



## APPENDIX **E**

# Cisco ISE 3300 シリーズ アプライアンスの ポート リファレンス

---

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、伝送制御プロトコル (TCP) およびユーザ データグラム プロトコル (UDP) のポートの一覧を示します。

表 E-1 に、ポートの一覧を TCP および UDP のポート番号ごとに表示して、関連機能、サービス、またはプロトコルを示し、またすべての特定のポートに関連する情報を説明します。これは、4 つのギガビットイーサネットポート (GbEth0、GbEth1、GbEth2、および GbEth3) に適用されます。この表に示される Cisco ISE ポートは、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。ポートのリストは、ファイアウォールの設定、アクセス コントロール リスト (ACL) の作成、および Cisco ISE ネットワーク上でのサービスの設定の際に役立つ可能性のある情報を提供します。

表 E-1 Cisco ISE のサービスとポート

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
管理 ISE ノード	管理	<ul style="list-style-type: none"> <li>TCP : 22 (セキュア シェル [SSH] サーバ)</li> <li>TCP : 80<sup>1</sup> (HTTP)</li> <li>TCP : 443<sup>1</sup> (HTTPS)</li> </ul> <p>(注) ポート 80 は、ポート 443 にリダイレクトされます (設定不可)。</p> <p>(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、デフォルトでイネーブルになっています。</p>	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。	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。	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。
	複製および同期	<ul style="list-style-type: none"> <li>TCP : 443 (HTTPS SOAP)</li> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> <li>インターネット制御メッセージ プロトコル (ICMP) (ハートビート)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>
	監視	<ul style="list-style-type: none"> <li>UDP : 161 (Simple Network Management Protocol [SNMP] クエリー)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p>			

表 E-1 Cisco ISE のサービスとポート (続き)

Cisco ISE ノード	ISE サービス	ギガビットイーサネット 0 のポート	ギガビットイーサネット 1 のポート	ギガビットイーサネット 2 のポート	ギガビットイーサネット 3 のポート
モニタリング ISE ノード	管理	<ul style="list-style-type: none"> <li>TCP : 22 (SSH サーバ)</li> <li>TCP : 80<sup>1</sup> (HTTP)</li> <li>TCP : 443<sup>1</sup> (HTTPS)</li> </ul>			
	複製および同期	<ul style="list-style-type: none"> <li>TCP : 443 (HTTPS)</li> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> <li>ICMP (ハートビート)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>
	ロギング	<ul style="list-style-type: none"> <li>UDP : 20514 (syslog)</li> </ul> <p>(注) デフォルトポートは、外部ログ用に設定できます。</p>	<ul style="list-style-type: none"> <li>UDP : 20514 (syslog)</li> </ul> <p>(注) デフォルトポートは、外部ログ用に設定できます。</p>	<ul style="list-style-type: none"> <li>UDP : 20514 (syslog)</li> </ul> <p>(注) デフォルトポートは、外部ログ用に設定できます。</p>	<ul style="list-style-type: none"> <li>UDP : 20514 (syslog)</li> </ul> <p>(注) デフォルトポートは、外部ログ用に設定できます。</p>
ポリシーサービス ISE ノード	管理	<ul style="list-style-type: none"> <li>TCP : 22 (SSH サーバ)</li> <li>TCP : 80<sup>1</sup> (HTTP)</li> <li>TCP : 443<sup>1</sup> (HTTPS)</li> </ul>			
	複製および同期	<ul style="list-style-type: none"> <li>TCP : 443 (HTTPS)</li> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> <li>ICMP (ハートビート)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 1521<sup>2</sup> (データベース リスナーおよび AQ)</li> </ul>

表 E-1 Cisco ISE のサービスとポート (続き)

