MACsec as a Service：暗号化ソリューション

このドキュメントでは、Cisco WAN MACsec およびイーサネット仮想回線（EVC）を使用してネットワークトラフィックを保護するために、暗号化ソリューションである Cisco MACsec as a Service を展開する方法について説明します。このソリューションは、MACsec Key Agreement（MKA）プロトコルを使用した Media Access Control Security（MACsec）のイーサネット仮想回線（EVC）サポートを提供します。MKA を使用した MACsec では、EVC が検出され、EVC 基準に一致する物理インターフェイスが有効になります。この機能により、ユーザーは、WAN リンクを介して複数の企業からのレイヤ 2 トラフィックを転送し、EVC を介した MACsec によってトラフィックを個別に保護できます。

MACsec as a Service 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 *1 : MACsec as a Service* の機能情報

機能名	リリース	機能情報
MACsec as a Service：MACsec および MKA のイーサネット仮想回線サポート	Cisco IOS XE Gibraltar 16.12.1a	このドキュメントでは、MACsec Key Agreement（MKA）プロトコルによる MACsec のイーサネット仮想回線（EVC）サポートを使用して暗号化ソリューションを展開する方法について説明します。MKA を使用した MACsec では、EVC が検出され、EVC 基準に一致する物理インターフェイスが有効になります。この機能により、ユーザーは、WAN リンクを介して複数の企業からのレイヤ 2 トラフィックを転送し、EVC を介した MACsec によってトラフィックを個別に保護できます。 このリリースでは、この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでのみサポートされています。 次のコマンドが導入または変更されました： **mka pre-shared-key key-chain** *key-chain-name*、**mka policy** *policy-name*、**mka default-policy**、**macsec replay-protection window** *window size*、**eapol destination-address** *destination-address*{*bridge-group-address* | *broadcast-address* | *lldp-multicast-address* | *unicast mac-address*}、**eapol eth-type** *eth-type*。

MACsec および MKA のイーサネット仮想回線サポートの前提条件

- WAN MACsec には MACsec ライセンスが必要です。『Cisco ASR 1000 シリーズ イーサネット ラインカード データシート』の表を参照してください。
- レイヤ 2 の透過型イーサネットサービスが使用可能であることを確認します。サービス プロバイダー ネットワークが、Extensible Authentication Protocol over LAN（EAPoL）などの透過的な MACsec レイヤ 2 制御プロトコルを提供する必要があります。

MACsec および MKA のイーサネット仮想回線サポートに関する制約事項

- この機能は、Cisco 1000 シリーズ アグリゲーション サービス ルータでのみサポートされています。
- この機能は、Cisco IOS XE Gibraltar 16.12.1a 以降でサポートされています。

- MACsec を使用した EVC では、dot1q ベースのヘッダーのみがサポートされています。

  ポートあたりの MKA P2P セッションの数は、1 ギガインターフェイスで 8、10 ギガインターフェイスで 32 です。

- MACsec または MKA セッションが、物理インターフェイスまたはサブインターフェイスですでに設定されている場合、同じ物理インターフェイスのサービスインスタンスまたは EVC モードで MKA セッションを使用して MACsec を設定することはできません。その逆も同様です。

- MACsec EVC は、MKA PSK ベースのセッションでのみサポートされています。

MACsec および MKA のイーサネット仮想回線サポートに関する情報

MACsec および MKA の概要

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディアアクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP フォンなどのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。

MKA による 802.1AE 暗号化は、ルータまたはスイッチとホストデバイスの間の暗号化用に、ダウンリンクポートでサポートされます。MKA は、IEEE 規格の 802.1X で定義されている MACsec のコントロールプレーンです。MKA フレームは、EAPoL フレームの一部を形成します。MACsec は、パケット処理プロセスの最終段階であり、EAPoL フレームを除くすべてのトラフィックを暗号化します。

WAN MACsec および MKA を実装する場合は、MACsec の有効化を試みる前に、基本的なレイヤ 2 イーサネット接続が確立されていることを確認します。詳細については、「MACsec および MKA の概要」を参照してください。

シスコのイーサネット仮想回線

イーサネット仮想回線（EVC）は、レイヤ2サービスの単一インスタンスのエンドツーエンド表現です。さまざまなパラメータが統合されて、サービスが提供されます。シスコの EVC 構造では、ブリッジドメインは、サービスインスタンスと呼ばれているレイヤ2インターフェイス（1つまたは複数）で設定されます。サービス インスタンスは、あるルータ上のあるポート上で EVC をインスタンス化したものです。サービスインスタンスは、設定に基づいてブリッジドメイン（BD）に関連付けられます。

