導入の計画

プランニング ワークフロー

Cisco DNA Center アプライアンスの設置、設定、セットアップを試みる前に、次の計画と情報収集のタスクを実行する必要があります。これらのタスクを完了したあと、データセンターにアプライアンスを物理的に設置すると続行できます。

1. スタンドアロン設置とクラスタ設置で推奨されるケーブル接続とスイッチングの要件を確認します。「インターフェイスケーブル接続」を参照してください。
2. アプライアンスの設定時に適用するIPアドレッシング、サブネット化などのIPトラフィック情報を収集します。「必要な IP アドレスおよびサブネット」を参照してください。
3. 必要なWebベースのリソースに対するアクセスのソリューションを準備します。「必要なインターネット URL と完全修飾ドメイン名」と「インターネットへのアクセスを保護する」を参照してください。
4. Cisco DNA Center トラフィックのファイアウォールとセキュリティポリシーを再設定します。「必要なネットワークポート」を参照してください。Cisco DNA Center を使用して Cisco Software-Defined Access（SD-Access）ネットワークを管理している場合は「必要なポートとプロトコル： Cisco Software-Defined Access」も参照してください。

5. アプライアンスの構成時と初回設定時に使用される追加情報を収集します。「必須の設定情報」と「必要な初期設定情報」を参照してください。

Cisco DNA CenterおよびCisco Software-Defined Access

Cisco SD-Access ファブリックアーキテクチャを使用するネットワークも含め、すべてのネットワークタイプで Cisco DNA Centerを使用できます。Cisco SD-Accessは、従来のネットワークをインテントベースのネットワークに変換します。これにより、ビジネスロジックがネットワークの物理的な部分になり、構成、プロビジョニング、トラブルシューティングなどの日常的なタスクを簡単に自動化できるようになります。Cisco SD-Access ソリューションは、ネットワークをビジネスニーズに合わせ、問題解決を改善し、セキュリティ侵害の影響を軽減するために必要な時間を短縮します。

Cisco SD-Access ソリューションの詳細については、このガイドの範囲外です。Cisco DNA Center で使用する Cisco SD-Access ファブリックアーキテクチャの実装を計画しているネットワークアーキテクトや管理者は、次のリソースから追加情報とガイダンスを入手できます。

- 通常のネットワークのアプローチと技術では不可能なソリューションを自動化するために、Cisco DNA Center が Cisco SD-Access を活用する方法については、『ソフトウェア定義型アクセス：インテントベースのネットワーキングの実現』を参照してください。
- Cisco SD-Access アクセスセグメンテーションを使用したネットワークセキュリティの強化に関するガイダンスについては、『*SD-Access*アクセスセグメンテーション設計ガイド』を参照してください。
- Cisco DNA Center での SDA の展開に関するガイダンスは、『ソフトウェア定義型アクセス導入ガイド』を参照してください。
- Cisco DNA Center と Cisco SD-Access ソリューションの基盤であるデジタル ネットワークアーキテクチャの詳細と、この革新的なアーキテクチャで他のシスコ製品やソリューション、サードパーティの製品やソリューションが果たす役割については、『Cisco DNA Design Zone』を参照してください。

インターフェイスケーブル接続

次のタイプのネットワークアクセスを提供するスイッチに、アプライアンスのポートを接続します。Cisco DNA Center の機能に必要なため、少なくともエンタープライズおよびクラスタ内ポートインターフェイスを設定する必要があります。

アプライアンスで NIC ボンディングが有効になっている場合、エンタープライズ、クラスタ内、管理、およびインターネットポートのセカンダリインスタンスは Intel X710-DA4 NIC に存在します。これらのポートを、各ポートのプライマリインスタンスを接続するスイッチとは異なるスイッチに接続します（NIC ボンディングの概要を参照してください）。

（注）

- アプライアンス設定中、Maglev設定ウィザードは、**クラスタリンク**オプションをインターフェイスに割り当てるまで続行できません。実稼働環境の単一ノード展開と3ノード展開の両方で、クラスタ内ポートをクラスタリンクとして割り当てます。
- クラスタリンクとしてマークされたインターフェイスは、設定が完了した後は変更できないことに注意してください。後で、クラスタリンクとしてマークされたインターフェイスを変更する必要がある場合は、アプライアンスのイメージを作成しなおす必要があります。Cisco DNA Centerアプライアンスのイメージを作成し直すために完了する必要があるタスクの説明については、アプライアンスのイメージの再作成を参照してください。将来的に3ノードクラスタに拡張できるようにするため、IPアドレスを使用してクラスタポートを設定するようお勧めします。また、クラスタリンクインターフェイスがスイッチポートに接続されており、稼働状態になっていることを確認します。
- 複数のクラスタを構築する場合は、クラスタ間の相互作用（クラスタが破損する可能性がある）を防ぐために、クラスタごとに個別のIPスキームを使用する必要があります。

- （必須）10 Gbpsエンタープライズポート（ネットワークアダプタ1）：このポートの目的は、Cisco DNA Centerがネットワークと通信し、ネットワークを管理できるようにすることです。このポートを、エンタープライズネットワークに接続しているスイッチに接続し、ポートのサブネットマスクを使用してIPアドレスを1つ設定します。

  プライマリインスタンス：

  - 44および56コアアプライアンスでは、これはPCIeスロット1に搭載されているIntel X710-DA2 NICの左側にあるポートです。
  - 112コアアプライアンスでは、これはPCIeスロット9に搭載されているIntel X710-DA2 NICの上部にある10 Gbpsポートです。

  セカンダリインスタンス：

  - 44および56コアアプライアンスでは、これはPCIeスロット2に搭載されているIntel X710-DA4 NICの2番目のポートです。
  - 112コアアプライアンスでは、これはPCIeスロット12に搭載されているIntel X710-DA4 NICの上から3番目の10 Gbpsポートです。

- （必須）10 Gbpsクラスタ内ポート（ネットワークアダプタ2）：このポートの目的は、クラスタ内のプライマリノードとセカンダリノード間の通信を可能にすることです。このポートをクラスタ内の他のノードに接続しているスイッチに接続し、ポートのサブネットマスクを使用してIPアドレスを1つ設定します。

  プライマリインスタンス：

  - 44および56コアアプライアンスでは、これはPCIeスロット1に搭載されているIntel X710-DA2 NICの右側にあるポートです。

- 112 コアアプライアンスでは、これは PCIe スロット 9 に搭載されている Intel X710-DA2 NIC の下部にある 10 Gbps ポートです。

セカンダリインスタンス：

- 44 および 56 コアアプライアンスでは、これは PCIe スロット 2 に搭載されている Intel X710-DA4 NIC の最初のポートです。
- 112 コアアプライアンスでは、これは PCIe スロット 12 に搭載されている Intel X710-DA4 NIC の下部にある 10 Gbps ポートです。

- （オプション）1 Gbps または 10 Gbps の管理ポート（ネットワークアダプタ 3）：このポートから Cisco DNA Center GUI にアクセスできるため、ユーザーはアプライアンス上でソフトウェアを使用できます。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

  プライマリインスタンス：アプライアンスの背面パネルに 1 というラベルが付いています。

  セカンダリインスタンス：

  - 44 および 56 コアアプライアンスでは、これは PCIe スロット 2 に搭載されている Intel X710-DA4 NIC の 4 番目のポートです。
  - 112 コアアプライアンスでは、これは PCIe スロット 12 に搭載されている Intel X710-DA4 NIC の上部にある 10 Gbps ポートです。

