



JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

SeciossLinkを利用したSAMLシングルサインオン

(cybozu.com 編)

Ver.1.0

2013年8月

- ・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン

目次

1. はじめに	4
1.1. 本書について	4
1.2. 本書における環境	4
1.3. 本書における構成	5
2. SeciossLink の設定	5
2.1. 信頼する認証局の設定	5
2.2. 認証ルールの作成	6
2.3. シングルサインオンの設定	8
3. Gléas の管理者設定 (PC)	9
3.1. UA (ユーザ申込局) 設定	9
4. クライアント側での操作 (PC)	9
4.1. クライアント証明書のインストール	9
4.2. cybozu.com へのシングルサインオン	11
5. Gléas の管理者設定 (iPad)	14
5.1. UA (ユーザ申込局) 設定	14
6. クライアント側での操作 (iPad)	16
6.1. 構成プロファイルのインストール	16
6.2. cybozu.com へのシングルサインオン	18
7. 問い合わせ	20

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベートCA Gléas」で発行した電子証明書を利用して、セシオス株式会社の提供するシングルサインオン（SSO）・統合ID管理サービス「SeciossLink」を経由してサイボウズ株式会社の提供する「cybozu.com」に対しSecurity Assertion Markup Language（SAML）を用いたシングルサインオン環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- 【SSOサービス】 SeciossLink
- 【認証局】 JS3 プライベートCA Gléas （バージョン1.10）
※以後、「Gléas」と記載します
- 【アプリケーション】 cybozu.com（cybozu.com office9）
※以後、「cybozu.com」と記載します
- 【クライアント：PC】 Microsoft Windows 7 Professional SP1
※以後、「PC」と記載します
- 【クライアント：タブレット】 Apple iPad（iOS 6.1.2）
※以後、「iPad」と記載します

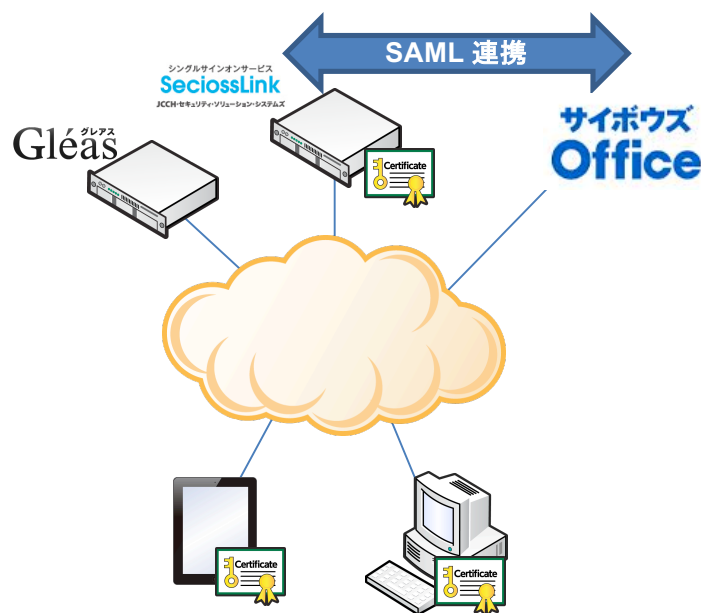
以下については、本書では説明を割愛します。

- cybozu.comの設定
- SeciossLinkのシングルサインオン設定
※セシオス株式会社のWEBサイトでcybozu.com認証連携を含めたSeciossLinkの設定方法を記載したマニュアルが公開されていますので、構築時の参考にしてください
参考URL：<http://support.secioss.co.jp/docs/SlinkManagementGuide.pdf>
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



1. デバイス（PC・iPad）はGléasよりクライアント証明書を取得する
2. ブラウザでcybozu.comのログイン画面にアクセスすると、ブラウザから有効なクライアント証明書を要求されるので、Gléasより取得した証明書により認証をおこないます。
3. 続いてSeciossLinkからユーザIDとパスワードによる認証がおこなわれます。この時のユーザIDはクライアント証明書のサブジェクトのcn（Common Name）が利用されます。
4. SeciossLinkへのログインに成功すると、自動的にcybozu.comに転送されます。

