CHAPTER 5

Cisco ISE の管理

グローバル設定の指定と Cisco ISE で必要な機能の設定には、この章のタスクと参照情報を使用します。

- 「Cisco ISE へのログイン」（P.5-1）
- 「Cisco ISE でのプロキシ設定の指定」（P.5-3）
- 「管理者ポータルで使用されるポート」（P.5-3）
- 「システム時刻と NTP サーバ設定の指定」（P.5-3）
- 「システムの時間帯の変更」（P.5-4）
- 「通知をサポートするように SMTP サーバを設定」（P.5-5）
- 「ソフトウェア パッチのインストール」（P.5-6）
- 「ソフトウェア パッチのロールバック」（P.5-7）
- 「パッチのインストールおよびロールバック変更の表示」（P.5-9）
- 「Cisco ISE での FIPS モードの有効化」（P.5-9）
- 「管理者 CAC 認証のための Cisco ISE の設定」（P.5-11）
- 「Diffie-Hellman アルゴリズムを使用した SSH キー交換の保護」（P.5-13）
- 「コモン クライテリア コンプライアンス対応の安全な Syslog 送信のための Cisco ISE の設定」（P.5-14）

Cisco ISE へのログイン

管理者のユーザ名とパスワードを使用して Cisco ISE にログインします。

ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば *https://<ise hostname or ip address>/admin/*）。

ステップ 2 ユーザ名と、Cisco ISE の初期セットアップで指定して設定した大文字と小文字が区別されるパスワードを入力します。

ステップ 3 [ログイン（Login）] をクリックするか、Enter を押します。

ログインに失敗した場合は、[ログイン（Login）] ページの [ログインで問題が発生する場合（Problem logging in?）] リンクをクリックして、ステップ 2 の説明に従ってください。

関連項目

- 「管理者ログイン ブラウザのサポート」（P.5-2）
- 「ログインの試行に失敗した後の管理者のロックアウト」（P.5-2）
- 管理者のパスワードをリセットする必要がある場合は、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』の「Performing Post-Installation Tasks」の章を参照してください。

管理者ログイン ブラウザのサポート

次のブラウザを使用して Cisco ISE 管理者ポータルにアクセスできます：

- Mozilla Firefox バージョン 5.*x*、8.*x*、9.*x*、14.*x*、15.*x*、18.*x*（Windows、Mac OS X、Linux ベースのオペレーティング システムに適用可能）
- Windows Internet Explorer 8.*x* および 9.*x*（Internet Explorer 8 の互換モード）

コメント Admin Potal は Microsoft IE8 ブラウザの IE7 互換モードでの使用をサポートしていません（Microsoft IE8 は IE8 モードのみがサポートされています）。

クライアント ブラウザを実行しているシステムに、Adobe Flash Player 11.2.0.0 以降がインストールされている必要があります。

管理者ポータルを表示してよりよいユーザ エクスペリエンスを得るために必要な最小画面解像度は、1280 X 800 ピクセルです。

ログインの試行に失敗した後の管理者のロックアウト

管理者ユーザ ID に対して誤ったパスワードを入力した回数が所定の数に達すると、ユーザは「ロックアウト」されて管理者ポータルからシステムにアクセスできなくなり、ログ エントリが [サーバ管理者ログイン（Server Administrator Logins）] レポートに記録され、その管理者 ID のクレデンシャルは一時停止されます。一時停止を解除するには、その管理者 ID に関連付けられたパスワードをリセットする必要があります。手順については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』の「Performing Post-Installation Tasks」の章を参照してください。管理者アカウントを無効にするのに必要な試行失敗回数は、「ユーザ アカウントのカスタム属性およびパスワード ポリシー」（P.14-2）で説明しているガイドラインに従って設定できます。管理者ユーザ アカウントがロックアウトされると、関連付けられた管理者ユーザに電子メールが送信されます。

無効になったシステム管理者のステータスは、Active Directory ユーザを含むすべてのスーパー管理者が有効にできます。

Cisco ISE でのプロキシ設定の指定

既存のネットワーク トポロジにおいて、外部リソース（たとえば、クライアント プロビジョニングやポスチャ関連のリソースが存在するリモート ダウンロード サイト）にアクセスするために、Admin portal に対してプロキシを使用することが要求されている場合は、Cisco ISE ユーザ インターフェイスを使用してプロキシのプロパティを指定できます。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）] を選択します。

ステップ 2　プロキシの IP アドレスまたは DNS 解決可能ホスト名を [プロキシ アドレス（Proxy Address）] に入力し、Cisco ISE との間のプロキシ トラフィックを通過させるポートを [プロキシ ポート（Proxy Port）] で指定します。

ステップ 3　[次のホストとドメインに対するプロキシのバイパス設定（Bypass Proxy Settings for these Hosts & Domain）] に、バイパスするホストまたはドメインの IP アドレスまたはアドレス範囲を入力します。

