管理アクセス

この章では、Telnet、SSH、およびHTTPS（ASDMを使用）経由でシステム管理のためにASAにアクセスする方法、ユーザーを認証および許可する方法、およびログインバナーを作成する方法について説明します。

管理リモート アクセスの設定

ここでは、ASDM 用の ASA アクセス、Telnet または SSH、およびログイン バナーなどのその他のパラメータの設定方法について説明します。

HTTPS、Telnet、または SSH の ASA アクセスの設定

この項では、（ASDM および CSM を含む）HTTPS、Telnet、または SSH に Cisco ASA アクセスを設定する方法について説明します。次のガイドラインを参照してください。

- ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。必要なのは、この章の各項の説明に従って管理アクセスを設定することだけです。ただし、HTTP リダイレクトを設定して HTTP 接続を HTTPS に自動的にリダイレクトするには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスがHTTPポートをリッスンできません。

- ASAへの通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスはサポートされません。たとえば、管理ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定 （18 ページ）を参照してください。

- ASA では以下の接続が許可されます。

- コンテキストごとに最大 5 つの同時 Telnet 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
- コンテキストごとに最大 5 つの同時 SSH 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
- シングルコンテキストモードでは、最大 5 の ASDM 同時セッションを設定できます。マルチコンテキストモードでは、コンテキストごとに最大 5 つの同時 ASDM セッションを使用でき、全コンテキスト間で最大 200 の ASDM インスタンスの使用が可能です。

  ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、マルチ コンテキスト モード システムの ASDM セッションの制限が 200 の場合、HTTPS セッション数は 400 に制限されます。
- シングルコンテキストモードまたはコンテキストごとに最大 6 つの非 ASDM HTTPS 同時セッション（使用可能な場合）、すべてのコンテキスト間で最大または 100 の HTTPS セッション。

ASDM、その他のクライアントの HTTPS アクセスの設定

この項では、ASDM や CSM など、HTTPS に ASA アクセスを設定する方法について説明します。

同じインターフェイス上で SSL（[webvpn] > [インターフェイスの有効化（enable interface）]）と HTTPS アクセスの両方を有効にした場合、**https://***ip_address* から セキュアクライアント にアクセスでき、**https://***ip_address*/**admin** から ASDM にアクセスできます。どちらもポート 443 を使用します。HTTPS の認証も有効にする（CLI、ASDM、および enable コマンドアクセス認証の設定 （26 ページ））場合は、ASDM アクセス用に別のポートを指定する必要があります。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [ASDM/HTTPS] を選択します。

ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレス設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。VPN 管理アクセスのみ（VPN トンネルを介した管理アクセスの設定 （18 ページ）を参照してください）の場合、名前付き BVI インターフェイスを指定します。

ステップ 4 証明書認証を要件にするには、[Specify the interface requires client certificate to access ASDM] 領域で [Add] をクリックし、インターフェイスとオプションで証明書マップを指定します。証明書マップを指定する場合、その証明書マップと一致しなければ、認証は成功しません。証明書マップを作成するには、**[構成（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細設定（Advanced）] > [IPSec] > [証明書と接続のマッピング（Certificate to Connection Map）] > [ルール（Rules）]**の順に選択します。

ステップ 5 [HTTP Settings] を設定します。

- [Enable HTTP Server]：HTTPS サーバーを有効にします。
- [Port Number]：ポート番号を設定します。デフォルトは 443 です。
- [Idle Timeout]：ASDM 接続のアイドルタイムアウトを 1 ～ 1440 分の範囲で設定します。デフォルトは 20 分です。ASA は、設定した期間アイドル状態の ASDM 接続を切断します。
- [Session Timeout]：ASDM セッションのセッションタイムアウトを 1 ～ 1440 分の範囲で設定します。このタイムアウトはデフォルトで無効になっています。ASA は、設定した期間を超えた ASDM 接続を切断します。
- [Connection Session Timeout]：ASDM、WebVPN、および他のクライアントを含むすべての HTTPS 接続のアイドルタイムアウトを 10 ～ 86400 秒の範囲で設定します。このタイムアウトはデフォルトで無効になっています。ASA は、設定した期間アイドル状態の接続を切断します。[Idle Timeout] と [Connection Session Timeout] の両方を設定した場合は、[Connection Session Timeout] が優先されます。

ステップ 6 [Apply] をクリックします。

ステップ 7 （任意） 非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。

多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。

a) **[Configuration] > [Device Management] > [Management Access] > [HTTP Non-Browser Client Support]** を選択し、[Add] をクリックします。
b) [User-Agent String from the HTTP Header] フィールドに、HTTP 要求の HTTP ヘッダーにあるクライアントの User-Agent 文字列を指定します。

完全な文字列または部分文字列を指定できます。部分文字列については、User-Agent 文字列の先頭と一致している必要があります。セキュリティを強化するために完全な文字列をお勧めします。文字列では大文字と小文字が区別されることに注意してください。

たとえば、 **curl** は次の User-Agent 文字列と一致します。

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

curl は、次の User-Agent 文字列とは一致しません。

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

CURL は、次の User-Agent 文字列とは一致しません。

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

SSH アクセスの設定

SSH ガイドライン

- また、ASA インターフェイスに SSH アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの SSH アクセスはサポートされません。たとえば、SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。
- ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 SSH 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。ただし、設定コマンドは変更されるリソースをロックする可能性があるため、すべての変更が正しく適用されるように、一度に 1 つの SSH セッションで変更を行う必要があります。
- SSH では次の機能はサポートされていません。
  - EDDSA キーペア
  - FIPS モードの RSA キーペア
- Cisco ASA **copy** コマンドを使用して SCP サーバーとの間でファイルをコピーするには、次の手順を実行する必要があります。
  - コマンドを使用して、Cisco ASA で SCP サーバーサブネット/ホストの SSH アクセスを有効にします。
  - キーペアを生成します（物理 Cisco ASA の場合のみ）。

- フェールオーバーを使用する場合、message-of-the-day (motd) バナーを設定すると、ログインしているユニットのフェールオーバー状態と最後のフェールオーバー時刻に関する情報がバナーに表示されます。この情報は、CLI で障害対応などのアクションを実行しており、セッション間でフェールオーバーが発生する場合に役立ちます。

  ログイン バナーの設定 （21 ページ）を参照してください。

- SSH デフォルトユーザー名はサポートされなくなりました。**pix** または **asa** ユーザー名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、AAA 認証を設定し（**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authentication]** の順に選択）、続いてローカルユーザーを定義する必要があります（**[Configuration]** > **[Device Management]** > **[Users/AAA]** の順に選択）。ローカル データベースの代わりに AAA サーバーを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

- SSH バージョン 2 のみがサポートされます。

Cisco ASA への SSH アクセスを構成するには、SSH サーバーをイネーブルにして、許可する IP アドレスを指定します。ユーザーを認証するために、次の方法を使用できます。

- ローカルデータベースまたは AAA サーバーのいずれかを使用するユーザー名とパスワード。
- ローカルデータベースを使用したユーザー名と公開キー。
- X.509v3 証明書（ユーザー名は証明書から派生）およびローカルデータベースまたは AAA サーバーからの承認。

デフォルトでは、SSH クライアントでサポートされているアルゴリズムに応じて、X.509 証明書または公開キー認証方式のいずれかが試行されますが、同じセッションで両方が試行されることはありません。X.509 認証も公開キー認証も成功しなかった場合、Cisco ASA はパスワード認証を試みます。必要に応じて、メソッドを禁止できます。

SSH サーバーの有効化

SSH サーバーを有効にし、接続を許可する IP アドレスを指定します。その他の SSH サーバー設定を行うこともできます。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[設定（Configuration）]>[デバイス管理（Device Management）]>[管理アクセス（Management Access）] > [ASDM/HTTPS/Telnet/SSH]** の順に選択し、[追加（Add）] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [SSH] を選択します。

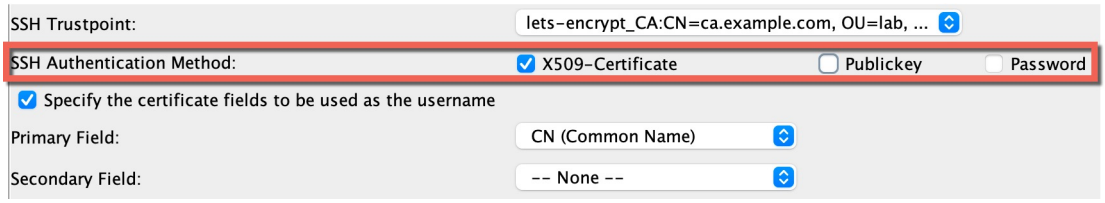
ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレス設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。

ステップ 4 （任意） [SSH Settings] を設定します。

- [SSH Timeout]：1 ～ 60 分にタイムアウトを設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。
- [キー交換ホストキー（Key Exchange Hostkey）]：（パスワードまたは公開キー認証のみ）デフォルトでは、Cisco ASA は、存在する場合、ECDSA、RSA の順にキーの使用を試みます。RSA キーを明示的に選択する場合は、2048 ビット以上のキーを生成する必要があります。アップグレードの互換性のために、ASA はデフォルトのホストキー設定が使用されている場合にのみ、より小さい RSA ホストキーを使用します。
- [DHキー交換（DH Key Exchange）]（管理コンテキストのみ）：該当するオプションボタンをクリックして、Diffie-Hellman（DH）キー交換グループを選択します。DH グループ キー交換方式を指定しないと、DH グループ 14 SHA256 のキー交換方式が使用されます。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。キー交換は管理コンテキストでのみ設定できます。この値はすべてのコンテキストで使用されます。
- 使用しない認証方式をオフにして、1 つまたは複数の認証方式を無効にします。

図 *1*：認証方式の無効化



デフォルトでは、SSH クライアントでサポートされているアルゴリズムに応じて、X.509 証明書または公開キー認証方式のいずれかが試行されますが、同じセッションで両方が試行されることはありません。X.509 認証も公開キー認証も成功しなかった場合、Cisco ASA はパスワード認証を試みます。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 （任意） SSH 暗号の暗号化アルゴリズムと整合性アルゴリズムを設定します。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [高度（Advanced）] > [SSH暗号（SSH Ciphers）]** の順に選択します。

b) [Encryption] を選択し、[Edit] をクリックします。

c) [SSH cipher security level] ドロップダウンリストから、次のいずれかのレベルを選択します。

暗号方式は、リストされた順に使用されます。事前定義されたリストでは、暗号方式が最も高いの順で、最も低いセキュリティに割り当てられています。

- [すべて（All）]：すべての暗号（AEAD_AES_256_GCM aes256-gcm@openssh.com 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr chacha20-poly1305@openssh.com aes192-ctr aes256-ctr aes256-gcm@openssh.com）を使用することを指定します
- [Custom]：カスタム暗号ストリングを設定する場合はこのオプションを選択し、[Cipher algorithms/custom string] フィールドに各暗号ストリングをコロンで区切って入力します。
- [Fips]：FIPS に準拠する暗号（AEAD_AES_256_GCM aes256-gcm@openssh.com aes128-cbc aes256-cbc）のみを指定します
- [高（High）]：非常に強力な暗号（AEAD_AES_256_GCM aes256-gcm@openssh.com aes256-cbc chacha20-poly1305@openssh.com aes256-ctr aes256-gcm@openssh.com）のみを使用することを指定します
- [低（Low）]：低、中、高程度の暗号（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr AEAD_AES_256_GCM aes256-gcm@openssh.com）を使用することを指定します
- [中（Medium）]：デフォルト値で、中、高程度の暗号（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr AEAD_AES_256_GCM aes256-gcm@openssh.com）を使用することを指定します

d) [Integrity] を選択し、[Edit] をクリックします。

e) [SSH cipher security level] ドロップダウン リストから、次のいずれかのレベルを選択します。

- [All]：すべての暗号方式（hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96）を使用することを指定します。
- [Custom]：カスタム暗号ストリングを設定する場合はこのオプションを選択し、[Cipher algorithms/custom string] フィールドに各暗号ストリングをコロンで区切って入力します。
- [Fips]：FIPS 対応の暗号方式のみ（hmac-sha1 hmac-sha2-256 ）を指定します。
- [High]：強度が高の暗号方式のみ（ hmac-sha2-256）を指定します（デフォルト）。
- [Low]：強度が低、中、高の暗号方式（hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96）を使用する場合は、このオプションを選択します。

