基本設定

この章では、ASA を機能させるためのコンフィギュレーションに一般的に必要となる、基本的な設定を指定する方法を説明します。次の項で構成されています。

ホスト名、ドメイン名、およびパスワードの設定

この項では、次の内容について説明します。

ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードの設定

ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Device Name/Password] を選択します。

ステップ 2　ホスト名を入力します。デフォルトのホスト名は「asa」です。

ホスト名はコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。ホスト名は syslog メッセージでも使用されます。

マルチコンテキスト モードでは、システム実行スペースで設定したホスト名がすべてのコンテキストのコマンド ラインのプロンプトに表示されます。コンテキストで設定したホスト名を、コマンドラインに表示せず、バナーに表示するオプションもあります。

ステップ 3　ドメイン名を入力します。デフォルト ドメイン名は default.domain.invalid です。

ASA は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

（注） マルチ コンテキスト モードの場合は、[Enable Password] 領域はコンテキストだけに表示され、システム実行スペースには表示されません。

ステップ 4　特権モード（イネーブル）パスワードを変更します。

イネーブル パスワードを使用すると、ログイン後に特権 EXEC モードにアクセスできます または、ユーザ名をブランクでASDMにアクセスする場合にこのパスワードが使用されます。（イネーブル アクセスのユーザ認証を設定する場合は、ユーザごとに個別のパスワードを指定します。このイネーブル パスワードは使用しません。さらに、HTTP/ASDM アクセスにも認証を設定できます）。

ステップ 5　古いパスワードを入力します。

ステップ 6　新しいパスワードを入力します。

ステップ 7　新しいパスワードを確認します。

（注） マルチ コンテキスト モードの場合は、[Telnet Password] 領域はコンテキストだけに表示され、システム実行スペースには表示されません。

ステップ 8　Telnet アクセス用のログイン パスワードを変更します。

Telnet パスワードにはログイン パスワードを設定します。9.1（1）では、デフォルトは「cisco」です。9.1（2）以降は、デフォルトのパスワードはありません。ASA に接続して Telnet SSH セッションを実行している場合、ログイン パスワードで EXEC モードにアクセスできます （Telnet アクセスのユーザ認証を設定する場合は、ユーザごとに個別のパスワードを指定します。このログイン パスワードは使用しません）。

ステップ 9　古いパスワードを入力します。

ステップ 10　新しいパスワードを入力します。

ステップ 11　新しいパスワードを確認します。

ステップ 12　[Apply] をクリックして変更内容を保存します。

ホスト名、ドメイン名、パスワードの機能履歴

表 16-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 16-1　マスター パスフレーズの機能履歴

機能名	プラットフォーム リリース	機能情報
デフォルトのパスワードはなくなりました。	9.0（2）、9.1（2）	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。**注**：Telnet ユーザ認証を設定していない場合、ログイン パスワードは Telnet 接続にのみ使用されます。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」をリストアしていました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 変更された ASDM 画面はありません。

日付と時刻の設定

（注） ASASM の日時を設定しないでください。この設定は、ホスト スイッチから受信します。

この項では、次のトピックについて取り上げます。

- 「NTP サーバを使用する日付と時刻の設定」（P.16-3）
- 「手動での日付と時刻の設定」（P.16-4）

NTP サーバを使用する日付と時刻の設定

NTP サーバから日付と時刻を取得するには、[Configuration] > [Device Setup] > [System Time] > [NTP] の順に選択します。

手順の詳細

ASA で時刻を動的に設定するために NTP サーバを定義するには、[NTP] ペインを使用します。時刻は ASDM のメイン ウィンドウの下部にあるステータスバーに表示されます。NTP サーバから取得された時刻によって、[Clock] ペインで手動で設定した時刻が上書きされます。

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。ASA は一番下の階層からサーバを選択し、データ信頼度の尺度にします。

NTP サーバ設定の追加または編集

NTP サーバを追加または編集するには、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [System Time] > [NTP] の順に選択します。

ステップ 2　[Add] をクリックして、[Add NTP Server Configuration] ダイアログボックスを表示します。

ステップ 3　NTP サーバの IP アドレスを入力します。

ステップ 4　[Preferred] チェックボックスをオンにして、このサーバを優先サーバに設定します。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。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、ASA では、精度の高いそのサーバを使用します。