着信フレームは、次の基準に基づいてサービス インスタンスとして分類できます。

- シングル 802.1Q VLAN タグ、優先度タグ付き、または 802.1ad VLAN タグ
- 両 QinQ（内部および外部）VLAN タグ、または 802.1ad S-VLAN と C-VLAN タグの両方
- 外部 802.1p CoS ビット、内部 802.1p CoS ビット、またはその両方
- サービスインスタンスは、他のマッピング基準もサポートします。
- [Untagged]：802.1Q または 802.1ad ヘッダがないすべてのフレームにマッピングします。
- [Default]：すべてのフレームにマッピングします。

EVC アーキテクチャの詳細については、『Carrier Ethernet Configuration Guide』の「Configuring Ethernet Virtual Circuit」のセクションを参照してください。

イーサネット サービス インスタンスまたはイーサネットフローポイント

イーサネットフローポイント（EFP）は、インターフェイス上のイーサネットサービスのトランスポートに依存しない抽象化です。EFP は、ユーザー定義の基準に基づいて、同じ物理ポートからのフレームを、そのポートに関連付けられた複数のサービスインスタンスの 1 つに分類します。各 EFP に、異なる転送アクションと動作を関連付けることができます。

Extensible Authentication Protocol over LAN 宛先アドレス

MACsec セキュアセッションを確立する前に、MACsec Key Agreement（MKA）が制御プロトコルとして使用されます。MKA は、暗号化に使用する暗号スイートを選択し、必要なキーとパラメータをピア間で交換します。

MKA は、MKA メッセージを送信するためのトランスポート プロトコルとして Authentication Protocol over LAN（EAPoL）を使用します。デフォルトでは、EAPoL は宛先マルチキャスト MAC アドレスとして 01:80: c2:00:00:03 を使用して、複数の宛先へパケットをマルチキャストします。EAPoL は標準ベースのプロトコルであり、IEEE 802.1 x などの他の認証メカニズムでも同じプロトコルが使用されます。サービス プロバイダー クラウド内のデバイスは、（宛先マルチキャスト MAC アドレスに基づいて）このパケットを消費し、EAPoL パケットの処理を試み、最終的にはパケットをドロップします。これにより、MKA セッションが失敗します。

インターフェイス上でサービス プロバイダーに送信される EAPoL パケットの宛先 MAC アドレスを変更するには、**eapol destination-address** コマンドを使用します。これにより、サービス プロバイダーは、パケットを消費せずに、他のデータ パケットと同様にトンネリングできます。

（注） EAPoL宛先アドレスは、物理レベルまたはサブインターフェイスレベルで設定できます。物理インターフェイスで設定する場合、設定はサブインターフェイスによって自動的に継承されます。サブインターフェイスでの明示的な設定は、そのサブインターフェイスで継承された値またはポリシーよりも優先されます。

ブリッジドメイン（BD）は、プラットフォーム内部のブロードキャストドメインを定義し、VLAN からブロードキャストドメインを分離できます。そのため、ポートごとの VLAN シグニフィカンスが可能になります。これにより、単一のボックス単位の VLAN ID 空間に関連する拡張性の制限がなくなります。EVCが各イーサネットフローポイント（EFP）でさまざまなカプセル化を使用する機能を提供する方法の詳細については、「□ブリッジドメインインターフェイスのカプセル化」を参照してください。

イーサネット仮想回線を使用した MACsec および MKA の利点

- WAN リンクを介して複数の企業顧客からのレイヤ 2 VLAN を転送し、MACsec によってトラフィックを個別に保護します。

  MACsec を使用した WAN 経由の LAN トラフィックの選択的暗号化

WAN MACsec および MKA のサポートの利点の詳細については、「WAN MACsec および MKA のサポート機能強化の利点」の項を参照してください。

イーサネット仮想回線を使用した MACsec as a Service

次のトポロジは、ポイントツーポイントおよびポイントツーマルチポイントのシナリオでWAN MACsec を使用してイーサネット仮想回線（EVC）を EoMPLS ネットワークに展開する方法を示しています。暗号化されたトラフィックが、CVLAN を持つ CE から CE ルータに伝送され、ネットワーク内の CE ルータが、データが宛先に到達することを確認します。

