



Cisco Defense Orchestrator を利用した FDM 管理対象デバイス への ASA の移行

初版：2019年6月17日

最終更新：2020年5月6日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

使用する前に 1

- 適切な移行プロセスの選択 1
- Cisco Defense Orchestrator の移行プロセスについて 1
- 移行プロセスのライセンス 3
- 注意事項と制約事項 3
- CDO 上の対応 IP プロトコル 9
- ベストプラクティス 11

第 2 章

ASA を FDM 管理対象デバイスに移行するワークフロー 13

- 移行プロセスの導入方法 13
 - 移行の準備 14
 - ASA デバイスのオンボーディング 14
 - 移行前の ASA ポリシーの最適化 15
 - 移行前に EtherChannel 設定を FDM 管理対象デバイスに追加 15
 - 移行の実行 16
 - 移行するデバイスの選択 16
 - (任意) 移行名の更新 17
 - (オプション) 実行構成の保持 (Preserve the Running Configuration) 18
 - ASA 設定を解析する 19
 - 移行の適用 20
 - 移行アクションの表示 24
 - 設定の展開 26

付録 A :

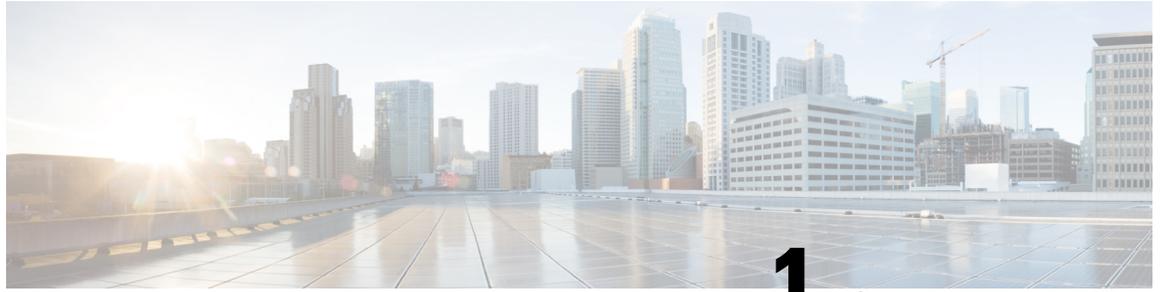
テレメトリ 27

Cisco Success Network 27

付録 B :

FAQ 29

トラブルシューティングの FAQ 29



第 1 章

使用する前に

- 適切な移行プロセスの選択 (1 ページ)
- Cisco Defense Orchestrator の移行プロセスについて (1 ページ)
- 移行プロセスのライセンス (3 ページ)
- 注意事項と制約事項 (3 ページ)
- CDO 上の対応 IP プロトコル (9 ページ)
- ベストプラクティス (11 ページ)

適切な移行プロセスの選択

Cisco Defense Orchestrator (CDO) を使用して適応型セキュリティアプライアンス (ASA) の設定を FDM による管理 デバイスに移行するには、2 つの方法があります。

- CDO ソリューション：ASA 設定を FDM による管理 デバイスに移行し、FTD デバイスを CDO および Firepower Device Manager で管理する場合は、CDO でクラウドベースのプロセスを使用して ASA 設定を移行します。
- オンプレミスソリューション (Firepower Device Manager)：ASA 設定を FDM による管理 デバイスに移行する場合は、CDO でクラウドベースのプロセスを使用して ASA 設定を移行します。その後、Firepower Device Manager を使用して構成を管理できます。

このガイドは、読者が CDO 操作の基本を理解していることを前提としています。詳細については、『[CDO Data Sheet](#)』を参照してください。

Cisco Defense Orchestrator の移行プロセスについて

CDO は、適応型セキュリティアプライアンス (ASA) を FDM による管理 デバイスに移行するのに役立ちます。CDO には、ASA の実行構成を FDM テンプレートに移行するための [ASA から FDM に移行 (ASA to FDM Migration)] ウィザードが用意されています。



- (注) [ツールとサービス (Tools & Services)] で [ASAからFDMに移行 (ASA to FDM Migration)] オプションを表示するには、show-fdm および enable-asa-to-ftd-migration 機能フラグを有効にする必要があります。[ツールとサービス (Tools & Services)] で利用できない場合は、TAC に連絡して、[ASAからFDMに移行 (ASA to FDM Migration)] オプションをアクティブにします。

[ASAからFDMに移行 (ASA to FDM Migration)] ウィザードを使用して、ASA の実行設定の次の要素を FDM テンプレートに移行できます。

- インターフェイス
- ルート
- アクセス制御ルール (ACL)
- ネットワークアドレス変換 (NAT) ルール
- ネットワークオブジェクトとネットワーク グループ オブジェクト



- (注) CDO は、予約済みキーワードを含むオブジェクト名をサポートしていません。オブジェクト名を、「ftdmig」というサフィックスを追加して変更してください。

- サービスオブジェクトとサービス グループ オブジェクト
- サイト間 VPN

CDO は、参照されたオブジェクトのみを移行します。アクセス制御リスト内で、定義されているがアクセスグループに参照されていないオブジェクトは移行されません。CDO が特定の要素の移行に失敗する一般的な理由には、次の 1 つ以上が当てはまる場合があります。

- ICMP コードのない ICMP アクセスリスト
- TCP/UDP アクセスリストにアクセスグループが設定されていない
- IP アクセスリストがサイト間 VPN プロファイルにマップされていない
- アクセスリストを参照するネットワークオブジェクトまたはグループのいずれかが移行されていない
- インターフェイスがシャットダウンとして参照される



- (注) 構成内の参照されていないオブジェクトまたはオブジェクトグループも削除され、移行中に未使用としてマークされます。移行されていない要素の詳細については、「移行レポート」を参照してください。

