



ISE-PIC の概要

不正な脅威からネットワークを保護するには、ユーザアイデンティティを認証する必要があります。これを行うために、セキュリティ製品がネットワークに実装されます。各セキュリティ製品には必要な認証を取得する独自の方法があり、多くの場合は、認証されたユーザではなく、認証された IP アドレスを識別します。その結果、これらの製品は、ユーザログイン情報に基づいて認証を実行するさまざまな外部サーバと方式を参照し、分散型ネットワークを実現します。Cisco Identity Services Engine (ISE) の Passive Identity Connector (ISE-PIC) は、集中管理されたインストールと実装を提供し、さまざまな送信元からパッシブ認証データを簡単に収集し、それらのアイデンティティをセキュリティ製品のサブスクリバと共有できるようにします。

- [Cisco ISE-PIC の用語 \(1 ページ\)](#)
- [ISE-PIC 概要 \(3 ページ\)](#)
- [Cisco ISE-PIC のアーキテクチャ、展開、およびノード \(4 ページ\)](#)
- [の利点 ISE-PIC \(5 ページ\)](#)
- [ISE および CDA と ISE-PIC の比較 \(5 ページ\)](#)

Cisco ISE-PIC の用語

このガイドでは、Cisco ISE-PIC について説明する際に次の用語を使用します。

用語	定義
GUI	グラフィック ユーザ インターフェイス GUI は、ISE-PIC のソフトウェアインストールのすべての画面とタブを示します。
NIC	ネットワーク インターフェイス カード。
ノード	個別の物理または仮想の Cisco ISE-PIC アプリアンス。

用語	定義
PAN	ISE-PIC展開のメインノードはプライマリ管理ノード（PAN）であり、使用可能なすべてのアクションを実行できるノードです。ISE-PICでは、最大2つのノードをインストールできます。インストールする2番目のノードは、セカンダリ管理ノード（セカンダリ PAN）と呼ばれます。
パーサー	syslog メッセージを受信し、その入力を分割して管理、マッピング、および ISE-PIC にパブリッシュできる ISE-PIC のバックエンドコンポーネント。パーサーは、到着する syslog メッセージの各行の情報を調べて、重要な情報を探します。たとえば、「mac=」を検索するようにパーサーが設定されている場合、パーサーはそのフレーズを検索しながら各行を解析します。パーサーは、設定された主要なフレーズを検出すると、定義された情報を ISE に送信するように設定されています。
プライマリ ノード	ISE-PIC展開のメインノードはプライマリ管理ノード（PAN）であり、使用可能なすべてのアクションを実行できるノードです。ISE-PICでは、最大2つのノードをインストールできます。インストールする2番目のノードは、セカンダリ管理ノード（セカンダリ PAN）と呼ばれます。
プローブ	プローブは特定の送信元からデータを収集するメカニズムです。プローブは任意のメカニズムを説明する一般的な用語ですが、データの収集方法や収集対象を具体的に説明するものではありません。たとえば、Active Directory（AD）のプローブは ISE-PIC が AD からデータを収集するのに役立ちますが、syslog のプローブは syslog メッセージを読み取るパーサーからデータを収集します。
プロバイダー	ISE-PIC がユーザアイデンティティ情報を受信し、マッピングし、公開するクライアントまたは送信元です。

用語	定義
セカンダリ ノード	ISE-PIC 展開のメインノードはプライマリ管理ノード (PAN) であり、使用可能なすべてのアクションを実行できるノードです。ISE-PIC では、最大 2 つのノードをインストールできます。インストールする 2 番目のノードは、セカンダリ管理ノード (セカンダリ PAN) と呼ばれます。
サブスクリバ	ユーザアイデンティティ情報を受信するために ISE-PIC サービスをサブスクライブするシステム。

ISE-PIC 概要

パッシブ ID コネクタ (ISE-PIC) は一元的なワンストップインストールおよび実装を提供します。これにより、ユーザ ID 情報を受信してさまざまなセキュリティ製品 (Cisco Firepower Management Center (FMC) や Stealthwatch など) のサブスクリバと共有するように、ネットワークを容易に設定できます。パッシブ ID の完全なブローカとして、ISE-PIC はさまざまなプロバイダーソース (Active Directory ドメインコントローラ (AD DC) など) からユーザ ID を収集し、ユーザ ログイン情報を使用中の該当する IP アドレスにマッピングし、そのマッピング情報を、設定されているサブスクリバセキュリティ製品と共有します。

