



# ファイアウォール デバイスでのサーバアクセスの設定

[Server Access] セクションには、ファイアウォールデバイスでサーバアクセスを設定するためのページが含まれています。[Server Access] は、デバイスセクタまたはポリシーセクタの [Device Admin] の下にあります。

この章は次のトピックで構成されています。

- [AUS] ページ (1 ページ)
- [DHCP Relay] ページ (6 ページ)
- [DHCPリレーIPv6 (DHCP Relay IPv6) ] ページ (10 ページ)
- DHCP サーバーの設定 (14 ページ)
- [DNS] ページ (20 ページ)
- DDNS の設定 (25 ページ)
- [NTP] ページ (29 ページ)
- [SMTP Server] ページ (31 ページ)
- [TFTP Server] ページ (32 ページ)

## [AUS] ページ

[AUS] ページでは、[Auto Update] 指定をサポートするサーバからのセキュリティアプライアンスのリモート更新を設定できます。[Auto Update] によって、設定変更およびソフトウェア更新が、リモートサーバからアプライアンスに自動的に適用されます。



- (注) このページで指定するサーバと、([Tools] メニューから [Device Properties] を選択して表示される) [Device Properties] の [Auto Update] セクションで指定するサーバは、同じである必要があります。[Device Properties] 情報は、Security Manager が設定更新を送信する宛先の AUS サーバを指定します。これに対し、このページの情報は、デバイスが更新のために接続するサーバを定義します。また、[Device Properties] で指定する [Device Identity] と、このページの [Device ID] とが一致している必要もあります。

AUSサーバを変更した場合、デバイスは、新しい設定を受け取るまで現在の設定内に定義されている AUS サーバを引き続き使用することに注意してください。したがって、AUS ポリシーは変更しますが、設定の展開には前の AUS サーバを使用する必要があります。展開が正常に完了したあとで、新しいサーバを指し示すように [Device Properties] を変更します。AUS への展開の詳細については、[Auto Update Server](#) または [CNS Configuration Engine](#) を使用した設定の展開を参照してください。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセクタから [プラットフォーム (Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [AUS] を選択します。
- (ポリシービュー) ポリシータイプセクタから [PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [AUS] を選択します。共有ポリシーセクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

### 関連項目

- [\[Add Auto Update Server\]/\[Edit Auto Update Server\] ダイアログボックス \(5 ページ\)](#)

### フィールドリファレンス

表 1: [AUS] ページ

要素	説明
自動更新サーバーテーブル	<p>このテーブルには、現在設定されている Auto Update Server が一覧表示されます。テーブルの下のボタンを使用して、これらのエントリを管理します。</p> <p>エントリは、AUSサーバに接続するための優先順位の高いものから一覧表示されます。リストの順序を変更するには、上下の矢印ボタンを使用して、選択したエントリを上下に移動します。</p> <p>[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、エントリを追加、編集、または削除します。[Add Row] を選択すると、[Add Auto Update Server] ダイアログボックスが開きます。[Edit Row] を選択すると、選択した行の [Edit Auto Update Server] ダイアログボックスが開きます。これらのダイアログボックスについては、<a href="#">[Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス (5 ページ)</a> を参照してください。</p> <p>(注) この AUS サーバーに接続するための URL は、[自動更新サーバーの追加 (Add Client Update)]/[自動更新サーバーの編集 (Edit Client Update)] ダイアログボックスで指定される <i>Protocol://Username:Password@IP IP Address (:Port)/Path</i> を連結して生成されます。ポートは、デフォルトの 443 以外のポート番号を入力した場合にかぎり含まれます。</p>

要素	説明
デバイス ID タイプ (Device ID Type)	<p>AUS サーバでこのデバイスを識別するために使用する方式を選択します。</p> <ul style="list-style-type: none"><li>• [ホスト名 (Host Name)] : [デバイスプロパティ (Device Properties)] ウィンドウ ([ツール (Tools)] &gt; [デバイスプロパティ (Device Properties)]) で指定されている、このデバイスのホスト名。</li><li>• [シリアル番号 (Serial Number)] : このデバイスのシリアル番号。</li><li>• [IPアドレス (IP Address)] : 指定されたインターフェイスの IP アドレス。このオプションを選択すると、[Interface] フィールドが表示されます。目的のデバイス インターフェイスを入力するか、または選択します。</li><li>• [MACアドレス (MAC Address)] : 指定されたインターフェイスの MAC アドレス。このオプションを選択すると、[Interface] フィールドが表示されます。目的のデバイス インターフェイスを入力するか、または選択します。</li><li>• [定義されたユーザ (User Defined)] : ユーザ指定の一意の ID が使用されます。このオプションを選択すると、[User Defined] フィールドが表示されます。このフィールドに英数字文字列を入力します。この文字列は、[Device Properties] ウィンドウ ([Tools] &gt; [Device Properties]) の [Device Identity] フィールドにも表示されている必要があります。</li></ul>

要素	説明
Poll Type	<p>更新のために AUS サーバをポーリングする頻度を定義する方式を選択します。</p> <ul style="list-style-type: none"> <li>• [指定した頻度で (At Specified Frequency)] : このオプションを選択すると、[ポーリング期間 (Poll Period)] フィールドが表示されます。 <ul style="list-style-type: none"> <li>• [ポーリング期間 (Poll Period)] : デバイスが AUS サーバのポーリングと次のポーリングの間待機する時間を分で指定します。有効な値は 1 ~ 35791 です。</li> </ul> </li> <li>• [スケジュールした時間に (At Scheduled Time)] : このオプションを選択すると、次のフィールドが表示されます (バージョン 7.2 以降を実行している ASA/PIX デバイスにかぎり使用可能)。 <ul style="list-style-type: none"> <li>• [曜日 (Days of the week)] : デバイスが AUS サーバをポーリングする 1 日以上の日を選択します。</li> <li>• [ポーリング開始時間 (Polling Start Time in Hours)] : 選択した日にポーリングを開始する時間 (24 時間形式に基づく)。</li> <li>• [ポーリング開始時間 (分) (Polling Start Time in Mins)] : ポーリングを開始する時間の分の値。</li> <li>• [開始時間のランダム化を有効にする (Enable Randomization of the Start Time)] : ランダムなポーリング時間枠を指定する場合は、このオプションを選択します。[時間枠のランダム化 (Randomization Window)] フィールドが有効になります。</li> </ul> </li> </ul> <p>[時間枠のランダム化 (Randomization Window)] : デバイスが指定のポーリング時間をランダム化するために使用できる最大分数。有効な値は 1 ~ 1439 です。</p>
再試行回数 (Retry Count)	<p>デバイスが新しい情報のために AUS サーバへのポーリングを試行する回数。任意。このフィールドに 0 を入力した場合、またはこのフィールドを空白のままにした場合、デバイスはポーリング試行の失敗後に再試行しません。</p>
Retry Period	<p>[Retry Count] が 0 でも空白でもない場合に、デバイスがポーリング試行の失敗後に AUS サーバへの再ポーリングを待機する時間 (分)。有効な値は 1 ~ 35791 です。[Retry Count] が 0 でも空白でもないのに、このフィールドを空白のままにした場合、値はデフォルトで 5 分に設定されます。</p>
Disable Device After:	<p>このオプションを選択すると、指定されたタイムアウト期間中に AUS サーバからの応答がない場合、セキュリティ アプライアンスによって通過中のトラフィックが停止されます。</p> <ul style="list-style-type: none"> <li>• [タイムアウト (Timeout)] : AUS サーバからの応答がない場合にファイアウォールデバイスがタイムアウトを待機する時間 (分)。</li> </ul>

## [Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス

[Add Auto Update Server] ダイアログボックスを使用して、新しい AUS サーバ定義を設定します。セキュリティアプライアンスは、このサーバを自動的にポーリングして、イメージおよび設定の更新がないかどうかを確認します。

