Cisco Secure Access Control System 5.4 ユーザ ガイド

2013 年 1 月

Text Part Number: OL-26225-01-J

【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。

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: 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)

このマニュアルで使用している IP アドレスは、実際のアドレス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、および図は、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 Secure Access Control System 5.4 ユーザ ガイド
© 2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

はじめに xxiii

対象読者 xxiii

表記法 xxiii

マニュアルの更新 xxiv

関連資料 xxiv

マニュアルの入手方法およびテクニカル サポート xxv

CHAPTER 1 **ACS 5.4 の導入** 1-1

ACS の概要 1-1

ACS の分散展開 1-2

ACS 4.x と 5.4 の複製 1-2

ACS のライセンス モデル 1-3

ACS 管理インターフェイス 1-3

ACS Web ベース インターフェイス 1-4

ACS コマンドライン インターフェイス 1-4

ACS プログラム インターフェイス 1-5

ACS でサポートされているハードウェア モデル 1-5

CHAPTER 2 **ACS 4.x から ACS 5.4 への移行** 2-1

移行プロセスの概要 2-2

移行の要件 2-2

移行サポート バージョン 2-2

はじめる前に 2-3

移行ファイルのダウンロード 2-3

ACS 4.x から ACS 5.4 への移行 2-4

ACS 4.x から ACS 5.4 への機能マッピング 2-6

移行の一般的なシナリオ 2-8

CSACS 1120 の ACS 4.2 から ACS 5.4 への移行 2-8

ACS 3.x から ACS 5.4 への移行 2-9

他の AAA サーバから ACS 5.4 へのデータの移行 2-9

CHAPTER 3 **ACS 5.x ポリシー モデル** 3-1

ACS 5.x ポリシー モデルの概要 3-1

ポリシーの用語 3-3
単純なポリシー 3-4
ルールベースのポリシー 3-4
ポリシーのタイプ 3-5
アクセス ポリシー 3-6
ID ポリシー 3-9
グループ マッピング ポリシー 3-11
デバイス管理用の認可ポリシー 3-11
複数のコマンド セットを持つ規則の処理 3-11
認可ポリシーの例外規則 3-12
サービス セレクション ポリシー 3-12
単純なサービス セレクション 3-13
ルール ベースのサービス セレクション 3-13
アクセス サービスおよびサービス セレクションのシナリオ 3-13
最初の一致規則テーブル 3-14
ポリシーの条件 3-16
ポリシーの結果 3-16
ネットワーク アクセスの認可プロファイル 3-17
複数の認可プロファイルを含む規則の処理 3-17
ポリシーおよび ID 属性 3-17
ポリシーおよびネットワーク デバイス グループ 3-18
ルール ベース ポリシーの例 3-18
サービスおよびポリシーの設定フロー 3-19

CHAPTER 4 **ACS を使用した一般的なシナリオ 4-1**
デバイス管理の概要 4-2
セッション管理 4-3
コマンド認可 4-4
TACACS+ のカスタム サービスおよび属性 4-5
パスワードベースのネットワーク アクセス 4-5
パスワードベースのネットワーク アクセスの概要 4-5
パスワードベースのネットワーク アクセスの設定フロー 4-7
証明書ベースのネットワーク アクセス 4-9
証明書ベースのネットワーク アクセスの概要 4-9
ACS で証明書を使用する方法 4-10
証明書ベースのネットワーク アクセス 4-10
証明書によるブラウザからの ACS Web インターフェイスの認可 4-12
LDAP セキュア認証接続の確認 4-12

エージェントレス ネットワーク アクセス 4-12
エージェントレス ネットワーク アクセスの概要 4-13
ホスト ルックアップ 4-13
コール チェックを使用する認証 4-14
Service-Type Call Check の処理 4-15
PAP/EAP-MD5 認証 4-15
エージェントレス ネットワーク アクセスのフロー 4-17
内部 ID ストアへのホストの追加 4-18
ホスト ルックアップ用の LDAP 外部 ID ストアの設定 4-18
ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定 4-19
ホスト ルックアップ用のアクセス サービスの作成 4-19
ホスト ルックアップ要求用の ID ポリシーの設定 4-20
ホスト ルックアップ要求用の認可ポリシーの設定 4-21
VPN リモート ネットワーク アクセス 4-21
サポートされる認証プロトコル 4-22
サポートされる ID ストア 4-22
サポートされる VPN ネットワーク アクセス サーバ 4-23
サポートされる VPN クライアント 4-23
VPN リモート アクセス サービスの設定 4-23
ACS と Cisco Security Group Access 4-24
Security Group Access 用デバイスの追加 4-25
セキュリティ グループの作成 4-25
SGACL の作成 4-26
NDAC ポリシーの設定 4-26
Security Group Access 用の EAP-FAST 設定の構成 4-27
Security Group Access アクセス用のアクセス サービスの作成 4-27
エンドポイント アドミッション コントロール ポリシーの作成 4-28
出力ポリシーの作成 4-28
デフォルト ポリシーの作成 4-29
RADIUS および TACACS+ プロキシ要求 4-30
サポートされるプロトコル 4-32
サポートされる RADIUS 属性 4-32
TACACS+ の本文の暗号化 4-32
TACACS+ サーバへの接続 4-33
プロキシ サービスの設定 4-34

CHAPTER 5 **[My Workspace] の概要** 5-1
[Welcome] ページ 5-1
タスク ガイド 5-2

[My Account] ページ 5-2
ログイン バナー 5-3
Web インターフェイスの使用方法 5-3
Web インターフェイスへのアクセス 5-4
ログイン 5-4
ログアウト 5-5
Web インターフェイスについて 5-5
Web インターフェイスのデザイン 5-6
ナビゲーション ペイン 5-7
コンテンツ領域 5-8
Web インターフェイスを使用した ACS オブジェクトのインポートおよびエクスポート 5-19
サポートされる ACS オブジェクト 5-20
インポート ファイルの作成 5-22
Web インターフェイスからのテンプレートのダウンロード 5-22
CSV テンプレートについて 5-23
インポート ファイルの作成 5-24
一般的なエラー 5-27
同時実行競合エラー 5-27
削除エラー 5-28
システム障害エラー 5-30
アクセシビリティ 5-30
表示および可読性機能 5-30
キーボードとマウスの機能 5-31
その他のアクセシビリティ情報の入手 5-31

CHAPTER 6 **インストール後の設定タスク 6-1**
最小システム セットアップの設定 6-1
ACS によるシステム管理タスクの実行の設定 6-2
ACS によるアクセス ポリシーの管理の設定 6-4
ACS によるネットワークの問題の監視およびトラブルシューティングの設定 6-4

CHAPTER 7 **ネットワーク リソースの管理 7-1**
ネットワーク デバイス グループ 7-2
ネットワーク デバイス グループの作成、複製、および編集 7-2
ネットワーク デバイス グループの削除 7-3
階層内でのネットワーク デバイス グループの作成、複製、および編集 7-4
階層からのネットワーク デバイス グループの削除 7-5
ネットワーク デバイスおよび AAA クライアント 7-5

ネットワーク デバイスの一括操作の表示および実行 7-6
ネットワーク デバイスおよび AAA クライアントのエクスポート 7-8
ネットワーク リソースおよびユーザに関する一括操作の実行 7-8
ネットワーク リソースおよびユーザのエクスポート 7-10
ネットワーク デバイスの作成、複製、および編集 7-11
ネットワーク デバイスおよび AAA クライアントの設定 7-11
ネットワーク デバイス プロパティの表示 7-15
ネットワーク デバイスの削除 7-18
デフォルトのネットワーク デバイスの設定 7-18
外部プロキシ サーバの使用 7-20
外部プロキシ サーバの作成、複製、および編集 7-21
外部プロキシ サーバの削除 7-22
OCSP サービスの使用 7-22
OCSP サーバの作成、複製、および編集 7-23
OCSP サーバの削除 7-25

CHAPTER 8 ユーザおよび ID ストアの管理 8-1
概要 8-1
内部 ID ストア 8-1
外部 ID ストア 8-2
2 要素認証の ID ストア 8-3
ID グループ 8-3
証明書ベースの認証 8-3
ID 順序 8-4
内部 ID ストアの管理 8-4
認証情報 8-5
ID グループ 8-6
ID グループの作成 8-6
ID グループの削除 8-7
ID 属性の管理 8-7
標準属性 8-8
ユーザ属性 8-8
ホスト属性 8-9
ユーザの認証設定の設定 8-9
内部ユーザの作成 8-11
内部 ID ストアからのユーザの削除 8-14
内部 ID ストア ユーザの一括操作の表示および実行 8-15
ID ストアでのホストの作成 8-16
内部ホストの削除 8-18

内部 ID ストア ホストの一括操作の表示および実行 8-18
外部 ID ストアの管理 8-19
LDAP の概要 8-19
ディレクトリ サービス 8-20
LDAP を使用した認証 8-20
複数の LDAP インスタンス 8-20
フェールオーバー 8-21
LDAP 接続管理 8-21
バインド接続を使用したユーザの認証 8-21
グループ メンバーシップ情報の取得 8-22
属性取得 8-23
証明書取得 8-23
外部 LDAP ID ストアの作成 8-23
外部 LDAP サーバ接続の設定 8-24
外部 LDAP ディレクトリ構成の設定 8-27
外部 LDAP ID ストアの削除 8-31
LDAP グループの設定 8-31
LDAP 属性の表示 8-32
外部 MAB データベースとしての Cisco NAC Profiler の利用 8-32
Cisco NAC Profiler での LDAP インターフェイスのイネーブル化による ACS との通信 8-33
ID ポリシーで使用するための ACS での NAC Profiler LDAP 定義の設定 8-35
Profiler の統合による MAB 認証のトラブルシューティング 8-39
Microsoft AD 8-39
マシン認証 8-42
認可のための属性取得 8-42
認可のためのグループ取得 8-42
EAP-TLS 認証のための証明書取得 8-42
同時接続管理 8-43
ユーザおよびマシン アカウントの制限 8-43
マシン アクセス制限 8-43
分散 MAR キャッシュ 8-44
ダイヤルイン アクセス権 8-45
ダイヤルイン ユーザのコールバック オプション 8-46
AD ドメインへの ACS の追加 8-47
AD ID ストアの設定 8-47
AD グループの選択 8-51
AD 属性の設定 8-52
マシン アクセス制限の設定 8-54
RSA SecurID サーバ 8-55

RSA SecurID エージェントの設定 8-55
RSA SecurID トークン サーバの作成および編集 8-56
RADIUS ID ストア 8-61
サポートされる認証プロトコル 8-61
フェールオーバー 8-61
パスワード プロンプト 8-62
ユーザ グループ マッピング 8-62
グループおよび属性マッピング 8-62
ID 順序での RADIUS ID ストア 8-62
認証失敗メッセージ 8-63
Safeword サーバでのユーザ名の特殊フォーマット 8-63
ユーザ属性キャッシュ 8-64
RADIUS ID サーバの作成、複製、および編集 8-64
CA 証明書の設定 8-69
認証局の追加 8-70
認証局の編集および証明書失効リストの設定 8-71
認証局の削除 8-72
認証局のエクスポート 8-73
証明書認証プロファイルの設定 8-73
ID ストア順序の設定 8-75
ID ストア順序の作成、複製、および編集 8-76
ID ストア順序の削除 8-78

CHAPTER 9 ポリシー要素の管理 9-1
ポリシー条件の管理 9-1
日付と時刻の条件の作成、複製、および編集 9-3
カスタム セッション条件の作成、複製、および編集 9-5
セッション条件の削除 9-6
ネットワーク条件の管理 9-7
ネットワーク条件のインポート 9-8
ネットワーク条件のエクスポート 9-9
端末フィルタの作成、複製、および編集 9-9
デバイス フィルタの作成、複製、および編集 9-12
デバイス ポート フィルタの作成、複製、および編集 9-16
認可および権限の管理 9-19
ネットワーク アクセス用の認可プロファイルの作成、複製、および編集 9-19
認可プロファイルの指定 9-20
認可プロファイルでの共通属性の指定 9-21
認可プロファイルでの RADIUS 属性の指定 9-23

セキュリティ グループの作成および編集 9-25
デバイス管理用のシェル プロファイルの作成、複製、および編集 9-25
シェル プロファイルの一般プロパティの定義 9-27
共通タスクの定義 9-27
カスタム属性の定義 9-30
管理デバイス用のコマンド セットの作成、複製、および編集 9-31
ダウンロード可能 ACL の作成、複製、および編集 9-33
認可および権限のポリシー要素の削除 9-34
セキュリティ グループ アクセス コントロール リストの設定 9-35

CHAPTER 10 アクセス ポリシーの管理 10-1
ポリシー作成フロー 10-1
ネットワークの定義とポリシーの目的 10-2
ポリシー作成フローのポリシー要素 10-3
アクセス サービス ポリシーの作成 10-4
サービス セレクション ポリシーの作成 10-4
ポリシーのカスタマイズ 10-4
サービス セレクション ポリシーの設定 10-5
単純なサービス セレクション ポリシーの設定 10-6
[Service Selection Policy] ページ 10-6
サービス セレクション規則の作成、複製、および編集 10-8
ヒット カウントの表示 10-9
サービス セレクション規則の削除 10-10
アクセス サービスの設定 10-11
デフォルトのアクセス サービスの編集 10-11
アクセス サービスの作成、複製、および編集 10-12
アクセス サービスの一般プロパティの設定 10-13
アクセス サービスの許可されたプロトコルの設定 10-16
アクセス サービス テンプレートの設定 10-20
アクセス サービスの削除 10-21
アクセス サービス ポリシーの設定 10-22
ID ポリシーの表示 10-22
ルール ベースの ID ポリシーの表示 10-24
ID ポリシー規則のプロパティの設定 10-25
グループ マッピング ポリシーの設定 10-26
グループ マッピング ポリシー規則のプロパティの設定 10-29
ネットワーク アクセスのセッション認可ポリシーの設定 10-30
ネットワーク アクセス認可規則のプロパティの設定 10-32
デバイス管理認可ポリシーの設定 10-33

デバイス管理認可規則のプロパティの設定 10-34
デバイス管理認可例外ポリシーの設定 10-34
デバイス管理のシェル / コマンド認可ポリシーの設定 10-35
認可例外ポリシーの設定 10-36
ポリシー規則の作成 10-38
規則の複製 10-39
ポリシー規則の編集 10-39
ポリシー規則の削除 10-40
複合条件の設定 10-41
複合条件の構築ブロック 10-41
複合条件のタイプ 10-42
複合式ビルダーの使用方法 10-45
[Security Group Access Control] ページ 10-46
[Egress Policy Matrix] ページ 10-46
出力ポリシー マトリクスのセルの編集 10-47
出力ポリシーのデフォルト ポリシーを定義するためのページ 10-47
NDAC ポリシー ページ 10-48
[NDAC Policy Properties] ページ 10-49
[Network Device Access EAP-FAST Settings] ページ 10-51
最大ユーザ セッション数 10-51
Max Session User Settings 10-52
Max Session Group Settings 10-52
最大セッションのグローバル設定 10-53
ユーザ セッションの削除 10-54
分散環境の最大ユーザ セッション 10-55
プロキシ シナリオの最大ユーザ セッション 10-56

CHAPTER 11 **ACS での監視とレポート 11-1**
認証レコードと詳細 11-2
ダッシュボード ページ 11-2
ポートレットの操作 11-4
[Authentication Lookup] ポートレットの操作 11-5
[Authentication Lookup] レポートの実行 11-6
ダッシュボード内のタブの設定 11-6
ダッシュボードへのタブの追加 11-6
タブへのアプリケーションの追加 11-7
ダッシュボード内のタブの名前変更 11-7
ダッシュボードのレイアウトの変更 11-8
ダッシュボードからのタブの削除 11-8

CHAPTER 12 アラームの管理 12-1
アラームについて 12-1
アラームしきい値の評価 12-2
ユーザへのイベントの通知 12-3
受信ボックスでのアラームの表示および編集 12-3
アラーム スケジュールについて 12-9
アラーム スケジュールの作成と編集 12-10
しきい値へのアラーム スケジュールの割り当て 12-10
アラーム スケジュールの削除 12-11
アラームしきい値の作成、編集、および複製 12-11
一般的なしきい値情報の設定 12-13
しきい値基準の設定 12-14
Passed Authentications 12-14
Failed Authentications 12-16
Authentication Inactivity 12-18
TACACS Command Accounting 12-19
TACACS Command Authorization 12-20
ACS Configuration Changes 12-21
ACS System Diagnostics 12-22
ACS Process Status 12-23
ACS System Health 12-24
ACS AAA Health 12-25
RADIUS Sessions 12-26
Unknown NAD 12-27
External DB Unavailable 12-28
RBACL Drops 12-29
NAD-Reported AAA Downtime 12-31
しきい値通知の設定 12-32
アラームしきい値の削除 12-33
システム アラーム設定の設定 12-34
アラーム Syslog ターゲットについて 12-35
アラーム Syslog ターゲットの作成と編集 12-35
アラーム Syslog ターゲットの削除 12-36

CHAPTER 13 レポートの管理 13-1
お気に入りレポートの使用 13-3
[Favorites] ページへのレポートの追加 13-3
お気に入りレポートのパラメータの表示 13-4
お気に入りレポートの編集 13-5

お気に入りレポートの実行 13-6
お気に入りからのレポートの削除 13-6
レポートの共有 13-7
カタログ レポートの使用 13-7
カタログで使用可能なレポート 13-8
カタログ レポートの実行 13-12
カタログ レポートの削除 13-13
名前付きレポートの実行 13-13
report_name ページについて 13-15
デバイスでの RADIUS CoA オプションのイネーブル化 13-18
認可の変更、およびアクティブな RADIUS セッションの接続解除 13-18
レポートのカスタマイズ 13-20
レポートの復元 13-20
レポートの表示 13-21
標準ビューアについて 13-21
Interactive Viewer について 13-21
Interactive Viewer のコンテキスト メニューについて 13-22
レポート内の移動 13-23
目次の使用方法 13-23
レポート データのエクスポート 13-24
レポートの印刷 13-27
Interactive Viewer におけるレポート デザインの保存 13-27
Interactive Viewer におけるレポートのフォーマット 13-28
ラベルの編集 13-28
ラベルのフォーマット 13-29
データのフォーマット 13-29
カラムのサイズ変更 13-30
カラム データの配置の変更 13-30
カラム内のデータのフォーマット 13-30
集計行のデータのフォーマット 13-31
データ型のフォーマット 13-31
数値データのフォーマット 13-32
固定数値、科学的数値、またはパーセントのフォーマット 13-33
カスタム数値データのフォーマット 13-34
ストリング データのフォーマット 13-34
カスタム ストリング データのフォーマット 13-35
日時のフォーマット 13-36
日付と時刻のカスタム フォーマット 13-36
ブール データのフォーマット 13-37

条件フォーマットの適用 13-38
カラムへの条件フォーマットの設定 13-39
条件フォーマットの削除 13-41
詳細カラムにおける改ページの設定および削除 13-41
グループ カラムにおける改ページの設定および削除 13-42
レポート データの構成 13-42
レポート データの表示および構成 13-43
Interactive Viewer におけるカラムの並べ替え 13-43
カラムの削除 13-45
レポート項目の非表示または表示 13-45
カラムの非表示 13-46
非表示カラムの表示 13-46
カラムのマージ 13-46
マージされたカラムからのカラムの選択 13-48
データのソート 13-48
単一のカラムのソート 13-48
複数のカラムのソート 13-48
データのグループ化 13-50
グループの追加 13-51
日付または時刻に基づくデータのグループ化 13-51
内部グループの削除 13-53
レポート計算の作成 13-53
サポートされている計算関数について 13-54
サポートされている演算子について 13-61
式における数値および日付の使用方法 13-61
計算カラムにおける値の乗算の使用方法 13-62
既存の日付値への日付の加算 13-62
計算カラムにおける日付値の減算 13-63
集計データの使用 13-63
集計データ行の作成 13-64
追加の集計行の追加 13-66
集計行の削除 13-67
レポート データの非表示およびフィルタリング 13-67
カラム データの非表示または表示 13-67
重複値の表示 13-68
グループまたはセクションの詳細行の非表示または表示 13-69
フィルタの使用 13-69
フィルタ条件のタイプ 13-70
フィルタ値の設定 13-71
フィルタの作成 13-72

フィルタの変更またはクリア 13-73
複数の条件を持つフィルタの作成 13-73
複数の条件を含むフィルタからの 1 つのフィルタ条件の削除 13-75
カラムの上位または下位の値のフィルタリング 13-75
グラフについて 13-76
グラフの変更 13-77
グラフ データのフィルタリング 13-77
グラフ サブタイプの変更 13-78
グラフ フォーマットの変更 13-78

CHAPTER 14 Monitoring and Report Viewer を使用した ACS のトラブルシューティング 14-1
利用可能な診断ツールおよびトラブルシューティング ツール 14-1
接続テスト 14-1
ACS サポート バンドル 14-1
Expert Troubleshooter 14-2
接続テストの実行 14-3
診断情報用の ACS サポート バンドルのダウンロード 14-4
Expert Troubleshooter の使用 14-6
RADIUS 認証のトラブルシューティング 14-6
ネットワーク デバイス上での show コマンドの実行 14-10
ネットワーク デバイスの設定の評価 14-10
ネットワーク デバイスと ACS との間での SGACL ポリシーの比較 14-12
デバイスとそのピアとの間での SXP-IP マッピングの比較 14-12
デバイスの IP-SGT ペアと ACS によって割り当てられた SGT レコードとの比較 14-14
デバイス SGT と ACS によって割り当てられたデバイス SGT との比較 14-15

CHAPTER 15 Monitoring and Report Viewer でのシステムの動作と設定の管理 15-1
データの削除と増分バックアップの設定 15-3
NFS ステージングの設定 15-7
バックアップからのデータの復元 15-7
ログ収集の表示 15-8
[Log Collection Details] ページ 15-10
ログ メッセージのリカバリ 15-12
スケジューリングされたジョブの表示 15-12
プロセス ステータスの表示 15-14
データ アップグレード ステータスの表示 15-15
障害理由の表示 15-15
障害理由の編集 15-15

電子メール設定の指定 15-16
SNMP プリファレンスの設定 15-16
収集フィルタについて 15-17
収集フィルタの作成および編集 15-17
収集フィルタの削除 15-18
システム アラーム設定の指定 15-18
アラーム syslog ターゲットの設定 15-18
リモート データベース設定の指定 15-18

CHAPTER 16 システム管理者の管理 16-1
管理者ロールおよびアカウントについて 16-2
認証について 16-3
システム管理者およびアカウントの設定 16-3
ロールについて 16-3
ロールの割り当て 16-3
静的ロールの割り当て 16-4
動的ロールの割り当て 16-4
権限 16-4
事前定義済みのロール 16-5
ロールの関連付けの変更 16-6
管理者アカウントとロールの関連付け 16-6
リカバリ管理者アカウント 16-7
管理者アカウントの作成、複製、編集、および削除 16-7
事前定義済みのロールの表示 16-9
ロール プロパティの表示 16-10
管理者の認証設定 16-10
セッション アイドル タイムアウトの設定 16-13
管理者アクセスの設定 16-13
管理アクセス コントロールの使用 16-14
管理者 ID ポリシー 16-15
ルール ベースの ID ポリシーの表示 16-16
ID ポリシー規則のプロパティの設定 16-18
管理者認可ポリシー 16-19
管理者認可ポリシーの設定 16-19
管理者認可規則のプロパティの設定 16-20
管理者のログイン プロセス 16-21
管理者パスワードのリセット 16-22
管理者パスワードの変更 16-22

自分の管理者パスワードの変更 16-22
別の管理者のパスワードのリセット 16-23

CHAPTER 17 システムの動作の設定 17-1
分散展開について 17-2
セカンダリ サーバのアクティベーション 17-3
セカンダリ サーバの削除 17-4
セカンダリ サーバの昇格 17-4
ローカル モードについて 17-4
完全な複製について 17-5
ハードウェアの置き換えの指定 17-5
スケジューリング バックアップ 17-6
スケジューリング バックアップの作成、複製、および編集 17-6
プライマリ インスタンスとセカンダリ インスタンスのバックアップ 17-8
バックアップ / 復元後のプライマリ インスタンスとセカンダリ インスタンスの同期 17-9
インスタンスの編集 17-9
プライマリ インスタンスの表示および編集 17-10
セカンダリ インスタンスの表示および編集 17-13
セカンダリ インスタンスの削除 17-14
セカンダリ インスタンスのアクティベーション 17-14
プライマリ インスタンスへのセカンダリ インスタンスの登録 17-15
[Distributed System Management] ページでのセカンダリ インスタンスの登録解除 17-18
[Deployment Operations] ページでのセカンダリ インスタンスの登録解除 17-18
[Distributed System Management] ページでのセカンダリ インスタンスの昇格 17-19
[Deployment Operations] ページでのセカンダリ インスタンスの昇格 17-20
プライマリ インスタンスからのセカンダリ インスタンスの複製 17-20
[Distributed System Management] ページでのセカンダリ インスタンスの複製 17-21
[Deployment Operations] ページでのセカンダリ インスタンスの複製 17-21
プライマリ サーバからのプライマリ インスタンスの IP アドレスの変更 17-22
フェールオーバー 17-23
[Deployment Operations] ページでのローカル モード インスタンスの作成 17-24
ソフトウェア リポジトリの作成、複製、編集、および削除 17-25
Web インターフェイスおよび CLI でのソフトウェア リポジトリの管理 17-26

CHAPTER 18 システム管理設定の管理 18-1
グローバル システム オプションの設定 18-1
TACACS+ の設定 18-1
EAP-TLS の設定 18-2

PEAP の設定 18-3
EAP-FAST の設定 18-3
EAP-FAST PAC の生成 18-4
RSA SecurID プロンプトの設定 18-4
ディクショナリの管理 18-5
RADIUS 属性と TACACS+ 属性の表示 18-5
RADIUS ベンダー固有属性の作成、複製、および編集 18-6
RADIUS ベンダー固有サブ属性の作成、複製、および編集 18-7
RADIUS ベンダー固有サブ属性の表示 18-9
ID ディクショナリの設定 18-10
内部ユーザ ID 属性の作成、複製、および編集 18-10
内部 ID 属性の設定 18-11
内部ユーザ ID 属性の削除 18-12
内部ホスト ID 属性の作成、複製、および編集 18-13
内部ホスト ID 属性の削除 18-13
[Internal Identity Store] でのユーザへのスタティック IP アドレスの追加 18-14
ローカル サーバ証明書の設定 18-14
ローカル サーバ証明書の追加 18-15
サーバ証明書のインポートおよびプロトコルとの関連付け 18-16
自己署名証明書の生成 18-16
証明書署名要求の生成 18-17
CA 署名付き証明書のバインド 18-18
証明書の編集と更新 18-19
証明書の削除 18-20
証明書のエクスポート 18-20
未処理の署名要求の表示 18-21
ログの設定 18-21
リモート ログ ターゲットの設定 18-22
リモート ログ ターゲットの削除 18-23
ローカル ログの設定 18-24
ローカル ログ データの削除 18-24
ロギング カテゴリの設定 18-24
グローバル ロギング カテゴリの設定 18-25
インスタンスごとのロギング カテゴリの設定 18-30
インスタンスごとのセキュリティおよびログの設定 18-31
インスタンスごとのリモート syslog ターゲットの設定 18-32
ロギング カテゴリの表示 18-33
ログ コレクタの設定 18-34
ログ メッセージ カタログの表示 18-34

ライセンスの概要 18-35
ライセンスの種類 18-35
ライセンス ファイルのインストール 18-36
基本ライセンスの表示 18-38
基本サーバ ライセンスのアップグレード 18-39
ライセンス機能オプションの表示 18-40
展開ライセンス ファイルの追加 18-41
展開ライセンス ファイルの削除 18-42
使用可能なダウンロード 18-42
移行ユーティリティ ファイルのダウンロード 18-43
UCP Web サービス ファイルのダウンロード 18-43
サンプル Python スクリプトのダウンロード 18-43
Rest サービスのダウンロード 18-44

CHAPTER 19 ロギングの概要 19-1
ロギングについて 19-1
ログ ターゲットの使用方法 19-2
ロギング カテゴリ 19-2
グローバルおよびインスタンスごとのロギング カテゴリ 19-4
ログ メッセージの重大度レベル 19-4
ローカル ストア ターゲット 19-5
重大なログ ターゲット 19-7
リモート Syslog サーバ ターゲット 19-8
レポート サーバ ターゲットの監視 19-10
ログ メッセージの表示 19-10
デバッグ ログ 19-11
ACS 4.x と ACS 5.4 のロギング 19-12

APPENDIX A AAA プロトコル A-1
一般的な使用例 A-1
デバイス管理（TACACS+） A-1
セッション アクセス要求（デバイス管理 [TACACS+]） A-2
コマンド認可要求 A-2
ネットワーク アクセス（EAP 使用および未使用の RADIUS） A-2
EAP 認証を使用しない RADIUS ベースのフロー A-3
EAP 認証を使用する RADIUS ベースのフロー A-3
アクセス プロトコル：TACACS+ および RADIUS A-5
TACACS+ の概要 A-5

RADIUS の概要 A-6
RADIUS VSA A-6
AAA サーバとしての ACS 5.4 A-7
ACS 5.4 での RADIUS 属性サポート A-8
RADIUS 属性の書き換え動作 A-9
RADIUS アクセス要求 A-11

APPENDIX B ACS 5.4 での認証 B-1
認証方式の検討 B-1
認証とユーザ データベース B-1
PAP B-2
RADIUS PAP 認証 B-3
EAP B-3
EAP-MD5 B-5
EAP-MD5 の概要 B-5
ACS 5.4 での EAP-MD 5 フロー B-5
EAP-TLS B-6
EAP-TLS の概要 B-6
ユーザ証明書認証 B-6
PKI 認証 B-7
PKI クレデンシャル B-8
PKI の使用方法 B-8
固定管理証明書 B-9
信頼証明書のインポート B-9
ローカル証明書の取得 B-9
ACS サーバ証明書のインポート B-10
自己署名証明書の初期生成 B-10
証明書の生成 B-10
クレデンシャルのエクスポート B-11
クレデンシャルの配布 B-12
ハードウェアの置換と証明書 B-12
暗号機密資料のセキュリティ保護 B-12
秘密キーとパスワードのバックアップ B-13
ACS 5.4 での EAP-TLS フロー B-13
PEAPv0/1 B-14
PEAP の概要 B-15
サポートされる PEAP 機能 B-16
ACS 5.4 での PEAP フロー B-17
TLS トンネルの作成 B-18

MSCHAPv2 による認証 B-19
EAP-FAST B-19
EAP-FAST の概要 B-19
EAP-FAST の利点 B-21
ACS 5.4 での EAP-FAST B-21
マスターキーについて B-22
PAC について B-22
プロビジョニング モード B-23
PAC のタイプ B-23
ACS でサポートされる PAC の機能 B-25
マスターキー生成と PAC TTL B-27
TLS 再ネゴシエーション用の EAP-FAST B-27
ACS 5.4 での EAP-FAST フロー B-27
EAP-FAST PAC 管理 B-28
キー配布アルゴリズム B-29
EAP-FAST PAC-Opaque のパックとアンパック B-29
無効化の方式 B-29
ACS 4.x からの PAC の移行 B-30
RADIUS キー ラップありの EAP 認証 B-30
EAP-MSCHAPv2 B-31
EAP-MSCHAPv2 の概要 B-31
ユーザ認証用の MSCHAPv2 B-31
パスワード変更のための MSCHAPv2 B-31
AD に対する Windows マシン認証 B-32
ACS 5.4 での EAP-MSCHAPv2 フロー B-32
CHAP B-32
LEAP B-32
証明書属性 B-33
証明書のバイナリ比較 B-33
テキスト属性に関連する規則 B-34
証明書の失効 B-34
マシン認証 B-35
認証プロトコルと ID ストアの互換性 B-36

APPENDIX C **オープン ソース ライセンス通知** C-1
通告 C-1
OpenSSL/Open SSL Project C-1
License Issues C-1

GLOSSARY

INDEX

はじめに

このマニュアルでは、Cisco Secure Access Control System（ACS）5.4 の使用方法について説明します。

対象読者

このマニュアルは、ACS を使用したり、ネットワークやアプリケーションのセキュリティをセットアップおよび管理するセキュリティ管理者を対象としています。

表記法

このマニュアルで使用する表記法では、^ 記号は *Ctrl* キーを表します。たとえば、**^z** というキーの組み合わせは、Ctrl キーを押しながら z キーを押すことを意味します。

コマンドの説明では、次の表記法を使用しています。

- システム プロンプトが含まれる例はインタラクティブなセッションを示し、プロンプトでコマンドを入力する必要があります。システム プロンプトは、現在の EXEC コマンド インタープリタのレベルを示しています。たとえば、プロンプト `Router>` はユーザ レベル、プロンプト `Router#` は *特権*レベルであることを表しています。通常、特権レベルにアクセスするにはパスワードが必要です。
- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 角カッコ（[ ]）の中の要素は、省略可能です。
- 必ずいずれか 1 つを選択しなければならないキーワードは、波カッコ（{}）で囲み、縦棒（|）で区切って示しています。

例を挙げて説明する場合は、次の表記法を使用しています。

- 端末セッションおよびコンソール画面例は、`screen` フォントで示しています。
- ユーザが入力する情報は、**太字の `screen` フォント**で示しています。
- パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
- システム プロンプトに対するデフォルトの応答は、角カッコ（[]）で囲んで示しています。
- 行の先頭に感嘆符（!）がある場合には、コメント行であることを示します。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記載されています。

ワンポイントアドバイス 「*時間節約*」の意味です。ここに紹介している方法で作業を行うと、時間を短縮できます。

（注） 「*注釈*」です。次に進む前に検討する必要がある重要情報、役に立つ情報、このマニュアル以外の参照資料などを紹介しています。

マニュアルの更新

表 1 に、『*Cisco Secure Access Control System 5.4 ユーザ ガイド*』の更新内容を示します。

表 1　『Cisco Secure Access Control System 5.4 ユーザ ガイド』の更新内容

日付	説明
2012/10/30	マニュアルを Cisco 3415 Secure Access Control System の情報で更新しました。
2012/10/23	Cisco Secure Access Control System, Release 5.4。

関連資料

表 2 に、Cisco.com で参照できる関連技術マニュアル セットを示します。Cisco.com ですべての製品のエンドユーザ向けマニュアルを検索するには、次の URL に移動してください。
http://www.cisco.com/go/techdocs

[Products] > [Security] > [Access Control and Policy] > [Policy and Access Management] > [Cisco Secure Access Control System] を選択します。

（注） 初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、http://www.cisco.com で確認してください。

表 2　製品マニュアル

マニュアル タイトル	利用形式
『Cisco Secure Access Control System In-Box Documentation and China ROHS Pointer Card』	http://www.cisco.com/en/US/products/ps9911/products_licensing_information_listing.html
『License and Documentation Guide for Cisco Secure Access Control System 5.4』	http://www.cisco.com/en/US/products/ps9911/products_documentation_roadmaps_list.html
『Release Notes for Cisco Secure Access Control System 5.4』	http://www.cisco.com/en/US/products/ps9911/prod_release_notes_list.html
『Migration Guide for Cisco Secure Access Control System 5.4』	http://www.cisco.com/en/US/products/ps9911/prod_installation_guides_list.html

表 2　　製品マニュアル （続き）

マニュアル タイトル	利用形式
『*CLI Reference Guide for Cisco Secure Access Control System 5.4*』	http://www.cisco.com/en/US/products/ps9911/prod_command_reference_list.html
『*Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.4*』	http://www.cisco.com/en/US/products/ps9911/products_device_support_tables_list.html
『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.4*』	http://www.cisco.com/en/US/products/ps9911/prod_installation_guides_list.html
『*Software Developer's Guide for the Cisco Secure Access Control System 5.4*』	http://www.cisco.com/en/US/products/ps9911/products_programming_reference_guides_list.html
『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System 5.4*』	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/regulatory/compliance/csacsrcsi.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

ACS 5.4 の導入

ここでは、次の内容について説明します。

- 「ACS の概要」（P.1-1）
- 「ACS の分散展開」（P.1-2）
- 「ACS 管理インターフェイス」（P.1-3）

ACS の概要

ACS は、規格準拠の認証、許可、アカウンティング（AAA）サービスをネットワークに提供するポリシーベースのセキュリティ サーバです。ACS を使用すると、シスコおよびシスコ以外のデバイスとアプリケーションを簡単に管理できます。

有力な企業ネットワーク アクセス コントロール プラットフォームである ACS は、ネットワーク アクセス コントロールと ID 管理の統合ポイントとして機能します。

ACS 5.x では、動的な条件と属性に基づいてネットワーク アクセスを制御できる、ルール ベースのポリシー モデルを提供します。ルール ベースのポリシーは、複雑なアクセス ポリシー ニーズを満たす設計になっています。ACS のルール ベースのポリシー モデルの詳細については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

2 つの主要な AAA プロトコルである RADIUS と TACACS+ のより強力なコンテキストにおいて、ACS では次の基本的な機能領域を提供します。

- RADIUS プロトコルのフレームワークにおいては、ACS ではネットワークへの有線および無線アクセスをユーザおよびホスト マシンごとに制御し、使用されるネットワーク リソースのアカウンティングを管理します。

  ACS では、PAP、CHAP、MSCHAPv1、MSCHAPv2 などの複数の RADIUS ベースの認証方式がサポートされています。さらに、EAP-MD5、LEAP、PEAP、EAP-FAST、EAP-TLS など、EAP プロトコル ファミリの多くのメンバーもサポートされています。

  また、ACS では、PEAP または EAP-FAST と連携する場合、EAP-MSCHAPv2、EAP-GTC、および EAP-TLS もサポートされます。認証方式の詳細については、「Authentication in ACS 5.4」を参照してください。

- TACACS+ プロトコルのフレームワークにおいては、ACS を使用すると、スイッチ、無線アクセス ポイント、ルータ、ゲートウェイなどのシスコおよびシスコ以外のネットワーク デバイスを簡単に管理できます。また、ダイヤルアップ、バーチャル プライベート ネットワーク（VPN）、ファイアウォールなどのサービスやエンティティの管理にも役立ちます。

ACS は、ネットワークに接続しようとするユーザとデバイスを識別する、ネットワーク内のポイントとなります。この ID 設定は、ローカル ユーザ認証用の ACS 内部 ID リポジトリを使用して直接実行される場合、および、外部 ID リポジトリを使用して実行される場合があります。

たとえば、ACS では、Active Directory を外部 ID リポジトリとして使用してユーザを認証し、ネットワークへのユーザ アクセス権を付与できます。ID の作成およびサポートされる ID サービスの詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

ACS には、ACS の展開の管理に役立つ高度な監視ツール、レポート ツール、およびトラブルシューティング ツールが備えられています。ACS の監視機能、レポート機能、およびトラブルシューティング機能の詳細については、第 11 章「ACS での監視とレポート」を参照してください。

ACS を使用したデバイス管理およびネットワーク アクセス シナリオの詳細については、第 4 章「ACS を使用した一般的なシナリオ」を参照してください。

Cisco Secure ACS には次の機能があります。

- VPN および無線ユーザのアクセス ポリシーの適用
- デバイス管理の簡略化
- 高度な監視ツール、レポート ツール、およびトラブルシューティング ツールの提供

ACS 5.3 と比較して、ACS 5.4 にはいくつかの変更点および拡張機能があります。新機能および変更された機能の完全なリストは、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/release/notes/acs_54_rn.html

関連トピック

- 「ACS の分散展開」（P.1-2）
- 「ACS 管理インターフェイス」（P.1-3）

ACS の分散展開

ACS 5.4 は、標準の Cisco Linux ベース アプライアンスにあらかじめ搭載された状態で提供され、完全な分散展開をサポートします。

ACS の展開は、単一のインスタンスで構成されることも、複数のインスタンスで構成されることもあります。後者の場合、インスタンスは分散環境に展開され、システム内のすべてのインスタンスが集中管理されます。この場合、1 つの ACS インスタンスが*プライマリ インスタンス*となり、その他の ACS インスタンスは*セカンダリ インスタンス*としてプライマリ インスタンスに登録できます。すべてのインスタンスが展開全体に対する設定を持つため、設定データには冗長性が発生します。

プライマリ インスタンスによって、展開されたインスタンスの設定が集中化されます。プライマリ インスタンスで行った設定変更は、セカンダリ インスタンスに自動的に複製されます。

セカンダリ インスタンスへの*完全複製*を強制実行できます。完全複製は、新しいセカンダリ インスタンスの登録時、およびセカンダリ インスタンスとプライマリ インスタンスの間の複製のギャップが大きい場合に使用されます。

関連項目

- 「ACS 4.x と 5.4 の複製」（P.1-2）

ACS 4.x と 5.4 の複製

ACS 4.x では、プライマリ インスタンスからセカンダリ インスタンスに複製するデータベース オブジェクト タイプ（またはクラス）を選択する必要があります。オブジェクトを複製すると、設定の完全なコピーがセカンダリ インスタンスに作成されます。

ACS 5.4 では、プライマリ インスタンスに加えられたすべての設定変更が、セカンダリ インスタンスに即時に複製されます。*前回の複製後*に行われた設定変更だけがセカンダリ インスタンスに伝播されます。

ACS 4.x では差分複製機能がなく、完全複製機能だけが備えられていたため、複製のためのサービス ダウンタイムが発生しました。ACS 5.4 では、サービス ダウンタイムのない差分複製機能が備えられています。

また、設定変更が複製されなかった場合は、セカンダリ インスタンスへの完全複製を*強制実行*することもできます。完全複製は、新しいセカンダリ インスタンスを登録するとき、およびセカンダリ インスタンスとプライマリ インスタンスの間の複製のギャップが大きい場合に使用されます。

表 1-1 に、ACS 4.x と 5.4 の複製の違いをいくつか示します。

表 1-1　ACS 4.x と 5.4 の複製の違い

ACS 4.x	ACS 5.4
複製するデータ項目を選択できる。	複製するデータ項目を選択できない。デフォルトでは、すべてのデータ項目が複製されます。
マルチレベルまたはカスケード複製がサポートされている。	固定のフラット複製だけがサポートされている。カスケード複製はサポートされていません。
外部データベース設定などの一部のデータ項目は複製されない。	データベース キー、データベース証明書およびマスター キーを除く、すべてのデータ項目が複製される。サーバ証明書、証明書署名要求（CSR）、秘密キーは複製されますが、インターフェイスには表示されません。

分散展開の設定の詳細については、「システムの動作の設定」（P.17-1）を参照してください。

（注）　Network Address Translation（NAT）は、ACS 分散展開環境ではサポートされていません。つまり、プライマリまたはセカンダリ インスタンスのネットワーク アドレスを変換すると、データベースの複製が正しく機能しないことがあり、共有秘密の不一致エラーが表示される場合があります。

ACS のライセンス モデル

ACS を操作するには、有効なライセンスが必要です。Web インターフェイスに初めてアクセスするときに、ACS によって有効なベース ライセンスのインストールを要求するプロンプトが表示されます。分散展開では、各サーバに固有の基本ライセンスが必要です。

インストールできるライセンスの種類の詳細については、「ライセンスの種類」（P.18-35）を参照してください。ライセンスの詳細については、「ライセンスの概要」（P.18-35）を参照してください。

関連項目

- 「ACS の分散展開」（P.1-2）

ACS 管理インターフェイス

ここでは、次の内容について説明します。

- 「ACS Web ベース インターフェイス」（P.1-4）

- 「ACS コマンドライン インターフェイス」（P.1-4）
- 「ACS プログラム インターフェイス」（P.1-5）

ACS Web ベース インターフェイス

ACS Web ベース インターフェイスを使用して、ACS の展開を完全に設定し、監視とレポートの操作を実行できます。Web インターフェイスでは、設定する領域に関わりなく、一貫性のあるユーザ エクスペリエンスが提供されます。

ACS Web インターフェイスは、6.x から 9.x までの Microsoft Internet Explorer の HTTPS 対応バージョンおよび 3.x から 10.x までの Mozilla Firefox バージョンでサポートされます。

新しい Web インターフェイス設計と構成には、次の機能があります。

- ユーザの視点でのポリシー管理に基づいて構成された、新しいポリシー モデルを反映する。新しいポリシー モデルは、ポリシー要素間に以前に存在していた複雑な相互関係が分離されているため、使いやすさが向上しました。

  ポリシー要素とは、たとえば、ユーザ グループ、ネットワーク デバイス グループ（NDG）、ネットワーク アクセス フィルタ、ネットワーク アクセス プロファイルなどです。

- 多くの一般的なシナリオに適用できる論理的な順序で、設定タスクを提示する。

  たとえば、最初に [Policy Elements] ドロワでポリシーの条件と認可を設定したあと、[Policies] ドロワに移動し、定義済みポリシー要素を使用してポリシーを設定します。

- 項目のリストのソートやフィルタリングなどの新しいページ機能を提供する。

詳細については、「Web インターフェイスの使用方法」（P.5-3）を参照してください。

関連トピック

- 「ACS コマンドライン インターフェイス」（P.1-4）

ACS コマンドライン インターフェイス

テキストベースのインターフェイスである ACS コマンドライン インターフェイス（CLI）を使用して、一部の設定および操作タスクと監視を実行できます。ACS 固有の CLI にアクセスするには、ACS 5.4 による管理者認証が必要です。

ACS 以外のコンフィギュレーション モードを使用するには、ACS 管理者である必要はなく、また、ACS 5.4 にログインする必要もありません。ACS コンフィギュレーション モードのコマンド セッションは、診断ログに記録されます。

ACS 5.4 は、Cisco 1121 Secure Access Control System（CSACS-1121）または Cisco 3415 Secure Access Control System（CSACS-3415）で出荷されます。ADE-OS ソフトウェアでは、次のコマンド モードがサポートされています。

- EXEC：これらのコマンドを使用して、システムレベルの操作タスクを実行します。操作タスクとは、たとえば、アプリケーションのインストール、起動、停止、ファイルのコピーとインストール、バックアップの復元、情報の表示などです。

  また、特定の EXEC モード コマンドには、ACS 固有の機能があります。たとえば、ACS インスタンスの開始、ACS ログの表示とエクスポート、ACS 設定の出荷時のデフォルト設定への復元などです。このようなコマンドについては、マニュアルに詳しく記載されています。

- ACS 設定：これらのコマンドを使用して、ACS の管理およびランタイム コンポーネントのデバッグ ログ レベルを設定（イネーブルまたはディセーブル）します。また、システム設定を表示します。
- 設定：これらのコマンドを使用して、ADE-OS 環境のアプライアンス サーバに対して追加の設定タスクを実行します。

（注）　CLI には、設定のリセット オプションがあります。このオプションが発行されると、すべての ACS 設定情報がリセットされますが、ネットワーク設定などのアプライアンス設定は保持されます。

CLI の使用については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

関連項目

- 「ACS Web ベース インターフェイス」（P.1-4）

ACS プログラム インターフェイス

ACS 5.4 には、ソフトウェア開発者とシステム インテグレータが一部の ACS 機能にプログラムを通じてアクセスできる Web サービスおよびコマンドライン インターフェイス（CLI）コマンドが備えられています。ACS 5.4 では、ACS を監視およびトラブルシューティングするカスタム アプリケーションを作成する場合に使用できる、Monitoring and Report Viewer データベースにもアクセスできます。

UCP Web サービスでは、ACS 内部データベースに定義されているユーザが、最初に認証を受けてから自身のパスワードを変更できます。ACS では、企業に展開できるカスタム Web ベース アプリケーションを作成できるように UCP Web サービスを公開しています。

Monitoring and Report Viewer Web サービスでは、ACS のイベントをトラッキングおよびトラブルシューティングするカスタム アプリケーションを作成できます。

ACS によって提供されている CLI コマンドを使用して、ACS オブジェクトに対する Create, Read, Update, and Delete（CRUD; 作成、読み取り、更新、および削除）操作を実行するシェル スクリプトを開発できます。また、自動化されたシェル スクリプトを作成して、一括操作を実行することもできます。

REST PI（Representational State Transfer Programming Interface）は、ユーザ、ホスト、ID グループ、ネットワーク デバイス、ネットワーク デバイス グループ、およびネットワーク デバイス グループ タイプなどのエンティティを自分の管理アプリケーションで管理し、ACS にこれらのエンティティを移動することができるようにします。このように、これらのエンティティを定義して、その後で独自のシステムや ACS で使用できます。

これらの Web サービスおよびそれらの機能にアクセスする方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/acs_sdk.html

ACS でサポートされているハードウェア モデル

表 1-2 に、ACS 5.4 でサポートされているハードウェア モデルの詳細を示します。

表 1-2　ACS 5.4 でサポートされているハードウェア モデル

Config	HDD	RAM	NIC
UCS 3415	500 GB	8 GB	2 x 2（4-1 Gb）
IBM 1121	2 x 250 GB	4 GB	4 x 10/100/1000 RJ-45
CAM25-1-2-4	2 x 250 GB	4 x 1 GB	2 x 1 GE
VMware ESX i5.0	60 ～ 750 GB	4 GB	NIC x 2

CHAPTER 2

ACS 4.x から ACS 5.4 への移行

ACS 4.x では、TACACS+ コマンド セットなどのポリシーおよび認証情報は、ユーザおよびユーザ グループ レコードに格納されます。ACS 5.4 では、ポリシーおよび認証情報は独立した共有コンポーネントであり、ポリシーを設定するときに、構築ブロックとして使用します。

新しいポリシー モデルの構築ブロック、つまりポリシー要素を使用してポリシーを再構築すると、新しいポリシー モデルを最大限かつ効率的に活用できます。この方法を使用すると、適切な ID グループ、ネットワーク デバイス グループ（NDG）、条件、認可プロファイル、およびルールを作成することが必要となります。

ACS 5.4 には、ACS 4.x の移行サポート バージョンから ACS 5.4 マシンにデータを転送する、移行ユーティリティが備えられています。ACS 5.4 移行プロセスでは、ACS 5.4 にデータをインポートする前に、手動でデータを解決する管理的介入が必要となる場合があります。

このプロセスは、バージョン ACS 3.x から ACS 4.x へのアップグレード プロセスとは異なります。ACS 3.x から ACS 4.x へのアップグレード プロセスでは、ACS 4.x システムが ACS 3.x と同じ方法で動作するため、管理的介入は不要です。

ACS 5.4 の移行ユーティリティでは、展開内のすべての ACS 4.x サーバを ACS 5.4 に移行する複数インスタンス移行がサポートされています。複数インスタンスの移行の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/migration_guide.html

アップグレードは、ACS 5.3 サーバから ACS 5.4 へのデータ転送プロセスです。アップグレード プロセスの詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/installation/guide/csacs_upg.html

この章の内容は、次のとおりです。

- 「移行プロセスの概要」（P.2-2）
- 「はじめる前に」（P.2-3）
- 「移行ファイルのダウンロード」（P.2-3）
- 「ACS 4.x から ACS 5.4 への移行」（P.2-4）
- 「ACS 4.x から ACS 5.4 への機能マッピング」（P.2-6）
- 「移行の一般的なシナリオ」（P.2-8）

移行プロセスの概要

移行ユーティリティは、次の 2 つのフェーズでデータ移行プロセスを完了します。

- 分析およびエクスポート
- インポート

分析およびエクスポート フェーズでは、5.4 にエクスポートするオブジェクトを指定します。移行ユーティリティではこれらのオブジェクトを分析し、データを集約してエクスポートします。

分析およびエクスポート フェーズが完了すると、移行ユーティリティによって、すべてのデータ互換性エラーを示すレポートが生成されます。このエラーは、これらのオブジェクトを正常に 5.4 にインポートするために手動で解決できます。

分析およびエクスポート フェーズは反復的なプロセスであり、インポートされるデータに確実にエラーがなくなるまで複数回繰り返すことができます。分析およびエクスポート フェーズが完了すると、インポート フェーズを実行してデータを ACS 5.4 にインポートできるようになります。

ここでは、次の内容について説明します。

- 「移行の要件」（P.2-2）
- 「移行サポート バージョン」（P.2-2）

移行の要件

移行ユーティリティを実行するには、次のマシンを配置する必要があります。

- 移行元の ACS 4.x マシン：このマシンには、ACS 4.x Solution Engine または ACS for Windows 4.x マシンのいずれかを使用できます。移行元のマシンでは、移行サポート バージョンの ACS が稼働している必要があります。詳細については、「移行サポート バージョン」（P.2-2）を参照してください。
- 移行マシン：このマシンは、移行元のマシンと同じバージョンの ACS（パッチを含む）が稼働している Windows プラットフォームである必要があります。ACS 運用マシンまたは ACS アプライアンス マシンは、移行マシンとして使用できません。ACS for Windows が稼働している Windows サーバである必要があります。移行マシンには 2 GB RAM が必要です。
- 移行先の ACS 5.4 マシン：インポート プロセスを開始する前に、ACS 5.4 設定データをバックアップし、ACS 5.4 で移行インターフェイスがイネーブルになっていることを確認します。新しい ACS 5.4 データベースにデータをインポートすることを推奨します。移行インターフェイスをイネーブルにするには、ACS CLI から次のように入力します。

  ```
  acs config-web-interface migration enable
  ```

移行サポート バージョン

ACS 5.4 では、次の ACS 4.x バージョンからの移行がサポートされています。

- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1

（注）　ここに記載されている移行サポート バージョンに対して、最新のパッチをインストールしておく必要があります。また、他のバージョンの ACS 4.x がインストールされている場合は、ACS 5.4 に移行する前に、サポート対象バージョンのいずれかにアップグレードして、そのバージョンの最新パッチをインストールする必要があります。

はじめる前に

ACS 4.x から ACS 5.4 にデータを移行する前に、次のことを確認します。

- ACS 4.x 移行元マシンにデータベース破損の問題がないこと。
- 移行元マシンと移行マシンに、同じ ACS バージョン（パッチを含む）がインストールされていること。
- 移行マシンに単一の IP アドレスが設定されていること。
- 移行元の ACS 4.x データがバックアップしてあること。
- 移行マシンと ACS 5.4 サーバの間に完全なネットワーク接続があること。
- ACS 5.4 サーバで移行インターフェイスがイネーブルになっていること。
- 移行ユーティリティの実行中は、ACS 5.4 のデフォルトのスーパー管理者アカウント **acsadmin** だけを使用すること。

リモート デスクトップを使用して、移行マシンに接続し、移行ユーティリティを実行することはできません。移行ユーティリティは移行マシンで実行するか、VNC を使用して移行マシンに接続する必要があります。

（注）　ACS 5.4 移行ユーティリティは、Windows 2008 64 ビットではサポートされません。

移行ファイルのダウンロード

ACS 5.4 の移行アプリケーション ファイルおよび移行ガイドをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Migration Utility] を選択します。

[Migration from 4.x] ページが表示されます。

ステップ 2　[Migration application files] をクリックして、移行ユーティリティを実行する場合に使用するアプリケーション ファイルをダウンロードします。

ステップ 3　[Migration Guide] をクリックして、『*Migration Guide for Cisco Secure Access Control System 5.4*』をダウンロードします。

ACS 4.x から ACS 5.4 への移行

ACS 4.x の任意の移行サポート バージョンから ACS 5.4 にデータを移行できます。移行ユーティリティによって、次の ACS 4.x データ エンティティが移行されます。

- ネットワーク デバイス グループ（NDG）
- AAA クライアントおよびネットワーク デバイス
- 内部ユーザ
- （Interface Configuration セクションの）ユーザ定義フィールド
- ユーザ グループ
- 共有シェル コマンド認可セット
- （ユーザ属性に移行される）ユーザ TACACS+ Shell Exec 属性
- （シェル プロファイルに移行される）グループ TACACS+ Shell Exec 属性
- ユーザ TACACS+ コマンド認可セット
- グループ TACACS+ コマンド認可セット
- 共有ダウンロード可能 ACL
- EAP-FAST マスター キー
- 共有 RADIUS Authorization Component（RAC; RADIUS 認可コンポーネント）
- RADIUS VSA

（注） 移行ユーティリティでは、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）設定データは移行されず、証明書の移行もサポートされていません。

ACS 4.x から ACS 5.4 にデータを移行するには、次の手順を実行します。

ステップ 1　ACS 4.x サーバで、現在、移行サポート バージョンのいずれも稼働していない場合は、ACS 4.x バージョンを移行サポート バージョンにアップグレードします。

ACS の移行サポート バージョンのリストについては、「移行サポート バージョン」（P.2-2）を参照してください。

ステップ 2　移行マシン（Windows サーバ）に同じ移行サポート バージョンの ACS をインストールします。

ステップ 3　ACS 4.x データをバックアップして、移行マシンで復元します。

ステップ 4　移行マシンに移行ユーティリティを保存します。

移行ユーティリティは、Installation and Recovery DVD から取得できます。

ステップ 5　移行マシンで、移行ユーティリティの分析およびエクスポート フェーズを実行します。

ステップ 6　分析およびエクスポート フェーズで発生した問題を解決します。

ステップ 7　移行マシンで、移行ユーティリティのインポート フェーズを実行します。

インポート フェーズでは、データを 5.4 サーバにインポートします。

（注）　大規模な内部データベースがある場合、スタンドアロンの 5.x プライマリ サーバにデータをインポートし、複数のセカンダリ サーバに接続しているサーバにはデータをインポートしないことを推奨します。データの移行が完了すると、セカンダリ サーバをスタンドアロンの 5.x プライマリ サーバに登録できるようになります。

移行ユーティリティの使用方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/migration_guide.html

データを移行したあと、移行されたオブジェクトを使用してポリシーを再構築できます。

ACS 4.x から ACS 5.4 への機能マッピング

ACS 5.4 では、認可、シェル プロファイル、属性、およびその他のポリシー要素を、ユーザまたはグループ定義の一部としてではなく、独立した再利用可能なオブジェクトとして定義します。

表 2-1 に、ACS 5.4 での ID、ネットワーク リソース、およびポリシー要素の設定場所を示します。この表を使用して、移行したデータ ID を表示または変更します。ACS 5.4 ポリシー モデルの概要については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

表 2-1　ACS 4.x から ACS 5.4 への機能マッピング

設定内容	ACS 4.x での選択	ACS 5.4 での選択	5.4 の追加情報
ネットワーク デバイス グループ	[Network Configuration] ページ	[Network Resources] > [Network Device Groups] 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。	NDG はポリシー ルール内の条件として使用できます。 ACS 5.4 では NDG 共有パスワードがサポートされていません。移行後は、メンバー デバイスに NDG 共有パスワード情報が格納されます。
ネットワーク デバイスおよび AAA クライアント	[Network Configuration] ページ	[Network Resources] > [Network Devices and AAA Clients] 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。	RADIUS キー ラップのキー（KEK および MACK）は、ACS 4.x から ACS 5.4 に移行されます。
ユーザ グループ	[Group Setup] ページ	[Users and Identity Stores] > [Identity Groups] 「ID 属性の管理」（P.8-7）を参照してください。	ID グループはポリシー ルール内の条件として使用できます。
内部ユーザ	[User Setup] ページ	[Users and Identity Stores] > [Internal Identity Stores] > [Users] 「内部 ID ストアの管理」（P.8-4）を参照してください。	ACS 5.4 は、内部 ID ストアに対してだけ内部ユーザを認証します。 認証に外部データベースを使用していた移行済みユーザには、最初のアクセス時に変更が必要なデフォルトの認証パスワードが割り当てられます。
内部ホスト	[Network Access Profiles] > [Authentication]	[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] 「ID ストアでのホストの作成」（P.8-16）を参照してください。	内部ホストは、[Host Lookup] の ID ポリシーで使用できます。
ID 属性（ユーザ定義フィールド）	[Interface Configuration] > [User Data Configuration]	[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] 「ディクショナリの管理」（P.18-5）を参照してください。	定義済みの ID 属性フィールドが [User Properties] ページに表示されます。これらをアクセス サービス ポリシーの条件として使用できます。

表 2-1　ACS 4.x から ACS 5.4 への機能マッピング （続き）

設定内容	ACS 4.x での選択	ACS 5.4 での選択	5.4 の追加情報
コマンド セット（コマンド認可セット）	次のいずれかが必要です。 • [Shared Profile Components] > [Command Authorization Set] • [User Setup] ページ • [Group Setup] ページ	[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Command Set] 「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-31）を参照してください。	デバイス管理アクセス サービスの認可ポリシー ルールの結果として、コマンド セットを追加できます。
Shell exec パラメータ	[User Setup] ページ	[System Administration] > [Dictionaries] > [Identity] > [Internal Users] 「ディクショナリの管理」（P.18-5）を参照してください。	定義済みの ID 属性フィールドが [User Properties] ページに表示されます。 これらをアクセス サービス ポリシーの条件として使用できます。
シェル プロファイル（shell exec パラメータまたはシェル コマンド認可セット）	[Group Setup] ページ	[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profile] 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）を参照してください。	デバイス管理アクセス サービスの認可ポリシー ルールの結果として、シェル プロファイルを追加できます。
日時条件（時間帯アクセス） 日時条件は移行できません。ACS 5.4 で再作成する必要があります。	[Group Setup] ページ	[Policy Elements] > [Session Conditions] > [Date and Time] 「日付と時刻の条件の作成、複製、および編集」（P.9-3）を参照してください。	日時条件は、サービス セレクション ポリシーのポリシー ルールまたはアクセス サービスの認可ポリシーに追加できます。
RADIUS 属性	次のいずれかが必要です。 • [Shared Profile Components] > [RADIUS Authorization Component] • [User Setup] ページ • [Group Setup] ページ ユーザおよびグループ設定の RADIUS 属性は移行できません。ACS 5.4 で再作成する必要があります。	[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profile] > [Common Tasks] タブ または [Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profile] > [RADIUS Attributes] タブ 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-19）を参照してください。	RADIUS 属性は、ネットワーク アクセス認可プロファイルの一部として設定できます。 ネットワーク アクセス サービスの認可ポリシーの結果として認可プロファイルを追加できます。

表 2-1　ACS 4.x から ACS 5.4 への機能マッピング （続き）

設定内容	ACS 4.x での選択	ACS 5.4 での選択	5.4 の追加情報
ダウンロード可能 ACL	共有プロファイル コンポーネント	[Policy Elements] > [Authorization and Permissions] > [Named Permission Objects] > [Downloadable ACLs] 「ダウンロード可能 ACL の作成、複製、および編集」（P.9-33）を参照してください。	ネットワーク アクセス認可プロファイルに Downloadable ACL（DACL; ダウンロード可能 ACL）を追加できます。 認可プロファイルを作成したあと、ネットワーク アクセス サービスの認可ポリシーの結果としてこれを追加できます。
RADIUS VSA	インターフェイス コンフィギュレーション	[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS] > [RADIUS VSA] 「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）を参照してください。	RADIUS VSA 属性は、ネットワーク アクセス認可プロファイルの一部として設定します。 ネットワーク アクセス サービスの認可ポリシーの結果として認可プロファイルを追加できます。

移行の一般的なシナリオ

次に、ACS 5.4 への移行時に発生する一般的なシナリオを示します。

- 「CSACS 1120 の ACS 4.2 から ACS 5.4 への移行」（P.2-8）
- 「ACS 3.x から ACS 5.4 への移行」（P.2-9）
- 「他の AAA サーバから ACS 5.4 へのデータの移行」（P.2-9）

CSACS 1120 の ACS 4.2 から ACS 5.4 への移行

展開において、CSACS 1120 にある ACS 4.2 を ACS 5.4 に移行する場合は、次の手順を実行する必要があります。

ステップ 1　移行マシンに Cisco Secure Access Control Server 4.2 for Windows をインストールします。

ステップ 2　CSACS 1120 で ACS 4.2 データをバックアップします。

ステップ 3　移行マシンでデータを復元します。

ステップ 4　移行マシンで、移行ユーティリティの分析およびエクスポート フェーズを実行します。

ステップ 5　CSACS 1120 に ACS 5.4 をインストールします。

ステップ 6　移行マシンのデータを、ACS 5.4 がインストールされている CSACS 1120 にインポートします。

各手順の詳しい説明については、http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/migration_guide.html を参照してください。

ACS 3.x から ACS 5.4 への移行

使用環境に ACS 3.x を展開している場合、ACS 5.4 への直接移行はできません。次の手順を実行する必要があります。

ステップ 1　ACS 4.x の移行サポート バージョンにアップグレードします。移行サポート バージョンのリストについては、「移行サポート バージョン」（P.2-2）を参照してください。

ステップ 2　ACS 3.x のアップグレード パスを確認します。

- ACS Solution Engine については、次を参照してください：

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.1/installation/guide/solution_engine/upgap.html#wp1120037

- ACS for Windows については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/install.html#wp1102849

ステップ 3　ACS 3.x サーバを ACS 4.x の移行サポート バージョンにアップグレードします。

アップグレード後、ACS 4.x から ACS 5.4 への移行方法を示した手順を実行します。詳細については、『*Migration Guide for Cisco Secure Access Control System 5.4*』を参照してください。

他の AAA サーバから ACS 5.4 へのデータの移行

ACS 5.4 では、ACS Web インターフェイスおよび CLI を使用して、さまざまな ACS オブジェクトの一括インポートを実行できます。インポートできる ACS オブジェクトは次のとおりです。

- ユーザ
- ホスト
- ネットワーク デバイス
- ID グループ
- NDG
- ダウンロード可能 ACL
- コマンド セット

ACS では、カンマ区切り形式（.csv）ファイルを使用して、データの一括インポートを実行できます。データは、ACS が要求する形式で .csv ファイルに入力する必要があります。ACS には、ACS 5.4 にインポート可能なそれぞれのオブジェクト用に .csv テンプレートが用意されています。このテンプレートは Web インターフェイスからダウンロードできます。

他の AAA サーバから ACS 5.4 にデータを移行するには、次の手順を実行します。

ステップ 1　.csv ファイルにデータを入力します。

.csv テンプレートの概要の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1064565

ステップ 2　ACS 5.4 アプライアンスを設定します。

ステップ 3　ACS 5.4 に対してデータの一括インポートを実行します。

ACS オブジェクトの一括インポートの実行の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1056244

これで、他の AAA サーバのデータを ACS 5.4 で使用できます。

CHAPTER 3

ACS 5.x ポリシー モデル

ACS 5.x は、ポリシーベースのアクセス コントロール システムです。ACS 5.x での*ポリシー モデル*という用語は、ポリシー管理者のポリシー要素、ポリシー オブジェクト、およびポリシー規則を表しています。ACS 5.x では、4.x バージョンで使用されていたグループベースのモデルの代わりに、ルール ベース ポリシー モデルが使用されています。

ここでは、次の内容について説明します。

- 「ACS 5.x ポリシー モデルの概要」（P.3-1）
- 「アクセス ポリシー」（P.3-6）
- 「サービス セレクション ポリシー」（P.3-12）
- 「ネットワーク アクセスの認可プロファイル」（P.3-17）
- 「ポリシーおよび ID 属性」（P.3-17）
- 「ポリシーおよびネットワーク デバイス グループ」（P.3-18）
- 「ルール ベース ポリシーの例」（P.3-18）
- 「サービスおよびポリシーの設定フロー」（P.3-19）

（注） ACS 4.x および ACS 5.4 での概念の対応については、「ACS 4.x から ACS 5.4 への機能マッピング」（P.2-6）を参照してください。

ACS 5.x ポリシー モデルの概要

ACS 5.x のルール ベース ポリシー モデルを使用すると、以前のグループベースの手法よりも強力で柔軟なアクセス コントロールを実現できます。

以前のグループベース モデルでは、*グループ*を使用してポリシーを定義していました。これは、グループに次の 3 つのタイプの情報が結合されていたためです。

- 識別情報：この情報は、AD グループまたは LDAP グループでのメンバーシップ、または ACS 内部ユーザの静的割り当てに基づいています。
- その他の制約事項または条件：時間の制限、デバイスの制限など。
- 権限：VLAN または Cisco IOS の特権レベル。

ACS 5.x ポリシー モデルは、次の形式の*規則*に基づいています。

If *condition* then *result*

たとえば、グループベース モデルに関して記述されている次の情報を使用します。

If *identity-condition, restriction-condition* then *authorization-profile*

ACS 5.4 では、条件および結果をグローバルな共有オブジェクトとして定義します。これらを定義しておくと、規則を作成するときに参照できます。ACS 5.4 では、これらの共有オブジェクトに対して*ポリシー要素*という用語を使用しています。ポリシー要素は、規則を作成するための構築ブロックとなります。

表 3-1 に、以前のグループに含まれていたすべての情報をさまざまなポリシー要素によって定義する方法を示します。

表 3-1　ポリシー要素の情報

ACS 4.x グループの情報	ACS 5.4 ポリシー要素の情報
識別情報	• AD グループ メンバーシップおよび属性 • LDAP グループ メンバーシップおよび属性 • ACS 内部 ID グループおよび属性
その他のポリシー条件	• 時刻と日付の条件 • カスタム条件
権限	認可プロファイル

*ポリシー*は、アクセス要求を評価して決定を返すために ACS 5.x で使用される規則セットです。規則セットの例は次のとおりです。

- *認可ポリシー*の規則セットでは、任意のアクセス要求に関する認可の決定が返されます。
- *ID ポリシー*では、任意のアクセス要求の ID 属性の認証方法および取得方法が決定されます。

ACS 5.x では、独立したポリシーの順序（ポリシー ワークフロー）が*アクセス サービス*に編成され、アクセス要求を処理するために使用されます。複数のアクセス サービスを作成して、異なる種類のアクセス要求を処理できます。たとえば、デバイス管理アクセスやネットワーク アクセスなどです。詳細については、「アクセス ポリシー」（P.3-6）を参照してください。

単純なポリシーおよびルール ベース ポリシーを定義できます。ルール ベース ポリシーは、さまざまな条件をテストする複雑なポリシーです。単純なポリシーでは、条件なしですべての要求に対して単一の結果を適用します。

さまざまなタイプのポリシーがあります。

さまざまなタイプのポリシーの詳細については、「ポリシーのタイプ」（P.3-5）を参照してください。

ポリシー モデルの用語の詳細については、「ポリシーの用語」（P.3-3）を参照してください。

関連トピック

- 「ポリシーおよび ID 属性」（P.3-17）
- 「サービスおよびポリシーの設定フロー」（P.3-19）

ポリシーの用語

表 3-2 に、ルール ベース ポリシーの用語を示します。

表 3-2　ルール ベース ポリシーの用語

用語	説明
アクセス サービス	アクセス要求の処理に使用される一連のポリシー セット。ACS 5.x を使用すると、複数のアクセス サービスを定義して、独立および分離された複数のポリシー セットを単一の ACS システムでサポートできます。 2 つのデフォルト アクセス サービスがあります。1 つはデバイス管理用（デバイス シェルまたは CLI への TACACS+ ベースのアクセス）であり、もう一つはネットワーク アクセス用（ネットワーク接続への RADIUS ベースのアクセス）です。
ポリシー要素	ポリシー条件（たとえば、時刻や日付、またはユーザ選択属性に基づくカスタム条件）および権限（認可プロファイルなど）を定義するグローバルな共有オブジェクト。ポリシー要素は、ポリシー規則を作成するときに参照されます。
認可プロファイル	RADIUS ベースのネットワーク アクセス サービス用の基本的な権限コンテナであり、ネットワーク アクセス要求に許可するすべての権限を定義します。 VLAN、ACL、URL リダイレクト、セッション タイムアウト、再認可タイマー、または応答で返されるその他のあらゆる RADIUS 属性が、認可プロファイルで定義されます。
シェル プロファイル	TACACS+ ベースのデバイス管理ポリシー用の基本的な権限コンテナであり、シェル アクセス要求に許可する権限を定義します。 IOS 特権レベル、セッション タイムアウトなどがシェル プロファイルで定義されます。
コマンド セット	TACACS+ ベースの許可コマンドのセットがコマンド認可単位で格納されます。
Policy	特定のポリシー決定に到達するために使用される規則セット。たとえば、認証方法や許可する認可。デフォルト規則を持つポリシーの場合、ポリシーは、ユーザ作成規則と一致しない要求に対するデフォルト規則を持つ最初の一致規則テーブルになります。
ID ポリシー	任意の要求の ID 属性を認証および取得する方法を選択するための ACS 5.4 ポリシー。ACS 5.4 では、2 つのタイプの ID ポリシーを使用できます。1 つは単純で静的なポリシーで、もう 1 つはより複雑な状況で使用するルール ベース ポリシーです。
ID グループ マッピング ポリシー	ID ストアから収集された識別情報（グループ メンバーシップ、ユーザ属性など）を、単一の ACS ID グループにマッピングするための任意のポリシー。 このポリシーは、識別情報を標準化し、単なるタグまたは識別分類である単一の ID グループに要求をマッピングする場合に役立ちます。必要に応じて、ID グループを認可ポリシーの条件として使用できます。
認可ポリシー	アクセス要求に認可属性を割り当てるための ACS 5.4 ポリシー。認可ポリシーによって単一の規則が選択されたあと、その規則の結果として参照される認可プロファイルの内容が応答に読み込まれます。
例外ポリシー	認可ポリシーの特別なオプション。例外ポリシーを使用すると、認可ポリシーの例外と免除に対して使用する条件と認可の結果セットを別個に定義できます。例外ポリシーが定義されている場合は、主要な（標準）認可ポリシーの前にチェックされます。
デフォルト規則	ACS 5.4 ポリシーのキャッチオール規則。この規則を編集して、デフォルトの結果または認可アクションを指定できます。この規則は、特定の要求が、ユーザ作成規則で指定されている条件と一致しなかった場合のポリシー決定として使用できます。

単純なポリシー

すべての ACS ポリシーをルール ベース ポリシーとして設定できます。ただし、場合によっては、条件なしですべての要求に適用する単一の結果を選択する単純なポリシーを設定することもできます。

たとえば、さまざまな条件の規則セットを含むルール ベースの認証ポリシーを定義できます。または、内部データベースをすべての認証に使用する場合は、単純なポリシーを定義できます。

表 3-3 は、各ポリシー タイプが単純なポリシーとして設定できるかどうかを判断する場合に役立ちます。

- 単純なポリシーを作成および保存してからルール ベースのポリシーに変更すると、単純なポリシーはルール ベースのポリシーのデフォルト規則になります。
- ルール ベース ポリシーを保存してから単純なポリシーに変更した場合、ACS ではデフォルト規則が単純なポリシーとして自動的に使用されます。

関連項目

- 「ポリシーのタイプ」（P.3-5）

ルールベースのポリシー

ルール ベース ポリシーは、ID ベース ポリシーでの課題を克服するために導入されました。以前のバージョンの ACS では、ユーザ グループのメンバーシップによってメンバーにアクセス権が付与されていましたが、特定の制限も課されていました。

ユーザがアクセスを要求すると、ID ストアを使用してそのユーザのクレデンシャルが認証され、そのユーザは適切なユーザ グループに関連付けられます。認可はユーザ グループと関連付けられているため、ユーザ グループのすべてのメンバーは常に同じアクセス制限と権限を持ちます。

このタイプのポリシー（単純なポリシー）では、権限は特定のユーザ グループとのユーザの関連付けに基づいて付与されます。これは、ユーザの ID だけが主要な条件である場合に役立ちます。ただし、さまざまな条件下で異なる権限が必要なユーザの場合、このポリシーは機能しません。

ACS 5.x では、ID に関係なくさまざまな条件に基づく規則を作成できます。ユーザ グループにすべての情報が含まれるわけではありません。

たとえば、従業員がキャンパスで勤務しているときにはフル アクセスを許可し、リモートで勤務しているときにはアクセスを制限する場合は、ACS 5.4 でルール ベース ポリシーを使用してこれを実現できます。

ID 以外のさまざまな条件に基づいて権限を設定することができ、権限はユーザ グループに関連付けられなくなりました。セッション属性および環境属性（アクセス場所、アクセス タイプ、端末の健全性、日付、時刻など）を使用して、許可するアクセスのタイプを決定できます。

認可は、次のように規則セットに基づいています。

If *conditions* then *apply the respective permissions*

ルール ベース ポリシーでは、条件は使用可能なセッション属性の任意の組み合わせで構成可能であり、権限は認可プロファイルで定義されます。VLAN、ダウンロード可能 ACL、QoS 設定、および RADIUS 属性を含めるように認可プロファイルを定義します。

ポリシーのタイプ

表 3-3 に、ACS で設定可能なポリシーのタイプを示します。

ポリシーは評価順に示されています。あるポリシーで取得された属性は、そのポリシー以降のすべてのポリシーで使用できます。唯一の例外は、ID ストアからの属性だけを使用する ID グループ マッピング ポリシーです。

表 3-3　ACS ポリシー タイプ

ポリシー	例外ポリシーを含めることができるかどうか	単純[1] およびルール ベースのポリシー	条件に使用できるディクショナリ	使用可能な結果タイプ	取得される属性
サービス セレクション 着信要求に適用するアクセス サービスを決定します。	No	Yes	ID ストア関連以外すべて	Access Service	—
ID 認証用の ID ソースを決定します。	No	Yes	ID ストア関連以外すべて	ID ソース、エラー オプション	ID 属性、内部 ID ストアの ID グループ
ID グループ マッピング 外部 ID ストアから ACS ID グループへの属性およびグループのマッピングを定義します。	No	Yes	ID ストア ディクショナリだけ	Identity Group	外部 ID ストアの ID グループ
ネットワーク アクセス認可 ネットワーク アクセス用の認可および権限を決定します。	Yes	ルール ベースだけ	すべてのディクショナリ	認可プロファイル、Security Group Access	—
デバイス管理の認可 デバイス管理用の認可および権限を決定します。	Yes	ルール ベースだけ	すべてのディクショナリ	シェル プロファイル、コマンド セット	—

1. 単純なポリシーでは、ACS がすべての要求に適用する単一の結果セットを指定します。つまり、実際には単一規則ポリシーです。

アクセス ポリシー

アクセス サービスは、ACS 5.x での不可欠な構成要素です。アクセス サービスを使用すると、ネットワークに接続するユーザとデバイス、およびネットワーク デバイスを管理する管理者用のアクセス ポリシーを設定できます。

ACS 5.x では、認証要求および認可要求はアクセス サービスによって処理されます。アクセス サービスは、次の要素で構成されています。

- ID ポリシー：ユーザの認証方法を指定します。パスワードの確認に使用される、許可された認証プロトコルおよびユーザ リポジトリが含まれています。
- グループ マッピング ポリシー：ユーザの ACS ID グループが、外部 ID ストアのユーザ属性またはグループ メンバーシップに基づいてダイナミックに設定されるかどうかを指定します。ユーザの ID グループをユーザの認可の一部として使用できます。
- 認可ポリシー：ユーザの認可規則を指定します。

アクセス サービスは、アクセス要求の処理に使用される、独立したポリシー セットです。

ACS 管理者は、さまざまな種類のアクセス要求の処理を明確に区別および分離するために、複数のアクセス サービスを作成できます。ACS では、次の 2 つのデフォルト アクセス サービスが提供されています。

- Default Device Admin：デバイス CLI への TACACS+ ベースのアクセスに使用
- Default Network Access：ネットワーク接続への RADIUS ベースのアクセスに使用

これらのアクセス サービスをそのまま使用したり、必要に応じて変更または削除したりできます。追加のアクセス サービスを作成することもできます。

TACACS+ プロトコルによって、認証が認可から分離されます。つまり、ACS では、TACACS+ 認証要求と認可要求が個別に処理されます。表 3-4 に、RADIUS アクセス サービスと TACACS+ アクセス サービスのその他の相違点を示します。

表 3-4　RADIUS アクセス サービスと TACACS+ アクセス サービス

ポリシー タイプ	TACACS+	RADIUS
Identity	オプション[1]	必須
Group Mapping	オプション	オプション
Authorization	オプション[1]	必須

1. TACACS+ の場合、ID または認可を選択する必要があります。

TACACS+ の場合、すべてのポリシー タイプが任意ですが、1 つのサービスで少なくとも 1 つのポリシー タイプを選択する必要があります。TACACS+ の ID ポリシーを定義していない場合は、ACS によって認証要求に対して認証エラーが返されます。

同様に、認可ポリシーを定義していない場合に、ACS がセッションまたはコマンドの認可要求を受信すると、その要求は失敗します。RADIUS アクセス サービスと TACACS+ アクセス サービスの両方で、サービスの作成後、ポリシーを追加するためにサービスを変更できます。

（注） アクセス サービスにはサービス セレクション ポリシーは含まれていません。サービス セレクション規則は独立して定義されています。

複数のアクセス サービス（さまざまな使用例、ネットワーク、地域、管理ドメイン用のサービスなど）を保持および管理できます。サービス セレクション ポリシーを設定します。サービス セレクション ポリシーとは、各新規アクセス要求を適切なアクセス サービスに送信するサービス セレクション規則セットのことです。

表 3-5 に、アクセス サービス セットの例を示します。

表 3-5　アクセス サービス リスト

アクセス サービス A（デバイス管理用）	アクセス サービス B（802.1X エージェントレス ホストへのアクセス用）	アクセス サービス C（802.1X 有線および無線デバイスからのアクセス用）
ID ポリシー A	ID ポリシー B	ID ポリシー C
シェル/コマンド認可ポリシー A	セッション認可ポリシー B	セッション認可ポリシー C

表 3-6 に、サービス セレクション ポリシーを示します。

表 3-6　サービス セレクション ポリシー

ルール名	条件	結果
DevAdmin	protocol = TACACS+	アクセス サービス A
Agentless	Host Lookup = True	アクセス サービス C
Default	—	アクセス サービス B

ACS 5.4 は、TACACS+ アクセス要求を受信すると、ID ポリシー A に従って要求を認証するアクセス サービス A を適用します。その後、シェル/コマンド認可ポリシーに従って認可および権限を適用します。このサービスによって、すべての TACACS+ 要求が処理されます。

ACS 5.4 は、ホスト ルックアップであると判断した RADIUS 要求（たとえば、RADIUS の service-type 属性が *call-check* と同一）を受信すると、ID ポリシー C に従って認証するアクセス サービス C を適用します。その後、セッション認可ポリシー C に従ってセッション認可プロファイルを適用します。このサービスによって、すべてのホスト ルックアップ要求（MAC 認証バイパス要求とも呼ばれる）が処理されます。

アクセス サービス B によって、その他の RADIUS 要求が処理されます。このアクセス サービスでは、ID ポリシー B に従って認証が行われ、セッション認可ポリシー B が適用されます。このサービスによって、上記の規則で処理されるホスト ルックアップを除き、すべての RADIUS 要求が処理されます。

アクセス サービス テンプレート

ACS では、新しいサービスを作成するときにテンプレートとして使用できる定義済みのアクセス サービスが提供されています。アクセス サービス テンプレートを選択すると、ACS によって、ポリシー セットが含まれたアクセス サービスが作成され、それぞれのサービスにカスタマイズされた条件セットが設定されます。

サービスにポリシーを追加したり、サービスからポリシーを削除したりすることにより、アクセス サービスの構造を変更できます。また、ポリシー条件セットを変更することにより、ポリシーの構造を変更することもできます。アクセス サービス テンプレートおよび説明のリストについては、「アクセス サービス テンプレートの設定」（P.10-20）を参照してください。

RADIUS および TACACS+ プロキシ サービス

ACS 5.4 は、RADIUS、RADIUS プロキシまたは TACACS+ プロキシ サーバとして機能できます。

- RADIUS プロキシ サーバとしての場合、ACS は NAS から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS サーバに転送します。
- TACACS+ プロキシ サーバとしての場合、ACS は NAS から認証、許可、およびアカウンティング要求を受信し、これらの要求を外部 TACACS+ サーバに転送します。

ACS は要求の結果を受け入れて NAS に返します。ACS で RADIUS および TACACS+ サーバに要求が転送されるように、外部 RADIUS および TACACS+ サーバを ACS で設定する必要があります。タイムアウト時間および接続試行回数を定義できます。

ACS プロキシのリモート ターゲットは、次のパラメータを含むリモート RADIUS および TACACS+ サーバのリストです。

- IP
- 認証ポート
- アカウンティング ポート
- 共有秘密キー
- 応答タイムアウト
- リトライ回数
- 接続ポート
- ネットワーク タイムアウト

プロキシ サービスでは次の情報を使用できます。

- リモート RADIUS または TACACS+ サーバ リスト
- アカウンティング プロキシ ローカル / リモート / 両方
- ユーザ名からのプレフィックス / サフィックスのストリッピング

RADIUS プロキシ サーバは、要求を受信すると、リスト内の最初のリモート RADIUS または TACACS+ サーバにその要求を転送します。プロキシ サーバは、指定されたタイムアウト間隔および試行回数内に応答を受信しない場合、その要求をリスト内の次の RADIUS または TACACS+ サーバに転送します。

最初の応答をリスト内のいずれかのリモート RADIUS または TACACS+ サーバから受信すると、プロキシ サービスによってその応答が処理されます。応答が有効な場合は、ACS によってその応答が NAS に戻されます。

表 3-7 に、ACS 4.2 リリースと 5.4 リリース間での RADIUS プロキシ サービスの相違点を示します。

表 3-7　ACS 4.2 と 5.4 間での RADIUS および TACACS+ プロキシ サービスの相違点

機能	ACS 5.4	ACS 4.2
設定可能なタイムアウト（RADIUS）	Yes	No
設定可能な再試行カウント（RADIUS）	Yes	No
ネットワーク タイムアウト（TACACS+）	Yes	No
認証ポートおよびアカウンティング ポート（RADIUS）	Yes	Yes
接続ポート（TACACS+）	Yes	No
プロキシ サイクルの検出	Yes（RADIUS の場合のみ）	No
ユーザ名のストリッピング	Yes	Yes

表 3-7　ACS 4.2 と 5.4 間での RADIUS および TACACS+ プロキシ サービスの相違点 （続き）

機能	ACS 5.4	ACS 4.2
アカウンティング プロキシ（ローカル、リモート、または両方）	Yes	Yes
アカウント遅延タイムアウトのサポート（RADIUS）	No	No

ACS は、複数の外部 RADIUS および TACACS+ サーバへのプロキシ サーバとして同時に機能できます。ACS がプロキシ サーバとして機能するには、ACS で RADIUS または TACACS+ プロキシ サービスを設定する必要があります。RADIUS プロキシ サービスの設定方法については、「アクセス サービスの一般プロパティの設定」（P.10-13）を参照してください。

RADIUS および TACACS+ 要求のプロキシ処理の詳細については、「RADIUS および TACACS+ プロキシ要求」（P.4-30）を参照してください。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ポリシーのタイプ」（P.3-5）
- 「サービスおよびポリシーの設定フロー」（P.3-19）

ID ポリシー

次の 2 つの主要メカニズムによって、要求の認証に使用されるメカニズムとソースが定義されます。

- パスワードベース：ユーザがユーザ名とパスワードを入力したあと、データベースに照らして認証が実行されます。MAC アドレスを指定することにより、ホストでこの認証をバイパスできます。ただし、ID ポリシー認証の場合は、ホスト ルックアップもパスワードベースであると見なされます。
- 証明書ベース：クライアントがセッション認証用の証明書を提示します。ACS 5.4 では、証明書ベースの認証は、PEAP-TLS または EAP-TLS プロトコルを選択した場合に発生します。

また、要求内のプリンシパルの属性を取得するためにデータベースを使用できます。

ID ソースは、ID ポリシーの 1 つの結果であり、次のいずれかのタイプになります。

- アクセス拒否：ユーザへのアクセスは拒否され、認証は実行されません。
- ID データベース：単一の ID データベース。ID ポリシーの結果として単一の ID データベースが選択された場合、外部データベース（LDAP や AD）または内部データベース（ユーザやホスト）のいずれかが結果として選択されます。

  選択されたデータベースを使用してユーザ/ホストの認証が行われ、そのユーザ/ホストに関してデータベースに格納されている定義済み属性が取得されます。
- 証明書認証プロファイル：証明書の構造および内容が含まれており、具体的には証明書属性を内部ユーザ名にマッピングします。証明書ベースの認証の場合は、証明書認証プロファイルを選択する必要があります。

  証明書ベースの要求の場合、証明書を使用して自身を特定するエンティティは、証明書に格納されている公開キーに関連付けられている秘密キーを保持します。証明書認証プロファイルでは、次のことを定義することにより、基本的な PKI 処理が拡張されています。

  - ユーザ名の定義に使用される証明書属性。証明書属性のサブセットを選択して、要求のコンテキストに*ユーザ名*フィールドを読み込むことができます。このユーザ名は、要求の残りのユーザを識別する場合に使用されます。ログで使用される識別情報にも使用されます。
  - 証明書の失効ステータスの確認に使用される LDAP または AD データベース。LDAP または AD データベースを選択すると、証明書データが LDAP または AD データベースから取得され、クライアントが入力したデータに照らして比較されて、クライアント証明書の追加確認が行われます。

- ID 順序：ID データベースの順序。この順序は認証に使用されます。追加の順序が指定されている場合は、その追加順序を使用して属性だけが取得されます。ID ポリシーの結果として複数の ID 方式を選択できます。ID 方式を ID 順序オブジェクトで定義します。ID 順序には任意のタイプの方式を含めることができます。

  ID 順序には 2 つのコンポーネントがあります。1 つは認証用であり、もう一つは属性取得用です。管理者は、証明書および ID データベースのいずれか、またはその両方に基づいて認証を実行できます。

  - 証明書に基づいて認証を実行する場合は、ACS によって単一の証明書認証プロファイルが選択されます。
  - ID データベースに基づいて認証を実行する場合は、認証が成功するまで順番にアクセスされるデータベースのリストを定義する必要があります。認証が成功すると、データベース内の定義済み属性が取得されます。

  また、任意のデータベース リストを定義して、そこから追加属性を取得することもできます。これらの追加データベースには、使用された認証がパスワードベースであるか証明書ベースであるかに関係なく、アクセスできます。

  証明書ベースの認証が使用された場合、ユーザ名フィールドは、証明書属性から読み込まれ、属性の取得に使用されます。リストで定義されているすべてのデータベースにアクセス可能であり、ユーザに一致するレコードが見つかった場合は、対応する属性が取得されます。

  ユーザのパスワードに要変更のマークが付いている場合でも、またはユーザ アカウントがディセーブルになっている場合でも、そのユーザの属性を取得できます。ユーザのアカウントをディセーブルにした場合でも、そのユーザの属性は属性ソースとして引き続き使用できます。ただし、認証には使用できません。

エラー オプション

ID ポリシーの処理中にエラーが発生した場合、そのエラーは次の 3 つの主要タイプのいずれかになります。

- Authentication failed：ACS は、認証が失敗したことを示す明示的な応答を受信します。たとえば、正しくないユーザ名やパスワードが入力された場合、またはユーザがディセーブルにされた場合があります。
- User/host not found：指定されたユーザ / ホストが認証データベースで見つかりませんでした。
- Process failed：定義されたデータベースへのアクセス中にエラーが発生しました。

ID データベースから返されたすべてのエラーは、上記のいずれかのタイプになります。各エラー タイプに対して、次のオプションを設定できます。

- Reject：ACS によって拒否応答が送信されます。
- Drop：応答は返されません。
- Continue：ACS によって、サービスで定義されている次のポリシーに対して処理が続行されます。

認証ステータス システム 属性で、ID ポリシー処理の結果が保持されます。エラーの発生時にポリシー処理の続行を選択した場合は、後続のポリシー処理でこの属性を条件として参照して、ID ポリシー処理が成功しなかった場合を区別できます。

使用される基本プロトコルでの制限が原因で、[Continue] オプションを選択しても処理を続行できない場合があります。このことは PEAP、LEAP、および EAP-FAST の場合に該当し、[Continue] オプションを選択しても要求は拒否されます。

規則を作成する場合、次のデフォルト値をエラー オプションに使用できます。

- Authentication failed：デフォルトは *reject* です。
- User/host not found：デフォルトは *reject* です。
- Process failure：デフォルトは *drop* です。

グループ マッピング ポリシー

ID グループ マッピング ポリシーは、標準ポリシーです。条件は、外部属性ストアだけ、または証明書から取得される属性またはグループに基づきます。結果は ID グループ階層内の ID グループになります。

ID ポリシーが内部ユーザまたはホスト ID ストアにアクセスすると、対応するユーザまたはホスト レコードから ID グループが直接設定されます。この処理は、グループ マッピング ポリシーの暗黙的な処理部分です。

したがって、このデフォルト規則は、グループ マッピング ポリシーの処理の一部として、次の条件が両方とも満たされる場合にだけ適用されます。

- グループ マッピング テーブル内のいずれの規則も一致しない。
- ID グループが内部ユーザまたはホスト レコードから設定されていない。

グループ マッピング ポリシーの結果は、システム ディクショナリ内の **IdentityGroup** 属性に格納され、ID グループ条件を選択することにより、ポリシーにこの属性を含めることができます。

デバイス管理用の認可ポリシー

シェル プロファイルによってデバイス CLI へのアクセスが決まります。コマンド セットによってコマンド認可ごとの TACACS+ が決まります。デバイス管理アクセス サービス用の認可ポリシーでは、単一のシェル プロファイルおよび複数のコマンド セットを含めることができます。

複数のコマンド セットを持つ規則の処理

認可ポリシーに複数のコマンド セットを持つ規則が含まれている場合は、ACS によってアクセス要求内のコマンドが処理される方法を理解することが重要です。規則の結果に複数のコマンド セットが含まれており、その規則の条件がアクセス要求に一致した場合、ACS では、その規則内の各コマンド セットに照らしてアクセス要求内のコマンドが処理されます。

1. コマンド セットにコマンドとその引数との一致が含まれる場合、その一致が *Deny Always* であると、ACS によってそのコマンド セットは *Commandset-DenyAlways* として指定されます。
2. コマンド セット内のコマンドの一致に *Deny Always* がない場合は、最初の一致が見つかるまで、コマンド セット内のすべてのコマンドが順番にチェックされます。
   - 最初の一致が *Permit* である場合、そのコマンド セットは *Commandset-Permit* として指定されます。
   - 最初の一致が *Deny* である場合、そのコマンド セットは *Commandset-Deny* として指定されます。
3. ACS は、すべてのコマンド セットを分析したあと、コマンドを次のように認可します。

a. コマンド セットが *Commandset-DenyAlways* として指定された場合、ACS によってそのコマンドは拒否されます。

b. *Commandset-DenyAlways* がない場合、コマンド セットが *Commandset-Permit* である場合はそのコマンドが許可されます。そうでない場合、そのコマンドは拒否されます。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ネットワーク アクセスの認可プロファイル」（P.3-17）

認可ポリシーの例外規則

現実世界での一般的な問題は、日々の運用で、ポリシーの免除または例外を許可する必要が頻繁に発生することです。特定のユーザが、特殊なアクセスを短期間必要とする場合があります。または、あるユーザが休暇中の他のユーザの代理を務めるために追加のユーザ権限を必要とする場合があります。

ACS では、認可ポリシーの例外ポリシーを定義できます。例外ポリシーには、ポリシーの例外および免除用の個別のポリシー セットが含まれています。これらは、通常、臨時および一時的なものです。例外規則は、主要規則テーブルの規則よりも優先されます。

例外規則では、主要ポリシーとは異なる条件および結果セットを使用できます。たとえば、主要ポリシーでは条件として ID グループと場所を使用し、関連する例外ポリシーでは異なる条件を使用することがあります。

デフォルトでは、例外ポリシーは複合条件および時刻と日付の条件を使用します。時刻と日付の条件は、例外規則に明確な開始時刻と終了時刻を設定する必要がある場合は特に重要となります。

例外ポリシーは、主要ポリシーよりも優先されます。例外ポリシーには、例外ポリシー独自のデフォルト規則は必要ありません。例外ポリシーで一致が見つからなかった場合は、独自のデフォルト規則を持つ主要ポリシーが適用されます。

例外を使用すると、標準ポリシーの一時的変更に対処できます。たとえば、あるグループの管理者 *John* が休暇中で、別のグループの管理者 *Bob* がその代理を務める場合、*John* と同じアクセス権を休暇の間 *Bob* に付与する例外規則を作成できます。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ポリシーの条件」（P.3-16）
- 「ポリシーの結果」（P.3-16）
- 「ポリシーおよび ID 属性」（P.3-17）

サービス セレクション ポリシー

ACS では、さまざまなアクセス要求を受信すると、サービス セレクション ポリシーを使用してこれらの要求が処理されます。次の 2 つのモードのサービス セレクションが提供されています。

- 「単純なサービス セレクション」（P.3-13）
- 「ルール ベースのサービス セレクション」（P.3-13）

単純なサービス セレクション

単純なサービス セレクション モードでは、ACS によってすべての AAA 要求が 1 つのアクセス サービスを使用して処理されます。実際にはサービスは選択されません。

ルール ベースのサービス セレクション

ルール ベースのサービス セレクション モードでは、さまざまな設定可能オプションに基づいて、使用するアクセス サービスが決定されます。オプションの一部を次に示します。

- AAA Protocol：要求に使用されるプロトコル。TACACS+ または RADIUS です。
- Request Attributes：要求内の RADIUS 属性または TACACS+ 属性。
- Date and Time：ACS が要求を受信した日付および時刻。
- Network Device Group：AAA クライアントが属しているネットワーク デバイス グループ。
- ACS Server：要求を受信する ACS サーバ。
- AAA Client：要求を送信した AAA クライアント。
- Network condition objects：ネットワーク条件の基になるもの。
  - End Station：接続を開始および終了する端末。
  - Device：要求を処理する AAA クライアント。
  - Device Port：この条件では、デバイス以外に、端末が関連付けられているポートもチェックされます。

ポリシー条件の詳細については、「ポリシー条件の管理」（P.9-1）を参照してください。

ACS は、2 つのデフォルト アクセス サービス（Default Device Admin および Default Network Access）を使用して事前設定されています。ルール ベースのサービス セレクション モードは、AAA プロトコルを選択基準として使用するように設定されています。このため、TACACS+ 要求を受信した場合は Default Device Admin サービスが使用され、RADIUS 要求を受信した場合は Default Network Access サービスが使用されます。

アクセス サービスおよびサービス セレクションのシナリオ

ACS を使用すると、組織では、複数のシナリオ（有線、無線、リモート VPN、デバイス管理など）で ID 要件およびアクセス コントロール要件を管理できます。アクセス サービスは、これらのさまざまなシナリオをサポートする場合に主要な役割を果たします。

アクセス サービスを使用すると、独立した個別のネットワーク アクセス ポリシーを作成して、さまざまなネットワーク アクセス シナリオにおける固有のポリシー要件に対処できます。さまざまなシナリオに対して個別のポリシーを使用すると、組織のネットワークをより適切に管理できます。

たとえば、デバイス管理とネットワーク アクセスに使用するデフォルトのアクセス サービスには、ネットワーク デバイスにアクセスするネットワーク管理者と、企業のネットワークにアクセスする組織のスタッフとの典型的な区別がポリシーに反映されています。

ただし、複数のアクセス サービスを作成すると、さまざまな管理ドメインを区別できます。たとえば、アジア太平洋地域での無線アクセスを、ヨーロッパのユーザによる無線アクセスを管理しているチームとは異なるチームが管理できます。この場合、次のアクセス サービスが必要となります。

- APAC ワイヤレス：アジア太平洋地域のワイヤレス ユーザ用のアクセス サービス。
- ヨーロッパ ワイヤレス：ヨーロッパ諸国のワイヤレス ユーザ用のアクセス サービス。

追加のアクセス サービスを作成することにより、単一のアクセス サービス内に複数のポリシーが存在する複雑な状況を軽減できます。このためには、複数のアクセス サービス間で複合ポリシーを作成します。たとえば、大規模な組織で 802.1x ネットワーク アクセスを展開する場合、次のアクセス サービスが可能となります。

- 802.1x：常勤スタッフのマシン、ユーザ パスワード、および証明書ベースの認証用。
- エージェントレス デバイス：電話やプリンタなど、EAP サプリカントを持たないデバイス用。
- ゲスト アクセス：ゲスト無線ネットワークにアクセスするユーザ用。

この例では、802.1x、エージェントレス デバイス、およびゲスト アクセス用のネットワーク アクセス ポリシーを 1 つのアクセス サービスで作成する代わりに、このポリシーを 3 つのアクセス サービスに分割します。

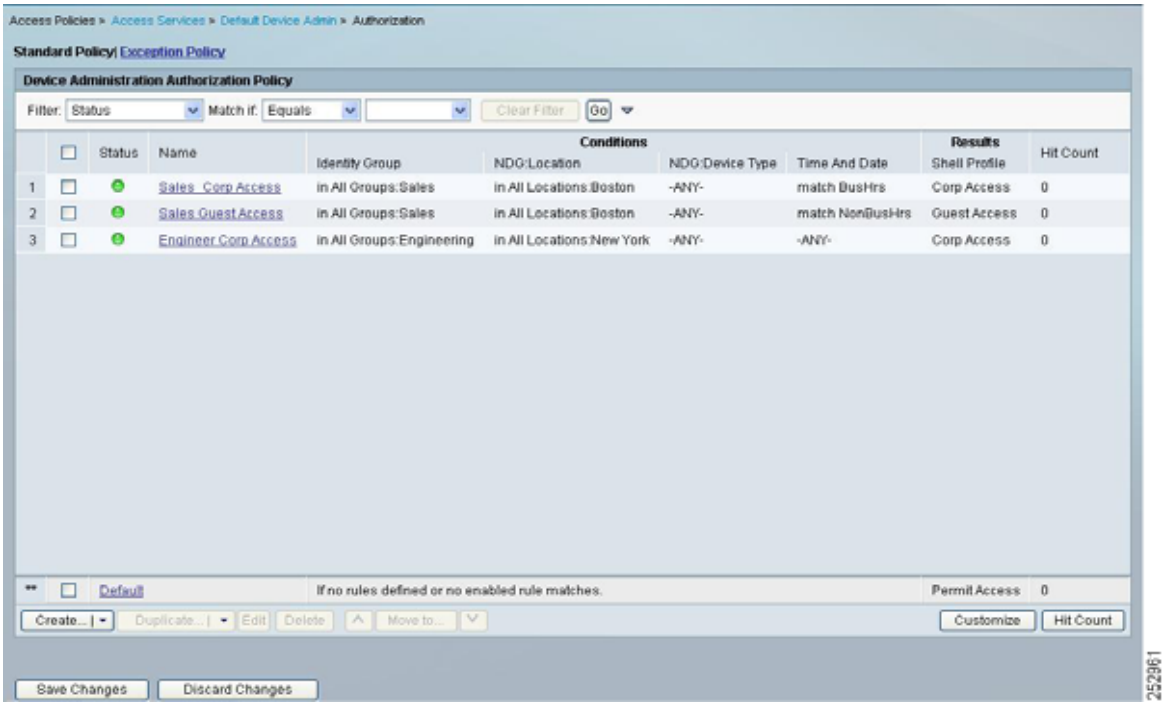
最初の一致規則テーブル

ACS 5.4 では、規則セットを評価するための最初の一致規則テーブルを使用してポリシーを決定できます。規則テーブルには条件および結果が含まれています。条件は、単純または複合のいずれかとなります。単純な条件は、属性演算子値で構成され、True または False のいずれかとなります。複合条件には、AND または OR 演算子で結合された、より複雑な条件が含まれています。詳細については、「ポリシーの条件」（P.3-16）を参照してください。

管理者は、ポリシーに含める単純な条件を選択します。これらの条件は規則テーブルでカラムとして表示されます。規則テーブルでは、カラム見出しは条件の名前になり、通常は属性の名前です。

規則はカラム見出しの下に表示され、各セルには、条件を形成するために属性と結合される演算子および値が表示されます。*ANY* の場合、図 3-1 に定義済みの条件タイプが含まれているカラムベースの規則テーブルを示します。

図 3-1　　ポリシー規則テーブルの例



カラム	説明
Status	規則のステータスを、次のようにイネーブル、ディセーブル、または監視対象として定義できます。 • Enabled：ACS は、イネーブルにされた規則を評価し、規則の条件がアクセス要求に一致すると、規則の結果を適用します。 • Disabled：規則が規則テーブルに表示されますが、ACS はその規則をスキップし、評価しません。 • Monitor Only：ACS は監視対象の規則を評価します。規則の条件がアクセス要求と一致すると、ACS は、その一致に関する情報を含むログ レコードを作成します。 結果は適用しないで、以降の規則に対して処理を続行します。規則の使用開始時にこのステータスを使用して、その規則が必要であるかどうかを確認します。
Name	説明的な名前。規則の目的を示す任意の名前を指定できます。デフォルトでは、ACS によって規則名ストリング *rule-number* が生成されます。
Conditions	
Identity Group	この例では、内部 ID グループの 1 つと照合されます。
NDG: Location	Location ネットワーク デバイス グループ。2 つの事前定義済みの NDG は、Location および Device Type です。
Results	
Shell Profile	デバイス管理タイプのポリシーに使用され、TACACS+ シェル アクセス要求用の権限（Cisco IOS 特権レベルなど）が含まれています。
Hit Counts	ポリシーのヒット カウンタの最後のリセット以降、規則が着信要求と一致した回数が表示されます。ACS では、監視対象の規則またはイネーブルになっている規則に関して、すべての条件が着信要求と一致した場合に、ヒットをカウントします。次にヒット カウントの説明を示します。 • イネーブルになっている規則のヒット カウントは、ACS が要求を処理するときに発生した一致を示します。 • 監視対象の規則のヒット カウントは、ACS が要求を処理するときに規則がイネーブルになっていた場合に、それらの規則の結果となるカウントを示します。 ACS 展開内のプライマリ サーバによってヒット カウントが表示されます。このカウントは、ACS 展開でのすべてのサーバにおける各規則の一致合計を示しています。セカンダリ サーバでは、ポリシー テーブルのすべてのヒット カウントはゼロと表示されます。

デフォルト規則では、他の規則が存在しないか、またはアクセス要求内の属性値が規則と一致しない場合に ACS で使用されるポリシー結果が指定されています。

ACS は、現在のアクセス要求に関連付けられている属性値を、規則で表されている条件セットと比較することによって、最初の一致規則テーブル内の規則セットを評価します。

- 属性値が条件に一致しない場合、ACS は規則テーブル内の次の規則に進みます。
- 属性値が条件と一致すると、その規則で指定されている結果が ACS によって適用され、残りの規則はすべて無視されます。
- 属性値がいずれの条件とも一致しない場合は、ポリシーのデフォルト規則で指定されている結果が適用されます。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ポリシーの条件」（P.3-16）
- 「ポリシーの結果」（P.3-16）
- 「認可ポリシーの例外規則」（P.3-12）

ポリシーの条件

次の条件内の属性に基づいて、単純な条件を規則テーブルに定義できます。

- Customizable conditions : ACS が認識するプロトコル ディクショナリおよび ID ディクショナリに基づいたカスタム条件を作成できます。ポリシー規則ページでカスタム条件を定義します。個別の条件オブジェクトとして定義することはできません。
- Standard conditions : デバイス IP アドレス、プロトコル、ユーザ名関連のフィールドなど、常に使用可能な属性に基づいた標準条件を使用できます。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ポリシーの結果」（P.3-16）
- 「認可ポリシーの例外規則」（P.3-12）
- 「ポリシーおよび ID 属性」（P.3-17）

ポリシーの結果

ポリシー規則には、ポリシーのタイプに応じた結果情報が含まれています。独立した共有オブジェクトとしてポリシーの結果を定義します。ポリシーの結果はユーザまたはユーザ グループの定義には関連付けられません。

たとえば、認可ポリシー用の認可結果と権限結果を定義するポリシー要素を次に示します。

- ID ポリシーの結果としての ID ソースおよびエラー オプション。「ネットワーク アクセスの認可プロファイル」（P.3-17）を参照してください。
- グループ マッピングの ID グループ。「グループ マッピング ポリシー」（P.3-11）を参照してください。
- 「ネットワーク アクセスの認可プロファイル」（P.3-17）。
- 「デバイス管理用の認可ポリシー」（P.3-11）。
- Cisco Security Group Access のセキュリティ グループおよびセキュリティ グループ アクセス コントロール リスト（ACL）。「ACS と Cisco Security Group Access」（P.4-24）を参照してください。

その他のポリシー結果については、「認可および権限の管理」（P.9-19）を参照してください。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ポリシーの条件」（P.3-16）
- 「認可ポリシーの例外規則」（P.3-12）
- 「ポリシーおよび ID 属性」（P.3-17）

ネットワーク アクセスの認可プロファイル

認可プロファイルでは、認可の成功後に ACS によってユーザに返される RADIUS 属性セットを定義します。アクセス認可情報には、認可特権と権限、およびダウンロード可能 ACL などのその他の情報が含まれています。

複数の認可プロファイルをネットワーク アクセス ポリシー結果として定義できます。この方法では、規則の結果として認可プロファイルを組み合わせて使用できるため、個々のプロファイルで組み合わせ自体をすべて保持するよりも、保持する認可プロファイルの数が少なくなります。

複数の認可プロファイルを含む規則の処理

セッション認可ポリシーには、複数の認可プロファイルを持つ規則を含めることができます。認可プロファイルには、一般情報（名前と説明）および RADIUS 属性だけが含まれています。複数の認可プロファイルを使用した場合は、ACS によってそれらのプロファイルが単一の属性セットにマージされます。特定の属性の出現状況によって、次のように処理されます。

- 結果として生成される認可プロファイルの 1 つだけに出現する場合、属性はその認可結果に含められます。
- 結果プロファイルに複数回出現する場合は、結果セットで最初に出現したプロファイル内の属性値に基づいて、認可結果の属性値が決定されます。

  たとえば、VLAN が最初のプロファイルに出現する場合、リスト内の 2 番めまたは 3 番めのプロファイルに出現する VLAN よりも優先されます。

（注） 複数の認可プロファイルを使用する場合は、優先順位の高い順に並べる必要があります。

プロトコル ディクショナリ内の RADIUS 属性定義では、属性が応答で 1 回だけ出現するか、または複数回出現するかを指定します。いずれの場合も、応答で属性値が何回出現するかにかかわらず、ACS によって、1 つのプロファイルだけから任意の属性の値が取得されます。唯一の例外は、Cisco Attribute Value（AV）ペアです。このペアは、結果に含まれるすべてのプロファイルから取得されます。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「デバイス管理用の認可ポリシー」（P.3-11）

ポリシーおよび ID 属性

ID ストアには、ポリシー条件の一部として、認可結果で使用できる ID 属性が含まれています。ポリシーを作成するときに、ID 属性およびユーザ属性を参照できます。

これにより、認可規則内の権限にグループを直接マッピングする際の柔軟性が高まります。ACS がユーザまたはホストの要求を処理するときに、ID 属性が取得され、認可ポリシー条件で使用できるようになります。

たとえば、ACS 内部ユーザの ID ストアを使用する場合、その内部ユーザの ID グループを参照したり、その内部ユーザの属性を参照したりできます （ACS では、内部 ID ストア レコード用に追加のカスタム属性を作成できることに注意してください）。

外部 Active Directory（AD）を使用している場合は、AD グループを認可規則で直接参照できます。また、AD ユーザ属性を認可規則で直接参照できます。ユーザ属性には、ユーザの部門またはマネージャの属性が含まれている場合があります。

関連トピック

- 「ユーザおよび ID ストアの管理」（P.8-1）
- 「ポリシーの用語」（P.3-3）
- 「ポリシーのタイプ」（P.3-5）

ポリシーおよびネットワーク デバイス グループ

ネットワーク デバイス グループ（NDG）をポリシー条件として参照できます。ACS では、デバイスの要求を受信すると、そのデバイスと関連付けられている NDG が取得され、ポリシー テーブルの NDG に照らして比較されます。この方法を使用すると、複数のデバイスをグループ化し、同じポリシーを割り当てることができます。たとえば、特定の場所にあるすべてのデバイスをグループ化して、同じポリシーを割り当てることができます。

ネットワーク デバイスからネットワークへのアクセス要求を受信すると、ACS はネットワーク デバイス リポジトリを検索して、IP アドレスが一致するエントリを見つけます。その IP アドレスを使用して ACS が識別したデバイスから要求を受信した場合、ACS はそのデバイスに関連付けられているすべての NDG を取得します。

関連トピック

- 「ユーザおよび ID ストアの管理」（P.8-1）
- 「ポリシーの用語」（P.3-3）
- 「ポリシーのタイプ」（P.3-5）

ルール ベース ポリシーの例

次の例に、ポリシー要素を使用してポリシー規則を作成する方法を示します。

ある企業では、ネットワークを 2 つの地域（East および West）に分割しており、各地域にネットワーク操作エンジニアが常駐しています。エンジニアは、次のことを可能にするアクセス ポリシーを作成します。

- 自分の地域のネットワーク デバイスへのフル アクセス。
- 自分の地域以外のデバイスへの読み取り専用アクセス。

ACS 5.4 ポリシー モデルを次の目的のために使用できます。

- East および West のネットワーク デバイス グループを定義し、ネットワーク デバイスを該当するグループに割り当てる。
- East および West の ID グループを定義し、ユーザ（ネットワーク エンジニア）を該当するグループにマップする。
- フル アクセスまたは読み取り専用の認可プロファイルを定義する。
- ネットワーク デバイス グループの場所に応じて各 ID グループにフル アクセスまたは読み取り専用アクセスを許可する規則を定義する。

これを行う前に、2 つのユーザ グループ（エンジニアが常駐する場所ごとに 1 つのグループ。それぞれのグループに権限に関する個別の定義などが設定されます）を作成しておく必要があります。この定義では、ルール ベース モデルのような柔軟性や細かさは提供されません。

図 3-2 に、ポリシー規則テーブルの例を示します。

図 3-2　ルール ベース ポリシーの例

このポリシー テーブル内の各行は、単一の規則を表します。

最後のデフォルト規則を除き、各規則には 2 つの条件（ID グループと場所）および結果（認可プロファイル）が含まれています。ID グループは ID ベースの分類であり、場所は非 ID 条件です。認可プロファイルには、セッションの権限が含まれています。

ID グループ、場所、および認可プロファイルはポリシー要素です。

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ポリシーのタイプ」（P.3-5）
- 「アクセス ポリシー」（P.3-6）
- 「サービスおよびポリシーの設定フロー」（P.3-19）

サービスおよびポリシーの設定フロー

表 3-8 に、サービスとポリシーを設定する場合の、推奨される基本フローを示します。このフローには、ユーザ定義の条件および属性の設定は含まれていません。このフローでは、NDG、ID グループ、および複合条件を規則で使用できます。

前提条件

サービスおよびポリシーを設定する前に、次のことを実行しておく必要があります。

- ACS へのネットワーク リソースの追加、およびネットワーク デバイス グループの作成。「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）および「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。
- 内部 ACS ID ストアへのユーザの追加、または外部 ID ストアの追加。「内部ユーザの作成」（P.8-11）、「ID 属性の管理」（P.8-7）、または「外部 LDAP ID ストアの作成」（P.8-23）を参照してください。

表 3-8　サービスおよびポリシーの設定手順

ステップ	アクション	Web インターフェイスのドロワ
ステップ 1	ポリシー結果を定義します。 • デバイス管理用の認可および権限：シェル プロファイルまたはコマンド セット。 • ネットワーク アクセス用の認可および権限：認可プロファイル。 次を参照してください。 • 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25） • 「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-31） • 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-19）	ポリシー要素
ステップ 2	（任意）カスタム条件をポリシー規則に定義します。このステップは、ステップ 6 でポリシー規則を定義する前に実行できます。つまり、規則の作成中にカスタム条件を定義できます。「カスタム セッション条件の作成、複製、および編集」（P.9-5）を参照してください。	—
ステップ 3	アクセス サービスを作成します。構造および許可プロトコルだけを定義します。ポリシーについてはまだ定義する必要はありません。「アクセス サービスの作成、複製、および編集」（P.10-12）を参照してください。	アクセス ポリシー
ステップ 4	要求に使用するアクセス サービスを決定するために、規則をサービス セレクション ポリシーに追加します。次を参照してください。 • 「ポリシーのカスタマイズ」（P.10-4） • 「サービス セレクション規則の作成、複製、および編集」（P.10-8）	アクセス ポリシー
ステップ 5	ID ポリシーを定義します。要求の認証に使用する ID ストアまたは順序を選択し、ID 属性を取得します。「ユーザおよび ID ストアの管理」を参照してください。	ユーザおよび ID ストア
ステップ 6	認可規則を次のように作成します。 • デバイス管理：シェル/コマンド認可ポリシー。 • ネットワーク アクセス：セッション認可ポリシー。 次を参照してください。 • 「ポリシーのカスタマイズ」（P.10-4） • 「アクセス サービス ポリシーの設定」（P.10-22）	アクセス ポリシー

関連トピック

- 「ポリシーの用語」（P.3-3）
- 「ポリシーの条件」（P.3-16）
- 「ポリシーの結果」（P.3-16）
- 「ポリシーおよび ID 属性」（P.3-17）

CHAPTER 4

ACS を使用した一般的なシナリオ

ネットワーク コントロールとは、ネットワークへのアクセスを制御するプロセスのことです。従来は、ネットワークに対するユーザの認証には、ユーザ名とパスワードが使用されていました。近年の急速な技術の進歩により、ユーザ名とパスワードによる従来のネットワーク アクセス管理方式では不十分となっています。

ユーザによるネットワークへのアクセス方法およびユーザのアクセス対象は、大きく変化しています。したがって、ネットワークへのアクセスを制御するには、複雑でダイナミックなポリシーを定義する必要があります。

たとえば、これまでは、ユーザは自分が所属するグループに基づいてネットワークへのアクセスを許可され、特定のアクションの実行を認可されていました。現在では、ユーザが所属するグループに加えて、次のような他の要素も考慮する必要があります。

- アクセスが勤務時間内か勤務時間外か
- リモート アクセスかどうか
- サービスおよびリソースへのアクセスがフル アクセスか制限付きアクセスか

ユーザ以外に、各種のデバイスもネットワークへの接続を試みます。

ユーザやデバイスがネットワーク アクセス サーバ（無線アクセス ポイント、802.1x スイッチ、VPN サーバなど）を介してネットワークに接続する場合は、ACS によってその要求が認証および認可され、接続が確立されます。

認証とは、ネットワークへの接続を試みるユーザまたはデバイスの ID を確認するプロセスのことです。ACS は、クレデンシャルという形式でユーザまたはデバイスの ID 証明を受け取ります。認証には、次のような 2 つの異なる方式があります。

- パスワードベースの認証：より単純なユーザ認証方式です。ユーザが入力するのは、ユーザ名とパスワードです。サーバが内部または外部のデータベースでユーザ名とパスワードをチェックし、それらが登録されていれる場合、そのユーザはアクセスを許可されます。アクセスのレベル（認可）は作成済みの規則と条件によって定義されます。
- 証明書ベースの認証：ACS は、Extensible Authentication Protocol-Transport Level Security（EAP-TLS）と Protected Extensible Authentication Protocol-Transport Level Security（PEAP-TLS）を使用した証明書ベースの認証をサポートします。これらはサーバによるクライアント認証とクライアントによるサーバ認証に証明書を使用します。

  証明書ベースの認証方式は、パスワードベースの認証方式と比べて強力なセキュリティを備えているため、この方式を推奨します。

認可では、ユーザまたはデバイスに許可するアクセスのレベルを決定します。ACS 5.x のルール ベースのポリシー モデルを使用すると、規則の中に複雑な条件を定義できます。ACS は規則（ポリシー）のセットを使用してアクセス要求を評価し、判断を返します。

個別のポリシーからなる順序をアクセス サービスにまとめ、これを使用してアクセス要求を処理します。複数のアクセス サービスを作成して、異なる種類のアクセス要求を処理できます。たとえば、デバイス管理アクセスやネットワーク アクセスなどです。

Cisco Secure Access Control System（ACS）を使用すると、ネットワークのサービスおよびリソース（IP 電話やプリンタなどのデバイスも含む）へのアクセスを一元的に管理できます。ACS 5.4 はポリシーベースのアクセス コントロール システムであり、複雑なポリシー条件を作成できるだけでなく、政府によるさまざまな規制に準拠することもできます。

ネットワークに ACS を展開する場合は、ネットワークへのアクセスを決定する適切な認証方式を選択する必要があります。

この章では、一般的ないくつかのシナリオについてのガイドラインを示します。この章の内容は、次のとおりです。

- 「デバイス管理の概要」（P.4-2）
- 「パスワードベースのネットワーク アクセス」（P.4-5）
- 「証明書ベースのネットワーク アクセス」（P.4-9）
- 「エージェントレス ネットワーク アクセス」（P.4-12）
- 「VPN リモート ネットワーク アクセス」（P.4-21）
- 「ACS と Cisco Security Group Access」（P.4-24）
- 「RADIUS および TACACS+ プロキシ要求」（P.4-30）

デバイス管理の概要

デバイス管理を使用すると、ネットワーク デバイスに対して実行される管理操作を ACS で制御および監査できます。デバイス管理には次の方法を使用します。

- セッション管理：ネットワーク デバイスへのセッション認可要求により、ACS 応答が発生します。この応答には、ネットワーク デバイスにより解釈されるトークンが含まれています。ネットワーク デバイスにより、セッション期間中に実行できるコマンドが制限されます。「セッション管理」（P.4-3）を参照してください。
- コマンド認可：管理者がネットワーク デバイスに対して操作コマンドを発行すると、その管理者がコマンドの発行を認可されているかどうかを判定する問い合わせが ACS に行われます。「コマンド認可」（P.4-4）を参照してください。

デバイス管理の結果は、シェル プロファイルまたはコマンド セットにすることができます。

シェル プロファイルでは、セッション認可要求への応答で返される属性を選択できます。最も一般的に使用される属性は特権レベルです。シェル プロファイルには、シェル アクセス セッションに使用する共通属性と、その他のタイプのセッションに使用するユーザ定義属性があります。

ACS 5.4 では、カスタム TACACS+ 認可サービスおよび属性を作成できます。次のことを定義できます。

- 上記属性の任意の A-V ペア
- 任意または必須の属性
- 同じ名前を持つ複数の A-V ペア（マルチパート属性）

また、ACS では、タスク固有の事前定義済みシェル属性がサポートされています。TACACS+ シェル プロファイルを使用すると、シェル認可応答で返されるカスタム属性を指定できます。「TACACS+ のカスタム サービスおよび属性」（P.4-5）を参照してください。

コマンド セットでは、許可または拒否されるコマンドのセットおよびコマンド引数を定義します。認可を要求するコマンドを受信すると、認可結果に含まれている使用可能なコマンド セット内のコマンドと比較されます。

コマンドがコマンド セットに一致すると、そのコマンドに対応する許可または拒否の設定が取得されます。一致した規則の中で複数の結果が該当する場合は、その結果が統合され、コマンドに対する単一の許可または拒否の結果が返されます。その条件は次のとおりです。

- コマンド セット内に明示的な deny-always 設定が存在する場合、コマンドは拒否される。
- コマンド セット内に明示的な deny-always 設定が存在せず、すべてのコマンド セットが許可の結果を返す場合、コマンドは許可される。
- 上記 2 つの条件のどちらにも当てはまらない場合、コマンドは拒否される。

許可および拒否の設定は、デバイス管理規則テーブルで設定します。デバイス管理規則テーブル内では、一致する条件または一致しない条件としてポリシー要素を設定します。この規則テーブルにより、マッチング プロセスを通じて特定の要求条件がデバイス管理結果にマップされます。規則テーブルで処理された結果は、要求の種類に応じてシェル プロファイルまたはコマンド セットとなります。

セッション管理要求にはシェル プロファイル結果が含まれています。この中には、セッションのプロビジョニングで使用される属性の値が入っています。コマンド認可要求にはコマンド認可結果が含まれています。この中には、コマンドおよび引数の確認に使用されるコマンド セットのリストが入っています。

このモデルを使用すると、特定のデバイスを管理できるように管理者レベルを設定できます。たとえば、あるユーザに Network Device Administrator のロールを割り当てるとデバイス管理機能にフル アクセスできますが、Read Only Admin の場合は管理機能を実行できません。

セッション管理

次の手順では、管理者がネットワーク デバイスとのセッション（通信する機能）を確立するためのフローについて説明します。

1. 管理者がネットワーク デバイスにアクセスします。
2. ネットワーク デバイスから、RADIUS または TACACS+ のアクセス要求が ACS に送信されます。
3. ACS が ID ストア（外部 LDAP、Active Directory、RSA、RADIUS ID サーバ、または内部 ACS ID ストア）を使用して、管理者のクレデンシャルを確認します。
4. RADIUS 応答または TACACS+ 応答（accept または reject）がネットワーク デバイスに送信されます。accept 応答には管理者の最大特権レベルも含まれており、セッション期間中の管理者のアクセス レベルはこの値によって決定されます。

セッション管理ポリシー（デバイス管理規則テーブル）を設定して通信を許可するには、次の手順を実行します。

ステップ 1　TACACS+ プロトコルのグローバル設定およびユーザ認証オプションを設定します。「TACACS+ の設定」（P.18-1）を参照してください。

ステップ 2　ネットワーク リソースを設定します。「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。

ステップ 3　ユーザおよび ID ストアを設定します。「内部 ID ストアの管理」（P.8-4）または「外部 ID ストアの管理」（P.8-19）を参照してください。

ステップ 4　必要に応じてシェル プロファイルを設定します。「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）を参照してください。

ステップ 5　アクセス サービス ポリシーを設定します。「アクセス サービス ポリシーの作成」（P.10-4）を参照してください。

ステップ 6　サービス セレクション ポリシーを設定します。「サービス セレクション ポリシーの作成」（P.10-4）を参照してください。

ステップ 7　認可ポリシー（規則テーブル）を設定します。「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）を参照してください。

コマンド認可

ここでは、管理者がネットワーク デバイスにコマンドを発行するためのフローについて説明します。

（注）　このデバイス管理コマンド フローが対応しているのは、TACACS+ プロトコルだけです。

1. 管理者がネットワーク デバイスにコマンドを発行します。
2. ネットワーク デバイスから、アクセス要求が ACS に送信されます。
3. ACS が任意で ID ストア（外部 Lightweight Directory Access Protocol [LDAP]、Active Directory、RADIUS ID サーバ、または内部 ACS ID ストア）を使用して、ポリシー処理に含まれるユーザ属性を取得します。
4. 応答には、管理者がコマンドの発行を認可されているかどうかが示されています。

コマンド認可ポリシー（デバイス管理規則テーブル）を設定して、管理者がネットワーク デバイスにコマンドを発行できるようにするには、次の手順を実行します。

ステップ 1　TACACS+ プロトコルのグローバル設定およびユーザ認証オプションを設定します。「TACACS+ の設定」（P.18-1）を参照してください。

ステップ 2　ネットワーク リソースを設定します。「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。

ステップ 3　ユーザおよび ID ストアを設定します。「内部 ID ストアの管理」（P.8-4）または「外部 ID ストアの管理」（P.8-19）を参照してください。

ステップ 4　必要に応じてコマンド セットを設定します。「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-31）を参照してください。

ステップ 5　アクセス サービス ポリシーを設定します。「アクセス サービス ポリシーの作成」（P.10-4）を参照してください。

ステップ 6　サービス セレクション ポリシーを設定します。「サービス セレクション ポリシーの作成」（P.10-4）を参照してください。

ステップ 7　認可ポリシー（規則テーブル）を設定します。「デバイス管理のシェル / コマンド認可ポリシーの設定」（P.10-35）を参照してください。

関連トピック

- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「システム管理者およびアカウントの設定」（P.16-3）
- 「ユーザおよび ID ストアの管理」（P.8-1）

- 「外部 ID ストアの管理」（P.8-19）
- 「ポリシー条件の管理」（P.9-1）
- 「アクセス ポリシーの管理」（P.10-1）

TACACS+ のカスタム サービスおよび属性

ここでは、TACACS+ のカスタム属性およびサービスを定義する設定フローについて説明します。

ステップ 1　要求に応じて TACACS+ サービスに移行するためのカスタム TACACS+ 条件を作成します。次の手順を実行します。

a. [Policy Elements] > [Session Conditions] > [Custom] に移動し、[Create] をクリックします。

b. カスタム TACACS+ 条件を作成します。「カスタム セッション条件の作成、複製、および編集」（P.9-5）を参照してください。

ステップ 2　TACACS+ シェル プロファイルを結果として使用し、デバイス管理用のアクセス サービスを作成します。「デバイス管理のシェル / コマンド認可ポリシーの設定」（P.10-35）を参照してください。

ステップ 3　カスタム TACACS+ 属性を作成します。「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）を参照してください。

パスワードベースのネットワーク アクセス

ここでは、次の内容について説明します。

- 「パスワードベースのネットワーク アクセスの概要」（P.4-5）
- 「パスワードベースのネットワーク アクセスの設定フロー」（P.4-7）

パスワードベースのプロトコルの詳細については、を参照してください。付録 B「ACS 5.4 での認証」

パスワードベースのネットワーク アクセスの概要

単純で暗号化されていないユーザ名とパスワードの使用は確実な認証メカニズムではありませんが、インターネット アクセスのように認可レベルまたは特権レベルが低い場合は十分です。

暗号化を使用すると、ネットワーク上でパスワードが不正に取得されるリスクが小さくなります。RADIUS などのクライアント / サーバ アクセス コントロール プロトコルでは、パスワードを暗号化することにより、ネットワーク内でパスワードが不正に取得される事態を防止します。ただし、RADIUS は AAA クライアントと ACS 間でだけ動作します。認証プロセスにおけるこの時点の前の段階で、認可されていないユーザが暗号化されていないパスワードを入手する可能性があります。たとえば、次のような場合です。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザ クライアントとの間の通信
- ネットワークアクセス サーバで終端する ISDN 回線
- エンドユーザ クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

ACS はさまざまな認証方式をサポートしており、ACS のサポートする各種 ID ストアに対する認証を行います。認証プロトコルと ID ストアの互換性の詳細については、「認証プロトコルと ID ストアの互換性」（P.B-36）を参照してください。

パスワードの処理は、使用するセキュリティ制御プロトコル（RADIUS など）のバージョンと種類、および AAA クライアントとエンドユーザ クライアントの設定に基づいて、上記のパスワード認証プロトコルを使用して行うことができます。

ACS では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。基本的なセキュリティ レベルは、Password Authentication Protocol（PAP; パスワード認証プロトコル）によって確保されます。PAP で得られるセキュリティ レベルはごく基本的なレベルですが、クライアントにとってはシンプルで有用なプロトコルです。エンドユーザ クライアントから AAA クライアントに通信するときに MSCHAPv2 を使用すると、パスワードが暗号化されるため、暗号化しない場合よりも高いセキュリティ レベルを確保できます。

（注）　パスワードベースのアクセス（または証明書ベースのアクセス）では、ACS の設定に応じてユーザの認証だけでなく*認可*も行われます。さらに、NAS によってアカウンティング要求が送信される場合は、ユーザのアカウンティングも行われます。

ACS では、次に示すパスワードベースの認証方式がサポートされています。

- プレーンな RADIUS パスワード認証方式
  - RADIUS-PAP
  - RADIUS-CHAP
  - RADIUS-MSCHAPv1
  - RADIUS-MSCHAPv2
- RADIUS EAP ベースのパスワード認証方式
  - PEAP-MSCHAPv2
  - PEAP-GTC
  - EAP-FAST-MSCHAPv2
  - EAP-FAST-GTC
  - EAP-MD5
  - LEAP

認証方式は、次の要素に基づいて選択する必要があります。

- ネットワーク アクセス サーバ：無線アクセス ポイント、802.1X 認証スイッチ、VPN サーバなど
- クライアント コンピュータおよびソフトウェア：EAP サプリカント、VPN クライアントなど
- ユーザの認証に使用する ID ストア：内部または外部（AD、LDAP、RSA トークン サーバ、または RADIUS ID サーバ）

関連トピック

- 「ACS 5.4 での認証」（P.B-1）
- 「パスワードベースのネットワーク アクセスの設定フロー」（P.4-7）
- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「アクセス ポリシーの管理」（P.10-1）

パスワードベースのネットワーク アクセスの設定フロー

ここでは、パスワードベースのネットワーク アクセスに関してエンドツーエンドのフローについて説明し、実行が必要なタスクを示します。タスクを設定する方法に関する情報は、該当するタスクの章にあります。

パスワードベースのネットワーク アクセスを設定するには、次の手順を実行します。

ステップ 1　ネットワーク デバイスおよび AAA クライアントを設定します。

a. 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）で、[Authentication Setting] を [RADIUS] に設定します。

b. 共有秘密を入力します。

詳細については、「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。

ステップ 2　ユーザおよび ID ストアを設定します。詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

ステップ 3　ポリシー条件および認可プロファイルを定義します。詳細については、第 9 章「ポリシー要素の管理」を参照してください。

ステップ 4　アクセス サービスを定義します。詳細については、「アクセス サービスの作成、複製、および編集」（P.10-12）を参照してください。

a. [Access Service Type] を [Network Access] に設定します。

b. [Allowed Protocols] ページで ACS 対応プロトコルのいずれかを選択し、表 4-1 の処理カラムの手順を実行します。

ステップ 5　アクセス サービスをサービス セレクション ポリシーに追加します。詳細については、「サービス セレクション規則の作成、複製、および編集」（P.10-8）を参照してください。

ステップ 6　作成したサービスに戻り、[Authorization Policy] ページで認可規則を定義します。詳細については、「アクセス サービス ポリシーの設定」（P.10-22）を参照してください。

表 4-1　ネットワーク アクセス認証プロトコル

プロトコル	アクション
Process Host Lookup（MAB）	[Allowed Protocols] ページで [Process Host Lookup] を選択します。
RADIUS PAP	[Allowed Protocols] ページで [Allow PAP/ASCII] を選択します。
RADIUS CHAP	[Allowed Protocols] ページで [Allow CHAP] を選択します。
RADIUS MSCHAPv1	[Allowed Protocols] ページで [Allow MS-CHAPv1] を選択します。
RADIUS MSCHAPv2	[Allowed Protocols] ページで [Allow MS-CHAPv2] を選択します。
EAP-MD5	[Allowed Protocols] ページで [Allow EAP-MD5] を選択します。
LEAP	[Allowed Protocols] ページで [Allow LEAP] を選択します。

表 4-1　ネットワーク アクセス認証プロトコル （続き）

プロトコル	アクション
PEAP	[Allowed Protocols] ページで [PEAP] を選択します。PEAP 内部方式の場合は、[EAP-MSCHAPv2] か [EAP-GTC]、またはその両方を選択してください。
EAP-FAST	1. [Allowed Protocols] ページで [Allow EAP-FAST] を選択し、EAP-FAST 設定をイネーブルにします。 2. EAP-FAST 内部方式の場合は、[EAP-MSCHAPv2] か [EAP-GTC]、またはその両方を選択してください。 3. [Allow Anonymous In-Band PAC Provisioning] か [Allow Authenticated In-Band PAC Provisioning]、またはその両方を選択します。 Windows マシンで Microsoft AD に対する認証を行う場合、およびパスワード変更機能の場合は、次の手順を実行します。 1. [Use PACS] オプション ボタンをクリックします。PAC の詳細については、「PAC について」（P.B-22）を参照してください。 2. [Allow Authenticated In-Band PAC Provisioning] をオンにします。 3. [Allow Machine Authentication] をオンにします。 4. [Machine PAC Time to Live] を入力します。 5. [Enable Stateless Session Resume] をオンにします。 6. [Authorization PAC Time to Live] を入力します。 7. [Preferred EAP Protocol] をオンにしてリストから優先プロトコルを設定します。

RADIUS、EAP 以外の認証方式（RADIUS/PAP、RADIUS/CHAP、RADIUS/MS-CHAPv1、RADIUS/MSCHAPv2）、および単純な EAP 方式（EAP-MD5 と LEAP）の場合は、表 4-1 に定義されている [Allowed Protocols] ページのプロトコルだけを設定する必要があります。

一部の複雑な EAP プロトコルでは、次に示す追加設定が必要です。

- EAP-TLS の場合は、次の設定も行う必要があります。
  - EAP-TLS 設定（[System Administration] > [Configuration] > [EAP-TLS Settings]）。
  - ローカル サーバ証明書（[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates]）。
  - CA 証明書（[Users and Identity Stores] > [Certificate Authorities]）。
- PEAP の場合は、次の設定も行う必要があります。
  - [Allowed Protocols] ページの内部方式。さらに、パスワード変更が許可されるかどうかを指定します。
  - PEAP 設定（[System Administration] > [Configuration] > [PEAP Settings]）。
  - ローカル サーバ証明書（[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates]）。
- EAP-FAST の場合は、次の設定も行う必要があります。
  - [Allowed Protocols] ページの内部方式。さらに、パスワード変更が許可されるかどうかを指定します。
  - PAC を使用するかどうか。さらに、PAC を使用する場合は In-Band PAC Provisioning を許可する方法を指定します。

- EAP-FAST 設定（[System Administration] > [Configuration] > [EAP-FAST] > [Settings]）。
- ローカル サーバ証明書（[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates]、Authenticated PAC Provisioning がイネーブルの場合にかぎります）。

関連トピック

- 「ACS 5.4 での認証」（P.B-1）
- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「アクセス ポリシーの管理」（P.10-1）
- 「アクセス サービスの作成、複製、および編集」（P.10-12）
- 「PAC について」（P.B-22）

証明書ベースのネットワーク アクセス

ここでは、次の内容について説明します。

- 「証明書ベースのネットワーク アクセスの概要」（P.4-9）
- 「ACS で証明書を使用する方法」（P.4-10）
- 「証明書ベースのネットワーク アクセス」（P.4-10）

証明書ベースのプロトコルの詳細については、付録 B「ACS 5.4 での認証」を参照してください。

証明書ベースのネットワーク アクセスの概要

EAP-TLS を使用するには、ACS のコンピュータ証明書をインストールする必要があります。インストールされるコンピュータ証明書は、アクセス クライアントが信頼するルート CA まで証明書チェーンをたどることができる CA によって発行される必要があります。

さらに、ACS でアクセス クライアントのユーザ証明書またはコンピュータ証明書を確認するには、そのアクセス クライアントにユーザ証明書またはコンピュータ証明書を発行したルート CA の証明書をインストールしておく必要があります。

ACS では、EAP-TLS プロトコルを使用する証明書ベースのネットワーク アクセスがサポートされています。このプロトコルでは、クライアントによるサーバ認証およびサーバによるクライアント認証に証明書を使用します。

PEAP、または EAP-FAST の authenticated-provisioning モードなどの他のプロトコルでもクライアントによるサーバ認証に証明書を利用しますが、これらは証明書ベースのネットワーク アクセスとは見なされません。これは、サーバがクライアント認証に証明書を使用しないためです。

ACS 公開キー インフラストラクチャ（PKI）の証明書ベース認証は、X509 証明書 ID に基づいています。証明書によって自分自身を識別するエンティティでは、証明書に格納された公開キーに対応する秘密キーを保持します。

証明書は自己署名することも、別の CA に署名してもらうこともできます。証明書の階層を作成すると、その CA に対する各エンティティの信頼関係を構築できます。信頼できるルート CA とは、他のすべての CA の証明書に署名し、結果として階層内の各証明書に署名するエンティティのことです。

ACS は、自分自身の証明書を使用して ACS 自身を識別します。Certificate Trust List（CTL; 証明書信頼リスト）をサポートしており、接続証明書を認可します。また、チェーン証明書のすべてが提示された場合は、アイデンティティ証明書を認可する複雑な階層もサポートします。

証明書で使用する、複数の RSA キー サイズ（512、1024、2048、または 4096 ビット）をサポートしています。その他のキーサイズを使用することもできます。ACS 5.4 では RSA がサポートされています。ACS はデジタル署名アルゴリズム（DSA）をサポートしません。ただし、一部の使用例では、ACS は DSA 暗号スイートが証明書ベースの認証に使用されないようにしません。

ネットワーク アクセス認証に使用するすべての証明書は、X.509 証明書の要件を満たし、SSL/TLS を使用する接続で動作する必要があります。この最小要件を満たしたうえで、クライアントおよびサーバの証明書には追加の要件があります。

ACS では次の 2 種類の証明書を設定できます。

- 信頼証明書：CA 証明書とも呼ばれます。CTL 信頼階層を形成し、リモート証明書の確認に使用します。
- ローカル証明書：ローカル サーバ証明書とも呼ばれます。クライアントは、ローカル証明書をさまざまなプロトコルとともに使用し、ACS サーバを認証します。この証明書は秘密キーと関連付けて保持され、秘密キーは証明書を所持していることの証明に利用されます。

（注）　証明書ベースのアクセス（またはパスワードベースのアクセス）では、ACS の設定に応じてユーザの認証だけでなく*認可*も行われます。さらに、NAS によってアカウンティング要求が送信される場合は、ユーザのアカウンティングも行われます。

関連トピック

- 「CA 証明書の設定」（P.8-69）
- 「ローカル サーバ証明書の設定」（P.18-14）
- 「ACS で証明書を使用する方法」（P.4-10）

ACS で証明書を使用する方法

次に、ACS 5.4 における証明書の使用例を 3 つ示します。

- 「証明書ベースのネットワーク アクセス」（P.4-10）
- 「証明書によるブラウザからの ACS Web インターフェイスの認可」（P.4-12）
- 「LDAP セキュア認証接続の確認」（P.4-12）

証明書ベースのネットワーク アクセス

TLS 関連の EAP および PEAP プロトコルの場合は、ローカル証明書ストアからサーバ証明書をセットアップし、クライアントを認証する信頼証明書リストを設定する必要があります。信頼証明書は、ローカル証明書ストアにある任意の証明書から選択できます。

EAP-TLS または PEAP（EAP-TLS）を使用するには、信頼証明書を入手してインストールする必要があります。タスクを実行する方法に関する情報は、該当するタスクの章にあります。

はじめる前に

次を設定してサーバをセットアップします。

- EAP-TLS または PEAP（EAP-TLS）
- ローカル証明書。「ローカル サーバ証明書の設定」（P.18-14）を参照してください。

EAP-TLS または PEAP（EAP-TLS）の証明書ベースのネットワーク アクセスを設定するには、次の手順を実行します。

ステップ 1　信頼証明書リストを設定します。詳細については、「CA 証明書の設定」（P.8-69）を参照してください。

ステップ 2　LDAP 外部 ID ストアを設定します。LDAP に格納された証明書に対して証明書を確認するときに、この設定が必要となる場合があります。詳細については、「外部 LDAP ID ストアの作成」（P.8-23）を参照してください。

ステップ 3　証明書認証プロファイルをセットアップします。詳細については、「証明書認証プロファイルの設定」（P.8-73）を参照してください。

ステップ 4　ポリシー要素を設定します。詳細については、「ポリシー条件の管理」（P.9-1）を参照してください。

カスタム条件を作成すると、証明書の属性をポリシー条件として使用できます。詳細については、「カスタム セッション条件の作成、複製、および編集」（P.9-5）を参照してください。

ステップ 5　アクセス サービスを作成します。詳細については、「アクセス サービスの設定」（P.10-11）を参照してください。

ステップ 6　[Allowed Protocols] ページで、[EAP-TLS or PEAP (EAP-TLS) as inner method] を選択します。

ステップ 7　アクセス サービスの ID ポリシーおよび認可ポリシーを設定します。詳細については、「アクセス サービス ポリシーの設定」（P.10-22）を参照してください。

（注）　ID ポリシーの規則を作成した結果、証明書認証プロファイルまたは ID 順序が作成される場合があります。詳細については、「ID ポリシーの表示」（P.10-22）を参照してください。

ステップ 8　認可ポリシーを設定します。「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）を参照してください。

ステップ 9　サービス セレクション ポリシーを設定します。「サービス セレクション ポリシーの設定」（P.10-5）を参照してください。

表 4-2　ネットワーク アクセス認証プロトコル

プロトコル	アクション
EAP-TLS	[Allowed Protocols] ページで [Allow EAP-TLS] を選択し、EAP-TLS 設定をイネーブルにします。 • [Enable Stateless Session resume]：アクセス サービスごとにステートレス セッション再開機能をイネーブルにするには、このチェックボックスをオンにします。この機能では、次のオプションを設定することが可能です。 – [Proactive Session Ticket update]：セッション チケットが更新される前に経過する必要がある存続可能時間の量を示すパーセント値を入力します。たとえば、値 10 を入力した場合、セッション チケットの更新は存続可能時間の 10 パーセントが過ぎた後に実行されます。 – [Session ticket Time to Live]：正の整数を使用して日、週、月、および年に対応する最大値を入力します。
PEAP	[Allowed Protocols] ページで [PEAP] を選択します。PEAP 内部方式の場合、[EAP-TLS] または [PEAP Cryptobinding TLV] を選択します。

関連トピック

- 「ローカル サーバ証明書の設定」（P.18-14）
- 「CA 証明書の設定」（P.8-69）

- 「ACS 5.4 での認証」（P.B-1）
- 「EAP-TLS の概要」（P.B-6）

証明書によるブラウザからの ACS Web インターフェイスの認可

ブラウザを使用して ACS に接続する場合は、HTTPS 証明書ベースの認証を使用します。ブラウザから ACS Web インターフェイスを認可するときは、ACS のローカル サーバ証明書が使用されます。ACS ではブラウザ認証がサポートされていません（相互認証はサポートされていません）。

ACS にはデフォルトのローカル サーバ証明書がインストールされているため、ブラウザから ACS に接続できます。デフォルト証明書は自己署名証明書であり、インストール時にこの証明書は変更できません。

関連トピック

- 「ACS で証明書を使用する方法」（P.4-10）
- 「ローカル サーバ証明書の設定」（P.18-14）

LDAP セキュア認証接続の確認

LDAP 外部 ID ストア用にセキュアな外部認証接続を定義するには、CA 証明書を使用して接続を確認します。

証明書を使用して LDAP セキュア認証接続を確認するには、次の手順を実行します。

ステップ 1　LDAP 外部 ID ストアを設定します。「外部 LDAP ID ストアの作成」（P.8-23）を参照してください。

ステップ 2　[LDAP Server Connection] ページで [Use Secure Authentication] をオンにします。

ステップ 3　ドロップダウン メニューから [Root CA] を選択して ACS 用の LDAP 設定を続行します。

関連トピック

- 「ACS で証明書を使用する方法」（P.4-10）
- 「ローカル サーバ証明書の設定」（P.18-14）
- 「外部 ID ストアの管理」（P.8-19）

エージェントレス ネットワーク アクセス

ここでは、次の内容について説明します。

- 「エージェントレス ネットワーク アクセスの概要」（P.4-13）
- 「ホスト ルックアップ」（P.4-13）
- 「エージェントレス ネットワーク アクセスのフロー」（P.4-17）

ネットワーク アクセスに使用するプロトコルの詳細については、「ACS 5.4 での認証」（P.B-1）を参照してください。

エージェントレス ネットワーク アクセスの概要

エージェントレス ネットワーク アクセスとは、ホスト デバイスに適切なエージェント ソフトウェアがない場合に、ポートベースの認証および認可を実行するメカニズムのことです。

たとえば、802.1x サプリカントのないホスト デバイスやサプリカントがディセーブルにされているホスト デバイスなどです。

ホスト デバイス、およびそのデバイスが接続するスイッチでは、802.1x をイネーブルにする必要があります。802.1x サプリカントのないホストまたはデバイスが、802.1x がイネーブルなポートに接続しようとすると、デフォルト セキュリティ ポリシーの対象となります。

デフォルト セキュリティ ポリシーによって、802.1x 認証が成功してからネットワークへのアクセスを許可する必要があることが通知されます。したがって、デフォルトでは 802.1x 非対応のデバイスは 802.1x で保護されたネットワークにアクセスできません。

802.1x をサポートするデバイスの数は増加していますが、ネットワーク接続が必要なデバイスには、802.1x をサポートしない、またはサポートできないデバイスが常に存在します。このようなデバイスの例としては、ネットワーク プリンタ、バッジ リーダー、およびレガシー サーバなどを挙げることができます。これらのデバイスについては、何らかのプロビジョニングを行う必要があります。

非 802.1x デバイスに対応するために、シスコでは 2 つの機能を提供しています。たとえば、MAC Authentication Bypass（ホスト ルックアップ）および Web 認証を使用したゲスト VLAN アクセスです。

ACS 5.4 では、802.1x サプリカントが存在しない場合にホスト ルックアップ フォールバック メカニズムがサポートされます。ホスト ルックアップが設定されている場合、ポートで 802.1x がタイムアウトしたあとにホスト ルックアップに成功すると、ポートはオープン ステートに移行できます。

関連トピック

- 「ホスト ルックアップ」（P.4-13）
- 「エージェントレス ネットワーク アクセスのフロー」（P.4-17）

ホスト ルックアップ

ACS は、クレデンシャル（パスワードや証明書など）に従って ID を認証できない場合の検証方法として、ホスト ルックアップを使用します。ID の検証には、ID ストアのルックアップを行う必要があります。

ホスト ルックアップを使用する例としては、ネットワーク デバイスが MAC 認証バイパス（MAB）を要求するように設定されている場合があります。これは、ポートで 802.1x がタイムアウトしたあと、または認証バイパスを実行するようにポートが明示的に設定されている場合に発生します。MAB を適用すると、ホストはネットワーク アクセス デバイスに接続します。

デバイスは適切なソフトウェア エージェントがホストに存在しないことを検出すると、MAC アドレスによってホストを識別する必要があると判断します。*service-type=10* およびホストの MAC アドレスを含む RADIUS 要求を Calling-Station-Id 属性で ACS に送信します

一部のデバイスで、PAP 認証または EAP-MD5 認証を送信して MAB 要求を実行するように設定されている場合があります。このとき、ユーザ名、ユーザ パスワード、および CallingStationID 属性にホストの MAC アドレスが含まれますが、*service-type=10* 属性は含まれません。

ホスト ルックアップのほとんどの使用例は MAC アドレスの取得ですが、デバイスが個別のパラメータ検証を要求する場合や、MAC アドレスの代わりにこの値が Calling-Station-Id 属性に含まれる場合など、その他のシナリオも考えられます。たとえば、レイヤ 3 での使用例では IP アドレスとなります。

表 4-3 に、ホスト ルックアップの使用例に必要な RADIUS パラメータを示します。

表 4-3　ホスト ルックアップの使用例に対する RADIUS 属性

属性	使用例		
	PAP	802.1x	EAP-MD5
RADIUS::ServiceType	—	コール チェック（PAP または EAP-MD5 を使用）	—
RADIUS::UserName	MAC アドレス	任意の値（通常は MAC アドレス）	MAC アドレス
RADIUS::UserPassword	MAC アドレス	任意の値（通常は MAC アドレス）	MAC アドレス
RADIUS::CallingStationID	MAC アドレス	MAC アドレス	MAC アドレス

ACS では、次の ID ストアのホスト ルックアップがサポートされています。

- 内部ホスト
- 外部 LDAP
- 内部ユーザ
- Active Directory

Active Directory には LDAP API 経由でアクセスできます。

内部ユーザ ID ストアに関連ホストがすでにリストされていて、内部ホスト ID ストアにデータを移動しない場合は、ホスト ルックアップに内部ユーザ ID ストアを使用できます。

ACS が使用するのは MAC 形式（XX-XX-XX-XX-XX-XX）であり、その他の形式に変換することはできません。User-Name 属性（xx:xx:xx:xx:xx:xx など）を使用して内部ユーザ ID ストアを検索するには、[Process Host Lookup] オプションをオフにしておく必要があります。ACS では要求を PAP 要求として処理します。

ホスト ルックアップ設定によって、PAP または EAP-MD5 上での MAC アドレス認証が検出されない場合、認証および認可は通常の PAP または EAP-MD5 のユーザ認証と同様に実行されます。ID ストアには、これらの認証プロトコルをサポートする任意のストアを使用できます。ACS は、RADIUS User-Name 属性で示した MAC アドレス形式を使用します。

関連トピック

- 「ホスト ルックアップ用のアクセス サービスの作成」（P.4-19）
- 「内部 ID ストア ホストの一括操作の表示および実行」（P.8-18）
- 「ユーザおよび ID ストアの管理」（P.8-1）
- 「コール チェックを使用する認証」（P.4-14）

コール チェックを使用する認証

Call Check 属性を含むネットワーク アクセス要求をホスト ルックアップ（RADIUS::ServiceType = 10）として識別する場合、ACS は認証ポリシーに従って、設定された ID ストアで Calling-Station-ID 属性（MAC アドレスなど）の値をルックアップし、ホストを認証（確認）および認可します。

ACS は RADIUS メッセージを受信すると、基本的な分析と確認を実行し、Call Check 属性（RADIUS ServiceType(6)）の値が 10 に等しいかどうかを確認します。RADIUS ServiceType が 10 に等しい場合は、システム ディクショナリ属性 UseCase をホスト ルックアップの値に設定します。

ACS のパケット処理フローでは、Call Check service-type によるホスト ルックアップの検出はサービス セレクション ポリシーの前に実行されます。サービス セレクション ポリシーでは条件 *UseCase equals Host Lookup* を使用できます。

RADIUS 要求の処理では、まず RADIUS User-Name 属性が System UserName 属性にコピーされます。RADIUS Service-Type が 10 の場合は、RADIUS Calling-Station-ID 属性が System User-Name 属性にコピーされ、RADIUS User-Name 属性の値が上書きされます。

ACS では、次の 4 つの MAC アドレス形式がサポートされています。

- ハイフンで区切られた 6 グループの 2 桁 16 進数字：01-23-45-67-89-AB
- コロンで区切られた 6 グループの 2 桁 16 進数字：01:23:45:67:89:AB
- ドットで区切られた 3 グループの 4 桁 16 進数字：0123.4567.89AB
- 区切り文字なしの連続する 12 桁の 16 進数字：0123456789AB

Calling-Station-ID 属性が、サポートされている上記 4 つの MAC アドレス形式のいずれかである場合は、ACS によって XX-XX-XX-XX-XX-XX の形式で User-Name 属性にコピーされます。MAC アドレスが上記 4 つ以外の形式である場合は、ストリングがそのままコピーされます。

Service-Type Call Check の処理

CallingStationID 属性値を System UserName 属性値にコピーしない場合があります。[Process Host Lookup] オプションがオンの場合、ACS は RADIUS User-Name 属性からコピーされた System UserName 属性を使用します。

[Process Host Lookup] オプションがオフの場合は、[HostLookup] フィールドは無視され、元の System UserName 属性の値を使用して認証および認可が行われます。要求の処理は、メッセージ プロトコルに従って続行されます。たとえば、PAP の RADIUS User-Name や User-Password の属性などに従います。

[Process Host Lookup] オプションの設定については、「ホスト ルックアップ用のアクセス サービスの作成」（P.4-19）を参照してください。

PAP/EAP-MD5 認証

MAC アドレス認証に PAP または EAP-MD5 を使用するようにデバイスを設定してある場合は、ネットワーク アクセス サービス内で要求をホスト ルックアップ要求として検出するように、ACS を設定できます。デバイスは、User-Name、User-Password、および Calling-Station-ID の各属性にホストの MAC アドレスを含む要求を送信します。

ホスト ルックアップを検出するように ACS を設定しない場合、アクセス要求は通常の PAP または EAP-MD5 認証要求として処理されます。

[Process HostLookup] フィールドをオンにし、PAP または EAP-MD5 を選択すると、ACS::UseCase 属性に HostLookup 値が設定されます。User-Password 属性は、検出アルゴリズムで無視されます。

ACS は、要求が Call Check 属性を使用している場合と同様に認証プロセスを継続し、その要求をホスト ルックアップ（Service-Type=10）要求として処理します。RADIUS ディクショナリ属性 ACS::UseCase は HostLookup の値に設定されます。

PAP および EAP-MD5 MAC 認証の [Detect Host Lookup] オプションは、サービス セレクション ポリシーのあとに実行されます。サービス セレクション規則が ACS::UseCase = Host Lookup に一致するように設定されている場合、要求はホスト ルックアップ カテゴリに分類されます。

PAP 認証または EAP-MD5 認証を MAC 認証フローとして検出するように ACS が設定されていない場合、ACS では [Detect Host Lookup] オプションが考慮されません。これらの要求は通常のユーザ認証要求と同様に処理され、選択されている ID ストア内でユーザ名とパスワードが検索されます。

関連トピック

- 「ホスト ルックアップ用のアクセス サービスの作成」（P.4-19）
- 「アクセス ポリシーの管理」（P.10-1）
- 「内部 ID ストア ホストの一括操作の表示および実行」（P.8-18）
- 「ユーザおよび ID ストアの管理」（P.8-1）

エージェントレス ネットワーク アクセスのフロー

ここでは、エンドツーエンドのエージェントレス ネットワーク アクセス フローについて説明し、実行が必要なタスクを示します。タスクを設定する方法に関する情報は、該当するタスクの章にあります。

ACS でエージェントレス ネットワーク アクセスを設定するには、リストされた順序で次の手順を実行します。

ステップ 1　ネットワーク デバイスおよび AAA クライアントを設定します。

これは、ACS でネットワーク デバイスおよび AAA クライアントを設定する一般的なタスクです。エージェントレス ネットワーク アクセスに固有のタスクではありません。[Network Resources] > [Network Devices and AAA Clients] を選択し、[Create] をクリックします。「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。

ステップ 2　内部ホストの ID ストアを設定します。

- 内部 ID ストアを設定します。「内部 ID ストアへのホストの追加」（P.4-18）を参照してください。

  または

- 外部 ID ストアを設定します。「ホスト ルックアップ用の LDAP 外部 ID ストアの設定」（P.4-18）を参照してください。

詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

ステップ 3　ID グループを設定します。「ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定」（P.4-19）を参照してください。

詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

ステップ 4　ホスト ルックアップ要求用のポリシー要素および認可プロファイルを定義します。

詳細については、第 9 章「ポリシー要素の管理」を参照してください。

ステップ 5　ホスト ルックアップ用のアクセス サーバを定義することによって、空のサービスを作成します。詳細については、「ホスト ルックアップ用のアクセス サービスの作成」（P.4-19）を参照してください。

ステップ 6　作成したサービスに戻ります。

a. ID ポリシーを定義します。詳細については、「ホスト ルックアップ要求用の ID ポリシーの設定」（P.4-20）を参照してください。

ACS には、複数の ID ストアでホスト MAC アドレスを検索するオプションがあります。

たとえば、MAC アドレスは、内部ホスト ID ストア、設定済みの LDAP ID ストアのいずれか、または内部ユーザ ID ストア内に格納されている可能性があります。

MAC アドレス ルックアップは設定済みの ID ストアのいずれかで行い、MAC 属性は ID 順序で設定した別の ID ストアから取り出すことができます。

ID ストアで MAC アドレスが検出されなかった場合でも、ホスト ルックアップ要求の処理を続行するように、ACS を設定できます。管理者は、MAC アドレスが検出されたかどうかに関係なく、イベントに基づいて認可ポリシーを定義できます。

ACS::UseCase 属性は認証ポリシーの選択に使用できますが、ホスト ルックアップのサポートには必須ではありません。

b. 作成したサービスに戻ります。

c. 認可ポリシーを定義します。詳細については、「ホスト ルックアップ要求用の認可ポリシーの設定」（P.4-21）を参照してください。

ステップ 7　サービス セレクションを定義します。

ステップ 8　アクセス サービスをサービス セレクション ポリシーに追加します。詳細については、「サービス セレクション規則の作成、複製、および編集」（P.10-8）を参照してください。

関連トピック

- 「ユーザおよび ID ストアの管理」（P.8-1）
- 「アクセス ポリシーの管理」（P.10-1）

内部 ID ストアへのホストの追加

ホスト ルックアップ用の内部 ID ストアを設定するには、次の手順を実行します。

ステップ 1　[Users and Identity Store] > [Internal Identity Stores] > [Hosts] を選択し、[Create] をクリックします。

詳細については、「内部 ID ストア ホストの一括操作の表示および実行」（P.8-18）を参照してください。

ステップ 2　[Users and Identity Stores] > [Internal Identity Store] > [Hosts] > [Create] ページの説明に従って、フィールドに入力します。

ステップ 3　[Submit] をクリックします。

前の手順：

「ネットワーク デバイスおよび AAA クライアント」（P.7-5）

次の手順：

「ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定」（P.4-19）

ホスト ルックアップ用の LDAP 外部 ID ストアの設定

ホスト ルックアップ用に LDAP 外部 ID ストアを設定するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、[Create] をクリックします。詳細については、「外部 LDAP ID ストアの作成」（P.8-23）を参照してください。

ステップ 2　LDAP データベース作成の手順を実行します。

[LDAP: Directory Organization] ページで MAC アドレス形式を選択します。

MAC アドレスは、選択した形式で LDAP 外部 ID ストアに保存されます。

ステップ 3　[Finish] をクリックします。

前の手順：
「ネットワーク デバイスおよび AAA クライアント」（P.7-5）

次の手順：
「ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定」（P.4-19）

関連トピック
- 「外部 LDAP ID ストアの作成」（P.8-23）
- 「外部 LDAP ID ストアの削除」（P.8-31）

ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定

ホスト ルックアップ ネットワーク アクセス要求用に ID グループを設定するには、次の手順を実行します。

ステップ 1　[Users and Identity Store] > [Identity Groups] を選択し、[Create] をクリックします。
詳細については、「ID 属性の管理」（P.8-7）を参照してください。

ステップ 2　必要に応じてフィールドに入力します。
ID グループには、プリンタや電話機など、任意のエージェントレス デバイスを指定できます。

ステップ 3　[Submit] をクリックします。

前の手順：
- 「内部 ID ストアへのホストの追加」（P.4-18）
- 「ホスト ルックアップ用の LDAP 外部 ID ストアの設定」（P.4-18）

次の手順：
- 「ホスト ルックアップ用のアクセス サービスの作成」（P.4-19）

関連項目
- 「ID 属性の管理」（P.8-7）

ホスト ルックアップ用のアクセス サービスの作成

アクセス サービスを作成してから、エージェントレス ホストの処理をイネーブルにします。

ホスト ルックアップ用にアクセス サービスを作成するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Service] を選択し、[Create] をクリックします。詳細については、「アクセス サービスの設定」（P.10-11）を参照してください。

ステップ 2　[Access Service Properties - General] ページの説明に従って、フィールドに入力します。

a.　[Service Structure] セクションで [User Selected Policy Structure] を選択します。

b.　[Access Service Type] を [Network Access] に設定し、ポリシー構造を定義します。

c. [Network Access] を選択し、[Identity] および [Authorization] をオンにします。

グループ マッピングおよび [External Policy] オプションは任意です。

d. [Process Host Lookup] を選択する必要があります。

ACS で PAP 認証または EAP-MD5 認証を検出して MAC アドレスを取得し（「PAP/EAP-MD5 認証」（P.4-15）を参照）、ホスト ルックアップ要求（MAB 要求など）と同様に処理する場合は、次の手順を実行します。

e. [Allowed Protocols] ページで、ACS がサポートしている MAB 用のプロトコルのいずれか（EAP-MD5 または PAP）を選択します。

f. ホスト ルックアップとして [Detect PAP/EAP-MD5] を選択します。

関連トピック

- 「アクセス ポリシーの管理」（P.10-1）
- 「ACS 5.4 での認証」（P.B-1）
- 「コール チェックを使用する認証」（P.4-14）
- 「Service-Type Call Check の処理」（P.4-15）

ホスト ルックアップ要求用の ID ポリシーの設定

ホスト ルックアップ要求用に ID ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] > [<access_servicename> Identity] を選択します。

詳細については、「ID ポリシーの表示」（P.10-22）を参照してください。

ステップ 2　[Customize] を選択し、認可ポリシー条件をカスタマイズします。

条件のリストが表示されます。このリストには、ID 属性、システム条件、およびカスタム条件が含まれています。詳細については、「ポリシーのカスタマイズ」（P.10-4）を参照してください。

ステップ 3　[Available] カスタマイズ条件から [Use Case] を選択し、[Selected] 条件に移動します。

ステップ 4　[Identity Policy] ページで [Create] をクリックします。

a. 規則の [Name] を入力します。

b. [Conditions] 領域で [Use Case] をオンにし、値が一致する必要があるかどうかを確認します。

c. [Host Lookup] を選択し、[OK] をクリックします。

この属性選択によって、アクセス要求の処理中に、ACS によって IP アドレスではなくホストが検索されます。

d. 使用する [Identity Source] として、ホスト ルックアップをサポートする ID ストアのいずれかを選択します。

e. [OK] をクリックします。

ステップ 5　[Save Changes] をクリックします。

関連項目

- 「アクセス ポリシーの管理」（P.10-1）

ホスト ルックアップ要求用の認可ポリシーの設定

ホスト ルックアップ要求用に認可ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] > [<access_servicename> Authorization] を選択します。

詳細については、「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）を参照してください。

ステップ 2　[Customize] を選択し、認可ポリシー条件をカスタマイズします。

条件のリストが表示されます。このリストには、ID 属性、システム条件、およびカスタム条件が含まれています。

詳細については、「ポリシーのカスタマイズ」（P.10-4）を参照してください。

ステップ 3　[Available] カスタマイズ条件から [Use Case] を選択し、[Selected] 条件に移動します。

ステップ 4　カスタマイズ結果から [Authorization Profiles] を選択し、[Selected] 条件に移動して [OK] をクリックします。

ステップ 5　[Authorization Policy] ページで [Create] をクリックします。

a.　規則の [Name] を入力します。

b.　[Conditions] 領域で [Use Case] をオンにし、値が一致する必要があるかどうかを確認します。

c.　[Host Lookup] を選択し、[OK] をクリックします。

この属性選択によって、アクセス要求の処理中に、ACS によって IP アドレスではなくホストが検索されます。

d.　認可プロファイルから [Authorization Profile] を選択し、[Selected] 結果カラムに移動します。

e.　[OK] をクリックします。

ステップ 6　[Save Changes] をクリックします。

関連項目

- 「アクセス ポリシーの管理」（P.10-1）

VPN リモート ネットワーク アクセス

リモート アクセス バーチャル プライベート ネットワーク（VPN）を使用すると、パブリックなインターネットからプライベートな企業ネットワークに安全に接続できます。自宅またはその他の場所から、自社のネットワークにアクセスすることも可能です。この VPN は、自社の境界ネットワーク（DMZ）に接続されます。VPN ゲートウェイでは同時 VPN 接続を管理できます。

関連トピック

- 「サポートされる認証プロトコル」（P.4-22）
- 「サポートされる ID ストア」（P.4-22）
- 「サポートされる VPN ネットワーク アクセス サーバ」（P.4-23）
- 「サポートされる VPN クライアント」（P.4-23）
- 「VPN リモート アクセス サービスの設定」（P.4-23）

サポートされる認証プロトコル

ACS 5.4 では、VPN トンネル内の内部認証用に次のプロトコルがサポートされています。

- RADIUS/PAP
- RADIUS/CHAP
- RADIUS/MS-CHAPv1
- RADIUS/MS-CHAPv2

MS-CHAPv1 プロトコルまたは MS-CHAPv2 プロトコルを使用すると、作成されるトンネルを暗号化するための MPPE キーを ACS で生成できます。

関連トピック

- 「VPN リモート ネットワーク アクセス」（P.4-21）
- 「サポートされる ID ストア」（P.4-22）
- 「サポートされる VPN ネットワーク アクセス サーバ」（P.4-23）
- 「サポートされる VPN クライアント」（P.4-23）
- 「VPN リモート アクセス サービスの設定」（P.4-23）

サポートされる ID ストア

ACS は、次の ID ストアに対する VPN 認証を実行できます。

- ACS 内部 ID ストア：RADIUS/PAP、RADIUS/CHAP、RADIUS/MS-CHAP-v1、および RADIUS/MS-CHAP-v2
- Active Directory：RADIUS/PAP、RADIUS/MS-CHAP-v1、および RADIUS/MS-CHAP-v2
- LDAP：RADIUS/PAP
- RSA SecurID サーバ：RADIUS/PAP
- RADIUS トークン サーバ：RADIUS/PAP（ダイナミック OTP）

関連トピック

- 「VPN リモート ネットワーク アクセス」（P.4-21）
- 「サポートされる認証プロトコル」（P.4-22）
- 「サポートされる VPN ネットワーク アクセス サーバ」（P.4-23）
- 「サポートされる VPN クライアント」（P.4-23）
- 「VPN リモート アクセス サービスの設定」（P.4-23）

サポートされる VPN ネットワーク アクセス サーバ

ACS 5.4 では、次の VPN ネットワーク アクセス サーバがサポートされています。

- Cisco ASA 5500 シリーズ
- Cisco VPN 3000 シリーズ

関連トピック

- 「VPN リモート ネットワーク アクセス」（P.4-21）
- 「サポートされる認証プロトコル」（P.4-22）
- 「サポートされる ID ストア」（P.4-22）
- 「サポートされる VPN クライアント」（P.4-23）
- 「VPN リモート アクセス サービスの設定」（P.4-23）

サポートされる VPN クライアント

ACS 5.4 では、次の VPN クライアントがサポートされています。

- Cisco VPN Client 5.0 シリーズ
- Cisco Clientless SSL VPN（WEBVPN）
- Cisco AnyConnect VPN クライアント 2.3 シリーズ
- MS VPN クライアント

関連トピック

- 「VPN リモート ネットワーク アクセス」（P.4-21）
- 「サポートされる認証プロトコル」（P.4-22）
- 「サポートされる ID ストア」（P.4-22）
- 「サポートされる VPN ネットワーク アクセス サーバ」（P.4-23）
- 「VPN リモート アクセス サービスの設定」（P.4-23）

VPN リモート アクセス サービスの設定

VPN リモート アクセス サービスを設定するには、次の手順を実行します。

ステップ 1　デフォルト ネットワーク アクセス サービスの [Allowed Protocols] ページで、VPN プロトコルを設定します。詳細については、「アクセス サービスの許可されたプロトコルの設定」（P.10-16）を参照してください。

ステップ 2　ディクショナリ タイプ、および Tunneling-Protocols 属性のタイプと値を選択して、VPN の認可プロファイルを作成します。詳細については、「認可プロファイルでの RADIUS 属性の指定」（P.9-23）を参照してください。

ステップ 3　[Submit] をクリックし、VPN 認可プロファイルを作成します。

関連トピック

- 「VPN リモート ネットワーク アクセス」（P.4-21）
- 「サポートされる認証プロトコル」（P.4-22）
- 「サポートされる ID ストア」（P.4-22）
- 「サポートされる VPN ネットワーク アクセス サーバ」（P.4-23）
- 「サポートされる VPN クライアント」（P.4-23）
- 「VPN リモート アクセス サービスの設定」（P.4-23）

ACS と Cisco Security Group Access

（注）　ACS は、Security Group Access 機能をイネーブルにするために追加機能ライセンスが必要です。

Cisco Security Group Access（以後、Security Group Access と呼ぶ）は、シスコ製品の新しいセキュリティ アーキテクチャです。ネットワーク トラフィックの機密保持、メッセージ認証、整合性、アンチリプレイ保護を提供する信頼できるネットワーク ファブリックを作成するために Security Group Access を使用できます。

Security Group Access では、すべてのネットワーク デバイスに ID を設定し、それらのデバイスがネットワーク内で動作を開始する前に認証および認可を行う必要があります。この対策により、セキュアなネットワーク内に不適切なネットワーク デバイスが接続されることを予防できます。

これまで、ACS はユーザおよびホストだけを認証し、ネットワークへのアクセスを許可していました。Security Group Access により、ACS は、名前とパスワードを使用して、ルータやスイッチなどのデバイスも認証します。ネットワーク インターフェイス カード（NIC）が取り付けられているすべてのデバイスは、デバイス自身を認証するか、または信頼ネットワークには接続しないようにする必要があります。

IP アドレスではなく名前によってデバイスを識別できるため、セキュリティが向上し、デバイス管理が簡素化されます。

（注）　Cisco IOS 12.2(33) SXI が稼働する Cisco Catalyst 6500 および DataCenter 3.0（Nexus 7000）NX-OS 4.0.3 デバイスは Security Group Access をサポートします。Cisco Catalyst 6500 では Security Group Tag（SGT）がサポートされていますが、このリリースでは Security Group Access Control List（SGACL）はサポートされていません。

