CHAPTER 12

dhcpd address コマンド ～ distribute-list out コマンド

dhcpd address

DHCP サーバで使用される IP アドレス プールを定義するには、グローバル コンフィギュレーション モードで **dhcpd address** コマンドを使用します。既存の DHCP アドレス プ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。

dhcpd address *ip_address1*[*-ip_address2*] *interface_name*

no dhcpd address *interface_name*

構文の説明

interface_name	アドレス プールを割り当てるインターフェイス。トランスペアレント モードでは、ブリッジ グループ メンバー インターフェイスを指定します。ルーテッドモードでは、ルーテッドインターフェイスまたは BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。
ip_address1	DHCP アドレス プールの開始アドレス。
ip_address2	DHCP アドレス プールの終了アドレス。

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
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。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードで BVI にこのコマンドを設定できるようになりました。

使用上のガイドライン

DHCP サーバの ASA アドレス プールは、そのアドレス プールが有効な ASA インターフェイスと同じサブネット内にある必要があります。また、*interface_name* を使用して関連する ASA インターフェイスを指定する必要があります。

アドレス プールのサイズは、ASA でプールあたり 256 に制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、ASA インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

DHCP クライアントは、物理的に ASA DHCP サーバ インターフェイスのサブネットに接続されている必要があります。

dhcpd address コマンドでは、「-」（ダッシュ）文字がオブジェクト名の一部ではなく、範囲指定子と解釈されるため、この文字を含むインターフェイス名は使用できません。

no dhcpd address *interface_name* コマンドは、指定されたインターフェイスに設定されている DHCP サーバ アドレス プールを削除します。

ASA に DHCP サーバ機能を実装する方法の詳細については、CLI 設定ガイドを参照してください。

例

次に、ASA の DMZ インターフェイスに DHCP クライアントのアドレス プールおよび DNS サーバを設定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 209.165.200.226
ciscoasa(config)# dhcpd enable dmz
```

次に、内部インターフェイスに DHCP サーバを設定する例を示します。**dhcpd address** コマンドは、そのインターフェイスで DHCP サーバに 10 個の IP アドレスのプールを割り当てます。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd auto_config

DHCP または PPPoE クライアントを実行しているインターフェイスから取得した値、または VPN サーバから取得した値に基づいて、ASA で DHCP サーバに対して DNS、WINS およびドメイン名の値を自動的に設定できるようにするには、グローバル コンフィギュレーション モードで **dhcpd auto_config** コマンドを使用します。DHCP パラメータの自動設定を解除するには、このコマンドの **no** 形式を使用します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

構文の説明

client_if_name	DNS、WINS、およびドメイン名パラメータを提供する DHCP クライアントを実行している、インターフェイスを指定します。
interface *if_name*	アクションが適用されるインターフェイスを指定します。
vpnclient-wins-override	vpnclient パラメータにより、インターフェイス DHCP または PPPoE クライアントの WINS パラメータを上書きします。

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
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
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

CLI コマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定によって取得されたパラメータは、CLI により設定されたパラメータで上書きされます。

例

次に、内部インターフェイスに DHCP を設定する例を示します。外部インターフェイス上の DHCP クライアントから取得した DNS、WINS、およびドメイン情報を、内部インターフェイス上の DHCP クライアントに渡すには、**dhcpd auto_config** コマンドを使用します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd auto_config outside
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show ip address dhcp server	DHCP クライアントとして動作するインターフェイスに DHCP サーバから提供される、DHCP オプションに関する詳細情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd dns

DHCP クライアントに対して DNS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。定義されたサーバをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

no dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

構文の説明

dnsip1	DHCP クライアントに対するプライマリ DNS サーバの IP アドレスを指定します。
dnsip2	（オプション）DHCP クライアントに対する代替 DNS サーバの IP アドレスを指定します。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

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
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。

使用上のガイドライン

dhcpd dns コマンドは、DHCP クライアントに対する DNS サーバの IP アドレスを 1 つまたは複数指定します。2 つの DNS サーバを指定できます。**no dhcpd dns** コマンドは、コンフィギュレーションから DNS IP アドレスを削除します。

例

次に、ASA の DMZ インターフェイスに DHCP クライアントのアドレス プールおよび DNS サーバを設定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 192.168.1.2
ciscoasa(config)# dhcpd enable dmz
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
dhcpd wins	DHCP クライアントに対して WINS サーバを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd domain

DHCP クライアントに対して DNS ドメイン名を定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。DNS ドメイン名をクリアするには、このコマンドの **no** 形式を使用します。

dhcpd domain *domain_name* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

構文の説明

domain_name	DNS ドメイン名（example.com）を指定します。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

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
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。

使用上のガイドライン

dhcpd domain コマンドは、DHCP クライアントに対する DNS ドメイン名を指定します。**no dhcpd domain** コマンドは、コンフィギュレーションから DNS ドメイン サーバを削除します。

例

次に、ASA で DHCP サーバによって DHCP クライアントに提供されるドメイン名を設定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd enable

DHCP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd enable** コマンドを使用します。DHCP サーバ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。

dhcpd enable *interface*

no dhcpd enable *interface*

構文の説明

interface	DHCP サーバをイネーブルにするインターフェイスを指定します。

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
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。

使用上のガイドライン

DHCP サーバは、DHCP クライアントにネットワーク コンフィギュレーション パラメータを提供します。ASA 内で DHCP サーバをサポートすることにより、ASA は DHCP を使用して接続されるクライアントを設定できるようになります。**dhcpd enable** *interface* コマンドを使用すると、DHCP デーモンによる、DHCP 対応のインターフェイス上での DHCP クライアントの要求のリッスンをイネーブルにできます。**no dhcpd enable** コマンドは、指定したインターフェイス上の DHCP サーバ機能をディセーブルにします。

(注) マルチ コンテキスト モードの場合は、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP サーバをイネーブルにすることはできません。

ASA が DHCP クライアント要求に応答する場合、要求を受信したインターフェイスの IP アドレスとサブネット マスクを、デフォルト ゲートウェイの IP アドレスとサブネット マスクとして応答で使用します。

（注） ASA DHCP サーバ デーモンは、直接 ASA インターフェイスに接続されていないクライアントはサポートしません。

ASA に DHCP サーバ機能を実装する方法の詳細については、CLI 設定ガイドを参照してください。

例

次に、inside インターフェイスで DHCP サーバをイネーブルにする例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
debug dhcpd	DHCP サーバのデバッグ情報を表示します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd lease

DHCP リース期間を指定するには、グローバル コンフィギュレーション モードで **dhcpd lease** コマンドを使用します。リースの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。

dhcpd lease *lease_length* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
lease_length	DHCP サーバから DHCP クライアントに付与される IP アドレス リース期間を秒単位で指定します。有効な値は 300 ～ 1048575 秒です。

デフォルト

lease_length のデフォルト値は 3600 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	• 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

dhcpd lease コマンドは、DHCP クライアントに与えるリース期間を秒単位で指定します。このリース期間は、DHCP サーバが割り当てた IP アドレスを DHCP クライアントが使用できる期間を示します。

no dhcpd lease コマンドは、コンフィギュレーションから指定したリース期間を削除して、この値をデフォルト値の 3600 秒に置き換えます。

例

次に、DHCP クライアントに対する DHCP 情報のリース期間を指定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
```

```
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd option

DHCP オプションを設定するには、グローバル コンフィギュレーション モードで **dhcpd option** コマンドを使用します。オプションをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd option *code* {**ascii** *string*} | {**ip** *IP_address* [*IP_address*]} | {**hex** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

構文の説明

ascii *string*	オプション パラメータがスペースなしの ASCII 文字列であることを指定します。
code	設定する DHCP オプションを表す数字を指定します。有効な値は、0 ～ 255 であり、いくつかの例外があります。サポートされていない DHCP オプション コードのリストについては、「使用上のガイドライン」の項を参照してください。
hex *hex_string*	オプション パラメータが 16 進数の文字列（偶数個の桁数を含み、スペースを含まない）ではないことを指定します。0x プレフィックスを使用する必要はありません。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
ip	オプション パラメータが IP アドレスであることを指定します。最大 2 つの IP アドレスを **ip** キーワードに指定できます。
IP_address	ドット付き 10 進表記の IP アドレスを指定します。

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
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。

使用上のガイドライン

dhcpd option コマンドを使用して、TFTP サーバ情報を Cisco IP Phone およびルータに提供することができます。

DHCP オプション要求が ASA DHCP サーバに到着すると、ASA は **dhcpd option** コマンドで指定された値を、クライアントに対する応答に入れます。

dhcpd option 66 コマンドおよび **dhcpd option 150** コマンドは、Cisco IP Phone およびルータがコンフィギュレーション ファイルをダウンロードするときに使用する TFTP サーバを指定します。これらのコマンドは、次のように使用します。

- **dhcpd option 66 ascii** *string*。ここで、*string* は TFTP サーバの IP アドレスまたはホスト名です。オプション 66 には、TFTP サーバを 1 つだけ指定できます。
- **dhcpd option 150 ip** *IP_address* [*IP_address*]。ここで、*IP_address* は TFTP サーバの IP アドレスです。オプション 150 には、最大 2 つの IP アドレスを指定できます。

(注) **dhcpd option 66** コマンドは **ascii** パラメータのみ受け付け、**dhcpd option 150** コマンドは **ip** パラメータのみ受け付けます。

dhcpd option 66 | 150 コマンドに IP アドレスを指定するときには、次のガイドラインに従ってください。

- TFTP サーバが DHCP サーバ インターフェイス上にある場合、TFTP サーバのローカル IP アドレスを使用します。
- TFTP サーバが DHCP サーバ インターフェイスよりもセキュリティが低いインターフェイス上にある場合は、一般の発信ルールが適用されます。DHCP クライアント用の NAT エントリ、グローバル エントリ、およびアクセス リスト エントリを作成し、TFTP サーバの実際の IP アドレスを使用します。
- TFTP サーバがよりセキュリティの高いインターフェイス上にある場合は、一般の着信ルールが適用されます。TFTP サーバ用のスタティック ステートメントとアクセス リスト ステートメントのグループを作成し、TFTP サーバのグローバル IP アドレスを使用します。

その他の DHCP オプションの詳細については、RFC 2132 を参照してください。

(注) ASA は、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。たとえば、**dhcpd option 46 ascii hello** コマンドを入力できます。RFC 2132 では、オプション 46 は 1 桁の 16 進数値として定義されていますが、ASA はこのコンフィギュレーションを受け入れます。

dhcpd option コマンドで次の DHCP オプションは設定できません。

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD

オプション コード	説明
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

例

次に、DHCP オプション 66 に TFTP サーバを指定する例を示します。

