

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®

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 サイボウズ Office</p>	 <p>管理機能を求める中堅・大企業向け Garoon</p>	 <p>社内のExcelが業務アプリに kintone</p>	 <p>このメール 対応します 前回は 山本さんが 作成してるの メールワイズ</p>
 <p>グループウェアをスマートフォンで サイボウズ KUNAI</p>		オプション <ul style="list-style-type: none">セキュアアクセステレビ会議ディスク増設メールサーバー	システム情報 <ul style="list-style-type: none">運用環境 (SLO)動作環境制限事項 <p>その他のクラウド製品</p>

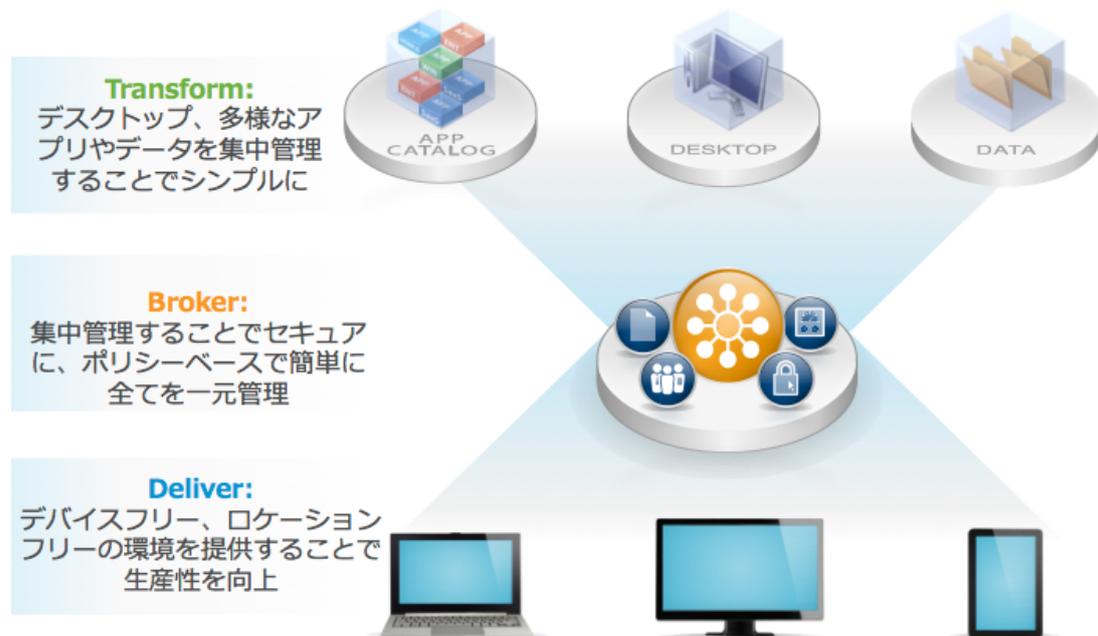
2.2 VMware Horizon Workspace

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
- 確認用パスワード
- 氏名
- 部署
- 電話番号

※ 英字と数字の組合わせで、8文字以上必要です。

個人のお客様はチェックしてください

お試しになるサービス

- サイボウズ Office
- Kintone
- Garoon
- メールクイズ
- 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。

VMware Horizon - ダッシュボード

TKY07-SATSUMA

ようこそ Administrator | ヘルプ | ログアウト

ユーザー、グループ、またはアプリケーションを検索

モジュール システム情報

モジュール	ユーザー数	合計数	ステータス
Horizon Files	16	16	有効
Web アプリケーション	2	16	有効
モバイル管理	9	16	有効
View	8	16	有効
ThinApp パッケージ	10	16	有効

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

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。

The screenshot shows the VMware Horizon dashboard for user 'TKY07-SATSUMA'. The page title is 'アプリケーションを追加' (Add Applications). Below the title, there is a section 'このグローバル カタログから選択' (Select from this global catalog) displaying a grid of application icons. The 'cybozu.com' icon is highlighted with a red box. The grid includes icons for Accellion, ADP, AXIOM, BlackLine, BlueJeans, Box.Net, Brainspark, Clarizen, Cybozu, Easy Match, EchoSign, Egnyte, Fieldglass, FoundationIP, Google Search Appliance, Google Apps, Juniper SSL VPN, Model N, NETEXAM, Peoplefluent, Plus One, Rally, Salesforce, salesPRISM, SAVO, Smartsheet, Socialcast, SpringCM, SuccessFactors, SugarCRM, Syncplicity, Varicent, Video Vault, VolunteerMatch, WebEx, Yammer, Zimbra SSO, and Zoho.

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 interface. The browser address bar displays 'VMware Horizon - ダッシュボード' and the URL 'https://'. The page header includes 'TKY07-SATSUMA' and 'ようこそ Administrator | ヘルプ | ログアウト'. A navigation menu contains '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, a sidebar for the application 'Cybozu' shows its icon, name, UUID, and version, along with tabs for '詳細', '構成', '資格', 'ライセンス', and 'プロビジョニング'. The main configuration area, titled '基本情報', contains fields for '名前' (Cybozu), '説明', 'アイコン' (with a 'ファイルを選択' button), and '認証プロファイル' (SAML20). A '保存' button is at the bottom. A footer contains copyright information for VMware and the text 'VMware Horizon'.

