ファイアウォール デバイスでのセキュリティ コンテキストの設定

1 つのセキュリティ アプライアンスに対して複数のセキュリティ「コンテキスト」を定義できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立した仮想デバイスとして機能します。マルチ コンテキストとは、複数のスタンドアロン デバイスが存在するようなものです。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多数の機能がサポートされています。VPN、マルチキャスト、ダイナミック ルーティング プロトコルなど、サポートされていない機能もあります。セキュリティ コンテキストでは、スタティック ルートしかサポートしていないため、マルチ コンテキスト モードで OSPF または RIP をイネーブルにすることはできません。また、ASA デバイスおよび PIX デバイスの IPS フィーチャ セットなど、Cisco Security Manager によって直接管理されない機能もあります。

マルチ コンテキスト モードでは、セキュリティ アプライアンスに各コンテキストの設定が含まれます。この設定で、セキュリティ ポリシーやインターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションが指定されます。システム管理者は、システム設定でコンテキストを設定することにより、コンテキストを追加および管理します。これは、シングルモード設定と同様に起動設定です。システム設定には、セキュリティ アプライアンスの基本的な設定が指定されていますが、それ自身のネットワーク インターフェイスまたはネットワーク設定は含まれていません。システムがネットワーク リソースにアクセスする必要がある場合は（サーバからコンテキストをダウンロードする場合など）、管理コンテキストとして指定されたコンテキストが使用されます。システム設定は、基本的なコンテキスト設定の追加、削除、および編集に使用します（ネットワーク インターフェイスをさまざまなコンテキストに割り当てる場合など）。

管理コンテキストは他のコンテキストと似ていますが、ユーザが管理コンテキストにログインすると、そのユーザはシステム管理者権限を持ち、システム設定およびその他すべてのコンテキストにアクセスできるという点が異なります。

この章は次のトピックで構成されています。

マルチコンテキストモードのイネーブル化とディセーブル化

Cisco Security Manager では、既存のデバイスでマルチ コンテキスト モードに切り替えることはサポートされていません。このタスクを実行するには、Security Manager からデバイスを削除し、デバイス マネージャまたは CLI 入力を使用してマルチコンテキスト モードをイネーブルにした後、再びデバイスを Security Manager に追加する必要があります。マルチ コンテキスト モードでデバイスを追加したあとは、セキュリティ コンテキストを追加、編集、および削除できます。

（注） マルチコンテキストデバイスを手動で定義する場合は、[新しいデバイス - デバイス情報（New Device - Device Information）] ダイアログボックスの [オペレーティングシステム（Operating System）] セクションで 、[コンテキスト（Contexts）] リストから [マルチ（Multi）] を選択します。

同様に、Cisco Security Manager では、既存のデバイスをシングルコンテキスト モードに復元することはサポートされていません。このタスクを実行するには、Security Manager からデバイスおよびその子コンテキストすべてを削除し、デバイス マネージャまたは CLI 入力を使用してシングルコンテキストの動作を復元した後、再びデバイスを Security Manager に追加する必要があります。

（注） シングルコンテキストデバイスを手動で定義する場合は、[新しいデバイス - デバイス情報（New Device - Device Information）] ダイアログボックスの [オペレーティングシステム（Operating System）] セクションで 、[コンテキスト（Contexts）] リストから [シングル（Single）] を選択します。

関連項目

- マルチ セキュリティ コンテキストを設定するためのチェックリスト （3 ページ）
- セキュリティ コンテキストの管理 （6 ページ）
  - [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA） （10 ページ）
  - [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （8 ページ）

マルチ セキュリティ コンテキストを設定するためのチェックリスト

セキュリティ コンテキストを使用すると、1つの物理デバイスを複数の独立したファイアウォールとして使用できます。各セキュリティ コンテキストは、独自の設定を持つ1つの仮想ファイアウォールを定義します。物理デバイスの場合と同様に、各セキュリティ コンテキストは適切に設定する必要があります。そうしない場合、全体的なセキュリティが低下するおそれがあります。このため、同じ物理アプライアンス上で複数のファイアウォールを定義して設定する際は、特に注意が必要です。

