



# Firepower Threat Defense のハイ アベイラビリティ

次のトピックでは、Cisco Firepower Threat Defense のハイ アベイラビリティを達成するためにアクティブ/スタンバイ フェールオーバーを設定する方法について説明します。

- [ハイ アベイラビリティ Firepower Threat Defense について \(1 ページ\)](#)
- [ハイ アベイラビリティ のガイドライン \(18 ページ\)](#)
- [Firepower Threat Defense ハイ アベイラビリティ ペアの追加 \(19 ページ\)](#)
- [オプションの高可用性パラメータの設定 \(22 ページ\)](#)
- [ハイ アベイラビリティ の管理 \(25 ページ\)](#)
- [ハイ アベイラビリティ のモニタリング \(33 ページ\)](#)

## ハイ アベイラビリティ Firepower Threat Defense について

フェールオーバーとも呼ばれるハイアベイラビリティを設定するには、専用フェールオーバーリンク（および任意でステートリンク）を介して相互に接続された2台の同じFirepower Threat Defense デバイスが必要です。Firepower Threat Defense はアクティブ/スタンバイ フェールオーバーをサポートしています。つまり1台のユニットがアクティブなユニットとなりトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニタされます。所定の条件に一致すると、フェールオーバーが行われます。



(注) ハイ アベイラビリティは、パブリック クラウドで実行される Firepower Threat Defense Virtual ではサポートされていません。

## ハイ アベイラビリティ のシステム要件

この項では、ハイ アベイラビリティ コンフィギュレーションにある Firepower Threat Defense デバイスのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

### ハードウェア要件

ハイ アベイラビリティ コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。さらに、コンテナ インスタンスでは、同じリソース プロファイル属性を使用する必要があります。

ハイ アベイラビリティ ペアを FMC に追加した後にリソース プロファイルを変更する場合は、**[Devices] > [Device Management] > [Device] > [System] > [Inventory]** ダイアログ ボックスで各ユニットのインベントリを更新します。

- インターフェイスの数とタイプが同じであること。

プラットフォームモードでは、ハイ アベイラビリティ を有効にする前に、すべてのインターフェイスが FXOS で同一に事前構成されている必要があります。ハイ アベイラビリティ を有効にした後でインターフェイスを変更する場合は、スタンバイユニットの FXOS でインターフェイスを変更し、アクティブユニットで同じ変更を行います。

ハイ アベイラビリティ コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してください。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

### ソフトウェア要件

ハイ アベイラビリティ コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- 同じファイアウォール モードにあること（ルーテッドまたはトランスペアレント）。
- ソフトウェア バージョンが同じであること。
- Firepower Management Center 上で、同じドメインまたはグループに入っていること。
- NTP 設定が同じであること。[脅威に対する防御のための NTP 時刻同期の設定](#)を参照してください。
- 非コミットの変更で、Firepower Management Center 上で完全に展開していること。
- どのインターフェイスでも、DHCP または PPPoE は変更していないこと。
- (Firepower 4100/9300) 同じフローオフロードモードを使用し、両方とも有効または無効になっている。

## 高可用性ペアでの FTD デバイスのライセンス要件

ハイアベイラビリティ構成での Firepower Threat Defense デバイスは、すべて同じライセンスである必要があります。ハイアベイラビリティを確立する前に、どのライセンスがセカンダリ/スタンバイ デバイスに割り当てられているかどうかは問題にはなりません。ハイアベイラビリティの設定中に、Firepower Management Center はスタンバイに割り当てられている不要なライセンスをすべて削除し、プライマリ/アクティブ デバイスに割り当てられているのと同じライセンスで置き換えます。たとえば、アクティブ デバイスは基本ライセンスと Threat ライセンスであり、スタンバイ デバイスは基本ライセンスだけの場合、Firepower Management Center は Cisco Smart Software Manager と通信して、アカウントからスタンバイ デバイス用に使用可能な Threat ライセンスを取得します。スマートライセンス アカウントで十分な数の資格が購入されていない場合は、正しい数のライセンスを購入するまで、アカウントは非準拠の状態になります。ハイアベイラビリティ構成には、2つのスマートライセンス資格（ペアを構成するデバイスごとに1つ）が必要です。

## フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2つの装置間の専用接続です。シスコでは、フェールオーバーリンクまたはステートフルフェールオーバーリンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス (eth0) を使用します。

### フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

### フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態 (アクティブまたはスタンバイ)
- hello メッセージ (キープアライブ)
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

### フェールオーバー リンクのインターフェイス

使用されていないデータ インターフェイス (物理、冗長、または EtherChannel) はいずれもフェールオーバー リンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。サブインターフェイスを使用することもできません。コンテナインスタンスの Firepower 4100/9300 シャーシで定義されたサブインターフェイスを除きます。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとして

は設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。

FTD は、ユーザ データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバーリンクやデータのために使用することもできません（Firepower 4100/9300 シャーシのサブインターフェイスのみ）。フェールオーバーリンクに対して Firepower 4100/9300 サブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと親自体をフェールオーバーリンクとして使用することは制限されています。



- (注) フェールオーバーまたはステートリンクとして EtherChannel または冗長インターフェイスを使用している場合、ハイ アベイラビリティを確立する前に、両方のデバイスで同じメンバインターフェイスを備えた同じ EtherChannel または冗長インターフェイスが存在していることを確認する必要があります。

フェールオーバーリンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください:

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットの検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

フェールオーバーリンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中の EtherChannel の設定は変更できません。

## フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- Firepower Threat Defense デバイスのフェールオーバーインターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他のデバイスのないスイッチを使用する。
- イーサネットケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

## ステートフル フェールオーバー リンク

ステートフルフェールオーバーを使用するには、接続ステート情報を渡すためのステートフルフェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。



(注) ステートフルフェールオーバー リンクの帯域幅は、少なくともデータ インターフェイスの帯域幅と同等にすることを推奨します。

### フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステートリンクとフェールオーバーリンク専用のインターフェイスを検討する必要があります。

### ステートフル フェールオーバー リンクの専用インターフェイス

ステートリンク専用のデータ インターフェイス（物理、冗長、または EtherChannel）を使用できます。ステートリンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。

次の 2 つの方法のいずれかで、専用のステート リンクを接続します。

- Firepower Threat Defense デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他のデバイスのないスイッチを使用する。
- イーサネット ケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