2. SeciossLink の設定

2.1. 信頼する認証局の設定

SeciossLinkに管理者としてログインし、画面上部のメニューより[システム]をクリックします。左ペインの[システム管理]メニューより[テナント情報]をクリック

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン

すると、右ペインに以下の設定画面が表示されるので以下を設定します。

テナント	
テナントID	jccch-sss.com
テナント名	JCCCH・セキュリティ・ソリューション・システムズ
最大ユーザー数	10
現在のユーザー数	3
SAML	1. SAML SP 最大ユーザー数 10 現在のユーザー数 0 2. SAML SP 最大ユーザー数 10 現在のユーザー数 0 3. SAML SP 最大ユーザー数 10 現在のユーザー数 0 4. SAML SP 最大ユーザー数 10 現在のユーザー数 0 5. SAML SP 最大ユーザー数 10 現在のユーザー数 0 6. SAML SP 最大ユーザー数 10 現在のユーザー数 0 7. SAML SP 最大ユーザー数 10 現在のユーザー数 0 8. SAML SP 最大ユーザー数 10 現在のユーザー数 0 9. SAML SP 最大ユーザー数 10 現在のユーザー数 0 10. SAML SP 最大ユーザー数 10 現在のユーザー数 0
サービス	Google Apps 最大ユーザー数 10 現在のユーザー数 1 Office 365 最大ユーザー数 10 現在のユーザー数 1 Salesforce 最大ユーザー数 10 現在のユーザー数 0
機能	証明書認証

- [証明書のサブジェクト]には、アクセスを許可するクライアント証明書のサブジェクトを入力（前方一致か後方一致で空欄不可。3つまで入力可能）
- [CA証明書]には、[ファイルを選択]ボタンを押して事前に準備したGléasの認証局証明書を選択しインポート
- [CRLのURL]には、失効リスト（CRL）の取得用のURLを入力
※GléasのデフォルトのCRL配布ポイントは以下のとおりです。SeciossLinkからアクセス可能である必要があります
<http://hostname.example.com/crl/ia1.crl>
※SeciossLinkは、失効リストを定期的に自動取得します

2.2. 認証規則の作成

上部メニューより[認証] > [新規登録]をクリックします。
新規設定画面で以下を設定します。

認証ルール	
ID	test
認証方法	認証方法一覧: ID/パスワード認証, 証明書認証 選択した認証方法: 証明書認証, ID/パスワード認証 追加 AND > 追加 OR > [△] [▽] 削除
優先度	1
クライアント端末	<input checked="" type="checkbox"/> Webブラウザ <input type="checkbox"/> 携帯電話 <input type="checkbox"/> スマートフォン <input checked="" type="checkbox"/> iPad
登録	

以下を設定します。

- [ID]には、認証ルールを識別する任意の ID 名を入力
[認証方法]には、[証明書認証]と[ID/パスワード認証]を[追加 AND >]を使って選択
※パスワード入力を省略したい場合は、[証明書認証]だけにすることも可能
 - [優先度]には、他の認証ルールと併用する場合の優先度を選択（数字が大きい方が優先）
 - [クライアント端末]には、[Web ブラウザ] [iPad]にチェック
- 設定後、[登録]をクリックします。

認証ルールが作成されると、このルールを適用するクライアントのアクセス元 IP アドレスの制限（[ネットワークの設定]）や、時刻による制限（[時間の設定]）の指定が可能となります。

認証ルール test		
新規登録		正常に登録されました。
認証ルール	ネットワークの設定	時間の設定

SeciossLink では複数の WEB サービスにシングルサインオンをおこなう際などに、特定の WEB サービス（cybozu.com 等）に限定してクライアント証明書認証を追加するような設定も可能です。

詳細は[アクセス制御]メニューを参照してください。本ドキュメントでは説明は省略します。

2.3. シングルサインオンの設定

上部メニューより[シングルサインオン] をクリックします。

左メニューより[cybozu.com]をクリックします。

cybozu.com	
シングルサインオンの設定	<input checked="" type="checkbox"/> 有効
cybozu.com サブドメイン	<input type="text" value="jcch"/>
cybozu.com 管理アカウント名	<input type="text" value="Administrator"/>
管理アカウントのパスワード	<input type="password"/>
利用するサービス	<input type="checkbox"/> kintone <input type="checkbox"/> garoon <input checked="" type="checkbox"/> office <input type="checkbox"/> mailwise <input type="checkbox"/> secureAccess <input type="checkbox"/> mailserver
<input type="button" value="保存"/>	