次のチェックリストに、複数のセキュリティ コンテキストを使用してファイアウォール デバイスを設定する際に必要な基本手順について概説します。これらの各手順の中にさらに複数の手順が含まれることがあります。すべての手順を、示されている順序どおりに実行してください。たとえば、さまざまなコンテキストを設定する前に、インターフェイスを定義する必要があります。

ステップ	タスク
ステップ 1	**物理アプライアンスで、インターフェイスとサブインターフェイス、またはVLANを定義します。** このタスクでは、FWSM でインターフェイスとサブインターフェイス、または VLAN を定義します。これらは、あとで作成するときに、さまざまなセキュリティ コンテキストに割り当てられます。物理インターフェイスのパラメータを指定します。たとえば、接続タイプ（イーサネット、ギガビットイーサネットなど）、ハードウェアポート ID、速度、デュプレックスモード、VLAN ID（サブインターフェイスを定義する場合）を指定します。 結果：すべてのインターフェイスおよびサブインターフェイスが定義されます。 詳細については、ファイアウォールデバイスのインターフェイスの設定を参照してください。

ステップ	タスク
ステップ 2	**基本セキュリティ アプライアンスを管理するための管理コンテキストを定義します。** セキュリティ アプライアンスの管理専用にコンテキストおよび IP アドレスを定義するために、このタスクは個別に呼び出されます。このプロセスは、セキュリティ コンテキストを定義するプロセスと同じです。ただし、プロセスの間は、これを管理コンテキストとして指定するために、必ず [管理コンテキスト（Admin Context）] をオンにしてください。 管理コンテキストは、アプライアンスの管理で使用される以外にも、追加の処理のために syslog および SNMP メッセージをモニタリング デバイス（Cisco Security Monitoring、Analysis and Response System（CS-MARS）など）に公開する場合にも使用されます。 特定の管理 IP アドレスを管理コンテキストに関連付けるまでは、デバイスを定義するときに指定した IP アドレスが、セキュリティ アプライアンスの管理に使用されます。管理 IP アドレスを管理コンテキストに関連付けて指定すると、この IP アドレスが [Device Properties] ページの IP アドレスよりも優先されます。 結果：管理コンテキストが定義され、物理インターフェイスに関連付けられます。 詳細については、以下を参照してください。 • [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）（10 ページ） • [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）（8 ページ）

ステップ	タスク
ステップ 3：	**基本アプライアンスで各セキュリティ コンテキスト（仮想ファイアウォール）を定義します。** このタスクでは、個々のセキュリティ コンテキストを定義します。それぞれに名前を付け、その設定ファイルのロケーションを割り当て、インターフェイスを割り当てます。各セキュリティ コンテキストは、仮想ファイアウォールを表します。また、その定義には、制御下にあるインターフェイスおよび関連付けられた VLAN ID の範囲が含まれます。 （注） 管理コンテキストはファイアウォール デバイスとして使用できますが、通常このように使用されるのは、シングルコンテキスト モードの場合だけです。このため、このチェックリストでは、セキュリティ コンテキストを個別のエンティティとして扱っています。 セキュリティ コンテキストを定義するときに、新しいインターフェイスを追加したり、ハードウェアのポート値を変更したりはできません。すでに定義されているインターフェイスを、コンテキストに割り当てるために選択するだけです。 結果：各セキュリティコンテキストが定義され、物理インターフェイスに関連付けられます。また、セキュリティコンテキストがトラフィックを調査する VLAN も指定されます。 詳細については、以下を参照してください。 • [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）（10 ページ） • [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （8 ページ）

