



IGMP スヌーピングの構成

この章では、Cisco Nexus 3600 プラットフォーム スイッチにインターネット グループ管理プロトコル (IGMP) スヌーピングを構成する方法を説明します。

この章は、次の項で構成されています。

- [IGMP スヌーピングの情報 \(1 ページ\)](#)
- [IGMP スヌーピングに関する注意事項と制限事項 \(4 ページ\)](#)
- [IGMP スヌーピングのデフォルト設定 \(5 ページ\)](#)
- [IGMP スヌーピング パラメータの設定 \(6 ページ\)](#)
- [IGMP スヌーピング設定の確認 \(14 ページ\)](#)
- [マルチキャスト ルートの間隔を設定 \(15 ページ\)](#)
- [IGMP スヌーピング統計情報の表示 \(15 ページ\)](#)
- [IGMP スヌーピングの設定例 \(15 ページ\)](#)

IGMP スヌーピングの情報

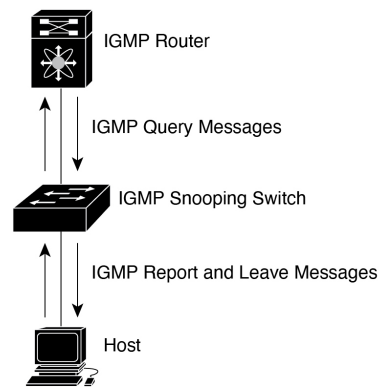


- (注) スイッチでは、IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、スイッチで不正なフラッドイングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

インターネットグループ管理プロトコル (IGMP) スヌーピングソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャストトラフィックを調査し、関係する受信機が常駐するポートを発見します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッドイングを回避します。IGMP スヌーピング機能は、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバーシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピングソフトウェアが応答します。デフォルトでは、IGMP スヌーピングがスイッチでイネーブルにされています。

次の図では、ホストと IGMP ルータ間にある IGMP スヌーピング スイッチを示します。IGMP スヌーピング スイッチは、IGMP メンバーシップ レポートおよび Leave メッセージをスヌーピングして、必要な場合にだけ接続された IGMP ルータに転送します。

図 1: IGMP スヌーピング スイッチ



IGMP スヌーピング ソフトウェアは、IGMPv1、IGMPv2、および IGMPv3 コントロールプレーン パケットの処理に関与し、レイヤ 3 コントロールプレーン パケットを代行受信して、レイヤ 2 の転送処理を操作します。

IGMP の詳細については、「[IGMP の設定](#)」を参照してください。

Cisco NX-OS IGMP スヌーピング ソフトウェアには、次のような独自の機能があります。

- 送信元フィルタリングにより、宛先および送信元の IP アドレスに基づいて、マルチキャスト パケットを転送できます。
- MAC アドレスでなく、IP アドレスに基づいてマルチキャスト転送を実行します。
- Optimized Multicast Flooding (OMF) により、未知のトラフィックをルータだけに転送して、データに基づくステート作成を行いません。

IGMP スヌーピングの詳細については、「[RFC 4541](#)」を参照してください。

このセクションは、次のトピックで構成されています。

IGMPv1 および IGMPv2

IGMPv1 および IGMPv2 は、メンバーシップ レポートの抑制機能をサポートしています。つまり、同じサブネットに属する 2 つのホストが、同じグループのマルチキャスト データを要求している場合、一方のホストからメンバー レポートを受信した他方のホストで、レポートの送信が抑制されます。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリーメッセージがホストに送信されません。ソフトウェアは IGMP Leave メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP Leave メッセージが存在しないため、特定のグループについてマルチキャストデータを要求するホストが存続しないことを示すために、メンバーシップメッセージ タイムアウトが利用されます。



- (注) 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、最終メンバーのクエリー インターバル設定が無視されます。

IGMPv3

Cisco NX-OS にはフル機能の IGMPv3 スヌーピングが実装されており、IGMPv3 レポートに含まれる (S、G) 情報に基づいて、フラッドイングを制御することができます。この発信元をベースとするフィルタリングにより、マルチキャストグループにトラフィックを送信する発信元に基づくポートのセットにマルチキャストトラフィックを制限するようにスイッチがイネーブルにされます。

