backup コマンド～ browse-networks コマンド

backup

ASA のコンフィギュレーション、証明書、キー、およびイメージをバックアップするには、特権 EXEC モードで **backup** コマンドを使用します。

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

構文の説明

/noconfirm	**location** パラメータと **cert-passphrase** パラメータの入力を要求しないように指定します。警告およびエラー メッセージをバイパスしてバックアップを続行できるようにします。
context *ctx-name*	システム実行スペースからのマルチ コンテキスト モードで、**context** キーワードを入力して、指定したコンテキストをバックアップします。各コンテキストを個別にバックアップする必要があります。つまり、各ファイルに対して **backup** コマンドをもう一度入力します。
interface *name*	(任意)バックアップをコピーするインターフェイスの名前を指定します。インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。
location *path*	バックアップの **location** にはローカル ディスクまたはリモート URL を指定できます。location を指定しない場合は、次のデフォルト名が使用されます。 • シングル モード: disk0:*hostname*.backup.*timestamp*.tar.gz • マルチ モード: disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz
passphrase *value*	VPN 証明書および事前共有キーのバックアップ中、証明書を符号化するために、**cert-passphrase** キーワードで指定された秘密キーが必要です。PKCS12 形式の証明書を符号化および復号化するために使用するパスフレーズを入力する必要があります。バックアップに含まれるのは証明書に関連する RSA キー ペアだけであり、スタンドアロン証明書は除外されます。

デフォルト

location を指定しない場合は、次のデフォルト名が使用されます。

- シングル モード：disk0:*hostname*.backup.*timestamp*.tar.gz
- マルチ モード：disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。
9.5(1)	**interface** *name* 引数が追加されました。

使用上のガイドライン

次のガイドラインを参照してください。

- バックアップを開始する前に、バックアップ場所に 300 MB 以上のディスク領域が使用可能である必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。その結果、ASA が異なる動作をする可能性があります。
- バックアップは一度に 1 つだけ開始できます。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、新しい ASA OS のロード時に、ASA によって常駐スタートアップ コンフィギュレーションが自動的にアップグレードされます。
- クラスタリングを使用する場合、バックアップできるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスター パスフレーズが不明な場合は、CLI 設定ガイドを参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。

- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキー ペアには必ず同じ名前を使用してください。
- インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。管理専用インターフェイスを経由するデフォルト ルートがある場合は、すべての**バックアップ** トラフィックがそのルートに一致するため、データ ルーティング テーブルが確認されることはありません。このシナリオでは、データ インターフェイスを経由してバックアップする必要がある場合は常にインターフェイスを指定します。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- backup location コマンドを発行する場合、ディレクトリパスに二重スラッシュ「//」を使用してください。次に例を示します。

  ```
  ciscoasa# backup location disk0://sample-backup
  ```

- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    AnyConnect（SVC）クライアントのイメージおよびプロファイル

    AnyConnect（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - アプリケーション プロファイルのカスタム フレームワーク（APCF）
  - ブックマーク
  - カスタマイゼーション
  - ダイナミック アクセス ポリシー（DAP）
  - プラグイン
  - 接続プロファイル用の事前入力スクリプト
  - プロキシ自動設定
  - 変換テーブル
  - Web コンテンツ
  - バージョン情報

例

次に、バックアップを作成する例を示します。

```
ciscoasa# backup location disk0://sample-backup
Backup location [disk0://sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco. You will be
required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file is used to
restore to a device with a different master passphrase, you will need to provide the
current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

関連コマンド

コマンド	説明
restore	バックアップ ファイルから ASA のコンフィギュレーション、キー、証明書、およびイメージを復元します。

backup interface

ASA 5505 など、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **backup interface** コマンドを使用して、ISP などへのバックアップ インターフェイスとして VLAN インターフェイスを指定します。通常の動作に戻すには、このコマンドの **no** 形式を使用します。

backup interface vlan *number*

no backup interface vlan *number*

構文の説明

vlan *number*	バックアップ インターフェイスの VLAN ID を指定します。

デフォルト

デフォルトでは、**backup interface** コマンドはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
7.2(2)	Security Plus ライセンスでは、VLAN インターフェイス数の制限（通常のトラフィック用は 3 つ、バックアップ インターフェイス用は 1 つ、フェールオーバー用は 1 つ）がなくなり、最大 20 のインターフェイスを設定できるようになりました（最大数以外の制限はありません）。したがって、4 つ以上のインターフェイスをイネーブルにするために **backup interface** コマンドを使用する必要はありません。

使用上のガイドライン

このコマンドを入力できるのは、VLAN インターフェイスのインターフェイス コンフィギュレーション モードだけです。このコマンドは、プライマリ インターフェイスを経由するデフォルト ルートがダウンしない限り、指定したバックアップ インターフェイスを通過しようとするトラフィックをすべてブロックします。

backup interface コマンドで Easy VPN を設定した場合は、バックアップ インターフェイスがプライマリになると、ASA は VPN ルールを新しいプライマリ インターフェイスに移動します。バックアップ インターフェイスの状態を表示する方法については、**show interface** コマンドを参照してください。

必ずプライマリ インターフェイスとバックアップ インターフェイスの両方にデフォルト ルートを設定して、プライマリ インターフェイスに障害が発生した場合にバックアップ インターフェイスを使用できるようにしてください。たとえば、2 つのデフォルト ルートを設定して、1 つはアドミニストレーティブ ディスタンスが低いプライマリ インターフェイス用とし、もう 1 つはアドミニストレーティブ ディスタンスが高いバックアップ インターフェイス用とすることができます。DHCP サーバから取得したデフォルト ルートのアドミニストレーティブ ディスタンスを上書きする方法については、**dhcp client route distance** コマンドを参照してください。デュアル ISP サポートの設定の詳細については、**sla monitor** コマンドおよび **track rtr** コマンドを参照してください。

management-only コマンドをすでに設定しているインターフェイスをバックアップ インターフェイスに設定することはできません。

例

次に、4 つの VLAN インターフェイスを設定する例を示します。backup-isp インターフェイスは、プライマリ インターフェイスがダウンしている場合に限り、通過トラフィックを許可します。**route** コマンドでは、プライマリ インターフェイスとバックアップ インターフェイスのデフォルト ルートを作成し、バックアップ ルートには低いアドミニストレーティブ ディスタンスを設定しています。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# backup interface vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# route outside 0 0 10.1.1.2 1
ciscoasa(config)# route backup-isp 0 0 10.1.2.2 2
```

関連コマンド

コマンド	説明
forward interface	インターフェイスが別のインターフェイスへのトラフィックを開始することを制限します。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
dhcp client route distance	DHCP サーバから取得したデフォルト ルートのアドミニストレーティブ ディスタンスを上書きします。
sla monitor	スタティック ルートのトラッキングの SLA モニタリング動作を作成します。
track rtr	SLA モニタリング動作の状態を追跡します。

backup-package auto

Cisco ISA 3000 で自動バックアップと復元の操作を設定するには、特権 EXEC モードで **backup-package auto** コマンドを使用します。自動バックアップまたは復元を無効にするには、このコマンドの **no** 形式を使用します。

backup-package {**backup** | **restore**} **auto**

no backup-package {**backup** | **restore**} **auto**

構文の説明

バックアップ	自動バックアップを設定していることを示します。
restore	自動復元を設定していることを示します。

デフォルト

デフォルトのバックアップと復元のモードは手動です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

バックアップと復元のモードは独立しており、個別に設定できます。

自動バックアップと復元の操作にバックアップと復元の設定パラメータを指定するには、**backup-package location** コマンドを使用します。

例

次に、**backup-package** コマンドを使用して自動バックアップを設定する例を示します。

```
ciscoasa# backup-package backup auto
```

関連コマンド

コマンド	説明
show backup-package summary	バックアップと復元のパッケージ パラメータのサマリーを表示します。

backup-package location

Cisco ISA 3000 で後続のバックアップおよび復元の操作に使用するバックアップおよび復元の場所を設定するには、特権 EXEC モードで **backup-package location** コマンドを使用します。バックアップまたは復元の場所をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

backup-package {**backup** | **restore**} [**interface** *name*] **location disk***n***:** [**passphrase** *string*]

no backup-package {**backup** | **restore**} **location**

構文の説明

backup	バックアップ パラメータを定義していることを示します。
interface *name*	(任意)バックアップまたは復元の通信に使用するインターフェイスの名前。
location disk*n***:**	バックアップ パッケージ情報が保存されるストレージ メディアの場所。
passphrase *string*	(任意)バックアップ情報の暗号化、またはバックアップされた情報の取得に使用するパスフレーズ。
restore	復元パラメータを定義していることを示します。

デフォルト

デフォルトの場所は **disk3:** で、SD カードが含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

バックアップと復元の操作は独立しており、個別に設定できます。

一般に、**backup-package** 情報の設定は、追加のパラメーターを指定しなくても後で手動でデバイス構成をバックアップおよび復元できるようにするための 1 回限りの操作です。

例

次に、**backup-package location** コマンドを使用して、暗号化パスフレーズとして「cisco」を使用してバックアップ パラメータを設定する例を示します。

```
ciscoasa# backup-package backup location disk3: passphrase cisco
```

