Cisco ISE のネットワーク デプロイメント

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 デプロイメントの用語

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、次のペルソナ：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 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ノード
- 自動フェールオーバー用の 1 組のモニタリング 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、およびアカウンティ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。

モニタリング ノード

モニタリング 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 モニタリング ノードおよびセカンダリ モニタリング 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 モニタリング ノードがダウンした場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング 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、モニタリング ノードはモニタ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 の分散デプロイメント環境では、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、デプロイメント環境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

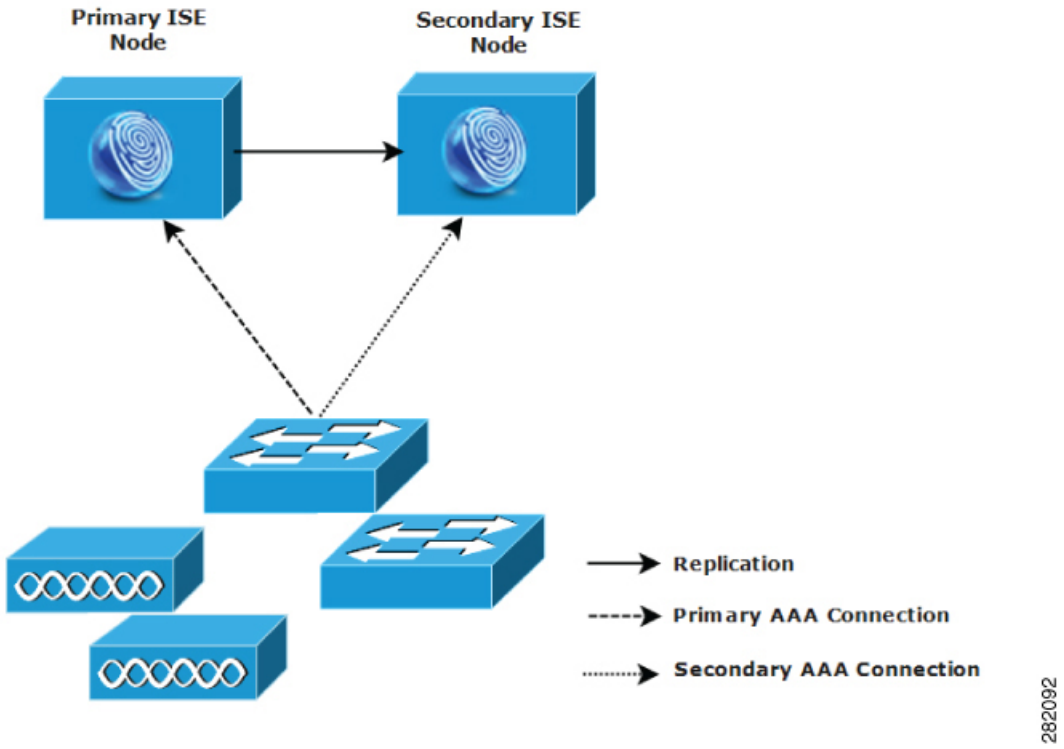
小規模のネットワーク デプロイメント

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、アカウンティング（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*：小規模のネットワーク デプロイメント



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、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

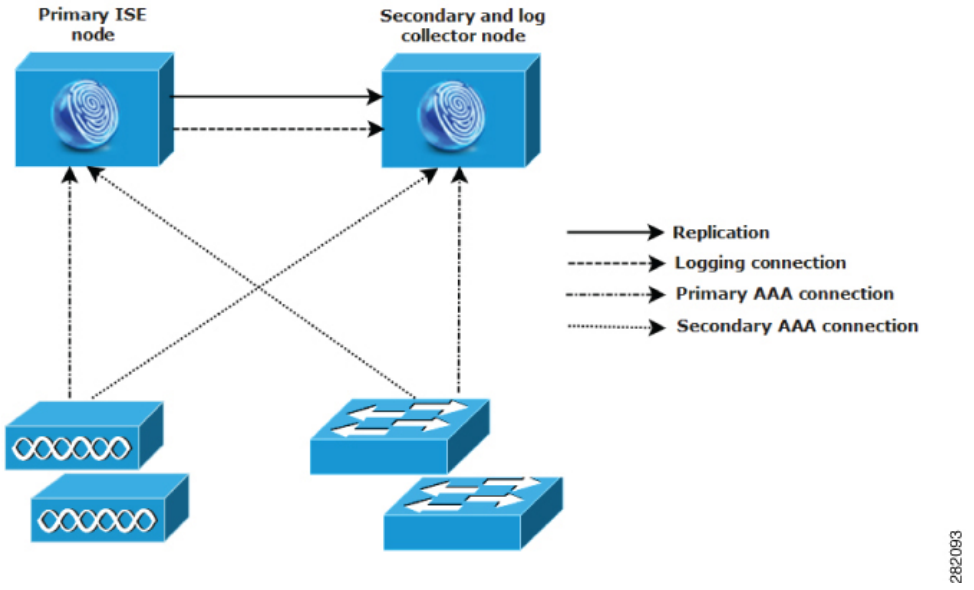
分割 Cisco ISE デプロイメント環境でも、小規模な Cisco ISE デプロイメント環境で説明したように、プライマリ ノードとセカンダリ ノードを維持することができます。ただし、AAA ロードは、AAA ワークフローを最適化するためにこの 2 つの Cisco ISE ノード間で分割されます。AAA 接続で問題がある場合は、各 Cisco ISE アプライアンス（プライマリまたはセカンダリ）がすべてのワークロードを処理できる必要があります。通常のネットワーク運用では、プライマリ ノードとセカンダリ ノードのどちらもすべての AAA 要求を処理することはできません。これは、このワークロードがこの 2 つのノード間で分散されているためです。

