CHAPTER 3

Cisco ISE Task Navigator

この章では、Cisco Identity Service Engine（ISE）の Task Navigator について説明します。次のトピックを扱います。

複数の作業手順のナビゲート

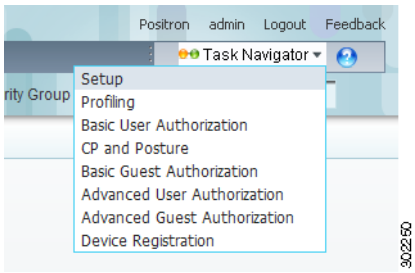
Task Navigator は、複数のユーザ インターフェイス ページに及ぶ Cisco ISE の管理および設定プロセス全体に、ビジュアル パスを提供します。Task Navigator の直線表示は、作業を完了させる順序の概要を示し、同時に、作業を実行するページへの直接リンクも提供します。

（注） Task Navigator では、完了した作業に関する情報は保持されません。これはビジュアル ガイドであり、ユーザ インターフェイス ページに直接移動して関連作業を実行できます。

Task Navigator のメニュー

Task Navigator のメニューは、Cisco ISE ウィンドウの右上隅に表示されます。

図 3-1　Task Navigator のメニュー



Task Navigator の起動と使用

Task Navigator のそれぞれのオプションによってポップアップ ダイアログが表示され、作業のリストが一列に並んで示されます。作業は、左から右に、実行が必要な順序に整列されています。

Task Navigator を起動して使用するには、次の手順を実行します。

ステップ 1　[Task Navigator] メニューを右クリックし、ドロップダウン メニューから次のいずれかのオプションを選択します。

- [セットアップ（Setup）]：Cisco ISE セットアップ プロセスの最初の部分を実行します。
- [プロファイリング（Profiling）]：エンドポイントをプロファイルします。
- [基本ユーザ許可（Basic User Authorization）]：基本的なユーザ許可を設定します。
- [クライアント プロビジョニングとポスチャ（Client Provisioning and Posture）]：クライアント プロビジョニングとポスチャを設定します。
- [基本ゲスト許可（Basic Guest Authorization）]：基本的なゲスト許可を設定します。
- [拡張ユーザ許可（Advanced User Authorization）]：クライアント プロビジョニングおよびポスチャと一緒にユーザ許可を設定します。
- [拡張ゲスト許可（Advanced Guest Authorization）]：クライアント プロビジョニングおよびポスチャと一緒にゲスト許可を設定します。

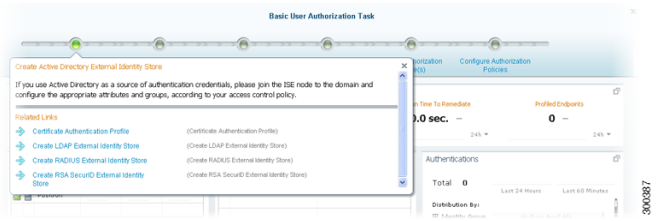
選択した Task Navigator がウィンドウの上部に表示されます。

ステップ 2　左から右に、表示されている順序で作業を完了します。

（注）　Task Navigator では、完了した作業に関する情報は保持されません。これはビジュアル ガイドであり、ユーザ インターフェイス ページに直接移動して関連作業を実行できます。

ステップ 3　作業の情報を表示するには、作業項目の点の上にマウス カーソルを移動します。クイック ビュー ダイアログが表示されます。

図 3-2　基本ユーザ許可の作業



ステップ 4　作業を開始するには、オプション ボタン アイコンをクリックします。ページが切り替わり、その作業を開始できる画面に直接移動します。

ステップ 5　ナビゲーション パスの最後の作業が完了すると、ダイアログが閉じます。

次の手順

Task Navigator のそれぞれのオプションについては、この章の他の項を参照してください。

セットアップ（Setup）

表 3-1 に、Cisco ISE ネットワークをセットアップするために実行する最初の作業を示します。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-1　セットアップの作業マップ

