

# 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

VMware株式会社

**vmware**<sup>®</sup>

## 目次

1	はじめに .....	2
2	製品紹介 .....	3
2.1	cybozu.com .....	3
2.2	VMware Horizon Workspace .....	4
3	環境構築 .....	6
3.1	cybozu.com のアカウント取得 .....	6
3.2	Horizon Workspace の導入 .....	7
3.3	Horizon Workspace の SAML 設定 .....	7
3.4	cybozu.com 側の SAML 設定 .....	13
3.5	ユーザーに対する cybozu.com の資格の割り当て .....	14

## 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ア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。

#### cybozu.comのサービス

シェアNo.1のグループウェア		Webデータベース	導入数No.1のメール共有
 <p>まずは手軽に使い始めたい方へ <b>サイボウズ Office</b></p>	 <p>管理機能を求める中堅・大企業向け <b>Garoon</b></p>	 <p>社内のExcelが業務アプリに <b>kintone</b></p>	 <p>このメール 対応します 前回は 山手さんが 担当してたの <b>メールワイズ</b></p>
 <p>グループウェアをスマートフォンで <b>サイボウズ KUNAI</b></p>		<b>オプション</b> <ul style="list-style-type: none"><li>セキュアアクセス</li><li>テレビ会議</li><li>ディスク増設</li><li>メールサーバー</li></ul>	<b>システム情報</b> <ul style="list-style-type: none"><li>運用環境 (SLO)</li><li>動作環境</li><li>制限事項</li></ul> <p>その他のクラウド製品</p>

## 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。

お試し環境のお申し込みページ

<https://www.cybozu.com/jp/service/com/trial/>

試用申し込み | サイボウズ製品サイト- cybozu.com

https://www.cybozu.com/jp/service/com/trial/?utm\_expId=50517813-11\_JQW59MW2TBeOvq

cybozu.com

**cybozu.com 30日間無料体験**  
30日間終了後、自動的に課金されることはありません

- 1、お試しアカウント登録
- 2、3分程度でご案内メールを送信
- 3、メール内のURLをクリックしてお試し開始！  
すべての機能をお試しいただけます。

**3min**

ストアアカウントの作成

- \* Email
- \* パスワード  
英字と数字の組合わせで、8文字以上が必要です。
- \* 確認用パスワード  
☐ 他人のお客様はチェックしてください
- \* 会社名
- \* 部門
- \* 担当者の氏名
- 電話番号

お試しになるサービス

- ☐ サイボウズ Office ☐ Kintone
- ☐ Ganson ☐ メールワIZ
- ☐ セキュアアクセス
- ☐ cybozu.com サービスご利用規約に同意する