- （オプション）1 Gbps または 10 Gbps のインターネットポート（ネットワークアダプタ 4）：このポートは、背面パネルに 2 というラベルが付いており、オプションです。10 Gbps のエンタープライズポート（ネットワークアダプタ 1）を使用してアプライアンスをインターネット（インターネット プロキシ サーバーを含む）に接続できない場合にのみ使用してください。このポートを使用する必要がある場合は、インターネット プロキシ サーバーに接続しているスイッチに接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

  プライマリインスタンス：アプライアンスの背面パネルに 2 というラベルが付いています。

  セカンダリインスタンス：

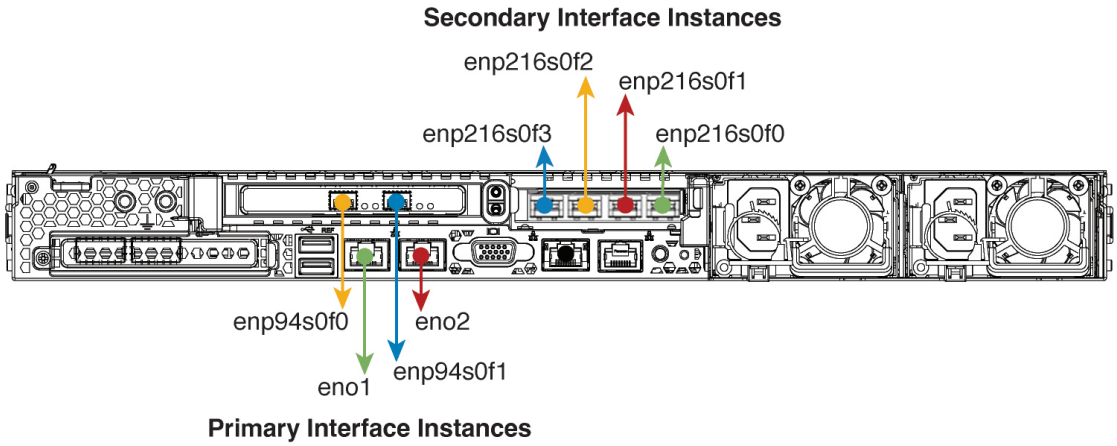
  - 44 および 56 コアアプライアンスでは、これは PCIe スロット 2 に搭載されている Intel X710-DA4 NIC の 3 番目のポートです。
  - 112 コアアプライアンスでは、これは PCIe スロット 12 に搭載されている Intel X710-DA4 NIC の上から 2 番目の 10 Gbps ポートです。

- （オプション、ただし強く推奨）1 Gbps Cisco IMC ポート：このポートで、Cisco Integrated Management Controller（CIMC）アウトオブバンド アプライアンス管理インターフェイスとその GUI にブラウザがアクセスします。その目的は、アプライアンスとそのハードウェ

アを管理できるようにすることです。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用してIPアドレスを1つ設定します。

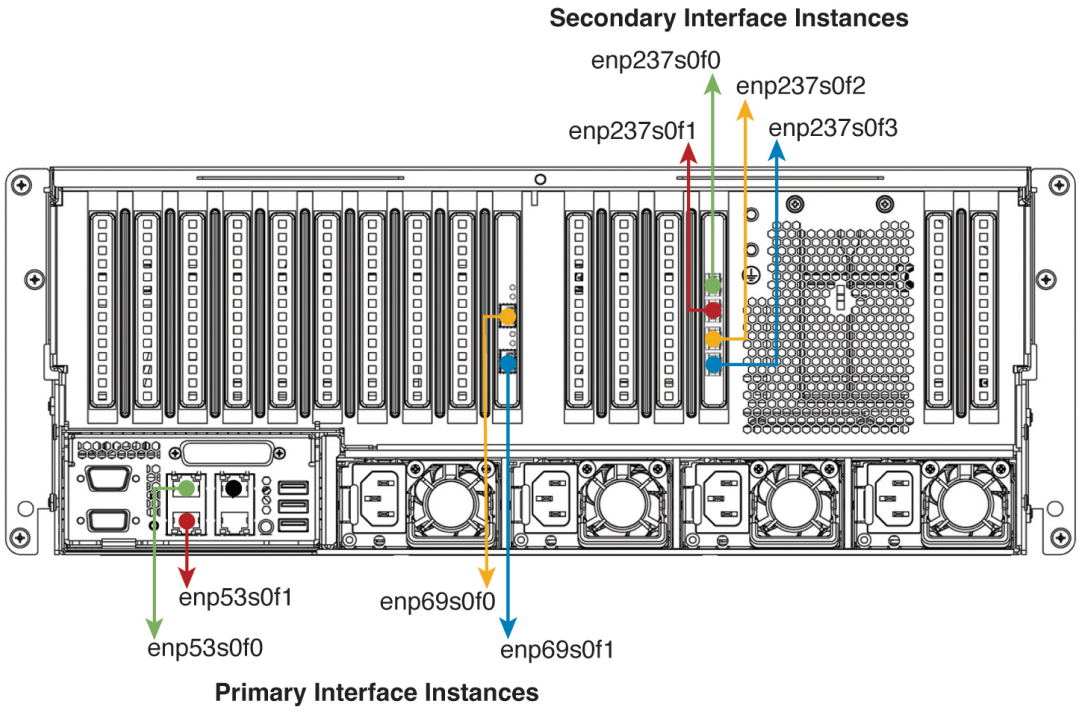
次の図は、シングルノードCisco DNA Centerクラスタで推奨される接続と、各インターフェイスに割り当てられているラベルを示しています。

図 *1 : 44* および *56* コアアプライアンスに推奨されるケーブル接続



（注） 管理インターフェイスとインターネットインターフェイスの両方とも、プライマリインスタンスの帯域幅は 1 Gbps で、セカンダリインスタンスの帯域幅は 10 Gbps です。

図 *2 : 112* コアアプライアンスに推奨されるケーブル接続



（注） 管理インターフェイスとインターネットインターフェイスの両方とも、プライマリインスタンスの帯域幅は 1 Gbps で、セカンダリインスタンスの帯域幅は 10 Gbps です。

3 ノード Cisco DNA Center クラスタ内の各ノードの接続は、シングルノードクラスタの場合と同じであり、同じポートが使用されます。3 ノードクラスタをケーブル接続する場合は、次の手順を実行します。

- 各ノードのエンタープライズ、クラスタ内、管理、およびインターネットポートのプライマリインスタンスと Cisco IMC ポートをプライマリスイッチに接続します。
- 各ノードのエンタープライズ、クラスタ内、管理、およびインターネットポートのセカンダリインスタンスをセカンダリスイッチに接続します。

各ポートの詳細については、前面パネルと背面パネルにあるシャーシの背面パネルの図と付属の説明を参照してください。

（注） マルチノードクラスタの導入では、すべてのメンバノードを同じサイトの同じネットワーク内にする必要があります。アプライアンスは、複数のネットワークまたはサイト間でのノードの配布をサポートしていません。

10 Gbps のエンタープライズポートとクラスタポートを接続する場合は、ポートで次のメディアタイプのみがサポートされていることに注意してください。

- SFP-10G-SR-S（ショートレンジ、MMF）
- SFP-10G-LR（ロングレンジ、SMF）
- SFP-H10GB-CU1M（Twinax ケーブル、パッシブ、1 m）
- SFP-H10GB-CU3M（Twinax ケーブル、パッシブ、3 m）
- SFP-H10GB-CU5M（Twinax ケーブル、パッシブ、5 m）
- SFP-H10GB-ACU7M（Twinax ケーブル、アクティブ、7 m）

必要な IP アドレスおよびサブネット

設置を開始する前に、使用する予定の各アプライアンスポートに割り当てるのに十分な IP アドレスがネットワークにあることを確認する必要があります。アプライアンスをシングルノードクラスタとしてインストールするか、3 ノードクラスタのプライマリまたはセカンダリノードとしてインストールするかによって、次のアプライアンスポート（NIC）アドレスが必要になります。

