SAML ベースの SSO ソリューション

SAML SSO ソリューションについて

重要 Cisco Jabber を Cisco Webex Meeting Server と共に展開する場合、Unified Communications Manager と Webex Meeting Server は同じドメインに存在している必要があります。

SAML は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のシスコのコラボレーションアプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。これは、サービス プロバイダ（例：Unified Communications Manager）がユーザの認証に使用する認証プロトコルです。SAML により、ID プロバイダー（IdP）とサービスプロバイダーの間で、セキュリティ認証情報を交換できます。

SAML SSO は SAML 2.0 プロトコルを使用して、シスコのコラボレーション ソリューションのドメイン間と製品間で、シングル サインオンを実現しています。SAML 2.0 は、Cisco アプリケーション全体で SSO を有効にし、Cisco アプリケーションと IdP 間でフェデレーションを有効にします。SAML 2.0 では、高度なセキュリティ レベルを維持しながら、シスコの管理ユー

ザが安全なウェブ ドメインにアクセスして、IdP とサービス プロバイダーの間でユーザ認証と承認データを交換できます。この機能が安全なメカニズムを提供していることで、さまざまなアプリケーションにわたり、共通の資格情報や関連情報を使用します。

SAML SSO の管理者権限は、シスコのコラボレーション アプリケーションでローカルに設定されたロールベース アクセス コントロール（RBAC）に基づき認証されます。

SAML SSO は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダーは IdP のユーザ情報を信頼しており、さまざまなサービスやアプリケーションにアクセスできるようにします。

重要 サービス プロバイダーが認証にかかわることはありません。SAML 2.0 では、サービス プロバイダーではなく、IdP に認証を委任します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。クライアントはサービス プロバイダーにアサーションを示します。CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

シングル サインオン単一サービス プロバイダー合意

シングル サインオンを使用すると、いずれか 1 つのシスコ コラボレーション アプリケーションにログオンした後、複数のコラボレーション アプリケーションにアクセスできます。Unified Communications Manager リリース 11.5 より前のリリースでは、管理者が SSO を有効にすると、各クラスタ ノードが URL と証明書を使って独自のサービス プロバイダ メタデータ（SP メタデータ）ファイルを作成しました。作成された各ファイルを ID プロバイダ（IDP）サーバに個別にアップロードする必要がありました。IDP サーバがそれぞれの IDP/SAML 交換を個別の合意と見なしたので、クラスタ内のノード数と等しい数の合意が作成されました。

ユーザ エクスペリエンスを改善し、大規模な導入でのソリューション全体のコストを削減するために、このリリースでは機能強化されました。現在では、Unified Communications Manager クラスタ（Unified Communications Manager とインスタント メッセージングおよびプレゼンス（IM and Presence））で単一の SAML 合意がサポートされます。

SAML-Based SSO の機能

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザー名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。SAML SSO を使用することで、IdP とサービスプロバイダーの間で信頼の輪を作成できます。サービス プロバイダーは IdP 信頼して、ユーザを認証します。

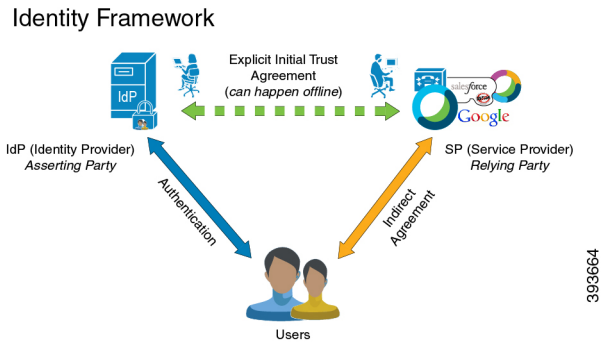
- 認証情報を保護し、安全に保ちます。暗号化機能により、IdP、サービス プロバイダー、ユーザの間で認証情報を保護します。SAML SSO では、IdP とサービスプロバイダー間で転送される認証メッセージを外部ユーザーから保護することもできます。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