ステップ	タスク
ステップ 4：	**送信/展開を実行して、仮想ファイアウォールを基本アプライアンスの子として生成します。** 各コンテキストの個々の設定の定義を開始するには、セキュリティアプライアンスで必要なコンテキストを作成しておく必要があります。アプライアンスでコンテキストを作成するには、コンテキストを定義してから、Workflow モードでは変更を送信し、Workflow 以外のモードでは変更をセキュリティ アプライアンスに展開します。 セキュリティコンテキストを作成すると、デバイスビューで元のセキュリティアプライアンスの下に「仮想ファイアウォールデバイス」が表示されます。各仮想デバイスは、点線で縁取られた関連するデバイスアイコンで表されます。その名前は、基本セキュリティ アプライアンス名、アンダースコア（_）、コンテキスト名で構成されます。たとえば、仮想デバイス asaMultiRouted_admin は、「asaMultiRouted」という名前のセキュリティアプライアンスの管理コンテキスト（「admin」という名前）を表します。同様に、asaMultiRouted_security1 は、同じ基本アプライアンスのセキュリティコンテキスト「security1」を表します。 結果：変更が（Workflowモードに応じて）送信または展開されます。これにより、管理コンテキストおよびセキュリティコンテキストが基本セキュリティアプライアンスの子として作成されます。 詳細については、以下を参照してください。 • ワークフローおよびアクティビティの概要 • 承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） • 展開および Configuration Archive の使用
ステップ 5	**セキュリティ コンテキストごとに追加の設定を定義します。** デバイスセレクタで仮想ファイアウォールデバイスを選択し、使用可能なポリシー（アクセスルールや変換オプションなど）を編集することにより、各セキュリティコンテキストの定義を完了できます。 結果：各セキュリティコンテキストが完全に定義され、仮想ファイアウォールとして使用できるようになります。

セキュリティ コンテキストの管理

[Security Contexts] ページに、選択したデバイスに設定されているセキュリティ コンテキストが一覧表示されます。このページから、マルチコンテキスト モードで実行されている ASA、PIX 7.0 以降、または FWSM デバイスのセキュリティ コンテキストを追加、編集、および削除できます。

ヒント FWSM デバイスからセキュリティ コンテキストを削除すると、デバイスの実行コンフィギュレーションからセキュリティ コンテキストが削除されますが、関連付けられた設定ファイルは削除されません。このため、すでに削除されたセキュリティ コンテキストと同じ名前で別のセキュリティ コンテキストをあとから追加すると、問題が発生することがあります。これは、FWSM の既知の問題であり、Security Manager の動作とは関連していません。この問題を回避するには、CLI を使用してデバイスから設定ファイルを削除します。

Security Manager を使用してコンテキストを設定するには、セキュリティ アプライアンスがマルチコンテキスト モードになっている必要があります。詳細については、マルチ コンテキスト モードのイネーブル化とディセーブル化 （2 ページ）を参照してください。

セキュリティ コンテキストを管理するには、次の手順を実行します。

ステップ 1 デバイスビューが現在のアプリケーションビューであることを確認します。必要に応じて、ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

デバイス ビューを使用したデバイス ポリシーの設定の詳細については、デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理を参照してください。

ステップ 2 設定するアプライアンスを選択します。

ステップ 3 デバイスポリシーセレクタで [セキュリティコンテキスト（Security Contexts）] を選択して、[セキュリティコンテキスト（Security Contexts）] ページを表示します。

（注） マルチモード デバイスの子コンテキストは、シングル モードのファイアウォール デバイスとは別のアイコンを使用して表されます。

ステップ 4 必要に応じて、コンテキストを追加、編集、および削除します。

- 新しいコンテキストを定義するには、ページの一番下にある [行の追加（Add Row）] ボタンをクリックして、[セキュリティコンテキストの追加（Add Security Context）] ボックスを開きます。
- 既存のコンテキストを編集するには、[セキュリティコンテキスト（Security Contexts）] リストで目的のエントリを選択し、ページの一番下にある [行の編集（Edit Row）] ボタンをクリックして、[セキュリティコンテキストの編集（Edit Security Context）] ダイアログボックスを開きます。
- 既存のコンテキストを削除するには、リストから目的のエントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。

（注） ここでセキュリティ コンテキストを削除すると、セキュリティ コンテキスト デバイスもデバイス インベントリから削除されます。

セキュリティ コンテキストおよび対応するセキュリティ コンテキスト デバイスを削除することを確認します。

（注） タイトルを除き、[Add Security Context] ダイアログボックスと [Edit Security Context] ダイアログボックスは同じです。PIX/ASA デバイスの場合、詳細については[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA） （10 ページ）を参照してください。FWSM の場合、詳細については[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （8 ページ）を参照してください。

