CHAPTER 1

Cisco ISE の概要

Cisco Identity Services Engine（ISE）は、企業でのコンプライアンスの順守、インフラストラクチャのセキュリティの強化、およびサービス オペレーションの合理化を実現する、次世代のアイデンティティおよびアクセス コントロール ポリシーのプラットフォームです。Cisco ISE 固有のアーキテクチャにより、企業はネットワーク、ユーザ、およびデバイスから状況に応じた情報をリアルタイムで収集できるようになります。その後、管理者はその情報を使用して、積極的に管理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 Security Group Access Solution のキー コンポーネントです。

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 管理者と許可されたスポンサーの管理者またはその両方に、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）によってセキュリティ グループ アクセス（SGA）などの高度な強化機能を使用します。
- 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。

Cisco ISE で提供される次の重要な機能によって、アクセス ネットワーク全体を管理できるようになります。

ID ベースのネットワーク アクセスの提供

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。

詳細については、第 4 章「ID および管理者アクセスの管理」を参照してください。

さまざまな展開シナリオの管理

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。

また、Cisco ISE プラットフォームをインライン ポスチャ ノードとして展開することによって、ポリシーの適用を実施するとともに、Cisco ISE ポリシー管理を簡易化するために必要な機能がサポートされない WLC や VPN コンセントレータを経由してユーザがネットワークにアクセスする環境で、許可変更（CoA）要求を実行することもできます。

詳細については、次のトピックを参照してください。

- 第 9 章「分散環境での Cisco ISE の設定」
- 第 10 章「インライン ポスチャの設定」

基本的なユーザ認証および許可の提供

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、認証が失敗した場合、ユーザが見つからなかった場合、および処理が失敗した場合の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、認証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。

詳細については、次のトピックを参照してください。

- 第 16 章「認証ポリシーの管理」
- 第 17 章「許可ポリシーおよびプロファイルの管理」

FIPS 140-2 実装のサポート

Cisco ISE では、連邦情報処理標準（FIPS）140-2 共通基準 EAL2 へのコンプライアンスがサポートされます。FIPS 140-2 は、米国政府が定めるコンピュータ セキュリティ標準の 1 つであり、暗号化モジュールの認定に使用されています。Cisco ISE では、埋め込み型の FIPS 140-2 実装が使用されています。これは、検証済みの C3M および Cisco ACS NSS モジュールを使用するものであり、FIPS 140-2 Implementation Guidance セクション G.5 のガイドラインに準拠しています。

また、FIPS 標準では、特定のアルゴリズムの使用が制限されます。この標準を適用するには、Cisco ISE で FIPS の動作を有効にする必要があります。Cisco ISE では、RADIUS 共有秘密およびキー管理手法を経由した FIPS 140-2 へのコンプライアンスが有効になり、証明書の SHA-256 暗号化および復号化機能が提供されます。FIPS モードのときは、FIPS に準拠しないアルゴリズムを使用する機能を実行しようとしても失敗し、したがって一部の認証機能は無効になります。

Cisco ISE で FIPS モードを有効にすると、次の機能が影響を受けます。

- IEEE 802.1X 環境
  - EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）
  - EAP-Transport Layer Security（EAP-TLS）
  - PEAP
  - RADIUS

（注）

- EAP-Message Digest 5（EAP-MD5）、Lightweight Extensible Authentication Protocol（LEAP）、PAP など、その他のプロトコルは FIPS 140-2 に準拠したシステムと互換性がなく、Cisco ISE が FIPS モードのときは無効になります。
- FIPS モードを有効にすると、Cisco ISE のゲスト ログイン機能に必要な PAP および CHAP プロトコルも自動的に無効になります。レイヤ 3 ゲスト ログイン実装に伴うこの問題への対処方法の詳細については、第 21 章「ユーザ アクセスの管理」を参照してください。

- Secure Shell（SSH）クライアントは SSHv2 のみを使用できる
- Lightweight Directory Access Protocol（LDAP）over Secure Sockets Layer（SSL）
- インライン ポスチャ ノードの RADIUS キー ラップ
- 管理者 ISE ノードとインライン ポスチャ ノードの両方に対する HTTPS プロトコル通信