ステップ 4　該当するフィールドに、プロキシ サーバへの認証に使用するユーザ名とパスワードを入力します。

ステップ 5　[保存（Save）] をクリックします。

次の作業

プロキシ設定の指定が完了した後で、次に示すクライアント プロビジョニング機能をシステム全体で有効化することもできます。

- 「クライアント プロビジョニングの有効化と無効化」（P.22-2）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）

関連項目

- 「リモート クライアントのプロビジョニング リソースをダウンロードできない」（P.G-13）

管理者ポータルで使用されるポート

管理者ポータルは HTTP ポート 80 および HTTPS ポート 443 を使用するように設定され、これらの設定は変更できません。Cisco ISE はまた、あらゆるエンドユーザ ポータルが同じポートを使用することを禁止して、管理者ポータルへのリスクを減らすようになっています。

関連項目

- 「Web ポータルのポート設定」（P.A-56）
- 「エンドユーザ ポータルに対するイーサネット インターフェイスの指定」（P.15-3）

システム時刻と NTP サーバ設定の指定

Cisco ISE では、Network Time Protocol（NTP）サーバを 3 台まで設定することができます。NTP サーバを使用すると、正確な時刻を維持でき、複数の時間帯の間で時刻を同期できます。また、認証済みの NTP サーバのみを Cisco ISE で使用するかどうかを指定することもでき、そのための認証キーを入力できます。

シスコは、すべての Cisco ISE ノードを協定世界時（UTC）の時間帯に設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。この手順では、展開内にあるさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。

はじめる前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

プライマリおよびセカンダリの両方の Cisco ISE ノードがある場合は、セカンダリ ノードのユーザ インターフェイスにログインし、環境内の各 Cisco ISE ノードのシステム時間と NTP サーバ設定を個別に設定する必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [システム タイム（System Time）] を選択します。

ステップ 2　NTP サーバに一意の IP アドレスを入力します。

ステップ 3　システムおよびネットワーク時間の維持に認証済みの NTP サーバだけを使用するように Cisco ISE を制限する場合は、[認証済みの NTP サーバのみ可能（Only allow authenticated NTP servers）] チェックボックスをオンにします。

ステップ 4　指定したサーバのいずれかが認証キーによる認証を必要とする場合は、[NTP 認証キー（NTP Authentication Keys）] タブをクリックし、1 つ以上の認証キーを次のように指定します。

a. [追加（Add）] をクリックします。

b. [キー ID（Key ID）] と [キー値（Key Value）] に必要な値を入力します。そのキーが信頼できる場合は、[信頼できるキー（Trusted Key）] オプションをオンにし、[OK] をクリックします。[キー ID（Key ID）] フィールドは 1 ～ 65535 の数値をサポートし、[キー値（Key Value）] フィールドは最大 15 文字の英数字をサポートします。

c. NTP サーバの認証キーの入力が終了したら、[NTP サーバ設定（NTP Server Configuration）] タブに戻ります。

ステップ 5　[保存（Save）] をクリックします。

関連項目

- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）

システムの時間帯の変更

一度設定すると、管理者ポータルからの時間帯の編集はできません。時間帯設定を変更するには、Cisco ISE CLI で次のコマンドを入力します。

clock timezone *timezone*

注意　インストール後に Cisco ISE アプライアンス上で時間帯を変更すると、そのノード上で Cisco ISE アプリケーションを使用できなくなります。ただし、初期設定ウィザードで時間帯の設定を求めるプロンプトが表示されたら、優先する時間帯（デフォルト UTC）をインストール中に設定できます。

時間帯を変更すると、以下ように別の Cisco ISE ノード タイプに影響します。

スタンドアロンまたはプライマリ ISE ノード

インストールの後の時間帯の変更は、スタンドアロンまたはプライマリ ISE ノードでサポートされていません。ただし誤って時間帯を変更した場合は、次の手順を実行します。

- 時間帯に戻ります。（変更される前の時間帯）。
- そのノードの CLI から application reset-config ise コマンドを実行します。
- そのノードで時間帯が変更される前の、正常な既知の最終バックアップから復元します。

セカンダリ ISE ノード

セカンダリ ノードで時間帯を変更すると、展開に使用できなくなります。プライマリ ノードの時間帯と同じになるようにセカンダリ ノードの時間帯を変更する場合、次の手順を実行します。

- セカンダリ ノードの登録を解除します。
- プライマリ ノードと同じになるように時間帯を修正します。
- そのノードの CLI から application reset-config ise コマンドを実行します。
- プライマリ ノードにセカンダリ ノードとしてノードを再登録します。

clock timezone コマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。

通知をサポートするように SMTP サーバを設定

アラームの電子メール通知を送信し、電子メールまたは Short Message Service（SMS）のテキスト メッセージを使用してスポンサーがゲストに自分のアカウント クレデンシャルを送信できるようにするために、Simple Mail Transfer Protocol（SMTP）サーバをセット アップします。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTP サーバ（SMTP Server）] を選択します。