Firepower Threat Defense デバイスは、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステートリンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

## フェールオーバーリンクとデータリンクの中断の回避

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバーリンクとデータインターフェイスは異なるパスを通すことを推奨します。フェールオーバーリンクがダウンした場合、フェールオーバーが必要かどうかの決定に、Firepower Threat Defense デバイスはデータインターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバーリンクの正常性が復元されるまで停止されます。

耐障害性フェールオーバーネットワークの設計については、次の接続シナリオを参照してください。

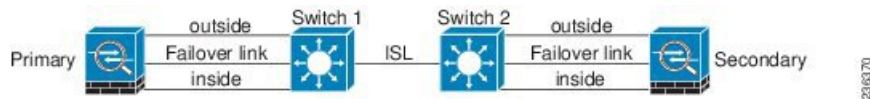
### シナリオ 1：非推奨

2つの Firepower Threat Defense デバイス間のフェールオーバーとデータインターフェイスの両方を接続するために1つのスイッチまたは一連のスイッチを使用している場合、スイッチまたはスイッチ間リンクがダウンしていると、両方の Firepower Threat Defense デバイスがアクティブになります。したがって、次の図で示されている2つの接続方式は推奨しません。

図 1: 単一のスイッチを使用した接続：非推奨



図 2: 2つのスイッチを使用した接続：非推奨



### シナリオ 2：推奨

フェールオーバーリンクには、データインターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバーリンクを接続します。

図 3: 異なるスイッチを使用した接続

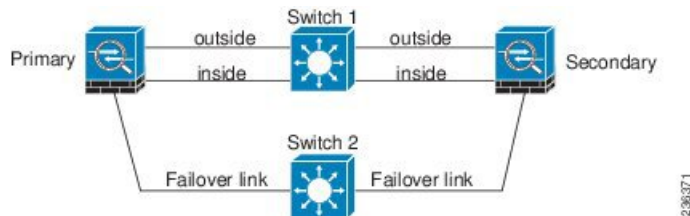
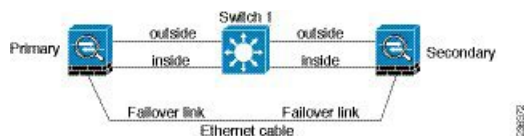


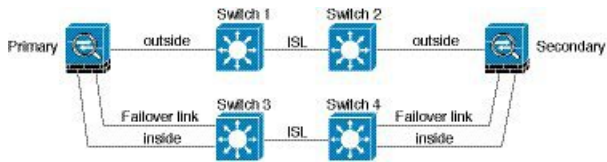
図 4: ケーブルを使用した接続



## シナリオ 3 : 推奨

Firepower Threat Defense データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバーリンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 5: セキュア スイッチを使用した接続



## シナリオ 4 : 推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバーリンクに冗長インターフェイスを使用します。

図 6: 冗長インターフェイスを使用した接続

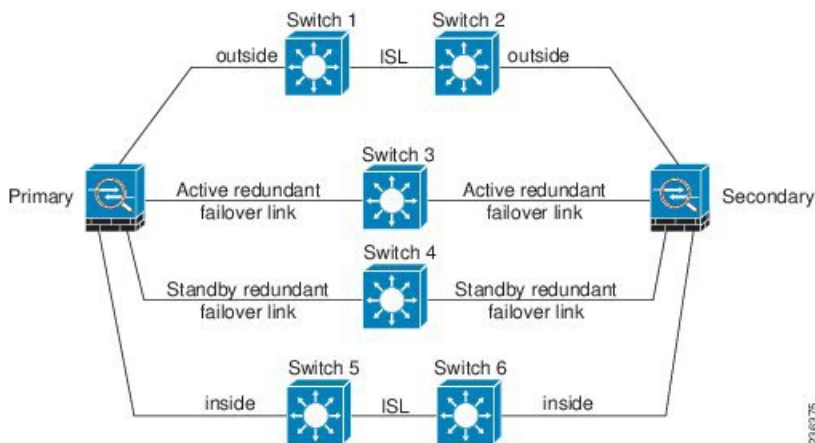
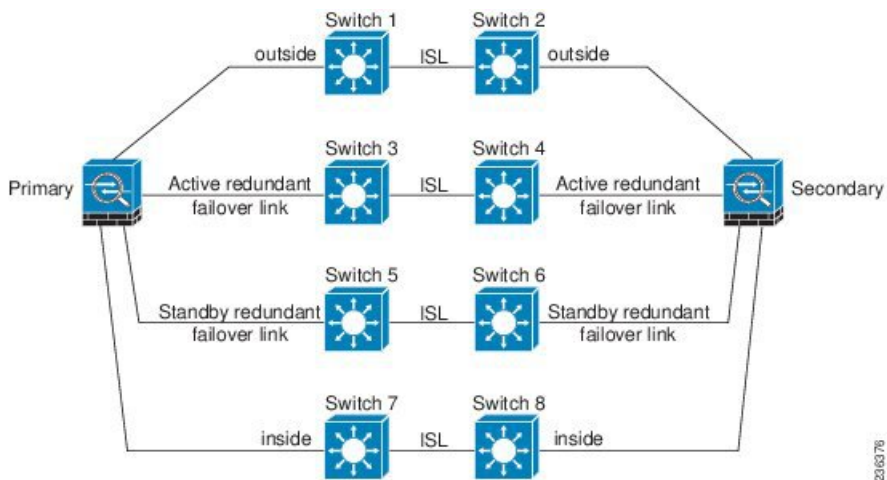


図 7: Inter-Switch Link (ISL) を使用した接続



## ハイ アベイラビリティ の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。一般的に、フェールオーバーが発生した場合、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。



- (注) スタンバイアドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

ステートリンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

### アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ ハイ アベイラビリティ の場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. アクティブな装置は常にプライマリ装置の IP アドレスと MAC アドレスを使用します。
2. アクティブ装置が故障すると、スタンバイ装置は故障した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
3. 故障した装置がオンラインに復帰すると、スタンバイ状態となり、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ (アクティブ) 装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワークトラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想 MAC アドレスを設定しなかった場合、トラフィックフローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。Firepower Threat Defense デバイスは MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。



## 仮想 MAC アドレス

Firepower Threat Defense デバイスには、仮想 MAC アドレスを設定する複数の方法があります。1つの方法のみを使用することをお勧めします。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