試用開始

## 3.2 Horizon Workspace の導入

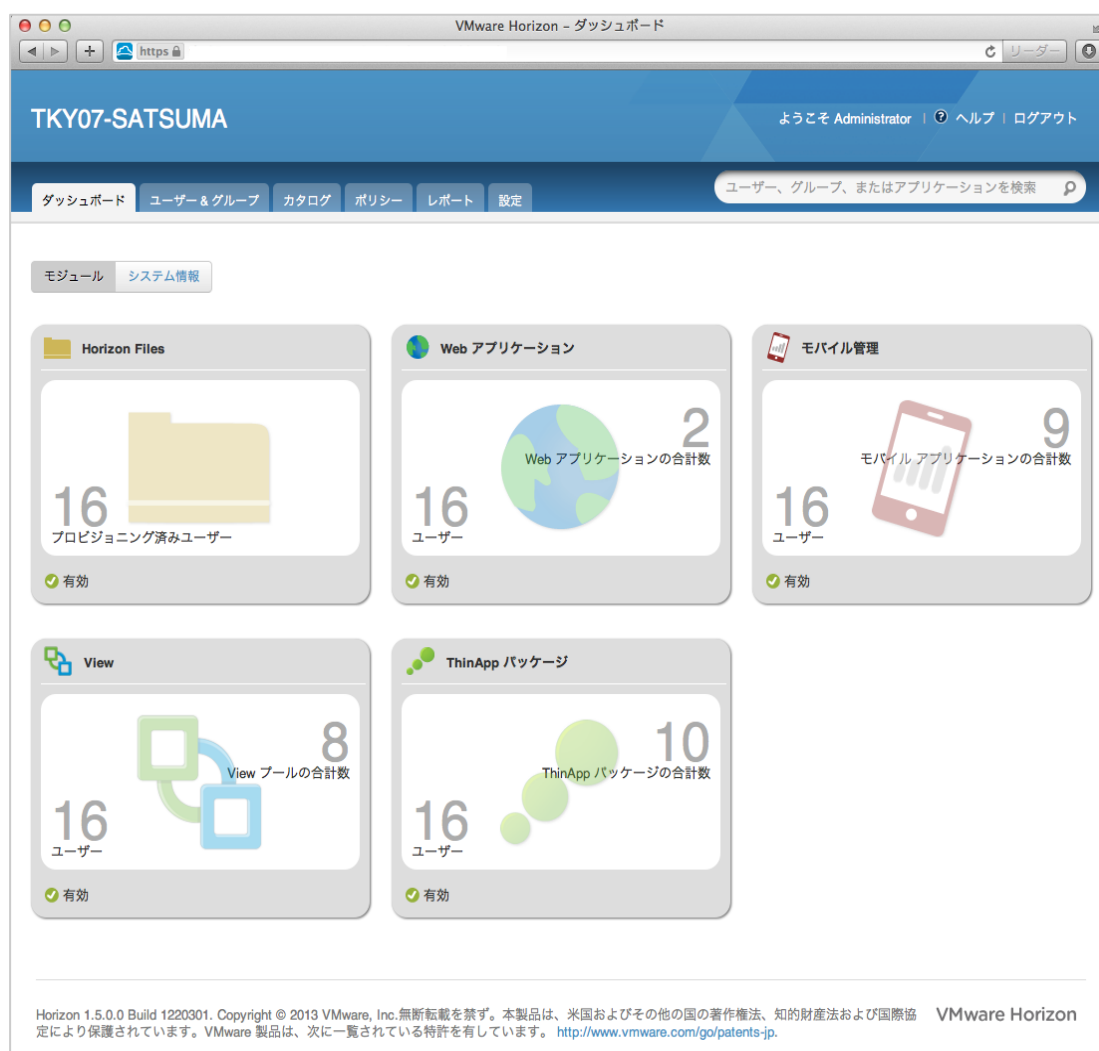
Horizon Workspace は仮想アプライアンスとして提供されています。仮想基盤として業界最大シェアを持つ vSphere で構築されたクラウド環境に、仮想アプライアンスを展開するだけで導入作業は完了します。作業手順については以下のドキュメントを参照下さい。

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。

The screenshot shows the VMware Horizon Administrator web interface. The browser address bar indicates the URL is https://. The page title is 'TKY07-SATSUMA'. The user is logged in as 'Administrator'. The navigation menu includes 'ダッシュボード', 'ユーザー & グループ', 'カタログ', 'ポリシー', 'レポート', and '設定'. A search bar is present with the text 'ユーザー、グループ、またはアプリケーションを検索'. The main content area is titled 'アプリケーションを変更' and includes a link 'カタログに戻る'. On the left, there is a sidebar for 'アプリケーション情報' (Application Information) for 'Cybozu', showing its UUID, version, and links for '詳細', '構成', '資格', 'ライセンス', and 'プロビジョニング'. The main section is '基本情報' (Basic Information) for 'Cybozu', with fields for '名前' (Name), '説明' (Description), 'アイコン' (Icon), and '認証プロファイル' (Authentication Profile). The '名前' field contains 'Cybozu'. The '説明' field is empty. The 'アイコン' field has a button 'ファイルを選択' and the text 'ファイル未選択'. The '認証プロファイル' field is set to 'SAML20'. A green '保存' (Save) button is at the bottom. At the bottom of the page, there is a footer with copyright information and the VMware Horizon logo.

