ID Federation 重要事項ご説明書

2023年1月11日

ID Federation（以下、本サービス）のご利用にあたっては、電気通信事業法第26条（提供条件の説明）を鑑みた、この「重要事項に関する説明について」の内容を十分にご理解の上、お申し込み下さい。
■事業者の名称 エヌ・ティ・ティ・コミュニケーションズ株式会社
代表者の氏名 代表取締役社長　丸岡　亨

■サービスに関するお問合せ（ご契約前）
以下のお問い合わせフォームをご利用ください。
https://www.ntt.com/idf
お問い合わせの受付は、24時間365日行っておりますが、当社からの回答は、10:00～17:00（土曜、日曜、祝日、年末年始を除く。）となります。

■サービスの設定方法／料金等に関するお問合せ（ご契約後）
開通時にお客さまに送付させて頂きます「ご利用内容のご案内」に掲載された【お問い合わせ】をご確認ください。
お問い合わせの受付は、10:00～17:30（土曜、日曜、祝日、年末年始を除く）となります。
故障に関するお問い合わせについては、24時間365日受け付けます。

大項目	中項目	詳細	記事／備考
ご利用に際して	アカウントの削除	本サービス上のユーザアカウントを削除すると、ユーザアカウントデータ及び関連データを復元させることはできません。	
	利用プロトコル	本サービスへのアクセスで利用するプロトコル及びポート番号はTCP/80(HTTP)、TCP/443(HTTPS)となります。 ご利用いただく環境から、上記プロトコルの通信が可能である必要があります。	
	接続元IPアドレスの制限	ご契約いただいた本サービスへアクセス可能なIPアドレスを制限する場合、本サービス開通後お客様自身で設定いただく必要があります。 ※設定方法の詳細については管理者マニュアルをご参照下さい。	
	利用環境	・本サービスはインターネット回線または弊社VPNサービス「Arcstar Universal One （L3）」およびFlexible Interconnectサービスを経由して、ご利用いただくサービスです。インターネット環境の状況により、ご利用しづらい場合があります。 また、インターネット環境にProxyや、コンテンツフィルタ等をご利用いただいている場合は、本サービスが正常に動作しない場合があります。 ・本サービスで接続するFQDNは、www.cloud-idf.com、admin.cloud-idf.com,sso.connect.pingidentity.com、desktop.pingone.comです。 ユーザ端末からFQDNに対する通信が可能である必要があります。OIDC接続の場合はアプリケーションからも、sso.connect.pingidentity.comに対する通信が可能であるこが必要です。 ・本サービスから送信される各種メールは、文字コードをUTF-8として送信されます。クライアントの環境やその他の要因によって、受信時にデコードが正しく行われずメールの文字化けが発生する場合があります。また、「no-reply@cloud-idf.com」を送信元として送付されますので、お客様環境で、受信が出来るよう設定いただく必要があります。また、送信元メール	
	Active Directory	AD FS(Active Directory Federation Service)連携を利用する際、ActiveDirectory及びAD FSについてはお客様ご自身でご準備ください。	
	サーバ設備	本サービスが提供するユーザのポータル画面等の一部機能についてPing Identity社のサーバ設備を利用しております。	
	対応ブラウザ	本サービスは、以下の推奨環境で使用して頂く必要があります。 利用者 OS: Windows10 / Microsoft Edge: 最新Ver. / Firefox: 最新Ver. / Google Chrome: 最新Ver. OS: Windows11 / Microsoft Edge: 最新Ver. / Firefox: 最新Ver. / Google Chrome: 最新Ver. OS: MacOS / Microsoft Edge: — / Firefox: 最新Ver. / Google Chrome: 最新Ver. 管理者 OS: Windows10 / Microsoft Edge: 最新Ver. / Firefox: 最新Ver. / Google Chrome: 最新Ver. OS: Windows11 / Microsoft Edge: 最新Ver. / Firefox: 最新Ver. / Google Chrome: 最新Ver. OS: MacOS / Microsoft Edge: — / Firefox: 最新Ver. / Google Chrome: 最新Ver. 利用者 OS: iPhone/iPad: iOS13以降 / Android: Android8.0以降 ブラウザ: iPhone/iPad: safari / Android: Chrome また、ブラウザ設定に関する主な留意事項として、以下項目を確認ください。 ・JavaScriptが有効にされていること。 ・Cookieが利用可能であること。 ・Webページで指定された表示が可能であること。 ・TLS1.2（Transport Layer Security)通信が可能であること。 ・サービス画面に表示されているボタン以外の操作で［戻る］の操作が行われた場合、正常に処理が完了しない場合があります。 ・サービスログインURLをブックマークされる場合は、企業管理者ポータルの「契約情報」に記載のURLを設定してください。 ・ブラウザ以外のアプリケーションのURLリンクからのアクセスをしないこと。（例えば、Excelのハイパーリンクからの接続。）	Microsoft Edge（IEモード）はサポート対象外です。
