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。規則を削除するには、このコマンドの **no** 形式を使用します。

すべての規則を削除するには、**no client-access-rule** コマンドの priority 引数だけを指定して使用します。この指定により、**client-access-rule none** コマンドを入力して作成されたヌル規則を含む、設定されたすべての規則が削除されます。

クライアントのアクセス規則がない場合、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規則を継承します。ユーザがクライアントのアクセス規則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。クライアントのアクセス規則を継承しない場合、すべてのクライアント タイプおよびバージョンに接続できます。

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

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

シンタックスの説明

deny	特定のタイプとバージョンの両方またはいずれか一方のデバイスの接続を拒否します。
none	クライアントのアクセス規則を許可しません。client-access-rule をヌル値に設定して、制限を許可しません。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両方またはいずれか一方のデバイスの接続を許可します。
priority	規則の優先順位を決定します。最も小さい整数の規則が、一番高い優先順位となります。したがって、クライアント タイプとバージョンの両方またはいずれか一方に一致する最も小さい整数の規則が、適用される規則です。優先順位の低い規則が矛盾している場合、セキュリティ アプライアンスはその規則を無視します。

type *type*	VPN 3002 などの自由形式の文字列を利用して、デバイス タイプを指定します。* 記号をワイルドカードとして使用できる場合を除き、文字列は **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。
version *version*	7.0(1) などの自由形式の文字列を使用して、デバイス バージョンを指定します。* 記号をワイルドカードとして使用できる場合を除き、文字列は **show vpn-sessiondb remote** 表示の外観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、アクセス規則はありません。

コマンド モード

次の表は、このコマンドを入力でき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	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

次の注意に従って規則を作成します。

- 規則を定義しない場合、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。
- クライアントが規則のいずれ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 deny 規則を定義する場合は、少なくとも 1 つの permit 規則も定義する必要があります。permit 規則を定義しないと、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 クライアントのどちらも、タイプおよびバージョンが **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。
- * 記号はワイルドカードで、各規則内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 タイプを拒否する優先順位 3 のクライアントのアクセス規則を作成します。
- 1 つのグループ ポリシーにつき最大 25 の規則を作成できます。
- 一連の規則全体に 255 文字の制限があります。
- クライアント タイプとバージョンの両方またはいずれか一方を送信しないクライアントに n/a を使用できます。

例

次の例では、FirstGroup という名前のグループ ポリシーのクライアントのアクセス規則を作成する方法を示します。これらの規則は、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、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-firewall

セキュリティ アプライアンスが IKE トンネルのネゴシエーション中に 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 ポリシーを含む、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**

シンタックスの説明

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確実に実行されていることを確認します。「Are You There?」と表示され、応答がない場合、セキュリティ アプライアンスはトンネルを終了します。
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	Custom ファイアウォール タイプを指定します。
description <*string*>	ファイアウォールについて説明します。
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て、拒否します。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

次の表は、このコマンドを入力でき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**	**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

このコマンドで設定できるインスタンスは 1 つだけです。

例

次の例では、FirstGroup という名前のグループ ポリシーの 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方法を示します。

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

client-update

全トンネル グループまたは特定のトンネル グループのアクティブなすべてのリモート VPN ソフトウェアとハードウェア 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 アップデートを発行するには、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 アップデートのパラメータをグローバル レベル（VPN ソフトウェアとハードウェア 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 ソフトウェアとハードウェア クライアント用のクライアント アップデート トンネル グループ IPSec アトリビュート 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 アトリビュート 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。

クライアントが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場合は、ソフトウェアをアップデートする必要はありません。クライアントが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場合は、アップデートする必要があります。

クライアント アップデートをディセーブルにするには、このコマンドの ***no*** 形式を使用します。

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 アトリビュート 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*

シンタックスの説明

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*	Auto Update クライアント自体に固有の ID が付いている場合は、その文字列と同じものを指定します。最大長は 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 アップデートをイネーブルにします。
family *family_name*	Auto Update クライアントをデバイス ファミリで識別するように設定している場合は、同じデバイス ファミリを指定します。これは、asa、pix、または 7 文字までの文字列です。