ASA 実行構成のこれらの要素を FDM テンプレートに移行したら、その FDM テンプレートを、CDO によって管理される新しい FDM による管理 デバイスに適用できます。FDM による管理 デバイスはテンプレートで定義された構成を採用するため、FDM による管理は ASA の実行構成のいくつかの側面を使用して構成されるようになりました。

ASA 実行コンフィギュレーションの他の要素は、このプロセスを使用して移行されません。これらの他の要素は、FDM テンプレートでは空の値で表されます。テンプレートが FDM による管理 デバイスに適用されると、移行された値が新しいデバイスに適用され、空の値は無視されます。新しいデバイスの他のデフォルト値は、すべて保持されます。移行されなかった ASA 実行コンフィギュレーションのその他の要素は、移行プロセス以外で FDM による管理 デバイスで再作成する必要があります。

移行プロセスのライセンス

FDM による管理 デバイス移行プロセスは CDO の一部であり、CDO ライセンス以外の特定のライセンスは必要ありません。

注意事項と制約事項



- (注) CDO でサポートされていない設定は、移行中にサポート対象外として削除され、移行レポートで報告されます。

機能名	移行できるもの	移行に関する制限
ファイアウォールモード	ルーテッドファイアウォールモード	トランスペアレントモードの設定は移行できません。

機能名	移行できるもの	移行に関する制限
インターフェイス設定	<ul style="list-style-type: none"> • 物理インターフェイス • サブインターフェイス 	<ul style="list-style-type: none"> • FDMによる管理デバイスには、移行するASA インターフェイスの設定と同等以上の物理インターフェイスが必要です。 • サブインターフェイス (サブインターフェイス ID は移行時の VLAN ID と同じ番号に常に設定されます) • 次のインターフェイス設定はFDMによる管理 デバイスに移行されません。 <ul style="list-style-type: none"> • ASA インターフェイスのセカンダリ VLAN • Redundant Interface • □ブリッジグループ インターフェイス • 仮想トンネル インターフェイス

機能名	移行できるもの	移行に関する制限
EtherChanel	<p>物理インターフェイスで設定された EtherChannel。</p> <p>EtherChanel にマッピングされたメンバーインターフェイスは、移行中も保持されます。</p>	<ul style="list-style-type: none"> • 設定を移行する前に、CDO を使用して FDM による管理 デバイスに同等の数の EtherChannel を作成する必要があります。 「FDM 管理対象デバイスの EtherChannel インターフェイスの追加」を参照してください。 • Firepower 1000 または 2100 シリーズのハードウェアデバイス (1010、1120、1140、1150、2110、2120、2130、2140) の設定にのみ移行できます。 • EtherChannel 設定を、ASA 8.4+ からソフトウェアバージョン 6.5+ で動作する FDM による管理 デバイスに移行できます。 • 移行前に FDM による管理 デバイスで作成されている EtherChannel は、移行される EtherChannel と同じタイプである必要があります。 <p>CDO が移行するのは、EtherChannel から EtherChannel へ、および物理インターフェイスから物理インターフェイスへのみです。</p> <ul style="list-style-type: none"> • FDM テンプレートで EtherChannel にマッピングされたメンバーインターフェイスを、移行ウィザードのインターフェイスマッピングステップでユーザーが使用することはできません。ただし、それらは保持され、割り当てられた EtherChannel に移行されます。
ルーティング	スタティック ルート	<ul style="list-style-type: none"> • 同じネットワークを宛先とする静的ルートが複数ある場合、最小のメトリック値を持つ 1 つのルートのみが移行され、その他のルートはドロップされます。 • 次のルート機能は FDM による管理 デバイスに移行されません。 <ul style="list-style-type: none"> • トンネルルート • Null 0 インターフェイスルート • SLA トラックを持つ静的ルート

機能名	移行できるもの	移行に関する制限
<p>アクセス制御ルール (ACL)</p>	<ul style="list-style-type: none"> • 有効化されたアクセス制御ルール • 送信元オブジェクトと宛先オブジェクト • CDO は、FDM による管理デバイスの許可、信頼、ブロックなどのアクションをサポートしています。移行時に、移行元の ASA の設定における許可アクションと拒否アクションが処理され、CDO で FDM による管理デバイスに関してサポートされているアクションにマッピングされます。 • CDO は、ポリシー、インターフェイス、またはアクセスグループ (IP プロトコルを持たない) に付加された ACL の移行をサポートしています。 • 非暗号化 L3 トンネルプロトコルを使用した ACE 	<p>次の ACL 機能は FDM による管理デバイスに移行されません。</p> <ul style="list-style-type: none"> • CDO と Firepower Device manager は、IPv4 と IPv6 の混在プロトコルを使用した ACL をサポートしていません。 • 重大度情報のロギング • 非アクティブのルールまたは無効化されたルール • TCP、UDP、または ICMP 以外のプロトコルを持つサービスオブジェクトまたはサービスグループを使用した ACE • TCP または UDP 以外のサービスオブジェクトを使用した ACE • インラインオブジェクトを使用した ACE の TCP または UDP 以外のプロトコル • 時間範囲を使用した ACE • アクセスグループを使用してマッピングされていないアクセスリスト

