CHAPTER 17

管理アクセスの設定

この章では、Telnet、SSH、および HTTPS（ASDM を使用）を介したシステム管理のために ASA 1000V にアクセスする方法、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。

この章は、次の項で構成されています。

（注） また、管理アクセス用の ASA 1000V インターフェイスにアクセスする場合は、ホスト IP アドレスを許可するアクセスリストは不要です。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。

ASDM、Telnet、または SSH の ASA 1000V アクセスの設定

この項では、ASDM、Telnet、または SSH を使用した ASA 1000V へのアクセスをクライアントに許可する方法について説明します。次の項目を取り上げます。

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。

- IPSec サイトツーサイト 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。
- ASA 1000V 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、IPsec サイトツーサイト接続を介した場合のみです。「IPsec サイトツーサイト トンネル上の管理アクセスの設定」（P.17-10）を参照してください。
- ASA 1000V では、以下のことが可能です。
  - 最大 5 つの同時 Telnet 接続。
  - 最大 5 つの同時 SSH 接続。
  - 最大 5 つの同時 ASDM インスタンス。
- ASA 1000V は SSH バージョン 1 および 2 で提供されている SSH リモート シェル機能をサポートし、DES 暗号および 3DES 暗号をサポートします。
- SSL および SSH での XML 管理はサポートされていません。
- SSH デフォルト ユーザ名はサポートされなくなりました。**pix** または **asa** ユーザ名とログイン 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** コマンドを使用して AAA 認証を設定し、**username** コマンドを入力してローカル ユーザを定義する必要があります。ローカル データベースの代わりに AAA サーバ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。

Telnet アクセスの設定

クライアント IP アドレスを、ASA 1000V に Telnet を使用して接続できるよう指定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ1	**telnet** *source_IP_address mask source_interface* **例：** `hostname(config)# telnet 192.168.1.2 255.255.255.255 inside`	アドレスまたはサブネットごとに、ASA 1000V が接続を許可する IP アドレスを指定します。 インターフェイスが 1 つしかない場合は、インターフェイスのセキュリティ レベルが 100 である限り、そのインターフェイスにアクセスするように Telnet を設定することができます。
ステップ2	**telnet timeout** *minutes* **例：** `hostname(config)# telnet timeout 30`	（任意）ASA 1000V がセッションを切断するまでに Telnet セッションがアイドル状態を維持する時間の長さを設定します。 タイムアウトは 1 ～ 1440 分に設定します。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。

例

次の例は、アドレスが 192.168.1.2 の内部インターフェイスのホストで ASA 1000V にアクセスする方法を示しています。

```
hostname(config)# telnet 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASA 1000V にアクセスできるようにする方法を示しています。

```
hostname(config)# telnet 192.168.3.0 255.255.255.0 inside
```

Telnet クライアントの使用

ASA 1000V CLI に Telnet を使用してアクセスするには、**password** コマンドで設定したログイン パスワードを入力します。Telnet 認証を設定している場合（「CLI および ASDM アクセス認証の設定」（P.18-21）を参照）、AAA サーバまたはローカル データベースで定義したユーザ名とパスワードを入力します。

SSH アクセスの設定

クライアント IP アドレスを指定して、ASA 1000V に SSH を使用して接続できるユーザを定義するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ1	**crypto key generate rsa modulus** *modulus_size* **例：** `hostname(config)# crypto key generate rsa modulus 1024`	（任意）RSA キー ペアを生成します。これは、SSH で必要です。 係数の値（ビット単位）は 512、768、1024、または 2048 です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 1024 にすることをお勧めします。
ステップ2	**write memory** **例：** `hostname(config)# write memory`	RSA キーを永続的なフラッシュ メモリに保存します。
ステップ3	**aaa authentication ssh console LOCAL**	SSH アクセスのローカル認証をイネーブルにします。AAA サーバを使用して認証を設定することもできます。詳細については、「CLI および ASDM アクセス認証の設定」（P.18-21）を参照してください。
ステップ4	**username** *username* **password** *password*	SSH アクセスに使用できるユーザをローカル データベースに作成します。

	コマンド	目的
ステップ5	**ssh** *source_IP_address mask source_interface* **例：** hostname(config)# ssh 192.168.3.0 255.255.255.0 inside	アドレスまたはサブネットごとに、ASA 1000V が接続を許可する IP アドレスと、SSH を実行するインターフェイスを指定します。Telnet と異なり、SSH は最も低いセキュリティ レベルのインターフェイスで実行できます。
ステップ6	（任意） **ssh timeout** *minutes* **例：** hostname(config)# ssh timeout 30	ASA 1000V がセッションを切断するまでに SSH がアイドル状態を維持する時間の長さを設定します。 タイムアウトは 1 ～ 60 分に設定します。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。
ステップ7	（任意） **ssh version** *version_number* **例：** hostname(config)# ssh version 2	SSH バージョン 1 または 2 へのアクセスを制限します。デフォルトでは、SSH はバージョン 1 と 2 の両方を許可します。
ステップ8	**ssh key-exchange** {**dh-group1** | **dhgroup14**} **例：** hostname(config)# ssh key-exchange dh-group14	（任意）Diffie-Hellman グループ 1 と Diffie-Hellman グループ 14 のどちらが後に続き、キー交換に使用する必要があるかを指定します。値を指定しない場合は、Diffie-Hellman グループ 1 がデフォルトになります。

例

次の例は、RSA キーを生成し、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASA 1000V にアクセスする方法を示しています。

