FlexConfig ポリシー

次のトピックでは、FlexConfig ポリシーを設定して導入する方法について説明します。

FlexConfig ポリシーの概要

FlexConfig ポリシーは FlexConfig オブジェクトの番号付きリストのコンテナです。各オブジェクトは、定義する一連の Apache Velocity のスクリプト言語コマンド、ASA ソフトウェアの設定コマンド、および変数に影響を与えます。各 FlexConfig オブジェクトの内容は、基本的に、割り当てられたデバイスに展開する一連の ASA コマンドを生成するプログラムです。このコマンド シーケンスは、その後、Threat Defense デバイスで関連機能を設定します。

Threat Defense では、ASA 設定コマンドを使用して、すべての機能ではなく一部の機能を実装します。Threat Defense 設定コマンドの一意のセットはありません。代わりに、FlexConfig のポイントは、Management Center ポリシーおよび設定を介して直接まだサポートされていない機能を設定できることです。

注意 シスコでは、ASA に精通している上級ユーザーが自身の責任で行う場合にのみ FlexConfig ポリシーを使用することを**強く**お勧めします。禁止されていないコマンドはすべて、設定できます。FlexConfig ポリシーによって機能を有効にすると、他の設定された機能により意図しない結果を引き起こす可能性があります。

設定した FlexConfig ポリシーに関するサポートについては、Cisco Technical Assistance Center にお問い合わせください。Cisco Technical Assistance Center は、顧客に代わってカスタム設定を設計したり、作成したりしません。シスコは、その他の Firepower システムの機能との正しい動作または相互運用性を保証しません。FlexConfig 機能は廃止になる可能性があります。完全に保証された機能のサポートについては、Management Center サポートを待つ必要があります。判別できない場合は、FlexConfig ポリシーを使用しないでください。

FlexConfig ポリシーの推奨される使用法

FlexConfig ポリシーには、推奨される使用法が主に 2 つあります。

- ASA から Threat Defense に変換し、Management Center で直接サポートされない互換機能を使用している（および引き続き使用する必要がある）場合。この場合、ASA で **show running-config** コマンドを使用してその互換機能の設定を確認し、その機能を実装する FlexConfig オブジェクトを作成します。オブジェクトの導入設定（1 回/毎回、前に付加/後ろに付加）をいろいろと試して、正しい設定になるようにします。2 台のデバイスでの **show running-config** の出力を比較して確認します。
- Threat Defense を使用しているものの、構成が必要な設定または機能がある場合（たとえば、Cisco Technical Assistance Center から、発生している特定の問題を解決するための具体的な設定を指示された場合）。複雑な機能については、ラボデバイスを使用して FlexConfig をテストし、期待する動作を得られることを確認します。

システムには、テスト対象の設定を表す一連の定義済み FlexConfig オブジェクトが含まれています。これらのオブジェクトのなかに必要な機能を表すものがない場合は、まず、標準ポリシーで同等の機能を設定できるかどうかを判断します。たとえば、アクセス コントロール ポリシーには侵入検知および防御、HTTP およびその他のタイプのプロトコル インスペクション、URL フィルタリング、アプリケーション フィルタリング、アクセス制御が含まれており、ASA はこれらの要素を別個の機能を使用して実装します。多くの機能は CLI コマンドを使用して設定されていないので、**show running-config** の出力にすべてのポリシーが表示されるわけではありません。

（注） 常に、ASA と Threat Defense との間の重複は 1 対 1 であるわけではないことに注意してください。Threat Defense デバイスで ASA 設定を完全に作成し直そうとしないでください。設定する機能は、FlexConfig を使用して慎重にテストする必要があります。

FlexConfig オブジェクトの CLI コマンド

Threat Defense では一部の機能の設定に ASA コンフィギュレーション コマンドを使用します。ASA のすべての機能に Threat Defense との互換性があるわけではありませんが、Threat Defense で使用はできるが Management Center ポリシーでは設定できない機能があります。こうした機能を設定するには、FlexConfig オブジェクトを使って必要な CLI を指定します。

FlexConfig を使って手動で機能を設定する場合、ユーザは自身の責任において正しいコマンド シンタックスを理解し、実装してください。FlexConfig ポリシーは CLI コマンド シンタックスの検証は行いません。正しいシンタックスと CLI コマンドの設定に関する詳細については、ASA ドキュメンテーションを参照してください。

- 『ASA CLI Configuration Guides』では機能を設定する方法について説明しています。ガイドはこちらからご覧ください。 https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- 『ASA Command References』ではコマンド名ごとにその他の情報が記載されています。リファレンスはこちらからご覧ください。 https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

ここでは、コンフィギュレーション コマンドについて詳しく説明します。

ASA ソフトウェアのバージョンおよび現在の CLI 設定の特定

システムが ASA ソフトウェア コマンドを使用して一部の機能を設定するため、Threat Defense デバイスで実行するソフトウェアで使用されている現在の ASA バージョンを特定する必要があります。このバージョン番号に従って、機能設定時の手順に使用する ASA CLI 設定ガイドを選択します。また、現在の CLI ベースの設定を確認し、実装する ASA 設定と比較する必要があります。

Threat Defense 設定とどの ASA 設定も大きく異なることに注意してください。Threat Defense ポリシーの多くは CLI の外部で設定されるため、コマンドを調べても設定を確認することができません。ASA と Threat Defense 設定が 1 対 1 で対応するように作成しようとしないでください。

この情報を表示するには、デバイスの管理インターフェイスへの SSH 接続を確立し、次のコマンドを発行します。

- **show version system** また、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号を検索します。（Secure Firewall Management Center CLI ツールを使用してコマンドを発行する場合は、**system** キーワードを省略します。）
- **show running-config** 現在の CLI 設定を表示します。
- **show running-config all** 現在の CLI 設定にすべてのデフォルト コマンドを含めます。

また、次の手順を使用して、Management Center 内からこれらのコマンドを発行することもできます。

手順

ステップ 1 **[システム（System）]** > **[ヘルス（Health）]** > **[モニタ（Monitor）]** を選択します。

ステップ 2 FlexConfig ポリシーの対象となるデバイスの名前をクリックします。

目的のデバイスを表示するために、[ステータス（Status）] テーブルの [カウント（Count）] カラムにある開く/閉じるの矢印をクリックする必要がある場合があります。

ステップ 3 [システムとトラブルシューティングの詳細を表示（View System and Troubleshoot Details）] をクリックします。

ステップ 4 [詳細なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 5 [脅威防御 CLI（Threat Defense CLI）] をクリックします。

ステップ 6 [デバイス（Device）] を選択し、次にコマンドとして **show** を選択し、パラメータとして **version** を入力するか、他のコマンドの 1 つを入力します。

ステップ 7 [実行（Execute）] をクリックします。

version を入力した場合、Cisco 適応型セキュリティアプライアンス ソフトウェアのバージョン番号の出力を検索します。

後で実行する分析のために、出力を選択して Ctrl + C を押し、テキスト ファイルに貼り付けることができます。

禁止された CLI コマンド

FlexConfig の目的は、Management Center を使用している Threat Defense デバイスで設定できない ASA デバイスで使用可能な機能を設定することです。

したがって、Management Center に同等の機能がある ASA 機能は設定することができません。次の表に、これらの禁止されたコマンド領域のいくつかを示します。

また、一部の **clear** コマンドは管理対象ポリシーと重複しており、管理対象ポリシーの設定の一部を削除する可能性があるため禁止されています。

FlexConfig オブジェクト エディタでは、禁止されたコマンドをオブジェクトに含めることはできません。

禁止された CLI コマンド	説明
AAA	設定がブロックされます。
AAA-Server	設定がブロックされます。

禁止された CLI コマンド	説明
Access-list	高度 ACL、拡張 ACL、および標準 ACL がブロックされます。Ethertype ACL は許可されます。 テンプレート内のオブジェクト マネージャで定義されている標準および拡張 ACL オブジェクトを変数として使用することができます。
ARP Inspection	設定がブロックされます。
As-path Object	設定がブロックされます。
Banner	設定がブロックされます。
BGP	設定がブロックされます。
Clock	設定がブロックされます。
Community-list Object	設定がブロックされます。
コピー（Copy）	設定がブロックされます。
削除（Delete）	設定がブロックされます。
DHCP	設定がブロックされます。
パスワードを有効にする（Enable Password）	設定がブロックされます。
削除（Erase）	設定がブロックされます。
Fragment Setting	**fragment reassembly** を除きブロックされます。
Fsck	設定がブロックされます。
HTTP	設定がブロックされます。
ICMP	設定がブロックされます。
インターフェイス（Interface）	**nameif**、**mode**、**shutdown**、**ip address**、および **mac-address** コマンドのみがブロックされます。
Multicast Routing	設定がブロックされます。
NAT	設定がブロックされます。
Network Object/Object-group	FlexConfig オブジェクトでの Network オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているネットワーク オブジェクトとグループを変数として使用することができます。

禁止された CLI コマンド	説明
NTP	設定がブロックされます。
OSPF/OSPFv3	設定がブロックされます。
ポケットベル	設定がブロックされます。
パスワードの暗号化	設定がブロックされます。
Policy-list Object	設定がブロックされます。
Prefix-list Object	設定がブロックされます。
リロード（Reload）	リロードはスケジュールできません。システムは、システムを再起動するために **reload** コマンドを使用せず、**reboot** コマンドを使用します。
RIP	設定がブロックされます。
Route-Map Object	FlexConfig オブジェクトでの Route-map オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているルートマップ オブジェクトを変数として使用することができます。
Service Object/Object-group	FlexConfig オブジェクトでの Service オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているポート オブジェクトを変数として使用することができます。
SNMP	設定がブロックされます。
SSH	設定がブロックされます。
Static Route	設定がブロックされます。
Syslog	設定がブロックされます。
Time Synchronization	設定がブロックされます。
Timeout	設定がブロックされます。
VPN	設定がブロックされます。

テンプレート スクリプト

スクリプト言語を使用して、FlexConfig オブジェクト内部での処理を制御できます。スクリプト言語命令は、Apache Velocity 1.3.1 テンプレート エンジンでサポートされているコマンドの

サブセットです。Velocity テンプレート エンジンは、ループ、if/else ステートメント、および変数をサポートする Java ベースのスクリプト言語です。

スクリプト言語の使用方法についての詳細は、『*Velocity Developer Guide*』（http://velocity.apache.org/engine/devel/developer-guide.html）を参照してください。

FlexConfig 変数

コマンドまたは処理手順の一部がスタティック情報ではなくランタイム情報に依存する場合は、FlexConfig オブジェクトに変数を使用できます。展開時に、変数は変数のタイプに基づいてデバイスのその他の設定から取得された文字列に置き換えられます。

- ポリシー オブジェクト変数は、Management Center で定義されているオブジェクトから取得された文字列に置き換えられます。
- システム変数は、デバイス自体やデバイスに設定されたポリシーから取得した情報に置き換えられます。
- プロセス変数は、スクリプト コマンドの処理時に、ポリシー オブジェクトまたはシステム変数の内容とともにロードされます。たとえば、ループで、ポリシーオブジェクトまたはシステム変数から 1 つの値をプロセス変数に反復してロードし、プロセス変数を使用して、コマンド文字列を形成するか、その他のアクションを実行します。これらのプロセス変数は、FlexConfig オブジェクト内の [変数（Variables）] リストに表示されません。また、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用してこれらを追加しません。
- 秘密キー変数は、FlexConfig オブジェクト内の変数に定義された単一の文字列に置き換えられます。

変数は、$ 文字で始まりますが、@ で始まる秘密キーを除きます。たとえば、$ifname は次のコマンドのポリシー オブジェクト変数で、@keyname は秘密キーです。

```
interface $ifname
key @keyname
```

（注） ポリシーオブジェクトまたはシステム変数を初めて挿入する場合は、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用して挿入する必要があります。このアクションによって、FlexConfig オブジェクト エディタの下部にある [変数（Variables）] リストに変数が追加されます。ただし、システム変数を使用する場合でも、後続の使用では変数文字列を入力する必要があります。オブジェクトまたはシステム変数の割り当てがないプロセス変数を追加する場合は、[挿入（Insert）] メニューを使用しないでください。秘密キーを追加する場合は、常に [挿入（Insert）] メニューを使用します。秘密キーの変数は [変数（Variables）] リストに表示されません。

変数が単一の文字列、文字列のリスト、または値のテーブルのいずれとして解決されるかは、変数に割り当てるポリシーオブジェクトまたはシステム変数のタイプによって決まります（秘

密キーは、常に、単一の文字列として解決されます）。変数を適切に処理するには、何が返されるかを理解する必要があります。

次の各トピックでは、変数のさまざまなタイプとその処理方法について説明します。

変数の処理方法

ランタイムで、変数は単一の文字列、同じタイプの文字列のリスト、異なるタイプの文字列のリスト、あるいは名前付き値の表として解決することができます。また、複数の値に解決される変数の長さは一定、不定のどちらにすることもできます。変数を正しく処理するためには、何が返されるかを理解する必要があります。

返される値には、主に次の可能性があります。

単一値変数

変数が常に単一の文字列に解決される場合、FlexConfig スクリプトを変更せずに、その変数をそのまま使用できます。

たとえば、定義済みのテキスト変数 tcpMssBytes は常に単一の値（数値でなければなりません）に解決されます。**Sysopt_basic** FlexConfig は if/then/else 構造を使用して、別の単一値テキスト変数 tcpMssMinimum に基づきセグメントの最大サイズを設定します。