- [Enterprise Port Address]（必須）：サブネットマスクを持つ 1 つの IP アドレス。
- [Cluster Port Address]（必須）：サブネットマスクを持つ 1 つの IP アドレス。
- [Management Port Address]（オプション）：サブネットマスクを持つ 1 つの IP アドレス。
- [Internet Port Address]（オプション）：サブネットマスクを持つ 1 つの IP アドレス。これはオプションのポートであり、エンタープライズポートを使用してクラウドに接続できない場合にのみ使用されます。この目的で使用する必要がある場合を除き、インターネットポートの IP アドレスは必要ありません。
- [CIMC Port Address]（オプション、ただし強く推奨）：サブネットマスクを持つ 1 つの IP アドレス。

（注） これらの要件で要求されるすべての IP アドレスは、有効な IPv4 ネットマスクを持つ有効な IPv4 アドレスである必要があります。アドレスと対応するサブネットが重複していないことを確認します。重複している場合、サービスの通信の問題が発生する可能性があります。

また、次の追加の IP アドレスと専用 IP サブネットが必要になります。これは、アプライアンスの設定時に入力が求められ、適用されます。

- **クラスタ仮想 IP アドレス（Cluster Virtual IP Addresses）**：クラスタごとに設定されたネットワークインターフェイスごとに 1 つの仮想 IP（VIP）アドレス。この要件は3 ノードクラスタと、将来3 ノードクラスタに変換される可能性のある単一ノードクラスタに適用されます。設定するネットワークインターフェイスごとに VIP を指定する必要があります。各 VIP は、対応する設定済みインターフェイスの IP アドレスと同じサブネットからのものである必要があります。各アプライアンスには、エンタープライズ、クラスタ、管理、およびインターネットの 4 つのインターフェイスがあります。Cisco DNA Center の機能に必要なため、最低でも企業およびクラスタのポートインターフェイスを設定する必要があります。サブネットマスクと 1 つ以上の関連ゲートウェイまたはスタティックルートとともに IP をインターフェイスに指定すると、そのインターフェイスは設定されていると見なされます。設定時にインターフェイスを完全にスキップすると、そのインターフェイスは設定されていないと見なされます。

  次の点に注意してください。

  - 単一ノード設定で、今後 3 ノードクラスタに変換する予定がない場合は、VIP アドレスを指定する必要はありません。ただし、これを行う場合は、設定されているすべてのネットワークインターフェイスに VIP アドレスを指定する必要があります（3 ノードクラスタの場合と同様）。
  - 単一ノードクラスタのクラスタ内リンクがダウンすると、管理インターフェイスとエンタープライズ インターフェイスに関連付けられているVIP アドレスもダウンします。これが発生すると、クラスタ内リンクが復元されるまで Cisco DNA Center を使用できません（ソフトウェアイメージ管理 [SWIM] と Cisco Identity Services Engine [ISE] の統合が動作しません。またネットワーク データ プラットフォーム [NDP] コレクタから情報を収集できないため、Cisco DNA アシュアランスデータが表示されません）。
  - エンタープライズインターフェイスまたは管理インターフェイスには、リンクローカルまたはルーティング不可能な IP アドレスを使用しないでください。

- **デフォルトゲートウェイ IP アドレス（Default Gateway IP Address）**：ネットワークの優先デフォルトゲートウェイの IP アドレス。他のルートがトラフィックに一致しない場合、トラフィックはこの IP アドレスを経由してルーティングされます。通常は、インターネットにアクセスするネットワーク設定内のインターフェイスにデフォルトゲートウェイを割り当てる必要があります。Cisco DNA Center の導入時に留意すべきセキュリティ上の考慮事項については、『Cisco Digital Network Architecture Center セキュリティ ベスト プラクティス ガイド』を参照してください。

- **DNS サーバの IP アドレス（DNS Server IP Addresses）**：1 つ以上のネットワークの優先 DNS サーバの IP アドレス。設定時に、DNS サーバの IP アドレスをスペースで区切ったリストとして入力することによって、複数の値を指定できます。

- **（オプション）スタティックルートアドレス（Static Route Addresses）**：1 つ以上のスタティックルートの IP アドレス、サブネットマスク、およびゲートウェイ。設定時に、複

数のスタティックルートの IP アドレス、ネットマスク、およびゲートウェイを、スペースで区切ったリストとして入力することによってそれらを指定できます。

アプライアンスの任意のインターフェイスに対して 1 つ以上のスタティックルートを設定できます。デフォルトゲートウェイ以外の特定の方向でトラフィックをルーティングする場合は、スタティックルートを指定する必要があります。スタティックルートを持つ各インターフェイスは、IP route コマンドテーブルでトラフィックがルーティングされるデバイスとして設定されます。このため、トラフィックが送信されるインターフェイスとスタティックルートの方向を一致させることが重要です。

スタティックルートは、スイッチやルータで使用されるようなネットワークデバイスのルーティングテーブルでは推奨されません。この場合はダイナミック ルーティング プロトコルの方が適しています。ただし、他の方法では到達できないネットワークの特定の部分にアプライアンスがアクセスできるようにするには、必要に応じてスタティックルートを追加する必要があります。

- **NTP サーバの IP アドレス（NTP Server IP Addresses）**：DNS 解決可能なホスト名、または 1 つ以上の Network Time PROTOCOL（NTP）サーバの IP アドレス。

  設定時に、NTP サーバの IP アドレスやマスクまたはホスト名をスペースで区切ったリストとして入力することによって、複数の値を指定できます。実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定することを推奨します。

  これらの NTP サーバは、事前にハードウェアを同期するときに指定し、クラスタ内の各アプライアンスでソフトウェアを設定する際に再度指定します。時刻の同期は、マルチホストクラスタ全体でのデータの精度と処理の調整にとって重要です。アプライアンスを実稼働環境に展開する前に、アプライアンスのシステムクロックの時刻が現在の時刻であること、および指定した NTP サーバが正確な時刻を維持していることを確認してください。アプライアンスを ISE と統合する予定の場合は、ISE がアプライアンスと同じ NTP サーバと同期していることも確認する必要があります。

- **コンテナサブネット（Container Subnet）**：アシュアランス、インベントリ収集などの内部アプリケーションサービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。デフォルトでは、Cisco DNA Center によりリンクローカルサブネット（**169.254.32.0/20**）がこのパラメータに設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、Cisco DNA Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりしていないことを確認してください。また、サブネットの最小サイズが 21 ビットであることを確認してください。指定するサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。

  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 100.64.0.0/10

詳細については、RFC 1918 では『プライベートインターネット用のアドレス割り当て』を、RFC 6598 では『IANA-Reserved IPv4 Prefix For Shared Address Space』を参照してください。

重要

- 有効なCIDRサブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20 および 172.17.61.0/20 サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了した後、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません（「アプライアンスの再イメージ化」を参照してください）。

- **クラスタサブネット（Cluster Subnet）**：データベースアクセス、メッセージバスなどのインフラストラクチャ サービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。デフォルトでは、Cisco DNA Center によりリンクローカルサブネット（**169.254.48.0/20**）がこのパラメータに設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、Cisco DNA Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりしていないことを確認してください。また、サブネットの最小サイズが 21 ビットであることを確認してください。指定するサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 100.64.0.0/10

  詳細については、RFC 1918 では『プライベートインターネット用のアドレス割り当て』を、RFC 6598 では『IANA-Reserved IPv4 Prefix For Shared Address Space』を参照してください）

  コンテナサブネットとして 10.10.10.0/21 を指定する場合は、これら 2 つのサブネットは重複しないため、10.0.8.0/21 のクラスタサブネットを指定することもできます。また、設定ウィザードによって、これらのサブネット間の重複（存在する場合）が検出され、重複を修正するように求められることにも注意してください。

