

【J-MOTTO 会員ログイン】
SAML 認証ログインマニュアル
[HENNGE 用]

目次

1	はじめに.....	2
2	初期設定 (HENNGE ONE).....	3
	サービスプロバイダーの追加.....	3
3	初期設定 (J-MOTTO / 会員情報管理画面への設定).....	5
4	ログイン許可について.....	8
	SAML の仕組みと制限事項.....	8
	特に注意頂きたいこと.....	8
	HENNGE ONE での実際の許可設定.....	9
5	一般ユーザー向け (ログインの仕方について).....	11
	お問合せ.....	12

1 はじめに

【概要】

HENNGE ONE の SAML 認証の仕組みを使い J-MOTTO サイトに通常は「会員 ID」「ユーザーID」「パスワード」の 3 要素でログインして頂いたものを HENNGE ONE のログイン方法に統一できます。
本書では前提条件や注意事項、管理者による設定の手順について説明します。

【前提条件】

SAML によるログイン連携を行うには、「HENNGE ONE」の「サービスプロバイダー」に当社専用のアプリケーション (SAML 認証用) を設定頂く必要があります。

その為、HENNGE ONE のご契約においてもこの「HENNGE ONE」および「サービスプロバイダー」の設定が可能であることがご利用の条件になります。

【行程概要】

- ① HENNGE ONE 側の「サービスプロバイダー」に SAML 設定をおこなう
- ② HENNGE ONE 側の SAML 設定から必要ファイルを二つダウンロードする
- ③ J-MOTTO サイト上の会員情報管理の専用設定画面からダウンロードしたファイルをアップロードする
- ④ SAML ログインさせたいユーザーに対して、HENNGE ONE 側のエンタープライズアプリケーションの利用権限を付与する
- ⑤ J-MOTTO 会員情報管理のユーザー情報「メールアドレス」を HENNGE ONE 側の「UPN」(UserPrincipalName) と対応させる
※例: 00001 のメールアドレス設定を (00001 を使うユーザーに対応する) UPN に変更し、他に重複がないか確認する
- ⑥ SAML ログインさせたいユーザーに SAML ログイン専用の URL を伝える

2 初期設定 (HENNGE ONE)

サービスプロバイダーの追加

本操作では HENNGE ONE における管理者権限で設定してください。
SAML 認証が利用できるように HENNGE ONE に「サービスプロバイダー」を設定します。

お客様ご契約の HENNGE ONE にログインします。
HENNGE ONE のサイドメニューから「サービスプロバイダー設定」を選択します。



「サービスプロバイダーの追加」をクリックします。



「カスタム」をクリックします。



【J-MOTTO 会員ログイン】SAML 認証ログインマニュアル

「名前」に対して弊社用の SAML 設定であることがわかる名前を自由につけてください。ただし、HENNGE ONE 内で設定されている他のサービスプロバイダーの名称と同じにはできません。

「Entity ID」には「j-motto.co.jp/login」と設定してください。

j-motto.co.jp/login 以外が設定されている場合には SAML 機能が働かず、ログインできません。

「ACS URL」には「https://www2j-motto.co.jp/saml/sso」を設定してください。

設定できたら「次へ」をクリックしてください。



The screenshot shows a web form titled "サービスプロバイダーの追加" (Add Service Provider). At the top, there are four buttons: "プリセット" (Preset), "+ メタデータアップロード" (Upload Metadata), "カスタム" (Custom), and "リンク" (Link). Below these are several input fields: "名前" (Name), "ACS URL", "Entity ID", "署名鍵" (Signature Key) with a dropdown menu set to "2048-bits (推奨)" (Recommended), "Name ID" with a text box containing "{user.upn}", "ログインURL" (Login URL), and "固有番号" (Unique ID). At the bottom center, a button labeled "+ 次へ" (Next) is highlighted with a green box.

