InterSystems IRIS for Health および HealthShare Health Connect のレジストリ・ガイド

Version 2023.1
2024-01-02

InterSystems Corporation　1 Memorial Drive　Cambridge MA 02142　www.intersystems.com

InterSystems IRIS for Health および HealthShare Health Connect のレジストリ・ガイド
InterSystems Version 2023.1 2024-01-02

インターシステムズ社の製品に関するサポートやご質問は、以下にお問い合わせください：

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

目次

1

サービス・レジストリの管理

サービス・レジストリでは、サービスの宛先のリストを管理します。これらは通常、システム内または外部宛先向けの SOAP サービスの URL です。

1.1 サービスの追加または変更

新しいサービスを追加したり、既存のサービスを変更したりするには、以下の操作を行います。

1. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースの名前を選択します。
3. [Health] > [**サービス・レジストリ**] をクリックします。
4. 新しいサービスを追加するには、[**サービス追加**] をクリックします。または、[**Web サービス URL の解析**] をクリックして新しい SOAP サービスを追加し、ダイアログで URL を入力して、[OK] をクリックします。URL が解析され、サービス・レジストリ・エントリの該当するフィールドに入力されます。
5. 既存のサービスを変更するには、テーブルでそのサービスの行をクリックします。テーブルの上にある [**サービス・タイプ**] ドロップダウンを使用すると、テーブルに表示されているサービスのリストがフィルタされます。
6. サービスに関する情報を入力し、[**保存**] をクリックします。設定については、次の節で説明します。

1.2 サービス・レジストリの設定

サービスのデータ入力画面には 2 つの部分があります。上部は固定されており、9 つのフィールドがあります。下部の内容は、選択した [**サービス・タイプ**] によって異なります。上部の設定について以下で説明します。特定のサービス・タイプに関する設定については、この後の各項で説明します。

サービス・レジストリのデータ入力画面の上部セクションには、以下のフィールドが表示されます。

名前

必須項目。それぞれのサービスには一意の名前が必要です。

タイムアウト

オプションで、サービスがタイムアウトになるまでの秒数を入力します。

デバイス

オプションで、OID レジストリ内のコードを入力して、このエントリをデバイス OID に関連付けます。

ホーム・コミュニティ

オプションで、OID レジストリ内のコードを入力して、このエントリをホーム・コミュニティ OID に関連付けます (XCA の場合)。

割り当て機関

オプションで、OID レジストリ内のコードを入力して、このエントリを割り当て機関 OID に関連付けます。

リポジトリ

オプションで、OID レジストリ内のコードを入力して、このエントリをリポジトリ OID に関連付けます。

デバイス関数

サービス・レジストリ・エントリの中には、特定のデバイスの関数を実行するものがあります。使用可能なエントリは、FHIR インストーラの実行時にインストールしたコンポーネントによって異なります。標準のエントリは以下のとおりです。

- `XCA.Query` ― 前述のようにホーム・コミュニティ OID を指定する必要があります。指定したホーム・コミュニティ内で XCA クエリ・トランザクションを転送する宛先の URL を識別します。
- `XCA.Retrieve` ― 前述のようにホーム・コミュニティ OID を指定する必要があります。指定したホーム・コミュニティ内で XCA 取得トランザクションを転送する宛先の URL を識別します。
- `XDSb.Query` ― XDS.b クエリの転送先となるドキュメント・レジストリを識別します。
- `XDSb.Retrieve` ― 前述のようにリポジトリ OID を指定する必要があります。そのリポジトリ OID について XDS.b 取得トランザクションを転送する宛先の URL を識別します。
- `PDQv3.Supplier` ― PDQv3 サプライヤ・サービスを識別します。

サービス・タイプ

必須項目。ドロップダウンからサービスのタイプを選択します。選択した **[サービス・タイプ]** によって、画面の下部に表示されるフィールドが制御されます。オプションは以下のとおりです。

- SOAP
- ファイル
- FTP
- HTTP
- TCP
- UDP

以下の各節では、それぞれのサービス・タイプに固有の設定について説明します。必須項目として指定されている設定はありません。それぞれのサービス・タイプについて、通信を正常に実行するために必要な数の設定を入力してください。

1.2.1 SOAP サービスの設定

SOAP サービスを選択した場合、以下のフィールドが表示されます。

ホスト

ホスト名または IP アドレスを入力します。

ポート

ポート番号を入力します。

SSL構成

この接続の認証に使用する既存の Secure Socket Layer (SSL) 構成または Transport Layer Security (TLS) 構成の名前を入力します。SSL/TLS 構成を作成するには、"TLS 構成の作成または編集" を参照してください。SSL/TLS 構成には、**[構成名]** と呼ばれるオプションが含まれています。これは、この設定で使用する文字列です。**SSL Configuration** 文字列の末尾に、垂直バー (**|**) に続けて秘密鍵パスワードを追加できます。

URL

Web サービスの URL を入力します。

プロキシ・ホスト

プロキシのホスト名を入力します (該当する場合)。

プロキシ・ポート

プロキシのポート番号を入力します (該当する場合)。

HTTPCredentialsConfig

HTTP ヘッダで使用するユーザ名とパスワードを含むプロダクション認証情報の ID を入力します。プロダクション認証情報の作成については、"プロダクションの構成" の “認証情報の定義” の節を参照してください。