ソフトウェアのデフォルト設定では、各 VLAN ポートに接続されたホストが追跡されます。この明示的なトラッキング機能は、高速脱退メカニズムをサポートしています。すべての IGMPv3 ホストがメンバーシップレポートを送信するため、レポート抑制は、スイッチにより他のマルチキャスト対応ルータに送信されるトラフィックの量を制限します。レポート抑制をイネーブルにすると、過去にいずれの IGMPv1 ホストまたは IGMPv2 ホストからも対象のグループへの要求がなかった場合には、プロキシ レポートが作成されます。プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

IGMPv3 メンバーシップ レポートには LAN セグメント上のグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、メンバーシップクエリーが送信されます。最終メンバーのクエリーインターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合に、グループ ステートが解除されます。

IGMPスヌーピングクエリア

マルチキャスト トラフィックをルーティングする必要がないために、Protocol-Independent Multicast (PIM) がインターフェイス上でディセーブルになっている場合は、メンバーシップクエリーを送信するように IGMP スヌーピングクエリアを設定する必要があります。このクエリアは、マルチキャスト送信元と受信者を含み、その他のアクティブ クエリアを含まない VLAN で定義します。

IGMP スヌーピングクエリアがイネーブルの場合、スイッチは定期的にクエリーを送信します（構成されたクエリア アドレスの送信元アドレスを使用します）。これらのクエリーは、IP マルチキャスト トラフィックを受信するホストからの IGMP レポート メッセージをトリガーします。

ルータ ポートでの IGMP フィルタ処理

IGMP フィルタ処理を使用すると、スイッチをレイヤ 3 マルチキャスト スイッチに接続するルータポートをスイッチに構成できます。スイッチは、手動で構成されたすべてのスタティック ルータ ポートをルータ ポート リストに保存します。

IGMP パケットを受信すると、スイッチは VLAN 内のルータ ポートを介してトラフィックを転送します。スイッチは、PIM hello メッセージまたはスイッチが受信した IGMP クエリーを介して、ポートをルータ ポートとして認識します。

IGMP スヌーピングに関する注意事項と制限事項

IGMP スヌーピングに関する注意事項および制約事項は次のとおりです。

- Cisco Nexus 3600 プラットフォーム スイッチは、IPv4 の IGMP スヌーピングのみをサポートします。
- Cisco Nexus 3600 プラットフォーム スイッチは、vPC を使用した IGMP スヌーピングをサポートします。
- IGMP スヌーピング構成は、vPC ペアの両方の vPC ピアで同一である必要があります。両方の vPC ピアで IGMP スヌーピングを有効または無効にします。



(注) 両方の vPC ピアで IGMP スヌーピングを有効または無効にすると、異なる MVR 送信元 VLAN から同じ MVR 受信者 VLAN への IGMP クエリーの転送も有効になります。結果の IGMP クエリーは、異なるバージョンとクエリー間隔でクエリーを送信する場合があります。Cisco NX-OS リリース 7.0 (3) I3 (1) より前の動作を維持する場合は、**mvr-suppress-query** コマンドを使用します。IGMP 一般クエリー転送の抑制の詳細については、「[VLAN からの IGMP クエリー転送の抑制](#)」を参照してください。

- Cisco NX-OS リリース 7.0 (3) I3 (1) より前のリリースで、vPC ピアを構成している場合、2 台のデバイス間の IGMP スヌーピング構成オプションに相違があると、次のような結果になります。
 - 一方のデバイスで IGMP スヌーピングを有効にして、他方で無効にすると、スヌーピングが無効であるデバイスではすべてのマルチキャストトラフィックがフラッドイングします。
 - マルチキャスト ルータまたはスタティック グループの設定の相違は、トラフィック損失の原因になり得ます。
 - 高速脱退、明示的な追跡、およびレポート抑制のオプションをトラフィックの転送に使用する場合、これらのオプションに相違が生じる可能性があります。