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

この例では、FlexConfig オブジェクト エディタで [挿入（Insert）] メニューを使用して最初の $tcpMssBytes の使用を追加しますが、#else 行には直接この変数を入力します。

秘密鍵の変数は、特殊なタイプの単一値変数です。秘密鍵では、変数を繰り返し使用する場合でも常に [挿入（Insert）] メニューを使用して変数を追加します。これらの変数は、FlexConfig オブジェクト内の [変数（Variables）] リストに表示されません。

（注） ネットワーク オブジェクトのポリシー オブジェクト変数も、IP アドレスの単一の指定（ホスト アドレス、ネットワーク アドレス、アドレス範囲のいずれか）になります。ただしこの場合、ASA コマンドには特定のアドレス タイプが必要であるため、期待されるアドレスのタイプを把握している必要があります。たとえば、コマンドにホストアドレスが必要な場合、ネットワーク アドレスを含むオブジェクトを指すネットワーク オブジェクト変数を使用すると、導入時にエラーが発生します。

同じタイプの複数の値を持つ変数

ポリシーオブジェクトおよびシステム変数のなかには、同じタイプの複数の値に解決されるものがあります。たとえば、ネットワーク オブジェクト グループを指すオブジェクト変数は、

そのグループ内の IP アドレスのリストに解決されます。同様に、システム変数 $SYS_FW_INTERFACE_NAME_LIST は、インターフェイス名のリストに解決されます。

同じタイプの複数の値に対応するテキスト オブジェクトを作成することもできます。たとえば、定義済みのテキストオブジェクト enableInspectProtocolList には複数のプロトコル名を含めることができます。

同じタイプの項目のリストに解決される複数の値を持つ変数は、長さが不定であることはよくあります。たとえば、ユーザは随時インターフェイスを設定または設定解除できるので、デバイス上にある名前付きインターフェイスの数を前もって知ることはできません。

そのため、同じタイプの複数の値を持つ変数を処理するには、通常はループを使用します。たとえば、定義済みの FlexConfig **Default_Inspection_Protocol_Enable** では、#foreach ループを使用して enableInspectProtocolList オブジェクトの各値を処理します。

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

この例では、スクリプトが各値を順に $protocol 変数に代入し、その結果を ASA の **inspect** コマンドで使用して、そのプロトコルに対してインスペクションエンジンを有効にします。この場合、変数名として単純に $protocol と入力します。オブジェクトやシステム値を変数に代入するわけではないので、[挿入（Insert）] メニューを使用して変数を追加することはしません。ただし、$enableInspectProtocolList を追加する場合は、[挿入（Insert）] メニューを使用する必要があります。

システムは $enableInspectProtocolList 内の値がなくなるまで、#foreach と #end の間にあるコードをループ処理します。

タイプが異なる複数の値を持つ変数

それぞれの値が異なる目的を果たす、複数の値を持つテキストオブジェクトを作成できます。たとえば、定義済みの **netflow_Destination** テキスト オブジェクトに、インターフェイス名、宛先 IP アドレス、UDP ポート番号という 3 つの値がこの順で設定されているとします。

このように定義するオブジェクトは、既定の数の値を持たなければなりません。そうでないと、処理するのが難しくなります。

このようなオブジェクトを処理するには、get メソッドを使用します。オブジェクト名の末尾に **.get(*n*)** と入力し、*n* をそのオブジェクトのインデックスで置き換えます。テキスト オブジェクトは値を 1 からリストしますが、インデックスは 0 からカウントします。

たとえば、Netflow_Add_Destination オブジェクトは次の行を使用して、netflow_Destination に含まれる 3 つの値を ASA の **flow-export** コマンドに追加します。

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

この例では、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用して $netflow_Destination の最初の使用を追加してから、**.get(0)** を追加します。ただし、**$netflow_Destination.get(1)** および **$netflow_Destination.get(2)** の変数は直接入力して指定する必要があります。

値のテーブルに解決される、複数の値を持つ変数

システム変数のなかには、値のテーブルを返すものがあります。そのような変数に該当するのは、たとえば $SYS_FTD_ROUTED_INTF_MAP_LIST のように、MAP が名前に含まれる変数です。ルーテッド インターフェイス マップは、以下のようなデータを返します（わかりやすくするために改行が追加されています）。

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]
```

上記の例では、4 つのインターフェイスに関する情報が返されています。インターフェイスごとに、名前付き値のテーブルが含まれています。たとえば、intf_hardwarare_id はインターフェイス ハードウェアの名前プロパティであり、GigabitEthernet0/0 などの文字列として返されます。

このような変数は、通常は長さが不定であるため、値を処理するにはループ処理を使用する必要があります。また、取得対象の値を示すために、変数名にプロパティ名も追加する必要があります。

たとえば、IS-IS 構成では、インターフェイス コンフィギュレーション モードで、論理名を持つインターフェイスに ASA の **isis** コマンドを追加する必要があります。ただし、このモードを開始する際は、インターフェイスのハードウェア名を使用します。したがって、論理名を持つインターフェイスを識別してから、それらのインターフェイスだけをそれぞれのハードウェア名を使用して設定する必要があります。ISIS_Interface_Configuration の定義済み FlexConfig は、そのために、ループ内にネストされた if/then 構造を使用します。以下のコードを見るとわかるように、#foreach スクリプト コマンドで各インターフェイス マップを $intf 変数に読み込んだ後、#if ステートメントでマップ（$intf.intf_logical_name）から intf_logical_name の値を取得し、その値が isisIntfList 定義済みテキスト変数で定義されているリストに含まれている場合は、intf_hardwarare_id の値（$intf.intf_hardwarare_id）を使用してインターフェイス コマンドを入力します。IS-IS を設定するインターフェイスの名前を追加する場合は、isisIntfList 変数を編集する必要があります。

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

変数がデバイスに関して返す内容を表示する方法

変数が何を返すかを評価する簡単な方法は、変数の注釈付きリストを処理するだけの簡単な FlexConfig オブジェクトを作成することです。次に、作成したオブジェクトを FlexConfig ポリシーに割り当て、ポリシーをデバイスに割り当てます。ポリシーを保存してから、そのデバイスの設定のプレビューをプレビューします。解決された値がプレビューに表示されます。プレビューのテキストを選択し、Ctrl キーを押した状態で C キーを押し、出力を分析用にテキストファイルに貼り付けることができます。

（注） ただし、FlexConfig には有効な設定コマンドが一切含まれていないため、FlexConfig をデバイスに展開しないでください。展開すると展開エラーが生じます。プレビューの取得後、FlexConfig ポリシーから FlexConfig オブジェクトを削除し、ポリシーを保存します。

たとえば、次の FlexConfig オブジェクトを作成することができます。

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

このオブジェクトのプレビューは以下のように表示されます（明確にするために改行が追加されています）。

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###
```

```
###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, management]
```

FlexConfig ポリシー オブジェクト変数

ポリシー オブジェクト変数は、オブジェクト マネージャで設定されている特定のポリシー オブジェクトに関連付けられます。FlexConfigオブジェクトにポリシー オブジェクト変数を挿入する場合、変数に名前を付け、これに関連付けられているオブジェクトを選択します。

関連付けられているオブジェクトと完全に同じ名前を変数に付けても、変数自体は、関連付けられたオブジェクトと同じではありません。FlexConfig で初めてスクリプトに変数を追加し、オブジェクトとの関連付けを確立するには、FlexConfig オブジェクト エディタの **[挿入（Insert）] > [ポリシー オブジェクトの挿入（Insert Policy Object）] > *[オブジェクト タイプ（Object Type）]*** メニューを使用する必要があります。単に $ 記号に続けてオブジェクト名を入力しても、ポリシー オブジェクト変数は作成されません。

以下のタイプのオブジェクトを指す変数を作成できます。各変数に適切なタイプのオブジェクトを作成するようにしてください。オブジェクトを作成するには、**[オブジェクト（Objects）]> [オブジェクト管理（Object Management）]** に移動します。

- テキスト オブジェクト（Text Objects）：テキスト文字列の場合。これには、IP アドレス、番号や、インターフェイス、ゾーン名などの自由形式のテキストが含まれます。コンテンツ テーブルから **[FlexConfig]** > **[テキスト オブジェクト（Text Object）]** を選択し、[テキスト オブジェクトの追加（Add Text Object）] をクリックします。単一の値または複数の値を含むようにこれらのオブジェクトを設定できます。これらのオブジェクトは柔軟性が高く、FlexConfig オブジェクト内で使用するよう特別に構築されています。詳細については、FlexConfig テキスト オブジェクトの設定 （34 ページ）を参照してください。
- ネットワーク（Network）：IP アドレスの場合。ネットワーク オブジェクトまたはグループを使用できます。コンテンツ テーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** または [グループの追加（Add Group）] を選択します。グループ オブジェクトを使用すると、変数によりグループ内の各 IP アドレス指定のリストが返されます。アドレスは、オブジェクトの内容に応じて、ホスト、ネットワーク、またはアドレス範囲にできます。ネットワークを参照してください。
- セキュリティ ゾーン（Security Zones）：セキュリティ ゾーンまたはインターフェイス グループ内のインターフェイスの場合。コンテンツ テーブルから [インターフェイス（Interface）] を選択し、**[追加（Add）]** > **[セキュリティ ゾーン（Security Zones）]** または [インターフェイス グループ（Interface Group）] を選択します。セキュリティ ゾーン変数では、設定中のデバイスのゾーンまたはグループ内のインターフェイスのリストが返されます。インターフェイス（Interface）を参照してください。
- 標準 ACL オブジェクト（Standard ACL Object）：標準アクセス コントロール リストの場合。標準 ACL 変数では、標準 ACL オブジェクトの名前が返されます。コンテンツ テーブルから **[アクセス リスト（Access List）]** > **[標準（Standard）]** を選択し、[標準アクセス リスト オブジェクトの追加（Add Standard Access List Object）] をクリックします。アクセス リストを参照してください。
- 拡張 ACL オブジェクト（Extended ACL Object）：拡張アクセス コントロール リストの場合。拡張 ACL 変数では、拡張 ACL オブジェクトの名前が返されます。コンテンツ テーブルから **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択し、[拡張アクセス リスト オブジェクトの追加（Add Extended Access List Object）] をクリックします。アクセス リストを参照してください。
- ルート マップ（Route Map）：ルート マップ オブジェクトの場合。ルート マップ変数では、ルート マップ オブジェクトの名前が返されます。コンテンツ テーブルから [ルート マップ（Route Map）] を選択し、[ルート マップの追加（Add Route Map）] をクリックします。ルート マップ を参照してください。

FlexConfig システム変数

システム変数は、デバイス自体やデバイスに設定されたポリシーから取得した情報に置き換えられます。

FlexConfig オブジェクト エディタの **[挿入（Insert）]** > **[システム変数の挿入（Insert System Variable）]** > ***[変数名]*** メニューを使用して、最初の変数を FlexConfig のスクリプトに追加し、

システム変数とのアソシエーションを確立します。単に$記号に続けてシステム変数名を入力しても、FlexConfig オブジェクトのコンテキストでのシステム変数は作成されません。

次の表に、使用可能なシステム変数の説明を示します。変数を使用する前に、通常、その変数に何が返されるかを確認します。変数がデバイスに関して返す内容を表示する方法 （11 ページ）を参照してください。

名前	説明
SYS_FW_OS_MODE	デバイスのオペレーティング システム モード。値はROUTED または TRANSPARENT です。
SYS_FW_OS_MULTIPLICITY	デバイスがシングル コンテキスト モードまたはマルチ コンテキスト モードのいずれで動作するか。値は、SINGLE、MULTI、または NOT_APPLICABLE です。
SYS_FW_MANAGEMENT_IP	デバイスの管理 IP アドレス。
SYS_FW_HOST_NAME	デバイスのホスト名。
SYS_FTD_INTF_POLICY_MAP	キーがインターフェイス名で、値がポリシーマップのマップ。この変数は、デバイスにインターフェイスベースのサービス ポリシーが定義されていない場合、値を返しません。
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	インスペクションが有効になっているプロトコルのリスト。
SYS_FTD_ROUTED_INTF_MAP_LIST	デバイスのルーテッド インターフェイス マップのリスト。各マップには、ルーテッド インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_SWITCHED_INTF_MAP_LIST	デバイスのスイッチド インターフェイス マップのリスト。各マップには、スイッチド インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_INLINE_INTF_MAP_LIST	デバイスのインライン インターフェイス マップのリスト。各マップには、インライン セット インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_PASSIVE_INTF_MAP_LIST	デバイスのパッシブ インターフェイス マップのリスト。各マップには、パッシブ インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_INTF_BVI_MAP_LIST	デバイスのブリッジ仮想インターフェイスマップのリスト。各マップには、BVI 構成に関連する一連の名前付き値が含まれます。
SYS_FW_INTERFACE_HARDWARE_ID_LIST	GigabitEthernet0/0 など、デバイスのインターフェイスのハードウェア名のリスト。
SYS_FW_INTERFACE_NAME_LIST	内部など、デバイスのインターフェイスの論理名のリスト。

名前	説明
SYS_FW_INLINE_INTERFACE_NAME_LIST	パッシブまたは ERSPAN パッシブとして設定されたインターフェイスの論理名のリスト。
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	すべてのルーテッド インターフェイスなど、インライン セットの一部ではないインターフェイスの論理名のリスト。

定義済みの FlexConfig オブジェクト

定義済みの FlexConfig オブジェクトは、選択機能に検証済みの設定を提供します。Management Center を使用して設定できない機能を設定する必要がある場合は、これらのオブジェクトを使用します。

