Kivuto™

Digital Distribution. Simplified.

Shibboleth ユーザー認証

お客様実装ガイド

2018-10-03

バージョン 4.3

目次

はじめに

このセクションは、次の内容で構成されています。

- 目的及び対象読者
- 頻出用語

目的及び対象読者

このドキュメントでは、既存のShibboleth IdPプロバイダーとKivuto ELMS Webストア間で、シングルサインオン機構を確立する方法について詳細に説明します。

このドキュメントの主な対象読者は、組織のためにアイデンティティーサービスを管理するELMSサイト管理者、および技術スタッフです。

このドキュメントは、ELMS管理Webサイトのオンラインヘルプと合わせてお読みください。

頻出用語

用語	定義の説明
ELMS	電子ライセンス管理システム
お客様	ELMS Webストアを利用するための購買者の認証方法をShibbolethとしている組織。ELMS管理Webサイトでは、お客様は組織として定義されます。
購買者	ELMS Webストアにサインインしているユーザー。
Webストア	お客様に代わって製品を提供する Kivuto 社のELMS e コマースWebサイト。
組織のWebストア	組織全体のソフトウェア配布契約が関連付けられているWebストアです。この組織に所属するメンバーはWebストア を通じてソフトウェアを注文することができます。

用語	定義の説明
学部のWebストア	学部のソフトウェア配布契約が関連付けられているWebストアです。特定の学部に所属するユーザーのみ、このタイプのWebストア を通じてソフトウェアを注文することができます。
統合Webストア	このELMS Webストアは、組織全体と学部の複数のソフトウェア配布契約が関連付けられています。組織に属する全ユーザーは、このタイプのWebストアにサインインして組織単位で契約されたソフトウェアの注文が可能です。対象学部ユーザーは学部ごとの契約を通じて提供されるソフトウェアにアクセスできます。
ELMS管理	ユーザー認証の設定だけでなく、Webストアを管理するための機能がELMSには含まれています。これにより、認証されたユーザーのみWebストアへアクセスできます。
SHibboleth（シボレス）	http://shibboleth.net：より ″Shibboleth システムは、組織内、および組織の境界を超えたWebへのシングル サインオンのための、標準ベースのオープン ソース ソフトウェア パッケージです。これによって各サイトは、プライバシーを保護しながら、保護されたオンラインリソースに対する個々のアクセスについて、情報に基づく認証決定を行うことができます。”
IdP（IDプロバイダー）	「Id プロバイダー」。ユーザーがシングルサインオンを使用して、他のWebサイトにアクセスできるようにするプロバイダー。
SP（サービスプロバイダー）	「サービス プロバイダー」。ソフトウェアを提供するWebサイトを管理するプロバイダー（Kivutoなど）。
Entity Id	Shibboleth設定内のIdP(IDプロバイダー)またはSP（サービスプロバイダー）の一意の名前。 Kivuto のEntity Id の値はこちらです。https://e5.onthehub.com
メタデータ	相互通信するIdPとSPにより用いられる構成日付。
属性	電子メール アドレスまたは一意の識別子など、IdPが個人について指定するアサーション。
外部組織コード	Shibboleth のようなシングル サインオン認証サービスによって交信している間、組織によって、またはその親組織によって、それを特定するためのコードが提供されます。資格ある学部ユーザーのみ学部別のWebストアにアクセスできるようにするためには、このコードに一致した属性がパスされなければなりません。
WAYF	Where Are You From - 検索サービス

Shibboleth ユーザー認証の概要

このセクションは、次の内容で構成されています。

ユーザーの認証とは何か？

ユーザーの認証は、Webストアからソフトウェアを注文する利用資格を認証する方法です。

Webストアでは、認証されたユーザーのみソフトウェアを注文することができます。ELMS管理者は、ユーザーの認証方法を定義する必要があります。これがいわゆる認証方法です。認証方法では、電子メールドメイン、ユーザーインポート、統合ユーザー認証（IUV）、Shibboleth（フェデレーション　アイデンティティ　プログラムから）などがあります。

SHIBBOLETH とは何か？

Shibboleth(シボレス) は、全世界で広範囲に採用されているシングル サインオン（SSO）認証方式です。このように広範囲に導入されているのは、個人や組織が外部に公開する個人情報を確実に管理できる、オープンソースを原点としたプライバシー保護モデルによります。

Shibbolethは、フェデレーション、または組織のグループによって多く使用されています。例えば、InCommon は米国における組織のフェデレーションです。The Canadian Access Deferationは、カナダの教育機関にShibbolethを提供している団体です。

Shibboleth の背景情報については、 http://shibboleth.netをご参照ください。

サインオン手続きの段階的な詳細は、以下のサイトからご覧いただけます。 http://www.switch.ch/aai/demo/easy.html

SHIBBOLETH FEDERATIONS（シボレス　フェデレーション）

ELMSによって Shibboleth をご利用のお客様は、 Kivutoが SP（サービスプロバイダー）である フェデレーションの会員でなければなりません。Kivuto がサポートするフェデレーションのリストは、**表1**をご覧ください。