SOAP バージョン

必要な SOAP バージョンを入力します。以下の値のいずれかを使用します。

- `""` – SOAP 1.1 または 1.2 の場合はこの値を使用します。
- `"1.1"` – SOAP 1.1 の場合はこの値を使用します。これが既定値です。
- `"1.2"` – SOAP 1.2 の場合はこの値を使用します。

ユーザ名トークン・プロファイル

SOAP 要求の WS-Security ヘッダで使用するユーザ名とパスワードを含むプロダクション認証情報の ID を指定します。

暗号化用 X509 トークン・プロファイル

メッセージ本文の暗号化に使用する X509 証明書のエイリアスを入力します。これらの認証情報の作成については、"Web サービスの保護" の “InterSystems IRIS 資格情報セットの作成と編集” を参照してください。

デジタル署名用 X509 トークン・プロファイル

メッセージのデジタル署名に使用する X509 証明書のエイリアスを入力します。これらの認証情報の作成については、"Web サービスの保護" の “InterSystems IRIS 資格情報セットの作成と編集” を参照してください。

MTOM

MTOMドキュメントを添付として受け取るXDS.bリポジトリの場合、このチェック・ボックスにチェックを付けます。

XUA 構成

ドロップダウンから XUA 構成を選択して、SAML クリエータと SAML プロセッサを指定します。XUA の詳細は、“XUA レジストリの管理”を参照してください。

SAML アサーションの送信

SAML トークンを SOAP 呼び出しのセキュリティ・ヘッダで送信するかどうかを制御します。

以下のような複数のオプションがあります。

- [なし] ー SAML アサーションを作成したり、要求メッセージで見つかった SAML アサーションを転送したりしません。
- [転送] ー XUA 構成で指定した SAML クリエータ・クラスを使用して、要求メッセージで見つかった SAML アサーションを転送します。SAML アサーションを作成しません。
- [作成] ー XUA 構成で指定した SAML クリエータ・クラスを使用して、要求メッセージのデータに基づいて新しい SAML アサーションを作成します。要求メッセージで見つかった SAML アサーションを転送しません。
- [作成して転送] および [転送して作成] ー XUA 構成で指定した SAML クリエータ・クラスを使用して SAML アサーションを作成し、さらに要求メッセージで見つかった SAML アサーションを転送します。セキュリティ・ヘッダに表示される順序は、選択した特定のオプションによって決まります。作成または転送に失敗すると、エラーが生成されます。
- [転送または作成] ー XUA 構成で指定した SAML クリエータ・クラスを使用して、要求メッセージで見つかった SAML アサーションを転送します。SAML アサーションが見つからなかった場合は作成します。両方の操作に失敗した場合にのみ、エラーが生成されます。

セキュリティ・クラス

SOAP メッセージで使用されるシグニチャおよび暗号化の既定のセキュリティ・コードをオーバーライドするオプションのクラス。セキュリティ・クラスは HS.Util.SOAPClient.Base を拡張し、AddSecurity() クラス・メソッドをオーバーライドする必要があります。

1.2.2 ファイル・サービスの設定

ファイル・サービスを選択した場合、以下のフィールドが表示されます。

ファイル名

ローカル・システム上のファイルの名前を入力します。

ファイル・パス

指定したファイルのディレクトリのフル・パス名を入力します。このディレクトリは存在するディレクトリであること、また、ローカル・マシンのファイル・システムからアクセス可能なディレクトリであることが必要です。

既存のファイルを上書き

既存のファイルを上書きする場合、このチェック・ボックスにチェックを付けます。チェックを付けなかった場合は、新しいデータが既存のファイルに追加されます。

1.2.3 FTP サービスの設定

FTP サービスを選択した場合、以下のフィールドが表示されます。

ファイル名

FTP サーバ上の書き込み先のファイルの名前を入力します。

ファイル・パス

指定したファイルの FTP サーバ上のディレクトリのフル・パス名を入力します。このディレクトリは存在するディレクトリであること、また、指定された認証情報を使用してアクセス可能なディレクトリであることが必要です。

既存のファイルを上書き

既存のファイルを上書きする場合、このチェック・ボックスにチェックを付けます。チェックを付けなかった場合は、新しいデータが既存のファイルに追加されます。

ホスト

FTP サーバの IP アドレスまたはサーバ名を入力します。

ポート

FTP サーバで使用する TCP ポート番号を入力します。既定値は 21 です。

ユーザ認証情報構成

FTP サーバへの接続を承認できるプロダクション認証情報を入力します。プロダクション認証情報の作成については、"プロダクションの構成" の “認証情報の定義” の節を参照してください。

パッシブを使用

パッシブ FTP モードを使用する場合、このチェック・ボックスにチェックを付けます。このモードでは、サーバがデータ・ポート・アドレスを返し、クライアントがそれに接続します。制御 TCP 接続とデータ TCP 接続の両方がクライアントから開始されるため、ほとんどのファイアウォールでパッシブ・モード FTP を受け入れやすくなります。

1.2.4 HTTP サービスの設定

HTTP サービスを選択した場合、以下のフィールドが表示されます。

ホスト

サーバの IP アドレスまたはホスト名を入力します。

ポート

サーバの TCP ポートを入力します。既定値は 80 です (**SSL Configuration** を指定した場合は 443 です)。

SSL構成

この接続の認証に使用する既存の Secure Socket Layer (SSL) 構成または Transport Layer Security (TLS) 構成の名前を入力します。SSL/TLS 構成を作成するには、"TLS 構成の作成または編集" を参照してください。SSL/TLS 構成には、**[構成名]** と呼ばれるオプションが含まれています。これは、この設定で使用する文字列です。**SSL Configuration** 文字列の末尾に、垂直バー (|) に続けて秘密鍵パスワードを追加できます。