次の画面になりましたら「送信」をクリックしてください。



The screenshot shows a web form titled "サービスプロバイダー設定" (Service Provider Settings). The "Name ID" field contains "{user.upn}" and the "固有番号" (Unique ID) field is empty. The "セッション有効時間 (時間)" (Session Valid Time) field contains "8". There is a checkbox for "非表示" (Hidden) which is unchecked. The "ロゴ画像" (Logo Image) section has a "ファイルを選択" (Select File) button, a "選択されていません" (Not selected) status, and an unchecked checkbox for "ロゴを削除" (Delete Logo). Below this, it says "現在のロゴ: ロゴが選択されていません" (Current logo: No logo selected). A section titled "属性の設定" (Attribute Settings) is visible, with a table header "属性 値" (Attribute Value) and a "+ 属性の追加" (Add Attribute) button. At the bottom center, a button labeled "送信" (Send) is highlighted with a green box.

【J-MOTTO 会員ログイン】SAML 認証ログインマニュアル

送信後、このような状態になっていればエンタープライズアプリケーションの設定は完了です。
 ※ほかの項目はデフォルト(変更なし)のままとしてください。

+ サービスプロバイダーの追加 表示切替					
名前	メタデータ	アクセスポリシーグループ数	ユーザー数	完了	管理
名前	表示 ダウンロード	0	0	完了	 

3 初期設定 (J-MOTTO/会員情報管理画面への設定)

本操作では HENNGE ONE における管理者権限 および J-MOTTO の会員情報管理に管理者でアクセスできる方で設定してください。
 ※J-MOTTO「グループウェア」の管理者権限は必要ありません。

HENNGE ONE から会員情報管理で使うファイルをダウンロード

サービスプロバイダー設定 (Entity ID や ACS URL の設定) で利用した SAML 設定画面を表示します。
 その画面上で作成したサービスプロバイダーの「ダウンロード」をクリックし、XML をダウンロードします。

+ サービスプロバイダーの追加 表示切替					
名前	メタデータ	アクセスポリシーグループ数	ユーザー数	完了	管理
名前	表示 ダウンロード	0	0	完了	 

「メタデータ」の「表示」をクリックします。

+ サービスプロバイダーの追加 表示切替					
名前	メタデータ	アクセスポリシーグループ数	ユーザー数	完了	管理
名前	表示 ダウンロード	0	0	完了	 

「ダウンロード」をクリックし、証明書をダウンロードします。

エンドポイントを表示する ✕

Issuer

シングルサインオンURL

シングルサインアウトURL

ダイレクトログインURL

証明書 ダウンロード

会員情報管理画面に証明書とフェデレーションメタデータ XML をアップロード

J-MOTTO の管理者権限でログインすると、管理者メニューに専用のメニューがありますので「設定一覧」をクリックすると、HENNGE ONE の項目が出ますので変更ボタンをクリックします。

- ◎ 通知設定
- ◎ 履歴管理
- ◎ SSO設定
- ◎ 設定一覧
- ◎ ユーザー情報
- ◎ その他

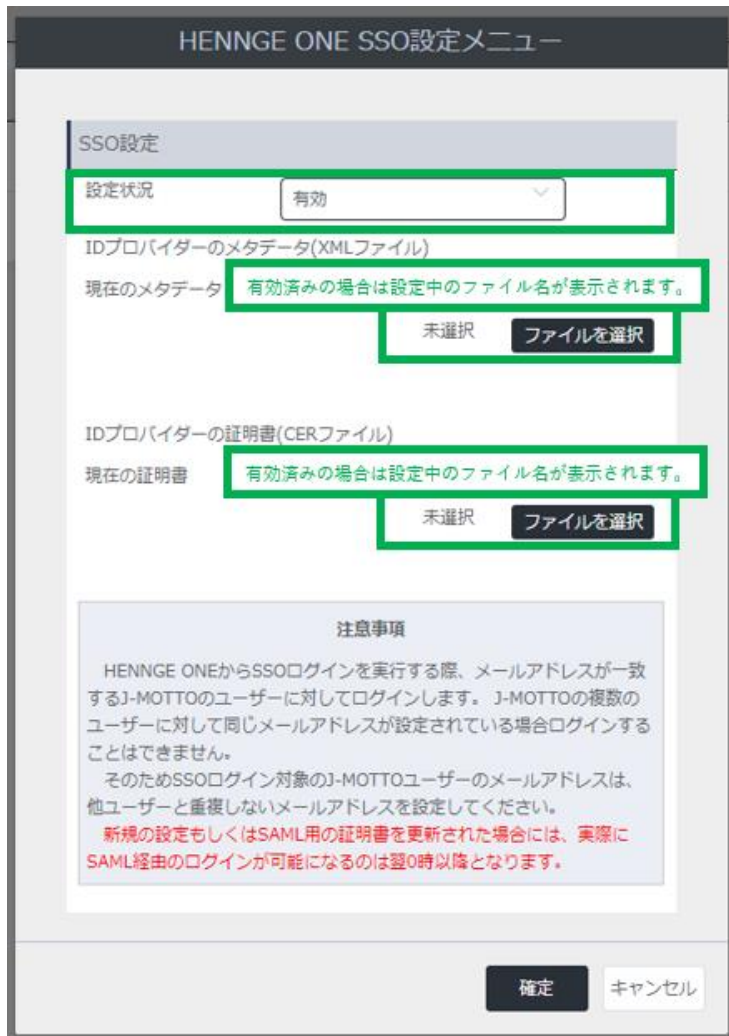
SSO設定一覧		
SSO設定		
AzureAD	無効	変更
HENNGE ONE	無効	変更