表 1：フェデレーション リスト

フェデレーション	国
AAF	オーストラリア
ACOnet	オーストリア
ARNES	スロベニア
Belnet	ベルギー
Canadian Access Federation (CAF)	カナダ
DFN-AAI	ドイツ
Edugate	アイルランド
GakuNin	日本
GRNET AAI	ギリシャ
Haka	フィンランド
IDEM GARR	イタリア
InCommon	米国
KAFE	韓国

フェデレーション	国
RCTsaai	ポルトガル
RENATER	フランス
SWAMID	スウェーデン
SWITCHaai	スイス
Tuakiri	ニュージーランド
UK Federation	英国
WAYFDK	デンマーク

SHIBBOLETH のしくみ

ELMS Webストアでの Shibboleth サインオンの一般的な手順は次のとおりです。

購買者がELMS Webストアを訪れる：購買者がリンクをクリックしてサインインするか、認証を必要とする操作（ショッピング カートに商品を追加するなど）を行うと、ELMS Webストアに統合されているShibboleth SP（サービスプロバイダー）ソフトウェアによって、お客様のShibboleth IdPサインインページ、または必要に応じてリモートの検索サービス（WAYF）に購買者がリダイレクトされます。

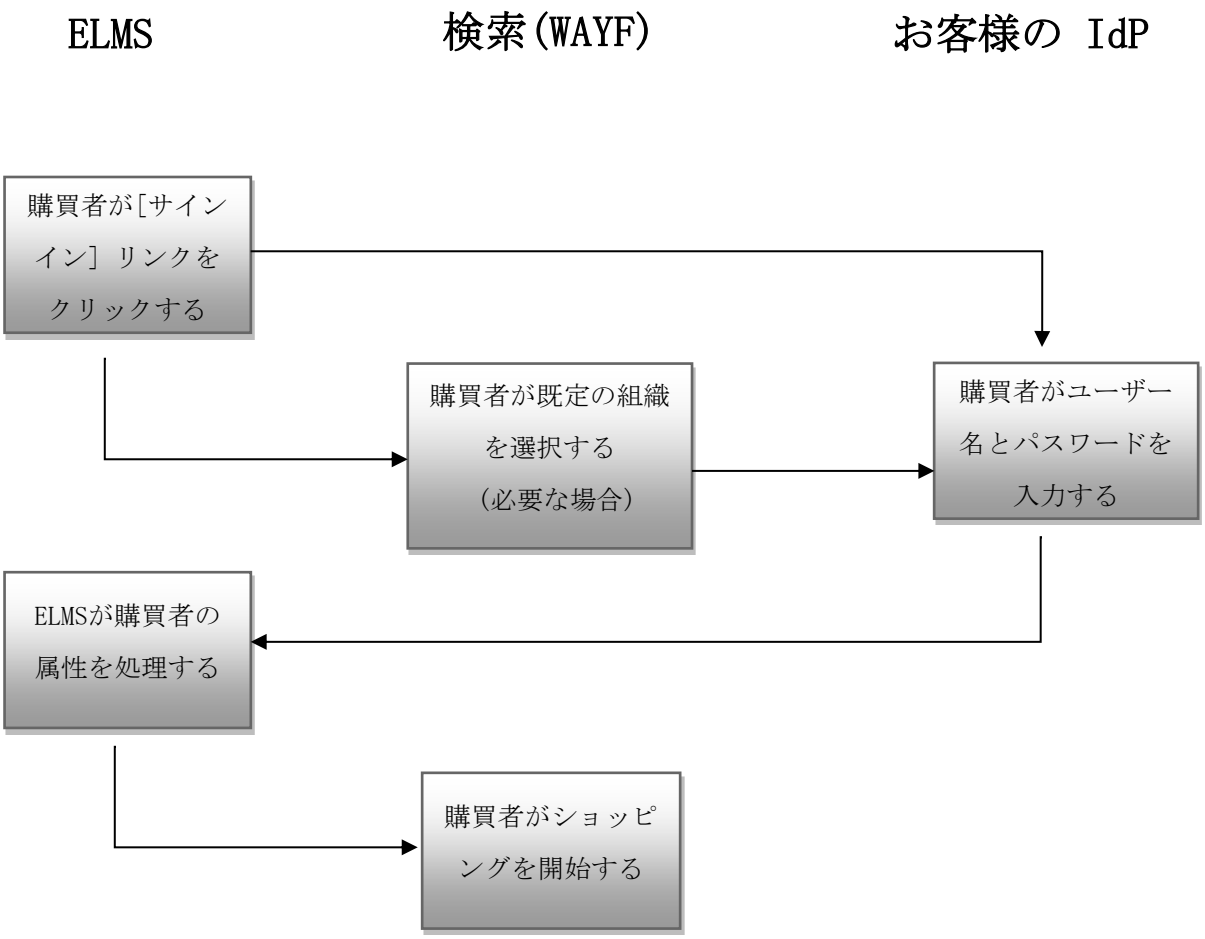
購買者が既定の組織を選択する：この手順は通常は不要ですが、フェデレーションの複数のメンバーが同じELMS Webストアにアクセスする場合に実行できます。検索サービスが購買者に組織のリストを提供し、購買者がそのリストから既定の組織を選択すると、その後、購買者がそのお客様のサイトにリダイレクトされます。

