



# Cisco ISE のネットワーク デプロイメント

- その他の参考資料 (1 ページ)
- 通信、サービス、およびその他の情報 (1 ページ)
- Cisco ISE ネットワークアーキテクチャ (2 ページ)
- Cisco ISE 展開の用語 (2 ページ)
- 分散デプロイメント環境のノードタイプおよびペルソナ (3 ページ)
- ISE のスタンドアロン デプロイメント環境と分散デプロイメント環境 (5 ページ)
- 分散デプロイメント環境のシナリオ (5 ページ)
- 小規模のネットワーク デプロイメント (5 ページ)
- 中規模のネットワーク デプロイメント (7 ページ)
- 大規模のネットワーク デプロイメント (8 ページ)
- Cisco ISE 展開のサイズ設定ガイドライン (11 ページ)
- Cisco ISE のサポートに必要なスイッチおよびワイヤレス LAN コントローラの設定 (11 ページ)

## その他の参考資料

次のリンクには、Cisco ISE で作業するときを使用できる追加のリソースが含まれています。  
[https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco\\_ISE\\_End\\_User\\_Documentation.html](https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html)

## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) [英語] にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) [英語] にアクセスしてください。

- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

## シスコバグ検索ツール

[Ciscoシスコバグ検索ツール \(BST\)](#) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

## マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

## Cisco ISE ネットワークアーキテクチャ

Cisco ISE アーキテクチャには、次のコンポーネントが含まれます。

- ノードおよびペルソナの種類
  - Cisco ISE ノード : Cisco ISE ノードは管理、ポリシー サービス、モニタリング、または pxGrid のペルソナのいずれかまたはすべてを担当することができます。
- ネットワーク リソース
- エンドポイント

ポリシー情報ポイントは、外部の情報がポリシー サービス ペルソナに伝送されるポイントを表します。たとえば、外部情報は Lightweight Directory Access Protocol (LDAP) 属性になります。

## Cisco ISE 展開の用語

このガイドでは、Cisco ISE デプロイメント シナリオについて説明する際に次の用語を使用します。

用語	定義
サービス	ネットワークアクセス、プロファイリング、ポスチャ、セキュリティグループアクセス、モニターリング、およびトラブルシューティングなど、ペルソナが提供する特定の機能。
ノード	個別の物理または仮想 Cisco ISE アプライアンス。
ノードタイプ	Cisco ISE ノードは、管理、ポリシー サービス、モニターリングのペルソナのいずれかを担当することができます。
ペルソナ	ノードによって提供されるサービスを決定します。Cisco ISE ノードは、のペルソナのいずれかまたはすべてを担うことができます。管理ユーザーインターフェイスで使用できるメニューオプションは、ノードが担当するロールおよびペルソナによって異なります。
ロール	ノードがスタンドアロン、プライマリ、セカンダリノードのいずれであるかを決定し、管理ノードとモニターリングノードだけに適用されます。

## 分散デプロイメント環境のノードタイプおよびペルソナ

Cisco ISE ノードは担当するペルソナに基づき、各種のサービスを提供できます。デプロイメントの各ノードは、管理、ポリシーサービス、pxGrid、およびモニターリングのペルソナのいずれかを担当することができます。分散デプロイメントでは、ネットワーク上で次の組み合わせのノードを使用できます。

- ハイ アベイラビリティ用のプライマリ管理ノードとセカンダリ管理 ISE ノード
- 自動フェールオーバー用の 1 組のモニターリング ノード
- セッション フェールオーバー用の 1 つ以上のポリシー サービス ノード
- pxGrid サービスの 1 つ以上の pxGrid ノード

### 管理ノード

管理ペルソナの Cisco ISE ノードは、Cisco ISE のすべての管理操作を実行することができます。このノードは、認証、認可、およびアカウントリングなどの機能に関するすべてのシステム関連の設定を扱います。分散デプロイメント環境では、最大 2 つの管理ペルソナを実行するノードを実行できます。管理ペルソナは、スタンドアロン、プライマリ、セカンダリのロールを担当できます。

