cybozu.com と Horizon Workspace の SAML 連携環境構築

テクニカルホワイトペーパー

サイボウズ株式会社

cybozu.com

ヴイエムウェア株式会社

vmware®

目次

1　はじめに

本書は、国内グループウェア市場で国内最大シェアを持つサイボウズ社が提供するクラウドサービスである cybozu.com と、VMware Horizon Workspace を SAML 連携させるために必要な手順について記載したドキュメントです。

SAML とは Security Assertion Markup Language の略で、クラウドサービスとの認証連携で用いられる業界標準的な認証の仕組みです。Identity Provider となる Horizon Workspace、Service Provider となる cybozu.com の双方のプロダクトが SAML 連携出来る準備が整ったことから、その容易な設定手順を広く展開することを目的に作成しました。

2　製品紹介

2.1　cybozu.com

「cybozu.com」は、サイボウズ社が独自に開発したクラウド基盤です。国内シェア No.1 グループウェア「サイボウズ Office」をはじめ、大企業ニーズに合わせた管理機能を備えたエンタープライズグループウェア「Garoon」や業務に必要なアプリケーションをノンプログラミングで素早く作れる「kintone」等の企業向けのアプリケーションを提供しています。
近年、仮想化等の技術革新やネットワークインフラの整備が進み、クラウドサービスを導入する企業が増加しています。そして、クラウドサービスにはバックアップや障害対応、ソフトウェアのアップデートといったシステム運用コストの削減、ハードウェアの購入や構築にかかる初期導入期間の短縮などが期待されています。「cybozu.com」ではバックアップやデータ保全にかかる運用の自動化をしてヒューマンエラーの発生を防ぐとともに、オペレーションの効率化を行い、効率的なシステム運用をサポートしています。
また、安全にクラウド環境をご利用いただくため、IP アドレス制限や証明書などによる接続元の認証と ID＋パスワードなどによる認証のツーファクタ認証を採用しております。常時 SSL や、IP アドレス制限、BASIC 認証、サブドメイン発行などは標準でご利用いただけます。

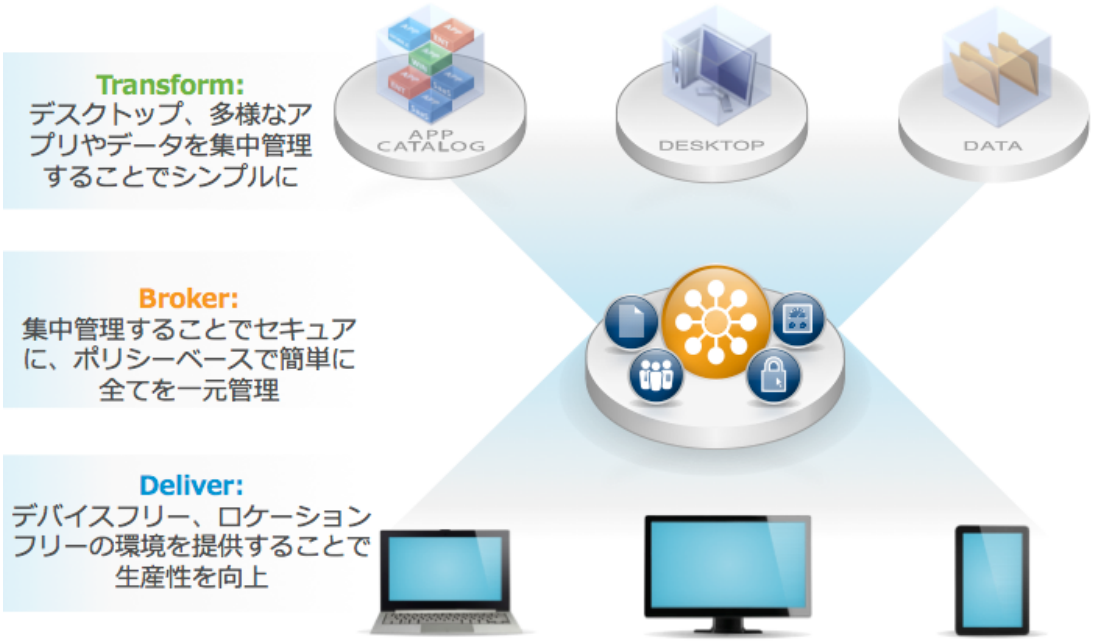
2.2 VMware Horizon Workspace

スマートフォンやタブレットによって、業務のやり方が変わりつつあります。企業が提供する PC に縛られることなく、従業員は状況に応じて最も便利なデバイスで作業できる環境にあります。企業の IT 部門が、従業員が望むデバイスにアプリケーションを提供できなかった場合、従業員は外部の一般的なソリューションを使用するため、セキュリティと管理性に影響が及びます。このような新しいモバイル環境によって、IT 部門の責任者は多くの課題に直面することとなりました。複数のデバイスに複数のアプリケーションを提供するだけでなく、完全なセキュリティ保護と高可用性を実現する必要があるからです。このような要件を満たそうとすると、単体のソリューションを複数寄せ集めることになり、最終的に企業のコストと複雑性が増大します。それぞれのソリューションは問題の一部を解決しますが、すべての問題に対応するものではありません。