機能名	移行できるもの	移行に関する制限
ネットワークアドレス変換 (NAT) ルール	<ul style="list-style-type: none"> • ネットワークオブジェクト (自動) および Twice (手動) NAT または PAT • スタティック NAT • ダイナミック NAT または PAT • アイデンティティ NAT • 送信元ポート (サービス) 変換 	<p>次の NAT ルール機能は FDM による管理 デバイスに移行されません。</p> <ul style="list-style-type: none"> • PAT プール • 単一方向 (Unidirectional) • 非アクティブ • Twice NAT の場合、宛先ポート (サービス) 変換のための宛先サービスオブジェクトの使用 (送信元と宛先の両方を持つサービスオブジェクトを含む) • 宛先ポート変換 • NAT46、NAT64 <p>(注) CDO は、0.0.0.0/32 のネットワークオブジェクトをサポートしていません。</p>
サービスオブジェクトとサービスグループオブジェクト	<p>サービスオブジェクトとネストされたグループ</p> <p>CDO がサポートしているサービスオブジェクトで使用されるプロトコルのリストについては、「CDO 上の対応 IP プロトコル」を参照してください。</p>	<ul style="list-style-type: none"> • プロトコル、BCC-RCC-MON、および BBN-RCC-MON はサポートされていません。 • 「より小さい (less than)」、「より大きい (greater than)」、「等しくない (not equal to)」などの演算子はサポートされていません。 • オブジェクトグループのネスト
ネットワークオブジェクトとネットワークグループオブジェクト	<p>ネットワークオブジェクトとネットワークグループオブジェクト</p>	<p>次のネットワークオブジェクトまたはネットワークグループはサポートされていません。</p> <ul style="list-style-type: none"> • 不連続マスクベース • IPv4 アドレスで最初のオクテットが「0」の IP アドレス

機能名	移行できるもの	移行に関する制限
ICMP タイプ	ICMP タイプ	<p>次の ICMP タイプはサポートされていません。</p> <ul style="list-style-type: none"> 無効な ICMP タイプまたはコードを持つ ICMP ベースのサービス オブジェクト エントリ ICMPv4 または ICMPv6 タイプのコードのないサービスタイプまたは ICMP タイプ オブジェクト 未割り当ての ICMP タイプ (IANA に従う) または無効な ICMP タイプ
その他のサポートされていないオブジェクト	-	<p>次の各種オブジェクトはサポートされていません。</p> <ul style="list-style-type: none"> SGT ベースのネットワーク オブジェクト グループ ユーザーベースのネットワーク オブジェクト グループ
サイト間 VPN	<ul style="list-style-type: none"> IKEv1 と IKEv2 の両方のフェーズ 1 およびフェーズ 2 プロポーザル IKEv1 と IKEv2 の両方の完全転送秘密 (PFS) ネストされたオブジェクトグループを使用したクリプトアクセスリスト 複数のピア IP を使用したクリプトマップ 暗号マップでトンネルに使用される IKEv1 と IKEv2 の両方 	<p>次のサイト間 VPN 機能はサポートしていません。</p> <ul style="list-style-type: none"> vpn-filter vpn-idle-timeout isakmp keepalive threshold 10 retry 10 crypto map vpnmap 200 set security-association lifetime seconds 360 set security-association lifetime kilobytes unlimited set security-association lifetime seconds 3600 証明書認証 ダイナミック クリプト マップ ルートベースの VPN (仮想トンネルインターフェイス)

注意事項と制約事項の詳細については、「[ASA 構成の注意事項と制約事項](#)」および「[FDM による管理 デバイスに関する注意事項と制約事項](#)」を参照してください。

CDO 上の対応 IP プロトコル

CDO がサービスオブジェクトでサポートする IP プロトコルは、次のとおりです。

サービスオブジェクトの IP プロトコル			
1 = ICMP	34 = THREEPC	73 = CPHB	106 = QNX
2 = IGMP	35 = IDPR	74 = WSN	107 = AN
3 = GGP	36 = XTP	75 = PVP	108 = IPCOMP
5 = ST2	37 = DDP	76 = BRSATMON	109 = SNP
6 = TCP	38 = IDPRCMTTP	78 = WBMON	110 = COMPAQPEER
7 = CBT	39 = TPPLUSPLUS	77 = SUNND	111 = IPXINIP
8 = EGP	40 = IL	79 = WBEXPAK	112 = VRRP
9 = IGP	42 = SDRP	80 = ISOIP	113 = PGM
10 = BBNRCCMON	45 = IDRP	81 = VMTP	115 = L2TP
11 = NVP2	46 = RSVP	82 = SECUREVMTP	116 = DDX
12 = PUP	48 = MHRP	83 = VINES	117 = IATP
13 = ARGUS	49 = BNA	84 = TTP	118 = ST
14 = EMCON	50 = ESP	85 = NSFNETIGP	119 = SRP
15 = XNET	51 = AH	86 = DGP	120 = UTI
16 = CHAOS	52 = INLSP	87 = TCF	121 = SMP
17 = UDP	53 = SWIPE	88 = EIGRP	122 = SM
18 = MUX	54 = NARP	89 = OSPFIGP	123 = PTP
19 = DCNMEAS	55 = MOBILE	90 = SPRITERPC	124 = ISIS
20 = HMP	56 = TLSP	91 = LARP	125 = FIRE
21 = PRM	57 = SKIP	92 = MTP	126 = CRTP
22 = XNSIDP	58 = IPv6-ICMP	93 = AX25	127 = CRUDP
23 = TRUNK1	59 = IPv6NONXT	94 = IPIP	128 = SSCOPMCE
24 = TRUNK2	62 = CFTP	95 = MICP	129 = IPLT
25 = LEAF1	64 = SATEXPAK	96 = SCCSP	130 = SPS
26 = LEAF2	65 = KRYPTOLAN	97 = ETHERIP	131 = PIPE
27 = RDP	66 = RVD	98 = ENCAP	132 = SCTP
28 = IRTP	67 = IPPC	100 = GMTP	133 = FC
29 = ISOTP4	69 = SATMON	101 = IFMPP	254 = DIVERT
30 = NETBLT	70 = VISA	102 = PNNI	
31 = MFENSP	71 = IPCV	103 = PIM	
32 = MERITINP	72 = CPNX	104 = ARIS	
33 = SEP		105 = SCPS	

ベストプラクティス

CDO を使用して ASA 設定を FDM テンプレートに移行する場合は、次のベストプラクティスに従ってください。

- モデルデバイスの移行で **show run** コマンドを使用して、ASA デバイスから実行構成を取得していることを確認します。
- スキップされた設定、サポートされていない設定、および部分的にサポートされている設定について、移行レポートを確認します。
- 移行後、FDM による管理 デバイスに展開する前に、移行されたルールとオブジェクトを FDM テンプレートで確認します。
- ASA ポリシーを FDM テンプレートに移行する前に最適化します。
- 移行した ASA 設定は、既存の設定がない FDM による管理 デバイスに展開することをお勧めします。