	同時ログイン	同一ブラウザでの同時ログイン（同一アカウント・他アカウント問わず）は、動作保証しておりませんのでご注意ください。	同時ログインを制限することはできません。
	多要素認証（PingID）	・PingIDの認証方式には、モバイルアプリ認証（スワイプ,生体認証）,FIDO2生体認証、デスクトップOTP認証があります。 PingIDにはモバイルアプリ認証（スワイプ）が標準で搭載されています。他の認証方式はお申込みにより有効になります。 ・PingIDで接続するFQDNは、idpxnyl3m.pingidentity.com,authenticator.pingone.comです。ユーザ端末からFQDNに対する通信が可能である必要があります。 ・インターネット環境の状況により、PingID認証ができない場合があります。 [モバイルアプリ認証（スワイプ、生体認証）] ・スマートフォンを用いた認証となります。Ping Identity社が提供する「PingID」アプリのインストールが必要です。 ・生体認証の利用が申し込まれている場合は、生体認証が優先されます。端末のOSで生体認証が無効になっている、またはデバイスが生体認証をサポートしていない場合は、標準で搭載されているスワイプが使用されます。 [FIDO2生体認証] FIDO2生体認証に対応している端末と指紋や顔など生体登録が必要です。以下の条件でご利用いただけます。 1)WindowsHello ・Microsoft Edgev44.17763以降などのFIDO2バイオメトリクスの使用をサポートするブラウザおよびWindows10、OSビルド1809以降。 ・Google Chromeブラウザ76以降およびWindows10、OSビルド1903以降。 2)AppleMac TouchID ・MacデバイスにTouchIDがあり、FIDO2プラットフォームの生体認証をサポートしていること ・Google ChromeやSafariなどのFIDO2生体認証をサポートするブラウザーおよびブラウザの最新バージョンを使用していること。 ・Mac Touch ID FIDO2認証はブラウザ固有であるため、SafariブラウザとChromeブラウザの両方でサポートされていますが、 デバイスをペアリングする場合、アカウントのペアリングに使用したブラウザと同じブラウザを使用してのみ認証できます。 3)Androidバイオメトリクス ・Google ChromeやMicrosoftEdgeなどのFIDO2生体認証使用をサポートするブラウザーおよびブラウザの最新バージョンを使用していること。 4)TouchID,iPad ・iOS 14、iPadOS 14、デフォルトブラウザとなるSafari v14。 ・MacOS 11 BigSur以降。 ・Google ChromeはiOSでサポートされていません。 [デスクトップOTP認証] ・PCにPing Identity社が提供する「PingID」デスクトップアプリのインストールが必要です。 ・「PingID」デスクトップアプリは、Mac OS仮想マシン（VM）では実行されません。 ・デスクトップOTP認証は、お客様社内ネットワーク環境のプロキシに対応するために、PCに個別の設定が必要な場合があります。	2021年10月４日にスワイプ認証の名称はPingIDに変更しました。スワイプ認証はPingIDのモバイルアプリ認証（スワイプ）に該当します。
	多要素認証（TOTP認証）	TOTP認証はスマートフォンを用いた認証となります。ご利用いただく場合は,RFC6238に準拠したTOTPアプリケーションをご利用いただく必要があります。弊社動作確認済みクライアントアプリケーションをご利用いただくことを推奨します。 【動作確認済クライアント】 Google authenticator(iOS/Android) OTP Auth(iOS) DUO Mobile（Android）	
	多要素認証（機体認証）	Microsoft社のWindows8.1+IEのサポート終了に伴いベストエフォート対応となります。 ・スマートフォンではご利用できません。 ・機体情報初期設定のご案内メールは、管理者による設定後10分以内にユーザへ送信されます。機体認証は、ご案内メールに従って機体情報を登録完了された後にご利用いただけます。 ・PCに専用のモジュール（ActiveX）をインストールする必要がある為、新規導入や機能バージョンアップなどの際には対象PCのAdministrators権限保持ユーザーによる操作が必要となります。 ・機体情報初期設定時と異なるネットワーク接続環境（LAN設定ONからOFFへの変更等）でご利用される場合、機体認証に失敗する場合があります。 ・PC環境（ActiveXが正常に動作しない環境等）により、機体情報が取得できない等の理由でサービスをご利用いただけない場合があります。 ・端末1台につき、1ブラウザでの動作を保証します。 ・サービス画面に表示されているボタン以外の操作で［戻る］の操作が行われた場合、正常に処理が完了しない場合があります。 ・端末や通信状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合の動作は保証対象外 となります。	機体認証は20203年1月31日をもちまして、サービスを終了いたします。