関連コマンド

コマンド	説明
show backup-package status	バックアップまたは復元用のパッケージ情報を表示します。
show backup-package summary	バックアップと復元のパッケージ パラメータのサマリーを表示します。

backup-servers

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを使用します。バックアップ サーバを削除するには、このコマンドの **no** 形式を使用します。

backup-servers {*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**}

no backup-servers [*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**]

構文の説明

clear-client-config	クライアントがバックアップ サーバを使用しないことを指定します。ASA は、ヌルのサーバ リストをプッシュします。
keep-client-config	ASA がバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバ リストを使用します(設定されている場合)。
server1 server 2.... server10	プライマリ ASA が利用できない場合に VPN クライアントが使用するサーバのリストを指定します。各サーバをスペースで区切り、プライオリティの高い順に並べます。サーバは、IP アドレスまたはホスト名で指定します。リストには 500 文字まで入力できますが、10 個のエントリのみを含めることができます。

デフォルト

クライアント上またはプライマリ ASA 上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

実行コンフィギュレーションから backup-servers 属性を削除するには、このコマンドの **no** 形式を引数なしで使用します。これにより、バックアップ サーバの値を別のグループ ポリシーから継承できます。

IPsec バックアップ サーバにより、VPN クライアントは、プライマリ ASA が利用できない場合でもセントラル サイトに接続できます。バックアップ サーバを設定すると、IPsec トンネルが確立されるときに ASA がクライアントにサーバ リストをプッシュします。

バックアップ サーバは、クライアント上またはプライマリ ASA 上に設定します。ASA 上にバックアップ サーバを設定すると、適応型セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュして、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注） ホスト名を使用する場合は、バックアップ DNS サーバおよびバックアップ WINS サーバを、プライマリ DNS サーバおよびプライマリ WINS サーバとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。また、ホスト名を使用している場合に DNS サーバが使用不可になると、大幅な遅延が発生するおそれがあります。

例

次に、「FirstGroup」という名前のグループ ポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner（グローバル）

ASDM バナー、セッション バナー、ログイン バナー、または Message-of-The-Day バナーを設定するには、グローバル コンフィギュレーション モードで banner コマンドを使用します。指定されたバナー キーワード（**exec**、**login**、あるいは **motd**）からすべての行を削除するには、このコマンドの **no** 形式を使用します。

banner {**asdm** | **exec** | **login** | **motd** *text*}

[no] banner {**asdm** | **exec** | **login** | **motd** [*text*]}

構文の説明

asdm	ASDM へのログインに成功した後にバナーを表示するようにシステムを設定します。続行してログインを完了するか、または切断するかを確認するプロンプトがユーザに表示されます。このオプションを使用すると、接続の前に、書面によるポリシー条件の受け入れをユーザに求めることができます。
exec	イネーブル プロンプトを表示する前に、バナーを表示するようにシステムを設定します。
login	Telnet またはシリアル コンソールを使用して ASA にアクセスする場合、パスワード ログイン プロンプトを表示する前にバナーを表示するようにシステムを設定します。
motd	初めて接続したときに Message-of-The-Day バナーを表示するようにシステムを設定します。
text	表示するメッセージ テキスト行。

デフォルト

デフォルトでは、バナーは表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(4)/8.0(3)	**asdm** キーワードが追加されました。
9.0(1)	**banner login** コマンドは、シリアル コンソール接続をサポートします。

使用上のガイドライン

banner コマンドは、指定したキーワードに対応して表示されるようにバナーを設定します。*text* ストリングは、最初の空白（スペース）の後に続く、行末（復帰または改行（LF））までのすべての文字で構成されます。テキスト内のスペースは維持されます。ただし、CLI ではタブを入力できません。

最初に既存のバナーをクリアしない限り、後続の *text* エントリは既存のバナーの末尾に追加されていきます。

（注） $(domain) トークンと $(hostname) トークンは、ASA のドメイン名とホスト名にそれぞれ置き換えられます。コンテキスト コンフィギュレーションで $(system) トークンを入力すると、このコンテキストでは、システム コンフィギュレーションで設定されているバナーが使用されます。

バナーを複数行にするには、追加する行ごとに banner コマンドを新たに入力します。これにより、既存のバナーの末尾に各行が追加されます。

（注） バナーの認可プロンプトの最大長は、235 文字または 31 単語（最初に制限に達した方）です。

Telnet または SSH を介して ASA にアクセスする場合は、バナー メッセージの処理に必要なシステム メモリが十分ないか、または TCP 書き込みエラーが発生すると、セッションが閉じます。**exec** および **motd** バナーだけが、SSH を介した ASA へのアクセスをサポートしています。ログイン バナーは、初期接続の一部としてユーザ名を渡さない SSHv1 クライアントまたは SSH クライアントをサポートしていません。

バナーを置き換えるには、**no banner** コマンドを使用してから、新しい行を追加します。

指定したバナー キーワードのすべての行を削除するには、**no banner {exec | login | motd}** コマンドを使用します。

no banner コマンドでは、テキスト ストリングを選択して削除することはできません。そのため、**no banner** コマンドの末尾に入力したテキストはすべて無視されます。

例

次に、**asdm**、**exec**、**login**、および **motd** の各バナーを設定する例を示します。

```
ciscoasa(config)#  banner asdm You successfully logged in to ASDM
ciscoasa(config)#  banner motd Think on These Things
ciscoasa(config)#  banner exec Enter your password carefully
ciscoasa(config)#  banner login Enter your password to log in
ciscoasa(config)# show running-config banner
asdm:
You successfully logged in to ASDM

exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

次に、**motd** バナーに 2 行目を追加する例を示します。

```
ciscoasa(config)# banner motd and Enjoy Today
ciscoasa(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

関連コマンド

コマンド	説明
clear configure	すべてのバナーを削除します。
show running-config	すべてのバナーを表示します。

banner（グループ ポリシー）

リモート クライアントの接続時にリモート クライアント上でバナーまたはウェルカム テキストを表示するには、グループ ポリシー コンフィギュレーション モードで **banner** コマンドを使用します。バナーを削除するには、このコマンドの **no** 形式を使用します。

banner {**value** *_string* | **none**}

no banner

(注) VPN グループ ポリシーで複数のバナーを設定し、いずれかのバナーを削除すると、すべてのバナーが削除されます。

構文の説明

none	バナーにヌル値を設定して、バナーを禁止します。デフォルトまたは指定したグループ ポリシーのバナーを継承しません。
value *banner_string*	バナー テキストを設定します。ログイン後バナーの最大文字列サイズは 4,000 文字です。復帰改行を挿入するには、「\n」シーケンスを使用します。クライアントやブラウザは各行の表示制限近辺でラッピングを行うため、行ごとに 80 ～ 100 文字を設定することを推奨します。

デフォルト

デフォルトのバナーはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	ログイン後バナー長の値を 4,000 に拡大しました。

使用上のガイドライン

バナーは ASA 上にローカルで設定されるため、ユーザはログイン後バナーに対して [Accept] または [Disconnect] をクリックする必要があります。

（注） IKEv1 や AnyConnect バージョン 3 などの古いアーキテクチャでの動作はエラーを発生させずにサポートされています。

バナーを継承しないようにするには、**banner none** コマンドを使用します。

IPsec VPN クライアントは、バナー用の完全な HTML をサポートしています。ただし、クライアントレス ポータルおよび AnyConnect クライアントは部分的な HTML をサポートしています。バナーがリモート ユーザに正しく表示されるようにするには、次のガイドラインに従います。

- IPsec クライアント ユーザの場合は、/n タグを使用します。
- AnyConnect クライアント ユーザの場合は、
 タグを使用します。
- クライアントレス ユーザの場合は、
 タグを使用します。

例

次に、「FirstGroup」という名前のグループ ポリシーにバナーを作成する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

base-url

(任意)クライアントレス VPN のベース URL を設定します。この URL は、サードパーティ IdP に提供される SAML メタデータで使用されます。これにより IdP は ASA にエンドポイント ユーザをリダイレクトできるようになります。

この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

base-url {value *_string*}

no base-url

構文の説明

base-url	カウントレス VPN の URL

デフォルト

なし。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

- base-url が設定されている場合、これは AssertionConsumerService と SingleLogoutService のベース URL であり、**show saml metadata** で表示されます。
- base-url が設定されていない場合、ベース URL は ASA の hostname と domain-name から作成されます。たとえば、hostname 名が「ssl-vpn」、domain-name 名が「cisco.com」である場合、**show saml metadata** で表示されるベース URL は **https://ssl-vpn.cisco.com** です。
- base-url、または hostname と domain-name のいずれも設定されていない場合、**show saml metadata** はエラーを表示します。