• [Medium]：強度が中および高の暗号方式（hmac-sha1 hmac-sha1-96）を指定します。

ステップ 7 セキュアコピーサーバーをイネーブルにします。

a) コンテキスト モードによって次のように異なります。

• シングル モードの場合、[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP)] の順に選択します。

• マルチ モードの場合、[Configuration] > [Device Management] > [Device Administration] > [Secure Copy] の順に選択します。

b) [Enable secure copy server] チェック ボックスをオンにします。

ステップ 8 [適用（Apply）] をクリックします。

例

次に、ASA への SCP セッションの例を示します。外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

scp -v -pw *password* [*path*/]*source_filename*
username@asa_address:{**disk0**|**disk1**}:/[*path*/]*dest_filename*

-v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

パスワードアクセス用の SSH の設定

ユーザー名とパスワードを使用して SSH 認証を設定します。

始める前に

• マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAアクセス（AAA Access）] > [認証（Authentication）]**を選択します。

ステップ 2 [SSH] チェックボックスをオンにします。

ステップ 3 [サーバーグループ（Server Group）] ドロップダウンリストから [LOCAL] データベース（または AAA サーバー）を選択します。

この設定は、公開キーが構成されているユーザー名に対するローカル公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカル データベースを暗黙的に使用します。この設定は、ローカルのユーザー名とパスワードにのみ影響します。ローカルユーザーが公開キー認証またはパスワードを使用できるようにするには、この設定を使用してローカル認証を明示的に設定し、パスワードアクセスを許可する必要があります。

ステップ 4 [適用（Apply）] をクリックします。

ステップ 5 SSH アクセスに使用できるローカルデータベースまたは AAA サーバーでユーザーを作成します。ローカルユーザー名を追加するには、次の手順を参照してください（推奨）。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [ユーザーアカウント（User Accounts）]**の順に選択し、[追加（Add）] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

b) ユーザー名とパスワードを入力し、パスワードを確認します。

同じローカルユーザーに対して、公開キー認証またはパスワード認証を使用できます。AAA サーバーを使用した公開キー認証はサポートされていません。

c) [OK] をクリックし、続いて [Apply] をクリックします。

ステップ 6 キーペアを生成します（物理 ASA の場合のみ）。

ASAv の場合、キーペアは導入後に自動的に作成されます。ASAv は RSA キーのみをサポートします。

a) **[構成（Configuration）] > [デバイス管理（Device Management）] > [証明書管理（Certificate Management）] > [ID証明書（Identity Certificates）]** の順に選択します。

b) [Add] をクリックし、[Add a new identity certificate] オプション ボタンをクリックします。

c) [New] をクリックします。

d) [キーペアを追加（Add Key Pair）] ダイアログボックスで、タイプとサイズを指定して [今すぐ生成（Generate Now）] をクリックします。

使用されるデフォルトのキーペアは、ECDSA、RSA です。RSA の場合は、2048 ビット以上のサイズを選択します。.

キーペアを生成するだけであるため、証明書のダイアログボックスをキャンセルできます。

e) [Apply] をクリックします。

公開キーアクセス用の SSH の設定

公開キーを使用して SSH 認証を設定します。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替え

るには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 SSH アクセスに使用できるユーザーをローカル データベースに作成します。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [ユーザーアカウント（User Accounts）]**の順に選択し、[追加（Add）] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

b) ユーザー名とパスワードを入力し、パスワードを確認します。

ユーザーにパスワード認証ではなく公開キー認証を強制する場合は、パスワードなしでユーザーを作成することを推奨します。公開キー認証およびパスワードの両方を設定した場合、ユーザーはいずれの方法でもログインできます（この手順で AAA 認証を明示的に設定した場合）。

c) 公開キー認証を有効にします。次のペインのいずれかを選択します。

- [Public Key Authentication]：Base64 でエンコードされた公開キーに貼り付けます。ssh-rsa、または ecdsa-sha2-nistp raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、キーを生成できます。既存のキーを表示する場合は、キーは SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼りつける場合は、[Key is hashed] チェックボックスをオンにします。

  認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。

- [Public Key Using PKF]：[Specify a new PKF key] チェックボックスをクリックして、公開キー ファイル（PKF）でフォーマットされたキー（4096 ビットまで）を貼りつけるかインポートします。Base64 形式で貼り付けるには大きすぎるキーにはこのフォーマットを使用します。たとえば、ssh の keygen を使用して 4096 ビット キーを生成し、PKF に変換して、このペインでインポートします。既存のキーを表示する場合は、SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼り付ける必要がある場合は、[Public Key Athentication] ペインからコピーし、[Key is hashed] チェックボックスをオンにした新しい ASA のペインに貼り付けます。

  認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。

d) [OK] をクリックし、続いて [Apply] をクリックします。

ステップ 2 キーペアを生成します（物理 ASA の場合のみ）。

ASAv の場合、キーペアは導入後に自動的に作成されます。ASAv は RSA キーのみをサポートします。

a) **[構成（Configuration）] > [デバイス管理（Device Management）] > [証明書管理（Certificate Management）] > [ID証明書（Identity Certificates）]** の順に選択します。
b) [Add] をクリックし、[Add a new identity certificate] オプション ボタンをクリックします。
c) [New] をクリックします。
d) [キーペアを追加（Add Key Pair）] ダイアログボックスで、タイプとサイズを指定して [今すぐ生成（Generate Now）] をクリックします。

   使用されるデフォルトのキーペアは、ECDSA、RSA です。RSA の場合は、2048 ビット以上のサイズを選択します。.

