GPO を使用した VXLAN ファブリックのマイクロセグメンテーション

初版：2023 年 12 月 14 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。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

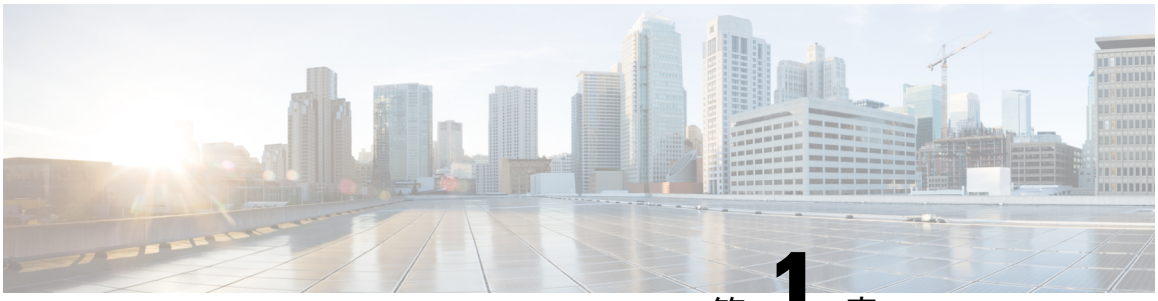
このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



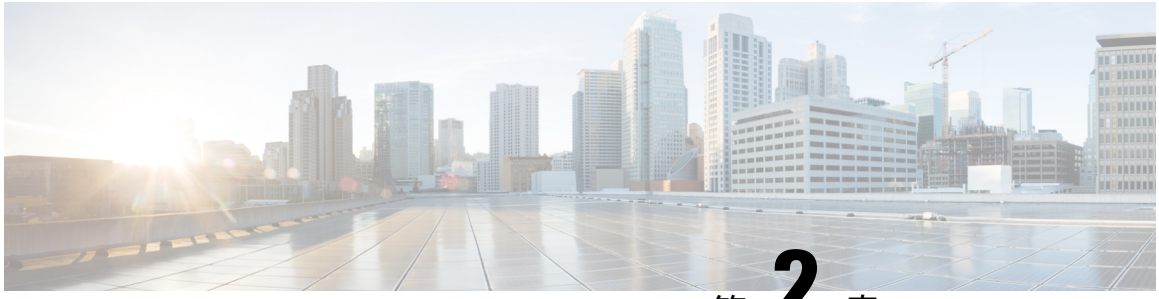
第 1 章

新機能および変更された機能に関する情報

新機能と更新情報

表 *1* : 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
グループ ポリシー オプションを使用した VXLAN ファブリックのマイクロセグメンテーション	グループ ポリシー オプション機能を使用した VXLAN ファブリックのマイクロセグメンテーションの追加	10.4(2)F	GPO を使用した VXLAN ファブリックのマイクロセグメンテーションの構成 （3 ページ）



第 2 章

GPO を使用した VXLAN ファブリックのマイクロセグメンテーションの構成

概要

従来のデータセンター環境では、アプリケーションまたはワークロードのセキュリティは、外部のデータセンターファブリックからのユーザーが入る境界または南北境界に実装されることがよくあります。これは、多くの場合、境界ファイアウォールやその他のセキュリティ検査デバイスを使用して実装されます。ただし、このアプローチは、最近の攻撃の高度な性質に対しては効果的ではありません。攻撃対象領域は、East-West および North-South フローを含むデータセンター全体に及ぶ。

セキュリティ グループおよびセキュリティ グループ ACL でマイクロセグメンテーションを使用すると、この機能は NX-OS プラットフォームのユーザーに効果的なソリューションを提供できます。マイクロセグメンテーションを使用すると、組織は、アプリケーションがネットワーク内のどこに常駐するかに関係なく、アプリケーション ワークロードの通信方法を指定するアプリケーション固有のポリシーを提供できます。

