改訂：2026 年 9 月 22 日

Cisco Identity Services Engine：用語

Cisco Identity Services Engine

Cisco Identity Services Engine（Cisco ISE）は、共通のポリシーエンジンを介してエンドポイントアクセスを制御し、ネットワークデバイスを管理できる、ID ベースのネットワーク アクセス コントロールおよびポリシー適用ソリューションです。展開は、スタンドアロンノードとして開始し、専用の管理、ポリシーサービス、モニタリング、pxGrid ノードを使用する分散展開に拡張できます。

Cisco Identity Services Engine の用語

適応型ネットワーク制御ポリシー

適応型ネットワーク制御（ANC）ポリシーは、セキュリティイベントに応答してエンドポイントのネットワークアクセスを変更します。たとえば、Cisco ISE は検疫ポリシーを適用し、ネットワーク アクセス デバイスがエンドポイントを再認証するように CoA を発行できます。

管理者ペルソナ

展開設定および管理サービスを提供する Cisco ISE ノードのペルソナ。分散展開では、プライマリポリシー管理ノード（PAN）がアクティブ、セカンダリ PAN がスタンバイになります。プライマリ PAN で行われた設定変更はセカンダリ PAN に複製されます。

エージェントレスポスチャ

永続的にインストールされたポスチャエージェントを必要とせずに、サポートされているエンドポイントからコンプライアンス情報を収集する Cisco ISE のポスチャメソッド。

ANC ポリシー

エンドポイントに割り当てられた適応型ネットワーク制御の状態を表す Cisco ISE の承認条件。

認証プロファイル

Cisco ISE で、認証ルールが一致した場合に返される承認結果のコレクション。アクセス、ネットワーク割り当て、リダイレクト、またはその他の適用属性を指定できます。

ブロックリストポータル

個人デバイスがブロックリストに登録されており、ネットワークにアクセスできないことをユーザーに通知する Cisco ISE デバイスポータル。

BYOD ポータル

従業員がネイティブ サプリカント プロビジョニングによってデバイスを登録するために使用する個人デバイスポータル。Cisco ISE は、ユーザーを認証してエンドポイントを登録し、ネットワークアクセス用にサポートされているデバイスをプロビジョニングする、Bring Your Own Device（BYOD）フローの一部としてこのポータルを使用します。

証明書プロビジョニング ポータル

承認されたユーザーが、標準のオンボーディングフローを使用できないデバイスの証明書を要求してダウンロードできる Cisco ISE ポータル。

Cisco ISE API ゲートウェイ

外部 API リクエストが Cisco ISE サービス API に到達するまでに通過する単一のエントリポイント。

Cisco ISE データ接続

レポートおよび分析用の設定および運用データベースビューへの読み取り専用アクセスを提供する Cisco ISE の機能。

Cisco ISE 内部認証局

エンドポイントの証明書の発行と管理を行う内部認証局（Cisco ISE CA）。

Cisco ISE パッシブ アイデンティ コネクタ

ISE-PIC と略される Cisco ISE 仮想アプライアンス。認証データを収集し、統合されたパッシブ ID 情報を登録システムに提供します。

クライアント プロビジョニング ポリシー

Cisco ISE がエンドポイントに提供するエージェント、コンプライアンスモジュール、設定、またはその他のプロビジョニングリソースを決定する一連のルール。Cisco ISE は、ID グループやオペレーティングシステムなどの属性を評価して、プロビジョニング結果を選択します。

クライアント プロビジョニング ポータル

エンドポイントがネットワークアクセスまたはポスチャアセスメントに必要なクライアントプロビジョニング リソースを取得する Cisco ISE ポータル。

クラウド多要素分類プロファイラ

観測されたエンドポイント属性をクラウドサービスと共有し、返された分類ラベルを適用する Cisco ISE プロファイリングサービス。

条件スタジオ

ポリシー条件の作成、結合、保存、再利用に使用される Cisco ISE ポリシーエディタ。

デバイス管理ポリシーセット

デバイス管理者のTACACS+認証および承認を制御するポリシーコンテナ。通常のデバイス管理ポリシーセットには、認証および承認ルールテーブルが含まれています。その認証ルールは、TACACS+ コマンドセットおよびシェルプロファイルを返すことができます。プロキシシーケンス ポリシー セットは、設定されたリモートプロキシサーバーにリクエストを転送します。

