暗号化ガイド

Version 2023.1
2024-01-02

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

暗号化ガイド
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

マネージド・キー暗号化について

InterSystems IRIS® データ・プラットフォームにはマネージド・キー暗号化のサポートが含まれています。これは保存データを保護する一連のテクノロジです。これらのテクノロジには以下のものがあります。

- ブロック・レベルのデータベース暗号化 (単にデータベース暗号化とも呼ばれます) ― すべてのデータが暗号化されるデータベースの作成と管理を可能にする管理ツールのセット。そのようなデータベースは、管理ポータルで管理されます。
- アプリケーションのデータ要素暗号化 (単にデータ要素暗号化とも呼ばれます) ― ディスクにおける格納や取得の際に個々のデータ要素 (特定のクラス・プロパティなど) の暗号化および解読を行うコードをアプリケーションで含めることができるようにする、プログラムによるインタフェース。
- 暗号化キー管理 (単にキー管理とも呼ばれます) ― データベースまたはデータ要素を暗号化するために使用するキーを作成および管理するためのツールのセット。

データベースまたはデータ要素を暗号化するためのキーは、データ暗号化キーと呼ばれ、単にキーと呼ばれる場合もあります (コンテキストが明確な場合)。各インスタンスでは、データベース暗号化用のデータ暗号化キーを最大 256 個、データ要素暗号化用のデータ暗号化キーを最大 4 個同時に有効化できます。キーを有効化することで、そのキーを暗号化操作と解読操作に利用できるようになります。

暗号化キーは以下の 2 つの方法で保存できます。

- 標準のマシン上のキー・ファイル
- Key Management Interoperability Protocol (KMIP) を介してキーにアクセス可能な専用ハードウェア

注釈　　キー・ファイル内の 1 つのキーをデータベース暗号化とデータ要素暗号化に同時に使用できます。

InterSystems IRIS では、インスタンスによるディスクに対する書き込みまたは読み取りの際に、AES (Advanced Encryption Standard) を使用して暗号化と解読が実行されます。データベースの場合、InterSystems IRIS は固定長ブロックで書き込みと読み取りを行い、単一のラベル・ブロックを除き、データベース全体が暗号化されます。この暗号化されるコンテンツには、データ自体、インデックス、ビットマップ、ポインタ、割り当てマップ、およびインクリメンタル・バックアップ・マップが含まれます。データ要素の場合、指定されたデータのみが暗号化され、暗号化キーの一意の識別子は暗号化データと共にディスクに格納されます。

暗号化と解読は最適化されていて、どのような InterSystems IRIS プラットフォームでも、暗号化と解読による影響は少なくて予測可能ですInterSystems IRIS データベース暗号化が、データベースに関連するがデータベースとは分離されている機能に与える影響の詳細は、"暗号化とデータベース関連機能" を参照してください。

2
キー管理タスク

キーはデータ暗号化キーの略称で、128 ビット、196 ビット、または 256 ビットのビット文字列です。これは、データの暗号化や解読を可逆的に行う暗号化アルゴリズムで使用されます。それぞれのキーには一意の識別子 (GUID とも呼ばれます) があり、InterSystems IRIS® データ・プラットフォームはこれをキー管理アクティビティの一部として表示します。

キー管理は、キーの作成、キーの有効化、キーの無効化、さまざまなアクティビティの既定のキーの割り当て、およびキーの削除に関連するアクティビティのセットです。また、キーの保存に関連する管理アクティビティも含まれます。キーは、以下の 2 つの方法のいずれかで保存できます。

- キー・ファイル ー キー・ファイルとは、最大 256 個のキーの暗号化コピーを保持するファイルです。キーを解読して使用するためのパスワードはキー・ファイル管理者が提供します。
- KMIP サーバ ー KMIP サーバは、Key Management Interoperability Protocol (KMIP) を使用して通信を送受信できるキー管理サーバです。KMIP サーバはさまざまなサードパーティ・ベンダから発売されており、KMIP サーバの一般的な構成および使用方法は、これらのベンダによって提供されています。

注釈　ジャーナル・ファイルまたは IRISTEMP および IRISLOCALDATA データベース用の暗号化を構成する場合、これは InterSystems IRIS の起動構成の一部です。詳細は、"暗号化の起動設定の構成" を参照してください。

2.1 キー・ファイル内のキーの管理

キー・ファイルとは、1 つ以上のデータ暗号化キーの暗号化コピーを保持するファイルです。キー・ファイルの管理は、キー・ファイルにおける管理者の追加や削除など、キー・ファイル自体に関連するアクティビティのセットです。特定のキー・ファイル内では、すべての管理者がすべてのキーにアクセスできます。すべてのキーは管理者情報と共に暗号化された形式で格納されます。各データ暗号化キーは、マスタ・キーを使用して個別に暗号化されます。キー・ファイルの管理者ごとに、一意の暗号化されたマスタ・キーのコピーがあり、これはキー暗号化キーを使用して暗号化されます。各キー暗号化キーは個々のキー管理者のパスワードから導出されます。暗号化タスクでは有効なデータ暗号化キーが必要であり、InterSystems IRIS ではそのキーを解読して有効化できるようにするために、管理者のユーザ名とパスワードが必要です。

キー・ファイルを使用した処理としては、以下のタスクがあります。

- キー・ファイルの作成
- キー・ファイルへのキーの追加またはキー・ファイルからのキーの削除
- キー・ファイルへの管理者の追加またはキー・ファイルからの管理者の削除
- キー・ファイルからのデータベース暗号化キーの有効化またはデータベース暗号化キーの無効化

- キー・ファイルからのデータ要素暗号化キーの有効化またはデータ要素暗号化キーの無効化
- 複数インスタンス・テクノロジを使用したキーとキー・ファイルの管理
- インスタンスの既定の暗号化キーまたはジャーナリング暗号化キーの指定

注釈　インスタンスで起動時に複数のキーが使用される場合 (例えば、ジャーナル・ファイル、監査データベース、およびその他のデータベースのキー)、これらのキーをすべて 1 つのキー・ファイルに配置する必要があります。これにより、これらのキーすべてがインスタンスの起動時に使用可能になります。

2.1.1 キー・ファイルの作成

暗号化キー・ファイルを作成すると、キーが 1 つ含まれます。暗号化キー・ファイルおよびその最初のキーを作成するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[暗号キー作成]** ページ (**[システム管理]** > **[暗号化]** > **[新規暗号キー・ファイル作成]**) に移動します。
2. **[暗号キー作成]** ページで、以下の値を指定します。
   - **[キー・ファイル]** – 暗号化キーを格納するファイルの名前。これは、絶対パス名と相対パス名のいずれでも指定できます。

     絶対ファイル名を入力すると、キー・ファイルは指定したドライブの指定したディレクトリに配置されます。相対ファイル名を入力すると、キー・ファイルは InterSystems IRIS インスタンスの管理者ディレクトリ (InterSystems IRIS のインストール先ディレクトリの下、つまり <install-dir>/mgr/) に置かれます。また、このファイル名には拡張子が付加されないので、ファイル MyKey はそのままの名前で保存されます。このフィールドの右にある **[参照]** ボタンを使用して、キー・ファイルが作成されるディレクトリを選択することもできます(既存のファイル名を指定した場合、そのファイルは上書きされず、保存に失敗します)。

     警告　<install-dir>/Mgr/Temp にキーを格納すると、InterSystems IRIS が次回起動するときにすべて削除されます。したがって、<install-dir>/Mgr/Temp にはキーを絶対に格納しないでください。

   - **[管理者名]** – キーを有効にできる管理者の名前。管理者を 1 人以上指定する必要があります。

     データベース暗号化機能と InterSystems IRIS のセキュリティとは互いに独立しているので、InterSystems IRIS のセキュリティで設定されていないユーザ名をここで指定してもかまいません。既定では、最初に設定した管理者名が現在のユーザ名になっています。管理者名には、Unicode 文字を使用できません。

   - **[パスワード]** – このユーザのパスワード。

     データベース暗号化機能とインターシステムズのセキュリティとは互いに独立しているので、InterSystems IRIS のセキュリティでユーザが使用しているものではないパスワードをここで指定してもかまいません。このパスワードは、ディスクのどこにも格納されません。したがって、管理者は、この情報を紛失しないように注意する必要があります。

     管理者パスワードの強固さに関するガイドラインに従ったパスワードとすることをお勧めします。有効なパスワードを第三者が推測できる場合、そのパスワードのポリシーは脆弱すぎます。また、このパスワードに Unicode 文字を使用することはできません。

     重要　キー管理者のパスワードはディスクのどこにも保存されません。この情報を紛失しないよう努めることは、キー管理者の責任です。

   - **[パスワード確認]** – 確認のために、このユーザのパスワードをもう一度入力します。
   - **[暗号化セキュリティ・レベル]** – キーの長さ。選択肢には、128 ビット、192 ビット、および 256 ビットがあります。

- [キー説明] – 最初に作成され、キー・ファイルに格納されているキーを説明するテキスト。このテキストは [キー・ファイルで定義されている暗号化キー] テーブルの [説明] 列に表示されます。

3. ページの上部の [保存] をクリックして、キー・ファイルをディスクに保存します。
4. キーを作成したら、"暗号化データのアクセスにおける偶発的な損失からの保護" の指示に従い、新たに更新されたキー・ファイルのバックアップ・コピーを作成および保存します。

これで単一のデータベース暗号化キーおよび単一の管理者を持つキー・ファイルが作成されます。ページにはキーの ID が表示されます。その文字列は、9158980E-AE52-4E12-82FD-AA5A2909D029 などのようになります。キー ID は、InterSystems IRIS がここやその他のページに表示するキーの一意の識別子です。その場所に関係なく、キーを追跡する手段を提供します。キー・ファイルを保存するとどこへでも移動できる (つまり、InterSystems IRIS ではキー・ファイルの場所によって追跡することはできない) ため、これは重要です。

キーはマスタ暗号化キーを使用して暗号化されます。また、マスタ暗号化キーの単一コピーがあり、これは管理者のキー暗号化キー (KEK) を使用して暗号化されます。"キー・ファイルへのキーの追加" の指示に従い、キー・ファイルにキーを追加できます。"キー・ファイルへの管理者の追加" の指示に従い、キー・ファイルに管理者を追加できます。

警告 キー・ファイルのバックアップ・コピーを作成および保存することを強くお勧めします。データベース暗号化キーを作成するたびに、それは再作成が不可能な一意のキーになります。同じ管理者とパスワードを使用して新しいキーを作成しても、まったく別の一意なキーが作成されます。まだ有効にしていないキーを紛失し、それをリカバリできない場合は、そのキーで保護されている暗号化データベースを読み取ることはできなくなり、そのデータは永久に失われます。

2.1.2 キー・ファイルへのキーの追加

キー・ファイルを使用する場合、キーを作成するには 2 つの異なる方法があります。

- キー・ファイルの作成。これにより、InterSystems IRIS でキーが作成され、ファイルに配置されます。キー・ファイルを作成するには、" キー・ファイルの作成" を参照してください。
- 既存のキー・ファイルへのキーの追加。このセクションで説明します。

キーを既存のキー・ファイルに追加するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、[暗号化キー・ファイルの管理] ページ ([システム管理] > [暗号化] > [暗号化キー・ファイルの管理]) に移動します。
2. [暗号化キー・ファイルの管理] ページの [キー・ファイル] フィールドで、キーを追加および格納するキー・ファイル名を入力し、[OK] をクリックします。これにより、そのキー・ファイルの情報が表示されます。塗りつぶされた領域の下部で、[キーファイルに定義されている暗号化キー] テーブルにキー・ファイル内の 1 ～ 256 個のキーのリストが表示されます。ファイル内のキーが 3 つ以下である場合、新しいキーを作成してファイルに追加できます。
3. [キー・ファイルで定義されている暗号化キー] テーブルの下にある [追加] ボタンをクリックして、キーをキー・ファイルに追加します。これにより、[新しい暗号化キーの追加] 画面が表示されます。
4. [新しい暗号化キーの追加] 画面で、以下のフィールドに値を入力します。
   - [既存の管理者名] – キー・ファイルに関連付けられた管理者の名前(ファイルに関連付けられた管理者は、[暗号化キー・ファイルの管理] ページの [キー・ファイルで定義されている管理者] テーブルに表示されます)。
   - [既存の管理者パスワード] – この管理者のパスワード。
   - [説明] – キーを説明するテキスト。このテキストは [キー・ファイルで定義されている暗号化キー] テーブルの [説明] 列に表示されます。
5. [OK] をクリックして、キーをキー・ファイルに保存します。これにより、[キー・ファイルで定義されている暗号化キー] テーブルのキーの情報が表示されます。これにはキーの ID が含まれ、その文字列は、

9158980E-AE52-4E12-82FD-AA5A2909D029 などのようになります(キー ID は、InterSystems IRIS がここやその他のページに表示するキーの一意の識別子です。その場所に関係なく、キーを追跡する手段を提供します。キー・ファイルを保存するとどこへでも移動できる (つまり、InterSystems IRIS ではキー・ファイルの場所によって追跡することはできない) ため、これは重要です)。

6. 新しいキーをキー・ファイルに追加したら、"暗号化データのアクセスにおける偶発的な損失からの保護" の指示に従い、新たに更新されたキー・ファイルのバックアップ・コピーを作成および保存します。

警告 キー・ファイルのバックアップ・コピーを作成および保存することを強くお勧めします。データベース暗号化キーを作成するたびに、それは再作成が不可能な一意のキーになります。同じ管理者とパスワードを使用して新しいキーを作成しても、まったく別の一意なキーが作成されます。まだ有効にしていないキーを紛失し、それをリカバリできない場合は、そのキーで保護されている暗号化データベースを読み取ることはできなくなり、そのデータは永久に失われます。

2.1.3 キー・ファイルからのキーの削除

キーをキー・ファイルから削除するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[暗号化キー・ファイルの管理]** ページ (**[システム管理]** > **[暗号化]** > **[暗号化キー・ファイルの管理]**) に移動します。
2. **[暗号化キー・ファイルの管理]** ページの**[キー・ファイル]** フィールドで、キーを削除するキー・ファイル名を入力し、**[OK]** をクリックします。これにより、そのキー・ファイルの情報が表示されます。塗りつぶされた領域の下部で、**[キーファイルに定義されている暗号化キー]** テーブルにキー・ファイル内の 1 ～ 256 個のキーのリストが表示されます。ファイル内にキーが複数ある場合、ファイルからキーを削除できます。
3. キーのテーブルで、キーの行にある **[削除]** をクリックして、そのキーを削除します。**[削除]** をクリックすると、削除の操作を確認するページが表示されます