   （注）
   CiscoSSH スタックでは、接続の確立時に設定されたキーペアのみが Cisco ASA によって共有されます。

   キーペアを生成するだけであるため、証明書のダイアログボックスをキャンセルできます。

e) [適用（Apply）] をクリックします。

例

次に、PKF 形式のキーを使用して認証する例を示します。

次の例では、Linux または Macintosh システムの SSH の共有キーを生成して、ASA にインポートします。

1. コンピューターで 4,096 ビットの RSA 公開キーおよび秘密キーを生成します。

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
```

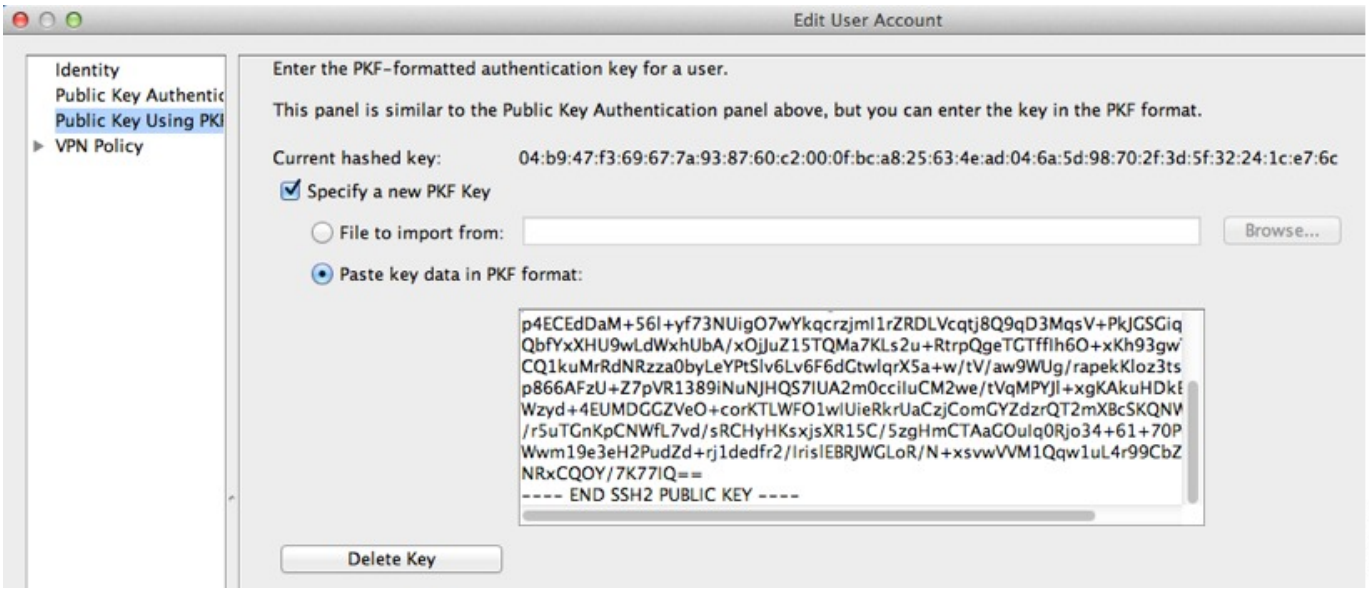
```
+-----------------+
```

2. PKF 形式にキーを変換します。

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. キーをクリップボードにコピーします。

4. ASDM で、**[構成（Configuration）] > [デバイス管理（Device Management）] > [ユーザ/AAA（Users/AAA）] > [ユーザアカウント（User Accounts）]** の順に選択し、ユーザ名を選択してから [編集（Edit）] をクリックします。[Public Key Using PKF] をクリックして、ウィンドウにキーを貼り付けます。



5. ユーザが ASA に SSH できることを確認します。パスワードには、キーペアの作成時に指定した SSH キーパスワードを入力します。

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
```

```
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

次のダイアログボックスが、パスフレーズを入力するために表示されます。

一方、端末セッションでは、以下が表示されます。

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

X.509 証明書アクセス用の SSH の設定

X.509v3 証明書による認証および承認を有効にします。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 トラストポイントを設定します。CA 証明書の設定を参照してください。

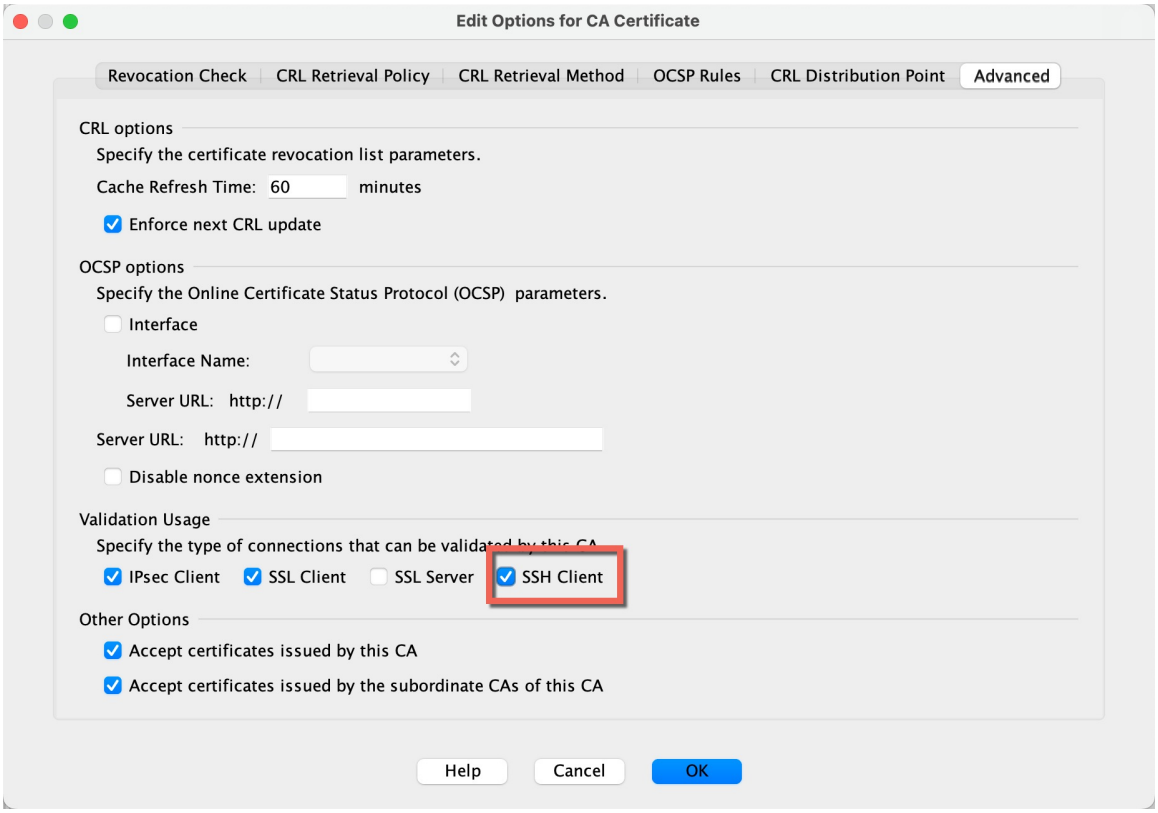
ステップ 2 SSH クライアントを検証するトラストポイントを有効にします。

a) **[構成（Configuration）] > [デバイス管理（Device Management）] > [証明書管理（Certificate Management）] > [CA証明書（CA Certificates）]** の順に選択し、トラストポイントを選択し、[編集（Edit）] をクリックします。

b) [Advanced] タブをクリックします。

c) [検証の使用（Validation Usage）] で、[SSHクライアント（SSH Client）] をオンにします。

図 *2 : SSH* クライアントの確認



d) [OK] をクリックし、さらに [Apply] をクリックします。

ステップ 3 証明書から取得されたユーザー名と一致するユーザーを認可サーバーに追加します。

- AAA サーバー：AAA サーバーおよびサーバーグループを参照して、AAA サーバーグループを Cisco ASA に追加します。
- ローカルデータベース：ローカル データベースへのユーザー アカウントの追加を参照してください。

このユーザーに対してもパスワード認証を許可する場合、ユーザーパスワードを設定できます。パスワード認証を設定しない場合、パスワードなしでユーザーを追加できます。この場合、パスワードを設定しても無視されます。

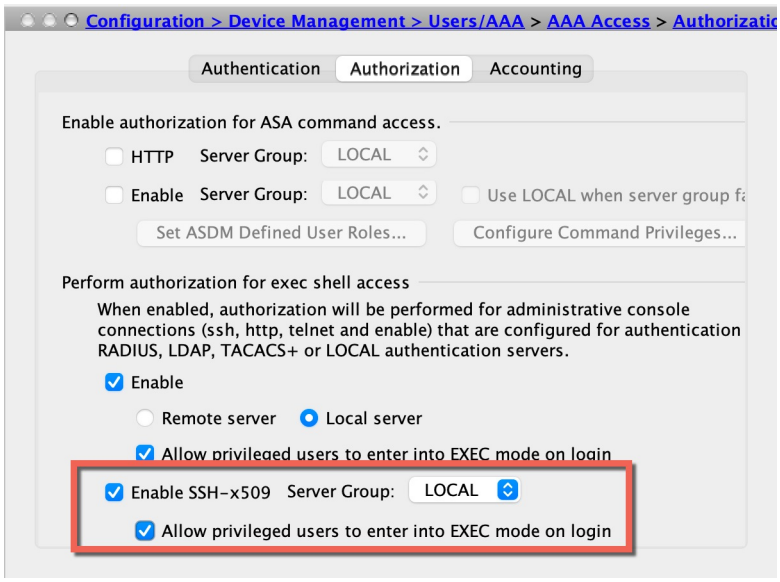
コンソール特権は、認可サーバーから返された属性に基づいて割り当てられます。ユーザーに設定する属性については、管理許可による CLI および ASDM アクセスの制限 （29 ページ）を参照してください。

ステップ 4 ローカルデータベースまたは AAA サーバーを使用してユーザーを認可します。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAアクセス（AAA Access）] > [承認（Authorization）]** を選択します

b) [SSH-x509を有効化（Enable SSH-x509）] にチェックを入れ、[サーバーグループ（Server Group）] のドロップダウンリストから [LOCAL] データベースまたは AAA サーバーを選択します。

図 3 : SSH 承認



c) （任意）[ログイン時に特権ユーザーがEXECモードを開始することを許可（Allow privileged users to enter into EXEC mode on login）] をオンにします。

このオプションは、十分な認証特権を持つ管理者が、ログインするときに特権 EXEC モードに自動的に入ることができます。

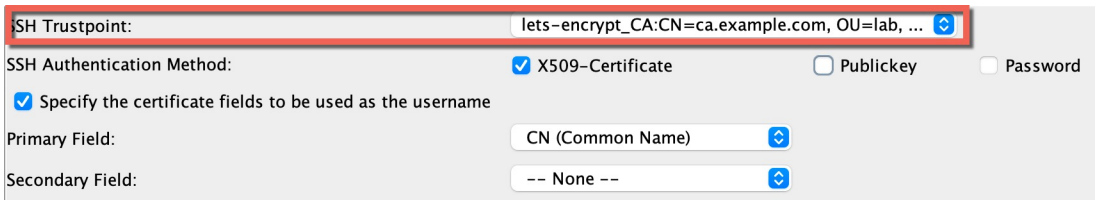
d) [適用（Apply）] をクリックします。

ステップ 5 **[構成（Configuration）]>[デバイス管理（Device Management）]>[管理アクセス（Management Access）] > [ASDM/HTTPS/Telnet/SSH]** の順に選択します。

ステップ 6 [SSH Settings] を設定します。

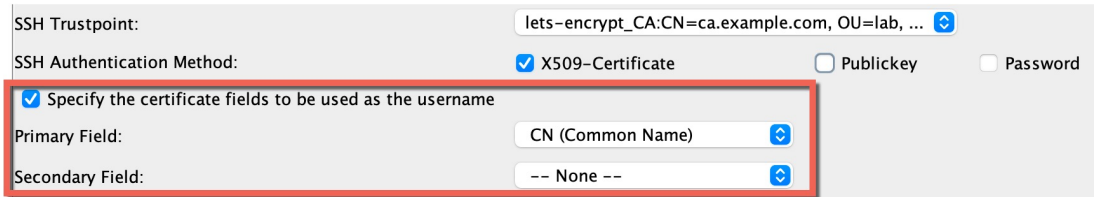
a) [SSHトラストポイント（SSH Trustpoint）] ドロップダウンリストから SSH に使用するトラストポイントを選択します。

図 4 : SSH トラストポイント



b) [ユーザー名として使用する証明書フィールドを指定する（Specify the certificate fields to be used as the username）] をオンにし、[プライマリフィールド（Primary Field）] ドロップダウンリストから方式を選択します。

図 *5:* 証明書のユーザー名



c) （任意）[セカンダリフィールド（Secondary Field）] ドロップダウンリストから方式を選択します。

d) [Apply] をクリックします。

Telnet アクセスの設定

この項では、Telnet に ASA アクセスを設定する方法について説明します。VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- ASA CLI に Telnet を使用してアクセスするには、ログイン パスワードを入力します。Telnet を使用する前に手動でパスワードを設定する必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [Telnet] を選択します。

ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレス設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。VPN 管理アクセスのみ（VPN トンネルを介した管理アクセスの設定 （18 ページ）を参照してください）の場合、名前付き BVI インターフェイスを指定します。

ステップ 4 （任意）[Telnet Timeout] を設定します。デフォルトのタイムアウト値は 5 分です。

ステップ 5 [Apply] をクリックします。

ステップ 6 Telnet で接続する前に、ログインパスワードを設定します。デフォルトのパスワードはありません。

a) **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** の順に選択します。
b) [Telnet Password] 領域で [Change the password to access the console of the security appliance] チェックボックスをオンにします。
c) 古いパスワードを入力して（新しい ASA の場合はこのフィールドを空白にする）、新しいパスワードを入力してから、確認として新しいパスワードを再入力します。
d) [Apply] をクリックします。

ASDM アクセスまたはクライアントレス SSL VPN のための HTTP リダイレクトの設定

ASDM またはクライアントレス SSL VPN を使用して ASA に接続するには、HTTPS を使用する必要があります。利便性のために、HTTP 管理接続を HTTPS にリダイレクトすることができます。たとえば、HTTP をリダイレクトすることによって、**http://10.1.8.4/admin/** または **https://10.1.8.4/admin/** と入力し、ASDM 起動ページで HTTPS アドレスにアクセスできます。

IPv4 と IPv6 の両方のトラフィックをリダイレクトできます。

始める前に

通常、ホスト IP アドレスを許可するアクセス ルールは必要ありません。ただし、HTTP リダイレクトのためには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[HTTP Redirect]** の順に選択します。

表には、現在設定されているインターフェイスと、リダイレクトがインターフェイスで有効化されているかどうかを示しています。

ステップ 2 ASDM に使用するインターフェイスを選択し、[Edit] をクリックします。

ステップ 3 [Edit HTTP/HTTPS Settings] ダイアログボックスで次のオプションを設定します。

- [Redirect HTTP to HTTPS]：HTTP 要求を HTTPS にリダイレクトします。
- [HTTP Port]：インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトは 80 です。

ステップ 4 [OK] をクリックします。

VPN トンネルを介した管理アクセスの設定

あるインターフェイスで VPN トンネルが終端している場合、別のインターフェイスにアクセスして ASA を管理するには、そのインターフェイスを管理アクセス インターフェイスとして指定する必要があります。たとえば、外部インターフェイスから Cisco ASA に入る場合は、この機能を使用して、ASDMまたは Telnet 経由で内部インターフェイスに接続するか、外部インターフェイスから入るときに内部インターフェイスに ping を実行できます。

（注） この機能は SSH ではサポートされません。

（注） この機能は SNMP ではサポートされません。VPN 経由の SNMP の場合、ループバック インターフェイスで SNMP を有効にすることをお勧めします。ループバック インターフェイスで SNMP を使用するために、管理アクセス機能を有効にする必要はありません。ループバックは SSH でも機能します。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの VPN アクセスはサポートされません。たとえば、VPN アクセスが外部インターフェイスにある場合、外部インターフェイスへの直接接続のみ開始できます。複数のアドレスを覚える必要がないように、ASA の直接アクセス可能インターフェイスの VPN を有効にし、名前解決を使用してください。

管理アクセスは、IPsec クライアント、IPsec サイト間、Easy VPN、セキュアクライアント SSL VPN の VPN トンネルタイプ経由で行えます。

始める前に

- この機能は管理専用インターフェイスではサポートされません。
- 管理アクセスインターフェイスを使用し、アイデンティティ NAT を構成する場合、ルート ルックアップ オプションを使用して NAT を構成する必要があります。詳細については、『ASA Firewall CLI Configuration Guide』の適切なリリースの「*NAT Examples and Reference*」の章の「NAT and VPN Management Access」の項を参照してください。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Interface]** の順に選択します。

ステップ 2 [Management Access Interface] ドロップダウン リストからセキュリティが最も高いインターフェイス（内部インターフェイス）を選択します。

サイト間トンネルでは、名前付き BVI を指定できます（ルーテッドモード）。

ステップ 3 [Apply] をクリックします。

管理インターフェイスが割り当てられ、変更内容が実行コンフィギュレーションに保存されます。

コンソール タイムアウトの変更

コンソール タイムアウトでは、接続を特権 EXEC モードまたはコンフィギュレーション モードにしておくことができる時間を設定します。タイムアウトに達すると、セッションはユーザー EXEC モードになります。デフォルトでは、セッションはタイムアウトしません。この設定は、コンソール ポートへの接続を保持できる時間には影響しません。接続がタイムアウトすることはありません。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Command Line (CLI)]** > **[Console Timeout]** の順に選択します。

ステップ 2 新しいタイムアウト値を分単位で定義します。無制限の時間を指定する場合は、「0」と入力します。デフォルト値は 0 です

ステップ 3 [Apply] をクリックします。

タイムアウト値の変更が実行コンフィギュレーションに保存されます。

CLI プロンプトのカスタマイズ

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしている ASA を一目で確認することができます。この機能は、フェールオーバー時に、両方の ASA に同じホスト名が設定されている場合に便利です。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

デフォルトでは、プロンプトに ASA のホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには、次の項目を表示できます。

cluster-unit	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
コンテキスト	（マルチ モードのみ）現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。

hostname	ホスト名を表示します。
priority	フェールオーバープライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。
