システム管理およびセキュリティ

Version 2023.1
2024-01-02

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

システム管理およびセキュリティ
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

システム管理およびセキュリティ

このページでは、InterSystems IRIS® データ・プラットフォームの管理ポータルへのアクセス、およびポータルのその他のセキュリティ関連機能について説明します。

1 InterSystems IRIS のセキュリティ・ドメインの管理

インターシステムズのセキュリティ・ドメインでは、Kerberos レルムと Windows ドメインに対応するグループにユーザが分類されます。Kerberos を使用しているインスタンスの場合、その InterSystems IRIS ドメインは Kerberos レルムに対応しています。Windows ドメインを使用している場合は、そのドメインが Kerberos レルムに対応します。

セキュリティ・ドメインの名前は、インターネット・ドメインの名前と同じ形式をとることが普通ですが、必ずしもこれは必須ではありません。セキュリティ・ドメイン名には、アット・マーク (@) 以外のあらゆる文字を使用できます。

1.1 単一ドメインと複数ドメイン

InterSystems IRIS は、単一ドメインまたは複数ドメインの使用をサポートしています。

単一ドメインまたは複数ドメインのサポートを指定するには、"システム規模のセキュリティ・パラメータ" で説明されている、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]**) の **[複数セキュリティドメインを許可する]** フィールドを使用します。

単一ドメインを持つインスタンスでは、以下のようになります。

- $USERNAME 変数にはドメイン名は含まれていません。
- システム・ユーティリティでユーザ名を表示すると、ドメイン名は表示されません。
- 既定のドメイン以外のドメインにあるユーザ名を指定することはできません (以下のセクションで説明します)。

複数ドメインを持つインスタンスでは、以下のようになります。

- $USERNAME 変数にはドメイン名が含まれています。
- システム・ユーティリティでユーザ名を表示すると、ドメイン名も表示されます。これには、**[ ]** ページ (**[セキュリティ管理]** > **[セキュリティ]** > **[ユーザ]**) も含まれます。
- ユーザは、各自のドメインにおける完全修飾名 (documentation@intersystems.com など) を使用してログインします。完全修飾名の最初の部分を共有し、ドメイン名が異なる 2 つのアカウントがある場合、これらは 2 つの別個のユーザ・アカウントとして格納されます (それぞれに独自の属性があり、これらの属性に異なる値を指定できます)。
- ユーザ名を編集することはできません。

1.2 既定のセキュリティ・ドメイン

インスタンスごとに既定のセキュリティ・ドメインがあります。ユーザ名にドメインが指定されていない場合には、既定のドメイン名が使用されていると見なされます。例えば、既定のドメインが “intersystems.com” である場合、“info” と “info@intersystems.com” は同じものを指します。InterSystems IRIS をインストールすると、このパラメータの初期値にはローカル・ドメイン名が使用されます。

複数のセキュリティ・ドメインを持つインスタンスでは、"システム規模のセキュリティ・パラメータ" のセクションで説明されているように、[**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**]) の [**デフォルトセキュリティドメイン**] フィールドを使用して既定のセキュリティ・ドメインを新規に選択できます。

1.3 セキュリティ・ドメインのリスト、作成、編集、削除

[**LDAP 構成**] ページには、インスタンスの既存のセキュリティ・ドメインと構成がリストされ、構成やドメインを作成したり、既存のドメインや構成を変更したり、削除したりできます。

1.3.1 セキュリティ・ドメインのリスト

インスタンスのドメインのリストを表示するには、[**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。このページには、ドメインごとに以下の情報が表示されます。

- [**ログインドメイン名**] – ドメインの名前。クリックすると、ドメインのプロパティを編集できます。
- [**LDAP 有効**] – このドメインで LDAP 接続を有効にするかどうか。
- [**説明**] – ドメインの説明。
- [**削除**] リンク – 確認後、ドメインをインスタンスから削除します。

注釈　インスタンスで Kerberos が有効になっている場合、このページに移動するには、メニュー [**LDAP/Kerberos 構成**] を選択します。ページの名前は [**セキュリティ LDAP/Kerberos 構成**] です。

1.3.2 セキュリティ・ドメインの作成

使用するインスタンスのドメインを作成するには、そのドメインを指定する LDAP 構成を作成します。LDAP 構成を作成すると、ドメインが作成されます。

1. [**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. [**新しい LDAP 構成を作成**] ボタンをクリックします。このボタンを選択すると、[**LDAP 構成を編集**] ページが表示されます。
3. [**LDAP 構成を編集**] ページで、[**ログインドメイン名**] とオプションの説明を入力します。
4. 他の構成フィールドに値を入力して [**保存**] をクリックし、構成とドメインを作成します。