お客様のサイトによって購買者が認証される：お客様のサイトで購買者の資格情報を要求するプロンプトが表示され、ユーザーが認証されます。この認証は、お客様のShibboleth IdPソフトウェアによって調整されます。IdPは購買者のためにKivutoが要求する属性の最小限のセットを作成します。購買者は、

このサイトからELMS Webストアにリダイレクトされます。

ELMS Webストアが購買者を認証する：お客様の IdP によってリリースされた属性は、ELMS Webストアで資格情報のセット（ユーザーアカウント）を作成するために使用されます。この処理によって認証プロセスが完了し、購買者が要求したもとのページが表示されます。

顧客経験の略図



一目で分かるSHIBBOLETHの実装

IdP を設定します

Kivuto Entity Idに属性をリリースします

+

IdP と通信するようにELMSを設定します

+

統合をテストします

IdPを設定します

このセクションは、次の内容で構成されています。

- メタデータと Kivuto Entity Id
- 属性

メタデータと KIVUTO ENTITY ID

お客様の組織が、Kivutoをサービスプロバイダーとするフェデレーションの IDプロバイダーである場合、それぞれはフェデレーションが公開したメタデータに含まれることになります。

Kivuto によって使用されるEntity IDは、次のとおりです。**https://e5.onthehub.com**

属性

Kivuto が必要とするIDアサーションの最小限のセットは次のとおりです。

- 購買客の一意の識別情報
  - これにより、何度ログインしても同一の購買者として識別されます。
- グループ所属機関のリスト
  - これによって、購買者は特定のユーザーグループ一限定の製品を利用できるようになります。例えば、教職員のみ利用可能な製品などがあります。

ELMS Webストアでユーザー別の詳細設定を行うために、さらにIdアサーションが作成される（統合中にパスされる）場合があります。

属性の一覧については、**表2** の属性を参照してください。

注意: どの属性がパスされなければならないかは、実装シナリオによります。お客様の実装にどの属性が必要かを決定するには、Shibboleth実装シナリオをご覧ください。

表2：属性

属性	説明
eduPersonTargetedID urn:mace:dir:attribute-def:eduPersonTargetedID: urn:oid:1.3.6.1.4.1.5923.1.1.1.10	ユーザーの一意の識別情報。不明瞭な場合は、「ユーザー名の非表示」を設定することが望ましい場合があります。（**表3**の設定を参照してください。）
persistent ID (SAML 2.0) urn:oasis:names: tc : SAML:2.0:nameid-format:persistent	ユーザーの一意の識別情報。
uid urn:mace : dir:attribute-def:uid urn: oid:0.9.2342.19200300.100.1.1	ユーザーの一意の識別情報。
SwissEP_UniqueID urn:mace:switch.ch:attribute-def:swissEduPersonUniqueID urn:oid:2.16.756.1.2.5.1.1.1	ユーザーの一意の識別情報(SWITCHaai)。
eduPersonPrincipalName urn:mace:dir:attribute-def:eduPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6	ユーザーの一意の識別情報。他の一意のIDと合わせて使用できます。その場合はeduPersonPrincipalNameがユーザー名になり、他のIDがユーザー認証におけるメンバー識別情報として取得されます。
eduPersonScopedAffiliation urn:mace:dir:attribute-def:eduPersonScopedAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9	ユーザー グループ メンバーシップを介してユーザーに資格を付与します。属性値はユーザー グループに次のようにマップされます。 **重要：**この属性および利用できる規定値は、学術機関が使用するためのものです。企業組織は、別のパラメーターを使用してユーザーの利用資格を示す必要がある場合があります。詳細は、サイト管理者までお問い合わせください。 student-> 学生 faculty-> 教員 staff-> 職員
eduPersonAffiliation urn:mace:dir:attribute-def:eduPersonAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.1	ユーザーに利用資格を付与します。範囲が指定された属性と同様にマップされます。

