CHAPTER 8

client access rule コマンド～ crl configure コマンド

client-access-rule

リモートアクセス クライアントのタイプを制限する規則およびセキュリティ アプライアンスを通して IPSec 経由で接続できるバージョンを設定するには、グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用します。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。

すべてのルールを削除するには、priority 引数だけを指定して **no client-access-rule command** コマンドを使用します。これにより、**client-access-rule none** コマンドを発行して作成されたヌル ルールを含む、設定済みのすべてのルールが削除されます。

クライアント アクセス ルールがない場合、ユーザはデフォルトのグループ ポリシー内に存在するすべてのルールを継承します。ユーザがクライアント アクセス ルールを継承しないようにするには、**client-access-rule none** コマンドを使用します。これにより、すべてのクライアント タイプおよびバージョンが接続できるようになります。

client-access-rule *priority* **{permit | deny} type** *type* **version** *version* **| none**

no client-access-rule *priority* [**{permit | deny} type** *type* **version** *version*]

構文の説明

deny	特定のタイプとバージョンのデバイスの接続を拒否します。
none	クライアント アクセス ルールを許可しません。client-access-rule をヌル値に設定します。これにより制限が許可されなくなります。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンのデバイスの接続を許可します。
priority	ルールのプライオリティを決定します。最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアントのタイプとバージョン（またはこのいずれか）に一致する最も小さい整数のルールが、適用されるルールとなります。プライオリティの低いルールに矛盾がある場合、セキュリティ アプライアンスはそのルールを無視します。
type *type*	VPN 3002 などの自由形式のストリングを使用して、デバイス タイプを指定します。文字列は、* 文字をワイルドカードとして使用できる点を除き、**show vpn-sessiondb remote** で表示される値と完全に一致する必要があります。
version *version*	7.0 などの自由形式のストリングを使用して、デバイス バージョンを指定します。文字列は、* 文字をワイルドカードとして使用できる点を除き、**show vpn-sessiondb remote** で表示される値と完全に一致する必要があります。

デフォルト

デフォルトでは、アクセス ルールはありません。

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	透過	シングル	マルチ	
				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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

次の注意に従ってルールを作成します。

- ルールを定義しない場合、セキュリティ アプライアンスはすべての接続タイプを許可します。
- クライアントがいずれのルールにも一致しない場合、セキュリティ アプライアンスは接続を拒否します。つまり、拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。許可ルールを定義しないと、セキュリティ アプライアンスはすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントの両方について、タイプおよびバージョンが **show vpn-sessiondb remote** での表示の内容と完全に一致する必要があります。
- ***** 文字はワイルドカードであり、各ルールで複数回使用できます。たとえば、**client-access-rule 3 deny type * version 3.*** は、リリース バージョン 3.x ソフトウェアを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス ルールを作成します。
- 1 つのグループ ポリシーにつき最大 25 のルールを作成できます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプとバージョンを送信しないクライアントに対して n/a を使用できます。

例

次に、FirstGroup という名前のグループ ポリシーのクライアント アクセス ルールを作成する例を示します。これらのルールは、ソフトウェア バージョン 4.1 を実行している VPN クライアントを許可する一方で、すべての VPN 3002 ハードウェア クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client（CTL プロバイダー）

証明書信頼リスト プロバイダーへの接続が許可されるクライアントを指定するか、またはクライアント認証用のユーザ名とパスワードを指定するには、CTL プロバイダー コンフィギュレーション モードで **client** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

no client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

構文の説明

encrypted	パスワードの暗号化を指定します。
interface *if_name*	接続が許可されるインターフェイスを指定します。
ipv4_addr	クライアントの IP アドレスを指定します。
username *user_name*	クライアント認証用のユーザ名を指定します。
password *password*	クライアント認証用のパスワードを指定します。

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	透過	シングル	コンテキスト	システム
CTL プロバイダー コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダーへの接続を許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードを設定するには、CTL プロバイダー コンフィギュレーション モードで **client** コマンドを使用します。複数のコマンドを発行して、複数のクライアントを定義できます。ユーザ名とパスワードは、CallManager クラスタ用の CCM 管理者のユーザ名およびパスワードと一致する必要があります。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

client（TLS プロキシ）

トラストポイント、キー ペア、および暗号スイートを設定するには、TLS プロキシ コンフィギュレーション モードで **client** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]]

no client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]

構文の説明

cipher-suite *cipher_suite*	暗号スイートを指定します。オプションには、des-sha1、3des-sha1、aes128-sha1、aes256-sha1、および null-sha1 が含まれます。
issuer *ca_tp_name*	クライアントのダイナミック証明書を発行するローカル CA トラストポイントを指定します。
keypair *key_label*	クライアントのダイナミック証明書で使用する RSA キー ペアを指定します。
ldc	ローカル ダイナミック証明書の発行者またはキー ペアを指定します。

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	透過	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

TLS プロキシで TLS クライアント ロールを持つセキュリティ アプライアンスの TLS ハンドシェイク パラメータを制御するには、TLS プロキシ コンフィギュレーション モードで **client** コマンドを使用します。これには、暗号スイートのコンフィギュレーションか、ローカル ダイナミック証明書の発行者またはキー ペアの設定が含まれます。クライアントのダイナミック証明書を発行するローカル CA は、**crypto ca trustpoint** コマンドで定義され、トラストポイントでは **proxy-ldc-issuer** を設定するか、デフォルトのローカル CA サーバ（LOCAL-CA-SERVER）を使用する必要があります。

キー ペア値は、**crypto key generate** コマンドを使用して生成されている必要があります。

クライアント プロキシ（サーバに対して TLS クライアントとして機能するプロキシ）の場合、ユーザ定義の暗号スイートによって、デフォルトの暗号スイート、または **ssl encryption** コマンドで定義された暗号スイートが置き換えられます。このコマンドでは、2 つの TLS セッション間で異なる暗号を設定できます。CallManager サーバでは、AES 暗号を使用する必要があります。

例

次の例では、TLS プロキシ インスタンスを作成する方法を示します。

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

client-firewall

IKE トンネルのネゴシエーション時に セキュリティ アプライアンス が VPN クライアントにプッシュするパーソナル ファイアウォール ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を使用します。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを使用します。**client-firewall none** コマンドを発行して作成したヌル ポリシーを含め、すべての設定済みファイアウォール ポリシーが削除されます。

ファイアウォール ポリシーがなくなると、ユーザはデフォルトまたはその他のグループ ポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがそれらのファイアウォール ポリシーを継承しないようにするには、**client-firewall none** コマンドを使用します。

client-firewall none

client-firewall {**opt** | **req**} **custom vendor-id** *num* **product-id** *num* **policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*} [**description** *string*]

client-firewall {**opt** | **req**} **zonelabs-integrity**

（注） ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバによって決められます。

client-firewall {**opt** | **req**} **zonelabs-zonealarm policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **zonelabs-zonealarmorpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **zonelabs-zonealarmpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **cisco-integrated acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **sygate-personal**

client-firewall {**opt** | **req**} **sygate-personal-pro**

client-firewall {**opt** | **req**} **sygate-personal-agent**

client-firewall {**opt** | **req**} **networkice-blackice**

client-firewall {**opt** | **req**} **cisco-security-agent**

構文の説明

acl-in <*acl*>	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out <*acl*>	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。セキュリティ アプライアンスは、ファイアウォールが実行されていることを確認するためのチェックを行います。「Are You There?」と表示され、応答がない場合は、セキュリティ アプライアンスによりトンネルが切断されます。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。

cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアント ファイアウォール ポリシーのソースとしてプッシュされるポリシーを指定します。
custom	カスタム ファイアウォール タイプを指定します。
description <*string*>	ファイアウォールの説明を示します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーをヌル値に設定します。これによりファイアウォール ポリシーが禁止されます。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバ ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

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**	**透過**	**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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**zonelabs-integrity** ファイアウォール タイプが追加されました。

使用上のガイドライン

設定できるのは、このコマンドの 1 つのインスタンスのみです。

例

次に、FirstGroup という名前のグループ ポリシーについて、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client trust-point

Cisco Unified Presence Server（CUPS）の TLS プロキシを設定する場合、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS プロキシ コンフィギュレーション モードで **client trust-point** コマンドを使用します。プロキシ トラストポイント証明書を削除するには、このコマンドの **no** 形式を使用します。

client trust-point *proxy_trustpoint*

no client trust-point [*proxy_trustpoint*]

構文の説明

proxy_trustpoint	**crypto ca trustpoint** コマンドによって定義されるトラストポイントを指定します。

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	透過	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	•	•	•	•	—

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。

使用上のガイドライン

client trust-point コマンドは、セキュリティ アプライアンスが TLS クライアントの役割を果たしている場合に、TLS ハンドシェイク時にセキュリティ アプライアンスが使用するトラストポイントと関連証明書を指定します。証明書は、セキュリティ アプライアンス が所有している必要があります（ID 証明書）。

証明書には、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。**client trust-point** コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

例

次に、client trust-point コマンドを使用して、TLS サーバでの TLS ハンドシェイクでトラストポイント「ent_y_proxy」の使用を指定する例を示します。ハンドシェイクは、エンティティ Y から開始され、TLS サーバが常駐するエンティティ X に対して行われるとします。ASA は、エンティティ Y の TLS プロキシとして機能します。

```
hostname(config-tlsp)# client trust-point ent_y_proxy
```

