LADP ガイド

Version 2023.1
2024-01-02

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

LADP ガイド
InterSystems IRIS Data Platform　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

LDAP と InterSystems IRIS®

InterSystems IRIS® は、LDAP (Lightweight Directory Access Protocol) を使用した認証および承認をサポートします。LDAP システムには、InterSystems IRIS が情報を取得するユーザ情報の一元管理リポジトリがあります。例えば Windows の場合、Active Directory を使用するドメイン・コントローラが LDAP サーバになります。

以下がサポートされます。

- LDAP 認証 – InterSystems IRIS により、ユーザにユーザ名とパスワードの入力を求めるプロンプトが表示されます。インスタンスは LDAP サーバに関連付けられ、LDAP サーバは認証を実行し、ユーザのロールおよびその他の承認情報を取得します。インスタンスが LDAP サーバに接続できない場合に、キャッシュ認証情報を使用してユーザを認証するようインスタンスを構成することもできます。
- LDAP 承認 – インターシステムズは LDAP グループをサポートしており、承認の一部としてロールを指定できます。ローカルの InterSystems IRIS ターミナルでは、LDAP 承認と OS ベースの認証が併用されます (ターミナルへのアクセスは、Windows では **%Service_Console** によって、他のすべてのオペレーティング・システムでは **%Service_Terminal** によって管理されます)。

InterSystems IRIS では、同時に複数の LDAP ドメインに認証と承認を提供することもできます。

LDAP を InterSystems IRIS の代行認証機能と併用することもできます。これにより、カスタム・メカニズムを実装して、インターシステムズのセキュリティに含まれる認証とロール管理アクティビティを置き換えることができます。

InterSystems IRIS では以下に対する LDAP サポートが提供されます。

- Active Directory
- OpenLDAP
- LDAP バージョン 3 プロトコル (これより前の LDAP プロトコルはサポートされていません)

2

LDAP 認証

2.1 LDAP 認証の設定の概要

認証に LDAP サーバを使用するように InterSystems IRIS のサービスまたはアプリケーションを構成する手順は以下のとおりです。

1. LDAP サーバを使用するように InterSystems IRIS を構成します。
   a. インスタンスで LDAP および関連機能を有効化します。
   b. InterSystems IRIS のインスタンスで使用する LDAP 構成を作成します。ここで、InterSystems IRIS ユーザのプロパティの値を設定するために使用する LDAP ユーザ・プロパティの名前を指定します。
   c. オプションで、LDAP 構成をテストします。
   d. オプションで、複数の LDAP ドメインをサポートするようにインスタンスを構成します。
   e. インスタンスへのログインに必要なロールを設定します。
   f. インスタンスの関連サービスおよびアプリケーションで LDAP を有効化します。この設定では、InterSystems IRIS のインスタンス全体で LDAP を有効にして、関連するサービスやアプリケーションに対して LDAP を有効にします。

注釈　プログラムで LDAP 認証を実行するには、InterSystems IRIS の代行認証を使用します。

2.2 インスタンスでの LDAP の有効化

LDAP を使用するように InterSystems IRIS のインスタンスを構成するには、まず、使用する機能を有効にします。

1. 管理ポータルのホーム・ページで、**[認証/Web セッション・オプション]** ページ (**[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[認証/Web セッション・オプション]**) に移動します。
2. **[認証/Web セッション・オプション]** ページで、以下の手順を実行します。
   - LDAP 認証を有効にするには、**[LDAP認証を許可]** を選択します。
   - LDAP キャッシュ資格情報を使用した認証を有効にするには、**[LDAPキャッシュ credentials 認証を許可]** を選択します。このトピックの詳細は、"LDAP キャッシュ認証情報" を参照してください。

3. [保存] をクリックすると、変更内容が適用されます。

2.2.1 LDAP キャッシュ認証情報

LDAP キャッシュ認証情報を使用するようにインスタンスを構成すると、そのインスタンスでは、各ユーザの認証に前回使用した認証情報のコピーが保存 (キャッシュ) されます。インスタンスでキャッシュ認証情報がサポートされている場合に、そのインスタンスが LDAP サーバに接続できないときは、キャッシュされている LDAP 認証情報を使用してユーザを認証します。この状況は、LDAP サーバ自体または LDAP サーバへの接続に問題がある場合に生じる可能性があります。

キャッシュ認証情報を保護するために、InterSystems IRIS では、すべての LDAP パスワードを単方向ハッシュとしてセキュリティ・データベースに格納します。インスタンスが LDAP サーバを使用してユーザを検証できない場合、以下のことを確認しようとします。

- 入力されたパスワードのハッシュが、格納されているパスワードのハッシュと一致している
- 前回の LDAP ログインからのキャッシュされた有効期限に達していない

両方の条件を満たす場合、インスタンスはユーザを認証して、ログインが続行します。それ以外の場合、ログインは失敗します。

2.3 LDAP 構成の作成または変更

LDAP 認証を実行するために、InterSystems IRIS は LDAP 構成を使用します。LDAP 構成では、特定のセキュリティ・ドメインに関する LDAP サーバへの接続を指定し、以下の処理を行うために必要な情報を定義します。

- LDAP サーバに接続し、クエリを実行します。
- 認証するユーザについて必要な情報を取得します。

注釈　インスタンスに対して Kerberos が有効になっている場合、LDAP 構成のすべてのメニュー項目と他のラベルは LDAP/Kerberos 構成を指します。以下の手順では、この点について状況ごとに個別には注記していません。

LDAP 構成を作成または変更する手順は以下のとおりです。

1. 管理ポータルの [セキュリティ LDAP 構成] ページ ([システム管理] > [セキュリティ] > [システム・セキュリティ] > [LDAP 構成]) に移動します。

   インストール時に、現在 LDAP サーバを使用しているマシンに InterSystems IRIS をインストールすると、LDAP サーバのドメインおよびその他の構成情報に基づいて LDAP 構成が作成されます。

2. 構成を作成または変更します。
   - 既存の構成を変更するには、その名前をクリックします。例えば、ローカル LDAP サーバに関連付けられた構成を使用する場合、その構成の属性をチェックし、必要に応じて変更します。
   - 構成を作成するには、[新規 LDAP 構成の作成] ボタンをクリックします。[LDAP 構成の編集] ページが表示されます。

     注釈　構成の作成時には、[LDAP 構成の編集] ページの [LDAP 構成] チェック・ボックスにチェックを付けます (使用可能な場合)。LDAP 構成を定義するフィールドが表示されます。

3. このフィールドを変更するか、値を入力して、構成を定義します (以下に表示)。

4. 複数の構成を作成する場合は、[システムワイドセキュリティパラメータ] ページ ([セキュリティ管理] > [セキュリティ] > [システム・セキュリティ] > [システムワイドセキュリティパラメータ]) で [デフォルトセキュリティドメイン] ドロップダウンを使用して、既定のものを指定する必要があります。

2.3.1 LDAP 構成フィールド

LDAP 構成には以下のフィールドがあります。

- **[ログインドメイン名]** ― 必須。LDAP 構成の名前です。これは通常、example.com や example.org のような形式です。

  ピリオドを含まない値を入力した場合、.com が自動的に追加されるため、example は example.com になります。値を大文字で入力した場合は自動的に小文字になるため、EXAMPLE.COM は example.com になります。両方の変換がシステムによって適宜実行されます。

  [名前] フィールドの変換後の値を使用して、[検索に使用するLDAPベースDN] フィールドに値が入力されます。

- **[説明]** ― 構成を説明する任意のテキスト。

- **[コピー元]** ― 構成の作成時にのみ使用できます。この LDAP 構成の初期値を指定するために InterSystems IRIS が既存の LDAP 構成から属性をコピーするかどうか。

- **[LDAP 有効]** ― InterSystems IRIS が LDAP サーバに接続するためにこの構成を使用できるかどうか。

- **[LDAP サーバは Windows Active Directory サーバ]** ― Windows のみ。LDAP サーバが Windows Active Directory サーバであるかどうか。

- **[LDAP ホスト名]** ― 必須。LDAP サーバが動作しているホストの名前。ホスト名の複雑さは、未修飾のホスト名から、ポート番号を持つ完全修飾ホスト名まで多岐にわたります。ホスト名の必要な形式は、その構成により異なります。

  複数のホスト名を指定する場合は、名前を空白で区切ります。LDAP サーバが特定のポートを使用するように構成されている場合、ホスト名に “:portname” を追加してそれを指定できます。一般的には、ポートは指定せず、以下のように、LDAP 機能で既定のポートを使用するようにします。

  ```
  ldapserver.example.com
  ldapserver.example.com ldapbackup.example.com
  ```

  重要　[LDAPホスト名] の値にポート番号を含めると、接続を確立する際の TLS の動作を制御できます。

  - 指定した値に 636 以外のポート番号が含まれていて (`ldapserver.example.com:389` など)、[LDAPセッションに TLS/SSL 暗号化を使用する] チェック・ボックスにチェックが付いている場合、そのインスタンスは LDAP サーバとのプレーン・テキスト接続を確立し、StartTLS コマンドを発行して接続を暗号化しようとします。
  - LDAP ホスト名に指定した値にポート番号 636 が含まれている場合 (`ldapserver.example.com:636` など)、そのインスタンスは、[LDAPセッションに TLS/SSL 暗号化を使用する] チェック・ボックスにチェックが付いているかどうかに関係なく、LDAP サーバとの TLS 接続を確立しようとします。ただし、UNIX® クライアント・インスタンスからポート 636 に直接接続することはサポートされていません。