次の表に、使用可能なオブジェクトを示します。関連するテキスト オブジェクトをメモしてください。定義済みの FlexConfig オブジェクトの動作をカスタマイズするには、これらのテキスト オブジェクトを編集する必要があります。テキスト オブジェクトにより、ネットワークおよびデバイスで必要な IP アドレスとその他の属性を使用して、設定をカスタマイズできます。

定義済みの FlexConfig オブジェクトを変更する必要がある場合は、オブジェクトをコピーしてそれを変更し、新しい名前で保存します。定義済みの FlexConfig オブジェクトを直接編集することはできません。

FlexConfig を使用して、他の ASA ベースの機能を設定できますが、これらの機能の設定は検証されていません。ASA 機能が Management Center ポリシーで設定できる機能と重複している場合は、FlexConfig を使用して設定しないでください。

たとえば、Snort 検査には HTTP プロトコルが含まれるため、ASA スタイルの HTTP 検査を有効にしないでください。（実際に、enableInspectProtocolList オブジェクトに **http** を追加することはできません。この場合、デバイスを誤って設定することが回避されます）。代わりに、必要に応じて、アプリケーションまたは URL フィルタリングを実行するアクセス コントロール ポリシーを設定し、HTTP 検査要件を実装します。

表 *1*：定義済みの *FlexConfig* オブジェクト

FlexConfig オブジェクト名	説明	関連するテキストオブジェクト
Default_Inspection_Protocol_Disable	global_policy デフォルト ポリシー マップのプロトコルを無効にします。	disableInspectProtocolList
Default_Inspection_Protocol_Enable	global_policy デフォルト ポリシー マップのプロトコルを有効にします。	enableInspectProtocolList
Inspect_IPv6_Configure	global_policy ポリシー マップで IPv6 検査を設定し、IPv6 ヘッダー コンテンツに基づいてトラフィックを記録およびドロップします。	IPv6RoutingHeaderDropLogList、IPv6RoutingHeaderLogList、IPv6RoutingHeaderDropList。

FlexConfig オブジェクト名	説明	関連するテキストオブジェクト
Inspect_IPv6_UnConfigure	IPv6 検査をクリアおよび無効にします。	—
ISIS_Configure	IS-IS ルーティングのグローバル パラメータを設定します。	isIsNet、isIsAddressFamily、isISType
ISIS_Interface_Configuration	インターフェイス レベルの IS-IS 設定。	isIsAddressFamily、IsIsIntfList また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します
ISIS_Unconfigure	デバイスの IS-IS ルータ設定をクリアします。	—
ISIS_Unconfigure_All	デバイスから IS-IS ルータ設定をクリアします（デバイスインターフェイスの IS-IS ルータ割り当てなど）。	—
NGFW_TCP_NORMALIZATION	デフォルト TCP 正規化設定を変更します。	—
Policy_Based_Routing	この設定例を使用するには、コピーしてインターフェイス名を変更し、r-map-object テキストオブジェクトを使用してオブジェクト マネージャでルート マップ オブジェクトを特定します。	—
Policy_Based_Routing_Clear	デバイスからポリシーベース ルーティング設定をクリアします。	—
Sysopt_AAA_radius	RADIUS アカウンティング応答内の認証キーを無視します。	—
Sysopt_AAA_radius_negate	Sysopt_AAA_radius 設定を拒否します。	—
Sysopt_basic	sysopt 待機時間、TCP パケットの最大セグメントサイズ、詳細トラフィック統計情報を設定します。	tcpMssMinimum、tcpMssBytes
Sysopt_basic_negate	sysopt_basic 詳細トラフィック統計情報、待機時間、TCP 最大セグメント サイズをクリアします。	—
Sysopt_clear_all	デバイスからすべての sysopt 設定をクリアします。	—

FlexConfig オブジェクト名	説明	関連するテキストオブジェクト
Sysopt_noproxyarp	noproxy arp CLI を設定します。	システム変数 SYS_FW_NON_INLINE_INTF_NAME_LIST を使用します
Sysopt_noproxyarp_negate	Sysopt_noproxyarp 設定をクリアします。	システム変数 SYS_FW_NON_INLINE_INTF_NAME_LIST を使用します
Sysopt_Preserve_Vpn_Flow	syopt 保存 VPN フローを設定します。	—
Sysopt_Preserve_Vpn_Flow_negate	Sysopt_Preserve_Vpn_Flow 設定をクリアします。	—
Sysopt_Reclassify_Vpn	sysopt 再分類 vpn を設定します。	—
Sysopt_Reclassify_Vpn_Negate	sysopt 再分類 vpn を拒否します。	—
Threat_Detection_Clear	脅威検出TCP代行受信設定をクリアします。	—
Threat_Detection_Configure	TCP代行受信によって代行受信される攻撃の脅威検出統計情報を設定します。	threat_detection_statistics
Wccp_Configure	このテンプレートはWCCPを設定する例を提供します。	isServiceIdentifier、serviceIdentifier、wccpPassword
Wccp_Configure_Clear	WCCP 設定をクリアします。	—

廃止された FlexConfig オブジェクト

次の表に、GUI でネイティブに設定できるようになった機能を設定するオブジェクトを示します。できるだけ早くこれらのオブジェクトの使用を中止してください。

表 *2*：廃止された定義済みの *FlexConfig* オブジェクト

廃止されたバージョン	FlexConfig オブジェクト	説明	現在の設定場所
7.3	DHCPv6_Prefix_Delegation_Configure	IPv6 プレフィックス委任の 1 つの外部インターフェイス（プレフィックス委任クライアント）と 1 つの内部インターフェイス（委任されたプレフィックスの受信者）を設定します。このテンプレートを使用するには、テンプレートをコピーして変数を変更します。 関連するテキストオブジェクト：pdoutside、pdinside また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します	インターフェイス IPv6 の設定。
7.3	DHCPv6_Prefix_Delegation_UnConfigure	DHCPv6 プレフィックス委任設定を削除します。	インターフェイス IPv6 の設定。
6.3	Default_DNS_Configure	デフォルト DNS グループを設定します。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバーを定義します。 関連するテキストオブジェクト：defaultDNSNameServerList, defaultDNSParameters	プラットフォームの設定。
6.3	DNS_Configure	デフォルト以外の DNS サーバグループの DNS サーバを設定します。グループの名前を変更するには、オブジェクトをコピーします。	オブジェクトマネージャの **DNS サーバーグループ**。
6.3	DNS_UnConfigure	Default_DNS_Configure と DNS_Configure で実行される DNS サーバの構成を削除します。DNS_Configure を変更した場合に DNS サーバ グループ名を変更するには、オブジェクトをコピーします。	オブジェクトマネージャの **DNS サーバーグループ**。

廃止されたバージョン	FlexConfig オブジェクト	説明	現在の設定場所
7.2	Eigrp_Configure	EIGRP ルーティングのネクストホップ、自動集約、ルータ ID、eigrp スタブを設定します。 関連するテキストオブジェクト：eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary	すべての EIGRP オブジェクトについては、EIGRPを参照してください。 システムでは、アップグレード後に展開できますが、EIGRP 構成をやり直すように警告されます。このプロセスを支援するために、コマンドライン移行ツールが用意されています。
7.2	Eigrp_Interface_Configure	EIGRP インターフェイス認証モード、認証キー、Hello インターバル、ホールド時間、スプリット ホライズンを設定します。 関連するテキストオブジェクト：eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します	
7.2	Eigrp_Unconfigure	デバイスから自律システムの EIGRP 設定をクリアします。	
7.2	Eigrp_Unconfigure_all	すべての EIGRP 設定をクリアします。	
7.4	Netflow_Add_Destination	NetFlow エクスポートの宛先を作成し、設定します。 関連するテキストオブジェクト：Netflow_Destinations, netflow_Event_Types	プラットフォームの設定。
7.4	Netflow_Clear_Parameters	NetFlow エクスポートのグローバル デフォルト設定を復元します。	プラットフォームの設定。

廃止されたバージョン	FlexConfig オブジェクト	説明	現在の設定場所
7.4	Netflow_Delete_Destination	NetFlowエクスポートの宛先を削除します。 関連するテキストオブジェクト：Netflow_Destinations, netflow_Event_Types	プラットフォームの設定。
7.4	Netflow_Set_Parameters	NetFlowエクスポートのグローバル パラメータを設定します。 関連するテキストオブジェクト：netflow_Parameters	プラットフォームの設定。
6.3	TCP_Embryonic_Conn_Limit	初期接続制限を設定して SYN フラッド サービス妨害（DoS）攻撃から保護します。 関連するテキストオブジェクト：tcp_conn_misc、tcp_conn_limit	サービスポリシー。
6.3	TCP_Embryonic_Conn_Timeout	初期接続タイムアウトを設定して SYN フラッド サービス妨害（DoS）攻撃から保護します。 関連するテキストオブジェクト：tcp_conn_misc、tcp_conn_timeout	サービスポリシー。
7.2	VxLAN_Clear_Nve	デバイスから VxLAN_Configure_Port_And_Nve が使用される場合、NVE 1 設定を削除します。	すべての VXLAN オブジェクトについては、VXLAN インターフェイスの設定を参照してください。 以前のバージョンで FlexConfig を使用して VXLANインターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN設定をやり直す場合は、FlexConfig 設定を削除します。
7.2	VxLAN_Clear_Nve_Only	展開時にインターフェイスで設定された NVE 設定をクリアします。	

廃止されたバージョン	FlexConfig オブジェクト	説明	現在の設定場所
7.2	VxLAN_Configure_Port_And_Nve	VLAN ポートと NVE 1 を設定します。 関連するテキストオブジェクト：vxlan_Port_And_Nve	
7.2	VxLAN_Make_Nve_Only	NVE のみのインターフェイスを設定します。 関連するテキストオブジェクト：vxlan_Nve_Only また、システム変数 SYS_FTD_ROUTED_MAP_LIST と SYS_FTD_SWITCHED_INTF_MAP_LIST を使用します	
7.2	VxLAN_Make_Vni	VNI インターフェイスを作成します。これを展開した後、VNI インターフェイスを正しく検出するには、デバイスの登録を解除して、再登録する必要があります。 関連するテキストオブジェクト：vxlan_Vni	

定義済みのテキスト オブジェクト

複数の定義済みのテキスト オブジェクトがあります。これらのオブジェクトは、定義済みの FlexConfig オブジェクトで使用される変数に関連付けられています。ほとんどの場合、関連付けられた FlexConfig オブジェクトを使用するにはこれらのオブジェクトを編集して値を追加する必要があります。そうしない場合、展開中にエラーが表示されます。これらのオブジェクトの一部にはデフォルト値が含まれていますが、その他は空となっています。

テキスト オブジェクトの編集の詳細については、FlexConfig テキスト オブジェクトの設定（34 ページ）を参照してください。

名前	説明	関連する FlexConfig オブジェクト
defaultDNSNameServerList (非推奨メソッド.)	デフォルト DNS グループで設定する DNS サーバの IP アドレス。 バージョン 6.3 以降では、Threat Defense プラットフォーム設定ポリシーでデータインターフェイスの DNS を設定します。	Default_DNS_Configure
defaultDNSParameters (非推奨メソッド.)	デフォルト DNS サーバー グループの DNS 動作を制御するパラメータ。オブジェクトには、再試行、タイムアウト、有効期限エントリ タイマー、ポール タイマー、ドメイン名の個別のエントリが順番に含まれています。 バージョン 6.3 以降では、Threat Defense プラットフォーム設定ポリシーでデータインターフェイスの DNS を設定します。	Default_DNS_Configure
disableInspectProtocolList	デフォルト ポリシー マップ（global_policy）のプロトコルを無効にします。	Disable_Default_Inspection_Protocol
dnsNameServerList	ユーザ定義の DNS グループで設定する DNS サーバの IP アドレス。	DNS_Configure
dnsParameters	デフォルト以外の DNS サーバ グループの DNS 動作を制御するパラメータ。オブジェクトには、再試行、タイムアウト、ドメイン名、ドメイン名、ネーム サーバ インターフェイスの個別のエントリが順番に含まれています。	DNS_Configure
enableInspectProtocolList	デフォルト ポリシー マップ（global_policy）のプロトコルを有効にします。検査が Snort 検査と競合するプロトコルを追加することはできません。	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	ユーザが拒否する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査でドロップをログに記録せずにドロップされます。	Inspect_IPv6_Configure

名前	説明	関連する FlexConfig オブジェクト
IPv6RoutingHeaderDropLogList	ユーザが拒否し、ログに記録する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査でドロップされ、ドロップに関する syslog メッセージが送信されます。	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	許可するが、ログに記録する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査で許可されますが、ヘッダーの存在に関する syslog メッセージが送信されます。	Inspect_IPv6_Configure
isIsAddressFamily	IPv4 または IPv6 アドレス ファミリ。	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	論理インターフェイス名のリスト。	ISIS_Interface_Configuration
isIsISType	IS タイプ（level-1、level-2-only、または level-1-2）。	ISIS_Configure
isIsNet	ネットワーク エンティティ。	ISIS_Configure
isServiceIdentifier	false の場合は、標準 **web-cache** サービス識別子を使用します。	Wccp_Configure
netflow_Destination	1 つの NetFlow エクスポート宛先のインターフェイス、接続先、および UDP ポート番号を定義します。	Netflow_Add_Destination
netflow_Event_Types	エクスポートされる宛先のイベントのタイプを **all**、**flow-create**、**flow-defined**、**flow-teardown**、**flow-update** のいずれかのサブセットとして定義します。	Netflow_Add_Destination
netflow_Parameters	NetFlow エクスポートのグローバル設定を指定します。アクティブ更新間隔（フロー更新イベント間の分数）、遅延（フロー作成遅延（秒単位）。デフォルトの 0 ではコマンドは表示されません）、およびテンプレートタイムアウト レート（分単位）。	Netflow_Set_Parameters