state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、state キーワードに対して次の値が表示されます。 • [act]：フェールオーバーが有効であり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailover]：フェールオーバーは無効であり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーは無効であり、装置ではトラフィックを通過させていません。これは、スタンバイユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタリングの場合、制御とデータの値が表示されます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Command Line (CLI)]** > **[CLI Prompt]** の順に選択します。

ステップ 2 次のいずれかを実行してプロンプトをカスタマイズします。

- [Available Prompts] リストで属性をクリックしてから、[Add] をクリックします。プロンプトには複数の属性を追加できます。属性が [Available Prompts] リストから [Selected Prompts] リストに移動します。
- [Selected Prompts] リストで属性をクリックしてから、[Delete] をクリックします。属性が [Selected Prompts] リストから [Available Prompts] リストに移動します。
- [Selected Prompts] リストで属性をクリックして、[Move Up] または [Move Down] をクリックして属性の表示順序を変更します。

プロンプトが変化して、[CLI Prompt Preview] フィールドに表示されます。

ステップ 3 **Apply** をクリックします。

変更されたプロンプトが、実行コンフィギュレーションに保存されます。

ログイン バナーの設定

ユーザーが ASA に接続するとき、ログインする前、または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。「ウェルカム」や「お願いします」などの表現は侵入者を招き入れているような印象を与えるので使用しないでください。以下のバナーでは、不正アクセスに対して正しい表現を設定しています。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- バナーが追加された後、次の場合に ASA に対する Telnet または SSH セッションが終了する可能性があります。
  - バナー メッセージを処理するためのシステム メモリが不足している場合。
  - バナー メッセージの表示を試みたときに、TCP 書き込みエラーが発生した場合。
- フェールオーバーを使用する場合、message-of-the-day (motd) バナーを設定すると、ログインしているユニットのフェールオーバー状態と最後のフェールオーバー時刻に関する情報がバナーに表示されます。この情報は、CLI で障害対応などのアクションを実行しており、セッション間でフェールオーバーが発生する場合に役立ちます。
- バナー メッセージのガイドラインについては、RFC 2196 を参照してください。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Command Line (CLI)]** > **[Banner]** の順に選択します。

ステップ 2 CLI 用に作成するバナー タイプ用のフィールドにバナー テキストを追加します。

- [session (exec)] バナーは、ユーザーが CLI で特権 EXEC モードにアクセスした場合に表示されます。
- [login] バナーは、ユーザが CLI にログインした場合に表示されます。
- [message-of-the-day (motd)] バナーは、ユーザーが CLI に初めて接続する場合に表示されます。

- [ASDM] バナーは、ユーザーが認証を受けた後 ASDM に接続した場合に表示されます。ユーザーは、次のいずれかのオプションを使用して、表示されたバナーを消去できます。
  - [Continue]：バナーを消去して、ログインを完了します。
  - [Disconnect]：バナーを消去して、接続を終了します。
- 使用できるのは、改行（Enter キー）も含めて ASCII 文字だけです。ただし、改行文字は 2 文字に相当します。
- また、タブ文字は、CLI バージョンでは無視されるため、バナーには使用しないでください。
- RAM およびフラッシュ メモリに関するもの以外、バナーに長さ制限はありません。
- ASA のホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。
- システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** という文字列を使用することにより、コンテキスト内でバナー テキストを使用できます。

ステップ 3 [Apply] をクリックします。

新しいバナーが、実行コンフィギュレーションに保存されます。

管理セッション クォータの設定

ASA で許可する ASDM、SSH、および Telnet の同時最大セッション数を設定できます。この最大値に達すると、それ以降のセッションは許可されず、syslog メッセージが生成されます。システム ロックアウトを回避するために、管理セッション割り当て量のメカニズムではコンソール セッションをブロックできません。

（注） マルチコンテキストモードではASDMセッションの数を設定することはできず、最大セッション数は 5 で固定されています。

（注） また、最大管理セッション（SSHなど）のコンテキストあたりのリソース制限を設定した場合は、小さい方の値が使用されます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、

[Configuration] > **[Device List]** ペインで、アクティブなデバイスの IP アドレスの下のコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Session Quota]** の順に選択します。

ステップ 2 同時セッションの最大数を入力します。

- **Aggregate**：1 ～ 15 のセッションの集約数を設定します。デフォルトは 15 です。
- **HTTP Sessions**：1 ～ 5 の HTTPS（ASDM）セッションの最大数を設定します。デフォルトは 5 分です。
- **SSH Sessions**：1 ～ 5 の SSH セッションの最大数を設定します。デフォルトは 5 分です。
- **Telnet Sessions**：1 ～ 5 の Telnet セッションの最大数を設定します。デフォルトは 5 分です。
- **User Sessions**：1 ～ 5 のユーザーごとのセッションの最大数を設定します。デフォルトは 5 分です。

ステップ 3 [Apply] をクリックして、設定の変更を保存します。

システム管理者用 AAA の設定

この項では、システム管理者の認証、管理許可、コマンド許可を設定する方法について説明します。

管理認証の設定

CLI および ASDM アクセスの認証を設定します。

管理認証について

ASA へのログイン方法は、認証を有効にしているかどうかによって異なります。

SSH 認証の概要

認証ありまたは認証なしでの SSH アクセスについては、次の動作を参照してください。

- 認証なし：SSH は認証なしでは使用できません。
- 認証あり：SSH 認証を有効にした場合は、AAA サーバーまたはローカルユーザーデータベースに定義されているユーザー名とパスワードを入力します。公開キーの認証では、

ASA はローカル データベースのみをサポートします。 SSH 公開キー認証を設定した場合、ASA ではローカル データベースを暗黙的に使用します。ログインにユーザー名とパスワードを使用する場合に必要なのは、SSH認証を明示的に設定することのみです。ユーザー EXEC モードにアクセスします。

Telnet 認証の概要

認証の有無にかかわらず、Telnet アクセスについては、次の動作を参照してください。

- 認証なし：Telnet の認証を有効にしていない場合は、ユーザー名を入力しません。ログイン パスワードを入力します。デフォルトのパスワードはありません。したがって、ASA へ Telnet 接続するには、パスワードを設定する必要があります。ユーザー EXEC モードにアクセスします。
- 認証あり：Telnet認証を有効にした場合は、AAA サーバーまたはローカルユーザーデータベースに定義されているユーザー名とパスワードを入力します。ユーザー EXEC モードにアクセスします。

ASDM 認証の概要

認証ありまたは認証なしでのASDMアクセスに関しては、次の動作を参照してください。AAA認証の有無にかかわらず、証明書認証を設定することも可能です。

- 認証なし：デフォルトでは、ブランクのユーザー名と **enable password** コマンドを使用して ASDM にログインできます。空白のままにしないように、できるだけ早くイネーブル パスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定を参照してください。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDMにログインしたときには、この動作は適用されません。ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされることに注意してください。
- 証明書認証（シングル、ルーテッドモードのみ）：ユーザーに有効な証明書を要求できます。証明書のユーザー名とパスワードを入力すると、ASA が PKI トラストポイントに対して証明書を検証します。
- AAA 認証：ASDM（HTTPS）認証を有効にした場合は、AAA サーバーまたはローカル ユーザーデータベースに定義されているユーザー名とパスワードを入力します。これで、ブランクのユーザー名とイネーブル パスワードで ASDM を使用できなくなりました。
- AAA 認証と証明書認証の併用（シングル、ルーテッド モードのみ）：ASDM（HTTPS）認証を有効にした場合は、AAA サーバーまたはローカル ユーザー データベースに定義されているユーザー名とパスワードを入力します。証明書認証用のユーザー名とパスワードが異なる場合は、これらも入力するように求められます。ユーザー名を証明書から取得してあらかじめ入力しておくよう選択できます。

シリアル認証の概要

認証ありまたは認証なしでのシリアル コンソール ポートへのアクセスに関しては、次の動作を参照してください。

- 認証なし：シリアルアクセスの認証を有効にしていない場合は、ユーザー名、パスワードを入力しません。ユーザー EXEC モードにアクセスします。
- 認証あり：シリアルアクセスの認証を有効にした場合は、AAA サーバーまたはローカル ユーザーデータベースで定義されているユーザー名とパスワードを入力します。ユーザー EXEC モードにアクセスします。

enable 認証の概要

ログイン後に特権EXECモードに入るには、**enable**コマンドを入力します。このコマンドの動作は、認証がイネーブルかどうかによって異なります。

- 認証なし：enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力します。デフォルトは空白です。**enable** コマンドを最初に入力したときに、それを変更するように求められます。ただし、enable 認証を使用しない場合、**enable**コマンドを入力した後は、特定のユーザーとしてログインしていません。これにより、コマンド認可などユーザーベースの各機能が影響を受けることがあります。ユーザー名を維持するには、enable 認証を使用してください。
- 認証あり：enable 認証を設定した場合は、ASA はプロンプトにより AAA サーバーまたはローカルユーザーデータベースで定義されているユーザー名とパスワードを要求します。この機能は、ユーザーが入力できるコマンドを判別するためにユーザー名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカル データベースを使用する enable 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** コマンドによりユーザー名が維持されますが、認証をオンにするための設定は必要ありません。

⚠

注意 CLIにアクセスできるユーザーや特権EXECモードを開始できないようにするユーザーをローカルデータベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザーは、CLI で自分のパスワードを使用して特権EXECモード（およびすべてのコマンド）にアクセスできます。あるいは、認証処理でローカルデータベースではなく AAA サーバーを使用してログイン コマンドを回避するか、またはすべてのローカル ユーザーをレベル 1 に設定することにより、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザーを制御できます。

ホスト オペレーティング システムから ASA へのセッション

一部のプラットフォームでは、ASAの実行を別のアプリケーションとしてサポートしています（例：Firepower 4100/9300 の ASA）。ホスト オペレーティング システムから ASA へのセッションの場合、接続のタイプに応じてシリアルおよび Telnet 認証を設定できます。

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はこれらのセッションにも適用されます。この場合、管理コンテキストの AAA サーバーまたはローカル ユーザー データベースが使用されます。

CLI、ASDM、および enable コマンド アクセス認証の設定

始める前に

- Telnet、SSH、または HTTP アクセスを設定します。
- 外部認証の場合は、AAA サーバー グループを設定します。ローカル認証の場合は、ローカル データベースにユーザーを追加します。
- HTTP 管理認証では、AAA サーバー グループの SDI プロトコルをサポートしていません。
- この機能は、**ssh authentication** コマンドによるローカル ユーザー名に関する SSH 公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカル データベースを暗黙的に使用します。この機能は、ユーザー名とパスワードにのみ影響します。ローカル ユーザーが公開キー認証またはパスワードを使用できるようにするには、この手順を使用してローカル認証を明示的に設定し、パスワード アクセスを許可する必要があります。

手順

ステップ 1 **enable** コマンドを使用するユーザーを認証する場合は、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authentication]** の順に選択し、次の設定を行います。

a) [Enable] チェックボックスを選択します。
b) サーバー グループ名または LOCAL データベースを選択します。
c) （オプション）AAA サーバーを選択する場合は、AAA サーバーが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。

ステップ 2 CLI または ASDM にアクセスするユーザーを認証する場合は、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authentication]** の順に選択し、次の設定を行います。

a) 次のチェックボックスをオンにします（複数可）。
