Cisco ISE の機能

Cisco ISE の概要

Cisco ISE はネットワーク リソースへのセキュアなアクセスを提供するセキュリティ ポリシー管理プラットフォームです。Cisco ISE はポリシー デシジョン ポイントとして動作し、企業に

おけるコンプライアンスの遵守、インフラストラクチャのセキュリティの向上、およびサービス オペレーションの合理化を可能にします。企業は、Cisco ISE を使用して、ネットワーク、ユーザ、およびデバイスから状況情報をリアルタイムで収集できます。その後、管理者はその情報を使用して、ガバナンス上の決定を下すことができます。これを行うには、ID をアクセス スイッチ、ワイヤレス LAN コントローラ（WLC）、バーチャル プライベート ネットワーク（VPN）ゲートウェイ、データセンター スイッチなどのさまざまなネットワーク要素に結び付けます。Cisco ISE は、Cisco TrustSec ソリューションのポリシー マネージャとして機能し、TrustSec ソフトウェアによって定義されたセグメンテーションをサポートします。

ISE コミュニティ リソース

ISE コミュニティに参加して、リソースを参照し、質問を投稿し、ディスカッションに参加しましょう。ISE 製品マニュアル、YouTube ビデオ、トレーニング リソースを参照してください。

（注） ISE コミュニティ リソースで提供される例やスクリーンショットは、旧リリースの Cisco ISE のものである可能性があります。新しい機能、追加の機能、更新については、GUI を確認してください。

主要な機能

Cisco ISE は、既存の Cisco ポリシー プラットフォームで使用できる機能のスーパーセットを組み込む、統合されたポリシーベースのアクセス制御システムです。Cisco ISE では次の機能が実行されます。

- 認証、許可、アカウンティング（AAA）、ポスチャ、およびプロファイラを 1 つのアプライアンスに結合します。
- Cisco ISE 管理者、認可されたスポンサー管理者、またはその両方向けの、包括的なゲスト アクセス管理を提供します。
- 包括的なクライアント プロビジョニングの方法を提供し、802.1X 環境など、ネットワークにアクセスするすべてのエンドポイントのデバイス ポスチャを評価することによって、エンドポイントのコンプライアンスを強化します。
- ネットワーク上のエンドポイント デバイスの検出、プロファイリング、ポリシーベースの配置、モニタリングのサポートを提供します。
- 集中型展開および分散型展開においてポリシーの一貫性が維持され、サービスを必要な場所に配信できるようになります。
- セキュリティ グループ タグ（SGT）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（SGACL）を使用した TrustSec などの高度な適用機能を利用します。
- 小さな事務所から大企業まで様々な環境の展開シナリオに対応するスケーラビリティをサポートします。

- ワーク センターを介して TACACS 対応デバイスの管理を容易にします。[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。ただし、[ユーザ（Users）]、[ユーザIDグループ（User Identity Groups）]、[ネットワークデバイス（Network Devices）]、[デフォルトのネットワークデバイス（Default Network Devices）]、[ネットワークデバイスグループ（Network Device Groups）]、[認証（Authentication）] および [許可条件（Authorization Conditions）] などのページは、他のメニュー オプションと共有されます。

ID ベースのネットワーク アクセス

Cisco ISE ソリューションでは、次の領域で、コンテキストに対応した ID 管理が提供されます。

- Cisco ISE は、許可され、ポリシーに準拠したデバイスからユーザがネットワークにアクセスしているかどうかを確認します。
- Cisco ISE は、コンプライアンスとレポーティングに使用できる、ユーザの ID、ロケーション、およびアクセス履歴を確認します。
- Cisco ISE は、割り当て済みのユーザ ロール、グループ、関連付けられたポリシー（ジョブ ロール、ロケーション、デバイス タイプなど）に基づいてサービスを割り当てます。
- Cisco ISE は、認証結果に基づいて、ネットワークの特定のセグメントへのアクセスと、特定のアプリケーションおよびサービスへのアクセスのいずれかまたは両方を、認証されたユーザに許可します。

複数の展開シナリオのサポート

Cisco ISE は企業インフラストラクチャ全体に展開することが可能で、802.1X 有線、無線、およびバーチャル プライベート ネットワーク（VPN）がサポートされます。