Security Group Access 用に ACS を設定するには、次の手順を実行します。

1. ユーザの追加

   これは、ACS でユーザを追加する一般的なタスクです。Security Group Access に固有ではありません。[Users and Identity Stores] > [Internal Identity Store] > [Users] を選択し、[Create] をクリックします。詳細については、「内部ユーザの作成」（P.8-11）を参照してください。

2. Security Group Access 用デバイスの追加。
3. セキュリティ グループの作成。
4. SGACL の作成。
5. NDAC ポリシーの設定。

6. Security Group Access 用の EAP-FAST 設定の構成。
7. Security Group Access アクセス用のアクセス サービスの作成。
8. エンドポイント アドミッション コントロール ポリシーの作成。
9. 出力ポリシーの作成。
10. デフォルト ポリシーの作成。

Security Group Access 用デバイスの追加

RADIUS プロトコルには、AAA クライアントとサーバ間の共有秘密情報が必要です。ACS では、RADIUS 要求が既知の AAA クライアントから送信された場合にだけ、この要求が処理されます。共有秘密情報を使用して ACS の AAA クライアントを設定する必要があります。

Security Group Access デバイスは、同じ共有秘密を使用して設定する必要があります。Security Group Access では、すべてのデバイスが、セキュア ネットワークに参加する新しいデバイスに対して AAA クライアントとして動作できる必要があります。

すべての Security Group Access デバイスは、EAP Flexible Authentication via Secured Tunnel（EAP-FAST）プロトコルの一部として、Protected Access Credential（PAC）を所有しています。PAC は、AAA クライアントの識別に使用されます。RADIUS 共有秘密情報は、この PAC から取得できます。

ネットワーク デバイスを追加するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Client] を選択し、[Create] をクリックします。詳細については、「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。

ステップ 2　[Network Devices and AAA Clients] ページのフィールドに入力します。

- デバイスをシード Security Group Access デバイスとして追加するには、[RADIUS] および [Security Group Access] をオンにし、Security Group Access クライアントとしてデバイスを追加するには、[Security Group Access] のみをオンにします。

  RADIUS クライアントとしてデバイスを追加する場合は、[IP Address] および [RADIUS/Shared Secret] を入力します。

  Security Group Access デバイスとしてデバイスを追加する場合は、[Security Group Access] セクションのフィールドに入力します。
- [Advanced Settings] をオンにして、Security Group Access デバイス設定の詳細設定を表示し、デフォルト設定を修正できます。

場所またはデバイス タイプは、NDAC ポリシー規則を設定するための条件として使用できます。

ステップ 3　[Submit] をクリックします。

セキュリティ グループの作成

Security Group Access は、入力でパケットにタグを付加するためにセキュリティ グループを使用して、あとで出力時にフィルタできるようにします。セキュリティ グループを使用した結果、セキュリティ グループ タグが付加されます。これは、ネットワーク デバイスに送信される 4 バイトのストリング ID です。

Web インターフェイスでは 10 進数および 16 進数で表示されます。SGT の値は一意です。セキュリティ グループを編集するときに、名前は変更できますが SGT ID は変更できません。

セキュリティ グループ名 *Unknown* および *Any* は予約されています。この予約名は、出力ポリシー マトリクスで使用します。出力ポリシーが変更されると、生成 ID が変更されます。

デバイスで考慮されるのは SGT の値だけです。セキュリティ グループの名前および説明は管理上の便宜のためのものであり、デバイスには伝達されません。したがって、セキュリティ グループの名前と説明を変更しても、SGT の生成 ID には影響ありません。

セキュリティ グループを作成するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorizations and Permissions] > [Network Access] > [Security Groups] を選択し、[Create] をクリックします。

ステップ 2　「セキュリティ グループ アクセス コントロール リストの設定」（P.9-35）の説明に従って、フィールドに入力します。

ヒント　セキュリティ グループを編集すると、セキュリティ グループ タグおよび生成 ID が表示されます。

ステップ 3　[Submit] をクリックします。

SGACL の作成

Security Group Access Control List（SGACL）は、標準的な IP ベースの ACL によく似ており、TCP、ユーザ データグラム プロトコル（UDP）、およびポートまでのトランスポート プロトコル、FTP、または Secure Shell Protocol（SSH）の通信を許可または拒否するかどうかを指定できます。

セキュリティ グループ間の通信に適用する SGACL も作成できます。ACS で Security Group Access ポリシー管理を適用するには、カスタマイズ可能な出力マトリクス ビューを使用して送信元および宛先のセキュリティ グループの共通部分、または個々の送信元および宛先のセキュリティ グループ ペアにこれらの SGACL を設定します。

SGACL を作成するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorizations and Permissions] > [Named Permissions Objects] > [Security Group ACLs] を選択してから、[Create] をクリックします。

ステップ 2　「セキュリティ グループ アクセス コントロール リストの設定」（P.9-35）の説明に従って、フィールドに入力します。

ステップ 3　[Submit] をクリックします。

NDAC ポリシーの設定

Network Device Admission Control（NDAC; ネットワーク デバイス アドミッション コントロール）ポリシーでは、デバイスに送信されるセキュリティ グループを定義します。NDAC ポリシーを設定する場合は、NDG など、あらかじめ定義されている条件を使用して規則を作成します。

NDAC ポリシーは単一のサービスで、1 つ以上の規則が定義された単一のポリシーが含まれます。認証、ピア認可、および環境の各要求に対する応答の設定には同じポリシーが使用されるため、同じデバイスに適用した場合は、すべての要求タイプについて同じ SGT が返されます。

（注）　サービス セレクション ポリシーのサービスとして NDAC ポリシーを追加できません。ただし、NDAC ポリシーは Security Group Access デバイスに自動的に適用されます。

デバイスに NDAC ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Security Group Access Control] > [Security Group Access] > [Network Device Access] > [Authorization Policy] を選択します。

ステップ 2　[Customize] をクリックし、NDAC ポリシー規則で使用する条件を選択します。

[Default Rule] は、一致する規則がない場合、または規則が定義されていない場合のデフォルト規則となります。[Default Rule] 結果のデフォルト セキュリティ グループ タグは [Unknown] です。

ステップ 3　[Create] をクリックし、新しい規則を作成します。

ステップ 4　[NDAC Policy Properties] ページのフィールドに入力します。

ステップ 5　[Save Changes] をクリックします。

Security Group Access 用の EAP-FAST 設定の構成

RADIUS 情報は PAC から取得されるため、EAP-FAST トンネル PAC の存続時間を定義する必要があります。アクティブな PAC の存続可能時間を更新することもできます。

トンネル PAC の EAP-FAST 設定を行うには、次の手順を実行します。

ステップ 1　[Access Policies] > [Security Group Access Control] > [Network Device Access] を選択します。

ステップ 2　[Network Device Access EAP-FAST Settings] ページのフィールドに入力します。

ステップ 3　[Submit] をクリックします。

Security Group Access アクセス用のアクセス サービスの作成

エンドポイント デバイスに対するエンドポイント アドミッション コントロール ポリシー用のアクセス サービスを作成し、サービス セレクション ポリシーにそのサービスを追加できます。

（注）　NDAC ポリシーは Security Group Access デバイスに自動的に適用されるサービスです。Security Group Access デバイス用のアクセス サービスを作成する必要はありません。

アクセス サービスを作成するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Service] を選択し、[Create] をクリックします。詳細については、「アクセス サービスの設定」（P.10-11）を参照してください。

ステップ 2　必要に応じて、[Access Service Properties - General] ページのフィールドに入力します。

ステップ 3　[Service Structure] セクションで [User selected policy structure] を選択します。

ステップ 4　[Network Access] を選択し、[Identity] および [Authorization] をオンにします。

ステップ 5　[Next] をクリックします。

[Access Services Properties] ページが表示されます。

ステップ 6　[Authentication Protocols] 領域で、使用するアクセス サービスに関連するプロトコルのチェックボックスをオンにします。

ステップ 7　[Finish] をクリックします。

エンドポイント アドミッション コントロール ポリシーの作成

サービスを作成したあとに、エンドポイント アドミッション コントロール ポリシーを設定します。エンドポイント アドミッション コントロール ポリシーは、エンドポイントに対する SGT および認可プロファイルを返します。複数のポリシーを作成し、デフォルト規則ポリシーを設定できます。デフォルトは Deny Access および Unknown セキュリティ グループです。

アクセス サービスにセッション認可ポリシーを追加するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] > ***service*** > [Authorization] を選択します。

ステップ 2　認可ポリシーを設定します。「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）を参照してください。

ステップ 3　[Network Access Authorization Rule Properties] ページのフィールドに入力します。

[Default Rule] は、一致する規則がない場合、または規則が定義されていない場合のデフォルト規則となります。デフォルト規則結果のデフォルトは [Deny Access] です。この設定ではネットワークへのアクセスが拒否されます。セキュリティ グループ タグは [Unknown] です。

セキュリティ グループは、Security Group Access のセッション認可ポリシー作成時に変更できます。

ステップ 4　[OK] をクリックします。

ステップ 5　[Access Policies] > [Service Selection Policy] を選択し、エンドポイント ポリシーに追加するサービスを選択します。詳細については、「サービス セレクション ポリシーの設定」（P.10-5）を参照してください。

ステップ 6　[Service Select Policy] ページのフィールドに入力します。

ステップ 7　[Save Changes] をクリックします。

出力ポリシーの作成

出力ポリシー（SGACL ポリシーとも呼ばれます）によって、送信元および宛先の SGT に基づいてネットワークの出力ポイントで適用される SGACL が決定されます。出力ポリシーはマトリクスで表現され、X 軸および Y 軸がそれぞれ宛先 SGT および送信元 SGT を表します。また、各セルにはこれら 2 つの SGT の共通部分に適用される SGACL のセットが入ります。

この SGT を伝送するエンドポイント（または Security Group Access デバイス）がパケットを送信する場合は、任意のセキュリティ グループが送信元 SGT の役割を果たすことができます。パケットが、この SGT を伝送するエンドポイント（または Security Group Access デバイス）を宛先とする場合は、任

意のセキュリティ グループが宛先 SGT の役割を果たすことができます。したがって、出力マトリクスには既存のセキュリティ グループが両方の軸にすべてリストされ、SGT セットとその SGT セット自身のデカルト積（SGT x SGT）となります。

マトリクスの先頭行（最上部）にはカラム ヘッダーがあり、ここには宛先 SGT が表示されます。先頭列（左端）には行タイトルがあり、送信元 SG が表示されます。これらの軸の共通部分が原点セル（左上隅）で、軸のタイトル、つまり宛先および送信元が入ります。

他のすべてのセルは、定義済みの SGACL が含まれる内部マトリクス セルです。行および列は、SGT 名に従ってアルファベット順に並べられます。SGACL ごとに、200 個の ACE を保持できます。

最初のうち、マトリクスには未知の送信元 SG および未知の宛先 SG が入っています。*未知*というのは、事前に定義された SG のことであり、この値は変更できません。SG を追加すると、新しい行と新しい列がマトリクスに追加されます。新規に追加されるセルの内容は空です。

出力ポリシーを追加して出力マトリクスにデータを入力するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択します。

出力マトリクスが表示されます。セキュリティ グループは定義した順序で表示されます。

ステップ 2　セルをクリックして [Edit] をクリックします。

ステップ 3　必要に応じてフィールドに入力します。

ステップ 4　セルに適用する SGACL のセットを選択し、選択したセットを [Selected] カラムに移動します。

この ACL は、セルの座標に一致する送信元および宛先の SGT の出力ポイントで使用されます。SGACL は表示される順序で適用されます。

ステップ 5　[Up] および [Down] の矢印を使用し、順序を変更します。デバイスは、設定された順序でポリシーを適用します。選択したセキュリティ グループのパケットに SGACL が適用されます。

ステップ 6　[Submit] をクリックします。

デフォルト ポリシーの作成

出力マトリクスで送信元 SG および宛先 SG の出力ポリシーを設定したあとに、デフォルト出力ポリシーを設定することを推奨します。デフォルト ポリシーは、SGT が割り当てられていないデバイスに適用されます。デフォルト ポリシーは、ネットワーク デバイスによって、セルに定義されている特定のポリシーに追加されます。デフォルト ポリシーの初期設定は *Permit All* です。

*デフォルト ポリシー*という用語は、すべてのセキュリティ グループ ポリシーのすべてのセキュリティ グループと関連しています。Security Group Access ネットワーク デバイスで、デフォルト ポリシーは特定セルのポリシーの最後に連結されます。

セルがブランクの場合は、デフォルト ポリシーだけが適用されます。セルにポリシーが含まれている場合、得られるポリシーはセル固有のポリシーのあとにデフォルト ポリシーを結合したものになります。

特定セルのポリシーとデフォルト ポリシーの結合方法は、デバイスで稼働しているアルゴリズムによって異なります。結果は、2 つのポリシーを連結した場合と同じになります。

最初にパケットが分析され、セルの SGACL によって定義された ACE に一致するかどうかが確認されます。一致しない場合、そのパケットでは不成立となり、デフォルト ポリシーの ACE と一致するかどうかが確認されます。

セル固有ポリシーとデフォルト ポリシーの結合は、ACS ではなく、Security Group Access ネットワーク デバイスによって行われます。ACS 側から見ると、セル固有ポリシーとデフォルト ポリシーは 2 組の異なる SGACL であり、2 つの別々なポリシー クエリーに対する応答でデバイスに送信されます。

デフォルト ポリシーを作成するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択し、[Default Policy] を選択します。

ステップ 2　[Default Policy for Egress Policy] ページに従ってフィールドに入力します。

ステップ 3　[Submit] をクリックします。

RADIUS および TACACS+ プロキシ要求

ネットワーク アクセス サーバ（NAS）から RADIUS 認証要求および認証/許可 TACACS+ 要求を受信してそれらの要求をリモート サーバに転送するプロキシ サーバとして機能するように ACS を使用できます。次に ACS は、リモート RADIUS または TACACS+ サーバから転送された各要求の応答を受信し、その応答をクライアントに返送します。

ACS ではサービス セレクション ポリシーを使用して、ローカル処理が必要な着信認証要求およびアカウンティング要求と、リモート RADIUS または TACACS+ サーバへの転送が必要な要求とを区別します。

ACS は NAS からプロキシ要求を受信すると、リストにある最初のリモート RADIUS または TACACS+ サーバにその要求を転送します。リモート RADIUS サーバから届いた最初の有効または無効な応答を処理し、次の処理を実行します。

- Access-Challenge、Access-Accept、または Access-Reject など、応答が RADIUS に有効な場合、ACS は NAS に応答を返します。
- ACS が指定された期間内に、応答を受信しない場合、ACS は指定した回数の再試行の後で、または指定されたネットワーク タイムアウト後に、リスト内の次のリモート RADIUS サーバへ要求を転送します。
- 応答が無効な場合、ACS プロキシは次のリモート RADIUS サーバへのフェールオーバーを実行します。リストの最後のフェールオーバー リモート RADIUS サーバまで応答を取得せずに到達すると、ACS は要求をドロップし、NAS に応答をまったく送信しません。

ACS は、リモート TACACS+ サーバから届いた最初の有効または無効な応答を処理し、次の処理を実行します。

- TAC_PLUS_AUTHEN (REPLY) または TAC_PLUS_AUTHOR(RESPONSE) など、応答が TACACS+ に有効な場合、ACS は NAS に応答を返します。
- ACS が指定された期間内に、応答を受信しない場合、ACS は指定した回数の再試行の後で、または指定されたネットワーク タイムアウト後に、リスト内の次のリモート TACACS+ サーバへ要求を転送します。
- 応答が無効な場合、ACS プロキシは次のリモート TACACS+ サーバへのフェールオーバーを実行します。リストの最後のフェールオーバー リモート TACACS+ サーバまで応答を取得せずに到達すると、ACS は要求をドロップし、NAS に応答をまったく送信しません。

ユーザ名（RADIUS）またはユーザ（TACACS+）からプレフィックス、サフィックス、およびその両方を削除するように ACS を設定できます。たとえば、ユーザ名 acme\smith@acme.com から、\ および @ をそれぞれプレフィックスおよびサフィックスの区切り文字として指定すると、ユーザの名前 smith だけを抽出するように ACS を設定できます。

ACS では、ローカル アカウンティング、リモート アカウンティング、またはその両方を実行できます。両方を選択した場合、ACS はローカル アカウンティングを実行してからリモート アカウンティングに進みます。ローカル アカウンティングで何らかのエラーがあった場合、ACS はそのエラーを無視してリモート アカウンティングに進みます。

プロキシ処理の実行中、ACS は次の処理を行います。

1. NAS から次のパケットを受信し、リモート RADIUS サーバに転送します。
- Access-Request
2. リモート RADIUS サーバから次のパケットを受信し、NAS に返送します。
- Access-Accept
- Access-Reject
- Access-Challenge
3. NAS から次のパケットを受信し、リモート TACACS+ サーバに転送します。
- TAC_PLUS_AUTHOR
- TAC_PLUS_AUTHEN
4. 次のパケットをリモート TACACS+ サーバから受信し、NAS に返送します。この動作は設定可能です。
- TAC_PLUS_ACCT

応答のない外部 RADIUS サーバをおよそ *タイムアウト* X *リトライ回数*秒間待機してから、フェールオーバーによって次のサーバに移行します。

最初に応答のあるサーバに到達するまでに、リストには応答のないサーバがいくつか存在する可能性があります。この場合、応答のある外部 RADIUS サーバに転送される各要求は、*以前に応答のなかったサーバ数* X *タイムアウト* X *リトライ回数*の間、遅延します。

この遅延は、EAP または RADIUS カンバセーションにおける 2 つのメッセージ間の外部 RADIUS サーバ タイムアウトよりも長くなる可能性があります。このような場合、外部 RADIUS サーバで要求がドロップされる場合があります。

フェールオーバーによって次のサーバに移行するまで無応答の外部 TACACS+ サーバが待機する秒数を設定できます。

ACS 5.4 は、RADIUS（IPv4）および TACACS+（IPv4 と IPv6）プロキシ用に複数のネットワーク インターフェイス コネクタをサポートします。仮想マシン、UCS、IBM、または CAM プラットフォームの ACS 5.4 には最大 4 つのネットワーク インターフェイス（イーサネット 0、イーサネット 1、イーサネット 2、およびイーサネット 3）が搭載されています。詳細については、『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.4*』の「Connecting the Network Interface」セクションの「Multiple Network Interface Connector」を参照してください。

関連トピック

- 「サポートされるプロトコル」（P.4-32）
- 「サポートされる RADIUS 属性」（P.4-32）
- 「プロキシ サービスの設定」（P.4-34）

サポートされるプロトコル

ACS の RADIUS プロキシ機能では、次のプロトコルがサポートされています。

- すべての RADIUS プロトコルの転送のサポート
- すべての EAP プロトコル
- ACS でサポートされていないプロトコル（ACS プロキシはプロトコルのカンバセーションに干渉せず、単に要求を転送するため）

（注）　ACS プロキシは暗号化された RADIUS 属性を使用するプロトコルをサポートできません。

ACS の TACACS+ プロキシ機能では、次のプロトコルがサポートされています。

- PAP
- ASCII
- CHAP
- MSCHAP 認証タイプ

関連トピック

- 「RADIUS および TACACS+ プロキシ要求」（P.4-30）
- 「サポートされる RADIUS 属性」（P.4-32）
- 「プロキシ サービスの設定」（P.4-34）

サポートされる RADIUS 属性

サポートされている次の RADIUS 属性は暗号化されます。

- User-Password
- CHAP-Password
- Message-Authenticator
- MPPE-Send-Key および MPPE-Recv-Key
- Tunnel-Password
- LEAP セッション キー Cisco AV-Pair

TACACS+ の本文の暗号化

NAS から暗号化された本文があるパケット（フラグ TAC_PLUS_UNECRYPTED_FLAG は 0x0）を受信すると、ACS は NAS と ACS 間の共有秘密および sessionID などの共通データで本文を復号化し、ACS および TACACS+ プロキシ サーバ間の共通データで本文を暗号化します。パケットの本文がクリア テキストの場合、ACS はクリア テキストでそれを TACACS+ サーバへ再送信します。

TACACS+ サーバへの接続

ACS は別の TACACS+ サーバへの単一の接続をサポートします（フラグ TAC_PLUS_SINGLE_CONNECT_FLAG は 1）。リモート TACACS+ サーバが単一 TCP 接続による多重化 TACACS+ セッションをサポートしない場合、ACS はセッションごとに接続を開くか閉じます。

関連トピック

- 「RADIUS および TACACS+ プロキシ要求」（P.4-30）
- 「サポートされるプロトコル」（P.4-32）
- 「プロキシ サービスの設定」（P.4-34）

プロキシ サービスの設定

プロキシ サービスを設定するには、次の手順を実行します。

ステップ 1　一連のリモート RADIUS および TACACS+ サーバを設定します。リモート サーバを設定する方法の詳細については、「外部プロキシ サーバの作成、複製、および編集」（P.7-21）を参照してください。

ステップ 2　外部プロキシ サービスを設定します。外部プロキシ サービスを設定する方法の詳細については、「アクセス サービスの一般プロパティの設定」（P.10-13）を参照してください。

[User Selected Service Type] オプションを選択し、[Access Service Properties - General] ページで [Access Service Policy Structure] として [External proxy] を選択する必要があります。

ステップ 3　許可されるプロトコルを設定したら、[Finish] をクリックして外部プロキシ サービスの設定を完了します。

関連トピック

- 「RADIUS および TACACS+ プロキシ要求」（P.4-30）
- 「サポートされるプロトコル」（P.4-32）
- 「サポートされる RADIUS 属性」（P.4-32）

CHAPTER 5

[My Workspace] の概要

Cisco Secure ACS Web インターフェイスは、Microsoft Internet Explorer バージョン 6.x から 9.x および Mozilla Firefox バージョン 3.x から 10.x を使用して表示されるように設計されています。Web インターフェイスを使用して、ACS を表示および管理できる以外に、ネットワーク内のイベントを監視およびレポートできます。

これらのレポートは、接続アクティビティのトラッキング、現在ログインしているユーザの表示、失敗した認証および認可の試行のリストなどを行います。

[My Workspace] ドロワには、次の項目があります。

- 「[Welcome] ページ」（P.5-1）
- 「タスク ガイド」（P.5-2）
- 「[My Account] ページ」（P.5-2）
- 「ログイン バナー」（P.5-3）
- 「Web インターフェイスの使用方法」（P.5-3）
- 「Web インターフェイスを使用した ACS オブジェクトのインポートおよびエクスポート」（P.5-19）
- 「一般的なエラー」（P.5-27）
- 「アクセシビリティ」（P.5-30）

[Welcome] ページ

[Welcome] ページは、ACS の起動時に表示され、一般的な ACS タスクへのショートカットと情報へのリンクを提供します。

ACS セッション中に、いつでも [Welcome] ページに戻ることができます。このページに戻るには、[My Workspace] > [Welcome] を選択します。

表 5-1　[Welcome] ページ

フィールド	説明
Before You Begin	ACS ポリシー モデルと関連用語を説明するセクションへのリンクがあります。
Getting Started	このセクションのリンクは、ACS タスクの実行手順を示す ACS タスク ガイドを表示します。
Quick Start	クイック スタート シナリオに関するタスク ガイドを開きます。これらの手順は、試験環境、評価環境、またはデモンストレーション環境で ACS を迅速に稼働させるための最小限のシステム設定手順を示します。

表 5-1　[Welcome] ページ （続き）

フィールド	説明
Initial System Setup	初期システム設定に関するタスク ガイドを開きます。このシナリオでは、必要に応じて ACS を操作用に設定するために必要な手順を示します。多くの手順は任意です。
Policy Setup Steps	ポリシー設定に関するタスク ガイドを開きます。このシナリオでは、ACS ポリシーを設定するために必要な手順を示します。
New in ACS 5	このセクションのオプションは、ACS オンライン ヘルプのトピックにリンクします。オプションをクリックすると、選択したトピックに関する情報を表示するオンライン ヘルプ ウィンドウが開きます。 ACS の機能とタスクに関する詳細情報を表示するには、オンライン ヘルプ トピックのリンクおよびオンライン ヘルプの [Contents] ペインのリンクを使用します。
Tutorials & Other Resources	次の項目へのリンクがあります。 • 概要紹介のビデオ • 一般的な ACS シナリオの手順を示す設定ガイド

ACS 5.4 では、ようこそページにバナーを表示することもできます。[Login Banner] ページからこの [After Login] バナー テキストをカスタマイズできます。

タスク ガイド

[My Workspace] ドロワから、タスク ガイドにアクセスできます。いずれかのタスクをクリックすると、Web インターフェイスの右側にフレームが開きます。このフレームには、手順以外に、追加情報へのリンクが表示されます。ACS には、次のタスク ガイドが備えられています。

- Quick Start：ACS を迅速に起動して稼働させるために必要な最小限の手順をリストします。
- Initial System Setup：任意の手順に関する情報など、基本操作用に ACS を設定するために必要な手順をリストします。
- Policy Setup Steps : ACS アクセス コントロール ポリシーを定義するために必要な手順をリストします。

[My Account] ページ

（注）　すべての ACS 管理者アカウントには、1 つ以上の管理ロールが割り当てられています。アカウントに割り当てられているロールに応じて、一部の手順で説明する操作を実行できる場合とできない場合があり、オプションが表示される場合と表示されない場合があります。適切な管理者特権を設定するには、「システム管理者およびアカウントの設定」（P.16-3）を参照してください。

[My Account] ページは、現在 ACS にログインしている管理者の管理者パスワードを更新および変更する場合に使用します。

このページを表示するには、[My Workspace] > [My Account] を選択します。

表 5-2　[My Account] ページ

フィールド	説明
General	現在ログインしている管理者に関する次の情報を表示する読み取り専用フィールドです。 • 管理者名 • 説明 • 電子メール アドレス（使用可能な場合）
Change Password	パスワード ポリシーに基づくパスワード定義の規則が表示されます。 パスワードを変更するには、次の手順を実行します。 1. [Password] フィールドに現在のパスワードを入力します。 2. [New Password] フィールドに新しいパスワードを入力します。 3. [Confirm Password] フィールドに新しいパスワードをもう一度入力します。
Assigned Roles	現在ログインしている管理者に割り当てられているロールを表示します。

関連トピック

- 「管理者の認証設定」（P.16-10）
- 「管理者パスワードの変更」（P.16-22）

ログイン バナー

ACS 5.4 では、ログイン バナーのテキストのカスタマイズをサポートします。2 組のバナー テキストを設定できます。たとえば、ロギング前に一方のバナー テキストを表示でき、ログイン後に別のバナー テキストを表示できます。[Login Banner] ページからこのカスタマイズを行うことができます。著作権ステートメントは両方のバナーのデフォルトです。

ログイン バナーをカスタマイズするには、[My Workspace] > [Login Banner] を選択します。

表 5-3　[Login Banner] ページ

フィールド	説明
Before Login	ログイン前にバナーに表示するテキストを入力します。
After Login	ログイン後にバナーに表示するテキストを入力します。

Web インターフェイスの使用方法

ACS Web インターフェイスを使用して、ACS を設定および管理できます。ACS Web インターフェイスでは、ページへのアクセス、設定タスクの実行、およびインターフェイス設定エラーの表示を行うことができます。この章の内容は次のとおりです。

- 「Web インターフェイスへのアクセス」（P.5-4）
- 「Web インターフェイスについて」（P.5-5）
- 「一般的なエラー」（P.5-27）
- 「アクセシビリティ」（P.5-30）

Web インターフェイスへのアクセス

ACS Web インターフェイスは、Microsoft Internet Explorer の HTTPS 対応バージョン 6.x から 9.x までおよび Mozilla Firefox バージョン 3.x から 10.x までサポートされます。

この項の構成は、次のとおりです。

- 「ログイン」（P.5-4）
- 「ログアウト」（P.5-5）

ログイン

インストール後、初めて ACS Web インターフェイスにログインする場合は、次の手順を実行します。

ステップ 1　ブラウザに ACS URL を入力します。たとえば、**https://***acs_host*/**acsadmin**、**https://[***IPv6 address*]/**acsadmin**、または **https://ipv4 address/acsadmin** と入力します。ここで、/acs_host は IP アドレスまたはドメイン ネーム システム（DNS）ホスト名です。IPv6 用の DNS ホスト名が機能するのは、IP アドレスが IPv4 と IPv6 の両方の形式で解決される場合です。

（注）　IPv6 アドレスを使用した ACS Web インターフェイスの起動は、Mozilla Firefox バージョン 4.x 以降でサポートされていません。

ログイン ページが表示されます。

ステップ 2　[Username] フィールドに **ACSAdmin** と入力します。値の大文字と小文字は区別されません。

ステップ 3　[Password] フィールドに **default** と入力します。値の大文字と小文字は区別されます。

このパスワード（default）は、インストール後、初めてログインするときにだけ有効です。必要な場合は、[Reset] をクリックし、[Username] フィールドと [Password] フィールドをクリアして最初からやり直します。

ステップ 4　[Login] をクリックするか、Enter を押します。

ログイン ページが再び表示され、パスワードを変更するよう求められます。

インストール後 Web インターフェイスに初めてログインするとき、および、ACS で設定されている認証設定に基づくその他の状況で、ACS によってパスワードの変更を要求するプロンプトが表示されます。

ステップ 5　[Old Password] フィールドに **default** と入力してから、[New Password] フィールドと [Confirm Password] フィールドに新しいパスワードを入力します。

ユーザ名またはパスワードを忘れた場合は、**acs reset-password** コマンドを使用して、ユーザ名を ACSAdmin に、パスワードを default にリセットします。リセット後、パスワードを変更するよう求められます。詳細については、『*Command Line Reference Guide for ACS 5.4*』を参照してください。

ステップ 6　[Login] をクリックするか、Enter を押します。

有効なライセンスをインストールすることを要求するプロンプトが表示されます。

（注）　ライセンス ページは、ACS に初めてログインするときにだけ表示されます。

ステップ 7　有効なライセンスをインストールするには、「ライセンス ファイルのインストール」（P.18-36）を参照してください。

- ログインに成功すると、ACS の Web インターフェイスのメイン ページが表示されます。
- ログインに失敗すると、次のエラー メッセージが表示されます。

  ```
  Access Denied.Please contact your Security Administrator for assistance.
  ```

  [Username] フィールドと [Password] フィールドがクリアされます。

ステップ 8　有効なユーザ名とパスワードを再度入力し、[Login] をクリックします。

ログアウト

ACS の Web インターフェイスの見出しで [Logout] をクリックし、管理セッションを終了します。ACS からログアウトするかどうかを確認するダイアログボックスが表示されます。[OK] をクリックします。

注意　セキュリティ上の理由から、管理セッションを完了したときに ACS からログアウトすることが推奨されます。ログアウトしない場合、ACS Web インターフェイスでは、セッションが非アクティブのまま一定期間（設定可能）が経過すると、ユーザをログアウトさせます。この場合、送信されていない設定データは保存されません。セッション アイドル タイムアウトの設定については、「セッション アイドル タイムアウトの設定」（P.16-13）を参照してください。

Web インターフェイスについて

ここでは、ACS Web インターフェイスについて説明します。

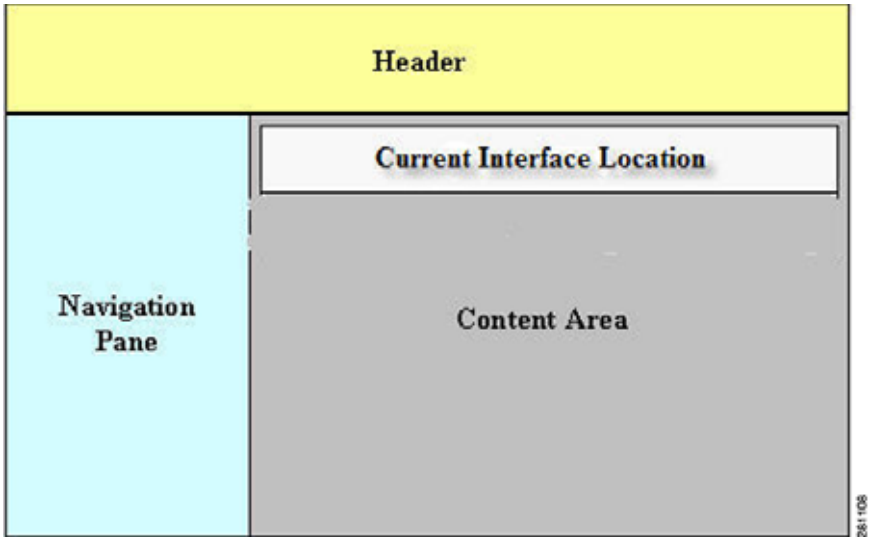
- 「Web インターフェイスのデザイン」（P.5-6）
- 「ヘッダー」（P.5-6）
- 「ナビゲーション ペイン」（P.5-7）

- 「コンテンツ領域」（P.5-8）

Web インターフェイスのデザイン

図 5-1 に、ACS Web インターフェイスの全体的なデザインを示します。

図 5-1　　ACS Web インターフェイス



インターフェイスには次の項目があります。

- 「ヘッダー」（P.5-6）
- 「ナビゲーション ペイン」（P.5-7）
- 「コンテンツ領域」（P.5-8）

ヘッダー

ヘッダーでは、次の操作を行います。

- 現在のユーザ（ユーザ名）の ID
- オンライン ヘルプへのアクセス
- ログアウト
- インストールされている ACS Web インターフェイスのバージョンに関する情報を調べることのできるバージョン情報へのアクセス

これらの項目は、ヘッダーの右側に表示されます（図 5-2 を参照）。

図 5-2　　ヘッダー

関連トピック

- 「ナビゲーション ペイン」（P.5-7）
- 「コンテンツ領域」（P.5-8）

ナビゲーション ペイン

ナビゲーション ペインは、Web インターフェイスのドロワをナビゲートする場合に使用します（図 5-3 を参照）。

図 5-3　　ナビゲーション ペイン

表 5-4 に、各ドロワの機能を示します。

表 5-4　　ナビゲーション ペインのドロワ

ドロワー	機能
My Workspace	タスク ガイドと、一般的なタスクへのショートカットおよび詳細情報へのリンクがある [Welcome] ページにアクセスします。詳細については、第 5 章「[My Workspace] の概要」を参照してください。
Network Resources	ネットワーク デバイス、AAA クライアント、およびネットワーク デバイス グループを設定します。詳細については、第 7 章「ネットワーク リソースの管理」を参照してください。
Users and Identity Stores	内部ユーザおよび ID ストアを設定します。詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。
Policy Elements	ポリシー条件および結果を設定します。詳細については、第 9 章「ポリシー要素の管理」を参照してください。
Access Policies	アクセス ポリシーを設定します。詳細については、第 10 章「アクセス ポリシーの管理」を参照してください。
Monitoring and Reports	ログ メッセージを表示します。詳細については、第 11 章「ACS での監視とレポート」を参照してください。
System Administration	ACS を管理および保守します。詳細については、第 16 章「システム管理者の管理」を参照してください。

ドロワを開くには、そのドロワをクリックします。そのドロワのオプションのリストが表示されます。一度に 1 つのドロワのコンテンツだけを表示できます。ドロワを開くと、それまで開いていたドロワが自動的に閉じます。

オプションをクリックして、項目の階層と現在の設定を表示したり、コンテンツ領域でそのオプションに関連付けられている設定タスクを実行したりします。コンテンツ領域の詳細については、「コンテンツ領域」（P.5-8）を参照してください。

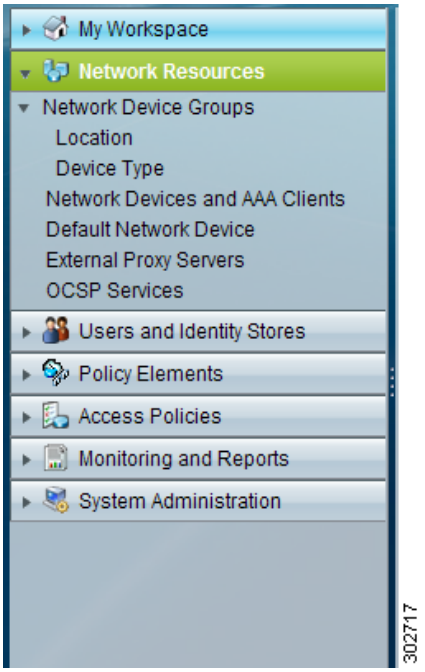
ナビゲーション ペインを非表示にしてコンテンツ領域を展開するには、ナビゲーション ペインとコンテンツ領域に間の縦方向の中央にある縮小矢印をクリックします。縮小矢印をもう一度クリックすると、ナビゲーション ペインが表示されます。

ナビゲーション ペインのドロワの下にリストされているオプションは、必要に応じてツリー構造に編成されています。ツリー構造内のオプションは動的であり、管理者のアクションに基づいて変化する場合があります。コンテンツ領域でオブジェクトを作成、削除、または名前変更すると、ナビゲーション ペインのオプションの表示が変化する場合があります。

たとえば、[Network Resources] > [Network Device Groups] オプションの下には、2 つの設定済みネットワーク デバイス グループ（オプション）である [Location] と [Device Type] があります。

図 5-4 に、管理者が [Network Device Groups] オプション ページを使用して Business というネットワーク デバイス グループを追加作成した場合に、このグループがナビゲーション ペインのツリー構造内に表示されることを示します。

図 5-4　　ナビゲーション ペイン：動的ツリー構造



関連トピック

- 「ヘッダー」（P.5-6）
- 「コンテンツ領域」（P.5-8）

コンテンツ領域

コンテンツ領域では、インターフェイス内での現在の場所の表示、設定の表示、AAA サービスの設定、および ACS の管理を行います。

コンテンツ領域には、次の項目があります。

- 「Web インターフェイスの場所」（P.5-9）
- 「リスト ページ」（P.5-9）

- 「セカンダリ ウィンドウ」（P.5-14）
- 「規則テーブル ページ」（P.5-17）

Web インターフェイスの場所

インターフェイス内での現在の場所が、コンテンツ領域の上部に表示されます。図 5-5 は、場所が [Policy Elements] ドロワの [Network Devices and AAA Clients] ページであることを示しています。

この場所を例として使用すると、ACS のドキュメントでは、[Policy Elements] > [Policy Conditions] > [Network Devices and AAA Clients] > [Location] という表記法を使用してインターフェイスの場所を示します。コンテンツ領域の残りの部分は、選択したページのコンテンツを示します。

また、インターフェイスの場所には、設定しているアクションも表示されます。たとえば、[Users and Identity Stores] > [Internal Identity Stores] > [Users] ページが表示されている状態で、特定のユーザを複製しようとする場合、インターフェイスの場所は次のようになります。

[Users and Identity Stores] > [Internal Identity Stores] > [Users] > [Duplicate: ***user_name***]。*user_name* は、複製の対象として選択したユーザの名前です。また、ACS のマニュアルでも、この表記法を使用します。

リスト ページ

リスト ページには、項目のリストがあります（図 5-5 を参照）。

リスト ページを使用して、ナビゲーション ペインで選択したオプションから 1 つ以上の項目を削除できます。

図 5-5　　リスト ページ

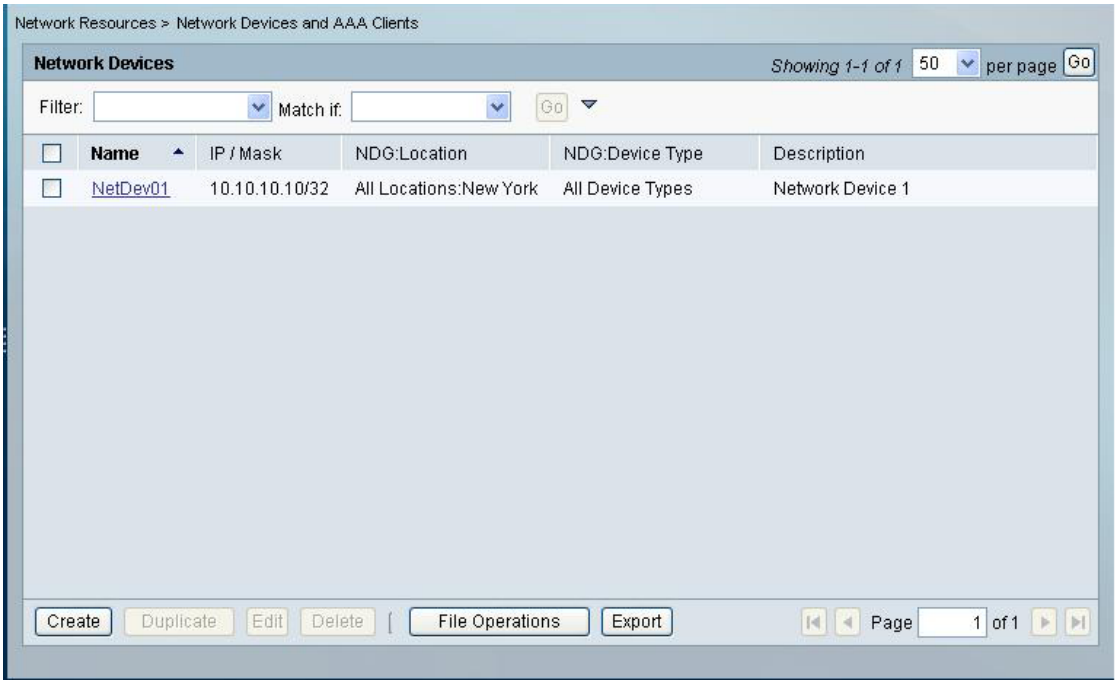


表 5-5 に、リスト ページに共通するコンテンツ領域のボタンとフィールドを示します。

表 5-5　リスト ページに共通するコンテンツ領域のボタンとフィールド

ボタンまたは フィールド	説明
Rows per page	ドロップダウン リストを使用して、このページに表示する項目数を指定します。オプション： • 10：最大 10 • 25：最大 25 • 50：最大 50 • 100：最大 100
Go	クリックすると、[Rows per page] フィールドで指定した項目数が表示されます。
チェックボックス またはオプション ボタン	編集、複製、または削除アクションを実行するリスト内の対象項目を選択または選択解除します。オプション： • オン（チェックボックス）またはクリック（オプション ボタン）：項目を選択します。 リスト内のすべての項目を選択するには、ヘッダー行のチェックボックスをオンにします。リスト内の特定の項目を選択するには、個々のチェックボックスをオンにします。 • オフ（チェックボックス）またはアンクリック（オプション ボタン）：項目を選択しません。
リスト カラム	特定の設定タスクに関連付けられている項目の表形式または階層形式での表示。図 5-5 では、設定したネットワーク デバイス名のリストとしてのリスト カラムを示しています。このリスト カラムの見出しは [Name] です。
スクロール バー	コンテンツ領域のスクロール バーを使用して、必要に応じてページ内のすべてのデータを表示します。
Create	新しい項目を作成する場合にクリックします。ウィザードまたは単一ページがコンテンツ領域に表示されます。 [Create] をクリックすると、コンテンツ領域で行った選択が無視され、コンテンツ領域には、ページ固有のデフォルト値（存在する場合）を示す [Edit] ページが表示されます。
Duplicate	選択した項目を複製する場合にクリックします。単一ページまたはタブ付きページがコンテンツ領域に表示されます。
Edit	選択した項目を編集する場合にクリックします。単一ページまたはタブ付きページがコンテンツ領域に表示されます。

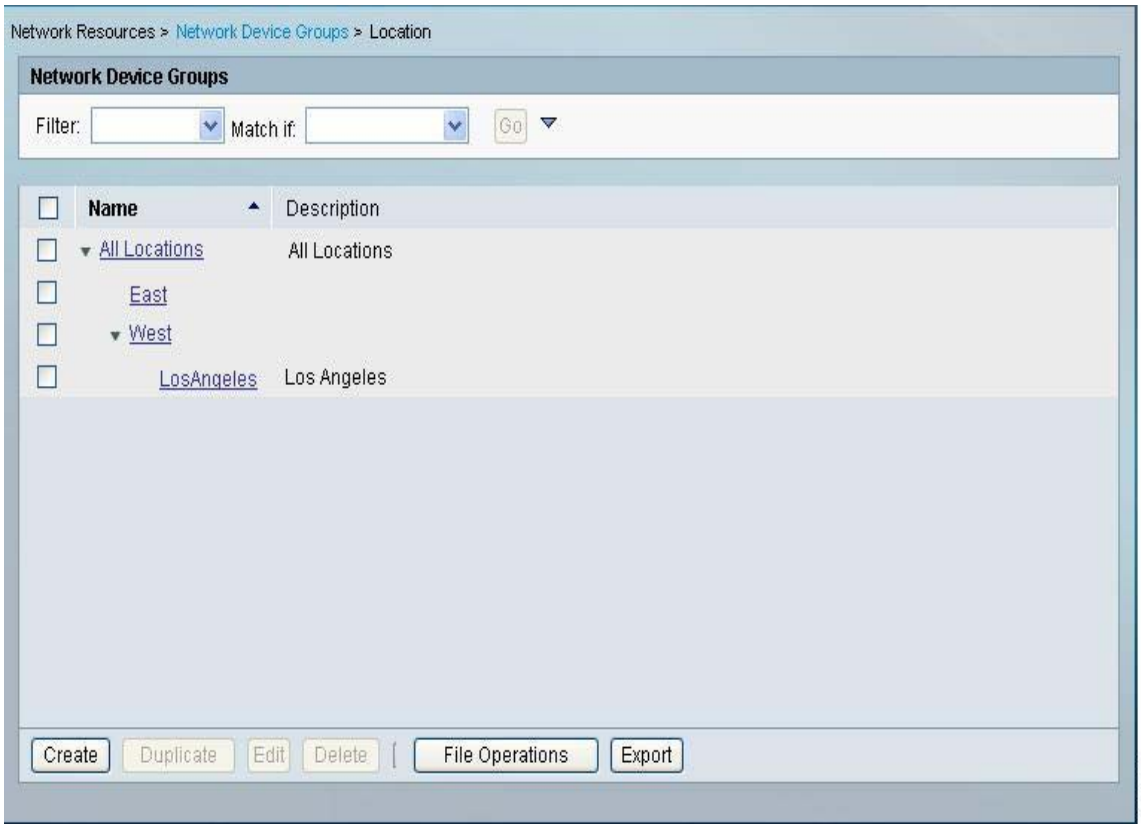
表 5-5　リスト ページに共通するコンテンツ領域のボタンとフィールド （続き）

ボタンまたは フィールド	説明
Delete	選択した 1 つ以上の項目を削除する場合にクリックします。削除することを選択した項目について、Are you sure you want to delete item/items? という問い合わせメッセージを示すダイアログボックスが 表示されます。確認ダイアログボックスには、[OK] と [Cancel] があります。次のいずれかをクリックします。 • [OK]：選択した項目が削除されます。リスト ページが表示されます。このとき、削除された項目は表示されません。 • [Cancel]：削除操作が取り消されます。変更のないリスト ページが表示されます。 スクロール バーを使用して表示できるページのコンテンツを含め、ページで参照できる項目だけを削除できます。 複数のページにまたがるテーブルの場合、参照できないページで選択した行の削除は無視され、選択した行は削除されません。
Page *num* of n	リスト ページのコンテンツ領域に表示するページ番号（*num* は表示するページ）を入力し、[Go] をクリックします。 ツリー テーブル ページには使用できません。
方向矢印	コンテンツ領域の右下にある矢印は、最初のページ、前のページ、次のページ、または最後のページにアクセスする場合にクリックします。矢印は必要に応じてアクティブになります。 ツリー テーブル ページには使用できません。

ツリー テーブル ページは、リスト ページのバリエーションです（図 5-6 を参照）。ページ移動を除き、リスト ページで実行できるのと同じ操作をツリー テーブル ページで実行できます。また、ツリー テーブル ページには次の特徴があります。

- 行の背景色が濃い場合は、ツリーの最上位レベルであることを示す。
- ツリーの最初のフォルダに含まれている項目が 50 個未満の場合は、最初のフォルダが展開され、他のすべてのフォルダが縮小される。縮小されたフォルダの内容を表示するには、展開アイコン（+）を使用してください。
- ツリーの最初のフォルダに含まれている項目が 50 個以上の場合は、ツリーのすべてのフォルダが縮小される。フォルダの内容を表示するには、展開アイコン（+）をクリックしてください。
- フォルダ（親）のチェックボックスをオンにした場合は、そのフォルダのすべての子が選択される。
- フォルダ（親）のチェックボックスをオンにしてから、いずれかの子をオフにすると、親フォルダが自動的にオフになる。

図 5-6　ツリー テーブル ページ



フィルタリング

コンテンツ領域ウィンドウまたはセカンダリ ウィンドウ（図 5-9 を参照）のリストが大きいと、ナビゲートして目的のデータを選択することが難しくなる場合があります。Web インターフェイスを使用してこれらのウィンドウのデータをフィルタリングし、選択した基準と条件に基づいて、リストに表示されるデータを削減できます。表 5-6 に、フィルタリング オプションを示します。

（注）　すべてのフィールドですべてのフィルタリング オプションを使用できるとはかぎりません。

表 5-6　コンテンツ領域ウィンドウとセカンダリ ウィンドウのフィルタリング

ボタンまたはフィールド	説明
Filter（ドロップダウン リスト ボックス）	フィルタリングするカラムの名前をドロップダウン リスト ボックスから選択します。
Match if（ドロップダウン リスト ボックス）	フィルタ処理に適用する条件を選択します。 • Contains • Doesn't Contain • Ends With • Equals • Is Empty • Not Empty • Not Equals • Starts With 条件は、[Filter] ドロップダウン リスト ボックスで選択したカラムに適用されます。
v（下矢印）	条件を選択してフィルタ処理を絞り込むまたは拡張するフィルタ行を追加する場合にクリックします。追加のフィルタ行の前に `And:` というテキストが表示されます。
^（上矢印）	無関係のフィルタ行を削除する場合にクリックします。
Go	フィルタ処理を実行する場合にクリックします。
Clear Filter	現在のフィルタ オプションをクリアする場合にクリックします。
OK	選択したデータを設定に追加し、セカンダリ ウィンドウを閉じる場合にクリックします。 このボタンは、セカンダリ ウィンドウでだけ使用できます（図 5-9 を参照）。

（注）　ツリー テーブル ページでは、最上位の親であるルート ノードでだけフィルタリングを実行できます。

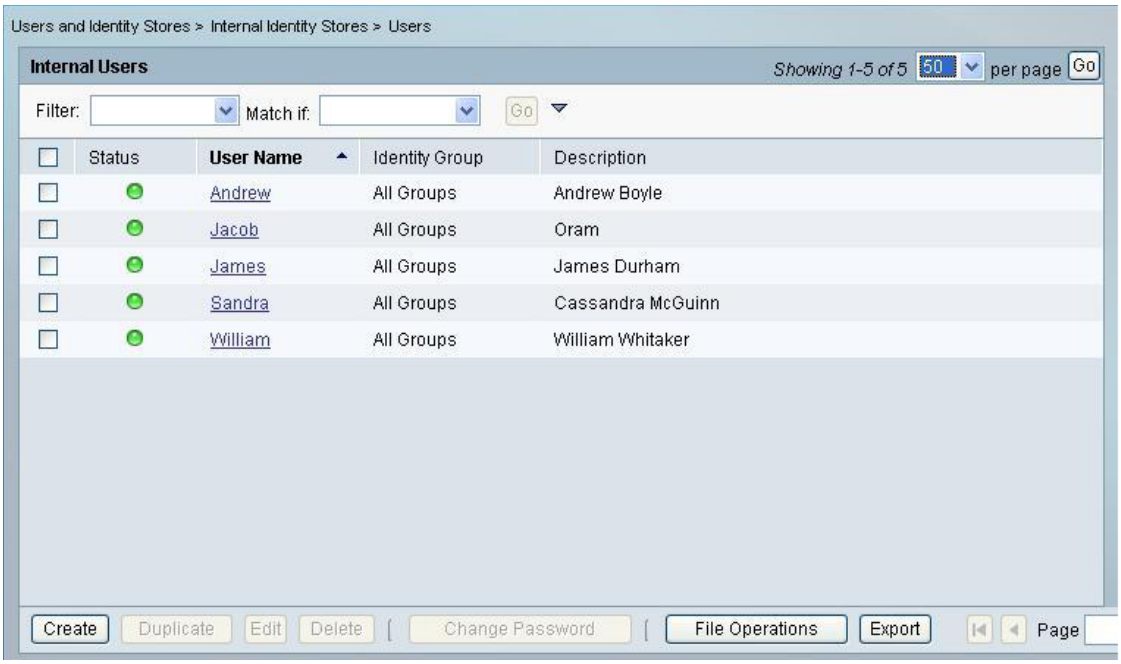
ソート

ほとんどの非ツリー リスト ページでは、[Name] カラムまたは [Description] カラムでのソートがサポートされています（使用可能な場合）。ページを昇順または降順にソートできます。

[Name] または [Description] カラムのないページでは、ソート メカニズムはページの一番左のカラムまたは [Description] カラムでサポートされる場合があります。そのカラムでソートできるかどうかを判断するには、カラム見出しの上にカーソルを置きます。ソートできる場合は、カーソルが手の形に変わり、`Click to sort` というテキストが表示されます。

テーブルがソートされると、カラム見出しのテキストが強調表示され、上矢印または下矢印がテキストの横に表示されます（図 5-7 を参照）。矢印をクリックすると、逆方向に再ソートされます。

図 5-7　ソートの例



セカンダリ ウィンドウ

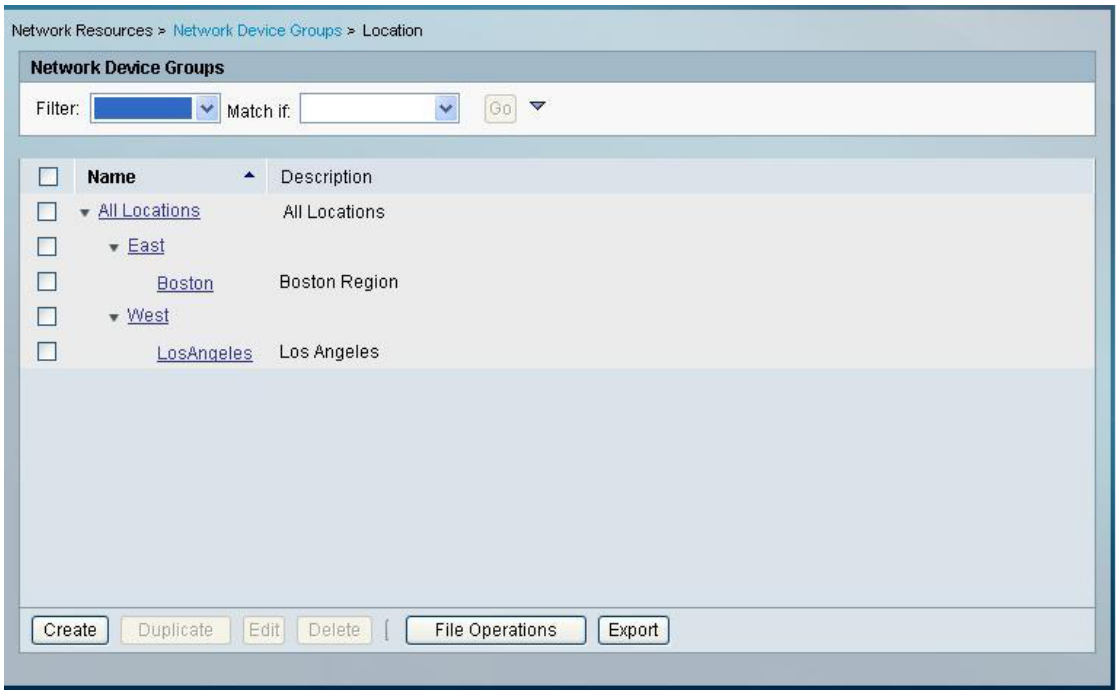
コンテンツ領域は、単一ページ、タブ付きページ、またはウィザード ページから [Select]（図 5-8 を参照）をクリックしてアクセスするセカンダリ（ポップアップ）ウィンドウの起動場所として機能します。これらのセカンダリ ウィンドウを使用して、設定で使用するデータをフィルタリングおよび選択します（図 5-9 および表 5-6 を参照）。

選択オプションに応じて、セカンダリ ウィンドウから 1 つ以上の項目を選択して設定に含めることができます。

セカンダリ ウィンドウにオプション ボタンとともに表示される項目では、設定に含める 1 つの項目を選択でき、チェックボックスとともに表示される項目では、複数の項目を選択できます。

図 5-8　[Select] ボタン：セカンダリ ウィンドウへのアクセス

図 5-9　セカンダリ ウィンドウ



データの選択とフィルタリングに加えて、セカンダリ ウィンドウ内で選択可能なオブジェクトを作成できます。

たとえば、ユーザの内部 ID ストアを作成し、[Select] をクリックしてストアを ID グループ（選択可能オブジェクト）に割り当てようとしたときに、関連付ける ID グループが使用可能でない場合は、セカンダリ ウィンドウの [Create] をクリックして目的のオブジェクトを作成できます。

オブジェクトを作成し、[Submit] をクリックすると、セカンダリ ウィンドウが更新されて新規に作成したオブジェクトが表示されるため、そのオブジェクトを設定に対して選択できます。ここで示す例では、新規に作成した ID グループを選択して、ユーザの内部 ID ストアに割り当てることができます。

転送ボックス

転送ボックスは、コンテンツ領域ページの共通要素です（図 5-10 を参照）。これらのボックスを使用して、設定で使用する項目を選択および削除したり、ニーズに合せて並べ替えたりします。図 5-10 に、転送ボックスのオプションを示します。表 5-7 に、転送ボックスのオプションを示します。

図 5-10　転送ボックス

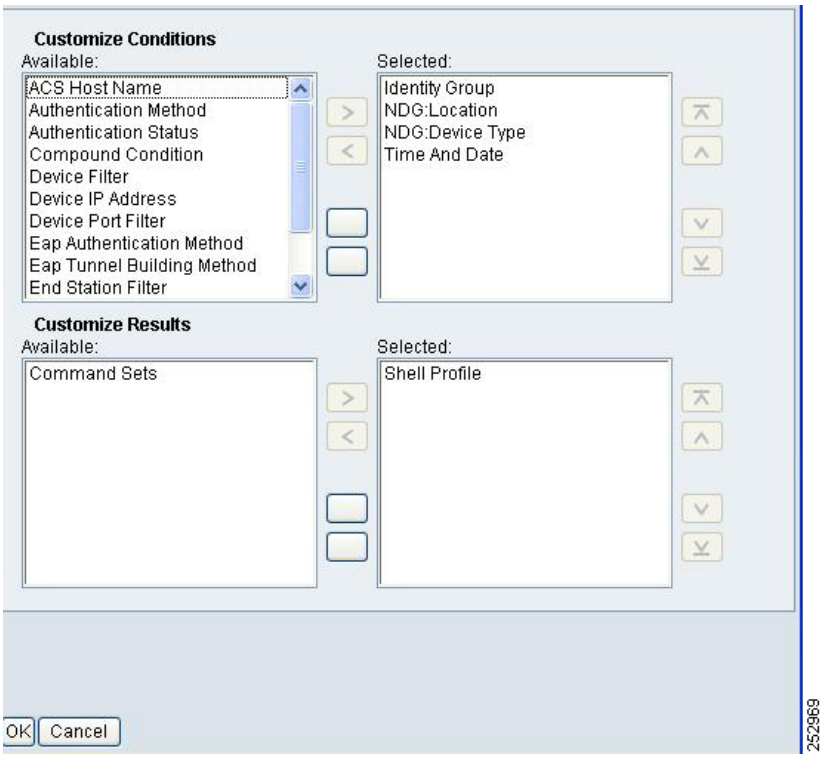


表 5-7　転送ボックスのフィールドとボタン

フィールドまたはボタン	説明
Available	選択できる項目のリスト。
Selected	選択した項目の順序付きリスト。
右矢印（>）	選択した 1 つの項目を [Available] リストから [Selected] リストに移動します。
左矢印（<）	選択した 1 つの項目を [Selected] リストから [Available] リストに移動します。
二重右矢印（>>）	すべての項目を [Available] リストから [Selected] リストに移動します。
二重左矢印（<<）	すべての項目を [Selected] リストから [Available] リストに移動します。
上線が付いた上矢印	選択した 1 つの項目を順序付き [Selected] 項目リストの一番上に移動します。
上矢印	選択した 1 つの項目を順序付き [Selected] 項目リストの 1 つ上の位置に移動します。
下矢印	選択した 1 つの項目を順序付き [Selected] 項目リストの 1 つ下の位置に移動します。
下線が付いた下矢印	選択した 1 つの項目を順序付き [Selected] 項目リストの一番下に移動します。

スケジュール ボックス

スケジュール ボックスは、コンテンツ領域ページの共通要素です（図 5-10 を参照）。スケジュール ボックスを使用して、グリッドからポリシー要素のアクティブ時間を選択します。各行は曜日を表し、行の各四角は時間を表します。

1 時間アクティブにするには、四角を 1 つクリックします。表 5-8 に、スケジュール ボックスのオプションを示します。

図 5-11　　スケジュール ボックス

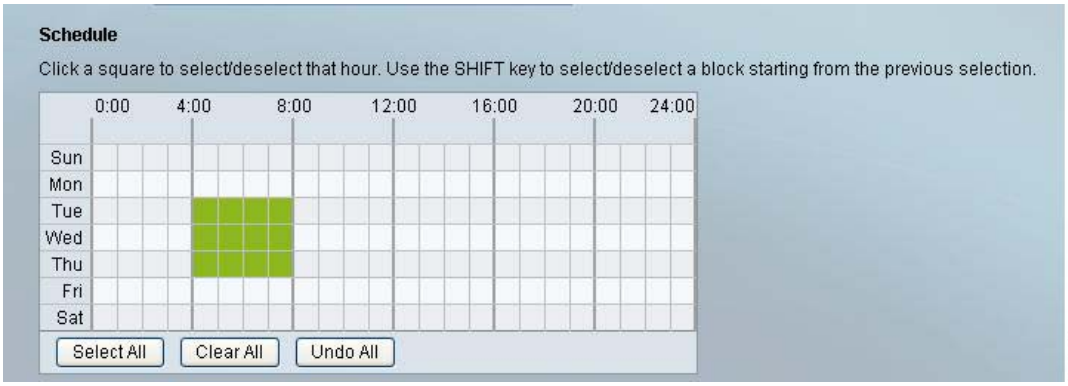


表 5-8　　スケジュール ボックスのフィールドとボタン

フィールドまたはボタン	説明
Mon	各年の各週の月曜日を示す行。
Tue	各年の各週の火曜日を示す行。
Wed	各年の各週の水曜日を示す行。
Thu	各年の各週の木曜日を示す行。
Fri	各年の各週の金曜日を示す行。
Sat	各年の各週の土曜日を示す行。
Sun	各年の各週の日曜日を示す行。
0:00 ～ 24:00	カラム内の時間を示します。0:00 は東部標準時（EST）の深夜 0 時の 1 秒後に開始する時間、24:00 は ACS インスタンスが位置するタイム ゾーンの深夜 0 時から午前 1:00 までです。
（グリッドの）四角	1 時間アクティブにするには、四角を 1 つクリックします。
Set All	すべての四角（時間）を選択します。
Clear All	すべての四角（時間）を選択解除します。
Undo All	最新の選択内容を取り消します。

規則テーブル ページ

規則テーブル ページには、ポリシーを構成する規則が表示されます。規則テーブル ページ内で規則を並べ替えたり、テーブルに関連付けられているポリシーを送信したりできます。規則テーブルからプロパティおよびカスタマイゼーション ページにアクセスして、ポリシーを設定できます。

特定の規則テーブル ページの詳細と、プロパティおよびカスタマイゼーション ページについては、「「アクセス ポリシーの管理」」を参照してください。

規則テーブルのすぐ上には、2 つの表示オプションがあります。

- Standard Policy：標準のポリシー規則テーブルを表示する場合にクリックします。
- Exception Policy：標準のポリシー規則テーブルのコンテンツよりも優先される例外ポリシー規則テーブルを表示する場合にクリックします。

表 5-9 に、標準および例外規則テーブル ページの共通オプションを示します。

表 5-9　規則テーブル ページのオプション

オプション	説明
#	規則テーブル内の規則の順序付きカラム。規則を並べ替え、追加、または削除してから [Save Changes] をクリックして再番号付けを完了することにより、規則の番号を付け直すことができます。 新しい規則は順序付きカラムの最後に追加されるため、新しい規則を順序付きリスト内の別の位置に移動する場合は、並べ替える必要があります。 デフォルト（catch-all）規則を並べ替えることはできません。この規則は規則テーブルの一番下に残ります。
Check box	1 つ以上のチェックボックスをオンにして、処理の実行対象の関連付けられた規則を選択します。
Status	（*表示のみ*）規則テーブル内の規則のステータスを示します。次のステータスがあります。 • イネーブル：白いチェック マークの付いた緑色（または明るい色）の丸で示されます。 • ディセーブル：白い x の付いた赤色（または濃い色の丸）で示されます。 • 監視のみ：黒い i の付いたグレーの丸で示されます。
Name	各規則の固有の名前（デフォルトの catch-all 規則以外）。関連付けられた規則を編集するには名前をクリックします。新しい規則を追加すると、その規則には `Rule-num` という形式の名前が付きます。*num* は、次に使用可能な連続する整数です。 名前を編集して、より説明的な名前にすることができます。規則には、規則名にサービス名およびポリシー名を連結した名前を付けることを推奨します。
Conditions	可変数の条件タイプがリストされます。ポリシー タイプによってはサブカラムに表示される場合があります。
Results	可変数の結果タイプがリストされます。ポリシー タイプによってはサブカラムに表示される場合があります。
[Hit Counts] カラム	規則のヒット数を表示します。ヒットは、どのポリシー規則が呼び出されたかを示します。
規則のスクロール バー	規則行の右にあるスクロール バーでは、規則リストを上下にスクロールします。
条件および結果のスクロール バー	[Conditions] および [Results] カラムの下にあるスクロール バーでは、条件および結果情報を左右にスクロールします。
Default rule	catch-all 規則を設定する場合にクリックします。このオプションは、例外ポリシー規則テーブルでは使用できません。
Customize	規則テーブルで使用される条件と結果のセットおよび順序を判断できるセカンダリ ウィンドウを開きます。
[Hit Counts] ボタン	次の操作を実行できるセカンダリ ウィンドウを開きます。 • ヒット カウンタが最後にリセットまたは更新されたのはいつかの表示 • 収集期間の表示 • ヒット数のリセットまたは更新の要求 詳細については、「ヒット カウントの表示」（P.10-9）を参照してください。
Move to...	[^] および [v] ボタンを使用して、規則テーブル内で選択した規則を並べ替えます。

表 5-9　規則テーブル ページのオプション （続き）

オプション	説明
Save Changes	設定変更を送信します。
Discard Changes	設定変更を保存する前に廃棄します。

関連項目

- 「ACS 5.x ポリシー モデル」

Web インターフェイスを使用した ACS オブジェクトのインポートおよびエクスポート

ACS のインポート機能を使用して、複数の ACS オブジェクトを同時に追加、更新、または削除できます。ACS では、カンマ区切り形式（CSV）ファイルを使用して、これらの一括操作を実行します。この *.csv* ファイルをインポート ファイルと呼びます。ACS には、各 ACS オブジェクトの追加、更新、および削除操作用に、個別の *.csv* テンプレートが備えられています。

.csv ファイル内の最初のレコードは、カラム（フィールド）名を含むテンプレートのヘッダー レコードです。これらのテンプレートは ACS Web インターフェイスからダウンロードする必要があります。テンプレートのヘッダー レコードは、インポートする .csv ファイルの最初の行に含まれている必要があります。

（注） すべての ACS オブジェクトをインポートするのに同じテンプレートは使用できません。各 ACS オブジェクト用に設計されたテンプレートをダウンロードし、対応するテンプレートをオブジェクトのインポート時に使用する必要があります。ただし、特定のオブジェクトのエクスポート ファイルを使用し、ヘッダーを保持してデータを更新し、それを同じオブジェクトのインポート ファイルとして使用することはできます。

エクスポート機能を使用して、ACS 内部ストアで使用可能な特定のオブジェクト タイプのすべてのレコードを含む *.csv* ファイルを作成できます。

インポートおよびエクスポート操作を実行するには、CLI 管理者レベル アクセス権が必要です。さらに、次の権限が必要です。

- ACS 設定データをインポートする場合は、特定の設定オブジェクトに対する CRUD 権限
- リモート リポジトリにデータをエクスポートする場合は、特定の設定オブジェクトに対する読み取り権限

この機能は、すべての ACS オブジェクトで使用可能であるとはかぎりません。ここでは、サポートされる ACS オブジェクトと、インポート ファイルの作成方法について説明します。

この項の構成は、次のとおりです。

- 「サポートされる ACS オブジェクト」（P.5-20）
- 「インポート ファイルの作成」（P.5-22）

サポートされる ACS オブジェクト

ACS 5.4 では、インポート機能を使用して ACS オブジェクトに対する一括操作（追加、更新、削除）を実行できますが、すべての ACS オブジェクトをインポートできるわけではありません。ACS 5.4 のインポート機能では、次の ACS オブジェクトがサポートされています。

- ユーザ
- ホスト
- ネットワーク デバイス
- ID グループ
- NDG
- ダウンロード可能 ACL
- コマンド セット

表 5-10 に、ACS オブジェクト、そのプロパティ、およびプロパティのデータ型をリストします。各オブジェクトのインポート テンプレートには、この表で説明されているプロパティが含まれています。

（注）　表 5-10 に記載されている制限は、内部データベース内のユーザにのみ適用され、外部データベース（AD、LDAP、または RSA）のユーザには適用されません。

表 5-10　ACS オブジェクト：プロパティ名とデータ型

プロパティ名	プロパティのデータ型
オブジェクト タイプ：ユーザ	
Username	（作成、編集、および削除で必須）文字列。最大長は 64 文字です。
Description	（任意）文字列。最大長は 1024 文字です。
Enabled	（作成で必須）ブール。
Change Password	（作成で必須）ブール。
Password	（作成で必須）文字列。最大 32 文字まで可能です。エクスポートでは使用できません。
Enable Password	（任意）文字列。最大 32 文字まで可能です。
Password Type	（作成で必須）文字列。最大長は 256 文字です。
User Identity Group	（任意）文字列。最大長は 256 文字です。
List of attributes	（任意）文字列およびその他のデータ型。
オブジェクト タイプ：ホスト	
MAC address	（作成、編集、削除で必須）文字列。最大長は 64 文字です。
Description	（任意）文字列。最大長は 1024 文字です。
Enabled	（任意）ブール。
Host Identity Group	（任意）文字列。最大長は 256 文字です。
List of attributes	（任意）文字列。
オブジェクト タイプ：ネットワーク デバイス	
Name	（作成、編集、削除で必須）文字列。最大長は 64 文字です。
Description	（任意）文字列。最大長は 1024 文字です。

表 5-10　ACS オブジェクト：プロパティ名とデータ型 （続き）

プロパティ名	プロパティのデータ型
Subnet	（作成で必須）サブネット IPv4：a.b.c.d/32 を除く <a.b.c.d>/m、ワイルドカード（*、-）。 IPv6：<a:b:c:d:e:f:g:h>/n、ワイルドカード（:、::）。 除外範囲は IPv4 アドレスだけに適用されます。
Support RADIUS	（作成で必須）ブール。
RADIUS secret	（任意）文字列。最大 32 文字まで可能です。
coaPort	（任意）整数。
SupportKeyWrap	（任意）ブール。
KeywrapKEK	（任意）文字列。最大 32 文字まで可能です。
KeywrapMACK	（任意）文字列。最大長は 40 文字です。
KeywrapDisplayInHex	（任意）ブール。
Support TACACS	（作成で必須）ブール。
TACACS secret	（任意）文字列。最大 32 文字まで可能です。
Single connect	（任意）ブール。
Legacy TACACS	（任意）ブール。
Support SGA	（作成で必須）ブール。
SGA Identity	（任意）文字列。最大 32 文字まで可能です。
SGA trusted	（任意）ブール。
Password	（任意）文字列。最大 32 文字まで可能です。
sgACLTTL	（任意）整数。
peerAZNTTL	（任意）整数。
envDataTTL	（任意）整数。
Session timeout	（任意）整数。
List of NDG names	（任意）文字列。
Location	（任意）文字列。最大 32 文字まで可能です。
Device Type	（任意）文字列。最大 32 文字まで可能です。
オブジェクト タイプ：ID グループ	
Name	（作成、編集、削除で必須）文字列。最大長は 64 文字です。
Description	（任意）文字列。最大長は 1024 文字です。
オブジェクト タイプ：NDG	
Name	（作成、編集、削除で必須）文字列。最大長は 64 文字です。
Description	（任意）文字列。最大長は 1024 文字です。
オブジェクト タイプ：ダウンロード可能 ACL	
Name	（作成、編集、削除で必須）文字列。最大長は 64 文字です。
Description	（任意）文字列。最大長は 1024 文字です。
Content	（作成、編集、削除で必須）文字列。ACL コンテンツはセミコロン（;）で区切られた許可 / 拒否ステートメントに分割されます。各ステートメントの最大長は 256 文字です。ACL コンテンツに制限はありません。

表 5-10　ACS オブジェクト：プロパティ名とデータ型 （続き）

プロパティ名	プロパティのデータ型
オブジェクト タイプ：コマンド セット	
Name	（作成、編集、削除で必須）文字列。最大長は 64 文字です。
Description	（任意）文字列。最大長は 1024 文字です。
Commands（*grant*:*command*:*arguments* の形式）	（任意）文字列。 これは、*grant* に対して指定する値のリストです。複数の値をセパレータ（:）で区切る形式となります。

任意指定のフィールドは、空のままにすると、ACS によってそれぞれのフィールドのデフォルト値に置換されます。

たとえば、階層に関連するフィールドを空白のままにすると、ACS によって、階層のルート ノードの値が割り当てられます。ネットワーク デバイスでは、Security Group Access がイネーブルの場合、すべての関連設定フィールドがデフォルト値に設定されます。

インポート ファイルの作成

ここでは、ACS オブジェクトに対して一括操作を実行するための *.csv* ファイルの作成方法について説明します。ACS Web インターフェイスから、各オブジェクトに適したテンプレートをダウンロードできます。この項の構成は、次のとおりです。

- 「Web インターフェイスからのテンプレートのダウンロード」（P.5-22）
- 「CSV テンプレートについて」（P.5-23）
- 「インポート ファイルの作成」（P.5-24）

Web インターフェイスからのテンプレートのダウンロード

インポート ファイルを作成する前に、ACS Web インターフェイスからインポート ファイル テンプレートをダウンロードする必要があります。

内部ユーザを追加するためにインポート ファイル テンプレートをダウンロードするには、次の手順を実行します。

ステップ 1　ACS 5.4 Web インターフェイスにログインします。

ステップ 2　[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択します。

[Users] ページが表示されます。

ステップ 3　[File Operations] をクリックします。

File Operations wizard が表示されます。

ステップ 4　次のいずれか 1 つを選択します。

- Add：既存のリストにユーザを追加します。このオプションでは、既存のリストは修正されません。代わりに、追加操作を実行します。
- Update：既存の内部ユーザ リストを更新します。
- Delete：内部 ID ストアから、インポート ファイル内のユーザのリストを削除します。

ステップ 5　[Next] をクリックします。

[Template] ページが表示されます。

ステップ 6　[Download Add Template] をクリックします。

ステップ 7　[Save] をクリックして、テンプレートをローカル ディスクに保存します。

次のリストに、各オブジェクトに適したテンプレートを取得できる場所を示します。

- ユーザ：[Users and Identity Stores] > [Internal Identity Stores] > [Users]
- ホスト：[Users and Identity Stores] > [Internal Identity Stores] > [Hosts]
- ネットワーク デバイス：[Network Resources] > [Network Devices and AAA Clients]
- ID グループ：[Users and Identity Stores] > [Identity Groups]
- NDG
  - 場所：[Network Resources] > [Network Device Groups] > [Location]
  - デバイス タイプ：[Network Resources] > [Network Device Groups] > [Device Type]
- ダウンロード可能 ACL：[Policy Elements] > [Authorization and Permissions] > [Named Permission Objects] > [Downloadable ACLs]
- コマンド セット：[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Command Sets]

ここで説明する手順に従って、オブジェクトに適したテンプレートをダウンロードします。

CSV テンプレートについて

Microsoft Excel またはその他のスプレッドシート アプリケーションで CSV テンプレートを開き、テンプレートをローカル ディスクに *.csv* ファイルとして保存できます。*.csv* テンプレートには、対応する ACS オブジェクトのプロパティをリストするヘッダー行があります。

たとえば、internal user Add テンプレートには、表 5-11 で説明するフィールドがあります。

表 5-11　internal user Add テンプレート

ヘッダー フィールド	説明
name:String(64):Required	ユーザのユーザ名
description:String(1024)	ユーザの説明
enabled:Boolean (True,False):Required	ユーザをイネーブルにする必要があるか、またはディセーブルにする必要があるかを示すブール フィールド
changePassword:Boolean (True,False):Required	ユーザが最初にログインするときにパスワードを変更する必要があるかどうかを示すブール フィールド
password:String(32):Required	ユーザのパスワード
enablePassword:String(32)	ユーザのイネーブル パスワード
UserIdentityGroup:String(256)	ユーザが属する ID グループ
指定したすべてのユーザ属性はここに表示されます。	

.csv ファイルの各行は、1 つの内部ユーザ レコードに対応します。ユーザを ACS にインポートする前に、値を *.csv* ファイルに入力し、保存する必要があります。インポート ファイルの作成方法の詳細については、「インポート ファイルの作成」（P.5-24）を参照してください。

この例は、internal user Add テンプレートに基づいています。その他の ACS オブジェクト テンプレートは、ヘッダー行に、そのオブジェクトについて表 5-10 で説明されているプロパティが含まれています。

インポート ファイルの作成

ローカル ディスクにインポート ファイル テンプレートをダウンロードしたあとで、ACS にインポートするレコードを、テンプレートで指定されている形式で入力します。すべてのレコードを *.csv* ファイルに入力したあとで、インポート機能に進むことができます。インポート プロセスには次の処理が関係します。

- 「ACS 内部ストアへのレコードの追加」（P.5-24）
- 「ACS 内部ストア内のレコードの更新」（P.5-24）
- 「ACS 内部ストアからのレコードの削除」（P.5-26）

ACS 内部ストアへのレコードの追加

ACS 内部ストアにレコードを追加する場合は、レコードを既存のリストに追加します。これは追加操作であり、*.csv* ファイル内のレコードは、ACS に存在するリストに追加されます。

内部ユーザ レコードを追加テンプレートに追加するには、次の手順を実行します。

ステップ 1　internal user Add テンプレートをダウンロードします。詳細については、「Web インターフェイスからのテンプレートのダウンロード」（P.5-22）を参照してください。

ステップ 2　internal user Add テンプレートを、Microsoft Excel またはその他のスプレッドシート アプリケーションで開きます。テンプレートのヘッダー行のフィールドの説明については、表 5-10 を参照してください。

ステップ 3　内部ユーザ情報を入力します。.csv テンプレートの各行は、1 つのユーザ レコードに対応します。

図 5-12 に、サンプルの add users インポート ファイルを示します。

図 5-12　add users：インポート ファイル

	A	B	C	D	E	F	G	H	I	J	K
1	name:String(64):Re	description:Str	enabled:	changePassw	password:Stri	enablePasswo	UserIdentityGroup:Sti	attr-Real Name	attr-Description:String(256)		
2	John		TRUE	FALSE	1234		All Groups:SanJose				
3	Kenneth		TRUE	FALSE	1235		All Groups:SanJose				
4	Abraham		TRUE	FALSE	1236		All Groups:Texas				
5	Kelly		TRUE	FALSE	1237		All Groups:Texas				
6	Sandra		TRUE	FALSE	1238		All Groups:Florida				
7	Nilofer		TRUE	FALSE	1239		All Groups:Florida				
8	James		TRUE	FALSE	1240		All Groups:SanJose				
9	Albert		TRUE	FALSE	1241		All Groups:Florida				
10	Kevin		TRUE	FALSE	1242		All Groups:Florida				
11	Samantha		TRUE	FALSE	1243		All Groups:Texas				

252953

ステップ 4　add users インポート ファイルをローカル ディスクに保存します。

ACS 内部ストア内のレコードの更新

ACS ストア内のレコードを更新すると、インポート プロセスによって、内部ストアの既存のレコードが *.csv* ファイルのレコードで上書きされます。この操作では、ACS に存在するレコードが *.csv* ファイルのレコードで置換されます。

更新操作は、更新テンプレートに追加できる 1 つの追加カラムを除き、追加操作と同様です。更新テンプレートには、内部ユーザおよびその他の ACS オブジェクトの [Updated name] カラムと、内部ホストの [Updated MAC address] カラムが含まれる場合があります。名前が [Updated Name] で置換されます。

ワンポイントアドバイス

各 ACS オブジェクトの更新テンプレートをダウンロードする代わりに、そのオブジェクトのエクスポート ファイルを使用して、ヘッダー行を保持し、データを更新して更新 .csv ファイルを作成できます。

更新された名前または MAC アドレスを ACS オブジェクトに追加するには、特定の更新テンプレートをダウンロードして使用する必要があります。また、NDG の場合、エクスポート テンプレートには NDG 名だけが含まれているため、他のプロパティを更新するには、NDG 更新テンプレートをダウンロードして使用してください。

例として、図 5-13 に、既存のユーザ レコードを更新するサンプル インポート ファイルを示します。

図 5-13　ユーザの更新：インポート ファイル

	A	B	C	D	E	F	G	H	I	J	K	L
1	name:Strir	Updated name:Strir	description	enabled:Bo	changePas	password:S	enablePas	UserIdentit	attr-Real N	attr-Description:String(256)		
2	John	Mark		TRUE	FALSE	1234		All Groups:SanJose				
3	Kenneth	David		TRUE	FALSE	1235		All Groups:SanJose				
4	Abraham	Jamie		TRUE	FALSE	1236		All Groups:Texas				
5	Kelly	Lucy		TRUE	FALSE	1237		All Groups:Texas				
6	Sandra	Tina		TRUE	FALSE	1238		All Groups:Florida				
7	Nilofer	William		TRUE	FALSE	1239		All Groups:Florida				
8	James	Frank		TRUE	FALSE	1240		All Groups:SanJose				
9	Albert	George		TRUE	FALSE	1241		All Groups:Florida				
10	Kevin	Paul		TRUE	FALSE	1242		All Groups:Florida				
11	Samantha	Patrick		TRUE	FALSE	abcd		All Groups:Texas				

252971

（注）　2 番めのカラムの [Updated name] は、更新テンプレートに追加できる追加のカラムです。

ACS 内部ストアからのレコードの削除

このオプションを使用して、ACS 内部ストアからレコードのサブセットを削除できます。インポートする *.csv* ファイルに存在するレコードは、ACS 内部ストアから削除されます。削除テンプレートには、削除する必要のあるレコードを識別するキー カラムだけが含まれます。

たとえば、内部ユーザのセットを ACS 内部 ID ストアから削除するには、内部ユーザの削除テンプレートをダウンロードし、削除するユーザのリストをこのインポート ファイルに追加します。図 5-14 に、内部ユーザ レコードを削除するサンプル インポート ファイルを示します。

ワンポイントアドバイス　すべてのユーザを削除するには、すべてのユーザをエクスポートし、同じエクスポート ファイルを、ユーザを削除するためのインポート ファイルとして使用できます。

図 5-14　ユーザの削除：インポート ファイル

	A	B	C	D	E	F
1	name:String(64):Required					
2	kenneth					
3	jamie					
4	john					
5	joseph					
6	nilofer					
7	casey					
8	lucie					
9	jacob					
10	george					

252956

一般的なエラー

次の一般的なエラーが発生することがあります。

- 「同時実行競合エラー」（P.5-27）
- 「削除エラー」（P.5-28）
- 「システム障害エラー」（P.5-30）
- 「アクセシビリティ」（P.5-30）

同時実行競合エラー

同時実行競合エラーは、複数のユーザが同じオブジェクトを更新しようとした場合に発生します。[Submit] をクリックしたときに Web インターフェイスがエラーを検出すると、エラー メッセージと [OK] ボタンのあるダイアログボックスが表示されます。エラー メッセージを確認し、[OK] をクリックして、必要に応じて設定を再送信します。

発生する可能性があるエラー メッセージ、説明、および推奨処置は、次のとおりです。

エラー メッセージ　`The item you are trying to Submit has been modified elsewhere while you were making your changes.`

説明　編集を実行して設定を開始するために項目にアクセスしました。同時に別のユーザがアクセスし、修正を正常に送信しました。送信試行は失敗しました。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、コンテンツ領域リスト ページを表示します。このページには、すべての項目の最新バージョンが表示されています。必要に応じて設定を再送信します。

エラー メッセージ　`The item you are trying to Submit has been deleted while you were making your changes.`

説明　別のユーザが同時にアクセスして削除した編集項目を送信しようとした場合は、送信試行が失敗します。このエラー メッセージは、ダイアログボックスに [OK] ボタンとともに表示されます。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、コンテンツ領域リスト ページを表示します。このページには、すべての項目の最新バージョンが表示されています。送信しようとした項目は保存または表示されません。

エラー メッセージ　The item you are trying to Duplicate from has been deleted.

エラー メッセージ　The item you are trying to Edit has been deleted.

説明　選択した項目を複製または編集しようとしましたが、その項目へのアクセスを試行したのと同時に別のユーザが項目を削除しました。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、コンテンツ領域リスト ページを表示します。このページには、すべての項目の最新バージョンが表示されています。複製または編集しようとした項目は保存または表示されません。

エラー メッセージ　The item you are trying to Submit is referencing items that do not exist anymore.

説明　項目を編集または複製しようとしましたが、その項目は、変更を送信しようとしたときに別のユーザが削除した項目を参照しています。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、前のページ（[Create] ページまたは [Edit] ページ）を表示します。試行した変更は保存されず、ページにも表示されません。

エラー メッセージ　Either Import or Export is already in progress.

説明　直前のインポートまたはエクスポートがまだ進行中に、.csv ファイルをインポートまたはエクスポートしようとしました。後続のインポートまたはエクスポートは失敗します。元のインポートまたはエクスポートは、このエラーによって中断されません。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、前のページを表示します。現在実行中のインポート プロセスについては、[Import Progress] セカンダリ ウィンドウを調べて、[Save Log] ボタンがイネーブルになるまで待機します。ログを保存してから、次の .csv ファイルのインポートまたはエクスポートを試行します。

削除エラー

削除エラーは、別の項目が参照している項目を削除しようとすると、発生します。[Delete] をクリックしたときにエラーが検出されると、エラー メッセージと [OK] ボタンのあるダイアログボックスが表示されます。エラー メッセージを確認し、[OK] をクリックして、推奨処置を実行します。

発生する可能性があるエラー メッセージ、説明、および推奨処置は、次のとおりです。

エラー メッセージ　The item you are trying to Delete is referenced by other Items. You must remove all references to this item before it can be deleted.

エラー メッセージ　Some of the items you are trying to Delete are referenced by other Items. You must remove all references to the items before they can be deleted.

説明　別の項目が参照している 1 つ以上の項目を削除しようとした場合は、システムによって削除が阻止されます。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、コンテンツ領域リスト ページを表示します。削除は実行されず、項目はページに表示されたままになります。削除する 1 つまたは複数の項目に対するすべての参照を削除したあと、削除を実行します。

システム障害エラー

システム障害エラーは、システムの誤動作が検出された場合に発生します。システム障害エラーが検出されると、エラー メッセージと [OK] ボタンのあるダイアログボックスが表示されます。エラー メッセージを確認し、[OK] をクリックして、推奨処置を実行します。

発生する可能性があるエラー メッセージ、説明、および推奨処置は、次のとおりです。

エラー メッセージ　`The following System Failure occurred: <description>.`

description に該当する箇所には、具体的な誤動作に関する説明が示されます。

説明　設定を変更しようとしたときに、同時にシステムが障害を検出しました。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、コンテンツ領域リスト ページを表示します。変更は保存されません。可能であれば、検出された誤動作を調査してトラブルシューティングします。

エラー メッセージ　`An unknown System Failure occurred.`

説明　設定を変更しようとしたとき、同時に未知のエラーが検出されました。

推奨処置　[OK] をクリックしてエラー メッセージを閉じ、コンテンツ領域リスト ページを表示します。可能な場合は、システム障害の原因を調査します。

アクセシビリティ

ACS 5.4 Web インターフェイスには、視力や動作に制限のあるユーザのためのアクセシビリティ機能があります。

ここでは、次の内容について説明します。

- 「表示および可読性機能」（P.5-30）
- 「キーボードとマウスの機能」（P.5-31）
- 「その他のアクセシビリティ情報の入手」（P.5-31）

表示および可読性機能

ACS 5.4 Web インターフェイスには、次の機能があります。

- コンピュータ画面の項目の可視性を向上させる機能
- スクリーン リーダー ソフトウェアを使用して、Web インターフェイスのテキストと要素を読み上げる機能

表示および可読性機能には、次の機能があります。

- イメージ マップやグラフとして表示される情報を伝える有用なテキスト説明。
- テーブル、ボタン、フィールド、およびその他の Web インターフェイス要素に対する、わかりやすく一貫性のあるラベル。
- 適用対象の要素のすぐ上、または物理的に近い場所へのラベルの配置。

- インジケータとしてではなく、情報の拡張としてだけ使用される色。たとえば、必須フィールドは赤いアスタリスクに関連付けられています。
- 重要な設定およびアクションに関する確認メッセージ。
- ユーザが制御できる、Web インターフェイス全体のフォント、サイズ、色、およびコントラスト。

キーボードとマウスの機能

キーボードとマウスを使用してアクションを実行することにより、ACS 5.4 Web インターフェイスと対話できます。キーボードとマウスの機能は次のとおりです。

- 動的なコンテンツを表示するページへの、キーボードでアクセス可能なリンク。
- すべてのマウス アクションに対して、標準キーボードでの同等のアクションを実行できます。
- いずれのアクションに対しても、複数のキーを同時に押す必要はありません。
- いずれのアクションに対しても、キーを長時間押す必要はありません。
- 間違った入力を修正する場合は、Back Space キーおよび削除を使用できます。

その他のアクセシビリティ情報の入手

詳細については、Cisco Accessibility Program を参照してください。

- 電子メール：accessibility@cisco.com
- Web：http://www.cisco.com/go/accessibility

CHAPTER 6

インストール後の設定タスク

この章では、ACS を使用するために実行する必要がある設定タスクについて説明します。この章の内容は、次のとおりです。

- 「最小システム セットアップの設定」（P.6-1）
- 「ACS によるシステム管理タスクの実行の設定」（P.6-2）
- 「ACS によるアクセス ポリシーの管理の設定」（P.6-4）
- 「ACS によるネットワークの問題の監視およびトラブルシューティングの設定」（P.6-4）

最小システム セットアップの設定

表 6-1 に、試験、評価、またはデモ環境で ACS を迅速に稼働させるための最小システム セットアップについて従う必要がある手順を示します。

表 6-1　最小システム セットアップ

ステップ番号	作業	ドロワー	参照先
ステップ 1	ネットワーク デバイスを追加します。	[Network Resources] > [Network Devices and AAA Clients]	「ネットワーク デバイスの作成、複製、および編集」（P.7-11）。
ステップ 2	ユーザの追加	[Users and Identity Stores] > [Internal Identity Stores] > [Users]	「内部ユーザの作成」（P.8-11）。
ステップ 3	アクセスを許可または拒否する認可規則を作成します。	[Policy Elements] > [Authorization and Permissions]	「認可および権限の管理」（P.9-19）。

ACS によるシステム管理タスクの実行の設定

表 6-2 に、ACS を管理するために実行する必要があるシステム管理タスクを示します。

表 6-2　システム管理タスク

ステップ番号	作業	ドロワー	参照先
ステップ 1	ACS ライセンスをインストールします。	[System Administration] > [Configuration] > [Licensing]	「ライセンスの概要」（P.18-35）。
ステップ 2	システム証明書をインストールします。	[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates]	「ローカル サーバ証明書の設定」（P.18-14）。
ステップ 3	管理者およびユーザ用のパスワード ポリシー規則を設定します。	• 管理者用： [System Administration] > [Administrators] > [Settings] > [Authentication] • 管理者アクセス設定用： [System Administration] > [Administrators] > [Settings] > [Access] • ユーザ用： [System Administration] > [Users] > [Authentication] [Settings]	• 管理者用： 「管理者の認証設定」（P.16-10）。 • 管理者アクセス設定用： 「管理者アクセスの設定」（P.16-13） • ユーザ用： 「ユーザの認証設定の設定」（P.8-9）。
ステップ 4	ACS 管理者を追加します。	[System Administration] > [Administrators] > [Accounts]	「システム管理者およびアカウントの設定」（P.16-3）
ステップ 5	プライマリおよびセカンダリ ACS インスタンスを設定します。	[System Administration] > [Operations] > [Distributed System Management]	「分散展開について」（P.17-2）。
ステップ 6	ロギングを設定します。	[System Administration] > [Configuration] > [Log Configuration]	「ログの設定」（P.18-21）。
ステップ 7	ネットワーク デバイスを追加します。	[Network Resources] > [Network Devices and AAA Clients]	「ネットワーク デバイスの作成、複製、および編集」（P.7-11）。

表 6-2　システム管理タスク （続き）

ステップ番号	作業	ドロワー	参照先
ステップ 8	ユーザまたはホストを内部 ID ストアに追加するか、外部 ID ストアを定義するか、またはその両方を実行します。	• 内部 ID ストア用： [Users and Identity Stores] > [Internal Identity Stores] • 外部 ID ストア用： [Users and Identity Stores] > [External Identity Stores]	• 内部 ID ストア用： – 「内部ユーザの作成」（P.8-11）。 – 「ID ストアでのホストの作成」（P.8-16）。 • 外部 ID ストア用： – 「外部 LDAP ID ストアの作成」（P.8-23）。 – 「AD ドメインへの ACS の追加」（P.8-47）。 – 「RSA SecurID トークンサーバの作成および編集」（P.8-56）。 – 「RADIUS ID サーバの作成、複製、および編集」（P.8-64）。
ステップ 9	エンドユーザ証明書を追加します。	[Users and Identity Stores] > [Certificate Authorities]	「認証局の追加」（P.8-70）。
ステップ 10	ID 順序を設定します。	[Users and Identity Stores] > [Identity Store Sequences]	「ID ストア順序の作成、複製、および編集」（P.8-76）。

ACS によるアクセス ポリシーの管理の設定

表 6-3 に、アクセス制限およびアクセス権を管理するために実行する必要があるタスクを示します。

表 6-3　アクセス ポリシーの管理

ステップ番号	作業	ドロワー	参照先
ステップ 1	ポリシー条件を定義します。	[Policy Elements] > [Session Conditions]	「ポリシー条件の管理」(P.9-1)。
ステップ 2	認可および権限を定義します。	[Policy Elements] > [Authorization and Permissions]	「認可および権限の管理」(P.9-19)。
ステップ 3	アクセス サービスおよびサービス セレクション ポリシーを定義します。	[Access Policies] > [Access Services]	• アクセス サービスを設定するには、次の手順を実行します。 「アクセス サービスの設定」(P.10-11)。 • アクセス サービス ポリシーを設定するには、次の手順を実行します。 「アクセス サービス ポリシーの設定」(P.10-22)。 • 複合条件を設定するには、次の手順を実行します。 「複合条件の設定」(P.10-41)。

ACS によるネットワークの問題の監視およびトラブルシューティングの設定

表 6-4 に、Monitoring and Report Viewer のトラブルシューティングのために実行する必要のある一連の設定タスクを示します。

表 6-4　監視およびトラブルシューティングの設定

ステップ番号	作業	ドロワー	参照先
ステップ 1	データの削除およびバックアップを設定します。	[Monitoring Configuration] > [System Operations] > [Data Management] > [Removal and Backup]	「データの削除と増分バックアップの設定」(P.15-3)。
ステップ 2	電子メール設定を指定します。	[Monitoring Configuration] > [System Configuration] > [Email Settings]	「電子メール設定の指定」(P.15-16)。
ステップ 3	収集フィルタを設定します。	[Monitoring Configuration] > [System Configuration] > [Collection Filters]	「収集フィルタについて」(P.15-17)。

表 6-4　監視およびトラブルシューティングの設定 （続き）

ステップ番号	作業	ドロワー	参照先
ステップ 4	システム アラームをイネーブルにし、通知を受信する方法を指定します。	[Monitoring Configuration] > [System Configuration] > [System Alarm Settings]	「システム アラーム設定の指定」（P.15-18）。
ステップ 5	スケジュールを定義し、しきい値アラームを作成します。	[Monitoring and Reports] > [Alarms]	• スケジュールを定義するには、次の手順を実行します。 「アラーム スケジュールについて」（P.12-9）。 • しきい値アラームを作成するには、次の手順を実行します。 「アラームしきい値の作成、編集、および複製」（P.12-11）。
ステップ 6	アラーム syslog ターゲットを設定します。	[Monitoring Configuration] > [System Configuration] > [Alarm Syslog Targets]	「アラーム syslog ターゲットの設定」（P.15-18）。
ステップ 7	Monitoring and Report Viewer データをエクスポートするようにリモート データベースを設定します。	[Monitoring Configuration] > [System Configuration] > [Remote Database Settings]	「リモート データベース設定の指定」（P.15-18）。

CHAPTER 7

ネットワーク リソースの管理

[Network Resources] ドロワでは、ACS に要求を発行するネットワーク内の要素、または要求処理の一環として ACS が対話する要素が定義されます。これらの要素には、要求を発行するネットワーク デバイス、および RADIUS プロキシとして使用される RADIUS サーバなどの外部サーバが含まれます。

ドロワを使用して、次の内容を設定できます。

- ネットワーク デバイス グループ：ネットワーク デバイスの論理的なグループ。設定すると、ポリシー条件で使用できます。
- ネットワーク デバイス：ACS ネットワークにアクセスする、ACS デバイス リポジトリ内のすべてのネットワーク デバイスの定義。
- デフォルトのネットワーク デバイス：特定の IP アドレスのデバイス定義が ACS で見つからなかった場合に、ACS によって RADIUS 要求または TACACS+ 要求に使用されるデフォルトのネットワーク デバイス定義。
- 外部プロキシ サーバ：RADIUS プロキシとして使用できる RADIUS サーバ。
- OCSP サービス：Online Certificate Status Protocol（OCSP）サービスが x.509 デジタル証明書の状態を検査するために使用され、証明書失効リスト（CRL）への代替として使用できます。

ネットワーク デバイスからネットワークへのアクセス要求を受信すると、ACS はネットワーク デバイス リポジトリを検索して、IP アドレスが一致するエントリを見つけます。次に、ACS はネットワーク デバイス定義から取得した秘密情報を共有秘密情報と比較します。

これらの情報が一致する場合は、そのネットワーク デバイスに関連付けられているネットワーク デバイス グループが取得され、ポリシー決定で使用できるようになります。ポリシー決定の詳細については、「「ACS 5.x ポリシー モデル」」を参照してください。

[Network Resources] ドロワには、次の項目が含まれています。

- 「ネットワーク デバイス グループ」（P.7-2）
- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「デフォルトのネットワーク デバイスの設定」（P.7-18）
- 「外部プロキシ サーバの使用」（P.7-20）
- 「OCSP サービスの使用」（P.7-22）

ネットワーク デバイス グループ

ACS では、デバイスのセットであるネットワーク デバイス グループ（NDG）を定義できます。NDG を使用すると、デバイスを論理的にグループ化でき（デバイスの場所、タイプなど）、それらのグループをポリシー条件で使用できます。

ACS では、デバイスの要求を受信すると、そのデバイスに関連付けられているネットワーク デバイス グループが取得され、ポリシー テーブルのネットワーク デバイス グループと比較されます。この方法を使用すると、複数のデバイスをグループ化し、同じポリシーを割り当てることができます。たとえば、特定の場所にあるすべてのデバイスをグループ化して、同じポリシーを割り当てることができます。

デバイス グループ階層は、ネットワーク デバイス グループが含まれた階層構造です。これらの 2 つ、つまり *Location* と *Device Type* は事前定義済みで、その名前は編集できますが、削除することはできません。ルートを含む最大 6 個の追加階層を追加できます。

NDG は、階層内の任意のノードと関連し、デバイスが関連付けられているエンティティです。これらのノードには、リーフノードだけでなく、階層内のあらゆるノードが該当します。

（注）　ルート ノードを含み、最大で 6 つのノードを NDG 階層に含めることができます。

関連トピック

- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）
- 「ネットワーク デバイス グループの削除」（P.7-3）

ネットワーク デバイス グループの作成、複製、および編集

ネットワーク デバイス グループを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。追加のネットワーク デバイス グループを定義済みである場合は、それらのグループが [Network Device Groups] オプションの下の左側のナビゲーション ペインに表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するネットワーク デバイス グループの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するネットワーク デバイス グループ名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Hierarchy - General] ページが表示されます。

ステップ 3　表 7-1 の説明に従って、[Hierarchy - General] ページのフィールドを変更します。

表 7-1　[Device Groups - General] ページのフィールド説明

フィールド	説明
Name	ネットワーク デバイス グループ（NDG）の名前を入力します。

表 7-1　[Device Groups - General] ページのフィールド説明 （続き）

Description	（任意）NDG の説明を入力します。
Root Node Name/Parent	NDG に関連付けられているルート ノードの名前を入力します。NDG は、反転ツリーとして構造化されており、ルート ノードは反転ツリーの最上部にあります。ルート ノード名には、NDG と同じ名前を指定できます。 NDG 名は、[Network Resources] ドロワで NDG をクリックすると表示されます。

ステップ 4　[Submit] をクリックします。

ネットワーク デバイス グループの設定が保存されます。[Network Device Groups] ページが表示され、新しいネットワーク デバイス グループ設定が示されます。

関連トピック

- 「ネットワーク デバイス グループ」（P.7-2）
- 「ネットワーク デバイス グループの削除」（P.7-3）
- 「階層内でのネットワーク デバイス グループの作成、複製、および編集」（P.7-4）
- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）

ネットワーク デバイス グループの削除

ネットワーク デバイス グループを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。

ステップ 2　削除するネットワーク デバイス グループの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のエラー メッセージが表示されます。

```
You have requested to delete a network device group. If this group is referenced from a
Policy or a Policy Element then the delete will be prohibited. If this group is referenced
from a network device definition, the network device will be modified to reference the
root node name group.
```

ステップ 3　[OK] をクリックします。

[Network Device Groups] ページが表示されます。このとき、削除されたネットワーク デバイス グループは表示されません。

階層内でのネットワーク デバイス グループの作成、複製、および編集

新しいネットワーク デバイス グループ ノード、または複製および編集されたネットワーク デバイス グループ ノードに対して親と子の関係を選択することによって、ネットワーク デバイス グループ ノード階層をニーズに従って配置できます。また、ネットワーク デバイス グループ ノードを階層から削除することもできます。

階層内でネットワーク デバイス グループ ノードを作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。

ステップ 2　新しいネットワーク デバイス グループを作成する [Location]、[Device Type]、または定義済みの別のネットワーク デバイス グループをクリックし、そのグループの階層に追加します。

[Network Device Group] 階層ページが表示されます。

ステップ 3　次のいずれかを実行します。

- [Create] をクリックします。選択済みのグループが存在する場合に [Create] をクリックすると、新しいグループは、選択済みの親グループの子になります。[Create] 画面で [Select] を選択して、階層内の親およびそのすべての子を移動できます。
- 複製するネットワーク デバイス グループ名の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するネットワーク デバイス グループ名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Device Group - General] ページが表示されます。

ステップ 4　表 7-2 に従い、[Device Groups - General] ページのフィールドを変更します。

表 7-2　[Device Groups - General] ページのフィールド説明

フィールド	説明
Name	NDG の名前を入力します。
Description	（任意）NDG の説明を入力します。
Parent	NDG に関連付けられている親の名前を入力します。NDG は反転ツリーとして構造化されており、親の名前がツリーの最上部の名前となります。 [Select] をクリックして、[Groups] ダイアログボックスを開きます。このダイアログボックスで、グループの適切な親を選択できます。

ステップ 5　[Submit] をクリックします。

ネットワーク デバイス グループの新しい設定が保存されます。[Network Device Groups] 階層ページが表示され、新しいネットワーク デバイス グループ設定が示されます。

関連トピック

- 「ネットワーク デバイス グループ」（P.7-2）
- 「ネットワーク デバイス グループの削除」（P.7-3）
- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）

- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）

階層からのネットワーク デバイス グループの削除

ネットワーク デバイス グループを階層から削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Device Groups] を選択します。

[Network Device Groups] ページが表示されます。

ステップ 2　ネットワーク デバイス グループ ノードを編集する必要がある [Location]、[Device Type]、または定義済みの別のネットワーク デバイス グループをクリックします。

[Network Device Groups] ノード階層ページが表示されます。

ステップ 3　削除するノードを選択し、[Delete] をクリックします。

次のメッセージが表示されます。

```
You have requested to delete a network device group. If this group is referenced from a
Policy or a Policy Element then the delete will be prohibited. If this group is referenced
from a network device definition, the network device will be modified to reference the
root node name group.
```

ステップ 4　[OK] をクリックします。

（注）　グループのルート ノードは、NDG 階層から削除できません。削除しようとすると、次のエラー メッセージが表示されます。

```
Selected node can be removed only with a root group.
```

ネットワーク デバイス グループ ノードが設定から削除されます。[Network Device Groups] 階層ページが表示されます。このとき、削除したデバイス グループ ノードは表示されません。

ネットワーク デバイスおよび AAA クライアント

ネットワークにアクセスする、ACS デバイス リポジトリ内のすべてのデバイスを定義する必要があります。ネットワーク デバイス定義は、特定の IP アドレス、またはサブネット内のすべての IP アドレスがネットワークにアクセスできるサブネット マスクに関連付けることができます。

デバイス定義には、ネットワーク デバイス グループ（NDG）へのデバイスの関連付けが含まれています。デバイスが TACACS+ または RADIUS を使用するかどうか、およびデバイスが Security Group Access デバイスであるかどうかも設定します。

（注）　サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。たとえば、サブネット マスク 255.255.255.0 は、256 個の固有の IP アドレスがあることを意味します。

デバイスおよびその設定をネットワーク デバイス リポジトリにインポートできます。

要求を受信すると、ACS はネットワーク デバイス リポジトリを検索して、一致する IP アドレスを持つデバイスを見つけ、次に、その秘密情報やパスワード情報をネットワーク デバイス定義から取得した情報と比較します。情報が一致すると、そのデバイスと関連付けられている NDG が取得され、ポリシー決定で使用されます。

Security Group Access のオプションをイネーブルにするには、Security Group Access ライセンスをインストールする必要があります。Security Group Access のオプションは Security Group Access ライセンスをインストールした場合にだけ表示されます。Security Group Access ライセンスの詳細については、「ライセンスの概要」（P.18-35）を参照してください。

ネットワーク デバイスの一括操作の表示および実行

ネットワーク デバイスおよび AAA クライアントを表示できます。これらは、ACS にアクセス要求を送信するデバイスです。アクセス要求は、TACACS+ または RADIUS を介して送信されます。

ネットワーク デバイスを表示およびインポートするには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Device] ページが表示され、すべての設定済みネットワーク デバイスが示されます。表 7-3 に、[Network Device] ページのフィールドの説明を示します。

表 7-3　[Network Device] ページのフィールドの説明

オプション	説明
Name	ACS でのユーザ指定のネットワーク デバイス名。名前をクリックして、関連付けられているネットワーク デバイスを編集します（「ネットワーク デバイス プロパティの表示」（P.7-15）を参照）。
IP Address	*表示のみ*。各ネットワーク デバイスの IP アドレスまたはサブネット マスクです。IPv4 または IPv6 タイプの最初の 3 個の IP アドレスがフィールドにそれぞれカンマ（,）で区切られて表示されます。 このフィールドにサブネット マスクが含まれている場合、指定したサブネット マスク内のすべての IP アドレスは、ネットワークへのアクセスが許可され、ネットワーク デバイス定義に関連付けられます。 サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。次に例を示します。 IPv4：サブネットマスク 255.255.255.0 は 256 個の固有の IPv4 アドレスがあることを意味します。デフォルトでは、IPv4 のサブネット マスクの値は 32 です。 IPv6：サブネット マスク 2001:0DB8:0:CD30::/127 は 2 個の固有の IPv6 アドレスがあることを意味します。デフォルトでは、IPv6 のサブネット マスクの値は 128 です。 指定された IP アドレスの横に、除外された IP アドレスがある場合はそれを表示できます。
NDG: *string*	ネットワーク デバイス グループ。2 つの事前定義済みの NDG は、Location および Device Type です。追加のネットワーク デバイス グループを定義済みである場合は、それらのグループもここに示されます。
Description	*表示のみ*。ネットワーク デバイスの説明。

ステップ 2　次のいずれかを実行します。

- 新しいネットワーク デバイスを作成するには、[Create] をクリックします。「ネットワーク デバイスの作成、複製、および編集」（P.7-11）を参照してください。
- 編集するネットワーク デバイスの隣にあるチェックボックスをオンにし、[Edit] をクリックします。「ネットワーク デバイスの作成、複製、および編集」（P.7-11）を参照してください。

- 複製するネットワーク デバイスの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。「ネットワーク デバイスの作成、複製、および編集」（P.7-11）を参照してください。
- 次のカテゴリに基づいてネットワーク デバイスを検索できます。
  - Name
  - IP Address
  - Description
  - NDG Location
  - Device Type

  完全な IP アドレス、またはワイルドカード「*」や [15-20] のような IP アドレス範囲を使用した IP アドレスを IP アドレスの検索フィールドに指定できます。ワイルドカード「*」と IP 範囲 [15-20] オプションは IP アドレスのすべての 4 オクテットに指定できます。IP アドレスで検索する場合は、[Equal] オプションのみが検索条件に表示されます。

（注）　IP アドレスまたは IP 範囲のアドレスを検索する際、検索結果は、検索の IP アドレス（または）IP 範囲のアドレスが除外された IP アドレス（または）範囲にある場合でも、検索条件に一致するすべてのレコードを表示します。

- [File Operations] をクリックして、次のいずれかの機能を実行します。
  - Add : インポート ファイルからネットワーク デバイスのリストを単一ショットに追加する場合は、このオプションを選択します。
  - Update : ACS でのネットワーク デバイスのリストをインポート ファイル内のネットワーク デバイスに置き換えるには、このオプションを選択します。
  - Delete : インポート ファイルでリストされているネットワーク デバイスを ACS から削除するには、このオプションを選択します。

  詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。

インポート ファイルの作成方法については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1055255.

ワンポイントアドバイス

ACS オブジェクトに対する一括での追加、編集、または削除操作を実行するには、そのオブジェクトのエクスポート ファイルを使用し、ヘッダー行を保持して、.csv インポート ファイルを作成できます。ただし、更新された名前または MAC アドレスを ACS オブジェクトに追加する場合は、特定の更新テンプレートをダウンロードして使用してください。また、NDG の場合、エクスポート テンプレートには NDG 名だけが含まれているため、他のプロパティを更新するには、NDG 更新テンプレートをダウンロードして使用してください。

関連トピック：

- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）
- 「階層内でのネットワーク デバイス グループの作成、複製、および編集」（P.7-4）

ネットワーク デバイスおよび AAA クライアントのエクスポート

（注）　エクスポート プロセスが正常に完了するように、ブラウザのポップアップ ブロッカーをオフにする必要があります。

ネットワーク デバイスのリストをエクスポートするには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Device] ページが表示されます。

ステップ 2　フィルタ条件および if 演算子 Match を選択し、検索するフィルタ基準をテキスト ボックスに入力します。

ステップ 3　[Go] をクリックします。

フィルタ基準と一致するレコードのリストが表示されます。このリストを .csv ファイルにエクスポートできます。

ステップ 4　[Export] をクリックして、レコードを .csv ファイルにエクスポートします。

システム メッセージ ボックスが表示され、ファイル転送中に .csv ファイルを暗号化するための暗号化パスワードを要求するプロンプトが表示されます。

エクスポート .csv ファイルを暗号化するには、[Password] チェックボックスをオンにして暗号化パスワードを入力します。任意で、転送中にファイルを暗号化しないことを選択できます。

ステップ 5　[Start Export] をクリックして、エクスポート プロセスを開始します。

[Export Progress] ウィンドウが表示され、エクスポート プロセスの進行状況が表示されます。このプロセスでエラーが発生した場合は、そのエラーが [Export Progress] ウィンドウに表示されます。

エクスポート プロセスは、このプロセス中にいつでも終了することができます。エクスポート プロセスを打ち切るまでのすべてのレポートがエクスポートされます。再開するには、エクスポート プロセスを最初からやり直す必要があります。

ステップ 6　エクスポート プロセスの完了後、[Save File] をクリックして、エクスポート ファイルをローカル ディスクに保存します。

エクスポート ファイルは、export.zip として圧縮された .csv ファイルです。

ネットワーク リソースおよびユーザに関する一括操作の実行

ファイル操作機能を使用して、データベースで次の項目に対して一括操作（追加、更新、および削除）を実行できます。

- 内部ユーザ
- 内部ホスト
- ネットワーク デバイス

一括操作の場合は、ACS から .csv ファイル テンプレートをダウンロードし、追加、更新、または削除するレコードを .csv ファイルに追加し、そのファイルをローカル ディスクに保存する必要があります。Download Template 機能を使用して、.csv ファイルが要件に準拠するようにします。

ユーザ、内部ホスト、およびネットワーク デバイス用の .csv テンプレートは、それぞれのタイプに固有のテンプレートです。たとえば、[Users] ページからアクセスしてダウンロードしたテンプレートは、内部ホストやネットワーク デバイスの追加には使用できません。.csv ファイルは次の要件に準拠している必要があります。

- 最初のレコード（.csv ファイルの最初の行）の内容は変更しないでください。
- 各レコードに対して使用するのは 1 行だけです。
- フィールドに改行文字を埋め込まないでください。
- 英語以外の言語では、.csv ファイルを utf-8 符号化で符号化するか、Unicode をサポートするフォントを使用して保存します。

一括操作を開始する前に、ブラウザのポップアップ ブロッカーがディセーブルになっていることを確認します。

ステップ 1　Web インターフェイスの [Users]、[Network Devices]、または [MAC Address] ページで、[File Operations] をクリックします。

[Operation] ダイアログボックスが表示されます。

ステップ 2　.csv ファイル テンプレートがない場合は、[Next] をクリックして、.csv ファイル テンプレートをダウンロードします。

ステップ 3　テンプレートベースの .csv ファイルをローカル ディスクにすでに作成している場合は、次の操作のいずれかをクリックします。

- Add：.csv ファイル内のレコードを、ACS で現在使用可能なレコードに追加します。
- Update：ACS のレコードを .csv ファイルのレコードで上書きします。
- Delete：.csv ファイル内のレコードを ACS のリストから削除します。

ステップ 4　[Next] をクリックして、次のページに移動します。

ステップ 5　[Browse] をクリックして、.csv ファイルに移動します。

ステップ 6　インポート プロセス時にエラーが発生した場合に ACS で実行するオプションを次の中から選択します。

- 残りのレコードの処理を続行します。処理に成功したレコードだけがインポートされます。
- 残りのレコードの処理を停止します。エラーの発生前にインポートが成功したレコードだけがインポートされます。

ステップ 7　.csv ファイルが GPG 形式で暗号化されている場合は、[Password] チェックボックスをオンにして、.csv ファイルを暗号化するためのパスワードを入力します。

ステップ 8　[Finish] をクリックして、一括操作を開始します。

[Import Progress] ウィンドウが表示されます。このウィンドウを使用して、一括操作の進行状況を監視します。.csv ファイルのレコードのデータ転送失敗が表示されます。

[Abort] ボタンをクリックして、進行中のデータのインポートを停止できますが、転送に成功したデータはデータベースから削除されません。

操作が完了すると、[Save Log] ボタンがイネーブルになります。

ステップ 9　[Save Log] をクリックして、ログ ファイルをローカル ディスクに保存します。

ステップ 10　[OK] をクリックして、[Import Progress] ウィンドウを閉じます。

システムに一度に送信できる .csv ファイルは 1 つだけです。操作が進行中である場合、追加の操作は、最初の操作が完了するまで成功しません。

インポート ファイルの作成方法については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1055255.

ワンポイントアドバイス

ACS オブジェクトに対する一括での追加、編集、または削除操作を実行するには、そのオブジェクトのエクスポート ファイルを使用し、ヘッダー行を保持して、.csv インポート ファイルを作成できます。ただし、更新された名前または MAC アドレスを ACS オブジェクトに追加するには、特定の更新テンプレートをダウンロードして使用してください。また、NDG の場合、エクスポート テンプレートには NDG 名だけが含まれているため、他のプロパティを更新するには、NDG 更新テンプレートをダウンロードして使用してください。

ネットワーク リソースおよびユーザのエクスポート

ネットワーク リソースまたはユーザのリストをエクスポートするには、次の手順を実行します。

ステップ 1　Web インターフェイスの [Users]、[Network Devices]、または [MAC Address] ページで、[Export] をクリックします。

[Network Device] ページが表示されます。

ステップ 2　フィルタ条件および if 演算子 Match を選択し、検索するフィルタ基準をテキスト ボックスに入力します。

ステップ 3　[Go] をクリックします。

フィルタ基準と一致するレコードのリストが表示されます。これらのレコードを .csv ファイルにエクスポートできます。

ステップ 4　[Export] をクリックして、レコードを .csv ファイルにエクスポートします。

システム メッセージ ボックスが表示され、ファイル転送中に .csv ファイルを暗号化するための暗号化パスワードを要求するプロンプトが表示されます。

エクスポート .csv ファイルを暗号化するには、[Password] チェックボックスをオンにして暗号化パスワードを入力します。任意で、転送中にファイルを暗号化しないことを選択できます。

ステップ 5　[Start Export] をクリックして、エクスポート プロセスを開始します。

[Export Progress] ウィンドウが表示され、エクスポート プロセスの進行状況が表示されます。このプロセスでエラーが発生した場合は、そのエラーが [Export Progress] ウィンドウに表示されます。

エクスポート プロセスは、このプロセス中にいつでも終了することができます。エクスポート プロセスを終了すると、終了までのすべてのレポートがエクスポートされます。再開する場合は、エクスポート プロセスを最初からやり直す必要があります。

ステップ 6　エクスポート プロセスの完了後、[Save File] をクリックして、エクスポート ファイルをローカル ディスクに保存します。

エクスポート ファイルは、export.zip として圧縮された .csv ファイルです。

ネットワーク デバイスの作成、複製、および編集

一括インポート機能を使用すると、多数のネットワーク デバイスを 1 回の操作でインポートできます。詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。または、このトピックで説明する手順を使用して、ネットワーク デバイスを作成できます。

ネットワーク デバイスを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Devices] ページが表示され、設定済みのネットワーク デバイスがある場合は、そのリストが示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するネットワーク デバイス名の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するネットワーク デバイス名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

新しいネットワーク デバイスを作成している場合は、ネットワーク デバイス作成プロセスの最初のページが表示されます。ネットワーク デバイスを複製または編集している場合は、選択したデバイスの [Network Device Properties] ページが表示されます。

ステップ 3　必要に応じてフィールドを変更します。フィールドの説明については、「ネットワーク デバイスおよび AAA クライアントの設定」（P.7-11）を参照してください。

ステップ 4　[Submit] をクリックします。

新しいネットワーク デバイス設定が保存されます。[Network Devices] ページが表示され、新しいネットワーク デバイス設定が示されます。

関連トピック

- 「ネットワーク デバイスの一括操作の表示および実行」（P.7-6）
- 「ネットワーク デバイスおよび AAA クライアントの設定」（P.7-11）

ネットワーク デバイスおよび AAA クライアントの設定

このページを表示するには、[Network Resources] > [Network Devices and AAA Clients] を選択してから、[Create] をクリックします。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成

オプション	説明
General	
Name	ネットワーク デバイスの名前。ネットワーク デバイスを複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Description	ネットワーク デバイスの説明。
Network Device Groups	

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
Location	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Location ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Device Type	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Device Type ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
IP Address ネットワーク デバイスに関連付けられる IP アドレスとサブネット マスク。単一の IP アドレスを入力するか、範囲を定義するかを選択します。	
Single IP Address	単一の IP アドレスを入力することを選択します。IP アドレスは IPv4 または IPv6 にできます。アドレスがサポートされる形式で入力されると、ACS 5.4 はその IP アドレスを検証します。入力された形式が正しくない場合は、エラー メッセージを表示します。 **（注）**　IPv6 アドレスは、TACACS+ プロトコルだけでサポートされています。
IP Range(s) By Mask	IP アドレス範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。このフィールドでサブネット マスクを使用する場合、指定したサブネット マスク内のすべての IP アドレスは、ネットワークへのアクセスが許可され、ネットワーク デバイス定義に関連付けられます。 サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。たとえば、サブネット マスク 255.255.255.0 は、256 個の固有の IP アドレスがあることを意味します。デフォルトでは、IPv4 のサブネット マスクの値は 32、IPv6 の値は 128 です。 最初の 6 個の IP アドレスがフィールドに表示されます。それ以外に設定されている IP アドレスを表示するには、スクロール バーを使用します。 IP アドレスの範囲を指定する場合は、ワイルドカード用のマスクだけが必要となります。アスタリスク（*）はワイルドカードとして使用できません。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
IP Range	IP アドレスの単一または複数の範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。サブセットがすでに追加されている場合には、設定された範囲からその IP アドレス範囲のサブネットを除外できます。 IP アドレスの範囲を指定するにはハイフン（-）を使用できます。最大 40 個の IP アドレスが単一の IP 範囲で許可されます。 ワイルドカードで IP アドレスを追加することもできます。ワイルド カードとしてアスタリスク（*）を使用できます。 IP アドレス範囲の入力例をいくつか次に示します。 • 単一範囲：10.77.10.1-10,,,, 192.120.10-12.10 • 複数範囲：10.*.1-20.10, 192.1-23.*.100-150 • 範囲から除外：10.10.1-255.* exclude 10.10.10-200.100-150 動的なデバイス IP アドレス範囲（たとえば、1-5.*.7.9）を使用すると、ランタイムと管理の両方のパフォーマンスに影響する可能性があります。 したがって、可能な限り IP アドレスとサブネット マスクを使用することを推奨します。動的 IP アドレス範囲は、範囲を IP アドレスおよびサブネット マスクを使用して記述できない場合にのみ使用する必要があります。 **（注）**　ワイルドカードを使用する AAA クライアントは、4.x から 5.x. に移行されます。 **（注）**　ACS 5.4 は、IPv6 範囲をサポートしていません。
Authentication Options	
TACACS+	Cisco IOS TACACS+ プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 ネットワーク デバイスが Management Center for Firewalls などのシスコ デバイス管理アプリケーションである場合は、このオプションを使用する必要があります。ネットワーク デバイスが Cisco アクセス サーバ、ルータ、またはファイアウォールである場合は、このオプションを使用する必要があります。 IPv4 または IPv6 の IP アドレスを使用する場合には [TACACS+] をオンにします。
TACACS+ Shared Secret	ネットワーク デバイスの共有秘密情報（TACACS+ プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Single Connect Device	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを選択します。 • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が使用されます。
RADIUS	RADIUS プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 IPv6 アドレスを使用する場合は、このオプションをオフにします。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
RADIUS Shared Secret	ネットワーク デバイスの共有秘密情報（RADIUS プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
CoA Port	ユーザ認証用に、RAIUS CoA ポートをセッション ディレクトリに設定する場合に使用します。このセッション ディレクトリは、[Monitoring and Troubleshooting Viewer] ページから起動できます。デフォルトでは、CoA ポートの値は 1700 となります。
Enable KeyWrap	PEAP、EAP-FAST、および EAP-TLS 認証での RADIUS キー ラップの共有秘密キーをイネーブルにする場合にオンにします。それぞれのキーは一意で、RADIUS 共有キーとは明確に区別される必要があります。これらの共有キーは、AAA クライアントごとに設定できます。キー ラップのデフォルトのキー モードは、16 進数ストリングです。
Key Encryption Key (KEK)	Pairwise Master Key（PMK）の暗号化に使用されます。ASCII モードでは、キーの長さを正確に 16 文字で入力し、16 進数モードでは 32 文字で入力します。
Message Authentication Code Key (MACK)	RADIUS メッセージに対して keyed キー付きハッシュ メッセージ認証コード（HMAC）を計算するのに使用します。 入力するキーの長さは、ASCII モードで 20 文字、16 進数モードで 40 文字となります。
Key Input Format	ASCII または 16 進数ストリングとしてキーを入力します。デフォルトは 16 進数です。
Security Group Access	Cisco Security Group Access 機能をイネーブルにした場合にだけ表示されます。ネットワーク デバイスで Security Group Access 機能を使用する場合にオンにします。ネットワーク デバイスがシード デバイス（Security Group Access ネットワーク内の最初のデバイス）である場合、[RADIUS] チェックボックスもオンにする必要があります。
Use Device ID for Security Group Access Identification	Security Group Access の識別にデバイス ID を使用する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、次のフィールド（Device ID）がディセーブルになります。
Device ID	このデバイスの Security Group Access の識別に使用される名前。デフォルトでは、設定済みのデバイス名を使用できます。別の名前を使用する場合は、[Use device name for Security Group Access identification] チェックボックスをオフにして、[Identification] フィールドに名前を入力します。
Password	Security Group Access 認証パスワード。
Security Group Access Advanced Settings	追加の Security Group Access フィールドを表示する場合にオンにします。
Other Security Group Access devices to trust this device (SGA trusted)	デバイスのピア デバイスすべてによってこのデバイスが信頼されるかどうかを指定します。デフォルトはオンです。ピア デバイスでこのデバイスが信頼され、このデバイスから受信するパケットの SGT は変更されません。 このチェックボックスをオフにした場合、ピア デバイスによって、このデバイスからのパケットが関連するピア SGT で塗り替えられます。
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	ピア認可ポリシーの有効期限を指定します。ACS によって、この情報はピア ポリシー要求への応答でデバイスに返されます。デフォルトは 1 日です。
Download SGACL lists every: Weeks Days Hours Minutes Seconds	SGACL リストの有効期限を指定します。ACS によって、この情報は SGACL リストの要求への応答でデバイスに返されます。デフォルトは 1 日です。

表 7-4　ネットワーク デバイスおよび AAA クライアントの作成 （続き）

オプション	説明
Download environment data every: Weeks Days Hours Minutes Seconds	環境データの有効期限を指定します。ACS によって、この情報は環境データの要求への応答でデバイスに返されます。デフォルトは 1 日です。
Re-authentication every: Weeks Days Hours Minutes Seconds	dot1x（.1x）再認証期間を指定します。ACS によって、これはサプリカントに対して設定され、この情報はオーセンティケータに返されます。デフォルトは 1 日です。

ネットワーク デバイス プロパティの表示

[Network Resources] > [Network Devices and AAA Clients] を選択してから、デバイス名をクリックします、または、デバイス名の隣にあるチェックボックスをオンにして [Edit] または [Duplicate] をクリックします。

[Network Devices and AAA Clients Properties] ページが表示され、表 7-5 で説明されている情報が示されます。

表 7-5　[Network Devices and AAA Clients Properties] ページ

オプション	説明
Name	ネットワーク デバイスの名前。ネットワーク デバイスを複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Description	ネットワーク デバイスの説明。
Network Device Groups	
Location: Select	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付けるネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Device Type: Select	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Device Type ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
IP Address ネットワーク デバイスに関連付けられる IP アドレスおよびサブネット マスク。単一の IP アドレスを入力するか、範囲を定義するかを選択します。	
Single IP Address	単一の IP アドレスを入力することを選択します。

表 7-5　[Network Devices and AAA Clients Properties] ページ （続き）

オプション	説明
IP Range(s) By Mask	IP アドレス範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。このフィールドでサブネット マスクを使用する場合、指定したサブネット マスク内のすべての IP アドレスは、ネットワークへのアクセスが許可され、ネットワーク デバイス定義に関連付けられます。 サブネット マスクを使用する場合、固有の IP アドレスの数は、サブネット マスクによって使用可能な IP アドレスの数によって決まります。たとえば、サブネット マスク 255.255.255.0 は、256 個の固有の IP アドレスがあることを意味します。 最初の 6 個の IP アドレスがフィールドに表示されます。それ以外に設定されている IP アドレスを表示するには、スクロール バーを使用します。 IP アドレスの範囲を指定する場合は、ワイルドカード用のマスクだけが必要となります。ワイルドカードとしてアスタリスク（*）は使用できません。
IP Range	IP アドレスの単一または複数の範囲を入力することを選択します。ネットワーク デバイスごとに最大 40 の IP アドレスまたはサブネット マスクを設定できます。サブセットがすでに追加されている場合には、設定された範囲からその IP アドレス範囲のサブネットを除外できます。 IP アドレスの範囲を指定するにはハイフン（-）を使用できます。ワイルドカードで IP アドレスを追加することもできます。ワイルド カードとしてアスタリスク（*）を使用できます。 IP アドレス範囲の入力例をいくつか次に示します。 • 単一範囲：10.77.10.1-10,,,, 192.120.10-12.10 • 複数範囲：10.*.1-20.10, 192.1-23.*.100-150 • 範囲から除外：10.10.1-255.* exclude 10.10.10-200.100-150 動的なデバイス IP アドレス範囲（たとえば、1-5.*.7.9）を使用すると、ランタイムと管理の両方のパフォーマンスに影響する可能性があります。 したがって、可能な限り IP アドレスとサブネット マスクを使用することを推奨します。動的 IP アドレス範囲は、範囲を IP アドレスおよびサブネット マスクを使用して記述できない場合にのみ使用する必要があります。
Authentication Options	
TACACS+	Cisco IOS TACACS+ プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 ネットワーク デバイスが Management Center for Firewalls などのシスコ デバイス管理アプリケーションである場合は、このオプションを使用する必要があります。ネットワーク デバイスが Cisco アクセス サーバ、ルータ、またはファイアウォールである場合は、このオプションを使用する必要があります。
TACACS+ Shared Secret	ネットワーク デバイスの共有秘密情報（TACACS+ プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Single Connect Device	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを選択します。 • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が使用されます。

表 7-5　[Network Devices and AAA Clients Properties] ページ （続き）

オプション	説明
RADIUS	RADIUS プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。
RADIUS Shared Secret	ネットワーク デバイスの共有秘密情報（RADIUS プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
CoA Port	ユーザ認証用に、RAIUS CoA ポートをセッション ディレクトリに設定する場合に使用します。このセッション ディレクトリは、[Monitoring and Troubleshooting Viewer] ページから起動できます。デフォルトでは、CoA ポートの値は 1700 となります。
Enable KeyWrap	PEAP、EAP-FAST、および EAP-TLS 認証での RADIUS キー ラップの共有秘密キーをイネーブルにする場合にオンにします。キーはそれぞれ一意で、RADIUS 共有キーとは明確に区別される必要があります。これらの共有キーは、AAA クライアントごとに設定できます。
Key Encryption Key (KEK)	Pairwise Master Key（PMK）の暗号化に使用します。入力するキーの長さは、ASCII モードで 16 文字、16 進数モードで 32 文字となります。
Message Authentication Code Key (MACK)	RADIUS メッセージに対して keyed キー付きハッシュ メッセージ認証コード（HMAC）を計算するのに使用します。 入力するキーの長さは、ASCII モードで 20 文字、16 進数モードで 40 文字となります。
Key Input Format	ASCII または 16 進数ストリングとしてキーを入力します。デフォルトは 16 進数です。
Security Group Access	Cisco Security Group Access 機能をイネーブルにした場合にだけ表示されます。ネットワーク デバイスで Security Group Access 機能を使用する場合にオンにします。ネットワーク デバイスがシード デバイス（Security Group Access ネットワーク内の最初のデバイス）である場合、[RADIUS] チェックボックスもオンにする必要があります。
ID	このデバイスの Security Group Access の識別に使用される名前。デフォルトでは、設定済みのデバイス名を使用できます。別の名前を使用する場合は、[Use device name for Security Group Access identification] チェックボックスをオフにして、[Identification] フィールドに名前を入力します。
Password	Security Group Access 認証パスワード。
Security Group Access Advanced Settings	追加の Security Group Access フィールドを表示する場合にオンにします。
Other Security Group Access devices to trust this device	デバイスのピア デバイスすべてによってこのデバイスが信頼されるかどうかを指定します。デフォルトはオンです。ピア デバイスでこのデバイスが信頼され、このデバイスから受信するパケットの SGT は変更されません。 このチェックボックスをオフにした場合、ピア デバイスによって、このデバイスからのパケットが関連するピア SGT で塗り替えられます。
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	ピア認可ポリシーの有効期限を指定します。ACS によって、この情報はピア ポリシー要求への応答でデバイスに返されます。デフォルトは 1 日です。
Download SGACL lists every: Weeks Days Hours Minutes Seconds	SGACL リストの有効期限を指定します。ACS によって、この情報は SGACL リストの要求への応答でデバイスに返されます。デフォルトは 1 日です。

表 7-5　[Network Devices and AAA Clients Properties] ページ （続き）

オプション	説明
Download environment data every: Weeks Days Hours Minutes Seconds	環境データの有効期限を指定します。ACS によって、この情報は環境データの要求への応答でデバイスに返されます。デフォルトは 1 日です。
Re-authentication every: Weeks Days Hours Minutes Seconds	dot1x（.1x）再認証期間を指定します。ACS によって、これはサプリカントに対して設定され、この情報はオーセンティケータに返されます。デフォルトは 1 日です。

関連トピック：

- 「ネットワーク デバイスの一括操作の表示および実行」（P.7-6）
- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）

ネットワーク デバイスの削除

ネットワーク デバイスを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

[Network Devices] ページが表示され、設定済みのネットワーク デバイスのリストが示されます。

ステップ 2　削除するネットワーク デバイスの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[Network Devices] ページが表示されます。このとき、削除されたネットワーク デバイスは表示されません。ネットワーク デバイスがデバイス リポジトリから削除されます。

デフォルトのネットワーク デバイスの設定

要求の処理時に、ACS はネットワーク デバイス リポジトリを検索して、その要求で示されている IP アドレスと一致する IP アドレスを持つネットワーク デバイスを見つけます。この検索で一致するアドレスが見つからなかった場合、ACS では、RADIUS 要求または TACACS+ 要求に対して、デフォルトのネットワーク デバイス定義を使用します。

デフォルトのネットワーク デバイスによって、使用する共有秘密情報が定義され、また、デフォルトのネットワーク デバイス定義を使用する、RADIUS 要求または TACACS+ 要求のための NDG 定義も提供されます。

[Network Resources] > [Default Network Device] を選択して、デフォルトのネットワーク デバイスを設定します。[Default Network Device] ページが表示され、表 7-6 で説明されている情報が表示されます。

表 7-6　[Default Network Device] ページ

オプション	説明
Default Network Device	
デフォルトのデバイス定義は、デバイスの IP アドレスと一致する特定のデバイス定義が見つからなかった場合に任意で使用できます。	
Default Network Device Status	ドロップダウン リスト ボックスから [Enabled] を選択して、デフォルトのネットワーク デバイスをアクティブ状態にします。
Network Device Groups	
Location	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Location ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Device Type	[Select] をクリックして、[Network Device Groups] 選択ボックスを表示します。ネットワーク デバイスに関連付ける Device Type ネットワーク デバイス グループの隣にあるオプション ボタンをクリックします。 ネットワーク デバイス グループの作成については、「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。
Authentication Options	
TACACS+	Cisco IOS TACACS+ プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。 ネットワーク デバイスが Management Center for Firewalls などのシスコ デバイス管理アプリケーションである場合は、このオプションを使用する必要があります。ネットワーク デバイスが Cisco アクセス サーバ、ルータ、またはファイアウォールである場合は、このオプションを使用する必要があります。
Shared Secret	ネットワーク デバイスの共有秘密情報（TACACS+ プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Single Connect Device	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを選択します。 • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が ACS で使用されます。
RADIUS	RADIUS プロトコルを使用してネットワーク デバイスとの通信を認証する場合にオンにします。
Shared Secret	ネットワーク デバイスの共有秘密情報（RADIUS プロトコルをイネーブルにした場合）。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。

表 7-6　[Default Network Device] ページ （続き）

オプション	説明
CoA Port	ユーザ認証用に、RAIUS CoA ポートをセッション ディレクトリに設定する場合に使用します。このセッション ディレクトリは、[Monitoring and Troubleshooting Viewer] ページから起動できます。デフォルトでは、CoA ポートの値は 1700 となります。
Enable KeyWrap	PEAP、EAP-FAST、および EAP-TLS 認証での RADIUS キー ラップの共有秘密キーをイネーブルにする場合にオンにします。キーはそれぞれ一意で、RADIUS 共有キーとは明確に区別される必要があります。これらの共有キーは、AAA クライアントごとに設定できます。
Key Encryption Key (KEK)	Pairwise Master Key（PMK）の暗号化に使用します。入力するキーの長さは、ASCII モードで 16 文字、16 進数モードで 32 文字となります。
Message Authentication Code Key (MACK)	RADIUS メッセージに対して keyed キー付きハッシュ メッセージ認証コード（HMAC）を計算するのに使用します。 入力するキーの長さは、ASCII モードで 20 文字、16 進数モードで 40 文字となります。
Key Input Format	ASCII または 16 進数ストリングとしてキーを入力します。デフォルトは 16 進数です。

関連トピック

- 「ネットワーク デバイス グループ」（P.7-2）
- 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）
- 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）

外部プロキシ サーバの使用

ACS 5.4 は、RADIUS および TACACS+ サーバとしても RADIUS および TACACS+ プロキシ サーバとしても機能できます。プロキシ サーバとして機能する場合、ACS は NAS から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS または TACACS+ サーバに転送します。

ACS は要求の結果を受け入れて NAS に返します。ACS が要求を外部 RADIUS または TACACS+ サーバに転送するように、この外部 RADIUS または TACACS+ サーバを ACS で設定する必要があります。タイムアウト時間および接続試行回数を定義できます。

ACS は、複数の外部 RADIUS または TACACS+ サーバへのプロキシ サーバとして同時に機能できます。

RADIUS プロキシ サーバはループ シナリオを処理できるのに対し、TACACS+ プロキシ サーバはできません。

（注）　ここで設定した外部 RADIUS または TACACS+ サーバは、RADIUS または TACACS+ プロキシ サーバ タイプのアクセス サービスで使用できます。

ここでは、次の内容について説明します。

- 「外部プロキシ サーバの作成、複製、および編集」（P.7-21）
- 「外部プロキシ サーバの削除」（P.7-22）

外部プロキシ サーバの作成、複製、および編集

外部プロキシ サーバを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [External Proxy Servers] を選択します。

[External Proxy Servers] ページが表示され、設定されているサーバのリストが示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する外部プロキシ サーバの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する外部プロキシ サーバ名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[External Proxy Servers] ページが表示されます。

ステップ 3　表 7-7 に従い、[External Proxy Servers] ページのフィールドを編集します。

表 7-7　[External Policy Servers] ページ

オプション	説明
General	
Name	外部 RADIUS または TACACS+ サーバの名前。
Description	（任意）外部 RADIUS または TACACS+ サーバの説明。
Server Connection	
Server IP Address	外部 RADIUS または TACACS+ サーバの IP アドレス。これは、IPv4 または IPv6 アドレスにできます。アドレスがサポートされる形式で入力されると、ACS 5.4 はその IP アドレスを検証します。入力された形式が正しくない場合は、エラー メッセージを表示します。
Shared Secret	外部 RADIUS または TACACS+ サーバの認証に使用される、ACS と外部 RADIUS または TACACS+ サーバ間の共有秘密情報。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証されるようにこれらの情報を提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。 [Show/Hide] ボタンはプレーン テキストまたは非表示の形式の共有秘密を表示するために利用できます。
Advanced Options	
RADIUS	RADIUS プロキシ サーバを作成することを選択します。RADIUS は IPv4 アドレスのみをサポートします。
TACACS+	TACACS+ プロキシ サーバを作成することを選択します。TACACS+ は、IPv4 アドレスおよび IPv6 アドレスをサポートします。
Cisco Secure ACS	デフォルトの選択。RADIUS と TACACS+ の両方をサポートします。IPv4 アドレスを使用する場合に、[Cisco Secure ACS] を選択できます。
Authentication Port	RADIUS 認証ポート番号。デフォルト値は 1812 です。
Accounting Port	RADIUS アカウンティング ポート番号。デフォルト値は 1813 です。
Server Timeout	ACS が外部 RADIUS サーバからの応答を待つ秒数。デフォルトは 5 秒です。有効な値の範囲は 1 ～ 999 です。

表 7-7　[External Policy Servers] ページ （続き）

オプション	説明
Connection Attempts	ACS が外部 RADIUS サーバへの接続を試みる回数。デフォルトは 3 回に設定されています。有効値は 1 ～ 99 です。
Connection Port	TACACS+ 接続ポート。デフォルトは 49 です。
Network Timeout	ACS が外部 TACACS+ サーバからの応答を待つ秒数。デフォルトは 20 秒です。

ステップ 4　[Submit] をクリックして変更を保存します。

外部プロキシ サーバの設定が保存されます。[External Proxy Server] ページが表示され、新しい設定が示されます。

（注） ACS で未知の RADIUS 属性を転送する場合は、プロキシの VSA を定義する必要があります。

関連トピック

- 「RADIUS および TACACS+ プロキシ サービス」（P.3-7）
- 「RADIUS および TACACS+ プロキシ要求」（P.4-30）
- 「アクセス サービスの一般プロパティの設定」（P.10-13）
- 「外部プロキシ サーバの削除」（P.7-22）

外部プロキシ サーバの削除

外部プロキシ サーバを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [External Proxy Servers] を選択します。

[External Proxy Servers] ページが表示され、設定されているサーバのリストが示されます。

ステップ 2　削除する外部 RADIUS または TACACS+ サーバの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

[External Proxy Servers] ページが表示されます。このとき、削除されたサーバは表示されません。

OCSP サービスの使用

ACS 5.4 では、新しいプロトコル、Online Certificate Status Protocol（OCSP）が導入されています。これは、x.509 デジタル証明書の状態を検査するために使用されます。このプロトコルは、証明書失効リスト（CRL）の代替として使用できます。また、CRL の処理時に生じる問題に対処することもできます。

ACS 5.4 は HTTP で OCSP サービスと通信して、認証における証明書の状態を検証します。OCSP は再利用可能なコンフィギュレーション オブジェクトで設定され、OCSP は、ACS で設定されている任意の認証局（CA）証明書から参照できます。複数の CA のオブジェクトが同じ OCSP サービスを参照できます。

ACS で最大 2 台の OCSP サーバを設定できます。これらはプライマリおよびセカンダリ OCSP サーバと呼ばれます。ACS はプライマリ OCSP サーバとの通信中にタイムアウトが発生した場合にセカンダリ OCSP サーバと通信します。

OCSP は、特定の証明書要求に次の 3 つの値を返す可能性があります。

- Good：証明書は使用に適しています。
- Revoked：証明書は取り消されています。
- Unknown：証明書ステータスは不明です。
  特定の証明書 CA を処理するように OCSP が設定されていない場合、証明書のステータスは不明です。この場合、証明書は不明な証明書として扱われます。つまり、検証プロセスは *Reject the request if no status* フラグを検査します。要求が拒否されないようにフラグがセットされている場合、OCSP は証明書が ACS に設定されているかどうかの検査を CRL まで続けます。

ACS は、すべての OCSP 応答をキャッシュします。これは、パフォーマンスを最大化し、OCSP サーバの負荷を軽減するためです。OCSP の検証時に、ACS はキャッシュの関連情報を最初に検索します。関連情報が見つからない場合、ACS は OCSP サーバへの接続を確立します。ACS は各 OCSP サービスのすべての OCSP レコードの有効期間を定義します。また、各 OCSP 応答に、新しい要求を行うまでの間隔を定義する存続可能時間があります。各キャッシュ エントリは、存続可能時間またはキャッシュ有効期間のいずれか短い方の間、保持されます。この OCSP サービスに関連付けられたすべてのキャッシュ レコードを取りクリアするには、[Clear Cache] をクリックします。[Clear Cache] は、分散型システムのセカンダリ ACS サーバのレコードもクリアします。

ACS は、キャッシュされた応答データベースのレプリケーションをサポートしません。キャッシュは永続的でないため、キャッシュされた応答は、ACS アプリケーションを再起動した後でクリアされます。

ここでは、次の内容について説明します。

- 「OCSP サーバの作成、複製、および編集」（P.7-23）
- 「OCSP サーバの削除」（P.7-25）

OCSP サーバの作成、複製、および編集

OCSP サーバを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Network Resources] > [OCSP Services] を選択します。

[OCSP Services] ページが表示され、設定されている OCSP サーバのリストが示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する OCSP サーバの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する OCSP サーバ名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[OCSP Servers] ページが表示されます。

ステップ 3　表 7-8 に従い、[OCSP Servers] ページのフィールドを編集します。

表 7-8　[OCSP Servers] ページ

オプション	説明
Name	OCSP サーバの名前。
Description	（任意）OCSP サーバの説明。
Server Connection	
Enable Secondary Server	[Always Access Primary Server First] および [Failback] オプションなどのセカンダリ サーバ設定を有効にするには、このチェックボックスをオンにします。
Always Access Primary Server First	プライマリ サーバから直前の応答がなかった場合でも、セカンダリ サーバに進む前にプライマリ サーバを最初に確認するには、このオプションを有効にします。
Failback To Primary Server	プライマリが完全にダウンしたときにセカンダリ サーバを指定した時間だけ使用するには、このオプションを有効にします。時間の範囲は 1 ～ 999 分です。
Primary Server	
URL	プライマリ サーバの URL または IP アドレスを入力します。
Enable Nonce Extension Support	OCSP 要求にナンスを使用する場合に、このチェックボックスをオンにします。 このオプションは、OCSP 要求にランダムな番号を含めます。このオプションを選択すると、要求に含まれる番号と応答で受信される番号を比較します。ナンスは、古い通信が再利用されないようにします。 ナンスは Windows 2008 サーバで設定できます。ACS サーバからのナンスが Windows サーバと一致しない場合、Windows は無許可応答を返します。そのため、ACS は要求に失敗し、これを不明な証明書であると見なします。
Validate Response Signature	OCSP 応答側に応答に次のシグニチャの 1 つを含めるように指示するには、このチェックボックスをオンにします。 • CA 証明書 • CA 証明書とは別の証明書 ACS は、OCSP 応答署名に基づいて、応答の証明書を検証します。OCSP 応答署名が見つからない場合、ACS は応答に失敗し、証明書のステータスを判断できません。
Network Timeout	ACS がプライマリ OCSP サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は、1 ～ 999 秒です。
Secondary Server	
URL	セカンダリ サーバの URL または IP アドレスを入力します。
Enable Nonce Extension Support	OCSP 要求にナンスを使用する場合に、このチェックボックスをオンにします。 このオプションは、OCSP 要求にランダムな番号を含めます。このオプションを選択すると、要求に含まれる番号と応答で受信される番号を比較します。ナンスは、古い通信が再利用されないようにします。 ナンスは Windows 2008 サーバで設定できます。ACS サーバからのナンスが Windows サーバと一致しない場合、Windows は無許可応答を返します。そのため、ACS は要求に失敗し、これを不明な証明書であると見なします。
Validate Response Signature	OCSP 応答側に応答に次のシグニチャの 1 つを含めるように指示するには、このチェックボックスをオンにします。 • CA 証明書 • CA 証明書とは別の証明書 ACS は、OCSP 応答署名に基づいて、応答の証明書を検証します。OCSP 応答署名が見つからない場合、ACS は応答に失敗し、証明書のステータスを判断できません。

表 7-8　[OCSP Servers] ページ （続き）

オプション	説明
Network Timeout	ACS がプライマリ OCSP サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値の範囲は 1 ～ 999 です。
Response Cache	
Cache Entry Time To Live	新しい OCSP 要求を行うまでの間隔を定義します。分単位の値を入力します。デフォルト値は 300 分です。
Clear Cache	すべての関連する認証局に選択された OCSP サービスのキャッシュをクリアします。 [Clear Cache] オプションでは、展開内のこの OCSP サービスに関連付けられているすべてのノードと対話できます。このオプションは、選択すると更新された状態も表示します。

ステップ 4　[Submit] をクリックして変更を保存します。

OCSP サーバの設定が保存されます。[OCSP Server] ページが表示され、新しい設定が示されます。

関連トピック

- 「OCSP サーバの削除」（P.7-25）

OCSP サーバの削除

OCSP サーバを削除するには、次の手順を実行します。

ステップ 1　[Network Resources] > [OCSP Services] を選択します。

[OCSP Services] ページが表示され、設定されている OCSP サーバのリストが示されます。

ステップ 2　削除する OCSP サーバの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

[OCSP Servers] ページが表示されます。このとき、削除されたサーバは表示されません。

CHAPTER 8

ユーザおよび ID ストアの管理

概要

ACS は、ACS ネットワーク リソース リポジトリおよび ID ストアを使用して、ネットワーク デバイスおよびその他の ACS クライアントを管理します。特定のネットワーク リソースへのアクセスを要求するホストが ACS を介してネットワークに接続すると、ACS はホストを認証し、ホストがネットワーク リソースと通信できるかどうかを決定します。

ユーザまたはホストを認証および認可するために、ACS は ID ストア内のユーザ定義を使用します。ID ストアには、次の 2 つのタイプがあります。

- 内部：ACS がローカルで保持する ID ストア（ローカル ストアとも呼ばれる）は*内部 ID ストア*と呼ばれます。内部 ID ストアの場合、ACS はユーザがユーザ レコードを設定および保持するためのインターフェイスを提供します。
- 外部：ACS の外部に存在する ID ストアは*外部 ID ストア*と呼ばれます。ACS は、これらの外部 ID ストアに接続し、認証を実行してユーザ情報を取得するために、設定情報を必要とします。

ユーザおよびホストを認証する以外に、ほとんどの ID ストアはユーザおよびホストに関連付けられている属性を返します。要求の処理中にポリシー条件でこれらの属性を使用でき、RADIUS 属性について返された値を認可プロファイルに読み込むこともできます。

内部 ID ストア

ACS では、ユーザ レコードおよびホスト レコードを保持するために、さまざまな内部 ID ストアが保持されます。ID ストアごとに、その特定のストアに関連付けられた ID 属性を定義できます。ユーザ レコードまたはホスト レコードの作成中に、このストアに対して値が定義されます。

これらの ID 属性は、ACS アプリケーションの [System Administration] セクションで ID ディクショナリの一部として定義できます（[System Administration] > [Configuration] > [Dictionaries] > [Identity]）。

各内部ユーザ レコードにはパスワードが含まれており、2 番めのパスワードを TACACS+ イネーブル パスワードとして定義できます。内部ユーザ ID ストアに保存されるパスワードは、特定の期間後に失効してユーザに自分のパスワードを定期的に変更させるように設定できます。

ユーザは、自分のパスワードを RADIUS または TACACS+ プロトコルで変更するか、UCP Web サービスを使用できます。パスワードは、ACS で定義するパスワード複雑度基準に準拠している必要があります。

内部ユーザ レコードは、固定および設定可能という 2 つのコンポーネント タイプで構成されます。

固定コンポーネントは次のとおりです。

- 名前
- 説明
- パスワード
- イネーブルまたはディセーブルのステータス
- ユーザが所属する ID グループ

設定可能コンポーネントは次のとおりです。

- TACACS+ 認証のイネーブル パスワード
- ユーザ定義の表示および入力方法を決定する ID 属性のセット

ユーザを作成する前に ID 属性を設定することを推奨します。ID 属性が設定されると、次のことを実行できます。

- ユーザ定義の一部として、対応する値を入力できます。
- ユーザが認証するときに、ポリシー決定で使用できます。
- RADIUS 属性について返された値を認可プロファイルに読み込むために使用できます。

内部ユーザ ID 属性は、ユーザのセッション継続中にユーザに適用されます。

内部 ID ストアには、内部ユーザを認証するために使用される内部ユーザ属性およびクレデンシャル情報が含まれています。

内部ホスト レコードは内部ユーザ レコードに類似していますが、パスワード情報が含まれていません。ホストは MAC アドレスによって識別されます。内部 ID ストアの管理については、「内部 ID ストアの管理」（P.8-4）を参照してください。

外部 ID ストア

外部 ID ストアは外部データベースであり、ACS はこれに基づいて内部ユーザおよび外部ユーザの認証を実行します。ACS 5.4 では、次の外部 ID ストアがサポートされます。

- LDAP
- Active Directory
- RSA SecurID トークン サーバ
- RADIUS ID サーバ

外部 ID ストアのユーザ レコードには、特定のストアにアクセスするために必要な設定パラメータが含まれています。RSA SecurID トークン サーバを除くすべての外部 ID ストアで、ユーザ レコードの属性を定義できます。外部 ID ストアには、ACS サーバ証明書の証明書情報および証明書認証プロファイルも含まれています。

外部 ID ストアの管理方法の詳細については、「外部 ID ストアの管理」（P.8-19）を参照してください。

2 要素認証の ID ストア

RSA SecurID トークン サーバおよび RADIUS ID サーバを使用すると、2 要素認証を実現できます。これらの外部 ID ストアでは、セキュリティを強化する OTP が使用されます。これらの外部 ID ストアに対して、次の追加設定オプションを使用できます。

- ID キャッシング：ACS の ID キャッシングをイネーブルにすると、認証が実行されない場合に、要求の処理中に ID ストアを使用できます。ユーザ認証なしでユーザ ルックアップを実行できる LDAP や AD とは異なり、RSA SecurID トークン サーバと RADIUS ID サーバではユーザ ルックアップはサポートされません。

  たとえば、認証が実行されないために ID ストアでデータを取得できない場合に備えて、認証要求とは別に TACACS+ 要求を認可するため、ユーザに対して正常に行われた最後の認証から取得した結果と属性をキャッシュするように、ID キャッシングをイネーブルにすることができます。このキャッシュを使用して、要求を認可できます。

- 認証拒否の処理：RSA および RADIUS ID ストアでは、認証試行が拒否された場合、次の結果は区別されません。
  - Authentication Failed
  - User Not Found

  この区別は、フェール オープン操作を決定する場合に重要です。設定オプションが使用可能であり、いずれの結果を使用する必要があるかを定義できます。

ID グループ

ID グループは、階層内に定義される論理エンティティであり、ユーザおよびホストに関連付けられます。これらの ID グループは、ポリシー決定を行うために使用されます。内部ユーザおよびホストの場合、ID グループはユーザまたはホスト定義の一部として定義されます。

外部 ID ストアが使用される場合は、外部 ID ストアから取得された属性およびグループを ACS ID グループにマッピングするために、グループ マッピング ポリシーが使用されます。ID グループは、Active Directory のグループと概念は似ていますが、より基本的な性質を持ちます。

証明書ベースの認証

ユーザおよびホストは、証明書ベースのアクセス要求を使用して自身を識別できます。この要求を処理するには、ID ポリシーに証明書認証プロファイルを定義する必要があります。

証明書認証プロファイルには、ユーザまたはホストの識別に使用される証明書の属性が含まれます。また任意で、要求に存在する証明書の検証に使用できる LDAP ID ストアまたは AD ID ストアを含めることもできます。証明書および証明書ベースの認証の詳細については、次の項を参照してください。

- 「CA 証明書の設定」（P.8-69）
- 「証明書認証プロファイルの設定」（P.8-73）

ID 順序

要求の処理に複数の ID ストアおよびプロファイルが使用される複雑な条件を設定できます。これらの ID 方式は、ID 順序オブジェクト内に定義できます。順序内の ID 方式のタイプは任意です。

ID 順序は、認証用と属性取得用の 2 つのコンポーネントで構成されます。

- 証明書に基づく認証の実行を選択した場合は、単一の証明書認証プロファイルが使用されます。
- ID データベースに基づく認証の実行を選択した場合は、認証が成功するまで順番にアクセスされる ID データベースのリストを定義できます。認証が成功すると、データベース内の属性が取得されます。

また、追加属性を取得できる任意のデータベースのリストを設定することもできます。これらの追加データベースは、パスワードベースの認証を使用するか証明書ベースの認証を使用するかに関係なく、設定できます。

証明書ベースの認証を実行する場合、ユーザ名は証明書属性から読み込まれ、このユーザ名がリスト内のすべてのデータベースから属性を取得するために使用されます。証明書属性の詳細については、「CA 証明書の設定」（P.8-69）を参照してください。

ユーザについて一致するレコードが見つかると、対応する属性が取得されます。ACS では、アカウントがディセーブルのユーザやパスワードに変更のマークが付いているユーザについても、属性が取得されます。

（注）　ディセーブルの内部ユーザ アカウントは、属性のソースとして使用できますが、認証のソースとしては使用できません。

ID 順序の詳細については、「ID ストア順序の設定」（P.8-75）を参照してください。

この章の内容は、次のとおりです。

- 「内部 ID ストアの管理」（P.8-4）
- 「外部 ID ストアの管理」（P.8-19）
- 「CA 証明書の設定」（P.8-69）
- 「証明書認証プロファイルの設定」（P.8-73）
- 「ID ストア順序の設定」（P.8-75）

内部 ID ストアの管理

ACS には、ユーザ用の内部 ID ストアとホスト用の内部 ID ストアがあります。

- ユーザ用の内部 ID ストアは、ユーザ、ユーザ属性、およびユーザ認証オプションのリポジトリです。
- ホスト用の内部 ID ストアには、MAC Authentication Bypass（ホスト ルックアップ）のホストに関する情報が含まれています。

各ユーザおよびホストを ID ストア内に定義でき、ユーザおよびホストのファイルをインポートできます。

ユーザ用の内部 ID ストアは、展開内のすべての ACS インスタンスで共有され、各ユーザについて次の内容を含んでいます。

- 標準属性

- ユーザ属性
- 認証情報

（注）　ACS 5.4 では、内部 ID ストアに対してだけ、内部ユーザの認証がサポートされます。

ここでは、次の内容について説明します。

- 「認証情報」（P.8-5）
- 「ID グループ」（P.8-6）
- 「ID 属性の管理」（P.8-7）
- 「ユーザの認証設定の設定」（P.8-9）
- 「内部ユーザの作成」（P.8-11）
- 「内部 ID ストア ユーザの一括操作の表示および実行」（P.8-15）
- 「ID ストアでのホストの作成」（P.8-16）
- 「内部 ID ストア ホストの一括操作の表示および実行」（P.8-18）

認証情報

ユーザの TACACS+ イネーブル パスワードを定義する内部ユーザ レコードの一部として保存される、追加パスワードを設定できます。このパスワードによって、デバイスへのアクセス レベルが設定されます。このオプションを選択しない場合、標準ユーザ パスワードが TACACS イネーブルにも使用されます。

システムが TACACS+ イネーブル操作に使用されていない場合は、このオプションを選択しないでください。

ID ストア順序機能を使用するには、順番にアクセスされる ID ストアのリストを定義します。同じ ID ストアを認証順序リストと属性取得順序リストに含めることができます。ただし、ID ストアが認証用に使用される場合、追加属性を取得するために ID ストアにアクセスされることはありません。

証明書ベースの認証の場合、ユーザ名は証明書属性から読み込まれ、属性取得用に使用されます。

認証プロセス中に、ユーザまたはホストの複数のインスタンスが内部 ID ストアに存在する場合、認証は失敗します。アカウントがディセーブルのユーザやパスワード変更が必要なユーザについて、属性は取得されます（ただし、認証は拒否されます）。

次のような失敗が ID ポリシーの処理中に発生する場合があります。

- 認証失敗。考えられる原因としては、不正なクレデンシャル、ディセーブルなユーザなどがあります。
- ユーザまたはホストが認証データベースに存在しない。
- 定義されているデータベースへのアクセス中に失敗が発生した。

フェール オープン オプションを定義して、これらの失敗が発生したときに実行するアクションを設定できます。

- 拒否：拒否応答を送信します。
- ドロップ：応答を送信しません。
- 続行：サービス内の次の定義済みポリシーへ処理を続行します。

システム属性 *AuthenticationStatus* に、ID ポリシー処理の結果が保持されます。失敗の発生時にポリシー処理を続行することを選択する場合、後続のポリシー処理の条件でこの属性を使用して、ID ポリシー処理が成功しなかった場合を区別できます。

PAP/ASCII、EAP-TLS、または EAP-MD5 で認証が失敗した場合、処理を続行できます。その他のすべての認証プロトコルでは、要求は拒否され、この結果に対するメッセージがロギングされます。

ID グループ

各内部ユーザを 1 つの ID グループに割り当てることができます。ID グループは、階層構造で定義されます。ユーザに関連付けられる論理エンティティですが、付けられた名前以外のデータや属性は含まれていません。

ポリシー条件で ID グループを使用して、同じポリシー結果が適用されるユーザの論理グループを作成します。内部 ID ストア内の各ユーザを単一の ID グループに関連付けることができます。

ACS でユーザの要求が処理されるときに、そのユーザの ID グループが取得され、規則テーブルの条件で使用可能になります。ID グループは、階層構造になっています。

グループ マッピング ポリシーを使用して、外部 ID ストア内の ID グループおよびユーザを ACS の ID グループにマッピングできます。

ID グループの作成

ID グループを作成するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Identity Groups] を選択します。

[Identity Groups] ページが表示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する ID グループの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する ID グループ名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。
- [File Operations] をクリックして、次の操作を実行します。
  - Add：ID グループをインポートから ACS に追加します。
  - Update：ACS 内の既存の ID グループを、インポートのリストで上書きします。
  - Delete：インポートにリストされている ID グループを ACS から削除します。
- [Export] をクリックして、ID グループのリストをローカル ハードディスクにエクスポートします。

  [File Operations] オプションの詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。

[Create]、[Duplicate]、または [Edit] オプションを選択すると、[Create] ページまたは [Edit] ページが表示されます。

ステップ 3　次のフィールドに情報を入力します。

- [Name]：ID グループの名前を入力します。ID グループを複製する場合は、固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
- [Description]：ID グループの説明を入力します。
- [Parent]：[Select] をクリックして、ID グループのネットワーク デバイス グループの親を選択します。

ステップ 4　[Submit] をクリックして変更を保存します。

ID グループの設定が保存されます。[Identity Groups] ページが新しい設定で表示されます。新しい ID グループを作成した場合は、このページの階層内で親 ID グループ選択の下に配置されます。

関連トピック

- 「ユーザおよび ID ストアの管理」（P.8-1）
- 「内部 ID ストアの管理」（P.8-4）
- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）
- 「ID グループ」（P.8-3）
- 「ID グループの作成」（P.8-6）
- 「ID グループの削除」（P.8-7）

ID グループの削除

ID グループを削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Identity Groups] を選択します。

[Identity Groups] ページが表示されます。

ステップ 2　削除する ID グループの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のエラー メッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

[Identity Groups] ページが表示されます。このとき、削除した ID グループは表示されません。

関連項目

- 「ID 属性の管理」（P.8-7）

ID 属性の管理

管理者は、ポリシー条件の要素となる ID 属性のセットを定義できます。ACS 5.4 ポリシー モデルについては、第 3 章「ACS 5.x ポリシー モデル」を参照してください。認証時に、ID 属性がポリシー条件の一部である場合に内部データ ストアから取得されます。

ACS 5.4 は ID 要素と連携動作して、ユーザを認証し、ACS ポリシーへの入力のために属性を取得します。

属性定義には、関連付けられたデータ型および有効な値が含まれています。値のセットは、型によって異なります。たとえば、型が *integer* の場合、定義には有効な範囲が含まれます。ACS 5.4 には、属性値がない場合に使用できるデフォルト値の定義があります。デフォルト値により、すべての属性は少なくとも 1 つの値を持ちます。

関連トピック

- 「標準属性」（P.8-8）

- 「ユーザ属性」（P.8-8）
- 「ホスト属性」（P.8-9）

標準属性

表 8-1 に、内部ユーザ レコードの標準属性を示します。

表 8-1　標準属性

属性	説明
Username	ACS は、認証要求のユーザ名に対してこのユーザ名を比較します。比較では大文字と小文字は区別されません。
Status	• イネーブル ステータスは、アカウントがアクティブであることを示します。 • ディセーブル ステータスは、ユーザ名の認証が失敗することを示します。
Description	属性のテキスト説明。
Identity Group	ACS は各ユーザを ID グループに関連付けます。詳細については、「ID 属性の管理」（P.8-7）を参照してください。

ユーザ属性

管理者は、ID 属性のセットからユーザ定義の属性を作成および追加できます。内部 ID ストア内のユーザごとにこれらの属性のデフォルト値を割り当て、デフォルト値が必須か任意かを定義できます。

ACS でユーザを定義する必要があります。各内部ユーザと ID グループとの関連付け、説明（任意）、パスワード、イネーブル パスワード（任意）、内部および外部ユーザ属性などです。

内部ユーザは、固定および設定可能という 2 つのコンポーネントで定義されます。固定コンポーネントは、次の属性で構成されます。

- 名前
- 説明
- パスワード
- イネーブルまたはディセーブルのステータス
- 所属する ID グループ

設定可能コンポーネントは、次の属性で構成されます。

- TACACS+ 認証のイネーブル パスワード
- ユーザ定義の表示および入力方法を決定する ID 属性のセット

ユーザを作成する前に ID 属性を設定することを推奨します。ID 属性が設定されると、次のことを実行できます。

- ユーザ定義の一部として、対応する値を入力できます。
- ユーザが認証するときに、ポリシー決定で使用できます。

内部ユーザ ID 属性は、ユーザのセッション継続中にユーザに適用されます。

内部 ID ストアには、（ポリシーで定義したように）内部ユーザを認証するために使用される内部ユーザ属性およびクレデンシャル情報が含まれています。

外部 ID ストアは外部データベースであり、これに基づいて（ポリシーで定義したように）内部ユーザおよび外部ユーザのクレデンシャルおよび認証の確認を実行します。

ACS 5.4 では、自分のポリシー内で使用する ID 属性を次の順序で設定できます。

1. （ユーザ ディクショナリを使用して）ID 属性を定義します。
2. ポリシーで使用するカスタム条件を定義します。
3. 内部データベースの各ユーザの値を読み込みます。
4. この条件に基づいて規則を定義します。

ACS 5.4 およびユーザの ID 属性について理解が深まると、ポリシー自体はより堅牢で複雑になっていきます。

ユーザ定義の属性値を使用して、ポリシーおよび認可プロファイルを管理できます。ユーザ属性の作成方法については、「内部ユーザ ID 属性の作成、複製、および編集」（P.18-10）を参照してください。

ホスト属性

内部ホスト用の追加属性を設定できます。内部ホストを作成するときに、次のことを実行できます。

- ホスト属性の作成
- ホスト属性へのデフォルト値の割り当て
- デフォルト値が必須か任意かの定義

これらのホスト属性に対して値を入力でき、その値を使用してポリシーおよび認可プロファイルを管理できます。ホスト属性の作成方法については、「内部ホスト ID 属性の作成、複製、および編集」（P.18-13）を参照してください。

ユーザの認証設定の設定

ACS でユーザ アカウントの認証設定を設定して、ユーザに強力なパスワードの使用を強制できます。[Authentication Settings] ページで行うパスワード ポリシー変更は、すべての内部 ID ストア ユーザ アカウントに適用されます。[User Authentication Settings] ページには、次のタブがあります。

- Password Complexity
- Advanced

パスワード ポリシーを設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Users] > [Authentication Settings] を選択します。

[Password Complexity] タブおよび [Advanced] タブがある [User Authentication Settings] ページが表示されます。

ステップ 2　[Password Complexity] タブで、ユーザ パスワードの設定に使用する各チェックボックスをオンにします。

表 8-2 に、[Password Complexity] タブのフィールドを示します。

表 8-2　[Password Complexity] タブ

オプション	説明
Applies to all ACS internal identity store user accounts	
Minimum length	必要な最小長。有効なオプションは 4 ～ 20 です。
Password may not contain the username	パスワードにユーザ名またはユーザ名を逆にしたものを使用できるかどうか。

表 8-2　[Password Complexity] タブ （続き）

オプション	説明
Password may not contain 'cisco'	パスワードに *cisco* という単語を使用できないことを指定する場合にオンにします。
Password may not contain	入力した文字列をパスワードに使用しないことを指定する場合にオンにします。
Password may not contain repeated characters four or more times consecutively	パスワードで文字を 4 回以上連続して繰り返すことができないことを指定する場合にオンにします。
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	パスワードには、アルファベットの小文字が少なくとも 1 文字含まれている必要があります。
Upper case alphabetic characters	パスワードには、アルファベットの大文字が少なくとも 1 文字含まれている必要があります。
Numeric characters	パスワードには、数字が少なくとも 1 文字含まれている必要があります。
Non alphanumeric characters	パスワードには、英数字以外の文字が少なくとも 1 文字含まれている必要があります。

ステップ 3　[Advanced] タブで、ユーザ認証プロセスに対して設定する基準の値を入力します。表 8-3 に、[Advanced] タブのフィールドを示します。

表 8-3　[Advanced] タブ

オプション	説明
Account Disable	
内部ユーザのアカウントの無効化ポリシーをサポートします。	
Never	アカウントには期限がありません。これがデフォルトのオプションです。このポリシーが理由でディセーブルになっているすべての内部ユーザは、このオプションを選択するとイネーブルになります。
Disable account if Date exceeds	設定した日付を超過すると、内部ユーザがディセーブルになります。たとえば、設定された日付が 2010 年 12 月 28 日である場合、すべての内部ユーザは 2010 年 12 月 28 日の深夜 12 時にディセーブルになります。 日付には、現在のシステム日付または将来の日付を設定できます。現在のシステム日付よりも古い日付は入力できません。 日付超過オプションによってディセーブル化されたすべての内部ユーザは、日付超過オプションの設定を変更するとイネーブルになります。
Disable account if Days exceed	内部ユーザは、設定された日数を超えた場合にディセーブルになります。たとえば、あるユーザのアカウントをディセーブルにする日数の設定値が 60 日の場合、その特定のユーザのアカウントがイネーブルになってから 60 日後に、そのユーザはディセーブルになります。
Disable account if Failed Attempts Exceed	内部ユーザは、連続した失敗試行の回数が設定された値に達するとディセーブルになります。たとえば、設定された値が 5 の場合、連続した失敗試行回数が 5 に達すると、その内部ユーザはディセーブルになります。
Reset current failed attempts count on submit	選択すると、すべての内部ユーザの失敗試行回数が 0 に設定されます。 [Failed Attempts Exceed] オプションによってディセーブルにされたすべての内部ユーザがイネーブルになります。
Password History	

表 8-3　[Advanced] タブ （続き）

オプション	説明
Password must be different from the previous *n* versions.	比較対象とするこのユーザの以前のパスワードの数を指定します。このオプションによって、ユーザが以前に使用したパスワードを設定できないようにします。有効なオプションは 1 ～ 99 です。
Password Lifetime	
ユーザに定期的にパスワード変更を求めることができます。	
Disable user account after *n* days if password is not changed	パスワードが変更されていない場合、*n* 日後にユーザ アカウントをディセーブルにする必要があることを指定します。有効なオプションは 1 ～ 365 です。
Display reminder after *n* days	パスワード変更の通知を *n* 日後に表示します。有効なオプションは 1 ～ 365 です。このオプションを設定すると、通知だけが表示されます。新しいパスワードは要求されません。
TACACS Enable Password	
ユーザ レコードに、イネーブル パスワードを保存する別のパスワードを定義する必要があるかどうかを選択します。	
TACACS Enable Password	TACACS 認証用の別のパスワードをイネーブルにする場合に、このチェックボックスをオンにします。