例

次に、base-url を設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp myIdp
ciscoasa(config-webvpn-saml-idp)# base url https://ClientlessVPN.com
```

関連コマンド

コマンド	説明
signature	SAML 要求のシグニチャをイネーブルまたはディセーブルにします。デフォルトでは、シグニチャはディセーブルです。
timeout	SAML IdP タイムアウトを設定します。
trustpoint	saml-idp サブモードでトラストポイントを設定します。
url	SAML IdP URL を設定します。

basic-mapping-rule

マッピングアドレスおよびポート(MAP)ドメイン内の基本マッピングルールを設定するには、MAP ドメインのコンフィギュレーション モードで **basic-mapping-rule** コマンドを使用します。基本マッピングルールを削除するには、このコマンドの **no** 形式を使用します。

basic-mapping-rule

no basic-mapping-rule

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MAP ドメイン コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

カスタマーエッジ(CE)デバイスは、基本マッピングルールを使用して、専用 IPv4 アドレッシングまたは共有アドレスとポート セットの割り当てを決定します。CE デバイスは最初に、システムの IPv4 アドレスをプールのプレフィックスおよびポート範囲内の IPv4 アドレスおよびポート(NAT44 を使用)に変換し、次にルールの IPv6 プレフィックスによって定義されたプール内の IPv6 アドレスに、新しい IPv4 アドレスを変換します。その後、パケットはサービスプロバイダーの IPv6 専用ネットワークを介してボーダーリレー(BR)デバイスに送信されるようになります。

basic-mapping-rule コマンドを入力すると、MAP ドメインの基本マッピング ルール コンフィギュレーション モードが開始されます。ここでは、ルールの IPv4、IPv6、およびポートのプロパティを設定できます。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート(MAP)ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート(MAP)ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

basic-security

IP オプション インスペクションが設定されたパケット ヘッダーでセキュリティ(SEC)オプションが発生したときのアクションを定義するには、パラメータ コンフィギュレーション モードで **basic-security** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

basic-security action {allow | clear}

no basic-security action {allow | clear}

構文の説明

allow	セキュリティ IP オプションを含むパケットを許可します。
clear	セキュリティ オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、セキュリティ IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# basic-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

bfd echo

インターフェイスで BFD エコー モードをイネーブルにするには、インターフェイス コンフィギュレーション モードで **bfd echo** コマンドを使用します。BFD エコー モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

bfd echo

no bfd echo

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

BFD エコー モードは、BFD IPv4 セッションではデフォルトディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

エコー モードはデフォルトでイネーブルになっていますが、BFD IPv6 セッションではサポートされていません。キーワードを指定せずに **no bfd echo** コマンドを入力すると、エコー パケットの送信がオフになり、ASA が BFD ネイバー ルータから受信したエコー パケットを転送しないことを示します。

エコー モードをイネーブルにすると、最小エコー送信間隔と必要最短送信間隔の値が **bfd interval milliseconds min_rx milliseconds** パラメータから取得されます。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、**no ip redirects** コマンドを入力して、インターネット制御メッセージ プロトコル(ICMP)リダイレクト メッセージの送信をディセーブルにする必要があります。

例

次に、BFD マップに BFD テンプレートを関連付ける例を示します。

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd echo
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd interval

インターフェイスで基準 BFD パラメータを設定するには、インターフェイス コンフィギュレーション モードで **bfd** コマンドを使用します。ベースライン BFD セッション パラメータを削除するには、このコマンドの **no** 形式を使用します。

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

構文の説明

interval	BFD 制御パケットが BFD ピアに送信される速度を指定します。有効値は 50 ～ 999 ミリ秒です。
min_rx	BFD 制御パケットが BFD ピアから受信されるときに期待される速度を指定します。有効値は 50 ～ 999 ミリ秒です。
multiplier	BFD ピアから紛失してよい BFD 制御パケットのレートを指定します。このレートに達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。
milliseconds	この値はミリ秒単位です。
multiplier-value	乗数の値。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD マップに BFD テンプレートを関連付ける例を示します。

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd map

アドレスをマルチホップ テンプレートに関連付ける BFD マップを設定するには、グローバル コンフィギュレーション モードで、**bfd map** コマンドを使用します。BFD マップを削除するには、このコマンドの **no** 形式を使用します。

bfd map {ipv4 | ipv6} *destination/cdir source/cdir template-name*

no bfd map

構文の説明

ipv4	IPv4 アドレスを設定します。
ipv6	IPv6 アドレスを設定します。
destination/cdir	宛先プレフィクス/長さです。
source/cdir	送信元プレフィクス/長さです。
template-name	BFD マップに関連付ける BFD テンプレートの名前です。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD マップに BFD テンプレートを関連付ける例を示します。

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 multihop-template1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。

コマンド	説明
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd slow-timers

BFD スロー タイマー値を設定するには、グローバル コンフィギュレーション モードで **bfd slow-timers** コマンドを使用します。

bgp slow-timers *[milliseconds]*

構文の説明

milliseconds	（任意）BFD スロー タイマー値（ミリ秒）です。指定できる範囲は 1000 ～ 30,000 です。デフォルトは 1000 です。

デフォルト

BFD スロー タイマーのデフォルト値は 1,000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、14,000 ミリ秒の BFD スロー タイマーを設定する例を示します。

```
ciscoasa(config)# bfd slow-timers 14000
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。

コマンド	説明
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd template

シングルホップ BFD テンプレートをインターフェイスにバインドするには、インターフェイス コンフィギュレーション モードで **bfd template** コマンドを使用します。シングルホップ BFD テンプレートをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

bfd template *template-name*

no bfd template *template-name*

構文の説明

template-name	BFD テンプレートの名前。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

bfd-template コマンドを使用してテンプレートを作成していない場合でも、インターフェイスでテンプレート名を設定できますが、テンプレートを定義するまでテンプレートは無効と見なされます。テンプレート名を再設定する必要はありません。名前は自動的に有効になります。

例

次に、インターフェイスにシングル ホップ BFD テンプレートをバインドする例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# bfd template template-1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd-template

BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **bfd-template** コマンドを使用します。BFD テンプレートをディセーブルにするには、このコマンドの **no** 形式を使用します。

bfd-template [single-hop | multi-hop] *template-name*

no bfd-template [single-hop | multi-hop] *template-name*

構文の説明

single-hop	シングルホップ BFD テンプレートを指定します。
multi-hop	マルチホップ BFD テンプレートを指定します。
template-name	BFD テンプレートの名前。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、BFD テンプレートを作成し、BFD コンフィギュレーション モードを開始するために使用します。また、テンプレートで一連の BFD 間隔値を指定できます。BFD テンプレートの一部として指定される BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。

例

次に、シングルホップ BFD テンプレートを設定する例を示します。

```
ciscoasa(config)# bfd single-hop node1
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

次に、マルチホップ BFD テンプレートを設定する例を示します。

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bgp aggregate-timer

BGP ルートが集約される間隔を設定する場合、またはタイマーに基づくルート集約をディセーブルにする場合は、アドレス ファミリ コンフィギュレーション モードで **bgp aggregate-timer** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

bgp aggregate-timer *seconds*

no bgp aggregate-timer

構文の説明

seconds	システムが BGP ルートを集約する間隔（秒単位）。 有効な値は 6 ～ 60 の範囲か、または 0（ゼロ）です。 デフォルト値は 30 です。 値を 0（ゼロ）に設定すると、タイマーに基づく集約をディセーブルにし、集約をただちに開始します。

デフォルト

bgp 集約タイマーのデフォルト値は 30 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション、アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

このコマンドは、BGP ルートが集約されるデフォルト間隔を変更するために使用します。

非常に大規模なコンフィギュレーションでは、**aggregate-address summary-only** コマンドを設定した場合でも、より具体的なルートがアドバタイズされ、後で取り消されます。この動作を回避するには、**bgp aggregate-timer** を 0（ゼロ）に設定します。これにより、集約ルートがただちにチェックされ、特定のルートが抑制されます。

例

次に、20 秒間隔で BGP ルート集約を設定する例を示します。

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

次に、BGP ルート集約をただちに開始する例を示します。

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始して、標準 IP バージョン 4（IPv4）アドレス プレフィックスを使用するルーティング セッションを設定します。
aggregate-address	Border Gateway Protocol（BGP）データベース内に集約エントリを作成します。

bgp always-compare-med

異なる自律システムにあるネイバーからのパスの Multi Exit Discriminator（MED）を比較できるようにするには、ルータ コンフィギュレーション モードで **bgp always-compare-med** コマンドを使用します。比較を禁止するには、このコマンドの **no** 形式を使用します。

bgp always-compare-med

no bgp always-compare-med

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドがイネーブルになっていない場合、またはこのコマンドの **no** 形式を入力した場合、ASA ルーティング ソフトウェアは異なる自律システムにあるネイバーからのパスの MED を比較しません。

MED が比較されるのは、比較されるルートの自律システム パスが同じである場合だけです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

MED は、RFC 1771 に記述されているように、オプションの非推移的属性で、4 オクテットの負でない整数です。この属性の値は、BGP の最適パス選択プロセスで、隣接自律システムへの複数の出力点を区別するために使用されることがあります。

MED は、多数のパスの選択肢の中から最適パスを選択するときに考慮されるパラメータの 1 つです。MED が低いパスの方が、MED が高いパスよりも優先されます。最適パス選択プロセス中、MED 比較は、同じ自律システムからのパスに対してだけ行われます。この動作を変更するには、**bgp always-compare-med** コマンドを使用して、受信したパスが属する自律システムに関係なくすべてのパスについて MED 比較を実行します。

bgp deterministic-med コマンドを設定すると、同じ自律システムから受信したすべてのパスについて確定的な MED 値比較を実行できます。

例

次の例では、受信したパスが属する自律システムに関係なくパスの選択肢から MED を比較するように、ローカル BGP ルーティング プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp always-compare-med
```