[Auto Update] 指定では、Auto Update Server が設定情報をプッシュしてセキュリティアプライアンスに情報の要求を送信するか、または Auto Update Server に対する定期的なポーリングをセキュリティアプライアンスで行うように設定することによって設定情報をプルするかを選択できます。また、Auto Update Server は、セキュリティアプライアンスにコマンドを送信して、いつでも即時ポーリング要求を送信できます。Auto Update Server とセキュリティアプライアンスが互いに通信を行うには、各セキュリティアプライアンス上に通信パスとローカル CLI 設定が必要です。



- (注) この AUS サーバに接続するための URL は、これらのダイアログボックスで指定されている Protocol://Username:Password@IP IP Address(:Port)/Path を連結して生成します。ポートは、デフォルトの 443 以外のポート番号を入力した場合にかぎり含まれます。

[Edit Auto Update Server] ダイアログボックスと [Add Auto Update Server] ダイアログボックスは、タイトルを除けば同じです。次の説明は両方に適用されます。

### ナビゲーションパス

[Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックスには、[\[AUS\] ページ \(1 ページ\)](#) からアクセスできます。

### フィールドリファレンス

表 2: [Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス

要素	説明
プロトコル	AUS サーバとの通信に使用されるプロトコル。[http] または [https] を選択します。  (注) Auto Update Server と通信するためのプロトコルとして [https] を選択した場合、セキュリティアプライアンスでは SSL が使用されます。この場合、セキュリティアプライアンスには DES、3DES、AES ライセンスが必要です。
IP アドレス	IP アドレスを入力するか、またはこの AUS サーバを表すネットワーク/ホスト オブジェクトを選択します。

要素	説明
[ポート (Port)]	AUS サーバとの通信が行われるポートの番号を入力します。[Protocol] に [http] を選択した場合は、デフォルトで 80 に設定されます。[https] を選択した場合は、443 に設定されます。任意のポート番号を入力した場合、AUS サーバが同じポートを使用するように設定されていることを確認してください。
パス (Path)	サーバ上の AUS サービスへのパス。標準のパスは autoupdate/AutoUpdateServlet です。AUS サーバが ASA の場合にのみ、admin/auto-update に変更します。
AUS Interface	Auto Update Server のポーリングに使用するインターフェイスを入力または選択します。
Verify Certificate	このオプションを選択すると、AUS サーバからの SSL 検証が必要になります。サーバから返された証明書は、Certification Authority (CA; 証明局) ルート証明書に基づいてチェックされます。これには、AUS サーバとこのデバイスが同じ認証局を使用している必要があります。
ユーザー名	AUS 認証に使用するユーザ名を入力します (任意)。
パスワード	AUS 認証に使用するパスワードを入力します (任意)。
確認 (Confirm)	パスワードを再入力します (任意)。

## [DHCP Relay] ページ

[DHCP Relay] ページを使用して、セキュリティ デバイスの DHCP リレー サービスを設定します。Dynamic Host Configuration Protocol (DHCP) リレーでは、あるインターフェイス上で受信された DHCP 要求が、別のインターフェイスの背後にある外部 DHCP サーバに渡されます。DHCP リレーを設定するには、少なくとも 1 つの DHCP リレー サーバを指定してから、DHCP 要求を受信するインターフェイスで DHCP リレー エージェントをイネーブルにする必要があります。



- (注) DHCP リレー サーバが設定されているインターフェイスでは、DHCP リレー エージェントをイネーブルにできません。DHCP リレー エージェントは外部 DHCP サーバでだけ動作します。DHCP 要求は、DHCP サーバとして設定されているセキュリティ アプライアンス インターフェイスには転送されません。

Security Manager バージョン 4.9 以降、DHCP リレー IPv4 は、ソフトウェアバージョン 9.4.0 以降を実行している ASA クラスタデバイスでサポートされています。

ASA-SM 9.1.2+ では、DHCP リレー サーバをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサー

バーに対してのみリレーされます。インターフェイス固有のサーバーが設定されていないインターフェイスにDHCP要求が届くと、ASAはその要求をすべてのグローバルサーバーにリレーします。インターフェイスにインターフェイス固有のサーバーが設定されている場合、グローバルサーバーは使用されません。インターフェイス単位のDHCPリレーでは、IPv6はサポートされません。詳細については、[\[Add Interface\]/\[Edit Interface\] ダイアログボックス - \[Advanced\] タブ \(ASA/PIX 7.0 以降\)](#) を参照してください。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセクタから [プラットフォーム (Platform) ] > [デバイス管理 (Device Admin) ] > [サーバーアクセス (Server Access) ] > [DHCPリレー (DHCP Relay) ] を選択します。
- (ポリシービュー) ポリシータイプセクタから [PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform) ] > [デバイス管理 (Device Admin) ] > [サーバーアクセス (Server Access) ] > [DHCPリレー (DHCP Relay) ] を選択します。共有ポリシーセクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

### フィールドリファレンス

表 3: [DHCP Relay] ページ

要素	説明
[DHCP Relay Agent] テーブル	このテーブルには、DHCPリレーが設定されているインターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および[Delete Row] ボタンを使用して、これらのエントリを管理します。  [Add Row] ボタンでは [Add DHCP Relay Agent Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Relay Agent Configuration] ダイアログボックスが開きます。詳細については、 <a href="#">[Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス (8 ページ)</a> を参照してください。
[DHCP Servers] テーブル	このテーブルには、DHCP要求がリレーされるグローバルDHCPサーバーが一覧表示されています。[Add Row]、[Edit Row]、および[Delete Row] ボタンを使用して、これらのエントリを管理します。  [Add Row] ボタンでは [Add DHCP Relay Server Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Relay Server Configuration] ダイアログボックスが開きます。詳細については、 <a href="#">[Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックス (9 ページ)</a> を参照してください。
タイムアウト (秒)	DHCPアドレスネゴシエーションに許可される時間を秒単位で指定します。有効値の範囲は1 ~ 3600秒で、デフォルト値は60秒です。

要素	説明
信頼情報 (Option 82)	<p>信頼するすべての DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。</p> <p>(注) 信頼するインターフェイスを個別に指定することもできます。詳細については、<a href="#">[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ (ASA/PIX 7.0 以降)</a> を参照してください。</p> <p>DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレーエージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド (サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド) が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。</p>

## [Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス

[Add DHCP Relay Agent Configuration] ダイアログボックスを使用して、インターフェイスで DHCP リレーエージェントを設定してイネーブルにします。[Edit DHCP Relay Agent Configuration] ダイアログボックスを使用して、既存のインターフェイスリレーエージェントを更新します。



- (注) DHCP リレー サーバが設定されているインターフェイスでは、DHCP リレー エージェントをイネーブルにできません。DHCP リレー エージェントは外部 DHCP サーバでだけ動作します。DHCP 要求は、DHCP サーバとして設定されているセキュリティアプライアンスインターフェイスには転送されません。

[Add DHCP Relay Agent Configuration] ダイアログボックスと [Edit DHCP Relay Agent Configuration] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

### ナビゲーションパス

[Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックスには、[\[DHCP Relay\] ページ \(6 ページ\)](#) からアクセスできます。



## 関連項目

- [\[Add DHCP Relay Server Configuration\]/\[Edit DHCP Relay Server Configuration\] ダイアログボックス \(9 ページ\)](#)

## フィールドリファレンス

表 4: [Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス

要素	説明
インターフェイス (Interface)	DHCP リレー エージェントを設定するインターフェイスの名前を入力または選択します。
Enable DHCP Relay	このチェックボックスをオンにすると、指定したインターフェイスで DHCP リレーがイネーブルになります。
Set Route	このチェックボックスをオンにして、DHCP サーバから返された情報内のデフォルト ルータ アドレスが変更されるように DHCP リレー エージェントを設定します。このオプションを選択した場合、DHCP リレー エージェントは、DHCP サーバから返された情報内のデフォルト ルータ アドレスを、選択されたインターフェイスで置き換えます。

