



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

client-access-rule

IPSec を介して FWSM に接続できるリモート アクセスのクライアント タイプとバージョンを制限するルールを設定するには、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** コマンドを使用します。これは、**client-access-rule none** コマンドを発行して作成したヌルルールを含む、設定したすべてのルールを削除します。

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 ポリシーに存在する任意のルールを継承します。ユーザがクライアント アクセス ルールを継承できないようにするには、**client-access-rule none** コマンドを使用します。これを行うことにより、すべてのクライアント タイプとバージョンの接続が可能になります。

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

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

シンタックスの説明

deny	特定のタイプとバージョン、またはそのいずれか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 ルールを無効にします。 client-access-rule をヌル値に設定します。その結果、制限が無効となります。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからの値の継承を禁止します。
permit	特定のタイプとバージョン、またはそのいずれかのデバイスの接続を許可します。
<i>priority</i>	ルールのプライオリティを判別します。最小の整数を持つルールが、最大のプライオリティを持ちます。したがって、クライアント タイプとバージョン、またはそのいずれかに一致し、最小の整数を持つ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が相反する場合、FWSM は無視します。

type <i>type</i>	フリー形式の文字列（たとえば、VPN 3002）で、デバイスのタイプを指定します。ワイルドカードとして * 文字を使用できる場合を除いて、文字列が show vpn-sessiondb remote 出力の表示と完全に一致する必要があります。
version <i>version</i>	フリー形式の文字列（たとえば、7.0）で、デバイスのバージョンを指定します。ワイルドカードとして * 文字を使用できる場合を除いて、文字列が show vpn-sessiondb remote 出力の表示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	トランスペ アレント	シングル	マルチ コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

次の注意事項に従って、ルールを作成します。

- ルールを定義しない場合、FWSM がすべての接続タイプを許可します。
- クライアントがルールと一致しない場合、FWSM は接続を拒否します。これは、拒否ルールを定義する場合に、最低 1 つの許可ルールも定義する必要があることを意味します。そうしないと、FWSM がすべての接続を拒否します。
- ソフトウェアおよびハードウェア クライアントの両方で、タイプとバージョンが **show vpn-sessiondb remote** 出力の表示に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、各ルールで 2 回以上使用できます。たとえば、**client-access-rule 3 deny type * version 3.*** は、リリース バージョン 3.x のソフトウェアを実行す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。
- 各グループ ポリシーに最大 25 のルールを作成できます。
- すべてのルール セットで使用できる文字数が、最大 255 文字に制限されています。
- クライアント タイプとバージョン、またはそのいずれか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 ポリシーにクライアント 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し、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

IKE トンネルのネゴシエーション時に FWSM 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。

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-zonealarm 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 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-security-agent

client-firewall opt | req networkkice-blackice

client-firewall opt | req cisco-security-agent

シンタックスの説明

acl-in <ACL>	クライアントがインバウンドトラフィックに使用するポリシーを提供します。
acl-out <ACL>	クライアントがアウトバウンドトラフィックに使用するポリシーを提供します。
AYT	クライアント PC 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ように指定します。FWSM は、ファイアウォールが稼働しているかどうかをチェックします。[Are You There?] と尋ね、応答がないと FWSM によってトンネルが取り除かれます。
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 ポリシーの送信元として Policy Pushed 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記述します。
networkkice-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。ポリシーが使用されないように、ファイアウォール ポリシーにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからファイアウォール ポリシーを継承できないようにします。
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	必須のファイアウォール 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 ベンダーを指定します。
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

このコマンドには、デフォルトの動作または値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、1つのインスタンスだけを設定できます。

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。これは、**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、設定したすべてのファイアウォール ポリシーを削除します。

ファイアウォール ポリシーがない場合、ユーザはデフォルトまたは他のグループ ポリシーに存在する任意のポリシーを継承します。ユーザがこのようなファイアウォール ポリシーを継承できないようにするには、**client-firewall none** コマンドを使用します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、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-update

クライアントの更新パラメータを設定および変更するには、`tunnel-group ipsec-attributes` 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表示されているソフトウェア バージョンをすでに実行している場合、ソフトウェアを更新する必要はありません。クライアントがリストに表示されているソフトウェア バージョンを実行していない場合は、更新する必要があります。最大 4 つのクライアントの更新エントリを指定できます。