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 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 アプライアンスは、1 つしか指定できません。文字列の最大長は 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 アップデートの有効なトンネル 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）クライアントのアップデートを知らせるリモート PC のオペレーティング システムか、Auto Update 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。次のものを指定できます。 • pix-515：Cisco PIX 515 Firewall • pix-515e：Cisco PIX 515E Firewall • pix-525：Cisco PIX 525 Firewall • pix-535：Cisco PIX 535 Firewall • asa5505：Cisco 5505 Adaptive Security Appliance • asa5510：Cisco 5510 Adaptive Security Appliance • asa5520：Cisco 5520 Adaptive Security Appliance • asa5540：Cisco Adaptive Security Appliance • 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 • 15 文字までのテキスト文字列
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、このクライアントに応じたファイルを示す必要があります。URL 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

次の表は、このコマンドを入力でき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	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 アトリビュート 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。
7.1(1)	トンネル グループ ipsec アトリビュート 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 アトリビュート コンフィギュレーション モードでは、このアトリビュートを IPSec リモートアクセス トンネル グループ タイプだけに適用できます。

client-update コマンドでは、アップデートのイネーブル化、アップデート適用先のクライアントのタイプとリビジョン番号の指定、アップデート取得先の URL または IP アドレスの指定が可能です。また、Windows クライアントの場合は、オプションで、VPN クライアント バージョンをアップデートする必要があることをユーザに通知できます。Windows クライアントに対しては、アップデート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、アップデート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 アプライアンスの場合は、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 アップデート 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 アップデート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 アップデート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と、最新イメージの取得先 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 コンポーネントのタイプ（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は、そのクライアントをアップデート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 アップデート パラメータを設定します。次の例を参考にしてください。

```
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 グループの設定については、「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。

Windows クライアントと VPN3002 ハードウェア クライアントでは、特定のタイプの全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 アップデートを設定することもできます（ステップ 3 を参照）。

（注）　ブラウザが自動的に起動されるように設定することができます。それには、URL の末尾にアプリケーション名を含めます（例：**https://support/updates/vpnclient.exe**）。

ステップ 3　クライアント アップデートをイネーブルにした後は、特定の ipsec-ra トンネル グループの一連のクライアント アップデート 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 アトリビュート モードで、トンネル グループの名前とタイプ、および最新イメージの取得先 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は、そのクライアントをアップデート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 アップデート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 グループの設定については、「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アップデートされ、ユーザへの通知メッセージは送信されません。

ステップ 4　オプションで、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 クライアントをアップデートする必要が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最新の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ことも、特定のトンネル グループのクライアントに送信することもできます。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、次のコマンドを特権 EXEC モードで入力します。

```
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は、そのクライアントをアップデートする必要はありません。また、ユーザへの通知メッセージは送信されません。VPN 3002 クライアントは、ユーザの介入なしでアップデートされ、ユーザへの通知メッセージは送信されません。

（注）　クライアント アップデートのタイプを ***windows***（Windows ベースの全プラットフォーム）に指定し、その後、同じエンティティに ***win9x*** タイプまたは ***winnt*** タイプを入力しなければならなくなった場合は、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 コマンドを入力して新しいタイプのクライアントを指定してください。

例

グローバル コンフィギュレーション モードで入力した次の例では、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 アップデートをイネーブルにしています。

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

次の例は、Windows（win9x、winnt、または windows）にだけ適用されます。グローバル コンフィギュレーション モードで入力したこの例では、すべての Windows ベース クライアントのクライアント アップデート 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 アトリビュート コンフィギュレーション モードで入力されたこの例では、IPSec リモートアクセス トンネル グループ「salesgrp」のクライアント アップデート パラメータを設定します。リビジョン番号 4.7 を指定し、IP アドレス 192.168.1.1 を持つサイトからの最新ソフトウェアの取得に TFTP プロトコルを使用します。

```
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)#
```

次の例は、Auto Update クライアントとして設定されている Cisco 5520 Adaptive Security Appliance のクライアント アップデートを発行する方法を示します。