マルチインスタンス機能では、FXOS シャーシがすべてのインターフェイスにプライマリ MAC アドレスのみを自動生成します。プライマリおよびセカンダリ MAC アドレスの両方で、生成された MAC アドレスを仮想 MAC アドレスで上書きすることができますが、セカンダリ MAC アドレスを事前に定義することは必須ではありません。セカンダリ MAC アドレスを設定すると、セカンダリ装置のハードウェアが新しい場合に、to-the-box 管理トラフィックが中断されないようになります。

## ステートフル フェールオーバー

ステートフルフェールオーバー中にアクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報を利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

## サポートされる機能

ステートフルフェールオーバーでは、次のステート情報がスタンバイ Firepower Threat Defense デバイスに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および HTTP 接続状態を含む状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- 厳密な TCP 強制を含む、Snort の接続状態、インスペクション結果、およびピンホール情報。
- ARP テーブル
- レイヤ 2 ブリッジテーブル (ブリッジグループ用)
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリングセッションとピンホール。
- スタティックおよびダイナミックルーティングテーブル: ステートフルフェールオーバーはダイナミックルーティングプロトコル (OSPF や EIGRP など) に参加するため、アクティブ装置上のダイナミックルーティングプロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース (RIB) テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリユニットには最初にプライマリユニットをミラーリン

グするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIBテーブルのエポック番号が増加します。再コンバージェンス中に、OSPFおよびEIGRPルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルートエントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIBには新しくアクティブになった装置での最新のルーティングプロトコル転送情報が含まれています。



(注) ルートは、アクティブ装置上のリンクアップまたはリンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミックルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイスで設定された DHCP サーバは、DHCP クライアントにアドレスを付与する前にアドレスが使用されていないことを確認するために ping を送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS とは関連性はありません。
- アクセス コントロール ポリシーの判断：フェールオーバー時には、トラフィックの照合（URL、URL カテゴリ、地理位置情報など）、侵入検知、マルウェア、ファイルタイプに関する判断が保持されます。ただし、フェールオーバーの時点で評価される接続には、次のような注意事項があります。
  - AVC：App-ID 判定は複製されますが、検出状態は複製されません。フェールオーバーが発生する前に、App-ID 判定が完了および同期されていれば、正常に同期は行われます。
  - 侵入検知状態：フェールオーバーの際、フロー中にピックアップが発生すると、新しいインスペクションは完了しますが、古い状態は失われます。
  - ファイル マルウェア ブロックング：ファイルの処分は、フェールオーバー前にできるようになる必要があります。
  - ファイル タイプ検出とブロックング：ファイルタイプは、フェールオーバー前に特定される必要があります。元のアクティブ デバイスでファイルを特定している間にフェールオーバーが発生すると、ファイルタイプの同期は失われます。ファイル ポリシーでそのファイルタイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。
- ユーザ エージェントと ISE セッション ディレクトリを介してパッシブに収集されたユーザと IP アドレスのマッピングを含むアイデンティティ ポリシーや、キャプティブ ポータルを介したアクティブ認証の、ユーザ識別の判断。フェールオーバーの時点でアクティブ認証していたユーザには、再度認証を求めるプロンプトが表示されることがあります。

- ネットワーク AMP：クラウドルックアップは各デバイスから独立しているため、一般的に、フェールオーバーはこの機能には影響しません。具体的には次のとおりです。
  - 署名ルックアップ：ファイルの送信中にフェールオーバーが発生した場合、ファイルイベントは生成されず、検出も発生しません。
  - ファイルストレージ：ファイルの保存中にフェールオーバーが発生した場合、元のアクティブデバイスに保存されます。ファイルの保存中に元のアクティブなデバイスがダウンした場合、ファイルは保存されません。
  - ファイルの事前分類（ローカル分析）：事前分類中にフェールオーバーが発生した場合、検出は失敗します。
  - ファイル ダイナミック分析（クラウドとの接続性）：フェールオーバーが発生しても、システムはクラウドにファイルを提出できます。
  - アーカイブ ファイル サポート：分析中にフェールオーバーが発生した場合、システムはファイル/アーカイブ内の可視性を失います。
  - カスタムブラックリスト：フェールオーバーが発生した場合、イベントは生成されません。
- セキュリティインテリジェンス判断。ただし、フェールオーバーの時点で処理されていた DNS ベースの判断は完了しません。
- RA VPN：リモートアクセス VPN エンドユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバープロセス中にパケットを失って、パケット損失から回復できない可能性があります。

## サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ Firepower Threat Defense デバイスに渡されません。

- GRE や IP-in-IP などのプレーンテキストトンネル内のセッション。トンネル内のセッションは複製されず、新しいアクティブノードは、既存のインスペクションの判定を再利用して、正しいポリシー ルールを照合することができません。
- SSL 復号ポリシーにより復号された接続：復号状態は同期されず、現在の復号された接続はリセットされ、ブロックされます。新しい接続が適切に機能します。（復号しないルールと一致する）復号されない接続は影響を受けず、他の TCP 接続と同様に正しく複製されます。
- TCP ステート バイパス接続
- マルチキャスト ルーティング。

## ハイ アベイラビリティのためのブリッジグループの要件

ブリッジグループを使用する場合は、ハイ アベイラビリティに関して特別な考慮事項があります。

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパンニング ツリー プロトコル (STP) を実行しているスイッチ ポートは、トポロジ変更を検出すると 30 ~ 50 秒間ブロッキング状態に移行できます。ポートがブロッキング状態の間の□ブリッジグループメンバーインターフェイスでのトラフィックの損失を回避するために、次の回避策のいずれかを設定できます。

- アクセス モードのスイッチ ポート : スイッチで STP PortFast 機能を有効にします。

```
interface interface_id
  spanning-tree portfast
```

PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディングモードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがグループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- スイッチ ポートがトランク モードになっている場合、または STP PortFast を有効にできない場合は、フェールオーバー機能または STP の安定性に影響を与える、次のあまり望ましくない回避策のいずれかを使用できます。
  - ブリッジグループおよびメンバー インターフェイスでインターフェイス モニタリングを無効にします。
  - フェールオーバー基準のインターフェイス保留時間を、ユニットがフェールオーバーする前に STP が収束できる大きな値に増やします。
  - スイッチの STP タイマーを短くして、STP がインターフェイス保留時間よりも早く収束できるようにします。