ステップ 5　ドロップダウン リストからインターフェイスを選択します。この設定では、NTP パケットの発信インターフェイスが指定されます。インターフェイスが空白の場合、ASA が使用するデフォルトの管理コンテキスト インターフェイスは、ルーティング テーブルによって決まります。管理コンテキスト（および使用可能なインターフェイス）を変更する場合は、安定性のために [None]（デフォルト インターフェイス）を選択します。

ステップ 6　ドロップダウン リストから、キー番号を選択します。この設定では、この認証キーのキー ID を指定します。これにより、MD5 認証を使用して NTP サーバと通信できます。NTP サーバのパケットも、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。

ステップ 7　[Trusted] チェックボックスをオンにして、この認証キーを信頼できるキーとして指定します。これは、認証を成功させるために必要です。

ステップ 8　認証キーを設定するめのキー値を入力します。この値は、最大 32 文字の文字列です。

ステップ 9　このキー値を再入力して、正しく 2 回入力したことを確認します。

ステップ 10　[OK] をクリックします。

ステップ 11　[Enable NTP authentication] チェックボックスをオンにして、NTP 認証を有効にします。

ステップ 12　[Apply] をクリックして変更内容を保存します。

手動での日付と時刻の設定

時刻は 24 時間形式で、ASDM のメイン ペインの下部にあるステータスバーに表示されます。

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

NTP サーバを使用して時刻を動的に設定する場合は、[Configuration] > [Device Setup] > [System Time] > [NTP] の順に選択します。[Clock] ペインで手動設定した時刻は、NTP サーバから取得した時刻によって上書きされます。

ASA の日付と時刻を手動で設定するには、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [System Time] > [Clock] の順に選択します。

ステップ 2　ドロップダウン リストからタイム ゾーンを選択します。この設定では、適切な時差を GMT に加えた（または GMT から差し引いた）タイム ゾーンを指定します。[Eastern Time]、[Central Time]、[Mountain Time]、または [Pacific Time] ゾーンを選択すると、次の時間帯で、時間が自動的に夏時間に調整されます。3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時。

（注）　ASA の時間帯を変更すると、インテリジェント SSM との接続がドロップされる場合があります。

ステップ 3　[Date] ドロップダウン リストをクリックしてカレンダーを表示します。続いて、次の方法を使用して正しい日付を検索します。

- 月の名前をクリックし、月のリストを表示し、次に目的の月をクリックします。カレンダーがその月に変わります。
- 年をクリックして年を変更します。上矢印と下矢印を使用して複数年をスクロールすることも、入力フィールドに年を入力することもできます。
- 年月の左右にある矢印をクリックすると、カレンダーが一度に 1 か月ずつ前後にスクロールします。
- カレンダーの日にちをクリックして日を設定します。

ステップ 4　時刻（時間、分、および秒）を手動で入力します。

ステップ 5　[Update Display Time] をクリックして、ASDM ペインの右下に表示される時刻を更新します。現在時刻は 10 秒ごとに自動更新されます。

マスター パスフレーズの設定

この項では、次のトピックについて取り上げます。

マスター パスフレーズに関する情報

マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスター パスフレーズを使用する機能としては、次のものがあります。

- OSPF

- EIGRP
- VPN ロード バランシング
- VPN（リモート アクセスおよびサイトツーサイト）
- フェールオーバー
- AAA サーバ
- ロギング
- 共有ライセンス

マスター パスフレーズのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

フェールオーバーのガイドライン

フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

[Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Shared Key] フィールドに任意の文字を入力するか、またはフェールオーバー 16 進キーを選択している場合はバックスペースを除く 32 の 16 進数（0-9A-Fa-f）を入力します。次に、[Apply] をクリックします。

マスター パスフレーズの追加または変更

マスター パスフレーズを追加または変更するには、次の手順を実行します。

ステップ 1　シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。

マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] の順に選択します。

ステップ 2　[Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスター パスフレーズがない場合は、[Apply] をクリックすると警告メッセージが表示されます。[OK] または [Cancel] をクリックして続行できます。

後からパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードはいずれも変更されず、マスター パスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

ステップ 3　[Change the encryption master passphrase] チェックボックスをオンにして、新しいマスター パスフレーズを入力および確認できるようにします。デフォルトでは、これらはディセーブルです。

