# Cisco DNA Spaces を使ってみる

この章では、Cisco Digital Network Architecture（DNA）Spaces の概要、その機能、プロセスフロー、ライセンスパッケージ、およびCisco DNA Spaces のシステム要件について説明します。

この章は、次の項で構成されています。



## Cisco Spaces の概要

Cisco Spaces は、物理的なビジネス拠点にいる訪問者を把握し、訪問者とつながり関与することを可能にするマルチチャネル エンゲージメント プラットフォームです。

Cisco Spaces は、顧客が大規模なビジネス成果を達成できるようにする、業界で最も拡張性のあるエンドツーエンドの屋内ロケーション サービス クラウド プラットフォームです。包括的なサービススイートにより、すべてのロケーションベースのニーズに向けた強力なソリューションを提供します。

Cisco Spaces また、施設内の資産を監視および管理するためのソリューションも提供します。

次のようなさまざまな業種（分野）が対象です。

- 小売
- manufacturing
- サービス業
- ヘルスケア
- 教育（Education）
- 金融サービス

- 企業ワークスペースなど。

Cisco Spacesを使用すると、ユーザーは、統合されたダッシュボード インターフェイスを介して、すべてのロケーションテクノロジーとインテリジェンスに一か所からアクセスできます。既存の Cisco Aironet、Cisco Catalyst、および Cisco Meraki インフラストラクチャとの互換性を考慮して設計された Cisco Spaces は、ロケーションベースのサービスニーズに合わせた汎用性の高いソリューションとして優れています。

# シスコ フェデレーション プロセス

シスコフェデレーションプロセスにより、外部パートナー組織とのシングルサインオン（SSO）統合が可能になります。これにより、セキュリティ境界を維持しながら、シームレスな認証が可能になります。このシステムでは、シスコの CCI-Okta インフラストラクチャを使用して、外部のアイデンティティ プロバイダー（IdP）とフェデレーションします。

主な利点

- **セキュリティの強化**：パスワードはパートナードメインから出ることはなく、シスコがパスワードにアクセスすることも、保存することもありません。
- **シームレスなユーザー体験**：シスコアプリケーション間でのシングルサインオン
- **ジャストインタイムプロビジョニング**：最小限の必要属性による自動ユーザープロビジョニング
- **フレキシブル認証フロー**：ユーザー認証のための複数のエントリポイント

### Cisco Customer Identity の統合

Cisco Customer Identity（CCI）は、 Cisco Spaces アプリケーション全体でユーザーのセキュリティとアクセス性を向上させる統合認証プラットフォームです。これは、個々のアプリケーション固有のアイデンティティ プロバイダー（IdP）を置き換える共通の認証レイヤとして機能し、ユーザーアクセスを合理化して、セキュリティ管理を向上させます。

従来のオンボーディングでは、Cisco Spaces にさまざまな IdP が使用されていたため、他のアプリケーションを有効にするときに課題がありました。Cisco Customer Identity（CCI）には、CCI以外の顧客に対する将来の統合課題を回避するための共通の認証インターフェイスが用意されています。進化するシスコ製品エコシステムとの互換性を確保するには、ユーザーはCCI統合への移行が求められます。

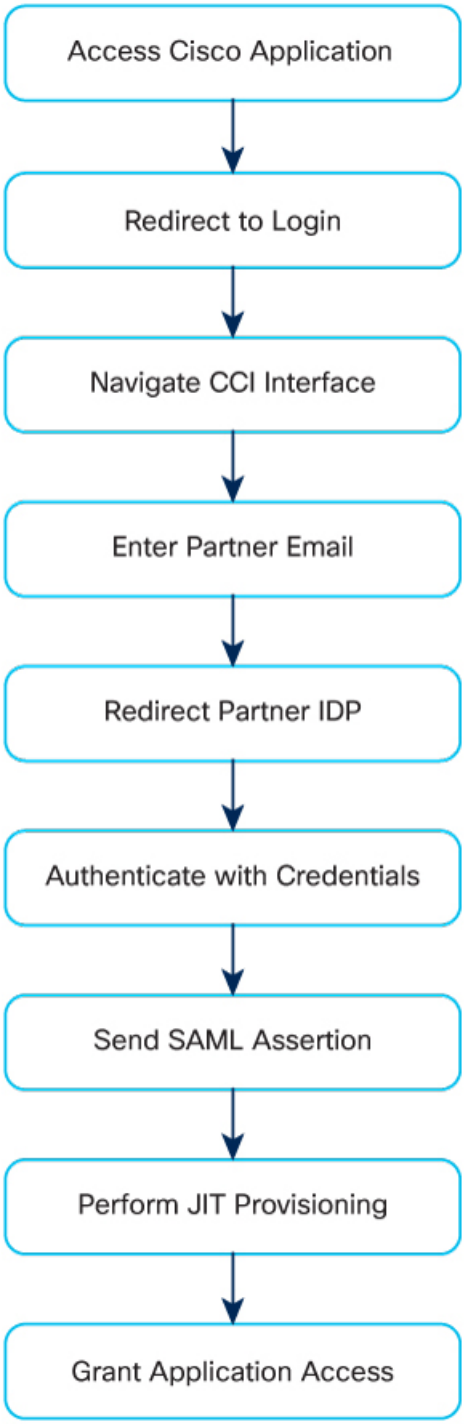
CCI の統合により、すべてのシスコアプリケーションのユーザー認証が一元化されるため、一貫したセキュリティポリシーが保証され、ユーザーの管理が簡素化されます。このアプローチは将来の拡張性をサポートし、認証を CCI に依存する追加のシスコ製品のシームレスなアクティブ化を可能にします。