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. 管理者パスワード ポリシー	Cisco ISE 管理者のパスワード ポリシーを確認して、会社のセキュリティ ポリシーに従っていることを確認します。	[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [パスワード ポリシー（Password Policy）]	「管理者アカウントのパスワード ポリシーの設定」（P.4-67）
2. ネットワーク アクセス パスワード ポリシー	ネットワーク アクセスを要求している内部ユーザのパスワード ポリシーを確認して、会社のセキュリティ ポリシーに従っていることを確認します。	[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザ パスワード ポリシー（User Password Policy）]	「ネットワーク アクセス ユーザ アカウントのユーザ パスワード ポリシーの設定」（P.4-73）
3. ゲスト アクセス パスワード ポリシー	ネットワーク アクセスを要求している内部ユーザのパスワード ポリシーを確認して、会社のセキュリティ ポリシーに従っていることを確認します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [パスワード ポリシー（Password Policy）]	「ゲスト パスワード ポリシーの設定」（P.21-71）

表 3-1　セットアップの作業マップ （続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
4. ライセンシング	購入した製品の正しいライセンシングを所有していることを確認します。	[管理（Administration）] > [システム（System）] > [ライセンシング（Licensing）] > [現在のライセンス（Current Licenses）]	「ライセンスの追加およびアップグレード」（P.12-3）
5. 時刻	システム時刻、日付、および NTP を設定および確認します。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [システム時刻（System Time）]	「システム時刻と NTP サーバの設定」（P.8-18）
6. プロキシ	Cisco ISE ノードが更新のために外部と通信できるように、適切なプロキシ サーバの設定を行います。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）]	「Cisco ISE でのプロキシ設定の指定」（P.8-17）
7. 証明書署名要求	証明書署名要求（CSR）を作成します。	[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [ローカル証明書（Local Certificates）]	「証明書署名要求の生成」（P.13-9）
8. 証明書署名要求のエクスポート	会社の適切な認証局（CA）に送信される CSR をエクスポートします。	[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]	「証明書署名要求の表示およびエクスポート」（P.13-16）
9. 認証局証明書	ノード間通信、Cisco ISE 管理、およびクライアント認証の信頼性を確立するために必要な CA 証明書をインポートします。	[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局証明書 (Certificate Authority Certificates）]	「認証局証明書の追加」（P.13-19）
10. 電子メール設定のモニタリングおよびトラブルシューティング	適切な運用チームにアラームを送信できるように、正しいシンプル メール転送プロトコル（SMTP）サーバを設定します。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [モニタリング（Monitoring）] > [電子メール設定（Email Settings）]	「電子メール設定の指定」（P.8-20）
11. システム アラーム設定のモニタリングおよびトラブルシューティング	運用要件を満たすように必要なアラームを設定します。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [モニタリング（Monitoring）] > [システム アラーム設定（System Alarm Settings）]	「システム アラーム設定の指定」（P.8-21）
12. システム ロギング設定	環境に適したイベント管理操作を保証するために、ロギング機能を設定します。	[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ローカル ログ設定（Local Log Settings）]	第 14 章「ロギング」

表 3-1　セットアップの作業マップ （続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
13. スケジュール バックアップ	データ リカバリ ポリシーに基づいた自動バックアップ スケジュールを設定します。	[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [データ管理（Data Management）] > [管理ノード（Administration Node）] > [スケジュール バックアップ（Scheduled Backup）]	「バックアップのスケジュール作成」（P.15-7）
14. 分散展開	インストール環境内の Cisco ISE ノードの数、タイプ、および同期ステータスが適切であることを確認します。	[管理（Administration）] > [システム（System）] > [展開（Deployment）]	• 展開内のノードを設定するには、次の各項を参照してください。 – 「Cisco ISE ノードの設定」（P.9-7） – 「セカンダリ ノードの登録および設定」（P.9-13） • 展開内のノードの同期ステータスを確認するには、「分散環境でのプライマリ ノードとセカンダリ ノードの同期」（P.15-13）を参照してください。

プロファイリング（Profiling）

表 3-2 に、エンドポイントのプロファイリングを設定するために実行する作業を示します。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-2　Task Navigator : [プロファイリング（Profiling）]