## [Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックス

新しい DHCP リレー サーバを定義する場合は、[Add DHCP Relay Server Configuration] ダイアログボックスを使用します。既存のサーバ情報を更新する場合は、[Edit DHCP Relay Server Configuration] ダイアログボックスを使用します。シングルモードおよびコンテキストごとに、グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとには、4 台まで設定できます。



- (注) 7.2 より前の OS を実行している PIX ファイアウォールは、4 つの DHCP リレー サーバーのみをサポートします。

[Add DHCP Relay Server Configuration] ダイアログボックスと [Edit DHCP Relay Server Configuration] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

## ナビゲーションパス

[Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックスには、[\[DHCP Relay\] ページ \(6 ページ\)](#) からアクセスできます。

## 関連項目

- [\[Add DHCP Relay Agent Configuration\]/\[Edit DHCP Relay Agent Configuration\]](#) ダイアログボックス (8 ページ)

## フィールド リファレンス

表 5: [\[Add DHCP Relay Server Configuration\]/\[Edit DHCP Relay Server Configuration\]](#) ダイアログボックス

要素	説明
サーバー	IP アドレスを入力するか、または DHCP 要求の転送先の外部 DHCP サーバを表すネットワーク/ホスト オブジェクトを選択します。
インターフェイス	DHCP 要求の外部 DHCP サーバへの転送に使用されるインターフェイスを入力または選択します。

## [DHCPリレーIPv6 (DHCP Relay IPv6)] ページ

[DHCPリレーIPv6 (DHCP Relay IPv6)] ページを使用して、セキュリティデバイスの DHCP リレーサービスを設定します。Dynamic Host Configuration Protocol v6 (DHCPv6) リレーは、あるインターフェイスで受信した DHCPv6 要求を、別のインターフェイスの背後にある外部 DHCPv6 サーバーに渡します。DHCPv6 リレーを構成するには、少なくとも 1 つの DHCPv6 リレーサーバーを指定してから、DHCPv6 要求を受信するインターフェイスで DHCPv6 リレーエージェントをイネーブルにする必要があります。



- (注) DHCPv6 リレーサーバーが構成されているインターフェイスでは、DHCPv6 リレーエージェントは有効にできません。DHCPv6 リレーエージェントは、外部 DHCPv6 サーバーでのみ機能しますが、DHCPv6 サーバーとして設定されたセキュリティ アプライアンス インターフェイスには DHCPv6 要求を転送しません。Security Manager バージョン 4.9 以降、DHCP リレー IPv6 は、ソフトウェアバージョン 9.4.0 以降を実行している ASA クラスタデバイスでサポートされています。

## ナビゲーションパス

- (デバイスビュー) デバイスポリシーセクタから [\[プラットフォーム \(Platform\)\]](#) > [\[デバイス管理 \(Device Admin\)\]](#) > [\[サーバーアクセス \(Server Access\)\]](#) > [\[DHCPリレーIPv6 \(DHCP Relay IPv6\)\]](#) を選択します。
- (ポリシービュー) ポリシータイプセクタから [\[PIX/ASA/FWSMプラットフォーム \(PIX/ASA/FWSM Platform\)\]](#) > [\[デバイス管理 \(Device Admin\)\]](#) > [\[サーバーアクセス \(Server Access\)\]](#) > [\[DHCPリレーIPv6 \(DHCP Relay IPv6\)\]](#) を選択します。共有ポリシーセクタから既存のポリシーを選択するか、または新しいポリシーを作成します。



- (注) DHCPv6には、「managed-config-flag」と「other-config-flag」という2つの新しいインターフェイス設定が導入されました。詳細については、[IPv6 インターフェイスの設定 \(ASA/FWSM\)](#)を参照してください。

### フィールドリファレンス

表 6 : [DHCPリレーIPv6 (DHCP Relay IPv6) ]ページ

要素	説明
[DHCPリレーIPv6 エージェント (DHCP Relay IPv6 Agent) ]テーブル	<p>このテーブルには、DHCP リレー IPv6 が設定されているインターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。</p> <p>[行の追加 (Add Row) ] ボタンでは [DHCPリレーIPv6エージェント構成の追加 (Add DHCP Relay Agent Configuration) ] ダイアログボックスが開き、[行の編集 (Edit Row) ] では [DHCPリレーIPv6エージェント構成の編集 (Edit DHCP Relay Agent Configuration) ] ダイアログボックスが開きます。詳細については、<a href="#">[DHCPリレーIPv6エージェント構成の追加 (Add DHCP Relay IPv6 Agent Configuration) ]/[DHCPリレーIPv6エージェント構成の編集 (Edit DHCP Relay IPv6 Agent Configuration) ] ダイアログボックス (12 ページ)</a> を参照してください。</p>
[DHCP Servers] テーブル	<p>このテーブルには、DHCP リレー IPv6 が設定されているインターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。</p> <p>[行の追加 (Add Row) ] ボタンでは [DHCPリレーIPv6サーバー設定の追加 (Add DHCP Relay Agent Configuration) ] ダイアログボックスが開き、[行の編集 (Edit Row) ] では [DHCPリレーIPv6サーバー設定の編集 (Edit DHCP Relay Agent Configuration) ] ダイアログボックスが開きます。詳細については、<a href="#">[DHCPリレーIPv6サーバー設定の追加 (Add DHCP Relay IPv6 Server Configuration) ]/[DHCPリレーIPv6サーバー設定の編集 (Edit DHCP Relay IPv6 Server Configuration) ] ダイアログボックス (13 ページ)</a> を参照してください。</p>
タイムアウト (秒)	DHCPv6 アドレスネゴシエーションに許可される時間を秒単位で指定します。有効値の範囲は 1 ~ 3600 秒で、デフォルト値は 60 秒です。

## [DHCPリレーIPv6エージェント構成の追加 (Add DHCP Relay IPv6 Agent Configuration)]/[DHCPリレーIPv6エージェント構成の編集 (Edit DHCP Relay IPv6 Agent Configuration)] ダイアログボックス

[DHCPリレーIPv6エージェント構成の追加 (Add DHCP Relay IPv6 Agent Configuration)] ダイアログボックスを使用して、インターフェイスでDHCPv6リレーエージェントを設定して有効にします。[DHCPリレーIPv6エージェント構成の編集 (Edit DHCP Relay IPv6 Agent Configuration)] ダイアログボックスを使用して、既存のインターフェイスリレーエージェントを更新します。



- (注) DHCPv6リレーサーバーが構成されているインターフェイスでは、DHCPv6リレーエージェントは有効にできません。DHCPv6リレーエージェントは、外部DHCPv6サーバーでのみ機能しますが、DHCPv6サーバーとして設定されたセキュリティアプライアンスインターフェイスにはDHCPv6要求を転送しません。

[DHCPリレーIPv6エージェント構成の追加 (Add DHCP Relay IPv6 Agent Configuration)] ダイアログボックスと [DHCPリレーIPv6エージェント構成の編集 (Edit DHCP Relay IPv6 Agent Configuration)] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

### ナビゲーションパス

[DHCPリレーIPv6エージェント構成の追加 (Add DHCP Relay IPv6 Agent Configuration)]/[DHCPリレーIPv6エージェント構成の編集 (Edit DHCP Relay IPv6 Agent Configuration)] ダイアログボックスには、[\[DHCPリレーIPv6 \(DHCP Relay IPv6\)\] ページ \(10 ページ\)](#) からアクセスできます。

### 関連項目

- [\[DHCPリレーIPv6サーバー設定の追加 \(Add DHCP Relay IPv6 Server Configuration\)\]/\[DHCPリレーIPv6サーバー設定の編集 \(Edit DHCP Relay IPv6 Server Configuration\)\] ダイアログボックス \(13 ページ\)](#)