クライアントの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。

`client-update type type {url url-string} {rev-nums rev-nums}`

`no client-update [type]`

シンタックスの説明

<code>rev-nums rev-nums</code>	このクライアントのソフトウェアまたはファームウェア イメージを指定します。カンマで区切り、最大 4 つまで入力できます。
<code>type</code>	クライアントの更新を通知する OS (オペレーティング システム) を指定します。OS リストには、次の内容が含まれます。 <ul style="list-style-type: none"> 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 のプラットフォーム WinNT : Windows NT 4.0、Windows 2000、および Windows XP のプラットフォーム vpn3002 : VPN 3002 ハードウェア クライアント
<code>url url-string</code>	ソフトウェア / 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適切なファイルを指している必要があります。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

この属性を適用できるのは、IPSec リモートアクセス トンネルグループ タイプだけです。クライアントがリビジョン番号のリストに表示されているソフトウェア バージョンをすでに実行している場合、ソフトウェアを更新する必要はありません。クライアントがリストに表示されているソフトウェア バージョンを実行していない場合は、更新する必要があります。

例 次に、config-ipsec コンフィギュレーション モードで、リモート アクセス トンネル グループ remotegrp にクライアントの更新パラメータを設定する例を示します。リビジョン番号 4.6.1 と更新を取得するための URL (<https://support/updates>) を指定します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたトンネル グループをすべて消去します。
show running-config tunnel-group	指定された証明書マップ エントリを表示します。
tunnel-group-map enable	crypto ca certificate map コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。

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、元のコマンドが起動します。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を提供することが必要な場合もあります。

```
command-alias mode command_alias original_command
```

```
no command-alias mode command_alias original_command
```

シンタックスの説明

<i>mode</i>	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。たとえば、 exec (ユーザ モードおよび特権 EXEC モード)、 configure 、または interface を指定します。
<i>command_alias</i>	既存のコマンドに対して新しい名前を指定します。
<i>original_command</i>	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付きの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 モードのエイリアスが設定されます。

h — *help*

lo — *logout*

p — *ping*

s — *show*

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

コマンドの最初の部分に対するエイリアスを作成しても、通常どおりに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 エイリアスにはアスタリスク (*) が適用され、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] で開始する他の特権 EXEC モード コマンドと一緒に表示されます。