- デバイス間でクエリー パラメータが異なると、一方のデバイスではマルチキャストステートが期限切れとなり、もう一方のデバイスでは転送が継続されます。この相違によって、トラフィック損失または転送の長時間化が発生します。
- IGMP スヌーピング クエリアを両方のデバイスで設定している場合、クエリーがトラフィックで確認されると、IGMP スヌーピング クエリアはシャットダウンするので、一方のクエリアだけがアクティブになります。

IGMP スヌーピングのデフォルト設定

次のテーブルでは、IGMP スヌーピング パラメータのデフォルト設定をリスト化しています。

表 1: デフォルト IGMP スヌーピング パラメータ

パラメータ	デフォルト
IGMP スヌーピング	有効
明示的な追跡	有効
高速脱退	無効
最終メンバー クエリ間隔	1 秒
スヌーピング クエリア	無効
レポート抑制	有効
リンクローカル グループ抑制	有効
スイッチ全体での IGMPv3 レポート抑制	無効
VLAN ごとの IGMPv3 レポート抑制	有効 (Enabled)



- (注)
- マルチキャスト ルータ ポートを送信元ポートとして SPAN セッションが設定されている場合、送信元ポートに実際に転送されているトラフィックがない場合でも、宛先ポートはすべてのマルチキャスト トラフィックを認識します。これは、マルチキャスト/SPAN 実装の現在の制限によるものです。
 - Cisco Nexus 3548 シリーズ スイッチは、未知のマルチキャスト トラフィックをすべての VLAN のマルチキャスト ルータ ポートに複製しますが、マルチキャスト トラフィックは 1 つの特定の VLAN で受信されます。これはデフォルトの動作であり、構成できません。

IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作に影響を与えるには、次の表に示すオプションの IGMP スヌーピング パラメータを構成します。

表 2: IGMP スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	スイッチまたは、VLAN ごとに IGMP スヌーピングを有効にします。デフォルトではイネーブルになっています。 (注) グローバル設定が無効になっている場合、すべての VLAN は、有効かどうかに関係なく無効として扱われます。
アクセス グループ	VLAN ごとに IGMP Join をフィルタ処理するポリシーを構成します。
明示的な追跡	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトではイネーブルになっています。
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリー メッセージを送信することなく、グループ ステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが 1 つしか存在しない場合に使用されます。デフォルトではディセーブルになっています。
最終メンバー クエリ間隔	IGMP クエリーの送信後に待機する時間を設定します。この時間が経過すると、ソフトウェアは、特定のマルチキャスト グループについてネットワーク セグメント上に受信要求を行うホストが存在しないと見なします。いずれのホストからも応答がないまま、最終メンバーのクエリ インターバルの期限が切れると、対応する VLAN ポートからグループが削除されます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。

パラメータ	説明
プロキシ脱退メッセージ	プロキシ脱退メッセージの宛先アドレスを、脱退するグループのアドレスに変更します。 通常、IGMP スヌーピング モジュールによって生成される IGMP プロキシ脱退メッセージは、すべてのホストがグループを脱退するとき、224.0.0.2 マルチキャストルータアドレスを使用します。マルチキャストアプリケーションがレポートの受信に依存し、パケットの宛先アドレスに基づいてマルチキャストトラフィックを開始または停止するメッセージを残す場合は、この構成を実装する必要があります。
レポートをフラッドして脱退	VLAN のすべてのアクティブ インターフェイスまたは特定のインターフェイスのみでIGMP レポートをフラッドします。そして、脱退します。 IGMP レポートは、通常、IGMP スヌーピング モジュールによって検出されるとマルチキャストルータ ポートに転送されるので、VLAN でフラッディングされません。ただし、このコマンドを実行すると、スイッチはマルチキャストルータ ポートに加えて、VLAN に属するカスタム ポートにも IGMP レポートを送信します。マルチキャストアプリケーションがトラフィックを送信するために IGMP レポートを表示する機能を必要とする場合は、この構成を実装する必要があります。
スヌーピング クエリア	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、インターフェイスにスヌーピング クエリアを設定します。
レポート抑制	スイッチまたは、VLAN ごとにマルチキャスト対応ルータに送信されるメンバーシップ レポートトラフィックを制限します。レポート抑制をディセーブルにすると、すべてのIGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。