   - [HTTP/ASDM]：HTTPS を使用して ASA にアクセスする ASDM クライアントを認証します。
   - [Serial]：コンソール ポートを使用して ASA にアクセスするユーザーを認証します。

- **SSH**：SSH を使用して ASA にアクセスするユーザーを認証します（パスワードのみ。公開キー認証では暗黙のうちにローカル データベースが使用されます）。
- [Telnet]：Telnet を使用して ASA にアクセスするユーザーを認証します。

b) チェックボックスをオンにしたサービスごとに、サーバー グループ名または LOCAL データベースを選択します。

c) （オプション）AAA サーバーを選択する場合は、AAA サーバーが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。

ステップ 3 [Apply] をクリックします。

ASDM 証明書認証の構成

AAA 認証の有無にかかわらず証明書認証を必須にできます。ASA は証明書を PKI トラストポイントに照合して検証します。

始める前に

- シングルモードおよびルーテッドモードのみでサポートされています。
- クライアント証明書（.pfx 形式）およびサーバー証明書（.p12 形式）が必要です。証明書をインポートするための復号パスフレーズを記憶します。

手順

ステップ 1 ID 証明書を Cisco ASA に追加します。アイデンティティ証明書の追加またはインポートを参照してください。

ステップ 2 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** の順に選択します。

ステップ 3 [Specify the interface requires client certificate to access ASDM] 領域で [Add] をクリックし、インターフェイスとオプションで証明書マップを指定します。認証が成功するには、その証明書マップと一致している必要があります。

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。証明書マップを作成するには、**[Configuration]** > **[Site-to-Site VPN]** > **[Advanced]** > **[IPSec]** > **[Certificate to Connection Map]** > **[Rules]** を表示します。

ステップ 4 （任意） ASDM で証明書からユーザー名を抽出する際に使用する属性を設定するには、**[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Certificate Rule]** の順に選択します。

次の方法の中から 1 つを選択してください。

- [Specify the Certificate Fields to be used]：[Primary Field] ドロップダウン リストと [Secondary Field] ドロップダウン リストから値を選択します。
- **[Use the entire DN as the username]**
- [Use script to select username]：[Add] をクリックし、スクリプトの内容を追加します。

認証を求めるプロンプトにユーザー名を事前入力するには、[Prefill Username] チェックボックスをオンにします。そのユーザー名が最初に入力したものと異なる場合、最初のユーザー名が事前入力された新しいダイアログボックスが表示されます。そこに、認証用のパスワードを入力できます。

デフォルトでは、ASDM は CN OU 属性を使用します。

ステップ 5 [Apply] をクリックします。

ステップ 6 Windows ASDM Launcher の手順。

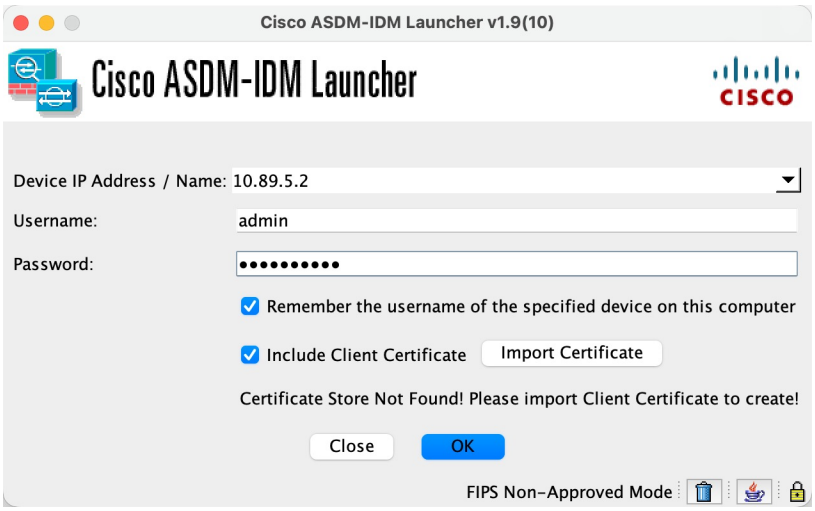
a) （FIPS 非承認モード）クライアント証明書をインストールします。

1. .pfx ファイルをダブルクリックして、証明書をインストールします。
2. 復号パスワードを入力します。

   Windows の証明書の詳細については、https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/working-with-certificates を参照してください。

b) ASDM Launcher を起動します。

図 6 : ASDM Launcher



c) [デバイスのIPアドレス（Device IP Address）]、[ユーザー名（Username）]および[パスワード（Password）] を入力します。
d) [クライアント証明書を含める（Include Client Certificate）] をオンにします。
e) （FIPS 承認モード）[証明書をインポート（Import Certificate）] をオンにして、.pfx 形式のクライアント証明書を参照します。パスワードを入力し、[OK] をクリックします。

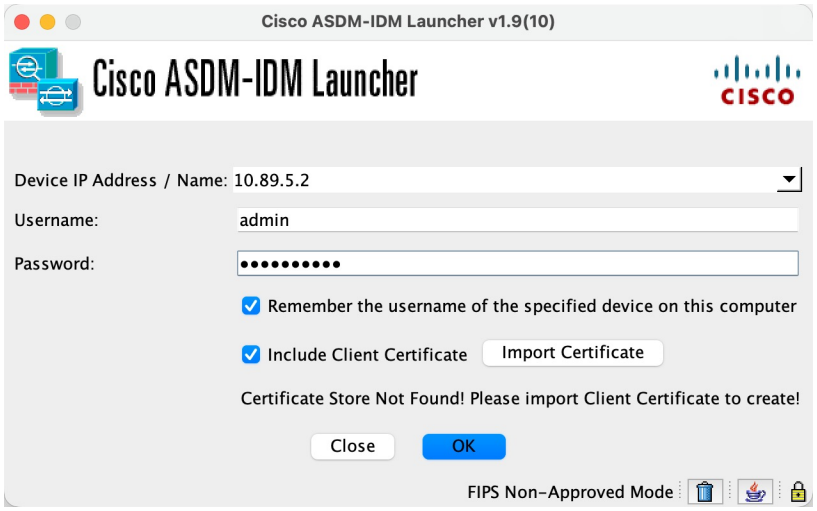
   Windows での FIPS 非承認モードでは、クライアント証明書は、Windows 証明書ストアで取得できます。また、[証明書をインポート（Import Certificate）] ボタンが表示されます。

f) （FIPS 承認モード）証明書を更新するには、[証明書を更新（Update Certificate）] ボタンをクリックして、新しい証明書をインポートします。

ステップ 7 MacOS ASDM Launcher の手順。

a) ASDM Launcher を起動します。

図 *7 : ASDM Launcher*



b) [デバイスのIPアドレス（Device IP Address）]、[ユーザー名（Username）]および[パスワード（Password）] を入力します。
c) [クライアント証明書を含める（Include Client Certificate）] をオンにします。
d) [証明書をインポート（Import Certificate）] をオンにして、.pfx 形式のクライアント証明書を参照します。パスワードを入力し、[OK] をクリックします。
e) 証明書を更新するには、[証明書を更新（Update Certificate）] ボタンをクリックして、新しい証明書をインポートします。

管理許可による CLI および ASDM アクセスの制限

ASA ではユーザーの認証時に管理アクセス ユーザーとリモート アクセス ユーザーを区別できるようになっています。ユーザー ロールを区別することで、リモート アクセス VPN ユーザーやネットワーク アクセス ユーザーが ASA に管理接続を確立するのを防ぐことができます。

SSH X.509 証明書の承認については、「X.509 証明書アクセス用の SSH の設定 （13 ページ）」を参照してください。

始める前に

RADIUS または LDAP（マッピング済み）ユーザー

ユーザーが LDAP 経由で認証されると、ネイティブ LDAP 属性とその値が Cisco ASA 属性にマッピングされ、特定の許可機能が提供されます。Cisco VSA CVPN3000-Privilege-Level の値を 0 ～ 15 の範囲で設定した後、LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。

RADIUS IETF の **service-type** 属性が、RADIUS 認証および許可要求の結果として access-accept メッセージで送信される場合、この属性は認証されたユーザーにどのタイプのサービスを付与するかを指定するために使用されます。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が access-accept メッセージで送信される場合は、ユーザーの権限レベルを指定するために使用されます。

TACACS+ ユーザー

「service=shell」で許可が要求され、サーバーは PASS または FAIL で応答します。

ローカル ユーザー

指定したユーザー名の [Access Restriction] オプションを設定します。アクセス制限のデフォルト値は [Full Access] です。この場合、[Authentication] タブのオプションで指定されたすべてのサービスに対して、フル アクセスが許可されます。

管理許可の属性

管理許可の AAA サーバー タイプおよび有効な値については、次の表を参照してください。ASA ではこれらの値を使用して管理アクセス レベルを決定します。

管理レベル	RADIUS/LDAP の（マッピングされた）属性	TACACS+ 属性	ローカル データベースの属性
[Full Access]： [Authentication] タブのオプションで指定されたすべてのサービスに対してフル アクセスが許可されます。	Service-Type 6（アドミニストレーティブ）、Privilege-Level 1	PASS、特権レベル 1	admin
[Partial Access]：**[Authentication]** タブのオプションで設定すると、CLI または ASDM に対するアクセスが許可されます。ただし、[Enable] オプションを使用して **enable** 認証を設定する場合、CLI y ユーザーは **enable** コマンドを使用して特権 EXEC モードにアクセスすることはできません。	Service-Type 7（NAS プロンプト）、Privilege-Level 2 以上 Framed (2) および Login (1) サービス タイプは同様に扱われます。	PASS、特権レベル 2 以上	nas-prompt

管理レベル	RADIUS/LDAP の（マッピングされた）属性	TACACS+ 属性	ローカル データベースの属性
[No Access]：管理アクセスが拒否されます。ユーザーは [Authentication] タブのオプションで指定されたいずれのサービスも使用できません（[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザーは、引き続き自身のリモート アクセス セッションを認証および終了できます。他のすべてのサービス タイプ（ボイス、ファクスなど）も同様に処理されます。	Service-Type 5（アウトバウンド）	FAIL	remote-access

その他のガイドライン

- シリアル コンソール アクセスは管理許可に含まれません。
- この機能を使用するには、管理アクセスに AAA 認証も設定する必要があります。CLI、ASDM、および enable コマンド アクセス認証の設定 （26 ページ）を参照してください。
- 外部認証を使用する場合は、この機能をイネーブルにする前に、AAA サーバー グループを設定しておく必要があります。
- HTTP 許可は、シングル ルーテッド モードでのみサポートされます。

手順

ステップ 1 HTTP セッションの管理許可をイネーブルにするには、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択し、[Enable Authorization for ASA Command Access] 領域の [HTTP] チェックボックスをオンにします。

（注）
ASA コマンド アクセスを設定するには、ローカル コマンド許可の設定 （34 ページ）を参照してください。

ステップ 2 Telnet および SSH セッションの管理許可をイネーブルにするには、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択し、[Perform authorization for exec shell access] 領域の [Enable] チェックボックスをオンにします。

ステップ 3 [Remote] または [Local] オプション ボタンを選択して、EXEC シェル アクセスの許可に使用するサーバーを指定します。

ステップ 4 管理認可をイネーブルにするには、[Allow privileged users to enter into EXEC mode on login] チェックボックスをオンにします。

[auto-enable] オプションを選択すると、フル アクセスが許可されたユーザーが直接特権 EXEC モードを開始できます。それ以外では、ユーザーはユーザー EXEC モードになります。

コマンド認可の設定

コマンドへのアクセスを制御する場合、ASA ではコマンド許可を設定でき、ユーザーが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザー EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバー特権レベル

コマンド認可について

コマンド認可を有効にし、承認済みのユーザーにのみコマンド入力を許容することができます。

サポートされるコマンド認可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA でコマンド特権レベルを設定します。ローカル ユーザー、RADIUS ユーザー、または LDAP ユーザー（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザーをローカルデータベース、RADIUS、または LDAP サーバーで定義されている特権レベルに所属させます。ユーザーは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザーは、初めてログインするときに、ユーザー EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザーは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル データベース内にユーザーが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可を有効にするまで使用されません。

- TACACS+ サーバー特権レベル：TACACS+ サーバーで、ユーザーまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザーが入力するすべてのコマンドは、TACACS+ サーバーで検証されます。

セキュリティ コンテキストとコマンド許可

AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

コマンド許可を設定する場合は、各セキュリティコンテキストを別々に設定する必要があります。この設定により、異なるセキュリティコンテキストに対して異なるコマンド許可を実行できます。

セキュリティコンテキストを切り替える場合、管理者は、ログイン時に指定したユーザー名で許可されるコマンドが新しいコンテキストセッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティコンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。

（注） システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

コマンド権限レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは特権レベル 15 に割り当てられます。

- **show checksum**
- **show curpriv**
- イネーブル化
