

# サイボウズのクラウドサービス基盤 「cybozu.com」との認証連携方法

## はじめに

本レポートでは、サイボウズのクラウドサービス基盤である「cybozu.com」とHP IceWall SSOとの認証連携方法と、その検証結果に関して記述します。

## cybozu.comとは？

cybozu.comはグループウェア/コラボレーションソフトを開発・販売するサイボウズ株式会社の提供するクラウドサービス基盤です。情報セキュリティマネジメントシステム (ISMS) を構築し、クラウドサービス基盤 (サーバー及びOS) の運用について、ISO/IEC 27001:2005 の認証を取得しています。(認証番号: IS 577142 認証登録日: 2011/11/10)

## cybozu.comの特徴

### すぐにつかえる

お申し込み後、すぐに利用が開始できます。  
お申し込みから最短5分でお客専用環境を用意し、必要な時にすぐに利用開始できます。また、各サービスの画面は社員全員が使えるように設計されており、導入したその日から運用開始することが可能です。

### モバイル対応

複雑なネットワーク設定や追加料金なしで、スマートフォンやタブレットなどモバイル端末からの接続を行います。スマートフォン向けには、専用アプリケーション「サイボウズ KUNAI」を用意。快適な操作性で、スケジュールやワークフロー機能を利用できます。

### 安心のクラウドサービス

常に最新バージョンのサービスをサイボウズが管理するデータセンターでご利用いただけます。バックアップや障害対応など、サーバーの運用作業は不要です。バックアップや冗長化をデータセンターに任せることで、データ消失などのリスクも低減できます。

## cybozu.com でSAMLの認証連携ができるメリット

業務用のアプリケーションが社内に複数存在する場合、シングルサインオンを導入することがあります。近年クラウドサービスが普及し、社内環境と社外にあるクラウド環境といったようにネットワークをまたぐ複数の環境を利用することが増えています。

「cybozu.com」の提供するグループウェア機能は、企業内の情報系システムの入り口として利用頻度が高く、認証を簡略化させることによって利用促進を図ることができます。

SAMLはB2Bサービスにおける認証技術のデファクトスタンダードとなっています。SAMLをサポートすることで、上述のような社内とcybozu.comとのシングルサインオンを実現することができると同時に、多様なサービスとのシングルサインオンを可能にしています。

## SAMLとは？

Security Assertion Markup Language (SAML) とは、異なるセキュリティドメイン間で認証情報を連携するための、XMLベースの標準仕様です。SAML認証を設定すると、社内のIdentity Provider (IdP) に登録されたユーザーアカウントで、cybozu.comにシングルサインオン (SSO) できます。cybozu.comはSAML 2.0に対応し、Service Provider (SP) として動作します。

ここではSAML認証を使用したSSOの流れ、およびcybozu.comの設定手順を説明します。

本ページでは、構築済みのIdPとしてHP Ice Wall SSO とcybozu.comをSAML認証で連携する方法を説明します。

## SAML認証を使用したSSOの流れ

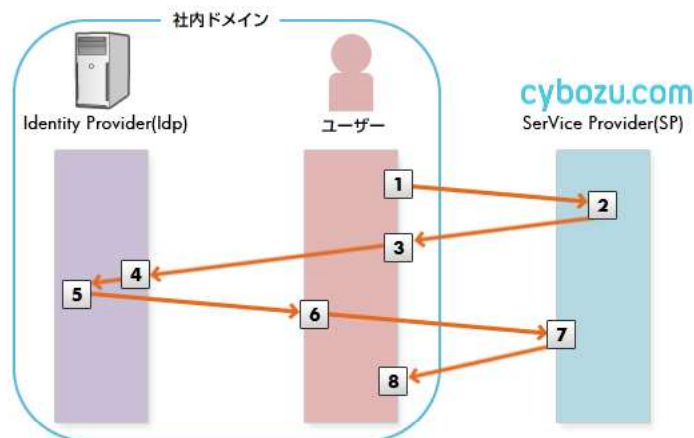
SAML認証を有効にすると、cybozu.comはSP InitiatedなSSOを行います。

SAMLリクエストとSAMLレスポンスには、次のバインディングを使用します。

SAMLリクエスト: HTTP Redirect Binding

SAMLレスポンス: HTTP POST Binding

cybozu.comがユーザーを認証する流れは、次のとおりです。



1. ユーザーがcybozu.comにアクセスする。
2. cybozu.comがSAMLリクエストを生成する。
3. ユーザーが、SPからSAMLリクエストを受け取る。
4. IdPがユーザーを認証する。
5. IdPがSAMLレスポンスを生成する。
6. ユーザーが、IdPからSAMLレスポンスを受け取る。
7. cybozu.comがSAMLレスポンスを受け取り、検証する。
8. SAMLレスポンスの内容に問題がない場合は、ユーザーがcybozu.comにログインした状態になる。