ステップ 2　[SMTP サーバ（SMTP Server）] フィールドにアウトバウンド SMTP サーバのホスト名を入力します。この SMTP ホスト サーバには Cisco ISE サーバからアクセスできる必要があります。このフィールドの最大長は 60 文字です。

ステップ 3　次のオプションのいずれかを選択します。

- スポンサーの電子メール アドレスからゲスト通知メールを送信するには、[スポンサーの電子メール アドレスを使用（Use email address from Sponsor）] を選択して、[通知の有効化（Enable Notifications）] を選択します。
- すべてのゲスト通知の送信元となる電子メールアドレスを指定するには、[デフォルトの電子メール アドレスを使用（Use Default email address）] を選択して、それを [デフォルトの電子メール アドレス（Default email address）] に入力します。

ステップ 4　[保存（Save）] をクリックします。

アラーム通知の受信者は、[電子メールにシステム アラームを含む（Include system alarms in emails）] オプションが有効になっている内部管理ユーザです。アラーム通知を送信する送信者の電子メール アドレスは、ise@<hostname> としてハード コードされています。

関連項目

- 「ゲスト通知のカスタマイズ」（P.16-9）

- 「アラームの有効化および設定」（P.25-11）
- 「新しい Cisco ISE 管理者の作成」（P.6-2）

ソフトウェア パッチのインストール

展開内の Cisco ISE にパッチをインストールする作業は、プライマリ管理ノードから行うことができます。管理者ポータルからパッチをインストールするには、Cisco.com からクライアント ブラウザを実行しているシステムにパッチをダウンロードします。

（注）　Cisco ISE のパッチをインライン ポスチャ ノードにインストールする作業を実行できるのは、CLI からに限られます。

CLI からパッチをインストールするには、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。

はじめる前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）] > [インストール（Install）] を選択します。

ステップ 2　[参照（Browse）] をクリックし、Cisco.com からダウンロードしたパッチを選択します。

ステップ 3　[インストール（Install）] をクリックしてパッチをインストールします。

プライマリ管理ノードでのパッチのインストールが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

（注）　パッチ インストールの進行中は、[パッチ管理（Patch Management）] ページ上の機能のうち、アクセスできるのは [ノード ステータスを表示（Show Node Status）] のみです。

ステップ 4　ログインして、ダッシュボード ページ下部の [アラーム（Alarms）] リンクをクリックします。

ステップ 5　[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）] を選択して、[パッチのインストール（Patch Installation）] ページに戻ります。

ステップ 6　セカンダリ ノードにインストールしたパッチの横のオプション ボタンをクリックし、[ノード ステータスを表示（Show Node Status）] をクリックしてインストールが完了したことを確認します。

次の作業

1 つ以上のセカンダリ ノードでパッチをインストールする必要がある場合は、ノードが動作中であることを確認して、ステップ 1 からのプロセスを繰り返して残りのノードにパッチをインストールします。

関連項目

- 「Cisco ISE ソフトウェア パッチ」（P.5-7）
- 「ソフトウェア パッチ インストールのガイドライン」（P.5-7）
- 「ソフトウェア パッチのロールバック」（P.5-7）
- 「パッチのインストールおよびロールバック変更の表示」（P.5-9）

• 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）

Cisco ISE ソフトウェア パッチ

通常 Cisco ISE パッチは累積されます。ただし、パッチ インストールの制限事項については、パッチに付属している *「Readme」* で説明されています。Cisco ISE では、パッチのインストールおよびロールバックを CLI または GUI から実行できます。

ソフトウェア パッチ インストールのガイドライン

パッチのインストールまたはロールバックをスタンドアロンまたはプライマリの管理ノードから実行したときは、Cisco ISE によってアプリケーションが再起動されます。再びログインできる状態になるまで、数分かかることがあります。

インストールするパッチが、ネットワーク内に展開されている Cisco ISE のバージョンに適用されるものであることを確認してください。Cisco ISE はパッチ ファイルのバージョンの不一致とあらゆるエラーをレポートします。

Cisco ISE に現在インストールされているパッチよりも低いバージョンのパッチをインストールできません。同様に、あるバージョンのパッチの変更をロールバックしようとしたときに、それよりも高いバージョンのパッチがその時点で Cisco ISE にインストール済みの場合は、ロールバックはできません。たとえば、パッチ 3 が Cisco ISE サーバにインストール済みの場合に、パッチ 1 または 2 をインストールしたり、パッチ 1 または 2 にロールバックすることはできません。