## ポリシー サービス ノード

ポリシー サービス ペルソナの Cisco ISE ノードは、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 サービスを提供します。このペルソナはポリシーを評価し、すべての決定を行います。複数のノードがこのペルソナを担当できます。通常、1つの分散デプロイメントに複数のポリシー サービス ノードが存在します。同じ高速ローカルエリア ネットワーク (LAN) またはロード バランサの背後に存在するポリシー サービス ノードはすべて、グループ化してノードグループを形成することができます。ノードグループのいずれかのノードで障害が発生した場合、その他のノードは障害を検出し、URL にリダイレクトされたセッションをリセットします。

分散セットアップでは、少なくとも 1 つのノードがポリシー サービス ペルソナを担当する必要があります。

## モニターリング ノード

モニターリング ペルソナの機能を持つ Cisco ISE ノードがログ コレクタとして動作し、ネットワーク内のすべての管理およびポリシー サービス ノードからのログを保存します。このペルソナは、ネットワークとリソースを効果的に管理するために使用できる高度なモニターリング およびトラブルシューティングツールを提供します。このペルソナのノードは収集したデータを集約して関連付けを行い、有意義なレポートを提供します。Cisco ISE では、このペルソナを持つノードを最大 2 つ使用することができます。これらのノードは、ハイアベイラビリティ用のプライマリ ロールまたはセカンダリ ロールを担うことができます。プライマリ モニターリング ノードおよびセカンダリ モニターリング ノードの両方が、ログメッセージを収集します。プライマリ モニターリング ノードがダウンした場合は、セカンダリ モニターリング ノードが自動的にプライマリ モニターリング ノードになります。

分散セットアップでは、少なくとも 1 つのノードが監視ペルソナを担当する必要があります。同じ Cisco ISE ノードで、モニターリング ペルソナとポリシー サービス ペルソナを有効にしないことをお勧めします。最適なパフォーマンスを実現するために、モニターリング ノードはモニターリング専用とすることをお勧めします。

## pxGrid ノード

Cisco pxGrid を使用すると、Cisco ISE セッションディレクトリからの状況依存情報を、ISE エコシステムのパートナー システムなどの他のネットワーク システムや他のシスコ プラットフォームと共有できます。pxGrid フレームワークは、Cisco ISE とサードパーティのベンダー間でのタグおよびポリシー オブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用できます。また、その他の情報交換にも使用できます。Cisco pxGrid によって、サードパーティ システムは適応型のネットワーク制御アクション (EPS) を呼び出し、ネットワークまたはセキュリティ イベントに応じてユーザーまたはデバイスを隔離できます。タグ定義、値、および説明のような TrustSec 情報は、TrustSec トピックを通して Cisco ISE から別のネットワークに渡すことができます。完全修飾名 (FQN) を持つエンドポイントプロファイルは、エンドポイントプロファイル メタ トピックを通して Cisco ISE から他のネット

ワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイント プロファイルの一括ダウンロードもサポートしています。

pxGrid 経由で SXP バインディング (IP-SGT マッピング) を発行および受信登録できます。SXP バインディングの詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「[Source Group Tag Protocol](#)」のセクションを参照してください。

ハイアベイラビリティ設定で、Cisco pxGrid サーバーは、PAN を通してノード間で情報を複製します。PAN がダウンすると、pxGrid サーバーは、クライアントの登録およびサブスクリプション処理を停止します。pxGrid サーバーの PAN をアクティブにするには、手動で昇格する必要があります。

## ISE のスタンドアロン デプロイメント環境と分散デプロイメント環境

単一の Cisco ISE ノードがあるデプロイメント環境は「スタンドアロン デプロイメント」と呼ばれます。このノードは、管理、ポリシーサービス、およびモニタリングのペルソナを実行します。