Cisco ISE アーキテクチャでは、1 台のマシンがプライマリ ロール、もう 1 台の「バックアップ」マシンがセカンダリ ロールとなる環境において、スタンドアロン展開と分散（別名「ハイアベイラビリティ」または「冗長」）展開の両方がサポートされます。Cisco ISE は、個別の設定可能なペルソナ、サービス、およびロールを特徴としており、これらを使用して、Cisco ISE サービスを作成し、ネットワーク内の必要な箇所に適用できます。これにより、フル機能を備え統合されたシステムとして動作する包括的な Cisco ISE 展開が実現します。

Cisco ISE ノードは、1 つ以上の管理ペルソナ、モニタリング ペルソナ、およびポリシー サービス ペルソナとして展開できます。各ペルソナは、ネットワーク ポリシー管理トポロジ内の異なる部分で重要な役割を担います。Cisco ISE を管理ペルソナとしてインストールすると、集中型ポータルからネットワークを設定および管理することによって、効率と使いやすさを向上させることができます。

UCS ハードウェアのサポート

Cisco ISE 2.3 は、次のハードウェア プラットフォームをサポートしています。

- SNS-3415（小）
- SNS-3495（大）
- SNS-3515（小）
- SNS-3595（大）

ハードウェアの仕様については、『Cisco Identity Services Engine Data Sheet』の表 3 を参照してください。

基本的なユーザ認証および許可

Cisco ISE のユーザ認証ポリシーを使用すると、パスワード認証プロトコル（PAP）、チャレンジ ハンドシェイク認証プロトコル（CHAP）、保護拡張認証プロトコル（PEAP）、拡張認証プロトコル（EAP）などのさまざまな標準認証プロトコルを使用して、多くのユーザ ログイン セッション タイプに対応した認証を提供できます。Cisco ISE では、ユーザが認証を試みるネットワーク デバイスで使用できるプロトコル、およびユーザ認証の検証元となる ID ソースが指定されます。

Cisco ISE では、許可ポリシーの範囲内で広範な可変要素が許可されるため、許可されたユーザのみが、ネットワークにアクセスしたときに目的のリソースにアクセスできます。Cisco ISE の最初のリリースでは、RADIUS によって管理された、内部ネットワークとそのリソースへのアクセスのみがサポートされます。

最も基本的なレベルにおいて、Cisco ISE では、802.1X、MAC 認証バイパス（MAB）、およびブラウザベースの Web 認証ログインが、有線ネットワークと無線ネットワークの両方を介した基本的なユーザ認証およびアクセスに対してサポートされます。認証要求を受信すると、認証ポリシーの「外側部分」を使用して、要求の処理に使用できる一連のプロトコルが選択されます。その後、認証ポリシーの「内側部分」を使用して、要求の認証に使用する ID ソースが選択されます。ID ソースは、特定の ID ストア、またはユーザが最終的な許可応答を受信するまでアクセス可能な一連の ID を一覧表示する ID ストア順序で構成できます。

認証が成功すると、セッション フローは許可ポリシーに進みます。（認証が成功しなかった場合でも Cisco ISE に許可ポリシーの処理を許可するオプションも提供されます）。Cisco ISE を使用すると、「認証失敗」、「ユーザが見つからない」、および「プロセスの失敗」に対する動作を設定できます。また、要求を拒否またはドロップ（応答は発行されません）するか、許可ポリシーに進むかを判断することもできます。Cisco ISE が許可の実行に進む場合、「NetworkAccess」ディクショナリの「AuthenicationStaus」属性を使用して、認証結果を許可ポリシーの一部として組み込むことができます。

許可ポリシーの結果として、Cisco ISE によって割り当てられる許可プロファイルには、ネットワーク ポリシー適用デバイス上のトラフィック管理を指定する、ダウンロード可能な ACL

が含まれる場合があります。このダウンロード可能な ACL では、認証中に返される RADIUS 属性が指定され、この属性により、Cisco ISE で認証されると付与されるユーザ アクセス権限が定義されます。

