



## 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 \(2 ページ\)](#)
- [Cisco ISE インフラストラクチャ \(2 ページ\)](#)
- [オペレーティング システム ポート \(5 ページ\)](#)
- [Cisco ISE 管理ノードのポート \(8 ページ\)](#)
- [Cisco ISE モニターリング ノードのポート \(13 ページ\)](#)
- [Cisco ISE ポリシー サービス ノードのポート \(15 ページ\)](#)
- [Cisco ISE pxGrid サービス ポート \(21 ページ\)](#)
- [OCSP および CRL サービス ポート \(22 ページ\)](#)
- [Cisco ISE プロセス \(22 ページ\)](#)
- [必要なインターネット URL \(23 ページ\)](#)

## 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	<ul style="list-style-type: none"> <li>• HTTPS (SOAP) : TCP/443</li> <li>• データの同期/レプリケーション (JGroups) : TCP/12001 (グローバル)</li> <li>• ISE メッセージング サービス : SSL : TCP/8671</li> <li>• ISE 内部通信 : TCP/15672</li> <li>• 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</li> </ul>	—

## Cisco ISE インフラストラクチャ

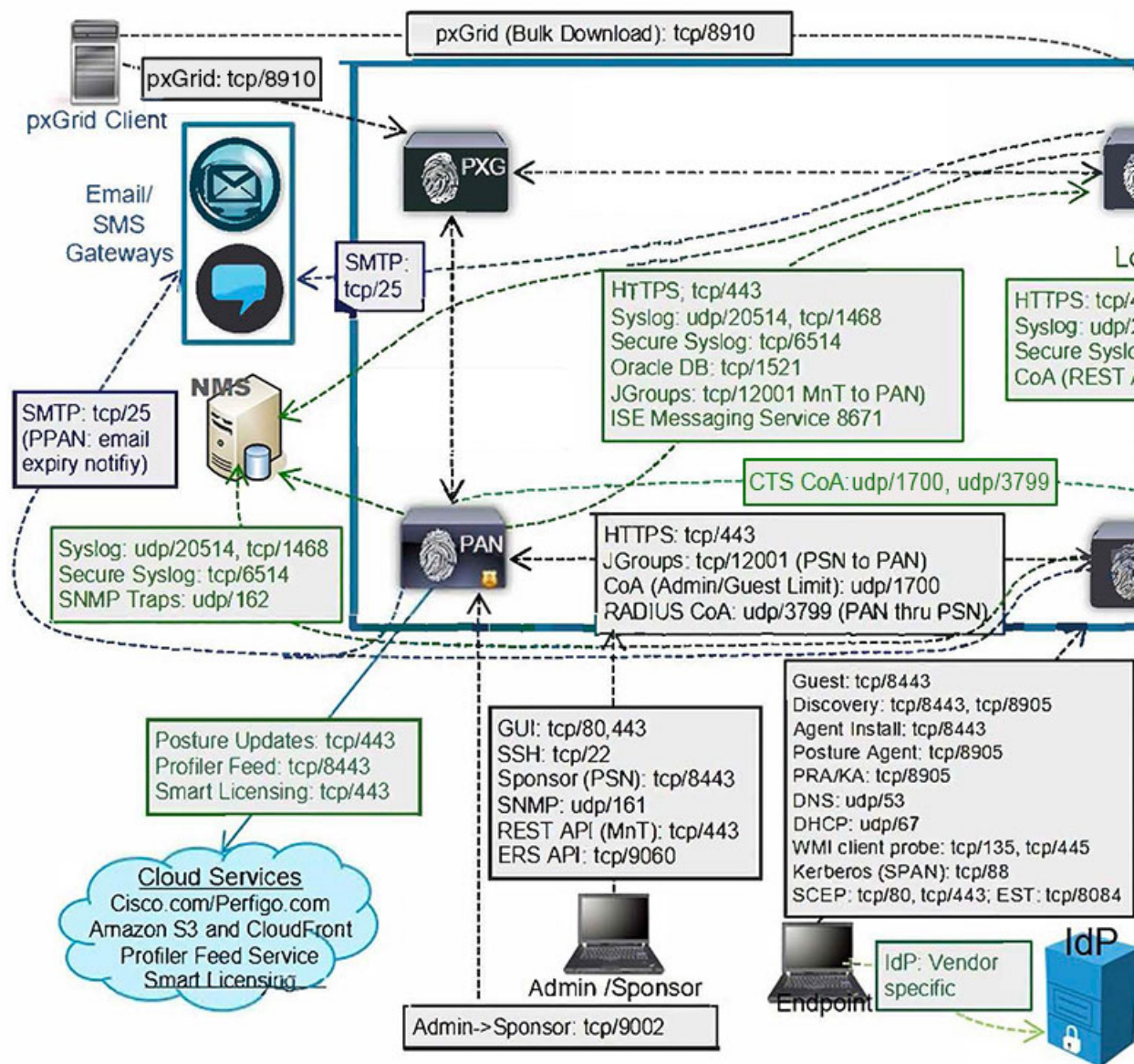
この付録では、Cisco ISE が外部アプリケーションやデバイスとのイントラネットワーク通信に使用する、TCP および User Datagram Protocol (UDP) のポートの一覧を示します。この付録に示される Cisco ISE ポートが、対応するファイアウォールでオープンになっている必要があります。