関連コマンド

コマンド	説明
client（**TLS プロキシ**）	TLS プロキシ インスタンスのトラストポイント、キー ペア、および暗号スイートを設定します。
server trust-point	セキュリティ アプライアンスが TLS サーバの役割を果たす場合、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

client-types（クリプト CA トラスト ポイント）

ユーザ接続に関連付けられた証明書の検証にこのトラストポイントを使用できるクライアント接続タイプを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **client-types command** コマンドを使用します。指定した接続にトラストポイントを使用できないように指定するには、このコマンドの **no** 形式を使用します。

[no] client-types {ssl | ipsec}

構文の説明

ipsec	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを IPSec 接続の検証に使用できることを指定します。
ssl	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを SSL 接続の検証に使用できることを指定します。

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。

コマンド履歴

	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	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

同じ CA 証明書に関連付けられているトラストポイントが複数ある場合、特定のクライアント タイプに設定できるのは 1 つのトラストポイントだけです。ただし、1 つのトラストポイントを 1 つのクライアント タイプに設定し、別のトラストポイントを別のクライアント タイプに設定することができます。

同じ CA 証明書に関連付けられているトラストポイントがあり、これがすでに 1 つのクライアント タイプに設定されている場合は、この同じクライアント タイプ設定に新しいトラストポイントを設定することはできません。このコマンドの no 形式を使用して設定をクリアして、トラストポイントがいずれのクライアント検証にも使用できないようにすることができます。

リモート アクセス VPN では、配置の要件に応じて、Secure Sockets Layer（SSL）VPN、IP Security（IPSec; IP セキュリティ）、またはこの両方を使用して、事実上すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを SSL トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# client-types ssl
hostname(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを IPsec トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# client-types ipsec
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
id-usage	トラストポイントの登録された ID の使用方法を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

client-update

すべてのトンネル グループまたは特定のトンネル グループで、アクティブなすべてのリモート VPN ソフトウェア クライアントとハードウェア クライアント、および Auto Update クライアントとして設定されているセキュリティ アプライアンス用のクライアント更新を発行するには、特権 EXEC モードで **client-update** コマンドを使用します。

クライアント更新のパラメータをグローバル レベル（VPN ソフトウェア クライアントとハードウェア クライアント、および Auto Update クライアントとして設定されているセキュリティ アプライアンスを含む）で設定および変更するには、グローバル コンフィギュレーション モードで **client-update** コマンドを使用します。

VPN ソフトウェア クライアントとハードウェア クライアント用のクライアント更新トンネル グループ IPSec 属性パラメータを設定および変更するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **client-update** コマンドを使用します。

リビジョン番号のリストにあるソフトウェア バージョンをすでに実行しているクライアントの場合は、ソフトウェアを更新する必要はありません。リストにあるソフトウェア バージョンを実行していないクライアントの場合は、ソフトウェアを更新する必要があります。

クライアント更新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。

グローバル コンフィギュレーション モードのコマンドは、次のとおりです。

client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

no client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

トンネル グループ IPSec 属性モードのコマンドは、次のとおりです。

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

特権 EXEC モードのコマンドは、次のとおりです。

client-update {**all** | *tunnel-group*}

no client-update *tunnel-group*

構文の説明

all	（特権 EXEC モードでのみ使用可能）すべてのトンネル グループのすべてのアクティブ リモート クライアントにアクションを適用します。キーワード **all** をこのコマンドの **no** 形式で使用することはできません。
component {**asdm** | **image**}	Auto Update クライアントとして設定されているセキュリティ アプライアンスのソフトウェア コンポーネント。
device-id *dev_string*	固有のストリングで自身を識別するように Auto Update クライアントが設定されている場合は、クライアントが使用するのと同じストリングを指定します。最大で 63 文字です。
enable	（グローバル コンフィギュレーション モードでのみ使用可能）リモート クライアントのソフトウェア更新をイネーブルにします。
family *family_name*	デバイス ファミリで自身を識別するように Auto Update クライアントが設定されている場合は、クライアントが使用するのと同じデバイス ファミリを指定します。これは、asa、pix、または最大 7 文字のテキスト ストリングです。

rev-nums *rev-nums*	（特権 EXEC モードでは使用不可）このクライアントのソフトウェア イメージまたはファームウェア イメージを指定します。Windows、WIN9X、WinNT、および vpn3002 の各クライアントは、任意の順番で 4 つまで、カンマで区切って指定できます。セキュリティ アプライアンスの場合は、1 つしか指定できません。ストリングの最大長は 127 文字です。
tunnel-group	（特権 EXEC モードでのみ使用可能）リモート クライアント更新の有効なトンネル グループの名前を指定します。
type *type*	（特権 EXEC モードでは使用不可）クライアント更新を通知するために、リモート PC のオペレーティング システム、または Auto Update クライアントとして設定されているセキュリティ アプライアンスのタイプを指定します。このリストは、次の内容で構成されます。 • asa5505：Cisco 5505 適応型セキュリティ アプライアンス • asa5510：Cisco 5510 適応型セキュリティ アプライアンス • asa5520：Cisco 5520 適応型セキュリティ アプライアンス • asa5540：Cisco 適応型セキュリティ アプライアンス • linux：Linux クライアント • mac：MAC OS X クライアント • pix-515：Cisco PIX 515 Firewall • pix-515e：Cisco PIX 515E Firewall • pix-525：Cisco PIX 525 Firewall • pix-535：Cisco PIX 535 Firewall • Windows：Windows ベースのすべてのプラットフォーム • WIN9X：Windows 95、Windows 98、および Windows ME プラットフォーム • WinNT：Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム • vpn3002：VPN 3002 ハードウェア クライアント • 最大 15 文字のテキスト ストリング
url *url-string*	（特権 EXEC モードでは使用不可）ソフトウェア イメージまたはファームウェア イメージの URL を指定します。この URL は、クライアントに適合するファイルを指している必要があります。ストリングの最大長は 255 文字です。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec 属性コンフィギュレーション モードが追加されました。
7.2(1)	Auto Update サーバとして設定されたセキュリティ アプライアンスをサポートするために、**component**、**device-id**、および **family** キーワードとその引数が追加されました。

使用上のガイドライン　トンネル グループ ipsec 属性コンフィギュレーション モードでは、この属性を IPSec リモート アクセス トンネル グループ タイプのみに適用できます。

client-update コマンドを使用すると、更新のイネーブル化、更新の適用先となるクライアントのタイプとリビジョン番号の指定、更新の取得元となる URL または IP アドレスの指定を実行できます。また、Windows クライアントの場合は、VPN クライアント バージョンを更新する必要があることを任意でユーザに通知できます。Windows クライアントに対しては、更新を実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアント ユーザに対しては、更新は通知なしで自動的に実行されます。クライアントのタイプが別のセキュリティ アプライアンスである場合は、このセキュリティ アプライアンスが Auto Update サーバとして機能します。

クライアント更新メカニズムを設定するには、次の手順を実行します。

ステップ 1　グローバル コンフィギュレーション モードで、次のコマンドを入力してクライアント更新をイネーブルにします。

```
hostname(config)# client-update enable
hostname(config)#
```

ステップ 2　グローバル コンフィギュレーション モードで、特定のタイプのすべてのクライアントに適用する、クライアント更新用のパラメータを設定します。つまり、クライアントのタイプ、および更新されたイメージの取得元となる URL または IP アドレスを指定します。Auto Update クライアントの場合は、ソフトウェア コンポーネント（ASDM またはブート イメージ）を指定します。また、リビジョン番号も指定する必要があります。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。このコマンドは、セキュリティ アプライアンス全体にわたって、指定したタイプのすべてのクライアントに適用されるクライアント更新パラメータを設定します。次に例を示します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

VPN 3002 ハードウェア クライアントのトンネル グループを設定する場合の図については、「例」の項を参照してください。

（注） すべての Windows クライアントと Auto Update クライアントで、URL のプレフィックスとして、「http://」または「https://」プロトコルを使用する必要があります。VPN3002 ハードウェア クライアントに対しては、代わりにプロトコル「tftp://」を指定する必要があります。

また、Windows クライアントと VPN3002 ハードウェア クライアントでは、特定のタイプのすべてのクライアントではなく、個々のトンネル グループだけのクライアント更新を設定することもできます（ステップ 3 を参照）。

（注） URL の末尾にアプリケーション名を含めることで（例：**https://support/updates/vpnclient.exe**）、アプリケーションを自動的に起動するようにブラウザを設定できます。

ステップ 3　クライアント更新をイネーブルにした後に、特定の ipsec-ra トンネル グループの一連のクライアント更新パラメータを定義できます。これを行うには、トンネル グループ ipsec 属性モードで、トンネル グループの名前とタイプ、および更新されたイメージの取得元となる URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。たとえば、すべての Windows クライアント用のクライアント更新を発行する必要はありません。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

VPN 3002 ハードウェア クライアントのトンネル グループを設定する場合の図については、「例」の項を参照してください。VPN 3002 クライアントはユーザの介入なしで更新され、ユーザは通知メッセージを受信しません。

ステップ 4　任意で、古い Windows クライアントを使用しているアクティブ ユーザに、VPN クライアントの更新が必要であることを知らせる通知を送信できます。これらのユーザに対しては、ポップアップ ウィンドウが表示されます。ユーザはこのポップアップ ウィンドウからブラウザを起動して、URL で指定されているサイトから、更新されたソフトウェアをダウンロードできます。このメッセージで設定可能な部分は URL だけです （ステップ 2 または 3 を参照）。アクティブでないユーザは、次回ログイン時に通知メッセージを受信します。この通知は、すべてのトンネル グループのすべてのアクティブ クライアントに送信するか、または特定のトンネル グループのクライアントに送信できます。たとえば、すべてのトンネル グループのすべてのアクティブ クライアントに通知する場合は、特権 EXEC モードで次のコマンドを入力します。

```
hostname# client-update all
hostname#
```

ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。また、ユーザは通知メッセージを受信しません。VPN 3002 クライアントはユーザの介入なしで更新され、ユーザは通知メッセージを受信しません。

（注）　クライアント更新のタイプを **windows**（Windows ベースのすべてのプラットフォーム）に指定し、その後、同じエンティティに **win9x** または **winnt** のクライアント更新タイプを入力する必要が生じた場合は、まずこのコマンドの **no** 形式で windows クライアント タイプを削除してから、新しい client-update コマンドを使用して新しいクライアント タイプを指定します。

例

次に、グローバル コンフィギュレーション モードで、すべてのトンネル グループのすべてのアクティブ リモート クライアントに対してクライアント更新をイネーブルにする例を示します。

```
hostname(config)# client-update enable
hostname#
```

次の例は、Windows（win9x、winnt、または windows）だけに適用されます。グローバル コンフィギュレーション モードで、Windows ベースのすべてのクライアントのクライアント更新パラメータを設定します。リビジョン番号 4.7、および更新を取得する URL（https://support/updates）を指定します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.7
hostname(config)#
```

次の例は、VPN 3002 ハードウェア クライアントだけに適用されます。トンネル グループ ipsec 属性コンフィギュレーション モードに入ると、IPSec リモート アクセス トンネル グループ「salesgrp」用のクライアント アップデート パラメータが設定されます。リビジョン番号 4.7 を指定し、TFTP プロトコルを使用して、更新されたソフトウェアを IP アドレス 192.168.1.1 のサイトから取得します。

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
hostname(config-tunnel-ipsec)#
```

次に、Auto Update クライアントとして設定されている Cisco 5520 適応型セキュリティ アプライアンスであるクライアントのクライアント更新を発行する例を示します。

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

次に、特権 EXEC モードで、クライアント ソフトウェアの更新が必要なトンネル グループ「remotegrp」内の、接続中のすべてのリモート クライアントにクライアント更新通知を送信する例を示します。他のグループのクライアントは、更新通知を受け取りません。

```
hostname# client-update remotegrp
hostname#
```

関連コマンド

コマンド	説明
clear configure client-update	クライアントアップデート コンフィギュレーション全体をクリアします。
show running-config client-update	現在のクライアント アップデート コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

clock set

セキュリティ アプライアンスのクロックを手動で設定するには、特権 EXEC モードで **clock set** コマンドを使用します。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

構文の説明

day	1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。
hh:*mm*:*ss*	時、分、秒を 24 時間形式で設定します。たとえば、午後 8 時 54 分は **20:54:00** のように設定します。
month	月を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。
year	たとえば、**2004** など、4 桁で年を設定します。年の範囲は 1993 ～ 2035 です。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clock コンフィギュレーション コマンドを入力していない場合、**clock set** コマンドのデフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して **clock set** コマンドを入力した後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。ただし、**clock timezone** コマンドを使用して時間帯を設定した後に **clock set** コマンドを入力した場合は、UTC ではなく、新しい時間帯に応じた時間を入力します。同様に、**clock set** コマンドの後に **clock summer-time** コマンドを入力した場合、時間は夏時間に調整されます。**clock summer-time** コマンドの後に **clock set** コマンドを入力した場合は、夏時間の正しい時間を入力します。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、**clock set** コマンドの新しい時刻を設定する必要があります。

例

次に、時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定し、MDT の現在の時間を 2004 年 7 月 27 日の午後 1 時 15 分に設定する 例を示します。

```
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname(config)# exit
hostname# clock set 13:15:0 jul 27 2004
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

次に、クロックを UTC 時間帯で 2004 年 7 月 27 日の 8 時 15 分に設定し、次に時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定する例を示します。終了時間（MDT の 1 時 15 分）は前の例と同じです。

```
hostname# clock set 20:15:0 jul 27 2004
hostname# configure terminal
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

関連コマンド

コマンド	説明
clock summer-time	夏時間を表示する日付の範囲を設定します。
clock timezone	時間帯を設定します。
show clock	現在時刻を表示します。

clock summer-time

セキュリティ アプライアンスの時間の表示に夏時間の日付範囲を設定するには、グローバル コンフィギュレーション モードで **clock summer-time** コマンドを使用します。夏時間の日付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。

clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

no clock summer-time [*zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]]

clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

no clock summer-time [*zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]]

構文の説明

date	夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このキーワードを使用する場合は、日付を毎年リセットする必要があります。
day	1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。
hh:mm	時間と分を 24 時間形式で設定します。
month	月をストリングで設定します。**date** コマンドでは、たとえば、標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。
offset	（任意）夏時間の時間を変更する分数を設定します。デフォルト値は 60 分です。
recurring	夏時間の開始日と終了日を、年の特定の日付ではなく、月の日時の形式で指定します。このキーワードを使用すると、定期的な日付範囲を設定できるため、毎年変更する必要がありません。日付を指定しない場合、セキュリティ アプライアンスが米国で使用するデフォルトの日付範囲は、3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時となります。
week	（任意）週を 1 ～ 4 の整数で指定するか、**first** や **last** の語で指定します。たとえば、日付が 5 週目に当たる場合は、**last** を指定します。
weekday	（任意）**Monday**、**Tuesday**、**Wednesday** などの曜日を指定します。
year	たとえば、**2004** など、4 桁で年を設定します。年の範囲は 1993 ～ 2035 です。
zone	太平洋夏時間の時間帯をストリング（**PDT** など）で指定します。このコマンドで設定した日付範囲に従ってセキュリティ アプライアンスが夏時間を表示する場合、時間帯はここで設定した値に変更されます。基本の時間帯を UTC 以外の時間帯に設定するには、**clock timezone** を参照してください。

デフォルト

デフォルトのオフセットは 60 分です

定期的な日付範囲のデフォルト値は、3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時。

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	透過	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	変更後の定期的な日付範囲のデフォルト値は、3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時。

使用上のガイドライン

南半球の場合、セキュリティ アプライアンスは、開始月が終了月よりも後に来る（10 月～ 3 月など）ことを受け入れます。

例

次に、オーストラリアの夏時間の日付範囲を設定する例を示します。

```
hostname(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

国によっては、夏時間が特定の日付に開始されます。次の例では、夏時間は 2004 年 4 月 1 日午前 3 時に始まり、2004 年 10 月 1 日午前 4 時に終わるように設定されています。

```
hostname(config)# clock summer-time UTC date 1 April 2004 3:00 1 October 2004 4:00
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show clock	現在時刻を表示します。

clock timezone

セキュリティ アプライアンスのクロックの時間帯を設定するには、グローバル コンフィギュレーション モードで **clock timezone** コマンドを使用します。時間帯をデフォルトの UTC に戻すには、このコマンドの **no** 形式を使用します。**clock set** コマンド、または NTP サーバから生成された時間は、時間を UTC で設定します。このコマンドを使用して、時間帯を UTC のオフセットとして設定する必要があります。

clock timezone *zone* [**-**]*hours* [*minutes*]

no clock timezone [*zone* [**-**]*hours* [*minutes*]]

構文の説明

zone	太平洋標準時間の時間帯をストリング（**PST** など）で指定します。
[**-**]*hours*	UTC からのオフセットの時間数を設定します。たとえば、PST は **-8** 時間です。
minutes	（任意）UTC からのオフセットの分数を設定します。

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	透過	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

夏時間を設定するには、**clock summer-time** コマンドを参照してください。

例

次に、時間帯を太平洋標準時間（UTC から -8 時間）に設定する例を示します。

```
hostname(config)# clock timezone PST -8
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。

コマンド	説明
ntp server	NTP サーバを指定します。
show clock	現在時刻を表示します。

cluster-ctl-file

フラッシュ メモリに格納されている既存の CTL ファイルから、すでに作成されているトラストポイントを使用するには、CTL ファイル コンフィギュレーション モードで **cluster-ctl-file** コマンドを使用します。CTL ファイルのコンフィギュレーションを削除して、新しい CTL ファイルを作成できるようにするには、このコマンドの **no** 形式を使用します。

cluster-ctl-file *filename_path*

no cluster-ctl-file *filename_path*

構文の説明

filename_path	ディスクまたはフラッシュ メモリに格納されている CTL ファイルのパスおよびファイル名を指定します。

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	透過	シングル	コンテキスト	システム
CTL ファイル コンフィギュレーション	•	—	•	—	—

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。

使用上のガイドライン

このコマンドが設定されている場合、電話プロキシは、フラッシュ メモリに格納されている CTL ファイルを解析し、その CTL ファイルからのトラストポイントをインストールし、フラッシュのそのファイルを使用して新しい CTL ファイルを作成します。

例

次に、**cluster-ctl-file** コマンドを使用して、フラッシュ メモリに格納されている CTL ファイルを解析し、そのファイルからトラストポイントをインストールする例を示します。

```
hostname(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。

コマンド	説明
ctl-file（Phone-Proxy）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

cluster encryption

仮想ロード バランシング クラスタ上で交換されるメッセージの暗号化をイネーブルにするには、VPN ロード バランシング コンフィギュレーション モードで **cluster encryption** コマンドを使用します。暗号化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。

cluster encryption

no cluster encryption

（注） VPN ロード バランシングには、アクティブな 3DES または AES ライセンスが必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