[AddSecurityContext]/[EditSecurityContext]ダイアログボックス（FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[Add Security Context]/[Edit Security Context] ダイアログボックスでは、現在選択されているファイアウォール サービス モジュールのコンテキストを定義および管理できます（タイトルを除き、2 つのダイアログボックスは同じです）。

少なくとも 1 つのセキュリティ コンテキストを管理コンテキストとして指定する必要があります。

注意 Security Manager は、FWSM に対してマッピングされた（つまり、「名前付き」または「エイリアス付き」の）インターフェイスをサポートしていません。名前付きインターフェイスを使用する FWSM を検出してから、関連する設定を変更した場合、再展開は失敗します。インターフェイス エイリアスを適切な VLAN ID で置き換えてください。

ナビゲーション パス

セキュリティ コンテキストの管理 （6 ページ）で説明されているように、[Add Security Context]/[Edit Security Context] ダイアログボックスには [Security Contexts] ページからアクセスできます。

フィールド リファレンス

表 1 : [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）

要素	説明
名前	最大 32 文字のコンテキスト名を入力します。System と Null（大文字と小文字の区別なし）は予約済みであるため使用できません。 （注） コンテキスト名は、デバイス上では大文字と小文字が区別されますが、Security Manager では区別されません。つまり、Security Manager では、名前が同じで大文字と小文字が異なる 2 つのコンテキストを設定することはできません。

要素	説明
Mode（FWSM 3.1 以降）	このセキュリティ コンテキストのモード（[Router] または [Transparent]）を選択します。 （注） [Edit Security Context] ダイアログボックスでは、選択されているモードを変更できません。
管理コンテキスト	このコンテキストをこのデバイスの管理コンテキストにする場合、このチェックボックスをオンにします。 （注） デバイスの管理コンテキストの名前は、[Security Contexts] テーブルの下に表示されます。
VLAN IDs	このコンテキストに割り当てる VLAN を入力します。複数の VLAN エントリを区切るには、カンマを使用します。
Config URL	ファイルシステム プロトコルを選択し、アクセスするコンテキスト設定ファイルのパスと名前を入力して、コンテキスト設定の場所を URL タイプのアドレスとして指定します。 つまり、ドロップダウン リストからプロトコル タイプを選択し、サーバ名（リモート ファイル システムの場合）、パス、およびファイル名を関連するテキスト フィールドに入力します。たとえば、FTP の場合、組み合わせた URL は ftp://server.example.com/configs/admin.cfg の形式になります。 使用可能なプロトコルは次のとおりです。 • disk:/ • ftp:// • http:// • https:// • tftp://
フェールオーバー グループ	このコンテキストがアクティブ/アクティブ フェールオーバー設定の一部である場合は、このコンテキストが属するフェールオーバー グループを選択します。
説明	（任意）コンテキストの説明を入力します。

[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[セキュリティコンテキストの追加（Add Security Context）]/[セキュリティコンテキストの編集（Edit Security Context）] ダイアログボックスでは、現在選択されている PIX/ASA セキュリティアプライアンスのコンテキストを定義および管理できます（タイトルを除き、2 つのダイアログボックスは同じです）。

少なくとも 1 つのセキュリティ コンテキストを管理コンテキストとして指定する必要があります。

ナビゲーション パス

セキュリティ コンテキストの管理 （6 ページ）で説明されているように、[Add Security Context]/[Edit Security Context] ダイアログボックスには [Security Contexts] ページからアクセスできます。

フィールド リファレンス

表 *2 : [Add Security Context]/[Edit Security Context]* ダイアログボックス（*PIX/ASA*）

要素	説明
名前	最大 32 文字のコンテキスト名を入力します。System と Null（大文字と小文字の区別なし）は予約済みであるため使用できません。 （注） コンテキスト名は、デバイス上では大文字と小文字が区別されますが、Security Manager では区別されません。つまり、Security Manager では、名前が同じで大文字と小文字が異なる 2 つのコンテキストを設定することはできません。
説明	（任意）コンテキストの説明を入力します。
モード（ASA 9.0+）	このセキュリティ コンテキストのモード（[Router] または [Transparent]）を選択します。 （注） [Edit Security Context] ダイアログボックスでは、選択されているモードを変更できません。