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 トランッキングを無効にし、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 ～ 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。

# ISE 3.2 Node Communications



## 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。

## オペレーティングシステム ポート

次の表に、NMAP が OS のスキャンに使用する TCP ポートを示します。また、NMAP は ICMP および UDP ポート 51824 を使用します。

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	54	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
[1000]	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040 ~ 1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244

1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998 ~ 2010	2013	2020	2021
2022	2030	2033	2034	2035	2038	2040 ~ 2043	2045 ~ 2049	2065
2068	2099	2100	2103	2105 ~ 2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381 ~ 2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000 ~ 4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550

4567	4662	4848	4899	4900	4998	5000 ~ 5004	5009	5030
5033	5050	5051	5054	[5060]	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900 ~ 5907	5910	5911	5915	5922	5925	5950	5952	5959
5960 ~ 5963	5987 ~ 5989	5998 ~ 6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565 ~ 6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080 ~ 8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9,000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968

9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

## 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
	<ul style="list-style-type: none"> <li>• HTTP : TCP/80、HTTPS : TCP/443 （TCP/443 にリダイレクトされた TCP/80。設定不可）</li> <li>• SSH サーバー : TCP/22</li> <li>• CoA</li> <li>• 外部 RESTful サービス（ERS） REST API : TCP/9060</li> </ul> <p>（注） ERS サービスと OpenAPI サービスは、 ポート 443 を介して動 作する HTTPS 専用の REST API です。現 在、ERS API もポート 9060 を介して動作し ます。ただし、ポート 9060 は、以降の Cisco ISE リリースの ERS API ではサポートされ ない可能性があります。 ERS API にはポート 443 のみを使用する ことをお勧めします。</p> <ul style="list-style-type: none"> <li>• DNAC 統合モードの外部 RESTful サービス（ERS）REST API ベー スの認証 : TCP/9062</li> <li>• 管理者 GUI からのゲストアカウン トの管理 : TCP/9002</li> <li>• 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</li> </ul> <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 フォルトで有効になってい ます。</p>	

Cisco ISE サービス	ギガビットイーサネット0またはポート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、またはポート1および2）のポート
	<p>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。</p> <p>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。</p> <p>(注) SAML 管理者ログインの場合、管理者が SAML ログインを試行しているデバイスから PSN のポート 8443 に到達可能である必要があります。</p>	
モニターリング	<ul style="list-style-type: none"> <li>• SNMP クエリー : UDP/161</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>• ICMP</li> </ul>	
ロギング（アウトバウンド）	<ul style="list-style-type: none"> <li>• syslog : UDP/20514、TCP/1468</li> <li>• セキュア syslog : TCP/6514</li> </ul> <p>(注) デフォルトポートは外部ロギング用に設定できます。</p> <ul style="list-style-type: none"> <li>• SNMP トラップ : UDP/162</li> </ul>	

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）	<p>• 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：</p> <ul style="list-style-type: none"> <li>• LDAP : TCP/389、3268、UDP/389</li> <li>• SMB : TCP/445</li> <li>• KDC : TCP/88</li> <li>• KPASS : TCP/464</li> </ul> <p>• WMI : TCP/135</p> <p>• ODBC :</p> <p>(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。</p> <ul style="list-style-type: none"> <li>• Microsoft SQL : TCP/1433</li> <li>• Sybase : TCP/2638</li> <li>• PostgreSQL : TCP/5432</li> <li>• Oracle : TCP/1521、TCPS/2484</li> </ul> <p>• NTP : UDP/323 (localhost インターフェイスのみ)</p> <p>• DNS : UDP/53、TCP/53</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• Cisco ISE は、Active Directory 接続に対する接続の診断中 に、DNS に対して ICMP ping を実行します。</li> </ul>	
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	<ul style="list-style-type: none"> <li>• HTTP : TCP/80、HTTPS : TCP/443</li> <li>• SSH サーバー : TCP/22</li> </ul>	—
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。 <ul style="list-style-type: none"> <li>• ICMP</li> </ul>	
ログ	<ul style="list-style-type: none"> <li>• syslog : UDP/20514、TCP/1468</li> <li>• セキュア syslog : TCP/6514</li> </ul> (注) デフォルトポートは外部ロギング用に設定できます。 <ul style="list-style-type: none"> <li>• SMTP : アラームの電子メール用の TCP/25</li> <li>• SNMP トラップ : UDP/162</li> </ul>	