IdPとcybozu.comをSAML認証で連携するには、IdPとcybozu.comの両方で設定を行います。

#### IdPにcybozu.comを登録する

cybozu.comをSPとして設定するため、IdPに次の情報を登録します。

IdPとなるHP IceWall Federationでの設定方法は後述しますが、ここでは登録に必要な情報を記述します。

- cybozu.comのエンドポイントURL: `https://(お客様が指定したドメイン名).cybozu.com/saml/acs`
- エンティティID: `https://(お客様が指定したドメイン名).cybozu.com`  
URLの最後に"/" (スラッシュ) をつけないでください。
- ユーザーを識別する要素: NameID

cybozu.comをSPとして登録する際に、メタデータファイルを使用することもできます。

メタデータファイルを入手するには、「cybozu.com共通管理」の「ログインのセキュリティ設定」画面で「SAML認証を有効にする」を選択し、「Service Providerメタデータのダウンロード」をクリックします。

#### ■ cybozu.comでSAML認証を設定する

cybozu.comでSAML認証を有効化し、IdPの情報を設定します。

手順:

1. 「cybozu.com共通管理」画面の「セキュリティ」の「ログイン」をクリックします。
2. 「SAML認証を有効にする」を選択します。
3. 必要な項目を設定します。
  - Identity ProviderのSSOエンドポイントURL(HTTP-Redirect) SAMLリクエストの送信先を設定します。
  - cybozu.comからのログアウト後に遷移するURL cybozu.comからログアウトした後に表示される、IdPのURLを設定します。
  - Identity Providerが署名に使用する公開鍵の証明書  
RSAかDSAのアルゴリズムで生成された、公開鍵の証明書ファイルを添付します。  
X.509形式の証明書のみ利用できます。
4. [保存]をクリックします。
5. SAML認証を使用してログインするユーザーのログイン名を確認します。cybozu.comのユーザーのログイン名に、NameIDに関連付けた値が登録されているかどうかを確認します。
6. SAML認証を使用してcybozu.comにSSOできるかどうかを確認します。次の操作ができれば、設定は完了です。
  - cybozu.comにアクセスすると、IdPの認証に成功し、ログイン後の画面が表示される。
  - ログイン後の画面で、右上のユーザー名 > [ログアウト]の順にクリックすると、正常にログアウトできる。

#### ■ HP IceWall Federation を設定する

IdP側として、HP IceWall SSOのバックエンドに配置したHP IceWall Federationで、cybozu.comの情報を設定します。

事前準備:

「HP IceWall Federation Version 3.0 導入ガイド」に従って、IWFA 連携モジュールが導入されているものとします。

手順:

「HP IceWall Federation Version 3.0ユーザーズマニュアル」に従って、必要な項目を設定します。以下の設定例では、HP IceWall SSOにログインするユーザーのログイン名をNameIDにて、cybozu.comのユーザーのログイン名と関連付けるようにしています。

環境に応じて、IWFA 連携モジュール設定ファイル(iwidp.conf)の以下の値を編集します。詳細については「HP IceWall Federation Version 3.0 リファレンスマニュアル」を参照してください。

Identity ProviderのエンティティIDを設定します。

ISSUER= `https://(IceWall Federationのドメイン名)`

例: `https://sso.yourcompany.com`

Service ProviderのエンティティIDを設定します。

SP\_ENTITY\_ID=`https://(お客様が指定したドメイン名).cybozu.com`

URLの最後に"/" (スラッシュ) をつけないでください。

Service ProviderのSSOエンドポイントURL(HTTP-POST) SAMLレスポンスの送信先を設定します。

ACS\_URL= `https://(お客様が指定したドメイン名).cybozu.com/saml/acs`

#### ■ アクセス方法

ユーザーがHP IceWall SSOにログインしていない状態でcybozu.comにアクセスする場合、`https://(お客様が指定したドメイン名).cybozu.com/` にアクセスすると自動的にHP IceWall SSOのログイン画面が表示されます。ログイン・パスワードを入力して認証が完了すると自動的にcybozu.comの画面に移行し、サービスを利用することができます。

ユーザーが先に他のアプリケーションを使用していて、HP IceWall SSOへのログインが完了している状態でcybozu.comにアクセスすると、ログイン画面が表示せずそのままcybozu.comを使用できます。

cybozu.comに関するお問い合わせ

サイボウズ株式会社 インフォメーションセンター

[contactus@cybozu.co.jp](mailto:contactus@cybozu.co.jp)

※HP IceWall Federation の設定方法やHP IceWall SSOについてのお問い合わせは[こちら](#)をご覧ください。