複数の Cisco ISE ノードがあるデプロイメント環境は「分散デプロイメント」と呼ばれます。フェールオーバーをサポートし、パフォーマンスを改善するために、複数の Cisco ISE ノードを分散方式でセットアップできます。Cisco ISE の分散導入環境では、管理およびモニタリングアクティビティは一元化され、処理はポリシーサービスノード間で分配されます。パフォーマンスのニーズに応じて、導入の規模を変更できます。Cisco ISE ノードは、管理、ポリシーサービス、およびモニタリングのペルソナのいずれかまたはすべてを担当することができます。

## 分散デプロイメント環境のシナリオ

- 小規模のネットワーク デプロイメント
- 中規模のネットワーク デプロイメント
- 大規模のネットワーク デプロイメント

## 小規模のネットワーク デプロイメント

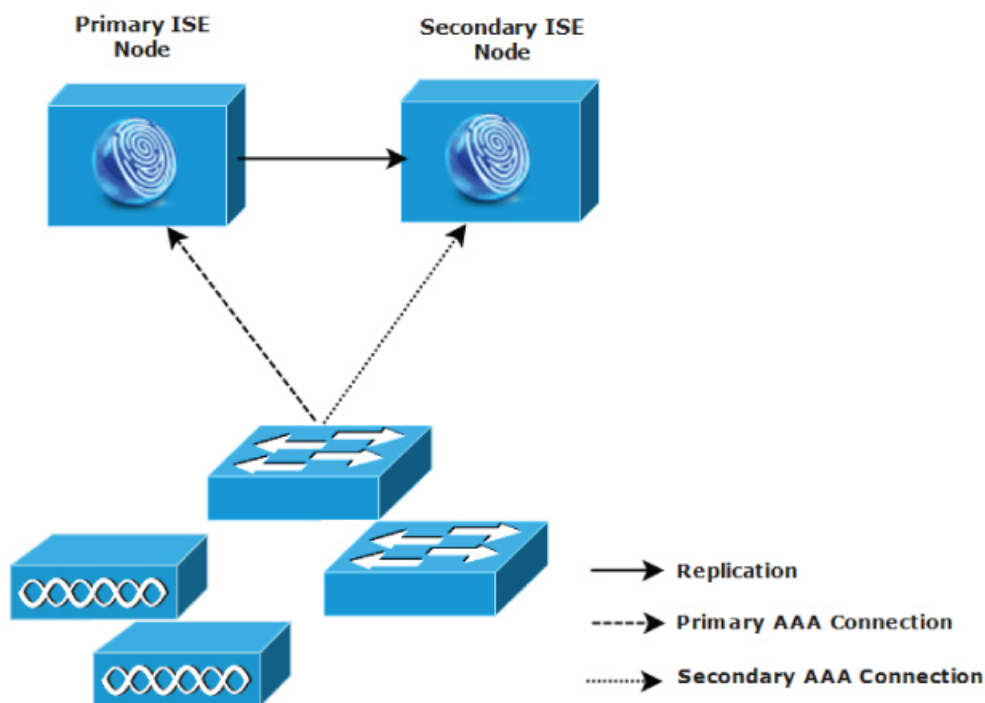
最も小規模な Cisco ISE デプロイメント環境は、2つの Cisco ISE ノードから構成されます (小規模なネットワークでは1つの Cisco ISE ノードがプライマリ アプライアンスとして動作します)。

プライマリ ノードは、このネットワークモデルに必要なすべての設定、認証、およびポリシー機能を提供し、セカンダリ Cisco ISE ノードはバックアップ ロールで稼働します。セカンダリ

ノードはプライマリノードをサポートし、プライマリノードとネットワークアプライアンス、ネットワークリソース、またはRADIUSとの間で接続が失われたときにネットワークを稼働し続けます。