（注） Cisco ISE は、着信アカウンティング パケットの認証セッションを識別しながら、次の順序で属性を処理します。

- シスコ デバイスの場合：
  1. クラス/状態
  2. audit-session-id
- サード パーティ製のデバイスの場合：
  1. クラス/状態
  2. Calling-Station-ID
  3. 認証セッションを識別できない場合、Cisco ISE は Calling-Station-ID、NAS-Port、および NAS-IP-Address に基づいて新しいセッション ID を作成します。

ポリシー セット

ネットワーク アクセス ポリシーは、[ポリシー（Policy）]>[ポリシーセット（Policy Sets）] からアクセスできる [ポリシー セット（Policy Sets）] にまとめて統合されます。各ポリシー セットは、ポリシー階層の最上位レベルで定義されたコンテナであり、その下にそのセットのすべての関連する認証および許可ポリシーおよびポリシー例外ルールが設定されます。条件に基づいて、認証と許可の両方に複数のルールを定義できます。条件と追加の関連設定は、[ポリシー セット（Policy Set）] インターフェイスから簡単にアクセスして直接再利用することもできます。

Common Access Card 機能のサポート

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 とは、内蔵の電子チップに X.509 クライアント証明書が記録された身分証明バッジであり、この証明書によって、米国国防総省（DoD）などの特定の 1 人の職員が識別されます。CAC によるアクセスには、カードを挿入し PIN 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。

CAC カードを使用して認証を行うことの利点は、次のとおりです。

- Common Access Card X.509 証明書は、802.1X EAP-TLS 認証の ID ソースです。
- Common Access Card X.509 証明書は、Cisco ISE 管理に対する認証および許可用の ID ソースでもあります。

Cisco ISE は、管理者ポータルへのログインのみをサポートします。次のアクセス方法では、CAC 認証はサポートされません。

- Cisco ISE コマンドライン インターフェイスの管理に CAC 認証ログインは使用できません。
- 外部の REST API（モニタリングおよびトラブルシューティング）とエンドポイント保護サービス適応型ネットワーク制御 API では、CAC 認証はサポートされません。
- ゲスト サービスとゲスト スポンサー管理からのアクセスでは、Cisco ISE 内での CAC 認証はサポートされません。

クライアント ポスチャ評価

Cisco ISE を使用すると、適用されたネットワーク セキュリティ対策の適切さと効果を維持するために、保護されたネットワークにアクセスする任意のクライアントマシンに対してセキュリティ機能を検証し、そのメンテナンスを行うことができます。Cisco ISE 管理者は、クライアントマシンで最新のセキュリティ設定またはアプリケーションを使用できるよう設計されたポスチャ ポリシーを使用することによって、どのクライアント マシンでも、企業ネットワークへのアクセスについて定義されたセキュリティ標準を満たし、その状態を継続することを保証できます。ポスチャ コンプライアンス レポートによって、ユーザがログインしたとき、および定期的再評価が行われるたびに、クライアントマシンのコンプライアンス レベルのスナップショットが Cisco ISE に提供されます。

ポスチャ評価およびコンプライアンスは、Cisco ISE で提供される次のいずれかのエージェント タイプを使用して行われます。

- AnyConnect ISE Agent：Windows または Mac OS X クライアントにインストールできる永続的なエージェントであり、ポスチャ コンプライアンス機能を実行します。
- Cisco Temporal Agent：コンプライアンス ステータスを確認するためにクライアント上で実行される一時実行可能ファイル。エージェントは、ログインセッションが終了した後にクライアント マシンから削除されます。デフォルトでは、エージェントは Cisco ISE ISO イメージに存在し、インストール中に Cisco ISE にアップロードされます。

Mobile Device Manager と Cisco ISE との相互運用性

モバイルデバイス管理（MDM）サーバはモバイル事業者、サービスプロバイダー、企業にわたって展開されたモバイルデバイスの保護、モニタ、管理、およびサポートを行います。MDM はエンドポイントにポリシーを適用しますが、ユーザにデバイスの登録や、修復を強制するこ

とはできません。ISE は MDM サーバからポリシーを取得し、ユーザが自分のデバイスを登録したときにそれらのポリシーを適用します。ISE デバイス ポリシーで MDM を必要とし、デバイスが MDM に準拠していない場合、ISE はユーザを MDM オンボーディング ポータルにリダイレクトし、ネットワークにアクセスするためにデバイスを更新するようユーザに求めます。ISE では、MDM コンプライアンスに従っていないユーザに対してインターネット アクセスのみを許可することもできます。