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. ノード センサーの設定	展開内の各 Cisco ISE ノードを調べ、すべてのノードが適切に設定されているかどうかが、プロファイリング センサーによってプローブされていることを確認します。	[管理（Administration）] > [システム（System）] > [展開（Deployment）] >（ノードを選択）> [編集（Edit）] > [プロファイリング設定（Profiling Configuration）]	「プローブの設定」（P.18-14）
2. プロファイラ条件の確認 / 作成	プロファイリング要件のプロファイラ条件を確認するか、または新しいプロファイラ条件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [プロファイリング（Profiling）] > [条件（Conditions）]	「プロファイリング条件の作成」（P.18-60）
3. プロファイラ ポリシーの確認 / 作成	プロファイラ ポリシーを確認するか、またはプロファイラ条件を使用してプロファイラ ポリシーを作成します。	[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング ポリシー（Profiling Policies）] > [エンドポイント ポリシー（Endpoint Policies）]	「エンドポイント プロファイリング ポリシーの作成」（P.18-44）
4. ダウンロード可能 ACL の作成[1]	セキュリティの設定に適したダウンロード可能 ACL を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）]> [DACL 管理（DACL Management）] > [追加（Add）]	「DACL の設定」（P.17-35）
5. 許可プロファイルの作成	展開およびセキュリティ ポリシーに使用する、権限のタイプに基づく許可プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）] > [標準許可プロファイル（Standard Authorization Profiles）] > [追加（Add）]	「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）
6. プロファイリングされたエンドポイントの許可ルールの作成	使用環境に関連しているプロファイリングされたエンドポイントの許可ルールを作成します。	[ポリシー（Policy）] > [許可（Authorization）] > [標準（Standard）]	「許可ポリシーについて」（P.17-1）

1. ダウンロード可能なアクセス コントロール リスト（ACL）

基本ユーザ許可（Basic User Authorization）

基本ユーザ許可の設定プロセスでは、ユーザ インターフェイスの複数のページを使用する必要があります。表 3-3 に実行する作業を示します。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-3　Task Navigator : [基本ユーザ許可（Basic User Authorization）]

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. Active Directory の外部 ID ストアの作成	Active Directory を認証クレデンシャルのソースとして使用する場合は、Cisco ISE ノードをドメインに追加し、アクセス コントロール ポリシーに従って適切な属性とグループを設定します。	[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]	「ISE と Active Directory の統合」（P.5-6）
2. ID ソース順序の作成	前の作業で作成した外部 ID ストアに基づく ID ソース順序を作成します。	[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]	「ID ソース順序の作成」（P.5-54）
3. 認証ポリシーの確認	作業 2 で作成した新規 ID ソース順序を含むように認証ポリシーを作成または変更します。	[ポリシー（Policy）] > [認証（Authentication）]	• 単純な認証ポリシーについては、「単純な認証ポリシーの設定」（P.16-30）を参照してください。 • ルールベースの認証ポリシーについては、「ルールベースの認証ポリシーの設定」（P.16-32）を参照してください。
4. ダウンロード可能 ACL の作成	必要に応じて、セキュリティの設定に適したダウンロード可能 ACL を作成します。	[ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）]	「新しい DACL の権限の作成および設定」（P.17-35）
5. 許可プロファイルの作成	展開およびセキュリティ ポリシーに使用する、権限のタイプに基づく許可プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [標準許可プロファイル（Standard Authorization Profiles）]	「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）
6. 許可ポリシーの作成	実装に適したアクセス権限を付与する許可ポリシーを作成します。	[ポリシー（Policy）] > [許可（Authorization）]	「新しい許可ポリシーの作成」（P.17-15）

クライアント プロビジョニングとポスチャ（Client Provisioning and Posture）

表 3-4 に、クライアント プロビジョニングとポスチャを設定するために実行する作業を示します。ログインしてポスチャに成功した後、このフローには含まれない利用規定および再評価で、ポスチャの追加作業を実行することが必要になる場合もあります。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-4　Task Navigator : [クライアント プロビジョニングとポスチャ（Client Provisioning and Posture）]