名前	説明	関連する FlexConfig オブジェクト
PrefixDelegationInside	DHCPv6 プレフィックス委任の内部インターフェイスを設定します。オブジェクトには、インターフェイス名、IPv6 サフィックスとプレフィックス長、およびプレフィックス プール名の複数のエントリが順番に含まれています。	なし、ただし DHCPv6_Prefix_Delegation_Configure のコピーとともに使用できます。
PrefixDelegationOutside	外部 DHCPv6 プレフィックス委任クライアントを設定します。オブジェクトには、インターフェイス名と IPv6 プレフィックス長の複数のエントリが順番に含まれています。	なし、ただし DHCPv6_Prefix_Delegation_Configure のコピーとともに使用できます。
serviceIdentifier	ダイナミック WCCP サービス ID 番号。	Wccp_Configure
tcp_conn_limit (非推奨メソッド.)	TCP 初期接続制限を設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能をThreat Defense サービス ポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Limit
tcp_conn_misc (非推奨メソッド.)	TCP 初期接続設定を設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能を Threat Defense サービスポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Limit、TCP_Embryonic_Conn_Timeout
tcp_conn_timeout (非推奨メソッド.)	TCP 初期接続タイムアウトを設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能を Threat Defense サービスポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Timeout

名前	説明	関連する FlexConfig オブジェクト
tcpMssBytes	最大セグメント サイズ（バイト単位）。	Sysopt_basic
tcpMssMinimum	このフラグが true の場合にのみ設定される最大セグメントサイズ（MSS）を設定するかどうかをチェックします。	Sysopt_basic
threat_detection_statistics	TCP 代行受信の脅威検出統計情報に使用されるパラメータ。	Threat_Detection_Configure
vxlan_Nve_Only	インターフェイスで NVE-only を設定するためのパラメータ： • インターフェイスの論理名 • IPv4 アドレス（ルーテッド インターフェイスではオプション） • IPv4 ネットマスク（ルーテッドインターフェイスではオプション）	VxLAN_Make_Nve_Only
vxlan_Port_And_Nve	VXLAN のポートおよび NVE を設定するために使用されるパラメータ： • vxlan ポート • 送信元インターフェイス（論理名） • タイプ（ピアまたは mcast） • ピアとなる IP アドレスまたは default-mcast-group	VxLAN_Configure_Port_And_Nve

名前	説明	関連する FlexConfig オブジェクト
vxlan_Vni	VNIを作成するために使用されるパラメータ： • インターフェイス番号（1 ～ 10000） • segment-id（1 ～ 16777215） • nameif（インターフェイスの論理名） • タイプ（ルーテッドまたはトランスペアレント） • IPアドレス（ルーテッドモードのデバイスの場合に使用）またはブリッジグループ番号（トランスペアレントモードのデバイスの場合に使用） • ネットマスク（デバイスがルーテッドモードの場合）または未使用	VxLAN_Make_Vni
wccpPassword	WCCP パスワード。	Wccp_Configure

FlexConfig ポリシーの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

FlexConfig の注意事項と制約事項

- FlexConfig ポリシーに誤りがあると、システムは失敗した FlexConfig を含む展開の試行に含まれるすべての変更をロールバックします。展開の失敗が原因でロールバックに設定の

クリアが含まれるため、ネットワークに悪影響を及ぼす可能性があります。営業時間外の FlexConfig の変更を含む、展開のタイミングを検討します。また、FlexConfig の変更だけが含まれるように展開を分離し、その他のポリシーの更新が行われないようにします。

- VxLAN_Make_VNI オブジェクトを使用する場合は、クラスタまたはハイ アベイラビリティ ペアを形成する前に、同じ FlexConfig をクラスタまたはハイ アベイラビリティ ペアのすべてのユニットに展開する必要があります。管理センターでは、クラスタまたはハイアベイラビリティペアを形成する前に、すべてのデバイスで VXLAN インターフェイスを照合する必要があります。
- SIP インスペクションなどの接続に適用されるサービスを設定する場合は、デバイスの CLI に移動し、**clear conn** コマンドを入力して接続をクリアします。接続が再構築されると、新しい設定がセッションに適用されます。

FlexConfig ポリシーによるデバイス設定のカスタマイズ

FlexConfig ポリシーを使用して、Threat Defense デバイスの設定をカスタマイズします。

FlexConfig を使用する前に、Management Center のその他の機能を使用して、必要なすべてのポリシーと設定を設定してみます。FlexConfig は、Threat Defense との互換性があるが、他の方法では Management Center で設定できない ASA ベースの機能を設定するための最終手段です。

次に、FlexConfig ポリシーを設定し、導入するためのエンドツーエンドの手順を示します。

手順

ステップ 1 設定する CLI コマンド シーケンスを特定します。

ASA デバイスに機能する設定がある場合は、**show running-config** を使用して必要なコマンドのシーケンスを取得します。必要に応じてインターフェイス名、IP アドレスなどの項目を調整します。

新しい機能の場合は、ラボの設定で ASA デバイスに実装して、コマンド シーケンスが適切であることを確認することをお勧めします。

詳細は、次のトピックを参照してください。

- FlexConfig ポリシーの推奨される使用法 （2 ページ）
- FlexConfig オブジェクトの CLI コマンド （3 ページ）

ステップ 2 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツテーブルから **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]** を選択します。

事前定義済み FlexConfig オブジェクトを確認して、必要なコマンドを生成できるかどうかを判断します。[表示（View）]（  ） をクリックして、オブジェクトの内容を表示します。既存のオブジェクトが必要なオブジェクトに近い場合は、最初にオブジェクトをコピーして、そのコピーを編集します。定義済みの FlexConfig オブジェクト （15 ページ） を参照してください。

また、オブジェクトの確認によって、FlexConfig オブジェクトの構造、コマンド構文、および予測されるシーケンシングを把握できます。

（注） 使用するオブジェクトを見つけた場合は、オブジェクトの下の [変数（Variables）] リストを直接またはコピーして確認します。SYS で始まるすべて大文字の変数名（システム変数）を除くすべての変数名を記録します。これらの変数は、特にデフォルト値のカラムでオブジェクトに値がないことが示されている場合に、編集またはオーバーライドの定義が必要になる可能性があるテキスト オブジェクトです。

ステップ 3 独自の FlexConfig オブジェクトを作成する必要がある場合は、必要な変数を特定し、関連オブジェクトを作成します。

導入する必要がある CLI には、時間の経過とともに調整する必要がある IP アドレス、インターフェイス名、ポート番号、およびその他のパラメータが含まれている場合があります。これらは、必要な値が含まれているオブジェクトを指す変数に隔離することをお勧めします。また、設定の一部であるが、時間の経過とともに変化する可能性がある文字列の変数が必要な場合があります。

さらに、ポリシーを割り当てる各デバイスに異なる値が必要かどうかを特定します。たとえば、3 つのデバイスの機能を設定し、これらのデバイスそれぞれに指定されたコマンドで異なるインターフェイス名または IP アドレスの指定が必要になる場合があります。各デバイスのオブジェクトをカスタマイズする必要がある場合は、オブジェクトを作成するときにオーバーライドを有効にして、デバイスごとのオーバーライド値を定義します。

変数のさまざまなタイプおよび必要に応じた関連オブジェクトの設定方法については、次のトピックを参照してください。

- FlexConfig 変数 （7 ページ）
- FlexConfig ポリシー オブジェクト変数 （12 ページ）
- FlexConfig システム変数 （13 ページ）
- FlexConfig テキスト オブジェクトの設定 （34 ページ）

ステップ 4 事前定義済み FlexConfig オブジェクトを使用する場合は、変数として使用されるテキスト オブジェクトを編集します。

FlexConfig テキスト オブジェクトの設定 （34 ページ）を参照してください。

ステップ 5 （必要な場合）FlexConfig オブジェクトの設定 （29 ページ）。

事前定義済みオブジェクトが機能しない場合にのみ、オブジェクトを作成する必要があります。

ステップ 6 FlexConfig ポリシーの設定 （36 ページ）。

ステップ 7 FlexConfig ポリシーのターゲット デバイスの設定 （38 ページ）。

ポリシーを作成するときに、デバイスにポリシーを割り当てることもできます。ポリシーをプレビューするには、そのポリシーに 1 つ以上のデバイスが割り当てられている必要があります。

ステップ 8 FlexConfig ポリシーのプレビュー （38 ページ）。

ポリシーをプレビューする前に変更を保存する必要があります。

生成されたコマンドが目的のものであること、およびすべての変数が正しく解決されていることを確認します。

ステップ 9 メニューバーで、**[展開（Deploy）]** > **[展開（Deployment）]** を選択します。

ステップ 10 ポリシーに割り当てられたデバイスを選択して [展開（Deploy）] をクリックします。

展開が完了するまで待機します。

ステップ 11 展開された構成の確認 （39 ページ）。

ステップ 12 （必要な場合）FlexConfig を使用した設定済み機能の削除 （42 ページ）。

他のタイプのポリシーとは異なり、単にデバイスから FlexConfig を割り当て解除しても関連設定は削除されません。FlexConfig で生成された設定を削除するには、指示された手順に従う必要があります。

現在製品によって直接サポートされているために機能を削除する場合は、FlexConfig から管理対象機能への変換 （43 ページ）も参照してください。

FlexConfig オブジェクトの設定

FlexConfig オブジェクトを使用して、デバイスに展開する設定を定義します。各 FlexConfig ポリシーは、FlexConfig オブジェクトのリストで構成されるため、オブジェクトは基本的に Apache Velocity スクリプト コマンド、ASA ソフトウェア コンフィギュレーション コマンド、および変数で構成されるコード モジュールです。

直接使用できる事前定義済みの FlexConfig オブジェクトがいくつかあります。これらを編集する必要がある場合は、コピーすることができます。また、独自のオブジェクトをはじめから作成することもできます。FlexConfig オブジェクトの内容の範囲は、単一の簡単なコマンド文字列から、変数およびスクリプトコマンドを使用してデバイスまたは展開ごとに内容が異なるコマンドを展開する複雑な CLI コマンド構造におよびます。

また、FlexConfig ポリシーを定義するときに、FlexConfig ポリシー オブジェクトを作成できます。

始める前に

次の点を考慮してください。

- FlexConfig オブジェクトはデバイスに展開されるコマンドに変換されます。これらのコマンドは、グローバル コンフィギュレーション モードですでに発行されています。したがって **enable** コマンドと **configure terminal** コマンドを FlexConfig オブジェクトの一部として含めないでください。
- 必要な変数のタイプを特定し、必要なポリシー オブジェクトを作成します。FlexConfig オブジェクトの編集時に変数のオブジェクトを作成することはできません。

- コマンドがデバイスの VPN またはアクセス コントロール設定とまったく競合していないことを確認します。
- インターフェイスのコマンド セットが複数ある場合は、最後のコマンド セットだけが展開されます。したがって、開始コマンドと終了コマンドを使用してインターフェイスを設定しないことを推奨します。インターフェイスを設定する例として、事前定義済み FlexConfig オブジェクトの ISIS_Interface_Configuration を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクト タイプのリストから **[FlexConfig]** > **[FlexConfig オブジェクト（FlexConfig Object）]** を選択します。

ステップ 3 次のいずれかを実行します。

- [FlexConfig オブジェクトの追加（Add FlexConfig Object）] をクリックして、新しいオブジェクトを作成します。
- **[編集（Edit）]**（  ）をクリックして、既存のオブジェクトを編集します。
- [表示（View）]（  ）をクリックして、事前定義済みオブジェクトの内容を表示します。
- 事前定義済みオブジェクトを編集するには、[コピー（Copy）]（  ）をクリックして、同じ内容の新しいオブジェクトを作成します。

ステップ 4 **名前**を入力し、オプションでオブジェクトの説明を入力します。

ステップ 5 オブジェクト本体領域に、必要な設定を生成するためのコマンドと命令を入力します。

オブジェクトの内容は、有効な ASA ソフトウェアのコマンド シーケンスを生成する一連のスクリプト コマンドおよびコンフィギュレーション コマンドです。Threat Defense デバイスでは、ASA ソフトウェア コマンドを使用して一部の機能を設定します。スクリプト コマンドおよびコンフィギュレーション コマンドの詳細については、次を参照してください。

- テンプレート スクリプト （6 ページ）
- FlexConfig オブジェクトの CLI コマンド （3 ページ）

変数を使用して、ランタイムにのみ通知される情報やデバイスごとに異なる情報を指定できます。プロセス変数に入力しますが、[挿入（Insert）] メニューを使用して、ポリシーオブジェクトまたはシステム変数に関連付けられているか、秘密キーである変数を追加する必要があります。変数の詳細については、FlexConfig 変数 （7 ページ）を参照してください。

- システム変数を挿入するには、**[挿入（Insert）]** > **[システム変数の挿入（Insert System Variable）]** > **[変数名]** を選択します。これらの変数の詳細については、FlexConfig システム変数 （13 ページ）を参照してください。
- ポリシー オブジェクトの変数を挿入するには、**[挿入（Insert）]** > **[ポリシー オブジェクトの挿入（Insert Policy Object）]** > **[オブジェクト タイプ]** を選択し、適切なオブジェクトの

