Cisco TrustSec の IPsec インライン タギングの GET VPN サポート

Cisco TrustSec（CTS）アーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってネットワークを保護します。ネットワーク デバイスがネットワークに認証されると、クラウド内のデバイス間のリンクを使用する通信は、暗号化、メッセージ整合性チェック、およびリプレイ保護メカニズムを組み合わせることで保護されます。

CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットまたはフレームにタグを付けることで各パケットまたはフレームの分類が維持されます。これにより、パケットはデータ パス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの前提条件

この機能を有効にするすべてのキー サーバ（KS）およびグループ メンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.5 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

この機能は、ネットワークのすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの制約事項

- この機能は、IPv6 トラフィックをサポートしません。
- この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、または第 2 世代シスコ サービス統合型ルータ（ISR G2）用の Cisco VPN 内部サービス モジュールのトランスポート モードをサポートしません。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートに関する情報

セキュリティ グループ タギング機能のグループ メンバー登録

KS はグループ メンバー（GM）からセキュリティ アソシエーション（SA）登録要求を受信するか、連携 KS から接続確立要求を受信すると、グループ SA が SGT インライン タギングを有効にしているかどうかを確認します。有効にしている場合、承認を得るためには、すべての GM と連携 KS が GET VPN ソフトウェア バージョン 1.0.5 以降を使用して登録する必要があります。そうでない場合、登録要求または確立要求は拒否され、KS はネットワーク管理者に通知する syslog メッセージを生成します。

セキュリティ グループ タギングが有効な SA の作成

（**tag cts sgt** コマンドを使用して）グループ SA で IPsec インラインタギングの GET VPN サポートを有効にして、（**crypto gdoi ks rekey** コマンドを使用して）キー再生成をトリガーすると、KS は互換性のあるソフトウェアバージョンを使用しないグループ内の GM および連携 KS をチェックします。見つかると、警告メッセージが表示されます。

```
WARNING for group GETVPN: some devices cannot support SGT inline tagging. Rekey can cause
 traffic disruption and GM registration failures. Please check 'show crypto gdoi feature
 sgt'.
Are you sure you want to proceed ? [yes/no]:
```

グループ メンバー データ プレーンのセキュリティ グループ タグの処理

出力トラフィックとは、GM の GDOI 保護インターフェイスから送信されるトラフィックです。次の表は、出力パスにおける GM の動作を示したものです。

表 *1:* セキュリティ グループ タグの出力処理

セキュリティ グループ タギングが SA で有効	CTS が SGT を提供	GM データ プレーンの動作
対応	対応	SGT を Cisco メタデータに追加し、暗号化
対応	非対応	SGT なしで暗号化
非対応	はい	SGT なしで暗号化
非対応	非対応	SGT なしで暗号化

入力トラフィックとは、GM の GDOI 保護インターフェイスが受信するトラフィックです。次の表は、入力パスにおける GM の動作を示したものです。

表 *2:* セキュリティ グループ タグの入力処理

セキュリティ グループ タギングが SA で有効	CTS が SGT を提供	GM データ プレーンの動作
対応	対応	CTS の SGT を復号して抽出
対応	非対応	SGT の処理なしで復号
非対応	はい	復号して SGT を無視
非対応	非対応	SGT の処理なしで復号

セキュリティ グループ タギング使用時のパケットのオーバーヘッドとフラグメンテーション

各 GDOI パケットに SGT 情報を含む Cisco メタデータが追加されるため、SGT インライン タギングではパケットのオーバーヘッドが 8 バイト（または、時間ベースのアンチリプレイを有効にすると 16 バイト）増加します。

パケットが GDOI の暗号化の前に分割される場合、各フラグメントはそれに応じた SGT 情報とともにインライン タギングされます。パケットが GDOI 暗号化の後で分割される場合、最初のフラグメントのみが SGT 情報とともにインライン タギングされます。