```
ciscoasa(config)# dhcpd option 66 ascii MyTftpServer
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd ping_timeout

DHCP ping のデフォルト タイムアウトを変更するには、グローバル コンフィギュレーション モードで **dhcpd ping_timeout** 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。

dhcpd ping_timeout *number* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
number	ミリ秒単位の ping タイムアウト値。最小値は 10、最大値は 10000 です。デフォルトは 50 です。

デフォルト

number のデフォルトのミリ秒は 50 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	• 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

アドレスの競合を避けるため、DHCP サーバは、アドレスを DHCP クライアントに割り当てる前に 2 つの ICMP ping パケットをアドレスに送信します。ASA は、DHCP クライアントに IP アドレスを割り当てる前に、両方の ICMP ping パケットがタイムアウトになるのを待ちます。たとえば、デフォルト値が使用された場合、ASA は IP アドレスを割り当てる前に、1500 ミリ秒（各 ICMP ping パケットに対して 750 ミリ秒）待ちます。

ping のタイムアウト値が長いと、DHCP サーバのパフォーマンスに悪影響を及ぼす場合があります。

例

次に、**dhcpd ping_timeout** コマンドを使用して、DHCP サーバの ping タイムアウト値を変更する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd reserve-address

インターフェイスの DHCP アドレスを予約するには、グローバル コンフィギュレーション モードで **dhcpd reserved-address** コマンドを使用します。既存の DHCP アドレス予約を削除するには、このコマンドの **no** 形式を使用します。

dhcpd reserve-address *ip_address mac_address if_name*

no dhcpd reserve_address *ip_address mac_address if_name*

構文の説明

ip_address	クライアントの MAC アドレスに基づいて DHCP クライアントに割り当てられたアドレスプールの IP アドレス。
mac_address	クライアントの MAC アドレス。
if_name	IP アドレスを予約するインターフェイス。

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
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
9.13(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

予約済みアドレスは設定済みのアドレスプールから取得する必要があり、アドレスプールは ASA インターフェイスと同じサブネット上にある必要があります。トランスペアレントモードでは、ブリッジ グループ メンバー インターフェイスを指定します。ルーテッドモードでは、ルーテッドインターフェイスまたは BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。