   キーの **[削除]** ボタンが使用できない場合、これは、そのキーがファイルの既定の暗号化キーまたはジャーナル暗号化キーであるためです。キーを削除するには、まず別のキーがファイルの既定の暗号化キーまたはジャーナル暗号化キーであることを、**[既定に設定]** または **[ジャーナル設定]** をクリックして指定します。
4. 確認ダイアログで **[OK]** をクリックして、ファイルからキーを削除します。

警告 キーの唯一の既存コピーを削除する前に、そのコピーを使用している既存の暗号化コンテンツがないことを確実に確認してください。データを解読するために必要なキーのコピーがないと、そのキーで保護されている暗号化データは読み取り不能になり、永久に失われます。

2.1.4 キー・ファイルへの管理者の追加

管理者を既存のキー・ファイルに追加するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[暗号化キー・ファイルの管理]** ページ (**[システム管理]** > **[暗号化]** > **[暗号化キー・ファイルの管理]**) に移動します。
2. **[キー・ファイル]** フィールドで、開くキー・ファイルのパスとファイル名を入力し、**[OK]** をクリックします。**[参照]** ボタンを使用してキーを探すこともできます。ポータルでキー・ファイルを開くと、ファイルにリストされた管理者が記載されたテーブルが表示されます。管理者名は、定義されたときの文字に関係なく、すべて大文字で表示されます。
3. 管理者のテーブルで **[追加]** をクリックし、新しい管理者を追加します。以下のフィールドがあるページが表示されます。
   - **[既存の管理者名]** – 既にファイルにある管理者の名前。
   - **[既存の管理者パスワード]** – ファイルに既に存在する管理者に関連付けられたパスワード。

- **[新しい管理者名]** – ファイルに追加される新しい管理者の名前。暗号化機能と InterSystems IRIS のセキュリティとは互いに独立しているので、InterSystems IRIS のセキュリティで設定されていない管理者名をここで指定してもかまいません。このユーザ名に Unicode 文字を使用することはできません。
- **[新しい管理者パスワード]** – 新しい管理者のパスワード。管理者パスワードの強固さに関するガイドラインに従ったパスワードとすることをお勧めします。また、このパスワードは Unicode 文字を使用することはできません。データベース暗号化機能と InterSystems IRIS のセキュリティとは互いに独立しているので、InterSystems IRIS のセキュリティで設定されていないパスワードをここで指定してもかまいません。
- **[新しい管理者パスワードの確認]** – 新しい管理者のパスワードの確認。

これらのフィールドを入力して、**[OK]** をクリックします。これで新しい管理者がキー・ファイルに追加されました。

新しい管理者がキー・ファイルに追加されると、キー・ファイルをコピーし、各コピーを安全な場所に格納することが必要となる場合があります。さらに、キーごとに複数の管理者を作成し、そのいずれか 1 人の名前とパスワードを書面に記録して、耐火金庫などの安全な場所に保管することを強くお勧めします。ただし、ここでキー・ファイルのコピーを作成しても、後で管理機能として新しく管理者を追加すると、新しい管理者のあるキー・ファイルのコピーのみが最新のものになります。

注釈　新しい管理者をキー・ファイルに追加すると、管理者のパスワードは、ファイルに作成された管理者名のエントリに永久に関連付けられます。割り当てたパスワードは変更できません。新しいパスワードを割り当てるには、その管理者名のエントリをキー・ファイルから削除した後、同じ管理者名と新しいパスワードで新しいエントリを作成します。

2.1.5 キー・ファイルからの管理者の削除

管理者をキー・ファイルから削除するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[暗号化キー・ファイルの管理]** ページ (**[システム管理]** > **[暗号化]** > **[暗号化キー・ファイルの管理]**) に移動します。
2. **[キー・ファイル]** フィールドで、キーのパスとファイル名を入力して **[OK]** をクリックします。ファイルにリストされた管理者を含むテーブル (およびファイル内の暗号化キーのテーブル) が表示されます。
3. 管理者のテーブルで、管理者の横にある **[削除]** をクリックし、そのキーの管理者を削除します。**[削除]** をクリックすると、削除の操作を確認するページが表示されます(ファイル内に管理者が 1 人のみの場合、その管理者を削除することはできないため、**[削除]** ボタンはありません)。
4. **[OK]** をクリックして、ファイルから管理者を削除します。

2.1.6 キー・ファイルからのデータベース暗号化キーの有効化

InterSystems IRIS では、データベース暗号化で同時に 256 個までの有効なキーがサポートされています。データベース暗号化でキー・ファイルからキーを有効にするには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[データベース暗号化]** ページ (**[システム管理]** > **[暗号化]** > **[データベース暗号化]**) に移動します。有効になっているキーがある場合、ページにはそれらをリストするテーブルが表示されます。
2. このページで、**[キーを有効にする]** をクリックします。これによって、キーを有効にするためのフィールドが表示されます
3. 以下のフィールドの値を入力します。
   - **[キー・ファイル]** – 暗号化キーを保存するファイルの名前。絶対ファイル名を入力すると、指定したドライブの指定したディレクトリにあるキー・ファイルが検索されます。相対ファイル名を入力すると、InterSystems IRIS インスタンスの管理者ディレクトリ (InterSystems IRIS のインストール・ディレクトリの下、つまり **<install-dir>/mgr/**) か

ら、キー・ファイルの検索が開始されます。[参照] ボタンを使用してキー・ファイルを開くダイアログを表示することもできます。

- [管理者名] – このキーが作成されたときまたは編集されたときに指定された、このキーの管理者の名前。
- [パスワード] – 指名した管理者に対して指定されているパスワード。

4. [有効化] ボタンをクリックします。

InterSystems IRIS により、指定したファイル内のすべてのキーの有効化が試行されます。スロットが不足していて、ファイル内のすべてのキーを有効にできない場合、できる限り多くのキーが開かれます。

キーが有効化されると、有効なキーのテーブルが [データベース暗号化] ページに表示されます。InterSystems IRIS により有効化されたキーそれぞれについて、有効なキーのテーブルにキーが追加され、そのキーの識別子がページで表示されます。有効なキーそれぞれに対し、以下のさまざまな操作も実行できます。

- [既定に設定] – これをクリックして、新しい暗号化データベースの作成時に InterSystems IRIS でこのキーが使用されるように指定します。詳細は、"インスタンスの既定の暗号化キーまたはジャーナリング暗号化キーの指定" を参照してください。
- [ジャーナルの設定] – これをクリックして、InterSystems IRIS でそのキーを使用してジャーナル・ファイルを暗号化するように指定します。詳細は、"インスタンスの既定の暗号化キーまたはジャーナリング暗号化キーの指定" を参照してください。
- [無効] – これをクリックして、このキーを無効にします。詳細は、"データベース暗号化キーの無効化" を参照してください。

注釈　キーのテーブルにファイルやパスの情報は表示されません。キー・ファイルが作成されると、十分な特権のあるオペレーティング・システム・ユーザはキー・ファイルを移動できるので、InterSystems IRIS ではオペレーティング・システムの場所に関して正確な情報がなくなる場合があり、信頼できるのは、メモリにある有効なキーの GUID の正確性のみとなるためです。2 番目以降のキーを有効化する場合は、まず、現在有効化されているキーの識別子をメモしてください。これによって新しいキーを識別できます。

2.1.7 キー・ファイルからのデータ要素暗号化キーの有効化

InterSystems IRIS では、データ要素暗号化で一度に 4 つまでの有効なキーがサポートされています。データ要素暗号化でキーを有効にするには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、[データ要素暗号化] ページ ([システム管理] > [暗号化] > [データ要素暗号化]) に移動します。有効になっているキーがある場合、ページにはそれらをリストするテーブルが表示されます。
2. [データ要素暗号化] ページで、[キーを有効にする] を選択します。これによって、キーを有効にするためのフィールドが表示されます。キー有効化が利用できない場合、データ要素暗号化キーは既に 4 つ有効になっています。
3. 以下のフィールドの値を入力します。
   - [キー・ファイル] – 暗号化キーを保存するファイルの名前。絶対ファイル名を入力すると、指定したドライブの指定したディレクトリにあるキー・ファイルが検索されます。相対ファイル名を入力すると、InterSystems IRIS インスタンスの管理者ディレクトリ (InterSystems IRIS のインストール・ディレクトリの下、つまり <install-dir>/mgr/) から、キー・ファイルの検索が開始されます。
   - [管理者名] – このキーが作成されたときまたは編集されたときに指定された、このキーの管理者の名前。
   - [パスワード] – 指名した管理者に対して指定されているパスワード。
4. [有効化] ボタンをクリックします。

InterSystems IRIS により、指定したファイル内のすべてのキーの有効化が試行されます。スロットが不足していて、ファイル内のすべてのキーを有効にできない場合、できる限り多くのキーが開かれます。

キーが有効化されると、有効なキーのテーブルが **[データ要素暗号化]** ページに表示されます。InterSystems IRIS により有効化されたキーそれぞれについて、有効なキーのテーブルにキーが追加され、そのキーの識別子がページで表示されます。

注釈　キーのテーブルにファイルやパスの情報は表示されません。キー・ファイルが有効になると、十分な特権のあるオペレーティング・システム・ユーザはキーを移動できるので、InterSystems IRIS ではオペレーティング・システムの場所に関して正確な情報がなくなる場合があり、信頼できるのは、メモリにある有効なキーの GUID の正確性のみとなるためです。2 番目以降のキーを有効化する場合は、まず、現在有効化されているキーの識別子をメモしてください。これによって新しいキーを識別できます。

2.1.8 複数インスタンス・テクノロジを使用したキーとキー・ファイルの管理

InterSystems IRIS のクラスタ内で暗号化データベースやジャーナル・ファイルを使用している場合、クラスタのすべてのノード上の InterSystems IRIS インスタンスは、単一のデータベース暗号化キーを共有する必要があります。

InterSystems IRIS ミラーに属しているインスタンスに対してジャーナル・ファイルの暗号化を有効にする前に、"ミラー内ジャーナル暗号の有効化" を参照して重要な情報を確認してください (データベース暗号化についてはミラーリングに関する要件はありません)。

単一のキーの共有を有効にする方法は 2 つあります。

- すべてのインスタンスは、1 つのクラスタ・ノードまたはミラー・メンバにある単一のキー・ファイルを共有しています。

  この場合、キー・ファイルの単一のコピーを変更すれば、すべてのノードまたはメンバでその変更を認識できます。ただし、キー・ファイルを保持しているホストが他のノードまたはメンバで利用できなくなると、キー・ファイルからキーを読み取れず、InterSystems IRIS インスタンスを正しく再起動できなくなる可能性があります。

- キー・ファイルのコピーをクラスタ・ノードごとまたはミラー・メンバごとに保持します。

  この場合、キー・ファイルを変更したら、同じキーを含むキー・ファイルのコピーを他のすべてのノードまたはメンバに配布します。この方法では、(通常は負荷が小さい) キー・ファイルを管理する負担が大きくなりますが、各 InterSystems IRIS インスタンスで起動時にキーを確実に利用できます。

重要　キー・ファイルが単一または複数のどちらの場合でも、データベース暗号化キー自体はすべてのインスタンスに共通です。

2.1.8.1 単一のキー・ファイルの使用

単一のキー・ファイルを使用するには、以下の手順に従います。

1. データベース暗号化キーを 1 台のノードまたはメンバ上に作成します。この手順の詳細は、"キー・ファイルの作成" を参照してください。
2. "暗号化データのアクセスにおける偶発的な損失からの保護" の指示に従い、このキーを保護します。

   注意　これらの予防措置を怠ると、暗号化データベースまたはジャーナル・ファイルを読み取れず、そのデータが永久に失われる結果になることがあります。

3. 無人で起動するように各 InterSystems IRIS インスタンスを構成して、InterSystems IRIS にキー・ファイルのパスを提供します。この手順の詳細は、"無人のキー有効化による起動" を参照してください。

すべての InterSystems IRIS インスタンスは同じキーを使用するため、暗号化されたデータをインスタンス間で読み取れます。キー・ファイルを変更すると、すべてのインスタンスでその変更を認識できます。

2.1.8.2 複数のキー・ファイルの使用

キー・ファイルのコピーを複数使用するには、以下の手順に従います。

1. データベース暗号化キーを 1 台のノードまたはメンバ上に作成します。この手順の詳細は、"キー・ファイルの作成" を参照してください。
2. "暗号化データのアクセスにおける偶発的な損失からの保護" の指示に従い、このキーを保護します。

   注意　これらの予防措置を怠ると、暗号化データベースまたはジャーナル・ファイルを読み取れず、そのデータが永久に失われる結果になることがあります。

3. キー・ファイルのコピーを残りのノードまたはメンバごとに作成します。
4. ノードまたはメンバごとに次の手順を実行します。
   a. キー・ファイルのコピーを取得して、マシン上の安全で安定した場所にそのコピーを置きます。
   b. 無人で起動するように各 InterSystems IRIS インスタンスを構成します。この手順の詳細は、"無人のキー有効化による起動" を参照してください。

キー・ファイルの各コピーには同じキーが含まれるため、すべての InterSystems IRIS インスタンス間で暗号化されたデータを読み取ることができます。各 InterSystems IRIS インスタンスのマシン上にキー・ファイルがあるので、InterSystems IRIS の再起動時に確実にキー・ファイルを使用できます。管理者の追加や削除などでキー・ファイルを変更した場合は、各マシンにそのキー・ファイルの新しいコピーを配布して、(古いコピーと同じ場所に新しいコピーを置いた場合でも) 新しいコピーを使用して無人で起動するように各 InterSystems IRIS インスタンスを再構成する必要があります。

2.2 Key Management Interoperability Protocol (KMIP) を使用したキーの管理

インターシステムズは、KMIP サーバを使用したデータベース暗号化キー管理をサポートしています。KMIP の使用には以下のタスクが含まれます。

- KMIP サーバ構成の作成、編集、または削除
- KMIP サーバ構成のリスト
- KMIP サーバ構成の詳細のリスト
- KMIP サーバ上のキーの作成またはKMIP サーバ上のキーの削除
- KMIP サーバ上のキーのリスト
- KMIP サーバからのデータベース暗号化キーの有効化またはデータベース暗号化キーの無効化
- KMIP サーバからのデータ要素暗号化キーの有効化またはデータ要素暗号化キーの無効化
- KMIP サーバからキー・ファイルへのキーのコピー
- インスタンスの既定の暗号化キーまたはジャーナリング暗号化キーの指定

注釈
- InterSystems IRIS は、KMIP プロトコルのバージョン 1.0–2.1 をサポートしています。
- KMIP のアクティビティは、InterSystems IRIS の macOS インスタンスではサポートされません。

2.2.1 KMIP サーバ構成の作成

InterSystems IRIS と KMIP サーバとの間の接続を確立する場合、KMIP サーバのプロパティを定義してそれを InterSystems IRIS インスタンス内で表す KMIP サーバ構成を作成します。KMIP サーバ構成を作成するには、以下の手順に従います。