分散展開の一部であるプライマリ管理ノードからパッチのインストールを実行するときは、Cisco ISE によってそのパッチが展開内のプライマリ ノードとすべてのセカンダリ ノードにインストールされます。パッチのインストールがプライマリ ノードで成功すると、Cisco ISE はセカンダリ ノードでパッチのインストールを続行します。プライマリ ノードで失敗した場合は、インストールはセカンダリ ノードに進みません。ただし、何らかの理由でセカンダリ ノードのいずれかでインストールに失敗した場合は、処理が続行され、展開内の次のセカンダリ ノードでインストールが実行されます。パッチがセカンダリ Cisco ISE ノード上にインストールされると、そのノードは続けて再起動されます。パッチをセカンダリ ノードにインストールしている間も、プライマリ ノードの管理タスクの実行を続けることができます。

ソフトウェア パッチのロールバック

分散展開の一部であるプライマリ管理ノードからパッチのロールバックを実行するときは、Cisco ISE によってそのパッチが展開内のプライマリ ノードとすべてのセカンダリ ノードにインストールされます。

はじめる前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）] を選択します。

ステップ 2　変更をロールバックするパッチ バージョンのオプション ボタンをクリックしてから、[ロールバック（Rollback）] をクリックします。

（注） パッチのロールバックの進行中は、[パッチ管理（Patch Management）] ページ上の機能のうち、アクセスできるのは [ノード ステータスを表示（Show Node Status）] のみです。

プライマリ管理ノードからのパッチのロール バックが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

ステップ 3　ログイン後に、ページの一番下にある [アラーム（Alarms）] リンクをクリックしてロールバック操作のステータスを表示します。

ステップ 4　[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）] を選択します。

ステップ 5　パッチのロールバックの進行状況を表示するには、[パッチ管理（Patch Management）] ページでパッチを選択し、[ノード ステータスを表示（Show Node Status）] をクリックします。

ステップ 6　パッチのオプション ボタンをクリックし、すべてのセカンダリ ノード上で [ノード ステータスを表示（Show Node Status）] をクリックして、そのパッチが展開内のすべてのノードからロールバックされたことを確認します。

そのパッチがロールバックされていないセカンダリ ノードがある場合は、そのノードが稼働中であることを確認してから、ステップ 1 以降のプロセスをもう一度実行して残りのノードから変更をロールバックしてください。Cisco ISE は、このバージョンのパッチがインストールされているノードからのみパッチをロールバックします。

関連項目

- 「ソフトウェア パッチ ロールバックのガイドライン」（P.5-8）
- CLI からパッチをロールバックするには、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。
- 「ソフトウェア パッチのインストール」（P.5-6）
- 「パッチのインストールおよびロールバック変更の表示」（P.5-9）
- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）

ソフトウェア パッチ ロールバックのガイドライン

展開の Cisco ISE ノードからパッチをロールバックするには、最初にプライマリ ノードから変更をロールバックします。これに成功すると、セカンダリ ノードからパッチがロールバックされます。プライマリ ノードでロールバック処理が失敗した場合は、セカンダリ ノードからのパッチ ロールバックは行われません。ただし、セカンダリ ノードでパッチが失敗しても、展開内の次のセカンダリ ノードからのパッチのロールバックは継続されます。

Cisco ISE によるセカンダリ ノードからのパッチ ロールバックが進行中のときも、引き続きプライマリ管理ノード GUI から他の作業を実行することができます。セカンダリ ノードは、ロールバック後に再起動されます。

パッチのインストールおよびロールバック変更の表示

Cisco ISE のモニタリングおよびトラブルシューティングのコンポーネントは、指定した期間に Cisco ISE ノードで実施されたパッチのインストールとロールバック操作の情報を提供します。

はじめる前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

ステップ 1　[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [サーバ インスタンス（Server Instance）] を選択します。

ステップ 2　[サーバ操作監査（Server Operations Audit）] オプション ボタンをクリックしてから [実行（Run）] をクリックし、レポートを生成する期間を選択します。

ステップ 3　ページ右上の [Interactive Viewer を起動（Launch Interactive Viewer）] リンクをクリックすると、このレポートのデータの表示、並べ替え、およびフィルタリングを行うことができます。

関連項目

- Cisco ISE ソフトウェア パッチ
- ソフトウェア パッチのインストール
- ソフトウェア パッチのロールバック
- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）
- 「レポートの実行および表示」（P.26-2）

Cisco ISE での FIPS モードの有効化

Cisco ISE ネットワークは、Federal Information Processing Standard（FIPS）140-2 準拠の暗号化と復号化をサポートしています。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [FIPS モード（FIPS Mode）] を選択します。