詳細については、次のトピックで、特定の FIPS 140-2 設定オプションに関する説明を参照してください。

- 第 6 章「ネットワーク デバイスの管理」
- 第 8 章「Cisco ISE の管理」（「Cisco ISE での FIPS モードの有効化」（P.8-3））
- 第 13 章「証明書の管理」
- 第 16 章「認証ポリシーの管理」

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 経由でアクセスするには、カード リーダーが必要です。ユーザは、リーダーにカードを挿入して PIN を入力します。これで、カードからの証明書が Windows 証明書ストアに転送され、Cisco ISE を実行するローカル ブラウザなどのアプリケーションで使用できるようになります。

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 では、管理者ユーザ インターフェイスへのログインのみがサポートされます。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 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。

Cisco ISE における CAC 認証の設定の詳細については、第 8 章「Cisco ISE の管理」を参照してください。

クライアント ポスチャ評価の組み込み

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。

- Cisco NAC Web Agent は、ログイン時にユーザがシステムにインストールする一時的なエージェントであり、ログイン セッションが終了すると、クライアント マシンには表示されなくなります。
- Cisco NAC Agent は、一度インストールすると、Windows または Mac OS X クライアント マシン上で維持される永続的なエージェントであり、ユーザ ログインとセキュリティ コンプライアンスに関するすべての機能を Windows XP、Windows Vista、Windows 7、または Mac OS 10.5 および 10.6 クライアントに対してそれぞれ実行できます。

詳細については、次のトピックを参照してください。

- 第 19 章「クライアント プロビジョニング ポリシーの設定」
- 第 20 章「クライアント ポスチャ ポリシーの設定」

スポンサーの定義とゲスト セッションの管理

ゲスト スポンサーとして Cisco ISE ゲスト登録ポータルへの適切なアクセスを許可された Cisco ISE 管理者と従業員は、ゲスト、ビジター、請負業者、コンサルタント、および顧客がネットワークにアクセスできるように、一時ゲスト ログイン アカウントを作成し、使用可能なネットワーク リソースを指定できます。ゲスト アクセス セッションには有効期限タイマーが関連付けられるため、ゲスト アクセスを特定の日付や期間に制限できます。

ゲスト ユーザ セッションのすべての側面（アカウントの作成と停止を含む）は追跡され、Cisco ISE に記録されるため、必要に応じて監査情報を提供したり、セッション アクセスのトラブルシューティングを行うことができます。

詳細については、次のトピックを参照してください。

- 第 21 章「ユーザ アクセスの管理」
- 『*Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x*』

インライン ポスチャ ノードを使用したワイヤレスおよび VPN トラフィックの管理

インライン ポスチャ ノードは、Cisco ISE アクセス ポリシーを適用し、CoA 要求を処理するゲートキーパー ノードです。（EAP/802.1X と RADIUS を使用した）初期認証後も、クライアント マシンはポスチャ評価を受ける必要があります。ポスチャ評価プロセスによって、クライアントからネットワークへのアクセスを制限するか、拒否するか、フル アクセスを許可するかが決定されます。クライアントが WLC または VPN デバイスを通じてネットワークにアクセスする場合、インライン ポスチャ ノードは、他のネットワーク デバイスが対応できないポリシー適用と CoA に対応します。この理由から、Cisco ISE を、ネットワーク上の他のネットワーク アクセス デバイス（WLC や VPN コンセントレータなど）の背後にインライン ポスチャ ノードとして展開できます。

詳細については、第 10 章「インライン ポスチャの設定」を参照してください。

ネットワーク上のプロファイル 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、それぞれのデバイス 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 の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。

詳細については、第 18 章「エンドポイント プロファイリング ポリシーの設定」を参照してください。

さまざまなハードウェアおよび VMware プラットフォームへのインストール

Cisco ISE は、さまざまなパフォーマンス上の特徴を備えた広い範囲の物理アプライアンスにあらかじめインストールされた状態で提供されます。Cisco Application Deployment Engine（ADE）と Cisco ISE ソフトウェアは、専用の Cisco ISE 3300 シリーズ アプライアンスまたは VMware サーバ（Cisco ISE VM）のいずれかで実行します。Cisco ISE ソフトウェア イメージでは、この専用プラットフォームにその他のパッケージまたはアプリケーションをインストールできません。Cisco ISE が本来備えている拡張性によってアプライアンスを展開に追加し、必要に応じてパフォーマンスと復元力を向上させることができます。

ハードウェア プラットフォームと Cisco ISE のインストールの詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*』を参照してください。