



許可用の AAA Dialed Number Information Service (DNIS) マップ

許可用の AAA DNIS マップ機能を使用すると、着信番号識別サービス (DNIS) 番号を特定の認証、許可、およびアカウントिंग (AAA) サーバーグループに割り当てることができます。これによって、サーバーグループは、その DNIS を使用して、ネットワークにダイヤルインするユーザーの認証、許可、アカウントINGの要求を処理できます。すべての電話回線 (通常の自宅電話または商用の T1/PRI 回線) を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。

- [許可用の AAA DNIS マップの前提条件 \(1 ページ\)](#)
- [許可用の AAA DNIS マップに関する情報 \(2 ページ\)](#)
- [許可用の AAA DNIS マップの設定方法 \(4 ページ\)](#)
- [許可用の AAA DNIS マップの設定例 \(9 ページ\)](#)
- [その他の参考資料 \(11 ページ\)](#)
- [許可用の AAA DNIS マップの機能情報 \(12 ページ\)](#)

許可用の AAA DNIS マップの前提条件

- サーバーグループの DNIS に基づいて特定の AAA サーバーグループを選択するようにデバイスを設定する前に、RADIUS サーバーホストと AAA サーバーグループの一覧を設定する必要があります。
- AAA 事前認証を設定する前に、**aaa new-model** コマンドを設定して、サポートする事前認証アプリケーションが使用中のネットワークの RADIUS サーバーで実行されていることを確認する必要があります。

許可用の AAA DNIS マップに関する情報

DNIS に基づく AAA サーバー グループの選択

Cisco ソフトウェアを使用すると、DNIS 番号を特定の AAA サーバグループに割り当てることができます。これによって、サーバグループは、その DNIS を使用して、ネットワークにダイヤルインするユーザの認証、認可、アカウントिंगの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続するシスコ デバイスは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる RADIUS サーバグループを割り当て可能です（つまり、DNIS 番号ごとに異なる RADIUS サーバ）。さらに、サーバグループを使用して、複数の AAA サービスに同じサーバグループを指定できます。また、各 AAA サービスに個別のサーバグループを指定できます。

Cisco ソフトウェアには、認証サービスとアカウントングサービスを複数の方法で実装できる柔軟性があります。

- **グローバル**：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバ上のすべてのインターフェイスに、一般的に適用されます。
- **インターフェイス別**：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバに設定されているインターフェイスにだけ適用されます。
- **DNIS マッピング**：DNIS を使用して、AAA サーバが AAA サービスを提供するように指定します。

このような複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバまたはサーバグループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- **DNIS 別**：DNIS を使用し、AAA サービスを提供するサーバグループを指定または決定するようにネットワーク アクセス サーバを設定している場合、この方式がその他の AAA 選択方式よりも優先されます。
- **インターフェイス別**：サーバから AAA サービスを提供する方法を決定するために、インターフェイス別にネットワーク アクセス サーバを設定してアクセス リストを使用する場合、この方式は、他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。

- グローバル：セキュリティ サーバーが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバーを設定する場合、この方式には最も低い優先度が使用されます。

AAA 事前認証

ISDN PRI または個別線信号方式 (CAS) による AAA 事前認証を設定すると、サービス プロバイダーは、既存の RADIUS ソリューションを使用するポートの管理性を改善し、共有リソースの使用を効率的に管理して、各種のサービスレベル契約を提供できるようになります。ISDN PRI または CAS によって、着信コールに関する情報をネットワーク アクセス サーバー (NAS) で使用してから、コールを接続できます。使用できるコール情報は次のとおりです。

- 着信番号識別サービス (DNIS) 番号 (着信者番号とも呼ばれます)
- 発呼回線 ID (CLID) 番号 (発番号とも呼ばれます)
- コール タイプ (ベアラ機能とも呼ばれます)

AAA 事前認証の機能を使用すると、Cisco NAS で、DNIS 番号、CLID 番号、またはコール タイプに基づいて着信コールを接続するかどうかを決定することができます。(ISDN PRI を使用する場合、ユーザーの認証と認可を行ってから、コールに応答できます。CAS を使用する場合、コールに応答する必要はありますが、事前認証に失敗した場合、コールをドロップできません)。

パブリック ネットワーク スイッチからコールを着信し、まだ接続前の場合、AAA 事前認証によって、NAS から DNIS 番号、CLID 番号、およびコール タイプを RADIUS サーバーに送信し、認可を受けることができます。サーバーがコールを認可すると、NAS はコールを許可します。サーバーがコールを認可しない場合、NAS からパブリック ネットワーク スイッチに接続解除メッセージが送信され、コールが拒否されます。