例

次の例では、**dhcpd reserve-address** コマンドを使用して、クライアントの MAC アドレスに基づきアドレスプールからクライアントに特定のアドレスを割り当てる方法について示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd enable inside
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

関連コマンド

コマンド	説明
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd update dns

DHCP サーバによる DDNS アップデートの実行をイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd update dns** コマンドを使用します。DHCP サーバによる DDNS 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。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

構文の説明

both	DHCP サーバが A と PTR の両方の DNS RR を更新するように指定します。
interface	DDNS 更新が適用される ASA インターフェイスを指定します。
override	DHCP サーバが DHCP クライアント要求を上書きするように指定します。
srv_ifc_name	このオプションを適用するインターフェイスを指定します。

デフォルト

デフォルトでは、DHCP サーバは PTR RR 更新のみを実行します。

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	—

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。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。更新は DHCP サーバと連携して実行されます。**dhcpd update dns** コマンドはサーバによる更新をイネーブルにします。

名前とアドレスのマッピングは、次の 2 タイプの RR に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

dhcpd update dns コマンドを使用すると、DHCP サーバが A RR と PRT RR の両方の更新、または PTR RR 更新のみを実行するように設定できます。DHCP クライアントからの更新要求を上書きするように設定することもできます。

例

次に、DDNS サーバが DHCP クライアントからの要求を上書きし、A と PTR の両方のアップデートを実行するよう設定する例を示します。

```
ciscoasa(config)# dhcpd update dns both override
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update	DDNS アップデート方式を ASA インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcpd wins

DHCP クライアントに対して WINS サーバ IP アドレスを定義するには、グローバル コンフィギュレーション モードで **dhcpd wins** コマンドを使用します。コンフィギュレーションから WINS サーバ IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

dhcpd wins *server1* [*server2*] [**interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
server1	プライマリの Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。
server2	（任意）代替の Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。

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
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。

使用上のガイドライン

dhcpd wins コマンドは、DHCP クライアント用の WINS サーバのアドレスを指定します。**no dhcpd wins** コマンドは、コンフィギュレーションから WINS サーバの IP アドレスを削除します。

例

次に、DHCP クライアントに送信される WINS サーバ情報を指定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
```

```
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd dns	DHCP クライアントに対して DNS サーバを定義します。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcprelay enable

DHCP リレー エージェントをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcprelay enable** コマンドを使用します。DHCP リレー エージェン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。

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

構文の説明

interface_name	DHCP リレー エージェントがクライアント要求を受け入れるインターフェイスの名前。

デフォルト

DHCP リレー エージェント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
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
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

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

ASA が **dhcprelay enable** *interface_name* コマンドを使用して DHCP リレー エージェントを開始するには、**dhcprelay server** コマンドがコンフィギュレーションにすでに存在している必要があります。このコマンドがない場合、ASA は次に示すようなエラー メッセージを表示します。

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

次の条件下では、DHCP リレーをイネーブルにできません。

- 同じインターフェイス上で DHCP リレーと DHCP リレー サーバをイネーブルにすることはできません。
- 同じインターフェイス上で DHCP リレーと DHCP サーバ（**dhcpd enable**）をイネーブルにすることはできません。

- DHCP サーバもイネーブルになっている場合、DHCP リレー エージェントをイネーブルにできません。
- マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP リレーをイネーブルにすることはできません。

no dhcprelay enable *interface_name* コマンドは、*interface_name* 引数で指定されたインターフェイスの DHCP リレー エージェント コンフィギュレーションだけを削除します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントを ASA の外部インターフェイスに設定し、クライアント要求を ASA の内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

次に、DHCP リレー エージェントをディセーブルにする例を示します。

```
ciscoasa(config)# no dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcp relay	DHCP リレー エージェントのデバッグ情報を表示します。
dhcprelay server	DHCP リレー エージェントが DHCP 要求を転送する DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay information trust-all

指定されたインターフェイスを信頼できるインターフェイスとして設定するには、グローバル コンフィギュレーション モードで **dhcprelay information trust-all** コマンドを使用します。

dhcprelay information trust-all

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

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。

コマンド モード	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	
	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
9.1(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、特定のインターフェイスを信頼できるインターフェイスとして設定します。インターフェイス固有の信頼できるコンフィギュレーションを表示するには、インターフェイス コンフィギュレーション モードで **show running-config dhcprelay interface** コマンドを使用します。インターフェイス コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**dhcprelay information trusted** コマンドを使用します。グローバル コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**show running-config dhcprelay** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで指定のインターフェイスを信頼できるインターフェイスとして設定する例を示します。

```
ciscoasa(config-if)# interface vlan501
ciscoasa(config-if)# nameif inside
ciscoasa(config)# dhcprelay information trust-all
ciscoasa(config)# show running-config dhcprelay
dhcprelay information trust-all
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay information trusted

指定されたインターフェイスを信頼できるインターフェイスとして設定するには、インターフェイス コンフィギュレーション モードで **dhcprelay information trusted** コマンドを使用します。

dhcprelay information trusted

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

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
9.1(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、特定のインターフェイスを信頼できるインターフェイスとして設定します。インターフェイス固有の信頼できるコンフィギュレーションを表示するには、インターフェイス コンフィギュレーション モードで **show running-config dhcprelay interface** コマンドを使用します。グローバル コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**dhcprelay information trust-all** コマンドを使用します。グローバル コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**show running-config dhcprelay** コマンドを使用します。

例

次に、指定されたインターフェイスを信頼できるインターフェイスとして設定する例を示します。

```
ciscoasa(config-if)# interface gigabitEthernet 0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay information trusted
ciscoasa(config)# show running-config dhcprelay
interface gigabitEthernet 0/0
nameif inside
dhcprelay information trusted
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server（グローバル）

DHCP 要求の転送先の DHCP サーバを指定するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP サーバを DHCP リレー コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

dhcprelay server [*interface_name*]

no dhcprelay server [*interface_name*]

構文の説明

interface_name	DHCP サーバが常駐する ASA インターフェイスの名前を指定します。

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。

コマンド モード	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	
	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
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