グループ ポリシー オプション（GPO）が有効になっている VXLAN ネットワークでは、管理者はセキュリティ グループを作成できます。これは、一意のセキュリティ グループ タグが適用されるネットワーク リソースの論理的な集合です。セキュリティ グループ タグは IP アドレスから取得されます。送信元属性から派生したタグは送信元セキュリティ グループ タグ（SGT）と呼ばれ、接続先属性から派生したタグは接続先セキュリティ グループ タグ（DGT）と呼ばれます。セキュリティ グループ間のトラフィックは、セキュリティ グループアクセス コントロール リスト（SGACL）（セキュリティ コントラクトとも呼ばれる）によって制御できます。これは、セキュリティ グループ タグによって送信元と接続先のセキュリティ グループを照合します。

GPO は VXLAN の下位互換性のある拡張機能であり、セキュリティ ポリシーを適用するために VXLAN ヘッダーにセキュリティ グループ タグを追加します。

VXLAN環境では、GPOを使用すると、管理者はアプリケーション属性などの特定の基準に基づいてポリシーを定義し、ネットワーク トポロジに関係なく、それらのポリシーをネットワーク リソースの特定のグループに適用できます。セキュリティ ポリシーを設定する場合、GPOは従来の汎用アクセス制御リスト（ACL）よりも柔軟性が高く、複雑さが軽減されます。

リーフ スイッチは、適用デバイスとして機能します。ほとんどの適用は入力であり、タグは送信元タグ情報とポリシー適用ビットの両方を伝送します。設定すると、出力の適用を回避できます。送信元タグは、ポリシー適用ビットが設定されていない場合、出力の適用に役立ちます。

GPOは、Cisco NX-OS リリース 10.4(2) 以降で使用可能です。

機能セキュリティ グループについて

VXLAN EVPN ファブリックにセキュリティグループを作成し、ネットワーク構造やその他の属性を使用してアプリケーション中心のセグメンテーションを定義できます。小規模で分離されたアプリケーション セグメントを定義することで、アプリケーション階層間およびアプリケーション間のネットワーク トラフィックのフローをより適切に制御できるマイクロセグメンテーションポリシーを展開できます。マイクロセグメンテーションにより、サービスが必要な場所にのみ適用され、アプリケーションとワークロードのセキュリティが向上し、セキュリティ体制が向上します。

マイクロセグメンテーションには、次の 2 つの主要な原則があります。

- **ESG**： エンドポイント セキュリティ グループ。属性/セレクタに基づいて分類される物理または仮想ネットワーク エンドポイントのコレクションを含む論理エンティティです。
- **SGACL**： セキュリティ グループ ACL は、L4 フィルタとともに照合にセキュリティ タグを使用する ACL です。タグは、IP、MAC、VLAN、ポート/VLAN、VM 属性から取得されます。このリリースでは、IPv4 および IPv6 セレクタに基づいてタグを取得できます。

セキュリティ グループを使用したマイクロセグメンテーションの機能は次のとおりです。

- 各セキュリティ グループは、VRF インスタンスに関連付けられます。セキュリティ グループ セレクタは、VRF インスタンス内のどのエンドポイントと外部 IP がセキュリティ グループに属するかを定義します。
- デフォルトでは、VRF は非適用モードで作成されます。つまり、SGACL コントラクトは VRF で適用されません。SGACL を使用するには、VRF モードを適用するように設定する必要があります。

  デフォルトで作成されたすべての VRF は、SGACL 適用モードを **UnEnforced**として取得します。これは、VRF で処理されるトラフィックに対して SGACL コントラクトが適用されないことを意味します。VRF で SGACL の適用を有効にするには、VRF を [強制（**Enforced**）] モードで明示的に設定する必要があります。
- 適用 VRF モードを設定する場合、デフォルトの動作を次のいずれかに定義できます。

- [拒否（Deny）]：許可リストで許可されていない限り、すべてのユニキャスト パケット フローがドロップされます。
- [許可（Permit）]：拒否リストによって拒否されない限り、すべてのユニキャスト パケット フローが許可されます。