クライアントとプライマリ Cisco ISE ノード間の一元化された認証、認可、アカウントिंग (AAA) 操作は RADIUS プロトコルを使用して行われます。Cisco ISE は、プライマリ Cisco ISE ノードに存在するすべてのコンテンツをセカンダリ Cisco ISE ノードに同期 (複製) します。したがって、セカンダリノードは、プライマリノードの状態と同じになります。小規模なネットワークデプロイメントでは、このような設定モデルにより、このタイプのデプロイメントまたは同様の方法を使用して、すべての RADIUS クライアントでプライマリノードとセカンダリノードの両方を設定することが可能です。

図 1: Cisco ISE ノードの小規模なネットワークデプロイメント



282092

ネットワーク環境で、デバイス、ネットワークリソース、ユーザー、およびAAAクライアントの数が増えた場合、基本的な小規模モデルからデプロイメント環境の設定を変更し、分割または分散されたデプロイメントモデルを使用する必要があります。

## 分割デプロイメント

分割 Cisco ISE デプロイメント環境でも、小規模な Cisco ISE デプロイメント環境で説明したように、プライマリノードとセカンダリノードを維持することができます。ただし、AAA ロードは、AAA ワークフローを最適化するためにこの2つの Cisco ISE ノード間で分割されます。AAA 接続で問題がある場合は、各 Cisco ISE アプライアンス (プライマリまたはセカンダリ)

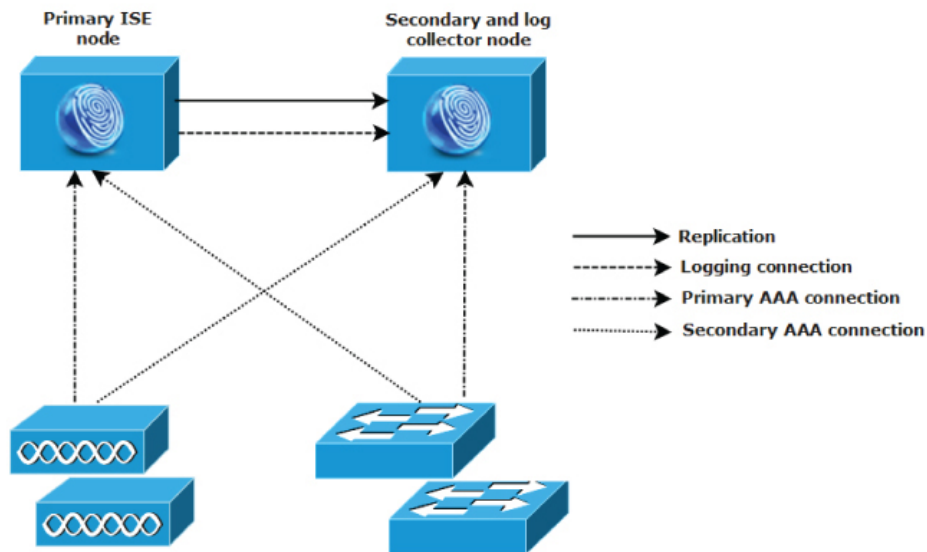
がすべてのワークロードを処理できる必要があります。通常のネットワーク運用では、プライマリノードとセカンダリノードのどちらもすべての AAA 要求を処理することはできません。これは、このワークロードがこの 2 つのノード間で分散されているためです。

このように負荷を分割することにより、システムの各 Cisco ISE ノードに対する負荷はただちに減少します。また、負荷の分割により優れた負荷の制御が実現する一方で、通常のネットワーク運用中のセカンダリノードの機能ステータスはそのまま保持されます。

分割された Cisco ISE の導入環境では、各ノードが、ネットワーク アドミッションやデバイス管理などの独自の固有操作を実行でき、障害発生時でもすべての AAA 機能を引き続き実行することができます。認証要求を処理し、アカウントングデータを AAA クライアントから収集する 2 つの Cisco ISE ノードがある場合は、Cisco ISE ノードのいずれかがログコレクタとして動作するように設定することを推奨します。