ネットワークのプロファイリングされたエンドポイント

プロファイラ サービスは、ネットワーク上にあるすべてのエンドポイントの機能（Cisco ISE では ID とも呼ばれる）を、デバイス タイプにかかわらず識別、検索、および特定して、企業ネットワークへの適切なアクセスを保証および維持するのに役立ちます。Cisco ISE プロファイラ機能では、さまざまなプローブを使用して、ネットワーク上にあるすべてのエンドポイントの属性を収集し、それらを既知のエンドポイントが関連ポリシーおよび ID グループに従って分類されるプロファイラ アナライザに渡します。

プロファイラ フィード サービスによって、管理者は、新規および更新されたエンドポイントプロファイリング ポリシーや更新された OUI データベースを、指定された Cisco フィード サーバからの、サブスクリプションを介した Cisco ISE へのフィードとして取得できます。

pxGrid ペルソナ

Cisco pxGrid は、Cisco ISE セッション ディレクトリから Cisco Adaptive Security Appliance（ASA）などの他のポリシー ネットワーク システムへのコンテキスト ベースの情報の共有を有効にするために使用されます。pxGrid フレームワークは、ポリシー データや設定データをノード間で交換するためにも使用できます（たとえば、ISE とサードパーティ ベンダー間でのタグやポリシー オブジェクトの共有）。また、脅威情報など、非 ISE 関連情報の交換用にも使用できます。

TACACS+ デバイス管理

Cisco ISE は、ネットワーク デバイスの設定を制御および監査するための Terminal Access Controller Access-Control System（TACACS+）のセキュリティ プロトコルを使用したデバイス管理をサポートしています。ネットワーク デバイスは、デバイス管理者の操作の認証および認可のために ISE にクエリを行うために設定され、ISE のアカウンティング メッセージを送信して操作をログに記録します。これによって、どのネットワーク デバイスに誰がアクセスできて関連するネットワーク設定を変更できるかについて、きめ細かい制御が容易になります。ISE 管理者は、コマンド セットやシェル プロファイルなどの TACACS 結果をデバイス管理アクセス サービスの許可ポリシー ルールで選択できるようにするポリシー セットを作成できます。ISE モニタリング ノードでは、デバイス管理に関する高度なレポートが提供されます。[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。

ISE には、TACACS+ を使用するためのデバイス管理ライセンスが必要です。

SXP のサポート

リソース グループ タグ（SGT）の交換プロトコル（SXP）は、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播するために使用されます。SXP は、ある SGT 対応ネットワーク デバイスから別のデバイスに IP アドレスとともにエンドポイントの SGT を転送するために使用されます。

ノードで SXP サービスをイネーブルにするには、[ノードの一般設定（General Node Settings）] ページで [SXPサービスの有効化（Enable SXP Service）] チェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。

各 SXP 接続には、SXP スピーカーとして指定されたピアと、SXP リスナーとして指定されたピアがあります。ピアは双方向モードで設定することもでき、そのモードでは、それぞれがスピーカーとリスナーの両方として機能します。接続はいずれかのピアによって開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。

サードパーティ デバイスのサポート

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、一部のサードパーティ製ネットワーク アクセス デバイス（NAD）をサポートします。これらのプロファイルによって、ゲスト、BYOD、MAB、ポスチャなどのフローを有効にするために Cisco ISE が使用する機能が定義されます。

Cisco ISE には、次のベンダーからのネットワーク デバイスの定義済みプロファイルが含まれています。

- シスコ：有線および無線
- Aruba：無線
- HP：有線および無線
- Motorola：無線
- Brocade：有線
- Alcatel：有線
- Ruckus：無線

また、定義済みプロファイルがないその他のサードパーティ製ネットワーク デバイス用のプロファイルを作成することもできます。AnyConnect クライアントのプロビジョニングとポスチャ検出では、CoA と URL のリダイレクションは必須ではありません。

リリース 2.0 以前のシスコ以外の NAD を展開し、それらを使用するようにポリシー ルール/RADIUS ディクショナリを作成した場合、これらはアップグレード後に通常どおりに機能し続けます。