Horizon Workspace は、アプリケーションやデータを 1 つのワークスペースに統合することで、IT 部門によるモバイル エンド ユーザーの管理を効率化します。このワークスペースには必要なデータやアプリケーションが含まれているため、従業員がどこで作業しようとも、生産性が低下することはありません。管理者にとっては、管理項目が減少し、容易になります。エンドユーザーは、時間や場所を問わずワークスペースにアクセスできるため、いつでもどこでも作業できるようになります。

Horizon Workspace は、SAML 連携可能な Web アプリケーション(SaaS)、ThinApp 化した Windows アプリケーション、Mobile アプリケーションなどをアプリケーションカタログとして定義します。同じく、VMware Horizon View を用いて構築された仮想デスクトップをデスクトップサービスとして、またオンプレミス型のクラウドストレージ機能を提供するデータサービスをサービスカタログとして定義します。カタログ化した各種サービスを人に紐づく形で割り当てる Broker を介し、エンドユーザーにはデバイスフリー/ロケーションフリーで業務出来る環境を、管理者には各種サービスを統合管理出来る環境を提供します。

VMware Horizon が実現する次世代 EUC Platform



3　環境構築

本章では、Horizon Workspace と cybozu.com を SAML 連携するために必要な設定について記載します。

3.1　cybozu.com のアカウント取得

サイボウズの新しいクラウドサービス基盤をサイトからお申し込みできます。わずか数分でお客様専用の環境を用意できます。

お試し環境のお申込みページ
https://www.cybozu.com/jp/service/com/trial/

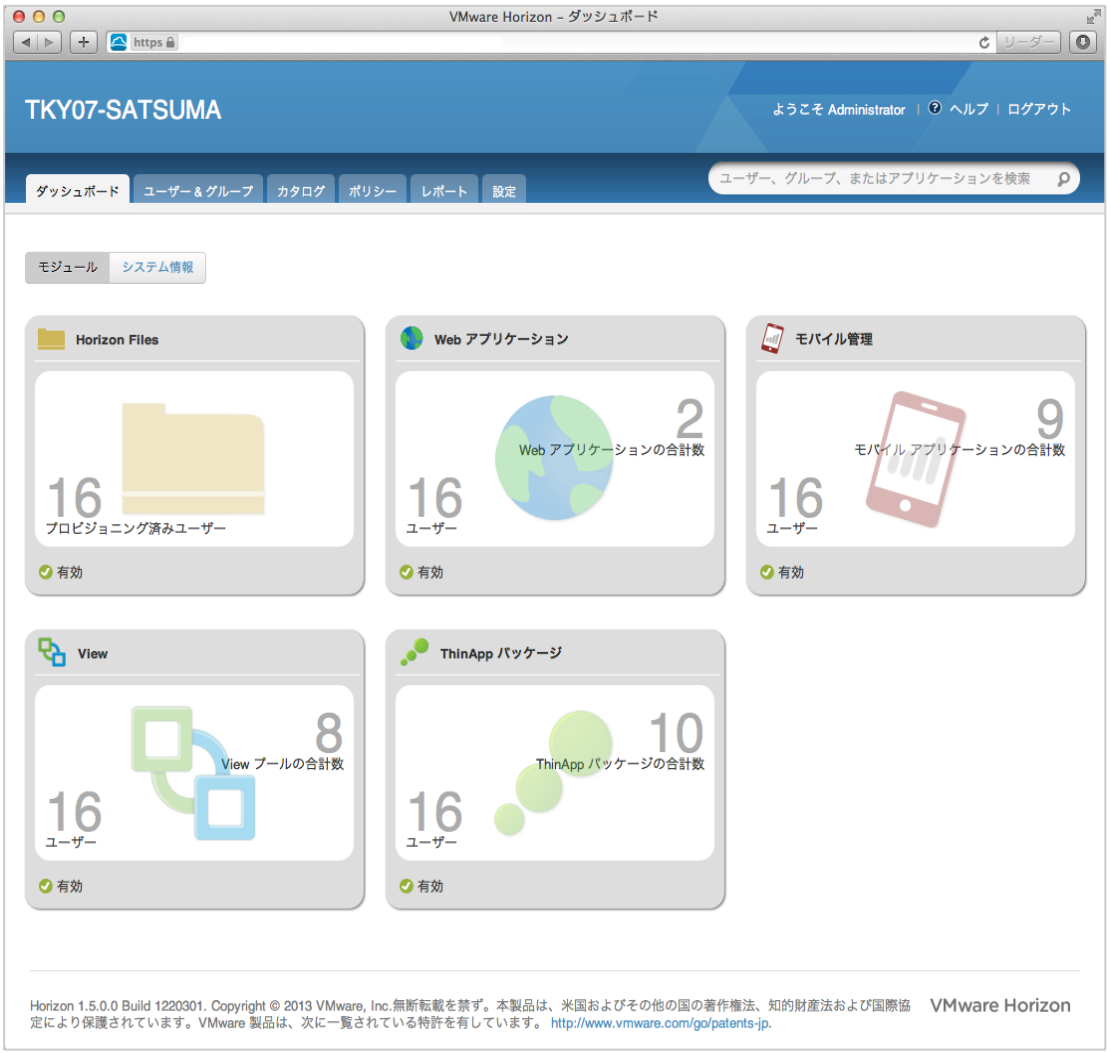
3.2　Horizon Workspace の導入

Horizon Workspace は仮想アプライアンスとして提供されています。仮想基盤として業界最大シェアを持つ vSphere で構築されたクラウド環境に、仮想アプライアンスを展開するだけで導入作業は完了します。作業手順については以下のドキュメントを参照下さい。

VMware Horizon Workspace レビューアガイド
http://www.vmware.com/go/jp-pdf-workspace-guide