ステップ 4　[Submit] をクリックします。

ユーザ パスワードは、定義した基準を使用して設定されます。これらの基準は、以降のログインだけに適用されます。

（注） いずれかのユーザがディセーブルになった場合、失敗試行回数の値を複数回再設定する必要があります。このような場合、管理者はそのユーザの現在の失敗試行回数を別個に留意するか、すべてのユーザについて回数を 0 にリセットする必要があります。

内部ユーザの作成

ACS では、セキュリティ上の理由から外部 ID ストアにアクセスしない内部ユーザを作成できます。

一括インポート機能を使用して、数百の内部ユーザを一度にインポートできます。詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。または、ここで説明する手順に従って、内部ユーザを 1 つずつ作成できます。

ステップ 1　[Users and Identity Stores] > [Internal Identity Store] > [Users] を選択します。

[Internal Users] ページが表示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製するユーザの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するユーザ名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。
- パスワードを変更するユーザの隣にあるチェックボックスをオンにし、[Change Password] をクリックします。

  [Change Password] ページが表示されます。

ステップ 3　表 8-4 の説明に従ってフィールドに入力し、内部ユーザのパスワードを変更します。

表 8-4　[Internal User] - [Change Password] ページ

オプション	説明
Password Information	
Password Type	設定されているすべての外部 ID ストア名と、デフォルトのパスワード タイプである [Internal User] が表示されます。リストから 1 個の ID ストアを選択できます。 ユーザ認証の際に、ユーザに外部 ID ストアが設定されている場合、内部 ID ストアは外部 ID ストアに認証要求を転送します。 外部 ID ストアを選択した場合、ユーザのパスワードは設定できません。パスワード編集ボックスはディセーブルです。 パスワード タイプの外部 ID ストアとして ID 順序を使用することはできません。 [Users and Identity Stores] > [Internal Identity Stores] > [Users] ページにある [Change Password] ボタンを使用してパスワード タイプを変更できます。
Password	ユーザの現在のパスワード。[System Administration] > [Users] > [Authentication Settings] で定義したパスワード ポリシーに準拠する必要があります。
Confirm Password	ユーザのパスワード。[Password] のエントリと正確に一致する必要があります。
Change Password on Next Login	次回のユーザ ログインで、古いパスワードによる認証のあとに、ユーザのパスワードを変更するプロセスを開始する場合に、このボックスをオンにします。
Enable Password Information	
Enable Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。4 ～ 32 文字です。このオプションはディセーブルにすることができます。詳細については、「認証情報」（P.8-5）を参照してください。
Confirm Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。[Enable Password] のエントリと正確に一致する必要があります。

- [File Operations] をクリックして、次の操作を実行します。
  - Add：内部ユーザをインポートから ACS に追加します。
  - Update：ACS 内の既存の内部ユーザをインポートのユーザのリストで上書きします。
  - Delete：インポートにリストされている内部ユーザを ACS から削除します。
- [Export] をクリックして、内部ユーザのリストをローカル ハードディスクにエクスポートします。

[File Operations] オプションの詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。

[Create]、[Duplicate]、または [Edit] オプションを選択すると、[User Properties] ページが表示されます。[Edit] ビューで、ユーザの最初の作成および最終変更の情報を参照できます。この情報は編集できません。

ステップ 4　表 8-5 の説明に従って、フィールドに入力します。

表 8-5　[Users and Identity Stores] > [Internal Identity Store] > [User Properties] ページ

オプション	説明
General	
Name	ユーザ名。
Status	ドロップダウン リスト ボックスを使用して、ユーザのステータスを選択します。 • Enabled：このユーザの認証要求は許可されます。 • Disabled：このユーザの認証要求は失敗します。
Description	（任意）ユーザの説明。
Identity Group	[Select] をクリックして、[Identity Groups] ウィンドウを表示します。ID グループを選択して [OK] をクリックし、特定の ID グループを使用してユーザを設定します。
Account Disable	
Disable Account if Date Exceeds	各ユーザに対してアカウントの無効化ポリシーを使用する場合、このチェックボックスをオンにします。このオプションによって、設定した日付が超過したときに、ユーザ アカウントをディセーブルにすることができます。このオプションは、グローバルなユーザ アカウントの無効化ポリシーを上書きします。すなわち、管理者が必要に応じてユーザごとに異なる有効期限を設定できます。このオプションのデフォルト値は、アカウント作成日から 60 日後です。ユーザ アカウントは、設定された日付の深夜 12 時にディセーブルになります。
Password Information このページのこのセクションは、内部ユーザを作成した場合にだけ表示されます。 パスワードは最低 4 文字です。	
Password Type	設定されているすべての外部 ID ストア名と、デフォルトのパスワード タイプである [Internal User] が表示されます。リストから 1 個の ID ストアを選択できます。 ユーザ認証の際に、ユーザに外部 ID ストアが設定されている場合、内部 ID ストアは外部 ID ストアに認証要求を転送します。 外部 ID ストアを選択した場合、ユーザのパスワードは設定できません。パスワード編集ボックスはディセーブルです。 パスワード タイプの外部 ID ストアとして ID 順序を使用することはできません。 [Users and Identity Stores] > [Internal Identity Stores] > [Users] ページにある [Change Password] ボタンを使用してパスワード タイプを変更できます。
Password	ユーザのパスワード。[System Administration] > [Users] > [Authentication Settings] で定義したパスワード ポリシーに準拠する必要があります。
Confirm Password	ユーザのパスワード。[Password] のエントリに正確に一致する必要があります。
Change Password on next login	ユーザが次回ログインするときに、古いパスワードの認証後にユーザのパスワードを変更するプロセスを開始する場合に、このボックスをオンにします。
Enable Password Information このページのこのセクションは、内部ユーザを作成した場合にだけ表示されます。 パスワードは 4 ～ 32 文字です。	
Enable Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。4 ～ 32 文字です。このオプションはディセーブルにすることができます。詳細については、「認証情報」（P.8-5）を参照してください。
Confirm Password	（任意）内部ユーザの TACACS+ イネーブル パスワード。[Enable Password] のエントリと正確に一致する必要があります。

表 8-5　[Users and Identity Stores] > [Internal Identity Store] > [User Properties] ページ （続き）

オプション	説明
User Information	
定義されている場合、このセクションにはユーザ レコードに対して定義された追加 ID 属性が表示されます。	
Creation/Modification Information	
このページのこのセクションは、内部ユーザを作成または変更したあとにだけ表示されます。	
Date Created	*表示のみ*。ユーザのアカウントが作成された日付と時刻。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。
Date Modified	*表示のみ*。ユーザのアカウントが最後に変更（更新）された日付と時刻。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。

ステップ 5　[Submit] をクリックします。

ユーザ設定が保存されます。[Internal Users] ページが新しい設定で表示されます。

関連トピック

- 「ユーザの認証設定の設定」（P.8-9）
- 「内部 ID ストア ユーザの一括操作の表示および実行」（P.8-15）
- 「内部 ID ストアからのユーザの削除」（P.8-14）

内部 ID ストアからのユーザの削除

内部 ID ストアからユーザを削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Store] > [Users] を選択します。

[Internal Users] ページが表示されます。

ステップ 2　削除するユーザの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[Internal Users] ページが表示されます。このとき、削除したユーザは表示されません。

関連トピック

- 「内部 ID ストア ユーザの一括操作の表示および実行」（P.8-15）
- 「内部ユーザの作成」（P.8-11）

内部 ID ストア ユーザの一括操作の表示および実行

内部 ID ストア ユーザに対する一括操作を表示および実行するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択します。

[Internal Users] ページが表示され、設定されているすべてのユーザについて次の情報が示されます。

- [Status]：ユーザのステータス
- [User Name]：ユーザのユーザ名
- [Identity Group]：ユーザが所属している ID グループ
- [Description]：（任意）ユーザの説明

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。内部ユーザの作成の詳細については、「内部ユーザの作成」（P.8-11）を参照してください。
- 情報を編集する内部ユーザの隣にあるチェックボックスをオンにし、[Edit] をクリックします。内部ユーザ編集ページのさまざまなフィールドの詳細については、「内部ユーザの作成」（P.8-11）を参照してください。
- 情報を複製する内部ユーザの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。内部ユーザ複製ページのさまざまなフィールドの詳細については、「内部ユーザの作成」（P.8-11）を参照してください。
- [File Operations] をクリックして、次の一括操作を実行します。
  - [Add]：内部ユーザをインポート ファイルから ACS に追加するには、このオプションを選択します。
  - [Update]：ACS の内部ユーザのリストをインポート ファイルの内部ユーザのリストで置換するには、このオプションを選択します。
  - [Delete]：インポート ファイルにリストされている内部ユーザを ACS から削除するには、このオプションを選択します。

    一括操作の詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。

関連トピック

- 「内部ユーザの作成」（P.8-11）

- 「内部 ID ストア ユーザの一括操作の表示および実行」（P.8-15）
- 「内部 ID ストアからのユーザの削除」（P.8-14）

ID ストアでのホストの作成

MAC アドレスを作成、複製、または編集し、ID グループを内部ホストに割り当てるには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] を選択します。

[Internal Hosts] ページが表示され、設定されている内部ホストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する MAC アドレスの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する MAC アドレスをクリックします。または、MAC アドレスの隣にあるチェックボックスをオンにして [Edit] をクリックします。
- [File Operations] をクリックして、一括操作を実行します。インポート プロセスの詳細については、「内部 ID ストア ホストの一括操作の表示および実行」（P.8-18）を参照してください。
- [Export] をクリックして、ホストのリストをローカル ハード ドライブにエクスポートします。

[Create]、[Duplicate]、または [Edit] オプションをクリックすると、[Internal Hosts General] ページが表示されます。

ステップ 3　表 8-6 の説明に従って、[Internal MAC Address Properties] ページのフィールドに入力します。

表 8-6　[Internal Hosts Properties] ページ

オプション	説明
General	
MAC Address	新しいホストを内部 ID ストアに追加するとき、ACS 5.4 ではワイルドカードがサポートされます。有効な MAC アドレスを入力します。次の形式のいずれかを使用します。 • 01-23-45-67-89-AB/01-23-45-* • 01:23:45:67:89:AB/01:23:45:* • 0123.4567.89AB/0123.45* • 0123456789AB/012345* ACS は、上記のいずれかの形式の MAC アドレスを受け入れ、ハイフンで区切られた 6 個の 16 進数に変換して保存します。たとえば、01-23-45-67-89-AB のように変換します。
Status	ドロップダウン リスト ボックスを使用して、MAC アドレスをイネーブルまたはディセーブルにします。
Description	（任意）MAC アドレスの説明を入力します。
Identity Group	MAC アドレスを関連付ける ID グループを入力するか、[Select] をクリックして [Identity Groups] ウィンドウを表示します。MAC アドレスを関連付ける ID グループを選択し、[OK] をクリックします。
MAC Host Information	*表示のみ*。MAC ホストの ID 属性情報が表示されます。
Creation/Modification Information	
このページのこのセクションは、MAC アドレスを作成または変更したあとにだけ表示されます。	

表 8-6　[Internal Hosts Properties] ページ （続き）

オプション	説明
Date Created	*表示のみ*。ホスト アカウントが作成された日付。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。
Date Modified	*表示のみ*。ホスト アカウントが最後に変更（更新）された日付。形式は *Day Mon dd hh:mm:ss* **UTC** *YYYY* です。ここで、 • *Day* = 曜日。 • *Mon* = 月を表す 3 文字。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • *DD* = 日を表す 2 桁の数字。1 桁の日（1 ～ 9）の前にはスペースが付きます。 • *hh*:*mm*:*ss* = 時、分、秒。 • *YYYY* = 年を表す 4 桁の数字。

ステップ 4　[Submit] をクリックして変更を保存します。

MAC アドレスの設定が保存されます。[Internal MAC list] ページが新しい設定で表示されます。

（注） MAC アドレスのワイルドカード（サポートされるフォーマット）を持つホストは 4.x から 5.x. に移行されます。

（注） 組織固有識別子（OUI）クライアントの全範囲を許可する MAC アドレスのワイルドカードを追加できます。
例：シスコの MAC アドレス 00-00-0C-* を追加すると、シスコ デバイスの範囲全体がホストに追加されます。

関連トピック

- 「ホスト ルックアップ」（P.4-13）
- 「内部ホストの削除」（P.8-18）
- 「内部 ID ストア ホストの一括操作の表示および実行」（P.8-18）
- 「ポリシーおよび ID 属性」（P.3-17）
- 「ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定」（P.4-19）

内部ホストの削除

MAC アドレスを削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] を選択します。

[Internal MAC List] ページが表示され、設定されている MAC アドレスが示されます。

ステップ 2　削除する内部ホストの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[Internal MAC List] ページが、削除された MAC アドレスなしで表示されます。

関連トピック

- 「ホスト ルックアップ」（P.4-13）
- 「内部 ID ストア ホストの一括操作の表示および実行」（P.8-18）
- 「ID ストアでのホストの作成」（P.8-16）
- 「ポリシーおよび ID 属性」（P.3-17）
- 「ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定」（P.4-19）

内部 ID ストア ホストの一括操作の表示および実行

内部 ID ストアに対する一括操作を表示および実行するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] を選択します。

[Internal Hosts] ページが表示され、設定されている内部ホストが示されます。

ステップ 2　[File Operations] をクリックして、次のいずれかの機能を実行します。

- [Add]：内部ホストをインポート ファイルから ACS に追加するには、このオプションを選択します。
- [Update]：ACS の内部ホストのリストをインポート ファイルの内部ホストで置換するには、このオプションを選択します。
- [Delete]：インポート ファイルにリストされている内部ホストを ACS から削除するには、このオプションを選択します。

一括操作の詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。

関連トピック

- 「ホスト ルックアップ」（P.4-13）
- 「ID ストアでのホストの作成」（P.8-16）

- 「内部ホストの削除」（P.8-18）
- 「ポリシーおよび ID 属性」（P.3-17）
- 「ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定」（P.4-19）

外部 ID ストアの管理

ACS 5.4 は、数多くの方法で外部 ID システムと統合します。外部認証サービスを利用するか、または外部システムを使用して、必要な属性を取得してプリンシパルを認証することにより、属性を ACS ポリシーに統合できます。

たとえば、ACS は Microsoft AD を利用してプリンシパルを認証できます。また、LDAP バインド操作を使用して、データベース内のプリンシパルを検索して認証することもできます。ACS は、AD グループ所属などの ID 属性を取得して、ACS ポリシー決定を行うことができます。

（注）　ACS 5.4 には、Windows ユーザのダイヤルイン アクセス権属性の組み込みチェックはありません。LDAP または Windows AD を使用して msNPAllowDialin 属性を設定する必要があります。この属性の設定方法については、次の URL で Microsoft 社のマニュアルを参照してください。
http://msdn.microsoft.com/en-us/library/ms678093%28VS.85%29.aspx

ここでは、ACS 5.4 でサポートされている外部 ID ストアの概要と、それらの設定方法について説明します。

ここでは、次の内容について説明します。

- 「LDAP の概要」（P.8-19）
- 「外部 MAB データベースとしての Cisco NAC Profiler の利用」（P.8-32）
- 「Microsoft AD」（P.8-39）
- 「RSA SecurID サーバ」（P.8-55）
- 「RADIUS ID ストア」（P.8-61）

LDAP の概要

Lightweight Directory Access Protocol（LDAP）は、TCP/IP および UDP 上で動作するディレクトリ サービスの問い合わせおよび変更のためのネットワーキング プロトコルです。LDAP は、x.500 ベースのディレクトリ サーバにアクセスするためのライトウェイト メカニズムです。LDAP は RFC 2251 で定義されています。

ACS 5.4 は、LDAP プロトコルを使用して LDAP 外部データベース（ID ストアとも呼ばれる）と統合します。LDAP ID ストアの設定については、「外部 LDAP ID ストアの作成」（P.8-23）を参照してください。

ここでは、次の内容について説明します。

- 「ディレクトリ サービス」（P.8-20）
- 「LDAP を使用した認証」（P.8-20）
- 「複数の LDAP インスタンス」（P.8-20）
- 「フェールオーバー」（P.8-21）
- 「LDAP 接続管理」（P.8-21）

- 「バインド接続を使用したユーザの認証」（P.8-21）
- 「グループ メンバーシップ情報の取得」（P.8-22）
- 「属性取得」（P.8-23）
- 「証明書取得」（P.8-23）
- 「外部 LDAP ID ストアの作成」（P.8-23）
- 「LDAP グループの設定」（P.8-31）
- 「LDAP 属性の表示」（P.8-32）

ディレクトリ サービス

ディレクトリ サービスは、コンピュータ ネットワークのユーザおよびネットワーク リソースに関する情報を保存および編成するためのソフトウェア アプリケーション（アプリケーションのセット）です。ディレクトリ サービスを使用すると、これらのリソースへのユーザ アクセスを管理できます。

LDAP ディレクトリ サービスは、クライアント/サーバ モデルに基づきます。クライアントは、LDAP サーバに接続することで LDAP セッションを開始し、操作要求をサーバに送信します。サーバは、応答を送信します。1 台以上の LDAP サーバに、LDAP ディレクトリ ツリーまたは LDAP バックエンド データベースからのデータが含まれています。

ディレクトリ サービスは、ディレクトリを管理します。ディレクトリは、情報を保有するデータベースです。ディレクトリ サービスは、情報を保存するために分散モデルを使用します。その情報は、通常はディレクトリ サーバ間で複製されます。

LDAP ディレクトリは、単純なツリー階層で編成されており、数多くのサーバ間で分散できます。各サーバには、定期的に同期化されるディレクトリ全体の複製バージョンを配置できます。

ツリーのエントリには属性のセットが含まれており、各属性には名前（属性タイプまたは属性の説明）と 1 つ以上の値があります。属性はスキーマに定義されます。

各エントリには、固有識別情報、つまり Distinguished Name（DN; 認定者名）があります。この名前には、エントリ内の属性で構成されている Relative Distinguished Name（RDN; 相対識別名）と、それに続く親エントリの DN が含まれています。DN は完全なファイル名、RDN はフォルダ内の相対ファイル名と考えることができます。

LDAP を使用した認証

ACS 5.4 は、ディレクトリ サーバでバインド操作を実行し、プリンシパルを検索および認証することによって、LDAP ID ストアに対してプリンシパルを認証できます。認証が成功した場合、ACS はプリンシパルに所属するグループおよび属性を取得できます。取得する属性は、ACS Web インターフェイス（LDAP ページ）で設定できます。ACS は、これらのグループおよび属性を使用してプリンシパルを認可できます。

ユーザの認証または LDAP ID ストアの問い合わせを行うために、ACS は LDAP サーバに接続し、接続プールを保持します。「LDAP 接続管理」（P.8-21）を参照してください。

複数の LDAP インスタンス

ACS 5.4 に複数の LDAP インスタンスを作成できます。IP アドレスまたはポートの設定が異なる複数の LDAP インスタンスを作成することにより、異なる LDAP サーバを使用するか、または同じ LDAP サーバ上の異なるデータベースを使用して認証を行うように、ACS を設定できます。

プライマリ サーバの各 IP アドレスおよびポートの設定は、セカンダリ サーバの IP アドレスおよびポートの設定とともに、ACS LDAP ID ストア インスタンスに対応する LDAP インスタンスを形成します。

ACS 5.4 では、個々の LDAP インスタンスが固有の LDAP データベースに対応している必要はありません。複数の LDAP インスタンスを、同一のデータベースにアクセスするように設定できます。

この方法は、LDAP データベースにユーザまたはグループのサブツリーが複数含まれている場合に役立ちます。各 LDAP インスタンスでは、ユーザとグループに対してそれぞれ単一のサブツリー ディレクトリだけをサポートするため、ACS が認証要求を送信する必要があるユーザ ディレクトリ サブツリーとグループ ディレクトリ サブツリーの組み合わせごとに、別々の LDAP インスタンスを設定する必要があるからです。

フェールオーバー

ACS 5.4 では、プライマリ LDAP サーバとセカンダリ LDAP サーバ間でのフェールオーバーがサポートされています。ACS による LDAP 認証のコンテキストでは、ACS が LDAP サーバに接続できないために認証要求が失敗した場合に、フェールオーバーが適用されます。

たとえば、サーバがダウンした場合や ACS がサーバに到達できない場合などです。この機能を使用するには、プライマリとセカンダリの LDAP サーバを定義する必要があり、フェールオーバー設定を行う必要があります。

フェールオーバー設定を行い、ACS が接続しようとする最初の LDAP サーバに到達できない場合には、常に ACS は他の LDAP サーバへの接続を試みます。

ACS が接続を試みる最初のサーバは、プライマリ LDAP サーバであるとはかぎりません。ACS が接続を試みる最初の LDAP サーバは、その前に試みた LDAP 認証と、[Failback Retry Delay] ボックスに入力する値によって決まります。

LDAP 接続管理

ACS 5.4 では、複数の同時 LDAP 接続がサポートされています。接続は、最初の LDAP 認証時にオンデマンドで開かれます。最大接続数は、LDAP サーバごとに設定されます。事前に接続を開いておくと、認証時間が短縮されます。

同時バインディング接続に使用する最大接続数を設定できます。開かれる接続の数は、LDAP サーバ（プライマリまたはセカンダリ）ごとに異なる場合があり、サーバごとに設定される最大管理接続数によって決まります。

ACS は、ACS で設定されている LDAP サーバごとに、開いている LDAP 接続（バインド情報を含む）のリストを保持します。認証プロセス中に、Connection Manager は開いている接続をプールから検索しようとします。開いている接続が存在しない場合、新しい接続が開かれます。

LDAP サーバが接続を閉じた場合、Connection Manager はディレクトリを検索する最初のコールでエラーをレポートし、接続を更新しようとします。

認証プロセスが完了したあと、Connection Manager は Connection Manager への接続を解放します。

バインド接続を使用したユーザの認証

ACS は、バインド要求を送信して、LDAP サーバに対してユーザを認証します。バインド要求には、ユーザの DN およびユーザ パスワードがクリア テキストで含まれています。ユーザの DN およびパスワードが LDAP ディレクトリ内のユーザ名およびパスワードと一致した場合に、ユーザは認証されます。

- 認証エラー：ACS は認証エラーを ACS ログ ファイルにロギングします。
- 初期化エラー：LDAP サーバのタイムアウト設定を使用して、LDAP サーバでの接続または認証が失敗したと判断する前に ACS が LDAP サーバからの応答を待つ秒数を設定します。

  LDAP サーバが初期化エラーを返す理由で考えられるのは、次のとおりです。

  - LDAP がサポートされていない。
  - サーバがダウンしている。
  - サーバがメモリ不足である。
  - ユーザに特権がない。
  - 間違った管理者クレデンシャルが設定されている。
- バインド エラー

  LDAP サーバがバインド（認証）エラーを返す理由で考えられるのは、次のとおりです。

  - フィルタリング エラー：フィルタ基準を使用した検索が失敗する。
  - パラメータ エラー：無効なパラメータが入力された。
  - ユーザ アカウントが制限されている（ディセーブル、ロックアウト、期限切れ、パスワード期限切れなど）。

外部リソース エラーとして次のエラーがロギングされ、LDAP サーバで考えられる問題が示されます。

- 接続エラーが発生した。
- タイムアウトが期限切れになった。
- サーバがダウンしている。
- サーバがメモリ不足である。

未知ユーザ エラーとして次のエラーがロギングされます。

データベースにユーザが存在しない。

無効パスワード エラーとして次のエラーがロギングされます。ユーザは存在しますが、送信されたパスワードが無効です。

```
An invalid password was entered.
```

グループ メンバーシップ情報の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、ACS は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバは、サブジェクト（ユーザまたはホスト）とグループ間の関連付けを次の 2 つの方法のいずれかで表します。

- グループがサブジェクトを参照：グループ オブジェクトには、サブジェクトを指定する属性が含まれています。サブジェクトの識別子は、次のようなグループに保存できます。
  - 認定者名（DN）
  - プレーン ユーザ名
- サブジェクトがグループを参照：サブジェクト オブジェクトには、所属するグループを指定する属性が含まれています。

LDAP ID ストアには、グループ メンバーシップ情報の取得のために次のパラメータが含まれています。

- Reference Direction：グループ メンバーシップを決定するときに使用する方法を指定します（Groups to Subjects または Subjects to Groups）。
- Group Map Attribute：グループ メンバーシップ情報を含む属性を示します。
- Group Name Attribute：グループ名情報を含む属性を示します。
- Group Object Class：特定のオブジェクトをグループとして認識することを決定します。
- Group Search Subtree：グループ検索の検索ベースを示します。
- Member Type Option：グループ メンバー属性にメンバーが保存される方法を指定します（DN として、またはプレーン ユーザ名として）。

属性取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、ACS は LDAP データベースからサブジェクト属性を取得する必要があります。LDAP ID ストアのインスタンスごとに、ID ストア ディクショナリが作成されます。これらのディレクトリでは、次のデータ型の属性がサポートされています。

- String
- Unsigned Integer 32
- IP アドレス：IP バージョン 4（IPv4）または IP バージョン 6（IPv6）アドレスを指定できます。

符号なし整数および IP アドレス属性の場合、ACS は取得した文字列を対応するデータ型に変換します。変換が失敗した場合、または属性に対して値が取得されなかった場合、ACS ではデバッグ メッセージをロギングしますが、認証およびルックアップ プロセスは失敗しません。

変換が失敗した場合、または ACS で属性に対して値が取得されなかった場合、ACS が使用できる属性のデフォルト値を任意で設定できます。

証明書取得

ユーザ ルックアップの一部として証明書取得を設定した場合、ACS は証明書属性の値を LDAP から取得する必要があります。これを実行するには、LDAP ID ストアの設定時に、取得する属性のリストに証明書属性を設定しておく必要があります。

外部 LDAP ID ストアの作成

（注）　ACS 用の LDAP ID ストアを設定しても、LDAP データベースの設定には影響を与えません。ACS は LDAP データベースを認識し、データベースを認証の対象とすることができます。使用している LDAP データベースを管理するには、そのデータベースのマニュアルを参照してください。

LDAP ID ストアを作成すると、ACS によって次のものも作成されます。

- そのストア用の新しいディクショナリ。2 つの属性 ExternalGroups および IdentityDn があります。
- ExternalGroup 属性からのグループ マッピングのカスタム条件。条件名の形式は LDAP:*ID_store_name* ExternalGroups です。

事前定義済みの条件名を編集でき、[Custom condition] ページで IdentityDn 属性からカスタム条件を作成できます。「カスタム セッション条件の作成、複製、および編集」（P.9-5）を参照してください。

外部 LDAP ID ストアを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

[LDAP Identity Stores] ページが表示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する ID ストアの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する ID ストア名をクリックします。または、名前の隣にあるボックスをオンにして [Edit] をクリックします。

ID ストアを作成している場合は、ウィザードの最初のページである [General] が表示されます。

ID ストアを複製している場合は、[External Identity Stores] > [Duplicate: "<*idstore*>"] ページの [General] タブが表示されます。*idstore* は、選択した外部 ID ストアの名前です

ID ストアを編集している場合は、[External Identity Stores] > [Edit: "*idstore*"] ページの [General] タブが表示されます。*idstore* は、選択した外部 ID ストアの名前です。

ステップ 3　必要に応じて、[Name] フィールドおよび [Description] フィールドに入力します。

ステップ 4　パスワードの変更、パスワードの有効期限の検出、およびパスワードのリセットを行うには、[Enable Password Change] オプションをオンにします。

ステップ 5　[Next] をクリックします。

ステップ 6　「外部 LDAP サーバ接続の設定」（P.8-24）に進みます。

（注）　外部 LDAP サーバとして、NAC ゲスト サーバも使用できます。外部 LDAP サーバとして NAC ゲスト サーバを使用する手順については、以下の URL を参照してください。
http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/20/g_sponsor.html#wp1070105

関連項目

- 「外部 LDAP ID ストアの削除」（P.8-31）

外部 LDAP サーバ接続の設定

このページは、外部 LDAP ID ストアを設定する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、次のいずれかをクリックします。

- [Create]。ウィザードに従います。
- [Duplicate]。次に [Next] をクリックします。[Server Connection] ページが表示されます。
- [Edit]。次に [Next] をクリックします。[Server Connection] ページが表示されます。

表 8-7　[LDAP: Server Connection] ページ

オプション	説明
Server Connection	
Enable Secondary Server	セカンダリ LDAP サーバをイネーブルにする場合にオンにします。プライマリ LDAP サーバに障害が発生した場合のバックアップとして使用します。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバの設定パラメータを入力する必要があります。
Always Access Primary Server First	セカンダリ LDAP サーバにアクセスする前にプライマリ LDAP サーバにアクセスする場合にクリックします。
Failback to Primary Server After <*min.*> Minutes	プライマリ サーバに到達できない場合に ACS がセカンダリ LDAP サーバを使用して認証する時間（分単位）を設定する場合にクリックします。<***min.***> は時間（分単位）です。この時間のあと、ACS はプライマリ LDAP サーバを使用した認証を再試行します（デフォルト = 5）。
Primary Server	
Hostname	プライマリ LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
Port	プライマリ LDAP サーバが受信している TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバの管理者に問い合わせることによって、ポート番号を取得できます。
Anonymous Access	LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバによって、クライアントが誰かは区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへのクライアント読み取りアクセスが許可されます。 認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。
Authenticated Access	LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[Admin DN] および [Password] フィールドの情報を入力します。
Admin DN	管理者の認定者名を入力します。つまり、User Directory Subtree 内の必要なすべてのユーザの検索が許可され、グループの検索が許可されている LDAP アカウントです。 指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、LDAP が認証したユーザのグループ マッピングは失敗します。
Password	LDAP 管理者アカウントのパスワードを入力します。
Use Secure Authentication	Secure Sockets Layer（SSL）を使用して ACS とプライマリ LDAP サーバ間の通信を暗号化する場合にクリックします。[Port] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションをイネーブルにした場合は、ルート CA を選択する必要があります。
Root CA	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証をイネーブルにします。
Server Timeout <*sec.*> Seconds	プライマリ LDAP サーバでの接続または認証が失敗したと判断する前に ACS がプライマリ LDAP サーバからの応答を待つ秒数を入力します。<*sec.*> は秒数です。有効な値は 1 ～ 300 です（デフォルト = 10）。
Max Admin Connections	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、User Directory Subtree および Group Directory Subtree の下にあるユーザおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です（デフォルト = 8）。

表 8-7　[LDAP: Server Connection] ページ （続き）

オプション	説明
Test Bind To Server	プライマリ LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。
Secondary Server	
Hostname	セカンダリ LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
Port	セカンダリ LDAP サーバが受信している TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP マシン上に DS プロパティを表示することによって、ポート番号を取得できます。
Anonymous Access	LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバによって、クライアントが誰かは区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへのクライアント アクセス（読み取りおよび更新）が許可されます。 認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。
Authenticated Access	LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[Admin DN] および [Password] フィールドの情報を入力します。
Admin DN	管理者のドメイン名を入力します。つまり、User Directory Subtree 内の必要なすべてのユーザの検索が許可され、グループの検索が許可されている LDAP アカウントです。 指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、LDAP が認証したユーザのグループ マッピングは失敗します。
Password	LDAP 管理者アカウントのパスワードを入力します。
Use Secure Authentication	Secure Sockets Layer（SSL）を使用して ACS とセカンダリ LDAP サーバ間の通信を暗号化する場合にクリックします。[Port] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションをイネーブルにした場合は、ルート CA を選択する必要があります。
Root CA	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証をイネーブルにします。
Server Timeout <*sec.*> Seconds	セカンダリ LDAP サーバでの接続または認証が失敗したと判断する前に ACS がセカンダリ LDAP サーバからの応答を待つ秒数を入力します。<*sec.*> は秒数です。有効な値は 1 ～ 300 です （デフォルト = 10）。
Max Admin Connections	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、User Directory Subtree および Group Directory Subtree の下にあるユーザおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です （デフォルト = 8）。
Test Bind To Server	セカンダリ LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。

ステップ 2　[Next] をクリックします。

ステップ 3　「外部 LDAP ディレクトリ構成の設定」（P.8-27）に進みます。

外部 LDAP ディレクトリ構成の設定

このページは、外部 LDAP ID ストアを設定する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、次のいずれかをクリックします。

- [Create]。[Directory Organization] ページに到達するまでウィザードに従います。
- [Duplicate]。[Directory Organization] ページが表示されるまで [Next] をクリックします。
- [Edit]。[Directory Organization] ページが表示されるまで [Next] をクリックします。

表 8-8　[LDAP: Directory Organization] ページ

オプション	説明
Schema	
Subject Object class	サブジェクトを識別する LDAP *objectClass* 属性の値。多くの場合、サブジェクト レコードの *objectClass* 属性には複数の値があり、サブジェクトに固有のものや、他のオブジェクト タイプと共有されているものがあります。 このボックスには、共有されていない値を入力する必要があります。有効な値は 1 ～ 20 文字であり、有効な LDAP オブジェクト タイプである必要があります。このパラメータには、任意の UTF-8 文字を含めることができます。（デフォルト = Person）。
Group Object class	オブジェクトをグループとして識別する検索で使用するグループ オブジェクト クラスを入力します （デフォルト = GroupOfUniqueNames）。
Subject Name Attribute	サブジェクト名を含むサブジェクト レコード内の属性名。この属性名は、ディレクトリ サーバから取得できます。この属性によって、LDAP スキーマ内のサブジェクト名が指定されます。この属性を使用して、サブジェクト オブジェクトを検索するクエリーを作成します。 詳細については、LDAP データベースに関するドキュメントを参照してください。有効な値は 1 ～ 20 文字であり、有効な LDAP 属性である必要があります。このパラメータには、任意の UTF-8 文字を含めることができます。一般的な値は、*uid* および *CN* です（デフォルト = uid）。

表 8-8　[LDAP: Directory Organization] ページ （続き）

オプション	説明
Group Map Attribute	ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、ACS は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバは、サブジェクト（ユーザまたはホスト）とグループ間の関連付けを次の 2 つの方法のいずれかで表します。 • グループがサブジェクトを参照 • サブジェクトがグループを参照 [Group Map Attribute] には、マッピング情報を入力します。 マッピング情報を含む属性（次の条件に従って、サブジェクトまたはグループの属性）を入力する必要があります。 • [Subject Objects Contain Reference To Groups] オプション ボタンを選択した場合は、サブジェクト属性を入力します。 • [Group Objects Contain Reference To Subjects] オプション ボタンを選択した場合は、グループ属性を入力します。
Group Name Attribute	グループ名を含むグループ レコード内の属性名。この属性名は、ディレクトリ サーバから取得できます。この属性によって、LDAP スキーマ内のグループ名が指定されます。この属性を使用して、グループ オブジェクトを検索するクエリーを作成します。 詳細については、LDAP データベースに関するドキュメントを参照してください。一般的な値は DN および CN です。（デフォルト = DN）。
Certificate Attribute	証明書定義を含む属性を入力します。証明書認証プロファイルの一部として定義されたときに、これらの定義を任意で使用して、クライアントによって提示された証明書を確認できます。その場合、クライアント証明書と LDAP ID ストアから取得された証明書の間でバイナリ比較が実行されます。
Subject Objects Contain Reference To Groups	サブジェクト オブジェクトにグループの参照が含まれる場合にクリックします。
Group Objects Contain Reference To Subjects	グループ オブジェクトにサブジェクトの参照が含まれる場合にクリックします。
Subjects In Groups Are Stored In Member Attribute As	ドロップダウン リスト ボックスを使用して、グループ内のサブジェクトがメンバー属性に次のうちのいずれとして保存されるかを指定します。 • Username • Distinguished name
Directory Structure	

Subject Search Base	すべてのサブジェクトを含むサブツリーの認定者名（DN）を入力します。次に例を示します。
	`o=corporation.com`
	サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて
	`o=corporation.com`
	または
	`dc=corporation,dc=com`
	と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

表 8-8　[LDAP: Directory Organization] ページ （続き）

オプション	説明

Group Search Base	すべてのグループを含むサブツリーの認定者名（DN）を入力します。次に例を示します。
	`ou=organizational unit[,ou=next organizational unit]o=corporation.com`
	グループを含むツリーがベース DN である場合は、LDAP 設定に応じて
	`o=corporation.com`
	または
	`dc=corporation,dc=com`
	と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

Test Configuration	設定の結果として生ずる可能性があるユーザおよびグループの数をカウントすることによって、予期される接続およびスキーマの結果を取得する場合にクリックします。

表 8-8　[LDAP: Directory Organization] ページ （続き）

オプション	説明
Username Prefix\Suffix Stripping	
Strip start of subject name up to the last occurrence of the separator	ユーザ名からドメイン プレフィックスを削除するために適切なテキストを入力します。 ユーザ名の中で、[*start_string*] ボックスに指定した区切り文字が検出されると、そのユーザ名の初めから区切り文字までのすべての文字が削除されます。 ユーザ名に、[*start_string*] ボックスに指定した文字が複数含まれている場合は、最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザ名が DOMAIN\echamberlain である場合、echamberlain が LDAP サーバに送信されます。 [start_string] ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。ACS では、ユーザ名にこれらの文字を使用できません。X ボックスにこれらの文字のいずれかを入力すると、ストリッピングが失敗します。
Strip end of subject name from the first occurrence of the separator	ユーザ名からドメイン サフィックスを削除するために適切なテキストを入力します。 ユーザ名の中で、Y ボックスに指定した区切り文字が検出されると、その区切り文字からユーザ名の末尾までのすべての文字が削除されます。 ユーザ名に、Y ボックスに指定した文字が複数含まれる場合は、最初の区切り文字から文字が削除されます。たとえば、区切り文字がアットマーク（@）で、ユーザ名が *jwiedman@domain* である場合、*jwiedman* が LDAP サーバに送信されます。 [*end_string*] ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。ACS では、ユーザ名にこれらの文字を使用できません。[*end_string*] ボックスにこれらの文字のいずれかを入力すると、ストリッピングが失敗します。
MAC Address Format	
Search for MAC Address in Format <*format*>	内部 ID ストアの MAC アドレスは、xx-xx-xx-xx-xx-xx 形式で保存されます。LDAP データベースの MAC アドレスは、別の形式で保存できます。ただし、ACS でホスト ルックアップ要求が受信されると、MAC アドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リスト ボックスを使用して、特定の形式での MAC アドレスの検索をイネーブルにします。<*format*> は次のいずれかです。 • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx • xxxx.xxxx.xxxx 選択する形式は、LDAP サーバに保存されている MAC アドレスの形式と一致している必要があります。

ステップ 2　[Finish] をクリックします。

作成した外部 ID ストアが保存されます。

関連トピック

- 「LDAP グループの設定」（P.8-31）

- 「外部 LDAP ID ストアの削除」（P.8-31）

外部 LDAP ID ストアの削除

1 つ以上の外部 LDAP ID ストアを同時に削除できます。

外部 LDAP ID ストアを削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

[LDAP Identity Stores] ページが表示され、設定されている外部 ID ストアのリストが示されます。

ステップ 2　削除する外部 ID ストアの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のエラー メッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[External Identity Stores] ページが表示されます。このとき、削除した ID ストアはリストに含まれません。

関連項目

- 「外部 LDAP ID ストアの作成」（P.8-23）

LDAP グループの設定

このページは、外部 LDAP グループを設定する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、次のいずれかをクリックします。

- [Create]。ウィザードに従います。
- [Duplicate]。次に [Directory Groups] タブをクリックします。
- [Edit]。次に [Directory Groups] タブをクリックします。

[Selected Directory Groups] フィールドに、規則テーブル グループ マッピング条件でオプションとして使用できるグループのリストが表示されます。

ステップ 2　次のいずれかを実行します。

- [Select] をクリックして、[Groups] セカンダリ ウィンドウを開きます。このウィンドウからグループを選択して [Selected Directory Groups] リストに追加できます。
- または、[Group Name] フィールドに LDAP グループを入力して [Add] をクリックすることもできます。

選択したグループを [Selected Directory Groups] リストから削除するには、そのグループを [Selected Directory Groups] リストで選択して [Deselect] をクリックします。

ステップ 3　[Submit] をクリックして変更を保存します。

LDAP 属性の表示

このページは、外部 LDAP 属性を表示する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

ステップ 2　属性を表示する LDAP ID ストアの隣にあるチェックボックスをオンにし、[Edit] をクリックして、[Directory Attributes] タブをクリックします。

ステップ 3　[Name of example Subject to Select Attributes] フィールドに、属性を取得するオブジェクト例の名前を入力し、[Select] をクリックします。

たとえば、オブジェクトをユーザにして、オブジェクト名をユーザ名またはユーザの DN にすることができます。

ステップ 4　表 8-9 の説明に従って、フィールドに入力します。

表 8-9　[LDAP: Attributes] ページ

オプション	説明
Attribute Name	ポリシー条件で使用可能な属性のリストに含める属性名を入力します。
Type	[Attribute Name] フィールドに入力した属性名に関連付けるタイプを選択します。
Default	[Attribute Name] フィールドに入力した属性名に関連付けるデフォルト値を指定します。デフォルト値を指定しない場合、デフォルトは使用されません。 [Select] ボタンによって [Attribute Name/Type/Default] ボックスに属性がインポートされた場合は、これらのデフォルト値が使用されます。 • String：属性名 • Unsigned Integer 32 • IP Address：IPv4 または IPv6 アドレスを指定できます。
Policy Condition Name	（*任意*）この属性のカスタム条件の名前を指定します。この条件は、ポリシーの条件をカスタマイズするときに選択できます。

ステップ 5　[Add] をクリックすると、入力した情報が画面上のフィールドに追加されます。

ここに表示される属性をポリシー条件で使用できます。

ステップ 6　[Submit] をクリックして変更を保存します。

外部 MAB データベースとしての Cisco NAC Profiler の利用

ACS は、Cisco NAC Profiler と通信して、802.1X 非対応デバイスが 802.1X 対応ネットワークで認証できるようにします。802.1X を使用して認証できないエンドポイントは、スイッチで MAC 認証バイパス（MAB）機能を使用して、802.1X 対応ネットワークに接続します。

一般的に、プリンタ、ファクス装置、IP 電話、無停電電源（UPS）などの非ユーザ接続デバイスには、802.1x サプリカントは装備されていません。

つまり、これらのデバイスが接続するスイッチ ポートは、デバイスまたはユーザ クレデンシャルの 802.1X 交換を使用してデバイスを認証できず、デバイスがネットワークに接続するには、スイッチ ポートはポートベースの認証以外の認証メカニズム（一般的に、エンドポイント MAC アドレスベース）に戻る必要があります。

Cisco NAC Profiler は、これらのシステムの認証コンポーネントと連携動作できないエンドポイントを識別して特定するためのソリューションを提供します。その結果、これらのエンドポイントにネットワークへのアドミッションのための代替メカニズムを提供できます。

NAC Profiler は、LDAP 対応ディレクトリで構成されます。このディレクトリは、MAC 認証バイパス（MAB）に使用できます。したがって、NAC Profiler は ACS の外部 LDAP データベースとして機能して、802.1X 非対応デバイスを認証します。

（注）　ACS 内部ホスト データベースを使用すると、802.1X 非対応デバイスの MAC アドレスを定義できます。ただし、NAC Profiler がすでにネットワーク内にある場合は、それを外部 MAB データベースとして使用できます。

Cisco NAC Profiler を外部 MAB データベースとして利用するには、次のことを実行する必要があります。

- Cisco NAC Profiler で LDAP インターフェイスをイネーブルにします。「Cisco NAC Profiler での LDAP インターフェイスのイネーブル化による ACS との通信」（P.8-33）を参照してください。
- ACS で NAC Profiler を設定します。「ID ポリシーで使用するための ACS での NAC Profiler LDAP 定義の設定」（P.8-35）を参照してください。

Cisco NAC Profiler での LDAP インターフェイスのイネーブル化による ACS との通信

（注）　NAC Profiler で LDAP インターフェイスをイネーブルにする前に、NAC Profiler Collector で NAC Profiler を設定しておきます。Cisco NAC Profiler 設定の詳細については、次の Web サイトで『*Cisco NAC Profiler Installation and Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html

NAC Profiler で LDAP インターフェイスをイネーブルにして ACS と通信するには、次の手順を実行します。

ステップ 1　Cisco NAC Profiler にログインします。

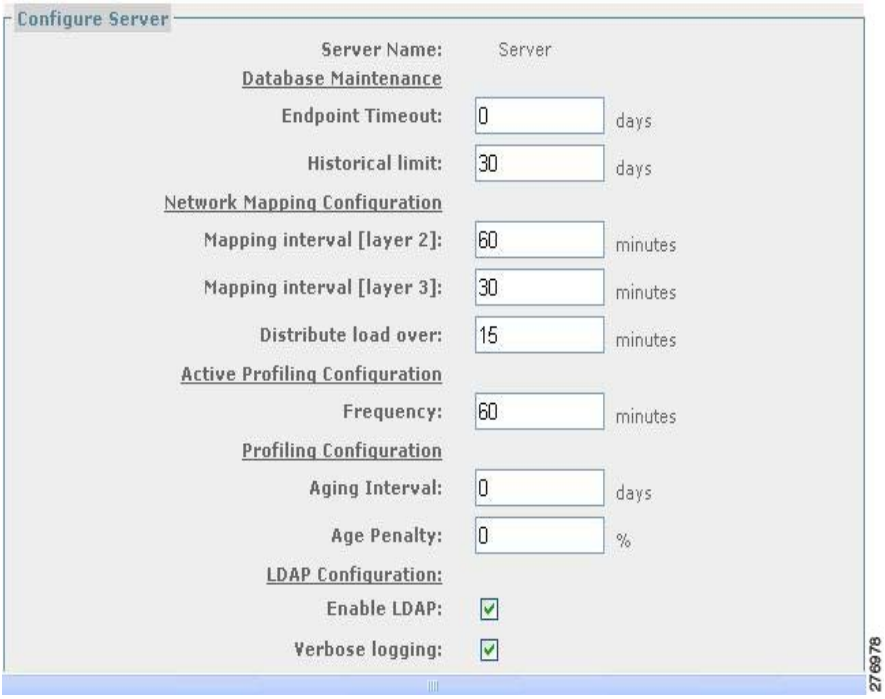
ステップ 2　[Configuration] > [NAC Profiler Modules] > [List NAC Profiler Modules] を選択します。

ステップ 3　[Server] をクリックします。

[Configure Server] ページが表示されます。

ステップ 4　[LDAP Configuration] 領域で、図 8-1 に示すように [Enable LDAP] チェックボックスをオンにします。

図 8-1　NAC Profiler での LDAP インターフェイス設定



ステップ 5　[Update Server] をクリックします。

ステップ 6　[Configuration] タブをクリックし、[Apply Changes] をクリックします。

[Update NAC Profiler Modules] ページが表示されます。

ステップ 7　[Update Modules] をクリックして、ACS で LDAP を使用できるようにします。

Cisco NAC Profiler に対して認証するエンドポイント プロファイルをイネーブルにする必要があります。その実行方法については、「LDAP 認証に対する NAC Profiler でのエンドポイント プロファイルの設定」（P.8-34）を参照してください。

適切なアクティブ応答イベントを確保するため、Cisco NAC Profiler UI からアクティブ応答遅延時間を設定する必要があります。これには、[Configuration] > [NAC Profiler Modules] > [Configure Server] > [Advanced Options] > [Active Response Delay] を選択します。

LDAP 認証に対する NAC Profiler でのエンドポイント プロファイルの設定

認証する非 802.1X エンドポイントについて、LDAP 認証に対して NAC Profiler で対応するエンドポイント プロファイルをイネーブルにする必要があります。

（注）　プロファイルが LDAP に対してイネーブルになっていない場合、Cisco NAC Profiler によるプロファイルのエンドポイントの認証は行われません。

LDAP 認証に対してエンドポイント プロファイルをイネーブルにするには、次の手順を実行します。

ステップ 1　NAC Profiler にログインします。

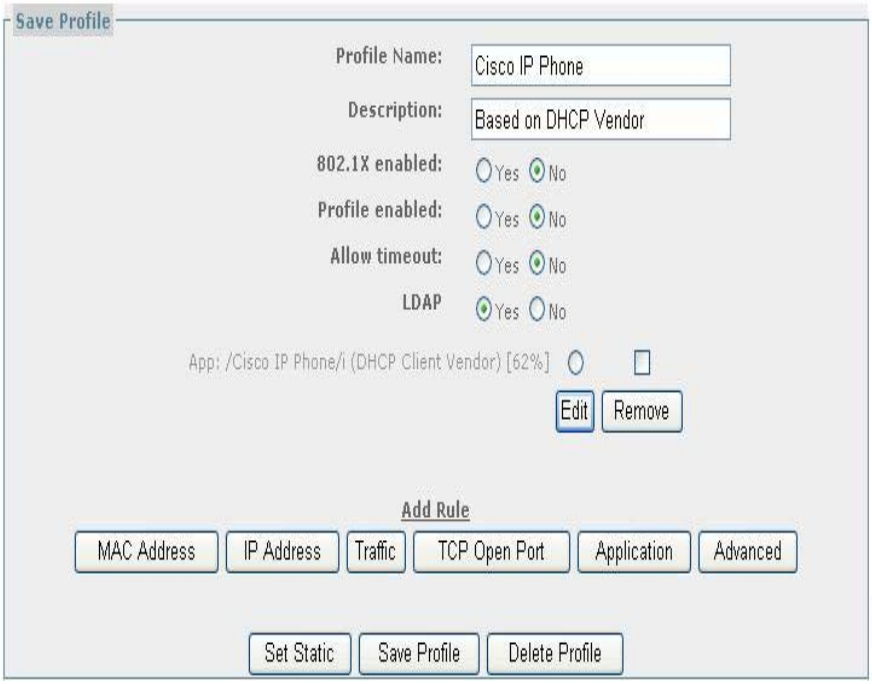
ステップ 2　[Configuration] > [Endpoint Profiles] > [View/Edit Profiles List] を選択します。

プロファイルのリストがテーブルに表示されます。

ステップ 3　プロファイルの名前をクリックして編集します。

ステップ 4　[Save Profile] ページで、図 8-2 に示すように、まだ行っていない場合は [LDAP] オプションの隣にある [Yes] オプション ボタンをクリックしてイネーブルにします。

図 8-2　NAC Profiler でのエンドポイント プロファイルの設定



ステップ 5　[Save Profile] をクリックします。

ID ポリシーで使用するための ACS での NAC Profiler LDAP 定義の設定

ACS をインストールすると、NAC Profiler 用の事前定義済み LDAP データベース定義がインストールされます。NAC Profiler に対して事前に定義されたこのデータベースの定義には、初期接続の確立に必要なすべてのデータが含まれています。ただし、特定の展開設定によって異なるホスト情報を除きます。

次の手順では、ホスト情報の設定方法、接続の確認方法、およびポリシーでのプロファイル データベースの使用方法について説明します。

（注）　[Access Policies] > [Access Services] > [Default Network Access] > [Identity] で ACS NAC Profiler が選択されていることを確認します。

（注）　LDAP 外部 ID ストアで使用できる ACS の **NAC Profiler** テンプレートは、Cisco NAC Profiler バージョン 2.1.8 以降で使用できます。

ACS で NAC Profiler テンプレートを編集するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択します。

ステップ 2　NAC Profiler テンプレートの名前をクリックします。または、NAC Profiler テンプレートの隣にあるチェックボックスをオンにして [Edit] をクリックします。

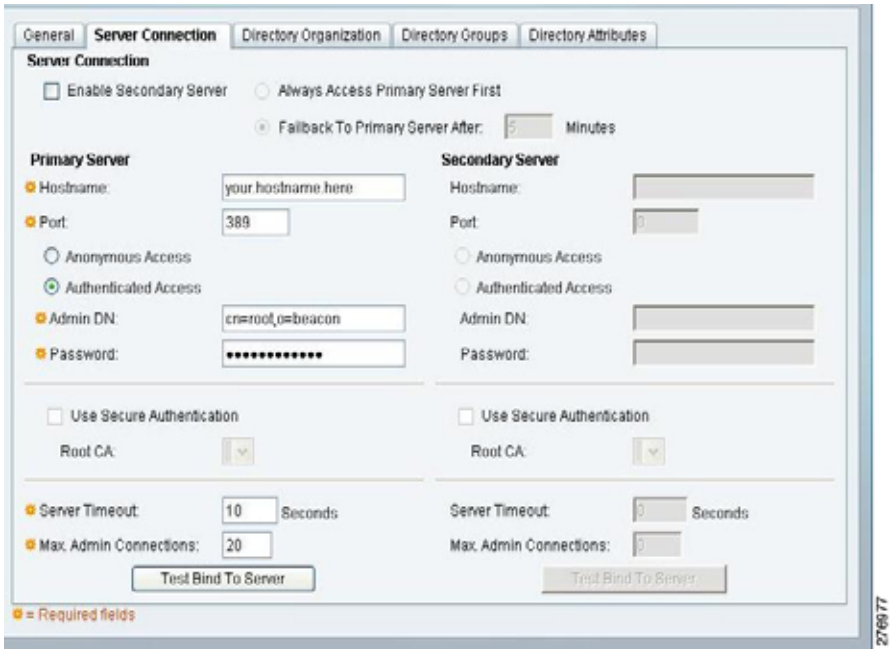
図 8-3 に示すように、[Edit NAC Profiler definition] ページが表示されます。

図 8-3　[Edit NAC Profiler Definition - General] ページ

ステップ 3　[Server Connection] タブをクリックします。

図 8-4 に示すように、[Edit] ページが表示されます。

図 8-4　[Edit NAC Profiler Definition - Server Connection] ページ



ステップ 4　[Primary Server Hostname] フィールドに、Profiler Server の IP アドレスまたは完全修飾ドメイン名を入力します。または、Profiler がハイ アベイラビリティ設定されている場合は、Profiler ペアのサービス IP を入力します。

ステップ 5　[Test Bind to Server] をクリックして、接続をテストし、ACS が LDAP を使用して Profiler と通信できることを確認します。

図 8-5 に示すような小さなポップアップ ダイアログが表示されます。

図 8-5　[Test Bind to Server] ダイアログボックス

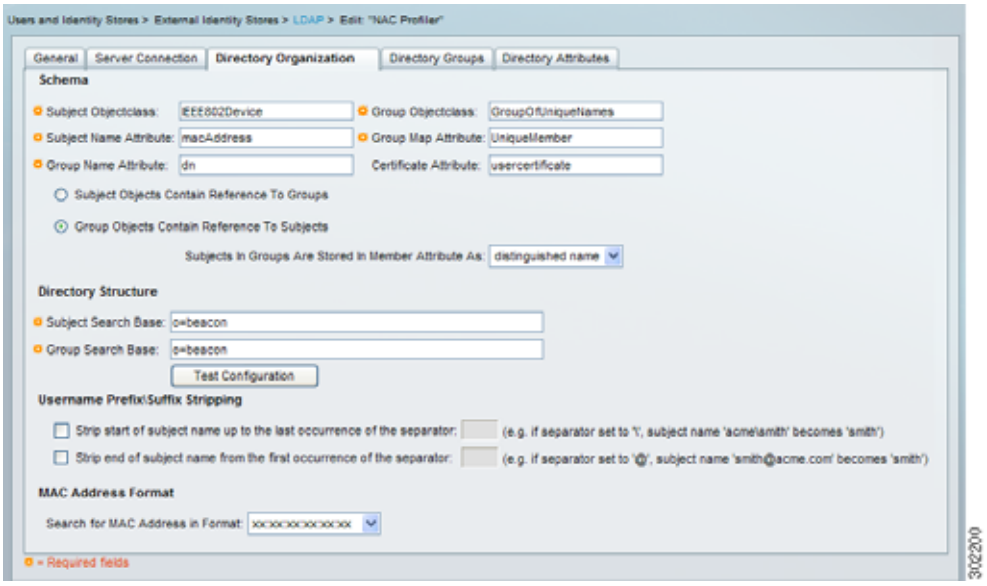
詳細については、「外部 LDAP ID ストアの作成」（P.8-23）を参照してください。

（注）　LDAP のデフォルト パスワードは *GBSbeacon* です。このパスワードを変更する場合は、次の Web サイトで『*Cisco NAC Profiler Installation and Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/311/p_ldap31.html#wp1057155

ステップ 6　成功した場合は、[Directory Organization] タブに移動します。

図 8-6 に示すように、[Edit] ページが表示されます。

図 8-6　[Edit NAC Profiler Definition - Directory Organization] ページ

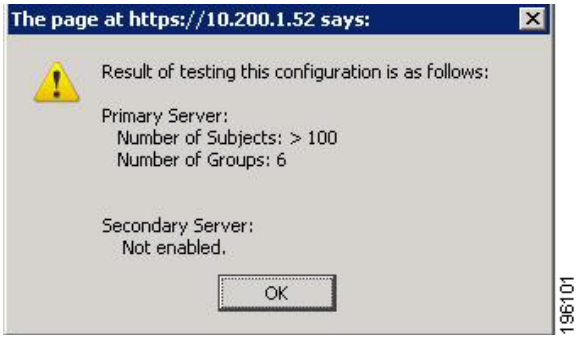


ステップ 7　[Test Configuration] をクリックします。

図 8-7 に示すダイアログボックスが表示され、Profiler に対応するデータが示されます。次に例を示します。

- Primary Server
- Number of Subjects: 100
- Number of Directory Groups: 6

図 8-7　[Test Configuration] ダイアログボックス



Number of Subjects：この値は、Cisco NAC Profiler によってすでにプロファイリングされている実際のサブジェクト デバイス（Profiler に対してイネーブルな実際のデバイス）に対応します。

Profiler が初期 SNMP トラップ情報をスイッチから受信したあと、Profiler は SNMP を使用してスイッチをポーリングし、スイッチおよび接続するエンドポイントに関する MIB（管理情報ベース）情報を収集できます。

Profiler は、エンドポイントについて学習すると（MAC アドレス、スイッチ ポートなど）、エンドポイントをデータベースに追加します。Profiler のデータベースに追加されたエンドポイントは、1 つのサブジェクトと見なされます。

Number of Directory Groups：この値は、Profiler で LDAP に対してイネーブルにされた実際のプロファイルに対応します。ネットワークで Profiler をすでに実行している場合は、エンドポイントのデフォルト プロファイルが事前設定されています。

ただし、すべてのプロファイルは LDAP に対してイネーブルではなく、「LDAP 認証に対する NAC Profiler でのエンドポイント プロファイルの設定」（P.8-34）の説明に従って設定する必要があります。Profiler を初めて設定した場合、Profiler が稼働すると、最初は 0 グループと表示される点に注意してください。

（注）　サブジェクトおよびディレクトリ グループは、数が 100 未満の場合に表示されます。サブジェクトまたはディレクトリ グループの数が 100 を超えた場合、サブジェクトおよびディレクトリ グループは表示されません。代わりに、次のようなメッセージが表示されます。

```
More than 100 subjects are found.
```

ステップ 8　サブジェクト レコードのディレクトリ属性をポリシー規則でポリシー条件として使用する場合は、[Directory Attributes] タブをクリックします。詳細については、「LDAP 属性の表示」（P.8-32）を参照してください。

ステップ 9　ID ポリシーの結果（ID ソース）として NAC Profiler を選択します。詳細については、「ID ポリシーの表示」（P.10-22）を参照してください。

ACS サーバからエンドポイントが正常に認証されると、ACS はただちに認可変更（CoA）を実行し、VLAN を変更します。この目的のために、ACS サーバにスタティック VLAN マッピングを設定できます。詳細については、「認可プロファイルでの共通属性の指定」（P.9-21）を参照してください。

エンドポイントが正常に認証されると、スイッチに次のメッセージが表示されます。

```
ACCESS-Switch# #show authentication sessions
Interface MAC Address Method Domain Status Session ID
Fa1/0/1 0014.d11b.aa36 mab DATA Authz Success 505050010000004A0B41FD15
```

イベント配信方法やアクティブ応答などの機能の詳細については、次の Web サイトで『*Cisco NAC Profiler Installation and Configuration Guide, Release 3.1*』を参照してください。

http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/310/p_prof_events31.html

Profiler の統合による MAB 認証のトラブルシューティング

NAC Profiler との統合中に MAB 認証のトラブルシューティングを行い、エンドポイントが正常に認証されることを確認するには、次の手順を実行します。

ステップ 1　エンドポイント デバイスに接続されたスイッチで次のコマンドを実行します。

```
ACCESS-Switch# show authentication sessions
```

次の出力が表示されます。

```
Interface  MAC Address     Method   Domain  Status         Session ID
Fa1/0/1    0014.d11b.aa36 mab      DATA     Authz Success  505050010000004A0B41FD15 reject
```

ステップ 2　スイッチで、SNMP、AAA、および 802.1X に対するデバッグをイネーブルにします。

ステップ 3　認証の失敗または成功について、[Monitoring and Reports Viewer] > [Troubleshooting] で MAB 認証ログを確認します。

Microsoft AD

ACS は Microsoft Active Directory（AD）を外部 ID ストアとして使用して、ユーザ、マシン、グループ、属性などのリソースを格納します。ACS は、これらのリソースを AD に対して認証します。

サポートされる認証プロトコル

- EAP-FAST および PEAP：ACS 5.4 では、MSCHAPv2 および EAP-GTC という内部方式による EAP-FAST と PEAP を使用した、AD に対するユーザとマシンの認証およびパスワード変更がサポートされます。
- PAP：ACS 5.4 では、PAP を使用した AD に対する認証がサポートされ、AD ユーザ パスワードを変更することもできます。
- MSCHAPv1：ACS 5.4 では、MSCHAPv1 を使用した AD に対するユーザとマシンの認証がサポートされます。MSCHAPv1 バージョン 2 を使用すると、AD ユーザ パスワードを変更できます。ACS では、ユーザの MS-CHAP MPPE-Keys はサポートされませんが、MPPE-Send-Key および MPPE-Recv-Key はサポートされます。

（注）　ACS 5.4 では、MSCHAP バージョン 1 を使用した AD に対するユーザ パスワードの変更はサポートされません。

- MSCHAPv2：ACS 5.4 では、MSCHAPv2 を使用した AD に対するユーザとマシンの認証がサポートされます。ACS では、ユーザの MS-CHAP MPPE-Keys はサポートされませんが、MPPE-Send-Key および MPPE-Recv-Key はサポートされます。
- EAP-GTC：ACS 5.4 では、EAP-GTC を使用した AD に対するユーザとマシンの認証がサポートされます。

- EAP-TLS：ACS では、EAP-TLS を使用した AD に対するユーザとマシンの認証をサポートするために、5.4 で導入された証明書取得オプションが使用されます。

ACS 5.x では、TACACS+ PAP/ASCII、EAP-MSCHAP および EAP-GTC 方式で Active Directory に対して認証されたユーザのパスワード変更をサポートします。内部 MSCHAPv2 による EAP-FAST および PEAP のパスワード変更もサポートされています。

上記の方法を使用した AD ユーザ パスワードの変更では、AD パスワード ポリシーに準拠する必要があります。AD 管理者と相談して、AD パスワード ポリシーのすべてのルール セットを決定してください。特に重要な AD パスワード ポリシーは次のとおりです。

- Enforce password history: N passwords are remembered.
- Maximum password age is N days.
- Minimum password age is N days.
- Minimum password length is N characters.
- Password must meet complexity requirements.

AD は、[Maximum password age is N days] ルールを使用して、パスワードの期限切れを検出します。他のルールはすべてパスワードの変更を試行する際に使用されます。

ACS では、次に示す AD ドメインがサポートされています。

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

ACS Machine Access Restriction（MAR）機能は、AD を使用してマシン認証をユーザ認証および認可にマッピングし、マシン認証と、同じマシンからのユーザの認証の間で許可される最大時間を設定します。

通常、MAR は、ユーザのホスト マシンが認証に成功しない場合、またはマシンおよびユーザの認証間の時間が指定されたエージング タイムを超えた場合に、ユーザの認証に失敗します。必要に応じて、認証および認可規則の条件として MAR を追加できます。

ACS を AD ドメインに追加しようとするときに、ACS と AD は同期化されている必要があります。ACS の時間は、ネットワーク タイム プロトコル（NTP）サーバに従って設定されます。AD と ACS は、いずれも同じ NTP サーバによって同期化されている必要があります。ACS を AD ドメインに追加するときに時間が同期化されていない場合、ACS によってクロック スキュー エラーが表示されます。アプライアンスでコマンドライン インターフェイスを使用して、AD ドメインが同期化されている同じ NTP サーバと連携するように NTP クライアントを設定する必要があります。

NTP プロセスがダウンした場合は、自動的に再起動します。2 種類の方法で NTP プロセスのステータスを調べることができます。

- CLI インターフェイスで `sh app status acs` コマンドを使用します。
- ACS Web インターフェイスで [Monitoring and Reports] > [Reports] > [Catalog] > [ACS Instance] > [ACS_Health_Summary] を選択します。

詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli.html

ACS アプライアンスは、パフォーマンスを最適化するために、AD グループによって異なるキャッシング レベルを使用します。AD グループは固有識別子（SID、セキュリティ ID）で識別されます。ACS は、ユーザに属する SID を取得し、グループの完全な名前およびパスと SID とのキャッシュされ

たマッピングを使用します。AD クライアント コンポーネントは 24 時間マッピングをキャッシュしています。ACS のランタイム コンポーネントは、ACS が動作している限り、AD クライアントを照会し、結果をキャッシュします。

ACS 5.4 では、AD の接続の問題をトラブルシューティングするための AD クライアント トラブルシューティング ツールが提供されています。AD の接続問題をトラブルシューティングするには、コマンド adinfo、adcheck および ldapsearch を使用します。ACS はこれらの CLI コマンドを提供し、実行するために必要となるパラメータ、フラグ、条件も完全に同じです。また、ACS は、これらの CLI コマンド出力を ACSADAgent.log にリダイレクトします。

これらのコマンドの詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

（注）　ACS が古いマッピングを使用しないように、既存のマッピングを変更または移動するのではなく、新しい AD グループを作成する必要があります。既存のグループを変更または移動した場合、すべてのキャッシュ データを更新するために、24 時間待ってから ACS サービスを再起動しなければなりません。

ACS 5.4 では、証明書認可がサポートされています。

ACS と AD の間にファイアウォールがある場合は、ACS が AD と通信できるように特定のポートを開く必要があります。開く必要があるデフォルトのポートは次のとおりです。

プロトコル	ポート番号
LDAP	389/udp
SMB	445/tcp
KDC	88/tcp
グローバル カタログ	3268/tcp
KPASS	464/tcp
NTP	123/udp

（注）　ACS では、ダイヤルイン ユーザは AD によってサポートされません。

ここでは、次の内容について説明します。

- 「マシン認証」（P.8-42）
- 「認可のための属性取得」（P.8-42）
- 「認可のためのグループ取得」（P.8-42）
- 「EAP-TLS 認証のための証明書取得」（P.8-42）
- 「同時接続管理」（P.8-43）
- 「ユーザおよびマシン アカウントの制限」（P.8-43）
- 「マシン アクセス制限」（P.8-43）
- 「ダイヤルイン アクセス権」（P.8-45）
- 「ダイヤルイン ユーザのコールバック オプション」（P.8-46）
- 「AD ドメインへの ACS の追加」（P.8-47）
- 「AD グループの選択」（P.8-51）

- 「AD 属性の設定」（P.8-52）
- 「マシン アクセス制限の設定」（P.8-54）

マシン認証

マシン認証では、Active Directory にリストされているコンピュータに対してだけ、ネットワーク サービスへのアクセスが提供されます。このことは、無線ネットワークの場合に特に重要になります。権限のないユーザがオフィスの建物の外から無線アクセス ポイントにアクセスしようとする場合があるためです。

マシン認証は、コンピュータの起動時またはコンピュータへのログイン時に発生します。Funk Odyssey などのサプリカントは、サプリカントの実行中にマシン認証を定期的に実行します。

マシン認証をイネーブルにすると、ユーザ認証要求が到達する前に ACS はコンピュータを認証します。ACS は、コンピュータによって与えられたクレデンシャルを Windows ユーザ データベースに対して確認します。クレデンシャルが一致した場合に、ネットワークへのアクセスがコンピュータに与えられます。

認可のための属性取得

認可およびグループ マッピング規則で使用されるユーザまたはマシンの AD 属性を取得するように ACS を設定できます。属性は ACS ポリシー結果にマッピングされ、ユーザまたはマシンの承認レベルが決定されます。

ACS は、ユーザまたはマシンの認証が成功したあとにユーザおよびマシンの AD 属性を取得します。認証とは別に、認可およびグループ マッピングのために属性を取得することもできます。

認可のためのグループ取得

ACS は、認証が成功したあとにユーザまたはマシン グループを Active Directory から取得できます。認証とは別に、認可およびグループ マッピングのためにユーザまたはマシン グループを取得することもできます。AD グループ データを認可およびグループ マッピング テーブルで使用でき、特殊条件を導入して、取得したグループと突き合せることができます。

EAP-TLS 認証のための証明書取得

ACS 5.4 では、EAP-TLS プロトコルを使用するユーザまたはマシン認証のための証明書取得がサポートされています。AD 上のユーザまたはマシン レコードには、バイナリ データ型の証明書属性が含まれています。これに 1 つ以上の証明書を含めることができます。ACS ではこの属性は userCertificate として参照され、この属性に対して他の名前を設定することはできません。

ACS は、ユーザまたはマシンの ID を確認するためにこの証明書を取得します。証明書認証プロファイルによって、証明書を取得するために使用されるフィールド（SAN、CN、SSN、SAN-Email、SAN-DNS、またはその他の SAN 名）が決まります。

ACS は、証明書を取得したあと、この証明書とクライアント証明書とのバイナリ比較を実行します。複数の証明書が受信された場合、ACS は、それらのいずれかが一致するかどうかをチェックするために証明書を比較します。一致が見つかった場合、ACS はユーザまたはマシンにネットワークへのアクセスを付与します。

同時接続管理

起動時に、ACS が AD ドメインに接続したあと、ACS はパフォーマンス向上のために、AD ID ストアによって使用される数多くのスレッドを作成します。各スレッドに独自の接続があります。

ユーザおよびマシン アカウントの制限

ユーザまたはマシンの認証または問い合わせ中に、ACS は次のことをチェックします。

- ユーザ アカウントがディセーブルかどうか
- ユーザ アカウントがロックアウトされているかどうか
- ユーザ アカウントが期限切れかどうか
- クエリー実行が指定されたログイン時間外かどうか

ユーザにこれらの制限のいずれかがある場合、AD 専用ディクショナリ上の *AD1::IdentityAccessRestricted* 属性が設定され、ユーザのアクセスが制限されることが示されます。この属性は、グループ マッピングおよび認可規則に使用できます。

マシン アクセス制限

MAR は、マシン認証の結果をユーザ認証および認可プロセスに結びつけるのに役立ちます。MAR の最も一般的な使用法は、ホスト マシンが正常に認証されないユーザの認証を拒否することです。MAR は、すべての認証プロトコルに効果的です。

MAR の機能は、次の点に基づいています。

- マシンの RADIUS `Calling-Station-ID attribute (31)` は、マシン認証の結果として今後の参照用にキャッシュされます。
- 管理者は、AD の設定ページで上記のキャッシュ エントリの存続可能時間（TTL）を設定できます。
- 管理者は、AD の設定ページで MAR をイネーブルにするかどうかを設定できます。ただし、MAR を動作させる場合は、次の制限事項を考慮する必要があります。
  - 認証プロトコルの設定で、マシン認証をイネーブルにする必要があります。
  - AAA クライアントは、Internet Engineering Task Force（IETF）RADIUS `Calling-Station-Id attribute (31)` で値を送信する必要があります。
  - ACS は、正常なマシン認証から `Calling-Station-Id attribute` 値のキャッシュを複製しません。
  - ACS は、`Calling-Station-Id attribute` のキャッシュを保持しません。したがって、ACS を再起動したり、ACS がクラッシュしたりすると、キャッシュの内容は失われます。管理者がマシン認証に影響する可能性のある設定変更を行った場合、内容の整合性は確認されません。
- ユーザが AD 外部 ID ストアに対して PEAP または EAP-FAST を使用した認証を行うと、ACS は追加のアクションを実行します。ACS は、ユーザの `Calling-Station-Id` のキャッシュを検索します。このキャッシュが見つかった場合は、セッション コンテキストで **Was-Machine-Authenticated** 属性を true に設定し、見つからなかった場合は false に設定します。
- 上記を正しく機能させるため、ユーザ認証要求に `Calling-Station-Id` が含まれていることが必要です。この属性が含まれていない場合は、**Was-Machine-Authenticated** 属性を false に設定します。

- 管理者は、AD GM 属性とマシン認証の必須属性に基づいた規則を認可ポリシーに追加できます。これらの 2 つの属性を含む規則は、次の条件を満たしている場合のみ適用されます。
  - MAR 機能がイネーブルであること
  - 認証プロトコルの設定で、マシン認証がイネーブルであること
  - 外部 ID ストアが AD であること
- 上記のような規則が評価されると、AD GM および **Was-Machine-Authenticated** の属性がセッション コンテキストから取得され、規則の条件と照合されます。この評価の結果に応じて、認可結果が設定されます。
- 免除リストの機能は、（ACS 4.x とは対照的に）暗黙的にサポートされています)。所定のユーザ グループを MAR から免除するため、管理者は、[AD Group] カラムを免除するグループで構成し、[Machine Authentication Required] カラムを [*No*] で構成するように規則を設定できます。次に示すテーブルの 2 番めの規則がその一例です。

  たとえば、管理者は、次のように認可ポリシーに規則を追加します。

AD Group	Machine Authentication Required	…	ATZ プロファイル
Engineers	Yes	…	VLAN X
Managers	No	…	VLAN B
…	…	…	DENY ACCESS

[Engineers] の規則は、マシンが Windows DB に対して正常に認証された場合に限り、エンジニアにアクセスを許可する MAR 規則の例です。

[Managers] の規則は、MAR からの免除の例です。

分散 MAR キャッシュ

ACS 5.4 では、ACS の配置ごとにマシン アクセス制限キャッシュをサポートします。つまり、マシン認証結果を配置内の各ノードにキャッシュできます。

MAR キャッシュ分散グループ

ACS 5.4 では、ACS ノードを MAR キャッシュ分散グループにグループ化できます。このオプションは、ACS のパフォーマンスとメモリ使用量に与える MAR キャッシュ分散操作による影響を制御するために使用されます。

MAR キャッシュ分散グループ値と呼ばれるテキスト ラベルが各 ACS ノードに割り当てられます。ACS ノードは MAR キャッシュ分散グループ値に基づいてグループ化されます。同じ MAR キャッシュ分散グループに割り当てられた ACS ノード間でのみ、MAR キャッシュ分散操作を実行できます。

ACS ノードのグループ値が空の場合は、MAR キャッシュ分散グループに割り当てられていないと見なされます。このような ACS ノードは MAR キャッシュ分散操作に参加しません。

分散 MAR キャッシュの操作

ACS ランタイム コンポーネントは分散 MAR キャッシュを実装するために、2 種類の操作を組み合わせます。

- 配信保証なしの MAR キャッシュのレプリケーション
- MAR キャッシュ分散検索

MAR キャッシュのレプリケーション

ACS ランタイム コンポーネントは、マシン認証の間に、MAR エントリ `authenticated Calling-Station-ID` を MAR キャッシュに保存します。最初に、ACS は MAR エントリをローカル MAR キャッシュに保存します。次に、ACS ランタイム コンポーネントが、同じ MAR キャッシュ分散グループに属している ACS ノードに MAR エントリを複製します。

レプリケーションは、ACS Web インターフェイスで設定された [Cache entry replication attempts] および [Cache entry replication timeout] に基づいて実行されます。

レプリケーション操作はバックグラウンドで行われ、このレプリケーションを発生させたユーザ認証を中断または遅延させません。

MAR キャッシュ分散検索

最初に、ACS は MAR エントリをローカル MAR キャッシュで検索します。MAR エントリがローカルの MAR キャッシュに存在しない場合、ACS は同じ MAR キャッシュ分散グループに割り当てられた ACS ノードに問い合わせます。

分散検索は、ACS Web インターフェイスで設定された [Cache entry query attempts] および [Cache entry query timeout] に基づいて実行されます。また、MAR エントリ検索は、照会された ACS ノードのいずれかから最初の成功応答が返されるまで、最大で設定された [Cache entry query timeout] の時間まで延期されます。

ACS View での分散 MAR キャッシュの出力

- 24422：ACS は、Active Directory ユーザの以前の成功したマシン認証を確認しました。
- 24423：ACS は、Active Directory ユーザの以前の成功したマシン認証を確認できませんでした。
- 24701：ACS ピアは、Active Directory ユーザの以前の成功したマシン認証を確認しました。
- 24702：ACS ピアは、Active Directory ユーザの以前の成功したマシン認証を確認できませんでした。

分散 MAR キャッシュの信頼性

ACS ランタイム コンポーネントは、高い信頼性を確保するために、分散 MAR キャッシュを実装するために、2 種類の操作を組み合わせます。

分散検索オプションは、レプリケーション メッセージが何らかの理由で配信されない場合にフォールバック機能を提供します。この場合、マシン認証を実行する ACS ノードか、同じ MAR キャッシュ分散グループの ACS ノードのいずれかで、キャッシュ エントリを検索できます。また、分散検索オプションは、マシン認証を実行する ACS ノードの再起動時にフォール バック機能を提供します。

この場合も、同じ MAR キャッシュ分散グループの ACS ノードのいずれかで MAR キャッシュ エントリを検索できます。

ACS 展開の ACS ノードすべてを再起動すると MAR キャッシュ エントリが失われます。

ダイヤルイン アクセス権

ユーザのダイヤルイン アクセス権は、認証または Active Directory からのクエリーで確認されます。ダイヤルインのチェックは、次の認証プロトコルで、マシンではなくユーザの認証でサポートされます。

- PAP
- MSCHAPv2
- EAP-FAST

- PEAP
- EAP-TLS。

結果は次のとおりです。

- Allow Access
- Deny Access
- Control Access through Remote Access Policy。このオプションは、Windows 2000 ネイティブ ドメイン、Windows Server 2003 ドメインの場合のみ使用可能です。
- Control Access through NPS Network Policy。これはデフォルトの結果です。このオプションは、Windows Server 2008 および Windows 2008 R2 ドメインの場合のみ使用可能です。

ダイヤルイン ユーザのコールバック オプション

コールバック オプションがイネーブルの場合、サーバは接続プロセス中に発信者にコールバックします。サーバによって使用される電話番号は、発信者またはネットワーク管理者によって設定されます。

コールバック オプションは次のいずれかです。

- No callback
- Set by Caller（ルーティングとリモート アクセス サービスのみ）。このオプションは、接続が行われたときにルーティングとリモート アクセス サービスを実行しているサーバのルーティング テーブルに追加される一連のスタティック IP ルートの定義に使用できます。
- Always callback to（番号を設定するオプションを含む）。このオプションは、接続が行われたときにユーザに特定の IP アドレスを割り当てるために使用できます。

コールバック属性は、デバイスへの RADIUS 応答で返される必要があります。

ダイヤルイン サポートの属性

Active Directory のユーザ属性は、次のサーバでサポートされます。

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

ACS は、Windows 2000 のダイヤルイン ユーザをサポートしません。

ACS 応答

ACS Active Directory でダイヤルインのチェックをイネーブルにした場合、ユーザのダイヤルイン オプションが Active Directory で [Deny Access] の場合、認証要求は拒否され、ダイヤルイン アクセスが拒否されたことを示すメッセージがログに記録されます。ダイヤルインがイネーブルでない場合に、ユーザが MSCHAP v1/v2 の認証で失敗すると、ACS は EAP 応答で適切なエラー コード（NT エラー = 649）を設定します。

コールバック オプションがイネーブルの場合、ACS RADIUS 応答には、次のように返されたサービス タイプおよびコールバック番号属性が含まれます。

- コールバック オプションが [Set by Caller] または [Always Callback To] の場合、service-type 属性は、ユーザ認証時に Active Directory に問い合わせる必要があります。service-type は次のようになります。
  - 3 = コールバック ログイン

  - 4 = コールバック構築
  - 9 = コールバック NAS プロンプト

  この属性は、service-type RADIUS 属性でデバイスに返す必要があります。RADIUS 応答で service-type 属性を返すように ACS がすでに設定されている場合、Active Directory のユーザを問い合わせるための service-type 値に置き換えられます。

- コールバック オプションが [Always Callback To] の場合、Active Directory ユーザのコールバック番号も問い合わせる必要があります。この値は、RADIUS 応答の Cisco-AV-Pair 属性に次の値で設定されます。
  - cisco-av-pair=lcp:callback-dialstring=[コールバック番号値]
  - cisco-av-pair=Shell:callback-dialstring=[コールバック番号値]
  - cisco-av-pair=Slip:callback-dialstring=[コールバック番号値]
  - cisco-av-pair=Arap:callback-dialstring=[コールバック番号値]

  コールバック番号値も、RADIUS 属性 CallbackNumber（#19）を使用して、RADIUS 応答で返されます。
- コールバック オプションが [Set by Caller] の場合、RADIUS 応答には、値なしで次の属性が含まれます。
  - cisco-av-pair=lcp:callback-dialstring=
  - cisco-av-pair=Shell:callback-dialstring=
  - cisco-av-pair=Slip:callback-dialstring=
  - cisco-av-pair=Arap:callback-dialstring=

AD ドメインへの ACS の追加

ACS 5.4 では、同じ展開の ACS ノードを異なる AD ドメインに追加できます。ただし、各ノードは、単一の AD ドメインにのみ追加できます。これらの ACS ノードのポリシー定義は変更されず、同じ AD ID ストアを使用します。

AD ID ストアの設定方法の詳細については、「AD ID ストアの設定」（P.8-47）を参照してください。

（注）　AD ドメインに ACS を追加する Windows AD アカウントは、独自の組織ユニット (OU) で作成できます。アカウントを作成するときまたは後で独自 OU で作成できますが、アプライアンスの名前が AD アカウント名に一致する必要があります。

関連トピック

「マシン認証」（P.B-35）

AD ID ストアの設定

AD の設定はデフォルトで表示されず、最初に ACS をインストールしたとき、AD ドメインに追加されません。AD の設定ページを開くと、分散展開内のすべての ACS ノードのリストが表示されます。

AD ID ストアを設定すると、ACS によって次のものも作成されます。

- 2 個の属性（ExternalGroup 属性と、[Directory Attributes] ページから取得される属性用の別の属性）を持つそのストア用の新しいディクショナリ。
- 新しい属性 IdentityAccessRestricted。この属性のカスタム条件を手動で作成できます。

- ExternalGroup 属性からのグループ マッピングのカスタム条件（カスタム条件名は AD1:ExternalGroups）、および [Directory Attributes] ページで選択された各属性用の別のカスタム条件（AD1:cn など）。

事前定義済みの条件名を編集でき、[Custom condition] ページからカスタム条件を作成できます。「カスタム セッション条件の作成、複製、および編集」（P.9-5）を参照してください。

（注）　ACS サーバの再イメージ化とアップグレードの方法で ACS を ACS 5.4 バージョンにアップグレードする場合、AD が定義されている設定を復元するには、AD ドメインに ACS を手動で追加する必要があります。アップグレード方法の詳細については、『Installation and Upgrade Guide for Cisco Secure Access Control System』を参照してください。

（注）　アプリケーション アップグレード バンドルを使用した ACS サーバのアップグレードの方法で ACS を ACS 5.4 にアップグレードする場合、AD にすでに ACS を結合している場合は、ACS はアプリケーションのアップグレード後も AD に追加されたままです。

ユーザを認証し、ACS を AD ドメインに追加するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択します。

[Active Directory] ページが表示されます。

AD の設定ページは、すべての ACS ノードの集中 AD 管理ツールとして機能します。単一の ACS ノードまたは複数の ACS ノードに対して、このページで追加操作および接続テスト操作を実行できます。また、展開内のすべての ACS ノードの追加結果が一目でわかるように表示されます。

ステップ 2　表 8-10 の説明に従って、[General] タブのフィールドを変更します。

表 8-10　[Active Directory: General] ページ

オプション	説明
Connection Details	
Join/Test Connection	クリックすると、入力したユーザ、ドメイン、パスワードを使用して、AD ドメインとの間で追加または ACS 接続のテストが行われます。「AD ドメインへのノードの追加」（P.8-49）を参照してください。
Leave	入力したユーザ、ドメイン、パスワードを使用して、AD ドメインから単一ノードまたは複数ノードを切断する場合にクリックします。「AD ドメインからノードの接続解除」（P.8-50）を参照してください。
End User Authentication Settings	
Enable password change	パスワード変更を許可する場合にクリックします。
Enable machine authentication	マシン認証を許可する場合にクリックします。
Enable dial-in check	認証またはクエリー時にユーザのダイヤルイン アクセス権を確認する場合にクリックします。ダイヤルイン アクセス権が拒否されている場合は、チェックの結果により認証拒否の原因になります。 結果は AD ディクショナリに保存されません。
Enable callback check for dial-in clients	認証またはクエリー時にユーザのコールバック オプションを検査する場合にクリックします。チェックの結果は、RADIUS 応答でデバイスに返されます。 結果は AD ディクショナリに保存されません。

表 8-10　[Active Directory: General] ページ （続き）

オプション	説明
Connectivity Status	
Joined to Domain	（*表示のみ。*）設定の保存後（[Save Changes] をクリック）、ACS が追加されたドメイン名が表示されます。
Connectivity Status	（*表示のみ。*）設定の保存後（[Save Changes] をクリック）、ACS が追加されたドメイン名の接続ステータスが表示されます。

ステップ 3　次のいずれかをクリックします。

- 設定を保存するには、[Save Changes]。
- 変更をすべて廃棄するには、[Discard Changes]。
- AD がすでに設定されており、それを削除する場合は、次のことを確認したあとで [Clear Configuration] 。
  - AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がない。
  - 使用可能なアクセス サービスで AD が ID ソースとして選択されていない。
  - AD に ID ストア順序がない。

Active Directory の設定が保存されます。[Active Directory] ページが新しい設定で表示されます。

（注）　AD ドメインとの ACS 接続をテストする間、サーバの応答が遅い場合、Centrify の設定が影響を受けます（または切断されることがあります）。ただし、設定は他のアプリケーションでは正常に機能します。

（注）　NETBIOS の制限により、ACS ホスト名は 15 文字以下にする必要があります。

AD ドメインへのノードの追加

AD ドメインに単一ノードまたは複数ノードを追加するには、次の手順を実行してください。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択します。

[Active Directory] ページが表示されます。

ステップ 2　単一ノードまたは複数ノードを選択し、[Join/Test Connection] をクリックします。

[Join/Test Connection] ページが表示されます。

ステップ 3　表 8-11 の説明に従って、[Join/Test Connection] ページのフィールドに入力します。

表 8-11　[Join/Test Connection] ページ

オプション	説明
Active Directory Domain Name	ACS を追加する AD ドメインの名前。
Username	事前定義された AD ユーザのユーザ名を入力します。ACS でのドメイン アクセスに必要な AD アカウントには、次のいずれかが必要です。 • 対応するドメインのドメイン ユーザにワーク ステーションを追加する権限。 • ACS マシンのアカウントが事前に作成される（ACS マシンをドメインに追加する前に作成される）対応するコンピュータ コンテナに対してコンピュータ オブジェクトを作成する権限またはコンピュータ オブジェクトを削除する権限。 ACS アカウントのロックアウト ポリシーをディセーブルにし、不正なパスワードがこのアカウントに使用された場合に管理者にアラートを送信するように AD インフラストラクチャを設定することを推奨します。これは、誤ったパスワードを入力した場合、ACS が必要なときにマシン アカウントを作成または変更しないため、すべての認証が拒否されるためです。
Password	ユーザ パスワードを入力します。パスワードは、少なくとも 1 文字の小文字、1 文字の大文字、1 文字の数字、および 1 文字の特殊文字を組み合わせて、8 文字以上にする必要があります。すべての特殊文字がサポートされています。

ステップ 4　次のいずれかをクリックします。

- [Join]：AD ドメインに選択したノードを追加します。ノードの状態が結合の結果によって変化します。
- [Test Connection]：接続をテストして、入力されたクレデンシャルが正しく、AD ドメインが到達可能であることを確認します。AD サーバがネットワーク内でルーティング可能かどうか、および指定の AD ユーザ名およびパスワードの認証も実行するかどうかを示すメッセージが表示されます。接続テストの結果は表形式で別のダイアログボックスに表示されます。
- [Cancel]：接続をキャンセルします。

AD ドメインからノードの接続解除

AD ドメインから単一ノードまたは複数ノードを接続解除するには、次の手順を実行してください。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択します。

[Active Directory] ページが表示されます。

ステップ 2　単一ノードまたは複数ノードを選択し、[Leave] をクリックします。

[Leave Connection] ページが表示されます。

ステップ 3　表 8-12 の説明に従って、[Leave Connection] ページのフィールドに入力します。

表 8-12　[Leave Connection] ページ

オプション	説明
Username	事前定義された AD ユーザのユーザ名を入力します。ACS でのドメイン アクセスに必要な AD アカウントには、次のいずれかが必要です。 • 対応するドメインのドメイン ユーザにワーク ステーションを追加する権限。 • ACS マシンのアカウントが事前に作成される（ACS マシンをドメインに追加する前に作成される）対応するコンピュータ コンテナに対してコンピュータ オブジェクトを作成する権限またはコンピュータ オブジェクトを削除する権限。 ACS アカウントのロックアウト ポリシーをディセーブルにし、不正なパスワードがこのアカウントに使用された場合に管理者にアラートを送信するように AD インフラストラクチャを設定することを推奨します。これは、誤ったパスワードを入力した場合、ACS が必要なときにマシン アカウントを作成または変更しないため、すべての認証が拒否されるためです。
Password	ユーザ パスワードを入力します。
Do not try to remove machine account	クレデンシャルがわからない場合または DNS の問題がある場合に、選択したノードを AD ドメインから接続解除するには、このチェックボックスをオンにします。 この操作は、AD ドメインからノードを切断し、データベースにこのノードのエントリをそのまま残します。管理者だけが、データベースからこのノード エントリを削除できます。

ステップ 4　次のいずれかをクリックします。

- [Leave]：選択したノードを AD ドメインから切断します。
- [Cancel]：操作をキャンセルします。

（注）　管理者は、セカンダリ サーバから追加、削除、接続テストなどの操作を実行できます。セカンダリ サーバで次の操作を実行すると、セカンダリ サーバだけに影響します。

関連トピック

- 「AD グループの選択」（P.8-51）
- 「AD 属性の設定」（P.8-52）
- 「マシン アクセス制限の設定」（P.8-54）

AD グループの選択

このページは、ポリシー条件に使用できるグループを選択する場合に使用します。

（注）　AD からグループおよび属性を選択するには、ACS がその AD に接続されている必要があります。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択し、[Directory Groups] タブをクリックします。

[Groups] ページが表示されます。[Selected Directory Groups] フィールドに、選択して保存した AD グループが表示されます。[External User Groups] ページで選択した AD グループが表示され、規則テーブルのグループ マッピング条件でオプションとして使用できます。

表示されていない他の信頼ドメインまたはフォレストにさらにグループがある場合は、検索フィルタを使用して検索結果を絞り込むことができます。[Add] ボタンを使用して新しい AD グループを追加することもできます。

（注）　ACS 5.4 は、ドメイン ローカル グループを取得しません。ACS ポリシーでドメイン ローカル グループを使用することは推奨されません。その理由は、ドメイン ローカル グループでのメンバーシップ評価には時間がかかるためです。そのため、デフォルトでは、ドメイン ローカル グループは評価されません。

ステップ 2　[Select] をクリックして、ドメイン（および同じフォレスト内の他の信頼ドメイン）で使用可能な AD グループを表示します。

[External User Groups] ダイアログボックスが表示され、ドメインおよび同じフォレスト内の他の信頼ドメインの AD グループのリストが表示されます。

表示されていないグループがさらにある場合は、検索フィルタを使用して検索を絞り込み、[Go] をクリックします。

ステップ 3　AD グループを入力するか、リストから選択し、[OK] をクリックします。

AD グループをリストから削除するには、AD グループをクリックして [Deselect] をクリックします。

ステップ 4　次のいずれかをクリックします。

- 設定を保存するには、[Save Changes]。
- 変更をすべて廃棄するには、[Discard Changes]。
- AD がすでに設定されており、それを削除する場合は、AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がないことを確認したあとで、[Clear Configuration] をクリックします。

（注）　ACS 5.x で AD ID ストアを設定する場合、Active Directory に定義されているセキュリティ グループが列挙され、使用できますが、分散グループは表示されません。Active Directory の分散グループはセキュリティ対応でないため、ユーザの集合に電子メールを送信するために電子メール アプリケーションで使用することしかできません。分散グループの詳細については、Microsoft のマニュアルを参照してください。

（注）　ACS が外部 ID ストアの 1015 グループ以上に属するユーザを認証しようとすると、Active Directory でログイン認証が失敗することがあります。これは、Active Directory のローカル セキュリティ認証（LSA）の制限によるものです。

AD 属性の設定

このページは、ポリシー条件に使用できる属性を選択する場合に使用します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択し、[Directory Attributes] タブをクリックします。

ステップ 2　表 8-13 の説明に従って、[Active Directory: Attributes] ページのフィールドに入力します。

表 8-13　[Active Directory: Attributes] ページ

オプション	説明
Name of example Subject to Select Attributes	追加されたドメインで見つかったユーザまたはコンピュータの名前を入力します。ユーザまたはコンピュータの CN または識別名を入力できます。 表示される属性のセットは、指定するサブジェクトに所属します。属性のセットは、ユーザおよびコンピュータごとに異なります。
Select	[Attributes] セカンダリ ウィンドウにアクセスする場合にクリックします。このウィンドウには、上記のフィールドに入力した名前の属性が表示されます。
Attribute Name List：セカンダリ [Selected Attributes] ウィンドウで選択した属性が表示されます。複数の属性を選択し、同時に送信できます。	
Attribute Name	• 次のいずれかを実行します。 – 属性の名前を入力します。 – リストから属性を選択し、[Edit] をクリックして属性を編集することもできます。 • [Add] をクリックして、属性を [Attribute Name list] に追加します。
Type	属性名に関連付けられた属性タイプ。有効なオプションは次のとおりです。 • String • Unsigned Integer 64 • IP Address：IPv4 または IPv6 アドレスを指定できます。
Default	選択した属性に対して指定されている属性デフォルト値。 • String：属性名。 • Unsigned Integer 64：0。 • IP Address：デフォルト設定なし。
Policy Condition Name	この属性のカスタム条件名を入力します。たとえば、カスタム条件名が *AAA* の場合は、このフィールドに **AAA** を入力します。**AD1:***att_name* ではありません。
[Select Attributes] セカンダリ ウィンドウ	[Attributes] セカンダリ ウィンドウからだけ使用できます。
Search Filter	ユーザ名またはマシン名を指定します。 • ユーザ名の場合、認定者名、SAM、NetBios、または UPN フォーマットを指定できます。 • マシン名の場合、MACHINE$、NETBiosDomain\MACHINE$、host/MACHINE、または host/machine.domain フォーマットのいずれかを指定できます。ユーザ名およびマシン名には英語以外の文字を指定できます。
Attribute Name	上記のフィールドで入力したユーザ名またはマシン名の属性の名前。
Attribute Type	属性のタイプ。
Attribute Value	指定したユーザまたはマシンの属性の値。

ステップ 3　次のいずれかをクリックします。

- 設定を保存するには、[Save Changes]。

- 変更をすべて廃棄するには、[Discard Changes]。
- AD がすでに設定されており、それを削除する場合は、AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がないことを確認したあとで、[Clear Configuration] をクリックします。

マシン アクセス制限の設定

マシン アクセス制限を設定するには、次の手順を実行してください。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択してから、[Machine Access Restrictions] タブをクリックします。

ステップ 2　表 8-14 の説明に従って、[Active Directory: Machine Access Restrictions] ページのフィールドに入力します。

表 8-14　[Active Directory: Machine Access Restrictions] ページ

オプション	説明
Enable Machine Access Restrictions	Web インターフェイスでのマシン アクセス制限の制御をイネーブルにするには、このチェックボックスをチェックします。これにより、マシン認証結果がユーザの認証および認可に結び付けられます。この機能をイネーブルにした場合は、[Aging time] を設定する必要があります。
Aging time (hours)	マシンが認証されたあと、そのマシンからユーザを認証できる時間。この時間が経過すると、ユーザ認証は失敗します。デフォルト値は 6 時間です。有効な範囲は 1 ～ 8760 時間です。
MAR Cache Distribution	
Cache entry replication timeout	キャッシュ エントリのレプリケーションがタイムアウトする時間を秒単位で入力します。デフォルト値は 5 秒です。有効な範囲は 1 ～ 10 です。
Cache entry replication attempts	ACS が MAR キャッシュ エントリのレプリケーションを実行しなければならない回数を入力します。デフォルト値は 2 です。有効な範囲は 0 ～ 5 です。
Cache entry query timeout	キャッシュ エントリのクエリーがタイムアウトする時間を秒単位で入力します。デフォルト値は 2 秒です。有効な範囲は 1 ～ 10 です。
Cache entry query attempts	ACS がキャッシュ エントリのクエリーを実行しなければならない回数を入力します。デフォルト値は、1 です 有効な範囲は 0 ～ 5 です。
Node	この AD ドメインに接続されているすべてのノードが表示されます。
Cache Distribution Group	選択したノードのキャッシュ分散グループを入力します。ここには、最大 64 文字のテキスト文字列を入力できます。

ステップ 3　次のいずれかをクリックします。

- 設定を保存するには、[Save Changes]。
- 変更をすべて廃棄するには、[Discard Changes]。
- AD がすでに設定されており、それを削除する場合は、AD ディクショナリに基づくカスタム条件を使用しているポリシー規則がないことを確認したあとで、[Clear Configuration] をクリックします。

ユーザが多数のグループに属する AD の導入

ACS 5.3 では、ユーザが多数のグループ（50 を超えるグループ）に属している場合、AD ドメイン間を移動すると、ユーザ認証がタイムアウト エラーになります。しかし、同じユーザまたは同じグループに属する他のユーザの後続の認証は適切に動作します。これは、ACS AD エージェント構成の adclient.get.builtin.membership パラメータが原因です。このパラメータを true に設定すると、多くの追加要求が実行され、多数のグループに属するユーザで時間がかかります。
adclient.get.builin.membership パラメータが true に設定された後、AD の組み込みグループが ACS ポリシーで使用できなくなることがわかります。そのため、この問題を解決するには、**adclient.get.builtin.membership** パラメータを false に設定する必要があります。

adclient.get.builin.membership パラメータを設定するには、ACS CLI から次の手順を実行します。

ステップ 1　コンフィギュレーション モードで ACS CLI にログインします。

ステップ 2　次のコマンドを入力します。

```
acs-config
ad-agent-configuration adclient.get.builtin.membership false
```

（注）　多数のグループに属するユーザの最初の認証がタイムアウト エラーで失敗することがあります。しかし、同じユーザまたは同じグループに属する他のユーザの後続の認証は適切に動作します。

RSA SecurID サーバ

ACS では、外部データベースとして RSA SecurID サーバがサポートされています。RSA SecurID の 2 要素認証は、ユーザの個人識別番号（PIN）と、タイム コード アルゴリズムに基づいて使い捨てのトークン コードを生成する個別に登録された RSA SecurID トークンで構成されます。

異なるトークン コードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。RSA SecurID サーバでは、この動的な認証コードが確認されます。各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。

そのため、正しいトークン コードが PIN とともに提示された場合、その人が有効なユーザである確実性が高くなります。したがって、RSA SecurID サーバでは、従来の再使用可能なパスワードよりも信頼性の高い認証メカニズムが提供されます。

次のいずれかの方法で、RSA SecurID 認証テクノロジーと統合できます。

- RSA SecurID エージェントの使用：ユーザは、RSA のネイティブ プロトコルによってユーザ名およびパスコードで認証されます。
- RADIUS プロトコルの使用：ユーザは、RADIUS プロトコルによってユーザ名およびパスコードで認証されます。

ACS 5.4 の RSA SecurID トークン サーバは、RSA SecurID エージェントを使用して RSA SecurID 認証テクノロジーと統合します。

RSA SecurID エージェントの設定

RSA SecurID サーバ管理者は、次のことを実行できます。

- 「エージェント レコード（sdconf.rec）の作成」（P.8-56）
- 「ノード秘密（securid）のリセット」（P.8-56）
- 「自動ロード バランシングの無効化」（P.8-56）
- 「手動介入によるダウンした RSA SecurID サーバの削除」（P.8-56）

エージェント レコード（sdconf.rec）の作成

ACS 5.4 の RSA SecurID トークン サーバを設定するには、ACS 管理者に *sdconf.rec* ファイルが必要です。*sdconf.rec* ファイルは、RSA エージェントと RSA SecurID サーバ領域との通信方法を指定する設定レコード ファイルです。

sdconf.rec ファイルを作成するために、RSA SecurID サーバ管理者は、RSA SecurID サーバ上のエージェント ホストとして ACS ホストを追加し、このエージェント ホストの設定ファイルを生成する必要があります。

ノード秘密（securid）のリセット

エージェントが最初に RSA SecurID サーバと通信したあと、サーバは securid というノード秘密ファイルをエージェントに提供します。サーバとエージェント間のその後の通信は、ノード秘密の交換による相手の認証の確認によって行われます。

ノード秘密をリセットする必要がある場合があります。ノード秘密をリセットするには、次の手順を実行します。

- RSA SecurID サーバ管理者は、RSA SecurID サーバの Agent Host レコードの [Node Secret Created] チェックボックスをオフにする必要があります。
- ACS 管理者は、securid ファイルを ACS から削除する必要があります。

自動ロード バランシングの無効化

RSA SecurID エージェントでは、RSA SecurID サーバ上の要求された負荷は領域内で自動的に分散されます。ただし、負荷を手動で分散するオプションがあります。エージェント ホストが認証要求を一部のサーバに他のサーバよりも頻繁に送信するように、各エージェント ホストが使用する必要があるサーバを指定し、各サーバに優先順位を割り当てることができます。

優先順位設定をテキスト ファイルに指定し、sdopts.rec として保存する必要があります。それを ACS にアップロードできます。

手動介入によるダウンした RSA SecurID サーバの削除

RSA SecurID サーバがダウンした場合、自動除外メカニズムが迅速に機能しないことがあります。このプロセスを迅速化するために、*sdstatus.12* ファイルを ACS から削除できます。

RSA SecurID トークン サーバの作成および編集

ACS 5.4 では、ワンタイム パスワードによってセキュリティを向上させるために、ユーザ認証用の RSA SecurID トークン サーバがサポートされています。RSA SecurID トークン サーバによって、ユーザの認証を確実にする 2 要素認証が提供されます。

RSA ID ストアに対してユーザを認証するには、最初に ACS で RSA SecurID トークン サーバを作成し、領域、ACS インスタンス、および高度な設定を設定する必要があります。

ACS 5.4 では、1 つの RSA 領域だけがサポートされています。RSA 領域設定を設定できます。1 つの領域に数多くの ACS インスタンスを含めることができます。

（注）　RSA SecurID サーバ管理者から *sdconf.rec* ファイルを受け取り、ACS に保存する必要があります。

RSA SecurID トークン サーバを作成または編集するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [RSA SecurID Token Servers] を選択します。

[RSA SecurID Token Servers] ページが表示されます。

ステップ 2　[Create] をクリックします。

変更する ID ストア名をクリックするか、名前の隣にあるボックスをオンにして [Edit] をクリックすることもできます。

ステップ 3　表 8-15 の説明に従って、[RSA Realm Settings] タブのフィールドに入力します。

表 8-15　[RSA Realm Settings] タブ

オプション	説明
General	
Name	RSA 領域の名前。
Description	（任意）RSA 領域の説明。
Server Connection	
Server Timeout *n* seconds	タイムアウトまでに、ACS は RSA SecurID トークン サーバへの接続を *n* 秒間待機します。
Reauthenticate on Change PIN	変更 PIN で再認証する場合に、このチェックボックスをオンにします。
Realm Configuration File	
Import new 'sdconf.rec' file	[Browse] をクリックして、マシンから *sdconf.rec* ファイルを選択します。
Node Secret Status	ユーザが RSA SecurID トークン サーバに対して最初に認証されると、[Node Secret Status] に [Created] と表示されます。

ステップ 4　[ACS Instance Settings] タブをクリックします。詳細については、「ACS インスタンス設定の設定」（P.8-58）を参照してください。

ステップ 5　[Advanced] タブをクリックします。詳細については、「高度なオプションの設定」（P.8-60）を参照してください。

ステップ 6　[Submit] をクリックして、RSA SecurID ストアを作成します。

設定したサーバが含まれた [RSA SecurID Token Server] ページが表示されます。

関連トピック：

- 「RSA SecurID サーバ」（P.8-55）
- 「ACS インスタンス設定の設定」（P.8-58）
- 「高度なオプションの設定」（P.8-60）

ACS インスタンス設定の設定

[ACS Instance Settings] タブには、アクティブな ACS インスタンスの最新のリストが表示されます。これらのエントリを追加または削除することはできません。ただし、これらの ACS インスタンスそれぞれの使用可能な RSA 領域設定は編集できます。

表 8-16 に、[ACS Instance Settings] タブのフィールドを示します。

表 8-16　[ACS Instance Settings] タブ

オプション	説明
ACS Instance	ACS インスタンスの名前。
Options File	オプション ファイルの名前。
Node Secret Status	ノード秘密のステータス。次のいずれかになります。 • Created • Not created

このページに表示される ACS インスタンスの設定を編集できます。次の手順を実行します。

ステップ 1　編集する ACS インスタンスの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[ACS instance settings] ダイアログボックスが表示されます。このダイアログボックスには、次のタブがあります。

- RSA Options File：詳細については、「ACS インスタンス設定の編集」（P.8-58）を参照してください。
- Reset Agents Files：詳細については、「ACS インスタンス設定の編集」（P.8-58）を参照してください。

ステップ 2　[OK] をクリックします。

関連トピック

- 「RSA SecurID サーバ」（P.8-55）
- 「RSA SecurID トークン サーバの作成および編集」（P.8-56）
- 「ACS インスタンス設定の編集」（P.8-58）
- 「ACS インスタンス設定の編集」（P.8-58）
- 「高度なオプションの設定」（P.8-60）

ACS インスタンス設定の編集

ACS インスタンス設定を編集して、次のことを実行できます。

- 「RSA オプション ファイルのイネーブル化」（P.8-58）
- 「エージェント ファイルのリセット」（P.8-59）

RSA オプション ファイルのイネーブル化

各 ACS インスタンスで RSA オプション ファイル（*sdopts.rec*）をイネーブルにして、領域内の RSA エージェントと RSA サーバ間の接続のルーティング優先順位を制御できます。

表 8-17 に、[RSA Options File] タブのフィールドを示します。

表 8-17　[RSA Options File] タブ

オプション	説明
各 ACS インスタンスで RSA オプション ファイル（sdopts.rec）をイネーブルにして、領域内の RSA エージェントと RSA サーバ間の接続のルーティング優先順位を制御できます。sdopts.rec のフォーマットの詳細については、RSA のマニュアルを参照してください。	
Use the Automatic Load Balancing status maintained by the RSA Agent	RSA エージェントが保持する自動ロード バランシング ステータスを使用する場合に、このオプションを選択します。
Override the Automatic Load Balancing status with the sdopts.rec file selected below	sdopts.rec ファイルで指定される自動ロード バランシング ステータスを使用する場合に、このオプションを選択します。
Current File	現在選択されている sdopts.rec ファイルが表示されます。
Timestamp	sdopts.rec ファイルが最後に変更された時刻。
File Size	sdopts.rec ファイルのサイズ。
Import new 'sdopts.rec' file	[Browse] をクリックして、ハード ドライブから新しい sdopts.rec ファイルをインポートします。
（注）　このポップアップを起動したページが送信されるまで、変更は有効になりません。	

次のいずれかを実行します。

- [OK] をクリックしてコンフィギュレーションを保存します。
- 領域内のアクティブおよび非アクティブ サーバの秘密キー情報またはステータスをリセットするには、[Reset Agent Files] タブをクリックします。

関連トピック

- 「RSA SecurID サーバ」（P.8-55）
- 「RSA SecurID トークン サーバの作成および編集」（P.8-56）
- 「ACS インスタンス設定の設定」（P.8-58）
- 「ACS インスタンス設定の編集」（P.8-58）
- 「高度なオプションの設定」（P.8-60）

エージェント ファイルのリセット

このページは、次の項目をリセットする場合に使用します。

- ノード秘密キー ファイル。RSA サーバとの通信が暗号化されるようにします。
- 領域内のサーバのステータス。

ステップ 1　次のオプションのいずれかを選択します。

- エージェント ホストのノード秘密をリセットするには、[Remove securid file on submit] チェックボックスをオンにします。

エージェント ホストのノード秘密をリセットする場合、RSA サーバでエージェント ホストのノード秘密をリセットする必要があります。

- 領域内のサーバのステータスをリセットするには、[Remove sdstatus.12 file on submit] チェックボックスをオンにします。

ステップ 2　[OK] をクリックします。

関連トピック

- 「RSA SecurID サーバ」（P.8-55）
- 「RSA SecurID トークン サーバの作成および編集」（P.8-56）
- 「ACS インスタンス設定の設定」（P.8-58）
- 「ACS インスタンス設定の編集」（P.8-58）
- 「高度なオプションの設定」（P.8-60）

高度なオプションの設定

このページは、次のことを実行する場合に使用します。

- RSA SecurID トークン サーバからのアクセス拒否がどのような意味を持つかを定義します。
- ID キャッシングのイネーブル化：RSA でのユーザのキャッシングは、キャッシングのロジックと目的が同じであるため、RADIUS トークンでのユーザのキャッシングと似ています。唯一の違いは、RSA ではユーザの属性取得がないため、属性のキャッシングがないことです。認証されたユーザはキャッシュされますが、属性はキャッシュされません。

RSA 領域の高度なオプションを設定するには、次の手順を実行します。

ステップ 1　次のいずれかを実行します。

- [Treat Rejects as Authentication failed] オプション ボタンをクリック：ACS は認証失敗として RSA SecurdID ストアからの認証拒否と解釈します。
- [Treat Rejects as User not found] オプション ボタンをクリック：ACS は「ユーザが見つかりませんでした」として RSA SecurID ストアからの認証拒否と解釈します。

ステップ 2　ID キャッシングをイネーブルにして、RSA サーバによって認証されない要求を ACS で処理できるようにします。

最後に成功した認証から取得された結果が、指定された時間、キャッシュ内で使用可能になります。

ステップ 3　[Enable identity caching] チェックボックスをオンにします。

ステップ 4　エージング タイムを分単位で入力します。

ID キャッシュには、ここで指定した時間だけ、成功したログインの結果が格納されます。

ステップ 5　[Submit] をクリックします。

関連トピック

- 「RSA SecurID サーバ」（P.8-55）
- 「RSA SecurID トークン サーバの作成および編集」（P.8-56）
- 「ACS インスタンス設定の設定」（P.8-58）
- 「ACS インスタンス設定の編集」（P.8-58）
- 「ACS インスタンス設定の編集」（P.8-58）

RADIUS ID ストア

RADIUS サーバは、RADIUS インターフェイスをサポートするサードパーティ製サーバです。ACS の一部である RADIUS ID ストアは、RADIUS サーバに接続されます。

RADIUS サーバとは、標準 RADIUS インターフェイスが組み込まれたサーバ、および RADUIS インターフェイスをサポートするその他のサーバのことです。ACS 5.4 では、RADIUS RFC 2865 準拠の任意のサーバが外部 ID ストアとしてサポートされています。ACS 5.4 では、複数の RADIUS トークン サーバ ID がサポートされています。

たとえば、RSA SecurID サーバや SafeWord サーバなどです。RADIUS ID ストアは、ユーザを認証するために使用される任意の RADIUS トークン サーバと連携できます。RADIUS ID ストアでは、認証セッションに UDP ポートが使用されます。すべての RADIUS 通信に同じ UDP ポートが使用されます。

（注）　ACS で RADIUS メッセージを RADIUS 対応サーバに正常に送信するには、RADIUS 対応サーバと ACS の間のゲートウェイ デバイスが、UDP ポートを介した通信を許可するように設定されている必要があります。UDP ポートは、ACS Web インターフェイスを介して設定できます。

ここでは、次の内容について説明します。

- 「サポートされる認証プロトコル」（P.8-61）
- 「フェールオーバー」（P.8-61）
- 「パスワード プロンプト」（P.8-62）
- 「ユーザ グループ マッピング」（P.8-62）
- 「グループおよび属性マッピング」（P.8-62）
- 「ID 順序での RADIUS ID ストア」（P.8-62）
- 「認証失敗メッセージ」（P.8-63）
- 「Safeword サーバでのユーザ名の特殊フォーマット」（P.8-63）
- 「ユーザ属性キャッシュ」（P.8-64）
- 「RADIUS ID サーバの作成、複製、および編集」（P.8-64）

サポートされる認証プロトコル

ACS では、RADIUS ID ストアに対して次の認証プロトコルがサポートされています。

- RADIUS PAP
- TACACS+ ASCII/PAP
- 内部 EAP-GTC を含む PEAP
- 内部 EAP-GTC を含む EAP-FAST

フェールオーバー

ACS 5.4 では、複数の RADIUS ID ストアを設定できます。各 RADIUS ID ストアには、プライマリ RADIUS サーバとセカンダリ RADIUS サーバを指定できます。ACS からプライマリ サーバに接続できない場合は、セカンダリ サーバが使用されます。

パスワード プロンプト

RADIUS ID ストアでは、パスワード プロンプトを設定できます。パスワード プロンプトは、ACS Web インターフェイスを介して設定できます。

ユーザ グループ マッピング

ACS 4.x で使用できるユーザ単位のグループ マッピング機能を提供するために、ACS 5.4 では、RADIUS ID ストアによって認証されるユーザの属性取得および認可メカニズムが使用されます。

このために、[009\001] cisco-av-pair 属性を含む認証応答を返すように RADIUS ID ストアを設定する必要があります。属性の値は次のとおりです。

ACS:CiscoSecure-Group-Id=*N*。ここで、*N* は、ACS によってユーザに割り当てられる 0 ～ 499 の任意の ACS グループ番号です。

この属性は、認可およびグループ マッピング規則の作成時に ACS Web インターフェイスのポリシー設定ページで使用できます。

グループおよび属性マッピング

RADIUS ID ストアに対する認証中に取得された RADIUS 属性を、認可およびグループ マッピングの ACS ポリシー条件で使用できます。RADIUS ID ストアを設定するときに、ポリシー条件で使用する属性を選択できます。これらの属性は、RADIUS ID ストア専用ディクショナリに保持され、ポリシー条件を定義するために使用できます。

（注） 要求された属性を RADIUS サーバに問い合わせることはできません。要求された属性を返すように RADIUS ID ストアを設定できるだけです。これらの属性は、Access-Accept 応答で属性リストの一部として使用できます。

ACS 5.4 の属性サブスクリプション機能を使用して、デバイスへの ACS 応答の RADIUS ID ストア属性を受信できます。次の RADIUS 属性が返されます。

- RADIUS RFS にリストされている属性
- ベンダー固有属性

次の属性タイプがサポートされています。

- String
- Unsigned Integer
- IP Address
- Enumeration

複数の値を持つ属性が返される場合、値は無視され、デフォルト値が設定されている場合はその値が返されます。ただし、この属性は問題がある属性としてカスタマー ログでレポートされます。

ID 順序での RADIUS ID ストア

ID 順序で認証順序用の RADIUS ID ストアを追加できます。ただし、属性取得順序用の RADIUS ID ストアを追加することはできません。これは、認証しないで RADIUS ID ストアを問い合わせることはできないためです。ACS では、RADIUS サーバによる認証中に、異なるエラー状況を区別できません。

すべてのエラー状況に対して RADIUS サーバから Access-Reject メッセージが返されます。たとえば、RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは User Unknown ステータスの代わりに Access-Reject メッセージが返されます。

ただし、ACS Web インターフェイスの RADIUS ID ストアのページで使用できる [Treat Rejects as Authentication Failure] または [Treat Rejects as User Not Found] オプションをイネーブルにすることができます。

認証失敗メッセージ

RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは Access-Reject メッセージが返されます。ACS には、ACS Web インターフェイスを使用して、このメッセージを Authentication Failed または Unknown User として設定するオプションがあります。

ただし、このオプションでは、ユーザが未知の状況だけでなく、すべての失敗状況に対して Unknown User メッセージが返されます。

表 8-18 に、RADIUS ID サーバで発生するさまざまな失敗状況を示します。

表 8-18　エラー処理

認証失敗の原因	失敗状況
Authentication Failed	• ユーザが未知である。 • ユーザが不正なパスコードでログインしようとしている。 • ユーザ ログイン時間が期限切れになった。
Process Failed	• RADIUS サーバが ACS で正しく設定されていない。 • RADIUS サーバが使用できない。 • RADIUS パケットが偽装として検出されている。 • RADIUS サーバとのパケットの送受信の問題。 • タイムアウト。
Unknown User	認証が失敗し、「Fail on Reject」オプションが false に設定されている。

Safeword サーバでのユーザ名の特殊フォーマット

Safeword トークン サーバでは、次のユーザ名フォーマットでの認証がサポートされています。

ユーザ名：Username, OTP

ACS により、ユーザ名が解析されて次のように変換されます。

ユーザ名：Username

Safeword トークン サーバでは、両方のフォーマットがサポートされています。ACS はさまざまなトークン サーバと連携します。Safeword サーバを設定する場合、ACS でユーザ名を解析して指定のフォーマットに変換するには、[Safeword Server] チェックボックスをオンにする必要があります。

この変換は、要求が RADIUS トークン サーバに送信される前に、RADIUS トークン サーバ ID ストアで実行されます。

ユーザ属性キャッシュ

RADIUS トークン サーバでは、デフォルトではユーザ ルックアップはサポートされていません。ただし、ユーザ ルックアップは次の ACS 機能に不可欠です。

- PEAP セッション再開：認証の成功後、EAP セッションの確立中に発生
- EAP/FAST 高速再接続：認証の成功後、EAP セッションの確立中に発生
- T+ 認可：T+ 認証の成功後に発生

ACS では、これらの機能のユーザ ルックアップ要求を処理するために、成功した認証の結果がキャッシュされます。成功した認証すべてについて、認証されたユーザの名前と取得された属性がキャッシュされます。失敗した認証はキャッシュに書き込まれません。

キャッシュは、実行時にメモリで使用可能であり、分散展開の ACS ノード間で複製されません。ACS Web インターフェイスを介してキャッシュの存続可能時間（TTL）制限を設定できます。ID キャッシング オプションをイネーブルにし、エージング タイムを分単位で設定する必要があります。指定した時間、キャッシュはメモリで使用可能です。

RADIUS ID サーバの作成、複製、および編集

ACS 5.4 では、ワンタイム パスワードによってセキュリティを向上させるために、外部 ID ストアとして RADIUS ID サーバがサポートされています。RADIUS ID サーバによって、ユーザの認証を確実にする 2 要素認証が提供されます。

RADIUS ID ストアに対してユーザを認証するには、最初に ACS で RADIUS ID サーバを作成し、RADIUS ID ストア設定を設定する必要があります。ACS 5.4 では、次の認証プロトコルがサポートされています。

- RADIUS PAP
- TACACS+ ASCII\PAP
- 内部 EAP-GTC を含む PEAP
- 内部 EAP-GTC を含む EAP-FAST

RADIUS ID サーバでの正常な認証には、次のことが必要です。

- RADIUS ID サーバと ACS との間のゲートウェイ デバイスで、UDP ポートを介した通信が許可されている。
- ACS Web インターフェイスで RADIUS ID サーバに対して設定する共有秘密情報が、RADIUS ID サーバ上で設定されている共有秘密情報と同一である。

RADIUS ID サーバを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [External Identity Stores] > [RADIUS Identity Servers] を選択します。

[RADIUS Identity Servers] ページが表示され、RADIUS 外部 ID サーバのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する ID ストアの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する ID ストア名をクリックします。または、名前の隣にあるボックスをオンにして [Edit] をクリックします。

ステップ 3　[General] タブのフィールドに入力します。[General] タブのフィールドについては、「一般設定」（P.8-65）を参照してください。

ステップ 4　次の作業を実行できます。

- [Submit] をクリックして RADIUS ID サーバを保存します。
- [Shell Prompts] タブをクリックします。[Shell Prompts] タブのフィールドについては、「シェル プロンプトの設定」（P.8-67）を参照してください。
- [Directory Attributes] タブをクリックします。[Directory Attributes] タブのフィールドについては、「ディレクトリ属性の設定」（P.8-67）を参照してください。
- [Advanced] タブをクリックします。[Advanced] タブのフィールドについては、「高度なオプションの設定」（P.8-68）を参照してください。

ステップ 5　[Submit] をクリックして変更を保存します。

関連トピック

- 「RADIUS ID ストア」（P.8-61）
- 「RADIUS ID サーバの作成、複製、および編集」（P.8-64）

一般設定

表 8-19 に、[RADIUS Identity Servers] ページの [General] タブのフィールドを示します。

表 8-19　[RADIUS Identity Server] - [General] タブ

オプション	説明
Name	外部 RADIUS ID サーバの名前。
Description	（任意）RADIUS ID サーバの簡単な説明。
SafeWord Server	SafeWord サーバを使用した 2 要素認証をイネーブルにする場合に、このチェックボックスをオンにします。
Server Connection	
Enable Secondary Server	セカンダリ RADIUS ID サーバを、プライマリ RADIUS ID サーバに障害が発生したときにバックアップ サーバとして使用する場合に、このチェックボックスをオンにします。 セカンダリ サーバをイネーブルにする場合、セカンダリ RADIUS ID サーバのパラメータを設定する必要があり、次のオプションのいずれかを選択する必要があります。 • Always Access Primary Server First：ACS がセカンダリ サーバにアクセスする前に常にプライマリ RADIUS ID サーバにアクセスするようにするには、このオプションを選択します。 • Failback To Primary Server After *n* Minutes：ACS が認証にセカンダリ サーバを使用できる時間（分単位）を設定するには、このオプションを選択します。 この時間を過ぎると、ACS はプライマリ サーバを使用して認証を再試行する必要があります。デフォルト値は 5 分です。
Primary Server	
Server IP Address	プライマリ RADIUS ID サーバの IP アドレス。

表 8-19　[RADIUS Identity Server] - [General] タブ （続き）

オプション	説明
Shared Secret	ACS とプライマリ RADIUS ID サーバ間の共有秘密情報。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Authentication Port	サーバが受信に使用するポート番号。有効なオプションは 1 ～ 65,535 です。デフォルト値は 1812 です。
Server Timeout *n* Seconds	プライマリ サーバへの接続に失敗したと判断する前に ACS がプライマリ RADIUS ID サーバからの応答を待つ秒数 *n*。有効なオプションは 1 ～ 300 です。デフォルト値は 5 です。
Connection Attempts	セカンダリ RADIUS ID サーバに接続するか、セカンダリ サーバが設定されていない場合は接続をドロップする前に、ACS が再接続を試行する回数を指定します。有効なオプションは 1 ～ 10 です。デフォルト値は 3 です。
Secondary Server	
Server IP Address	セカンダリ RADIUS ID サーバの IP アドレス。
Shared Secret	ACS とセカンダリ RADIUS ID サーバ間の共有秘密情報。共有秘密情報は、RADIUS ID サーバ上で設定されている共有秘密情報と同一である必要があります。 共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前に提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。
Authentication Port	RADIUS セカンダリ サーバが受信に使用するポート番号。有効なオプションは 1 ～ 65,535 です。デフォルト値は 1812 です。
Server Timeout *n* Seconds	セカンダリ サーバへの接続に失敗したと判断する前に ACS がセカンダリ RADIUS ID サーバからの応答を待つ秒数 *n*。 有効なオプションは 1 ～ 300 です。デフォルト値は 5 です。
Connection Attempts	要求をドロップする前に ACS が再接続を試行する回数を指定します。有効なオプションは 1 ～ 10 です。デフォルト値は 3 です。

関連トピック

- 「RADIUS ID ストア」（P.8-61）
- 「RADIUS ID サーバの作成、複製、および編集」（P.8-64）
- 「シェル プロンプトの設定」（P.8-67）
- 「ディレクトリ属性の設定」（P.8-67）
- 「高度なオプションの設定」（P.8-68）

シェル プロンプトの設定

TACACS+ ASCII 認証の場合、ACS はパスワード プロンプトをユーザに返す必要があります。RADIUS ID サーバでは、この機能はパスワード プロンプト オプションによってサポートされています。ACS では、ACS Web インターフェイスの [Shell Prompts] ページで設定するプロンプトを使用できます。このプロンプトが空の場合、TACACS+ グローバル設定で設定されているデフォルトのプロンプトがユーザに表示されます。

RADIUS ID サーバとの接続を確立するときに、最初の要求パケットにパスワードが含まれていない場合があります。パスワードを要求する必要があります。このページを使用して、パスワードの要求に使用されるプロンプトを定義できます。次の手順を実行します。

ステップ 1　プロンプトのテキストを [Prompt] フィールドに入力します。

ステップ 2　次のいずれかを実行します。

- パスワードを要求するプロンプトを設定するには、[Submit] をクリックします。
- ポリシー規則の条件で使用する属性のリストを定義するには、[Directory Attributes] タブをクリックします。詳細については、「ディレクトリ属性の設定」（P.8-67）を参照してください。

関連トピック

- 「RADIUS ID ストア」（P.8-61）
- 「RADIUS ID サーバの作成、複製、および編集」（P.8-64）
- 「一般設定」（P.8-65）
- 「ディレクトリ属性の設定」（P.8-67）
- 「高度なオプションの設定」（P.8-68）

ディレクトリ属性の設定

RADIUS ID サーバが要求に応答するときに、RADIUS 属性が応答とともに返されます。これらの RADIUS 属性をポリシー規則で使用できます。

[Directory Attributes] タブで、ポリシー規則の条件で使用する RADIUS 属性を指定できます。ACS では、これらの属性のリストが個別に保持されます。

ステップ 1　表 8-20 の説明に従って、[Directory Attributes] タブのフィールドを変更します。

表 8-20　[RADIUS Identity Servers] - [Directory Attributes] タブ

オプション	説明
Attribute List	このセクションを使用して、ポリシー条件に含める対象リストを作成します。各属性を含めると、その名前、タイプ、デフォルト値、およびポリシー条件名がテーブルに表示されます。変更後： • RADIUS 属性を追加するには、テーブルの下のフィールドに入力し、[Add] をクリックします。 • RADIUS 属性を編集するには、テーブルの該当する行を選択し、[Edit] をクリックします。テーブルの下のフィールドに RADIUS 属性のパラメータが表示されます。必要に応じて編集し、[Replace] をクリックします。

表 8-20　[RADIUS Identity Servers] - [Directory Attributes] タブ

オプション	説明
Dictionary Type	RADIUS ディクショナリ タイプ。ドロップダウン リスト ボックスをクリックして、RADIUS ディクショナリ タイプを選択します。
RADIUS Attribute	RADIUS 属性の名前。[Select] をクリックして、RADIUS 属性を選択します。この名前は、選択した属性が Cisco AV-Pair である場合、属性名と AV-pair をサポートする拡張子という 2 つの部分で構成されます。 たとえば、属性 **cisco-av-pair** と AV-pair 名 **some-avpair** の場合、ACS では **cisco-av-pair.some-avpair** と表示されます。 IETF およびベンダー VSA 属性名には、任意のサフィックス *-nnn* が含まれています。*nnn* は属性の ID です。
Type	RADIUS 属性タイプ。有効なオプションは次のとおりです。 • String • Unsigned Integer 32 • IPv4 address
Default	（任意）RADIUS ID サーバからの応答の属性を使用できない場合に使用できるデフォルト値。この値は、指定した RADIUS 属性タイプである必要があります。
Policy Condition Name	この属性を使用するカスタム ポリシー条件の名前を指定します。

ステップ 2　次のいずれかを実行します。

- 変更を保存して [RADIUS Identity Servers] ページに戻るには、[Submit] をクリックします。
- 失敗メッセージ処理を設定し、ID キャッシングをイネーブルにするには、[Advanced] タブをクリックします。詳細については、「高度なオプションの設定」（P.8-68）を参照してください。

関連トピック

- 「RADIUS ID ストア」（P.8-61）
- 「RADIUS ID サーバの作成、複製、および編集」（P.8-64）
- 「一般設定」（P.8-65）
- 「シェル プロンプトの設定」（P.8-67）
- 「高度なオプションの設定」（P.8-68）

高度なオプションの設定

[Advanced] タブでは、次のことを実行できます。

- RADIUS ID サーバからのアクセス拒否がどのような意味を持つかを定義します。
- ID キャッシングをイネーブルにします。

表 8-21 に、[RADIUS Identity Servers] ページの [Advanced] タブのフィールドを示します。

表 8-21　[RADIUS Identity Server] - [Advanced] タブ

オプション	説明
この ID ストアでは、認証試行が拒否された場合に「認証失敗」と「ユーザが見つからない」は区別されません。次のオプションから、ID ポリシーの処理とレポートのために、ID ストアからのそのような認証拒否を ACS でどのように解釈するかを選択します。	
Treat Rejects as 'authentication failed'	不明瞭なアクセス拒否試行をすべて認証失敗と見なす場合に、このオプションをクリックします。
Treat Rejects as 'user not found'	不明瞭なアクセス拒否試行をすべて未知ユーザと見なす場合に、このオプションをクリックします。
ID キャッシングは、サーバに対する認証を実行しない要求の処理を許可するために使用されます。キャッシュには、サブジェクトの最後に成功した認証から取得された結果および属性が保持されます。	
Enable identity caching	ID キャッシングをイネーブルにする場合に、このチェックボックスをオンにします。ID キャッシングをイネーブルにする場合、ACS で ID キャッシュを保持する時間を分単位で入力する必要があります。
Aging Time *n* Minutes	ACS で ID キャッシュを保持する時間を分単位で入力します。有効なオプションは 1 ～ 1440 です。

[Submit] をクリックして RADIUS ID サーバを保存します。

関連トピック

- 「RADIUS ID ストア」（P.8-61）
- 「RADIUS ID サーバの作成、複製、および編集」（P.8-64）

CA 証明書の設定

クライアントが EAP-TLS プロトコルを使用して ACS サーバに対して自身を認証する場合、自身を識別するクライアント証明書をサーバに送信します。クライアント証明書の ID および正確さを確認するために、サーバにはクライアント証明書をデジタル署名した Certificate Authority（CA; 認証局）からの証明書が事前にインストールされている必要があります。

ACS がクライアントの CA 証明書を信頼しない場合、ACS が信頼する上位レベル CA 証明書まで、連続して署名された CA 証明書のチェーン全体を ACS にインストールする必要があります。CA 証明書は、信頼証明書とも呼ばれます。

CA オプションを使用して、EAP-TLS 認証をサポートするデジタル証明書をインストールします。ACS は、X.509 v3 デジタル証明書標準を使用します。ACS は証明書の手動取得をサポートし、証明書信頼リスト（CTL）と Certificate Revocation List（CRL; 証明書失効リスト）を管理する手段も提供します。

デジタル証明書は、秘密情報も保存データベース クレデンシャルも共有する必要がありません。どちらも規模拡大が可能で、大きく展開しても信頼できます。正しく管理すれば、共有秘密システムより強力でセキュアな認証方式として動作させることができます。

相互信頼には、エンドユーザ クライアント側で確認できる証明書が ACS にインストールされている必要があります。このサーバ証明書は、CA から発行されたものを使用することもできますし、自己署名証明書を使用することもできます。詳細については、「ローカル サーバ証明書の設定」（P.18-14）を参照してください。

（注）　ACS では、追加した CA 証明書で証明書チェーンが作成され、TLS ネゴシエーション中にこのチェーンが使用されます。サーバ証明書に署名した証明書を CA に追加する必要があります。チェーンが正しく署名され、すべての証明書が有効であることを確認する必要があります。

サーバ証明書およびサーバ証明書に署名した CA が ACS にインストールされている場合、ACS は証明書チェーン全体をクライアントに送信します。

関連トピック

- 「認証局の追加」（P.8-70）
- 「認証局の編集および証明書失効リストの設定」（P.8-71）
- 「認証局の削除」（P.8-72）
- 「認証局のエクスポート」（P.8-73）

認証局の追加

サポートされている証明書形式は DER、PEM、CER です。

信頼できる認証局（CA）証明書を追加するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate] ページが表示されます。

ステップ 2　[Add] をクリックします。

ステップ 3　表 8-22 の説明に従って、[Certificate File to Import] ページのフィールドに入力します。

表 8-22　[Certificate Authority Properties] ページ

オプション	説明
Certificate File to Import	
Certificate File	証明書ファイルの名前を入力します。[Browse] をクリックして、信頼証明書があるクライアント マシン上の場所に移動します。
Trust for client with EAP-TLS	ACS が EAP プロトコルの証明書信頼リストを使用する場合に、このボックスをオンにします。
Allow Duplicate Certificates	同じ CN および SKI で、Valid From、Valid To、Serial numbers が異なる証明書の追加を許可します。
Description	CA 証明書の説明を入力します。

ステップ 4　[Submit] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Trust Certificate List] ページが表示されます。

関連トピック

- 「ユーザ証明書認証」（P.B-6）
- 「EAP-TLS の概要」（P.B-6）

認証局の編集および証明書失効リストの設定

このページは、信頼できる認証局（CA）証明書を編集する場合に使用します。

ステップ 1　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate] ページが表示され、設定されている証明書のリストが示されます。

ステップ 2　変更する名前をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

表 8-23 の説明に従って、[Edit Trust Certificate List Properties] ページのフィールドに入力します。

ACS が CA CRL を遅延すると、CA は、ローカル ファイル システムに保存されます。CA は再送信するまで更新されません。

デフォルトでは、CRL が失効した CA のすべてのユーザ証明書が ACS で失敗します。

- CA が再送信されると、次のエラーが表示されます。*12514 EAP-TLS failed SSL/TLS handshake* これは、不明な CA が原因です。
- CA が再送信されていない場合、次のエラーが表示されます。*12515 EAP-TLS failed SSL/TLS handshake*。これは、期限切れの CRL が原因です。

[Ignore CRL Expiration] を選択すると、失効した証明書に対する認証が失敗し、失効していない証明書で成功します。

表 8-23　[Edit Certificate Authority Properties] ページ

オプション	説明
Issuer	
Friendly Name	証明書に関連付けられている名前。
Description	（任意）CA 証明書の簡単な説明。
Issued To	*表示のみ*。証明書の発行先エンティティ。名前は、証明書のサブジェクトから表示されます。
Issued By	*表示のみ*。証明書を発行した認証局。
Valid from	*表示のみ*。証明書の有効開始日。X509 証明書は、開始日から終了日までの間（両方の日を含む）だけ有効です。
Valid To (Expiration)	*表示のみ*。証明書の有効最終日。
Serial Number	*表示のみ*。証明書のシリアル番号。
Description	証明書の説明。
Usage	
Trust for client with EAP-TLS	ACS が TLS 関連の EAP プロトコルの信頼リストを使用する場合に、このボックスをオンにします。
Certificate Status Validation	
OCSP Configuration	このセクションは、OCSP サービスを設定するために使用します。
Validate against OCSP service	このボックスをチェックし、ドロップダウン リストから OCSP サービスを選択して、選定した OCSP サービスに対して要求を確認します。
Reject the request if certificate status could not be determined by OCSP	証明書のステータスが OCSP サービスによって判断できない場合に要求を拒否するには、このボックスをチェックします。
Certificate Revocation List Configuration	このセクションは、CRL を設定するために使用します。

表 8-23　[Edit Certificate Authority Properties] ページ （続き）

オプション	説明
Download CRL	CRL をダウンロードする場合に、このボックスをオンにします。
CRL Distribution URL	CRL 配布 URL を入力します。HTTP を使用する URL を指定できます。
Retrieve CRL	ACS は最初に CA から CRL をダウンロードしようとします。ACS が CA から新しい CRL を取得する時間設定を切り替えます。 • Automatically：CRL ファイルから次の更新時間を取得します。取得に失敗した場合、ACS は最初の失敗から定期的に、成功するまで CRL の取得を試みます。 • Every：取得試行の頻度を指定します。時間間隔を入力します。
If Download Failed Wait	CRL の取得が失敗した場合に、次に取得を試行する時間を入力します。
Bypass CRL Verification if CRL is not Received	オフの場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、ACS によって CRL が受信されるまで拒否されます。オンの場合、クライアント要求は CRL が受信される前に受け入れられます。
Ignore CRL Expiration	期限切れの CRL に対して証明書をチェックする場合に、このボックスをオンにします。 • オンの場合、ACS は期限切れの CRL を使用し続け、CRL の内容に従って EAP-TLS 認証を許可または拒否します。 • オフの場合、ACS は、CRL ファイルの [Next Update] フィールドで CRL の有効期限を調べます。CRL が期限切れの場合、選択した CA によって署名された証明書を使用するすべての認証は拒否されます。

ステップ 3　[Submit] をクリックします。

編集した証明書が含まれた [Trust Certificate] ページが表示されます。

管理者には、CRL および OCSP 検証を設定する権限があります。CRL と OCSP の検証が同時に設定されている場合、ACS は、まず OCSP の検証を実行します。プライマリまたはセカンダリ サーバとの通信の問題が検出された場合、または指定された証明書のステータスが不明として検証から返された場合、ACS は CRL 検証の実行に進みます。

関連トピック

- 「ユーザ証明書認証」（P.B-6）
- 「EAP-TLS の概要」（P.B-6）

認証局の削除

このページは、信頼できる認証局（CA）証明書を削除する場合に使用します。

ステップ 1　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate List] ページが表示され、設定されている証明書のリストが示されます。

ステップ 2　削除する証明書の隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

ステップ 4　確認のために [Yes] をクリックします。

[Trust Certificate] ページが表示されます。このとき、削除した証明書は表示されません。

関連項目

- 「EAP-TLS の概要」（P.B-6）

認証局のエクスポート

信頼証明書をエクスポートするには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Certificate Authorities] を選択します。

[Trust Certificate List] ページが表示され、設定されている証明書のリストが示されます。

ステップ 2　エクスポートする証明書の隣にあるボックスをオンにします。

ステップ 3　[Export] をクリックします。

この操作によって、信頼できる証明書がクライアント マシンにエクスポートされます。

ステップ 4　確認のために [Yes] をクリックします。

エクスポートした証明書をクライアント マシンにインストールするように要求されます。

関連トピック

- 「ユーザ証明書認証」（P.B-6）
- 「EAP-TLS の概要」（P.B-6）

証明書認証プロファイルの設定

証明書認証プロファイルによって、証明書ベースのアクセス要求に使用される X509 証明書情報が定義されます。ユーザ名として使用される属性を証明書から選択できます。

証明書属性のサブセットを選択して、要求のコンテキストにユーザ名フィールドを読み込むことができます。このユーザ名は、要求の残りのユーザを識別する場合に使用されます。ログで使用される識別情報にも使用されます。

証明書認証プロファイルを使用して証明書データを取得し、LDAP または AD クライアントから提示される証明書をさらに確認できます。証明書認証プロファイルのユーザ名を使用して、LDAP または AD ID ストアの問い合わせが行われます。

ACS は、クライアント証明書を LDAP または AD ID ストアから取得されたすべての証明書と 1 つずつ比較し、いずれかが一致するかどうかを確認します。ACS は、要求を受け入れるか、または拒否します。

（注）　ACS が要求を受け入れるには、LDAP または AD ID ストアの証明書が 1 つだけ、クライアント証明書と一致する必要があります。

ACS が証明書ベースの認証要求を処理するときに、次の 2 つのうちのいずれかが行われます。証明書のユーザ名と、要求を処理している ACS のユーザ名とが比較されます。あるいは、選択した LDAP または AD ID ストアに定義されている情報を使用して、ACS によって証明書情報が確認されます。

証明書認証プロファイルを複製して、既存の証明書認証プロファイルと同じか、または類似した新しいプロファイルを作成できます。複製の完了後、各プロファイル（元のプロファイルおよび複製されたプロファイル）に個別にアクセスして、編集または削除します。

ACS 5.4 では、現在、証明書の名前制約拡張をサポートします。これにより、発行元に名前制約拡張が含まれるクライアント証明書を受け入れます。また、CA およびサブ CA 証明書についてクライアント認証を確認します。この拡張は、証明書パスの後続の証明書におけるすべてのサブジェクト名の名前空間を定義します。これは、サブジェクト識別名とサブジェクト代替名の両方に適用されます。これらの制約は、指定された名前形式がクライアント証明書に存在する場合にのみ適用されます。ACS 認証は、クライアント証明書が名前空間により除外されている、または許可されていない場合、失敗します。

サポートされる名前制約

- ディレクトリ名
- DNS
- 電子メール
- URL

サポートされない名前制約

- IP アドレス
- その他の名前

証明書認証プロファイルを作成、複製、または編集するには、次の手順を実行してください。

ステップ 1　[Users and Identity Stores] > [Certificate Authentication Profile] を選択します。

[Certificate Authentication Profile] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する証明書認証プロファイルの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する証明書認証プロファイルをクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Certificate Authentication Profile Properties] ページが表示されます。

ステップ 3　表 8-24 の説明に従って、[Certificate Authentication Profile Properties] ページのフィールドに入力します。

表 8-24　[Certificate Authentication Profile Properties] ページ

オプション	説明
General	
Name	証明書認証プロファイルの名前を入力します。
Description	証明書認証プロファイルの説明を入力します。
Certificate Definition	

表 8-24　[Certificate Authentication Profile Properties] ページ （続き）

オプション	説明
Principal Username X509 Attribute	x509 認証に使用できるプリンシパル ユーザ名属性のセット。選択肢は次のとおりです。 • Common Name • Subject Alternative Name • Subject Serial Number • Subject • Subject Alternative Name - Other Name • Subject Alternative Name - EMail • Subject Alternative Name - DNS
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory	選択した LDAP または AD ID ストアに対する認証のために証明書情報を確認する場合に、このチェックボックスをオンにします。 このオプションを選択する場合、LDAP または AD ID ストアの名前を入力するか、[Select] をクリックして使用可能なリストから LDAP または AD ID ストアを選択する必要があります。

ステップ 4　[Submit] をクリックします。

[Certificate Authentication Profile] ページが再表示されます。

関連トピック

- 「ID ポリシーの表示」（P.10-22）
- 「ID ストア順序の設定」（P.8-75）
- 「外部 LDAP ID ストアの作成」（P.8-23）

ID ストア順序の設定

アクセス サービス ID ポリシーによって、ACS が認証および属性取得のために使用する ID ソースが決まります。ID ソースは、1 つの ID ストアまたは複数の ID 方式で構成されます。複数の ID 方式を使用する場合、最初にそれらを ID ストア順序内に定義し、次に ID ストア順序を ID ポリシー内に指定する必要があります。

ID ストア順序によって、認証および属性取得のために使用される順序、および追加属性を取得するための任意の追加順序が定義されます。

認証順序

ID ストア順序には、証明書ベースの認証またはパスワードベースの認証あるいはその両方の定義を含めることができます。

- 証明書に基づく認証を実行することを選択した場合は、すでに ACS で定義されている 1 つの証明書認証プロファイルを指定します。
- パスワードに基づく認証を実行することを選択した場合は、アクセスされるデータベースのリストを順番に定義できます。

認証が成功すると、データベース内の定義済み属性が取得されます。ACS でデータベースを定義しておく必要があります。

属性取得順序

追加属性を取得するデータベースのリストを任意に定義できます。これらのデータベースには、パスワードベースの認証を使用するか、証明書ベースの認証を使用するかに関係なくアクセスできます。証明書ベースの認証を使用すると、ACS によって証明書属性からユーザ名フィールドに読み込まれ、ユーザ名を使用して属性が取得されます。

ACS では、次の場合でもユーザの属性を取得できます。

- ユーザのパスワードに変更必須のフラグが付けられている。
- ユーザのアカウントがディセーブルになっている。

パスワードベースの認証を使用する場合、認証リストと属性取得リストに同じ ID データベースを定義できます。ただし、データベースが認証に使用される場合、属性取得フローの一部として再度アクセスされることはありません。

ACS では、ID ストア内のユーザまたはホストは、そのユーザまたはホストで単一の一致が存在する場合にだけ認証されます。外部データベース内に同じユーザの複数のインスタンスがある場合、認証は失敗します。同様に、ACS では、ユーザまたはホストの単一の一致が存在する場合にだけ属性が取得されます。それ以外の場合、そのデータベースからの属性取得はスキップされます。

ここでは、次の内容について説明します。

- 「ID ストア順序の作成、複製、および編集」（P.8-76）
- 「ID ストア順序の削除」（P.8-78）

ID ストア順序の作成、複製、および編集

ID ストア順序を作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Identity Store Sequences] を選択します。

[Identity Store Sequences] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する順序の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する順序名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

表 8-25 に示すように、[Identity Store Sequence Properties] ページが表示されます。

表 8-25　[Identity Store Sequence Properties] ページ

オプション	説明
General	
Name	ID ストア順序の名前を入力します。
Description	ID ストア順序の説明を入力します。
Authentication Method List	
Certificate Based	証明書ベースの認証方式を使用する場合に、このチェックボックスをオンにします。このオプションを選択する場合、証明書認証プロファイルを入力する必要があります。[Select] をクリックして、使用可能なプロファイルのリストからプロファイルを選択します。

表 8-25　[Identity Store Sequence Properties] ページ （続き）

オプション	説明
Password Based	パスワードベースの認証方式を使用する場合に、このチェックボックスをオンにします。このオプションを選択する場合、一致が見つかるまで ACS が 1 つずつアクセスする ID ストアのセットを選択する必要があります。 このオプションを選択する場合、ACS が ID ストアに 1 つずつアクセスするために、[Authentication and Attribute Retrieval Search List] 領域で ID ストアのリストを選択する必要があります。
Authentication and Attribute Retrieval Search List	
（注）　このセクションは、[Password Based] オプションをオンにした場合にだけ表示されます。	
Available	アクセス対象として使用可能な ID ストアのセット。
Selected	認証が成功するまで順番にアクセスされる選択済み ID ストアのセット。リストの右にある上向きおよび下向き矢印を使用して、アクセスの順序を定義します。 ACS により、認証用に選択した ID ストアから属性が自動的に取得されます。属性を取得するために同じ ID ストアを選択する必要はありません。
Additional Attribute Retrieval Search List	
Available	属性取得用に使用可能なその他の ID ストアのセット。
Selected	（任意）属性取得用に選択されたその他の ID ストアのセット。リストの右にある上向きおよび下向き矢印を使用して、アクセスの順序を定義します。 ACS により、認証用に選択した ID ストアから属性が自動的に取得されます。属性を取得するために同じ ID ストアを選択する必要はありません。
Internal User/Host	
If internal user/host is not found or disabled then exit the sequence and treat as User Not Found	このオプションは、内部 ID ストアが属性取得のリストに含まれている場合に、属性フェーズで適用されます。 このオプションが選択され、ユーザが見つからないか、またはディセーブルにされているとき、ACS はシーケンスを終了し、「ユーザが見つかりません」として扱います。
Advanced Options	
Break sequence	このオプションが選択され、現在の ID ストアに対する認証の試行がプロセス エラーになった場合、フローは ID ストア シーケンスを終了します。次に、ID ポリシーで設定された [Fail-Open] オプションに進みます。 同じことが属性取得にも適用されます。
Continue to next identity store in the sequence	これがオンで、現在の ID ストアに対する認証がプロセス エラーになった場合、フローは認証リストの次の ID ストアで認証を試行します。 同じことが属性取得のフェーズにも適用されます。

ステップ 3　[Submit] をクリックします。

[Identity Store Sequences] ページが再表示されます。

関連トピック

- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）
- 「ID ポリシーの表示」（P.10-22）
- 「内部 ID ストアの管理」（P.8-4）

- 「外部 ID ストアの管理」（P.8-19）
- 「証明書認証プロファイルの設定」（P.8-73）
- 「ID ストア順序の削除」（P.8-78）

ID ストア順序の削除

ID ストア順序を削除するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Identity Store Sequences] を選択します。

[Identity Store Sequences] ページが表示され、設定されている ID ストア順序のリストが示されます。

ステップ 2　削除する ID ストア順序の隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のエラー メッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[Identity Store Sequences] ページが表示されます。このとき、削除した ID ストア順序はリストに含まれません。

関連トピック

- 「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）
- 「ID ポリシーの表示」（P.10-22）
- 「内部 ID ストアの管理」（P.8-4）
- 「外部 ID ストアの管理」（P.8-19）
- 「証明書認証プロファイルの設定」（P.8-73）
- 「ID ストア順序の作成、複製、および編集」（P.8-76）

CHAPTER 9

ポリシー要素の管理

ACS ネットワークにアクセスを試みるクライアントを認証および認可する処理は、ポリシーによって定義されます。ユーザ、ネットワーク デバイス、またはネットワーク デバイスに関連付けられているユーザがクライアントとなります。

ポリシーは、規則のセットです。規則にはポリシー要素が含まれています。ポリシー要素は、規則テーブルに編成された条件と結果のセットです。ポリシーの設計および ACS でのポリシーの実装方法の詳細については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

ポリシー規則を設定する前に、ポリシー要素を作成する必要があります。ポリシー要素は、ポリシーで使用される条件および結果です。作成したポリシー要素は、ポリシー規則で使用できます。サービス、ポリシー、およびポリシー規則の管理の詳細については、第 10 章「アクセス ポリシーの管理」を参照してください。

この章は、次の内容で構成されています。

- 「ポリシー条件の管理」（P.9-1）
- 「認可および権限の管理」（P.9-19）
- 「ダウンロード可能 ACL の作成、複製、および編集」（P.9-33）

（注） Cisco Security Group Access ライセンスがインストールされている場合は、後で Security Group Access の認可ポリシーで使用できる、セキュリティ グループ アクセス コントロール リスト（SGACL）およびセキュリティ グループを設定することもできます。Security Group Access のセキュリティ グループの設定については、「セキュリティ グループの作成」（P.4-25）を参照してください。

ポリシー条件の管理

規則テーブルには、次の項目を条件として設定できます。

- 要求/プロトコル属性：これらの属性は、ACS によって、ユーザが発行した認証要求から取得されます。
- ID 属性：これらの属性は、要求を実行するユーザの ID と関連しています。これらの属性は、内部 ID ストア内のユーザ定義、または外部 ID ストア（LDAP や AD など）に保存されているユーザ定義から取得できます。
- ID グループ：ACS では、すべてのタイプのユーザおよびホストに使用される単一の ID グループ階層が保持されます。内部ユーザまたはホストの各定義に、この階層内の単一の ID グループとの関連付けを含めることができます。

グループ マッピング ポリシーを使用して、ユーザおよびホストを ID グループにマッピングできます。グループ内のすべてのユーザに対する共通のポリシー条件を設定するために、ID グループを条件に含めることができます。ID グループの作成の詳細については、「ID 属性の管理」（P.8-7）を参照してください。

- ネットワーク デバイス グループ（NDG）：要求を発行するデバイスが、1 つ以上、最大 12 のデバイス階層に含まれています。ポリシー条件には階層の要素を含めることができます。NDG の作成の詳細については、「ネットワーク デバイス グループ」（P.7-2）を参照してください。
- 日付と時刻の条件：複数の特定の曜日について特定の時間間隔を定義する、名前付き条件を作成できます。また、日付と時刻の条件に有効期限を関連付けることもできます。

  日付と時刻の条件に現在の日付および時刻を指定すると、実質的に、条件が満たされているかどうかを示す true または false が返されます。日付と時刻の条件には、次の 2 つのコンポーネントがあります。

  - 期間のイネーブル化：このオプションは、開始時刻、終了時刻、または両方を任意で指定して、条件をイネーブルにする期間を制限する場合に使用します。このコンポーネントを使用すると、期間が限定され、実質的に失効する規則を作成できます。

    この条件がイネーブルでない場合は、日付と時刻の条件のこのコンポーネントによって false が返されます。
  - 時間間隔：ACS Web インターフェイスには、曜日および各日の時間を示す、時間のグリッドが表示されます。グリッド内の各セルは、1 時間を表します。これらのセルを設定またはクリアできます。

    要求が処理される日付および時刻が、対応する時間間隔が設定された時間内に収まる場合は、日付と時刻の条件のこのコンポーネントによって true が返されます。

  要求が処理されるとき、日付と時刻の条件の両方のコンポーネントが考慮されます。日付と時刻の条件は、両方のコンポーネントによって true 値が返された場合にだけ評価されます。
- ネットワークの条件：ネットワークへのアクセスを制限するために、次のタイプのフィルタを作成できます。

  - 端末フィルタ：接続を開始および終了する端末を対象とします。端末は、要求から取得される IP アドレス、MAC アドレス、発信番号識別（CLI）、または Dialed Number Identification Service（DNIS; 着信番号識別サービス）の各フィールドによって識別されます。
  - ネットワーク デバイス フィルタ：要求を処理する AAA クライアントを対象とします。ネットワーク デバイスは、その IP アドレス、ネットワーク デバイス リポジトリで定義されているデバイス名、または NDG によって識別されます。
  - デバイス ポート フィルタ：ネットワーク デバイス定義は、端末が関連付けられているデバイス ポートによって補完される場合があります。

  各ネットワーク デバイス条件には、オブジェクトのリストを定義します。このリストは、あとでポリシー条件に含めることができ、これにより、要求で示される定義と照合される定義セットになります。

  条件で使用する演算子は、*match*（示されている値がネットワーク条件の少なくとも 1 つのエントリと一致する必要がある場合）、または *no matches*（フィルタに存在するオブジェクト セット内のいずれのエントリにも一致しない必要がある場合）のいずれかになります。

プロトコル属性および ID 属性をカスタム条件または複合条件で定義して、これらの属性を条件に含めることができます。

複合条件は、ポリシー規則プロパティ ページで定義し、個別の名前付き条件としては定義しません。「複合条件の設定」（P.10-41）を参照してください。

カスタム条件および日付と時刻の条件は、セッション条件と呼ばれます。

ここでは、次の内容について説明します。

- 「日付と時刻の条件の作成、複製、および編集」（P.9-3）
- 「カスタム セッション条件の作成、複製、および編集」（P.9-5）
- 「セッション条件の削除」（P.9-6）
- 「ネットワーク条件の管理」（P.9-7）

ポリシー規則で使用できる（ただし設定はできない）その他の条件については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

日付と時刻の条件の作成、複製、および編集

日付と時刻の条件を作成して、時間間隔および期間を指定します。たとえば、特定の休日期間におけるシフトを定義できます。ACS で日付と時刻の条件を含む規則が処理されるとき、日付と時刻の条件は、要求を処理している ACS インスタンスの日付と時刻の情報と比較されます。この条件に関連付けられているクライアントは、セッションの継続中はこの条件の対象となります。

ポリシー決定を行うとき、ACS サーバでの時刻が使用されます。したがって、ACS サーバが属しているタイムゾーンに対応して、日付と時刻の条件を設定したことを確認してください。ユーザが使用しているタイムゾーンが ACS サーバのタイムゾーンとは異なる場合があります。

セッション条件を複製して、既存のセッション条件と同じか、または類似する新しいセッション条件を作成できます。複製の完了後、（元のまたは複製された）各セッション条件に個別にアクセスして、編集または削除します。

日付と時刻の条件を作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Date and Time] を選択します。

[Date and Time Conditions] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する条件の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する条件の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Date and Time Properties] ページが表示されます。

ステップ 3　表 9-1 の説明に従って、必須フィールドに有効な設定データを入力します。

表 9-1　[Date and Time Properties] ページ

オプション	説明
General	
Name	時刻と日付の条件の名前を入力します。
Description	時刻と日付の条件の具体的な日付や時刻などの説明を入力します。

表 9-1　[Date and Time Properties] ページ （続き）

オプション	説明
Duration	
Start	次のオプションのいずれかをクリックします。 • Start Immediately：この条件に関連付けられている規則が有効であり、それらの規則が現在の日付から開始されることを指定します。 • Start On：関連するフィールドの隣にあるカレンダー アイコンをクリックして開始日を指定することで、条件がアクティブになる特定の開始日を選択します（開始日の始まりは 24 時間クロックでの時刻 00:00:00 として示されます）。 時刻は *hh*:*mm* 形式で指定できます。
End	次のオプションのいずれかをクリックします。 • No End Date：日付と時刻の条件に関連付けられている規則が、指定された開始日のあとは常にアクティブとなることを指定します。 • End By：関連するフィールドの隣にあるカレンダー アイコンをクリックして終了日を指定することで、日付と時刻の条件が非アクティブになる特定の終了日を選択します（終了日の終わりは 24 時間クロックでの時刻 23:59:59 として示されます）。 時刻は *hh*:*mm* 形式で指定できます。
Days and Time	
Days and Time section grid	日付と時刻グリッドのそれぞれの四角は、1 時間に相当します。四角いグリッドを選択して、対応する時間をアクティブにします。日付と時刻の条件に関連付けられている規則がその時間中は有効になります。 緑の（または色の濃い）四角いグリッドは、アクティブな時間を示します。 ACS サーバが属しているタイムゾーンに対応する日付と時刻の条件を設定していることを確認してください。ユーザが使用しているタイムゾーンが ACS サーバのタイムゾーンとは異なる場合があります。 たとえば、現在の時刻よりも 1 時間先であるものの、ACS サーバのタイムゾーンではすでに過去の時間となっている日付と時刻の条件を設定すると、エラー メッセージが表示される場合があります。
Select All	グリッド内のすべての四角をアクティブ状態に設定する場合にクリックします。日付と時刻の条件に関連付けられている規則が、常に有効になります。
Clear All	グリッド内のすべての四角を非アクティブ状態に設定する場合にクリックします。日付と時刻の条件に関連付けられている規則が、常に無効になります。
Undo All	日付と時刻のグループに対して選択した日付と時刻のアクティブ化および非アクティブ化に関する最新の変更内容を削除する場合にクリックします。

日付と時刻の条件をポリシーに追加するには、最初に規則テーブルをカスタマイズする必要があります。「ポリシーのカスタマイズ」（P.10-4）を参照してください。

ステップ 4　[Submit] をクリックします。

日付と時刻の条件が保存されます。[Date and Time Conditions] ページが表示され、作成または複製した新しい日付と時刻の条件が示されます。

（注）　ACS には時間的制約があるリソースとサービスがあります。したがって、クロック、タイムゾーン、NTP の変更などの操作の実行後、すべてのサービスを再起動することをお勧めします。これらの操作の後に再起動しない場合、AD、データベース接続および暗号情報などの機能が中断する可能性があります。

関連トピック

- 「カスタム セッション条件の作成、複製、および編集」（P.9-5）
- 「セッション条件の削除」（P.9-6）
- 「アクセス サービス ポリシーの設定」（P.10-22）

カスタム セッション条件の作成、複製、および編集

プロトコルおよび ID ディクショナリには、多数の属性が含まれています。これらの属性のいずれかをポリシー規則の条件として使用するには、その属性のカスタム条件を最初に作成する必要があります。カスタム条件により、ポリシー条件で使用する小さな属性サブセットを定義し、規則テーブル用の条件タイプの選択時に使用する焦点を絞った小さなリストを指定します。

複合条件にプロトコル属性および ID 属性を含めることもできます。複合条件の詳細については、「複合条件の設定」（P.10-41）を参照してください。

カスタム条件を作成するには、いずれかのディクショナリから特定のプロトコル（RADIUS や TACACS+）または ID 属性を選択し、カスタム条件に名前を付ける必要があります。プロトコルおよび ID ディクショナリの詳細については、「グローバル システム オプションの設定」（P.18-1）を参照してください。

ID 属性または RADIUS 属性を含むカスタム条件を作成する場合は、これらの属性の定義を含めることもできます。これにより、特定の属性に関連付けられている既存のカスタム条件を簡単に表示できます。

カスタム セッション条件を作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Custom] を選択します。

[Custom Conditions] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する条件の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する条件の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Custom Condition Properties] ページが表示されます。

ステップ 3　表 9-2 に従い、必須フィールドに有効な設定データを入力します。

表 9-2　[Policy Custom Condition Properties] ページ

オプション	説明
General	
Name	カスタム条件の名前。
Description	カスタム条件の説明。

表 9-2　[Policy Custom Condition Properties] ページ （続き）

オプション	説明
Condition	
Dictionary	ドロップダウン リスト ボックスから、特定のプロトコルまたは ID ディクショナリを選択します。
Attribute	[Dictionary] フィールドでの選択に基づいて外部 ID ストア ディクショナリのリストを表示するには、[Select] をクリックします。カスタム条件に関連付ける属性を選択し、[OK] をクリックします。ポリシーで使用されているカスタム条件を編集している場合は、そのカスタム条件によって参照される属性は編集できません。

カスタム条件をポリシーに追加するには、最初に規則テーブルをカスタマイズする必要があります。「ポリシーのカスタマイズ」（P.10-4）を参照してください。

ステップ 4　[Submit] をクリックします。

新しいカスタム セッション条件が保存されます。[Custom Condition] ページが表示され、新しいカスタム セッション条件が示されます。この条件に関連付けられているクライアントは、セッションの継続中はこの条件の対象となります。

関連トピック

- 「日付と時刻の条件の作成、複製、および編集」（P.9-3）
- 「セッション条件の削除」（P.9-6）
- 「アクセス サービス ポリシーの設定」（P.10-22）

セッション条件の削除

セッション条件を削除するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > *session condition* を選択します。ここで、*session condition* は、[Date and Time] または [Custom] です。

[Session Condition] ページが表示されます。

ステップ 2　削除するセッション条件の隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

[Session Condition] ページが表示されます。このとき、削除したカスタム セッション条件は表示されません。

関連トピック

- 「日付と時刻の条件の作成、複製、および編集」（P.9-3）
- 「カスタム セッション条件の作成、複製、および編集」（P.9-5）

ネットワーク条件の管理

フィルタは、端末、ネットワーク デバイス、およびネットワーク デバイス ポート用に作成した再利用可能なネットワーク条件です。フィルタを使用すると、ACS 5.4 では次のことを実行できます。

- ユーザおよびデイバスにネットワーク アクセスを許可するか許可しないかを決定する。
- ポリシーで使用する ID ストア、サービスなどに関する決定を行う。

名前の付いたフィルタを作成すると、その名前を参照して、さまざまな規則およびポリシーでそのフィルタを何度でも再利用できます。

（注） ACS 5.4 でのフィルタは、ACS 4.x での NAR に似ています。ACS 4.x では、NAR はユーザまたはユーザ グループに基づいていました。5.4 でのフィルタは、さまざまな規則およびポリシーで再利用できる独立した条件です。

ACS では、次の 3 つのタイプのフィルタが用意されています。

- 端末フィルタ：端末（端末の IP アドレス、MAC アドレス、CLID 番号、または DNIS 番号に基づいて接続を開始するラップトップやプリンタなど）をフィルタリングします。

  端末の ID は、端末を一意に識別する IP アドレス、MAC アドレス、またはその他の任意の文字列になります。これは、プロトコル認識属性タイプの文字列であり、端末 ID のコピーが含まれています。

  - RADIUS 要求では、この ID は属性 31（Calling-Station-Id）で使用できます。
  - TACACS 要求では、ACS によって、（すべてのフェーズの）開始要求のリモート アドレス フィールドからこの ID が取得されます。ACS では、スラッシュ（/）区切り文字が存在する場合は、その前のリモート アドレス値が取得され、それ以外の場合はリモート アドレス値全体が取得されます。

  端末の IP アドレスは、端末 ID の IPv4 または IPv6 です。端末 MAC は、端末 ID の標準化された MAC アドレスです。

- デバイス フィルタ：端末の Policy Enforcement Point（PEP）として機能するネットワーク デバイス（AAA クライアント）を、ネットワーク デバイスの IP アドレスや名前、またはそれが属しているネットワーク デバイス グループに基づいてフィルタリングします。

  デバイス ID は、デバイスの IP アドレスや名前である場合、またはデバイスが属するネットワーク デバイス グループに基づく場合があります。

  この IP アドレスは、IPv4 または IPv6 タイプのプロトコル非認識属性であり、要求から取得したデバイス IP アドレスのコピーが含まれています。

  - RADIUS 要求では、属性 4（NAS-IP-Address）が存在すると、ACS によって属性 4 から IP アドレスが取得されます。それ以外の場合は、属性 32（NAS-Identifier）が存在すると、ACS によって属性 32 から IP アドレスが取得されるか、または受信したパケットから IP アドレスが取得されます。
  - TACACS 要求では、IP アドレスは ACS が受信したパケットから取得されます。

  デバイス名は、ACS リポジトリから取得されるデバイス名のコピーを含む文字列タイプの属性です。

  デバイス ディクショナリ（NDG ディクショナリ）には、Location、Device Type、NDG を表すその他の動的に作成された属性などのネットワーク デバイス グループ属性が含まれています。これらの属性には、現在のデバイスが関連付けられているグループが含まれています。

- デバイス ポート フィルタ：端末が接続しているデバイスの物理ポートをフィルタリングします。フィルタリングはデバイスの IP アドレス、名前、デバイスが属している NDG、およびポートに基づいて行われます。

  デバイス ポート ID は、次のような文字列タイプの属性です。

  - RADIUS 要求では、属性 5（NAS-Port）が要求に含まれていると、ACS によって属性 5 から値が取得され、属性 87（NAS-Port-Id）が要求に含まれていると、ACS によって属性 87 から要求が取得されます。
  - TACACS 要求では、ACS によって、（すべてのフェーズの）開始要求のポート フィールドからこの ID が取得されます。

  デバイス名は、ACS リポジトリから取得されるデバイス名のコピーを含む文字列タイプの属性です。

  デバイス ディクショナリ（NDG ディクショナリ）には、Location、Device Type、NDG を表すその他の動的に作成された属性などのネットワーク デバイス グループ属性が含まれています。これらの属性には、現在のデバイスが関連付けられているグループが含まれています。

これらのフィルタを作成、複製、および編集できます。フィルタの内容を .csv ファイルから一括インポートしたり、ACS のフィルタを .csv ファイルにエクスポートしたりできます。ネットワーク条件の一括インポート方法の詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ここでは、次の内容について説明します。

- 「ネットワーク条件のインポート」（P.9-8）
- 「ネットワーク条件のエクスポート」（P.9-9）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-16）

ネットワーク条件のインポート

一括インポート機能を使用して、次のネットワーク条件の内容をインポートできます。

- 端末フィルタ
- デバイス フィルタ
- デバイス ポート フィルタ

一括インポートの場合は、ACS から .csv ファイル テンプレートをダウンロードし、.csv ファイルにインポートするレコードを追加し、そのファイルをハード ドライブに保存する必要があります。Download Template 機能を使用して、.csv ファイルが要件に準拠するようにします。

端末フィルタ、デバイス フィルタ、およびデバイス ポート フィルタの .csv テンプレートは、それぞれのタイプに固有のテンプレートです。たとえば、[End Station Filters] ページからアクセスしてダウンロードしたテンプレートは、デバイス フィルタまたはデバイス ポート フィルタのインポートには使用できません。.csv ファイルは次の要件に準拠している必要があります。

- 最初のレコード（.csv ファイルの最初の行）の内容は変更しないでください。
- 各レコードに対して使用するのは 1 行だけです。
- フィールドに改行文字を埋め込まないでください。
- 英語以外の言語では、.csv ファイルを utf-8 符号化で符号化するか、Unicode をサポートするフォントを使用して保存します。

インポート プロセスでは、ACS の既存のフィルタ リストにフィルタが追加されるのではなく、既存のリストが置き換えられます。.csv ファイルからレコードをインポートすると、ACS の既存のフィルタ設定が、.csv ファイルのフィルタ設定に置き換えられます。

ステップ 1　Web インターフェイスの [End Station Filter]、[Device Filter]、または [Device Port Filter] ページ上の [Replace from File] ボタンをクリックします。

[Replace from File] ダイアログボックスが表示されます。

ステップ 2　.csv ファイル テンプレートがない場合は、[Download Template] をクリックして、.csv ファイル テンプレートをダウンロードします。

ステップ 3　[Browse] をクリックして、.csv ファイルに移動します。

ステップ 4　[Start Replace] をクリックして、一括インポート プロセスを開始します。

インポートの進行状況が同じページに表示されます。一括インポートの進行状況を監視できます。.csv ファイルのレコードのデータ転送失敗が表示されます。

ステップ 5　[Import Progress] ウィンドウを閉じるには、[Close] をクリックします。

システムに一度に送信できる .csv ファイルは 1 つだけです。インポートが進行中である場合、追加のインポートは、最初のインポートが完了するまで成功しません。

ワンポイントアドバイス　テンプレートをダウンロードしてインポート ファイルを作成する代わりに、特定のフィルタのエクスポート ファイルを使用して、そのファイル内の情報を更新し、保存し、それをインポート ファイルとして再利用できます。

ネットワーク条件のエクスポート

ACS 5.4 では、フィルタ設定データを .csv ファイル形式でエクスポートするための一括エクスポート機能を提供しています。次のフィルタ設定をエクスポートできます。

- 端末フィルタ
- デバイス フィルタ
- デバイス ポート フィルタ

これらいずれかのフィルタの作成、編集、または複製のページで、[Export to File] をクリックして、フィルタ設定を .csv ファイルとしてローカル ハード ドライブに保存します。

端末フィルタの作成、複製、および編集

[End Station Filters] ページを使用して、端末フィルタを作成、複製、および編集します。次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Network Conditions] > [End Station Filters] を選択します。

[End Station Filters] ページが表示され、設定した端末フィルタのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

- [Export] をクリックして、端末フィルタのリストを .csv ファイルに保存します。詳細については、「ネットワーク条件のエクスポート」（P.9-9）を参照してください。
- [Replace from File] をクリックして、.csv インポート ファイルから端末フィルタの一括インポートを実行します。詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ステップ 3　次のフィールドに値を入力します。

- [Name]：端末フィルタの名前。
- [Description]：端末フィルタの説明。

ステップ 4　次の 1 つ以上のタブのフィールドを編集します。

- [IP Address]：このタブのフィールドについては、「IP アドレスベースの端末フィルタの定義」（P.9-10）を参照してください。
- [MAC Address]：このタブのフィールドについては、「MAC アドレスベースの端末フィルタの定義」（P.9-11）を参照してください。
- [CLI/DNIS]：このタブのフィールドについては、「CLI または DNIS ベースの端末フィルタの定義」（P.9-12）を参照してください。

（注）　フィルタを設定するには、最低限、3 つのタブの少なくとも 1 つにフィルタ基準を入力する必要があります。

ステップ 5　[Submit] をクリックして変更を保存します。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「ネットワーク条件のインポート」（P.9-8）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-16）

IP アドレスベースの端末フィルタの定義

端末へのアクセスを許可または拒否する場合、その端末の IP アドレスを作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[IP Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する IP ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する IP ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　次のいずれかを選択します。

- [Single IP Address]：このオプションを選択した場合、次のように有効なアドレスを入力する必要があります。
  - *x.x.x.x* という形式の IPv4 アドレス。*x* には 0 ～ 255 の任意の値を指定できます。

  - *x*:*x*:*x*:*x*:*x*:*x*:*x*:*x* という形式の IPv6 アドレス。*x* はアドレスの 8 つの 16 ビット部分の 1 ～ 4 桁の 16 進数を表します。これには、0 ～ 9 の数字または A ～ F の文字を指定できます。
- [IP Range(s)]：このオプションを選択した場合、有効な IPv4 アドレスおよびサブネット マスクを入力して、IP アドレスの範囲をフィルタリングする必要があります。デフォルトでは、IPv4 のサブネット マスクの値は 32、IPv6 の値は 128 です。

（注）　IPv6 範囲は ACS 5.4 ではサポートされません。

（注）　IPv6 アドレスは、TACACS+ プロトコルだけでサポートされています。

ステップ 3　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「MAC アドレスベースの端末フィルタの定義」（P.9-11）
- 「CLI または DNIS ベースの端末フィルタの定義」（P.9-12）