Cisco ISE ノード	ISE サービス	ギガビット イーサ ネット 0 のポート	ギガビット イーサ ネット 1 のポート	ギガビット イーサ ネット 2 のポート	ギガビット イーサ ネット 3 のポート
ポリシー サービス ISE ノード (続き)	セッション	<ul style="list-style-type: none"> <li>UDP : 1645、1812 (RADIUS 認証)</li> <li>UDP : 1646、1813 (RADIUS アカウンティング)</li> <li>UDP : 1700、3799 (RADIUS 認可変更 [CoA])</li> </ul> <p>(注) UDP ポート 1700 は、設定できません。</p> <ul style="list-style-type: none"> <li>TCP : 88、389、464 (アウトバウンド AD および Lightweight Directory Access Protocol [LDAP])</li> <li>UDP : 30514 (syslog)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul> <p>(注) UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。</p>	<ul style="list-style-type: none"> <li>UDP : 1645、1812 (RADIUS 認証)</li> <li>UDP : 1646、1813 (RADIUS アカウンティング)</li> <li>UDP : 1700、3799 (RADIUS 認可変更 [CoA])</li> </ul> <p>(注) UDP ポート 1700 は、設定できません。</p> <ul style="list-style-type: none"> <li>TCP : 88、389、464 (アウトバウンド AD および Lightweight Directory Access Protocol [LDAP])</li> <li>UDP : 30514 (syslog)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul> <p>(注) UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。</p>	<ul style="list-style-type: none"> <li>UDP : 1645、1812 (RADIUS 認証)</li> <li>UDP : 1646、1813 (RADIUS アカウンティング)</li> <li>UDP : 1700、3799 (RADIUS 認可変更 [CoA])</li> </ul> <p>(注) UDP ポート 1700 は、設定できません。</p> <ul style="list-style-type: none"> <li>TCP : 88、389、464 (アウトバウンド AD および Lightweight Directory Access Protocol [LDAP])</li> <li>UDP : 30514 (syslog)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul> <p>(注) UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。</p>	<ul style="list-style-type: none"> <li>UDP : 1645、1812 (RADIUS 認証)</li> <li>UDP : 1646、1813 (RADIUS アカウンティング)</li> <li>UDP : 1700、3799 (RADIUS 認可変更 [CoA])</li> </ul> <p>(注) UDP ポート 1700 は、設定できません。</p> <ul style="list-style-type: none"> <li>TCP : 88、389、464 (アウトバウンド AD および Lightweight Directory Access Protocol [LDAP])</li> <li>UDP : 30514 (syslog)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul> <p>(注) UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。</p>

表 E-1 Cisco ISE のサービスとポート (続き)

Cisco ISE ノード	ISE サービス	ギガビットイーサネット 0 のポート	ギガビットイーサネット 1 のポート	ギガビットイーサネット 2 のポート	ギガビットイーサネット 3 のポート
ポリシーサービス ISE ノード (続き)	ゲストおよびスポンサーポータル	<ul style="list-style-type: none"> <li>TCP : 8443 (HTTPS)</li> </ul> <p>(注) TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。</p>	<ul style="list-style-type: none"> <li>TCP : 8443 (HTTPS)</li> </ul> <p>(注) TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。</p>	<ul style="list-style-type: none"> <li>TCP : 8443 (HTTPS)</li> </ul> <p>(注) TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。</p>	<ul style="list-style-type: none"> <li>TCP : 8443 (HTTPS)</li> </ul> <p>(注) TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。</p>
	クライアントプロビジョニング	<ul style="list-style-type: none"> <li>TCP : 80、8443 (Web または Cisco NAC エージェントのインストール)</li> </ul> <p>(注) TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。ゲストの設定にも対応しています。</p> <ul style="list-style-type: none"> <li>TCP : 8905 (Cisco NAC エージェントのアップデート)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 8905 (Cisco NAC エージェントのアップデート)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 8905 (Cisco NAC エージェントのアップデート)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 8905 (Cisco NAC エージェントのアップデート)</li> </ul>
	ポスチャおよびハートビート	<ul style="list-style-type: none"> <li>TCP : 8905 検出 (HTTPS)</li> <li>UDP : 8905 (レイヤ 2) 検出 (SWISS)</li> <li>UDP : 8905 PRA/Keep-alive (SWISS)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 8905 検出 (HTTPS)</li> <li>UDP : 8905 (レイヤ 2) 検出 (SWISS)</li> <li>UDP : 8905 PRA/Keep-alive (SWISS)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 8905 検出 (HTTPS)</li> <li>UDP : 8905 (レイヤ 2) 検出 (SWISS)</li> <li>UDP : 8905 PRA/Keep-alive (SWISS)</li> </ul>	<ul style="list-style-type: none"> <li>TCP : 8905 検出 (HTTPS)</li> <li>UDP : 8905 (レイヤ 2) 検出 (SWISS)</li> <li>UDP : 8905 PRA/Keep-alive (SWISS)</li> </ul>

表 E-1 Cisco ISE のサービスとポート (続き)

