ドメイン

次のトピックでは、ドメインを使用してマルチテナンシーを管理する方法について説明します。

- ドメインを使用したマルチテナンシーの概要 （1 ページ）
- ドメインの要件と前提条件 （5 ページ）
- ドメインの管理 （5 ページ）
- 新しいドメインの作成 （6 ページ）
- ドメイン間のデータの移動 （7 ページ）
- ドメイン間のデバイスの移動 （8 ページ）
- ドメイン管理の履歴 （12 ページ）

ドメインを使用したマルチテナンシーの概要

Firewall Management Center では、ドメインを使用したマルチテナンシーを実装できます。ドメインは、管理対象デバイス、構成、およびイベントへのユーザーアクセスをセグメント化します。最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 のサブドメインを作成できます。

Firewall Management Center にログインすると、現在のドメインと呼ばれる単一ドメインにログインします。ユーザアカウントによっては、他のドメインに切り替えることができる場合があります。

ユーザーロールによる制限に加えて、現在のドメインレベルによってさまざまな設定の変更が制限される場合もあります。Firewall Management Center では、システムソフトウェア更新などのほとんどの管理タスクは、グローバルドメインに制限されます。

Firewall Management Center では、その他のタスクは、サブドメインがないドメインであるリーフドメインに制限されます。たとえば、各管理対象デバイスをリーフ ドメインと関連付け、そのリーフ ドメインのコンテキストからデバイス管理タスクを実行する必要があります。各デバイスは単一のドメインにのみ属することができることに注意してください。

各リーフ ドメインは、そのリーフ ドメインのデバイスで集められた検出データに基づいて独自のネットワーク マップを作成します。管理対象デバイスによって報告されたイベント（接続、侵入、マルウェアなど）もデバイスのリーフ ドメインに関連付けられます。

1 ドメイン レベル：グローバル

マルチテナンシーを設定しない場合、すべてのデバイス、構成、およびイベントはグローバル ドメインに属します。グローバル ドメインは、このシナリオの場合はリーフ ドメインでもあります。ドメイン管理を除き、サブドメインを追加するまでは、ドメイン固有の構成および分析オプションは非表示になります。

2 ドメイン レベル：グローバル、セカンドレベル

2 レベルのマルチドメイン展開では、グローバル ドメインには直接の子孫ドメインのみがあります。たとえば、マネージドセキュリティ サービス プロバイダー（MSSP）は、1 つの Firewall Management Center を使用して複数の顧客のネットワーク セキュリティを管理できます。

- グローバルドメインにログインしている MSSP の管理者は、顧客の展開を表示または編集することはできません。顧客の展開を管理するには、それぞれのセカンドレベルの指定されたサブドメインにログインする必要があります。
- 各顧客の管理者は、サブドメインと呼ばれるセカンドレベルにログインして、その組織に適用されるデバイス、構成、およびイベントのみを管理できます。これらのローカル管理者は、MSSP の他の顧客の展開を表示したり、その環境に影響を与えることはできません。

3 ドメイン レベル：グローバル、セカンドレベル、サードレベル

3 レベルのマルチドメイン展開では、グローバル ドメインにはサブドメインがあり、そのうち少なくとも 1 つに独自のサブドメインがあります。前の例を拡張するには、MSSP 顧客（すでにサブドメインに制限されている）がその展開をさらにセグメント化しようとしているシナリオを考えてみます。この顧客は、2 つのクラスのデバイス（ネットワーク エッジに配置されているデバイスと内部に配置されているデバイス）を個別に管理しようとしています。

- セカンドレベルサブドメインにログインしている顧客の管理者は、顧客のエッジネットワークの展開を表示または編集することはできません。ネットワークエッジで展開されたデバイスを管理するには、それぞれのリーフドメインにログインする必要があります。
- 顧客のエッジ ネットワークの管理者は、サードレベル（リーフ）ドメインにログインして、ネットワーク エッジに展開されているデバイスに適用されるデバイス、構成、およびイベントのみを管理できます。同様に、顧客の内部ネットワークの管理者は、別のサードレベル ドメインにログインして、内部のデバイス、構成、およびイベントを管理できます。エッジと内部の管理者は、互いの展開を表示できません。