### フィールドリファレンス

表 7: [DHCPリレーIPv6エージェント構成の追加 (Add DHCP Relay IPv6 Agent Configuration)]/[DHCPリレーIPv6エージェント構成の編集 (Edit DHCP Relay IPv6 Agent Configuration)] ダイアログボックス

要素	説明
インターフェイス (Interface)	DHCPv6リレーエージェントを設定するインターフェイスの名前を入力または選択します。
DHCPv6リレーの有効化 (Enable DHCPv6 Relay)	オンにすると、指定したインターフェイスでDHCPv6リレーが有効になります。

要素	説明
Set Route	このチェックボックスをオンにして、DHCPv6 サーバーから返された情報内のデフォルトルータアドレスが変更されるように DHCPv6 リレーエージェントを設定します。このオプションを選択した場合、DHCPv6 リレーエージェントは、DHCPv6 サーバーから返された情報内のデフォルトルータアドレスを、選択されたインターフェイスのアドレスで置き換えます。

## [DHCPリレーIPv6サーバー設定の追加 (Add DHCP Relay IPv6 Server Configuration)]/[DHCPリレーIPv6サーバー設定の編集 (Edit DHCP Relay IPv6 Server Configuration)] ダイアログボックス

新しい DHCP リレーサーバーを定義する場合は、[DHCPリレーIPv6サーバー設定の追加 (Add DHCP Relay IPv6 Server Configuration)] ダイアログボックスを使用します。既存のサーバー情報を更新する場合は、[DHCPリレーIPv6サーバー設定の編集 (Edit DHCP Relay IPv6 Server Configuration)] ダイアログボックスを使用します。最大 10 台の DHCPv6 リレーサーバーを定義できます。



- (注) [DHCPリレーIPv6サーバー設定の追加 (Add DHCP Relay IPv6 Server Configuration)] ダイアログボックスと [DHCPリレーIPv6サーバー設定の編集 (Edit DHCP Relay IPv6 Server Configuration)] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

### ナビゲーションパス

[DHCPリレーIPv6サーバー設定の追加 (Add DHCP Relay IPv6 Server Configuration)]/[DHCPリレーIPv6サーバー設定の編集 (Edit DHCP Relay IPv6 Server Configuration)] ダイアログボックスには、[\[DHCPリレーIPv6 \(DHCP Relay IPv6\)\] ページ \(10 ページ\)](#) からアクセスできます。

### 関連項目

- [\[DHCPリレーIPv6エージェント構成の追加 \(Add DHCP Relay IPv6 Agent Configuration\)\]/\[DHCPリレーIPv6エージェント構成の編集 \(Edit DHCP Relay IPv6 Agent Configuration\)\] ダイアログボックス \(12 ページ\)](#)

## フィールドリファレンス

表 8: [DHCPリレーIPv6サーバー設定の追加 (Add DHCP Relay IPv6 Server Configuration)]/[DHCPリレーIPv6サーバー設定の編集 (Edit DHCP Relay IPv6 Server Configuration)]

要素	説明
サーバー	IP アドレスを入力するか、または DHCPv6 要求の転送先の外部 DHCPv6 サーバーを表すネットワーク/ホストオブジェクトを選択します。
インターフェイス	DHCPv6 要求が外部 DHCPv6 サーバーに転送されるインターフェイスを入力または選択します。

## DHCP サーバーの設定

Dynamic Host Configuration Protocol (DHCP) サーバは、IP アドレスなどのネットワーク設定パラメータを DHCP クライアントに提供します。セキュリティアプライアンスは、セキュリティアプライアンスのインターフェイスに接続された DHCP クライアントに、DHCP サーバまたは DHCP リレーサービスを提供できます。DHCP サーバは、ネットワーク設定パラメータを DHCP クライアントに直接提供します。一方、DHCP リレーでは、あるインターフェイスで受信された DHCP 要求が、別のインターフェイスの背後にある外部 DHCP サーバに渡されます。DHCP リレーの詳細については、[\[DHCP Relay\] ページ \(6 ページ\)](#) を参照してください。



- (注) セキュリティアプライアンスの DHCP サーバは BOOTP 要求をサポートしません。マルチコンテキストモードの場合、複数のコンテキストが使用するインターフェイス上で DHCP サーバまたは DHCP リレーをイネーブルにすることはできません。

セキュリティアプライアンスの各インターフェイスで、DHCP サーバを設定できます。各インターフェイスは、アドレスの導出元としてそれぞれのアドレスプールを持つことができます。ただし、その他の DHCP 設定 (DNS サーバ、ドメイン名、オプション、ping タイムアウト、WINS サーバなど) は、グローバルに設定され、すべてのインターフェイスの DHCP サーバによって使用されます。

DHCP サーバがイネーブルになっているインターフェイスで、DHCP クライアントまたは DHCP リレーサービスを設定することはできません。また、DHCP クライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。

外部インターフェイスでファイアウォールも DHCP クライアントとして動作している場合は、IP 設定のオートネゴシエーションをイネーブルにできます。これにより、ファイアウォールは、(DHCP クライアントとして) 外部インターフェイスから取得した DNS、WINS、およびドメイン名のパラメータを、内部ネットワークのホストに渡すことができます。あるいは、DNS、WINS、およびドメイン名のパラメータを手動で指定することもできます。これらのパラメータを手動で指定したが、自動設定も有効になっている場合、自動設定よりも手動で指定した値が優先されます。

DHCP サーバ定義を管理するには、[\[DHCP Server\] ページ \(15 ページ\)](#) を使用します。

## [DHCP Server] ページ

[DHCP Server] ページを使用して、グローバル DHCP サーバおよび Dynamic DNS (DDNS) での更新オプションの設定、1つ以上のデバイスインターフェイスでの DHCP サーバの設定、および拡張サーバ オプションの設定を行います。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセレクトタから **[プラットフォーム (Platform)]** > **[デバイス管理 (Device Admin)]** > **[サーバアクセス (Server Access)]** > **[DHCPサーバ (DHCP Server)]** を選択します。
- (ポリシービュー) ポリシータイプセレクトタから **[PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)]** > **[デバイス管理 (Device Admin)]** > **[サーバアクセス (Server Access)]** > **[DHCPサーバ (DHCP Server)]** を選択します。共有ポリシーセレクトタから既存のポリシーを選択するか、または新しいポリシーを作成します。

### 関連項目

- [DHCP サーバの設定 \(14 ページ\)](#)

### フィールドリファレンス

表 9: [DHCP Server] ページ

要素	説明
Ping Timeout	ファイアウォールデバイスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で入力します。アドレス競合を回避するために、ファイアウォールデバイスは2つの ICMP ping パケットをアドレスに送信してから、そのアドレスを DHCP クライアントに割り当てます。有効値の範囲は 10 ~ 10000 ミリ秒です。
Lease Length	リースが期限切れになる前に、クライアントが割り当てられた IP アドレスを使用できる時間を秒単位で指定します。有効な値の範囲は、300 ~ 1048575 秒です。デフォルト値は 3600 秒 (1 時間) です。

要素	説明
自動設定有効 (Enable auto-configuration) (PIX および ASA 限定)	このオプションを選択すると、DHCP 自動設定がイネーブルになります。  DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動設定によって取得された情報のいずれかが手動でも指定されている場合は、手動で指定された情報の方が、検出された情報よりも優先されます。
インターフェイス	[Enable auto-configuration] チェックボックスがオンになっている場合、このフィールドが使用可能になります。DNS、WINS、およびドメイン名のパラメータを提供する DHCP クライアントを実行しているインターフェイスを入力または選択します。
[設定の定義 (Define settings) ] (任意)	
ドメイン名	DHCP クライアントの DNS ドメイン名を指定します。有効な DNS ドメイン名 (example.com など) を入力します。
プライマリ DNS サーバ (Primary DNS Server)	IP アドレスを入力するか、または DHCP クライアントのプライマリ DNS サーバを表すネットワーク/ホスト オブジェクトを選択します。
プライマリ WINS サーバ (Primary WINS Server)	IP アドレスを入力するか、または DHCP クライアントのプライマリ WINS サーバを表すネットワーク/ホスト オブジェクトを選択します。
セカンダリ DNS サーバ (Secondary DNS Server)	IP アドレスを入力するか、または DHCP クライアントの代替 DNS サーバを表すネットワーク/ホスト オブジェクトを選択します。
セカンダリ WINS サーバ (Secondary WINS Server)	IP アドレスを入力するか、または DHCP クライアントの代替 WINS サーバを表すネットワーク/ホスト オブジェクトを選択します。
Dynamic DNS Update	