VMware Horizon – ダッシュボード

TKY07-SATSUMA

ようこそ Administrator | ヘルプ | ログアウト

ダッシュボード ユーザー & グループ **カタログ** ポリシー レポート 設定

ユーザー、グループ、またはアプリケーションを検索

### アプリケーションを変更

« カタログに戻る

アプリケーション情報 ✕ 削除



**Cybozu**

UUID 0f35009c-ea8d-4376-ad55-092eadda4033  
バージョン 1.0

詳細 ➡

構成

資格

ライセンス

プロビジョニング

このアプリケーションをエクスポート

#### 基本情報

名前 \* Cybozu

説明

アイコン  ファイル未選択

認証プロファイル SAML20  
認証プロファイル

Horizon 1.5.0.0 Build 1220301. Copyright © 2013 VMware, Inc. 無断転載を禁ず。本製品は、米国およびその他の国の著作権法、知的財産法および国際協定により保護されています。VMware 製品は、次に一覧されている特許を有しています。 <http://www.vmware.com/go/patents-jp> VMware Horizon

“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(このページでは赤字部分のみ設定が必要です)。

VMware Horizon - ダッシュボード

TKY07-SATSUMA

ようこそ Administrator | ヘルプ | ログアウト

ダッシュボード ユーザー & グループ カタログ ポリシー レポート 設定

ユーザー、グループ、またはアプリケーションを検索

### アプリケーションを変更

アプリケーション情報 ✕ 削除

**cybozu**

UUID 0f35009c-ea8d-4376-ad55-092eadda4033

バージョン 1.0

詳細

構成 +

資格

ライセンス

プロビジョニング

このアプリケーションをエクスポート

### プロファイル構成

起動 URL https://tky07-satsuma.vmware.com/SAAS/API/1.0/GET/apps/launch/app/0f35009c-ea8d-4376-ad55-092eadda4033

RelayState

例：ディープリンクに渡すRelayStateパラメータ

ログインリダイレクト URL https://{domain}.cybozu.com

(オプション) 一部のアプリケーションでは、ページを開始するためにログイン プロセスが必要です。ログインリダイレクト URL は、認証のためにユーザーを Horizon Workspace にリダイレクトします。

接続先を含める ☒ 応答に接続先を含めます (推奨)

応答に署名 ☒ 応答全体に署名します (推奨)

アサーションに署名 ☒ アサーションに署名します

次を使用して構成 ☐ 自動検出 (メタデータ) URL ☐ メタデータ XML ☒ 手動構成

アサーション コンシューマ サービス https://{domain}.cybozu.com/saml/acs

SAML の投稿先 URL

Name ID の形式

ユーザー ID の送信方法

Name ID 値

受信者名 https://{domain}.cybozu.com/saml/acs

サービス プロバイダー (SP) のアサーション コンシューマ サービス URL。

対象者 https://{domain}.cybozu.com

サービス プロバイダー (SP) の一意の ID。

アサーション有効期間 200

SAML が有効な秒数 (デフォルト: 200)

署名付き証明書

PEM フォーマットの X509 SAML 署名証明書

### アプリケーション パラメータ

名前	説明	デフォルト	値
domain	Domain		<input type="text"/>

### 属性マッピング

これらの属性を特定のユーザー プロファイル値にマップできます。

名前	フォーマット	値
<input type="text"/>	<input type="text" value="基本"/>	<input type="text"/>

別の属性を追加 削除

保存

Horizon 1.5.0.0 Build 1220301. Copyright © 2013 VMware, Inc. 無断転載を禁ず。本製品は、米国およびその他の国の著作権法、知的財産法および国際協定により保護されています。 VMware 製品は、次に一覧されている特許を有しています。 <http://www.vmware.com/go/patents-jp>