1. ベンダの指示に従って KMIP サーバを設定します。

   注意　KMIP サーバを構成する場合、ベンダの指示に従って適切なバックアップ手順をすべて実行してください。キーのバックアップ・コピーがないと、データが永久に失われることがあります。

   サーバを設定したら、InterSystems IRIS で KMIP サーバ構成を設定できます。

2. KMIP サーバ構成を設定するには、以下が必要です。
   - KMIP サーバに対する認証局 (CA) の証明書。これは、信頼された CA である必要があります。KMIP サーバを提供するベンダからこの証明書を受け取るか、そのベンダの指示に従って証明書を入手する必要があります。
   - KMIP サーバと通信する InterSystems IRIS の各インスタンスの公開鍵証明書と秘密鍵。証明書は、信頼された CA によって発行されている必要があります。KMIP サーバを提供するベンダからこの証明書と秘密鍵を受け取るか、そのベンダの指示に従ってそれらを入手する必要があります。
   - KMIP サーバに関する以下の情報
     - その完全修飾 DNS 名または IP アドレス
     - 接続を受け付けるポート番号
     - サーバがサポートする KMIP プロトコルのバージョン
     - クライアントのために必要な TLS 設定

3. KMIP サーバと通信する InterSystems IRIS インスタンス上で、KMIP サーバに対してそのインスタンスを表す TLS 構成を作成します。
   a. ポータルで、**[SSL/TLS 構成]** ページ (**[ホーム]**→**[システム管理]**→**[セキュリティ]**→**[SSL/TLS 構成]**) に移動します。
   b. **[SSL/TLS 構成]** ページで **[新規構成の作成]** ボタンをクリックして、**[新規 SSL/TLS 構成]** ページを表示します。
   c. **[新規 SSL/TLS 構成]** ページで、TLS 構成を設定します。以下に示すフィールドで、以下のように値を指定または選択します。
      - **[有効]** ― このチェック・ボックスにチェックを付けます。
      - **[タイプ]** ― **[クライアント]** を選択します。

      他のフィールド (**[サーバ証明書の検証]**、**[このクライアントの認証情報]**、および **[暗号方式設定]** の各フィールド) の値は、KMIP サーバの要件によって異なります。**[このクライアントの認証情報]** フィールドの値は、クライアントの証明書、クライアントの秘密鍵、および KMIP サーバを提供するベンダから受け取った CA 証明書によって異なります。

      ここで TLS 構成を作成する方法の詳細は、"TLS 構成の作成または編集" を参照してください。

4. KMIP サーバに対して構成を作成します。
   a. ターミナルを起動し、十分な特権を持つユーザとしてログインします。
   b. ターミナル・プロンプトで、**%SYS** ネームスペースに移動します。

```
>set $namespace="%SYS"
```

c. ^SECURITY を実行します。

```
%SYS>do ^SECURITY
```

d. ^SECURITY で、オプション [14]、[KMIP サーバの設定] を選択します。

e. [KMIP サーバの設定] の選択肢で、オプション [1]、[KMIP サーバの作成] を選択します。

f. [KMIP サーバの作成] プロンプトで、以下の値を指定します。

- [作成する KMIP サーバ?]— KMIP サーバ構成の名前。
- [説明?]— 説明テキスト。
- [サーバ・ホストの DNS 名?]— KMIP サーバの完全修飾 DNS 名または IP アドレス。
- [TCP ポート番号?]— KMIP サーバが接続を受け付けるポート番号。
- [OASIS KMIP プロトコル・バージョン?]— KMIP サーバでサポートされているプロトコル・バージョンに関連する数字。これは、KMIP サーバを提供するベンダから受け取った情報の一部です。
- [SSL/TLS 構成名?]— 前の手順で作成した TLS 構成の名前。

  注釈　ここに入力する値の大文字と小文字は、定義されている TLS 構成名と一致する必要があります。

- [非ブロッキング I/O?]— KMIP サーバとの接続で非ブロッキング I/O を有効にするかどうか。[はい] を選択して、非ブロッキング I/O を有効にすることをお勧めします。

  非ブロッキング I/O が有効の場合、[I/O タイムアウト (秒)?] プロンプト (以下を参照) で指定したタイムアウトの経過後に、制御がアプリケーションに戻ります。非ブロッキング I/O が無効の場合は、オペレーティング・システムのタイムアウト (これは発生しない可能性があります) の経過後に制御がアプリケーションに戻ります。
- [自動再接続?]— 接続が解除された場合に InterSystems IRIS が KMIP サーバに再接続するかどうか。インターシステムズでは、[いいえ] を選択して、接続が解除された場合に自動的に再接続を試行しないようにすることをお勧めします。
- [I/O タイムアウト (秒)?]— KMIP サーバとの接続がタイムアウトするまでの時間 (秒)。これは、構成で非ブロッキング I/O が有効になっている場合にのみ関係があります。
- [KMIP メッセージのログ?]— KMIP サーバに送信するメッセージを InterSystems IRIS がログに記録するかどうか。メッセージをログに記録する場合、ログは <install-dir>/mgr/kmipcmd.log ファイルに保存されます。
- [SSL/TLS のデバッグ?]— InterSystems IRIS が TLS デバッグ情報をログに記録するかどうか。情報をログに記録する場合、情報は <install-dir>/mgr/kmipssl.log ファイルに保存されます。

g. KMIP サーバのプロパティの入力を求めるプロンプトの後、[KMIP サーバの作成の確認] プロンプトで、KMIP サーバを作成することを確認します。

注釈　複数の KMIP サーバを使用したり、複数の構成を持つ単一の KMIP サーバを使用したりできます。最後に有効化した構成が既定になります。

2.2.2 KMIP サーバ構成の編集

既存の KMIP サーバ構成のプロパティの値を変更するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、%SYS ネームスペースに移動します。

```
>set $namespace="%SYS"
```

3. ^SECURITY を実行します。

```
%SYS>do ^SECURITY
```

4. ^SECURITY で、オプション [14]、[KMIP サーバの設定] を選択します。
5. [KMIP サーバの設定] の選択肢で、オプション [2]、[KMIP サーバの編集] を選択します。
6. [KMIP サーバの編集] プロンプトで、編集する構成の名前を入力します。
7. ^SECURITY により、KMIP サーバ構成の作成時と同じプロパティの入力を求めるプロンプトが表示されます。構成のプロパティの既存値が既定値として使用されます。必要に応じて、これらの値を変更します。
8. KMIP サーバのプロパティの入力を求めるプロンプトの後、[KMIP サーバ <servername> の変更の確認] プロンプトで、KMIP サーバのプロパティに加えた編集を確認します。

2.2.3 KMIP サーバ構成の削除

KMIP サーバ構成を削除するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、%SYS ネームスペースに移動します。

```
>set $namespace="%SYS"
```

3. ^SECURITY を実行します。

```
%SYS>do ^SECURITY
```

4. ^SECURITY で、オプション [14]、[KMIP サーバの設定] を選択します。
5. [KMIP サーバの設定] の選択肢で、オプション [5]、[KMIP サーバの削除] を選択します。
6. [削除する KMIP サーバ?] プロンプトで、削除する構成の名前を入力します。
7. プロンプトが表示されたら、削除を確認します。

2.2.4 KMIP サーバ構成のリスト

InterSystems IRIS インスタンスの KMIP サーバ構成をリストするには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、%SYS ネームスペースに移動します。

```
>set $namespace="%SYS"
```

3. ^SECURITY を実行します。

```
%SYS>do ^SECURITY
```

4. ^SECURITY で、オプション [14]、[KMIP サーバの設定] を選択します。
5. [KMIP サーバの設定] の選択肢で、オプション [3]、[KMIP サーバのリスト] を選択します。

^SECURITY により、KMIP サーバの既存の構成のリストが、現在使用されているかどうかに関係なく、名前別に表示されます。

2.2.5 KMIP サーバ構成の詳細のリスト

特定の KMIP サーバ構成の詳細を表示するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、**%SYS** ネームスペースに移動します。

   ```
   >set $namespace="%SYS"
   ```

3. ^SECURITY を実行します。

   ```
   %SYS>do ^SECURITY
   ```

4. ^SECURITY で、オプション **[14]**、**[KMIP サーバの設定]** を選択します。
5. **[KMIP サーバの設定]** の選択肢で、オプション **[4]**、**[KMIP サーバの詳細リスト]** を選択します。
6. [どの KMIP 構成を表示しますか?] プロンプトで、KMIP サーバ構成の名前を入力します。

^SECURITY により、指定した構成のプロパティと各プロパティの値のリストが表示されます。

2.2.6 KMIP サーバ上のキーの作成

KMIP サーバ上にデータ暗号化キーを作成するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、**%SYS** ネームスペースに移動します。

   ```
   >set $namespace="%SYS"
   ```

3. ^EncryptionKey を実行します。

   ```
   %SYS>do ^EncryptionKey
   ```

4. ^EncryptionKey で、オプション **[5]**、**[KMIP サーバの管理]** を選択します。
5. プロンプトが表示されたら、キーを作成する KMIP サーバの構成の名前を入力します。
6. 実行するアクションを選択する次のプロンプトで、オプション **[2]**、**[KMIP サーバ上に新規キーを作成]** を選択します。
7. 次のプロンプトで、キー長を選択します。

^EncryptionKey ルーチンによってキーが作成され、そのキー ID が表示されます。新しく作成されたキーは既定では有効化されていません。キーを有効化するには、"KMIP サーバからのデータベース暗号化キーの有効化" を参照してください。

重要　　インターシステムズでは、後で参照できるようにキー ID を記録しておくことをお勧めします。

2.2.7 KMIP サーバ上のキーの削除

KMIP サーバ上の暗号化キーを削除するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、**%SYS** ネームスペースに移動します。

   ```
   >set $namespace="%SYS"
   ```

3. ^EncryptionKey を実行します。

```
%SYS>do ^EncryptionKey
```

4. ^EncryptionKey で、オプション [5]、[KMIP サーバの管理] を選択します。
5. プロンプトが表示されたら、キーを削除する KMIP サーバの構成の名前を入力します。
6. 実行するアクションを選択する次のプロンプトで、オプション [3]、[KMIP サーバ上の既存キーの破棄] を選択します。
7. KMIP サーバ上のキーがリストされ、削除するキーを指定するよう求められます。[キーの選択] プロンプトでキーを指定します。

   警告　キーの唯一の既存コピーを削除する前に、そのコピーを使用している既存の暗号化コンテンツがないことを確実に確認してください。データを解読するために必要なキーのコピーがないと、そのキーで保護されている暗号化データは読み取り不能になり、永久に失われます。

8. プロンプトが表示されたら、キーを削除することを確認します。

KMIP サーバからキーが削除されます。

2.2.8 KMIP サーバ上のキーのリスト

KMIP サーバ上の暗号化キーをリストするには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、%SYS ネームスペースに移動します。

   ```
   >set $namespace="%SYS"
   ```

3. ^EncryptionKey を実行します。

   ```
   %SYS>do ^EncryptionKey
   ```

4. ^EncryptionKey で、オプション [5]、[KMIP サーバの管理] を選択します。
5. プロンプトが表示されたら、キーをリストする KMIP サーバの構成の名前を入力します。
6. 次のプロンプトで、オプション [1]、[KMIP サーバ上のキーのリスト] を選択します。

KMIP サーバ上にあるすべてのキーのリストが表示されます。

2.2.9 KMIP サーバからのデータベース暗号化キーの有効化

KMIP サーバからデータベース暗号化キーを有効化するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、%SYS ネームスペースに移動します。

   ```
   >set $namespace="%SYS"
   ```

3. ^EncryptionKey を実行します。

   ```
   %SYS>do ^EncryptionKey
   ```

4. ^EncryptionKey で、オプション [3]、[データベース暗号化] を選択します。
5. [データベース暗号化] の選択肢で、オプション [1]、[データベース暗号化キーの有効化] を選択します。
6. [データベース暗号化キーの有効化] の選択肢で、オプション [2]、[KMIP サーバの使用] を選択します。

注釈　このプロンプトが表示されない場合、インスタンスに KMIP サーバ構成がありません。このプロセスの手順は、"KMIP サーバ構成の作成" を参照してください。

7. プロンプトが表示されたら、キーを有効化する KMIP サーバの構成の名前を入力します。
8. KMIP サーバ上のキーがリストされ、有効化するキーを指定するよう求められます。**[キーの選択]** プロンプトでキーを指定します。

キーが有効化され、その ID が表示されます。

InterSystems IRIS により有効化されたキーそれぞれについて、有効なキーのテーブルにキーが追加され、そのキーの識別子が **[データベース暗号化]** ページ (**[システム管理]** > **[暗号化]** > **[データベース暗号化]**) に表示されます。

注釈　キーのテーブルにファイルやパスの情報は表示されません。2 番目以降のキーを有効化する場合は、まず、現在有効化されているキーの識別子をメモしてください。これによって新しいキーを識別できます。

2.2.10 KMIP サーバからのデータ要素暗号化キーの有効化

InterSystems IRIS では、データ要素暗号化で一度に 4 つまでの有効なキーがサポートされています。KMIP サーバからデータ要素暗号化キーを有効にするには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、**%SYS** ネームスペースに移動します。

```
>set $namespace="%SYS"
```

3. ^EncryptionKey を実行します。

```
%SYS>do ^EncryptionKey
```

4. ^EncryptionKey で、オプション **[4]**、**[アプリケーションのデータ要素暗号化]** を選択します。
5. **[アプリケーションのデータ要素暗号化]** の選択肢で、オプション **[1]**、**[データ要素暗号化キーの有効化]** を選択します。
6. **[データ要素暗号化キーの有効化]** の選択肢で、オプション **[2]**、**[KMIP サーバの使用]** を選択します。

   注釈　このプロンプトが表示されない場合、インスタンスに KMIP サーバ構成がありません。このプロセスの手順は、"KMIP サーバ構成の作成" を参照してください。

7. KMIP サーバのプロンプトで、キーを有効化する KMIP サーバの構成の名前を入力します。
8. KMIP サーバ上のキーがリストされ、有効化するキーを指定するよう求められます。**[キーの選択]** プロンプトでキーを指定します。

キーが有効化され、その ID が表示されます。

InterSystems IRIS により有効化されたキーそれぞれについて、有効なキーのテーブルにキーが追加され、そのキーの識別子が **[データ要素暗号化]** ページ (**[システム管理]** > **[暗号化]** > **[データ要素暗号化]**) に表示されます。

注釈　キーのテーブルにファイルやパスの情報は表示されません。2 番目以降のキーを有効化する場合は、まず、現在有効化されているキーの識別子をメモしてください。これによって新しいキーを識別できます。