ダイナミック再認証スケジューラ

学習した期限日および時刻に許可されたセッションを終了する Cisco ISE の機能。

エンドポイントのデバッグ ログ コレクタ

指定されたエンドポイントに関連付けられているデバッグログを収集する Cisco ISE の障害対応機能。

エンドポイント ID グループ

Cisco ISE がポリシーの評価と管理のためにエンドポイントを分類するときに使用する論理グループ。ポータルおよび登録フローではエンドポイント ID グループにデバイスを配置でき、認証ルールではこのグループを条件として使用できます。

エンドポイント消去ポリシー

エンドポイントデータベースから削除するエンドポイントレコードを定義する Cisco ISE ポリシー。

ゲストタイプ

Cisco ISE で、アカウント有効期間、アクセス時間、ID グループ、アカウントの作成を許可されたスポンサーグループなど、ゲストアカウントのクラスを定義する再利用可能な一連の設定。

正常性チェックノード

Cisco ISE で、プライマリポリシー管理ノードを監視し、プライマリノードが使用できない場合にセカンダリノードの自動昇格を開始する非管理ノード。

ホットスポット ゲスト ポータル

ユーザー名とパスワードを要求せずにネットワークアクセスを提供するゲストポータル。Cisco ISE は、ネットワーク アクセス デバイスおよびデバイス登録 Web 認証と連携してゲストエンドポイントを承認します。このポータルでは、アクセスコードまたはアクセプタブル ユース ポリシーの受け入れを求められる場合があります。

ID ソース順序

Cisco ISE で、Cisco ISE が認証中に検索する順序付けられた ID ソースのセット。証明書認証プロファイルを含めることもできます。

モニタリングおよび障害対応ノード（MnT）

管理およびポリシーサービスノードからログを収集し、モニタリング、レポート、障害対応機能を提供する Cisco ISE ノード。

モニタリングペルソナ

運用データと監査データを収集し、モニタリング、レポート、障害対応機能を提供する Cisco ISE ノードのペルソナ。分散展開では、プライマリとセカンダリのモニタリングおよび障害対応（MnT）ノードはアクティブ/スタンバイペアを形成し、ポリシーサービスノードは両方に運用データを送信します。

デバイス ポータル

従業員がデバイスを追加、登録、管理するために使用する個人デバイスポータル。ネイティブサプリカントプロビジョニングを使用できないデバイスをサポートします。ポータルを介して追加されたデバイスはエンドポイントとして記録され、別の静的割り当てが存在しない限り、登録済みデバイスのエンドポイント ID グループに配置されます。

ネイティブ サプリカント プロビジョニング

セキュアなアクセスのためにサポートされているエンドポイントのネイティブ ネットワーク サプリカントを設定する BYOD プロセス。Cisco ISE は、エンドポイントのオペレーティングシステムに基づいて、ネイティブ サプリカント プロファイルから該当するプロビジョニングフローを選択します。

ネットワーク デバイス グループ

Cisco ISE で、ネットワークデバイスの階層的なグループ化を意味し、一般的にポリシー条件で使用できる場所やデバイスタイプなどの属性別に整理されます。

ポリシー管理ノード（PAN）

管理ペルソナを実行する Cisco ISE ノード。ポリシー管理ノード（PAN）は、展開とそのポリシーを設定するための中心点です。高可用性展開では、プライマリ PAN とセカンダリ PAN が使用されます。

ポリシーサービスノード（PSN）

エンドポイントセッションを処理し、ネットワーク アクセス ポリシーを評価する Cisco ISE ノード。ポリシーサービスノード（PSN）は、RADIUS の認証と承認、ゲストアクセス、プロファイリング、ポスチャ、デバイス管理などのサービスを提供できます。分散展開では、セッションフェールオーバーに PSN グループを使用できます。

ポリシー サービス ノード グループ

メンバーがノード障害を検出し、影響を受ける URL リダイレクトされたセッションをリセットする Cisco ISE ポリシーサービスノードのグループ。

ポリシーサービスペルソナ

アクセスポリシーを評価し、ネットワークアクセス、ポスチャ、ゲストアクセス、クライアントプロビジョニング、およびプロファイリングサービスを提供する Cisco ISE ペルソナ。