注釈　インスタンスで Kerberos が有効になっている場合、このページに移動するには、メニュー [**LDAP/Kerberos 構成**] を選択します。ページの名前は [**セキュリティ LDAP/Kerberos 構成**] です。

1.3.3 セキュリティ・ドメインの編集

ドメインを編集するには、以下の手順を実行します。

1. [**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. [**ログインドメイン名**] をクリックして、ドメインとその構成フィールドを編集します。
3. [**保存**] をクリックして、変更した構成とドメインを保存します。

注釈　1. ドメインの名前は変更できません。または、目的の名前のドメインが必要な場合は、その名前でドメインを新規に作成した後で既存のドメインを削除します。

2. インスタンスで Kerberos が有効になっている場合、このページに移動するには、メニュー [LDAP/Kerberos 構成] を選択します。ページの名前は [セキュリティ LDAP/Kerberos 構成] です。

1.3.4 セキュリティ・ドメインの削除

ドメインを削除するには、以下の手順を実行します。

1. [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。ドメインのリストが表示されます。
2. ドメインの行で [削除] をクリックします。
3. 削除を確認します。

注釈　インスタンスで Kerberos が有効になっている場合、このページに移動するには、メニュー [LDAP/Kerberos 構成] を選択します。ページの名前は [セキュリティ LDAP/Kerberos 構成] です。

2 パスワードの強固さとパスワードのポリシー

InterSystems IRIS では、以下の形式の文字列を使用することでユーザ・パスワードに対する要件を指定できます。

```
X.Y[ANP]
```

以下はその説明です。

- X は、パスワードに使用する文字の最小数です。
- Y は、パスワードに使用する文字の最大数です。
- A、N、および P は、それぞれアルファベット文字、数字、および句読点文字をパスワードに使用できるかどうかを指定します。

これらの規則は、ObjectScript のパターン・マッチング機能に基づいています。この機能は、"パターン・マッチング" で説明されています。

注釈　このパラメータの設定によって、既存のパスワードが影響を受けることはありません。

2.1 管理者パスワードに推奨される強固さ

管理者パスワードは、大文字と小文字のアルファベット文字、数字、および句読点文字が無作為に混在したものとすることが理想的です。このようなランダムな文字を使用して、最低でも 12 文字のパスワードを使用することを強くお勧めします。

3 緊急アクセス

InterSystems IRIS には、特定の緊迫した状況下で使用できる特別な緊急アクセス・モードが用意されています。このような状況としては、セキュリティ構成情報に深刻な損傷が発生した場合、**%Admin_Manage:Use** 特権または

%Admin_Security:Use 特権を持っているユーザが存在しない場合 (つまり、すべてのユーザがロックアウトされている場合) などがあります。InterSystems IRIS には、このような事態を回避するために **%All** ロールを付与されたユーザを常に 1 人以上確保する仕組みがありますが、そのユーザが不在であることや、そのユーザがパスワードを忘れてしまうこともあります。

InterSystems IRIS のインスタンスへの緊急アクセスを取得するには、インスタンスが実行されている場所で root 特権または管理者特権 (インスタンスを root でインストールした場合) を持っているか、インスタンスをインストールしたユーザである必要があります (インスタンスを root でインストールしていない場合)。このような要件があるため、緊急アクセスは、インスタンスに対する管理操作 (新しいインスタンスを既存のインスタンス上にインストールするなど) を実行するための十分な特権を既に持っているユーザに限られます。

緊急アクセスに関するトピック:

- 緊急アクセスの仕組み
- Windows での緊急アクセス・モードの呼び出し
- UNIX®、Linux、および macOS での緊急アクセス・モードの呼び出し

3.1 緊急アクセス・モードの仕組み

InterSystems IRIS が緊急アクセス・モードで動作しているとき、アクセスが許可されるユーザは 1 人のみです (このユーザを緊急ユーザといいます)。このユーザ名は、InterSystems IRIS 内であらかじめ定義されていなくてもかまいません。インスタンスに既に緊急ユーザと同じ名前を持つユーザ・アカウントがある場合、緊急ユーザは、既存の標準ユーザ・アカウントの特権ではなく、緊急アクセス・モードに関連する特権を持ちます。

緊急ユーザのアカウントとパスワードは、緊急モードでの 1 回の起動のみに対して有効です。緊急ユーザに指定したユーザ名が、InterSystems IRIS のインスタンスで以前に定義したユーザ名である場合、システムを通常モードで再起動すると、以前に定義したそのユーザの元のパスワードとセキュリティ特権が復元されます。緊急ユーザに指定したユーザ名が新規である場合、InterSystems IRIS を通常モードで再起動するときに、その新規ユーザのアカウントが無効であっても、そのユーザのログイン資格情報とセキュリティ特権が保存されます。