  背景情報については、%SYS.LDAP.Init() メソッドのクラス・リファレンスを参照してください。

- LDAP 検索情報 ― 状況により異なります。
  - **[検索に使用するLDAPユーザ名]** ― Windows Active Directory サーバの場合のみ。使用可能な場合は必須。初期接続を確立し、LDAP 検索の実行に使用するために LDAP サーバに提供されるユーザ名です。このユーザは検索ユーザとも呼ばれます。

検索ユーザには、LDAP データベース全体の読み取り許可が必要です。検索ユーザの LDAP データベースへのアクセスが遮られないようにすることが重要です。例えば、ユーザの LDAP アカウントは、以下のように設定する必要があります。

- ユーザがアカウントのパスワードを変更できない
- パスワードの有効期限を無期限にする
- アカウントの有効期限を無期限にする

LDAP データベースでの検索の詳細は、"LDAP データベース内でターゲット・ユーザが検索される仕組み" を参照してください。

- **[LDAP 検索ユーザー DN]** ― Windows 以外のすべてのプラットフォームおよび Windows Active Directory 以外のサーバの場合。使用可能な場合は必須。初期接続を確立し、LDAP 検索の実行に使用するために LDAP サーバに提供されるユーザの識別名 (DN) です。このユーザは検索ユーザとも呼ばれます。

  検索ユーザには、LDAP データベース全体の読み取り許可が必要です。検索ユーザの LDAP データベースへのアクセスは遮られないようにすることが重要です。例えば、ユーザの LDAP アカウントは、以下のように設定する必要があります。

  - ユーザがアカウントのパスワードを変更できない
  - パスワードの有効期限を無期限にする
  - アカウントの有効期限を無期限にする

  例えば、検索ユーザが“ldapsearchuser”である場合、LDAP DN (識別名) は以下のようになります。

  ```
  uid=ldapsearchuser,ou=People,dc=example,dc=com
  ```

  LDAP データベースでの検索の詳細は、"LDAP データベース内でターゲット・ユーザが検索される仕組み" を参照してください。

- **[LDAPユーザ名パスワード]** ― 構成の作成時または変更時にのみ使用可能。最初の接続に使用するアカウントに関連付けられたパスワード。
- **[検索に使用するLDAPベースDN]** ― 必須。検索を開始する起点となるディレクトリ・ツリー内のポイント。通常は、`DC=example,DC=com` のように、ドメイン・コンポーネントで構成されます。
- **[LDAP Base DN to use for Nested Groups searches]** ― 必須。ネストしたグループの検索を開始する起点となるディレクトリ・ツリー内のポイント。一般的に組織単位とドメインの要素で構成され、`OU=IRIS,OU=Groups,DC=test,DC=com` のようになります。既定では、**[検索に使用するLDAPベースDN]** と同じ値に設定されています。
- **[LDAPユニーク検索属性]** ― 必須。各レコードの一意の識別要素。これにより、適切な検索が行われます。LDAP データベースでの検索の詳細は、"LDAP データベース内でターゲット・ユーザが検索される仕組み" を参照してください。
- **[LDAPセッションに TLS/SSL 暗号化を使用する]** ― InterSystems IRIS インスタンスと LDAP サーバが TLS を使用して通信を暗号化するかどうか (既定では無効)。

  重要　　LDAP に対して TLS 暗号化を有効にすることをお勧めします。

  Active Directory サーバへの接続の場合は、以下の点に注意してください。

  - この設定を Windows 上のインスタンスから Active Directory サーバへの LDAP 接続で有効にした場合、接続はポート 636 (TLS で暗号化されたポート) を使用します。

- この設定を UNIX® 上のインスタンスから Active Directory サーバへの LDAP 接続で有効にした場合、InterSystems IRIS は最初にポート 389 (暗号化されていない LDAP ポート) で接続を確立し、その後、StartTLS 呼び出しによって暗号化が有効になります。

Active Directory サーバで LDAP server signing requirements パラメータを `Require signature` に設定することもお勧めします。これにより、チャンネルが StartTLS で暗号化されている場合を除き、サーバのポート 389 で LDAP bind コマンドが実行されるのを防ぐことができます。詳細は、Microsoft Web サイトのドメイン コントローラーの LDAP サーバー署名要件の記事を参照してください。

- **[File with Certificate Authority certificate(s) to authenticate the LDAP server]** — UNIX® のみ。サーバの認証に使用される TLS 証明書 (PEM 形式) を含むファイルの場所。

  Windows で、サーバ証明書の認証に使用される TLS 証明書 (PEM 形式) を含むファイルの場所を指定して、安全な LDAP 接続を確立するには、Microsoft Certificate Services を使用します。証明書は、**Certificates (Local Computer)¥Trusted Root Certification Authorities** 証明書ストアにインストールする必要があります。

- **[ISC_LDAP_CONFIGURATION 環境変数を許可]** — OS ベースの LDAP および複数のドメインを使用する場合、ISC_LDAP_CONFIGURATION 環境変数を使用するかどうかを指定します。この環境変数が定義されている場合、OS ベースの LDAP は、これを使用して、認証に使用する LDAP 構成を特定します。

- **[ロール、ルーチン、ネームスペースで LDAP グループを使用する]** — ユーザのロール、ルーチン、およびネームスペースが、ユーザのグループ・メンバシップから取得されるかどうか (既定では True です)。グループ・メンバシップから取得されない場合、ユーザの LDAP レコードの属性フィールドから取得されます。このフィールドを選択すると、他のフィールドが有効または無効になります (詳細は、後続の各フィールドを参照してください)。

  注釈　承認には LDAP 属性 (登録されている LDAP プロパティを含む) ではなく、LDAP グループの使用をお勧めします。既存のコードがある、または登録されているプロパティを使用する必要がある場合、詳細は "LDAP 属性を使用した承認の構成" を参照してください。

- **[ネストしたグループのロール/ルーチン/ネームスペースを検索]** — **[LDAP サーバが Windows アクティブ・ディレクトリ・サーバ]** および **[ロール/ルーチン/ネームスペースに LDAP グループを使用]** が選択されている場合にのみ有効です。ユーザの入れ子になったグループすべてを検索で返すかどうか。入れ子になったグループの詳細は、"入れ子になったグループ" を参照してください。

- **[グループ名の組織IDプレフィックス]** — **[ロール/ルーチン/ネームスペースに LDAP グループを使用]** が選択されている場合にのみ有効です。詳細は、"LDAP グループ名の構成" を参照してください。

- **[ユニバーサルグループ承認を許可する]** — **[ロール/ルーチン/ネームスペースに LDAP グループを使用]** が選択されている場合にのみ有効です。すべての InterSystems IRIS インスタンスに関連する、LDAP サーバ上の属性を検索で使用するかどうか。詳細は、"ユニバーサル LDAP 承認グループの作成" を参照してください。

- **[承認グループID]** — **[ロール/ルーチン/ネームスペースに LDAP グループを使用]** が選択されている場合にのみ有効です。このインスタンスが属する複数インスタンス・グループ。詳細は、"複数のインスタンスを対象とする LDAP 承認グループ (複数インスタンス・グループ) の作成" を参照してください。

- **[承認インスタンスID]** — **[ロール/ルーチン/ネームスペースに LDAP グループを使用]** が選択されている場合にのみ有効です。このインスタンスが属する単一インスタンス・グループ。詳細は、"1 つのインスタンスを対象とする LDAP 承認グループ (単一インスタンス・グループ) の作成" を参照してください。

- **[デフォルトネームスペースを取得するためのユーザ属性]** (LDAP グループが選択されている場合は無効) — 値がユーザの Startup namespace プロパティのソースである属性。InterSystems IRIS ユーザのこのプロパティについては、"ユーザ・アカウントのプロパティ" で説明されています。この LDAP プロパティの詳細は、"LDAP 属性を使用した承認の構成" を参照してください。

- **[デフォルトルーチンを取得するためのユーザ属性]** (LDAP グループが選択されている場合は無効) — 値がユーザの Tag^Routine プロパティのソースである属性。InterSystems IRIS ユーザのこのプロパティについては、"ユーザ・アカウントのプロパティ" で説明されています。この LDAP プロパティの詳細は、"LDAP 属性を使用した承認の構成" を参照してください。