2.2.11 KMIP サーバからキー・ファイルへのキーのコピー

データベース暗号化キーを KMIP サーバからキー・ファイルにコピーできます。これにより、バックアップ、およびネットワークや KMIP サービスの障害からのリカバリの両方でキーを利用できるようになります。以下を実行できます。

- KMIP サーバからのキーのコピーを使用して、データベース暗号化キー・ファイルを作成する
- データベース暗号化キーのコピーを KMIP サーバから既存のキー・ファイルに追加する

重要　　暗号化キー・ファイルは必ず、しっかりと施錠された保管場所で管理されたリムーバブル・デバイスに保存してください。

2.2.11.1 KMIP サーバからのキーのコピーを使用したキー・ファイルの作成

キー・ファイルを作成して、そのキー・ファイルに KMIP サーバからキーをコピーするには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、**%SYS** ネームスペースに移動します。

```
>set $namespace="%SYS"
```

3. ^EncryptionKey を実行します。

```
%SYS>do ^EncryptionKey
```

4. ^EncryptionKey で、オプション [1]、**[新規暗号化キー・ファイルの作成]** を選択します。
5. 続いて表示されるプロンプトで、以下を指定します。
   - キー・ファイルの名前 (**<install-dir>/mgr/** ディレクトリを基準にした相対名)。
   - キー・ファイルの説明。
   - キーの管理者の名前 – これは新しい管理者で、新しい名前を付けることができます。
   - その管理者のパスワード (および確認) – これは新しいパスワードで、有効な値を指定できます。
   - 利用可能な暗号セキュリティ・レベル – ファイルに保存されるキーの暗号化に使用するキーの長さ。
6. 次のプロンプトで、オプション [2]、**[KMIP サーバからキーをコピー]** を選択します。^EncryptionKey により、ファイルにコピーするキーを指定するよう求められます。
7. **[キーの選択]** プロンプトで、コピーするキーの番号を指定します。

^EncryptionKey により、指定した管理者のユーザ名とパスワードを使用してファイルが作成され、選択したキーがそのファイルに配置されます。

2.2.11.2 KMIP サーバから既存のキー・ファイルへのキーのコピーの追加

KMIP サーバから既存のキー・ファイルにキーを追加するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。
2. ターミナル・プロンプトで、**%SYS** ネームスペースに移動します。

```
>set $namespace="%SYS"
```

3. ^EncryptionKey を実行します。

```
%SYS>do ^EncryptionKey
```

4. ^EncryptionKey で、オプション [2]、**[既存の暗号化キー・ファイルの管理]** を選択します。
5. **[暗号化キー・ファイル]** プロンプトで、キーを追加するキー・ファイルのパスと名前を入力します。パスは **<install-dir>/mgr/** ディレクトリを基準にした相対パスです。

6. 次のプロンプトで、オプション [5]、[**暗号化キーの追加**] を選択します。続いて表示されるプロンプトで、以下を行います。
   a. [**既存の管理者**] で、キー・ファイルの管理者のユーザ名とパスワードを [**ユーザ名**] および [**パスワード**] に入力します。
   b. キー・ファイルに追加するキーの説明を入力します。
7. 次のプロンプトで、オプション [2]、[**KMIP サーバからキーをコピー**] を選択します。続いて表示されるプロンプトで、以下を行います。
   a. [**KMIP サーバ**] プロンプトで、キーのコピー元の KMIP サーバの名前を入力します。
   b. [**キーの選択**] プロンプトで、コピーするキーの番号を指定します。

^EncryptionKey により、選択したキーが選択したキー・ファイルに追加されます。

2.3 保存に依存しないキー管理タスク

一部のタスクは、ファイル内のキーおよび KMIP サーバ上のキーに対して行うタスクと同じです。

- データベース暗号化キーの無効化
- データ要素暗号化キーの無効化
- インスタンスの既定のデータベース暗号化キーまたはジャーナル暗号化キーの指定

2.3.1 データベース暗号化キーの無効化

データベース暗号化キーを無効にするには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、[**データベース暗号化**] ページ ([**システム管理**] > [**暗号化**] > [**データベース暗号化**]) に移動します。現在キーが有効になっている場合、キーの識別子はキーのテーブルに表示されます。
2. キーが新しい暗号化データベースまたはジャーナル・ファイルの暗号化の既定のキーである場合、そのキーを無効にすることはできません。これらいずれかのアクティビティに使用されているキーを無効にするには、それらに使用する別のキーを選択する必要があります。これを実行するには、別のキーに対して [**既定に設定**] または [**ジャーナル設定**] をクリックします。キーが前述のいずれかのアクティビティに使用されていない場合、キーの [**無効化**] ボタンが使用できるようになります。
3. キーを無効にするには、キーの行の [**無効化**] をクリックします。

   注釈　何らかの理由でキーを無効にできない場合、ポータルではエラー・メッセージが出力されます。以下の場合、キーを無効にできません。

   - IRISTEMP データベースおよび IRISLOCALDATA データベースが暗号化されている場合
   - このキーで暗号化され現在マウントされている (IRISTEMP および IRISLOCALDATA 以外の) 暗号化データベースがある場合
   - 現在、キーがジャーナル・ファイルの暗号化に使用されている場合(ジャーナル・ファイルの暗号化キーを変更する場合、ジャーナル・ファイルを切り替えるまで古い暗号化キーが引き続き使用されます)

   基盤となる状況への対処方法は、以下を参照してください。

4. 確認ダイアログで [OK] をクリックして、キーを無効にします。

キーを無効にするには、基盤となる状況に応じたアクションを実行する必要があります。

- IRISTEMP および IRISLOCALDATA 以外の暗号化データベースの場合、[**データベース**] ページ ([**システム処理**] > [**データベース**]) でデータベースをディスマウントします。これでキーを無効にできます。
- IRISTEMP および IRISLOCALDATA の場合、これらのデータベースが暗号化されないように指定して、InterSystems IRIS を再起動します。そのためには、[**データベース暗号化**] ページで [**起動設定の構成**] を選択します。起動時にデータベース暗号化キーを有効にしないように選択するか (この場合、InterSystems IRIS により IRISTEMP および IRISLOCALDATA の暗号化が無効にされます)、あるいは起動時にインタラクティブにまたは無人でデータベース暗号化キーを有効にするように選択できます (この場合、IRISTEMP および IRISLOCALDATA を暗号化するかどうかを選択できるので、[いいえ] を選択します)。
- 暗号化されたジャーナル・ファイルの場合、暗号化されたジャーナル・ファイルがリカバリに必要ないことを確認します。詳細は、"暗号化されたジャーナル・ファイル" を参照してください。

2.3.2 データ要素暗号化キーの無効化

データ要素暗号化キーを無効にするには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、[**データ要素暗号化**] ページ ([**システム管理**] > [**暗号化**] > [**データ要素暗号化**]) に移動します。有効になっているキーがある場合、ページにはそれらをリストするテーブルが表示されます。
2. 有効になっているキーのテーブルで、無効にするキーの [**無効化**] をクリックします。操作を確認するダイアログが表示されます。
3. 確認ダイアログで [OK] をクリックします。

[**データ要素暗号化**] ページが再び表示されると、無効化されたキーの行はテーブルに存在しなくなります。

2.3.3 インスタンスの既定のデータベース暗号化キーまたはジャーナル暗号化キーの指定

インスタンスにはそれぞれ既定のデータベース暗号化キーおよび既定のジャーナル暗号化キーがあります。インスタンスは、管理者がデータベース暗号化キーを初めてアクティブ化するときに、これらのそれぞれに初期値を設定します。最初に既定になるキーは、アクティブ化されたキー・ファイルにあるキーによって決まります。これらの値は、InterSystems IRIS をシャットダウンしてから再起動しても保持されます。

これらいずれかの目的で新しいキーを指定するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、[**データベース暗号化**] ページ ([**システム管理**] > [**暗号化**] > [**データベース暗号化**]) に移動します。現在有効なインスタンスの暗号化キーのテーブルが表示されます。
2. 暗号化キーのテーブルで、以下を実行します。
   - 新しい既定の暗号化キーを指定するには、そのキーに対して [**既定に設定**] をクリックします。現在の既定のキーに対する [**既定に設定**] ボタンは使用できません。
   - 新しいジャーナル暗号化キーを指定するには、そのキーに対して [**ジャーナル設定**] をクリックします。現在のジャーナル暗号化キーに対する [**ジャーナル設定**] ボタンは使用できません。
3. アクションの確認を求めるプロンプトが表示されたら、[OK] をクリックします。

InterSystems IRIS により、選択したキーが既定の暗号化キーまたはジャーナル暗号化キーとして設定されます。キーが既定の暗号化キーまたはジャーナル暗号化キーのいずれかである場合、そのキーは削除できません (InterSystems IRIS インスタンスの操作に必要なため)。したがって、キーをこれらのいずれかに指定すると、キーの [**削除**] ボタンは使用できなくなります。

3

暗号化データベースの使用法

機密情報が含まれるデータベース全体を保護するために、InterSystems IRIS® データ・プラットフォームではブロック・レベルのデータベース暗号化（または、データベース暗号化と略されています）がサポートされています。データベース暗号化は、エンティティ全体として暗号化されるデータベースの作成と管理ができるテクノロジです。InterSystems IRIS のキー管理ツールを使用して、これらのアクティビティをサポートします。

データベースの作成時に、これを暗号化することを選択できます。現在有効になっているキーがある場合にこのオプションを選択できます。暗号化データベースを作成すると、暗号化されていないデータベースと同様にこれを使用できます。暗号化テクノロジは透過的で、パフォーマンスに及ぼす影響は小さくて予測可能になります。

ここでは、暗号化データベースを作成および管理する方法を説明します。データベース暗号化機能では、監査ログとジャーナル・ファイルを暗号化する機能もサポートされています。これらの機能は両方とも、"暗号化の起動設定の構成"の説明に従って、起動時にデータベース暗号化キーにアクセスする必要があります。

3.1 暗号化データベースの作成

暗号化データベースを作成する場合は、データベースを新規作成するときに暗号化を指定します。ただし、暗号化データベースを作成する前に、InterSystems IRIS でデータベース暗号化キーを有効にしておく必要があります。以下はその方法です。

1. データベース暗号化キーを有効にします。
2. 管理ポータルのホーム・ページで、**[ローカルデータベース]** ページ（**[システム管理]** > **[構成]** > **[システム構成]** > **[ローカルデータベース]**）に移動します。
3. **[ローカルデータベース]** ページで、**[新規データベース作成]** を選択します。**[データベース]** ウィザードが表示されます。
4. ウィザードの 2 ページ目で、**[暗号化データベース?]** ボックスで **[はい]** を選択します。これによって、暗号化データベースが作成されます。ウィザードのその他すべてのページで、データベースを作成する際にデータベースに設定する特性を選択します（データベースの作成の詳細は、"ローカル・データベースの作成" を参照してください）。

注釈　InterSystems IRIS には、暗号化されていないデータベースの暗号化や暗号化データベースの解読のための暗号化管理ツールも必要に応じて用意されています。

3.2 暗号化データベースへのアクセスの確立

ミラーにデータベースを追加するなど、さまざまな操作を実行するには、データベースをマウントする必要があります。ただし、暗号化データベースをマウントする場合、そのキーを有効にする必要があります。したがって、データベースにアクセスするには、キーを有効にし、データベースをマウントする必要があります。その手順は以下のとおりです。

1. キーを有効にします。
2. 管理ポータルのホーム・ページで、[**データベース**] ページ ([**システム処理**] > [**データベース**]) に移動します。
3. このページで、マウントするデータベースに対して、データベースのテーブルでその行の右端の列にある [**マウント**] ボタンを選択します。確認画面で [OK] を選択すると、データベースがマウントされます。キーが有効になっていないと、データベースはマウントできず、エラー・メッセージが表示されます。

これで、データベースのデータにアクセスできるようになります。

3.3 暗号化データベースへの接続の切断

暗号化データベースへの接続を切断するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、[**データベース**] ページ ([**システム処理**] > [**データベース**]) に移動します。
2. このページで、データベースのテーブルで右にある [**ディスマウント**] ボタンを選択します。確認画面で [OK] を選択すると、データベースがディスマウントされます。
3. キーを無効にします。

データベースに対する読み取りおよび書き込みのたびに、有効になっているキーが使用されるので、先にデータベースをディスマウントしないとキーを無効にできません。データベースをディスマウントせずにキーを無効にしようとすると、エラー・メッセージが表示されます。

3.4 インスタンス間での暗号化データベースの移動

複数の InterSystems IRIS インスタンスを使用している組織では、あるインスタンスで異なるキーを使用して作成された暗号化データベースを別のインスタンスで使用することが必要になる場合があります。インスタンス間でデータを移動するには、データベースをバックアップした後、利用可能な暗号化管理ツールを使用してそのデータベースを再暗号化する必要があります。詳細は、"^EncryptionKey を使用したデータベース暗号化の変更" を参照してください。

3.5 暗号化の起動設定の構成

ここでは、データベース暗号化を行う 3 つの起動オプションそれぞれを設定する方法について説明します。

- キーを有効化しない起動 (既定) ― インスタンスには、起動時に利用可能なデータベース暗号化キーはありません。
- インタラクティブにキーを有効化する起動 ― インスタンスは、起動時にインタラクティブにデータベース暗号化キー情報を収集します。

- 無人のキー有効化による起動 ーインスタンスでは起動時に人的操作なしにデータベース暗号化キー情報を収集します。これは無人起動とも呼ばれます。

InterSystems IRIS のいくつかの機能では、起動時に (インタラクティブに、または無人起動によって) キーが利用可能である必要があります。

- InterSystems IRIS 監査ログの暗号化。
- **IRISTEMP** データベースおよび **IRISLOCALDATA** データベースの暗号化(両方とも暗号化するか、または両方とも暗号化しないかのいずれかです)。
- InterSystems IRIS ジャーナル・ファイルの暗号化。
- 暗号化データベースの起動時のマウント

3.5.1 キーを有効化しない起動

まだどのキーも有効化していない場合、これが InterSystems IRIS のインスタンスの既定の動作です。起動時のキーの有効化が設定されている場合に、これを解除するには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[データベース暗号化]** ページ (**[システム管理]** > **[暗号化]** > **[データベース暗号化]**) に移動します。
2. **[起動設定の構成]** を選択します。InterSystems IRIS の起動の構成用オプション、および暗号化データベース用のその他のオプションがある領域が表示されます。
3. この領域で、**[起動オプション]** リストから **[なし]** を選択します。
4. **[保存]** をクリックします。以下の場合、このアクションを実行できない可能性があります。
   - 起動時に暗号化データベースが必要な場合。詳細は、"起動時に暗号化データベースが必要な場合"を参照してください。
   - 暗号化されたジャーナル・ファイルのいずれかでトランザクションが開いている場合。詳細は、"暗号化されたジャーナル・ファイル" を参照してください。
   - 監査ログが暗号化されている場合 (この場合、エラー・メッセージで暗号化データベースが参照されます。これは、監査ログが **IRISAUDIT** と呼ばれる InterSystems IRIS データベースに格納されているためです)。詳細は、"暗号化された監査ログ" を参照してください。