関連コマンド

コマンド	説明
bgp deterministic-med	同じ自律システムから受信したすべてのパスについて Multi Exit Discriminator（MED）値の確定的な比較を実行します。

bgp asnotation dot

デフォルトの表示を変更し、Border Gateway Protocol（BGP）の 4 バイト自律システム番号の正規表現マッチング形式を asplain 表記（10 進数値）からドット付き表記にするには、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトの 4 バイト自律システム番号の表示と正規表現マッチング形式をリセットして asplain に戻すには、このコマンドの **no** 形式を使用します。

bgp asnotation dot

no bgp asnotation dot

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

BGP 自律システム番号は画面出力に asplain（10 進数値）形式で表示されます。正規表現で 4 バイト自律システム番号とマッチングするデフォルト形式は asplain です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述されているように、2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は 1 ～ 65535 の範囲の 2 オクテットの数値でした。

自律システム番号の要求の増加に伴い、インターネット割り当て番号局（IANA）により割り当てられる自律システム番号は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。
- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

シスコが採用している 4 バイト自律システム番号では、自律システム番号のデフォルト表示形式として asplain が使用されますが、4 バイト自律システム番号を asplain と asdot の両方の形式で設定できます。また、正規表現で 4 バイト自律システム番号とマッチングするためのデフォルト形式は asplain であるため、4 バイト自律システム番号とマッチングする正規表現はすべて、asplain 形式で記述する必要があります。デフォルトの **show** コマンド出力で、4 バイト自律システム番号が asdot 形式で表示されるように変更する場合は、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式がイネーブルにされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。次の表に示すように、4 バイト自律システム番号は asplain と asdot のどちらにも設定できますが、**show** コマンド出力と正規表現を使用した 4 バイト自律システム番号のマッチング制御には 1 つの形式だけが使用されます。デフォルトは asplain 形式です。

show コマンド出力の表示と正規表現のマッチング制御で asdot 形式の 4 バイト自律システム番号を使用する場合、**bgp asnotation dot** コマンドを設定する必要があります。**bgp asnotation dot** コマンドをイネーブルにした後で、**clearbgp *** コマンドを入力し、すべての BGP セッションについて、ハード リセットを開始する必要があります。

表4-1　asplain をデフォルトとする 4 バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 6553 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 6553 4 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 6553 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 6553 4 バイト：65536 ～ 4294967295

表4-2　asdot を使用する 4 バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535

例

次の **show bgp summary** コマンドの出力は、4 バイト自律システム番号のデフォルト asplain 形式を示しています。ここで、asplain 形式で表された 4 バイト自律システム番号 65536 および 65550 に注意してください。

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04       0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15       0
```

次のコンフィギュレーションは、デフォルトの出力形式を asdot 表記形式に変更するために実行されます。

```
ciscoasa# configure terminal
ciscoasa(config)# router bgp 65538
ciscoasa(config-router)# bgp asnotation dot
```

コンフィギュレーションの実行後、次の **show bgp summary** コマンド出力に示すように、出力が asdot 表記形式に変換されます。asdot 形式で表された 4 バイト自律システム番号 1.0 および 1.14 に注意してください（これらは自律システム番号 65536 と 65550 を asdot 変換したものです）。

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13       0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24       0
```

bgp asnotation dot コマンドを設定すると、4 バイト自律システム パスの正規表現マッチング形式が asdot 表記形式に変更されます。4 バイト自律システム番号は、asplain 形式または asdot 形式のいずれかを使用して、正規表現で設定できますが、現在のデフォルト形式を使用して設定された 4 バイト自律システム番号だけがマッチングされます。1 つ目の例では、**show bgp regexp** コマンドは、asplain 形式で表された 4 バイト自律システム番号を使用して設定されています。現在のデフォルト形式は asdot 形式なのでマッチングは失敗し、何も出力されません。asdot 形式を使用した 2 番目の例では、マッチングは成功し、4 バイトの自律システム パスに関する情報が asdot 表記法を使って表示されます。

```
ciscoasa(config-router)# show bgp regexp ^65536$
ciscoasa(config-router)# show bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

（注） この asdot 表記法で使用されているピリオドは、シスコの正規表現では特殊文字です。特殊な意味を取り除くには、ピリオドの前にバックスラッシュをつけます。

関連コマンド

コマンド	説明
show bgp summary	すべての Border Gateway Protocol（BGP）接続のステータスを表示します。
show bgp regexp	自律システム パスの正規表現と一致するルートを表示します。

bgp bestpath compare-routerid

最適パス選択プロセス中に異なる外部ピアから受信された同一ルートを比較し、最適パスとして最も小さいルータ ID を持つルートを選択するように、Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp bestpath compare-routerid** コマンドを使用します。

BGP ルーティング プロセスをデフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドの動作はデフォルトでディセーブルであり、同一の属性を持つ 2 つのルートが受信されたとき、BGP は最初に受信されたルートを選択します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp bestpath compare-routerid コマンドは、2 つの異なるピア（ルータ ID を除くすべての属性が同じ）から 2 つの同一のルートが受信されたときに最適パス選択のタイ ブレーカーとしてルータ ID を使用するように BGP ルーティング プロセスを設定するために使用します。このコマンドがイネーブルになっている場合、その他の属性がすべてが等しければ、最も小さいルータ ID が最適パスとして選択されます。

例

次の例では、異なるピアから同一のパスが受信されたときに、パスを比較し、最適パス選択のタイ ブレーカーとしてルータ ID を使用するように、BGP ルーティング プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath compare-routerid
```

bgp bestpath med missing-as-worst

Multi Exit Discriminator（MED）属性がないルートに無限の値を割り当てる（MED 値のないパスを最も不適切なパスとする）ように Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp bestpath med missing-as-worst** コマンドを使用します。ルータをデフォルトの動作に戻す（MED のないルートに 0 の値を割り当てる）には、このコマンドの **no** 形式を使用します。

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ASA ソフトウェアは、MED 属性のないルートに 0 の値を割り当てるため、MED 属性がないルートを最適パスと見なします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次の例では、MED 属性がないルートを無限の値（4294967294）を持つルートと見なし、このパスを最も不適切なパスとするように BGP ルータ プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath med missing-as-worst
```

bgp-community new-format

コミュニティを AA:NN 形式（自律システム番号:コミュニティ番号/4 バイトの数値）で表示するように BGP を設定するには、グローバル コンフィギュレーション モードで **bgp-community new-format** コマンドを使用します。コミュニティを 32 ビットの数値として表示するように BGP を設定するには、このコマンドの **no** 形式を使用します。

bgp-community new-format

no bgp-community new-format

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドがイネーブルになっていない場合、または **no** 形式を入力した場合、BGP コミュニティは（AA:NN 形式で入力したときも）32 ビットの数値として表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp-community new-format コマンドは、BGP コミュニティを RFC-1997 準拠の AA:NN 形式で表示するようにローカル ルータを設定するために使用します。

このコマンドは、BGP コミュニティが表示される形式のみに影響を与え、コミュニティやコミュニティの交換には影響を与えません。ただし、32 ビットの数値でなく AA:NN 形式でマッチングを行うように、ローカルに設定された正規表現と一致する拡張 IP コミュニティ リストを更新する必要がある場合があります。

RFC 1997『*BGP Communities Attribute*』には、BGP コミュニティがそれぞれ 2 バイト長の 2 つの部分で構成されると規定されています。1 つ目の部分は自律システム番号で、2 つ目の部分はネットワーク オペレータによって定義された 2 バイトの数値です。

例

次の例では、32 ビットの数値のコミュニティ形式を使用するルータを、AA:NN 形式を使用するようにアップグレードしています。

```
ciscoasa(config)# bgp-community new-format
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

次の出力例は、**bgp-community new-format** コマンドがイネーブルになっている場合に BGP コミュニティ番号がどのように表示されるかを示しています。

```
ciscoasa(router)# show bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
Advertised to non peer-group peers:
10.0.33.35
35
10.0.33.35 from 10.0.33.35 (192.168.3.3)
Origin incomplete, metric 10, localpref 100, valid, external
Community: 1:1
Local
0.0.0.0 from 0.0.0.0 (10.0.33.34)
Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

bgp default local-preference

デフォルトのローカル プリファレンス値を変更するには、ルータ コンフィギュレーション モードで **bgp default local-preference** コマンドを使用します。ローカル プリファレンス値をデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

bgp default local-preference *number*

no bgp default local-preference *number*

構文の説明

number	0 ～ 4294967295 の範囲のローカル プリファレンス値。

デフォルト

このコマンドがイネーブルになっていない場合、またはこのコマンドの **no** 形式を入力した場合、ASA ソフトウェアはローカル プリファレンス値 100 を適用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ローカル プリファレンス属性は、BGP の最適パス選択プロセス中にプリファレンス レベルをルートに適用するために使用される任意の属性です。この属性は iBGP ピア間だけで交換され、ローカル ポリシーを決定するために使用されます。ローカル プリファレンス値が最大のルートが優先されます。

例

次の例では、ローカル優先順位値は 200 に設定されます。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp default local-preference 200
```

bgp deterministic-med

同じ自律システムから受信されたすべてのパスについて Multi Exit Discriminator（MED）値の確定的な比較を実行するには、ルータ コンフィギュレーション モードで **bgp deterministic-med** コマンドを使用します。必要な MED 比較をディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp deterministic-med

no bgp deterministic-med

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ASA ソフトウェアは、同じ自律システムから受信されたすべてのパスについて MED 変数の確定的な比較を実行しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp always-compare-med コマンドは、異なる自律システムにあるネイバーからのパスの Multi Exit Discriminator（MED）の比較をイネーブルにするために使用します。**bgp always-compare-med** コマンドの設定後、同じ自律システムにある異なるネイバーから受信された同じプレフィックスのパスはすべてグループ化され、昇順の MED 値でソートされます（受信専用のパスは無視され、グループ化もソートもされません）。

