SAML 認証マニュアル



Copyright (C) NI Consulting Co., Ltd. All rights reserved.

1.はじめに	2
1-1.SAML 認証の概要	2
1-2.設定の流れ	7
2 セットアップ壬順(IdP・ΔD FS の提合)	٩
2. Cノーツ ノノ デルペ (101, AD + 3 0) 勿口 /	ر ع
2-1-2 事前進備	9
2-3.NI 製品の設定	
2-4.IdPの設定(Windows Server 2012 R2)	
2-5.IdPの設定(Windows Server 2016 – ÁDFS)	32
2-6.IdP の設定(Windows Server 2019)	48
2-7.仮名 ID 取得	49
2-8.動作確認	50
2-9.トラブルシューティング	51
2-10.運用時の注意	55
3.セットアップ手順(IdP: Microsoft Entra ID の場合)	56
3-1.システム構成	56
3-2.IdP の設定	56
3-3.NI 製品の設定	63
3-4.仮名 ID 取得	67
3-6.トラノルシューティング	
3-7. 建用时仍注息	
4.トラブルシューティング	71
4-1.シングルサインオンができない場合の対応方法	71
4-2.SAML 認証のログを確認する	72
4-3.SAML 認証エラーの原因を調べる。	73
4-4.1dP に接続个可の端末から NI 製品にアクセスする	74
5.制限事項	75
5-1.技術的・運用的制限	75
5-2.対応製品	75

1.はじめに

SAML 認証とは、NI 製品へのログインの際、SAML のプロトコルを利用し、シングルサインオン(自動ログイン)を可能とするオプション製品です。



1-1.SAML 認証の概要

1-1-1.SAML とは

SAML とは、認証、認可、ユーザ属性情報などを XML で送受信するための仕様です。

SAML 認証では、SAML2.0 の仕様に基づいたシングルサインオン処理を行います。



具体的には、SAML 認証の導入により以下のようなことが可能となります。

- ・社内の Active Directory ドメインに参加している PC から、NI 製品へのシングルサインオン (※IdP に AD FS を利用し、認証方法に「Windows 認証」を利用している場合)
- ・他社 SAML 対応製品(Google Apps、Microsoft 365 等)に同様の方法でシングルサインオン

•	・SAML 認証は Active Directory と NI 製品のユーザー/グループマスターを
12 注意	連携させるものではめりません。 ・モバイル端末を利用する場合、AD FS プロキシサーバー等を利用し、IdP が外部から
	アクセス可能である必要があります。

1-1-2.SAMLの用語解説

SAML 認証で用いられる特有の用語について、解説します。

用語	詳細	
Identity Provider	認証・認可の情報を提供する役割を担います。	
(以下、IdP)	IdP で認証されたユーザーは SP のサービスにアクセス可能となります。	
	例: AD FS、Microsoft Entra ID	
Service Provider	シングルサインオン対象の Web アプリケーションを指します。	
(以下、SP)	IdP が発行した認証・認可の情報に応じてユーザーにサービスを提供します。	
	例:NI 製品、Google Apps、Microsoft 365	
バインディング	SAML メッセージの送信方法を規定したもの。	
(Binding)	例:HTTP Redirect Binding、HTTP POST Binding	
Active Directory ドメイン	Microsoft 社によって開発されたディレクトリ・サービス・システム。	
サービス(以下、AD)	ユーザーとコンピュータリソースを管理するコンポーネント群の総称です。	
Active Directory フェデレ	Windows Server の機能です。	
ーション サービス	AD のユーザー情報を使用した認証が可能です。	
(以下、AD FS)	SAML 認証では IdP に相当します。	
Microsoft Entra ID	Microsoft 社が提供するクラウドベースの ID およびアクセス管理サービスです。	
	フェデレーションサーバーの機能も有します。	
	SAML 認証では IdP に相当します。	

1-1-3.認証方法について

以下 2 通りの認証方法が利用可能です。

Point	・認証方法は設定画面で切り替え可能です。	
-------	----------------------	--

パスワード認証

IdPのログイン画面にて、ID/パスワードを入力することで認証されます。

組織アカウントを使用してサインインしてください
someone@example.com
パスワード
9 AUAU
2012 Marcane

Windows 認証

ドメインにログイン済みの Windows PC にて、Microsoft Edge、または Google Chrome を 使用している場合、自動で認証されます。

それ以外の場合、認証ダイアログが表示され、ID/パスワードを入力することで認証されます。

	Windows 認証を利用する場合、コントロールパネルから下記の設定を行う必要があります。
	1. [インターネット オプション] > [セキュリティ]に移動します。
	2. 「ローカルイントラネット」が選択された状態で、「レベルのカスタマイズ」ボタンをクリック
	します。
	3.「ユーザー認証」>「ログオン」で「イントラネットゾーンでのみ自動的にログオンする」を
~	選択し、「OK」ボタンをクリックします。
注意 注意	4. 「ローカルイントラネット」が選択された状態で、「サイト」 ボタンをクリックします。
-	5.「詳細設定」ボタンをクリックします。
	6.「この Web サイトをゾーンに追加する」部分に「https:// <idp サーバーのアドレス="">」を</idp>
	入力し、「追加」ボタンをクリックします。
	※ <idp サーバーのアドレス="">は、システム管理者にお問い合わせください。</idp>
	7. ご使用のブラウザを再起動します。

「ローカルイントラネット」ではなく「インターネット」、または「信頼済みサイト」として設定
される場合は、上記の「3.」で「現在のユーザー名とパスワードで自動的にログオンする」を選択
してください。

1-1-4.ユーザーアカウント連携方法について

SAML 認証では、IdP と NI 製品間でユーザーアカウントの紐付けが必要です。ユーザーアカウントの紐付けには、 以下の 2 通りの方法が利用可能です。



仮名を利用する方法

IdP が発行するランダム文字列(仮名 ID)を用いて認証を行います。

- ・各ユーザーは初回ログイン時に、仮名取得の作業を行う必要があります。仮名取得後、次回のログイン時 からシングルサインオンが可能となります。
- ・NI 製品の社員ログイン ID と、IdP のユーザーID を一致させておく必要はありません。

社員ログイン ID を利用する方法(仮名を利用しない方法)

NI 製品の社員ログイン ID と IdP のユーザーID をシステムが自動で紐付け認証を行います。

・各ユーザーは初回ログイン時からシングルサインオンが可能となります。

・NI 製品の社員ログイン ID と、IdP のユーザーID を一致させておく必要があります。

1-1-5.IdP による動作の違い

基本的には SAML2.0 に対応した IdP 製品であれば認証可能ですが、IdP 製品により一部機能が制限される場合 があります。

【IdP のシングルサインオン機能対応表】

機能名	AD FS	Microsoft Entra ID
認証方法:パスワード認証	0	0
認証方法:Windows 認証	0	×
仮名	0	0



・ IdP の動作確認は AD FS、Microsoft Entra ID でのみ行っております。 動作確認済みシステム構成は、下記 2.~4.のセットアップ手順をご確認ください。

1-2.設定の流れ

1-2-1.事前準備

設定を行う前に以下の作業が必要です。

- ・NI製品へ社員情報の登録
- ・ディレクトリサービス(Active Directory、Microsoft Entra ID)動作環境の構築
- ・ディレクトリサービス(Active Directory、Microsoft Entra ID)へユーザーアカウントの登録

1-2-2.SSL(https)での接続設定を行う

SAML 認証を利用する場合、SSL(https)での接続が必須となります。

システム設定画面の「セキュリティ > 全体接続制限」より、「SSL(https) での接続のみ許可する」にチェック

して、「保存する」をクリックします。

※携帯版は SAML 認証に非対応のため、http 接続も可能です。

セキュリティ > 制限/全体接続制限		
接続制限設定を間違え 全体接続制限を設定す 次に設定した個人で 接続方法の制限で「S SSLでの接続ができた SSLは443ボート固定 全体接続制限の設定す	えると製品に接続できなくなる恐れがあります。 する場合は、まず個別接続制限で個人(システム管理者以外を推奨)を設定してください。 製品にログインし設定情報が正しいことを確認した上で設定してください。 SSL(https)を用いた接続のみを許可する」場合は、実際にhttpsでの接続ができることを確認した よい場合は、別途サーバー側に設定が必要です。 ことなります。 まての まで個別接続制限にも反映させたい情報は、個別接続制限にも設定してください。	
低仔		
接続元の制限:	標準版への接続 携帯版への接続	
	許可するIPアドレスを改行区切りで入力してください。 未設定の場合はすべてのIPアドレスからの接続が許可されます。 ここで指定したIPアドレスからの接続しかできなくなります。 *(アスタリスク)での指定が可能です。(例:192.168.1.*の場合は最後の桁が無視されます。)	
接続方法の制限:	SSL(https)を用いた接続のみを許可する 除外対象: ■標準版 ■携帯版 ■アプリ SSLでの接続ができない場合は、別途サーバー側に設定が必要です。 SSLは443ポート固定となります。	

1-2-3.設定ステップ

SAML 認証によるシングルサインオンを利用するには、以下の設定ステップを実施します。



Step 1

NI 製品の設定	NI 製品のシステム設定を行い、SP メタデータをダウンロードします。 IdP のメタデータを NI 製品にアップロードします。
Step 2	
IdP の設定	SP メタデータをアップロードし、IdP の設定を行います。
Step3	
仮名 ID 取得 (※仮名を利用する場合のみ)	各ユーザーが初回ログイン後に、オプション設定画面より、仮名 ID を取得 します。
Step4	
	シングルサインオンが可能であることを確認します。

2.セットアップ手順(IdP:AD FS の場合)

2-1.システム構成

以下の構成でセットアップを行います。

・認証サーバー

ディレクトリサービス	AD	
IdP	AD FS	
OS	Windows Server 2012 R2 Standard	
	Windows Server 2016 Standard	
	Windows Server 2019 Standard	
	(※基本的に上記すべての OS で設定方法は同様であるが	
	「IdPの設定」のみ、OSの種類によって画面が異なるため、	
	2-4~2-6 と分けて記載します。)	
IdP サーバーのアドレス	adfs.ni-saml.com	
	(※設定手順内の IdP サーバーのアドレスは、実際に使用するものに置き換えて	
	ください。)	

※AD と AD FS は、同一のサーバー上で稼働するものとします。

※AD、AD FS のインストール手順の詳細は、Microsoft 社の情報をご確認ください。

2-2.事前準備

2-2-1.証明書の準備

第三者認証機関が承認した、認証に使用する AD FS のサーバー証明書を.pfx 形式でエクスポートします。 証明書を取得する一般的な方法には、OpenSSL を使用する方法、Certreq.exe を使用する方法、IIS を使用す る方法の 3 種類があります。(※詳細は認証局の設定手順にしたがってください。)

OpenSSL を使用する方法は、以下 Microsoft 社の情報もご確認ください。

https://docs.microsoft.com/ja-jp/azure/app-service/configure-ssl-certificate#export-certificate-topfx

2-2-2.AD FS の構成

1.サーバーマネージャーより「このサーバーにフェデレーションサービスを構成します。」をクリックします。



2. 「フェデレーションサーバーファームに最初のフェデレーションサーバーを作成します」を選択し、「次へ」を クリックします。



3.「次へ」をクリックします。

a	Active Directory フェデレーション サービス構成ウィザード	_ D X
Active Director	y ドメイン サービスへの接続	ターゲット サーバー adfs.ni-saml.com
ようこそ AD DS への接続 サービスのプロパティの指定 サービス アカウントの指定 データペースの指定 オプションの確認 前提条件の確認 インストール 結果	フェデレーション サービス構成を実行するための Active Directory ドメイン管理者のアク カウントを指定してください。 NI-SAML¥administrator (現在のユーザー) 変更(<u>C</u>)…	セス許可を持っているア
	<前へ(P) 次へ(N) > 構成(C) キャンセル

4.「インポート」をクリックし、.pfx 形式の証明書ファイルを選択します。 証明書にパスワードが設定されている場合は入力して「OK」をクリックします。

B	Active Directory フェデレ-	-ション サービス構成ウィザード
サービスのプロパティ	ィの指定	ターゲット サーバー adfs.ni-saml.com
ようこそ AD DS への接続 サービスのプロパティの指定	SSL 証明書:	▼ インポート(I) 表示
サービス アカウントの指定 データベースの指定	フェデレーション サービス名:	▼ 例: fs.contoso.com
オプションの確認 前提条件の確認 インストール 結果	フェデレーション サービスの表示名:	* ユーザーはサインイン時に表示名を確認します。 例: Contoso Corporation
		< 前へ(P) 次へ(N) > 構成(C) キャンセル
· · · · · · · · · · · · · · · · · · ·		
	書のパスワードの入力 されています。秘密キーのパスワードを入力して	X
	OK(0)	キャンセル(C)

5.フェデレーションサービスの表示名を入力し、「次へ」をクリックします。

※表示名は、パスワード認証使用時に、IdPのログイン画面に表示される名称です。

a	Active Directory フェデレー	-ション サービス構成ウィザード	_ D X
サービスのプロパテ	んの指定	ad	ターゲット サーバー fs.ni-saml.com
ようこそ AD DS への接続 サービスのプロバティの指定	SSL 証明書:	adfs.ni-saml.com ▼ 表示	インボート(<u>I</u>)
サービス アカウントの指定 データベースの指定	フェデレーション サービス名:	adfs.ni-saml.com v	
オブションの確認 前提条件の確認 インストール 結果	フェデレーション サービスの表示名:	NI Consulting ユーザーはサインイン時に表示名を確認します。 例: Contoso Corporation	
1100			
		<前へ(<u>P</u>) 次へ(<u>N</u>) > 構成(<u>C</u>)	キャンセル

6.サービスアカウントに「Administrator」を選択し、パスワードを入力し、「次へ」をクリックします。

a	Active Directo	ory フェデレーション サービ	ス構成ウィザード	_ D X
サービス アカウント	の指定			ターゲット サーバー adfs.ni-saml.com
▲ KDS ルート キーが設定されて	「いないため、グループ管理	里サービス アカウントを利用できま	ŧせん。 次の PowerShe	ell コマンドを… 詳細表示 ×
ようこそ AD DS への接続 サービスのプロパティの指定	ドメイン ユーザー ア ○ グループ管理サ	カウントまたはグループの管理され ービス アカウントを作成します	たサービス アカウントを打	旨定してください。
サービスアカウントの指定	アカウント名:	NI-S/	AML¥	
データベースの指定	◎ 既存のドメイン:	ユーザー アカウントまたはグループ	の管理されたサービス フ	アカウントを使用してください
オプションの確認 前提条件の確認	アカウント名:	*<未排	旨定>	選択(<u>S</u>)
も見				
		<前へ(P)	次へ(<u>N</u>) >	構成(<u>C</u>) キャンセル
<u>л_+</u> +	・または サービス アナ	ロウント の選択	x	
オゴミェクトの運輸の設現(の)。				
ユーザー または サービス アカウント		オブジェクト	の種類(0)	
場所の指定(F):				
ni-saml.com		場所	ŕ(L)	
選択するオブシェクト名を入力してくださ	い (<u>例</u>)(E):			
Administrator		名前の	₩確認(C)	
; 詳細設定(A)		ок	キャンセル	

B	Active Directory 71	デレーション サービス構成ウィザード
サービス アカウント	の指定	ターゲット サーバー adfs.ni-sami.com
▲ KDS ルートキーが設定されて ようこそ AD DS への接続 サービスのプロパティの指定 サービス アカウントの指定 データペースの指定 オプションの確認 前提条件の確認 インストール 結果	 いないため、クループ管理サービス ドメイン ユーザー アカウント表 ○ グループ管理サービス ア: アカウント名: ④ 既存のドメイン ユーザー アカウント名: アカウント名: アカウント名: アカウント名: 	くアカウントを利用できません。次の PowerShell コマンドを… 詳細表示 × たはグループの管理されたサービス アカウントを指定してください。 カウントを作成します NI-SAML¥ アカウントを成功レープの管理されたサービス アカウントを使用してください NI-SAML¥ NI-SAML¥ ●●●●●●●●●● ●●●●●●●●●
		<前へ(P) 次へ(N) > 構成(C) キャンセル

7. 「Windows Internal Database を使用してサーバーにデータベースを作成します。」を選択して、「次へ」をクリックします。

B	Active Directory フェデレーション	サービス構成ウィザード	_ 🗆 X
▶ ▶	Active Directory フェデレーション つ 指定 Active Directory フェデレーション サービス © Windows Internal Database を使 O SQL Server データベースの場所を指述 データベースのホスト名: データベース インスタンス:	サービス構成ウイザード の構成データを格納するためのデータベースを 用してサーバーにデータベースを作成します。 こしてください。 既定のインスタンスを使用するには、このフィ にします。	ターゲット サーバー adfs.ni-saml.com 指定してください。
	< fi	项へ(<u>P)</u> ズへ(<u>N</u>) > 構成(2) ≠ 72711