また、分割 Cisco ISE デプロイメント環境の設計は、拡張に対応しているため、メリットがもたらされます。

図 2: Cisco ISE での分割ネットワークデプロイメント



282093

## 中規模のネットワーク デプロイメント

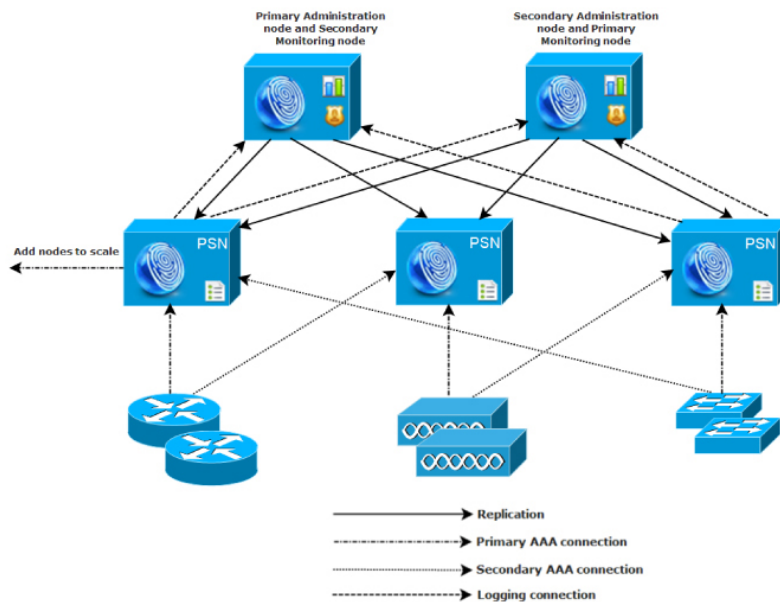
小規模なネットワークが大きくなった場合に、Cisco ISE ノードを追加して中規模なネットワークを作成することで、素早くネットワークの拡大に対応できます。中規模なネットワークデプロイメントでは、新規ノードをすべての AAA 機能専用とし、元のノードを設定およびログイン機能のために使用します。



- (注) 中規模のネットワーク デプロイメントでは、管理ペルソナ、モニターリング ペルソナ、またはその両方を実行しているノードでポリシー サービス ペルソナを有効にできません。専用のポリシー サービス ノードが必要です。

ネットワークでログ トラフィックの量が増加した場合は、セカンダリ Cisco ISE ノードの 1 つまたは 2 つを、ネットワークでのログ収集に使用することを選択できます。

図 3: Cisco ISE での中規模のネットワークデプロイメント



## 大規模のネットワーク デプロイメント

### 集中ロギング

大規模な Cisco ISE ネットワークには集中ロギングを使用することをお勧めします。集中ロギングを使用するには、大規模で通信量の多いネットワークが生成することがある大きな syslog トラフィックを処理するモニターリングペルソナ（モニターリングおよびロギング用）として動作する、専用ロギングサーバーを最初に設定する必要があります。

syslog メッセージは発信ログ トラフィックに対して生成されるため、どの RFC 3164 準拠の syslog アプライアンスでも、発信ロギング トラフィックのコレクタとして動作できます。専用ロギングサーバーでは、すべての Cisco ISE ノードをサポートするために Cisco ISE で使用できるレポート機能およびアラート機能を使用できます。