このようにロードを分割できるため、システムの各 Cisco ISE ノードに対する負荷は減少します。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 のデプロイメント環境では、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、アカウンティング 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:* 分割ネットワーク デプロイメント



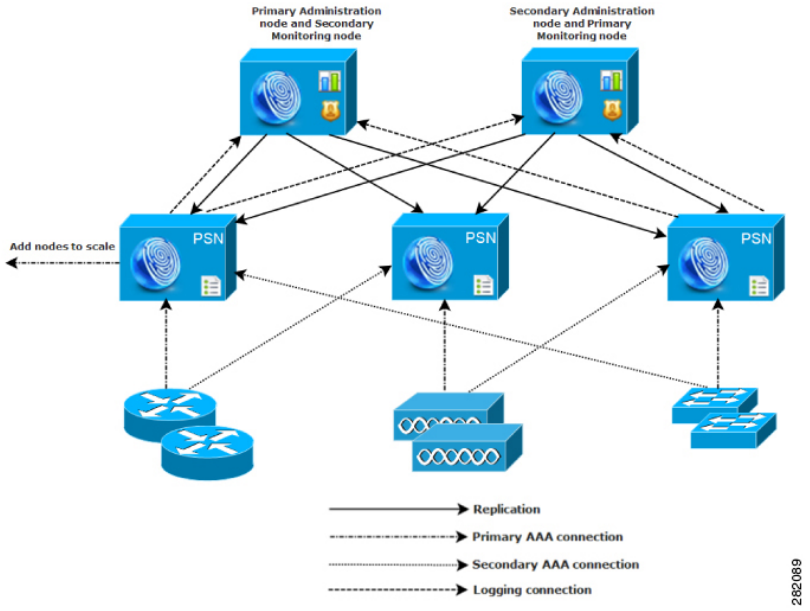
中規模のネットワーク デプロイメント

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ギング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*：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リング ペルソナ（モニタ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 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。

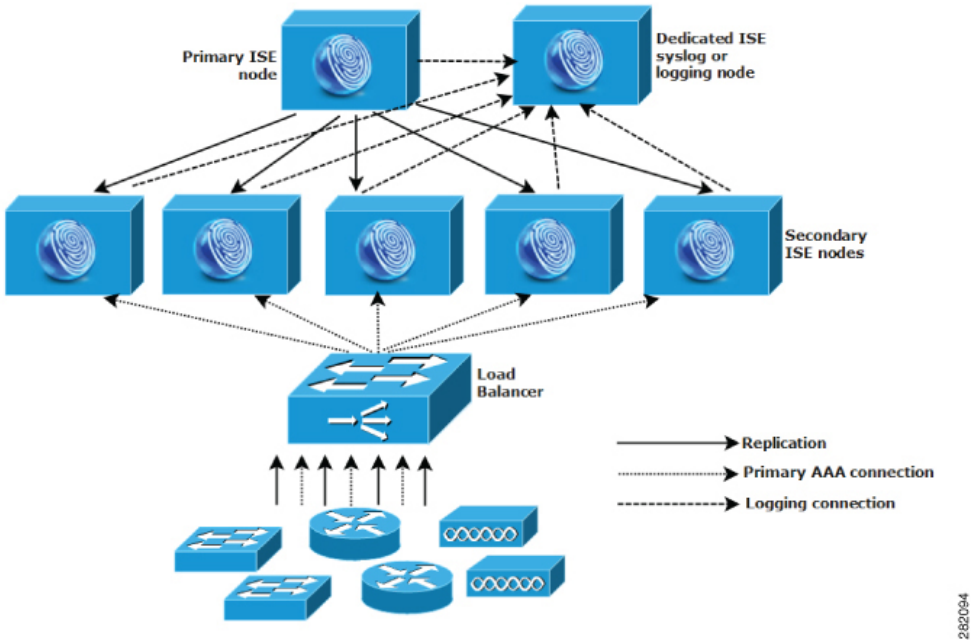
また、アプライアンスが Cisco ISE ノードの監視ペルソナと汎用 syslog サーバの両方にログを送信するよう設定することもできます。汎用 syslog サーバを追加することにより、Cisco ISE ノード上の監視ペルソナがダウンした場合に冗長なバックアップが提供されます。