パッシブ ID について

認証、許可、およびアカウントリング (AAA) サーバを提供し、802.1X や Web 認証などのテクノロジーを使用する Cisco Identity Services Engine (ISE) などの製品は、ユーザまたはエンドポイントと直接通信し、ネットワークへのアクセスを要求し、ログインクレデンシャルを使用して ID を検証およびアクティブに認証します。

パッシブ ID サービスはユーザを直接認証するのではなく、プロバイダーと呼ばれる Active Directory などの外部認証サーバからユーザ ID および IP アドレスを収集し、サブスクリバとこの情報を共有します。ISE-PIC は、通常、ユーザのログインとパスワードに基づいてプロバイダーからユーザ ID 情報を受信し、ユーザ ID および関連する IP アドレスを照合するために必要な確認とサービスを実行し、認証済み IP アドレスをサブスクリバに提供します。

Passive Identity Connector (ISE-PIC) のフロー

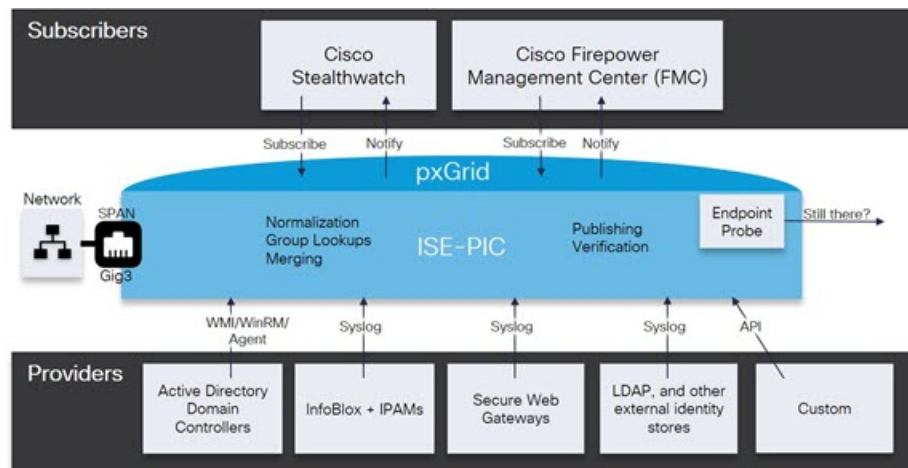
ISE-PIC のフローは次のとおり。

1. プロバイダーがユーザまたはエンドポイントの認証を実行します。
2. プロバイダーが認証済みのユーザ情報を ISE-PIC に送信します。
3. ISE-PIC によりユーザ情報の正規化、ルックアップ、マージ、解析、および IP アドレスへのマッピングが行われ、マッピングされた詳細情報が pxGrid に対して公開されます。

4. pxGrid サブスクリバはマッピングされたユーザの詳細情報を受信します。

次の図に、ISE-PIC の全体的なフローを示します。

図 1: 全体的なフロー



Cisco ISE-PIC のアーキテクチャ、展開、およびノード

Cisco ISE-PIC 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 : Cisco ISE-PIC では、次に示すように、最大 2 つのノードを設定できます。
- ネットワーク リソース
- エンドポイント

展開内の Cisco ISE-PIC ノードが 1 つの場合は「スタンドアロン展開」と呼ばれます。

Cisco ISE-PIC ノードを 2 つ含む展開は「ハイアベイラビリティ展開」と呼ばれ、1 つのノードがプライマリプライアンス（プライマリ管理ノード、または PAN）として機能します。ハイアベイラビリティ展開により、サービスの可用性が向上します。

PAN は、このネットワーク モデルに必要なすべての設定を提供し、セカンダリ Cisco ISE ノード（セカンダリ PAN）はバックアップロールで機能します。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の接続が失われるたびに機能を再開します。

Cisco ISE-PIC は、セカンダリノードがプライマリノードの状態と一致するように（したがって、バックアップとして使用できるように）、プライマリ Cisco ISE-PIC ノードが存在するコンテンツのすべてをセカンダリ ISE-PIC ノードと同期するか、複製します。