要素	説明
ダイナミック DNS 更新有効 (Enable Dynamic DNS Update)	<p>グローバルな DDNS 更新オプションを定義する場合は、このチェックボックスをオンにします。</p> <ul style="list-style-type: none"> <li>リソースレコード更新のタイプとして、[PTRレコードのみ (PTR Record only)] または [A および PTRレコード (A Record and PTR Record)] を選択します。</li> <li>[Override DHCP Client Request] も選択できます。選択した場合、DHCP クライアントによって要求されたすべての更新が、DHCP サーバ更新によって上書きされます。</li> </ul> <p>これらのオプションは、ASA/PIX 7.2 以降でのみ使用可能です。</p>
[DHCP Server Interface Configuration] テーブル	
Interface table	<p>このテーブルには、DHCP サーバ、DDNS 更新、またはその両方が設定されているデバイス インターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。</p> <p>[Add Row] ボタンでは [Add DHCP Server Interface Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Server Interface Configuration] ダイアログボックスが開きます。詳細については、<a href="#">[Add DHCP Server Interface Configuration]/[Edit DHCP Server Interface Configuration] ダイアログボックス (17 ページ)</a> を参照してください。</p>
詳細オプション	
[Advanced] ボタン	<a href="#">[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス (18 ページ)</a> が開きます。

## [Add DHCP Server Interface Configuration]/[Edit DHCP Server Interface Configuration] ダイアログボックス

これらのダイアログボックスを使用すると、DHCP をイネーブルにして、指定したインターフェイスに DHCP アドレスプールを指定したり、インターフェイスで Dynamic DNS (DDNS) 更新をイネーブルにしたりすることができます。



(注) タイトルを除き、この 2 つのダイアログボックスは同じです。

## ナビゲーションパス

[DHCPサーバーインターフェイス設定の追加 (Add DHCP Server Interface Configuration) ]/[DHCPサーバーインターフェイス設定の編集 (Edit DHCP Server Interface Configuration) ] ダイアログボックスには、[\[DHCP Server\] ページ \(15 ページ\)](#) からアクセスできます。

## 関連項目

- [DHCP サーバーの設定 \(14 ページ\)](#)

## フィールドリファレンス

表 10: [Add DHCP Server Interface Configuration]/[Edit DHCP Server Interface Configuration] ダイアログボックス

要素	説明
インターフェイス (Interface)	DHCPサーバを設定するインターフェイスを識別します。インターフェイス名を入力するか、またはインターフェイスオブジェクトを選択します。
DHCP Address Pool	DHCP サーバが IP アドレスの割り当て時に使用する IP アドレスまたは (ハイフンで区切った) アドレス範囲を入力します。範囲の開始アドレスと終了アドレスは同じサブネット内にある必要があり、開始アドレスを終了アドレスより大きくすることはできません。
Enable DHCP Server	このインターフェイスでDHCPサーバーをイネーブルにするには、このチェックボックスをオンにします。
ダイナミック DNS 更新有効 (Enable Dynamic DNS Update)	この DHCP サーバによる DDNS 更新をイネーブルにするには、このチェックボックスをオンにします。更新するレコードを指定します。 <ul style="list-style-type: none"> <li>• PTR レコードのみ (PTR Record only)</li> <li>• <b>A Record and PTR Record</b></li> </ul> <p>[DHCPクライアントリクエストのオーバーライド (Override DHCP Client Request) ]も選択できます。選択した場合、DHCP クライアントによって要求されたすべての更新が、DHCPサーバ更新によって上書きされます。</p>

## [Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス

[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックスでは、DHCPサーバに設定されているDHCPオプションを管理できます。DHCPオプションで、DHCPクライアントに追加情報を提供します。たとえば、DHCPオプション 150 お

よび DHCP オプション 66 は、Cisco IP Phone および Cisco IOS ルータに TFTP サーバ情報を提供します。

### ナビゲーションパス

[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックスにアクセスするには、[\[DHCP Server\] ページ \(15 ページ\)](#) で [Advanced] ボタンをクリックします。

### 関連項目

- [DHCP サーバーの設定 \(14 ページ\)](#)

### フィールドリファレンス

表 11: [Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス

要素	説明
[Options] テーブル	<p>このテーブルには、設定されている DHCP サーバ オプションが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。</p> <p>[Add Row] ボタンでは [Add DHCP Server Interface Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Server Interface Configuration] ダイアログボックスが開きます。詳細については、<a href="#">[Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックス (19 ページ)</a> を参照してください。</p>

### [Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックス

[Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックスでは、DHCP クライアントに追加情報を提供する DHCP サーバ オプション パラメータを設定できます。たとえば、DHCP オプション 150 および DHCP オプション 66 は、Cisco IP Phone および Cisco IOS ルータに TFTP サーバ情報を提供します。

### ナビゲーションパス

[Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックスには、[\[Add DHCP Server Advanced Configuration\]/\[Edit DHCP Server Advanced Configuration\] ダイアログボックス \(18 ページ\)](#) からアクセスできます。

### 関連項目

- [DHCP サーバーの設定 \(14 ページ\)](#)
- [\[DHCP Server\] ページ \(15 ページ\)](#)

## フィールド リファレンス

表 12: [Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックス

要素	説明
オプションコード	<p>使用可能なオプションコードのリストから、オプションを選択します。オプション 1、12、50～54、58～59、61、67、82 を除き、すべての DHCP オプション（オプション 1～255）がサポートされています。</p> <p>DHCP オプションコードの詳細情報については、<a href="http://cisco.com">cisco.com</a> の『<a href="#">DHCP Options Reference</a>』を参照してください。</p>
タイプ (Type)	<p>オプションが DHCP クライアントに返す情報のタイプを選択します。</p> <ul style="list-style-type: none"> <li>• <b>IP</b> : このタイプを選択すると、1 つまたは 2 つの IP アドレスが DHCP クライアントに返されるように指定されます。最大 2 つの IP アドレスを指定します。</li> <li>• <b>ASCII</b> : このタイプを選択すると、ASCII 値が DHCP クライアントに返されるように指定されます。ASCII 文字列を指定します。スペースを含めることはできません。</li> <li>• <b>HEX</b> : このタイプを選択すると、16 進数値が DHCP クライアントに返されるように指定されます。桁数が偶数の HEX 文字列を、スペースを含めずに指定します。0x プレフィックスを使用する必要はありません。</li> </ul>

## [DNS] ページ

DNS ページを使用して、DNS サーバグループを設定します。ファイアウォールデバイスは、これらの DNS サーバを使用して、完全修飾ドメイン名（ホスト名）を、ID 認証ファイアウォールポリシーで使用する SSL VPN、証明書、および FQDN ネットワーク/ホストオブジェクトの IP アドレスに解決します。サーバ名を定義するその他の機能（AAA など）は DNS 解決をサポートしていません。IP アドレスを入力するか、IP アドレスへの名前を手動で解決する必要があります。



**ヒント** DefaultDNS サーバグループは ASA で事前定義されており、FQDN ネットワーク/ホストオブジェクトの解決に使用されます。FQDN オブジェクトを使用する場合は、このグループの DNS サーバを設定していることを確認してください。そうでない場合、名前を解決できません。セキュリティを強化するため、できればネットワーク内にある、信頼できる DNS サーバを指定してください。詳細については、[ID 認証ファイアウォールポリシーの要件](#)を参照してください。