重要

- 有効なCIDRサブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20および172.17.61.0/20サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了した後、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません（「アプライアンスの再イメージ化」を参照してください）。
- クラスタポート、コンテナサブネット、またはクラスタサブネットの IP アドレスを入力する場合は、169.254.0.0/23 サブネット内のアドレスを指定しないでください。

コンテナとクラスタの 2 つのサブネットで推奨される合計 IP アドレス空間には、4096 のアドレスが含まれており、それぞれ 2048 のアドレスの 2/21 サブネットに分割されています。2/21 サブネットを重複させることはできません。Cisco DNA Center の内部サービスは、専用の IP アドレスセットの動作に必要です（Cisco DNA Center マイクロサービス アーキテクチャの要件）。この要件に対応するには、Cisco DNA Center システムごとに 2 つの専用サブネットを割り当てる必要があります。

アプライアンスがこのようなアドレス空間を必要とする理由の 1 つは、システムパフォーマンスを維持するためです。東西（ノード間）通信には内部ルーティングおよびトンネリングテクノロジーが使用されているため、重複するアドレス空間を使用すると、アプライアンスが仮想ルーティングを実行し、内部的に FIB を転送（FIB）するように強制されることがあります。これにより、1 つのサービスから別のサービスに送信されるパケットに対して複数の encap/decap が発生し、高いレイヤでのカスケードの影響により、非常に低いレベルの高い内部遅延が発生します。

もう 1 つの理由は Cisco DNA Center Kubernetes ベースのサービスコンテナ化アーキテクチャです。各アプライアンスは Kubernetes K8 ノードごとにこの空間の IP アドレスを使用します。複数のノードが 1 つのサービスを構成できます。現在、Cisco DNA Center は、複数の IP アドレスを必要とするサービスを 100 余りサポートしており、新しい機能と対応するサービスが常に追加されています。IP アドレスが不足したり、お客様がシステムをアップグレードするためだけに連続するアドレス空間を再割り当てすることを要求したりすることなく、シスコが新しいサービスや機能を追加できるようにするために、アドレス空間の要件は最初は意図的に大きく維持されています。

これらのサブネットでサポートされているサービスは、レイヤ 3 でも有効になっています。クラスタスペースは、特に、アプリケーションサービスとインフラストラクチャ サービスの間でデータを伝送し、頻繁に使用されます。

RFC 1918 および RFC 6598 の要件は、クラウドからパッケージとアップデートをダウンロードするための Cisco DNA Center の要件によるものです。選択した IP アドレス範囲が RFC 1918 および RFC 6598 に準拠していない場合、すぐにパブリック IP アドレスの重複の問題につながる可能性があります。

必要なインターネット URL と完全修飾ドメイン名

アプライアンスでは、次の URL と完全修飾ドメイン名（FQDN）の表へのセキュアなアクセスが必要です。

この表では、各 URL と FQDN を使用する機能について説明します。IP トラフィックがアプライアンスとこれらのリソースとの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 と FQDN 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。

インターネットへのプロキシアクセスの要件の詳細については、「インターネットへのアクセスを保護する」を参照してください。

表 *1*：必要な *URL* と *FQDN* アクセス

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
システムとアプリケーション パッケージ ソフトウェアにアップデートをダウンロードし、製品チームにユーザフィードバックを送信します。	推奨：*.ciscoconnectdna.com:443[1] ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • https://www.ciscoconnectdna.com • https://cdn.ciscoconnectdna.com • https://registry.ciscoconnectdna.com • https：//registry-cdn.ciscoconnectdna.com
Cisco DNA Center アップデートパッケージ	• https://*.ciscoconnectdna.com/* • *.cloudfront.net • *.tesseractcloud.com
スマートアカウントおよび SWIM ソフトウェアのダウンロード	• https://apx.cisco.com • https://cloudsso.cisco.com/as/token.oauth2 • https://*.cisco.com/* • https://download-ssc.cisco.com/
クラウドドメインで認証します。	https://dnaservices.cisco.com
ThousandEyes と統合します。	• *.awsglobalaccelerator.com • api.thousandeyes.com

目的	…Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco Enterprise Network Function Virtualization Infrastructure Software（NFVIS）デバイスを管理します。	*.amazonaws.com
顧客動向テレメトリを収集します。	https://data.pendo.io
API 呼び出しを許可して、Cisco CX Cloud Success Tracks へのアクセスを有効にします。そうしないと、Machine Reasoning Engine（MRE）がサポートする Security Advisories、Bug Identifier、および EOX 機能の拡張構成ベースのスキャンに追加された拡張機能が期待どおりに動作しません。	https://api-cx.cisco.com
Webex と統合します。	• http://analytics.webexapis.com • https://webexapis.com
ユーザフィードバック	https://dnacenter.uservoice.com
Cisco Meraki と統合します。	推奨：*.meraki.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • dashboard.meraki.com:443 • api.meraki.com:443 • n63.meraki.com：443
OCSP/CRL を使用した SSL/TLS 証明書の失効ステータスを確認します。	• http://validation.identrust.com • http://commercial.ocsp.identrust.com （注） 上記の URL は、直接でも Cisco DNA Center で構成されているプロキシサーバー経由でも到達できるようにする必要があります。
Cisco DNA Center リモートサポート機能が有効になっている場合、シスコの認定スペシャリストがトラブルシューティング データを収集できるようにします。	wss://prod.radkit-cloud.cisco.com:443

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
cisco.com とシスコ スマート ライセンスと統合します。	*.cisco.com：443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • software.cisco.com • cloudsso.cisco.com • cloudsso1.cisco.com • cloudsso2.cisco.com • apiconsole.cisco.com • api.cisco.com • apx.cisco.com • sso.cisco.com • apmx-prod1-vip.cisco.com • apmx-prod2-vip.cisco.com • tools.cisco.com • tools1.cisco.com • tools2.cisco.com • smartreceiver.cisco.com
Network-Based Application Recognition（NBAR）に接続します。	prod.sdavc-cloud-api.com:443
サイトとロケーションマップで正確な情報をレンダリングします。	• www.mapbox.com • *. tiles.mapbox.com/*: 443 プロキシの場合、宛先は *.tiles.mapbox.com/* です。
Cisco AI Network Analytics のデータ収集では、クラウドホストへのアウトバウンド HTTPS（TCP 443）アクセスを許可するようにネットワークまたは HTTP プロキシを設定します。	• https://api.use1.prd.kairos.ciscolabs.com（米国東部リージョン） • https://api.euc1.prd.kairos.ciscolabs.com（欧州中央リージョン）
GUI から特定のタスクを完了できる対話型ヘルプフローのメニューにアクセスします。	https://ec.walkme.com
ライセンスサービスにアクセスします。	https://swapi.cisco.com

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco Spaces と統合します。	• https://dnaspaces.io • https://dnaspaces.eu • https://ciscospaces.sg

[1] シスコは ciscoconnectdna.com とそのサブドメインを所有し、維持しています。Cisco Connect DNA インフラストラクチャは、シスコのセキュリティおよび信頼に関するガイドラインを満たし、継続的なセキュリティテストを実施しています。このインフラストラクチャは堅牢であり、組み込みのロードバランシング機能と自動化機能を備えています。24 時間 365 日の可用性を確保するために、クラウド運用チームが監視と保守を行います。

インターネットへのアクセスを保護する

デフォルトでは、アプライアンスは、インターネット経由でアクセスして、ソフトウェアアップデート、ライセンス、デバイスソフトウェアをダウンロードしたり、最新のマップ情報、ユーザフィードバックなどを提供したりするように設定されています。これらの目的でインターネット接続を提供することは必須要件です。