8.「次へ」をクリックします。

6	Active Directory フェデレーション サービス構成ウィザード
オプションの確認	ターゲット サーバー WIN-642PECKEL6K.ni-saml.com
ようこそ AD DS への接続 サービスのプロパティの指定 サービス アカウントの指定 データペースの指定 オブションの確認 前提条件の確認 インストール 結果	次の選択を確認してください: このサーバーは、新しい AD FS ファーム 'ni-saml.com' でプライマリ サーバーとして構成されます。 AD FS 構成は Windows Internal Database に格納されます。 Windows Internal Database 機能がこのサーバーにまだインストールされていない場合はインストールされま す。 NI-SAML¥Administrator として実行されるようにフェデレーション サービスが構成されます。
	これらの設定は、追加のインストールを自動化する Windows PowerShell スクリプトに エクスポートできます スクリプトの表示(V)
	<前へ(P) 次へ(N) > 構成(C) キャンセル

9.「構成」をクリックします。

画面に「このサーバーは正常に構成されました」と表示されることを確認します。



	Active Directory フェデレーション サービス構成ウィザード	_ □ ×
結果		ターゲット サーバー adfs.ni-saml.com
	れました	詳細表示 ×
ようこそ AD DS への接続 サービスのプロバティの指定 サービス アカウントの指定 データペースの指定 上書きの確認 オプションの確認 前提条件の確認 インストール 結果	✓ 詳細な操作結果を表示する(V)]
	フェデレーション サービス展開を完了するために必要な次の手順	
	< 前へ(P) 次へ(N) >	閉じる キャンセル

2-3.NI 製品の設定

2-3-1.システム設定

1.システム設定の セキュリティ より「SAML 認証」を選択します。

⇒「認証/SAML 認証」画面が表示されます。

2.以下の項目を入力し、

ボタンをクリックします。

項目名称	説明	設定値
シングルサインオン設定	· 定	
シングルサインオン	シングルサインオンを利用するかしないかを設定します。	利用する
有効範囲	SAML 認証を許可する接続元 IP アドレスを改行区切りで指定し	※補足を参照
	ます。空白の場合は、すべての接続で SAML 認証を行います。	
Service Provider(NI 掌	製品)設定	
エンティティ ID	Service Provider の識別子。任意の文字列を設定します。	https://xxx.xxx.xxx.xxx/ni/
	※初期値の URL から変更する必要はありません。	
エンドポイント URL	SAML レスポンスを受信する URL です。	-
	※Identity Provider のセットアップに使用する固定値です。	
仮名	仮名 ID を用いた認証を利用するかしないかを設定します。	利用する / 利用しない
認証方法	認証にパスワード認証を用いるか、Windows 認証を用いるかを	Windows 認証 / パスワード認証
	設定します。	
ログアウト URL	NI 製品からログアウト後に遷移する URL を設定します。	https:// <idp td="" サーバーのアドレ<=""></idp>
		ス>/adfs/ls/?wa=wsignout1.0
		(※IdP のログアウト画面)

	・NI 製品からログアウトする際に、IdP からもログアウトする必要がない場合は、 ログアウト URL に下記 URL を設定することで、通常の NI 製品ログイン画面に遷移します。
▲ 補足	https://<任意の NI 製品 URL>?saml=no
	・社内端末の IP アドレスを「有効範囲」に指定することで、モバイル端末など社外からの接続に
	より IdP に接続不可の場合は、「有効範囲」外となるため、SAML 認証が適用されず、通常の ログイン画面が表示されます。
1 注意	・エンティティ ID、仮名を変更した場合、IdP の再設定が必要になります。

・仮名を利用するかしないかで、IdPの設定手順が異なります。

3.IdP メタデータをアップロードします。

下記 URL にブラウザでアクセスし、IdP メタデータ XML ファイルを PC に保存します。

https://<IdP サーバーのアドレス>/FederationMetadata/2007-06/FederationMetadata.xml

NI 製品システム設定「認証/SAML 認証」画面の、Identity Provider 設定の「メタデータ」に

上記で保存した IdP メタデータ XML ファイルを添付します。

読み込みボタンをクリックします。



以下の設定項目が自動で入力されます。

項目名称	説明	設定サンプル値
Identity Provider 設定		
エンティティ ID	Identity Provider の識別子を設定します。	http:// <idp td="" サーバーのアドレス<=""></idp>
		>/adfs/services/trust
エンドポイント URL	SAML リクエストを送信する URL を設定します。	https:// <idp td="" サーバーのアドレ<=""></idp>
		ス>/adfs/ls/
証明書	Identity Provider が署名に使用する公開鍵を設定します。	Base64 エンコードされた文字列
	カンマ区切りで複数証明書を指定できます。	

4.SP メタデータをダウンロードします。

Service Provider(NI 製品)設定の「メタデータ」の ダウンロード ボタンをクリックします。



⇒SP メタデータ XML ファイルがダウンロードされます。次項「<u>2-4.IdP の設定 (Windows Server 2012</u> R2)」または「2-5.IdP の設定(Windows Server 2016 – ADFS)」にて使用します。

5. 保存 ボタンをクリックします。

2-4.IdPの設定(Windows Server 2012 R2)

IdP サーバーで下記の設定を行います。

2-4-1.証明書利用者信頼(SP)の追加

1.AD FS の管理ツールを表示し、「証明書利用者信頼の追加」をクリックします。



2.証明書利用者信頼の追加ウィザードが表示されたら、「開始」をクリックします。

\$ 1	証明書利用者信頼の追加ウィザード	x
ようこそ		
ステップ ・ ようこそ ・ データ ソースの違訳 ・ 今すぐ多要素認証を構成しますか? ・ 発行承認規則の違訳 ・ 信頼の追加の準備完了 ・ 完了	証明書利用者信頼の追加ウィザードの間始 このウィザードでは、新しい証明書利用者信頼を AD FS 構成データベースに追加します。証明書利用者が このフェアレーション サービスによって発行されたゼキュリティ トークンの要求を使用して認証および承認の決定 行います。 このウィザードで作成する証明書利用者信頼では、フェアレーション サービスが証明書利用者を認識する方 法 あたび渡印書利用者信利者の要求の発行方法を定義します。このウィザードの完了後、証明書利用者 要求を発行するための発行変換規則を定義できます。	t. 王を 新に
	< 前へ(P) 開始(S) キャンセ ノ	ŀ

3. 「証明書利用者についてのデータをファイルからインポートする」を選択し、「参照」ボタンを クリックします。

「2-3-1.システム設定」でダウンロードした SP メタデータを選択します。





信頼の追加の準備完了	
 ステップ よこそ テータソースの違訳 表示名の指定 タイシッ果和記証を構成しま すか? 発行承認規則の違訳 信頼の追加の準備完了 完了 	証明書利用者信頼が構成されました。次の設定を確認し、し次へ】をクリックして、AD FS 構成データベースに証明書利用者信頼を追加して(ださい。) 監視 識別子 暗号化 署名 受け付ける要求 組織 エンドポイント 注意事項 詳細設定 SAML プロトコルおよび WS-FederationPassive プロトコルに使用するエンドポイントを指定してください。 URL イン パインデ 既定 応答 URL SAML アサーション コンシューマー エンドポイント https://xxx.xxx.xxx/ni 1 POST (14)12 1

4.表示名を入力し、「次へ」をクリックします。

※表示名は AD FS の管理ツール上で表示される名称です。

\$	証明書利用者信頼の追加ウィザード	x
表示名の指定		
ステップ	この証明書利用者の表示名およびオプションの注意事項を入力してください。	
💩 ಕಿನಿದಕ	表示名(D):	
🥥 データソースの選択	NI-SP	
◎ 表示名の指定	注意事項(0):	
 今すぐ多要素認証を構成しますか? 		^
◎ 発行承認規則の選択		
◎ 信頼の追加の準備完了		
❷ 完了		
	< 前へ(P) 次へ(N) > キャンセノ	ŀ

5.「現時点ではこの証明書利用者信頼に他要素認証を構成しない」を選択し、「次へ」をクリックします。

\$	証明書利用者信頼の追加ウィザード
ステップ ● ようこそ ● データ ソースの選択	この証明書利用者信頼の多要素認証設定を構成します。指定した要件のいずれかに一致する場合、多要素認証が必要です。
 ● 表示名の指定 ● 今すぐ多要素認証を構成しま オか? 	多要素認証 クローバル設定 要件 ユーザー/グループ 未構成
 発行承認規則の選択 信頼の追加の準備完了 完了 	デバイス 未構成 場所 未構成
	 現時点ではこの証明書利用者信頼に多要素認証を構成しない。(1) この証明書利用者信頼に多要素認証設定を構成する。(C) 認証ポリシーノードに移動して、この証明書利用者信頼に多要素認証設定を構成することもできます。詳細については、認証ポリシーの構成を参照してください。
	<前へ(P) 次へ(N) > キャンセル

6.「すべてのユーザーに対してこの証明書利用者へのアクセスを許可する」を選択し、「次へ」をクリックします。

\$	証明書利用者信頼の追加ウィザード
発行承認規則の選択	
 ステップ ようこそ データ・ソースの違択 表示名の指定 今すぐ多要未認証を構成しますが? 発行承認規則の道知 信頼の追加の準備完了 完了 	 第行承認規則にとって、証明書利用者の要求の受信をユーザーが許可されるかどうかが決まります。この証明書利用者の発行承認規則の利期動作として、次のいずれかのオジュンを選択してください。 すべてのユーザーに対してこの証明書利用者へのアクセスを許可する(A) すべてのユーザーに対してこの証明書利用者へのアクセスを許可する(A) すべてのユーザーに対してこの証明書利用者へのアクセスを許否することもできます。 すべてのユーザーに対してこの証明書利用者へのアクセスを拒否する(D) すべてのユーザーに対してこの証明書利用者へのアクセスを拒否する(D) すべてのユーザーに対してこの証明書利用者へのアクセスを拒否するように証明書承認規則が構成されます。 ユーザーかこの証明書利用者にアクセスできるようにするには、後で発行承認規則が増成されます。 この証明書利用者の発行承認規則を変更するには、証明書利用者信頼を選択し、操作ウィンドウで「要求規則の編集」をクリックしてください。
	<前へ(P) 次へ(N) > キャンセル

7.「次へ」をクリックします。



8.証明書利用者信頼の追加が完了したので、「閉じる」ボタンをクリックします。

\$	証明書利用者信頼の追加ウィザード
完了	
ステップ ようこそ データソースの選択 表示名の指定 今すぐや要素認証を構成しますか? 発行承認規則の選択 信頼の追加の準備完了 完了 	証明書利用者信頼が AD FS 構成データベースに追加されました。 AD FS の管理スナップインの [プロパティ] ダイアログ ボックスを使用して、この証明書利用者信頼を変更できま す。 ▼ ウィザードの終了時にこの証明書利用者信頼の [要求規則の編集] ダイアログを開く(O)
	開Uる(C)

1.AD FS の管理ツールを表示し、「証明書利用者信頼」メニューを選択します。 追加した証明書利用者信頼を右クリックし、「プロパティ」を選択します。

\$	AD	FS		_ 🗆 X
🧌 ファイル(F) 操作(A) 表示(V) ウィンドウ(W) ヘルプ(H)			_ 8 ×
AD FS	· 証明書利用者信頼			操作
p = 5-CA ▲ = 信頼関係	表示名 Device Registration Service	(はい)	種類 識別子 WS-T., urn:ms-drs:ni-sam	証明書利用者信頼 ▲
一 東支市ルマター信頼 「 毎日書利田秀信頼」	NI-SP フェデレーション メタデータから更新(更新(い)	WS-T., https://ni-sfa-nl/	証明書利用者信頼の追加
通行に行う	要求規則の編集(E)			表示 •
▶ 🧰 認証ボリシー	Ⅲah(S)			ファから新しいウィンのウ
	プロパティ			
	削除(D)			
	へルプ(H)			1007
				NI-SP 🔺
				フェデレーション メタデータから更新
				要求規則の編集
				無効
				プロパティ
				🗙 削除
				👔 へいプ
選択した証明書利用者信頼の要求規則を編集します				1

2.SAML リクエスト用エンドポイントの追加

「エンドポイント」タブを選択し、「SAMLの追加」をクリックします。

NI-SP のプロパ	ም	x
監視 識別子 暗号化 署名 エンドポイント プロキシ エンドポイント SAML プロトコルおよび WS-FederationPassiv イントを指定してください。	受け付ける要求 注意事項 re プロトコルに使	求 組織 詳細設定 用するエンドポ
URL イン SAML アサーション コンシューマー エンドポー https://xxx xxx xxx xxx/ni/z 1	バインデ… 月 <mark>イント</mark> POST (既定 応 いえ
< III SAML の追加(D) WS-Federation の追加(W) OK キ	削除(R) 「 Fヤンセル	> 編集(E) 適用(A)

下記の値を設定し、「OK」をクリックします。

- ・エンドポイントの種類:「SAMLアサーションコンシューマー」を選択します。
- ・バインディング:「Redirect」を選択します。
- ・「信頼された URL」:次の URL を入力します。

https://<IdP サーバーのアドレス>/adfs/ls/

エンドポイントの追加
エンドポイントの種類(E): SAML アサーション コンシューマー
バインディング(<u>B</u>): Redirect
 □ 信頼された URL を既定として設定する(S) インデックス(N):
信頼された URL(T): https://adfs.ni-saml.com/adfs/ls/
例: https://sts.contoso.com/adfs/ls 応答 URL(<u>R</u>):
例: https://sts.contoso.com/logout

3.ログアウト用エンドポイントの追加

「エンドポイント」タブを選択し、「SAMLの追加」をクリックします。

NI-SP のプロハ	パティ	x
監視 識別子 暗号化 署名 エンドポイント プロキシェンドポイント SAML プロトコルおよび WS-Federation Passin イントを指定してください。	受け付ける要求 注意事項 ve プロトコルに使用す	<u>組織</u> 洋細設定 なエンドポ
URL イン	バインデ 既定	応
SAML アサーション コンシューマー エンドボ	イントーーーー	
https://xxx.xxx.xxx.xxx/ni/z 1	POST (N();	ž 🛛
SAML の追加(D) WS-Federation の追加(W)	削除(<u>B</u>) 編	集(<u>E</u>)
ОК	キャンセル ì	箇用(A)

下記の値を設定し、「OK」をクリックします。

- ・エンドポイントの種類:「SAML ログアウト」を選択します。
- ・バインディング:「Redirect」を選択します。
- ・「信頼された URL」:次の URL を入力します。

https://<IdP サーバーのアドレス>/adfs/ls/?wa=wsignout1.0

エンドポイントの追加
エンドポイントの種類(E): SAML ログアウト V
バインディング(<u>B</u>): Redirect ・
 □ 信頼された URL を既定として設定する(S) インデックス(N):
信頼された URL(T): https://adfs.ni-saml.com/adfs/ls/?wa=wsignout1.0 例: https://sts.contoso.com/adfs/ls
応答 URL(<u>R</u>):
例: https://sts.contoso.com/logout OK(Q) キャンセル

4.「OK」をクリックします。

	NI-SP (のプロパ	ティ		2
監視 識別 : エンドポイント	子 暗号化 いまう	略 イント	受け付ける	要求	組織 細設定
。 SAML プロトコルお イントを指定してくだ	よび WS-Federatio さい。	onPassiv	e ติดห่วมผล	使用する	5エンドボ
URL		イン	バインデ	既定	応
SAML アサージ	ション コンシューマー	エンドポー	イント		
https://xxx:	xxx xxx xxx/ni/z	. 1	POST	いいえ	
https://adfs	ni-saml.com/ad	. 0	Redirect	いいえ	
SAMI D/J70	トエンドポイント				
https://adfs	ni-saml.com/ad		Redirect	いいえ	
<					>
SAML の追加(D)				
WS-Federation	の追加(<u>W</u>)…	[削除(<u>R</u>)	編集	€(<u>E</u>)
	ОК	4	キャンセル	適	用(A)