属性	説明
eduPersonPrimaryAffiliation urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.5	ユーザーに利用資格を付与します。範囲が指定された属性と同様にマップされます。
isMemberOf urn:mace:dir:attribute-def:isMemberOf urn:oid:1.3.6.1.4.1.5923.1.5.1.1	カスタム ユーザー グループまたは組織のマッピングに使用します。複数の値を指定する場合は、区切り文字としてコンマまたはセミコロンを使用します。例えば値は、 *urn:mace:example.edu:groups:groupCode.*のように修飾できます。修飾された値の最後の部分は、システム コードとの一致を確認する場合に使用されます。 ユーザー グループの値はELMS 管理ポータルの[ユーザー]>>[ユーザーグループ]セクションにある、[ユーザーグループのコード]フィールドに対して一致する値が確認されます。一致した場合、ユーザーは一致するグループの会員権が付与されます。 組織の場合は、Webストア組織またはその関連組織の外部組織コード（一旦Kivutoにご提供いただいた後は、ELMS管理ポータルの「組織」のページでご覧いただけます）と照合されます。一致が確認されると、ユーザー認証が作成され、所属するユーザーグループを通じて組織にリンクされます。これらは、ユーザーが特定の学部のメンバーである場合に使用することができます。 **注意：**学部別Webストアを有する組織は、外部組織コードと一致する組織マッピングに使用される属性に合致しなければなりません。

属性	説明
eduPersonEntitlement urn:mace:dir:attribute-def:eduPersonEntitlement SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.7	カスタム ユーザー グループまたは組織のマッピングに使用します。値のマッピングの詳細については、**isMemberOf** を参照してください。URIの値は、URN または URL です。 あらゆる有効なUrn を使うことができます(例：urn:mace:school.edu:exampleResource)URN全部の値（urn:mace:school.edu:exampleResource）と、ネームスペース特有の文字列の一部（exampleResource）の両方とも、グループおよび組織マッピングと照合されます。 **http://[SP]/資格/[IdP]/[コード】**形式のURLのみ使用できます。パラメーターはURL形式ですが、これはWEbサイトを指しているということではありません。値の一部([コード]）は、グループおよび組織のマッピングと照合されます。 **注意:**学部別Webストアを有する組織は、外部組織コードと一致する組織マッピングに使用される属性に合致しなければなりません。
ou urn:mace:dir:attribute-def:ou urn: oid:2.5.4.11	組織のマッピングに使用されます。複数の値を指定する場合は、区切り文字としてコンマまたはセミコロンを使用します。 値は、外部組織のコード（一旦 Kivuto にご提供いただいた後は、ELMS管理ポータルの[組織] ページでご覧いただけます)と照合されます。一致が確認されると、ユーザー認証が作成され、所属するユーザーグループを通じて組織にリンクされます。これらは、ユーザーが特定の学部のメンバーである場合に使用することができます。 **注意:**学部別Webストアを有する組織は、外部組織コードと一致する組織マッピングに使用される属性に合致しなければなりません。

属性	説明
eduPersonOrgUnitDN urn:mace:dir:attribute-def:eduPersonOrgUnitDN urn:oid:1.3.6.1.4.1.5923.1.1.1.4	組織のマッピングに使用されます。ユーザーの組織単位を表すディレクトリ エントリの識別名。複数の値を指定する場合は、区切り文字としてパイプ（"|"）文字を使用します。 値は、DN形式で指定します。例：*"ou = Potions、o = Hogwarts、dc = hsww, dc wiz ="*. この例では、 *Potions*は解析された値であり、外部の組織コード フィールドに対して一致が確認されます （ouを参照してください）。 **注意:**学部別Webストアを有する組織は、外部組織のコードと一致する組織のマッピングに使用される属性に合致しなければなりません。
Surname urn: mace:dir:attribute-def:sn urn: oid:2.5.4.4	ユーザーの姓。
givenName urn: mace:dir:attribute-def:givenName urn: oid:2.5.4.42	ユーザーの名。
mail urn: mace:dir:attribute-def:mail urn: oid:0.9.2342.19200300.100.1.3	ユーザーの電子メール アドレス。
homeOrganization urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganization urn:oid:2.16.756.1.2.5.1.1.4	ユーザーが所属している組織(SWITCHaai)。
homeOrganizationType urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganizationType urn:oid:2.16.756.1.2.5.1.1.5	ユーザーが所属する組織の種類です。ユーザーが教育機関向けの利用資格を得るには、値”university”または”uas”が必要です（SWITCHaai)。

ELMS Webストアでの Shibbolethの設定

このセクションは、次の内容で構成されています。

重要：このセクションで説明されている内容は、アカウント登録済みの有効なELMS管理者によって、以下の管理者ポータルにサインイン中に実行されなければなりません。(e5.onthehub.com) サインインするには組織のアカウント番号、有効なユーザー名、およびパスワードが必要です。