Tipヒント **%ALL** ロールが登録された休眠アカウントが InterSystems IRIS のインスタンスに蓄積されないように、緊急ユーザには、新規ユーザ名ではなく以前に定義したユーザ名を使用することをお勧めします。これにより、複数の管理者がいるシステムでは、それぞれの管理者がそのユーザ名を使用して緊急アクセス・モードを初期化するのであれば、緊急アクセス・モード中に発生した変更の作成情報を、ログを通じて追跡することもできます。

緊急アクセス・モードの InterSystems IRIS には、以下の制約と機能があります。

- 緊急ユーザのみにアクセスが許可されます。他のユーザはログインできません。緊急ユーザは **%ALL** ロールを保持します。
- インスタンス認証を使用するアクセスのみになります。他の認証メカニズムはサポートされません。2 要素認証は無効になります。これによって、2 要素認証で緊急ユーザが認証できない状況が回避されます。
- Web アプリケーションでポータル (/csp/sys および /csp/sys/*) を制御する場合、カスタム・ログイン・ページが利用できても、緊急アクセス中には標準のログイン・ページ (%CSP.Login.cls) が使用されます。カスタム・ログイン・ページでは認証が行われなくなる場合があるので、これによって緊急ユーザが確実にポータルにアクセスできるようにします。他の Web アプリケーションの場合、カスタム・ログイン・ページがあると、そのページが緊急ログインの際に使用されます。
- 緊急アクセスによるログイン後、InterSystems IRIS は、アクティブ・プロセスに対するすべてのイベントの監査を試みます。これが不可能であっても、InterSystems IRIS の起動は継続します。緊急アクセス・モードでのログインの失敗は、監査されません。
- 有効になっているサービスは、コンソール、ターミナル、および Web ゲートウェイ (**%Service_Console**、**%Service_Terminal**、および **%Service_WebGateway**) のみです。それ以外のサービ

スはすべて無効化されます。これによって、緊急モード以外のモードで InterSystems IRIS が起動するときに、サービスの有効または無効の状態が変化することはありません。影響を受けるのは、現時点 (緊急モード) でメモリにある、サービスに関する情報のみです。

- 有効なサービスに対しては、認証されたアクセスのみが許可されます。該当のサービスに対しては InterSystems IRIS 独自のパスワード認証が使用されるので、緊急ユーザのユーザ名とパスワードを使用する必要があります。
- 緊急ユーザは InterSystems IRIS の構成を変更できますが、その変更が有効になるのは、次回に InterSystems IRIS を通常のモードで起動したときです。緊急モードで起動しても有効になりません。これは、InterSystems IRIS の通常の動作とは異なる点です。通常の動作では、InterSystems IRIS を再起動しなくても、構成の変更はほとんどその場で有効になります。

3.2 Windows での緊急アクセス・モードの呼び出し

InterSystems IRIS を緊急アクセス・モードで起動するには、ユーザは管理者グループのメンバである必要があります。以下の手順を実行します。

1. コマンド・プロンプトを起動して、管理者として実行します。以下のいずれかの方法で行います。
   - Windows コマンド・プロンプト・プログラム。メニューの **[コマンド プロンプト]** 選択項目を右クリックして、**[管理者として実行]** を選択します。
   - Windows PowerShell。管理者または他の特権のないユーザとしてこれを実行できますが、この手順では管理者として実行していることを想定しています。他の特権のないユーザとして実行するには、コマンドを呼び出すときに `-verb runas` 引数を使用します。PowerShell のドキュメントを参照してください。
2. InterSystems IRIS のインストール先にある bin ディレクトリに移動します。
3. このディレクトリで、コマンド行から適切なスイッチを使用し、緊急ユーザのユーザ名とパスワードを指定して、InterSystems IRIS を呼び出します。これは、使用しているコマンド・プロンプトによって決まります。
   - Windows コマンド・プロンプトの場合のコマンドは以下のとおりです。

     ```
     iris start <instance> /EmergencyId=<username>,<password>
     ```

     これにより、ユーザが 1 人だけ認められる緊急モードの InterSystems IRIS セッションが開始します。各パラメータは以下のとおりです。
     - 〈instance〉 は、緊急モードで開始するインスタンスを指定します。
     - 〈username〉 は、システムの唯一のユーザです。
     - 〈password〉 は、そのユーザのパスワードです。
   - Windows PowerShell の場合のコマンドは以下のとおりです。

     ```
     start-process .\iris.exe -ArgumentList "start <instance> /EmergencyId=<username>,<password>"
     ```

     これにより、ユーザが 1 人だけ認められる緊急モードの InterSystems IRIS セッションが開始します。各パラメータは以下のとおりです。
     - 〈instance〉 は、緊急モードで開始するインスタンスを指定します。
     - 〈username〉 は、システムの唯一のユーザです。
     - 〈password〉 は、そのユーザのパスワードです。