テレメトリ

インストール後、管理者ポータルに初めてログインすると、Cisco ISE テレメトリ バナーが画面に表示されます。この機能を使用して、Cisco ISE は、ユーザの展開、ネットワーク アクセス デバイス、プロファイラ、およびユーザが使用している他のサービスに関する非機密情報を安全に収集します。収集されたデータは、今後のリリースでよりよいサービスと追加機能を提供するために使用されます。デフォルトでは、テレメトリ機能は有効になっています。管理者ポータルからディセーブルにすることができます。

IPv6 のサポート

Cisco ISE リリース 2.0 以降、次の IPv6 機能をサポートしています。

- IPv6 対応エンドポイントのサポート：Cisco ISE は、エンドポイントからの IPv6 トラフィックを検出、管理、保護できます。IPv6 属性を使用して、IPv6 対応エンドポイントからの要求を処理し、エンドポイントが準拠していることを保証するための、許可プロファイルおよびポリシーを Cisco ISE で設定できます。
- レポートでの IPv6 サポート：リリース 2.0 のレポートは IPv6 の値をサポートしています。ライブ セッションおよびライブ認証ページもまた IPv6 の値をサポートしています。
  - ipv6 address：ネットワーク インターフェイスごとにスタティック IPv6 アドレス設定を許可する場合
  - ipv6 enable：すべてのネットワーク インターフェイスで IPv6 を有効化または無効化する場合
  - ipv6 route：IPv6 スタティック ルートを設定する場合
  - ip host：ホストのローカル テーブルでの IPv6 アドレスの追加を許可する場合
  - show IPv6 route：IPv6 ルートを表示する場合

これらのコマンドの詳細については、ご使用のリリースの ISE の『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

ロケーションに基づく認証

Cisco ISE は、Cisco モビリティ サービス エンジン（MSE）と統合し、物理ロケーション ベースの認証を導入します。Cisco ISE は、MSE からの情報を使用して、MSE によって報告されるユーザの実際の位置に基づいて差別化されたネットワーク アクセスを提供します。

この機能を使用すると、エンドポイントのロケーション情報を使用して、ユーザが適切なゾーンにいる場合にネットワークアクセスを提供できます。また、エンドポイントのロケーションをポリシーの追加属性として追加して、デバイスのロケーションに基づいてより詳細なポリシー許可のセットを定義することもできます。次のように、ロケーションベースの属性を使用する許可ルール内で条件を設定できます。

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

ロケーション階層（キャンパス/ビルディング/フロア構造）を定義して、Cisco Prime Infrastructure のアプリケーションを使用してセキュアおよび非セキュアのゾーンを設定できます。ロケーション階層を定義した後、ロケーション階層データをMSEサーバと同期する必要があります。

ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。ロケーション ツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。

Cisco ISE 認証局

Cisco ISE は、一元的なコンソールからエンドポイントのデジタル証明書を発行および管理して、従業員が自分のパーソナルデバイスを使用して企業のネットワークに接続できるようにするネイティブの認証局（CA）を提供します。Cisco ISE CA は、スタンドアロンおよび下位の展開をサポートします。

証明書プロビジョニング ポータル

Cisco ISE では証明書プロビジョニング ポータルが提供され、そこで従業員はオンボーディングフローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスは、BYODフローを通過できず、証明書を手動で発行する必要があります。証明書プロビジョニングポータルで、権限のある一連のユーザは、そのようなデバイスに対する証明書要求をアップロードし、キーペアを生成し（必要に応じて）、証明書をダウンロードできます。従業員は、このポータルにアクセスして、1 つの証明書について要求を行うか、または CSV ファイルを使用して一括証明書要求を行うことができます。

証明書テンプレートの拡張子

Cisco ISE の内部 CA には、エンドポイント証明書を作成するために使用された証明書テンプレートを表す拡張子が含まれています。内部 CA によって発行されたすべてのエンドポイント証明書には、証明書テンプレート名の拡張子が含まれています。この拡張子は、そのエンドポイント証明書を作成するために使用された証明書テンプレートを表します。CERTIFICATE: テンプレート名属性を許可ポリシーの条件に使用して、評価の結果に基づいて適切なアクセス権限を割り当てることができます。