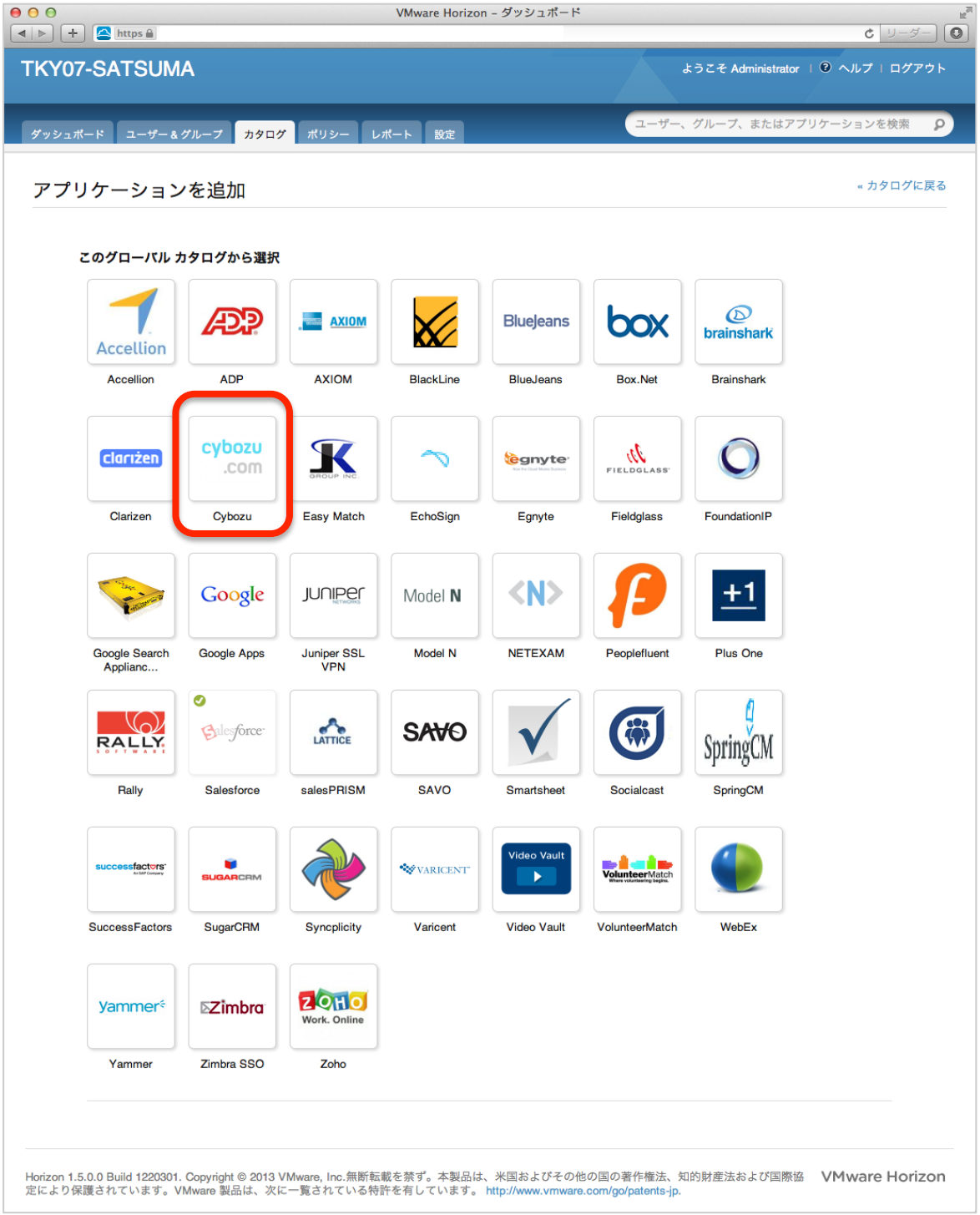
3.3　Horizon Workspace の SAML 設定

前項で導入した Workspace に管理者アカウントでログインします。