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。インターフェイスあたり最大 10 個の DHCP リレー サーバを追加できます。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドを ASA コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上には、DHCP クライアントを設定できません。

dhcprelay server コマンドは、指定したインターフェイス上で UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントを ASA の outside インターフェイスに設定し、クライアント要求を ASA の inside インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
```

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server（インターフェイス）

DHCP 要求の転送先の DHCP リレー インターフェイス サーバを指定するには、インターフェイス コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP リレー インターフェイス サーバを DHCP リレー コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

dhcprelay server *ip_address*

no dhcprelay server *ip_address*

構文の説明

ip_address	DHCP リレー エージェントがクライアント DHCP 要求を転送する DHCP リレー インターフェイス サーバの IP アドレスを指定します。

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
9.1(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

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。インターフェイスあたり最大 4 つの DHCP リレー サーバを追加できます。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドを ASA コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上には、DHCP クライアントを設定できません。

dhcprelay server コマンドは、指定したインターフェイス上で UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。

インターフェイス コンフィギュレーション モードでは、**dhcprelay server** *ip_address* コマンドを使用して、インターフェイスごとに DHCP リレー サーバ（ヘルパーと呼ばれる）アドレスを設定できます。これは、インターフェイスで DHCP 要求を受信し、ヘルパー アドレスが設定されている場合、その要求はそれらのサーバにのみ転送されることを意味します。

no dhcprelay server *ip_address* コマンドを使用すると、インターフェイスはそのサーバへの DHCP パケットの転送を停止し、*ip_address* 引数で指定されている DHCP サーバの DHCP リレー エージェント コンフィギュレーションを削除します。

このコマンドは、グローバル コンフィギュレーション モードで設定された DHCP リレー サーバより優先されます。つまり、DHCP リレー エージェントは、クライアント検出メッセージを最初に DHCP リレー インターフェイス サーバに、次に DHCP グローバル リレー サーバに転送します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP リレー インターフェイス サーバに対する DHCP リレー エージェントを ASA の outside インターフェイスに設定し、クライアント要求を ASA の inside インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# interface vlan 10
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay server 10.1.1.1
ciscoasa(config-if)# exit
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay enable inside
dhcprelay timeout 90

interface vlan 10
nameif inside
dhcprelay server 10.1.1.1
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server (vti tunnel)

VTI トンネルインターフェイスを介して DHCP リレーサーバに到達するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。

dhcprelay server *ip_address vti-ifc-name*

構文の説明

ip_address	クライアント DHCP 要求を転送する DHCP リレーサーバの IP アドレスを指定します。
vti-ifc-name	DHCP リレーエージェントが DHCP サーバに DHCP パケットを転送する VTI インターフェイスの名前を指定します。

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
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
9.14(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

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。ただし、リレーエージェントは物理インターフェイスでのみ設定できます。VTI インターフェイスは論理インターフェイスであったため、DHCP リレー要求を転送できませんでした。

ASA 9.14(1) 以降は、このコマンドを使用して、DHCP リレーサーバが VTI トンネルインターフェイスを介してパケットを転送できます。

例

次の例では、DHCP リレーエージェントを VTI トンネルで設定する方法について示します。まず、次のように VTI トンネルを作成します。

```
ciscoasa(config)# interface Tunnel100
ciscoasa(config-if)# nameif vti
ciscoasa(config-if)# ip address 10.1.1.10 255.255.255.0
ciscoasa(config-if)# tunnel source interface outside
ciscoasa(config-if)# tunnel destination 192.168.2.111
```

```
ciscoasa(config-if)# tunnel mode ipsec ipv4
ciscoasa(config-if)# tunnel protection ipsec profile PROFILE1
```

ここで、トンネル名を使用して DHCP リレーサーバを設定します。

```
ciscoasa(config)# dhcprelay server 192.168.3.112 vti
```

dhcprelay setroute

DHCP 応答にデフォルト ゲートウェイ アドレスを設定するには、グローバル コンフィギュレーション モードで **dhcprelay setroute** コマンドを使用します。デフォルト ル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。

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

構文の説明

interface	最初のデフォルト IP アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように DHCP リレー エージェントを設定します。

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
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
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

このコマンドを使用すると、DHCP 応答のデフォルト IP アドレスは、指定された ASA インターフェイスのアドレスに置き換えられます。**dhcprelay setroute** *interface* コマンドを使用すると、DHCP リレー エージェントが最初のデフォルト ルータ アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように設定できます。

パケット内にデフォルトのルータ オプションがない場合、ASA は *interface* アドレスを含むデフォルト ルータを追加します。その結果、クライアントは自分のデフォルト ルートが ASA に向かうように設定できます。

dhcprelay setroute *interface* コマンドを設定しない場合（かつパケット内にデフォルトのルータ オプションがある場合）、パケットは、ルータ アドレスが変更されないまま ASA を通過します。

例

次に、DHCP 応答のデフォルト ゲートウェイを外部 DHCP サーバから ASA の inside インターフェイスに設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay setroute inside
ciscoasa(config)# dhcprelay enable inside
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay timeout

DHCP リレー エージェントのタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **dhcprelay timeout** コマンドを使用します。タイムアウト値を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。

dhcprelay timeout *seconds*

no dhcprelay timeout

構文の説明

seconds	DHCP リレー アドレス ネゴシエーション用に許可されている時間（秒）を指定します。

デフォルト

DHCP リレー タイムアウトのデフォルト値は 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
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
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

dhcprelay timeout コマンドは、DHCP サーバからの応答がリレー バインディング構造を通して DHCP クライアントに進むことが許されている時間を秒単位で設定します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントを ASA の外部インターフェイスに設定し、クライアント要求を ASA の内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求を転送する DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dialog

WebVPN ユーザに表示されるダイアログボックス メッセージ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 **dialog** 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。

dialog {**title** | **message** | **border**} **style** *value*

no dialog {**title** | **message** | **border**} **style** *value*

構文の説明

border	境界線への変更を指定します。
message	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。
title	タイトルへの変更を指定します。
value	表示する実際のテキストまたは CSS パラメータ（最大 256 文字）。

デフォルト

デフォルトのタイトルのスタイルは background-color:#669999;color:white です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:black です。

デフォルトの境界線のスタイルは border:1px solid black;border-collapse:collapse 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
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、任意の有効な 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 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 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目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、ダイアログボックス メッセージの文字表示色を青色に変更するよう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)# dialog message 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。
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。

diameter

カスタム Diameter 属性値ペア（AVP）を Diameter インスペクション クラスまたはポリシー マップに使用するために作成するには、**diameter** コマンドを使用します。既存のカスタム AVP を削除するには、このコマンドの **no** 形式を使用します。

diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

no diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

構文の説明

name	作成するカスタム AVP の名前（最大 32 文字）。Diameter インスペクション ポリシー マップまたはクラス マップでの **match avp** コマンドでこの名前を参照します。
code *value*	256-4294967295 からのカスタム AVP コード値。システムで定義済みのコードとベンダー ID の組み合わせを入力することはできません。
data-type *type*	AVP のデータ型。次のいずれかの型で AVP を定義できます。新しい AVP が別の型の場合は、その型のカスタム AVP は作成できません。 – **address**：IP アドレスの場合。 – **diameter-identity**：Diameter ID データ。 – **diameter-uri**：Diameter の Uniform Resource Identifier（URI）。 – **float32**：32 ビット浮動小数点。 – **float64**：64 ビット浮動小数点。 – **int32**：32 ビット整数。 – **int64**：64 ビット整数。 – **octetstring**：オクテット文字列。 – **time**：時刻値。 – **uint32**：32 ビット符号なし整数。 – **uint64**：64 ビット符号なし整数。
vendor-id *id_number*	（任意）AVP を定義したベンダーの 0 ～ 4294967295 の ID 番号。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
description *text*	（任意）AVP の説明（最大 80 文字）。スペースを含める場合は、説明を引用符で囲みます。

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。

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

新しい属性値ペア（AVP）が定義され、登録されると、カスタム Diameter AVP を作成して、Diameter インスペクション ポリシー マップにそれらを定義し、使用することができます。RFC または AVP を定義するその他のソースから AVP の作成に必要な情報を取得します。

カスタム AVP は、AVP 照合用の Diameter インスペクション ポリシー マップまたはクラス マップで使用する場合にのみ、作成します。

例

次に、カスタム AVP の作成方法と、Diameter インスペクション ポリシー マップでの使用方法の例を示します。