仮名を利用する場合



1.以下の2つの変換要求規則を追加します。

要求規則テンプレートに「カスタム規則を使用して要求を送信」を選択して、「次へ」をクリックします。

\$	変換要求規則の追加ウィザード エ
規則テンプレートの選択	
 入万 • 月息りの種類の選択 ● 要求規則の構成 	住成する要求規則のテンプレートを次の一覧から選択してください。各要求規則テンプレートの詳細は説明に記 要求規則テンプレート(C): カスタム規則を使用して要求を送信 ▼ 要求規則テンプレートの説明 カスタム規則を使用すると、規則テンプレートでは作成できない規則を作成できます。カスタム規則は、AD PS 要求規則言語で記述します。次次機能を使用する場合は、カスタム規則を作成する必要があります: ・ 30L 簡性と入アから要求を送信する ・ カスタムの LDAP フィルターを使用して LDAP 層性ストアから要求を送信する ・ カスタムの LDAP フィルターを使用して LDAP 層性ストアから要求を送信する ・ 入力方向の要求の値に材積な次更を加えて要求を送信する ・ 入力方向の要求の値に材積な次更を加えて要求を送信する ・ 以降の規則で使用するだけの目的で要求を送信する
	< 前へ(P) 次へ(N) > キャンセル

以下のカスタムルールをコピー&ペーストし、完了をクリックします。

```
c:[type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname" ]
=> add(
store = "_OpaqueIdStore",
types = ("http://mycompany/internal/persistentId"),
query = "{0};{1};{2}",
param = "ppid",
param = c.Value,
```

param = c.OriginalIssuer);

\$ 1	変換要求規則の追加ウィザード
規則の構成	
ステップ 決則の種類の選択 要求決規則の構成 	カスタムの要求規則(律数の入力方向の要求を必要とする規則)、SOL 厨性ストアから要求を抽出する規則体 と)を構成できます。カスタム規則を構成するには、AD FS 要求規則言語を使用して、1 つ以上のオプションの 案件を発行ステートメントを入力します。 要求規則や名(C): 水統約仮名の発行 規則テンプレート:カスタム規則を使用して要求を送信 カスタム規則(U): S:[type == "("http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name"] => add(store = "_OpaqueIdStore", types = ("http://mycompany/internal/persistentId"), query = "(0):(1):(2)", param = C.Value, param = c.Value, param = c.OriginalIssuer);
	< 前へ(P) 完了 キャンセル

「入力方向の要求を変換」を選択し、「次へ」をクリックします。

\$	変換要求規則の追加ウイザード	x
規則テンプレートの選択		
 規則f ンフレートの 選択 ステップ 規則の種類の選択 要求規則の構成 	作成する要求規則のテンプレートを次の一覧から選択してください。各要求規則テンプレートの詳細は説明に記 またれています。 要求規則テンプレート(C): 入力方向の要求を変換	3
	<前へ(P) 次へ(N) キャンセル	

以下の値を選択し、「完了」をクリックします。

- ・要求規則名:任意の名称を入力します。
- ・入力方向の要求の種類:「http://mycompany/internal/persistentId」をコピー&ペーストで入力します。
- ・出力方向の要求の種類:「名前 ID」を選択します。
- ・出力方向の名前 ID の形式:「永続 ID」を選択します。

\$	変換要求	規則の追加ウィザード
規則の構成		
ステ ⇒ブ ● 規則の種類の選択 ● 要求規則の構成	この規則を構成することにより、 す。オプションとして、入力方向 要求の種類に関連付ける入力 します。	入力方向の要求の種類を出力方向の要求の種類に関連付けることができま の要求の値を出力方向の要求の値に関連付けることをできます。出力方向の 方向の要求の種類と、要求値を新しい要求値に関連付けるかどうかを指定
	要求規則名(C):	
	NameIDとして返却	
	規則テンフレート:人力方向の	
	人力方向の要求の種類(1):	http://mycompany/internal/persistentId
	入力方向の名前 ID の形式 (M)	指定なし ~
	出力方向の要求の種類(0):	名前 ID 🗸 🗸
	出力方向の名前 ID の形式 (E):	永続 ID V
	◉ すべての要求値をパス スル・	ーする(S)
	○ 入力方向の要求の値を異な	なる出力方向の要求の値に置き換える(R)
	入力方向の要求の値(V):	
	出力方向の要求の値(U):	参照(B)
	○ 入力方向の電子メール サコ	フィックス要求を新しい電子メール サフィックスに置き換える(X)
	新しい電子メール サフィッ	
	クス(W):	例: fabrikam.com
		< 前へ(P) 完了 キャンセル

2.「OK」をクリックします。

•	þ.		Ν	NI-SP の要	求規則	」の編集	_		x
	発	行変換	規則 発行承認規則	委任承認規	則				
		次の変換	奥規則は、証明書利用	者へ送信する	要求を指	定します。			
		順序	規則名			発行済み要求			
		1	永続时候名の発行 NamelDとして返却			〈要求規則の表示〉 名前 ID			
								1	▶
		規則(D 追加(A) 規則の)編集(E)	規則の	削除(R)			
								_	
						K キャンセル		適用	(P)



・NameID として、AD のユーザー情報を返すように設定を行います。

1.AD FS の管理ツールを表示し、「証明書利用者信頼」メニューを選択します。 追加した証明書利用者信頼を右クリックし、「要求規則の編集」を選択します。

\$	AD FS			_ 🗆 X
🧌 ファイル(F) 操作(A) 表示(V) ウィンドウ(1	W) ヘルプ(H)			_ 8 ×
AD FS	証明書利用者信頼			操作
	表示名 Device Registration Service	有効 種類 はい WS-	頁 識別子 -T urn:ms-drs:ni-sam	証明書利用者信頼 ▲
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	NI-SP ファデレーション・ソクデータから更好(1.0)	WS-	-T https://ni-sfa-nl/	記名目が1万日に残りに加い。
	要求規則の編集(E)			
▷ 🧰 認証ポリシー	##X9(S)			ここから新しいウィンドウ
	プロパティ			日本の情報に更新
	削除(D)			
	ヘルプ(H)			
				NI-5P
				フェブレーション メップ 一クから走向 亜皮相肌の症性
				10-31-30-0-30-0-0-0-0-0-0-0-0-0-0-0-0-0-
	<		>	
選択した証明書利用者信頼の要求規則を編集します	p			

2.「規則の追加」ボタンをクリックします。

\$	NI-SP の要求規則の編集	- 🗆 X
発行変換規則 発行承認	2規則 委任承認規則	
次の変換規則は、証明書	書利用者へ送信する要求を指定します。	
順序 規則名	発行済み要求	
		1
		-
規則の追加(A)	規則の編集(E) 規則の削除(R)	
	OK キャンセル	レ 適用(P)

3.以下の要求規則を追加します。

要求規則テンプレートに「LDAP 属性を要求して送信」を選択し、「次へ」をクリックします。

\$	変換要求規則の追加ウイザード ×
規則テンプレートの選択	
ステップ 規則(の獲貨の)選択 要求規則(の構成) 	作成する要求規則のテンプレートを次の一覧から選択してください。各要求規則テンプレートの詳細は説明に記 数されています。 要求規則テンプレート(G): □DAP 腐性を要求として送信 ■ マ ■ 要求規則テンプレートの説明 □DAP 腐性を要求として送信計規則テンプレートを使用すると、Active Directory などの、DAP 腐性スト 対応腐性を選択して送信計規則テンプレートを使用すると、Active Directory などの、DAP 腐性スト 対応腐性を選択して送信計規則テンプレートを使用すると、ロック腐性の存在地にして、こうための 値を 2つの現れる出力可の要求として送信する場合にできます。の規則を使用して、2 ーサーのす べてのグループ メンバーシップを選信することできます。グループ メンバーシップを個別に送信する場合は、1 グループ メンバーシップを要求として送信計規則テンプレートを使用します。
	< 前へ(P) (次へ(N) > (キャンセル)

以下の値を選択し、「完了」をクリックします。

- ・要求規則名:任意の名称を入力します。
- ・属性ストア:「Active Directory」を選択します。
- ・LDAP 属性:「SAM-Account-Name」

※ここでは検証のため、AD の「ユーザーログオン名(Windows 2000 より前)」に紐づく

「SAM-Account-Name」を選択しています。

LDAP 属性については、「2-5-3.変換要求規則の追加」の「仮名を利用しない場合」を参照してください。

・出力方向の要求の種類:「名前 ID」を選択します。

\$ 1	変換要求規則の追加ウィザード
規則の構成	
 ステップ 規則の種類の選択 要求規則の構成 	Cの規則依頼成することにより、LDAP 局性の値を要求として送信できます。まず、LDAP 属性の抽出元となる病 性ネパクを選択します。次に、規則的ら発行する出力方向の要求の種類に属性を関連付ける方法を指定しま す。 要求規則论(C): NameID 規則デンプレード: LDAP 属性を要求として送信 属性ストア(S): Active Directory
	〈前へ(P) 完了 キャンセル

1.AD FS の管理ツールを表示し、「認証ポリシー」メニューを選択します。

グローバルプライマリ認証の編集をクリックします。

Space 1		AD FS		_ _ ×
マデイル(F) 操作(A) 表示(V) ウインドウ(M) ヘルプ(H)			_ 8 ×
(+ +) 2 II 🖬 II				
ad FS	認証ポリシー			操作
▲ ● サービス ■ エンボポイント	認証ポリシーの概要		^	BRET-HILE
証明書	フライマル認証教室と多要素認証教室は、グローバ	いまたは証明書利用者信頼ことに構成することができます。		グローバルプライマリ認証の編集
4 11 信頼関係	詳細			クロー/00岁安美GAE0編AG 表示
要求プロバイダー信頼 近日書20日期/信頼	認証ポリシーを構成しています			ここから第しいウィンドウ
	AD FS AJU7			@ 最新の情報に更新
2 認証ポリシー 一般時間を利用する情報ごと	プライマリ認証			NUT
	認識に AD FS を使用するアプリケーションにアクセス クローバルおよびカスタムのプライマリ認識認識定を構成	くするすべてのユーザーには、ブライマリ認証が必要です。次のオブションも 成できます。	使用して、	
	グローバル設定			
	認証方法 エクストラネット フォ イントラネット フォ	+-14288 +-14228 +-14228	編集	
	デバイス認証 無分	ndows acces 効		
	カスタム設定			
	証明書利用者あたり		183里 =	
	多要素認証			
	次のオブションを使用して、ユーザー/グループ、デバー 体介いずわれに通会する場合、各専業が存在の実	イス、および場所データに基づいて、多要素認証設定を構成できます。 PFオー	指定した要	
	ガローバル確定	e () e		
	東件 ユーザー/グループ 未得	構成	編集	
	デバイス 未 増加 まれ	構成		
	2011万法 未	構成		
	カスタム設定			
	証明書利用者あたり		管理	
			Ľ	

2.利用する認証方法を有効にし、「OK」をクリックします。

・パスワード認証の場合

エクストラネット:「フォーム認証」にチェックします。

イントラネット :「フォーム認証」にチェックします。

・Windows 認証の場合

エクストラネット:「フォーム認証」にチェックします。

イントラネット :「フォーム認証」と「Windows 認証」にチェックします。

グローバル認証ポリシーの編集	x
プライマリ 多要素	
認証方法を選択してください。複数の認証方法を選択すると、ユーザーはサインイン#寺に複数の 沢肢から認証方法を選択できるようになります。	選
統合 Windows 認証方法を指定した場合、統合 Windows 認証をサポートするブラウザーでは 定の認証方法として表示されます。	Æ
エクストラネット	
✓ フォーム425社 □ 510月書記25社	
1215491	51
♥ フォーム#28社 ♥ Windows 記2証 ■ 証明月書記2証	
□ デバイス認証を有効にする(E)	
)

2-5.IdPの設定(Windows Server 2016-ADFS)

IdP サーバーで下記の設定を行います。

2-5-1.証明書利用者信頼(SP)の追加

1.AD FS の管理ツールを表示し、「証明書利用者信頼の追加」をクリックします。



2.証明書利用者信頼の追加ウィザードが表示されたら、「要求に対応する」を選択し、

「開始」をクリックします。

🏟 証明書利用者信頼の追加ウ	−⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢⊢<th>×</th>	×
ようこそ		
 ステップ ようこそ データ ソースの選択 アクセス制御ポリシーの選択 信頼の追加の準備完了 売了 	正明書利用者信頼の追加ウィザードの開始 要求に対応するアウゾケーションは、セキュリティトークン内の要求を使用して認証と承認を決定しす。 更大に対応するのクロン用には Web アブリケーション プロキシを通じて公開できます。 証拠し ● 要求に対応しない(N)	
	< 前へ(P) 開始(S) キャンセル	,

3.「証明書利用者についてのデータをファイルからインポートする」を選択し、

「参照」ボタンをクリックします。

「2-3-1.システム設定」でダウンロードした SP メタデータを選択します。

훾 証明書利用者信頼の追加ウ	чザ-ř ×	(
データ ソースの選択		
 ステップ ようこそ データ ソースの選択 アクセス制御ポリシーの選択 信頼の追加の準備完了 完了 	この証明書利用者についてのデータを取得するために使用するオブションを選択してください: ● オンラインまたはローカル ネットワークで公開されている証明書利用者についてのデータをインボートする(M) このオブションを使用すると、フェデレーション、メタデータをオンラインまたはローカル ネットワークで公開している 証明書利用者組織から必要なデータあよび証明書をインボートできます。 フェデレーション メタデータのアドレス (ホスト名または URL)(E): 例 fs contosocom または https://www.contosocom/app ● 証明書利用者についてのデータをアァイルからインボートする(Q) このオブションを使用すると、ファイルの発行テンの検証は行いません。 フェデレーション メタデータカら でください、このワイザードでは、ファイルの現行行ごの検証は行いません。 フェデレーション メタデータファイルの現代(E): Ci¥Users¥Administrator¥Desktop¥sp_metadataxml ● 証明書利用者についてのデータを手動で入力する(T) このオブションを使用すると、この証明書利用者組織についての必要なデータを手動で入力できます。]
	<前へ(<u>P</u>) 次へ(<u>N</u>) キャンセル	





4.表示名を入力し、「次へ」をクリックします。

※表示名は AD FS の管理ツール上で表示される名称です。

 ・ ・	ウィザード	×
ステップ 	この証明書利用者の表示名およびオブションの注意事項を入力してください。 まニックロン	
 ● ボータ ソースの選択 	表示のACD/ NF-SP	
◎ 表示名の指定	xE(Q):	
 アクセス制御ボリシーの選択 ・ 信頼の追加の準備完了 		^
◎ 完了		
		\vee
	< 前へ(P) 次へ(N) > キャンセル	,

5.表示された画面のまま、「次へ」をクリックします。

🧌 証明書利用者信頼の追加ウィザード 🛛 🕹			
アクセス制御ボリシーの選択			
 ステップ ようこそ データソースの選択 表示名の指定 アクセス制御ポリシーの選択 信頼の追加の準備完了 完了 	アクセス制御水りシーを選択してください: 名前 すべてのユーザーにイントラネット アクセスを許可 すべてのユーザーを許可し、MFA を要求 すべてのユーザーを許可し、MFA を要求 すべてのユーザーを許可し、IDストラネット アクセスで MFA を要求 すべてのユーザーを許可し、特定のグループに MFA を要求 すべてのユーザーを許可し、認証されていないデバイスから MFA を… 特定のグループを許可 ★ 水リシー 次の場合にすべてのユーザーを許可する	説明 イントラネット ユーザーにアクセスを許可し すべてのユーザーにアクセスを許可します。 すべてのユーザーにアクセスを許可し、デノ イントラネット ユーザーにアクセスを許可し、デノ イントラネット ユーザーにアクセスを許可し、「ジ オべてのユーザーにアクセスを許可し、認 指定した 1つ以上のグループのユーザー(
	〈前へ	(P) 次へ(N)> キャンセル	

6.「次へ」をクリックします。

翰 証明書利用者信頼の追加ウ	⊣ <i>ฃ</i> −⊦ั	×
信頼の追加の準備完了		
 1 年代の 足 カルウ + 1 アノ 1 ステップ ようこそ データ ソースの 違択 表示名の指定 アクセス 制御 ポリシーの 選択 信頼の追加の 準備完了 完了 		
	< 前へ(<u>P</u>) 次へ(<u>N</u>) > キャンセ	ιL
7.証明書利用者信頼の追加が完了したので、「このアプリケーションの要求発行ポリシーを構成する」に

チェックを付けたまま、「閉じる」ボタンをクリックします。

	17	
🥦 証明書利用者信頼の追加り	17-ト	X
完了		
ステップ ようこそ データ ソースの選択 表示名の指定 アクセス制御ポリシーの選択 信頼の追加の準備完了 完了 	証明書利用者信頼が正常に3自加されました。	
		閉じる(<u>C</u>)