【J-MOTTO 会員ログイン】SAML 認証ログインマニュアル

設定メニューが表示されます。

HENNGE ONE から会員情報管理で使うファイルをダウンロードした二つのファイル(XML形式、CER形式)をアップロードします。

「現在のメタデータ」にXML形式のファイルを、「現在の証明書」にCER形式のファイルを選択、アップロードし、最後に確定ボタンを押してください。実際にファイルがアップロードされ、設定が完了します。



SSO設定

設定状況

IDプロバイダーのメタデータ(XMLファイル)

現在のメタデータ

IDプロバイダーの証明書(CERファイル)

現在の証明書

注意事項

HENNGE ONEからSSOログインを実行する際、メールアドレスが一致するJ-MOTTOのユーザーに対してログインします。J-MOTTOの複数のユーザーに対して同じメールアドレスが設定されている場合ログインすることはできません。

そのためSSOログイン対象のJ-MOTTOユーザーのメールアドレスは、他ユーザーと重複しないメールアドレスを設定してください。

新規の設定もしくはSAML用の証明書を更新された場合には、実際にSAML経由のログインが可能になるのは翌0時以降となります。

SAML 認証はこれでいつでも利用できる状態になりました。

次は実際に一般ユーザーで利用を開始するまでをご案内します。

4 ログイン許可について

SAML の仕組みと制限事項

SAML 認証は HENNGE ONE 上ではユーザーごとに利用許可を設定することで J-MOTTO へのシングルサインオンの利用／利用不可を制御可能です。

設定完了の直後はユーザーに利用許可がありませんので、許可するユーザーに対しては本手順書で作成したサービスプロバイダーの利用許可を与えてください。

※J-MOTTO「グループウェア」の管理者権限は必要ありません。

なお、ログイン許可するユーザーについては、事前に J-MOTTO 側のユーザー設定において HENNGE ONE からそのユーザーに割り当てられている「UPN」(メールアドレス形式で、お客様によっては UPN=メールアドレスの場合もあり)を J-MOTTO ユーザー設定の「メールアドレス」に設定してください。

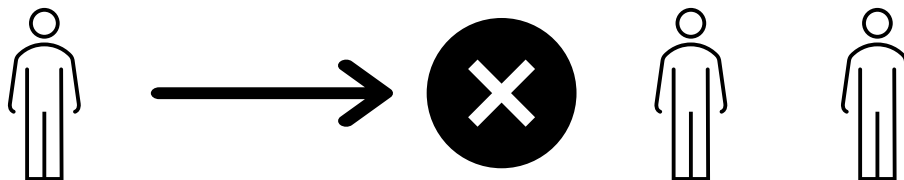
※グループウェア内の通知先メールアドレスではありません。

特に注意頂きたいこと

一つの UPN を、複数の J-MOTTO ユーザーの「メールアドレス」に設定しないでください。
グループウェア内の「プロフィール」は SAML 認証で利用していませんので重複しても問題ありません。