```
ciscoasa(config)# diameter avp eg_custom_avp code 9999 data-type int32
ciscoasa(config)# policy-map type inspect diameter avp-filter-pmap
asa3(config-pmap)# match avp eg_custom_avp
```

関連コマンド

コマンド	説明
class-map type inspect diameter	Diameter インスペクション クラス マップを作成します。
match avp	Diameter 属性値ペア（AVP）を照合します。
policy-map type inspect diameter	Diameter インスペクション ポリシー マップを作成します。

dir

ディレクトリの内容を表示するには、特権 EXEC モードで **dir** コマンドを使用します。

dir [/all] [**all-filesystems**] [**/recursive**] [**disk0: | disk1: | flash: | system:**] [*path]*

構文の説明

/all	(任意)すべてのファイルを表示します。
/recursive	(任意)ディレクトリの内容を再帰的に表示します。
all-filesystems	(任意)すべてのファイル システムのファイルを表示します。
disk0:	(任意)内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	(任意)外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	(任意)デフォルト フラッシュ パーティションのディレクトリの内容を表示します。
path	(任意)特定のパスを指定します。
system:	(任意)ファイル システムのディレクトリの内容を表示します。

デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

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	—	• 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

キーワードまたは引数のない **dir** コマンドは、現在のディレクトリの内容を表示します。

例

次に、ディレクトリの内容を表示する例を示します。

```
ciscoasa# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次に、ファイル システム全体の内容を再帰的に表示する例を示します。

```
ciscoasa# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次に、フラッシュ パーティションの内容を表示する例を示します。

```
ciscoasa# dir flash:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。
mkdir	ディレクトリを作成します。
rmdir	ディレクトリを削除します。

director-localization

ディレクタのローカリゼーションを有効にして、データセンターのサイト間クラスタリングのパフォーマンスを向上させ、ラウンドトリップ時間の遅延を減らすには、クラスタ グループ コンフィギュレーション モードで **director-localization** コマンドを使用します。ディレクタのローカリゼーション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。

director-localization

no director-localization

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。

コマンド デフォルト

このコマンドは、デフォルトで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
クラスタ グループ 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
9.7(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

通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。ただし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。

ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。

次のトラフィック タイプは、ローカリゼーションをサポートしていません：NAT および PAT トラフィック、SCTP 検査されたトラフィック、フラグメンテーション所有クエリ。

例

次に、cluster1 のディレクタのローカリゼーションをイネーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# director-localization
ciscoasa(cfg-cluster)# enable noconfirm
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループ コンフィギュレーション モードを開始します。
show asp table cluster chash	ローカル cHash テーブルを表示します。
show conn	conn フラグ「l」は、スタブ フローがローカル ディレクタ「Yl」または ローカル バックアップ「yl」であることを示します。
site-id	サイト間クラスタリングで使用するクラスタ ユニットのサイト ID を設定します。

disable（キャッシュ）

WebVPN に対するキャッシングをディセーブルにするには、キャッシュ コンフィギュレーション モードで **disable** コマンドを使用します。キャッシングを再度イネーブルにするには、このコマンドの **no** 形式を使用します。

disable

no disable

デフォルト

キャッシングは、各キャッシュ属性に対するデフォルトの設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	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
キャッシュ 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

キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。キャッシングにより、WebVPN とリモート サーバおよびエンド ユーザのブラウザの両方の間のトラフィックが削減されて、多くのアプリケーションの実行効率が大幅に向上されます。

例

次に、キャッシングをディセーブルにしてから、それを再度イネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# disable
ciscoasa(config-webvpn-cache)# no disable
ciscoasa(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	webvpn キャッシュ コンフィギュレーション モードを開始します。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。

コマンド	説明
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

disable（特権 EXEC）

特権 EXEC モードを終了してユーザ EXEC モードに戻るには、特権 EXEC モードで **disable** コマンドを使用します。

disable

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

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
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
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

enable コマンドを使用して、特権モードを開始します。**disable** コマンドは、特権モードを終了して、ユーザ モードに戻ります。

（注） ユーザ名を使用して ASA にログインしている場合、**disable** と入力するとユーザ ID がデフォルトの enable_1 ユーザ名に変更されます。

例

次の例は、特権モードを開始する方法を示しています。

```
ciscoasa> enable
ciscoasa#
```

次に、特権モードを終了する例を示します。

```
ciscoasa# disable
ciscoasa>
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードを有効にします。

disable service-settings（廃止）

電話プロキシ機能の使用時に IP 電話のサービス設定をディセーブルにするには、電話プロキシ コンフィギュレーション モードで **disable service-settings** コマンドを使用します。IP 電話の設定を保持するには、このコマンドの **no** 形式を使用します。

disable service-settings

no disable service-settings

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

サービス設定はデフォルトで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
Phone-Proxy 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
8.0(4)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

デフォルトでは、次の設定内容が IP 電話ではディセーブルになります。

- PC Port
- Gratuitous ARP
- Voice VLAN Access
- Web Access
- Span to PC Port

設定されている各 IP フォンの CUCM で設定されている設定を保持するには、**no disable service-settings** コマンドを設定します。

例

次に、ASA で電話プロキシ機能を使用する IP Phone の設定を保持する例を示します。