MAC アドレスベースの端末フィルタの定義

端末または宛先へのアクセスを許可または拒否する場合、その端末または宛先の MAC アドレスを作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[MAC Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する MAC アドレスベースの端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する MAC アドレスベースの端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　[End Station MAC] チェックボックスをオンにして、端末の MAC アドレスを入力します。

任意で、このフィールドを ANY に設定して任意の MAC アドレスを参照できます。

ステップ 3　[Destination MAC] チェックボックスをオンにして、宛先マシンの MAC アドレスを入力します。

任意で、このフィールドを ANY に設定して任意の MAC アドレスを参照できます。

（注）　MAC アドレスを *xxxxxxxxxxxx*、*xx-xx-xx-xx-xx-xx*、*xx*:*xx*:*xx*:*xx*:*xx*:*xx*、または *xxxx.xxxx.xxxx* のいずれかの形式で入力する必要があります。x は、0 ～ 9 または A ～ F の任意の数字です。MAC アドレスにワイルドカード文字は使用できません。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「IP アドレスベースの端末フィルタの定義」（P.9-10）
- 「CLI または DNIS ベースの端末フィルタの定義」（P.9-12）

CLI または DNIS ベースの端末フィルタの定義

端末や宛先へのアクセスを許可または拒否する場合、その端末や宛先の CLI および DNIS 番号を作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[CLI/DNIS] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する CLI または DNIS ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する CLI または DNIS ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　[CLI] チェックボックスをオンにして、端末の CLI 番号を入力します。

任意で、このフィールドを ANY に設定して任意の CLI アドレスを参照できます。

ステップ 3　[DNIS] チェックボックスをオンにして、宛先マシンの DNIS 番号を入力します。

任意で、このフィールドを ANY に設定して任意の DNIS 番号を参照できます。

（注）　? 文字 およびワイルドカード文字（*）を使用して、任意の単一文字または 1 つ以上の連続する文字をそれぞれ参照できます。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「IP アドレスベースの端末フィルタの定義」（P.9-10）
- 「MAC アドレスベースの端末フィルタの定義」（P.9-11）

デバイス フィルタの作成、複製、および編集

[Device Filters] ページを使用して、デバイス フィルタを作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Network Conditions] > [Device Filters] を選択します。

[Device Filters] ページが表示され、設定したデバイス フィルタのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製するデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集するデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- [Export] をクリックして、デバイス フィルタのリストを .csv ファイルに保存します。詳細については、「ネットワーク条件のエクスポート」（P.9-9）を参照してください。
- [Replace from File] をクリックして、.csv インポート ファイルからデバイス フィルタの一括インポートを実行します。詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ステップ 3　次のフィールドに値を入力します。

- [Name]：デバイス フィルタの名前。
- [Description]：デバイス フィルタの説明。

ステップ 4　次のいずれかのタブまたはすべてのタブのフィールドを編集します。

- [IP Address]：このタブのフィールドについては、「IP アドレスベースのデバイス フィルタの定義」（P.9-13）を参照してください。
- [Device Name]：このタブのフィールドについては、「名前ベースのデバイス フィルタの定義」（P.9-14）を参照してください。
- [Network Device Group]：このタブのフィールドについては、「NDG ベースのデバイス フィルタの定義」（P.9-15）を参照してください。

（注）　フィルタを設定するには、最低限、3 つのタブの少なくとも 1 つにフィルタ基準を入力する必要があります。

ステップ 5　[Submit] をクリックして変更を保存します。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「ネットワーク条件のインポート」（P.9-8）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-16）

IP アドレスベースのデバイス フィルタの定義

ネットワーク デバイスへのアクセスを許可または拒否する場合、そのネットワーク デバイスの IP アドレスを作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[IP Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する IP ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する IP ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　次のいずれかを選択します。

- [Single IP Address]：このオプションを選択した場合、次のように有効なアドレスを入力する必要があります。
  - *x.x.x.x* という形式の IPv4 アドレス。*x* には 0 ～ 255 の任意の値を指定できます。
  - *x:x:x:x:x:x:x:x* という形式の IPv6 アドレス。*x* はアドレスの 8 つの 16 ビット部分の 1 ～ 4 桁の 16 進数を表します。これには、0 ～ 9 の数字または A ～ F の文字を指定できます。
- [IP Range(s)]：このオプションを選択した場合、有効な IPv4 または IPv6 アドレスおよびサブネット マスクを入力して、IP アドレスの範囲をフィルタリングする必要があります。デフォルトでは、IPv4 のサブネット マスクの値は 32、IPv6 の値は 128 です。

（注）　IPv6 範囲は ACS 5.4 ではサポートされません。

ステップ 3　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「名前ベースのデバイス フィルタの定義」（P.9-14）
- 「NDG ベースのデバイス フィルタの定義」（P.9-15）

名前ベースのデバイス フィルタの定義

ネットワーク デバイスへのアクセスを許可または拒否する場合、そのネットワーク デバイスの名前を作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[Device Name] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する名前ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する名前ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイスを選択します。

ステップ 3　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「IP アドレスベースのデバイス フィルタの定義」（P.9-13）
- 「NDG ベースのデバイス フィルタの定義」（P.9-15）

NDG ベースのデバイス フィルタの定義

ネットワーク デバイス グループ タイプへのアクセスを許可または拒否する場合、そのネットワーク デバイス グループ タイプを作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[Network Device Group] タブから、次のいずれかを実行します。

a. [Create] をクリックします。

b. 複製する NDG ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

c. 編集する NDG ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ タイプを選択します。

ステップ 3　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ値を選択します。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「IP アドレスベースのデバイス フィルタの定義」（P.9-13）
- 「名前ベースのデバイス フィルタの定義」（P.9-14）

デバイス ポート フィルタの作成、複製、および編集

[Device Port Filters] ページを使用して、デバイス ポート フィルタを作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Network Conditions] > [Device Port Filters] を選択します。

[Device Port Filters] ページが表示され、設定したデバイス ポート フィルタのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製するデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集するデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- [Export] をクリックして、デバイス ポート フィルタのリストを .csv ファイルに保存します。詳細については、「ネットワーク条件のエクスポート」（P.9-9）を参照してください。
- [Replace from File] をクリックして、.csv インポート ファイルからデバイス ポート フィルタの一括インポートを実行します。詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ステップ 3　次のフィールドに値を入力します。

- [Name]：デバイス ポート フィルタの名前。
- [Description]：デバイス ポート フィルタの説明。

ステップ 4　次のいずれかのタブまたはすべてのタブのフィールドを編集します。

- [IP Address]：このタブのフィールドについては、「IP アドレスベースのデバイス ポート フィルタの定義」（P.9-17）を参照してください。
- [Device Name]：このタブのフィールドについては、「NDG ベースのデバイス ポート フィルタの定義」（P.9-18）を参照してください。
- [Network Device Group]：このタブのフィールドについては、「NDG ベースのデバイス ポート フィルタの定義」（P.9-18）を参照してください。

（注）　フィルタを設定するには、最低限、3 つのタブの少なくとも 1 つにフィルタ基準を入力する必要があります。

ステップ 5　[Submit] をクリックして変更を保存します。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「ネットワーク条件のインポート」（P.9-8）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）

IP アドレスベースのデバイス ポート フィルタの定義

ネットワーク デバイス ポートへのアクセスを許可または拒否する場合、そのネットワーク デバイス ポートの IP アドレスを作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[IP Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する IP ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する IP ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　次のいずれかを選択します。

- [Single IP Address]：このオプションを選択した場合、次のように有効なアドレスを入力する必要があります。
  - *x.x.x.x* という形式の IPv4 アドレス。*x* には 0 ～ 255 の任意の値を指定できます。
  - *x:x:x:x:x:x:x:x* という形式の IPv6 アドレス。*x* はアドレスの 8 つの 16 ビット部分の 1 ～ 4 桁の 16 進数を表します。これには、0 ～ 9 の数字または A ～ F の文字を指定できます。
- [IP Range(s)]：このオプションを選択した場合、有効な IPv4 または IPv6 アドレスおよびサブネット マスクを入力して、IP アドレスの範囲をフィルタリングする必要があります。デフォルトでは、IPv4 のサブネット マスクの値は 32、IPv6 の値は 128 です。

（注）　IPv6 範囲は ACS 5.4 ではサポートされません。

ステップ 3　[Port] チェックボックスをオンにして、ポート番号を入力します。このフィールドは文字列タイプであり、数字または文字を含めることができます。次のワイルドカード文字を使用できます。

- ? : 単一文字の一致
- * : 一連の文字の一致

たとえば、文字列「p*1*」は、「p」の文字で始まり、数字の 1 を含むすべての単語と一致します（port1、port15 など）。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-16）
- 「名前ベースのデバイス ポート フィルタの定義」（P.9-17）
- 「NDG ベースのデバイス ポート フィルタの定義」（P.9-18）

名前ベースのデバイス ポート フィルタの定義

ネットワーク デバイスおよびポートへのアクセスを許可または拒否する場合、そのネットワーク デバイスおよびポートの名前を作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[Device Name] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する名前ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する名前ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイスを選択します。

ステップ 3　[Port] チェックボックスをオンにして、ポート番号を入力します。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-16）
- 「IP アドレスベースのデバイス ポート フィルタの定義」（P.9-17）
- 「NDG ベースのデバイス ポート フィルタの定義」（P.9-18）

NDG ベースのデバイス ポート フィルタの定義

ネットワーク デバイス グループ タイプおよびポートへのアクセスを許可または拒否する場合、そのネットワーク デバイス グループ タイプおよびポートの名前を作成、複製、および編集できます。次の手順を実行します。

ステップ 1　[Network Device Group] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する NDG ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する NDG ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ タイプを選択します。

ステップ 3　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ値を選択します。

ステップ 4　[Port] チェックボックスをオンにして、ポート番号を入力します。

ステップ 5　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-7）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「IP アドレスベースのデバイス フィルタの定義」（P.9-13）
- 「名前ベースのデバイス フィルタの定義」（P.9-14）

認可および権限の管理

認可および権限を定義して、特定のポリシー規則に関連付けられている結果を決定できます。

次のことを定義できます。

- ネットワーク アクセス認可用の認可プロファイル（RADIUS 用）。
- TACACS+ シェル セッション用のシェル プロファイル、およびデバイス管理用のコマンド セット。
- ダウンロード可能 ACL。
- Cisco Security Group Access のセキュリティ グループおよびセキュリティ グループ ACL。これらのポリシー要素の設定については、「ACS と Cisco Security Group Access」（P.4-24）を参照してください。

次の項で、認可および権限を管理する方法について説明します。

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-19）
- 「セキュリティ グループの作成および編集」（P.9-25）
- 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）
- 「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-31）
- 「ダウンロード可能 ACL の作成、複製、および編集」（P.9-33）
- 「認可および権限のポリシー要素の削除」（P.9-34）
- 「セキュリティ グループ アクセス コントロール リストの設定」（P.9-35）

ネットワーク アクセス用の認可プロファイルの作成、複製、および編集

認可プロファイルを作成して、さまざまなタイプのユーザにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザには、有線接続を介してネットワークへのアクセスを試みるユーザよりも厳しく取り扱うことを定義できます。

認可プロファイルでは、Access-Accept 応答が返す属性と値のセットが定義されます。次を指定することができます。

- VLAN 情報、リダイレクト用の URL などの共通データ。この情報は、未加工の RADIUS パラメータ情報に自動的に変換されます。
- RADIUS 認可パラメータ：任意の RADIUS 属性を選択し、返す対応値を指定できます。

認可プロファイルを複製して、既存の認可プロファイルと同じか、または類似する新しい認可プロファイルを作成できます。複製の完了後、（元のまたは複製された）各認可プロファイルに個別にアクセスして、編集または削除します。

作成した認可プロファイルは、ネットワーク アクセス セッションの認可ポリシーの結果として使用できます。

認可プロファイルを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profile] を選択します。

[Authorization Profiles] ページが表示され、表 9-3 で説明されているフィールドが示されます。

表 9-3　[Authorization Profiles] ページ

オプション	説明
Name	既存のネットワーク アクセス認可定義のリスト。
Description	*表示のみ*。ネットワーク アクセス認可定義の説明。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する認可プロファイルの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Authorization Profile Properties] ページが表示されます。

ステップ 3　各タブの必須フィールドに有効な設定データを入力します。次を参照してください。

- 「認可プロファイルの指定」（P.9-20）
- 「認可プロファイルでの共通属性の指定」（P.9-21）
- 「認可プロファイルでの RADIUS 属性の指定」（P.9-23）

ステップ 4　[Submit] をクリックします。

認可プロファイルが保存されます。[Authorization Profiles] ページが表示され、作成または複製した認可プロファイルが示されます。

認可プロファイルの指定

認可プロファイルのタブを使用して、ネットワーク アクセス認可プロファイルの名前および説明を設定します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、次の項目をクリックします。

- 新しいネットワーク アクセス認可定義を作成するには、[Create]。
- ネットワーク アクセス認可定義を複製するには、[Duplicate]。
- ネットワーク アクセス認可定義を編集するには、[Edit]。

ステップ 2　表 9-4 に従い、[Authorization Profile: General] ページの必須フィールドに入力します。

表 9-4　[Authorization Profile: General] ページ

オプション	説明
Name	ネットワーク アクセス認可定義の名前。
Description	ネットワーク アクセス認可定義の説明。

ステップ 3　次のいずれかをクリックします。

- 変更を保存して [Authorization Profiles] ページに戻るには、[Submit]。

- 認可プロファイルの共通タスクを設定するには、[Common Tasks] タブ。「認可プロファイルでの共通属性の指定」（P.9-21）を参照してください。
- 認可プロファイルの RADIUS 属性を設定するには、[RADIUS Attributes] タブ。「認可プロファイルでの RADIUS 属性の指定」（P.9-23）を参照してください。

認可プロファイルでの共通属性の指定

認可プロファイルのタブを使用して、ネットワーク アクセス認可プロファイルに含める共通 RADIUS 属性を指定します。ACS では、指定した値が必須の RADIUS 属性と値のペアに変換され、[RADIUS Attributes] タブに表示されます。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、次の項目をクリックします。

- [Create] をクリックして新しいネットワーク アクセス認可定義を作成してから、[Common Tasks] タブをクリックします。
- [Duplicate] をクリックしてネットワーク アクセス認可定義を複製してから、[Common Tasks] タブをクリックします。
- [Edit] をクリックしてネットワーク アクセス認可定義を編集してから、[Common Tasks] タブをクリックします。

ステップ 2　表 9-5 に従い、[Authorization Profile: Common Tasks] ページの必須フィールドに入力します。

表 9-5　[Authorization Profile: Common Tasks] ページ

オプション	説明
ACL	
Downloadable ACL Name	定義済みのダウンロード可能 ACL が含まれます。ダウンロード可能 ACL の定義については、「ダウンロード可能 ACL の作成、複製、および編集」（P.9-33）を参照してください。
Filter-ID ACL	ACL フィルタ ID が含まれます。
Proxy ACL	プロキシ ACL が含まれます。
Voice VLAN	
Permission to Join	[Static] を選択します。このパラメータの値が表示されます。
VLAN	
VLAN ID/Name	VLAN 割り当てが含まれます。
Reauthentication	
Reauthentication Timer	セッション タイムアウト値を使用するかどうかを選択します。 • [Static] を選択した場合は、[Seconds] フィールドに値を入力する必要があります。デフォルト値は 3600 秒です。 • [Dynamic] を選択した場合は、ダイナミック パラメータを選択する必要があります。
Maintain Connectivity during Reauthentication	再認証の実行時に接続が確実に保持されるようにするには、[Yes] をクリックします。デフォルトでは、[Yes] が選択されています。このフィールドは、再認証タイマーを定義した場合にだけイネーブルになります。
QoS	
Input Policy Map	QoS 入力ポリシー マップが含まれます。
Output Policy Map	QoS 出力ポリシー マップが含まれます。
802.1X-REV	
LinkSec Security Policy	[Static] を選択した場合は、802.1X-REV LinkSec セキュリティ ポリシーの値を選択する必要があります。有効なオプションは次のとおりです。 • must-not-secure • should-secure • must-secure
URL Redirect URL がリダイレクト用に定義されている場合は、ACL も定義する必要があります。	
URL for Redirect	URL リダイレクトが含まれます。
URL Redirect ACL	URL リダイレクト用のアクセス コントロール リスト（ACL）の名前が含まれます。 URL リダイレクトを定義した場合は、その URL リダイレクション用の ACL も定義する必要があります。

認可プロファイルでの RADIUS 属性の指定

認可プロファイルのタブを使用して、認可プロファイルの Access-Accept パケットに含める RADIUS 属性を設定します。タブには、[Common Tasks] タブで選択した RADIUS 属性パラメータも表示されます。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、次の項目をクリックします。

- [Create] をクリックして新しいネットワーク アクセス認可定義を作成してから、[RADIUS Attributes] タブをクリックします。
- 複製する認可プロファイルの隣にあるチェックボックスをオンにして、[Duplicate] をクリックし、次に、[RADIUS Attributes] タブをクリックします。
- 編集する認可プロファイルの隣にあるチェックボックスをオンにして、[Edit] をクリックし、次に、[RADIUS Attributes] タブをクリックします。

ステップ 2　表 9-6 に従い、[Authorization Profile: RADIUS Attributes] ページの必須フィールドに入力します。

表 9-6　[Authorization Profile: RADIUS Attributes] ページ

オプション	説明
Common Tasks Attributes	[Common Tasks] タブで定義した属性の名前、値、およびタイプが表示されます。
Manually Entered	このセクションを使用して、認可プロファイルに含める RADIUS 属性を定義します。各属性を定義しているとき、その名前、値、およびタイプがテーブルに表示されます。変更後： • RADIUS 属性を追加するには、テーブルの下のフィールドに入力し、[Add] をクリックします。 • RADIUS 属性を編集するには、テーブルの該当する行を選択し、[Edit] をクリックします。RADIUS パラメータがテーブルの下のフィールドに表示されます。必要に応じて編集し、[Replace] をクリックします。
Dictionary Type	使用する RADIUS 属性が含まれているディクショナリを選択します。

表 9-6　[Authorization Profile: RADIUS Attributes] ページ （続き）

オプション	説明
RADIUS Attribute	RADIUS 属性の名前。[Select] をクリックして、指定したディクショナリから RADIUS 属性を選択します。 ネットワーク内の VPN デバイスを認証するには、VPN 属性を認可プロファイルに手動で追加する必要があります。ACS は、次に示すようにレイヤ 2 およびレイヤ 3 のさまざまなプロトコルで動作できます。 • IPSec：レイヤ 3 で動作します。必須属性を ACS 認可プロファイルで設定する必要はありませんが、任意の属性を設定できます。 • L2TP：L2TP トンネリング用です。次の属性を使用して ACS を設定する必要があります。 – CVPN3000/ASA/PIX7.x-Tunneling Protocols：この属性は、使用されるトンネリングのタイプを指定します。 – CVPN3000/ASA/PIX7.x-L2TP-Encryption：この属性が設定されている場合、VPN3000 は、MSCHAPv1 または MSCHAPv2 認証方式のいずれかで使用する必要がある Microsoft Point-to-Point Encryption（MPPE）キーをクライアントに伝えることができます。 • PPTP：トンネリング用です。次の属性を使用して ACS を設定する必要があります。 – CVPN3000/ASA/PIX7.x-Tunneling Protocols：この属性は、使用されるトンネリングのタイプを指定します。 – CVPN3000/ASA/PIX7.x-PPTP-Encryption：この属性が設定されていると、VPN3000 は、MSCHAPv1 または MSCHAPv2 認証方式のいずれかで使用する必要がある Microsoft Point-to-Point Encryption（MPPE）キーをクライアントに伝えることができます。
Attribute Type	ACS がアクセス要求を許可する対象となる、属性のクライアント ベンダー タイプ。これらの属性タイプについては、使用する AAA クライアントで稼働している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。
Attribute Value	属性の値。[Select] をクリックして、属性値のリストを表示します。これらの属性値については、使用する AAA クライアントで稼働している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。 トンネル プロトコルの場合、RFC 2868 に従って、特定のタグが付いた属性値が ACS によってアクセス応答内のデバイスに提供されます。 RADIUS 属性タイプとして [Tagged Enum] または [Tagged String] を選択した場合は、[Tag] フィールドが表示されます。タグ値については、同じトンネルに属す属性をグループ化するために ACS で使用する数字を入力します。 Tagged Enum 属性タイプの場合： • 適切な属性値を選択します。 • 適切なタグ値（0 ～ 31）を入力します。 Tagged String 属性タイプの場合： • 適切な文字列属性値（最大 256 文字）を入力します。 • 適切なタグ値（0 ～ 31）を入力します。

ステップ 3　次の設定を行います。

- 認可プロファイルの基本情報。「認可プロファイルの指定」（P.9-20）を参照してください。

- 認可プロファイルの共通タスク。「認可プロファイルでの共通属性の指定」（P.9-21）を参照してください。

セキュリティ グループの作成および編集

セキュリティ グループのページを使用して、セキュリティ グループおよび Security Group Tag（SGT; セキュリティ グループ タグ）の名前および詳細を表示し、セキュリティ グループを作成、複製、および編集するためのページを開きます。

セキュリティ グループを作成すると、ACS によって固有の SGT が生成されます。ネットワーク デバイスは、ACS に SGT 情報を問い合わせることができます。ネットワーク デバイスでは、この SGT 情報を使用して、入力時にパケットにタグ付けまたはペイントを行い、それらのパケットが出力時に出力ポリシーに従ってフィルタリングできるようにします。出力ポリシーの設定については、「[Egress Policy Matrix] ページ」（P.10-46）を参照してください。

ステップ 1　[Policy Elements] > [Authorizations and Permissions] > [Network Access] > [Security Groups] を選択します。

表 9-7 で説明されている [Security Groups] ページが表示されます。

表 9-7　[Security Groups] ページ

オプション	説明
Name	セキュリティ グループの名前。
SGT (Dec / Hex)	10 進数形式または 16 進数形式でのセキュリティ グループ タグの表現。
Description	セキュリティ グループの説明。

ステップ 2　次のいずれかをクリックします。

- 新しいセキュリティ グループを作成するには、[Create]。
- セキュリティ グループを複製するには、[Duplicate]。
- セキュリティ グループを編集するには、[Edit]。

ステップ 3　[Name] フィールドおよび [Description] フィールドに必須情報を入力し、[Submit] をクリックします。

関連項目

- 「セキュリティ グループの作成」（P.4-25）

デバイス管理用のシェル プロファイルの作成、複製、および編集

Cisco IOS シェル プロファイルおよびコマンド セットの認可を設定できます。シェル プロファイルとコマンド セットは、認可のために結合されています。シェル プロファイル認可によって、認可を要求しているユーザに次の機能を許可するかどうかが決定され、この決定は、そのユーザのセッションの間適用されます。

- 特権レベル。
- デバイス管理やネットワーク アクセスなどの一般的な機能。

シェル プロファイル定義は、次の 2 つのコンポーネントに分けられています。

- 共通タスク
- カスタム属性

[Common Tasks] タブを使用すると、頻繁に使用されるプロファイル属性を選択および設定できます。このタブに含まれている属性は、TACACS プロトコルのドラフト規格で定義されている属性です。これらの属性は、特に、シェル サービスに関連しています。ただし、これらの値は、他のサービスからの要求の認可に使用される場合があります。

[Custom Attributes] タブを使用すると、追加の属性を設定できます。各定義は、属性名、属性が必須であるか任意であるかの指定、および属性の値で構成されています。カスタム属性は、非シェル サービスに対して定義できます。

シェル プロファイルで指定する属性については、使用する AAA クライアントで稼働している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。

作成したシェル プロファイルおよびコマンド セットは、規則テーブル内の認可および権限で使用できます。

既存のシェル プロファイルと同じか、または類似する新しいシェル プロファイルを作成する場合は、シェル プロファイルを複製できます。

複製の完了後、（元のまたは複製された）各シェル プロファイルに個別にアクセスして、編集または削除します。

シェル プロファイルを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択します。

[Shell Profiles] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するシェル プロファイルの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Shell Profile Properties] ページの [General] タブが表示されます。

ステップ 3　各タブの必須フィールドに有効な設定データを入力します。最小設定としてシェル プロファイルの固有の名前を入力する必要があります。その他のフィールドはすべて任意です。次を参照してください。

- 「シェル プロファイルの一般プロパティの定義」（P.9-27）
- 「共通タスクの定義」（P.9-27）
- 「カスタム属性の定義」（P.9-30）

ステップ 4　[Submit] をクリックします。

シェル プロファイルが保存されます。[Shell Profiles] ページが表示され、作成または複製したシェル プロファイルが示されます。

関連トピック

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-19）

- 「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-31）
- 「認可および権限のポリシー要素の削除」（P.9-34）
- 「デバイス管理のシェル/コマンド認可ポリシーの設定」（P.10-35）

シェル プロファイルの一般プロパティの定義

シェル プロファイルのページを使用して、シェル プロファイルの一般プロパティを定義します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択してから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製するシェル プロファイルの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

ステップ 2　表 9-8 で説明されている [Shell Profile: General] フィールドに入力します。

表 9-8　[Shell Profile: General] ページ

オプション	説明
Name	シェル プロファイルの名前。
Description	（任意）シェル プロファイルの説明。

ステップ 3　次のいずれかをクリックします。

- 変更を保存して [Shell Profiles] ページに戻るには、[Submit]。
- 認可プロファイルの特権レベルを設定するには、[Common Tasks] タブ。「共通タスクの定義」（P.9-27）を参照してください。
- 認可プロファイルの RADIUS 属性を設定するには、[Custom Attributes] タブ。「カスタム属性の定義」（P.9-30）を参照してください。

関連トピック

- 「共通タスクの定義」（P.9-27）
- 「カスタム属性の定義」（P.9-30）

共通タスクの定義

共通タスクのページを使用して、シェル プロファイルの特権レベルおよび属性を定義します。これらの属性は、TACACS+ プロトコルによって定義されます。

これらの属性については、使用する AAA クライアントで稼働している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択してから、次の項目をクリックします。

- [Create] をクリックして新しいシェル プロファイルを作成してから、[Common Tasks] をクリックします。
- [Duplicate] をクリックしてシェル プロファイルを複製してから、[Common Tasks] をクリックします。
- [Edit] をクリックしてシェル プロファイルを編集してから、[Common Tasks] をクリックします。

ステップ 2　表 9-9 の説明に従って、[Shell Profile: Common Tasks] ページに入力します。

表 9-9　Shell Profile: Common Tasks

オプション	説明
Privilege Level	
Default Privilege	（任意）シェル認可を介してクライアントに許可する最初の特権レベル割り当てをイネーブルにします。ディセーブルの場合、この設定は認可および権限で解釈されません。
	[Default Privilege Level] では、シェル プロファイルのデフォルトの（最初の）特権レベルを指定します。[Enable Default Privilege] オプションとして [Static] を選択すると、デフォルトの特権レベルを選択できます。有効なオプションは 0 ～ 15 です。 [Enable Default Privilege] オプションとして [Dynamic] を選択した場合、代わりの属性に動的 ACS ディクショナリから属性を選択できます。
Maximum Privilege	（任意）最初のシェル認可のあと、クライアントに許可する最大特権レベル割り当てをイネーブルにします。
	[Maximum Privilege Level] では、シェル プロファイルの最大特権レベルを指定します。[Enable Change of Privilege Level] オプションを選択すると、最大特権レベルを選択できます。有効なオプションは 0 ～ 15 です。 デフォルトの特権レベルの割り当てと最大特権レベルの割り当てを両方選択する場合は、デフォルトの特権レベルの割り当てが最大特権レベルの割り当て以下である必要があります。
Shell Attributes	
次のオプションをイネーブルにしない場合は、それらのオプションに対して [Not in Use] を選択します。 [Dynamic] を選択した場合、リストされた動的ディクショナリの 1 つからの別の属性の値で TACACS+ 属性の静的な値を置換できます	
Access Control List	（任意）[Static] を選択し、イネーブルにするアクセス コントロール リストの名前を指定します。アクセス コントロール リストの名前は最大 27 文字まで可能で、次を含むことはできません。 ハイフン（-）、左角カッコ（[）、右角カッコ（]）、スラッシュ（/）、バックスラッシュ（\）、アポストロフィ（'）、左山カッコ（<）、右山カッコ（>）。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。
Auto Command	（任意）[Static] を選択し、イネーブルにするコマンドを指定します。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。
No Callback Verify	（任意）[Static] を選択し、コールバック検証が必要であるかどうかを指定します。有効なオプションは次のとおりです。 • [True]：コールバック検証が不要であることを指定します。 • [False]：コールバック検証が必要であることを指定します。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。

表 9-9　Shell Profile: Common Tasks （続き）

オプション	説明
No Escape	（任意）[Static] を選択し、エスケープ防止が必要であるかどうかを指定します。有効なオプションは次のとおりです。 • [True]：エスケープ防止をイネーブルにすることを指定します。 • [False]：エスケープ防止をイネーブルにしないことを指定します。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。
No Hang Up	（任意）[Static] を選択し、ハングアップが必要であるかどうかを指定します。有効なオプションは次のとおりです。 • [True]：切断なしを許可することを指定します。 • [False]：切断を許可することを指定します。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。
Timeout	（任意）[Static] を選択して、許可されたタイムアウト期間を値フィールドでイネーブルにし、分単位で指定します。有効な範囲は 0 ～ 999 です。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。
Idle Time	（任意）[Static] を選択して、許可されたアイドル時間の期間を値フィールドでイネーブルにし、分単位で指定します。有効な範囲は 0 ～ 999 です。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。
Callback Line	（任意）[Static] を選択して、コールバック電話回線を値フィールドでイネーブルにし、指定します。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。
Callback Rotary	（任意）[Static] を選択して、コールバック ロータリー電話回線を値フィールドでイネーブルにし、指定します。 代わりの属性に動的 ACS ディクショナリから属性を選択するには、[Dynamic] を選択します。

ステップ 3　次のいずれかをクリックします。

- 変更を保存して [Shell Profiles] ページに戻るには、[Submit]。
- 認可プロファイルの名前および説明を設定するには、[General] タブ。「シェル プロファイルの一般プロパティの定義」（P.9-27）を参照してください。
- 認可プロファイルのカスタム属性を設定するには、[Custom Attributes] タブ。「カスタム属性の定義」（P.9-30）を参照してください。

リストされた動的ディクショナリの 1 つからの別の属性の値で TACACS+ 属性の静的な値を置換するには、次のステップを実行します

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] を選択して、属性を内部ユーザ ディクショナリに追加します。

ステップ 2　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択してシェル プロファイルを作成します。

ステップ 3　[Custom Attributes] タブを選択して新しい属性を作成し、属性値として [Dynamic] を選択し、内部ユーザ ディクショナリの作成された属性に関連付けます。

ステップ 4　新しいルールを [Access Policies] > [Access Services] > [Default Device Admin] > [Authorization] で作成し、代わりにシェル プロファイルとして作成される結果を選択します。

認可後、内部 ID ストアから動的な属性値として応答が表示されます。

関連トピック

- 「カスタム属性の定義」（P.9-30）
- 「デバイス管理のシェル / コマンド認可ポリシーの設定」（P.10-35）

カスタム属性の定義

カスタム属性のタブを使用して、シェル プロファイルのカスタム属性を定義します。このタブには、[Common Tasks] タブで選択した共通タスク属性も表示されます。

ステップ 1　表 9-10 の説明に従って、[Custom Attributes] タブのフィールドを編集します。

表 9-10　[Shell Profile: Custom Attributes] ページ

オプション	説明
Common Tasks Attributes	[Common Tasks] タブで定義した共通タスク属性の名前、要件、および値が表示されます。
Manually Entered	このセクションを使用して、認可プロファイルに含めるカスタム属性を定義します。各属性を定義しているとき、その名前、要件、および値がテーブルに表示されます。変更後： • カスタム属性を追加するには、テーブルの下のフィールドに入力し、[Add] をクリックします。 • カスタム属性を編集するには、テーブルの該当する行を選択し、[Edit] をクリックします。 カスタム属性パラメータがテーブルの下のフィールドに表示されます。必要に応じて編集し、[Replace] をクリックします。
Attribute	カスタム属性の名前。
Requirement	カスタム属性が必須であるか任意であるかを選択します。
Attribute Value	カスタム属性がスタティックであるかダイナミックであるかを選択します。

ステップ 2　次のいずれかをクリックします。

- 変更を保存して [Shell Profiles] ページに戻るには、[Submit]。
- 認可プロファイルの名前および説明を設定するには、[General] タブ。「シェル プロファイルの一般プロパティの定義」（P.9-27）を参照してください。
- シェル プロファイルの特権レベルおよび属性を認可プロファイルに設定するには、[Common Tasks] タブ。「共通タスクの定義」（P.9-27）を参照してください。

関連トピック

- 「シェル プロファイルの一般プロパティの定義」（P.9-27）
- 「共通タスクの定義」（P.9-27）

管理デバイス用のコマンド セットの作成、複製、および編集

コマンド セットによって、デバイス管理用に許可されたコマンドおよび引数が決まります。デバイス設定認可ポリシーの結果としてコマンド セットを指定できます。シェル プロファイルとコマンド セットは、認可のために統合されており、ユーザ セッションの間適用されます。

既存のコマンド セットと同じか、または類似する新しいコマンド セットを作成する場合は、コマンド セットを複製できます。複製の完了後、（元のまたは複製された）各コマンド セットに個別にアクセスして、編集または削除します。

作成したコマンド セットは、規則テーブル内の認可および権限で使用できます。規則に複数のコマンド セットが含まれている場合があります。「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）を参照してください。

（注）　コマンド セットでは、TACACS+ プロトコル属性だけがサポートされています。

新しいコマンド セットを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Command Sets] を選択します。

[Command Sets] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。

  [Command Set Properties] ページが表示されます。
- 複製するコマンド セットの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

  [Command Set Properties] ページが表示されます。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

  [Command Set Properties] ページが表示されます。
- [File Operations] をクリックして、次のいずれかの機能を実行します。
  - Add：コマンド セットをインポート ファイルから ACS に追加するには、このオプションを選択します。
  - Update：ACS でのコマンド セットのリストをインポート ファイル内のコマンド セットのリストに置き換えるには、このオプションを選択します。
  - Delete：インポート ファイルでリストされているコマンド セットを ACS から削除するには、このオプションを選択します。

  一括操作の詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。
- ACS からコマンド セットをローカル ハードディスクにエクスポートするには、[Export] をクリックします。

  ダイアログボックスが表示され、コマンド セットをセキュアにエクスポートするための暗号化パスワードを入力するよう要求するプロンプトが表示されます。

a. [Password] チェックボックスをオンにして、エクスポート プロセスでファイルを暗号化するためのパスワードを入力し、[Start Export] をクリックします。

b. 暗号化を使用しない場合は、[Start Export] をクリックして、コマンド セットをエクスポートします。

ステップ 3　必須フィールドに有効な設定データを入力します。

最小設定としてコマンド セットの固有の名前を入力する必要があります。その他のフィールドはすべて任意です。コマンドおよび引数を定義できます。他のコマンド セットのコマンドと引数を追加することもできます。

[Command Set Properties] ページのフィールドについては、表 9-11 を参照してください。

表 9-11　[Command Set Properties] ページ

フィールド	説明
Name	コマンド セットの名前。
Description	（任意）コマンド セットの説明。
Permit any command that is not in the table below	Grant 表でコマンドが明示的に拒否されている場合を除き、要求されたすべてのコマンドを許可する場合にオンにします。Grant 表で明示的に許可されているコマンドだけを許可する場合はオフにします。
Command Set table	このセクションを使用して、認可プロファイルに含めるコマンドを定義します。各コマンドを定義しているとき、コマンドの詳細が表に表示されます。変更後： • コマンドを追加するには、表の下のフィールドに入力し、[Add] をクリックします。 • コマンドを編集するには、表の該当する行を選択し、[Edit] をクリックします。コマンド ライン パラメータが、表の下のフィールドに表示されます。必要に応じて編集し、[Replace] をクリックします。 Command Set 表内のコマンドの順序が重要となります。これは、最初に一致したコマンドおよび引数に応じてポリシー規則表の処理が決まり、ポリシー結果の選択に関する決定が行われるためです。Command Set 表の右にあるコントロール ボタンを使用して、コマンドの順序を変更します。
Grant	関連付けられたコマンドの権限レベルを選択します。次のオプションがあります。 • Permit：関連付けられたコマンドおよび引数は、自動的に許可されます。 • Deny：関連付けられたコマンドおよび引数は、自動的に拒否されます。 • Deny Always：関連付けられたコマンドおよび引数は、常に拒否されます。
Command	コマンド名を入力します。このフィールドは、大文字と小文字が区別されません。アスタリスク（*）を使用して、コマンド名のゼロ（0）以上の文字を表すことができます。疑問符（?）を使用して、コマンド名の単一文字を表すことができます。 有効なコマンド名のエントリ例： • SHOW • sH* • sho? • Sh*?
Arguments (field)	コマンド名に関連付けられている引数を入力します。このフィールドは、大文字と小文字が区別されません。 ACS 5.4 では、UNIX タイプの標準正規表現が使用されます。
Select Command/ Arguments from Command Set	別のコマンド セットからコマンドを追加するには、次の手順を実行します。 1. コマンド セットを選択します。 2. [Select] を選択して、使用可能なコマンドおよび引数がリストされているページを開きます。 3. コマンドを選択し、[OK] をクリックします。

ステップ 4　[Submit] をクリックします。

コマンド セットが保存されます。[Command Sets] ページが表示され、作成または複製したコマンド セットが示されます。

関連トピック

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-19）
- 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）
- 「認可および権限のポリシー要素の削除」（P.9-34）
- 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）

ダウンロード可能 ACL の作成、複製、および編集

ダウンロード可能 ACL を定義して、Access-Accept メッセージを返すことができます。ACL を使用して、ネットワークに不要なトラフィックが発生することを防止します。ACL では、RADIUS プロトコルを使用して、送信元 IP アドレスと宛先 IP アドレス、トランスポート プロトコルなどをフィルタリングできます。

名前付き権限オブジェクトとして作成したダウンロード可能 ACL は、認可プロファイルに追加できます。その後、これらの認可プロファイルを認可ポリシーの結果として指定できます。

既存のダウンロード可能 ACL と同じか、または類似する新しいダウンロード可能 ACL を作成する場合は、ダウンロード可能 ACL を複製できます。

複製の完了後、（元のまたは複製された）各ダウンロード可能 ACL に個別にアクセスして、編集または削除します。

ダウンロード可能 ACL を作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Named Permission Objects] > [Downloadable ACLs] を選択します。

[Downloadable ACLs] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。

  [Downloadable ACL Properties] ページが表示されます。
- 複製するダウンロード可能 ACL の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

  [Downloadable ACL Properties] ページが表示されます。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

  [Downloadable ACL Properties] ページが表示されます。
- [File Operations] をクリックして、次のいずれかの機能を実行します。
  - [Add]：インポート ファイルから ACL を ACS に追加するには、このオプションを選択します。
  - [Update]：ACS での ACL のリストをインポート ファイル内の ACL のリストに置き換えるには、このオプションを選択します。

- [Delete] : インポート ファイルでリストされている ACL を ACS から削除するには、このオプションを選択します。

一括操作の詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。

- ACS から DACL をローカル ハードディスクにエクスポートするには、[Export] をクリックします。

  ダイアログボックスが表示され、DACL をセキュアにエクスポートするための暗号化パスワードを入力するよう要求するプロンプトが表示されます。

  - [Password] チェックボックスをオンにして、エクスポート プロセスでファイルを暗号化するためのパスワードを入力し、[Start Export] をクリックします。
  - 暗号化を使用しない場合は、[Start Export] をクリックして、DACL をエクスポートします。

ステップ 3　表 9-12 に従い、有効な設定データを必須フィールドに入力し、標準 ACL 構文を使用して 1 つ以上の ACL を定義します。

表 9-12　[Downloadable ACL Properties] ページ

オプション	説明
Name	DACL の名前。
Description	DACL の説明。
Downloadable ACL Content	ACL コンテンツを定義します。 標準 ACL コマンド構文と意味を使用します。ACL 定義は、1 つ以上の ACL コマンドで構成されています。各 ACL コマンドは、個別の行に挿入されています。 ACL 定義の詳細については、デバイス コンフィギュレーション ガイドのコマンド リファレンスを参照してください。

ステップ 4　[Submit] をクリックします。

ダウンロード可能 ACL が保存されます。[Downloadable ACLs] ページが表示され、作成または複製したダウンロード可能 ACL が示されます。

関連トピック

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-19）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「認可および権限のポリシー要素の削除」（P.9-34）

認可および権限のポリシー要素の削除

認可および権限のポリシー要素を削除するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] を選択してから、必要なオプションに移動します。

対応するページが表示されます。

ステップ 2　削除する項目の隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

ページが表示されます。このとき、削除されたオブジェクトは表示されません。

セキュリティ グループ アクセス コントロール リストの設定

セキュリティ グループ アクセス コントロール リスト（SGACL）が、送信元 SGT および宛先 SGT に基づいて、入力時に適用されます。このページは、SGACL を表示、作成、複製、および編集する場合に使用します。SGACL の名前またはコンテンツを変更すると、ACS ではその生成 ID が更新されます。SGACL の生成 ID が変更されると、関連する Security Group Access ネットワーク デバイスによって SGACL のコンテンツがリロードされます。

また、SGACL は、Role-Based ACL（RBACL; ロールベースの ACL）とも呼ばれます。

ステップ 1　[Policy Elements] > [Authorizations and Permissions] > [Named Permissions Objects] > [Security Group ACLs] を選択します。

[Security Group Access Control Lists] ページが表示され、表 9-13 で説明されているフィールドが示されます。

表 9-13　[Security Group Access Control Lists] ページ

オプション	説明
Name	SGACL の名前。
Description	SGACL の説明。

ステップ 2　次のオプションのいずれかをクリックします。

- 新しい SGACL を作成する場合は、[Create]。
- SGACL を複製する場合は、[Duplicate]。
- SGACL を編集する場合は、[Edit]。

ステップ 3　表 9-14 の説明に従って、[Security Group Access Control Lists Properties] ページのフィールドに入力します。

表 9-14　[Security Group Access Control List Properties] ページ

オプション	説明
General	
Name	SGACL の名前。名前にはスペース、ハイフン（-）、疑問符（?）、または感嘆符（!）を使用できません。SGACL を作成すると、その生成 ID が表示されます。
Generation ID	*表示のみ*。次の項目を変更すると、ACS では SGACL の生成 ID が更新されます。 • SGACL の名前。 • SGACL のコンテンツ（ACE）。 SGACL の説明を変更しても、生成 ID は更新されません。

表 9-14　[Security Group Access Control List Properties] ページ （続き）

オプション	説明
Description	SGACL の説明。
Security Group ACL Content	ACL コンテンツを入力します。ACL 定義の構文および意味が有効であることを確認します。

ステップ 4　[Submit] をクリックします。

CHAPTER 10

アクセス ポリシーの管理

ACS 5.4 では、すべてのアクティビティはポリシーに従って実行されます。ポリシーは、主に、ポリシーの処理を決定する規則で構成されています。アクセス サービスを作成して、要求の認証および認可ポリシーを定義します。グローバル サービス セレクション ポリシーには、着信要求を処理するアクセス サービスを決定する規則が含まれています。

ポリシーとそのすべての要素を設定するための基本的なワークフローについては、「サービスおよびポリシーの設定フロー」（P.3-19）を参照してください。通常、ポリシー規則を設定する前に、ID、条件、認可、権限などの必要なすべての要素を設定する必要があります。

詳細については、次を参照してください。

- ID の管理については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。
- 条件の設定については、「ポリシー要素の管理」（P.9-1）を参照してください。
- 認可と権限の設定については、「システムの動作の設定」（P.17-1）を参照してください。

ここでは、次の内容について説明します。

- 「ポリシー作成フロー」（P.10-1）
- 「ポリシーのカスタマイズ」（P.10-4）
- 「サービス セレクション ポリシーの設定」（P.10-5）
- 「アクセス サービスの設定」（P.10-11）
- 「アクセス サービス ポリシーの設定」（P.10-22）
- 「複合条件の設定」（P.10-41）
- 「[Security Group Access Control] ページ」（P.10-46）
- 「最大ユーザ セッション数」（P.10-51）

Cisco Security Group Access 用の出力および NDAC ポリシーについては、「NDAC ポリシーの設定」（P.4-26）を参照してください。

ポリシー作成フロー

ポリシー作成は、ネットワーク設定および個々のポリシーに対する改良の程度に依存します。ポリシー作成のエンドポイントは、サービス セレクション ポリシーの結果として実行されるアクセス サービスです。各ポリシーは規則に従って実行されます。

つまり、次を決定する必要があります。

- ネットワーク設定の詳細
- ポリシーを実装するアクセス サービス
- アクセス サービスを実行できる条件を定義する規則

ここでは、次の内容について説明します。

- 「ネットワークの定義とポリシーの目的」（P.10-2）
- 「ポリシー作成フローのポリシー要素」（P.10-3）
- 「アクセス サービス ポリシーの作成」（P.10-4）
- 「サービス セレクション ポリシーの作成」（P.10-4）

ネットワークの定義とポリシーの目的

ポリシー作成の最初の手順では、ポリシーを適用するデバイスとユーザを決定します。その後、ポリシー要素を設定できます。

基本的なポリシー作成では、Web インターフェイスの左側のナビゲーション ペインに表示されるドロワの順序に従って操作できます。一部のポリシー要素は他のポリシー要素に依存するため、ドロワの順序が役立ちます。ポリシー ドロワを順番に使用する場合、現在のドロワに必要な要素を、最初に前に戻って定義する必要がなくなります。

たとえば、ネットワーク設定の次の要素から簡単なデバイス管理ポリシーを作成できます。

- デバイス：ルータとスイッチ。
- ユーザ：ネットワーク エンジニア。
- デバイス グループ：デバイスを場所およびデバイス タイプでグループ化します。
- ID グループ：ネットワーク技術者を場所およびアクセス レベルでグループ化します。

ポリシーの結果は、各サイトの管理スタッフに適用されます。

- 自分のサイトのデバイスに対するフル アクセス
- 他のすべてのデバイスに対する読み取り専用アクセス
- スーパーバイザの場合はすべてに対するフル アクセス

ポリシー自体は、ネットワーク操作およびデバイス管理ポリシー内の特権を持つ管理者に適用されます。ユーザ（ネットワーク技術者）は、内部 ID ストアに格納されます。

ポリシー結果は、アクセス要求に応じて適用された認可と権限です。これらの認可と権限は、ポリシー要素としても設定されます。

ポリシー作成フロー：次の手順

- 「ポリシー作成フローのポリシー要素」（P.10-3）
- 「アクセス サービス ポリシーの作成」（P.10-4）
- 「サービス セレクション ポリシーの作成」（P.10-4）

ポリシー作成フローのポリシー要素

Web インターフェイスには、デバイス グループや ID グループの定義に使用できる次のデフォルトが用意されています。

- All Locations
- All Device Types
- All Groups

作成する場所、デバイス タイプ、および ID グループは、これらのデフォルトの子です。

基本的なデバイス管理ポリシーの構築ブロックを作成するには、次の手順を実行します。

ステップ 1　ネットワーク リソースを作成します。[Network Resources] ドロワで、次を作成します。

a. [All Locations] > [East]、[West]、[HQ] など、場所のデバイス グループ

b. [All Device Types] > [Router]、[Switch] など、デバイス タイプのデバイス グループ

c. [EAST-ACCESS-SWITCH]、[HQ-CORE-SWITCH]、[WEST-WAN-ROUTER] など、AAA クライアント（AAA スイッチとルータのクライアント、それぞれのアドレス、およびそれぞれのプロトコル）

ステップ 2　ユーザおよび ID ストアを作成します。[Users and Identity Stores] ドロワで、次を作成します。

a. ID グループ（Network Operations および Supervisor）

b. 特定のユーザおよび ID グループとの関連付け（[Name]、[Identity Group]、[Password] など）

ステップ 3　デバイス管理の認可と権限を作成します。[Policy Elements] ドロワで、次を作成します。

a. フル アクセス、読み取り専用などの特定の特権（[Shell Profiles] 内）

b. アクセスを許可または拒否するコマンド セット（[Command Sets] 内）

このポリシーでは、次の構築ブロックが作成されます。

- 次のようなネットワーク デバイス グループ（NDG）。
  - 場所：East、HQ、West
  - デバイス タイプ：Router、Switch
- 次のような ID グループ。
  - ネットワーク運用サイト：East、HQ、West
  - アクセス レベル：フル アクセス
- デバイス：ネットワーク デバイス グループに割り当てられているルータとスイッチ。
- ユーザ：ID グループに割り当てられている内部 ID ストア内のネットワーク技術者。
- シェル プロファイル：各管理者に適用できる、次のような特権。
  - 完全な特権
  - 読み取り専用の特権
- コマンド セット：各管理者に対して認可を許可または拒否。

ポリシー作成フロー：前の手順

- 「ネットワークの定義とポリシーの目的」（P.10-2）

ポリシー作成フロー：次の手順

- 「アクセス サービス ポリシーの作成」（P.10-4）
- 「サービス セレクション ポリシーの作成」（P.10-4）

アクセス サービス ポリシーの作成

基本要素を作成したあと、ID グループと特権を含むアクセス ポリシーを作成できます。たとえば、次のデータを使用する認可および認証ポリシーが含まれる、NetOps というデバイス管理用のアクセス サービスを作成できます。

- Supervisor ID グループのユーザ：すべての場所にあるすべてのデバイスに対する完全な特権を持ちます。
- East、HQ、および West ID グループのユーザ：対応する East、HQ、および West デバイス グループのデバイスに対する完全な特権を持ちます。
- 一致しない場合：アクセスを拒否します。

ポリシー作成フロー：前の手順

- 「ネットワークの定義とポリシーの目的」（P.10-2）
- 「ポリシー作成フローのポリシー要素」（P.10-3）

ポリシー作成フロー：次の手順

- 「サービス セレクション ポリシーの作成」（P.10-4）

サービス セレクション ポリシーの作成

ACS は、さまざまなアクセス使用例に対応しています。たとえば、デバイス管理、無線アクセス、ネットワーク アクセス コントロールなどがあります。これらの使用例それぞれについてアクセス ポリシーを作成できます。サービス セレクション ポリシーでは、着信要求に適用するアクセス ポリシーを決定します。

たとえば、TACAC+ プロトコルを使用するアクセス要求に NetOps アクセス サービスを適用するサービス セレクション規則を作成できます。

ポリシー作成フロー：前の手順

- 「ネットワークの定義とポリシーの目的」（P.10-2）
- 「ポリシー作成フローのポリシー要素」（P.10-3）
- 「アクセス サービス ポリシーの作成」（P.10-4）

ポリシーのカスタマイズ

ACS ポリシー規則には、条件と結果が含まれています。ポリシーの規則の定義を開始する前に、ポリシーに含める条件のタイプを設定する必要があります。この手順はポリシーのカスタマイズと呼ばれます。選択した条件タイプは、[Policy] ページに表示されます。[Policy] ページに表示される条件タイプだけを適用できます。ポリシー条件の詳細については、「ポリシー条件の管理」（P.9-1）を参照してください。

デフォルトでは、[Policy] ページには複合式の条件カラムが 1 つ表示されます。複合条件の詳細については、「複合条件の設定」（P.10-41）を参照してください。

Security Group Access 機能を実装している場合は、認可ポリシーの結果をカスタマイズすることもできます。

注意　すでに規則を定義している場合は、規則で条件のカスタマイズ時に削除する条件が使用されていないことを確認してください。条件カラムを削除すると、そのカラムに存在するすべての設定済み条件が削除されます。

ポリシーをカスタマイズするには、次の手順を実行します。

ステップ 1　カスタマイズする [Policy] ページを開きます。手順は次のとおりです。

- サービス セレクション ポリシーの場合は、[Access Policies] > [Service Selection Policy] を選択します。
- アクセス サービス ポリシーの場合は、[Access Policies] > [Access Services] > *service* > *policy* を選択します。*service* はアクセス サービスの名前、*policy* はカスタマイズするポリシーの名前です。

ステップ 2　[Policy] ページで [Customize] をクリックします。

条件のリストが表示されます。このリストには、ID 属性、システム条件、およびカスタム条件が含まれています。

（注）　ID 関連の属性は、サービス セレクション ポリシー内の条件としては使用できません。

ステップ 3　条件を [Available] リスト ボックスと [Selected] リスト ボックスの間で移動します。

ステップ 4　[OK] をクリックします。

選択した条件が [Conditions] カラムに表示されます。

ステップ 5　[Save Changes] をクリックします。

ポリシーの設定：次の手順

- 「サービス セレクション ポリシーの設定」（P.10-5）
- 「アクセス サービス ポリシーの設定」（P.10-22）

サービス セレクション ポリシーの設定

サービス セレクション ポリシーでは、着信要求を処理するアクセス サービスを決定します。すべての要求に同じアクセス サービスを適用する単純なポリシー、またはルール ベースのサービス セレクション ポリシーを設定できます。

ルール ベースのポリシーでは、各サービス セレクション規則に 1 つ以上の条件、および着信要求に適用されるアクセス サービスである結果が含まれます。サービス セレクション ポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。

ここでは、次の内容について説明します。

- 「単純なサービス セレクション ポリシーの設定」（P.10-6）

- 「サービス セレクション規則の作成、複製、および編集」（P.10-8）

（注）　単純なポリシーを作成および保存してからルール ベースのポリシーに変更すると、単純なポリシーはルール ベースのポリシーのデフォルト規則になります。ルール ベースのポリシーを保存してから単純なポリシーに変更すると、デフォルト規則以外の規則はすべて失われます。デフォルト規則は、ACS によって自動的に単純なポリシーとして使用されます。

単純なサービス セレクション ポリシーの設定

単純なサービス セレクション ポリシーでは、すべての要求に同じアクセス サービスを適用します。

単純なサービス セレクション ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] を選択します。

デフォルトでは、[Simple Service Selection Policy] ページが表示されます。

ステップ 2　適用するアクセス サービスを選択するか、[Deny Access] を選択します。

ステップ 3　[Save Changes] を選択して、ポリシーを保存します。

[Service Selection Policy] ページ

このページは、着信要求に適用するサービスを決定する単純なポリシーまたはルール ベースのポリシーを設定する場合に使用します。

このページを表示するには、[Access Policies] > [Service Selection] を選択します。

すでにサービス セレクション ポリシーが設定されている場合は、対応する単純なポリシー ページ（表 10-1 を参照）またはルール ベースのポリシー ページ（表 10-2 を参照）が開きます。設定されていない場合は、デフォルトで単純なポリシー ページが開きます。

表 10-1　[Simple Service Selection Policy] ページ

オプション	説明
Policy type	ポリシーのタイプを定義します。 • Select one result：結果はすべての要求に適用されます。 • Rule-based result selection：設定規則により、要求に応じて異なる結果が適用されます。
Service Selection Policy	すべての要求に適用するアクセス サービス。デフォルトは [Deny Access] です。

表 10-2　[Rule-based Service Selection Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • Select one result：結果はすべての要求に適用されます。 • Rule-based result selection：設定規則により、要求に応じて異なる結果が適用されます。
Status	サービス セレクションを実行する規則の現在のステータス。規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor Only：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	サービスの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。 ID ベースの条件は、サービス セレクション規則で使用できません。
Results	規則の評価結果として実行されるサービス。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] をクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

ルール ベースのサービス セレクション ポリシーを設定するには、次の項を参照してください。

- 「サービス セレクション規則の作成、複製、および編集」（P.10-8）
- 「サービス セレクション規則の削除」（P.10-10）

サービス セレクション ポリシーの設定後、引き続きアクセス サービス ポリシーを設定できます。「アクセス サービス ポリシーの設定」（P.10-22）を参照してください。

サービス セレクション規則の作成、複製、および編集

着信要求を処理するアクセス サービスを決定するサービス セレクション規則を作成します。一致する規則がないか、または規則が定義されていない場合は、デフォルト規則によってデフォルトのアクセス サービスが指定されます。

規則を作成するときは、規則の順序が重要であることに注意してください。ACS ネットワークにアクセスしようとするクライアントの要求が ACS によって処理されるときに一致が見つかると、その後の処理はすべて停止され、その一致に関連する結果が検索されます。一致が見つかったあとは、それ以降の規則は考慮されません。

サービス セレクション規則を複製して、既存の規則と同じか、または既存の規則によく似た新規の規則を作成できます。複製された規則名では、元の規則に複製を示すカッコが付けられます。たとえば、Rule-1(1) です。複製の完了後は、各規則（元の規則および複製された規則）に個別にアクセスします。デフォルト規則は複製できません。

サービス セレクション規則のすべての値を編集できます。また、デフォルト規則内の指定したアクセス サービスを編集できます。

（注） すべての要求に同じアクセス サービスを適用する単純なポリシーを設定するには、「単純なサービス セレクション ポリシーの設定」（P.10-6）を参照してください。

はじめる前に

- サービス セレクション ポリシーで使用する条件を設定します。「ポリシー条件の管理」（P.9-1）を参照してください。

  （注） ID 関連の属性は、サービス セレクション ポリシー内の条件としては使用できません。

- サービス セレクション ポリシーで使用するアクセス サービスを作成します。「アクセス サービスの作成、複製、および編集」（P.10-12）を参照してください。サービス セレクション ポリシーを設定する前にアクセス サービスのポリシーを設定する必要はありません。
- ポリシー規則で使用する条件のタイプを設定します。詳細については、「ポリシーのカスタマイズ」（P.10-4）を参照してください。

サービス セレクション ポリシーを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] を選択します。次の場合があります。

- ルール ベースのポリシーを前に作成したことがある場合は、設定されている規則のリストを含む [Rule-Based Service Selection Policy] ページが表示されます。
- ルール ベースのポリシーを作成したことがない場合は、[Simple Service Selection Policy] ページが表示されます。[Rule-Based] をクリックします。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する規則の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する規則名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Rule] ページが表示されます。

ステップ 3　値を入力するか変更します。

- ユーザ定義の規則：任意の値を編集できます。少なくとも 1 つの条件が含まれていることを確認します。規則を複製する場合は、規則名を変更する必要があります。
- デフォルト規則：アクセス サービスだけを変更できます。

フィールドの説明については、表 10-3 を参照してください。

表 10-3　[Service Selection Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor Only：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。 デフォルトでは、複合条件が表示されます。表示された条件を変更するには、[Policy] ページで [Customize] をクリックします。 各条件のデフォルト値は、[*ANY*] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。
Results	
Service	規則の評価結果として実行されるアクセス サービスの名前。

ステップ 4　[OK] をクリックします。

設定した規則を含む [Service Selection Policy] ページが表示されます。

ステップ 5　[Save Changes] をクリックします。

関連トピック

- 「アクセス サービスの設定」（P.10-11）
- 「サービス セレクション規則の削除」（P.10-10）

ヒット カウントの表示

このページは、ルール ベースのポリシー ページの [Hit Count] 表示をリセットおよび更新する場合に使用します。

このページを表示するには、ルール ベースのポリシー ページの [Hit Count] をクリックします。

表 10-4　[Hit Count] ページ

オプション	説明
Hit Counts Reset	
Last time hit counts were reset for this policy	このポリシーで最後にヒット カウントがリセットされた日付と時刻を表示します。
Reset hit counts display for this policy	[Policy] ページのすべての規則について [Hit Count] 表示をゼロ（0）にリセットするには、[Reset] をクリックします。
Hit Counts Collection	
Hit counts are collected every:	ヒット カウント収集の間隔を表示します。
Last time hit counts were collected for this policy:	このポリシーで最後にヒット カウントが更新された日付と時刻を表示します。
Refresh hit counts display for this policy	[Policy] ページのヒット カウント表示をすべての規則の更新されたヒット カウントで更新するには、[Refresh] をクリックします。前回のヒット カウントは削除されます。 TACACS+ 認証要求が成功すると、対応する ID ポリシー規則と認可ポリシー規則の両方のヒット カウントは 1 ずつ増えます。

サービス セレクション規則の削除

（注）　デフォルトのサービス セレクション規則は削除できません。

サービス セレクション規則を削除するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] を選択します。

設定されている規則のリストを含む [Service Selection Policy] ページが表示されます。

ステップ 2　削除する規則の隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

[Service Selection Rules] ページが表示されます。このとき、削除した規則は表示されません。

ステップ 4　[Save Changes] をクリックして、新しい設定を保存します。

アクセス サービスの設定

アクセス サービスには、要求の認証および認可ポリシーが含まれています。使用例ごとに異なるアクセス サービスを作成できます。たとえば、デバイス管理、無線ネットワーク アクセスなどの使用例があります。

アクセス サービスを作成するときに、サービスに含まれるポリシーのタイプとポリシー構造を定義します。たとえば、デバイス管理やネットワーク アクセス用のポリシーがあります。

（注）　サービス セレクション規則を定義する前にアクセス サービスを作成する必要がありますが、サービスのポリシーを定義する必要はありません。

ここでは、次の内容について説明します。

- 「アクセス サービスの作成、複製、および編集」（P.10-12）
- 「アクセス サービスの削除」（P.10-21）

アクセス サービスの作成後、そのサービスをサービス セレクション ポリシーで使用できます。「サービス セレクション ポリシーの設定」（P.10-5）を参照してください。

アクセス サービスのポリシーはカスタマイズおよび変更できます。「アクセス サービス ポリシーの設定」（P.10-22）を参照してください。

関連項目

- 「アクセス サービスの作成、複製、および編集」（P.10-12）

デフォルトのアクセス サービスの編集

ACS 5.4 には、2 つのデフォルトのアクセス サービスが事前設定されています。1 つはデバイス管理用、もう 1 つはネットワーク アクセス用です。これらのアクセス サービスは編集可能です。

デフォルトのアクセス サービスを編集するには、次の手順を実行します。

ステップ 1　次のいずれかを選択します。

- [Access Policies] > [Access Services] > [Default Device Admin]
- [Access Policies] > [Access Services] > [Default Network Access]

[Default *Service* Access Service] 編集ページが表示されます。

ステップ 2　[Default *Service* Access Service] ページのフィールドを編集します。

[General] タブのフィールドについては、表 10-5 を参照してください。

表 10-5　Default Access Service：[General] ページ

オプション	説明
General	
Name	アクセス サービスの名前。
Description	アクセス サービスの説明。
Service Type	（表示のみ）サービスのタイプ。デバイス管理またはネットワーク アクセス。
Policy Structure	

表 10-5　Default Access Service：[General] ページ （続き）

オプション	説明
Identity	アクセス サービスに ID ポリシーを含めて、ACS で認証および属性の取得に使用する ID ストアを定義する場合にオンにします。
Group Mapping	アクセス サービスにグループ マッピング ポリシーを含めて、外部 ID ストアから取得したグループと属性を ACS の ID グループにマッピングする場合にオンにします。
Authorization	アクセス サービスに認可ポリシーを含めて、次を適用する場合にオンにします。 • ネットワーク アクセス サービスの認可プロファイル。 • デバイス管理サービスのシェル プロファイルおよびコマンド セット。

ステップ 3　表 10-7 の説明に従って、[Allowed Protocols] タブのフィールドを編集します。

ステップ 4　[Submit] をクリックして、デフォルトのアクセス サービスに対する変更を保存します。

アクセス サービスの作成、複製、および編集

アクセス サービスには、要求の認証および認可ポリシーが含まれています。

アクセス サービスを作成するときに、次を定義します。

- ポリシー構造：サービスに含めるポリシーのタイプ。これらは、サービス テンプレート、既存のサービス、または使用例に従って定義できます。

  サービスには次のポリシーを含めることができます。

  - ID ポリシー：認証に使用する ID ストアを定義します。
  - グループ マッピング ポリシー：マッピング先の ID グループを定義します。
  - 認可ポリシー：ネットワーク アクセスの場合、このポリシーでは、適用するセッション認可プロファイルを定義します。デバイス管理の場合、適用するシェル プロファイルまたはコマンド セットを定義します。
- 許可されたプロトコル：このアクセス サービスに許可される認証プロトコルを指定し、ACS がそれらのプロトコルを認証に使用する方法に関する詳細情報を指定します。

サービス テンプレートを使用して、特定の条件タイプを使用するようにカスタマイズされたポリシーを含むアクセス サービスを定義します。サービス テンプレートの詳細については、「アクセス サービス テンプレートの設定」（P.10-20）を参照してください。

既存のアクセス サービスと同じか、または既存のアクセス サービスによく似た規則を含む新規のアクセス サービスを作成するには、アクセス サービスを複製します。複製の完了後は、各サービス（元のサービスおよび複製されたサービス）に個別にアクセスします。

複製元サービスの規則を複製しないでサービス ポリシー構造を複製するには、既存のサービスに基づいて新しいアクセス サービスを作成します。

アクセス サービスを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] を選択します。

[Access Services] ページが表示され、設定されているサービスのリストが示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するアクセス サービスの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するアクセス サービス名をクリックします。または、名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。
- 左側のナビゲーション タブでアクセス サービス名をクリックします。

[Access Service Properties] の [General] ページが表示されます。

- 新規のアクセス サービスを作成する場合は、次の手順を実行します。

a. アクセス サービスの名前とポリシー構造を定義します。

b. [Next] をクリックして、[Allowed Protocols] ページに進みます。

c. [Finish] をクリックして、新規のアクセス サービスを保存します。

- アクセス サービスを複製または編集する場合は、次の手順を実行します。

a. [Properties] ページのタブのフィールドを必要に応じて変更します。ポリシーを追加できますが、既存のポリシーは削除できません。

b. [Submit] をクリックして変更を保存します。

有効なフィールド オプションの詳細については、次を参照してください。

- 「アクセス サービスの一般プロパティの設定」（P.10-13）
- 「アクセス サービスの許可されたプロトコルの設定」（P.10-16）
- 「アクセス サービス テンプレートの設定」（P.10-20）

アクセス サービスの設定が保存されます。新しい設定を含む [Access Services] ページが表示されます。

関連トピック

- 「アクセス サービスの削除」（P.10-21）
- 「アクセス サービス ポリシーの設定」（P.10-22）
- 「サービス セレクション ポリシーの設定」（P.10-5）

アクセス サービスの一般プロパティの設定

アクセス サービス定義には、一般および許可されたプロトコル情報が含まれています。サービスを複製および編集する場合、[Access Service properties] ページにタブが表示されます。

ステップ 1　[Access Policies] > [Access Services] を選択し、[Create]、[Duplicate]、または [Edit] をクリックします。

ステップ 2　表 10-6 の説明に従って、フィールドに入力します。

表 10-6　[Access Service Properties] : [General] ページ

オプション	説明
General	
Name	アクセス サービスの名前。サービスを複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。

表 10-6　[Access Service Properties] : [General] ページ （続き）

オプション	説明
Description	アクセス サービスの説明。
Access Service Policy Structure	
Based on service template	定義済みのテンプレートに基づいたポリシーを含むアクセス サービスを作成します。このオプションは、サービスの作成だけに使用できます。
Based on existing service	既存のアクセス サービスに基づいたポリシーを含むアクセス サービスを作成します。新しいアクセス サービスには、既存のサービスのポリシー規則は含まれません。このオプションは、サービスの作成だけに使用できます。ポリシー規則を含めてサービスを複製するには、既存のアクセス サービスを複製します。
User selected service type	アクセス サービス タイプを選択するためのオプションがあります。使用できるオプションは、[Network Access]、[Device Administration]、および [External Proxy] です。設定できるポリシーのリストは、選択したアクセス サービス タイプによって異なります。
User Selected Service Type : [Network Access] および [Device Administration]	
Policy Structure	
Identity	アクセス サービスに ID ポリシーを含めて、ACS で認証および属性の取得に使用する ID ストアを定義する場合にオンにします。
Group Mapping	アクセス サービスにグループ マッピング ポリシーを含めて、外部 ID ストアから取得したグループと属性を ACS の ID グループにマッピングする場合にオンにします。
Authorization	アクセス サービスに認可ポリシーを含めて、次を適用する場合にオンにします。 • ネットワーク アクセス サービスの認可プロファイル。 • デバイス管理サービスのシェル プロファイルおよびコマンド セット。
[User Selected Service Type] : [External Proxy]	
[External Proxy Servers] : プロキシに使用する外部サーバのセットを選択します。これらのサーバの使用順序を指定することもできます。	
Available External Proxy Servers	使用可能な外部 RADIUS および TACACS+ サーバのリスト。プロキシに使用する外部サーバを選択し、[Selected External Proxy Servers] リストに移動します。
Selected External Proxy Servers	選択した外部プロキシ サーバのリスト。
Advanced Options	
Accounting	
Remote Accounting	リモート アカウンティングをイネーブルにする場合にオンにします。
Local Accounting	ローカル アカウンティングをイネーブルにする場合にオンにします。
Username Prefix\Suffix Stripping	
Strip start of subject name up to the first occurrence of the separator	プレフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名が acme\smith、区切り文字が \ の場合、ユーザ名は smith になります。デフォルトの区切り文字は \ です。
Strip end of subject name from the last occurrence of the separator	サフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名が smith@acme.com、区切り文字が @ の場合、ユーザ名は smith になります。デフォルトの区切り文字は @ です。
[RADIUS Attributes] : プロキシ サーバに送信する前に、RADIUS 属性が入力属性を処理するために使用されます。	
Add	RADIUS 属性を定義した後で、RADIUS 属性リストに追加するには、[ADD] をクリックします。

表 10-6　[Access Service Properties] : [General] ページ （続き）

オプション	説明
Edit	リストされている RADIUS 属性を編集するには、リストから属性を選択し、[Edit] をクリックします。属性のプロパティがフィールドに表示されます。プロパティを必要に応じて変更し、[Replace] をクリックします。
Replace	選択した RADIUS 属性を、[RADIUS] フィールドに現在定義されているもので置き換えるには、[Replace] をクリックします。
Delete	リストから選択した RADIUS 属性を削除するには、[Delete] をクリックします。
Dictionary Type	使用する RADIUS 属性が含まれているディクショナリを選択します。
RADIUS Attribute	RADIUS 属性の名前。[Select] をクリックして、指定したディクショナリから RADIUS 属性を選択します。
Attribute Type	選択した RADIUS 属性のタイプ。ACS がアクセス要求を許可する対象となる、属性のクライアント ベンダー タイプ。これらの属性タイプについては、使用する AAA クライアントで稼働している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。
Operation	次の 3 つの操作を実行できます。 • 選択した RADIUS 属性の新しい属性値を追加するには、[ADD] を選択します。 – [Multiple not allowed] の場合：この属性が要求に存在しない場合に限り、選択した属性の新しい値を追加します。 – [Multiple allowed] の場合：新しい値を持つ属性を必ず追加します。 • 選択した RADIUS 属性の既存の値を更新するには、[UPDATE] を選択します。 – [Multiple not allowed] の場合：属性が要求に存在する場合に、新しい値で属性値を更新します。 – [Multiple allowed] の場合：この属性の出現をすべて削除し、新しい値を持つ属性を 1 つ追加します。 – 属性が cisco-avpair（キー = 値のペア）の場合、更新はキーに基づいて行われます。 • 選択した RADIUS 属性の値を削除するには、[DELETE] を選択します。 属性操作ステートメントは順序付けられます。管理者は、設定時にステートメントの順序を変更できます。ACS は、設定された順序に従って属性に動作を実行します。詳細については、「RADIUS 属性の書き換え動作」（P.A-9）を参照してください。
Attribute New Value	選択した RADIUS 属性の新しい値を入力します。このオプションは削除操作を選択した場合は使用できません。

ステップ 3　[Next] をクリックして、許可されたプロトコルを設定します。「アクセス サービスの許可されたプロトコルの設定」（P.10-16）を参照してください。

関連項目

- 「アクセス サービスの許可されたプロトコルの設定」（P.10-16）
- 「アクセス サービス テンプレートの設定」（P.10-20）

アクセス サービスの許可されたプロトコルの設定

アクセス サービス作成の第 2 部は、許可されたプロトコルです。アクセス サービス定義には、一般および許可されたプロトコル情報が含まれています。サービスを複製および編集する場合、[Access Service properties] ページにタブが表示されます。

ステップ 1　[Access Policies] > [Access Services] を選択し、次の操作を実行します。

- [Create] をクリックして新規のアクセス サービスを作成してから、[Next] をクリックして [Allowed Protocols] 画面に進みます。
- [Duplicate] をクリックしてアクセス サービスを複製してから、[Next] をクリックして [Allowed Protocols] 画面に進みます。
- [Edit] をクリックしてアクセス サービスを編集してから、[Next] をクリックして [Allowed Protocols] 画面に進みます。

ステップ 2　表 10-7 に示すように、フィールドに入力します。

表 10-7　[Access Service Properties] : [Allowed Protocols] ページ

オプション	説明
Process Host Lookup	たとえば RADIUS Service-Type が 10 の場合に [Host Lookup] フィールドを処理し、RADIUS Calling-Station-ID 属性の System UserName 属性を使用するように ACS を設定する場合にオンにします。 ACS でホスト ルックアップ要求を無視し、認証と認可に system UserName 属性の元の値を使用する場合はオフにします。オフにすると、メッセージ処理はプロトコル（たとえば PAP）に従って行われます。
Authentication Protocols	
Allow PAP/ASCII	PAP/ASCII をイネーブルにします。PAP は、平文パスワード（つまり暗号化されていないパスワード）を使用する最もセキュリティ レベルの低い認証プロトコルです。 [Allow PAP/ASCII] をオンにすると、[Detect PAP as Host Lookup] をオンにして、ネットワーク アクセス サービスでこのタイプの要求を PAP ではなくホスト ルックアップ要求として検出するように ACS を設定できます。
Allow CHAP	CHAP 認証をイネーブルにします。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Windows Active Directory では使用できません。
Allow MS-CHAPv1	MS-CHAPv1 をイネーブルにします。
Allow MSCHAPv2	MSCHAPv2 をイネーブルにします。
Allow EAP-MD5	EAP ベースの Message Digest 5 ハッシュ認証をイネーブルにします。 [Allow EAP-MD5] をオンにすると、[Detect EAP-MD5 as Host Lookup] をオンにして、ネットワーク アクセス サービスでこのタイプの要求を EAP-MD5 ではなくホスト ルックアップ要求として検出するように ACS を設定できます。

表 10-7　[Access Service Properties] : [Allowed Protocols] ページ （続き）

オプション	説明
Allow EAP-TLS	EAP-TLS 認証プロトコルをイネーブルにし、EAP-TLS 設定を行います。エンドユーザ クライアントからの EAP Identity 応答で提示されたユーザ ID を ACS が確認する方法を指定できます。ユーザ ID は、エンドユーザ クライアントによって提示された証明書の情報に照らして確認されます。この比較は、ACS とエンドユーザ クライアントとの間に EAP-TLS トンネルが確立されたあとに行われます。[Allow EAP-TLS] を選択した場合は、次を設定できます。 • [Enable Stateless Session resume] : アクセス サービスごとにステートレス セッション再開機能をイネーブルにするには、このチェックボックスをオンにします。この機能では、次のオプションを設定することが可能です。 – [Proactive Session Ticket update] : セッション チケットが更新される前に経過する必要がある存続可能時間の量を示すパーセント値を入力します。たとえば、値 10 を入力した場合、セッション チケットの更新は存続可能時間の 10 パーセントが過ぎた後に実行されます。 – [Session ticket Time to Live] : 正の整数を使用して日、週、月、および年に対応する最大値を入力します。 EAP-TLS は、証明書ベースの認証プロトコルです。EAP-TLS 認証が行われるのは、証明書の設定に必要な手順を完了した場合にかぎられます。詳細については、「ローカル サーバ証明書の設定」（P.18-14）を参照してください。
Allow LEAP	LEAP 認証をイネーブルにします。
Allow PEAP	PEAP 認証プロトコルと PEAP 設定をイネーブルにします。デフォルトの内部方式は、MSCHAPv2 です。 [Allow PEAP] をオンにすると、次の PEAP 内部方式を設定できます。 • [Allow EAP-TLS] : 内部方式として EAP-TLS を使用する場合にオンにします。 • [Allow EAP-MSCHAPv2] : 内部方式として EAP-MSCHAPv2 を使用する場合にオンにします。 – [Allow Password Change] : ACS でパスワード変更をサポートする場合にオンにします。 – [Retry Attempts] : ACS でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ～ 3 です。 • [Allow EAP-GTC] : 内部方式として EAP-GTC を使用する場合にオンにします。 – [Allow Password Change] : ACS でパスワード変更をサポートする場合にオンにします。 – [Retry Attempts] : ACS でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ～ 3 です。 • [Allow PEAP Cryptobinding TLV] : PEAP 暗号化バインド TLV のサポートを使用する場合にオンにします。 • [Allow PEAPv0 only for legacy clients] : PEAP サプリカントが PEAPv0 にかぎりネゴシエーションできるようにするには、このオプションをオンにします。 **（注）** 少数のレガシー クライアントは PEAPv1 プロトコル規格を確認しません。その結果、EAP カンバセーションは「`Invalid EAP payload`」エラー メッセージでドロップされます。

表 10-7　[Access Service Properties] : [Allowed Protocols] ページ （続き）

オプション	説明
Allow EAP-FAST	EAP-FAST 認証プロトコルと EAP-FAST 設定をイネーブルにします。EAP-FAST プロトコルは、同じサーバ上の複数の内部プロトコルをサポートできます。デフォルトの内部方式は、MSCHAPv2 です。 [Allow EAP-FAST] をオンにすると、EAP-FAST 内部方式を設定できます。 • Allow EAP-MSCHAPv2 – [Allow Password Change] : ACS で EAP-FAST のフェーズ 0 とフェーズ 2 でのパスワード変更をサポートする場合にオンにします。 – [Retry Attempts] : ACS でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ～ 3 です。 • Allow EAP-GTC – [Allow Password Change] : ACS で EAP-FAST のフェーズ 0 とフェーズ 2 でのパスワード変更をサポートする場合にオンにします。 – [Retry Attempts] : ACS でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ～ 3 です。 • [Allow TLS-Renegotiation] : ACS で TLS 再ネゴシエーションをサポートする場合にオンにします。このオプションでは、エンドユーザ クライアントと ACS の間で匿名の TLS ハンドシェイクが可能になります。EAP-MS-CHAP は、フェーズ 0 の内部方式としてのみ使用されます。 • [Use PACs] : EAP-FAST クライアントに認可 PAC をプロビジョニングするように ACS を設定する場合に選択します。追加の「PAC オプション」が表示されます。 • [Don’t use PACs] : トンネルまたはマシン PAC を発行したり受け入れたりしないで EAP-FAST を使用するように ACS を設定する場合に選択します。PAC のすべての要求は無視され、ACS は PAC を含まない Success-TLV で応答します。 このオプションを選択すると、マシン認証を実行するように ACS を設定できます。

表 10-7　[Access Service Properties] : [Allowed Protocols] ページ （続き）

オプション	説明
Allow EAP-FAST（続き）	**PAC オプション** • [Tunnel PAC Time To Live] : 存続可能時間（TTL）の値によって PAC のライフタイムが制限されます。ライフタイム値と単位を指定します。デフォルトは 1 日です。 • [Proactive PAC Update When]: <*n%*> of PAC TTL is Left : Update 値により、クライアントに有効な PAC が保持されます。ACS は、最初に認証が成功してから TTL によって設定された有効期限までに更新を開始します。Update 値は、TTL の残り時間のパーセンテージです （デフォルト：10%）。 • [Allow Anonymous In-band PAC Provisioning] : ACS でクライアントとのセキュアな匿名 TLS ハンドシェイクを確立し、クライアントにいわゆる PAC をプロビジョニングする場合にオンにします。その際、EAP-FAST のフェーズ 0 と EAP-MSCHAPv2 が使用されます。 **（注）** 匿名 PAC プロビジョニングをイネーブルにするには、内部方式として EAP-MSCHAPv2 と EAP-GTC の両方を選択する必要があります。 • [Allow Authenticated In-band PAC Provisioning] : ACS は Secure Socket Layer（SSL）サーバ側の認証を使用して、EAP-FAST のフェーズ 0 中にクライアントに PAC をプロビジョニングします。このオプションは匿名プロビジョニングよりもセキュアですが、サーバ証明書および信頼できるルート CA が ACS にインストールされている必要があります。 このオプションをオンにすると、認証された PAC プロビジョニングの成功後に Access-Accept メッセージをクライアントに返すように ACS を設定できます。 • [Allow Machine Authentication] : ACS でエンドユーザ クライアントにマシン PAC をプロビジョニングし、（マシン クレデンシャルを持たないエンドユーザ クライアントに対して）マシン認証を実行する場合にオンにします。 マシン PAC は、要求（インバンド）によって、または管理者（アウトオブバンド）によって、クライアントにプロビジョニングできます。ACS がエンドユーザ クライアントから有効なマシン PAC を受信すると、その PAC からマシン ID の詳細が抽出され、ACS 外部 ID ストアで確認されます。その詳細が正しいことが確認されると、その後の認証は実行されません。 **（注）** ACS 5.4 では、マシン認証の外部 ID ストアとして Active Directory だけがサポートされます。 このオプションをオンにすると、マシン PAC を使用するために受け入れることができる期間の値を入力できます。ACS は、期限切れのマシン PAC を受け取ると、（エンドユーザ クライアントからの新規マシン PAC 要求を待たずに）エンドユーザ クライアントに新規マシン PAC を自動的に再プロビジョニングします。 • [Enable Stateless Session Resume] : ACS で EAP-FAST クライアントに認可 PAC をプロビジョニングし、常に EAP-FAST のフェーズ 2 を実行する場合にオンにします（デフォルトはオン）。 次の場合は、このオプションをオフにします。 – ACS が EAP-FAST クライアントに認可 PAC をプロビジョニングしないようにする場合 – EAP-FAST のフェーズ 2 を常に実行する場合 このオプションをオンにすると、ユーザ認可 PAC の認可期間を入力できます。この期間の終了後、PAC は期限切れになります。ACS は期限切れの認可 PAC を受信すると、EAP-FAST 認証のフェーズ 2 を実行します。

表 10-7　[Access Service Properties] : [Allowed Protocols] ページ （続き）

オプション	説明
Preferred EAP protocol	使用可能な次のオプションから、優先させる EAP プロトコルを選択します。 • EAP-FAST • PEAP • LEAP • EAP-TLS • EAP-MD5 このオプションでは、特定のプロトコルが実装されていない場合に、No-Acknowledgement を送信する機能を持たない古いサプリカント（エンド デバイス）と連携するよう、ACS に柔軟性を持たせることができます。このオプションを使用して、デバイスとネゴシエーションしているプロトコルのリストの先頭に特定のプロトコルを配置し、ネゴシエーションを成功させることができます。

ステップ 3　[Finish] をクリックして、アクセス サービスの変更を保存します。

アクセス サービスをイネーブルにするには、サービス セレクション ポリシーに追加する必要があります。

アクセス サービス テンプレートの設定

サービス テンプレートを使用して、特定の条件タイプを使用するようにカスタマイズされたポリシーを含むアクセス サービスを定義します。

ステップ 1　「アクセス サービスの一般プロパティの設定」（P.10-13）で、[Based on service template] を選択し、[Select] をクリックします。

ステップ 2　表 10-8 の説明に従って、フィールドに入力します。

表 10-8　アクセス サービス テンプレート

テンプレート名	アクセス サービス タイプ	プロトコル	ポリシー	状態	結果
Device Admin - Simple	デバイス管理	PAP/ASCII	ID	None - Simple	内部ユーザ
			認可	Identity group、NDG:Location、NDG:Device Type、Time and Date	シェル プロファイル
Device Admin - Command Auth	デバイス管理	PAP/ASCII	ID	None - Simple	内部ユーザ
			認可	Identity group、NDG:Location、NDG: Time and Date	コマンド セット
Network Access - Simple	ネットワーク アクセス	PEAP、EAP-FAST	ID	None - Simple	内部ユーザ
			認可	NDG:Location、Time and date	認可プロファイル
Network Access - MAC Authentication Bypass	ネットワーク アクセス	Process Host Lookup、PAP/ASCII（Detect PAP as Host Lookup）、EAP-MD5（Detect EAP-MD5 as Host Lookup）	ID	None - Simple	内部ユーザ
			認可	Use case	認可プロファイル

アクセス サービスの削除

アクセス サービスを削除するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] を選択します。

[Access Services] ページが表示され、設定されているサービスのリストが示されます。

ステップ 2　削除するアクセス サービスの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックし、確認メッセージの [OK] をクリックします。

[Access Policies] ページが表示されます。このとき、削除したアクセス サービスは表示されません。

関連項目

- 「アクセス サービスの作成、複製、および編集」（P.10-12）

アクセス サービス ポリシーの設定

アクセス サービスの作成後、アクセス サービス ポリシーを設定します。

- 「ID ポリシーの表示」（P.10-22）
- 「ID ポリシー規則のプロパティの設定」（P.10-25）
- 「グループ マッピング ポリシーの設定」（P.10-26）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「デバイス管理のシェル/コマンド認可ポリシーの設定」（P.10-35）

すべての着信要求に同じアクセス サービスを適用する単純なポリシーを設定するか、またはルール ベースのポリシーを作成できます。

（注）　単純なポリシーを作成および保存してからルール ベースのポリシーに変更すると、単純なポリシーはルール ベースのポリシーのデフォルト規則になります。ルール ベースのポリシーを保存してから単純なポリシーに変更すると、デフォルト規則以外の規則はすべて失われます。デフォルト規則は、ACS によって自動的に単純なポリシーとして使用されます。

ポリシー規則の設定を開始する前に、次の操作を行う必要があります。

- ポリシー条件および結果を設定します。「ポリシー条件の管理」（P.9-1）を参照してください。
- ポリシー規則によって適用される条件および結果のタイプを選択します。「ポリシーのカスタマイズ」（P.10-4）を参照してください。

ポリシー規則の設定の詳細については、次を参照してください。

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

ID ポリシーの表示

アクセス サービスの ID ポリシーでは、ACS で認証と属性の取得に使用する ID ソースを定義します。ACS は、取得した属性をその後のポリシーで使用できます。

次の ID ソースがあります。

- パスワードベースの認証の ID ソースは、単一の ID ストアまたは ID ストア順序にすることができます。
- 証明書ベースの認証の ID ソースは、証明書認証プロファイルまたは ID ストア順序にすることができます。

ID ストア順序は、認証に使用される順序および属性を取得する任意の追加順序を定義します。「ID ストア順序の設定」（P.8-75）を参照してください。

ID ポリシーを含むアクセス サービスを作成した場合は、このポリシーを設定および変更できます。すべての要求の認証に同じ ID ソースを適用する単純なポリシー、またはルール ベースの ID ポリシーを設定できます。

ルール ベースのポリシーでは、各規則に 1 つ以上の条件、および認証に使用される ID ソースである結果が含まれます。ID ポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。

注意　単純なポリシー ページとルール ベースのポリシー ページを切り替えると、以前に保存したポリシーは失われます。

単純な ID ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] > *service* > [Identity] を選択します。*service* は、アクセス サービスの名前です。

デフォルトでは、表 10-9 で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。

表 10-9　[Simple Identity Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple]：結果がすべての要求に適用されることを指定します。 • [Rule-based]：要求に応じて異なる結果が適用されるように規則を設定します。 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Identity Source	すべての要求に適用する ID ソース。デフォルトは [Deny Access] です。手順は次のとおりです。 • パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。 • 証明書ベースの認証の場合、証明書認証プロファイルまたは ID ストア順序を選択します。 ID ストア順序は、認証に使用される順序および属性を取得する任意の追加順序を定義します。「ID ストア順序の設定」（P.8-75）を参照してください。
Advanced options	次のオプションについて、要求を拒否またはドロップするか、認証を続行するかを指定します。 • [If authentication failed]：デフォルトは拒否です。 • [If user not found]：デフォルトは拒否です。 • [If process failed]：デフォルトはドロップです。 基になるプロトコルの制限により、ACS では、[Continue] オプションが選択された場合でも処理を続行できない場合があります。PAP/ASCII、EAP-TLS、または Host Lookup の場合、認証に失敗しても ACS は処理を続行できます。 その他のすべての認証プロトコルの場合、[Continue] オプションを選択しても要求はドロップされます。

ステップ 2　認証用の ID ソースを選択するか、または [Deny Access] を選択します。

その他の高度なオプションを設定できます。「ID ポリシー規則のプロパティの設定」（P.10-25）を参照してください。

ステップ 3　[Save Changes] を選択して、ポリシーを保存します。

ルール ベースの ID ポリシーの表示

[Access Policies] > [Access Services] > *service* > [Identity] を選択します。*service* は、アクセス サービスの名前です。

デフォルトでは、表 10-9 で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。設定されている場合は、表 10-10 で説明されているフィールドを含む [Rules-Based Identity Policy] ページが表示されます。

表 10-10　[Rule-based Identity Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple]：結果がすべての要求に適用されることを指定します。 • [Rule-based]：要求に応じて異なる結果が適用されるように規則を設定します。 **注意**　ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Status	規則の現在のステータス。規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	ポリシーの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。
Results	規則の評価結果として認証に使用される ID ソース。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

ルール ベースのポリシーを設定するには、次の項を参照してください。

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

ホスト ルックアップ要求用の ID ポリシー設定の詳細については、「ホスト ルックアップ要求用の認可ポリシーの設定」（P.4-21）を参照してください。

関連トピック

- 「グループ マッピング ポリシーの設定」（P.10-26）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「デバイス管理のシェル/コマンド認可ポリシーの設定」（P.10-35）

ID ポリシー規則のプロパティの設定

ID ポリシー規則を作成、複製、または編集して、クライアントの認証に使用する ID データベースを決定したり、クライアントの属性を取得したりできます。

このページを表示するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] > ***service*** > [Identity] を選択し、次のいずれかを実行します。

- [Create] をクリックします。
- 規則チェックボックスをオンにし、[Duplicate] をクリックします。
- 規則名をクリックするか規則チェックボックスをオンにし、[Edit] をクリックします。

ステップ 2　表 10-11 の説明に従って、[Identity Rule Properties] ページのフィールドに入力します。

表 10-11　[Identity Rule Properties] ページ

オプション	説明
General	
Rule Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Rule Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[*ANY*] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。
Results	
Identity Source	要求に適用する ID ソース。デフォルトは [Deny Access] です。手順は次のとおりです。 • パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。 • 証明書ベースの認証の場合、証明書認証プロファイルまたは ID ストア順序を選択します。 ID ストア順序は、認証に使用される順序および追加属性を取得する任意の順序を定義します。「ID ストア順序の設定」（P.8-75）を参照してください。
Advanced options	次のオプションについて、要求を拒否またはドロップするか、認証を続行するかを指定します。 • [If authentication failed]：デフォルトは拒否です。 • [If user not found]：デフォルトは拒否です。 • [If process failed]：デフォルトはドロップです。 基になるプロトコルの制限により、ACS では、[Continue] オプションが選択された場合でも処理を続行できない場合があります。PAP/ASCII、EAP-TLS、または Host Lookup の場合、認証に失敗しても ACS は処理を続行できます。 その他のすべての認証プロトコルの場合、[Continue] オプションを選択しても、要求はドロップされます。

グループ マッピング ポリシーの設定

外部 ID ストアから取得したグループと属性を ACS ID グループにマッピングするグループ マッピング ポリシーを設定します。ACS によってユーザまたはホストの要求が処理されるときに、このポリシーによって認可ポリシー規則で使用できる関連 ID グループが取得されます。

グループ マッピング ポリシーを含むアクセス サービスを作成した場合は、このポリシーを設定および変更できます。すべての要求に同じ ID グループを適用する単純なポリシー、またはルール ベースのポリシーを設定できます。

ルール ベースのポリシーでは、各規則に 1 つ以上の条件と結果が含まれます。条件は、外部属性ストアから取得された属性またはグループだけに基づくことができます。結果は、ID グループ階層内の ID グループです。ポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。

注意　単純なポリシー ページとルール ベースのポリシー ページを切り替えると、以前に保存したポリシーは失われます。

単純なグループ マッピング ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Access Services] > *service* > [Group Mapping] を選択します。*service* は、アクセス サービスの名前です。

デフォルトでは、[Simple Group Mapping Policy] ページが表示されます。フィールドの説明については、表 10-12 を参照してください。

[Rule-Based Group Mapping Policy] ページのフィールドの説明については、表 10-13 を参照してください。

表 10-12　[Simple Group Mapping Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple]：結果がすべての要求に適用されることを指定します。 • [Rule-based]：要求に応じて異なる結果が適用されるように規則を設定します。 **注意**　ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Identity Group	すべての要求の属性とグループをマッピングする ID グループ。

表 10-13　[Rule-based Group Mapping Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple]：結果がすべての要求に適用されることを指定します。 • [Rule-based]：要求に応じて異なる結果が適用されるように規則を設定します。 **注意**　ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Status	規則の現在のステータス。規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	ポリシーの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。
Results	規則の評価結果として使用される ID グループ。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

ステップ 2　ID グループを選択します。

ステップ 3　[Save Changes] を選択して、ポリシーを保存します。

ルール ベースのポリシーを設定するには、次の項を参照してください。

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）

- 「ポリシー規則の削除」（P.10-40）

関連トピック

- 「ID ポリシーの表示」（P.10-22）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「デバイス管理のシェル/コマンド認可ポリシーの設定」（P.10-35）

グループ マッピング ポリシー規則のプロパティの設定

このページは、外部データベースから取得された属性とグループの ACS ID グループへのマッピングを定義するグループ マッピング ポリシー規則を作成、複製、または編集する場合に使用します。

ステップ 1　[Access Policies] > [Access Services] > ***service*** > [Group Mapping] を選択し、次のいずれかを実行します。

- [Create] をクリックします。
- 規則チェックボックスをオンにし、[Duplicate] をクリックします。
- 規則名をクリックするか規則チェックボックスをオンにし、[Edit] をクリックします。

ステップ 2　表 10-14 の説明に従って、フィールドに入力します。

表 10-14　[Group Mapping Rule Properties] ページ

オプション	説明
General	
Rule Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Rule Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。
Results	
Identity Group	要求の属性とグループをマッピングする ID グループ。

ネットワーク アクセスのセッション認可ポリシーの設定

ネットワーク アクセス認可のアクセス サービスを作成すると、セッション認可ポリシーが作成されます。その後、このポリシーに規則を追加し、変更してクライアント セッションのアクセス権を決定できます。

標準の最初に一致する規則テーブルであるスタンドアロン認可ポリシーをアクセス サービスに作成できます。例外ポリシーを含む認可ポリシーを作成することもできます。「認可例外ポリシーの設定」（P.10-36）を参照してください。要求が例外規則に一致すると、ポリシー例外規則の結果が常に適用されます。

規則には、任意の条件と複数の結果を含めることができます。

- 認可プロファイル：ユーザ定義属性を定義し、任意で、Access-Accept メッセージによって返されるダウンロード可能 ACL を定義します。
- セキュリティ グループ タグ (SGT)：Cisco Security Group Access をインストールした場合、要求に適用する SGT を認可規則で定義できます。

ACS が複数の認可プロファイルを含む規則を処理する方法の詳細については、「複数の認可プロファイルを含む規則の処理」（P.3-17）を参照してください。

認可ポリシーを設定するには、次の項を参照してください。

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

認可ポリシーの作成については、次を参照してください。

- ホスト ルックアップ要求については、「ACS と Cisco Security Group Access」（P.4-24）を参照してください。
- Security Group Access のサポートについては、「エンドポイント アドミッション コントロール ポリシーの作成」（P.4-28）を参照してください。

ステップ 1　[Access Policies] > [Access Services] > ***service*** > [Authorization] を選択します。

ステップ 2　表 10-15 の説明に従って、フィールドに入力します。

表 10-15　[Network Access Authorization Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	
Identity Group	マッチング対象の内部 ID グループの名前。
NDG:*name*	ネットワーク デバイス グループ。2 つの事前定義済みの NDG は、Location および Device Type です。
conditions	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	
Authorization Profile	対応する規則が一致したときに適用される認可プロファイルを表示します。 Security Group Access 機能をイネーブルにすると、規則の結果をカスタマイズできます。規則では、エンドポイントのアクセス権限、そのエンドポイントのセキュリティ グループ、またはその両方を決定できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。 Security Group Access 機能をイネーブルにすると、規則の結果セットを選択することもできます（セッション認可プロファイルのみ、セキュリティ グループのみ、または両方）。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

ネットワーク アクセス認可規則のプロパティの設定

このページは、ネットワーク アクセス サービスのアクセス権を決定する規則を作成、複製、および編集する場合に使用します。

ステップ 1　[Access Policies] > [Access Services] > <***service***> > [Authorization] を選択し、[Create]、[Edit]、または [Duplicate] をクリックします。

ステップ 2　表 10-16 の説明に従って、フィールドに入力します。

表 10-16　[Network Access Authorization Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。
Results	
Authorization Profiles	使用可能なプロファイルと選択されたプロファイルのリスト。要求に適用する複数の認可ポリシーを選択できます。矛盾を解決する場合の認可ポリシー順序の重要性については、「複数の認可プロファイルを含む規則の処理」（P.3-17）を参照してください。
Security Group	（Security Group Access のみ）適用するセキュリティ グループ。 Security Group Access をイネーブルにすると、セッション認可プロファイルのみ、セキュリティ グループのみ、または両方を表示するように結果オプションをカスタマイズできます。

デバイス管理認可ポリシーの設定

デバイス管理認可ポリシーは、ネットワーク管理者の認可と権限を決定します。

認可ポリシーは、アクセス サービスの作成中に作成します。[Access Service Create] ページの詳細については、「アクセス サービスの一般プロパティの設定」（P.10-13）を参照してください。

このページを使用して、次のことを行います。

- 規則を表示します。
- 規則を削除します。
- 規則を作成、複製、編集、およびカスタマイズできるページを開きます。

[Access Policies] > [Access Services] > ***service*** > [Authorization] を選択します。

表 10-17 で説明されている [Device Administration Authorization Policy] ページが表示されます。

表 10-17　[Device Administration Authorization Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用されるシェル プロファイルとコマンド セットを表示します。 規則の結果をカスタマイズできます。規則によって、シェル プロファイル、コマンド セット、またはその両方を適用できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件および結果のタイプを選択する [Customize] ページを開きます。[Conditions] および [Results] カラムには、カスタマイゼーション設定が反映されます。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

デバイス管理認可規則のプロパティの設定

このページは、デバイス管理アクセス サービスの認可および権限を決定する規則を作成、複製、および編集する場合に使用します。

[Access Policies] > [Access Services] > ***service*** > [Authorization] を選択し、[Create]、[Edit]、または [Duplicate] をクリックします。

表 10-18 で説明されている [Device Administration Authorization Rule Properties] ページが表示されます。

表 10-18　[Device Administration Authorization Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。
Results	
Shell Profiles	ルールに適用するシェル プロファイル。
Command Sets	使用可能なコマンド セットと選択されたコマンド セットのリスト。適用する複数のコマンド セットを選択できます。

デバイス管理認可例外ポリシーの設定

定義済み認可ポリシーのデバイス管理認可例外ポリシーを作成できます。例外規則の結果は、常に認可ポリシー規則よりも優先されます。

このページを使用して、次のことを行います。

- 例外規則を表示します。
- 例外規則を削除します。
- 例外規則を作成、複製、編集、およびカスタマイズするページを開きます。

[Access Policies] > [Access Services] > ***service*** > [Authorization] を選択し、[Device Administration Authorization Exception Policy] をクリックします。

表 10-19 で説明されている [Device Administration Authorization Exception Policy] ページが表示されます。

表 10-19　[Device Administration Authorization Exception Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	
Identity Group	マッチング対象の内部 ID グループの名前。
NDG:*name*	ネットワーク デバイス グループ。2 つの事前定義済みの NDG は、Location および Device Type です。
Condition	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用されるシェル プロファイルとコマンド セットを表示します。 規則の結果をカスタマイズできます。規則によって、シェル プロファイル、コマンド セット、またはその両方を決定できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。対応する認可ポリシーと同じ条件および結果のセットを使用する必要はありません。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

デバイス管理のシェル/コマンド認可ポリシーの設定

アクセス サービスを作成してデバイス管理のサービス ポリシー構造を選択すると、ACS によって自動的にシェル/コマンド認可ポリシーが作成されます。その後、ポリシー規則を作成および変更できます。

Web インターフェイスでは、デバイス管理の複数のコマンド セットを作成する機能がサポートされています。この機能を使用すると、保持する基本コマンド セットの数を少なくすることができます。すべての組み合わせを個々のコマンド セットで保持するのではなく、規則の結果としてコマンド セットを組み合わせて選択できます。

例外ポリシーを含む認可ポリシーを作成して、標準のポリシー結果よりも優先させることもできます。「認可例外ポリシーの設定」（P.10-36）を参照してください。

ACS が複数のコマンド セットを含む規則を処理する方法の詳細については、「複数のコマンド セットを持つ規則の処理」（P.3-11）を参照してください。

規則を設定するには、次の項を参照してください。

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

認可例外ポリシーの設定

認可ポリシーには例外ポリシーを含めることができます。一般に、例外は一時ポリシーです。たとえば、ビジターに一時的なアクセス権を付与したり、特定のユーザに対してアクセス レベルを上げたりします。例外ポリシーは、変化する状況やイベントに効率的に対応するために使用します。

例外規則の結果は、常に標準の認可ポリシー規則よりも優先されます。

例外ポリシーは、メインの認可ポリシー テーブルとは別の規則テーブルに作成します。対応する標準の認可ポリシーで使用されているのと同じポリシー条件を例外ポリシーで使用する必要はありません。

例外ポリシー規則のページにアクセスするには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] > *service* > *authorization policy* を選択します。*service* はアクセス サービスの名前、*authorization policy* はセッション認可またはシェル / コマンド セット認可ポリシーです。

ステップ 2　ルール ベースのポリシー ページで、規則テーブルの上にある [Exception Policy] リンクをクリックします。

表 10-20 で説明されているフィールドを含む [Exception Policy] テーブルが表示されます。

表 10-20　[Network Access Authorization Exception Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	
Identity Group	マッチング対象の内部 ID グループの名前。
NDG:*name*	ネットワーク デバイス グループ。2 つの事前定義済みの NDG は、Location および Device Type です。
Condition Name	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用される認可プロファイルを表示します。 Security Group Access 機能をイネーブルにすると、規則の結果をカスタマイズできます。規則では、エンドポイントのアクセス権限、そのエンドポイントのセキュリティ グループ、またはその両方を決定できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。対応する認可ポリシーと同じ条件のセットを使用する必要はありません。 Security Group Access 機能をイネーブルにすると、規則の結果セットを選択することもできます（セッション認可プロファイルのみ、セキュリティ グループのみ、または両方）。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

規則を設定するには、次の項を参照してください。

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

関連トピック

- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「デバイス管理のシェル/コマンド認可ポリシーの設定」（P.10-35）

ポリシー規則の作成

規則を作成するときは、規則の順序が重要であることに注意してください。ACS ネットワークにアクセスしようとするクライアントの要求が ACS によって処理されるときに一致が見つかると、その後の処理はすべて停止され、その一致に関連する結果が検索されます。一致が見つかったあとは、それ以降の規則は考慮されません。

一致する規則がないか、または規則が定義されていない場合は、デフォルト規則によってデフォルトのポリシーが指定されます。デフォルト規則の結果は編集できます。

はじめる前に

- ポリシー条件および結果を設定します。「ポリシー条件の管理」（P.9-1）を参照してください。
- ポリシー規則によって適用される条件および結果のタイプを選択します。「ポリシーのカスタマイズ」（P.10-4）を参照してください。

新規のポリシー規則を作成するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。*service* はアクセス サービスの名前、*policy* はポリシーのタイプです。次の場合があります。

- ルール ベースのポリシーを前に作成したことがある場合は、設定されている規則のリストを含むルール ベースのポリシー ページが表示されます。
- ルール ベースのポリシーを作成したことがない場合は、単純なポリシー ページが表示されます。[Rule-Based] をクリックします。

ステップ 2　[Rule-Based Policy] ページで、[Create] をクリックします。

[Rule] ページが表示されます。

ステップ 3　規則を定義します。

ステップ 4　[OK] をクリックします。

新しい規則を示す [Policy] ページが表示されます。

ステップ 5　[Save Changes] をクリックして、新規の規則を保存します。

アクセス サービスによって処理されるすべての要求に同じ結果を使用する単純なポリシーを設定するには、次を参照してください。

- 「ID ポリシーの表示」（P.10-22）
- 「グループ マッピング ポリシーの設定」（P.10-26）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-30）
- 「デバイス管理のシェル/コマンド認可ポリシーの設定」（P.10-35）

関連トピック

- 「規則の複製」（P.10-39）

- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

規則の複製

既存の規則と同じか、または既存の規則によく似た新規の規則を作成する場合は、規則を複製できます。複製された規則名では、元の規則に複製を示すカッコが付けられます。たとえば、Rule-1(1) です。

複製の完了後は、各規則（元の規則および複製された規則）に個別にアクセスします。

（注）　デフォルト規則は複製できません。

規則を複製するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。*service* はアクセス サービスの名前、*policy* はポリシーのタイプです。

設定されている規則のリストを含む [Policy] ページが表示されます。

ステップ 2　複製する規則の隣にあるチェックボックスをオンにします。デフォルト規則は複製できません。

ステップ 3　[Duplicate] をクリックします。

[Rule] ページが表示されます。

ステップ 4　規則の名前を変更し、他の該当するフィールド オプションに入力します。

ステップ 5　[OK] をクリックします。

新しい規則を示す [Policy] ページが表示されます。

ステップ 6　[Save Changes] をクリックして、新規の規則を保存します。

ステップ 7　重複する規則をキャンセルするには、[Discard Changes] をクリックします。

関連トピック

- 「ポリシー規則の作成」（P.10-38）
- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

ポリシー規則の編集

ポリシー規則のすべての値を編集できます。また、デフォルト規則の結果を編集することもできます。

規則を編集するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。*service* はアクセス サービスの名前、*policy* はポリシーのタイプです。

設定されている規則のリストを含む [Policy] ページが表示されます。

ステップ 2　変更する規則名をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

[Rule] ページが表示されます。

ステップ 3　適切な値を編集します。

ステップ 4　[OK] をクリックします。

編集された規則を示す [Policy] ページが表示されます。

ステップ 5　[Save Changes] をクリックして、新しい設定を保存します。

ステップ 6　編集した情報をキャンセルするには、[Discard Changes] をクリックします。

関連トピック

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

ポリシー規則の削除

（注）　デフォルト規則は削除できません。

ポリシー規則を削除するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Service Selection Policy] > *service* > *policy* を選択します。*service* はアクセス サービスの名前、*policy* はポリシーのタイプです。

設定されている規則のリストを含む [Policy] ページが表示されます。

ステップ 2　削除する規則の隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

[Policy] ページが表示されます。このとき、削除した規則は表示されません。

ステップ 4　[Save Changes] をクリックして、新しい設定を保存します。

ステップ 5　削除された情報を保持するには、[Discard Changes] をクリックします。

関連トピック

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）

複合条件の設定

複合条件は、単純なポリシー条件で許可された属性に基づく条件のセットを定義する場合に使用します。複合条件はポリシー規則ページで定義します。個別の条件オブジェクトとして定義することはできません。

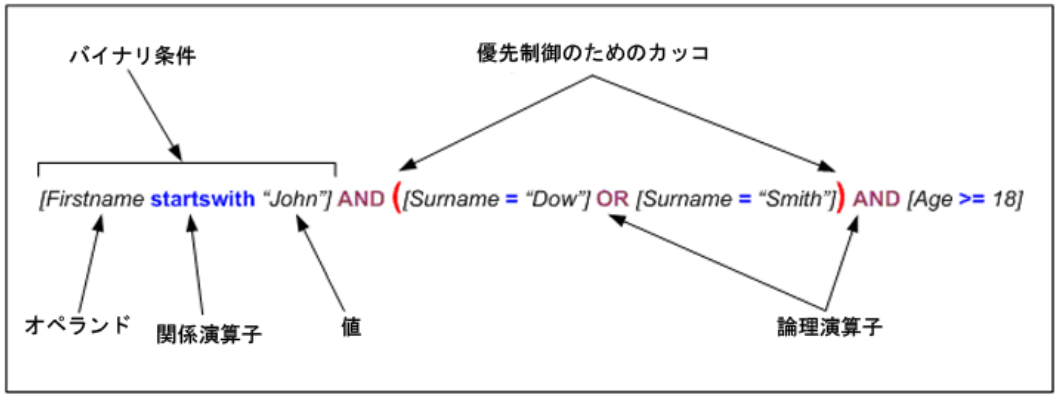
ここでは、次の内容について説明します。

- 「複合条件の構築ブロック」（P.10-41）
- 「複合条件のタイプ」（P.10-42）
- 「複合式ビルダーの使用方法」（P.10-45）

複合条件の構築ブロック

図 10-1 に、複合条件の構築ブロックを示します。

図 10-1　　複合条件の構築ブロック



- **オペランド**：属性または条件のタイプ。プロトコル/要求属性、ID 属性、ID グループ、ネットワーク デバイス グループ（NDG）、日付/時刻、カスタムまたは標準条件など。
- **関係演算子**：オペランドと値の関係を指定する演算子。等号（=）、一致しない、など。条件で使用できる演算子は、オペランドのタイプによって異なります。
- **バイナリ条件**：指定されたオペランドと値の関係を定義します。[username = "Smith"] など。
- **論理演算子**：バイナリ条件、またはバイナリ条件の間に適用されます。サポートされている論理演算子は、AND と OR です。
- **優先制御**：カッコを使用して、論理演算子の優先順位を変更できます。管理者はカッコを入れ子にして優先順位を制御できます。論理演算子の通常の優先順位、つまりカッコを使用しない場合の優先順位は、NOT、AND、OR の順です。NOT の優先順位が最も高く、OR の優先順位が最も低くなります。

表 10-21 に、複合条件の構築中にサポートされる動的属性マッピングの概要を示します。

表 10-21　ポリシーの複合条件でサポートされる動的属性マッピング

オペランド 1	オペランド 2	例
文字列属性	文字列属性	—
整数属性	整数属性	—
列挙型属性	列挙型属性	—
ブール属性	ブール属性	—
IP アドレス属性	IP アドレス属性	—
特別な場合		
階層型属性	文字列属性	NDG：顧客対 「内部ユーザ」文字列属性
文字列属性	階層型属性	—

（注）　動的属性マッピングは、「String Enum」タイプの ExternalGroups 属性および「Date Time Period」タイプの「Time And Date」属性には適用できません。

階層型属性の場合、階層型属性と比較する文字列属性を設定する際に、文字列属性の値は階層型属性名で始まる必要があるため、値には属性名が付きます。

次に例を示します。

- NDG の下で作成された *DeviceGroup* 属性と比較する *UrsAttr* という新しい文字列属性を定義する場合、*UsrAttr* の値は次のように設定する必要があります。

  DeviceGroup: *Value*

- 各内部ユーザ内の階層型属性である *UserIdentityGroup* と文字列属性を比較する場合は、文字列属性を次のように設定する必要があります。

  IdentityGroup:All Groups:"Identity Group Name"

関連トピック

- 「複合条件のタイプ」（P.10-42）
- 「複合式ビルダーの使用方法」（P.10-45）

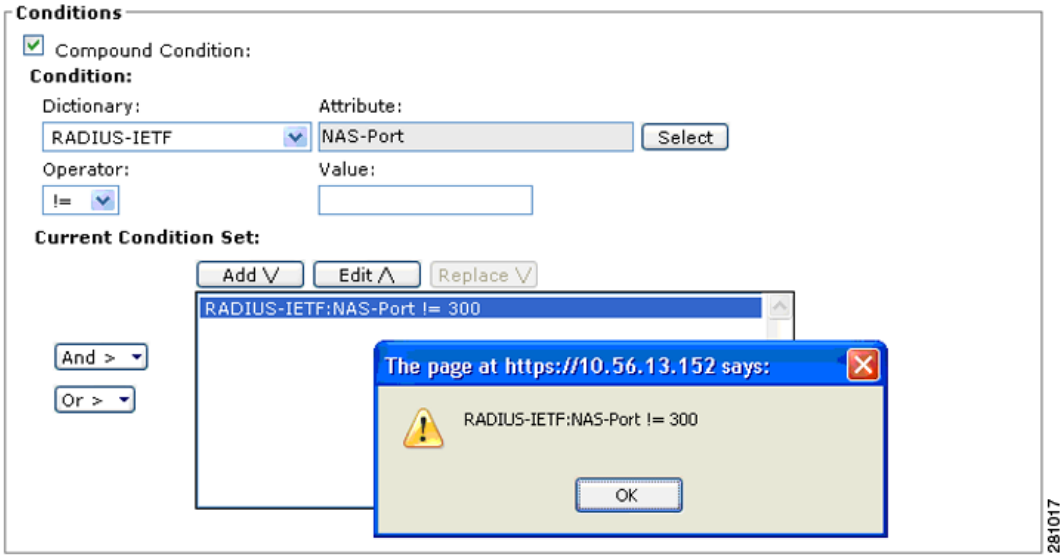
複合条件のタイプ

3 つのタイプの複合条件を作成できます。

アトミック条件

1 つの述語で構成され、リスト内の唯一のエントリです。NDG を除いて、規則テーブル内のすべての単純な条件では、属性と値の間で等号（=）演算が行われると想定されるため、アトミック条件は等号（=）以外の演算子の選択に使用されます。例については、図 10-2 を参照してください。

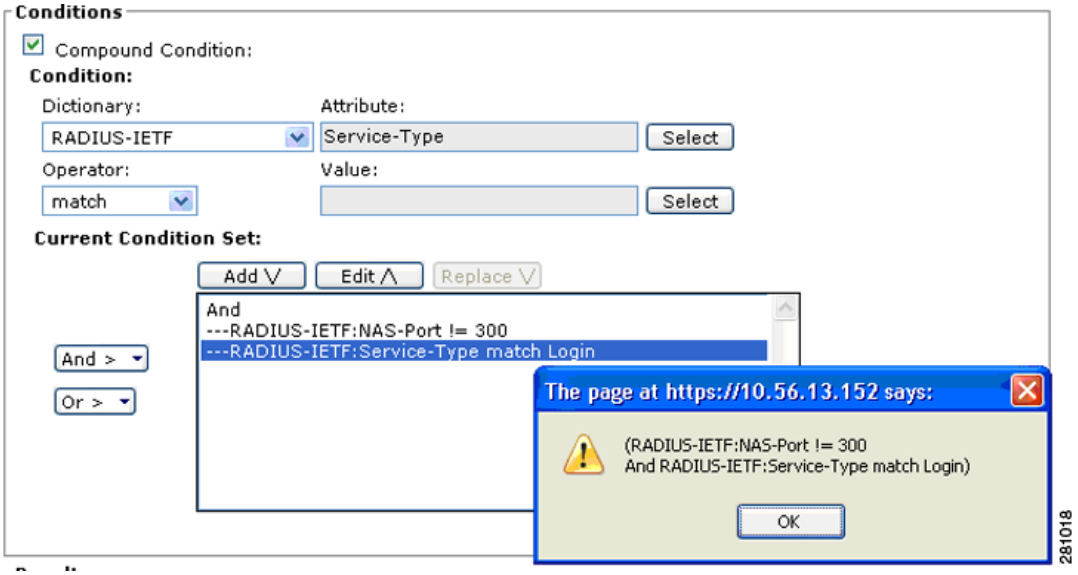
図 10-2　　複合式：アトミック条件



単一の入れ子になった複合条件

単一の演算子とそのあとに続く述語のセット（2 つ以上）で構成されます。演算子は、それぞれの述語の間に適用されます。例については、図 10-3 を参照してください。プレビュー ウィンドウには、論理演算子の優先を示すカッコ [()] が表示されます。

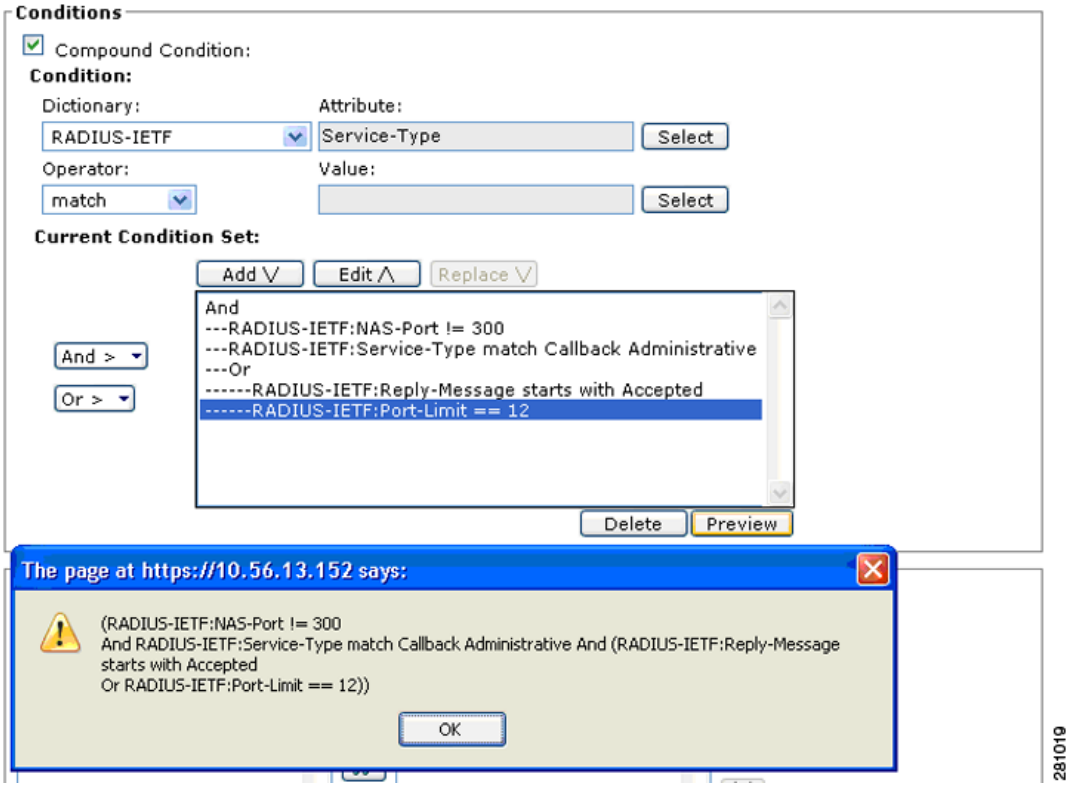
図 10-3　　単一の入れ子になった複合式



複数の入れ子になった複合条件

条件の任意の述語を別の単純な入れ子になった複合条件に置き換えることによって、単一の入れ子になった複合条件を拡張できます。例については、図 10-4 を参照してください。プレビュー ウィンドウには、論理演算子の優先を示すカッコ [()] が表示されます。

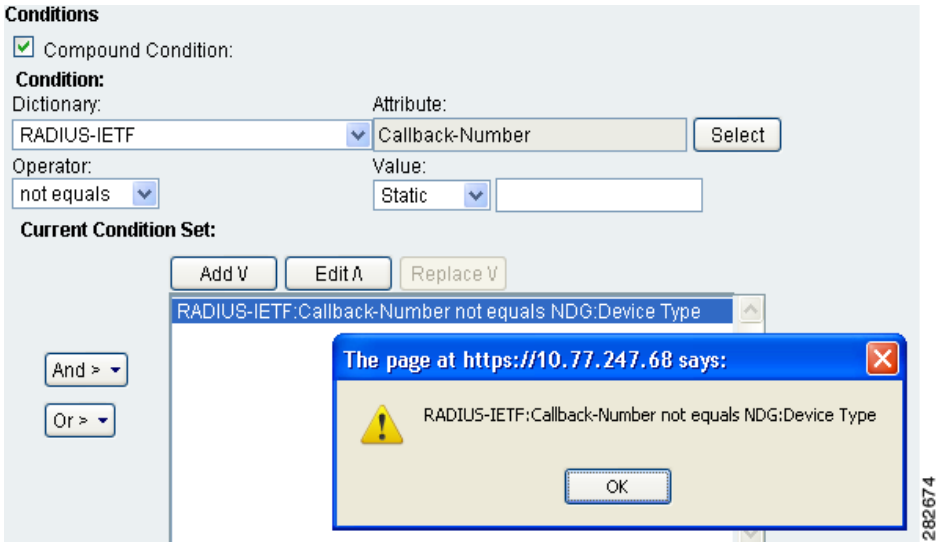
図 10-4　　複数の入れ子になった複合式



動的な値を持つ複合式

オペランドとして選択されたディクショナリ属性と比較する、別のディクショナリ属性を選択するために動的な値を選択できます。例については、図 10-5 を参照してください。

図 10-5　　動的な値を持つ複合式ビルダー



関連トピック

- 「複合条件の構築ブロック」（P.10-41）
- 「複合式ビルダーの使用方法」（P.10-45）

複合式ビルダーの使用方法

複合条件を作成するには、規則のプロパティ ページで式ビルダーを使用します。式ビルダーには 2 つのセクションがあります。プライマリ条件を作成する述語ビルダーと、式を管理するためのコントロールです。

最初のセクションでは、プライマリ条件を定義します。オペランドを定義するディクショナリと属性を選択し、演算子を選択し、条件の値を指定します。2 番めのセクションでは、条件の順序を整理し、バイナリ条件またはバイナリ条件の間に適用される論理演算子を指定します。

表 10-22 に、条件式ビルダーのフィールドを示します。

表 10-22　式ビルダーのフィールド

フィールド	説明
Condition	このセクションでは、プライマリ条件を定義します。
Dictionary	オペランドを取得するディクショナリを指定します。使用できるオプションは、定義するポリシーによって異なります。たとえば、サービス セレクション ポリシーを定義する場合、ID ディクショナリは使用できません。
Attribute	条件のオペランドである属性を指定します。使用できる属性は、選択したディクショナリによって異なります。
Operator	関係演算子の内容は、上記のオペランド フィールドの選択内容に従って動的に決定されます。
Value	条件の値。このフィールドのタイプは、条件または属性のタイプによって異なります。次の 2 つのオプションのいずれかを選択します。 • [Static]：選択した場合、属性タイプに応じて、静的な値を入力または選択する必要があります。 • [Dynamic]：選択した場合、オペランドとして選択されたディクショナリ属性と比較する、別のディクショナリ属性を選択できます。
Current Condition Set	このセクションでは、条件の順序を整理し、バイナリ条件またはバイナリ条件の間に適用する論理演算子を指定します。
Condition list	複合条件の定義済みバイナリ条件および関連付けられている論理演算子のリストが表示されます。
Add	バイナリ条件の定義後、[Add] をクリックして条件を条件リストに追加します。
Edit	バイナリ条件を編集するには、条件リストで条件を選択し、[Edit] をクリックします。[Condition] フィールドに条件のプロパティが表示されます。条件を必要に応じて変更し、[Replace] をクリックします。
Replace	選択した条件を [Condition] フィールドで現在定義されている条件に置き換える場合にクリックします。
And Or	選択した条件に適用する論理演算子、または選択した条件とその上の条件間に適用する論理演算子を指定します。適切な演算子をクリックし、[Insert] をクリックして演算子を別の行として追加します。または、演算子をクリックし、[Replace] をクリックして選択した行を置き換えます。
Delete	選択したバイナリ条件または演算子を条件リストから削除する場合にクリックします。
Preview	現在の式を対応するカッコ表現で表示する場合にクリックします。複合式の作成後、規則テーブルにカッコ表現が表示されます。

関連トピック

- 「複合条件の構築ブロック」（P.10-41）
- 「複合条件のタイプ」（P.10-42）

[Security Group Access Control] ページ

ここでは、次の内容について説明します。

- 「[Egress Policy Matrix] ページ」（P.10-46）
- 「出力ポリシー マトリクスのセルの編集」（P.10-47）
- 「出力ポリシーのデフォルト ポリシーを定義するためのページ」（P.10-47）
- 「NDAC ポリシー ページ」（P.10-48）
- 「[NDAC Policy Properties] ページ」（P.10-49）
- 「[Network Device Access EAP-FAST Settings] ページ」（P.10-51）

[Egress Policy Matrix] ページ

出力ポリシーは SGACL ポリシーとも呼ばれ、送信元および宛先 SGT に基づいてネットワークの出力ポイントで適用する SGACL を決定します。ACS は、出力ポリシーをマトリクスとして表します。送信元および宛先の軸にすべてのセキュリティ グループを表示します。マトリクス内の各セルには、対応する送信元および宛先 SGT に適用する ACL のセットを含めることができます。

ネットワーク デバイスによって、セルに定義した特定のポリシーにデフォルト ポリシーが追加されます。空のセルの場合、デフォルト ポリシーだけが適用されます。

出力ポリシーのマトリクスを使用して、対応する送信元および宛先 SGT に適用する ACL のセットを表示、定義、および編集します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択します。

表 10-23　[Egress Policy Matrix] ページ

オプション	説明
Destination Security Group	すべての宛先セキュリティ グループが表示されるカラムの見出し。
Source Security Group	すべての送信元セキュリティ グループが表示される行の見出し。
Cells	対応する送信元および宛先セキュリティ グループに適用する SGACL を含めます。
Edit	セルをクリックしてから [Edit] をクリックして、そのセルの [Edit] ダイアログボックスを開きます。「出力ポリシー マトリクスのセルの編集」（P.10-47）を参照してください。
Default Policy	デフォルトの出力ポリシーを定義するためのダイアログボックスを開く場合にクリックします。「出力ポリシーのデフォルト ポリシーを定義するためのページ」（P.10-47）を参照してください。
Set Matrix View	出力ポリシーのマトリクス表示を変更するには、オプションを選択し、[Go] をクリックします。 • [All]：出力ポリシー マトリクスのすべての行とカラムを消去します。 • [Customize View]：選択したセルに対応する送信元および宛先セキュリティ グループをカスタマイズできるウィンドウを開きます。

関連項目

- 「出力ポリシーの作成」（P.4-28）

出力ポリシー マトリクスのセルの編集

このページは、選択したセルのポリシーを設定する場合に使用します。対応する送信元および宛先セキュリティ グループに適用する SGACL を設定できます。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択し、セルを選択してから [Edit] をクリックします。

表 10-24　[Edit Cell] ページ

オプション	説明
Configure Security Groups	*表示のみ。*選択したセルの送信元および宛先セキュリティ グループ名が表示されます。
General	セルのポリシーの説明。
ACL	対応する送信元および宛先セキュリティ グループに適用する SGACL を、[Available] リストから [Selected] リストに移動します。SGACL のリストの順序を指定するには、上向き（^）および下向き（v）矢印を使用します。

関連項目

- 「出力ポリシーの作成」（P.4-28）

出力ポリシーのデフォルト ポリシーを定義するためのページ

このページは、デフォルトの出力ポリシーを定義する場合に使用します。ネットワーク デバイスによって、セルに定義されている特定のポリシーにデフォルト ポリシーが追加されます。空のセルの場合、デフォルト ポリシーだけが適用されます。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択し、[Default Policy] をクリックします。

表 10-25　[Default Policy] ページ

オプション	説明
ACL	対応する送信元および宛先セキュリティ グループに適用する SGACL を、[Available] リストから [Selected] リストに移動します。SGACL のリストの順序を指定するには、上向き（^）および下向き（v）矢印を使用します。 最終的な catch-all 規則として [Permit All] または [Deny All] を選択します。

関連トピック

- 「出力ポリシーの作成」（P.4-28）
- 「デフォルト ポリシーの作成」（P.4-29）

NDAC ポリシー ページ

ネットワーク デバイス アドミッション コントロール（NDAC）ポリシーは Security Group Access 環境のネットワーク デバイスの SGT を決定します。NDAC ポリシーは次の要求を処理します。

- あるデバイスからのネイバーに関するピア認可要求。
- 環境要求（デバイスはそのデバイス自体に関する情報を収集します）。

要求のタイプにかかわらず、特定のデバイスについては同じ SGT がポリシーによって返されます。

（注）　NDAC ポリシーはデフォルトで実装されるため、アクセス サービスに追加しないでください。ただし、エンドポイント アドミッション コントロールの場合、アクセス サービスとセッション認可ポリシーを定義する必要があります。セッション認可ポリシーの作成については、「ネットワーク アクセス認可規則のプロパティの設定」（P.10-32）を参照してください。

このページは、すべてのデバイスに同じセキュリティ グループを割り当てる単純なポリシーを設定するか、またはルール ベースのポリシーを設定する場合に使用します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Network Device Access] > [Authentication Policy] を選択します。

すでに NDAC ポリシーが設定されている場合は、対応する単純なポリシー ページまたはルール ベースのポリシー ページが開きます。設定されていない場合は、デフォルトで単純なポリシー ページが開きます。

単純なポリシー ページ

このページは、単純な NDAC ポリシーを定義する場合に使用します。

表 10-26　[Simple NDAC Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple]：結果がすべての要求に適用されることを指定します。 • [Rule-based]：要求に応じて異なる結果が適用されるように規則を設定します。 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Security Group	デバイスに割り当てるセキュリティ グループを選択します。デフォルトは [Unknown] です。

ルール ベースのポリシー ページ

ルール ベースのポリシーに関するこのページを使用して、次のことを行います。

- 規則を表示します。
- 規則を削除します。
- 規則を作成、複製、編集、およびカスタマイズするページを開きます。

表 10-27　[Rule-Based NDAC Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple]：結果がすべての要求に適用されることを指定します。 • [Rule-based]：要求に応じて異なる結果が適用されるように規則を設定します。 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。デフォルト規則は次の場合に条件に使用できます。 • イネーブルな規則が一致しない。 • 規則が定義されていない。 規則を編集または複製するには、リンクをクリックします。 デフォルト規則は編集できますが、削除、ディセーブル、または複製することはできません。
Conditions	ポリシー規則の定義に使用できる条件。規則の条件の表示を変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する条件に一致した場合にデバイスに割り当てられるセキュリティ グループが表示されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。対応する認可ポリシーと同じ条件のセットを使用する必要はありません。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

関連トピック：

- 「NDAC ポリシーの設定」（P.4-26）
- 「[NDAC Policy Properties] ページ」（P.10-49）

[NDAC Policy Properties] ページ

このページは、デバイスの SGT を決定する規則を作成、複製、および編集する場合に使用します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Network Device Access] > [Authentication Policy] を選択し、[Create]、[Edit]、または [Duplicate] をクリックします。

（注）　エンドポイント アドミッション コントロールの場合、アクセス サービスとセッション認可ポリシーを定義する必要があります。セッション認可ポリシーの作成については、「ネットワーク アクセス認可規則のプロパティの設定」（P.10-32）を参照してください。

表 10-28　[NDAC Policy Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を入力します。 複合式の条件が使用できる場合は、[Compound Expression] をオンにすると、式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。 ポリシーの条件のリストを変更するには、「NDAC ポリシー ページ」（P.10-48）の [Customize] ボタンをクリックします。
Results	
Security Group	対応する条件に一致した場合にデバイスに割り当てるセキュリティ グループを選択します。

関連トピック：

- 「NDAC ポリシーの設定」（P.4-26）
- 「NDAC ポリシー ページ」（P.10-48）

[Network Device Access EAP-FAST Settings] ページ

このページは、NDAC ポリシーで使用する EAP-FAST プロトコルのパラメータを設定する場合に使用します。

このページを表示するには、[Access Policies] > [Security Group Access Control] > [Network Device Access] を選択します。

表 10-29　[Network Device Access EAP-FAST Settings] ページ

オプション	説明
EAP-FAST Settings	
Tunnel PAC Time To Live	PAC が期限切れになり置換する必要が生じるまでの PAC の存続可能時間（TTL）または期間。
Proactive PAC Update When % of PAC TTL is Left	PAC の更新が必要になる時点における PAC TTL の残り時間のパーセンテージ。

関連トピック：

- 「NDAC ポリシーの設定」（P.4-26）
- 「Security Group Access 用の EAP-FAST 設定の構成」（P.4-27）
- 「NDAC ポリシー ページ」（P.10-48）

最大ユーザ セッション数

最適なパフォーマンスを得るには、ネットワーク リソースにアクセスする同時ユーザ数を制限できます。ACS 5.4 は、ユーザ 1 人あたりの同時サービス セッションの数に制限を課します。

制限はいくつかの方法で設定されます。ユーザ レベルまたはグループ レベルで制限を設定できます。最大ユーザ セッションの設定に応じて、セッション カウントはユーザに適用されます。

（注） 最大セッション数をユーザに有効にするには、管理者は RADIUS アカウンティングを設定する必要があります。

（注） 最大セッション数をデバイス管理に有効にするには、管理者は T+ セッション認可およびアカウンティングを設定する必要があります。

ここでは、次の内容について説明します。

- 「Max Session User Settings」（P.10-52）
- 「Max Session Group Settings」（P.10-52）
- 「最大セッションのグローバル設定」（P.10-53）
- 「ユーザ セッションの削除」（P.10-54）
- 「分散環境の最大ユーザ セッション」（P.10-55）
- 「プロキシ シナリオの最大ユーザ セッション」（P.10-56）

Max Session User Settings

最大ユーザ セッションは各ユーザに最大セッション値を課すように設定できます。

最大ユーザ セッション数を設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Max User Session Policy] > [Max Session User Settings] を選択します。

ステップ 2　[Max User Session Value] を、許可される同時セッションの最大数に指定します。

ステップ 3　ユーザのセッション数を無制限にするには、[Unlimited Sessions] チェックボックスをオンにします。

ステップ 4　[Submit] をクリックします。

（注）　最大セッションがユーザとグループ レベルで設定されている場合、小さい方の値が優先されます。

次に例を示します。

ユーザ Bob が *America:US:West* グループに属している場合。グループ *America:US:West* の最大セッション値は 5 セッション、最大ユーザ セッション値は 10 です。この場合、ユーザ Bob に可能な最大セッションは 5 だけになります。

関連項目

- 「最大ユーザ セッション数」（P.10-51）
- 「Max Session Group Settings」（P.10-52）
- 「最大セッションのグローバル設定」（P.10-53）
- 「ユーザ セッションの削除」（P.10-54）
- 「分散環境の最大ユーザ セッション」（P.10-55）
- 「プロキシ シナリオの最大ユーザ セッション」（P.10-56）

Max Session Group Settings

ID グループの最大セッションを設定できます。任意の 1 つの ID グループを選択し、そのグループの最大セッションを設定できます。

グループの最大セッション数を設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Max User Session Policy] > [Max Session Group Settings] を選択します。

設定した ID グループがすべて一覧表示されます。

ステップ 2　最大セッションを設定するグループの横にあるチェックボックスを選択します。

ステップ 3　[Edit] をクリックします。

ステップ 4　表 10-30 の説明に従って、フィールドに入力します。

ステップ 5　[Submit] をクリックします。

表 10-30　[Max User Session Global Settings] ページ

オプション	説明
General	
Name	ID グループの名前。
Description	ID グループの説明。
Max Session Group Settings	
Unlimited Session	グループに無制限セッションを提供する場合に、このチェックボックスをオンにします。
Max Session for Group	グループに許可する同時セッションの最大数の値を指定します。

[Unlimited] がデフォルトで選択されています。階層に基づいてグループ レベルのセッションが適用されます。次に例を示します。

グループ階層は、*:America:US:West:CA* で最大セッションは次のとおりです。

- America: 最大 100 セッション
- US: 最大 80 セッション
- West: 最大 75 セッション
- CA: 最大 50 セッション

ユーザが *America/US/West* に属している場合、ACS は、セッション数がグループ *America/US/West*、*America/US*、*America* に指定された制限を超えていないことを確認します。100 としてユーザ グループの最大セッション グループ設定を設定すると、そのグループのメンバーによって設定されたすべてのセッションの合計数が 100 を超えることはできないことを意味します。セッションが許可されると、3 つのノードの [Number of Active Sessions Availed] カウンタが 1 増加します。ACS ランタイム コンポーネントは、認証中にこの検証を処理します。

関連項目

- 「最大ユーザ セッション数」（P.10-51）
- 「Max Session User Settings」（P.10-52）
- 「最大セッションのグローバル設定」（P.10-53）
- 「ユーザ セッションの削除」（P.10-54）
- 「分散環境の最大ユーザ セッション」（P.10-55）
- 「プロキシ シナリオの最大ユーザ セッション」（P.10-56）

最大セッションのグローバル設定

RADIUS および TACACS+ 要求にセッション キーを割り当てることができます。セッション キーには、RADIUS および TACACS+ の一連の属性が提供されます。環境に従ってセッション キーの属性をカスタマイズできます。セッション キーを割り当てない場合、ACS はデフォルトのセッション キー値を使用します。

セッション キーは、ユーザ セッションを追跡するために使用される固有のキーです。セッション キーは、同じセッションに再認証するユーザと新しいセッションを開始するユーザとを ACS が区別できるようにします。単一のセッションのセッション キー属性はアクセス要求とアカウンティング開始パケットとでが同じなる必要があります。これは、ACS がセッションを適切に識別するのに役立ちます。ACS が同じセッションを再認証する場合は、同じキーが保持されます。

最大ユーザ セッションのグローバル設定を設定するには、[System Administrator] > [Users] > [Max User Session Global Settings] を選択します。

表 10-31　[Max User Session Global Settings] ページ

オプション	説明
RADIUS Session Key Assignment	
Available Session Keys	割り当てに使用可能な RADIUS セッション キー。 **（注）** RADIUS セッション キーで RADIUS Acct-Session-Id（属性 #44）を使用するには、管理者はアクセス要求 Router(config)# radius-server attribute 44 include-in-access-req で送信される Acct-Session-Id を設定する必要があります。
Assigned Session Keys	割り当てられた RADIUS セッション キー。RADIUS のデフォルトのセッション キーは、UserName:NAS-Identifier:NAS-Port:Calling-Station-ID です。
TACACS+ Session Key Assignment	
Available Session Keys	割り当てに使用可能な TACACS+ セッション キー。
Assigned Session Keys	割り当てられた TACACS+ セッション キー。TACACS+ のデフォルトのセッション キーは、User:NAS-Address:Port:Remote-Address です。
Max User Session Timeout Settings	
Unlimited Session Timeout	タイムアウトなし。
Max User Session Timeout	セッション タイムアウトに到達した場合、ACS は各セッションを閉じて、セッション カウントを更新するために疑似停止パケットを送信します。 **（注）** ユーザはデバイスでログアウトを強制されません。

関連項目

- 「最大ユーザ セッション数」（P.10-51）
- 「Max Session User Settings」（P.10-52）
- 「Max Session Group Settings」（P.10-52）
- 「ユーザ セッションの削除」（P.10-54）
- 「分散環境の最大ユーザ セッション」（P.10-55）
- 「プロキシ シナリオの最大ユーザ セッション」（P.10-56）

ユーザ セッションの削除

ユーザが [Logged-in] として示されていますが、AAA クライアントへの接続は失われて、ユーザは実際にはログインしていない場合にのみ、[Purge] オプションを使用できます。

削除しても AAA クライアントからユーザはログオフされませんが、セッション カウントは 1 減ります。カウントがゼロの間、デバイスから届く停止パケットまたは中間アップデートは廃棄されます。別の AAA クライアントに同じユーザ名とパスワードでユーザがログインしている場合に、この削除により、このセッションが影響を受けることはありません。

（注） 疑似アカウンティング停止は、セッション カウント値に関係なく送信されます。

ユーザ セッションを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Users] > [Purge User Sessions] に移動します。

[Purge User Session] ページにすべての AAA クライアントのリストが表示されます。

ステップ 2　ユーザ セッションを削除する AAA クライアントを選択します。

ステップ 3　[Get Logged-in User List] をクリックします。

すべてのログイン ユーザのリストが表示されます。

ステップ 4　特定の AAA クライアントにログインしているすべてのユーザ セッションを削除するには、[Purge All Sessions] をクリックします。

関連項目

- 「最大ユーザ セッション数」（P.10-51）
- 「Max Session User Settings」（P.10-52）
- 「Max Session Group Settings」（P.10-52）
- 「最大セッションのグローバル設定」（P.10-53）
- 「分散環境の最大ユーザ セッション」（P.10-55）
- 「プロキシ シナリオの最大ユーザ セッション」（P.10-56）

分散環境の最大ユーザ セッション

分散環境では、ランタイムによって保持される最大ユーザ セッションに関するセッション キャッシュ関連情報を除くすべてのユーザおよび ID グループの設定がセカンダリに複製されます。このため、各サーバのランタイムには独自のセッションによって確立された詳細があります。また、最大セッション カウントは、認証/アカウンティング要求が受信される ACS サーバに基づいて適用されます。

関連項目

- 「最大ユーザ セッション数」（P.10-51）
- 「Max Session User Settings」（P.10-52）
- 「Max Session Group Settings」（P.10-52）
- 「最大セッションのグローバル設定」（P.10-53）
- 「ユーザ セッションの削除」（P.10-54）
- 「プロキシ シナリオの最大ユーザ セッション」（P.10-56）

プロキシ シナリオの最大ユーザ セッション

認証要求とアカウンティング要求は同じ ACS サーバに送信する必要があります。そうしないと、最大セッション機能は希望どおりに働きません。

関連項目

- 「最大ユーザ セッション数」（P.10-51）
- 「Max Session User Settings」（P.10-52）
- 「Max Session Group Settings」（P.10-52）
- 「最大セッションのグローバル設定」（P.10-53）
- 「ユーザ セッションの削除」（P.10-54）
- 「分散環境の最大ユーザ セッション」（P.10-55）

CHAPTER 11

ACS での監視とレポート

[Monitoring and Reports] ドロワがプライマリ Web インターフェイス ウィンドウに表示されます。このドロワには、[Launch Monitoring and Report Viewer] オプションがあります。

Monitoring and Report Viewer には、ネットワーク内の ACS サーバに対する監視機能、レポート機能、およびトラブルシューティング機能が備えられています。高度なレポートとトラブルシューティングを実行するために、統合ログ、設定、および診断データを 1 つ以上の ACS サーバから抽出できます。

ネットワークに Network Access Device（NAD）を設定して、Monitoring and Report Viewer に syslog メッセージを送信できます。この操作を実行するには、NAD のロギング ポートを UDP 20514 に設定する必要があります。

たとえば、ネットワーク内の NAD が Monitoring and Report Viewer に syslog メッセージを送信できるようにするには、CLI コンフィギュレーション モードで NAD に次のコマンドを入力する必要があります。

1. **logging monitor informational**
2. **logging origin-id ip**
3. **logging host** *ip* **transport udp port 20514** : *ip* はネットワーク内のログ コレクタの IP アドレスです。
4. **epm logging**

[Launch Monitoring and Report Viewer] をクリックすると、セカンダリ Web インターフェイス ウィンドウで Monitoring and Reports Viewer が開きます。このビューアには、次のドロワがあります。

- Monitoring and Reports
- Monitoring Configuration （「Monitoring and Report Viewer でのシステムの動作と設定の管理」（P.15-1）を参照）。

[Monitoring and Reports] ドロワには、次の機能があります。

- Dashboard：展開された ACS サーバの概要（リアルタイムで更新されます）、認証アクティビティ、および各 ID ストアに対する認証の要約が表示されます。「ダッシュボード ページ」（P.11-2）を参照してください。
- Alarms：許容できるシステム パフォーマンスを表すしきい値を定義できます。測定が継続的に行われ、これらのしきい値と比較されます。しきい値を超過した場合は、アラームが生成されます。「アラームについて」（P.12-1）を参照してください。
- Reports：豊富なレポートのセットを使用できます。「レポートの管理」を参照してください。
- Troubleshooting：システム接続のテストやサポート バンドルをダウンロードするツールなど、ACS システムのトラブルシューティングに役立つツールが用意されています。「Monitoring and Report Viewer を使用した ACS のトラブルシューティング」を参照してください。

- Support for non-English characters (UTF-8)：次の項目では英語以外の文字を使用できます。
  - Syslog メッセージ：設定可能な属性値、ユーザ名、ACS の名前付き設定オブジェクト
  - GUI 入力フィールド
  - クエリー ページ
  - レポートと Interactive Viewer
  - アラーム
  - ダッシュボード ルックアップ
  - 失敗の理由のテキスト

（注）　[Monitoring and Reports] ドロワ ページでは、ページ領域の下矢印（v）を使用して領域のコンテンツを非表示にでき、右矢印（>）を使用してコンテンツを表示できます。

関連項目

- 「認証レコードと詳細」（P.11-2）

認証レコードと詳細

レポートの情報の主なソースは認証レコードです。要求に使用されたアクセス サービス、要求で参照されたユーザまたはホスト、要求を行ったデバイスなどの複数のカテゴリに従って、これらのレコードを分析するレポートが提供されています。ACS では各カテゴリのインスタンスごとに認証の要約が提供され、管理者はさらに詳細な情報を取得できます。

各認証レコード内に、認証レコードの詳細を表示するオプションがあります。詳細には、次の情報が含まれます。

- Authentication Details：要求の詳細、要求に対して選択されたサービス、ポリシー、規則、応答で返された結果などを含む認証の詳細。
- Authentication Result：結果の応答の内容。
- Steps：要求の処理時に実行された手順の順序がリストされます。

認証の詳細情報は、特定の正常な応答が返された理由を理解する場合、および、失敗した応答が返されたときに実行した手順をトラッキングする場合に非常に役立ちます。

ダッシュボード ページ

Monitoring and Report Viewer を起動すると、セカンダリ Web インターフェイス ウィンドウにダッシュボードが表示されます。

ACS 5.4 には、新しいカスタマイズ可能なダッシュボードが備えられています。ダッシュボードにはタブとポートレットが含まれており、ここで、お気に入りのクエリー、最近のアラームとレポート、および ACS インスタンスの健全性ステータスが、Monitoring and Report Viewer によって統合されます。これらの各タブには、各ポートレットに選択したアプリケーションが含まれる、複数のポートレットが表示される場合があります。

使用可能なアプリケーションのリストから、アプリケーションを選択できます。デフォルトでは、Monitoring and Report Viewer のダッシュボードには次のタブとアプリケーションが用意されています。

（注）　これらのタブはカスタマイズが可能で、次のタブを修正または削除できます。

- [General]：[General] タブには次の項目がリストされます。
  - [Five most recent alarms]：アラームの名前をクリックすると、アラームの詳細とステータスを示すダイアログボックスが表示されます。このダイアログボックスの [Status] タブの情報を更新して、アラームをトラッキングできます。[Status] タブのフィールドの説明については、表 12-5 を参照してください。
  - [Favorite reports]：お気に入りレポートがアルファベット順に表示されます。レポートを表示するには、レポートの名前をクリックします。このレポートは、Interactive Viewer で表示できます。このリストをカスタマイズしてお気に入りレポートを含めることができます。これにより、これらのレポートをダッシュボードからすばやく起動できます。
- [Troubleshooting]：[Troubleshooting] タブには、次のペインがあります。
  - [Live Authentications]：その日のライブ認証が表示されます。このペインに表示されるレコードはフィルタリングできます。
  - [My Links]：お気に入りのリンクをこのペインに追加できます。
  - [NAD Show Command]：このペインから、任意の NAD デバイスに対して表示コマンドを実行できます。NAD 表示コマンドを実行するには、次の操作を行う必要があります。
    a. NAD の IPv4 または IPv6 IP アドレスを入力します（必須）。
    b. NAD のユーザ名とパスワードを入力します。
    c. プロトコルとして Telnet または SSHv2 を選択します（必須）。
    d. ポート番号を入力します。デフォルトは 23 です（必須）。
    e. イネーブル パスワードを入力します。
    f. コンソール サーバを使用する場合は、[Use Console Server] チェックボックスをオンにします。
    g. コンソール サーバの Ipv4 または Ipv6 アドレスを入力します。このフィールドは、[Use Console Server] チェックボックスをオンにした場合に必須です。
    h. NAD に対して実行する表示コマンドを入力します（必須）。

    Monitoring and Report Viewer で NAD 表示コマンドを実行するとき、より詳細な情報の入力を要求される場合があります。[Progress Details] ページのフィールドの説明については、表 14-5 を参照してください。[Done] をクリックしたあと、[Show Results Summary] をクリックすると、表 14-6 に示すような結果を表示できます。
  - [Authentication Lookup]：このポートレットを使用して、デフォルトのパラメータで認証レポートを実行したり、ユーザまたは MAC アドレスに対する認証レコードを検索したりできます。また、ユーザに対するユーザ要約レポートやエンド ポイントに対するエンドポイント要約レポートを実行できます。[Authentication Lookup] ポートレットの詳細については、「[Authentication Lookup] ポートレットの操作」（P.11-5）を参照してください。
- [Authentication Trends]：[Authentication Trends] タブには次のペインがあります。
  - [Authentication Trend]：最大で過去 30 日間の認証の傾向がグラフィカルな表形式で表示されます。グラフィカルな表示では、時間が X 軸にプロットされ、認証が Y 軸にプロットされます。

    表形式の表示では、それぞれの日の成功、失敗、および削除された認証の数が表示されます。図の右下隅にあるボタン（ ）を使用して、2 つのビュー間を切り替えることができます。

  - [Top <N> Authentications] : 上位 <N> 個の認証がグラフィカルに表示されます。時間が X 軸にプロットされ、認証が Y 軸にプロットされます。
  - [Authentication Snapshot] : 最大で過去 30 日間の認証のスナップショットがグラフィカルな表形式で表示されます。グラフィカルな表示では、レコードのグループ化の基準になるフィールドが X 軸にプロットされ、認証が Y 軸にプロットされます。

    表形式の表示では、[Category]、[Pass Count]、[Daily, Weekly, or Monthly Pass Count]、[Fail Count]、[Daily, Weekly, or Monthly Fail Count] が表示されます。図の右下隅にあるボタン（ ）を使用して、2 つのビュー間を切り替えることができます。

- [ACS Health] : [ACS Health] タブには、ACS インスタンスのシステム健全性と AAA 健全性が表示されます。この情報は表形式で表示されます。
  - システム ステータスは、CPU 使用状況、メモリ使用状況、ディスク入力 / 出力使用状況、および /opt ディスクと /local ディスクのディスク使用状況のパラメータによって決定されます。
  - AAA ステータスは、RADIUS および TACACS+ の遅延によって決定されます。

  凡例（Critical、Warning、Healthy）の上にマウス ポインタを移動すると、ACS インスタンスのステータスを決定する基準が表示されます。ACS インスタンスの健全性の詳細なグラフィカル表示については、ACS インスタンスの名前をクリックしてください。ACS 健全性の要約レポートが表示されます。このレポートは、Interactive Viewer で表示できます。

ダッシュボードのタブは、ニーズに合せて設定できます。ダッシュボードのタブの設定方法およびタブへのアプリケーションの追加方法の詳細については、「ダッシュボード内のタブの設定」（P.11-6）を参照してください。

関連トピック

- 「ポートレットの操作」（P.11-4）
- 「ダッシュボード内のタブの設定」（P.11-6）
- 「タブへのアプリケーションの追加」（P.11-7）

ポートレットの操作

ポートレットは、ダッシュボード内の小さな完全独立ウィンドウであり、リアルタイム グラフや表形式レポートなどの形式で情報が表示されます。ダッシュボード内の各タブは、1 つ以上のポートレットから構成されています。図 11-1 に、[General] タブの 2 つのポートレットを示します。

図 11-1　ポートレット

[Top 5 Alarms] と [My Favorite Reports] が別々のウィンドウに表示されます。これらの各ポートレットを個別に編集できます。

ポートレットを編集するには、ウィンドウの右上隅にある編集ボタン（ ）をクリックします。Monitoring and Report Viewer では、ニーズに合せてポートレット内の情報をカスタマイズできます。タブの追加、編集、削除、ポートレット内のアプリケーション設定の編集、およびポートレットの削除を行うことができます。

[Authentication Lookup] ポートレットの操作

ダッシュボードに [Authentication Lookup] ポートレットを追加できます。

[Authentication Lookup] ポートレットを追加するには、「タブへのアプリケーションの追加」（P.11-7）を参照してください。

[Authentication Lookup] ポートレットには次のフィールドがあります。

- [Username/MAC Address]：（要約レポートでは必須）ユーザのユーザ名または aa-bb-cc-dd-ee-ff 形式での MAC アドレス。Monitoring and Report Viewer では、他の形式の MAC アドレスは使用できません。
- [View]：[Authentication] を選択して認証レポートを実行するか、[Summary] を選択して要約レポートを実行します。
- [Time Range]：選択した [View] オプションに応じて、[Time Range] ドロップダウン リスト ボックスにデータが読み込まれます。レポートの生成対象の時間範囲を選択します。
- [Start Date]：（[Custom time range] オプションを選択するとイネーブルになります）開始日を選択します。
- [End Date]：（[Custom time range] オプションを選択するとイネーブルになります）終了日を選択します。

- [Protocol] : [Protocol] ドロップダウン リスト ボックスから [RADIUS] または [TACACS+] を選択します。プロトコルは、エンドポイント要約レポートでは考慮されません。

関連項目

- 「ダッシュボード ページ」（P.11-2）
- 「[Authentication Lookup] レポートの実行」（P.11-6）

[Authentication Lookup] レポートの実行

[Authentication Lookup] レポートを実行する場合は、次のことを考慮します。

- [Username or MAC Address] に aa-bb-cc-dd-ee-ff 形式の値を指定した場合は、この MAC アドレスに対して認証レポートが実行される。
- [Username or MAC Address] にその他の形式の値を指定した場合は、値がユーザ名と見なされ、そのユーザに対して認証レポートが実行される。
- [Username or MAC Address] フィールドが空の場合は、選択したプロトコルと時間範囲に対してデフォルトのパラメータを使用して認証レポートが実行される（カタログ ページで RADIUS または TACACS 認証レポートを実行する場合と同様）。
- [Username or MAC Address] フィールドに有効な MAC アドレス値を指定し、[Summary View] オプションを選択した場合は、エンドポイント要約レポートが実行される。選択したプロトコルに関係なく、常に RADIUS プロトコルに対してエンドポイント要約レポートが実行されます。

指定した MAC アドレス値が規定の形式でない場合は、ユーザ名と見なされ、選択した時間範囲とプロトコルに対してユーザ認証要約レポートが実行されます。

ダッシュボード内のタブの設定

ここでは、ダッシュボード内のタブの設定方法とタブにアプリケーションを追加する方法について説明します。この項の構成は、次のとおりです。

- 「ダッシュボードへのタブの追加」（P.11-6）
- 「ダッシュボード内のタブの名前変更」（P.11-7）
- 「ダッシュボードのレイアウトの変更」（P.11-8）
- 「ダッシュボードからのタブの削除」（P.11-8）

ダッシュボードへのタブの追加

Monitoring and Report Viewer ダッシュボードでは、ダッシュボード内のタブと、タブから使用可能なアプリケーションをカスタマイズできます。ダッシュボードにタブを追加するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer から、[Monitoring and Reports] > [Dashboard] を選択します。

[Dashboard] ページが表示されます。

ステップ 2　[Dashboard] ページの右上隅にある [Configure] ドロップダウン リストをクリックします。

ステップ 3　[Add New Page] をクリックします。

ステップ 4　[Add New Page] テキスト ボックスに、作成するタブの名前を入力します。

ステップ 5　[Add Page] をクリックします。

選択した新しいタブが作成されます。このタブで、最も頻繁に監視するアプリケーションを追加できます。

タブへのアプリケーションの追加

タブにアプリケーションを追加するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer から、[Monitoring and Reports] > [Dashboard] を選択します。

[Dashboard] ページが表示されます。

ステップ 2　アプリケーションを追加するタブを選択します。

アプリケーションを新しいタブに追加する場合は、アプリケーションを追加する前にダッシュボードに新しいタブを追加する必要があります。

ステップ 3　[Dashboard] ページの右上隅にある [Configure] ドロップダウン リストをクリックします。

ステップ 4　[Add Application] をクリックします。

[Add Application] ウィンドウが表示されます。

ステップ 5　[View Dashboard] をクリックして、ダッシュボードに追加できるアプリケーションのリストを表示します。

または、[Search Content] テキスト ボックスにアプリケーションの名前を入力できます。

アプリケーションのリストが表示されます。

ステップ 6　追加するアプリケーションの横の [Add] リンクをクリックします。

選択したアプリケーションがタブに追加されます。このタブでパラメータを編集できます。

ダッシュボード内のタブの名前変更

ダッシュボードの既存のタブの名前を変更するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer から、[Monitoring and Reports] > [Dashboard] を選択します。

[Dashboard] ページが表示されます。

ステップ 2　名前を変更するタブを選択します。

ステップ 3　[Dashboard] ページの右上隅にある [Configure] ドロップダウン リストをクリックします。

ステップ 4　[Rename Page] をクリックします。

ステップ 5　[Rename Page] テキスト ボックスに新しい名前を入力します。

ステップ 6　[Update] をクリックします。

タブが新しい名前で表示されます。

ダッシュボードのレイアウトの変更

ダッシュボードのルック アンド フィールを変更できます。ACS には、9 種類の組み込みレイアウトが用意されています。別のレイアウトを選択するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer から、[Monitoring and Reports] > [Dashboard] を選択します。

[Dashboard] ページが表示されます。

ステップ 2　レイアウトを変更するタブを選択します。

ステップ 3　[Dashboard] ページの右上隅にある [Configure] ドロップダウン リストをクリックします。

レイアウト オプションのリストが表示されます。

ステップ 4　このタブに使用するレイアウト スタイルの横のオプション ボタンをクリックします。

ステップ 5　[Save] をクリックしてレイアウトを変更します。

ダッシュボードからのタブの削除

ダッシュボードからタブを削除するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer から、[Monitoring and Reports] > [Dashboard] を選択します。

[Dashboard] ページが表示されます。

ステップ 2　[Dashboard] ページの右上隅にある [Configure] ドロップダウン リストをクリックします。

ステップ 3　[Manage Pages] をクリックします。

ステップ 4　[Page Display Order] リスト ボックスで、削除するタブを選択します。

ステップ 5　 をクリックして、選択したタブを削除します。

ワンポイント アドバイス　または、削除するタブの名前の上にマウス ポインタを移動すると、 というアイコンが表示されます。このアイコンをクリックしてタブを削除します。

CHAPTER 12

アラームの管理

ACS のモニタリング機能では、クリティカルなシステム条件を通知するアラームが生成されます。モニタリング コンポーネントでは、データが ACS から取得されます。このデータにしきい値と規則を設定して、アラームを管理できます。

アラーム通知は Web インターフェイスに表示され、電子メールおよび Syslog メッセージを通じてイベントの通知を取得できます。ACS は、重複するアラームをデフォルトでフィルタリングします。

この章の内容は、次のとおりです。

- 「アラームについて」（P.12-1）
- 「受信ボックスでのアラームの表示および編集」（P.12-3）
- 「アラーム スケジュールについて」（P.12-9）
- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「アラームしきい値の削除」（P.12-33）
- 「システム アラーム設定の設定」（P.12-34）
- 「アラーム Syslog ターゲットについて」（P.12-35）

アラームについて

ACS には 2 種類のアラームがあります。

- 「しきい値アラーム」（P.12-1）
- 「システム アラーム」（P.12-2）

しきい値アラーム

しきい値アラームは、特定のイベントを通知する ACS サーバから収集されたログ データに定義されます。たとえば、ACS システムの健全性、ACS プロセスのステータス、認証がアクティブかどうかなどを通知するようにしきい値アラームを設定できます。

これらのデータ セットに対してしきい値条件を定義します。しきい値条件が満たされると、アラームがトリガーされます。しきい値を定義するときには、しきい値をいつ適用する必要があるか（期間）、アラームの重大度、および通知の送信方法も定義します。

使用可能なアラームしきい値の 15 個のカテゴリを使用すると、ACS システムの動作の多くの異なる側面を監視できます。しきい値アラームの詳細については、「アラームしきい値の作成、編集、および複製」（P.12-11）を参照してください。

システム アラーム

システム アラームは、ACS Monitoring & Reporting Viewer の実行中に検出されたクリティカル条件を通知します。システム アラームは、データ削除イベントや、ログ コレクタによる View データベースへのデータ入力の失敗など、システム アクティビティの情報ステータスも提供します。

システム アラームは定義済みであり、設定できません。ただし、システム アラームをディセーブルにしたり、イネーブルにした場合の通知方法を決定したりするオプションはあります。

ここでは、次の内容について説明します。

- 「アラームしきい値の評価」（P.12-2）
- 「ユーザへのイベントの通知」（P.12-3）

アラームしきい値の評価

ACS は、スケジュールに基づいてしきい値条件を評価します。これらのスケジュールを定義し、しきい値の作成時にしきい値にスケジュールを割り当てます。スケジュールは、週の中の 1 つ以上の連続または不連続期間で構成されます。

たとえば、月曜日から金曜日までの午前 8:00 から ～午後 5 時 00 分、月曜日～金曜日。詳細については、「アラーム スケジュールについて」（P.12-9）を参照してください。このスケジュールをしきい値に割り当てると、ACS によってしきい値が評価され、アクティブな期間中にだけアラームが生成されます。

ACS は、現在イネーブルになっているしきい値の数に応じてしきい値を定期的に評価します。

表 12-1 に、特定のしきい値数の評価サイクルの長さを示します。

表 12-1　アラームしきい値の評価サイクル

イネーブルになっているしきい値の数	評価サイクル[1]
1 ～ 20	2 分ごと
21 ～ 50	3 分ごと
51 ～ 100	5 分ごと

1. しきい値の評価にかかる時間が長くなると、評価サイクルが 2 分から 3 分、3 分から 5 分、5 分から 15 分に増加します。評価サイクル時間は、12 時間ごとに 2、3、および 5 分にリセットされます。

評価サイクルが開始されると、ACS はイネーブルになっている各しきい値を次々に評価します。しきい値に関連付けられているスケジュールでしきい値の実行が許可されている場合、ACS はしきい値条件を評価します。条件が満たされるとアラームがトリガーされます。詳細については、「アラームしきい値の作成、編集、および複製」（P.12-11）を参照してください。

（注） システム アラームには関連付けられているスケジュールがなく、発生後即時に送信されます。システム アラームは全体としてだけイネーブルまたはディセーブルにすることができます。

ユーザへのイベントの通知

しきい値に達するかシステム アラームが生成されると、アラームが Web インターフェイスの [Alarms Inbox] に表示されます。このページから、アラームの詳細を表示したり、アラームに関するコメントを追加したりできます。また、ステータスを変更して、[Acknowledged] または [Closed] であることを示すことができます。

アラームをトリガーしたイベントを調査するときに役立つ関連レポートが 1 つ以上ある場合は、このページのアラーム詳細に、それらのレポートへのリンクが表示されます。

ダッシュボードには、最新の 5 つのアラームも表示されます。確認または終了したアラームは、ダッシュボードのこのリストから削除されます。

ACS では、次の形式で通知を受信するオプションが提供されています。

- 電子メール：アラーム詳細ページに表示されるすべての情報が含まれます。この電子メールを送信する必要がある受信者のリストを設定できます。ACS 5.4 には、HTML 形式の電子メールを介してイベントの通知を受信するオプションがあります。
- Syslog メッセージ：アラーム syslog ターゲットとして設定した Linux または Windows マシンに送信されます。最大 2 つのアラーム syslog ターゲットを設定できます。

受信ボックスでのアラームの表示および編集

ACS サーバから収集されたデータのセットに対するしきい値設定または規則に基づいて ACS が生成するアラームを表示できます。設定されたしきい値を満たしたアラームは、受信ボックスに送信されます。アラームを表示したあとで、アラームのステータスの編集、管理者へのアラームの割り当て、およびイベントをトラッキングするためのメモの追加を行うことができます。

受信ボックスのアラームを表示するには、[Monitoring and Reports] > [Alarms] > [Inbox] を選択します。

ACS によってトリガーされたアラームのリストがある [Inbox] ページが表示されます。表 12-2 に、[Alarms] ページのフィールドを示します。表 12-3 に、ACS 5.4 のシステム アラームと、その重大度を示します。

表 12-2　[Alarms] ページ

オプション	説明
Severity	*表示のみ*。関連付けられているアラームの重大度を示します。次のオプションがあります。 • Critical • Warning • Info
Name	アラームの名前を示します。クリックして [Alarms: Properties] ページを表示し、アラームを編集できます。

表 12-2　[Alarms] ページ （続き）

オプション	説明
Time	*表示のみ*。関連付けられているアラーム生成時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* 形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • *timezone* = タイムゾーン。 • yyyy = 年を表す 4 桁の数字。
Cause	*表示のみ*。アラームの原因を示します。
Assigned To	*表示のみ*。アラームを調査する担当者を示します。
Status	*表示のみ*。アラームのステータスが表示されます。次のオプションがあります。 • New：アラームは新規です。 • Acknowledged：アラームは既知です。 • Closed：アラームは終了しました。
Edit	編集するアラームの隣にあるチェックボックスをオンにし、[Edit] をクリックしてアラームのステータスを編集し、対応するレポートを表示します。
Close	終了するアラームの隣にあるチェックボックスをオンにし、[Close] をクリックしてアラームを終了します。アラームを終了する前に終了メモを入力できます。 アラームを終了すると、アラームがダッシュボードからだけ削除されます。アラーム自体は削除されません。
Delete	削除するアラームの隣にあるチェックボックスをオンにし、[Delete] をクリックしてアラームを削除します。

表 12-3　ACS 5.4 のシステム アラーム

アラーム	重大度
パージ関連のアラーム	
バックアップが失敗しました。データベースのパージの前に、バックアップが失敗しました。	Critical
バックアップが正常に行われました。データベースのパージの前に、バックアップが失敗しました。	Info
日次テーブルのデータベースの削除が失敗しました。例外で詳細が示されます。	Critical
月次テーブルのデータベースの削除が失敗しました。例外で詳細が示されます。	Critical
年次テーブルのデータベースの削除が失敗しました。例外で詳細が示されます。	Critical

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
増分バックアップが設定されていません。データベースのパージを正常に行うには、増分バックアップを設定する必要があります。これによってディスク領域の問題を回避できます。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actual db size GB です。	Warning
増分バックアップ データ リポジトリをリモート リポジトリとして設定してください。そうしないと、バックアップが失敗し、増分バックアップ モードがオフに変更されます。	Warning
パージの前に、データをバックアップするために使用するリモート リポジトリをパージ設定で設定します。	Warning
View データベース サイズが上限の maxlimit GB を超えています。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actualDBSize GB です。View データベース サイズが上限の maxLimit GB を超えています。	Critical
View データベース サイズが上限の upperLimit GB を超えています。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actualDBSize GB です。View データベース サイズが上限の upperLimit GB を超えています。	Critical
ACS View DB のサイズが下限の lowerLimit GB を超えています。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actualDBSize GB です。View データベース サイズが下限の lowerLimit GB を超えています。	Warning
DB の削除。データベースが削除を開始します。	Info
ディスク容量の制限の超過 - 次のウィンドウ：ディスク容量制限が、1 か月のデータで推奨されるしきい値を超過しました。下限に達するまで週次データを削除します。	Warning
ACS View アプリケーションが、許可された最大ディスク サイズを超えました。ディスク領域が推奨されるしきい値を超えました。余分な monthsinnumber か月のデータを削除します。	Warning
ACS View アプリケーションが、許可された最大ディスク サイズを超えました。ディスク領域が推奨されるしきい値を超えました。monthsinnumber か月のデータを削除します。	Info
削除が成功しました。View データベースに存在するレコードのサイズは actualsizeinGB GB です。ディスク上の View データベースの物理サイズは sizeinGB GB です。View データベースの物理サイズを減らす場合は、コマンドラインで ACS コンフィギュレーション モードから acsview-db-compress コマンドを実行します。	Warning
下限に達するまでパージ プロセスによって week 週のデータが削除されました。	Info
パージ プロセスが直前 3 週間のデータを削除して、下限に達するまで最大データを削除しようとしましたが、acsview データベース サイズが下限よりも大きいままです。現在、直前 1 週間のデータしか保管されていません。	Warning
入力ログ メッセージの数がしきい値（GB）に近づいています。メッセージの重要なカテゴリだけをログ コレクタに送信するように ACS を設定してください。	Warning
増分バックアップ	
オンデマンド完全バックアップが失敗しました。例外で詳細が示されます。	Critical
データベースの完全バックアップが失敗しました。例外で詳細が示されます。	Critical

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
データベース削除の完全バックアップが失敗しました。例外で詳細が示されます。	Critical
増分バックアップが失敗しました。例外で詳細が示されます。	Critical
増分リストアが成功しました。	Info
増分リストアが失敗しました。理由：例外で詳細が示されます。	Critical
オンデマンド完全バックアップが失敗しました。例外で詳細が示されます。	Critical
データベースの完全バックアップが失敗しました。例外で詳細が示されます。	Critical
データベース削除の完全バックアップが失敗しました。例外で詳細が示されます。	Critical
増分バックアップが失敗しました。例外で詳細が示されます。	Critical
ログのリカバリ	
ログ メッセージのリカバリが失敗しました。例外で詳細が示されます。	Critical
View の圧縮	
データベースの再構築操作が開始されました。ログ コレクタ サービスはこの操作中にシャット ダウンされ、再構築処理が完了した後で構成されます。ログのリカバリ オプションがすでにイネーブルの場合、再構築処理中に受信したログ メッセージがあれば、ログ コレクタ サービスの起動後にリカバリされます。	Critical
データベースのリロード操作が完了しました。	Info
システムがデータベースの圧縮の必要性を検出しました。メンテナンス ウィンドウで View データベースの圧縮操作を手動で実行してください。実行しない場合、ディスク領域の問題を避けるため、データベースの自動再構築がトリガーされます。	Warning
データベースの自動再構築操作が開始されました。ログ コレクタ サービスはこの操作中にシャット ダウンされ、再構築処理が完了した後で構成されます。ログのリカバリ オプションがすでにイネーブルの場合、再構築処理中に受信したログ メッセージがあれば、ログ コレクタ サービスの起動後にリカバリされます。	Critical
データベースのリロード操作が完了しました。	Info
データベースの自動再構築処理は、ディスク領域の問題を避けるために、データベースのサイズが上限を超えるとトリガーされます。ログ リカバリ機能をイネーブルにすると、データベースの再構築中に失われたログ メッセージをリカバリできます。データベースの再構築操作はログ リカバリ機能を有効にするまで継続しません。	Warning
しきい値のエグゼキュータ	
割り当てられた thresholdEvaluationInterval 分のインターバルで、すべてのしきい値の実行を完了できませんでした。しきい値は、次のインターバルで再度評価されます。このエラーは、次の場合に発生する可能性があります。システムに重い負荷がかかっている（例：パージなど）。現時点でアクティブなしきい値が多すぎる。	Info
セッション モニタ	
アクティブなセッションが制限値を超えています。セッションが 250000 を超えています。	Warning
Syslog Collector の失敗	

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
詳細についてはコレクタ ログを参照してください。	Critical
ACS のスケジュール バックアップ	
ACS 設定データベースのスケジュール バックアップは、バックアップ名に無効な文字があるために開始されませんでした。	Critical
ACS 設定データベースのスケジュール バックアップは、リポジトリが無効であるために開始できませんでした。リポジトリがあることを確認してください。	Critical
ホスト名を取得できません。ACS 設定データベースのスケジュール バックアップは失敗しました。詳細については、ADE.log を参照してください。	Critical
バックアップ ライブラリをロードできませんでした。ACS 設定データベースのスケジュール バックアップは失敗しました。詳細については、ADE.log を参照してください。	Critical
シンボル ルックアップのエラー。ACS 設定データベースのスケジュール バックアップは失敗しました。詳細については、ADE.log を参照してください。	Critical
内部エラーのため、ACS バックアップを実行できませんでした。詳細については、ADE.log を参照してください。	Critical
ディスク サイズの確認	
バックアップ サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、バックアップ プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
パッチ サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、パッチのインストール プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
サポート バンドル サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、サポート バンドル収集プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
バックアップ サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、復元プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
ディスク クォータ	
ACS DB のサイズが許可されているクォータを超えました。	Critical
ACS View DB のサイズが許可されているクォータを超えました。	Critical
View データのアップグレード	
データベースの変換が正常に完了しました。View の newVersion データベースが installedVersion にアップグレードされ、アクティブ化する準備が整いました。	Warning
データベースの変換が正常に完了しませんでした。View の newVersion のアップグレード プロセスでエラーが発生し、完了できませんでした。アップグレード ログに詳細情報が含まれます。	Critical
その他	
アグリゲータがビジーです。Syslog はドロップされます。	Critical