ステップ 2　[FIPS モード（FIPS Mode）] ドロップダウン リストで [有効（Enabled）] オプションを選択します。

ステップ 3　[保存（Save）] をクリックして、マシンを再起動します。

次の作業

FIPS モードを有効にしたら、次の FIPS 140-2 準拠機能を有効化し設定します。

- 「Cisco ISE へのネットワーク デバイスのインポート」（P.9-4）
- 「自己署名証明書の生成」（P.8-18）
- 「証明書署名要求の生成」（P.8-19）
- 「RADIUS 認証設定」（P.A-40）

さらに、「管理者 CAC 認証のための Cisco ISE の設定」（P.5-11）のガイドラインに従って Common Access Card（CAC）機能を使用して、管理者アカウント許可を有効化することもできます。許可のために CAC 機能を使用することは、厳密には FIPS 140-2 の要件ではありませんが、セキュア アクセスの手法としてよく知られており、多くの環境で FIPS 140-2 準拠を強化するために使用されています。

FIPS モードのサポート

Cisco ISE は、連邦情報処理標準（FIPS）140-2 Common Criteria EAL2 準拠をサポートしています。FIPS 140-2 は暗号モジュールとして使用されている米国政府のコンピュータ セキュリティ標準です。Cisco ISE は、FIPS 140-2 実装ガイダンスのセクション G.5 ガイドラインに従って認可済みの C3M および Cisco ACS NSS モジュールを使用した組み込み FIPS 140-2 実装を使用しています。

FIPS モードを有効にすると、Cisco ISE 管理者インタフェースのページの右上のノード名の左側に FIPS Mode アイコンが表示されます。

FIPS 140-2 レベル 1 標準でサポートされないプロトコルや証明書が検出された場合は、Cisco ISE からの警告にそのプロトコルの名前が表示されます。FIPS モードは、そのプロトコルへの適切な対処が完了するまで有効化されません。

FIPS モードを有効にしたら、展開内の他のすべてのノードを再起動する必要があります。ネットワークの中断を最小限にするために、Cisco ISE は自動的にローリング再起動を実行します。具体的には、最初にプライマリの管理ノードを再起動し、その後でセカンダリ ノードを 1 つずつ再起動します。

ヒント　データベース移行を行う場合は、移行が完了してから FIPS モードを有効にすることを推奨します。

FIPS モードの動作パラメータ

FIPS 標準では特定のアルゴリズムの使用について制限が設けられています。この標準を適用するには、Cisco ISE での FIPS 動作を有効にする必要があります。Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードでは、非 FIPS 準拠のアルゴリズムを使用するすべての機能が失敗するほか、特定の認証機能が無効になります。サポートするプロトコルを含む詳細については、「FIPS 140-2 の実装」（P.1-4）および「Common Access Card 機能のサポート」（P.1-5）を参照してください。

また FIPS モードを有効化すると、Cisco ISE のゲスト ログイン機能に必要な Password Authentication Protocol（PAP）および Challenge Handshake Authentication Protocol（CHAP）プロトコルが自動的に無効化されます。レイヤ 3 ゲスト ログイン実装でのこの問題の対処方法については、第 16 章「ゲストに許可されるネットワーク アクセスのサポート」を参照してください。

FIPS モードが有効のときの Cisco NAC Agent の要件

Cisco NAC Agent は、Cisco ISE ネットワークを検出するために、常に Windows Internet Explorer TLS 1.0 の設定を探します。（この TLS 1.0 設定が Internet Explorer で有効化されている必要があります）。したがって、ネットワークにアクセスするクライアント マシン上で Cisco ISE のポスチャ評価機能を動作させるには、そのマシンに Windows Internet Explorer バージョン 7、8、または 9 がインストールされて TLS1.0 が有効化されている必要があります。Cisco NAC Agent は、Cisco ISE で FIPS モードが有効になっている場合に、自動的に Windows Internet Explorer の TLS 1.0 設定を有効化することができます。

管理者 CAC 認証のための Cisco ISE の設定

はじめる前に

設定を始める前に、次の手順を実行してください：

- （任意）「Cisco ISE での FIPS モードの有効化」（P.5-9）の手順に従って FIPS モードをオンにします。FIPS モードは証明書ベースの認証には必要ありませんが、この 2 つのセキュリティ手段は多くの場合、組み合わせて使用されます。Cisco ISE を FIPS 140-2 準拠の環境に展開する予定があり、CAC 証明書ベース許可も使用する場合は、必ず FIPS モードを有効にするとともに、適切な秘密キーと暗号化/復号化設定を最初に指定してください。
- Cisco ISE のドメイン ネーム サーバ（DNS）が Active Directory に設定されていることを確認します。
- Active Directory のユーザとユーザ グループ メンバーシップが、管理者証明書ごとに定義されていることを確認します。

Cisco ISE による管理者の認証と許可を、ブラウザから送信された CAC ベースのクライアント証明書に基づいて実行できるようにするには、次の設定が完了していることを確認してください。