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、configure コマンドも同じレベルに移動してください。このようにしないと、ユーザーはコンフィギュレーション モードに入ることができません。

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザーを特定の特権レベルに定義でき、各ユーザーは割り当てられた特権レベル以下のコマンドを入力できます。ASA は、ローカル データベース、RADIUS サーバー、または LDAP サーバー（LDAP 属性を RADIUS 属性にマッピングする場合）に定義されているユーザー特権レベルをサポートしています。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択します。

ステップ 2 **[Enable authorization for ASA command access]** > **[Enable]** チェック ボックスをオンにします。

ステップ 3 [Server Group] ドロップダウン リストから [LOCAL] を選択します。

ステップ 4 ローカル コマンド許可をイネーブルにすると、オプションで、特権レベルを個々のコマンドまたはコマンド グループに手動で割り当てたり、事前定義済みユーザー アカウント特権をイネーブルにしたりできます。

- 事前定義のユーザー アカウント特権を使用するには、[Set ASDM Defined User Roles] をクリックします。

  [ASDM Defined User Roles Setup] ダイアログボックスが表示されます。[Yes] をクリックすると、事前定義済みユーザー アカウント特権を使用できるようになります。事前定義済みユーザー アカウント特権には、[Admin]（特権レベル 15、すべての CLI コマンドへのフル アクセス権）、[Read Only]（特権レベル 5、読み取り専用アクセス権）、[Monitor Only]（特権レベル 3、[Monitoring] セクションへのアクセス権のみ）があります。

- コマンド レベルを手動で設定するには、[Configure Command Privileges] をクリックします。

  [Command Privileges Setup] ダイアログボックスが表示されます。[Command Mode] ドロップダウン リストから [All Modes] を選択すると、すべてのコマンドを表示できます。代わりに、コンフィギュレーション モードを選択し、そのモードで使用可能なコマンドを表示することもできます。たとえば、[context] を選択すると、コンテキスト コンフィギュレーション モードで使用可能なすべてのコマンドを表示できます。コンフィギュレーション モードだけでなく、ユーザー EXEC モードや特権 EXEC モードでも入力が可能で、かつモードごとに異なるアクションが実行されるようなコマンドを使用する場合は、これらのモードに対して別個に特権レベルを設定できます。

  [Variant] カラムには、[show]、[clear]、または [cmd] が表示されます。特権は、コマンドの show 形式、clear 形式、または configure 形式に対してのみ設定できます。コマンドの

configure 形式は、通常、未修正コマンド（show または clear プレフィックスなしで）または no 形式として、コンフィギュレーションの変更を引き起こす形式です。

コマンドのレベルを変更する場合は、コマンドをダブルクリックするか、[Edit] をクリックします。レベルは 0 ～ 15 の範囲で設定できます。設定できるのは、main コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

表示されているすべてのコマンドのレベルを変更する場合は、[Select All] をクリックした後に、[Edit] をクリックします。

[OK] をクリックして変更内容を確定します。

ステップ 5 （任意） **[Perform authorization for exec shell access]** > **[Enable]** チェック ボックスをオンにして、コマンド認可のための AAA ユーザーを有効にします。このオプションを入力しない場合、ASA は、ローカル データベース ユーザの特権レベルだけをサポートし、他のタイプのユーザをすべてデフォルトでレベル 15 に割り当てます。

さらに、このコマンドは管理認証を有効にします。管理許可による CLI および ASDM アクセスの制限 （29 ページ）を参照してください。

ステップ 6 [Apply] をクリックします。

許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

TACACS+ サーバーでのコマンドの設定

グループまたは個々のユーザーの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバーでコマンドを設定できます。サードパーティの TACACS+ サーバーの場合は、コマンド許可サポートの詳細については、ご使用のサーバーのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- ASA は、シェル コマンドとして許可するコマンドを送信し、TACACS+ サーバーでシェル コマンドとしてコマンドを設定します。

（注） Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプは ASA コマンド許可に使用しないでください。

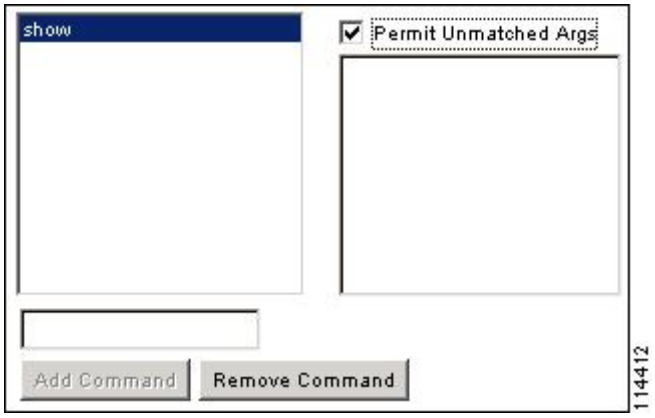
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンドフィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスをオンにすると、明示的に拒否していないすべてのコマンド引数を許可できます。

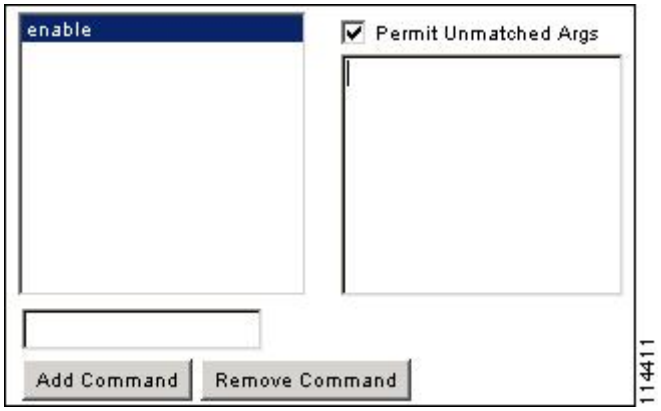
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（次の図を参照）。

  図 *8*：関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する必要があります（次の図を参照）。

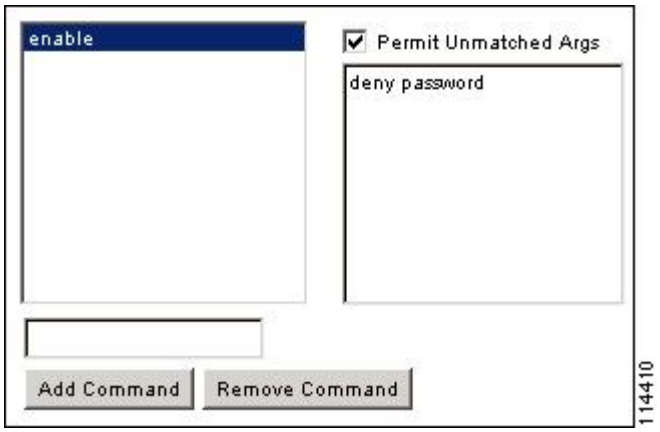
  図 *9*：単一ワードのコマンドの許可



- 引数を拒否するには、その引数の前に **deny** を入力します。

  たとえば、**enable** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンドフィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスをオンにしてください（次の図を参照）。

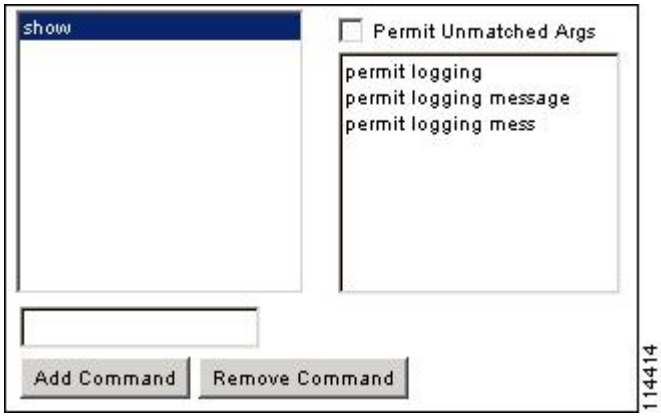
図 *10* : 引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、ASA はプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバーに送信します。

  たとえば、**sh log** と入力すると、ASA は完全なコマンド **show logging** を TACACS+ サーバーに送信します。一方、**sh log mess** と入力すると、ASA は展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバーに送信します。省略形を予想して同じ引数の複数のスペルを設定できます（次の図を参照）。

図 *11* : 省略形の指定



- すべてのユーザーに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **イネーブル化**
  - **help**
  - **show history**
  - **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

TACACS+ コマンド許可の設定

TACACS+ コマンド認可をイネーブルにし、ユーザーが CLI でコマンドを入力すると、ASA はそのコマンドとユーザー名を TACACS+ サーバーに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバーで定義されたユーザーとして ASA にログインしていること、および ASA の設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザーとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

意図したとおりに機能することが確認できるまで、設定を保存しないでください。間違いによりロックアウトされた場合、通常はASAを再始動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバー システムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバー プールに、インターフェイス 1 に接続された 1 つのサーバーとインターフェイス 2 に接続された別のサーバーを含めます。TACACS+ サーバーが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。

TACACS+ サーバーを使用したコマンド許可を設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択します。

ステップ 2 **[Enable authorization for command access]** > **[Enable]** チェックボックスをオンにします。

ステップ 3 [Server Group] ドロップダウン リストから AAA サーバー グループ名を選択します。

ステップ 4 （オプション）AAA サーバーが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。設定するには、[Use LOCAL when server group fails] チェックボックスをオンにします。ローカルデータベースではAAA サーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASAのプロンプトでは、どの方式が使用されているかが示されないためです。必ずローカルデータベースのユーザーとコマンド特権レベルを設定してください。

ステップ 5 [Apply] をクリックします。

コマンド許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

ローカル データベース ユーザーのパスワード ポリシーの設定

ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。

パスワード ポリシーはローカル データベースを使用する管理ユーザーに対してのみ適用されます。ローカルデータベースを使用するその他のタイプのトラフィック（VPN や AAA によるネットワーク アクセスなど）や、AAA サーバーによって認証されたユーザーには適用されません。

パスワードポリシーの設定後は、自分または別のユーザーのパスワードを変更すると、新しいパスワードに対してパスワードポリシーが適用されます。既存のパスワードについては、現行のポリシーが適用されます。新しいポリシーは、[User Accounts] ペインおよび [Change My Password] ペインを使用したパスワードの変更に適用されます。

始める前に

- ローカルデータベースを使用して CLI または ASDM アクセスの AAA 認証を設定します。
- ローカル データベース内にユーザー名を指定します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Password Policy]** の順に選択します。

ステップ 2 次のオプションを任意に組み合わせて設定します。

- [Minimum Password Length]：パスワードの最小長を入力します。有効値の範囲は 3 ～ 64 文字です。推奨されるパスワードの最小長は 8 文字です。
- [Lifetime]：リモート ユーザー（SSH、Telnet、HTTP）のパスワードの有効期間を日数で指定します。コンソール ポートのユーザーが、パスワードの有効期限切れでロックされることはありません。有効な値は、0 ～ 65536 です。デフォルト値は 0 日です。この場合、パスワードは決して期限切れになりません。

  パスワードの有効期限が切れる 7 日前に、警告メッセージが表示されます。パスワードの有効期限が切れると、リモート ユーザーのシステム アクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。

  - 他の管理者にパスワードを変更してもらいます。

- 物理コンソール ポートにログインして、パスワードを変更します。

- [Minimum Number Of]：次のタイプの最短文字数を指定します。
  - [Numeric Characters]：パスワードに含めなければならない数字の最小文字数を入力します。有効な値は、0 ～ 64 文字です。デフォルト値は 0 です
  - [Lower Case Characters]：パスワードに含めなければならない小文字の最小文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  - [Upper Case Characters]：パスワードに含めなければならない大文字の最小文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  - [Special Characters]：パスワードに含めなければならない特殊文字の最小文字数を入力します。有効値の範囲は 0 ～ 64 文字です。特殊文字には、!、@、#、$、%、^、&、*、(および) が含まれます。デフォルト値は 0 です。
  - [Different Characters from Previous Password]：新しいパスワードと古いパスワードで変えなければならない最小文字数を入力します。有効な値は、0～64 文字です。デフォルト値は 0 です文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

- [Enable Reuse Interval]：以前に使用された 2 ～ 7 個のパスワードと一致するパスワードの再利用を禁止することができます。以前のパスワードは、**password-history** コマンドを使用して、暗号化された形で各ユーザー名の設定に保存されます。このコマンドをユーザーが設定することはできません。

- [Prevent Passwords from Matching Usernames]：ユーザー名と一致するパスワードを禁止します。

ステップ 3 （オプション）[Enable Password and Account Protection] チェックボックスをオンにして、ユーザーが [User Accounts] ペインではなく、[Change My Password] ペインでパスワードを変更することを要件とします。デフォルト設定はディセーブルです。どちらの方法でも、ユーザーはパスワードを変更することができます。

この機能をイネーブルにして、[User Accounts] ペインでパスワードを変更しようとすると、次のエラー メッセージが表示されます。