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. ポスチャ更新 URL の設定	初期コンプライアンス モジュール ダウンロード（ポスチャ更新）には、初めての場合 15 ～ 20 分かかります。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]	Web およびオフラインでポスチャ更新については、「ポスチャ更新」（P.20-24）を参照してください。
2. クライアント プロビジョニングの設定	クライアント プロビジョニングの更新フィード URL を設定します。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）]	「グローバル クライアント プロビジョニング機能の設定」（P.19-29）
3. クライアント プロビジョニング リソースの手動ダウンロードとエージェント プロファイルの作成	ローカル リソースとリモート リソースから追加できるクライアント プロビジョニング リソースをダウンロードします。 ローカル リソースとリモート リソースから追加できるクライアント プロビジョニング エージェント プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）]	• クライアント プロビジョニング リソースのダウンロードについては、「Cisco ISE へのクライアント プロビジョニング リソースの追加」（P.19-5）を参照してください。 • クライアント プロビジョニング エージェント プロファイルの作成については、「エージェント プロファイルの作成」（P.19-12）を参照してください。
4. クライアント プロビジョニング ポリシーの作成	ID グループとオペレーティング システムに基づくクライアント プロビジョニング ポリシーを作成します。	[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]	「クライアント プロビジョニング リソース ポリシーの設定」（P.19-32）
5. ポスチャ条件の確認 / 作成	コンプライアンス モジュール更新（ポスチャ更新）が完全にダウンロードされ、事前定義された単純条件がダウンロードされた Cisco ISE 上の場所にインストールされていることを確認します。 必要に応じてポスチャの単純条件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]	ポスチャの単純条件を作成するには、次の各項を参照してください。 • 「ファイル条件」（P.20-48） • 「レジストリ条件」（P.20-60） • 「アプリケーション条件」（P.20-74） • 「サービス条件」（P.20-80）

表 3-4　Task Navigator : [クライアント プロビジョニングとポスチャ（Client Provisioning and Posture）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
6. ポスチャ複合条件の確認 / 作成	コンプライアンス モジュール更新（ポスチャ更新）が完全にダウンロードされ、事前定義された複合条件およびアンチウイルスとアンチスパイウェアのサポート表更新がダウンロードされた Cisco ISE 上の場所にインストールされていることを確認します。 すでに作成されているポスチャの単純条件を使用して、ポスチャの複合条件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]	ポスチャの複合条件を作成するには、次の各項を参照してください。 • 「複合条件」（P.20-87） • 「アンチウイルス複合条件」（P.20-96） • 「アンチスパイウェア複合条件」（P.20-103）
7. 修復アクションの作成	アルファベット順に表示される修復アクションを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）]	修復アクションを作成するには、「カスタム ポスチャ修復アクションの設定」（P.20-125）を参照してください。
8. ポスチャ要件の確認 / 作成	ポスチャの単純条件または複合条件を使用して、ポスチャ要件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]	「クライアント ポスチャ評価の要件」（P.20-165）
9. ポスチャ ポリシーの確認 / 作成	ポスチャ要件を使用してポスチャ ポリシーを作成します。	[ポリシー（Policy）] > [ポスチャ（Posture）]	「クライアント ポスチャ評価ポリシー」（P.20-36）

基本ゲスト許可（Basic Guest Authorization）

表 3-5 に、ゲストの基本的な許可を設定するために実行する作業を示します。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-5　Task Navigator : [基本ゲスト許可（Basic Guest Authorization）]

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. Active Directory の外部 ID ストアの作成	Active Directory を認証クレデンシャルのソースとして使用する場合は、Cisco ISE ノードをドメインに追加し、アクセス コントロール ポリシーに従って適切な属性とグループを設定します。 この作業では、Active Directory の設定によって、エンドポイントが正しく機能していない状況やサポートされていない状況で、従業員がゲスト ポータルを使用してネットワーク アクセスを行うことが許可されます。	[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]	「ISE と Active Directory の統合」（P.5-6）
2. ID ソース順序の作成	必要に応じて、前の作業で作成した外部 ID ストアに基づく ID ソース順序を作成します。	[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]	「ID ソース順序の作成」（P.5-54）
3. ゲストの設定	ゲスト要件に従ってゲストの設定を行います。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータル設定（Multi-portal Configurations）]	「マルチポータルの設定」（P.21-50）
4. セルフサービス ゲストの設定	作業 3 の設定で [セルフサービスの許可（allow for self-service）] を選択した場合は、セルフサービス ゲストの設定を行います。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal policy）]	「ゲスト ポータル ポリシーの設定」（P.21-70）
5. 時間プロファイルの作成	ゲストの時間プロファイルを作成します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [時間プロファイル（Time profiles）]	「時間プロファイル」（P.21-72）