タイプを選択します。次に、変数に名前を付け（関連付けられたポリシーオブジェクトと同じ名前にすることができます）、変数に関連付けるオブジェクトを選択し、[保存（Save）] をクリックします。これらのタイプの詳細については、FlexConfig ポリシーオブジェクト変数 （12 ページ）を参照してください。手順の詳細については、FlexConfig オブジェクトへのポリシーオブジェクト変数の追加 （32 ページ）を参照してください。

- 秘密キーの変数を挿入するには、**[挿入（Insert）]** > **[秘密キー（Secret Key）]** を選択し、変数名と値を定義します。手順の詳細については、秘密キーの設定 （33 ページ）を参照してください。

（注） [挿入（Insert）] メニューを使用して、新しいポリシー オブジェクトまたはシステム変数を作成する必要があります。ただし、その変数を後で使用するために、$ を含めて入力する必要があります。これは、システム変数にも当てはまります。システム変数を初めて使用する場合は、[挿入（Insert）] メニューから追加します。次に、後で使用するために入力します。1 つのシステム変数に [挿入（Insert）] メニューを複数回使用すると、システム変数が [変数（Variables）] リストに複数回追加され、FlexConfig が有効ではなくなるため、変更を保存できなくなります。プロセス変数（ポリシーオブジェクトやシステム変数に関連付けられていない）の場合は、変数を入力します。秘密キーを追加する場合は、常に [挿入（Insert）] メニューを使用します。秘密キーの変数は [変数（Variables）] リストに表示されません。

ステップ 6 展開の頻度およびタイプを選択します。

- [展開（Deployment）]：オブジェクトにコマンドを [1 回（Once）] または [毎回（Everytime）] 展開することを指定します。適切なオプションを選択する唯一の方法は、展開の結果をテストする方法です。

  最初に [毎回（Everytime）] を選択します。次に、FlexConfig ポリシーにオブジェクトをアタッチして、設定を展開します。展開に成功したら、FlexConfig ポリシーに戻り、FlexConfig ポリシーのプレビュー （38 ページ）の説明に従って、割り当てられたいずれかのデバイスの設定をプレビューします。`###CLI generated from managed features ###` のラベルが付いたセクションに、オブジェクト内のコマンドの clear または negate コマンドが含まれていて、`###Flex-config Appended CLI ###` セクションに機能を再設定するためのコマンドが含まれている場合、[毎回（Everytime）] が適切なオプションであることがわかります。

  negate コマンドが表示されていない場合でも、デバイス設定に少し変更を加えて、別の展開を実行します。展開が正常に完了したら、展開トランスクリプトを確認できます（展開された構成の確認 （39 ページ）を参照）。（コマンドがすでに設定されている場合でも）コマンドがエラーなく再発行されているのを確認できたら、[毎回（Everytime）] のままにします。

  システムがオブジェクト内のコマンドを最初に取り消してから再発行しない場合、または展開の結果に、コマンドに固有のエラーがある場合にのみ [1 回（Once）] に変更します。場合によっては、設定済みのコマンドの発行を許可されないことがありますが、それは例外的です。

  追加のヒント：

- FlexConfig オブジェクトが、ネットワーク オブジェクトや ACL オブジェクトなどのシステム管理対象オブジェクトを指している場合は、[毎回（Everytime）] を選択します。そうしないと、オブジェクトに対する更新が展開されない可能性があります。
- オブジェクトで行う操作が設定のクリアだけの場合は、[1回（Once）] を使用します。そして、次の展開後に FlexConfig ポリシーからオブジェクトを削除します。

- [タイプ（Type）]：次のいずれかを選択します。
  - [後に付加（Append）]：（デフォルト）。オブジェクトのコマンドは、Management Center ポリシーから生成された設定の最後に配置されます。管理対象オブジェクトから生成されたオブジェクトを指すポリシー オブジェクトの変数を使用する場合は、[後に付加（Append）] を使用する必要があります。その他のポリシー向けに生成されたコマンドがオブジェクトで指定されているものと重複する場合は、このオプションを選択してコマンドが上書きされないようにする必要があります。これは最も安全なオプションです。
  - [前に付加（Prepend）]：オブジェクトのコマンドは、Management Center ポリシーから生成された設定の最初に配置されます。通常、設定をクリアまたは除外するコマンドに [前に付加（Prepend）] を使用します。

ステップ 7 （オプション）オブジェクト本体の上にある **[Validate]**（） をクリックして、スクリプトの整合性を確認します。

[保存（Save）] をクリックするたびに、オブジェクトが検証されます。無効なオブジェクトを保存することはできません。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

FlexConfig オブジェクトへのポリシーオブジェクト変数の追加

FlexConfig ポリシー オブジェクトに、ポリシー オブジェクトの他のタイプと関連付けられた変数を挿入できます。FlexConfig をデバイスに展開すると、これらの変数は関連づけられたオブジェクトの名前やコンテンツに合わせて変換されます。

FlexConfig オブジェクトで初めてポリシー オブジェクト変数を使うときは、次の手順に従ってください。オブジェクトを再度参照する必要が生じたら、（$マークを含めて）変数を入力します。変数の使用方法を理解するには、変数の処理方法 （8 ページ）を参照してください。

始める前に

FlexConfig オブジェクトの設定の詳細については、FlexConfig オブジェクトの設定 （29 ページ） を参照してください。

手順

ステップ 1 FlexConfig ポリシーオブジェクトの編集中に、[挿入（Insert）]>[ポリシーオブジェクトの挿入（Insert Policy Object）]>[オブジェクトのタイプ（Object Type）] から、適切なタイプのオブジェクトを選択します。

ステップ 2 変数の名前を入力し、任意で説明を入力します。

名前は、FlexConfig オブジェクトのコンテキストの中で一意なものである必要があります。スペースを含めることはできません。変数に関連付けるオブジェクトと同一の名前を使用できます。

ステップ 3 変数と関連付けるオブジェクトを選択し、[追加（Add）]をクリックしてこれを[選択済みオブジェクト（Selected Object）] リストに移動します。

変数には、1 つのみのオブジェクトを関連付けることができます。

（注） テキストオブジェクトには、必要に応じて前もって定義されたオブジェクトを選択できます。しかし、これらオブジェクトの多くにはデフォルト値はありません。オブジェクトの更新では、必須の値を直接与えるか、ないしはFlexConfig オブジェクトを展開するデバイスのオーバーライドとして与える必要があります。これらのオブジェクトを更新せずに FlexConfig の展開を試行しても、多くの場合展開のエラーにつながります。

ステップ 4 [保存（Save）] をクリックします。

変数は、FlexConfig オブジェクトエディタの下の変数リストに表示されます。

秘密キーの設定

秘密キーは、パスワードなどの、内容をマスクする単一文字列の変数です。機密情報の拡散を防ぐため、これらの変数にはシステムによって特別な処理が行われます。

秘密キー変数は FlexConfig オブジェクトの変数リストに表示されません。

FlexConfig オブジェクトで秘密キー変数を作成、挿入、および管理するには、次の手順を使用します。他のタイプ変数とは異なり、所定の秘密キー変数を挿入する必要があるたびに **Insert** コマンドを使用できます。処理については、これらの変数は単一値のテキストオブジェクト変数と同様に機能します。単一値変数 （8 ページ）を参照してください。

（注） 秘密キー変数で定義されたデータは、FlexConfig ポリシーのプレビュー時を除き、ユーザからマスクされます。また、FlexConfig ポリシーをエクスポートする場合、すべての秘密キー変数の内容が消去されます。ポリシーをインポートする場合、各秘密キー変数を手動で編集してデータを入力する必要があります。

始める前に

FlexConfig オブジェクトの設定の詳細については、FlexConfig オブジェクトの設定 （29 ページ）を参照してください。

手順

ステップ 1 FlexConfig ポリシー オブジェクトを編集する際には、**[挿入（Insert）]** > **[秘密キー（Secret Key）]** を選択します。

ステップ 2 [秘密キーの挿入（Insert Secret Key）] ダイアログボックスで、次のいずれかの手順を実行します。

- 新しいキーを作成するには、[秘密キーの追加（Add Secret Key）] をクリックし、次の情報を入力して [追加（Add）] をクリックします。
  - [秘密キー名（Secret Key Name）]：変数の名前。この名前は、前に @ が付けられて FlexConfig オブジェクトに表示されます。
  - [パスワード（Password）]、[パスワードの確認（Confirm Password）]：入力と同時に、アスタリスクでマスクされる秘密の文字列です。
- FlexConfig オブジェクトに秘密キー変数を挿入するには、変数のチェックボックスをオンにします。
- 秘密キー変数の値を編集するには、変数の **[編集（Edit）]**（ ）をクリックします。変更を加えて、[追加（Add）] をクリックします。
- 秘密キー変数を削除するには、変数の [削除（Delete）]（ ） をクリックします。

ステップ 3 [保存（Save）] をクリックします。

FlexConfig テキスト オブジェクトの設定

ポリシー オブジェクト変数の対象として FlexConfig オブジェクトでテキスト オブジェクトを使用します。変数を使用して、ランタイムにのみ通知される情報やデバイスごとに異なる情報を指定できます。展開中に、テキスト オブジェクトを指す変数はテキスト オブジェクトの内容に置き換えられます。

テキスト オブジェクトには自由形式の文字列が含まれます。キーワード、インターフェイス名、番号、IP アドレスなどにすることも可能です。内容は、FlexConfig スクリプト内の情報の使用方法によって異なります。

テキスト オブジェクトを作成または編集する前に、必要な内容を特定します。これにはオブジェクトの処理方法が含まれます。これを決めることで、1 つの文字列オブジェクトまたは複数の文字列オブジェクトのいずれを作成するかを決定するのに役立ちます。次のトピックを参照してください。

- FlexConfig 変数 （7 ページ）
- 変数の処理方法 （8 ページ）

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクト タイプのリストから **[FlexConfig]** > **[テキスト オブジェクト（Text Object）]** を選択します。

ステップ 3 次のいずれかを実行します。

- [テキスト オブジェクトの追加（Add Text Object）] をクリックして、新しいオブジェクトを作成します。
- **[編集（Edit）]**（ ） をクリックして、既存のオブジェクトを編集します。事前定義済み FlexConfig オブジェクトを使用する場合に必要となる、事前定義済みテキスト オブジェクトを編集できます。

ステップ 4 **名前**を入力し、オプションでオブジェクトの説明を入力します。

ステップ 5 （新しいオブジェクトのみ）ドロップダウン リストから**変数タイプ**を選択します。

- [単一（Single）]：オブジェクトに単一のテキスト文字列を含める必要がある場合。
- [複数（Multiple）]：オブジェクトにテキスト文字列のリストを含める必要がある場合。

オブジェクトの保存後は変数タイプを変更できません。

ステップ 6 変数タイプが [複数（Multiple）] の場合は、上下矢印を使用して [カウント（Count）] を指定します。

数を変更すると、オブジェクトの行が追加されたり、削除されたりします。

ステップ 7 オブジェクトに内容を追加します。

変数番号の横のテキスト ボックスをクリックして値を入力するか、テキスト オブジェクトを使用する FlexConfig オブジェクトを割り当てられる各デバイスに対してデバイスの上書きを設定できます。両方行うこともできますが、この場合、ベース オブジェクトで設定した値は、指定したデバイスの上書きが存在しない場合にデフォルト値として機能します。

事前定義済みオブジェクトの編集時には、デバイスの上書きを使用することをお勧めします。これは、別の FlexConfig ポリシーでオブジェクトを使用する必要がある他のユーザ用に、デ

フォルトが残るようにするためです。実行するアプローチは、組織の要件に応じて異なります。

ヒント 一部の事前定義済みオブジェクトには、各値が特定の目的を提供する複数の値が必要です。オブジェクトの予測される値を特定するために、説明テキストを注意深く読みます。手順では、base 値を変更する代わりに上書きを使用する必要があることが指定される場合があります。enableInspectProtocolList の場合は、インスペクションに Snort インスペクションとの互換性がないプロトコルを入力できません。

デバイスの上書きを使用する場合は、次の手順を実行します。

a) [オーバーライドを許可（Allow Override）] チェックボックスにマークを付けます。
b) [オーバーライド（Overrides）] を展開し（必要な場合）、[追加（Add）] をクリックします。

上書きがデバイスにすでにある場合は、上書きの編集アイコンをクリックして変更します。

c) [オブジェクトのオーバーライドの追加（Add Object Override）] ダイアログボックスの [ターゲット（Targets）] で、値を定義するデバイスを選択し、[追加（Add）] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。
d) [オーバーライド（Overrides）] をクリックし、必要に応じて [カウント（Count）] を調整し、変数フィールドをクリックして、デバイスの値を入力します。
e) [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

FlexConfig ポリシーの設定

FlexConfig ポリシーには、FlexConfig オブジェクトの 2 つの順序のリストが含まれています。1 つは先頭に追加されたリスト、もう 1 つは末尾に追加されたリストです。先頭に追加/末尾に追加の説明については、FlexConfig オブジェクトの設定 （29 ページ）を参照してください。