- **[ロール取得のためのユーザ属性]** (LDAP グループが選択されている場合は無効) – その値によってユーザの割り当て先のロールを決定する属性。この属性はLDAP 複数値属性として指定し、作成する必要があります。InterSystems IRIS ユーザのロールの詳細は、ユーザの **[ユーザ編集]** ページの **[ロール]** タブを参照してください。この LDAP プロパティについては、"LDAP 属性を使用した承認の構成" に説明があります。
- **[コメント属性を取得するためのユーザ属性]** – 値がユーザの Comment プロパティのソースである属性。このプロパティの詳細は、"ユーザ・アカウントのプロパティ" を参照してください。ユーザがログインすると、Security.Users.Get() メソッドを使用して、このプロパティの値を取得できます。
- **[フルネームを取得するためのユーザ属性]** – 値がユーザの Full name プロパティのソースである属性。このプロパティの詳細は、"ユーザ・アカウントのプロパティ" を参照してください。ユーザがログインすると、Security.Users.Get() メソッドを使用して、このプロパティの値を取得できます。
- **[メールアドレスを取得するユーザー属性]** – 値がユーザの Email address プロパティのソースである属性。このプロパティの詳細は、"ユーザ・アカウントのプロパティ" を参照してください。ユーザがログインすると、Security.Users.Get() メソッドを使用して、このプロパティの値を取得できます。
- **[携帯電話番号を取得するユーザー属性]** – 値がユーザの Mobile Phone Number プロパティのソースである属性。このプロパティの詳細は、"ユーザ・アカウントのプロパティ" を参照してください。ユーザがログインすると、Security.Users.Get() メソッドを使用して、このプロパティの値を取得できます。
- **[携帯電話プロバイダを取得するためのユーザ属性]** – 値がユーザの Mobile Phone Service Provider プロパティのソースである属性。このプロパティの詳細は、"ユーザ・アカウントのプロパティ" を参照してください。ユーザがログインすると、Security.Users.Get() メソッドを使用して、このプロパティの値を取得できます。
- **[各ユーザに取得するLDAP属性]** – 値がアプリケーション固有の変数のソースである属性。これにより、アプリケーション・コードで Security.Users クラスの Get メソッドを使用してこの情報が返されます。

LDAP 構成の各フィールドの値は、Security.LDAPConfigs クラスのインスタンスに保存されます。

2.3.2 LDAP/Kerberos 構成フィールドに関する注意事項

インスタンスに対して Kerberos 認証が有効になっている場合、LDAP 構成を作成するページは、**[LDAP/Kerberos 構成を編集]** ページです。このページには、**[LDAP 構成を編集]** ページと同じフィールドがあります。"LDAP 構成フィールド" を参照してください。

2.4 LDAP 構成のテスト

LDAP 構成を作成したら、それをテストできます。これにより、LDAP サーバに適切に接続できることを確認することや、問題が発生する場合はトラブルシューティングすることができます。構成をテストする手順は以下のとおりです。

1. 管理ポータルで、**[セキュリティ LDAP 構成]** ページ (**[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[LDAP 構成]**) に移動します。
2. **[LDAP 認証のテスト]** をクリックします。
3. **[ユーザ名]** フィールドと **[パスワード]** フィールドに、LDAP サーバで定義されている有効なユーザ名とパスワードを入力します。複数のドメインを使用するようにインスタンスが構成されている場合は、`EndUser@example.com` のように、完全修飾ユーザ名を入力する必要があります。インスタンスが 1 つのドメインのみを使用している場合は、`EndUser` のように、単に未修飾のユーザ名 (@ 記号やドメイン名なし) を入力します。
4. **[テスト]** をクリックします。

[テスト結果] フィールドに、LDAP サーバからの出力が表示されます。

注釈　この機能は、インスタンスが LDAP サーバに接続して、入力されたユーザの認証チェックを実行できるかどうかのみをテストします。承認チェックまたは許可チェックを実行して、ユーザがシステムに正常にログインできるかどうかは確認しません。

入力されたユーザのテストは成功したのにユーザがログインできない場合は、ログイン・エラーがないかどうか監査レコードを確認してください。正常にログインするために、ユーザに追加の許可を付与しなければならないことがあります。

2.5 複数の LDAP ドメインの使用

InterSystems IRIS では、複数のドメインでの LDAP 認証がサポートされています。これにより、EndUser@example.com や EndUser@otherexample.com など、複数のドメインに属する同じユーザ名を含むユーザ・アカウントをインスタンスで保持できます。この機能は、さまざまなシナリオで役立ちます。次に例を示します。

- 各ユーザの一意の識別子を保持しながら、複数のドメインの個々のユーザ・セットを 1 つの大きなグループにマージできます。
- それぞれ特権が異なるアカウントを同じ個人が複数のドメインに持つことができます。

複数のドメインを使用する手順は以下のとおりです。

1. ″LDAP 構成の作成または変更″ で説明した手順に従って、追加の LDAP 構成を作成します。
2. 複数のドメインを使用するようにインスタンスを構成し、既定のドメインを指定します。
   a. インスタンスで複数のドメインの使用を有効にします。管理ポータルの **[システムワイドセキュリティパラメータ]** ページ (**[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[システムワイドセキュリティパラメータ]**) で、**[複数セキュリティドメインを許可する]** チェック・ボックスにチェックを付けます。
   b. 既定のドメインを指定します。管理ポータルの **[システムワイドセキュリティパラメータ]** ページ (**[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[システムワイドセキュリティパラメータ]**) で、**[デフォルトセキュリティドメイン]** ドロップダウンを使用して既定のドメインを選択します。
   c. **[保存]** をクリックします。

   このページの詳細は、″システム規模のセキュリティ・パラメータ″ を参照してください。

注釈　複数のドメインを使用する場合も、各ユーザの名前は一意である必要があります。ユーザのタイプが異なっていても、一意でなければなりません。したがって、パスワード・ユーザである EndUser@example.com などのユーザを作成した場合、ユーザ EndUser@example.com として LDAP を介して InterSystems IRIS にログインすることはできません。InterSystems IRIS では、EndUser@example.com のアカウントを LDAP ユーザとして作成できないためです。

2.6 必要なログイン・ロールの設定

InterSystems IRIS のインスタンスが複数あり、LDAP 認証または OS ベースの認証と LDAP 承認を使用する場合、インスタンスに接続するユーザに必要なロールを各インスタンスで作成することを強くお勧めします。このメカニズムにより、ユーザは、十分な特権がないインスタンスにはアクセスできなくなります。このようにしないと、あるインスタンスでさまざまなロールを保持しているユーザが、意図していないインスタンスで同じロールを持つ可能性があります。

必要なログイン・ロールを設定する手順は以下のとおりです。

1. インスタンスごとに、必要なロールがまだ存在しない場合は、"ロールの作成" の手順に従ってロールを作成します。
2. インスタンスごとに、必要なロールを [**システムセキュリティ設定**] ページの [**このシステムに接続するのに必要なロール**] フィールド ([**システム管理**]→[**セキュリティ**]→[**システム・セキュリティ**]→[**システムワイドセキュリティパラメータ**]) で指定します。
3. 必要なロールの名前を含む名前の LDAP グループを追加します。グループの名前の形式は以下のとおりです。

   `intersystems-Instance-`instanceID`-Role-`rolename

   各要素の内容は以下のとおりです。

   - instanceID は、LDAP サーバにおけるインスタンスの一意の識別子です。
   - rolename は、接続に必要なロールの名前です。

注釈　ミラーリングを使用している場合など、特定の状況では、複数のインスタンス間で必要な 1 つのログイン・ロールを作成する方が望ましいこともあります。

例えば、2 つのシステム TEST と PRODUCTION があるとします。それらのシステムのセキュリティを個別に確保するには、**TEST** に **TESTACCESS** ロールを作成し、**PRODUCTION** に **PRODUCTIONACCESS** ロールを作成します。**TEST** では、[**このシステムに接続するのに必要なロール**] フィールドの値に **TESTACCESS** を設定します。**PRODUCTION** では、このフィールドの値に **PRODUCTIONACCESS** を設定します。その後で、**TEST** システムへのアクセスのみをユーザに許可する場合は、そのユーザに **TESTACCESS** ロールのみを割り当てて、**PRODUCTIONACCESS** ロールは割り当てないようにします。両方のシステムにアクセスできるユーザには、**PRODUCTIONACCESS** ロールと **TESTACCESS** ロールの両方を割り当てます。

2.7 サービスおよびアプリケーションでの LDAP の有効化

インスタンスで LDAP 認証を有効にしたら、インスタンスの関連サービスまたはアプリケーションで LDAP 認証を有効にします。

1. LDAP 認証がインスタンスで有効になっているため、LDAP 認証をサポートするサービスの [**サービス編集**] ページと Web アプリケーションの [**ウェブ・アプリケーション編集**] ページに [LDAP] チェック・ボックスが表示されます。
2. 必要に応じて、サービスおよびアプリケーションで LDAP 認証を有効にします。

LDAP 認証をサポートしているサービスは以下のとおりです。

- **%Service_Bindings**
- **%Service_CallIn**
- **%Service_ComPort**
- **%Service_Console**
- **%Service_Login**
- **%Service_Terminal**
- **%Service_Telnet**
- **%Service_WebGateway**

これらのサービスは、アクセス・モードによっていくつかのカテゴリに分類されます。

- ローカル・アクセス ー

  %Service_CallIn、**%Service_ComPort**、**%Service_Console**、**%Service_Login**、**%Service_Terminal**、**%Service_Telnet**