第 2 章

ASA を FDM 管理対象デバイスに移行する ワークフロー

- ・移行プロセスの導入方法 (13 ページ)

移行プロセスの導入方法

	操作内容
ステップ 1	移行の準備 (14 ページ) <ul style="list-style-type: none">・ASA デバイスのオンボーディング・移行前の ASA ポリシーの最適化・移行前に EtherChannel 設定を FDM 管理対象デバイスに追加 (15 ページ)
ステップ 2	移行の実行 (16 ページ) <ul style="list-style-type: none">・移行するデバイスの選択・(任意) 移行名の更新・ASA 設定を解析する・移行の適用<ul style="list-style-type: none">・今すぐ移行を適用・後で移行を適用
ステップ 3 :	移行アクションの表示
ステップ 4 :	設定の展開 (26 ページ)

移行の準備

移行のためにデバイスを準備するには、次の点を確認してください。

- CDO テナントがあり、ログインできる必要があります。詳細については、「[最初のログイン](#)」を参照してください。
- FDM による管理 デバイスに移行する ASA デバイスまたは ASA 構成ファイルがテナントに導入準備されている必要があります。
ASA の実行構成ファイルは、4.5 MB および 22,000 行未満である必要があります。「[ASA 実行設定サイズを確認する](#)」を参照してください。
- 移行プロセスの直後に ASA 構成をデバイスに移行する場合または EtherChannel 設定を FDM による管理 デバイスに移行する場合は、FDM による管理 デバイスを CDO に導入準備している必要があります。詳細については、「[Onboard an FTD device](#)」を参照してください。
- デバイスは同期状態である必要があります。
これにより、デバイスの実行構成と CDO に保存されている実行構成が同じになります。
- ASA はソフトウェアバージョン 8.4 以降を実行している必要があります。

デバイスサポートサマリー、サポートされていないデバイス、ハードウェアとソフトウェアの仕様の詳細については、「[CDO でサポートされるソフトウェアとハードウェア](#)」を参照してください。

ASA デバイスのオンボーディング

[インベントリ (Inventory)] ページで (+) をクリックします。

[導入準備] ページには、デバイスを導入準備できる場所が表示されます。

ASA デバイスの導入準備方法

以下の手順に従って、いずれかのオプションで ASA デバイスを導入準備します。

- ライブ ASA デバイスを導入準備します。
- オフライン管理用の構成をインポートします。
 - デバイス名を入力し、[デバイスタイプ] を ASA として選択します。
 - [参照 (Browse)] をクリックして、ASA 構成ファイル (.TXT または .CFG ファイル) を選択します。
 - [アップロード (Upload)] をクリックします。

移行前の ASA ポリシーの最適化

すべての ASA を導入準備したので、CDO を使用してネットワークオブジェクトの問題を特定して修正し、既存のポリシーを最適化し、VPN 接続を確認して、ASA を最新リリースにアップグレードします。

ネットワークオブジェクトの問題を解決する

ネットワーク ポリシー [オブジェクト](#)の問題を解決することにより、ASA のセキュリティポリシーの最適化を開始します。

- [未使用のオブジェクト](#) : CDO は、デバイス構成内に存在するものの、別のオブジェクト、アクセスリスト、または NAT ルールによって参照されていないネットワーク ポリシー オブジェクトを識別します。そのような未使用のオブジェクトを見つけて削除します。
- [重複するオブジェクト](#) : 重複するオブジェクトは、同じデバイス上にある、名前は異なるものの値が同じである 2 つ以上のオブジェクトです。重複するオブジェクトは、通常、偶然に作成され、同じ目的を果たし、さまざまなポリシーによって使用されます。一部の重複は正当な理由で存在することを認識しつつ、名前を標準化する機会を探します。
- [不整合オブジェクト](#) : 不整合オブジェクトとは、2 つ以上のデバイス上にある、名前は同じであるものの値が異なるオブジェクトです。ユーザーは、さまざまな設定の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。該当するオブジェクトの値の標準化や、名前の変更により、別のオブジェクトとして識別されるようにすることを検討してください。

シャドウルールの修正

ネットワークオブジェクトの問題を解決したら、次に[シャドウルール](#)のネットワークポリシーを確認して修正します。シャドウルールは、ネットワークポリシーのページで半月のバッジで示されます。シャドウルールは、トリガーされることのないルールです。ポリシー内で高い優先順位を付与されたルールは、パケットがシャドウ化されたルールに到達する前にすべてのパケットで動作するためです。到達されることのないシャドウ化されたルールが存在する場合は、そのルールを削除するか、[ポリシーを編集](#)してルールのシャドウ化を解除します。

移行前に EtherChannel 設定を FDM 管理対象デバイスに追加

始める前に

次の情報を確認します。

- [移行の準備](#) (14 ページ)
- EtherChannel を移行するための[注意事項と制約事項](#) (3 ページ)。

手順

ステップ 1 EtherChannel 設定を移行する前に、ASA から移行する FDM による管理 デバイス上で、同じ数の EtherChannel を作成する必要があります。EtherChannel を作成するには CDO を使用できません。手順については、「[FDM 管理対象デバイスの EtherChannel インターフェイスの追加](#)」を参照してください。

EtherChannel の最小構成は、EtherChannel ID と少なくとも 1 つの EtherChannel メンバーです。

ステップ 2 変更を、お使いの FDM による管理 デバイスに展開します。

次のタスク

[移行の実行 \(16 ページ\)](#) に進みます。

移行の実行

移行するデバイスの選択

次のいずれかの方法を使用して、移行する ASA デバイスを選択できます。

- [FDM 移行ウィザードを起動してデバイスを選択](#)
- [デバイスを選択して FDM 移行ウィザードを起動](#)