   変更を妨げている問題に対処してから、この手順を再び実行してください。問題が修正されると、キーを有効化しない起動への変更を正常に行えるようになります。

3.5.1.1 起動時に暗号化データベースが必要な場合

起動時に必要な暗号化データベースがインスタンスにある場合、起動時にキーの有効化を含めないよう構成しようとすると、起動時に暗号化データベースが必要であること、およびキーの有効化オプションの変更が不可であることを示すエラー・メッセージが管理ポータルに表示されます (エラー・メッセージで **IRISAUDIT** データベースが参照されている場合、監査ログは暗号化されています)。

暗号化キーを有効化せずに InterSystems IRIS が起動するよう構成するために、起動後にのみ暗号化データベースをマウントできます。起動後にデータベースがマウントされるように構成するには、以下の手順に従います。

1. データベースがマウントされていることを確認し、そうでなければデータベースをマウントします。
   a. 管理ポータルのホーム・ページで、**[データベース]** ページ (**[システム処理]** > **[データベース]**) に移動します。

b. データベースのテーブルで、そのデータベースの行を検索します。データベースがマウントされている場合、その行に [**ディスマウント**] オプションがあります。データベースがマウントされていない場合、[**ディスマウント**] オプションではなく、[**マウント**] オプションがあります。

c. データベースがマウントされていない場合、[**マウント**] を選択します。

d. 確認画面で [OK] を選択します(データベースは書き込み可能である必要があるため、[**読み取り専用**] チェック・ボックスにチェックを付けないでください)。

2. データベースが起動時にマウントされないよう、データベースのプロパティを編集します。

a. [**ローカルデータベース**] ページ ([**システム管理**] > [**構成**] > [**システム構成**] > [**ローカルデータベース**]) に移動します。

b. データベースのテーブルで、そのデータベースの行を検索します。

c. データベース名をクリックしてデータベースを選択します。データベースを編集するためのページが表示されます。

d. この [**編集**] ページで、[**起動時にマウントが必要**] チェック・ボックスのチェックを外します。

e. [**保存**] をクリックします。

これでデータベースは起動時にマウントされなくなります。つまり、データベースは起動時にキーの有効化を必要としなくなります (他の理由で必要となる場合があります)。

3.5.1.2 暗号化されたジャーナル・ファイル

インスタンスでジャーナリングが使用されている場合、起動時にキーの有効化を含めないよう構成しようとすると、起動時にキーの有効化をオフにできない場合があります。該当する状況は以下のとおりです。

- そのジャーナル・ファイルを暗号化するようにインスタンスが構成されている場合
- 開いているトランザクションが (使用率の高いシステム上にある可能性が高い) ジャーナル・ファイルにある場合

この状況に該当する場合、起動時のキー有効化設定を変更する前に、暗号化されたジャーナル・ファイルの使用を中断する必要があります。そのための手順は以下のとおりです。

1. [**データベース暗号化**] ページ ([**システム管理**]→[**暗号化**]→[**データベース暗号化**]) で、[**暗号化ジャーナルファイル**] の設定を [**いいえ**] に変更します。[**起動時のキー有効化**] の設定はそのままにします。
2. ジャーナル・ファイルを切り替えます。これを行うには、[**ジャーナル**] ページ ([**システム処理**] > [**ジャーナル**]) で [**ジャーナル切り替え**] をクリックします。

暗号化されたジャーナル・ファイルで開いているトランザクションがすべてコミットまたはロールバックされると、InterSystems IRIS の起動の構成を変更できます。

注意　開いているトランザクションがなくなった後も、データベースをリストアする際に暗号化されたジャーナル・ファイルが必要になる場合があります。そのため、これらのファイルの暗号化に使用するキーがあるキー・ファイルのコピーを維持することが非常に重要です。

ジャーナル・ファイルの全般的な詳細は、"ジャーナリング" を参照してください。

3.5.1.3 暗号化された監査ログ

インスタンスに暗号化された監査ログがある場合、起動時にキーの有効化を含めないよう構成しようとすると、InterSystems IRIS では、起動時に暗号化データベースが必要であるという以下のようなエラー・メッセージが表示されます。

```
ERROR #1217: Can not disable database encryption key activation at startup.
Encrypted databases are required at startup:
C:\InterSystems\IRIS\Mgr\IRISAudit\
```

このエラー・メッセージでは暗号化データベースが参照されています。これは、監査ログが **IRISAUDIT** という InterSystems IRIS データベースに格納されているためです。

暗号化キーを有効化せずに InterSystems IRIS を起動すると、監査ログを暗号化できません。起動時にキーの有効化を含めないよう構成するには、InterSystems IRIS の設定を変更して、暗号化されていない監査ログをインスタンスで使用するように指定する必要があります。以下はその方法です。

1. インスタンスの監査データをバックアップします。
2. **[データベース暗号化]** ページ (**[システム管理]** > **[暗号化]** > **[データベース暗号化]**) に移動します。
3. **[起動設定の構成]** を選択すると、InterSystems IRIS の起動の構成用オプションおよび暗号化データベース用のその他のオプションがある領域が表示されます。
4. **[オプションで暗号化されたデータ]** の **[監査ログ暗号化]** リストで、**[いいえ]** をクリックします。

この設定を変更すると、既存の監査データがすべて消去され (ある場合)、直ちに暗号化されていない監査の使用が開始され、監査ログに AuditChange イベントが書き込まれます。

注意　監査データをバックアップしていない場合、監査ログの暗号化設定を変更すると該当する既存の監査データが失われます。

3.5.2 インタラクティブにキーを有効化する起動

キーが有効化されている場合、これが InterSystems IRIS のインスタンスの既定の動作です。インタラクティブなキーの有効化では、InterSystems IRIS のインスタンスにより、起動時にキーの場所およびキーの関連情報を入力するよう求められます。

重要　Windows の場合、インタラクティブなキーの有効化は、システム起動の一環で自動的に開始するサービスとして InterSystems IRIS を構成していると両立できなくなります。

インタラクティブなキーの有効化に対応するように InterSystems IRIS を構成するには、以下の操作を実行します。

1. 管理ポータルのホーム・ページで、**[データベース暗号化]** ページ (**[システム管理]** > **[暗号化]** > **[データベース暗号化]**) に移動します。
2. **[起動設定の構成]** を選択します。**[起動オプション]** 領域が表示され、**[起動時のキー有効化]** リストが表示されます。
3. **[起動時のキー有効化]** リストで、**[インタラクティブ]** を選択します。それまでのこのフィールドの値が **[なし]** となっていた場合は、この操作によってページの **[オプションで暗号化されたデータ]** 領域が表示されます。
4. この領域のフィールドは以下のとおりです。
   - **[IRISTEMP および IRISLOCALDATA データベースの暗号化]** – IRISTEMP データベースと IRISLOCALDATA データベースを暗号化するかどうかを指定できます。暗号化する場合は **はい** を選択し、暗号化しない場合は **[いいえ]** を選択します。
   - **[暗号化ジャーナルファイル]** – インスタンスで独自のジャーナル・ファイルを暗号化するかどうかを指定できます。ジャーナル・ファイルを暗号化する場合は **[はい]** を選択し、暗号化しない場合は **[いいえ]** を選択します。InterSystems IRIS を起動すると新しいジャーナル・ファイルが作成されるため、選択は起動オプションによって決まります。暗号化を選択した場合は、起動時にキーが必要です。

     注釈　この変更は、InterSystems IRIS が次にジャーナル・ファイルを切り替えたときに有効になります。再起動せずにジャーナル・ファイルの暗号化を開始するには、このページの操作を完了してからジャーナル・ファイルを切り替えます。

- **[監査ログ暗号化]** – InterSystems IRIS が監査ログを暗号化するかどうかを指定できます。監査ログを暗号化する場合は **[はい]** を選択し、暗号化しない場合は **[いいえ]** を選択します。InterSystems IRIS を起動するとさまざまなイベントが監査ログに記録されるため、選択は起動オプションによって決まります。暗号化を選択した場合は、起動時にキーが必要です。

  注意　この変更は直ちに反映され、既存の監査データがすべて削除されます。この設定を変更する前に監査データベースをバックアップしてください。そうしないと、監査データが失われます。

5. **[保存]** をクリックして、選択した設定内容を保存します。

重要　InterSystems IRIS が以下のように構成されている場合を考えます。

- **IRISTEMP** および **IRISLOCALDATA**、ジャーナル・ファイル、または監査ログを暗号化する
- 起動時に暗号化データベースを必要とする

この場合、必要な暗号化キーを有効にしないと InterSystems IRIS の起動に失敗します。起動に失敗した場合は、InterSystems IRIS の緊急起動モードを使用して、起動時に暗号化機能をまったく必要としないように InterSystems IRIS を構成します。

3.5.3 無人のキー有効化による起動

無人でキーを有効化する起動は無人起動とも呼ばれ、キーを有効化し、可能であれば起動時に人的操作なしに暗号化データベースをマウントします。無人起動を正常に実行するには、インスタンスが以下にアクセスできる必要があります。

- 暗号化データベース。
- データベース暗号化キー。以下のいずれかの方法によります。
  - キーを格納する KMIP サーバ
  - データベース暗号化キー・ファイル（キー、およびユーザ名とパスワード（データベース暗号化キーの無人有効化に使用されます）が格納されます）

このセクションでは、以下のトピックについて説明します。

- KMIP サーバ上のキーを使用した無人起動の構成
- キー・ファイル内のキーを使用した無人起動の構成
- 無人起動の問題への一時的な対処

注意　これらの要素をすべて利用可能にすることで、InterSystems IRIS にあるデータのセキュリティは、これらの要素が保持されているマシンの物理的セキュリティに、全面的に依存することになります。このような物理的セキュリティが確保されていないサイトのデータは、そのデータが暗号化されていない場合と同等のセキュリティ上のリスクにさらされます。この状態を避けるには、インタラクティブな起動を使用するか（こうすれば、すべての要素が同時にリスクにさらされることがなくなります）、関連するマシンの物理的セキュリティを確保するようにします。

3.5.3.1 KMIP サーバ上のキーを使用した無人起動の構成

KMIP サーバ上のキーを使用して無人で起動するよう InterSystems IRIS インスタンスを構成するには、以下の手順に従います。

1. 関連するインスタンスに対して、ターミナルを起動し、十分な特権を持つユーザとしてログインします。

2. ターミナル・プロンプトで、%SYS ネームスペースに移動します。

```
>set $namespace="%SYS"
```

3. ^EncryptionKey を実行します。

```
%SYS>do ^EncryptionKey
```

4. ^EncryptionKey で、オプション [3]、[**データベース暗号化**] を選択します。
5. 次のプロンプトで、オプション [4]、[**起動オプションの構成**] を選択します。
6. 次のプロンプトで、オプション [4]、[**KMIP サーバを使用したキーの無人有効化**] を選択します。
7. [**KMIP サーバのインスタンス名**] プロンプトで、KMIP サーバ構成の名前を入力します。
8. 続いて表示されるプロンプトで、暗号化する項目を指定します(これらすべての項目で起動時に有効なキーが必要になります)。
   - [**暗号化ジャーナルファイル**] (既定は [いいえ]) – インスタンスで独自のジャーナル・ファイルを暗号化するかどうかを指定できます。ジャーナル・ファイルを暗号化する場合は [**はい**] を入力し、暗号化しない場合は [**いいえ**] (既定) を入力または選択します。InterSystems IRIS を起動すると新しいジャーナル・ファイルが作成されるため、選択は起動オプションによって決まります。暗号化を選択した場合は、起動時にキーが必要です。

     この変更は、InterSystems IRIS が次にジャーナル・ファイルを切り替えたときに有効になります。既定では、これは InterSystems IRIS を次回再起動したときに実行されます。再起動せずにジャーナル・ファイルの暗号化を開始するには、このページの操作を完了してからジャーナル・ファイルを切り替えます。
   - [**IRISTEMP および IRISLOCALDATA データベースの暗号化**] (既定は [いいえ]) – IRISTEMP データベースと IRISLOCALDATA データベースを暗号化するかどうかを指定できます。暗号化する場合は [**はい**] を入力し、暗号化しない場合は [**いいえ**] (既定) を入力または選択します。
   - [**監査データベースの暗号化**] (既定は [いいえ]) – InterSystems IRIS が監査ログを暗号化するかどうかを指定できます。監査ログを暗号化する場合は [**はい**] を選択し、暗号化しない場合は [**いいえ**] (既定) を選択します。InterSystems IRIS を起動するとさまざまなイベントが監査ログに記録されるため、選択は起動オプションによって決まります。暗号化を選択した場合は、起動時にキーが必要です。

     注意　この変更は直ちに反映され、既存の監査データがすべて削除されます。この設定を変更する前に監査データベースをバックアップしてください。そうしないと、監査データが失われます。
9. 続いて、起動時に有効化する KMIP キーの現在のリストが表示され、次のアクションを指定するよう求められます。
   - 起動キーのリストにキーを追加するには、オプション [1]、[**キーをリストに追加**] を選択します。
   - 起動キーのリストからキーを削除するには、オプション [2]、[**キーをリストから削除**] を選択します。
   - 起動キーのリストを保存するには、オプション [3]、[**リストの保存**] を選択します。
10. リストに、起動時に有効化する KMIP キーの目的のリストが含まれる場合、オプション [3] を選択して、リストを保存します。

3.5.3.2 キー・ファイル内のキーを使用した無人起動の構成

注意　無人起動するように InterSystems IRIS を構成すると、そのインスタンスによってデータベース暗号化キー・ファイルに別の管理者が追加されます。その管理者にはシステムによって生成された名前とパスワードがあります。InterSystems IRIS によってキー・ファイルが変更されてこのユーザ名とパスワードが追加された後は、鍵付きのラック設置式 CD-ROM ドライブまたは DVD ドライブのように物理的に鍵がかけられるハードウェア上にのみキー・ファイルのコピーを配置することを強くお勧めします。さらに、このハードウェアが格納されているデータ・センタの施設を施錠して監視下に置く必要があります。データベース暗号化キーは、そのキーを使用して暗号化したデータベースと同じドライブには格納しないでください。