（注） マルチテナントを使用する Firewall Management Center では、SSO 設定により、SAML ユーザーを特定のサブドメインに割り当てることができます。これは、グローバル ドメイン レベルでのみ設定できます。

関連トピック

SAML シングルサインオンの設定

ドメインの用語

このマニュアルでは、ドメインおよびマルチドメイン展開を説明する際に次の用語を使用します。

グローバル ドメイン

マルチドメイン展開でのトップレベル ドメイン。マルチテナンシーを設定しない場合、すべてのデバイス、設定、およびイベントはグローバル ドメインに属します。グローバル ドメインの Administrators は、Cisco Secure Firewall システム全体の導入を管理できます。

サブドメイン

第 2 または第 3 レベルのドメイン。

第 2 レベル ドメイン

グローバル ドメインの子。第 2 レベル ドメインは、リーフ ドメインにするか、サブドメインを持つことができます。

第 3 レベル ドメイン

第 2 レベル ドメインの子。第 3 レベル ドメインは常にリーフ ドメインです。

リーフ ドメイン

サブドメインを持たないドメイン。各デバイスはリーフ ドメインに属している必要があります。

子孫ドメイン

階層の現在のドメインから下のドメイン。

子ドメイン

ドメインの直接子孫。

先祖ドメイン

現在のドメインより上にある同じ系統のドメイン。

親ドメイン

ドメインの直接先祖。

兄弟ドメイン

同じ親を持つドメイン。

現在のドメイン

現在ログインしているドメイン。システムでは、Webインターフェイスの右上のユーザ名の前に現在のドメイン名が表示されます。ユーザー ロールが制限されている場合を除き、現在のドメインの設定を編集できます。

ドメインのプロパティ

ドメインのプロパティを変更するには、そのドメインの親ドメインのAdministratorアクセス権が必要です。

名前と説明

各ドメインには、階層内で一意の名前が必要です。説明は任意です。

[Parent Domain]

第2および第3レベルのドメインには親ドメインがあります。ドメインを作成した後にドメインの親を変更することはできません。

デバイス

リーフドメインにのみデバイスを含めることができます。つまり、1つのドメインにはサブドメインまたはデバイスを含めることができますが、両方を含めることはできません。非リーフドメインが直接デバイスを制御している展開を保存することはできません。

ドメインエディタで、ドメイン階層の現在の場所に応じて、Webインターフェイスに使用可能な選択されたデバイスが表示されます。

ホスト制限（Host Limit）

Firewall Management Centerがモニタでき、ネットワークマップに保存できるホストの数。モデルによって異なります。マルチドメイン展開では、リーフドメインは使用可能なモニタされたホストのプールを共有しますが、個別のネットワークマップを持っています。

各リーフドメインがネットワークマップに値を入力できるように、ホスト制限を各サブドメインレベルで設定できます。ドメインのホスト制限を**0**に設定すると、ドメインは一般的なプールで共有します。

ホスト制限を設定すると、各ドメインレベルで異なる効果があります。

- リーフ：リーフドメインの場合、ホスト制限は単に、リーフドメインがモニタできるホスト数の制限です。
- 第2レベル：第3レベルのリーフドメインを管理する第2レベルのドメインの場合、ホスト制限は、リーフドメインがモニタできるホストの総数を表します。リーフドメインは、使用可能なホストのプールを共有します。
- グローバル：グローバルドメインの場合、ホスト制限は、Firewall Management Centerがモニタできるホストの総数に等しくなります。変更することはできません。