  ローカル接続で LDAP 認証を使用するには、サービスの LDAP 認証を有効にします。

- クライアント・サーバ・アクセス ー

  %Service_Bindings

  クライアント・サーバ接続で LDAP 認証を使用するには、サービスの LDAP 認証を有効にします。

- Web アクセス ー

  %Service_WebGateway

  指定したユーザが LDAP 認証を使用して Web アプリケーションにログインできるためには、関連の Web アプリケーションで LDAP を使用できるようにする必要があります。Web アプリケーションに認証メカニズムを追加する方法の詳細は、"アプリケーション" の "セキュリティの設定" を参照してください。サービスで LDAP を有効にすると、Web ゲートウェイ自体でも LDAP 認証を使用した認証が可能になります。

2.8 LDAP 認証後のインスタンスの状態

LDAP 認証を使用して最初に認証されるユーザは、“LDAP ユーザ” というタイプで **[ユーザ]** ページ (**[システム管理]→[セキュリティ]→[ユーザ]**) のユーザ・テーブルに表示されます。システム管理者が管理ポータル (またはその他の InterSystems IRIS ネイティブ機能) を使用して明示的にユーザを作成した場合、そのユーザのタイプは “InterSystems IRIS パスワード・ユーザ” になります。ユーザが LDAP 認証を使用してログインを試行し、認証が正常に行われる場合でも、そのユーザが既に (LDAP ユーザではなく) InterSystems IRIS ユーザとして存在することを InterSystems IRIS が検出すると、ログインは失敗します。

2.9 ポータルでの LDAP 構成の %Operator としての表示

管理ポータルに **%Operator** ロールまたは **%Admin_Operate:Use** 特権を持つユーザとしてログインしている場合は、インスタンスの LDAP 構成を表示できます (ただし、編集はできません)。

1. ポータルで、**[LDAP 構成]** ページ (**[システム処理]** > **[LDAP 構成]**) に移動します。
2. このページで、表示する構成の名前をクリックすると、その構成の **[LDAP 構成の表示]** が表示されます。

LDAP 構成を編集するには、**[セキュリティ LDAP 構成]** ページ (**[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[LDAP 構成]**) に移動します。**%Admin_Secure:Use** 特権を持っている必要があります。

2.9.1 [セキュリティ LDAP 構成] ページ

ポータルの **[セキュリティ LDAP 構成]** ページ (**[システムオペレーション]→[LDAP 構成]**) には、インスタンスの LDAP 構成のリストが表示されます。構成名をクリックすると、そのプロパティが表示されます。インスタンスに対して Kerberos 認証が有効になっている場合、このページは **[セキュリティ LDAP/Kerberos 構成]** ページという名前になります (**[システム処理]** > **[LDAP/Kerberos 構成]**)。

3

LDAP 承認

LDAP を使用した認証の実行に加え、InterSystems IRIS では LDAP 承認がサポートされます。ロール、ルーチン、およびネームスペース定義の管理には、LDAP 属性ではなく LDAP グループを使用することをお勧めします。

3.1 LDAP 承認の構成の概要

承認に LDAP を使用するようにインターシステムズのサービスまたはアプリケーションを構成する手順は以下のとおりです。

1. LDAP 認証または OS ベースの認証を使用できるようにインスタンスを構成します。
2. LDAP 承認について、以下の手順を実行します。
   a. InterSystems IRIS インスタンスにおける LDAP 承認のグループを設計します。
   b. それらのグループを使用するように LDAP サーバを構成します。

3.2 LDAP グループを使用した承認の構成

- LDAP グループと InterSystems IRIS
- LDAP 承認グループ・モデル
  - 1 つのインスタンスを対象とする LDAP 承認グループ (単一インスタンス・グループ) の作成
  - 複数のインスタンスを対象とする LDAP 承認グループ (複数インスタンス・グループ) の作成 (ミラーリングの承認を含む)
  - ユニバーサル LDAP 承認グループの作成
- LDAP グループを使用した LDAP 承認に関するその他のトピック

3.2.1 LDAP グループと InterSystems IRIS

LDAP グループを使用すると、LDAP サーバを使用してユーザに特権を割り当てることができます。

- LDAP サーバのスキーマによって、グループの名前が指定されます。通常は、LDAP 管理者がこれらの名前を定義します。InterSystems IRIS では、後述する、事前定義された 3 つの名前構造のいずれかが使用されます。
- 各グループには、一意に識別できる識別名 (DN) があります。
- 各グループでは、InterSystems IRIS のロール、ルーチン、またはネームスペースへのアクセスを指定します。

InterSystems IRIS は、以下のインスタンスを対象として承認を提供する LDAP グループをサポートしています。

- 1 つのインスタンス
- 複数のインスタンス
- すべてのインスタンス

InterSystems IRIS で使用するグループを設定する手順は以下のとおりです。

1. 1 つのインスタンス、複数のインスタンス、すべてのインスタンスのいずれを対象とするグループを使用するかを決定します。
2. 適切な命名規則に準拠する名前で 1 つ以上のグループを作成します。各グループでは、ユーザのロール、既定のネームスペース、または既定のルーチンを指定します。ユーザは複数のロールを持つことができるので、ロールを指定する複数のグループに属することもできます。

   注釈　LDAP サーバ上でこれらのグループを定義する際、ディストリビューション・グループとしてではなく、セキュリティ・グループとして作成する必要があります。

3. LDAP ユーザを構成して、どのユーザがどのグループに属するかを指定します。そのためには、各ユーザの LDAP アカウントについて、1 つ以上のロール、既定のネームスペース、および既定のルーチンを指定する複数のグループにユーザを割り当てる必要があります。これにより、ログイン後に各ユーザに付与されるロール、ユーザの既定のネームスペース、およびユーザの既定のルーチンが決まります。
4. LDAP サーバで指定されたすべてのロールの定義が含まれるように、ローカル InterSystems IRIS インスタンスを構成します。

3.2.2 LDAP 承認グループ・モデル

InterSystems IRIS では、LDAP を使用した 3 種類のグループ承認がサポートされています。

- 1 つのインスタンスを対象とする LDAP 承認グループ (単一インスタンス・グループ) の作成
- 複数のインスタンスを対象とする LDAP 承認グループ (複数インスタンス・グループ) の作成 (ミラーリングを含む)
- ユニバーサル LDAP 承認グループの作成

3.2.2.1 1 つのインスタンスを対象とする LDAP 承認グループ (単一インスタンス・グループ) の作成

InterSystems IRIS では、1 つのインスタンスのみを対象として承認を提供する LDAP グループを作成できます。このような各グループは、単一インスタンス・グループと呼ばれます。この種類の承認グループを作成する手順は以下のとおりです。

1. InterSystems IRIS インスタンスで、LDAP パラメータ **[承認インスタンス ID]** の値を確認または変更します。既定では、その値は NodeName_InstanceName です。NodeName は InterSystems IRIS インスタンスが実行されているマシン、InstanceName はそのインスタンスの名前です。

   パラメータの値を手動で設定するには、以下の手順を実行します。

   a. 管理ポータルで、**[セキュリティ LDAP 構成]** ページ (**[管理ポータル]** > **[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[LDAP 構成]**) に移動します。

b. そのページで、編集する構成の名前をクリックして選択します。

c. 表示される、構成を編集するためのページで、**[ロール、ルーチン、ネームスペースで LDAP グループを使用する]** を選択します。

d. 次に、**[承認インスタンス ID]** フィールドにパラメータの値を入力し、**[保存]** をクリックします。

2. LDAP サーバで、`Instance` キーワードに続けて **[承認インスタンス ID]** の値を使用して、必要なインターシステムズの構造に準拠する名前でロール、ネームスペース、およびルーチンのグループを定義します。これらの文字列は大文字と小文字を区別しません。これらのグループ名の形式は以下のとおりです。

   `intersystems-Instance-`AuthorizationInstanceIDValue`-Role-`RoleName

   `intersystems-Instance-`AuthorizationInstanceIDValue`-Routine-`RoutineName

   `intersystems-Instance-`AuthorizationInstanceIDValue`-Namespace-`NamespaceName

   各要素の内容は以下のとおりです。

   - AuthorizationInstanceIDValue は、[承認インスタンス ID] フィールドに指定された値です。
   - RoleName、RoutineName、および NamespaceName はそれぞれ、ロール、既定のルーチン、または既定のネームスペースの名前です。

     注釈　ユーザは、任意の数のロールを持つことができます。通常、システムへのアクセスには少なくとも 1 つのロールが必要です。ユーザは、1 つの既定のルーチンおよび 1 つの既定のネームスペースのみを持つことができます。ただし、これらは必須ではないため、ユーザが既定のルーチンや既定のネームスペースを持たなくてもかまいません。

   - RoleName には、複数のロールを“^”で区切って含めることができます。例えば、“%All^Admin^Application4”には、“%All”ロール、“Admin”ロール、および“Application4”ロールが含まれます。

3. InterSystems IRIS インスタンスで、各グループに関連するロールを構成します。

例えば、Node1 というマシン上にある Test というインスタンスでアプリケーションを実行しているとします。以下の 3 つのユーザ・カテゴリを設定します。

- アプリケーション・ユーザ ー アプリケーションのみを実行できます。
- 管理ユーザ ー さまざまな管理ツールとアプリケーションを実行できます。
- スーパーユーザ ー フル・アクセス権を持ちます。