FDM 移行ウィザードを起動してデバイスを選択

手順

ステップ 1 CDO テナントにログインします。

ステップ 2 ナビゲーションバーで、[ツールとデバイス (Tools & Services)] をクリックします。

ステップ 3 [ツールとサービス (Tools & Services)] で、[ASAからFDMに移行 (ASA to FDM Migration)] を選択します。

(注) [ツールとサービス (Tools & Services)] で [ASAからFDMに移行 (ASA to FDM Migration)] オプションを表示するには、show-fdm および enable-asa-to-ftd-migration 機能フラグを有効にする必要があります。[ツールとサービス (Tools & Services)] で利用できない場合は、TAC に連絡して、[ASAからFDMに移行 (ASA to FDM Migration)] オプションをアクティブにします。

ステップ 4 [FDM移行 (FDM Migration)] ページで (+) をクリックして ASA デバイスを追加するか、FDM 管理対象デバイスに移行する構成ファイルをアップロードします。

ステップ 5 ASA 構成ファイルをアップロードするか、ドロップダウンリストからデバイスを選択します。

このデバイスを以前に移行している場合、選択したデバイスからの移行結果が表示されます。フィルタリングの詳細については、「[移行フィルタについて](#)」を参照してください。

これが新しい移行の場合は、[(デバイス名) の新しい移行を開始する (Start a new migration for (device name))] をクリックします。

デバイスを選択して FDM 移行ウィザードを起動

手順

- ステップ 1** CDO テナントにログインします。
- ステップ 2** ナビゲーションバーで、[インベントリ (Inventory)] をクリックします。
- ステップ 3** [デバイス (Devices)] タブをクリックして、デバイスを見つけます。
- ステップ 4** [ASA] タブをクリックし、FDM による管理 デバイスに移行する ASA デバイスまたはモデルを選択します。

ロケーション、モデル、シリアルなど、選択した ASA デバイスの詳細が [デバイスの詳細] ペインに表示されます。
- ステップ 5** [デバイスアクション (Device Actions)] ペインで、[FDMに移行 (Migrate to FDM)] をクリックします。

このデバイスを以前に移行している場合、選択したデバイスからの移行結果が表示されます。フィルタリングの詳細については、「[移行フィルタについて](#)」を参照してください。

これが新しい移行の場合は、[(デバイス名) の新しい移行を開始する (Start a new migration for (device name))] をクリックします。
- ステップ 6** (任意) 別の ASA デバイスまたはモデルを選択して FDM テンプレートに移行する場合は、「[移行フィルタについて](#)」を参照してください。

(任意) 移行名の更新

移行名は、デバイス名とタイムスタンプに基づいて自動生成されます。

手順

- ステップ 1** [FDM 移行 (FDM Migration)] 画面では、移行名を更新することも、デフォルト名を保持することもできます。CDO では、移行名で移行リストを検索できます。

(注) FDM テンプレート名は、デフォルトでは移行名と同じになります。

ステップ 2 [次へ] をクリックして移行を開始します。

(オプション) 実行構成の保持 (Preserve the Running Configuration)



(注) これは、[インベントリ (Inventory)] ページからライブ ASA を選択した場合にのみ適用されます。

[実行構成の保持 (Preserve the Running Configuration)] では、移行ツールを使用して、ASA の実行構成の CDO のコピーを構成ファイルとして保存できます。このモデルデバイス設定は移行に使用されるため、ライブ ASA には影響しません。

ASA の実行構成の CDO のコピーを FDM による管理デバイスに移行するには、次のオプションを使用できます。

- ASA の実行中デバイスの CDO のコピーから構成ファイルを作成します。



(注) 移行の開始時点で ASA 設定のスナップショット (モデルデバイス) を保持できます。移行のために設定を変更する必要がある場合は、ASA の実行構成の CDO のコピーに影響を与えたり、中断したりすることなく、構成ファイルを使用できます。

- デバイスから直接設定を移行する



(注) 移行のソースとなる設定は、ASA の実行構成の CDO のコピーです。移行ツールでは、移行が開始された時点での設定のみが考慮されます。後で ASA の実行構成の CDO のコピーを変更しても、結果の移行には反映されません。ASA の実行構成の変更された CDO のコピーからの追加の移行試行により、異なる FDM による管理デバイス設定が生じる可能性があります。

手順

ステップ 1 [モデルデバイス名 (Model Device Name)] フィールドにモデルデバイス名を入力します。

ステップ 2 次のいずれかの操作を行います。

- a) [Next] をクリックします。

モデルデバイスが作成され、そのデバイスの移行がトリガーされます。

- b) [スキップ] をクリックして、ライブ ASA で移行をトリガーします。

ASA 設定を解析する



- (注) 構成ファイルのサイズ、および他のデバイスまたはサービスの数によっては、構成の解析に時間がかかる場合があります。詳細については、「[ASA 実行設定サイズを確認する](#)」を参照してください。

移行の解析は、成功または失敗するまで続行されます。移行プロセスでは、ASA 情報が収集されて解析され、FDM テンプレートが作成され、この FDM テンプレートを CDO でデバイスに適用することが可能になります。FDM テンプレートについての詳細は、「[テンプレート](#)」を参照してください。解析フェーズ中に、移行プロセスによって、次を特定する**移行レポート**と**移行ログ**が生成されます。

- 完全に移行された、部分的に移行された、移行がサポートされていない、および移行が無視された ASA 構成項目。
- 移行プロセスで認識できない ASA CLI を示す、エラーのある ASA 構成行（これにより、移行がブロックされています）。



- (注) 管理インターフェイスと、管理インターフェイスに関連付けられている静的ルートは移行されません。

移行エラーの修正

移行エラーが発生した場合は、[FDM移行 (FDM Migration)] 画面で[移行レポートのレビュー (Review Migration Report)] と [移行ログのレビュー (Review Migration Log)] を確認できます。