WEBストアの認証タイプとして SHIBBOLETH を設定

お客様のELMS Webストアと連携するShibbolethを設定する前に、Shibbolethを認証タイプとして定義する必要があります。

Shibboleth を認証タイプとして設定するには；

1. ELMS 管理ポータルで、Webストアをクリックします。
2. ［認証］タブをクリックすると、現在設定されている認証タイプが表示されます。“ユーザーインポート”または他の認証方法Webストア開設時にデフォルト設定されている場合があります。
3. Shibboleth以外の認証タイプの横のチェックボックスにチェックを入れ削除をクリック（または、Shibboleth認証以外の動作欄にある“非アクティブ化”、をクリック）します。クリックして、
4. **“追加”**ボタンをクリックすると、新しいウィンドウが開きます。
5. Shibboleth の横にあるチェック ボックスをクリックします。
6. **“OK”**ボタンをクリックすると、選択した認証が保存されます。

SHIBBOLETH認証の構成

Shibbolethが認証タイプとしてお客様の組織に定義されますと、次に設定が必要となります。

Shibboleth を設定するには

1. メイン メニューより、**Webストア**をクリックします。
2. ［**認証**］タブをクリックします。
3. **Shibboleth**のリンクをクリックすると、新しいウィンドウが開き、設定と診断タブが表示されます。

［詳細］タブ

このタブ上で、フィールドの既定値の変更は通常必要ありませんので、お勧めいたしません。

「セクター」と「認証の有効期限」を変更する場合はご注意ください。これらの値を変更すると実装が中断され、エンドユーザーがELMS Webストアにサインインできなくなる可能性があります。

［設定］タブ

［設定］ページでは、Kivuto が必要なお客様の情報について説明しています。**表3** の設定をご参照ください。

注意: どの設定が必要かは実装のシナリオによって決まります。どの設定がお客様の実装に必要かを決定するには、*Shibboleth実装シナリオ*をご覧ください。

表3：設定

情報	説明
証明書利用者	Kivuto が会員になっているフェデレーションのリスト(例、InCommon、SWITCHaai)。
Id プロバイダー Entity Id	フェデレーション検索サービス（WAYF）はこの設定の値を指定することでバイパスできます。Webストアが単一のIdPに固有である場合には、この値は必須です。 この値は、メタデータ内の値と正確に一致している必要があります。例えば、 "urn:mace:incommon:myorg.edu"または"https://shibboleth.myorg.edu"
IUV 管理者の電子メール アドレス	ELMSからメッセージを受信する各管理者の電子メールアドレス（または配布リスト）です。
ユーザー名の非表示	この設定をオンにすると、ユーザーの一意の識別情報がWebストアのユーザーインターフェイス内の複数個所に表示されないようになります。 これは、画面表示に適したユーザー名（GUIDなど）が、IdPから属性のセットとしてリリースされていない場合に役立ちます。
リダイレクトURLのログアウト	WebストアとSHibboleth SP（サービスプロバイダー）からサインアウトしたときにユーザーがリダイレクトされるURL。 チェック欄にチェックを入れない場合、サインアウトしたユーザーはWebストアに残り、次のようなメッセージが表示されます。 “このWebサイトからサインアウトしましたが、シングル　サインオンシステムにサインインしたままの状態です。完全にログアウトする場合は、必ずブラウザーを閉じてください。”
診断モードを有効にする	チェックボックスにチェックを入れると、すべてのサインインに対してサーバーの状態がデータとして取り込まれ、[診断]タブで最新のデータが参照できます。お客様の統合テストセクション内にある、トラブルシューティングをご覧ください。

情報	説明
利用資格の制限の範囲	チェックボックスにチェックを入れた場合、ユーザーについてのみ組織のマッピング情報 （ou、eduPersonOrgUnitDN、isMemberOf、eduPersonEntitlement）が含まれた属性が付随する利用資格属性(eduPersonScopedAffiliationなど)が処理されます。 チェックを入れない場合は、すべてのユーザーについて利用資格属性が処理されます。組織のマッピング属性が付随している場合は、一致する組織のメンバーシップがユーザーに与えられます。このデータはログイン後に一致するユーザー認証（[ユーザー] >> [ユーザー名を選択] >> 認証）で確認できます。 **注意:**このオプションは、純粋に学部別WebストアにShibbolethの設定がある場合のみ、適切な学部のユーザーへ利用資格が付与されるように選択していただく必要があります。これは、このオプションが選択される時のみ有効です。

[診断] タブ

[診断] ページには最近のサインイン試行中に取り込まれたデータが表示されます。[設定]ページを通じて診断モードが有効になっていない限り何も表示されません（表3 [設定] を参照してください)。

