インターシステムズの承認について

Version 2024.1
2024-06-03

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

インターシステムズの承認について
InterSystems IRIS Data Platform　Version 2024.1　2024-06-03

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

インターシステムズの承認について

ユーザが認証された後、セキュリティに関連する次の手順は、そのユーザに使用、閲覧、または変更が認められている資源が何であるかを判断することです。Assets（資源）には、以下のものが含まれます。

- データベース ― データまたはコードが含まれる物理ファイル。
- サービス ― InterSystems IRIS に接続するためのツール（例 ： クライアント・サーバ・サービス、Telnet）。
- アプリケーション ― InterSystems IRIS プログラム（例 ： Web アプリケーション）。
- 管理アクション ― タスクのセット（例: InterSystems IRIS の開始および停止、バックアップの作成）。

組織のすべてのユーザがシステム上のあらゆる資源を表示して変更できる状況は望ましくありません。資源へのアクセスの決定と制御を承認と呼びます。

ユーザと資源との関係を承認で管理します。InterSystems IRIS® のデータ・プラットフォームでは、この関係をリソースとして表現します。InterSystems IRIS では、その承認モデルとしてロールベースのアクセス制御（RBAC）を採用しています。このモデルでは、システム管理者がタスクベースの 1 つ以上のロールにユーザを割り当てます。各ロールには、リソースの特定の組み合わせを使用して、アクティビティの特定の組み合わせを実行することが認められています。アプリケーションで、ユーザが持つロールを一時的に拡張できます。

このページでは、InterSystems IRIS に実装されている RBAC 承認モデルの概要について説明します。実際の操作を通じたインターシステムズの RBAC の説明は、"Configuring Role-Based Access" を参照してください。

1 リソース、許可、および特権

セキュリティの最大の目的は、情報や機能である資源を何らかの形式で保護することです。InterSystems IRIS データ・プラットフォームでは、データベース、サービス、アプリケーション、ツールなどのほか、管理アクションも資源と捉えることができます。

InterSystems IRIS では各資源はリソースで表現され、1 つのリソースが複数の資源を表すこともあります。

システム管理者は、リソースに許可を割り当てることで、資源へのアクセスを制御します。許可を付与または取り消すことで、リソースが表現している資源に対して実行できるアクティビティへのアクセスを有効または無効にします。データベースの場合、許可は Read と Write です。その他ほとんどのリソース・タイプで関連する許可は Use です。

リソースとそれに関連する許可の組み合わせを特権といいます。これは、多くの場合、以下の省略表現を使用して記述されます。`Resource-Name:Permission`。例えば、EmployeeInfo データベースに対する読み取り許可と書き込み許可を付与する特権は、以下のように表現できます。`%DB_EmployeeInfo:Read,Write` または `%DB_EmployeeInfo:RW`。

詳細は、"リソースの使用による資源の保護" と "特権および許可" を参照してください。

2 ユーザとロール

インターシステムズのロールベースのアクセス制御モデルでは、以下のようにユーザがリソースを操作できます。

1. 前のセクションの説明のとおり、許可にリソースを関連付けて特権を確立します。
2. 特権の集合をロールに関連付けます。

3. ロールに、ユーザなどのメンバを割り当てます。

ユーザは InterSystems IRIS に接続して一連のタスクを実行します。ロールは、ユーザが持つ一連の特権を記述するものであり、したがってユーザが実行できるタスクを表すと言えます。

ロールは、ユーザと特権を仲介する機能を提供します。ユーザの人数に応じて数多くの特権のセットを作成する代わりに、ロールを使用すれば、タスク固有の特権のセットを作成できます。ロールで保持された特権を付与、変更、削除できます。この内容は、そのロールに関連するすべてのユーザに自動的に伝播されます。特権のセットを個人ユーザや全ユーザごとに管理するのではなく、ロールを極めて少ない数に抑えて管理することになります。

例えば、病院向けのアプリケーションには、巡回を担当する医師 (**RoundsDoctor**) のロールと救急処置室に勤務する医師 (**ERDoctor**) のロールがあり、それぞれのロールに適切な特権が関連付けられています。

個々のユーザを複数のロールのメンバとすることができます。上記の例を使用すると、病院の医長は、すべての診療科の医師が使用する機能を必要とすることがあります。このユーザには、**RoundsDoctor** ロールと **ERDoctor** ロールの両方を割り当てることが考えられます。また、これら両方のロールのメンバであると同時に、それに応じて特権を継承した **MedicalDirector** ロールをシステム管理者が作成することもできます。

ロールベースのアクセス制御によるネイティブな InterSystems の実装は、InterSystems IRIS がサポートするすべてのタイプの認証メカニズム (LDAP、Kerberos、OS ベースなど) で使用できます。また、LDAP や代行認証を使用してロールを割り当てることもできます。詳細は、"ロール" および "ユーザ・アカウント" を参照してください。

3 アプリケーション

インターシステムズのセキュリティは、柔軟なアプリケーション・セキュリティ・モデルを提供します。アプリケーションを使用する機能も 1 つのリソースであるため、特定のアプリケーションの使用を特定のユーザ・グループに限定することも、すべてのユーザが使用できるようにすることもできます。アプリケーションを使用できるユーザについては、セキュリティ・モデルではロール・エスカレーション・モデルがサポートされます。つまり、ユーザはアプリケーションを使用している間は、通常であればアクセスできない特定のリソースにアクセスできます。

複数タイプのアプリケーションの詳細は、"アプリケーション" を参照してください。