   注釈　Windows では、他のオペレーティング・システムと異なり、`EmergencyId` スイッチの前にスラッシュ (“/”) を記述します。

例えば、MyIRIS というインスタンスで、purple22 というパスワードを持つユーザ jmd が InterSystems IRIS を緊急モードで起動する場合は、以下のように入力します。

```
iris start MyIRIS /EmergencyId=jmd,purple22
```

この状態でログインできるのは、以下のように適切なパスワードを使用する緊急ユーザのみです。

```
Username: jmd
Password: ********
Warning, bypassing system security, running with elevated privileges
```

InterSystems IRIS が起動すると、InterSystems IRIS ランチャーからターミナルを起動できるほか、任意の Web アプリケーションを実行することもできます。これによって、管理ポータルおよび文字ベースのすべてのユーティリティにアクセスできるようになります。これらにアクセスし、必要に応じて設定を変更した後、InterSystems IRIS を通常のモードで再起動します。

3.3 UNIX®、Linux、および macOS での緊急アクセス・モードの呼び出し

InterSystems IRIS を緊急アクセス・モードで起動するには、root アクセス権を持っているか、対象インスタンスの所有者である必要があります。コマンド行から適切なスイッチを使用し、緊急ユーザのユーザ名とパスワードを指定して、InterSystems IRIS を呼び出します。

```
./iris start <instance-name> EmergencyId=<username>,<password>
```

これにより、ユーザが 1 人だけ認められる緊急モードの InterSystems IRIS セッションが開始します。各パラメータは以下のとおりです。

- 〈instance-name〉 は、緊急モードで開始するインスタンスを指定します。
- 〈username〉 は、システムの唯一のユーザです。
- 〈password〉 は、〈username〉 のパスワードです。

注釈　これらのオペレーティング・システムのいずれかから Windows に移行する場合、Windows では `EmergencyId` スイッチの前にスラッシュ (“/”) が必要になる点に注意します。

例えば、MyIRIS というインスタンスで、purple22 というパスワードを持つユーザ jmd が InterSystems IRIS を緊急モードで起動する場合は、以下のように入力します。

```
./iris start MyIRIS EmergencyId=jmd,purple22
```

この状態でログインできるのは、以下のように適切なパスワードを使用する緊急ユーザのみです。

```
Username: jmd
Password: ********
Warning, bypassing system security, running with elevated privileges
```

InterSystems IRIS が起動すると、ターミナルまたは任意の Web アプリケーションを実行できます。これによって、管理ポータルおよび文字ベースのすべてのユーティリティにアクセスできるようになります。これらにアクセスし、必要に応じて設定を変更した後、InterSystems IRIS を通常のモードで再起動します。

4 [システムセキュリティ設定] ページ

[システムセキュリティ設定] 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]**) には、InterSystems IRIS® インスタンス全体のセキュリティを構成するページへのリンクが用意されています。このページは以下のとおりです。

4.1 システム規模のセキュリティ・パラメータ

ここでは、InterSystems IRIS のインスタンス全体に影響するセキュリティの問題について説明します。システムワイド・セキュリティ・パラメータや、メモリ・イメージに存在する機密性の高いデータの扱いなどを取り上げます。

InterSystems IRIS には、多数のシステム規模のセキュリティ・パラメータが用意されています。これらのパラメータは、**[システムセキュリティ設定]** 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]**) で構成できます。これらのパラメータには以下のものがあります。

- **[監査を有効に]** – 監査を有効または無効にします。このチェック・ボックスの機能は、**[監査]** ページ (**[システム管理]** > **[セキュリティ]** > **[監査]**) にある **[監査を有効に]** リンクおよび **[監査を無効に]** リンクと同じです。監査の詳細は、"監査ガイド" を参照してください。既定では無効になっています。
- **[監査データベースにエラーが発生したときにシステムをフリーズしますか]** – (監査が有効な場合にのみ使用可能)。監査データベースへの書き込み中にエラーが発生した場合、インスタンスを停止 (フリーズ) します。詳細は、"監査データベースに書き込めない場合のシステムのフリーズ" を参照してください。
- **[構成セキュリティを有効に]** – "構成のセキュリティ" の説明にあるように、構成のセキュリティを有効にするかどうかを指定します。既定では無効になっています。
- **[デフォルトセキュリティドメイン]** – インスタンスの既定のセキュリティ・ドメインを選択できます。セキュリティ・ドメインの詳細は、"InterSystems IRIS のセキュリティ・ドメインの管理" を参照してください。既定のドメインは、インストールのときに設定されたドメインです。
- **[不活動上限 (0–365)]** – ユーザ・アカウントを使用しない状態で保持できる最大日数を指定します。これは、2 回の正常なログインの間の時間間隔です。アカウントを使用しない期間がこの限度に達すると、そのアカウントは無効になります。0 を指定しておくと、アカウントを使用せずに放置しても、そのアカウントは無効になりません。既定値は、"初期のユーザ・セキュリティ設定" に説明があります。