次に、最適パス選択アルゴリズムにより、既存のルールを使用して最適パスが選択されます。比較は、ネイバーの自律システムごとに行われ、続いてグローバルに行われます。パスのグループ化およびソートは、このコマンドを入力するとただちに行われます。正しい結果を得るには、ローカル自律システム内のすべてのルータでこのコマンドがイネーブル（またはディセーブル）になっている必要があります。

例

次の例では、1 つの連合内の同じサブ自律システムによってアドバタイズされたルートのパス選択中に MED を比較するように BGP を設定しています。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp deterministic-med
```

次の **show bgp** コマンド出力例は、**bgp deterministic-med** コマンドのコンフィギュレーションによってルート選択がどのように影響を受けるかを示しています。**bgp deterministic-med** コマンドがイネーブルになっていない場合、ルートの受信順序によって最適パス選択でどのようにルートが選択されるかが決まります。次の **show bgp** コマンドの出力例は、同じプレフィックス（10.100.0.0）に対して受信された 3 つのパスを示しています。**bgp deterministic-med** コマンドはイネーブルになっていません。

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external, best
```

ルータで bgp deterministic-med 機能がイネーブルになっていない場合、ルートの受信順序によってルート選択が影響を受けることがあります。次のシナリオで、1 つのルータが同じプレフィックスに対して 3 つのパスを受信した場合を考えてみます。

ローカル ルーティング テーブルのすべてのルートをクリアするために、**clear bgp *** コマンドを入力します。

```
ciscoasa(router)# clear bgp *
```

ルーティング テーブルへの再書き込みが行われた後、**show bgp** コマンドを再度発行します。BGP セッションをクリアした後、パスの順序が変わることに注意してください。2 番目のセッションではパスの受信順序が異なっていたため、選択アルゴリズムの結果も変わっています。

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal, best
```

bgp deterministic-med コマンドがイネーブルになっている場合、ローカル ルータがパスを受信した順序に関係なく、選択アルゴリズムの結果は常に同じになります。このシナリオでは、ローカル ルータで **bgp deterministic-med** コマンドを入力した場合、常に次の出力が生成されます。

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 15
```

```
Paths: (3 available, best #1, advertised over EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal, best 3
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
```

関連コマンド

コマンド	説明
bgp always compare-med	異なる自律システムにあるネイバーからのパスの Multi Exit Discriminator（MED）の比較をイネーブルにします。
clear bgp	ハードまたはソフト再構成を使用して BGP 接続をリセットします。
show bgp	Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示します。

bgp enforce-first-as

着信アップデート内の AS_PATH の先頭に自律システム番号が示されていない外部 BGP（eBGP）ピアから受信したアップデートを拒否するように ASA を設定するには、ルータ コンフィギュレーション モードで **bgp enforce-first-as** コマンドを使用します。この動作をディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp enforce-first-as

no bgp enforce-first-as

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドの動作は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp enforce-first-as コマンドは、AS_PATH 属性内の最初のセグメントとして自律システム番号が示されていない eBGP ピアから受信した着信アップデートを拒否するために使用します。このコマンドをイネーブルにすると、間違った設定のピアや権限のないピアが、別の自律システムからのルートであるかのようにルートをアドバタイズすることによってトラフィックを誤った宛先に送信する（ローカル ルータをスプーフィングする）ことを回避できます。

例

次に、BGP ピアからのすべての着信アップデートを調べて、AS_PATH 内の最初の自律システム番号が送信側ピアのローカル AS 番号であることを確認する例を示します。次の例では、最初の AS 番号が 65001 でなければ、ピア 10.100.0.1 からのアップデートは廃棄されます。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp enforce-first-as
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.100.0.1 remote-as 65001
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。
neighbor remote-as	BGP またはマルチプロトコル BGP ルーティング テーブルにエントリを追加します。

bgp fast-external-fallover

これらのピアにアクセスするためのリンクがダウンした場合に外部 BGP ピアリング セッションをただちにリセットするように Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp fast-external-fallover** コマンドを使用します。BGP 高速外部フォールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp fast-external-fallover

no bgp fast-external-fallover

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

BGP 高速外部フォールオーバーはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp fast-external-fallover コマンドは、直接接続されている外部ピアとの BGP ピアリング セッションにおける高速外部フォールオーバーをディセーブルまたはイネーブルにするために使用します。リンクがダウンするとセッションは即座にリセットされます。直接接続されているピアのみサポートされます。BGP 高速外部フォールオーバーがディセーブルの場合、BGP ルーティング プロセスはデフォルトのホールド タイマーの期限（3 回のキープアライブ）が切れるまで待ってピアリング セッションをリセットします。また、**ip bgp fast-external-fallover** インターフェイス コンフィギュレーション コマンドを使用して、BGP 高速外部フォールオーバーをインターフェイス単位で設定することもできます。

例

次に、BGP 高速外部フォールオーバー機能をディセーブルにする例を示します。このセッションを伝送するリンクがフラップしても、接続はリセットされません。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# no bgp fast-external-fallover
```

関連コマンド

コマンド	説明
ip bgp fast-external-fallover	インターフェイス単位で高速外部フォールオーバーを設定します。

bgp graceful-restart

ノンストップ転送設定でグレースフル リスタートの Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp graceful-restart** コマンドを使用します。BGP グレースフル リスタートをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]

no bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]

構文の説明

restart-time *seconds*	リスタート イベントが発生した後、グレースフル リスタート対応ネイバーが通常の動作に戻るまでシステムが待機する最大時間（秒）。デフォルトは 120 秒です。値は 1 ～ 3600 秒です。
stalepath-time *seconds*	リスタートしているピアの古いパスをシステムが保持する最大時間（秒）。すべての古いパスは、このタイマーが期限切れになった後に削除されます。デフォルト値は 360 秒です。値は 1 ～ 3600 秒です。

デフォルト

BGP グレースフル リスタートはデフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

ノンストップ転送のグレースフル リスタートを有効にするには、このコマンドを使用します。グレースフル リスタートを使用すると、システムは、再起動中にアドレス グループのフォワーディング ステートを維持する機能をアドバタイズできます。各 BGP ネイバー ルータの再起動機能を設定するには、**neighbor ha-mode graceful-restart** コマンドを使用します。

例

次に、デフォルトのタイマーを使用してグレースフル リスタートをグローバルにイネーブルにする例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp graceful-restart
```

関連コマンド

コマンド	説明
neighbor ha-mode graceful-restart	BGP ネイバーの Border Gateway Protocol（BGP）グレースフル リスタート機能を設定します。

bgp inject-map

より具体的なルートを Border Gateway Protocol（BGP）ルーティング テーブルに挿入するように条件付きルート注入を設定するには、アドレス ファミリ コンフィギュレーション モードで **bgp inject-map** コマンドを使用します。条件付きルート注入の設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

no bgp inject-map *inject-map* **exist-map** *exist-map*

構文の説明

inject-map	ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
exist-map *exist-map*	BGP スピーカーが追跡するプレフィックスを含むルート マップの名前を指定します。
copy-attributes	（オプション）注入されたルートが集約ルートの属性を継承するように設定します。

デフォルト

特定のルートが BGP ルーティング テーブルに注入されることはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション、アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

bgp inject-map コマンドは、条件付きルート注入を設定するために使用します。条件付きルート注入により、一致するものがなくても、より具体的なプレフィックスを BGP ルーティング テーブルにすることができます。2 つのルート マップ（*exist-map* および *inject-map*）をグローバル コンフィギュレーション モードで設定してから、アドレス ファミリ コンフィギュレーション モードの **bgp inject-map** コマンドで指定します。

exist-map 引数は、BGP スピーカーが追跡するプレフィックスを定義するルート マップを指定します。このルート マップには、集約プレフィックスを指定するための **match ip address prefix-list** コマンド ステートメントと、ルート ソースを指定するための **match ip route-source prefix-list** コマンド ステートメントが含まれる必要があります。

inject-map は、ルーティング テーブルで作成され、このテーブルに格納されるプレフィックスを定義します。注入されたプレフィックスは、ローカル BGP RIB に格納されます。有効な親ルートが存在する必要があります。集約ルート（既存プレフィックス）と同じかそれより具体的なプレフィックスのみを注入できます。