1.AD FS の管理ツールを表示し、「証明書利用者信頼」メニューを選択します。 追加した証明書利用者信頼を右クリックし、「プロパティ」を選択します。

🧌 AD FS							– 🗆 ×
🧌 ファイル(F) 操作(A) 表示(V) ウィンドウ(W)) ヘルプ(H)						- 6" ×
🗢 🧼 🙇 📰 🛛 🖬							
AD FS	証明書利用者信頼						操作
> 単サービス 第一次クセスを見知ざけとこ。	表示名	;	有効 租	類識別	7	アクセス制御术	証明書利用者信頼 ▲
□ 証明書利用者信頼	NESP		HAX U.	S-T., https	://ni-php7l/ni_saml/	すべてのユーザ	証明書利用者信頼の追加
── 要求フロバイター信頼		フェテレーションメッテーツから更用					表示
アプリケーション クループ		要求発行ポリシーの編集(E)					ここから新しいウィンドウ
		無効(S)					 G 最新の情報に更新
		プロパティ					🛛 ヘルプ
		削除(D)					NI-SP
		ヘルプ(H)					フェデレーション メタデータから更新
							アクセス制御ポリシーの編集
							要求発行ポリシーの編集
							無効
							プロパティ
							🗙 削除
	<					>	
違いしに項目をノエテレージョン メツテーツから更新します							

2.SAML リクエスト用エンドポイントの追加

「エンドポイント」タブを選択し、「SAMLの追加」をクリックします。

NI-SP のプロパティ					×
 監視 識別: エンドポイント SAML プロトコルお イントを指定してくれ 	子 暗号化 プロキシ エンド よび WS-Federa ざい。	署名 ポイント ationPassive	受け付ける 注意事項 e プロトコル(2)	要求 詳細 使用する:	組織 田設定 エンドポ
URL SAML アサーシ	י=דרקרב ה	イン - エンドポイン	バインデ ハ	既定	応
https://xxx	xxx xxx xxx/ni_	<u>.</u> s 1	POST	いいえ	
< SAML の追加()	D)				>
WS-Federation	の追加(<u>W</u>)…		削除(<u>R</u>)	編集	(<u>E</u>)
	ОК	+	ャンセル	適用	Ħ(<u>A</u>)

下記の値を設定し、「OK」をクリックします。

- ・エンドポイントの種類:「SAMLアサーションコンシューマー」を選択します。
- ・バインディング:「Redirect」を選択します。
- ・「信頼された URL」:次の URL を入力します。

https://<IdP サーバーのアドレス>/adfs/ls/

エンドポイントの追加	×
エンドポイントの種業員(E):	
SAML アサーション コンシューマー 💦 🗸	
バインディング(B):	
Redirect ~	
インデックス(<u>N</u>): 0 🚖	
信頼された URL(工):	
https://niadfs5ni-saml.com/adfs/ls/	
例: https://sts.contoso.com/adfs/ls	
応答 URL(<u>R</u>):	
例: https://sts.contoso.com/logout	
OK(() ++	ンセル

3.ログアウト用エンドポイントの追加

「エンドポイント」タブを選択し、「SAMLの追加」をクリックします。

NI-SP のプロパティ		×
監視 識別子 暗号化 署名 エンドポイント プロキシ エンドポイント SAML プロトコルおよび WS-FederationPass イントを指定してください。	受け付ける要求 注意事項 sive プロトコルに使用	組織 詳細設定 するエンドポ
URL イン. SAML アサーション コンシューマー エンドポー	. バインデ 既た イント	包 応
https://xxxxxxxxxxxxxxxx/ni_s 1 https://niadfs5ni-saml.com 0	POSI (۱)(Redirect (۱)(え え
く SAMLの)追加(D)		>
WS-Federation の追加(W)	削除(<u>R</u>)	扁集(<u>E</u>)
ОК	キャンセル	適用(<u>A</u>)

下記の値を設定し、「OK」をクリックします。

- ・エンドポイントの種類:「SAML ログアウト」を選択します。
- ・バインディング:「Redirect」を選択します。
- ・「信頼された URL」:次の URL を入力します。

https://<IdP サーバーのアドレス>/adfs/ls/?wa=wsignout1.0

エンドポイントの追加 ×
エンドポイントの種類(E):
SAML ログアウト 〜
バインディング(B):
Redirect ~
信頼された URL を既定として設定する(S)
信頼された URL(<u>T</u>):
https://niadfs5ni-saml.com/adfs/ls/?wa=wsignout1.0
例:https://sts.contoso.com/adfs/ls
応答 URL(<u>R</u>):
例: https://sts.contoso.com/logout
OK(<u>0</u>) キャンセル

4.「OK」をクリックします。

NI-SP のプロパティ					×
監視 エンドポイント SAML プロトコルお。 イントを指定してくだ	F 暗号化 プロキシエンド はび WS-Federa さい。	署名 ポイント ationPass	受け付ける 注意事項 ive プロトコル(2	要求 新 詳細 使用する1	11織 1設定 ニンドポ
URL SAML アサーショ	-ד-בפעב ענ	イン - エンドポイ	バインデ (ントーーー	既定	応
https://xxxx	oxxxxxxxx/ni_	s 1	POST	いいえ	
https://niadi	5ni-saml.com	/ 0	Redirect	いいえ	
SAML ログアウ https://niadi	トエンドポイント is5ni-saml.con	n	Redirect	いいえ	
٢					>
SAML の追加(<u>D</u>)				
WS-Federation	の追加(<u>W</u>)…		削除(<u>R</u>)	編集(<u>E</u>)
	ОК		キャンセル	適用	(<u>A</u>)

仮名を利用する場合



1.以下の2つの変換要求規則を追加します。

要求規則テンプレートに「カスタム規則を使用して要求を送信」を選択して、「次へ」をクリックします。



以下のカスタムルールをコピー&ペーストし、完了をクリックします。

```
c:[type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname" ]
=> add(
store = "_OpaqueIdStore",
types = ("http://mycompany/internal/persistentId"),
query = "{0};{1};{2}",
param = "ppid",
param = c.Value,
```

param = c.OriginalIssuer);

翰 変換要求規則の追加ウィザー	ř ×
規則の構成	
 ステップ ● 規則の種類の選択 ● 要求規則の構成 	カスタムの要求規則(複数の入力方向の要求を必要とする規則、SQL 居住ストアから要求を抽出する規則な ど)を構成できます。カスタム規則を構成するには、AD FS 要求規則言語を使用して、1つ以上のオプションの 条件を発行ステートメントを入力します。 要求規則名(Q): 永徳的仮名の発行 規則テンプレート カスタム規則を使用して要求を送信 カスタム規則(U): c[type == "http://schemas.microsoft.com/ws/2008/08/identity/claims/windowsaccountname"] store = "OpaqueIdStore", types = ("http://mycompany/internal/persistentId"), query = "pid", param = colliginalIssuer);
	<前へ(P) 完了 キャンセル

「入力方向の要求を変換」を選択し、「次へ」をクリックします。

🧌 変換要求規則の追加ウィザ-	Ч	×
規則テンプレートの選択		
 ステップ 規則の種類の選択 要求規則の構成 	作成する要求規則のテンプレートを次の一覧から選択してください。各要求規則テンプレートの詳細は説明に 載されています。 要求規則テンプレート(①) 入力方向の要求を変換 マ 要求規則テンプレートの説明 入力方向の要求を変換見則テンプレートを使用すると、入力方向の要求を選択して要求の種類を変更 することや、必要に応じて要求値を変更する。こかできます。たとだは、この規則デンプレートを使用して、入力 方向のグループ要求し何に要求値を変更することができます。たとだは、この規則デンプレートを使用して、入力 方向のグループ要求したのできます。たとだは、この規則で以、一体使用して、 値が、管理書である。入力方向のの要求を表見いき言できます。入力方向の要求の取得て は、編集する規則によって異なります。	
	< 前へ(P) 次へ(N) > キャンセル	

以下の値を選択し、「完了」をクリックします。

- ・要求規則名:任意の名称を入力します。
- ・入力方向の要求の種類:「http://mycompany/internal/persistentId」をコピー&ペーストで入力します。
- ・出力方向の要求の種類:「名前 ID」を選択します。
- ・出力方向の名前 ID の形式:「永続 ID」を選択します。

翰 変換要求規則の追加ウ	rザ−ド	×				
規則の構成						
ステ ップ ● 規則の種業類の選択 ● 要求規則の構成	この規則を構成することにより、入う す。オブションとして、入力方向の要求の種類に関連付ける入力方向の す。 更な規則名(C):	っ方向の要求の種類を出力方向の要求の種類に関連付けることができま まれの値を出力方向の要求の値に関連付けることもできます。出力方向の要 の要求の種類と、要求値を新しい要求値に関連付けるかどうかを指定しま				
	NameIDとして返却する	要求のRPP-GUDF NameIDとして返却する				
	規則テンプレート:入力方向の要求	· 交交換				
	入力方向の要求の種類(1):	http://mycompany/internal/persistentId				
	人力方向の名前 ID の形式(M):					
	出力方向の要求の種類(0):	名前 ID V				
	出力方向の名前 ID の形式(E):	永続 IDI V				
	 すべての要求値をパス スルーす 入力方向の要求の値を異なる 入力方向の要求の値(い): 出力方向の要求の値(い): 入力方向の要求の値(い): 入力方向の電子メールサフィッ 新しい電子メール サフィックス(い) 	る(S) 出力方向の要求の値に置き換える(B) ゆス要求を新しい電子メール サフィックスに置き換える(2) 例 fabrik.am.com				
		< 前へ(P) 完了 キャンセル				

2.「OK」をクリックします。

NI-SP の要求発行ポリシーの編集	×
発行変換規則	
次の変換規則は、証明書利用者へ送信す	る要求を指定します。
順序 規則名	発行済み要求
1 永続的仮名の発行 1 Name Tokel スキョキオス	〈要求規則の表示〉
2 NameroCOC/2019-20	
<	>
規則の追加(A) 規則の編集(E)	規則の肖耶徐(R)
	いた キャンセル 週用(円)



・NameID として、AD のユーザー情報を返すように設定を行います。

1.AD FS の管理ツールを表示し、「証明書利用者信頼」メニューを選択します。

追加した証明書利用者信頼をクリックし、画面右側の「要求発行ポリシーの編集」を選択します。



2.「規則の追加」ボタンをクリックします。



3.以下の要求規則を追加します。

要求規則テンプレートに「LDAP 属性を要求して送信」を選択し、「次へ」をクリックします。



以下の値を選択し、「完了」をクリックします。

- ・要求規則名:任意の名称を入力します。
- ・属性ストア:「Active Directory」を選択します。
- ・LDAP 属性:「SAM-Account-Name」

※ここでは検証のため、ADの「ユーザーログオン名(Windows 2000 より前)」に紐づく

「SAM-Account-Name」を選択しています。

LDAP 属性については、補足を参照してください。

・出力方向の要求の種類:「名前 ID」を選択します。

🧌 変換要求規則の追加ウ	ィザード		×
規則の構成			
ステップ ● 相則の種類の遅択	この規則 性ストリ	lを構成することにより、LDAP 属性の値を要求と を選択します。次に、規則から発行する出力方向	して送信できます。まず、LDAP 属性の抽出元となる属 向の要求の種類に属性を関連付ける方法を指定しま
 要求規則の構成 	す。 要求規	則名(<u>C</u>):	
	Name	 D	
	規則テ	バンレート:LDAP 周性を要求として送信	
	庸性ス Activ	∼P(S): Directory	~
	LDAP	、 属性の出力方向の要求の種類への関連付け(M);
		LDAP 属性(さらに追加する場合は 選択または入力してください)	カ方向の要求の種類(さらに追加する場合は選択 たは入力してください)
	•	SAM-Account-Name ~ 名前	前 IDJ V
		× .	~
			<前へ(<u>P)</u> 完了 キャンセル