RADIUS サーバー アプリケーションが使用不能になった場合、または応答が遅くなった場合、NAS でガード タイマーを設定できます。タイマーが期限切れになると、NAS は設定可能なパラメータを使用して、認可されなかった着信コールを許可または拒否します。

AAA 事前認証の機能では、事前認証の動作を指定するために、RADIUS サーバー アプリケーションによる属性 44 の使用、および RADIUS 事前認証 プロファイルに設定されている RADIUS 属性の使用がサポートされています。また、これらの属性は、たとえば、以降の認証を実行するかどうか、また実行する場合、どの認証方式を使用するかを指定するためにも使用できます。

ISDN PRI および CAS による AAA 事前認証には、次の制約事項が適用されます。

- 属性 44 は、事前認証またはリソース プーリングをイネーブルにした CAS コールにだけ使用できます。
- マルチシャーシ マルチリンク PPP (MMP) は、ISDN PRI では使用できません。
- AAA 事前認証は、一部のハードウェア プラットフォームでのみ使用できます。
- ISDN PRI は、一部のハードウェア プラットフォームでのみサポートされています。

コール処理のガードタイマー

事前認証要求および認可要求の応答時間はさまざまなので、ガードタイマーを使用してコールの処理を制御できます。ガードタイマーは、DNISがRADIUSサーバーに送信されると開始されます。ガードタイマーが期限切れになる前にNASがAAAから応答を受信しない場合、タイマーの設定に基づいてコールを許可または拒否します。

許可用の AAA DNIS マップの設定方法

AAA DNIS 事前認証の設定

DNIS 事前認証を使用すると、着信番号に基づいてコール設定時に事前認証を実行できます。DNIS 番号は、コールの着信時にセキュリティサーバーに直接送信されます。コールがAAAによって認証されると、そのコールは許可されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group {radius | tacacs+ | server-group}**
5. **dnis [password string]**
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 モードを有効にします。 • 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 preauthorization 例： Device(config)# aaa preauthorization	AAA 事前認証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	group {radius tacacs+ server-group} 例：	(任意) AAA 事前認証要求に使用するセキュリティサーバーを選択します。

	コマンドまたはアクション	目的
	Device(config-preauth)# group radius	• デフォルトは RADIUS です。
ステップ 5	dnis [password string] 例 : Device(config-preauth)# dnis password dnisspass	DNIS を使用して事前認証をイネーブルにし、必要に応じて Access-Request パケットに使用するパスワードを指定します。
ステップ 6	end 例 : Device(config-preauth)# end	AAA 事前認証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。

DNIS に基づく AAA サーバー グループの選択の設定

サーバー グループの DNIS に基づいて特定の AAA サーバー グループを選択するようにデバイスを設定するには、DNIS マッピングを設定します。DNIS 番号を使用してサーバー グループをグループ名とマッピングするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa dnis map enable**
4. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
5. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
6. **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*
7. **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 モードを有効にします。 • 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 dnis map enable 例 :	DNIS マッピングをイネーブルにします。

	コマンドまたはアクション	目的
	Device(config)# aaa dnis map enable	
ステップ 4	aaa dnis map <i>dnis-number</i> authentication ppp group <i>server-group-name</i> 例 : Device(config)# aaa dnis map 7777 authentication ppp group sg1	DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、認証に使用されます。
ステップ 5	aaa dnis map <i>dnis-number</i> authorization network group <i>server-group-name</i> 例 : Device(config)# aaa dnis map 7777 authorization network group sg1	DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、認可に使用されます。
ステップ 6	aaa dnis map <i>dnis-number</i> accounting network [none start-stop stop-only] group <i>server-group-name</i> 例 : Device(config)# aaa dnis map 8888 accounting network stop-only group sg2	DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、アカウントングに使用されます。
ステップ 7	exit 例 : Device(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、特権 EXEC モードに戻ります。

AAA 事前認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** *server-group*
5. **clid** [*if-avail* | **required**] [**accept-stop**] [**password** *string*]
6. **ctype** [*if-avail* | **required**] [**accept-stop**] [**password** *string*]
7. **dnis** [*if-avail* | **required**] [**accept-stop**] [**password** *string*]
8. **dnis bypass** *dnis-group-name*
9. **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 モードを有効にします。 • 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 preauthorization 例： Device(config)# aaa preauthorization	AAA 事前認証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	group server-group 例： Device(config-preauth)# group sg2	事前認証に使用する AAA RADIUS サーバー グループを指定します。
ステップ 5	clid [if-avail required] [accept-stop] [password string] 例： Device(config-preauth)# clid required	CLID 番号に基づいて、コールを事前認証します。
ステップ 6	ctype [if-avail required] [accept-stop] [password string] 例： Device(config-preauth)# ctype required	コールタイプに基づいて、コールを事前認証します。
ステップ 7	dnis [if-avail required] [accept-stop] [password string] 例： Device(config-preauth)# dnis required	DNIS 番号に基づいて、コールを事前認証します。
ステップ 8	dnis bypass dnis-group-name 例： Device(config-preauth)# dnis bypass group1	事前認証をバイパスする DNIS 番号のグループを指定します。
ステップ 9	end 例：	事前認証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。