  注釈　ミラー・メンバでは、InactiveLimit パラメータは起動時に自動的に 0 に設定されます。これにより、ユーザ・アカウントが他のミラー・メンバ上で非アクティブになるのを防ぎます。

- **[不正ログイン回数制限 (0 – 64)]** – 連続して失敗できるログインの最大回数を指定します。ログインの失敗回数がこの限度に達すると、アカウントが無効になるか、ログインしようとするたびに遅延時間が長くなります。このアクションは、**[ログイン制限に達するとアカウントを無効にする]** フィールドの値で決まります。0 を指定しておくと、何回ログインに失敗しても、引き続き通常どおりにログインを試すことができます。既定値は 5 です。
- **[ログイン制限に達するとアカウントを無効にする]** – チェックを付けておいた場合は、不正ログインの回数が、前に説明したフィールドで指定した回数に達すると、そのユーザ・アカウントは無効になります。
- **[パスワード有効期限 (0–99999)]** – パスワードが無効になる頻度、つまりパスワードの変更が必要になる頻度を日数で指定します。最初に設定するときは、パスワードが無効になるまでの日数を指定します。0 を指定すると、パスワードはいつまでも有効です。ただし、このフィールドを 0 に設定しても、**[次回ログイン時にパスワード変更]** フィールドが設定されているユーザには影響しません。既定値は 0 です。

  注意　この設定は、InterSystems IRIS 自身で使用されているアカウントも含め、該当の InterSystems IRIS インスタンスのすべてのアカウントに影響します。これらのアカウントでは、パスワードを更新しないとさまざまな処理が実行できず、予測できない結果となることがあります。

- **[パスワードパターン]** – 新規に作成するパスワードで使用できる形式を指定します。詳細は、"パスワードの強固さとパスワードのポリシー" を参照してください。既定値は、"初期のユーザ・セキュリティ設定" に説明があります。

- **[パスワード検証ルーチン]** – パスワードを検証するためにユーザによって提供されたルーチン (またはエントリ・ポイント) を指定します。詳細は、Security.System クラスの PasswordValidationRoutine メソッドを参照してください。
- **[このシステムへの接続に必要なロール]** – 既存のロールに設定すると、ユーザがシステムにログインするためには、そのユーザは、ログイン・ロールとしてのその既存のロールのメンバであることが必要になります。

  LDAP 認証または OS ベースの LDAP 認証を使用している場合は、接続に必要なロールを作成して、このフィールドにそのロール名を指定することを強くお勧めします。詳細は、"ログインに必要なロールの設定" を参照してください。
- **[パーセントで始まるグローバルへの書き込みを有効に]** – パーセントで始まるグローバルに対する書き込みアクセス権を暗黙的にすべてのユーザに与えるかどうかを指定します。チェックを外すと、書き込みアクセス権は通常のセキュリティ機能で制御されます。パーセントで始まるグローバルおよびそれを保持しているデータベースである IRISSYS の詳細は、"IRISSYS (マネージャ・データベース)" を参照してください。既定の設定では、アクセス権は通常のセキュリティ機能で制御されます。
- **[複数セキュリティドメインを許可する]** – 複数のインターシステムズのセキュリティ・ドメインをサポートするかどうかを指定します。セキュリティ・ドメインの詳細は、"InterSystems IRIS のセキュリティ・ドメインの管理" を参照してください。既定では、単一のドメインのみがサポートされています。
- **[スーパーサーバSSL/TLSサポート]** – スーパーサーバがクライアント接続に TLS の使用をサポートまたは要求するかを指定します。

  重要　TLS を使用するようスーパーサーバを構成する前に、%SuperServer と呼ばれる構成が存在する必要があります。InterSystems IRIS スーパーサーバでの TLS の使用に関する詳細は、"TLS を使用するための InterSystems IRIS スーパーサーバの構成" を参照してください。

  オプションは以下のとおりです。

  - **[無効]** – TLS を使用するクライアント接続を拒否します (つまり、TLS を使用しないクライアント接続のみを受け入れます)。
  - **[有効]** – TLS を使用するクライアント接続を受け入れますが、それは必須ではありません。
  - **[必須]** – TLS を使用するクライアント接続を要求します。
- **[Telnet server SSL/TLS Support]** – Telnet サーバがクライアント接続に TLS の使用をサポートまたは要求するかを指定します。