🧌 変換要求規則の追加ウ	ウイザード			
規則の構成				
ステ ップ の 規則の種類の選択	この規則を構成することにより、LDAP 属性の値を要求として送信できます。まず、LDAP 属性の抽出元とな 性ストアを選択します。次に、規則から発行する出力方向の要求の種類に属性を関連付ける方法を指定し			
 ● 要求規則の構成 	す。 要求規則(名(C)):			
	NameID			
	ー 規則テンプレート: LDAP 属性を要求として送信			
	属性ストア(S):			
	Active Directory \checkmark			
	LDAP 属性の出力方向の要求の種類への関連付け(M):			
	LDAP 腐性(だらに追加する場合は 出力方向の要求の種類(たらに追加する場合は選邦			
	選択または人力しくくたさい) または人力しくくたさい) SAM-Account Name 名前 ID			
	Company			
	Department Display-Name			
	E-Mail-Addresses Employee-ID			
	Employee-Number			
	Given-Name			
	Is-Member-Ot-DL Organizational-Unit-Name			
	Organization-Name Proxy-Addresses			
	SAM-Account-Name State-Or-Province-Name			
	Street-Address			
	Telephone-Number			
	Itte Token-Groups (SID) く前へ(P) 完了 キャンセ			
	Token-Groups - ドメイン名を含む			
	Token-Groups - ドメイン名を含む Token-Groups - 完全修飾ドメイン名を含 Token-Groups - 名前の指定なし User-Principal-Name			
	Token-Groups - ドメイン名を含む Token-Groups - 完全修飾ドメイン名を含 Token-Groups - 名前の指定なし User-Principal-Name			
創めに使用される	Token-Groups - ドメイン名を含む Token-Groups - 完全(第所ドメイン名を含) Token-Groups - 名前の指定なし User-Principal-Name			
−般的に使用される	Token-Groups - FX1 2名を含む Token-Groups - 名前の指定なし User-Principal-Name			
-般的に使用される ・LDAP 属性「SAM-	Token-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name			
-般的に使用される ・LDAP 属性「SAM・ AD の「ユーザー[Token-Groups - FXY 2名を含む Token-Groups - 名前の指定なし User-Principal-Name			
-般的に使用される ・ LDAP 属性「SAM・ AD の「ユーザー[_{専川係のプロパティ}	Token-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Pincipal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? ×			
-般的に使用される LDAP 属性「SAM- AD の「ユーザー[^{専川 祭のプロパティ}	Token-Groups - PX/28を365 Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。			
-般的に使用される ・LDAP 属性「SAM・ AD の「ユーザー[Token-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × スワードレブリケーション ダイヤルイン オブジェクト 環境 セッション リモート制御			
 一般的に使用される ・ LDAP 属性「SAM・ AD の「ユーザー」 ・ クリーン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Token-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × (スワ-ドレブリケ-ション ダイヤルイン オブジェクト 環境 セッション リモート制御 DTロファイル COM+ 属性エディタ- フリガナ			
 一般的に使用される ・ LDAP 属性「SAM・ AD の「ユーザー[寺川 傑のブロパティ 所属するグルーブ パ セキュリティ リモート デスクトップ サービスの 全般 住所 アカウ 	Token-Groups - PX1 28を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × (スワ-ドレブリケ-ション ダイヤルイン オブジェクト 環境 セッション リモート制御 27027イル COM+ 属性エディタ- フリガナ ント プロファイル 電話 組織 公開された証明書			
-般的に使用される ・ LDAP 属性「SAM- AD の「ユーザー[Indeen-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × マ × マ × 環境 セッション リモー制御 ワブロファイル COM+ 属性エディター フリガナ フロファイル 電話 組織			
-般的に使用される ・ LDAP 属性「SAM- AD の「ユーザー[寺川 傑のプロパティ 所属するグループ パ セキュリティ リモート デスクトップ サービスの 全般 住所 アカウ ユーザーログオン名(U): terakawa	Token-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × (スワードレブリケーション ダイヤルイン オブジェクト 環境 セッション リモート制御 のプロファイル COM+ 属性エディター フリガナ ント プロファイル 電話 組織 公開された証明音 @ xxxxx.com			
-般的に使用される LDAP 属性「SAM- AD の「ユーザー[専川 傑のプロパティ 時属するグループ パ セキュリティ リモートデスクトップサービ20 全般 住所 7カウ ユーザーログオン名(U): terakawa ユーザーログオン名(Window	Indeen-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × (スワードレブリケーション ダイヤルイン オブジェクト 環境 セッション リモート制御 のプロファイル COM+ 属性エディター フリガナ ント プロファイル 電話 組織 公開された証明書 (@ xxxxx.com (@ xxxxx.com			
-般的に使用される LDAP 属性「SAM- AD の「ユーザー[専川 傑のブロバティ 所属するグルーブ パ レキュリティ リモート デスクトッブ サービ20 全般 住所 アカウ ユーザー ログオン名(U): terakawa ユーザー ログオン名 (Window NI-SAML¥	Indeen-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × パフ-ドレブリケ-ション ダイヤルイン オブジェクト 環境 セッション リモート制御 のプロファイル COM+ 属性エディター フリガナ ント プロファイル 電話 組織 公開された証明書 @ xxxxx.com ws 2000 より前)(W: terakawa			
-般的に使用される ・LDAP 属性「SAM・ AD の「ユーザー[専川 係のブロバティ 所属するグループ パ 「 「 レキュリティ リモートデスクトップサービスの 全般 住所 アカウ ユーザーログオン名(U): terakawa ユーザーログオン名(Window NI-SAML¥	Indeen-Groups - ドメイン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 -Account-Name」 アメ マメ (スワードレブリケーション ダイヤルイン オブジェクト 環境 セッション ダイヤルイン オブジェクト マメ (スワードレブリケーション ダイヤルイン オブジェクト マメ (スワードレブリケーション ダイヤルイン オブジェクト マリカー (の xxxxx.com) ws 2000 より前)(W): (の xxxx.com) レナ プロファイル (の xxxx.com) ログオン生の			
 一般的に使用される ・LDAP属性「SAM- ADの「ユーザー[Token-Groups - PX1 28を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 ログオン名(Windows 2000 より前)」を使用します。 ? × パフ-ドレブリケ-ション ダイヤルイン オブジェクト 環境 セッション リモー制御 071027イル COM - 属性エディター フグロファイル マロッション リモー制御 0 xxxxx.com (2000 より前)(W): terakawa ログオン先口			
 一般的に使用される ・ LDAP 属性「SAM・ ADの「ユーザー」 ◆川像のブロパティ ・ 「「「「「「「「」」」」」 ・ 「」」」、「」」 ・ 「」」、「」」、「」、「」、「」、「」、「」、「」、「」、」、」、」、」、」、	Token-Groups - PX/28を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 マ × (スワ-ドレブリケ-ション ダイヤルイン オブジェクト 環境 セッション リモート制御 プロファイル COM+ 属性エディタ- フリガナ プロファイル マの4 ログオン先口…			
-般的に使用される ・LDAP 属性「SAM- AD の「ユーザー」 参川 傑のプロパティ 所属するグループ パ セキュリティ リモート デスクトップ サービスの 全般 住所 アカウ ユーザー ログオン名(U): terakawa ユーザー ログオン名(Window NI-SAML¥ ログオン時間(L)	Token-Groups - PX1 28を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × 1000000000000000000000000000000000000			
-般的に使用される LDAP 属性「SAM- AD の「ユーザー[寺川 係のプロパティ 所属するグループ パ セキュリティ リモートデスクトップ サービスの 全般 住所 アカウ ユーザーログオン名(U): terakawa ユーザーログオン名(Window NI-SAML¥ ログオン時間(L) ビアカウントのロックを解除: アカウントオブション(O):	Token-Groups - PX1 28を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × (27-ドレブリケ-ション (27-ドレブリケ-ション (27-ドレブリケ-ション (27-ドレブリケ-ション (27-ドレブリケ-ション (27-ドレブリケ-ション (27-ドレブリケ-ション (27-ドレブリケーション (27-ドレブリケーション (27-ドレブリケーション (27-ドレブリケーション (27-ドレブリケーション			
-般的に使用される ADの「ユーザー[参川像のブロパティ 所属するグループ パ 「サートデスクトップサービスの 全般 住所 アカウ ユーザーログオン名(U): terakawa ユーザーログオン名(U): terakawa ユーザーログオン名(Window NI-SAML¥ ログオン時間(L) ビアカウントのロックを解除す アカウントオブション(Q): コーザーは次回ログオン	Indeen-Groups - たメリン名を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 コグオン名(Windows 2000 より前)」を使用します。 ? × (X7-ドレブリケ-ション 9 × × (X7-ドレブリケ-ション 9 × × 1000000000000000000000000000000000000			
-般的に使用される LDAP 属性「SAM- AD の「ユーザー[専川 係のブロパティ 所属するグループ パ ゼキュリティ リモートデスクトップサービ20 全般 住所 アカウ ユーザーログオン名(U): terakawa ユーザーログオン名(U): terakawa ユーザーログオン名(U): terakawa ユーザーログオン名(Window NI-SAML¥ ログオン時間(L)	Indeen-Groups - PX1 28を含む Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? × パフードレブリケーション ダイヤルイン オブジェクト 環境 セッション リモート制御 Dプロファイル COM+ 属性エディター フリガナ ント プロファイル 電話 組織 公開された証明書 @ xxxxx.com ws 2000 より前)W: ① グカン先口 オブシア・「変更が必要 変更できない			
-般的に使用される LDAP 属性「SAM- AD の「ユーザー[専川 除のブロバティ 所属するグループ パ(リモートデスクトップサービスの 全般 住所 アカウ ユーザーログオン名(U): terakawa ユーザーログオン名(U): terakawa ユーザーログオン名(Window NI-SAML¥ ログオン時間(L) ジアカウントのロックを解除: アカウントオブション(O): コーザーはパスワードを 二パスワードを無期限に:	Ideen-Groups - 完全(変) Token-Groups - 完全(変) Token-Groups - 完全(変) Token-Groups - 完全(変) Token-Groups - 完全(windows 2000 より前)] -Account-Name] コグオン名(Windows 2000 より前)] ク(ガオン名(Windows 2000 より前)] を使用します。 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??? ?? ?? ?? ?? ??<			
-般的に使用される ADの「ユーザー[専川 傑のブロパティ 所属するグルーブ」パ 「たちュリティ リモートデスクトップサービスの 全般 住所 アカウ ユーザーログオン名(U): terakawa ユーザーログオン名(U): terakawa ユーザーログオン名(U): (ログオン時間(L) 「アカウントのロックを解除: アカウントオブション(O): コーザーは次回ログオ: コーザーは次同ログオ: コーザーは次同に大きます。	Ideen-Groups - 完全修飾ドメノン名を含 Token-Groups - 完全修飾ドメレン名を含 Token-Groups - 名前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 ログオン名(Windows 2000 より前)」を使用します。 マ × マ × マ × マ × マ × マログオン名(Windows 2000 より前)」を使用します。 マ × マ × マログオン名(Windows 2000 より前)」を使用します。 マ ×			
-般的に使用される LDAP 属性「SAM- AD の「ユーザー[専川 傑のブロパティ 所属するグルーブ パ セキュリティ リモート デスクトップ サービスの 全般 住所 アカウ ユーザーログオン名(U): terakawa ユーザーログオン名(U): terakawa ユーザーログオン名(U): でわウントのロックを解除: アカウントの可少のを解除: フガウントの可少のを解除: フガウントの可少のを解除: アカウントの可必のにに戻せるは アカウントの別限	Iden-Groups - 完全資産所ドメレン名を含 Token-Groups - 完全前の指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? パンキン名(Windows 2000 より前)」を使用します。 ? ? マンドレブリケ-ション ダイヤルイン オブジント 環境 セッション リモート制御 D7D7アイル COM+ 属性エディター フリガナ ント プロファイル COM+ 属性エディター フリガナ ? ? ************************************			
 一般的に使用される LDAP属性「SAM- ADの「ユーザー[Iden-Groups - 完全修飾ドメレン名を含 Token-Groups - 完全修飾ドメレン名を含 Token-Groups - 完全的が指定なし User-Principal-Name 「LDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 コグオン名(Windows 2000 より前)」を使用します。 ? パードレブリケ-ション ダイヤルイン オブジェクト 環境 セッション リモート制御 D7D7p+/ル COM+ 属性エディター フリガナ ント プロファイル COM+ 属性エディター フリガナ ント プロファイル 電話 組織 公園された証明書 @ xxxxx.com ws 2000 より前)(W): セロオン先口 な園された証明書 アウドレ/スワード変更が必要 変更できない する 比較でパスワードを保存する			
 一般的に使用される LDAP属性「SAM- ADの「ユーザーE ◆川像のブロパティ ・ 「「「「「「「「」」」」」」」」 ・ 「」」」」」」」 ・ 「」」」」」」」 ・ 「」」」」」」」」 ・ 「」」」」」」」」 ・ 「」」」」」」」」 ・ 「」」」」」」」」」 ・ 「」」」」」」」」」」」」」」」」 ・ 「」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」	Iden-Groups - 完全修飾が入りるを含む Token-Groups - 完全修飾が入りるを含む Token-Groups - 完全修飾が入りるを含む TLDAP 属性」の選択肢と AD の情報との紐づけは以下のようにな -Account-Name」 ログオン名(Windows 2000 より前)」を使用します。 ? × パロードレブリケーション ダイヤルイン オブジェクト ************************************			

Ŋ

寺川 傑のプロパティ	?	×
所属するグループ	パスワードレブリケーション ダイヤルイン オブジェク	/ ト
セキュリティ リモート デスクトッ	環境 セッション リモート制御 ブ <u>サービスのプロフ</u> ァイル COM+ 属性エディター フリナ	í ,
全般 住所	アカウント プロファイル 電話 組織 公開された証	明書
ユーザー ログオン名 terakawa	4(<u>U</u>):	. 1
ユーザー ログオン名	(Windows 2000 より前)(W):	
NI-SAML¥	terakawa]
ログオン時間(し	.) ログオン先(<u>I</u>)	
	ックを解除する(N)	
アカウント オプショ	ン(<u>O</u>):	
□ ユーザーは2	欠回ログオン時にパスワード変更が必要 ^	
□ ユーザーは/ □ パスワードを	(スワードを変更できない (無期限にする	
□ 暗号化をテ	こに戻せる状態でパスワードを保存する 🗸 🗸 🗸 🗸	
アカウントの期限	₹	
 ● なし(V) ○ 右动期限(E): 2023年 7月15日 🔍 🗸	
Г	OK キャンセル 適用(A) ヘルフ	f
LDAP 属性「	E-Mail-Addresses」 メール」を使用します。	
LDAP 属性「 AD の「電子 ^{専川 傑のプロパティ}	E-Mail-Addresses」 メール」を使用します。 ?	×
LDAP 属性「 AD の「電子 ^{専川 係のプロパティ}	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン オブジェク	×
 DAP 属性「 Dの「電子 寺川 係のプロパティ 所属するグループ セキュリティ リエート ジョクループ 	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン オブジェク 環境 セッション リモート制御	×
LDAP 属性「 AD の「電子 ^{専川 傑のブロパティ}	E-Mail-Addresses」 メール」を使用します。	× ト ナ 月書
LDAP 属性「 AD の「電子 寺川 係のプロパティ 所属するグループ セキュリティ リエートデスクトップ 全般 住所 美 ・	E-Mail-Addresses」 メール」を使用します。 ? /(スワードレブリケーション ダイヤルイン オブジェク 環境 セッション リモート制御 プサービスのブロファイル COM+ 属性エディター フリカ アカウント プロファイル 電話 組織 公開された証明	× ト け 語
DAP 属性「 Dの「電子 ^{専川 傑のプロパティ} 所属するグループ セキュリティ リ <u>モート</u> テスクトップ 全般 住所 ・ 専川	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン オブジェク 環境 セッション リモート制御 プサービスのブロファイル COM+ 属性エディター フリカ アカウント プロファイル 電話 組織 公開された証明	× ト け 用書
DAP 属性「 AD の「電子 寺川 傑のブロパティ 所属するグループ セキュリティ リモートデスクトッフ 全般 住所 楽 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	E-Mail-Addresses」 メール」を使用します。	× ト ナ 唐
DAP 属性「 D の「電子 寺川 傑のブロパティ 所属するグループ セキュリティ リモート・デスクトッフ 全般 住所 美 会(L): 名(E):	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン 環境 セッション プサービスのブロファイル COM+ アカウント プロファイル 電話 組織 公開された証明 11 例 キリII 使 イニシャル(D):	× ト け
DAP 属性「 D の「電子 寺川 傑のプロパティ 所属するグループ セキュリティ リモートテスクトップ 全般 住所 美田 会し: 表示名(S):	E-Mail-Addresses」 メール」を使用します。	× ト け 間書
DAP 属性「 D の「電子 専川 傑のブロパティ 所属するグループ セキュリティ リモート デスクトップ 全般 住所 美 、 な(L): 表示名(S): 説明(D):	E-Mail-Addresses」 メール」を使用します。	× ト け 月書
DAP 属性「 AD の「電子 寺川 傑のブロパティ 所属するグループ セキュリティ リモートテスクトッン 全般 住所 楽 ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン 環境 セッション サービスのプロファイル COM+ アカウント プロファイル 電話 組織 公開された証明 II 傑 専川 (年) オニシャル(D):	× ト け 門 目
DAP 属性「 AD の「電子	E-Mail-Addresses」 メール」を使用します。	× ト ナ 月書
DAP 属性「 D の「電子 寺川 係のブロパティ 所属するグループ セキュリティ リエートテスクトップ 全般 住所 美 、 な(L): 名(E): 表示名(S): 説明(D): 事業所(C): 電話番号(D):	E-Mail-Addresses」 メール」を使用します。	× ト ナ 月 日 1
DAP 属性「 AD の「電子 寺川 傑のブロパティ 所属するグループ セキュリティ リモートデスクトップ 全般 住所 ・ 楽・ ・ なくし: 表示名(S): 説明(D): 事業所(C): 電話番号(D): 電子メール(M):	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン 環境 セッション ブサ・ビスのプロファイル COM+ アカウント プロファイル マカウント プロファイル マカウント プロファイル 電話 組織 公開された証明 II 傑 ・ ・	× ト け 月書
LDAP 属性「 AD の「電子 ^{専川 (保のブロパティ)} ^{FK}	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン 環境 セッション サービスのブロファイル COM+ 宮地 公開された証明 11 傑 (1=2)ヤル(1): 専川 (1=2)ヤル(1): 専川 傑 (1=2)ヤル(1): 「古の他(2) その他(2) との他(5) その他(5)	× ト ナ 月書
LDAP 属性「 AD の「電子 ^{専川 (保のブロパティ)} ^ド ^R ^R ^R ^R ^R ^R ^R ^R	E-Mail-Addresses」 メール」を使用します。	× ト け 月 月 日
LDAP 属性「 AD の「電子 ^{専川 傑のブロパティ} ^{所属するグループ ^{セキュリティ} ^{リモート デスクトップ ^{全般} 住所 ^{シート} ^{キート} ⁽¹⁾ }}	E-Mail-Addresses」 メール」を使用します。 ? パスワードレブリケーション ダイヤルイン 環境 セッション サービスのブロファイル COM+ ス開された証明 オーシン フリカ アカウント プロファイル マロション リモート制御 ケービスのブロファイル COM+ ス開された証明 日御 今川 電話 毎川 イニシャル(D: ● 寺川 傑 「日の他(Q) その他(Q)	× ト ナ 月 月 日
LDAP 属性「 AD の「電子 ^{専川 傑のブロパティ} ^{所属するグルーブ} ^{セキュリティ} ^{リモートデスクトップ ^{全般} (住所 ^{全般} ^{キー}}	・ ・ その他(B) ・ ・ ・	
LDAP 属性「 AD の「電子 寺川 傑のブロパティ 下属するグルーブ セキュリティ リモートデスクトッフ 全般 住所 シート デスクトッフ 全般 (住所 シート マストッフ (住所 シート マストッフ (中) ・ マストッフ ・ マストッコ ・ マストッフ ・ マストッフ ・ マストッフ ・ マストッフ ・ マストッフ ・ マストッフ ・ マストッフ ・ マストッフ ・ マストッフ ・ マストッフ ・ マー ・ ・ ・ ・ ・ 、 ・ い ・ ・ 、 ・ 、 ・ 、 ・ 、 ・ 、 ・ ・ 、 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	E-Mail-Addresses」 メール」を使用します。	× ト ナ 月 書

1.AD FS の管理ツールを表示し、「認証方法」メニューを選択します。

プライマリ認証方法の編集をクリックします。

S AD FS		- 🗆 X
😪 ファイル(E) 操作(A) 表示(V) ウィンドウ(W)	0 NU/E	- 8 >
💠 🔿 🙍 🖬 📓 🖬		
🛅 AD FS	響至方法	操作
✓ ■ サービス	認証方法の概要	17日1日日本
認証方法	ゴルノフリが正大とした。な事業の行大士を描述できます	プライマリ認証方法の環策
は明智	Etanta B	多要素認証方法の編集
■ 要求能还 ■ Device Registration	AD FS ヘルプ	表示 ▶
エンドポイント	プライマリ辺証方法	ここから新しいウィンドウ
□ スコーフ記述 Web アブリケーション プロキシ	ジンプイマンBIG BELフリアム 認証に AD FS を使用するアプリケーションにアクセスするすべてのユーザーには、プライマリ認証が必要です。次のオプションを使用して、プライマリ認証方	 最新の接報に更新
アクセス制御ボリシー	法の設定を構成できます。	
証明書利用者信頼 第二方式ノダーの柄	エンストンキット フォームの起こ Microsoft Passport 認証	
デブリケーション グループ	イントラネット フォーム閲覧、 Windows 開発	
	Microsoft Passport IEIE	
	追加の認証方法	
	次のオプションを使用して、追加の認証方法の設定を構成できます。	
	認証方法 未構成 機業	