[FDM移行 (FDM Migration)] 画面から [レポートのダウンロード (Download Report)] と [ログのダウンロード (Download Log)] を選択して、移行レポートとログをダウンロードします。

レポートとログから、解析失敗の原因となった ASA 設定の行を出力できる必要があります。移行のために選択した ASA デバイスに移動し、ASA 設定を更新してから、新しい移行を再開します。

解析は成功したが FDM テンプレートの作成が失敗した場合は、[テンプレート (Template)] > [ワークフロー (Workflows)] または [移行 (Migration)] > [ワークフロー (Workflows)] に移動して、失敗を特定し、問題に対処します。

移行エラー修正後の再解析

移行エラーを修正後、ASA 設定を再解析できます。次の手順を実行します。

- [FDM移行 (FDM Migration)] 画面で、[設定に移動 (Go to Configuration)] をクリックします。
- 特定の設定に移動し、変換失敗の原因となった設定を変更します。
- 正しい設定の更新を実行したら、[設定の再解析 (Re-parse the configuration)] をクリックして、変更された設定に対して移行をトリガーします。



(注) [設定の再解析 (Re-parse the configuration)] オプションは、構成ファイルを更新した場合にのみ、解析エラーのある設定にのみ適用できます。

移行の適用

移行を適用する場合、次のいずれかのオプションを選択できます。

- [今すぐ移行を適用](#)
- [後で移行を適用](#)

CDO のテンプレートの適用機能に従って、移行中に作成された FDM テンプレートにより、デバイスでの変更がインターフェイス、NAT、ACL、オブジェクト、およびルートにのみ展開されます。

インターフェイス情報は移行中に変更されるため、DHCP およびデータ DNS 設定はデフォルトに復元されます。

VPN、HA などのその他の設定は、デバイスで同じ状態で維持されます。

今すぐ移行を適用



(注) デバイスに移行を適用する前に、デバイスが**同期**状態にあるかどうかを確認してください。

FDM テンプレートを任意のデバイスに適用し、デバイステンプレートを確認して、後で FDM による管理 デバイスを選択してデバイスに展開できます。

手順

ステップ 1 [今すぐ移行を適用 (Apply Migration Now)] を選択します。

- [FTD デバイスを選択 (Select FTD Device)] ドロップダウンリストから、FDM デバイステンプレートを適用する FDM による管理 デバイスを選択します。

デバイスは、接続が [オンライン] で [同期 (Synced)] 状態である必要があります。

- [選択 (Select)] をクリックして、FDM による管理 デバイスを選択します。

ステップ 2 [次へ (Next)] をクリックします。

ステップ 3 [インターフェイスのマップ (Map Interface)] 行で、移行ツールは FDM による管理 デバイス上の [テンプレートインターフェイス (Template Interfaces)] と [デバイスインターフェイス (Devices Interfaces)] のリストを取得します。デフォルトでは、ファイアウォール移行ツールは ASA のインターフェイスと FDM による管理 デバイスを、インターフェイス ID に従ってマッピングします。[Continue] をクリックします。

ASA インターフェイスと FDM による管理 デバイスのマッピングの詳細については、『[Map ASA Interfaces with Firewall Threat Defense Interfaces](#)』を参照してください。

ステップ 4 FDM による管理 デバイ스에適用する FDM テンプレート情報を確認し、[テンプレートの適用 (Apply Template)] をクリックします。

ステップ 5 [完了 (Done)] 行では、次の操作を実行できます。

選択した FDM による管理 デバイ스에、移行された設定を正常に適用しました。

- [移行に使用したモデルデバイスを削除 (Remove model device used for migration)] チェックボックスをクリックします。

このチェックボックスをオンにすると、ライブ ASA から作成されたモデルデバイスが削除されます。これにより、モデルデバイスも削除され、移行ログと移行に関連付けられたファイルも削除されます。

(注) このチェックボックスは、ライブ ASA が [インベントリ (Inventory)] ページから選択され、ユーザーがモデルデバイスを作成した場合にのみ表示されます。

- [移行した設定をテンプレートとして保存 (Save migrated configuration as a template)] チェックボックスをクリックします。

(注) このチェックボックスは、FDM テンプレートが正常に適用されている場合にのみ表示され、デフォルトでオンになっています。

チェックボックスがオフの場合、FDM テンプレートは保存されません。

FDM テンプレートの適用中にエラーが発生した場合は、[デバイス (Device)] > [ワークフロー (Workflows)] に移動してエラーを表示し、問題に対処します。

(注) FDM テンプレートには [デバイスとサービス (Devices & Services)] ページからアクセスできます。FDM テンプレートについての詳細は、「[テンプレート](#)」を参照してください。

(注) FDM テンプレートが正常に保存されたら、次のアクションを実行できます。

次のいずれかの操作を行います。

- [プレビューと展開 (Preview and Deploy)] をクリックして、設定を展開します。

[プレビューと展開 (Preview and Deploy)] ページで、展開されるオブジェクトのリストを確認できます。

- [デバイスに移動 (Go to Devices)] をクリックします。設定を展開するオプションが提供されます。

(オプション) 移行後のタスク

- 移行結果を確認するには、FDM テンプレートに移動します。
- CDO の機能を使用して構成を最適化します。
- FDM テンプレートをデバイスに展開します。

管理アクセスインターフェイス移行による FDM 管理対象デバイスのサポート



- (注) [テンプレートの適用 (Apply Template)] 機能は、管理アクセスインターフェイスを持つターゲットデバイスではサポートされていません。ターゲット FDM による管理デバイスに適用する前に、FDM テンプレートを手動で変更します。