URL

URL パスを入力します (http:// やサーバ・アドレスは含めません)。

プロキシ・ホスト

プロキシ・サーバの IP アドレスまたはホスト名を入力します (該当する場合)。

プロキシ・ポート

プロキシのポート番号を入力します (該当する場合)。既定値は 8080 です。

HTTPCredentialsConfig

指定された宛先 URL への接続を承認できるプロダクション認証情報の ID を入力します。プロダクション認証情報の作成については、"プロダクションの構成" の “認証情報の定義” の節を参照してください。

HTTPSプロキシ

クライアントでこの設定を使用している場合は、この値がクライアントのものと同じであることを確認します。

プロキシ・トンネル

クライアントでこの設定を使用している場合は、この値がクライアントのものと同じであることを確認します。

HTTPS プロキシ SSL 接続

クライアントでこの設定を使用している場合は、この値がクライアントのものと同じであることを確認します。

1.2.5 TCP サービスの設定

TCP サービスを選択した場合、以下のフィールドが表示されます。

ホスト

TCP 接続先となる IP アドレスを入力します。アドレスが ! 文字で始まる場合、アダプタはリモート・システムからの接続を待機します。! 文字の後に IP アドレスが指定されていない場合、任意のリモート・システムが接続できます。それ以外の場合は、リストされている IP アドレス (およびポート) のみが接続を許可されます。

ポート

接続先の TCP ポートを入力します。TCP ポート番号の最大値は 65535 です。

SSL構成

この接続の認証に使用する既存の Secure Socket Layer (SSL) 構成または Transport Layer Security (TLS) 構成の名前を入力します。SSL/TLS 構成を作成するには、"TLS 構成の作成または編集" を参照してください。SSL/TLS 構成には、**[構成名]** と呼ばれるオプションが含まれています。これは、この設定で使用する文字列です。**SSL Configuration** 文字列の末尾に、垂直バー (|) に続けて秘密鍵パスワードを追加できます。

接続を維持

- 操作の完了後、ここで指定した秒数だけリモート・システムとの接続を維持する場合は、正の値に設定します。
- 操作が完了するたびに直ちに切断する場合は、ゼロに設定します。
- アイドル・タイムでも常時接続を維持する場合は、-1 (既定値) に設定します。

1.2.6 UDP サービスの設定

UDP サービスを選択した場合、以下のフィールドが表示されます。

ホスト

UDP 接続先となる IP アドレスを入力します。

ポート

接続先の UDP ポートを入力します。

UDP センダ・コマンド

目的の UDP センダ・コマンドを入力します。

1.3 サービスの削除

既存のサービスを削除するには、以下の操作を行います。

1. 管理ポータルを開きます。
2. Foundation ネームスペースの名前を選択します。
3. **[サービス・レジストリ]** をクリックします。
4. テーブルでそのサービスの行をクリックします。テーブルの上にある **[サービス・タイプ]** ドロップダウンを使用すると、テーブルに表示されているサービスのリストがフィルタされます。
5. 画面の下部にある **[削除]** をクリックします。
6. 確認ダイアログ・ボックスで [OK] をクリックします。

2

OID レジストリの管理

OID レジストリでは、オブジェクト識別子 (OID) のリストを管理します。OID は、グローバルに一意な ISO 識別子です。インターシステムズ製品で使用される OID は、数字とドットで構成されます (例 : 1.3.6.1.4.1.21367.2010.1.2)。OID ではツリー構造が使用され、一番左の数字はルートを表し、一番右の数字はリーフを表します。

OID を使用して、以下のものを識別することができます。

- 施設
- ゲートウェイ
- 割り当て機関
- デバイス
- ホーム・コミュニティ
- コード体系
- リポジトリ

HL7 などの登録機関から組織のルート OID を取得できます。インストールしたインターシステムズ製品について OID を取得するには、HL7.org の Web サイト (http://www.hl7.org/oid/index.cfm) にアクセスし、“Click to Obtain or Register an OID” のリンクをクリックします。

ルート OID を取得したら、独自のネームスペース・サブツリーを設計できます。ISC では、このサブツリーをどのようにマップするかについて計画を練ることを推奨しています。DICOM 規格との互換性を確保するために、OID が 64 文字を超えないようにしてください。

2.1 OID の追加または変更

新しい OID レジストリ・エントリを追加したり、既存のものを変更したりするには、以下の操作を行います。

1. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースの名前を選択します。
3. **[Health]** > **[IHE 構成]** > **[OID レジストリ]** を選択します。
4. 新しい OID を追加するには、**[OID の追加]** をクリックします。既存の OID を変更するには、テーブルでその OID の行をクリックします。テーブルの上にある **[識別タイプ]** ドロップダウンを使用すると、テーブルに表示されている OID のリストがフィルタされます。
5. OID に関する情報を入力し、**[保存]** をクリックします。設定については、次の節で説明します。