サブドメインのホスト制限の合計を、親ドメインのホスト制限より多くすることができます。たとえば、グローバルドメインのホスト制限が150,000の場合、複数のサブドメインを設定して、それぞれのホスト制限を100,000にすることができます。これらのドメインのいずれか（すべてではない）が100,000のホストをモニタできます。

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または長期間非アクティブになっているホストを置換することができます。各リーフドメインには独自のネットワーク検出ポリシー

があるため、各リーフドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

ドメインのホスト制限を軽減した場合に、そのネットワークマップに新しい制限より多くのホストが含まれている場合、システムは最も長い間非アクティブになっているホストを削除します。

関連トピック

ホスト制限（Host Limit）
ネットワーク検出のデータ ストレージ設定

ドメインの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者

ドメインの管理

ドメインのプロパティを変更するには、そのドメインの親ドメインへの管理者アクセス権が必要です。

手順

ステップ 1 [システム（System）]（⚙）>**[ドメイン（Domains）]**を選択します。

ステップ 2 次のようにドメインを管理します。

- 追加：[ドメインの追加（Add Domain）]をクリックするか、または親ドメインの横にある[サブドメインの追加（Add Subdomain）]をクリックします（新しいドメインの作成 （6 ページ） を参照）。
- 編集：変更するドメインの横 [編集（Edit）]（✎） をクリックします（ドメインのプロパティ （4 ページ） を参照）。
- 削除：削除する空のドメインの横 [削除（Delete）]（🗑） をクリックして、選択内容を確認します。宛先ドメインを編集することによって、削除するドメインからデバイスを移動します。

ステップ 3 ドメイン構造への変更を行い、すべてのデバイスをリーフドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 4 プロンプトが表示されたら、追加の変更を行います。

- リーフドメインを親ドメインに変更した場合は、古いネットワークマップを移動または削除します（ドメイン間のデータの移動 （7 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティゾーンまたはインターフェイスグループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （8 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

新しいドメインの作成

最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 のサブドメインを作成できます。

ドメイン設定を実装する前に、リーフ ドメインにすべてのデバイスを割り当てる必要があります。リーフドメインにサブドメインを追加すると、ドメインはリーフドメインではなくなるので、デバイスを再度割り当てる必要があります。

手順

ステップ 1 グローバルまたはセカンドレベルドメインで、[システム（System）]（⚙）>**[ドメイン（Domains）]** を選択します。

ステップ 2 [ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] をクリックします。

ステップ 3 [Name] と [Description] を入力します。

ステップ 4 [親ドメイン（Parent Domain）] を選択します。

ステップ 5 [デバイス（Devices）] で、ドメインに追加する [使用可能なデバイス（Available Devices）] を選択し、[ドメインに追加（Add to Domain）] をクリックするか、または [選択されたデバイス（Selected Devices）] のリストにドラッグアンドドロップします。

ステップ 6 必要に応じて、[詳細設定（Advanced）]をクリックして、新しいドメインがモニタできるホスト数を制限します（ドメインのプロパティ （4 ページ） を参照）。

ステップ 7 [保存（Save）] をクリックして、ドメイン管理ページに戻ります。

デバイスが非リーフドメインに割り当てられている場合は、システムによって警告が表示されます。これらのデバイスに新しいドメインを作成するには、[新しいドメインの作成（Create New Domain）] をクリックします。デバイスを既存のドメインに移動する予定がある場合は、[未割り当てのままにする（Keep Unassigned）] をクリックします。

ステップ 8 ドメイン構造への変更を行い、すべてのデバイスをリーフドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 9 プロンプトが表示されたら、追加の変更を行います。

- リーフドメインを親ドメインに変更した場合は、古いネットワークマップを移動または削除します（ドメイン間のデータの移動 （7 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティゾーンまたはインターフェイスグループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （8 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ドメイン間のデータの移動