この承認モデルを設定するには、LDAP サーバで以下のグループを作成します。

```
intersystems-Instance-Node1_Test-Role-Administrator
intersystems-Instance-Node1_Test-Role-LocalApplication
intersystems-Instance-Node1_Test-Role-%All
intersystems-Instance-Node1_Test-Routine-LocalApplication
intersystems-Instance-Node1_Test-Routine-%SS
intersystems-Instance-Node1_Test-Routine-%pmode
intersystems-Instance-Node1_Test-Namespace-%SYS
intersystems-Instance-Node1_Test-Namespace-USER
```

次に、各ユーザ・カテゴリに対応するロールを作成します。

- 管理者
- LocalApplication

注釈　**`%All`** ロールは既に存在するため、作成する必要はありません。

最後に、3 つのユーザ・カテゴリを作成します。

- アプリケーション・ユーザ ー アプリケーション LocalApplication のみを実行できます。以下の LDAP グループに割り当てられます。
  - `intersystems-Instance-Node1_Test-Role-LocalApplication`
  - `intersystems-Instance-Node1_Test-Routine-LocalApplication`
  - `intersystems-Instance-Node1_Test-Namespace-USER`
- 管理ユーザ ー さまざまな管理ツールとアプリケーションを実行できます。以下の LDAP グループに割り当てられます。
  - `intersystems-Instance-Node1_Test-Role-LocalApplication`
  - `intersystems-Instance-Node1_Test1-Role-Administrator`
  - `intersystems-Instance-Node1_Test-Routine-%SS`
  - `intersystems-Instance-Node1_Test-Namepace-%SYS`
- スーパーユーザ ー **`%All`** アクセス権を持ちます。以下の LDAP グループに割り当てられます。
  - `intersystems-Instance-Node1_Test-Role-%All`
  - `intersystems-Instance-Node1_Test-Namespace-%SYS`
  - `intersystems-Instance-Node1_Test-Routine-%pmode`

3.2.2.2 複数のインスタンスを対象とする LDAP 承認グループ (複数インスタンス・グループ) の作成

InterSystems IRIS では、複数のインスタンスを対象として承認を提供する LDAP グループを作成できます。このような各グループは、複数インスタンス・グループと呼ばれます。この種類の承認グループを作成する手順は以下のとおりです。

1. 個々のインスタンスがグループ間でどのように情報を共有するかを決定します。これにより、各インスタンスのグループとユーザがアクセスできる情報が決まります。
2. グループ内の各インスタンスについて、LDAP パラメータ **[承認グループ ID]** の値をグループ内の他のインスタンスと同じになるように変更します。

   パラメータの値を手動で設定するには、以下の手順を実行します。

   a. 管理ポータルで、**[セキュリティ LDAP 構成]** ページ (**[管理ポータル]** > **[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[LDAP 構成]**) に移動します。

   b. そのページで、編集する構成の名前をクリックして選択します。

   c. 表示される、構成を編集するためのページで、**[ロール、ルーチン、ネームスペースで LDAP グループを使用する]** を選択します。

   d. 次に、**[承認グループ ID]** フィールドにパラメータの値を入力し、**[保存]** をクリックします。

3. LDAP サーバで、`Group` キーワードに続けて **[承認グループ ID]** の値を使用して、必要なインターシステムズの構造に準拠するロール、ネームスペース、およびルーチンのグループを設定します。これらの文字列は大文字と小文字を区別しません。これらのグループ名の形式は以下のとおりです。

   `intersystems-Group-`AuthorizationGroupIDValue`-Role-`RoleName

   `intersystems-Group-`AuthorizationGroupIDValue`-Routine-`RoutineName

   `intersystems-Group-`AuthorizationGroupIDValue`-Namespace-`NamespaceName

   各要素の内容は以下のとおりです。

- AuthorizationGroupIDValue は、[承認グループ ID] フィールドに指定された値です。
- RoleName、RoutineName、および NamespaceName はそれぞれ、ロール、既定のルーチン、または既定のネームスペースの名前です。

  注釈　ユーザは、任意の数のロールを持つことができます。通常、システムへのアクセスには少なくとも 1 つのロールが必要です。ユーザは、1 つの既定のルーチンおよび 1 つの既定のネームスペースのみを持つことができます。ただし、これらは必須ではないため、ユーザが既定のルーチンや既定のネームスペースを持たなくてもかまいません。

- RoleName には、複数のロールを“^”で区切って含めることができます。例えば、“%All^Admin^Application4”には、“%All”ロール、“Admin”ロール、および“Application4”ロールが含まれます。

4. それらを使用するすべてのインスタンスで、必要なロールを構成します。

例えば、5 台のデータベース・サーバに接続された 7 台の ECP アプリケーション・サーバがあるとします。データベース・サーバのうちの 2 台はフェイルオーバー・ペアで、それ以外の 3 台は非同期レポート・メンバです。これらのサーバ (アプリケーション・サーバとデータベース・サーバの両方) はすべて、SALES アプリケーションを実行します。アプリケーションのエンド・ユーザに必要な特権のセットは限定されますが、その管理ユーザはより多くの特権を必要とします。したがって、以下の 3 つのユーザ・カテゴリを設定します。

- アプリケーション・ユーザ ー アプリケーションのみを実行できます。
- アプリケーション・サーバ管理者 ー アプリケーションを実行できます。アプリケーション・サーバへのフル・アクセス権を持ちますが、データベース・サーバにはアクセスできません。
- データベース管理者 ー アプリケーション・サーバへのフル・アクセス権とデータベース・サーバへの管理アクセス権を持ちます。

これらの要件をサポートするように LDAP 承認を構成する手順は以下のとおりです。

- アプリケーション・サーバの **[承認グループ ID]** を SALESAPP に設定します。
- データベース・サーバの **[承認グループ ID]** を SALESDB に設定します。

LDAP サーバで、グループを以下のように定義します。

```
intersystems-Group-SALESAPP-Role-%All
intersystems-Group-SALESAPP-Role-LocalApplication
intersystems-Group-SALESAPP-Routine-LocalApplication
intersystems-Group-SALESAPP-Routine-%pmode
intersystems-Group-SALESAPP-Namespace-USER
intersystems-Group-SALESAPP-Namespace-%SYS
intersystems-Group-SALESDB-Role-Administrator
intersystems-Group-SALESDB-Routine-INTEGRIT
intersystems-Group-SALESDB-Namespace-%SYS
```

次に、各ユーザ・カテゴリに対応するロールを作成します。

- 管理者
- LocalApplication

注釈　**%All** ロールは既に存在するため、作成する必要はありません。

最後に、3 つのユーザ・カテゴリを作成します。

- アプリケーション・ユーザ ー アプリケーション LocalApplication のみを実行できます。以下の LDAP グループに割り当てられます。
  - `intersystems-Group-SALESAPP-Role-LocalApplication`

- intersystems-Group-SALESAPP-Routine-LocalApplication
- intersystems-Group-SALESAPP-Namespace-USER

· アプリケーション・サーバ管理者 – アプリケーションを実行できます。アプリケーション・サーバへのフル・アクセス権を持ちますが、データベース・サーバにはアクセスできません。以下の LDAP グループに割り当てられます。

- intersystems-Group-SALESAPP-Role-LocalApplication
- intersystems-Group-SALESAPP-Namespace-USER
- intersystems-Group-SALESAPP-Role-%All
- intersystems-Group-SALESAPP-Routine-%pmode

· データベース管理者 – アプリケーション・サーバへのフル・アクセス権とデータベース・サーバへの管理アクセス権を持ちます。以下の LDAP グループに割り当てられます。

- intersystems-Group-SALESAPP-Role-%All
- intersystems-Group-SALESAPP-Routine-%pmode
- intersystems-Group-SALESAPP-Namespace-%SYS
- intersystems-Group-SALESDB-Role-Administrator
- intersystems-Group-SALESDB-Routine-INTEGRIT
- intersystems-Group-SALESDB-Namespace-%SYS

この時点で、完全に機能する承認モデルが存在しますが、データベース・サーバへの (**%All** を持つ) スーパーユーザ・アクセスが含まれていません。このようなアクセスを追加するには、ユーザを作成して以下の新しいグループに追加します。

intersystems-Group-SALESDB-Role-%All

3.2.2.3 ミラーリングを含む LDAP 承認グループの構成

LDAP とミラーリングを使用する場合は、複数インスタンス LDAP グループを使用して承認を構成することをお勧めします。必要な複数インスタンス・グループを作成し、それらのグループを使用するようにすべてのメンバ (非同期メンバを含む) のすべてのユーザを構成します。