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
コレクタがビジーです。Syslog はドロップされます。	Critical
登録解除された ACS サーバのサーバ名です。	Warning
不明なメッセージ コードを受信しました。	Critical

（注）　クォータを超える ACS データベースのアラームは、ACS データベースの合計サイズがクォータを超えた場合にだけ送信されます。ACS データベースの合計サイズ = acs*.log + acs.db で、acs*.log は ACS データベース ログ ファイルです。acs*.log および acs.db ファイルは、どちらも /opt/CSCOacs/db にあります。

（注）　ACS は、リモート syslog サーバとして使用できません。ただし、syslog サーバとして外部サーバを使用できます。syslog サーバとして外部サーバを使用する場合、syslog メッセージが外部の syslog サーバに送信されるため、ACS ビューではアラームを生成できません。ACS ビューでアラームを生成するには、CLI を使用してロギング オプションを localhost に設定します。

アラームを編集するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Inbox] を選択します。

ACS によってトリガーされたアラームのリストがある [Inbox] ページが表示されます。

ステップ 2　編集するアラームの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

次のタブがある [Inbox - Edit] ページが表示されます。

- [Alarm]：このタブは、アラームをトリガーしたイベントに関する詳細情報を示します。表 12-4 に、[Alarm] タブのフィールドを示します。[Alarm] タブのフィールドは編集できません。

表 12-4　[Inbox - Alarm] タブ

オプション	説明
Occurred At	アラームがトリガーされた日時。
Cause	アラームをトリガーしたイベント。
Detail	アラームをトリガーしたイベントに関する詳細情報。通常、ACS では、指定したしきい値を超過した項目のカウントがリストされます。
Report Links	イベントをさらに調査するための関連レポートがある場合は、それらのレポートへの 1 つ以上のハイパーリンクが表示されます。
Threshold	しきい値設定に関する情報。

- [Status]：このタブでは、アラームのステータスを編集したり、イベントをトラッキングするための説明を追加したりできます。

ステップ 3　必要に応じて、[Status] タブのフィールドを変更します。表 12-5 に、各フィールドを示します。

表 12-5　[Inbox - Status] タブ

オプション	説明
Status	アラームのステータス。アラームの生成時のステータスは [New] です。アラームを表示したあとで、アラームのステータスを [Acknowledged] または [Closed] に変更してアラームの現在のステータスを示します。
Assigned To	（任意）このアラームが割り当てられるユーザの名前を指定します。
Notes	（任意）記録するアラームに関する追加情報を入力します。

ステップ 4　[Submit] をクリックして変更を保存します。

変更が反映された [Alarms] ページが表示されます。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「アラームしきい値の削除」（P.12-33）

アラーム スケジュールについて

アラーム スケジュールを作成して、特定のアラームしきい値をいつ実行するかを指定できます。アラーム スケジュールを作成、編集、および削除できます。週 7 日のさまざまな時刻に実行するアラーム スケジュールを作成できます。

デフォルトでは、ACS には non-stop アラーム スケジュールが付属しています。このスケジュールは、1 日 24 時間、週 7 日にわたってイベントを監視します。

アラーム スケジュールのリストを表示するには、[Monitoring and Reports] > [Alarms] > [Schedules] を選択します。[Alarm Schedules] ページが表示されます。表 12-6 に、[Alarm Schedules] ページのフィールドを示します。

表 12-6　[Alarm Schedules] ページ

オプション	説明
Filter	検索基準に基づいてアラーム スケジュールをフィルタリングするための検索基準を入力します。
Go	検索を開始するには [Go] をクリックします。
Clear Filter	検索結果をクリアし、すべてのアラーム スケジュールをリストするには、[Clear Filter] をクリックします。
Name	アラーム スケジュールの名前。
Description	（任意）アラーム スケジュールの簡単な説明。

ここでは、次の内容について説明します。

- 「アラーム スケジュールの作成と編集」（P.12-10）
- 「しきい値へのアラーム スケジュールの割り当て」（P.12-10）
- 「アラーム スケジュールの削除」（P.12-11）

アラーム スケジュールの作成と編集

アラーム スケジュールを作成または編集するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Schedules] を選択します。

[Alarm Schedules] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 編集するアラーム スケジュールの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[Alarm Schedules - Create or Edit] ページが表示されます。表 12-7 に、[Alarm Schedules - Create or Edit] ページのフィールドを示します。

表 12-7　[Alarm Schedules - Create or Edit] ページ

オプション	説明
ID	
Name	アラーム スケジュールの名前。名前は最大 64 文字です。
Description	アラーム スケジュールの簡単な説明。最大 255 文字です。
Schedule	
四角をクリックして、その時間を選択または選択解除します。前回の選択から開始するブロックを選択または選択解除するには、Shift キーを使用します。スケジュール ボックスの詳細については、「スケジュール ボックス」（P.5-17）を参照してください。	
Select All	1 日 24 時間、週 7 日にわたってイベントを監視するスケジュールを作成するには、[Select All] をクリックします。
Clear All	すべての選択を解除するには、[Clear All] をクリックします。
Undo All	スケジュールの編集時に、[Undo All] をクリックすると直前のスケジュールに戻ります。

ステップ 3　[Submit] をクリックしてアラーム スケジュールを保存します。

作成したスケジュールが [Threshold] ページの [Schedule] リスト ボックスに追加されます。

しきい値へのアラーム スケジュールの割り当て

アラームしきい値を作成する場合は、しきい値のアラーム スケジュールを割り当てる必要があります。アラーム スケジュールを割り当てるには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択します。

[Thresholds] ページが表示されます。

（注）　この手順では、しきい値にスケジュールを割り当てる方法についてだけ説明します。しきい値の作成、編集、または複製方法の詳細については、「アラームしきい値の作成、編集、および複製」（P.12-11）を参照してください。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 編集するしきい値の隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- 複製するしきい値の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

ステップ 3　[General] タブで、目的のスケジュールを [Schedule] ドロップダウン リスト ボックスから選択します。

ステップ 4　[Submit] をクリックしてしきい値にスケジュールを割り当てます。

アラーム スケジュールの削除

（注）　アラーム スケジュールを削除する前に、ACS で定義されているしきい値によって参照されていないことを確認します。デフォルトのスケジュール（nonstop）またはしきい値によって参照されているスケジュールは削除できません。

アラーム スケジュールを削除するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Schedules] を選択します。

[Alarm Schedules] ページが表示されます。

ステップ 2　削除するアラーム スケジュールの隣にあるチェックボックスをオンにし、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item(s)?
```

ステップ 3　アラーム スケジュールを削除するには [Yes] をクリックします。

アラーム スケジュール ページが表示されます。このとき、削除したスケジュールは表示されません。

アラームしきい値の作成、編集、および複製

このページは、各アラーム カテゴリのしきい値を設定する場合に使用します。最大 100 個のしきい値を設定できます。

アラーム カテゴリのしきい値を設定するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択します。

表 12-8 で説明する [Alarms Thresholds] ページが表示されます。

表 12-8　[Alarm Thresholds] ページ

オプション	説明
Name	アラームしきい値の名前。
Description	アラームしきい値の説明。
Category	アラームしきい値のカテゴリ。オプションは次のとおりです。 • Passed Authentications • Failed Authentications • Authentication Inactivity • TACACS Command Accounting • TACACS Command Authorization • ACS Configuration Changes • ACS System Diagnostics • ACS Process Status • ACS System Health • ACS AAA Health • RADIUS Sessions • Unknown NAD • External DB Unavailable • RBACL Drops • NAD-reported AAA Down
Last Modified Time	アラームしきい値がユーザによって最後に変更された時刻。
Last Alarm	関連付けられているアラームしきい値によってアラームが最後に生成された時刻。
Alarm Count	関連付けられているアラームが生成された回数。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するアラームの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するアラーム名をクリックします。または、変更するアラームの隣にあるチェックボックスをオンにして [Edit] をクリックします。
- イネーブルにするアラームの隣にあるチェックボックスをオンにし、[Enable] をクリックします。
- ディセーブルにするアラームの隣にあるチェックボックスをオンにし、[Disable] をクリックします。

ステップ 3　必要に応じて、[Thresholds] ページのフィールドを変更します。有効なフィールド オプションに関する情報については、以降のページを参照してください。

- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値基準の設定」（P.12-14）
- 「しきい値通知の設定」（P.12-32）

ステップ 4　[Submit] をクリックして設定を保存します。

アラームしきい値設定が保存されます。新しい設定を示す [Threshold] ページが表示されます。

関連トピック

- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値基準の設定」（P.12-14）
- 「しきい値通知の設定」（P.12-32）

一般的なしきい値情報の設定

一般的なしきい値情報を設定するには、[Thresholds] ページの [General] タブのフィールドに入力します。表 12-9 に、各フィールドを示します。

表 12-9　[General] タブ

オプション	説明
Name	しきい値の名前。
Description	（任意）しきい値の説明。
Enabled	このしきい値の実行を許可する場合に、このチェックボックスをオンにします。
Schedule	ドロップダウン リスト ボックスを使用して、しきい値を実行するスケジュールを選択します。使用可能なスケジュールのリストが表示されます。

関連トピック

- 「しきい値基準の設定」（P.12-14）
- 「しきい値通知の設定」（P.12-32）

しきい値基準の設定

ACS 5.4 には、異なるしきい値基準を定義するための次のしきい値カテゴリがあります。

- 「Passed Authentications」（P.12-14）
- 「Failed Authentications」（P.12-16）
- 「Authentication Inactivity」（P.12-18）
- 「TACACS Command Accounting」（P.12-19）
- 「TACACS Command Authorization」（P.12-20）
- 「ACS Configuration Changes」（P.12-21）
- 「ACS System Diagnostics」（P.12-22）
- 「ACS Process Status」（P.12-23）
- 「ACS System Health」（P.12-24）
- 「ACS AAA Health」（P.12-25）
- 「RADIUS Sessions」（P.12-26）
- 「Unknown NAD」（P.12-27）
- 「External DB Unavailable」（P.12-28）
- 「RBACL Drops」（P.12-29）
- 「NAD-Reported AAA Downtime」（P.12-31）

Passed Authentications

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の成功した認証が調べられます。

これらの認証レコードは、ACS Instance、User、Identity Group などの共通属性によってグループ化されています。これらの各グループ内のレコード数が計算されます。これらのグループのいずれかで計算されたカウントが、指定したしきい値を超えた場合、アラームがトリガーされます。

たとえば、Passed authentications greater than 1000 in the past 20 minutes for an ACS instance というしきい値を設定するとします。ACS がこのしきい値を評価したときに、3 つの ACS インスタンスが成功した認証を次のように処理していたとします。

ACS インスタンス	成功した認証のカウント
New York ACS	1543
Chicago ACS	879
Los Angeles	2096

この場合、過去 20 分間に少なくとも 1 つの ACS インスタンスで成功した認証が 1000 を超えているため、アラームがトリガーされます。

（注）　1 つ以上のフィルタを指定して、しきい値評価の対象となる成功した認証を制限できます。各フィルタは認証レコード内の特定の属性に関連付けられており、フィルタ値が指定した値と一致したレコードだけがカウントされます。複数のフィルタを指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

表 12-10 の説明に従って、[Criteria] タブのフィールドを変更し、成功した認証の基準を持つしきい値を作成します。

表 12-10　Passed Authentications

オプション	説明
Passed Authentications	次のようにデータを入力します。 greater than *count* > **occurrences** |**%**> in the past *time* > Minutes | Hours for a *object*。ここで、 • *count* 値は、発生の絶対数またはパーセントです。次の値が有効です。 – *count* は、greater than に対して 0 ～ 99 の範囲である必要があります。 – *count* は、lesser than に対して 1 ～ 100 の範囲である必要があります。 • **occurrences** | **%**> 値は、occurrences（発生）または % です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel 分散展開では、2 つの ACS インスタンスがある場合、カウントはインスタンスごとに絶対数またはパーセンテージとして計算されます。ACS インスタンスのいずれかの個別のカウントが、指定したしきい値を超えた場合にだけ、ACS によってアラームがトリガーされます。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。
Identity Store	[Select] をクリックして、しきい値を設定する有効な ID ストア名を選択します。
Access Service	[Select] をクリックして、しきい値を設定する有効なアクセス サービス名を選択します。
MAC Address	[Select] をクリックして、しきい値を設定する有効な MAC アドレスを選択または入力します。このフィルタは、RADIUS 認証だけに使用できます。

表 12-10　Passed Authentications （続き）

オプション	説明
NAD Port	[Select] をクリックして、しきい値を設定するネットワーク デバイスのポートを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthZ Profile	[Select] をクリックして、しきい値を設定する認可プロファイルを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthN Method	[Select] をクリックして、しきい値を設定する認証方式を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP AuthN	[Select] をクリックして、しきい値を設定する EAP 認証値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP Tunnel	[Select] をクリックして、しきい値を設定する EAP トンネル値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

Failed Authentications

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の失敗した認証が調べられます。これらの認証レコードは、ACS Instance、User、Identity Group などの共通属性によってグループ化されています。

これらの各グループ内のレコード数が計算されます。これらのグループのいずれかで計算されたカウントが、指定したしきい値を超えた場合、アラームがトリガーされます。

たとえば、Failed authentications greater than 10 in the past 2 hours for Device IP というしきい値を設定するとします。ACS がこのしきい値を評価したときに、過去 2 時間に 4 つの IP アドレスに対して失敗した認証が次のように発生していたとします。

デバイス IP	失敗した認証のカウント
a.b.c.d	13
e.f.g.h	8
i.j.k.l	1
m.n.o.p	1

この場合、過去 2 時間に少なくとも 1 つのデバイス IP で失敗した認証が 10 を超えているため、アラームがトリガーされます。

（注）　1 つ以上のフィルタを指定して、しきい値評価の対象となる失敗した認証を制限できます。各フィルタは認証レコード内の特定の属性に関連付けられており、フィルタ値が指定した値と一致したレコードだけがカウントされます。複数のフィルタを指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

表 12-11 の説明に従って、[Criteria] タブのフィールドを変更し、失敗した認証の基準を持つしきい値を作成します。

表 12-11　Failed Authentications

オプション	説明
Failed Authentications	次のようにデータを入力します。 greater than *count* > **occurrences** | **%**> in the past *time*> *Minutes*|*Hours* for a *object*。ここで、 • *count* 値は、発生の絶対数またはパーセントです。有効な値は 0 ～ 99 の範囲です。 • **occurrences** | **%**> 値は、occurrences（発生）または % です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel 分散展開では、2 つの ACS インスタンスがある場合、カウントはインスタンスごとに絶対数またはパーセンテージとして計算されます。ACS インスタンスのいずれかの個別のカウントが、指定したしきい値を超えた場合にだけ、ACS によってアラームがトリガーされます。
フィルタ	
Failure Reason	[Select] をクリックして、しきい値を設定する有効な失敗理由名を入力します。
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

表 12-11　Failed Authentications （続き）

オプション	説明
Identity Store	[Select] をクリックして、しきい値を設定する有効な ID ストア名を選択します。
Access Service	[Select] をクリックして、しきい値を設定する有効なアクセス サービス名を選択します。
MAC Address	[Select] をクリックして、しきい値を設定する有効な MAC アドレスを選択または入力します。このフィルタは、RADIUS 認証だけに使用できます。
NAD Port	[Select] をクリックして、しきい値を設定するネットワーク デバイスのポートを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthZ Profile	[Select] をクリックして、しきい値を設定する認可プロファイルを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthN Method	[Select] をクリックして、しきい値を設定する認証方式を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP AuthN	[Select] をクリックして、しきい値を設定する EAP 認証値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP Tunnel	[Select] をクリックして、しきい値を設定する EAP トンネル値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

Authentication Inactivity

このしきい値が ACS で評価される場合、過去 31 日間までの指定した時間間隔中に発生した RADIUS または TACACS+ の認証が調べられます。指定した時間間隔中に認証が行われなかった場合、アラームがトリガーされます。

指定した時間間隔中に特定の ACS インスタンスまたはデバイス IP アドレスで認証が行われなかった場合にアラームを生成するフィルタを指定できます。

認証の非アクティブしきい値で指定した時間間隔が、継続的に実行されている集約ジョブの完了にかかった時間よりも短い場合は、このアラームが抑制されます。

集約ジョブは、毎日 00:05 に開始されます。23:50 から集約ジョブが完了するまで、認証の非アクティブ アラームは抑制されます。

たとえば、本日の 01:00 に集約ジョブが完了した場合、認証の非アクティブ アラームは 23:50 から 01:00 まで抑制されます。

（注）　00:05 から 05:00 までの間に ACS をインストールした場合、または 00:05 にメンテナンスのためにアプライアンスをシャットダウンしていた場合は、認証の非アクティブ アラームが 05:00 まで抑制されます。

このカテゴリを選択して、非アクティブな認証に基づくしきい値基準を定義します。表 12-12 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-12　Authentication Inactivity

オプション	説明
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device	[Select] をクリックして、しきい値を設定する有効なデバイスを選択します。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+
Inactive for	ドロップダウン リスト ボックスを使用して、次のいずれかの有効なオプションを選択します。 • [Hours]：1 ～ 744 の範囲の時間数を指定します。 • [Days]：1 ～ 31 の範囲の日数を指定します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

TACACS Command Accounting

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信した TACACS+ アカウンティング レコードが調べられます。

1 つ以上の TACACS+ アカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は前回と今回のアラーム評価サイクルの間に受信した TACACS+ アカウンティング レコードを調べます。I

1 つ以上の TACACS+ アカウンティング レコードが、指定したコマンドまたは特権レベルと一致した場合、アラームがトリガーされます。

1 つ以上のフィルタを指定して、しきい値評価の対象となるアカウンティング レコードを制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、TACACS コマンドに基づくしきい値基準を定義します。表 12-13 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-13　TACACS Command Accounting

オプション	説明
Command	しきい値を設定する TACACS コマンドを入力します。
Privilege	ドロップダウン リスト ボックスを使用して、しきい値を設定する特権レベルを選択します。有効なオプションは次のとおりです。 • Any • 0 ～ 15 の数字。
フィルタ	
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

TACACS Command Authorization

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信した TACACS+ アカウンティング レコードが調べられます。

1 つ以上の TACACS+ アカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は前回と今回のアラーム評価サイクルの間に受信した TACACS+ 認可レコードを調べます。

1 つ以上の TACACS+ 認可レコードが、指定したコマンド、特権レベル、および成功または失敗した結果と一致した場合、アラームがトリガーされます。

1 つ以上のフィルタを指定して、しきい値評価の対象となる認可レコードを制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、TACACS コマンド認可プロファイルに基づくしきい値基準を定義します。表 12-14 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-14　TACACS Command Authorization

オプション	説明
Command	しきい値を設定する TACACS コマンドを入力します。
Privilege	ドロップダウン リスト ボックスを使用して、しきい値を設定する特権レベルを選択します。有効なオプションは次のとおりです。 • Any • 0 ～ 15 の数字。

表 12-14　TACACS Command Authorization （続き）

オプション	説明
Authorization Result	ドロップダウン リスト ボックスを使用して、しきい値を設定する認可結果を選択します。有効なオプションは次のとおりです。 • Passed • Failed
フィルタ	
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS Configuration Changes

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信したアカウンティング レコードが調べられます。

1 つ以上のアカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は前回と今回のアラーム評価サイクルの間に行われた ACS 設定変更を調べます。1 つ以上の変更が行われていた場合、アラームがトリガーされます。

1 つ以上のフィルタを指定して、しきい値評価の対象となる設定変更を制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ACS インスタンスで行われた設定変更に基づくしきい値基準を定義します。表 12-15 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-15　ACS Configuration Changes

オプション	説明
Administrator	[Select] をクリックして、しきい値を設定する有効な管理者ユーザ名を選択します。
Object Name	しきい値を設定するオブジェクトの名前を入力します。
Object Type	[Select] をクリックして、しきい値を設定する有効なオブジェクト タイプを選択します。

表 12-15　ACS Configuration Changes （続き）

オプション	説明
Change	ドロップダウン リスト ボックスを使用して、しきい値を設定する管理変更を選択します。有効なオプションは次のとおりです。 • Any • [Create] :「複製」および「編集」管理アクションを含みます。 • Update • Delete
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS System Diagnostics

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信したアカウンティング レコードが調べられます。

1 つ以上のアカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は時間間隔中に監視対象の ACS が生成したシステム診断レコードを調べます。

1 つ以上の診断が指定したセキュリティ レベル以上で生成されていた場合、アラームがトリガーされます。1 つ以上のフィルタを指定して、しきい値評価の対象となるシステム診断レコードを制限できます。

各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ACS インスタンスのシステム診断に基づくしきい値基準を定義します。表 12-16 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-16　ACS System Diagnostics

オプション	説明
Severity at and above	ドロップダウン リスト ボックスを使用して、しきい値を設定する重大度レベルを選択します。この設定により、しきい値で指定した重大度レベルおよびそれよりも上の重大度レベルが取得されます。有効なオプションは次のとおりです。 • Fatal • Error • Warning • Info • Debug
Message Text	しきい値を設定するメッセージ テキストを入力します。最大文字数は 1024 文字です。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS Process Status

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信したアカウンティング レコードが調べられます。

1 つ以上のアカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS はその時間中にいずれかの ACS プロセスが失敗したかどうかを調べます。

ACS が 1 つ以上の失敗を検出した場合、アラームがトリガーされます。特定のプロセス、特定の ACS インスタンス、またはその両方のチェックに制限できます。

このカテゴリを選択して、ACS プロセス ステータスに基づくしきい値基準を定義します。表 12-17 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-17　ACS Process Status

オプション	説明
Monitor Processes	
ACS Database	ACS データベースをしきい値設定に追加する場合に、このチェックボックスをオンにします。
ACS Management	ACS 管理をしきい値設定に追加する場合に、このチェックボックスをオンにします。
ACS Runtime	ACS ランタイムをしきい値設定に追加する場合に、このチェックボックスをオンにします。
Monitoring and Reporting Database	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。

表 12-17　ACS Process Status （続き）

オプション	説明
Monitoring and Reporting Collector	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
Monitoring and Reporting Alarm Manager	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
Monitoring and Reporting Job Manager	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
Monitoring and Reporting Log Processor	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS System Health

このしきい値が ACS で評価される場合、いずれかのシステム健全性パラメータが、過去 60 分間までの指定した時間間隔中に、指定したしきい値を超えたかどうかが調べられます。これらの健全性パラメータには、CPU 使用率やメモリ消費率などが含まれます。

パラメータのいずれかが指定したしきい値を超えた場合、アラームがトリガーされます。デフォルトでは、しきい値は展開されているすべての ACS インスタンスに適用されます。必要に応じて、1 つの ACS インスタンスだけにチェックを制限できます。

このカテゴリを選択して、ACS のシステム健全性に基づくしきい値基準を定義します。表 12-18 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-18　ACS System Health

オプション	説明
Average over the past	ドロップダウン リスト ボックスを使用して、設定に対して設定する時間を選択します。<min> は分で、次のいずれかです。 • 15 • 30 • 45 • 60
CPU	しきい値設定に対して設定する CPU 使用率を入力します。有効な範囲は 1 ～ 100 です。
Memory	しきい値設定に対して設定するメモリ使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk I/O	しきい値設定に対して設定するディスク使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。

表 12-18　ACS System Health （続き）

オプション	説明
Disk Space Used/opt	しきい値設定に対して設定する /opt ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk Space Used/local disk	しきい値設定に対して設定するローカル ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk Space Used/	しきい値設定に対して設定する / ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk Space Used/tmp	しきい値設定に対して設定する一時ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS AAA Health

このしきい値が ACS で評価される場合、いずれかの ACS 健全性パラメータが、過去 60 分間までの指定した時間間隔中に、指定したしきい値を超えたかどうかが調べられます。ACS は次のパラメータを監視します。

- RADIUS Throughput
- TACACS Throughput
- RADIUS Latency
- TACACS Latency

パラメータのいずれかが指定したしきい値を超えた場合、アラームがトリガーされます。デフォルトでは、しきい値は展開されているすべての監視対象 ACS インスタンスに適用されます。必要に応じて、1 つの ACS インスタンスだけにチェックを制限できます。

表 12-19 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-19　ACS AAA Health

オプション	説明
Average over the past	ドロップダウン リスト ボックスを使用して、設定に対して設定する時間を選択します。<min> は分で、次のいずれかです。 • 15 • 30 • 45 • 60
RADIUS Throughput	しきい値設定に対して設定する 1 秒あたりの RADIUS トランザクション数（指定した値以下）を入力します。有効な範囲は 1 ～ 999999 です。
TACACS Throughput	しきい値設定に対して設定する 1 秒あたりの TACACS トランザクション数（指定した値以下）を入力します。有効な範囲は 1 ～ 999999 です。
RADIUS Latency	しきい値設定に対して設定する RADIUS 遅延（指定した値以上）をミリ秒単位で入力します。有効な範囲は 1 ～ 999999 です。
TACACS Latency	しきい値設定に対して設定する TACACS+ 遅延（指定した値以上）をミリ秒単位で入力します。有効な範囲は 1 ～ 999999 です。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

RADIUS Sessions

このしきい値が ACS で評価される場合、セッションのアカウンティング開始イベントが受信されていない認証済み RADIUS セッションが過去 15 分間に発生したかどうかが判断されます。これらのイベントは、デバイス IP アドレスでグループ化され、いずれかのデバイス IP に対する発生カウントが指定したしきい値を超過した場合にアラームがトリガーされます。フィルタを設定して、評価を 1 つのデバイス IP に制限できます。

このカテゴリを選択して、RADIUS セッションに基づくしきい値基準を定義します。表 12-20 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-20　RADIUS Sessions

オプション	説明
More than *num* authenticated sessions in the past 15 minutes, where accounting start event has not been received for a Device IP	*num*：過去 15 分間の認証済みセッションの数。

表 12-20　RADIUS Sessions （続き）

オプション	説明
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。

Unknown NAD

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の失敗した認証が調べられます。これらの失敗した認証から、ACS は失敗理由が [Unknown NAD] である認証を識別します。

未知のネットワーク アクセス デバイス（NAD）認証レコードは、ACS インスタンス、ユーザなどの共通属性によってグループ化され、各グループ内のレコード カウントが計算されます。いずれかのグループのレコード カウントが指定したしきい値を超えた場合、アラームがトリガーされます。これは、たとえば、しきい値を次のように設定した場合に発生します。

Unknown NAD count greater than 5 in the past 1 hour for a Device IP

過去 1 時間に未知の NAD の失敗理由で失敗した認証が 2 つの異なるデバイス IP アドレスに対して次の表のように発生した場合は、少なくとも 1 つのデバイス IP アドレスのカウントが 5 を超えているためアラームがトリガーされます。

デバイス IP	未知の NAD 認証レコードのカウント
a.b.c.d	6
e.f.g.h	1

1 つ以上のフィルタを指定して、しきい値評価の対象となる失敗した認証を制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、未知の NAD により失敗した認証に基づくしきい値基準を定義します。表 12-21 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-21　Unknown NAD

オプション	説明
Unknown NAD count	greater than *num* in the past *time Minutes|Hours* for a *object*。ここで、 • *num* 値は、ゼロ（0）以上の 5 桁の任意の数字です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – Device IP
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

External DB Unavailable

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の失敗した認証が調べられます。

これらの失敗した認証から、ACS は失敗理由が [External DB unavailable] である認証を識別します。この失敗理由を持つ認証レコードは、ACS インスタンス、ユーザなどの共通属性によってグループ化され、各グループ内のレコード カウントが計算されます。

いずれかのグループのレコード カウントが指定したしきい値を超えた場合、アラームがトリガーされます。これは、たとえば、しきい値を次のように設定した場合に発生します。

デバイス IP の過去 1 時間の [External DB Unavailable] 数が 5 よりも大きい

過去 1 時間に [External DB Unavailable] の失敗理由で失敗した認証が 2 つの異なるデバイス IP アドレスに対して次の表のように発生した場合は、少なくとも 1 つのデバイス IP アドレスのカウントが 5 を超えているためアラームがトリガーされます。

デバイス IP	外部 DB が使用不能な認証レコードのカウント
a.b.c.d	6
e.f.g.h	1

1 つ以上のフィルタを指定して、しきい値評価の対象となる失敗した認証を制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ACS が接続できない外部データベースに基づくしきい値基準を定義します。表 12-22 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-22　External DB Unavailable

オプション	説明
External DB Unavailable	*percent*|*count* greater than *num* in the past *time Minutes*|*Hours* for a *object*。ここで、 • Percent|Count 値は Percent（パーセント）または Count（カウント）です。 • *num* 値は次のいずれかです。 – パーセントの場合は 0 ～ 99 – カウントの場合は 0 ～ 99999 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – Identity Store
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Identity Store	[Select] をクリックして、しきい値を設定する有効な ID ストア名を選択します。
Access Service	[Select] をクリックして、しきい値を設定する有効なアクセス サービス名を選択します。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

RBACL Drops

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した Cisco Security Group Access RBACL ドロップが調べられます。RBACL ドロップ レコードは、NAD、SGT などの特定の共通属性によってグループ化されます。

これらの各グループ内のこのようなレコードのカウントが計算されます。いずれかのグループのカウントが指定したしきい値を超えた場合、アラームがトリガーされます。たとえば、次のしきい値設定について考えます。

SGT による過去 4 時間の [RBACL Drops] が 10 よりも大きい

過去 4 時間に RBACL ドロップが 2 つの異なる送信元グループ タグに対して次の表のように発生した場合は、少なくとも 1 つの SGT のカウントが 10 を超えているためアラームがトリガーされます。

SGT	RBACL ドロップのカウント
1	17
3	14

1 つ以上のフィルタを指定して、しきい値評価の対象となる RBACL ドロップ レコードを制限できます。各フィルタは RBACL ドロップ レコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

表 12-23 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-23　RBACL Drops

オプション	説明
RBACL drops	greater than *num* in the past *time Minutes|Hours* by a *object*。ここで、 • *num* 値は、ゼロ（0）以上の 5 桁の任意の数字です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – NAD – SGT – DGT – DST_IP
フィルタ	
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
SGT	[Select] をクリックして、しきい値を設定する有効な送信元グループ タグを選択または入力します。
DGT	[Select] をクリックして、しきい値を設定する有効な宛先グループ タグを選択または入力します。
Destination IP	[Select] をクリックして、しきい値を設定する有効な宛先 IP アドレスを選択または入力します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

NAD-Reported AAA Downtime

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した NAD レポート AAA ダウン イベントが調べられます。AAA ダウン レコードは、IP アドレスやデバイス グループなどの特定の共通属性によってグループ化され、各グループ内のレコード カウントが計算されます。

いずれかのグループのカウントが指定したしきい値を超えた場合、アラームがトリガーされます。たとえば、次のしきい値設定について考えます。

AAA Down count greater than 10 in the past 4 hours by a Device IP

過去 4 時間に NAD レポート AAA ダウン イベントが 3 つの異なるデバイス IP アドレスに対して次の表のように発生した場合は、少なくとも 1 つのデバイス IP アドレスのカウントが 10 を超えているためアラームがトリガーされます。

デバイス IP	NAD レポート AAA ダウン イベントのカウント
a.b.c.d	15
e.f.g.h	3
i.j.k.l	9

1 つ以上のフィルタを指定して、しきい値評価の対象となる AAA ダウン レコードを制限できます。各フィルタは AAA ダウン レコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ネットワーク アクセス デバイスがレポートする AAA ダウンタイムに基づくしきい値基準を定義します。表 12-24 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-24　NAD-Reported AAA Downtime

オプション	説明
AAA down	greater than *num* in the past *time Minutes|Hours* by a *object*。ここで、 • *num* 値は、ゼロ（0）以上の 5 桁の任意の数字です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – Device IP – Device Group

表 12-24　NAD-Reported AAA Downtime （続き）

オプション	説明
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

しきい値通知の設定

このページは、アラームしきい値通知を設定する場合に使用します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択し、次のいずれかを実行します。

- [Create] をクリックして、新しいアラームしきい値を作成します。
- アラームしきい値の名前をクリックするか、既存のアラームしきい値の隣にあるチェックボックスをオンにし、[Edit] をクリックして、選択したアラームしきい値を編集します。
- アラームしきい値の名前をクリックするか、既存のアラームしきい値の隣にあるチェックボックスをオンにし、[Duplicate] をクリックして、選択したアラームしきい値を複製します。

ステップ 2　[Notifications] タブをクリックします。

表 12-25 で説明する [Thresholds: Notifications] ページが表示されます。

表 12-25　[Thresholds: Notifications] ページ

オプション	説明
Severity	ドロップダウン リスト ボックスを使用して、アラームしきい値の重大度レベルを選択します。有効なオプションは次のとおりです。 • Critical • Warning • Info
Send Duplicate Notifications	重複するアラームを通知する場合に、このチェックボックスをオンにします。同じしきい値に対して以前に生成されたアラームが現在のアラームに対して指定された時間枠内に発生した場合は、アラームが重複と見なされます。

表 12-25　[Thresholds: Notifications] ページ （続き）

オプション	説明
Email Notification	
Email Notification User List	電子メール アドレスまたは ACS 管理者名あるいはその両方のカンマ区切りリストを入力します。次のいずれかを実行します。 • 電子メール アドレスを入力します。 • [Select] をクリックして、有効な ACS 管理者名を入力します。管理者設定に電子メール識別情報が指定されている場合にだけ、関連付けられた管理者に電子メールで通知されます。詳細については、「管理者アカウントの作成、複製、編集、および削除」（P.16-7）を参照してください。 しきい値アラームが発生した場合は、[Email Notification User List] 内のすべての受信者に電子メールが送信されます。 このフィールドをクリアするには、[Clear] をクリックします。
Email in HTML Format	電子メール通知を HTML 形式で送信する場合は、このチェックボックスをオンにします。電子メール通知をプレーン テキストで送信する場合は、このチェックボックスをオフにします。
Custom Text	アラームしきい値に関連付けるカスタム テキスト メッセージを入力します。
Syslog Notification	
Send Syslog Message	ACS で生成される各システム アラームの syslog メッセージを送信する場合に、このチェックボックスをオンにします。 **（注）** ACS で syslog メッセージを正常に送信するには、[Alarm Syslog Targets] を設定する必要があります。これは、syslog メッセージの宛先です。詳細については、「アラーム Syslog ターゲットについて」（P.12-35）を参照してください。

関連トピック

- 「受信ボックスでのアラームの表示および編集」（P.12-3）
- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「アラームしきい値の削除」（P.12-33）

アラームしきい値の削除

アラームしきい値を削除するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択します。

[Alarms Thresholds] ページが表示されます。

ステップ 2　削除するしきい値の隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

ステップ 3　[OK] をクリックして、選択したアラームを削除することを確認します。

[Alarms Thresholds] ページが表示されます。このとき、削除されたしきい値は表示されません。

システム アラーム設定の設定

システム アラームは、次の情報をユーザに通知するために使用されます。

- Monitoring and Reporting サービスで発生したエラー
- データの削除に関する情報

このページは、システム アラームをイネーブルにしたり、アラーム通知の送信先を指定したりする場合に使用します。システム アラームをイネーブルにした場合は、アラームが [Alarms Inbox] に送信されます。また、選択した受信者にアラーム通知を電子メールで送信することや、アラーム syslog ターゲットとして指定された宛先に syslog メッセージとして送信することを選択できます。

Monitoring and Report Viewer から、[Monitoring Configuration] > [System Configuration] > [System Alarm Settings] を選択します。

表 12-26　[System Alarm Settings] ページ

オプション	説明
System Alarm Settings	
Notify System Alarms	システム アラーム通知をイネーブルにする場合に、このチェックボックスをオンにします。
System Alarms Suppress Duplicates	ドロップダウン リスト ボックスを使用して、重複するシステム アラームが [Email Notification User List] に送信されないようにする時間数を指定します。有効なオプションは、1、2、4、6、8、12、および 24 です。
Email Notification	
Email Notification User List	電子メール アドレスまたは ACS 管理者名あるいはその両方のカンマ区切りリストを入力します。次のいずれかを実行します。 • 電子メール アドレスを入力します。 • [Select] をクリックして、有効な ACS 管理者名を入力します。管理者設定に電子メール識別情報が指定されている場合にだけ、関連付けられた管理者に電子メールで通知されます。詳細については、「管理者アカウントの作成、複製、編集、および削除」（P.16-7）を参照してください。 システム アラームが発生した場合は、[Email Notification User List] 内のすべての受信者に電子メールが送信されます。 このフィールドをクリアするには、[Clear] をクリックします。
Email in HTML Format	電子メール通知を HTML 形式で送信する場合は、このチェックボックスをオンにします。電子メール通知をプレーン テキストで送信する場合は、このチェックボックスをオフにします。
Syslog Notification	
Send Syslog Message	ACS で生成される各システム アラームの syslog メッセージを送信する場合に、このチェックボックスをオンにします。 ACS で syslog メッセージを正常に送信するには、[Alarm Syslog Targets] を設定する必要があります。これは、syslog メッセージの宛先です。詳細については、「アラーム Syslog ターゲットについて」（P.12-35）を参照してください。

ここでは、次の内容について説明します。

- 「アラーム Syslog ターゲットの作成と編集」（P.12-35）
- 「アラーム Syslog ターゲットの削除」（P.12-36）

アラーム Syslog ターゲットについて

アラーム syslog ターゲットは、アラーム syslog メッセージが送信される宛先です。Monitoring and Report Viewer は、syslog メッセージの形式でアラーム通知を送信します。これらの syslog メッセージを受信するように、syslog サーバを実行するマシンを設定する必要があります。

設定した syslog ターゲットのリストを表示するには、[Monitoring Configuration] > [System Configuration] > [Alarm Syslog Targets] を選択します。

（注）　Monitoring and Report Viewer で、最大 2 つの syslog ターゲットを設定できます。

ここでは、次の内容について説明します。

- 「アラーム Syslog ターゲットの作成と編集」（P.12-35）
- 「アラーム Syslog ターゲットの削除」（P.12-36）

アラーム Syslog ターゲットの作成と編集

アラーム syslog ターゲットを作成または編集するには、次の手順を実行します。

ステップ 1　[Monitoring Configuration] > [System Configuration] > [Alarm Syslog Targets] を選択します。

[Alarm Syslog Targets] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 編集するアラーム syslog ターゲットの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[Alarm Syslog Targets Create or Edit] ページが表示されます。

ステップ 3　表 12-27 で説明されているフィールドを変更します。

表 12-27　[Alarm Syslog Targets Create or Edit] ページ

オプション	説明
ID	
Name	アラーム syslog ターゲットの名前。名前は最大 255 文字です。
Description	（任意）作成するアラームの簡単な説明。説明は最大 255 文字です。
Configuration	
IP Address	syslog メッセージを受信するマシンの IP アドレス。このマシンでは、syslog サーバを実行している必要があります。Windows または Linux マシンを使用して syslog メッセージを受信することを推奨します。

表 12-27　[Alarm Syslog Targets Create or Edit] ページ （続き）

オプション	説明
Use Advanced Syslog Options	
Port	リモート syslog サーバが受信するポート。デフォルトでは、514 に設定されます。有効なオプションは 1 ～ 65535 です。
Facility Code	ロギングに使用する Syslog ファシリティ コード。有効なオプションは、Local0 ～ Local7 です。

ステップ 4　[Submit] をクリックします。

関連トピック

- 「アラーム Syslog ターゲットについて」（P.12-35）
- 「アラーム Syslog ターゲットの削除」（P.12-36）

アラーム Syslog ターゲットの削除

（注）　デフォルトの *nonstop* スケジュールは削除できません。

アラーム syslog ターゲットを削除するには、次の手順を実行します。

ステップ 1　[Monitoring Configuration] > [System Configuration] > [Alarm Syslog Targets] を選択します。

[Alarm Syslog Targets] ページが表示されます。

ステップ 2　削除するアラーム syslog ターゲットの隣にあるチェックボックスをオンにし、[Delete] をクリックします。

次のメッセージが表示されます。

```
Do you want to delete the selected item(s)?
```

ステップ 3　[Yes] をクリックします。

[Alarm Syslog Targets] ページが表示されます。このとき、削除したアラーム syslog ターゲットは表示されません。

CHAPTER 13

レポートの管理

ACS の Monitoring and Report Viewer コンポーネントでは、展開されたさまざまな ACS サーバからログおよび設定データが収集され、それらが集約されて、データの分析に役立つインタラクティブなレポートが提供されます。Monitoring and Report Viewer には、ネットワークを効率的に管理し、ネットワーク関連の問題のトラブルシューティングを行うための、統合された監視、レポート、およびトラブルシューティング機能が備えられています。

Monitoring and Report Viewer には、展開されたすべての ACS サーバの健全性を監視するために使用できる強力なダッシュボードが用意されています。ダッシュボードでは、ネットワークを効率的に管理するために使用できる、ネットワーク アクセス パターンおよびトラフィックの傾向についての情報も提供されます。

Monitoring and Report Viewer によって、リアルタイムのデータや重要な統計情報が提供されます。これらは、ネットワークを予防的に管理して、攻撃を防ぐために役立ちます。

ACS には、事前に定義済みのレポートがいくつか用意されています。これらのレポートを実行することによって、ACS サーバから取得されたログおよび設定データに含まれている重要な情報を入手できます。表 13-2 に、ACS で使用可能なさまざまなカテゴリのレポートを示します。

これらのレポートでは、認証、セッション トラフィック、デバイス管理、ACS サーバ設定および管理、およびトラブルシューティングに関連する情報が提供されます。これらのレポートは、表、グラフ、または図として表示され、さらに詳細なデータにドリルダウンすることもできます。

さらに、ACS では、次の操作を行うこともできます。

- 各自の要件に基づいた、レポートのデータのフィルタリング
- CSV 形式でのレポートのエクスポート、およびその印刷
- お気に入りリストへのレポートの追加、およびお気に入りリストからレポートへの簡単なアクセス
- 他のユーザとのレポートの共有
- Interactive Viewer を使用したレポートのカスタマイズ

[Monitoring and Reports] ドロワがプライマリ Web インターフェイス ウィンドウに表示されます。このドロワには、[Launch Monitoring and Report Viewer] オプションがあります。

セカンダリ Web インターフェイス ウィンドウに Monitoring and Report Viewer を開くには、[Launch Monitoring and Report Viewer] をクリックします。セカンダリ Web インターフェイス ウィンドウには、次のドロワが含まれています。

- Monitoring and Reports
- Monitoring Configuration （「Monitoring and Report Viewer でのシステムの動作と設定の管理」（P.15-1）を参照）。

レポートは、次のいずれかのページから実行できます。

- Favorites：[Monitoring and Reports] > [Reports] > [Favorites]

- Shared：[Monitoring and Reports] > [Reports] > [Shared]
- Catalog：[Monitoring and Reports] > [Reports] > [Catalog] > *<report_type>*

簡単にアクセスするために、レポートを [Favorites] ページに追加できます。このページから、レポートをカスタマイズしたり、削除したりできます。グループ内で共有する必要があるレポートをカスタマイズして、[Shared] ページに追加できます。[Catalog] の下のページには、展開された ACS サーバから取得されたログ、診断、およびトラブルシューティング データについてのさまざまなレポートが用意されています。

これらのページには、次のタイプのレポートがあります。

- システム レポート：ACS ソフトウェアに事前に定義されているレポート。システム レポートのリストは、[Reports] > [Catalog] の下のページで表示できます。
- カスタマイズされたレポート：設定して保存したシステム レポート（「レポートのカスタマイズ」（P.13-20）を参照）。

（注）　Internet Explorer（IE）7.0 では、IE 7.0 の新機能であるフィッシング フィルタのために、レポートのパフォーマンスが低下します。この問題を解決するには、Microsoft 社から最新のセキュリティ更新プログラムを入手してください。このことに関する詳細については、次の URL を参照してください。
http://support.microsoft.com/kb/928089/

また、ACS 5.4 では、新しいレポートである [RADIUS Active Sessions] レポートを介した動的な認可変更（CoA）機能が導入されています。この機能を使用すると、アクティブな RADIUS セッションを動的に制御できます。この機能を使用して、次の目的で再認証または接続解除要求を NAD に送信できます。

- 認証に関連する問題のトラブルシューティング：[Disconnect:None] オプションを使用して、再認証を試みることができます。

  アクセスを制限するために接続解除オプションを使用しないでください。アクセスを制限するには、シャットダウン オプションを使用します。
- 問題のあるホストのブロック：[Disconnect:Port Disable] オプションを使用して、ネットワークに大量のトラフィックを送信する、ウイルスなどに感染したホストをブロックできます。

  RADIUS プロトコルでは、シャットダウンされたポートを再度イネーブルにするための方法は現在サポートされていません。
- エンドポイントでの IP アドレス再取得の強制：サプリカントまたはクライアントを持たないエンドポイントに対して [Disconnect:Port Bounce] オプションを使用し、VLAN 変更後に DHCP 要求を生成できます。
- エンドポイントへの更新された認可ポリシーのプッシュ：[Re-Auth] オプションを使用して、管理者の裁量に基づいた既存のセッションの認可ポリシーの変更などの、更新されたポリシー設定を適用できます。

  たとえば、ポスチャ確認がイネーブルである場合にエンドポイントが最初にアクセスを許可されると、通常、エンドポイントは隔離されます。エンドポイントの ID およびポスチャが確認されたあと、CoA Re-Auth コマンドをエンドポイントに送信して、エンドポイントがそのポスチャに基づいて実際の認可ポリシーを取得できるようにすることが可能です。

従来の NAS デバイスでは、CoA 機能はサポートされていません。シスコでは、NPF プログラムの一環として、すべてのデバイスで CoA をサポートすることを計画しています。

（注）　デバイスによって CoA コマンドが正しく認識されるためには、適切にオプションを設定することが重要です。

CoA 機能が適切に動作するには、認可を動的に変更するすべてのデバイスの共有秘密情報を ACS に設定する必要があります。ACS では、デバイスからのアクセス要求、およびデバイスへの CoA コマンドの発行の両方において、共有秘密情報設定が使用されます。

詳細については、「認可の変更、およびアクティブな RADIUS セッションの接続解除」（P.13-18）を参照してください。

この章では、次の内容について詳細に説明します。

- 「お気に入りレポートの使用」（P.13-3）
- 「レポートの共有」（P.13-7）
- 「カタログ レポートの使用」（P.13-7）
- 「レポートの表示」（P.13-21）
- 「Interactive Viewer におけるレポートのフォーマット」（P.13-28）
- 「レポート データの構成」（P.13-42）
- 「レポート データの非表示およびフィルタリング」（P.13-67）
- 「グラフについて」（P.13-76）

お気に入りレポートの使用

頻繁に使用するレポートを [Favorites] ページに追加すると、それらのお気に入りレポートを表示するために毎回メニューからレポートに移動する必要がなくなります。Monitoring and Report Viewer では、次のことを実行できます。

- 各お気に入りレポートに設定されているパラメータの表示
- レポート実行前のパラメータの編集

たとえば、レポートをお気に入りのリストに追加すると、次に同じレポートを異なるパラメータのセットを使用して表示する場合に、新たにレポートを作成する必要がありません。単にお気に入りレポートのパラメータを編集することによって、異なるパラメータを使用したレポートを生成できます。

ここでは、次の内容について説明します。

- 「[Favorites] ページへのレポートの追加」（P.13-3）
- 「お気に入りレポートのパラメータの表示」（P.13-4）
- 「お気に入りレポートの編集」（P.13-5）
- 「お気に入りレポートの実行」（P.13-6）
- 「お気に入りからのレポートの削除」（P.13-6）

[Favorites] ページへのレポートの追加

お気に入りの Web サイトをブラウザにブックマークするのと同じように、頻繁にアクセスするレポートのお気に入りリストを作成できます。

[Favorites] ページにレポートを追加するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Catalog] > *report_type* を選択します。*report_type* は、レポートのタイプです。

選択したレポート タイプで使用可能なレポートが表示されます。

ステップ 2　お気に入りに追加するレポートの隣にあるオプション ボタンをクリックします。有効なフィールド オプションについては、表 13-5 を参照してください。

ステップ 3　[Add to Favorites] をクリックします。

[Add to Favorite] ページが表示されます。

ステップ 4　必要に応じて、[Add to Favorites] ページのフィールドを変更します。

ステップ 5　[Add to Favorite] をクリックします。

[Favorites] ページにレポートが追加されます。

関連トピック

- 「お気に入りレポートの使用」（P.13-3）
- 「お気に入りレポートのパラメータの表示」（P.13-4）
- 「お気に入りレポートの編集」（P.13-5）
- 「お気に入りからのレポートの削除」（P.13-6）
- 「report_name ページについて」（P.13-15）

お気に入りレポートのパラメータの表示

お気に入りレポートを実行する前に、設定されているパラメータを表示して、それらを編集できます。お気に入りレポートのパラメータを表示するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Favorites] を選択します。

[Favorites] ページが表示され、お気に入りレポートのリストが示されます。

ステップ 2　パラメータを表示するお気に入りレポートの隣にあるチェックボックスをオンにし、[Parameters] をクリックします。

図 13-1 に示すようなウィンドウが表示され、お気に入りレポートのパラメータおよびその値がリストされます。

図 13-1　お気に入りレポートのパラメータの表示

ステップ 3　[Cancel] をクリックするか、またはパラメータ ウィンドウの右上隅にある [Close] ボタンをクリックして、[Favorites] ページに戻ります。

お気に入りレポートの編集

お気に入りレポートの既存のパラメータを表示したあと、それらを編集できます。お気に入りレポートのパラメータを編集するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Favorites] を選択します。

[Favorites] ページが表示され、お気に入りレポートのリストが示されます。

ステップ 2　編集するお気に入りレポートの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[Edit Favorite Report] ページが表示されます。

ステップ 3　[Edit Favorite Report] ページで、さまざまなパラメータの値を編集します。

ステップ 4　次のいずれかをクリックします。

- 変更内容を保存する場合は [Edit Favorite]。
- 値をリセットする場合は [Reset]。
- 変更をキャンセルして、[Favorites] ページに戻る場合は [Cancel]。

お気に入りレポートを編集した場合、Monitoring and Report Viewer では、お気に入りレポートが正常に編集されたことを示すステータス メッセージが [Favorite] ページに表示されます。

関連トピック

- 「[Favorites] ページへのレポートの追加」（P.13-3）
- 「お気に入りレポートのパラメータの表示」（P.13-4）

- 「お気に入りレポートの実行」（P.13-6）
- 「report_name ページについて」（P.13-15）

お気に入りレポートの実行

[Favorites] ページのレポートを実行するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Favorites] を選択します。

[Favorites] ページが表示され、表 13-1 で説明されているフィールドが表示されます。

表 13-1　[Favorites] ページ

オプション	説明
Favorite Name	お気に入りレポートの名前。クリックすると、関連付けられているレポートの概要が表示されます。
Report Name	カタログ（レポート）タイプに関連付けられているレポート名。
Report Type	レポートに関連付けられている、一般的なグループ名。

ステップ 2　次のいずれかを実行します。

- 実行するレポート名の隣にあるチェックボックスをオンにし、[Run] をクリックします。
- 実行するレポート名をクリックします。

ページに、レポートが生成されます。

ステップ 3　その他のオプションについては、[Launch Interactive Viewer] をクリックします。

関連トピック

- 「[Favorites] ページへのレポートの追加」（P.13-3）
- 「お気に入りレポートのパラメータの表示」（P.13-4）
- 「お気に入りレポートの実行」（P.13-6）
- 「report_name ページについて」（P.13-15）

お気に入りからのレポートの削除

（注）　[Favorites] ページからシステム レポートを削除しても、そのシステム レポートは該当する [Reports] > [Catalog] の下のページには残っています。

[Favorites] ページからレポートを削除するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Favorites] を選択します。

ステップ 2　削除するレポートの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

ステップ 3　[OK] をクリックして、選択したレポートを削除することを確定します。

[Favorites] ページが表示されます。このとき、削除したレポートは表示されません。

レポートの共有

Shared フォルダにレポートを追加して、すべてのユーザが使用できるようにすることができます。Shared フォルダにレポートを追加するには、次の手順を実行します。

ステップ 1　共有するレポートを選択します。

たとえば、[ACS Health Summary] レポートを共有するには、[Monitoring and Reports] > [Reports] > [Catalog] > [ACS Instance] を選択します。

[ACS Instance reports] ページが表示されます。

ステップ 2　レポートを実行します。詳細については、「カタログ レポートの実行」（P.13-12）を参照してください。

この例では、[ACS Health Summary] レポートが表示されます。

ステップ 3　Interactive Viewer でレポートを起動します。

ステップ 4　[Interactive Viewer] ページの左上隅にある [Save] アイコンをクリックします。

[Save] ウィンドウが表示されます。

ステップ 5　[Choose a Folder] リスト ボックスから、Shared フォルダを選択します。

ステップ 6　任意のファイル名を入力します。

ステップ 7　[Save] をクリックします。

レポートが Shared フォルダに保存され、すべてのユーザが使用できるようになります。

（注）　ACS の以前のバージョンで作成した共有レポートは、ACS の旧バージョンを ACS 5.4 にアップグレードするか、ACS 5.4 を新規インストールすると機能しなくなります。そのため、共有レポートを削除し、ACS 5.4 で追加する必要があります。

カタログ レポートの使用

カタログ レポートは、ACS に事前に定義されているシステム レポートです。この項の構成は、次のとおりです。

- 「カタログで使用可能なレポート」（P.13-8）
- 「カタログ レポートの実行」（P.13-12）
- 「カタログ レポートの削除」（P.13-13）
- 「名前付きレポートの実行」（P.13-13）
- 「認可の変更、およびアクティブな RADIUS セッションの接続解除」（P.13-18）
- 「レポートのカスタマイズ」（P.13-20）
- 「レポートの復元」（P.13-20）

カタログで使用可能なレポート

表 13-2 に、[Monitoring and Reports] を選択し、Monitoring and Report Viewer を起動して、[Monitoring and Reports] > [Reports] > [Catalog] を選択した場合に使用可能なレポートを示します。

表 13-2　使用可能な ACS レポート

レポート名	説明	ロギング カテゴリ
AAA Protocol		
AAA diagnostics	選択された期間における、重大度に基づいた AAA 診断の詳細が提供されます。	ポリシー診断、ID ストア診断、認証フロー診断、RADIUS 診断、TACACS+ 診断
Authentication Trend	選択された期間における RADIUS および TACACS+ 認証概要情報がグラフ表示とともに提供されます。	成功した認証、失敗した試行
RADIUS Accounting	選択された期間における、RADIUS に基づいたユーザ アカウンティング情報が提供されます。	RADIUS アカウンティング
RADIUS Authentication	選択された期間における、RADIUS 認証の詳細が提供されます。	成功した認証、失敗した試行
TACACS Accounting	選択された期間における、TACACS+ 認証のユーザまたはコマンド アカウンティング情報が提供されます。	TACACS アカウンティング
TACACS Authentication	選択された期間における、TACACS+ 認証の詳細が提供されます。	成功した認証、失敗した試行
TACACS Authorization	選択された期間における、TACACS+ 認可の詳細が提供されます。	成功した認証、失敗した試行
Access Service		
Access Service Authentication Summary	選択された期間における特定のアクセス サービスの RADIUS および TACACS+ 認証概要情報がグラフ表示とともに提供されます。	成功した認証、失敗した試行
Top N Authentications By Access Service	選択された期間における RADIUS および TACACS+ の認証について、アクセス サービス別の上位 N の成功した認証数、失敗した認証数、および合計認証数が提供されます。	成功した認証、失敗した試行
ACS Instance		
ACS Administrator Entitlement	ACS における管理者のロール、および次の内容が示されます。 • ACS において管理者がアクセスを許可されているタスク • これらの各操作において管理者が付与されている特権	なし
ACS Administrator Logins	ログイン、ログアウト、イベント、失敗したログイン試行の理由を含む、管理者のアクセス関連イベントが提供されます。	管理および操作の監査
ACS Configuration Audit	選択された期間における、管理者が ACS で行ったすべての設定変更が提供されます。	管理および操作の監査

表 13-2　使用可能な ACS レポート （続き）

レポート名	説明	ロギング カテゴリ
ACS Health Summary	CPU とメモリの使用率、RADIUS と TACACS+ の待ち時間およびスループット（表形式およびグラフ形式）が提供されます。 また、選択された期間における、特定の ACS インスタンスのプロセス ステータス、プロセス ダウンタイム、およびディスク領域の使用率も提供されます。	システム統計
ACS Instance Authentication Summary	選択された期間における特定の ACS インスタンスの RADIUS および TACACS+ 認証概要情報がグラフ表示とともに提供されます。 このレポートは、データベース内のレコード数によっては、実行に数分かかる場合があります。 このレポートをリロードすると、受信する syslog メッセージが 1 秒あたり約 150 メッセージ以上である場合には、グラフの上に表示される成功した認証と失敗した認証の合計数、および表に表示される成功した認証と失敗した認証の数が一致しません。	成功した認証、失敗した試行
ACS Log Information	選択された期間における特定のログ カテゴリおよび ACS サーバの ACS ログ情報が提供されます。	すべてのログ カテゴリ
ACS Operations Audit	選択された期間における、管理者が ACS で行ったすべての操作変更が提供されます。	管理および操作の監査
ACS System Diagnostics	選択された期間における、重大度に基づいたシステム診断の詳細が提供されます。	内部操作診断、分散管理、管理者の認証と認可
Top N Authentication by ACS Instance	選択された期間における RADIUS および TACACS+ プロトコルについて、ACS インスタンス別の上位 N の成功した認証数、失敗した認証数、および合計認証数が提供されます。	成功した認証、失敗した試行
User Change Password Audit	内部ユーザのユーザ名、ID ストア名、ACS インスタンス名、およびユーザ パスワードが変更された時刻が提供されます。 すべての ACS インターフェイスにおいて、内部ユーザ パスワードのすべての変更を追跡する場合に役立ちます。	管理および操作の監査
Endpoint		
Endpoint MAC Authentication Summary	選択された期間における特定の MAC または MAB の RADIUS 認証概要情報がグラフ表示とともに提供されます。	成功した認証、失敗した試行
Top N Authentications By Endpoint MAC Address	選択された期間における RADIUS プロトコルについて、MAC アドレスまたは MAB アドレス別の上位 N の成功した認証数、失敗した認証数、および合計認証数が提供されます。	成功した認証、失敗した試行

表 13-2　使用可能な ACS レポート （続き）

レポート名	説明	ロギング カテゴリ
Top N Authentications By Machine	選択された期間における RADIUS プロトコルについて、マシン情報別の上位 N の成功した認証数、失敗した認証数、および合計認証数が提供されます。	成功した認証、失敗した試行
Failure Reason		
Authentication Failure Code Lookup	特定の失敗理由について、説明および適切な解決手順が提供されます。	該当なし
Failure Reason Authentication Summary	選択された期間における特定の失敗理由の RADIUS および TACACS+ 認証概要情報がグラフ表示とともに提供されます	失敗した試行
Top N Authentications By Failure Reason	選択された期間における RADIUS および TACACS+ プロトコルについて、失敗理由別の上位 N の失敗した認証数が提供されます。	失敗した試行
Network Device		
AAA Down Summary	選択された期間内に NAD によってロギングされた AAA 到達不能イベントの数が提供されます。	該当なし
Network Device Authentication Summary	選択された期間における特定のネットワーク デバイスの RADIUS および TACACS+ 認証概要情報がグラフ表示とともに提供されます。	成功した認証、失敗した試行
Network Device Log Messages	指定された期間における、特定のネットワーク デバイスのログ情報が提供されます。	該当なし
Session Status Summary	SNMP によって取得された、特定のネットワーク デバイスのポート セッションおよびステータスが提供されます。 このレポートでは、レポートに指定されたコミュニティ ストリングまたは Web インターフェイスの [Monitoring And Reports] -> [Launch Monitoring And Report Viewer] -> [Monitoring Configuration] -> [SNMP Settings] で設定されたコミュニティ ストリングを使用します。	該当なし
Top N AAA Down By Network Device	各ネットワーク デバイスで発生した AAA ダウン イベントの数が提供されます。	該当なし
Top N Authentications by Network Device	選択された期間における RADIUS および TACACS+ プロトコルについて、ネットワーク デバイス別の上位 N の成功した認証数、失敗した認証数、および合計認証数が提供されます。	成功した認証、失敗した試行
Security Group Access		
RBACL Drop Summary	選択された期間における、RBACL ドロップ イベントの概要が提供されます。	該当なし
SGT Assignment Summary	選択された期間における、SGT 割り当ての概要が提供されます。	成功した認証
Top N RBACL Drops By Destination	選択された期間における、送信先別の上位 N の RBACL ドロップ イベント数が提供されます。	該当なし

表 13-2　使用可能な ACS レポート （続き）

レポート名	説明	ロギング カテゴリ
Top N RBACL Drops By User	選択された期間における、ユーザ別の上位 N の RBACL ドロップ イベント数が提供されます。	該当なし
Top N SGT Assignments	選択された期間における、上位 N の SGT 割り当て数が提供されます。	成功した認証
Session Directory		
RADIUS Active Sessions	RADIUS の認証されたセッション、認可されたセッション、および開始されたセッションについての情報が提供されます。 ACS 5.4 では、[RADIUS Active Sessions] レポートを介した認可変更（CoA）機能が導入されています。この機能を使用すると、アクティブな RADIUS セッションを動的に制御できます。 この機能を使用して、次の目的で再認証または接続解除要求を NAD に送信できます。 • ユーザの再認証 • セッションの終了 • セッションの終了およびポートの再起動 • セッションの終了およびポートのシャットダウン	成功した認証、RADIUS アカウンティング
RADIUS Session History	選択された期間における、認証されたセッション、アクティブ セッション、終了されたセッションの合計数や、セッションの継続時間とスループットの合計および平均などの、RADIUS セッション履歴の概要が提供されます。	成功した認証、RADIUS アカウンティング
RADIUS Terminated Sessions	選択された期間における、すべての終了された RADIUS セッションの情報が提供されます。	成功した認証、RADIUS アカウンティング
TACACS Active Sessions	TACACS+ のアクティブ セッションについての情報が提供されます。	TACACS アカウンティング
TACACS Session History	選択された期間における、アクティブ セッションと終了されたセッションの合計数や、セッションの継続時間とスループットの合計および平均などの、TACACS+ セッション履歴の概要が提供されます。	TACACS アカウンティング
TACACS Terminated Sessions	選択された期間における、終了された TACACS セッションの詳細が提供されます。	TACACS アカウンティング
User		
Top N Authentications By User	選択された期間における RADIUS および TACACS+ プロトコルについて、ユーザ別の上位 N の成功した認証数、失敗した認証数、および合計認証数が提供されます。	成功した認証、失敗した試行
User Authentication Summary	選択された期間における特定のユーザの RADIUS および TACACS+ 認証概要情報がグラフ表示とともに提供されます。	成功した認証、失敗した試行

カタログ レポートの実行

カタログ内のレポートを実行するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Catalog] > *report_type* を選択します。*report_type* は、実行するレポートのタイプです。

表 13-3 に示した情報とともに、選択したレポート タイプで使用可能なレポートが表示されます。

表 13-3　<report_type> ページ

オプション	説明
Report Name	選択したレポート タイプで使用可能なレポート。
Type	レポートのタイプ。
Modified At	*Ddd Mmm dd hh:mm:ss timezone yyyy* の形式で表された、関連するレポートが最後に管理者によって変更された日時。 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • *timezone* = タイムゾーン。 • yyyy = 年を表す 4 桁の数字。

ステップ 2　実行するレポート名の隣にあるオプション ボタンをクリックして、[Run] の下にある次のいずれかのオプションを選択します。

- [Run for Today]：指定したレポートが実行されて、生成された結果が表示されます。
- [Run for Yesterday]：指定したレポートが前日の値を使用して実行されて、生成された結果が表示されます。
- [Query and Run]：レポート生成時に使用するパラメータを入力できる [Run Report] 画面が表示されます。

ステップ 3　デフォルトのレポート パラメータに戻すには、[Reset Reports] をクリックします。カタログ内のシステム レポート ファイルを工場出荷時のデフォルトにリセットするかどうかを確認するメッセージが表示されます。

ステップ 4　その他のオプションについては、[Launch Interactive Viewer] をクリックします。

関連トピック

- 「カタログで使用可能なレポート」（P.13-8）
- 「カタログ レポートの削除」（P.13-13）
- 「report_name ページについて」（P.13-15）

カタログ レポートの削除

[Reports] > [Catalog] の下のページからレポートを削除するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Catalog] > *report_type* を選択します。*report_type* は、削除するレポートのタイプです。

（注）　[Reports] > [Catalog] の下のページでは、システム レポートは削除できず、カスタマイズしたレポートだけを削除できます。

ステップ 2　削除するレポートの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

ステップ 3　[OK] をクリックして、選択したレポートを削除することを確認します。

[Catalog listing] ページが表示されます。このとき、削除したレポートは表示されません。

名前付きレポートの実行

このページは、特定の名前付きレポートを実行する場合に使用します。

[Monitoring and Reports] > [Reports] > [Catalog] > *report_type* > report_name を選択します。*report_type* はレポートのタイプ（表 13-3 を参照）であり、*report_name* はアクセスまたは実行するレポートの名前です。表 13-4 に、レポートを実行する場合に使用可能なタイプおよび名前を示します。

表 13-4　[Reports] > レポートタイプおよび名前

<report_type>	<report_name>
AAA Protocol	AAA Diagnostics
	Authentication Trend
	RADIUS Accounting
	RADIUS Authentication
	TACACS Accounting
	TACACS Authentication
	TACACS Authorization
Access Service	Access Service Authentication Summary
	Top N Authentications By Access Service

表 13-4　[Reports] > レポートタイプおよび名前 （続き）

<report_type>	<report_name>
ACS Instance	ACS Administrator Entitlement
	ACS Administrator Logins
	ACS Configuration Audit
	ACS Health Summary
	ACS Instance Authentication Summary
	ACS Log Information
	ACS Operations Audit
	ACS System Diagnostics
	Top N Authentications By ACS Instance
	User Change Password Audit
Endpoint	Endpoint MAC Authentication Summary
	Top N Authentications By Endpoint MAC Address
	Top N Authentications By Machine
Failure Reason	Authentication Failure Code Lookup
	Failure Reason Authentication Summary
	Top N Authentications By Failure Reason
Network Device	AAA Down Summary
	Network Device Authentication Summary
	Network Device Log Messages
	Session Status Summary
	Top N AAA Down By Network Device
	Top N Authentications By Network Device
Security Group Access	RBACL Drop Summary
	SGT Assignment Summary
	Top N RBACL Drops By Destination
	Top N RBACL Drops By User
	Top N SGT Assignments
Session Directory	RADIUS Active Sessions
	RADIUS Session History
	RADIUS Terminated Sessions
	TACACS Active Sessions
	TACACS Session History
	TACACS Terminated Sessions
User	Top N Authentications By User
	User Authentication Summary

関連トピック

- 「カタログ レポートの使用」（P.13-7）

- 「report_name ページについて」（P.13-15）

report_name ページについて

（注）　すべてのレポートのデータ選択で表 13-5 に示されているすべてのオプションを使用するわけではありません。

表 13-5　<report_name> ページ

オプション	説明
User	ユーザ名を入力するか、または [Select] をクリックして、しきい値を設定する有効なユーザ名を入力します。
MAC Address	MAC アドレスを入力するか、または [Select] をクリックして、レポートを実行する有効な MAC アドレスを入力します。
Identity Group	ID グループ名を入力するか、または [Select] をクリックして、レポートを実行する有効な ID グループ名を入力します。
Device Name	デバイス名を入力するか、または [Select] をクリックして、レポートを実行する有効なデバイス名を入力します。
Device IP	デバイスの IP アドレスを入力するか、または [Select] をクリックして、レポートを実行する有効なデバイスの IP アドレスを入力します。
SNMP Community	MIB オブジェクトへのアクセスを認証するように SNMP プリファレンスを設定します。詳細については、「SNMP プリファレンスの設定」（P.15-16）を参照してください。このコミュニティ ストリングは、AAA クライアントで SNMP を使用して情報を問い合わせるために ACS で使用されますが、SNMP マネージャで ACS の MIB 情報を問い合わせるために使用することはできません。
Device Group	デバイス グループ名を入力するか、または [Select] をクリックして、レポートを実行する有効なデバイス グループ名を入力します。
Access Service	アクセス サービス名を入力するか、または [Select] をクリックして、レポートを実行する有効なアクセス サービス名を入力します。
Identity Store	ID ストア名を入力するか、または [Select] をクリックして、レポートを実行する有効な ID ストア名を入力します。
ACS Instance	ACS インスタンス名を入力するか、または [Select] をクリックして、レポートを実行する有効な ACS インスタンス名を入力します。
Failure Reason	失敗理由名を入力するか、または [Select] をクリックして、レポートを実行する有効な失敗理由名を入力します。
Protocol	ドロップダウン リスト ボックスを使用して、レポートを実行するプロトコルを選択します。有効なオプションは次のとおりです。 • RADIUS • TACACS+
Authentication Status	ドロップダウン リスト ボックスを使用して、レポートを実行する認証ステータスを選択します。有効なオプションは次のとおりです。 • Pass Or Fail • Pass • Fail

表 13-5　<report_name> ページ （続き）

オプション	説明
Radius Audit Session ID	レポートを実行する RADIUS 監査セッション識別名を入力します。
ACS Session ID	レポートを実行する ACS セッション識別名を入力します。
Severity	ドロップダウン リスト ボックスを使用して、レポートを実行する重大度レベルを選択します。この設定により、しきい値で指定した重大度レベルおよびそれよりも上の重大度レベルが取得されます。有効なオプションは次のとおりです。 • Fatal • Error • Warning • Info • Debug
End Point IP Address	レポートを実行するエンド ポイント IP アドレスを入力します。
Command Accounting Only	コマンド アカウンティングに対するレポートの実行をイネーブルにする場合にこのチェックボックスをオンにします。
Top	ドロップダウン リスト ボックスを使用して、レポートを実行する場合に上位（最も頻繁な）何件のアクセス サービス別の認証数を表示するかを選択します。有効なオプションは次のとおりです。 • 10 • 50 • 100 • 500 • 1000 • All
By	ドロップダウン リスト ボックスを使用して、レポートを実行する認証のタイプを選択します。有効なオプションは次のとおりです。 • Passed Authentications • Failed Authentications • Total Authentications
Administrator Name	管理者ユーザ名を入力するか、または [Select] をクリックして、レポートを実行する管理者ユーザ名を選択します。
Object Type	レポートを実行する有効なオブジェクト タイプを入力します。
Object Name	名前を入力するか、または [Select] をクリックして、レポートを実行するオブジェクトのオブジェクト名を選択します。
Authorization Status	ドロップダウン リスト ボックスを使用して、レポートを実行する認証ステータスを選択します。有効なオプションは次のとおりです。 • Pass Or Fail • Pass • Fail

表 13-5　<report_name> ページ （続き）

オプション	説明
Time Range	ドロップダウン リスト ボックスを使用して、レポートを実行する期間を選択します。有効なオプションは次のとおりです。 • [Last Hour]（[ACS Health Summary] レポートだけ） • Today • Yesterday • Last 7 Days • Last 30 Days • [Custom]：[Start Date] と [End Date]、または [Day] を設定する必要があります。 （注）　さまざまなレポートうち、一部の [Time Range] エントリにおいては、一部のオプションが有効ではない場合があります。
Start Date	日付を入力するか、または日付セレクタ アイコンをクリックして、レポート実行の開始日を入力します。
End Date	日付を入力するか、または日付セレクタ アイコンをクリックして、レポート実行の終了日を入力します。
Start Time	レポートの実行に使用する開始時刻を入力します。
End Time	レポートの実行に使用する終了時間を入力します。
Day	日付を入力するか、または日付セレクタ アイコンをクリックして、レポート実行の終了日を入力します。
Clear	関連するテキスト ボックスの内容を削除する場合にクリックします。
Export	レコードを .csv ファイルにエクスポートし、表示する場合にクリックします。レポートの生成中に 5000 を超えるレコードが作成されると、ACS は .csv ファイルを使用してレコードをエクスポートして表示するように、ユーザに通知します。スケジューラ ページのレコードの状態を追跡できます。データのエクスポート時、[Submit] ボタンはディセーブルです。 （注）　このエクスポート オプションは RADIUS 認証、RADIUS アカウンティング、TACACS+ 認証、TACACS+ 許可および TACACS+ アカウンティング レコードに対してのみ使用できます。 （注）　エクスポートしたレポートを Microsoft Excel で表示する場合は、ワークシートのサイズ制限に注意する必要があります。Microsoft Excel 2007 および 2010 では、ワークシートのサイズの上限は 16,384 カラム、1,048,576 行です。詳細については、http://office.microsoft.com/en-us/excel-help/excel-specifications-and-limits-HP010342495.aspx を参照してください。
Run	選択したレポートを実行する場合にクリックします。

関連トピック

- 「カタログ レポートの使用」（P.13-7）
- 「お気に入り レポートの使用」（P.13-3）
- 「カタログで使用可能なレポート」（P.13-8）
- 「カタログ レポートの実行」（P.13-12）

デバイスでの RADIUS CoA オプションのイネーブル化

すべての [RADIUS Active Session] レポートを表示するには、デバイスで RADIUS CoA オプションをイネーブルにする必要があります。

RADIUS CoA オプションを設定するには、次の手順を実行します。

ステップ 1　NAD で、ACS RADIUS サーバに対する MAB、802.1X、および Web 認証を設定します。

ステップ 2　サプリカントに接続されている NAD で CoA を次のように設定します。

```
aa server radius dynamic-author
client {<ip_addr> - <name>} [vrf <vrfname>] [server-key<string>]
server-key [0 - 7] <string>
port <port-num>
auth-type {any - all - session-key}
ignore session-key
ignore server-key
```

ステップ 3　認証順序（Flex-Auth）を設定します。

認可の変更、およびアクティブな RADIUS セッションの接続解除

（注）　展開されている NAD の一部では、リロード後にアカウンティング停止パケットまたはアカウンティング オフ パケットが送信されません。このため、[Session Directory] の下のレポートでは、有効なセッションと期限切れのセッションの 2 つのセッションが表示される場合があります。したがって、アクティブな RADIUS セッションの認可を動的に変更する場合や、アクティブな RADIUS セッションの接続を解除する場合には、必ず最新のセッションを選択する必要があります。

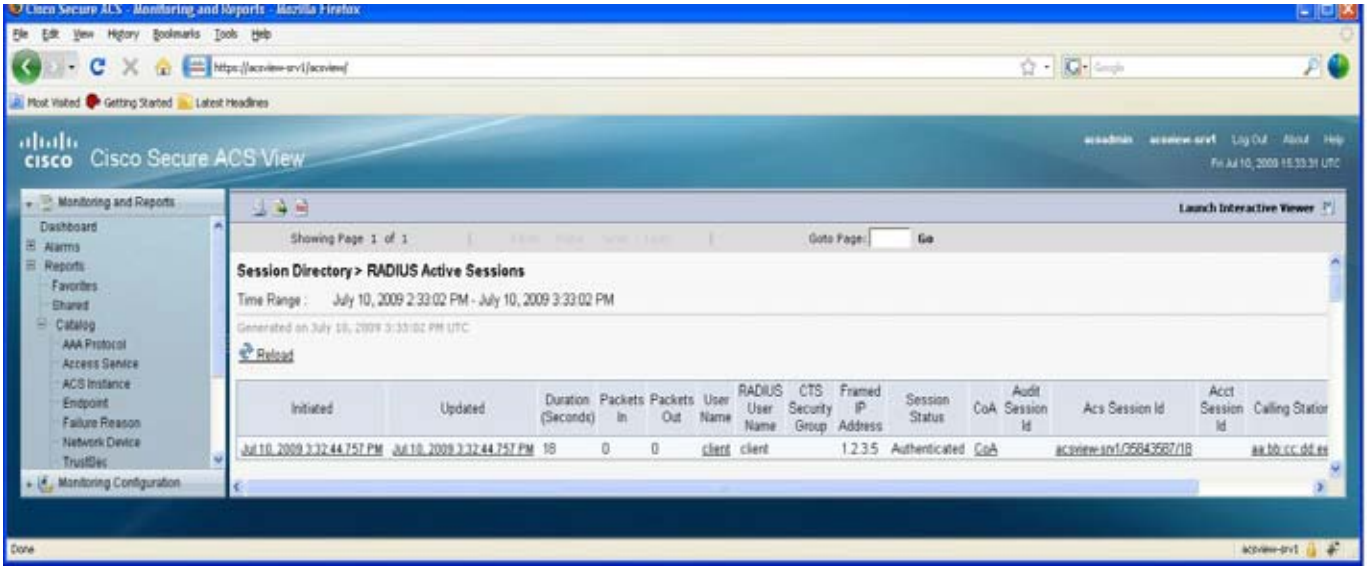
認可の変更またはアクティブな RADIUS セッションの接続解除を行うには、次の手順を実行します。

ステップ 1　[Session Directory] の下にある [RADIUS Active Sessions] レポートを実行します。

[RADIUS Active Sessions] レポートの実行方法については、「カタログ レポートの実行」（P.13-12）を参照してください。

図 13-2 に示すようなレポートが表示されます。

図 13-2　[RADIUS Active Sessions] レポート



ステップ 2　再認証または終了する RADIUS セッションの [CoA] リンクをクリックします。

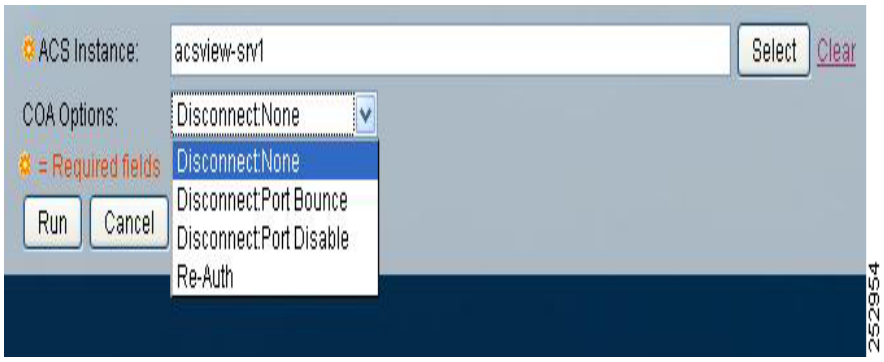
[Change of Authorization Request] ページが表示されます。

ステップ 3　図 13-3 に示す CoA オプションのドロップダウン リスト ボックスから、CoA オプションを選択します。

有効なオプションは次のとおりです。

- Disconnect:None：セッションを終了しません。
- Disconnect:Port Bounce：セッションを終了して、ポートを再起動します。
- Disconnect:Port Disable：セッションを終了して、ポートをシャットダウンします。
- Re-Auth：ユーザを再認証します。

図 13-3　CoA オプション



ステップ 4　[Run] をクリックして、RADIUS セッションを再認証または接続解除します。

認可変更に失敗した場合は、次の理由が考えられます。

- デバイスで CoA がサポートされていない

- ID または認可ポリシーに変更があった
- 共有秘密情報が一致しない

ステップ 5　認可変更の試行が失敗した場合のトラブルシューティングについては、「RADIUS 認証のトラブルシューティング」（P.14-6）を参照してください。

失敗した動的な CoA は、失敗した RADIUS 認証として表示されます。

レポートのカスタマイズ

システム レポートをカスタマイズするには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Reports] > [Catalog] > report_type > *report_name* を選択します。*report_type* はレポートのタイプであり、*report_name* はカスタマイズするレポートの名前です。

[Reports] ページが表示されます。

ステップ 2　カスタマイズするレポートの名前の隣にあるオプション ボタンをクリックするか、またはカスタマイズするレポートの名前をクリックします。

ステップ 3　[Run] をクリックします。

[Run Report] ページが表示されます。

ステップ 4　必要に応じて、[Run Reports] ページのフィールドを変更します。

ステップ 5　[Run] をクリックします。

レポートが表示されます。

ステップ 6　[Launch Interactive Viewer] をクリックします。

ステップ 7　必要に応じてレポート内容を変更し、[Save As] をクリックして、カスタマイズしたレポートを [Catalog] > [Reports] の下の任意のページに同じレポート名または異なるレポート名で保存します。

（注）　カスタマイズしたレポートを元のシステム レポートと同じ名前で保存した場合（つまり元のシステム レポートを上書きした場合）、そのレポートは削除できません。カスタマイズしたレポートをデフォルトの事前に定義されたシステム レポート設定に復元する方法については、「レポートの復元」（P.13-20）を参照してください。

カスタマイズしたレポートが、指定した場所に保存されます。

レポートの復元

カスタマイズしたシステム レポートを元の事前に定義されたシステム レポート設定に復元するには、このトピックで説明されている手順を使用します。

この手順では、レポート カタログ タイプ内のすべてのレポートがリセットされます。たとえば、[Monitoring and Reports] > [Reports] > [Catalog] > [Endpoint] ページにあるカスタマイズした特定のレポートをリセットする必要がある場合にこの手順を実行すると、そのレポート以外に、[Endpoint] ページの他のすべてのレポートもリセットされます。

ステップ 1　[Monitoring and Reports] > [Reports] > [Catalog] > *report_type* を選択します。*report_type* は、元のシステム レポート設定にリセットするカスタマイズしたレポートが存在するレポートのタイプです。

ステップ 2　[Reset Reports] をクリックします。

ステップ 3　[Yes] をクリックして、システム レポート ファイルを工場出荷時のデフォルトにリセットすることを確認します。

ページが更新されて、[Catalog] > *report_type* のレポートが工場出荷時のデフォルトにリセットされます。

レポートの表示

このセクションでは、レポートの表示方法、および標準ビューアまたは Interactive Viewer でのさまざまなタスクの実行方法について説明します。標準ビューアまたは Interactive Viewer で、レポート内の移動、データの印刷、別の形式へのデータのエクスポートができます。Interactive Viewer では、コンテンツの変更、レポートの編成、レポートの書式設定もできます。ACS 5.4 では、Report Viewer の IP アドレス フィールドに、正しい形式で IPv6 アドレスが表示されます。

ここでは、次の内容について説明します。

- 「標準ビューアについて」（P.13-21）
- 「Interactive Viewer について」（P.13-21）
- 「Interactive Viewer のコンテキスト メニューについて」（P.13-22）
- 「レポート内の移動」（P.13-23）
- 「レポート データのエクスポート」（P.13-24）
- 「レポートの印刷」（P.13-27）
- 「Interactive Viewer におけるレポート デザインの保存」（P.13-27）

標準ビューアについて

標準ビューアから、目次のオープン、レポート内の移動、データのスプレッドシート形式でのエクスポート、レポートの印刷を行うことができます。

[Launch Interactive Viewer] をクリックすると、標準ビューアを閉じて、Interactive Viewer でレポートを表示できます。「Interactive Viewer について」（P.13-21）を参照してください。

Interactive Viewer について

Interactive Viewer では、標準ビューアのすべての機能、およびレポートのレイアウトとフォーマットに関する数多くの設定の変更がサポートされています。Interactive Viewer ツールバーは、標準ビューアのツールバーよりも大幅に機能が拡張されています。「Interactive Viewer のコンテキスト メニューについて」（P.13-22）を参照してください。

（注）　Interactive Viewer の機能は、Internet Explorer バージョン 8.x および 9.x. では適切に動作しません。Internet Explorer バージョン 8.x および 9.x でレポートを正しく表示するには、Internet Explorer ブラウザの [Tools] メニューから [Compatibility View] オプションをイネーブルにします。

Interactive Viewer のコンテキスト メニューについて

Interactive Viewer には、データに対して実行するフォーマット タスク、ソート タスク、およびグループ化タスクの多くがサポートされたコンテキスト メニューが用意されています。図 13-4 に、カラム用のコンテキスト メニューを示します。このメニューを使用すると、カラムの追加または削除、データのソート、グループの追加または削除、フォントおよびテキスト配置の設定を実行できます。

また、データのソートおよびフィルタリング、計算の作成、複数行の集計を行うこともできます。このコンテキスト メニューにアクセスするには、カラムを選択して右クリックします。

図 13-4　Interactive Viewer のカラム データ用のコンテキスト メニュー

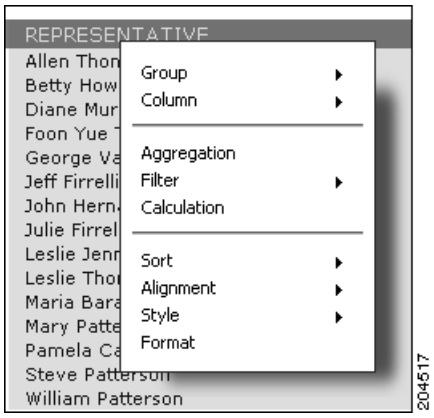
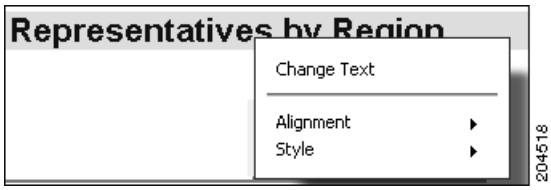


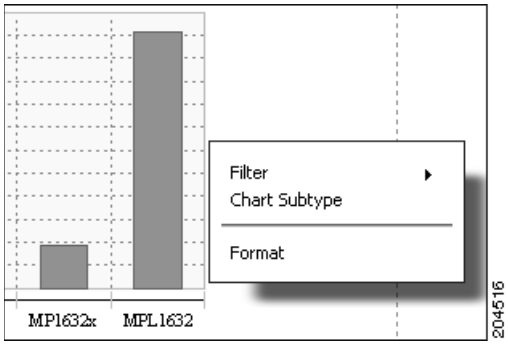
図 13-5 に、Interactive Viewer でラベルを変更する場合に使用するコンテキスト メニューを示します。このメニューを表示するには、ラベルを選択して右クリックします。ラベル テキストの編集や、ラベルのテキスト配置プロパティまたはフォント プロパティの変更を行う場合にこのメニューを使用します。

図 13-5　Interactive Viewer のラベル用のコンテキスト メニュー



レポートにグラフが含まれている場合は、図 13-6 に示すグラフ用のコンテキスト メニューを使用して、グラフのフォーマットやサブタイプなどのプロパティを変更できます。

図 13-6　Interactive Viewer のグラフ用のコンテキスト メニュー



各コンテキスト メニューにおいて、右矢印が表示されたエントリを選択すると、関連するコンテキスト メニューの選択肢にアクセスできます。たとえば、カラムを右クリックして [Alignment] を選択すると、[Left]、[Center]、または [Right] を選択でき、これにより目的の配置タイプを指定できます。

レポート内の移動

ビューアでレポートを開くと、データの先頭ページが表示されます。データを表示または操作する場合は、レポート内の移動を支援するツールを使用します。

ビューア内では、図 13-7 に示すページ移動ツールを使用して、レポート内のページ間を移動できます。このツールでは、矢印をクリックして、レポートの先頭ページ、最終ページ、1 つ前のページ、または 1 つあとのページに移動できます。

図 13-7　ページ移動ツール

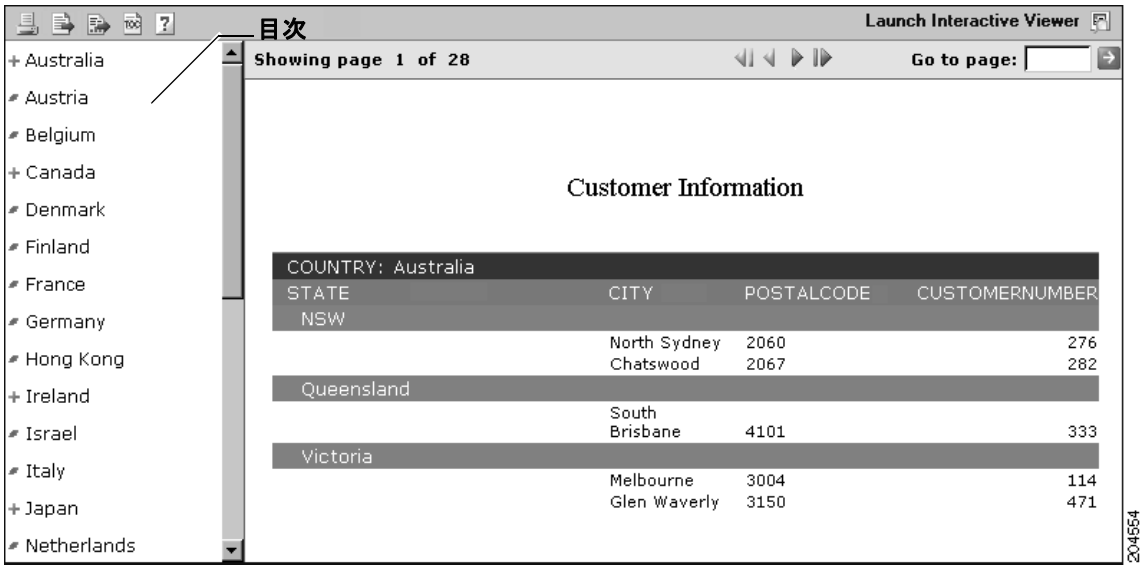
また、ビューアでは、図 13-8 に示すように [Go to page] にページ番号を入力し、このフィールドの隣にある矢印をクリックすることによって、特定のページに移動することもできます。

図 13-8　特定のページへの移動

目次の使用方法

ビューアでは、目次を開いて、レポート構造を表示し、レポート内を移動できます。目次を開くには、ツールバーの目次ボタンを選択します。図 13-9 に、目次が開いた状態の標準ビューアのレポートを示します。

図 13-9　目次を使用した移動



目次内の各エントリは、レポート内のページへのリンクとなっています。エントリの隣にプラス記号（+）がある場合は、そのプラス記号をクリックするとエントリを展開できます。図 13-10 に、展開されたエントリを示します。

図 13-10　目次の展開されたエントリ

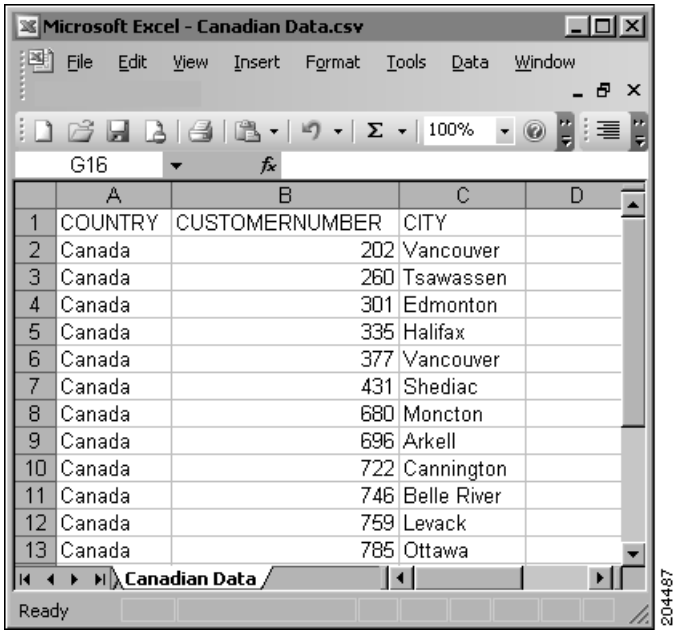
特定のページに移動するには、関連するリンクをクリックします。

レポート データのエクスポート

ビューアでは、カンマ区切り形式（.csv）ファイル、パイプ区切り形式（.psv）ファイル、またはタブ区切り形式（.tsv）ファイルとして Excel スプレッドシートにレポート データをエクスポートする機能がサポートされています。カラムのデータ型をエクスポートするオプションを選択できます。

スプレッドシートのデータは、情報オブジェクトまたはテンプレートのデータと同様にフォーマットされます。たとえば、レポート デザインでカラム ヘッダーを編集したり、数値データをフォーマットしても、スプレッドシートにはそれらの内容は反映されません。図 13-11 に、サンプルの CSV 出力ファイルを示します。

図 13-11　Microsoft Excel にエクスポートされたレポート データ



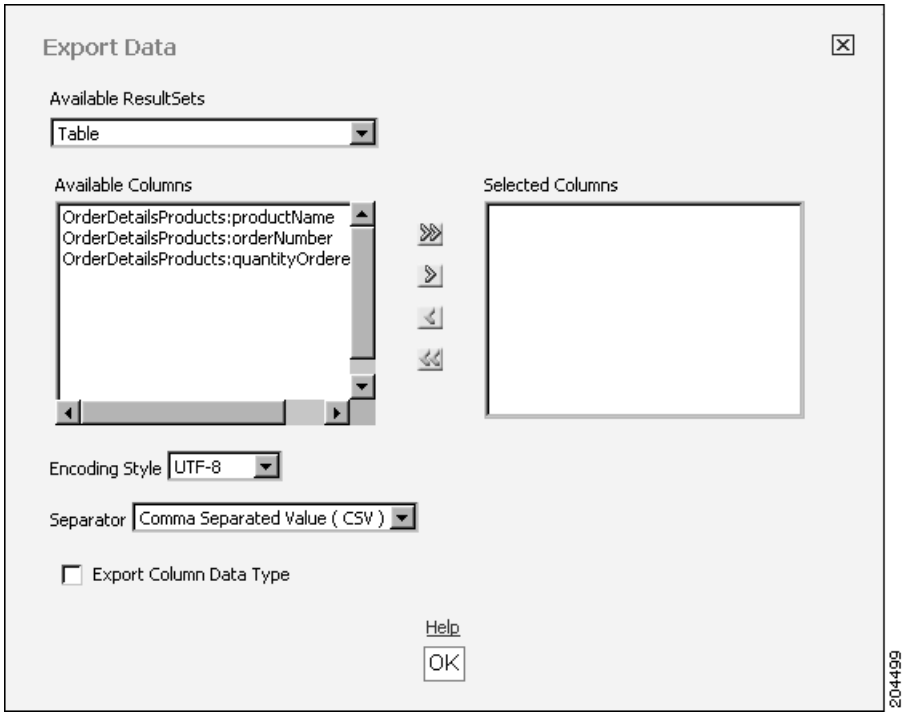
	A	B	C	D
1	COUNTRY	CUSTOMERNUMBER	CITY	
2	Canada	202	Vancouver	
3	Canada	260	Tsawassen	
4	Canada	301	Edmonton	
5	Canada	335	Halifax	
6	Canada	377	Vancouver	
7	Canada	431	Shediac	
8	Canada	680	Moncton	
9	Canada	696	Arkell	
10	Canada	722	Cannington	
11	Canada	746	Belle River	
12	Canada	759	Levack	
13	Canada	785	Ottawa	

Excel では、他のスプレッドシートと同様に、カラムのサイズを変更したり、データをフォーマットしたりできます。

ステップ 1　ビューアで、[Export Data] を選択します。

図 13-12 に示すように、[Export Data] ダイアログボックスが表示されます。

図 13-12　[Export Data] ダイアログボックス



[Available Result Sets] には、レポート内の表がリストされます。

[Available Columns] には、指定した表からエクスポートできるカラムがリストされます。集計行や計算カラムのデータを含む、レポートで使用されているすべてのデータをエクスポートできます。レポートで複数のデータ ソースが使用されている場合には、各データ ソースのデータを別々にエクスポートできます。

ステップ 2　[Available Columns] で、エクスポートするカラムを選択して、一重右矢印を選択します。

すべてのカラムを選択するには、二重右矢印を選択して、[OK] をクリックします。

[File Download] ダイアログボックスが表示され、ファイルに割り当てられたデフォルト名とファイル拡張子 .csv が表示されます。ファイル名は、ステップ 4 で変更できます。

ステップ 3　[Save] をクリックします。

ステップ 4　[Save As] ダイアログボックスで、次の手順を実行します。

- [Save in] で、このファイルを保存するフォルダに移動します。
- [File name] で、ファイルの名前を変更します。

ステップ 5　[Save] をクリックします。

新しい場所に CSV ファイルが保存されます。

このファイルを開くと、編集可能な Microsoft Excel ワークシートにデータが表示されます。データ全体を表示するには、カラムの幅を広げる必要がある場合があります。

レポートの印刷

ビューアに表示されるレポートを HTML 形式または PDF 形式で印刷できます。Interactive Viewer では、レポートの変更が可能であるため、元のレポートを印刷することも、変更したレポートを印刷することもできます。

ステップ 1　ビューアで、[Print Report] を選択します。

[Print] ダイアログボックスが表示されます。

ステップ 2　[Format] フィールドで、[HTML] または [PDF] を選択します。

ステップ 3　[Page Range] フィールドで、印刷するページを選択します。

ステップ 4　[OK] をクリックします。

ステップ 5　ステップ 2 で選択した形式に応じて、次のオプションがあります。

- HTML 形式を選択した場合は、プリンタ オプションを指定できる印刷ダイアログボックスが表示されます。
- PDF 形式を選択した場合は、Web ブラウザに PDF ビューア プラグインを使用してレポートが表示されます。レポートを確認し、プラグインの印刷アイコンを選択して、プリンタ オプションを指定できます。

（注）　ACS の以前のバージョンで作成した共有レポートは、ACS の旧バージョンを ACS 5.4 にアップグレードするか、ACS 5.4 を新規インストールすると機能しなくなります。そのため、共有レポートを削除し、ACS 5.4 で追加する必要があります。

Interactive Viewer におけるレポート デザインの保存

デザイン環境または Interactive Viewer での作業中に、Interactive Viewer からレポート デザインを保存できます。

ステップ 1　[Save] をクリックします。

[Save] ダイアログボックスが表示されます。図 13-13 に例を示します。

図 13-13　[Save] ダイアログボックス

ステップ 2　ファイルを保存する場所に移動します。

ステップ 3　ファイル名を入力して、[Save] をクリックします。

ステップ 4　表示される確認メッセージで [OK] をクリックします。

Interactive Viewer におけるレポートのフォーマット

Interactive Viewer を使用して、レポートをフォーマットできます。

ここでは、次の内容について説明します。

- 「ラベルの編集」（P.13-28）
- 「ラベルのフォーマット」（P.13-29）
- 「条件フォーマットの適用」（P.13-38）
- 「詳細カラムにおける改ページの設定および削除」（P.13-41）

ラベルの編集

ラベルは、レポートのタイトルやフッターの項目などの、静的なテキストを含むフィールドです。一般的なレポートには、編集できるラベルと編集できないラベルがあります。

たとえば、テンプレートには、機密保持規定を示すラベルや、レポートのフッターにレポート作成者名を示すラベルなどが含まれています。機密保持規定は編集できませんが、作成者はフッターに各自の名前を挿入できます。

カラム ヘッダーなどのラベルが編集可能である場合は、フォント、フォント サイズ、背景色などのプロパティを変更できます。ラベルのテキストを編集することもできます。

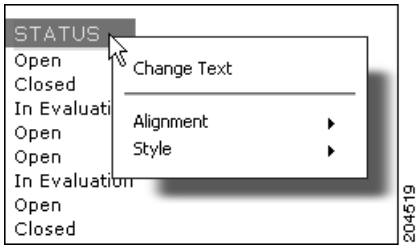
カラム ヘッダーのテキストは、データ ソースから取得されます。カラム ヘッダーがデータ ソースで大文字だけ、かつ単語間のスペースなしで指定されている場合には、レポート デザインでも同じようにカラム ヘッダー名が表示されます。カラム ヘッダーの内容は、コンテキスト メニューを使用して変更できます。

カラム ヘッダーのフォーマットは、レポート テンプレートまたはテーマから取得されます。フォーマットがレポート テンプレートから取得される場合、フォーマットは変更できません。フォーマットがテーマから取得される場合は、テーマを変更することによって、フォーマットを変更できます。

ステップ 1　Interactive Viewer で、ラベルを選択して右クリックします。

図 13-14 に示すようなコンテキスト メニューが表示されます。

図 13-14　Interactive Viewer のコンテキスト メニュー



ステップ 2　[Change Text] を選択します。

[Edit Text] ダイアログボックスが表示されます。

ステップ 3　必要に応じてテキストを変更し、[Apply] をクリックします。

ラベルのフォーマット

ラベルのフォーマットを変更するには、次の手順を実行します。

ステップ 1　ラベルをクリックして、[Style] > [Font] を選択します。

[Font] ダイアログボックスが表示されます。

ステップ 2　必要なフォーマットを選択して、[Apply] をクリックします。

データのフォーマット

レポート データのフォーマットを変更するには、いくつかの方法があります。次の作業を実行できます。

- カラムのサイズ変更。
- カラム内のデータの配置の変更。
- カラムの非表示、表示、削除、または並べ替え。
- カラムにおける連続した重複値の非表示指定。
- データ値のフィルタリング。

- データ値のソート。
- テキストのフォント、色、スタイルなどのプロパティの変更。
- カラムの大文字または小文字での表示の指定。
- 集計行におけるデータ値のデフォルト フォーマットの変更。
- データ型のフォーマット。たとえば、カラムに数値が表示される場合、そのデータを通貨、パーセント、または科学的数値としてフォーマットできます。

カラムのサイズ変更

Interactive Viewer では、カラムの幅、およびカラム内のデータの配置を変更できます。カラムの幅を変更するには、次の手順を実行します。

ステップ 1　カラムを選択して右クリックします。

ステップ 2　コンテキスト メニューから [Column] > [Column Width] を選択します。

[Column Properties] フォームが表示されます。

ステップ 3　[Column Properties] フォームで、新しいカラム幅を入力して、[Apply] をクリックします。

カラム データの配置の変更

カラム内のデータの配置を変更するには、カラムを右クリックして、コンテキスト メニューから [Alignment] を選択します。その後、[Left]、[Center]、または [Right] のいずれかの配置オプションを選択します。

カラム内のデータのフォーマット

カラム データのデフォルトのフォーマットは、データ ソースから取得されます。通常は、レポートを見やすくするためにカラム データのフォーマットを変更します。カラム データのフォーマットを行うと、カラム ヘッダーと集計行を除いて、カラム全体に同じフォーマットが適用されます。データ自体は変更できません。

ステップ 1　カラムを選択して右クリックします。

コンテキスト メニューが表示されます。

ステップ 2　[Style] > [Font] を選択します。

ステップ 3　[Font] フォームで、任意のスタイル プロパティを変更します。

変更を行うと、変更内容が [Preview] フィールドに表示されます。

ステップ 4　新しいテキスト スタイルをレポートのすべてのカラムに適用するか、または選択したカラムに適用するかを指定します。

デフォルト設定では、選択したカラムに新しいスタイルが適用されます。

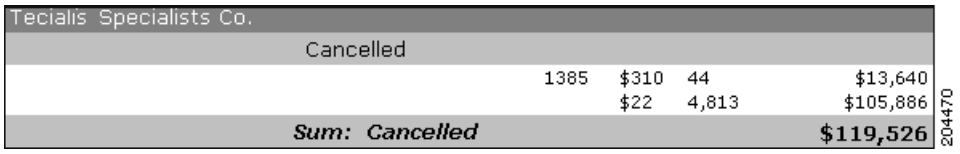
ステップ 5　[Apply] をクリックします。

集計行のデータのフォーマット

集計行には、カラムの合計や平均などの集計データが表示されます。集計行の作成方法については、あとの章で学習します。図 13-15 に、レポートの末尾に表示された集計行を示します。通常、集計行のデフォルトのフォーマットは、テンプレートまたはテーマから取得されます。

集計データ値のフォーマット、およびデータ値の前に表示されるラベルのフォーマットを変更できます。ラベルのテキストやデータ値は変更できません。

図 13-15　集計行のデータのフォーマット



ステップ 1　集計データ値を選択して、[Font] をクリックします。

[Font] ダイアログボックスが表示されます。

ステップ 2　必要に応じて設定を変更し、[Apply] をクリックします。

データ型のフォーマット

情報オブジェクトにおいては、情報オブジェクトの基礎となるリレーショナル データベースと同様に、カラム ヘッダーを除いてカラム内のすべてのデータが同じデータ型となります。カラムには、数値データ、日時データ、またはストリング データが表示されます。

それぞれのデータ型には、さまざまな独自のフォーマットがあります。たとえば、数値データは、通貨、パーセント、または小数値として表示できます。同様に、日付は、月の完全な名前を含む長い日付フォーマットや、月を数字で表した短い日付フォーマットで表示できます。

表 13-6 に、使用可能なデータ型フォーマットを示します。表内のほとんどの例は、アメリカ英語のロケールについて示しています。異なるロケールを使用する場合は、[Custom] フォーマット オプションを使用して、各自のロケールにあわせてデータをフォーマットできます。

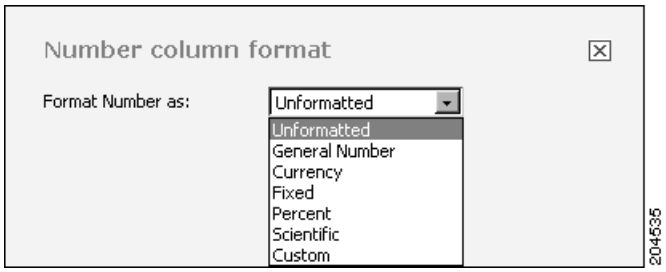
表 13-6　データ型とフォーマット

データ型	オプション	説明
Date and Time	Unformatted	データでは、テンプレートまたはテーマによって設定されたデフォルトのフォーマットが維持されます。
	General Date	June 5, 2006 12:00:00 AM GMT +00:00
	Long Date	June 5, 2006
	Medium Date	Jun 5, 2006
	Short Date	6/5/06
	Long Time	12:00:00 AM GMT +00:00
	Medium Time	12:00:00 AM
	Short Time	12:00
	Custom	フォーマットは、入力するフォーマット コードによって異なります。たとえば、yyyy/mm と入力すると 2006/10 となります。フォーマットについては、この章の後半で詳しく説明します。
Number	Unformatted	数値では、テンプレートまたはテーマによって設定されたデフォルトのフォーマットが維持されます。
	General Number	小数点の設定および 3 桁ごとの区切り文字の設定に応じて、6066.88 や 6067 など。
	Currency	ロケールおよび任意の設定に応じて、$6,067.45 や ¥6067 など。
	Fixed	任意の設定に応じて、6067、6,067、6067.45 など。
	Percent	任意の設定に応じて、45% や 45.8% など。
	Scientific	任意の設定に応じて、2E04 や 2.67E04 など。E のあとの数字は 10 の指数を表します。たとえば、2.67E04 は、2.67 に 10 の 4 乗を乗算した数値です。
	Custom	フォーマットは、入力するフォーマット コードによって異なります。たとえば、#,### と入力すると、3 桁ごとの区切り文字としてカンマを使用し、かつ小数点なしのフォーマットとなります。カスタム フォーマットについては、この章の後半で詳しく説明します。
String	Unformatted	ストリングでは、テンプレートまたはテーマによって設定されたデフォルトのフォーマットが維持されます。
	Uppercase	ストリングは、GREAT NEWS のようにすべて大文字で表示されます。
	Lowercase	ストリングは、great news のようにすべて小文字で表示されます。
	Custom	フォーマットは、入力するフォーマット コードによって異なります。カスタム フォーマットは、郵便番号や電話番号などの、標準的なフォーマットに適合しないデータに使用します。

数値データのフォーマット

数値データにはいくつかの形式があります。郵便番号のカラムでは、売上金額のカラムとは異なるフォーマットが必要となります。図 13-16 に、使用可能な数値フォーマットを示します。

図 13-16　数値データのフォーマット



カラムのデータ型は、データ ソースによって決定されます。テキストやストリングのデータ型にも数字が含まれることがあります。たとえば、多くの場合、電話番号はデータ ソースではストリング データで表されます。フォーマット ダイアログボックスのタイトルには、カラムのデータ型が示されます。

ステップ 1　数値データを含むカラムを選択して、[Format] を選択します。

[Number column format] ダイアログボックスが表示されます。

ステップ 2　[Format Number as] フィールドで、[General Number]、[Currency]、[Fixed]、[Percent]、または [Scientific] を選択します。

[Number column format] の下部には、そのタイプのフォーマットをサポートするフィールドが表示されます。

ステップ 3　[Symbol] フィールドで、通貨記号を選択します。

ステップ 4　[Symbol Position] では、次のように選択します。

- 通貨記号またはパーセント記号を数値の前に配置する場合には、[Before] を選択します。
- 記号を数値の後ろに配置する場合には、[After] を選択します。

ステップ 5　[Decimal Places] で、小数点以下の表示桁数を選択します。

ステップ 6　カンマ（,）やピリオド（.）などの 3 桁ごとの区切り文字を使用する場合は、[Use 1000s Separator] を選択します。

区切り文字は、ロケール設定によって決まります。

ステップ 7　[Negative Numbers] で、負の数値を表示する場合に、数値の前にマイナス記号を使用するか、または数値全体をカッコで囲むかを選択します。

ステップ 8　[Apply] をクリックします。

固定数値、科学的数値、またはパーセントのフォーマット

ステップ 1　数値データを含むカラムを選択して、[Format] を選択します。

[Number column format] ダイアログボックスが表示されます。

ステップ 2　[Format Number as] フィールドで、[Fixed]、[Scientific]、または [Percent] を選択します。

ステップ 3　[Decimal Places] フィールドで、小数点以下の表示桁数を選択します。

ステップ 4　スペース、カンマ（,）、ピリオド（.）などの 3 桁ごとの区切り文字を使用する場合は、[Use 1000s Separator] を選択します。

ステップ 5　[Negative Numbers] で、負の数値を表示する場合に、数値の前にマイナス記号を使用するか、または数値全体をカッコで囲むかを選択します。

ステップ 6　[Apply] をクリックします。

カスタム数値データのフォーマット

カスタム フォーマットを定義するには、フォーマット パターンを構築するための特別な記号を使用します。フォーマット パターンによって、通貨記号、3 桁ごとの区切り文字、小数点、またはカンマを配置する場所が指定されます。表 13-7 に、カスタム フォーマットパターン、およびそれらのパターンが数値データに適用された場合の結果の例を示します。

表 13-7　カスタム数値フォーマット パターンの結果

フォーマット パターン	データ セット内のデータ	フォーマットの結果
0000.00	12.5 124.5 1240.553	0012.50 0124.50 1240.55
#.000	100 100.25 100.2567	100.000 100.250 100.257
$#,###	2000.00 20000.00	$2,000 $20,000
ID #	15	ID 15

ステップ 1　数値データ カラムを選択して、[Format] をクリックします。

[Number column format] ダイアログボックスが表示されます。

ステップ 2　[Format Number as] フィールドで、ドロップダウン リストから [Custom] を選択します。

2 番めのフィールド [Format Code] が表示されます。

ステップ 3　[Format Code] フィールドで、表 13-7 に示すようなフォーマット パターンを入力します。

ステップ 4　[Apply] をクリックします。

ストリング データのフォーマット

ステップ 1　ストリング データを含むカラムのフォーマットを定義するには、カラムを選択して、[Format] をクリックします。

[String column format] ダイアログボックスが表示されます。

ステップ 2　ドロップダウン リストからオプションを選択します。標準的なストリング データ型のオプションについては、表 13-6 を参照してください。

ステップ 3　[Apply] をクリックします。

カスタム ストリング データのフォーマット

ストリングの特定の位置にスペースや句読点を配置するなどの特別なフォーマットを含むようにストリング データをフォーマットできます。たとえば、次のようなフォーマットで電話番号を表示できます。

```
(415) 555-2121 ext. 2296
415.555.2121
415-555-2121
```

ストリング データのカスタム フォーマットを作成できます。表 13-8 に、カスタム ストリング フォーマットを定義する場合に使用できる記号を示します。

表 13-8　カスタム ストリング フォーマット定義用の記号

記号	説明
@	文字のプレースホルダです。各 @ 文字は、ストリング内の 1 文字を表します。フォーマット パターン内の @ 記号の数よりもストリングの文字数が少ない場合は、スペースが挿入されます。 プレースホルダには、右詰めで文字が設定されます。ただし、フォーマット パターンの先頭に感嘆符（!）を指定した場合は、左詰めとなります。例については、表 13-9 を参照してください。
&	ストリングの文字数が少ない場合にスペースが挿入されない点を除いて、@ と同じです。例については、表 13-9 を参照してください。
!	プレースホルダに左詰めで文字を設定することを指定します。例については、表 13-9 を参照してください。
>	ストリングの文字を大文字に変換します。
<	ストリングの文字を小文字に変換します。

表 13-9 に、カスタム ストリング フォーマット パターン、およびそれらのパターンがテキスト データに適用された場合の結果の例を示します。

表 13-9　カスタム ストリング フォーマット パターンの結果

フォーマット パターン	データ ソース内のデータ	フォーマットの結果
(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 (　) 555-1007
(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 () 555-1007
!(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 (555) 100-7
!(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 (555) 100-7
!(@@@) @@@-@@@@ + ext 9	5551007	(555) 100-7　+ ext 9
!(&&&) &&&-&&&& + ext 9	5551007	(555) 100-7 + ext 9
>&&&-&&&&&-&&	D1234567xy	D12-34567-XY
<&&&-&&&&&-&&	D1234567xy	d12-34567-xy

ステップ 1　ストリング データのカラムを選択して、[Format] をクリックします。

[String column format] ウィンドウが表示されます。

ステップ 2　[Format String as] フィールドで、[Custom] を選択します。

2 番めのフィールド [Format Code] が表示されます。

ステップ 3　[Format Code] フィールドで、表 13-9 に示すようなフォーマット パターンを入力します。

ステップ 4　[Apply] をクリックします。

日時のフォーマット

日時のデータのフォーマットは、使用しているロケールに応じて異なります。たとえば、太平洋標準時タイム ゾーンのアメリカ英語ロケールでは、次の日時が表示されます。

```
March 5, 2007 11:00:00 AM PST
```

次の例は、同じ日時をフランス語（フランス）ロケールで表示したものです。

```
5 mars 2007 11:00:00 HNP (ÈUA)
```

日時のカラムでは、データ ソースによって日付と時刻の両方、日付だけ、または時刻だけが提供されます。データ ソースによって日付データと時刻データの両方が提供される場合は、日付だけ、時刻だけ、または日付と時刻の両方を表示するフォーマットをカラムに適用できます。また、日付または時刻の具体的なフォーマットを選択することもできます。たとえば、データ カラムに次の値が表示されているとします。

```
April 3, 2006 11:35 a.m.
```

この場合、カラムに対して [Short Date] フォーマットを選択すると、データの日付部分だけが次のフォーマットで表示されます。

```
4/3/06
```

表 13-6 に、標準的な日時データ型のフォーマットを示します。

ステップ 1　日付または時刻のデータが含まれているカラムを選択して、[Format] をクリックします。

[Date or Time Format] ウィンドウが表示されます。

ステップ 2　[Format Date or Time As] フィールドで、目的のオプションを選択します。

ステップ 3　[Apply] をクリックします。

日付と時刻のカスタム フォーマット

カスタム日付フォーマットを設定できます。ただし、カスタム日付フォーマットは、レポートが単一ロケールで表示される場合にだけ使用してください。カスタム フォーマットを使用すると、常に設定したフォーマットで日付が表示されるため、異なるロケールでは内容が伝わらない可能性があります。

たとえば、MM-dd-yy というフォーマットを使用すると、2006 年 1 月 10 日は、レポートが表示されるロケールとは関係なく常に 01-10-06 と表示されます。日 - 月 - 年というフォーマットで日付が表示されるロケールでは、01-10-06 は 2006 年 10 月 1 日と解釈されます。

表 13-10 に、カスタム フォーマット、およびデータ ソースに 2006 年 4 月 15 日として保存されている日付にそれらのフォーマットが適用された場合の結果の例を示します。

表 13-10　カスタム日付フォーマットの結果

フォーマット	フォーマットの結果
MM-dd-yy	04-15-06
E, M/d/yyyy	Fri, 4/15/2006
MMM d	Apr 15
MMMM	April
yyyy	2006
W	3（その月の何週めか）
w	14（その年の何週めか）
D	105（その年の何日めか）

日付または時刻のカスタム フォーマットを作成するには、次の手順を実行します。

ステップ 1　日時のカラムを選択して、[Format] をクリックします。

[Date or Time column format] ウィンドウが表示されます。

ステップ 2　[Format Date or Time As] フィールドで、[Custom] を選択します。

2 番めのフィールド [Format Code] が表示されます。

ステップ 3　[Format Code] フィールドで、表 13-10 に示すようなフォーマット パターンを入力します。

ステップ 4　[Apply] をクリックします。

ブール データのフォーマット

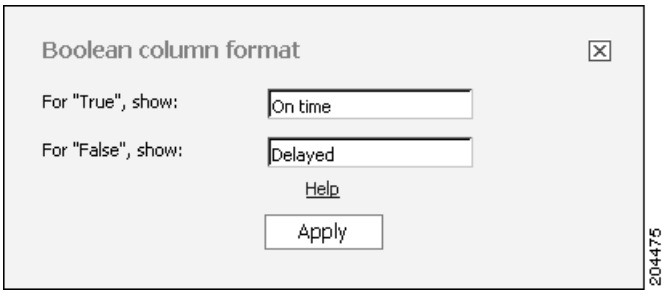
ブール式は、True または False と評価されます。たとえば、次の式によって計算カラムを作成するとします。

```
ActualShipDate <= TargetShipDate
```

実際の出荷日が目標出荷日以前であれば、式は True となります。実際の出荷日が目標出荷日よりあとであれば、式は False となります。

ブール データ型のカラムをフォーマットしない場合、カラムには True および False という値が表示されます。異なるラベルを指定するには、カラムを選択して、[Format Data] を選択します。その後、図 13-17 に示すように、[Boolean Column Format] でラベルを入力します。

図 13-17　True および False の表示値の指定



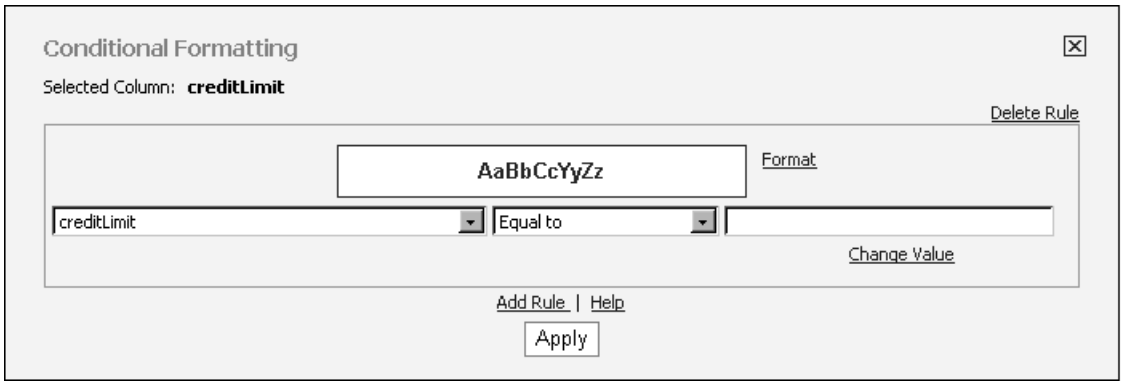
条件フォーマットの適用

条件フォーマットを使用すると、一定の条件が満たされた場合にデータのフォーマットが変更されます。たとえば、顧客の期限超過請求書を表示するレポートにおいて、期限を 90 日以上超過しているすべての顧客名を赤色で強調表示できます。また、それに加えて、期限を 60 日以上超過しているすべての顧客名を青色で強調表示することもできます。

条件フォーマットを設定するには、カラムを右クリックし、[Style] > [Conditional Formatting] を選択して、[Conditional Formatting] ダイアログボックスを開きます。1 つのカラムに、最大 3 つの条件フォーマット規則を設定できます。条件フォーマットを削除または変更することもできます。

[Conditional Formatting] で、選択したカラムのデータを表示するための規則、つまり条件を作成します。規則には、満たされる必要がある条件、および適用するフォーマットの両方が含まれます。
図 13-18 に、[Conditional Formatting] ダイアログボックスを示します。

図 13-18　Interactive Viewer の [Conditional Formatting] ダイアログボックス



カラムのフォーマットを他のカラムの値に基づいて決定できます。たとえば、[CustomerName] カラムを選択し、[creditRank] カラムに基づいて条件を設定することによって、顧客の creditRank が特定の値である場合に顧客名に条件フォーマットを適用できます。

比較対象カラムのデータが null である場合や False である場合などの、さまざまなタイプの比較を設定できます。また、カラム値を 1 つまたは 2 つの他の値と比較することもできます。たとえば、データがある値以下の場合に条件フォーマットを適用するように指定できます。

値が 2 つの値の範囲内にあるか、または範囲外にあるかをチェックすることもできます。たとえば、注文合計金額が $10,000 と $100,000 の間にある場合に条件フォーマットを適用するように指定できます。この設定を行った場合、注文合計金額が $10,000 と $100,000 の間にあるすべての顧客の名前に条件フォーマットが適用されます。

条件を作成したあと、条件を満たすデータを表示するためのフォーマットを設定します。フォーマットは、条件を設定するときに使用したカラムではなく、[Selected Column] のカラムに適用されます。

カラムへの条件フォーマットの設定

カラムに対して条件フォーマットを設定したり、条件フォーマットを変更したりできます。

ステップ 1　条件フォーマットを表示するカラムを右クリックします。

コンテキスト メニューが表示されます。

ステップ 2　[Style] > [Conditional Formatting] を選択します。

[Conditional Formatting] ダイアログボックスが表示されます。[Selected Column] フィールドに、条件フォーマットを表示するカラムの名前が表示されます。

ステップ 3　条件フォーマット規則を設定します。

a. 1 つめのドロップダウン リストで、条件フォーマットを適用するかどうかを決定する基準となる値を含むカラムを選択します。たとえば、顧客番号が 1000 と 1999 の間にある場合に顧客名を青色で表示するには、[CustomerNumber] を選択します。

このフィールドで選択したカラムは、[Selected Column] のカラムと同じでも、異なっていてもかまいません。

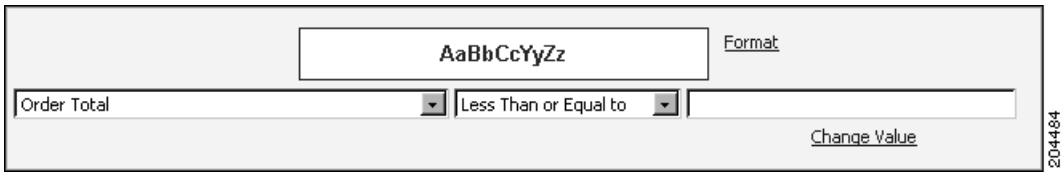
b. 次のフィールドで、ドロップダウン リストを使用して、選択したカラムに適用する演算子を選択します。[Equal to]、[Less than]、[Less than or Equal to] などを選択できます。

選択内容に応じて、0 ～ 2 つのフィールドが右側に表示されます。[Is Null]、[Is Not Null]、[Is True]、または [Is False] を選択した場合、右側にフィールドは表示されません。2 つの値を比較する演算子を選択した場合は、1 つ以上の追加のフィールドが表示されます。

c. 右側にフィールドが表示されたら、各フィールドに比較値を入力します。

たとえば、[Less than or Equal to] を選択した場合は、図 13-19 に示すように 3 つめのフィールドが表示されます。このフィールドに、比較値を入力します。入力した値以下であるすべてのデータに条件フォーマットが適用されます。

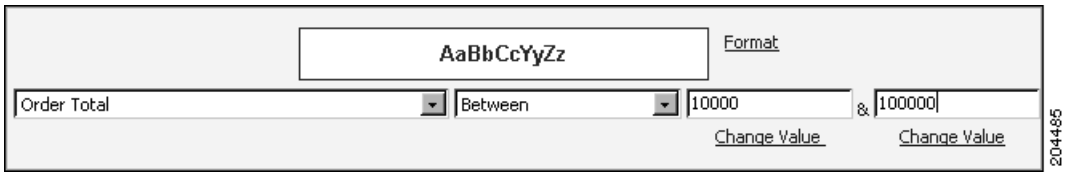
図 13-19　比較値フィールド



[Between] または [Not Between] を選択した場合は、右側に 2 つのフィールドが表示されます。これらのフィールドに、それぞれ下限値と上限値を入力します。たとえば、図 13-20 に示すように、3 つめのフィールドに注文合計金額 10,000 を、4 つめのフィールドに注文合計金額 100,000 を入力します。

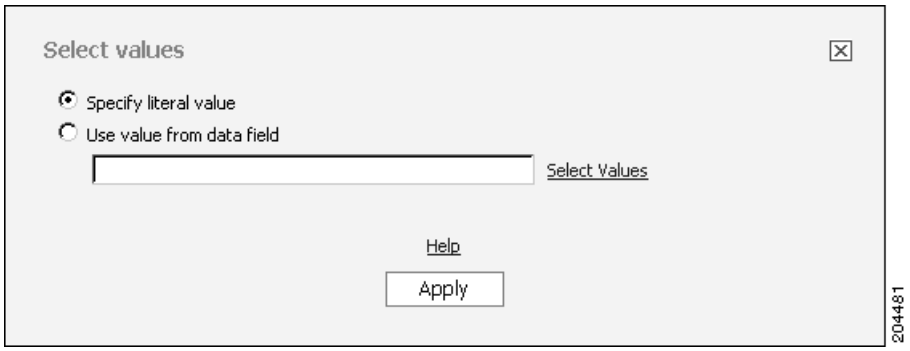
注文合計金額が $10,000 と $100,000 の間にあるすべての顧客の名前に条件フォーマットが適用されます。

図 13-20　Between 演算子で表示された 2 つの比較値フィールド



比較のための値は、直接入力することも、指定したレポート カラムから取得することもできます。図 13-21 に示す [Select values] ダイアログボックスを表示するには、[Change Value] を選択します。

図 13-21　リテラル値またはカラム値の指定

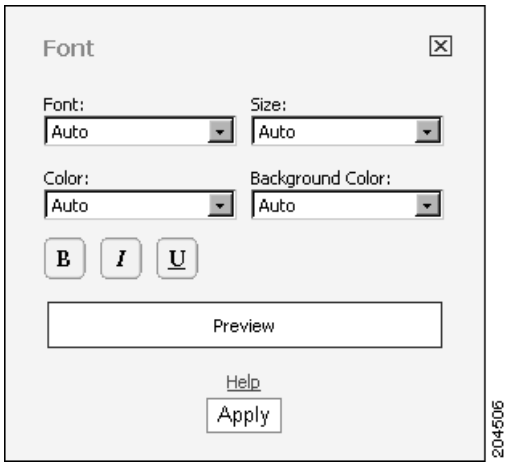


リテラル値は、直接入力することも、指定したカラムの値のリストから選択することもできます。また、レポート内の他の指定したカラムの値から取得することもできます。

ステップ 4　[Conditional Formatting] で、[Format] を選択して、条件テキスト用のフォーマットを設定します。フォント、フォント サイズ、フォント色、および背景色を設定できます。また、データを太字、イタリック体、または下線付きのフォント スタイルで表示するように指定することもできます。

ステップ 5　図 13-22 に示すように、ラベルのフォーマットに使用したのと同じ [Font] ダイアログボックスを使用してフォーマットを設定します。

図 13-22　[Font] ダイアログボックス



フォーマットを設定すると、ウィンドウの [Preview] セクションに選択したフォーマットが表示されます。

追加の条件フォーマット規則を追加するには、[Add Rule] を選択して、新しい各規則に対してステップ 3 および 4 を繰り返します。

ステップ 6　[Apply] をクリックします。

指定した条件フォーマットが適用されたレポート デザインが表示されます。

条件フォーマットの削除

カラムの条件フォーマットを削除するには、次の手順を実行します。

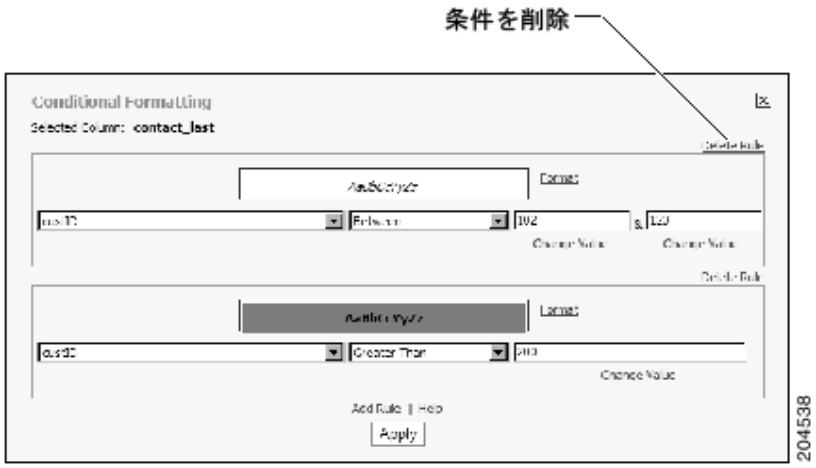
ステップ 1　カラムを選択して右クリックします。

ステップ 2　[Style] > [Conditional Formatting] を選択します。

ステップ 3　図 13-23 に示すように、[Conditional Formatting] ダイアログボックスで、削除する各条件フォーマット規則に対して [Delete Rule] をクリックします。

カラムのすべての条件フォーマットを削除するには、すべての条件フォーマット規則を削除します。

図 13-23　Interactive Viewer における条件フォーマットの削除



ステップ 4　[Apply] をクリックします。

詳細カラムにおける改ページの設定および削除

Interactive Viewer では、事前に設定した行数ごとに強制的に改ページできます。

ステップ 1　詳細カラムを選択して、右クリックします。

ステップ 2　コンテキスト メニューから、[Group] > [Page Break] を選択します。

[Page Break] ウィンドウが表示されます。

ステップ 3　[Interval] フィールドに、何行ごとに強制的に改ページするかを示す数値を入力します。

ステップ 4　[Apply] をクリックします。

グループ カラムにおける改ページの設定および削除

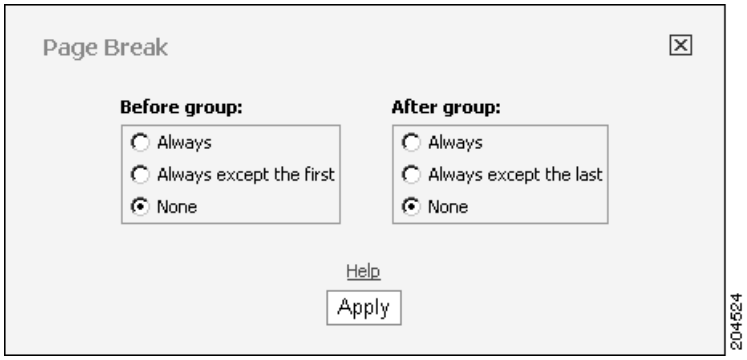
レポート デザインにグループ化されたデータが含まれている場合は、Interactive Viewer で、グループ化されたデータの前またはあとに改ページを設定できます。

ステップ 1　グループ化されたカラムを選択して、右クリックします。

ステップ 2　コンテキスト メニューから、[Group] > [Page Break] を選択します。

図 13-24 に示すように、[Page Break] ウィンドウが表示されます。

図 13-24　　改ページの設定



ステップ 3　各グループの前に改ページを設定するか、あるいは最初のグループまたは最後のグループを除いて各グループに改ページを設定するかを指定します。

既存の改ページを削除するには、[Before group] または [After group] で [None] を選択します。

ステップ 4　[Apply] をクリックします。

レポート データの構成

Interactive Viewer を使用して、レポート データを構成できます。

ここでは、次の内容について説明します。

- 「レポート データの表示および構成」（P.13-43）
- 「カラムのマージ」（P.13-46）
- 「データのソート」（P.13-48）
- 「データのグループ化」（P.13-50）
- 「レポート計算の作成」（P.13-53）
- 「集計データの使用」（P.13-63）

レポート データの表示および構成

データ ソースにアクセスして、使用するデータ セットを選択したあと、レポートにデータを表示する最適な方法を決定します。データ セットを構成するには、いくつかの方法があります。

- データ カラムを昇順または降順でソートする。
- データをグループに整理する。グループを使用すると、特定の種類の項目についてのすべての情報が 1 箇所にまとめて表示されます。たとえば、グループごとに、特定の顧客についてのすべての情報を表示できます。
- 集計データを作成する。たとえば、顧客グループの最後に、その顧客が購入した合計金額や、各注文の平均金額を表示できます。また、合計、標準偏差、順位、差異などの計算を作成することもできます。

Interactive Viewer におけるカラムの並べ替え

カラムを並べ替えるには、次の手順を実行します。

ステップ 1　カラムを選択して右クリックします。

ステップ 2　コンテキスト メニューから、[Column] > [Reorder Columns] を選択します。

[Arrange Columns] ウィンドウが表示されます。

ステップ 3　移動するカラムを選択します。

（注）　詳細行だけを選択できます。グループやセクションは選択できません。

ステップ 4　右側にある上矢印または下矢印をクリックして、カラムを適切な位置に移動します。

ステップ 5　[Apply] をクリックします。

カラムからグループ ヘッダーへのデータ値の移動

データ値をカラムの詳細行からグループ ヘッダーに移動できます。

ステップ 1　カラムを選択して右クリックします。

たとえば、図 13-25 は、顧客の [Name] カラムが選択されている様子を示しています。

図 13-25　国によってグループ化された顧客が表示されたレポート

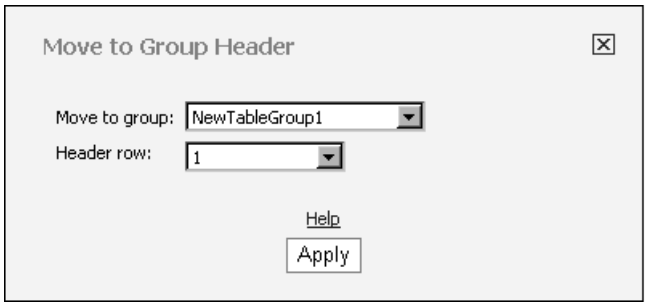
	Customer Number	Name	City	State	Sales Volume	Credit Limit
⊟ Australia						
	114	Alustrian Collectors, Co.	Melbourne	Victoria	1611	117300
	276	Anna's Decorations, Ltd	North Sydney	NSW	1611	107800
	282	Souveniers And Things Co.	Chatswood	NSW	1611	93300
	333	Alustrian Gift Network, Co	South Brisbane	Queensland	1611	51600
	471	Alustrian Collectables, Ltd	Glen Waverly	Victoria	1611	60300
⊟ Austria						
	382	Salzburg Collectables	Salzburg		1401	71700
	452	Mini Auto Werke	Graz		1401	45300

204533

ステップ 2　[Column] > [Move to Group Header] を選択します。

図 13-26 に示すように、[Move to Group Header] ウィンドウが表示されます。

図 13-26　[Move to Group Header] ダイアログボックス



ステップ 3　[Move to Group] フィールドから、値を選択します。

ステップ 4　[Header row] フィールドで、ステップ 3 で選択した値を移動する先の行番号を選択します。

ステップ 5　[Apply] をクリックします。

図 13-27 に示すように、各グループの最初の詳細行のデータ値が、各グループ ヘッダーに表示されます。[Name] カラムには、各国のグループ ヘッダーの隣に顧客名が 1 つ表示されます。

図 13-27　各グループ ヘッダーに顧客名が表示されたレポート

	Name	Customer Number	City	State	Sales Volume	Credit Limit
⊟ Australia	Alustrian Collectors, Co.					
		114	Melbourne	Victoria	1611	117300
		276	North Sydney	NSW	1611	107800
		282	Chatswood	NSW	1611	93300
		333	South Brisbane	Queensland	1611	51600
		471	Glen Waverly	Victoria	1611	60300
⊟ Austria	Salzburg Collectables					
		382	Salzburg		1401	71700
		452	Graz		1401	45300

204534

カラムの削除

カラムを削除するには、カラムを選択して、[Delete] をクリックします。レポートからカラムを削除しても、カラムは情報オブジェクトまたはその他のデータ ソースからは削除されません。

複数のカラムを削除するには、Ctrl キーを押しながら削除するカラムを選択します。その後、[Delete] をクリックします。

レポート項目の非表示または表示

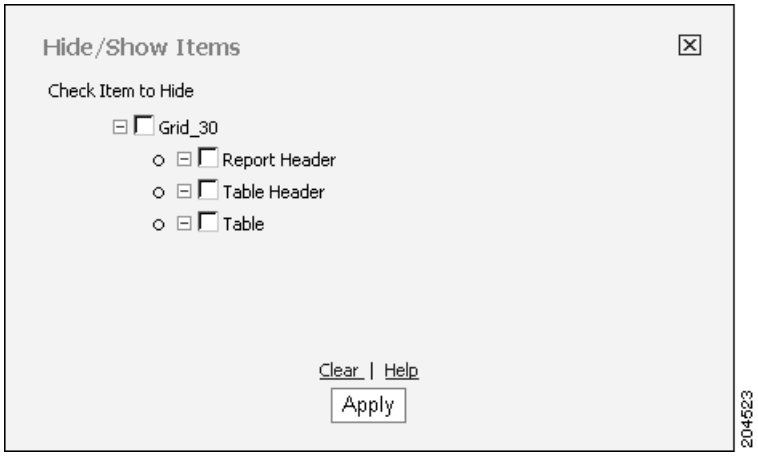
レポート項目を表示または非表示にするには、次の手順を実行します。

ステップ 1　カラムを選択して右クリックします。

ステップ 2　[Hide or Show Items] を選択します。

図 13-28 に示すような [Hide/Show Items] ダイアログボックスが表示されます。

図 13-28　レポート項目の非表示または表示



ステップ 3　非表示にするすべての項目をオンにするか、表示するすべての非表示項目をオフにします。
すべての非表示項目を表示するには、[Clear] をクリックします。

ステップ 4　[Apply] をクリックします。

カラムの非表示

カラムを表示または非表示にするには、次の手順を実行します。

ステップ 1　カラムを選択して右クリックします。

ステップ 2　[Column] > [Hide Column] を選択します。
Interactive Viewer で表示されるレポートには、非表示にしたカラムは表示されなくなります。

非表示カラムの表示

非表示カラムを表示するには、次の手順を実行します。

ステップ 1　カラムを選択して右クリックします。

ステップ 2　[Column] > [Show Columns] を選択します。
[Show Columns] ダイアログボックスが表示されます。

ステップ 3　表示するすべての項目を選択します。複数のカラムを選択する場合は、Ctrl を押しながら選択します。

ステップ 4　[Apply] をクリックします。

カラムのマージ

2 つ以上のカラムのデータを 1 つのカラムにマージできます。たとえば、図 13-29 では、[City and state or province] カラム ヘッダーの下のカラムは別々のカラムになっています。

図 13-29　別々のカラム

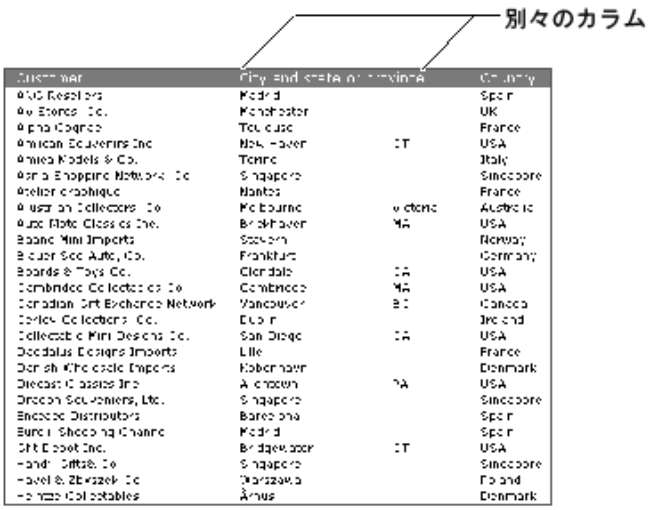


図 13-30 では、これら 2 つのカラムのデータが 1 つのカラムにマージされています。

図 13-30　マージされたカラム

Customer	City and state or province	Country
ANG Resellers	Madrid	Spain
AV Stores, Co.	Manchester	UK
Alpha Cognac	Toulouse	France
American Souvenirs Inc	New Haven CT	USA
Amica Models & Co.	Torino	Italy
Asnia Shopping Network, Co	Singapore	Singapore
Atelier graphique	Nantes	France
Alustrian Collectors, Co.	Melbourne Victoria	Australia
Auto-Moto Classics Inc.	Brickhaven MA	USA
Baane Mini Imports	Stavern	Norway
Blauer See Auto, Co.	Frankfurt	Germany
Boards & Toys Co.	Glendale CA	USA
Cambridge Collectables Co.	Cambridge MA	USA

204530

複数のカラムのデータをマージするには、次の手順を実行します。

ステップ 1　カラムを選択して右クリックします。

ステップ 2　[Column] > [Merge Columns] を選択します。

マージされたカラムからのカラムの選択

複数のカラムからマージされたデータを含むカラムのデータを集計、フィルタリング、およびグループ化できます。まず、データを集計、フィルタリング、またはグループ化する対象のカラムを 1 つ選択する必要があります。

マージされたカラムから 1 つのカラムを選択するには、次の手順を実行します。

ステップ 1　マージされたカラムを選択し、右クリックして、適用するコマンドを [Aggregation]、[Filter] > [Filter]、[Group] > [Add Group] などのコンテキスト メニューから選択します。

[Select data item] ダイアログボックスが表示されます。

ステップ 2　[Select data] ドロップダウン リストから、コマンドを適用するカラム名を選択して、[Apply] をクリックします。

コマンドを適用するために追加の情報を指定する必要がある場合は、Interactive Viewer によってダイアログボックスが表示されます。たとえば、[Aggregation] を選択した場合は、[Aggregation] ダイアログボックスが表示されます。

データのソート

レポート デザインでデータを配置すると、データ ソースによってデータ行のデフォルトのソート順序が決定されます。データ ソースでカラムが昇順でソートされている場合、そのカラムは、デザインでも昇順でソートされます。ただし、通常は、データ ソース内ではデータはランダムに並べられています。

たとえば、通常は、顧客名のカラムは、アルファベット順ではなく、顧客がデータベースに追加された順に並べられています。したがって、見やすいレポートを作成するために、データのソートは重要なタスクとなります。

データをソートするには、3 種類の方法があります。

- 「単一のカラムのソート」（P.13-48）
- 「複数のカラムのソート」（P.13-48）

単一のカラムのソート

単一のカラムに対して単純なソートを実行するには、カラムを選択して、[Sort Ascending] または [Sort Descending] を選択します。レポート内のすべてのデータ行が調整されて、新しいソート順序が反映されます。

単純なソートを実行したあとにデータを元の順序に戻すには、[Undo] を選択します。

複数のカラムのソート

レポート内の複数のカラムをソートできます。

ステップ 1　カラムを選択して右クリックします。

ステップ 2　コンテキスト メニューから、[Sort] > [Advanced Sort] を選択します。

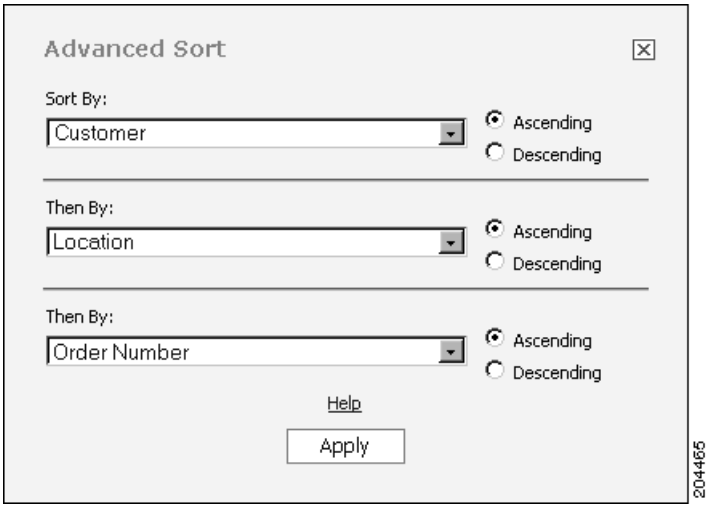
ステップ 3　1 つめのドロップダウン リストからカラムを選択し、順序として [Ascending] または [Descending] を選択します。後続のカラムも選択して、ソート順序を選択します。

複数のカラムをソートする場合は、ソートの優先順位を理解することが重要です。[Advanced Sort] では、最初に選択したカラムが最も優先的にソートされるカラムとなります。レポート データは、まずこのカラムによってソートされます。

たとえば、[Customer] カラムを最初に選択し、ソート順序として [Ascending] を選択した場合、レポートでは顧客がアルファベット順に表示されます。次のカラムとして [Location] を選択し、ソート順序として [Ascending] を選択した場合、[Customer] の各エントリ内で、場所が昇順でソートされます。

3 つめのカラムとして [Order Number] を選択し、ソート順序として [Ascending] を選択した場合、各場所内で、注文番号が昇順でソートされます。図 13-31 に、この複数カラムによるソートの結果を示します。

図 13-31　　複数のカラムのソート



Customer	Location	Order Number	Order Status	Unit Price	Quantity	Order Totals
Barginton Financial	Boston	1555	Open	$4	212	$848
		1625		$6	158	$948
				$8	161	$1,288
				$11	160	$1,760
				$11	161	$1,771
				$12	159	$1,908
	New Haven	1570		$9	215	$1,935
				$15	157	$2,355
				$15	157	$2,355
Chardlen Corporation	Dallas	1345		$12	210	$2,520
				$18	158	$2,844
	Sacramento	1621		$15	210	$3,150
				$20	158	$3,160
				$21	159	$3,339

204547

グループ化されたデータがレポートで使用されている場合、[Advanced Sort] のドロップダウン リストには、レポートの詳細カラムだけが表示されます。データのグループ化に使用したカラムは表示されません。

データのグループ化

レポートには、大量のデータが含まれる場合があります。企業が所有するすべての品目、および各品目の購入価格、購入日、在庫タグ番号、仕入先などの情報をリストするタスクを考えます。

レポートでこれらすべての品目をばらばらの状態で表示した場合、品目はレポート全体に散らばっているため、たとえば企業が重機にいくら支出したかを特定できなくなります。

オフィス家具を最も低い価格で販売する仕入先を確認することもできません。また、どの在庫品目が現地事務所にあり、どの品目が倉庫にあるかを判断することも簡単ではありません。図 13-32 に、グループ化されていないレポートの 1 ページめの例を示します。

図 13-32　　グループ化されていないデータ

Item	Category	Inventory Code	Description	Building Location	Office Location	Purchase Price	Purchase Date	Supplier
Executive desk with return	Office Furniture	1007-431	Mahogany, 71"x 28", 4 drawers	Bldg 1	Office 601	789.99	2/1/2004	Grant Furniture
Forklift	Equipment	219-62389	3000 lb capacity, model 3398	Warehouse A		1594.78	3/6/2004	Grant Furniture
Wing chair	Office Furniture	1509-4459	Dark brown leather with stud trim	Bldg 1	Lobby A	259.98	1/17/2005	Grant Furniture
Light tower	Heavy Equipment	4408-3221	2002 Genie TML4000N	Warehouse C		4200.00	1/6/2003	Sal's Dining Rooms
Credenza	Office Furniture	336-9887	Mahogany, 64"x 36"x 48", 6 drawers	Bldg 1	Office 601	449.75	2/1/2004	Grant Furniture
Air compressor	Heavy Equipment	3398-9907	Diesel, 185 CFM	Warehouse C		9500.00	3/6/2004	Grant Furniture
Dining table	Cafeteria Furniture	1248-4339	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Secretary's chair	Office Furniture	1005-4498	Black ergonomic chair	Bldg 2	Office 422	149.99	3/2/2002	Sal's Dining Rooms
Conference table	Office Furniture	1098-7543	Oval mahogany table, 8 ft x 5 ft x 30"	Bldg 1	Board room	1459.98	4/17/2002	Grant Furniture
Credenza	Office Furniture	336-9887	Mahogany, 64"x 36"x 48, 6 drawers	Bldg 1	Office 403	449.75	2/1/2004	Grant Furniture
Forklift	Equipment	219-66737	5,000 lb capacity, model 2890	Warehouse A		2200.78	3/6/2004	Sal's Dining Rooms
Dining table	Cafeteria Furniture	1248-4401	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	Cafeteria Furniture	1248-4335	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Wing chair	Office Furniture	1508-3389	Dark brown leather with stud trim	Bldg 1	Lobby A	259.98	1/17/2005	Sal's Dining Rooms
Executive desk with return	Office Furniture	1004-322	Steel, 71"x 36", 3 drawers	Bldg 2	Office 423	629.29	3/3/2005	Grant Furniture
Credenza	Office Furniture	336-9887	Mahogany, 64"x 36"x 48, 6 drawers	Bldg 1	Office 423	449.75	2/1/2004	Sal's Dining Rooms
Executive desk with return	Office Furniture	1005-2112	Mahogany, 71"x 28", 4 drawers	Bldg 1	Office 604	789.99	2/1/2004	Sal's Dining Rooms
Secretary's chair	Office Furniture	1005-4498	Black ergonomic chair	Bldg 2	Office 422	149.99	3/2/2002	Sal's Dining Rooms
Crawler loader	Heavy equipment	2020-3731	Model 450D	Warehouse A		9200.00	6/04/2003	Grant Furniture

204513

これらすべての情報を見やすい在庫レポートに整理するために、データ グループおよびデータ セクションを作成します。データ グループには、関連するデータ行が含まれます。

たとえば、あるグループにはすべての重機が、別のグループにはすべてのオフィス家具が、さらに別のグループにはすべての通信機器が含まれているレポートを作成できます。各グループでは、合計購入額や、グループ内の品目数などの集計データを表示できます。

データをグループ化することによって、レポートはより洗練されて見やすくなり、簡単にデータを比較したり、計算したりできるようになります。

図 13-33 に、同じ在庫をカテゴリごとにグループ化し、各ページに 1 つのカテゴリを表示したレポートを示します。

図 13-33　グループ化されたデータ

Category: Cafeteria Furniture							
Item	**Inventory Code**	**Description**	**Building Location**	**Office Location**	**Purchase Price**	**Purchase Date**	**Supplier**
Dining table	1248-4339	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	1248-4401	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	1248-4335	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	1248-4492	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Total purchase price					515.92		

204512

データは、レポート デザイン エディタまたは Interactive Viewer でグループ化できます。ビューアで行った変更は、レポート デザインには反映されません。Enterprise モードで作業している場合は、変更内容を反映したレポート出力を保存できます。

必要なグループ化がレポート デザインで行われていない場合には、Interactive Viewer でデータ グループを追加または削除できます。ここで変更した内容は、Interactive Viewer を閉じるまでの間有効です。

グループの追加

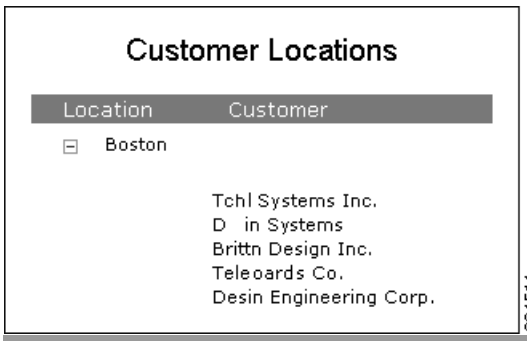
グループを追加するには、次の手順を実行します。

ステップ 1　グループの作成に使用するカラムを選択して右クリックします。

ステップ 2　コンテキスト メニューから、[Group] > [Add Group] を選択します。

ビューアに、新しいグループが表示されます。図 13-34 に示すように、グループを展開すると、すべての詳細行が表示されます。グループを縮小するには、グループ名の隣にあるマイナス記号（-）をクリックします。

図 13-34　グループの追加



日付または時刻に基づくデータのグループ化

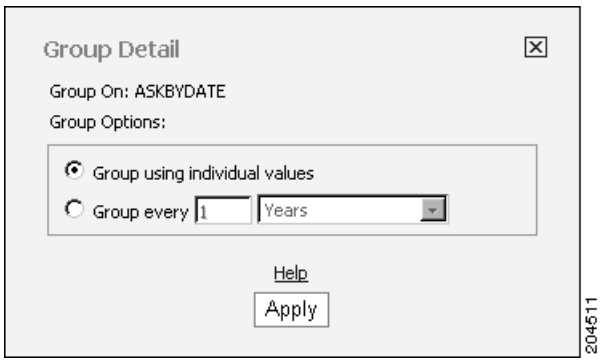
日付または時刻のデータを含むカラムに基づいてグループを作成する場合は、グループ化の基準となる間隔を設定できます。たとえば、カラムに時刻データが含まれている場合は、一定の時間数、分数、または秒数ごとにグループ化できます。

ステップ 1　グループの作成に使用するカラムを選択して右クリックします。

ステップ 2　コンテキスト メニューから、[Group] > [Add Group] を選択します。

図 13-35 に示すように、[Group Detail] ダイアログボックスが表示されます。

図 13-35　日付または時刻のデータに基づくグループ化

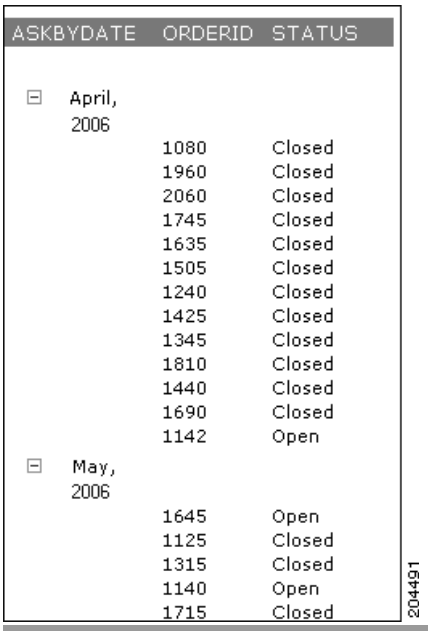


ステップ 3　個別の日付または時刻の値を表示する場合は、デフォルトの [Group using individual values] 設定のままにします。

ステップ 4　グループ化の間隔を設定するには、[Group every] を選択して、値を入力し、グループ化間隔の単位を選択します。

たとえば、月ごとに新しいグループを作成する場合は、1 を入力して、ドロップダウン リストから [Month] を選択します。これにより、図 13-36 に示すように、レポートに月次データのグループが表示されます。

図 13-36　月ごとにグループ化されたデータ



内部グループの削除

内部グループを削除するには、次の手順を実行します。

ステップ 1　削除するグループのカラムを選択して、右クリックします。

ステップ 2　コンテキスト メニューから、[Group] > [Delete Inner Group] を選択します。

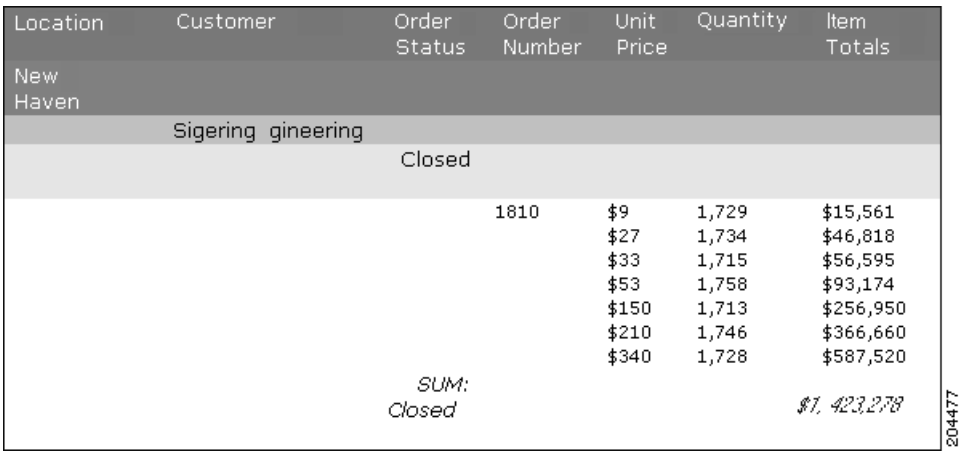
レポート計算の作成

ほとんどのレポートでは、売上、会計、在庫などの重要な事業活動を追跡するための何らかの計算が必要となります。倉庫内の品目数を単純に集計するだけでよい場合もあれば、株式ポートフォリオのパフォーマンスを経時的に追跡するなどの複雑な会計データを提供する必要がある場合もあります。

カウント、加算、減算、乗算、除算などの、一般的な数学的関数を使用できます。さらに、これらの基本的な関数を拡張した式を記述することもできます。

計算したデータをレポートに表示するには、図 13-37 に示すような計算カラムを作成します。この図では、[Item Totals] カラムには、単価に数量を乗算した積が表示されています。

図 13-37　計算カラム



Location	Customer	Order Status	Order Number	Unit Price	Quantity	Item Totals
New Haven						
	Sigering gineering					
		Closed				
			1810	$9	1,729	$15,561
				$27	1,734	$46,818
				$33	1,715	$56,595
				$53	1,758	$93,174
				$150	1,713	$256,950
				$210	1,746	$366,660
				$340	1,728	$587,520
		SUM: Closed				$1,423,278

204477

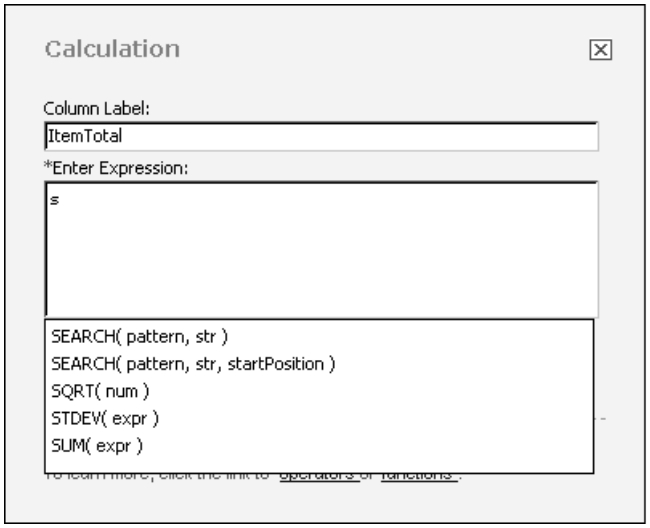
計算を作成するには、次の手順を実行します。

- 計算カラムのタイトルを指定します。
- どのデータを使用し、計算したデータをレポート内でどのように表示するかを示す式を記述します。

  式には、1 つの関数と、1 つ以上の引数が含まれます。引数とは、計算を作成するために使用するデータを示します。

  図 13-38 に示すように、[Calculation] の [Enter Expression] に関数名の 1 文字めを入力すると、その文字で始まる関数のリストが表示されます。関数を選択して、引数を指定します。

図 13-38　関数の選択



サポートされている計算関数について

表 13-11 に、計算の作成に使用できる関数の例を示します。

（注）　[Calculation] ダイアログボックスでは、式における大文字の TRUE 関数および FALSE 関数の使用はサポートされていません。1 文字めが大文字の True と False の使用もサポートされていません。これらの関数は、すべて小文字で記述する必要があります。

表 13-11　関数の例

機能	説明	使用例
ABS(num)	カラムのデータの絶対値が表示されます。	`ABS([TemperatureCelsius])`
ADD_DAY(date, daysToAdd)	指定した日数を日付の値に加算して、その結果が日付の値として表示されます。	`ADD_DAY([ClosingDate], 30)`
ADD_HOUR(date, hoursToAdd)	指定した時間数を時刻の値に加算して、その結果が時刻の値として表示されます。	`ADD_HOUR([OpenHour], 8)`
ADD_MINUTE(date, minutesToAdd)	指定した分数を時刻の値に加算して、その結果が時刻の値として表示されます。	`ADD_MINUTE([StartTime], 60)`
ADD_MONTH(date, monthsToAdd)	指定した月数を日付の値に加算して、その結果が日付の値として表示されます。	`ADD_MONTH([InitialRelease], 2)`
ADD_QUARTER(date, quartersToAdd)	指定した四半期数が日付の値に加算されます。	`ADD_QUARTER([ForecastClosing], 2)`
ADD_SECOND(date, secondsToAdd)	指定した秒数が時刻の値に加算されます。	`ADD_SECOND([StartTime], 30)`
ADD_WEEK(date, weeksToAdd)	指定した週数を日付の値に加算して、その結果が日付の値として表示されます。	`ADD_WEEK([askByDate], 4)`
ADD_YEAR(date, yearsToAdd)	指定した年数が日付の値に加算されます。	`ADD_YEAR([HireDate], 5)`

表 13-11　関数の例 （続き）

機能	説明	使用例
AND	2 つの条件を組み合わせて、両方の条件に一致するレコードが返されます。たとえば、1 年間に $50,000 より多く支出し、かつ信用格付けが A である顧客のレコードを要求できます。	この関数は、式で句を接続する場合に使用し、引数を取りません。
AVERAGE(expr)	カラムの平均値が表示されます。	`AVERAGE([CostPerUnit])`
AVERAGE(expr, groupLevel)	指定したグループ レベルの平均値が表示されます。	`AVERAGE([TotalCost], 2)`
BETWEEN(value, upperBound, lowerBound)	指定したカラムで、値が指定した 2 つの値の範囲内にある場合には True が、範囲外にある場合は False が表示されます。 ストリング値および日付値または時刻値は、引用符で囲む必要があります。日付および時刻については、短い日付フォーマットおよび短い時刻フォーマットを使用します。	`BETWEEN([PostalCode], 11209, 12701)` `BETWEEN([ReceiptDate], "10/01/06", "12/31/06")`
CEILING(num, significance)	0 から始まって、指定した基準値の倍数に最も近い整数に数値が切り上げられます。 倍精度実数や単精度実数から整数に変換されたデータにおいては、単精度実数または倍精度実数以上の最も小さい整数が表示されます。	`CEILING([PortfolioAverage], 1)`
COUNT( )	テーブルの行数がカウントされます。	`COUNT( )`
COUNT(groupLevel)	指定したグループ レベルの行数がカウントされます。	`COUNT(2)`
COUNTDISTINCT(expr)	テーブル内の重複しない値を含む行数がカウントされます。	`COUNTDISTINCT([CustomerID])` `COUNTDISTINCT([Volume]*2)`
COUNTDISTINCT (expr, groupLevel)	指定したグループ レベルにおける重複しない値を含む行数がカウントされます。	`COUNTDISTINCT([CustomerID], 3)`
DAY(date)	日時の値において、その月の何日めであるかが 1 ～ 31 の数字で表示されます。	`DAY([forecastShipping])`
DIFF_DAY(date1, date2)	2 つの日付の値の差異が日数で表示されます。	`DIFF_DAY([checkoutDate], [returnDate])`
DIFF_HOUR(date1, date2)	2 つの時刻の値の差異が時間数で表示されます。	`DIFF_HOUR([StartTime],[Finish Time])`
DIFF_MINUTE(date1, date2)	2 つの時刻の値の差異が分数で表示されます。	`DIFF_MINUTE([StartTime], [FinishTime])`
DIFF_MONTH(date1, date2)	2 つの日付の値の差異が月数で表示されます。	`DIFF_MONTH([askByDate], [shipByDate])`
DIFF_QUARTER(date1, date2)	2 つの日付の値の差異が四半期数で表示されます。	`DIFF_QUARTER([PlanClosing], [ActualClosing])`
DIFF_SECOND(date1, date2)	2 つの時刻の値の差異が秒数で表示されます。	`DIFF_SECOND([StartTime], [FinishTime])`
DIFF_WEEK(date1, date2)	2 つの日付の値の差異が週数で表示されます。	`DIFF_WEEK([askByDate], [shipByDate])`
DIFF_YEAR(date1, date2)	2 つの日付の値の差異が年数で表示されます。	`DIFF_YEAR([HireDate], [TerminationDate])`

表 13-11　関数の例 （続き）

機能	説明	使用例
False	ブール値の False です。この関数は、引数が false であることを示すために式で使用します。	次の例は、2 つめの引数 ascending（昇順）が False であり、したがって値が降順で返される必要があることを示しています。 `RANK([Score], false)`
FIND(strToFind, str)	指定したテキストが最初に出現する場所のインデックスが表示されます。インデックスは 0 が基準です。検索では、大文字と小文字が区別されます。また、検索ストリングにワイルドカードを含めることはできません。 strToFind 引数の値は、引用符で囲む必要があります。	`FIND("HQ", [OfficeName])`
FIND(strToFind, str, startPosition)	FIND(strToFind, str) と同様ですが、検索開始位置を指定できます。インデックスは 0 が基準です。	`FIND("HQ", [OfficeName], 3)`
FIRST(expr)	指定したカラムで最初に出現する値が計算カラムに配置されます。この関数では、特定の値に対する行ごとの比較結果の表示がサポートされています。	`FIRST([customerID])`
FIRST(expr, groupLevel)	指定したグループ レベルにおいて、指定したカラムで最初に出現する値が表示されます。	`FIRST([customerID], 3)`
IF(condition, doIfTrue, doIfFalse)	If...Then...Else 文の結果が表示されます。	`IF([purchaseVolume] >5 , 7 , 0)` 値は次のとおりです。 • [purchaseVolume] はカラム名であり、>5 がテスト条件です。 • 7 は、条件が true である場合に新しいカラムに配置される値です。 • 0 は、条件が false である場合に新しいカラムに配置される値です。

IN(value, check)	データ行に check 引数で指定された値が含まれている場合は True が、含まれていない場合は False が表示されます。
	ストリング値および日付値または時刻値は、引用符で囲む必要があります。日付および時刻については、使用するロケールの短い日付フォーマットおよび短い時刻フォーマットを使用します。
		`IN([custID], 101)`
		`IN([city], "New Haven")`
		`IN([FinishTime], "16:09")`

IN(value, check1, ..., checkN)	データ行に check 引数のリストで指定されたいずれかの値が含まれている場合は True が、含まれていない場合は False が表示されます。 ストリング値および日付値または時刻値は、引用符で囲む必要があります。日付および時刻については、使用するロケールの短い日付フォーマットおよび短い時刻フォーマットを使用します。	`IN([city], "New Haven", "Baltimore", "Cooperstown")` `IN([ShipDate], "05/01/06", "05/10/06", "05/15/06")`
ISBOTTOMN(expr, n)	式の値が下位 *n* 個に含まれる場合は True が、含まれない場合は False が表示されます。	`ISBOTTOMN([OrderTotals], 50)`

表 13-11　関数の例 （続き）

機能	説明	使用例
ISBOTTOMN(expr, n, groupLevel)	指定したグループ レベルにおいて、式の値が下位 *n* 個に含まれる場合は True が、含まれない場合は False が表示されます。	`ISBOTTOMN([OrderTotals], 50, 2)`
ISBOTTOMNPERCENT (expr, percent)	下位 *n* パーセントに含まれるかどうかが表示されます。	`ISBOTTOMNPERCENT([Sales Total], 5)`
ISBOTTOMNPERCENT (expr, percent, groupLevel)	指定したグループ レベルにおいて、式の値が下位 *n* パーセントに含まれるかどうかが表示されます。	`ISBOTTOMNPERCENT([Sales Total], 5, 3)`
ISNULL(value)	行に値が表示されていない場合は、True が表示されます。行に値が表示されている場合は、False が表示されます。	`ISNULL([DepartmentName])`
ISTOPN(expr, n)	式の値が上位 *n* 個に含まれる場合は True が、含まれない場合は False が表示されます。	`ISTOPN([OrderTotals], 10)`
ISTOPN(expr, n, groupLevel)	指定したグループ レベルにおいて、式の値が上位 *n* 個に含まれる場合は True が、含まれない場合は False が表示されます。	`ISTOPN([OrderTotals], 10, 3)`
ISTOPNPERCENT(expr, percent)	値が上位 *n* パーセントに含まれる場合は True が、含まれない場合は False が表示されます。	`ISTOPNPERCENT([SalesTotals], 5)`
ISTOPNPERCENT(expr, percent, groupLevel)	指定したグループ レベルにおいて、式の値が上位 *n* パーセントに含まれる場合は True が、含まれない場合は False が表示されます。	`ISTOPNPERCENT([SalesTotals], 5, 3)`
LAST(expr)	指定したカラムの最後の値が表示されます。	`LAST([FinishTime])`
LAST(expr, groupLevel)	指定したグループ レベルにおける式の最後の値が表示されます。	`LAST([FinishTime], 3)`
LEFT(str)	指定したストリングの左端の文字が表示されます。	`LEFT([city])`
LEFT(str, n)	カラムのストリングの、左端から数えて指定した文字数分のストリングが表示されます。	`LEFT([city], 3)`
LEN(str)	スペースや句読点を含む、ストリングの長さが表示されます。	`LEN([Description])`
LIKE(str)	値が一致する場合は True が、一致しない場合は False が表示されます。ストリング パターンの指定には、SQL 構文を使用します。 次の規則が適用されます。 • リテラル パターン文字は、正確に一致する必要があります。LIKE では、大文字と小文字が区別されます。 • パーセント文字（%）は、0 文字以上の文字に一致します。 • アンダースコア文字（_）は、任意の 1 文字に一致します。 • リテラルのパーセント文字、アンダースコア文字、またはバックスラッシュ文字（\）は、バックスラッシュ文字でエスケープします。	`LIKE([customerName], "D%")` `LIKE([quantityOrdered], "2_")`

表 13-11　関数の例 （続き）

機能	説明	使用例
LOWER(str)	指定したカラムのストリングが小文字で表示されます。	LOWER([cityName])
MAX(expr)	指定したカラムの最大値が表示されます。	MAX([OrderTotal])
MAX(expr, groupLevel)	指定したグループ レベルにおける式の最大値が表示されます。	MAX([OrderTotal], 2)
MEDIAN(expr)	指定したカラムの中央値が表示されます。	MEDIAN([HomePrices])
MEDIAN(expr, groupLevel)	指定したグループ レベルにおける式の中央値が表示されます。	MEDIAN([HomePrices], 2)
MIN(expr)	指定したカラムの最小値が表示されます。	MIN([OrderTotal])
MIN(expr, groupLevel)	指定したグループ レベルにおける式の最小値が表示されます。	MIN([OrderTotal], 1)
MOD(num, div)	数値を除数で除算した余りが表示されます。結果の符号は、除数と同じ符号となります。	MOD([Salary], 12)
MONTH(date)	指定した日時値の月の名前が表示されます。	MONTH([ForecastShipDate])
MONTH(date, option)	次の 3 つのフォーマットオプションのいずれかを使用して、指定した日時値の月が表示されます。 • 1：月が 1 ～ 12 の数字で表示されます。 • 2：ユーザのロケールでの月の完全な名前が表示されます。 • 3：ユーザのロケールでの月の名前が省略形で表示されます。	MONTH([Semester], 2)
MOVINGAVERAGE (expr, window)	一定の日数における平均価格や平均数量などの、指定した期間における平均値が表示されます。	MOVINGAVERAGE([Price], [Days])
NOTNULL(value)	指定したカラムのデータ値が空ではない場合は、True が表示されます。データ値が空の場合は、False が表示されます。	NOTNULL([DepartmentID])
NOW( )	現在のタイムスタンプが表示されます。	NOW([PastDueDate])
OR	論理 OR 演算子です。	この関数は、式で句を接続する場合に使用し、引数を取りません。
PERCENTILE(expr, pct)	百分位数の値が表示されます。百分位数とは、100 を基準としたスケールを使用して求められる値です。このスケールでは、指定された値以下の分布割合（パーセント）が示されています。 有効な pct 引数の範囲は、0 ～ 1 です。0 は系列の最小値を返します。1 は系列の最大値を返します。	PERCENTILE([Rank], 1)
PERCENTILE(expr, pct, groupLevel)	指定したグループ レベルにおける式の百分位数の値が表示されます。 有効な pct 引数の範囲は、0 ～ 1 です。0 は系列の最小値を返します。1 は系列の最大値を返します。	PERCENTILE([Income], 60, 1)
PERCENTRANK(expr)	値の順位がパーセントで表示されます。	PERCENTRANK([TestScores])
PERCENTRANK(expr, groupLevel)	指定したグループ レベルにおける値の順位がパーセントで表示されます。	PERCENTRANK([TestScores], 2)

表 13-11　関数の例 （続き）

機能	説明	使用例
PERCENTSUM(expr)	合計のパーセントとして値が表示されます。	`PERCENTSUM([OrderTotals])`
PERCENTSUM(expr, groupLevel)	指定したグループ レベルにおける合計のパーセントとして値が表示されます。	`PERCENTSUM([OrderTotals], 3)`
QUARTER(date)	指定した日時値の四半期番号が 1 ～ 4 で表示されます。	`QUARTER([ForecastCloseDate])`
QUARTILE(expr, quart)	四分位数が表示されます。quart 引数は、0 ～ 4 の整数です。	`QUARTILE([OrderTotal], 3)`
QUARTILE(expr, quart, groupLevel)	指定したグループ レベルにおける式の四分位数が表示されます。quart 引数は、0 ～ 4 の整数です。	`QUARTER([OrderTotal], 2, 3)`
RANK(expr)	数値、ストリング、または日時値の、1 から始まる順位が表示されます。重複した値には同じ順位が割り当てられますが、重複が発生してもそのあとの値の順位には影響がありません。	`RANK([AverageStartTime])`
RANK(expr, ascending, groupLevel)	指定したグループ レベルにおける、数値、ストリング、または日時値の昇順または降順の順位が表示されます。 値を昇順で表示するには、2 つめの引数として True を使用します。値を降順で表示するには、2 つめの引数として False を使用します。	`RANK([Score], false, 3)` `RANK([Score], true, 2)`
RIGHT(str)	指定したストリングの右端の文字が表示されます。	`RIGHT([name])`
RIGHT(str, n)	ストリングの、右端から数えて指定した文字数分のストリングが表示されます。	`RIGHT([name], 3)`
ROUND(num)	数値が丸められます。	`ROUND([SalesTarget])`
ROUND(num, dec)	指定した桁数で数値が丸められます。dec のデフォルト値は 0 です。	`ROUND([StockValue], 2)`
ROUNDDOWN(num)	数値が切り捨てられます。	`ROUNDDOWN([StockPrice])`
ROUNDDOWN(num, dec)	1 の位から数えて指定した桁数で数値が切り捨てられます。dec のデフォルト値は 0 です。	`ROUNDDOWN([StockPrice], 2)`
ROUNDUP(num)	数値が切り上げられます。	`ROUNDUP([TotalValue])`
ROUNDUP(num, dec)	1 の位から数えて指定した桁数で数値が切り上げられます。dec のデフォルト値は 0 です。	`ROUNDUP([TotalValue], 2)`
RUNNINGSUM(expr)	連続したデータ行の値を加算した累積合計が表示されます。	`RUNNINGSUM([StockValue])`
SEARCH(pattern, str)	ワイルドカード文字を使用できる検索関数です。大文字と小文字は区別されません。 アスタリスク（*）は、スペースを含む任意のストリングに一致します。 疑問符（?）は、任意の 1 文字に一致します。	次のように検索すると、[City] カラムから New York や New Haven などが検索されます。 `SEARCH([CustomerData:city], "new*")`
SEARCH(pattern, str, startPosition)	ストリング内の指定した位置から開始して、指定したパターンをストリング内で検索します。ワイルドカード文字を使用できる検索関数です。大文字と小文字は区別されません。	`SEARCH([Location], "new", 1)`
SQRT(num)	値の平方根が表示されます。	`SQRT([PrincipalValue])`

表 13-11　関数の例 （続き）

機能	説明	使用例
STDEV(expr)	標準偏差が表示されます。	`STDEV([PurchaseFrequency])`
SUM(expr)	指定した 2 つの値の合計が表示されます。	`SUM([Price]+[Tax])`
TODAY( )	現在の日付の午前 0 時に相当するタイムスタンプ値が表示されます。	`TODAY([DueDate])`
TRIM(str)	先頭および末尾にあるすべてのブランク文字を削除したストリングが表示されます。すべての連続するブランク文字も削除されます。先頭および末尾のブランク文字とは、スペースやタブなどを指します。	`TRIM([customerName])`
TRIMLEFT(str)	先頭にあるすべてのブランク文字を削除したストリングが表示されます。連続するブランク文字は削除されません。	`TRIMLEFT([PortfolioName])`
TRIMRIGHT(str)	末尾にあるすべてのブランク文字を削除したストリングが表示されます。連続するブランク文字は削除されません。	`TRIMRIGHT([Comments])`
True	ブール値の True です。この関数は、引数が true であることを示すために式で使用します。	次の例は、2 つめの引数 ascending（昇順）が true であり、したがって値が昇順で返される必要があることを示しています。 `RANK([Score], true)`
UPPER(str)	指定したカラムのストリングがすべて大文字で表示されます。	`UPPER([cityName])` `UPPER("new haven")`
VAR(expr)	指定した式の分散が表示されます。	`VAR([EstimatedCost])`
WEEK(date)	日時の値において、何週めであるかが 1 ～ 52 の数字で表示されます。	`WEEK([LeadQualifyingDate])`
WEEKDAY(date, option)	次のいずれかのフォーマットオプションを使用して、曜日が表示されます。 • 1 : 1（日曜日）～ 7（土曜日）の曜日番号が返されます。1 がデフォルトのオプションです。 • 2 : 1（月曜日）～ 7（日曜日）の曜日番号が返されます。 • 3 : 0（月曜日）～ 6（日曜日）の曜日番号が返されます。 • 4 : ユーザのロケールに従って、曜日名が返されます。 • 5 : ユーザのロケールに従って、曜日名が省略形で返されます。	`WEEKDAY([DateSold], 4)`
WEIGHTEDAVERAGE (value, weight)	指定した値の加重平均が表示されます。	`WEIGHTEDAVERAGE([Score], weight)`
YEAR(date)	日時の値の年を表す 4 桁の値が表示されます。	`YEAR([ClosingDate])`

サポートされている演算子について

表 13-12 に、計算カラムを作成する式を記述する場合に使用できる算術演算子および論理演算子を示します。

表 13-12　式の記述に使用する、サポートされている演算子

演算子	説明
x + y	数値の加算
x - y	数値の減算
x * y	数値の乗算
x / y	数値の除算
x%	数値のパーセント
x & y	ストリング値の連結
x = y	2 つの値の等価テスト
x > y	x が y よりも大きいかどうかのテスト
x < y	x が y よりも小さいかどうかのテスト
x >= y	x が y 以上であるかどうかのテスト
x <= y	x が y 以下であるかどうかのテスト
x <> y	x と y の非等価テスト
x AND y	値が条件 x および条件 y の両方を満たすかどうかのテスト
x OR y	値が条件 x または条件 y のいずれかを満たすかどうかのテスト
NOT x	値が x ではないことのテスト

式における数値および日付の使用方法

数値を含む式を作成する場合は、アメリカ英語ロケールの表記法に従って数値を入力する必要があります。つまり、小数点としてカンマ（,）ではなくピリオド（.）を使用します。次に例を示します。