Cisco ISE 内部 CA は ASA VPN ユーザに証明書を発行します

内部 ISE CA は、ASA VPN 経由で接続するクライアント マシンに証明書を発行できます。ISE は、Simple Certificate Enrollment Protocol（SCEP）を使用して登録を行い、証明書を Cisco ISE からクライアント マシンにプロビジョニングします。

Active Directory マルチドメイン フォレストのサポート

Cisco ISE では、マルチドメイン フォレストの Active Directory がサポートされます。Cisco ISE は単一のドメインに接続しますが、Cisco ISE が接続されているドメインと他のドメイン間に信頼関係が確立されている場合は、Active Directory フォレストの他のドメインからリソースにアクセスできます。

SAnet デバイスのサポート

Cisco ISE は、セッション認識型ネットワーク（SAnet）が限定的にサポートされます。SAnet は、可視性、認証、許可などのアクセスセッションの管理における一貫性と柔軟性を高める、スイッチのセッション管理フレームワークです。SAnet は、デバイスだけでなく、ISE の両方によって受け入れられる許可オブジェクトであるサービステンプレートの概念を定義します。このことは、デバイスに送信される前に属性のリストにマージされ、フラット化される RADIUS 許可属性のコンテナである Cisco ISE 許可プロファイルと矛盾します。同様に、SAnet サービス テンプレートも RADIUS 許可属性のコンテナですが、デバイスに送信する前にリストにフラット化されません。代わりに、Cisco ISE はサービス テンプレートの名前を送信し、デバイスはキャッシュされたか、または静的に定義されたバージョンがまだない場合コンテンツ（RADIUS 属性）をダウンロードします。さらに、サービス テンプレートの定義が変更された、つまり、RADIUS 属性が追加、削除、または変更された場合、Cisco ISE はデバイスに CoA 通知を送信します。

Cisco ISE は、許可プロファイルを「サービス テンプレート」互換としてマークする特別なフラグを含む許可プロファイルとして、サービステンプレートを実装します。このように、許可プロファイルでもあるサービステンプレートは、SAnet 対応デバイスと同時にレガシーデバイスから接続するセッションをサポートする単一のポリシーステートメントで使用することができます。

管理ノードの自動フェールオーバーのサポート

Cisco ISE は、管理ペルソナの自動フェールオーバーをサポートしています。自動フェールオーバー機能をイネーブルにするには、分散セットアップで少なくとも 2 つのノードが管理ペルソナを引き継ぎ、1 つのノードが非管理ペルソナを引き継ぐ必要があります。プライマリ管理ノード（PAN）がダウンした場合は、セカンダリ管理ノードの自動プロモーションが開始されます。この場合、非管理セカンダリ ノードが各管理ノードのヘルス チェック ノードとして指定されます。ヘルス チェック ノードは、設定された間隔で PAN の正常性を確認します。PAN の

正常性について受信されたヘルス チェック応答がダウンまたは到達不能により良好でない場合、ヘルス チェック ノードは、設定されたしきい値まで待機した後、プライマリ ロールを引き継ぐようにセカンダリ管理ノードのプロモーションを開始します。セカンダリ管理ノードの自動フェールオーバー後に使用できなくなる機能がいくつかあります。Cisco ISE は、元の PAN へのフォールバックをサポートしていません。詳細については、「管理ノードのハイ アベイラビリティ」の項を参照してください。

GUI ベースのアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスはさらに簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。

（注） GUI ベースのアップグレードは、リリース 2.0 からそれ以降のリリースにアップグレードする場合、または Cisco ISE 2.0 の限定提供リリースを一般提供リリースにアップグレードする場合にのみ適用できます。

高度なトラブルシューティングのテクニカルサポートのトンネル

Cisco ISE は、Cisco IronPort トンネル インフラストラクチャを使用して、展開内の ISE サーバに接続してシステムの問題をトラブルシューティングするための、シスコ テクニカル サポート エンジニア用のセキュア トンネルを作成します。Cisco ISE は SSH を使用して、トンネル経由のセキュアな接続を作成します。管理者として、トンネルアクセスを制御できます。サポート エンジニアにアクセス権を付与する時期と期間を選択できます。シスコ カスタマー サポートは、ユーザの介入なしにトンネルを確立できません。サービス ログインに関する通知を受信します。任意の時点でトンネル接続をディセーブルにできます。