新しいマスター パスフレーズの長さは 8 ～ 128 文字にする必要があります。

既存のパスフレーズを変更する場合は、新しいパスフレーズを入力する前に、古いパスフレーズを入力する必要があります。

マスター パスフレーズを削除するには、[New master passphrase] および [Confirm master passphrase] フィールドを空白のままにします。

ステップ 4　[Apply] をクリックします。

[Apply] をクリックした場合、次の条件では警告メッセージが表示されます。

- [Change the encryption master passphrase] フィールドがイネーブルで、新しいマスター パスフレーズ フィールドが空白であり、**no key configuration-key password-encrypt** コマンドがデバイスに送信された場合。
- 古いマスター パスフレーズが、**show password encryption** コマンド出力のハッシュ値と一致しない場合。
- 移植できない文字、特に 8 ビット表記の上位ビット セットの文字を使用している場合。
- マスター パスフレーズおよびフェールオーバーが有効だが、フェールオーバー共有キーを削除しようとすると、エラー メッセージが表示される場合。
- 暗号化がディセーブルだが、新しいマスター パスフレーズまたは置換マスター パスフレーズが指定された場合。[OK] または [Cancel] をクリックして続行します。
- マスター パスフレーズがセキュリティ コンテキスト モードで変更された場合。
- アクティブ/アクティブ フェールオーバーが設定されており、マスター パスフレーズが変更された場合。
- HTTP または HTTPS を使用するコンテキスト設定 URL のように、実行コンフィギュレーションがサーバに保存できないように設定されている場合、およびマスター パスフレーズが変更された場合。

マスター パスフレーズのディセーブル化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキスト パスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェア バージョンにダウングレードする場合は、パスフレーズを削除しておくと便利です。

ディセーブルにする現在のマスター パスフレーズがわかっていなければなりません。パスフレーズが不明の場合は、「マスター パスフレーズの回復」（P.16-8）を参照してください。

マスター パスフレーズをディセーブルにするには、次の手順を実行します。

ステップ 1　シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。

マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] の順に選択します。

ステップ 2　[Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスター パスフレーズがない場合は、[Apply] をクリックすると警告文が表示されます。[OK] または [Cancel] をクリックして続行します。

ステップ 3　[Change the encryption master passphrase] チェックボックスをオンにします。

ステップ 4　[Old master passphrase] フィールドに、古いマスター パスフレーズを入力します。ディセーブルにする古いマスター パスフレーズを指定する必要があります。

ステップ 5　[New master passphrase] フィールドと [Confirm master passphrase] フィールドを空白のままにします。

ステップ 6　[Apply] をクリックします。

マスター パスフレーズの回復

マスター パスフレーズは回復できません。マスター パスフレーズがわからなくなった場合や不明な場合は、削除できます。

マスター パスフレーズを削除するには、次の手順を実行します。

マスター パスフレーズの機能履歴

表 16-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 16-2　マスター パスフレーズの機能履歴

機能名	プラットフォーム リリース	機能情報
マスター パスフレーズ	8.3(1)	この機能が導入されました。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [Master Passphrase]。[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase]。

DNS サーバの設定

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。

他の機能（**ping** コマンドや **traceroute** コマンドなど）では、トレースルートのために ping する名前を入力できます。ASA では、DNS サーバと通信してこの名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。

（注）　ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。これらの機能では、サーバ名を IP アドレスに解決するために、[Configuration] > [Firewall] > [Objects] > [Network Object/Groups] ペインでサーバ名を追加して、IP アドレスを手動で入力する必要があります。

ダイナミック DNS の詳細については、「ダイナミック DNS（DDNS）の設定」（P.17-2）を参照してください。

前提条件

DNS ドメイン ルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングを設定し、DNS サーバに到達できるようにしてください。ルーティングの詳細については、「ルーティングに関する情報」（P.24-1）を参照してください。

ステップ 1　[ASDM] メイン ウィンドウで、[Configuration] > [Device Management] > [DNS] > [DNS Client] を選択します。

