SAML-Based 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 と共に導入する場合、Cisco 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、ユーザを認証するために、サービス プロバイダ（Cisco Unified Communications Manager など）が使用する認証プロトコルです。SAML により、ID プロバイダ（IdP）とサービス プロバイダの間で、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。この機能は、さまざまなアプリケーションにわたり、共通の資格情報と関連情報を使用するための安全な機構を提供します。

SAML SSO 管理アクセスの許可は、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）に基づいています。

SAML SSO は、IdP とサービス プロバイダ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 プロバイダは IdP のユーザ情報を信頼して、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 プロバイダが認証に関わることはありません。SAML 2.0 では、サービス プロバイダではなく、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。

管理ユーザが、SAML SSO を有効にして、シスコのさまざまなコラボレーション アプリケーションにどのようにアクセスするかについては、SAML SSO コール フロー, （9 ページ） を参照してください。

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。Cisco 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、Cisco 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 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 を使用して、IdP とサービス プロバイダの間で信頼の輪を作成できます。サービス プロバイダは 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、ユーザの間で認証情報を保護します。SAML SSO では、外部ユーザに対して、IdP とサービス プロバイダの間で渡される認証メッセージを非表示に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。

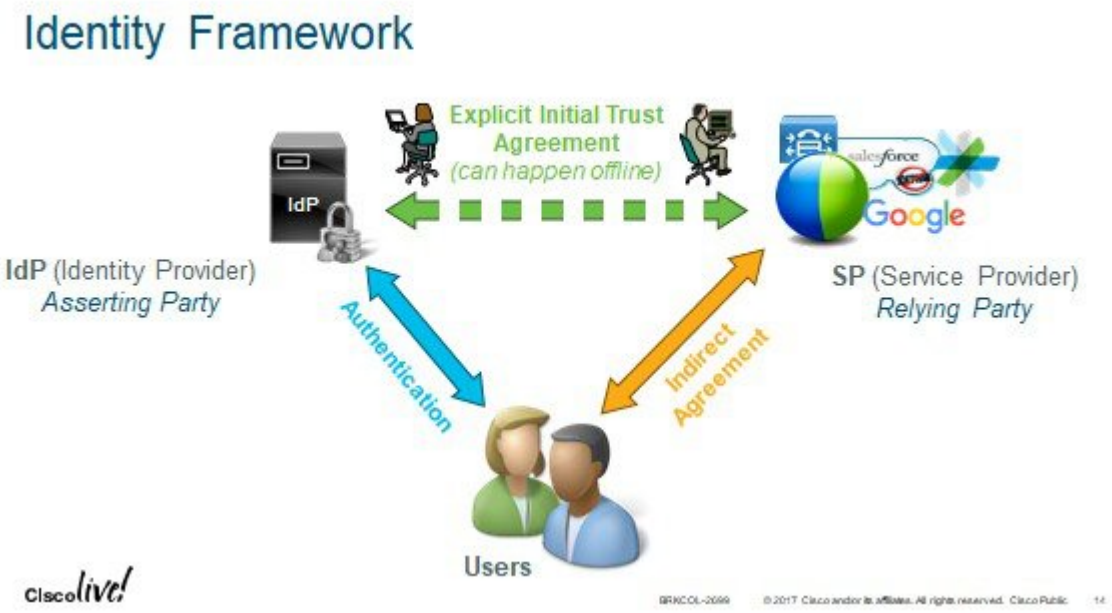
SAML SSO ソリューションの基本要素

- 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：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。Cisco Unified Communications Manager はその一例です。
- ID プロバイダ（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 ユーザは、Unified Communications サーバ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 要求：これは、Unified Communications アプリケーションにより生成される認証要求です。LDAP ユーザを認証するために、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、共通の 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（Cisco Unified Communications Manager、Cisco Unity Connection など）および IdP により生成される 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 プロバイダの間に信頼関係が確立されます。
- Assertion Consumer Service（ACS）URL：この URL は、アサーションを POST 形式で送信する場所を IdP に指示します。ACS URL は、最終的な SAML 応答を特定の URL に POST 形式で送信するように 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 ソリューションのアイデンティティ フレームワークについて、下の図を参照してください。

図 *1*：***SAML SSO*** ソリューションのアイデンティティ フレームワーク



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

- Cisco Unified Communications Manager
- Cisco 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 機能設定のその他の有用な情報については、『*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 の設定手順の詳細については、『*Cisco Prime Collaboration 10.0 Assurance Guide - Advanced*』ガイドにある、「Managing Users」の章の「Single Sign-On for Prime Collaboration」の項を参照してください。

- Cisco Unified Real-Time Monitoring Tool（RTMT）の Windows バージョン。

（注） RTMT 用に SAML SSO を有効化する方法について、詳しくは『*System Configuration Guide for Cisco Unified Communications Manager*』ガイドの「Configure Initial System and Enterprise Parameters」の章の「Configure SSO for RTMT」の手順を参照してください。

- Cisco Expressway

（注） Cisco Expressway での SAML SSO 設定については、『*Cisco Expressway Administrator Guide*』を参照してください。