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

別のモードで同じエイリアスを使用できます。たとえば、次のように特権 EXEC モードとコンフィギュレーション モードで [happy] を使用して、同じエイリアスで異なるコマンドを表示できます。

```
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、スペースで入力行を開始します。また、コマンドエイリアスを避けるには、スペースを使用してから、コマンドを入力します。次の例では、happy? コマンドの前にスペースがあるので、エイリアスの happy が表示されていません。

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

コマンドでは、CLI ヘルプを使用して、コマンドエイリアスのあとに入力可能な引数とキーワードを表示できます。

完全な形式のコマンドエイリアスを入力する必要があります。短縮形のエイリアスは受け入れられません。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* コマンドに対する [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	非デフォルト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	設定された非デフォルトのすべてのコマンドエイリアスを表示します。

command-queue

応答待機中にキューに格納される 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

シンタックスの説明

limit キューに格納する最大コマンド数を指定します。範囲は、1 ~ 2147483647 です。

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です。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスパレント	シングル	マルチコンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	No

コマンド履歴

リリース	変更
3.1	このコマンドが追加されました。

使用上のガイドライン

応答待機中にキューに格納される 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。許容範囲値は、1 ~ 4294967295 です。デフォルトの値は、200 です。制限に達した場合に、新しいコマンドが着信すると、キュー格納期間が最も長いコマンドが削除されます。

例

次に、MGCP コマンドキューを 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 のデバッグ情報を表示できるようにします。
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開始します。
show mgcp	MGCP の設定およびセッション情報を表示します。
timeout [mgcp]	MGCP メディア接続が閉じられるまでのアイドルタイムアウトを設定します。
timeout [mgcp-pat]	MGCP PAT xlate が削除されるまでのアイドルタイムアウトを設定します。

compatible rfc1583

サマリー ルート コスト計算で使用する方式を RFC 1583 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 の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。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキスト	システム
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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン コンフィギュレーションに含まれるのは、コマンドの **no** 形式だけです。

例 次に、RFC 1583 に準拠したルート サマリー 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に指定されているコマンドを表示します。

configure http

HTTP (HTTPS) 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 http** コマンドを使用します。このコマンドは IPv4 および IPv6 アドレスをサポートします。

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

シンタックスの説明

<code>:password</code>	(任意) HTTP (HTTPS) 認証に対して、パスワードを指定します。
<code>:port</code>	(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。
<code>@</code>	(任意) 名前とパスワード、またはそのいずれかを入力する場合、サーバの IP アドレスの前にアットマーク (@) を入力します。
<code>filename</code>	コンフィギュレーションのファイル名を指定します。
<code>http[s]</code>	HTTP または HTTPS のいずれかを指定します。
<code>path</code>	(任意) ファイル名へのパスを指定します。
<code>server</code>	サーバの IP アドレスまたは名前を指定します。IPv6 サーバのアドレスでは、ポートを指定する場合、IP アドレスをカッコで囲み、IP アドレスのコロンがポート番号の前のコロンであると誤って解釈されないようにする必要があります。たとえば、次のアドレスとポートを入力します。 [fe80::2e0:b6ff:fe01:3b7a]:8080
<code>user</code>	(任意) HTTP (HTTPS) 認証に対して、ユーザ名を指定します。

デフォルト

HTTP の場合、デフォルトのポートは 80 です。HTTPS の場合、デフォルトのポートは 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。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

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を実行コンフィギュレーションに追加し、新しいバージョンと競合するコマンドを上書きします。たとえば、コマンドが複数のインスタンスを許可する場合、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。コマンドが 1 つのインスタンスだけを許可する場合、新しいコマンドが実行コンフィギュレーションのコマンドを上書きします。マージでは、実行コンフィギュレーションに存在していても新しいコンフィギュレーションに設定されていないコマンドは削除しません。

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 モードでは、このコマンドはシステムの実行スペースでしか利用できないので、**configure http** コマンドがコンテキスト内で使用する場合の代わりにコマンドとなります。

■ configure http

例 次に、HTTPS 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 ファイル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に実行コンフィギュレーションをマージします。
configure net	指定された TFTP URL のコンフィギュレーション ファイルに実行コンフィギュレーションをマージします。
show running-config	実行コンフィギュレーションを表示します。

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 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 このコマンドには、デフォルトの動作または値はありません。

コマンド モード 次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン 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を実行コンフィギュレーションに追加し、新しいバージョンと競合するコマンドを上書きします。たとえば、コマンドが複数のインスタンスを許可する場合、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。コマンドが 1 つのインスタンスだけを許可する場合、新しいコマンドが実行コンフィギュレーションのコマンドを上書きします。マージでは、実行コンフィギュレーションに存在して、新しいコンフィギュレーションに設定されていないコマンドは削除しません。

コンフィギュレーションをマージしない場合、実行コンフィギュレーションをクリアし (FWSM を通過する通信を中断させます)、**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 モードでは、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** コマンドで指定された場所にあります。

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
	<code>clear configure</code>	実行コンフィギュレーションをクリアします。
	<code>configure http</code>	指定した HTTP (HTTPS) 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。
	<code>configure net</code>	指定された TFTP URL のコンフィギュレーション ファイルに実行コンフィギュレーションをマージします。
	<code>configure factory-default</code>	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。
	<code>show running-config</code>	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 アドレスをサポートします。