キー・ファイル内のキーを使用して無人で起動するよう InterSystems IRIS インスタンスを構成するには、以下の手順に従います。

1. 先にキーを有効にしておく必要があります。キーを有効にするには、"キーの有効化" を参照してください。
2. 管理ポータルのホーム・ページで、**[データベース暗号化]** ページ (**[システム管理]→[暗号化]→[データベース暗号化]**) に移動します。
3. **[起動設定の構成]** を選択します。**[起動オプション]** リストが表示されます。
4. **[起動オプション]** で、**[自動 (推奨されていません)]** を選択します。これにより、ページに表示されるフィールドが変更されます。
5. **[起動オプション]** 領域が展開され、3 つのフィールドが表示されます。以下を設定します。
   - **[キー・ファイル]** – データベース暗号化キー・ファイルのパス。ここでは絶対パスと相対パスのどちらでも指定できます。相対パスで指定した場合は、InterSystems IRIS のインストール・ディレクトリが基準になります。**[参照]** をクリックすると、ファイル・システム上でデータベース暗号化キー・ファイルを探します。
   - **[管理者名]** – このキー・ファイルの管理者。
   - **[パスワード]** – 管理者のパスワード。
6. **[オプションで暗号化されたデータ]** 領域で、以下のフィールドにすべて入力します。
   - **[IRISTEMP および IRISLOCALDATA データベースの暗号化]** – IRISTEMP データベースと IRISLOCALDATA データベースを暗号化するかどうかを指定できます。暗号化する場合は **はい** を選択し、暗号化しない場合は **[いいえ]** を選択します。
   - **[暗号化ジャーナルファイル]** – インスタンスで独自のジャーナル・ファイルを暗号化するかどうかを指定できます。ジャーナル・ファイルを暗号化する場合は **[はい]** を選択し、暗号化しない場合は **[いいえ]** を選択します。InterSystems IRIS を起動すると新しいジャーナル・ファイルが作成されるため、選択は起動オプションによって決まります。暗号化を選択した場合は、起動時にキーが必要です。

     注釈　この変更は、InterSystems IRIS が次にジャーナル・ファイルを切り替えたときに有効になります。既定では、これは InterSystems IRIS を次回再起動したときに実行されます。再起動せずにジャーナル・ファイルの暗号化を開始するには、このページの操作を完了してからジャーナル・ファイルを切り替えます。

   - **[監査ログ暗号化]** – InterSystems IRIS が監査ログを暗号化するかどうかを指定できます。監査ログを暗号化する場合は **[はい]** を選択し、暗号化しない場合は **[いいえ]** を選択します。InterSystems IRIS を起動するとさまざまなイベントが監査ログに記録されるため、選択は起動オプションによって決まります。暗号化を選択した場合は、起動時にキーが必要です。

     注意　この変更は直ちに反映され、既存の監査データがすべて削除されます。この設定を変更する前に監査データベースをバックアップしてください。そうしないと、監査データが失われます。

7. [保存] をクリックして、選択した設定内容を保存します。

3.5.3.3 無人起動の問題への一時的な対処

InterSystems IRIS が以下のように構成されている場合を考えます。

- IRISTEMP および IRISLOCALDATA、ジャーナル・ファイル、または監査ログを暗号化する
- 起動時に暗号化データベースを必要とする

この場合、暗号化キーを有効にしないと InterSystems IRIS の起動に失敗します。起動に失敗した場合は、InterSystems IRIS の緊急起動モードを使用して、起動時に暗号化機能をまったく必要としないように InterSystems IRIS を構成します。

3.6 InterSystems IRIS 付属のデータベースの暗号化

InterSystems IRIS の各インスタンスには、数多くのデータベースが付属しています。暗号化する機能および暗号化の値は、以下のようにデータベースによって異なります。

- IRISLOCALDATA：IRISTEMP データベースと組み合わせて暗号化できます。IRISLOCALDATA を暗号化するには、起動時にこのデータベースを必要とするため、キーが起動時に使用可能である必要があります。
- IRISAUDIT：暗号化できます。IRISAUDIT を暗号化するには、起動時にこのデータベースを必要とするため、キーが起動時に使用可能である必要があります。
- IRISLIB：暗号化しないでください。(IRISLIB の内容はすべて公開されます。)
- IRISSYS：暗号化しないでください。インスタンスに含まれているこのデータベースが暗号化された形式になっている場合、InterSystems IRIS は起動できません。
- IRISTEMP：IRISLOCALDATA データベースと組み合わせて暗号化できます。IRISTEMP を暗号化するには、起動時にこのデータベースを必要とするため、キーが起動時に使用可能である必要があります。
- USER：暗号化できます。

3.7 ^EncryptionKey を使用したデータベース暗号化の変更

管理ポータルからは実行できない暗号化管理操作の実行が必要になる場合があります。^EncryptionKey ユーティリティを使用すると、以下のアクションを実行できます。

- 暗号化されていないデータベースを暗号化データベースに変換する
- 暗号化データベースを暗号化されていないデータベースに変換する
- 新しいキーを使用するように暗号化データベースを変換する

^EncryptionKey ユーティリティで使用されるツールには以下のことが当てはまります。

^EncryptionKey ユーティリティでは、一連の暗号化管理ツールが使用されます。

- 暗号化関連アクティビティで組み込みのハードウェア命令が利用可能な場合、これらのアクティビティは、ソフトウェア・ベースの暗号化よりもかなり高速です。暗号化管理ツールは、利用可能であればハードウェア命令を使用します。

- 暗号化管理ツールは、KMIP サーバ上に保存されたキーを使用できます。
- 暗号化管理ツールは FIPS モードで実行できます。

注釈　暗号化管理ツールはジャーナル・ファイルでは動作しません。

3.7.1 暗号化されていないデータベースを暗号化データベースに変換する

暗号化されていないデータベースを暗号化データベースに変換するには、以下の手順に従います。

1. 暗号化されるデータベースのデータをバックアップします。

   InterSystems IRIS は、所定位置のデータを暗号化します。つまり、この処理ではディスク上の領域を使用します(データベースを別の場所にコピーして正常解読後に現在のディスクの場所にデータベースをリストアする処理は行いません)。処理が完了する前にユーティリティが無効になった場合、データベースは暗号化された部分と暗号化されていない部分が混在して、使用不可能になります。

   注意　データベースを変換する前にそのバックアップを作成しておくことは重要です。バックアップを作成しておかないと、データが失われる可能性があります。

2. データベースを暗号化するキーをキー・ファイルまたは KMIP サーバから有効化します。
3. ターミナルを開始します。
4. %SYS ネームスペースで、^EncryptionKey ユーティリティを実行します。
5. ^EncryptionKey で、オプション [3]、[**データベース暗号化**] を選択します。
6. [データベース暗号化] サブメニューで、オプション [7]、[**既存データベースの暗号化ステータスの変更**] を選択します。
7. [**データベースディレクトリ**] サブメニューで、変更するデータベースを選択します。データベースがディレクトリ別にリストされます。データベースを選択すると、データベースが暗号化されているかどうかが通知されます。
8. データベースが暗号化されていない場合、このルーチンで暗号化できます。[**データベースを暗号化しますか?**] プロンプトで、yes または y を入力します。大文字と小文字は区別されません。
9. [**暗号化のキーの選択**] プロンプトで、データベースの暗号化に使用するキーを選択します。データベースが現在マウントされている場合は、その情報が表示されます。
10. データベースが現在マウントされている場合は、その旨が表示されます。[**データベースディスマウント**] プロンプトで、yes または y を入力します。大文字と小文字は区別されません。

    重要　データベースをディスマウントしてから再マウントすると操作が中断されるため、適切な予防措置を実施して、問題が発生しないようにしてください。

続いて、ルーチンによってデータベースが暗号化されます。このプロセスの一部として、データベースがマウントされていた場合、データベースをディスマウントしてマウントしたことを示すメッセージが表示されます。データベースが再びマウントされたら、暗号化は完了です。

3.7.2 暗号化データベースを暗号化されていないデータベースに変換する

暗号化データベースを暗号化されていないデータベースに変換するには、以下の手順に従います。

1. 暗号化されないデータベースのデータをバックアップします。

   InterSystems IRIS は、所定位置のデータの暗号化を解除します。つまり、この処理ではディスク上の領域を使用します(データベースを別の場所にコピーして正常解読後に現在のディスクの場所にデータベースをリストアする処理

は行いません)。処理が完了する前にユーティリティが無効になった場合、データベースは暗号化された部分と暗号化されていない部分が混在して、使用不可能になります。

注意　データベースを変換する前にそのバックアップを作成しておくことは重要です。バックアップを作成しておかないと、データが失われる可能性があります。

2. データベースを暗号化するキーをキー・ファイルまたは KMIP サーバから有効化します。
3. ターミナルを開始します。
4. %SYS ネームスペースで、^EncryptionKey ユーティリティを実行します。
5. ^EncryptionKey で、オプション [3]、[**データベース暗号化**] を選択します。
6. [データベース暗号化] サブメニューで、オプション [7]、[**既存データベースの暗号化ステータスの変更**] を選択します。
7. [**データベースディレクトリ**] サブメニューで、変更するデータベースを選択します。データベースがディレクトリ別にリストされます。データベースを選択すると、データベースが暗号化されているかどうかが通知されます。データベースが暗号化されていて、その暗号化キーが有効化されていない場合、その旨も通知されます。
8. データベースが暗号化されている場合、このルーチンで解読できます。[**データベースを解読しますか?**] プロンプトで、yes または y を入力します。大文字と小文字は区別されません。
9. データベースの暗号キーがレポートされた後、データベースを別のキーで暗号化するかどうかを尋ねられます。Enter キーを押して、データベースを解読済みデータベースに変換し、新しいキーを使用して暗号化します。
10. データベースが現在マウントされている場合は、その情報が表示されます。[**データベースディスマウント**] プロンプトで、yes または y を入力します。大文字と小文字は区別されません。

重要　データベースをディスマウントしてから再マウントすると操作が中断されるため、適切な予防措置を実施して、問題が発生しないようにしてください。

続いて、ルーチンによってデータベースが解読されます。このプロセスの一部として、データベースがマウントされていた場合、データベースをディスマウントしてマウントしたことを示すメッセージが表示されます。データベースが再びマウントされたら、解読は完了です。

3.7.3 新しいキーを使用するように暗号化データベースを変換する

新しいキーを使用するように暗号化データベースを変換するには、以下の手順に従います。

1. 再暗号化されるデータベースのデータをバックアップします。

   InterSystems IRIS は、所定位置のデータを暗号化します。つまり、この処理ではディスク上の領域を使用します(データベースを別の場所にコピーして正常解読後に現在のディスクの場所にデータベースをリストアする処理は行いません)。処理が完了する前にユーティリティが無効になった場合、データベースは暗号化された部分と暗号化されていない部分が混在して、使用不可能になります。

   注意　データベースを変換する前にそのバックアップを作成しておくことは重要です。バックアップを作成しておかないと、データが失われる可能性があります。

2. キー・ファイルまたは KMIP サーバから、データベースを暗号化するキーと再暗号化するキーを有効化します。
3. ターミナルを開始します。
4. %SYS ネームスペースで、^EncryptionKey ユーティリティを実行します。
5. ^EncryptionKey で、オプション [3]、[**データベース暗号化**] を選択します。

6. [データベース暗号化] サブメニューで、オプション [7]、[**既存データベースの暗号化ステータスの変更**] を選択します。
7. [**データベースディレクトリ**] サブメニューで、変更するデータベースを選択します。データベースがディレクトリ別にリストされます。データベースを選択すると、データベースが暗号化されているかどうかが通知されます。
8. データベースが暗号化されている場合、このルーチンで解読できます。[**データベースを解読しますか?**] プロンプトで、yes または y を入力します。大文字と小文字は区別されません。
9. 次のプロンプト [**データベースを再暗号化しますか?**] で、yes または y を入力します。大文字と小文字は区別されません。
10. [**暗号化のキーの選択**] プロンプトで、データベースの暗号化に使用するキーを選択します。
11. データベースが現在マウントされている場合は、その情報が表示されます。[**データベースディスマウント**] プロンプトで、yes または y を入力します。大文字と小文字は区別されません。

    重要　　データベースをディスマウントしてから再マウントすると操作が中断されるため、適切な予防措置を実施して、問題が発生しないようにしてください。

続いて、ルーチンによってデータベースが再暗号化されます。このプロセスの一部として、データベースがマウントされていた場合、データベースをディスマウントしてマウントしたことを示すメッセージが表示されます。データベースが再びマウントされたら、暗号化は完了です。

4

データ要素暗号化の使用法

データ要素暗号化により、データベース全体を暗号化するよりも、アプリケーション・データをよりきめ細かく暗号化する方法が実現されます。漏洩防止が必要な機密データ要素のためのものです。例えば、顧客のレコードでクレジット・カード情報のフィールドを排他的に暗号化できます。検査結果 (HIV 検査など) を表示するフィールドを患者レコードで排他的に暗号化できます。社会保障番号が記載されたレコードで該当フィールドを排他的に暗号化できます。

データ要素暗号化は、管理ポータルからではなく、(API により) プログラムで使用できます。API によりアクセスできるので、アプリケーション・コードでこれを使用できます。データ要素暗号化をデータベース暗号化で使用するオプションがあります (両方を使用する必要はありません)。

アプリケーションでデータ要素暗号化を使用するには、アプリケーション実行時に必要なキーが使用可能である必要があります。キーを使用可能にするには、これを有効にします。詳細は、"プログラムで管理するキー"、またはポータルを使用する場合は "データ要素暗号化キーの有効化" を参照してください。キーが有効化されると、InterSystems IRIS® データ・プラットフォームではその一意の識別子が有効化キーのテーブルに表示されます。アプリケーションではその識別子を使用してキーを参照し、暗号化処理のためにメモリにロードできます。同時に 4 つまでのキーを有効にできるので、データ要素暗号化では複数のキーが必要なタスクのインフラストラクチャが実現します。

データ要素暗号化のデータを暗号化する際、InterSystems IRIS では結果として得られる暗号化テキストと共に暗号化キーの一意の識別子を格納します。一意の識別子により、暗号化テキスト自体のみを使用して解読時にシステムでキーを識別できます。

ここでは以下について説明します。

- プログラムで管理するキー
- データ要素暗号化の呼び出し
- リアルタイムのデータの再暗号化のサポート

4.1 プログラムで管理するキー

データ要素暗号化は API により使用できるので、キーを管理するための一連の呼び出しもあります。

- $SYSTEM.Encryption.CreateEncryptionKey
- $SYSTEM.Encryption.ActivateEncryptionKey
- $SYSTEM.Encryption.DeactivateEncryptionKey
- $SYSTEM.Encryption.ListEncryptionKeys

これらはすべて、%SYSTEM.Encryption クラスのメソッドです。

4.2 データ要素暗号化の呼び出し

データ要素暗号化で利用できるシステム・メソッドは、%SYSTEM.Encryption クラスのすべてのメソッドで、以下のとおりです。

- $SYSTEM.Encryption.AESCBCManagedKeyEncrypt
- $SYSTEM.Encryption.AESCBCManagedKeyDecrypt
- $SYSTEM.Encryption.AESCBCManagedKeyEncryptStream
- $SYSTEM.Encryption.AESCBCManagedKeyDecryptStream