このコマンドには、引数または変数はありません。

デフォルト

暗号化は、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	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

このコマンドは、仮想ロード バランシング クラスタ上で交換されるメッセージの暗号化のオンとオフを切り替えます。

cluster encryption コマンドを設定する前に、まず **vpn load-balancing** コマンドを使用して VPN ロード バランシング モードを開始する必要があります。また、クラスタの暗号化をイネーブルにする前に、**cluster key** コマンドを使用してクラスタ共有秘密キーを設定する必要があります。

（注）　暗号化を使用する場合は、最初にコマンド **isakmp enable** *inside* を設定する必要があります。ここで、*inside* は、ロード バランシングの内部インターフェイスを示します。ロード バランシングの内部インターフェイスで ISAKMP がイネーブルでない場合は、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

例

次に、仮想ロード バランシング クラスタの暗号化をイネーブルにする **cluster encryption** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
cluster key	クラスタの共有秘密キーを指定します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

cluster ip address

仮想ロード バランシング クラスタの IP アドレスを設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster ip address** コマンドを使用します。IP アドレスの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

構文の説明

ip-address	仮想ロード バランシング クラスタに割り当てる IP 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	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

最初に、**vpn load-balancing** コマンドを使用して VPN ロード バランシング コンフィギュレーション モードを開始し、仮想クラスタ IP アドレスが指すインターフェイスを設定する必要があります。

このクラスタ IP アドレスは、仮想クラスタを設定する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。

このコマンドの **no** 形式では、任意の *ip-address* 値を指定した場合、**no cluster ip address** コマンドを実行するには、その値が既存のクラスタの IP アドレスと一致する必要があります。

例

次に、仮想ロード バランシング クラスタの IP アドレスを 209.165.202.224 に設定する **cluster ip address** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
```

```
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
interface	デバイスのインターフェイスを設定します。
nameif	インターフェイスに名前を割り当てます。
vpn load-balancing	VPN ロード バランシング モードを開始します。

cluster key

仮想ロード バランシング クラスタ上で交換される IPSec サイトツーサイト トンネルの共有秘密を設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster key** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

cluster key *shared-secret*

no cluster key [*shared-secret*]

構文の説明

shared-secret	VPN ロード バランシング クラスタの共有秘密を定義する 3 ～ 17 文字のストリング。ストリングに特殊文字を含めることはできますが、スペースを含めることはできません。

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	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。クラスタの暗号化には、**cluster key** コマンドで定義された秘密も使用されます。

共有秘密を設定するには、クラスタの暗号化をイネーブルにする前に **cluster key** コマンドを使用する必要があります。

このコマンドの **no cluster key** 形式で *shared-secret* の値を指定した場合、共有秘密の値は既存のコンフィギュレーションと一致する必要があります。

例

次に、仮想ロード バランシング クラスタの共有秘密を 123456789 に設定する **cluster key** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
```

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

cluster-mode

クラスタのセキュリティ モードを指定するには、電話プロキシ コンフィギュレーション モードで **cluster-mode** コマンドを使用します。クラスタのセキュリティ モードをデフォルト モードに設定するには、このコマンドの **no** 形式を使用します。

cluster-mode [**mixed** | **nonsecure**]

no cluster-mode [**mixed** | **nonsecure**]

構文の説明

mixed	電話プロキシ機能の設定時に、クラスタ モードを混合モードとすることを指定します。
nonsecure	電話プロキシ機能の設定時に、クラスタ モードを非セキュア モードとすることを指定します。

デフォルト

デフォルトのクラスタ モードは非セキュアです。

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	透過	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	•	—	•	—	—

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。

使用上のガイドライン

電話プロキシを混合モード クラスタ（セキュア モードと非セキュア モードの両方）で実行するように設定する場合は、一部の電話が認証または暗号化モードで設定されている場合に備えて LDC 発行元も設定する必要があります。

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

例

次に、**cluster-mode** コマンドを使用して、電話プロキシを混合（IP 電話がセキュア モードと非セキュア モードの両方で動作）に設定する例を示します。

```
hostname(config-phone-proxy)# cluster-mode mixed
```

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。
tls-proxy	TLS プロキシ インスタンスを設定します。

cluster port

仮想ロード バランシング クラスタの UDP ポートを設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster port** コマンドを使用します。ポートの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster port *port*

no cluster port [*port*]

構文の説明

port	仮想ロード バランシング クラスタに割り当てる UDP ポート。

デフォルト

デフォルトのクラスタ ポートは 9023 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	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。

任意の有効な UDP ポート番号を指定できます。範囲は 1 ～ 65535 です。

このコマンドの **no cluster port** 形式で *port* の値を指定した場合、指定したポート番号は既存の設定済みポート番号と一致する必要があります。

例

次に、仮想ロード バランシング クラスタの UDP ポートを 9023 に設定する **cluster port address** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
```

```
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

command-alias

コマンドのエイリアスを作成するには、グローバル コンフィギュレーション モードで **command-alias** コマンドを使用します。エイリアスを削除するには、このコマンドの **no** 形式を使用します。コマンド エイリアスを入力すると、元のコマンドが呼び出されます。たとえば、コマンド エイリアスを作成して、長いコマンドのショートカットにすることができます。

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

構文の説明

mode	**exec**（ユーザ EXEC モードおよび特権 EXEC モード）、**configure**、**interface** など、コマンド エイリアスを作成するコマンド モードを指定します。
command_alias	既存のコマンドに付ける新しい名前を指定します。
original_command	コマンド エイリアスを作成する既存のコマンドまたはキーワードがあるコマンドを指定します。

デフォルト

デフォルトでは、次のユーザ EXEC モード エイリアスが設定されます。

help の場合は **h**

logout の場合は **lo**

ping の場合は **p**

show の場合は **s**

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	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

任意のコマンドの最初の部分のエイリアスを作成し、さらに通常どおり追加のキーワードと引数を入力できます。

CLI ヘルプを使用する場合、コマンド エイリアスはアスタリスク（*）で示され、次の形式で表示されます。

```
*command-alias=original-command
```

たとえば、**lo** コマンド エイリアスは、次のように、「lo」で始まる他の特権 EXEC モードのコマンドとともに表示されます。

```
hostname# lo?
*lo=logout login  logout
```

同じエイリアスをさまざまなモードで使用できます。たとえば、次のように、特権 EXEC モードおよびコンフィギュレーション モードで、「happy」を異なる複数のコマンドのエイリアスとして使用できます。

```
hostname(config)# happy?

configure mode commands/options:
*happy="username crichton password test"

exec mode commands/options:
*happy=enable
```

コマンドだけを表示し、エイリアスを省略するには、入力行の先頭にスペースを入力します。また、コマンド エイリアスを回避するには、コマンドを入力する前にスペースを使用します。次の例では、happy? コマンドの前にスペースがあるため、エイリアスの happy が表示されていません。コマンドを使用します。

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname#   happy?
ERROR: % Unrecognized command
```

コマンドの場合と同様に、CLI ヘルプを使用して、コマンド エイリアスの後に続く引数およびキーワードを表示できます。

完全なコマンド エイリアスを入力する必要があります。短縮されたエイリアスは使用できません。次の例では、パーサーはエイリアスの happy を示すコマンドの hap を認識しません。

```
hostname# hap
% Ambiguous command: "hap"
```

例

次に、**copy running-config startup-config** コマンドに対して「**save**」という名前のコマンド エイリアスを作成する例を示します。

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
hostname#
```

関連コマンド

コマンド	説明
clear configure command-alias	デフォルト以外のすべてのコマンド エイリアスをクリアします。
show running-config command-alias	デフォルト以外の設定済みのコマンド エイリアスをすべて表示します。

command-queue

応答を待つ間キューに入れられる MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

command-queue *limit*

no command-queue *limit*

構文の説明

limit	キューに入れるコマンドの最大数（1 ～ 2147483647）を指定します。

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。

MGCP コマンド キューのデフォルトは 200 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	透過	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(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

応答を待つ間キューに入れられる MGCP コマンドの最大数を指定するには **command-queue** コマンドを使用します。許可されている値の範囲は、1 ～ 4294967295 です。デフォルトは 200 です。制限値に達した状態で新しいコマンドが着信すると、最も長時間キューに入っているコマンドが削除されます。

例

次に、MGCP コマンドのキューを 150 コマンドに制限する例を示します。

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。

コマンド	説明
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。
timeout	アイドル タイムアウトを設定します。タイムアウト後に、MGCP メディア接続または MGCP PAT xlate 接続が閉じられます。

compatible rfc1583

RFC 1583 に従った集約ルート コストの計算に使用した方式に戻すには、ルータ コンフィギュレーション モードで **compatible rfc1583** コマンドを使用します。RFC 1583 互換性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。

compatible rfc1583

no compatible rfc1583

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。

例

次に、RFC 1583 互換のルート集約コスト計算をディセーブルにする例を示します。

```
hostname(config-router)# no compatible rfc1583
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	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。

compression

SVC 接続および WebVPN 接続で圧縮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 **compression** コマンドを使用します。このコマンドを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。

compression {**all** | **svc** | **http-comp**}

no compression {**all** | **svc** | **http-comp**}

構文の説明

all	使用可能なすべての圧縮技術をイネーブルにすることを指定します。
svc	SVC 接続に対する圧縮を指定します。
http-comp	WebVPN 接続に対する圧縮を指定します。