## フェールオーバーのヘルス モニタリング

Firepower Threat Defense デバイスは、各装置について全体的なヘルスおよびインターフェイスヘルスをモニタします。この項では、各装置の状態を判断するために、Firepower Threat Defense デバイスがテストを実行する方法について説明します。

### 装置のヘルス モニタリング

Firepower Threat Defense デバイスは、hello メッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、フェールオーバーリンクを含む各データインターフェイスで LANTEST メッセージを送信し、ピアが応答するかどうかを確認します。Firepower Threat Defense デバイスが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- Firepower Threat Defense デバイスがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- Firepower Threat Defense デバイスがフェールオーバー リンクで応答を受信せず、データインターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- Firepower Threat Defense デバイスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

## インターフェイス モニタリング

ユニットは、モニタ対象のインターフェイス上で 15 秒間 hello メッセージを受信しなかった場合に、インターフェイステストを実行します。1つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、デバイスはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ ([**デバイス (Devices)**] > [**デバイス管理 (Device Management)**] > [**ハイアベイラビリティ (High Availability)**] > [**フェールオーバートリガー条件 (Failover Trigger Criteria)**] を参照)、さらに、アクティブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したデバイスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイモードに戻ります。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、デバイスは IPv4 を使用してヘルス モニタリングを実行します。インターフェイスに IPv6 アドレスだけが設定されている場合、デバイスは ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリングテストを実行します。ブロードキャスト ping テストの場合、デバイスは IPv6 全ノードアドレス (FE02::1) を使用します。

## インターフェイス テスト

Firepower Threat Defense デバイスでは、次のインターフェイステストが使用されます。各テストの時間は。

1. リンクアップ/ダウンテスト：インターフェイスステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、デバイスは障害が発生し、テストが停止したと見なします。ステータスがアップの場合、デバイスはネットワーク アクティビティを実行します。

2. ネットワーク アクティビティ テスト：ネットワークの受信アクティビティのテストです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると思われ見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思われ見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスは ARP テストを開始します。
3. ARP テスト：ARP が正しく応答するかどうかをテストします。各ユニットは、ARP テーブル内の最新のエントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると思われ見なされます。ユニットが ARP 応答を受信しない場合、デバイスは、ARP テーブル内の「次の」エントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると思われ見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思われ見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスはブートストラップ ping テストを開始します。
4. ブロードキャスト Ping テスト：ping 応答が正しいかどうかをテストします。各ユニットがブロードキャスト ping を送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると思われ見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思われ見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARP テストを使用してテストが再開されます。両方のユニットが ARP およびブロードキャスト Ping テストからトラフィックを受信し続けない場合、これらのテストは引き続き永続的に実行されます。

## インターフェイス ステータス

モニタ対象のインターフェイスには、次のステータスがあります。

- **Unknown**：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合があります。
- **Normal**：インターフェイスはトラフィックを受信しています。
- **Normal (Waiting)**：インターフェイスは起動していますが、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- **Normal (Not-Monitored)**：インターフェイスは動作中ですが、フェールオーバープロセスによってモニタされていません。
- **Testing**：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。

- Link Down : インターフェイスまたは VLAN は管理上ダウンしています。
- Link Down (Waiting) : インターフェイスまたは VLAN は管理上ダウンしており、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- Link Down (Not-Monitored) : インターフェイスまたは VLAN は管理上ダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- No Link : インターフェイスの物理リンクがダウンしています。
- No Link (Waiting) : インターフェイスの物理リンクがダウンしており、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。
- No Link (Not-Monitored) : インターフェイスの物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- Failed : インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

## フェールオーバー トリガーおよび検出タイミング

次の表に、フェールオーバー トリガー イベントと、関連する障害検出のタイミングを示します。フェールオーバーが発生した場合、フェールオーバーの理由およびその他のハイアベイラビリティ ペアに関するさまざまな作業をメッセージセンターで表示できます。

表 1 : Firepower Threat Defense フェールオーバー時間

| フェールオーバートリガー イベント  | 最小      | デフォルト | 最大数  |
|--|---------|-------|------|
| アクティブ ユニットで電源切断が生じる、または通常の動作が停止する。                         | 800 ミリ秒 | 15 秒  | 45 秒 |
| アクティブ ユニット インターフェイス物理リンクがダウンする。                            | 500 ミリ秒 | 5 秒   | 15 秒 |
| アクティブ ユニットの インターフェイスは実行されているが、接続の問題により インターフェイス テストを行っている。 | 5 秒     | 25 秒  | 75 秒 |

## アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Firepower Threat Defense デバイスに引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

### プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーを設定する場合、1つのユニットをプライマリとして設定し、もう1つのユニットをセカンダリとして設定します。設定中に、プライマリユニットのポリシーは、セカンダリユニットに同期化されます。この時点で、2つのユニットは、デバイスおよびポリシー設定に関して単一のデバイスとして機能します。ただし、イベント、ダッシュボード、レポートおよびヘルスマonitoringに関しては、別々のデバイスとして引き続き表示されます。

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリ ユニット（設定で指定）とセカンダリ ユニットとの間には、いくつかの相違点があります。

- 両方のユニットが同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ ユニットが常にアクティブユニットになります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバーリンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ ユニットの MAC アドレスが使用されます。

### 起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

### フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われません。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたは



フェールオーバーなし)、アクティブユニットが行うアクション、スタンバイユニットが行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 2: フェールオーバー イベント

| 障害イベント                       | ポリシー       | アクティブグループのアクション      | スタンバイグループのアクション            | 注記 (Notes)   |
|------------------------------|------------|----------------------|----------------------------|--|
| アクティブユニットが故障 (電源またはハードウェア)   | フェールオーバー   | 適用対象外                | アクティブになる<br>アクティブに故障とマークする | モニタ対象インターフェイスまたはフェールオーバーリンクで hello メッセージは受信されません。                                  |
| 以前にアクティブであったユニットの復旧          | フェールオーバーなし | スタンバイになる             | 動作なし                       | なし。  |
| スタンバイユニットが故障 (電源またはハードウェア)   | フェールオーバーなし | スタンバイに故障とマークする       | 適用対象外                      | スタンバイユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。              |
| 動作中にフェールオーバーリンクに障害が発生した      | フェールオーバーなし | フェールオーバーリンクに故障とマークする | フェールオーバーリンクに故障とマークする       | フェールオーバーリンクがダウンしている間、ユニットはスタンバイユニットにフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。 |
| スタートアップ時にフェールオーバーリンクに障害が発生した | フェールオーバーなし | フェールオーバーリンクに故障とマークする | アクティブになる                   | スタートアップ時にフェールオーバーリンクがダウンしていると、両方のユニットがアクティブになります。                                  |
| ステートリンクの障害                   | フェールオーバーなし | 動作なし                 | 動作なし                       | ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。   |

| 障害イベント                          | ポリシー       | アクティブグループのアクション | スタンバイグループのアクション | 注記 (Notes)  |
|---------------------------------|------------|-----------------|-----------------|---|
| アクティブユニットにおけるしきい値を超えたインターフェイス障害 | フェールオーバー   | アクティブに故障とマークする  | アクティブになる        | なし。   |
| スタンバイユニットにおけるしきい値を超えたインターフェイス障害 | フェールオーバーなし | 動作なし            | スタンバイに故障とマークする  | スタンバイユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。 |