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

特権 EXEC モードで入力した次の例では、「remotegrp」という名前のトンネル グループに属する、クライアント ソフトウェアをアップデートする必要のある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 アップデート通知を送信します。他のグループのクライアントには、アップデート通知は送信されません。

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

関連コマンド

コマンド	説明
clear configure client-update	client-update コンフィギュレーション全体を消去します。
show running-config client-update	現在の client-update 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 アトリビュートを設定します。

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*

シンタックスの説明

day	1 ～ 31 の日を設定します。たとえば、標準の日付形式に応じて、月日を **april 1** や **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** や **1 april** のように入力できます。
year	4 桁で西暦年を設定します（たとえば、**2004**）。西暦年の範囲は 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

次の表は、このコマンドを入力でき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	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のものです。

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確立した後に **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** コマンドに新しい時間を設定する必要があります。

例

次の例では、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 の現在の時間を西暦 2004 年 7 月 27 日の午後 1 時 15 分に設定します。

```
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
```

次の例では、クロックを UTC 時間帯で西暦 2004 年 7 月 27 日の 8 時 15 分に設定し、次に時間帯を MST に、夏時間を米国のデフォルト期間に設定します。終了時間（MDT の 1 時 15 分）は上記の例と同じです。

```
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範囲を設定します。
clock timezone	時間帯を設定します。
show clock	現在の時刻を表示します。

clock summer-time

セキュリティ アプライアンスの時間の表示用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*]]

シンタックスの説明

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した場合は、日付を毎年リセットする必要があります。
day	1 ～ 31 の日を設定します。たとえば、標準の日付形式に応じて、月日を **April 1** や **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	月を文字列で設定します。***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** や **1 April** のように入力できます。
offset	（オプション）夏時間の時間を変更する分数を設定します。この値は、デフォルトで 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、月の日と時間の形式で指定します。このキーワードを使用すると、毎年変更する必要がない定期的な日付範囲を設定できます。日付を指定しない場合、セキュリティ アプライアンスは、米国のデフォルトの日付範囲（4 月の最初の日曜日の午前 2 時～ 10 月の最後の日曜日の午前 2 時）を使用します。
week	（オプション）週を 1 ～ 4 の整数で、あるいは ***first*** または ***last*** の語で指定します。たとえば、日が 5 週目になった場合は、**last** を指定します。
weekday	（オプション）**Monday**、**Tuesday**、**Wednesday** など、曜日を指定します。
year	4 桁で西暦年を設定します（たとえば、**2004**）。西暦年の範囲は 1993 ～ 2035 です。
zone	たとえば、太平洋夏時間は **PDT** のように、時間帯を文字列で指定します。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。

デフォルトの定期的な日付範囲は、4 月の最初の日曜日の午前 2 時から 10 月の最後の日曜日の午前 2 時です。

コマンド モード

次の表は、このコマンドを入力でき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	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のものです。

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、たとえば 10 月から 3 月のように、開始月が終了月よりも後に来ることを受け入れます。

例

次の例では、オーストラリアの夏時間の範囲を設定します。

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

国によっては、夏時間は特定の日付に開始されます。次の例では、夏時間を西暦 2004 年 4 月 1 日午前 3 時に開始し、西暦 2004 年 10 月 1 日午前 4 時に終了するように設定します。

```
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	現在の時刻を表示します。

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 UTC の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。**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*]]

シンタックスの説明

zone	たとえば、太平洋標準時間は **PST** のように、時間帯を文字列で指定します。
[**-**]*hours*	UTC からのオフセットの時間を設定します。たとえば、PST は **-8** 時間です。
minutes	（オプション）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

次の表は、このコマンドを入力でき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	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のものです。