前述の例で定義したグループ構造に基づく、以下の例を検討してみましょう。さらに、以下のように仮定します。

· フェイルオーバー・ペアである SALESDBMIR というミラーと 3 つのレポート非同期メンバがあります。

· **%All** を持つユーザを作成しますが、フェイルオーバー・ペアのみでこのアクセス権を持ちます。

このミラーの承認を構成する手順は以下のとおりです。

1. フェイルオーバー・ペアへのフル・アクセス権を提供するために、以下のグループを作成します。

   intersystems-Group-SALESDBMIRFAILOVER-Role-%All

2. 非同期メンバへのフル・アクセス権を提供するために、以下のグループを作成します。

   intersystems-Group-SALESDBMIRASYNC-Role-%All

3. フェイルオーバー・ペアの各メンバの LDAP パラメータ [**承認インスタンス ID**] を SALESDBMIRFAILOVER に設定します。

重要　災害復旧 (DR) 非同期メンバはフェイルオーバー・メンバに昇格することがあるため、DR 非同期メンバの [**承認インスタンス ID**] も SALESDBMIRFAILOVER に設定する必要があります。

4. ミラーの非同期メンバの LDAP パラメータ [**承認グループ ID**] を SALESDBMIRASYNC に設定します。
5. 次に、アプリケーション・サーバへの **%All** アクセス権、ミラーリングされていないデータベース・サーバへの管理アクセス権、およびフェイルオーバー・ペアのみへの **%All** アクセス権を持つミラー管理者を作成します。これらのユーザは、以下の LDAP グループに割り当てられます。
   - `intersystems-Group-SALESAPP-Role-%All`
   - `intersystems-Group-SALESAPP-Routine-%pmode`
   - `intersystems-Group-SALESAPP-Namespace-%SYS`
   - `intersystems-Group-SALESDB-Role-Administrator`
   - `intersystems-Group-SALESDB-Routine-INTEGRIT`
   - `intersystems-Group-SALESDB-Namespace-%SYS`
   - `intersystems-Group-SALESDBMIRFAILOVER-Role-%All`
6. 最後に、すべてのメンバ (アプリケーション・サーバ、データベース・サーバ、フェイルオーバー・ペア、および非同期メンバ) への **%All** アクセス権を持つフル管理者を作成します。これらのユーザは、以下の LDAP グループに割り当てられます。
   - `intersystems-Group-SALESAPP-Role-%All`
   - `intersystems-Group-SALESDB-Role-%All`
   - `intersystems-Group-SALESDBMIRFAILOVER-Role-%All`
   - `intersystems-Group-SALESDBMIRASYNC-Role-%All`

3.2.2.4 ユニバーサル LDAP 承認グループの作成

InterSystems IRIS では、1 つの LDAP サーバを使用するすべてのインスタンスを対象として承認を提供する LDAP グループを作成できます。これらは、ユニバーサル承認グループと呼ばれます。この種類の承認グループを作成する手順は以下のとおりです。

1. 現在のインスタンスでユニバーサル承認グループの使用を有効にします。
   a. 管理ポータルで、[**セキュリティ LDAP 構成**] ページ ([**管理ポータル**] > [**システム管理**] > [**セキュリティ**] > [**システム・セキュリティ**] > [**LDAP 構成**]) に移動します。
   b. そのページで、編集する構成の名前をクリックして選択すると、その構成を編集するためのページが表示されます。
   c. 構成を編集するためのページで、[**ロール、ルーチン、ネームスペースで LDAP グループを使用する**] を選択します。
   d. [**ユニバーサルグループ承認を許可する**] を選択します。
   e. [**保存**] をクリックします。
2. LDAP サーバで、必要なインターシステムズの構造に準拠するロール、ネームスペース、およびルーチンのグループを設定します。これらの文字列は大文字と小文字を区別しません。これらのグループ名の形式は以下のとおりです。

   `intersystems-Role-`RoleName

`intersystems-Routine-`RoutineName

`intersystems-Namespace-`NamespaceName

RoleName、RoutineName、および NamespaceName はそれぞれ、ロール、既定のルーチン、または既定のネームスペースの名前です。RoleName には、複数のロールを“^”で区切って含めることができます。例えば、“%All^Admin^Application4”には、“%All”ロール、“Admin”ロール、および“Application4”ロールが含まれます。

注釈　ユーザは、任意の数のロールを持つことができます。通常、システムへのアクセスには少なくとも 1 つのロールが必要です。ユーザは、1 つの既定のルーチンおよび 1 つの既定のネームスペースのみを持つことができます。ただし、これらは必須ではないため、ユーザが既定のルーチンや既定のネームスペースを持たなくてもかまいません。

3. LDAP サーバを使用するすべてのインスタンスで、必要なロールを構成します。

例えば、LocalApplication というアプリケーションがあり、LDAP サーバを使用するすべての InterSystems IRIS インスタンスで、そのアプリケーションに対するさまざまなレベルのアクセス権をユーザに付与するとします。以下の LDAP グループを定義します。

```
intersystems-Role-%All
intersystems-Role-Administrator
intersystems-Role-LocalApplication
intersystems-Routine-%SS
intersystems-Routine-LocalApplication
intersystems-Namespace-USER
intersystems-Namespace-%SYS
```

次に、各ユーザ・カテゴリに対応するロールを作成します。

- Admin
- LocalApplication

注釈　**`%All`** ロールは既に存在するため、作成する必要はありません。

最後に、3 つのユーザ・カテゴリを作成します。

- アプリケーション・ユーザ ー すべてのサーバ上のアプリケーションにアクセスできます。以下の LDAP グループに割り当てられます。
  - `intersystems-Role-LocalApplication`
  - `intersystems-Routine-LocalApplication`
  - `intersystems-Namespace-USER`
- 管理者 ー すべてのサーバへの管理アクセス権を持ちます。以下の LDAP グループに割り当てられます。
  - `intersystems-Role-Administrator`
  - `intersystems-Routine-%SS`
  - `intersystems-Namespace-%SYS`
- スーパーユーザ ー すべてのサーバへのフル・アクセス権を持ちます。以下の LDAP グループに割り当てられます。
  - `intersystems-Role-%All`

3.2.3 LDAP グループを使用した LDAP 承認に関するその他のトピック

トピックは以下のとおりです。

- LDAP グループ定義の構造
- LDAP グループ名の構成
- さまざまな種類のグループの混合
- 入れ子になったグループ
- LDAP グループによって InterSystems IRIS へのアクセスが規制される仕組み

3.2.3.1 LDAP グループ定義の構造

通常、グループ定義の内容は以下のとおりです。

- グループ名
- グループの組織単位の宣言 (`OU=Groups`)
- ドメイン・コンポーネント (DC) の宣言 (`DC=example,DC=com` など)
- 必要なその他の情報

例えば、以下のようなグループ定義が考えられます。

```
CN=intersystems-Role-Administrator,OU=Groups,DC=intersystems,DC=com
CN=intersystems-Group-MyGroup-Namespace-USER,OU=Groups,DC=intersystems,DC=com
CN=intersystems-Instance-MyNode:MyInstance-Routine-INTEGRIT,OU=Groups,DC=intersystems,DC=com
```

3.2.3.2 LDAP グループ名の構成

InterSystems IRIS では、LDAP グループ名をさらに細かく構成できます。以下のセクションでは、既定の構成、構成可能なプロパティ、およびプロパティの変更手順について説明します。

- 既定のグループ名の構成
- グループ名のプロパティ
- プロパティの変更手順

既定のグループ名の構成

既定では、LDAP グループ名では以下の構文を使用します。

`intersystems-Role-`RoleName

`intersystems-Routine-`RoutineName

`intersystems-Namespace-`NamespaceName

`intersystems-Group-`GroupName`-Role-`RoleName

`intersystems-Group-`GroupName`-Routine-`RoutineName

`intersystems-Group-`GroupName`-Namespace-`NamespaceName

`intersystems-Instance-`InstanceName`-Role-`RoleName

`intersystems-Instance-`InstanceName`-Routine-`RoutineName

`intersystems-Instance-`InstanceName`-Namespace-`NamespaceName

グループ名のプロパティ

グループ名は、以下の構成可能なプロパティで構成されます。

- OrganizationID ー 既定値は `intersystems` です。グループ名の `intersystems` セグメントをユーザ定義文字列または空文字列に置き換えます。例えば、`OrgABC` に設定した場合、グループ名は以下のようになります。

  `OrgABC-Role-`RoleName

  `OrgABC-Group-`GroupName`-Routine-`RoutineName

  `OrgABC-Instance`InstanceName`-Namespace-`NamespaceName

  空文字列に設定した場合、グループ名は以下のようになります。

  `Role-`RoleName

  `Group-`GroupName`-Routine-`RoutineName

  `Instance-`InstanceName`-Namespace-`NamespaceName

- DelimiterID ー 既定値は hyphen (-) です。これは、グループ名に含まれるセグメントを区切る区切り文字です。例えば、アンダースコア (_) に設定した場合、グループ名は以下のようになります。