デフォルト

デフォルトは、*all* です。使用可能なすべての圧縮技術が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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

SVC 接続の場合、グローバル コンフィギュレーション モードで設定した **compression** コマンドによって、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定した **svc compression** コマンドは上書きされます。

たとえば、グループ ポリシー webvpn モードで特定のグループに対する **svc compression** コマンドを入力し、次にグローバル コンフィギュレーション モードで **no compression** コマンドを入力した場合、そのグループに対して設定した **svc compression** コマンドの設定は上書きされます。

逆に、グローバル コンフィギュレーション モードで **compression** コマンドを使用して圧縮をオンに戻した場合は、グループ設定が有効となり、圧縮動作は最終的にグループ設定によって決定されます。

no compression コマンドを使用して圧縮をディセーブルにした場合、新しい接続だけが影響を受けます。アクティブな接続は影響を受けません。

例

次に、SVC 接続で圧縮をオンにする例を示します。

```
hostname(config)# compression svc
```

次に、SVC 接続および WebVPN 接続で圧縮をディセーブルにする例を示します。

```
hostname(config)# no compression svc http-comp
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションに関する情報を表示します。
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc compression	特定のグループまたはユーザに対して SVC 接続を介する HTTP データの圧縮をイネーブルにします。

config-register

次回セキュリティ アプライアンスをリロードするときに使用されるコンフィギュレーション レジスタ値を設定するには、グローバル コンフィギュレーション モードで **config-register** 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。このコマンドは、ASA 5500 適応型セキュリティ アプライアンスでのみサポートされています。コンフィギュレーション レジスタ値は、ブート元のイメージおよび他のブート パラメータを決定します。

config-register *hex_value*

no config-register

構文の説明

hex_value	コンフィギュレーション レジスタ値を 0x0 ～ 0xFFFFFFFF の 16 進数値に設定します。この数は 32 ビットを表し、各 16 進文字は 4 ビットを表します。それぞれのビットが異なる特性を制御します。ただし、ビット 32 ～ 20 は将来の使用のために予約されており、ユーザが設定できないか、または現在セキュリティ アプライアンスで使用されていません。したがって、これらのビットを表す 3 つの文字は常に 0 に設定されているため、無視できます。関連するビットは、5 桁の 16 進文字（0x*nnnnn*）で表されます。 文字の前の 0 は含める必要はありません。後続の 0 は含める必要があります。たとえば、0x2001 は 0x02001 と同じですが、0x10000 の 0 はすべて必要です。関連するビットに使用できる値の詳細については、表 8-1 を参照してください。

デフォルト

デフォルト値は 0x1 であり、ローカル イメージおよびスタートアップ 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	透過	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(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

5 つの文字には、右から左への方向で 0 ～ 4 の番号が付けられます。これは、16 進数および 2 進数の場合には標準的です。各文字に対して 1 つの値を選択したり、必要に応じて値を組み合わせて一致させたりすることができます。たとえば、文字番号 3 に対して 0 または 2 を選択できます。他の値との競合が生じる場合、一部の値が優先されます。たとえば、セキュリティ アプライアンスを TFTP サーバとローカル イメージの両方からブートするように設定する 0x2011 を設定した場合、セキュリティ アプライアンスは TFTP サーバからブートします。この値は、TFTP のブートが失敗した場合、セキュリ

ティ アプライアンスが直接 ROMMON でブートすることも定めているため、デフォルト イメージからブートすることを指定したアクションは無視されます。

0 の値は、他に指定されていなければ、アクションを実行しないことを意味します。

表 8-1 に、各 16 進文字に関連付けられたアクションを示します。各文字に対して 1 つの値を選択します。

表 8-1　コンフィギュレーション レジスタ値

プレフィックス	16 進数文字番号 4、3、2、1、および 0				
0x	**0**	**0**	**0**[1]	**0**[2]	**0**[2]
	1 起動中に 10 秒の ROMMON のカウントダウンをディセーブルにします。通常は、カウントダウン中に Escape キーを押して ROMMON を開始できます。	**2** TFTP サーバからブートするようにセキュリティ アプライアンスを設定している場合、ブートが失敗すると、この値は直接 ROMMON でブートします。		**1** ROMMON ブート パラメータ（存在する場合は、**boot system tftp** コマンドと同じ）で指定されたように TFTP サーバ イメージからブートします。この値は、文字 1 に設定された値よりも優先されます。	**1** 最初の **boot system** *local_flash* コマンドで指定されたイメージをブートします。そのイメージがロードされない場合、セキュリティ アプライアンスは、正常にブートするまで後続の **boot system** コマンドで指定された各イメージのブートを試行します。
					3、5、7、9 特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値 3 を指定すると最初の **boot system** コマンドで指定されたイメージが、値 5 を指定すると 2 つめのイメージが起動されます。以降同様に起動されます。 イメージが正常にブートしない場合、セキュリティ アプライアンスは他の **boot system** コマンド イメージに戻ることを試行しません（この点が値 1 と値 3 の使用における違いです）。ただし、セキュリティ アプライアンスには、ブートが失敗した場合に内部フラッシュ メモリのルート ディレクトリ内で検出された任意のイメージからブートを試行するフェールセーフ機能があります。フェールセーフ機能を有効にしない場合は、ルート以外のディレクトリにイメージを保存します。
				4[3] スタートアップ コンフィギュレーションを無視してデフォルトのコンフィギュレーションをロードします。	**2、4、6、8** ROMMON で、**boot** コマンドを引数なしで入力した場合、セキュリティ アプライアンスは特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値 3 を指定すると最初の **boot system** コマンドで指定されたイメージが、値 5 を指定すると 2 つめのイメージが起動されます。以降同様に起動されます。この値はイメージを自動的にブートしません。
				5 上記の両方のアクションを実行します。	

1. 将来的な使用のために予約されています。

2. 文字番号 0 および 1 が、イメージを自動的にブートするように設定されていない場合、セキュリティ アプライアンスは直接 ROMMON でブートします。
3. **service password-recovery** コマンドを使用してパスワード回復をディセーブルにした場合は、スタートアップ コンフィギュレーションを無視するようにコンフィギュレーション レジスタを設定することはできません。

コンフィギュレーション レジスタ値はスタンバイ ユニットに複製されませんが、アクティブ ユニットにコンフィギュレーション レジスタを設定すると、次の警告が表示されます。

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

confreg コマンドを使用して、コンフィギュレーション レジスタ値を ROMMON で設定することもできます。

例

次に、デフォルト イメージからブートするようにコンフィギュレーション レジスタを設定する例を示します。