```
Correct:        1234.56
Incorrect:      1234,56
```

日付を含む式を作成する場合は、ログイン時に選択したロケールの表記法に従って日付を入力します。たとえば、フランス語（フランス）ロケールでは、2007 年 12 月 3 日を表すのに、12/03/2007 ではなく 03/12/2007 と入力します。日付、または日時を入力できます。日付および時刻は、次のように二重引用符（"）で囲む必要があります。

```
"03/12/2007"
"03/12/2007 11:00 AM"
```

計算カラムにおける値の乗算の使用方法

計算カラムにおける値の乗算を使用するには、次の手順を実行します。

ステップ 1　カラムを選択します。レポートで、選択したカラムの*右側*に新しい計算カラムが表示されます。

ステップ 2　[Add Calculation] を選択します。

[Calculation] ダイアログボックスが表示されます。

ステップ 3　[Column Label] フィールドに、計算カラムのヘッダーを入力します。

ヘッダーはアルファベットで始まる必要があり、アルファベット、数字、アンダースコア、およびスペースだけを使用できます。

ステップ 4　[Enter Expression] フィールドで、左角カッコ（[）を入力します。

レポート内のカラムのリストが表示されます。このリストには、レポートに含まれているすべての計算カラムも含まれています。

ステップ 5　被乗数を含むカラムを選択します。

たとえば、単価と注文数量を乗算する場合は、単価を含むカラムを選択します。

ステップ 6　乗算演算子としてアスタリスク（*）を入力します。カラム名のあとにスペースを挿入する必要はありません。

ステップ 7　左角カッコ（[）をもう一つ入力して、乗数を選択します。

たとえば、被乗数が単価である場合は、注文数量を含むカラムを乗数として選択します。

ステップ 8　式を確認するには、[Validate] をクリックします。

式の構文が正しい場合は、確認メッセージを示すダイアログボックスが表示されます。

式の構文が誤っている場合は、エラー内容説明のメッセージを示すダイアログボックスが表示されます。

ステップ 9　式を確認したあと、[Apply] をクリックします。

入力したカラム ヘッダーを使用して、レポートに計算カラムが表示されます。

既存の日付値への日付の加算

他のカラムの日付値に一定の日数を加算した日付を表示するカラムを作成できます。

ステップ 1　カラムを選択します。

選択したカラムの*右側*に計算カラムが表示されます。

ステップ 2　[Add Calculation] を選択します。

[Calculation] ダイアログボックスが表示されます。

ステップ 3　[Column Label] に、計算カラムの名前を入力します。たとえば、Forecast Shipping Date と入力します。

ステップ 4　[Enter Expression] に、文字 **A** を入力します。

A で始まる関数が表示されたドロップダウン リストが表示されます。

ステップ 5　[ADD_DAY(date, daysToAdd)] を選択します。

ステップ 6　1 つめの引数として、左角カッコ（[）を入力し、ドロップダウン リストから日付カラムを選択します。たとえば、[Order Date] を選択します。

ステップ 7　2 つめの引数として、加算する日数を入力します。ここでは、7 と入力します。

ステップ 8　式を確認し、[Apply] をクリックします。

レポートに、新しい計算カラムが表示されます。[Order Date] カラムのすべての値に対して、このカラムが示す注文日に 7 日を加算した日付が計算カラムに表示されます。

計算カラムにおける日付値の減算

2 つの日付値の差異を表示できます。

ステップ 1　カラムを選択します。

レポートで、選択したカラムの右側に計算カラムが表示されます。

ステップ 2　[Add Calculation] を選択します。

[Calculation] ダイアログボックスが表示されます。

ステップ 3　[Column Label] に、計算カラムの名前を入力します。

たとえば、依頼日から実際の出荷日を減算する場合は、Shipping Delay と入力します。

ステップ 4　[Enter Expression] に、文字 **d** を入力します。

d で始まる関数が表示されたドロップダウン リストが表示されます。

ステップ 5　[DIFF_DAY(date1, date2)] を選択します。

ステップ 6　1 つめの引数として、左角カッコ（[）を入力し、ドロップダウン リストから 1 つめの日付カラムを選択します。

たとえば、[Date Requested] を選択します。

ステップ 7　2 つめの引数として、左角カッコ（[）を入力し、ドロップダウン リストから 2 つめの日付カラムを選択します。

たとえば、[Actual Shipping Date] を選択します。

ステップ 8　式を確認し、[Apply] をクリックします。

2 つの日付の差異を示す新しい計算カラムがレポートに表示されます。

集計データの使用

データの集計においては、データ行のセットに対して計算が実行されます。たとえば、価格 * 数量を計算するカラムがあるレポートにおいては、これらの計算すべての合計を算出して、すべての品目の合計金額を取得できます。計算カラムに対して、最大 3 つの集計を作成できます。

データを集計する場合、集計をテーブル ヘッダーに表示するか、またはテーブル フッターに表示するかを選択します。カラムがデータ グループの詳細カラムである場合は、集計値をグループ ヘッダーまたはグループ フッターに表示できます。図 13-39 に、グループ フッターに表示された集計データを示します。

図 13-39　グループの集計行

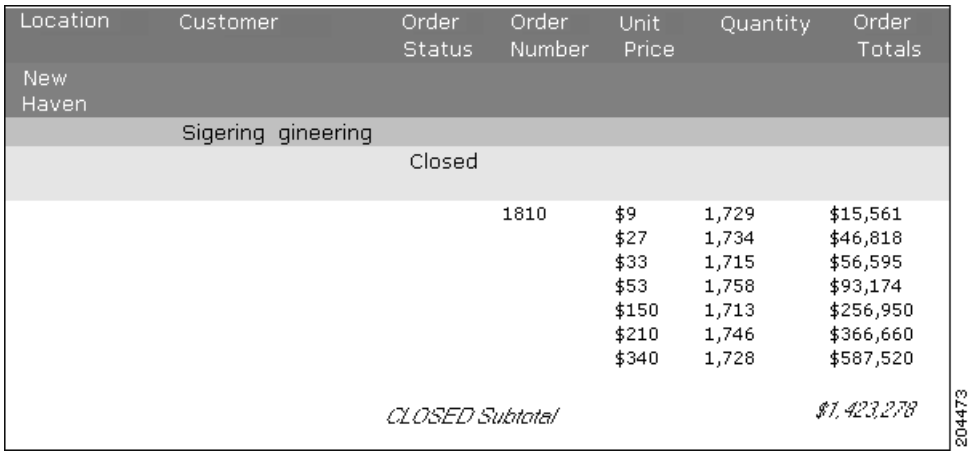


表 13-13 に、使用可能な集計関数を示します。

表 13-13　集計関数

集計関数	説明
Average	データ値のセットの平均値が計算されます。
Count	カラム内のデータ行がカウントされます。
Count Value	カラム内の重複しない値がカウントされます。
First	カラムの最初の値が返されます。
Last	カラムの最後の値が返されます。
Max	カラムの最大値が返されます。
Median	カラムの中央値が返されます。
Min	カラムの最小値が返されます。
Mode	カラム内で最も頻繁に出現する値が返されます。
Quartile	選択した分位点に基づいて、均等なサイズで 4 つに分割されたデータのセットの 1 つが返されます。 たとえば、第 1 四分位数を要求すると、上位 4 分の 1 のデータ セットを取得でき、第 4 四分位数を要求すると、下位 4 分の 1 のデータ セットを取得できます。
Standard Deviation	分散の平方根である標準偏差が返されます。
Sum	カラムの値の合計が返されます。
Variance	平均値または期待値を中心とした分散の度合いを示す値が返されます。
Weighted average	データ行のセットに対する、数値フィールドの加重平均が返されます。加重平均では、一部の数値が他の数値よりも重視されます。つまり、重み付けされます。

集計データ行の作成

集計データ行を作成するには、次の手順を実行します。

ステップ 1　カラムを選択して、[Aggregation] を選択します。

[Aggregation] ダイアログボックスが表示されます。選択したカラムの名前が、[Selected Column] フィールドに表示されます。

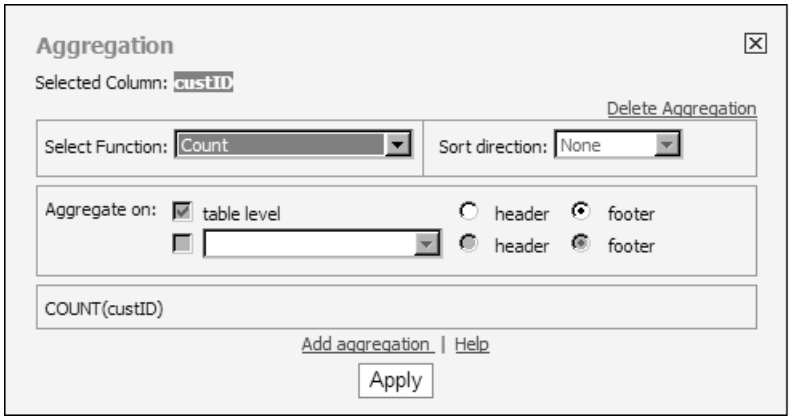
ステップ 2　[Select Function] メニューから、使用する関数を選択します。

使用可能な関数は、カラムに含まれているデータ型に応じて異なります。

- カラムにテキスト データが含まれている場合は、カラム内のすべての値のカウント、カラム内の重複しない値のカウントなどを実行できます。
- カラムに数値データが含まれている場合は、値のカウント、平均値または加重平均の取得、カラムの合計値の取得などを実行できます。

図 13-40 に示すように、[Aggregation] ダイアログボックスの下部に、選択した関数の構文が表示されます。

図 13-40　Interactive Viewer の [Aggregation] ダイアログボックス



ステップ 3　[Aggregate on] フィールドで、次の手順を実行します。

- 集計値をテーブル ヘッダーに表示するか、またはテーブル フッターに表示するかを選択します。デフォルト設定では、集計値はテーブル フッターに表示されます。
- 選択したカラムが *グループ化された*カラムである場合は、集計値をグループ ヘッダーに表示するか、またはグループ フッターに表示するかを選択します。

ステップ 4　[Apply] をクリックします。

レポート デザインで、集計データを配置した場所に集計データが表示されます。

追加の集計行の追加

カラムに対して単一の集計行を作成したあと、同じカラムに対して最大であと 2 つの集計行を追加できます。たとえば、品目の注文合計金額のカラムに対して、すべての値の合計、すべての値のカウント、および注文合計金額の平均を作成できます。

集計行を追加するには、次の手順を実行します。

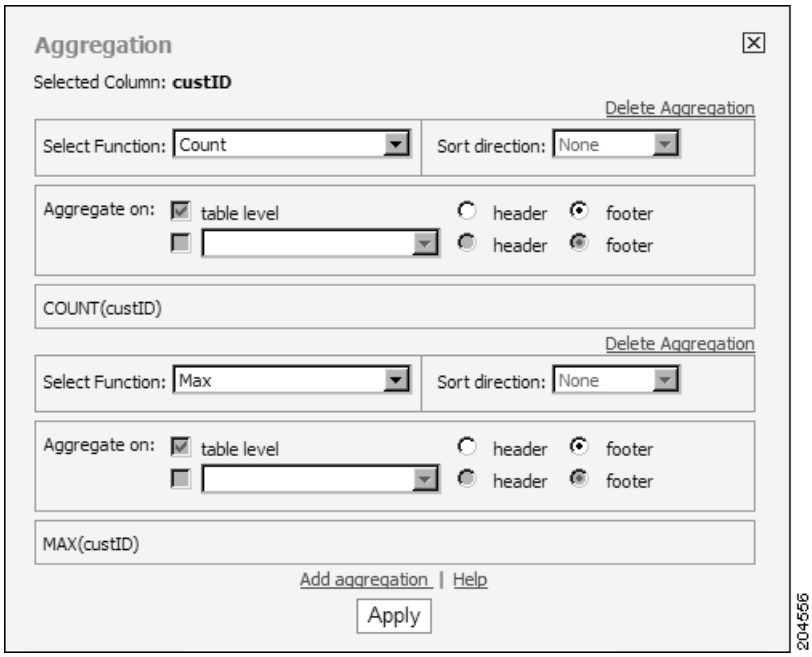
ステップ 1　集計行を含む計算カラムを選択して、[Aggregation] を選択します。

[Aggregation] ウィンドウが表示されます。

ステップ 2　[Add aggregation] をクリックします。

図 13-41 に示すように、[Aggregation] ダイアログボックスに追加のセクションが表示されます。

図 13-41　Interactive Viewer におけるカラムの集計行の追加



ステップ 3　2 つめの集計行を作成して、[Apply] をクリックします。

集計行の削除

集計行を削除するには、次の手順を実行します。

ステップ 1　削除する集計を含む計算カラムを選択して、[Aggregation] を選択します。

[Aggregation] ダイアログボックスが表示され、カラムのすべての集計が表示されます。

ステップ 2　削除する集計で [Delete Aggregation] を選択して、[Apply] をクリックします。

レポート データの非表示およびフィルタリング

レポートのデータの非表示または表示を次の複数の方法で指定できます。

- 詳細行を非表示または表示するように指定できます。
- 重複した行のうち 1 つだけを表示するように指定できます。
- データ セットによってレポートで必要とする以上の情報が提供されている場合は、不要なデータをフィルタリングできます。また、ユーザが実行時パラメータを使用してフィルタ値を指定できるようにすることもできます。

カラム データの非表示または表示

多くの場合、レポートのすべてのデータを表示する必要はありません。たとえば、詳細のカラムには、重複した値が複数のデータ行に連続して表示されることがあります。重複した値を表示する必要がない場合や、重複した値が表示されることによってレポートが読みづらくなる場合には、連続した重複値を非表示にできます。

また、レポートのデザイン時に、グループやセクションを縮小して、カラム ヘッダーや、集計データ行などの概要データだけを表示できます。

重複値の非表示

レポートでデータのフォーマットや調整を開始する前の時点では、データ行はデータ ソースに指定されているとおりにレポートに表示されます。たとえば、図 13-42 に示すレポートでは、都市名が出現するたびにその都市名が [Location] カラムに表示されています。

図 13-42　カラムの重複値

Customer	Location	State	Representative
Tchl Systems Inc.	Boston	MA	1401
D in Systems	Boston	MA	1401
Brittn Design Inc.	Boston	MA	1401
Teleoards Co.	Boston	MA	1401
Desin Engineering Corp.	Boston	MA	1401
Tek ards Corp.	Philadelphia	PA	1216
D in Solutions	Philadelphia	PA	1216
Signl MicroSystems	Philadelphia	PA	1216
Sign ialists Corp.	NYC	NY	1286
Tchl MicroSystems Inc.	NYC	NY	1286
Infohgineering	NYC	NY	1286
Advc Design Inc.	NYC	NY	1286
Tchl Design Inc.	NYC	NY	1286
Desi Sol Corp.	NYC	NY	1286

204497

図 13-43 に示すように、重複した値を 1 回だけ表示すると、レポートが読みやすくなります。

図 13-43　値を非表示にしたレポート

Customer	Location	State	Representative
Tchl Systems Inc.	Boston	MA	1401
D in Systems			
Brittn Design Inc.			
Teleoards Co.			
Desin Engineering Corp.			
Tek ards Corp.	Philadelphia	PA	1216
D in Solutions			
Signl MicroSystems			
Sign ialists Corp.	NYC	NY	1286
Tchl MicroSystems Inc.			
Infohgineering			
Advc Design Inc.			
Tchl Design Inc.			

204549

重複した値を非表示にすると、レポートが読みやすくなります。ただし、連続して出現する重複値だけを非表示にできます。図 13-43 の [Location] カラムでは、Boston という値が 2 行め、3 行め、4 行め、および 5 行めで非表示になっています。NYC のあとに再度 Boston という値が出現した場合、その Boston は表示され、そのあとに連続して続く Boston は非表示になります。完全に同一の重複値だけが非表示になります。

カラムが複数のページにまたがる場合、そのカラムで重複値が非表示になっていても、各ページの最初の行では値が表示されます。

この機能を非表示にするには、次の手順を実行します。

ステップ 1　重複値を含むカラムを選択して、右クリックします。

ステップ 2　コンテキスト メニューから、[Column] > [Do Not Repeat Values] を選択します。

重複値の表示

重複値を表示するには、次の手順を実行します。

ステップ 1　重複値が繰り返し表示されないカラムを選択して、右クリックします。

ステップ 2　コンテキスト メニューから、[Column] > [Repeat Values] を選択します。

グループまたはセクションの詳細行の非表示または表示

レポートにグループが含まれている場合は、コンテキスト メニューを使用して、グループを縮小および展開できます。

たとえば、図 13-44 は、*creditrank* によってデータがグループ化され、各 creditrank 値の詳細行が表示されているレポートを示しています。

図 13-44　グループの詳細行が表示されたレポート

creditrank	custID	contact_last	contact_first
⊟ A			
	102	Murphy	Leslie
	106	Young	Jeff
	109	Frick	Michael
	111	Hernandez	Maria
	113	Yu	Kwai
	115	Thompson	Bill
	116	Brown	William
	117	Lewis	Bill
	120	Thompson	Steve
	122	Firrelli	Dan

204493

図 13-45 は、creditrank によるグループ化の詳細行を非表示にした結果を示しています。

図 13-45　グループの詳細行が非表示にされたレポート

creditrank	custID	contact_last	contact_first
A			
B			
C			

204492

- グループまたはセクションを縮小するには、縮小するグループまたはセクションのメンバーを選択して、右クリックします。

  コンテキスト メニューが表示されます。
- グループ メンバーを詳細行なしで表示するには、[Group] > [Hide Detail] を選択します。
- グループ メンバーを詳細行とともに表示するには、[Group] > [Show Detail] を選択します。

フィルタの使用

フィルタを使用すると、レポートに表示されるデータを制限できます。たとえば、顧客データのデータベースを利用することによって、フィルタを使用して、特定の都道府県在住の顧客だけをリストしたり、合計購入額が 150 万ドルを超える顧客だけをリストしたりするレポートを実行できます。

さらにデータを制限して、たとえば特定の都道府県に在住しており、与信限度額が $50,000 未満で、かつ過去 90 日間に商品を購入していない顧客をリストすることもできます。

フィルタは、レポート内の 1 つ以上のフィールドに基づいて実行されます。

1 つのフィールドに基づくフィルタを作成するには、条件と値を 1 つずつ選択します。たとえば、特定の値と一致する値を返すフィルタ、特定の値よりも小さい値を返すフィルタ、2 つの値の間にある値を返すフィルタなどを作成できます。表 13-14 に、選択できる条件を示します。

表 13-14　フィルタで使用する条件

条件	説明
Any Of	指定した値のいずれかに一致する値が返されます。
Between	指定した 2 つの値の間にある値が返されます。[Between] を選択した場合、2 番めのデフォルト値用として 2 つめの [Value] フィールドが表示されます。
Bottom N	カラムの下位 *n* 個の値が返されます。
Bottom Percent	カラムの下位 *n* パーセントの値が返されます。
Equal to	指定した値と等しい値が返されます。
Greater Than	指定した値よりも大きい値が返されます。
Greater Than or Equal to	指定した値以上の値が返されます。
Is False	True または False と評価されるカラムにおいて、false 値を含むデータ行が返されます。
Is Not Null	値を含むデータ行が返されます。
Is Null	値を含まないデータ行が返されます。
Is True	True または False と評価されるカラムにおいて、true 値を含むデータ行が返されます。
Less Than	指定した値未満の値が返されます。
Less Than or Equal to	指定した値以下の値が返されます。
Like	指定したストリングに全部または一部が一致するストリングが返されます。% は、0 個以上の文字と一致します。_ は、1 文字と一致します。
Not Between	指定した 2 つの値の間にない値が返されます。[Not Between] を選択した場合、2 つめのデフォルト値用の 2 つめの [Value] フィールドが表示されます。
Not Equal to	指定した値と等しくない値が返されます。
Not Like	指定したストリングに全部または一部が一致しないストリングが返されます。% は、0 個以上の文字と一致します。_ は、1 文字と一致します。
Top N	カラムの上位 *n* 個の値が返されます。
Top Percent	カラムの上位 *n* パーセントの値が返されます。

フィルタ条件のタイプ

表 13-15 では、フィルタ条件のタイプを示し、フィルタ条件がどのようにデータ ソースに対する命令に変換されるかを示す例について説明します。

表 13-15　フィルタ条件の例

フィルタ条件のタイプ	説明	データ ソースに対する命令の例

比較	次の条件を使用して、ある式の値と他の式の値を比較します。
	• Equal to
	• Not Equal to
	• Less Than
	• Less Than or Equal to
	• Greater Than
	• Greater Than or Equal to
		`quantity = 10`
		`custName = 'Acme Inc.'`
		`custName > 'P'`
		`custState <> 'CA'`
		`orderDate > {d '2005-06-30'}`

範囲	Between または Not Between を使用して、式の値が一定の値の範囲内にあるか、または範囲外にあるかをテストします。このテストでは、範囲の両端の値が含まれます。	`price BETWEEN 1000 AND 2000`
		`custName BETWEEN 'E' AND 'K'`
		`orderDate BETWEEN`
		`{d '2005-01-01'} AND {d '2005-06-30'}`

メンバーシップ	Any Of を使用して、式の値が値のセットのうちの 1 つに一致するかどうかをテストします。	`officeCode IN (101,103,104)`
		`itemType IN ('sofa', 'loveseat', 'endtable', 'clubchair')`
		`orderDate IN`
		`({d '2005-10-10'}, {d '2005-10-17'})`

パターン マッチング	Like または Not Like を使用して、ストリング フィールドの値が指定したパターンに一致するか、または一致しないかをテストします。% は、0 個以上の文字と一致します。
	_ は、1 文字と一致します。
		`custName LIKE 'Smith%'`
		`custName LIKE 'Smiths_n'`
		`custState NOT LIKE 'CA%'`

ヌル値	Null または Is Not Null を使用して、フィールドがヌル値であるか、またはヌル値でないかをテストします。ヌル値であるとは、値が存在しないことを示します。	`manager IS NULL`
		`shipDate IS NULL`
		`shipDate IS NOT NULL`

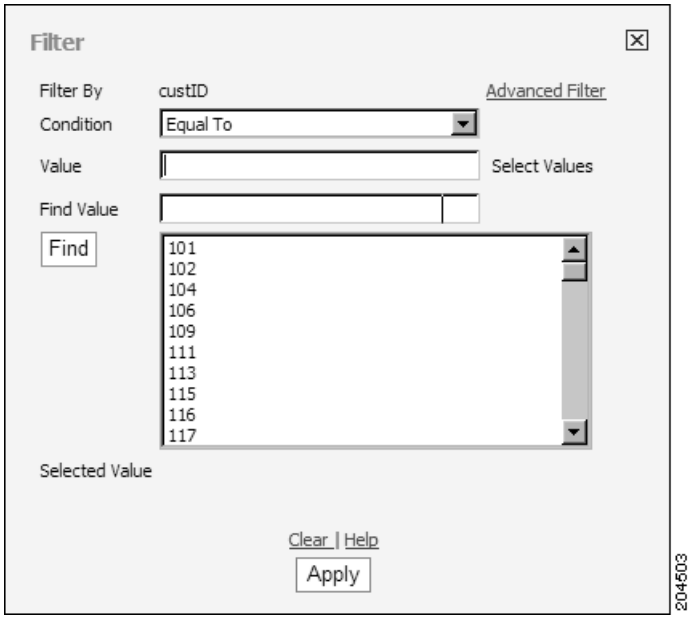
フィルタ値の設定

条件を選択したあと、フィルタ値を設定します。

ステップ 1　選択したカラムのすべての値を表示するには、[Select Values] を選択します。

図 13-46 に示すように、[Filter] ダイアログボックスに追加のフィールドが表示されます。これらのフィールドを使用して、フィルタ値を検索および選択できます。

図 13-46　Interactive Viewer におけるフィルタ値の選択



ステップ 2　値を検索するには、[Find Value] フィールドに値を入力して、[Find] をクリックします。

フィルタ テキストに一致するすべての値が返されます。たとえば、次のように入力したとします。

```
40
```

この場合、カラム内の 40 で始まるすべての値がテキスト ボックスに表示されます。次に例を示します。

```
40
400
4014
40021
```

大きなテキスト ボックスに目的の値を見つけたら、その値をダブルクリックします。値が [Value] フィールドに表示されます。

フィルタの作成

フィルタを作成するには、次の手順を実行します。

ステップ 1　Interactive Viewer で、詳細カラムを選択して、[Filter] を選択します。

選択した詳細カラムがマージされたカラムである場合は、[Select data item] ダイアログボックスが表示されます。

ステップ 2　[Select data] ドロップダウン リストから、フィルタを適用するカラム名を選択して、[Apply] をクリックします。

[Filter] ダイアログボックスが表示されます。選択したカラムの名前が、[Filter By] フィールドに表示されます。この名前は変更できません。

ステップ 3　[Condition] プルダウン メニューから、条件を選択します。表 13-14 に、選択できる条件を示します。

- [Between] または [Not Between] を選択した場合は、値の範囲を表示する追加のフィールド [Value From] および [Value To] が表示されます。
- [Is False]、[Is True]、[Is Null]、または [Is Not Null] を選択した場合、値フィールドは表示されません。その他の条件を選択した場合は、値フィールドが 1 つ表示されます。

ステップ 4　使用可能な各フィールドに、値を入力します。

カラムのすべての値の中から選択するには、[Select Values] をクリックして、ドロップダウン リストから選択します。

ステップ 5　[Apply] をクリックします。

フィルタを適用した結果が表示されます。

フィルタの変更またはクリア

フィルタを変更またはクリアするには、次の手順を実行します。

ステップ 1　フィルタを使用するカラムを選択します。

ステップ 2　[Filter] を選択します。

[Filter] ダイアログボックスが開き、既存のフィルタ条件が表示されます。

- フィルタを変更するには、[Condition] フィールドの設定を変更するか、または値を変更します。
- フィルタを削除するには、[Clear] をクリックします。

ステップ 3　[Apply] をクリックします。

複数の条件を持つフィルタの作成

複数の条件を持つフィルタを作成できます。たとえば、信用格付けが A または B であり、かつ未出荷の注文合計金額が $250,000 ～ $500,000 である顧客の名前を取得するフィルタを作成できます。

複数の条件を持つフィルタを作成するには、[Filter] ダイアログボックスで [Advanced Filter] を選択して、[Advanced Filter] ダイアログボックスを使用します。図 13-47 に、Interactive Viewer の [Advanced Filter] ダイアログボックスを示します。

図 13-47　Interactive Viewer の [Advanced Filter] ダイアログボックス

[Advanced Filter] では、非常に柔軟にフィルタ値を設定できます。等価性をテストする条件および Between 条件では、リテラル値を設定することも、他のデータ カラムの値に基づいて値を設定することもできます。

たとえば、実際の出荷日が出荷予定日を過ぎているデータや、実際の売上が売上目標に達していないデータを要求できます。次の手順を実行します。

ステップ 1　カラムを選択して、[Filter] を選択します。

[Filter] ダイアログボックスが表示されます。

ステップ 2　[Advanced Filter] をクリックします。

[Advanced Filter] ダイアログボックスが表示されます。[Filter By] フィールドに、レポート内の最初のカラムの名前が表示されます。

ステップ 3　[Filter By] メニューから、フィルタリングするデータを含むカラムを選択します。

ステップ 4　[Condition] フィールドで、[Equal To]、[Between]、[Less Than] などの条件を選択します。

ステップ 5　[Value] で、次のいずれかのオプションを選択します。

- [Specify literal value] : これはデフォルトの選択です。リテラル値を指定するには、表示されているフィールドに値を入力します。[Select Values] をクリックすると、指定したカラムのすべてのデータ値が表示されたフィールドが表示されます。このリストが長い場合は、[Filter Text] フィールドに値を入力し、[Find] をクリックすることによって、値を検索できます。
- [Use value from data] : [Use value from data] フィールドを選択すると、カラムのドロップダウン リストが表示されます。このリスト内のカラムのデータ型は、[Filter By] フィールドで選択したカラムのデータ型と同じです。

ステップ 6　[Add Condition] をクリックします。

[Filters] に、フィルタ条件が表示されます。

ステップ 7　[Validate] をクリックして、フィルタ構文を確認します。

これで、1 つの条件を持つフィルタが作成されました。次のステップは、条件の追加です。

ステップ 8　ステップ 3 ～ステップ 7 の手順を繰り返して、必要な追加のフィルタ条件を作成します。

ステップ 9　[Filters] で、フィルタ条件を調整して、目的のフィルタリングを完成させます。条件は、次のように組み合わせることができます。

- AND、OR、および NOT を使用します。

  デフォルトで、2 つめのフィルタ条件は AND で連結されます。AND は、両方の条件が満たされたデータ行だけがレポートに表示されることを意味します。[OR] を選択すると、AND を OR に変更できます。OR は、いずれか一方の条件が満たされたデータ行がレポートに表示されることを意味します。

  [NOT] を選択すると、AND や OR のあとに NOT が表示されます。NOT は、条件が満たされないデータ行がレポートに表示されることを意味します。

- 複数の条件を追加した場合、カッコのボタンを使用して、条件をグループ化できます。

  複数のフィルタ条件をカッコで囲むと、カッコの中の条件が最初に評価されます。その後、フィルタ式全体が評価されます。

  たとえば、A AND B OR C という式は左から右へと評価されます。そのため、A および B が満たされるか、または C が満たされるデータ行がレポートに表示されます。A AND (B OR C) という式では、B OR C の部分が最初に評価されます。そのため、A が満たされ、かつ B または C が満たされるデータ行がレポートに表示されます。

複数の条件を含むフィルタからの 1 つのフィルタ条件の削除

フィルタ条件を削除するには、次の手順を実行します。

ステップ 1　詳細カラムを選択して、[Filter] を選択します。

[Filter] ダイアログボックスが表示されます。

ステップ 2　[Advanced Filter] をクリックします。

[Advanced Filter] ダイアログボックスが表示されます。[Advanced Filter] の下部に、レポートのすべてのフィルタ条件が表示されます。

ステップ 3　削除するフィルタ条件を選択して、[Delete] をクリックします。

ステップ 4　[Apply] をクリックします。

カラムの上位または下位の値のフィルタリング

テーブルに数百もの行が含まれている場合、カラムの上位または下位の値を表示すると役立つことがあります。たとえば、最も多くの売上を記録した営業担当者上位 10 名や、エネルギー消費の上位 25% を表示できます。

このようなタイプのフィルタを実行するには、次の手順を実行します。

ステップ 1　選択したカラムを右クリックして、[Filter] > [Top or Bottom N] を選択します。

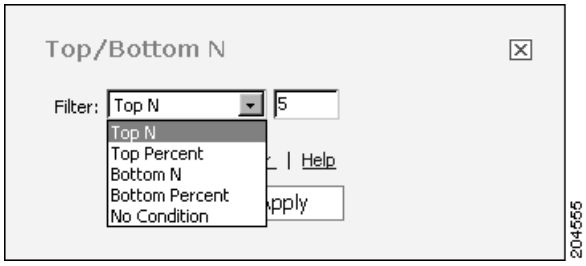
[Top/Bottom N] ダイアログボックスが表示されます。

ステップ 2　図 13-48 に示すように、[Filter] プルダウン メニューから、行を表示する基準となる特定の種類の数または割合を選択します。

ステップ 3　[Filter] プルダウン メニューの隣にあるフィールドに値を入力して、表示する行の数または割合を指定します。

たとえば、売上高上位 10 名の営業担当者を選択するには、売上高のデータを含むカラムを選択して、[Filter] > [Top or Bottom N] を選択します。その後、[Top/Bottom N] ダイアログボックスで [Top N] を選択して、***10*** を入力します。

図 13-48　　カラムの上位または下位の値のソート



ステップ 4　[Apply] をクリックします。

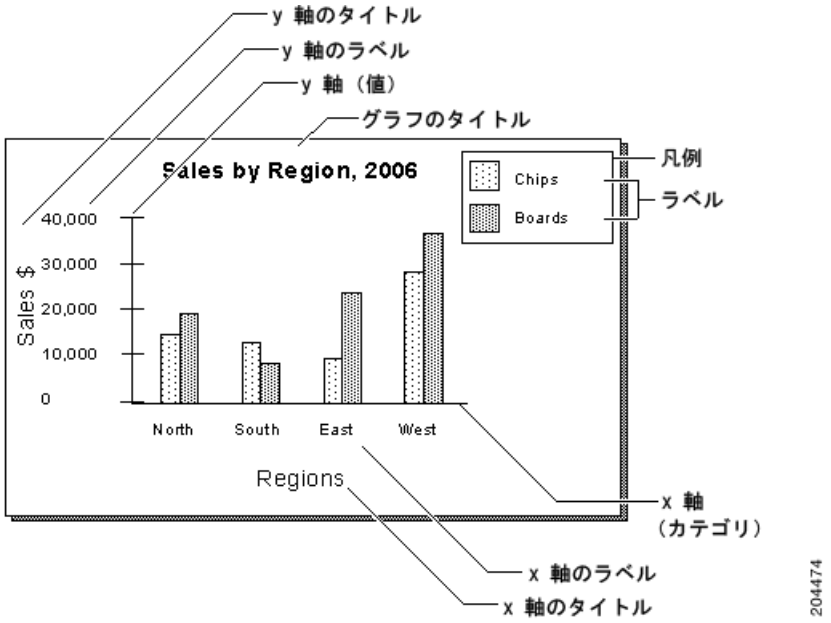
グラフについて

グラフは、データ、またはデータ セット間の関係をグラフィカルに表現したものです。グラフには、複雑なデータがわかりやすい形式で表示されます。図 13-49 に、基本的な棒グラフの構成要素を示します。グラフには、ポイントのセットを 1 つ以上組み合わせてデータが表示されます。グラフでは、データ ポイントが、系列と呼ばれる値のセットに編成されます。系列には、次の 2 つのタイプがあります。

- カテゴリ系列：カテゴリ系列では、通常、x 軸にどのようなテキスト、数値、または日付を表示するかが決定されます。
- 値系列：値系列では、通常、y 軸におけるテキスト、数値、または日付が決定されます。

図 13-49 では、カテゴリ系列には地域のセットが、値系列には売上金額値のセットが含まれています。

図 13-49　基本的な棒グラフの構成要素



さまざまなタイプのグラフがあります。データのタイプによって、それぞれ表示に最適な特定のタイプのグラフが存在します。グラフそのものをレポートとして使用できます。また、レポートを表形式のデータ レポート スタイルとともに使用することもできます。

グラフの変更

グラフの基本的な特性は、レポート デザイン エディタで決定されます。グラフ タイプやデータ ソースなどはレポート デザインの一部であり、ビューアでは変更できません。グラフについて、次の内容を変更できます。

Interactive Viewer には、次の機能が用意されています。

- グラフに表示されたデータのフィルタリング
- グラフ サブタイプの変更
- グラフ フォーマットの変更

Interactive Viewer でグラフを右クリックして、コンテキスト メニューからこれらのオプションを選択します。

グラフ データのフィルタリング

グラフに表示されているデータは、データ カラムをフィルタリングするのとほぼ同じ方法でフィルタリングできます。グラフでは、x 軸または y 軸をフィルタリングできます。次の手順を実行します。

ステップ 1　グラフを右クリックして、コンテキスト メニューを表示します。

ステップ 2　[Filter] を選択します。

[Chart Filter] ダイアログボックスが表示されます。

グラフ サブタイプの変更

グラフにはサブタイプがあり、必要に応じて変更できます。

- 棒グラフ：集合棒グラフ、積み上げ棒グラフ、100% 積み上げ棒グラフ
- 折れ線グラフ：重ね折れ線グラフ、積み上げ折れ線グラフ、100% 積み上げ折れ線グラフ
- 面グラフ：重ね面グラフ、積み上げ面グラフ、100% 積み上げ面グラフ
- メーター グラフ：標準メーター グラフ、重ねメーター グラフ
- 株価グラフ：ろうそく足グラフ、棒形グラフ

多くのグラフ タイプでは、グラフの形状がグラフの背景に対して平面的に表示される 2 次元のサブタイプが提供されています。一部のグラフでは、深さを表現することもできます。深さが表現されたグラフは、3 次元に見えます。次の手順を実行します。

ステップ 1　サブタイプを変更するグラフを右クリックします。

ステップ 2　[Chart Subtype] を選択します。

[Chart Subtype] ダイアログボックスが表示されます。

ステップ 3　目的のグラフ サブタイプを選択します。

グラフ フォーマットの変更

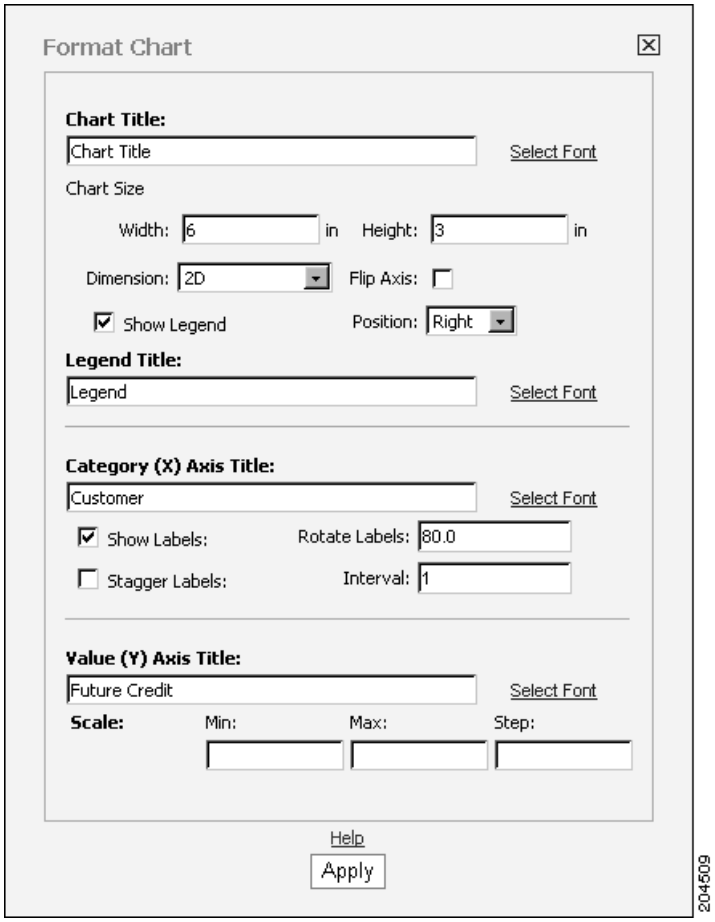
棒グラフの棒の色やグラフの背景色などの一部のグラフ フォーマットは、レポート テンプレートまたはテーマから取得されます。

レポートを表示する場合、グラフ タイトルや軸ラベルのフォントとフォント サイズ、グラフの高さと幅などの、グラフ フォーマットのその他の項目を変更できます。軸ラベルの非表示、ラベル配置時の軸に対する相対的な角度の指定、凡例の非表示、グラフに対する凡例の相対的表示位置の指定などを行うことができます。

グラフの外観のその他の項目は、グラフを右クリックして、[Format] を選択することによって変更できます。表示されるダイアログボックスで、必要なフォーマット プロパティを選択します。

グラフの外観のその他の項目を変更するには、図 13-50 に示す [Format Chart] を使用します。

図 13-50　グラフ フォーマット オプション



このページを使用して、次のことを行います。

- デフォルトのグラフ タイトルの編集およびフォーマット。
- カテゴリ軸、つまり x 軸のデフォルト タイトルの編集およびフォーマット。
- x 軸のラベルの設定の変更。次の作業を実行できます。
  - x 軸のラベルを表示するかどうかの指定。
  - x 軸のラベルを回転させるかどうかの指定、および回転角度の設定。
  - x 軸のラベルを一定間隔で表示するかどうかの指定。たとえば、3 か月ごと、10 日ごと、2 年ごとにデータ ポイントを表示できます。
  - 一定間隔で表示する x 軸ラベルの間隔の設定。
- グラフで y 軸が使用される場合には、y 軸のデフォルト タイトルの編集およびフォーマット。
- グラフの高さおよび幅の設定。
- 次元の設定。2 次元、および 2 次元に深さを加えたもののいずれかを選択できます。
- グラフの x 軸と y 軸を反転するかどうかの指定。
- 凡例を表示するかどうかの指定。表示する場合には、グラフの上、下、左、右のいずれに配置するかの指定。

CHAPTER 14

Monitoring and Report Viewer を使用した ACS のトラブルシューティング

この章では、Monitoring and Report Viewer が提供する Cisco Secure Access Control System 用の診断ツールおよびトラブルシューティング ツールについて説明します。

この章の内容は、次のとおりです。

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テストの実行」（P.14-3）
- 「診断情報用の ACS サポート バンドルのダウンロード」（P.14-4）
- 「Expert Troubleshooter の使用」（P.14-6）

利用可能な診断ツールおよびトラブルシューティング ツール

Monitoring and Report Viewer には、次のツールが用意されています。

- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

接続テスト

認証に問題がある場合は、接続テストを実行して、接続に関する問題をチェックできます。接続先のネットワーク デバイスのホスト名または IP アドレスを入力して、Web インターフェイスから **ping**、**traceroute**、および **nslookup** コマンドを実行できます。

Monitoring and Report Viewer に、これらのコマンドの出力が表示されます。接続テストの実行方法の詳細な手順については、「接続テストの実行」（P.14-3）を参照してください。

ACS サポート バンドル

ACS サポート バンドルを使用して、TAC が ACS の問題をトラブルシューティングするための診断情報を準備できます。

通常、サポート バンドルには、ACS データベース、ログ ファイル、コア ファイル、および Monitoring and Report Viewer のサポート ファイルが含まれています。ACS ノードごとに、サポート バンドルから特定のファイルを除外できます。サポート バンドルは、ローカル コンピュータにダウンロードできます。ブラウザに、（設定に応じて）ダウンロードの進行状況が表示され、適切な場所にサポート バンドルを保存するように要求するプロンプトが表示されます。

- ACS サーバがプライマリ インスタンスである場合、サポート バンドルには、ACS 設定のエクスポートが含まれています。
- ACS サーバがセカンダリ インスタンスである場合、ACS データベースは含まれていません。
- ACS サーバがログ コレクタである場合、サポートバンドルには、監視およびレポートの設定のエクスポート、および収集された AAA の監査ログと診断ログが含まれています。
- ACS サーバがログ コレクタでない場合、サポート バンドルには、監視およびレポートの設定は含まれていません。ACS サポート バンドルのダウンロード方法の詳細な手順については、「診断情報用の ACS サポート バンドルのダウンロード」（P.14-4）を参照してください。

Expert Troubleshooter

Expert Troubleshooter は、展開されている ACS の問題の診断およびトラブルシューティングに役立つ、Web ベースの使いやすいトラブルシューティング ユーティリティです。このユーティリティを使用すると、問題を診断する時間を短縮でき、問題の解決方法の詳細な手順が提供されます。

Expert Troubleshooter を使用して、成功した認証および失敗した認証を診断およびトラブルシューティングできます。たとえば、ユーザがネットワークへのアクセス権を取得できない場合、Expert Troubleshooter を使用して、問題の原因を診断できます。

Expert Troubleshooter では、ACS Web インターフェイスから任意のネットワーク デバイス上で **show** コマンドを実行できます。**show** コマンドの出力は、コンソールへの出力とまったく同じ形式で返されます。

Expert Troubleshooter を使用して、任意のネットワーク デバイスの設定を評価し、問題を引き起こすような矛盾が存在しないかどうかを確認できます。ACS 5.4 は、IPv4 と IPv6 を介したネットワーク デバイスとの通信の評価をサポートします。

さらに、Expert Troubleshooter には Security Group Access デバイス関連の問題をトラブルシューティングするための 4 つの診断ツールが用意されています。

Expert Troubleshooter によって、問題の原因が特定され、問題を解決するために実行可能な一連のアクションが示されます。Expert Troubleshooter に用意されているさまざまなツールの詳細については、「Expert Troubleshooter の使用」（P.14-6）を参照してください。

表 14-1 に、ACS 5.4 に用意されている診断ツールを示します。

表 14-1　Expert Troubleshooter：診断ツール

診断ツール	説明
RADIUS Authentication Troubleshooting	RADIUS 認証をトラブルシューティングします。詳細については、「RADIUS 認証のトラブルシューティング」（P.14-6）を参照してください。
Execute Network Device Command	ネットワーク デバイス上で任意の **show** コマンドを実行します。詳細については、「ネットワーク デバイス上での show コマンドの実行」（P.14-10）を参照してください。
Evaluate Configuration Validator	ネットワーク デバイスの設定を評価します。詳細については、「ネットワーク デバイスの設定の評価」（P.14-10）を参照してください。

表 14-1　Expert Troubleshooter：診断ツール （続き）

診断ツール	説明
TrustSec ツール	
Egress (SGACL) Policy	ネットワーク デバイスと ACS との間で出力ポリシー（SGACL）を比較します。詳細については、「ネットワーク デバイスと ACS との間での SGACL ポリシーの比較」（P.14-12）を参照してください。
SXP-IP Mappings	デバイスとピアとの間で SXP マッピングを比較します。詳細については、「デバイスとそのピアとの間での SXP-IP マッピングの比較」（P.14-12）を参照してください。
IP User SGT	デバイスの IP-SGT を、ACS 認証で割り当てられたユーザ IP-SGT レコードと比較します。詳細については、「デバイスの IP-SGT ペアと ACS によって割り当てられた SGT レコードとの比較」（P.14-14）を参照してください。
Device SGT	デバイスの SGT を、ACS によって割り当てられた SGT と比較します。詳細については、「デバイス SGT と ACS によって割り当てられたデバイス SGT との比較」（P.14-15）を参照してください。

接続テストの実行

ネットワーク デバイスのホスト名または IP アドレスを使用して、デバイスへの接続をテストできます。たとえば、接続テストを実行することによって、ID ストアへの接続を確認できます。ACS 5.4 では、リモート マシンの接続もテストできます。

ACS と、デバイスのホスト名または IP アドレスとの間の接続をテストするには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Connectivity Tests] を選択します。

[Connectivity Tests] ページが表示されます。

ステップ 2　適切な IP アドレスの種類を選択するために [IPv4] または [IPv6] オプション ボタンをクリックします。

ステップ 3　表 14-2 の説明に従って、[Connectivity Tests] ページのフィールドを変更します。

表 14-2　Connectivity Tests

オプション	説明
Hostname or IP Address	テストする接続のホスト名または IP アドレスを入力します。入力したホスト名または IP アドレスをクリアするには、[Clear] をクリックします。
ping	送受信されたパケット、パケット損失（存在する場合）、およびテストが完了するまでの時間を示す **ping** コマンドの出力を確認する場合にクリックします。
traceroute	ACS とテスト対象のホスト名または IP アドレスとの間の中間 IP アドレス（ホップ）、および各ホップ完了までの時間を示す **traceroute** コマンドの出力を確認する場合にクリックします。
nslookup	テスト対象のホスト名または IP アドレスをドメイン ネーム サーバに問い合わせた結果としてのサーバ名および IP アドレスを示す **nslookup** コマンドの出力を確認する場合にクリックします。

ステップ 4　実行するテストに応じて、[ping]、[traceroute]、または [nslookup] をクリックします。

[ping]、[traceroute]、または [nslookup] コマンドの出力が表示されます。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

診断情報用の ACS サポート バンドルのダウンロード

ACS サポート バンドルを作成およびダウンロードするには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [ACS Support Bundle] を選択します。

[ACS Support Bundle] ページが表示され、表 14-3 で説明されているフィールドが表示されます。

表 14-3　[ACS Support Bundle] ページ

オプション	説明
Server	ACS ノード インスタンスの名前。ACS ノード インスタンスの ACS サポート バンドルを作成およびダウンロードするための [Download Parameters for the Server] ページを表示する場合にクリックします。
IP Address	*表示のみ*。関連する ACS ノードの IP アドレスを示します。
Node Designation	*表示のみ*。関連する ACS ノードのプライマリ インスタンスまたはセカンダリ インスタンスを示します。

ステップ 2　サーバを選択して、[Get Support Bundle] をクリックします。

[Download Parameters for the Server] ページが表示されます。関連する ACS ノード インスタンスの ACS サポート バンドルを作成およびダウンロードできます。

（注）　ACS 5.4 では、IPv6 URL で指定された宛先にサポート バンドルをダウンロードすることができます。

ステップ 3　ACS サポートの .tar.gz ファイルに組み込むダウンロード オプションを選択します。

ファイルのサイズが非常に大きい場合には、サポート バンドルのダウンロードに時間がかかる場合があります。ダウンロード時間を短縮するためには、サポート バンドルにコア ファイルおよび Monitoring & Report Viewer のサポート ファイルを含めないでください。

次のオプションがあります。

- [Encrypt Support Bundle]：サポート バンドルを暗号化するには、このチェックボックスをオンにします。[Passphrase] に復号化用のパスワードを指定し、[Confirm Passphrase] でそのパスワードを確認します。
- [Include full configuration database]：サポート バンドルにデータベース全体を組み込む場合にこのチェックボックスをオンにします。このオプションがオフの場合、サポート バンドルには、データベースのサブセットだけが組み込まれます。ログに機密情報を含めるかどうかを指定するには、[Include sensitive information] または [Exclude sensitive information] をクリックします。

機密情報には、暗号化されたパスワードや、ACS 設定データなどがあります。

- [Include debug logs]：デバッグ ログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Recent] をクリックして、組み込むデバッグ ログの範囲を [file(s)] フィールドに 1 ～ 999 の値で入力します。
- [Include local logs]：ローカル ログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Recent] をクリックして、組み込むローカル ログの範囲を [file(s)] フィールドに 1 ～ 999 の値で入力します。
- [Include core files]：コア ファイルを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Include files from the last] をクリックして、[day(s)] フィールドに 1 ～ 365 の値を入力します。
- [Include monitoring and reporting logs]：監視ログおよびレポート ログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Include files from the last] をクリックして、[day(s)] フィールドに 1 ～ 365 の値を入力します。

  次のどの監視ログおよびレポート ログを組み込むかを指定します。
  - AAA Audit
  - AAA Diagnostics
  - System Diagnostics
  - AAA Accounting
  - Administrative and Operational Audit
- [Include system logs]：システム ログを組み込む場合にこのチェックボックスをオンにします。その後、[All] をクリックするか、または [Recent] をクリックして、[file(s)] フィールドに 1 ～ 999 の値を入力します。

必要に応じて、[Description] フィールドに説明を入力できます。

ステップ 4　次のいずれかをクリックします。

- 指定したオプションを使用してサポート バンドルをダウンロードするには、[Download] をクリックします。サポート バンドルが作成およびダウンロードされます。
- 行った変更をクリアして、デフォルト設定に戻すには、[Restore Defaults] をクリックします。

（注）　ACS は、デフォルトで関連する ACS ノード インスタンスのサポート バンドルを作成またはダウンロードする際にコア ファイルを選択しません。サポート バンドルにコア ファイルを含める場合は、[Include core files] チェックボックスをオンにできます。ACS でサポート バンドルを暗号化するには [Encrypt Support Bundle] チェックボックスをオンにできます。コア ファイルが暗号化され、サポート バンドルに含まれるようになります。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

Expert Troubleshooter の使用

次の項では、Expert Troubleshooter 診断ツールの使用方法について説明します。

- 「RADIUS 認証のトラブルシューティング」（P.14-6）
- 「ネットワーク デバイス上での show コマンドの実行」（P.14-10）
- 「ネットワーク デバイスの設定の評価」（P.14-10）
- 「ネットワーク デバイスと ACS との間での SGACL ポリシーの比較」（P.14-12）
- 「デバイスとそのピアとの間での SXP-IP マッピングの比較」（P.14-12）
- 「デバイスの IP-SGT ペアと ACS によって割り当てられた SGT レコードとの比較」（P.14-14）
- 「デバイス SGT と ACS によって割り当てられたデバイス SGT との比較」（P.14-15）

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

RADIUS 認証のトラブルシューティング

RADIUS Authentication Troubleshooting 診断ツールを使用すると、RADIUS 認証に関する問題をトラブルシューティングできます。これを行うには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

[Expert Troubleshooter] ページが表示されます。

ステップ 2　トラブルシューティング ツールのリストから、[RADIUS Authentication Troubleshooting] を選択します。

[RADIUS Authentication Troubleshooter] ページが表示されます。

ステップ 3　表 14-4 に示すようにフィールドを変更して、トラブルシューティング対象の RADIUS 認証をフィルタリングします。

表 14-4　[RADIUS Authentication Troubleshooter] ページ

オプション	説明
トラブルシューティング対象の RADIUS 認証の検索および選択	
Username	認証をトラブルシューティングするユーザのユーザ名を入力するか、または [Select] をクリックしてリストからユーザ名を選択します。ユーザ名をクリアするには、[Clear] をクリックします。
MAC Address	トラブルシューティングするデバイスの MAC アドレスを入力するか、または [Select] をクリックしてリストから MAC アドレスを選択します。MAC アドレスをクリアするには、[Clear] をクリックします。
Audit Session ID	トラブルシューティングする監査セッション ID を入力します。監査セッション ID をクリアするには、[Clear] をクリックします。

表 14-4　[RADIUS Authentication Troubleshooter] ページ （続き）

オプション	説明
NAS IP	NAS IP アドレスを入力するか、または [Select] をクリックしてリストから NAS IP アドレスを選択します。NAS IP アドレスをクリアするには、[Clear] をクリックします。
NAS Port	NAS ポート番号を入力するか、または [Select] をクリックしてリストから NAS ポート番号を選択します。NAS ポート番号をクリアするには、[Clear] をクリックします。
Authentication Status	[Authentication Status] ドロップダウン リスト ボックスから、RADIUS 認証のステータスを選択します。次のオプションを使用できます。 • Pass or Fail • Pass • Fail
Failure Reason	失敗理由を入力するか、または [Select] をクリックしてリストから失敗理由を選択します。失敗理由をクリアするには、[Clear] をクリックします。
Time Range	[Time Range] ドロップダウン リスト ボックスから期間を定義します。Monitoring and Report Viewer によって、この期間に作成された RADIUS 認証レコードが取得されます。次のオプションを使用できます。 • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time	（[Time Range] として [Custom] を選択した場合だけ）開始日時を入力するか、またはカレンダ アイコンをクリックして開始日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
End Date-Time	（[Time Range] として [Custom] を選択した場合だけ）終了日時を入力するか、またはカレンダ アイコンをクリックして終了日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
Fetch Number of Records	Monitoring and Report Viewer で一度に取得するレコード数を [Fetch Number of Records] ドロップダウン リストから選択します。使用可能なオプションは、[10]、[20]、[50]、[100]、[200]、および [500] です。
Active Directory Domain Name	Active Directory ドメイン名を入力します。AD レコードは、AD の詳細が提供されたときにのみ取得されます。
Active Directory Domain Admin Name	Active Directory のドメイン管理者名を入力します。AD レコードは、AD の詳細が提供されたときにのみ取得されます。
Active Directory Domain Admin Password	Active Directory のドメイン管理者パスワードを入力します。AD レコードは、AD の詳細が提供されたときにのみ取得されます。

ステップ 4　[Search] をクリックして、検索条件に一致する RADIUS 認証を表示します。

[Search Result] テーブルに、検索結果が読み込まれます。このテーブルには、[Time]、[Status]、[Username]、[MAC Address]、[Audit Session ID]、[Network Device IP]、[Failure Reason]、および [Access Service] というフィールドがあります。

ステップ 5　このテーブルから、トラブルシューティングする RADIUS 認証レコードを選択して、[Troubleshoot] をクリックします。

Expert Troubleshooter によって、RADIUS 認証のトラブルシューティングが開始されます。必要に応じて、Monitoring and Report Viewer によって追加入力が要求されます。

たとえば、Expert Troubleshooter からネットワーク デバイスへの接続が必要な場合は、接続パラメータおよびログイン クレデンシャルの入力を要求するプロンプトが表示されます。

（注）　RADIUS 認証が AD に対して実行された場合、ACS はトラブルシューティング プロセスを開始する前に AD 証明書を要求します。これらのレポートにアクセスするたびに AD クレデンシャルを入力する必要があります。

ステップ 6　[User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。

ステップ 7　[Submit] をクリックします。

[Progress Details] ページが表示されます。このページには概要が表示されます。また、必要に応じて追加入力を要求するプロンプトが表示されます。Monitoring and Report Viewer で追加入力を必要とする場合は、[Click User Input Required] ボタンをクリックする必要があります。ダイアログボックスが表示されます。

表 14-5 の説明に従ってダイアログボックスのフィールドを変更して、[Submit] をクリックします。

表 14-5　[Progress Details] ページ : [User Input] ダイアログボックス

オプション	説明
ネットワーク デバイス a.b.c.d の接続パラメータの指定	
Username	ネットワーク デバイスにログインするためのユーザ名を入力します。
Password	パスワードを入力します。
Protocol	[Protocol] ドロップダウン リストからプロトコルを選択します。有効なオプションは次のとおりです。 • Telnet • SSHv2 [Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続をイネーブルにする必要があります。
Port	ポート番号を入力します。
Enable Password	イネーブル パスワードを入力します。
Same As Login Password	イネーブル パスワードがログイン パスワードと同じ場合は、このチェックボックスをオンにします。
Use Console Server	コンソール サーバを使用する場合にこのチェックボックスをオンにします。
Console IP Address	([Use Console Server] チェックボックスをオンにした場合だけ）コンソールの IP アドレスを入力します。

表 14-5　[Progress Details] ページ : [User Input] ダイアログボックス （続き）

オプション	説明
高度なオプション（「Expect timeout error」が表示される場合や、デバイスから非標準のプロンプト ストリングが返される場合に使用）	
高度なオプションは、一部のトラブルシューティング ツールに対してだけ表示されます。	
Username Expect String	Username: や Login: などの、ネットワーク デバイスによってユーザ名入力用プロンプトとして使用されるストリングを入力します。
Password Expect String	Password: などの、ネットワーク デバイスによってパスワード入力用プロンプトとして使用されるストリングを入力します。
Prompt Expect String	ネットワーク デバイスで使用されるプロンプトを入力します。たとえば、#、>、@ を入力します。
Authentication Failure Expect String	Incorrect password や Login invalid などの、認証エラーが発生した場合にネットワーク デバイスから返されるストリングを入力します。

ステップ 8　[Done] をクリックして、[Expert Troubleshooter] に戻ります。

[Progress Details] ページは定期的に更新されて、トラブルシューティングの進行中に実行されたタスクが表示されます。トラブルシューティングが完了すると、[Show Results Summary] ボタンが表示されます。

ステップ 9　[Show Results Summary] をクリックします。

[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。

表 14-6　[Results Summary] ページ

オプション	説明
Diagnosis and Resolution	
Diagnosis	問題の診断がここに表示されます。
Resolution	問題の解決手順がここに詳細に表示されます。
Troubleshooting Summary	
Summary	トラブルシューティング情報の各ステップの概要がここに表示されます。任意のステップを展開して、詳細を表示できます。 すべての設定エラーが赤いテキストで示されます。

ステップ 10　[Done] をクリックして、[Expert Troubleshooter] に戻ります。

Monitoring and Report Viewer によって、診断、問題の解決手順、および問題の解決に役立つトラブルシューティング概要が提供されます。

（注）　RADIUS Authentication Troubleshooting は、RADIUS 認証レポート ページからも起動できます。この診断ツールを起動する場合は、特定の RADIUS 認証の詳細ページまでドリルダウンする必要があります。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）

- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

ネットワーク デバイス上での show コマンドの実行

Execute Network Device Command 診断ツールを使用すると、ACS Web インターフェイスからネットワーク デバイス上で任意の **show** コマンドを実行できます。**show** コマンドの結果は、コンソールに表示される場合とまったく同じ形式であり、デバイス設定の問題を特定するために使用できます。任意のネットワーク デバイス上で **show** コマンドを実行するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

ステップ 2　トラブルシューティング ツールのリストから、[Execute Network Device Command] を選択します。

[Expert Troubleshooter] ページが更新され、表 14-7 で説明されているフィールドが表示されます。

表 14-7　ネットワーク デバイス上での show コマンドの実行

オプション	説明
情報の入力	
Network Device IP	**show** コマンドを実行するネットワーク デバイスの IPv4 または IPv6 アドレスを入力します。
Command	実行する **show** コマンドを入力します。

ステップ 3　[Run] をクリックして、指定したネットワーク デバイスで **show** コマンドを実行します。

[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。

ステップ 4　[User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。

ステップ 5　[Submit] をクリックして、ネットワーク デバイス上で show コマンドを実行し、出力を表示します。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

ネットワーク デバイスの設定の評価

この診断ツールを使用して、ネットワーク デバイスの設定を評価し、不足している設定や誤っている設定を特定できます。Expert Troubleshooter によって、デバイスの設定が標準設定と比較されます。次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

ステップ 2　トラブルシューティング ツールのリストから、[Evaluate Configuration Validator] をクリックします。

[Expert Troubleshooter] ページが更新され、表 14-8 で説明されているフィールドが表示されます。

表 14-8　Evaluate Configuration Validator

オプション	説明
情報の入力	
Network Device IP	設定を評価するネットワークの IPv4 または IPv6 アドレスを入力します。
推奨テンプレートと比較する設定項目を、次のうちから選択します。	
AAA	デフォルトはオンです。
RADIUS	デフォルトはオンです。
Device Discovery	デフォルトはオンです。
Logging	デフォルトはオンです。
Web Authentication	Web 認証設定を比較する場合にこのチェックボックスをオンにします。
Profiler Configuration	Profiler 設定を比較する場合にこのチェックボックスをオンにします。
SGA	Security Group Access 設定を比較する場合にこのチェックボックスをオンにします。
802.1X	802.1X 設定を比較する場合にこのチェックボックスをオンにします。次のいずれかのオプションを選択します。 • Open Mode • Low Impact Mode (Open Mode + ACL) • High Security Mode (Closed Mode)

ステップ 3　[Run] をクリックします。

[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。

ステップ 4　[User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。

[Troubleshooting Progress Details] ページが表示されます。Expert Troubleshooter によって、ネットワーク デバイスから CLI 応答が取得されます。新しいウィンドウが表示されて、インターフェイス設定を分析するインターフェイスの選択を要求するプロンプトが表示されます。

ステップ 5　分析するインターフェイスの隣にあるチェックボックスをオンにし、[Submit] をクリックして、インターフェイスの設定を評価します。

[Progress Details] ページが表示され、概要が示されます。

ステップ 6　[Show Results Summary] をクリックして、トラブルシューティング概要を表示します。

[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。不足している設定は赤色で表示されます。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

ネットワーク デバイスと ACS との間での SGACL ポリシーの比較

Security Group Access 対応デバイスでは、ACS に設定した出力ポリシー マトリクスに基づいて、ACS によって送信元 SGT と宛先 SGT の各ペアに対して SGACL が割り当てられます。Egress Policy 診断ツールでは、次の処理が実行されます。

1. IP アドレスを指定したデバイスに接続して、送信元 SGT と宛先 SGT の各ペアに対する ACL が取得されます。
2. ACS に設定された出力ポリシーがチェックされ、送信元 SGT と宛先 SGT の各ペアに対する ACL が取得されます。
3. ネットワーク デバイスから取得された SGACL ポリシーと、ACS から取得された SGACL ポリシーが比較されます。
4. ポリシーが一致しない送信元 SGT と宛先 SGT のペアが表示されます。また、追加情報として、一致するエントリも表示されます。

ネットワーク デバイスと ACS との間で SGACL ポリシーを比較するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

ステップ 2　トラブルシューティング ツールのリストから、[Egress (SGACL) Policy] を選択します。

[Expert Troubleshooter] ページが更新され、[Network Device IP] フィールドが表示されます。

ステップ 3　ACS と SGACL ポリシーを比較する Security Group Access デバイスの IP アドレスを入力します。

ステップ 4　[Run] をクリックして、ACS とネットワーク デバイスとの間で SGACL ポリシーを比較します。

[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。

ステップ 5　[User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。

ステップ 6　[Submit] をクリックします。

[Progress Details] ページが表示され、結果の概要が示されます。

ステップ 7　[Show Results Summary] をクリックして、診断および解決手順を表示します。

[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

デバイスとそのピアとの間での SXP-IP マッピングの比較

Security Group Access デバイスは、ピアと通信し、その SGT 値を学習します。Security Exchange Protocol（SXP）-IP Mappings 診断ツールは、指定した IP アドレスのデバイスに接続して、ピア デバイスの IP アドレスおよび SGT 値をリストします。

デバイスのピアを 1 つ以上選択する必要があります。このツールは、選択した各ピアに接続し、その SGT 値を取得して、これらの値が以前に取得した値と同じであるかどうかを確認します。

この診断ツールを使用すると、デバイスとそのピアとの間で SXP-IP マッピングを比較できます。次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

ステップ 2　トラブルシューティング ツールのリストから、[SXP-IP Mappings] を選択します。

[Expert Troubleshooter] ページが更新され、[Network Device IP] フィールドが表示されます。

ステップ 3　ネットワーク デバイスの IP アドレスを入力します。

ステップ 4　トラブルシューティング ツールのリストから、[SXP-IP Mappings] をクリックします。

[Expert Troubleshooter] ページが更新されて、次のフィールドが表示されます。

Network Device IP：ネットワーク デバイスの IP アドレスを入力します。

ステップ 5　[Run] をクリックします。

[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。

ステップ 6　[User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。

[Troubleshooting Progress Details] ページが表示されます。Expert Troubleshooter によって、ネットワーク デバイスから SGA SXP 接続が取得されて、ピア SXP デバイスを選択するように再度要求するプロンプトが表示されます。

ステップ 7　[User Input Required] ボタンをクリックします。

表 14-9 で説明されているフィールドを持つ新しいウィンドウが表示されます。

表 14-9　ピア SXP デバイス

オプション	説明
ピア SXP デバイス	
Peer IP Address	ピア SXP デバイスの IP アドレス。
VRF	ピア デバイスの VRF インスタンス。
Peer SXP Mode	送信者であるかまたは受信者であるかなどの、ピア デバイスの SXP モード。
Self SXP Mode	送信者であるかまたは受信者であるかなどの、ネットワーク デバイスの SXP モード。
Connection State	接続のステータス。
共通接続パラメータ	
User Common Connection Parameters	すべてのピア SXP デバイスの共通接続パラメータをイネーブルにする場合にこのチェックボックスをオンにします。 共通接続パラメータが指定されていない場合、または何らかの理由で共通接続パラメータが機能しない場合には、Expert Troubleshooter によって再度その特定のピア デバイスに対する接続パラメータの入力を要求するプロンプトが表示されます。
Username	ピア SXP デバイスのユーザ名を入力します。
Password	ピア デバイスにアクセスするためのパスワードを入力します。

表 14-9　ピア SXP デバイス （続き）

オプション	説明
Protocol	• [Protocol] ドロップダウン リスト ボックスからプロトコルを選択します。有効なオプションは次のとおりです。 – Telnet – SSHv2 [Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続をイネーブルにする必要があります。
Port	• ポート番号を入力します。デフォルトのポート番号は、Telnet は 23、SSH は 22 です。
Enable Password	イネーブル パスワードがログイン パスワードと異なる場合に入力します。
Same as login password	イネーブル パスワードがログイン パスワードと同じ場合は、このチェックボックスをオンにします。

ステップ 8　SXP マッピングを比較するピア SXP デバイスのチェックボックスをオンにして、表 14-9 の説明に従って共通接続パラメータを入力します。

ステップ 9　[Submit] をクリックします。

[Progress Details] ページが表示され、結果の概要が示されます。

ステップ 10　[Show Results Summary] をクリックして、診断および解決手順を表示します。

[Results Summary] ページが表示され、表 14-6 で説明されている情報が表示されます。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

デバイスの IP-SGT ペアと ACS によって割り当てられた SGT レコードとの比較

Security Group Access 対応デバイスでは、ACS によって、RADIUS 認証を通して各ユーザに SGT 値が割り当てられます。IP User SGT 診断ツールは、指定した IP アドレスのネットワーク デバイスに接続して、次の処理を行います。

1. ネットワーク デバイス上のすべての IP-SGT 割り当てのリストを取得します。
2. 各 IP-SGT ペアの RADIUS 認証レコードおよびアカウンティング レコードをチェックして、ACS によって割り当てられた最新のユーザ IP-SGT 値を確認します。
3. IP-SGT ペアを表形式で表示して、ACS によって割り当てられた最新の SGT 値とデバイス上の SGT 値が同じであるかどうかが特定されます。

この診断ツールを使用すると、デバイスの IP-SGT 値と ACS によって割り当てられた SGT を比較できます。次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

ステップ 2　トラブルシューティング ツールのリストから、[IP User SGT] をクリックします。

[Expert Troubleshooter] ページが更新され、表 14-10 で説明されているフィールドが表示されます。

表 14-10　IP User SGT

オプション	説明
情報の入力	
Network Device IP	ネットワーク デバイスの IPv4 または IPv6 アドレスを入力します。
フィルタ結果	
Username	レコードをトラブルシューティングするユーザのユーザ名を入力します。
User IP Address	レコードをトラブルシューティングするユーザの IP アドレスを入力します。
SGT	ユーザ SGT 値を入力します。

ステップ 3　[Run] をクリックします。

[Progress Details] ページが表示されます。Monitoring and Report Viewer により、追加入力が要求されます。

ステップ 4　[User Input Required] ボタンをクリックし、表 14-5 の説明に従ってフィールドを変更します。

ステップ 5　[Submit] をクリックします。

[Progress Details] ページが表示され、結果の概要が示されます。

ステップ 6　[Show Results Summary] をクリックして、診断および解決手順を表示します。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

デバイス SGT と ACS によって割り当てられたデバイス SGT との比較

Security Group Access 対応デバイスでは、ACS によって、RADIUS 認証を通して各ネットワーク デバイスに SGT 値が割り当てられます。Device SGT 診断ツールは、指定した IP アドレスのネットワーク デバイスに接続して、次の処理を行います。

1. ネットワーク デバイスの SGT 値を取得します。
2. RADIUS 認証レコードをチェックして、ACS によって割り当てられた最新の SGT 値を特定します。
3. デバイス SGT ペアを表形式で表示して、SGT 値が同じであるかどうかが特定されます。

この診断ツールを使用すると、デバイス SGT を、ACS によって割り当てられたデバイス SGT と比較できます。次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Troubleshooting] > [Expert Troubleshooter] を選択します。

[Expert Troubleshooter] ページが表示されます。

ステップ 2　トラブルシューティング ツールのリストから、[Device SGT] をクリックします。

[Expert Troubleshooter] ページが更新され、表 14-11 で説明されているフィールドが表示されます。

表 14-11　Device SGT

オプション	説明
情報の入力	
Network Device IPs（カンマ区切りのリスト）	カンマ区切りのネットワーク デバイス IPv4 または IPv6 アドレス（SGT を、ACS によって割り当てられたデバイス SGT と比較するデバイスの場合）を入力します。
共通接続パラメータ	
Use Common Connection Parameters	比較時に次の共通接続パラメータを使用する場合にこのチェックボックスをオンにします。 • [Username]：ネットワーク デバイスのユーザ名を入力します。 • [Password]：パスワードを入力します。 • [Protocol]：[Protocol] ドロップダウン リスト ボックスからプロトコルを選択します。有効なオプションは次のとおりです。 – Telnet – SSHv2 [Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続をイネーブルにする必要があります。 • [Port]：ポート番号を入力します。デフォルトのポート番号は、Telnet は 23、SSH は 22 です。
Enable Password	イネーブル パスワードがログイン パスワードと異なる場合に入力します。
Same as login password	イネーブル パスワードがログイン パスワードと同じ場合は、このチェックボックスをオンにします。

ステップ 3　[Run] をクリックします。

[Progress Details] ページが表示され、概要が示されます。

ステップ 4　[Show Results Summary] をクリックして、デバイス SGT 比較の結果を表示します。

[Results Summary] ページが表示されて、診断、解決策、およびトラブルシューティング概要が表示されます。

関連トピック

- 「利用可能な診断ツールおよびトラブルシューティング ツール」（P.14-1）
- 「接続テスト」（P.14-1）
- 「ACS サポート バンドル」（P.14-1）
- 「Expert Troubleshooter」（P.14-2）

CHAPTER 15

Monitoring and Report Viewer でのシステムの動作と設定の管理

この章では、Monitoring and Report Viewer を設定および管理するために実行する必要があるタスクについて説明します。[Monitoring Configuration] ドロワでは、次の操作を実行できます。

- データの管理：Monitoring and Report Viewer では、ACS サーバからの大量のデータを処理します。時間が経つにつれ、Monitoring and Report Viewer のパフォーマンスと効率は、データをどう管理するかによって変わってきます。

  データを効率よく管理するには、データを定期的にバックアップして、それをリモートのリポジトリに転送する必要があります。このタスクは、ジョブを定期的に実行するようにスケジューリングすることによって自動化できます。データのバックアップの詳細については、「データの削除と増分バックアップの設定」（P.15-3）を参照してください。

- ログ収集の表示：Monitoring and Report Viewer では、展開内の ACS サーバからログおよび設定データを収集し、そのデータを Monitoring and Report Viewer サーバに格納し、それを処理してレポートとアラームを生成します。展開内の任意のサーバから収集されたログの詳細を表示できます。詳細については、「ログ収集の表示」（P.15-8）を参照してください。

- ログ メッセージのリカバリ：Monitoring and Report Viewer では、ログの収集時に失われたログ エントリをリカバリします。ログ メッセージは、Monitoring and Report Viewer サーバがダウンした場合、または Monitoring and Report Viewer と ACS サーバ間の接続が切断された場合に失われます。

  接続が復旧すると、Monitoring and Report Viewer では失われたエントリを検出し、ACS サーバに通知します。ACS サーバはこの通知を受信すると、Monitoring and Report Viewer にエントリを再送信します。詳細については、「ログ メッセージのリカバリ」（P.15-12）を参照してください。

- スケジューリングされたジョブの表示：Monitoring and Report Viewer では、定期的に実行する必要があるタスクをスケジュールすることができます。

  たとえば、増分バックアップまたは完全バックアップを定期的に実行するようにスケジューリングできます。スケジューラを使用して、これらのタスクの詳細を表示できます。スケジューラの詳細については、「スケジューリングされたジョブの表示」（P.15-12）を参照してください。

- プロセス ステータスの表示：Monitoring and Report Viewer で実行される各種プロセスのステータスを表示できます。Monitoring and Report Viewer で実行される各種プロセスの詳細については、「プロセス ステータスの表示」（P.15-14）を参照してください。

- データ アップグレード ステータスの表示：CLI を使用して ACS 5.3 から ACS 5.4 にアップグレードしたあと、Monitoring and Report Viewer データ アップグレードが完了していることを確認する必要があります。Web インターフェイスを使用して Monitoring and Report Viewer データ アップグレード ステータスを表示して、アップグレードが完了している場合は Monitoring and Report Viewer データベースを切り替えることができます。詳細については、「データ アップグレード ステータスの表示」（P.15-15）を参照してください。

- 障害理由の設定および編集：Monitoring and Report Viewer では、障害理由コードの説明を設定し、問題の解決手順を入力できます。障害理由の説明と解決手順を編集する方法の詳細については、「障害理由の表示」（P.15-15）を参照してください。
- 電子メール設定の指定：電子メール サーバと管理者の電子メール アドレスを設定できます。詳細については、「電子メール設定の指定」（P.15-16）を参照してください。
- 収集フィルタの設定：Monitoring and Report Viewer には、監視またはトラブルシューティングの目的で使用しないデータをフィルタするためのオプションが用意されています。フィルタしたデータはデータベースには格納されないため、必要となるディスク容量を大幅に減らすことができます。収集フィルタを設定する方法の詳細については、「収集フィルタについて」（P.15-17）を参照してください。
- システム アラームの設定：システム アラームにより、ACS Monitoring & Report Viewer の実行時に発生した重大な状態が通知されます。システム アラームの通知を受信するかどうか、またどのように受信するかを設定できます。詳細については、「システム アラーム設定の指定」（P.15-18）を参照してください。
- syslog ターゲットの設定：システム アラーム通知を syslog メッセージとして送信するように Monitoring and Report Viewer を設定した場合は、通知を受信する syslog ターゲットを設定する必要があります。詳細については、「アラーム syslog ターゲットの設定」（P.15-18）を参照してください。
- Monitoring and Report Viewer データのエクスポート：Monitoring and Report Viewer データをエクスポートするためのリモート データベース（Oracle SID または Microsoft AD のいずれか）を設定できます。

  リモート データベース内のデータを使用するカスタム レポート アプリケーションを作成して実行できます。Monitoring and Report Viewer でリモート データベースを設定する方法の詳細については、「リモート データベース設定の指定」（P.15-18）を参照してください。

ACS には、Monitoring and Report Viewer でジョブをスケジューリングするためのオプションが用意されています。ジョブをスケジューリングすると、指定した間隔で監視タスクを自動的に実行できます。スケジューリングされたジョブのステータスを表示し、イベントを制御して、必要に応じて介入できます。スケジューリングできるジョブは次のとおりです。

- データの削除
- バックアップ
- イベント通知（システム アラームおよびしきい値アラーム）
- リモート データベースへの Monitoring and Report Viewer データのエクスポート

この章の内容は、次のとおりです。

- 「データの削除と増分バックアップの設定」（P.15-3）
- 「バックアップからのデータの復元」（P.15-7）
- 「ログ収集の表示」（P.15-8）
- 「ログ メッセージのリカバリ」（P.15-12）
- 「スケジューリングされたジョブの表示」（P.15-12）
- 「プロセス ステータスの表示」（P.15-14）
- 「データ アップグレード ステータスの表示」（P.15-15）
- 「障害理由の表示」（P.15-15）
- 「障害理由の編集」（P.15-15）
- 「電子メール設定の指定」（P.15-16）

- 「SNMP プリファレンスの設定」（P.15-16）
- 「収集フィルタについて」（P.15-17）
- 「システム アラーム設定の指定」（P.15-18）
- 「アラーム syslog ターゲットの設定」（P.15-18）
- 「リモート データベース設定の指定」（P.15-18）

データの削除と増分バックアップの設定

Monitoring and Report Viewer データベースでは、大量のデータが処理されます。データベースのサイズが大きくなりすぎると、すべてのプロセスの速度が低下します。常にすべてのデータが必要になるわけではありません。したがって、データを効率よく管理し、ディスク容量を有効に利用するには、データを定期的にバックアップして、必要なディスク容量を使用している不要なデータを削除する必要があります。データを削除すると、そのデータはデータベースから削除されます。

Monitoring and Report Viewer データベース サイズは大きいため、バックアップ プロセスが完了するまでに長く時間がかかります。増分バックアップ オプションを使用すると、Monitoring and Report Viewer データベースの完全バックアップを 1 回実行したら、それ以降はデータを増分的にバックアップできるようになっています（つまり、更新だけがバックアップされ、別個に格納されます）。

増分バックアップの初回実行時には完全なデータベース バックアップが実行され、それ以降はデータベースに加えられた更新だけがバックアップされます。したがって、増分バックアップでは、処理時間が短縮され、ディスク容量が有効に利用されます。また、増分バックアップの頻度と時間を設定することもできます。

増分バックアップでは、複数のバックアップ ファイルがリポジトリに格納されます。ただし、増分バックアップからデータを復元するときには、完全バックアップから最新の増分バックアップまでのすべてのバックアップ ファイルからデータが復元されます。

（注） 何らかの理由で増分バックアップをディセーブルにした場合、次回は完全バックアップを実行しないと、増分バックアップを再び続けることはできません。

また、完全なデータベース バックアップを設定して、その頻度と時間を定義することもできます。

さらに、ACS では、完全な Monitoring and Report Viewer データベースのバックアップを即座に実行することもできます。ただし、増分バックアップ、完全バックアップ、およびデータの削除を同時に実行することはできません。これらのジョブのいずれかが実行中の場合は、次のジョブを開始するまでに 90 分間待機する必要があります。

ワンポイント アドバイス 完全バックアップを毎回実行するのではなく、最初に完全バックアップを実行し、それ以降はデータを増分的にバックアップすることを推奨します。

（注） 毎日の増分バックアップと週に 1 回または月に 1 回の完全バックアップをスケジュールすることを強く推奨します。そうでないと、データベース削除プロセスはデータの削除に失敗し、それがディスク領域の問題につながります。毎月のスケジュール バックアップは、月の最後の日に発生し、毎週のスケジュール バックアップは、週の最後の日に実行されます。

（注）　削除前にデータが確実にバックアップされるようにするには、CLI または ACS Web インターフェイス（[System Administration] > [Operations] > [Software Repositories]）を使用してデータ リポジトリを設定します。リポジトリを設定する方法の詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

増分バックアップをイネーブルにすると、データは毎日午前 4 時に削除されます。これは、View プロセスを実行している ACS インスタンスが存在するローカル タイムゾーンの時間です。

ACS 5.4 では、ビュー データベースは opt パーティションのサイズに基づいて割り当てられます。ACS View データベースは opt パーティションのサイズの 42 パーセントです。

削除には、次のデータベース制限が適用されます。

- データベースのディスク使用量が割り当てられたビュー データベース サイズの 60 パーセントを超える場合、ダッシュボードにアラームが送信されます。
- データベースのディスク使用量が割り当てられたビュー データベース サイズの 80 パーセントを超える場合、データベースのディスク使用量が割り当てられたビュー データベース サイズの 60 パーセントを下回るまで、バックアップが実行され直後に削除が続きます。バックアップが失敗した場合は、データベースのディスク使用量を再度確認してください。Monitoring and Report Viewer データが、データベースから削除されます。最初に最も古いデータが削除されます。
  - データベースのディスク使用量が割り当てられたビュー データベース サイズの 60 パーセントを超える場合、データベースのディスク使用量が割り当てられたビュー データベース サイズの 60 パーセントを下回るまで、バックアップが実行され直後に削除が続きます。
  - バックアップが失敗し、データベースのディスク使用量が割り当てられたビュー データベース サイズの 60 パーセントを超える場合、Monitoring and Report Viewer で待機が決定されます。

  次に例を示します。

  - 1 ヵ月のデータを維持することを指定したときに、データベース サイズが割り当てられたビュー データベース サイズの 100 パーセントを 1 ヵ月以内に超える場合は、削除によって、データベース サイズが割り当てられたビュー データベース サイズの 80 パーセントに達するまでデータを毎週削除します。
  - 1 ヵ月を超えるデータ（たとえば、5 カ月のデータ）を維持することを指定したが、データベース サイズが割り当てられたビュー データベース サイズの 80 パーセントを超える場合、削除が発生します。削除後にデータベース サイズが割り当てられたビュー データベース サイズの 80 パーセントを超えたままの場合、追加の月のデータは削除され、4 カ月分のデータが維持される結果になります。削除前に、データベースがバックアップされます。
- データベース サイズが割り当てられたビュー データベース サイズの 100 パーセントを超える場合、削除はデータベース バックアップが実行されたかどうかにかかわらず発生します。データベース サイズが割り当てられたビュー データベース サイズの 80 パーセントを超えたままの場合は、追加の削除が、データベースが割り当てられたビュー データベース サイズの 80 パーセントになるまで行われます。

（注）　リポジトリが設定されない状態で、増分バックアップが ON に設定された場合、データベース バックアップは失敗し、増分バックアップ モードは OFF に変更されます。

（注）　増分バックアップがディセーブルになっている場合、データは毎月末（UTC 時間）に削除されます。

[Data Purging and Incremental Backup] ページでは、次の操作を実行できます。

- 削除ウィンドウ サイズの設定
- データベースからのデータの削除
- （削除ジョブの）バックアップを管理するためにバックアップ場所として使用するデータ リポジトリの割り当て
- 増分バックアップと完全バックアップのスケジュールの設定
- 即座のバックアップの設定

ACS データベースはメンテナンス操作の一部として圧縮する必要があります。ビュー データベースの物理サイズと実際のサイズに差がある場合、ビュー データベースの物理サイズを小さくするために ACS コンフィギュレーション モードから **acsview-db-compress** コマンドを実行できます。ACS 5.4 は圧縮処理中にログ コレクタ サービスのみを停止し、圧縮処理の完了後は稼働しています。ログ リカバリ機能をイネーブルにして、データベースの圧縮処理中に受信したログ メッセージをリカバリする必要があります。

ACS 5.4 では、データベースの圧縮処理は自動化されています。午前 5 時に ACS View データベースを毎日自動的に圧縮するために、[Enable ACS View Database Compress] チェックボックスをオンにできます。データベースの圧縮処理は必要があるたびに毎日午前 5 時に自動的に実行されます。

（注） ログ リカバリ オプションをイネーブルにして、データベースの圧縮処理中に受信した可能性のあるログ メッセージをリカバリする必要があります。ログ リカバリ機能がイネーブルになっていない場合、ACS はログのリカバリ機能をイネーブルにするためにアラート メッセージを送信します。

次のデータベース制限が、ACS データベースの圧縮に適用されます。

- 自動データベース圧縮処理はデータベース サイズが割り当てられたビュー データベース サイズの 80 パーセントを超えるとすぐに、次の日の午前 5 時に開始されます。
- ACS はビュー データベースの物理サイズと実際のサイズの差が割り当てられたビュー データベース サイズの 7 パーセントを超え、かつ割り当てられたビュー データベース サイズの 36 パーセントを下回る場合にアラート メッセージを表示します。また、自動データベース圧縮処理はディスク領域の問題を回避するためにデータベースのサイズが割り当てられたビュー データベース サイズの 80 パーセントを超えたときにトリガーされます。
- ACS はビュー データベースの物理サイズと実際のサイズの差が割り当てられたビュー データベース サイズの 36 パーセントを超える場合にアラート メッセージを表示します。
  - ログ リカバリ機能がイネーブルになっていないときに、ACS ビュー データベース圧縮オプションがイネーブルの場合、自動データベース圧縮処理は、ディスク領域の問題を回避するためにデータベースのサイズが割り当てられたビュー データベース サイズの 80 パーセントを超えたときに、ログ リカバリ機能を有効にした後でだけトリガーされます。
  - ログ リカバリ機能と ACS ビュー データベース圧縮オプションがイネーブルの場合は、ディスク領域の問題を回避するために自動データベース圧縮処理が開始されます。ログ コレクタ サービスはこの処理中にシャットダウンされ、圧縮処理完了後は稼働しています。ログ リカバリ機能をすでにイネーブルにしているため、データベース圧縮処理中に受信されたすべてのログ メッセージがログ コレクタ サービスの稼働後にリカバリされます。
  - ログ リカバリ機能と ACS ビュー データベース圧縮オプションがイネーブルになっていない場合、ACS はデータベース圧縮処理をトリガーしません。ただし、データベースのサイズが割り当てられたビュー データベースの 80 パーセントを超えると、自動データベース圧縮処理はディスク領域の問題を回避するためにログ リカバリ機能を有効にした後でだけトリガーされます。

– ログ リカバリ機能がイネーブルになっているときに、ACS ビュー データベース圧縮オプションがイネーブルでない場合、自動データベース圧縮処理は、ディスク領域の問題を回避するためにデータベースのサイズが割り当てられたビュー データベース サイズ制限の 80 パーセントを超えたときに開始されます。ログ コレクタ サービスはこの処理中にシャットダウンされ、圧縮処理完了後は稼働しています。ログ リカバリ機能をすでにイネーブルにしているため、データベース圧縮処理中に受信されたすべてのログ メッセージがログ コレクタ サービスの稼働後にリカバリされます。

（注） メンテナンス時間中にデータベースの圧縮を実行することを推奨します。DB の圧縮は、データベースのサイズに応じて時間が長くかかる可能性があります。データベースの圧縮は削除操作の完了後にする必要があります。

Monitoring and Report Viewer で、[Monitoring Configuration] > [System Operations] > [Data Management] > [Removal and Backup] を選択します。

表 15-1　[Data Purging and Incremental Backup] ページ

オプション	説明
Data Purging	
Data Repository	ドロップダウン リスト ボックスを使用して、データの削除時にバックアップ場所として使用するデータ リポジトリを選択します。 データ リポジトリを追加する方法については、『*CLI Reference for ACS 5.4*』を参照してください。
Maximum Stored Data Period *num* months.	ドロップダウン リスト ボックスを使用して、月数を指定します。*num* は、Monitoring and Report Viewer データベースに何ヶ月間のデータを保持するかを表す数値です。
Enable ACS View Database Compress	午前 5 時に ACS View データベースを毎日自動的に圧縮するために、[Enable ACS View Database Compress] チェックボックスをオンにします。
On-Demand Data Purge	
Purge Now	データを削除するには、[Purge Now] をクリックします。この削除は、すでに設定されている削除の制限を上書きします。 **（注）**　オンデマンド削除を実行する前に、フル バックアップをすることが推奨されます。
View Full Database Backup Now	
Data Repository	ドロップダウン リスト ボックスを使用して、完全なデータベース バックアップを格納するためのバックアップ場所として使用するデータ リポジトリを選択します。
Backup Now	完全な Monitoring and Report Viewer データベース バックアップを開始するには、[Backup Now] をクリックします。
Incremental Backup	
On	増分バックアップをイネーブルにするには、[On] オプション ボタンをクリックします。増分バックアップがイネーブルである場合は、デルタがバックアップされます。
Off	増分バックアップをディセーブルにするには、[Off] オプション ボタンをクリックします。
Configure Incremental View Database Backup	
Data Repository	ドロップダウン リスト ボックスを使用して、バックアップ ファイル用のデータ リポジトリを選択します。
Schedule	ドロップダウン リスト ボックスを使用して、増分バックアップを実行する時間を選択します。

表 15-1　[Data Purging and Incremental Backup] ページ （続き）

オプション	説明
Frequency	ドロップダウン リスト ボックスを使用して、増分バックアップを実行する頻度を選択します。有効なオプションは次のとおりです。 • Daily • [Weekly]：通常は毎週末に発生します。 • [Monthly]：通常は毎月末に発生します。
Configure Full View Database Backup	
Data Repository	ドロップダウン リスト ボックスを使用して、バックアップ ファイルを格納するデータ リポジトリを選択します。
Schedule	ドロップダウン リスト ボックスを使用して、完全な View データベース バックアップを実行する時間を選択します。
Frequency	ドロップダウン リスト ボックスを使用して、完全な View データベース バックアップを実行する頻度を選択します。有効なオプションは次のとおりです。 • Daily • [Weekly]：通常は毎週末に発生します。 • [Monthly]：通常は毎月末に発生します。

NFS ステージングの設定

/opt の使用率が 30 パーセントを超えると、View データベースのバックアップを成功させ、サポート バンドルを生成するためにリモート リポジトリで NFS ステージングを使用する必要があります。これらの処理には大量のディスク容量が必要であるため、NFS ステージングはバックアップ / サポート バンドル要求中に追加のディスク容量のステージング領域として、Network File System（NFS）共有を使用します。**backup-staging-url** コマンドを使用して CLI によって NFS ステージングをイネーブルにできます。**backup-staging-url** コマンドの詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

（注）　ビューのバックアップおよびサポート バンドルの生成と同じディスク容量制限の影響は受けないため、この項は、ACS バックアップ操作には適用されません。

関連項目

「バックアップからのデータの復元」（P.15-7）

バックアップからのデータの復元

このページは、以前にバックアップされた View データベースからデータを復元する場合に使用します。増分バックアップと完全バックアップのいずれからでもデータを復元できます。増分バックアップ データを復元するように指定した場合は、完全な View データ バックアップが復元されてから、残りの増分バックアップが正しい順序で一度に 1 つずつ復元されます。

バックアップからデータを復元するには、次の手順を実行します。

ステップ 1　[Monitoring Configuration] > [System Operations] > [Data Management] > [Restore] を選択します。

[Incremental Backup Restore] ページが表示され、[Available Backups to Restore] テーブルが示されます。表 15-2 に、テーブルのカラムを示します。

表 15-2　[Incremental Backup Restore] ページ

カラム	説明
Skip View Database backup before Restore	バックアップからデータを復元する前に、Monitoring and Report Viewer データベース バックアップをスキップするには、このチェックボックスをオンにします。このオプションをオンにしていると、復元プロセスが速くなります。 復元プロセス中に障害が発生すると現在のデータが失われる可能性があるため、このチェックボックスはオフにすることを推奨します。
Name	バックアップ ファイルの名前。バックアップ ファイルの名前には、タイムスタンプが含まれています。たとえば、ACSViewBackup-20090618_003400 のようになります。 増分バックアップの場合、[Expand] アイコンをクリックすると、関連付けられている完全バックアップと増分バックアップが表示されます。
Date	バックアップの実行日。
Repository	バックアップ ファイルが格納されているリポジトリの名前。
Type	バックアップのタイプ（[Incremental] または [Full]）。

ステップ 2　復元するバックアップ ファイルを選択します。

（注）　増分バックアップ ファイルを復元するように指定した場合は、以前に関連付けられたすべての増分バックアップと完全バックアップが復元されます。この復元プロセスでは、Monitoring and Report Viewer データだけが復元されます。

ステップ 3　[Restore] をクリックして、バックアップ ファイルを復元します。

関連項目

「データの削除と増分バックアップの設定」（P.15-3）

ログ収集の表示

このページは、ACS サーバから最近収集されたログを表示する場合に使用します。

Monitoring and Report Viewer で、[Monitoring Configuration] > [System Operations] > [Log Collection] を選択します。

（注）　更新記号を使用して、ページの内容を更新できます。

表 15-3　[Log Collection] ページ

オプション	説明
ACS Server	ACS サーバの名前。クリックすると、[Log Collection Details] ページが開き、最近収集されたログが表示されます。
Last Syslog Message	*表示のみ*。最新の syslog メッセージの到達時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* 形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • timezone = タイムゾーン。分散環境では、すべてのセカンダリ サーバに対して表示されるタイムゾーンは、表示がアクティブなサーバのタイムゾーンに対応しています。 プライマリ インスタンスのタイムゾーンが PDT であり、セカンダリ インスタンスが UTC である場合、セカンダリ インスタンスでは、プライマリ インスタンスのタイムゾーンに対応する PDT の syslog メッセージのタイムゾーンおよびタイムスタンプが表示されます。 • yyyy = 年を表す 4 桁の数字。
Last Error	*表示のみ*。最新のエラー メッセージの名前を示します。
Last Error Time	*表示のみ*。最新のエラー メッセージの到達時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* 形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • timezone = タイムゾーン。分散環境では、すべてのセカンダリ サーバに対して表示されるタイムゾーンは、表示がアクティブなサーバのタイムゾーンに対応しています。 プライマリ インスタンスのタイムゾーンが PDT であり、セカンダリ インスタンスが UTC である場合、セカンダリ インスタンスでは、プライマリ インスタンスのタイムゾーンに対応する PDT の syslog メッセージのタイムゾーンおよびタイムスタンプが表示されます。 • yyyy = 年を表す 4 桁の数字。
Get Details	クリックすると、選択した ACS サーバについて最近収集されたログが表示されます。

関連項目

「[Log Collection Details] ページ」（P.15-10）

[Log Collection Details] ページ

このページは、ACS サーバについて最近収集されたログの名前を表示する場合に使用します。

ステップ 1　Monitoring and Report Viewer で、[Monitoring Configuration] > [System Operations] > [Log Collection] を選択します。

ステップ 2　次のいずれかを実行します。

- ACS サーバの名前をクリックします。
- 最近収集されたログを表示するために使用する ACS サーバ名のオプション ボタンを選択し、[Get Details] をクリックします。

（注）　更新記号を使用して、ページの内容を更新できます。

表 15-4　[Log Collection Details] ページ

オプション	説明
Log Name	ログ ファイルの名前。
Last Syslog Message	*表示のみ*。最新の syslog メッセージの到達時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* 形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • timezone = タイムゾーン。分散環境では、すべてのセカンダリ サーバに対して表示されるタイムゾーンは、表示がアクティブなサーバのタイムゾーンに対応しています。 プライマリ インスタンスのタイムゾーンが PDT であり、セカンダリ インスタンスが UTC である場合、セカンダリ インスタンスでは、プライマリ インスタンスのタイムゾーンに対応する PDT の syslog メッセージのタイムゾーンおよびタイムスタンプが表示されます。 • yyyy = 年を表す 4 桁の数字。
Last Error	*表示のみ*。最新のエラー メッセージの名前を示します。
Last Error Time	*表示のみ*。最新のエラー メッセージの到達時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* 形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • timezone = タイムゾーン。分散環境では、すべてのセカンダリ サーバに対して表示されるタイムゾーンは、表示がアクティブなサーバのタイムゾーンに対応しています。 プライマリ インスタンスのタイムゾーンが PDT であり、セカンダリ インスタンスが UTC である場合、セカンダリ インスタンスでは、プライマリ インスタンスのタイムゾーンに対応する PDT の syslog メッセージのタイムゾーンおよびタイムスタンプが表示されます。 • yyyy = 年を表す 4 桁の数字。
Back	クリックすると、[Log Collection] ページに戻ります。
Refresh	クリックすると、このページのデータが更新されます。

関連項目

- 「ログ収集の表示」（P.15-8）

ログ メッセージのリカバリ

ACS サーバは、成功した認証、失敗した試行、許可、アカウンティングなどのアクティビティについて Monitoring and Report Viewer に syslog メッセージを送信します。

syslog メッセージにはシーケンス番号が添付されています。Monitoring and Report Viewer がダウンした場合、または ACS からメッセージを受信できない場合、Monitoring and Report Viewer は、ロギング リカバリ メカニズムを使用して、これらの失われたログを ACS から再試行します。

Monitoring and Report Viewer は、syslog メッセージを処理し、シーケンスに不一致があればそれを特定します。このようにして、失われたメッセージを見つけます。

Monitoring and Report Viewer は、欠落しているログ メッセージを再送するように ACS サーバに通知します。ACS サーバはローカル ストアに保存されているメッセージを処理し、それらを Monitoring and Report Viewer に再送します。

（注） ログ メッセージのリカバリ機能が希望どおりに動作するように、[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] で ACS の関連するロギング カテゴリの [Log to Local Target] オプションをイネーブルにします。

ログ メッセージのリカバリを有効にするには、[Monitoring Configuration] > [System Operations] > [Log Message Recovery] を選択します。

表 15-5　[Log Message Recovery] ページ

オプション	説明
Log Message Recovery Option	
On	ログ メッセージのリカバリ機能をイネーブルにします。
Off	ログ メッセージのリカバリ機能をディセーブルにします。
Configure Log Message Recovery Intervals	
Run Every Minute(s)	リカバリを実行する分単位の期間を設定します。
Run Every Hour(s)	リカバリを実行する時間単位の期間を設定します。
Configure Missing Entry count to be re-sent by Collector	
No.of Missing Entries to be re-sent by Collector during recovery at a time	ACS サーバによって一度に送信できる欠落エントリの最大数。デフォルトの制限値は 1000 で、最大値は 9999 です。これより大きい値を設定した場合、ACS パフォーマンスがダウンする可能性があります。

（注） ビュー ロギング リカバリは、ビュー ロギング リカバリ機能がディセーブルでビューがダウンしている場合には、失われたログを取得しません。

スケジューリングされたジョブの表示

このページは、スケジューリングされたジョブを表示する場合に使用します。

Monitoring and Report Viewer で、[Monitoring Configuration] > [System Operations] > [Scheduler] を選択します。

表 15-6　[Scheduler Status] ページ

オプション	説明
Name	*表示のみ。*ジョブの名前。
Type	*表示のみ。*関連付けられているジョブのタイプ（たとえば、[Incremental Backup Utility]、[Session Termination]、[DB Aggregation Event]、[Database Purge Utility] など）。このリストには、システム定義ジョブとユーザ定義ジョブの両方が含まれています。
Owner	*表示のみ。*関連付けられているジョブの所有者：[System]。
Last Run Time	*表示のみ。*関連付けられているジョブの時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* の形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • *timezone* = タイムゾーン。 • yyyy = 年を表す 4 桁の数字。
Last Run Result	*表示のみ。*関連付けられているジョブの前回の実行結果。
Status	*表示のみ。*関連付けられているジョブのステータス。

（注）　ACS Web インターフェイスからスケジュールを変更した場合、新しいスケジュールを有効にするには、Job Manager プロセスを手動で再起動する必要があります。プロセスを再起動するための CLI コマンドの詳細については、次を参照してください。
http://preview.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli_app_a.html

プロセス ステータスの表示

このページは、ACS 環境で実行されているプロセスのステータスを表示する場合に使用します。

Monitoring and Report Viewer で、[Monitoring Configuration] > [System Operations] > [Process Status] を選択します。

（注）　更新記号をクリックして、ページの内容を更新できます。

表 15-7　[Process Status] ページ

オプション	説明
Process Name	*表示のみ*。プロセスの名前。オプションは次のとおりです。 • Database • Management（ACS 管理サブシステム） • Ntpd • Runtime（ACS 実行時サブシステム） • View-alertmanager • View-collector • View-database • View-jobmanager • View-logprocessor
Status	*表示のみ*。関連付けられているプロセスのステータスを示します。
CPU Utilization	*表示のみ*。関連付けられているプロセスの CPU 使用率を示します。
Memory Utilization	*表示のみ*。関連付けられているプロセスのメモリ使用率を示します。
Uptime	*表示のみ*。プロセスが正常に開始された時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* の形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • *timezone* = タイムゾーン。 • yyyy = 年を表す 4 桁の数字。

データ アップグレード ステータスの表示

ACS 5.4 にアップグレードしたあとは、Monitoring and Report Viewer データベースのアップグレードが完了していることを確認します。

この作業は、ACS Web インターフェイスから行うことができます。アップグレード プロセスの詳細については、『*Installation Guide for Cisco Secure Access Control System 5.4*』を参照してください。

Monitoring and Report Viewer データ アップグレードのステータスを表示するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer で、[Monitoring Configuration] > [System Operations] > [Data Upgrade Status] を選択します。

ステップ 2　[Data Upgrade Status] ページが表示され、次の情報が示されます。

[Status] : Monitoring and Report Viewer データ アップグレードが完了しているかどうかを示します。

障害理由の表示

このページは、障害理由を表示する場合に使用します。

Monitoring and Report Viewer で、[Monitoring Configuration] > [System Configuration] > [Failure Reasons Editor] を選択します。

表 15-8 に、[Failure Reasons] ページのフィールドを示します。

表 15-8　[Failure Reasons] ページ

オプション	説明
Failure Reasons	考えられる障害理由の説明。障害理由の名前をクリックすると、[Failure Reasons Editor] ページが開きます。

関連項目

- 「障害理由の編集」（P.15-15）

障害理由の編集

このページは、障害理由を編集し、管理者が同じ障害に直面したときに参考にできるように解決手順の候補を追加する場合に使用します。

ステップ 1　Monitoring and Report Viewer で、[Monitoring Configuration] > [System Configuration] > [Failure Reasons Editor] を選択します。

ステップ 2　次のいずれかをクリックします。

- 編集する障害理由の名前。
- 編集する障害理由に関連付けられているオプション ボタン。そのあと、[Edit] をクリックします。

表 15-9 に示す [Failure Reason Editor] ページが表示されます。

表 15-9　[Failure Reasons Editor] ページ

オプション	説明
Failure Reason	表示のみ。エラー コードおよび関連付けられている障害理由の名前。
Description	管理者が参考にできるように、障害理由の説明を自由形式のテキストで入力します。
Resolution Steps	管理者が参考にできるように、障害理由に対する解決手順の候補の説明を自由形式のテキストで入力します。

関連項目

「障害理由の表示」（P.15-15）

電子メール設定の指定

このページは、電子メール サーバと管理者の電子メール アドレスを指定する場合に使用します。

Monitoring and Report Viewer で、[Monitoring Configuration] > [System Configuration] > [Email Settings] を選択します。

表 15-10　[Email Settings] ページ

オプション	説明
Mail Server	有効な IPv4 または IPv6 電子メール ホスト サーバを入力します。
Mail From	ユーザがシステムから電子メールを受信したときに表示されるようにする電子メール アドレスの名前を入力します。

SNMP プリファレンスの設定

MIB オブジェクトへのアクセスを認証するように SNMP プリファレンスを設定できます。SNMP プリファレンスについて入力するテキスト文字列は、埋め込みパスワードとして機能します。

SNMP プリファレンスを設定するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer で、[Monitoring Configuration] > [System Configuration] > [SNMP Settings] を選択します。

[SNMP Preferences] ページが表示されます。

ステップ 2　[SNMP V2 Read Community String] フィールドに、MIB オブジェクトの認証に使用するパスワードを入力します。

ステップ 3　[Submit] をクリックします。

収集フィルタについて

監視またはトラブルシューティングの目的で使用しない syslog イベントをフィルタして除去できる収集フィルタを作成できます。収集フィルタを設定すると、Monitoring and Report Viewer でこれらのイベントがデータベースに記録されなくなるため、必要となるディスク容量が大幅に減ります。

（注）　ACS 5.4 は、IPv6 ソースからの syslog メッセージの収集をサポートします。

ここでは、次の内容について説明します。

- 「収集フィルタの作成および編集」（P.15-17）
- 「収集フィルタの削除」（P.15-18）

収集フィルタの作成および編集

このページは、収集フィルタを作成または編集する場合に使用します。次の手順を実行します。

ステップ 1　Monitoring and Report Viewer で、[Monitoring Configuration] > [System Configuration] > [Collection Filters] を選択します。

[Collection Filters] ページが表示されます。

ステップ 2　[Filters] 領域で、次のいずれかの操作を実行します。

- [Create] をクリックして、収集フィルタを作成します。
- 編集する syslog 属性のチェックボックスをオンにして、[Edit] をクリックします。
- 削除する syslog 属性のチェックボックスをオンにして、[Delete] をクリックします。

表 15-11 に示す [Add or Edit Collection Filters] ページが表示されます。

表 15-11　[Add or Edit Collection Filters] ページ

オプション	説明
Syslog Attribute	• [Add Filter] ページで、次の syslog 属性のいずれかを選択します。 – [NAS IP Address]：IPv4 および IPv6 アドレスがサポートされます。 – Access Service – MAC Address – User • [Edit Filter] ページでは、このフィールドは表示専用です。
Value	syslog 属性の値を入力します。 • [NAS IP Address]：フィルタする NAS の IP アドレスを入力します。 • [Access Service]：フィルタするアクセス サービスの名前を入力します。 • [MAC Address]：フィルタするマシンの MAC アドレスを入力します。 • [User]：フィルタするユーザのユーザ名を入力します。

ステップ 3　[Submit] をクリックします。

関連トピック

- 「収集フィルタの作成および編集」（P.15-17）
- 「収集フィルタの削除」（P.15-18）

収集フィルタの削除

収集フィルタを削除するには、次の手順を実行します。

ステップ 1　[Monitoring Configuration] > [System Configuration] > [Collection Filters] を選択します。

[Collection Filters] ページが表示されます。

ステップ 2　削除する 1 つ以上の収集フィルタのチェックボックスをオンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item(s)?
```

ステップ 3　[Yes] をクリックします。

[Collection Filters] ページが表示されます。このとき、削除された収集フィルタは表示されません。

システム アラーム設定の指定

システム アラーム設定を指定する方法については、「システム アラーム設定の設定」（P.12-34）を参照してください。

アラーム syslog ターゲットの設定

syslog ターゲットを設定する方法については、「アラーム Syslog ターゲットについて」（P.12-35）を参照してください。

リモート データベース設定の指定

このページは、Monitoring and Report Viewer データをエクスポートするためのリモート データベースを設定する場合に使用します。データは、指定した間隔でこのリモート データベースにエクスポートされます。エクスポート ジョブは、1、2、4、6、8、12、または 24 時間ごとに 1 回実行するようにスケジューリングできます。ACS 5.4 では、20 ～ 40 分ごとに実行するエクスポート ジョブをスケジュールすることもできます。このリモート データベースと連携動作するカスタム レポート アプリケーションを作成できます。ACS では、次のデータベースがサポートされています。

- Oracle SQL Developer
- Microsoft SQL Server 2005

リモート データベースを設定するには、次の手順を実行します。

ステップ 1　Monitoring and Report Viewer で、[Monitoring Configuration] > [System Configuration] > [Remote Database Settings] を選択します。

表 15-12 に示す [Remote Database Settings] ページが表示されます。

表 15-12　[Remote Database Settings] ページ

オプション	説明
Publish to Remote Database	ACS でリモート データベースに定期的にデータをエクスポートするには、このチェックボックスをオンにします。デフォルトでは、データは 4 時間ごとにリモート データベースにエクスポートされます。
Server	リモート データベースの DNS 名または IP アドレスを入力します。
Port	リモート データベースのポート番号を入力します。
Username	リモート データベースへのアクセスに使用するユーザ名を入力します。
Password	リモート データベースへのアクセスに使用するパスワードを入力します。
Export Every Minutes	ドロップダウン リスト ボックスから時間間隔を選択して、ACS によって指定した間隔でデータがエクスポートされるようにします。有効なオプションは 20 分と 40 分です。デフォルトの間隔は 20 分です。 **（注）** 40 分として間隔を選択すると、ACS によってリモート データベースのエクスポート操作がただちに初めて開始され、そこから 40 分ごとに操作が継続します。
Export Every Hours	ドロップダウン リスト ボックスから時間間隔を選択して、ACS によって指定した間隔でデータがエクスポートされるようにします。有効なオプションは 1、2、4、6、8、12、および 24 時間です。デフォルトの間隔は 4 時間です。
Database Type	設定するリモート データベースのタイプ。 • Microsoft データベースを設定するには、[Microsoft Database] オプション ボタンをクリックし、リモート データベースの名前を入力します。 • Oracle データベースを設定するには、[Oracle SID] オプション ボタンをクリックし、Oracle データベースのシステム識別子を入力します。
Download Remote Database schema files	リモート データベース スキーマ ファイルをダウンロードするには、このリンクをクリックします。次の 2 つのスキーマ ファイルがダウンロードされます。 • acsview_microsoft_schema.sql • acsview_oracle_schema.sql

ステップ 2　[Submit] をクリックして、リモート データベースを設定します。

（注）　特殊文字はリモート データベースの名前ではサポートされません。

（注）　スケジューラを使用して、エクスポート ジョブのステータスを表示できます。詳細については、「スケジューリングされたジョブの表示」（P.15-12）を参照してください。

CHAPTER 16

システム管理者の管理

システム管理者は、ネットワーク内の ACS サーバを展開、設定、管理、および監視します。システム管理者は、ACS 管理インターフェイスを使用して、ACS でさまざまな操作を実行できます。ACS で管理者を定義するとき、パスワードおよびロールまたはロールのセットを割り当てます。ロールによって、さまざまな操作に対する管理者のアクセス権が決定されます。

管理者アカウントを作成するとき、最初にパスワードを割り当てます。管理者は、あとで ACS Web インターフェイスを使用して、このパスワードを変更できます。割り当てられているロールに関係なく、管理者は自分のパスワードを変更できます。

ACS では、次の設定可能なオプションを使用して、管理者パスワードを管理できます。

- Password Complexity：パスワードの必要な長さと文字タイプを指定します。
- Password History：同じパスワードを繰り返し使用できないようにします。
- Password Lifetime：指定された時間が経過したあと、管理者に対してパスワードの変更を強制します。
- Account Inactivity：指定時間使用されていない管理者アカウントをディセーブルにします。
- Password Failures：管理者アカウントが指定した回数連続してログインに失敗した場合に、そのアカウントをディセーブルにします。

さらに、ACS には、管理者が ACS 管理 Web インターフェイスへのアクセスに使用する IP アドレスおよびセッション継続時間を決定する、設定可能なオプションがあります。セッション継続時間を経過すると、アイドル セッションはシステムからログアウトします。

Monitoring and Report Viewer を使用して、システムへの管理者アクセスを監視できます。システムに現在アクセスしている管理者またはアクセスしようとしている管理者を監視するには、Administrator Access レポートを使用します。

Administrator Entitlement レポートを表示すると、管理者が持っているアクセス権、管理者が加えた設定変更、および管理者アクセスの詳細を表示できます。また、Configuration Change および Operational Audit レポートを使用して、各管理者が実行する特定の操作の詳細を表示することもできます。

ACS Web インターフェイスの [System Administrator] セクションでは、次の操作を実行できます。

- 管理者アカウントの作成、編集、複製、または削除
- 他の管理者のパスワード変更
- 事前定義済みのロールの表示
- 管理者へのロールの関連付け
- パスワードの複雑さ、アカウントのライフタイム、非アクティブなアカウントなどの認証設定

- 管理者セッションの設定
- 管理者アクセスの設定

ACS 5.4 に初めてログインすると、事前定義済みの管理者ユーザ名（*ACSAdmin*）の入力を要求するプロンプトが表示され、事前定義済みのパスワード名（*default*）を変更することを要求されます。パスワードを変更したあと、システムの設定を開始できます。

事前定義済みの管理者には、すべての ACS リソースに対するスーパー管理者権限（Create、Read、Update、Delete、および eXecute（CRUDX））があります。プライマリ インスタンスにセカンダリ インスタンスを登録すると、プライマリ インスタンスで作成された任意のアカウントを使用できます。プライマリ インスタンスで作成したクレデンシャルは、セカンダリ インスタンスに適用されます。

（注）　インストール後、ACS に初めてログインするときに、ACS Web インターフェイスからログインしてライセンスをインストールする必要があります。インストール後すぐに CLI から ACS にログインすることはできません。

ここでは、次の内容について説明します。

- 「管理者ロールおよびアカウントについて」（P.16-2）
- 「システム管理者およびアカウントの設定」（P.16-3）
- 「ロールについて」（P.16-3）
- 「管理者アカウントの作成、複製、編集、および削除」（P.16-7）
- 「事前定義済みのロールの表示」（P.16-9）
- 「管理者の認証設定」（P.16-10）
- 「セッション アイドル タイムアウトの設定」（P.16-13）
- 「管理者アクセスの設定」（P.16-13）
- 「管理アクセス コントロールの使用」（P.16-14）
- 「管理者パスワードのリセット」（P.16-22）
- 「管理者パスワードの変更」（P.16-22）

管理者ロールおよびアカウントについて

ACS 5.4 に初めてログインすると、事前定義済みの管理者ユーザ名（*ACSAdmin*）の入力を要求するプロンプトが表示され、事前定義済みのパスワード名（*default*）を変更することを要求されます。

（注）　ACSAdmin アカウントは名前を変更したり、ディセーブルにしたり、削除したりできません。

パスワードを変更したあと、システムの設定を開始できます。事前定義済みの管理者には、すべての ACS リソースに対するスーパー管理者権限（Create、Read、Update、Delete、および eXecute（CRUDX））があります。

きめ細かなアクセス コントロールが必要ない場合は、Super Admin ロールが最も便利です。このロールは、事前定義済みの ACSAdmin アカウントに割り当てられています。

きめ細かなアクセス コントロールを行うには、次の手順を実行します。

1. 管理者を定義します。「システム管理者およびアカウントの設定」（P.16-3）を参照してください。
2. 管理者にロールを関連付けます。「ロールについて」（P.16-3）を参照してください。

これらの手順が完了すると、定義された管理者はシステムにログインして操作を開始できます。

認証について

認証要求は、すべての管理セッションに対して最初に行われる処理です。認証に失敗すると、管理セッションが終了します。認証に成功した場合、管理セッションは管理者がログアウトするかセッションがタイムアウトするまで継続します。

ACS 5.4 では、ユーザ資格情報（ユーザ名とパスワード）を使用してすべてのログイン操作を認証します。その後、ACS では、管理者とロールの定義を使用して、適切な権限を取得し、後続の認可要求に対応します。

ACS ユーザ インターフェイスには、必要な管理者特権を持っている機能とオプションだけが表示されます。

（注）　システムの変更が反映されるように、しばらく待ってから再度ログインしてください。

関連トピック

- 「管理者ロールおよびアカウントについて」（P.16-2）
- 「システム管理者およびアカウントの設定」（P.16-3）

システム管理者およびアカウントの設定

ここでは、次の内容について説明します。

- ロールについて
- 管理者アカウントとロールの関連付け
- 管理者アカウントの作成、複製、編集、および削除
- ロール プロパティの表示

ロールについて

ロールは一般的な管理者タスクで構成され、それぞれのタスクに権限のセットが関連付けられています。各管理者には複数の事前定義済みのロールを指定でき、1 つのロールを複数の管理者に適用できます。これにより、1 人の管理者に複数のタスクを設定したり、1 つのタスクに複数の管理者を設定したりできます。

ロールを割り当てるには、[Administrator Accounts] ページを使用します。一般的に、最初に正確にロールを定義しておくことを推奨します。詳細は「管理者アカウントの作成、複製、編集、および削除」（P.16-7）を参照してください。

ロールの割り当て

内部管理者アカウントにロールを割り当てることができます。ACS 5.4 には、内部管理者にロールを割り当てるために、以下の 2 通りの方法が用意されています。

- 静的ロール割り当て：ロールは、内部管理者アカウントに手動で割り当てられます。

- 動的ロール割り当て：ロールは、AAC 認可ポリシーの規則に基づいて割り当てられます。

静的ロールの割り当て

ACS 5.4 では、内部管理者アカウントに管理者ロールを静的に割り当てることができます。これは内部管理者アカウントにのみ適用されます。この静的オプションを選択した場合は、それぞれの内部管理者アカウントには管理者ロールを手動で選択する必要があります。管理者がアカウントにアクセスしようとした場合に、その管理者が静的ロール割り当てとともに管理者内部 ID ストアに設定されていると、ID ポリシーだけが認証で実行されます。認可ポリシーはスキップされます。ID ポリシーが正常に実行された後で、管理者には管理者アカウント用に選択されたロールが割り当てられます。

動的ロールの割り当て

ACS 5.4 では、内部管理者アカウントに管理者ロールを静的に割り当てることができます。

管理者アカウントが外部または内部 ID ストアに設定され、かつ動的ロール割り当てがある場合、ACS は、認可ポリシーを評価し、その結果として、管理者ロールのリストを取得して動的に使用するか、[Deny Access] を使用します。スーパー管理者が管理者に動的ロールを割り当て、認可ポリシーを設定しない場合、その管理者アカウントの認可はデフォルト値「deny access」を使用します。その結果、この管理者アカウントの認可は拒否されます。ただし、管理者に静的ロールを割り当てると、認可ポリシーは、その管理者の認可にまったく影響しません。

選択したロールに基づいて、ACS は認証を行い、管理者のアクセス制限と認証を管理します。Deny Access が評価の結果である場合、ACS は管理者へのアクセスを拒否し、カスタマー ログに失敗の理由を記録します。

（注） ACS Web ユーザ インターフェイスには、自分が特権を持っている機能だけが表示されます。たとえば、ロールが Network Device Admin の場合、[System Administration] ドロワは表示されません。これは、そのドロワ内の機能に対する権限がないためです。

権限

権限は、特定の管理タスクに適用されるアクセス権です。権限の構成要素は次のとおりです。

- **リソース**：管理者がアクセスできる ACS コンポーネント（ネットワーク リソース、ポリシー要素など）のリスト。
- **特権**：特権には、Create、Read、Update、Delete、および eXecute（CRUDX）があります。特定のリソースに適用できない特権もあります。たとえば、ユーザ リソースは実行できません。

特権のない管理者にリソースを割り当てても、その管理者はリソースにアクセスできません。また、権限は独立しています。Create、Update、および Delete 特権がリソースに適用されている場合、Read 特権は使用できません。

オブジェクトに権限が定義されていない場合、管理者はこのオブジェクトにアクセスできず、読み取ることもできません。

（注） 権限は変更できません。

事前定義済みのロール

表 16-1 に、ACS の事前定義済みのロールを示します。

表 16-1　事前定義済みのロールの説明

ロール	権限
ChangeAdminPassword	このロールは、他の管理者アカウントを管理する ACS 管理者用です。このロールが割り当てられた管理者は、他の管理者のパスワードを変更できます。
ChangeUserPassword	このロールは、内部ユーザ アカウントを管理する ACS 管理者用です。このロールが割り当てられた管理者は、内部ユーザのパスワードを変更できます。
NetworkDeviceAdmin	このロールは、デバイスの追加、更新、削除など、ACS ネットワーク デバイス リポジトリの管理だけを実行する必要がある ACS 管理者用です。このロールには、次の権限があります。 • ネットワーク デバイスに対する読み取りおよび書き込み権限 • NDG および [Network Resources] ドロワ内のすべてのオブジェクト タイプに対する読み取りおよび書き込み権限
PolicyAdmin	このロールは、ACS アクセス サービスとアクセス ポリシー規則、およびポリシー規則によって参照されるポリシー要素を作成および管理する ACS ポリシー管理者用です。このロールには、次の権限があります。 • ポリシーで使用されているすべての要素（認可プロファイル、NDG、IDG、条件など）に対する読み取りおよび書き込み権限 • サービス ポリシーに対する読み取りおよび書き込み権限
ReadOnlyAdmin	このロールは、ACS ユーザ インターフェイスのすべての部分に対する読み取り専用アクセスを必要とする ACS 管理者用です。 このロールには、すべてのリソースに対する読み取り専用アクセス権があります。
ReportAdmin	このロールは、ACS Monitoring and Report Viewer にアクセスしてレポートまたはモニタリング データだけを生成および表示する必要がある管理者用です。 このロールには、ログに対する読み取り専用アクセス権があります。
SecurityAdmin	このロールは、ACS 管理者アカウントの作成、更新、または削除、管理ロールの割り当て、および ACS パスワード ポリシーの変更を行うために必要です。このロールには、次の権限があります。 • 内部プロトコル ユーザおよび管理者パスワード ポリシーに対する読み取りおよび書き込み権限 • 管理者アカウント設定に対する読み取りおよび書き込み権限 • 管理者アクセス設定に対する読み取りおよび書き込み権限
SuperAdmin	Super Admin ロールには、すべての ACS 管理機能に対する完全なアクセス権があります。きめ細かなアクセス コントロールが必要ない場合は、このロールが最も便利です。このロールは、事前定義済みの *ACSAdmin* アカウントに割り当てられています。 このロールには、すべてのリソースに対する Create、Read、Update、Delete、および eXecute（CRUDX）権限があります。

表 16-1　事前定義済みのロールの説明 （続き）

ロール	権限
SystemAdmin	このロールは、ACS システムの設定と操作を行う管理者用です。このロールには、次の権限があります。 • アカウント定義を除くすべてのシステム管理アクティビティに対する読み取りおよび書き込み権限 • ACS インスタンスに対する読み取りおよび書き込み権限
UserAdmin	このロールは、内部ユーザや内部ホストなど、内部 ACS ID ストア内のエントリを追加、更新、または削除する管理者用です。このロールには、次の権限があります。 • ユーザとホストに対する読み取りおよび書き込み権限 • IDG に対する読み取り権限

（注）　最初のログイン時には、特定の管理者に Super Admin だけが割り当てられています。

関連トピック

- 管理者アカウントとロールの関連付け
- 管理者アカウントの作成、複製、編集、および削除

ロールの関連付けの変更

ACS のすべてのロールは、事前に定義される設計になっており、変更できません。ACS では、ロールの関連付けだけを変更できます。ロールの関連付けを変更する特権は、システム全体の認可ステータスに悪影響を及ぼす可能性があるため、ACS の Super Admin ロールと SecurityAdmin ロールにだけ割り当てられています。

ロールの関連付けの変更は、影響を受ける管理者がログアウトし、再度ログインしたあとで初めて有効になります。新たにログインするとき、ACS によってロールの関連付けの変更が読み取られ、適用されます。

（注）　ロールの関連付けの変更はグローバルに影響するため、ACS の Super Admin ロールと SecurityAdmin ロールを割り当てる場合は注意が必要です。

管理者アカウントとロールの関連付け

管理者アカウントの定義は、名前、ステータス、説明、電子メール アドレス、パスワード、およびロールの割り当てで構成されています。

（注）　ユーザごとに固有の管理者を作成することを推奨します。これにより、操作が監査ログに明確に記録されます。

管理者は、内部データベースに対してだけ認証されます。

既存のアカウントを編集および削除できます。ただし、最後のスーパー管理者を削除またはディセーブルにしようとすると、Web インターフェイスにエラー メッセージが表示されます。

ID や証明書は、適切な管理者だけが設定できます。[System Administration] ドロワで設定された ID は [Users and Identity Stores] ドロワで使用できますが、変更はできません。

新しい管理者を作成した場合は、パスワード タイプに ID ストアのタイプを選択できます。新しい管理者はこのパスワード タイプに基づいて認証されます。パスワード タイプにできるのは、内部管理者、AD、LDAP です。すべての既存の管理者のデフォルト値は `AdminsIDStore` です。パスワード タイプには、管理者アカウントと ID ストアとの間に関連付けを作成するために定義された新しい関連付けがあります。内部管理者の認証中に、管理者が内部データベースに存在する場合は、パスワード タイプ フィールドの値が読み込まれ属性リストに入力されます。この属性値が `AdminsIDStore` に等しくなければ、認証はパスワード タイプ フィールドで設定した値に基づいて LDAP または AD の ID ストアにルーティングされます。AD および LDAP に対して管理者を認証するために ACS は PAP 認証を使用します。

リカバリ管理者アカウント

ACS 5.4 ではシステム管理者がリカバリ アカウントとして少なくとも 1 つの管理者アカウントを保持する必要があります。アカウントがリカバリ アカウントとして設定されていると、ACS はその特定の管理者を認証するために管理者 ID ポリシーおよび認可ポリシーをバイパスします。このリカバリ管理者アカウントは管理者内部 ID ストアに対して認証されます。リカバリ アカウントを使用して ACS にアクセスしようとすると、内部管理者ユーザに対して認証され、ロールは静的に割り当てられます。複数のリカバリ アカウントを持つことができます。デフォルトでは、Super Admin アカウントはリカバアカウントとして設定されます。新しい管理者アカウントを作成すると、ACS によってそのアカウントはリカバリ アカウントとして設定されませんが、アカウント設定でリカバリ アカウントとして設定する必要があります。

リカバリ アカウントとして管理者アカウントを設定するには、次の操作を実行する必要があります。

- 管理者アカウントに静的ロールを割り当てます。
- 管理者アカウントに Super Admin ロールを割り当てます。
- パスワード タイプを使用して管理者アカウントに外部 ID ストアを設定しないでください。

関連トピック

- ロールについて
- 管理者アカウントの作成、複製、編集、および削除

管理者アカウントの作成、複製、編集、および削除

管理者アカウントを作成、複製、編集、または削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrators] > [Accounts] を選択します。

表 16-2 で説明されている設定済み管理者のリストを含む [Administrators] ページが表示されます。

表 16-2　[Accounts] ページ

オプション	説明
Status	この管理者の現在のステータス。 • Enabled：この管理者はアクティブです。 • Disabled：この管理者はアクティブではありません。 ディセーブルになっている管理者アカウントを使用して ACS にログインすることはできません。
Name	管理者の名前。
Role(s)	管理者に割り当てられているロール。
Description	この管理者の説明。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するアカウントの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するアカウントをクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。
- パスワードを変更するアカウントの隣にあるチェックボックスをオンにし、[Change Password] をクリックします。詳細については、「別の管理者のパスワードのリセット」（P.16-23）を参照してください。

（注）　[Duplicate] ページでは、少なくとも [Admin Name] を変更する必要があります。

- 削除するアカウントの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

ステップ 3　表 16-3 の説明に従って、[Administrator Accounts Properties] ページのフィールドに入力します。

表 16-3　[Administrator Accounts Properties] ページ

オプション	説明
General	
Admin Name	この管理者に設定されている名前。規則を複製する場合は、必ず固有の名前を入力してください。
Status	[Status] ドロップダウン メニューから、アカウントをイネーブルにするかディセーブルにするかを選択します。このオプションは、[Account never disabled] チェックボックスをオンにした場合はディセーブルになっています。
Description	この管理者の説明。
Email Address	管理者の電子メール アドレス。ACS View によって、この電子メール アドレスに警告が送信されます。
Recovery Account	リカバリ アカウントとしてアカウントを設定するには、このオプションをオンにします。このオプションが使用されると、ACS は、管理者 ID ポリシーおよび認可ポリシーをバイパスして、管理者を認証します。詳細については、「リカバリ管理者アカウント」（P.16-7）を参照してください。

表 16-3　[Administrator Accounts Properties] ページ （続き）

オプション	説明
Account never disabled	アカウントをディセーブルにしない場合にオンにします。アカウントは、次の場合にもディセーブルになりません。 • パスワードが失効した場合 • アカウントが非アクティブになった場合 • 指定されたログイン試行回数を超えた場合
Authentication Information	
Password Type	設定されている外部 ID ストア名および内部管理者（デフォルトのパスワード タイプ）を表示します（AD、LDAP のみ）。リストから任意の ID ストアを選択できます。 管理者の認証中に、外部 ID ストアが管理者に設定されている場合、内部 ID ストアは設定されている外部 ID ストアに認証要求を転送します。 外部 ID ストアが選択された場合、管理者のパスワードを設定できません。パスワード編集ボックスはディセーブルです。 パスワード タイプの外部 ID ストアとして ID 順序を使用することはできません。 [System Administration] > [Administrators] > [Accounts] ページにある [Change Password] ボタンを使用してパスワード タイプを変更できます。
Password	認証パスワード。
Confirm Password	認証パスワードの確認。
Change password on next login	次回のログイン時にユーザに新しいパスワードの入力を求める場合にオンにします。
Role Assignment	
Available Roles	設定されているすべてのロールのリスト。この管理者に割り当てるロールを選択し、[>] をクリックします。この管理者にすべてのロールを割り当てる場合は、[>>] をクリックします。
Assigned Roles	この管理者に適用されるロール。

ステップ 4　[Submit] をクリックします。

新しいアカウントが保存されます。作成または複製した新しいアカウントを含む [Administrators] ページが表示されます。

関連トピック

- 「ロールについて」（P.16-3）
- 「管理者アカウントとロールの関連付け」（P.16-6）
- 「事前定義済みのロールの表示」（P.16-9）
- 「管理者の認証設定」（P.16-10）

事前定義済みのロールの表示

ACS の事前定義済みのロールについては、表 16-1 を参照してください。

事前定義済みのロールを表示するには、次の手順を実行します。

[System Administration] > [Administrators] > [Roles] を選択します。

事前定義済みのロールのリストを含む [Roles] ページが表示されます。表 16-4 に、[Roles] ページのフィールドを示します。

表 16-4　[Roles] ページ

フィールド	説明
Name	設定されているすべてのロールのリスト。事前定義済みのロールのリストについては、「事前定義済みのロール」（P.16-5）を参照してください。
Description	各ロールの説明。

ロール プロパティの表示

このページは、各ロールのプロパティを表示する場合に使用します。

[System Administration] > [Administrators] > [Roles] を選択し、ロールをクリックするか、またはロールのオプション ボタンを選択して [View] をクリックします。

表 16-5 で説明されている [Roles Properties] ページが表示されます。

表 16-5　[Roles Properties] ページ

フィールド	説明
Name	ロールの名前。ロールを複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。ロールは作成または編集できません。事前定義済みのロールのリストについては、表 16-4 を参照してください。
Description	ロールの説明。詳細については、「事前定義済みのロール」（P.16-5）を参照してください。
Permissions List	
Resource	使用可能なリソースのリスト。
Privileges	各リソースに割り当てることができる特権。特権が適用されない場合、特権のチェックボックスは選択できません（使用できません）。 行の色は、特定の特権が使用可能かどうかとは関係ありません。[Privileges] カラムの明示的なテキストによって決まります。

関連トピック

- 「ロールについて」（P.16-3）
- 「管理者アカウントとロールの関連付け」（P.16-6）
- 「管理者の認証設定」（P.16-10）

管理者の認証設定

認証設定は、管理者に強力なパスワードの使用や定期的なパスワードの変更などを強制することによって、セキュリティを強化する規則のセットです。パスワード ポリシーの変更は、すべての ACS システム管理者アカウントに適用されます。

パスワード ポリシーを設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrators] > [Settings] > [Authentication] を選択します。

[Password Complexity] タブと [Advanced] タブを含む [Password Policies] ページが表示されます。

ステップ 2　[Password Complexity] タブで、管理者パスワードの設定に使用する各チェックボックスをオンにします。

表 16-6 に、[Password Complexity] タブのフィールドを示します。

表 16-6　[Password Complexity] タブ

オプション	説明
Applies to all ACS system administrator accounts	
Minimum length	必要な最小長。有効なオプションは 4 ～ 20 です。
Password may not contain the username or its characters in reversed order	パスワードにユーザ名または逆順のユーザ名を含めることができないことを指定する場合にオンにします。たとえば、ユーザ名が john の場合、パスワードを john または nhoj にすることはできません。
Password may not contain 'cisco' or its characters in reversed order	パスワードに *cisco* という単語またはその逆順の文字列（つまり *ocsic*）を含めることができないことを指定する場合にオンにします。
Password may not contain '' or its characters in reversed order	パスワードに、入力した文字列またはその逆順の文字列を含めることができないことを指定する場合にオンにします。たとえば、文字列 polly を指定した場合、パスワードを polly または yllop にすることはできません。
Password may not contain repeated characters four or more times consecutively	パスワードで文字を 4 回以上連続して繰り返すことができないことを指定する場合にオンにします。たとえば、パスワードとして apppple を使用できません。これは、文字 p が 4 回連続して使用されているためです。
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	パスワードには、アルファベットの小文字が少なくとも 1 文字含まれている必要があります。
Upper case alphabetic characters	パスワードには、アルファベットの大文字が少なくとも 1 文字含まれている必要があります。
Numeric characters	パスワードには、数字が少なくとも 1 文字含まれている必要があります。
Non alphanumeric characters	パスワードには、英数字以外の文字が少なくとも 1 文字含まれている必要があります。

ステップ 3　[Advanced] タブで、管理者の認証プロセスに設定する基準の値を入力します。

表 16-7 に、[Advanced] タブのフィールドを示します。

表 16-7　[Advanced] タブ

オプション	説明
Password History	
Password must be different from the previous *n* versions	比較対象となる、この管理者の旧パスワードの数を指定します。このオプションを指定すると、管理者は最近使用したパスワードを設定できなくなります。有効なオプションは 1 ～ 99 です。
[Password Lifetime]：管理者は定期的にパスワードを変更する必要があります	
Display reminder after *n* days	パスワード変更の通知を *n* 日後に表示します。有効なオプションは 1 ～ 365 です。このオプションを設定すると、通知だけが表示されます。新しいパスワードは要求されません。

表 16-7　[Advanced] タブ （続き）

オプション	説明
Require a password change after *n* days	パスワードを *n* 日後に変更する必要があることを指定します。有効なオプションは 1 ～ 365 です。このオプションを設定すると、n 日後にパスワードを変更する必要があります。
Disable administrator account after *n* days if password is not changed	パスワードが変更されていない場合に、管理者アカウントを *n* 日後にディセーブルにする必要があることを指定します。有効なオプションは 1 ～ 365 です。 ACS では、[Display reminder after *n* days] オプションを設定しないでこのオプションを設定することはできません。
Account Inactivity	
Inactive accounts are disabled	
Require a password change after *n* days of inactivity	アカウントが非アクティブになってから *n* 日後にパスワードを変更する必要があることを指定します。有効なオプションは 1 ～ 365 です。このオプションを設定すると、*n* 日後にパスワードを変更する必要があります。 ACS では、[Display reminder after *n* days] オプションを設定しないでこのオプションを設定することはできません。
Disable administrator account after *n* days of inactivity	管理者アカウントが非アクティブになってから *n* 日後にそのアカウントをディセーブルにする必要があることを指定します。有効なオプションは 1 ～ 365 です。 ACS では、[Display reminder after *n* days] オプションを設定しないでこのオプションを設定することはできません。
Incorrect Password Attempts	
Disable account after *n* successive failed attempts	最大ログイン試行回数を指定します。この回数を超えると、アカウントはディセーブルになります。有効なオプションは 1 ～ 10 です。

（注）　ACS は、最後のログイン、最後のパスワード変更、またはログイン試行回数に基づいてアカウントを自動的に無効またはディセーブルにします。CLI および PI ユーザ アカウントはブロックされ、Web インターフェイスからパスワードを変更できるという内容の通知を受信します。アカウントがディセーブルになっている場合は、アカウントをイネーブルにするよう、別の管理者に依頼します。

ステップ 4　[Submit] をクリックします。

管理者パスワードに定義された基準が設定されます。これらの基準は、以降のログインだけに適用されます。

関連トピック

- 「ロールについて」（P.16-3）
- 「管理者アカウントとロールの関連付け」（P.16-6）
- 「事前定義済みのロールの表示」（P.16-9）

セッション アイドル タイムアウトの設定

デフォルトでは、GUI セッションには 30 分のタイムアウト時間が割り当てられます。タイムアウト時間は、5 ～ 90 分の範囲で指定できます。

タイムアウト時間を設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrators] > [Settings] > [Session] を選択します。

[GUI Session] ページが表示されます。

ステップ 2　[Session Idle Timeout] の値を分単位で入力します。有効な値は 5 ～ 90 分です。

ステップ 3　[Submit] をクリックします。

（注）　CLI クライアント インターフェイスには、6 時間のデフォルトのセッション タイムアウト値が設定されています。CLI クライアント インターフェイスではセッション タイムアウト時間を設定できません。

管理者アクセスの設定

ACS 5.4 では、リモート クライアントの IP アドレスに基づいて ACS への管理アクセスを制限できます。次のいずれかの方法で IP アドレスをフィルタリングできます。

- 「すべての IP アドレスに接続を許可する」（P.16-13）
- 「IP アドレスの選択リストからのリモート管理を許可する」（P.16-13）
- 「IP アドレスの選択リストからのリモート管理を拒否する」（P.16-14）

すべての IP アドレスに接続を許可する

[Allow all IP addresses to connect] オプションを選択すると、すべての接続を許可できます。これがデフォルトのオプションです。

IP アドレスの選択リストからのリモート管理を許可する

管理者に ACS へのリモート アクセスを許可するには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrators] > [Settings] > [Access] を選択します。

[IP Addresses Filtering] ページが表示されます。

ステップ 2　[Allow only listed IP addresses to connect] オプション ボタンをクリックします。

[IP Range(s)] 領域が表示されます。

ステップ 3　[IP Range(s)] 領域で [Create] をクリックします。

新しいウィンドウが表示されます。ACS へのリモート アクセスを許可するマシンの IPv4 または IPv6 アドレスを入力します。IP アドレス範囲全体のサブネット マスクを入力します。ACS は、入力されたアドレスが IPv4 または IPv6 でサポートされる形式であるかどうかを確認します。

ステップ 4　[OK] をクリックします。

[IP Range(s)] 領域に IP アドレスが読み込まれます。ステップ 3 を繰り返して、リモート アクセスを許可する他の IP アドレスまたは範囲を追加します。

ステップ 5　[Submit] をクリックします。

IP アドレスの選択リストからのリモート管理を拒否する

管理者による ACS へのリモート アクセスを拒否するには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrators] > [Settings] > [Access] を選択します。

[IP Addresses Filtering] ページが表示されます。

ステップ 2　[Reject connections from listed IP addresses] オプション ボタンをクリックします。

[IP Range(s)] 領域が表示されます。

ステップ 3　[IP Range(s)] 領域で [Create] をクリックします。

新しいウィンドウが表示されます。

ステップ 4　ACS へのリモート アクセスを許可しないマシンの IP アドレスを入力します。IP アドレス範囲全体のサブネット マスクを入力します。

ステップ 5　[OK] をクリックします。

[IP Range(s)] 領域に IP アドレスが読み込まれます。ステップ 3 を繰り返して、拒否する他の IP アドレスまたは範囲を追加します。

ステップ 6　[Submit] をクリックします。

（注）　すべての IP アドレスからの接続を拒否できます。この設定は、ACS Web インターフェイスではリセットできません。ただし、次の CLI コマンドを使用できます。

```
acs reset-password
```

詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

管理アクセス コントロールの使用

ACS 5.4 では、管理アクセス コントロール（AAC）サービスという新しいサービス タイプが導入されています。AAC サービスは、ACS 管理者の認証と認可を扱います。

拡張 AAC Web インターフェイスは次のとおりです。

- ポリシーベースの認証および認可
- 外部データベースに対する認証は次で実行可能です。
  - 内部 ID ストア管理者の管理者アカウントのパスワード タイプ。
  - 外部データベースと照合する ID ポリシー（認証ポリシー）の設定。

この AAC サービスは、インストール時に自動的に作成されます。新しい AAC サービスの削除または追加はできません。AAC はサービス セレクション ポリシーでは使用できず、管理者ログイン時に自動的に選択されます。

AAC サービスでは、管理者ログインのための一連のポリシーを識別します。AAC サービス内で提供されるポリシーは次のとおりです。

- 管理者 ID ポリシーは管理者の認証に使用される ID データベースを決定し、以降の認可ポリシーで使用される可能性のある管理者の属性の取得も行います。
- 管理者認可ポリシーは、ACS のセッションの管理者のロールを決定します。割り当てられたロールによって、管理者の権限が決定されます。各ロールに権限の事前定義リストがあります。それはロール ページで見ることができます。

AAC サービスがこれら 2 つのポリシーを順番に処理します。管理者 ID ポリシーおよび管理者認可ポリシーの両方を設定する必要があります。両方のポリシーのデフォルトは次のとおりです。

ID ポリシー：デフォルトは、[Internal Identity Store] です。

認可ポリシー：デフォルトは [Deny Access] です。

AAC サービスは PAP 認証タイプだけをサポートします。Super Admin のみが管理者アクセス コントロールを設定することを許可されます。

ACS アプリケーションを ACS 5.4 にアップグレードする場合は、AAC は次の変更を実施します。

- 単一 AAC サービスは、アップグレード時に自動的に作成されます。
- AAC サービスの ID ポリシーは、[Administrators Internal Identity Store] に設定されます。
- すべての既存の管理者は静的ロール割り当てで検証されます。
- Super Admin ロールを持つすべての管理者はリカバリ アカウントとして自動的に設定されます。

5.4 に ACS アプリケーションをアップグレードした後で、管理者アカウントを更新しないと、アップグレードされた管理者アカウントは管理者内部 ID ストアに対して認証され、静的割り当てによりロールを取得します。アップグレード時にバックアップを復元すると、ACS 5.4 はスキーマ ファイルとデータのアップグレードを処理します。

ここでは、次の内容について説明します。

- 「管理者 ID ポリシー」（P.16-15）
- 「管理者認可ポリシー」（P.16-19）

管理者 ID ポリシー

管理アクセス コントロールの ID ポリシーでは、ACS で認証と属性の取得に使用する ID ソースを定義します。グループおよび属性は、外部データベースからのみ取得できます。ACS は、取得した属性をその後の認可ポリシーでのみ使用できます。

AAC サービスは次の 2 種類の ID ポリシーをサポートします。その内容は次のとおりです。

- 単一結果選択
- ルール ベース結果選択

Super Admin は、このポリシーを設定および変更できます。すべての要求の認証に同じ ID ソースを適用する単純なポリシー、またはルール ベースの ID ポリシーを設定できます。

単純なポリシーでサポートされる識別方法は次のとおりです。

- アクセス拒否：ユーザへのアクセスは拒否され、認証は実行されません。
- ID ストア：単一の ID ストア。

  次の ID ストアのいずれかを選択できます。

  - 内部管理者 ID ストア

- Active Directory ID ストア
- LDAP ID ストア

[Deny Access] が結果として選択されている場合、管理者のアクセスは拒否されます。

ルール ベースのポリシーでは、各規則に 1 つ以上の条件、および認証に使用される ID ソースである結果が含まれます。

サポートされる条件は次のとおりです。

- システム ユーザ名
- システムの日付と時刻
- 管理者クライアント IP アドレス

AAC サービスの ID ポリシーは結果として ID ストア順序をサポートしません。ID ポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。

注意　単純なポリシー ページとルール ベースのポリシー ページを切り替えると、以前に保存したポリシー設定は失われます。

単純な ID ポリシーを設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrative Access Control] > [Identity] を選択します。

デフォルトでは、表 16-8 で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。

表 16-8　[Simple Identity Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple] : 結果がすべての要求に適用されることを指定します。 • [Rule-based] : 要求に応じて異なる結果が適用されるように規則を設定します。 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Identity Source	すべての要求に適用する ID ソース。デフォルトは [Deny Access] です。パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。

ステップ 2　認証用の ID ソースを選択するか、または [Deny Access] を選択します。

ステップ 3　[Save Changes] を選択して、ポリシーを保存します。

ルール ベースの ID ポリシーの表示

[System Administration] > [Administrative Access Control] > [Identity] を選択します。

デフォルトでは、表 16-8 で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。設定されている場合は、表 16-9 で説明されているフィールドを含む [Rule-Based Identity Policy] ページが表示されます。

表 16-9　[Rule-Based Identity Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 • [Simple]：結果がすべての要求に適用されることを指定します。 • [Rule-based]：要求に応じて異なる結果が適用されるように規則を設定します。 **注意**　ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Status	規則の現在のステータス。規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	ポリシーの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。
Results	規則の評価結果として認証に使用される ID ソース。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

ルール ベースのポリシーを設定するには、次の項を参照してください。

- 「ポリシー規則の作成」（P.10-38）
- 「規則の複製」（P.10-39）
- 「ポリシー規則の編集」（P.10-39）
- 「ポリシー規則の削除」（P.10-40）

ID ポリシー規則のプロパティの設定

ID ポリシー規則を作成、複製、または編集して、管理者の認証に使用する ID データベースを決定したり、管理者の属性を取得したりできます。属性の検索は、外部データベースを使用する場合だけ可能です。

このページを表示するには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrative Access Control] > [Identity] を選択し、次のいずれかを実行します。

- [Create] をクリックします。
- 規則チェックボックスをオンにし、[Duplicate] をクリックします。
- 規則名をクリックするか規則チェックボックスをオンにし、[Edit] をクリックします。

ステップ 2　表 16-10 の説明に従って、[Identity Rule Properties] ページのフィールドに入力します。

表 16-10　[Identity Rule Properties] ページ

オプション	説明
General	
Rule Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Rule Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[*ANY*] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。
Results	
Identity Source	要求に適用する ID ソース。デフォルトは管理者内部 ID ストアです。パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。

管理者認可ポリシー

管理アクセス コントロールの認可ポリシーはログイン時に管理者に動的にロールを割り当てるために使用されます。管理者のロールは、ポリシーで定義された規則に従って設定されます。ポリシーに定義されている規則に従って、条件には、外部データベースで認証されるときにグループおよび属性を含めることができます。ACS は、取得した属性をその後のポリシーで使用できます。

認可ポリシー ベースのロール割り当ては内部および外部管理者アカウントの両方に適用されます。外部管理者アカウントにロールを割り当てるのに使用可能なこれが唯一の方法です。

管理者認可ポリシーでは、各規則に 1 つ以上の条件があり、認証と結果に使用されます。

サポートされる条件は次のとおりです。

- システム ユーザ名
- システムの日付と時刻
- 管理者クライアント IP アドレス
- AD ディクショナリまたは LDAP ディレクトリ（外部グループおよび属性）

管理者 ID ポリシーおよびパスワード タイプ機能により、管理者は Active Directory または LDAP の ID ストアなどの外部 ID ストアの要求を認証し、管理者グループおよび属性を取得することができます。管理者認可ポリシー規則は、次の取得したグループと属性に基づいて設定できます。

管理者に割り当てられる一連の管理者ロールで管理者認可ポリシーの結果を設定できます。

サポートされる認可ポリシーの結果は次のとおりです。

- [Administrator Role Result]：1 つ以上の管理者ロール
- [Deny Access]：認証失敗

認可ポリシー内の規則は、作成、複製、編集、および削除できます。また、規則はイネーブルおよびディセーブルにすることもできます。

管理者認可ポリシーの設定

管理者認可ポリシーは、ACS 管理者のロールを決定します。

AAC アクセス サービスのプロパティ ページの説明については、「アクセス サービスの一般プロパティの設定」（P.10-13）を参照してください。

このページは、次のことを実行する場合に使用します。

- 規則を表示します。
- 規則を削除します。
- 規則を作成、複製、編集、およびカスタマイズできるページを開きます。

[System Administration] > [Administrative Access Control] > [Authorization] > [Standard Policy] を選択します。

表 16-11 で説明されている [Administrator Administration Authorization Policy] ページが表示されます。

表 16-11　[Administrator Authorization Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用される管理者ロールを表示します。 規則の結果をカスタマイズできます。規則は、管理者ロールを適用できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件および結果のタイプを選択する [Customize] ページを開きます。[Conditions] および [Results] カラムには、カスタマイゼーション設定が反映されます。 **注意**　規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。「ヒット カウントの表示」（P.10-9）を参照してください。

管理者認可規則のプロパティの設定

このページは、AAC アクセス サービスの管理者ロールを決定する規則を作成、複製、および編集する場合に使用します。

[System Administration] > [Administrative Access Control] > [Authorization] > [Standard Policy] を選択し、[Create]、[Edit]、[Duplicate] のいずれかをクリックします。

表 16-12 で説明されている [Administrator Authorization Rule Properties] ページが表示されます。

表 16-12　[Administrators Authorization Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Status	規則のステータスは、次のとおりです。 • Enabled：規則はアクティブです。 • Disabled：ACS によって規則の結果は適用されません。 • Monitor：規則はアクティブですが、ACS によって規則の結果は適用されません。ヒット カウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を表示して確認する場合に特に役立ちます。
Conditions	
conditions	これらは、規則に対して設定できる条件です。デフォルトでは、複合条件が表示されます。[Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、「複合条件の設定」（P.10-41）を参照してください。
Results	
Roles	規則に適用されるロール。

管理者のログイン プロセス

管理者が ACS Web インターフェイスにログインすると、ACS 5.4 では、次のように認証を実行します。

管理者アカウントが管理者内部 ID ストアのリカバリ アカウントとして設定されていると、ACS は、ID ポリシーおよび認可ポリシーをバイパスし、管理者内部 ID ストアに対して管理者を認証し、ロールを静的に割り当てます。管理者アカウントがリカバリ アカウントでない場合、ACS はポリシーベースの認証に進みます。

ポリシーベースの認証の一環として、ACS では、ID ポリシーおよび認可ポリシーの設定で AAC サービスを取得します。ACS は、ID ポリシーを評価し、その結果として ID ストアを取得します。ID ポリシーの結果が管理者内部 ID ストアである場合、ACS はパスワードを評価し、結果として ID ストアを取得します。

ACS は、管理者アカウントが外部 ID ストアに設定されている場合に、選択されている ID ストアに対して管理者を認証し、ユーザ グループとユーザ属性を取得します。

管理者アカウントが内部 ID ストアに設定されているときに、静的ロール割り当てがある場合は、ACS は管理者ロールのリストを抽出します。

管理者アカウントが、外部または内部 ID ストアに設定されているときに、動的ロール割り当てがある場合は、ACS は、認可ポリシーを評価して、管理者ロールのリストを取得し、それを動的に使用するか、結果として [Deny Access] を取得します。

選択したロールに基づいて、ACS は認証を行い、管理者のアクセス制限と認証を管理します。Deny Access が評価の結果である場合、ACS は管理者へのアクセスを拒否し、カスタマー ログに失敗の理由を記録します。

（注）　AD または LDAP サーバの管理者パスワードが期限切れまたはリセットの場合、ACS は Web インターフェイスへの管理者アクセスを拒否します。

管理者パスワードのリセット

管理者アクセスの設定中、すべての管理者アカウントがロックアウトされ、管理者が企業内のいずれの IP アドレスからも ACS にアクセスできなくなる場合があります。この場合、ACS Config CLI から管理者パスワードをリセットする必要があります。すべての管理者パスワードをリセットするには、次のコマンドを使用する必要があります。

access-setting accept-all

このコマンドの詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli_app_a.html#wp1893005

（注）　ACS Web インターフェイスでは管理者パスワードをリセットできません。

管理者パスワードの変更

ACS 5.4 には、新しい Change Admin Password というロールが導入されました。このロールが割り当てられた管理者は、別の管理者のパスワードを変更できます。管理者のアカウントがディセーブルになっている場合、Change Admin Password ロールが割り当てられている他の管理者は、ACS Web インターフェイスからディセーブルになっているアカウントをリセットできます。ここでは、次の内容について説明します。

- 「自分の管理者パスワードの変更」（P.16-22）
- 「別の管理者のパスワードのリセット」（P.16-23）

自分の管理者パスワードの変更

（注）　すべての管理者は、自分のパスワードを変更できます。この操作を実行するのに特別なロールは必要ありません。

パスワードを変更するには、次の手順を実行します。

ステップ 1　[My Workspace] > [My Account] を選択します。

[My Account] ページが表示されます。有効な値については、「[My Account] ページ」（P.5-2）を参照してください。

ステップ 2　[Password field] セクションに、現在の管理者パスワードを入力します。

ステップ 3　[New Password] フィールドに、新しい管理者パスワードを入力します。

ステップ 4　[Confirm Password] フィールドに、新しい管理者パスワードを再入力します。

ステップ 5　[Submit] をクリックします。

管理者パスワードが作成されます。

---

acs reset-password コマンドを使用して ACSAdmin アカウントのパスワードをリセットすることもできます。このコマンドの詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli_app_a.html#wp1887660

別の管理者のパスワードのリセット

別の管理者のパスワードをリセットするには、次の手順を実行します。

ステップ 1　[System Administration] > [Administrators] > [Accounts] を選択します。

管理者アカウントのリストを含む [Accounts] ページが表示されます。

ステップ 2　パスワードを変更する管理者アカウントの隣にあるチェックボックスをオンにし、[Change Password] をクリックします。

[Authentication Information] ページが表示され、管理者のパスワードが最後に変更された日付が示されます。

ステップ 3　[Password] フィールドに、新しい管理者パスワードを入力します。

ステップ 4　[Confirm Password] フィールドに、新しい管理者パスワードを再入力します。

ステップ 5　他の管理者が最初のログイン時にパスワードを変更できるように、[Change password on next login] チェックボックスをオンにします。

ステップ 6　[Submit] をクリックします。

管理者パスワードがリセットされます。

関連トピック

- 「管理者の認証設定」（P.16-10）
- 「ロールについて」（P.16-3）
- 「管理者アカウントとロールの関連付け」（P.16-6）
- 「事前定義済みのロールの表示」（P.16-9）

CHAPTER 17

システムの動作の設定

1 つの ACS インスタンスが*プライマリ インスタンス*になり、他の ACS インスタンスを*セカンダリ インスタンス*として、そのプライマリ インスタンスに登録できるように、ACS インスタンスを設定して展開できます。ACS インスタンスは、ネットワーク上で動作する ACS ソフトウェアに対応付けられます。

ACS の展開は、単一のインスタンスで構成されることも、複数のインスタンスで構成されることもあります。後者の場合、インスタンスは分散環境に展開され、システム内のすべてのインスタンスが集中管理されます。1 つのシステムのすべてのインスタンスに同じ設定が使用されます。

展開のすべてのインスタンスを管理するには、[Distributed System Management] ページ（[System Administration] > [Operations] > [Distributed System Management]）を使用します。インスタンスを管理できるのは、プライマリ インスタンスからだけです。[Deployment Operations] ページは展開内の任意のインスタンスから呼び出すことができますが、その制御対象はローカル サーバ上での動作に限られます。

（注） 任意のプライマリ インスタンスまたは任意のセカンダリ インスタンスを別のプライマリ インスタンスに登録できます。ただし、セカンダリ インスタンスが登録されているプライマリ インスタンスは登録できません。

インストール プロセスの一環として作成されたプライマリ インスタンスで、登録されているセカンダリ インスタンスの設定が集中管理されます。プライマリ インスタンスで行った設定変更は、セカンダリ インスタンスに自動的に複製されます。設定変更がセカンダリ インスタンスに複製されない場合、セカンダリ インスタンスに対して*完全な複製*を強制的に実行できます。

この章の内容は、次のとおりです。

- 「分散展開について」（P.17-2）
- 「スケジューリング バックアップ」（P.17-6）
- 「バックアップ/復元後のプライマリ インスタンスとセカンダリ インスタンスの同期」（P.17-9）
- 「インスタンスの編集」（P.17-9）
- 「セカンダリ インスタンスのアクティベーション」（P.17-14）
- 「プライマリ インスタンスへのセカンダリ インスタンスの登録」（P.17-15）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「[Deployment Operations] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「プライマリ サーバからのプライマリ インスタンスの IP アドレスの変更」（P.17-22）
- 「フェールオーバー」（P.17-23）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの昇格」（P.17-19）

- 「プライマリ インスタンスからのセカンダリ インスタンスの複製」（P.17-20）
- 「[Deployment Operations] ページでのローカル モード インスタンスの作成」（P.17-24）

分散展開について

展開内に複数の ACS サーバを設定できます。どの展開でも、1 つのサーバを *プライマリ* サーバとして指定し、他のサーバはすべて *セカンダリ* サーバになります。

一般的に、設定変更はプライマリ サーバだけで行い、その変更はすべてのセカンダリ サーバに伝播されます。これらのセカンダリ サーバでは、設定データを読み取り専用データとして表示できます。サーバ証明書の設定など、設定変更の数が少ない場合は、セカンダリ サーバで変更できます。これらの変更はサーバにローカルに保持されます。

セカンダリ サーバ間で通信は行われません。通信は、プライマリ サーバとセカンダリ サーバの間でだけ行われます。セカンダリ サーバでは、展開内の他のセカンダリのステータスは認識されません。

ACS を使用すると、ファイアウォールの内側に ACS インスタンスを展開できます。各種管理インターフェイスを介して ACS にアクセスできるようにするために、ファイアウォールで開く必要があるポートを 表 17-1 に示します。

表 17-1　ファイアウォールで開くポート

サービス	ポート
ACS Web インターフェイス /Web サービス	443
データベース複製	TCP 2638
RADIUS サーバ	• 1812 および 1645（RADIUS 認証および認可） • 1813 および 1646（RADIUS アカウンティング） RADIUS サーバでポート 1812 を使用する場合は、PIX ファイアウォール ソフトウェアがバージョン 6.0 以降であることを確認してください。そのあと、次のコマンドを実行して、ポート 1812 を使用するようにします。 **aaa-server radius-authport** *1812*
メッセージ バスを介した複製	TCP 61616
RMI	TCP 2020（RMI レジストリ サービス用）
	TCP 2030（着信コール用）
SNMP（要求用）	UDP 161
SNMP（通知用）	UDP 162
SSH	22
TACACS+ サーバ	TCP 49
コレクタの表示	UDP 20514

[Distributed System Management] ページを使用して、展開内のサーバのステータスを監視したり、サーバ上の操作を実行したりできます。

ACS 5.4 では、大規模な ACS 展開内に 1 つのプライマリ サーバと 20 のセカンダリ サーバをサポートします。中規模な ACS 展開は、1 つのプライマリ サーバおよび 12 のセカンダリ サーバで構成されます。また、すべての ACS 5.4 展開で 100,000 の AAA クライアント、10,000 のネットワーク デバイス グループおよび 150,000 のホストがサポートされます。ACS 5.4 ログ コレクタ サーバは、展開されているさまざまな ACS ノードからログ コレクタ サーバへの送信による負荷に対して、1 日 2,000,000 件のレコード、毎秒 750 件のメッセージを処理できます。ACS サーバの展開の詳細については、http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/installation/guide/csacs_deploy.html を参照してください。

（注）　ACS 5.4 は、21 を超える ACS インスタンスを持つ大規模な展開をサポートしません。

関連トピック

- 「セカンダリ サーバのアクティベーション」（P.17-3）
- 「セカンダリ サーバの削除」（P.17-4）
- 「セカンダリ サーバの昇格」（P.17-4）
- 「ローカル モードについて」（P.17-4）
- 「完全な複製について」（P.17-5）
- 「ハードウェアの置き換えの指定」（P.17-5）

セカンダリ サーバのアクティベーション

展開にサーバを追加するには、次の手順を実行します。

ステップ 1　セカンダリ サーバで、[Deployment Operations] オプションを選択して、プライマリ サーバへの登録要求を発行します。

ステップ 2　プライマリ サーバでセカンダリ インスタンスをアクティブにします。

セカンダリ インスタンスで設定情報を受信できるようにするには、プライマリ インスタンスでセカンダリ インスタンスをアクティブにする必要があります。これにより、アドミッション コントロールのメカニズムが提供されます。

ただし、手動アクティベーション要求を実行する代わりに、新しく追加されたセカンダリ インスタンスを自動的にアクティブにするためのオプションも用意されています。

関連トピック

- 「セカンダリ サーバの削除」（P.17-4）
- 「セカンダリ サーバの昇格」（P.17-4）
- 「ローカル モードについて」（P.17-4）
- 「完全な複製について」（P.17-5）
- 「ハードウェアの置き換えの指定」（P.17-5）

セカンダリ サーバの削除

展開からセカンダリ サーバを完全に削除するには、まずセカンダリ サーバを登録解除してから、プライマリから削除する必要があります。サーバを登録解除するための要求は、登録解除するセカンダリ サーバから実行することも、プライマリ サーバから実行することもできます。

関連トピック

- 「セカンダリ サーバのアクティベーション」（P.17-3）
- 「分散展開について」（P.17-2）

セカンダリ サーバの昇格

プライマリ サーバとして機能できるサーバは 1 つだけです。ただし、セカンダリ サーバを昇格させて、展開内のすべてのサーバに対するプライマリ ロールを代行させることができます。昇格操作は、プライマリ ロールを代行させるセカンダリ サーバで実行するか、またはプライマリ サーバで実行します。

（注） プライマリ サーバがダウンしている場合は、2 つのセカンダリ サーバを同時に昇格させないでください。

関連トピック

- 「セカンダリ サーバのアクティベーション」（P.17-3）
- 「セカンダリ サーバの削除」（P.17-4）
- 「ローカル モードについて」（P.17-4）
- 「完全な複製について」（P.17-5）

ローカル モードについて

次のローカル モード オプションを使用できます。

- セカンダリ サーバからプライマリ サーバに到達できず（たとえば、ネットワークが切断している場合）、セカンダリ サーバに対して設定変更を行う必要がある場合は、セカンダリ サーバを *ローカル モード*にするように指定できます。
- 試験的に、いくつかの設定変更を 1 つのサーバにだけ加え、展開内のすべてのサーバには影響を及ぼさないようにする場合は、セカンダリ サーバの 1 つを *ローカル モード*にするように指定できます。

ローカル モードでは、ローカルの Web インターフェイスを介して単一の ACS インスタンスに変更を加えることができ、その変更は対象のインスタンスだけで有効になります。Monitoring and Report Viewer で使用可能な [Configuration Audit] レポートには、ローカル モードで加えた設定変更だけがレポートされるようにするオプションがあります。

このレポートを生成して、ローカル モードのセカンダリ サーバに加えた変更を記録できます。レポートの詳細、および ACS からレポートを生成する方法の詳細については、第 13 章「レポートの管理」を参照してください。

プライマリ サーバに対する接続が再開したら、切断されているローカル モードのセカンダリ インスタンスをプライマリ サーバに再接続できます。ローカル モードのセカンダリ インスタンスで、プライマリ インスタンスに再接続するための管理ユーザ名とパスワードを指定します。セカンダリ サーバがローカル モードのときに加えた設定変更は、すべて失われます。

関連トピック

- 「セカンダリ サーバのアクティベーション」（P.17-3）
- 「完全な複製について」（P.17-5）

完全な複製について

通常の環境では、各設定変更がすべてのセカンダリ インスタンスに伝播されます。完全な複製が実行されていた ACS 4.x とは異なり、ACS 5.4 では特定の変更だけが伝播されます。設定変更が実行されると、管理者は、（[Distributed System Management] ページで）複製のステータスと最後の複製 ID を監視して、セカンダリ サーバが最新の状態であることを確認できるようになります。

設定変更が期待どおりに複製されていない場合、管理者はサーバに対して完全な複製を要求できます。完全な複製を要求すると、設定データの完全なセットがセカンダリ サーバに転送され、セカンダリ サーバ上の設定データが再同期されます。

（注） メッセージ バスでの複製は、TCP ポート 61616 を使用して実行されます。完全な複製は、Sybase DB TCP ポート 2638 を使用して実行されます。

警告 **ACS 管理サービスは、接続に失敗したときに警告メッセージが表示された場合でも開始されます。サービスは初期化段階で膠着状態になることはありません。**

関連トピック

- 「セカンダリ サーバのアクティベーション」（P.17-3）
- 「セカンダリ サーバの昇格」（P.17-4）
- 「ローカル モードについて」（P.17-4）

ハードウェアの置き換えの指定

ハードウェアの置き換えを実行して、新規または既存の ACS インスタンス ハードウェアをプライマリ サーバに再登録し、プライマリ サーバ上の既存の設定が引き継がれるようにできます。このことは、ACS インスタンスで障害が発生し、物理的な置き換えが必要となった場合に役立ちます。

ハードウェアの置き換えを行うには、次の手順を実行します。

ステップ 1　プライマリ インスタンスの Web インターフェイスで、置き換え対象のサーバを登録解除済みとしてマークする必要があります。

ステップ 2　セカンダリ サーバからプライマリ サーバに登録します。

プライマリ サーバに接続するための標準管理クレデンシャル（ユーザ名 / パスワード）に加え、プライマリ サーバで設定を識別するために使用される置き換えキーワードを指定する必要があります。キーワードは、置き換え対象のインスタンスのホスト名です。