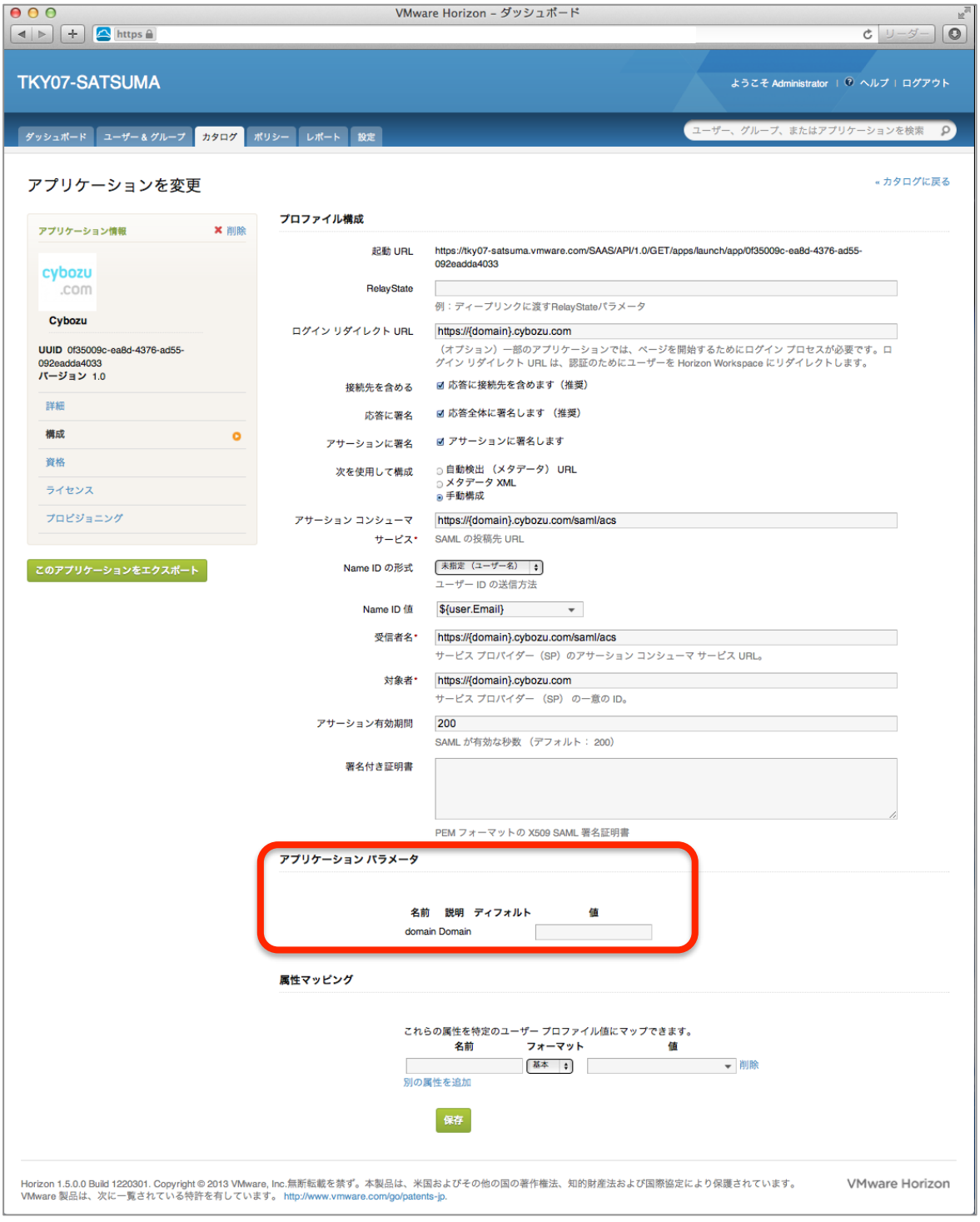
SAML 連携を行う Web アプリケーションの登録は、”カタログ”タブから実施します。”＋Web アプリケーション”ボタンをクリックした後に、”グローバル　カタログから”を選択して下さい。