- 外部 ID ソース（次の例では Active Directory）
- 管理者が属する Active Directory のユーザ グループ
- ユーザのアイデンティティを証明書の中で見つける方法
- Active Directory ユーザ グループから Cisco ISE RBAC 権限へのマッピング
- クライアント証明書に署名する認証局（信頼）証明書
- クライアント証明書がすでに CA によって失効させられたかどうかを判断する方法

Cisco ISE にログインする場合、資格情報を認証するために Common Access Card（CAC）を使用できます。

ステップ 1　「Cisco ISE での FIPS モードの有効化」（P.5-9）の説明のように FIPS モードを有効にします。FIPS モードを有効化すると、システムを再起動するように促されます。CA 証明書もインポートする場合は、再起動を遅らせることができます。

ステップ 2　Cisco ISE の Active Directory アイデンティティ ソースを設定し、「外部 ID ソースとしての Active Directory の設定」（P.14-13）に示されているように Active Directory にすべての Cisco ISE ノードを結合します。

ステップ 3　「証明書認証プロファイルの追加」（P.14-8）のガイドラインに従って証明書認証プロファイルを設定します。

[プリンシパル名 X.509 属性（Principal Name X.509 Attribute）] フィールドでは、証明書内で管理者ユーザ名が格納されている属性を選択します。（CAC カードの場合は、カード上の署名証明書が通常は Active Directory でのユーザの検索に使用されます。プリンシパル名は、この証明書の「サブジェクト代替名」拡張情報の中にあります。具体的には、この拡張情報の「他の名前」というフィールドです。したがって、ここで選択する属性は「Subject Alternative Name - Other Name」となります）。

ユーザの AD レコードにユーザの証明書が格納されている場合に、ブラウザから受信した証明書を AD の証明書と比較するには、[証明書のバイナリ比較（Binary Certificate Comparison）] チェックボックスをオンにして、Active Directory インスタンス名を選択します（で指定したものです）。

ステップ 4　「外部 ID ストアを使用したパスワード ベースの認証の設定」（P.6-18）の説明のように、パスワードベースの管理者認証用に Active Directory を有効化します。Cisco ISE に接続し結合された Active Directory インスタンス名を選択します。

（注） その他の設定が完了するまでは、パスワード ベースの認証を使用します。この手順の最後に、クライアント ベースの認証に認証タイプを変更できます。

ステップ 5 外部管理グループを作成して、Active Directory グループにマッピングします。[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）] を選択します。「外部管理者グループの作成」（P.6-18）の説明のように、外部システム管理者グループを作成します。

ステップ 6 「外部管理者認証用の RBAC ポリシーの作成」（P.6-19）の説明のように、外部管理グループに RBAC 権限を割り当てる管理者認可ポリシーを設定します。

警告 **外部スーパー管理者グループを作成して Active Directory グループにマッピングし、スーパー管理者権限を持つ管理者許可ポリシー（メニュー アクセスおよびデータ アクセス）を設定し、Active Directory グループに少なくとも 1 人のユーザを作成することを強く推奨します。このマッピングにより、クライアント証明書ベースの認証が有効になると、少なくとも 1 人の外部管理者がスーパー管理者権限を持つことが保障されます。これができないと、Cisco ISE 管理者が管理者ポータルの重要な機能から締め出される状況になる可能性があります。**

ステップ 7 [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書ストア（Certificate Store）] を選択して、認証局証明書を Cisco ISE 証明書ストアにインポートします。

Cisco ISE がクライアント証明書を受け入れるには、そのクライアント証明書の信頼チェーンの CA 証明書が Cisco ISE 証明書ストアの中にあることが条件となります。Cisco ISE 証明書ストアには適切な CA 証明書をインポートする必要があります。

a. [参照（Browse）] をクリックして証明書を選択します。

b. [クライアント認証を信頼（Trust for client authentication）] チェックボックスをオンにします。

c. [送信（Submit）] をクリックします。

Cisco ISE は、証明書をインポートしたら展開内のすべてのノードを再起動することを促します。すべての証明書をインポートするまで、再起動を遅らせることができます。ただし、すべての証明書のインポートしたら、次に進む前に Cisco ISE を再起動する必要があります。

ステップ 8 失効ステータス確認のための認証局証明書の設定

a. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [OSCP サービス（OSCP Service）] を選択します。

b. OSCP サーバの名前、説明（任意）、サーバの URL を入力します。

c. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書ストア（Certificate Store）] を選択します。

d. クライアント証明書に署名できる CA 証明書のそれぞれについて、その CA の失効ステータス チェックを行う方法を指定する必要があります。リストから CA 証明書を選択して [編集（Edit）] をクリックします。編集ページで、OCSP または CRL 検証の一方あるいは両方を選択します。OCSP を選択した場合は、CA に使用する OCSP サービスを選択します。CRL を選択した場合は、CRL Distribution URL などの設定パラメータを指定します。詳細については、「「OCSP サービス」（P.8-32）」と「「証明書ストアの証明書の編集」（P.8-29）」を参照してください。