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
ポリシー サービス ISE ノード (続き)	Profiler	<ul style="list-style-type: none"> <li>UDP : 9996 (NetFlow)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>UDP : 67、68 (DHCP)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>TCP : 80、8080 (DHCPSPAN プロブおよび HTTP)</li> <li>UDP : 30514 (RADIUS)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>NMAP は、ポート 0 ~ 65535<sup>3</sup> を使用します (アウトバウンド)。</li> <li>UDP : 53 (DNS ルックアップ)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 161 (SNMP クエリー)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 162 (SNMP トラップ)</li> </ul> <p>(注) このポートは、設定可能です。</p>	<ul style="list-style-type: none"> <li>UDP : 9996 (NetFlow)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>UDP : 67、68 (DHCP)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>TCP : 80、8080 (DHCPSPAN プロブおよび HTTP)</li> <li>UDP : 30514 (RADIUS)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>NMAP は、ポート 0 ~ 65535<sup>3</sup> を使用します (アウトバウンド)。</li> <li>UDP : 53 (DNS ルックアップ)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 161 (SNMP クエリー)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 162 (SNMP トラップ)</li> </ul> <p>(注) このポートは、設定可能です。</p>	<ul style="list-style-type: none"> <li>UDP : 9996 (NetFlow)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>UDP : 67、68 (DHCP)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>TCP : 80、8080 (DHCPSPAN プロブおよび HTTP)</li> <li>UDP : 30514 (RADIUS)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>NMAP は、ポート 0 ~ 65535<sup>3</sup> を使用します (アウトバウンド)。</li> <li>UDP : 53 (DNS ルックアップ)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 161 (SNMP クエリー)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 162 (SNMP トラップ)</li> </ul> <p>(注) このポートは、設定可能です。</p>	<ul style="list-style-type: none"> <li>UDP : 9996 (NetFlow)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>UDP : 67、68 (DHCP)</li> </ul> <p>(注) このポートは、設定可能です。</p> <ul style="list-style-type: none"> <li>TCP : 80、8080 (DHCPSPAN プロブおよび HTTP)</li> <li>UDP : 30514 (RADIUS)</li> </ul> <p>(注) これは、セッション サービスを介した内部サービスです。</p> <ul style="list-style-type: none"> <li>NMAP は、ポート 0 ~ 65535<sup>3</sup> を使用します (アウトバウンド)。</li> <li>UDP : 53 (DNS ルックアップ)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 161 (SNMP クエリー)</li> </ul> <p>(注) このポートは、ルート テーブルによって異なります。</p> <ul style="list-style-type: none"> <li>UDP : 162 (SNMP トラップ)</li> </ul> <p>(注) このポートは、設定可能です。</p>

表 E-1 Cisco ISE のサービスとポート (続き)

Cisco ISE ノード	ISE サービス	ギガビットイーサネット 0 のポート	ギガビットイーサネット 1 のポート	ギガビットイーサネット 2 のポート	ギガビットイーサネット 3 のポート
ポリシーサービス ISE ノード (続き)	クラスタリング	<ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul>	<ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul>	<ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul>	<ul style="list-style-type: none"> <li>UDP : 45588、45590</li> </ul>
インラインポスチャ ISE ノード	管理	<ul style="list-style-type: none"> <li>TCP : 22 (SSH サーバ)</li> <li>TCP : 8443 (HTTPS)</li> </ul> <p>(注) 管理 ISE ノードによって使用されます。</p>	—	—	—
	インラインポスチャ	<ul style="list-style-type: none"> <li>UDP : 1645、1812 (認証用 RADIUS プロキシ)</li> <li>UDP : 1646、1813 (アカウントリング用 RADIUS プロキシ)</li> <li>UDP : 1700、3799 (RADIUS CoA)</li> </ul>	<ul style="list-style-type: none"> <li>UDP : 1645、1812 (認証用 RADIUS プロキシ)</li> <li>UDP : 1646、1813 (アカウントリング用 RADIUS プロキシ)</li> <li>UDP : 1700、3799 (RADIUS CoA)</li> </ul>	—	—
<b>(注)</b> ハイアベイラビリティおよび管理サービスは、インラインポスチャ固有のものであり、他の Cisco ISE ノードタイプには適用されません。					
	ハイアベイラビリティ	—	—	UDP : 694 (ハートビート)	UDP : 694 (ハートビート)
	管理	TCP : 9090 (リダイレクト)	TCP : 9090 (リダイレクト)	—	—

- インラインポスチャノードは、管理ペルソナをサポートしていないため、このポートへのアクセスはありません。
- インラインポスチャノードは、データベースリスナー機能をサポートしていないため、このポートへのアクセスはありません。
- NMAP OS スキャンは、ポート 0 ~ 65535 を使用して、エンドポイントのオペレーティングシステムを検出します。