2.利用する認証方法を有効にし、「OK」をクリックします。

・パスワード認証の場合

エクストラネット:「フォーム認証」にチェックします。

イントラネット :「フォーム認証」にチェックします。

・Windows 認証の場合

エクストラネット:「フォーム認証」にチェックします。

イントラネット :「フォーム認証」と「Windows 認証」にチェックします。

認証方法の編集 ×
プライマリ 追加
認証方法を選択してください。複数の認証方法を選択すると、ユーザーはサインイン時に複数の選 択肢から認証方法を選択できるようになります。
統合 Windows IZ証方法を指定した場合、統合 Windows IZ証をサポートするブラウザーでは既 定のIZI証方法として表示されます。
<u>Azure Mult</u> i-Factor Authentication (MFA)の詳細情報。
エクストラネット
マフォーム221日 目辺り発き22日 デデバイス22日 Microsoft Passport 記録
-1ントラネット
□ ゴニノフリレーズ追加の範囲ゴロバノガーキャンデオス(か)
Azure Active Directory テナントが構成されるまで Azure MFA 認証方法は利用でき ません。詳細情報
● プライマリ認証方法としてデバイス認証を使用するには、Device Registration を構成する 必要があります。
OK キャンセル 通用(P)

2-6.IdPの設定(Windows Server 2019)

Windows Server 2016 同様の手順となります。

「2-5.IdPの設定(Windows Server 2016-ADFS)」を参照してください。

2-7.仮名 ID 取得



・仮名を利用する場合のみ、各ユーザーが下記の作業を行う必要があります。

2-7-1.オプション設定

1.仮名を利用する場合、初回ログイン時はシングルサインオンに失敗するため、

通常の NI 製品ログイン画面より、ID/パスワードを入力し、ログインしてください。

2.NI 製品の「オプション設定」画面を表示し、「SAML 認証」を選択します。

⇒ 「SAML 認証」 画面が表示されます。

3. 取得する ボタンをクリックして、Identity Provider から仮名 ID を取得します。

※新規ウィンドウが開き、Identity Provider へ接続します。仮名 ID 取得後に Window は自動的に閉じられ ます。_____

4.最後に 保存 ボタンを押します。

2-8.動作確認

1.NI 製品の任意の URL にブラウザでアクセスします。

2.IdP にログインします。

パスワード認証の場合、AD FS のログイン画面にて、ID/パスワードを入力することで認証されます。

NI Consulting
組織アカウントを使用してサインインしてください
someone@example.com
サインイン
© 2013 Microsoft

3. Windows 認証の場合、ドメインにログイン済みの Windows PC にて、

Microsoft Edge、または Google Chrome を使用しているときは、自動で認証されます。

それ以外の場合、認証ダイアログが表示され、ID/パスワードを入力することで認証されます。

4.NI 製品の目的の URL が表示されます。



・Windows Hello など多要素認証によるログインの場合も同様の動作となります。

2-9.トラブルシューティング ・AD FS で発生するエラーについて記載します。 ・NI 製品のアクセスログに出力されているエラーログへの対処については、「4.トラブルシューティング」を参照してください。

2-9-1.AD FS のエラー画面

以下のような画面が表示された場合、AD FS 側でエラーが発生しています。



通常のログイン画面の URL に「?saml=no」を追加し、NI 製品へログインしてください。

例)NI Collabo 360 https://xxx.xxx.xxx/ni/niware/portal/index.php?saml=no 例)Sales Force Assistant シリーズ https://xxx.xxx.xxx/ni/<各製品>/main/index.php?saml=no

2-9-2.AD FS のエラー詳細確認

エラーの内容を確認するには、IdP のサーバーマネージャーのメニューより「AD FS」を選択し、「イベント」項 目をチェックします。



AD FS の設定不備が原因で発生する主要なエラーを以下に記載します。

エラーID	エラーメッセージ	対応方法
364	パッシブな要求のフェデレーション中にエラーが発生しました。	認証中にエラーが発生すると、必ず
		ログに出力されるメッセージです。
	追加データ	※パッシブな要求 = Web ブラウザ
		からの要求
364	パッシブな要求のフェデレーション中にエラーが発生しました。	SP のエンティティ ID が誤っていま
	追加データ	す。
	プロトコル名:	(※上記原因の場合、エラーID:
	Saml	364 以外のエラーメッセージは出力
	証明書利用者:	されません。)
	https://xxx.xxx.xxx/ni/	証明書利用者信頼のプロパティの
	例外情報:	「識別子」タブから証明書利用者の
	Microsoft.IdentityServer.Web.InvalidScopeException:	識別子が正しいことを確認してくだ
	MSIS7007: 要求された証明書利用者信頼	さい。
	'https://xxx.xxx.xxx.xxx/ni/' は指定されていないか、またはサ	
	ポートされていません。証明書利用者信頼が指定されていた場合	
	は、証明書利用者信頼にアクセスするための許可がない可能性が	
	あります。詳細については、管理者に問い合わせてください。	
	場所 Microsoft.IdentityServer.Web.Protocols.	
	Saml.SamlSignInContext.Validate()	
	場所 Microsoft.IdentityServer.Web.Protocols…	
261	要求で、証明書利用者 'https://xxx.xxx.xxx.xxx/ni/' に構成され	SP のエンドポイント URL が誤って
	ていないアサーション コンシューマー サービス の URL	います。
	'https://xxx.xxx.xxx.xxx/ni/zcom/service/index.php?p=saml'	証明書利用者信頼のプロパティの
	が指定されました。	「エンドポイント」タブから
	アサーション コンシューマー サービスの URL:	「SAML アサーションコンシューマ
	https://xxx.xxx.xxx.xxx/ni/zcom/service/index.php?p=saml	ーエンドポイント」の URL が正し
	証明書利用者: https://xxx.xxx.xxx/ni/	いことを確認してください。
	この要求は失敗しました。	
	ユーザー操作	
	AD FS の管理スナップインを使用して、この証明書利用者用に指	
	定された URL を持つアサーション コンシューマー サービスを	
	構成してください。	

エラーID	エラーメッセージ	対応方法
321	SAML 認証要求に、満たすことができない NameID のポリシー	仮名 ID の利用有無に対し、IdP 側
	がありました。	の設定が正しく実施できていませ
	要求元: https://xxx.xxx.xxx/ni/	ሌ.
	名前識別子の形式: urn:oasis:names:tc:SAML:2.0:nameid-	「2-4-3変換要求規則の追加」項の
	format:persistent	手順が正しく実行できているか、確
	SPNameQualifier:	認してください。
	例外の詳細:	
	MSIS7070: SAML 要求に、発行されたトークンでは要件が満た	
	されない NameIDPolicy が含まれていました。要求された	
	NameIDPolicy: AllowCreate: True Format:	
	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	
	SPNameQualifier: 。実際の NameID プロパティ: Format: ,	
	NameQualifier: SPNameQualifier: , SPProvidedId: $_{\circ}$	
	この要求は失敗しました。	
	ユーザー操作	
	AD FS の管理スナップインを使用して、 必要な名前識別子を発	
	行する構成を設定してください。	
273	要求で、証明書利用者 'https://xxx.xxx.xxx.xxx/ni/' に対して構	IdP のエンドポイント URL 設定に、
	成またはサポートされていない アサーション コンシューマー サ	誤ったバインディングが指定されて
	ービスが指定されました。	います。
	要求パラメーター: ''、	「 <u>2-4-2 エンドポイント URL の追</u>
	'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'、	<mark>加</mark> 」項の手順が正しく実行できてい
	'https://xxx.xxx.xxx.xxx/ni/zcom/service/index.php?p=saml'	るか、確認してください。
	証明書利用者: https://xxx.xxx.xxx/ni/	
	この要求は失敗しました。	
	ユーザー操作	
	AD FS の管理スナップインを使用して、この証明書利用者用に指	
	定された パラメーターを持つアサーション コンシューマー サー	
	ビスを構成してください。 SAML アーティファクトが要求された	
	場合は、アーティファクト解決サービスが有効になっているかど	
	うかも確認してください。	

2-10.運用時の注意

2-10-1.証明書の更新について

\$ 1			AD FS				x
Ŷ I ファイル(E) 操作(A)	表示(⊻) ウィンドウ(₩) ヘルプ(且)						- 8 ×
🗢 🔿 🖄 📰 🛽 🖬							
ad FS	証明書					操作	
⊿ 🔛 サービス	サブジェクト 発行者	有効問始日	右轨其服	状能	プライマリ		-
□ 証明書 □ 要求記述	サービス通信 E=xxxxxxx@ni-consulcoj E=xxxxxxx@ni-consulco トーケン暗号化解除	2020/03/26	2021/03/26			トークン署名証明書の追加 トークン暗号化解除証明書の追加	
▶ 🔜 1言親関係 ▶ 🔛 認証ポリシー	図CN=ADFS Encryption - ni CN=ADFS Encryption - トークン業名	2020/03/26	2021/03/26		プライマリ	サービス通信証明書の設定 表示	
	CN=ADFS Signing - ni-sa… CN=ADFS Signing - ni	. 2020/03/26	2021/03/26		プライマリ	ここから新しいウィンドウ 最新の情報に更新	_

AD FS は、以下の3種類の証明書を利用して動作しています。

1.サービス通信証明書

「2-2-2 AD FS の構成」にて適用した、SSL(https)通信のための証明書です。

適用した証明書の期限に応じて、手動で更新を行ってください。

2.トークン暗号化解除証明書

利用していません。

3.トークン署名証明書

AD FS のセットアップ時に自動で作成される自己署名証明書です。

有効期限は既定では1年となっており、自動で更新されます。

また、AD FS では、自動証明書ロールオーバー機能(トークン署名証明書の自動更新)があり、既定ではこの機能が有効となっています。自動証明書ロールオーバーが発生した場合、証明書の有効期限 5 日前に NI 製品へのシングルサインオンでエラーが発生します。

対策として、AD FS の自動証明書ロールオーバー機能を無効にする、証明書の有効期限延長があります。 詳細は、Microsoft 社の情報をご確認ください。

https://docs.microsoft.com/ja-jp/archive/blogs/jpntsblog/ad-

fs-%E3%81%AE%E8%87%AA%E5%8B%95%E8%A8%BC%E6%98%8E%E6%9B%B8%E3%83%A D%E3%83%BC%E3%83%AB%E3%82%AA%E3%83%BC%E3%83%90%E3%83%BC%E6%A9%9 F%E8%83%BD%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6

有効期限切れ、有効期限延長により証明書が更新されると、「<u>2-3-1 システム設定</u>」項の「3. IdP メタデータ をアップロードします。」を再実行する必要があります。

3.セットアップ手順(IdP: Microsoft Entra IDの場合)

3-1.システム構成

以下の構成でセットアップを行います。

・認証サーバー

IdP	Microsoft Entra ID
101	

※Microsoft Entra ID の全てのエディションにて SAML 認証機能が利用可能です。

ただし、Microsoft 社がエディション毎の提供機能範囲を変更する可能性があります。

詳細は Microsoft 社の情報をご確認ください。

https://learn.microsoft.com/ja-jp/entra/fundamentals/whatis

3-2.IdP の設定

3-2-1. SP メタデータの準備

1.NI 製品システム設定の セキュリティ より「SAML 認証」を選択します。

⇒「認証/SAML 認証」画面が表示されます。

2.SP メタデータをダウンロードします。

Service Provider(NI 製品)設定の「メタデータ」の ダウンロード ボタンをクリックします。

メタデータ: Service Providerメタデータをダウンロードします。 ※Service Provider設定を変更した場合は再ダウンロードが必要です。
--

⇒SP メタデータ XML ファイルがダウンロードされます。次項「<u>3-2-2. Microsoft Entra アプリケーション</u> の作成・設定」にて使用します。

3-2-2. Microsoft Entra アプリケーションの作成・設定

1.ブラウザにて下記 URL にアクセスし、Microsoft Entra 管理センターの画面を表示します。

https://entra.microsoft.com

2.メニュー「ID」>「アプリケーション」>「エンタープライズ アプリケーション」>を表示し、 「新しいアプリケーション」をクリックします。

Microsoft Entra 管理センター		ハリソース、サービス、ドキュメントの検	素 (G+/) ロック の の username@samp また会社の	ole.o
↑ ホーム	Î	ホーム > エンタープライズ アプリケーション	ー リケーション すべてのアプリケーション …	×
★ お気に入り	\sim	株式会社20000000 - 従業員向けの Mi	rosoft Entra ID * 🔰 + 新しいアプリケーション 🜔 更新 🚽 ダウンロード (エクスポート) 🏮 カレビューの情報 🎫 列 国 カレビュー機能 🖗 フィードバックがある	場合
ID	^	概要	▲ Microsoft Cates ニナンある ID プロビノバー以上 水田 マネト2・50キナリフロス プロロの名供用ののプロレー とったまま コノロト 加速 特徴 ます	
① 概要		 截要 X	Microsoft Entra デンアをTD プロパイターといく使用するように気とられている。と目身のABMのシロンクソクーションを表示、ノイルターに圧、使用します。 組織で管理されているアプリケーションの以入れば、アプリケーションの登録にかります。	- 1
೩ ೨-೮-	\sim	管理		
が グループ	\sim	すべてのアプリケーション	アプリケーションの種類 == エンタープライズ アプリケーション × アプリケーション ID 次の値で始まる × ⁺ マ フィルターの追加	
品 デバイス	\sim	🐻 プライベート ネットワーク コネクタ	28 個のアプリケーションが見つかりました	
開 アプリケーション	~	🔷 ユーザー設定	名前 ↑。オフジェクト ID アフリケーション ID ホームページ URL 作成日 ↑。 証明書有効期限… アクラ	ティブな記
エンタープライズ アプリケー		🎟 アプリ起動ツール	A app1 7a45d43d-efo4-4··· 32bebf78-2496-4··· 2023/6/6	
ション		■ カスタム認証拡張機能	A app2 6782b04c-3799-4··· 010aef52-133c-4··· 2023/6/7	
アプリの登録			A app3 aae8cc4b-07bc-4··· 90098dc6-d13b-4··· 2023/6/7	

3.「独自のアプリケーションの作成」をクリックします。

Microsoft Entra 管理センター			/)	ର୍କ 🖉 🖓 🖓 ଅଟେଲାଆକୁ ଅନ୍ତର୍କ୍ଷ 🖉 🖓
🏫 ホーム	Å	ホーム > エンタープライズ アプリケーション すべてのアプ Microsoft Entra ギャラリーを参	^{ゲーション >} 照する …	独自のアプリケーションの作成 ×
★ お気に入り	~	+ 独自のアプリケーションの作成 🔗 フィードバックが	ある場合	☆ フィードバックがある場合
◆ ID ① 概要	^	Microsoft Entra アプリギャラリーは、シングル サインオン (S レートを活用して、ユーザーをより安全にアプリに接続することが は、次に説明されているプロセスを使用して要求を提出できます	SO)と自動ユーザープロビジョニングの展開と構成を簡単にするアプリが できます。ここで独自のアプリケーションを参照または作成してください。簡 す。この記事。	短目のアリケーションを開始している場合、アリリケーションフレキンを使用している場合、またはキキラリーに ないアプリケーションを統合する必要がある場合は、ここで独自のアプリケーションを作成できます。 お使いのアプリの名前は何ですか?
೩ ユーザー	\sim	アプリケーションを検索	シングル サインオン:すべて ユーザー アカウントの管理:All	NI_SAML接班 ✓
か グループ	\sim	クラウド プラットフォーム		アンジーション (このま) As 使用 Fer To (Con Con Sing) ハンガレンスのアガリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーション プロキシ **************
応 デバイス 戦 アプリケーション	~	Amazon Web Services (AWS)	Google Cloud Platform	で満知します アプリケーションを登録して Microsoft Entra ID と統合します(開発中のアプリ) ・ディョーに買っからないよの他のアプリケーションを統合します(ポキャー)ー以外) ・ ・ ドゥーレー以外)
エンタープライズ アプリケー ション アプリの登録		aws	<u></u>	エントレーとなるすのション・ションを使用することをお勧めします。 「シーレーとなるすのションクリーンションを使用することをお勧めします。
そ₀ 役割と管理者	\sim		Google Cloud	
L 課金	\sim			
 設定 	\sim			
合 保護	\sim	SAP		
 Identity Governance 詳細情報とサポート 	~	SAP		And
	**			TF 200