表 3-5　Task Navigator : [基本ゲスト許可（Basic Guest Authorization）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
6. スポンサー認証 ID 順序の設定	スポンサー認証ソースを指定します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [スポンサー（Sponsor）] > [認証ソース（Authentication source）]	「認証ソースの指定」（P.21-30）
7. ゲスト スポンサー グループの作成	スポンサー ログイン用のゲスト スポンサー グループを作成します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [スポンサー グループ（Sponsor Groups）]	「スポンサー グループ」（P.21-21）
8. スポンサー ポリシーの作成	ゲスト スポンサー ログイン ポリシーを作成します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [スポンサー グループ ポリシー（Sponsor Group Policy）]	「スポンサー グループ ポリシー」（P.21-17）

拡張ユーザ許可（Advanced User Authorization）

表 3-6 に、ユーザの許可をさらに拡張するために実行する作業を示します。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-6　Task Navigator : [拡張ユーザ許可（Advanced User Authorization）]

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. Active Directory の外部 ID ストアの作成	Active Directory を認証クレデンシャルのソースとして使用する場合は、Cisco ISE ノードをドメインに追加し、アクセス コントロール ポリシーに従って適切な属性とグループを設定します。 内部ゲスト ユーザには、Active Directory ID ストア設定は必要ありません。	[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]	「ISE と Active Directory の統合」（P.5-6）
2. ID ソース順序の作成	必要に応じて、前の作業で作成した外部 ID ストアに基づく ID ソース順序を作成します。	[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]	「ID ソース順序の作成」（P.5-54）

表 3-6　Task Navigator : [拡張ユーザ許可（Advanced User Authorization）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
3. 認証ポリシーの確認	前の作業で作成した新規 ID ソース順序を含むように認証ポリシーを作成または変更します。	[ポリシー（Policy）] > [認証（Authentication）]	• 単純な認証ポリシーについては、「単純な認証ポリシーの設定」（P.16-30）を参照してください。 • ルールベースの認証ポリシーについては、「ルールベースの認証ポリシーの設定」（P.16-32）を参照してください。
4. ポスチャ更新 URL の設定	初期コンプライアンス モジュール ダウンロード（ポスチャ更新）には、初めての場合 15 ～ 20 分かかります。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]	Web およびオフラインでポスチャ更新については、「ポスチャ更新」（P.20-24）を参照してください。
5. クライアント プロビジョニングの設定	クライアント プロビジョニングの更新フィード URL を設定します。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）]	「グローバル クライアント プロビジョニング機能の設定」（P.19-29）
6. 手動クライアント プロビジョニング リソース	ローカル リソースとリモート リソースから追加できるクライアント プロビジョニング リソースをダウンロードします。 ローカル リソースとリモート リソースから追加できるクライアント プロビジョニング エージェント プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）]	• クライアント プロビジョニング リソースのダウンロードについては、「Cisco ISE へのクライアント プロビジョニング リソースの追加」（P.19-5）を参照してください。 • クライアント プロビジョニング エージェント プロファイルの作成については、「エージェント プロファイルの作成」（P.19-12）を参照してください。
7. クライアント プロビジョニング ポリシーの作成	ID グループとオペレーティング システムに基づくクライアント プロビジョニング ポリシーを作成します。	[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]	「クライアント プロビジョニング リソース ポリシーの設定」（P.19-32）

