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 & 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 5.2 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。

この章は、次の内容で構成されています。

管理者ロールおよびアカウントについて

ACS 5.2 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制御が必要ない場合は、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制御を行うには、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 5.2 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.16-6）を参照してください。

（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] ドローアは表示されません。これは、そのドローア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	特権
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] ドローア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 & 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。

表 16-1　事前定義済みのロールの説明（続き）

ロール	特権
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制御が必要ない場合は、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。
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] ドローアで設定された ID は [Users and Identity Stores] ドローアで使用できますが、変更はできません。

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、「別の管理者パスワードのリセット」（P.16-14）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。
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	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	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.16-8）
- 「管理者の認証設定」（P.16-9）

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.16-4）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.16-4）を参照してください。
Permissions List	

表 16-5　[Roles Properties] ページ（続き）

フィールド	説明
Resource	使用できるリソースのリスト。
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.16-9）

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	

表 16-6　[Password Complexity] タブ（続き）

オプション	説明
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。
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。

表 16-7　[Advanced] タブ（続き）

オプション	説明
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.16-8）

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 5.2 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.16-12）
- 「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.16-12）
- 「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.16-12）

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 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 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。

```
access-setting accept-all
```

詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.2*』を参照してください。

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/5.2/command/reference/cli_app_a.html#wp1697683

（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 5.2 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.16-13）
- 「別の管理者パスワードのリセット」（P.16-14）

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/5.2/command/reference/cli_app_a.html#wp1208469

別の管理者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.16-9）
- 「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.16-8）