- 4.任意のアプリ名を入力します。
- 5.「ギャラリーに見つからないその他のアプリケーションを統合します(ギャラリー以外)」を選択し、 「作成」をクリックします。

⇒任意のアプリ名でアプリケーションが作成され、概要ページが表示されます。

6.「シングルサインオン」を選択します。

Microsoft Entra 管理センター	рIJ	ソース、サービス、ドキュメントの検索 (G+/)			Q	袋 : (୭ ନି	username@sample.o… 株式会社XXXXXXXX
↑ ホーム	A	ホーム > エンタープライズ アプリケーショ NI_SAML認証 エンタープライズ アプリケーション	₽ すべ 概要	にのアプリケーション > 夏 …				×
★ お気に入り	~		~					
D	^	■ 概要	Î					
① 概要		★ 問題の診断と解決						
೩ ユーザー	\sim	管理		アプ・レーション ID ① 22abc21d-0d4e-48bb-8697-7… D				
☆ グループ	\sim	プロパティ		オブジェクト ID ①				
品 デバイス	\sim	▶ 所有者		e0327e66-ea90-4d73-950d-b… 🗈				
 ■ アプリケーション エンタープライズ アプリケー ション 	^	 ユーザーと育理者 ユーザーとガルーブ シングル サインオン 		Getting Started				

- 7.「SAML」を選択します。
- 8. 「メタデータ ファイルをアップロードする」 をクリックします。



9. 「3-2-1. SP メタデータの準備」でダウンロードした SP メタデータを選択し、

追加ボタンをクリックします。

⇒値がセットされます。

M	licrosoft Entra 管理センター	۶ J	ソース、サービス、ドキュメントの検索 (G+/)	ා ලොක්දු දේශය දේශය දේශය දේශය දේශය දේශය දේශය දේශය	÷ 🕘
\$	л-д		ホーム > エンタープライズ アプリケーショ NI_SAML認証 SA	> すべてのアブリケーション > Microsoft Entra ギャラリーを参照する > NI_SAMLI認証 ML ベースのサインオン …	×
*	お気に入り	\sim	エンターブライズ アプリケーション	《 〒 メダデータ ファイルをアップロードする 🄊 シングル サインオン モードの変更 🗐 このアプリケーションをTest 🖗 フィードバッグがある場合	â
۵	ID	^		^ メタデータ ファイルをアップロードします。	
0	概要		★ 問題の診断と解決	以下のフィールドの値は NI_SAML認証 によって提供されます。値を手動で入力することもできますし、構成済みの SAML メタデータ ファイルが NI_SAML認証 によって提供されている場合にはそれをアップロードすることもできます。	D
8	ユーザー	\sim	管理	"sp_metadata.xml"	
Ŷχ ^α	グループ	\sim	11 วันเวรา		
石	デバイス	\sim	🌆 所有者		
⊞6	アプリケーション	~	🎝 ロールと管理者	参加子 (エンティティエD) 必須	. 1
	エンタープライズ アプリケー	アプリケー A ユーザーどグループ 応答 URL (Assertion Consumer Service 必須	応答 URL (Assertion Consumer Service 必須		
	ション		∋ シングル サインオン	URL) サインオン URL 省略可能	- 1
	アプリの登録		⑦ プロビジョニング	リレー状態(首略可能) 首昭可能 ログアウト URL (首略可能) 首昭可能	
്റ	役割と管理者	\sim	🐺 アプリケーション プロキシ		_



	・SP メタデータをアップロードすることで、以下の値が自動でセットされます。
	「識別子(エンティティ ID)」:NI 製品システム設定画面の「エンティティ ID」の値が
一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	セットされます。
	「応答 URL」:NI 製品システム設定画面の「エンドポイント URL」の値がセットされます。



・「IdP を起点としたシングルサインオン(IdP Initiated SSO)」を利用する場合、

下記の値をセットする必要があります。

「3-5-1. NI 製品を起点としたシングルサインオン」のみを利用する場合は、不要です。

自動セットされた値に加え、ログイン後に表示したい製品のログイン画面の URL を

「リレー状態」へセットしてください。

例) NI Collabo 360 を表示する場合:

https://xxx.xxx.xxx/ni/niware/portal/index.php

Sales Force Assistant シリーズを表示する場合:

https://xxx.xxx.xxx/ni/<各製品>/main/index.php

M	licrosoft Entra 管理センター		, ロリソース、サービス、ドキュメントの検索 (G+,)	C @ @ R username@sample.o @ #username@sample.o	
	ホーム	^	・・・・> エンタープライズ アプリケーション すべてのアプリケー:		基本的な SAML 構成 ×	
	10 14		NI_SAML認証 SAML	ベースの		
*	お気に入り	\mathbf{v}	エンタープライズ アプリケーション		🔜 保存 🚽 📈 フィードバックがある場合	
		- 1	*** #####	↑ メタデー		
۵	ID	^	 ·····························		課パリナ(上ノティティ ID)* ○ Microsoft Entra ID に対1,7アプリケーションを説別する一章の ID. この値は、Microsoft Entra ID テナント内のすべてのアプリケーションで	
1	概要			SAML (i	一意である必要があります。既定の識別子は、IDP で開始された SSO の SAML 応答の対象ユーザーになります。	
0	7_+ * _		× 同題の認知と解決	フェデレーショ: Connect ま	既定	
\sim	1-9-	Ť	管理	こちらをご覧く	https://xxx.xx.xxx.xx/ni/	
*	グループ	\sim	プロパティ	以下をお読み	識別子の追加	
-6	デバイス	\sim	🎥 所有者	1,		
₽	アプリケーション	~	🚨 ロールと管理者	a	応答 URL (Assertion Consumer Service URL) * ①	
~~	エンターブライズ アプリケー		🎎 ユーザーとグループ	12 12	応答 URL は、アプリケーションが認証トークンを受け取る場所です。これは、SAML では ¥"Assertion Consumer Service¥" (ACS) とも militionます	
	ション		∋ シングル サインオン	R	1914/189.	
	アプリの登録		⑦ プロビジョニング	U U	12… 既定	
A	保護	\sim	🐻 アプリケーション プロキシ		https://xxx.xx.xxx/nl/zcom/service/index.php?p=saml 1 💟 🛈 📋	
r sa	Identity Governance	~	😔 セルフサービス	2 .	论者 URL 的追加	
	identity dovernance	Ť	🧾 カスタム セキュリティ 属性	J#	井水(ホーロ)(学校可能)	
ųb	External Identities	\sim	ヤキュリティ	g	サインパン URL(目4日91月2) サービス プロバイダーによって開始されたシングル サインオンを実行する場合は、サインオン URL が使用されます。この値は、アプリケーションのサ	
	表示数を増やす		 条件付きアクセス 	e	インイン ページの URL です。ID プロバイダーによって開始されたシングル サインオンを実行する場合、このフィールドは不要です。	
-			- アクヤス許可	-	サインオン URL を入力してください 🗸	
4	保護	~	トークンの暗号化			
100	Identity Covernance		 I 28 (with 210) 	3 s	リルー状態 (省略可能) ⊙	
(4)	identity Governance	~	アクティビティ	F	リルー状態は、認証が完了した後にユーザーのリダイレクト先となるアプリケーションを指示します。通常、値は、ユーザーをアプリケーション内の特定	
	検証済み ID	\sim	● サインイン ログ	ŧ	の場所に移動する URL または URL バスです。	
_			前使用状况と分析情報	托卡	https://xxx.xxx.xxx.xxx/ni/niware/portal/index.php	
			国 監査ログ	j]		

- 11. 「保存」 ボタンをクリックします。
 - ⇒アプリケーションの SAML 設定が変更されます。



12.「ユーザーとグループ」を選択し、「ユーザーまたはグループの追加」をクリックします。

м	icrosoft Entra 管理センター		、 クリソース、サービス、ドキュメントの検索 (G+/)	දුවී ා ල ළ username@sample.o… ● අයදුවරාරාගාර
A	木一ム	^	ホーム> エンタープテイズ アブリケーション すべてのアブリケーション > Microsoft Entra ギャラリーを参照する > NI_SAML認証 ● NI_SAML認証 ユーザーとグループ …	×
*	お気に入り	\sim	エンタープライズ アプリクーション (+ ユーザーまたはグループの追加) / 別り当ての編集 回 開除 / 資格情報の /	亜新 │ 🎫 列 │ 🔗 フィードバックがある場合
۵	ID	^	■ 概要	するには、プロバティの中で [ユーザーに表示しますか?] を [いいえ] に設定しま →
()	概要		■ 9-0-11 m す。 ※ 問題の診断と解決	
8	ユーザー	\sim	管理 ここで、アプリケーションのアプリのロールにユーザーとグループを割り当てます。このアプリケーションの新	しいアプリのロールを作成するには、アプリケーション登録を使用します。
'n	グループ	\sim	. □ 見切ティ	
Ð	デバイス	\sim	5 所有者 表示名 オブジェクトの種類	割り当てられたロール
₿,	アプリケーション	^	ロールと管理者 アプリケーションの割り当てが見つかりませんでした	
1	エンターブライズ アプリケー ション		 ユーサーとクループ シングル サインオン 	
	アプリの登録		プロビジョニング	

13.アプリケーションを使用するユーザーを選択し、「割り当て」をクリックします。

⇒アプリケーションのアクセス設定が変更されます。

\$					6(0) (G1))				
	ж —Ь	^ 7	^{Kーム > エンタープライズ アプ 副り当ての追加}	ユーザー					×
*	お気に入り 〜		k式会社xxxxxxxx	① 探している	るものが見つからない場合は、こ	マイルターの変更または追	加をお試しください。	選択済み (2)	
۵	ID ^		▲ お客様の Active Directo	検索				9 Utyr	
0	概要		当てることはできます。	○ 5 件の結果が見	つかりました			XX XX username@sample.onmicrosoft.com	Û
8	ユーザー 〜		Lーザー 選択されていません	ৰুম্ব এ-	ザ –			xx xx	n
'n	グループ 🗸		ールを選択してください		名前	種類	詳細	username@sample.onmicrosoft.com	
£3	テバイス >				XXX XXX	ユーザー	username@sample.onmicrosoft.com		
8	アプリケーション ハ エンタープライズ アプリケー ション				XXX XXX	ユーザー	username@sample.onmicrosoft.com		
	アプリの登録				X0K X0K	ユーザー	username@sample.onmicrosoft.com		
-	役割と管理者 〜	1			201.201	7-#-	username@sample.onmicrosoft.com		
Ð	課金 〜	·			AA AA	-4-7	usernaine@sample.onmicrosorc.com		
٢	ROC ~	·			XXXXXX	ユーザー	username@sample.onmicrosoft.com		
8	保護	'							
3	Identity Governance 🗸 🗸	· •		4				Þ	
2	詳細情報とサポート	^	distant from						
м	icrosoft Entra 管理センター	م ر	リソース、サービス、ドキュメン	/トの検索 (G+/))		e	ା ହାର ଜ୍ୟାନ୍ତ (sample sample sam	e.o
♠	ホ−ム		▲ ホーム > エンターブ	ライズ アプリケー	ション すべてのアプリケーショ	> Microsoft Ent	ra ギャラリーを参照する > NI_SAML認証	ユーザーとグループ >	
			割り当ての	追加 …					
*	model (= 1 k)		株式会社xxxxxxxxx						×
	る別に入り	\sim	株式会社0000000						×
<u></u>	D D	~	株式会社20000000x	ive Directory 7	ランレベルでは、グループを取り出い	(ることができません。 個々の	0ユーザーをアプリケーションに取り		×
) () ()	お知に入り ID 概要	~	株式会社20000000 本式会社200000000 お容様の Acti 当てることはで	ive Directory プ きます。	ラン レベルでは、グループを割り当	てることができません。個々の	0ユーザーをアプリケーションに割り		×
ַ 	b3Alc入り ID 但要 ユーザー	< < >	株式会社0000000 本式会社0000000 単てることはで ユーザー ユーザー	ive Directory プ きます。	ラン レベルでは、グループを割り当	こることができません。 個々(0ユーザーをアプリケーシャンに割り		×
() () () () () () () () () () () () () (BRIL A 9 回 型 - ザー グループ	< < >	株式会社0000000 本式会社0000000 当てることはで ユーザー 2 人のユーザーが選択してくださ	ive Directory プ きます。 明Rされました。 むい	ラン レベルでは、グループを割り当	くることができません。 個々く	0ユーザーをアプリケーシャンに激け		×
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	BRACA9 ID 低度 ユーザー グループ デバイス	<pre></pre>	株式会社20000000 本 お客様の Act 当てることはで ユーザー 2 人のユーザーが調 ロールを選択してくださ User	ive Directory プ さます。 明心れました。 むい	ランレベルでは、グループを取り当	こることができません。 個々く	0ユーザーをアプリケーシャンに激け		×
 0 2 ∞ ∞ 	は し し こ ーザー ブルーブ デバイス アブリケーション	× × × × ×	株式会社20000000 ▲ お客様の Act 当てることはで、 ユーザー 2 人のユーザーが選択して代える User	ive Directory プ きます。 明心れました。 むい	ランレベルでは、グループを取り当	CGごとができません。 個々C	ロユーザーをアプリケーションに割り		×
○ ○ ○ ○ 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇	と 34(- ペリ 一切 一切 一づ デバイス アブリケーション エンタージョイズ アブリケーション ション	× × × × × ×	株式会社2000000 ▲ お衣格の Act ■でることはで コーザー 2 人のユーザーが用 ロール選択しては2 User	ive Directory ア まます。 BRされました。 SU	ランレベルでは、グループを取り当	こることができません。 個々(0ユーザーをアプジャーションに割り		×
 ♪ 〕 へ ポ 記 現	と SAIL AU	× × × × ×	株式会社2000000 ▲ お衣格の Act ■でることはで ユーザー 2 人のユーザーが用 ロールを選択してなど User	ive Directory ブ まます。 切るわました。 3し	ランレベルでは、グループを取り当	cockfreakth, @qq	0ユーザーをアプジーションに割り		×
	ID 43.5 2ザー グループ デブリケーション エンターブライズ アブリケーション マブリの登録 役別と管理者	× × × × ×	株式会社2000000 ▲ お存後のAct 当てることはて コーザー 2 人のユーザーが弱 ロールを選択してだと User	ive Directory プ きます。 明心れました。 い	ランレベルでは、グネーブを動り当	こここだできません。 個々(0.2-ザーをアプリケーションに取り		×
	ID 43.5 2ザー グループ デブリケーション エンターブライズ アブリケーション マブリの登録 役別と管理者 日本会	> < < > > < > > > > > > > > > > > > > >	株式会社2000000 ▲ お存後のAct 当てることはて コーザー 2、人のユーザーが弱 ロールを知识してた2 User	ive Directory プ まます。 明心されました。 とい	ランレベルでは、グネーブを動り当	こここだできません。 個々(0.2-ザーをアプリケーションに取り		×
	D All All	<pre>> <</pre>	株式会社2000000 ▲ お存根の Act 当てることはて コーザー 2 人のユーザーが弱いてでた2 User	ive Directory プ まます。 明心れました。 とい	ランレベルでは、グネーブを動り当	こここだできません。 個々(0.2 <i>-1f-0771/y-24</i> ンに取り		×
	と SAIL × V J レ 超更 ユーザー グルーブ デブリケーション エンターブライズ アブリケーション アブリの合録 総計と管理者 読定 確認	× × × × × × × × ×	株式会社2000000 ▲ お客様的 Act ■ ころことはで コーザー 2 人のユーザーが消 ロールが消化してた2 User	ive Directory 7 223. BR∂AISUR. 50	ランレベルでは、グループを取り当	(<u>उट</u> 257788स्प्रेस, आवित	0ユーザー&アプリケーションに激り		×
	ID 振	<pre></pre>	株式会社2000000 ▲ お茶味のAct 当てることはで コーザー 2 人のコーザー約 ロールを送用してのため USE*	Nwe Directory ブ 8334. BR∂t13UR. SU	ランレベルでは、グループを取り当	C5ごとができません。 個々(ロユーザーをアプリケーションに面印		×
 	と 341 - 人り 10 相応 400 <th>× · · · · · · · · · · · · · · · · · · ·</th> <th>株式会社2000000 ▲ お花枝の Act ■でることはで コーザー 2 人のユーザーケー約 日 一が送用してたと User</th> <th>ive Directory ל פור פור פור פור פור פור פור פור פור פור</th> <th>ランレベルでは、グループを取り当</th> <th>C.5ことができません。 個々の</th> <th>0ユーザー&アプリケーションに取り</th> <th></th> <th>×</th>	× · · · · · · · · · · · · · · · · · · ·	株式会社2000000 ▲ お花枝の Act ■でることはで コーザー 2 人のユーザーケー約 日 一が送用してたと User	ive Directory ל פור פור פור פור פור פור פור פור פור פור	ランレベルでは、グループを取り当	C.5ことができません。 個々の	0ユーザー&アプリケーションに取り		×

