Cisco ISE ポート リファレンス

Cisco ISE すべてのペルソナ ノード ポート

表 *1:* すべてのノードで使用されるポート

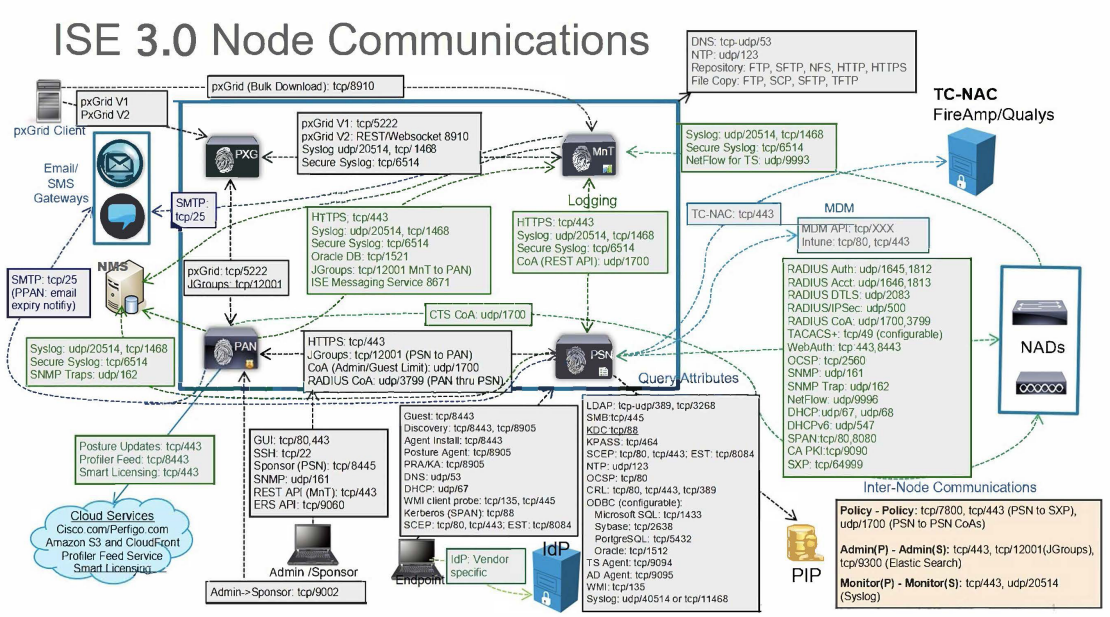
Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
複製および同期	• HTTPS（SOAP）：TCP/443 • データの同期/レプリケーション（JGroups）：TCP/12001（グローバル） • ISE メッセージング サービス：SSL：TCP/8671 • プロファイラエンドポイント所有権の同期/レプリケーション：TCP/6379	—

Cisco ISE インフラストラクチャ

この付録では、Cisco ISE が外部アプリケーションやデバイスとのイントラネットワーク通信に使用する、TCP および User Datagram Protocol（UDP）のポートの一覧を示します。この付録に示される Cisco ISE ポートが、対応するファイアウォールでオープンになっている必要があります。

Cisco ISE ネットワークでサービスを設定する場合は、次の情報に注意してください。

- ポートは、展開で有効になっているサービスに基づいて有効になります。ISE で実行中のサービスによって開かれるポートは別として、Cisco ISE は他のすべてのポートへのアクセスを拒否します。
- Cisco ISE 管理は、ギガビット イーサネット 0 でのみ使用できます。
- RADIUS はすべてのネットワーク インターフェイス カード（NIC）でリッスンします。
- Cisco ISE サーバー インターフェイスは VLAN タギングをサポートしていません。ハードウェア アプライアンス上にインストールする場合は、Cisco ISE ノードへの接続に使用するスイッチ ポートの VLAN トランキングを無効にし、アクセス レイヤ ポートとして設定してください。
- 一時ポート範囲は 10000 ー 65500 です。これは、Cisco ISE リリース 2.1 以降でも同じです。
- VMware on Cloud は、サイト間 VPN ネットワーク構成でサポートされます。したがって、ネットワーク アクセス デバイスおよびクライアントから Cisco ISE への IP アドレスまたはポートの到達可能性は、NAT またはポートフィルタリングを使用せずに確立する必要があります。
- すべての NIC が IP アドレスを使用して設定できます。
- 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。



関連コンセプト

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

（注） ISE の TCP キープアライブ時間は 60 分です。ISE ノード間にファイアウォールが存在する場合は、そのファイアウォールに応じて TCP タイムアウト値を調整します。