ポリシーセット

Cisco ISE で、ネットワークアクセスのユースケースの認証、承認、例外ルールをグループ化する最上位のポリシーコンテナ。

ポスチャ条件

Cisco ISE では、ソフトウェア、ファイル、サービス、またはその他のサポートされている属性の存在、ステータス、または設定など、指定されたエンドポイント状態のテスト。

ポスチャ リース

Cisco ISE が以前に決定したコンプライアンスポスチャ状態を再利用できる期間。リースの期限が切れると、後続の該当するユーザーセッションは再度ポスチャアセスメントを受ける必要があります。

ポスチャ要件

Cisco ISE で、ポスチャ条件を修復アクションとサポートされているオペレーティングシステムに関連付けるポリシー要素。

プロファイラサービス

Cisco ISE で、プローブとセンサーからエンドポイント属性を収集し、プロファイリングポリシーを適用してデバイスを分類するサービス。

プロトコルエンジン

特定の認証シナリオの証明書を検証して処理を最適化する専用サービス。プロトコルエンジンは、API コールを介して Cisco ISE アプリケーションサーバーと通信します。

pxGrid（Platform Exchange Grid）

Cisco ISE とサードパーティのセキュリティ プラットフォーム間におけるコンテキストとポリシー情報のセキュアでスケーラブルな双方向交換を可能にするフレームワーク。ネットワークエコシステム全体での ID とセキュリティデータのリアルタイム共有を容易にします。

pxGrid クラウド

Cisco ISE とクラウドベースのセキュリティ プラットフォーム間におけるセキュアな双方向データ交換を可能にするクラウドベースのフレームワーク。従来の pxGrid の機能を拡張し、ハイブリッド環境間でのコンテキストの共有とポリシーのオーケストレーションを容易にします。

pxGrid ノード

pxGrid ペルソナを実行し、承認された統合クライアントにコンテキスト共有サービスを提供する Cisco ISE ノード。

pxGrid ペルソナ

承認されたクライアントおよびエコシステム統合のための pxGrid サービスを実行する Cisco ISE ノードのペルソナ。これにより、システムはコンテキスト情報の公開、クエリ、およびコンテキスト情報への登録を行い、サポートされている制御アクションを要求できるようになります。

リモートサポート許可

管理者が、指定したシスコのスペシャリストに選択した Cisco ISE ノードへの期限および監査付きのアクセス権を付与する Cisco ISE の機能。

Secure Network Server（SNS）

Cisco ISE ソフトウェアをホストして実行するように設計された専用ハードウェア アプライアンス プラットフォーム。これらのアプライアンスは、エンタープライズグレードのポリシー管理に必要な最適化されたコンピュート、ストレージ、ネットワーキングリソースを提供します。

アカウント登録ゲスト ポータル

Cisco ISE で、訪問者が独自のゲストアカウントを作成する公認ゲストポータル。このフローでは、登録情報、スポンサー承認、またはアクセプタブル ユース ポリシーの受け入れを求められる場合があります。

スポンサー ポータル

Cisco ISE で、承認されたスポンサーが一時的なゲストアカウントのログイン情報を作成、インポート、管理、提供するポータル。

Sponsored-Guest ポータル

ゲストが承認されたスポンサーによって作成されたアカウントを使用する Cisco ISE の公認ゲストポータル。

TACACS+ コマンドセット

Cisco ISE で、デバイス管理者が実行を許可または拒否されるコマンドと引数を識別するデバイス管理承認結果。

TACACS+ プロファイル

Cisco ISE で、シェル権限レベルやベンダー固有の属性などの TACACS+ 属性を含むデバイス管理承認結果。

TC-NAC ノード

Threat Centric Network Access Control（TC-NAC）サービスを実行するように設定された Cisco ISE 展開のポリシーサービスノード（PSN）。このノードは、受信した脅威と脆弱性の属性を処理し、エンドポイントのリスクに基づいて認証ポリシーを動的に調整します。

テンポラルエージェント

永続的ポスチャアプリケーションをインストールせずに、Cisco ISE がエンドポイントポスチャを評価するために使用する一時的な実行可能ファイル。

Threat Centric Network Access Control サービス

脅威と脆弱性の属性を受信し、エンドポイントのリスクに基づいて認証ポリシーを動的に調整する Cisco ISE サービス。ポリシーサービスノード（PSN）で有効にすると、特定されたセキュリティ脅威に応じたネットワークアクセスの自動変更が可能になります。

翻訳について
このドキュメントは、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。