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

次の例では、時間帯を UTC から -8 時間の太平洋標準時間に設定します。

```
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範囲を設定します。
ntp server	NTP サーバを指定します。
show clock	現在の時刻を表示します。

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 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。有効な 3DES ライセンスまたは AES ライセンスが検出されなかった場合、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しません。また、ライセンスで許可されていない限り、ロードバランシング システムが 3DES の内部設定を行わないようにします。

シンタックスの説明

このコマンドには、引数も変数もありません。

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

次の表は、このコマンドを入力でき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	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 モード	•	—	•	—	—

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 モードに入る必要があります。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鍵も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です。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鍵を指定します。
vpn load-balancing	VPN ロードバランシング モードに入ります。

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 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*]

シンタックスの説明

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

次の表は、このコマンドを入力でき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	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 モード	•	—	•	—	—

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 モードに入り、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。

cluster ip address は、仮想クラスタを設定してい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、オプションの *ip-address* 値を指定した場合、その値は **no cluster ip address** コマンドが完了される前に、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 モードに入ります。

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 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*]

シンタックスの説明

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文字列。

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

次の表は、このコマンドを入力でき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	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 モード	•	—	•	—	—

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 モードに入る必要があります。クラスタの暗号化には、**cluster key** コマンドで定義されたシークレットも使用されます。

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 モードに入ります。

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 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*]

シンタックスの説明

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

次の表は、このコマンドを入力でき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	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 モード	•	—	•	—	—

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 モードに入る必要があります。

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の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 モードに入ります。

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、元のコマンドが実行されます。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もできます。

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

シンタックスの説明

mode	たとえば、**exec**（ユーザおよび特権 EXEC モードの場合）、**configure**、**interface** などの、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、ユーザ EXEC モードで次のエイリアスが設定されています。

h（***help*** のエイリアス）

lo（***logout*** のエイリアス）

p（***ping*** のエイリアス）

s（***show*** のエイリアス）

コマンド モード

次の表は、このコマンドを入力でき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	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共に表示されます。

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

同じエイリアスを別のモードで使用できます。たとえば、次のように、「happy」を特権 EXEC モードとコンフィギュレーション モードで異なるコマンドのエイリアスに使用できます。

```
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 エイリアスを避けるには、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 happy は表示されません。

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

コマンドと同様に、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、パーサーはコマンド hap を、エイリアス happy を示しているとは認識しません。

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

例

次の例では、***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方法を示します。

```
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	デフォルト以外のコマンド エイリアスをすべて消去します。
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

応答を待つキューに入る 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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

command-queue *limit*

no command-queue *limit*

シンタックスの説明

limit	キューに入るコマンドの最大数（1 ～ 2,147,483,647）を指定します。

デフォルト

このコマンドは、デフォルトでは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

次の表は、このコマンドを入力でき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	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

応答を待つキューに入る 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。許容値の範囲は、1 ～ 4,294,967,295 です。デフォルトは 200 です。限度に到達していて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

次の例では、MGCP コマンド キューを 150 コマンドに制限します。

```
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 に関する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。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。
timeout	MGCP メディア接続または MGCP PAT xlate 接続のアイドル タイムアウトを設定します。このタイムアウト後、その接続が終了します。

compatible rfc1583

RFC 1583 単位のサマリー ルート コスト計算で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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトでは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でき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	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のものです。

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** 形式だけが表示されます。

例

次の例では、RFC 1583 互換ルート サマリー コスト計算をディセーブルにする方法を示します。

```
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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

compression

SVC 接続および WebVPN 接続に対して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。

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

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

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。

シンタックスの説明

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です。

コマンド モード

次の表は、このコマンドを入力でき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	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、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

次の例では、SVC 接続に対して圧縮をオンにしています。

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

次の例では、SVC 接続および WebVPN 接続に対して圧縮をディセーブルにしています。

```
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ついての情報を表示します。
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	SVC 接続上の http データの圧縮を特定のグループまたはユーザに対してイネーブルにします。

config-register

次にセキュリティ 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 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

シンタックスの説明

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。各ビットは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、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、そ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、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