SAML SSO ソリューションの基本要素

- クライアント（ユーザのクライアント）：これは、認証用にブラウザインスタンスを活用できる、ブラウザベースのクライアントまたはクライアントです。システム管理者のブラウザはその一例です。
- サービスプロバイダー：これは、クライアントがアクセスを試みるアプリケーションまたはサービスです。たとえば、Cisco Unified Communications Manager です。
- ID プロバイダー（IdP）サーバ：これは、ユーザ資格情報を認証し、SAML アサーションを発行するエンティティです。
- Lightweight Directory Access Protocol（LDAP）ユーザ：これらのユーザは、Microsoft Active Directory や OpenLDAP などの LDAP ディレクトリと統合されます。非 LDAP ユーザーは、Unified Communications サーバー上にローカルに存在します。
- SAML アサーション：これは、ユーザ認証のために、IdP からサービス プロバイダーに転送されるセキュリティ情報で構成されます。アサーションは、ユーザ名や権限などのサブジェクトに関する信頼されたステートメントを含む、XML ドキュメントです。通常では、信頼性を確保するために、SAML アサーションはデジタル署名されます。
- SAML リクエスト：これは、Unified Communications アプリケーションにより生成される認証リクエストです。LDAP ユーザーを認証するために、Unified Communications アプリケーションは認証要求を IdP に委任します。
- 信頼の輪（CoT）：これは、共同で 1 つの IdP に対して共有と認証を行うさまざまなサービス プロバイダーで構成されます。
- メタデータ：これは、SSO 対応の Unified Communications アプリケーション（Unified Communications Manager、Cisco Unity Connection など）や IdP によって生成される XML ファイルです。SAML メタデータの交換により、IdP とサービス プロバイダーの間に信頼関係が確立します。
- Assertion Consumer Service（ACS）URL：この URL は、アサーションをポストする場所を IdP に指示します。ACS URL は、最終的な SAML 応答を特定の URL にポストすることを IdP に指示します。

（注） 認証が必要なすべてのインスコープ サービスでは、SSO のメカニズムとして SAML 2.0 を使用します。

SAML SSO ソリューションの ID フレームワークについては、次の図を参照してください。



SAML SSO をサポートする Cisco Unified Communications アプリケーション

- Unified Communications Manager
- Unified Communications Manager IM and Presence Service

（注） SAML SSO の設定の詳細については、『*Features and Services Guide for Cisco Unified Communications Manager, Release 10.0(1)*』の「SAML Single Sign-On」の章を参照してください。

- Cisco Unity Connection

（注） Cisco Unity Connection サーバでの SAML SSO 機能の設定の詳細については、『*System Administration Guide for Cisco Unity Connection Release 10.x*』の「Managing SAML SSO in Cisco Unity Connection」の章を参照してください。

- Cisco Prime Collaboration

（注） Cisco Prime Collaboration サーバでの SAML SSO 設定手順の詳細については、『 *Cisco Prime Collaboration 10.0 Assurance* ガイド - アドバンスド』ガイドの「Managing Users」の章にある「Single Sign-On for Prime Collaboration」の項を参照してください。

- Cisco Unified Real-Time Monitoring Tool（RTMT）

（注） RTMT の SAML SSO を有効にする方法の詳細については、『 *System Configuration Guide for Cisco Unified Communications Manager*』の「Configure Initial System and Enterprise Parameters」の章にある「Configure SSO for RTMT」の手順を参照してください。

- Cisco Expressway

（注） Cisco Expressway の SAML SSO 設定情報を取得するには、『 *Cisco Expressway* 管理者ガイド』 を参照してください。

Cisco Unified Communications Manager Web インターフェイスの SAML SSO サポート

このリリースでは、Cisco Unified OS Administration およびディザスタリカバリシステムが Security Assertion Markup Language（SAML）SSO でサポートされるアプリケーションになりました。SAML SSO が有効になっている場合、ID プロバイダ（IdP）でシングル サインインした後、RTMT アプリケーションや、サポートされる他のアプリケーション（Ciscoユニファイドコミュニケーション マネージャ など）を起動できます。これらのアプリケーションに個別にサインインする必要はなくなりました。