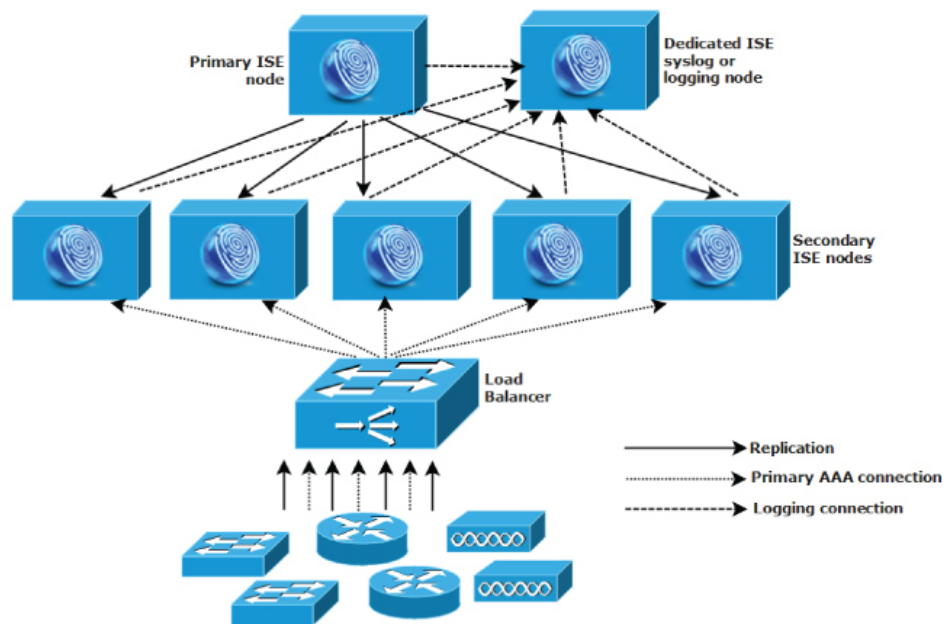
また、アプライアンスが Cisco ISE ノードの監視ペルソナと汎用 syslog サーバーの両方にログを送信するよう設定することもできます。汎用 syslog サーバーを追加することにより、Cisco ISE ノード上の監視ペルソナがダウンした場合に冗長なバックアップが提供されます。

## 集中型ネットワークでのロードバランサの使用

大規模な集中ネットワークでは、ロードバランサを使用する必要があります。これにより、AAAクライアントのデプロイメントが簡素化されます。ロードバランサを使用するには、AAAサーバーのエントリが1つだけ必要です。ロードバランサは、利用可能なサーバーへのAAA要求のルーティングを最適化します。

ただし、ロードバランサが1つだけしかない場合、シングルポイント障害が発生する可能性があります。この問題を回避するために、2つのロードバランサを導入し、冗長性とフェールオーバーを実現します。この構成では、各AAAクライアントで2つのAAAサーバーエントリを設定する必要があります（この設定は、ネットワーク全体で同じになります）。