## ナビゲーションパス

- (デバイスビュー) デバイスポリシーセクタから [プラットフォーム (Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [DNS] を選択します。
- (ポリシービュー) ポリシータイプセクタから [PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [DNS] を選択します。共有ポリシー セクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

## 関連項目

- [\[Add DNS Server\] ダイアログボックス \(24 ページ\)](#)

## フィールドリファレンス

表 13: [DNS] ページ

要素	説明
[DNS Server Groups] テーブル	このテーブルには、現在定義されている DNS サーバークラスタが一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのグループ エントリを管理します。  [Add Row] ボタンでは [Add DNS Server Group] ダイアログボックスが開き、[Edit Row] ボタンでは [Edit DNS Server Group] ダイアログボックスが開きます。タイトルを除き、これらのダイアログボックスは同じです。詳細については、 <a href="#">[Add DNS Server Group] ダイアログボックス (22 ページ)</a> を参照してください。
DNS グループ マップ	[ドメインへのDNSの有効化 (Enable DNS To Domain)] : このオプションをオンにすると、DNS サーバークラスタ名から DNS グループマップドメイン名へのマッピングが有効になります。このオプションがオフの場合、DNS グループマップテーブルは空になります。  DNS グループマップテーブルには、現在定義されている DNS グループマップが一覧表示されます。テーブルの下の [行の追加 (Add Row)]、[行の編集 (Edit Row)]、および [行の削除 (Delete Row)] ボタンを使用して、これらのグループ エントリを管理します。詳細については、「 <a href="#">[DNSサーバークラスタの追加 (Add DNS Server Group)] ダイアログボックス</a> 」を参照してください。
DNS Lookup Interfaces	DNS ルックアップをイネーブルにするインターフェイスが一覧表示されます。1 つ以上のインターフェイスまたはインターフェイス ロールを入力または選択します。

要素	説明
Enable DNS Guard (ASA/PIX 7.0(5)、7.2(x)、および 8.x のみ)	<p>このチェックボックスをオンにすると、選択したデバイスまたは共有ポリシーで DNS Guard がイネーブルになります。DNS Guard は、セキュリティアプライアンスによって DNS 応答が転送されるとすぐに、DNS クエリーと関連付けられた DNS セッションをティアダウンします。また、DNS Guard は、メッセージ交換をモニタして、DNS 応答の ID が DNS クエリーの ID と一致することを確認します。</p> <p>このコマンドは、DNS 検査が無効のインターフェイス上でのみ有効です。DNS インスペクションがイネーブルになっている場合、DNS Guard 機能は常に実行されます。</p> <p>(注) 7.0(5) よりも前のリリースでは、DNS インスペクションの設定に関係なく、DNS Guard 機能は常にイネーブルになります。</p>
DefaultDNS Server Group (ASA 8.4(2)+)	<p>DefaultDNS サーバグループのみに適用される追加設定。これらの設定は、FQDN ネットワーク/ホストオブジェクトを IP アドレスに解決するときを使用されます。</p> <ul style="list-style-type: none"> <li>• [ポーリングタイマー (Poll Timer) ] : FQDN ネットワーク/ホストオブジェクトを IP アドレスに解決するために使用するポーリングサイクルの時間 (分単位)。FQDN オブジェクトはファイアウォール ポリシーで使用される場合にのみ解決されます。タイマーによって解決間隔の最大時間が決まります。IP アドレス解決に対して更新するタイミングの決定には DNS エントリの存続可能時間 (TTL) 値も使用されるため、個々の FQDN がポーリングサイクルよりも頻繁に解決される場合があります。</li> </ul> <p>デフォルトは 240 (4 時間) です。指定できる範囲は 1 ~ 65535 分です。</p> <ul style="list-style-type: none"> <li>• [エントリの有効期限切れタイマー (Expire Entry Timer) ] : DNS エントリの期限が切れた (TTL が経過した) 後、そのエントリが DNS ルックアップテーブルから削除されるまでの分数。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくなる可能性があります。DNS エントリによっては TTL が極端に短い (3 秒程度) 場合があるため、この設定を使用して TTL を実質的に延長できます。</li> </ul> <p>デフォルトは 1 分です (つまり、TTL が経過してから 1 分後にエントリが削除されます)。指定できる範囲は 1 ~ 65535 分です。</p>

## [Add DNS Server Group] ダイアログボックス

[DNSサーバグループの追加 (Add DNS Server Group) ] ダイアログボックスを使用して、セキュリティデバイスが、名前解決をサポートするポリシーの IP アドレスにサーバ名を解決するときに使用する、DNS サーバグループの DNS サーバおよび設定を定義します。



(注) このダイアログボックスと [Edit DNS Server Group] ダイアログボックスは、タイトルを除けば同じです。次の説明は両方に適用されます。

### ナビゲーションパス

[Add DNS Server Group] および [Edit DNS Server Group] ダイアログボックスには、[\[DNS\] ページ \(20 ページ\)](#) からアクセスできます。

### フィールドリファレンス

表 14: [Add DNS Server Group]/[Edit DNS Server Group] ダイアログボックス

要素	説明
名前	DNS サーバグループの名前を指定します。  ヒント DefaultDNS という名前は ASA で事前定義されており、FQDN ネットワーク/ホストオブジェクトの解決など、特定のグループの選択を許可しないポリシーに使用されるサーバーが含まれています。
DNS サーバ	このグループの DNS サーバーを一覧表示します。DNS 要求を転送可能な宛先のサーバを最大 6 台指定できます。セキュリティアプライアンスは、応答を受け取るまで、各 DNS サーバを上から順に試行します。  (注) また、 <a href="#">[DNS] ページ (20 ページ)</a> の [DNS Lookup] セクションで、DNS がイネーブルになっているインターフェイスを少なくとも 1 つ指定する必要があります。  このリストの隣の各ボタンを使用して、エントリを管理します。上から順に次の機能があります。 <ul style="list-style-type: none"> <li>• DNS サーバをリストに追加する。<a href="#">[Add DNS Server] ダイアログボックス (24 ページ)</a> が開きます。</li> <li>• リストから、選択されている DNS サーバエントリを削除する。</li> <li>• 現在選択されているエントリを 1 つ上の行に移動する。</li> <li>• 現在選択されているエントリを 1 つ下の行に移動する。</li> </ul>
タイムアウト (Timeout)	次の DNS サーバの試行を待機する秒数を 1 ~ 30 の範囲で指定します。デフォルトは 2 秒です。セキュリティデバイスがサーバのリストを再試行するたびに、このタイムアウトは 2 倍に増えます。
Retries	セキュリティデバイスが応答を受信しない場合に DNS サーバのリストを再試行する回数を、0 ~ 10 の範囲で指定します。

要素	説明
ドメイン名	任意で、サーバーの有効な DNS ドメイン名を指定します（ <code>dnsexample.com</code> など）。

## [Add DNS Server] ダイアログボックス

[Add DNS Server] ダイアログボックスを使用して、[Add DNS Server Group] または [Edit DNS Server Group] ダイアログボックス内の DNS サーバリストに DNS サーバを追加します。

### ナビゲーションパス

[Add DNS Server] ダイアログボックスには、[Add DNS Server Group] または [Edit DNS Server Group] ダイアログボックスからアクセスできます。これらのダイアログボックスの詳細については、[\[Add DNS Server Group\] ダイアログボックス \(22 ページ\)](#) を参照してください。

### 関連項目

- [\[DNS\] ページ \(20 ページ\)](#)