```
ciscoasa(config-phone-proxy)# no disable service-settings
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
show phone-proxy	Phone Proxy 固有の情報を表示します。

display

ASA が DAP 属性データベースに書き込む属性値のペアを表示するには、DAP テスト属性モードで **display** コマンドを入力します。

display

コマンド デフォルト

デフォルトの値や動作はありません。

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
Dap テスト属性	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(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

通常、ASA は AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。ASA は、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。**display** コマンドを使用すると、これらの属性をコンソールに表示できます。

関連コマンドl

コマンド	説明
attributes	属性コンフィギュレーション モードを開始します。このモードでは属性値のペアを設定できます。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性サブモードを開始します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセスポリシーをコンソールに表示します。

distance

IS-IS プロトコルによって検出されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義するには、ルータ ISIS コンフィギュレーション モードで **distance** コマンドを使用します。コンフィギュレーション ファイルから distance コマンドを削除して、ソフトウェアがディスタンス定義を削除するようにシステムをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

distance *weight* **ip**

no distance *weight* **ip**

構文の説明

weight	IS-IS ルートに割り当てるアドミニストレーティブ ディスタンスです。指定できる範囲は 1 ～ 255 です。
ip	IP から取得されるルートに適用する距離です。

デフォルト

デフォルトは 115 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
9.6(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

アドミニストレーティブ ディスタンスは、1 ～ 255 の数値です。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブ ディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。重み値は主観的に選択します。重み値を選択するための定量的方法はありません。

distance コマンドは、IS-IS ルートがルーティング情報ベース（RIB）に挿入されるときに適用されるアドミニストレーティブ ディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性に影響を与えるために使用します。

例

次に、すべての IS-IS ルートに距離 20 を割り当てる例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)#distance 20 ip
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。

コマンド	説明
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

distance bgp

BGP ルートのアドミニストレーティブ ディスタンスを設定するには、アドレス ファミリ コンフィギュレーション モードで **distance bgp** コマンドを使用します。アドミニストレーティブ ディスタンスを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。

distance bgp *external-distance internal-distance local-distance*

no distance bgp

構文の説明

external-distance	外部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、外部自律システムから学習された場合は外部になります。この引数の値の範囲は 1 ～ 255 です。
internal-distance	内部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、ローカル自律システムのピアから学習された場合は内部です。この引数の値の範囲は 1 ～ 255 です。
local-distance	ローカル BGP ルートのアドミニストレーティブ ディスタンス。別のプロセスから再配布されているルータやネットワークの場合、ローカル ルートとは、**network** ルータ コンフィギュレーション コマンドで、通常はバック ドアとして表示されるネットワークです。この引数の値の範囲は 1 ～ 255 です。

デフォルト

このコマンドを設定しない場合、または no 形式を入力した場合は、次の値が使用されます。

external-distance：20
internal-distance：200
local-distance：200

(注) アドミニストレーティブ ディスタンスが 255 のルートはルーティング テーブルに格納されません。

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	• 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

distance bgp コマンドは、個々のルータやルータのグループなど、ルーティング情報送信元の信頼性の格付けを設定するために使用されます。アドミニストレーティブ ディスタンスを数値で表すと、1 ～ 255 の正の整数です。

通常は、値が大きいほど、信頼性の格付けが下がります。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。他のプロトコルが外部 BGP（eBGP）によって実際に学習されたルートよりも良いルートをノードに提供できることがわかっている場合、または一部の内部ルートが BGP によって優先されるべきである場合、このコマンドを使用します。

注意 内部 BGP ルートのアドミニストレーティブ ディスタンスを変更することは危険と見なされており、推奨されません。不適切な設定により、ルーティング テーブルの不整合性やルーティングの中断が発生する可能性があります。

distance mbgp コマンドは、**distance bgp** コマンドに置き換わりました。

例

次の例では、外部ディスタンスを 10、内部ディスタンスを 50、ローカル ディスタンスを 100 に設定しています。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# distance bgp 10 50 100
ciscoasa(config-router-af)# end
```

distance eigrp

内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定するには、ルータ コンフィギュレーション モードで **distance eigrp** 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。

distance eigrp *internal-distance external-distance*

no distance eigrp

構文の説明

external-distance	EIGRP 外部ルートのアドミニストレーティブ ディスタンス。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効な値は、1 ～ 255 です。
internal-distance	EIGRP 内部ルートのアドミニストレーティブ ディスタンス。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効な値は、1 ～ 255 です。

デフォルト

デフォルト値は次のとおりです。

- *external-distance* は 170 です。
- *internal-distance* は 90 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
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

各ルーティング プロトコルには、他のルーティング プロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティング プロトコルによって生成された同じ宛先への 2 つのルートのいずれが「最適パス」であるかは、必ずしも判別できません。アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先に複数の異なるルートがある場合に、ASA が最適なパスの選択に使用するルート パラメータです。

ASA で複数のルーティング プロトコルが実行されている場合、**distance eigrp** コマンドを使用して、EIGRP ルーティング プロトコルが検出するルートのデフォルト アドミニストレーティブ ディスタンスを、他のルーティング プロトコルと関連付けて調整できます。表12-1 に、ASA でサポートされているルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンスを示します。

表12-1　デフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP 集約ルート	5
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
不明（Unknown）	255

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、内部と外部の両方の EIGRP ルートのアドミニストレーティブ ディスタンスがデフォルトに戻されます。

例

次に、**distance eigrp** コマンドを使用して、すべての EIGRP 内部ルートのアドミニストレーティブ ディスタンスを 80 に、すべての EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定する例を示します。EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定すると、EIGRP によって検出されたルートが、RIP（OSPF ではなく）によって検出された同じルートを経由する特定の宛先設定に渡されます。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.7.0
ciscoasa(config-router)# network 172.16.0.0
ciscoasa(config-router)# distance eigrp 90 115
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

distance ospf（IPv6 ルータ OSPF）

ルート タイプに基づいて OSPFv3 ルートのアドミニストレーティブ ディスタンスを定義するには、IPv6 ルータ OSPF コンフィギュレーション モードで **distance** 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。

distance [**ospf** {**external** | **intra-area** | **inter-area**}] *distance*

no distance [**ospf** {**external** | **intra-area** | **inter-area**}] *distance*

構文の説明

distance	アドミニストレーティブディスタンスを指定します。有効値の範囲は 10 ～ 254 です。
external	（オプション）OSPFv3 ルートに外部タイプ 5 およびタイプ 7 のルートを指定します。
inter-area	（オプション）OSPFv3 ルートにエリア間ルートを指定します。
intra-area	（オプション）OSPFv3 ルートにエリア内ルートを指定します。
ospf	（オプション）OSPFv3 ルートにアドミニストレーティブ ディスタンスを指定します。

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
IPv6 ルータ OSPF 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
9.0(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

OSPFv3 ルートのアドミニストレーティブ ディスタンスを設定するには、このコマンドを使用します。

例

次に、OSPFv3 に対して外部タイプ 5 およびタイプ 7 のルートのアドミニストレーティブ ディスタンスを 200 に設定する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# distance ospf external 200
```