```
hostname(config)# crypto key generate rsa modulus 1024
hostnamehostname(config)# write memory
hostname(config)# aaa authentication ssh console LOCAL
WARNING: local database is empty!Use 'username' command to define local users.
hostname(config)# username exampleuser1 password examplepassword1
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh timeout 30
```

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASA 1000V にアクセスできるようにする方法を示しています。

```
hostname(config)# ssh 192.168.3.0 255.255.255.0 inside
```

SSH クライアントの使用

管理ホストの SSH クライアントで、「SSH アクセスの設定」（P.17-3）で設定したユーザ名とパスワードを入力します。SSH セッションを開始すると、次の SSH ユーザ認証プロンプトが表示される前に、ASA 1000V コンソール上にドット（.）が表示されます。

```
hostname(config)#.
```

ドットが表示されても、SSH の機能には影響を与えません。コンソールにドットが表示されるのは、ユーザ認証が始まる前で、サーバ キーを生成する場合か、または SSH キー交換中に秘密キーを使用してメッセージを暗号化する場合です。これらのタスクには 2 分以上かかることがあります。ドットは、ASA 1000V がビジー状態で、ハングしていないことを示す進捗インジケータです。

ASDM での HTTPS アクセスの設定

ASDM を使用するには、HTTPS サーバをイネーブルにし、ASA 1000V への HTTPS 接続を許可する必要があります。HTTPS アクセスは、工場出荷時のデフォルト設定の一部として、または **setup** コマンドを使用したときにイネーブルになっています。この項では、ASDM アクセスを手動で設定する方法について説明します。

ASDM への HTTPS アクセスを設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ1	**http** *source_IP_address mask source_interface* **例：** `hostname(config)# http 192.168.1.2 255.255.255.255 inside`	アドレスまたはサブネットごとに、ASA 1000V が HTTPS 接続を許可する IP アドレスを指定します。
ステップ2	**http server enable** [*port*] **例：** `hostname(config)# http server enable 443`	（任意）HTTPS サーバをイネーブルにします。 デフォルトでは、*port* は 443 です。ポート番号を変更する場合は、必ず ASDM アクセス URL に変更したポート番号を含めてください。たとえば、ポート番号を 444 に変更する場合は、次のように入力します。 **https://10.1.1.1:444**

例

次の例は、HTTPS サーバをイネーブルにし、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASDM にアクセスする方法を示しています。

```
hostname(config)# http server enable
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASDM にアクセスできるようにする方法を示しています。

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

CLI パラメータの設定

この項は、次の内容で構成されています。

- 「コンソール タイムアウトの変更」（P.17-8）

ログイン バナーの設定

ユーザが ASA 1000V に接続し、ユーザが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。

制限事項

バナーが追加された後、次の場合は ASA 1000V 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。

ガイドライン

- 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。侵入者を惹き付けるような「welcome」や「please」といった言葉を使用しないでください。次のバナーは、不正アクセスに対して適切な雰囲気を表しています。

  ```
  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 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。

ログイン バナーを設定するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
banner {**exec** | **login** | **motd**} *text* **例：** `hostname(config)# banner motd Welcome to $(hostname).`	ユーザが最初に接続したとき（「今日のお知らせ」（**motd**））、ユーザがログインしたとき（**login**）、ユーザが特権 EXEC モードにアクセスしたとき（**exec**）のいずれかに表示するバナーを追加します。ユーザが ASA 1000V に接続すると、まず「今日のお知らせ」バナーが表示され、その後にログイン バナーとプロンプトが表示されます。ユーザが ASA 1000V に正常にログインすると、exec バナーが表示されます。 複数の行を追加する場合は、各行の前に **banner** コマンドを置きます。 バナー テキストに関する注意事項： • スペースは使用できますが、CLI を使用してタブを入力することはできません。 • バナーの長さの制限は、RAM およびフラッシュ メモリに関するもの以外はありません。 • ASA 1000V のホスト名またはドメイン名は、**$(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。

例

次は、「今日のお知らせ」バナーの追加方法の例です。