HTTPS プロキシサーバを使用することは、リモート URL に安全にアクセスするための信頼性の高い方法です。「必要なインターネット URL と完全修飾ドメイン名」に記載されている URL にアプライアンスがアクセスするために必要なアクセス権を付与するには、HTTPS プロキシサーバを使用するようお勧めします。アプライアンス設置時に、この目的で使用するプロキシサーバの URL とポート番号を、プロキシのログインクレデンシャルとともに入力するように求められます（プロキシが必要な場合）。

このリリースでは、アプライアンスは HTTP を介したプロキシサーバとの通信のみをサポートしています。HTTPS プロキシサーバをネットワーク内の任意の場所に配置できます。プロキシサーバは HTTPS を使用してインターネットと通信しますが、アプライアンスは HTTP 経由でプロキシサーバと通信します。そのためアプライアンスの設定中、プロキシを設定するときにプロキシの HTTP ポートを指定するようお勧めします。

設定後にプロキシ設定を変更する必要が生じた場合は、GUI を使用して行うことができます。

必要なネットワークポート

次の表にアプライアンスが使用する既知のネットワークサービスポートを一覧表示します。これらのポートが、ファイアウォール設定またはプロキシゲートウェイのどちらで開くかを問わず、アプライアンスとの間で送受信されるトラフィックフローに対して開いていることを確認する必要があります。

SDA インフラストラクチャを採用するネットワークにアプライアンスを導入する場合は、追加のポート、プロトコル、およびトラフィックタイプに対応している必要があります。詳細については、「必要なポートとプロトコル： Cisco Software-Defined Access」を参照してください。

（注） Cisco DNA Center の展開時に留意すべきセキュリティ上の考慮事項については、『*Cisco DNA Center* セキュリティのベストプラクティスガイド』を参照してください。

表 *2:* ポート：着信トラフィック

ポート番号	許可されるトラフィック	プロトコル（**TCP** または **UDP**）
22	SSH	[TCP]
67	BOOTP	UDP
80	HTTP	TCP
111	NFS（アシュアランスのバックアップに使用）	TCP および UDP
123	NTP	UDP
162	SNMP	UDP
443	HTTPS	TCP
514	Syslog	UDP
2049	NFS（アシュアランスのバックアップに使用）	TCP および UDP
2068	HTTPS	TCP （注） このポートは、リモート KVM コンソールのリダイレクトポートとして機能します。アプライアンスの構成中に Cisco IMC を使用する場合は、アプライアンスの構成が完了するまでポートを開いておく必要があります。
2222	SSH	[TCP]
9991	マルチキャスト ドメイン ネーム システム（mDNS）	TCP
20048	NFS（アシュアランスのバックアップに使用）	TCP および UDP
21730	アプリケーション可視性サービス（CBAR デバイス通信に使用）	UDP

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
32767	NFS（アシュアランスのバックアップに使用）	TCP および UDP

表 *3:* ポート：発信トラフィック

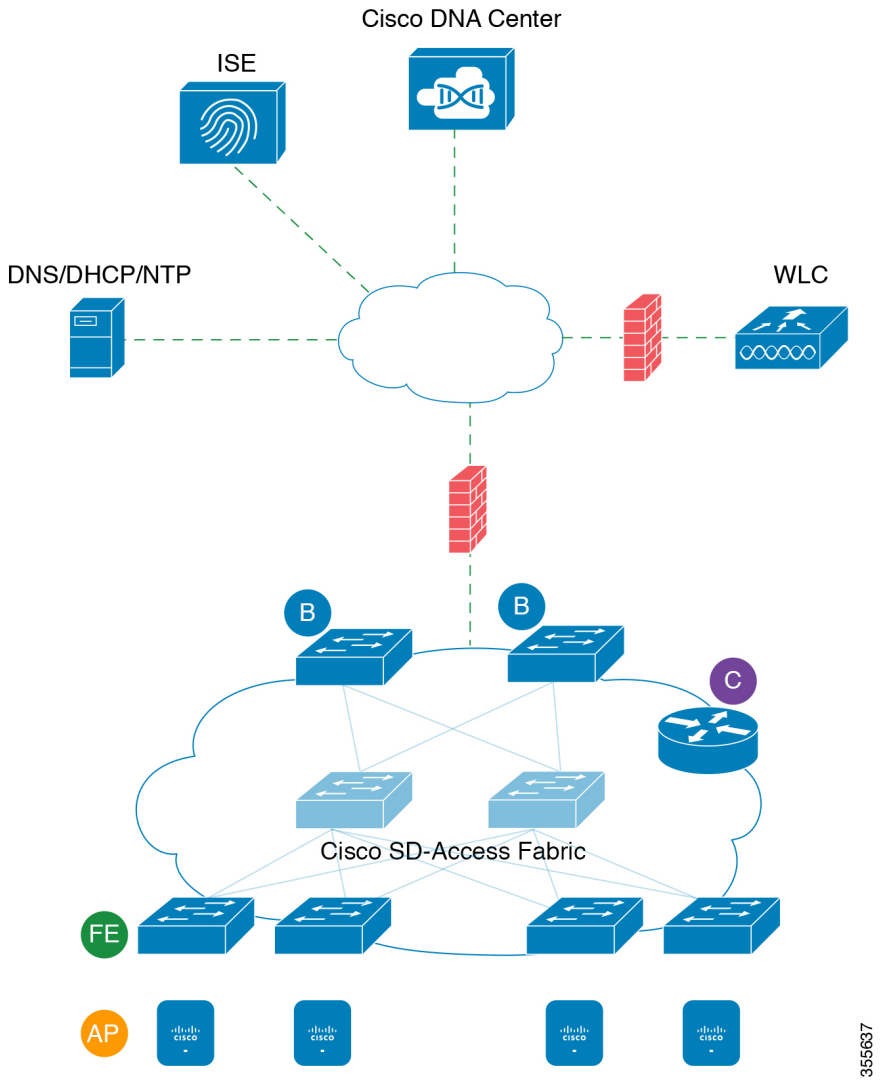
ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
22	SSH（ネットワークデバイスへ）	TCP
23	Telnet（ネットワークデバイスへ）	TCP
53	DNS	UDP
80	ポート 80 は発信プロキシ設定に使用できます。 プロキシが設定ウィザードによって設定されている場合（プロキシがすでにネットワークに使用されている場合）、ほかの一般的なポート（8080 など）も使用できます。 シスコのサポートする証明書プールとトラストプールにアクセスするには、アプライアンスから次のリストに記載されたシスコのアドレスに対する発信 IP トラフィックを許可するようにネットワークを設定します。 https://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP エージェント	UDP
443	HTTPS	TCP
5222、8910	Cisco ISE XMP（PxGrid 用）	TCP
9060	Cisco ISE ERS API トラフィック	TCP

（注） ほかにもアプライアンスからシスコのアドレス（https://www.cisco.com/security/pki/）に対する発信 IP トラフィックを許可するようネットワークを設定する方法があります。アプライアンスからシスコがサポートする証明書およびトラストプールにアクセスするには、上述の URL に記載されている IP アドレスを使用します。

必要なポートとプロトコル： Cisco Software-Defined Access

このトピックでは、次の図に示すような一般的なCisco SD-Accessファブリック展開にネイティブなポート、プロトコル、およびトラフィックのタイプについて詳しく説明します。

図 *3 : Cisco SD-Access* ファブリック インフラストラクチャ



ネットワークにCisco SD-Accessを実装している場合は、次の表の情報を使用して、ネットワーク管理の自動化に必要なアクセス権をCisco SD-Accessに提供しながら、Cisco DNA Centerインフラストラクチャを適切に保護するファイアウォールとセキュリティポリシーを計画します。