次の表は、このコマンドを入力でき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	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 0 ～ 4 の番号が付けられています。これは、16 進数および 2 進数の規格です。各文字に対して 1 つの値を選択し、必要に応じて値を組み合せたり一致させたりできます。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。値によっては、他の値と競合した場合に優先するものがあります。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設定する 0x2011 を設定する場合、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一覧表示します。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 ROMMON のカウントダウンを 10 秒間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 に入ることができます。	2 セキュリティ アプライアンスを TFTP サーバからブートするように設定し、ブートが失敗した場合、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 に設定された値に優先します。	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。そのイメージが読み込まれない場合、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。値が 3 であると最初の **boot system** コマンドで指定されたイメージがブートされ、値が 5 であると 2 番目のイメージがブートされます（以降同様）。 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（値 1 と値 3 の使用の違い）に戻ることを試行しません。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蔵フラッシュ メモリのルート ディレクトリ内で検出されたいずれか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 コンフィギュレーションを読み込みます。	**2**, **4**, **6**, **8** ROMMON から、引数なしで **boot** 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。値が 3 であると最初の **boot system** コマンドで指定されたイメージがブートされ、値が 5 であると 2 番目のイメージがブートされます（以降同様）。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. 将来の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は、セキュリティ アプライアンスが直接 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を回復できなくした場合は、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装置に複製されませんが、アクティブ装置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.
```

また、**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

次の例では、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工場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。工場出荷時のデフォルトは、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 と PIX 535 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*]]

シンタックスの説明

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

次の表は、このコマンドを入力でき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	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)	ASA 5505 適応型セキュリティ アプライアンスの工場出荷時にデフォルト コンフィギュレーションが追加されるようになりました。

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、工場出荷時のデフォルト 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ます。そのため、ASDM を使用してインターフェイスに接続し、残りの設定を行えます。ASA 5505 適応型セキュリティ アプライアンスでは、工場出荷時のデフォルト 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。透過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消去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消去してから、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。

工場出荷時のデフォルト コンフィギュレーションに戻した後で、内蔵フラッシュ メモリに保存するには、**write memory** コマンドを使用します。**write memory** コマンドは、前に **boot config** コマンドでデフォルトの場所を設定していても、コンフィギュレーションを消去したときにこのパスも消去されているので、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共に消去します。**boot system** コマンドを使用すると、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。工場出荷時のコンフィギュレーションに戻した後、次にセキュリティ アプライアンスをリロードするとき、セキュリティ アプライアンスは内蔵フラッシュ メモリの最初のイメージからブートします。内蔵フラッシュ 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効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 アプライアンスの工場出荷時のデフォルト 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 アドレスを設定しなかった場合は、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 アドレスを割り当てます。
- デフォルトのルートも DHCP によって割り当てられる。
- 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の PAT によって変換される。
- デフォルトでは、内部のユーザの外部へのアクセスはアクセス リストによって制御され、外部のユーザは内部にアクセスできない。
- 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る。
- HTTP サーバは ASDM 用にイネーブルになっており、192.168.1.0 ネットワーク上のユーザがアクセスできる。

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 アプライアンスの工場出荷時のデフォルト 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 アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- 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、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る。
- HTTP サーバは ASDM 用にイネーブルになっており、192.168.1.0 ネットワーク上のユーザがアクセスできる。

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 アプライアンスの工場出荷時のデフォルト 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 アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- 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、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る。
- HTTP サーバは ASDM 用にイネーブルになっており、192.168.1.0 ネットワーク上のユーザがアクセスできる。

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

次の例では、コンフィギュレーションを工場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	ブートするソフトウェア 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消去します。
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 http** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

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

シンタックスの説明

*:*password	（オプション）HTTP(S) 認証の場合、パスワードを指定します。
:port	（オプション）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。
@	（オプション）名前とパスワードの両方またはいずれか一方を入力する場合は、サーバの IP アドレスにアットマーク（@）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	（オプション）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 アドレスの場合、ポートを指定した場合は、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 アドレスを角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	（オプション）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

次の表は、このコマンドを入力でき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	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のものです。

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のすべてのコマンドが実行コンフィギュレーションに追加され、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、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

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、このコマンドを使用できるのはシステム実行スペースに限られるため、**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

次の例では、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消去します。
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 から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とマージします。
configure factory-default	CLI で入力する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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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	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のものです。

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のすべてのコマンドが実行コンフィギュレーションに追加され、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、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

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消去してから、**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読み込むことができます。

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

次の例では、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消去します。
configure http	指定した HTTP(S) URL から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とマージします。
configure net	指定した TFTP URL から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とマージします。
configure factory-default	CLI で入力する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 サーバから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 net** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

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

シンタックスの説明

: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ファイル名をすでに設定している場合、この引数はオプションです。 **tftp-server** コマンドで名前を指定したように、このコマンドでファイル名を指定すると、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、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。このアドレスが存在する場合は、**tftp-server** コマンドで設定したアドレスを上書きします。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 アドレスを角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 ゲートウェイ インターフェイスは最高レベルのセキュリティ 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

次の表は、このコマンドを入力でき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	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のものです。

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のすべてのコマンドが実行コンフィギュレーションに追加され、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、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

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、このコマンドを使用できるのはシステム実行スペースに限られるため、**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

次の例では **tftp-server** コマンドにサーバとファイル名を設定した後、**configure net** コマンドを使用してサーバを上書きします。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:
```