管理アクセスインターフェイスが設定されているターゲットデバイスに移行された FDM テンプレートを適用すると、マッピングされたインターフェイスの不一致が原因で、テンプレートの適用機能が失敗します。ターゲット FDM による管理デバイスでは、管理アクセスインターフェイスの設定と対応する静的ルートを保持して、CDO との接続を確保する必要があります。したがって、接続障害を回避するには、次の手順に従って、必要な静的ルートとともに管理アクセスインターフェイスを手動で設定してから、FDM テンプレートを適用する必要があります。このセクションでは、移行を確実に成功させるために従う必要がある手順について説明します。

複数の管理アクセスインターフェイスがあり、それらのインターフェイスが正しく設定されていないか、使用されていない場合は、ターゲット FDM による管理デバイスを更新して、設定された関連する管理アクセスインターフェイスのみを維持して、未使用のインターフェイスを移行された設定で使用できるようにする必要があります。

手順

ステップ 1 データインターフェイスの IP アドレスとサブネットマスクを、管理アクセスインターフェイスと同じになるように変更して、テンプレートの物理インターフェイスを更新します。

- (注) ターゲット FDM による管理デバイスの管理アクセスインターフェイスは、FDM テンプレートの管理アクセスインターフェイスにマッピングする必要があります。FDM テンプレートの IP アドレスとサブネットマスクは、ターゲット FDM による管理デバイスの IP アドレスとサブネットマスクと同じである必要があります。

- [インベントリ (Inventory)] ページに移動します。
- [Template] タブをクリックします。
- [脅威防御 (Threat Defense)] タブをクリックし、FDM デバイステンプレートを選択します。
- [管理] ペインから [インターフェイス] を選択します。

- e) [物理インターフェイスの編集 (Editing Physical Interface)] ダイアログボックスで、[編集] をクリックします。
- f) [IPアドレス (IP Address)] および [サブネットマスク (Subnet Mask)] を入力します。
- g) [保存 (Save)] をクリックします。

ステップ 2 テンプレート設定で、管理アクセスインターフェイスとしてデータインターフェイスを追加します。

- a) [インベントリ (Inventory)] ページに移動します。
- b) [Template] タブをクリックします。
- c) [脅威防御 (Threat Defense)] タブをクリックし、FDM デバイステンプレートを選択します。
- d) [管理] ペインの右側にある [設定] に移動します。
- e) [データインターフェイス (Data Interface)] ペインで、[+] をクリックして、管理アクセスインターフェイスとしてインターフェイスを追加します。

(注) データインターフェイスに名前、状態、および IP アドレスが設定されていることを確認します。

- f) [保存 (Save)] をクリックします。

ステップ 3 デバイスに関連付けられたインターフェイスで静的ルートを追加または更新します。管理アクセスインターフェイスを追加のインターフェイスにマッピングする場合は、選択した FDM による管理デバイスのルーティング設定を設定します。

静的ルートの追加または更新の詳細については、『[Configure Static for Threat Devices](#)』を参照してください。

後で移行を適用

手順

ステップ 1 [後で移行を適用 (Apply Migration Later)] を選択します。

移行テンプレートが保存されます。作成したテンプレートを保存し、そのテンプレートを後で FDM 管理対象デバイスに適用できます。

(注) [インベントリ (Inventory)] ページから FDM テンプレートにアクセスできます。

FDM テンプレートが正常に保存されると、次のアクションを実行できます。

- 移行結果を確認するには、FDM テンプレートに移動します。
- CDO 機能を使用して FDM テンプレートを最適化します。
- 移行元 FDM 管理対象デバイスに移動し、適用する必要がある FDM テンプレートを選択します。
- FDM テンプレートをデバイスに展開します。

ステップ 2 [完了 (Done)] をクリックします。

[インベントリ (Inventory)] ページに、事前を選択された FDM テンプレートが表示されます。CDO を使用すると、ポリシーや構成のレビューなど、テンプレートに関連するすべてのアクションを実行できます。

ステップ 3 FDM テンプレートを適用する準備ができたなら、次の手順を実行します。

1. [インベントリ (Inventory)] ページから、対象の FDM 管理対象デバイスを選択します。
2. [デバイスアクション] ペインから [テンプレートの適用 (Apply Template)] をクリックします。

[デバイスへの設定の適用 (Apply Device Configuration)] 画面が表示されます。

3. デバイスに適用する FDM テンプレートを選択します。
4. [Apply] をクリックします。

(注) デバイスで実行されている管理インターフェイス IP は変更されません。

移行アクションの表示

[移行テーブル (Migration Table)] 画面には、次の内容が表示されます。

- 移行名。デフォルトでは、CDO はデバイス名に基づいた移行名を生成します。この名前をカスタマイズすることもできます。「[\(任意\) 移行名の更新](#)」を参照してください。
- デバイスで実行された最後の移行アクティビティのタイムスタンプ。
- デバイスの移行状態を表示します。移行状態の詳細については、「[移行状態と説明](#)」を参照してください。
- 名前の変更、ログのダウンロードなど、さまざまなアクションを実行できます。アクションの詳細については、「[アクションと説明](#)」を参照してください。

表 1: 移行状態と説明

移行状態	説明
解析中 (Parsing)	移行が進行中です。
解析エラー (Parse Error)	解析は完了しましたが、エラーが発生しました。
変換エラー (Conversion Error)	変換は完了しましたが、エラーが発生しました。

移行状態	説明
テンプレートが作成されました (Template Created)	移行が完了しました。FDM テンプレートは正常に作成されましたが、検証エラーがあります。

移行エラーの修正については、「[移行エラーの修正](#)」を参照してください。

表 2: アクションと説明

アクション	説明
復帰 (Resume)	移行プロセスが停止していた手順から再開します。 たとえば、移行が完了すると、プロセスは FDM テンプレートの適用から再開します。
[名前の変更 (Rename)]	移行名の名前を変更します。
ワークフロー	ワークフロー画面を表示します。
ログをダウンロード (Download Log)	ログファイルを TXT 形式でダウンロードできます。これは解析ログです。
レポートをダウンロード (Download Report)	レポートの詳細を HTML 形式でダウンロードできます。
設定	移行が実行された ASA 設定を表示できます。
削除 (Remove)	移行ファイル、およびログファイルなどの関連ファイルを削除します。