“プロフィール構成”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.com

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

プロフィール構成

起動 URL

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

(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

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

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

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

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

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。

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)
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
新しい証明書
Idp.cer
参照 (最大100 KB)

Service Providerメタデータのダウンロード

保存

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。



The screenshot shows the VMware Horizon administrator console. The page title is "TKY07-SATSUMA" and the user is "Administrator". The "Groups" tab is selected, showing a table with 2 groups:

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

Buttons for "グループを作成" (Create Group) and "グループを削除" (Delete Group) are visible.

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 the 'TKY07-SATSUMA' environment. The user is logged in as 'Administrator'. The main navigation bar 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 also present.

The '資格' (Qualifications) section for the 'hwgroup' group is displayed, showing 14 qualifications. A '+ 資格を追加' (Add Qualification) button is visible. The qualifications are categorized as follows:

- Web アプリケーション (1)**:

項目	タイプ	展開	
Salesforce	Web アプリケーション	自動	資格を解除
- iOS アプリケーション (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	資格を解除
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	資格を解除
- Android アプリケーション (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			編集
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 ✕

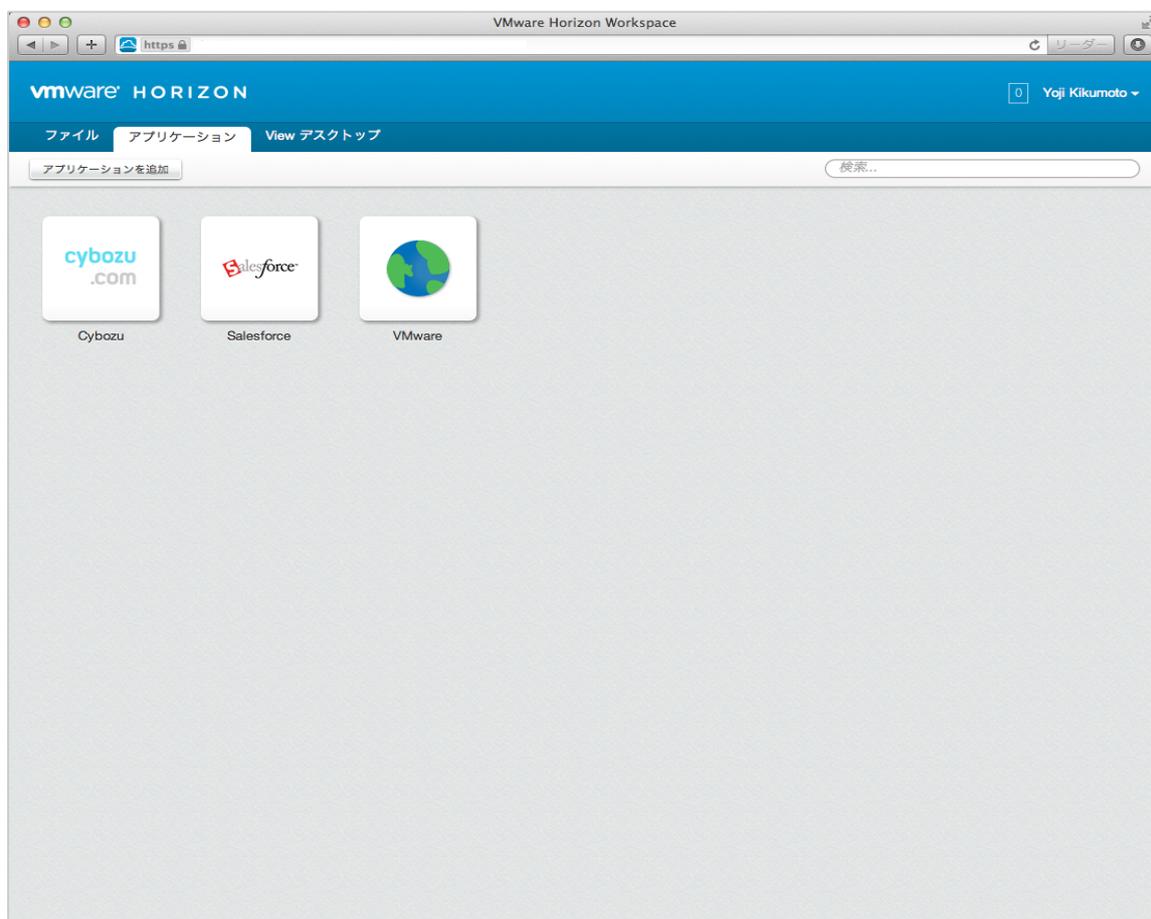
アプリケーションの種類 Web アプリケーション

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 cybozu.com	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。