主要な属性：

- 承認された電子メールドメイン（@abc.comなど）を持つユーザーに、すべてのシスコURLでシングルサインオン（SSO）エクスペリエンスを提供します。

- レガシーまたは個々のアプリケーション IdP を置き換えて、フラグメンテーションと複雑さを回避します。
- 顧客の IdP とシスコの間でのメタデータ交換を使用した SAML ベースの認証をサポートします。
- SAML 応答には、firstName、lastName、email、company、countryCode などの必須ユーザー属性が必要です。
- 認証のみのワークフローと、認証と承認の複合ワークフローの両方を容易にします。

*Figure 1:* 認証ワークフロー



# Cisco Customer Identity を使用した SSO のセットアップ

組織のアイデンティティ プロバイダーを Cisco Customer Identity（CCI）と統合することにより、指定されたドメインのユーザーに対してすべてのシスコアプリケーションでシングルサインオン（SSO）を有効にします。この統合認証により、ユーザー体験が向上し、アプリケーションセキュリティが強化されます。

シスコアプリケーションに一元化された認証が必要な場合は、このタスクを使用します。SSO のセットアップは、個々のアプリケーションレベルではなく、シスコドメインレベルで実行されるため、組織内のすべてのユーザーに一貫性のある安全なアクセスが提供されます。シスコの SSO イネーブルメントチーム と連携して、必要なメタデータと証明書を交換することにより、SSO が確実に機能し、組織のセキュリティ要件を満たします。

**Before you begin**

次の要件が満たされていることを確認します。

- **CCI-Okta**：シスコのアイデンティティプロバイダー
- **フェデレーション パートナー ドメイン**：外部組織のアイデンティティ プロバイダー
- **保護対象アプリケーション**：認証を必要とするシスコのアプリケーション
- **SAMLプロトコル**：セキュア認証メッセージング

SSO を設定するには、次の手順を実行します。

**Procedure**

**ステップ 1** ユーザーとして、次の詳細またはメタデータファイルを用意して、Cisco Spaces SSOイネーブルメントチームが SSO 統合できるようにします。

- **SubjectNameID**： キーアカウントリンク属性（通常はユーザーの電子メール）。
- **リモートIDP発行者のURI**：顧客の IdP の SAML メタデータ EntityID。
- **リモートIDPシングルサインオンURL**： CCI から SAML 認証要求を受信するエンドポイント。
- **リモートIDP署名証明書**：SAML 署名を検証するための公開キー証明書（PEMまたはDER）。

**ステップ 2** シスコから次の詳細情報が返ります。

- **Assertion Consumerサービス URI**：認証後に SAML アサーションを受信するエンドポイント。
- **Audience URI**：IdP のシスコのエンティティ記述子。
- **SP署名証明書**：認証リクエストの署名を検証するための公開キー証明書。

**ステップ 3** 応答で、シスコに次の必須属性を提供します。

- firstName
- lastName
- email
- company（会社名）
- countryCode （US、UK、BE、JP などの 2 文字コード）

### 標準的なフェデレーションユーザージャーニー

1. 認証が必要なシスコアプリケーションに移動します。アプリケーションはCCI/Okta セキュリティレイヤによって保護されています。
2. ログインプロセスを開始するには、[ログイン（Login）]をクリックします。システムにより認証フローにリダイレクトされます。
3. [CCIログイン（CCI Login）] ウィンドウに、パートナー組織のドメインに属する電子メールアドレス（`username@PartnerDomain.com`形式）を入力します。この電子メールドメインは、フェデレーションのセットアップで事前に設定されている必要があります。