6. SDA-FHIR 変換を使用する実行中のプロダクションの OID 設定を変更する場合は、`HS.FHIR.DTL.Util.HC.SDA3.FHIR.Process` ビジネス・プロセスおよび/または `HS.FHIR.DTL.Util.HC.FHIR.SDA3.Process` ビジネス・プロセスを再起動する必要があります。

2.2 OID レジストリの設定

OID レジストリでは以下の設定を入力します。

コード

必須項目。OID の識別コードを入力します。OID のタイプが異なっていれば、2 つ以上のエントリで同じ識別コードを使用できます。例えば、割り当て機関とホーム・コミュニティは OID を共有し、同じコードを使用できます。

OID

必須：OID 値。

エイリアス

オプション：この OID または URL にマップするコードが複数ある場合、それらをここに入力します。

URL

必須：指定されたコードのネームスペース URL。

説明

オプションで、OID エントリの説明を入力します。

タイプ

ドロップダウンから OID のタイプを 1 つまたは複数選択します。オプションは以下のとおりです。

- 施設
- ゲートウェイ
- 割り当て機関
- デバイス
- ホーム・コミュニティ
- コード体系
- リポジトリ

2.3 OID の削除

既存の OID レジストリ・エントリを削除するには、以下の操作を行います。

1. 管理ポータルに **`%HS_Administrator`** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースの名前を選択します。

3. [Health] > [IHE 構成] > [OID レジストリ] を選択します。
4. [OID の追加/編集] をクリックします。
5. テーブルでその OID エントリの行をクリックします。テーブルの上にある [識別タイプ] ドロップダウンを使用すると、テーブルに表示されている OID のリストがフィルタされます。
6. 画面の下部にある [削除] をクリックします。
7. 確認ダイアログ・ボックスで [OK] をクリックします。

2.4 ファイルからの OID のインポート

ファイルから OID レジストリに OID をインポートできます。

1. [OID レジストリ・インポート] ページに移動します。
   a. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
   b. Foundation ネームスペースの名前を選択します。
   c. [Health] > [IHE 構成] > [OID レジストリ] を選択します。
   d. [OID のインポート] をクリックします。
2. [ファイルの選択] をクリックして、インポート・ファイルの場所を指定します。インポート・ファイルには、次の例のように、1 つまたは複数の <OIDMap> エントリが XML 形式で含まれている必要があります。