以下を設定します。

- [シングルサインオンの設定]の「有効」をクリック
- [cybozu.com サブドメイン]に利用するサブドメインを記述（ここでは「jcch」とします。）
- [cybozu.com 管理アカウント名]に「cybozu.com 共通管理者」のログイン名を入力
- [管理アカウントパスワード]に先に入力した「cybozu.com 共通管理者」のログイン名に cybozu.com で設定したパスワードを入力
- 「利用するサービス」でセットアップが完了しているサービスを選択
- [保存]をクリックして設定が完了です。

※cybozu.com の管理画面でドメイン（ここでは「jcch.cybozu.com」）のセットアップが完了した後に上記設定を実施してください。

※cybozu.com に管理者でログインし、[共通管理]→[ログイン]→[SAML 認証]ページで以下を設定します。

- “SAML 認証を有効にする” をチェック
- [Identity Provider の SSO エンドポイント URL]に以下を入力
<https://slink.secioss.com/saml/saml2/idp/SSOService.php>
- [cybozu.com からのログアウト後に遷移する URL]に以下を入力
<https://slink.secioss.com/saml/saml2/idp/initSLO.php?RelayState=/saml/logout.php&logout=cybozu>
- [Identity Provider が署名に使用する公開鍵の証明書]

https://slink.secioss.com/public/PublicKey-idp.pem からダウンロードしたファイルをアップロードしてください。

- [保存]をクリックして設定が完了です。

3. Gléasの管理者設定 (PC)

GléasのUA (申込局) より発行済み証明書をクライアントPCにインポートできるように設定します。

※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

3.1. UA (ユーザ申込局) 設定

GléasのRA (登録局) にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA (申込局) をクリックします。



[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

<input checked="" type="checkbox"/> 証明書ストアへのインポート	証明書ストアの種類	ユーザストア
<input type="checkbox"/> ダウンロードを許可	<input checked="" type="checkbox"/> インポートワンスを利用する	

設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、[保存]をクリックします。

以上でGléasの設定は終了です。

4. クライアント側での操作 (PC)

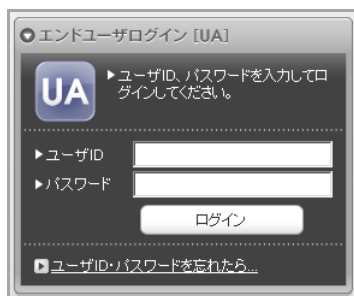
4.1. クライアント証明書のインストール

Internet ExplorerでGléasのUAサイトにアクセスします。

ログイン画面が表示されるので、GléasでのユーザIDとパスワードを入力しログイン

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン

します。



エンドユーザログイン [UA]

UA ユーザーID、パスワードを入力してログインしてください。

▶ユーザーID

▶パスワード

ログイン

▶ユーザーID・パスワードを忘れたら...

ログインすると、ユーザ専用ページが表示されます。

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

※初回ログインの際は、ActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。



ユーザー情報

テスト ユーザ さんのページ

ユーザー情報の確認・変更

▶ユーザー 登録日時: 2011/02/01 09:36

▶姓: テスト 名: ユーザ

▶ユーザーID: testuser

▶メールアドレス:

▶パスワード: *****

証明書情報

発行済み証明書

#	発行局	シリアル	有効期限	証明書ストアへインポート
1	JCCH-SSS demo CA	#9735	2012/02/29	証明書のインポート

「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン



4.2. cybozu.com へのシングルサインオン

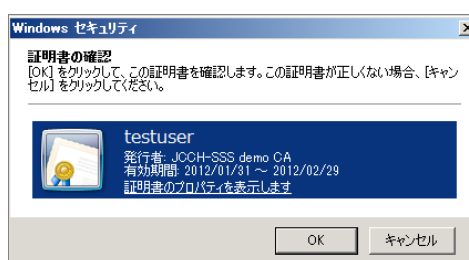
Internet Explorer (IE) でcybozu.comへアクセスします。URLは以下のとおりです。