上記のメソッド名の先頭はすべて“AESCBCManagedKey”になります。それらのメソッドが AES (Advanced Encryption Standard) を CBC (Cipher Block Chaining) モードで使用し、マネージド・キー暗号化の一連のツールの一部であるためです。

重要　“ManagedKey”が名前に含まれない AESCBC メソッドは、古いメソッドでこれらの目的では使用できません。

4.2.1 $SYSTEM.Encryption.AESCBCManagedKeyEncrypt

このメソッドのシグニチャは、通常の呼び出しと同様に以下のようになります。

```
$SYSTEM.Encryption.AESCBCManagedKeyEncrypt
        (
        plaintext As %String,
        keyID As %String,
        )
    As %String
```

各要素の内容は以下のとおりです。

- plaintext ー 暗号化対象となる暗号化されていないテキスト。
- keyID ー 平文の暗号化に使用されるデータ暗号化キーの GUID。
- メソッドは、暗号化されたテキストを返します。

メソッドが正常に実行できなかった場合、このメソッドは <FUNCTION> エラーまたは <ILLEGAL VALUE> エラーをスローします。このメソッドの呼び出しを Try-Catch ループに記述します。Try-Catch の詳細は、″TRY-CATCH メカニズム″を参照してください。

詳細は、″$SYSTEM.Encryption.AESCBCManagedKeyEncrypt″ のクラス・リファレンス・コンテンツを参照してください。

4.2.2 $SYSTEM.Encryption.AESCBCManagedKeyDecrypt

このメソッドのシグニチャは、通常の呼び出しと同様に以下のようになります。

```
$SYSTEM.Encryption.AESCBCManagedKeyDecrypt
        (
        ciphertext As %String
        )
    As %String
```

各要素の内容は以下のとおりです。

- ciphertext ー 解読対象となる暗号化テキスト。
- メソッドは、解読された平文を返します。

メソッドが正常に実行できなかった場合、このメソッドは <FUNCTION> エラーまたは <ILLEGAL VALUE> エラーをスローします。このメソッドの呼び出しを Try-Catch ループに記述します。Try-Catch の詳細は、"TRY-CATCH メカニズム" を参照してください。

キー ID は解読対象となる暗号化テキストに関連付けられるため、キー ID をこの呼び出しで含める必要はありません。

詳細は、"$SYSTEM.Encryption.AESCBCManagedKeyDecrypt" のクラス・リファレンス・コンテンツを参照してください。

4.2.3 $SYSTEM.Encryption.AESCBCManagedKeyEncryptStream

このメソッドのシグニチャは、通常の呼び出しと同様に以下のようになります。

```
$SYSTEM.Encryption.AESCBCManagedKeyEncryptStream
        (
        plaintext As %Stream.Object,
        ciphertext As %Stream.Object,
        keyID As %String,
        )
    As %Status
```

各要素の内容は以下のとおりです。

- plaintext ー 暗号化対象となる暗号化されていないストリーム。
- ciphertext ー 暗号化ストリームを受け取る変数。
- keyID ー plaintext の暗号化に使用されるデータ暗号化キーの GUID。
- メソッドは %Status コードを返します。

詳細は、"$SYSTEM.Encryption.AESCBCManagedKeyEncryptStream" のクラス・リファレンス・コンテンツを参照してください。

4.2.4 $SYSTEM.Encryption.AESCBCManagedKeyDecryptStream

このメソッドのシグニチャは、通常の呼び出しと同様に以下のようになります。

```
$SYSTEM.Encryption.AESCBCManagedKeyDecryptStream
        (
        ciphertext As %Stream.Object,
        plaintext As %Stream.Object
        )
    As %Status
```

各要素の内容は以下のとおりです。

- ciphertext ー 解読対象となる暗号化ストリーム。
- plaintext ー 解読ストリームを受け取る変数。
- メソッドは %Status コードを返します。

キー ID は解読対象となる暗号化テキストに関連付けられるため、キー ID をこの呼び出しで含める必要はありません。

詳細は、"$SYSTEM.Encryption.AESCBCManagedKeyDecryptStream" のクラス・リファレンス・コンテンツを参照してください。

4.3 リアルタイムのデータの再暗号化のサポート

データ要素暗号化では、InterSystems IRIS アプリケーションで、暗号化されたデータ要素を新しいキーで再暗号化する処理をサポートできます。

暗号化されたデータ要素には暗号化キーの識別子が格納されているので、これによって、データの再暗号化の処理が単純になります。暗号化テキストのハンドルと有効なキーを与えられるだけで、アプリケーションは再暗号化を実行できます。例えば、データ要素暗号化では、機密データをダウンタイムなしで再暗号化できる機能がサポートされています。これは特に、PCI DSS (Payment Card Industry Data Security Standard) 要件を満たすことが必要な場合など、法的な理由でこの処理が必要な場合に便利です。

データの再暗号化が必要な場合、新しいキーを作成し、アプリケーションに対して、これが新しい暗号化キーであることを指定します。その後、要素を解読してから新しいキーで暗号化するバックグラウンド・アプリケーションを実行するなどの処理を実行できます。この処理では暗号化に指定されたキーを使用し、解読にも必ずその適切なキーを使用します。これはキーが暗号化されたデータと共に格納されるためです。

5
データ損失に対する保護

暗号化データをいつでも利用できるようにするために、インターシステムズでは、以下の予防措置を取ることを強くお勧めします。

- キー・ファイルを使用している場合、使用している各ファイルに対して、以下の手順に従います。
  1. キー・ファイルの追加の管理者を作成します。
  2. その管理者のユーザ名とパスワードを紙に記録します。
  3. 記録したユーザ名とパスワードを、キーの使用場所から十分に離れたところにある耐火金庫などの物理的に安全な場所に配置します。
  4. キー・ファイルのバックアップ・コピーを作成し、記録したユーザ名とパスワードと同じ安全な場所に配置します。
- KMIP サーバを使用している場合は、サーバ・ベンダの指示に従って、そのサーバの内容をバックアップします。

注意　これらの予防措置を怠ると、暗号化データが永久にアクセス不能となり、そのデータをまったく読み取れなくなる場合があります。

6

緊急事態への対処

暗号化データが関係する緊急事態が生じた場合、その暗号化データへのアクセスが永久に失われることになる可能性があります。緊急事態が生じた場合は、データが永久に失われるリスクを最小限に抑えるために即座に対処する必要があります。

ここでは、暗号化データが関係する緊急事態が発生した場合に取るべき手順について説明します。緊急事態に対して予防措置を取るには、"データ損失に対する保護" を参照してください。

6.1 キー・ファイル使用時における緊急事態への対処

ここでは、データを損失する恐れがある事態において、どのように対処するべきかについて説明します。これらの状況には以下が含まれます。

- 有効なキーが保存されているファイルが損傷したり紛失した場合
  - 既知の管理者のユーザ名とパスワードのあるキー・ファイルのバックアップ・コピーがある場合
  - キー・ファイルのバックアップ・コピーがない場合、またはキーに既知の管理者のユーザ名とパスワードがない場合

    注意　　これは緊急事態です。即座に対処してください。

- 起動時に必要なデータベース暗号化キー・ファイルが存在しない場合
  - キー・ファイルを使用可能にできる場合
  - バックアップ・キー・ファイルが使用可能な場合
  - キー・ファイルが使用できない場合

6.1.1 有効なキーが保存されているファイルが損傷したり紛失した場合

この場合、以下の状況が発生します。

- データベース暗号化キーが InterSystems IRIS® データ・プラットフォーム・インスタンスに対して有効化されています。
- InterSystems IRIS が暗号化データを使用します。
- データベース暗号化キーが保存されているキー・ファイルが破損します。

6.1.1.1 既知の管理者のユーザ名とパスワードのあるキー・ファイルのバックアップ・コピーがある場合

注意　この手順は、InterSystems IRIS データベースの暗号化データが失われる恐れがある緊急事態に実行します。

有効なキーが保存されているファイルがアクセス不能になった場合や損傷した場合は、直ちに以下の手順を実行します。

1. キー・ファイルのバックアップ・コピーを取得します。これは、"暗号化データのアクセスにおける偶発的な損失からの保護" で説明されている手順に従って保存したコピーです。
2. キー・ファイルの新しいバックアップ・コピーを作成して、安全な場所に保存します。
3. キーの新しいコピーが使用されるように InterSystems IRIS を設定します。
   - インタラクティブな起動を使用している場合、スタートアップ・プロシージャにキーの新しいコピーを組み込みます。
   - 無人起動を使用している場合、以前と同じ起動オプションに設定している場合でも、キー・ファイルの新しいコピーで起動オプションを再構成します。

6.1.1.2 キー・ファイルのバックアップ・コピーがない場合、またはキーに既知の管理者のユーザ名とパスワードがない場合

警告　この手順は、InterSystems IRIS データベースの暗号化データが失われる恐れがある緊急事態に実行します。

有効なキーが保存されているファイルが InterSystems IRIS の実行中にアクセス不能になった場合や損傷した場合は、そのキーで暗号化されている各データベースに対し、直ちに以下の手順を実行します。

1. 警告　InterSystems IRIS をシャットダウンしたり有効になっているキーを無効にしたりすると、データが永久に失われます。

   InterSystems IRIS をシャットダウンしないでください。

   現在有効になっているキーは無効にしないでください。
2. インターシステムズのサポート窓口までお問い合わせください。サポート窓口のエンジニアが以下の手順をご案内して、あらゆるご質問にお答えします。
3. データベースをディスマウントします。これにより、暗号化されていないデータベースにデータをコピーしている最中に、暗号化されたコンテンツがあるデータベースではどのユーザも変更ができないようにします。
   a. 管理ポータルのホーム・ページで、[**データベース**] ページ ([**システム処理**] > [**データベース**]) に移動します。
   b. 暗号化データベースがマウントされている場合、[**データベース**] ページで、データベースの行にある最後から 2 番目の列で [**ディスマウント**] オプションを選択します。確認ダイアログで [OK] をクリックします。
   c. [**データベース**] ページが再び表示されたら、データベースの行にある最後の列で [**マウント**] オプションを選択します。
   d. [**データベースマウント**] 確認画面で、[**読み取り専用**] チェック・ボックスにチェックを付け、[OK] を選択します。

   この手順の間、誰もデータベースに対して変更を行わないことが重要です。データベースを読み取り専用でマウントすると、ユーザはデータを変更できなくなります。
4. 暗号化されていない状態ですべてのデータを別のデータベースにコピーします。データをコピーする手順は以下のとおりです。

a. ターミナルで、%SYS ネームスペースに移動します。

```
REGULARNAMESPACE>set $namespace="%SYS"
```

b. そのネームスペースで ^GBLOCKCOPY コマンドを実行します。

```
%SYS>d ^GBLOCKCOPY

This routine will do a fast global copy from a database to another database or
to a namespace. If a namespace is the destination, the global will follow any
mappings set up for the namespace.

1) Interactive copy
2) Batch copy
3) Exit

Option?1
```

c. ^GBLOCKCOPY プロンプトで、インタラクティブ・コピーとして 1 を指定します。

```
Option? 1

1) Copy from Database to Database
2) Copy from Database to Namespace
3) Exit

Option?
```

d. ^GBLOCKCOPY プロンプトで、コピー・タイプの入力が要求されたら、別のデータベースへのコピーを指定する 1 を選択します。

```
Option? 1
Source Directory for Copy (? for List)?
```

ここで、暗号化データベースの名前を指定するか、? と入力して番号付けされたデータベースのリストを表示します。リストには暗号化データベースが含まれます。? と入力すると、^GBLOCKCOPY は以下のようなリストを表示します。

```
Source Directory for Copy (? for List)? ?

1) C:\InterSystems\MyIRIS\mgr\
2) C:\InterSystems\MyIRIS\mgr\irislocaldata\
3) C:\InterSystems\MyIRIS\mgr\irisaudit\
4) C:\InterSystems\MyIRIS\mgr\irislib\
5) C:\InterSystems\MyIRIS\mgr\iristemp\
6) C:\InterSystems\MyIRIS\mgr\encrypted1\
7) C:\InterSystems\MyIRIS\mgr\encrypted2\
8) C:\InterSystems\MyIRIS\mgr\unencrypted\

Source Directory for Copy (? for List)?
```

暗号化データベースの数 (7 など) を入力します。

e. ^GBLOCKCOPY でデータのコピー先ディレクトリの入力を求められたら、暗号化されていないデータベースの名前を入力するか、? と入力してソース・ディレクトリのリストに類似したリストを表示します。

f. ^GBLOCKCOPY ですべてのグローバルをコピーするかどうかを尋ねられたら、Yes (Yes、Y、y などとすることができます) と入力します。

```
All Globals? No => y
```

g. 空のグローバルがデータベースにある場合、^GBLOCKCOPY で、これをコピーするかどうかを尋ねられます。これは、以下のように表示されます。

```
All Globals? No => y

^oddBIND     contains no data
Include it anyway? No =>
```

既定値の No (No、N、n などとすることができます) を入力します。

h. ^GBLOCKCOPY で、他の空のグローバルをすべてスキップするかどうかを尋ねられます。既定値の Yes (Yes、Y、y などとすることができます) を入力します。

```
Exclude any other similar globals without asking again? Yes =>
```

コピーされていないすべての空のグローバルのリストが表示されます。

```
Exclude any other similar globals without asking again? Yes => Yes
^oddCOM      contains no data --  not included
^oddDEP      contains no data --  not included
^oddEXT      contains no data --  not included
^oddEXTR     contains no data --  not included
^oddMAP      contains no data --  not included
^oddPKG      contains no data --  not included
^oddPROC     contains no data --  not included
^oddPROJECT  contains no data --  not included
^oddSQL      contains no data --  not included
^oddStudioDocument contains no data --  not included
^oddStudioMenu contains no data --  not included
^oddTSQL     contains no data --  not included
^oddXML      contains no data --  not included
^rBACKUP     contains no data --  not included
^rINC        contains no data --  not included
^rINCSAVE    contains no data --  not included
^rINDEXEXT   contains no data --  not included
^rINDEXSQL   contains no data --  not included
^rMACSAVE    contains no data --  not included
9 items selected from
29 available globals
```

i. ^GBLOCKCOPY で、この処理でジャーナリングを無効にするかどうかを尋ねられます。

```
Turn journaling off for this copy? Yes =>
```

既定値の Yes (Yes、Y、y などとすることができます) を入力します。

j. ^GBLOCKCOPY で、データをコピーすることの確認を求められます。

```
Confirm copy? Yes =>
```

既定値の Yes (Yes、Y、y などとすることができます) を入力します。データベースのサイズとプロセッサの処理速度によっては、コピーのステータスが進捗状況に応じて表示される場合があります。完了すると、^GBLOCKCOPY で以下のようなメッセージが表示されます。

```
Copy of data has completed
```

k. ^GBLOCKCOPY で、コピーに関連付けられた統計を保存するかどうかを尋ねられます。既定値の No (No、N、n などとすることができます) を入力します。

```
Do you want to save statistics for later review? No =>
```