表 *4 : Cisco DNA Center* トラフィック

送信元ポート[2]	送信元	宛先ポート	接続先	説明
いずれか（Any）	Cisco DNA Center	UDP 53	DNS Server	Cisco DNA Center から DNS サーバの間で使用
いずれか（Any）	Cisco DNA Center	TCP 22	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SSH に使用
いずれか（Any）	Cisco DNA Center	TCP 23	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で Telnet に使用
いずれか（Any）	Cisco DNA Center	UDP 161	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SNMP デバイス検出に使用
ICMP	Cisco DNA Center	ICMP	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SNMP デバイス検出に使用
いずれか（Any）	Cisco DNA Center	TCP 443	ファブリックアンダーレイ	スイッチと NFVIS のアプリケーション ホスティング
いずれか（Any）	Cisco DNA Center	UDP 6007	スイッチとルータ	Cisco DNA Center からスイッチおよびルータの間で NetFlow に使用
いずれか（Any）	Cisco DNA Center	TCP 830	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間で NETCONF に使用（Cisco SD-Access 組み込みワイヤレス）
UDP 123	Cisco DNA Center	UDP 123	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間で LAN 自動化中の初回期間に使用
いずれか（Any）	Cisco DNA Center	UDP 123	NTP Server	Cisco DNA Center から NTP サーバの間で使用
いずれか（Any）	Cisco DNA Center	TCP 22、UDP 161	シスコ ワイヤレス コントローラ	Cisco DNA Center からシスコ ワイヤレス コントローラの間で使用
ICMP	Cisco DNA Center	ICMP	シスコ ワイヤレス コントローラ	Cisco DNA Center からシスコ ワイヤレス コントローラの間で使用
いずれか（Any）	AP	TCP 32626	Cisco DNA Center	Cisco DNA アシュアランス インテリジェント キャプチャ（gRPC）機能で使用されるトラフィック統計情報とパケット キャプチャ データの受信に使用されます。

[2] クラスタ、PKI、SFTP サーバ、プロキシポートのトラフィックは、この表には含まれていません。

表 5: インターネット接続トラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
いずれか（Any）	Cisco DNA Center	TCP 443	registry.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	www.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	registry-cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	software.cisco.com	デバイスソフトウェアのダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	cloudsso.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか（Any）	Cisco DNA Center	TCP 443	cloudsso1.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか（Any）	Cisco DNA Center	TCP 443	cloudsso2.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか（Any）	Cisco DNA Center	TCP 443	apiconsole.cisco.com	CSSM スマートライセンス API
いずれか（Any）	Cisco DNA Center	TCP 443	sso.cisco.com	Cisco.com クレデンシャルとスマートライセンス
いずれか（Any）	Cisco DNA Center	TCP 443	api.cisco.com	Cisco.com クレデンシャルとスマートライセンス
いずれか（Any）	Cisco DNA Center	TCP 443	apx.cisco.com	Cisco.com クレデンシャルとスマートライセンス
いずれか（Any）	Cisco DNA Center	TCP 443	dashboard.meraki.com	Meraki の統合
いずれか（Any）	Cisco DNA Center	TCP 443	api.meraki.com	Meraki の統合
いずれか（Any）	Cisco DNA Center	TCP 443	n63.meraki.com	Meraki の統合
いずれか（Any）	Cisco DNA Center	TCP 443	dnacenter.uservoice.com	ユーザフィードバックの送信

いずれか（Any）	Cisco DNA Center Admin Client	TCP 443	*.tiles.mapbox.com	ブラウザでのマップのレンダリング（プロキシ経由のアクセスの場合、宛先は *.tiles.mapbox.com/*）
いずれか（Any）	Cisco DNA Center	TCP 443	www.mapbox.com	マップとシスコ ワイヤレス コントローラの国番号の識別

表 *6 : Cisco Software-Defined Access* ファブリック アンダーレイ トラフィック

送信元ポート[3]	送信元	宛先ポート	接続先	説明
UDP 68	ファブリックアンダーレイ	UDP 67	DHCP サーバ	ファブリックスイッチ、ルータからDHCPサーバの間で、ファブリックエッジノードによって開始される DHCP リレーパケットに使用。
いずれか（Any）	ファブリックアンダーレイ	TCP 80	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間で PnP に使用
いずれか（Any）	ファブリックアンダーレイ	TCP 443	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間でイメージのアップグレードに使用
いずれか（Any）	ファブリックアンダーレイ	UDP 162	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間で SNMP トラップに使用
いずれか（Any）	ファブリックアンダーレイ	UDP 514	Cisco DNA Center	ファブリックスイッチ、ルータから Cisco DNA アシュアランス
いずれか（Any）	ファブリックアンダーレイ	UDP 6007	Cisco DNA Center	ファブリックスイッチおよびルータから Cisco DNA Center の間で NetFlow に使用
いずれか（Any）	ファブリックアンダーレイ	UDP 123	Cisco DNA Center	ファブリックスイッチから Cisco DNA Center の間で LAN 自動化時に使用
ICMP	ファブリックアンダーレイ	ICMP	Cisco DNA Center	ファブリックスイッチ、ルータループバックから Cisco DNA Center の間で SNMP デバイス検出に使用
UDP 161	ファブリックアンダーレイ	いずれか（Any）	Cisco DNA Center	ファブリックスイッチ、ルータループバックから Cisco DNA Center の間で SNMP デバイス検出に使用
いずれか（Any）	ファブリックアンダーレイ	UDP 53	DNS Server	ファブリックスイッチ、ルータから DNS サーバの間で名前解決に使用

TCP および UDP 4342	ファブリックアンダーレイ	TCP および UDP 4342	ファブリック ルータおよびスイッチ	LISP でカプセル化された制御メッセージ
TCP および UDP 4342	ファブリックアンダーレイ	いずれか（Any）	ファブリック ルータおよびスイッチ	LISP コントロールプレーン通信
いずれか（Any）	ファブリックアンダーレイ	UDP 4789	ファブリック ルータおよびスイッチ	ファブリックカプセル化データパケット（VXLAN-GPO）
いずれか（Any）	ファブリックアンダーレイ	UDP 1645/1646/1812/1813	ISE	ファブリックスイッチ、ルータループバック IP から ISE の間で RADIUS に使用
ICMP	ファブリックアンダーレイ	ICMP	ISE	ファブリックスイッチ、ルータから ISE の間でトラブルシューティングに使用
UDP 1700/3799	ファブリックアンダーレイ	いずれか（Any）	ISE	ファブリックスイッチから ISE の間で気付アドレス（CoA）に使用
いずれか（Any）	ファブリックアンダーレイ	UDP 123	NTP Server	ファブリックスイッチ、ルータループバック IP から NTP サーバの間で使用
いずれか（Any）	control-plane	UDP および TCP 4342/4343	シスコ ワイヤレス コントローラ	コントロールプレーンのループバック IP からシスコ ワイヤレス コントローラの間でファブリック対応ワイヤレスに使用

[3] ボーダー ルーティング プロトコル、SPAN、プロファイリング、およびテレメトリトラフィックは、この表には含まれていません。

表 7: シスコ ワイヤレス コントローラ トラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 5246/5247/5248	シスコ ワイヤレス コントローラ	いずれか（Any）	AP IP アドレスプール	シスコ ワイヤレス コントローラから AP サブネットの間で CAPWAP に使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	AP IP アドレスプール	シスコ ワイヤレス コントローラから AP の間でトラブルシューティング目的の ping を許可するために使用