### フィールド リファレンス

表 15: [Add DNS Server] ダイアログボックス

要素	説明
DNS サーバー	DNS サーバーの IP アドレス、または DNS サーバーのアドレスを定義するホストネットワーク/ホストオブジェクト。アドレスを入力します。または、[選択 (Select)] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成します。
[インターフェイス (Interface)] (ASA 9.5(1) 以降)	[選択 (Select)] をクリックして、インターフェイスを選択します。[インターフェイス (Interface)] セレクタダイアログボックスには、インターフェイスロールのみが一覧表示され、物理インターフェイスは表示されません。そのため、送信元インターフェイスを選択する前に、インターフェイスロールに物理インターフェイスを追加する必要があります。インターフェイスにデフォルト値はありません。  この機能は、ASA バージョン 9.5(1) 以降を実行しているデバイスの Security Manager バージョン 4.9 以降で使用できます。

## [DNSサーバーグループの追加 (AddDNSServerGroup)] ダイアログボックス

DNS グループマップの名前とドメインを定義するには、[DNS グループマップの追加 (Add DNS Group Map)] ダイアログボックスを使用します。





- (注) グループマップエントリを編集するには、[DNS グループマップの編集 (Edit DNS Group Map) ] ダイアログボックスを使用します。

### ナビゲーションパス

[DNS グループマップの追加 (Add DNS Group Map) ]および [DNS グループマップの編集 (Edit DNS Group Map) ] ダイアログボックスには、[DNS] [\[DNS\] ページ \(20 ページ\)](#) 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 16: [DNS グループマップの追加 (Add DNS Group Map) ]/[DNS グループマップの編集 (Edit DNS Group Map) ] ダイアログボックス

要素	説明
名前	DNS グループマップの名前を指定します。
ドメイン名	グループマップの有効な DNS ドメイン名を指定します ( <b>dnsexample.com</b> など)。 (注) DNS グループマップ名ごとに一意のドメイン値を入力します。

## DDNS の設定

Dynamic DNS (DDNS) は、DHCP で割り当てられた IP アドレスが頻繁に変更されても各ホストが互いを検出できるように、IP アドレスとドメイン名のマッピングの更新を行います。また、バージョン 7.2(3) 以降では、Cisco セキュリティ アプライアンスは DDNS 更新を生成できます。この機能は、[DDNS] ページで設定します。

DDNS マッピングは、DHCP サーバーで 2 種類の Resource Record (RR) 内で管理されます。アドレス (A) レコードには、名前から IP アドレスへのマッピングが含まれ、ポインタ (PTR) レコードはアドレスをホスト名にマップします。

DDNS は、定義した間隔で割り当て済みのアドレスとホスト名の間のアソシエーションを自動的に記録するため、アドレスとホスト名のアソシエーションを頻繁に変更することができます。これにより、たとえばモバイルホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセレクトタから [\[プラットフォーム \(Platform\) \]](#) > [\[デバイス管理 \(Device Admin\) \]](#) > [\[サーバアクセス \(Server Access\) \]](#) > [\[DDNS\]](#) を選択します。

- (ポリシービュー) ポリシータイプセクタから **[PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)]** > **[デバイス管理 (Device Admin)]** > **[サーバアクセス (Server Access)]** > **[DDNS]** を選択します。共有ポリシーセクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

## フィールドリファレンス

表 17: [DDNS] ページ

要素	説明
Dynamic DNS Interface Settings	このテーブルには、現在定義されている DDNS インターフェイス更新方式が一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらの方式を管理します。[Add Row] および [Edit Row] ボタンを使用すると、 <a href="#">[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス (26 ページ)</a> が開きます。
DHCP Client requests DHCP Server to update records	DHCP クライアント更新要求のための、アプライアンスでのグローバル設定。このオプションでは、クライアントが DHCP サーバを介して DDNS 更新を送信できるようにし、更新するレコード (PTR リソース レコード、A リソース レコードと PTR リソース レコードの両方、またはどちらも更新しない) を指定します。[Not Selected]、[Only PTR Record]、[Both A and PTR Record]、または [No Update] を選択します。
DHCP Client ID Interface	グローバル DHCP クライアントの更新要求で使用するインターフェイスを指定します。インターフェイス名または IP アドレスを入力するか、インターフェイス オブジェクトを選択します。
DHCP クライアントブロードキャストの有効化 (Enable DHCP Client Broadcast)	このオプションを選択すると、デバイス上の DHCP クライアントが DDNS 更新をブロードキャストできます。ASA/PIX 7.2(3)+ デバイスだけで選択可能です。

## [Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス

[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックスを使用して、Dynamic DNS 更新のルールを管理します。これらのルールは、インターフェイスごとに定義します。

### ナビゲーションパス

[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックスには、[DDNS の設定 \(25 ページ\)](#) からアクセスします。

## 関連項目

- [\[DDNS Update Methods\] ダイアログボックス](#) (27 ページ)
- [\[Add DDNS Update Methods\]/\[Edit DDNS Update Methods\] ダイアログボックス](#) (28 ページ)

## フィールド リファレンス

表 18: [\[Add DDNS Interface Rule\]/\[Edit DDNS Interface Rule\] ダイアログボックス](#)

要素	説明
インターフェイス (Interface)	DDNSを設定するインターフェイスの名前を入力または選択します。 (注) 指定したインターフェイスでは、DHCP がイネーブルになっている必要があります。
メソッド名	以前に定義されている DDNS 更新方式を選択するか、または[更新方式の追加 (Add Update Method) ]/[更新方式の編集 (Edit Update Method) ]を選択して新しい方式を定義します。 <a href="#">[DDNS Update Methods] ダイアログボックス</a> (27 ページ) ダイアログボックスが開きます。
ホストネーム	更新の送信先の DDNS サーバホストの名前を入力します。
DHCP Client requests DHCP Server to update records	インターフェイスでの DHCP クライアントの更新要求の設定。DHCP サーバが、PTR リソース レコードだけを更新するか、A リソース レコードと PTR リソース レコードの両方を更新するか、またはどちらも更新しないかを指定します。  [Not Selected]、[Only PTR Record]、[Both A and PTR Record]、または [No Update] を選択します。[Not Selected] 以外の項目を選択すると、 <a href="#">DDNS の設定</a> (25 ページ) のグローバル設定が上書きされます。

## [DDNS Update Methods] ダイアログボックス

[DDNS Update Methods] ダイアログボックスを使用して、Dynamic DNS 更新の方式を管理します。定義済みの方式ではそれぞれ、更新間隔と、更新対象のリソースレコードが指定されています。

### ナビゲーションパス

[DDNS 更新方式 (DDNS Update Methods) ] ダイアログボックスにアクセスするには、[\[Add DDNS Interface Rule\]/\[Edit DDNS Interface Rule\] ダイアログボックス](#) (26 ページ) の [方式名 (Method Name) ] ドロップダウンリストから [更新方式の追加 (Add Update Method) ]/[更新方式の編集 (Edit Update Method) ] を選択します。

**[Add DDNS Update Methods]/[Edit DDNS Update Methods]** ダイアログボックス

## 関連項目

- [DDNS の設定 \(25 ページ\)](#)

## フィールド リファレンス

表 19: **[DDNS Update Methods]** ダイアログボックス

要素	説明
Update Methods	このテーブルには、現在定義されている更新方式が一覧表示されます。テーブルの下のボタンを使用して、これらのエントリを管理します。
[Add Row] ボタン	新しい更新方式を定義できる <a href="#">[Add DDNS Update Methods]/[Edit DDNS Update Methods]</a> ダイアログボックス (28 ページ) が開きます。
[Edit Row] ボタン	テーブルで現在選択されている方式を編集できる <a href="#">[Add DDNS Update Methods]/[Edit DDNS Update Methods]</a> ダイアログボックス (28 ページ) が開きます。
[Delete Row] ボタン	[更新方式 (Update Methods) ] テーブルで現在選択されている方式を削除します。確認が必要な場合があります。

**[Add DDNS Update Methods]/[Edit DDNS Update Methods]** ダイアログボックス

[Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックスを使用して、DDNS 更新方式を定義または編集します。現在定義されている方式は、[\[DDNS Update Methods\]](#) ダイアログボックス (27 ページ) に一覧表示されます。