```
ERROR: Changing your own password is prohibited
```

ステップ 4 [Apply] をクリックして、設定内容を保存します。

パスワードの変更

パスワードポリシーでパスワードの有効期間を設定した場合、有効期間を過ぎるとパスワードを新しいパスワードに変更する必要があります。パスワードポリシー認証をイネーブルにした

場合は、このパスワード変更のスキームが必須です。パスワードポリシー認証がイネーブルでない場合は、このメソッドを使用することも、直接ユーザーアカウントを変更することもできます。

username パスワードを変更するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Change Password]** の順に選択します。
ステップ 2 古いパスワードを入力します。
ステップ 3 新しいパスワードを入力します。
ステップ 4 確認のために新しいパスワードを再度入力します。
ステップ 5 [Make Change] をクリックします。
ステップ 6 [Save] アイコンをクリックして、実行コンフィギュレーションに変更を保存します。

ログインの履歴を有効にして表示する

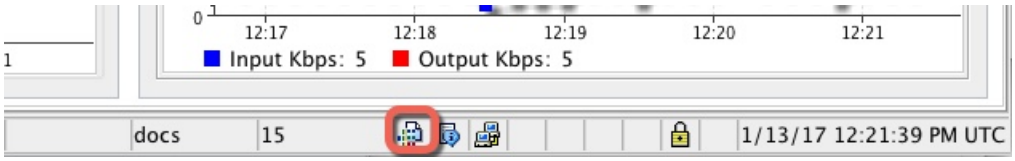
デフォルトでは、ログイン履歴は 90 日間保存されます。この機能を無効にするか、期間を最大 365 日まで変更できます。

始める前に

- ログイン履歴はユニット（装置）ごとに保存されます。フェールオーバーおよびクラスタリング環境では、各ユニットが自身のログイン履歴のみを保持します。
- ログインの履歴データは、リロードされると保持されなくなります。
- 1 つ以上の CLI 管理方式（SSH、Telnet、シリアル コンソール）でローカル AAA 認証をイネーブルにした場合、AAA サーバーのユーザー名またはローカルデータベースのユーザー名にこの機能が適用されます。ASDM のログインは履歴に保存されません。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Login History]** の順に選択します。
ステップ 2 [管理者のログイン履歴レポート設定]チェックボックスをオンにします。この機能は、デフォルトでイネーブルにされています。
ステップ 3 [期間] を 1 ～ 365 日の間で設定します。デフォルトは 90 です。
ステップ 4 ログイン履歴を表示するには、いずれかの ASDM 画面で [Status] バーにある [Login History] アイコンをクリックします。



すべてのユーザーのログイン履歴がダイアログボックスに表示されます。

管理アクセス アカウンティングの設定

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバーに送信できます。ユーザーがログインするとき、ユーザーが **enable** コマンドを入力するとき、またはユーザーがコマンドを発行するときのアカウンティングを設定できます。

コマンド アカウンティングに使用できるサーバーは、TACACS+ だけです。

管理アクセスおよびイネーブル コマンド アカウンティングを設定するには、次の手順を実行します。

手順

ステップ 1 **enable** コマンドを入力したユーザーのアカウンティングを有効にするには、次の手順を実行します。

a) **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Accounting]** の順に選択し、**[Require accounting to allow accounting of user activity]** > **[Enable]** チェックボックスをオンにします。

b) RADIUS または TACACS+ サーバー グループ名を選択します。

ステップ 2 ユーザーが Telnet、SSH、またはシリアル コンソールを使用して ASA にアクセスした場合にそのユーザーのアカウンティングを有効化するには、次の手順を実行します。

a) [Require accounting for the following types of connections] 領域で、[Serial]、[SSH]、または [Telnet] チェックボックスをオンにします。

b) 各接続タイプの RADIUS または TACACS+ サーバー グループ名を選択します。

ステップ 3 コマンド アカウンティングを設定するには、次の手順を実行します。

a) [Require accounting for the following types of connections] エリアで [Enable] チェックボックスをオンにします。

b) TACACS+ サーバー グループ名を選択します。RADIUS はサポートされていません。

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバーに送信できます。

c) [Command Privilege Setup] ダイアログボックスを使用してコマンド特権レベルをカスタマイズする際、[Privilege level] ドロップダウン リストで最小特権レベルを指定することで、

ASA のアカウンティング対象となるコマンドを制限できます。最小特権レベルよりも下のコマンドは、ASA で処理の対象となりません。

ステップ 4 [Apply] をクリックします。

アカウンティング設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

ロックアウトからの回復

状況によっては、コマンド許可やCLI認証をオンにすると、ASA CLIからロックアウトされる場合があります。通常は、ASAを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。

次の表に、一般的なロックアウト条件とその回復方法を示します。

表 *1 : CLI* 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベースにユーザーが設定していない。	ローカル データベース内にユーザーが存在しない場合は、ログインできず、ユーザーの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからASAへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザーを追加することができます。

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバーがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバーが到達不能である場合は、ログインもコマンドの入力もできません。	1. ログインし、パスワードと AAA コマンドをリセットします。 2. サーバーがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	1. ASA でネットワーク コンフィギュレーションが正しくないためにサーバーが到達不能である場合は、スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 2. サーバーがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。
TACACS+ コマンド許可	十分な特権のないユーザーまたは存在しないユーザーとしてログインした。	コマンド許可がイネーブルになりますが、ユーザーはこれ以上コマンドを入力できなくなります。	TACACS+ サーバーのユーザーアカウントを修正します。 TACACS+ サーバーへのアクセス権がなく、ASA をすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。
ローカル コマンド許可	十分な特権のないユーザーとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザーはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザー レベルを変更することができます。

デバイス アクセスのモニタリング

- **[Monitoring] > [Properties] > [Device Access] > [ASDM/HTTPS/Telnet/SSH Sessions]**

  上部ペインには、ASDM、HTTPS、および Telnet のセッションを介して接続するユーザーの接続タイプ、セッション ID、および IP アドレスが示されます。特定のセッションを切断するには、[Disconnect] をクリックします。

  下部ペインには、クライアント、ユーザー名、接続ステータス、ソフトウェア バージョン、入力暗号化タイプ、出力暗号化タイプ、入力 HMAC、出力 HMAC、SSH セッション ID、残りのキー再生成データ、残りのキー再生成時間、データベースのキー再生成、時間ベースのキー再生成、最後のキー再生成の時間が表示されます。特定のセッションを切断するには、[Disconnect] をクリックします。

- **[Monitoring] > [Properties] > [Device Access] > [Authenticated Users]**

  このペインには、AAA サーバーによって認証されたユーザーのユーザー名、IP アドレス、ダイナミック ACL、非活動タイムアウト（存在する場合）、および絶対タイムアウトが一覧表示されます。

- **[Monitoring] > [Properties] > [Device Access] > [AAA Locked Out Users]**

  このペインには、ロックアウトされた AAA ローカル ユーザーのユーザー名、失敗した認証の試行回数、およびユーザーがロックアウトされた回数が一覧表示されます。ロックアウトされた特定のユーザーをクリアするには、[Clear Selected Lockout] をクリックします。ロックアウトされたすべてのユーザーをクリアするには、[Clear All Lockouts] をクリックします。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

管理アクセスの履歴

表 *2:* 管理アクセスの履歴

機能名	プラットフォームリリース	説明
SSH X.509 証明書認証	9.20(4)/9.24(1)	X.509v3 証明書を使用して SSH のユーザーを認証できるようになりました（RFC 6187）。 （注） この機能は、将来の FXOS リリースの Firepower 4100/9300 でサポートされる予定です。 （注） ASDM 7.20(4) のバンドルバージョンには、この機能のサポートは含まれていません。機能をサポートするには、Cisco.com から ASDM 7.20(4) をダウンロードしてインストールしてください。バンドルバージョンを上書きする場合は、必ずイメージ名を asdm.bin に変更してください。 新しい/変更された画面： • **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAアクセス（AAA Access）] > [承認（Authorization）]** • **[設定（Configuration）] > [デバイス管理（Device Management）] > [証明書管理（Certificate Management）] > [CA証明書（CA Certificates）] > [トラストポイントの追加/編集（Add/Edit Trustpoint）] > [詳細設定（Advanced）]** • **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]**

機能名	プラットフォームリリース	説明
ASDM 証明書認証	9.24(1)	ASDM 7.24 に付属している ASDM ランチャー 1.9(10) では、ユーザー証明書認証がサポートされるようになりました。以前は、この機能は Java Web Start でのみサポートされていました（7.18 で廃止）。ASA コマンドが 9.18 で廃止されていないため、ASDM ランチャー 1.9(10) を含む ASDM バージョンを使用する場合は証明書認証を使用するように以前の ASA バージョンを設定できます。 新規/変更された画面： • ASDM ランチャーのログインウィンドウ。 • [**Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**] • [**Configuration** > **Site-to-Site VPN** > **Advanced** > **IPSec** > **Certificate to Connection Map** > **Rules**] • [**Configuration** > **Device Management** > **Management Access** > **HTTP Certificate Rule**]
AES-256-GCM SSH 暗号	9.20(4)/9.24(1)	ASA は、SSH の AES-256-GCM 暗号をサポートしています。デフォルトでは、暗号化レベル [すべて（all）] と [高（high）] で有効になっています。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [詳細設定（Advanced）] > [SSH暗号（SSH Ciphers）]**
Message-of-the-day (motd) バナーにフェールオーバー状態と最後のフェールオーバー時刻を表示	/9.24(1)	フェールオーバーを使用する場合、message-of-the-day (motd) バナーを設定すると、ログインしているユニットのフェールオーバー状態と最後のフェールオーバー時刻に関する情報がバナーに表示されます。この情報は、CLI で障害対応などのアクションを実行しており、セッション間でフェールオーバーが発生する場合に役立ちます。 新規または変更された画面： **[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner]** *9.24(1)* でも同様です。

機能名	プラットフォームリリース	説明
Cisco ASA SSH スタックが廃止されました	9.23(1)	Cisco ASA SSH スタックを使用できなくなりました。Cisco SSH スタックが唯一のスタックになりました。 新しい/変更された画面： • シングルコンテキストモード：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • マルチコンテキストモード：**[Configuration]** > **[Device Management]** > **[SSH Stack]**
CiscoSSH スタックのデフォルト化	9.19(1)	Cisco SSH スタックがデフォルトで使用されるようになりました。 新しい/変更された画面： • シングルコンテキストモード：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • マルチコンテキストモード：**[Configuration]** > **[Device Management]** > **[SSH Stack]**
SSH と Telnet のループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、次の機能に使用できるようになりました。 • SSH • Telnet 新規/変更されたコマンド：**interface loopback**、**ssh**、**telnet** 新規/変更された画面：[設定（Configuration）]>[デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [ループバックインターフェイスの追加（Add Loopback Interface）] ASDM サポートは 7.19 で追加されました。

機能名	プラットフォームリリース	説明
CiscoSSH スタック	9.17(1)	ASA は、SSH 接続に独自の SSH スタックを使用します。代わりに、OpenSSH に基づく CiscoSSH スタックを使用するように選択できるようになりました。デフォルトスタックは引き続き ASA スタックです。Cisco SSH は次をサポートします。 • FIPS の準拠性 • シスコおよびオープンソースコミュニティからの更新を含む定期的な更新 CiscoSSH スタックは次をサポートしないことに注意してください。 • VPN を介した別のインターフェイスへの SSH（管理アクセス） • EdDSA キーペア • FIPS モードの RSA キーペア これらの機能が必要な場合は、引き続き ASA SSH スタックを使用する必要があります。 CiscoSSH スタックでは、SCP 機能に若干の変更があります。ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、ASA で SCP サーバサブネット/ホストの SSH アクセスを有効にする必要があります。 新しい/変更された画面： • シングルコンテキストモード：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • マルチコンテキストモード：**[Configuration]** > **[Device Management]** > **[SSH Stack]**

機能名	プラットフォームリリース	説明
ローカルユーザーのロックアウトの変更	9.17(1)	設定可能な回数のログイン試行に失敗すると、ASA はローカルユーザーをロックアウトする場合があります。この機能は、特権レベル 15 のユーザーには適用されませんでした。また、管理者がアカウントのロックを解除するまで、ユーザーは無期限にロックアウトされます。管理者がその前に **clear aaa local user lockout** コマンドを使用しない限り、ユーザーは 10 分後にロック解除されるようになりました。特権レベル 15 のユーザーも、ロックアウト設定が適用されるようになりました。 新規/変更されたコマンド：**aaa local authentication attempts max-fail** 、**show aaa local user**