  重要　TLS を使用するよう Telnet サーバを構成する前に、%TELNET/SSL と呼ばれる構成が存在する必要があります。InterSystems IRIS Telnet サーバでの TLS の使用に関する詳細は、"TLS を使用するための InterSystems IRIS Telnet サーバの構成" を参照してください。

  オプションは以下のとおりです。

  - **[無効]** – TLS を使用するクライアント接続を拒否します (つまり、TLS を使用しないクライアント接続のみを受け入れます)。
  - **[有効]** – TLS を使用するクライアント接続を受け入れますが、それは必須ではありません。
  - **[必須]** – TLS を使用するクライアント接続を要求します。
- **[デフォルトの署名ハッシュ]** – XML 署名ハッシュを作成するために既定で使用されるアルゴリズムを指定します。ハッシュの作成でサポートされるアルゴリズムの詳細は、https://www.w3.org/ を参照してください。

4.2 認証オプション

[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 オプション]**) では、InterSystems IRIS インスタンス全体の認証メカニズムを有効または無効にできます。

- InterSystems IRIS インスタンス全体で無効に設定した認証メカニズムは、どのサービスでも使用できなくなります。
- InterSystems IRIS インスタンス全体で有効に設定した認証メカニズムは、それをサポートするすべてのサービスで使用できます。特定のサービスに対して認証メカニズムを有効にするには、その該当のプロパティの **[サービス編集]** ページを使用します。このページは、**[サービス]** ページ (**[システム管理]** > **[セキュリティ]** > **[サービス]**) からサービスを選択することで利用できます。

  注釈　すべてのサービスがすべてのメカニズムをサポートするわけではありません。

認証オプションは以下のとおりです。

- **[認証なしアクセスを許可]** – ユーザは認証なしに接続できます (ログイン・ダイアログが表示されたら、**[ユーザ名]** および **[パスワード]** フィールドを空白にしたまま **[OK]** をクリックしてログインできます)。
- **[OS 認証を許可]** – オペレーティング・システムのユーザ ID を使用してユーザを識別してから、インターシステムズの承認を使用します。
- **[代行認証によるOS認証を許可]** – オペレーティング・システムのユーザ ID を使用してユーザを識別してから、代行承認を使用します。
- **[LDAP認証によるOS認証を許可]** – オペレーティング・システムのユーザ ID を使用してユーザを識別してから、LDAP 承認を使用します。
- **[パスワード認証を許可]** – インスタンス認証と呼ばれる InterSystems IRIS 独自のネイティブ・ツールを使用してユーザを認証してから、インターシステムズの承認を使用します。
- **[代行認証を許可]** – 外部 (代行) 認証システムを呼び出して、使用します。代行認証は、インターシステムズの承認または代行承認と共に使用できます。
- **[Always try Delegated authentication]** – InterSystems IRIS は、インスタンス認証 (パスワード認証とも呼ばれる) で認証するユーザに対して代行認証コードを呼び出します。代行認証とインスタンス認証の両方を使用し、インスタンス認証ユーザには ZAUTHENTICATE の呼び出しも求める場合は、このオプションを選択します。
- **[Kerberos認証を許可]** – Kerberos を使用して認証を実行します。Kerberos 認証は、インターシステムズの承認または代行承認と共に使用できます。
- **[LDAP認証を許可]** – LDAP (Active Directory を含む) を使用してユーザを認証します。LDAP を認証と承認の両方に使用することも、LDAP をインターシステムズの承認と共に使用することもできます。
- **[LDAPキャッシュ credentials 認証を許可]** – キャッシュした LDAP 認証情報のコピーを使用して、LDAP データベースを利用できない場合でも LDAP ユーザを認証します。
- **[ログイン Cookie の作成を許可]** – InterSystems IRIS は、有効になっている Web アプリケーション間で共有される Cookie を使用してユーザを認証するため、新しいアプリケーションを初めて使用するときにユーザ名およびパスワードを入力する必要はありません。これは、CSP を使用する Web アプリケーションのみに関連します。
- **[ログイン Cookie の有効期間 (秒)]** – ログイン Cookie の有効期間 (秒)。このフィールドは、インスタンスに対してログイン Cookie が有効になっている場合のみ関係します。
- **[二要素タイムベースのワンタイム・パスワード認証を許可]** – InterSystems IRIS は、認証デバイス、またはユーザの携帯電話上で動作しているアプリケーションを使用して検証コードを提供します。その後ユーザはこのコードを入力して認証プロセスを完了します。これを選択すると、**[認証/ウェブセッションオプション]** ページに 2 要素認証を構成するためのフィールドが表示されます。