```
write net [server:[filename] | :filename]
```

シンタックスの説明

<code>:filename</code>	<p>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が設定されている場合は、この引数を省略できます。</p> <p>tftp-server コマンドの名前だけでなく、このコマンドでファイル名を指定する場合、FWSM は tftp-server コマンドのファイル名をディレクトリとして扱い、configure net コマンドのファイル名をそのディレクトリの下にあるファイルとして追加します。</p> <p>tftp-server コマンドの値を上書きするには、パスおよび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なく、絶対パスであることを示します。このファイルに対して生成された URL には、ファイル名パスの前に二重スラッシュ (//) が付加されます。必要なファイルが tftpboot ディレクトリ内にある場合は、ファイル名パスに tftpboot ディレクトリのパスを含めることができます。</p> <p>tftp-server コマンドを使用して TFTP サーバアドレスを指定した場合は、コロン (:) を入力し、そのあとにファイル名のみを入力します。</p>
<code>server:</code>	<p>TFTP サーバの IP アドレスまたは名前を設定します。このアドレスは、tftp-server コマンドで設定されたアドレス (存在する場合) を上書きします。IPv6 サーバのアドレスでは、IP アドレスをカッコで囲み、IP アドレスのコロンがファイル名の前のコロンであると誤って解釈されないようにする必要があります。たとえば、次のアドレスを入力します。</p> <pre>[fe80::2e0:b6ff:fe01:3b7a]</pre> <p>デフォルト ゲートウェイ インターフェイスは、セキュリティが最大のインターフェイスです。 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。</p>

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

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を実行コンフィギュレーションに追加し、新しいバージョンと競合するコマンドを上書きします。たとえば、コマンドが複数のインスタンスを許可する場合、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。コマンドが 1 つのインスタンスだけを許可する場合、新しいコマンドが実行コンフィギュレーションのコマンドを上書きします。マージでは、実行コンフィギュレーションに存在して、新しいコンフィギュレーションに設定されていないコマンドは削除しません。

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 モードでは、このコマンドはシステムの実行スペースでしか利用できないので、**configure net** コマンドがコンテキスト内で使用する場合の代替のコマンドとなります。



(注)

「:end」という文字列は、FWSM が設定の終わりを明示するために使用しているので、FWSM に導入する予定のテキストファイルの末尾に「:end」を付けないようにします。

例

次に、**tftp-server** コマンドで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無効にする例を示します。同じファイル名が使用されます。

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

次の例は、サーバとファイル名を無効にします。ファイル名へのデフォルトのパスは、/tftpboot/configs/config1 です。ファイル名の先頭にスラッシュ (/) を入力しない場合、デフォルトでパスの /tftpboot/ 部分が加えられます。このパスを無効にする予定で、またファイルが tftpboot に存在するので、**configure net** コマンドで tftpboot パスを加えます。

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

関連コマンド

コマンド	説明
configure http	指定した HTTP (HTTPS) 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に実行コンフィギュレーションをマージします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	その他のコマンドで使用する デフォルトの TFTP サーバおよびパスを設定します。
write net	TFTP サーバに実行コンフィギュレーションをコピーします。

configure terminal

コマンドラインで実行コンフィギュレーションを設定するには、特権 EXEC モードで **configure terminal** コマンドを使用します。このコマンドはグローバル コンフィギュレーション モードを開始し、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ようにします。

configure terminal

シンタックスの説明 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 このコマンドには、デフォルトの動作または値はありません。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスパ アレント	シングル	マルチ 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
2.2(1)	このコマンドが追加されました。

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 (HTTPS) 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に実行コンフィギュレーションをマージします。
	configure net	指定された TFTP URL のコンフィギュレーション ファイルに実行コンフィギュレーションをマージします。
	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の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	<p>コンテキストのコンフィギュレーションの URL を設定します。管理コンテキストからすべてのリモート URL にアクセス可能にする必要があります。次の URL 構文を参照してください。</p> <ul style="list-style-type: none"> • disk:[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、次のいずれかのキーワードを使用できます。 <ul style="list-style-type: none"> – 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 • ftpp:[user[:password]@]server[:port]/[path]/filename[:int=interface_name] サーバのアドレスへのルートが無効にする場合、インターフェイス名を指定します。
------------	---

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

コンテキストの 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んで、実行します。



(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。FWSM では、コンテキストのコンフィギュレーションを読み込む前にインターフェイスをコンテキストに割り当てる必要があります。コンテキストのコンフィギュレーションには、インターフェイスに関するコマンド (**interface**、**nat**、**global** など) が含まれる場合があります。最初に **config-url** コマンドを入力すると、FWSM はコンテキストのコンフィギュレーションをただちに読み込みます。コンテキストにインターフェイスに関連するコマンドが含まれている場合、これらのコマンドは機能しません。

ファイル名にファイルの拡張子を使用することは必須ではありませんが、`[.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 メモリ上に保管されている必要があります。

HTTP または HTTPS サーバからコンテキストのコンフィギュレーションをダウンロードする場合、**copy running-config startup-config** コマンドを使用して、これらのサーバに戻って変更内容を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。

サーバが使用できないために、システムがコンテキストのコンフィギュレーション ファイルを取得できない場合、またはファイルが存在しない場合には、システムは空のコンテキストを作成します。空のコンテキストは、CLI (コマンドライン インターフェイス) を使用してすぐに設定できます。

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。FWSM 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。同一の URL を再入力することによって、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。マージすると、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である場合、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する場合、マージの結果がコマンドによって異なります。エラーまたは予期せぬ結果が生じる場合があります。実行コンフィギュレーションが空の場合 (たとえば、サーバが使用できなかった場合や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) には、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、実行コンフィギュレーションをクリアし (コンテキストを通過する通信を中断させます)、新しい URL からコンフィギュレーションをリロードできます。

例

次に、管理コンテキストを `[administrator]` に設定し、内部フラッシュ メモリに `[administrator]` という名前のコンテキストを作成し、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 vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# class gold