次の例では、サーバとファイル名を上書きします。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/ の部分は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
```

次の例では、サーバだけを **tftp-server** コマンドに設定します。**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 から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とマージします。
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 モードに入ります。

configure terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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	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のものです。

例

次の例では、グローバル コンフィギュレーション モードに入ります。

```
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消去します。
configure http	指定した HTTP(S) URL から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とマージします。
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 から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。

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*

シンタックスの説明

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 シンタックス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 は内蔵フラッシュ 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、エイリアス関係にあります。
- ***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 は内蔵フラッシュ メモリを指します。
- ***ftp://***[*user*[***:***_password_]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;type=***_xx_]

  type には、次のいずれかのキーワードを指定できます。
  - ***ap***：ASCII パッシブ モード
  - ***an***：ASCII 通常モード
  - ***ip***：（デフォルト）バイナリ パッシブ 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

次の表は、このコマンドを入力でき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	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読み込み実行中になります。

（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読み込む前に、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読み込みます。コンテキストにインターフェイスを示すコマンドが含まれていない場合、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、内蔵フラッシュ 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変更内容をそれらのサーバに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。

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システムがコンテキスト コンフィギュレーション ファイルを取得できない場合、システムは、コマンドライン インターフェイスでただち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とマージします。同じ URL を再入力しても、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とマージされます。マージにより、新しいコンフィギュレーションのすべての新しいコマンドが実行コンフィギュレーションに追加されます。コンフィギュレーションが同じ場合、変更は行われません。コマンドが競合する場合、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、マージの効果はコマンドによって異なります。エラーが発生したり、予期しない結果が生じたりすることがあります。実行コンフィギュレーションがブランクの場合（たとえば、サーバが利用不可能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消去してから、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

次の例では、管理コンテキストを「administrator」と設定し、内蔵フラッシュ メモリに「administrator」という名前の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しています。

```
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 モードに入ります。
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*]

シンタックスの説明

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、コンソール セッションはタイムアウトしません。

コマンド モード

次の表は、このコマンドを入力でき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	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のものです。

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 セッションと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については、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の 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

次の例では、コンソール タイムアウトを 15 分に設定する方法を示します。

```
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。
clear configure timeout	コンフィギュレーションにあるアイドル期間をデフォルトに戻します。
show running-config console timeout	セキュリティ アプライアンスへの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。このモードには、**http-map** コマンドを使用してアクセスできます。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**]

シンタックスの説明

action	メッセージがこの検査に合格しなかったときに実行され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 ～ 65,535、**max** オプションでは 1 ～ 50,000,000 です。
drop	接続を終了します。
log	（オプション）syslog を生成します。
max	（オプション）使用可能な最大コンテキスト長を指定します。
min	使用可能な最小コンテキスト長を指定します。
reset	TCP リセット メッセージをクライアントまたはサーバに送信します。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力でき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	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、許可しない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 アプライアンスが TCP 接続をリセットして syslog エントリを作成するようにするには、**action** キーワードを使用します。