	多要素認証（メールOTP認証）	認証に使用するOTPは、インターネット経由でのメール配送で通知されますので、インターネット環境の状況により受信までに時間がかかる場合があります。	

<table>
<tr><td></td><td>多要素認証（証明書認証）</td><td>証明書認証オプションをご利用いただく場合は、以下推奨環境でお使いいただく必要があります。
Firefoxはご利用できません。
<table><tr><td></td><td>OS</td><td>Microsoft Edge</td><td>Google Chrome</td></tr><tr><td rowspan="3">利用者</td><td>Windows10</td><td>最新Ver.</td><td>最新Ver.</td></tr><tr><td>Windows11</td><td>最新Ver.</td><td>最新Ver.</td></tr><tr><td>MacOS</td><td></td><td>最新Ver.</td></tr></table><table><tr><td colspan="2"></td><td>iPhone/iPad</td><td>Android</td></tr><tr><td rowspan="2">利用者</td><td>OS</td><td>iOS13以降</td><td>Android8.0以降</td></tr><tr><td>ブラウザ</td><td>safari</td><td>Chrome</td></tr></table>・証明書認証特約書を締結していただきます。
・証明書発行サイトのルート証明書（or 中間証明書）およびクライアント証明書はお客様にてご準備いただきます。
・証明書認証で利用するポート番号は80,443,1443となります。 ユーザから証明書認証サーバまでの本ポートに対する通信を許可頂く必要があります。
・証明書認証で接続するFQDNは、pki-cert.cloud-idf.comです。ユーザ端末からFQDNに対する通信が可能である必要があります。
・有効期限切れや発行サービスのサービス仕様変更などで運用開始後に、ルート証明書もしくは、中間証明書の更新が必要な場合は、お客様より、ID Federationの保守窓口へご連絡を頂きます。当社側からの証明書の有効期限切れ間近である旨の連絡等は行いませんので、ご了承ください。
・証明書発行および証明書インストールに関する問い合わせはお受けできません。
証明書認証が利用できない等の問いあわせを頂く際に、切り分けのため、証明書とIDを借用させていただく可能性があります。借用させていただけない場合は、事象の特定が難しい場合があります。
・証明書認証機能を一度解約された場合は、利用開始時に初期登録した証明書等の情報は削除されます。解約後、改めて再契約する場合は、再度、初期登録が必要となります。</td><td></td></tr>
<tr><td></td><td>アカウント数の制限</td><td>登録可能なユーザアカウント数は本サービスの管理者画面から変更可能です。</td><td></td></tr>
<tr><td></td><td>利用者への通知</td><td>エンドユーザへのIDやパスワード等の通知については、企業管理者にて実施いただきます。</td><td></td></tr>
<tr><td></td><td>管理者パスワードリセット</td><td>管理者アカウントが1IDのみ登録されている場合は、弊社へのパスワードリセット依頼、または管理者追加登録申請が必要となります。※管理者追加登録申請は、契約変更申込みとなるため標準で6営業日かかります。
但し、管理者アカウントを複数ID設定することで、他の管理者により、パスワードリセットが可能になります。（管理者アカウントを複数ID設定されることを推奨します。）</td><td></td></tr>
<tr><td>サポート</td><td>ヘルプデスク</td><td>・ヘルプデスクの受付時間は、営業日の10：00～17：30(日本時間)での対応となります。故障の申告は、24時間365日受付となります。
・ヘルプデスクへのお問い合わせ等は、NTTCommunicationsオフィシャルサイト内「お客様サポートサイト」（http://support.ntt.com/id-federation）へ、予め規定した企業管理者からのみとさせていただきます。※カスタマイズオプションをご利用の場合、お問い合わせ先は、上記と異なり、別途ご案内するヘルプデスクとなります。</td><td>エンドユーザ向けのヘルプデスク機能は、提供しておりません。</td></tr>
<tr><td></td><td>工事(メンテナンス)情報</td><td>・工事を実施する場合は、毎月第一、三週の日曜日23時から翌月曜日6時（日本時間）を作業基本時間帯とします。但し、緊急工事の場合はこの限りではありません。
・工事情報は、「お客様サポートサイト」に掲載します。
・工事通知は、「お客さまサポートサイト」にサポートIDを登録し、工事情報メールの通知設定を行うことで可能となります。
※多要素認証（証明書認証）およびカスタマイズオプションをご利用の場合、工事（メンテナンス情報）は、上記と異なり、別途ご案内するヘルプデスクよりご連絡となります。</td><td>工事情報は、サービス影響がある場合に掲載します
工事情報メール未設定の場合、工事通知を受信することができませんので、ご注意ください。</td></tr>
<tr><td></td><td>故障情報</td><td>・故障情報は、「お客様サポートサイト」 に掲載します。