移行フィルタについて :

別の ASA デバイスまたはモデルを選択して FDM テンプレートに移行する場合は、次のオプションのいずれかを使用します。

- [デバイスごとのフィルタ (Filter by Devices)]
- [クリアオプションでフィルタ (Filter by Clear option)]

[デバイスごとのフィルタ (Filter by Devices)]

[移行 (Migrations)] ページのさまざまなフィルタを使用して、探しているオブジェクトを見つけることができます。移行フィルタを使用すると、デバイス、状態、および時間範囲でフィルタ処理できます。

表 3: フィルタ属性と説明

フィルタ属性 (Filter Attribute)	説明
[デバイスごとのフィルタ (Filter by Devices)]	移行する特定のデバイスを選択できます。
状態	<ul style="list-style-type: none"> • [エラー (Error)]: 解析エラーに基づいて移行リストを表示します。 • [完了 (Done)]: 正常に作成された FDM テンプレートに基づいて移行リストを表示します。
時間範囲	[開始 (Start)]、[終了]: 選択した移行の開始日と終了日に基づいてデバイスのリストを表示します。

[クリアオプションでフィルタ (Filter by Clear option)]

1. フィルタバーをクリアするには、[クリア] をクリックします。
2. [+] アイコンをクリックします。
3. リストからデバイスを選択するか、名前で検索して選択します。
4. [選択 (Select)] をクリックします。
[FDM移行 (FDM Migration)] 画面が表示されます。

設定の展開

最後のステップは、デバイスに行った設定の変更の展開です。

詳細については、「[デバイス設定の展開](#)」を参照してください。

CDOでのFDM管理デバイスのさまざまな側面とそのセキュリティポリシーの管理方法については、「[Cisco Defense Orchestrator を使用した FDM デバイスの管理](#)」および「[Cisco Defense Orchestrator を使用した FDM の管理](#)」を参照してください。



付録 **A**

テレメトリ

- [Cisco Success Network](#) (27 ページ)

Cisco Success Network



(注) CDO は Cisco Success Network 設定を管理しません。Device Manager ユーザーインターフェイスで、設定を管理し、テレメトリ情報を確認します。

Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、デバイスと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。

詳細については、「[Cisco Success Network : テレメトリデータ](#)」を参照してください。



付録 **B**

FAQ

- ・ [トラブルシューティングの FAQ \(29 ページ\)](#)

トラブルシューティングの FAQ

- Q.** 解析に時間がかかるのはなぜですか。
- A.** ASA 構成ファイルのサイズが大きいと、解析に時間がかかります。ASA の実行構成ファイルは、4.5 MB および 22,000 行未満である必要があります。詳細については、「[ASA 実行設定サイズを確認する](#)」を参照してください。
- Q.** 移行中に解析エラーが発生した場合は、どうすればいいですか。
- A.** エラーの詳細については、[移行レポートのレビュー (Review Migration Report)] と [移行ログのレビュー (Review Migration Log)] を参照してください。
- Q.** 移行中に解析エラーが発生しました。これらを修正するには、どうすればいいですか。
- A.** [移行 (Migration)] ページに移動し、特定のデバイスについて [ログのダウンロード (Download Logs)] をクリックしてエラーを修正します。
- Q.** FDM テンプレートの生成中に変換エラーが発生しました。どうすればいいですか。
- A.** [移行 (Migration)] ページに移動し、特定のデバイスについて [ワークフロー (Workflows)] をクリックしてエラーを確認します。
- Q.** FDM テンプレートの作成時にエラーが発生した場合は、どうすればいいですか。
- A.** FDM テンプレートの作成時に検証エラーが発生した場合は、[インベントリ (Inventory)] ページで FDM テンプレートを検索できます。[デバイスアクション (Devices Actions)] ペインで [ワークフロー (Workflows)] をクリックして、エラーの詳細を確認してください。
- Q.** CDO が変更ログへの書き込みに失敗します。どうしてですか。
- A.** ASA を CDO に導入準備すると、CDO は、そのデータベースに ASA の実行構成ファイルのコピーを保存します。一般に、その実行構成ファイルが大きすぎる (4.5 MB 以上) 場合、含まれる行が多すぎる (約 22,000 行) 場合、または単一のアクセスグループのアクセスリストエントリが多すぎる場合、CDO は、そのデバイスを予測どおりに管理できません。詳細については、「[ASA 実行設定サイズを確認する](#)」を参照してください。

また、シスコのアカウントチームに連絡して、セキュリティポリシーを中断することなく構成ファイルのサイズを安全に削減するための支援を得ることもできます。

- Q.** CDO は、移行前に ASA 構成ファイルの構文を検証しますか。
- A.** いいえ。CDO は、ASA 構成ファイルを FDM テンプレートに移行する前に、その構文を検証しません。CDO に導入準備した ASA モデルを移行しようとして失敗した場合は、FDM 移行画面で移行レポートと移行ログを確認してください。構成ファイルの構文を検証する必要がある場合があります。
- Q.** アクセスリストとネットワークオブジェクトの一部が移行されなかったのはなぜですか？
- A.** CDO は、参照されたオブジェクトのみを移行します。アクセス制御リスト内で、定義されているがアクセスグループに参照されていないオブジェクトは移行されません。さらに、CDO が特定の要素の移行に失敗する一般的な理由には、次の 1 つ以上が当てはまる場合があります。
- ICMP コードのない ICMP アクセスリスト
 - TCP/UDP アクセスリストにアクセスグループが設定されていない
 - IP アクセスリストがサイト間 VPN プロファイルにマップされていない
 - アクセスリストを参照するネットワークオブジェクトまたはグループのいずれかが移行されていない
 - インターフェイスがシャットダウンとして参照される

移行されていない要素の詳細については、「移行レポート」を参照してください。

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。