Cisco Unified OS Administration およびディザスタリカバリシステムで SAML SSO をサポートするために、レベル 4 の管理者は Active Directory にレベル 0 とレベル 1 の管理者を作成します。レベル 4 の管理者は、クラスタのすべてのノードにプラットフォーム管理者を追加します。この追加により、プラットフォーム管理者は Active Directory とプラットフォーム データベースの間で同期されます。プラットフォームデータベースでユーザーを設定する際、管理者はユーザーの **uid** 値を設定する必要があります。Cisco Unified OS Administration およびディザスタリカバリシステムアプリケーションは、**uid** 値を使用してユーザを承認します。IdP サーバーは、Active Directory サーバーに対してクレデンシャルを認証し、SAML 応答を送信します。認証後、Unified Communications Manager は **uid** 値を使用してプラットフォーム データベースからユーザを承認します。**uid** 値の詳細については、「プラットフォームユーザーの一意の識別値の設定 （6 ページ） 」の手順を参照してください。

既存のリリースでSAML SSOが有効になっていて、以前のリリースから新しいリリースにアップグレードする場合、SAML SSO サポートは新しいリリースの Unified OS Administration および Disaster Recovery System アプリケーションで使用できます。Unified Communications Manager Web アプリケーションの SAML SSO を有効にすると、これらのアプリケーションの SAML SSO サポートも有効になります。新しいリリースで SAML SSO サポートを有効にするには、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』の「SAML SSO Enablement」トピックを参照してください。

（注） Unified Communications Manager 管理者に対して SAML SSO サポートが有効になっている場合、クラスタ全体に適用できます。ただし、Cisco Unified OS Administration および Disaster Recovery System アプリケーションの場合、各プラットフォーム管理者はノードに固有であり、これらのユーザの詳細はクラスタ全体に複製されません。したがって、各プラットフォームユーザは、クラスタの各サブスクライバ ノードに作成されます。

プラットフォームユーザーの一意の識別値の設定

一意の識別（UID）値は、プラットフォーム ユーザがプラットフォーム ページで SSO ログインを実行することを許可するために使用されます。レベル4の管理者は、次のいずれかの方法でプラットフォーム管理者用にこの値を設定できます。

- CLI で **set account name** コマンドを使用します。
- 既存の **uid** 値を更新します。

（注） 詳細については、『 *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* 』の「**set account name** 」コマンドと「**set account ssouidvalue**」を参照してください。

Cisco Unified OS Administration のリカバリ URL サインインオプション

このリリースでは、プラットフォーム管理者は、SAML SSO 対応アプリケーションのいずれかにサインインするか、リカバリ URL オプションを使用して、Cisco Unified OS Administration にアクセスできます。このオプションは、SSO 対応ノードのメインページで [シングルサインオン（ **Single Sign On**）] リンクをバイパスするための**リカバリ URL** として使用できます。プラットフォームユーザは、リカバリ URL アクセス権を持っている場合、Cisco Unified OS Administration にサインインできます。

（注） SSO のみを有効にし、リカバリ URL を有効にせず、認証ユーザーに十分なアクセス権限がない場合、403 エラー（アクセス拒否応答）のみが表示されます。ただし、[リカバリ URL（Recovery URL）] を有効にすると、エラーが発生すると、認証ユーザは [リカバリ URL（Recovery URL）] ページにリダイレクトされます。

レベル 4 の管理者は、プラットフォームユーザーのリカバリ URL サインインオプションを設定します。管理者は、CLI を使用してプラットフォーム管理者を作成している間、または CLI コマンドを使用して詳細を更新しているときに、このオプションを有効にできます。新規および既存のプラットフォーム管理者用のリカバリ URL ログイン用の CLI コマンドの詳細については、『 *Cisco Unified Communications* ソリューション コマンド ライン インターフェイス リファレンス ガイド』 の **set account ssorecoveryurlaccess**コマンドを参照してください。