## ハイ アベイラビリティ のガイドライン

### モデルのサポート

- Firepower 9300 : シャーシ内ハイ アベイラビリティはサポートされません。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の Firepower Threat Defense Virtual では、レイヤ 2 接続が必要なため、ハイ アベイラビリティはサポートされません。

### その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパンニング ツリー プロトコル (STP) を実行している接続済みスイッチポートが、トポロジの変化を検出すると 30～50 秒間ブロッキング状態になる可能性があります。ポートがブロッキングステータスである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

#### **interface *interface\_id* spanning-tree portfast**

この回避策は、ルーテッド モードおよびブリッジ グループ インターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- ローカル CA サーバが設定されている場合、フェールオーバーを有効にできません。CA コンフィギュレーションを削除するには、**no crypto ca server** コマンドを使用します。

- Firepower Threat Defense フェールオーバー ペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュアポートで設定または学習されたセキュア MAC アドレスが別のセキュアポートに移動し、スイッチのポートセキュリティ機能によって違反フラグが付けられた場合に発生します。
- アクティブ/スタンバイ ハイ アベイラビリティ と VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブユニットとスタンバイユニットの両方をモニタすることはできません。スタンバイユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

## Firepower Threat Defense ハイ アベイラビリティ ペアの追加

| スマート ライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|------------|----------|--|-------------|---------------------|
| 任意 (Any)   | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

アクティブ/スタンバイの高可用性ペアを確立するには、一方のデバイスをプライマリ、他方をセカンダリとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合する場合、システムはプライマリとして指定されたデバイスの構成を適用します。

マルチドメインの導入環境では、高可用性ペアのデバイスが同じドメインに属している必要があります。



- (注) ステートフル フェールオーバー リンクがピア間のアプリケーション コンテンツの同期に使用されている場合には、システムはフェールオーバーリンクを使用して構成を同期します。フェールオーバーリンクとステートフルフェールオーバーリンクはプライベート IP スペースにあり、ハイアベイラビリティペアのピア間の通信にのみ使用されます。ハイアベイラビリティが確立された後は、ハイアベイラビリティペアを解除して再構成することなく、選択したインターフェイスリンクと暗号化設定を変更することはできません。



**注意** Firepower Threat Defense のハイ アベイラビリティ ペアを作成または破棄すると、プライマリおよびセカンダリ デバイスの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細は[Snort® の再起動によるトラフィックの動作](#)を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

### 始める前に

以下の点について両方のデバイスを確認してください。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。
- ドメインおよびグループが同じであること。
- 通常のヘルス ステータスであり、同じソフトウェアを実行していること。
- ルーティングされているか、またはトランスペアレント モードであること。
- NTP 設定が同じであること。[脅威に対する防御のための NTP 時刻同期の設定](#)を参照してください。
- 未確定の変更がない状態で、完全に展開されていること。
- すべてのインターフェイスで DHCP または PPPoE が設定されていないこと。



(注) プライマリ デバイスで利用可能な証明書がセカンダリ デバイスに存在しない場合は、2 台の Firepower Threat Defense デバイス間でハイ アベイラビリティを構成することができます。ハイ アベイラビリティが構成されると、証明書がセカンダリ デバイス上で同期されます。

### 手順

- ステップ 1** [Firepower Management Center へのデバイスの追加](#) に従って、両方のデバイスを Firepower Management Center に追加します。
- ステップ 2** **[Devices] > [Device Management]** を選択します。
- ステップ 3** **[追加 (Add)]** ドロップダウン メニューから、**[高可用性の追加 (Add High Availability)]** を選択します。
- ステップ 4** 高可用性ペアの表示用の **[名前 (Name)]** を入力してください。
- ステップ 5** **[デバイス タイプ (Device Type)]** では、**[Firepower Threat Defense]** を選択します。

- ステップ 6** 高可用性ペアの [プライマリ ピア (Primary Peer) ] デバイスを選択します。
- ステップ 7** 高可用性ペアの [セカンダリ ピア (Secondary Peer) ] デバイスを選択します。
- ステップ 8** [続行 (Continue) ] をクリックします。
- ステップ 9** LAN フェールオーバー リンクでは、フェールオーバーの通信のための十分な帯域幅の [インターフェイス (Interface) ] を選択します。
- (注) 論理名がなくセキュリティゾーンに属さないインターフェイスのみが、[ハイ アベイラビリティ ペアの追加 (Add High Availability Pair) ] ダイアログの [インターフェイス (Interface) ] ドロップダウンに一覧表示されます。
- ステップ 10** 識別するための任意の [論理名 (Logical Name) ] を入力します。
- ステップ 11** アクティブなユニットの、フェールオーバー リンクの [プライマリ IP (Primary IP) ] アドレスを指定します。このアドレスは、未使用のサブネット上になければなりません。
- (注) 169.254.0.0/16 および fd00:0:0:::/64 は内部で使用されるサブネットです。フェールオーバーやステート リンクにはこれらを使用できません。
- ステップ 12** 必要に応じて、[IPv6 アドレスを使用 (Use IPv6 Address) ] を選択します。
- ステップ 13** スタンバイ ユニットのフェールオーバー リンクの [セカンダリ IP (Secondary IP) ] アドレスを指定します。この IP アドレスはプライマリ IP アドレスのように、同じサブネット内になければなりません。
- ステップ 14** IPv4 アドレスを使用する場合、プライマリとセカンダリの IP アドレス両方に適用されるサブネットマスクを入力します。
- ステップ 15** 必要に応じて、ステートフル フェールオーバー リンクでは、同じインターフェイスを選択するか、または別のインターフェイスを選択し、高可用性の設定情報を入力します。
- (注) 169.254.0.0/16 および fd00:0:0:::/64 は内部で使用されるサブネットです。フェールオーバーやステート リンクにはこれらを使用できません。
- ステップ 16** 必要に応じて、フェールオーバー リンク間の IPsec 暗号化について、[有効 (Enabled) ] を選択し、さらに [キー生成 (key generate) ] メソッドを選択します。
- ステップ 17** [OK] をクリックします。システム データの同期が行われるため、このプロセスが完了するまでに数分かかります。