イベントおよびネットワークマップがリーフドメインに関連付けられているため、リーフドメインを親ドメインに変更する場合は、2 つの選択肢があります。

- ネットワークマップおよび関連付けられているイベントを新しいリーフドメインに移動します。
- ネットワークマップは削除しますが、イベントは保持します。この場合、システムが必要に応じてまたは設定されているようにイベントをプルーニングするまで、イベントは親ドメインに関連付けられたままとなります。または、古いイベントを手動で削除できます。

始める前に

以前のリーフドメインが現在の親ドメインになるドメイン設定を実行します（ドメインの管理 （5 ページ） を参照）。

手順

ステップ 1 現在は親ドメインである以前の各リーフドメインに対して、次の手順を実行します。

- **親ドメイン**のイベントおよびネットワークマップを継承するには、新しい**リーフドメイン**を選択します。
- 親ドメインのネットワークマップを削除するが、古いイベントは保持する場合は、[なし（None）] を選択します。

ステップ 2 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ドメイン間のデバイスの移動

デバイスを移動するドメインでソースドメインとターゲットドメインが表示されている限り、ドメイン間でデバイスを移動できます。ドメイン間でデバイスを移動すると、デバイスに適用された設定とポリシーに影響する可能性があります。ドメイン間でデバイスを移動している間、システムは次のデバイス設定を保持します。

- インターフェイス
- インラインセット
- ルーティング
- DHCP
- 関連オブジェクト
- SNMP（利用可能な場合）

デバイスをドメイン間で移動すると、デバイスの設定に次の変更が発生する可能性があります。

- デバイスがターゲットドメインに移動した後もシステムでデバイス設定を保持するには、以下を確認してください。
  - 共有アクセス コントロール ポリシーがグローバルドメインにあること。他の共有ポリシーもグローバルドメイン内に配置することをお勧めします。
- VPN 設定の場合、
  - サイト間 VPN 設定がターゲットドメインにあること。
  - リモートアクセスVPN設定とデバイス証明書は、グローバルドメインまたはターゲットドメインにあります。

- リモート アクセス VPN ポリシーをデバイスに割り当てるときは、ターゲット ドメインがリモート アクセス VPN の設定されているドメインの子孫である場合のみ、ドメイン間でデバイスを移動できます。

- SNMP のネットワークオブジェクトがグローバルドメインにあること。

- デバイスは、デバイス上の登録済み証明書を削除することなく子ドメインに移動できます。具体的には次のとおりです。
  - 移動したデバイスに割り当てられた正常性ポリシーが新しいドメインでアクセス不能の場合、新しい正常性ポリシーを選択できます。
  - 移動したデバイスに割り当てられたアクセス コントロール ポリシーが有効でない場合、または新しいドメインでアクセスできない場合は、新しいポリシーを選択します。すべてのデバイスに、割り当てられたアクセス コントロール ポリシーが必要です。
  - 移動したデバイス上のインターフェイスが、新しいドメインでアクセスできないセキュリティゾーンに属している場合は、新しいゾーンを選択できます。
  - インターフェイスは、以下から削除されます。
    - 新しいドメインでアクセス不能で、アクセス コントロール ポリシーで使用されていないセキュリティゾーン。
    - すべてのインターフェイスグループ。

デバイスでポリシーの更新が必要だが、ゾーン間でインターフェイスを移動する必要がない場合は、ゾーン設定が最新であることを示すメッセージが表示されます。たとえば、デバイスのインターフェイスが共通の先祖ドメインに設定されているセキュリティゾーンに属している場合は、サブドメインからサブドメインにデバイスを移動する場合はゾーン設定を更新する必要はありません。

始める前に

- 新しいドメインを作成します。詳細については、新しいドメインの作成 （6 ページ）を参照してください。
- デバイスをドメインからドメインに移動し、次に新しいポリシーとセキュリティゾーンを割り当てる必要があるドメイン構成を実装します（ドメインの管理 （5 ページ） を参照）。