グローバル カタログには、VMware が検証済の Web アプリケーション が登録されています。cybozu.com も検証済の Web アプリケーションの１つとして登録されています。cybozu.com のアイコンをクリックして下さい。



グローバル カタログに記載される Web アプリケーションは、アイコンや SAML 連携の設定などが予め登録済となっています。ユーザー環境ごとに固有となる設定情報を登録するだけで作業は終了です。それでは、”構成”をクリックして固有情報の設定を行います。

“プロファイル構成”にて、ユーザー環境ごとに固有設定となるサブドメイン情報を設定します。アプリケーション　パラメータの値に cybozu.com で割り当てられたサブドメインを入力し、最後に”保存”をクリックして下さい。入力したサブドメインの情報は、https://{domain}.cybozu.com の{domain}の文字列として使用されます(このページでは赤枠部分のみ設定が必要です)。



設定が完了すると、WEB アプリケーションの 1 つとしてカタログに登録されます。

次に、cybozu.com 側の設定で必要となる SAML 証明書を準備します。管理者画面の”設定”タブから”SAML 証明書”を選択して下さい。このページから 2 つの情報を取得します。1 つ目は cybozu.com 側の SAML 設定で必要となるログイン URL の取得です。この画面から ”ID プロバイダ(IdP)メタデータ” をクリックすると、定義情報が XML 形式で表示されます。その中から、以下の設定行の Location 以下の下線部分の情報をメモして下さい。

<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="**https://<Workspace の FQDN>/SAAS/API/1.0/POST/sso**"/>

続いて、署名書付き証明書を取得します。こちらは画面上に表示されているテキストの証明書をメモ帳にコピーペーストして、適当なファイル名（例. Idp.cer）をつけて保存して下さい。その際、” -----BEGIN CERTIFICATE-----”から” -----END CERTIFICATE-----”までの全ての文字列を保存します。