オプションのキーワード **copy-attributes** は、注入されたプレフィックスが集約ルートと同じ属性を継承するように任意で設定するために使用します。このキーワードを入力しない場合、注入されたプレフィックスは、ローカルで生成されたルートのデフォルト属性を使用します。

例

次の例では、条件付きルート注入を設定しています。注入されたプレフィックスは、集約（親）ルートの属性を継承します。

```
ciscoasa(config)# ip prefix-list ROUTE permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
ciscoasa(config)# route-map LEARNED_PATH permit 10
ciscoasa(config-route-map)# match ip address prefix-list ROUTE
ciscoasa(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
ciscoasa(config-route-map)# exit
ciscoasa(config)# route-map ORIGINATE permit 10
ciscoasa(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
ciscoasa(config-route-map)# set community 14616:555 additive
ciscoasa(config-route-map)# exit
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH
copy-attributes
```

関連コマンド

コマンド	説明
ip prefix-list	プレフィックス リストを作成するか、プレフィックス リスト エントリを追加します。
set community	BGP コミュニティ属性を設定します。
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。

bgp log-neighbor-changes

BGP ネイバー リセットのロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **bgp log-neighbor-changes** コマンドを使用します。BGP ネイバーとの隣接関係の変化に関するロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp log-neighbor-changes

no bgp log-neighbor-changes

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

BGP ネイバーのロギングはイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp log-neighbor-changes コマンドは、BGP ネイバー ステータスの変化（アップまたはダウン）およびリセットに関するロギングをイネーブルにします。ログはネットワークの接続問題のトラブルシューティングおよびネットワークの安定性の評価に使用します。ネイバーが突然リセットする場合は、ネットワークのエラー率の高いことやパケット損失の多いことが考えられるので、調査するようにしてください。

ステータスの変化に関するメッセージをロギングするために **bgp log-neighbor-changes** コマンドを使用しても、BGP アップデート デバッグを有効にする場合などと異なり、パフォーマンスに大きな影響を与えることはありません。

bgp log-neighbor-changes コマンドがイネーブルでない場合、ネイバー ステータスの変化に関するメッセージは、**show bgp neighbors** コマンドの出力として常に使用可能なリセットの理由を除いて、追跡されません。

eigrp log-neighbor-changes コマンドは、Enhanced Interior Gateway Routing Protocol（EIGRP）ネイバーとの隣接関係のロギングをイネーブルにしますが、BGP ネイバーに関するメッセージは **bgp log-neighbor-changes** コマンドで明確にイネーブルにされた場合にのみ記録されます。

BGP ネイバーの変化に関するログを表示するには、**show logging** コマンドを使用します。

例

次に、ルータ コンフィギュレーション モードで BGP のネイバーの変化をログする例を示します。

```
ciscoasa(config)# bgp router 40000
ciscoasa(config-router)# bgp log-neighbor-changes
```

関連コマンド

コマンド	説明
show BGP neighbors	ネイバーへの BGP 接続に関する情報を表示します。

bgp maxas-limit

AS パス内の自律システム番号が指定した値を超えるルートを廃棄するように Border Gateway Protocol（BGP）を設定するには、ルータ コンフィギュレーション モードで **bgp maxas-limit** コマンドを使用します。ルータをデフォルト動作に戻すには、このコマンドの **no** 形式を使用します。

bgp max-as limit *number*

no bgp max-as limit

構文の説明

number	BGP アップデート メッセージ内の AS パス属性にある自律システム番号の最大数（1 ～ 254）。このコマンドは、AS パス セグメント内の自律システム番号の数に制限を設定するだけでなく、AS パス セグメントの数を 10 に制限します。10 個の AS パス セグメントを許可する動作が、**bgp maxas-limit** コマンドに組み込まれています。

デフォルト

ルートは廃棄されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp maxas-limit コマンドは、着信ルートで許可される AS パス属性内の自律システム番号の数を制限するために使用します。設定した制限を超える AS パス セグメントを持つルートが受信されると、BGP ルーティング プロセスでこのルートが廃棄されます。

例

次に、AS パス属性内の自律システム番号の最大数を 30 に設定する例を示します。

```
ciscoasa(config)# router bgp 4000
ciscoasa(config)# bgp maxas-limit 30
```

bgp nexthop

Border Gateway Protocol（BGP）のネクストホップ アドレス トラッキングを設定するには、アドレス ファミリ コンフィギュレーション モードまたはルータ コンフィギュレーション モードで **bgp nexthop** コマンドを使用します。BGP ネクストホップ アドレス トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

no bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

構文の説明

トリガー	BGP ネクストホップ アドレス トラッキングの使用を指定します。ネクストホップ トラッキング遅延を変更するには、このキーワードを **delay** キーワードとともに使用します。ネクストホップ アドレス トラッキングをイネーブルにするには、このキーワードを **enable** キーワードとともに使用します。
delay	ルーティング テーブルに格納された更新済みのネクストホップ ルートに対するチェックの遅延間隔を変更します。
seconds	遅延に指定する秒数。有効な値は 0 ～ 100 です。デフォルトは 5 です。
enable	BGP ネクストホップ アドレス トラッキングをイネーブルにします。
route-map	BGP プレフィックスのネクストホップ ルートとして割り当てられたルーティング テーブル内のルートに適用されるルート マップの使用を指定します。
map-name	ルート マップの名前。

デフォルト

IPv4 では、BGP ネクストホップ アドレス トラッキングはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

BGP ネクストホップ アドレス トラッキングはイベント ドリブンです。BGP プレフィックスは、ピアリング セッションの確立時に自動的にトラッキングされます。ネクストホップの変更は、ルーティング情報ベース（RIB）で更新されると BGP に迅速に報告されます。この最適化によって、RIB にインストールされているルートのネクストホップの変更に対する応答時間が短縮されることで、全体的な BGP コンバージェンスが改善されます。BGP スキャナ サイクル間に最適パス計算が実行されると、変更内容だけが処理および追跡されます。

（注）

- BGP ネクストホップ アドレス トラッキングによって、BGP 応答時間を大幅に短縮できます。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアにより、BGP が不安定になることがあります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。
- IPv6 アドレス ファミリでは、BGP ネクストホップ アドレス トラッキングはサポートされていません。

BGP ネクストホップ アドレス トラッキングのルーティング テーブル ウォーク間の遅延間隔を変更するには、**trigger** キーワードを **delay** キーワードおよび *seconds* 引数とともに使用します。すべてのルーティング テーブル ウォーク間の遅延間隔を調整して IGP の調整パラメータと一致させることで、BGP ネクストホップ アドレス トラッキングのパフォーマンスを向上させることができます。デフォルトの遅延間隔は 5 秒であり、高速で調整される IGP の場合はこれが最適な値です。よりゆっくり収束する IGP の場合は、IGP コンバージェンス時間に応じて遅延間隔を 20 秒以上に変更できます。

BGP ネクストホップ アドレス トラッキングをイネーブルにするには、**trigger** キーワードを **enable** キーワードとともに使用します。BGP ネクストホップ アドレス トラッキングは、デフォルトでイネーブルになっています。

ルート マップを使用できるようにするには、**route-map** キーワードおよび *map-name* 引数を使用します。このルート マップは BGP 最適パス計算中に使用され、BGP プレフィックスの Next_Hop 属性に対応するルーティング テーブル内のルートに適用されます。ネクストホップ ルートがルート マップの評価に失敗した場合、ネクストホップ ルートは到達不能とマークされます。このコマンドはアドレス ファミリ単位で実行されるため、異なるアドレス ファミリ内のネクストホップ ルートでは別のルート マップを適用できます。

（注）

ルート マップでサポートされるコマンドは、**match ip address** コマンドだけです。**set** コマンドやその他の **match** コマンドはサポートされません。

例

次に、IPv4 アドレス ファミリ セッションによって 20 秒ごとに発生する BGP ネクストホップ アドレス トラッキングのルーティング テーブル ウォーク間の遅延間隔を変更する例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop trigger delay 20
```

次に、IPv4 アドレス ファミリのネクストホップ アドレス トラッキングをディセーブルにする例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# no bgp nexthop trigger enable
```

次に、アドレス マスクの長さが 25 を超える場合にのみルートをネクストホップ ルートと見なすことを許可するルート マップを設定する例を示します。このコンフィギュレーションによって、プレフィックスの集約がネクストホップ ルートと見なされることを回避できます。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP
ciscoasa(config-router-af)# exit-address-family
ciscoasa(config-router)# exit
ciscoasa(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
ciscoasa(config)# route-map CHECK-NEXTHOP permit 10
ciscoasa(config)# match ip address prefix-list FILTER25
```

bgp redistribute-internal

EIGRP や OSPF などの内部ゲートウェイ プロトコル（IGP）への iBGP 再配布を設定するには、アドレス ファミリ コンフィギュレーション モードで **bgp redistribute-internal** コマンドを使用します。ルータをデフォルトの動作に戻し、IGP への iBGP 再配布を停止するには、このコマンドの **no** 形式を使用します。

bgp redistribute-internal

no bgp redistribute-internal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

IBGP ルートが IGP に再配布されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

bgp redistribute-internal コマンドは、IGP への iBGP の再配布を設定するために使用します。このコマンドの設定後に、BGP 接続をリセットするために **clear bgp** コマンドを入力する必要があります。

BGP を IGP に再配布する際は、必ず、再配布されるプレフィックスの数を制限するために IP prefix-list ステートメントおよび route-map ステートメントを使用してください。

注意 iBGP を IGP に再配布する際は、慎重に行ってください。再配布されるプレフィックスの数を制限するために IP prefix-list ステートメントおよび route-map ステートメントを使用します。フィルタリングされていない BGP ルーティング テーブルを IGP に再配布すると、通常の IGP ネットワーク動作に影響を及ぼす可能性があります。

例

次の例では、BGP から OSPF へのルート再配布をイネーブルにしています。