<https://jcch.cybozu.com/>

今回アクセスしたURLはシングルサインオン設定がされているドメインとなりますので、アクセスするとSeciossLinkから証明書の提示を求められます。

クライアント証明書の選択ダイアログが出現します。証明書を確認して[OK]をクリックします。

※IEの設定によっては、クライアント証明書の選択ダイアログが出ない場合もあります



初回アクセス時にはテナントIDの入力を求められますので、入力して[選択]をクリックします。

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン



SeciossLinkのログイン画面が表示されます。
ユーザ名はクライアント証明書のサブジェクトのcn値にSeciossLinkのテナントID
が付加されたものとなります。



SeciossLinkでのログインパスワードを入力し、[ログイン]を入力するとcybozu.com
ログイン後の画面に転送されます。

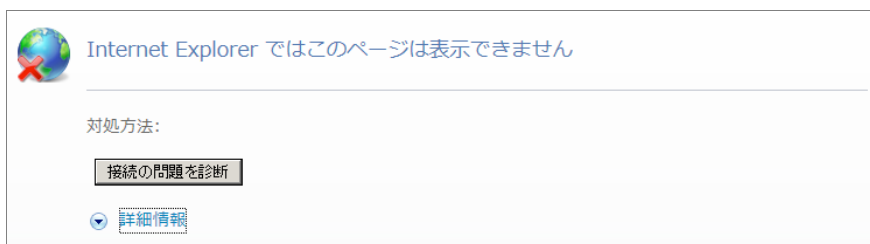


プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン

SeciossLinkにユーザ登録されていないサブジェクトcn値を持つクライアント証明書や、[テナント情報]で設定したものと異なるサブジェクトの証明書でアクセスした場合は以下のとおりエラーとなります。



クライアント証明書のない状態でアクセスすると以下のとおりエラーとなります。



失効したクライアント証明書でアクセスすると以下のとおりエラーとなります。

※失効情報がSeciossLinkに伝搬されている必要があります



5. Gléasの管理者設定 (iPad)

※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

5.1. UA (ユーザ申込局) 設定

GléasのRA (登録局) にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、iPad用となるUA (申込局) をクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [インポートワンスを利用する]のチェック、[ダウンロード可能時間(分)]の設定
この設定を行うと、GléasのUAからダウンロードしてから、指定した時間 (分) を経過した後に、構成プロファイルのダウンロードが不可能になります (「インポートロック」機能)。このインポートロックにより複数台のiPadへの構成プロファイルのインストールを制限することができます。

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン

基本設定

トークンへのインポート

証明書ストアへのインポート

ダウンロードを許可

ダウンロード可能時間(分)

登録申請を行わない

管理するトークン

証明書ストアの種類

インポートワンスを利用する

アカウントのワンタイムパスワードを利用する

保存

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

構成プロファイル生成に必要な情報を入力する画面が展開されるので、以下設定を行います。

- [iPhone用レイアウトを利用する]にチェック
- [iPhone構成プロファイル基本設定]の各項目を入力
 - ※[名前]、[識別子]、[プロファイルの組織名]、[説明]は必須項目となります
 - ※[削除パスワード]を設定すると、iPadユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPadユーザの故意や誤操作等による構成プロファイルの削除を防止できます）

認証デバイス情報

iPhone / iPadの設定

iPhone/iPad用 UAを利用する

画面レイアウト

iPhone用レイアウトを使用する

ログインパスワードで証明書を保護

OTA(Over-the-air)

OTAエンロールメントを利用する

接続する iOS デバイスを認証する

OTA用SCEP URL

OTA用認証局

iPhone 構成プロファイル基本設定

名前(デバイス上に表示)

識別子(例: com.jcch-sss.profile)

プロファイルの組織名

説明

削除パスワード

設定終了後、[保存]をクリックして設定を保存します。

以上でGléasの設定は終了です。

6. クライアント側での操作 (iPad)

GléasのUAに接続し、発行済みのクライアント証明書・構成プロファイルのインポートを行います。

6.1. 構成プロファイルのインストール

iPadのブラウザ (Safari) でGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。



ログインすると、そのユーザ専用ページが表示されるので、[構成プロファイルのダウンロード]をタップし、ダウンロードを開始します。

※インポートロックを有効にしている場合は、この時点からカウントが開始されます



ダウンロードが終了すると、自動的にプロファイル画面に遷移するので、[インストール]をタップします。

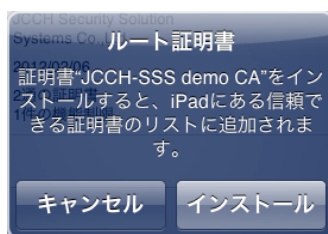
なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、必要に応じ確認してください。