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
     <OIDMap>
          <OID>2.16.840.1.113883.6.22</OID>
          <IdentityCode>XYZ81</IdentityCode>
          <IdentityTypes>
               <OIDType>
                    <Description>CodeSystem</Description>
               </OIDType>
          </IdentityTypes>
          <Description>My Test Code System</Description>
          <Types>CodeSystem</Types>
     </OIDMap>
     <OIDMap>
          <OID>1.3.6.1.4.1.21367.2010.1.2.300.2.44</OID>
          <IdentityCode>ABC123</IdentityCode>
          <IdentityTypes>
               <OIDType>
                    <Description>AssigningAuthority</Description>
               </OIDType>
               <OIDType>
                    <Description>Facility</Description>
               </OIDType>
               <OIDType>
                    <Description>Organization</Description>
               </OIDType>
          </IdentityTypes>
          <Description>My Test Assigning Authority</Description>
          <Types>AssigningAuthority,Facility,Organization</Types>
     </OIDMap>
</root>
```

注釈　XML ファイルでは、以下の点に注意してください。

- `<Description>` 要素 (`<OIDType><Description>` 要素ではありません) はオプションです。
- OID タイプは 2 回指定します。
  - 個々の `<OIDType>` 要素の `<Description>` でそれぞれ 1 回ずつタイプを指定します。
  - その後、`<Types>` 要素でコンマ区切りリストとしてまとめて指定します。

2.5 ファイルへの OID のエクスポート

OID レジストリまたはその一部をファイルにエクスポートできます。

1. **[OID レジストリ・エクスポート]** ページに移動します。
   a. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
   b. Foundation ネームスペースの名前を選択します。
   c. **[Health]** > **[IHE 構成]** > **[OID レジストリ]** を選択します。
   d. **[OID のエクスポート]** をクリックします。
2. **[エクスポート先の選択]** をクリックして、エクスポート・ファイルの場所を指定します。既定のファイル名は OIDRegistryExport_YYYY-MM-DD.xml です (例 : OIDRegistryExport_2015-10-01.xml)。
3. OID テーブルでエクスポートする行を選択して **[選択項目をエクスポート]** をクリックするか、**[すべてエクスポート]** をクリックします。

エクスポート・ファイルは、前の節で示したような XML 形式になります。

3

識別子の割り当て機関の管理

インターシステムズでは、さまざまなタイプの患者識別子や臨床医識別子をサポートしています。ほとんどの識別子は、特定の割り当て機関に関連付けられています。例えば、米国の運転免許証番号は州に関連付けられています。パスポート番号は国に関連付けられています。

インターシステムズ製品は、割り当て機関レジストリを保持しています。レジストリ内のエントリは、識別子タイプによって分類されています。既定の識別子タイプは以下のとおりです。

- 企業 ID
- 運転免許証
- 医師番号
- 保険 ID
- 医療レコード番号
- PIX 識別子

3.1 割り当て機関レジストリへのアクセス

割り当て機関を定義する場合、既存の割り当て機関の詳細を変更する場合、または割り当て機関を削除する場合は、**[割り当て機関レジストリ]** を使用します。このページにアクセスするには、以下の操作を行います。

1. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースを選択します。
3. [Health] > **[割り当て機関レジストリ]** をクリックします。

3.2 割り当て機関の追加または変更

割り当て機関を追加したり、その詳細を変更したりするには、以下の操作を行います。

1. 編集する割り当て機関の識別子タイプをドロップダウン・リストから選択します。
2. テーブルで、既存の割り当て機関の行をクリックするか、**[割り当て機関の追加]** をクリックして新しいエントリを作成します。

3. 割り当て機関の名前とコードを入力します。
4. オプションで、特定の個人についてこのタイプの複数の識別子を許可する場合、**[複数を許可]** チェック・ボックスにチェックを付けます (現時点では、この機能は実装されていません)。
5. QuadraMed MPI を使用している場合、QuadraMed がこの割り当て機関に対して指定したコードを **[その他の ID]** フィールドに入力します。QuadraMed を使用していない場合、このフィールドは空白のままにすることができます。
6. **[割り当て機関を保存]** をクリックして、変更内容を保存します。

3.3 割り当て機関の削除

割り当て機関を削除するには、以下の操作を行います。

1. 削除する割り当て機関の識別子タイプをドロップダウン・リストから選択します。
2. 既存の割り当て機関の行で **[削除]** をクリックします。
3. [OK] をクリックして操作を確定します。

4

構成レジストリの管理

構成レジストリは、キー/値ペアのデータベースです。ここには、カスタム Web ページ、カスタム関数、および特定の事前定義値の詳細を登録できます。

構成レジストリにアクセスするには、以下の操作を行います。

1. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースを選択します。
3. [Health] > **[構成レジストリ]** をクリックします。
4. 新しいキーを作成する場合は、**[値の追加]** ボタンをクリックします。既存のキーを変更する場合は、テーブルでそのキーを選択します。
5. 該当するフィールドにキーとその値を入力し、**[保存]** をクリックします。

構成レジストリのキー・カテゴリは以下のとおりです。

- ¥HomeCommunity ー ホーム・コミュニティの連絡先情報の詳細
- ¥IHE ー IHE 通信に必要な詳細
- ¥LegalAuthenticator ー エクスポートされた内容について法的責任を負う個人の詳細
- ¥UI ー 管理ポータルから呼び出されるカスタム Web ページの構成の詳細

これらのカテゴリについて、この後の各節で詳しく説明します。

4.1 ホーム・コミュニティ・キー

以下の `\HomeCommunity` キーを使用して、IHE ホーム・コミュニティの連絡先の詳細を格納します。

- `\HomeCommunity\Address\StreetLine1`
- `\HomeCommunity\Address\StreetLine2`
- `\HomeCommunity\Address\City`
- `\HomeCommunity\Address\State`
- `\HomeCommunity\Address\Zip`
- `\HomeCommunity\Address\Country`

- \HomeCommunity\Telecom\Workphone

4.2 IHE キー

\IHE キーを使用して、IHE 機能のさまざまな側面を制御します。

\IHE\HomeCommunity

ホーム・コミュニティの OID を指定するには、このキーを使用します。ホーム・コミュニティは、1 つの XDS ドキュメント・レジストリを持つエンティティです。このキーの値には、OID 値を使用することも、OID レジストリで指定された OID の IdentityCode を使用することもできます。例えば、AssigningAuthority タイプの OID と HomeCommunity タイプの OID の両方である“HomeCommunity”という OID があるとします。その場合は、このキーの値として HomeCommunity を入力します。

\IHE\AffinityDomain

アフィニティ・ドメインによって、1 つまたは複数のホーム・コミュニティに一意の MPI ID が割り当てられます。IHE アフィニティ・ドメイン割り当て機関の OID を指定するには、このキーを使用します。これには、OID 値を使用することも、OID レジストリで指定された OID のコードを使用することもできます。多くの場合、これは、\IHE\HomeCommunity の OID と同じ OID です。

\IHE\XDSb\Repository RepositoryName**\Retrieve\MTOMRequired**

RepositoryName という XDS.b リポジトリで MTOM 添付がサポートされていない場合、このキーをゼロに設定します。

4.3 法的認証者キー

以下の \LegalAuthenticator キーを使用して、エクスポートされた内容について法的責任を負う組織内の個人の連絡先の詳細と ID を格納します。

- \LegalAuthenticator\Name\Given
- \LegalAuthenticator\Name\Family
- \LegalAuthenticator\Address\StreetLine1
- \LegalAuthenticator\Address\StreetLine2
- \LegalAuthenticator\Address\City
- \LegalAuthenticator\Address\State
- \LegalAuthenticator\Address\Zip
- \LegalAuthenticator\Address\Country
- \LegalAuthenticator\Telecom\Workphone

4.4 UI キー

\UI キーでは、サイトにおいてカスタマイズされたユーザ・インタフェース・ページを指定します。$$$HSUILink マクロのいずれかによって呼び出されるページを含め、ユーザ・インタフェースの Zen ページのほとんどをカスタマイズできます。カスタム・ユーザ・インタフェース・ページは通常、標準の UI ページを拡張し、1 つまたは複数の XDATA ブロックを置き換えたものです。標準の UI ページを独自のページに置き換えるには、\UI\[subpackage \]...\class という形式のキーを使用して、置き換えるページを指定し、値をカスタム・ページの完全なクラス名に設定します。.cls 拡張子も含めてください。以下に例を示します。

クラス HS.UI.Logout.cls を置き換えるには、キー \UI\Logout と Custom.Logout.cls のような値を使用します。

注釈　カスタム・ページを追加した後、新しいページを表示するには、一度ログアウトしてから、改めてログインする必要があります。

4.4.1 アプリケーション・クラス

クラス HS.UI.Application では、すべての UI ページで使用されるスタイルとバナーを指定します。システム全体でスタイルやバナーをカスタマイズするには、HS.UI.Application.cls を拡張します。Style XDATA ブロックをオーバーライドしてスタイルシートをカスタマイズしたり、DrawTitle() メソッドをオーバーライドしてページ・ヘッダをカスタマイズしたりすることができます。

カスタム・アプリケーション・ページを登録するには、キー \UI\Application を使用します。

個々のページで、Style XDATA ブロックや DrawTitle() メソッドをページごとにオーバーライドすることもできます。

5
XUA レジストリの管理

Cross-Enterprise User Assertion (XUA) は、企業の境界を越えたユーザ認証をサポートし、SAML 2.0 ID アサーションを使用して、認証された ID に関するクレームを検証する IHE プロファイルです。SAML トークンは、SOAP 呼び出しのセキュリティ・ヘッダで送信されます。

XUA レジストリを使用して送信 SAML アサーションの作成を有効にするには、以下の操作を行います。

1. XUA レジストリで 1 つまたは複数の XUA 構成を作成します (次の節で説明します)。
2. 適切なサービス・レジストリ・エントリで **[XUA 構成]** を選択します。