- **[二要素 SMS テキスト認証を許可]** – InterSystems IRIS は、携帯電話のテキスト・メッセージを使用してセキュリティ・コードを提供します。その後ユーザはこのコードを入力して認証プロセスを完了します。これを選択すると、**[認証/ウェブセッションオプション]** ページに 2 要素認証を構成するためのフィールドが表示されます。

複数の認証オプションがサポートされている場合は、カスケード認証が使用されます。

5 変更内容の反映

さまざまなセキュリティ設定を変更した場合、その変更が反映されるまでの時間は以下のとおりです。

- ユーザのプロパティ(割り当てられたロールなど)に対する変更は、そのユーザが次回ログインしたときに有効になります。既に実行中のプロセスには反映されません。
- サービスに対する変更 (サービスを有効にするかどうか、認証を要求するかどうかなど) は、今後そのサービスに接続しようとしたときに有効になります。既存の接続には反映されません。
- ロールの定義に対する変更は、以降行われる特権のチェックですぐに有効になります。これらの変更はデータベースへのアクセスが発生するたびにチェックされるので、データベース・リソースに対しては直ちに反映されます。サービスとアプリケーションに対しては、変更の時点以降にサービスに接続しようとしたとき、またはアプリケーションを起動したときに反映されます。

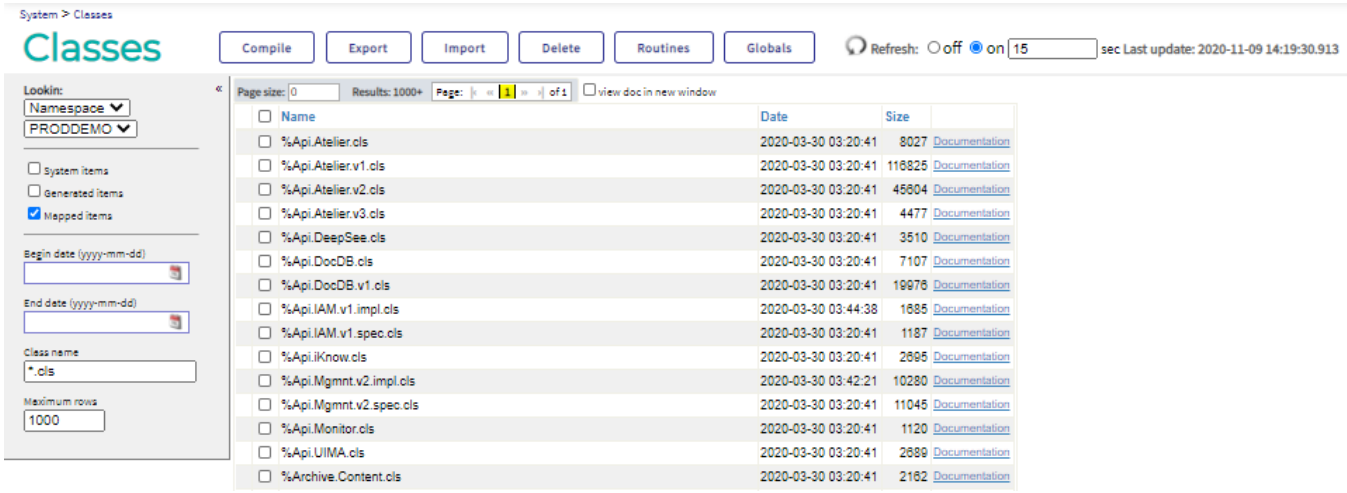
注釈　ここに挙げた時間は、変更が反映されるまでの最長時間なので、もっと早い時点で変更が有効になることもあります。

6 管理ポータルのページの自動更新の有効化

既定では、ユーザは  (**[ダイアグラムを更新]**) アイコンが使用可能な場合に、これをクリックすることによってのみ、管理ポータルのページを更新できます。ただし、InterSystems IRIS では、数秒ごとに管理ポータルのページを自動更新するメカニズムをユーザに提供できます。次に示すように、ターミナルから、このメカニズムを公開するよう ^%SYS グローバルを変更できます。

```
set ^%SYS("Portal","EnableAutoRefresh") = 1
```

これを行うと、管理ポータルの更新可能なページに一連のラジオ・ボタンが表示され、ユーザが自動更新のオン/オフを切り替えることができるようになります。一部のページでは、ユーザが更新間隔を指定することもできます。重要なこととして、管理者が `EnableAutoRefresh` ノードを `1` に設定すると、自動更新は既定でオフになります。以下の図は、自動更新が有効になっていて、更新間隔が 15 秒に設定されている **[クラス]** ページを示しています。



重要　　自動更新を行うと InterSystems IRIS サーバへの呼び出しが発生するため、自動ログアウトが有効になっている場合、ログアウトできなくなることがあります。詳細は、"管理ポータルの自動ログアウト動作" を参照してください。