いずれか（Any）	シスコ ワイヤレス コントローラ	• TCP 443（Cisco AireOS ワイヤレスコントローラ） • TCP 25103（Cisco 9800 ワイヤレスコントローラ）	Cisco DNA Center	シスコ ワイヤレス コントローラから Cisco DNA Center の間でアシュアランス に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 69/5246/5247 TCP 22	AP IP アドレス プール	シスコ ワイヤレス コントローラから AP サブネットの間で CAPWAP に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP および TCP 4342/4343	コントロール プレーン	シスコ ワイヤレス コントローラから コントロールプレーンのループバック IP アドレスの間で使用
いずれか（Any）	シスコ ワイヤレス コントローラ	TCP 22	Cisco DNA Center	シスコ ワイヤレス コントローラから Cisco DNA Center の間でデバイス検出に使用
UDP 161	シスコ ワイヤレス コントローラ	いずれか（Any）	Cisco DNA Center	シスコ ワイヤレス コントローラから Cisco DNA Center の間で SNMP に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 162	Cisco DNA Center	シスコ ワイヤレス コントローラから Cisco DNA Centerトラップの間で SNMP トラップに使用
いずれか（Any）	シスコ ワイヤレス コントローラ	TCP 16113	Cisco Mobility Services Engine（MSE）と Cisco SPECTRUM EXPERT	シスコ ワイヤレス コントローラから Cisco MSE、SPECTRUM EXPERT の間で NMSP に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 6007	Cisco DNA Center	ワイヤレスコントローラから Cisco DNA Center の間で NetFlow ネットワークテレメトリに使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	Cisco DNA Center	シスコ ワイヤレス コントローラから トラブルシューティング目的の ping を許可するために使用
いずれか（Any）	シスコ ワイヤレス コントローラと各種 Syslog サーバ	UDP 514	シスコ ワイヤレス コントローラ	Syslog（オプション）

いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 53	DNS Server	シスコ ワイヤレス コントローラから DNS サーバの間で使用
いずれか（Any）	シスコ ワイヤレス コントローラ	TCP 443	ISE	シスコ ワイヤレス コントローラから ISE の間でゲスト SSID Web 認証に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 1645、1812	ISE	シスコ ワイヤレス コントローラから ISE の間で RADIUS 認証に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 1646、1813	ISE	シスコ ワイヤレス コントローラから ISE の間で RADIUS アカウンティングに使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 1700、3799	ISE	シスコ ワイヤレス コントローラから ISE の間で RADIUS CoA に使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	ISE	シスコ ワイヤレス コントローラから ISE ICMP の間でトラブルシューティングに使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 123	NTP サーバ	シスコ ワイヤレス コントローラから NTP サーバの間で使用

表 *8*：ファブリック対応ワイヤレス *AP IP* アドレスプールトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 68	AP IP アドレスプール	UDP 67	DHCP サーバ	AP IP アドレスプールから DHCP サーバの間で使用
ICMP	AP IP アドレスプール	ICMP	DHCP サーバ	AP IP アドレスプールから ICMP の間でトラブルシューティングに使用
いずれか（Any）	AP IP アドレスプール	514	各種	Syslog—宛先設定可能。Default is 255.255.255.255.
いずれか（Any）	AP IP アドレスプール	UDP 69/5246/5247/5248	シスコ ワイヤレス コントローラ	AP IP アドレスプールからシスコ ワイヤレス コントローラの間で CAPWAP に使用
ICMP	AP IP アドレスプール	ICMP	シスコ ワイヤレス コントローラ	AP IP アドレスプールからシスコ ワイヤレス コントローラの間でトラブルシューティング目的の ping を許可するために使用

表 *9*：*Cisco ISE* トラフィック

送信元ポート[4]	送信元	宛先ポート	接続先	説明

いずれか（Any）	ISE	TCP 64999	Border	ISE からボーダーノードの間で SGT Exchange Protocol（SXP）に使用
いずれか（Any）	ISE	UDP 514	Cisco DNA Center	ISE から Syslog サーバ（Cisco DNA Center）の間で使用
UDP 1645/1646/1812/1813	ISE	いずれか（Any）	ファブリックアンダーレイ	ISE からファブリックスイッチ、ルータの間で RADIUS と認証用に使用
いずれか（Any）	ISE	UDP 1700/3799	ファブリックアンダーレイ、シスコ ワイヤレス コントローラ	ISE からファブリックスイッチ、ルータループバック IP アドレスの間で RADIUS 認可変更（CoA）に使用 ISE からワイヤレスコントローラの間で CoA に使用する場合、UDP ポート 3799 も開いている必要があります。
ICMP	ISE	ICMP	ファブリックアンダーレイ	ISE からファブリックスイッチの間でトラブルシューティングに使用
いずれか（Any）	ISE	UDP 123	NTP Server	ISE と NTP サーバの間で使用
UDP 1812/1645/1813/1646	ISE	いずれか（Any）	シスコ ワイヤレス コントローラ	ISEからシスコ ワイヤレス コントローラの間で RADIUS に使用
ICMP	ISE	ICMP	シスコ ワイヤレス コントローラ	ISEからシスコ ワイヤレス コントローラの間でトラブルシューティングに使用

[4] 注：高可用性およびプロファイリング トラフィックは、この表には含まれていません。

表 *10 : DHCP* サーバトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 67	DHCP サーバ	UDP 68	AP IP アドレスプール	DHCP サーバからファブリック AP の間で使用
ICMP	DHCP サーバ	ICMP	AP IP アドレスプール	トラブルシューティング用の ICMP：ファブリックから DHCP の間で使用
UDP 67	DHCP サーバ	UDP 68	ファブリックアンダーレイ	DHCP からファブリックスイッチ、ルータの間で使用
ICMP	DHCP サーバ	ICMP	ファブリックアンダーレイ	トラブルシューティング用の ICMP：ファブリックから DHCP の間で使用
UDP 67	DHCP サーバ	UDP 68	ユーザ IP アドレスプール	DHCP サーバからファブリックスイッチ、ルータの間で使用
ICMP	DHCP サーバ	ICMP	ユーザ IP アドレスプール	トラブルシューティング用のICMP：ユーザとDHCPの間で使用

表 *11 : NTP* サーバトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 123	NTP Server	いずれか（Any）	ISE	NTP サーバから ISE の間で使用
UDP 123	NTP Server	いずれか（Any）	Cisco DNA Center	NTP サーバから Cisco DNA Center
UDP 123	NTP Server	いずれか（Any）	ファブリックアンダーレイ	NTP サーバからファブリックスイッチ、ルータループバックの間で使用
UDP 123	NTP Server	いずれか（Any）	シスコ ワイヤレス コントローラ	NTP サーバからシスコ ワイヤレス コントローラの間で使用

表 *12 : DNS* トラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 53	DNS Server	いずれか（Any）	ファブリックアンダーレイ	DNS サーバからファブリックスイッチの間で使用
UDP 53	DNS Server	いずれか（Any）	シスコ ワイヤレス コントローラ	DNS サーバからシスコ ワイヤレス コントローラの間で使用

必須の設定情報

アプライアンスの設定中、必要な IP アドレスおよびサブネットに加えて、次の情報を入力するように求められます。

- **Linux ユーザ名（Linux User Name）**：これは **maglev** です。このユーザー名はプライマリノードとセカンダリノードの両方を含む、クラスタ内のすべてのアプライアンスで共通しており、変更できません。
- **Linux パスワード（Linux Password）**：Linux ユーザ名 **maglev** のパスワードを指定します。このパスワードは、Linux コマンドラインを使用して各アプライアンスへのセキュアなアクセスを保証します。必要に応じてクラスタ内の各アプライアンスの Linux ユーザ名 **maglev** ごとに異なる Linux パスワードを割り当てることができます。