**Note** システムにより、電子メールからパートナードメインが自動で検出され、組織のフェデレーション パートナー ドメイン ログインページ（ホーム組織のアイデンティティプロバイダー（IdP））にリダイレクトされます。

4. 組織のログインページで、自分のユーザー名とパスワードを入力します。必ず自組織のシステムに通常使用しているものと同じログイン情報を使用します。
5. 追加の認証要件（MFA が設定されている場合）を完了します。

**Note** 認証に成功すると、自動で CCI にリダイレクトされます。組織の IdP は、セキュアな SAML アサーションを CCI に送信して、ユーザーのアイデンティティを確認します。

6. CCI により認証が処理され、元のシスコアプリケーションにリダイレクトされます。アプリケーションは認証ステータスの確認を受信します。
7. アクセスが許可され、認証が完了します。アプリケーションのトップページに正常にランディングされます。権限設定に基づいて、アプリケーションへのフルアクセスが利用できるようになりました。

# Cisco Spaces 用シングル サインオン

Cisco Spaces ではシングルサインオン（SSO）がサポートされているため、ユーザーは SSO 資格情報を使用して Cisco Spaces にログインできます。たとえば、シスコのドメインで SSO が有効になっている場合、Cisco Spaces アカウントを持つシスコの従業員は、シスコの電子メールアドレスとパスワードを使用して Cisco Spaces にアクセスできます。さらに、シスコの従業員が他のシスコの Web サイトまたはアプリケーションを介してシスコドメインにすでにログインしている場合、そのシスコの従業員は、シスコの電子メールアドレスを指定するだけで Cisco Spaces にアクセスできます。

[Login] ボタンをクリックすると、[e-mail ID] フィールドのみが [Login] ウィンドウに表示され、あわせて [Continue] ボタンが表示されます。ユーザーがすでに SSO が有効なドメインにログインしている場合、[Continue] ボタンをクリックすると直接 Cisco Spaces ダッシュボードに移動します。Cisco Spaces アカウントが複数の顧客名をサポートしている場合は、[Select Customer] ウィンドウが表示されます。ユーザーがドメインにログインしていない場合、ログイン認証のために IDP ページにリダイレクトされ、SSO 資格情報を指定してログインできます。

- アカウント名
- SSO を有効にする必要があるドメイン名
- Application Name
- SSO のタイプ：現在、SAML のみがサポートされています。
- 認証のみが必要か、または認証と承認の両方を有効にする必要があるか。これは、authenticateOnly フラグを True または False に設定することで指定します。
  - True：ユーザーに対して認証のみが有効になります。
  - False：ユーザーに対して認証と承認の両方が有効になります。

（注）

- **authenticateOnly** を **`False`** に設定した場合、以下が必要になります。
  - ユーザーの詳細を送信するときに IDP から追加情報を渡す必要があります。たとえば、role =dnaspaces:174923535949:Dashboard_Admin などです。
  - **role** の値は必須であり、ユーザーの詳細を送信するときに IDP で使用可能である必要があります。
  - **Cisco Spaces ダッシュボード** > **[管理者管理（Admin Management）]** から個々のユーザーを招待する必要はありません。ユーザー招待とアクティブ化は、特定の顧客 IDP および Cisco Spaces による認証プロセスと承認プロセスの両方に基づきます。

    Cisco Spaces ダッシュボードの既存のデフォルトロールを使用するか、Cisco Spaces ダッシュボードで新しいロールを作成し、その特定のロール名を使用できます。

    カスタムロールを使用する場合は、**Cisco Spaces** > **[管理者管理（Admin Management）]** > **[ロール（Roles）]** でカスタムロールを作成し、IDP 応答で **role** 文字列値としてロール名を渡します。

- metadata.xml ファイルからの次の情報：
  - SSO の詳細
  - エンティティ
  - エントリポイント
- Entity ID
- 応答 URL（Assertion Consumer Service の URL とも呼ばれます）
- 次の情報を含むシスコのメタデータファイル：

IDP メタデータは、次のように **firstName**、**lastName**、および **email** フィールドを返すように設定する必要があります。

```
nameid-format:"emailAddress","firstName":"Jane","lastName":"Doe","phone":"9876543210","level":"info","
```

# Cisco Spaces のアイドル タイムアウト

# Cisco DNA Spaces ドキュメント

Cisco DNA Spaces ダッシュボードの右上に表示される [Cisco DNA Spaces Support] アイコン（  ）を使用して、コンフィギュレーション ガイドやリリースノートを含む Cisco DNA Spaces のドキュメントにアクセスできます。

[Spaces LaunchPad] セクションから、ドキュメント、発表、導入ガイド、ユースケース、サポート情報を表示することもできます。これを行うには、Cisco DNA Spaces UI の右下にある [Spaces LaunchPad] アイコンをクリックします。

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。

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。

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。