認証メカニズムの概要

Version 2024.1
2024-06-03

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

認証メカニズムの概要

InterSystems IRIS Data Platform　Version 2024.1　2024-06-03

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

目次

図一覧

認証メカニズムの概要

1 認証について

認証は、InterSystems IRIS® に接続しようとしているあらゆるユーザやその他のエンティティの身元を確認するプロセスです。よく言われるように、認証は、自分が自身で主張するとおりの人物であることを証明する方法です。

認証されたユーザは、InterSystems IRIS との接続を確立し、そのデータとツールを使用できるようになります。信頼できる認証がないと、あるユーザが他人になりすまして不正に入手した特権を利用できるため、承認が無意味なものになります。

2 認証メカニズム

ユーザを認証するための方法がいくつかあり、それぞれを認証メカニズムといいます。InterSystems IRIS では、以下のようなさまざまな認証メカニズムがサポートされています。

- Kerberos ー Kerberos プロトコルは、安全でないネットワーク上でサービスに対する安全な認証を提供することを目的として設計されました。Kerberos では、チケットを使用してユーザが認証され、ネットワーク上でのパスワードの交換が回避されます。
- オペレーティング・システム・ベース ー OS ベースの認証では、オペレーティング・システムでユーザごとに割り当てられている身元情報を使用して、InterSystems IRIS 向けにユーザを識別します。
- インスタンス認証 ー インスタンス認証では、ユーザにパスワードを要求し、ユーザが入力したパスワードのハッシュ値を格納値と比較します。
- Lightweight Directory Access Protocol (LDAP) ー LDAP により、InterSystems IRIS では LDAP サーバとして知られる一元管理リポジトリにある情報に基づいてユーザを認証します。
- 代行認証 ー 代行認証により、カスタマイズされた認証メカニズムを作成する方法が実現します。アプリケーション開発者は、代行認証コードのコンテンツを完全に制御します。

認証を一切実行せずに、すべてのユーザが InterSystems IRIS に接続できるようにすることも可能です。これを、認証なしアクセスといいます。認証なしアクセス・オプションは、外部との境界が強力に保護されている組織や、アプリケーションとデータの両方が攻撃の対象としてまったく興味を引かない場合に適用できます。

通常、認証なしアクセスを許可するようにインターシステムズの製品やサービスを構成する場合は、認証なしアクセスのみを使用することをお勧めします。認証メカニズムと、認証失敗時に適用する認証なしアクセスの両方をサポートする場合、この手法をカスケード認証といいます。詳細は、"カスケード認証" を参照してください。複数の認証メカニズムを使用する状況は、"複数の認証メカニズムの使用" を参照してください。通常、InterSystems IRIS はこれら認証メカニズムのうち 1 つのみを使用するように構成されます。

3 認証の仕組み

認証メカニズムは接続ツールで使用されます。これらのツールは、ユーザが InterSystems IRIS との接続を確立するための手段を指定します。それぞれの接続ツール (ターミナル、Java、Web など) はインターシステムズのサービスを使用し

ますが、このサービスは、サポートされる認証メカニズムを指定するために管理者が使用できるものです(インターシステムズのサービスは、InterSystems IRIS への接続を許可または拒否する機能を持ちます。サービスの詳細は、"サービス"を参照してください)。

接続ツールは 3 種類に分類でき、それぞれをアクセス・モードといいます。アクセス・モードごとに、独自の特性と独自のサポート対象のサービスがあります。アクセス・モードには以下のものがあります。

- ローカル ー ユーザは、InterSystems IRIS の実行可能プログラムが実行されているマシン上で、その実行可能プログラムを直接操作します。
- クライアント・サーバ ー ユーザは、InterSystems IRIS に接続する独立した実行可能プログラムを操作します。
- Web ー ユーザは Web ブラウザを使用して、Web ベースのアプリケーションを通じて InterSystems IRIS を操作します。

エンドユーザは接続ツールを使用し、特定の認証メカニズムによって特定のアクセス・モードで InterSystems IRIS を操作します。この章で説明しているプロセスそのものでは、認証されたアクセスは確立されません。これらのプロセスで確立されるのは、特定のアクセス・モードで特定の機構を通じてユーザを認証するときにアプリケーションで使用されるインフラストラクチャです。

3.1 さまざまなアクセス・モードについて

3.1.1 ローカル・アクセス・モード

ローカル・アクセスでは、InterSystems IRIS サーバと同じマシン上にエンドユーザが存在します。ユーザがデータにアクセスするには、共有メモリとの間で読み取りと書き込みを実行する InterSystems IRIS のプライベート・イメージを実行します。複数のローカル・ユーザが存在する場合、それぞれのユーザは InterSystems IRIS の実行可能プログラムの個人用コピーを使用し、これらすべての実行可能プログラムは同じ共有メモリを参照します。ユーザと実行可能プログラムが同じマシン上に存在することから、両者の間の通信を保護したり、暗号化したりする必要がありません。これは、この実行可能プログラムと他の実行可能プログラムとの間で情報が受け渡されることがないからです。ユーザと InterSystems IRIS との間の通信が単独のプロセスの範囲で処理されるので、この認証をプロセス内認証ともいいます。