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）	<ul style="list-style-type: none"> <li>• 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： <ul style="list-style-type: none"> <li>• LDAP : TCP/389、3268、UDP/389</li> <li>• SMB : TCP/445</li> <li>• KDC : TCP/88、UDP/88</li> <li>• KPASS : TCP/464</li> </ul> </li> <li>• WMI : TCP/135</li> <li>• ODBC : <p style="margin-left: 20px;">(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。</p> <ul style="list-style-type: none"> <li>• Microsoft SQL : TCP/1433</li> <li>• Sybase : TCP/2638</li> <li>• PostgreSQL : TCP/5432</li> <li>• Oracle : TCP/1521、15723、16820</li> </ul> </li> <li>• NTP : UDP/323 (localhost インターフェイスのみ)</li> <li>• DNS : UDP/53、TCP/53</li> </ul> <p>(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。</p>	

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
インバウンド通信に使用されるポート	<ul style="list-style-type: none"> <li>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</li> <li>TCP/1521：MnT ノードに対してポート 1521 を有効にする必要があります。PAN からのインバウンド通信にはポート 1521 が必要です。このポートが MnT ノードに対して有効になっていない場合、MnT ノードのフェールオーバーによってログまたはレポートが失われる可能性があります。</li> </ul> <p>(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。</p>	
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	<ul style="list-style-type: none"> <li>HTTP：TCP/80、HTTPS：TCP/443</li> <li>SSH サーバー：TCP/22</li> <li>OCSP：TCP/2560</li> </ul>	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 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
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。	
SXP	<ul style="list-style-type: none"> <li>• PSN (SXP ノード) から NAD : TCP/64999</li> <li>• PSN から SXP へ (同じ Cisco ISE での内部通信) : TCP/9644</li> </ul>	
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)	<ul style="list-style-type: none"> <li>• syslog : UDP/20514、TCP/1468</li> <li>• セキュア syslog : TCP/6514</li> </ul> (注) デフォルトポートは外部ロギング用に設定できます。 <ul style="list-style-type: none"> <li>• SNMP トラップ : UDP/162</li> </ul>	
セッション	<ul style="list-style-type: none"> <li>• RADIUS 認証 : UDP/1645、1812</li> <li>• RADIUS アカウンティング : UDP/1646、1813</li> <li>• RADIUS DTLS 認証/アカウンティング : UDP/2083</li> <li>• RADIUS 許可変更 (CoA) 送信 : UDP/1700</li> <li>• RADIUS 許可変更 (CoA) リッスン/リレー : UDP/1700、3799</li> </ul> (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)	<ul style="list-style-type: none"> <li>• 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 : <ul style="list-style-type: none"> <li>• LDAP : TCP/389、3268</li> <li>• SMB : TCP/445</li> <li>• KDC : TCP/88</li> <li>• KPASS : TCP/464</li> </ul> </li> <li>• WMI : TCP/135</li> <li>• ODBC : <p>(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。</p> <ul style="list-style-type: none"> <li>• Microsoft SQL : TCP/1433</li> <li>• Sybase : TCP/2638</li> <li>• PostgreSQL : TCP/5432</li> <li>• Oracle : TCP/1521</li> </ul> </li> <li>• NTP : UDP/323 (localhost インターフェイスのみ)</li> <li>• DNS : UDP/53、TCP/53</li> </ul> <p>(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。</p>	
パッシブ ID (インバウンド)	<ul style="list-style-type: none"> <li>• TS エージェント : TCP/9094</li> <li>• AD エージェント : TCP/9095</li> <li>• syslog : UDP/40514、TCP/11468</li> </ul>	

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
<p>Web ポータル サービス :</p> <ul style="list-style-type: none"> <li>- ゲスト/Web 認証</li> <li>- ゲスト スポンサー ポータル</li> <li>- デバイス ポータル</li> <li>- クライアントのプロビジョニング</li> <li>- 証明書のプロビジョニング</li> <li>- ブロックリストポータル</li> </ul>	<p>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) :</p> <ul style="list-style-type: none"> <li>• 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)</li> <li>• 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)</li> <li>• 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)</li> <li>• デバイスポータル : TCP/8000-8999 (デフォルトポートは TCP/8443)</li> <li>• スポンサーポータル : TCP/8000-8999 (デフォルトポートは TCP/8443)</li> <li>• 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</li> </ul>	