ステップ 3　プライマリでセカンダリ サーバを自動的にアクティブにするか、または手動要求を発行してアクティブにする必要があります。

関連トピック

- 「プライマリ インスタンスの表示および編集」（P.17-10）
- 「セカンダリ インスタンスの表示および編集」（P.17-13）
- 「セカンダリ インスタンスのアクティベーション」（P.17-14）
- 「プライマリ インスタンスへのセカンダリ インスタンスの登録」（P.17-15）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの昇格」（P.17-19）
- 「[Deployment Operations] ページでのローカル モード インスタンスの作成」（P.17-24）

スケジューリング バックアップ

バックアップを定期的に実行するようにスケジューリングできます。バックアップをスケジューリングするには、プライマリ Web インターフェイスまたはローカルの CLI を使用します。スケジューリング バックアップ機能では、ACS 設定データがバックアップされます。

以前のバージョンの ACS のデータをバックアップして、後続のバージョンに復元できます。

ACS を後続のバージョンにアップグレードする方法の詳細については、『*Installation and Setup Guide for Cisco Secure Access Control System 5.4*』を参照してください。

関連項目

「スケジューリング バックアップの作成、複製、および編集」（P.17-6）

スケジューリング バックアップの作成、複製、および編集

スケジューリング バックアップは、プライマリ インスタンスに対してだけ作成できます。スケジューリング バックアップを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Scheduled Backups] を選択します。

[Scheduled Backups] ページが表示されます。表 17-2 に、[Scheduled Backups] ページに表示されるフィールドを示します。

表 17-2　[Scheduled Backups] ページ

オプション	説明
バックアップ データ	
バックアップによって作成されるファイル名は、入力したプレフィックスにタイムスタンプおよびファイル タイプ情報が追加された形式になります。	
Filename Prefix	ファイル名プレフィックスを入力します。ACS によってバックアップ タイムスタンプがこれに追加されます。たとえば、ファイル名プレフィックスとして ACSBackup を入力し、バックアップが 2009 年 6 月 5 日の 20 時 37 分に実行された場合、ACS によってバックアップ ファイル ACSBackup-090506-2037.tar.gpg が作成されます。
Repository	[Select] をクリックして、[Software Update and Backup Repositories] ダイアログボックスを開きます。ここから、バックアップ ファイルを保存する適切なリポジトリを選択できます。

表 17-2　[Scheduled Backups] ページ （続き）

オプション	説明
スケジューリング オプション	
Time of Day	ACS で ACS 設定データをバックアップする時間を選択します。バックアップは、毎日、週に 1 回、または月に 1 回実行するようにスケジューリングできます。 • [Daily] : ACS で毎日指定した時間に ACS 設定データをバックアップするには、このオプションを選択します。 • [Weekly] : ACS で週に 1 回 ACS 設定データをバックアップするには、このオプションを選択し、曜日を指定します。 • [Monthly] : ACS で月に 1 回 ACS 設定データをバックアップするには、このオプションを選択し、日付を指定します。

ステップ 2　[Submit] をクリックして、バックアップをスケジューリングします。

関連項目

「プライマリ インスタンスとセカンダリ インスタンスのバックアップ」（P.17-8）

プライマリ インスタンスとセカンダリ インスタンスのバックアップ

ACS には、通常のスケジューリング バックアップ以外に、任意のタイミングでプライマリ インスタンスとセカンダリ インスタンスをバックアップできるオプションが用意されています。プライマリ インスタンスについては、次のデータをバックアップできます。

- ACS 設定データだけ
- ACS 設定データと ADE-OS 設定データ

（注）　ACS では、セカンダリ インスタンスについては、ADE-OS 設定データだけがバックアップされます。

バックアップを即座に実行するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示されます。

ステップ 2　[Primary Instance] テーブルまたは [Secondary Instances] テーブルで、バックアップするインスタンスを選択します。

バックアップ対象として選択できるプライマリ インスタンスは 1 つだけですが、セカンダリ インスタンスについては複数選択できます。

ステップ 3　[Backup] をクリックします。

[Distributed System Management - Backup] ページが表示されます。表 17-3 に、このページに表示されるフィールドを示します。

表 17-3　[Distributed System Management - Backup] ページ

オプション	説明
バックアップ データ	
バックアップによって作成されるファイル名は、入力したプレフィックスにタイムスタンプおよびファイル タイプ情報が追加された形式になります。	
Filename Prefix	ファイル名プレフィックスを入力します。ACS によってバックアップ タイムスタンプがこれに追加されます。たとえば、ファイル名プレフィックスとして ACSBackup を入力し、バックアップが 2009 年 6 月 5 日の 20 時 37 分に実行された場合、ACS によってバックアップ ファイル ACSBackup-090506-2037.tar.gpg が作成されます。
Repository	[Select] をクリックして、[Software Update and Backup Repositories] ダイアログボックスを開きます。ここから、バックアップ ファイルを保存する適切なリポジトリを選択できます。
バックアップ オプション（プライマリ インスタンスにだけ該当）	
ACS Configuration Backup	ACS 設定データだけをバックアップする場合は、このオプションをクリックします。
ACS Configuration and ADE-OS Backup	ACS 設定データと ADE-OS 設定データの両方をバックアップする場合は、このオプションをクリックします。

ステップ 4　[Submit] をクリックして、即座にバックアップを実行します。

関連項目

「スケジューリング バックアップ」（P.17-6）

バックアップ/復元後のプライマリ インスタンスとセカンダリ インスタンスの同期

プライマリ インスタンスでシステム バックアップが復元されるように指定しても、セカンダリ インスタンスは、プライマリ インスタンスに存在する、新しく復元されたデータベースに基づいて更新されません。

セカンダリ インスタンスが更新されるようにするには、セカンダリ インスタンスからハードウェアの置き換えを要求して、復元されたプライマリ インスタンスに再び加入させる必要があります。次の手順を実行します。

ステップ 1　セカンダリ インスタンスをプライマリ インスタンスから登録解除します。

ステップ 2　セカンダリ インスタンスの Web インターフェイスで、[Systems Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択し、[Deregister from Primary] をクリックします。

ステップ 3　[Systems Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

これによって、プライマリ インスタンスに対して再びセカンダリ インスタンスのハードウェアの置き換えを実行できます。

ステップ 4　プライマリのホスト名または IP アドレスと管理クレデンシャルを指定します。

ステップ 5　[Hardware Replacement] を選択してから、セカンダリ インスタンスのホスト名を指定します。

ステップ 6　[Register to Primary] をクリックします。

インスタンスの編集

[System Administration] > [Operations] > [Distributed System Management] を選択すると、プライマリ インスタンスまたはセカンダリ インスタンスを編集できます。プライマリ インスタンスとセカンダリ インスタンスのバックアップを実行できます。[Distributed System Management] ページでは、次の操作を実行できます。

- 「プライマリ インスタンスの表示および編集」（P.17-10）
- 「セカンダリ インスタンスの表示および編集」（P.17-13）
- 「プライマリ インスタンスとセカンダリ インスタンスのバックアップ」（P.17-8）
- 「バックアップ/復元後のプライマリ インスタンスとセカンダリ インスタンスの同期」（P.17-9）

プライマリ インスタンスの表示および編集

プライマリ インスタンスを編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示され、2 つのテーブルが示されます。

- [Primary Instance] テーブル：プライマリ インスタンスが表示されます。

  プライマリ インスタンスは、インストール プロセスの一環として作成されます。
- [Secondary Instances] テーブル：セカンダリ インスタンスのリストとステータスが表示されます。詳細については、「セカンダリ インスタンスの表示および編集」（P.17-13）を参照してください。

表 17-4 に、[Distributed System Management] ページに表示される情報を示します。

表 17-4　[Distributed System Management] ページ

オプション	説明
Primary Instance	
Name	プライマリ インスタンスのホスト名。
IP Address	プライマリ インスタンスの IP アドレス。
Online Status	プライマリ インスタンスがオンラインかオフラインかを示します。チェック マークは、プライマリ インスタンスがオンラインであることを示します。**x** は、プライマリ インスタンスがオフラインであることを示します。
Replication ID	プライマリ インスタンスに対する最後の設定変更を示すトランザクション ID。この値は、設定変更ごとに 1 ずつ増加します。有効な値は 1 ～ 無限大です。
Last Update	最後のデータベース設定変更のタイムスタンプ。タイムスタンプの形式は、*hh:mm dd:mm:yyyy* です。
Version	プライマリ ACS インスタンスで実行されている ACS ソフトウェアの現在のバージョン。有効な値は、バージョン文字列か、またはソフトウェア アップグレードが開始されている場合は *Upgrade in progress* です。
Description	プライマリ インスタンスの説明。
Edit	プライマリ インスタンスを選択し、このボタンをクリックしてプライマリ インスタンスを編集します。
Backup	プライマリ インスタンスを選択し、このボタンをクリックしてプライマリ インスタンスをバックアップします。詳細については、「プライマリ インスタンスとセカンダリ インスタンスのバックアップ」（P.17-8）を参照してください。
Secondary Instances	
Name	セカンダリ インスタンスのホスト名。
IP Address	セカンダリ インスタンスの IP アドレス。
Online Status	セカンダリ インスタンスがオンラインかオフラインかを示します。チェック マークは、セカンダリ インスタンスがオンラインであることを示します。**x** は、セカンダリ インスタンスがオフラインであることを示します。

表 17-4　[Distributed System Management] ページ （続き）

オプション	説明
Replication Status	レプリケーション ステータスの値は、次のとおりです。 • UPDATED：セカンダリ インスタンスで複製が完了しました。管理および実行時サービスの両方が、プライマリ インスタンスからの設定変更を反映して最新になります。 • PENDING：完全な複製の要求が開始されているか、またはプライマリで加えられた設定変更がまだセカンダリに伝播されていません。 • REPLICATING：プライマリからセカンダリへの複製の処理中です。 • LOCAL MODE：セカンダリ インスタンスでは展開から複製の更新を受信しておらず、独自のローカル設定を維持しています。 • DEREGISTERED：セカンダリ インスタンスはプライマリ インスタンスから登録解除され、展開の一部ではありません。 • INACTIVE：セカンダリ インスタンスは非アクティブです。このインスタンスをアクティブにするには、このインスタンスを選択し、[Activate] をクリックする必要があります。 • N/A：プライマリ インスタンスの複製はありません。
Replication Time	最後の複製のタイムスタンプ。タイムスタンプの形式は、*hh:mm dd:mm:yyyy* です。
Version	セカンダリ ACS インスタンスで実行されている ACS ソフトウェアの現在のバージョン。有効な値は、バージョン文字列か、またはソフトウェア アップグレードが開始されている場合は *Upgrade in progress* です。
Description	セカンダリ インスタンスの説明。
Edit	編集するセカンダリ インスタンスを選択し、このボタンをクリックして編集します。
Delete	削除するセカンダリ インスタンスを選択し、このボタンをクリックして削除します。
Activate	新しく登録されたセカンダリ インスタンスを自動的にアクティブにするためのオプションがディセーブルになっている場合、セカンダリは最初は非アクティブ状態になります。これらの非アクティブなセカンダリ インスタンスをアクティブにするには、[Activate] をクリックします。
Deregister[1]	セカンダリ インスタンスをプライマリ インスタンスから切断します。セカンダリ インスタンスでプライマリ インスタンスからの設定更新を受信しないようにします。登録解除では、登録解除されたノードが再起動されます。 完全な複製が進行中のインスタンスを登録解除しないでください。完全な複製が完了し、セカンダリ インスタンスが再起動するまで待機してから、セカンダリ インスタンスを登録解除します。
Promote	セカンダリ インスタンスをプライマリ インスタンスに昇格させるように要求します。すべての複製更新が完了するように、現在のプライマリ インスタンスに対するすべての更新が停止します。複製更新が完了すると、設定のプライマリ制御がセカンダリ インスタンスによって取得されます。 セカンダリ インスタンスをプライマリ インスタンスに昇格させるには、事前にそのセカンダリ インスタンスをアクティブにする必要があります。
Full Replication	セカンダリ インスタンスに対してプライマリ インスタンスのデータベース設定を複製します。ACS が再起動されます。 完全な複製が進行中のインスタンスを登録解除しないでください。完全な複製が完了し、セカンダリ インスタンスが再起動するまで待機してから、セカンダリ インスタンスを登録解除します。
Backup	バックアップするセカンダリ インスタンスを選択し、このボタンをクリックしてバックアップを実行します。詳細については、「プライマリ インスタンスとセカンダリ インスタンスのバックアップ」（P.17-8）を参照してください。

1. 登録解除が実行されると、登録解除されたノードが再起動されますが、ACS は再起動されません。登録および完全な複製が実行されると、データベースが置き換えられるため、ACS が再起動されます。

ステップ 2　[Primary Instance] テーブルで、変更するプライマリ インスタンスをクリックするか、または [Name] のチェックボックスをオンにして [Edit] をクリックします。

ステップ 3　表 17-5 の説明に従って、[Distributed System Management Properties] ページのフィールドに入力します。

表 17-5　[Distributed System Management Properties] ページ

オプション	説明
Instance Data	
Hostname	ACS ホスト マシンの名前。
Launch Session for Local GUI	選択した ACS マシンの新しいインスタンスを起動するには、このボタンをクリックします。プライマリ インスタンスまたはセカンダリ インスタンスにログインする必要があります。 このオプションは、別のインスタンスを表示または編集するときにだけ表示されます。
Role	プライマリ インスタンスまたはセカンダリ インスタンス、あるいは [Local] を指定します。
IP Address	プライマリ インスタンスまたはセカンダリ インスタンスの IP アドレス。
Port	管理サービス用のポート。
MAC Address	インスタンスの MAC アドレス。
Description	プライマリ インスタンスまたはセカンダリ インスタンスの説明。
Check Secondary Every（プライマリ インスタンスにだけ該当）	プライマリ インスタンスがセカンダリ インスタンスにハートビート ステータス要求を送信するレート。デフォルト値は 60 秒です。最小値は 30 秒、最大値は 30 分です。
Statistics Polling Period（プライマリ インスタンスにだけ該当）	プライマリ インスタンスがセカンダリ インスタンスにポーリングして統計情報およびロギング情報を問い合わせるレート。各ポーリング期間に、プライマリ サーバはすべてのセカンダリ サーバにクエリーを送信しませんが、すべての ACS サーバはそのヘルス情報をログ コレクタ サーバに送信します。最小値は 60 秒、最大値は 30 分です。ただし、ポーリングおよびロギングをオフにすることを示す値 0 を指定できます。その結果、ログ コレクタ サーバはヘルス ステータスを表示しません。デフォルト値は 60 秒です。
Enable Auto Activation for Newly Registered Instances（プライマリ インスタンスにだけ該当）	登録されているセカンダリ インスタンスを自動的にアクティブにするには、このチェックボックスをオンにします。
Instance Status	
Status	プライマリ インスタンスまたはセカンダリ インスタンスがオンラインかオフラインかを示します。
Version	ACS ソフトウェアの現在のバージョン。
Replication Status（セカンダリ インスタンスにだけ該当）	レプリケーション ステータスの値は、次のとおりです。 • UPDATED：ACS インスタンスで複製が完了しました。管理および実行時サービスの両方が、プライマリ インスタンスからの設定変更を反映して最新になります。 • PENDING：完全な複製の要求が開始されています。 • REPLICATING：プライマリからセカンダリへの複製の処理中です。 • DEREGISTERED：セカンダリ インスタンスがプライマリから登録解除されました。 • N/A：プライマリ インスタンスの複製はありません。
Last Update Time（プライマリ インスタンスにだけ該当）	最後のデータベース設定変更のタイムスタンプ。タイムスタンプの形式は、*hh:mm dd:mm:yyyy* です。

表 17-5　[Distributed System Management Properties] ページ（続き）

オプション	説明
Last Replication Time（セカンダリ インスタンスにだけ該当）	最後の複製のタイムスタンプ。タイムスタンプの形式は、*hh:mm dd:mm:yyyy* です。
Last Replication ID（プライマリ インスタンスにだけ該当）	セカンダリ インスタンスに対する最後の設定変更を示すトランザクション ID。この値は、設定変更ごとに 1 ずつ増加します。有効な値は 1 ～ 無限大です。
Primary Replication ID（セカンダリ インスタンスにだけ該当）	プライマリ インスタンスに対する最後の設定変更を示すトランザクション ID。この値は、設定変更ごとに 1 ずつ増加します。有効な値は 1 ～ 無限大です。

ステップ 4　[Submit] をクリックします。

[Distributed System Management] ページの [Primary Instance] テーブルに、編集したプライマリ インスタンスが表示されます。

関連トピック

- 「プライマリ インスタンスからのセカンダリ インスタンスの複製」（P.17-20）
- 「セカンダリ インスタンスの表示および編集」（P.17-13）

セカンダリ インスタンスの表示および編集

セカンダリ インスタンスを編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示され、2 つのテーブルが示されます。

- [Primary Instance] テーブル：プライマリ インスタンスが表示されます。
- [Secondary Instances] テーブル：プライマリ インスタンスに対して登録されているセカンダリ インスタンスのリストおよびステータスが表示されます。

カラムの定義については、表 17-4 を参照してください。

ステップ 2　[Secondary Instances] テーブルで、変更するセカンダリ インスタンスをクリックするか、またはセカンダリ インスタンスのチェックボックスをオンにして [Edit] をクリックします。

ステップ 3　表 17-5 の説明に従って、[Distributed System Management Properties] ページのフィールドに入力します。

ステップ 4　[Submit] をクリックします。

[Distributed System Management] ページの [Secondary Instances] テーブルに、編集したセカンダリ インスタンスが表示されます。

関連トピック

- 「インスタンスの編集」（P.17-9）
- 「プライマリ インスタンスの表示および編集」（P.17-10）

セカンダリ インスタンスの削除

セカンダリ インスタンスを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示され、[Secondary Instances] テーブルにセカンダリ インスタンスのリストが示されます。

ステップ 2　削除するセカンダリ インスタンスを登録解除します。「[Distributed System Management] ページでのセカンダリ インスタンスの登録解除」（P.17-18）を参照してください。

ステップ 3　削除するセカンダリ インスタンスの近くにある 1 つ以上のチェックボックスをオンにします。

ステップ 4　[Delete] をクリックします。

次の警告メッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 5　[OK] をクリックします。

[Distributed System Management] ページに、削除されたセカンダリ インスタンスのない [Secondary Instances] テーブルが表示されます。

セカンダリ インスタンスのアクティベーション

セカンダリ インスタンスをアクティブにするには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示され、2 つのテーブルが示されます。

- [Primary Instance] テーブル：プライマリ インスタンスが表示されます。
- [Secondary Instances] テーブル：プライマリ インスタンスに対して登録されているセカンダリ インスタンスのリストおよびステータスが表示されます。

カラムの説明については、表 17-4 を参照してください。

ステップ 2　[Secondary Instances] テーブルで、アクティブにするセカンダリ インスタンスの近くにあるチェックボックスをオンにします。

ステップ 3　[Activate] をクリックします。

ステップ 4　[Distributed System Management] ページの [Secondary Instances] テーブルに、アクティブにしたセカンダリ インスタンスが表示されます。有効なフィールド オプションについては、表 17-5 を参照してください。

関連トピック

- 「セカンダリ インスタンスの表示および編集」（P.17-13）
- 「セカンダリ インスタンスの削除」（P.17-14）
- 「プライマリ インスタンスからのセカンダリ インスタンスの複製」（P.17-20）
- 「プライマリ インスタンスへのセカンダリ インスタンスの登録」（P.17-15）

- 「[Deployment Operations] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの昇格」（P.17-19）
- 「[Deployment Operations] ページでのローカル モード インスタンスの作成」（P.17-24）

プライマリ インスタンスへのセカンダリ インスタンスの登録

プライマリ インスタンスにセカンダリ インスタンスを登録するには、次の手順を実行します。

ステップ 1　別の ACS サーバのセカンダリ インスタンスとして使用するマシンにログインします。

ステップ 2　[System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

[Deployment Operations] ページが表示されます。表 17-6 に、このページに表示される情報を示します。

表 17-6　[System Operations: Deployment Operations] ページ

オプション	説明
Instance Status	
現在のステータス	ログインするノードのインスタンスがプライマリとセカンダリのいずれであるかを識別します。また、ローカル モードで実行しているかどうかを識別します。
Primary Instance	プライマリ インスタンスのホスト名。
Primary IP	プライマリ インスタンスの IP アドレス。
Registration（ローカル モードで実行していないインスタンスに対してだけアクティブ）	
Primary Instance	セカンダリ インスタンスを登録するプライマリ サーバのホスト名。
Admin Username	管理者アカウントのユーザ名。
Admin Password	管理者アカウントのパスワード。
Hardware Replacement	新規または既存の ACS インスタンス ハードウェアをプライマリ インスタンスに再登録して、プライマリ インスタンスの既存の設定を取得できるようにする場合にオンにします。このことは、インスタンスで障害が発生し、物理的な置き換えが必要となった場合に役立ちます。
Recovery Keyword	置き換え対象のインスタンスの名前。この値は、置き換え対象のシステムのホスト名です。この情報の送信後に、このインスタンスはプライマリ インスタンスに接続します。 プライマリ インスタンスは、キーワードに基づいて、関連付けられた ACS インスタンス レコードを検索し、各レコードに登録済みのマークを付けます。
Register to Primary	リモート プライマリに接続し、セカンダリ インスタンスをプライマリ インスタンスに登録します。
Backup	
Backup	現在のインスタンスをバックアップします。
Local Mode	
Admin Username	管理者アカウントのユーザ名。
Admin Password	管理者アカウントのパスワード。
Reconnect このオプションは、ローカル モードのノードでだけ表示されます。このオプションを使用すると、クレデンシャルを入力するように要求するプロンプトが表示されます。	[Reconnect] をクリックして、プライマリ インスタンスに再接続します。 プライマリ インスタンスに再接続すると、ローカルのセカンダリ インスタンスに加えた設定変更は失われます。 ローカルのセカンダリ インスタンスに加えた設定変更を保持する場合は、次の手順を実行する必要があります。 1. ローカルのセカンダリ インスタンスを登録解除します（このインスタンスが新しいプライマリになります）。 2. 展開からすべてのインスタンスを登録解除します。 3. 設定変更を保持する新しいプライマリにすべてのインスタンスを登録します。
Request Local Mode このオプションは、登録されているセカンダリのページにだけ表示されます。	セカンダリ インスタンスをローカル モードにするように要求します。管理者は、対象のインスタンスに対してだけ設定変更を行うことができます。セカンダリ インスタンスに加えた変更は、プライマリ インスタンスに再接続しても自動的には更新されません。セカンダリ インスタンスに対して変更を手動で入力する必要があります。

表 17-6　[System Operations: Deployment Operations] ページ （続き）

オプション	説明
Deregistration	
Deregister from Primary	プライマリ インスタンスからセカンダリを登録解除します。セカンダリ インスタンスには、登録解除元のデータベース設定が保持されます。すべてのノードが登録解除済みおよび非アクティブとしてマークされ、そのセカンダリ インスタンスがプライマリ インスタンスになります。 完全な複製が進行中のインスタンスを登録解除しないでください。完全な複製が完了し、セカンダリ インスタンスが再起動するまで待機してから、セカンダリ インスタンスを登録解除します。
Promotion	
Promote to Primary	セカンダリ インスタンスをプライマリ インスタンスに昇格させるように要求します。すべての複製更新が完了するように、現在のプライマリ インスタンスに対するすべての更新が停止します。複製更新が完了すると、設定のプライマリ制御がセカンダリ インスタンスによって取得されます。
Replication	
Force Full Replication	セカンダリ インスタンスに対してプライマリ インスタンスのデータベース設定を複製します。 完全な複製が進行中のインスタンスを登録解除しないでください。完全な複製が完了し、セカンダリ インスタンスが再起動するまで待機してから、セカンダリ インスタンスを登録解除します。

ステップ 3　[Registration Section] で適切な値を指定します。

ステップ 4　[Register to Primary] をクリックします。

次の警告メッセージが表示されます。

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance.ACS will be restarted.You will be required to login again.Do you wish to
continue?
```

ステップ 5　[OK] をクリックします。

セカンダリ インスタンスが自動的に再起動します。

プライマリ インスタンスで作成した設定とクレデンシャルがセカンダリ インスタンスに適用されます。

ステップ 6　最初のセカンダリ インスタンスが正常に起動して稼働状態になったあと、同じ配置にセカンダリとして別の ACS マシンを登録します。展開内のすべてのセカンダリ マシンを登録するために同じ手順に従ってください。

（注）　70% のメモリ利用率は、ログ コレクタが実行中で、サーバに高い負荷がかかっている場合に、セカンダリ インスタンスで正常と見なされます。メモリ使用率が 70% を超えて増加し、約 4 ～ 5 時間持続した場合、それは異常と見なされ、分析する必要があります。

[Distributed System Management] ページでのセカンダリ インスタンスの登録解除

[Distributed System Management] ページでセカンダリ インスタンスを登録解除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示されます。

ステップ 2　[Secondary Instances] テーブルで、登録解除するセカンダリ インスタンスの隣にあるチェックボックスの 1 つをオンにします。

ステップ 3　[Deregister] をクリックします。

次の警告メッセージが表示されます。

```
This operation will deregister this server as a secondary with the primary server.ACS
will be restarted.You will be required to login again.Do you wish to continue?
```

ステップ 4　[OK] をクリックします。

ステップ 5　ACS マシンにログインします。

ステップ 6　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示され、プライマリ インスタンスから登録解除されたセカンダリ インスタンスが示されます。

関連トピック

- 「セカンダリ インスタンスの表示および編集」（P.17-13）
- 「セカンダリ インスタンスの削除」（P.17-14）
- 「セカンダリ インスタンスのアクティベーション」（P.17-14）
- 「[Deployment Operations] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの昇格」（P.17-19）
- 「[Deployment Operations] ページでのローカル モード インスタンスの作成」（P.17-24）

[Deployment Operations] ページでのセカンダリ インスタンスの登録解除

（注）　この場合、ログインしているローカル マシンがセカンダリ インスタンスです。

[Deployment Operations] ページでセカンダリ インスタンスを登録解除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

[Deployment Operations] ページが表示され、ログインしているセカンダリ インスタンスが示されます。有効なフィールド オプションについては、表 17-6 を参照してください。

ステップ 2　[Deregister from Primary] をクリックします。

次の警告メッセージが表示されます。

```
This operation will deregister this server as a secondary with the primary server.ACS
will be restarted.You will be required to login again.Do you wish to continue?
```

ステップ 3　[OK] をクリックします。

ステップ 4　ACS マシンにログインします。

ステップ 5　[System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

[Deployment Operations] ページが表示され、今までログインしていて、プライマリ インスタンスから登録解除されたセカンダリ インスタンスが示されます。

関連トピック

- 「セカンダリ インスタンスの表示および編集」（P.17-13）
- 「セカンダリ インスタンスの削除」（P.17-14）
- 「セカンダリ インスタンスのアクティベーション」（P.17-14）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの昇格」（P.17-19）
- 「[Deployment Operations] ページでのローカル モード インスタンスの作成」（P.17-24）

[Distributed System Management] ページでのセカンダリ インスタンスの昇格

[Distributed System Management] ページでセカンダリ インスタンスをプライマリ インスタンスに昇格させるには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示されます。有効なフィールド オプションについては、表 17-4 を参照してください。

ステップ 2　[Secondary Instances] テーブルで、プライマリ インスタンスに昇格させるセカンダリ インスタンスの隣にあるチェックボックスをオンにします。

ステップ 3　[Promote] をクリックします。

[Distributed System Management] ページが表示され、昇格したインスタンスが示されます。

関連トピック

- 「セカンダリ インスタンスの表示および編集」（P.17-13）
- 「セカンダリ インスタンスの削除」（P.17-14）
- 「セカンダリ インスタンスのアクティベーション」（P.17-14）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「[Deployment Operations] ページでのローカル モード インスタンスの作成」（P.17-24）

[Deployment Operations] ページでのセカンダリ インスタンスの昇格

[Deployment Operations] ページでセカンダリ インスタンスをプライマリ インスタンスに昇格させるには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Deployment Operations] ページが表示されます。有効なフィールド オプションについては、表 17-6 を参照してください。

ステップ 2　セカンダリ インスタンスをプライマリ インスタンスに登録します。「プライマリ インスタンスへのセカンダリ インスタンスの登録」（P.17-15）を参照してください。

ステップ 3　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Deployment Operations] ページが表示されます。

ステップ 4　プライマリ インスタンスに昇格させるセカンダリ インスタンスの隣にあるチェックボックスをオンにします。

ステップ 5　[Promote to Primary] をクリックします。

[Distributed System Management] ページが表示され、昇格したインスタンスが示されます。

関連トピック

- 「セカンダリ インスタンスの表示および編集」（P.17-13）
- 「セカンダリ インスタンスの削除」（P.17-14）
- 「プライマリ インスタンスからのセカンダリ インスタンスの複製」（P.17-20）
- 「セカンダリ インスタンスのアクティベーション」（P.17-14）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの登録解除」（P.17-18）
- 「[Distributed System Management] ページでのセカンダリ インスタンスの昇格」（P.17-19）
- 「[Deployment Operations] ページでのローカル モード インスタンスの作成」（P.17-24）

プライマリ インスタンスからのセカンダリ インスタンスの複製

セカンダリ インスタンスを複製するには、2 つの異なるページを使用できます。

- [Distributed System Management] ページでのセカンダリ インスタンスの複製
- [Deployment Operations] ページでのセカンダリ インスタンスの複製

（注）　複製の詳細については、「ACS 4.x と 5.4 の複製」（P.1-2）を参照してください。

[Distributed System Management] ページでのセカンダリ インスタンスの複製

（注）　すべての ACS アプライアンスは、AD ドメイン クロックと同期している必要があります。

セカンダリ インスタンスを複製するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示されます。

ステップ 2　[Secondary Instances] テーブルで、複製するセカンダリ インスタンスの隣にあるチェックボックスの 1 つをオンにします。

ステップ 3　[Full Replication] をクリックします。

次の警告メッセージが表示されます。

```
This operation will force a full replication for this secondary server.ACS will be
restarted.You will be required to login again.Do you wish to continue?
```

ステップ 4　[OK] をクリックします。

ステップ 5　ACS マシンにログインします。

ステップ 6　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示されます。[Secondary Instance] テーブルの [Replication Status] カラムに **UPDATED** と表示されます。セカンダリ インスタンスで複製が完了しました。管理および実行時サービスは、プライマリ インスタンスからの設定変更を反映して最新になります。

[Deployment Operations] ページでのセカンダリ インスタンスの複製

（注）　すべての ACS アプライアンスは、AD ドメイン クロックと同期している必要があります。

セカンダリ インスタンスを複製するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

[Deployment Operations] ページが表示されます。有効なフィールド オプションについては、表 17-6 を参照してください。

ステップ 2　[Force Full Replication] をクリックします。

次の警告メッセージが表示されます。

```
This operation will force a full replication for this secondary server.ACS will be
restarted.You will be required to login again.Do you wish to continue?
```

ステップ 3　[OK] をクリックします。

ステップ 4　ACS マシンにログインします。

ステップ 5　[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示されます。[Secondary Instance] テーブルの [Replication Status] カラムに **UPDATED** と表示されます。セカンダリ インスタンスで複製が完了しました。管理および実行時サービスは、プライマリ インスタンスからの設定変更を反映して最新になります。

プライマリ サーバからのプライマリ インスタンスの IP アドレスの変更

プライマリ ACS サーバの IP アドレスを変更するには、次の手順を実行します。

ステップ 1　ACS プライマリ Web インターフェイスにログインし、プライマリ ACS サーバからすべてのセカンダリ ACS インスタンスの登録を解除するために、[System Administration] > [Operations] > [Distributed System Management] を選択します。

[Distributed System Management] ページが表示されます。

ステップ 2　セカンダリ ACS インスタンスの近くにあるチェックボックスを 1 つずつオンにし、[Deregister] をクリックします。

すべてのセカンダリ ACS インスタンスを登録解除する前にログ コレクタがプライマリ ACS サーバで実行中であることを確認します。ログ コレクタがセカンダリ ACS サーバのいずれか 1 つで実行されている場合は、プライマリ ACS サーバをログ コレクタを変更します。

ログ コレクタを変更するには、「ログ コレクタの設定」（P.18-34）を参照してください。

ステップ 3　すべての登録解除されたセカンダリ ACS インスタンスを削除するには、登録解除されたセカンダリ ACS インスタンスの近くにあるチェックボックスをオンにします。

登録解除されたセカンダリ ACS インスタンスが削除されます。

ステップ 4　次を入力して管理モードで ACS サーバにログインします。

```
acs-5-2-a/admin# conf t
```

ステップ 5　次のコマンドを入力します。

```
int g 0
```

ip address *old ip address new ip address*

ステップ 6　Ctrl キーを押した状態で z キーを押します。

次の警告メッセージが表示されます。

```
Changing the hostname or IP may result in undesired side effects, such as installed
application(s) being restarted.Are you sure you want to proceed?[y/n]
```

ステップ 7　y を押します。

ステップ 8　管理モードと新しい IP アドレスを使用してプライマリ ACS サーバにアクセスします。

ステップ 9　すべてのプロセスが正しく実行されていることを確認するために、**show application status acs** コマンドを使用します。

ステップ 10　プライマリ ACS サーバにセカンダリ インスタンスを登録します。

「プライマリ インスタンスへのセカンダリ インスタンスの登録」（P.17-15）を参照してください。

フェールオーバー

ACS 5.4 では、配置シナリオに複数の ACS インスタンスを設定できます。各展開は 1 つのプライマリと複数のセカンダリ ACS サーバを持つことができます。

シナリオ 1：プライマリ ACS が分散展開でダウンする

3 つの ACS インスタンス ACS1、ACS2 および ACS3 があるとします。

ACS1 はプライマリで、ACS2 および ACS3 はセカンダリです。プライマリ サーバ ACS1 がダウンしている場合は、セカンダリ サーバに設定変更を加えることはできません。他のセカンダリ ACS サーバがすべてアクティブの場合、任意のセカンダリ サーバをプライマリ サーバにすることができます。

ステップ 1　差し当たり ACS2 をプライマリに昇格させ、それを使用して設定変更を加えます。

セカンダリ ACS サーバをプライマリ サーバとして昇格させるには、「[Distributed System Management] ページでのセカンダリ インスタンスの昇格」（P.17-19）および「[Deployment Operations] ページでのセカンダリ インスタンスの昇格」（P.17-20）を参照してください。

これで、ACS2 が新しいプライマリ インスタンスです。したがって、ACS2 で設定変更を行うことができ、それは ACS3 とすべてのセカンダリ サーバに即座に複製されます。

ここで、ACS1 をオンラインに戻すことを考慮します。ACS1 がスタンドアロンであるように ACS2 と展開の他で加えられた変更を保持する必要がある場合は、その変更を複製しないでください。

ステップ 2　ACS1 のセカンダリ サーバのリストから ACS2 および ACS3 を削除します。

ステップ 3　セカンダリとして ACS1 を登録するには、現在のプライマリ サーバである ACS2 から ACS1 を削除します。

これで、ACS2 が新しいプライマリ サーバです。展開はこれで、完全にオンラインに戻り動作可能な状態になり元の構造を持ちます。

シナリオ 2：プライマリ サーバのデータベース バックアップの復元

このシナリオでは、プライマリ サーバのデータベース バックアップを復元し、すべてのセカンダリ サーバにも復元したデータベースを持たせます。

プライマリ サーバのデータベース バックアップを復元するには、次の手順を実行します。

ステップ 1　`acs backup` コマンドを使用して、展開が正常に機能している場合にデータベース バックアップを行います。

ステップ 2　展開がプライマリで正常に機能していたときに行った古いデータベース バックアップ ファイルを復元します。

次の警告メッセージが表示されます。

```
restore AAA--?110907---?2140.tar.gpg rep chftp Restore requires restart of ACS
services.Continue?(yes/no) yes
```

データベースを復元すると、分散設定に影響します。

```
Restoring the data base will affect the distributed setup.For example, replication
between primary and secondary will be broken.It is recommended to schedule a downtime to
carry out the restore operation.After restore, you will have to configure each secondary
to local mode and then re-connect with primary.Do you want to continue with restore
operation?.<yes/no>:yes

Continuing restore.....

Stopping ACS.
```

```
Stopping Management and View..............
Stopping Runtime.......
Stopping Database........
Cleanup.......
Starting ACS....
```

プライマリ サーバ上のデータベースが正しく復元されます。

これで、分散展開のすべてのセカンダリ サーバが切断されたことを確認できます。

ステップ 3　セカンダリ Web インターフェイスにログインし、[System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択し、[Request Local Mode] をクリックします。

ローカル モードをアクティブにした後でメニューの変更を確認できます。

ステップ 4　管理者ユーザ名と管理者パスワードを入力し、[Reconnect] をクリックします。

セカンダリ ACS サーバが再起動されます。

プライマリ サーバで、セカンダリ サーバが稼働していることを確認できます。また、展開が適切に動作していたときに作成されたバック アップ データのみがデータベースに表示されることも確認できます。したがって、復元したデータベースの複製は正常です。

ステップ 5　再接続するために他のセカンダリ サーバでも同じ手順に従ってください。

[Deployment Operations] ページでのローカル モード インスタンスの作成

セカンダリ インスタンスがローカル モードの場合、プライマリ インスタンスからの設定変更を受信しません。セカンダリ インスタンスに加えた設定変更はローカルに保持され、プライマリ インスタンスには伝播されません。

[Deployment Operations] ページを使用してローカル モード インスタンスを作成するには、次の手順を実行します。

ステップ 1　[System Operations] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

[Deployment Operations] ページが表示されます。有効なフィールド オプションについては、表 17-4 を参照してください。

ステップ 2　登録するセカンダリ インスタンスについて、[Registration] セクションで適切な値を指定します。

ステップ 3　[Register to Primary] をクリックします。

次の警告メッセージが表示されます。

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance.ACS will be restarted.You will be required to login again.Do you wish to
continue?
```

ステップ 4　[OK] をクリックします。

ステップ 5　ACS ローカル マシンにログインします。

ステップ 6　[System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

[Deployment Operations] ページが表示されます。

ステップ 7　[Request Local Mode] をクリックします。

セカンダリ インスタンスがローカル モードになります。

セカンダリ インスタンスをプライマリ インスタンスに再接続すると、ローカルのセカンダリ インスタンスに加えた設定変更は失われます。プライマリ インスタンスの設定情報を手動で復元する必要があります。

対象のインスタンスの設定情報を手動で復元するには、[ACS Configuration Audit] レポートの設定情報を使用します。

ソフトウェア リポジトリの作成、複製、編集、および削除

ソフトウェア リポジトリを作成、複製、編集、または削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Operations] > [Software Repositories] を選択します。

[Software Repositories] ページが表示されます。表 17-7 に、このページに表示される情報を示します。

表 17-7　[Software Repositories] ページ

オプション	説明
Name	ソフトウェア リポジトリの名前。
Protocol	アップグレード ファイルを転送するために使用するプロトコル（DISK、FTP、SFTP、TFTP、NFS）の名前。
Server Name	サーバ名を指定します。
Path	アップグレード ファイルが存在するディレクトリのパスの名前。プロトコルおよびアップグレード ファイルの場所を指定する必要があります。たとえば、ftp://acs-home/updates です。
Description	ソフトウェア リポジトリの説明。

ステップ 2　次のアクションのいずれかを実行します。

- [Create] をクリックします。
- 複製するソフトウェア リポジトリの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するソフトウェア リポジトリをクリックするか、または [Name] のチェックボックスをオンにして [Edit] をクリックします。
- 削除するソフトウェア リポジトリの隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

[Software Update Repositories Properties] ページが表示されます。

ステップ 3　表 17-8 の説明に従って、[Software Update Repositories Properties] ページのフィールドに入力します。

表 17-8　[Software Update Repositories Properties] ページ

オプション	説明
General	
Name	ソフトウェア リポジトリの名前。
Description	ソフトウェア リポジトリの説明。

表 17-8　[Software Update Repositories Properties] ページ （続き）

オプション	説明
Repository Information	
Protocol	アップグレード ファイルを転送するために使用するプロトコルの名前。有効なオプションは次のとおりです。 • DISK：このプロトコルを選択した場合は、パスを指定する必要があります。 • FTP：このプロトコルを選択した場合は、サーバ名、パス、およびクレデンシャルを指定する必要があります。 • SFTP：このプロトコルを選択した場合は、サーバ名、パス、およびクレデンシャルを指定する必要があります。 • TFTP：このプロトコルを選択した場合は、TFTP サーバの名前を入力する必要があります。任意でパスを指定できます。 • NFS：このプロトコルを選択した場合は、サーバ名およびパスを指定する必要があります。任意でクレデンシャルを指定できます。このプロトコルを選択する場合は、ACS に NFS ファイル システムへのフル アクセスがあることを確認します。読み取りと書き込みの権限を所有し、NFS ファイル システムでルート アクセス権限を許可できる必要があります。
Server Name	FTP、SFTP、TFTP、または NFS サーバの名前。
（注） リポジトリが指す実際の位置は /localdisk/*pathname* です	
Path	アップグレード ファイルのパスの名前。プロトコルおよびアップグレード ファイルの場所を指定する必要があります。たとえば、ftp://acs-home/updates です。
User Credentials	
Username	管理者名。
Password	管理者パスワード。

ステップ 4　[Submit] をクリックします。

新しいソフトウェア リポジトリが保存されます。[Software Repository] ページが表示され、作成、複製、または編集した新しいソフトウェア リポジトリが示されます。

関連トピック

- 「Web インターフェイスおよび CLI でのソフトウェア リポジトリの管理」（P.17-26）

Web インターフェイスおよび CLI でのソフトウェア リポジトリの管理

Web インターフェイスまたは CLI でリポジトリを管理できます。Web インターフェイスまたは CLI でリポジトリを作成または削除する際には、次の規則に留意してください。

- CLI でリポジトリを作成した場合、そのリポジトリは Web インターフェイスには表示されず、CLI でだけ削除できます。
- Web インターフェイスでリポジトリを作成した場合、そのリポジトリは CLI では削除できますが、Web インターフェイスには引き続き残ります。Web インターフェイスを使用してソフトウェア更新用のリポジトリを作成すると、そのリポジトリは CLI で自動的に再作成されます。
- Web インターフェイスを使用してリポジトリを削除すると、そのリポジトリは CLI でも削除されます。

関連トピック

- 「ソフトウェア リポジトリの作成、複製、編集、および削除」（P.17-25）

CHAPTER 18

システム管理設定の管理

Cisco Secure ACS をインストールしたあとに、ネットワークを効率的に管理するように ACS を設定および管理する必要があります。ACS Web インターフェイスを使用すると、ACS を簡単に設定してさまざまな処理を実行できます。ACS の使用を開始するために必要なインストール後の設定作業のリストについては、第 6 章「インストール後の設定タスク」を参照してください。

[System Administration] > [Configuration] を選択すると、次の操作を実行できるページにアクセスできます。

- TACACS+、EAP-TLS、PEAP、EAP-FAST の設定など、グローバル システム オプションの設定。「グローバル システム オプションの設定」（P.18-1）を参照してください。
- プロトコル ディクショナリの設定。「ディクショナリの管理」（P.18-5）を参照してください。
- ローカル サーバ証明書の管理。「ローカル サーバ証明書の設定」（P.18-14）を参照してください。
- ログ設定の管理。「ログの設定」（P.18-21）を参照してください。
- ライセンスの管理。「ライセンスの概要」（P.18-35）を参照してください。

グローバル システム オプションの設定

[System Administration] > [Configuration] > [Global System Options] の各ページに、次のオプションがあります。

- 「TACACS+ の設定」（P.18-1）
- 「EAP-TLS の設定」（P.18-2）
- 「PEAP の設定」（P.18-3）
- EAP-FAST の設定
- EAP-FAST PAC の生成

TACACS+ の設定

[TACACS+ Settings] ページは、TACACS+ の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [TACACS+ Settings] を選択します。

表 18-1 で説明されている [TACACS+ Settings] ページが表示されます。

表 18-1　TACACS+ Settings

オプション	説明
Port to Listen	リッスンするポート番号。
Connection Timeout	接続がタイムアウトするまでの分数。
Session Timeout	セッションがタイムアウトするまでの分数。
Maximum Packet Size	最大パケット サイズ（バイト単位）。
Single Connect Support	単一接続のサポートをイネーブルにする場合にオンにします。
Login Prompts	
Username Prompt	ユーザ名プロンプトとして使用するテキスト文字列。
Password Prompt	パスワード プロンプトとして使用するテキスト文字列。
Password Change Control	
Enable TELNET Change Password	TELNET セッション中にパスワードを変更するオプションを指定する場合に選択します。
Prompt for Old Password:	古いパスワードのプロンプトとして使用するテキスト文字列。
Prompt for New Password	新しいパスワードのプロンプトとして使用するテキスト文字列。
Prompt for Confirm Password	パスワードの確認プロンプトとして使用するテキスト文字列。
Disable TELNET Change Password	TELNET セッション中にパスワードを変更しない場合に選択します。
Message when Disabled	[Disable TELNET Change Password] オプションを選択した場合に表示されるメッセージ。

EAP-TLS の設定

[EAP-TLS Settings] ページは、EAP-TLS の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [EAP-TLS Settings] を選択します。

表 18-2 で説明されている [EAP-TLS Settings] ページが表示されます。

表 18-2　EAP-TLS Settings

オプション	説明
General	
Enable EAP-TLS Session Resume	完全な EAP-TLS 認証に成功したユーザの簡略化された再認証をサポートする場合にオンにします。 この機能を使用すると、証明書を使用しないで SSL ハンドシェイクだけでユーザの再認証が行われます。EAP-TLS セッション再開機能は、指定された EAP-TLS セッション タイムアウト値以内でだけ動作します。
EAP-TLS Session Timeout	EAP-TLS セッションがタイムアウトするまでの秒数を入力します。デフォルト値は 7200 秒です。
Stateless Session Resume	

表 18-2　EAP-TLS Settings （続き）

オプション	説明
Master Key Generation Period	値が指定された期間後にマスター キーの再生成に使用されます。デフォルトは 1 週間です。
Revoke	以前のマスター キーをすべてキャンセルするには、[Revoke] をクリックします。この処理を使用する場合は注意が必要です。 ACS ノードがセカンダリ ノードの場合、[Revoke] オプションはディセーブルになります。

PEAP の設定

[PEAP Settings] ページは、PEAP の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [PEAP Settings] を選択します。

表 18-3 で説明されている [PEAP Settings] ページが表示されます。

表 18-3　PEAP Settings

オプション	説明
Enable PEAP Session Resume	オンにすると、ACS は、ユーザが PEAP 認証のフェーズ 2 で正常に認証された場合にかぎり、PEAP 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、ACS はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。 PEAP セッション再開機能を動作させるには、PEAP セッション タイムアウト値を指定する必要があります。
PEAP Session Timeout	PEAP セッションがタイムアウトするまでの秒数を入力します。デフォルト値は 7200 秒です。
Enable Fast Reconnect	セッション再開機能がイネーブルの場合に、PEAP セッションがユーザ クレデンシャルを確認しないで ACS で再開することを許可する場合にオンにします。

関連項目

- 「EAP-FAST PAC の生成」（P.18-4）

EAP-FAST の設定

[EAP-FAST Settings] ページは、EAP-FAST の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [EAP-FAST] > [Settings] を選択します。

表 18-4 で説明されている [EAP-FAST Settings] ページが表示されます。

表 18-4　EAP-FAST Settings

オプション	説明
General	
Authority Identity Info Description	クレデンシャルをクライアントに送信する ACS サーバを説明したわかりやすい文字列。クライアントは、この文字列を Protected Access Credentials Information（PAC-Info）Type-Length-Value（TLV）で認識できます。デフォルト値は [Cisco Secure ACS] です。
Master Key Generation Period	この値は、PAC の暗号化や復号化および署名や認証に使用されます。デフォルトは 1 週間です。
Revoke	
Revoke	以前のマスターキーと PAC をすべて無効にするには、[Revoke] をクリックします。この処理を使用する場合は注意が必要です。 ACS ノードがセカンダリ ノードの場合、[Revoke] オプションはディセーブルになります。

EAP-FAST PAC の生成

EAP-FAST の [Generate PAC] ページは、ユーザ PAC またはマシン PAC を生成する場合に使用します。

ステップ 1　[System Administration] > [Configuration] > [Global System Options] > [EAP-FAST] > [Generate PAC] を選択します。

表 18-5 で説明されている [Generate PAC] ページが表示されます。

表 18-5　Generate PAC

オプション	説明
Tunnel PAC	トンネル PAC を生成する場合に選択します。
Machine PAC	マシン PAC を生成する場合に選択します。
Identity	EAP-FAST プロトコルによって「内部ユーザ名」として提示されたユーザ名またはマシン名を指定します。ID 文字列がそのユーザ名と一致しない場合、認証は失敗します。
PAC Time To Live	秒、分、時間、日、週、月、および年に対応する最大値を入力します。正の整数を入力してください。
Password	パスワードを入力します。

ステップ 2　[Generate PAC] をクリックします。

RSA SecurID プロンプトの設定

ACS 展開用の RSA プロンプトを設定できます。設定した RSA プロンプトのセットは、構成内のすべての RSA 領域と ACS インスタンスに使用されます。RSA SecurID プロンプトを設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Global System Options] > [RSA SecurID Prompts] を選択します。

[RSA SecurID Prompts] ページが表示されます。

ステップ 2　表 18-6 で説明されているフィールドを変更します。

表 18-6　[RSA SecurID Prompts] ページ

オプション	説明
Passcode Prompt	パスコードを要求するテキスト文字列。デフォルト値は [Enter PASSCODE:] です。
Next Token Prompt	次のトークンを要求するテキスト文字列。デフォルト値は [Enter Next TOKENCODE:] です。
Choose PIN Type Prompt	PIN タイプを要求するテキスト文字列。デフォルト値は [Do you want to enter your own pin?] です。
Accept System PIN Prompt	システム生成の PIN を受け付けるテキスト文字列。デフォルト値は [ARE YOU PREPARED TO ACCEPT A SYSTEM-GENERATED PIN?] です。
次に示す 2 つの PIN 入力プロンプトでは、プロンプトに次の文字列が含まれている場合、次のように置き換えられます。 • {MIN_LENGTH}：RSA 領域に設定されている最小 PIN 長に置き換えられます。 • {MAX_LENGTH}：RSA 領域に設定されている最大 PIN 長に置き換えられます。 • /x/：新しい PIN 手順をキャンセルする。	
Alphanumeric PIN Prompt	英数字の PIN を要求するテキスト文字列。
Numeric PIN Prompt	数値の PIN を要求するテキスト文字列。
Re-Enter PIN Prompt	ユーザに PIN の再入力を要求するテキスト文字列。デフォルト値は [Reenter PIN:] です。

ステップ 3　[Submit] をクリックして RSA SecurID プロンプトを保存します。

ディクショナリの管理

[System Administration] > [Configuration] > [Dictionaries] を選択すると、次のタスクを実行できます。

- 「RADIUS 属性と TACACS+ 属性の表示」（P.18-5）
- 「ID ディクショナリの設定」（P.18-10）

RADIUS 属性と TACACS+ 属性の表示

RADIUS と TACACS+ の [Dictionary] ページには、次のディクショナリ内の使用可能なプロトコル属性が表示されます。

- RADIUS（IETF）
- RADIUS（Cisco）
- RADIUS（Microsoft）

- RADIUS（Ascend）
- RADIUS（Cisco Airespace）
- RADIUS（Cisco Aironet）
- RADIUS（Cisco BBSM）
- RADIUS（Cisco VPN 3000）
- RADIUS（Cisco VPN 5000）
- RADIUS（Juniper）
- RADIUS（Nortel [Bay Networks]）
- RADIUS（RedCreek）
- RADIUS（US Robotics）
- TACACS+

プロトコル ディクショナリの属性を表示および選択するには、[System Administration] > [Configuration] > [Dictionaries] > [Protocols] を選択してからディクショナリを選択します。

表 18-7 で説明されている使用可能な属性のリストを含む [Dictionary] ページが表示されます。

表 18-7　プロトコルの [Dictionary] ページ

オプション	説明
Attribute	属性の名前
ID	（RADIUS のみ）VSA ID。
Type	属性のデータ型。
Direction	（RADIUS のみ）属性の使用場所として、要求内、応答内、またはその両方を指定します。単一または双方向認証。
Multiple Allowed	（RADIUS のみ）複数の属性を許可します。*multiple allowed* を指定する属性は、1 つの要求または応答で複数回使用可能です。

属性のリストをスクロールするには、矢印を使用します。

ACS 5.4 では、RADIUS ベンダー固有属性（VSA）もサポートされています。事前定義済みの RADIUS VSA のセットを使用できます。ACS Web インターフェイスで追加のベンダーと属性を定義できます。RADIUS VSA は作成、編集、または削除できます。

新しく定義した VSA は、事前定義済みの VSA と同様にポリシー、認可プロファイル、および RADIUS トークン サーバで使用できます。詳細については、以下を参照してください。

- 「RADIUS VSA」（P.A-6）。
- 「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）

RADIUS ベンダー固有属性の作成、複製、および編集

ベンダー固有属性（VSA）を使用すると、ベンダーは RADIUS 属性の機能拡張を作成できます。ベンダーには固有のベンダー番号が割り当てられています。VSA は、サブ属性が含まれる属性です。ACS 5.4 では、RADIUS VSA を作成、複製、または編集できます。次の手順を実行します。

内部で使用される属性の一部は変更できません。

属性がポリシーまたはポリシー要素によって使用されている場合は、属性のタイプを変更できません。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS VSA] を選択します。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する RADIUS VSA の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する RADIUS VSA の隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[Create RADIUS VSA] ページが表示されます。表 18-8 で説明されているフィールドを変更します。

表 18-8　RADIUS VSA：作成、複製、編集ページ

オプション	説明
Attribute	RADIUS VSA の名前。
Description	（任意）RADIUS VSA の簡単な説明。
Vendor ID	RADIUS ベンダーの ID。
Attribute Prefix	（任意）ベンダーのすべての属性が同じプレフィックスで始まるように、RADIUS 属性にプリペンドするプレフィックス。
Use Advanced Vendor Options	
Vendor Length Field Size	VSA の長さを指定するための 8 ビットのベンダー長フィールド。VSA のベンダー長を選択します。有効なオプションは 0 と 1 です。デフォルト値は、1 です
Vendor Type Field Size	8 ビットのベンダー タイプ フィールド。VSA のベンダー タイプを選択します。有効なオプションは 1、2、および 4 です。デフォルト値は、1 です

ステップ 3　[Submit] をクリックして変更を保存します。

関連トピック

「RADIUS 属性と TACACS+ 属性の表示」（P.18-5）

RADIUS ベンダー固有サブ属性の作成、複製、および編集

RADIUS ベンダー固有サブ属性を作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS] > [RADIUS VSA] を選択します。

または、ナビゲーション ペインから [RADIUS VSA] を選択することもできます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックして、この RADIUS VSA のサブ属性を作成します。
- 複製する RADIUS VSA の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

- 編集する RADIUS VSA の隣にあるチェックボックスをオンにし、[Edit] をクリックします。

RADIUS VSA サブ属性の作成ページが表示されます。

ステップ 3　表 18-9 で説明されているフィールドに入力します。

表 18-9　RADIUS サブ属性の作成、複製、および編集

オプション	説明
General	
Attribute	サブ属性の名前。名前は一意である必要があります。
Description	（任意）サブ属性の簡単な説明。
RADIUS Configuration	
Vendor Attribute ID	サブ属性のベンダー ID フィールドを入力します。この値は、このベンダーに固有である必要があります。
Direction	属性の使用場所として、要求内、応答内、またはその両方を指定します。単一または双方向認証。
Multiple Allowed	複数の属性を許可します。*multiple allowed* を指定する属性は、1 つの要求または応答で複数回使用可能です。
Include attribute in the log	サブ属性をログに含める場合にオンにします。慎重に扱う必要がある属性の場合は、このチェックボックスをオフにして、属性がロギングされないようにすることができます。
Attribute Type	
Attribute Type	属性のタイプ。有効なオプションは次のとおりです。 • String • Unsigned Integer 32 • IPv4 Address • HEX String • [Enumeration]：このオプションを選択した場合は、ID-Value ペアを入力する必要があります。 ポリシー条件では、HEX String タイプの属性を使用できません。

表 18-9　RADIUS サブ属性の作成、複製、および編集 （続き）

オプション	説明
ID-Value	（任意）*Enumeration 属性タイプの場合のみ。* • [ID] : 0 ～ 999 の数字を入力します。 • [Value] : ID の値を入力します。 • [Add] をクリックして、この ID-Value ペアを ID-Value テーブルに追加します。 ID-Value ペアを編集、置換、および削除するには、次の手順を実行します。 • ID-Value テーブルから ID-Value ペアを選択します。 • [ID] および [Value] フィールドを編集するには、[Edit] をクリックします。必要に応じてフィールドを編集します • フィールドを変更したあとで新しいエントリを追加するには、[Add] をクリックします。 • 同じエントリを異なる値で置換するには、[Replace] をクリックします。 • ID-Value テーブルからエントリを削除するには、[Delete] をクリックします。
Attribute Configuration	
Add Policy Condition	このサブ属性を使用するポリシー条件を入力する場合にオンにします。
Policy Condition Display Name	このサブ属性を使用するポリシー条件の名前を入力します。

ステップ 4　[Submit] をクリックしてサブ属性を保存します。

RADIUS ベンダー固有サブ属性の表示

特定の RADIUS ベンダーでサポートされている属性を表示するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS] > [RADIUS VSA] を選択します。

[RADIUS VSA] ページが表示されます。

ステップ 2　属性を表示するベンダーの隣にあるチェックボックスをオンにし、[Show Vendor Attributes] をクリックします。

ベンダー固有属性および表 18-7 に示されているフィールドが表示されます。追加の VSA を作成したり、これらの属性を複製または編集したりできます。詳細については、「RADIUS ベンダー固有サブ属性の作成、複製、および編集」（P.18-7）を参照してください。

関連項目

「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）

ID ディクショナリの設定

ここでは、次の内容について説明します。

- 「内部ユーザ ID 属性の作成、複製、および編集」（P.18-10）
- 「内部ユーザ ID 属性の削除」（P.18-12）
- 「内部ホスト ID 属性の作成、複製、および編集」（P.18-13）
- 「内部ホスト ID 属性の作成、複製、および編集」（P.18-13）
- 「内部ホスト ID 属性の削除」（P.18-13）

内部ユーザ ID 属性の作成、複製、および編集

内部ユーザ ID 属性を作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] を選択します。

[Internal Users] ページに [Attributes] リストが表示されます。

ステップ 2　次のアクションのいずれかを実行します。

- [Create] をクリックします。
- 複製する属性の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する属性名をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

[Identity Attribute Properties] ページが表示されます。

ステップ 3　必要に応じて、[Identity Attributes Properties] ページのフィールドを変更します。フィールドの説明については、「内部 ID 属性の設定」（P.18-11）を参照してください。

ステップ 4　[Submit] をクリックします。

内部ユーザ属性の設定が保存されます。[Internal Users] ページの [Attributes] リストが新しい属性設定で表示されます。

関連トピック

- 「内部ユーザ ID 属性の削除」（P.18-12）
- 「内部ホスト ID 属性の作成、複製、および編集」（P.18-13）
- 「ポリシーおよび ID 属性」（P.3-17）

内部 ID 属性の設定

表 18-10 に、内部 <*users* | *hosts*> ID 属性のフィールドを示します。

表 18-10　[Identity Attribute Properties] ページ

オプション	説明
General	
Attribute	属性の名前
Description	属性の説明。
Attribute Type	
Attribute Type	（任意）ドロップダウン リスト ボックスを使用して、属性タイプを選択します。有効なオプションは次のとおりです。 • String：ページの [Maximum Length] フィールドと [Default Value] フィールドにデータが読み込まれます。属性タイプとして [String] を選択し、ヌル以外の値をユーザに入力すると、そのユーザはすでに設定されている値に一致する名前で ID ストアに対して、ユーザの詳細に示されている属性について認証されます（ACS-RESERVED-Authen-ID-Store）。 • Unsigned Integer 32：ページの [Valid Range From] フィールドと [Valid Range To] フィールドにデータが読み込まれます。 • [IP Address]：ページの [Default Value] フィールドにデータが読み込まれます。これは、IPv4 または IPv6 アドレスにできます。 • Boolean：ページの [Default Value] チェックボックスにデータが読み込まれます。Boolean 属性の値を true に設定すると、パスワードの有効期限ポリシーのグローバル設定を上書きし、ポリシーを非アクティブ化します（ACS-RESERVED-Never-Expired）。 • Date：ページの [Default Value] フィールドにデータが読み込まれ、カレンダー アイコンが表示されます。 • Enumeration：[ID] フィールドと [Value] フィールドにデータが読み込まれ、[Add]、[Edit]、[Replace]、および [Delete] ボタンが表示されます。
Maximum Length	（任意）*String 属性タイプの場合のみ*。属性の最大長を入力します。有効な範囲は 1 ～ 256 です（デフォルト = 32）。
Value Range	（任意）*Unsigned Integer 属性タイプの場合のみ*。 • From：受け入れられる最小整数値を入力します。有効な範囲は 0 ～ 2^31-1（2147483647）です。この値には、[Valid Range To] の値よりも小さい値を指定する必要があります。 • To：受け入れられる最大整数値を入力します。有効な範囲は 0 ～ 2^31-1（2147483647）です。この値には、[Valid Range From] の値よりも大きい値を指定する必要があります。

表 18-10　[Identity Attribute Properties] ページ （続き）

オプション	説明
Default Value	属性のデフォルト値を入力します。 • [String]：最大長まで （UTF-8 標準に従います）。a ～ z の文字、A ～ Z の文字、および 0 ～ 9 の数字を使用できます。 • [Unsigned Integer] 32：0 ～ 2^31-1（2147483647）の範囲の整数。 • [IP Address]：この属性に関連付ける IP アドレスを次の形式で入力します。 – IPv4 アドレス：*x.x.x.x*、ここで *x.x.x.x* は IPv4 アドレス（サブネット マスクなし） – IPv6 アドレス：*x:x:x:x:x:x:x:x*、ここで *x:x:x:x:x:x:x:x* は IPv6 アドレス（サブネット マスクなし） • [Date]：カレンダー アイコンをクリックして、表示されるカレンダーのポップアップで日付を選択します。 • [Boolean Value]：[True] または [False] を選択します。
ID-Value	（任意）*Enumeration 属性タイプの場合のみ。* • [ID]：0 ～ 999 の数字を入力します。 • [Value]：ID の値を入力します。 • [Add] をクリックして、この ID-Value ペアを ID-Value テーブルに追加します。 ID-Value ペアを編集、置換、および削除するには、次の手順を実行します。 • ID-Value テーブルから ID-Value ペアを選択します。 • [ID] および [Value] フィールドを編集するには、[Edit] をクリックします。必要に応じてフィールドを編集します • フィールドを変更したあとで新しいエントリを追加するには、[Add] をクリックします。 • 同じエントリを異なる値で置換するには、[Replace] をクリックします。 • ID-Value テーブルからエントリを削除するには、[Delete] をクリックします。
Attribute Configuration	
Mandatory Fields	この属性を [User Properties] ページの要件にする場合にオンにします。
Add Policy Condition	この属性からカスタム条件を作成する場合にオンにします。このオプションをオンにした場合は、[Policy Condition Display Name] フィールドに名前を入力する必要があります。
Policy Condition Display Name	ポリシー条件の名前を入力します。このページを送信すると、[Policy Elements] > [Session Conditions] > [Custom] ページに条件が表示されます。

内部ユーザ ID 属性の削除

内部ユーザ ID 属性を削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] を選択します。

[Internal Users] ページに [Attributes] リストが表示されます。

ステップ 2　削除する属性の隣にあるチェックボックスをオンにします。

ID 属性を削除すると処理に時間がかかる可能性があるため、削除できるのは一度に 1 つの属性だけです。

ステップ 3　[Delete] をクリックします。

ステップ 4　確認のため [OK] または [Cancel] をクリックします。

[Internal Users] ページに [Attributes] リストが表示されます。このとき、削除された属性は表示されません。

関連トピック

- 「内部ユーザ ID 属性の作成、複製、および編集」（P.18-10）
- 「ポリシーおよび ID 属性」（P.3-17）

内部ホスト ID 属性の作成、複製、および編集

内部ホスト ID 属性を作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Hosts] を選択します。

[Internal Hosts] ページに [Attributes] リストが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する属性の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する属性名をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

[Identity Attribute Properties] ページが表示されます。

ステップ 3　必要に応じて、[Identity Attributes Properties] ページのフィールドを変更します。フィールドの説明については、表 18-10 を参照してください。

ステップ 4　[Submit] をクリックします。

内部ホスト属性の設定が保存されます。[Internal Hosts] ページの [Attributes] リストが新しい属性設定で表示されます。

関連トピック

- 「内部ホスト ID 属性の削除」（P.18-13）
- 「ポリシーおよび ID 属性」（P.3-17）

内部ホスト ID 属性の削除

内部ホスト ID 属性を削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal User] を選択します。

[Internal Hosts] ページに [Attributes] リストが表示されます。

ステップ 2　削除する属性の隣にあるチェックボックスをオンにします。

属性を削除すると処理に時間がかかる可能性があるため、削除できるのは一度に 1 つの属性だけです。

ステップ 3　[Delete] をクリックします。

ステップ 4　確認のため [OK] または [Cancel] をクリックします。

[Internal Hosts] ページに [Attributes] リストが表示されます。このとき、削除された属性は表示されません。

関連トピック

- 「内部ホスト ID 属性の作成、複製、および編集」（P.18-13）
- 「ポリシーおよび ID 属性」（P.3-17）

[Internal Identity Store] でのユーザへのスタティック IP アドレスの追加

[Internal Identity Store] でユーザにスタティック IP アドレスを追加するには、次の手順を実行します。

ステップ 1　内部ユーザ属性ディクショナリにスタティック IP アドレスを追加するには、次の手順を実行します。

ステップ 2　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] を選択します。

ステップ 3　[Create] をクリックします。

ステップ 4　スタティック IP 属性を追加します。

ステップ 5　[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択します。

ステップ 6　[Create] をクリックします。

ステップ 7　ユーザのスタティック IP 属性を編集します。

ローカル サーバ証明書の設定

ローカル サーバ証明書は、ACS サーバ証明書とも呼ばれます。ACS は、ローカル サーバ証明書によってクライアントに識別されます。ローカル サーバ証明書は次のプロトコルまたはインターフェイスによって使用されます。

- SSL/TLS トンネリングを使用する EAP プロトコル
- Web インターフェイス（GUI）を認証する管理インターフェイス

ここでは、次の内容について説明します。

- 「ローカル サーバ証明書の追加」（P.18-15）
- 「サーバ証明書のインポートおよびプロトコルとの関連付け」（P.18-16）
- 「自己署名証明書の生成」（P.18-16）
- 「証明書署名要求の生成」（P.18-17）
- 「CA 署名付き証明書のバインド」（P.18-18）
- 「証明書の編集と更新」（P.18-19）
- 「証明書の削除」（P.18-20）

- 「証明書のエクスポート」（P.18-20）
- 「未処理の署名要求の表示」（P.18-21）

ローカル サーバ証明書の追加

ACS サーバ証明書とも呼ばれるローカル サーバ証明書を追加すると、クライアントで ACS サーバが識別されます。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

[Local Certificates] ページが表示され、表 18-11 の情報が表示されます。

表 18-11　[Local Certificates] ページ

オプション	説明
Friendly Name	証明書に関連付けられている名前。
Issued To	証明書の発行先エンティティ。名前は、証明書のサブジェクトから表示されます。
Issued By	証明書を発行した信頼できるパーティ。
Valid From	証明書の有効開始日。
Valid To (Expiration)	証明書の有効期限日。
Protocol	証明書に関連付けられているプロトコル。

ステップ 2　[Add] をクリックします。

ステップ 3　表 18-12 の説明に従って、[Local Certificate Store Properties] ページに情報を入力します。

表 18-12　[Local Certificate Store Properties] ページ

オプション	説明
Import Server Certificate	クライアント マシンでローカル証明書ファイルを参照し、秘密キーと秘密キーのパスワードをインポートする場合に選択します。「サーバ証明書のインポートおよびプロトコルとの関連付け」（P.18-16）を参照してください。 サポートされている証明書形式には、CER、DER、PEM、Microsoft 秘密キーの独自の形式などがあります。
Generate Self Signed Certificate	自己署名証明書を生成する場合に選択します。「自己署名証明書の生成」（P.18-16）を参照してください。
Generate Certificate Signing Request	証明書署名要求を生成する場合に選択します。「証明書署名要求の生成」（P.18-17）を参照してください。
Bind CA Signed Certificate	CA 証明書をバインドする場合に選択します。RA が要求に署名したあと、返された署名付き証明書を ACS にインストールし、証明書を対応する秘密キーにバインドできます。「CA 署名付き証明書のバインド」（P.18-18）を参照してください。

サーバ証明書のインポートおよびプロトコルとの関連付け

サポートされている証明書形式は、DER または PEM です。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Import Server Certificate] > [Next] を選択します。

ステップ 3　表 18-13 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-13　[Import Server Certificate] ページ

オプション	説明
Certificate File	クライアント マシンでローカル証明書ファイルを参照する場合に選択します。
Private Key File	秘密キーの場所を参照する場合に選択します。
Private Key Password	秘密キーのパスワードを入力します。値の最小長は 0、最大長は 256 です。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）に証明書を関連付ける場合にオンにします。
Management Interface	管理インターフェイスに証明書を関連付ける場合にオンにします。
Allow Duplicate Certificates	同じ CN および同じ SKI を持ち有効開始日、有効期限日、およびシリアル番号が異なる証明書を追加できます。
Override Policy	
Replace Certificate	既存の証明書の内容を、インポートする内容で置き換えるが、既存のプロトコル選択を保持する場合にオンにします。

ステップ 4　[Finish] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

自己署名証明書の生成

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Generate Self Signed Certificate] > [Next] を選択します。

ステップ 3　表 18-14 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-14　自己署名証明書の生成ステップ 2

オプション	説明
Certificate Subject	この要求の生成中に入力された証明書のサブジェクト。[Certificate Subject] フィールドには、英数字を入力できます。最大文字数は 1024 です。このフィールドには、「cn=」というプレフィックスが付けられます。
Key Length	この要求の生成中に入力されたキーの長さ。値は 512、1024、2048、または 4096 です。
Digest to Sign with	ドロップダウン リストから、管理証明書として [SHA1] または [SHA256] を選択します。
Expiration TTL	最大値（正の整数）を日、週、月、および年の単位で選択します。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）に証明書を関連付ける場合にオンにします。
Management Interface	管理インターフェイスに証明書を関連付ける場合にオンにします。
Allow Duplicate Certificates	同じ CN および同じ SKI を持ち有効開始日、有効期限日、およびシリアル番号が異なる証明書を追加できます。
Override Policy	
Replace Certificate	既存の証明書の内容を、インポートする内容で置き換えるが、既存のプロトコル選択を保持する場合にオンにします。

ステップ 4　[Finish] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

証明書署名要求の生成

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Generate Certificate Signing Request] > [Next] を選択します。

ステップ 3　表 18-15 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-15　署名要求の 生成ステップ 2

オプション	説明
Certificate Subject	この要求の生成中に入力された証明書のサブジェクト。[Certificate Subject] フィールドには、英数字を入力できます。最大文字数は 1024 です。このフィールドには、「cn=」というプレフィックスが付けられます。
Key Length	この要求の生成中に入力されたキーの長さ。値は 512、1024、2048、または 4096 です。
Digest to Sign with	ドロップダウン リストから、管理証明書として [SHA1] または [SHA256] を選択します。

ステップ 4　[Finish] をクリックします。

次のメッセージが表示されます。

```
A server certificate signing request has been generated and can be viewed in the
"Outstanding Signing Requests" list.
```

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

CA 署名付き証明書のバインド

このページは、CA 署名付き証明書を CA からの証明書の取得に使用された要求にバインドする場合に使用します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Bind CA Signed Certificate] > [Next] を選択します。

ステップ 3　表 18-16 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-16　CA 署名付き証明書のバインド ステップ 2

オプション	説明
Certificate File	クライアント マシンを参照し、インポートする証明書を選択します。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）に証明書を関連付ける場合にオンにします。
Management Interface	管理インターフェイスに証明書を関連付ける場合にオンにします。
Allow Duplicate Certificates	同じ CN および同じ SKI を持ち有効開始日、有効期限日、およびシリアル番号が異なる証明書を追加できます。
Override Policy	
Replace Certificate	既存の証明書の内容を、インポートする内容で置き換えるが、既存のプロトコル選択を保持する場合にオンにします。

ステップ 4　[Finish] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

関連トピック

- 「ローカル サーバ証明書の設定」（P.18-14）
- 「証明書ベースのネットワーク アクセス」（P.4-10）

証明書の編集と更新

既存の自己署名証明書は、削除したり新しい証明書を追加したりしなくても更新できます。これにより、ローカル証明書を使用するサービスは中断されることなく処理を続行できます。ローカル サーバ証明書を更新または延長するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

ステップ 2　変更する名前をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

ステップ 3　表 18-17 の説明に従って、証明書のプロパティを入力します。

表 18-17　[Edit Certificate Store Properties] ページ

オプション	説明
Issuer	
Friendly Name	証明書に関連付けられている名前。
Description	証明書の説明。
Issued To	*表示のみ。*証明書の発行先エンティティ。名前は、証明書のサブジェクトから表示されます。
Issued By	*表示のみ。*証明書を発行した認証局。
Valid From	*表示のみ。*証明書の有効開始日。X509 証明書は、開始日から終了日までの間（両方の日を含む）だけ有効です。
Valid To (Expiration)	*表示のみ。*証明書の有効最終日。
Serial Number	*表示のみ。*証明書のシリアル番号。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）でローカル証明書を使用する場合にオンにします。
Management Interface	ACS で SSL クライアント認証にローカル証明書を使用する場合にオンにします。
Renew Self Signed Certificate	
Certificate Expires On	*表示のみ。*証明書の期限が切れる日。
Renew Self Signed Certificate	期限切れの自己署名証明書の更新を許可する場合に選択します。
Expiration TTL	既存の証明書を延長する日数、月数、週数、または年数。有効なオプションは、[one day]、[one month]、[one week]、および [one year] です。 証明書は最大で 1 年間延長できます。

ステップ 4　[Submit] をクリックして、既存の証明書の有効期間を延長します。

編集した証明書が含まれた [Local Certificate Store] ページが表示されます。

関連項目

- 「ローカル サーバ証明書の設定」（P.18-14）

証明書の削除

証明書を削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

ステップ 2　削除する証明書の隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

ステップ 4　確認のため [Yes] または [Cancel] をクリックします。

[Certificate Store] ページが表示されます。このとき、削除した証明書は表示されません。

関連項目

- 「ローカル サーバ証明書の設定」（P.18-14）

証明書のエクスポート

証明書をエクスポートするには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

ステップ 2　エクスポートする証明書の隣にあるチェックボックスをオンにし、[Export] をクリックします。

[Export Certificate] ダイアログボックスが表示されます。

ステップ 3　次のオプションのいずれかを選択します。

- Export Certificate Only
- Export Certificate and Private Key

ステップ 4　[Private Key Password] フィールドに、秘密キーのパスワードを入力します。

ステップ 5　[Confirm Password] フィールドに同じパスワードを入力します。

（注）　秘密キーのエクスポートは、安全な操作ではありません。秘密キーが公開される可能性があるからです。

ステップ 6　[OK] または [Cancel] をクリックします。

関連項目

- 「ローカル サーバ証明書の設定」（P.18-14）

未処理の署名要求の表示

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Outstanding Signing Request] を選択します。

[Certificate Signing Request] ページが表示され、表 18-18 で説明されている情報が表示されます。

表 18-18　[Certificate Signing Request] ページ

オプション	説明
Name	証明書の名前。
Certificate Subject	この要求の生成中に入力された証明書のサブジェクト。[Certificate Subject] フィールドには、英数字を入力できます。最大文字数は 1024 です。このフィールドには、自動的に「cn=」というプレフィックスが付けられます。
Key Length	この要求の生成中に入力されたキーの長さ。値は 512、1024、2048、または 4096 です。
Timestamp	証明書が作成された日付。
Friendly Name	証明書に関連付けられている名前。

ステップ 2　[Export] をクリックして、ローカル証明書をクライアント マシンにエクスポートします。

ログの設定

次のメッセージのログ レコードが生成されます。

- アカウンティング メッセージ
- AAA 監査および診断メッセージ
- システム診断メッセージ
- 管理および操作の監査メッセージ

メッセージはツリー階層構造のロギング カテゴリ内に配置されます（「ロギング カテゴリの設定」（P.18-24）を参照）。

ログ メッセージは、ロギング カテゴリおよびメンテナンス パラメータに基づいてローカルまたはリモートに格納できます。

ここでは、次の内容について説明します。

- 「リモート ログ ターゲットの設定」（P.18-22）
- 「ローカル ログの設定」（P.18-24）
- 「ロギング カテゴリの設定」（P.18-24）
- 「グローバル ロギング カテゴリの設定」（P.18-25）
- 「インスタンスごとのロギング カテゴリの設定」（P.18-30）
- 「ロギング カテゴリの表示」（P.18-33）
- 「ログ コレクタの設定」（P.18-34）
- 「ログ メッセージ カタログの表示」（P.18-34）

事前に定義されたグローバルな ACS ロギング カテゴリおよび各カテゴリに含まれるメッセージについては、第 19 章「ロギングの概要」を参照してください。

リモート ログ ターゲットの設定

特定のロギング カテゴリのロギング メッセージを受信するように特定のリモート ログ ターゲット（syslog サーバ上だけ）を設定できます。リモート ログ ターゲットの詳細については、第 19 章「ロギングの概要」を参照してください。事前に設定された ACS ロギング カテゴリの詳細については、「ロギング カテゴリの設定」（P.18-24）を参照してください。

新しいリモート ログ ターゲットを作成するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Remote Log Targets] を選択します。

[Remote Log Targets] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するリモート ログ ターゲットの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するリモート ログ ターゲットの名前をクリックします。または、変更するリモート ログ ターゲットの名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

次のいずれかのページが表示されます。

- 新しいリモート ログ ターゲットを作成する場合は、[Remote Log Targets] > [Create]。
- リモート ログ ターゲットを複製する場合は、[Remote Log Targets] > [Duplicate: "*log_target*"]。*log_target* は、ステップ 2 で選択したリモート ログ ターゲットの名前です。
- リモート ログ ターゲットを変更する場合は、[Remote Log Targets] > [Edit: "*log_target*"]。*log_target* は、ステップ 2 で選択したリモート ログ ターゲットの名前です。

ステップ 3　表 18-19 の説明に従って、必須フィールドに入力します。

表 18-19　リモート ログ ターゲットの設定ページ

オプション	説明
General	
Name	リモート ログ ターゲットの名前。名前の最大長は 32 文字です。
Description	リモート ログ ターゲットの説明。説明の最大長は 1024 文字です。
Type	リモート ログ ターゲットのタイプ：[Syslog]（唯一のオプション）。
Target Configuration	
IP Address	リモート ログ ターゲットの IP アドレス（*x.x.x.x* の形式）。
Use Advanced Syslog Options	高度な syslog オプション（ポート番号、ファシリティ コード、および最大長）をイネーブルにする場合にクリックします。
Port	ACS とリモート ログ ターゲット間の通信チャネルとして使用されるリモート ログ ターゲットのポート番号（デフォルト = 514）。このオプションは、[Use Syslog Options] をクリックした場合にだけ表示されます。

表 18-19　リモート ログ ターゲットの設定ページ （続き）

オプション	説明
Facility Code	ファシリティ コード。有効なオプションは次のとおりです。 • LOCAL0（コード = 16） • LOCAL1（コード = 17） • LOCAL2（コード = 18） • LOCAL3（コード = 19） • LOCAL4（コード = 20） • LOCAL5（コード = 21） • LOCAL6（コード = 22、デフォルト） • LOCAL7（コード = 23） このオプションは、[Use Advanced Syslog Options] をクリックした場合にだけ表示されます。
Maximum Length	リモート ログ ターゲット メッセージの最大長。有効なオプションは 200 ～ 1024 です。このオプションは、[Use Advanced Syslog Options] をクリックした場合にだけ表示されます。

ステップ 4　[Submit] をクリックします。

リモート ログ ターゲット設定が保存されます。新しいリモート ログ ターゲット設定が示された [Remote Log Targets] ページが表示されます。

関連項目

- 「リモート ログ ターゲットの削除」（P.18-23）

リモート ログ ターゲットの削除

リモート ログ ターゲットを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Remote Log Targets] を選択します。

設定されているリモート ログ ターゲットのリストを含む [Remote Log Targets] ページが表示されます。

ステップ 2　削除するリモート ログ ターゲットの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のエラー メッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[Remote Log Targets] ページが表示されます。このとき、削除したリモート ログ ターゲットは表示されません。

関連項目

- 「リモート ログ ターゲットの設定」（P.18-22）

ローカル ログの設定

ローカル ログ データを保持する最大日数を設定するには、[Local Configuration] ページを使用します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Local Log Target] を選択します。

[Local Configuration] ページが表示されます。

ステップ 2　[Maximum log retention period] ボックスに、ローカル ログ メッセージ ファイルを保管する日数を入力します。<*num*> は入力する日数です。有効なオプションは 1 ～ 365 です （デフォルト = 7）。

（注）　ローカル ログ メッセージ ファイルを保管する日数を減らすと、指定した日数より古いログ メッセージ ファイルは自動的に削除されます。

[Delete Logs Now] をクリックすると、すべての非アクティブなログ ファイルなど、ローカル ログをすぐに削除できます。ログ データの削除の詳細については、「ローカル ログ データの削除」（P.18-24）を参照してください。

ステップ 3　[Submit] をクリックして変更を保存します。

設定が保存され、[Local Configuration] ページが更新されます。

ローカル ログ データの削除

ローカル ログ データを手動で削除するには、[Local Configuration] ページを使用します。この方法を使用して、ローカル ストアがいっぱいになったときに容量を解放できます。ローカル ストアの詳細については、「ローカル ストア ターゲット」（P.19-5）を参照してください。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Local Log Target] を選択します。

[Local Configuration] ページが表示されます。

ステップ 2　[Delete Logs Now] をクリックすると、現在アクティブなログ データ ファイル内のログ データを除くすべてのローカル ログ データ ファイルがすぐに削除されます。

[Local Configuration] ページが更新されます。

ロギング カテゴリの設定

ここでは、次の内容について説明します。

- 「グローバル ロギング カテゴリの設定」（P.18-25）
- 「インスタンスごとのロギング カテゴリの設定」（P.18-30）

親ロギング カテゴリに対して実行されたすべての設定は、そのロギング カテゴリ内の子に影響します。親ロギング カテゴリの子を選択して、個別に設定できます。その子に対する設定は、親ロギング カテゴリまたは他の子に影響しません。

グローバル ロギング カテゴリの設定

グローバル ロギング カテゴリを表示および設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] を選択します。

[Logging Categories] ページが表示されます。このページから、ロギング カテゴリを参照できます。

ステップ 2　設定するロギング カテゴリの名前をクリックします。または、設定するロギング カテゴリの隣にあるオプション ボタンをクリックして [Edit] をクリックします。

ステップ 3　表 18-20 の説明に従って、フィールドに入力します。

表 18-20　[Global: General] ページ

オプション	説明
Configure Log Category	
Log Severity	診断ロギング カテゴリの場合、ドロップダウン リスト ボックスを使用して、重大度レベルを選択します （監査およびアカウンティング カテゴリの場合、重大度は NOTICE だけであり、変更できません）。有効なオプションは次のとおりです。 • [FATAL]：緊急事態。ACS が使用できないため、すぐに対応する必要があります。 • [ERROR]：重大またはエラー状況。 • [WARN]：通常だが、重要な状況 （デフォルト） • [INFO]：通知メッセージ。 • [DEBUG]：診断バグ メッセージ。

表 18-20　[Global: General] ページ （続き）

オプション	説明
Configure Local Setting for Category	
Log to Local Target	ローカル ターゲットへのロギングをイネーブルにする場合にオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、ローカル ターゲットへのロギングはデフォルトでイネーブルであり、ディセーブルにすることはできません。
Local Target is Critical	*アカウンティングおよびAAA 監査（Passed Authentication）ロギング カテゴリ タイプの場合だけ使用できます。*このローカル ターゲットを重大なターゲットにする場合に、このチェックボックスをオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、このチェックボックスはデフォルトでオンであり、オフにすることはできません。このローカル ターゲットは重大なターゲットです。
Configure Logged Attributes	
—	*表示のみ。*すべての属性は、ローカル ターゲットにロギングされます。

設定が完了したら、ステップ 6 に進みます。

ステップ 4　リモート syslog ターゲットを設定するには、[Remote Syslog Target] をクリックし、ステップ 5 に進みます。

ステップ 5　表 18-21 の説明に従って、リモート syslog ターゲットのフィールドに入力します。

表 18-21　[Global: Remote Syslog Target] ページ

オプション	説明
Configure Syslog Targets	
Available targets	使用できるターゲットのリスト。このリストからターゲットを選択して、[Selected Targets] リストに移動できます。
Selected targets	選択されているターゲットのリスト。このリストからターゲットを選択して、[Available Targets] リストに移動し、設定から削除できます。

ステップ 6　[Submit] をクリックします。

設定したロギング カテゴリが示された [Logging Categories] ページが表示されます。

管理および操作の監査メッセージには、次のタイプの監査メッセージが含まれます。

- 設定変更
- 内部ユーザのパスワード変更
- 管理者アクセス
- 操作の監査

操作の監査メッセージの一部は、ローカル ログ ターゲットにロギングされません。ローカル ターゲットにロギングされない管理および操作のログのリストについては、表 18-22 を参照してください。ACS CLI からこれらのログを表示する方法については、「ADE-OS ログの表示」（P.18-29）を参照してください。

表 18-22 に、ローカル ターゲットにロギングされない管理および操作のログのセットをカテゴリ別に示します。

表 18-22　ローカル ターゲットにロギングされない管理および操作のログ

カテゴリ	ログと説明
Process-Management	• ACS_START_PROCESS：ACS プロセスが開始しました。 • ACS_STOP_PROCESS：ACS プロセスが停止しました。 • ACS_START：すべての ACS プロセスが開始しました。 • ACS_STOP：すべての ACS プロセスが停止しました。 • WD_RESTART_PROCESS：ACS プロセスがウォッチドッグによって再起動されました。 • WD_CONFIG_CHANGE：ウォッチドッグ設定がリロードされました。 • ACS_START_STOP_ERROR：ACS プロセスによって開始/停止エラーが報告されました。
DB-Management	• CARS_BACKUP：CARS バックアップが完了しました。 • CARS_RESTORE：CARS 復元が完了しました。 • ACS_BACKUP：ACS DB バックアップが完了しました。 • ACS_RESTORE：ACS DB 復元が完了しました。 • ACS_SUPPORT：ACS サポート バンドルが収集されました。 • ACS_RESET：ACS DB がリセットされました。
File-Management	• ACS_DELETE_CORE：ACS コア ファイルが削除されました。 • ACS_DELETE_LOG：ACS ログ ファイルが削除されました。

表 18-22　ローカル ターゲットにロギングされない管理および操作のログ （続き）

カテゴリ	ログと説明
Software-Management	• ACS_UPGRADE：ACS がアップグレードされました。 • ACS_PATCH：ACS パッチがインストールされました。 • UPGRADE_SCHEMA_CHANGE：ACS スキーマのアップグレードが完了しました。 • UPGRADE_DICTIONARY：ACS ディクショナリのアップグレードが完了しました。 • UPGRADE_DATA_MANIPULATION：ACS アップグレードのデータ処理段階が完了しました。 • UPGRADE_AAC：ACS AAC アップグレードが完了しました。 • UPGRADE_PKI：ACS PKI アップグレードが完了しました。 • UPGRADE_VIEW：ACS ビューのアップグレードが完了しました。 • CLI_ACS_UPGRADE：ACS アップグレードが開始しました。 • CLI_ACS_INSTALL：ACS インストールが開始しました。
System-Management	• ACS_MIGRATION_INTERFACE：ACS 移行インターフェイスがイネーブル/ディセーブルになりました。 • ACS_ADMIN_PSWD_RESET：ACS 管理者パスワードがリセットされました。 • CLI_CLOCK_SET：クロックが設定されました。 • CLI_TZ_SET：タイムゾーンが設定されました。 • CLI_NTP_SET：NTP サーバが設定されました。 • CLI_HOSTNAME_SET：ホスト名が設定されました。 • CLI_IPADDRESS_SET：IP アドレスが設定されました。 • CLI_IPADDRESS_STATE：IP アドレスの状態。 • CLI_DEFAULT_GATEWAY：デフォルト ゲートウェイが設定されました。 • CLI_NAME_SERVER：ネーム サーバが設定されました。 • ADEOS_XFER_LIBERROR：ADE OS Xfer ライブラリ エラー。 • ADEOS_INSTALL_LIBERROR：ADE OS インストール ライブラリ エラー。 • AD_JOIN_ERROR：AD エージェントが AD ドメインに参加できませんでした。 • AD_JOIN_DOMAIN：AD エージェントが AD ドメインに参加しました。 • AD_LEAVE_DOMAIN：AD エージェントが AD ドメインから離脱しました。 • IMPORT_EXPORT_PROCESS_ABORTED：インポート/エクスポート プロセスが中止されました。 • IMPORT_EXPORT_PROCESS_STARTED：インポート/エクスポート プロセスが開始しました。 • IMPORT_EXPORT_PROCESS_COMPLETED：インポート/エクスポート プロセスが完了しました。 • IMPORT_EXPORT_PROCESS_ERROR：インポート/エクスポート プロセス中にエラーが発生しました。

関連項目

- 「インスタンスごとのロギング カテゴリの設定」（P.18-30）

- 「ADE-OS ログの表示」（P.18-29）

ADE-OS ログの表示

表 18-22 に示すログは、ADE-OS ログに書き込まれます。ACS CLI から次のコマンドを使用して ADE-OS ログを表示できます。

show logging system

このコマンドを実行すると、すべての ADE-OS ログが表示されます。出力は次の例のようになります。

```
Sep 29 23:24:15 cd-acs5-13-179 sshd(pam_unix)[20013]: 1 more authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95
user=admin
Sep 29 23:24:34 cd-acs5-13-179 sshd(pam_unix)[20017]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 29 23:24:36 cd-acs5-13-179 sshd[20017]: Failed password for admin from 10.77.137.95
port 3635 ssh2
Sep 30 00:47:44 cd-acs5-13-179 sshd(pam_unix)[20946]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:47:46 cd-acs5-13-179 sshd[20946]: Failed password for admin from 10.77.137.95
port 3953 ssh2
Sep 30 00:54:59 cd-acs5-13-179 sshd(pam_unix)[21028]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:55:01 cd-acs5-13-179 sshd[21028]: Failed password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:35 cd-acs5-13-179 last message repeated 5 times
Sep 30 00:55:39 cd-acs5-13-179 sshd[21028]: Accepted password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:39 cd-acs5-13-179 sshd(pam_unix)[21038]: session opened for user admin by
(uid=0)
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[118] [admin]:
Invoked carsGetConsoleConfig
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[135] [admin]:
No Config file, returning defaults
Sep 30 01:22:20 cd-acs5-13-179 sshd[21038]: Received disconnect from 10.77.137.95: 11:
Connection discarded by broker
Sep 30 01:22:20 cd-acs5-13-179 sshd(pam_unix)[21038]: session closed for user admin
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 02:48:54 cd-acs5-13-179 sshd[22500]: Accepted password for admin from 10.77.137.58
port 4527 ssh2
Sep 30 02:48:54 cd-acs5-13-179 sshd(pam_unix)[22504]: session opened for user admin by
(uid=0)
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
```

所属するモジュールでグループ化されたログを表示できます。たとえば、モニタリングおよびトラブルシューティング ログには文字列 **MSGCAT** が含まれ、デバッグ ログには文字列 **debug** が含まれています。

ACS CLI で次の 2 つのコマンドを入力して、モニタリングおよびトラブルシューティング ログと管理ログを個別に表示できます。

- **show logging system | include MSGCAT**
- **show logging system | include debug**

show logging system | include MSGCAT の出力は次のようになります。

```
Sep 27 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 28 13:00:03 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 06:28:17 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 8363
Sep 29 06:28:28 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 06:31:41 cd-acs5-13-103 MSGCAT58037/admin: Installing ACS
Sep 29 09:52:35 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 32729
Sep 29 09:52:46 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 09:53:29 cd-acs5-13-103 MSGCAT58004/admin: ACS Starting
Sep 29 10:37:45 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 29 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 13:56:36 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:02 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:25 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 30 10:57:10 cd-acs5-13-103 MSGCAT58010/admin: info:[ACS backup] ACS backup completed
```

show logging コマンドの詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli_app_a.html#wp1917127

インスタンスごとのロギング カテゴリの設定

特定の上書きされる ACS インスタンスのカスタム ロギング カテゴリ設定を定義したり、すべてのインスタンスをデフォルトのグローバル ロギング カテゴリ設定に戻したりできます。

インスタンスごとのロギング カテゴリを表示および設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択します。

[Per-Instance] ページが表示されます。このページで、展開された個別の ACS インスタンスを表示できます。

ステップ 2　設定する ACS インスタンスの名前に関連付けられているオプション ボタンを選択し、次のいずれかのオプションを選択します。

- 選択した ACS インスタンスの現在のロギング カテゴリ設定を上書きするには、[Override] をクリックします。
- ACS インスタンスに関連付けられた [Logging Categories] ページを表示するには、[Configure] をクリックします。その後、ACS インスタンスのロギング カテゴリを編集できます。フィールドの説明については、「ロギング カテゴリの表示」（P.18-33）を参照してください。
- 選択した ACS インスタンスをデフォルトのグローバル ロギング カテゴリ設定に戻すには、[Restore to Global] をクリックします。

設定が保存され、[Per-Instance] ページが更新されます。

関連項目

- 「インスタンスごとのセキュリティおよびログの設定」（P.18-31）

インスタンスごとのセキュリティおよびログの設定

特定の上書きされる ACS インスタンスまたはカスタム ACS インスタンスについて、ロギング カテゴリ設定の重大度レベルとローカル ログを設定できます。このページを使用して、次のことを行います。

- 特定の ACS インスタンスに設定されているロギング カテゴリのツリーを表示します。
- 特定の ACS インスタンスについてロギング カテゴリの重大度レベル、ログ ターゲット、およびロギングされる属性を設定するページを開きます。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択し、[Configure] をクリックします。

表 18-23 で説明されている [Per-Instance: Configuration] ページが表示されます。

表 18-23　[Per-Instance: Configuration] ページ

オプション	説明
Name	AAA サービス ロギング カテゴリの展開可能なツリー構造。
Edit	選択したロギング カテゴリの [Edit: "*lc_name*"] ページを表示する場合にクリックします。*lc_name* は、ロギング カテゴリの名前です。

ステップ 2　次のいずれかを実行します。

- 設定するロギング カテゴリの名前をクリックします。
- 設定するロギング カテゴリの名前に関連付けられているオプション ボタンを選択し、[Edit] をクリックします。

[Per-Instance: General] ページが表示されます。

このページで、特定の ACS インスタンスについてロギング カテゴリ設定のセキュリティ レベルとローカル ログを設定できます。表 18-24 を参照してください。

表 18-24　[Per-Instance: General] ページ

オプション	説明
Configure Log Category	
Log Severity	リスト ボックスを使用して、診断ロギング カテゴリの重大度レベルを選択します（監査およびアカウンティング カテゴリの場合、重大度は NOTICE だけであり、変更できません）。有効なオプションは次のとおりです。 • [FATAL]：緊急事態。ACS が使用できないため、すぐに対応する必要があります。 • [ERROR]：重大またはエラー状況。 • [WARN]：通常だが、重要な状況 （デフォルト） • [INFO]：通知メッセージ。 • [DEBUG]：診断バグ メッセージ。
Configure Local Setting for Category	
Log to Local Target	ローカル ターゲットへのロギングをイネーブルにする場合にオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、ローカル ターゲットへのロギングはデフォルトでイネーブルであり、ディセーブルにすることはできません。
Local Target is Critical	*アカウンティングおよびPassed Authentication ロギング カテゴリ タイプの場合だけ使用できます。*このローカル ターゲットを重大なターゲットにする場合に、このチェックボックスをオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、このチェックボックスはデフォルトでオンであり、オフにすることはできません。このローカル ターゲットは重大なターゲットです。
Configure Logged Attributes	
—	*表示のみ。*すべての属性は、ローカル ターゲットにロギングされます。

インスタンスごとのリモート syslog ターゲットの設定

このページは、ロギング カテゴリのリモート syslog ターゲットを設定する場合に使用します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択し、[Configure] をクリックします。

表 18-23 で説明されている [Per-Instance: Configuration] ページが表示されます。

ステップ 2　次のいずれか 1 つの処理を実行します。

- 設定するロギング カテゴリの名前をクリックします。
- 設定するロギング カテゴリの名前に関連付けられているオプション ボタンを選択し、[Edit] をクリックします。

ステップ 3　[Remote Syslog Target] タブをクリックします。

表 18-25 で説明されている [Per-Instance: Remote Syslog Targets] ページが表示されます。

表 18-25　[Per-Instance: Remote Syslog Targets] ページ

オプション	説明
Configure Syslog Targets	
Available targets	使用できるターゲットのリスト。このリストからターゲットを選択して、[Selected Targets] リストに移動できます。
Selected targets	選択されているターゲットのリスト。このリストからターゲットを選択して、[Available Targets] リストに移動し、設定から削除できます。

ロギング カテゴリの表示

特定の ACS インスタンスに設定されているロギング カテゴリのツリーを表示できます。また、特定の ACS インスタンスについてロギング カテゴリの重大度レベル、ログ ターゲット、およびロギングされる属性を設定することもできます。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択し、[Configure] をクリックします。

ステップ 2　表 18-26 の説明に従って、フィールドに入力します。

表 18-26　[Per-Instance: Configuration] ページ

オプション	説明
Name	AAA サービス ロギング カテゴリの展開可能なツリー構造。
Edit	選択したロギング カテゴリの [Edit: "*lc_name*"] ページを表示する場合にクリックします。*lc_name* は、ロギング カテゴリの名前です。

ログ コレクタの設定

ログ データ コレクタを選択し、ログ データの送信を一時停止または再開するには、[Log Collector] ページを使用します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Log Collector] を選択します。

[Log Collector] ページが表示されます。

ステップ 2　表 18-27 の説明に従って、[Log Collector] ページのフィールドに入力します。

表 18-27　[Log Collector] ページ

オプション	説明
Log Data Collector	
Current Log Collector	*表示のみ。*ローカル ログ メッセージを送信するマシンを示します。
Select Log Collector	ドロップダウン リスト ボックスを使用して、ローカル ログ メッセージを送信するマシンを選択します。
Set Log Collector	[Select Log Collector] オプションの選択内容に従ってログ コレクタを設定する場合にクリックします。

ステップ 3　次のいずれかを実行します。

- 設定されているログ コレクタへのログ データの送信を一時停止するには、[Suspend] をクリックします。
- 設定されているログ コレクタへのログ データの送信を再開するには、[Resume] をクリックします。

設定が保存され、[Log Collector] ページが更新されます。

ログ メッセージ カタログの表示

[Log Message Catalog] ページは、表示される可能性があるすべてのログ メッセージを表示する場合に使用します。

[System Administration] > [Configuration] > [Log Configuration] > [Log Message Catalog] を選択します。

表 18-28 で説明されているフィールドを含む [Log Message Catalog] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。

表 18-28　[Log Message Catalog] ページ

オプション	説明
Message Code	*表示のみ。*メッセージに関連付けられている固有のメッセージ コード ID 番号。
Severity	*表示のみ。*メッセージに関連付けられている重大度レベル。
Category	*表示のみ。*メッセージが属するロギング カテゴリ。
Message Class	*表示のみ。*メッセージが属するグループ。

表 18-28　[Log Message Catalog] ページ （続き）

オプション	説明
Message Text	*表示のみ*。英語のメッセージ テキスト（メッセージの名前）。
Description	表示のみ。関連付けられているメッセージを説明する英語のテキスト。

ライセンスの概要

ACS を使用するには、有効なライセンスをインストールする必要があります。ACS では、初めて Web インターフェイスにアクセスしたときに、有効な基本ライセンスをインストールするよう求められます。分散展開では、各 ACS インスタンス（プライマリまたはセカンダリ）に固有の基本ライセンスが必要です。

（注）　分散展開では、各サーバに固有の基本ライセンスが必要です。

ライセンスの種類

表 18-29 に、ACS 5.4 のライセンス サポートを示します。

表 18-29　ACS ライセンスのサポート

ライセンス	説明
基本ライセンス	展開されているすべてのソフトウェア インスタンスと、すべてのアプライアンスに必要です。基本ライセンスをインストールすると、ライセンス制御機能を除くすべての ACS 機能を使用できます。また、すべてのレポート機能がイネーブルになります。基本ライセンスの特性は次のとおりです。 • 各 ACS インスタンス（プライマリとセカンダリ）で必要です。 • すべてのアプライアンスで必要です。 • 最大 500 台の管理対象デバイスを使用した展開をサポートします。 基本ライセンスには次の 3 つのタイプがあります。 • 永続：最大 500 台のデバイスをサポートします。 • 評価：最大 50 台のデバイスをサポートし、90 日で有効期限が切れます。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 評価ライセンスの期限が切れた場合、または間もなく切れる場合は、別の評価ライセンスを使用したり現在のライセンスを延長したりすることはできません。評価ライセンスの期限が切れる前に、永続ライセンスにアップグレードする必要があります。

表 18-29　ACS ライセンスのサポート （続き）

ライセンス	説明
アドオン ライセンス	サポートする管理対象デバイスの数に制限はありません。既存の ACS 永続基本ライセンスが必要です。アドオン ライセンスの評価タイプ ライセンスもあります。 Security Group Access 機能ライセンスは 3 種類です（永続、評価、NFR）。ただし、永続 Security Group Access 機能ライセンスは、永続基本ライセンスがある場合だけ使用できます。 大規模展開ライセンスも、永続基本ライセンスがある場合にだけ使用できます。
評価ライセンス（標準）	標準の集中型レポート機能がイネーブルになります。 • 同じプラットフォームでは再利用できません。 • 評価ライセンスは、プラットフォームごとに 1 つだけインストールできます。追加の評価ライセンスはインストールできません。 • 50 台の管理対象デバイスをサポートします。 • ライセンスのインストール時から 90 日間で期限が切れます。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの追加」（P.18-41）
- 「展開ライセンス ファイルの削除」（P.18-42）

ライセンス ファイルのインストール

有効なライセンス ファイルは、製品に付属している Product Activation Key（PAK; プロダクト アクティベーション キー）を使用して取得できます。ライセンス ファイルをインストールするには、次の手順を実行します。

ステップ 1　ACS Web インターフェイスにログインします。

ACS マシンに初めてログインすると、[Initial Licenses] ページが表示されます。

ステップ 2　[Cisco Secure ACS License Registration] をクリックします。

代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。

ステップ 3　[Install] をクリックして、購入したライセンス ファイルをインストールします。

ACS Web インターフェイスのログイン ページが再度表示されます。これで ACS アプリケーションを使用できます。

（注）　基本永続ライセンスはアップグレードできません。アップグレードできるのは基本評価ライセンスだけです。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの追加」（P.18-41）
- 「展開ライセンス ファイルの削除」（P.18-42）

基本ライセンスの表示

基本ライセンスをアップグレードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Base Server License] を選択します。

[Base Server License] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストが示されます。展開ライセンスのリストについては、「ライセンスの種類」を参照してください。

表 18-30 に、[Base Server License] ページのフィールドを示します。

表 18-30　[Base Server License] ページ

オプション	説明
ACS Deployment Configuration	
Primary ACS Instance	ACS 5.4 Web インターフェイスにログインするときに作成されたプライマリ インスタンスの名前。
Number of Instances	ACS データベース内の ACS インスタンス（プライマリまたはセカンダリ）の現在の数。
Current Number of Configured IP Addresses in Network Devices	ネットワーク デバイス設定の一部として設定したすべてのサブネットワーク内の IP アドレスの総数。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。
Maximum Number of IP Addresses in Network Devices	ライセンスでサポートされる IP アドレスの最大数。 • Base License：500 個の IP アドレスをサポートします。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 • Large Deployment：サポートする IP アドレスの数に制限はありません。
Use this link to obtain a valid License File	プロダクト アクティベーション キー（PAK）を使用して有効なライセンス ファイルを生成するために、Cisco.com に移動します。
Base License Configuration	
ACS Instance	ACS インスタンス（プライマリまたはセカンダリ）の名前。
Identifier	基本ライセンスの名前。
License Type	基本ライセンスのタイプ（永続または評価）を指定します。
Expiration	評価ライセンスの有効期限を指定します。永続ライセンスの場合、[Expiration] フィールドに *permanent* と表示されます。
Licensed to	この製品がライセンスされる会社の名前。
PAK	Cisco から受け取ったプロダクト アクティベーション キー（PAK）の名前。
Version	ACS ソフトウェアの現在のバージョン。

ライセンスをアップグレードするインスタンスの隣にあるオプション ボタンを 1 つ以上選択できます。

ステップ 2　[Upgrade] をクリックします。有効なフィールド オプションについては、「基本サーバ ライセンスのアップグレード」（P.18-39）を参照してください。

関連項目

- 「基本サーバ ライセンスのアップグレード」（P.18-39）

基本サーバ ライセンスのアップグレード

基本サーバ ライセンスをアップグレードできます。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Base Server License] を選択します。

[Base Server License] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストが示されます。展開ライセンスのリストについては、「ライセンスの種類」を参照してください。

ステップ 2　ライセンスを選択し、[Upgrade] をクリックします。

[Base Server License Edit] ページが表示されます。

ステップ 3　表 18-31 の説明に従って、フィールドに入力します。

表 18-31　[Base Server License Edit] ページ

オプション	説明
ACS Instance License Configuration	
Version	ACS ソフトウェアの現在のバージョンが表示されます。
ACS Instance	ACS インスタンス（プライマリまたはセカンダリ）の名前が表示されます。
License Type	ライセンス タイプを指定します。
Use this link to obtain a valid License File	代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。
License Location	
License File	[Browse] をクリックして、ライセンス ファイルが格納されているディレクトリに移動し、ファイルを選択します。

ステップ 4　[Submit] をクリックします。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンスの種類」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「展開ライセンス ファイルの追加」（P.18-41）
- 「展開ライセンス ファイルの削除」（P.18-42）

ライセンス機能オプションの表示

既存の展開ライセンスは追加、アップグレード、または削除できます。ページの上部にある設定ペインに、展開情報が表示されます。

[System Administration] > [Configuration] > [Licensing] > [Feature Options] を選択します。

表 18-32 で説明されている [Feature Options] ページが表示されます。

表 18-32　[Feature Options] ページ

オプション	説明
ACS Deployment Configuration	
Primary ACS Instance	ACS 5.4 Web インターフェイスにログインするときに作成されたプライマリ インスタンスの名前。
Number of Instances	ACS データベース内の ACS インスタンス（プライマリまたはセカンダリ）の現在の数。
Current Number of Configured IP Addresses in Network Devices	ネットワーク デバイス設定の一部として設定したすべてのサブネットワーク内の IP アドレスの総数。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。
Maximum Number of IP Addresses in Network Devices	ライセンスでサポートされる IP アドレスの最大数。 • Base License：500 個の IP アドレスをサポートします。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 • Large Deployment：サポートする IP アドレスの数に制限はありません。
Use this link to obtain a valid License File	代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。
Installed Deployment License Options	
Feature	• Large Deployment：サポートする管理対象デバイスの数に制限はありません。 • [Security Group Access Control]：Cisco Trusted Server（SGA）管理機能を有効にします。既存の ACS 基本ライセンスが必要です。
Licensed to	この製品がライセンスされる会社の名前。
License Type	ライセンス タイプ（永続または評価）を指定します。
Expiration	次の機能の有効期限。 • 大規模な導入 • SGA
Add/Upgrade	ライセンス機能オプションの表示にアクセスしたりライセンス ファイルを追加したりするには、[Add/Upgrade] をクリックします。
Delete	削除するライセンス機能の隣にあるオプション ボタンを選択し、[Delete] をクリックします。

展開ライセンス ファイルの追加

新しい基本展開ライセンス ファイルを追加するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Feature Options] を選択します。

[Feature Options] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストとそれらの設定が示されます。展開ライセンスのリストについては、「ライセンスの種類」の「アドオン ライセンス」を参照してください。フィールドの説明については、「ライセンス機能オプションの表示」（P.18-40）を参照してください。

ステップ 2　[Add] をクリックします。

[Feature Options Create] ページが表示されます。

ステップ 3　表 18-33 の説明に従って、フィールドに入力し、ライセンスを追加します。

表 18-33　[Feature Options Create] ページ

オプション	説明
ACS Deployment Configuration	
Primary ACS Instance	ACS 5.4 Web インターフェイスにログインするときに作成されたプライマリ インスタンスの名前。
Number of Instances	ACS データベース内の ACS インスタンス（プライマリまたはセカンダリ）の現在の数。
Current Number of Configured IP Addresses in Network Devices	ネットワーク デバイス設定の一部として設定したすべてのサブネットワーク内の IP アドレスの総数。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。
Maximum Number of IP Addresses in Network Devices	ライセンスでサポートされる IP アドレスの最大数。 • Base License：500 個の IP アドレスをサポートします。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 • Large Deployment：サポートする IP アドレスの数に制限はありません。
Use this link to obtain a valid License File	代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。
License Location	
License File	[Browse] をクリックして、インストールする購入済みライセンス ファイルの場所を参照し、ファイルを選択します。

ステップ 4　[Submit] をクリックしてライセンス ファイルをダウンロードします。

追加ライセンスを含む [Feature Options] ページが表示されます。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンスの種類」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの削除」（P.18-42）

展開ライセンス ファイルの削除

展開ライセンス ファイルを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Feature Options] を選択します。

[Feature Options] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストとそれらの設定が示されます。展開ライセンスのリストについては、「ライセンスの種類」の「アドオン ライセンス」を参照してください。フィールドの説明については、表 18-32 を参照してください。

ステップ 2　削除する展開の隣にあるオプション ボタンを選択します。

ステップ 3　[Delete] をクリックしてライセンス ファイルを削除します。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンスの種類」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの追加」（P.18-41）

使用可能なダウンロード

ここでは、ACS Web インターフェイスからダウンロードできるユーティリティとファイルについて説明します。

- 「移行ユーティリティ ファイルのダウンロード」（P.18-43）
- 「UCP Web サービス ファイルのダウンロード」（P.18-43）
- 「サンプル Python スクリプトのダウンロード」（P.18-43）
- 「Rest サービスのダウンロード」（P.18-44）

移行ユーティリティ ファイルのダウンロード

ACS 5.4 の移行アプリケーション ファイルおよび移行ガイドをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Migration Utility] を選択します。

[Migration from 4.x] ページが表示されます。

ステップ 2　[Migration application files] をクリックして、移行ユーティリティを実行する場合に使用するアプリケーション ファイルをダウンロードします。

ステップ 3　[Migration Guide] をクリックして、『*Migration Guide for Cisco Secure Access Control System 5.4*』をダウンロードします。

UCP Web サービス ファイルのダウンロード

このページから WSDL ファイルをダウンロードして、ACS を社内ポータルに統合し、ACS 内部 ID ストアに設定されている ACS ユーザに自分のパスワードの変更を許可できます。UCP Web サービスを使用すると、ユーザは自分のパスワードだけを変更できます。パスワードは、プライマリまたはセカンダリ ACS サーバ上で変更できます。

UCP Web サービスによって、入力した新しいパスワードと ACS でユーザに設定されているパスワード ポリシーが比較されます。新しいパスワードが定義されている基準に準拠している場合、新しいパスワードが有効になります。プライマリ ACS サーバでパスワードを変更すると、そのパスワードは ACS によってすべてのセカンダリ ACS サーバに複製されます。

UCP WSDL ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [User Change Password] を選択します。

[User Change Password (UCP) web service] ページが表示されます。

ステップ 2　次のいずれかをクリックします。

- [UCP WSDL] : WSDL ファイルをダウンロードします。
- [UCP Web application example] : アプリケーション ファイルをダウンロードします。
- [Python Script for Using the User Change Password Web Service] : サンプル Python スクリプトをダウンロードします。

UCP Web サービスの使用方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/ucp.html.

サンプル Python スクリプトのダウンロード

[Scripts] ページには、次のサンプル Python スクリプトがあります。

- UCP Web サービスの使用
- 一括インポートおよびエクスポート処理の自動化

これらのサンプル スクリプトをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Sample Python Scripts] を選択します。

[Sample Python Scripts] ページが表示されます。

ステップ 2　次のいずれかをクリックします。

- [Python Script for Using the User Change Password Web Service] : UCP Web サービスのサンプル スクリプトをダウンロードします。
- [Python Script for Performing CRUD Operations on ACS Objects] : インポートおよびエクスポート処理のサンプル スクリプトをダウンロードします。

ステップ 3　スクリプトをローカル ハード ドライブに保存します。

スクリプトには、インストール手順が付属しています。スクリプトの使用方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/acs_sdk.html

（注）　シスコのテクニカル サポートでは、デフォルトの Python スクリプトだけがサポートされています。変更されたスクリプトはサポートされていません。

Rest サービスのダウンロード

ACS Rest Service を使用すると、ACS データベースからオブジェクトを作成、更新、削除することができます。

（注）　WADL ファイルを読み取るためのコマンドラインを使用して Rest Service をイネーブルにする必要があります。

ACS Rest Service WADL ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Rest Service] を選択します。

[Rest Service] ページが表示されます。

ステップ 2　次のいずれかをクリックします。

- [Common or Identity] : ACS 5.4 Rest インターフェイスでサポートされるオブジェクトの構造を記述する XSD ファイルをダウンロードします。
- [Schema files] : スキーマ ファイルをダウンロードします。
- [SDK Samples] : SDK サンプルをダウンロードします。

Rest サービスの使用方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/rest.html

CHAPTER 19

ロギングの概要

この章では、ACS 5.4 のロギング機能について説明します。管理者とユーザは、ACS の各種の管理インターフェイスを使用してさまざまなタスクを実行します。管理アクセス コントロール機能を使用して、管理者とユーザにさまざまなタスクの実行権限を割り当てることができます。

これとは別に、管理者とユーザが実行するさまざまな処理をトラッキングするオプションが必要になることもあります。ACS では、これらの処理とイベントのトラッキングに使用できるいくつかのログが提供されています。

この章の内容は、次のとおりです。

- 「ロギングについて」（P.19-1）
- 「ACS 4.x と ACS 5.4 のロギング」（P.19-12）

ロギングについて

ACS では次のログを収集できます。

- カスタマー ログ：ACS の監査とトラブルシューティングに使用し、アカウンティング、監査、システムレベル診断などの日常的な操作を記録するログを含みます。
- デバッグ ログ：シスコ テクニカル サポートにエクスポートして評価およびトラブルシューティングに使用できる詳細レベルのテキスト メッセージです。ACS デバッグ ログは、コマンドライン インターフェイスを介して設定します。具体的には、コマンドライン インターフェイスを使用して、ACS デバッグ ログの重大度レベルをイネーブルおよび設定します。詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。
- プラットフォーム ログ：ACS アプライアンス オペレーティング システムによって生成されるログ ファイル。

デバッグ ログとプラットフォーム ログは、各 ACS サーバにローカルに格納されます。カスタマー ログは、展開されているすべてのサーバについて集中的に表示できます。

ロギングには次の ACS インターフェイスを使用できます。

- Web インターフェイス：プライマリ ロギング インターフェイス。ロギングするメッセージおよびメッセージをロギングする場所を設定できます。
- コマンドライン インターフェイス（CLI）：ログ、デバッグ ログ、およびデバッグ バックアップ ログをローカル ターゲットに表示およびダウンロードできます。CLI では、プラットフォーム ログも表示およびダウンロードできます。詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

ログ ターゲットの使用方法

カスタマー ログ情報を複数のコンシューマまたは*ログ ターゲット*に送信することを指定できます。また、ログ メッセージをテキスト フォーマットでローカルに格納するか、または syslog サーバに転送するかを指定できます。デフォルトでは、*ローカル ストア*と呼ばれる単一の定義済みローカル ログ ターゲットは、データを ACS サーバにテキスト フォーマットで格納し、ローカル ACS サーバからのログ メッセージだけを含んでいます。ローカル ストアに格納されているレコードは、CLI から表示できます。

ログを syslog サーバに転送することも指定できます。ACS では、syslog 転送を使用して、ログを Monitoring and Reports コンポーネントに転送します。ACS ログ メッセージを受信する追加の syslog サーバを定義することもできます。指定した追加の syslog サーバごとに、リモート ログ ターゲットを定義する必要があります。

分散展開では、セカンダリ ACS サーバの 1 つを Monitoring and Reports サーバとして指定する必要があり、そのサーバが展開されたすべてのサーバからログを受信することを指定する必要があります。デフォルトでは、*LogCollector* と呼ばれるログ ターゲットが Monitoring and Reports サーバを識別します。

分散展開が使用されている場合は、Web インターフェイスの [Log Collector] オプションで、ログ情報を収集するサーバを指定します。展開環境のセカンダリ サーバを Monitoring and Reports サーバとして機能するように指定することを推奨します。

ここでは、次の内容について説明します。

- 「ロギング カテゴリ」（P.19-2）
- 「ログ メッセージの重大度レベル」（P.19-4）
- 「ローカル ストア ターゲット」（P.19-5）
- 「ログ メッセージの表示」（P.19-10）
- 「デバッグ ログ」（P.19-11）

ロギング カテゴリ

各ログには、ログ メッセージの内容に従ってロギング カテゴリにバンドルされているメッセージ コードが関連付けられています。ロギング カテゴリは、含まれているメッセージの内容を説明する場合に役立ちます。

ロギング カテゴリは、ACS の機能、フロー、または使用例を説明するメッセージ コードのバンドルです。カテゴリは階層構造に配置され、ロギングの設定に使用されます。各カテゴリには次の項目があります。

- [Name]：説明的な名前
- [Type]：Audit、Accounting、または Diagnostics
- [Attribute list]：カテゴリに関連付けられているメッセージとともにロギングできる属性のリスト（該当する場合）

ACS では、ログ ターゲットを割り当てることのできる次の設定済みグローバル ACS ロギング カテゴリが提供されています（「ローカル ストア ターゲット」（P.19-5）を参照）。

- 次のような管理と操作の監査。
  - ACS の設定変更：ACS に対して行われたすべての設定変更をロギングします。項目が追加または編集された場合、設定変更イベントには、変更された属性の詳細とそれらの新しい値も含まれます。編集要求の結果、属性が新しい値を持たない場合、設定監査レコードは作成されません。

（注）　複雑な設定項目または属性（ポリシーや DACL の内容など）の場合は、新しい属性値が「New/Updated」としてレポートされ、監査に実際の属性値は含まれません。

  - ACS 管理者アクセス：管理者がログアウトするまで、管理者がシステムにアクセスしたときに発生したすべてのイベントをロギングします。管理者が明示的な要求で ACS を終了したか、またはセッションがタイムアウトになったかをロギングします。このログには、アカウントが非アクティブなために失敗したログイン試行も含まれます。ログインの失敗と失敗の理由がロギングされます。
  - ACS の操作変更：管理者が要求したすべての操作をロギングします（展開環境から ACS をプライマリとしてプロモートする、完全複製を要求する、ソフトウェアのダウンロードを実行する、バックアップまたは復元を実行する、PAC を生成および復元するなど）。
  - 内部ユーザ パスワードの変更：すべての管理インターフェイスで内部ユーザ パスワードに対して行われたすべての変更をロギングします。

  また、管理と操作の監査メッセージをローカル ストアにロギングする必要があります。任意で、これらのメッセージをリモート ロギング ターゲットにロギングできます（「ローカル ストア ターゲット」（P.19-5）を参照）。

- AAA 監査。これには、RADIUS および TACACS+ の認証の成功または失敗、コマンドアクセスの認証の成功または失敗、パスワード変更、RADIUS 要求応答などが含まれます。
- AAA 診断。これには、RADIUS および TACACS+ 診断要求と RADIUS 属性要求の認証、許可、アカウンティング情報、ID ストアと認証フローの情報などが含まれます。これらのメッセージのロギングは任意です。
- システム診断。これには、システムの起動とシャットダウンやロギング関連の診断メッセージが含まれます。
  - CLI および Web インターフェイスに関連する管理診断メッセージ
  - 外部サーバ関連メッセージ
  - ローカル データベース メッセージ
  - ローカル サービス メッセージ
  - 証明書関連メッセージ

  これらのメッセージのロギングは任意です。
- システム統計情報。これには、システム パフォーマンスとリソース使用状況に関する情報が含まれます。CPU とメモリの使用状況、プロセスの健全性、要求処理の遅延などのデータが含まれます。
- アカウンティング。これには、TACACS+ ネットワーク アクセス セッションの開始、停止、およびアップデート メッセージに加えて、コマンド アカウンティングに関連するメッセージが含まれます。また、これらのメッセージはローカル ストアにロギングできます。これらのメッセージのロギングは任意です。

ログ メッセージは、このトピックで説明するロギング カテゴリに含めるか、またはロギング サブカテゴリに含めることができます。各ロギング サブカテゴリを個別に設定することが可能であり、その設定は親カテゴリに影響しません。

ACS Web インターフェイスで、[System Administration] > [Configuration] > [Logging Categories] > [Global] を選択して、ロギング カテゴリとサブカテゴリの階層構造を表示します。Web インターフェイスで、[Monitoring and Reports] > [Catalog] を選択して、設定したロギング カテゴリに基づくレポートを実行します。

各ログ メッセージには、次の情報が含まれます。

- イベント コード：固有のメッセージ コード。
- ロギング カテゴリ：ログ メッセージが属するカテゴリを識別します。
- 重大度レベル：診断の重大度レベルを識別します。詳細については、「ログ メッセージの重大度レベル」（P.19-4）を参照してください。
- メッセージ クラス：RADIUS、ポリシー、EAP 関連コンテキストなど、コンテキストが類似するメッセージのグループを識別します。
- メッセージ テキスト：英語での短い説明テキスト。
- 説明：ログ メッセージの理由、トラブルシューティング情報（該当する場合）、および詳細情報への外部リンクを示す英語のテキスト。
- 失敗の理由（任意）：ログ メッセージが失敗の理由に関連付けられているかどうかを示します。

パスワードは、暗号化されているかどうかにかかわらずロギングされません。

グローバルおよびインスタンスごとのロギング カテゴリ

デフォルトでは、1 つのログ カテゴリ設定が、展開されたすべてのサーバに適用されます。各ログ カテゴリについて、ロギングされるメッセージの重大度のしきい値、メッセージがローカル ターゲットにロギングされるかどうか、およびメッセージの送信先のリモート syslog ターゲットが定義されます。

ログ カテゴリは階層構造に編成されるため、親カテゴリに対して行った設定変更はすべての子カテゴリに適用されます。ただし、管理者は展開された個々のサーバに異なる設定を適用できます。

たとえば、展開環境内の 1 つのサーバに、より集中的な診断ロギングを適用できます。インスタンスごとのロギング カテゴリ設定には、展開されたすべてのサーバが表示され、それらのサーバがグローバル ロギング設定を利用するように設定されているか、または固有のカスタム設定を持つかが示されます。

サーバのカスタム設定を定義するには、最初に [*Override*] オプションを選択してから、そのサーバの特定のログ カテゴリ定義を設定する必要があります。

ログ メッセージ カタログを使用して、生成できるすべてのログ メッセージを表示できます。ログ メッセージごとに、対応するカテゴリと重大度が表示されます。この情報は、ロギング カテゴリ定義の設定時に役立つことがあります。

ログ メッセージの重大度レベル

特定のロギング カテゴリに対して特定の重大度レベル以上のログをロギングするように設定し、これを設定要素として追加して、保存、表示、およびエクスポートするメッセージ数を制限または拡張できます。

たとえば、特定のロギング カテゴリに対して重大度レベル WARNING のログをロギングするように設定した場合は、重大度レベル WARNING のロギング カテゴリとそれよりも高いプライオリティ レベル（ERROR および FATAL）のロギング カテゴリに対するログ メッセージが、設定した場所に送信されます。表 19-1 に、重大度レベルおよび関連するプライオリティ レベルを示します。

表 19-1　ログ メッセージの重大度レベル

ACS 重大度レベル	説明	Syslog 重大度レベル
FATAL	緊急事態。ACS が使用できないため、すぐに対応する必要があります。	1（最高）
ERROR	クリティカルまたはエラー状況。	3
WARN	正常だが重要な状況。	4
NOTICE	監査およびアカウンティング メッセージ。重大度 NOTICE のメッセージは、指定された重大度しきい値に関係なく、常に設定済みログ ターゲットに送信され、フィルタ処理はされません。	5
INFO	診断情報メッセージ。	6
DEBUG	診断メッセージ。	7

ローカル ストア ターゲット

ローカル ストア内のログ メッセージはテキスト ファイルであり、それが属するロギング カテゴリに関係なく、*/opt/CSCOacs/logs/localStore/* にある 1 つのログ ファイルに送信されます。ローカル ストアには、ローカル ACS ノードからのログ メッセージだけを含めることができます。ローカル ストアは、他の ACS ノードからのログ メッセージを受け入れることができません。

ローカル ストアに送信されるログを設定できますが、ログ メッセージとともに送信される属性は設定できません。すべての属性が、送信されるログ メッセージとともに送信されます。

管理と操作の監査ログ メッセージは常にローカル ストアに送信され、リモート syslog サーバと Monitoring and Reports サーバ ターゲットにも送信できます。

ログ メッセージは、次の syslog メッセージ フォーマットでローカル ストアに送信されます。

time stamp sequence_num msg_code msg_sev msg_class msg_text attr=value

表 19-2 に、ローカル ストア syslog メッセージ フォーマットの内容を示します。

表 19-2　ローカル ストアと Syslog メッセージ フォーマット

フィールド	説明
timestamp	生成元の ACS のローカル クロックに従った、*YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm* フォーマットでのメッセージ生成の日付。値は次のとおりです。 • *YYYY* = 年を表す数字。 • *MM* = 月を表す数字。1 桁の月（1 ～ 9）の場合は、数字の前に 0 が付きます。 • *DD* = 日を表す数字。1 桁の日（1 ～ 9）の場合、数字の前に 0 が付きます。 • *hh* = 時間：00 ～ 23。 • *mm* = 分：00 ～ 59。 • *ss* = 秒：00 ～ 59。 • *xxx* = ミリ秒：000 ～ 999。 • *+/-zz:zz* = ACS サーバのタイムゾーンからのタイムゾーン オフセット。zh はオフセットの時間数、zm はオフセットの分数です。すべて先頭に、オフセットの方向を示すマイナスまたはプラス記号が付きます。 たとえば、+02:00 は、タイムスタンプによって示された時刻に、ACS サーバのタイムゾーンよりも 2 時間先行する ACS ノードでメッセージが発生したことを示します。
sequence_num	各メッセージのグローバル カウンタ。1 つのメッセージがローカル ストアに送信され、次に syslog サーバ ターゲットに送信された場合は、カウンタが 2 つ増加します。有効な値は 0000000001 ～ 999999999 です。
msg_code	ロギング カテゴリで定義されているメッセージ コード。
msg_sev	ログ メッセージのメッセージ重大度レベル（表 19-1 を参照）。
msg_class	同じコンテキストを持つメッセージのグループを識別するメッセージ クラス。
text_msg	英語の説明テキスト メッセージ。
attr=value	ロギングされたイベントの詳細を示す属性と値のペアのセット。カンマ (,) で各ペアを区切ります。 属性名は ACS ディクショナリで定義されています。 応答方向属性セットの値は、Response という 1 つの属性にバンドルされ、中カッコ {} で囲まれます。また、Response 内の属性と値のペアはセミコロンで区切られます。次に例を示します。 Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00; }

Web インターフェイスを使用して、ローカル ストア ログ ファイルを保持する日数を設定できます。デフォルトの設定では、データが 5 MB を超えるか、または 1 日 1 回削除されますが、このいずれかの制限に最初に達したときに削除されます。

ローカル ストア ファイルを 2 日以上保持するように設定し、結合されたファイルのデータ サイズが 95000 Mb に達した場合は、システム診断ログに FATAL メッセージが送信され、データが削除されるまでローカル ストアへのすべてのロギングが停止します。Web インターフェイスを使用して、ローカル ストア ログ ファイルを削除してください。削除処理は現在アクティブなログ ファイルにロギングされます。「ローカル ログ データの削除」（P.18-24）を参照してください。

現在のログ ファイルの名前は *acsLocalStore.log* です。古いログ ファイルの名前のフォーマットは *acsLocalStore.log.YYYY-MM-DD-hh-mm-ss-xxx* で、各項目の意味は次のとおりです。

- acsLocalStore.log = 非アクティブなローカル ストア ログ ファイルのプレフィックスに、タイムスタンプが追加されます。

（注）　タイムスタンプは、ファイルが最初に作成されたときに追加され、ファイル内の最初のログ メッセージのタイムスタンプと一致します。

  - *YYYY* = 年を表す数字。
  - *MM* = 月を表す数字。1 桁の月（1 ～ 9）の場合は、数字の前に 0 が付きます。
  - *DD* = 日を表す数字。1 桁の日（1 ～ 9）の場合、数字の前に 0 が付きます。
  - *hh* = 時間：00 ～ 23。
  - *mm* = 分：00 ～ 59。
  - *ss* = 秒：00 ～ 59。
  - *xxx* = ミリ秒：000 ～ 999。

ローカル ストアを重大なログ ターゲットとして設定できます。重大なログ ターゲットの詳細については、「ログ メッセージの表示」（P.19-10）を参照してください。

ログ メッセージは、ローカル ログ ターゲット（ローカル ストア）または最大 8 つのリモート ログ ターゲット（リモート syslog サーバ上）に送信できます。

- [System Administration] > [Configuration] > [Log Configuration] > [Remote Log Targets] を選択して、リモート ログ ターゲットを設定します。
- [System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] を選択して、どのログ メッセージをどのターゲットに送信するかを設定します。

重大なログ ターゲット

ローカル ストア ターゲットは、重大なログ ターゲット（ロギング カテゴリのプライマリまたは必須ログ ターゲット）として機能できます。

たとえば、管理と操作の監査メッセージは常にローカル ストアにロギングされますが、それらをリモート syslog サーバまたは Monitoring and Reports サーバ ログ ターゲットにロギングするように設定することもできます。ただし、リモート ログ ターゲットに追加でロギングされるように設定された管理と操作の監査メッセージは、ローカル ログ ターゲットへの最初のロギングが正常に行われた場合には、そのリモート ログ ターゲットにだけロギングされます。

重大なログ ターゲットを設定し、メッセージがその重大なログ ターゲットに送信される場合、メッセージは、ベスト エフォートに基づいて重大ではない設定済みログ ターゲットにも送信されます。

- 重大なログ ターゲットを設定し、メッセージがその重大なログ ターゲットにロギングされない場合、メッセージは重大ではない設定済みログ ターゲットにも送信されません。
- 重大なログ ターゲットを設定していない場合、メッセージは、ベスト エフォートに基づいて重大ではない設定済みログ ターゲットに送信されます。

[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] > *log_category* を選択します。*log_category* は、ロギング カテゴリの重大なログ ターゲットを設定するための特定のロギング カテゴリです。

（注） 重大なロギングは、アカウンティングおよび AAA 監査（成功した認証）カテゴリにだけ適用できます。AAA 診断、システム診断、およびシステム統計情報のカテゴリには重大なロギングを設定できません。

リモート Syslog サーバ ターゲット

Web インターフェイスを使用して、ロギング カテゴリ メッセージがリモート syslog サーバ ターゲットに送信されるように設定できます。ログ メッセージは、syslog プロトコル標準（RFC-3164 を参照）に従ってリモート syslog サーバ ターゲットに送信されます。syslog プロトコルはセキュアでない UDP です。

ログ メッセージは、ローカル ストア syslog メッセージ フォーマット（表 19-2 を参照）に先行する次の syslog メッセージ ヘッダー フォーマットでリモート syslog サーバに送信されます。

pri_num YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

表 19-3 に、リモート syslog メッセージ ヘッダー フォーマットの内容を示します。

表 19-3　リモート Syslog メッセージ ヘッダー フォーマット

フィールド	説明
pri_num	メッセージのプライオリティ値。メッセージのファシリティ値と重大度値の組み合わせです。プライオリティ値 =（ファシリティ値 * 8）+ 重大度値。ファシリティ コードの有効なオプションは次のとおりです。 • LOCAL0（コード = 16） • LOCAL1（コード = 17） • LOCAL2（コード = 18） • LOCAL3（コード = 19） • LOCAL4（コード = 20） • LOCAL5（コード = 21） • LOCAL6（コード = 22、デフォルト） • LOCAL7（コード = 23） 重大度値：重大度値については、表 19-1 を参照してください。
time	生成元の ACS のローカル クロックに従った、*YYYY Mmm DD hh:mm:ss* フォーマットでのメッセージ生成の日付。値は次のとおりです。 • *YYYY* = 年を表す数字。 • *Mmm* = 月の表現（Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec）。 • *DD* = 日を表す数字。1 桁の日付（1 ～ 9）の場合は、数字の前に空白が付きます。 • *hh* = 時間：00 ～ 23。 • *mm* = 分：00 ～ 59。 • *ss* = 秒：00 ～ 59。 一部のデバイスは、タイムゾーンを -/+hhmm のフォーマットで指定するメッセージを送信します。- と + は、ACS サーバのタイムゾーンからのオフセット方向を示します。hh はオフセットの時間数、mm はオフセット時間の分数です。 たとえば、+02:00 は、タイムスタンプによって示された時刻に、ACS サーバのタイムゾーンよりも 2 時間先行する ACS ノードでメッセージが発生したことを示します。
xx:xx:xx:xx/host_name	生成元 ACS の IP アドレス、またはホスト名。
cat_name	先頭に `CSCOacs` 文字列が付いたロギング カテゴリ名。
msg_id	固有のメッセージ ID。1 ～ 4294967295 です。メッセージ ID は、新しいメッセージごとに 1 つ増加します。メッセージ ID は、アプリケーションが再起動するたびに 1 から再開します。
total_seg	ログ メッセージ内のセグメントの総数。長いメッセージは複数のセグメントに分割されます。
seg_num	メッセージ内のセグメントの順序番号。この数値を使用して、メッセージのどのセグメントを表示しているかを判断します。

syslog メッセージ データまたはペイロードは、表 19-2 で説明しているローカル ストア メッセージ フォーマットと同じです。

リモート syslog サーバ ターゲットは、ファシリティ コード名 *LOCAL0* ～ *LOCAL7*（*LOCAL6* がデフォルトのロギング場所）によって示されます。リモート syslog サーバに割り当てるログ メッセージは、Linux syslog のデフォルトの場所（*/var/log/messages*）に送信されますが、サーバで別の場所を設定できます。

リモート syslog サーバは、重大なログ ターゲットとして機能できません。重大なログ ターゲットの詳細については、「重大なログ ターゲット」（P.19-7）を参照してください。

レポート サーバ ターゲットの監視

Web インターフェイスを使用して、ロギング カテゴリ メッセージが Monitoring and Reports サーバ ターゲットに送信されるように設定できます。ログ メッセージは、syslog プロトコル標準（RFC-3164 を参照）に従って Monitoring and Reports サーバ ターゲットに送信されます。syslog プロトコルはセキュアでない UDP プロトコルです。

ログ メッセージは、ローカル ストア syslog メッセージ フォーマット（表 19-2 を参照）に先行する syslog メッセージ ヘッダー フォーマット（表 19-3 を参照）で Monitoring and Reports サーバに送信されます。

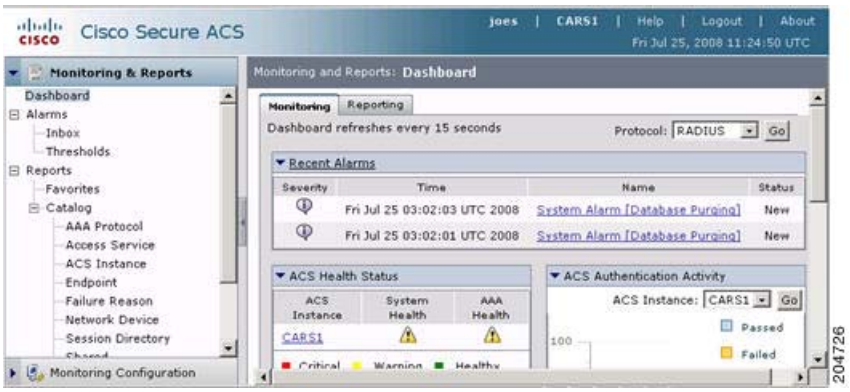
Monitoring and Reports サーバは、重大なログ ターゲットとして機能できません。重大なログ ターゲットの詳細については、「重大なログ ターゲット」（P.19-7）を参照してください。

ログ メッセージの表示

Web インターフェイスと CLI を使用すると、ローカルに格納されているログ メッセージを表示できます。リモート syslog サーバに送信されたログ メッセージは、Web インターフェイスまたは CLI で表示できません。

Web インターフェイスで、[Monitoring and Reports] > [Launch Monitoring and Report Viewer] を選択して、セカンダリ ウィンドウに Monitoring and Reports Viewer を開きます（図 19-1 を参照）。CLI を使用したログ メッセージの表示の詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

図 19-1　Monitoring and Reports Viewer



Monitoring and Report Viewer には、次の 2 つのドロワ オプションがあります。

- [Monitoring and Reports]：このドロワを使用して、アラームの表示と設定、ログ レポートの表示、およびトラブルシューティング タスクを実行します。
- [Monitoring Configuration]：このドロワを使用して、ロギング操作とシステム設定を表示および設定します。

「ロギング カテゴリ」（P.19-2）で説明したログ メッセージで取り込まれる情報に加えて、ビューア レポートには、成功および失敗した AAA 認証試行が Step 属性とともにリストされます。Step 属性では、同じセッションで発生した他のイベントに関する情報が提供されます。この情報によって、認証の成功または失敗の原因となった手順の順序を確認できます。

ビューアは、次の用途に使用できます。

- アラーム、レポート、およびトラブルシューティング情報の管理
- データの削除、ログの収集、ジョブのスケジューリング、ステータスの監視など、システム操作の管理
- 失敗理由の編集、電子メール、セッション ディレクトリ、アラーム設定の設定など、システム設定の管理

詳細については、「ACS での監視とレポート」（P.11-1）を参照してください。

デバッグ ログ

トラブルシューティングのサポートを受ける必要がある場合は、Web インターフェイスと CLI を使用して、デバッグ ログなどのログをシスコのテクニカル サポート担当者に送信できます。Web インターフェイスで、[Monitoring and Reports] > [Launch Monitoring and Report Viewer] > [Monitoring and Reports] > [Troubleshooting] > [ACS Support Bundle] を選択します。

CLI を使用して、Application Deployment Engine-OS 1.2 環境ログ内のハードウェア サーバを表示およびエクスポートすることもできます。これらのメッセージは */var/log/boot.log* だけに送信され、CLI が ACS デバッグ ログ メッセージを表示またはエクスポートする方法には関連しません。詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

ACS 4.x と ACS 5.4 のロギング

ACS 4.x のロギング機能に精通している場合は、かなり異なる ACS 5.4 のロギング機能にも慣れてください。表 19-4 に、ACS 4.x と ACS 5.4 のロギング機能の違いを示します。

表 19-4　ACS 4.x と ACS 5.4 のロギング機能

ロギング機能	ACS 4.x での処理	ACS 5.4 での処理
ログ タイプ	• AAA 関連ログには、ユーザによるリモート アクセス サービスの利用に関する情報が格納される。 • 監査ログには ACS システムとアクティビティに関する情報が含まれるため、システム関連イベントも記録される。 システム ログは、トラブルシューティングや監査に役立ちます。CSV 監査ログは常にイネーブルであり、他のロガーに対して監査ログをイネーブルまたはディセーブルにできます。監査ログの内容は設定できません。 監査ログでは、管理者が各ユーザに対して行った実際の変更を表示できます。ACS 監査ログには、特定のユーザに対して変更されたすべての属性がリストされます。	「ロギング カテゴリ」（P.19-2）を参照してください。
使用可能なログ ターゲット	• CSV ロガー • Syslog ロガー • ODBC ロガー • リモート ロギング	「リモート Syslog サーバ ターゲット」（P.19-8）および「ローカル ストア ターゲット」（P.19-5）を参照してください。
ログ ファイルの場所	• CSV ロガー：*sysdrive*:\Program Files\CiscoSecure ACS v*x.x*。	• ローカル ストア ターゲット ログ：*/opt/CSCOacs/logs/localStore/*。 • リモート syslog サーバ ターゲット ログ：*/var/log/messages*。
レポート タイプ	• CSV • ダイナミック管理 • 権限付与	「ACS での監視とレポート」（P.11-1）を参照してください。
エラー コードとメッセージ テキスト	ACS 4.2 では、CSAuth 診断ログにクライアント要求および応答の説明が表示されます。旧バージョンの ACS では、クライアント要求および応答に数値コードが使用されていました。	すべてのメッセージ。「ログ メッセージの表示」（P.19-10）を参照してください。

表 19-4　ACS 4.x と ACS 5.4 のロギング機能 （続き）

ロギング機能	ACS 4.x での処理	ACS 5.4 での処理
設定	[System Configuration] > [Logging] ページを使用して、次の項目を定義します。 • ロガーと個々のログ • クリティカル ロガー • リモート ロギング • CSV ログ ファイル • Syslog ログ • ODBC ログ	「ログの設定」（P.18-21）および『*CLI Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。
ログ メッセージの表示とダウンロード	[Reports and Activity] ページを使用します。	「ログ メッセージの表示」（P.19-10）を参照してください。
ログ メッセージを使用したトラブルシューティング	サービス ログ ファイルは、該当するサービス ディレクトリの *\Logs* サブディレクトリにあります。	「デバッグ ログ」（P.19-11）を参照してください。

APPENDIX A

AAA プロトコル

ここでは、次の内容について説明します。

- 「一般的な使用例」（P.A-1）
- 「アクセス プロトコル：TACACS+ および RADIUS」（P.A-5）
- 「TACACS+ の概要」（P.A-5）
- 「RADIUS の概要」（P.A-6）

一般的な使用例

ここでは、次の内容について説明します。

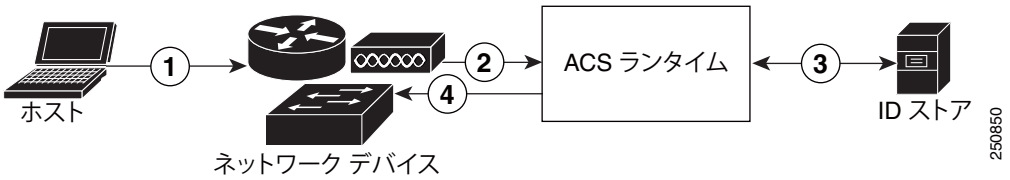
- 「デバイス管理（TACACS+）」（P.A-1）
- 「ネットワーク アクセス（EAP 使用および未使用の RADIUS）」（P.A-2）

デバイス管理（TACACS+）

図 A-1 に、デバイス管理に関するフローを示します。次の 2 つの主要なトリガーがあります。

- 「セッション アクセス要求（デバイス管理 [TACACS+]）」（P.A-2）。
- 「コマンド認可要求」（P.A-2）。

図 A-1　　デバイス管理フロー



セッション アクセス要求（デバイス管理 [TACACS+]）

（注）　番号は、図 A-1（P.A-1）に対応しています。

セッション要求の処理手順は、次のとおりです。

1. 管理者がネットワーク デバイスにログインします。
2. ネットワーク デバイスによって、TACACS+ アクセス要求が ACS に送信されます。
3. ACS は、ID ストアを使用してユーザのクレデンシャルを確認します。
4. ACS は、決定を適用するネットワーク デバイスに、TACACS+ 応答を送信します。応答には、セッション中の管理者アクセスのレベルを決定する特権レベルなどのパラメータが含まれています。

コマンド認可要求

（注）　番号は、図 A-1（P.A-1）に対応しています。

コマンド認可の処理手順は、次のとおりです。

1. 管理者が、ネットワーク デバイスでコマンドを発行します。
2. ネットワーク デバイスによって、TACACS+ アクセス要求が ACS に送信されます。
3. 任意の設定により、ACS では、ID ストアを使用して、ポリシー処理に含めるユーザ属性を取得します。
4. TACACS+ 応答は、管理者にコマンドの発行が認可されているかどうかを示します。

ネットワーク アクセス（EAP 使用および未使用の RADIUS）

ネットワーク アクセスでは、ホストはネットワーク デバイスに接続し、ネットワーク リソースの使用を要求します。ネットワーク デバイスは、新しく接続されたホストを識別し、転送方式として RADIUS プロトコルを使用して、ユーザの認証および認可を ACS に要求します。

ACS 5.4 では、RADIUS プロトコルを使用して転送されるプロトコルに応じて、次のカテゴリのネットワーク アクセス フローがサポートされます。

- EAP を含まない RADIUS ベースのプロトコル。
  - PAP
  - CHAP
  - MSCHAPv1
  - MSCHAPv2

  EAP を含まない RADIUS ベースのプロトコルの詳細については、「EAP 認証を使用しない RADIUS ベースのフロー」（P.A-3）を参照してください。
- RADIUS を使用して転送される EAP プロトコル ファミリ。さらに次のように分類できます。
  - 証明書を使用しない単純な EAP プロトコル。

    EAP-MD5

LEAP

- TLS ハンドシェイクを含み、クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP プロトコル。

  PEAP。内部方式 PEAP/EAP-MSCHAPv2 および PEAP/EAP-GTC のいずれかを使用します。

  EAP-FAST。内部方式 EAP-FAST/EAP-MSCHAPv2 および EAP-FAST/EAP-GTC のいずれかを使用します。

- 完全に証明書ベースの EAP プロトコル。このプロトコルでは、TLS ハンドシェイクによってサーバ認証とクライアント認証の両方に証明書が使用されます。

  EAP-TLS

  内部方式 EAP-TLS を含む PEAP

EAP 認証を使用する RADIUS ベースのフローの詳細については、「EAP 認証を使用する RADIUS ベースのフロー」（P.A-3）を参照してください。

EAP 認証を使用しない RADIUS ベースのフロー

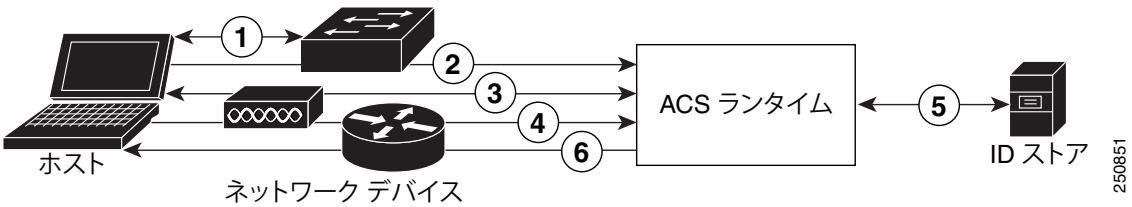
この項では、EAP 認証を使用しない RADIUS ベースのワークフローについて説明します。

PAP 認証を使用する RADIUS の処理手順は、次のとおりです。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスは、RADIUS Access-Request を ACS に送信します。使用されている特定のプロトコル（PAP、CHAP、MSCHAPv1、または MSCHAPv2）に適した RADIUS 属性が含まれています。
3. ACS は、ID ストアを使用してユーザのクレデンシャルを確認します。
4. RADIUS 応答（Access-Accept または Access-Reject）が、決定を適用するネットワーク デバイスに送信されます。

図 A-2 に、EAP を使用しない RADIUS ベースの認証を示します。

図 A-2　EAP 認証を使用しない RADIUS ベースのフロー



EAP 認証を使用する RADIUS ベースのフロー

EAP には、さまざまな認証タイプをサポートする拡張フレームワークがあります。これらのフレームワークの中で、ACS によってサポートされている具体的な EAP 方式は次のとおりです。

- 証明書を使用しない単純な EAP 方式
  - EAP-MD5
  - LEAP
- クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP 方式
  - PEAP/EAP-MSCHAPv2

  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- サーバ認証とクライアント認証の両方に証明書を使用する EAP 方式
  - EAP-TLS
  - PEAP/EAP-TLS

認証プロセスで EAP が使用される場合は常に、具体的にどの EAP 方式（および該当する場合は内部方式）を使用する必要があるかを決定するネゴシエーション フェーズが先行します。

すべての EAP 認証で、次の処理が実行されます。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが EAP 要求をホストに送信します。
3. ホストは、EAP 応答によって、ネットワーク デバイスに応答します。
4. ネットワーク デバイスは、ホストから受信した EAP 応答を RADIUS Access-Request 内に（EAP-Message RADIUS 属性を使用して）カプセル化し、RADIUS Access-Request を ACS に送信します。
5. ACS は、RADIUS パケットから EAP 応答を抽出して新しい EAP 要求を作成し、この EAP 要求を RADIUS Access-Challenge 内に（この場合も EAP-Message RADIUS 属性を使用して）カプセル化し、ネットワーク デバイスに送信します。
6. ネットワーク デバイスは、EAP 要求を抽出し、ホストへ送信します。

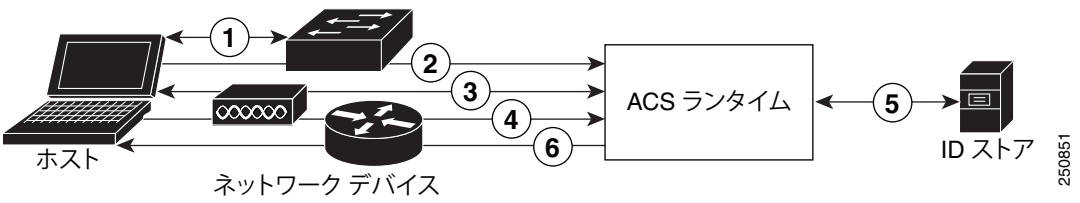
この方法で、ホストと ACS は間接的に EAP メッセージを交換します（EAP メッセージは、RADIUS を使用して転送され、ネットワーク デバイスを介して渡されます）。この方法で交換される EAP メッセージの最初のセットによって、特定の EAP 方式がネゴシエートされます。その後、認証を実行する場合に、この EAP 方式が使用されます。

その後交換される EAP メッセージは、実際の認証の実行に必要なデータを伝送するために使用されます。ネゴシエートされた特定の EAP 認証方式で必要な場合、ACS では ID ストアを使用してユーザのクレデンシャルを確認します。

ACS では、認証が成功か失敗かを決定したあと、EAP-Success または EAP-Failure メッセージを、RADIUS Access-Accept または Access-Reject メッセージ内にカプセル化された状態で、ネットワーク デバイスに（最終的にはホストにも）送信します。

図 A-3 に、EAP を使用する RADIUS ベースの認証を示します。

図 A-3　EAP を使用する RADIUS ベースの認証



ACS 5.4 の経験に影響する可能性のある既知のサプリカントの問題のリストについては、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/release/notes/acs_54_rn.html

アクセス プロトコル：TACACS+ および RADIUS

ここでは、次の内容について説明します。

- 「TACACS+ の概要」（P.A-5）
- 「RADIUS の概要」（P.A-6）

ACS 5.4 は、TACACS+ アクセス プロトコルと RADIUS アクセス プロトコルを使用できます。表 A-1 に、この 2 つのプロトコルの比較を示します。

表 A-1　TACACS+ プロトコルと RADIUS プロトコルの比較

比較項目	TACACS+	RADIUS
伝送プロトコル	TCP：コネクション型トランスポート層プロトコル、信頼性の高い全二重データ伝送。	UDP：コネクションレス型トランスポート層プロトコル、確認応答も配送保証もないデータグラム交換。UDP は、IP を使用してデータ ユニット（データグラムと呼ばれる）をコンピュータ間で移動します。
使用ポート	49	認証および認可：1645 および 1812。 アカウンティング：1646 および 1813。
暗号化	完全なパケット本体の暗号化。	16 バイト以下のパスワードにかぎり、暗号化する。
AAA アーキテクチャ	認証、許可、アカウンティングの各サービスを独立制御。	認証および認可が 1 つのサービスとして統合されている。
利用目的	デバイスの管理。	ユーザ アクセスの制御。

TACACS+ の概要

ネットワーク デバイスがシスコ デバイス管理アプリケーション、アクセス サーバ、ルータ、またはファイアウォールである場合は、TACACS+ を使用する必要があります。ACS 5.4 は、TACACS+ プロトコルで IPv6 アドレスをサポートします。ACS 5.4 では、管理アプリケーションを使用して管理対象ネットワーク デバイスを設定するネットワーク ユーザに対してコマンド認可を提供することにより、シスコ デバイス管理アプリケーションをサポートします。

認可に ACS を使用するように設定されている各管理アプリケーション対して、固有のコマンド セットを使用することによって、管理アプリケーションのユーザに対するコマンド認可のサポートを実現できます。

ACS 5.4 は、管理アプリケーションとの通信に TACACS+ を使用します。管理アプリケーションが ACS と通信できるようにするには、その管理アプリケーションを、ACS 5.4 に TACACS+ を使用する AAA クライアントとして設定する必要があります。

また、デバイス管理アプリケーションに有効な管理者名とパスワードを与える必要があります。管理アプリケーションが最初に ACS と通信するとき、これらの要件が通信の正当性を保証します。

パケットのヘッダーを除き、クライアントと TACACS+ サーバが通信するすべての情報（パケット本体に含まれている）は、共有秘密情報を使用することによって暗号化されます。共有秘密情報自体は、ネットワークで直接的には送信されません。

さらに、管理アプリケーションが使用する管理者は、Command Set 特権がイネーブルになっている必要があります。

RADIUS の概要

ここでは、次の内容について説明します。

- 「RADIUS VSA」（P.A-6）
- 「AAA サーバとしての ACS 5.4」（P.A-7）
- 「ACS 5.4 での RADIUS 属性サポート」（P.A-8）
- 「RADIUS アクセス要求」（P.A-11）

RADIUS は、クライアント/サーバ プロトコルです。リモート アクセス サーバは、このプロトコルを使用して中央サーバと通信してダイヤルイン ユーザを認証し、要求されたシステムまたはサービスへのアクセスを認可します。RADIUS を使用すると、企業は、すべてのリモート サーバが共有できる中央データベースにユーザ プロファイルを保持できます。

このプロトコルはセキュリティを向上させます。企業はこのプロトコルを使用して、単一の管理ネットワーク ポイントで適用されるポリシーを設定できます。

新旧の RFC をサポートするために、ACS 5.4 では認証の要求をポート 1645 およびポート 1812 で受け入れます。アカウンティングについては、ACS ではアカウンティング パケットをポート 1646 および 1813 で受け入れます。

RADIUS VSA

ACS 5.4 には、標準 IETF RADIUS 属性のセットがあります。現在は使用されていない RADIUS IETF 属性は、その名前で識別できます。使用されていない属性には、*attribute-nnn* という形式の名前が付けられています。*attribute* は属性の名前であり、*nnn* は属性の ID です。

また、ACS 5.4 では RADIUS VSA がサポートされています。ACS 5.4 のインストール後、次の事前定義済みの RADIUS VSA のセットを使用できます。

- Cisco
- Cisco VPN 5000
- Microsoft
- US Robotics
- Ascend
- Nortel（Bay Networks）
- RedCreek
- Juniper
- Cisco VPN 3000
- Cisco Business Service Management（BSM）
- Cisco Aironet
- Cisco Airespace

これらの事前定義済みの RADIUS VSA を変更するか、または新しい RADIUS VSA を定義できます。RADIUS VSA は、作成、編集、および複製できます。詳細については、「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）を参照してください。

AAA サーバとしての ACS 5.4

AAA サーバは、コンピュータ リソースへのユーザのアクセス要求を処理するサーバ プログラムであり、企業に対して AAA サービスを提供します。一般的に、AAA サーバは、ネットワーク アクセス サーバおよびゲートウェイ サーバ、ユーザ情報を格納するデータベースおよびディレクトリと連携動作します。現在、デバイスまたはアプリケーションと AAA サーバとの通信に使用されている標準は、RADIUS です。

ACS 5.4 は、1 台以上のネットワーク アクセス デバイス（NAD）の AAA サーバとして機能します。NAD は、ACS サーバのクライアントです。各クライアント NAD で ACS の IP アドレスを指定し、RADIUS プロトコルを使用してユーザ アクセス要求を ACS に送信する必要があります。

RADIUS は、エンドユーザからネットワーク リソースへのアクセスを保護するために、広く一般に使用されています。RADIUS サーバは、他の RADIUS サーバまたは他の種類の認証サーバへのプロキシとして動作できます。

NAD は、ネットワークのゲートキーパーとして機能し、ユーザの代理として Access-Request を ACS に送信します。ACS は、内部 ID ストアを使用するか、外部で設定された LDAP または Windows Active Directory ID ストアを使用して、ユーザ名、パスワード、および必要に応じてその他のデータを確認します。

ACS は、最終的に NAD に対して、Access-Reject メッセージまたは一連の認可属性を含む Access-Accept メッセージによって応答します。

ACS 5.4 では、UDP を使用したネットワーク転送を実行でき、RADIUS パケット解析および構成、必要なデータの確認、重複要求のトラッキングを含む RADIUS プロトコルが実装されています。

UDP を使用するいくつかの理由を次に示します。

- 処理時間が数秒である。
- クライアントおよびサーバの再起動またはオフライン化に特別な処理を必要としない。
- UDP はコネクションレス型プロトコルである。
- UDP は簡単にマルチスレッド サーバを実装して複数のクライアント要求を処理する。

RADIUS に対して UDP が割り当てるポート番号は、次のとおりです。

- 1812（アクセス要求）
- 1813（アカウンティング）
- 1645（アクセス要求）
- 1646（アカウンティング）

ACS 5.4 は認証システムへの入り口です。ACS は、特定の設定可能な UDP ポートで受信します。ネットワークからデータが着信した場合は、次の処理が実行されます。

1. ACS は、データを RADIUS クライアント要求またはプロキシ応答パケットとして処理しようとします。
2. ACS は、設定に登録されている NAD からパケットが着信したことを確認し、重複したパケット処理を防止します。
3. ACS は、RADIUS パケットを解析し、その内容について必要な確認を実行します。
4. 次に、ACS は処理のためにデータを適切なフローに渡します。
5. システムの応答準備が整うと、ACS では次の処理を実行します。
   a. データ処理の結果を受信します。
   b. クライアントへの対応する応答を作成します。
   c. 応答をネットワークに返します。

ACS 5.4 での RADIUS 属性サポート

ACS 5.4 では、RFC 2865 に記述されているように RADIUS プロトコルがサポートされています。

ACS 5.4 では、次のタイプの RADIUS 属性がサポートされています。

- IETF RADIUS 属性
- 一般的な VSA および Cisco VSA
- 他のベンダーの属性

ACS 5.4 では、RADIUS に対する次の拡張で定義されている属性もサポートされています。

- アカウンティング関連の属性。RFC 2866 で定義されています。
- トンネル プロトコルのサポート。RFC 2867 および 2868 で定義されています。
- EAP のサポート（EAP-Message 属性を使用）。RFC 2869 および 3579 で定義されています。

（注） RADIUS パラメータの参照には、表記法 [*attribute-number*] [*attribute name*] が使用されます。たとえば、[*1*]*User-Name* です。数字と名前は、仕様でパラメータに対して割り当てられている数字と名前に対応します。

RADIUS では、任意の RADIUS 属性の受信、送信、およびディクショナリベースの解析および構築がサポートされています。RADIUS 属性が通常の属性、VSA、または Cisco Attribute-Value（AV; 属性値）のペアのいずれであるかは関係ありません。ACS の RADIUS インターフェイスでは、RFC 2865 で定義されている次の属性データ型がサポートされています。

- *text*（UTF-8）
- *string*（バイナリ）
- *address*（IP）
- *integer*
- *time*

データ型 integer、string、および text の許可される値の列挙（ENUM）指定がサポートされています。属性値は、パケットの解析および構築が実行されるとき、これらに対してチェックされます。

ACS は、RADIUS State 属性（24）を使用して特定のカンバセーションを識別します。各カンバセーションには、固有の ID があります。すべてのカンバセーションは、特定の設定バージョン（カンバセーションが開始された時点で使用可能な最新バージョン）で処理されます。

（注） RADIUS State 属性（24）は、PAP 認証には使用されません。

クライアントと RADIUS サーバ間のすべてのトランザクションでは、各 RADIUS パケット内の Request/Response Authenticator フィールドを使用してメッセージの整合性が保護されます。このフィールドでは共有秘密情報が使用されます。共有秘密情報自体は、ネットワークで直接的には送信されません。

また、カプセル化された EAP-Message 属性が含まれるすべてのパケットを含む、一部の形式の RADIUS パケットでは、さらに、Message-Authenticator RADIUS 属性（これにも、共有秘密情報が使用されます）を使用して、すべての RADIUS 属性の整合性が保護されます。

さらに、クライアントと RADIUS サーバ間で送信される RADIUS パケット内のユーザ パスワードは常に暗号化され、セキュアでないネットワーク上の権限のないユーザがパスワードを簡単に判別できないように保護します。

認証

ACS では、RADIUS を使用して転送されるさまざまな認証プロトコルがサポートされています。EAP を使用しないサポート対象プロトコルは、次のとおりです。

- PAP
- CHAP
- MSCHAPv1
- MSCHAPv2

また、さまざまな EAP ベースのプロトコルを、RADIUS EAP-Message 属性内にカプセル化することによって、RADIUS を使用して転送できます。これらのプロトコルは、証明書を使用するかどうか、およびどの程度使用するかに応じて、より詳細に分類できます。次の作業を行います。

- 証明書を使用しない EAP 方式。
  - EAP-MD5
  - LEAP
- クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP 方式
  - PEAP/EAP-MSCHAPv2
  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- サーバ認証とクライアント認証の両方に証明書を使用する EAP 方式
  - EAP-TLS
  - PEAP/EAP-TLS

認可

認可は、設定されているアクセス ポリシーに従って許可されます。

アカウンティング

RADIUS の認証機能または認可機能とは別に、RADIUS プロトコルのアカウンティング機能を使用できます。RADIUS アカウンティング機能の一部を使用して、セッションの開始時および終了時にデータを送信でき、セッション中に使用したリソースの量（時間、パケット、バイトなど）を示すことができます。

ISP では、特別なセキュリティおよび課金の必要性に対応するために、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアを使用する場合があります。

RADIUS 属性の書き換え動作

ACS 5.4 では、追加の RADIUS 属性を定義するか、または既存の属性を更新するオプションがあります。更新された属性は、RADIUS 要求で、RADIUS プロキシ サーバに送信される前に書き換えられます。これらの属性の処理はプロキシ アクセス サービス定義の一部として設定されます。RADIUS 属性の書き換え機能は、RADIUS アクセス要求にのみ有効となり、アカウンティング要求には有効になりません。

RADIUS 属性の書き換え機能により、外部サーバにリダイレクトされるアクセス要求の RADIUS アクセス属性の追加、更新、削除を行えます。属性の処理は、属性動作ステートメントを定義し、プロキシ アクセス サービスの一部として設定されます。

管理者は特定のプロキシ アクセス サービスの属性動作句を設定できます。このサービスが選択されると、ACS はアクセス要求の動作を実行し、更新されたアクセス要求を外部サーバに転送します。ACS 5.4 は既存の値の調整をサポートしません。

属性動作ステートメントの例：

```
Operator-name ADD new value: "University A"
```

次の動作が、RADIUS 属性の書き換えで使用可能です。

- 「追加属性」（P.A-10）
- 「更新属性」（P.A-10）
- 「削除属性」（P.A-11）

追加属性

追加属性は選択した RADIUS 属性の新しい属性値を追加するために使用されます。

- 複数の属性が許可されない場合、追加動作は、選択した属性が要求に存在しないときにだけ、この属性の新しい値を追加します。

  例：

  Called-Station-Id – Attribute Multiple NOT allowed:

  アクセス要求上：

  Called-Station-Id NOT on the request

  属性動作ステートメント：

  Called-Station-Id ADD 1223

  サーバに転送される要求での属性処理の結果：

  Called-Station-Id =1223

  Called-Station-ID が元の要求にある場合、ACS はこの例で追加動作を実行しません。

- 複数の属性が許可される場合、追加動作は、新しい値を持つ属性を必ず追加します。

  例：

  Login-IP-Host – attribute Multiple allowed:

  アクセス要求上：

  Login-IP-Host=10.56.21.190

  属性動作ステートメント：

  Login-IP-Host ADD 10.56.1.1

  サーバに転送される要求での属性処理の結果：

  Login-IP-Host=10.56.21.190

  Login-IP-Host=10.56.1.1

更新属性

更新属性は選択した RADIUS 属性の既存の値を更新するために使用されます。

- 複数の属性が許可されない場合、更新動作は、既存の属性が要求上に存在する場合にだけ、新しい値でその属性を更新します。
- 複数の属性が許可される場合、更新動作は、この属性のすべての発生を削除して、新しい値を持つ属性を 1 つ追加します。

例：

Login-IP-Host – attribute Multiple allowed:

アクセス要求上：

Login-IP-Host=10.56.21.190

Login-IP-Host=10.56.1.1

属性動作ステートメント：

Login-IP-Host UPDATE 10.12.12.12

サーバに転送される要求での属性処理の結果：

Login-IP-Host=10.12.12.12

- 属性が cisco-avpair（キー = 値のペア）の場合、更新はキーに基づいて行われます。

例：

アクセス要求上：

cisco-avpair = url-redirect=www.cisco.com

cisco-avpair = url-redirect=www.yahoo.com

cisco-avpair = cmd=show

属性動作ステートメント：

cisco-avpair UPDATE new value:[url-redirect=www.google.com]

サーバに転送される要求での属性処理の結果：

cisco-avpair = url-redirect=www.google.com

cisco-avpair = cmd=show

削除属性

削除属性動作は選択された RADIUS 属性の値を削除するために使用されます。

例：

Login-IP-Host – attribute Multiple allowed

アクセス要求上：

Login-IP-Host=10.56.21.190

属性動作ステートメント：

Login-IP-Host DELETE

サーバに転送される要求での属性処理の結果：

Attribute Login-IP-Host NOT on the request

RADIUS アクセス要求

ユーザ ログインでは、ネットワーク アクセス デバイスから RADIUS サーバへのクエリー（Access-Request）と、それに対応するサーバからの応答（Access-Accept または Access-Reject）が行われます。Access-Request パケットには、ユーザ名、パスワード、NAD IP アドレス、および NAD ポートと、その他の関連属性が含まれています。

RADIUS サーバでは、NAD からアクセス要求を受信すると、データベースでユーザ名を検索します。データベース クエリーの結果に応じて、受け入れまたは拒否が送信されます。アクセス拒否メッセージには、拒否の理由を示すテキスト メッセージが付加される場合があります。

RADIUS では、認証と認可は対になっています。RADIUS サーバは、ユーザ名およびパスワードが正しいことを確認すると、Access-Accept 応答を返します。この応答には、このセッションで使用するパラメータを示す属性値のペアのリストが含まれています。このパラメータのリストによって、ユーザの認可権限が設定されます。

一般的なパラメータは、次のとおりです。

- サービス タイプ
- プロトコル タイプ
- ユーザに割り当てる IP アドレス（スタティックまたはダイナミック）
- 適用するアクセス リスト
- NAD ルーティング テーブルにインストールするスタティック ルート

RADIUS サーバ内の設定情報によって、インストール時に NAD で設定するパラメータが定義されます。

APPENDIX B

ACS 5.4 での認証

認証とは、ユーザ情報を検証してそのユーザの ID を確認することです。従来の認証方式では、名前とある決まったパスワードが使用されていました。さらに安全な方式では、Challenge Authentication Handshake Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）、OTP、および高度な EAP ベース プロトコルの内部で使用されるような暗号化技術を使用します。ACS は、これらのさまざまな認証方式をサポートしています。

認証と認可には基本的な暗黙の関係があります。ユーザに与えられる認可特権が多くなればなるほど、それに応じて認証を強化する必要があります。ACS では、さまざまな認証方式を提供することにより、この関係がサポートされています。

認証方式の検討

ユーザ名とパスワードは、最も一般的かつ単純で、低コストな認証方式です。この方式の欠点は、ユーザ名やパスワードの情報が簡単に第三者に伝えられたり、推測または不正に取得されたりする可能性がある点です。単純な暗号化されていないユーザ名とパスワードによる認証は確実な認証メカニズムとは言えませんが、インターネット アクセスなどのように認可レベルまたは特権レベルが低い場合は十分に対応可能です。

ネットワーク上でパスワードが不正に取得される危険性を低減するには、暗号化を使用する必要があります。TACACS+ および RADIUS などのクライアント/サーバ アクセス コントロール プロトコルでは、パスワードを暗号化して、ネットワーク内でパスワードが不正に取得される事態の発生を防止します。

ただし、TACACS+ と RADIUS は AAA クライアントと ACS 間でだけ動作します。認証プロセスでは、このポイントの前で、認可されていないユーザが次のようなセットアップで暗号化されていないパスワードを入手する可能性があります。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザ クライアントとの間の通信
- ネットワークアクセス サーバで終端する Integrated Services Digital Network（ISDN）回線
- エンドユーザ クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

認証とユーザ データベース

ACS は、さまざまなユーザ データベースをサポートしています。ACS 内部データベース以外にも、次のような外部ユーザ データベースをサポートしています。

- Windows Active Directory

- LDAP
- RSA SecurID サーバ
- RADIUS ID サーバ

この付録では、次の内容について説明します。

- EAP を含まない RADIUS ベースの認証：
  - 「PAP」（P.B-2）
  - 「CHAP」（P.B-32）
  - MSCHAPv1
  - 「EAP-MSCHAPv2」（P.B-31）
- RADIUS を使用して転送される EAP プロトコル ファミリ。さらに次のように分類できます。
  - 証明書を使用しない単純な EAP プロトコル。

    EAP-MD5：詳細については、「EAP-MD5」（P.B-5）を参照してください。

    LEAP：詳細については、「LEAP」（P.B-32）を参照してください。
  - TLS ハンドシェイクを伴い、クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP プロトコル。

    PEAP/EAP-MSCHAPv2 と PEAP/EAP-GTC のいずれかの内部方式を使用する PEAP：詳細については、「PEAPv0/1」（P.B-14）を参照してください。

    EAP-FAST/EAP-MSCHAPv2 と EAP-FAST/EAP-GTC のいずれかの内部方式を使用する EAP-FAST：詳細については、「EAP-FAST」（P.B-19）を参照してください。
  - 完全に証明書ベースの EAP プロトコル。このプロトコルでは、TLS ハンドシェイクによってサーバ認証とクライアント認証の両方に証明書が使用されます。

    EAP-TLS：詳細については、「EAP-TLS」（P.B-6）を参照してください。

    内部方式 EAP-TLS を含む PEAP については、「PEAPv0/1」（P.B-14）を参照してください。
- 「証明書属性」（P.B-33）
- 「マシン認証」（P.B-35）
- 「認証プロトコルと ID ストアの互換性」（P.B-36）

既知のサプリカントの問題のリストについては、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/release/notes/acs_54_rn.html