例

次の例では、HTTP トラフィックを 100 バイト以上 2,000 バイト以下のメッセージに制限しています。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先のトラフィック クラスを定義します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

content-type-verification

HTTP メッセージのコンテキスト タイプに基づいて 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-type-verification** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

no content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがコマンド検査に合格しなかったときに実行されるアクションを指定します。
allow	メッセージを許可します。
drop	接続を終了します。
log	（オプション）syslog メッセージを生成します。
match-req-rsp	（オプション）HTTP 応答の content-type フィールドが、対応する HTTP 要求メッセージの accept フィールドに一致するかどうかを確認します。
reset	TCP リセット メッセージをクライアントまたはサーバに送信します。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力でき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	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

このコマンドは次のチェックをイネーブルにします。

- ヘッダーの content-type の値が、サポートされているコンテンツ タイプの内部リストにあることを確認します。
- ヘッダーの content-type が、データ内の実際のコンテンツまたはメッセージのエンティティ本体の部分と一致していることを確認します。
- **match-req-rsp** キーワードは、HTTP 応答の content-type フィールドが、対応する HTTP 要求メッセージの **accept** フィールドに一致することを確認する追加のチェックをイネーブルにします。

メッセージが上記のいずれかのチェックに合格しなかった場合、セキュリティ アプライアンスは設定されたアクションを実行します。

次に、サポートされているコンテンツ タイプのリストを示します。

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

このリストの一部のコンテンツ タイプは、対応する正規表現（マジック ナンバー）がないためにメッセージの本体部分で確認できない場合があります。その場合、HTTP メッセージが許可されます。

例

次の例では、HTTP メッセージのコンテンツ タイプに基づいて HTTP トラフィックを制限します。サポートされていないコンテンツ タイプがメッセージに含まれている場合、セキュリティ アプライアンスは TCP 接続を制限し、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-type-verification match-req-rsp 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先のトラフィック クラスを定義します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

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 モードに入るには、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***]

シンタックスの説明

name	名前を最大 32 文字の文字列で指定します。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」と「CustomerA」という名前で 2 つのコンテキストを作成できます。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を使用することはできません。 「System」および「Null」（大文字および小文字）は予約されている名前であるため、使用できません。
noconfirm	（オプション）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、自動スクリプトに役立ちます。

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

次の表は、このコマンドを入力でき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	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消去した場合）、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のみ削除できます。

例

次の例では、管理コンテキストを「administrator」と設定し、内蔵フラッシュ メモリに「administrator」という名前の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しています。

```
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で切り替えを行います。
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	フェールオーバー グループにコンテキストを割り当てます。
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、**copy** コマンドを使用します。

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

シンタックスの説明

/noconfirm	確認プロンプトなし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 サーバを設定するには、**tftp-server** コマンドを参照してください。
running-config	実行コンフィギュレーションを指定します。
startup-config	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 の組み合せには、使用できないものもあります。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の間でのコピーに使用するためのものです。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を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。また、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** コマンドを参照してください。 次の URL シンタックス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 アプライアンスのみで使用でき、内蔵フラッシュ 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、エイリアス関係にあります。 • ***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 アプライアンスのみで使用でき、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、内蔵フラッシュ 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、次のいずれかのキーワードを指定できます。 — ***ap***：ASCII パッシブ モード — ***an***：ASCII 通常モード — ***ip***：（デフォルト）バイナリ パッシブ 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。 ただし、パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**copy tftp** コマンドではなく **tftp-server** コマンドでパスを設定してください。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力でき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	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

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。

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と、2 つのコンフィギュレーションがマージされます。マージにより、新しいコンフィギュレーションのすべての新しいコマンドが実行コンフィギュレーションに追加されます。コンフィギュレーションが同じ場合、変更は行われません。コマンドが競合する場合、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、マージの効果はコマンドによって異なります。エラーが発生したり、予期しない結果が生じたりすることがあります。

例

次の例では、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方法を示します。

```
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方法を示します。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、別の名前することもできます。