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
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	<ul style="list-style-type: none"> <li>• 検出 (クライアント側) : TCP/80 (HTTP)、TCP/8905 (HTTPS)</li> </ul> <p>(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。</p> <p>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。</p> <p>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。</p> <p>Cisco ISE 3.1 以降では、ポート 8905 は非ポリシーサービスノードでデフォルトで無効になっています。このポートを有効にするには、[全般設定 (General Settings)] ウィンドウ ([管理 (Administration)] &gt; [システム (System)] &gt; [設定 (Settings)] &gt; [ポスチャ (Posture)] &gt; [全般設定 (General Settings)]) で、[ポスチャサービスの非ポリシーサービスノードでポート 8905 を有効にする (Enable Port 8905 on non-Policy Service Nodes for Posture Services)] チェックボックスをオンにします。</p> <ul style="list-style-type: none"> <li>• 検出 (ポリシー サービス ノード側) : TCP/8443、8905 (HTTPS)</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• アセスメント - ポスチャ ネゴシエーションとエージェントレポート : TCP/8905 (HTTPS)</li> <li>• 双方向ポスチャフロー : TCP/8000 ~ 8999 (デフォルトポートは TCP/8449)</li> </ul>	

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	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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</li> <li>• 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</li> <li>• 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</li> <li>• 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)</li> </ul>	
モバイル デバイス管理 (MDM) API の統合	<ul style="list-style-type: none"> <li>• 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。</li> <li>• API : ベンダー固有</li> <li>• 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</li> </ul>	

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	<ul style="list-style-type: none"> <li>• NetFlow : UDP/9996 (注) このポートは、設定可能です。</li> <li>• DHCP : UDP/67 (注) このポートは、設定可能です。</li> <li>• DHCP SPAN プローブ : UDP/68</li> <li>• HTTP : TCP/80、8080</li> <li>• 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。</li> <li>• 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。</li> <li>• SNMP トラップ : UDP/162 (注) このポートは、設定可能です。</li> </ul>	

## Cisco ISE pxGrid サービス ポート



(注) Cisco ISE リリース 3.1 以降、すべての pxGrid 接続は pxGrid バージョン 2.0 に基づく必要があります。pxGrid バージョン 1.0 ベース (XMPP ベース) の統合は、リリース 3.1 以降の Cisco ISE では動作しなくなります。

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。

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
pxGrid 登録者数	TCP/8910	
ノード間通信	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します。次の表に示されている URL へのアクセスを提供できない場合は、関連する機能が損なわれたり、動作しなくなったりする可能性があります。

表 6: 必要な URL アクセス

機能	URL
ポスチャの更新	<a href="https://www.cisco.com/">https://www.cisco.com/</a> <a href="https://iseservice.cisco.com">https://iseservice.cisco.com</a>
フィードサービスのプロファイリング	<a href="https://ise.cisco.com">https://ise.cisco.com</a>
スマートライセンス	<a href="https://smartreceiver.cisco.com">https://smartreceiver.cisco.com</a>
テレメトリ	<a href="https://connectdna.cisco.com/">https://connectdna.cisco.com/</a>
Cisco AI Analytics	<a href="http://api.use1.prd.kairos.ciscolabs.com">http://api.use1.prd.kairos.ciscolabs.com</a> (米国東部リージョン)。 <a href="http://api.euc1.prd.kairos.ciscolabs.com">http://api.euc1.prd.kairos.ciscolabs.com</a> (欧州中部リージョン)。 これらの必要な URL へのネットワーク接続は、HTTPS TCP ポート 443 を介して行われます。

機能	URL
Microsoft Entra ID	login.microsoftonline.com:443 *.login.microsoftonline.com:443 *.login.microsoft.com:443
アカウント登録ゲストのソーシャルログイン	facebook.co akamaihd.net akamai.co fbcdn.net
Cisco ISE のカスタマー エクスペリエンス アンケート	Cisco ISE リリース 3.2 パッチ 4 以降では、 *.qualtrics.com へのブラウザアクセスが必要です。



(注) Cisco ISE リリース 3.1 以前では、Cisco ISE スマートライセンスは、特定のパッチがリリースされるまで、<https://tools.cisco.com> を必須のインターネット URL として使用します。詳細については、関連する Cisco ISE リリースのインストールガイドを参照してください。

インタラクティブヘルプ機能では、Cisco ISE が管理ポータルブラウザを使用して次の URL に接続する必要があります。

- \*.walkme.com
- \*.walkmeusercontent.com



## 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。