  `intersystems_Role_`RoleName

  `intersystems_Group_`GroupName`_Routine_`RoutineName

  `intersystems_Instance_`InstanceName`_Namespace_`NamespaceName

- GroupID ー 既定値は `Group` です。例えば、`SystemGrouping` に設定した場合、グループ名は以下のようになります。

  `intersystems-SystemGrouping-`GroupName`-Role-`RoleName

  `intersystems-SystemGrouping-`GroupName`-Routine-`RoutineName

  `intersystems-SystemGrouping-`GroupName`-Namespace-`NamespaceName

- InstanceID ー 既定値は `Instance` です。例えば、`SystemInstance` に設定した場合、グループ名は以下のようになります。

  `intersystems-SystemInstance-`InstanceName`-Role-`RoleName

  `intersystems-SystemInstance-`InstanceName`-Routine-`RoutineName

  `intersystems-SystemInstance-`InstanceName`-Namespace-`NamespaceName

- RoleID ー 既定値は `Role` です。例えば、`SystemRole` に設定した場合、グループ名は以下のようになります。

  `intersystems-SystemRole-`RoleName

  `intersystems-Group-`GroupName`-SystemRole-`RoleName

  `intersystems-Instance-`InstanceName`-SystemRole-`RoleName

- NamespaceID ー 既定値は `Namespace` です。例えば、`SystemNamespace` に設定した場合、グループ名は以下のようになります。

  `intersystems-SystemNamespace-`NamespaceName

  `intersystems-Group-`GroupName`-SystemNamespace-`NamespaceName

  `intersystems-Instance-`InstanceName`-SystemNamespace-`NamespaceName

- RoutineID ー 既定値は `Routine` です。例えば、`SystemRoutine` に設定した場合、グループ名は以下のようになります。

  `intersystems-SystemRoutine-`RoutineName

  `intersystems-Group-`GroupName`-SystemRoutine-`RoutineName

  `intersystems-Instance-`InstanceName`-SystemRoutine-`RoutineName

プロパティの変更手順

これらのプロパティを変更するには、以下の手順を実行します。

1. 管理ポータルで、**[セキュリティ LDAP 構成]** ページ (**[管理ポータル]** > **[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[LDAP 構成]**) に移動します。
2. 構成を編集するには、構成の名前をクリックします。
3. このページでは、OrganizationID プロパティを編集できます。**[詳細設定]** をクリックし、残りのプロパティを表示して編集します。
4. ページの上部の **[保存]** をクリックして、変更を保存します。

3.2.3.3 さまざまな種類のグループの混合

単一インスタンス・ロールまたは複数インスタンス・ロールと組み合わせてユニバーサル・グループを使用できます。

例えば、以下のように仮定します。

- 複数のインスタンスに、あるアプリケーションがあります。
- ユニバーサル・グループを使用しています。
- すべてのインスタンスでアプリケーションを実行できますが、いずれのマシンでも管理者としてアプリケーションを使用することはできない UserOne というユーザが存在します。

UserOne が以下の操作を行えるようにします。

- 引き続き、すべてのインスタンスでアプリケーションを実行できる
- さらに、Test という特定のマシン上の APPTEST という特定のインスタンスでアプリケーションを管理できる

これを行うには、以下を実行します。

1. Test マシン上の APPTEST インスタンスの承認インスタンス ID を Test:APPTEST に設定します。
2. LDAP サーバで以下のグループを作成します。

   `intersystems-Instance-Test_APPTEST-Role-Administrator`

3. LDAP サーバでこのグループを UserOne に割り当てます。
4. Test マシン上の APPTEST インスタンスで管理者ロールを作成し、管理アクセス権を付与します。

他の方法で承認グループを組み合わせて使用することもできます。例えば、LDAP サーバに対して認証されるすべてのインスタンスで UserTwo が **`%All`** 許可を持っている場合、Server10 というマシン上の SECRET というインスタンスで UserTwo に排他管理許可を付与できます。そのためには、**[ユニバーサル・グループ・アクセスを許可]** を無効にし、`intersystems-Instance-Server10_SECRET-Role-Administrator` をそのユーザに割り当てるプロセスを実行します。

3.2.3.4 入れ子になったグループ

Active Directory LDAP サーバで、LDAP グループは入れ子になったグループと呼ばれるものをサポートします。入れ子になったグループは、親グループのメンバであるグループです。つまり、入れ子になったグループのメンバであるユーザはすべて、暗黙的に親グループのメンバでもあります。例えば、ABC と DEF と呼ばれる 2 つの LDAP グループが定義されているとします。ABC を、DEF 内の入れ子になったグループにすることができます。つまり、ユーザが ABC のメンバである場合、明示的に DEF グループに割り当てなくても、このグループのメンバになります。

ユーザの入れ子になったグループを検索すると、LDAP サーバ上でセキュリティ・グループとして定義されたグループのみが返されます。入れ子になったグループを使用する場合、InterSystems IRIS システムでロールとして使用するグループはセキュリティ・グループとして作成するようにしてください。

注釈　入れ子になったグループを使用しないシステムでは、セキュリティ・グループとディストリビューション・グループの両方が返されます。

3.2.3.5 LDAP グループによって InterSystems IRIS へのアクセスが規制される仕組み

ユーザは、LDAP グループを通じて、既定のネームスペースおよび既定のルーチンと共にロールを受け取ります。ユーザに付与されたロールに、インスタンスの必要なアクセス・ポイントに対する十分な特権がない場合、ユーザはそのインスタンスへのアクセスを拒否されます。例えば、既定のルーチンを使用する十分な特権がユーザにない場合、そのユーザはアクセスを拒否されます。

さらに、以下のルールが適用されます。

- ユーザがロールのグループに割り当てられていても、ユーザがログインしているインスタンスでそのロールが定義されていない場合、ユーザはそのインスタンスではそのロールを持ちません。
- ユーザが既定のルーチンのグループに割り当てられていても、ユーザがログインしているインスタンスでそのルーチンが定義されていない場合、ユーザはそのインスタンスには接続できません。
- ユーザが既定のネームスペースのグループに割り当てられていても、ユーザがログインしているインスタンスでそのネームスペースが定義されていない場合、ユーザはそのインスタンスには接続できません。

3.3 オペレーティング・システム・ベースの認証と併用する LDAP 承認の構成

トピックは以下のとおりです。

- オペレーティング・システム LDAP 認証
- InterSystems IRIS インスタンスでの OS/LDAP の有効化
- %Service_Console および %Service_Terminal サービスでの OS/LDAP の有効化
- 単一ドメインおよび複数ドメインによる OS/LDAP
- 入力要求を簡略化するための複数ドメインによる OS/LDAP の構成

3.3.1 オペレーティング・システム LDAP 認証

InterSystems IRIS では、オペレーティング・システム・ベースの認証をサポートするように構成することで、LDAP 経由の承認を実行できます。これは、オペレーティング・システム LDAP 承認または OS/LDAP と呼ばれます。これにより、ユーザは、オペレーティング・システム・ログインからの認証情報を使用して InterSystems IRIS に対して認証を行った後、

LDAP サーバから承認情報を取得することができます。オペレーティング・システム LDAP 承認は、Windows のコンソールと、UNIX®、Linux、および macOS のターミナルで使用できます。

OS/LDAP を構成する手順は以下のとおりです。

1. InterSystems IRIS インスタンスで OS ベースの認証と LDAP 承認を有効化します。
2. 標準の LDAP 認証と同様に、インスタンスにログインするために必要なロールを設定します。
3. %Service_Console および %Service_Terminal サービスで OS/LDAP を有効化します。
4. 承認を構成します。これは、LDAP 認証に追加する場合と同じ方法で行います。"InterSystems IRIS の LDAP 承認の構成" を参照してください。
5. 複数のドメインを使用する場合は、オプションで入力要求を簡略化するように OS/LDAP を構成します。

3.3.2 InterSystems IRIS インスタンスでの OS/LDAP の有効化

OS/LDAP を使用するには、まず、インスタンスで OS/LDAP を有効にします。

1. 管理ポータルのホーム・ページで、**[認証/Web セッション・オプション]** ページ (**[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[認証/Web セッション・オプション]**) に移動します。
2. **[認証/Web セッション・オプション]** ページで、**[オペレーティング・システム LDAP 認証を許可]** を選択します。
3. **[保存]** をクリックすると、変更内容が適用されます。

3.3.3 %Service_Console および %Service_Terminal サービスでの OS/LDAP の有効化

インスタンスの関連サービスまたはアプリケーションで OS/LDAP を有効にする手順は以下のとおりです。

1. インスタンスで LDAP 認証が有効になっている場合、OS/LDAP をサポートするサービスである **%Service_Console** および **%Service_Terminal** の **[サービス編集]** ページに **[オペレーティング・システム LDAP 承認]** チェック・ボックスが表示されます。
2. 必要に応じて、それらのサービスで LDAP 認証を有効にします。

3.3.4 単一ドメインおよび複数ドメインによる OS/LDAP

OS/LDAP では、単一ドメインまたは複数ドメインの使用がサポートされています。

1 つのドメインのみをサポートするように InterSystems IRIS が構成されている場合、以下のように動作します。

1. ユーザは、最初のログイン時にユーザ名とパスワードの入力を求められます。
2. それ以降のログインについては、オペレーティング・システムによってユーザが既に認証されているため、入力を求められることはありません。