図 *1* : 単一の *SVLAN* を使用した *MKA* および *MACsec* トポロジ

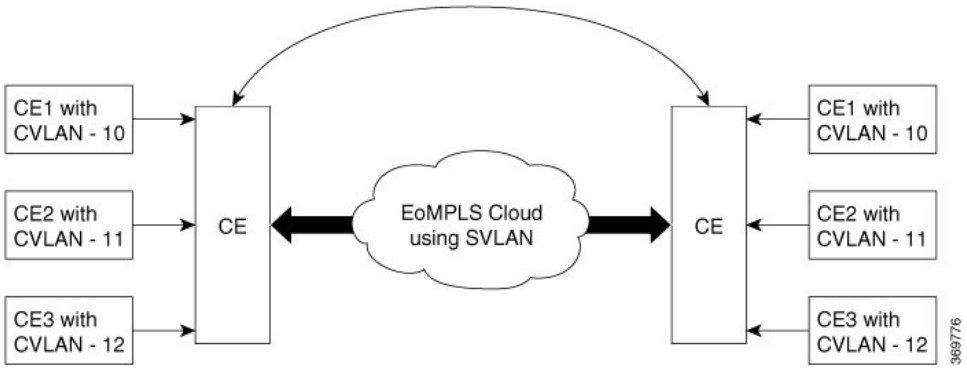
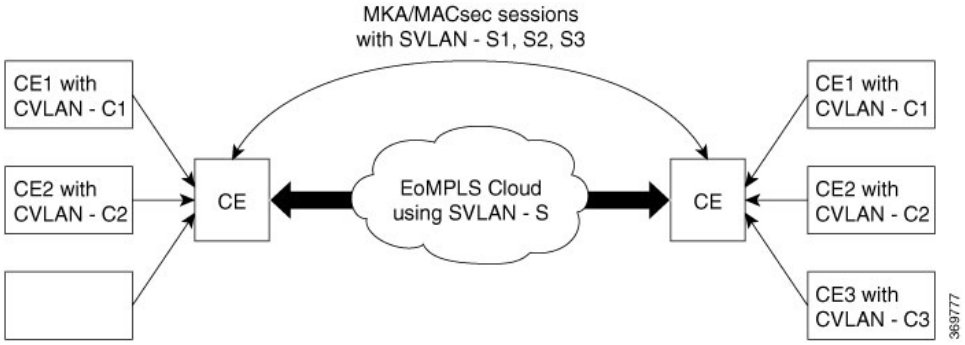


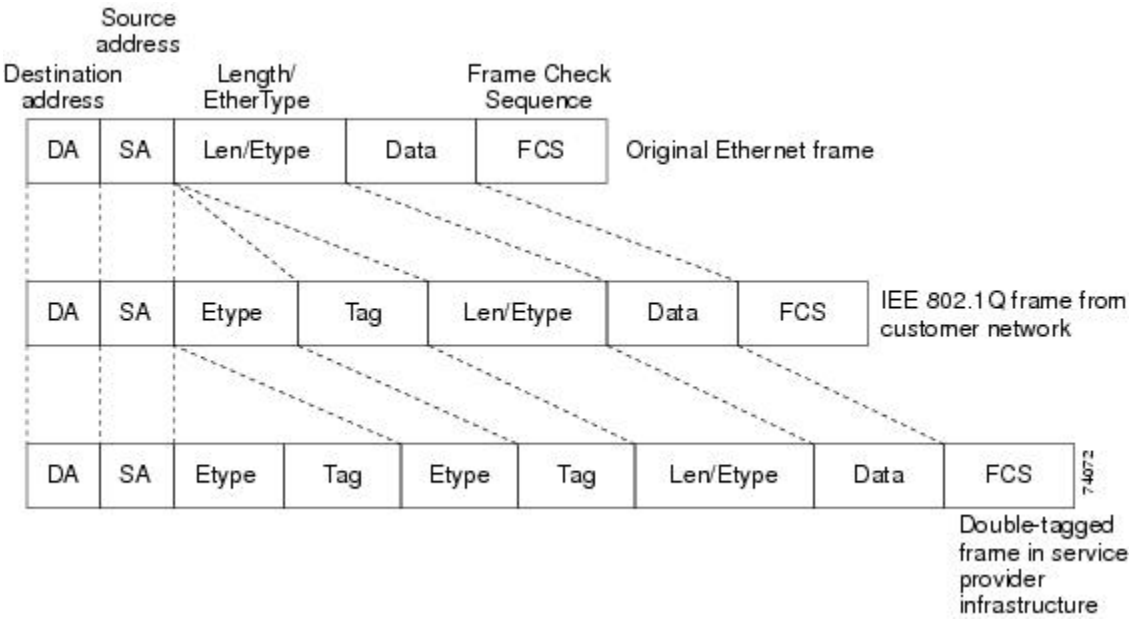
図 *2:* 複数の *SVLAN* を使用した *MKA* および *MACsec* トポロジ