ステップ 9 クライアント証明書ベースの認証の有効化。[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] を選択します。

a. [認証方法（Authentication Method）] タブの [クライアント証明書ベース（Client Certificate Based）] 認証タイプを選択します。

b. 設定済みの証明書認証プロファイルを選択します。

c. Active Directory のインスタンス名を選択します。

d. [保存（Save）] をクリックします。

ここで、パスワード ベースの認証からクライアント ベースの認証に切替えます。設定済みの証明書認証プロファイルにより、管理者による証明書の認証方法を指定します。管理者は外部アイデンティティ ソースにより許可されます。この例では、Active Directory です。

Active Directory での管理者の検索には、証明書認証プロファイルからのプリンシパル名属性が使用されます。

Cisco ISE は、管理者 CAC 認証に設定されています。

関連項目

- 「サポートされる Common Access Card 標準」（P.5-13）
- 「Cisco ISE での共通アクセス カードの動作」（P.5-13）

サポートされる Common Access Card 標準

Cisco ISE は、Common Access Card（CAC）認証デバイスを使用して自身を認証する米国政府ユーザをサポートします。CAC は特定の従業員を識別する一連の X.509 クライアント証明書を含む電子チップの認識票です。CAC によるアクセスには、カードを挿入しピンを入力するカード リーダーが必要です。カードからの証明書が Windows の証明書ストアに転送されます。Windows の証明書ストアは、Cisco ISE などのでローカル ブラウザで実行されているアプリケーションで使用可能です。

Windows Internet Explorer バージョン 8 または 9 を Windows 7 オペレーティング システムで使用している場合は、ActiveIdentity の ActivClient バージョン 6.2.0.133 をインストールする必要があります。このミドルウェアは、Cisco ISE を CAC とともに相互運用するためのサードパーティ製品です。ActiveIdentity のセキュリティ クライアント製品の詳細については、http://www.actividentity.com/products/securityclients/ActivClient/ を参照してください。

Cisco ISE での共通アクセス カードの動作

管理者ポータルは、クライアント証明書を使用してのみ Cisco ISE との認証許可されるように設定できます。ユーザ ID とパスワードなどの証明書ベースの認証はできません。クライアント証明書認証では、共通アクセス カード（CAC）カードを挿入して PIN を入力してから、ブラウザのアドレス フィールドに Cisco ISE 管理者ポータル URL を入力します。ブラウザによって証明書が Cisco ISE に転送され、Cisco ISE はログイン セッションを証明書の内容に基づいて認証および許可します。このプロセスが完了すると、[Cisco ISE モニタリングおよびトラブルシューティング（Cisco ISE Monitoring and Troubleshooting）] ホーム ページに表示され、適切な RBAC 権限が与えられます。

Diffie-Hellman アルゴリズムを使用した SSH キー交換の保護

Diffie-Hellman-Group14-SHA1 SSH キー交換しか許可しないように Cisco ISE を設定することができます。このためには、Cisco ISE の Command-Line Interface（CLI）コンフィギュレーション モードから次のコマンドを入力します。