要素	説明
管理コンテキスト	このコンテキストをこのデバイスの管理コンテキストにする場合、このチェックボックスをオンにします。 （注） デバイスの管理コンテキストの名前は、[Security Contexts] テーブルの下に表示されます。 （注） このボックスをオンにすると、[IPv4アドレスプール（IPv4 Address Pool）] フィールドが無効になります。
Config URL	ファイルシステムプロトコルを選択し、アクセスするコンテキスト設定ファイルのパスと名前を入力して、コンテキスト設定の場所を URL タイプのアドレスとして指定します。 つまり、ドロップダウン リストからプロトコル タイプを選択し、サーバ名（リモート ファイル システムの場合）、パス、およびファイル名を関連するテキストフィールドに入力します。たとえば、FTP の場合、組み合わせた URL は ftp://server.example.com/configs/admin.cfg の形式になります。 使用可能なプロトコルは次のとおりです。 • disk0:/ • disk1:/ • flash:/ • ftp:// • http:// • https:// • tftp://
マルチコンテキストモードの VPN：ASA バージョン 9.6(2) デバイス用の Security Manager バージョン 4.12 以降、マルチコンテキストのリモートアクセス VPN はフラッシュの仮想化をサポートします。マルチコンテキスト構造内で、作成されたユーザコンテキストはそれぞれ、使用可能な合計フラッシュに基づき、プライベートなストレージスペースと共有ストレージの場所を設定できます。	

要素	説明
ストレージ URL：プライベート	[プライベート（Private）] チェックボックスをオンにすると、該当ユーザのみに関連付けられ、該当ユーザ対象コンテンツ固有のファイルを保存します。ドロップダウンメニューから、作成したプライベートディレクトリを選択し、設定 URL で指定したものにマップします。マルチコンテキスト ASA 9.6(2) 以降のデバイスのプライベートストレージ URL について、次のいずれかのオプションを選択します。 • disk0:/ • flash:/ ストレージ URL のデフォルト値：プライベートは **disk0:/** です。この値は変更できます。このコンテキストラベル名は、ASA 9.6(2) マルチコンテキストデバイスのファイル展開アクティビティの実行中にディレクトリとして使用されます。
ストレージ URL：共有済み	[共有済み（Shared）] チェックボックスをオンにすると、共有ストレージスペースにファイルをアップロードし、あらゆるユーザコンテキストに読み取り/書き込みアクセスできます。ドロップダウンメニューから。作成した共有ディレクトリを選択し、設定 URL で指定したものにマップします。マルチコンテキスト ASA 9.6(2) 以降のデバイスの共有ストレージ URL には、次のいずれかのオプションを選択します。 • disk0:/ • flash:/ ストレージ URL のデフォルト値：共有は **shared**。この値は変更できます。このコンテキストラベル名は、ASA 9.6(2) マルチコンテキストデバイスのファイル展開アクティビティの実行中にディレクトリとして使用されます。
ScanSafe 設定	このコンテキストで ScanSafe インスペクションを有効にするには、[ScanSafe Webセキュリティを有効にする（Enable ScanSafe Web Security）] を選択します。システム コンフィギュレーションに設定されたライセンスを上書きする場合は、[ライセンス（License）] フィールドにライセンス ID（32 桁の 16 進数でなければならない）を入力します。

要素	説明
インターフェイス	このテーブルには、このコンテキストに割り当てられているインターフェイスとサブインターフェイス、およびそれらに関連付けられた設定が一覧表示されます。これらのインターフェイスおよびサブインターフェイスについて、セキュリティ コンテキストはトラフィックを調査します。 インターフェイスおよびサブインターフェイスをこのコンテキストに追加するには、テーブルの下の [Add Row] ボタンをクリックして [Allocate Interfaces] ダイアログボックス（PIX/ASA だけ） （13 ページ）を開きます。1 つ以上のインターフェイスを割り当てることができます。また任意で、各インターフェイスに 1 つまたは一定範囲のサブインターフェイスを割り当てることができます。 割り当てエントリを編集するには、エントリを選択し、テーブルの下の [Edit Row] ボタンをクリックして、[Edit Interface] ダイアログボックスを開きます。編集できるのは [Alias Name] と [Show hardware properties option] だけですので注意してください。インターフェイス/サブインターフェイスの割り当ては変更できません。これらのオプションの詳細については、 [Allocate Interfaces] ダイアログボックス（PIX/ASA だけ） （13 ページ）を参照してください。 インターフェイス/サブインターフェイスの割り当てを削除するには、このテーブルから該当する行を選択し、テーブルの下の [Delete Row] ボタンをクリックします。
フェールオーバーグループ	このコンテキストがアクティブ/アクティブ フェールオーバー設定の一部である場合は、このコンテキストが属するフェールオーバー グループを選択します。