2 つの方法を使用してフラグメンテーションを処理できます。1 つ目の方法は、Cisco メタデータを介した SGT 情報の伝達に使用される追加分のバイトを収容して暗号化を処理しているインターフェイスで **ip mtu** コマンドを使用することです。2 つ目の方法は、GM の LAN インターフェイスで **ip tcp adjst-mss 1352** コマンドを使用することです。このコマンドにより、LAN セグメントの最終的な IP パケットは 1392 バイト未満となり、それによって SGT を伝送するための任意のオーバーヘッドと Cisco メタデータに対して 108 バイトが提供されます。

MTU の問題に関する設計の詳細については、『Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide』の「Designing Around MTU Issues」のセクションを参照してください。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定方法

GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する

Cisco TrustSec の IPsec インライン タギング機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

ネットワーク内のすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature cts-sgt**
3. **show crypto gdoi feature cts-sgt | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature cts-sgt** 例： `Device# show crypto gdoi feature cts-sgt`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが Cisco TrustSec の IPsec インラインタギングをサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature cts-sgt | include No** 例： `Device# show crypto gdoi feature cts-sgt | include No`	（オプション）Cisco TrustSec の IPsec インライン タギングをサポートしていないデバイスのみ表示します。

Cisco TrustSec の IPsec インライン タギングの設定

Cisco TrustSec の IPsec インライン タギングを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **sa ipsec** *sequence-number*
7. **tag cts sgt**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GET-SGT`	GDOI グループを指定し、GDOI グループ 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	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Device(config-gdoi-group)# identity number 3333`
	例：
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**sa ipsec** *sequence-number* 例： `Device(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 7	**tag cts sgt** 例： `Device(gdoi-sa-ipsec)# tag cts sgt`	Cisco TrustSec の IPSec インライン タギングを有効化します。
ステップ 8	**end** 例： `Device(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec インライン タギングを有効にした後、キー再生成をトリガーする必要があります。詳細については「キー再生成のトリガー」セクションを参照してください。

キー再生成のトリガー

KS（またはプライマリ KS）でセキュリティ ポリシーを変更し（たとえば、DES から AES）、グローバル コンフィギュレーション モードを終了すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージが KS に表示されます。実行コンフィギュレーションの最新のポリシーに基づくキー再生成を送信するために、次のようにキー再生成をトリガーするコマンドを入力します。

キー再生成をトリガーするには KS（プライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**] 例： `Device# crypto gdoi ks group mygroup rekey`	すべての GM のキー再生成をトリガーします。 オプションの **replace-now** キーワードは、各 GM の古い TEK および KEK を即時に置き換え、SA が期限切れになる前に新しいポリシーを有効にします。 （注） **replace-now** キーワードを使用すると、一時的なトラフィックの不連続を引き起こすことがあります。

例

KS に次のようにメッセージが表示されます。

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

ポリシーの変更後、各 GM がこのトリガーされたキー再生成を受信すると、新しい SA（たとえば、AES 用）をインストールして、古い SA（たとえば、DES 用）のライフタイムを短縮します。各 GM はこの短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化および復号化を続けます。

セカンダリ KS のキー再生成をトリガーしようとすると、次のようにコマンドが拒否されます。

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの確認とトラブルシューティング

GM で実行されている設定を表示するには、**show running-config** コマンドを使用します。

SGT でタグ付けされたパケットの数を表示するには、次のコマンドを入力します。

```
Device# show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: GET, local addr 5.0.0.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   Group: GET-SGT
.
.
.
#pkts tagged (send): 0, #pkts untagged (rcv): 5
```

pkts tagged (send) フィールドは、アウトバウンド方向の SGT でタグ付けされたパケットを表示します。pkts untagged (rcv) フィールドは、インバウンド方向の SGT でタグ付けされていないパケットを表示します。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定例

例：GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature cts-sgt

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.5          Yes
        10.0.6.2         1.0.5          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
```

```
    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.5          Yes
        10.0.3.2         1.0.5          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）で Cisco TrustSec の IPsec インライン タギングをサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature cts-sgt | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