ローカル・アクセスは以下の場合に利用できます。

- ターミナル ー Windows の場合は **%Service_Console**、その他のオペレーティング・システムの場合は **%Service_Terminal**
- コールイン ー **%Service_CallIn**

3.1.2 クライアント・サーバ・アクセス モード

クライアント・サーバ・アクセスでは、InterSystems IRIS の実行可能プログラムはサーバであり、そのサーバから独立したマシンに、クライアント側の実行可能プログラムを置くことができます。InterSystems IRIS は、多くの場合はネットワーク経由でこのクライアントとの接続を受け入れます。この接続では、InterSystems IRIS でサポートされているものであれば、どのような言語またはプロトコルも使用できます。これには、以下のものがあります。

- ComPort ー **%Service_ComPort**
- Java ー **%Service_Bindings**
- JDBC ー **%Service_Bindings**
- ODBC ー **%Service_Bindings**
- Telnet ー **%Service_Telnet**

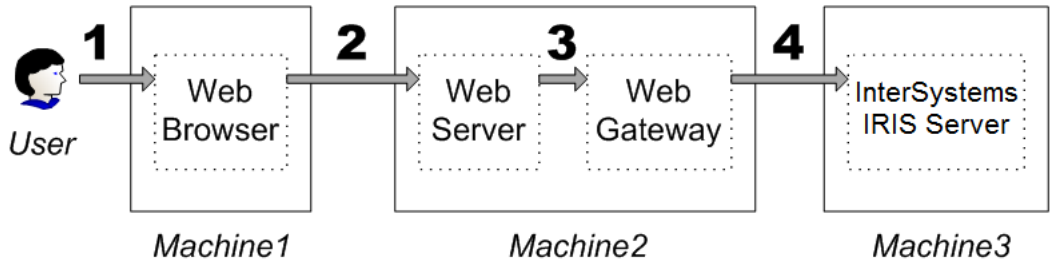
インスタンス認証を介した認証のみをサポートする **%Service_ComPort** を除くすべての接続ツールは、Kerberos またはインスタンス認証をサポートします。

どの場合でも、サポートされる認証タイプはサーバで指定されています。クライアントがサーバに対するアクセスを開始するときは、これらのサポートされている認証タイプのいずれかを使用する必要があります。他のタイプを使用すると、接続が拒否されます。接続ツールによっては、一部の認証タイプを使用できないことがあります。

3.1.3 Web アクセス・モード

Web アクセス・モードでは、以下の形式の接続がサポートされています。

図 1: Web 接続のアーキテクチャ



1. Web ブラウザで、ユーザがコンテンツまたはアクションを要求します。
2. ユーザの要求が Web ブラウザから Web サーバに渡されます。
3. Web ゲートウェイが Web サーバと同じ場所に置かれていて、ユーザの要求が Web ゲートウェイに渡されます。
4. ユーザの要求が Web ゲートウェイから InterSystems IRIS サーバに渡されます。

ユーザに関連したコンテンツが InterSystems IRIS サーバから提供されたとき、またはユーザに関連したアクションが InterSystems IRIS サーバで実行されたとき、上記と逆方向で同じプロセスが発生します。

InterSystems IRIS に認証されるユーザにとって、ユーザ名とパスワードは完全な形で渡される必要があります。このことから、このアクセス・モードはプロキシ・モードまたはプロキシ接続とも呼ばれます。InterSystems IRIS を実行しているマシンに情報が到達すれば、ユーザとサーバとの関係はローカル・アクセス・モードの場合と似たものになります。実際、Web アクセス・モードでは、プロセス内認証も使用されます。

4 認証の設定の概要

1. 認証メカニズムを選択します。認証の要件とアクセス・モードに基づいて選択できます。
2. 以下の手順に従って、認証を構成します。
   - Kerberos 認証
   - オペレーティング・システム・ベースの認証
   - インスタンス認証
   - LDAP 認証
   - 代行認証
3. オプションで 2 要素認証を実装します。
4. オプションで JSON Web トークン (JWT) 認証を実装します。

使用する認証メカニズムを InterSystems IRIS インスタンスごとに 1 つのみとすることと、InterSystems IRIS をインストールする前にインスタンスの認証メカニズムを選択しておくことをお勧めします。インストールを開始すると、選択した認証メカニズムを使用するように InterSystems IRIS を構成する作業を開始できます。この作業では以下の手順が必要です。

- Kerberos 認証の場合は、すべての InterSystems IRIS ユーザが、Kerberos の KDC (Key Distribution Center) または Windows のドメイン・コントローラに記録されていることを確認します。
- オペレーティング・システム・ベースの認証の場合は、すべての InterSystems IRIS ユーザがオペレーティング・システムのリストに記録されていることを確認します。
- すべての認証メカニズムについて、選択した認証メカニズムのみが使用されるように、サポート対象のすべてのサービスを構成します。
- すべての認証メカニズムについて、サポートされていないすべてのサービスを無効にします。
- すべての認証メカニズムについて、選択した認証メカニズムのみが使用されるように、すべてのアプリケーションを構成します。

注釈　選択した認証メカニズムに関係なく、起動するときとシャットダウンするときは、必ずオペレーティング・システムの認証が使用されます。