- ESG 内のホストは、明示的な SGACL なしで自由に通信できます。VRF モードが適用されている場合、すべての ESG 間通信に SGACL が必要です。
- SGACL はセキュリティ ルールのみを作成します。ESG は、サブネット展開やルート リークなどのネットワーク展開には使用されません。

注意事項と制約事項

GPO には、次の注意事項と制限事項 があります。

- GPO には、Cisco Nexus リリース 10.4(2) 以降が必要です。
- GPO は、次のプラットフォームでのみサポートされます。
  - N9K-93180YC-FX3
  - N9K-93180YC-FX3S
  - N9K-93600CD-GX
  - N9K-9364C-GX
  - N9K-9316D-GX
  - N9K-9364D-GX2A
  - N9K-9332D-GX2B
- SGACL は VXLAN EVPN 展開のコンテキストでのみサポートされ、VRF（テナント）にのみ適用されます。
- SGACL は、単一サイト内でのみサポートされます。
- GPO には下位互換性があり、GPO 拡張機能をサポートしていない VTEP は、VXLAN ヘッダー内の関連する予約済みビットを無視します。ただし、この機能をサポートしているピアまたは有効になっているピアの GPO 拡張のみを含める方が、運用上安全で保守的です。同様に、受信側では、着信 VXLAN カプセル化パケットの GPO 関連フィールドは、GPO をサポートしていることがわかっているピアからのみ処理する必要があります。
- SGACL は BUM およびマルチキャスト トラフィックには適用されません。

GPO の構成

GPO の有効化

グループ ポリシー オプション機能を有効にするには、次の手順を実行します。

この機能を初めて有効にする場合は、ルーティング テンプレートを **system routing template-security-groups** に構成し、スイッチをリロードする必要があります。機能セキュリティ グループのその後の無効化と再有効化は、リロードなしで実行できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**system routing template-security-groups** 例： `switch(config-if)# system routing template-security-groups`	スイッチのルーティング プロファイルを変更します。 （注） この手順では、 **copy running-config startup-config** の後にリロードが必要です。
ステップ 3	**[no] feature security-group** 例： `switch(config-if)# feature security-group`	グループ ポリシー オプション（GPO）機能を有効にします。機能を無効にするには、「no」プレフィックスを使用します。GPO機能は、実行時に無効または有効にできます。

ステップ 4	**show nve peers detail**
	例：
	`switch(config-if)# show nve peers detail`
	`Details of nve Peers:`
	`----------------------------------------`
	`Peer-Ip: 1.1.1.1`
	`NVE Interface : nve1`
	`Peer State : Up`
	`Peer Uptime : 1d12h`
	`Router-Mac : 5292.ca60.1b08`
	`Peer First VNI : 101`
	`Time since Create : 1d12h`
	`Configured VNIs : 100-101,200-201`
	`Provision State : peer-add-complete`
	`Learnt CP VNIs : 100-101,200-201`
	`vni assignment mode : SYMMETRIC`
	`Peer Location : FABRIC`
	`Group policy option : yes`
	`----------------------------------------`
		グループ ポリシー オプションが有効になっていることを確認します。

次のタスク

セキュリティ グループ セレクタを構成して、グループを作成します。

セキュリティ グループの作成

セキュリティ グループを作成または更新し、メンバー選択基準を設定するには、次の手順を実行します。グループ メンバーを選択するには、次の属性を任意に組み合わせて指定できます。

- 接続されたエンドポイントと外部サブネットの IPv4 アドレスまたはサブネット。
- 接続されたエンドポイントと外部サブネットの IPv6 アドレスまたはサブネット。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**security-group** *sg-id* **name** *sg-name* 例： `switch(config)# security-group 100 name webservers`	一意の ID が *sg-id* で名前が *sg-name*であるセキュリティ グループを作成（または既存を選択）します。