VMware Horizon

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。

VMware Horizon - ダッシュボード

TKY07-SATSUMA

ようこそ Administrator | ヘルプ | ログアウト

ダッシュボード ユーザー & グループ カatalog ポリシー レポート 設定

ユーザー、グループ、またはアプリケーションを検索

### SAML 証明書をダウンロード

これは組織の SAML 署名証明書です。Application Manager から、WebEx、Google App などの証明書利用者アプリケーションへのログインの認証に使用されます。証明書利用者アプリケーションが Application Manager からのログインを受け入れることができるように、以下の証明書をコピーして貼り付け、証明書利用者アプリケーションに送信してください。

SAML 2.0 を使用するその他の証明書利用者アプリケーションと統合するには、以下のメタデータ URL を使用することもできます。

SAML メタデータ	ID プロバイダ (IdP) メタデータ	サービス プロバイダ (SP) メタデータ
有効期限	2023/07/31	
発行者	CN=Horizon SAML Self-Signed Certificate,O=TKY07-SATSUMA,C=US	

署名付き証明書

```
-----BEGIN CERTIFICATE-----
MIIDMzCCAhuGAWIBAgIBATANBgkqhkiG9w0BAQUFADBUMS0wKwYDVQQDDC
RlB3Jp
em9uIFNBTUwgU2VsZi1TaWduZWQgQ2VydGimaWNhdGUxZjAUBGNVBAoMD
VRLWTA3
LVNBVFNTUEExCzAJBgNVBAYTAiVMB4XDTExMjE1MTQ1MjE1MjE1MjE1
czMTA1
NTkxN1owVDEIMCsGA1UEAwkSG9yaXpvaW50MTU1MjE1MjE1MjE1MjE1
nR0
ZmlyYXRIMRYwFAYDVQQKDA1US1kwNy1TQVRTVU1BMQswCQYDVQGEwJV
UzCCASiw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl4C1pA/kTSt8+emJSbmZp7
osZY
NwfaSWEPlzp3/Mi+20MyzEYmXYB+4bHr0VhxtCnd8Dp7ieSseAeO18xatLrrDD6
8
-----END CERTIFICATE-----
```

Horizon 1.5.0.0 Build 1220301. Copyright © 2013 VMware, Inc. 無断転載を禁ず。本製品は、米国およびその他の国の著作権法、知的財産法および国際協定により保護されています。VMware 製品は、次に一覧されている特許を有しています。 <http://www.vmware.com/go/patents-jp>.

VMware Horizon

### 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

SAML認証 ?

☒ SAML認証を有効にする

Identity ProviderのSSOエンドポイントURL (HTTP-Redirect)