## ナビゲーションパス

[Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックスにアクセスするには、[\[DDNS Update Methods\]](#) ダイアログボックス (27 ページ) で [Add Row] または [Edit Row] ボタンをクリックします。

## 関連項目

- [DDNS の設定 \(25 ページ\)](#)

## フィールド リファレンス

表 20: **[Add DDNS Update Methods]/[Edit DDNS Update Methods]** ダイアログボックス

要素	説明
メソッド名	この方式の識別子を指定します。

要素	説明
[アップデート間隔 (Update Interval) ]	この方式でのレコードの更新頻度を指定します。日数、時間数、分数、および秒数を指定します。時間、分、および秒のデフォルト値は0ですが、[Day]のデフォルト値はないため、[Day]には数字を入力する必要があります。
Update Records	更新するリソースレコードを指定します。[定義なし (Not Defined) ]、[A レコード (A Records) ]、または[A および PTR レコードの両方 (Both A and PTR Records) ]を選択してください。[A Records] または [Both A and PTR Records] を選択すると、 <a href="#">[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス (26 ページ)</a> の設定が上書きされます。

## [NTP] ページ

正確に同期された時刻をネットワークシステムに提供するサーバの階層システムを実装するには、ネットワーク タイム プロトコル (NTP) を使用します。正確なタイム スタンプが関連する時間依存操作 (Certificate Revocation List (CRL; 証明書失効リスト) など) では、時刻が正確である必要があります。複数の NTP サーバーを設定できます。セキュリティ デバイスは、(データの信頼度を測る手段として) 最下層のサーバを選択します。



- (注) このページは Catalyst 6500 サービス モジュール (ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール) では使用できません。

[NTP] ページを使用して、NTP をイネーブルにし、セキュリティ デバイスの時刻を動的に設定するために使用する NTP サーバを管理します。



- (注) NTP サーバーから取得された時刻によって、[クロック (Clock) ] ページで手動で設定した時刻がオーバーライドされます。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセレクトタから [プラットフォーム (Platform) ] > [デバイス管理 (Device Admin) ] > [サーバアクセス (Server Access) ] > [NTP] を選択します。
- (ポリシービュー) ポリシータイプセレクトタから [PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform) ] > [デバイス管理 (Device Admin) ] > [サーバアクセス (Server Access) ] > [NTP] を選択します。共有ポリシー セレクトタから既存のポリシーを選択するか、または新しいポリシーを作成します。

## フィールド リファレンス

表 21: [NTP] ページ

要素	説明
Enable NTP Authentication	NTP サーバでの認証をイネーブルまたはディセーブルにします。認証をディセーブルにしても、設定されているサーバのリストは変更されません。  認証をイネーブルにした場合、セキュリティ アプライアンスは、パケット内で適切な <b>trusted key</b> を使用している場合にだけ、NTP サーバと通信します。また、セキュリティ アプライアンスは、認証キーを使用して NTP サーバと同期します。
NTP Server Table	現在設定されている NTP サーバが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、このリストを管理します。 [Add Row] および [Edit Row] ボタンを使用すると、 <a href="#">[NTP Server Configuration] ダイアログボックス (30 ページ)</a> が開きます。

## [NTP Server Configuration] ダイアログボックス

[NTP Server Configuration] ダイアログボックスを使用して、NTP サーバ定義を追加または編集します。

## ナビゲーションパス

[NTP Server Configuration] ダイアログボックスには、[\[NTP\] ページ \(29 ページ\)](#) からアクセスできます。



(注) [NTP] ページは Catalyst 6500 サービスモジュール (ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール) では使用できません。

## フィールド リファレンス

表 22: [NTP Server Configuration] ダイアログボックス

要素	説明
IPアドレス	NTP サーバの IP アドレスを入力または選択します。

要素	説明
優先 (Preferred)	このチェックボックスをオンにした場合、複数のサーバの精度が同程度であれば、この NTP サーバが優先サーバとなります。  NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。複数のサーバの精度が同程度であれば、このオプションで指定されたサーバが使用されます。ただし、優先サーバよりもはるかに精度の高いサーバがある場合、セキュリティアプライアンスによって精度の高い方のサーバが使用されます。たとえば、セキュリティアプライアンスでは、第 3 層の優先サーバではなく第 2 層のサーバが使用されます。複数のサーバの層が同じである可能性が高い場合にだけ、NTP サーバを優先サーバとして設定することを推奨します。
インターフェイス	ルーティング テーブル内のデフォルト インターフェイスを上書きする場合は、NTP トラフィックに使用するインターフェイスを入力または選択します。
認証タイプ (Authentication Type)	MD5 に追加すると、ASA 9.13(1) 以降のデバイスでは、バージョン 4.20 以降の Cisco Security Manager で次の認証タイプもサポートされます。  <ul style="list-style-type: none"> <li>• sha1</li> <li>• sha256</li> <li>• sha512</li> <li>• cmac</li> </ul>
Key Number	この認証キーの ID を入力します。NTP サーバの packets も、常にこのキー ID を使用する必要があります。以前に別のサーバに対してキー ID を設定した場合は、そのキー ID をリストから選択できます。それ以外の場合は、1 ~ 4294967295 の数字を入力します。
信頼できる	このキーを <code>trustedkey</code> として設定します。認証を正常に行うには、このオプションを選択する必要があります。
Key Value	認証キーを最大 32 文字の文字列として入力します。
確認 (Confirm)	認証キーを再入力して、それが正しいことを確認します。

## [SMTP Server] ページ

[SMTPサーバー (SMTP Server)] ページを使用して、SMTP サーバの IP アドレスを指定し、必要に応じて、バックアップサーバの IP アドレスを指定します。バックアップサーバの IP アドレスには、特定のイベントへの応答として電子メールアラートと通知が送信されます。

## ナビゲーションパス

- (デバイスビュー) デバイスポリシーセレクタから [プラットフォーム (Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [SMTPサーバー (SMTP Server)] を選択します。
- (ポリシービュー) ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [SMTPサーバー (SMTP Server)] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

## フィールド リファレンス

表 23: [SMTP Server] ページ

要素	説明
Primary Server IP Address	SMTP サーバーの IP アドレスを入力または選択します。
セカンダリサーバーのIPアドレス (Secondary Server IP Address)	バックアップ SMTP サーバの IP アドレスを入力または選択します。

## [TFTP Server] ページ

簡易ファイル転送プロトコル (TFTP) は、単純なクライアント/サーバーファイル転送プロトコルで、RFC783 および RFC1350 Rev. 2 で規定されています。[TFTP Server] ページを使用して、セキュリティアプライアンスが実行設定のコピーを TFTP サーバに転送できるように、セキュリティアプライアンスを TFTP クライアントとして設定できます。この方法で、設定ファイルをバックアップして、複数のセキュリティアプライアンスに伝播できます。1台のサーバだけがサポートされます。

## ナビゲーションパス

- (デバイスビュー) デバイスポリシーセレクタから [プラットフォーム (Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [TFTPサーバー (TFTP Server)] を選択します。
- (ポリシービュー) ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)] > [デバイス管理 (Device Admin)] > [サーバアクセス (Server Access)] > [TFTPサーバー (TFTP Server)] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。



## フィールドリファレンス

表 24 : [TFTP Server] ページ

要素	説明
インターフェイス (Interface)	TFTP サーバへのアクセスに使用するインターフェイスの名前を入力または選択します。
IPアドレス	TFTP サーバーの IP アドレスを入力または選択します。
ディレクトリ	スラッシュ (/) で始まり、構成ファイルが書き込まれるファイル名で終わる TFTP サーバー上のパスを入力します (例 : /tftpboot/asa/config3)。  (注) パスの先頭には必ずスラッシュ (/) を付けます。



## 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。