Cisco ISE 管理ノードのポート

次の表に、管理ノードが使用するポートを示します。

表 *2:* 管理ノードが使用するポート

Cisco ISE サービス	ギガビット イーサネット **0** またはボンド **0** のポート	その他のイーサネット インターフェイス（ギガビット イーサネット **1** ～ **5**、またはボンド **1** および **2**）のポート
管理		—

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
	• HTTP：TCP/80、HTTPS：TCP/443（TCP/443 にリダイレクトされた TCP/80。設定不可） • SSH サーバー：TCP/22 • CoA • 外部 RESTful サービス（ERS）REST API：TCP/9060 • • 管理者 GUI からのゲストアカウントの管理：TCP/9002 • ElasticSearch（コンテキストの可視性、プライマリからセカンダリ管理者ノードへのデータのレプリケート）：TCP/9300 （注） ポート 80 および 443 は、管理 Web アプリケーションをサポートしていて、デフォルトで有効になっています。 ギガビット イーサネット 0 では、Cisco ISE への HTTPS および SSH アクセスは制限されています。 TCP/9300 は、着信トラフィックに対しプライマリとセカンダリ両方の管理ノードで開いている必要があります。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
モニターリング	• SNMP クエリー：UDP/161 （注） このポートは、ルート テーブルによって異なります。 • ICMP	
ロギング（アウトバウンド）	• syslog：UDP/20514、TCP/1468 • セキュア syslog：TCP/6514 （注） デフォルト ポートは外部ロギング用に設定できます。 • SNMP トラップ：UDP/162	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 および 2）のポート
外部 ID ソースおよびリソース（アウトバウンド）	• 管理ユーザー インターフェイスおよびエンドポイント認証： • LDAP：TCP/389、3268、UDP/389 • SMB：TCP/445 • KDC：TCP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： （注） ODBC ポートはサードパーティ データベース サーバーで設定できます。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521、 • NTP：UDP/123 • DNS：UDP/53、TCP/53 （注） ギガビット イーサネット 0 インターフェイス以外のインターフェイスのみから到達可能な外部のアイデンティティ ソースおよびサービス用に、適切にスタティック ルートを設定します。	
電子メール	ゲスト アカウントおよびユーザー パスワードの有効期限の電子メール通知：SMTP：TCP/25	
スマート ライセンス	TCP/443 経由のシスコのクラウドへの接続 TCP/443 と ICMP を介した SSM オンプレミス サーバーへの接続	

Cisco ISE モニターリング ノードのポート

次の表に、モニターリング ノードが使用するポートを示します。

表 *3:* モニターリング ノードが使用するポート

Cisco ISE サービス	**ギガビット イーサネット 0 またはボンド 0 のポート**	**その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート**
管理	• HTTP：TCP/80、HTTPS：TCP/443 • SSH サーバー：TCP/22	—
モニターリング	Simple Network Management Protocol [SNMP]：UDP/161 （注） このポートは、ルート テーブルによって異なります。 • ICMP	
ログ	• syslog：UDP/20514、TCP/1468 • セキュア syslog：TCP/6514 （注） デフォルト ポートは外部ロギング用に設定できます。 • SMTP：アラームの電子メール用の TCP/25 • SNMP トラップ：UDP/162	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
外部 ID ソースおよびリソース（アウトバウンド）	• 管理ユーザー インターフェイスおよびエンドポイント認証： • LDAP：TCP/389、3268、UDP/389 • SMB：TCP/445 • KDC：TCP/88、UDP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： （注） ODBC ポートはサードパーティ データベース サーバーで設定できます。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521、15723、16820 • NTP：UDP/123 • DNS：UDP/53、TCP/53 （注） ギガビット イーサネット 0 インターフェイス以外のインターフェイスのみから到達可能な外部のアイデンティティ ソースおよびサービス用に、適切にスタティック ルートを設定します。	
インバウンド通信に使用されるポート	• MnT REST API のルーティングのために有効になっている ISE API ゲートウェイを持つ ISE ノードからの MnT インバウンド通信：TCP/9443 • PAN からのグローバル検索：TCP/1521 （注） これらのポートは、オンプレミスかクラウドかに関係なく、すべてのタイプの展開で必要です。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
pxGrid の一括ダウンロード	SSL：TCP/8910	

Cisco ISE ポリシー サービス ノードのポート

Cisco ISE はセキュリティを強化するために HTTP Strict Transport Security（HSTS）をサポートしています。Cisco ISE は、HTTPS を使用してのみアクセスできるブラウザを示す HTTPS 応答を送信します。ユーザーが HTTPS ではなく HTTP を使用して ISE にアクセスしようとすると、ブラウザはネットワーク トラフィックを生成する前に接続を HTTPS に変更します。この機能により、ブラウザが暗号化されていない HTTP を使用して要求を Cisco ISE に送信することがなくなり、サーバーは暗号化された要求をリダイレクトできるようになります。