パラメータ	説明
マルチキャスト ルータ	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。
スタティック グループ	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。
リンクローカル グループ抑制	スイッチまたは各VLANに対して、リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。
IGMPv3 レポート抑制	スイッチまたは、VLAN ごとに IGMPv3 レポート抑制およびプロキシレポートを構成します。デフォルトでは、スイッチ全体で無効になっており、VLAN ごとに有効になっています。

手順の概要

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan configuration *vlan-id***
- 4.
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	ip igmp snooping 例 : <pre>switch(config)# ip igmp snooping</pre>	デバイスの IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 (注) このコマンドの no 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピング

	コマンドまたはアクション	目的				
		グがディセーブルになります。 IGMP スヌーピングをディセーブルにすると、レイヤ2マルチキャスト フレームがすべてのモジュールにフラッディングします。				
ステップ 3	vlan configuration <i>vlan-id</i> 例： switch(config)# vlan configuration 100 switch(config-vlan-config)#	VLAN を構成し、VLAN コンフィギュレーションモードを開始します。				
ステップ 4	<table><tr><th>オプション</th><th>説明</th></tr><tr><td>コマンド</td><td>目的</td></tr></table>	オプション	説明	コマンド	目的	
	オプション	説明				
	コマンド	目的				
	ip igmp snooping 例： switch(config-vlan-config)# ip igmp snooping	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。				
	ip igmp snooping access-group route-map-name 例： switch(config-vlan-config)# ip igmp snooping access-group rmap	VLAN ごとに IGMP Join をフィルタ処理するポリシーを構成します。デフォルトではディセーブルになっています。				
	ip igmp snooping explicit-tracking 例： switch(config-vlan-config)# ip igmp snooping explicit-tracking	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。				
ip igmp snooping fast-leave 例： switch(config-vlan-config)# ip igmp snooping fast-leave	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない					

コマンドまたはアクション		目的
オプション	説明	
	IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。	
ip igmp snooping last-member-query-interval seconds 例 : <pre>switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3</pre>	いずれのホストからも IGMP クエリー メッセージへの応答がないまま、最終メンバのクエリー インターバルの期限が切れた場合に、関連する VLAN ポートからグループを削除します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。	
[no] ip igmp snooping proxy-leave use-group-address 例 : <pre>switch(config-vlan-config)# ip igmp snooping proxy-leave use-group-address</pre>	プロキシ脱退メッセージの宛先アドレスを、脱退するグループのアドレスに変更します。 通常、IGMP スヌーピング モジュールによって生成される IGMP プロキシ脱退メッセージは、すべてのホストがグループを脱退するとき、224.0.0.2 マルチキャストルータア	

コマンドまたはアクション		目的
オプション	説明	
	ドレスを使用します。マルチキャストアプリケーションがレポートの受信に依存し、パケットの宛先アドレスに基づいてマルチキャストトラフィックを開始または停止するメッセージを残す場合は、この構成を実装する必要があります。	
[no] ip igmp snooping report-flood { all interface ethernet slot/port } 例 : <pre>switch(config-vlan-config)# ip igmp snooping report-flood interface ethernet 1/2 ip igmp snooping report-flood interface ethernet 1/3</pre>	VLAN のすべてのアクティブ インターフェイスまたは特定のインターフェイスのみで IGMP レポートをフラッドします。そして、脱退します。 IGMP レポートは、通常、IGMP スヌーピング モジュールによって検出されるとマルチキャスト ルータ ポートに転送されるので、VLAN でフラッディングされません。ただし、このコマンドを実行すると、スイッチはマルチキャスト ルータ ポートに加えて、VLAN に属するカスタム ポートにも IGMP レポートを送信しま	

コマンドまたはアクション		目的
オプション	説明	
	す。マルチキャストアプリケーションがトラフィックを送信するためにIGMP レポートを表示する機能が必要な場合は、この構成を実装する必要があります。	
ip igmp snooping querier ip-address 例 : <pre>switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106</pre>	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリアを設定します。IP アドレスは、メッセージの送信元として使用します。	
ip igmp snooping report-suppression 例 : <pre>switch(config-vlan-config)# ip igmp snooping report-suppression</pre>	マルチキャスト対応ルータに送信されるメンバシップ レポートトラフィックを制限します。レポート抑制をディセーブルにすると、すべてのIGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。 (注) グローバル コンフィギュレーションモードでこのコ	