例：Cisco TrustSec の IPsec インライン タギングの設定

次に、単一の GDOI グループを提供する KS 用の IPsec SA の CTS SGT インライン タギングを設定する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL-SGT
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET-SGT
Device(config-gdoi-group)# identity number 1
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL-SGT
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

次に、GET VPN バージョン 1.0.5 以降 にアップグレードした GM を使用する（したがって CTS SGT インライン タギングをサポートしている）グループと、まだアップグレードしていない GM を使用するグループの、2 つのグループを設定する方法の例を示します。アップグレード済みの GM は、グループ番号 1111（小さい暗号マップ シーケンス番号）にグループ番号 2222（大きい暗号マップ シーケンス番号）とともに登録します。アップグレードしていない GM はグループ番号 2222 にのみ登録します。

この例では、2 つのサイト間のトラフィックに対して SGT タギングを設定します。**permit ip** コマンドは、2 つのサイト間の通信を許可するアクセス制御リスト（ACL）にアクセス制御エントリ（ACE）を追加します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL_NET_AB
Device(config-ext-nacl)# permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
Device(config-ext-nacl)# permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
Device(config-ext-nacl)# exit
Device(config)# ip access-list extended ACL_ALL
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET1
Device(config-gdoi-group)# identity number 1111
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_NET_AB
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# exit
Device(gdoi-local-server)# exit
Device(config-gdoi-group)# exit
Device(config)# crypto gdoi group GET2
Device(config-gdoi-group)# crypto gdoi group GET2
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_ALL
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

（注） GET VPN は、ACL あたり最大 100 の ACE をサポートします。

例：グループ メンバーのキー再生成のトリガー

GM がキー再生成のトリガーをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、GET VPN ネットワークのデバイスのソフトウェアのバージョンを表示し、またポリシー変更後のキー再生成のトリガーをサポートするかどうかを表示するために、KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature policy-replace

Key Server ID       Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
```

```
 Group Member ID     Version  Feature Supported
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

次の例は、ポリシー交換後のキー再生成のトリガーをサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。

キー再生成のトリガー

次の例では、ポリシー変更の実行後にキー再生成をトリガーする方法を示します。この例では、**profile gdoi-p2** コマンドで IPSec ポリシーの変更（たとえば、DES から AES）が発生します。

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#

*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled

rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

次の例では、セカンダリ KS のキー再生成をトリガーしようとすると表示されるエラーメッセージを示します。

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

（注） 時間ベースのアンチリプレイ（TBAR）が設定されると、キー サーバは 2 時間（7200 秒）ごとに定期的にキー再生成をグループ メンバーに送信します。次の例では、有効期間が 8 時間（28800 秒）に設定されていますが、キー再生成タイマーは 2 時間に設定されています。

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

show crypto gdoi gm replay コマンドおよび **show crypto gdoi ks replay** コマンドにより TBAR 情報が表示されます。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』
Cisco TrustSec の設定	『Cisco TrustSec Configuration Guide, Cisco IOS Release 15M&T』
MTU の問題の迂回設計	『Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide』

標準および RFC

標準/RFC	タイトル
RFC 2401	『Security Architecture for the Internet Protocol』
RFC 6407	『The Group Domain of Interpretation』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3 : Cisco TrustSec* 用の *IPsec* インライン タギングの *GET VPN* のサポートの機能情報

機能名	リリース	機能情報
Cisco TrustSec の IPsec インライン タギングの GET VPN サポート		

機能名	リリース	機能情報
		Cisco TrustSec（CTS）アーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってネットワークを保護します。ネットワーク デバイスがネットワークに認証されると、クラウド内のデバイス間のリンクを使用する通信は、暗号化、メッセージ整合性チェック、およびリプレイ保護メカニズムを組み合わせることで保護されます。 CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットまたはフレームにタグを付けることで各パケットまたはフレームの分類が維持されます。これにより、パケットはデータ パス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。 Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。 次のコマンドが導入または変更されました。 **show crypto gdoi, show crypto ipsec sa, tag cts sgt.**

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。