（注） デフォルトでは、レベル 4 の管理者に対して [シングルサインオンをバイパスするリカバリ URL（ **Recovery URL to bypass Single Sign On** ）] リンクが有効になっています。このリンクは、以前のリリースから新しいリリースにアップグレードする場合、プラットフォーム管理者レベル 0 およびレベル 1 に対して有効になります。

ソフトウェア要件

SAML SSO 機能には、次のソフトウェア コンポーネントが必要です。

- Cisco Unified Communications アプリケーション、リリース 10.0(1) 以降。
- IdP サーバーによって信頼され、Cisco Unified Communications アプリケーションによってサポートされる LDAP サーバー。
- SAML 2.0 標準に準拠する IdP サーバー。
- Unified Communications Manager でサポートされるログインフローは SP によって開始されます。

ID プロバイダー（IdP）の選択

シスコ コラボレーション ソリューションは、SAML 2.0（セキュリティ アサーション マークアップ言語）を使用して、ユニファイド コミュニケーション サービスを利用するクライアント用の SSO（シングル サインオン）を有効にします。

SAML ベースの SSO は、企業ネットワーク内部から発信された UC サービス要求を認証するためのオプションであり、モバイルおよびリモートアクセス（MRA）を介して外部から UC サービスを要求するクライアントに拡張されました。

使用する環境に SAML ベース SSO を選択した場合は、次の点に注意してください。

- SAML 2.0 は、SAML 1.1 との互換性がないため、SAML 2.0 標準を使用する IdP を選択する必要があります。
- SAML ベースのアイデンティティ管理は、コンピューティングとネットワーキング業界のベンダーによって異なる方法で実装されています。したがって、SAML 標準に準拠するための幅広く受け入れられている規制はありません。
- 選択した IdP の設定や管理ポリシーは、Cisco TAC（テクニカル アシスタンス センター）のサポート対象外です。IdP ベンダーとの関係とサポート契約を利用して、IdP を正しく設定する上での支援を得られるようにしてください。Cisco は IdP に関するエラー、制限、または特定の設定に関する責任を負いません。

シスコ コラボレーション インフラストラクチャは、SAML 2.0 への準拠を主張する他の IdP と互換性がある可能性もありますが、シスコ コラボレーション ソリューションでテストされているのは次の IdP だけです。

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0、3.0、4.0、5.0
- Microsoft Azure
- PingFederate® 6.10.0.4
- F5 BIG-IP 11.6.0
- Okta 2017.38

SAML のコンポーネント

SAML SSO ソリューションは、特定のアサーション、プロトコル、バインディング、プロファイルの組み合わせに基づきます。さまざまなアサーションは、プロトコルやバインディングを使用しているアプリケーション間やサイト間で交換され、これらのアサーションによりサイト間でユーザを認証します。SAML のコンポーネントは次のとおりです。

- SAML アサーション：これは、IdP からサービス プロバイダーに転送される情報の構造と内容を定義します。セキュリティ情報のパケットで構成され、サービスプロバイダーがさまざまなレベルのアクセスコントロールの決定に使用するステートメントが含まれています。