手順

ステップ 1 グローバルドメインで、（[システム（System）]（⚙）） > [ドメイン（Domains）] を選択します。

ステップ 2 デバイスを移動する予定のターゲットドメインを編集します。

ステップ 3 [ドメインの編集（Edit Domain）] ダイアログボックスで、次を実行します。

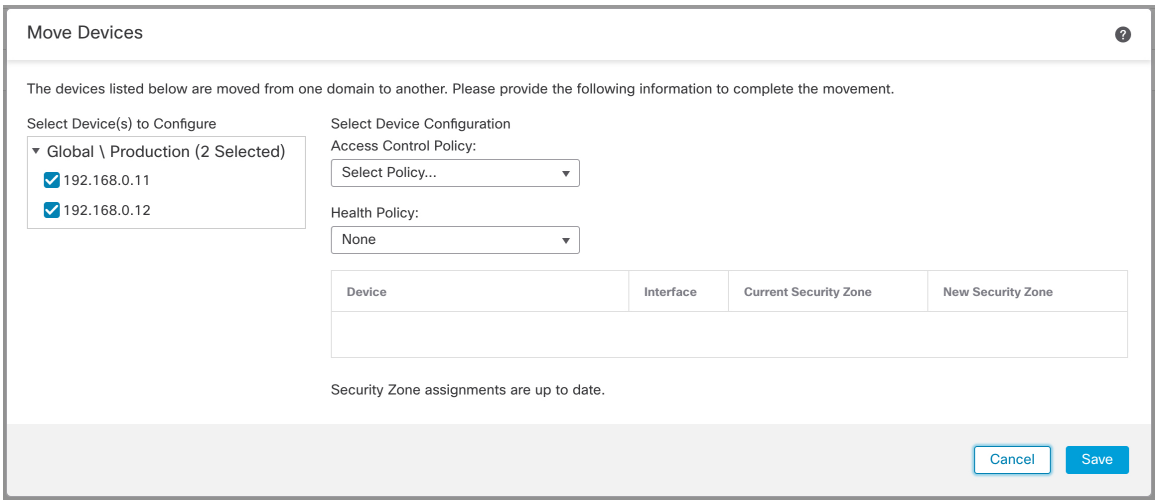
1. 移動するデバイスを選択し、[ドメインに追加（Add to Domain）] をクリックます。
2. [保存（Save）] をクリックします。

ステップ 4 [ドメイン（Domains）] ページで、[保存（Save）] をクリックします。

ステップ 5 **（アクセス コントロール ポリシーがグローバル ドメインにない場合）**[デバイスの移動（Move Devices）] ダイアログボックスで、次の手順を実行します。

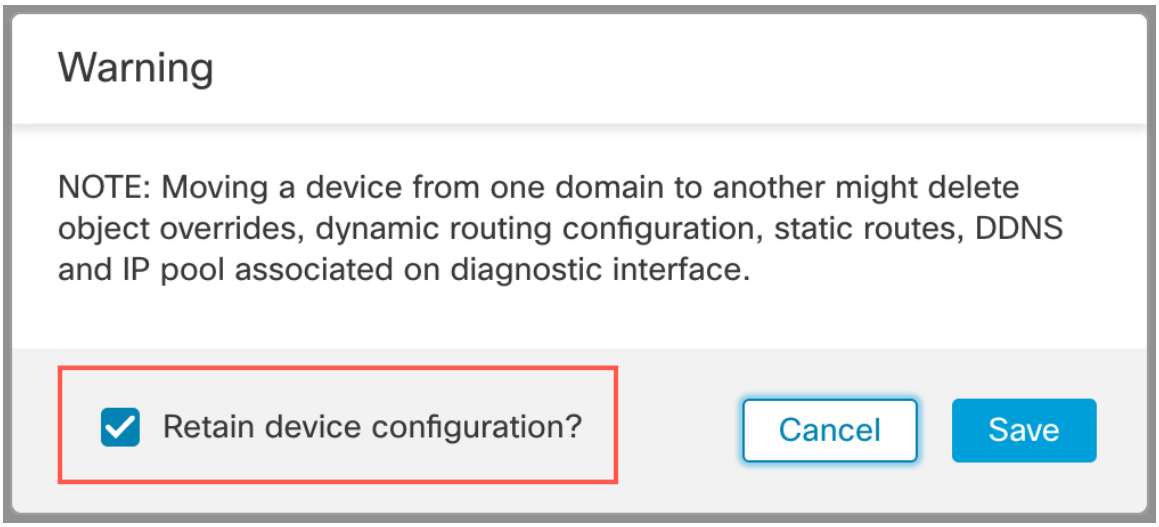
1. [設定するデバイスの選択（Select Device(s) to Configure）] で、設定するデバイスのチェックをオンにします。