```
hostname(config)# config-register 0x1
```

関連コマンド

コマンド	説明
boot	ブート イメージおよびスタートアップ コンフィギュレーションを設定します。
service password-recovery	パスワードの回復をイネーブルまたはディセーブルにします。

configure factory-default

コンフィギュレーションを出荷時のデフォルトに戻すには、グローバル コンフィギュレーション モードで **configure factory-default** コマンドを使用します。出荷時のデフォルトのコンフィギュレーションは、シスコが新しいセキュリティ アプライアンスに適用しているコンフィギュレーションです。このコマンドは、PIX 525 および PIX 535 のセキュリティ アプライアンスを除くすべてのプラットフォームでサポートされています。

configure factory-default [*ip_address* [*mask*]]

構文の説明

ip_address	デフォルトのアドレス 192.168.1.1 を使用する代わりに、管理インターフェイスまたは内部インターフェイスの IP アドレスを設定します。各モデルで設定されるインターフェイスの詳細については、「使用上のガイドライン」を参照してください。
mask	インターフェイスのサブネット マスクを設定します。マスクを設定しない場合、セキュリティ アプライアンスは IP アドレス クラスに適したマスクを使用します。

デフォルト

デフォルトの IP アドレスとマスクは 192.168.1.1 および 255.255.255.0 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	出荷時のデフォルトのコンフィギュレーションが ASA 5505 適応型セキュリティ アプライアンスに追加されました。

使用上のガイドライン

PIX 515/515E および ASA 5510 以上のセキュリティ アプライアンスでは、出荷時のデフォルトのコンフィギュレーションによって、管理用のインターフェイスが自動的に設定されるため、ASDM を使用してそのインターフェイスに接続し、残りの設定を実行できます。ASA 5505 適応型セキュリティ アプライアンスでは、出荷時のデフォルトのコンフィギュレーションによって、セキュリティ アプライアンスをネットワークですぐに使用できるように、インターフェイスと NAT が自動的に設定されます。

このコマンドは、ルーテッド ファイアウォール モードでのみ使用可能です。トランスペアレント モードはインターフェイスの IP アドレスをサポートしていません。インターフェイス IP アドレスの設定は、このコマンドが行うアクションの 1 つです。また、このコマンドはシングル コンテキスト モードでのみ使用できます。コンフィギュレーションをクリアされたセキュリティ アプライアンスには、このコマンドを使用して自動的に設定される定義済みのコンテキストはありません。

このコマンドは現在の実行コンフィギュレーションをクリアしてから、複数のコマンドを設定します。

configure factory-default コマンドで IP アドレスを設定した場合、**http** コマンドは、ユーザが指定したサブネットを使用します。同様に、**dhcpd address** コマンドの範囲は、指定したサブネット内のアドレスで構成されます。

出荷時のデフォルトのコンフィギュレーションに戻した後に、**write memory** コマンドを使用してこのコンフィギュレーションを内部フラッシュ メモリに保存します。**write memory** コマンドは、前に **boot config** コマンドで別の場所を設定している場合でも、その設定をクリアしたときにパスもクリアされているので、スタートアップ コンフィギュレーション用のデフォルトの場所に実行コンフィギュレーションを保存します。

（注）　このコマンドは、**boot system** コマンド（存在する場合）も、他のコンフィギュレーションとともにクリアします。**boot system** を使用すると、外部フラッシュ メモリ カードのイメージを含む特定のイメージからブートできます。出荷時のコンフィギュレーションに戻した後、次回セキュリティ アプライアンスをリロードすると、セキュリティ アプライアンスは、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、はブートしません。

完全なコンフィギュレーションに有用な追加の設定を行うには、**setup** コマンドを参照してください。

ASA 5505 適応型セキュリティ アプライアンスのコンフィギュレーション

ASA 5505 適応型セキュリティ アプライアンスの出荷時のデフォルトのコンフィギュレーションによって、次のように設定されます。

- イーサネット 0/1 ～ 0/7 スイッチ ポートを含む内部 VLAN 1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定していない場合、VLAN 1 の IP アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- イーサネット 0/0 スイッチ ポートを含む外部 VLAN 2 インターフェイス。VLAN 2 は、DHCP を使用してその IP アドレスを取得します。
- デフォルトのルートも DHCP から取得されます。
- すべての内部 IP アドレスが、外部にアクセスするときにインターフェイス PAT によって変換されます。
- デフォルトでは、内部ユーザはアクセス リストを使用して外部にアクセスでき、外部ユーザは内部にアクセスできません。
- セキュリティ アプライアンスで DHCP サーバがイネーブルになっているため、VLAN 1 インターフェイスに接続している PC は、192.168.1.2 ～ 192.168.1.254 のアドレスを受け取ります。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
```

```
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 以上の適応型セキュリティ アプライアンスのコンフィギュレーション

ASA 5510 以上の適応型セキュリティ アプライアンスの出荷時のデフォルトのコンフィギュレーションによって、次のように設定されます。

- 管理用 Management 0/0 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスおよびマスクは 192.168.1.1 および 255.255.255.0 です。
- セキュリティ アプライアンスでは DHCP サーバがイネーブルにされているため、このインターフェイスに接続する PC には、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E セキュリティ アプライアンスのコンフィギュレーション

PIX 515/515E セキュリティ アプライアンスの出荷時のデフォルトのコンフィギュレーションによって、次のように設定されます。

- 内部 Ethernet1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスおよびマスクは 192.168.1.1 および 255.255.255.0 です。

- セキュリティ アプライアンスでは DHCP サーバがイネーブルにされているため、このインターフェイスに接続する PC には、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

例

次に、コンフィギュレーションを出荷時のデフォルトにリセットし、IP アドレス 10.1.1.1 をインターフェイスに割り当て、次に新しいコンフィギュレーションをスタートアップ コンフィギュレーションとして保存する例を示します。

```
hostname(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
hostname(config)#
hostname(config)# copy running-config startup-config
```

関連コマンド

コマンド	説明
boot system	ブート元のソフトウェア イメージを設定します。
clear configure	実行コンフィギュレーションをクリアします。
copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
setup	セキュリティ アプライアンスの基本設定を設定するよう要求します。
show running-config	実行コンフィギュレーションを表示します。

configure http

HTTP(S) サーバから実行コンフィギュレーションにコンフィギュレーション ファイルをマージするには、グローバル コンフィギュレーション モードで **configure http** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

configure http[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*

構文の説明

:password	（任意）HTTP(S) 認証の場合、パスワードを指定します。
:*port*	（任意）ポートを指定します。HTTP の場合、デフォルトは 80 です。HTTPS の場合、デフォルトは 443 です。
@	（任意）名前とパスワードの両方またはいずれかを入力する場合は、サーバの IP アドレスの前にアットマーク（@）を付けます。
filename	コンフィギュレーション ファイル名を指定します。
http[**s**]	HTTP または HTTPS を指定します。
path	（任意）ファイル名へのパスを指定します。
server	サーバの IP アドレスまたは名前を指定します。IPv6 サーバ アドレスでポートを指定する場合は、IP アドレス内のコロンがポート番号の前のコロンと間違われないように、IP アドレスをカッコで囲む必要があります。たとえば、アドレスとポートを次のように入力します。 `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	（任意）HTTP(S) 認証の場合、ユーザ名を指定します。

デフォルト

HTTP の場合、デフォルト ポートは 80 です。HTTPS の場合、デフォルト ポートは 443 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	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィ

ギュレーション内のコマンドが上書きされます。マージによって実行コンフィギュレーションに存在しているコマンドが削除されることはありません。そのコマンドは新しいコンフィギュレーションでは設定されないだけです。

このコマンドは、**copy http running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドはシステム実行スペースでのみ使用できるため、**configure http** コマンドはコンテキスト内で使用するための代替です。

例

次に、コンフィギュレーション ファイルを HTTPS サーバから実行コンフィギュレーションにコピーする例を示します。

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure factory-default	CLI で入力されたコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure memory

スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージするには、グローバル コンフィギュレーション モードで **configure memory** コマンドを使用します。

configure memory

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	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィギュレーション内のコマンドが上書きされます。マージによって実行コンフィギュレーションに存在しているコマンドが削除されることはありません。そのコマンドは新しいコンフィギュレーションでは設定されないだけです。

コンフィギュレーションをマージしない場合は、セキュリティ アプライアンスを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、**configure memory** コマンドを入力して新しいコンフィギュレーションをロードできます。

このコマンドは、**copy startup-config running-config** コマンドと同じです。

マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、**config-url** コマンドで指定した場所にあります。

例

次に、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーする例を示します。

```
hostname(config)# configure memory
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure factory-default	CLI で入力されたコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure net

TFTP サーバのコンフィギュレーション ファイルを実行コンフィギュレーションにマージするには、グローバル コンフィギュレーション モードで **configure net** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

configure net [*server*:[*filename*] | :*filename*]

構文の説明

:*filename*	パスとファイル名を指定します。**tftp-server** コマンドを使用してすでにファイル名を設定してある場合、この引数はオプションです。 このコマンドでファイル名を指定し、**tftp-server** コマンドで名前を指定する場合、セキュリティ アプライアンスは **tftp-server** コマンド ファイル名をディレクトリとして扱い、**configure net** コマンド ファイル名をディレクトリの下のファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合は、コロン（:）の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。**tftp-server** コマンドで設定したアドレスがあっても、このアドレスが優先されます。IPv6 サーバ アドレスの場合、IP アドレス内のコロンがファイル名の前のコロンと間違われないように、IP アドレスをカッコで囲む必要があります。たとえば、アドレスを次のように入力します。 [fe80::2e0:b6ff:fe01:3b7a] デフォルトのゲートウェイ インターフェイスは最もセキュリティが高いインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

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	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィギュレーション内のコマンドが上書きされます。マージによって実行コンフィギュレーションに存在しているコマンドが削除されることはありません。そのコマンドは新しいコンフィギュレーションでは設定されないだけです。

このコマンドは、**copy tftp running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドはシステム実行スペースでのみ使用できるため、**configure net** コマンドはコンテキスト内で使用するための代替です。

例

次に、**tftp-server** コマンドにサーバとファイル名を設定してから、**configure net** コマンドを使用してサーバを上書きする例を示します。同じファイル名が使用されています。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

次に、サーバおよびファイル名を上書きする例を示します。ファイル名へのデフォルト パスは /tftpboot/configs/config1 です。ファイル名をスラッシュ（/）で始めない場合、パスの /tftpboot/ 部分がデフォルトで含まれます。このパスを上書きし、ファイルも tftpboot にある場合は、tftpboot パスを **configure net** コマンドに含めます。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

次に、サーバだけを **tftp-server** コマンドに設定する例を示します。**configure net** コマンドはファイル名だけを指定します。

```
hostname(config)# tftp-server inside 10.1.1.1
hostname(config)# configure net :configs/config1
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

configure terminal

実行コンフィギュレーションをコマンドラインで設定するには、特権 EXEC モードで **configure terminal** コマンドを使用します。このコマンドは、コンフィギュレーションを変更するコマンドを入力できるグローバル コンフィギュレーション モードを開始します。

configure terminal

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、グローバル コンフィギュレーション モードを開始する例を示します。

```
hostname# configure terminal
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
show running-config	実行コンフィギュレーションを表示します。

config-url

システムがコンテキスト コンフィギュレーションをダウンロードする URL を指定するには、コンテキスト コンフィギュレーション モードで **config-url** コマンドを使用します。

config-url *url*

構文の説明

url　コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストから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 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内部フラッシュ メモリを指します。**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 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。

- **flash:**/[*path*/]*filename*

  この URL は内部フラッシュ メモリを示します。

- **ftp:**//[*user*[**:***password*]**@**]*server*[*:port*]/[*path*/]*filename*[**;type=***xx*]

  type には次のキーワードのいずれかを指定できます。

  - **ap**：ASCII 受動モード
  - **an**：ASCII 通常モード
  - **ip**：（デフォルト）バイナリ受動モード
  - **in**：バイナリ通常モード

- **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[*:port*]/[*path*/]*filename*

- **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。

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	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(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

