ確立され、情報の損失が防止されます。
- ブロードキャスト レコードは、方式リストの最大 10 個のサーバ グループに送信できます。

ブロードキャスト アカウンティングと待機アカウンティングを同時に設定する場合は、次の点に注意してください。

- 方式リストの設定では、**mandatory** キーワードはブロードキャスト アカウンティングが設定されている場合にだけ使用できます。
- 待機アカウンティングが必要ない場合、すべてのサーバ グループへのブロードキャスト アカウンティングは、必須グループを定義しないで使用できます。
- ブロードキャスト アカウンティングの設定時に必須サーバ グループを指定しない場合は、待機アカウンティングの機能は Cisco GGSN リリース 7.0 以前と同じになります。
- 待機アカウンティングは PPP PDP コンテキストには適用されません。
- PDP は、すべての必須サーバからアカウンティング応答が受信された場合にだけ作成されます。

- 定期的なタイマーは、アカウンティング応答（PDP 作成）が受信されたときに開始されます。

（注） 複数のサーバ グループを必須サーバ グループとして方式リストで定義できます。

GGSN での AAA ブロードキャスト アカウンティングのサポート方法

GGSN でのブロードキャスト アカウンティングと待機アカウンティングの設定

この項の作業では、GGSN でブロードキャスト アカウンティングと待機アカウンティングを設定する方法を説明します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaaccountingnetwork**{*method-list-name* | **default**}
5. **action-type** {**start-stop** | **stop-only**| **none**}
6. **broadcast**
7. **group***server-group* [**mandatory**]
8. **exit**
9. **gprsaccess-point-list***list-name*
10. **access-point***access-point-index*
11. **aaa-groupaccounting***method-listname*
12. **gtp-response-messagewait-accounting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router# aaa new-model`	アクセス コントロールの新しいコマンドおよび機能を有効にします（以前のコマンドを無効にします）。
ステップ 4	**aaaaccountingnetwork**{*method-list-name* | **default**} 例： `Router(config)# aaa accounting network net1`	RADIUS 使用時の課金またはセキュリティ用に、要求されたサービスの認証、許可、アカウンティング（AAA）アカウンティングを有効にし、アカウンティング方式リスト モードを開始します。 • *method-list-name* 引数は、最大 31 文字の名前付きアカウンティング リストです。最大数を超える文字は、いずれも却下されます。 • **default** キーワードでは、デフォルトのアカウンティング リストを指定します。
ステップ 5	**action-type** {**start-stop** | **stop-only**| **none**} 例： `Router(cfg-acct-mlist)#action-type start-stop`	ある種のアクションをアカウンティング レコードで実行します。値は次のとおりです。 • **start-stop**：プロセスの最初にアカウンティング開始通知を送信し、プロセスの最後にアカウンティング停止通知を送信します。 • **stop-only**：要求されたユーザ プロセスの終了時に、「stop」アカウンティング通知を送信します。 • **none**：この回線またはインターフェイスでアカウンティング サービスをディセーブルにします。
ステップ 6	**broadcast** 例： `Router(cfg-acct-mlist)#broadcast`	（任意）複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。

	コマンドまたはアクション	目的
ステップ 7	**group***server-group* [**mandatory**] 例： `Router(cfg-acct-mlist)#group server1`	サーバ グループを指定します。必要に応じて、**mandatory** キーワードを指定して、サーバ グループを必須と定義します。サーバ グループが必須である場合、そのサーバ グループのサーバがアカウンティング開始メッセージに応答する必要があります。 （注） 最大 10 個のサーバ グループを 1 つの方式リストで定義できます。
ステップ 8	**exit**	アカウンティング方式リストのコンフィギュレーション モードを終了します。
ステップ 9	**gprsaccess-point-list***list-name* 例： `Router(config)# gprs access-point-list public1`	GGSN でパブリック データ ネットワーク（PDN）のアクセス ポイントを定義するためのアクセス ポイント リストを設定し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**access-point***access-point-index* 例： `Router(config-ap-list)# access-point 11`	アクセスポイント番号を指定し、アクセスポイントコンフィギュレーション モードを開始します。
ステップ 11	**aaa-groupaccounting***method-listname* 例： `Router(config-access-point)#aaa-group accounting net1`	アカウンティング サーバ グループを指定します。
ステップ 12	**gtp-response-messagewait-accounting** 例： `Router(config-access-point)# gtp-response-message wait-accounting`	サービング GPRS サポート ノード（SGSN）に Create PDP Context Response を送信する前に、RADIUS アカウンティング応答を待機するように APN を設定します。

AAA ブロードキャスト アカウンティング - 必須応答サポートの設定例

AAA ブロードキャスト アカウンティング - 必須応答サポートの例

次の例では、SGSN に Create PDP Context Response を送信する前に、RADIUS サーバからの RADIUS アカウンティング応答を待機するようにGGSNがグローバルに設定されます。GGSNは、access-point 1 を除くすべてのアクセス ポイントで受信された PDP コンテキスト要求の応答を待機します。RADIUS 応答メッセージの待機は、**no gtp response-message wait-accounting** コマンドを使用して access-point 1 で無効化されています。

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius abc
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.6.7.8 auth-port 1645 acct-port 1646
!
! Configures AAA authentication and authorization
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc
 action-type start-stop
 broadcast
 group SG1 mandatory
 group SG2
 group SG3 mandatory
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication abc
!
! Disables waiting for RADIUS response
! message at APN 1
!
  no gtp response-message wait-accounting
  exit
access-point 2
 access-mode non-transparent
 access-point-name www.pdn2.com
 aaa-group authentication abc
!
! Enables waiting for RADIUS response
! messages across all APNs (except APN 1)
!
gprs gtp response-message wait-accounting
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

その他の参考資料

ここでは、AAA ブロードキャスト アカウンティング - 必須応答サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
GGSN の設定の準備作業	『*Cisco GGSN Release 8.0 Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference Guide*』
AAA 機能	『*Cisco IOS Security Configuration Guide: Securing User Services*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

AAA ブロードキャスト アカウンティング - 必須応答サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *35* : ***AAA*** ブロードキャスト アカウンティング - 必須応答サポートの機能情報

機能名	リリース	機能情報
AAA ブロードキャスト アカウンティング - 必須応答サポート	Cisco IOS XE Release 3.9S	AAA ブロードキャスト アカウンティング - 必須応答サポート機能は、ゲートウェイ GPRS サポート ノード（GGSN）を介して各サーバグループでのブロードキャスト アカウンティングをサポートするメカニズムを実現します。GGSN は、General Packet Radio Service（GPRS）のワイヤレス データ ネットワークと、インターネットやプライベート ネットワークなどその他のネットワーク間のゲートウェイとして動作します。 次のコマンドが導入または変更されました。 **aaaaccountingnetwork**、**aaa-groupaccounting**、**access-point**、**action-type**、**broadcast**、**gprsaccess-point-list**、**group**、**gtp-response-messagewait-accounting**。