関連コマンド

コマンド	説明
default-information originate	OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成します。
redistribute	あるルーティング ドメインから別のルーティング ドメインへ IPv6 ルートを再配布します。

distance ospf（ルータ OSPF）

ルート タイプに基づいて OSPFv2 ルートのアドミニストレーティブ ディスタンスを定義するには、ルータ OSPF コンフィギュレーション モードで **distance ospf** 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。

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]

no distance ospf

構文の説明

d1、*d2*、*d3*	各ルート タイプの距離を指定します。有効値の範囲は、1 ～ 255 です。
external	（任意）再配布によって取得した他のルーティング ドメインからのルートに距離を設定します。
inter-area	（任意）あるエリアから別のエリアまでのルートすべての距離を設定します。
intra-area	（任意）あるエリア内のすべてのルートの距離を設定します。

デフォルト

d1、*d2*、および *d3* のデフォルト値は 110 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 OSPF 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

少なくとも 1 つのキーワードと引数を指定する必要があります。アドミニストレーティブ ディスタンスのタイプごとにコマンドを個別に入力することができますが、コンフィギュレーションでは 1 つのコマンドとして表示されます。アドミニストレーティブ ディスタンスを再入力する場合、対象ルート タイプのアドミニストレーティブ ディスタンスだけが変更されます。その他のルート タイプのアドミニストレーティブ ディスタンスは影響されません。

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、すべてのルート タイプのアドミニストレーティブ ディスタンスがデフォルトに戻されます。複数のルート タイプを設定している場合、1 つのルート タイプをデフォルトのアドミニストレーティブ ディスタンスに戻すには、次のいずれかを実行します。

- ルート タイプを、手動でデフォルト値に設定します。
- このコマンドの **no** 形式を使用してコンフィギュレーション全部を削除し、保持するルート タイプに対してコンフィギュレーションを再入力します。

例

次に、外部ルートのアドミニストレーティブ ディスタンスを 150 に設定する例を示します。

```
ciscoasa(config-router)# distance ospf external 105
ciscoasa(config-router)#
```

次に、各ルート タイプに入力した個別のコマンドが、ルータ コンフィギュレーションで 1 つのコマンドとして表示される例を示します。

```
ciscoasa(config-rtr)# distance ospf intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf intra-area 105
ciscoasa(config-rtr)# distance ospf external 105
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
ciscoasa(config)#
```

次に、各アドミニストレーティブ ディスタンスを 105 に設定し、次に外部アドミニストレーティブ ディスタンスのみを 150 に変更する例を示します。**show running-config router ospf** コマンドは、外部ルート タイプの値だけが変更され、その他のルート タイプでは以前に設定された値が保持されている状況を示します。

```
ciscoasa(config-rtr)# distance ospf external 105 intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf external 150
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
ciscoasa(config)#
```

関連コマンド

コマンド	説明
router ospf	OSPFv2 のルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションの OSPFv2 コマンドを表示します。

distribute-list

Open Shortest Path First（OSPF）アップデートで受信または転送されるネットワークをフィルタリングするには、ルータ OSPF コンフィギュレーション モードで **distribute-list** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの no 形式を使用します。

distribute-list *access-list name* [**in** |**out**] [**interface** *if_name*]

no distribute-list *access-list name* [**in** |**out**]

構文の説明

access-list name	標準 IP アクセス リスト名。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。
in	アクセス リストまたはルート ポリシーを着信ルーティング アップデートに適用します。
out	発信ルーティング アップデートにアクセス リストまたはルート ポリシーを適用します。**out** キーワードは、ルータ コンフィギュレーション モードでだけ使用可能です。
interface *if_name*	（オプション）ルーティング アップデートを適用するインターフェイス。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。

デフォルト

ネットワークはフィルタリングされません。

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 OSPF 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

インターフェイスが指定されていない場合、アクセス リストはすべての着信更新に適用されます。

例

次に、外部インターフェイスで受信する OSPF ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
ciscoasa(config)# access-list ospf_filter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ospf_filter deny any
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ospf_filter in interface outside
```

関連コマンド

コマンド	説明
distribute-list in	着信ルーティング アップデートをフィルタリングします。
router ospf	OSPF ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

distribute-list in（アドレス ファミリ）

Border Gateway Protocol（BGP）の着信アップデートで受信したルートまたはネットワークをフィルタリングするには、アドレスファミリ コンフィギュレーション モードで **distribute-list in** コマンドを使用します。アドレスファミリ コンフィギュレーション モードにアクセスするには、**router bgp** コマンドを入力します。配布リストを削除し、これを実行コンフィギュレーション ファイルから削除するには、このコマンドの **no** 形式を使用します。

distribute-list {*acl-name* | **prefix** *list-name*} **in**

no distribute-list {*acl-name* | **prefix** *list-name*} **in**

構文の説明

acl-name	標準 IP アクセス リスト名。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。
prefix *list-name*	プレフィックス リストの名前。プレフィックス リストは、一致プレフィックスに基づいて、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。

デフォルト

このコマンドが、事前定義済みのアクセス リストまたはプレフィックス リストなしで設定されている場合、配布リストではデフォルトですべてのトラフィックが許可されます。

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	• 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

distribute-list in コマンドは、BGP の着信アップデートをフィルタリングするために使用されます。このコマンドを設定する前に、アクセス リストまたはプレフィックス リストを定義する必要があります。標準アクセス リストおよび拡張アクセス リストがサポートされています。IP プレフィックス リストは、プレフィックス ビット長に基づいたフィルタリングに使用されます。ネットワーク全体、サブネット、スーパーネット、または単一のホスト ルートを指定できます。配布リストを設定する場合は、プレフィックス リストとアクセス リストのコンフィギュレーションは相互に排他的です。配布リストを有効にする前に、**clear bgp** コマンドを使用してセッションをリセットする必要があります。

例

次の例では、プレフィックス リストと配布リストを定義して、ネットワーク 10.1.1.0/24、ネットワーク 192.168.1.0、およびネットワーク 10.108.0.0 からのトラフィックだけを受け入れるように BGP ルーティング プロセスを設定しています。着信ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# ip prefix-list RED permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list RED permit 10.108.0.0/16
ciscoasa(config)# ip prefix-list RED permit 192.168.1.0/24
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list prefix RED in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

次の例では、アクセス リストと配布リストを定義して、ネットワーク 192.168.1.0 およびネットワーク 10.108.0.0 からのトラフィックだけを受け入れるように BGP ルーティング プロセスを設定しています。着信ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.1.0 255.255.255.0
ciscoasa(config)# access-list distribute-list-acl permit 10.108.0.0 255.255.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list distribute-list-acl in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

関連コマンド

コマンド	説明
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。
ip prefix-list	プレフィックス リストを作成したり、プレフィックス リスト エントリを追加したりします。

distribute-list in（ルータ）

着信ルーティング アップデートをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list in** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

distribute-list *acl* **in** [**interface** *if_name*]

no distribute-list *acl* **in** [**interface** *if_name*]

構文の説明

acl	標準アクセス リスト名。
interface *if_name*	（オプション）着信ルーティング アップデートを適用するインターフェイス。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。

デフォルト

着信更新の場合、ネットワークはフィルタリングされません。

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	—

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。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての着信更新に適用されます。

例

次に、外部インターフェイスで受信する RIP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
ciscoasa(config)# access-list ripfilter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter deny any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter in interface outside
```