hostname(config-ctx)# allocate-acl-partition 0

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# class silver
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスをコンテキストに割り当てます。
context	システム コンフィギュレーション内にセキュリティ 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 (システム実行スペース) リスト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

FWSM に対する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。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

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数 (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 です。この場合、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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース **変更**
3.1(1) このコマンドが追加されました。

使用上のガイドライン

console timeout コマンドは、Telnet または SSH タイムアウトを変更しません。これらのアクセス方法は、**timeout** コマンドを使用して独自のタイムアウト値を保持しています。

no console timeout コマンドは、コンソールのタイムアウト値をリセットして 0 のデフォルトのタイムアウトにします。つまり、コンソールはタイムアウトしません。

例

次に、コンソールのタイムアウトを 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	コンソール接続の設定をデフォルトに戻します。
show running-config console timeout	FWSM 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。
timeout	接続、変換 UDP、および RPC スロットのアイドル時間を設定します。

content-length

HTTP メッセージ本体の長さに基づいて 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、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をパスしない場合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。 min オプションの許容範囲は 1 ~ 65535 です。 max オプションの場合は 1 ~ 50000000 です。
drop	接続を終了します。
log	(任意) Syslog を生成します。
max	(任意) 許可されるコンテキストの最大長を指定します。
min	許可されるコンテキストの最小長を指定します。
reset	クライアントおよびサーバに TCP リセットメッセージを送信します。

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。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキスト	システム
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
3.1	このコマンドが追加されました。

使用上のガイドライン

content-length コマンドがイネーブルにされると、FWSM は設定された範囲内のメッセージだけを許可し、それ以外の場合は指定されたアクションを実行します。FWSM が TCP 接続をリセットし、Syslog エントリを作成するには、**action** キーワードを使用します。

例

次に、HTTP トラフィックを 100 ~ 2000 バイト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である場合、FWSM 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 検査を設定するために HTTP マップを定義します。
debug appfw	拡張 HTTP 検査に関連付けられたトラフィックの詳細情報を表示します。
inspect http	特定の HTTP マップがアプリケーション検査で使用されるようにします。
policy-map	特定のセキュリティアクションにクラス マップを対応付けます。

content-type-verification

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	メッセージがこのコマンドの検査をパスしない場合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。
drop	接続を終了します。
log	(任意) Syslog メッセージを生成します。
match-req-rsp	(任意) 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します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。

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。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキスト	システム
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
3.1	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、次のチェックをイネーブルにします。

- ヘッダーのコンテンツ タイプ値が、サポートされているコンテンツ タイプの内部リストに存在することを確認します。

- ヘッダーのコンテンツ タイプが、データ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に一致す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付加的な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パスしない場合、FWSM が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 タイプには、対応する正規表現（マジック番号）がない場合があります。そのため、メッセージの本体部分が確認されません。このような場合、HTTP メッセージが許可されます。

例

次に、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する例を示します。メッセージにサポートされていないコンテンツ タイプが含まれる場合、FWSM が 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-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トラフィック クラスを定義します。
http-map	拡張 HTTP 検査を設定するために HTTP マップを定義します。
debug appfw	拡張 HTTP 検査に関連付けられたトラフィックの詳細情報を表示します。
inspect http	特定の HTTP マップがアプリケーション検査で使用されるようにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。

context

システムの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て、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、コンテキストが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	名前として、32 文字までの長さのテキスト文字列を設定します。この名前は大文字と小文字が区別されるので、たとえば、[customerA] と [CustomerA] という名前の 2 つのコンテキストを設定できます。文字、数字、またはハイフンを使用できますが、ハイフンで名前を開始または終了することはできません。 [System] または [Null] (大文字または小文字) は予約名なので、使用できません。
noconfirm	(任意) 確認プロンプトを表示することなく、コンテキストを削除します。このオプションは、自動化されたスクリプトで便利です。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

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)、最初に追加するコンテキストが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場合は、**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ら、**context** コマンドを入力して、管理コンテキストを設定できます。

システムのコンフィギュレーションを編集することによってのみ、コンテキストを削除できます。このコマンドの **no** 形式を使用して、現在の管理コンテキストを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する場合にのみ、このコンテキストを削除できます。

例 次に、管理コンテキストを [administrator] に設定し、内部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、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 vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

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	各コンテキスト間またはシステムの実行スペースとの切り替えを行います。
config-url	コンテキスト設定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

ファイルを特定の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] {url | running-config | startup-config} {running-config | startup-config | url}
```