FlexConfig ポリシーは、複数のデバイスに割り当てることができる共有ポリシーです。

手順

ステップ 1 **[デバイス（Devices）] > [FlexConfig]**を選択します。
ステップ 2 次のいずれかを実行します。

- [新しいポリシー（New Policy）] をクリックして、新しい FlexConfig ポリシーを作成します。名前を入力するプロンプトが表示されます。必要に応じて、[使用可能なデバイス（Available Devices）] リストでデバイスを選択し、[ポリシーに追加（Add to Policy）] をクリックしてデバイスを割り当てます。[保存（Save）] をクリックします。
- **[編集（Edit）]**（） をクリックして、既存のポリシーを編集します。名前や説明を編集モードでクリックして変更できます。
- [コピー（Copy）]（） をクリックして、同じ内容の新しいポリシーを作成します。名前を入力するプロンプトが表示されます。デバイス割り当てはコピーに保持されません。
- 削除アイコンをクリックして、不要になったポリシーを削除します。

ステップ 3 ポリシーに必要な FlexConfig オブジェクトを [使用可能な FlexConfig（Available FlexConfig）] リストから選択し、[>] をクリックしてポリシーに追加します。

オブジェクトは FlexConfig オブジェクトで指定した展開タイプに基づいて、先頭に追加されたリストまたは末尾に追加されたリストに自動的に追加されます。

選択したオブジェクトを削除するには、オブジェクトの横にある [削除（Delete）]（） をクリックします。

ステップ 4 選択したオブジェクトごとに、オブジェクトの横にある [表示（View）]（） をクリックして、オブジェクトで使用されている変数を特定します。

SYS で始まるシステム変数を除き、変数に関連付けられているオブジェクトが空でないことを確認する必要があります。空白または間に何もない角カッコは、空のオブジェクトを示します。ポリシーを展開する前に、これらのオブジェクトを編集する必要があります。

（注） オブジェクトのオーバーライドを使用する場合、これらの値はこのビューに表示されません。したがって、空のデフォルト値は、必ずしもオブジェクトが必要な値で更新されていないことを意味するわけではありません。設定をプレビューすると、変数が所定のデバイスに対して正しく解決されるかどうかが示されます。FlexConfig ポリシーのプレビュー （38 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- ポリシーのターゲット デバイスを設定します。FlexConfig ポリシーのターゲット デバイスの設定 （38 ページ）を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。

FlexConfig ポリシーのターゲット デバイスの設定

FlexConfig ポリシーを作成するときに、ポリシーを使用するデバイスを選択できます。その後、次の説明に従って、ポリシーに対するデバイスの割り当てを変更できます。

（注） 通常、デバイスからポリシーの割り当てを解除すると、次回の展開時に、システムは関連付けられた設定を自動的に削除します。ただし、FlexConfig オブジェクトはカスタマイズされたコマンドを展開するためのスクリプトであるため、単にデバイスから FlexConfig ポリシーの割り当てを解除しても、FlexConfig オブジェクトによって設定されたコマンドは削除されません。FlexConfig によって生成されたコマンドをデバイスの構成から削除することが目的の場合は、FlexConfig を使用した設定済み機能の削除 （42 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、FlexConfig ポリシーを編集します。

ステップ 2 [ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 3 [ターゲットデバイス（Targeted Devices）] で、ターゲットリストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。ポリシーは、デバイス、高可用性ペア、およびクラスタを構成するデバイスに割り当てることができます。
- 削除：1 つのデバイスの横にある [削除（Delete）]（🗑） をクリックするか、複数のデバイスを選択して、右クリックしてから [選択項目の削除（Delete Selection）] を選択します。

ステップ 4 [OK] をクリックして選択内容を保存します。

ステップ 5 [保存（Save）] をクリックして、FlexConfig ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

FlexConfig ポリシーのプレビュー

FlexConfig ポリシーをプレビューして、FlexConfig オブジェクトが、どのように CLI コマンドに変換されるかを確認します。プレビューには、FlexConfig オブジェクトで使用されるスクリプトおよび変数から、選択したデバイスに応じて生成されるコマンドが示されます。変数はデバイスの設定に基づいて解決されるため、展開される内容を明確に理解できます。

プレビューを使用すると、FlexConfig オブジェクトの潜在的な問題が見つかります。期待される結果がプレビューに示されるまで、オブジェクトを修正します。

設定は、デバイスごとに個別にプレビューする必要があります。これは、変数がデバイス設定に基づいてさまざまに解決される可能性があるためです。

手順

ステップ 1 **[デバイス（Devices）] > [FlexConfig]** を選択して、FlexConfig ポリシーを編集します。

ステップ 2 未確定の変更がある場合は、[保存（Save）] をクリックします。

プレビューには、最後に保存したバージョンのポリシーに含まれる FlexConfig オブジェクトの結果のみが示されます。新しく追加したオブジェクトのプレビューを確認するには、ポリシーを保存する必要があります。

ステップ 3 [設定のプレビュー（Preview Config）] をクリックします。

ステップ 4 [デバイスの選択（Select Device）] ドロップダウンリストからデバイスを選択します。

システムは、デバイスからの情報と設定済みのポリシーを取得して、次回のデバイスへの展開時に生成する CLI コマンドを決定します。出力を選択してから Ctrl + C を押すことで、その出力をクリップボードにコピーできます。この出力は、詳細な分析のためにテキストファイルに貼り付けることができます。

プレビューには、次のセクションが含まれています。

- Flex-config により前に付加される CLI（Flex-config Prepended CLI）：FlexConfig によって生成されるコマンドであり、設定の前に付加されます。
- 管理対象の機能から生成された CLI（CLI generated from managed features）：Management Center で設定されたポリシーに応じて生成されるコマンドです。コマンドは、デバイスへの最後の正常な展開後の新規ポリシーまたは変更されたポリシーに対して生成されます。これらのコマンドは、割り当て済みのポリシーを実装するために必要なすべてのコマンドを表しているわけではありません。このセクション内のコマンドは、FlexConfig オブジェクトから生成されたものではありません。
- Flex-config により後に付加される CLI（Flex-config Appended CLI）：FlexConfig によって生成されるコマンドであり、設定の後に付加されます。

ステップ 5 [閉じる（Close）] ボタンをクリックして、プレビュー ダイアログを閉じます。

展開された構成の確認

デバイスに FlexConfig ポリシーを展開した後、展開が成功したこと、およびこの構成が期待どおりのものであることを確認します。また、デバイスが期待どおりに機能していることを確認します。

手順

ステップ 1 展開が成功したことを確認するには、次の手順を実行します。

a) メニューバーの [通知（Notifications）] をクリックします。このアイコンは、[展開（Deploy）] と [システム（System）] の間にある、名前のないアイコンです。

アイコンは、次のいずれかで、エラーがあると番号が付くことがあります。

- **（警告がないことを示す）**：警告とエラーはいずれもシステム上に存在していないことを示します。
- **（1 つ以上の警告があることを示す）**：1 つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
- **（1 つ以上のエラーがあることを示す）**：1 つ以上のエラーと任意の数の警告がシステム上に存在することを示します。

b) [展開（Deployment）] で、展開が成功したことを確認します。

c) 詳細な情報、特に失敗した展開の詳細を表示するには、[履歴の表示（Show History）] をクリックします。

d) 左側の列にあるジョブのリストで展開ジョブを選択します。

ジョブは新しい順に表示され、リストの一番上に最新のジョブが表示されます。

e) 右側の列にあるデバイスの [トランスクリプト（Transcript）] 列でダウンロードアイコンをクリックします。

展開トランスクリプトには、デバイスに送信されたコマンドおよびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、FlexConfig から送信したコマンドを含む、エラーを示すメッセージを探します。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注） 管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

たとえば、次のシーケンスは、論理名が outside の GigabitEthernet0/0 を設定するコマンドを Management Center が送信したことを示しています。デバイスは、自動的にセキュリティレベルを 0 に設定したことを応答しました。Threat Defense がセキュリティレベルを使用することはありません。FlexConfig に関連したメッセージは、トランスクリプトの [CLI 適用（CLI Apply）] セクションにあります。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

ステップ 2 展開された構成に必要なコマンドが含まれていることを確認します。

これは、デバイスの管理 IP アドレスへの SSH 接続を確立することで行うことができます。**show running-config** コマンドを使用して、設定を表示します。

または、Secure Firewall Management Center 内で CLI ツールを使用します。

a) **>[ヘルス（Health）]>[モニター（Monitor）]** を選択し、デバイスの名前をクリックします。

ステータス テーブルの [カウント（Count）] 列で開く/閉じる矢印をクリックしてデバイスを表示することが必要になる場合があります。

b) [詳細なトラブルシューティング（Advanced Troubleshooting）] をクリックします。
c) [脅威防御 CLI（Threat Defense CLI）] をクリックします。
d) コマンドとして [show] を選択し、パラメータとして「**running-config**」と入力します。
e) [実行（Execute）] をクリックします。

実行中の構成がテキスト ボックスに表示されます。構成を選択し、Ctrl キーを押した状態で C キーを押して、後で分析できるようにテキスト ファイルに貼り付けることができます。

ステップ 3 デバイスが期待どおりに機能していることを確認します。

機能に関連する **show** コマンドを使用して、詳細情報と統計情報を表示します。たとえば、追加のプロトコル インスペクションを有効にした場合、**show service-policy** コマンドを使用すると、この情報が提供されます。使用する正確なコマンドは機能に依存し、機能の設定方法を学習するときに使用した ASA 構成ガイドおよびコマンド リファレンスに記載されています。

統計情報を表示するコマンドで数（ヒット数、接続数など）が変更されていないことが示された場合、構成は有効であっても意味がないことがあります。トラフィックが、統計情報に表示されるはずのデバイスを通過していることがわかっている場合は、構成に欠如しているものを確認します。たとえば、トラフィックは、機能が適用される前に NAT またはアクセス ルールによってドロップまたは変更される場合があります。

SSH セッションまたは Management Center CLI ツールから **show** コマンドを使用できます。

ただし、使用する必要がある **show** コマンドを Threat Defense CLI 内で直接使用できない場合は、デバイスへのSSH接続を確立してコマンドを使用する必要があります。CLIから、次のコマンド シーケンスを入力して、診断 CLI 内で特権 EXEC モードに切り替えます。ここから、これらのサポートされない **show** コマンドを入力できます。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

FlexConfig を使用した設定済み機能の削除

FlexConfig を使用して設定した一連の設定コマンドの削除が必要な場合は、その設定を手動で削除する必要があります。デバイスから FlexConfig ポリシーの割り当てを解除しても、すべての設定が削除されないことがあります。

手動で設定を削除するには、新しい FlexConfig オブジェクトを作成して、設定コマンドを消去または無効化します。

始める前に

オブジェクトによって生成された設定の一部またはすべてを手動で削除する必要があるかどうかを確認するには、次の手順を実行します。

1. FlexConfig ポリシーのプレビュー （38 ページ）の説明に従い、設定のプレビューを調べます。FlexConfig オブジェクト内のすべてのコマンドを削除するための clear または negate コマンドが `###CLI generated from managed features ###` セクションに含まれている場合は、FlexConfig ポリシーから単純にオブジェクトを削除し、保存して再展開できます。
2. FlexConfig ポリシーからオブジェクトを削除し、変更を保存して、もう一度設定をプレビューします。`###CLI generated from managed features ###` セクションにまだ必要な clear または negate コマンドが含まれていない場合は、次の手順を実行して、手動で設定を削除する必要があります。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択して、FlexConfig オブジェクトを作成することで、設定コマンドを消去または取り消します。

機能に構成時の設定をすべて削除できる **clear** コマンドがある場合は、そのコマンドを使用します。たとえば、事前定義されている ISIS_Unconfigure_All オブジェクトには、次に示すように、すべての ISIS 関連の設定コマンドを削除する 1 つのコマンドが含まれています。

```
clear configure router isis
```

その機能に **clear** コマンドが存在しない場合は、削除する各コマンドの **no** 形式を使用する必要があります。たとえば、事前定義されている Sysopt_basic_negate オブジェクトは、事前定義されている Sysopt_basic オブジェクトで設定したコマンドを削除します。

```
no sysopt traffic detailed-statistics

no sysopt connection timewait
```

通常、設定を削除する FlexConfig オブジェクトを前に追加された、1 回のみ展開されるオブジェクトとして設定します。

ステップ 2 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、新しい FlexConfig ポリシーを作成するか、既存のポリシーを編集します。

設定コマンドを展開する FlexConfig ポリシーを保持する場合は、コマンドの取り消し専用の新しいポリシーを作成して、そのポリシーにデバイスを割り当てます。その後で、新しい FlexConfig オブジェクトをポリシーに追加します。

すべてのデバイスから完全に FlexConfig 設定オブジェクトを削除する場合は、既存の FlexConfig ポリシーから該当するコマンドを削除して、それらのコマンドを設定を取り消すオブジェクトで置き換えます。

ステップ 3 [保存（Save）] をクリックして、FlexConfig ポリシーを保存します。

ステップ 4 [設定のプレビュー（Preview Config）] をクリックして、消去および取り消しコマンドが適切に生成されていることを確認します。

ステップ 5 メニューバーの **[展開（Deploy）]** > **[展開（Deployment）]** を選択し、デバイスを選択して [展開（Deploy）] をクリックします。

展開が完了するまで待機します。

ステップ 6 コマンドが削除されたことを確認します。

デバイスの実行コンフィギュレーションを表示して、コマンドが削除されていることを確認します。詳細については、展開された構成の確認 （39 ページ）を参照してください。

ステップ 7 FlexConfig ポリシーの編集中に、[ポリシーの割り当て（Policy Assignments）] をクリックして、デバイスを削除します。必要に応じて、ポリシーから FlexConfig オブジェクトを削除します。