EAPoL フレームをサポートする Cisco WAN MACsec は、データを暗号化するだけでなく、さまざまなサービス プロバイダー ネットワークをシームレスに移動して、すべてのリモートサイトに安全に接続するために役立ちます。

EoMPLS ネットワークでは、異なる場所にある複数のレイヤ 2 イーサネットネットワークを接続できます。EoMPLS を介してさまざまなサービスプロバイダーに接続することを可能にするために、WAN MACsec は、暗号化されていない dot.1q タグをサポートしています。これは、サービス プロバイダー ネットワークの動作を中断することなくパブリック E-LINE または E-LAN サービスを介してリモートサイトに接続するために役立ちます。

図 *3: 802.1Q* および二重タグ付きイーサネットパケット形式



サービスプロバイダーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダーネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限（4096 個）を容易に超えてしまいます。

サービス プロバイダー ネットワークを使用してネットワーク間でデータを交換する場合、MACsec を使用した EVC は、転送中のデータの暗号化に役立ちます。暗号化されていない dot.1q タグにより、複雑なネットワークを保護するための多数の設計オプションが可能になります。サービスプロバイダーはEVCを使用して、複数のカスタマーVLAN ID（C-VLAN）と、サービスプロバイダー VLAN（S-VLAN）による単一の 0x8100 Ethertype VLAN タグを持ち、サービス プロバイダー ネットワークに入るパケットをカプセル化できます。サービス プロバイダー ネットワーク内では、パケットは、S-VLANに基づいてスイッチングされます。パケットがサービス プロバイダー ネットワークからカスタマーネットワークに出ると、S-VLAN タグのカプセル化が解除され、元のカスタマーパケットが復元されます。

MACsec および MKA のイーサネット仮想回線サポートの設定方法

キーチェーンの設定

キーチェーンを設定するには、次の手順を実行します。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

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 **key chain** *key-chain-name* **macsec**

例：

```
Device(config)# Key chain keychain1 macsec
```

キー チェーンを設定して、キー チェーン 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 **key** *hex-string*

例：

```
Device(config-keychain)# key 01
```

キーを設定して、キー チェーン コンフィギュレーション モードを開始します。

ステップ 5 **cryptographic-algorithm** {**gcm-aes-128** | **gcm-aes-256**}

例：

```
Device(config-keychain-key)# cryptographic-algorithm aes-128-cmac
```

暗号化認証アルゴリズムを設定します。

ステップ 6 **key-string** *pwd-string*}

例：

```
Device(config-keychain-key)# key-string 12345678901234567890123456789013
```

キー文字列のパスワードを設定します。

ステップ 7 **end**

例：

```
Device(config-keychain-key)# end
```

特権 EXEC モードに戻ります。

インターフェイスでの MKA および MACsec の設定

インターフェイスで MKA および MACsec を設定するには、次の手順を実行します。

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 **configure terminal**

例：

```
Device# configure terminal
```

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 **mka policy** *policy-name*

例：

```
Device(config)# mka policy
```

MKA ポリシーを設定します。

ステップ 4 **mka pre-shared-key key-chain** *key-chain-name*

例：

```
Device(config)# mka pre-shared-key key-chain 10
```

MKA 事前共有キーに keychain10 を設定します。

（注） MKA事前共有キーは、物理インターフェイスまたはサブインターフェイスのいずれかで設定できますが、物理インターフェイスとサブインターフェイスの両方で設定することはできません。

ステップ5 macsec

EAPOL フレームタイプの MACsec を設定します。

ステップ6 macsec replay-protection window *window-size*

リプレイウィンドウを 10 に変更します。

ステップ7 end

特権 EXEC モードに戻ります。

カスタマーエッジ方向の入力ポートでのイーサネット仮想回線の設定

ステップ1 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 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 interface GigabitEthernet0/0/2