コンテキスト URL を追加すると、システムはただちにコンテキストをロードし、実行中になります。

（注） **config-url** コマンドを入力する前に、**allocate-interface** コマンドを入力します。セキュリティ アプライアンスは、コンテキスト コンフィギュレーションをロードする前に、コンテキストにインターフェイスを割り当てる必要があります。コンテキスト コンフィギュレーションには、インターフェイス（**interface**、**nat**、**global** など）を示すコマンドが含まれている場合があります。最初に **config-url** コマンドを入力した場合、セキュリティ アプライアンスはただちにコンテキスト コンフィギュレーションをロードします。インターフェイスを示すコマンドがコンテキストに含まれている場合、それらのコマンドは失敗します。

ファイル名にファイル拡張子は必要ありませんが、「.cfg」を使用することを推奨します。

管理コンテキスト ファイルは、内部フラッシュ メモリに保存する必要があります。

HTTP または HTTPS サーバからコンテキスト コンフィギュレーションをダウンロードした場合、**copy running-config startup-config** コマンドを使用してこれらのサーバに変更内容を戻して保存することはできません。ただし、**copy tftp** コマンドを使用して実行コンフィギュレーションを TFTP サーバにコピーできます。

システムは、サーバが利用できない、またはファイルがまだ存在しないためにコンテキスト コンフィギュレーション ファイルを取得できない場合、コマンドライン インターフェイスですぐに設定できるブランクのコンテキストを作成します。

URL を変更するには、新しい URL で **config-url** コマンドを再入力します。

セキュリティ アプライアンスは、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。

例

次に、管理コンテキストに「administrator」を設定し、内部フラッシュ メモリに「administrator」というコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加する例を示します。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
```

```
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

console timeout

セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **console timeout** コマンドを使用します 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。

console timeout *number*

no console timeout [*number*]

構文の説明

number	コンソール セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。

デフォルト

デフォルトのタイムアウトは 0 であり、コンソール セッションがタイムアウトしないことを示します。

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	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

console timeout コマンドは、セキュリティ アプライアンスへの認証済みのすべてのイネーブル モード ユーザ セッションまたはコンフィギュレーション モード ユーザ セッションにタイムアウト値を設定します。**console timeout** コマンドによって、Telnet タイムアウトや SSH タイムアウトが変更されることはありません。これらのアクセス方式では、それぞれ独自のタイムアウト値が保持されています。

no console timeout コマンドは、コンソール タイムアウト値をデフォルトのタイムアウトである 0 にリセットします。この値は、コンソールがタイムアウトしないことを意味します。

例

次に、コンソール タイムアウトを 15 分に設定する例を示します。

```
hostname(config)# console timeout 15
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。

コマンド	説明
clear configure timeout	コンフィギュレーションのアイドル時間継続時間をデフォルトに戻します。
show running-config console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを表示します。

content-length

HTTP メッセージ本文の長さに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **content-length** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	メッセージがこのインスペクションに合格しなかったときに実行するアクションを指定します。
allow	メッセージを許可します。
bytes	バイト数を指定します。許容される範囲は、**min** オプションでは 1 ～ 65535、**max** オプションでは 1 ～ 50000000 です。
drop	接続を閉じます。
log	（任意）syslog を生成します。
max	（任意）許容される内容の最大長を指定します。
min	（任意）許容される内容の最小長を指定します。
reset	TCP リセット メッセージをクライアントおよびサーバに送信します。

デフォルト

デフォルトでは、この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	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(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

content-length コマンドをイネーブルにすると、セキュリティ アプライアンスは、設定された範囲内のメッセージだけを許可し、範囲外の場合は指定されたアクションを実行します。セキュリティ アプライアンスに TCP 接続をリセットさせて、Syslog エントリを作成させるには、**action** キーワードを使用します。

例

次に、HTTP トラフィックを 100 バイト以上 2000 バイト以下のメッセージに制限する例を示します。メッセージがこの範囲外の場合、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

context

システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト 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 **context** コマンドを使用します。コンテキストを削除するには、このコマンドの **no** 形式を使用します。コンテキスト コンフィギュレーション モードでは、コンテキストで使用できる、コンフィギュレーション ファイルの URL とインターフェイスを指定できます。

context *name*

no context *name* [**noconfirm**]

構文の説明

name	名前を最大 32 文字のストリングで設定します。この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。
noconfirm	（任意）確認を求めるプロンプトを表示せずにコンテキストを削除します。このオプションは自動スクリプトで役立ちます。

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	透過	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	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(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

管理コンテキストがない場合（たとえば、コンフィギュレーションをクリアした場合）、追加する最初のコンテキストは管理コンテキストである必要があります。管理コンテキストを追加するには、**admin-context** コマンドを参照してください。管理コンテキストを指定した後、**context** コマンドを入力して管理コンテキストを設定します。

コンテキストは、システム コンフィギュレーションを編集することによってのみ削除できます。現在の管理コンテキストはこのコマンドの **no** 形式を使用して削除することはできません。**clear configure context** コマンドを使用してすべてのコンテキストを削除した場合にのみ削除できます。

例

次に、管理コンテキストに「administrator」を設定し、内部フラッシュ メモリに「administrator」というコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加する例を示します。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキストとシステム実行スペースの間を切り替えます。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
show context	コンテキスト情報を表示します。

copy

ファイルをある場所から別の場所にコピーするには、特権 EXEC モードで **copy** コマンドを使用します。

copy [**/noconfirm** | **/pcap**] {*url* | **running-config** | **startup-config**}
{**running-config** | **startup-config** | *url*}

構文の説明

/noconfirm	確認のプロンプトを出さないでファイルをコピーします。
/pcap	事前に設定した TFTP サーバのデフォルトを指定します。デフォルトの TFTP サーバを設定する場合は、**tftp-server** コマンドを参照してください。
running-config	メモリに格納されている実行コンフィギュレーションを指定します。

startup-config	フラッシュ メモリに格納されているスタートアップ コンフィギュレーションを指定します。シングル モードのスタートアップ コンフィギュレーション、またはマルチ コンテキスト モードのシステムのスタートアップ コンフィギュレーションは、フラッシュ メモリ内の非表示のファイルです。スタートアップ コンフィギュレーションの場所は、コンテキスト内から **config-url** コマンドで指定します。たとえば、**config-url** コマンドで HTTP サーバを指定し、**copy startup-config running-config** コマンドを入力した場合、セキュリティ アプライアンスは管理コンテキスト インターフェイスを使用して、HTTP サーバからスタートアップ コンフィギュレーションをコピーします。

url

コピー元のファイルまたはコピー先のファイルを指定します。コピー元 URL とコピー先 URL のすべての組み合わせが許可されているわけではありません。たとえば、あるリモート サーバから別のリモート サーバにコピーすることはできません。このコマンドは、ローカルの場所とリモートの場所との間でファイルをコピーするために使用します。コンテキスト内では、コンテキスト インターフェイスを使用して、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションを TFTP サーバまたは FTP サーバにコピーできますが、サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコピーすることはできません。他のオプションについては、**startup-config** キーワードを参照してください。TFTP サーバから実行コンテキスト コンフィギュレーションにダウンロードするには、**configure net** コマンドを使用します。

次の URL 構文を使用します。

- **cache:**/[*path*/]*filename*]

  このオプションは、ファイル システム内のキャッシュ メモリを示します。
- **capture:**/[*path*/]*filename*]

  このオプションは、キャプチャ バッファ内の出力を示します。
- **disk0:**/[*path*/]*filename*]

  このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、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*]

  このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、外部フラッシュ メモリ カードを示します。
- **flash:**/[*path*/]*filename*]

  このオプションは、内部フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、**flash** は **disk0** のエイリアスです。
- **smb:**/[*path*/]*filename*]

  このオプションは、UNIX サーバ上のローカル ファイル システムを示します。サーバ メッセージ ブロック ファイル システム プロトコルは、データをパッケージ化し、他のシステムと情報を交換するために、LAN マネージャおよび類似のネットワーク オペレーティング システムで使用されます。
- **ftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]

  type には次のキーワードのいずれかを指定できます。
  - **ap**：ASCII 受動モード
  - **an**：ASCII 通常モード
  - **ip**：（デフォルト）バイナリ受動モード
  - **in**：バイナリ通常モード
- **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*]
- **system:**/[*path*/]*filename*]

  このオプションは、ファイル システム内のシステム 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、**nameif interface** コマンドを使用してインターフェイス名を指定します。

  パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**copy tftp** コマンドの代わりに **tftp-server** コマンドでパスを設定します。

デフォルト

このコマンドには、デフォルト設定がありません。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	DNS 名のサポートが追加されました。
8.0(2)	**smb:** URL オプションが追加されました。

使用上のガイドライン

コンフィギュレーションを実行コンフィギュレーションにコピーするには、2 つのコンフィギュレーションをマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

例

次に、システム実行スペースでファイルをディスクから TFTP サーバにコピーする例を示します。

```
hostname(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

次に、ファイルをディスク上のある場所からディスク上の別の場所にコピーする例を示します。宛先ファイルの名前は、コピー元のファイルの名前にすることも、別の名前にすることもできます。

```
hostname(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

次に、ASDM ファイルを TFTP サーバから内部フラッシュ メモリにコピーする例を示します。

```
hostname(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

次に、コンテキスト内の実行コンフィギュレーションを TFTP サーバにコピーする例を示します。

```
hostname(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

copy コマンドでは、IP アドレス（上の例の場合）だけでなく、DNS 名も指定できます。