---

### 次のタスク

デバイスがバックアップされていることを確認します。バックアップは、障害が発生したデバイスを迅速に交換するため、Firepower Management Center からリンク解除せずにハイ アベイラビリティ サービスを回復するために使用できます。デバイスのバックアップ手順については、[リモートでの デバイスのバックアップ](#)を参照してください。

## オプションの高可用性パラメータの設定

最初の高可用性構成を Firepower Management Center で確認できます。高可用性ペアを解除して再設定しないと、これらの設定を編集することはできません。

フェールオーバーの結果を改善するために、フェールオーバー トリガー条件を編集できます。インターフェイスモニタリングでは、どのインタフェースがフェールオーバーに適しているかを判断できます。

## スタンバイ IP アドレスとインターフェイス モニタリングの設定

| スマート ライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|------------|----------|--|-------------|---------------------|
| 任意 (Any)   | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

各インターフェイスにスタンバイ IP アドレスを設定します。スタンバイ アドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。

デフォルトでは、論理名が設定されているすべての物理インターフェイスでモニタリングが有効になっています。重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないようにできます。

### 手順

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** 編集するデバイス ハイ アベイラビリティ ペアの横にある 編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [High Availability] タブをクリックします

**ステップ 4** [モニタ対象インターフェイス (Monitored Interfaces)] エリアで、編集するインターフェイスの横にある 編集アイコン (✎) をクリックします。

**ステップ 5** [このインターフェイスの障害をモニタする (Monitor this interface for failures)] チェック ボックスをオンにします。

**ステップ 6** [IPv4] タブで、[スタンバイ IP アドレス (Standby IP Address)] を入力します。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリー アドレスである必要があります。

**ステップ 7** IPv6 アドレスを手動で設定した場合、[IPv6] タブでアクティブ IP アドレスの横にある 編集アイコン (✎) をクリックして、[スタンバイIPアドレス (Standby IP Address)] を入力し、[OK] をクリックします。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリー アドレスである必要があります。自動生成 [EUI 64の適用 (Enforce EUI 64)] アドレスの場合、スタンバイアドレスは自動的に生成されます。

**ステップ 8** [OK] をクリックします。

## ハイ アベイラビリティ フェールオーバー条件の編集

| スマート ライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|------------|----------|--|-------------|---------------------|
| 任意 (Any)   | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

ネットワーク配置に基づいてフェールオーバー条件をカスタマイズできます。

### 手順

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** 編集するデバイス ハイ アベイラビリティ ペアの横にある 編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [ハイアベイラビリティ (High Availability)] を選択します。

**ステップ 4** [フェールオーバートリガー条件 (Failover Trigger Criteria)] の横にある 編集アイコン (✎) をクリックします。

**ステップ 5** [インターフェイス障害しきい値 (Interface Failure Threshold)] で、デバイスがフェールオーバーする条件となるインターフェイスの失敗の数または割合を選択します。

**ステップ 6** [helloパケット間隔 (Hello packet Intervals)] で、フェールオーバー リンクを介して送信される hello パケットの頻度を選択します。

**ステップ 7** [OK] をクリックします。

## 仮想 MAC アドレスの設定

| スマートライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|-----------|----------|--|-------------|---------------------|
| 任意 (Any)  | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

フェールオーバーのため、以下の Firepower Management Center の 2 か所にアクティブ MAC アドレスとスタンバイ MAC アドレスを設定できます。

- [インターフェイスの編集 (Edit Interface)] ページの [詳細 (Advanced)] タブ。 [MAC アドレスの設定](#) を参照してください。
- [高可用性 (High Availability)] ページからアクセスする [インターフェイス MAC アドレスの追加 (Add Interface MAC Address)] ページ。次を参照してください。

アクティブ MAC アドレスとスタンバイ MAC アドレスが両方の場所で設定されている場合、フェールオーバーではインターフェイスの設定で定義されたアドレスが優先されます。

物理インターフェイスにアクティブ MAC アドレスとスタンバイ MAC アドレスを指定することでフェールオーバー中のトラフィック喪失を最低に抑えることができます。この機能は、フェールオーバーのための IP アドレスのマッピングに冗長性を提供します。

### 手順

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** 編集するデバイスハイアベイラビリティペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [ハイアベイラビリティ (High Availability)] を選択します。

**ステップ 4** インターフェイス MAC アドレスの横にある追加アイコン (+) を選択します。

**ステップ 5** [物理インターフェイス (Physical Interface)] を選択します。

**ステップ 6** [アクティブインターフェイス MAC アドレス (Active Interface Mac Address)] を入力します。

**ステップ 7** [スタンバイインターフェイス MAC アドレス (Standby Interface Mac Address)] を入力します。

**ステップ 8** [OK] をクリックします。



## ハイ アベイラビリティ の管理

この項では、ハイ アベイラビリティ の設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、ハイ アベイラビリティ を有効化した後にハイ アベイラビリティ 装置を管理する方法について説明します。

### Firepower Threat Defense ハイ アベイラビリティ ペアにおけるアクティブ ピアの切り替え

| スマート ライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|------------|----------|--|-------------|---------------------|
| 任意 (Any)   | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

Firepower Threat Defense ハイ アベイラビリティ ペアを確立した後、アクティブ ユニットとスタンバイ ユニートを手動で切り替えることができます。そうすることで、現在のアクティブ ユニットにおける持続的な障害やヘルスイベントなどに起因するフェールオーバーを効果的に実施できます。この手順を実行する前に、両方のユニートを完全に展開しておく必要があります。


#### 始める前に

[Firepower Threat Defense ハイ アベイラビリティ ペアにおけるノードステータスの更新 \(26 ページ\)](#)



(注) これにより、Firepower Threat Defense ハイ アベイラビリティ デバイス ペアのステータスと Firepower Management Center のステータスが同期されます。