・故障情報の通知は、「お客さまサポートサイト」 にサポートIDを登録し、故障情報メールの通知設定を行うことで可能になります。
※カスタマイズオプションをご利用の場合、故障情報は、上記と異なり、別途ご案内するヘルプデスクよりご連絡となります。</td><td>故障情報メール未設定の場合、故障通知を受信することができませんので、ご注意ください。</td></tr>
<tr><td></td><td>サポート内容</td><td>エンドユーザのID登録やグループ登録等、ご利用に必要な各種設定はお客様にて実施頂きます。ヘルプデスクでは設定代行は行いません。</td><td></td></tr>
<tr><td></td><td></td><td>SSO対象アプリケーションを起点としたご利用の場合は、本サービスとアプリケーション側との切り分けがつかない場合があります。また、SSO対象アプリケーション側の正常性をお客様にて切り分けの上、確認いただいていることを問い合わせの前提とさせていただきます。</td><td></td></tr>
<tr><td></td><td>故障対応</td><td>故障を申告いただいた際の切り分けや復旧作業について、インターネット環境やお客様環境に依存する要因については、対応できない場合があります。</td><td></td></tr>
<tr><td>接続先
アプリケーションの利用</td><td>利用</td><td>SSOで接続した後の各アプリケーションサービスの動作については、本サービスでは保証及びサポートはいたしません。アプリケーション利用に関するお問い合わせは、それぞれの窓口へお願いします。
各アプリケーションサービスの仕様変更により、SSOが使用できなくなる場合がございます。</td><td></td></tr>
<tr><td></td><td>メンテナンス時間</td><td>各アプリケーションサービスのメンテナンスは、本サービスのメンテナンスウインドウと異なります。</td><td></td></tr>
<tr><td>その他</td><td>新設/変更/廃止申込みに伴う受付処理期間</td><td>申込みから、新設/変更/廃止処理を完了するまでには、標準で6営業日となります。VPN接続の有無等、お申込みの内容よっては、標準以上の営業日が必要となります。</td><td></td></tr>
<tr><td></td><td>海外でのご利用について</td><td>本サービスのご契約は、日本国内企業（日本法人）に限ります。
利用する地域については、ご契約したお客さま（契約者）の責任で、利用者を管理するものとします。GDPR（EU一般データ保護規則）は未対応です。</td><td>本サービスを日本国外で利用する際には、下記を了承し、必要な対処をした上で、契約者の責任でご利用ください。。
・日本国外の電気通信事業法やその他の法律を遵守すること。
・日本国外のNW環境やクライアント環境に依存して、遅延等の悪影響や不具合が発生する可能性があること。
・日本国外利用地域の法指導等により、本サービスの利用を禁止される場合があること。
・日本国外利用地域の捜査機関等の要請に本サービスが応じられない場合があること。</td></tr>
<tr><td></td><td>SAML認証連携をご利用の場合の留意事項</td><td>本サービスの開通後、接続先アプリケーションとのSAML認証連携設定が完了した後にSSOがご利用いただけます。
接続設定においてお客様ご利用アプリケーションにインストールいただく本サービスの証明書ファイルは、お客様にて更新していただく必要がございます。</td><td></td></tr>
<tr><td></td><td>OIDC認証連携をご利用の場合の留意事項</td><td>・本サービスの開通後、接続先アプリケーションとのOIDC認証連携設定が完了した後にSSOがご利用いただけます。
・通信フローはAuthorization Code Flowに対応しています。
・アプリケーションからsso.connect.pingidentity.comに対する通信が可能である必要があります。</td><td></td></tr>
<tr><td></td><td>VPNを経由して、認証機能をご利用の場合の留意事項</td><td>お客様端末―認証サーバ間のID/Password認証はVPNでの通信となりますが、一部通信においてPing Identity社のサーバ設備と接続するため、その際、お客様端末と当該サーバ設備間の通信はインターネット（HTTPS）を経由します。 また、一部オプションメニューの多要素認証（PingID認証、証明書認証）の通信もインターネット（HTTPS）を経由した通信となります。</td><td></td></tr>
<tr><td></td><td>VPNを経由して、ご利用の場合の留意事項</td><td>・別途Arcstar Universal One(L3)及びFlexible InterConnectサービス（FIC Router,FIC-Router to Arcstar Universal One,FIC-Router to Azure (Private Peering)）のご契約が必要です。
・本サービスの設備用にお客様のプライベートIPアドレス/27を借用いたします。借用したプライベートIPアドレスから、弊社が割り当てるIPアドレスをお客様環境にて、名前解決に設定していただきます。
・本サービスは、状況に応じて、お客様への事前通知なく、メインサイト／バックアップサイト間で切り替えが発生する場合があります。</td><td></td></tr>
</table>