ステップ 3	**[no] match** [**connected-endpoints** | **external-subnets**] **vrf** *vrf-name* [**ipv4** | **ipv6**] *ip-prefix*
	例：
	`switch(config-security-group)# match connected-endpoints vrf vrf_blue ipv4 61.1.1.141/32`
	`switch(config-security-group)# match external-subnets vrf vrf_blue ipv4 10.0.0.0/8`
	`switch(config-security-group)# match connected-endpoints vrf vrf_blue ipv6 61:1:1:2:1::141/128`
	`switch(config-security-group)# match external-subnets vrf vrf_blue ipv6 10:11:12:13::/64`
		このコマンドは、ホスト（接続されたエンドポイント）または外部（外部サブネット）リソースの IPv4-VRF または IPv6-VRF セレクタです。
		機能を無効にするには、「no」プレフィックスを使用します。

ステップ 4	**show security-group id** *sg-id*
	例：
	`switch(config-if)# show security-group id 100`
	`Security Group ID 100 , Name 100`
	`  Selector Type : External IPv4 Selector`
	`    VRF-Name  IPv4-Address/mask-len`
	`    blue  10.1.1.3/32`
	`    blue  10.1.1.4/32`
	`  Selector Type : Host IPv4 Selector`
		グループ ポリシー セレクタを確認します。

	コマンドまたはアクション	目的
	VRF-Name IPv4-Address/mask-len blue 10.1.1.3/32 blue 10.1.1.4/32	

クラス マップの作成

クラス マップを作成するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **class-map type security match-any** *web-class* **match ip**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**class-map type security match-any** *web-class* **match ip**
	例：
	`switch# class-map type security match-any web-class2`
	`  match ipv4 udp sport 399 to 402 dport 400 to 403`
	`  match ipv6 udp sport 399 to 402 dport 400 to 403`
		クラス マップを作成します。

ポリシー マップの作成

ポリシー マップを作成するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **policy-map type security** *policy-map* **class web-class [permit | deny]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**policy-map type security** *policy-map* **class web-class [permit | deny]**	ポリシー マップを作成します。

セキュリティ グループを使用したセキュリティ コントラクトの構成

この手順では、セキュリティ グループを適用する SGACL（コントラクト）を作成します。

始める前に

セキュリティ グループを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* 例： `switch(config)# vrf context blue`	指定した VRF の構成モードを開始します。
ステップ 3	**security enforce tag** *sg-id* **default** [**permit** | **deny**] 例： `switch(config-vrf)# security enforce tag 100 default deny`	VRF の強制を有効にします。
ステップ 4	**security contract source** [*sg-id* | *any*] **destination** [*sg-id* | *any*] **policy policy-map-name** [*bidir* | *unidir*] 例： `switch(config-vrf)# security contract source 100 destination 200 policy policyMap1 bidir`	指定したセキュリティ グループの強制を有効にします。