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4 service instance 10 Ethernet

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5 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6 interface GigabitEthernet0/0/2

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 7 **encapsulation dot1q 10**

ステップ 8 **rewrite ingress tag push dot1q 20 symmetric**

ステップ 9 **bridge-domain** *number*

ステップ 10
```
interface GigabitEthernet0/0/2
   service instance 11 Ethernet
encapsulation dot1q 10
rewrite ingress tag push dot1q 20 symmetric
bridge-domain 21
interface GigabitEthernet0/0/2
   service instance 12 Ethernet
encapsulation dot1q 10
rewrite ingress tag push dot1q 20 symmetric
bridge-domain 22
```

サービス プロバイダー ネットワーク方向の出力ポートでの MACsec EVC の設定

ステップ 1 **enable**

ステップ 2 **configure terminal**

例：
```
interface tenGigabitEthernet0/1/1
    macsec dot1q-in-clear 1
    service instance 20 Ethernet
encapsulation dot1q 20
mka pre-shared-key key-chain kc1
macsec
bridge-domain 20
    service instance 21 Ethernet
encapsulation dot1q 21
mka pre-shared-key key-chain kc1
     macsec
     bridge-domain 21
    service instance 22 Ethernet
encapsulation dot1q 22
mka pre-shared-key key-chain kc1
macsec
bridge-domain 22
```

MACsec および MKA セッションに基づく事前共有キーの有効化の確認

手順の概要

1. **enable**

2.

手順の詳細

ステップ 1 **enable**

ステップ 2 例：

```
show running-config | sec kc1
key chain kc1 macsec
 key 01
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789012
 mka pre-shared-key key-chain kc1
  mka pre-shared key-chain kc1
```

次に、サービスインスタンスモードでデフォルトポリシーを使用して事前共有キー（PSK）ベースの MKA/MACsec セッションを有効にするための設定例を示します。

```
Device#show running-config interface gi0/0/0
Building configuration...
 …
 …
 …
Current configuration : 142 bytes
!
interface Ethernet0/0
  no ip address
  negotiation auto
  service instance 10 ethernet
    encapsulation dot1q 10
    rewrite ingress tag pop 1 symmetric
    mka pre-shared key-chain kc1
    macsec
    bridge-domain 100
 !
end
```

MACsec および MKA のイーサネット仮想回線サポートの設定例

例：一般的なトラブルシューティング

例：一般的なトラブルシューティング

例：設定された show mka コマンド

例：設定された **show mka** コマンド

例：統計の表示

```
MACsec statistics on an EFP: To validate MACsec Statistics on an EFP instance, use
show macsec statistics interface gi0/0/3 efp 10
------------------------------------------------------------
MACsec Statistics for Gi0/0/3.EFP10
SecY Counters
  Ingress Untag Pkts:       5
  Ingress No Tag Pkts:      63440
  Ingress Bad Tag Pkts:     0
  Ingress Unknown SCI Pkts: 0
  Ingress No SCI Pkts:      0
  Ingress Overrun Pkts:     0
  Ingress Validated Octets: 0
  Ingress Decrypted Octets: 0
  Egress Untag Pkts:        0
  Egress Too Long Pkts:     0
  Egress Protected Octets:  0
  Egress Encrypted Octets:  0
Controlled Port Counters
  IF In Octets:             0
  IF In Packets:            0
  IF In Discard:            63440
  IF In Errors:             0
  IF Out Octets:            0
  IF Out Packets:           0
  IF Out Errors:            0
 Transmit SC Counters (SCI: 70708BBA4683000A)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       0
Transmit SA Counters (AN 2)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       0
Receive SA Counters (SCI: 70708BBA4183000A  AN 2)
  In Pkts Unchecked:        0
  In Pkts Delayed:          0
  In Pkts OK:               0
```

```
In Pkts Invalid:          0
In Pkts Not Valid:        0
In Pkts Not using SA:     0
In Pkts Unused SA:        0
In Pkts Late:             0
```

例：show efp コマンド

例：show efp コマンド

MACsec および MKA のイーサネット仮想回線サポートに関する追加情報

関連資料

標準および RFC

標準/RFC	タイトル
標準	役職

MIB

MIB	MIB のリンク
• CISCO-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

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。