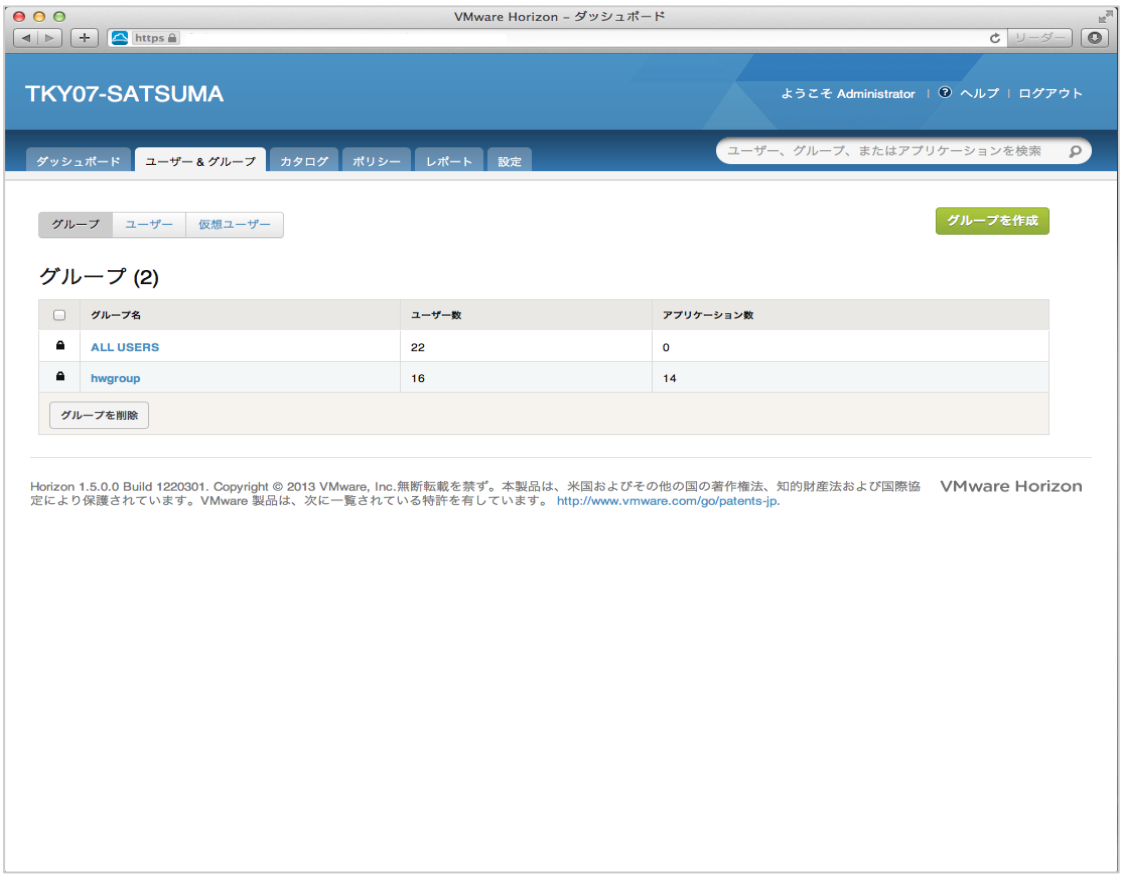
3.4　cybozu.com 側の SAML 設定

cybozu.com 共通管理に cybozu.com 共通管理者でログインし、「システム管理 > セキュリティ > ログイン」画面に移動し、「SAML 認証を有効にする」にチェックを入れて、Idp の SSO エンドポイント URL、ログアウト後に遷移する URL、署名書付き証明書を添付し、「保存」をクリックします。

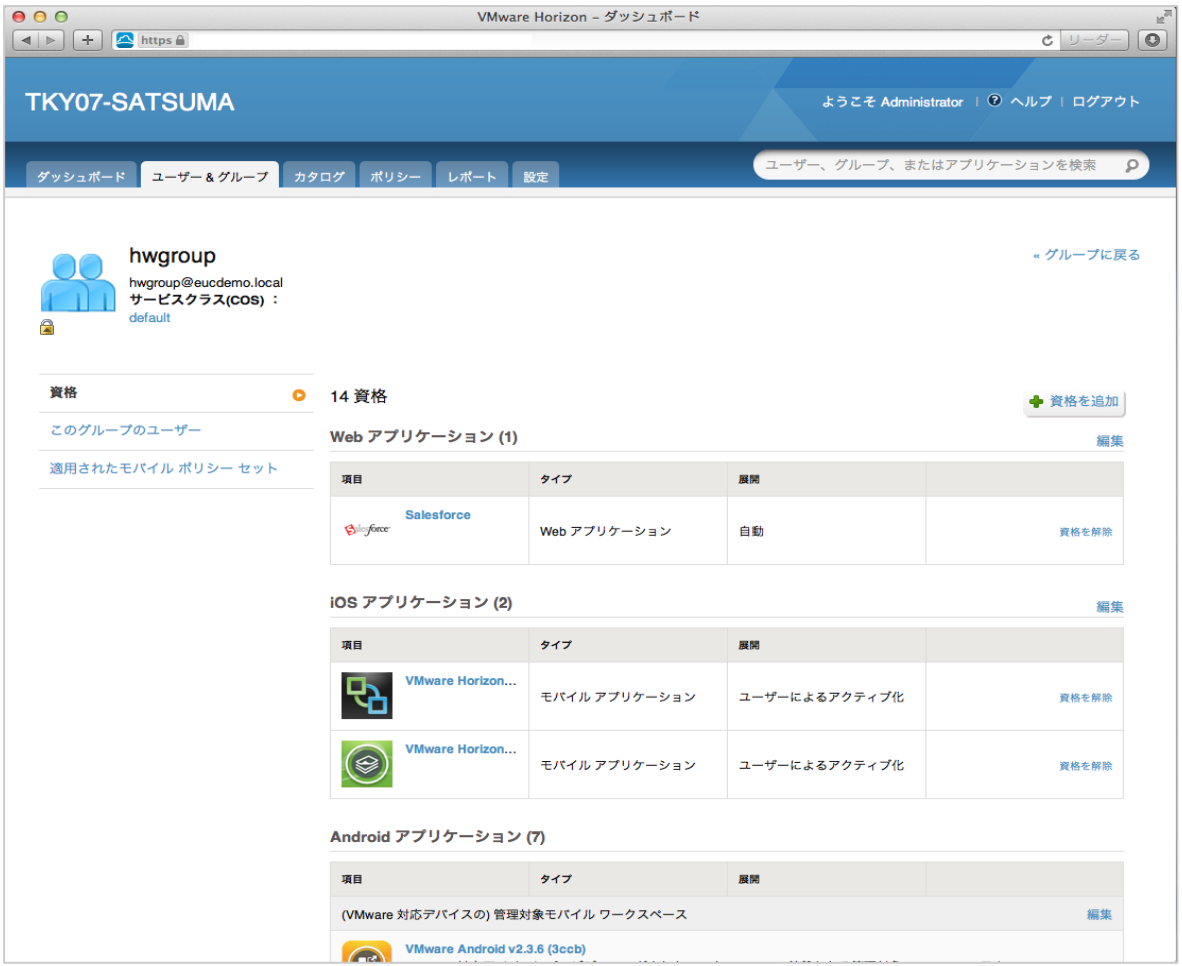
設定項目	設定内容
Identity ProviderのSSOエンドポイントURL（HTTP-Redirect）	https://<WorkspaceのFQDN>/SAAS/API/1.0/POST/sso
cybozu.com からのログアウト後に遷移する URL	https://{domain}.cybozu.com
Identity Providerが署名に使用する公開鍵の証明書	前述で保存した署名書付き証明書