#### 手順

- ステップ 1 [Devices] > [Device Management] を選択します。
- ステップ 2 アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (  ) をクリックします。
- ステップ 3 次の操作を実行できます。
  - ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい (Yes) ] をクリックします。

- キャンセルして [デバイス管理 (Device Management) ] ページに戻る場合は、[いいえ (No) ] をクリックします。

## Firepower Threat Defense ハイ アベイラビリティ ペアにおけるノード ステータスの更新

| スマート ライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|------------|----------|--|-------------|---------------------|
| 任意 (Any)   | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

ハイ アベイラビリティ ペアのアクティブ デバイスまたはスタンバイ デバイスが再起動されると、Firepower Management Center はどちらのデバイスでも正確なハイ アベイラビリティ ステータスを表示しない場合があります。これは、Firepower Threat Defense が再起動すると、高可用性ステータスが Firepower Threat Defense 上で直ちに更新され、対応するイベントが Firepower Management Center に送信されるためです。ただし、Firepower Threat Defense と Firepower Management Center 間の通信がまだ確立されていないため、ステータスが Firepower Management Center で更新されないことがあります。

Firepower Management Center と Firepower Threat Defense のデバイスとの間で通信障害が発生したり、通信チャンネルが不安定になったりすると、データの同期が失われる可能性があります。ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスを切り替えると、かなりの時間が経過しても変更が Firepower Management Center に反映されないことがあります。

これらのシナリオでは、ハイ アベイラビリティ ノードのステータスを更新して、ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスに関する正確な情報を取得できます。



- (注) ノードの更新操作は、Firepower Management Center バージョン 6.2.3 以降で管理されている Firepower Threat Defense の高可用性デバイスでのみ可能です。

### 手順

- ステップ 1** [Devices] > [Device Management] を選択します。
- ステップ 2** ノードステータスを更新するハイ アベイラビリティ ペアの横にある [HA ノードのステータス更新 (Refresh HA Node Status) ] アイコン (🔄) をクリックします。
- ステップ 3** 次の操作を実行できます。

- ハイ アベイラビリティ ペアのノード ステータスを更新する場合は、[はい (Yes) ] をクリックします。
- キャンセルして [デバイス管理 (Device Management) ] ページに戻る場合は、[いいえ (No) ] をクリックします。

## ハイ アベイラビリティの中断と再開

ハイ アベイラビリティ ペアの 1 つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状態で、フェールオーバー リンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。

ハイ アベイラビリティを中断すると、デバイスのペアがフェールオーバー ユニットとして動作しなくなります。現在アクティブなデバイスはアクティブなままで、すべてのユーザ接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の疑似-スタンバイ デバイスにフェールオーバーされることはなくなります。スタンバイ デバイスの設定は保持されますが、非アクティブのままです。

HA の中断と HA の破棄の主な違いは、中断された HA デバイスではハイ アベイラビリティ設定が保持されることです。HA を破棄すると、この設定は消去されます。そのため、中断されたシステムで HA を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバー ペアとして再び機能します。

HA を一時停止するには、**configure high-availability suspend** コマンドを使用します。

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

アクティブ装置からハイアベイラビリティを中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

フェールオーバーを再開するには、**configure high-availability resume** コマンドを使用します。

```
> configure high-availability resume
Successfully resumed high-availability.
```

ユニットが中断状態の場合にのみ、ユニットを再開できます。ユニットは、ピアユニットとアクティブ/スタンバイ ステータスをネゴシエートします。



- (注) ハイ アベイラビリティの中断は一時的な状態です。ユニットをリロードすると、ハイ アベイラビリティ設定が自動的に再開され、ピアとアクティブ/スタンバイ ステータスがネゴシエートされます。

## ハイ アベイラビリティ ペアでのユニット交換

次のいずれかの手順を使用すると、ハイ アベイラビリティ ペアで障害が発生したまたは修復済みの Firepower Threat Defense デバイスを交換できます。

- 障害が発生したデバイスのバックアップが利用可能な場合は、[バックアップからの FTD の復元：高可用性](#)の手順を実行するとデバイスを正常に交換できます。



- (注) 障害が発生した Firepower Threat Defense デバイスを Firepower Management Center から登録解除しないでください。復元手順では、トラフィックを損失せずに Firepower Management Center の設定と接続の復元を行います。

- デバイスのバックアップが利用不可の場合は、Firepower Management Center でデバイスを管理不能にし、デバイスを交換してから、ハイ アベイラビリティ ペアを再確立する必要があります。そのため、Firepower Threat Defense のハイ アベイラビリティを中断して再作成する必要があります。その結果、トラフィックが失われることがあります。詳細な手順については、[バックアップなしでのユニット交換 \(28 ページ\)](#) を参照してください。

## バックアップなしでのユニット交換

バックアップをしていない Firepower Threat Defense のハイ アベイラビリティ ペアにおいて故障したユニットを交換する必要がある場合、[ブレイクを強制 (Force Break)] オプション選択して、このペアを分離する必要があります。ユニットを交換するか、修理した後、Firepower Management Center のデバイスを登録し、高可用性を再度確立する必要があります。このプロセスは、デバイスがプライマリ、セカンダリであるかによって異なります。

### プライマリ ユニットの交換

| スマートライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|-----------|----------|--|-------------|---------------------|
| 任意 (Any)  | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

次に示す手順に従って、Firepower Threat Defense の高可用性ペアで障害が発生したプライマリ ユニットの交換します。ここに示した手順に従わないと、既存の高可用性設定を上書きする可能性があります。



**注意** Firepower Threat Defense のハイ アベイラビリティ ペアを作成または破棄すると、プライマリおよびセカンダリ デバイスの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細は[Snort®の再起動によるトラフィックの動作](#)を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

#### 手順

- ステップ 1** [強制切断 (Force Break) ] を選択して、高可用性ペアを分離します。[ハイ アベイラビリティ ペアにおけるユニットの分離 \(31 ページ\)](#) を参照してください。
- (注) 切断操作により、Firepower Threat Defense と Firepower Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。
- ステップ 2** 障害が発生したプライマリ Firepower Threat Defense デバイスの登録を Firepower Management Center から解除します。[Firepower Management Center からのデバイスの削除](#)を参照してください。
- ステップ 3** 交換した Firepower Threat Defense を Firepower Management Center に登録します。[Firepower Management Center へのデバイスの追加](#)を参照してください。
- ステップ 4** 登録時には、既存のセカンダリ/アクティブ ユニットのプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。[Firepower Threat Defense ハイ アベイラビリティ ペアの追加 \(19 ページ\)](#) を参照してください。