次に、外部インターフェイスで受信する EIGRP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
ciscoasa(config)# access-list eigrp_filter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list eigrp_filter deny any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter in interface outside
```

関連コマンド

コマンド	説明
distribute-list out	発信ルーティング アップデートをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

distribute-list out（アドレス ファミリ）

Border Gateway Protocol（BGP）の発信アップデートでネットワークがアドバタイズされないように抑制するには、アドレスファミリ コンフィギュレーション モードで **distribute-list out** コマンドを使用します。アドレスファミリ コンフィギュレーション モードにアクセスするには、**router bgp** コマンドを入力します。配布リストを削除し、これを実行コンフィギュレーション ファイルから削除するには、このコマンドの **no** 形式を使用します。

distribute-list {*acl-name* | **prefix** *list-name*} **out** [*protocol process-number* | **connected** | **static**]

no distribute-list {*acl-name* | **prefix** *list-name*} **out** [*protocol process-number* | **connected** | **static**]

構文の説明

acl-name	標準 IP アクセス リスト名。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。
prefix *list-name*	プレフィックス リストの名前。プレフィックス リストは、一致プレフィックスに基づいて、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。
protocol process-number	配布リストに適用するルーティング プロトコルを指定します。BGP、EIGRP、OSPF、および RIP がサポートされています。RIP を除くすべてのルーティング プロトコルについて、プロセス番号を入力します。プロセス番号は、1 ～ 65 までの値です。
connected	接続ルートを通じて学習したピアおよびネットワークを指定します。
static	スタティック ルートを通じて学習したピアおよびネットワークを指定します。

デフォルト

このコマンドが、事前定義済みのアクセス リストまたはプレフィックス リストなしで設定されている場合、配布リストではデフォルトですべてのトラフィックが許可されます。

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	• 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

distribute-list out コマンドは、BGP の発信アップデートをフィルタリングするために使用されます。このコマンドを設定する前に、アクセス リストまたはプレフィックス リストを定義する必要があります。標準アクセス リストだけがサポートされます。

IP プレフィックス リストは、プレフィックス ビット長に基づいたフィルタリングに使用されます。ネットワーク全体、サブネット、スーパーネット、または単一のホスト ルートを指定できます。配布リストを設定する場合は、プレフィックス リストとアクセス リストのコンフィギュレーションは相互に排他的です。配布リストを有効にする前に、**clear bgp** コマンドを使用してセッションをリセットする必要があります。

protocol 引数または *process-number* 引数（あるいはその両方）を入力すると、配布リストは、指定したルーティング プロセスから派生したルートだけに適用されます。distribute-list コマンドで指定されていないアドレスは、配布リストの設定後、発信ルーティング アップデートでアドバタイズされません。

発信アップデートでネットワークまたはルートが受信されないよう抑制するには、**distribute-list in** コマンドを使用します。

例

次の例では、プレフィックス リストと配布リストを定義して、ネットワーク 192.168.0.0 だけをアドバタイズするように BGP ルーティング プロセスを設定しています。アウトバウンド ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# ip prefix-list BLUE permit 192.168.0.0/16
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list prefix BLUE out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

次の例では、アクセス リストと配布リストを定義して、ネットワーク 192.168.0.0 だけをアドバタイズするように BGP ルーティング プロセスを設定しています。アウトバウンド ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.0.0 255.255.0.0
ciscoasa(config)# access-list distribute-list-acl deny 0.0.0.0 0.0.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list distribute-list-acl out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

関連コマンド

コマンド	説明
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。
ip prefix-list	プレフィックス リストを作成したり、プレフィックス リスト エントリを追加したりします。

distribute-list out（ルータ）

発信ルーティング アップデートをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list out** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

構文の説明

acl	標準アクセス リスト名。
connected	（任意）接続されたルートのみフィルタリングします。
eigrp *as_number*	（任意）指定した自律システム番号からの EIGRP ルートだけをフィルタリングします。*as_number* 引数は、ASA 上の EIGRP ルーティング プロセスの自律システム番号です。
interface *if_name*	（オプション）発信ルーティング アップデートを適用するインターフェイス。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。
ospf *pid*	（任意）指定した OSPF プロセスにより検出された OSPF ルートのみフィルタリングします。
rip	（任意）RIP ルートのみフィルタリングします。
static	（任意）スタティック ルートだけをフィルタリングします。

デフォルト

送信更新の場合、ネットワークはフィルタリングされません。

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	—	—

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。
8.0(2)	**eigrp** キーワードが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての発信更新に適用されます。

例

次に、任意のインターフェイスから送信された RIP 更新で 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
ciscoasa(config)# access-list ripfilter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter permit any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter out
```

次に、EIGRP ルーティング プロセスで外部インターフェイスの 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
ciscoasa(config)# access-list eigrp_filter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list eigrp_filter permit any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter out interface outside
```

関連コマンド

コマンド	説明
distribute-list in	着信ルーティング アップデートをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。