```
ciscoasa(config)# router ospf 300
ciscoasa(config-router)# redistribute bgp 200
ciscoasa(config-router)# exit
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp redistribute-internal
```

bgp router-id

Border Gateway Protocol（BGP）のローカル ルーティング プロセスの固定ルータ ID を設定するには、アドレス ファミリ ルータ コンフィギュレーション モードで **bgp router-id** コマンドを使用します。固定ルータ ID を実行コンフィギュレーション ファイルから削除し、デフォルト ルータ ID の選択に戻すには、このコマンドの **no** 形式を使用します。

bgp router-id *ip-address*

no bgp router-id

構文の説明

ip-address	IP アドレス形式のルータ ID。

デフォルト

このコマンドがイネーブルになっていない場合、ルータ ID は物理インターフェイスの最上位の IP アドレスに設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション ルータ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドが変更されました。

使用上のガイドライン

ローカル BGP ルーティング プロセスの固定ルータ ID を設定するには、**bgp router-id** コマンドを使用します。ルータ ID は IP アドレス形式で入力します。任意の有効な IP アドレスを使用できます。ルータでローカルに設定されていないアドレスでもかまいません。ルータ ID が変更されると、ピアリング セッションが自動的にリセットされます。コンテキストごとに個別のルータ ID を設定できます。

例

次に、固定 BGP ルータ ID が 192.168.254.254 であるローカル ルータを設定する例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

bgp scan-time

ネクスト ホップ検証用に Border Gateway Protocol（BGP）のスキャン間隔を設定するには、アドレス ファミリ コンフィギュレーション モードで **bgp scan-time** コマンドを使用します。ルータのスキャン間隔をデフォルトのスキャン間隔（60 秒）に戻すには、このコマンドの **no** 形式を使用します。

bgp scan-time *scanner-interval*

no bgp scan-time *scanner-interval*

構文の説明

scanner-interval	BGP ルーティング情報のスキャン間隔。 有効な値は 15 ～ 60 秒です。デフォルトは 60 秒です。

デフォルト

デフォルトのスキャン間隔は 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの **no** 形式を入力しても、スキャンはディセーブルになりませんが、**show running-config** コマンドの出力からは削除されます。

アドレス ファミリに対して **BGP ネクストホップ** アドレス トラッキング（NHT）がイネーブルになっている場合、そのアドレス ファミリで **bgp scan-time** コマンドは受け入れられず、デフォルト値の 60 秒は変更されません。ルータ モードまたはアドレス ファミリ モードで **bgp scan-time** コマンドを使用する場合は、あらかじめ NHT をディセーブルにしておく必要があります。

例

次のルータ コンフィギュレーションの例では、BGP ルーティング テーブルの IPv4 ユニキャスト ルートのネクスト ホップ検証のスキャン間隔を 20 秒に設定しています。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp scan-time 20
```

関連コマンド

コマンド	説明
show running-config	ASA で現在表示されているコンフィギュレーションを表示します。
bgp nexthop	BGP ネクストホップ アドレス トラッキングを設定します。

bgp suppress-inactive

ルーティング情報ベース（RIB）に導入されていないルートのアドバタイズメントを抑制するには、アドレス ファミリ モードまたはルータ コンフィギュレーション モードで **bgp suppress-inactive** コマンドを使用します。

bgp suppress-inactive

no bgp suppress-inactive

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

bgp suppress-inactive コマンドは、RIB（非アクティブなルート）に導入されていないルートがピアにアドバタイズされないようにするために使用します。この機能がイネーブルになっていない場合、またはこのコマンドの **no** 形式を使用した場合、Border Gateway Protocol（BGP）によって非アクティブなルートがアドバタイズされます。

（注） BGP は、RIB に導入されていないルートに RIB 失敗フラグを付けます。このフラグは、**show bgp** コマンドの出力にも、Rib-Failure (17) のように表示されます。このフラグは、ルートまたは RIB に関するエラーや問題を示しておらず、このコマンドのコンフィギュレーションによっては、このフラグがあってもルートをアドバタイズできる場合もあります。非アクティブなルートに関する情報を表示するには、**show bgp rib-failure** コマンドを入力します。

例

次の例では、RIB に導入されていないルートをアドバタイズしないように BGP ルーティング プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp suppress-inactive
```

関連コマンド

コマンド	説明
show bgp	BGP ルーティング テーブル内のエントリを表示します。
show bgp rib-failure	ルーティング情報ベース(RIB)テーブルにインストールできなかった BGP ルートを表示します。

bgp transport

Border Gateway Protocol（BGP）のすべてのセッションに対してグローバルに TCP トランスポート セッション パラメータをイネーブルにするには、ルータ コンフィギュレーション モードで **bgp transport** コマンドを使用します。すべての BGP セッションに対してグローバルに TCP トランスポート セッション パラメータをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp transport path-mtu-discovery

no bgp transport path-mtu-discovery

構文の説明

path-mtu-discovery	トランスポート パスの最大伝送ユニット（MTU）検出をイネーブルにします。

デフォルト

TCP パスの MTU 検出は、すべての BGP セッションに対してデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると BGP セッションでより大きな MTU リンクを活用できるようになり、これは内部 BGP（iBGP）セッションに非常に重要となることがあるため、このコマンドはデフォルトでイネーブルになっています。TCP パスの MTU 検出がイネーブルになっていることを確認するには、**show bgp neighbors** コマンドを使用します。

例

次に、すべての BGP セッションに対して TCP パスの MTU 検出をディセーブルにする例を示します。

```
ciscoasa(config)# router bgp 4500
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

次に、すべての BGP セッションに対して TCP パスの MTU 検出をイネーブルにする例を示します。

```
iscoasa(config)# router bgp 4500
ciscoasa(config-router)# bgp transport path-mtu-discovery
```

関連コマンド

コマンド	説明
show bgp neighbors	ネイバーへの BGP 接続に関する情報を表示します。

blocks

ブロック診断（**show blocks** コマンドで表示）に追加のメモリを割り当てるには、特権 EXEC モードで **blocks** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

構文の説明

memory_sizes	（任意）ダイナミックな値を適用するのではなく、ブロック診断用のメモリ サイズをバイト単位で設定します。この値が空きメモリよりも大きい場合は、エラー メッセージが表示され、値は受け入れられません。この値が空きメモリの 50 % を超える場合は、警告メッセージが表示されますが、値は受け入れられます。

デフォルト

ブロック診断の追跡に割り当てられるデフォルト メモリは、2136 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

現在割り当てられているメモリを表示するには、**show blocks queue history** コマンドを入力します。

ASA をリロードすると、メモリ割り当てがデフォルトに戻ります。

割り当てられるメモリ量は最大 150 KB ですが、空きメモリの 50 % を超えることはありません。必要に応じて、メモリ サイズを手動で指定できます。

例

次に、ブロック診断用のメモリ サイズを増やす例を示します。

```
ciscoasa# blocks queue history enable
```

次に、メモリ サイズを 3000 バイトに増やす例を示します。

```
ciscoasa# blocks queue history enable 3000
```

次に、メモリ サイズを 3000 バイトに増やすことを試みるものの、この値が使用可能な空きメモリを超えている例を示します。

```
ciscoasa# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

次に、メモリ サイズを 3000 バイトに増やすものの、この値が空きメモリの 50 % を超えている例を示します。

```
ciscoasa# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

関連コマンド

コマンド	説明
clear blocks	システム バッファの統計情報をクリアします。
show blocks	システム バッファの使用状況を表示します。

boot

システムが次回のリロードで使用するイメージ、およびシステムが起動時に使用するコンフィギュレーション ファイルを指定するには、グローバル コンフィギュレーション モードで **boot** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

boot {**config** | **system**} *url*

no boot {**config** | **system**} *url*

構文の説明

config	システムがロードされるときに使用するコンフィギュレーション ファイルを指定します。
system	システムがロードされるときに使用するシステム イメージ ファイルを指定します。
url	イメージまたはコンフィギュレーションの場所を設定します。マルチ コンテキスト モードでは、管理コンテキストですべてのリモート URL にアクセスできる必要があります。次の URL 構文を参照してください。 • **disk0:/**[*path*/]*filename* ASA では、この URL は内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:/**[*path*/]*filename* ASA では、この URL は外部フラッシュ メモリ カードを示します。このオプションは、ASA サービス モジュールでは使用できません。 • **flash:/**[*path*/]*filename* この URL は内部フラッシュ メモリを示します。 • **tftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 このオプションは、ASA 5500 シリーズの **boot system** コマンドだけで使用できます。**boot config** コマンドを使用するには、スタートアップ コンフィギュレーションがフラッシュ メモリに存在している必要があります。 **boot system tftp:** コマンドは、1 つのみ設定でき、かつ最初に設定する必要があります。