ステップ 2　[DNS Setup] 領域で、次のオプションの中から 1 つを選択します。

- Configure one DNS server group
- Configure multiple DNS server groups

ステップ 3　[Add] をクリックして、[Add DNS Server Group] ダイアログボックスを表示します。

ステップ 4　DNS 要求を転送できるアドレスを最大 6 つまで指定します。ASA では、応答を受信するまで各 DNS サーバを順に試します。

（注）　DNS サーバを追加する前に、少なくとも 1 つのインターフェイスで最初に DNS をイネーブルにする必要があります。[DNS Lookup] 領域に、インターフェイスの DNS ステータスが表示されます。[False] 設定は、DNS がディセーブルであることを示します。[True] 設定は、DNS がイネーブルであることを示します。

ステップ 5　設定済みの各 DNS サーバ グループの名前を入力します。

ステップ 6　設定済みのサーバの IP アドレスを入力し、[Add] をクリックして、これらをサーバ グループに含めます。設定済みサーバをグループから削除する場合は、[Delete] をクリックします。

ステップ 7　設定済みのサーバの順序を変更するには、[Move Up] または [Move Down] をクリックします。

ステップ 8　[Other Settings] 領域で、リスト内の次の DNS サーバを試行するまでの秒数を 1 ～ 30 秒で入力します。デフォルトは 2 秒です。ASA がサーバのリストを再試行するたびに、このタイムアウト時間は倍増します。

ステップ 9　グループ内の次の DNS サーバを試行するまでに待機する秒数を入力します。

ステップ 10　設定済みサーバのグループの有効な DNS ドメイン名を入力します。

ステップ 11　[OK] をクリックして、[Add DNS Server Group] ダイアログボックスを閉じます。

新しい DNS サーバ設定が表示されます。

ステップ 12　これらの設定を変更する場合は、[Edit] をクリックして、[Edit DNS Server Group] ダイアログボックスを表示します。

ステップ 13　必要な変更を行ってから、[OK] をクリックして [Edit DNS Server Group] ダイアログボックスを閉じます。

変更後の DNS サーバ設定が表示されます。

ステップ 14　DNS サーバ グループが DNS 要求を受信できるようにするには、[Set Active] をクリックします。

ステップ 15　[DNS Guard] 領域で、クエリーごとに 1 つの DNS 応答を実行するには、[Enable DNS Guard on all interfaces] チェックボックスをオンにします。DNS インスペクションがイネーブルな場合、選択したインターフェイスではこの設定が無視されます。

ステップ 16　変更を保存するには [Apply] をクリックし、変更を破棄して新しく入力するには [Reset] をクリックします。

ヒープ メモリ サイズの変更

このガイドのトラブルシューティング情報の使用に加えて、次の URL で *ASDM のトラブルシューティング*のドキュメントを参照してください：

http://www.cisco.com/en/US/products/ps6121/products_tech_note09186a0080aaeff5.shtml

ASDM でサポートされる最大設定サイズは 512 kb です。このサイズを超えると、パフォーマンスの問題が生じることがあります。たとえば、コンフィギュレーションのロード時には、完了したコンフィギュレーションの割合がステータス ダイアログボックスに表示されます。このとき、サイズの大きいコンフィギュレーションでは、ASDM によってまだコンフィギュレーションの処理が行われていても、完了した割合の増分が停止し、操作が中断されているように見えます。このような状況が発生した場合は、ASDM システム ヒープ メモリの増大を検討することを推奨します。

ASDM ヒープ メモリ サイズを拡大するには、次の手順を実行してランチャのショートカットを変更します。

ステップ 1　ASDM-IDM ランチャのショートカットを右クリックし、[Properties] を選択します。

ステップ 2　[Shortcut] タブをクリックします。

ステップ 3　[Target] フィールドで、「-Xmx」のプレフィックスが付いた引数を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768m に変更し、1 GB の場合は -Xmx1g に変更します。このパラメータの詳細については、http://docs.oracle.com/javase/1.5.0/docs/tooldocs/windows/java.html の Oracle の資料を参照してください。

DNS キャッシュのモニタリング

ASA では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報にローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカ

ル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバに DNS クエリーが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスと、対応するホスト名が一緒にローカル キャッシュに格納されます。

DNS キャッシュをモニタするには、次のペインを参照してください。

パス	目的
[Tools] > [Command Line Interface] **show** dns-hosts コマンドを入力し、[Send] を押します。	DNS キャッシュが表示されます。これには、DNS サーバからダイナミックに学習したエントリと **name** コマンドを使用して手動で入力された名前および IP アドレスが含まれます。