何が表示されるかの詳細については、「お客様の統合テスト」セクション内のトラブルシューティングをご参照ください。

統合のテスト

このセクションでは、統合が完了した後に実行していただく手順について説明します。項目は次のとおりです。

- 統合のテスト
- 管理者の役割の復元

統合のテスト

ワークフローのテスト

以下は、お客様の実装テストに必要な一般的な手順です。

1. IdP を設定します。
2. ELMS Webストアを構成します。
3. ELMS Webストアから認証プロセスを開始します。既に管理サイトにサインインしている場合は、サインアウトするか、別のブラウザーを使用する必要があります。Shibblethの認証タイプがテスト状態の場合、Webストアにアクセスする際のテスト認証方法を有効にするため、[Webストア] >> [認証]からご覧いただけるテストURLを使用する必要があります。
4. IdPの認証によって、ELMS Webストアに正しくサインインされているか確認します。
5. 次の章で説明されているように、ELMS Webストアでユーザーに対して作成されたデータを認証します。
6. 全てが正常に機能していることをご確認ください。Kivuto にご連絡いただいた場合は、パラメーターがパスされているか確認させていただきます。

検証

認証に成功しましたら、ユーザーのプロファイルを表示し、すべての利用資格グループと個人設定情報が正しく設定されているかどうか確認されることをお勧めいたします。

ELMS Webストアから

1. バナーの上にある、 **[利用アカウント/オーダー]**リンクをクリックします。
2. **[アカウントの詳細]** リンクをクリックすると、個人設定情報が表示されます。
3. **[利用アカウント/オーダー]**のページに戻り、利用資格リンクをクリックすると、アカウントが割り当てられているユーザーグループが表示されます。

ELMS管理ポータルから

1. メインメニューから、 **[ユーザー]**をクリックします。
2. ユーザー名をクリックすると詳細ページが表示されます。詳細タブには設定されたすべての個人情報が表示されます。
3. [**認証**] タブをクリックすると、アカウントが認証される度に利用資格のグループが一覧表示されます。

トラブルシューティング

認証中に問題が発生した場合、または個人設定や利用資格情報がお客様の希望するエンドユーザーと異なる場合は、[診断モードを有効にする（表3をご覧ください）]にチェックを入れると機能する場合があります。最近の試行中に取り込まれたデータは、サインインに成功したかどうかを問わず、Shibboleth 診断タブに表示されます。それぞれのサインイン試行をクリックすると、詳細ページが表示されます。

- **ユーザー**
  - ユーザー名、名前および苗字、電子メールアドレスでサインイン仕損じた場合は空欄。
- **ユーザー認証**
  - ユーザーは（ou、isMemberOf、などを介して）、一意のメンバー識別子、認証有効期限、およびユーザ グループとともに、一致するユーザー認証にマップされます。サインイン仕損じた場合は空欄。
- **Shibboleth サーバー変数**
  - Shibboleth セッションの一部であるIISサーバー変数は、サインイン試行中の間はアクティブです。あるべき属性がここに表示されない場合には、Shibboleth サーバーはサポートしていないマッピングもしくはフォーマッティングであるため、それらを破棄し

ます。Shibbolethサーバー変数のセクションで属性にマップされる内訳は、**表4**：Shibbolethサーバー変数をご覧ください。

- **その他のサーバー変数**
  - その他の IIS サーバー変数は、サインイン試行中の間はアクティブです。変数が正しく分類されなかった場合も Shibboleth セクションに表示されます。

表4：Shibboleth サーバー変数

変数名	属性名
HTTP_TARGETEDID	eduPersonTargetedID urn:oid:1.3.6.1.4.1.5923.1.1.1.10
HTTP_PERSISTENTID	urn:oasis:name:tc:SAML:2.0:nameid-format:persistent
HTTP_AFFILIATION	urn:mace：dir:attribute-def:eduPersonAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.1 urn:mace:dir:attribute-def:eduPersonScopedAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9 urn:mace：dir:attribute-def:eduPersonPrimaryAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.5
HTTP_ISMEMBEROF	urn:mace：dir:attribute-def:isMemberOf urn:oid:1.3.6.1.4.1.5923.1.5.1.1
HTTP_ACADEMICCAREER	urn:mace：dir:attribute-def:academicCareer rn:oid:1.3.6.1.4.1.5524.1.13
HTTP_PRINCIPALNAME	urn:mace：dir:attribute-def:eduPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6
HTTP_GIVENNAME	urn:mace：dir:attribute-def:givenName urn: oid:2.5.4.42
HTTP_MAIL	urn:mace：dir:attribute-def:mail urn: oid:0.9.2342.19200300.100.1.3
HTTP_SURNAME	urn:mace：dir:attribute-def:sn urn: oid:2.5.4.4