```
hostname(config)# banner motd Welcome to $(hostname).
hostname(config)# banner motd Contact me at admin@example.com for any
hostname(config)# banner motd issues.
```

CLI プロンプトのカスタマイズ

[CLI Prompt] ペインで、CLI セッション時に使用するプロンプトをカスタマイズできます。デフォルトでは、プロンプトに ASA 1000V のホスト名が表示されます。CLI プロンプトには、次の項目を表示できます。

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	ASA 1000V のトラフィック通過状態を表示します。状態には次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、ASA 1000V 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。ASA 1000V 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ディセーブルであり、ASA 1000V 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ディセーブルであり、ASA 1000V ではトラフィックを通過させていません。この状態はスタンバイ ASA 1000V でしきい値を上回るインターフェイス障害の場合に発生することがあります。

手順の詳細

CLI プロンプトをカスタマイズするには、次のコマンドを入力します。

コマンド	目的
prompt {[**hostname**] [**domain**] [**slot**] [**state**] [**priority**]} **例：** `hostname(config)# prompt hostname`	CLI プロンプトをカスタマイズします。

コンソール タイムアウトの変更

コンソール タイムアウトは、接続が特権 EXEC モードまたはコンフィギュレーション モードのままでいることの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 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になりません。コンソール ポートへの接続はタイムアウトになることはないため、この設定によってコンソール ポートへの接続継続時間は影響を受けません。

コンソールのタイムアウトを変更するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
console timeout *number* **例：** `hostname(config)# console timeout 0`	特権セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。デフォルトのタイムアウトは 0 であり、セッションがタイムアウトしないことを示します。

ICMP アクセスの設定

デフォルトでは、任意の ASA 1000V インターフェイスに ICMP パケットを送信できます。この項では、ASA 1000V への ICMP 管理アクセスを制限する方法について説明します。ASA 1000V への ICMP アクセスを許可するホストとネットワークのアドレスを制限することによって、ASA 1000V を攻撃から保護できます。

（注） ICMP トラフィックが ASA 1000V を通過できるようにするには、第 16 章「アクセス ルールの設定」を参照してください。

この項は、次の内容で構成されています。

- 「ICMP アクセスに関する情報」（P.17-8）
- 「ガイドラインと制限事項」（P.17-9）
- 「デフォルト設定」（P.17-9）
- 「ICMP アクセスの設定」（P.17-9）

ICMP アクセスに関する情報

ICMP 到達不能メッセージ タイプ（タイプ 3）の権限は常に付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになって、IPSec および PPTP トラフィックが停止することがあります。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

ICMP ルールを設定していると、ASA 1000V では、ICMP トラフィックに対する最初の照合の後に、すべてのエントリを暗黙の拒否が使用されます。つまり、最初に一致したエントリが許可エントリである場合、ICMP パケットは引き続き処理されます。最初に一致したエントリが拒否エントリであるか、

エントリに一致しない場合、ASA 1000V によって ICMP パケットは破棄され、syslog メッセージが生成されます。ICMP ルールが設定されていない場合は例外となります。その場合、許可文が想定されます。

ガイドラインと制限事項

- ASA 1000V は、ブロードキャスト アドレス宛ての ICMP エコー要求に応答しません。
- ASA 1000V は、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デフォルト設定

デフォルトでは、任意の ASA 1000V インターフェイスに ICMP パケットを送信できます。

ICMP アクセスの設定

ICMP アクセス ルールを設定するには、次のいずれかのコマンドを入力します。

手順の詳細

コマンド	目的
icmp {**permit** | **deny**} {**host** *ip_address* | *ip_address mask* | **any**} [*icmp_type*] *interface_name* **例：** `hostname(config)# icmp deny host 10.1.1.15 inside`	ICMP アクセス ルールを作成します。*icmp_type* を指定しないと、すべてのタイプが識別されます。番号または名前を入力できます。ping を制御するには、echo-reply（0）（ASA 1000V からホストへ）または echo（8）（ホストから ASA 1000V へ）を指定します。ICMP タイプのリストについては、「ICMP タイプ」（P.B-9）を参照してください。 *interface_name* 引数には、イーサネット インターフェイスの名前を指定します。

例

次の例は、10.1.1.15 のホストを除くすべてのホストで内部インターフェイスへの ICMP の使用を許可する方法を示しています。

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

次の例は、次のコマンドを入力して、10.1.1.15 のアドレスを持つホストに内部インターフェイスへの ping だけを許可する方法を示しています。

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

IPsec サイトツーサイト トンネル上の管理アクセスの設定

IPsec サイトツーサイト トンネルが、あるインターフェイスで終わっている場合に、別のインターフェイスにアクセスして ASA 1000V を管理する必要があれば、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識別できます。たとえば、外部インターフェイスから ASA 1000V に入る場合は、この機能を使用して、ASDM、SSH、Telnet、または SNMP 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。

この項は、次の内容で構成されています。

ガイドラインと制限事項

管理アクセス インターフェイスは 1 つだけ定義できます。

管理インターフェイスの設定

管理インターフェイスを設定するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
management access *management_interface* **例：** `hostname(config)# management access inside`	*management_interface* 引数は、別のインターフェイスから ASA 1000V に入るときにアクセスする管理インターフェイスの名前を指定します。

管理アクセスの機能履歴

表 17-1 に機能履歴を示します。

表 17-1　管理アクセスの機能履歴

機能名	プラットフォーム リリース	機能情報
管理アクセス	8.7(1)	VPN 経由での管理アクセスの場合、IPsec サイトツーサイト トンネルのみがサポートされます。