3.5　ユーザーに対する cybozu.com の資格の割り当て

ここまでの設定で、Workspace と cybozu.com の間における SAML 連携設定が完了しました。最後に、Workspace の管理者画面からユーザーに対して cybozu.com を使用出来るようにする資格の割り当てを行います。 まず、”ユーザー＆グループ”タブをクリックし、資格を割り当てるグループもしくはユーザーをクリックします。



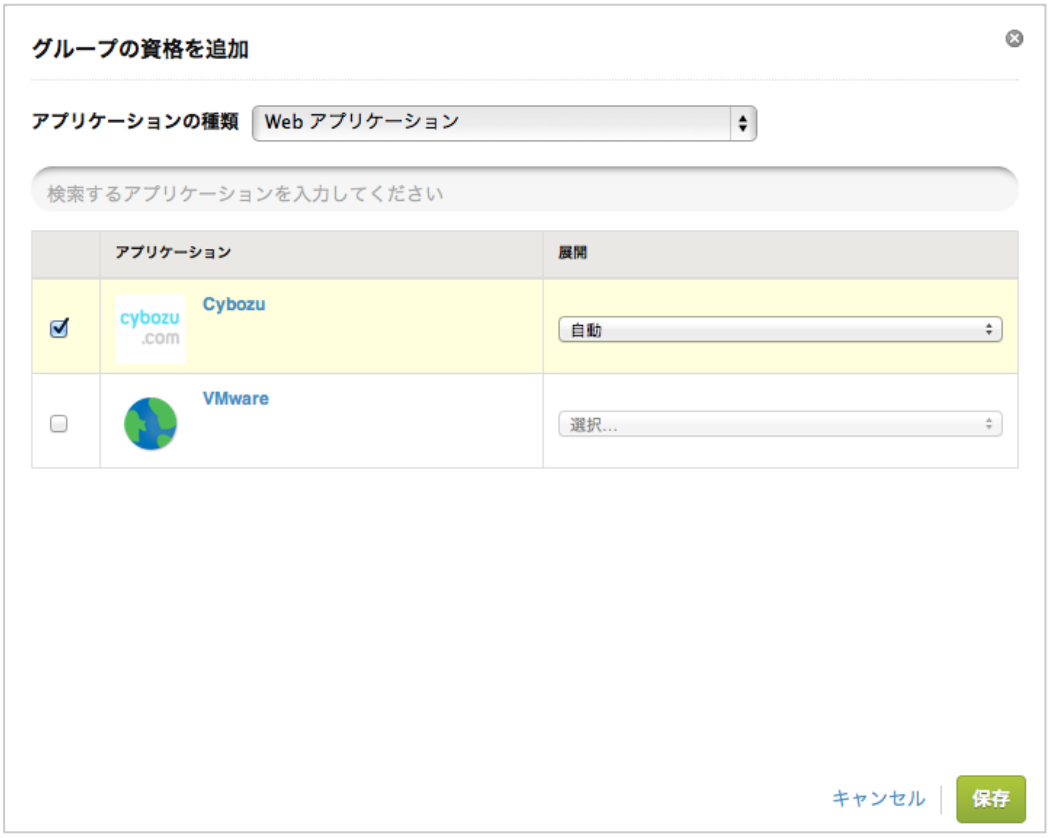
グループもしくはユーザーの資格割り当て画面にて、Web アプリケーションの”＋資格を追加”をクリックします。