ISE Community Resource

展開とスケーリングの詳細については、「[ISE Deployment Journey](#)」を参照してください。

の利点 ISE-PIC

ISE-PIC が提供するもの：

- さまざまなプロバイダーと連携する単一のアイデンティティ ソリューション。
- 設定、モニタリング、トラブルシューティングをシンプルにする使いやすい GUI
- シンプルなインストールと設定
- アクティブ認証用に ISE へ簡単にアップグレード。ISE-PIC から完全な ISE 展開へアップグレードし、ISE-PIC ノードを使用してスタンドアロン ISE 展開を作成するか、またはこのノードをプライマリノードとして既存の展開に追加すると、ISE はアップグレード前に ISE-PIC で使用可能だったすべての機能を引き続き提供し、既存の設定は保持されます。



(注) ISE にアップグレードするには、トライアルバージョンをダウンロードするか、またはライセンスのオプションについてシスコの担当者にお問い合わせください。

プライマリノードとしてではなく、既存の ISE 展開にアップグレードした ISE-PIC を追加すると、以前の ISE-PIC は上書きされます。

アップグレードフローの詳細については、[完全な ISE インストールへの ISE-PIC のアップグレード](#)を参照してください。

ISE および CDA と ISE-PIC の比較

ISE-PIC には、ISE へのスムーズかつ容易なアップグレード機能などのさまざまな利点があります。ISE-PIC と ISE の他に、追加のセキュリティメカニズムとして CDA が提供されています。3つの製品の違いを次に示す表で説明します。

- [ISE-PIC と ISE の詳細な比較 \(5 ページ\)](#)
- [ISE-PIC と ISE および CDA の比較の概要 \(8 ページ\)](#)

ISE-PIC と ISE の詳細な比較

ISE-PIC はパッシブ ID だけを共有し、許可サービスまたは認証サービスは提供しません。これらのサービスは、認証、許可、およびアカウントिंग (AAA) サーバを提供する ISE により提供されます。2つの製品の相違点について、次の表で詳しく説明します。

表 1: ISE-PIC と ISE の比較

カテゴリ (Category)	機能	ISE-PIC	ISE
スマート ライセンス		—	√
認証タイプと許可タイプ	許可ポリシー	—	√
	TrustSec	—	√
	Active Directory パッシブ認証 (WMI を含む)	√	√
パッシブ ID ソース		√	√
	Easy Connect	—	√
	SysLog ソース	√	√
	REST API ソース	√	√
	SPAN	√	√
	Security Group eXchange Protocol (SXP)	—	√
	RADIUS (RADIUS プロキシを含む)	—	√
	BYOD	—	√
	ゲスト	—	√
	ポスチャ (Posture)	—	√
	デバイス管理 (TACACS+)	—	√
pxGrid	pxGrid コントローラ	√ Cisco サブスクライバ専用	√
	pxGrid コントローラ冗長性	√	√
	トピックの拡張性	—	√

カテゴリ (Category)	機能	ISE-PIC	ISE
証明局 (CA)	pxGrid 証明書テンプレート	√	√
	エンドポイント CA	—	√
	Enrollment over secure transport (EST)	—	√
	その他の証明書テンプレート	—	√
可視性とコンテキスト	コンテキストディレクトリ	—	√
	プロファイリング	—	√
レポート		! (注) ISE-PIC に用意されているレポートを使用して、システムの正常性をモニタし、ネットワーク内の問題のトラブルシューティングを行うことができます。ただし、ISE と比較すると ISE-PIC では一部の機能だけが提供されるため、ISE-PIC. では一部の ISE レポートが使用できません。	√

ISE-PIC と ISE および CDA の比較の概要

CDA は IP アドレスをユーザ名にマッピングするメカニズムです。CDA により、セキュリティゲートウェイはどのユーザがネットワーク上のどの IP アドレスを使用しているかを認識でき、これらのユーザ（またはユーザが属するグループ）に基づいて決定を下すことができます。ただし、ISE-PIC は、ユーザ名、MAC アドレス、ポートなどの追加データにアクセスしてより正確にユーザ ID を収集します。次の表に ISE-PIC、ISE、および CDA の比較の概要を示します。

表 2: ISE および CDA と ISE-PIC の比較

パッシブ認証の詳細	完全な ISE	ISE-PIC	CDA
ドメインコントローラの数	100	100	80
サブスクライバの数	20	20	—
WMI (エージェントレス)	○	○	○
Windows サーバエージェントが使用可能	○	○	—
DCOM が必要	いいえ (SPAN)	いいえ (SPAN)	あり
Easy Connect	○	—	—
SPAN を使用した Kerberos スニフィング	○	○	—
バインド (IP アドレス、MAC アドレス、ユーザ名)	300,000	300,000	64,000