変数名	属性名
HTTP_UID	urn:mace : dir:attribute-def:uid urn: oid:0.9.2342.19200300.100.1.1 urn:mace : dir:attribute-def:employeeNumber urn: oid:2.16.840.1.113730.3.1.3
HTTP_ENTITLEMENT	urn:mace : dir:attribute-def:eduPersonEntitlement urn:oid:1.3.6.1.4.1.5923.1.1.1.7
HTTP_OU	urn:mace : dir:attribute-def:ou urn: oid:2.5.4.11
HTTP_ORGUNITDN	urn:mace : dir:attribute-def:eduPersonOrgUnitDN urn:oid:1.3.6.1.4.1.5923.1.1.1.4
HTTP_UNIQUEID	urn:mace:switch.ch:attribute-def:swissEduPersonUniqueID urn:oid:2.16.756.1.2.5.1.1.1
HTTP_HOMEORGANIZATION	urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganization urn:oid:2.16.756.1.2.5.1.1.4
HTTP_HOMEORGANIZATIONTYPE	urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganizationType urn:oid:2.16.756.1.2.5.1.1.5
HTTP_STUDYBRANCH1	urn:mace:switch.ch:attribute-def:swissEduPersonStudyBranch1 urn:oid:2.16.756.1.2.5.1.1.6
HTTP_STUDYBRANCH2	urn:mace:switch.ch:attribute-def:swissEduPersonStudyBranch2 urn:oid:2.16.756.1.2.5.1.1.7
HTTP_STUDYBRANCH3	urn:mace:switch.ch:attribute-def:swissEduPersonStudyBranch3 urn:oid:2.16.756.1.2.5.1.1.8
HTTP_STUDYLEVEL	urn:mace:switch.ch:attribute-def:swissEduPersonStudyLevel urn:oid:2.16.756.1.2.5.1.1.9

管理者権限の復元

Shibboleth （シボレス）の実装によって、各ユーザーごとに新規アカウントが作成されます。新しいユーザー名が以前のユーザー名と一致しない場合、管理者権限は以前のアカウントから新しいアカウン

トへは付与されません。このため、お客様のWebストア管理者は、新しいShibbolethアカウントでサインインすると、ELMS管理サイトにアクセスできない場合があります。

これまでどおり管理者権限の付与をご希望の場合は、2つのオプションがあります。

1. Kivuto のサポート チームにご連絡いただき、以前のアカウントに関連付けられている管理者権限を新しいアカウントに付与する旨ご要請ください。

   注意: 要請されている権限に応じて、その要請はお客様のWebストアの主要な管理者からのものでなければなりません（すなわち、お客様の組織のサブスクリプションはその方のお名前のもとでご契約いただいています）。

1. Shibboleth を介してではなく、引き続き従来のアカウント認証方法を使ってサインインする場合、下記の管理者サインインポータルからアクセスできます。e5.onthehub.com/admin

Shibboleth実装シナリオ

お客様の組織（教育機関、団体)、Webストア、およびソフトウェア配布契約書の性質によって、**表2**で説明されている属性のどれがKivutoに必要か、また**表3**で説明されているどの設定がShibboleth認証を正常に実装するために構成しなければならないかが決まります。

このセクションでは、最も一般的な Shibboleth 実装シナリオについて説明し、それぞれの一意の実装要件を要約しています。

- シナリオ 1:単一のフェデレーション メンバーを対象とする組織のELMS Webストア
- シナリオ 2:単一のフェデレーション メンバーを対象とする学部別のELMS Webストア
- シナリオ 3:単一のフェデレーションメンバーを対象とする統合されたELMS Webストア
- シナリオ 4:フェデレーションのすべてのメンバーを対象とするELMS Webストア

シナリオ 1:単一のフェデレーション メンバーを対象とする組織のELMS WEBストア

このシナリオではELMS Webストアは組織全体の契約に基づき単一の フェデレーション メンバー（組織）を対象として開設されています。組織が直接ユーザー探索サービス（WAYF）を使用して、組織を選択することなくフェデレーションに統合されます。

シナリオ 1 の実装の要件は次のとおりです。表示されたそれぞれの属性と設定の説明、ならびにオプションの追加的な属性/設定については、**表2** および **表3**をご覧ください。

属性の要件:

ユーザーの一意の識別子の例

- eduPersonTargetedID
- PersistentID
- UID
- eduPersonPrincipalName

利用資格（ユーザー グループ)ユーザーのための識別子の例

- eduPersonScopedAffiliation
- eduPersonAffiliation

ELMS設定要件:

ELMS Webストア認証設定ページにおいて、

- **証明書利用者**のドロップダウンリストから、お客様のフェデレーションを選択してください。
- **IDプロバイダーのEntityID欄**にお客様の検索サービスプロバイダーを特定してください。
- IUV 管理者の電子メール アドレスを提供して下さい。

- eduPersonPrimaryAffiliation
- isMemberOf（カスタム ユーザー グループを対象）
- eduPersonEntitlement（カスタム ユーザー グループを対象）