cybozu.comからのログアウト後に遷移するURL

Identity Providerが署名に使用する公開鍵の証明書

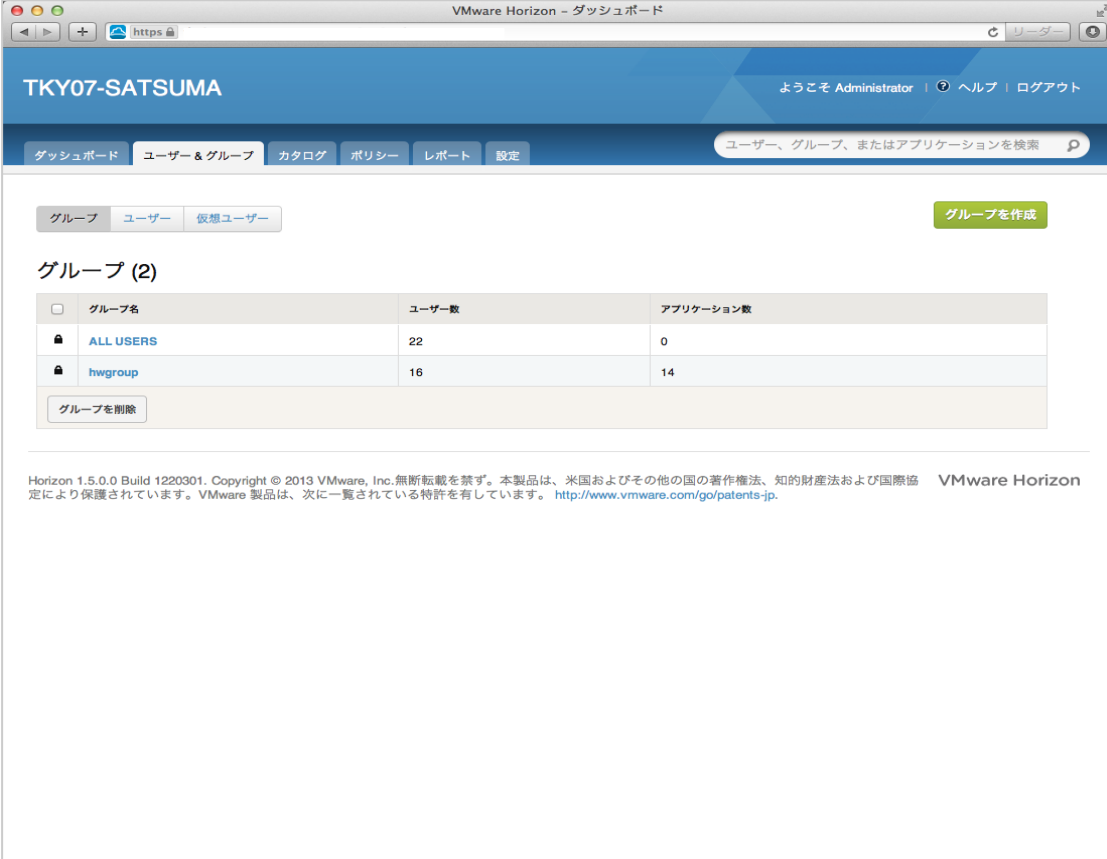
新しい証明書

(最大100 KB)

☒ Service Providerメタデータのダウンロード

### 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。



VMware Horizon - ダッシュボード

TKY07-SATSUMA

ようこそ Administrator | ヘルプ | ログアウト

ダッシュボード ユーザー & グループ カatalog ポリシー レポート 設定

ユーザー、グループ、またはアプリケーションを検索

グループ ユーザー 仮想ユーザー

グループを作成

グループ (2)

<input type="checkbox"/>	グループ名	ユーザー数	アプリケーション数
<input checked="" type="checkbox"/>	ALL USERS	22	0
<input checked="" type="checkbox"/>	hwgroup	16	14

グループを削除

Horizon 1.5.0.0 Build 1220301. Copyright © 2013 VMware, Inc. 無断転載を禁ず。本製品は、米国およびその他の国の著作権法、知的財産法および国際協定により保護されています。VMware 製品は、次に一覧されている特許を有しています。 <http://www.vmware.com/go/patents-jp> VMware Horizon

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。

The screenshot shows the VMware Horizon Dashboard for 'TKY07-SATSUMA'. The user is logged in as 'Administrator'. The '資格' (Qualifications) page for the 'hwgroup' is displayed, showing 14 qualifications. The page is divided into three sections: Web アプリケーション (1), iOS アプリケーション (2), and Android アプリケーション (7).

**資格** (Qualifications) section:

- このグループのユーザー (Users of this group)
- 適用されたモバイル ポリシー セット (Applied mobile policy set)

**Web アプリケーション (1)** (Web Applications (1))

項目	タイプ	展開	
Salesforce	Web アプリケーション	自動	<a href="#">資格を解除</a>

**iOS アプリケーション (2)** (iOS Applications (2))

項目	タイプ	展開	
VMware Horizon...	モバイル アプリケーション	ユーザーによるアクティブ化	<a href="#">資格を解除</a>
VMware Horizon...	モバイル アプリケーション	ユーザーによるアクティブ化	<a href="#">資格を解除</a>