表 3-6　Task Navigator : [拡張ユーザ許可（Advanced User Authorization）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
8. ポスチャ条件の確認 / 作成	コンプライアンス モジュール更新（ポスチャ更新）が完全にダウンロードされ、事前定義された単純条件がダウンロードされた Cisco ISE 上の場所にインストールされていることを確認します。 必要に応じてポスチャの単純条件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]	ポスチャの単純条件を作成するには、次の各項を参照してください。 • 「ファイル条件」（P.20-48） • 「レジストリ条件」（P.20-60） • 「アプリケーション条件」（P.20-74） • 「サービス条件」（P.20-80）
9. ポスチャ複合条件の確認 / 作成	コンプライアンス モジュール更新（ポスチャ更新）が完全にダウンロードされ、事前定義された複合条件およびアンチウイルスとアンチスパイウェアのサポート表更新がダウンロードされた Cisco ISE 上の場所にインストールされていることを確認します。 すでに作成されているポスチャの単純条件を使用して、ポスチャの複合条件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]	ポスチャの複合条件を作成するには、次の各項を参照してください。 • 「複合条件」（P.20-87） • 「アンチウイルス複合条件」（P.20-96） • 「アンチスパイウェア複合条件」（P.20-103）
10. 修復アクションの作成	アルファベット順に表示される修復アクションを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）]	修復アクションを作成するには、「カスタム ポスチャ修復アクションの設定」（P.20-125）を参照してください。
11. ポスチャ要件の確認 / 作成	ポスチャの単純条件または複合条件を使用して、ポスチャ要件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]	「クライアント ポスチャ評価の要件」（P.20-165）
12. ポスチャ ポリシーの確認 / 作成	ポスチャ要件を使用してポスチャ ポリシーを作成します。	[ポリシー（Policy）] > [ポスチャ（Posture）]	「クライアント ポスチャ評価ポリシー」（P.20-36）
13. ダウンロード可能 ACL の作成	必要に応じて、設定したセキュリティに適したダウンロード可能 ACL を作成します。	[ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）]	「新しい DACL の権限の作成および設定」（P.17-35）

表 3-6　Task Navigator : [拡張ユーザ許可（Advanced User Authorization）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
14. 許可プロファイルの作成	展開およびセキュリティ ポリシーに適用する、権限のタイプに基づく許可プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [標準許可プロファイル（Standard Authorization Profiles）]	「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）
15. 許可ポリシー	適切なアクセス権限を付与する許可ポリシーを作成します。各ルールの条件か属性、またはその両方を選択して、ネットワーク全体のアクセス ポリシーを作成します。 pre-posture および post-posture 許可ポリシーを作成します。	[ポリシー（Policy）] > [許可（Authorization）]	「新しい許可ポリシーの作成」（P.17-15）

拡張ゲスト許可（Advanced Guest Authorization）

表 3-7 に、ゲストの許可をさらに拡張するために実行する作業を示します。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-7　Task Navigator : [拡張ゲスト許可（Advanced Guest Authorization）]

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. Active Directory の外部 ID ストアの作成	Active Directory を認証クレデンシャルのソースとして使用する場合は、Cisco ISE ノードをドメインに追加し、アクセス コントロール ポリシーに従って適切な属性とグループを設定します。	[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]	「ISE と Active Directory の統合」（P.5-6）
2. ID ソース順序の作成	要件に従って、作業 1 で作成した外部 ID ストアに基づく ID ソース順序を作成します。	[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]	「ID ソース順序の作成」（P.5-54）
3. ゲストの設定	ゲスト要件に従ってゲストの設定を行います。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータル設定（Multi-portal Configuration）]	「マルチポータルの設定」（P.21-50）

表 3-7　Task Navigator : [拡張ゲスト許可（Advanced Guest Authorization）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
4. セルフサービス ゲストの設定	作業 3 で [セルフサービスの許可（allow for self-service）] を選択した場合は、セルフサービスゲストの設定を行います。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）]	「ゲスト ポータル ポリシーの設定」（P.21-70）
5. 時間プロファイルの作成	ゲストの時間プロファイルを作成します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [時間プロファイル（Time Profiles）]	「時間プロファイル」（P.21-72）
6. スポンサー認証 ID 順序の設定	スポンサー認証ソースを指定します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [スポンサー（Sponsor）] > [認証ソース（Authentication Source）]	「認証ソースの指定」（P.21-30）
7. ゲスト スポンサー グループの作成	スポンサー ログイン用のゲスト スポンサー グループを作成します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [スポンサー グループ（Sponsor Groups）]	「スポンサー グループ」（P.21-21）
8. スポンサー ポリシーの作成	ゲスト スポンサー ログイン ポリシーを作成します。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [スポンサー グループ ポリシー（Sponsor Group Policy）]	「スポンサー グループ ポリシー」（P.21-17）
9. 認証ポリシーの確認	作業 8 で作成した新規 ID ソース順序を含むように認証ポリシーを作成または変更します。	[ポリシー（Policy）] > [認証（Authentication）]	• 単純な認証ポリシーについては、「単純な認証ポリシーの設定」（P.16-30）を参照してください。 • ルールベースの認証ポリシーについては、「ルールベースの認証ポリシーの設定」（P.16-32）を参照してください。
10. ポスチャ更新 URL の設定	初期コンプライアンス モジュール ダウンロード（ポスチャ更新）には、初めての場合 15 ～ 20 分かかります。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]	Web およびオフラインでポスチャ更新については、「ポスチャ更新」（P.20-24）を参照してください。