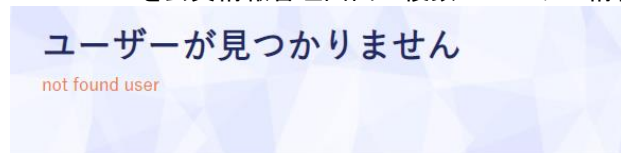
HENNGE ONE 側
ユーザーに割当した「UPN」

J-MOTTO 会員情報管理側
ユーザー設定の「メールアドレス」



J-MOTTO においてはこの「UPN」の情報と会員情報管理上のユーザー情報「メールアドレス」を照合してユーザーID(数字五桁)の部分特定し、ログイン済情報をログイン者(ブラウザ)に渡します。
そのため、HENNGE ONE の一つの UPN を J-MOTTO 側の複数アカウントに同時に設定された場合には、SAML 認証としてはどのユーザーID がログイン対象者が特定できないため、J-MOTTO 画面ではログインエラーとなります。

例: 一つの UPN を会員情報管理画面の複数のユーザー情報に登録していた場合のエラー画面例



[トップ](#) > ユーザーが見つかりません

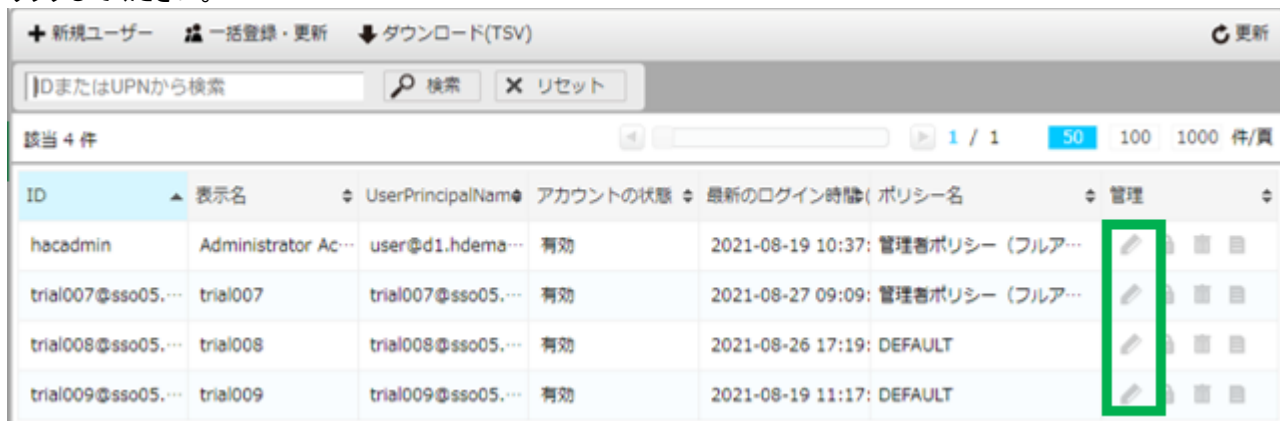
ログイン元のサービスと一致するJ-MOTTOユーザーが存在しません。
管理者に設定状況を確認してください。

HENNGE ONE での実際の許可設定













HENNGE ONE にログインし、サイドメニューの「ユーザー一覧」をクリックします。



ユーザー追加(削除)画面になりますので、HENNGE ONE によるログインを許可したいユーザーで鉛筆アイコン(編集)をクリックしてください。



The screenshot shows the user management interface. At the top, there are buttons for '+ 新規ユーザー', '一括登録・更新', and 'ダウンロード(TSV)', along with a search bar and a '更新' (Refresh) button. Below the search bar, it says '該当 4 件' (4 items match). The table below lists users with columns for ID, 表示名 (Display Name), UserPrincipalName, アカウントの状態 (Account Status), 最新のログイン時間(ポリシー名) (Last Login Time (Policy Name)), and 管理 (Management). The pencil icon in the '管理' column for the first user is highlighted with a green box.