[Allocate Interfaces] ダイアログボックス（PIX/ASA だけ）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

[Allocate Interfaces] ダイアログボックスでは、インターフェイスをコンテキストに割り当てることができます。また任意で、1 つまたは一定範囲の関連サブインターフェイスをコンテキストに割り当て、名前のエイリアス設定オプションを設定できます。

ナビゲーション パス

[Allocate Interfaces] ダイアログボックスには、[Add Security Context]/[Edit Security Context] ダイアログボックスからアクセスします。詳細については、を参照してください。

関連項目

- セキュリティ コンテキストの管理 （6 ページ）

フィールド リファレンス

表 3 : [Allocate Interfaces] ダイアログボックス

要素	説明
Physical Interface	このコンテキストに割り当てる物理インターフェイスを選択します。 トランスペアレント ファイアウォール モードでは、別のコンテキストに割り当てられていないインターフェイスだけを割り当てることができます。すでに別のコンテキストに割り当てられているインターフェイスを選択した場合は、サブインターフェイスも指定する必要があります。
[Sub Interface ID From]/[Sub Interface ID To]	これらのドロップダウン リストを使用して、1 つまたは一定範囲のサブインターフェイスを指定します。どちらのリストにも、選択した物理インターフェイスに関連付けられているサブインターフェイス ID が表示されます。 1 つのサブインターフェイスを指定するには、最初のリストから目的の ID を選択します。範囲を指定するには、（使用可能な場合）2 番めのリストから最後の ID を選択します（トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます）。
[View Allocation] ボタン	このボタンをクリックすると、[View Interface Allocation] ダイアログボックスが開きます。このダイアログボックスに、このデバイスで定義されているすべての物理インターフェイスと、それぞれに関連付けられているセキュリティ コンテキストおよびフェールオーバー グループが読み取り専用のリストで表示されます。これを使用すると、[Allocate Interfaces] ダイアログボックスを開いたまま、現在の割り当てをすばやく確認できます。
[コンテキストでエイリアス名を使用する（Use aliased name in context）]	このインターフェイスやサブインターフェイスのエイリアス名設定をイネーブルにするには、[セキュリティコンテキストでエイリアス名を使用する（Use aliased names in the security context）] をオンにし、[エイリアス名（Alias Name）] フィールドにエイリアスを入力します。 この物理インターフェイスまたはサブインターフェイスの名前は、このコンテキストに表示されるあらゆる場所（[Interfaces Page] の [Hardware Port] カラムなど）で、この指定したエイリアスに置き換わります。
エイリアス名	目的のエイリアスを入力します。エイリアスは文字で始まり、文字または数字で終わる必要があります。また、内側には文字、数字、およびアンダースコアだけを使用できます。

要素	説明
[Suffix Range From]/[Suffix Range To]	サブインターフェイスの範囲を指定した場合、これらのフィールドが使用可能になって、エイリアス名に数字のサフィックスを指定できます。各サブインターフェイスのエイリアス名は、この範囲からのシーケンス番号に、直前のフィールドで指定した [Alias Name] を追加した名前になります。 これらの値は、デフォルトで最初のサブインターフェイス ID 番号および最後のサブインターフェイス ID 番号に設定されますが、任意の有効な数字範囲を入力できます。
Show hardware properties in context	このオプションを選択すると、エイリアスを定義した場合でも、**show interface** CLI コマンドにより、コンテキストの物理インターフェイスプロパティが表示されます。選択しない場合、show interface の出力にはエイリアス名が含まれます。

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。