表 3-7　Task Navigator : [拡張ゲスト許可（Advanced Guest Authorization）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
11. クライアント プロビジョニングの設定	クライアント プロビジョニングの更新フィード URL を設定します。	[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）]	「グローバル クライアント プロビジョニング機能の設定」（P.19-29）
12. 手動クライアント プロビジョニング リソース	ローカル リソースとリモート リソースから追加できるクライアント プロビジョニング リソースをダウンロードします。 ローカル リソースとリモート リソースから追加できるクライアント プロビジョニング エージェント プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）]	• クライアント プロビジョニング リソースのダウンロードについては、「Cisco ISE へのクライアント プロビジョニング リソースの追加」（P.19-5）を参照してください。 • クライアント プロビジョニング エージェント プロファイルの作成については、「エージェント プロファイルの作成」（P.19-12）を参照してください。
13. クライアント プロビジョニング ポリシーの作成	ID グループとオペレーティング システムに基づくクライアント プロビジョニング ポリシーを作成します。	[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]	「クライアント プロビジョニング リソース ポリシーの設定」（P.19-32）
14. ポスチャ条件の確認 / 作成	コンプライアンス モジュール更新（ポスチャ更新）が完全にダウンロードされ、事前定義された単純条件がダウンロードされた Cisco ISE 上の場所にインストールされていることを確認します。 必要に応じてポスチャの単純条件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]	ポスチャの単純条件を作成するには、次の各項を参照してください。 • 「ファイル条件」（P.20-48） • 「レジストリ条件」（P.20-60） • 「アプリケーション条件」（P.20-74） • 「サービス条件」（P.20-80）
15. ポスチャ複合条件の確認 / 作成	コンプライアンス モジュール更新（ポスチャ更新）が完全にダウンロードされ、事前定義された複合条件およびアンチウイルスとアンチスパイウェアのサポート表更新がダウンロードされた Cisco ISE 上の場所にインストールされていることを確認します。 すでに作成されているポスチャの単純条件を使用して、ポスチャの複合条件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]	ポスチャの複合条件を作成するには、次の各項を参照してください。 • 「複合条件」（P.20-87） • 「アンチウイルス複合条件」（P.20-96） • 「アンチスパイウェア複合条件」（P.20-103）

表 3-7　Task Navigator : [拡張ゲスト許可（Advanced Guest Authorization）]（続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
16. 修復アクションの作成	アルファベット順に表示される修復アクションを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）]	修復アクションを作成するには、「カスタム ポスチャ修復アクションの設定」（P.20-125）を参照してください。
17. ポスチャ要件の確認 / 作成	ポスチャの単純条件または複合条件を使用して、ポスチャ要件を作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]	「クライアント ポスチャ評価の要件」（P.20-165）
18. ポスチャ ポリシーの確認 / 作成	ポスチャ要件を使用してポスチャ ポリシーを作成します。	[ポリシー（Policy）] > [ポスチャ（Posture）]	「クライアント ポスチャ評価ポリシー」（P.20-36）
19. ダウンロード可能 ACL の作成	設定したセキュリティの必要に応じて、適切なダウンロード可能 ACL を作成します。	[ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）]	「新しい DACL の権限の作成および設定」（P.17-35）
20. 許可プロファイルの作成	展開およびセキュリティ ポリシーに適用する、権限のタイプに基づく許可プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [標準許可プロファイル（Standard Authorization Profiles）]	「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）
21. 許可ポリシー	適切なアクセス権限を付与する許可ポリシーを作成します。各ルールの条件と属性を選択して、ネットワーク全体のアクセス ポリシーを作成します。 pre-posture および post-posture 許可ポリシーを作成します。	[ポリシー（Policy）] > [許可（Authorization）]	「新しい許可ポリシーの作成」（P.17-15）