   同じ正常性ポリシーとアクセス コントロール ポリシーを割り当てるには、複数のデバイスをオンにします。



2. デバイスに適用する [アクセスコントロールポリシー（Access Control Policy）] を選択するか、または新しいポリシーを作成するには[新しいポリシー（New Policy）] を選択します。
3. デバイスに適用する [正常性ポリシー（Health Policy）] を選択するか、またはデバイスに正常性ポリシーを適用しないままにするには [なし（None）] を選択します。
4. インターフェイスを新しいゾーンに割り当てるようにプロンプトが表示された場合は、リストされている各インターフェイスに [新しいセキュリティゾーン（New Security Zone）] を選択するか、または後で割り当てるには [なし（None）] を選択します。
5. すべての影響を受けるデバイスを設定した後、[保存（Save）] をクリックしてポリシーとゾーンの割り当てを保存します。

ステップ 6 移動後もデバイス設定を保持する場合は、[デバイス設定の保持（Retain device configuration?）] チェックボックスをオンにします。



このオプションを選択すると、デバイスがターゲットドメインに移動した後も、システムはデバイス設定を保持します。このオプションを選択しない場合、移動したデバイスのうち、移動による影響を受けたデバイスのデバイス設定を手動で更新する必要があります。

次の表は、さまざまなシナリオでオブジェクトがどのように処理されるかを示しています。

シナリオ	システムのアクション
オブジェクトは対象ドメインに存在します。	オブジェクトを再利用します。
ターゲットドメインに同じ名前と値のオブジェクトが存在します。	オブジェクトを再利用します。
ターゲットドメインに同じ名前で値が異なるオブジェクトが存在します。	• ネットワークとポート：オブジェクトのオーバーライドを作成します。 • インターフェイス オブジェクト：タイプが異なる場合に新しいオブジェクトを作成します。 • 名前の一致に応じて、他のすべてのオブジェクトタイプを再利用します。
ターゲットドメインにオブジェクトが存在しません。	新しいオブジェクトを作成します。

ステップ 7 [保存（Save）] をクリックして、ドメイン構成を実装します。

ステップ 8 ドメインの設定が完了したら、[OK] をクリックします。

次のタスク

- 移動の影響を受けた移動済みデバイスでその他の設定を更新します。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
- ドメイン間でデバイスを移動した後にシステムがデバイス設定を保持できない場合は、手動でデバイス設定を復元できます。詳細については、『Cisco Secure Firewall Management Center デバイス構成ガイド』の「*Export and Import the Device Configuration*」を参照してください。

ドメイン管理の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
サイト間 VPN に関連付けられたデバイス設定の保持	7.3	任意（Any）	ドメイン間でデバイスを移動するときに、サイト間 VPN がターゲットドメインで設定されている場合にのみ、サイト間 VPN に関連付けられているデバイス設定を保持できるようになりました。
デバイス設定の保持	7.2	任意（Any）	デバイスをドメイン間で移動しても、デバイス設定を保持できるようになりました。
サポートされているドメインの最大数の増加	6.5	任意（Any）	最大 100 ドメインを追加できるようになりました。以前は、最大で 50 ドメインでした。 サポートされているプラットフォーム： Secure Firewall Management Center

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。