  デフォルト値はないため、ユーザが Linux パスワードを作成する必要があります。パスワードは次の要件を満たしている必要があります。

  - 長さは 8 文字以上にすること。
  - タブや改行を含まないこと。

- 次のうち少なくとも 3 つのカテゴリの文字を含むこと。
  - 大文字の英字（A ～ Z）
  - 小文字の英字（a ～ z）
  - 数字（0 ～ 9）
  - 特殊文字（! や # など）

Linux パスワードは暗号化され、Cisco DNA Center データベースにハッシュされます。マルチノードクラスタを展開している場合は、各セカンダリノードにプライマリノードの Linux パスワードを入力することも求められます。

- **パスワード生成シード（Password Generation Seed）（オプション）**：Linux パスワードを作成する代わりに、シードフレーズを入力し、[Generate Password] をクリックする方法もあります。**[Maglev Configuration]** ウィザードでは、このシードフレーズを使用してランダムで安全なパスワードが生成されます。**[Auto Generated Password]**フィールドを使用すると、生成されたパスワードをさらに編集できます。
- **管理者パスフレーズ（Administrator Passphrase）**：クラスタ内の Cisco DNA Center への Web アクセスに使用されるパスワードを指定します。これはスーパーユーザーアカウント admin のパスワードであり、初めて Cisco DNA Center にログインするときに使用します（クイック スタート ワークフローの完了を参照）。初めてログインすると、このパスワードを変更するよう求められます。

  このパスワードにはデフォルトがないため、作成する必要があります。管理者のパスフレーズは、上述の Linux パスワードと同じ要件を満たす必要があります。
- **CISCO IMC ユーザパスワード**：Cisco IMC GUI へのアクセスに使用するパスワードを指定します。工場出荷時のデフォルトは「*password*」ですが、Web ブラウザを使用してアクセスするために CIMC を初めて設定するとき、変更を求められます（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。

  Cisco IMC ユーザパスワードは、上述の Linux パスワードと同じ要件を満たす必要があります。工場出荷時の初期状態にリセットした場合にのみ、*password* に戻すことができます。
- [Primary Node IP Address]：クラスタにセカンダリノードをインストールする場合にのみ必要です。これは、プライマリノード上のクラスタポートの IP アドレスです（「インターフェイスケーブル接続」を参照）。

必要な初期設定情報

アプライアンスを設定したら、Cisco DNA Center にログインして、必須の設定タスクを完了します。この初回設定では次の情報が必要になります。

- **スーパーユーザ権限を持つ管理者の新しいパスワード（New Admin Superuser Password）**：Cisco DNA Center 管理者の新しいスーパーユーザパスワードを入力するように求められます。スーパーユーザ権限を持つ管理者のパスワードをリセットすると、運用上のセキュリティが向上します。これはたとえばCisco DNA Centerアプライアンスを設置して設定した企業スタッフが Cisco DNA Center のユーザまたは管理者ではない場合に特に重要です。
- **Cisco.com ログイン情報（Cisco.com Credentials）**：ソフトウェアのダウンロードを登録し、電子メールでシステム通信を受信するために組織が使用する Cisco.com ユーザ ID とパスワード。
- **シスコ スマートアカウントのクレデンシャル（Cisco Smart Account Credentials）**：組織がデバイスとソフトウェアライセンスの管理に使用する Cisco.com スマートアカウントのユーザ ID とパスワード。
- **IP アドレスマネージャの URL とクレデンシャル（IP Address Manager URL and Credentials）**：Cisco DNA Center で使用する予定のサードパーティ製 IP アドレスマネージャ（IPAM）サーバのホスト名、URL、管理者ユーザ名、管理者パスワード。このリリースでは InfoBlox と Bluecat がサポートされています。
- **プロキシ URL、ポート、クレデンシャル（Proxy URL, Port and Credentials）**：Cisco DNA Centerソフトウェアのアップデートの取得、デバイスライセンスの管理などのダウンロード可能なコンテンツの取得のために Cisco DNA Center で使用するプロキシサーバの URL（ホスト名または IP アドレス）、ポート番号、ユーザ名、ユーザパスワード。
- **Cisco DNA Centerユーザ（Users）**：作成する新規 Cisco DNA Center ユーザのユーザ名、パスワード、権限の設定。シスコは通常の Cisco DNA Center 操作すべてで、常にこれらの新しいユーザアカウントのいずれかを使用するよう推奨しています。Cisco DNA Center の再設定や、スーパーユーザ権限が明示的に必要となるその他の操作を除き、管理者用スーパーユーザアカウントは使用しないようにしてください。

この情報を入力する初回セットアップウィザードを起動して対応する方法の詳細については、クイック スタート ワークフローの完了を参照してください。

また残りの設定タスクを完了するために次の情報が必要になります。これは初回ログイン後に実行できます。

- **ISE サーバの IP とログイン情報（ISE Server IP and Credentials）**：Cisco ISE サーバの IP アドレスとログイン情報、管理ユーザ名、パスワードが必要です。これらは「CISCO ISE と Cisco DNA Center の統合」で説明されているように、組織の ISE サーバにログインして Cisco DNA Center とのデータ共有設定を行うために必要です。

  新規またはアップグレードのインストールでは Cisco DNA Center が設定され、Cisco ISE が認証およびポリシー（AAA）サーバとして設定されているかどうかを確認します。正しいバージョンの Cisco ISE がすでに設定されている場合、Cisco ISE から Cisco DNA Center へのグループポリシーデータの移行を開始できます。

  Cisco ISE が設定されていない場合、または必要なバージョンの Cisco ISE が存在しない場合は、Cisco DNA Center がインストールされますが、グループベースのポリシーは無効になります。Cisco ISE をインストールまたはアップグレードして、Cisco DNA Center に接続する必要があります。その後はデータ移行を開始できます。

Cisco DNA Center 以前のバージョンに存在するデータは、アップグレード時に保持されます。データ移行操作では Cisco DNA Center と Cisco ISE のデータがマージされます。移行で競合が発生した場合は Cisco ISE のデータが優先されます。

Cisco DNA Center が使用できなくなった場合、さらに Cisco DNA Center より前のポリシーを管理する必要がある場合、Cisco ISE には読み取り専用設定を上書きするオプションがあります。これで Cisco ISE のポリシーを直接変更できます。Cisco DNA Center が再び使用可能になったら、Cisco ISE の読み取り専用設定を無効にして、Cisco DNA Center の [グループベースのアクセスコントロール設定（Group Based Access Control Settings）] ページを同期しなおす必要があります。Cisco ISE で直接行われた変更は Cisco DNA Center に反映されないため、絶対に必要な場合にのみこのオプションを使用してください。

- **認証およびポリシーサーバ情報（Authorization and Policy Server Information）**：認証サーバまたはポリシーサーバとして Cisco ISE を使用している場合、前項目と同じ情報が必要になるほか、ISE CLI ユーザ名、CLI パスワード、サーバ FQDN、サブスクライバ名（*cdnac* など）、ISE SSH キー（オプション）、プロトコル選択（RADIUS または TACACS）、認証ポート、アカウンティングポート、再試行、タイムアウトの設定が必要となります。

  Cisco ISE 以外の認証サーバ、ポリシーサーバを使用している場合、サーバの IP アドレス、プロトコルの選択（RADIUS または TACACS）、認証ポート、アカウンティングポート、再試行、タイムアウトの設定が必要になります。

  この情報は、選択した認証サーバ、ポリシーサーバと Cisco DNA Center を統合するために必要です。詳細については、認証サーバとポリシー サーバの設定を参照してください。

- **SNMP の再試行とタイムアウト値（SNMP Retry and Timeout Values）**：これは「SNMP プロパティの設定」で説明されているように、デバイスのポーリングとモニタリングをセットアップするために必要です。

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。