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン



インストール途中に、以下のようなルート証明書のインストール確認画面が現れますので、[インストール]をクリックして続行してください。

※ここでインストールされるルート証明書は、通常Gléasのルート認証局証明書になります。



インストール完了画面になりますので、[完了]をタップしてください。



元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてください。

以上で、iPadでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可能となります。

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン



この他に、iOS端末の識別番号を用いて端末を限定してクライアント証明書を配布することも可能です。詳細は弊社営業担当までお問い合わせください。

6.2. cybozu.com へのシングルサインオン

SafariでCybozu.comへアクセスします。URLは以下のとおりです。

<https://jcch.cybozu.com/>

提示可能なクライアント証明書が1枚の場合は、何も表示されずそのままSeciossLinkのログイン画面になります。(提示可能な証明書が複数ある場合は選択ダイアログが出現しますので、適切な証明書を選択してください)

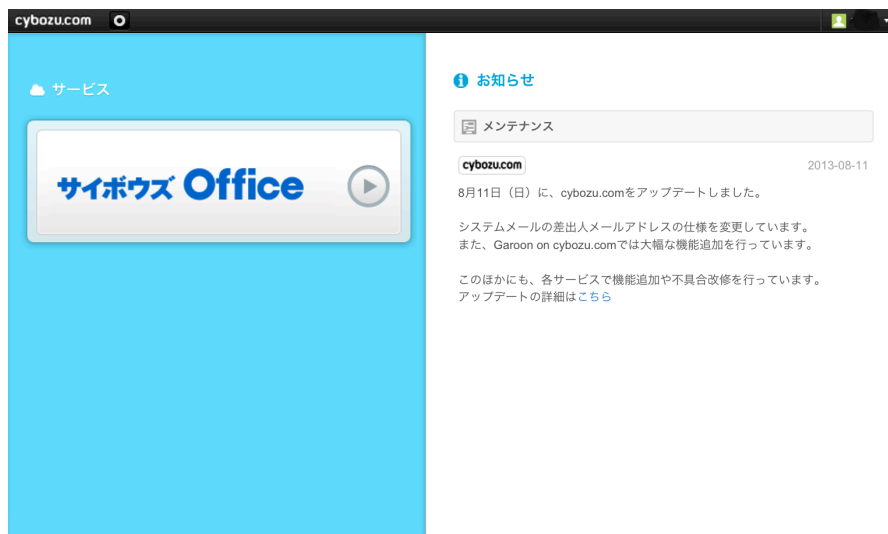
ユーザ名はクライアント証明書のサブジェクトのcn値にSeciossLinkのテナントIDが付加されたものとなります。



SeciossLinkでのログインパスワードを入力し、[ログイン]を入力するとCybozu.com

プライベート CA Gléas ホワイトペーパー
SeciossLink を利用した cybozu.com へのシングルサインオン

のログイン後の画面に転送されます。



SeciossLinkにユーザ登録されていないサブジェクトcn値を持つクライアント証明書や、[テナント情報]で設定したものと異なるサブジェクトの証明書でアクセスした場合は次のとおりエラーとなります。



クライアント証明書のない状態でアクセスすると以下のとおりエラーとなります。



失効したクライアント証明書でアクセスするとSeciossLinkのログイン画面まで進むことができません。

※失効情報がSeciossLinkに伝搬されている必要があります。

7. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com

■SeciossLinkに関するお問い合わせ

株式会社セシオス

Tel: 03-6265-0448

Mail: slink-jcch@secioss.co.jp

管理者ガイド :

<http://support.secioss.co.jp/docs/SlinkManagementGuide.pdf>

ユーザガイド :

<http://support.secioss.co.jp/docs/SlinkUserGuide.pdf>

■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

Mail: contactus@cybozu.co.jp

cybozu.com ヘルプ: <https://help.cybozu.com/ja/general/index.html>