  SAML SSO は、次のタイプのステートメントを提供します。

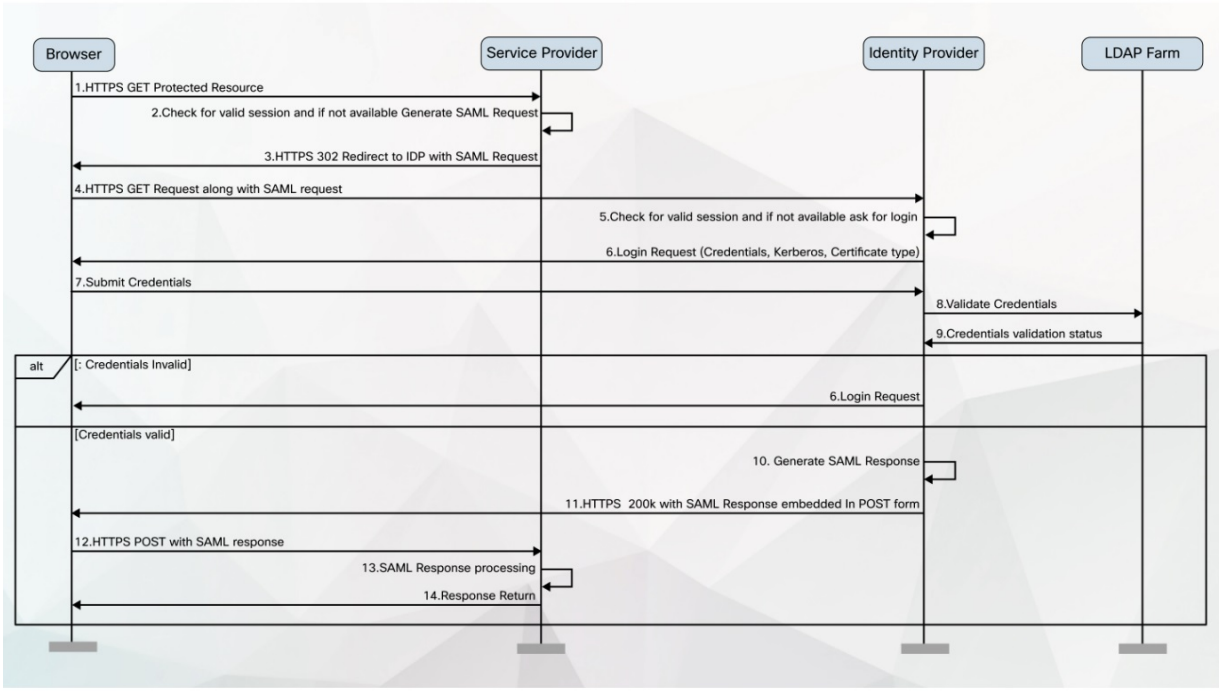
  - 認証ステートメント：これらのステートメントは、IdP とブラウザの間で特定の時間に行う認証の方法について、サービス プロバイダーにアサートします。
  - 属性ステートメント：これらのステートメントは、ユーザに関連付ける特定の属性（名前と値のペア）についてアサートします。属性アサーションには、ユーザに関する具体的な情報が含まれます。サービスプロバイダーは、属性を使用してアクセス制御の決定を行います。

- SAMLプロトコル：SAMLプロトコルは、SAMLがアサーションをどのように要求し、取得するかを定義します。このプロトコルは、特定の SAML エレメントまたはアサーションで構成されている、SAML 要求と応答エレメントに対応します。SAML 2.0 には次のプロトコルがあります。
  - アサーション クエリと要求のプロトコル
  - 認証要求のプロトコル
- SAML バインディング：SAML バインディングは、SOAP 交換のような、標準メッセージング形式または通信プロトコルとのSAMLアサーションまたはプロトコルメッセージ（またはその両方）の交換のマッピングを指定します。Unified Communications 10.0 は次の SAML 2.0 バインディングをサポートしています。
  - HTTP Redirect（GET）バインディング
  - HTTP POST バインディング
- SAMLプロファイル：SAMLプロファイルでは、明確に定義された使用事例をサポートするために、SAMLアサーション、プロトコル、およびバインディングの組み合わせについて詳細に説明しています。Unified Communications 10.0 は、SAML 2.0 Web ブラウザ SSO プロファイルをサポートしています。

SAML SSO コールフロー

このセクションでは、 SAML SSO 機能を使用して Unified Communications アプリケーションのシングルサインオンを有効にする方法について説明します。このセクションでは、IdP とサービスプロバイダーの関係についても説明し、シングルサインオンを有効にするためのさまざまな構成設定の重要性を特定するのに役立ちます。

図 *1 : IdP* からのクレデンシャル要求の *SAML SSO* コール フロー



1	ブラウザベースのクライアントが、サービスプロバイダーの保護されたリソースにアクセスしようとします。 （注）　ブラウザにサービスプロバイダーとの既存のセッションがありません。