次の表に、ポリシー サービス ノードが使用するポートを示します。

表 *4:* ポリシー サービス ノードが使用するポート

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
管理	• HTTP：TCP/80、HTTPS：TCP/443 • SSH サーバー：TCP/22 • OCSP：TCP/2560	Cisco ISE 管理は、ギガビット イーサネット 0 でのみ使用できます。
クラスタリング（ノード グループ）	ノード グループ/JGroups：TCP/7800	—
SCEP	TCP/9090	—
IPSec/ISAKMP	UDP/500	—
デバイス管理	TACACS+：TCP/49 （注） このポートは、リリース 2.1 以降のリリースで設定できます。	
TrustSec	HTTP と Cisco ISE REST API を使用して、ポート 9063 を介して TrustSec データをネットワークデバイスに転送します。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
SXP	• PSN（SXP ノード）から NAD：TCP/64999 • PSN から SXP へ（ノード間通信）： TCP/9644	
TC-NAC	TCP/443	
モニターリング	Simple Network Management Protocol [SNMP]：UDP/161 （注） このポートは、ルート テーブルによって異なります。	
ロギング（アウトバウンド）	• syslog：UDP/20514、TCP/1468 • セキュア syslog：TCP/6514 （注） デフォルト ポートは外部ロギング用に設定できます。 • SNMP トラップ：UDP/162	
セッション	• RADIUS 認証：UDP/1645、1812 • RADIUS アカウンティング：UDP/1646、1813 • RADIUS DTLS 認証/アカウンティング：UDP/2083 • RADIUS 許可変更（CoA）送信：UDP/1700 • RADIUS 許可変更（CoA）リッスン/リレー：UDP/1700、3799 （注） UDP ポート 3799 は、設定できません。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
外部 ID ソースおよびリソース（アウトバウンド）	• 管理ユーザーインターフェイスおよびエンドポイント認証： • LDAP：TCP/389、3268 • SMB：TCP/445 • KDC：TCP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： （注） ODBC ポートはサードパーティ データベース サーバーで設定できます。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521 • NTP：UDP/123 • DNS：UDP/53、TCP/53 （注） ギガビット イーサネット 0 インターフェイス以外のインターフェイスのみから到達可能な外部のアイデンティティ ソースおよびサービス用に、適切にスタティック ルートを設定します。	
パッシブ ID（インバウンド）	• TS エージェント：TCP/9094 • AD エージェント：TCP/9095 • syslog：UDP/40514、TCP/11468	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
Web ポータル サービス： - ゲスト/Web 認証 - ゲスト スポンサー ポータル - デバイス ポータル - クライアントのプロビジョニング - 証明書のプロビジョニング - ブロックリストポータル	HTTPS（インターフェイスは Cisco ISE のサービスに対して有効にする必要があります）： • ブロックリストポータル：TCP/8000-8999（デフォルトポートは TCP/8444 ） • ゲストポータルおよびクライアントのプロビジョニング：TCP/8000-8999（デフォルトポートは TCP/8443） • 証明書のプロビジョニングポータル：TCP/8000-8999（デフォルトポートは TCP/8443 ） • デバイスポータル：TCP/8000-8999（デフォルトポートは TCP/8443） • スポンサーポータル：TCP/8000-8999（デフォルトポートは TCP/8443） • ゲストとスポンサーのポータルからの SMTP ゲストの通知：TCP/25	
ポスチャ - 検出 - プロビジョニング - アセスメント/ハートビート	• 検出（クライアント側）：TCP/80（HTTP）、TCP/8905（HTTPS） （注） デフォルトでは、TCP/80 は TCP/8443 にリダイレクトされます。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 Cisco ISE は、TCP ポート 8905 のポスチャおよびクライアント プロビジョニングの管理証明書を提示します。 Cisco ISE は、TCP ポート 8443（またはポータルで使用するために設定したポート）のポータル証明書を提示します。 • 検出（ポリシー サービス ノード側）：TCP/8443、8905（HTTPS） AnyConnect リリース 4.4 以降が搭載された Cisco ISE リリース 2.2 以降から、このポートは設定可能です。	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
個人所有デバイスの持ち込み（BYOD）/ネットワーク サービス プロトコル（NSP） - リダイレクト - プロビジョニング - SCEP	• プロビジョニング - URL リダイレクト：「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • EST 認証付きの Android デバイスの場合：TCP/8084 Android デバイスの場合、ポート 8084 を リダイレクト ACL に追加する必要があります。 • プロビジョニング - ActiveX と Java アプレットのインストール（ウィザードのインストールの開始を含む）：「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • プロビジョニング - Cisco ISE からのウィザードのインストール（Windows および Mac OS）：TCP/8443 • プロビジョニング - Google Play（Android）からのウィザードのインストール：TCP/443 • プロビジョニング - サプリカントのプロビジョニング プロセス：TCP/8905 • CA への SCEP プロキシ：TCP/80 または TCP/443（SCEP RA URL の設定に基づく）	
モバイル デバイス管理（MDM）API の統合	• URL リダイレクト：「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • API：ベンダー固有 • エージェントのインストールおよびデバイスの登録：ベンダー固有	