Cisco Unified Communications Manager の Web インターフェイス用の 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 対応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、これらの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 Unified Communications Manager 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がなくなりました。

Cisco Unified OS Administration およびディザスタ リカバリ システム用に SAML SSO をサポートするには、レベル 4 管理者が Active Directory でレベル 0 およびレベル 1 管理者を作成します。レベル4管理者は、クラスタのすべてのノードでプラットフォーム管理者を追加します。追加すると、Active Directory とプラットフォーム データベースの間でプラットフォーム管理者が同期されます。プラットフォーム データベースでユーザを設定するとき、管理者はユーザの **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 システムのアプリ

ケーションは、**uid** 値を使ってユーザを許可します。IdP サーバは Active Directory サーバで資格情報を認証し、SAML 応答を送信します。認証後、Cisco Unified Communications Manager は **uid** 値を使ってプラットフォームデータベースからユーザを許可します。**uid** 値の詳細については、プラットフォーム ユーザー用の一意識別値の設定, （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 が有効になっている場合、旧リリースから新しいリリースにアップグレードすると、新しいリリースの Cisco Unified OS Administration およびディザスタ リカバリ システムのアプリケーションで SAML SSO サポートが使用可能になります。また、これらのアプリケーションの SAML SSO サポートは、いずれかの Cisco Unified Communications Manager Web アプリケーションで SAML SSO を有効にした場合にも使用可能になります。新しいリリースで SAML SSO サポートを有効にするには、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の中の SAML SSO 有効化に関するトピックを参照してください。

（注） Cisco Unified Communications Manager 管理者用に SAML SSO サポートが有効になっている場合、クラスタ全体にそれが適用されます。ただし、Cisco Unified OS Administration およびディザスタ リカバリ システムのアプリケーションでは各プラットフォーム管理者がノードに固有であり、このようなユーザ詳細はクラスタ全体に複製されません。したがって、クラスタの各サブスクライバ ノードに各プラットフォーム ユーザが作成されます。

プラットフォーム ユーザー用の一意識別値の設定

プラットフォーム ページで SSO ログインを行うために、一意識別（UID）値を使用してプラットフォーム ユーザを許可します。レベル 4 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** コマンドを使用してプラットフォーム ユーザを作成するとき。
- 既存の **uid** 値を更新するとき。

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

Cisco Unified OS Administration 用のリカバリ 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が Cisco Unified OS Administration にアクセスするには、いずれかの SAML SSO 対応アプリケーションにサインインするか、またはリカバリ URL オ

プションを使用できます。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 サインオンをバイパスするためのリカバリ URL（Recovery URL to bypass Single Sign On）] リンクとして使用できます。リカバリ URL にアクセスできるプラットフォーム ユーザは、Cisco Unified OS Administration にサインインできます。

レベル 4 管理者が、プラットフォーム ユーザのためにリカバリ URL サインイン オプションを設定します。この管理者は、CLI を介してプラットフォーム管理者を作成するとき、または CLI コマンドを使ってプラットフォーム管理者の詳細を更新するときに、このオプションを有効にすることができます。新規または既存のプラットフォーム管理者用のリカバリ URL ログインに関する CLI コマンドについて、詳しくは『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の中の **set account ssorecoveryurlaccess** コマンドを参照してください。

（注） デフォルトでは、[シングル サインオンをバイパスするためのリカバリ URL（Recovery URL to bypass Single Sign On）] リンクがレベル 4 管理者向けに有効になっています。以前のリリースから新しいリリースにアップグレードした場合、レベル 0 およびレベル 1 プラットフォーム管理者向けにこのリンクが有効になります。

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。
- SAML 2.0 規格に準拠した IdP サーバ。

アイデンティティ プロバイダ（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からの UC サービス要求を認証するためのオプションです。現在は、Mobile & Remote Access（MRA）経由で外部から UC サービスを要求するクライアントにまで拡張されました。

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。シスコは 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 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIG-IP 11.6.0
- Okta

SAML コンポーネント

SAML SSO ソリューションは、アサーション、プロトコル、バインディング、およびプロファイルの特定の組み合わせに基づいています。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アプリケーションおよびサイト間で交換され、これらのアサーションによってサイト間でユーザが認証されます。SAML のコンポーネントは次のとおりです。

- SAML アサーション：IdP からサービス プロバイダに転送される情報の構造と内容を定義します。これはセキュリティ情報のパケットで構成され、サービス プロバイダが、さまざまなレベルのアクセス制御を決定する際に使用するステートメントが含まれます。
  SAML SSO は、次の種類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、サービス プロバイダに対して、IdP とブラウザ間で特定の時点に行う認証の方法についてアサートします。
  - 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、ユーザに関する特定の情報が含まれます。サービス プロバイダは、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た SAML 要求および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 クエリー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、標準メッセージング形式または SOAP 交換などの通信プロトコルで、SAML アサーションやプロトコル メッセージ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