デフォルト

- ASA イメージ:
  - Firepower 1000 およびアプライアンス モードの Firepower 2100:以前実行していたブート イメージをブートします。
  - その他の物理 ASA:内部フラッシュ メモリ内で見つかった最初のアプリケーション イメージをブートします。
  - ASAv:最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。
  - Firepower 4100/9300 シャーシ:FXOS システムによってブートする ASA イメージが決定されます。この手順を使用して ASA イメージを設定することはできません。
  - プラットフォーム モードの Firepower 2100: どの ASA/FXOS パッケージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。
- スタートアップ コンフィギュレーション:デフォルトでは、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.13(1)	このコマンドはアプライアンスモードのサポートで Firepower 1000 および 2100 を追加しました。

使用上のガイドライン

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブート イメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、コンフィギュレーション ファイルを任意で指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 4100/9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティングシステム内で ASA をアップグレードすることはできません。したがって、このコマンドを ASA イメージに使用しないでください。ASA と FXOS を別々にアップグレードすることができ、FXOS ディレクトリ リストに別々にリストされます。ASA パッケージには常に ASDM が含まれています。
- プラットフォーム モードの Firepower 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージ更新は FXOS によって管理されます。ASA オペレーティングシステム内で ASA をアップグレードすることはできません。したがって、このコマンドを ASA イメージに使用しないでください。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。
- アプライアンス モードの Firepower 1000 および 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージの更新は、次のコマンドを使用して ASA によって管理されます。これらのプラットフォームでは、ブートするイメージを識別するために ASA が使用されますが、基盤となるメカニズムはレガシー ASA とは異なります。
- ASAv：初期展開の ASAv パッケージでは、ASA イメージが読み取り専用 boot:/ パーティションに配置されます。ASAv をアップグレードするときは、フラッシュ メモリに別のイメージを指定します。後でコンフィギュレーションをクリアすると（**clear configure all**）、ASAv は元の展開のイメージをロードするようになることに注意してください。初期展開の ASAv パッケージには、フラッシュ メモリに配置される ASDM イメージも含まれています。ASDM イメージを個別にアップグレードできます。

boot config コマンドを、**write memory** コマンドを使用してスタートアップ コンフィギュレーションに保存すると、CONFIG_FILE 環境変数にも設定が保存されます。ASA は、これらの環境変数を使用して、再起動時にブートするスタートアップ コンフィギュレーションを決定します。

現在の実行コンフィギュレーションとは異なる、新しい場所にあるスタートアップ コンフィギュレーション ファイルを使用する場合は、実行コンフィギュレーションを保存した後に、必ず、スタートアップ コンフィギュレーション ファイルを新しい場所にコピーしてください。このようにしないと、実行コンフィギュレーションの保存時に、実行コンフィギュレーションによって新しいスタートアップ コンフィギュレーションが上書きされます。

ヒント　ASDM イメージ ファイルは、**asdm image** コマンドで指定します。

アプライアンスモードの Firepower 1000 および 2100 のブートシステム

boot system コマンドは 1 つだけ入力できます。新しいイメージにアップグレードする場合は、**no boot system** を入力して、以前に設定したイメージを削除する必要があります。

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

boot system コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。このコマンドを入力した後で ASA フラッシュメモリから元のイメージ ファイルを削除することもできます。その場合、ASA はブート場所から正しく起動します。

他のモデルとは異なり、スタートアップ コンフィギュレーション内のこのコマンドは、ブート イメージに影響しません（本質的に表面的なものです）。リロード時には、最後にロードされたブート イメージが常に実行されます。このコマンドを入力した後で設定を保存しない場合、リロードすると、新しいイメージが起動された場合でも、古いコマンドが設定に出現します。設定を保存することにより、設定の同期を維持する必要があります。

Cisco ダウンロード サイトからロードできるのは、元のファイル名のイメージのみです。ファイル名を変更した場合はロードされません。Firepower Threat Defense（FTD）イメージをロードすることによって、FTD に再イメージ化することもできます。この場合は、すぐにリロードするように求められます。

他のモデルのブートシステム

最大 4 つの **boot system** コマンドエントリを入力して、複数のイメージをブートする順番に指定することができます。ASA は、最初に検出に成功したイメージをブートします。**boot system** コマンドを入力すると、エントリがリストの最後に追加されます。ブートエントリの順序を変更するには、**clear configure boot system** コマンドを使用してすべてのエントリを削除してから、エントリを目的の順序で再入力する必要があります。設定できる **boot system tftp** コマンドは 1 つだけです。これは、最初に設定する必要があります。

boot system コマンドを、**write memory** コマンドを使用してスタートアップ コンフィギュレーションに保存すると、BOOT 環境変数にも設定が保存されます。ASA は、これらの環境変数を使用して、再起動時にブートするスタートアップ コンフィギュレーションを決定します。

例

次に、起動時に ASA が configuration.txt という名前のコンフィギュレーション ファイルをロードするように指定する例を示します。

```
ciscoasa(config)# boot config disk0:/configuration.txt
```

関連コマンド

コマンド	説明
asdm image	ASDM ソフトウェア イメージを指定します。
show bootvar	ブート ファイルおよびコンフィギュレーションの環境変数を表示します。

border style

認証された WebVPN ユーザに表示される WebVPN ホームページの境界線をカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **border style** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

border style *value*

no border style *value*

構文の説明

value	使用する Cascading Style Sheet（CSS）パラメータを指定します。許容最大文字数は 256 文字です。

デフォルト

境界線のデフォルト スタイルは background-color:#669999;color:white です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進数値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

(注) WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、境界線の背景色を RGB カラー #66FFFF（緑色の一種）にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# border style background-color:66FFFF
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

bridge-group

トランスペアレント ファイアウォール モードのブリッジ グループにインターフェイスを割り当てるには、インターフェイス コンフィギュレーション モードで **bridge-group** コマンドを使用します。インターフェイスの割り当てを解除するには、このコマンドの **no** 形式を使用します。トランスペアレント ファイアウォールは、そのインターフェイスで同じネットワークを接続します。1 つのブリッジ グループに最大 4 つのインターフェイスが属することができます。9.6(2) 以降では、ブリッジ グループに最大 64 個のインターフェイスを追加できます。

bridge-group *number*

no bridge-group *number*

構文の説明

number	1 ～ 100 の整数を指定します。9.3(1) 以降、範囲が 1 ～ 250 に拡大されました。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.3(1)	250 BVI をサポートするために数値の範囲が 1 ～ 250 に増加しました。
9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。

使用上のガイドライン

9.2 以前では、シングル モードまたはマルチ モードのコンテキストごとに最大 8 個のブリッジ グループを設定できます。9.3(1) 以降では、最大 250 個のブリッジ グループを設定できます。各ブリッジ グループには、最大 4 つのインターフェイスを含めることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があることに注意してください。

(注) ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。

interface bvi コマンドの後に **ip address** コマンドを使用して、ブリッジ グループに管理 IP アドレスを割り当てます。

各ブリッジ グループは、別々のネットワークに接続します。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは ASA 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。

セキュリティ コンテキストのオーバーヘッドを防ぐ場合、またはセキュリティ コンテキストの使用を最小限に抑える場合、複数のブリッジ グループを使用することがあります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。

例

次に、ブリッジ グループ 1 に GigabitEthernet 1/1 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# bridge-group 1
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定します。
interface bvi	管理 IP アドレスを設定できるように、ブリッジ グループについてインターフェイス コンフィギュレーション モードを開始します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。

browse-networks

認証された WebVPN ユーザに表示される WebVPN ホームページの [Browse Networks] ボックスをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **browse-networks** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

browse-networks {**title** | **message** | **dropdown**} {**text** | **style**} *value*

no browse-networks [{**title** | **message** | **dropdown**} {**text** | **style**} *value*]

構文の説明

dropdown	ドロップダウン リストへの変更を指定します。
message	タイトルの下に表示されるメッセージへの変更を指定します。
style	スタイルへの変更を指定します。
text	テキストへの変更を指定します。
title	タイトルへの変更を指定します。
value	表示される実際のテキストを示します。許容最大文字数は 256 文字です。この値は、Cascading Style Sheet（CSS）パラメータにも適用されます。

デフォルト

デフォルトのタイトル テキストは「Browse Networks」です。

デフォルトのタイトル スタイルは、次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

デフォルトのメッセージ テキストは「Enter Network Path」です。

メッセージのデフォルト スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

デフォルトのドロップダウン テキストは「File Folder Bookmarks」です。

ドロップダウンのデフォルト スタイルは次のとおりです。

border:1px solid black;font-weight:bold;color:black;font-size:80%.

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、タイトルを「Browse Corporate Networks」に変更し、スタイル内のテキストを青色に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
ciscoasa(config-webvpn-custom)# browse-networks title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。