シナリオ 2:単一のフェデレーションメンバーを対象とする学部別のELMS WEBストア

このシナリオではELMS Webストアは特定の学部契約に基づき、単一のフェデレーション メンバーを対象として開設されています。

重要: このシナリオでは、資格を有する学部のメンバーのみアクセス可能となるよう、学部の外部組織コードと一致するパラメーターが必要となります。

シナリオ2の実装の要件は次のとおりです。表示されたそれぞれの属性と設定の説明、ならびにオプションの追加的な属性/設定については、**表2**と**表3**をご覧ください。

属性の要件:

ユーザーの一意の識別子の例

- eduPersonTargetedID
- PersistentID
- UID
- eduPersonPrincipalName

利用資格（ユーザー グループ）ユーザーのための識別子の例

- eduPersonScopedAffiliation
- eduPersonAffiliation
- eduPersonPrimaryAffiliation
- isMemberOf（カスタム ユーザー グループ対象）
- eduPersonEntitlement（カスタム ユーザー グループ対象）

組織（学部）の識別子は、適切な外部組織コードと一致するように設定します。識別子の例は以下の通りです。

- isMemberOf
- eduPersonOrgUnitDN
- ou

ELMS設定要件:

ELMS Webストア認証設定ページより、

- **証明書利用者**のドロップダウンリストから、お客様のフェデレーションを選択してください。。
- **Id プロバイダーのEntityId欄に**お客様の検索サービスプロバイダーを特定してください。
- IUV 管理者の電子メール アドレスを提供して下さい。
- **利用資格の範囲の制限**にチェックマークを入れることで 、適切な学部のみに制限されます（注意：このオプションはこのシナリオのみ適用されます）。

シナリオ 3:1 つに統合されたELMS WEBストア

このシナリオでは、統合された(つまり、教育機関全体と学部の異なる契約では、特定の学部に所属するユーザーはすべての製品にアクセスする資格がある一方、該当学部に所属していないユーザーは、アクセス可能な製品が限られています。)一つの組織としてサイトが開設されています。

シナリオ 3 の実装の要件は次のとおりです。表示されたそれぞれの属性と設定の説明、ならびにオプションの追加的な属性/設定については、**表2**および**表3**をご覧ください。

属性の要件:

ユーザーの一意の識別子の例

- eduPersonTargetedID
- PersistentID
- UID
- eduPersonPrincipalName

利用資格（ユーザー グループ）ユーザーのための識別子の例

- eduPersonScopedAffiliation
- eduPersonAffiliation
- eduPersonPrimaryAffiliation
- isMemberOf（カスタム ユーザー グループ対象）
- eduPersonEntitlement（カスタム ユーザー グループ対象）

組織 （学部） の識別子は、適切な外部組織コードと一致するように設定します。識別子の例は以下の通りです。

- isMemberOf
- eduPersonOrgUnitDN
- ou

ELMS設定要件:

ELMS Webストア認証設定ページより、

- **証明書利用者**のドロップダウンリストから、お客様のフェデレーションを選択してください。
- **Id プロバイダーEntityId**欄にお客様の検索サービスプロバイダーを特定してください。
- IUV 管理者の電子メール アドレスを提供して下さい。

＊＊注意：学部の外部組織コードに一致する値がパスされない場合でも、ユーザー はサインインすることができますが、組織のプログラムによって提供される製品のみアクセス可能です。

シナリオ 4:フェデレーションのすべてのメンバーを対象とするELMS WEBストア

このシナリオは、フェデレーションの全てのメンバーを対象とするELMS Webストア開設に関係します。

サインイン中、Webストアはユーザーに対して所属する組織を選択する検索サービス(WAYF)へと導きます。

シナリオ 4 の実装の要件は次のとおりです。表示されたそれぞれの属性と設定の説明、ならびにオプションの追加的な属性/設定については、**表2**ならびに**表3**をご覧ください。

属性の要件:

ユーザーの一意の識別子の例

- eduPersonTargetedID
- PersistentID
- UID
- eduPersonPrincipalName

利用資格（ユーザー グループ）ユーザーのための識別子の例

- eduPersonScopedAffiliation
- eduPersonAffiliation
- eduPersonPrimaryAffiliation
- isMemberOf（カスタム ユーザー グループ対象）
- eduPersonEntitlement（カスタム ユーザー グループ対象）

ELMS設定要件:

ELMS Webストア認証設定ページより、

- **証明書利用者**のドロップダウンリストから、お客様のフェデレーションを選択してください。
- **Id プロバイダーEntityId**欄にお客様の検索サービスプロバイダーを特定してください。
- IUV 管理者の電子メール アドレスを提供して下さい。

サポート

ELMSでShibboleth設定作業に問題、またはテクニカルサポートが必要な場合は、shibboleth_support@kivuto.comまで電子メールでお問い合わせください。

お問い合わせの際は、以下の項目をご記入ください。

- お客様のお名前
- ご連絡先
- ご連絡先Eメールアドレス
- ご連絡先の電話番号
- ELMS Webサイトのアカウント番号
- 問題や必要な情報の詳細