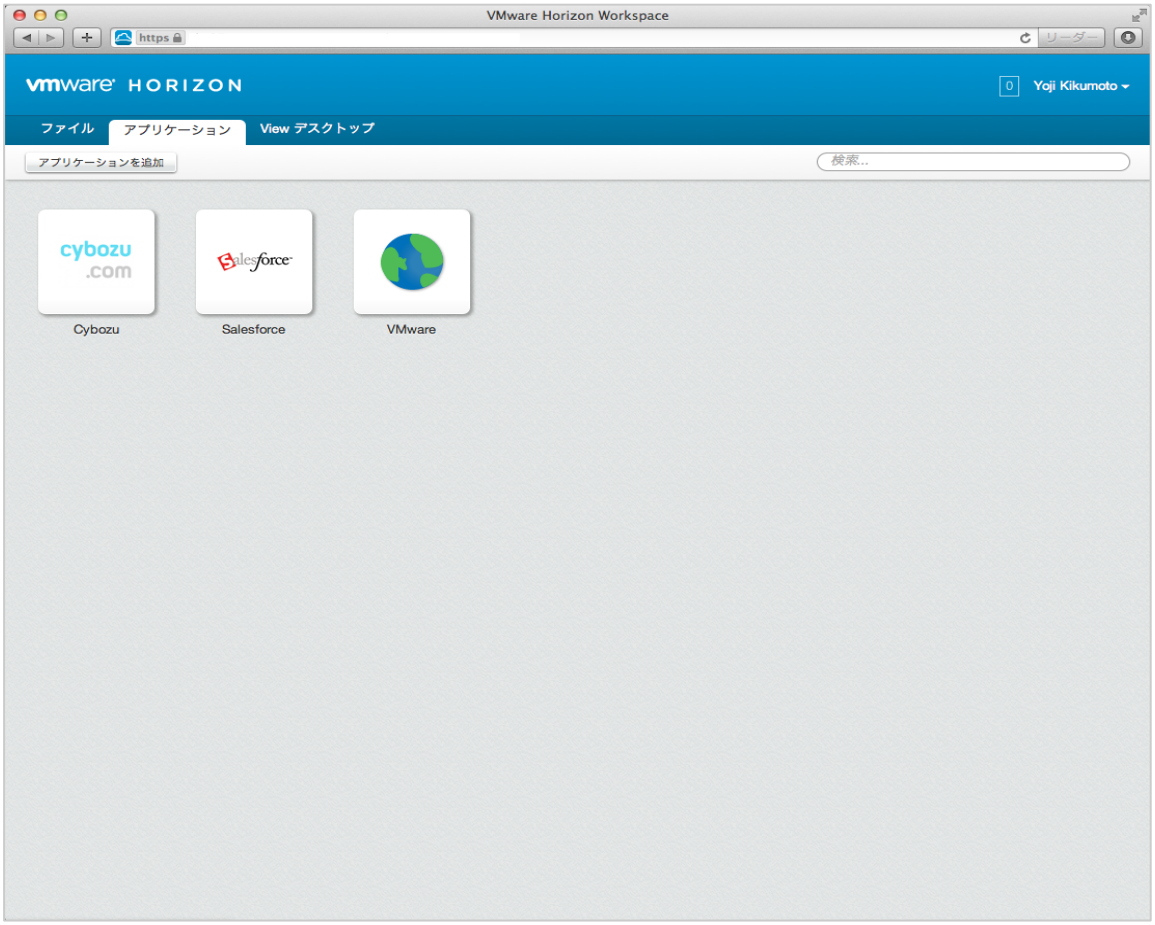
前項までに設定した”cybozu.com”がアプリケーション一覧に表示されますので、チェックボックスにチェックを入れます。展開方式には以下の 2 種類があります、要件に応じて選択下さい。最後に”保存”をクリックして資格の割り当ては終了です。

自動：ユーザーのアプリケーションカタログに管理者が強制的に割り当て

ユーザーによるアクティブ化：ユーザー自身がアプリケーションカタログから選択して使用



資格を割り当てたユーザーで Workspace にログインして”アプリケーション”タブを選択すると、以下の通り”cybozu.com”のアイコンが表示されます。



cybozu.com のアイコンをクリックして、cybozu.com に対してログインすることなくシングルサインオンできれば、次の画面が表示されます。
※利用するサービスによって表示されるサービスアイコンは異なります。

以上で cybozu.com と Horizon Workspace の SAML 連携環境構築作業は終了です。