3-3.NI 製品の設定

3-3-1. Microsoft Entra ID の設定値を確認する

1.追加した Microsoft Entra アプリケーションの画面を表示し、「シングルサインオン」をクリックします。

2.画面より、Microsoft Entra ID の設定に必要となる「フェデレーションメタデータ XML」の

「ダウンロード」をクリックし、XML ファイルを保存します。



3-3-2.システム設定

1.システム設定の セキュリティ より「SAML 認証」を選択します。

⇒「認証/SAML 認証」画面が表示されます。

2.以下の項目を入力し、

ボタンをクリックします。

項目名称	説明	設定値
シングルサインオン設定		
シングルサインオン	シングルサインオンを利用するかしないかを設定します。	利用する
有効範囲	SAML 認証を許可する接続元 IP アドレスを改行区切りで指定し	※補足を参照
	ます。空白の場合は、すべての接続で SAML 認証を行います。	
Service Provider(NI 婁	製品)設定	
エンティティ ID	Service Provider の識別子。任意の文字列を設定します。	https://xxx.xxx.xxx.xxx/ni/
	※初期値の URL から変更する必要はありません。	
エンドポイント URL	SAML レスポンスを受信する URL です。	-
	※Identity Provider のセットアップに使用する固定値です。	
仮名	仮名 ID を用いた認証を利用するかしないかを設定します。	利用する / 利用しない
認証方法	認証にパスワード認証を用いるか、Windows 認証を用いるかを	パスワード認証
	設定します。	
ログアウト URL	NI 製品からログアウト後に遷移する URL を設定します。	https://login.microsoftonline.c
		om/common/wsfederation?wa
		=wsignout1.0

✓ 補足	・NI 製品からログアウトする際に、IdP からもログアウトする必要がない場合は、 ログアウト URL に下記 URL を設定することで、通常の NI 製品ログイン画面に遷移します。
	https://<任意の NI 製品 URL>?saml=no ・社内端末の IP アドレスを「有効範囲」に指定することで、モバイル端末など社外からの接続 (ことり Idp に接続不可の提合は、「有効範囲」は とむるため、CAML 認証が適用されず
	通常のログイン画面が表示されます。

- ・Microsoft Entra ID は、認証方法「Windows 認証」に対応していません。
- ・エンティティ ID を変更した場合、IdP の再設定が必要になります。
- ・NI 製品の社員ログイン ID と、

注意

Microsoft Entra ID のユーザーID を一致させておく必要があります。

Microsoft Entra ID のユーザーID は、以下の画面から確認できます。

1. Microsoft Entra アプリケーションの画面から、

「ユーザーとグループ」をクリックします。

2. 対象のユーザーをクリックします。



3. Microsoft Entra ID のユーザーID が「ユーザープリンシパル名」として表示されます。



3.IdP メタデータをアップロードします。

NI 製品システム設定「認証/SAML 認証」画面の、Identity Provider 設定の「メタデータ」に

Microsoft Entra アプリケーションからダウンロードした「フェデレーションメタデータ XML」を添付します。

読み込み	ボタン	をクリックします。	
メタデータ	:	ドラッグ&ドロップで貼り付けることができます。	٦
		FederationMetadata.xml	*
		Identity Providerのメタデータをアップロードしてください。 読み込むことができるファイルは、拡張子が「xml」のファイルです。 XMLより設定値を抽出し、以下の項目を自動設定します。 (エンティティID, エンドポイントURL, 証明書) 読み込み	

以下の設定項目が自動で入力されます。

項目名称	説明	設定サンプル値						
Identity Provider 設定								
エンティティ ID	Identity Provider の識別子を設定します。	https://sts.windows.net/xxxxx						
		xxx-xxxx-xxxx-						
		xxxxxxxxxxx/						
エンドポイント URL	SAML リクエストを送信する URL を設定します。	https://login.microsoftonline.c						
		om/xxxxxxxx-xxxx-xxxx-xxxx-						
		xxxxxxxxxxx/saml2						
証明書	Identity Provider が署名に使用する公開鍵を設定します。	Base64 エンコードされた文字列						
	カンマ区切りで複数証明書を指定できます。							

4. 保存 ボタンをクリックします。

3-4.仮名 ID 取得



・仮名を利用する場合のみ、各ユーザーが下記の作業を行う必要があります。

3-4-1.オプション設定

1.仮名を利用する場合、初回ログイン時はシングルサインオンに失敗するため、

通常の NI 製品ログイン画面より、ID/パスワードを入力し、ログインしてください。

2.NI 製品の「オプション設定」画面を表示し、「SAML 認証」を選択します。

⇒ 「SAML 認証」 画面が表示されます。

3. 取得する ボタンをクリックして、Identity Provider から仮名 ID を取得します。

※新規ウィンドウが開き、Identity Provider へ接続します。仮名 ID 取得後に Window は自動的に閉じられ ます。

4.最後に 保存 ボタンを押します。

3-5.動作確認

3-5-1.NI 製品を起点としたシングルサインオン

1.NI 製品の任意の URL にブラウザでアクセスします。

2.IdP にログインします。

Microsoft Entra ID のログイン画面にて、ID/パスワードを入力することで認証されます。



3.NI 製品の目的の URL が表示されます。





3-6-1. Microsoft Entra ID のエラー画面

以下のような画面が表示された場合、Microsoft Entra ID 側でエラーが発生しています。



通常のログイン画面の URL に「?saml=no」を追加し、NI 製品へログインしてください。

例)NI Collabo 360

https://xxx.xxx.xxx/ni/niware/portal/index.php?saml=no

例) Sales Force Assistant シリーズ

https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php?saml=no

3-6-2. Microsoft Entra ID のエラー詳細確認

Microsoft Entra ID のエラー画面にて、赤枠内のメッセージを参照します。

エラーID	エラーメッセージ	対応方法
AADSTS70001	Application with identifier 'https://xxx.xxx.xxx.xxx/ni/'	SP のエンティティ ID が誤ってい
	was not found in the directory xxxxxxxx-xxxx-xxxx-xxxx-	ます。
	xxxxxxxxxxx	NI 製品システム設定> Service
		Provider(NI 製品)設定>「エンテ
		ィティ ID」と、Microsoft Entra
		アプリケーション設定の「アプリ
		ケーション ID/URI」に同じ値を
		設定してください。
AADSTS75011	Authentication method 'Password' by which the user	認証方法に「Windows 認証」を指
	authenticated with the service doesn't match requested	定した場合に表示されます。
	authentication method 'WindowsIntegrated'	「パスワード認証」に変更してく
		ださい。
AADSTS50105	Your administrator has configured the application xxxxx('	作成した Microsoft Entra アプリ
	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx	ケーションを使用する権限がない
	unless they are specifically granted ('assigned') access to	ユーザーでサインインした場合に
	the application. The signed in user ' xxxxxxxx @	表示されます。Microsoft Entra ア
	xxxxxx.onmicrosoft.com' is blocked because they are not a	プリケーションのアクセス設定を
	direct member of a group with access, nor had access	変更してください。
	directly assigned by an administrator. Please contact your	
	administrator to assign access to this application.	

3-7.運用時の注意

3-7-1.証明書の更新について

Microsoft Entra ID は、以下の証明書を利用して動作しています。

トークン署名証明書

Microsoft Entra ID では、定期的にロールオーバー(トークン署名証明書の更新)が発生します。

ロールオーバーされた場合、「<u>3-3-2 システム設定</u>」項の「4. IdP メタデータをアップロードします。」を 再実行する必要があります。

詳細は、Microsoft 社の情報をご確認ください。

https://learn.microsoft.com/ja-jp/entra/identity-platform/signing-key-rollover

4.トラブルシューティング

4-1.シングルサインオンができない場合の対応方法

以下の手順で対応を行ってください。

1.IdPのエラー画面が表示されている場合

各 IdP のトラブルシューティングを参照してください。

- → AD FS のトラブルシューティング
- → Microsoft Entra ID のトラブルシューティング

2.通常のログイン画面が表示される場合

ID/パスワードを入力して NI 製品にログインし、システム設定画面の「運用管理 > アクセス/アクセスログ」に、エラーメッセージが出力されていないかを確認してください。

→4-2.SAML 認証のログを確認する

→4-3.SAML 認証エラーの原因を調べる

3.IdP にアクセスできない場合

ブラウザに「このウェブページにアクセスできません」、「このページは表示できません」などのメッセージが 表示される場合、端末から IdP に接続できていません。

次の項を参照してください。

→4-4.IdPに接続不可の端末から NI 製品にアクセスする

4.エラーメッセージが出力されていない場合

システム設定画面の「セキュリティ > 認証/SAML認証」から、以下の設定が正しいことを確認します。

→シングルサインオンを「利用する」設定になっているかどうか

→有効範囲が正しく設定されているかどうか
4-2.SAML 認証のログを確認する

システム設定画面の「運用管理 > アクセスログ」より、SAML 認証についてのログを確認できます。 ログは区分「ログイン画面の接続監視」で出力されます。

メッセージ	説明
SAML 認証によるシングルサインオンに成功しました。	正常にシングルサインオンした際に表示されます。
[XXX]	(※XXX:ログインしたユーザー名)
SAML 認証によるシングルサインオンに失敗しました。	シングルサインオン処理に問題があった場合に表示され
(XXX)	ます。
	「 <u>4-3.SAML 認証エラーの原因を調べる</u> 」項を参照し
	て、設定値を見直してください。
	(※XXX:エラーの詳細メッセージ)
NameID に該当するユーザーが見つかりませんでした。	仮名を利用する際に、仮名 ID の設定を行っていない状態
(XXX)	で、シングルサインオンを実行した際に表示されます。
	オプション設定画面より、仮名 ID 取得を行ってくださ
	い。
	(※XXX:仮名 ID)
NameID に該当するユーザーが複数見つかりました。	複数の NI 製品ユーザーが、同じ IdP のアカウントと紐付
	いた状態でシングルサインオンを実行した際に表示され
	ます。
	再度オプション設定画面より、仮名 ID 取得を行い、正し
	いアカウントにてログインしてください。
SAML 認証対応製品ではありません。	SAML 認証に対応していない製品から、シングルサイン
	オン処理が行われた際に表示されます。
使用停止中です。[XXX]	使用停止中のユーザーに対して、シングルサインオンし
	た際に表示されます。
ロックアウト中です。[XXX]	パスワードを連続で間違えたことによりロックアウト状
	態のユーザーに対して、シングルサインオンした際に表
	示されます。

4-3.SAML 認証エラーの原因を調べる

SAML 認証によるシングルサインオン処理に問題があった場合に出力されるメッセージと、対応方法の一覧です。 以下の形式でアクセスログが出力されます。

SAML 認証によるシングルサインオンに失敗しました。(<エラーカテゴリ>:<エラーメッセージ詳細>)

エラーカテゴリ	エラーメッセージ詳細	対応方法
Invalid array settings	sp_entityId_not_found	SP のエンティティ ID が設定されていません。
		正しい値を設定してください。
	idp_entityId_not_found	IdP のエンティティ ID が設定されていませ
		ん。正しい値を設定してください。
	idp_sso_not_found	IdP のエンドポイント URL が設定されていま
		せん。正しい値を設定してください。
	idp_sso_url_invalid	IdP のエンドポイント URL が URL の書式にな
		っていません。正しい値を設定してください。
	idp_cert_or_fingerprint_	IdPの証明書が設定されていません。正しい値
	not_found_and_required	を設定してください。
invalid_response	The status code of the Response was	システム設定画面「セキュリティ > 認証/
	not Success, was Requester ->	SAML 認証」の Service Provider(NI 製品)設
	urn:oasis:names:tc:	定>「仮名」の値がセットアップ時から変更さ
	SAML:2.0:status:InvalidNameIDPolicy	れています。
		値を修正するか、再度 IdP の設定を行ってくだ
		さい。
	invalid_response: The status code of	AD FS の認証ポリシーの設定で、認証方法が
	the Response was not Success, was	無効となっています。
	Responder -> urn:oasis:names:tc:	「 <u>2-4-4.認証ポリシーの設定</u> 」の手順が正しく
	SAML:2.0:status:NoAuthnContext	実行できていることを確認してください。
	Signature validation failed. SAML	システム設定画面「セキュリティ > 認証/
	Response rejected	SAML 認証」の Identity Provider(NI 製品)設
		定>「証明書」の値が正しくありません。
		再度 Identity Provider のメタデータを取得
		し、アップロードしてください。
		※IdP側で署名鍵が更新された場合、このエラ
		ーが表示されます。

4-4.IdPに接続不可の端末から NI 製品にアクセスする

ブラウザに「このウェブページにアクセスできません」、「このページは表示できません」などのメッセージが表示される場合、以下の原因が考えられます。

1.IdPのアドレスの名前解決に失敗している。

端末の DNS サーバーの設定を確認してください。

2.IdPが社内ネットワークにある場合に、モバイル端末など、社外ネットワークから NI 製品にアクセスしている。 システム設定画面「セキュリティ > 認証/SAML 認証」の「有効範囲」の設定により、 接続元 IP アドレスに応じて、SAML 認証を行うか、通常のログイン画面を表示するかを 自動で切り替えられます。

社内接続でのみ SAML 認証を行いたい場合、有効範囲に社内端末の IP アドレスを指定してください。 指定された IP アドレス以外からアクセスした場合は、通常のログイン画面が表示されます。

保存	設定	
シングルサインオン *:	●利用する	◎利用しない
有効範囲:	192.168.1.* 192.168.2.1 192.168.2.2	
	SAML認証を許可する接続元IPアドレスを改行区切りで指定してください。 指定した接続元以外からのアクセスの場合、通常のログイン画面を表示します。 空白の場合は、すべての接続でSAML認証を行います。 *(アスタリスク)での指定が可能です。(例:192.168.1.*の場合は最後の桁が無視されます。)	

または、またはログイン画面の URL に「?saml=no」を追加して NI 製品にアクセスすることで、どの端末でも通常のログイン画面を表示できます。

例) NI Collabo 360

https://xxx.xxx.xxx/ni/niware/portal/index.php?saml=no

例) Sales Force Assistant シリーズ

https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php?saml=no

ただし、有効範囲を設定せず、上記 URL でアクセスした場合は、ログアウト時に「このウェブページにアクセ スできません」、「このページは表示できません」などのメッセージがブラウザに表示されますが、正常な動作 となります。

5.制限事項

5-1.技術的・運用的制限

- ・SSL(https)接続の利用が必須となります。
 - 「1-2-2.SSL(https)での接続設定を行う」項を参照してください。
- ・Windows 認証を使用する場合、コントロールパネルでの設定が必要です。
 - 「Windows 認証」項を参照してください。
- ・以下の場合は SAML 認証は行わず、通常のログイン画面が表示されます。
 - ・携帯版サイトにアクセスしている。
 - ・スマホ向けアプリで NI 製品にアクセスしている。
- ・SAML の仕様では、IdP が社内ネットワーク内であっても、シングルサインオン可能ですが、 NI 製品に社外からアクセスを行ったり、モバイル端末からアクセスする場合には、 IdP を外部から参照可能なサーバー構成にする、もしくはプロキシサーバーを構築する必要があります。
- ・SAML 認証メッセージの暗号化には対応していません。

5-2.対応製品

SAML 認証は、以下の製品に対応しています。

- ・Sales Force Assistant シリーズ
 - Sales Force Assistant 顧客創造
 - Sales Force Assistant 顧客創造 R
 - Sales Force Assistant 顧客深耕
 - Sales Force Assistant 深耕創造
 - Sales Force Assistant 顧客深耕 R
 - Sales Force Assistant 顧客深耕 AO
 - Sales Force Assistant ABM
 - ※顧客の声オプション含む
- NI Collabo 360
- MapScorer
- \cdot nyoibox
- Approach DAM
- Sales Quote Assistant
- Sales Billing Assistant

○ 商標

本説明書に登場する会社名、製品名は各社の登録商標、商標です。

○ 免責

本説明書に掲載されている手順による操作の結果、ハード機器に万一障害などが発生しても、弊社では一切の責任を負いま

せんのであらかじめご了解ください。

○ 発行

2024年4月16日 第 14 版

株式会社 NIコンサルティング

サポートデスク

E-mail : support@ni-consul.co.jp Fax : 082-511-2226

営業時間:月曜日~金曜日 9:00~12:00、13:00~17:00(当社休業日、土・日・祝日を除く)