   XCA と XDS.b の場合、サービス・レジストリ・エントリは、**[デバイス関数]** が `XCA.Retrieve` または `XDSb.Retrieve` に設定されているものでなければなりません。
3. サービス・レジストリ・エントリの **[SAML アサーションの送信]** フィールドで SAML アサーションのスタイルを選択します。アサーションのさまざまなスタイルの詳細は、"サービス・レジストリの管理" の章の "SOAP サービスの設定" を参照してください。

サービス・レジストリで SAML を設定すると、さまざまな SAML アサーション・タイプをさまざまなリポジトリ (さまざまなベンダのものを含む) に送信できます。例えば、複数の XDS.b リポジトリや複数の XCA ホーム・コミュニティにドキュメントを要求する場合、すべての要求に同じコンシューマ・オペレーションを使用することができます。サービス・レジストリ・エントリごとに異なる XUA 構成を割り当てることにより、SAML クリエータを各システムに合わせてカスタマイズできます。Health Connect は、ドキュメント要求のリポジトリ OID またはホーム・コミュニティ OID を使用して、その要求で使用するサービス・レジストリ・エントリ (および XUA 構成) を特定します。

注釈　XDS.b コンシューマ・オペレーションには [SendSAMLAssertion] 設定と [SAMLCreator] 設定が含まれていますが、サービス・レジストリの XUA 構成と設定を優先して非推奨になっています。サービス・レジストリの設定の方が柔軟性に優れているためです。

受信 SAML アサーションの処理を有効にするには、アサーションで見つかった組織 OID または URL を使用して送信組織を特定する XUA 構成を作成します。

5.1 XUA 構成の作成または編集

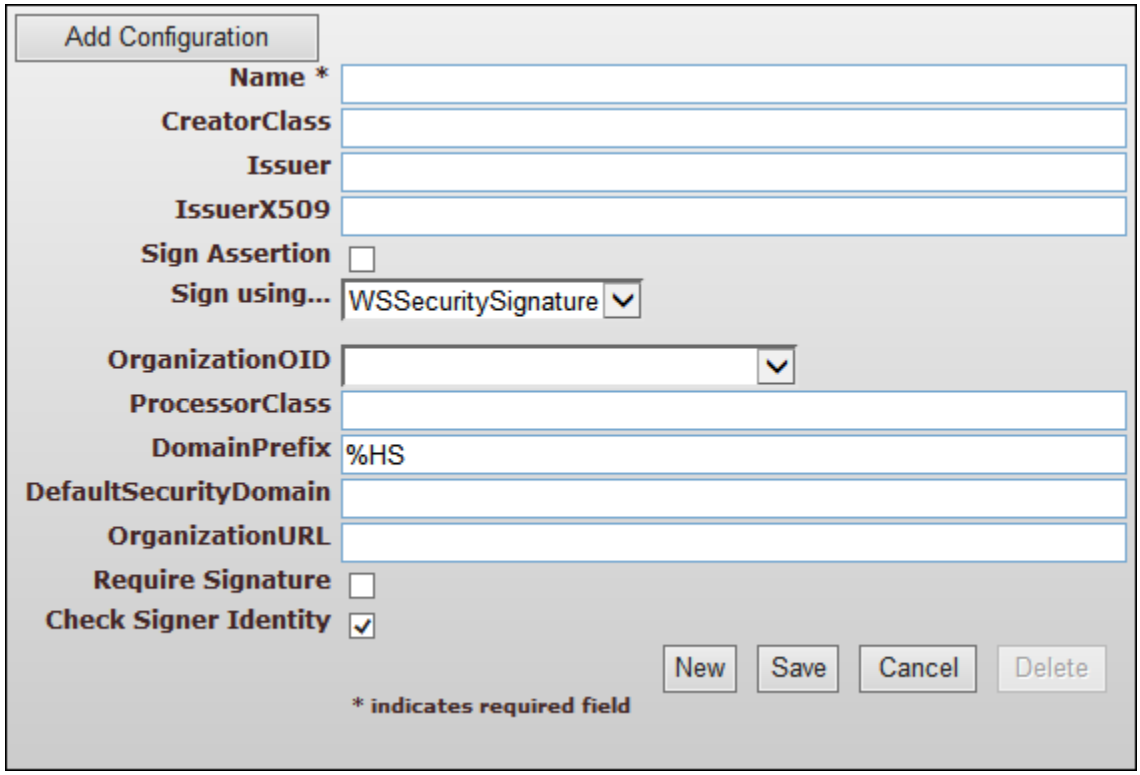
XUA 構成では、送信 SAML アサーションを作成する方法と受信 SAML アサーションを処理する方法を定義します。XUA 構成を作成または編集するには、以下の操作を行います。

1. 管理ポータルに **`%HS_Administrator`** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースを選択します。

3. [Health] > [IHE 構成] > [XUA 構成レジストリ] を選択します。
4. 既存の構成を編集する場合は、テーブルから構成を選択します。新しい構成を作成する場合は、[構成の追加] を選択します。
5. 個々の設定に適切な値を入力し、[保存] を選択します。設定については、次の節で説明します。

5.1.1 XUA 構成の設定

次の画像は [XUA 構成] 画面です。



設定の最初のブロックは、送信 SAML アサーションの作成に関連しています。設定の 2 つ目のブロックは、受信 SAML アサーションの処理に関連しています。

5.1.1.1 SAML アサーションの作成に関する XUA 設定

名前

構成の名前。構成を保存するには、[名前] を指定するだけでかまいませんが、アサーションを作成または処理する場合に XUA 構成が機能するためには、その他にもいくつかの設定が必要です。

クリエータ・クラス

SAML アサーションを作成するクラスの名前。この設定は、アサーションを作成する場合に必要です。クリエータ・クラスは、HS.IHE.XUA.Creator.cls、または HS.IHE.XUA.Creator を拡張するカスタム・クラスです。クラス HS.IHE.XUA.SHINNY.Creator.cls にサンプルがあります。

[発行者] または [発行者 X509]

SAML 発行者の名前に使用する文字列。どちらか一方のプロパティを設定します。

- [発行者] – 組織の証明書の識別名を含む文字列。

- [発行者 X509] – 組織の証明書を参照する X.509 証明書のエイリアス。[アサーションに署名] にチェックを付けると、SAML トークンの署名に X.509 証明書が使用されます。

[発行者] と [発行者 X509] の両方が空の場合、新しいトークンを作成する際にエラーが報告されます。両方の値が設定されている場合は、[発行者 X509] が [発行者] より優先されます。

アサーションに署名

[発行者 X509] 設定で指定した X.509 証明書で各 SAML トークンが署名されるようにするには、ここにチェックを付けます。[アサーションに署名] にチェックを付ける場合は、[発行者 X509] の値が設定されている必要があります。

次を使用して署名

WSSecuritySignature と Signature のどちらを使用してメッセージに署名するかを指定します。Signature は、プレースホルダ WSSecuritySignature のみが存在する場合にアサーションに署名しますが、完全な WSSecuritySignature を含むメッセージに対して検証されるため、両方で署名すると、Signature の検証時に問題が発生します。既定値は `WSSecuritySignature` です。

シグニチャ検証プロセスの一環として、XUA プロセッサは、SAML 2.0 仕様のセクション 5.4.2 に基づいて、参照 URI をアサーション ID と比較することにより、アサーション全体が実際に WSSecuritySignature または Signature によって署名されていることを確認します。

5.1.1.2 受信 SAML アサーションの処理に関する XUA 設定

[組織 OID] または [組織 URL]

組織を識別する OID レジストリ・エントリのコードを [組織 OID] フィールドで選択します。オプションで、組織の URL を [組織 URL] 設定で設定します。

受信 SAML アサーションには、何らかの組織識別子が含まれている必要があります。これは、OID 形式でも URL 形式でもかまいません。インターシステムズでは、組織識別子を使用して、アサーションを処理する XUA 構成が特定されます。インターシステムズでは、組織識別子について以下の形式の属性名が認識されます。

- IHE： `urn:oasis:names:tc:xspa:1.0:subject:organization-id`
- SHIN-NY： `UserOrganizationOID`

属性について異なる名前付け規約を使用する SAML アサーションを受け取る場合は、アサーション内で組織識別子を探すカスタム・メソッドを作成し、そのメソッドを Web サービスの `OrgURLAttributeCode` に割り当てます。このメソッドは、OID 形式または URL 形式の組織識別子を返す必要があります。クラス HS.IHE.XUA.SHINNY.Processor の GetOrganizationID() にメソッドのサンプルがあります。

プロセッサ・クラス