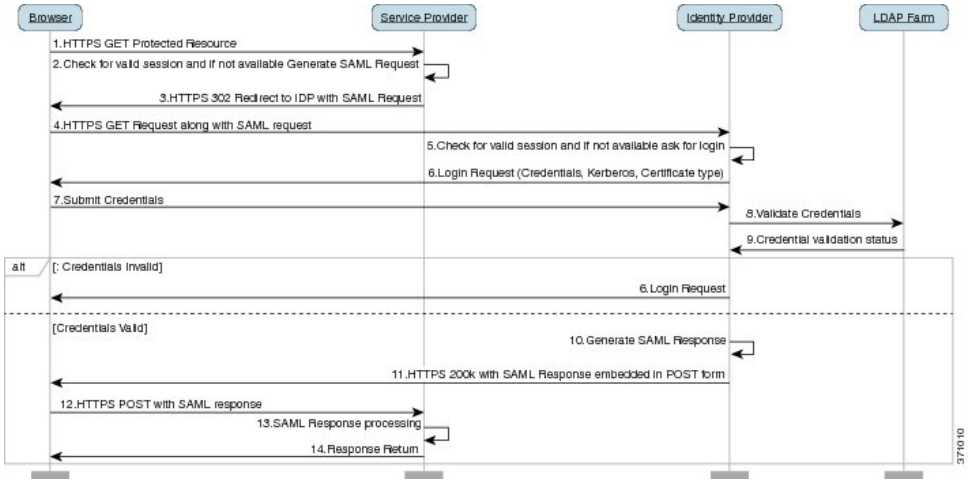
- SAML プロファイル：SAML プロファイルでは、明確に定義された使用例をサポートするために、SAML アサーション、プロトコル、およびバインディングの組み合わせについて詳細に説明しています。Unified Communications 10.0 は、SAML 2.0 の Web ブラウザ SSO プロファイルをサポートしています。

SAML SSO コール フロー

この項では、SAML SSO 機能が、Unified Communications アプリケーションに対してシングル サインオンをどのように有効にするかについて説明します。この項では、IdP とサービス プロバイダの関係も説明し、シングル サインオンを有効にするために、さまざまな設定が重要であることを示します。

以下の図に示す SAML SSO コール フローでは、IdP がユーザ名とパスワードを要求します。

図 *2*：*IdP* からの資格情報要求を含む *SAML SSO* コール フロー



1	ブラウザ ベースのクライアントは、サービス プロバイダ上の保護されたリソースにアクセスしようとします。 （注）　ブラウザには、サービス プロバイダとの既存セッションはありません。

2	ブラウザから要求を受信すると、サービス プロバイダは SAML 認証要求を生成します。 （注） SAML 要求には、どのサービス プロバイダが要求を生成したかを示す情報が含まれています。これにより、IdP は、どのサービス プロバイダが要求を開始したかを後で知ることができます。 IdP は、SAML 認証を正常に完了させるために、Assertion Consumer Service（ACS）URL を保持する必要があります。ACS URL は、最終的な SAML 応答を特定の URL に POST 形式で送信するように IdP に指示します。 （注） Cisco Unified Communications Manager では SAML 認証要求に Assertion Consumer Service URL を使用しなくなり、代わりに Assertion Consumer Service Index URL を使用します。 （注） リダイレクトまたは POST バインディングのいずれかを経由して、認証要求を IdP に送信でき、アサーションをサービス プロバイダに送信できます。たとえば、Cisco Unified Communications Manager は、いずれかの方向の POST バインディングをサポートしています。
3	サービス プロバイダは、要求をブラウザにリダイレクトします。 （注） IdP の URL は、SAML メタデータ交換の一部として、サービス プロバイダで事前設定されます。
4	ブラウザはリダイレクトに従い、IdP に HTTPS GET 要求を発行します。SAML 要求は、GET 要求でのクエリ パラメータとして維持されます。
5	IdP は、ブラウザとのセッションが有効であることを確認します。
[6]	ブラウザとの既存の cookie がない場合、IdP はブラウザへのログイン要求を生成します。また、IdP で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、お客様のセキュリティ要件と認証要件によって決定されます。これは、ユーザ名とパスワード、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	ユーザは、必要な資格情報をログイン フォームに入力し、IdP に POST 形式で戻します。 （注） ロギング対象となる認証チャレンジは、ブラウザと IdP の間です。サービス プロバイダは、ユーザ認証に関わりません。
8	IdP は、LDAP サーバに資格情報を送信します。
9	LDAP サーバは、資格情報のディレクトリを確認し、IdP に検証ステータスを返信します。
10	IdP は、資格情報を検証し、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 よりデジタル署名され、ユーザはサービス プロバイダが保護するリソースにアクセスできるようになります。IdP は、そのクッキーもここに設定します。
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、非表示フォームの POST 指示に従い、サービス プロバイダの ACS URL に POST 形式でアサーションを送信します。

13	サービス プロバイダは、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 プロバイダは、保護されたリソースへのアクセス権を許可し、ブラウザに 200 OK で返答することで、リソースの内容を提供します。 （注） サービス プロバイダは、そのクッキーをここに設定します。ブラウザがその他のリソースの要求を続けて行う場合、ブラウザはサービスプロバイダのクッキーを要求に加えます。サービス プロバイダは、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 ブラウザにリソースの内容が戻されます。