複数のドメインをサポートするように InterSystems IRIS が構成されている場合、以下のように動作します。

1. ユーザは、最初のログイン時にユーザ名とパスワードの入力を求められます。
2. それ以降のログインについては、既定では、オペレーティング・システムによってユーザ名とパスワードの入力が求められます。この入力要求が行われないように InterSystems IRIS を構成できます。次のセクションを参照してください。

3.3.5 入力要求を簡略化するための複数ドメインによる OS/LDAP の構成

OS/LDAP と複数のドメインを使用する場合、入力要求を簡略化するようにインスタンスを構成できます。既定では、ユーザはログインのたびにユーザ名とパスワードの入力を求められます。ユーザが最初にログインするときにのみユーザ名/パスワードの入力が求められ、それ以降の接続は入力要求なしで認証されるように InterSystems IRIS を構成できます。

このように動作するように InterSystems IRIS を構成する手順は以下のとおりです。

1. それぞれのユーザについて、ユーザが認証されるドメインの値を持つ環境変数 ISC_LDAP_CONFIGURATION を作成します。
2. ユーザが認証される各ドメインについて、以下の手順を実行します。
   a. LDAP 構成があることを確認するか、LDAP 構成を作成します。
   b. その LDAP 構成について、**[ISC_LDAP_CONFIGURATION 環境変数を許可]** チェック・ボックスにチェックを付けます。これにより、この環境変数を使用できるようになります。

3.4 LDAP 属性を使用した承認の構成

LDAP 承認には、LDAP グループを使用することをお勧めします。ただし、インターシステムズでは、LDAP 属性を使用した承認もサポートしています。承認情報を格納するために LDAP スキーマで使用できる OID が 3 つ登録されています。それぞれには、以下のような固有の目的があります。

- intersystems-Namespace ー ユーザの既定のネームスペースの名前 (OID 1.2.840.113556.1.8000.2448.2.1)。
- intersystems-Routine ー ユーザの既定のルーチンの名前 (OID 1.2.840.113556.1.8000.2448.2.2)。
- intersystems-Roles ー ユーザのログイン・ロールの名前 (OID 1.2.840.113556.1.8000.2448.2.3)。

これらの属性を使用するには、LDAP サーバで以下の手順を実行します。

1. 属性を有効にして使用できるようにします。そのためには、LDAP スキーマの objectClass フィールドで、その値のリストに `intersystemsAccount` の値を付加してこのフィールドの値を変更します(`intersystemsAccount` には 1.2.840.113556.1.8000.2448.1.1 という LDAP OID が設定されています)。
2. このフィールドを (必要なだけ) スキーマに追加します。
3. LDAP データベースのエントリにそれらの値を生成します。

注釈　登録済みの LDAP スキーマ名を使用する必要はありません。実際、使用している LDAP スキーマにある既存の属性を使用できます。

例えば、UNIX® LDAP サーバでは、InterSystems IRIS での LDAP 認証の使用に関するスキーマを定義するために、以下の定義に示されている内容を使用します。

```
# Attribute Type Definitions

attributetype ( 1.2.840.113556.1.8000.2448.2.1 NAME 'intersystems-Namespace'
       DESC 'InterSystems Namespace'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE )

attributetype ( 1.2.840.113556.1.8000.2448.2.2 NAME 'intersystems-Routine'
        DESC 'InterSystems Routine'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} SINGLE-VALUE )

attributetype ( 1.2.840.113556.1.8000.2448.2.3 NAME 'intersystems-Roles'
        DESC 'InterSystems Roles'
        EQUALITY caseIgnoreMatch
```

```
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# Object Class Definitions

objectclass ( 1.2.840.113556.1.8000.2448.1.1
        NAME 'intersystemsAccount'
        SUP top
        AUXILIARY
        DESC 'Abstraction of an account with InterSystems attributes'
        MAY (
                intersystems-Routine $
                intersystems-Namespace $
                intersystems-Roles
        )
)
```

このコンテンツは以下の 2 か所に配置します。

- /etc/openldap/schema/ ディレクトリの intersystems.schema ファイルに配置します。
- 他のコンテンツと共に、/etc/openldap/slapd.conf ファイルに組み込みます。

4

LDAP に関するその他のトピック

4.1 安全なアウトバウンド LDAP 接続の作成

このドキュメントでは主に、InterSystems IRIS に接続する際の認証と承認での LDAP の使用について説明していますが、InterSystems IRIS から LDAP サーバに接続することもできます。LDAP サーバへの安全なアウトバウンド接続を確立するために、InterSystems IRIS は TLS をサポートしています。このトピックの詳細は、Init メソッドのコンテンツにある %SYS.LDAP のクラス・ドキュメントを参照してください。

4.2 LDAP API の使用法

%SYS.LDAP クラスでは、プログラムによって LDAP がサポートされます。

UNIX® の認証で InterSystems IRIS LDAP API を使用していて、詳細なデバッグ情報が必要な場合、OpenLDAP パッケージの一部である ldapsearch プログラムを使用できます。認証に関する問題を修正したら、構成のテスト・ツールを使用して、接続が機能していることを確認できます。ldapsearch プログラムは、LDAP 接続の他の問題のデバッグにも役に立つ場合があります。

4.3 さまざまな LDAP アクションの動作

このセクションでは、LDAP 認証および承認に関連する特定のプロセス中に行われる処理について説明します。

- LDAP で認証および承認が実行される仕組み
- LDAP データベース内でターゲット・ユーザが検索される仕組み
- インスタンスで LDAP アカウントの条件に基づいてローカル・アカウントがチェックおよび削除される仕組み

4.3.1 LDAP で認証および承認が実行される仕組み

LDAP 認証を使用する InterSystems IRIS のインスタンスに対して認証を試行するプロセスは以下のようになります。

1. ユーザは、ユーザ名とパスワードの入力を要求されます。認証を試行するこのユーザはターゲット・ユーザと呼ばれます。

2. InterSystems IRIS は、[検索に使用するLDAPユーザ名] と [LDAPユーザ名パスワード] に指定された値を使用して、LDAP サーバへの接続を確立します。InterSystems IRIS が情報を取得できるように LDAP データベースを検索する特権を持つこのユーザは検索ユーザと呼ばれます。
3. 接続が確立されると、次に、[LDAPユニーク検索属性] を使用して LDAP データベース内でターゲット・ユーザが検索されます。
4. LDAP データベース内でターゲット・ユーザが見つかると、そのユーザに関連付けられた属性 (ユーザのロール、ネームスペース、ルーチンなど) が取得されます。
5. その後で、InterSystems IRIS は LDAP データベースに対してユーザの認証を試行します。このとき、手順 1 で入力したユーザ名とパスワードが使用されます。
6. 認証が成功すると、LDAP サーバで (グループ割り当てまたは属性を使用して) 承認が行われます。ユーザはその後、ロールおよび公開されている利用可能なリソースに関連付けられた特権に基づいて InterSystems IRIS と対話できます。管理ポータルに表示されるユーザのプロパティは読み取り専用で、InterSystems IRIS 内で編集することはできません。

4.3.2 LDAP データベース内でターゲット・ユーザが検索される仕組み

InterSystems IRIS が検索ユーザとして LDAP サーバへの接続を確立したら、次にターゲット・ユーザに関する情報を取得します。そのために、InterSystems IRIS は、ログイン時に入力されたユーザ名を LDAP Unique search attribute に対する LDAP データベース内の値と照合して確認します。この属性の名前は多くの場合、Active Directory LDAP サーバでは “sAMAccountName”、OpenLDAP サーバでは “uid” です。

InterSystems IRIS によりユーザが検索されると、属性情報が取得されます。InterSystems IRIS により、InterSystems IRIS LDAP 構成フィールド (″LDAP 構成の作成または変更″ で説明しています) で指定された各属性に関する情報が取得され、各属性に関連付けられたすべての値が取得されます。InterSystems IRIS では、InterSystems IRIS LDAP 構成フィールド内でユーザに指定されたすべての属性に関連付けられているすべての値が取得されることに注意してください。サブセットのみを取得するように構成することはできません。

4.3.3 インスタンスで LDAP アカウントの条件に基づいてローカル・アカウントがチェックおよび削除される仕組み

アカウントが以下のいずれかの条件を満たす場合、InterSystems IRIS ではローカル・インスタンスのユーザ・アカウントが削除されます。

- LDAP アカウントが既に存在しない
- LDAP アカウントが無効である
- Active Directory のみで、LDAP アカウントにパスワードの変更を要求するフラグが設定されている
- Active Directory のみで、LDAP アカウントが失効している

InterSystems IRIS は、以下の状況でこれらの条件をチェックし、アカウントを削除します。

- ユーザが InterSystems IRIS インスタンスにログインしようとすると、インスタンスによってユーザの LDAP アカウントがチェックされます。LDAP アカウントについて、記載された条件のいずれかを満たす場合、InterSystems IRIS はローカル・ユーザ・アカウントを削除します。
- セキュリティ・スキャン・タスクの結果として。InterSystems IRIS にはこのタスクが用意されています。タスクを実行して、ローカル・ユーザ・アカウントに関連付けられた LDAP アカウントについて、これらのいずれかの条件を満たすかどうかを確認します。いずれかの条件を満たす場合、InterSystems IRIS はローカル・ユーザ・アカウントを削除します。