シンタックスの説明

/noconfirm	確認プロンプトを表示することなく、ファイルをコピーします。
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 メモリで非表示になっているファイルです。コンテキスト内から、 config-url コマンドを使用して、スタートアップ コンフィギュレーションの場所が指定されます。たとえば、 config-url コマンドの HTTP サーバを指定してから、 copy startup-config running-config コマンドを入力する場合、FWSM 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 コピーする送信元または宛先ファイルを指定します。送信元 URL と宛先 URL のすべての組み合わせが許可されるとは限りません。たとえば、リモート サーバから別のリモート サーバにはコピーできません。このコマンドは、ローカルとリモート ロケーション間のコピー用です。コンテキストでは、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 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 サーバから実行中のコンテキスト コンフィギュレーションにダウンロードする場合は、**configure net** コマンドも参照してください。

次の URL 構文を参照してください。

- **disk:[path]/filename**
このオプションは、内部フラッシュ メモリのコンフィギュレーション パーティションを示します。
- **flash:[image | asdm]**
このオプションは、アプリケーション イメージまたは ASDM をコピーする内部フラッシュ メモリを示します。**image** は、デフォルトです。
- **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使用できます。
 - **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]**
サーバのアドレスへのルートを無効にする場合、インターフェイス名を指定します。
パス名にスペースを入れることはできません。パス名にスペースがある場合は、**copy tftp** コマンドではなく、**tftp-server** コマンドでパスを設定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。
3.1(1)	コンテキストからサーバにコピーする機能が追加されました。

使用上のガイドライン

実行コンフィギュレーションにコンフィギュレーションをコピーする場合、2 つのコンフィギュレーションをマージします。マージすると、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である場合、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する場合、マージの結果がコマンドによって異なります。エラーまたは予期せぬ結果が生じる場合があります。

例

次に、ディスクからシステムの実行スペース内の TFTP サーバにファイルをコピーする例を示します。

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

次に、ディスク上のある場所から別の場所にファイルをコピーする例を示します。コピー先のファイル名は、コピー元のファイル名でも、別のファイル名でも構いません。

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

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

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

次に、コンテキスト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
```

関連コマンド

コマンド	説明
configure net	TFTP サーバから実行コンフィギュレーションにファイルをコピーします。
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	TFTP サーバに実行コンフィギュレーションをコピーします。

copy capture

サーバにキャプチャ ファイルをコピーするには、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
```

シンタックスの説明

/noconfirm	確認プロンプトを表示することなく、ファイルをコピーします。
/pcap	未加工のデータとしてパケット キャプチャをコピーします。
buffer_name	キャプチャを識別するための一意の名前を指定します。
context_name/	セキュリティ コンテキストで定義されるパケット キャプチャをコピーします。
url	パケット キャプチャ ファイルをコピーする宛先を指定します。次の URL 構文を参照してください。 <ul style="list-style-type: none"> • disk:/path/filename このオプションは、内部フラッシュ メモリのコンフィギュレーション パーティションを示します。 • ftp://user[:password]@[server[:port]/path/filename[:type=xx] サーバ上の FTP パスは相対パス (<i>path/filename</i>) です。絶対パス (<i>/path/filename</i>) を使用するには、サーバアドレスの後にスラッシュ (/) を入力します。 ftp://server/path/filename type には、次のいずれかのキーワードを使用できます。 <ul style="list-style-type: none"> — 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] サーバのアドレスへのルートを無効にする場合、インターフェイス名を指定します。 パス名にスペースを入れることはできません。パス名にスペースがある場合は、copy tftp コマンドではなく、tftp-server コマンドでパスを設定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴	リリース	変更
	2.2(1)	このコマンドが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、このコマンドをシステム実行スペースに入力します。このコマンドをコンテキスト内に入力することはできません。