コマンドまたはアクション		目的
オプション	説明	
	マンドを実行し、すべてのインターフェイスを変更することもできます。	
ip igmp snooping mrouter interface interface 例 : <pre>switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1</pre>	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。 ethernet slot/port のように、インターフェイスはタイプおよび番号で指定できます。	
ip igmp snooping static-group group-ip-addr [source source-ip-addr] interface interface 例 : <pre>switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1</pre>	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。 ethernet slot/port のように、インターフェイスはタイプおよび番号で指定できます。	
ip igmp snooping link-local-groups-suppression 例 : <pre>switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression</pre>	リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。 (注) グローバル コンフィギュレーションモードでこのコマンドを実行し、	

コマンドまたはアクション		目的
オプション	説明	
	すべてのインターフェイスを変更することもできます。	
ip igmp snooping v3-report-suppression 例 : <pre>switch(config-vlan-config)# ip igmp snooping v3-report-suppression</pre>		IGMPv3 レポート抑制およびプロキシレポートを設定します。デフォルトでは、スイッチ全体のグローバルコマンドでディセーブルになっており、VLAN ごとにイネーブルになっています。 (注) グローバル コンフィギュレーションモードでこのコマンドを実行し、すべてのインターフェイスを変更することもできます。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	設定変更を保存します。

IGMP スヌーピング設定の確認

IGMP スヌーピングの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip igmp snooping [vlan vlan-id]	IGMP スヌーピング設定を VLAN 別に表示します。

コマンド	目的
show ip igmp snooping groups [source [group] group [source]] [vlan vlan-id] [detail]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping querier [vlan vlan-id]	IGMP スヌーピング クエリアを VLAN 別に表示します。
show ip igmp snooping mroute [vlan vlan-id]	マルチキャスト ルータ ポートを VLAN 別に表示します。
show ip igmp snooping explicit-tracking [vlan vlan-id]	IGMP スヌーピングの明示的な追跡情報を VLAN 別に表示します。

マルチキャスト ルートの間隔を設定

スイッチのマルチキャスト ルートの作成または削除のレートが高い場合（たとえば、IGMP 加入要求または脱退要求が多すぎる場合）、スイッチは要求が行われるのと同じ速さでマルチキャスト ルートをハードウェアにプログラムできません。この問題を解決するには、マルチキャスト ルートがハードウェアにプログラムされるまでの間隔を設定します。

1 秒あたりのマルチキャスト ルートの作成または削除が非常に少ない場合は、低い間隔（最大 50 ミリ秒）を設定します。間隔を小さくすると、デフォルトの間隔である 1 秒を使用する場合よりも高速にハードウェアをプログラムできます。

1 秒あたりのマルチキャスト ルートの作成数または削除数が非常に多い場合は、間隔を高く構成します（最大 2 秒）。間隔を長くすると、要求をドロップすることなく、ハードウェアをより長い期間にわたってプログラムできます。

IGMP スヌーピング統計情報の表示

IGMP スヌーピング統計情報を表示するには、**show ip igmp snooping statistics vlan** コマンドを使用します。この出力で、仮想ポート チャンネル（vPC）の統計情報を確認できます。

IGMP スヌーピング統計情報をクリアするには、**clear ip igmp snooping statistics vlan** コマンドを使用します。

IGMP スヌーピングの設定例

次に、IGMP スヌーピング パラメータの設定例を示します。

```
configure terminal
ip igmp snooping
vlan 2
ip igmp snooping
ip igmp snooping explicit-tracking
```

```
ip igmp snooping fast-leave
ip igmp snooping last-member-query-interval 3
ip igmp snooping querier 172.20.52.106
ip igmp snooping report-suppression
ip igmp snooping mrouter interface ethernet 2/1
ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
ip igmp snooping link-local-groups-suppression
ip igmp snooping v3-report-suppression
```

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。