	コマンドまたはアクション	目的
	Device(config-preauth)# end	

ガードタイマーの設定

RADIUS サーバーが認証要求または事前認証要求に応答できなかった場合にコールを許可または拒否するようにガードタイマーを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. **call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
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 モードを有効にします。 <ul style="list-style-type: none">• 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	interface <i>type number</i> 例： Device(config)# interface serial 1/0/0:23	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	isdn guard-timer <i>milliseconds</i> [on-expiry { accept reject }] 例： Device(config-if)# isdn guard-timer 8000 on-expiry reject	RADIUS サーバーが事前認証要求に応答できなかった場合にコールを許可または拒否できる ISDN ガードタイマーを設定します。
ステップ 5	call guard-timer <i>milliseconds</i> [on-expiry { accept reject }] 例：	RADIUS サーバーが事前認証要求に応答できなかった場合にコールを許可または拒否できる CAS ガードタイマーを設定します。

	コマンドまたはアクション	目的
	Device(config-if)# call guard-timer 2000 on-expiry accept	
ステップ 6	end 例 : Device(config-if)# end	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、特権 EXEC モードに戻ります。

許可用の AAA DNIS マップの設定例

例 : DNIS に基づく AAA サーバー グループの選択

次に、特定の AAA サービスを提供するために、DNIS に基づいて RADIUS サーバー グループを選択する例を示します。

```

! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5
! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
! with it.
aaa group server radius sg2
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1
! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group

```

```

! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3

```

例 : AAA 事前認証

次に、事前認証に DNIS 番号を指定する単純な設定を示します。

```

aaa preauthentication
  group radius
  dnis required

```

次に、事前認証に DNIS 番号と CLID 番号の両方を使用する設定の例を示します。DNIS 事前認証が先に実行され、次に CLID 事前認証が実行されます。

```

aaa preauthentication
  group radius
  dnis required
  clid required

```

次に、「dnis-group1」という DNIS グループに指定されている 2 つの DNIS 番号を除き、すべての DNIS 番号について事前認証を実行することを指定する例を示します。

```

aaa preauthentication
  group radius
  dnis required
  dnis bypass dnis-group1
dialer dnis group dnis-group1
  number 12345
  number 12346

```

次に、DNIS 事前認証を使用する AAA 設定の例を示します。

```

aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauthentication
  dnis password Cisco-DNIS
aaa nas port extended

```

```

!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey

```



- (注) 事前認証を設定するには、RADIUS サーバーでも事前認証プロファイルを設定する必要があります。

例：ISDN および CAS のガード タイマー

次に、8,000 ミリ秒に設定された ISDN ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバーが応答しないまま、タイマーが期限切れになった場合、コールは拒否されます。

```

interface serial 1/0/0:23
 isdn guard-timer 8000 on-expiry reject
aaa preauthentication
 group radius
 dnis required

```

次に、20,000 ミリ秒に設定された CAS ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバーが応答しないまま、タイマーが期限切れになった場合、コールは許可されます。

```

controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept
aaa preauthentication
 group radius
 dnis required

```

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』

関連項目	マニュアルタイトル
セキュリティコマンド	<ul style="list-style-type: none"> 『Cisco IOS Security Command Reference: Commands A to C』 [英語] 『Cisco IOS Security Command Reference: Commands D to L』 [英語] 『Cisco IOS Security Command Reference: Commands M to R』 [英語] 『Cisco IOS Security Command Reference: Commands S to Z』 [英語]
AAA	『Authentication, Authorization, and Accounting Configuration Guide』 (Securing User Services Configuration Library の一部)

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

許可用の AAA DNIS マップの機能情報

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 1: 許可用の AAA DNIS マップの機能情報

機能名	リリース	機能情報
許可用の AAA Dialed Number Information Service (DNIS) マップ	12.1(1)T 12.2(2)T 12.2(27)SBA Cisco IOS XE Release 2.3	<p>許可用の AAA DNIS マップ機能を使用すると、着信番号識別サービス (DNIS) 番号を特定の AAA サーバーグループに割り当てることができます。これによって、サーバーグループは、その DNIS を使用して、ネットワークにダイヤルインするユーザーの認証、認可、およびアカウントingの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。</p> <p>次のコマンドが導入または変更されました。aaa dnis enable、aaa dnis map authentication group、aaa dnis map authorization network group、および aaa dnis map accounting network</p>

翻訳について

このドキュメントは、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。