例

次の例は、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ています。

```
hostname# 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
!!!!!!!!!!!!!!
```

フルパスは、次のように指定できます。

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

TFTP サーバが設定されている場合は、次のように位置やファイル名を省略できます。

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

マルチ コンテキスト モードで、コンテキスト内からキャプチャをコピーするには、コンテキスト名を指定する必要があります。

```
hostname/Context1# capture abc access-list test interface inside
hostname/Context1# changeto system
hostname# copy capture:Context1/abc tftp:171.68.11.129/tftpboot/abc.cap
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能をイネーブルにして、パケット スニフィングおよびネットワーク障害検出を有効にします。
clear capture	キャプチャ バッファを消去します。
show capture	オプションが指定されていない場合に、キャプチャのコンフィギュレーションを表示します。

crashinfo force

FWSM を強制的にクラッシュするには、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	(任意) ページフォールトの結果を受けて、FWSM を強制的にクラッシュします。
watchdog	(任意) ウォッチドッグの結果を受けて、FWSM を強制的にクラッシュします。

デフォルト

デフォルトでは、FWSM が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。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスパ アレント	シングル	マルチ 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
3.1	このコマンドが追加されました。

使用上のガイドライン

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。FWSM 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、FWSM をクラッシュして、強制的にリロードします。

例

次の例は、**crashinfo force page-fault** コマンドを入力した場合に表示される警告を表示します。

```
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 CR (復帰) を入力するか、[y] キーまたは [Y] キーを押すと、FWSM 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、処理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、FWSM はコマンドラインプロンプトに戻ります。

関連コマンド

コマンド	説明
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	フラッシュ メモリへのクラッシュ情報の書き込みを禁止します。
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 FWSM 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 メモリにクラッシュ情報を書き込まないようにするには、グローバル コンフィギュレーション モードで *crashinfo save disable* 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、FWSM がフラッシュ 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。

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

コマンド履歴

リリース	変更
3.1(1)	<i>crashinfo save enable</i> コマンドは廃止され、すでに無効になっています。代わりに、 <i>no crashinfo save disable</i> コマンドを使用してください。

使用上のガイドライン

クラッシュ情報はフラッシュ メモリに書き込まれてから、コンソールに書き込まれます。



(注)

起動時に FWSM がクラッシュした場合、クラッシュ情報ファイルが保存されません。フラッシュ メモリにクラッシュ情報を保存するには、FWSM が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。

フラッシュ メモリに対するクラッシュ情報の保存を再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

コマンド	説明
clear crashinfo	クラッシュ ファイルの内容をクリアします。
crashinfo force	FWSM 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 FWSM 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

FWSM がフラッシュ メモリ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 このコマンドには、デフォルトの動作または値はありません。

コマンド モード 次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン 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ある場合、そのファイルが上書きされま
す。



(注) **crashinfo test** コマンドを入力しても、FWSM はクラッシュされません。

例 次に、クラッシュ情報ファイル test の出力例を示します。

```
hostname(config)# crashinfo test
```

関連コマンド	コマンド	説明
	clear crashinfo	クラッシュ ファイルの内容を削除します。
	crashinfo force	FWSM を強制的にクラッシュします。
	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禁止します。
	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のオプションを指定するには、`crypto 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

必須	ピア証明書の検証用に必須の CRL が使用可能である必要があります。
optional	必須の CRL が使用不可の場合でも、FWSM はピア証明書を受け入れることができます。
nocheck	FWSM が CRL のチェックを実行しないように指定します。

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。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスパ アレント	シングル	マルチ コンテキスト	システム
crypto 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
3.1(1)	このコマンドが追加されました。

例

次に、トラストポイント `central` の `crypto 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、トラストポイント `central` に対するピア証明書の検証用に CRL が使用可能であるように要求する例を示します。

```
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
<code>clear configure crypto ca trustpoint</code>	すべてのトラストポイントを削除します。
<code>crypto ca trustpoint</code>	トラストポイントサブモードを開始します。
<code>crl configure</code>	<code>crl</code> 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のコンフィギュレーション モードを開始するには、crypto 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 このコマンドには、デフォルトの動作または値はありません。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキスト	システム
crypto 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
3.1(1)	このコマンドが追加されました。

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 サブモードを開始します。