2	ブラウザから要求を受信すると、サービスプロバイダーは SAML 認証要求を生成します。 （注） SAML 要求には、要求を生成したサービス プロバイダーを示す情報が含まれます。後で、これにより、IdP は要求を開始した特定のサービスプロバイダーを知ることができます。 SAML 認証を正常に完了するには、IdP にアサーション コンシューマ サービス（ACS）URL が必要です。ACS URL は、最終的な SAML 応答を特定の URL にポストすることを IdP に指示します。 （注） Unified Communications Manager および VOS 製品は、SAML 2.0 標準に準拠したアサーション コンシューマ サービス インデックス URL を使用します。 （注） 認証要求は IdP に送信でき、アサーションはリダイレクトまたは POST バインディングを介してサービス プロバイダーに送信できます。たとえば、Unified Communications Manager は、いずれの方向でも POST バインディングをサポートします。
3	サービス プロバイダーは、ブラウザに要求をリダイレクトします。 （注） IdP URL は、SAML メタデータ交換の一部としてサービスプロバイダーで事前設定されています。
4	ブラウザはリダイレクトに従い、HTTPS GET 要求を IdP に発行します。SAML 要求は、GET 要求のクエリパラメータとして維持されます。
5	IdP は、ブラウザとの有効なセッションをチェックします。
6	ブラウザ内に既存の Cookie がない場合、IdP はブラウザへのログイン要求を生成し、IdP によって設定および適用されている認証メカニズムを使用してブラウザを認証します。 （注） 認証メカニズムは、顧客のセキュリティおよび認証要件によって決定されます。これは、ユーザー名とパスワード、Kerberos、PKI などを使用したフォームベースの認証である可能性があります。この例では、フォームベースの認証を想定しています。
7	ユーザーはログインフォームに必要なログイン情報を入力し、IdP にポストバックします。 （注） ロギングの認証チャレンジは、ブラウザと IdP の間で行われます。サービス プロバイダーが認証にかかわることはありません。
8	IdP は LDAP サーバーにクレデンシャルを送信します。
9	LDAP サーバーは、クレデンシャルのディレクトリをチェックし、検証ステータスを IdP に返します。

10	IdP はクレデンシャルを検証し、SAML アサーションを含む SAML 応答を生成します。 （注） アサーションは IdP によってデジタル署名され、ユーザーはサービス プロバイダーで保護されたリソースへのアクセスが許可されます。IdP もここでクッキーを設定します。
11	IdP は SAML 応答をブラウザにリダイレクトします。
12	ブラウザは非表示形式の POST 命令に従い、サービス プロバイダーの ACS URL にアサーションをポストします。
13	サービスプロバイダーは、アサーションを抽出し、デジタル署名を検証します。 （注） サービスプロバイダーは、このデジタル署名を使用して、IdP との信頼の輪を確立します。
14	サービス プロバイダーは、保護されたリソースへのアクセスを許可し、ブラウザに 200 OK と応答してリソース コンテンツを提供します。 （注） サービス プロバイダーは、リソース認証を担当します。たとえば、ユーザが IdP によって正常に認証されても、Cisco Unified Communications Manager で設定されている管理者ロールの権限を持っていない限り、Cisco Unified CM Administration インターフェイスにログインできない場合があります。 （注） サービスプロバイダーは、ここでクッキーを設定します。追加のリソースに対するブラウザによる後続の要求がある場合、ブラウザは要求にサービスプロバイダーのクッキーを含めます。サービスプロバイダーは、ブラウザとのセッションがすでに存在するかどうかを確認します。セッションが存在する場合、Web ブラウザはリソースの内容を返します。

Okta 経由の RTMT への SAML SSO ログインの Java 要件

Okta が id プロバイダーとして設定されている SAML SSO があり、SSO を使用して Cisco ユニファイド リアルタイム モニタリング ツールにログインする場合は、最小 Java バージョン8.221 を実行している必要があります。この要件は Ciscoユニファイド コミュニケーション マネージャ および IM and Presence Service の 12.5(x) リリースに適用されます。

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。