7 管理ポータルの自動ログアウト動作

InterSystems IRIS 管理ポータル Web アプリケーションにはそれぞれ [セッションタイムアウト] プロパティがあり、これによって、ユーザのセッションが期限切れになるまでユーザが非アクティブな状態でいられる時間が指定されています。既定では、ユーザのセッションが期限切れになってから 15 秒後に、管理ポータルは現在のページを更新してユーザをログアウトさせます。その際、保留中の変更はキャッシュされません。また、保留中の変更の保存を求めるプロンプトも表示されません。保存されていない変更は破棄されます。

重要　　非アクティブ状態の時間は、InterSystems IRIS サーバの呼び出しから次の呼び出しまでです。すべてのユーザ・アクションがサーバの呼び出しを引き起こすわけではありません。例えば、ユーザが **[保存]** をクリックした場合はサーバが呼び出されますが、テキスト・フィールドに入力した場合はサーバの呼び出しは生じません。このため、ユーザがデータ変換を編集していて、**[セッションタイムアウト]** のしきい値より長い間 **[保存]** をクリックしないと、ユーザのセッションは期限切れとなり、保存されていない変更はすべて破棄されます。

自動ログアウトの後、以下のシナリオが生じる可能性があります。

- ログイン・ページが表示されます。
- 管理ポータルがユーザをログアウトさせた直後に再度ログインさせます。これは、Web アプリケーションに [ID でグループ化] の値が設定されており、その結果、自動認証が行われるためです。この場合、管理ポータルの現在のページが更新され、保留中の変更はすべて削除されます。

以下の手順を実行して、ユーザの作業内容が破棄されるのを防ぐことができます。

- ユーザに定期的に作業を保存するよう伝えます。
- ユーザが時間のかかる構成タスク (データ変換の変更など) を行っている Web アプリケーションの **[セッションタイムアウト]** の値を延ばします。**[セッションタイムアウト]** の既定値は 15 分です。

さらに、既定の自動ログアウト動作を保持することをお勧めしますが、ユーザが管理ポータルの [**相互運用性**] のページを表示している場合は、ユーザが自分からログアウトするかブラウザを閉じるまで、ログインしたままにすることができます。これを実行するには、以下のように ^EnsPortal を使用します。

```
^EnsPortal("DisableInactivityTimeout","Portal") = 1
```

注釈　これは、ネームスペースごとの設定です。ログアウト動作を変更するには、ネームスペースごとに個別にこの値を設定する必要があります。

もう一度 ^EnsPortal を使用すると、自動ログアウトを元に戻すことができます。

```
^EnsPortal("DisableInactivityTimeout","Portal") = 0
```

変更を加える前に、生じる可能性のあるセキュリティ上の影響を検討することをお勧めします。

Web アプリケーションとその設定の詳細は、"アプリケーション" を参照してください。

8 その他のセキュリティ機能

ここでは、その他のセキュリティ機能のいくつかと考慮事項について説明します。内容は以下のとおりです。

- 保護されたデバッグ・シェルの使用の有効化
- メモリ・イメージに存在する機密データの保護

その他のセキュリティ・トピックは、以下を参照してください。

- InterSystems IRIS の構成情報の保護

8.1 保護されたデバッグ・シェルの使用の有効化

InterSystems IRIS には、ルーチンを中断し、完全なデバッグ機能をサポートするシェルに入る機能が含まれています ("コマンド行ルーチンのデバッグ" を参照)。InterSystems IRIS には保護されたデバッグ・シェルも含まれています。これには、割り当てられた特権の超越や迂回をユーザができないという利点があります。

既定では、デバッグ・プロンプトのユーザは、現在のレベルの特権を保持します。デバッグ・プロンプトの保護されたシェルを有効にし、このことによってユーザが発行できるコマンドを制限するには、ユーザは **%Secure_Break:Use** 特権 (**%Secure_Break** リソースの **Use** 許可) を保持している必要があります。ユーザにこの特権を付与するには、ユーザを、事前定義の **%SecureBreak** ロールなどの **%Secure_Break:Use** 特権を含むロールのメンバにします。

8.2 メモリ・イメージに存在する機密データの保護

エラー状態の中には、"コア・ダンプ" と呼ばれる、プロセス・メモリ・コンテンツのディスク・ファイルへの書き込みを発生させるものもあります。このファイルには、ダンプ時にプロセスで使用されていたすべてのデータのコピーが含まれます (潜在的に重要なアプリケーション・データおよびシステム・データを含む)。これを回避するには、システム全体でコア・ダンプを許可しないようにします。コア・ダンプを許可しないようにする方法は、使用しているオペレーティング・システムによって異なります。詳細は、オペレーティング・システムのドキュメントを参照してください。