## セカンダリ ユニットの交換

| スマートライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|-----------|----------|--|-------------|---------------------|
| 任意 (Any)  | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

次に示す手順に従って、Firepower Threat Defense の高可用性ペアで障害が発生したセカンダリ ユニットの交換します。



**注意** Firepower Threat Defense のハイ アベイラビリティ ペアを作成または破棄すると、プライマリおよびセカンダリ デバイスの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細は [Snort® の再起動によるトラフィックの動作](#) を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

## 手順

**ステップ 1** [強制切断 (Force Break) ] を選択して、高可用性ペアを分離します。 [ハイ アベイラビリティ ペアにおけるユニットの分離 \(31 ページ\)](#) を参照してください。

(注) 切断操作により、Firepower Threat Defense と Firepower Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。

**ステップ 2** セカンダリ Firepower Threat Defense デバイスの登録を Firepower Management Center から解除します。 [Firepower Management Center からのデバイスの削除](#) を参照してください。

**ステップ 3** 交換した Firepower Threat Defense を Firepower Management Center に登録します。 [Firepower Management Center へのデバイスの追加](#) を参照してください。

**ステップ 4** 登録時には、既存のプライマリ/アクティブユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。 [Firepower Threat Defense ハイ アベイラビリティ ペアの追加 \(19 ページ\)](#) を参照してください。

## ハイ アベイラビリティ ペアにおけるユニットの分離

| スマート ライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|------------|----------|--|-------------|---------------------|
| 任意 (Any)   | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

ハイ アベイラビリティ ペアを分断しても、アクティブ デバイスは完全な展開の機能を維持します。スタンバイ デバイスは、フェールオーバー設定とインターフェイス設定を失って、スタンドアロンのデバイスになります。

分断操作前のアクティブ デバイスに展開されていなかったポリシーは、分断操作完了後も展開されません。分断操作完了後、スタンドアロン デバイスにポリシーを展開します。



### ヒント

この例外は、**flex-config** ポリシーです。アクティブ なデバイスに展開されている **flex-config** ポリシーでは、HA の中断操作後に展開の失敗を表示する場合があります。**flex-config** ポリシーを変更してアクティブ なデバイス上に再展開する必要があります。



### (注)

Firepower Management Center を使用して高可用性ペアにアクセスできない場合は、CLI コマンド **configure high-availability disable** を使用して、両方のデバイスからフェールオーバー設定を削除します。

### 始める前に

[Firepower Threat Defense ハイ アベイラビリティ ペアにおけるノード ステータスの更新 \(26 ページ\)](#)



### (注)

これにより、Firepower Threat Defense ハイ アベイラビリティ デバイス ペアのステータスと Firepower Management Center のステータスが同期されます。

### 手順

- ステップ 1** [Devices] > [Device Management] を選択します。
- ステップ 2** 分断する高可用性ペアの横にある HA の分断アイコン (🔪) をクリックします。
- ステップ 3** 必要に応じて、スタンバイ ペアが応答しなかった場合に、強制的に分断するためのチェックボックスをオンにします。

**ステップ 4** [Yes] をクリックします。デバイスの高可用性ペアが分離されます。

分断操作によって、アクティブおよびスタンバイ デバイスからフェールオーバー設定が削除されます。

#### 次のタスク

(オプション) アクティブなデバイス上で flex-config ポリシーを使用している場合は、flex-config ポリシーを変更して再展開し、展開エラーを解消します。

## ハイ アベイラビリティ ペアの登録解除

| スマート ライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|------------|----------|--|-------------|---------------------|
| 任意 (Any)   | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

各ユニットで CLI を使用することによって、Firepower Management Center からペアを削除し、ハイ アベイラビリティを無効にすることができます。

#### 始める前に

この手順では、CLI アクセスが必要です。

#### 手順

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** 登録解除するハイ アベイラビリティ ペアの横にある削除アイコン (🗑️) をクリックします。

**ステップ 3** [Yes] をクリックします。デバイス ハイ アベイラビリティ ペアが削除されます。

**ステップ 4** 各ユニットで、Firepower Threat Defense CLI にアクセスし、次のコマンドを入力します。

#### **configure high-availability disable**

このコマンドを入力しない場合、ユニットを再登録して、新しい HA ペアを形成することはできません。

(注) ファイアウォールモードを変更する前に、このコマンドを入力します。モードを変更すると、ユニットでは **configure high-availability disable** コマンドを入力できなくなります。Firepower Management Center では、このコマンドを使用せずに HA ペアを再形成することはできません。



# ハイ アベイラビリティのモニタリング

このセクションの手順に従うことで、ハイアベイラビリティのステータスをモニタできます。

## フェールオーバー履歴の表示

| スマートライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|-----------|----------|--|-------------|---------------------|
| 任意 (Any)  | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

ハイアベイラビリティの両方のデバイスに関するフェールオーバーの履歴を1つのビューに表示できます。履歴は古いものから順番に表示され、すべてのフェールオーバーの理由が表示されます。

### 手順

**ステップ 1** [Devices] > [Device Management] を選択します。

**ステップ 2** 編集するデバイスハイアベイラビリティペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [サマリー (Summary)] を選択します。

**ステップ 4** [全般 (General)] の下で、表示アイコン (🔍) をクリックします。

## ステートフル フェールオーバーの統計情報の表示

| スマートライセンス | 従来のライセンス | サポートされるデバイス  | サポートされるドメイン | アクセス (Access)       |
|-----------|----------|--|-------------|---------------------|
| 任意 (Any)  | 該当なし     | Firepower Threat Defense<br>Firepower Threat Defense Virtual | 任意 (Any)    | Admin/Network Admin |

ハイ アベイラビリティ ペアのプライマリとセカンダリ デバイス両方のステートフルフェールオーバー リンク統計情報を表示できます。

### 手順

---

**ステップ 1** [Devices] > [Device Management]を選択します。

**ステップ 2** 編集するデバイスハイ アベイラビリティ ペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [ハイ アベイラビリティ (High Availability) ]を選択します。

**ステップ 4** ステートフルフェールオーバー リンクの下にある表示アイコン (🔍) をクリックします。

**ステップ 5** 統計情報を表示するデバイスを選択します。

---