FlexConfig ポリシーは単に不要な設定コマンドを削除するものであるため、削除の完了後にデバイスに割り当てたポリシーを保持する必要はありません。

ただし、FlexConfig ポリシーにデバイスで設定する必要のあるオプションが残っている場合は、そのポリシーから取り消しオブジェクトを削除します。これらは不要です。

FlexConfig から管理対象機能への変換

ソフトウェアリリースごとに、管理対象機能、つまり FlexConfig の外部で制御されるポリシーを介して直接設定する機能が製品に追加されます。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。ご使用の構成は自動的に変換されません。アップグレード後は、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできません。ソフトウェアのアップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。

FlexConfig を使用して設定した機能が管理対象機能としてサポートされるようになったら、FlexConfig の使用から管理対象機能の使用に変換する必要があります。ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。GUI と FlexConfig の両方で機能を設定することはサポートされていません。

（注） 移行する機能設定が移行ツールでサポートされている場合は、この手順の代わりに移行ツールを使用してください。

手順

ステップ 1 FlexConfig を使用した設定済み機能の削除 （42 ページ）で説明されているように、FlexConfig を削除します。

ステップ 2 新しくサポートされた管理対象機能の設定を構成します。

リリースノートには、そのリリースの新機能のリストがあります。

FlexConfig の例

次に、FlexConfig の使用例をいくつか示します。

高精度時間プロトコルの設定方法（ISA 3000）

高精度時間プロトコル（PTP）は、パケットベース ネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。それらのデバイスクロックは、一般的に精度と安定性が異なります。このプロトコルは、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

PTP システムは、PTP デバイスと非 PTP デバイスの組み合わせによる、分散型のネットワークシステムです。PTP デバイスには、オーディナリ クロック、境界クロック、およびトランスペアレント クロックが含まれます。非 PTP デバイスには、ネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。

Threat Defense デバイスは、トランスペアレントクロックとして設定できます。Threat Defense デバイスは、自身のクロックを PTP クロックと同期しません。Threat Defense デバイスは、PTP クロックで定義されている PTP のデフォルトプロファイルを使用します。

PTP デバイスを設定するときは、連携させるデバイスのドメイン番号を定義します。したがって、複数の PTP ドメインを設定した後、1 つの特定のドメインに PTP クロックを使用するように各非 PTP デバイスを設定できます。

始める前に

デバイスが使用する PTP クロックに設定されているドメイン番号を確認します。この例では、PTP ドメイン番号が 10 であることを前提としています。また、システムがドメイン内の PTP クロックに到達できるインターフェイスを決定します。

以下に、PTP の設定に関するガイドラインを示します。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。
- PTP は IPv6 ネットワークではなく、IPv4 ネットワークでのみ使用できます。
- PTP 設定は、スタンドアロンかブリッジ グループ メンバーかを問わず、物理イーサネット データ インターフェイスでサポートされます。管理インターフェイス、サブインターフェイス、Etherchannel、ブリッジ仮想インターフェイス（BVI）、またはその他の仮想インターフェイスではサポートされません。
- VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。
- PTP パケットが確実にデバイスを通過できるようにする必要があります。PTP トラフィックは UDP 宛先ポート 319 と 320、および宛先 IP アドレス 224.0.1.129 によって識別されます。そのため、このトラフィックを許可するアクセスコントロールルールはすべて動作します。
- ルーテッド ファイアウォール モードでは、PTP マルチキャストグループのマルチキャストルーティングを有効にする必要があります。さらに、PTP をイネーブルにしたインターフェイスがブリッジグループに含まれ**ていない**場合は、IGMP マルチキャスト グループ 224.0.1.129 に参加するようにインターフェイスを設定する必要があります。物理インターフェイスがブリッジグループメンバーである場合、IGMP マルチキャストグループに参加するように設定しないでください。

手順

ステップ 1 （ルーテッド モードのみ）マルチキャスト ルーティングを有効にし、インターフェイスの IGMP グループを設定します。

ルーテッド モードでは、マルチキャスト ルーティングを有効にする必要があります。また、スタンドアロンの物理インターフェイス、つまりブリッジ グループ メンバー以外のインターフェイスについても、224.0.1.129 IGMP グループに参加するようにインターフェイスを設定する必要があります。IGMP グループに参加するようにブリッジ グループ メンバーを設定することはできませんが、ブリッジ グループ メンバーの PTP 設定は IGMP 参加なしでも動作します。

PTP を設定するデバイスごとに次の手順を実行します。

（注） 各デバイス（GigabitEthernet1/1 など）の各 PTP クロック側インターフェイスのハードウェア名を書き留めます。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスを編集します。
b) [ルーティング（Routing）] をクリックします。
c) [マルチキャストルーティング（Multicast Routing）] > [IGMP] を選択します。

d) [マルチキャストルーティングの有効化（Enable Multicast Routing）]チェックボックスをオンにします。

e) [参加グループ（Join Group）] をクリックします。

f) [追加（Add）]をクリックし、[IGMP参加グループパラメータの追加（Add IGMP Join Group parameters）]ダイアログボックスで、次のオプションを設定して [OK] をクリックします。

- [インターフェイス（Interface）]：PTP クロック側スタンドアロンインターフェイスを選択します。
- [参加グループ（Join Group）]：新しいネットワークオブジェクトを追加するには、[+] をクリックします。アドレス 224.0.1.129 のホスト オブジェクトを作成します。追加インターフェイスを設定する場合は、このオブジェクトを選択するだけです。（ネットワーク オブジェクトの作成 を参照。）

デバイス上の PTP クロック側スタンドアロン インターフェイスごとにこの手順を繰り返します。

g) [ルーティング（Routing）] ページで [保存（Save）] をクリックします。

ステップ 2 FlexConfig オブジェクトを作成して、インターフェイス上で PTP をグローバルに有効にします。

次の手順では、設定しているすべてのデバイスで PTP クロック側インターフェイスが同じであると仮定しています。異なるデバイスで異なるインターフェイスを使用している場合は、組み合わせごとに個別のオブジェクトを作成する必要があります。たとえば、デバイス A および B で GigabitEthernet1/1、デバイス C と D で GigabitEthernet1/2、デバイス E と F で GigabitEthernet1/1 と 1/2 の両方を使用する場合は、3 つの個別の FlexConfig オブジェクトと、その後に 3 つの FlexConfig ポリシーをそれぞれ作成する必要があります（次の手順で説明）。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

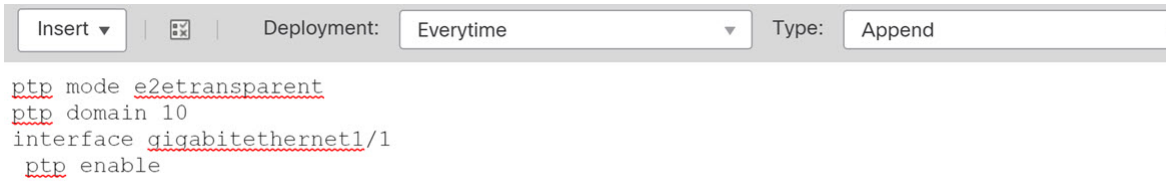
b) コンテンツのテーブルから **[FlexConfig] > [FlexConfigオブジェクト（FlexConfig Object）]** を選択します。

c) [FlexConfigオブジェクトの追加（Add FlexConfig Object）] をクリックし、次のプロパティを設定して、[保存（Save）] をクリックします。

- [名前（Name）]：オブジェクト名。たとえば、Enable_PTP などです。
- [展開（Deployment）]：[毎回（Everytime）] を選択します。この設定をすべての展開に送信し、設定されたままにする必要があります。
- [タイプ（Type）]：デフォルトの [後に付加（Append）] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。このため、インターフェイス設定に加えられた他の変更はこれらのコマンドの前に設定されます。
- [オブジェクト本文（Object body）]：オブジェクト本文で、PTP をグローバルに設定するために必要なコマンドを各 PTP クロック側インターフェイスで入力します。たとえば、PTP ドメイン 10 のグローバル設定と GigabitEthernet1/1 のインターフェイス設定に必要なコマンドは次のとおりです。

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

オブジェクト本文は、次のようになります。



ステップ 3 FlexConfig ポリシーを作成し、デバイスに割り当てます。

PTP クロック側インターフェイスのさまざまな組み合わせに対して複数の FlexConfig オブジェクトを作成した場合、オブジェクトごとに個別の FlexConfig ポリシーを作成し、設定する必要があるインターフェイスに基づいてそれらのポリシーを正しいデバイスに割り当てる必要があります。デバイスのグループごとに次の手順を繰り返します。

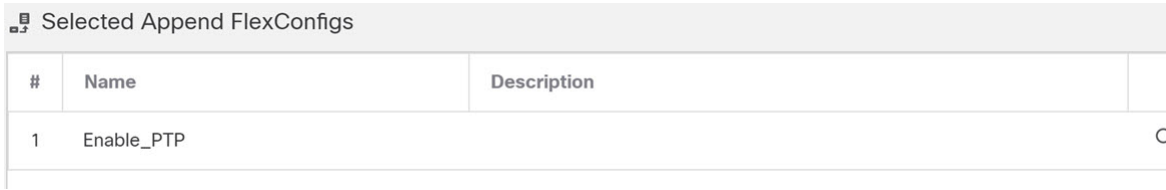
a) **[デバイス（Devices）]** > **[FlexConfig]** を選択します。

b) [新しいポリシー（New Policy）] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

c) コンテンツのテーブルの [ユーザー定義（User Defined）] フォルダ内にある PTP FlexConfig オブジェクトを選択し、[>] をクリックしてポリシーに割り当てます。

オブジェクトが [選択済み追加FlexConfig（Selected Append FlexConfigs）] リストに追加されます。



d) **[保存（Save）]** をクリックします。

e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存（Save）] の下にある **[ポリシー割り当て（Policy Assignment）]** リンクをクリックし、ここで割り当てを行います。

f) [設定のプレビュー（Preview Config）] をクリックし、[プレビュー（Preview）] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。PTP FlexConfig オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表

示されることに注意してください。PTP コマンドの場合、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

ステップ 4 変更を展開します。

FlexConfig ポリシーをデバイスに割り当てたため、展開に関する警告が常に表示されます。これは FlexConfig の使用方法に関する注意です。[続行（Proceed）] をクリックし、展開を続行します。

展開が完了したら、展開の履歴を確認し、展開のトランスクリプトを表示できます。これは展開に失敗した場合に特に役立ちます。展開された構成の確認 （39 ページ） を参照してください。

ステップ 5 各デバイスで PTP 設定を確認します。

SSH またはコンソール セッションから各デバイスにかけて PTP の設定を確認します。

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

停電時の自動ハードウェアバイパスの設定方法（ISA 3000）

ハードウェア バイパスを有効にして、停電時でもトラフィックがインターフェイス ペア間を通過できるようにできます。サポートされているインターフェイスペアは銅線インターフェイスの GigabitEthernet 1/1 と 1/2、および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルを保有している場合は、銅線イーサネット ペア（GigabitEthernet 1/1 と 1/2）でのみハードウェア バイパスがサポートされます。

ハードウェア バイパスがアクティブの場合、トラフィックはレイヤ1でそれらのインターフェイス ペア間を通過します。Threat Defense CLI は、インターフェイスがダウンしていると認識します。ファイアウォール機能はないため、トラフィックのデバイス通過を許可することのリスクを理解している必要があります。

CLI コンソールまたは SSH セッションで、**show hardware-bypass** コマンドを使用して動作ステータスをモニターします。

始める前に

ハードウェア バイパスを機能させるための前提条件：

- インターフェイス ペアは同じブリッジ グループに配置する必要があります。
- インターフェイスはスイッチのアクセスポートに接続する必要があります。トランク ポートには接続しないでください。

デバイスに割り当てられたアクセス コントロール ポリシーに付加された Threat Defense サービスポリシーを使用して、TCP シーケンス番号のランダム化をグローバルに無効にすることをお勧めします。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号（ISN）が乱数に書き換えられます。ハードウェア バイパスがアクティブになると、ISA 3000 はデータ パスには入らず、シーケンス番号は変換されません。受信側のクライアントが予期しないシーケンス番号を受信すると接続がドロップされるため、TCPセッションを再確立する必要があります。TCP シーケンス番号のランダム化が無効になっている場合でも、スイッチオーバー中に一時的にダウンするリンクがあるため、一部の TCP 接続は再確立する必要があります。

手順

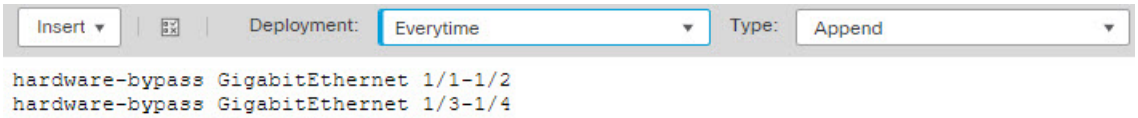
ステップ 1 自動バイパスを有効にする FlexConfig オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から**[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]**を選択します。
c) [FlexConfigオブジェクトの追加（Add FlexConfig Object）] をクリックし、次のプロパティを設定して、[保存（Save）] をクリックします。
   - [名前（Name）]：オブジェクト名。たとえば、Enable_HW-Bypass です。
   - [展開（Deployment）]：[毎回（Everytime）] を選択します。この設定をすべての展開に送信し、設定されたままにする必要があります。