```
hostname(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

関連コマンド

コマンド	説明
configure net	ファイルを TFTP サーバから実行コンフィギュレーションにコピーします。
copy capture	キャプチャ ファイルを TFTP サーバにコピーします。
tftp-server	デフォルトの TFTP サーバを設定します。

コマンド	説明
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

copy capture

キャプチャ ファイルをサーバにコピーするには、特権 EXEC モードで **copy capture** コマンドを使用します。

copy [**/noconfirm**] [**/pcap**] **capture:** [*context_name*/]*buffer_name url*

構文の説明

/noconfirm	確認のプロンプトを出さないでファイルをコピーします。
/pcap	パケット キャプチャを raw データとしてコピーします。
buffer_name	キャプチャを識別するための一意な名前。
context_name/	セキュリティ コンテキストで定義されたパケット キャプチャをコピーします。
url	パケット キャプチャ ファイルのコピー先を指定します。次の URL 構文を参照してください。 • **disk0:**/[*path*/]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用でき、内部フラッシュ カードを示します。**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* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用でき、外部フラッシュ カードを示します。 • **flash:**/[*path*/]*filename* このオプションは、内部フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、**flash** は **disk0** のエイリアスです。 • **ftp:**//[*user*[**:***password*]**@**]*server*[*:port*]/[*path*/]*filename*[**;type=***xx*] **type** には次のキーワードのいずれかを指定できます。 – **ap**：ASCII 受動モード – **an**：ASCII 通常モード – **ip**：（デフォルト）バイナリ受動モード – **in**：バイナリ通常モード • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[*:port*]/[*path*/]*filename* • **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。 パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**copy tftp** コマンドの代わりに **tftp-server** コマンドでパスを設定します。

デフォルト

このコマンドには、デフォルト設定がありません。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、フル パスを指定せずに **copy capture** コマンドを入力した場合に表示されるプロンプトの例を示します。

```
hostname(config)# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

次のようにフル パスを指定できます。

```
hostname(config)# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

TFTP サーバをすでに設定している場合は、次のようにファイルの位置や名前を省略できます。

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
clear capture	キャプチャ バッファをクリアします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

cpu profile activate

CPU のプロファイル コレクションに関する情報を表示するには、特権 EXEC モードで **cpu profile activate** コマンドを使用します。

cpu profile activate *n-samples*

構文の説明

n-samples	サンプル数 n を保存するためのメモリを割り当てます。値は 1 ～ 100000 で、デフォルトは 1000 です。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show cpu profile コマンドと、**cpu profile activate** コマンドを併用することで、CPU の問題の修復を支援するために TAC が収集および使用できる情報を表示できます。**show cpu profile** コマンドによって表示される情報は 16 進数です。

例

次の例では、プロファイラが稼働し、5000 個のサンプルの格納が命令されます。

```
hostname# cpu profile activate 5000
Activated CPU profiling for 5000 samples.
```

結果を確認するには、**show cpu profile** コマンドを使用します。

（注） **cpu profile activate** コマンドの実行中に **show cpu profile** を実行すると、進捗が表示されます。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 CPU profiling currently in
progress, 1640 out of 5000 samples collected.
```

完了すると、**show cpu profile** コマンドの出力に結果が表示されます。この情報をコピーし、デコードする TAC に提供します。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 Profiling finished, 5000 samples:
 00c483f5 00115283 002199d3 001151d1 002199e5 00116258 002199fc 00115230  0021984e
002198f6 00c48496 00219803 004a55b1 002198b1 00c484d9 00c48472
 00116258 00c48401 002199f3 00c48401 00c484b2 004a5580 0011520a 002198b4
 00116258 00219807 0011520a 00116258 002198a9 00116258 00219a2e 00112009  0021989c
00fff023 008be861 0011525e 002198be 0021984e 00115277 00219807  002199d0 00114a6d 002198af
0011520a 00115260 00115274 004a55a6 00c48472
 00c48472 00c48496 002199f9 002198ad 00c484c4 004a55a6 00115260 002198f4  0011528e
002198e0 00c484bb 00c48496 00c484a6 002199f3 00219810 001161d6 .
```

関連コマンド

コマンド	説明
show cpu profile	TAC で使用する CPU のプロファイルのアクティベーションに関する情報を表示します。

crashinfo console disable

フラッシュへのクラッシュの書き込みを読み取り、書き込み、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 **crashinfo console disable** コマンドを使用します。

crashinfo console disable

no crashinfo console disable

構文の説明

disable	クラッシュが発生した場合にコンソール出力を抑制します。

デフォルト

このコマンドには、デフォルト設定がありません。

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	透過	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、コンソールへの crashinfo の出力を抑制できます。crashinfo には、デバイスに接続しているすべてのユーザに表示するのは適切でない機密情報が含まれている場合があります。このコマンドとともに、crashinfo がフラッシュに書き込まれていることも確認する必要があります。これはデバイスのリブート後に確認できます。このコマンドは、crashinfo および checkheaps の出力に影響を与えます。この出力はフラッシュに保存され、トラブルシューティングに十分に役立ちます。

例

```
hostname(config)# crashinfo console disable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。

コマンド	説明
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

crashinfo force

セキュリティ アプライアンスを強制的にクラッシュさせるには、特権 EXEC モードで **crashinfo force** コマンドを使用します。

crashinfo force [**page-fault** | **watchdog**]

構文の説明

page-fault	（任意）ページ フォールトを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。
watchdog	（任意）ウォッチドッグを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

crashinfo force コマンドを使用して、クラッシュ出力の生成をテストできます。クラッシュ出力では、本物のクラッシュを、**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドによって発生したクラッシュと区別できません。これは、これらのコマンドによって実際にクラッシュが発生しているためです。セキュリティ アプライアンスは、クラッシュのダンプが完了するとリロードします。

注意　実働環境では **crashinfo force** コマンドを使用しないでください。**crashinfo force** コマンドはセキュリティ アプライアンスをクラッシュさせて、強制的にリロードを実行します。

例

次に、**crashinfo force page-fault** コマンドを入力したときに表示される警告の例を示します。

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
    Do you wish to proceed? [confirm]:
```

キーボードの Return キーまたは Enter キーを押して復帰改行を入力するか、**Y** キーまたは **y** キーを押すと、セキュリティ アプライアンスがクラッシュしてリロードが実行されます。これらの応答は、確認済みとして解釈されます。その他の文字はすべて **no** と解釈され、セキュリティ アプライアンスはコマンドライン プロンプトに戻ります。

関連コマンド

clear crashinfo	クラッシュ情報ファイルの内容をクリアします。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	クラッシュ情報ファイルの内容を表示します。

crashinfo save disable

フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにするには、グローバル コンフィギュレーション モードで **crashinfo save** コマンドを使用します。フラッシュ メモリへのクラッシュ情報の書き込みを許可し、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。

crashinfo save disable

no crashinfo save disable

構文の説明

このコマンドには、デフォルトの引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

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	透過	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	**crashinfo save enable** コマンドは廃止され、有効なオプションではなくなりました。代わりに、**no crashinfo save disable** コマンドを使用します。

使用上のガイドライン

クラッシュ情報は、まずフラッシュ メモリに書き込まれ、次にコンソールに書き込まれます。

（注） セキュリティ アプライアンスが起動中にクラッシュした場合、クラッシュ情報ファイルは保存されません。セキュリティ アプライアンスは、完全に初期化され、動作を開始した後に、クラッシュ情報をフラッシュ メモリに保存できます。

フラッシュ メモリへのクラッシュ情報の保存をもう一度イネーブルにするには、**no crashinfo save disable** コマンドを使用します。

例

```
hostname(config)# crashinfo save disable
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容をクリアします。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。

crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crashinfo test

フラッシュ メモリのファイルにクラッシュ情報を保存するセキュリティ アプライアンスの機能をテストするには、特権 EXEC モードで **crashinfo test** コマンドを使用します。

crashinfo test

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

フラッシュ メモリ内に以前のクラッシュ情報ファイルがすでに存在する場合、そのファイルは上書きされます。

（注）　**crashinfo test** コマンドを入力してもセキュリティ アプライアンスはクラッシュしません。

例

次に、クラッシュ情報ファイル テストの出力例を示します。

```
hostname# crashinfo test
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリにクラッシュ情報を書き込めないようにします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crl

CRL コンフィギュレーション オプションを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **crl** コマンドを使用します。

crl {**required | optional | nocheck**}

構文の説明

required	ピア証明書の検証に必要な CRL が使用可能である必要があります。
optional	必須の CRL が使用できない場合にも、セキュリティ アプライアンスはピア証明書を受け入れることができます。
nocheck	CRL チェックを実行しないようセキュリティ アプライアンスに指示します。

デフォルト

デフォルト値は **nocheck** 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	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。次の **revocation-check** コマンドに置き換わりました。 • **crl optional** は **revocation-check crl none** に置き換えられました。 • **crl required** は **revocation-check crl** に置き換えられました。 • **crl nocheck** は **revocation-check none** に置き換えられました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始し、ピア証明書がトラストポイント central に対して検証されるのに CRL を必要とする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。

コマンド	説明
crypto ca trustpoint	トラストポイント サブモードを開始します。
crl configure	CRL コンフィギュレーション モードを開始します。

crl configure

CRL コンフィギュレーション モードを開始するには、クリプト CA トラストポイント コンフィギュレーション モードで **crl configure** コマンドを使用します。

crl configure

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	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、トラストポイント central 内で crl コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。