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス、またはボンド 1 およびボンド 2
プロファイリング	• NetFlow：UDP/9996 （注） このポートは、設定可能です。 • DHCP：UDP/67 （注） このポートは、設定可能です。 • DHCP SPAN プローブ：UDP/68 • HTTP：TCP/80、8080 • DNS：UDP/53（ルックアップ） （注） このポートは、ルート テーブルによって異なります。 • SNMP クエリー：UDP/161 （注） このポートは、ルート テーブルによって異なります。 • SNMP トラップ：UDP/162 （注） このポートは、設定可能です。	

Cisco ISE pxGrid サービス ポート

次の表に、pxGrid サービス ノードが使用するポートを示します。

表 *5 : pxGrid* サービス ノードが使用するポート

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
管理	• SSL：TCP/5222（ノード間通信） • SSL：TCP/7400（ノード グループ通信）	—

Cisco ISE サービス	ギガビット イーサネット 0 またはボンド 0 のポート	その他のイーサネット インターフェイス（ギガビット イーサネット 1 ～ 5、またはボンド 1 およびボンド 2）のポート
pxGrid 登録者数	TCP/8910	

OCSP および CRL サービス ポート

Cisco ISE サービスおよびポートへの参照には Cisco ISE 管理ノード、ポリシー サービス ノード、モニターリング ノードで個別に使用される基本ポートが表示されますが、Online Certificate Status Protocol（OCSP）サービスおよび証明書失効リスト（CRL）の場合、ポートは CA サーバーまたは OCSP/CRL をホストするサービスによって異なります。

OCSP の場合、使用可能なデフォルト ポートは TCP 80 または TCP 443 です。Cisco ISE 管理者ポータルでは、OCSP サービス用の HTTP ベースの URL が予期されるため、TCP 80 がデフォルトです。デフォルト以外のポートも使用できます。

CRL の場合、デフォルトのプロトコルには、HTTP、HTTPS、および LDAP が含まれており、それぞれのデフォルト ポートは 80、443、および 389 になります。実際のポートは CRL サーバーで設定されます。

Cisco ISE プロセス

次の表に、Cisco ISE プロセスとそのサービスへの影響を示します。

プロセス名	説明	サービスへの影響
データベース リスナー	Oracle Enterprise データベース リスナー（Oracle Enterprise Database Listener）	すべてのサービスが正常に動作するには実行状態でなければならない
データベース サーバー	Oracle Enterprise データベース サーバー（Oracle Enterprise Database Server）。設定と処理データの両方を格納する	すべてのサービスが正常に動作するには実行状態でなければならない
アプリケーション サーバー（Application Server）	ISE 用メイン Tomcat サーバー	すべてのサービスが正常に動作するには実行状態でなければならない
Profiler データベース	ISE プロファイリング サービス用の Redis データベース	ISE プロファイリング サービスが正常に動作するには実行状態でなければならない

AD コネクタ	アクティブ ディレクトリ ランタイム	ISEがアクティブディレクトリ認証を実行するには実行状態でなければならない
MnT セッション データベース	MnT サービス用 Oracle TimesTen データベース	すべてのサービスが正常に動作するには実行状態でなければならない
MnT ログ コレクタ	MnT サービスのログ コレクタ	MnT 運用データのため実行状態でなければならない
MnT ログ プロセッサ	MnT サービスのログ プロセッサ	MnT 運用データのため実行状態でなければならない
証明書認証局サービス	ISE 内部 CA サービス	ISE 内部 CA が有効になっている場合は実行状態でなければならない

必要なインターネット URL

次の表に、特定の URL を使用する機能を示します。IP トラフィックが Cisco ISE とこれらのリソース間を移動できるように、ネットワークファイアウォールまたはプロキシサーバーのいずれかを設定する必要があります。リストされている URL にこのアクセスを提供できない場合は、関連付けられている機能が損なわれるか、または動作不能になります。

表 *6 :* 必要な *URL* アクセス

機能	URL
ポスチャの更新	https://www.cisco.com/ https://iseservice.cisco.com
フィードサービスのプロファイリング	https://ise.cisco.com
スマート ライセンス	https://tools.cisco.com
インタラクティブヘルプ	*.walkme.com *.walkmeusercontent.com