図 4: ロードバランサを使用した Cisco ISE での大規模なネットワークデプロイメント



282064

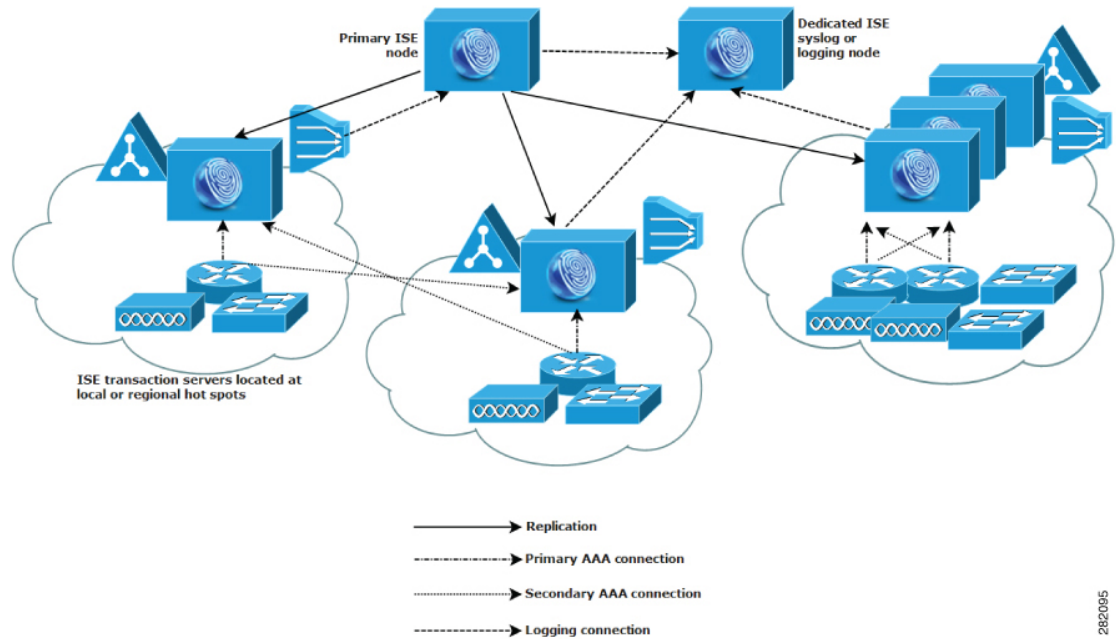
## Cisco ISE での分散ネットワークデプロイメント

分散 Cisco ISE ネットワーク デプロイメントは、主要な拠点があり、他の場所に地域、全国、またはサテライトの拠点がある組織に最も役に立ちます。主要な拠点は、プライマリ ネットワークが存在し、追加の LAN に接続される小規模～大規模な場所であり、異なる地域や距離が離れた場所のアプライアンスとユーザーをサポートします。

大規模なリモートサイトでは最適な AAA パフォーマンスのために独自の AAA のインフラストラクチャを持つことができます。集中管理モデルにより、同一の同期された AAA ポリシー

が保持されます。集中設定モデルでは、プライマリ Cisco ISE ノードとセカンダリ Cisco ISE ノードを使用します。Cisco ISE ノードで個別の監視ペルソナを使用することを推奨しますが、リモートの場所それぞれで独自の固有なネットワーク要件を満たす必要があります。

図 5: Cisco ISE での分散ネットワークデプロイメント



282095

## 複数のリモートサイトがあるネットワークを計画する際の考慮事項

- Microsoft Active Directory や Lightweight Directory Access Protocol (LDAP) などの中央または外部データベースが使用されているかどうかを確認します。AAA のパフォーマンスを最適化するために、各リモートサイトでは Cisco ISE がアクセスできる外部データベースの同期されたインスタンスが必要です。
- AAA クライアントの場所は重要です。ネットワーク遅延の影響と WAN 障害により引き起こされるアクセス損失の可能性を減らすために、Cisco ISE ノードを AAA クライアントのできるだけ近くに配置する必要があります。
- Cisco ISE では、バックアップなどの一部の機能にコンソールからアクセスできます。各サイトでターミナルを使用して、各ノードへのネットワークアクセスをバイパスする直接的で安全なコンソールアクセスを行うことができます。
- 小規模な場合は、リモートサイトが近くにあるため、他のサイトに信頼できる WAN 接続を行うことができます。また、冗長性を提供するために、ローカルサイトのバックアップとして Cisco ISE ノードを使用できます。
- 外部データベースに確実にアクセスできるようにするために、すべての Cisco ISE ノードでドメインネームシステム (DNS) を適切に設定する必要があります。

## Cisco ISE 展開のサイズ設定ガイドライン

展開のサイズ設定ガイドラインおよびさまざまなタイプの Cisco ISE 展開のスケール制限の詳細については、『[Performance and Scalability Guide for Cisco Identity Services Engine](#)』を参照してください。

## Cisco ISE のサポートに必要なスイッチおよびワイヤレス LAN コントローラの設定

Cisco ISE がネットワーク スイッチと相互運用することができ、Cisco ISE の機能がネットワーク セグメント全体で正常に使用できるよう保証するためには、ご使用のネットワーク スイッチを、必要とされる特定のネットワーク タイム プロトコル (NTP)、RADIUS/AAA、IEEE 802.1X、MAC 認証バイパス (MAB) などの設定を使用して設定する必要があります。

### [ISE Community Resource](#)

WLC 付き Cisco ISE の設定については、[Cisco ISE with WLC Setup Video](#) を参照してください。



## 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。