SSH および Telnet パスワード変更プロンプト	9.17(1)	ローカルユーザーが SSH または Telnet を使用して ASA に初めてログインすると、パスワードを変更するように求められます。また、管理者がパスワードを変更した後、最初のログインに対してもプロンプトが表示されます。ただし、ASA がリロードすると、最初のログインであっても、ユーザーにプロンプトは表示されません。 VPN などのローカル ユーザー データベースを使用するサービスは、SSH または Telnet ログイン中に変更された場合、新しいパスワードも使用する必要があることに注意してください。 新規/変更されたコマンド： **show aaa local user**

機能名	プラットフォームリリース	説明
SSH セキュリティの改善	9.16(1)	SSH が次の SSH セキュリティの改善をサポートするようになりました。 • ホストキーの形式：**crypto key generate** {**eddsa** | **ecdsa**}。RSA に加えて、EdDSA および ECDSA ホストキーのサポートが追加されました。ASA は、存在する場合、EdDSA、ECDSA、RSA の順にキーの使用を試みます。**ssh key-exchange hostkey rsa** コマンドで RSA キーを使用するように ASA を明示的に設定する場合は、2048 ビット以上のキーを生成する必要があります。アップグレードの互換性のために、ASA はデフォルトのホストキー設定が使用されている場合にのみ、より小さい RSA ホストキーを使用します。RSA のサポートは今後のリリースで削除されます。 • キー交換アルゴリズム：**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 暗号化アルゴリズム：**ssh cipher encryption chacha20-poly1305@openssh.com** • SSH バージョン 1 はサポートされなくなりました。**ssh version** コマンドは削除されました。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • **[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]** • **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
SNMP 向け管理アクセス	9.14(2)	サイト間 VPN 経由のセキュアな SNMP ポーリングを実現するための VPN 設定の一環として、VPN トンネル経由の管理アクセスを設定する際に、外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。

機能名	プラットフォームリリース	説明
HTTPS アイドルタイムアウトの設定	9.14(1)	ASDM、WebVPN、および他のクライアントを含む、ASA へのすべての HTTPS 接続のアイドルタイムアウトを設定できるようになりました。これまでは、**http server idle-timeout** コマンドを使用して ASDM アイドルタイムアウトを設定することしかできませんでした。両方のタイムアウトを設定した場合は、新しいコマンドによる設定が優先されます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** > **[HTTP Settings]** > **[Connection Idle Timeout]** チェックボックス。
事前定義されたリストに応じて最も高いセキュリティから最も低いセキュリティへという順序でSSH暗号化の暗号を表示	9.13(1)	事前定義されたリストに応じて、SSH暗号化の暗号が最も高いセキュリティから最も低いセキュリティへという順序（中または高）で表示されるようになりました。以前のリリースでは、最も低いものから最も高いものへの順序でリストされており、セキュリティが高い暗号よりも低い暗号が先に表示されていました。 新しい/変更された画面： **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
SSH キー交換モードの設定は、管理コンテキストに限定されています。	9.12(2)	管理コンテキストではSSHキー交換を設定する必要があります。この設定は、他のすべてのコンテキストによって継承されます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** > **[SSH Settings]** > **[DH Key Exchange]**
enable ログイン時のパスワードの変更が必須に	9.12(1)	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 文字以上の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドは現在サポートされていません。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザー）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブル パスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDMのデフォルトでは、ユーザー名を使用せず **enable** パスワードを使用してログインすることができます。 変更された画面はありません。

機能名	プラットフォームリリース	説明
管理セッションの設定可能な制限	9.12(1)	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードではHTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または16以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Session Quota]**
管理権限レベルの変更通知	9.12(1)	有効なアクセス（**aaa authentication enable console**）を認証するか、または特権 EXEC への直接アクセス（**aaa authorization exec auto-enable**）を許可すると、前回のログイン以降に割り当てられたアクセス レベルが変更された場合に ASA からユーザーへ通知されるようになりました。 新しい/変更された画面： [Status] バー > [Login History] アイコン
SSH によるセキュリティの強化	9.12(1)	次の SSH セキュリティの改善を参照してください。 • Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルトになりました。以前のデフォルトはGroup 1 SHA1 でした。 • HMAC-SHA256整合性暗号のサポート。デフォルトは、高セキュリティの暗号セット（hmac-sha2-256 のみ）になりました。以前のデフォルトは中程度のセットでした。 新規/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**

機能名	プラットフォームリリース	説明
非ブラウザベースの HTTPS クライアントによる ASA へのアクセスの許可	9.12(1)	非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。 新規/変更された画面： **[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Non-Browser Client Support]**
RSA キーペアは 3072 ビット キーをサポートしています	9.9(2)	モジュラス サイズを 3072 に設定できるようになりました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]**
ブリッジ型仮想インターフェイス（BVI）の VPN 管理アクセス	9.9(2)	VPN の **management-access** がその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で有効にできるようになりました。非 VPN 管理アクセスの場合は、ブリッジ グループ メンバ インターフェイスでこれらのサービスの設定を続行する必要があります。 新規または変更されたコマンド：**https**、**telnet**、**ssh**、**management-access**
SSH バージョン 1 の廃止	9.9(1)	SSH バージョン 1 は廃止され、今後のリリースで削除される予定です。デフォルト設定が SSH v1 と v2 の両方から SSH v2 のみに変更されました。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]**

機能名	プラットフォームリリース	説明
SSH公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(3)/9.8(1)	9.6(2) より前のリリースでは、ローカル ユーザー データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザーに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 変更された画面はありません。
ログイン履歴	9.8(1)	デフォルトでは、ログイン履歴は 90 日間保存されます。この機能を無効にするか、期間を最大 365 日まで変更できます。1 つ以上の管理メソッド（SSH、ASDM、Telnet など）でローカル AAA 認証を有効にしている場合、この機能はローカル データベースのユーザー名にのみ適用されます。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Login History]**
パスワードの再利用とユーザー名と一致するパスワードの使用を禁止するパスワード ポリシーの適用	9.8(1)	最大 7 世代にわたるパスワードの再利用と、ユーザー名と一致するパスワードの使用を禁止できるようになりました。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Password Policy]**
ASDM に対する ASA SSL サーバー モード マッチング	9.6(2)	証明書マップと照合するために、証明書で認証を行う ASDM ユーザーに対して証明書を要求できるようになりました。 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]**

機能名	プラットフォームリリース	説明
SSH 公開キー認証の改善	9.6(2)	以前のリリースでは、ローカル ユーザー データベース（）を使用して AAA SSH 認証を有効にしなくても、SSH 公開キー認証（）を有効にすることができました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザーが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザー名を作成できるようになりました。 次の画面が変更されました。 **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account]**
ASDM 管理認証	9.4(1)	HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定できるようになりました。 次の画面が変更されました。**[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAアクセス（AAA Access）] > [認証（Authorization）]**
証明書コンフィギュレーションの ASDM ユーザー名	9.4(1)	ASDM の証明書認証を有効にすると、ASDM が証明書からユーザー名を抽出する方法を設定できます。また、ログイン プロンプトでユーザー名を事前に入力して表示できます。 次の画面が導入されました。**[Configuration] > [Device Management] > [Management Access] > [HTTP Certificate Rule]**
改善されたワンタイムパスワード認証	9.2(1)	十分な認可特権を持つ管理者は、認証クレデンシャルを一度入力すると特権 EXEC モードに移行できます。**auto-enable** オプションが **aaa authorization exec** コマンドに追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]。
HTTP リダイレクトの IPv6 サポート	9.1(7)/9.6(1)	ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6 アドレスへ送信されるトラフィックもリダイレクトできるようになりました。 次の画面に機能が追加されました。**[Configuration] > [Device Management] > [HTTP Redirect]**

機能名	プラットフォームリリース	説明
設定可能なSSH暗号機能と整合性アルゴリズム	9.1(7.4)、9.3(3)、9.6(1)	ユーザーはSSH暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対してHMACと暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASAは3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctrの順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbcなどの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc**を使用します。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
SSHのAES-CTR暗号化	9.1(2)	ASAでのSSHサーバーの実装が、AES-CTRモードの暗号化をサポートするようになりました。
SSHキー再生成間隔の改善	9.1(2)	SSH接続は、接続時間60分間またはデータ トラフィック1 GBごとに再生成されます。 。
マルチコンテキストモードのASASMにおいて、スイッチからのTelnet認証および仮想コンソール認証をサポートしました。	8.5(1)	マルチ コンテキスト モードのスイッチからASASMへの接続はシステム実行スペースに接続しますが、これらの接続を制御するために管理コンテキストでの認証を設定できます。
ローカルデータベースを使用する場合の管理者パスワードポリシーのサポート	8.4(4.1)、9.1(2)	ローカル データベースを使用してCLIまたはASDMアクセスの認証を設定する場合は、指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。 次の画面が導入されました。[Configuration] > [Device Management] > [Users/AAA] > [Password Policy]。

機能名	プラットフォームリリース	説明
SSH 公開キー認証のサポート	8.4(4.1)、9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザー単位で有効にできます。公開キーファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication][Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。 *PKF* キー形式のサポートは *9.1(2)* 以降のみです。
SSH キー交換の Diffie-Hellman グループ 14 のサポート	8.4(4.1)、9.1(2)	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。
管理セッションの最大数のサポート	8.4(4.1)、9.1(2)	同時 ASDM、SSH、Telnet セッションの最大数を設定できます。 次の画面が導入されました。[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]。
SSH セキュリティが向上し、SSH デフォルトユーザー名はサポートされなくなりました。	8.4(2)	8.4(2) 以降、pix または asa ユーザー名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカルユーザーを定義する必要があります。定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバーを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

機能名	プラットフォームリリース	説明
管理アクセス	7.0(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] > [Management Access] > [ASDM/HTTPS/Telnet/SSH][Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner][Configuration] > [Device Management] > [Management Access] > [CLI PromptConfiguration] > [Device Management] > [Management Access] > [ICMP][Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client][Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server][Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Accounting]。

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。

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。