- [タイプ（Type）]：デフォルトの [後に付加（Append）] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
- [オブジェクト本文（Object body）]：オブジェクト本文に、自動ハードウェアバイパスを有効にするために必要なコマンドを入力します。たとえば、可能な両方のインターフェイスペアに必要なコマンドは次のとおりです。

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

オブジェクト本文は、次のようになります。



ステップ 2 FlexConfig ポリシーを作成し、デバイスに割り当てます。

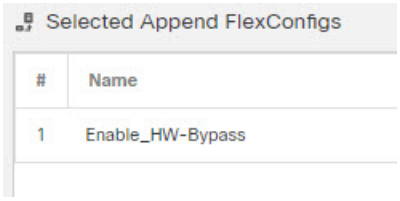
a) **[デバイス（Devices）]** > **[FlexConfig]** を選択します。

b) [新しいポリシー（New Policy）] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

c) 目次の [ユーザー定義（User Defined）] フォルダ内にあるハードウェアバイパス FlexConfig オブジェクトを選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加FlexConfig（Selected Append FlexConfigs）] リストに追加されます。



d) **[保存（Save）]** をクリックします。

e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存（Save）] の下にある **[ポリシー割り当て（Policy Assignment）]** リンクをクリックし、ここで割り当てを行います。

f) [設定のプレビュー（Preview Config）] をクリックし、[プレビュー（Preview）] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。ハードウェアバイパス FlexConfig オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。ハードウェア バイパス コマンドの場合、次のような出力が表示されます。

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

ステップ 3 変更を展開します。

FlexConfig ポリシーをデバイスに割り当てたため、展開に関する警告が常に表示されます。これはFlexConfigの使用方法に関する注意です。[続行（Proceed）]をクリックし、展開を続行します。

展開が完了したら、展開の履歴を確認し、展開のトランスクリプトを表示できます。これは展開に失敗した場合に特に役立ちます。展開された構成の確認 （39 ページ） を参照してください。

次のタスク

ハードウェアバイパスを手動で呼び出したり、手動でオフにしたりする場合は、次の 2 つの FlexConfig オブジェクトを作成する必要があります。

- 手動でバイパスを開始するもの。これには、両方のペアに対してバイパスを呼び出すかどうかに応じて、次のコマンドのいずれかまたは両方が含まれます。

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

- 手動でバイパスをオフにするもの。次のコマンドのいずれかまたは両方が含まれます。

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

次に、いずれかのオブジェクトをFlexConfigポリシーに追加し、変更を展開して、バイパスをオンまたはオフにする必要があります。また、展開後にFlexConfigポリシーからオブジェクトをすぐに削除する必要もあります。バイパスを手動で呼び出す場合は、プロセスを繰り返して再度オフにする必要があります。したがって、この手動による方法を使用するには、FlexConfig ポリシーと追加の展開を頻繁かつ慎重に編集する必要があります。

FlexConfig ポリシーの移行

注目 FlexConfig ポリシーの移行に関するこの項は、ECMP、VXLAN、および EIGRP ポリシーの移行のみを対象としています。

以前のバージョンの Management Center では、ECMP、VXLAN、および EIGRP ポリシーは FlexConfig オブジェクトとポリシーを使用して設定していましたが、Management Center の UI でそれらのポリシーを直接設定できるようになりました。Management Center を以前のバージョ

ンからアップグレードする場合、FlexConfig の設定は保持されます。ただし、UI からポリシーを管理するには、対応する**[デバイスの設定（Device（Edit））]** > **[ルーティング（Routing）]** ページで設定をやり直し、FlexConfig から設定を削除する必要があります。UI でのポリシーの作成を自動化するために、Management Center にはポリシーを FlexConfig から UI に移行するオプションがあります。ただし、移行されたポリシーは FlexConfig から削除されません。移行後の手順については、ステップ 7 （53 ページ）を参照してください。

始める前に

- 展開された FlexConfig ポリシーが最新であることを確認します。移行オプションは、少なくとも 1 つのデバイスでポリシーが最新の場合にのみ使用できます。古いポリシーを持つデバイスについては、移行は行われません。
- ポリシーが FlexConfig と Management Center の両方で設定されている場合：
  - ポリシーが **[デバイスの編集（Device (Edit)）]** > **[ルーティング（Routing）]** ですでに設定されている場合、移行は開始されません。
  - 展開中に、Management Center にエラーメッセージが表示されます。EIGRP 移行エラーメッセージの例：*EIGRP is configured through FlexConfig object and also under Device Listing ->Routing EIGRP for the device. Maintain the EIGRP configuration in either Routing EIGRP or FlexConfig.*（EIGRP は FlexConfig オブジェクトを使用して設定します。デバイスの [デバイスリスト（Device Listing）] ->[EIGRP のルーティング（Routing EIGRP）] で設定することもできます。EIGRP 設定のメンテナンスは、[EIGRP のルーティング（Routing EIGRP）] または FlexConfig で行ってください）
- ポリシーで使用されるネットワークオブジェクトが Management Center に存在する場合は、移行中にそのオブジェクトが再利用されます。移行中に IP アドレス設定に一致するネットワークオブジェクトがない場合、*bb* にタイムスタンプと整数が付加された新しいネットワークオブジェクトが作成されます。たとえば、***bb_<timestamp>_<integer>*** のようになります。このようなネットワークオブジェクトが複数ある場合、名前の整数変数は 1 ずつ増分されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[FlexConfig]** を選択し、移行する FlexConfig ポリシーに対して **[編集（Edit）]**（✎） をクリックします。

ステップ 2 [設定の移行（Migrate Config）] をクリックします。

（注） 移行が開始されると、[設定の移行（Migrate Config）] オプションと FlexConfig の [編集（Edit）] オプションの両方が使用できなくなります。

次の場合、[設定の移行（Migrate Config）] オプションは使用できません。

- 移行する FlexConfig CLI に該当するものが存在しない。
- FlexConfig ポリシーが、どの FlexConfig オブジェクトにも関連付けられていない。
- FlexConfig ポリシーに関連付けられたデバイスが存在しない。

ステップ 3 [Flex設定の移行（Migrate Flex Configuration）] ダイアログボックスで、設定の移行先のデバイスを選択し、[Ok] をクリックします。

移行の進捗状況はタスク通知として表示されます。移行が完了したら、[詳細の表示（View Details）] リンクをクリックして、移行レポート（PDF 形式）をダウンロードします。

ステップ 4 ポリシーの変更を表示するには、**[システム（System）] > [モニタリング（Monitoring）] > [監査（Audit）]** を選択し、[Flex Config の移行（Flex Config Migration）] メッセージをクリックします。

ステップ 5 FlexConfig 移行レポートを表示するには、**[システム（System）] > [モニタリング（Monitoring）] > [監査（Audit）]** を選択し、[Flex Configの移行（Flex Config Migration）] メッセージをクリックします。完全な移行レポートを表示するには、[レポート（Report）] アイコンをクリックします。

ステップ 6 対応する **[デバイスの編集（Device (Edit)）] > [ルーティング（Routing）]** ページで、移行された設定を確認します。

ステップ 7 デバイスの FlexConfig から特定のポリシー設定を削除するには、Management Center で次の手順を実行します。

a) デバイスで移行された FlexConfig ポリシーを識別します。
b) コピーオプションを使用して、FlexConfig ポリシーの複製を作成します。
c) 複製された FlexConfig ポリシーから対応する CLI オブジェクトを削除します。
d) 複製された FlexConfig ポリシーにデバイスを関連付けます。

ステップ 8 設定を保存して展開します。

FlexConfig の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 1000/2100 および Firepower 4100/9300 のデータプレーン障害後の迅速な回復。	7.4.1	7.4.1	データプレーンプロセスがクラッシュした場合、デバイスをリブートする代わりに、データプレーンプロセスのみリロードするようになりました。データプレーンプロセスのリロードに加えて、Snort および他のいくつかのプロセスもリロードされます。 ただし、ブートアップ中にデータプレーンプロセスがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードプロセスループの発生を回避できます。 この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。 新規/変更された CLI コマンド：**data-plane quick-reload**、**no data-plane quick-reload**、**show data-plane quick-reload status** サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300 プラットフォームの制限：マルチインスタンスモードではサポートされていません。 参照：『Cisco Secure Firewall Threat Defense コマンドリファレンス』および『Cisco Secure Firewall ASA シリーズ コマンド リファレンス』
移行ツールのサポート。	7.3.0	いずれか	Flex で構成された ECMP、VXLAN、および EIGRP ポリシーを Management Center に移行するサポートが導入されました。 新規/変更された画面：**[デバイス（Devices）] > [FlexConfig] > [FlexConfigの移行（Migrate FlexConfig）]**
FlexConfig での BFD 設定の削除。	7.3.0	いずれか	Management Center ユーザーインターフェイスで BFD ポリシーを直接設定するためのサポートが導入され、BFD ポリシーを設定するための FlexConfig サポートは削除されました。
プライオリティキューの削除。	7.2.5	7.2.5	Threat Defense でプライオリティキューを設定するためのサポートが削除されました。
FlexConfig での EIGRP 設定の削除。	7.2.0	いずれか	Management Center ユーザーインターフェイスで EIGRP を直接設定するためのサポートが導入され、EIGRP ポリシーを設定するための FlexConfig サポートは削除されました。

機能	最小 Management Center	最小 Threat Defense	詳細
PBR 設定の削除。	7.1.0	7.1.0	FMC ユーザーインターフェイスで PBR を直接設定するためのサポートが導入され、FTD 7.1 以降の PBR を設定するための FlexConfig サポートは削除されました。 新規/変更されたコマンド：**policy-route route-map***routemap-object-name*。
FlexConfig での ECMP ゾーン作成サポートの削除。	7.1.0	いずれか	FMC ユーザーインターフェイスで ECMP ゾーンを直接設定するためのサポートが導入され、EIGRP ゾーンを設定するための FlexConfig サポートは削除されました。
ISA 3000 デバイスの高精度時間プロトコル（PTP）の設定。	6.5.0	いずれか	FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。 FlexConfig オブジェクトに、**ptp**（インターフェイス モード）コマンド、グローバル コマンド **ptp mode e2etransparent**、**ptp domain** を追加できるようになりました。 新規/変更されたコマンド：**show ptp**。
委任された FlexConfig オブジェクト。	6.3.0	いずれか	FlexConfig を使用して設定した以前のリリースの一部の機能が、FMC で直接サポートされるようになりました。この FlexConfig オブジェクトを使用している場合は削除し、新しいオブジェクトを使用するように設定を変換する必要があります。次に、非推奨の FlexConfig オブジェクトおよびテキスト オブジェクトを示します。 • defaultDNSNameServerList および defaultDNSParameters テキスト オブジェクトを含む **Default_DNS_Configure**。プラットフォーム設定ポリシーで、データ インターフェイスの DNS を設定してください。 • **TCP_Embryonic_Conn_Limit**、tcp_conn_misc and tcp_conn_limit テキスト オブジェクト。これらの機能は、FTD サービスポリシーで設定します。ポリシーは、デバイスに割り当てられているアクセス制御ポリシーの [詳細（Advanced）] タブで確認できます。 • **TCP_Embryonic_Conn_Timeout**、tcp_conn_misc および tcp_conn_timeout テキスト オブジェクト。FTD サービスポリシーでこれらの機能を設定します。

機能	最小 Management Center	最小 Threat Defense	詳細
FlexConfig の更新。	6.2.1	いずれか	政府による認定要件に従って、パスワード、システム提供またはユーザ定義の FlexConfig オブジェクトの共有キーなどの機密情報はすべて、秘密キー変数を使用してマスクする必要があります。FMC をバージョン 6.2.1 以降に更新すると、FlexConfig オブジェクト内のすべての機密情報が秘密鍵の変数形式に変換されます。 さらに、次の新しい FlexConfig テンプレートが追加されます。 • **Default_DNS_Configure** テンプレートでは、デフォルトの DNS グループを使用できます。これはデータインターフェイスを介して名前を解決するコマンドまたは機能のホスト名を解決するために使用されます。 • **TCP 初期接続制限およびタイムアウト設定**テンプレートでは、SYN フラッド DoS 攻撃から保護するように初期接続制限/タイムアウト CLI を設定できます。 • **脅威検出の設定およびクリア**テンプレートでは、TCP 代行受信によって傍受された攻撃の脅威検出統計情報を設定できます。 • **IPV6 ルータ ヘッダーの検査**テンプレートでは、さまざまなタイプの特定のヘッダーを選択的に許可またはブロックするように IPV6 検査ヘッダーを設定できます（RH タイプ 2、モバイルの許可など）。 • **DHCPv6 プレフィックス委任**テンプレートでは、IPv6 プレフィックス委任に対して 1 つの外部インターフェイス（プレフィックス委任クライアント）と 1 つの内部インターフェイス（委任されたプレフィックスの受信者）を設定します。

機能	最小 Management Center	最小 Threat Defense	詳細
FlexConfig。	6.2.0	いずれか	FlexConfig 機能では、FMC を使用して ASA CLI テンプレートベースの機能をFTDデバイスに展開できます。この機能を使用すると、FTDデバイスで現在使用できない最も重要な ASA 機能の一部を有効にできます。この機能は、ポリシー内で連携するテンプレートとオブジェクトとして構造化されています。デフォルトのテンプレートは Cisco TAC で公式にサポートされています。 新規/変更された画面： • **[デバイス（Devices）] > [FlexConfig]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfigオブジェクト（FlexConfig Objects）]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [テキストオブジェクト（Text Object）]**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。