GPO の構成例

次に、GPO 構成に関連するいくつかの show コマンドを示します。

- **次の show コマンドは、セキュリティ グループを構成する方法を示しています。**

```
switch(config)show security-group id 1000
Security Group ID 1000 , Name webservers
  Selector Type : External IPv4 Subnets
    VRF-Name                          IPv4-Address/mask-len
    vrf_blue                          10.0.0.0/8
  Selector Type : Connected IPv4 Endpoints
```

```
    VRF-Name                          IPv4-Address/mask-len
    vrf_blue                          61.1.1.141/32
  Selector Type : External IPv6 Subnets
    VRF-Name                          IPv6-Address/mask-len
    vrf_blue                          10:11:12:13::/64
  Selector Type : Connected IPv6 Endpoints
    VRF-Name                          IPv6-Address/mask-len
    vrf_blue                          61:1:1:2:1::141/128  switch(config)
switch(config)

switch(config)# show security-group vrf vrf_blue ipv4
Security Group ID 1000 , Name webservers
  Selector Type : External IPv4 Subnets
    VRF-Name                          IPv4-Address/mask-len
    vrf_blue                          10.0.0.0/8
  Selector Type : Connected IPv4 Endpoints
    VRF-Name                          IPv4-Address/mask-len
    vrf_blue                          61.1.1.141/32
switch(config)

switch(config)# show security-group vrf vrf_blue ipv6
Security Group ID 1000 , Name webservers
  Selector Type : External IPv6 Subnets
    VRF-Name                          IPv6-Address/mask-len
    vrf_blue                          10:11:12:13::/64
  Selector Type : Connected IPv6 Endpoints
    VRF-Name                          IPv6-Address/mask-len
    vrf_blue                          61:1:1:2:1::141/128
switch(config)#

switch(config)#  show security-group name webservers
Security Group ID 1000 , Name webservers
  Selector Type : External IPv4 Subnets
    VRF-Name                          IPv4-Address/mask-len
    vrf_blue                          10.0.0.0/8
  Selector Type : Connected IPv4 Endpoints
    VRF-Name                          IPv4-Address/mask-len
    vrf_blue                          61.1.1.141/32
  Selector Type : External IPv6 Subnets
    VRF-Name                          IPv6-Address/mask-len
    vrf_blue                          10:11:12:13::/64
  Selector Type : Connected IPv6 Endpoints
    VRF-Name                          IPv6-Address/mask-len
    vrf_blue                          61:1:1:2:1::141/128
switch(config)#
```

- 次の **show** コマンドは、セキュリティ契約関連の情報を表示します。

```
switch(config)# show contracts

VRF              SGT   DGT   Policy           Dir    Stats        Class
Action       OperSt
-------------------------------------------------------------------------------------------
blue             1000  200   policyMap1       bidir  0            web-class1
permit       enabled
switch(config)

switch(config) show contracts sgt 1000

VRF              SGT   DGT   Policy           Dir    Stats        Class
Action       OperSt
-------------------------------------------------------------------------------------------
blue             1000  200   policyMap1       bidir  0            web-class1
permit       enabled
switch(config)
```

```
switch(config)  sh contracts dgt 2000

VRF              SGT   DGT   Policy           Dir    Stats        Class
Action       OperSt
-------------------------------------------------------------------------------------------------
vrf_blue         1000  2000  policyMap1       bidir  0            web-class1
permit       enabled
switch(config)


switch(config)# show contracts detail

VRF: blue
  Contract source group 1000 dest group 200
    Policy: policyMap1 Direction: bidir
      Stats: 0
      Class: web-class1
        match ip
      Action: permit
      OperSt: enabled
switch(config)

switch(config)show contracts policy policyMap1

VRF              SGT   DGT   Policy           Dir    Stats        Class
Action       OperSt
-------------------------------------------------------------------------------------------------
blue             1000  200   policyMap1       bidir  0            web-class1
permit       enabled
switch(config)

switch(config)show contracts vrf vrf_blue

VRF              SGT   DGT   Policy           Dir    Stats        Class
Action       OperSt
-------------------------------------------------------------------------------------------------
vrf_blue         1000  200   policyMap1       bidir  0            web-class1
permit       enabled
switch(config)
```

```
switch(config)# show run security-group

!Command: show running-config security-group
!Running configuration last done at: Fri Dec  8 12:23:52 2023
!Time: Fri Dec  8 12:27:09 2023

version 10.4(2) Bios:version 05.50
feature security-group

security-group 1000 name webservers
  match external-subnets vrf vrf_blue ipv4 10.0.0.0/8
  match external-subnets vrf vrf_blue ipv6 10:11:12:13::/64
  match connected-endpoints vrf vrf_blue ipv4 61.1.1.141/32
  match connected-endpoints vrf vrf_blue ipv6 61:1:1:2:1::141/128
class-map type security match-any web-class1
  match ip
class-map type security match-any web-class2
  match ipv4 udp sport 399 to 402 dport 400 to 403


 match ipv6 udp sport 399 to 402 dport 400 to 403
policy-map type security policyMap1
  class web-class1
```

```
vrf context vrf_blue
  security contract source 1000 destination 2000 policy policyMap1
  security enforce tag 100 default deny

switch(config)
```

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。