デバイスの登録（Device Registration）

表 3-8 に、ユーザ デバイスを登録するために実行する作業を示します。便宜上、作業に関する詳細情報へのリンクが用意されています。

表 3-8　Task Navigator : [デバイスの登録（Device Registration）]

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
1. 必要なネットワーク デバイスの追加またはインポート。	適切なネットワーク プロビジョニングの提供に必要な環境内の他のネットワーク デバイスが、Cisco ISE で認識されるようにします。	[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]	「デバイスの追加と編集」（P.6-3）
2. Active Directory の外部 ID ストアの作成。	Active Directory を認証クレデンシャルのソースとして使用する場合は、Cisco ISE ノードをドメインに追加し、アクセス コントロール ポリシーに従って適切な属性とグループを設定します。	[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]	「ISE と Active Directory の統合」（P.5-6）
3. ID ソース順序の作成。	要件に従って、作業 2 で作成した外部 ID ストアに基づく ID ソース順序を作成します。	[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]	「ID ソース順序の作成」（P.5-54）
4. ダウンロード可能 ACL の作成。	設定したセキュリティの必要に応じて、適切なダウンロード可能 ACL を作成します。	[ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）]	「新しい DACL の権限の作成および設定」（P.17-35）
5. 許可プロファイルの作成。	展開およびセキュリティ ポリシーに適用する、権限のタイプに基づく許可プロファイルを作成します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [標準許可プロファイル（Standard Authorization Profiles）]	「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）
6. サプリカント プロビジョニング ウィザードのダウンロードとサプリカント プロビジョニング プロファイルの作成。	ネットワークにアクセスするリモート ユーザが自身のアクセス デバイスを使用できるように Cisco ISE を設定します。	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]	• 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.19-5） • 「ネイティブ サプリカント プロファイルの作成」（P.19-25）
7. クライアント プロビジョニング ポリシーの作成。	ID グループとオペレーティング システムに基づくクライアント プロビジョニング ポリシーを作成します。	[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]	「クライアント プロビジョニング リソース ポリシーの設定」（P.19-32）

表 3-8　Task Navigator : [デバイスの登録（Device Registration）] （続き）

作業	説明	ユーザ インターフェイス ナビゲーション パス	マニュアル リンク
8. 認証ポリシーの確認。	作業 2 で作成した新規 ID ソース順序を含むように認証ポリシーを作成または変更します。	[ポリシー（Policy）] > [認証（Authentication）]	• 単純な認証ポリシーについては、「単純な認証ポリシーの設定」（P.16-30）を参照してください。 • ルールベースの認証ポリシーについては、「ルールベースの認証ポリシーの設定」（P.16-32）を参照してください。
9. 許可ポリシーの作成。	適切なアクセス権限を付与する許可ポリシーを作成します。各ルールの条件と属性を選択して、ネットワーク全体のアクセス ポリシーを作成します。 pre-posture および post-posture 許可ポリシーを作成します。	[ポリシー（Policy）] > [許可（Authorization）]	「新しい許可ポリシーの作成」（P.17-15）
10. セルフサービス ゲストの設定（ゲストおよび従業員用）	パーソナル デバイスを使用するユーザ ログインのセルフサービス ゲスト設定を行います。	[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータル設定（Multi-Portal Configurations）] > [デフォルト ゲスト ポータル（Default Guest Portal）] > [操作（Operations）] > [セルフプロビジョニング フローの有効化（Enable Self-Provisioning Flow）]	「複数のポータルのホスト」（P.21-51）
11. Simple Certificate Enrollment Protocol（SCEP）認証局（CA）プロファイルの設定。	1 つ以上の SCEP 要求プロファイルを作成します。	[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [SCEP CA プロファイル（SCEP CA Profile）]	「Simple Certificate Enrollment Protocol プロファイルの追加および変更」（P.13-26）