ロード バランサ

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 つだけしかないと、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デプロイし、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 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:* 大規模のネットワーク デプロイメント

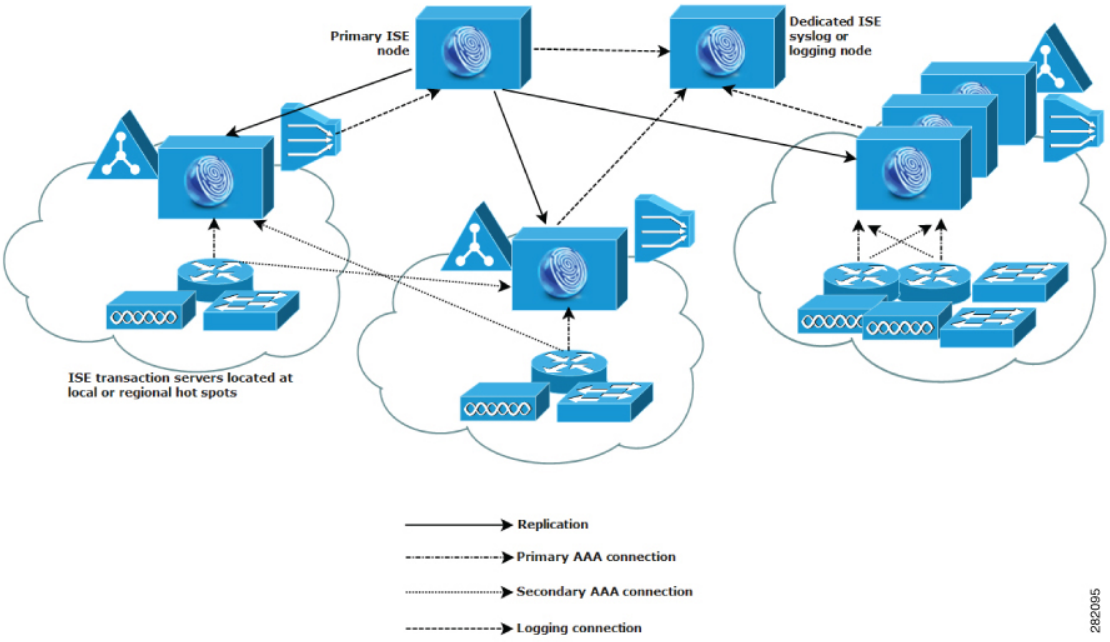


分散されたネットワーク デプロイメント

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:* 分散デプロイメント



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 接続を行えます。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。

各デプロイメントモデルでサポートされるセッションの最大数

次の表に、各デプロイメント モデルでサポートされるセッションの最大数を示します。

表 *1:* デプロイメント モデルごとにサポートされる最大セッション数

デプロイメント モデル	プラットフォーム	最大セッション数
スタンドアロン（単一ノード上のすべてのペルソナ）	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
基本的な 2 ノード デプロイメント（冗長）	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
ハイブリッド分散型デプロイメント（同一アプライアンス上の Admin および MnT、専用アプライアンスのポリシー サービス）	PAN と MnT としての 3615	10,000
	PAN と MnT としての 3655	25,000
	PAN と MnT としての 3695	50,000
	PAN と MnT としての 3515	7,500
	PAN と MnT としての 3595	20,000

デプロイメント モデル	プラットフォーム	最大セッション数
専用（PAN、MnT、PXG、および PSN ノード）	PAN と MnT としての 3595	500,000
	PAN と MnT としての 3655	500,000
	PAN/MnT としての 3695	2,000,000

表 *2:* 最大アクティブ セッション数（*PSN* あたり）

PSN[1]	最大アクティブ セッション数
SNS 3615	10,000
SNS 3655	50,000
SNS 3695	100,000
SNS 3515	7,500
SNS 3595	40,000

[1] 専用ポリシー ノードごとのスケーリング（合計デプロイメント サイズでゲートされる最大セッション数）

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。