受信 SAML アサーションを処理するクラスの名前。この設定は、アサーションを処理する場合に必要です。プロセッサ・クラスは、HS.IHE.XUA.Processor.cls、または HS.IHE.XUA.Processor を拡張するカスタム・クラスです。クラス HS.IHE.XUA.SHINNY.Processor.cls にサンプルがあります。

[ドメイン接頭語] と [既定のセキュリティ・ドメイン]

[既定のセキュリティ・ドメイン] は、既定のセキュリティ・ドメインの名前です。これはオプションです。

インターシステムズでは、SAML 属性から取得した情報をオプションの [ドメイン接頭語] と共に使用して、SAML ユーザが定義されている該当のセキュリティ・ドメインを探します。以下の値と連結された [ドメイン接頭語] の値によって識別されるドメインが以下の順序で検索されます。

1. SAML アサーションから取得した organization-id の OID レジストリ・コード

2. SAML アサーションから直接取得した organization の名前
3. SAML アサーションから取得した送信者の homeCommunityId の OID レジストリ・コード

[ドメイン接頭語] には、内部セキュリティ・ドメインに対応する“**%HS**”という値が指定されています。

該当する名前が付いたセキュリティ・ドメインが見つかると、そこでユーザが検索されます。見つからない場合は、ドメイン接頭語を含めずに、**[既定のセキュリティ・ドメイン]** の値を使用して、ユーザが検索されます。

例えば、お使いのシステムにおいて“SAML_”で始まるセキュリティ・ドメイン内にすべての SAML ユーザが指定されている場合、**[ドメイン接頭語]** フィールドに「**SAML_**」と入力します。以下の属性を持つ SAML アサーションがあるとします。

- “XYZ”という organization 属性
- OID レジストリ内の“XYZ-Organization”に解決される“1.2.3”という organization-id
- OID レジストリ内の“RHIO-A”に解決される“4.5.6”という homeCommunityID

以下の名前のドメインが以下の順序で検索されます。

1. “SAML_XYZ-Organization”
2. “SAML_XYZ”
3. “SAML_RHIO-A”

いずれのドメインも見つからなかった場合は、既定のドメイン内で検索されます。

この動作を変更できますが、そのためには、プロセッサ・クラスで GetDomain() メソッドをオーバーライドします。提供されているサンプルの **HS.IHE.XUA.SHINNY.Processor.cls** では、以下の方式が使用されます。

1. DomainPrefix_UserOrganizationOID
2. DomainPrefix_UserOrganizationName
3. DomainPrefix_UserRHIO (OID)

シグニチャが必要

受信 SAML アサーションを処理するためには X.509 証明書で署名されていることが必要な場合、ここにチェックを付けます。

署名者の ID をチェック

チェックを付けた場合 (既定)、XUA プロセッサは、シグニチャ検証の一環として受信 SAML アサーションのシグニチャの **KeyInfo** プロパティを検査します。以下の 2 つの条件を満たす場合にのみ、アサーションは検証に合格します。

- **KeyInfo** から署名者を識別できる。
- 署名者の認証情報が信頼されている。

  重要　X.509 証明書の代わりに RSA 公開鍵を使用する場合は、信頼された RSA 鍵レジストリに鍵を追加する必要があります。

チェックを付けなかった場合、RSA 公開鍵のみで署名されていたり対称暗号で署名されているアサーションは、署名者の識別を試みることなく検証に合格します。

6

信頼された RSA 鍵レジストリの管理

XUA メッセージングの受信 SAML アサーションの XML シグニチャに X.509 証明書全体を含める代わりに、RSA 公開鍵を含めることができます。受信 SAML アサーションに RSA 公開鍵を使用する場合は、信頼された RSA 鍵レジストリに鍵を追加する必要があります。

信頼された RSA 鍵レジストリに鍵を追加するには、以下の操作を行います。

1. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースを選択します。
3. [Health] > [IHE 構成] > [信頼された RSA 鍵レジストリ] を選択します。
4. 既存のエントリを編集する場合は、テーブルからエントリを選択します。新しいエントリを作成する場合は、[信頼された鍵の追加] を選択します。
5. 個々の設定に適切な値を入力し、[保存] を選択します。設定の説明は以下のとおりです。

エイリアス

必須項目。

公開鍵の法 (Base64 エンコード)

必須項目。

公開鍵の指数 (Base64 エンコード)

必須項目。

7

コード化エントリ・レジストリの管理

コード化エントリ・レジストリでは、IHE 通信に必要なコード、テンプレート、および識別子を定義します。インターシステムズ製品は、これらのコードの大規模なセットと共にインストールされます。さまざまなコード・タイプの詳細は、IHE の wiki を参照してください。

コード化エントリ・レジストリにアクセスするには、以下の操作を行います。

1. 管理ポータルに **%HS_Administrator** ロールを持つユーザとしてログインします。
2. Foundation ネームスペースを選択します。
3. [Health] > [IHE 構成] > [コード化エントリ・レジストリ] を選択します。
4. 既存のエントリを編集する場合は、テーブルからエントリを選択します。新しいエントリを作成する場合は、[コードの追加] を選択します。
5. 個々の設定に適切な値を入力し、[保存] を選択します。設定の説明は以下のとおりです。

[コード・タイプ] ドロップダウン・リストを使用して、コード・タイプに基づいてテーブルをフィルタするか、[検索] ボックスに語句を入力します。[ページサイズ] ボックスを使用して、各ページに表示されるエントリの数を調整することもできます。

各エントリには、以下の情報が含まれています。

コード・タイプ

以下のコード・タイプを使用できます。

- associationDocumentation
- classCode
- confidentialityCode
- contentTypeCode
- eventCodeList
- folderCodeList
- formatCode
- healthcareFacilityTypeCode
- practiceSettingCode
- typeCode

コード

コードの値。

スキーム

コードが準拠する標準。

説明

オプションの説明。