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

以下は例です。

```
ise/admin# conf t
ise/admin (config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

コモン クライテリア コンプライアンス対応の安全な Syslog 送信のための Cisco ISE の設定

コモン クライテリア（CC）コンプライアンス認証には、Cisco ISE ノード間およびモニタリング ノードに対して Cisco ISE は TLS 保護された安全な syslog だけを送信する必要があります。

はじめる前に

- 展開内のすべての Cisco ISE ノードに適切なサーバ証明書が設定されていることを確認します。FIPS 140-2 準拠にセットアップする場合は、証明書キーは 2,048 ビット以上のキー サイズが必要です。詳細については、第 8 章「証明書の管理」を参照してください。
- 管理者ポータルの FIPS モードを有効にします。詳細については、「Cisco ISE での FIPS モードの有効化」（P.5-9）を参照してください。
- デフォルト ネットワーク アクセス認証ポリシーが、あらゆるバージョンの SSL プロトコルを許可しないことを確認します。FIPS 認定アルゴリズムとともに、FIPS モードで TLS プロトコルを使用します。詳細については、第 19 章「認証ポリシーの管理」を参照してください。
- 展開内のすべてのノードがプライマリ管理ノードに登録されていることを確認します。また、展開の少なくとも 1 ノードにセキュアな syslog レシーバ（TLS サーバ）として動作するようになっている Monitoring ユーザが含まれることを確認します。詳細については、第 3 章「分散環境での Cisco ISE の設定」を参照してください。

Cisco ISE ノード間およびモニタリング ノードに TLS 保護された安全な syslog を送信するように Cisco ISE を設定するには、次の手順を実行します。

1. セキュア syslog リモート ロギング ターゲットを設定します。詳細については、「セキュア syslog リモート ロギング ターゲットの設定」（P.5-14）を参照してください。
2. セキュア syslog リモート ロギング ターゲットに監査可能なイベントを送信するロギング カテゴリを有効にします。詳細については、「ロギング カテゴリのセキュア syslog ターゲットへの監査可能イベント送信の有効化」（P.5-15）を参照してください。
3. TCP syslog および UDP syslog コレクタを無効化します。TLS 保護された syslog コレクタのみを有効化します。詳細については、「TCP syslog および UDP Syslog コレクタの無効化」（P.5-16）を参照してください。

セキュア syslog リモート ロギング ターゲットの設定

Cisco ISE システム ログは、さまざまな目的のために、ログ コレクタによって収集され保存されます。セキュア syslog ターゲットを設定するためには、ログ コレクタとして Cisco ISE モニタリング ノードを選択する必要があります。

ステップ 1　管理者ポータルにログインします。

ステップ 2　[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）] を選択します。

ステップ 3　[追加（Add）] をクリックします。

ステップ 4　セキュア syslog サーバの名前を入力します。

ステップ 5　[ターゲット タイプ（Target Type）] ドロップダウン リストからセキュア syslog を選択します。

ステップ 6　[ステータス（Status）] ドロップダウン リストで [有効化（Enabled）] を選択します。

ステップ 7　展開の Cisco ISE モニタリング ノードの IP アドレスを入力します。

ステップ 8　ポート番号として 6514 を入力します。セキュアな syslog レシーバは TCP ポート 6514 で受信します。

ステップ 9　syslog ファシリティ コードを選択します。デフォルト値は LOCAL6 です。

ステップ 10　最大長を入力します。デフォルトは 8192 です。

ステップ 11　リモートのセキュア syslog ロギング ターゲットが Cisco ISE ノードでない場合は、アラームが syslog サーバに送信されるように [このターゲットのアラームを含める（Include Alarms for this Target）] チェックボックスをオンにします。

セキュア syslog ロギングのターゲットとして Cisco ISE ノード（モニタリング）を設定した場合は、[このターゲットのアラームを含める（Include Alarms for this Target）] チェックボックスをオフにします。

ステップ 12　[サーバ ダウンの場合はバッファ メッセージ（Buffer Messages When Server is Down）] チェックボックスをオンにします。このオプションがオンの場合、Cisco ISE は、セキュア syslog レシーバが到達不能な場合にはログを格納し、セキュア syslog レシーバを定期的に検査し、セキュア syslog レシーバが起動すると転送します。

a.　バッファ サイズを入力します。

b.　定期的にセキュア syslog レシーバを検査するように、Cisco ISE の再接続タイムアウトを秒単位で入力します。

ステップ 13　Cisco ISE がセキュア syslog サーバに提示する CA 証明書を選択します。

ステップ 14　[サーバ証明書有効性を無視（Ignore Server Certificate validation）] チェックボックスをオフにします。このオプションをオンにしてはいけません。

ステップ 15　[送信（Submit）] をクリックします。

ロギング カテゴリのセキュア syslog ターゲットへの監査可能イベント送信の有効化

Cisco ISE がセキュア syslog ターゲットに監査可能イベントを送信できるように、ロギング カテゴリを有効化する必要があります。

ステップ 1　管理者ポータルにログインします。

ステップ 2　[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択します。

ステップ 3　AAA 監査ロギング カテゴリの横にあるオプション ボタンをクリックし、次に [編集（Edit）] をクリックします。

ステップ 4　[ログ重大度レベル（Log Severity Level）] ドロップダウン リストから [警告（WARN）] を選択します。

ステップ 5　作成済みのセキュア syslog リモート ロギング ターゲットを、選択したボックスに移動します。

ステップ 6　[保存（Save）] をクリックします。

ステップ 7　次のロギング カテゴリを有効にする場合は、この手順を繰り返し行います。

- Administrative and Operational Audit
- Posture and Client Provisioning Audit

TCP syslog および UDP Syslog コレクタの無効化

コモン クライテリア準拠のためには、TCP および UDP syslog コレクタを無効化して、セキュア syslog コレクタのみを有効にする必要があります。

ステップ 1　管理者ポータルにログインします。

ステップ 2　[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）] を選択します。

ステップ 3　TCP または UDP syslog コレクタの横にあるオプション ボタンをクリックします。

ステップ 4　[編集（Edit）] をクリックします。

ステップ 5　[ステータス（Status）] ドロップダウン リストから [無効化（Disabled）] を選択します。

ステップ 6　[保存（Save）] をクリックします。

ステップ 7　すべての TCP または UDP syslog コレクタが無効になるまで、このプロセスを繰り返します。