**Android アプリケーション (7)** (Android Applications (7))

項目	タイプ	展開	
(VMware 対応デバイスの) 管理対象モバイル ワークスペース			<a href="#">編集</a>
VMware Android v2.3.6 (3ccb)			



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

グループの資格を追加

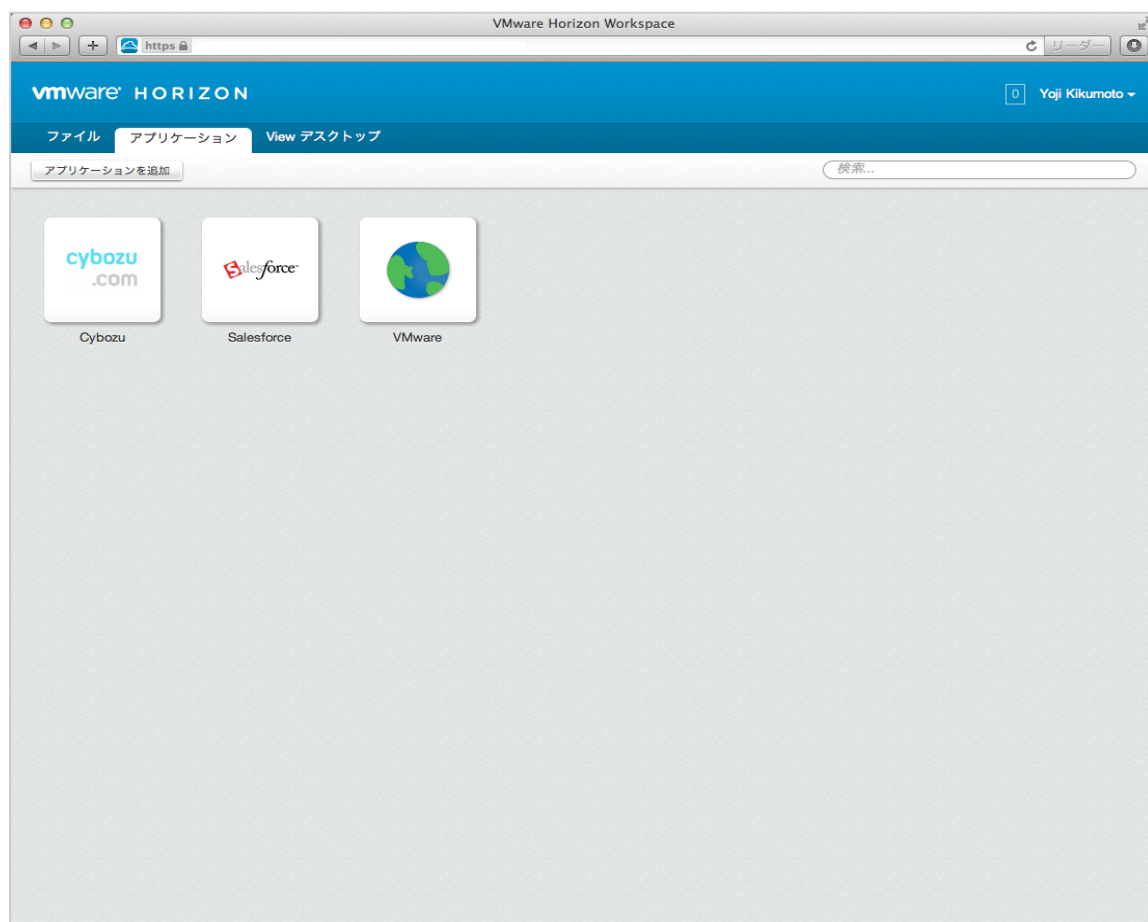
アプリケーションの種類 Web アプリケーション

検索するアプリケーションを入力してください

	アプリケーション	展開
<input checked="" type="checkbox"/>	 Cybozu	自動
<input type="checkbox"/>	 VMware	選択...

キャンセル | 保存

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。