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

次の例では、ASDM ファイルを TFTP サーバから内蔵フラッシュ メモリにコピーする方法を示しています。

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

次の例では、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方法を示しています。

```
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（上の例を参照）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。
write memory	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、グローバル コンフィギュレーション 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*

シンタックスの説明

/noconfirm	確認プロンプトなしでファイルをコピーします。
/pcap	パケット キャプチャを未加工の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の名前。
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 シンタックス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、内蔵フラッシュ カードを示します。***disk0*** の代わりに ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***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、内蔵フラッシュ 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、次のいずれかのキーワードを指定できます。 － ***ap***：ASCII パッシブ モード － ***an***：ASCII 通常モード － ***ip***：（デフォルト）バイナリ パッシブ 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。 ただし、パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**copy tftp** コマンドではなく **tftp-server** コマンドでパスを設定してください。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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
特権モード	•	•	•	—	•

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

次の例では、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 キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
clear capture	キャプチャ バッファを消去します。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

cpu profile activate

CPU プロファイル収集情報を開始するには、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*

シンタックスの説明

n-samples	n 個のサンプルを保存するためのメモリを割り当てます。値は 1 ～ 100000 です。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

次の表は、このコマンドを入力でき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	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のものです。

使用上のガイドライン

show cpu profile コマンドを **cpu profile activate** コマンドと組み合せて使用すると、TAC が CPU 問題のトラブルシューティングを支援するために収集および使用できる情報が表示されます。**show cpu profile** コマンドによって表示される情報は 16 進形式です。

例

次の例では、プロファイラを有効にし、5000 個のサンプルを格納するように指示します。

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

show cpu profile コマンドを使用して、結果を確認します。

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

```
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.
```

処理が完了すると、**show cpu profile** コマンド出力によって結果が表示されます。この情報をコピーし、TAC に提出します。TAC がこの情報をデコードします。

```
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 で使用される CPU プロファイル アクティベーション情報を表示します。

crashinfo console disable

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、および設定を行うには、**crashinfo console disable** コマンドを使用します。

crashinfo console disable

[no] crashinfo console disable

シンタックスの説明

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

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力でき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	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、crashinfo がコンソールに出力されないようにすることができます。crashinfo には、装置に接続されたすべてのユーザに対して表示されるのにふさわしくない機密情報が含まれている場合があります。このコマンドと共に、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。これは装置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 に格納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消去します。
fips enable	システムまたはモジュールで FIPS に準拠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	パワーオン セルフテストを実行します。
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**]

シンタックスの説明

page-fault	（オプション）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	（オプション）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

次の表は、このコマンドを入力でき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	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のものです。

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、本物のクラッシュと **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は区別できません。これは、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　実稼働環境では **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

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

```
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、いずれも操作に同意したものと解釈されます。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消去します。
crashinfo test	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する、セキュリティ アプライアンスの機能をテストします。
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。

crashinfo save disable

no crashinfo save disable

シンタックスの説明

このコマンドには、デフォルトの引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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	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。クラッシュ情報をフラッシュ メモリに保存するには、セキュリティ アプライアンスは完全に初期化されて、動作を開始している必要があります。

クラッシュ情報のフラッシュ メモリへ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 ファイルの内容を消去します。
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	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する、セキュリティ アプライアンスの機能をテストします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crashinfo test

セキュリティ アプライアンスの機能をテストして、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 test*** コマンドを使用します。

crashinfo test

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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	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のものです。

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

次の例では、クラッシュ情報ファイル テストの出力を示します。

```
hostname(config)# 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。
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、暗号 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**}

シンタックスの説明

required	必須の CRL は、検証されるピア証明書に対して使用できる必要があります。
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にセキュリティ 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

次の表は、このコマンドを入力でき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	透過	シングル	コンテキスト	システム
暗号 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)(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。新しい **revocation-check** コマンドは、次のとおりです。 • **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

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、CRL がトラストポイント central の検証されるピア証明書に対して使用できることを要求します。

```
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。
crypto ca trustpoint	トラストポイント サブモードに入ります。
crl configure	crl コンフィギュレーション モードに入ります。

crl configure

CRL 設定コンフィギュレーション モードに入るには、暗号 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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	透過	シングル	コンテキスト	システム
暗号 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

次の例では、トラストポイント central 内の crl コンフィギュレーション モードに入ります。

```
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 サブモードに入ります。