PAP

パスワード認証プロトコル（PAP）は、ユーザが双方向ハンドシェイクを使用してその ID を設定する単純な方式を提供します。PAP パスワードは共有秘密情報を使用して暗号化されるため、最もセキュリティ レベルの低い認証プロトコルです。

ACS は、認証を確認するか接続を終了するまで、ID とパスワードのペアを外部データベースである ID ストアと比較してチェックします。

PAP は、反復的な試行錯誤攻撃に対する保護がほとんどないため、確実な認証方式ではありません。

（注）　PAP 認証フローを使用する RADIUS には、試行の成功と失敗のロギングが含まれます。

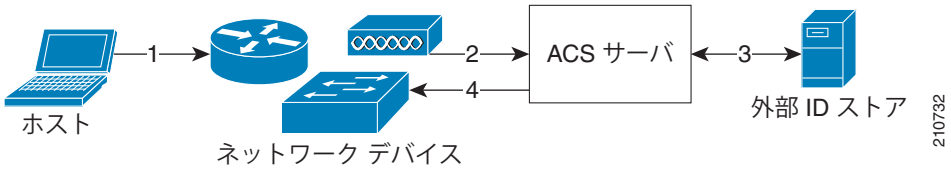
RADIUS PAP 認証

ACS では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。PAP は双方向ハンドシェイク手順を適用します。認証に成功した場合、ACS は確認応答を返します。認証に失敗した場合、ACS は接続を終了するか、認証の要求元にもう一度チャンスを与えます。

認証の要求元が、試行の頻度とタイミングを総合的に制御します。したがって、より強力な認証方式を使用できるサーバは、PAP よりも前にその方式のネゴシエーションを提案します。PAP は RFC 1334 で定義されています。

図 B-1 に、PAP 認証を使用した RADIUS を示します。

図 B-1　PAP 認証を使用した RADIUS の使用例



1	ホストがネットワークに接続します。ホストに応じて任意の通信プロトコルを使用できます。	**3**	ACS が外部 ID ストアを使用してユーザのクレデンシャルを確認します。
2	ネットワーク デバイスが RADIUS アクセス要求を ACS に送信します。	**4**	RADIUS 応答（Access-Accept または Access-Reject）が、決定を適用するネットワーク デバイスに送信されます。

EAP

Extensible Authentication Protocol（EAP）は、無線ネットワークとポイントツーポイント接続のための認証フレームワークです。EAP では、複数の認証方式がサポートされ、目的の認証方式のネゴシエーションに関する一般的な機能と規則が提供されます。

- サーバ認証要求
- クライアント認証応答
- サーバの成功した認証結果
- サーバの失敗した認証結果
- 整合性とセキュリティの条件を満たさない場合のクライアント パケットのサイレントな廃棄
- サーバが開始する EAP 方式ネゴシエーションの規則
- メッセージ シーケンシングと、要求に対する応答のトラッキング
- 再送信

EAP はロックステップ プロトコルです。最初の要求のあと、ACS はクライアントから有効な応答を受信するまで新しい要求を送信できません。

ACS 5.4 では、EAP は RADIUS プロトコルにカプセル化されています。着信および発信 EAP メッセージは、RADIUS EAP-Message 属性（79）に格納されます。特定の EAP メッセージのサイズが最大の RADIUS 属性データ サイズ（253 バイト）よりも大きい場合は、1 つの RADIUS パケットに複数の EAP-Message 属性を含めることができます。

RADIUS State 属性（24）は現在の EAP セッション参照情報を格納し、ACS は実際の EAP セッション データを格納します。

EAP 標準については次の資料で説明されています。

- RFC 3748：Extensible Authentication Protocol（EAP）
- RFC 3579：RADIUS Support For Extensible Authentication Protocol（EAP）

EAP プロセスでは、次の処理が行われます。

1. ホストがネットワークに接続したときに、ネットワーク デバイスが EAP 要求をホストに送信します。
2. ホストが EAP 応答をネットワーク デバイスに送信します。ネットワーク デバイスは、ホストから受信した EAP パケットを RADIUS 要求に埋め込み、EAP サーバとして動作している ACS に送信します。
3. ACS が認証について EAP 方式をネゴシエートします。クライアントは、EAP サーバが提示する EAP 方式に同意するか、Negative Acknowledgment（NAK; 否定応答）で応答して別の EAP 方式のリストを提示できます。サーバとクライアントは、認証のインスタンス化に使用する EAP 方式について合意する必要があります。

表 B-1 に、各タイプの EAP メッセージの EAP コードを示します。

表 B-1　EAP コード

EAP メッセージ タイプ	EAP コード
Accept-request	1
Response	2
Success	3
Failure	4

表 B-2 に、ACS 5.4 でサポートされる EAP 方式を示します。

表 B-2　サポートされる EAP 方式

EAP 方式	説明
EAP-MD5	Message Digest 5 プロトコル。詳細については、「EAP-MD5」（P.B-5）を参照してください。
LEAP	Lightweight Extensible Authentication Protocol。
PEAPv0v1	Protected Extensible Authentication Protocol バージョン 0 およびバージョン 1。詳細については、「PEAPv0/1」（P.B-14）を参照してください。
EAP-FAST	EAP Flexible Authentication via Secured Tunnel（EAP-FAST）プロトコル。詳細については、「EAP-FAST」（P.B-19）を参照してください。
EAP-MSCHAPv2	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。詳細については、「EAP-MSCHAPv2」（P.B-31）を参照してください。

表 B-2　サポートされる EAP 方式 （続き）

EAP 方式	説明
EAP-GTC	EAP Generic Token Card。
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security。詳細については、「クレデンシャルのエクスポート」（P.B-11）を参照してください。

ACS では、EAP タイプ ネゴシエーション、メッセージ シーケンシング、メッセージ再送信など、EAP インフラストラクチャがすべてサポートされます。すべてのプロトコルで、大きなメッセージのフラグメンテーションがサポートされます。

ACS 5.4 では、アクセス サービス設定の一部として、認証の EAP 方式を設定します。アクセス サービスの詳細については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

EAP-MD5

ここでは、次の内容について説明します。

- 「EAP-MD5 の概要」（P.B-5）
- 「ACS 5.4 での EAP-MD 5 フロー」（P.B-5）

EAP-MD5 の概要

EAP Message Digest 5（EAP-MD5）では、一方向のクライアント認証が提供されます。サーバは、クライアントにランダム チャレンジを送信します。クライアントは、チャレンジとそのパスワードを MD5 でハッシュすることにより、その ID を証明します。EAP-MD5 は、公開メディアで使用される場合にはディクショナリ攻撃に対して脆弱です。

これは、ハッカーがチャレンジと応答を見ることができるためです。サーバ認証が行われないため、偽造に対しても脆弱です。

関連トピック

- 「ホスト ルックアップ」（P.4-13）
- 「エージェントレス ネットワーク アクセスの概要」（P.4-13）

ACS 5.4 での EAP-MD 5 フロー

ACS では、ACS 内部 ID ストアに対する EAP-MD5 認証がサポートされます。EAP-MD5 プロトコルを使用している場合は、ホスト ルックアップもサポートされます。「ホスト ルックアップ」（P.4-13）を参照してください。

関連トピック

- 「認証プロトコルと ID ストアの互換性」（P.B-36）
- 「エージェントレス ネットワーク アクセスの概要」（P.4-13）

EAP-TLS

ここでは、次の内容について説明します。

- 「EAP-TLS の概要」（P.B-6）
- 「ACS 5.4 での EAP-TLS フロー」（P.B-13）

EAP-TLS の概要

EAP-TLS は、EAP 認証フレームワークの方式の 1 つであり、802.1x および EAP アーキテクチャに基づいています。802.1x および EAP 認証プロセスに関連するコンポーネントは次のとおりです。

- ホスト：エンド エンティティ。つまり、エンドユーザのマシン。
- AAA クライアント：ネットワーク アクセス ポイント。
- 認証サーバ：ACS。

EAP-TLS 標準については次の資料で説明されています。

- RFC 2716：PPP EAP-TLS Authentication Protocol
- RFC 3079：Deriving Keys for use with Microsoft Point-to-Point Encryption（MPPE）

ここでは、次の内容について説明します。

- 「ユーザ証明書認証」（P.B-6）
- 「PKI 認証」（P.B-7）

ホストでは、EAP-TLS 認証がサポートされている必要があります。アクセス ポイントでは、802.1x 環境で EAP 認証プロセスがサポートされている必要があります（アクセス ポイントは EAP 認証プロトコル タイプを認識しません）。

関連トピック

- 「CA 証明書の設定」（P.8-69）
- 「証明書ベースのネットワーク アクセス」（P.4-9）
- 「ACS と Cisco Security Group Access」（P.4-24）
- 「ACS 5.4 での EAP-TLS フロー」（P.B-13）

ユーザ証明書認証

EAP-TLS は、証明書ベースの認証の相互認証方式です。クライアントとサーバが、デジタル証明書を使用して相互に認証します。認証を成功させるには、証明書がサーバとクライアント上で特定の要件を満たす必要があります。EAP と TLS は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）RFC 標準です。

EAP プロトコルは、初期認証情報、具体的には IEEE 802.1x で確立されている EAP over LAN（EAPOL）のカプセル化を伝達します。TLS は、ユーザ認証とダイナミック短期セッション キー生成に証明書を使用します。

ピアが認証され、セッションが作成されると、情報が一定期間 ACS にキャッシュされます。証明書を追加で交換しなくても、EAP-TLS セッション ステートおよびセッション チケット再開を使用することでセッションを再確立できます。

ACS 5.4 は、EAP-TLS 処理中に使用するサーバ証明書と秘密キーを ACS サーバ上のファイルに保持します。信頼できる認証局（CA）を選択してクライアント証明書に署名できます。

EAP-TLS 認証では、次の 2 つの信頼要素が必要です。

- EAP-TLS ネゴシエーションにおいて、証明書によって署名されているキーペアをユーザが所有していることを RSA 署名検証で確認することによって、エンドユーザの信頼を確立する。

  これによって、エンドユーザが特定のデジタル証明書に対する正当なキー所有者であること、およびその証明書内のユーザ ID に対応していることが確認されます。しかし、ユーザが証明書を所有していることを信頼しても、ユーザ名 / キーペアを確認するに過ぎません。

- 証明書の情報を確認する第三者署名、通常は CA の署名を使用する。第三者による確認は、パスポートのスタンプの確認にあたります。

  パスポートが信頼できるのは、特定の国 / 地域のパスポート発行機関が、そのパスポートを作成する際に行った準備と身元確認が信頼できるためです。ルート証明書の CA の署名がインストールされていることで、デジタル証明書は信頼されます。

ルート証明書の CA の署名のインストールによって提供されるこの第 2 の信頼要素は、必要ない場合もあります。証明書の正当性に対するこのような外部検証が必要ない場合は、ACS 自己署名証明書機能を使用できます。

関係するエンドユーザ クライアントによっては、エンドユーザ クライアント コンピュータ上の信頼できるルート CA 用に、ACS サーバ証明書を発行した CA の CA 証明書がローカル ストレージで必要になる場合もあります。詳細については、「認証局の追加」（P.8-70）を参照してください。

EAP-TLS に準拠した AAA クライアントの例としては、次のものが挙げられます。

- Cisco 802.1x 対応のスイッチ プラットフォーム（Catalyst 6500 シリーズなど）
- Cisco Aironet Wireless ソリューション

EAP-TLS は、セキュアな Cisco Aironet 接続を実現するために、各ユーザ、各接続に固有のダイナミックなセッション キーを生成します。

ACS 5.4 では、現在、証明書の名前制約拡張をサポートします。これは、名前制約拡張を含める発行元のクライアント証明書を受け入れます。また、CA およびサブ CA 証明書についてクライアント認証を確認します。この拡張は、証明書パスの後続の証明書におけるすべてのサブジェクト名の名前空間を定義します。これは、サブジェクト識別名とサブジェクト代替名の両方に適用されます。これらの制限は、指定された名前形式がクライアント証明書に存在する場合にのみ適用されます。ACS 認証は、クライアント証明書が名前空間により除外されている、または許可されていない場合、失敗します。

関連トピック

- 「CA 証明書の設定」（P.8-69）
- 「証明書ベースのネットワーク アクセス」（P.4-9）

PKI 認証

EAP-TLS は、公開キー インフラストラクチャ（PKI）の概念を使用します。

- ホストは、LAN ネットワークに対する認証を行うために有効な証明書を必要とする。
- AAA サーバは、クライアントに対して ID の有効性を示すためにサーバ証明書を必要とする。
- 認証局サーバ インフラストラクチャは、AAA サーバとクライアントに対して証明書を発行する。

SSL/TLS トンネル認証は、両方のピアによって実行され、クライアントによって開始されます。ACS では、トンネルは次のものによって認証できます。

- 両方のピア
- 一方のピア
- クライアントとホストのどちらも行わない

認証なしで構築されているトンネルは匿名トンネルと見なされ、通常は Diffie-Hellman キー交換プロトコルによって構築されます。ACS では、TLS に対して SSL/TLS セッション再開機能がサポートされます。ACS は、トンネル通信の確立に使用されるトンネル キーと暗号を各セッションのキャッシュに保持します。以前のセッションの取得は、クライアントごとに固有のセッション ID に基づいて行われます。

キャッシュ内の各セッションのタイムアウトをプロトコルごとに個別に設定できます。セッションのライフタイムは、カンバセーションの開始時から測定され、TLS セッションの作成時に判断されます。

ACS では、EAP-FAST プロトコルに対して、クライアントとサーバが認識している一般に共有されるキーからのトンネルの確立がサポートされます。2 つのピア間でセキュアに合意されたキーを使用して、トンネルを開くために使用される共有トンネル TLS マスターキーを取得します。このメカニズムでは TLS ネゴシエーションが短くなります。

匿名 Diffie-Hellman トンネルとは、どのピアも自身を認証しない場合にクライアントとサーバ間に完全に匿名のトンネルを確立することを意味します。ACS ランタイムでは、EAP-FAST に対して、定義済み素数と定義済み生成元（2）を使用した匿名 Diffie-Hellman トンネルがサポートされます。匿名 Diffie-Hellman トンネル暗号スイート内ではサーバ認証は行われません。

認証付き Diffie-Hellman トンネルは、匿名 Diffie-Hellman トンネルと同様です。認証付き Diffie-Hellman トンネルの追加要素は、RSA 証明書を通じてピア認証が実行されることです。ACS では、EAP-FAST に対して、サーバが自身の証明書を使用して認証される認証付き Diffie-Hellman トンネルがサポートされます。

内部 EAP 方式に EAP-MSCHAPv2 や EAP-GTC などの他のプロトコルを使用して、トンネル内で追加のクライアント認証が実行されます。

関連トピック

- 「ローカル サーバ証明書の設定」（P.18-14）
- 「CA 証明書の設定」（P.8-69）
- 「証明書認証プロファイルの設定」（P.8-73）

PKI クレデンシャル

ここでは、次の内容について説明します。

- 「PKI の使用方法」（P.B-8）
- 「固定管理証明書」（P.B-9）
- 「信頼証明書のインポート」（P.B-9）
- 「クレデンシャルのエクスポート」（P.B-11）

PKI の使用方法

ACS では、さまざまな PKI 使用例に対して証明書の使用がサポートされます。主な使用例は、PKI がサーバの認証だけでなくクライアントの認証にも使用される EAP-TLS プロトコルです（PEAP と EAP-FAST もサーバ認証に証明書を使用しますが、クライアント認証は実行しません）。PKI クレデンシャルを使用するその他のプロトコルは、LDAPS、HTTPS 管理プロトコル、SSH、および SFTP です。

TLS 関連 EAP プロトコルでは、単一のローカル証明書を使用して、すべての TLS 関連 EAP プロトコルのサーバを認証します。ローカル証明書ストア内に秘密キーが含まれている任意の証明書から、使用する証明書を選択できます。

HTTPS、SFTP、SSH などのその他のプロトコル、およびメッセージ バス ActiveMQ 認証の場合は、ACS を認証するための単一の証明書を設定する必要があります。ローカル証明書ストア内に秘密キーが含まれている任意の証明書から、使用する証明書を選択できます。TLS 関連 EAP プロトコルと HTTPS 管理プロトコルに対して同じローカル証明書を設定できます。

HTTPS、SFTP、SSH、および ActiveMQ では、自動生成される自己署名証明書をサーバ認証の手段として使用できます。

固定管理証明書

ACS は、自己署名証明書を生成および使用して、Web ブラウザ、HTTPS、ActiveMQ SSH、SFTP などのさまざまな管理プロトコルを識別します。

自己署名証明書は、ACS のインストール時に生成され、ACS データベースの外部にあるファイルにローカルに保持されます。これらの証明書は修正またはエクスポートできません。ただし、インポートされた証明書を管理インターフェイスに割り当てることはできます。

信頼証明書のインポート

ACS では、PEM または DER 形式の X509 証明書ファイルがサポートされています。信頼証明書を信頼証明書ストアに追加できます。ACS は、インポートした証明書が X509 形式に準拠していることを確認し、階層証明書の署名の確認は実行しません。ACS では、Microsoft 独自の秘密キー形式もサポートされます。

TLS 関連 EAP プロトコルで直接信頼される取得済み証明書は、EAP CTL としてマークできます。信頼証明書ストアは、重複する信頼証明書を許可していません。証明書の拒否の規則は次のとおりです。

- 2 つの証明書が同じサブジェクトを持つことはできない。
- 2 つの証明書が同じ発行元と同じシリアル番号を持つことはできない。

ローカル証明書の取得

ここでは、ACS が PKI クレデンシャルを取得する方式と、ACS ドメイン内の各 ACS サーバに公開キーと秘密キー ペアを設定する方法について説明します。

X509 証明書には、公開キーを含むクレデンシャルと、一緒に送信されるパスワードで保護された秘密キーを保持する PKCS#12 [?10.1] が含まれています。

ACS ドメインには、複数の ACS サーバがある場合があります。各ドメインには、適切なインターフェイスを通じて自身の ID を証明するための PKI キーペアの固有のセットが必要です。

一部のインターフェイスは、サーバの IP に証明書をより適切にバインディングするために、Web インターフェイスに使用される HTTPS ACS サーバ証明書など、ACS を識別する証明書の Common Name（CN; 共通名）に ACS サーバの IP または FQDN が含まれていることを必要とします。

その他のインターフェイスでは、サーバ間で共有できる共通証明書を使用できる可能性がありますが、共通証明書の使用は推奨しません。各 ACS PKI クレデンシャルは、自己署名証明書から、または一般的な認証局（CA）によって署名された証明書から取得できます。

ACS の識別情報を必要とするプロトコルの場合、クライアントは、少なくとも、各 ACS の識別に使用されるすべての ACS サーバ証明書を支配する最小公倍数的な証明書で展開する必要があります。

組織で使用する PKI ポリシーを選択し、ACS ドメイン用に PKI クレデンシャルを設定できます。

設定された証明書とその秘密キーは、ACS マシンの外部では使用しないでください。

関連トピック

- 「ACS サーバ証明書のインポート」（P.B-10）
- 「自己署名証明書の初期生成」（P.B-10）
- 「証明書の生成」（P.B-10）

ACS サーバ証明書のインポート

ACS サーバ証明書を手動でインポートする場合は、証明書ファイル、秘密キー ファイル、および PKCS#12 秘密キーの復号化に使用される秘密キー パスワードを指定する必要があります。証明書とその秘密キーおよび秘密キー パスワードは、ローカル証明書ストアに追加されます。暗号化されていない秘密キーの場合、ユーザが指定したパスワードは無視されることがあります。

ACS では、PEM または DER 形式の X509 証明書ファイルがサポートされています。ACS は、インポートした証明書が X509 形式に準拠していることを確認し、階層証明書の署名の確認は実行しません。

証明書のインポート時に、TLS 関連 EAP プロトコルや HTTPS 管理プロトコルなど、ACS サーバ証明書を必要とするプロトコルの証明書を設定できます。

（注）　ACS 5.4 では、証明書ベースの認証に EAP プロトコルと HTTPS 管理プロトコルだけを設定できます。

暗号上の機密情報である入力パスワードと秘密キーは、HTTPS チャネルで渡されます。HTTPS サーバ認証の自己署名証明書など、HTTPS を非認証サーバとともに使用することは、この機密情報を渡すのにセキュアな方法ではありません。

関連トピック

- 「信頼証明書のインポート」（P.B-9）
- 「自己署名証明書の初期生成」（P.B-10）
- 「証明書の生成」（P.B-10）

自己署名証明書の初期生成

自動生成される自己署名証明書は、各 ACS サーバのローカル証明書ストアに配置されます。この証明書は、TLS 関連 EAP プロトコルおよび HTTPS 管理プロトコルの ACS の識別に使用されます。

自己署名証明書は、HTTPS 証明書に必要なマシンのホスト名と同じ CN で生成され、ACS のインストール時に生成されます。

証明書の生成

ACS サーバ証明書は、Web インターフェイスを通じて生成できます。このプロセスの出力は、証明書または証明書要求と、対応する秘密キーおよびパスワードです。生成される秘密キーは、ランダムな 128 ビット以上に基づいて自動生成される比較的強力なパスワードを使用して、暗号化された PKCS#12 として構造化されます。

生成する秘密キーの長さは、512、1024、2048、または 4096 ビットから選択できます。ACS で使用される証明書ダイジェスト アルゴリズムは SHA1 および SHA2 256 ビットです。

（注）　SHA2 256 ビット証明書を管理証明書として使用するには、Windows XP SP3 をインストールします。

証明書生成には次の 2 種類があります。

- 自己署名証明書生成：ACS では、X.509 証明書と PKCS#12 秘密キーの生成がサポートされます。PKCS#12 の秘密キーの暗号化に使用されるパスフレーズは、より強力なパスワードを自動的に生成し、秘密キーはローカル証明書ストアに隠されます。

  HTTPS 管理プロトコル、TLS 関連 EAP プロトコル、またはその両方に即時に使用するために、新規に生成された証明書を選択できます。

- 証明書要求生成：ACS では、PKCS#12 秘密キーを使用した PKCS#10 証明書要求の生成がサポートされます。要求は、Web インターフェイスを通じてダウンロードされ、REQ 拡張子を持つ PEM 表現でフォーマットする必要があります。

  PKCS#12 の秘密キーの暗号化に使用されるパスフレーズは、より強力なパスワードを自動的に生成し、秘密キーは ACS データベースに隠されます。RA によってオフラインで署名するために、要求ファイルをダウンロードできます。

  RA が要求に署名したあと、返された署名付き証明書を ACS にインストールし、証明書を対応する秘密キーにバインドできます。証明書とその秘密キーのバインディングは自動的に行われます。

  署名された証明書を秘密キーにバインドしたあとで、HTTPS 管理プロトコル、TLS 関連 EAP プロトコル、またはその両方に即時に使用するようにこの証明書をマークできます。

関連トピック

- 「CA 証明書の設定」（P.8-69）
- 「証明書認証プロファイルの設定」（P.8-73）
- 「ACS 5.4 での EAP-TLS フロー」（P.B-13）

クレデンシャルのエクスポート

一般的な信頼証明書、秘密キーあり、またはなしの ACS サーバ証明書、および以前に生成された証明書要求を証明書ストアからエクスポートできます。秘密キーに対する要求はエクスポートできません。*.CER* 拡張子を持つ証明書ファイルをダウンロードできます。ファイル フォーマットは、ACS にインポートされたフォーマットから変更されません。

秘密キーも含む ACS サーバ証明書については、公開証明書を、*.CER* 拡張子を持つ通常の証明書としてダウンロードできます。ファイル フォーマットは維持されます。

証明書要求については、公開要求をエクスポートして、RA に対する証明書要求を再発行できます。要求は REQ 拡張子付きでダウンロードされ、生成時のフォーマットと同じフォーマットになります。

最高の管理者特権を持つ管理者だけが、証明書秘密キーとそのパスワードをエクスポートできます。このようなアクションのセキュリティに関連する警告は、エクスポート操作を承認するために 2 回表示されます。

この二重チェックのあとに、秘密キー ファイルを *.PVK* 拡張子としてダウンロードできます。また、秘密キー パスワードを *.PWD* 拡張子としてダウンロードできます。秘密キー ファイルのフォーマットは維持されます。

クレデンシャルの配布

すべての証明書は、すべての ACS ノードに配布されてノード間で共有される ACS データベースに保持されます。ACS サーバ証明書は、特定の証明書を使用する特定のノードに関連付けられて指定されます。

公開証明書は、ACS 配布メカニズムを使用して、秘密キーおよび保護された秘密キー パスワードとともに配布されます。ACS は、保護の方式を実装して、秘密キーの指定対象であるサーバ以外のサーバによって秘密キーが使用されることを防ぎます。この保護メカニズムは、暗号化された秘密キーだけに適用されます。

秘密キーの PKI ポリシーでは、秘密キーの指定対象である ACS サーバに関連付けられていない他のエンティティはその秘密キーを使用できないことになっています。ACS では、指定対象の ACS サーバ マシンの外部で使用される可能性を防ぐために、秘密キーの暗号による保護がサポートされています。

ハードウェアの置換と証明書

ハードウェアに障害が発生した場合は、誤動作をしているノードの代わりに新しいノードが使用されます。誤動作しているノードの証明書はプライマリ サーバの配布済みデータベースから削除され、新しいノードの証明書が、新規に置換されたノードに関連付けられているプライマリに渡されます。

この証明書変更のプロセスは、新しいノードがドメインに登録されたときにハードウェア置換プロセスの一部として実行されます。証明書の配布は、サーバの IP アドレスに基づいて行われます。

暗号機密資料のセキュリティ保護

ACS データベースに格納される PKI 関連のキーにはいくつかの種類があります。これらのキーには、シスコのセキュリティ ベースラインの一部である SEC-RCV-CRED-2 に準拠する必要のあるさまざまな暗号保管要件があります。これらの要件は次のとおりです。

- 通常は証明書内にある公開キーは、クライアントにクリア テキストで渡すために使用され、公開キーだけを含んでいるため、公開されたプレーンな状態で格納できる。
- 秘密キーは、比較的強力なパスワードを使用して、PKCS#12 として暗号化して格納する必要がある。
- PKCS#12 秘密キーのパスワードは、ACS データベースに格納する必要がある。ACS データベースは暗号化されるため、セキュリティ上の重大な問題は発生しません。ACS 5.4 は、すべての ACS サーバにデータベース全体を配布します。

  ACS は、そのマシンに対してだけ存在するパスワードを使用して秘密キー パスワードを暗号化するため、秘密キーが他のマシンによって使用される可能性が阻止されます。秘密キーのパスワード キーは、ACS ファイルシステムの */opt/CSCOacs/config/prikeypwd.key* に保持されます。

tomcat キーストアなどのその他の証明書リポジトリには、ACS データベースと同じプロパティが必要です。秘密キーは、データベース内で常にセキュリティ保護されているパスワードによって暗号化されます。

秘密キーとパスワードのバックアップ

ACS データベース全体が、すべての証明書、秘密キー、および暗号化された秘密キー パスワードとともにプライマリ ACS 上に配布されてバックアップされます。プライマリ サーバの秘密キー パスワード キーも、プライマリのバックアップとともにバックアップされます。

その他のセカンダリ ACS の秘密キー パスワード キーはバックアップされません。バックアップは暗号化され、比較的セキュリティ保護された状態で ACS サーバの内部および外部に渡すこともできます。バックアップ内の秘密キーは、PKCS#12 とバックアップ ファイルの暗号化によって保護されます。PKCS#12 秘密キーを開くために使用されるパスワードは、バックアップ暗号化で保護されます。

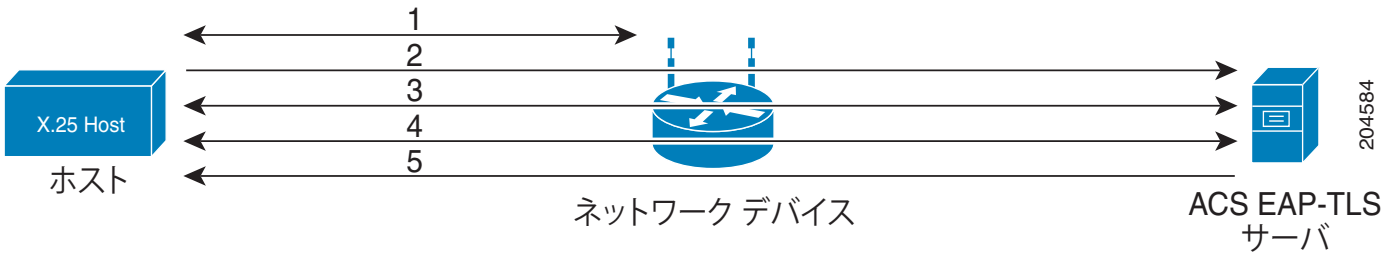
ACS 5.4 での EAP-TLS フロー

EAP-TLS サーバは、EAP 要求および応答パケットに基づくパケットを使用して、クライアントとデータを交換します。パケットは、特定の EAP-TLS データによって拡張されます。ACS は、EAP-TLS サーバとして機能し、Open Secure Sockets Layer（OpenSSL/CiscoSSL）ライブラリを使用して TLS カンバセーションを処理します。ACS EAP-TLS サーバは、クライアントとサーバ間の暗号化通信に使用される 128 ビットの MPPE 送信キーおよび受信キーを生成します。

ACS EAP-TLS サーバは、ベンダー コード Microsoft（311）、属性 MS-MPPE-Send-Key（16）および MS-MPPE-Recv-Key（17）を使用して、ベンダー固有の RADIUS 属性（26）でクライアントに MPPE キーを送信します。

図 B-2 に、ステートレス セッション再開オプションを使用しない場合のホスト、ネットワーク デバイス、および ACS EAP-TLS サーバ間の EAP-TLS 処理フローを示します。

図 B-2　EAP-TLS フロー



1	ホストがネットワークに接続します。ネットワーク デバイスが EAP 要求をホストに送信します。	**2**	ホストが EAP 応答をネットワーク デバイスに送信します。ネットワーク デバイスは、ホストから受信した EAP パケットを RADIUS RADIUS Access-Request に埋め込んで ACS に送信します。
3	ACS が認証について EAP 方式をネゴシエートします。サーバとクライアントは、EAP-TLS 認証をインスタンス化するための EAP 方式のネゴシエーション中に、EAP-TLS（EAP 要求方式 13）を使用するという合意に達する必要があります。	**4**	クライアント（ホスト）とサーバ（ACS）が証明書を交換します。この交換にはいくつかのメッセージが関係します。 クライアントとサーバが相互に認証されたあとで EAP-TLS 認証が成功し、各側が相手側に認証されたことを認識します。
5	ACS が、EAP Success（または EAP Failure）メッセージをホストに返し、セッション キーを含む RADIUS Access-Accept（または RADIUS Access-Reject）をネットワーク デバイスに返します。		

（注）　ホストと ACS 間のすべての通信は、ネットワーク デバイスを通じて行われます。

次の場合は EAP-TLS 認証が失敗します。

- サーバがクライアントの証明書を確認できず、EAP-TLS 認証を拒否した場合。
- クライアントがサーバの証明書を確認できず、EAP-TLS 認証を拒否した場合。

  証明書の確認は次の場合に失敗します。

  - 証明書の有効期限が切れている。
  - サーバまたはクライアントが証明書の発行元を見つけられない。
  - 署名のチェックに失敗した。
- クライアントがケースを廃棄したことにより、EAP パケットが不正な形式になった場合。

EAP-TLS では、セッション再開機能もサポートされます。ACS では、すでに完全な EAP-TLS 認証を渡したユーザを高速に再認証するために、EAP-TLS セッション再開機能がサポートされます。EAP-TLS 設定にセッション タイムアウト期間が含まれる場合、ACS はタイムアウト期間中に各 TLS セッションをキャッシュします。

ユーザが設定した EAP-TLS セッション タイムアウト期間内に再接続すると、ACS は、EAP-TLS セッションを再開し、証明書チェックなしで TLS ハンドシェイクだけでユーザを再認証します。

ACS 5.4 は、セッション ステートがサーバ上に格納されなくても、EAP-TLS セッション再開をサポートします。また、RFC 5077 で記述されているセッション チケット拡張をサポートします。ACS サーバはチケットを作成して EAP-TLS クライアントにそのチケットを送信します。クライアントはセッションを再開するためにそのチケットを ACS に提示します。

ステートレス セッション再開は、1 つのノードによって発行されたセッション チケットが別のノードによって受け入れられるように、分散展開でサポートされます。

チケット全体は、128 ビット認証キーとともに MAC を使用してそのフィールドによって認証されます。これらのフィールドは、チケットにある 128 ビット暗号キーおよび IV とともに AES-CBC を使用して暗号化されます。ACS 管理者はセッション チケットに対して制限付きライフタイムを設定します。

関連トピック

- 「PAC のタイプ」（P.B-23）
- 「ユーザ証明書認証」（P.B-6）

PEAPv0/1

ここでは、次の内容について説明します。

- 「PEAP の概要」（P.B-15）
- 「EAP-MSCHAPv2」（P.B-31）

ACS 5.4 では、次の PEAP サプリカントがサポートされます。

- Microsoft Built-In Clients 802.1x XP（PEAPv0 だけ）
- Microsoft Built-In Clients 802.1x Vista（PEAPv0 だけ）
- Microsoft Built-In Clients 802.1x Windows 7
- CSSC v.4.0

- CSSC v.5
- Cisco AC 3.x
- Funk Odyssey Access Client 4.0.2 および 5.x
- Intel Supplicant 12.4.x

PEAP の概要

PEAP は、EAP トランザクションの暗号化に使用するクライアント サーバ型のセキュリティ アーキテクチャです。これによって、EAP 認証の内容が保護されます。PEAP では、サーバ側公開キー証明書を使用してサーバが認証されます。

次に、クライアントと認証サーバ間に暗号化された SSL/TLS トンネルが作成されます。その後クライアントを認証するために行われる認証情報の交換は暗号化され、ユーザ クレデンシャルは盗聴から保護されます。

PEAP は EAP-TLS に似ていますが、別のクライアント認証方式を使用します。PEAP は、サーバ証明書を使用した認証、TLS トンネル、およびその暗号化されたトンネルを通じたクライアント認証を提供します。EAP-TLS とは異なり、PEAP ではクライアントが EAP-MSCHAPv2 などの別の EAP タイプを使用する必要があります。

PEAP 認証には常に 2 つのフェーズがあります。

- フェーズ 1 では、エンドユーザ クライアントが ACS を認証します。ここでは、サーバ証明書が要求され、ACS がエンドユーザ クライアントに対して認証されます。この結果、フェーズ 2 で送信されるユーザまたはマシンの資格情報が、信頼できる CA によって発行された証明書を持つ AAA サーバに送信されます。最初のフェーズは、TLS ハンドシェイクを使用して、エンドユーザ クライアントと AAA サーバ間に SSL トンネルを確立します。

（注） 関係するエンドユーザ クライアントによっては、エンドユーザ クライアント コンピュータ上の信頼できるルート CA 用に、ACS サーバ証明書を発行した CA の CA 証明書がローカル ストレージで必要になる場合もあります。

- 2 番めのフェーズでは、ACS が EAP 認証プロトコルを使用して、ユーザまたはマシンのクレデンシャルを認証します。フェーズ 1 で作成された SSL トンネルによって EAP 認証が保護されます。

  フェーズ 2 中にネゴシエーションされる内部方式認証タイプは EAP-MSCHAPv2、EAP-GTC、または EAP-TLS になります。特定の内部 EAP 方式と外部 PEAP 方式の組み合わせは、たとえば、PEAP(EAP-MSCHAPv2) または PEAP(EAP-GTC) のようにカッコ () を使用して示されます。

  PEAP によりセキュリティが向上していますが、その 1 つに ID 保護があります。この ID 保護により、すべての PEAP トランザクションにおいてユーザ名を保護できます。PEAP のフェーズ 1 が完了すると、通常はクリア テキストで送信されるユーザ名情報も含めて、すべてのデータが暗号化されます。

  Microsoft PEAPv0 クライアントでは ID 保護は使用できません。Microsoft PEAPv0 クライアントは、PEAP 認証のフェーズ 1 でユーザ名をクリア テキストで送信します。

ACS 5.4 では、PEAP は RADIUS プロトコルにカプセル化されています。内部方式 EAP メッセージは、EAP-TLV 方式にカプセル化されています。ACS では、MS PEAP に暗号化バインド TLV 拡張もサポートします。ACS 5.4 では、故意にレガシー クライアントだけに PEAPv0 をイネーブルにするオプションがあります。

サポートされる PEAP 機能

ここでは、次の内容について説明します。

- 「サーバ認証および非認証トンネル確立モード」（P.B-16）
- 「高速再接続」（P.B-16）
- 「セッションの再開」（P.B-16）
- 「任意のパラメータの保護された交換」（P.B-17）
- 「暗号化バインド TLV 拡張」（P.B-17）

サーバ認証および非認証トンネル確立モード

トンネルの確立は、攻撃者がクライアントとネットワーク アクセス サーバ（NAS）間にパケットを挿入することを防いだり、セキュリティの低い EAP 方式のネゴシエーションを可能にしたりするのに役立ちます。また、暗号化された TLS チャネルは、ACS に対する DoS 攻撃を防ぐのに役立ちます。

クライアント EAP メッセージは常に RADIUS Access-Request メッセージで送信され、サーバ EAP メッセージは常に RADIUS Access-Challenge メッセージで送信されます。EAP Success メッセージは、常に RADIUS Access-Accept メッセージで送信されます。

EAP Failure メッセージは、常に RADIUS Access-Reject メッセージで送信されます。ポリシー コンポーネントが設定されていないかぎり、クライアントの PEAP メッセージは、RADIUS クライアントのメッセージが廃棄される原因になることがあります。

高速再接続

セッションを再開するときに、認証時間を短縮する方法として内部方式をスキップすることもできます。これは高速再接続とも呼ばれます。トンネルが構築されたあと、認証フローは認証情報の交換に直接進みます。認証に成功した場合には Result TLV Success（v0）/ トンネル EAP Success メッセージ、認証に失敗した場合には EAP Failure メッセージが認証情報の交換に使用されます。

高速再接続オプションをイネーブルにするように ACS を設定できます。認証に成功したあと、クライアントは一定の期間にわたって高速再接続を実行できます。PEAP 高速再接続によって、クライアントによる認証要求から ACS による応答までの遅延時間が短縮されます。

また、高速再接続では無線クライアントが認証の要求を繰り返すことなくアクセス ポイント間を移動できるため、クライアントとサーバのリソース要件が軽減されます。

高速再接続を可能にするには、ユーザ認証（内部方式）に使用されるユーザ ID とプロトコルを TLS セッションとともにキャッシュする必要があります。

セッションの再開

ACS は、PEAP 認証済みユーザ セッションに対して、セッション再開機能をサポートしています。この機能がイネーブルの場合、ACS は、ユーザが PEAP 認証のフェーズ 2 で正常に認証された場合にかぎり、PEAP のフェーズ 1 で作成された TLS セッションをキャッシュします。

ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、ACS はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。

ACS は、完全認証に成功したあと、セッションをキャッシュに格納します。クライアントは、特定の期間中は同じセッションの再開を試行できます。サーバ証明書は提示されず、トンネルは OpenSSL/CiscoSSL セッション キャッシュからのセッション情報を使用して構築されます。認証フローは内部方式に直接進みます。

クライアントがセッション再開を実行しようとしたときにタイムアウト期間が経過していた場合、ACS は完全認証フローに戻ります。

セッション再開とタイムアウトの値を設定できます。

任意のパラメータの保護された交換

TLV タプルは、セキュアなチャネル内のピアと ACS 間で任意の情報を交換する方法を提供します。

暗号化バインド TLV 拡張

MS PEAP 認証の暗号化バインド TLV 拡張は、EAP ピア（クライアント）と EAP サーバ（ACS）の両方が、PEAP 認証の内部および外部 EAP 認証に参加するように保証するために使用されます。

この暗号化バインド プロセスは PEAP サーバと PEAP ピア間の 2 ウェイ ハンドシェイクとして実行されます。これは PEAP サーバから PEAP ピアに送信される暗号化バインド要求と PEAP ピアから PEAP サーバに返送される暗号化バインド応答の 2 つのメッセージで構成されます。この機能は、MS Win 7 サプリカントのプライマリとして ACS で実行されます。

TLV には、入力データとして TLV 本文を持つ HMAC-SHA1-160 に基づく PRF、PEAP のトンネル キーから取得されるキー、およびセッション キーとしての内部方式を使用して計算される複合 MAC が含まれます。ACS は暗号化バインド応答 TLV をクライアントから受信することを確認します。複合 MAC が予測されるデータに等しくない場合、ACS はカンバセーションに失敗します。暗号化バインドはすべての内部方式で利用可能です。保護される終端フローに違いがあるため、暗号化バインドは PEAPv0 に制限されます。暗号化バインドは PEAP セッション再開および高速再接続にも適用されます。一部のサプリカントは暗号化バインド TLV をサポートしない場合があります。暗号化バインドをサポートしないサプリカントに暗号化バインド TLV を送信する場合、サプリカントは適切な暗号化バインド応答を提供しません。この正しくない応答は ACS のエラーと見なされ、PEAP_CRYPTOBINDING_FAILED メッセージが添付されます。

ACS 5.4 での PEAP フロー

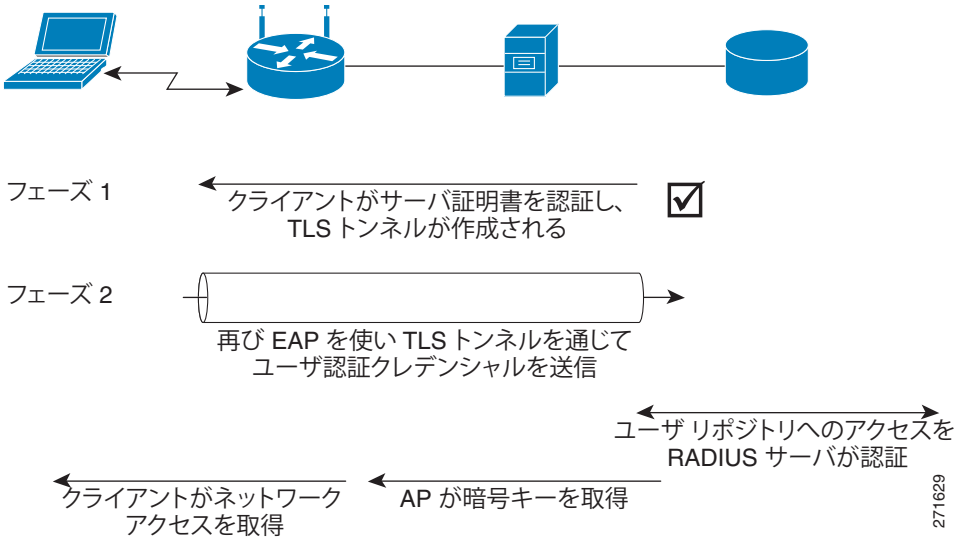
PEAP プロトコルでは、PKI ベースのセキュア トンネルの確立と、トンネル内の内部方式としての EAP-MSCHAPv2 プロトコルを使用して、ACS とピア間の認証を可能にします。ローカル証明書は、ピアによって確認されること（サーバ認証モード）と確認されないこと（サーバ非認証モード）があります。

この項の構成は、次のとおりです。

- 「TLS トンネルの作成」（P.B-18）
- 「MSCHAPv2 による認証」（P.B-19）

図 B-3 に、ホスト、アクセス ポイント、ネットワーク デバイス、および ACS EAP-TLS サーバ間の PEAP 処理フローを示します。

図 B-3　PEAP 処理フロー



TLS トンネルの作成

TLS トンネルの作成プロセスについて次に説明します。

1	論理リンクの作成後、無線 AP が EAP-Request/Identity メッセージを無線クライアントに送信します。	**2**	無線クライアントは、無線クライアントの ID（ユーザ名またはコンピュータ名）が含まれている EAP-Response/Identity メッセージで応答します。
3	無線 AP が EAP-Response/Identity メッセージを ACS に送信します。この時点から、無線 AP をパススルー デバイスとして使用して、ACS と無線クライアント間の論理通信が行われます。	**4**	ACS が EAP-Request/Start PEAP メッセージを無線クライアントに送信します。
5	無線クライアントと ACS が、TLS チャネルの暗号スイートのネゴシエーションに使用する一連の TLS メッセージを交換します。ACS 5.4 では、PEAP にクライアント証明書は使用されません。	**6**	PEAP ネゴシエーションの終了時に、ACS が無線クライアントに対する自己認証を行います。両方のノードが、（パスワードではなく公開キー暗号を使用して）TLS チャネルの相互の暗号化と署名キーを判断しています。

MSCHAPv2 による認証

TLS トンネルの作成後は、次の手順に従って、MSCHAPv2 で無線クライアントのクレデンシャルを認証します。

1	ACS が EAP-Request/Identity メッセージを送信します。	2	無線クライアントは、無線クライアントの ID（ユーザ名またはコンピュータ名）が含まれている EAP-Response/Identity メッセージで応答します。
3	ACS がチャレンジ文字列を含む EAP-Request/EAP-MSCHAPv2 チャレンジ メッセージを送信します。	4	無線クライアントは、ACS チャレンジ文字列への応答と ACS のチャレンジ文字列を含む EAP-Response/EAP-MSCHAPv2 Response メッセージで応答します。
5	ACS が EAP-Request/EAP-MSCHAPv2 成功メッセージを送信します。このメッセージは、無線クライアント応答が正しかったことを示し、無線クライアントのチャレンジ文字列への応答を含んでいます。	6	無線クライアントは、ACS 応答が正しかったことを示す EAP-Response/EAP-MSCHAPv2 確認応答メッセージで応答します。
7	ACS が EAP-Success メッセージを送信します。		

この相互認証の終了時に、無線クライアントは正しいパスワードを認識していることの証明（ACS チャレンジ文字列への応答）を提供し、ACS は正しいパスワードを認識していることの証明（無線クライアント チャレンジ文字列への応答）を提供しています。メッセージ交換全体が、PEAP で作成された TLS チャネルを通じて暗号化されます。

関連トピック

- 「認証プロトコルと ID ストアの互換性」（P.B-36）
- 「PEAP の設定」（P.18-3）

EAP-FAST

ここでは、次の内容について説明します。

- 「EAP-FAST の概要」（P.B-19）
- 「ACS 5.4 での EAP-FAST フロー」（P.B-27）
- 「EAP-FAST PAC 管理」（P.B-28）

EAP-FAST の概要

EAP Flexible Authentication via Secured Tunnel（EAP-FAST）プロトコルは、パブリックにアクセス可能な新しい IEEE 802.1x EAP タイプです。これは、強力なパスワード ポリシーを適用できないユーザがデジタル証明書を必要としない 802.1x EAP タイプを展開できるように、シスコが開発しました。

EAP-FAST は、さまざまなタイプのユーザ データベースやパスワード データベース、パスワードの変更や有効期間をサポートしています。そのため、柔軟性があり、展開や管理も容易です。EAP-FAST の詳細と、他の EAP タイプとの比較については、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

EAP-FAST は、TLS トンネルで EAP トランザクションを暗号化するクライアント サーバ型のセキュリティ アーキテクチャです。その点では PEAP に似ていますが、EAP-FAST トンネルの設定は、各ユーザに固有の強力な秘密に基づいていることが大きな相違点です。

これらの秘密は Protected Access Credentials（PAC）と呼ばれ、ACS が、ACS にしか知られていないマスターキーを使用して生成します。共有秘密情報に基づくハンドシェイクは PKI に基づくハンドシェイクよりも元々速いため、EAP-FAST は、サプリカントと ACS 間のトラフィックを暗号化するために TLS 接続を確立する高度な EAP プロトコル（EAP-TLS と PEAP を含む）の中で最も高速です。EAP-FAST の実装には証明書管理は必要ありません。

EAP-FAST は 3 つのフェーズで実行されます。

- フェーズ 0：フェーズ 0 は EAP-FAST に固有のフェーズであり、EAP-FAST エンドユーザ クライアントに、ネットワーク アクセスを要求するユーザ用の PAC を提供するトンネル セキュア機能です （「自動インバンド PAC プロビジョニング」（P.B-24）を参照）。

  エンドユーザ クライアントに PAC を提供することが、フェーズ 0 の唯一の目的です。匿名インバンド プロビジョニングの場合、トンネルは匿名の Diffie-Hellman キー交換に基づいて確立されます。認証付きインバンド プロビジョニングでは、他の暗号スイートを使用します。

  EAP-MSCHAPv2 または EAP-GTC 認証が成功すると、ACS はユーザに PAC を提供します。EAP-FAST フェーズ 0 をサポートしているデータベースを確認するには、「認証プロトコルと ID ストアの互換性」（P.B-36）を参照してください。

  （注）　フェーズ 0 は任意であり、PAC は手動でエンドユーザ クライアントに提供できます （「手動 PAC プロビジョニング」（P.B-25）を参照）。

  [Allow Anonymous In-Band PAC provisioning] オプションを選択すると、EAP-FAST フェーズ 0 を使用してエンドユーザ クライアントに PAC が提供されます。このチェックボックスをオンにすると、ACS は、エンドユーザ クライアントに新規 PAC を提供するために、そのクライアントとの安全な接続を確立します。

  このオプションでは、エンドユーザ クライアントと ACS の間で匿名の TLS ハンドシェイクが可能になります（EAP-MSCHAPv2 と EAP-GTC が内部方式として使用されます）。

  [Allow Authenticated In-Band PAC provisioning] オプションを選択すると、TLS サーバ側の認証とともに EAP-FAST フェーズ 0 を使用してエンドユーザ クライアントに PAC がプロビジョニングされます。このオプションを選択する場合は、サーバ証明書をインストールする必要があります。

  通常、EAP-FAST のフェーズ 0 ではネットワーク アクセスは認可されません。ただし、[Accept Client on Authenticated Provisioning] オプションを選択した場合は、ACS が PAC プロビジョニングのフェーズ 0 の正常終了時に RADIUS Access-Accept（EAP Success を含む）を送信し、クライアントは再認証を強制されません。

  このオプションは、[Allow Authenticated In-Band PAC Provisioning] オプションもイネーブルの場合にだけ、イネーブルにすることができます。

- フェーズ 1：フェーズ 1 では、ACS とエンドユーザ クライアントが、エンドユーザ クライアントによって示された PAC に基づいて TLS トンネルを確立します。このフェーズでは、ネットワーク アクセスの取得を試行するユーザ用の PAC がエンドユーザ クライアントに提供されていることと、PAC の期限が切れていないことが必要です。PAC プロビジョニングを実行する手段は関係ありません。自動プロビジョニングと手動プロビジョニングのどちらでも使用できます。

- フェーズ 2：フェーズ 2 では、ACS が EAP-MSCHAPv2 または EAP-GTC を内部 EAP 方式として使用して、フェーズ 1 で作成された保護 TLS トンネルからユーザのクレデンシャルを認証します。EAP-FAST フェーズ 2 をサポートしているデータベースを確認するには、「認証プロトコルと ID ストアの互換性」（P.B-36）を参照してください。

フェーズ 1 とフェーズ 2 は、同じ EAP-FAST カンバセーションの後続部分です。

EAP-FAST は、すべての EAP-FAST トランザクションでユーザ名を保護できます。ACS は、フェーズ 1 で示されたユーザ名に基づいてユーザ認証を実行しませんが、フェーズ 1 でユーザ名が保護されるかどうかは、エンドユーザ クライアントによって異なります。

フェーズ 1 でエンドユーザ クライアントが実際のユーザ名を送信しなければ、ユーザ名は保護されます。EAP-FAST のフェーズ 1 が完了すると、通常はクリア テキストで送信されるユーザ名情報も含めて、すべてのデータが暗号化されます。

ACS は、Windows ユーザ データベースによって認証されたユーザに対して、EAP-FAST でのパスワード エージングをサポートしています。パスワード エージングは、EAP-FAST のフェーズ 0 またはフェーズ 2 で処理できます。フェーズ 0 中にパスワード エージングでユーザがパスワードを変更する必要がある場合は、新規パスワードがフェーズ 2 で有効になります。

EAP-FAST の利点

EAP-FAST は、他の認証プロトコルに比べて次の利点があります。

- 相互認証：EAP サーバはピアの ID と信頼性を確認できる必要があり、ピアは EAP サーバの信頼性を確認できる必要があります。
- パッシブ ディクショナリ攻撃に対する耐性：多くの認証プロトコルでは、ピアから EAP サーバにパスワードがクリア テキストまたはハッシュとして明示的に提供される必要があります。
- Man-in-the-Middle（MitM; 中間者攻撃）に対する耐性：相互認証された保護トンネルの確立時に、プロトコルは、ピアと EAP サーバ間のカンバセーションに攻撃者が情報を挿入することを防ぐ必要があります。
- MSCHAPv2 や GTC などの多くの異なるパスワード認証インターフェイスをサポートできる柔軟性：EAP-FAST は、同じサーバで複数の内部プロトコルをサポートできる拡張可能なフレームワークです。
- 効率性：無線メディアを使用する場合、ピアは計算資源と電源リソースを制限されます。EAP-FAST では、ネットワーク アクセス通信の計算を軽量化できます。
- 認証サーバのユーザごとの認証状態要件の最小化：大規模な展開では、通常、多くのサーバが多くのピアに対する認証サーバとして機能する必要があります。

  ユーザ名とパスワードを使用してネットワークにアクセスするのと同じように、ピアが同じ共有秘密情報を使用してトンネルのセキュリティを確保することが推奨されます。EAP-FAST は、サーバがキャッシュおよび管理する必要のあるユーザごとおよびデバイスごとの状態を最小化できるようにする一方で、ピアによる単一の強力な共有秘密情報の使用を容易にします。

ACS 5.4 での EAP-FAST

ACS では、PKI または ADHP に基づく共有秘密クレデンシャル（PAC）を使用したピアのインバンド プロビジョニングがサポートされます（フェーズ 0）。ピアの認証と、ネットワークへのピア アクセスの許可は、フェーズ 1 とフェーズ 2 で実装されます。

ACS 5.4 では、EAP-FAST バージョン 1 および 1a がサポートされます。

ここでは、次の内容について説明します。

- 「マスターキーについて」（P.B-22）
- 「PAC について」（P.B-22）
- 「プロビジョニング モード」（P.B-23）
- 「PAC のタイプ」（P.B-23）
- 「ACS でサポートされる PAC の機能」（P.B-25）

- 「マスターキー生成と PAC TTL」（P.B-27）
- 「TLS 再ネゴシエーション用の EAP-FAST」（P.B-27）

マスターキーについて

EAP-FAST マスターキーは、ACS が自動的に生成し、ACS だけが認識している強力な秘密です。マスターキーがエンドユーザ クライアントに送信されることはありません。EAP-FAST でマスターキーが必要な理由は 2 つあります。

- **PAC 生成**：ACS は、アクティブ マスターキーを使用して PAC を生成します。PAC の詳細については、「PAC について」（P.B-22）を参照してください。
- **EAP-FAST フェーズ 1**：ACS は、エンドユーザ クライアントによって示された PAC が、認識しているマスターキーのいずれかによって生成されたかどうかを判別します。

EAP-FAST のセキュリティを強化するために、ACS は PAC の生成に使用するマスターキーを変更します。ACS は、定義された [Master Key Generation Period] の値を使用して、新規マスターキーを生成するタイミングとすべてのマスターキーの経過時間を決定します。

アクティブ マスターキーは、ACS が PAC を生成するために使用するマスターキーです。[Master Key Generation Period] の設定によって、マスターキーがアクティブである期間が決まります。アクティブであるマスターキーは常に 1 つだけです。PAC の更新またはプロビジョニングが必要かどうかが TTL 値によってどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-27）を参照してください。

PAC について

PAC は、ACS および EAP-FAST エンドユーザ クライアントをイネーブルにし、互いを認証して EAP-FAST フェーズ 2 で使用する TLS トンネルを確立する強力な共有秘密です。ACS は、アクティブ マスターキーとユーザ名を使用して PAC を生成します。

PAC は、次のもので構成されています。

- **PAC-Key**：クライアント（およびクライアント デバイス）とサーバの ID にバインドされている共有秘密情報。
- **PAC Opaque**：クライアントがキャッシュしてサーバに渡す暗号化されたフィールド。サーバは、PAC-Key およびクライアント ID を復号化して、クライアントとの相互認証を行います。
- **PAC-Info**：クライアントがさまざまな PAC をキャッシュできるように、少なくとも認証局 ID が含まれています。PAC の有効期限などの情報が含まれていることもあります。

EAP-FAST エンドユーザ クライアントは、クライアントを使用してネットワークにアクセスする各ユーザの PAC を保存します。さらに、EAP-FAST をサポートする AAA サーバには独自の認証局 ID があります。エンドユーザ クライアントは、ユーザの PAC を、それを生成した AAA サーバの認証局 ID に関連付けます。PAC により PKI（デジタル証明書）が不要になります。

EAP-FAST フェーズ 1 で、エンドユーザ クライアントは、現在のユーザ用、および EAP-FAST トランザクションの開始時に ACS によって送信された認証局 ID 用に備えている PAC を示します。PAC プロビジョニングという、エンドユーザ クライアントに PAC を提供する手段については、「自動インバンド PAC プロビジョニング」（P.B-24）および「手動 PAC プロビジョニング」（P.B-25）を参照してください。

マスターキー生成値を修正しても、すでに作成された PAC には影響しません。マスターキー生成値に対して行う修正では、次にマスターキーが生成される期間を指定します。

プロビジョニング モード

ACS は、アウトオブバンド プロビジョニング モードとインバンド プロビジョニング モードをサポートしています。インバンド プロビジョニング モードは、キー共有に対する匿名 DH または認証付き DH、あるいは RSA アルゴリズムによって確立された TLS トンネル内で機能します。

ユーザの資格情報が危険にさらされる可能性を最小限に抑えるために、保護されたトンネルの外部ではクリア テキスト パスワードを使用しないでください。したがって、EAP-MSCHAPv2 または EAP-GTC を使用して、保護されたトンネル内でユーザのクレデンシャルを認証します。PAC に含まれている情報は、内部 EAP 方式の完了後に認証セッションでも使用できます。

EAP-FAST は、機能が拡張されて、PAC プロビジョニングが実行される認証済みトンネル（サーバ証明書を使用）をサポートするようになりました。EAP-FAST および特にサーバ証明書に対する機能拡張となる、新しい暗号スイートが使用されます。

認証済みトンネルを使用するプロビジョニング セッションの終わりに、ネットワーク アクセスを許可できます。これは、サーバとユーザが互いを認証したためです。

ACS は、プロビジョニングのためにトンネル内部で次の EAP 方式をサポートしています。

- EAP-MSCHAPv2
- EAP-GTC

デフォルトでは、EAP-MSCHAP 内部方式を使用する場合、ACS は、初期認証試行に失敗した場合に [Service] ページで設定した値まで TLS トンネルの内部での認証試行を許可します。SSL トンネル内で 4 回めの認証試行に失敗したあと、ACS は EAP カンバセーションを終了し、その結果 RADIUS Access-Reject が生成されます。

ACS では、ACS にダウンロードできる PAC を生成できるようにアウトオブバンド PAC ファイルの発行がサポートされます。

PAC のタイプ

ACS では、次に示す PAC のタイプがサポートされます。

- トンネル v1 および v1a
- SGA
- マシン
- 認可

ACS は、共有秘密を含む PAC をサプリカントにプロビジョニングします。この共有秘密は、サプリカントと ACS の間に TLS トンネルを構築する場合に使用されます。ACS がサプリカントにプロビジョニングする PAC は、状況に応じてさまざまな用途を持ちます。

サーバ ポリシーに従って、次のタイプの PAC が ACS にプロビジョニングされます。

- **トンネル/マシン PAC**：ユーザまたはマシン情報を含みますが、ポリシー情報は含みません。
- **ユーザ認可 PAC**：ポリシー要素（たとえば、ユーザ認証で使用される内部方式など）を含みます。ユーザ認可 PAC を使用すると、「セッションの再開」（P.B-16）で説明しているように、ステートレスなサーバ セッション再開ができるようになります。

エンドユーザ クライアントが PAC を受信するさまざまな手段を次に示します。

- **PAC プロビジョニング**：エンドユーザ クライアントに PAC がない場合に必要です。マスターキーと PAC の状態によって PAC プロビジョニングが必要かどうかがどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-27）を参照してください。

  PAC プロビジョニングについては次の 2 つの手段がサポートされています。

  - **自動インバンド PAC プロビジョニング**：セキュア ネットワーク接続を使用して PAC を送信します。詳細については、「自動インバンド PAC プロビジョニング」（P.B-24）を参照してください。
  - **手動プロビジョニング**：ACS を使用してユーザ用の PAC ファイルを生成し、エンドユーザ クライアントを実行しているコンピュータに PAC ファイルをコピーし、エンドユーザ クライアントに PAC ファイルをインポートする必要があります。詳細については、「手動 PAC プロビジョニング」（P.B-25）を参照してください。

- **PAC 更新**：[Proactive PAC Update When] フィールドで指定した値に基づいて行われます。マスターキーと PAC の状態によって PAC が更新されるかどうかがどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-27）を参照してください。

PAC については、PAC TTL 設定によって次の 2 つの状態が決定されます。

- **アクティブ**：PAC TTL よりも新しい PAC はアクティブと見なされ、EAP-FAST フェーズ 1 の完了に使用できます。
- **期限切れ**：PAC TTL よりも古い PAC は期限切れと見なされます。EAP-FAST フェーズ 2 の終わりに ACS がユーザ用の新規 PAC を生成し、それをエンドユーザ クライアントに提供します。

自動インバンド PAC プロビジョニング

EAP-FAST フェーズ 0 と同じ自動インバンド PAC プロビジョニングは、セキュア ネットワーク接続を介して新規 PAC をエンドユーザ クライアントに送信します。自動インバンド PAC プロビジョニングをサポートするように ACS とエンドユーザ クライアントを設定した場合、自動インバンド PAC プロビジョニングにネットワーク ユーザまたは ACS 管理者の介入は必要ありません。

（注） ACS が各ユーザを単一の ID ストアと関連付ける場合、自動インバンド PAC プロビジョニングを使用するには、EAP-FAST フェーズ 0 と互換性のある ID ストアで EAP-FAST ユーザが認証されている必要があります。ACS が EAP-FAST フェーズ 0 とフェーズ 2 をサポートできるデータベースについては、「認証プロトコルと ID ストアの互換性」（P.B-36）を参照してください。

通常、EAP-FAST のフェーズ 0 ではネットワーク アクセスは認可されません。この一般的なケースでは、クライアントがフェーズ 0 の PAC プロビジョニングを正常に実行したあとで、クライアントは新しいフェーズ 1 トンネル確立を開始するために新しい EAP-FAST 要求を送信してから、フェーズ 2 の認証を行う必要があります。

ただし、[Accept Client on Authenticated Provisioning] オプションを選択した場合は、ACS が PAC プロビジョニングのフェーズ 0 の正常終了時に RADIUS Access-Accept（EAP Success を含む）を送信し、クライアントは再認証を強制されません。このオプションは、[Allow Authenticated In-Band PAC Provisioning] オプションもイネーブルの場合にだけ、イネーブルにすることができます。

フェーズ 0 での PAC の送信は MSCHAPv2 認証によって保護されており、MSCHAPv2 はディクショナリ攻撃に弱いため、自動インバンド PAC プロビジョニングの使用は EAP-FAST の最初の展開に限定することを推奨します。

大規模な EAP-FAST 展開後は、PAC に対する高度なセキュリティを確保するために、PAC プロビジョニングを手動で実行してください。手動 PAC プロビジョニングの詳細については、「手動 PAC プロビジョニング」（P.B-25）を参照してください。

ACS が自動インバンド PAC プロビジョニングを実行するかどうかを制御するには、[System Administration] ドロワの [Global System Options] ページのオプションを使用します。詳細については、「EAP-FAST」（P.B-19）を参照してください。

手動 PAC プロビジョニング

手動 PAC プロビジョニングでは、ACS 管理者が PAC ファイルを生成し、それを該当するネットワーク ユーザに配布する必要があります。ユーザは PAC ファイルでエンドユーザ クライアントを設定する必要があります。

EAP-FAST を使用してネットワークにアクセスするユーザを制御するには、手動 PAC プロビジョニングを使用します。自動インバンド PAC プロビジョニングをディセーブルにすると、PAC でプロビジョニングされていない EAP-FAST ユーザはネットワークにアクセスできません。

ACS 展開に、各ネットワーク セグメントへのアクセスが個別の ACS によって制御されるネットワーク セグメンテーションが含まれている場合は、手動 PAC プロビジョニングによってセグメントごとに EAP-FAST アクセスを許可できます。

たとえば、会社がシカゴとボストンのオフィスでのワイヤレス アクセス用に EAP-FAST を使用していて、これら 2 つのオフィスそれぞれの Cisco Aironet Access Point が別々の ACS を使用するよう設定されている場合に、シカゴのオフィスを訪れたボストンの従業員がワイヤレス アクセスを使用できるかどうかを、従業員ごとに決定できます。

手動 PAC プロビジョニングの管理オーバーヘッドは自動インバンド PAC プロビジョニングよりもはるかに大きくなりますが、ネットワーク上で PAC を送信するリスクはなくなります。PAC を手動でプロビジョニングすると、初期展開時の多数のエンドユーザ クライアントの設定で多くの作業が必要になりますが、このタイプのプロビジョニングは PAC を展開する最も安全な方法です。

大規模な EAP-FAST 展開後は、PAC に対する高度なセキュリティを確保するために、PAC プロビジョニングを手動で実行します。

特定のユーザ名の PAC ファイルを生成できます。マシンの PAC を生成し、クライアントに対して PAC を手動でプロビジョニングすることもできます。

PAC を作成するには次のパラメータが必要です。

- ユーザ PAC とマシン PAC のどちらであるかの指定
- [Internal Identity Store ID] フィールドに格納されている ID
- PAC 存続可能時間（TTL）
- PAC 暗号化のオンまたはオフ、および暗号化用のパスワード

PAC は、RC4 または AES アルゴリズムを使用して、指定したパスワードで暗号化できます。受信した PAC データを手動で復号化できるように、詳細な復号化アルゴリズムをクライアントに提供する必要があります。

ACS でサポートされる PAC の機能

ACS 5.4 では、PAC に対して次の機能がサポートされます。

マシン PAC 認証

マシン PAC ベースの認証では、ユーザ認証の前にマシンが制限付きでネットワークにアクセスできます。

予防的 PAC アップデート

ACS は、PAC TTL の設定済みパーセンテージが残っている場合に、認証の成功後に新しい PAC をクライアントに予防的に提供します。トンネル PAC アップデートは、PAC の有効期限が切れる前に実行された最初の正常な認証後に、サーバによって開始されます。

予防的 PAC アップデート時間は、[Allowed Protocols] ページで ACS サーバに対して設定されます。このメカニズムにより、クライアントは常に有効な PAC で更新されます。

（注）　マシン PAC と認可 PAC に対して予防的 PAC アップデートは行われません。

認証付きプロビジョニングでのピアの受け入れ

プロビジョニング フェーズ中にピアを認証できます。

PAC なし認証

PAC なし EAP-FAST 認証では、トンネル PAC またはマシンで生成された PAC を発行または受け入れせずに、ACS で EAP-FAST を実行できます。セキュア トンネルは、PAC 以外の証明書を使用して確立できます。一部の PAC は存続期間が長く更新されない場合があり、これが認証とセキュリティの問題の原因になることがあります。

PAC なし EAP-FAST がイネーブルになっている場合、PAC に対する要求は無視されます。認証は EAP-FAST フェーズ 0 で開始し、PAC に対する後続の要求は無視されます。フローは EAP-FAST フェーズ 2 に移動します。ACS は、Success-TLV メッセージで PAC なしで応答します。

クライアントが PAC でトンネルを確立しようとした場合、ACS は PAC Invalid メッセージで応答します。トンネルの確立は行われず、Access-Reject が送信されます。ホストまたはサプリカントは接続を再試行できます。

ADHP とも呼ばれる匿名フェーズ 0 は、プロトコルがフェーズ 2 へのロール オーバーをサポートしていないため、PAC なし認証に対してサポートされません。PAC なし EAP-Fast では設定がサポートされ、クライアント証明書は不要です。

表 B-3 に、さまざまなタイプの PAC と、それらに使用できる認証と認可の方式を示します。

表 B-3　PAC 規則の要約

PAC のタイプ	トンネル v1/v1a/SGA	マシン	認可
プロビジョニング時に要求に応じて PAC を提供	Yes	Yes	プロビジョニング時に要求に応じて PAC を提供します。
認証時に要求に応じて PAC を提供	Yes	Yes	この認証で PAC が使用されなかった場合だけ。
予防的アップデート	Yes	No	No
PAC の有効期限が切れたとき	拒否し、TLS フォールバックを試行し、認証の成功後にだけ新しい PAC を提供します（トンネル PAC）。	拒否し、TLS フォールバックを試行し、認証の成功後にだけ新しい PAC を提供します（マシン PAC）。	拒否し、認証の成功後にだけ新しい PAC を提供します（認可 PAC）。
ACS 3.x/4.x PAC のサポート	トンネル PAC v1/v1a だけ	Yes	No

関連トピック

- 「PAC について」（P.B-22）
- 「プロビジョニング モード」（P.B-23）

- 「PAC のタイプ」（P.B-23）
- 「マスターキー生成と PAC TTL」（P.B-27）

マスターキー生成と PAC TTL

マスターキー生成と PAC TTL の値によって、「マスターキーについて」（P.B-22）および「PAC のタイプ」（P.B-23）に説明するようにそれらの状態が判断されます。マスターキーと PAC の状態によって、EAP-FAST でのネットワーク アクセスの要求者に PAC プロビジョニングまたは PAC 更新が必要かどうかが判断されます。

関連トピック

- 「PAC について」（P.B-22）
- 「プロビジョニング モード」（P.B-23）
- 「PAC のタイプ」（P.B-23）
- 「ACS でサポートされる PAC の機能」（P.B-25）

TLS 再ネゴシエーション用の EAP-FAST

匿名の PAC プロビジョニング スキーマを使用する場合、パスワードの入力を 2 回求められることがあります。最初にパスワードを入力したときに、ACS は PAC をプロビジョニングして、access-reject をクライアントに送信します。次に、クライアントからプロンプトに対してパスワードを再入力すると、認証が可能になり、ネットワークへのアクセスが許可されます。

ACS は TLS クライアントのハンドシェイク レコードを確認します。TLS クライアントのハンドシェイク レコードを確認できた場合、ACS は、ユーザのアクセス要求を拒否する代わりに、EAP-FAST フェーズ 0 の最後に TLS 再ネゴシエーションを開始します。

ホストが匿名の PAC プロビジョニングを使用している場合、Vista クライアントではこのオプションを使用する必要があります。Vista クライアントではキャッシュにユーザ パスワードが保存されないので、パスワードの入力は 1 回になります。このオプションをイネーブルにしている場合、ACS は、PAC プロビジョニング後にアクセスの試行を拒否する代わりに、EAP-FAST フェーズ 0 の最後にクライアントへの TLS 再ネゴシエーション要求の送信を開始します。

ACS 5.4 での EAP-FAST フロー

（注）　EAP-FAST をサポートするようにエンドユーザ クライアントを設定する必要があります。ここでは、ACS の設定だけを取り上げます。

はじめる前に

この手順のステップの順番は、一例に過ぎません。ご使用のサイトで EAP-FAST をイネーブルにするときは、これらのステップを繰り返したり順番を変えたりして実行しなければならない場合があります。

たとえば、この手順では、PAC プロビジョニングをどのようにサポートするかの決定は、EAP-FAST をサポートするようユーザ データベースを設定したあとになっています。しかし、自動インバンド PAC プロビジョニングを選択すると、ユーザ データベース サポートの制限が変わります。

ACS で EAP-FAST 認証を実行できるようにするには、次の手順を実行します。

ステップ 1　EAP-FAST 認証をサポートするように ID ストアを設定します。

EAP-FAST 認証をサポートしている ID ストアを確認するには、「認証プロトコルと ID ストアの互換性」（P.B-36）を参照してください。ID ストアを設定する方法については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

ステップ 2　マスターキー生成と PAC TTL 値を決定します。

マスターキー生成と PAC TTL 値によって PAC プロビジョニングまたは PAC 更新が必要かどうかがどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-27）を参照してください。

ステップ 3　自動 PAC プロビジョニングと手動 PAC プロビジョニングのどちらを使用するかを決めます。

PAC プロビジョニングの 2 つの手段については、「自動インバンド PAC プロビジョニング」（P.B-24）および「手動 PAC プロビジョニング」（P.B-25）を参照してください。

自動インバンド PAC プロビジョニングの使用は、少数の新規エンドユーザ クライアントをネットワークに追加するため、および期限切れのマスターキーに基づく PAC を置換するために手動 PAC プロビジョニングを使用する前の、EAP-FAST の最初の展開に限定することを推奨します。

ステップ 4　ステップ 2 およびステップ 3 での決定を使用して、[Global Systems Options] ドロワで EAP-FAST をイネーブルにします。詳細については、「EAP-FAST」（P.B-19）を参照してください。

ACS が、EAP-FAST 認証を実行できる状態になります。

（注）　内部 ID は、`the workstation not allowed` というエラーが表示されたとき、SSL ハンドシェイクに失敗したとき、EAP-PAC がプロビジョニングされているとき、および ACS が無効な PAC を受信したときにはログに記録されません。

関連トピック

- 「内部 ID ストアの管理」（P.8-4）
- 「外部 ID ストアの管理」（P.8-19）

EAP-FAST PAC 管理

ACS の EAP-FAST マスターキーは、EAP-FAST がサプリカントごとにサーバ暗号化データを格納するために使用する PAC および PAC-Opaque を暗号化または復号化、署名、および認証するために使用されます。EAP-FAST には、ACS ドメイン内の各サーバが PAC（別のサーバでパックされた PAC も含む）をセキュアにパックおよびアンパックするための配布メカニズムが必要です。

EAP-FAST マスターキーには、ACS ドメイン内のすべてのサーバが認識している共通秘密情報が必要です。マスターキーは定期的に更新され、キーはすべての ACS サーバによってセキュアに同期して置換されます。FIPS-140 などの強力な暗号標準に準拠するために、キーは高いエントロピーで生成されます。

旧バージョンの ACS では、マスターキーは ACS 配布メカニズムによって配布され、それらのキーのセキュリティを高めるためにときどき置換されました。ACS 5.4 では、マスターキー配布の簡略性、正確性、ロバストネス、およびセキュリティを提供する新しいスキームが導入されています。

ACS EAP-FAST の新しい配布スキームには、共通シードキーを配布するセキュアな方法が含まれています。各 ACS サーバは、そこから同じマスターキーのセットを決定論的に取得できます。各 PAC にはマスターキーの取得元の情報が含まれ、各サーバは、PAC を暗号化および署名したマスターキーをセキュアに再構築できます。

このスキームは、送信される暗号機密情報の量を削減することでセキュリティを向上させます。

ここでは、次の内容について説明します。

- 「キー配布アルゴリズム」（P.B-29）
- 「EAP-FAST PAC-Opaque のパックとアンパック」（P.B-29）
- 「無効化の方式」（P.B-29）
- 「ACS 4.x からの PAC の移行」（P.B-30）

キー配布アルゴリズム

共通シードキーは、プライマリ ACS サーバによって生成される比較的大きく完全にランダムなバッファです。シードキーは、インストール時に 1 回だけ生成されるか、管理者が手動で再生成できます。シードキーを変更した場合、以前のマスターキーと PAC はすべて自動的に無効にされるため、シードキーを置換する必要はほとんどありません。

シードキーは、ランタイム暗号モジュール（CryptoLib）に存在する、FIPS で承認された RNG ジェネレータを使用して生成されます。ACS プライマリ サーバ管理は、シードキーがいつ生成されるかを判断し、新しいシードキーの生成を要求するために ACS ランタイムと通信します。

シードキーのサイズはさまざまですが、少なくとも 64 バイト（512 ビット）から構成されている必要があります。大きなシードはパフォーマンスに影響することがあります。各マスターキーの取得がそのシードに依存するためです。

任意のどの時点でも、各 ACS サーバが 1 つのシードキーを使用する必要があり、プライマリ ACS サーバが最新のシードキーをすべてのサーバに配布する必要があります。古いシードキーは廃棄する必要があります。

シードキーには、重要な暗号機密情報が含まれています。シードキー情報を開示すると、EAP-FAST PAC メカニズム全体で ID が攻撃を受けやすくなります。

このため、プライマリとセカンダリの ACS サーバ間でシードキーを送信するメカニズムは、セキュリティで十分に保護する必要があります。データベースへのシードキーの格納については、さらにセキュリティ手段を講じる必要があります。シードキーは、最も強力なセキュリティ手段で保護する必要があります。

EAP-FAST PAC-Opaque のパックとアンパック

サーバは、新しい PAC を生成するときに、使用するマスターキーを取得する必要があります。サーバが新しい PAC を受け入れるときには、マスターキー スキームに対する攻撃の可能性を防ぐために使用する検証を追加した同じアルゴリズムを、マスターキーの取得に使用する必要があります。マスターキーが過去にキャッシュにすでに配置されていた場合は、取得の計算をスキップできます。

無効化の方式

すべての PAC およびすべてのマスターキーを無効化できます。このタイプの広範な無効化で行う必要があるのは、シードキーの無効化と新しいシードキーでの置換だけです。

システムで 1 つのシードキーだけを使用すると、実装が容易になります。

ACS 4.x からの PAC の移行

設定を 4.x から移行できますが、PAC 自体はサプリカントだけに格納されているため、依然として ACS 3.x までのバージョンから発行できます。ACS 5.4 は、EAP-FAST 5.0 の予防的 PAC アップデートと同様に、バージョン 4.x 以降から移行されたマスターキーに従ってすべてのタイプの PAC を受け入れ、新しい 5.0 PAC を再発行します。

ACS 5.4 は、ACS 3.x または 4.x から PAC を受け入れると、ACS 4.x の設定から移行された 4.x マスターキーに従って PAC を復号化および認証します。このタイプの PAC の復号化と処理は、ACS 4.x の PAC が処理される方法と似ています。

移行プロセスでは、次のデータ項目の変換が行われます。

- ACS の EAP-FAST A-ID（認証局 ID）。パラメータは ACS 5.4 で展開された A-ID を置換します。
- 非アクティブな ACS 4.x マスターキーのリスト。リストは ACS 4.x の設定から取得され、ACS 5.4 の新しいテーブルに配置されます。移行された各マスターキーには、予想される有効期限が関連付けられています。テーブルは、マスターキー識別子（インデックス）、および各キーに割り当てられている PAC 暗号とともに移行されます。

RADIUS キー ラップありの EAP 認証

ACS は、RADIUS キー ラップありの PEAP、EAP-FAST、および EAP-TLS 認証を使用するように設定できます。この場合、ACS は、RADIUS メッセージを認証し、セッション キーをネットワーク アクセス サーバ（NAS）に配布できます。EAP セッション キーは、Advanced Encryption Standard（AES）を使用して暗号化され、RADIUS メッセージは HMAC-SHA-1 を使用して認証されます。

RADIUS は（EAP-Message 属性の）EAP メッセージの転送に使用されるため、RADIUS メッセージをセキュアに認証することにより、セキュアに認証された EAP メッセージ交換が保証されます。PEAP、EAP-FAST、および EAP-TLS 認証がイネーブルの場合には、RADIUS キー ラップを外部認証方式として使用できます。キー ラップは、EAP-TLS の内部方式（たとえば、EAP-FAST または PEAP）としてはサポートされません。

ACS でサポートされる RADIUS キー ラップでは、cisco-av-pair RADIUS ベンダー固有属性（VSA）の次の 3 つの新しい AVP を使用します（Cisco VSA の TLV 値は [26/9/1]）。

- Random-Nonce : NAS によって生成され、キー データの暗号化および認証にランダム性を付与し、要求と応答パケットをリンクさせてリプレイ アタックを防止します。
- Key : セッション キーの配布で使用されます。
- Message-Authenticator-Code : EAP-Message 属性と Key 属性を含む RADIUS メッセージの認証性を保証します。

RADIUS キー ラップの使用時に、ACS はメッセージ交換とキー配布でこれら 3 つの RADIUS キー ラップ AVP を適用します。ACS は、RADIUS キー ラップ AVP と標準の RADIUS Message-Authenticator 属性を含むすべての RADIUS（EAP）要求を拒否します。

PEAP、EAP-FAST、および EAP-TLS 認証で RADIUS キー ラップを使用するには、[Network Devices and AAA Clients] ページまたは [Default Network Device] ページで [EAP authentication with RADIUS Key Wrap] をイネーブルにする必要があります。

また、AAA クライアントごとに、2 つの共有秘密キーを定義する必要があります。キーはそれぞれ一意で、RADIUS 共有キーとは明確に区別される必要があります。RADIUS キー ラップはプロキシ機能をサポートしないため、プロキシ構成では使用しないでください。

EAP-MSCHAPv2

Microsoft Challenge Handshake Authentication Protocol（MSCHAP v2; 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 v2）は、相互認証とも呼ばれる双方向認証を提供します。リモート アクセス クライアントは、ダイヤルインするリモート アクセス サーバがユーザのパスワードにアクセスできることの確認を受信します。

ここでは、次の内容について説明します。

- 「EAP-MSCHAPv2 の概要」（P.B-31）
- 「ACS 5.4 での EAP-MSCHAPv2 フロー」（P.B-32）

EAP-MSCHAPv2 の概要

EAP 認証プロトコル ファミリの一部のメンバー（具体的には EAP-FAST と PEAP）は、「EAP 内部方式」の概念をサポートします。したがって、別の EAP ベース プロトコルは、最初のプロトコルのコンテキスト内で追加の認証を実行します。これを「EAP 外部方式」と呼びます。

EAP-FAST および PEAP 外部方式でサポートされる内部方式の 1 つは EAP-MSCHAPv2 です。この方式は、EAP によって確立された一般フレームワークに準拠する MSCHAPv2 プロトコルの応用です。

EAP-MSCHAPv2 を内部 EAP 方式として使用すると、次のコンテキストで、無線認証用のユーザ クレデンシャルのデータベースが関連付けられた Microsoft ディレクトリ テクノロジー（Windows Active Directory など）を容易に再利用できます。

- 「ユーザ認証用の MSCHAPv2」（P.B-31）
- 「パスワード変更のための MSCHAPv2」（P.B-31）
- 「AD に対する Windows マシン認証」（P.B-32）

ユーザ認証用の MSCHAPv2

ACS では、EAP-FAST および PEAP の内部方式として EAP-MSCHAPv2 認証プロトコルがサポートされます。このプロトコルは、MSCHAPv2 を EAP フレームワークにカプセル化したものです。相互認証は、設定されたクレデンシャル データベースに対して行われます。

クライアントはパスワードを送信せず、パスワードの暗号化機能を送信します。EAP-MSCHAPv2 をトンネリング プロトコルの内部方式として使用すると、セキュアな通信の保護が向上します。すべてのプロトコル メッセージはトンネルとサーバの内部で暗号化され、クライアント チャレンジはランダムに生成されずに、外部方式暗号情報から取得されます。

EAP-MSCHAPv2 は、AD および ACS 内部 ID ストアに対してサポートされています。

パスワード変更のための MSCHAPv2

EAP-MSCHAPv2 を（EAP 内部方式として）使用してパスワードの有効期限が切れたユーザを認証する場合、ACS は特定の EAP-MSCHAPv2 障害通知をクライアントに送信します。クライアントは、ユーザに新しいパスワードの入力を要求するプロンプトを表示してから、同じカンバセーションで ACS にそのパスワードを提供できます。

新しいパスワードは、古いパスワードを利用して暗号化されます。ユーザ パスワードが正常に変更されると、新しいユーザ パスワードがクレデンシャル データベースに格納されます。

EAP-MSCHAPv2 パスワード変更は、AD および ACS 内部 ID ストアに対してサポートされています。

AD に対する Windows マシン認証

EAP-MSCHAPv2 は、マシン認証に使用できます。EAP-MSCHAPv2 Windows マシン認証は、ユーザ認証と同じです。違いは、マシン パスワードは時間およびその他のパラメータの関数としてマシンと AD で自動的に生成できるため、Windows ドメインの Active Directory を使用する必要があることです。生成されたパスワードは、他のタイプのクレデンシャル データベースには格納できません。

ACS 5.4 での EAP-MSCHAPv2 フロー

802.1x および MSCHAPv2 認証プロセスに関連するコンポーネントは次のとおりです。

- ホスト：エンド エンティティ。つまり、エンドユーザのマシン。
- AAA クライアント：ネットワーク アクセス ポイント。
- 認証サーバ：ACS。

MSCHAPv2 プロトコルについては、RFC 2759 で説明されています。

関連項目

- 「認証プロトコルと ID ストアの互換性」（P.B-36）

CHAP

CHAP は、応答時に一方向の暗号化を使用するチャレンジ/レスポンス方式です。CHAP を使用することで、ACS は、セキュリティ レベルの高い順からセキュリティ暗号化方式をネゴシエートし、プロセス中に伝送されるパスワードを保護します。CHAP パスワードは再利用が可能です。

ACS 内部データベースを認証に使用している場合は、PAP または CHAP のどちらかを使用できます。CHAP は、Windows ユーザ データベースでは使用できません。RADIUS PAP と比較した場合、エンドユーザ クライアントから AAA クライアントに通信するときに CHAP を使用すると、パスワードが暗号化されるため、高いセキュリティ レベルを確保できます。

LEAP

ACS は、現時点では、Cisco Aironet ワイヤレス ネットワーキングに対してだけ LEAP を使用します。このオプションをイネーブルにしないと、LEAP 認証を実行するように設定された Cisco Aironet エンドユーザ クライアントは、ネットワークにアクセスできなくなります。Cisco Aironet エンドユーザ クライアントすべてが EAP-TLS などの異なる認証プロトコルを使用する場合は、このオプションをディセーブルにすることを推奨します。

（注） [Network Configuration] セクションで RADIUS（Cisco Aironet）デバイスとして定義された AAA クライアントを使用してユーザがネットワークにアクセスする場合は、LEAP、EAP-TLS、またはその両方をイネーブルにする必要があります。これ以外の場合、Cisco Aironet ユーザは認証を受けることができません。

証明書属性

ACS は、次のクライアント証明書の属性を解析します。

- 証明書シリアル番号（バイナリ形式）
- エンコード証明書（バイナリ DER 形式）
- サブジェクトの CN 属性
- サブジェクトの O 属性（Organization）
- サブジェクトの OU 属性（Organization Unit）
- サブジェクトの L 属性（Location）
- サブジェクトの C 属性（Country）
- サブジェクトの ST 属性（State Province）
- サブジェクトの E 属性（eMail）
- サブジェクトの SN 属性（Subject Serial Number）
- 発行元 I 属性
- Subject Alternative Name（SAN）

ポリシーを定義して、受信した証明書から取得される属性として TLS カンバセーションで使用するプリンシプル ユーザ名を設定できます。

プリンシプル ユーザ名として使用できる属性は次のとおりです。

- Subject CN
- Subject Serial-Number（SN）
- SAN
- Subject
- SAN-Email
- SAN-DNS
- SAN-otherName

設定された属性が証明書に含まれていない場合は、認証が失敗します。

（注）　ACS 5.4 では、EAP-TLS プロトコルに対してだけ、短いハードコード化された属性と証明書属性の確認がサポートされます。

証明書のバイナリ比較

ACS が外部 ID ストアから受信する証明書に対してバイナリ比較を実行し、比較に使用される ID ストアのパラメータを判断できます。

（注）　ACS 5.4 では、AD および LDAP は証明書を保持する唯一の外部 ID ストアです。

ACS は、設定されたプリンシプル ユーザ名を使用してユーザの証明書をクエリーしてから、外部 ID ストアから受信した証明書とクライアントから受信した証明書のバイナリ比較を実行します。比較は DER 証明書形式で実行されます。

テキスト属性に関連する規則

ACS は、クライアント証明書のテキスト属性を収集し、それらを ACS コンテキスト ディクショナリに配置します。ACS は、ACS の規則属性の場合と同様に、これらの属性にルール ベースのポリシーを適用できます。

規則の確認に使用できる属性は次のとおりです。

- サブジェクトの CN 属性
- サブジェクトの O 属性（Organization）
- サブジェクトの OU 属性（Organization Unit）
- サブジェクトの L 属性（Location）
- サブジェクトの C 属性（Country）
- サブジェクトの ST 属性（State Province）
- サブジェクトの E 属性（eMail）
- サブジェクトの SN 属性（Subject Serial Number）
- 発行元 I 属性
- Subject Alternative Name（SAN）
- Subject
- SAN-Email
- SAN-DNS
- SAN-otherName

証明書の失効

ACS が受信するすべてのクライアント証明書は、定義されているポリシーに従って、Certificate Revocation List（CRL; 証明書失効リスト）で確認されます。

CRL メカニズムは、クライアント証明書にまだ依存できるかどうかを確認します。この処理は、証明書のシリアル番号と、対応する証明書チェーンの各メンバーのシリアル番号を、失効したことがわかっている証明書のリストと比較チェックすることで行います。

証明書が失効する理由として、関連付けられている秘密キーが危険にさらされて疑いがあること、または証明書が不適切に発行されたことが判明したことが考えられます。このいずれかの条件に該当する場合は、証明書が拒否されます。

ACS では、ACS データベースに設定されている CRL ファイルの取得に使用される URL のリストを含む静的 CRL がサポートされます。

（注） ACS は証明書失効確認のデルタ CRL をサポートしません。

信頼されている各 CA 証明書の CRL アップデートに使用される URL のセットを設定できます。デフォルトでは、CA 証明書を追加すると、ACS が証明書 *crlDistributionPoint* に格納されているすべての URL をその CA の初期静的 CRL として自動的に設定します。ほとんどの場合、*crlDistributionPoint* は CA 証明書の無効化に使用される CRL の場所を指すために使用されますが、この CA によって発行された CRL ファイルを指すように URL を編集できます。設定できるのは、CA ごとに 1 つの HTTP ベース URL だけです。

各 CA のパラメータを設定できます。この設定は、CA に対して設定されているすべての URL に適用されます。ACS では 2 つのダウンロード モードがサポートされます。一方は定期的なダウンロード用で、もう一方は前の CRL の有効期限が切れる前に次の CRL アップデートをダウンロードするためのものです。

- 定期的なダウンロードでは、ダウンロード期間を定義できます。
- 自動ダウンロードでは、CRL ファイルの期限が切れて ACS による CRL のダウンロードが必要になるまでの時間を定義します。CRL の有効期限は [CRL nextUpdate] フィールドから取得します。

どちらのモードでも、ダウンロードでエラーが発生した場合に、ACS が CRL ファイルの再ダウンロードを試行する前に待機する時間を定義できます。

ACS は、ダウンロードした各 CRL ファイルについて、ダウンロードされた CRL ファイルが信頼ストア内のいずれかの CA によって正しく署名されていることと、それらが信頼されているかどうかを確認します。ACS は、署名の確認に成功した場合にだけ CRL ファイルを使用します。確認された CRL ファイルによって、同じ CA が発行した前の CRL ファイルが置換されます。

（注） CRL ファイルは永続化されないため、ACS の再起動時に再ダウンロードする必要があります。

URL と CA への関連付けの設定は、ACS ドメイン全体に配布されます。ダウンロードした CRL は配布されず、各 ACS サーバで並行して自動的に読み込まれます。

マシン認証

ACS では、EAP コンピュータ認証をサポートする Microsoft Windows オペレーティング システムを実行しているコンピュータの認証がサポートされます。マシン認証は、コンピュータ認証とも呼ばれ、Active Directory が認識しているコンピュータに対してだけネットワーク サービスを許可します。

この機能は、物理的な作業設備外から権限のないユーザが無線アクセス ポイントにアクセスできる無線ネットワークで特に役立ちます。

マシン認証をイネーブルにした場合、3 つの異なる種類の認証が行われます。コンピュータを起動すると、次の順序で認証が行われます。

- **マシン認証**：ACS はユーザ認証の前にコンピュータを認証します。ACS は、Windows ID ストアに対してコンピュータが与えたクレデンシャルをチェックします。

  Active Directory を使用していて AD 内の一致するコンピュータ アカウントに同じクレデンシャルがある場合、コンピュータは Windows ドメイン サービスへのアクセスを許可されます。

- **ユーザ ドメイン認証**：マシン認証が成功すると、ユーザが Windows ドメインで認証されます。マシン認証が失敗すると、コンピュータは Windows ドメイン サービスへのアクセスを許可されず、ローカル オペレーティング システムに保持されているキャッシュ クレデンシャルを使用してユーザ クレデンシャルが認証されます。

  この場合、ユーザはローカル システムにだけログインできます。ドメインの代わりにキャッシュ クレデンシャルでユーザが認証された場合、コンピュータは、ドメインによって指示されたログイン スクリプトの実行などのドメイン ポリシーを適用しません。

ヒント ユーザ パスワードが最後に変更されてから、ユーザがまだコンピュータを使用してドメインに正常にログインしていない場合は、そのコンピュータのマシン認証が失敗すると、コンピュータ上のキャッシュ クレデンシャルは新規パスワードと一致しません。ユーザがこのコンピュータからドメインへ正常にログインしたことがあれば、キャッシュ クレデンシャルはユーザの古いパスワードと一致していることになります。

- **ユーザ ネットワーク認証**：ACS はユーザを認証し、ネットワーク接続を許可します。ユーザが存在する場合は、指定された ID ストアがユーザの認証に使用されます。

  ID ストアが Windows ID ストアである必要はありませんが、ほとんどの Microsoft クライアントは、ユーザ ドメイン認証と同じクレデンシャルを使用してネットワーク認証を自動的に実行するように設定できます。この方法により、シングル サインオンが可能になります。

（注）　また、Microsoft PEAP クライアントは、ユーザがログオフするたびにマシン認証を開始できます。この機能は、次のユーザ ログインのネットワーク接続を準備するためです。Microsoft PEAP クライアントは、ユーザがログオフだけではなくコンピュータをシャットダウンまたは再起動した場合にも、マシン認証を開始する場合があります。

ACS では、マシン認証に EAP-TLS、EAP-FAST、PEAP（EAP-MSCHAPv2）、および PEAP（EAP-GTC）がサポートされます。[Active Directory: General] ページでそれぞれを個別にイネーブルにして、EAP-TLS、EAP-FAST、または PEAP（EAP-MSCHAPv2）で認証した複数のコンピュータを混合させることができます。

マシン認証を実行する Microsoft オペレーティング システムでは、ユーザ認証プロトコルが、マシン認証に使用されたのと同じプロトコルに制限される場合があります。

関連トピック

- 「Microsoft AD」（P.8-39）
- 「外部 ID ストアの管理」（P.8-19）

認証プロトコルと ID ストアの互換性

ACS では、サポートされる ID ストアで認証するさまざまな認証プロトコルがサポートされます。

表 B-4 に、EAP 以外の認証プロトコルのサポートを示します。

表 B-4　EAP 以外の認証プロトコルとユーザ データベースの互換性

ID ストア	ASCII/PAP	MSCHAPv1/MSCHAPv2	CHAP
ACS	Yes	Yes	Yes
Windows AD	Yes	Yes	No
LDAP	Yes	No	No
RSA ID ストア	Yes	No	No
RADIUS ID ストア	Yes	No	No

表 B-5 に、EAP 認証プロトコルのサポートを示します。

表 B-5　EAP 認証プロトコルとユーザ データベースの互換性

ID ストア	EAP-MD5	EAP-TLS[1]	PEAP-TLS[2]	PEAP EAP-MSCHAPv2	EAP-FAST MSCHAPv2	PEAP-GTC	EAP-FAST-GTC
ACS	Yes	Yes[3]	Yes	Yes	Yes	Yes	Yes
Windows AD	No	Yes	Yes	Yes	Yes	Yes	Yes
LDAP	No	Yes	Yes	No	No	Yes	Yes
RSA ID ストア	No	No	No	No	No	Yes	Yes
RADIUS ID ストア	No	No	No	No	No	Yes	Yes

1. EAP-TLS 認証では、ユーザは証明書の暗号確認によって認証されます。また、ACS 5.4 では、エンドユーザ クライアントから送信されたユーザの証明書を LDAP ID ストア内のユーザのレコードにある証明書とバイナリ比較することもできます。
2. PEAP-TLS 認証では、ユーザは証明書の暗号確認によって認証されます。また、ACS 5.4 では、エンドユーザ クライアントから送信されたユーザの証明書を LDAP ID ストア内のユーザのレコードにある証明書とバイナリ比較することもできます。
3. ACS ID ストアは証明書を格納できません。

APPENDIX C

オープン ソース ライセンス通知

Cisco Secure Access Control System 5.4 で使用されているすべてのオープン ソースおよびサードパーティのライセンスについては、http://www.cisco.com/en/US/products/ps9911/products_licensing_information_listing.html を参照してください。

通告

本ソフトウェア ライセンスに関連する通知内容を以下に示します。

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.See below for the actual license texts.Actually both licenses are BSD-style Open Source licenses.In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project.All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission.For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com).All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to.The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code.The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed.i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

GLOSSARY

A

AAA
認証、許可、アカウンティング（AAA）は、コンピュータ リソース アクセスの知的制御、ポリシーの実装、使用状況の監査、およびサービス請求に必要な情報の提供を実現するフレームワークを示す用語です。これらの処理を結合することは、効果的なネットワーク管理およびセキュリティにとって重要となります。ユーザがアクセスするコンピュータ リソースを管理し、ネットワーク上でのユーザ アクティビティを追跡する IP ベース ネットワーキングのシステムです。

AAA クライアント IP アドレス
AAA クライアントの IP アドレス。これを使用して、ネットワーク デバイスと相互作用するように AAA クライアントを Access Control Server（ACS）に設定します。複数のネットワーク デバイスを示すには、複数の IP アドレスを指定します。各 IP アドレスは、Enter を押して区切ります。

AAA サーバ
コンピュータ リソースへのユーザ アクセス要求を処理するサーバ プログラム。企業の場合は、認証、許可、アカウンティング（AAA）サービスを提供します。AAA サーバは一般的にネットワーク アクセス サーバやゲートウェイ サーバ、およびユーザ情報を含むデータベースやディレクトリと相互作用します。現在、デバイスまたはアプリケーションが AAA サーバと通信するための標準規格は、Remote Authentication Dial-In User Service（RADIUS）です。

ACS システム管理者
ACS Web インターフェイスの System Configuration セクションに定義される、さまざまなアクセス権を持つ管理者。これらの管理者は、ネットワーク内の ACS 展開を管理します。

ADR
アクセシビリティ設計要件（Accessibility Design Requirements）。アクセシビリティ製品、Web サイト、およびドキュメンテーションの設計方法に関する詳細を提供します。

AES
高度暗号化規格（Advanced Encryption Standard）。連邦情報処理標準（FIPS）の刊行物。米国政府機関が機密（非機密）情報を保護するために使用する暗号アルゴリズムを定めています。機密（機密扱いでない）情報を保護する政府機関。この規格では、米国政府機関（およびその他）が機密情報を保護するために使用する FIPS 承認の対称暗号化アルゴリズムとして、Rijndael を指定しています。

AP
アクセス ポイント（Access Point）。無線ネットワークのハブです。無線クライアントはアクセス ポイントに接続します。また、2 つのクライアント間のトラフィックはアクセス ポイントを通過する必要があります。

API
アプリケーション プログラム インターフェイス（Application Program Interface）。アプリケーション プログラムを作成するプログラマが、オペレーティング システムまたは別のアプリケーションへの要求を作成する場合に使用する特定の方法です。

AR
アクセス レジストラ（Access Registrar）。ダイヤル、ISDN、および新しいサービス（DSL、Telco リターンを使用するケーブル、無線、Voice over IP など）の配布をサポートするように設計されている RADIUS 準拠のアクセス ポリシー サーバです。

ARP
アドレス解決プロトコル（Address Resolution Protocol）。インターネット プロトコル アドレスを、ローカル ネットワーク内で認識されている物理マシン アドレスにマッピングするプロトコルです。通常は ARP キャッシュと呼ばれるテーブルを使用して、各 MAC アドレスと対応する IP アドレス間の相互関係を保持します。ARP は、この相互関係を構築し、両方向のアドレス変換を可能にするプロトコル ルールを提供します。

ARP アドレス解決プロトコル。ネットワーク環境内のハードウェア ユニットの物理アドレス（MAC アドレスなど）を取得するために使用されるプロトコルです。ホストは、ターゲット ハードウェア ユニットの IP アドレスを含む ARP 要求をブロードキャストすることにより、このような物理アドレスを取得します。要求によってこの IP アドレスを持つユニットが検出されると、このユニットは自身の物理ハードウェア アドレスを使用して応答します。

ARPANET Advanced Research Projects Agency Network。1970 年代初期に米国政府との契約の下で構築された先駆的なパケット スイッチド ネットワークです。今日のインターネットの発展を導き、1990 年 6 月に廃止されました。

B

BIND Berkeley Internet Name Domain。DNS の実装。DNS はドメイン名の IP アドレス解決に使用されます。

C

CA 認証局（Certificate Authority）。セキュリティ クレデンシャルとメッセージ暗号化および復号化のための公開キーを発行し、管理するネットワーク内の機関。CA は、公開キー インフラストラクチャ（PKI）の一部として、デジタル証明書の要求側が提供した情報を確認するために登録局（RA）に問い合わせます。RA によって要求側の情報が確認されると、CA は証明書を発行できます。

CA の署名 デジタル証明書の信頼性を保証するデジタル コード。CA の署名は、証明書を発行する認証局（CA）によって提供されます。

CGI コモン ゲートウェイ インターフェイス（Common Gateway Interface）。このメカニズムは、パラメータを実行可能スクリプトに渡して応答をダイナミックに生成するために、HTTP サーバ（Web サーバ）によって使用されます。

CHAP チャレンジ ハンドシェイク認証プロトコル（Challenge-Handshake Authentication Protocol）。リプレイ アタックを防ぐためにチャレンジごとに応答が変わる、チャレンジ / レスポンス認証メカニズムを使用するプロトコルです。

CHAP は、リンクの確立後にサーバが要求側にチャレンジを送信する認証技術です。要求側は、一方向ハッシュ関数を使用して取得された値を格納して応答します。サーバは、この値をサーバ側で予測しているハッシュ値の計算結果と比較することによって、応答を確認します。値が一致した場合は認証が認められ、そうでない場合は、通常、接続が終了します。

Cookie クライアント側の状態情報を格納し、あとで取り出してサーバが使用するために、HTTP サーバとブラウザ（サーバのクライアント）間で交換されるデータ。HTTP サーバはクライアントへのデータ送信時に同時にクッキーを送信し、クライアントは HTTP 接続が終了したあともこのクッキーを保持します。サーバはこのメカニズムを使用して、HTTP ベース アプリケーションのクライアント側の永続的状態情報を保持し、以降の接続でその状態情報を取り出すことができます。

CoS サービス クラス（Class of Service）。類似したタイプのトラフィック（電子メール、ストリーミング ビデオ、音声、大きなドキュメントのファイル転送など）をグループ化し、各タイプを専用のサービス優先レベルを持つクラスとして処理することによって、ネットワーク内のトラフィックを管理する方法。

CRC 巡回冗長検査（Cyclic Redundancy Check）。「巡回冗長コード」と呼ばれる場合もあります。暗号ハッシュではないが、データに対する偶発的な変更が予測されるデータ整合性サービスの実装に使用される、チェックサム アルゴリズムの 1 つのタイプです。

CRL 証明書失効リスト（Certificate Revocation List）。取り消し済みで、もう有効ではなく、いかなるシステム ユーザも信頼すべきではない証明書（正確には、証明書のシリアル番号）のリストです。

CRUD 作成、読み取り、更新、および削除（Create, Read, Update and Delete）。管理対象データで実行される基本的な管理操作です。

CSS カスケーディング スタイル シート（Cascading Style Sheet）。スタイル要素の定義が衝突した場合には定義済みの優先順位を使用して複数のソースから作成される Web ページです。

CSV カンマ区切り形式（Comma-Separated Value）。このファイル形式は、フィールドをカンマで区切り、レコードを改行で区切る区切りデータ形式です。

CUE コモン ユーザ エクスペリエンス（Common User Experience）。

D

Denial of Service システム リソースに対する認可済みアクセスの妨害、またはシステムの動作や機能の遅延。

DES データ暗号規格。広く使用されている、秘密キーを使用したデータ暗号化方式です。使用できる暗号キーは 72,000,000,000,000,000（72 千兆）以上あります。特定のメッセージごとに、この莫大な数のキーの中からランダムにキーが選択されます。他の秘密キー暗号方式と同様に、送信側と受信側の両方で同じ秘密キーを知っており、また使用する必要があります。

Diffie-Hellman Whitfield Diffie および Martin Hellman によって 1976 年に発表されたキー共有アルゴリズム。Diffie-Hellman はキーの設定であり、暗号化ではありません。ただし、作成されたキーは暗号化や高度なキー管理操作、または他の暗号法に使用される場合があります。

Directory System Agent（DSA） LDAP サーバなど、DAP または LDAP 対応のディレクトリ サービスを示す X.500 の用語。

DIT ディレクトリ インフォメーション ツリー（Directory Information Tree）。ネーミング コンテキストとも呼ばれます。ローカル ディレクトリ構造を構成するオブジェクトの階層。複数の DIT が LDAP サーバによってサポートされます。この情報はルート DSE によって提供されます。

DLL ダイナミック リンク ライブラリ（Dynamic Link Library）。コンピュータ内で実行している大きなプログラムから必要に応じてコールできる、小さなプログラムの集合。大きなプログラムとプリンタやスキャナなどの特定のデバイスとの通信を可能にする小さなプログラムは、多くの場合、DLL プログラム（通常、DLL ファイルと呼ばれる）としてパッケージ化されています。

DN Distinguished Name（認定者名）。DN は、目的のエントリからディレクトリ ルートまで DIT を上向きにたどって一意にネーミング属性を示す一連の RDN で構成されます。DN は左から右に記述され、次のようになります。

DNS ドメイン ネーム システム（Domain Name System）。インターネット ドメイン名を検索して、IP アドレスに変換する方法。ドメイン名はインターネット アドレスを示す、意味のある覚えやすい「ニックネーム」です。

DSA デジタル署名アルゴリズム（Digital Signature Algorithm）。大きな数値のペアの形式でデジタル署名を作成する非対称暗号アルゴリズム。署名者の ID および署名日の整合性を確認できるように、署名はルールとパラメータを使用して計算されます。

DSA Specific Entry（DSE） ローカル ディレクトリ サーバ内のエントリ。

DSS Digital Signature Standard（デジタル署名規格）。非対称暗号法を含むデジタル署名アルゴリズム（DSA）について定めている米国政府規格です。

dumpsec システムのユーザ、ファイル システム、レジストリ、権限、パスワード ポリシー、およびサービスに関するさまざまな情報をダンプするセキュリティ ツール。

E

EAP Extensible Authentication Protocol。Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）で使用されている認証方式を拡張する、無線ネットワークのプロトコル。多くの場合、コンピュータをインターネットに接続するときに使用されます。EAP は、トークン カード、スマート カード、証明書、ワンタイム パスワード、公開キー暗号認証など、複数の認証メカニズムをサポートできます。

EAP-MD5 Extensible Authentication Protocol-Message Digest 5。RSA Security によって開発された EAP セキュリティ アルゴリズム。生成された 128 ビットの数字列またはハッシュを使用してデータ通信の信頼性を確認します。

EAP-TLS Extensible Authentication Protocol-Translation Layer Security。クライアントとサーバの両方からの認証を要求する、EAP の高セキュリティ バージョン。これらのうちの一方で適切なオーセンティケータの提示に失敗した場合、接続は終了します。クライアント コンピュータにあらかじめデジタル証明書をインストールしておくことにより、802.1X のセキュア接続を作成できます。EAP-TLS は、クライアントとサーバ間の相互認証、および整合性が保持される暗号スイート ネゴシエーションやキー交換に役立つプロトコルです。クライアントとサーバの両方で X.509 証明書を使用して、相互に ID を確認します。

Ethernet 最も広く導入されている LAN テクノロジー。IEEE 802.3 規格で定められており、一般的にイーサネット LAN は同軸ケーブルまたは特別グレードのツイストペア線を使用します。デバイスはケーブルに接続され、CSMA/CD プロトコルを使用してアクセス権を競合します。

eXtensible Markup Language（XML） XML は共通の情報形式を作成して、ワールドワイド ウェブ、イントラネットなどで形式とデータの両方を共有するための柔軟な方法です。

F

FTP ファイル転送プロトコル（File Transfer Protocol）。テキストまたはバイナリ ファイルのネットワークでの転送を定めている TCP/IP プロトコルです。

H

HTML ハイパーテキスト マークアップ言語。ワールドワイド ウェブ ブラウザ ページに表示することを目的としたファイルに、挿入されるマークアップ記号またはコードのセットです。

HTTP ハイパーテキスト転送プロトコル。インターネット上でハイパーテキスト ドキュメントを転送するために使用されるインターネット プロトコル（IP）ファミリのプロトコルです。

HTTPS Hypertext Transfer Protocol over Secure Socket Layer または HTTP over SSL。HTTPS は Netscape が開発して自社のブラウザに組み込んだ Web プロトコルです。ユーザのページ要求と Web サーバから返されるページを暗号化および復号化します。URL の最初の部分（コロンの前の、アクセス スキームまたはプロトコルを指定する部分）で使用されると、この用語はセキュリティ メカニズム（通常、SSL）で拡張された HTTP を使用することを指定します。HTTPS は下位レイヤ、TCP/IP、および HTTP と TCP との間に追加された暗号化 / 認証レイヤとのやり取りに、HTTP ポート 80 ではなくポート 443 を使用します。

I

I18N 国際化およびローカリゼーションは、ネイティブ以外の環境（特に、他の国や文化）のソフトウェアを適合させる手段です。国際化は事実上、どのような場所でも使用できるように製品を適合させることであり、一方、ローカリゼーションは、特定のロケールで使用できるように特別な機能を追加することです。

ID グループ すべてのタイプのユーザおよびホストに関連付けられる論理エンティティ。

IETF インターネット技術特別調査委員会（Internet Engineering Task Force）。TCP/IP などの標準インターネット運用プロトコルを定義している団体です。IETF は、インターネット学会の Society Internet Architecture Board（IAB; インターネット アーキテクチャ委員会）によって管理されています。IETF のメンバーは、インターネット学会の個人および組織メンバーシップから選出されます。

IP インターネット プロトコル。インターネット上の 1 つのコンピュータから別のコンピュータにデータを送信するための手段またはプロトコルです。

IP インターネット プロトコル。インターネット上の 1 つのコンピュータから別のコンピュータにデータを送信するための手段またはプロトコルです。インターネット上の各コンピュータ（ホストと呼ばれる）には、そのコンピュータをインターネット上の他のすべてのコンピュータと区別して一意に識別する IP アドレスが最低 1 つ割り当てられます。

IPSec インターネット プロトコル セキュリティ（Internet Protocol Security）。ネットワーク通信のネットワークまたはパケット処理レイヤにおけるセキュリティの開発標準です。

IP アドレス インターネット プロトコルおよび他のプロトコルで使用するために割り当てられる、コンピュータのインターネットワーク アドレス。IP バージョン 4 アドレスは、ピリオドで区切られた 4 つの 8 ビット数値の並びで示されます。

IP スプーフィング 誤った IP アドレスを提供する方法。

IP 転送 ホストがルータとして動作することを許可するオペレーティング システムのオプション。2 つ以上のネットワーク インターフェイス カードを持つシステムでは、システムがルータとして動作できるように IP フォワーディングを有効にしておく必要があります。

IP フラッド プロトコル実装で処理可能な数よりも多いエコー要求（「ping」）パケットをホストに送信する DoS 攻撃（サービス拒絶攻撃）。

ISO 国際標準化機構（International Organization for Standardization）。1947 年に設立された国際条約に基づかないボランティアの非政府組織。参加国の指定された標準化団体である投票メンバーと、投票権のないオブザーバ組織で構成されます。

ISP Internet Service Provider（インターネット サービス プロバイダー）。インターネット アクセスおよび関連するサービスを消費者に提供するビジネスまたは組織。以前は、ほとんどの ISP が電話会社によって運営されていました。

J

JRE Java ランタイム環境（Java Runtime Environment）。コンピュータ システムで Java アプリケーションを実行できるようにするソフトウェア バンドルです。

K

Kerberos マサチューセッツ工科大学で開発されたシステム。パスワードおよび対称暗号法（DES）を利用して、チケットベースのピア エンティティ認証サービス、およびクライアント / サーバ ネットワーク環境に配布されるアクセス コントロール サービスを実装します。

L

LDAP クライアント LDAP サーバへのアクセスを提供するソフトウェア。大多数の標準 Web ブラウザでは、LDAP URL を使用して、限定された LDAP クライアントの機能を提供しています。LDAP ブラウザおよび Web インターフェイスはともに LDAP クライアントの非常に一般的な例です。オープン ソース クライアントのリスト。

Lightweight Directory Access Protocol（LDAP） TCP/IP 上で実行しているディレクトリ サービスに対して問い合わせおよび変更を行うネットワーキング プロトコル。LDAP プロトコルは、組織、個人、ネットワーク内のファイルやデバイスなどの他のリソースをパブリック インターネット上または企業イントラネット上で検索するために使用されます。

M

MAC アドレス 物理アドレス。ネットワーク デバイスを世界中に存在する他のすべてのデバイスと区別して一意に識別する数値です。

matchingRule（LDAP） 検索操作における属性の比較方式。matchingRule は、通常、OID と名前（caseIgnoreMatch [OID = 2.5.23.2] など）、および操作するデータ型（DirectoryString など）を含む ASN.1 定義です。

MD5 一方向の暗号ハッシュ関数。

MIB（管理情報ベース） 簡易ネットワーク管理プロトコル（SNMP）を使用して管理できるネットワーク オブジェクト セットの公式な記述。

Microsoft Point-to-Point Encryption（MPPE） ポイントツーポイント プロトコル（PPP）およびバーチャル プライベート ネットワーク リンク上のデータを暗号化するプロトコル。

Monitoring and Reports モニタリング、レポート、およびトラブルシューティング オプションを含む、ACS Web インターフェイスのドロワ。

N

NAS（ネットワーク アクセス サーバ） リモート リソースへの唯一のアクセス ポイント。NAS は、保護されたリソースへのアクセスを守るゲートウェイとして動作するように意図されています。これはたとえば、電話ネットワークからプリンタへ、またはインターネットへのゲートウェイです。

P

PAP（パスワード認証プロトコル） リモート アクセス サーバまたは Internet Service Provider（ISP; インターネット サービス プロバイダー）に対してユーザを認証するために使用される単純な認証プロトコル。

PI（プログラマチック インターフェイス） ACS PI は、ACS と通信して ACS を設定および操作する機能を、外部アプリケーションに提供するプログラマチック インターフェイスです。これには、ACS オブジェクトに対する作成、更新、削除、および読み取り操作の実行が含まれます。

PPP（ポイントツーポイント プロトコル） PPP はシリアル インターフェイスを使用する 2 つのコンピュータ間の通信プロトコルであり、一般に、パーソナル コンピュータを電話回線でサーバに接続する場合に使用されます。たとえば、インターネット サーバ プロバイダーは、プロバイダーのサーバでユーザ要求に応答し、その要求をインターネットに渡して、要求に対するインターネットからの応答をユーザに転送できるように、ユーザに PPP 接続を提供します。PPP はインターネット プロトコル（IP）を使用し、その他を処理するように設計されています。場合によっては、プロトコルの TCP/IP スイートのメンバーと見なされることもあります。開放型システム間相互接続（OSI）参照モデルと比較すると、PPP ではレイヤ 2（データリンク層）サービスが提供されます。基本的にこのサービスは、コンピュータの TCP/IP パケットをパッケージ化して、それらを実際にインターネット上に配置できるサーバに転送します。

R

RDN（LDAP） 相対認定者名（Relative Distinguished Name）（Relatively Distinguished Name と書かれることがよくありますが、これは正しくありません）。属性に与えられる、階層のそのレベルで一意の名前です。RDN は、単一値または多値になることがあり、後者の場合、2 つ以上の属性を「+」（プラス）で結合して RDN を作成します（cn+uid など）。RDN という用語は、選択したエントリ（または検索開始場所）からディレクトリ ルート（正確にはルート DSE）まで、DIT を上向きにたどって一意に属性を示す DN の一部として使用される場合にかぎり意味を持ちます。詳細。

RedHat Package Manager（RPM） RPM をパッケージ管理フォーマットとして使用する Linux ディストリビューションにインストールできる、ダウンロード可能なソフトウェア パッケージ。

referral（LDAP） LDAP サーバが LDAP クライアントに、LDAP クライアントが要求している情報を提供できる可能性のある、別の LDAP サーバの名前を（一般に、LDAP URL の形式で）返す動作。

Remote Authentication Dial-In User Service（RADIUS） RADIUS は、リモート アクセス サーバが中央サーバと通信してダイヤルイン ユーザを認証し、要求されたシステムまたはサービスへのアクセスを認可できるようにする、クライアント / サーバ プロトコルおよびソフトウェアです。RADIUS を使用すると、企業は、すべてのリモート サーバが共有できる中央データベースでユーザ プロファイルを管理できます。また、管理された単一のネットワーク ポイントで適用可能なポリシーを設定できるため、より優れたセキュリティが得られます。中央サービスがあるため、より簡単に課金状況を追跡したり、ネットワーク統計情報を保持したりすることもできます。

Request for Comments（RFC） インターネット テクノロジーに適用可能な新しい研究、手法、および方法論を含む一連の文書。

rootdn（LDAP） slapd.conf ファイル内の紛らわしい名前を持つディレクティブ。通常のディレクトリ アクセス ルールを無視できるスーパーユーザを定義します。

S

Secure Sockets Layer（SSL） Netscape 社が開発した、インターネット経由でプライベート ドキュメントを送信するプロトコル。SSL は、公開キーを使用して、SSL 接続で転送されるデータを暗号化することにより動作します。SSL は、Web ブラウジング、電子メール、インターネット ファクス、他のデータ転送などに、インターネットでの安全な通信を提供する暗号プロトコルです。SSL 3.0 と TLS 1.0 には多少違いがありますが、プロトコルは実質的には同じです。ここで使用される「TLS」という用語は、コンテキストで明確にされていないかぎり両方のプロトコルに適用されます。

Service Provisioning Markup Language（SPML） サービス プロビジョニング要求の統合および相互運用のためのオープン標準プロトコル。

SGA Security Group Access

Simple Object Access Protocol（SOAP） 非集中的な分散環境で情報を交換するための、軽量の XML ベース プロトコル。SOAP は、メッセージの内容と処理方法を示すためのフレームワークを定義するエンベロープ、アプリケーション定義のデータ型のインスタンスを表す符号化ルールのセット、リモート プロシージャ コールと応答を表現するための表記法の 3 つの部分で構成されます。

SLA（サービス レベル契約） 特定のサービス レベルが合意されているサービス契約部分。SLA は 2 者間の公式なネゴシエーションによる合意です。これは、お客様とサービス プロバイダーの間、またはサービス プロバイダー間に存在する契約です。サービス、優先度、責務、保証などに関する共通理解を書面にしたものであり、可用性、有用性、パフォーマンス、動作、その他課金などのサービスの属性のレベルを指定します。

SNMP（簡易ネットワーク管理プロトコル） ネットワーク デバイスを監視および制御して、設定、統計収集、パフォーマンス、およびセキュリティを管理する手段を提供する TCP/IP ネットワーク プロトコル。

SSH（セキュア シェル） リモート マシンでコマンドを実行したり、あるマシンのファイルを別のマシンに移動したりするために、ネットワーク上の別のコンピュータにログインするプログラム。

Subject Alternative Name（SAN） 証明書情報内の拡張フィールド。

T

TACACS Terminal Access Controller Access Control System（TACACS）は、リモート アクセス サーバがユーザのログイン パスワードを認証サーバに転送して、指定されたシステムへのアクセスを許可するかどうかを決定できるようにする、UNIX ネットワークに一般的な古い認証プロトコルです。TACACS は暗号化プロトコルであり、そのため、より最近の TACACS+ および Remote Authentication Dial-In User Service（RADIUS）プロトコルよりも安全性が低くなります。

TACACS+ 設定 TACACS+ ランタイム特性の設定に使用されます。

TCP/IP 伝送制御プロトコル / インターネット プロトコルは、基本的な通信言語またはインターネットのプロトコルです。TCP/IP は 2 レイヤ プログラムです。上位層である伝送制御プロトコルは、メッセージまたはファイルを小さなパケットに分割してインターネットで送信し、さらに受信側の TCP レイヤでこのパケットが元のメッセージに再構成されるよう管理します。下位レイヤであるインターネット プロトコルは、パケットが正しい宛先に到着するように、各パケットのアドレス部分を処理します。

U

UDP ユーザ データグラム プロトコル。インターネット プロトコル（IP）を使用するネットワークのコンピュータ間でメッセージが交換されるときに、制限されたサービスを提供する通信プロトコルです。

URL ユニフォーム リソース ロケータ。インターネット上にあるアクセス可能なファイルの一意のアドレスです。

V

VPN バーチャル プライベート ネットワーク。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN は「トンネリング」を使用して、IP レベルですべての情報を暗号化します。

VSA ベンダー固有属性（Vendor Specific Attribute）。Remote Authentication Dial-In User Service（RADIUS）の標準属性セットでは提供されない専用のプロパティまたは特性です。VSA は、リモート アクセス サーバのベンダーによって、RADIUS をベンダー サーバ用にカスタマイズするために定義されます。

W

WCS Cisco Wireless Control System は、企業によるシスコ製無線 LAN の設計、制御、および監視を支援するように設計されているプラットフォームです。WCS は無線 LAN を計画、設定、および管理するための業界最先端のプラットフォームです。

Web Services Description Language（WSDL） ビジネスが提供するサービスを記述し、個人および他のビジネスに、これらのサービスに電子的にアクセスする方法を提供するために使用される XML ベースの言語。

Web サーバ Web サーバは、クライアント / サーバ モデルおよびワールドワイド ウェブのハイパーテキスト転送プロトコル（HTTP）を使用して、Web ページを形成するファイルを Web ユーザ（要求を転送する HTTP クライアントがコンピュータにインストールされている）に提供するプログラムです。

Web サービス ネットワーク上の相互運用可能なマシン間の相互作用をサポートするように設計されているソフトウェア システム。Web サーバ インターフェイスは、マシン処理可能な形式である WSDL で記述されます。他のシステムは、一般的に XML シリアル化を使用する HTTP と他の Web 関連標準を併用して、Web サービスと相互に作用します。

X

X.509 公開キー インフラストラクチャの標準。X.509 は、特に、公開キー証明書の標準形式や証明書経路検証アルゴリズムを定めています。

あ

アイデンティティ ある人が何者か、またはある物が何なのかを識別するもの。たとえば、ある物を認識するための名前などです。

アカウント ユーザ セッションをログ ファイルに記録する ACS の機能。

アクセス 必要な情報を取得する機能。データ アクセスとは、コンピュータ上の特定のデータを取得できること（通常、使用権限があること）です。

アクセス コントロール リソースの使用権限があるユーザだけに、そのリソースの使用を許可します。

アクセス コントロール サービス 不正アクセスに対してシステム リソースを保護するセキュリティ サービス。このサービスを実装する基本メカニズムは ACL およびチケットの 2 つです。

アクセス コントロール システム（ACS; Access Control System） 認証、許可、アカウンティングを実行してネットワーク内のデバイスを管理する AAA サーバ。

アクセス コントロール リスト（ACL） リソース アクセスが許可されているシステム エンティティの ID をリストすることによって、システム リソースに対するアクセス コントロールを実装するメカニズム。

アクセス ポリシー ACS Web インターフェイスへのアクセスを、IP アドレス、TCP ポート範囲、および Secure Socket Layer（SSL）によって制限するポリシー。

アプレット Java プログラム。クライアントの Web ブラウザを使用してユーザ インターフェイスを提供するアプリケーション プログラムです。

暗号アルゴリズムまたはハッシュ 暗号化アルゴリズム、暗号アルゴリズムまたはハッシュ、デジタル署名アルゴリズム（DSA）、キー共有アルゴリズムなど、暗号法の技術を利用したアルゴリズム。

暗号化 メッセージを傍受した人間にはそのメッセージが理解できないような方法で、メッセージを文字化けさせます。

暗号化 データの元の意味を隠して、知られたり使用されたりしないようにする形式（「暗号文」と呼ばれる）に、データ（「プレーンテキスト」と呼ばれる）を暗号変換すること。

暗号解析 システム設計で提供される保護の破壊または回避に必要な知識を得るために、暗号化システムの分析を処理する数理科学。つまり、キーがわからない状態で暗号文をプレーンテキストに変換します。

暗号文 送信される暗号化形式のメッセージ。暗号文は暗号化されたデータです。暗号化プロセスの出力であり、適切な解読キーを使用することで判読可能な形式（プレーンテキスト）に戻せます。

アンチウイルス 既知または潜在するコンピュータ ウイルスを特定および削除するように設計されたソフトウェア プログラム。

い

イベント システムまたはネットワーク内の観察可能な事象。

え

エントリ（LDAP） LDAP 対応ディレクトリに格納されているオブジェクトに与えられた名前。各エントリは、1 つの親エントリ（オブジェクト）およびゼロ個以上の子エントリ（オブジェクト）を持ちます。エントリのデータ コンテンツは 1 つまたは複数の属性で構成され、これらの属性の 1 つ（または複数）が、このオブジェクトを DIT 内で一意に識別するネーミング属性（正確には RDN）として使用されます。

か

外部 ID ストア （ポリシーでの定義に従って）内部ユーザおよび外部ユーザのクレデンシャルと認証確認を実行するために ACS がアクセスする外部データベース。

拡張 ACL Cisco ルータにおける標準 ACL のさらに強力な形式。IP アドレス（発信元または宛先）、ポート（発信元または宛先）、プロトコル、およびセッションが確立されているかどうかに基づいて、フィルタリング決定を行うことができます。

カットスルー パケットが宛先に転送される前にパケットのヘッダーだけが読み取られるスイッチング方式。

カプセル化 あるデータ構造をしばらくの間隠しておくために、別の構造体の中に格納しておくこと。

監査 情報や資産を、ポリシーに準拠し、脆弱性から保護されているものとして保証するための情報の収集および資産の分析。

完全修飾ドメイン名 ホスト名のあとに完全ドメイン名を付けたサーバ名。

き

キー 暗号法では、キーは、暗号化されたテキストを生成するために、アルゴリズムを使用して暗号化されていないテキストの文字列またはブロックに適用されたり、または暗号化されたテキストを復号化したりする変数の値です。キーの長さは、特定のメッセージに含まれるテキストの復号化がどの程度難しくなるかを考慮するうえで、1 つの要因となります。

偽装通信 正常なシステム操作を使用して、2 つのパーティ間で密かに情報をやり取りする方法。たとえば、ファイル サーバ上の使用可能なハード ドライブ容量を変更することで情報をやり取りできます。

基本認証 要求ごとにユーザ名とパスワードを送信することで機能する、最も簡単な Web ベースの認証スキーム。

機密性 情報を表示する権限があるユーザだけに情報が明示されることを保証する必要性。

キャッシュ 特別な高速ストレージ メカニズム。メイン メモリの予約済みセクションまたは独立した高速ストレージ デバイスを使用できます。パーソナル コンピュータでは、通常、メモリ キャッシングとディスク キャッシングの 2 つのタイプのキャッシングが使用されます。

許可 誰かまたは何かが何かを行うことに対する承認、許可、または権限付与。

く

クライアント 「サーバ」と呼ばれる別のシステム エンティティによって提供されるサービスを要求して使用するシステム エンティティ。場合によっては、サーバ自身が別のサーバのクライアントになることもあります。

クライアント / サーバ 1 つのプログラム（クライアント）が別のプログラム（サーバ）のサービスを要求し、サーバがその要求を実行するという、2 つのコンピュータ プログラム間の関係を示します。クライアント / サーバの概念は、単一のコンピュータ内のプログラムでも使用できますが、ネットワークにおいてより重要な概念です。ネットワークでは、クライアント / サーバ モデルにより、さまざまな場所に効率的に配布されているプログラムを簡単に相互接続できます。

グローバル システム オプション TACACS+、EAP-TTLS、PEAP、および EAP-FAST のランタイム特性の設定および EAP-FAST PAC の生成。

け

ゲートウェイ 別のネットワークへの入り口として機能するネットワーク ポイント。

検索（LDAP） ベース ディレクトリ名（DN）、範囲、および検索フィルタを定義することによって実行される動作。

こ

公開キー 暗号法における公開キーとは、公開キーから派生される秘密キーと組み合わせた場合に、メッセージおよびデジタル署名の効果的な暗号化に使用できる暗号キーとして、指定機関から提供される値のことです。

公開キーと秘密キーを組み合わせて使用することを、非対称暗号法と呼びます。公開キーを使用するためのシステムを、公開キー インフラストラクチャ（PKI）と呼びます。

公開キー インフラストラクチャ（PKI） PKI を使用すると、インターネットなどの基本的に安全ではないパブリック ネットワークのユーザでも、信頼できる機関を通じて取得および共有される公開暗号キーと秘密暗号キー ペアを使用することにより、データや金銭を安全かつ内密に交換できます。公開キー インフラストラクチャは、個人または組織を識別できるデジタル証明書と、証明書を格納したり、必要に応じて無効にしたりできるディレクトリ サービスを提供します。PKI のコンポーネントは一般に理解されていますが、さまざまなベンダー アプローチおよびサービスが出現しつつあります。その一方で、PKI のインターネット標準は変わらず有効です。

コマンド セット TACACS+ ベースの許可コマンドのセットがコマンド認可単位で格納されます。

コミュニティ ストリング 簡易ネットワーク管理プロトコル（SNMP）要求に有効なソースを識別し、アクセス可能な情報の範囲を制限するために使用される文字列。Ravlin 装置はパスワードなどのコミュニティ ストリングを使用して、限定された管理ステーションのセットだけにその MIB へのアクセスを許可します。

コンピュータ ネットワーク ホスト コンピュータと、これらのホスト コンピュータでデータ交換できるサブネットワークまたはインターネットワークの集合。

さ

サーバ クライアントと呼ばれる他のシステム エンティティからの要求に応えて、サービスを提供するシステム エンティティ。

サービス選択ポリシー どのアクセス ポリシーが着信要求に適用されるかを決定するルールのセット。

サービス プロビジョニング 特定のアクティビティを実行するために必要な IT システムの構成要素または提供物を「事前準備」すること。これには、ユーザ アカウントやシステム、ネットワーク、アプリケーションのアクセス権限などのデジタル サービスのプロビジョニングと、携帯電話やクレジット カードなどの非デジタル、つまり「物理的な」リソースのプロビジョニングがあります。

サイファ 暗号化および復号化のための暗号アルゴリズム。判読可能なメッセージ（プレーンテキストまたはクリアテキストと呼ばれる）を、判読不能、スクランブル、または非表示のメッセージ（暗号文と呼ばれる）に変換するための方式。

サフィックス（LDAP） ルート、ベースとも呼ばれる、DIT 内の一番上のエントリを示す多数の用語の 1 つ。このエントリは、通常、OpenLDAP の slapd.conf ファイルの suffix パラメータで定義されるため、一般的にこの用語が使用されます。ルート DSE は一種のスーパー ルートです。サフィックスのネーミング。

サブタイプ（LDAP） LDAPv3 では多数のサブタイプを定義しますが、現時点で定義されているのは binary（RFC 2251）および lang（RFC 2596）の 2 つです。サブタイプは、属性の参照時に使用され、たとえば cn;lang-en-us=smith は US 英語を使用して検索を実行することを指定します。UTF-8（cn に使用）ではすべての言語タイプを使用できるため、サブタイプは符号化には影響しません。lang サブタイプは大文字と小文字が区別されます。

し

シェル プロファイル TACACS+ ベースのデバイス管理ポリシーの基本的な「権限コンテナ」であり、ここで、シェル アクセス要求に付与される権限を定義します。

指数バックオフ アルゴリズム ネットワーク デバイスが飽和状態のリンクのデータ送信をタイムアウトし続けないように、実行中に TCP タイムアウト値を調整するために使用されます。

システム管理 管理者グループによって実行されるロールベースの管理機能。

システム設定 システム パフォーマンスを設定するために管理者グループによって実行される、ロールベースの管理機能。

システム操作 ネットワーク内の ACS サーバを効果的に配置および管理するために実行する必要がある操作のセット。

システム ヘルス ダッシュボード 関連付けられた ACS インスタンスのヘルス ステータスに関する情報を提供する Monitoring and Report Viewer ダッシュボード。

出力フィルタリング アウトバウンド トラフィックのフィルタリング。

衝突 複数のシステムが同時に同じ回線で送信した場合に発生します。

証明書 公開キーなどのユーザまたはデバイス属性のデジタル表現であり、信頼できる秘密キーで署名されています。

証明書ベースの認証 HTTP トラフィックを認証および暗号化するために、Secure Sockets Layer（SSL）および証明書を使用すること。

侵入検知 コンピュータおよびネットワーク用のセキュリティ管理システム。IDS はコンピュータまたはネットワーク内のさまざまな領域から情報を収集および分析して、侵入（組織外からの攻撃）と誤用（組織内からの攻撃）の両方を対象に、可能性のあるセキュリティ侵犯を識別します。

信頼性 元の情報の正当性および適合性。

す

スキーマ（LDAP） （名目上）関連付けられることがある属性およびオブジェクト クラスのパッケージ。すべての ASN.1 関連情報を読み取りおよび解析できるように、アプリケーションで使用（参照）するオブジェクト クラスおよび属性をまとめたスキーマが LDAP サーバに対して特定されます。OpenLDAP では、これは slapd.conf ファイルで行われます。

せ

整合性 情報が偶然または故意に変更されておらず、また正確かつ完全であることを保証する必要性。

セキュリティ ポリシー システムまたは組織がどのようにセキュリティ サービスを提供して機密に関わる重要なシステム リソースを保護するかを、指定または規定するルールおよび慣例のセット。

セッション ネットワーク トラフィックが渡される 2 つのホスト間のバーチャル コネクション。

セッション キー 対称暗号化のコンテキストで、一時的または比較的短い期間使用されるキー。通常、セッション キーは単一の接続またはトランザクション セットの期間など、2 つのコンピュータ間の定義済みの通信期間に使用されるか、または比較的大容量のデータを保護し、そのために頻繁にキーを入力する必要があるアプリケーションで使用されます。

セッション条件 カスタム条件、および日時条件。

セッション（LDAP） LDAP クライアントがバインド コマンドを送信すると、クライアントとサーバ間でセッションが発生します。セッションは匿名または認証済みのいずれかになります。

設定管理 既知のベースライン条件を再確立して管理するプロセス。

全二重 一度に両方向にデータを伝送する二重通信チャネルのタイプ。同時に 2 つの方向にデータを送信することを意味しています。送信者と受信者の両方で同時に送信できる通信方式です。

そ

増分バックアップ ユーザが Monitoring and Report Viewer データベースの小規模なバックアップを定期的に作成できるようにするスケジュール ジョブ。

属性（LDAP） エントリ内のデータは属性値のペアに含まれています。各属性には名前（場合によっては、略称）があり、objectClass に属しています。属性の特性については、ASN.1 定義で詳しく説明されています。1 つまたは複数の objectClasses をスキーマに含めることができます。属性の ASN.1 定義に応じて、1 つのエントリ内に同じ名前を持つ属性の属性値のペアを複数指定できます。1 つ（または複数）の属性、ネーミング属性、または RDN により、エントリは常に一意に識別されます。

た

対応策 脅威が検出されたあと、エクスプロイトが実行されないようにする対処的方法。Intrusion Prevention Systems（IPS; 侵入防御システム）では、一般的に、侵入者がこれ以上コンピュータ ネットワークにアクセスしないようにする対応策が展開されています。その他の対応策としては、パッチ、アクセス コントロール リスト、およびマルウェア フィルタがあります。

ダイジェスト認証 Web クライアントがパスワードの MD5 ハッシュを計算して、パスワードを持っていることを証明できるようにします。

ち

チェックサム 関数によって計算され、データ オブジェクトのコンテンツによって決まる値。データ内の変更を検出するために、オブジェクトに格納されるか、またはオブジェクトと一緒に送信されます。

チャレンジ / レスポンス ユーザにいくつかの個人情報の入力（レスポンス）を要求（チャレンジ）する一般的な認証技術。スマート カードを利用する大部分のセキュリティ システムは、チャンレンジ / レスポンスに基づいています。スマート カードに入力するコード（チャレンジ）がユーザに与えられます。次に、スマート カードによって、ユーザがログインするために提示できる新しいコード（レスポンス）が示されます。

中断 システムのサービスおよび機能の正常な動作に割り込んだり、動作を妨害したりする状況またはイベント。

て

ディクショナリ RADIUS および TACACS+ プロトコル、内部ユーザ、および内部ホストの属性を設定するストア。

ディクショナリ攻撃 ディクショナリ内のフレーズまたはワードのすべてを試して、パスワードまたはキーを解読しようとする攻撃。可能なすべての組み合わせを試す総当たり攻撃に対して、ディクショナリ攻撃では定義済みのワード リストが使用されます。

データグラム Request for Comment 1594 には、「発信元と宛先のコンピュータと転送ネットワーク間の以前の交換に依存することなく、発信元から宛先のコンピュータに十分な情報を送信する、完全独立した自己充足型のデータ エンティティである」と記述されています。この用語は、一般にパケットという用語に置き換えられています。データグラムまたはパケットはメッセージの単位であり、インターネット プロトコルによって処理され、インターネットで転送されます。たとえば電話での音声会話のように、2 つの通信点の間に固定期間の接続がないため、データグラムまたはパケットは以前の交換に依存することなく完全独立している必要があります （このようなプロトコルをコネクションレス型と呼びます）。

デーモン 多くの場合、システム ブート時に開始され、システム上でユーザ介入なしで実行し続けるプログラム。デーモン プログラムは、必要に応じて要求を他のプログラム（またはプロセス）に転送します。デーモンという用語は UNIX の用語ですが、他の多くのオペレーティング システムでデーモンに対するサポートが提供されています。ただし、別の名前で呼ばれている場合もあります。たとえば、Windows では、デーモン、システム エージェント、サービスと呼ばれます。

デジタル証明書 Web 上でビジネスまたは他のトランザクションを実行するときに、ユーザのクレデンシャルを証明する電子的な「クレジット カード」。これは、認証局によって発行されます。デジタル証明書には、ユーザ名、シリアル番号、有効期限、証明書保持者の公開キーのコピー（メッセージおよびデジタル署名の暗号化に使用される）、および認証発行局のデジタル署名が格納され、これにより受信者はその証明書が本物であることを確認できます。

デジタル署名 メッセージの送信者を一意に識別し、送信されてからメッセージが変更されていないことを証明するメッセージのハッシュ。

デジタル封筒 暗号化されたセッション キーを使用する暗号化メッセージ。

デバイス管理 ネットワーク デバイス上で実行される管理操作を制御および監査する機能。ネットワーク デバイス管理者ロールには、ネットワーク デバイス上で管理操作を実行するための完全なアクセス権があります。

デュー デリジェンス 組織は、詐欺や悪用を防ぐための防護策を開発および展開し、さらにこれらが発生した場合の検出手段も展開する必要があるという要件。

と

等式（LDAP） ワイルドカードを含まない検索フィルタで使用すると、等式により属性の比較ルールが定義されます。このとき、コンテンツと長さの両方が正確に一致している必要があります。ワイルドカードが使用された場合、これはサブストリングと呼ばれ、SUBSTR ルールが使用されます。

盗聴 ファシリティまたはネットワークへのアクセスを可能にする情報がもれるおそれのあるプライベートな会話を聞くこと。

匿名（LDAP） LDAP セッションは、セッションの開始（バインドの送信）時にユーザ DN または秘密が指定されなかった場合、匿名となります。

ドメイン 名前で識別される認識の範囲、または一部のプログラム エンティティや多数のネットワーク ポイントまたはアドレスに関する事実の集合。インターネットでは、ドメインはネットワーク アドレスのセットで構成されます。インターネットのドメイン ネーム システムでは、ドメインは、サブドメインまたはホストを示すネーム サーバ レコードと関連付けられた名前です。Windows NT および Windows 2000 では、ドメインはユーザ グループ用のネットワーク リソース（アプリケーション、プリンタなど）のセットです。ユーザがネットワーク内のさまざまなサーバに格納されているリソースにアクセスするために必要なことは、ドメインにログインすることだけです。

ドメイン名 インターネット上の組織または他のエンティティの位置を示します。たとえば、ドメイン名「www.sans.org」は、「sans.org」のインターネット アドレスをインターネット ポイント 199.0.0.2 に位置付け、さらに「www」という名前の特定のホスト サーバを示します。ドメイン名の「org」の部分は、組織またはエンティティの目的を示し（この例では「組織」）、トップレベル ドメイン名と呼ばれます。ドメイン名の「sans」の部分は組織またはエンティティを定義し、トップレベルという呼び方にあわせて、セカンドレベル ドメイン名と呼ばれます。

な

内部 ID ストア 内部ユーザおよびホストの認証に使用される、内部ユーザの属性およびクレデンシャル情報を格納するデータベース。

名前空間（LDAP） 特定の Directory Information Tree（DIT; ディレクトリ インフォメーション ツリー）にある（DIT 内に含まれる、DIT によってバインドされている）すべての DN を示す用語。DIT ルートが dc=example,dc=com の場合、cn=people,dc=example,dc=com は名前空間にあると言えますが、ou=people,dc=example,dc=net は名前空間にあるとは言えません。これは dc=example,dc=net 名前空間にあることになります。

に

認可プロファイル RADIUS ベースのネットワーク アクセス サービスに使用される基本的な「権限コンテナ」。認可プロファイルは、ネットワーク アクセス要求に付与されるすべての権限を定義する場所です。応答で返される VLAN、ACL、URL リダイレクト、セッション タイムアウト、再認可タイマー、またはその他の RADIUS 属性を認可プロファイルに定義します。

認証 主張されている ID の正確さを確認するプロセス。

認証済み（LDAP） セッションの開始（バインドの送信）時にユーザ DN および秘密が指定された場合、セッションは認証済みとなります。

ね

ネーミング コンテキスト（LDAP） ルートの認定者名（DN）から始まり、これを含む一意の名前空間。namingContext またはディレクトリ インフォメーション ツリー（DIT）とも呼ばれます。

ネーミング属性（LDAP） ディレクトリ インフォメーション ツリー（DIT）内のエントリごとの一意の識別子。相対認定者名（RDN）とも呼ばれます。

ネットワーク デバイス グループ 場所およびタイプ別のネットワーク デバイスの論理グループ。

ネットワーク リソース ネットワーク デバイス グループ（NDG）、ネットワーク デバイス、AAA クライアント、外部ポリシー サーバなど、ACS ネットワークにアクセスするデバイス リポジトリ内のすべてのネットワーク デバイスを定義するドロワ。

は

ハイブリッド暗号化 2 つ以上の暗号化アルゴリズムを組み合わせた暗号法の適用。特に対称と非対称の暗号化の組み合わせです。

ハイブリッド攻撃 数字および記号をディクショナリ ワードに追加することによって、ディクショナリ攻撃方式を強化します。

バインド（LDAP） LDAP サーバに接続するときに実行される順序の最初の操作をバインドと呼びます。バインド操作により、認証に使用されるエントリの DN および使用されるパスワードが送信されます。匿名バインドの場合、両方とも値は NULL です。

破損 システムの機能またはデータを悪い方向に変更することによって、システムの動作に望ましくない変更を及ぼす危険な処理。

ハッシュ関数 大きなテキストの一方向の「チェックサム」を生成するために使用されます。このチェックサムは逆向きには使用できません。このハッシュ関数の結果を使用すると、大きなファイルが変更されたかどうかを、そのファイルを相互に比較せずに確認できます。よく使用されるハッシュ関数は MD5、SHA1、および SHA2 です。

ハブ 1 つのポートで受信したデータを他のすべてのポートに繰り返すことで機能するネットワーク デバイス。これにより、1 つのホストで送信されたデータが、ハブ上の他のすべてのホストに再送信されます。有線、無線に関係なく、スター型ネットワークの中心デバイスになります。無線アクセス ポイントは無線ネットワークのハブとして動作します。

ひ

非カプセル化 特定のレイヤのヘッダーを取り去って、パケットの残りをプロトコル スタック上の次の上位層に渡すプロセス。

非対称キー交換 非対称キーまたは公開キーの暗号法は、キー ペアの概念に基づいています。それぞれのペアの半分（片方のキー）だけで情報を復号化できるように、残りの半分（もう片方のキー）で情報を暗号化できます。キー ペアの片方である秘密キーを知っているのは指定されたオーナーだけであり、もう片方の公開キーは広く公開されますが、オーナーと関連付けられています。

ふ

ファイアウォール TCP/IP フラグメンテーション攻撃。この攻撃は、さまざまなメディア間でより効率的に転送できるように IP でパケットがフラグメントに分解されるため、発生します。TCP パケット（およびそのヘッダー）は IP パケットで伝送されます。この攻撃では、2 つめのフラグメントに不正なオフセットが格納され、パケットを再構築したときに、ポート番号が上書きされます。

フィルタ どのパケットを使用して、どのパケットを使用しないかを指定するために使用されます。スニファで使用すると、どのパケットを表示するかを決定できます。また、ファイアウォールでは、どのパケットをブロックするかを決定できます。

フィルタリング ルータ セキュリティ ポリシーに応じて、データ パケットの通過を選択的に妨げるインターネットワーク ルータ。フィルタリング ルータは、ファイアウォールまたはファイアウォールの一部として使用できます。ルータは、通常、ネットワークからパケットを受信して、2 つめのネットワーク上のいずれの場所に転送するかを決定します。フィルタリング ルータは同じことを行いますが、最初に何らかのセキュリティ ポリシーに従って、そもそもパケットを転送する必要があるのかどうかを判断します。ポリシーは、ルータにロードされているルール（パケット フィルタ）によって実装されます。

復号化 暗号化されたメッセージを元のプレーンテキストに変換するプロセス。

ブラウザ ワールドワイド ウェブ上のサーバから情報を取得して表示できるクライアント コンピュータ プログラム。

フラグメンテーション データ ファイルを、ストレージ メディアの 1 つの場所に連続した単一のビット順序で格納するのではなく、複数の「塊」、つまりフラグメントで格納するプロセス。

ブリッジ Local Area Network（LAN; ローカル エリア ネットワーク）を、同じプロトコル（イーサネット、トークン リングなど）を使用する別のローカル エリア ネットワークと接続する製品。

フレーム アドレス指定および必要なプロトコル制御情報を備えたユニットとして、ネットワーク ポイント間で送信されるデータ。フレームは、通常、シリアル ビット単位で送信され、フレームにはデータを「囲む」ヘッダー フィールドおよびトレーラ フィールドが含まれます （一部の制御フレームにはデータは含まれません）。

ブロードキャスト 同じメッセージを複数の受信者に同時に送信すること。1 つのホストからネットワーク上のすべてのホストへの送信です。

ブロードキャスト アドレス UDP または ICMP プロトコルを使用して、特定のネットワーク上のすべてのホストにデータグラムをブロードキャストするために使用されるアドレス。

プロキシ HTTP プロキシは、HTTP クライアントとサーバ間における通信の仲介として動作するサーバです。

ブロック暗号 一度に 1 つのデータ ブロックを暗号化します。

プロトコル 電気通信接続のエンド ポイントで通信時に使用する特別なルール セット。プロトコルは、電気通信接続のさまざまなレベルに存在します。たとえば、ハードウェア デバイス レベルのデータ交換プロトコルや、アプリケーション プログラム レベルのデータ交換プロトコルがあります。Open Systems Interconnection（OSI; 開放型システム間相互接続）として知られている標準モデルでは、電気通信交換の各レイヤに、交換の両端で認識および順守する必要があるプロトコルが 1 つまたは複数あります。多くの場合、プロトコルは業界標準または国際標準で記述されています。

分解 バイナリ プログラムを取得して、そこからソース コードを抽出するプロセス。

へ

ヘッダー プロトコル スタックでパケットを処理するために必要なパケット内の追加情報。

ほ

ポート設定 さまざまな IP アドレスまたはポート設定で 2 つ以上の LDAP インスタンスを作成することにより、異なる LDAP サーバまたは同じ LDAP サーバ上の異なるデータベースを使用して認証するように ACS を設定できます。

ホスト インターネット上の他のコンピュータに対して完全双方向アクセスが可能なコンピュータ。または、Web サーバで 1 つ以上の Web サイトにページを提供しているコンピュータです。

ホストベース ID ホストベースの侵入検知システムは、オペレーティング システムの監査レコードから得られる情報を使用して、侵入検知ソフトウェアがインストールされているホストで発生するすべての動作を監視します。これらの動作は、あらかじめ定義されているセキュリティ ポリシーと比較されます。侵入検知システムによって必ず使用される処理能力の増加のために、この監査証跡の分析は潜在的に大きなオーバーヘッド要件をシステムに課します。監査証跡のサイズおよびシステムの処理能力によっては、監査データを確認することによってリアルタイム分析機能が失われる可能性があります。

ポリシー条件 ポリシーに基づくルール ベースの共通条件。アクセス要求を評価して決定を返すために使用されるルールのセットです。

ポリシー要素 ポリシー条件（たとえば、時刻や日付、またはユーザ選択属性に基づくカスタム条件）および権限（認可プロファイルなど）を定義するグローバルな共有オブジェクト。ポリシー要素は、ポリシー ルールの作成時に参照されます。

本人拒否 認証システムが、有効なユーザの認識に失敗する場合。

ゆ

ユーザおよび ID ストア ユーザ、ユーザ属性、およびユーザ認証オプションのリポジトリ。

ユーザ属性設定 内部ユーザの ID 属性設定からなる管理タスク。

ユーザ認証オプション TACACS+ パスワード認証をイネーブルまたはディセーブルにするオプション。

る

ルート（LDAP） ルート エントリ（別名、ベース、サフィックス）は DIT の一番上のエントリを示す多数の用語の 1 つです。ルート DSE は一種のスーパー ルートです。

ルート DSE（LDAP） 概念的に LDAP 階層の一番上のエントリ。スーパー ルートとして見なされ、通常、非表示です（つまり、通常の操作ではアクセスできません）。ルート、ベース、またはサフィックスと混同されることがあります。DSE は DSA Specific Entry の略で、DSA は Directory System Agent（DAP または LDAP アクセスを提供するディレクトリ対応サービス）の略です。rootDSE に関する情報は、OpenLDAP で OpenLDAProoDSE クラスオブジェクトを問い合わせることにより取得できます。この情報により、サポート対象のプロトコル バージョン、サポート対象のサービス、およびサポート対象のネーミング コンテキストまたは DIT に関する情報が得られます。

れ

レイヤ 2 トンネリング プロトコル（L2TP） インターネット上でバーチャル プライベート ネットワークを操作できるようにするために、インターネット サービス プロバイダーによって使用されるポイントツーポイント トンネリング プロトコルの拡張。

レイヤ 2 フォワーディング プロトコル IP を介した PPP のトンネリングを使用して、ダイヤルアップ サーバで開始され、ダイヤルアップ ユーザに対して透過的なダイヤルアップ リンクの仮想拡張をネットワーク上に作成するインターネット プロトコル（シスコが開発）。

ろ

ローカル操作（セカンダリ サーバ専用） セカンダリ サーバを登録または登録解除したり、[Join a Distributed System] ページからセカンダリ サーバおよびローカル モード要求を複製したりするために実行する操作。

ロール それぞれに関連付けられた権限セットを持つ一般的な管理タスクのセット。管理者は複数の定義済みロールを持つことができ、また 1 つのロールは複数の管理者に適用できます。

ログ設定 ロギング カテゴリとメンテナンス パラメータを使用して、アカウンティング メッセージ、AAA 監査および診断メッセージ、システム診断メッセージ、管理監査メッセージについて生成されるログを設定および格納できるようにするシステム。

露出 機密データを直接不正なエンティティに公開する危険な処理。

わ

割り込み　何かが発生したことを OS に通知する信号。

INDEX

記号

! 13-35
% 演算子 13-61
& フォーマット記号 13-35
& 演算子 13-61
* 演算子 13-61
+ 演算子 13-61
/ 演算子 13-61
<= 演算子 13-61
<> 演算子 13-61
< フォーマット記号 13-35
< 演算子 13-61
= 演算子 13-61
>= 演算子 13-61
> フォーマット記号 13-35
> 演算子 13-61
@ フォーマット記号 13-35
- 演算子 13-61

数字

3 桁ごとの区切り文字 13-33

A

ABS 関数 13-54
ACS の分散展開 17-2
ADD_DAY 関数 13-54
ADD_HOUR 関数 13-54
ADD_MINUTE 関数 13-54
ADD_MONTH 関数 13-54
ADD_QUARTER 関数 13-54
ADD_SECOND 関数 13-54
ADD_WEEK 関数 13-54
ADD_YEAR 関数 13-54
Add Group コマンド 13-51, 13-52
Advanced Filter ダイアログ 13-73, 13-74, 13-75
Advanced Sort コマンド 13-48
Aggregation ダイアログ 13-65
AND 演算子 13-61, 13-75
Any Of 条件 13-70
arguments 13-53
Arrange Columns ダイアログ 13-43
AVERAGE 関数 13-55
Average 関数 13-64

B

Between 演算子 13-39
BETWEEN 関数 13-55
Between 条件 13-70, 13-74
Bottom N 条件 13-70
Bottom Percent 条件 13-70

C

Calculation ダイアログ 13-53, 13-62, 13-63
CEILING 関数 13-55
Chart Subtype コマンド 13-78
Cisco CAT 6K 4-24
Column Properties ダイアログ 13-30
Column Width コマンド 13-30
Conditional Formatting ダイアログ 13-38, 13-39, 13-41
COUNT_DISTINCT 関数 13-55
Count Value 関数 13-64

COUNT 関数 13-55
Count 関数 13-64
CRUD 操作 7-6
CSV ファイル 13-24, 13-26
Currency フォーマット オプション 13-32
Custom フォーマット オプション 13-32

D

Date and Time Format ダイアログ 13-36
Date or Time Column Format ダイアログ 13-37
DAY 関数 13-55
DIFF_DAY 関数 13-55
DIFF_HOUR 関数 13-55
DIFF_MINUTE 関数 13-55
DIFF_MONTH 関数 13-55
DIFF_QUARTER 関数 13-55
DIFF_SECOND 関数 13-55
DIFF_WEEK 関数 13-55
DIFF_YEAR 関数 13-55

E

EAP-FAST
- ID 保護 B-21
- PAC
  - 更新 B-27
  - 自動プロビジョニング B-24
  - 手動プロビジョニング B-25
  - 定義 B-22
- イネーブル化 B-27
- フェーズ B-20
- マスターキー
  - 定義 B-22
- ロギング B-20

EAP-FAST 設定
- 設定 18-3

EAP-TLS 設定
- 設定 18-2

Equal to 条件 13-70
Excel スプレッドシート 13-24
Export Data ダイアログ 13-25

F

false 関数 13-56
Filter ダイアログ 13-72, 13-73
Filter ドロップダウン リスト 13-76
FIND 関数 13-56
FIRST 関数 13-56
First 関数 13-64
Fixed フォーマット オプション 13-32
Font ダイアログボックス 13-40
Format Chart ページ 13-78
Format コマンド 13-78

G

General Date フォーマット オプション 13-32
General Number フォーマット オプション 13-32
Go to page 選択リスト 13-23
Greater Than or Equal to 条件 13-70
Greater Than 条件 13-70
Group Detail ダイアログ 13-52
Group ダイアログの Page Break 13-42

H

Hide Column コマンド 13-46
Hide Detail コマンド 13-69
Hide or Show Items ダイアログ 13-45
HTML ファイル 13-27

I

ID ストア順序 8-75
If...Then...Else 文 13-56

IF 関数 13-56
Interactive Viewer 13-21, 13-22
IN 関数 13-56
ISBOTTOMNPERCENT 関数 13-57
ISBOTTOMN 関数 13-56
Is False 演算子 13-39
Is False 条件 13-70
Is Not Null 演算子 13-39
Is Not Null 条件 13-70
Is Null 演算子 13-39
ISNULL 関数 13-57
Is Null 条件 13-70
ISTOPNPERCENT 関数 13-57
ISTOPN 関数 13-57
Is True 演算子 13-39
Is True 条件 13-70

L

LAST 関数 13-57
Last 関数 13-64
LEFT 関数 13-57
LEN 関数 13-57
Less Than or Equal to 条件 13-70
Less Than 条件 13-70
LIKE 関数 13-57
Like 条件 13-70
Long Date フォーマット オプション 13-32
Long Time フォーマット オプション 13-32
Lowercase フォーマット オプション 13-32
LOWER 関数 13-58

M

MAX 関数 13-58
Max 関数 13-64
MEDIAN 関数 13-58
Median 関数 13-64
Medium Date フォーマット オプション 13-32
Medium Time フォーマット オプション 13-32
MIN 関数 13-58
Min 関数 13-64
Mode 関数 13-64
MOD 関数 13-58
Monitoring and Report Viewer
スケジューリングされたジョブの表示 15-12
データ アップグレード ステータス 15-15
データのバックアップおよび削除 15-3
復元 15-7
プロセス ステータスの表示 15-14
リモート データベースの設定 15-18
Monitoring & Report Viewer
ダッシュボード 11-2
MONTH 関数 13-58
Move to Group Header コマンド 13-44
Move to Group Header ダイアログ 13-44
MOVINGAVERAGE 関数 13-58

N

Not Between 演算子 13-39
Not Between 条件 13-70
Not Equal to 条件 13-70
Not Like 条件 13-70
NOTNULL 関数 13-58
NOT 演算子 13-61, 13-75
NOW 関数 13-58
Number Column Format ダイアログ 13-33
Number column format ダイアログ 13-34

O

OR 演算子 13-61, 13-75

P

PAC

更新 B-27
自動プロビジョニング B-24
手動プロビジョニング B-25
定義 B-22
PDF ファイル 13-27
PEAP
ID 保護 B-15
フェーズ B-15
PEAP 設定
設定 18-3
PERCENTILE 関数 13-58
PERCENTRANK 関数 13-58
PERCENTSUM 関数 13-59
Percent フォーマット オプション 13-32
Print ダイアログ 13-27

Q

QUARTER 関数 13-59
QUARTILE 関数 13-59
Quartile 関数 13-64

R

RADIUS プロキシ 4-30
サポートされる RADIUS 属性 4-32
サポートされるプロトコル 4-32
プロキシ サービスの設定 4-34
RANK 関数 13-59
Reorder Columns コマンド 13-43
RIGHT 関数 13-59
ROUNDDOWN 関数 13-59
ROUNDUP 関数 13-59
ROUND 関数 13-59
RUNNINGSUM 関数 13-59

S

Save As ダイアログ 13-26
Scientific フォーマット オプション 13-32
SEARCH 関数 13-59
Select data item ダイアログ 13-72
Short Date フォーマット オプション 13-32
Short Time フォーマット オプション 13-32
Show Columns コマンド 13-46
Show Columns ダイアログ 13-46
Show Detail コマンド 13-69
SQRT 関数 13-59
Standard Deviation 関数 13-64
STDEV 関数 13-60
String Column Format ダイアログ 13-36
String column format ダイアログ 13-34
SUM 関数 13-60
Sum 関数 13-64

T

TACACS+ 設定
設定 18-1
TODAY 関数 13-60
Top N 条件 13-70
Top Percent 条件 13-70
TRIMLEFT 関数 13-60
TRIMRIGHT 関数 13-60
TRIM 関数 13-60
true 関数 13-60

U

Unformatted フォーマット オプション 13-32
Uppercase フォーマット オプション 13-32
UPPER 関数 13-60

V

Variance 関数 13-64
VAR 関数 13-60
VPN リモート アクセス 4-21
  アクセス サービスの設定 4-23
  サポートされる ID ストア 4-22
  サポートされるクライアント 4-23
  サポートされるネットワーク アクセス サーバ 4-23
  サポートされるプロトコル 4-22

W

WEEKDAY 関数 13-60
WEEK 関数 13-60
WEIGHTEDAVERAGE 関数 13-60
Weighted average 関数 13-64

X

x 軸の値 13-76

Y

YEAR 関数 13-60
y 軸の値 13-76

あ

アクセス
  Interactive Viewer 13-21
  データ 13-67
  目次のエントリ 13-24
値
  計算 13-43
  検索 13-72
  最後の値を返す 13-57, 13-64
  最小値を返す 13-58, 13-64, 13-70
  最大値を返す 13-58, 13-64
  指定した値のテスト 13-56
  指定した値を返す 13-70
  重複しない値のカウント 13-55, 13-64
  重複の非表示 13-67, 13-68
  順位の決定 13-59
  上位または下位のソート 13-75
  セットのテスト 13-71
  ヌル以外のテスト 13-58
  ヌルのテスト 13-57, 13-71
  ヌルを返す 13-70
  範囲のテスト 13-71
  比較 13-38, 13-39, 13-71
  頻繁に出現する値の表示 13-64
  平均化 13-55, 13-58, 13-60, 13-64
  丸め 13-55, 13-59
値系列 13-76
値の範囲 13-38, 13-39, 13-70, 13-71
アラーム 12-1
  syslog ターゲット 12-35
  システム アラーム 12-34
アラーム スケジュール 12-9

い

以下演算子 13-61
移行
  一般的なシナリオ 2-8
  検討 2-3
  サポートされるバージョン 2-2
  ダウンロード 2-3
  要件 2-2
以上演算子 13-61
一致する文字パターン 13-71
移動、カラムの 13-43
移動、レポート全体の 13-23
色 13-40
印刷 13-27
印刷オプション 13-27

インポートおよびエクスポート
インポート ファイルの作成 5-22
サポートされるオブジェクト 5-20

え

演算子 13-39, 13-61

お

大文字 13-60
大文字と小文字の変換 13-35
大文字と小文字を区別しない検索 13-59
大文字と小文字を区別する検索 13-56

か

外部 ID サーバ
RADIUS ID ストア 8-61
RSA SecurID 8-55
外部 ID ストア 8-2
LDAP 8-19
Microsoft AD 8-39
改ページ 13-42
科学的数値 13-33
加算演算子 13-61
カスタマイズ
フォーマット 13-34, 13-35
カテゴリ系列 13-76
カラム
型の決定 13-33
行のカウント 13-64
最後の値の決定 13-57, 13-64
最初の値の決定 13-56, 13-64
サイズ変更 13-25, 13-30
削除 13-45
順序の変更 13-43
データのソート 13-48, 13-75
データの配置 13-30
データの表示 13-31
データのフォーマット 13-38, 13-39
日付値と時刻値のグループ化 13-51
カラム ヘッダー 13-25
カラム名 13-72
関係 13-76
カンマ区切り形式のファイル。「CSV ファイル」を参照
管理者アクセス設定 16-13
管理者パスワードのリセット 16-22
管理者パスワード ポリシー 16-10
管理者ロール 16-2

き

機能 13-53, 13-54, 13-64, 13-65
行 13-67, 13-69
行ごとの比較 13-56

く

区切りテキスト ファイル 13-24, 13-26
グラフ
概要 13-76
クリア、データ フィルタの 13-73
グループ
改ページの設定 13-42
行のカウント 13-55
縮小 13-51, 13-69
追加 13-50, 13-51
データの集計 13-63
データのソート 13-49
データの表示 13-43, 13-67
グループ化
フィルタ条件 13-75
グループ化の間隔 13-51

け

計算　13-43
計算カラム
　値の配置　13-56
　作成　13-53, 13-61
　データの集計　13-63, 13-65, 13-66
検索　13-56, 13-59, 13-72
検索、テキスト値の　13-56, 13-59
減算演算子　13-61
検出、テキスト値の　13-56, 13-59

こ

合計　13-38, 13-59, 13-60, 13-64
降順のソート　13-48, 13-49
固定数値　13-33
小文字　13-58
コンテキスト メニュー　13-22

さ

サイズ変更、カラムの　13-25, 13-30
削除
　改ページ　13-42
　カラム　13-45
　条件フォーマット　13-41
　データ フィルタ　13-73
　フィルタ条件　13-75
作成
　計算カラム　13-53, 13-61
　集計行　13-65, 13-66
　データ グループ　13-50, 13-51
　データ フィルタ　13-70, 13-71, 13-72, 13-73
　フォーマット規則　13-38, 13-39
サブストリング　13-57, 13-59, 13-70
サブタイプ（グラフ）　13-78
算術演算子　13-61

し

式
　データの計算　13-61
　データのフィルタリング　13-70, 13-71, 13-73, 13-75
時刻値　13-36, 13-51
時刻データ型　13-32
時刻フォーマット　13-32, 13-36
集計値　13-43
集計関数　13-64, 13-65
集計行
　作成　13-65, 13-66
　データのフォーマット　13-31
重複値　13-67, 13-68
重複しない値　13-55, 13-64
縮小、データ グループの　13-51, 13-69
条件
　データのフィルタリング　13-70, 13-73
　データのフォーマット　13-38
条件フォーマット規則　13-38, 13-39
乗算　13-62
乗算演算子　13-61
昇順のソート　13-48, 13-49
小数値　13-33
情報オブジェクト　13-31
除算　13-58, 13-61
除算演算子　13-61

す

数学的関数　13-53, 13-54
数値　13-25, 13-34
数値式　13-61, 13-62
数値データ型　13-32
数値フォーマット　13-32, 13-33, 13-34
ストリング　13-34, 13-57, 13-70
ストリング データ型　13-32
ストリングの変換　13-35

ストリング パターン 13-59
ストリング フィールド 13-71
スプレッドシート レポート 13-24

せ

セキュリティ アクセス グループ 4-24
セクション 13-69
絶対値 13-54
先頭文字 13-60

そ

ソート順序 13-48
ソート、複数のカラムの 13-49

た

タイムスタンプ 13-58, 13-60
ダウンロード 18-42

ち

注意
　説明 ii-xxiv
中央値 13-58, 13-64
注、説明 ii-xxiv

つ

追加
　改ページ 13-42
　集計行 13-65, 13-66
　データ グループ 13-50, 13-51
　データ フィルタ 13-70, 13-71, 13-72, 13-73
　フォーマット規則 13-38, 13-39
通貨 13-33
通貨記号 13-33
通貨フォーマット オプション 13-33

て

データ
　アクセス 13-67
　関係のプロット 13-76
　配置 13-30
　非表示 13-45
　表示 13-31, 13-43, 13-67
データ型 13-33
データ行 13-67, 13-69
データ セクション 13-69
データ セット 13-43, 13-64, 13-67, 13-76
データ ソース 13-26, 13-33, 13-48, 13-67
データ フィルタ 13-70, 13-71, 13-72, 13-73
データ ポイント 13-76
テーブル
　行のカウント 13-55, 13-64
　データの集計 13-63, 13-65, 13-66
テーマ 13-78
テキスト
　値の集計 13-65
　大文字と小文字の変換 13-35
　検索 13-56, 13-59
　ラベルの変更 13-28
テキスト スタイル 13-40
テキスト パターン 13-71
テキスト ファイル 13-24, 13-26
テキスト フォーマット 13-32
デザイン
　データの構成 13-43
　データの非表示 13-67
　保存 13-27
テスト
　値のセット 13-71
　値の範囲 13-71
　ヌル値 13-57, 13-71
　ヌル以外の値 13-58

文字パターン 13-71
デフォルトのネットワーク デバイス 7-18
デフォルトのフォーマット 13-29, 13-30
展開、セクションまたはグループの 13-69
展開、目次のエントリの 13-24
テンプレート 13-29, 13-78

と

等価 13-61, 13-74
等価演算子 13-61
閉じる、標準ビューアを 13-21
トラブルシューティング
Expert Troubleshooter 14-2
サポート バンドル 14-1
接続 14-1

な

内部 ID ストア 8-1
ナビゲーション ツール 13-23
ナビゲート、レポート全体の 13-23

ぬ

ヌル値 13-57, 13-58, 13-70, 13-71
ヌル値フィルタ 13-71
ヌル以外の値 13-57, 13-58, 13-70

ね

ネーミング
計算カラム 13-62

は

パーセント 13-33, 13-57, 13-58
パーセント演算子 13-61
背景色 13-40
配置オプション 13-30
配置、データの 13-30
パターン マッチング フィルタ 13-71
範囲フィルタ 13-71

ひ

比較 13-38, 13-39, 13-56
比較演算子 13-39, 13-71
比較フィルタ 13-71
日付値 13-36, 13-51, 13-55
日付計算 13-63
日付式 13-61, 13-63
日付データ型 13-32
日付フォーマット 13-32, 13-36
等しくない演算子 13-61
非表示
重複値 13-67, 13-68
詳細行 13-69
レポート項目 13-45
非表示項目 13-46
ビューア 13-21
表示
詳細行 13-69
データ 13-31, 13-43, 13-67
特定のレポート ページ 13-23, 13-24
目次 13-23
レポート 13-21
表示、環境の 13-21
標準ビューア 13-21
標準偏差 13-60, 13-64
開く
Interactive Viewer 13-21
エクスポートされたデータ ファイル 13-26

ふ

フィールド 13-28

フィルタ 13-70, 13-71, 13-72, 13-73
フィルタ条件 13-70, 13-73, 13-75
ブール値 13-56, 13-60, 13-70
フォーマット
カスタマイズ 13-34, 13-35
カラム ヘッダー 13-29
条件フォーマットの削除 13-41
条件フォーマットのプレビュー 13-40
ストリング データ 13-34
選択 13-33
データ型 13-31
データのエクスポート 13-25
変更 13-29, 13-39
ラベル 13-28, 13-29
フォーマット オプション 13-33, 13-34, 13-36
フォーマット記号 13-34, 13-35
フォーマット規則 13-38, 13-39
フォーマット パターン 13-34, 13-35
フォント 13-40, 13-78
複数ページ レポート 13-68
フッター 13-63
負の数値 13-33
ブランク文字 13-60
プレビュー、条件フォーマットの 13-40
分散 13-60, 13-64

へ

平均 13-55, 13-58, 13-60, 13-64
平方根 13-59
ページ移動ツールバー 13-23
ヘッダー 13-25, 13-63
変換 13-35
変更
カラム ヘッダー 13-25, 13-29
グラフ サブタイプ 13-78
集計値 13-31
条件フォーマット 13-39
データ フィルタ 13-73
デフォルトのフォーマット 13-29
ラベル 13-28
レポート 13-21

ほ

保存
エクスポートされたデータ 13-26
レポート デザイン 13-27

ま

マスターキー
定義 B-22
末尾文字 13-60
丸め 13-55, 13-59

め

メニュー 13-22
メンバーシップ フィルタ 13-71

も

文字のプレースホルダ 13-35
文字パターン 13-59, 13-71
最も優先的にソートされるカラム 13-49

よ

要約値 13-59, 13-60, 13-64
より大きい演算子 13-61
より小さい演算子 13-61

ら

ライセンス 18-35
ラベル 13-28, 13-29

フォーマット 13-29

り

リテラル値 13-74

る

累積合計 13-59

れ

レポート 13-1
印刷 13-27
お気に入り 13-3
改ページの設定 13-42
カタログ 13-7
共有 13-7
全体のナビゲート 13-23
動的な認可変更 13-2
特定のページの表示 13-23, 13-24
表示 13-21
変更 13-21
レポート項目 13-45
レポート セクション 13-69
レポート デザイン
データの構成 13-43
データの非表示 13-67
保存 13-27
レポート テンプレート 13-29, 13-78
レポート ビューア 13-21
連結演算子 13-61

ろ

ロケール
グラフの作成 13-78
フォーマットのカスタマイズ 13-31, 13-33, 13-36
論理演算子 13-61

わ

ワイルドカード文字 13-59
ワンポイント アドバイス、説明 xxiv

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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/