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、ユーザー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、認証されたユーザーではなく、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、ユーザー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ーと方式を参照し、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ライバと共有できるようにします。

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 ユーザー 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 アプライアンス。

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 がユーザー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。
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。
サブスクライバ	ユーザー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、ユーザー 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）のサブスクライ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）からユーザー ID を収集し、ユーザー 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ライバ セキュリティ製品と共有します。

（注） ISE で検証されている FMC および Stealthwatch のリリースについては、『Cisco Identity Services Engine Network Component Compatibility』を参照してください。

パッシブ ID について

認証、許可、およびアカウンティング（AAA）サーバーを提供し、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、ユーザー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 サービスはユーザー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ーからユーザー ID および IP アドレスを収集し、サブスクライバとこの情報を共有します。ISE-PICは、通常、ユーザー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ー ID 情報を受信し、ユーザー 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ライバに提供します。

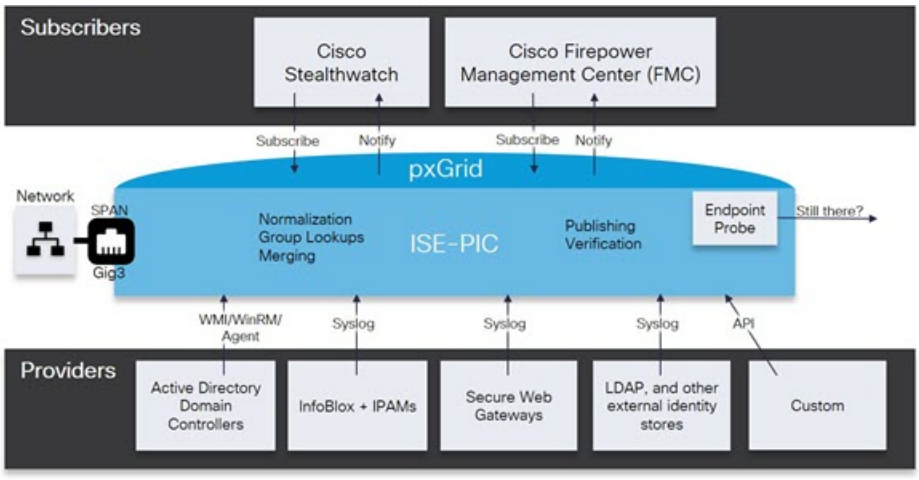
Passive Identity Connector（ISE-PIC）のフロー

ISE-PIC のフローは次のとおりです。

1. プロバイダーがユーザー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ー情報を ISE-PIC に送信します。
3. ISE-PIC によりユーザー情報の正規化、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 サブスクライバはマッピングされたユーザー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アプライアンス（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。

（注） Cisco ISE リリース 3.1 以降、すべての pxGrid 接続は pxGrid 2.0 に基づいている必要があります。pxGrid 1.0 ベース（XMPP ベース）の統合は、リリース 3.1 以降、Cisco ISE で機能しなくなります。

WebSocket に基づく pxGrid バージョン 2.0 は、Cisco ISE リリース 2.4 で導入されました。統合の中断を防ぐために、他のシステムを計画して pxGrid 2.0 準拠バージョンにアップグレードすることをお勧めします。

ISE-PICの利点

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-PIC と Cisco ISE および Cisco Context Directory Agent の比較

ISE-PIC には、Cisco 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 Cisco ISE の他に、シスコでは追加のセキュリティメカニズムとして Cisco

Context Directory Agent（CDA）を提供しています。3 つの製品の違いを次に示す表で説明します。

• ISE-PIC と Cisco ISE の詳細な比較 （6 ページ）
• ISE-PIC と Cisco ISE および CDA の比較の概要 （8 ページ）

ISE-PIC と Cisco 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、およびアカウンティング（AAA）サーバーを提供する 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 *Cisco ISE* の比較

カテゴリ	機能	ISE-PIC	Cisco 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	—	√
	デバイス管理（TACACS+）	—	√

カテゴリ	機能	ISE-PIC	Cisco ISE
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	—	√
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	—	√

カテゴリ	機能	ISE-PIC	Cisco ISE
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ーし、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 Cisco ISE および CDA の比較の概要

Cisco Context Directory Agent（CDA）は IP アドレスをユーザー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ー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、これらのユーザー（またはユーザーが属するグループ）に基づいて決定を下すことができます。ただし、ISE-PIC は、ユーザー名、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ーアイデンティティを収集します。次の表に ISE-PIC、Cisco ISE、および CDA の比較の概要を示します。

表 *2 : ISE-PIC* と *Cisco ISE* および *CDA* 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）	対応	対応	対応
Windows サーバーエージェントが使用可能	対応	対応	—
DCOM が必要	いいえ（SPAN）	いいえ（SPAN）	あり
Easy Connect	対応	—	—
SPAN を使用した Kerberos スニフィング	対応	対応	—
バインド（IP アドレス、MAC アドレス、ユーザー名）	300,000	300,000	64,000

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。