ID	表示名	UserPrincipalName	アカウントの状態	最新のログイン時間(ポリシー名)	管理
hacadmin	Administrator Ac...	user@d1.hdema...	有効	2021-08-19 10:37: 管理者ポリシー (フルア...	  
trial007@sso05...	trial007	trial007@sso05...	有効	2021-08-27 09:09: 管理者ポリシー (フルア...	  
trial008@sso05...	trial008	trial008@sso05...	有効	2021-08-26 17:19: DEFAULT	  
trial009@sso05...	trial009	trial009@sso05...	有効	2021-08-19 11:17: DEFAULT	  

【J-MOTTO 会員ログイン】SAML 認証ログインマニュアル

「許可するサービスプロバイダー」で作成したサービスプロバイダーにチェックを入れ、「送信」をクリックしてください。



ユーザー編集

OTP通知メールアドレス

非常用OTPトークン: ntoj1pe4 pc90kpr1 2rrrtml1 ld852nbl rfzvtr4

OTP共有鍵: yNHa6ZtFTX7Q8Vtu 生成する

QRコード

アクセスポリシーグループ: *DEFAULT

許可するサービスプロバイダー

- HENNGE Secure Transfer
- j-motto_saml_dev
- HENNGE Email DLP

送信

管理者側の設定は以上になります。

5 一般ユーザー向け(ログインの仕方について)

本操作で HENNGE ONE のログイン画面を利用した J-MOTTO グループウェアログインの方法をご案内します。

手順1

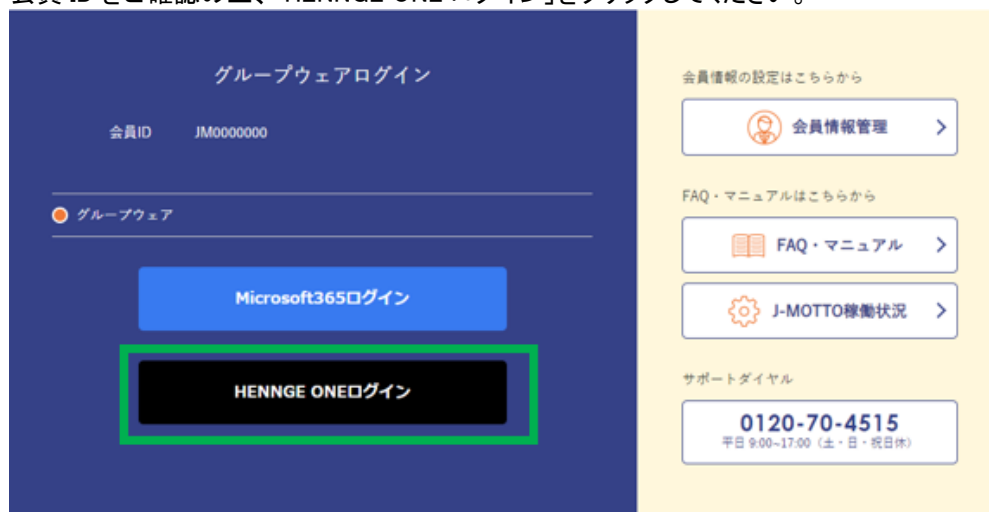
以下の URL にブラウザで直接アクセスします。
(ブラウザのお気に入りなどに登録されても構いません)
<https://www2.j-motto.co.jp/web/doLogin/>(会員 ID)

例:

<https://www2.j-motto.co.jp/web/doLogin/JM0000000>

手順2

J-MOTTO サイトからのログインとは異なり、(手順1の URL に対応した)会員 ID が表示されたページになりますので、会員 ID をご確認の上、「HENNGE ONE ログイン」をクリックしてください。



手順3

HENNGE ONE のログイン画面になるので「HENNGE ONE ログイン」で普段利用されている ID と PW でログインをしてください。

ログイン成功後はグループウェアの画面となります。

注意点

HENNGE ONE のログイン画面でエラーが出た場合は普段ご利用中の HENNGE ONE の ID、パスワードの入力に誤りがないかご確認ください。

J-MOTTO のサイト画面でエラーが出た場合は、管理者による利用許可がされていない場合がありますので、お客様で HENNGE ONE を管理されている管理者にご相談ください。

お客様ご契約の HENNGE ONE のパスワードについては、J-MOTTO お客様サポートセンターではお答えできませんのでご注意ください。

お問い合わせ

J-MOTTO お客様サポートセンター	
TEL	0120-70-4515 (通話料無料) 平日 10:00～17:00 (土・日・祝日休)
チャット	https://www.j-motto.co.jp/00000000/manual/ (上記 WEB サイト内右下部) 平日 09:00～18:00 (土・日・祝日休)
メール	support@j-motto.co.jp

ご不明な点がございましたら、お気軽にお問い合わせください。