コントロールはメイン・プロンプトに戻ります。

5. コピーされたデータが有効かどうかをテストします。このためには、管理ポータルのシステム・エクスプローラで、^GBLOCKCOPY におけるデータのコピー先のデータベースについて、クラス、テーブル、またはグローバルを調査します。
6. データが有効な場合、アクセス不能なキーまたは損傷したキーで暗号化されたデータベースごとに、この手順の 3 と 4 を実行します。
7. 暗号化されていないデータベースにすべての暗号化データベースをコピーしたら、それぞれのデータベースの 2 つ目のコピーを、できればそれぞれの最初のコピーがあるマシンとは別のマシンに作成します。

8. これで、すべての暗号化データベースをディスマウントし、有効なキー (紛失または損傷したキー・ファイルのキー) を無効にできます。この操作は、この時点でのみ可能です。InterSystems IRIS では、すべての暗号化データベースのキーを無効にするには、先にそれらのデータベースをディスマウントする必要があります。

以上で、暗号化されていない 1 つ以上のデータベースにデータがあり、有効なキーが存在しない状態になります。

以前に暗号化されたデータベースを再暗号化するには、以下の手順に従います。

1. ″キーの作成″ で説明されている手順に従い、新しいデータベース暗号化キーを作成します。
2. ″暗号化データのアクセスにおける偶発的な損失からの保護″ で説明されているように、キー・ファイルの新しいバックアップ・コピーを作成します。

   注意　″暗号化データのアクセスにおける偶発的な損失からの保護″ の説明にある注意事項が守られていることを確認します。この手順に従わないと、データが永久に失われる場合があります。

3. 新しいキーを使用して、新しい暗号化データベースを 1 つ以上作成します。
4. 前述の手順でエクスポートしたデータを新しい暗号化データベースにインポートします。

これで、正常なキーとそのキーがあるキー・ファイルのバップアップが存在する暗号化データベースにデータが格納されました。

6.1.2 起動時に必要なデータベース暗号化キー・ファイルが存在しない場合

起動時にデータベース暗号化キー・ファイルを使用する必要がある状況では、システムはシングル・ユーザ・モードで起動します。該当する状況は以下のとおりです。

- InterSystems IRIS がインタラクティブに起動または無人起動するように構成されている場合
- 起動時にジャーナル・ファイルまたは IRISTEMP データベースおよび IRISLOCALDATA データベース (あるいはこれらすべて) を暗号化するように指定されている場合、または起動時に暗号化データベースが必要であると指定されている場合
- データベース暗号化キー・ファイルが存在しない場合

6.1.2.1 キー・ファイルを使用可能にできる場合

InterSystems IRIS の起動時に適切なキー・ファイルが存在しないことだけが理由で (例えば、キー・ファイルを保持するメディアが現在使用できない場合)、この状況が発生する可能性があります。

この状況を改善するには、InterSystems IRIS の実行をシングル・ユーザ・モードで開始した後、以下の手順を実行します。

1. InterSystems IRIS をシャットダウンします。例えば、InterSystems IRIS インスタンスを “MyIRIS” とすると、シャットダウンを実行するコマンドは以下のようになります。

   ```
   iris force MyIRIS
   ```

2. InterSystems IRIS がデータベース暗号化キー・ファイルを検索する場所がわかっている場合は、その場所にキー・ファイルを配置します (わからない場合は、次のセクションに示すように ^STURECOV を実行する必要があります)。
3. InterSystems IRIS を再起動します。

InterSystems IRIS は通常モード (マルチ・ユーザ・モード) で起動し、適切に動作します。

6.1.2.2 バックアップ・キー・ファイルが使用可能な場合

InterSystems IRIS の起動時に適切なキー・ファイルが存在しないために使用できない場合、バックアップ・キー・ファイルを使用できます。この場合、状況を改善するには、InterSystems IRIS の実行をシングル・ユーザ・モードで開始した後、以下の手順を実行します。

1. インターシステムズのサポート窓口までお問い合わせください。サポート窓口のエンジニアが以下の手順をご案内して、あらゆるご質問にお答えします。
2. messages.log ファイルの最新エントリにある手順に従い、管理者ターミナル・セッションを開始します。通常、-B フラグでターミナル・セッションを開始するように指定されています。

   例えば、“MyIRIS” という InterSystems IRIS インスタンスが既定の場所にインストールされている場合、Windows のコマンド行で次のコマンドを入力します。

   ```
   c:\InterSystems\MyIRIS\bin\irisdb -sc:\InterSystems\MyIRIS\mgr -B
   ```

   オペレーティング・システムのターミナル・ウィンドウで InterSystems IRIS に接続します。このウィンドウのプロンプトは、オペレーティング・システムのプロンプトから InterSystems IRIS の %SYS プロンプトに変更されます。
3. データベース暗号化キー・ファイルのコピー (バックアップなど) があるか、入手できる場合、InterSystems IRIS にアクセス可能な場所にそのキー・ファイルのコピーを置きます。
4. ターミナル・プロンプトで、^STURECOV (スタートアップ・リカバリ) ルーチンを実行します。このルーチンでは、そのファイルの管理者のユーザ名とパスワードを使用して暗号化キーを有効にします (このプロセスが完了したときに、^STURECOV を終了する必要はありません)。
5. InterSystems IRIS を使用する準備ができたら、^STURECOV を使用してスタートアップ・プロシージャを完了します。マルチ・ユーザ・モードで InterSystems IRIS を起動します。

以上で、InterSystems IRIS が適切に動作します。

6.1.2.3 キー・ファイルが使用できない場合

データベース暗号化キー・ファイルのコピーがない場合、以下の手順を実行します。

1. インターシステムズのサポート窓口までお問い合わせください。サポート窓口のエンジニアが以下の手順をご案内して、あらゆるご質問にお答えします。
2. messages.log ファイルの最新エントリにある手順に従い、管理者ターミナル・セッションを開始します。通常、-B フラグでターミナル・セッションを開始するように指定されています。

   例えば、“MyIRIS” という InterSystems IRIS インスタンスが既定の場所にインストールされている場合、Windows のコマンド行で次のコマンドを入力します。

   ```
   c:\InterSystems\MyIRIS\bin\irisdb -sc:\InterSystems\MyIRIS\mgr -B
   ```

   オペレーティング・システムのターミナル・ウィンドウで InterSystems IRIS に接続します。このウィンドウのプロンプトは、オペレーティング・システムのプロンプトから InterSystems IRIS の %SYS プロンプトに変更されます。
3. 起動時にマウントする必要がある暗号化データベースがある場合、それらに対してこの機能を無効にします。
   a. 管理ポータルのホーム・ページで、[**ローカルデータベース**] ページ ([**システム管理**] > [**構成**] > [**システム構成**] > [**ローカルデータベース**]) に移動します。
   b. データベースのテーブルでデータベース名をクリックします。そのデータベースの [**編集**] ページが表示されます。
   c. [**編集**] ページで、[**起動時にマウントが必要**] チェック・ボックスのチェックを外します。
   d. [**保存**] をクリックします。

4. ターミナル・プロンプトで、^STURECOV ルーチンを実行します。そのルーチンで、データベース暗号化キーを必要としないように InterSystems IRIS データベースの起動オプションを構成します。これは、IRISTEMP データベースおよび IRISLOCALDATA データベースとジャーナル・ファイルが適切に動作して、暗号化データベースをマウントできないことを表します。
5. InterSystems IRIS を使用する準備ができたら、^STURECOV を使用してスタートアップ・プロシージャを完了します。マルチ・ユーザ・モードで InterSystems IRIS を起動します。

この手順を実行する際、サポート窓口の担当者の指示に従い、その他の操作を実行する必要がある場合があります。担当者の指示に従ってください。

注意　"暗号化データのアクセスにおける偶発的な損失からの保護" で説明されている操作を実行しないと、いずれの形式でもデータを使用できなくなる可能性があります。これは非常に深刻な問題ですが、キーがないと、失われたデータを取得する方法がありません。

6.2 KMIP サーバ使用時における緊急事態への対処

ここでは、KMIP サーバの使用時にデータを損失する恐れがある事態において、どのように対処するべきかについて説明します。これらの状況には以下が含まれます。

- 有効なキーが格納されている KMIP サーバが損傷または紛失した場合
  - KMIP サーバ上のキーのバックアップ・コピーがある場合
  - KMIP サーバ上のキーのバックアップ・コピーがない場合

    警告　これは緊急事態です。即座に対処してください。

- 起動時に KMIP サーバが必要で、KMIP サーバにアクセスできない場合
  - KMIP サーバへの接続が一時的に利用不可能である場合
  - KMIP サーバで長期的な障害が発生している場合

6.2.1 有効なキーが格納されている KMIP サーバが損傷または紛失した場合

この場合、以下の状況が発生します。

- データベース暗号化キーが InterSystems IRIS インスタンスに対して有効化されています。
- InterSystems IRIS が暗号化データを使用します。
- データベース暗号化キーが格納されている KMIP サーバが破損します。

6.2.1.1 KMIP サーバ上のキーのバックアップ・コピーがある場合

有効なキーが格納されている KMIP サーバがアクセス不能になったり損傷したりした場合、直ちにベンダの指示に従って KMIP サーバのリストア手順を実行します。

6.2.1.2 KMIP サーバ上のキーのバックアップ・コピーがない場合

警告　この手順は、InterSystems IRIS データベースの暗号化データが失われる恐れがある緊急事態に実行します。

有効なキーが格納されているKMIPサーバをバックアップからリストアする方法がない場合、そのキーで暗号化されている各データベースに対し、直ちに以下の手順を実行します。

1. 警告　InterSystems IRISをシャットダウンしたり有効になっているキーを無効にしたりすると、データが永久に失われます。

   InterSystems IRISをシャットダウンしないでください。

   現在有効になっているキーは無効にしないでください。

2. インターシステムズのサポート窓口までお問い合わせください。サポート窓口のエンジニアが以下の手順をご案内して、あらゆるご質問にお答えします。

3. データベースをディスマウントします。これにより、暗号化されていないデータベースにデータをコピーしている最中に、暗号化されたコンテンツがあるデータベースではどのユーザも変更ができないようにします。

   a. 管理ポータルのホーム・ページで、**[データベース]** ページ (**[システム処理]** > **[データベース]**) に移動します。

   b. 暗号化データベースがマウントされている場合、**[データベース]** ページで、データベースの行にある最後から2番目の列で **[ディスマウント]** オプションを選択します。確認ダイアログで [OK] をクリックします。

   c. **[データベース]** ページが再び表示されたら、データベースの行にある最後の列で **[マウント]** オプションを選択します。

   d. **[データベースマウント]** 確認画面で、**[読み取り専用]** チェック・ボックスにチェックを付け、[OK] を選択します。

   この手順の間、誰もデータベースに対して変更を行わないことが重要です。データベースを読み取り専用でマウントすると、ユーザはデータを変更できなくなります。

4. 暗号化されていない状態ですべてのデータを別のデータベースにコピーします。データをコピーする手順は以下のとおりです。

   a. ターミナルで、**%SYS** ネームスペースに移動します。

   ```
   REGULARNAMESPACE>set $namespace="%SYS"
   ```

   b. そのネームスペースで ^GBLOCKCOPY コマンドを実行します。

   ```
   %SYS>do ^GBLOCKCOPY

   This routine will do a fast global copy from a database to another database or
   to a namespace. If a namespace is the destination, the global will follow any
   mappings set up for the namespace.

   1) Interactive copy
   2) Batch copy
   3) Exit

   Option?1
   ```

   c. ^GBLOCKCOPY プロンプトで、インタラクティブ・コピーとして1を指定します。

   ```
   Option? 1

   1) Copy from Database to Database
   2) Copy from Database to Namespace
   3) Exit

   Option?
   ```

   d. ^GBLOCKCOPY プロンプトで、コピー・タイプの入力が要求されたら、別のデータベースへのコピーを指定する1を選択します。

   ```
   Option? 1
   Source Directory for Copy (? for List)?
   ```

ここで、暗号化データベースの名前を指定するか、? と入力して番号付けされたデータベースのリストを表示します。リストには暗号化データベースが含まれます。? と入力すると、^GBLOCKCOPY は以下のようなリストを表示します。

```
Source Directory for Copy (? for List)? ?

1) C:\InterSystems\MyIRIS\mgr\
2) C:\InterSystems\MyIRIS\mgr\irislocaldata\
3) C:\InterSystems\MyIRIS\mgr\irisaudit\
4) C:\InterSystems\MyIRIS\mgr\irislib\
5) C:\InterSystems\MyIRIS\mgr\iristemp\
6) C:\InterSystems\MyIRIS\mgr\encrypted1\
7) C:\InterSystems\MyIRIS\mgr\encrypted2\
8) C:\InterSystems\MyIRIS\mgr\unencrypted\

Source Directory for Copy (? for List)?
```

暗号化データベースの数 (7 など) を入力します。

e. ^GBLOCKCOPY でデータのコピー先ディレクトリの入力を求められたら、暗号化されていないデータベースの名前を入力するか、? と入力してソース・ディレクトリのリストに類似したリストを表示します。

f. ^GBLOCKCOPY ですべてのグローバルをコピーするかどうかを尋ねられたら、Yes (Yes、Y、y などとすることができます) と入力します。

```
All Globals? No => y
```

g. 空のグローバルがデータベースにある場合、^GBLOCKCOPY で、これをコピーするかどうかを尋ねられます。これは、以下のように表示されます。

```
All Globals? No => y

^oddBIND     contains no data
Include it anyway? No =>
```

既定値の No (No、N、n などとすることができます) を入力します。

h. ^GBLOCKCOPY で、他の空のグローバルをすべてスキップするかどうかを尋ねられます。既定値の Yes (Yes、Y、y などとすることができます) を入力します。

```
Exclude any other similar globals without asking again? Yes =>
```

コピーされていないすべての空のグローバルのリストが表示されます。

```
Exclude any other similar globals without asking again? Yes => Yes
^oddCOM      contains no data --  not included
^oddDEP      contains no data --  not included
^oddEXT      contains no data --  not included
^oddEXTR     contains no data --  not included
^oddMAP      contains no data --  not included
^oddPKG      contains no data --  not included
^oddPROC     contains no data --  not included
^oddPROJECT  contains no data --  not included
^oddSQL      contains no data --  not included
^oddStudioDocument contains no data --  not included
^oddStudioMenu contains no data --  not included
^oddTSQL     contains no data --  not included
^oddXML      contains no data --  not included
^rBACKUP     contains no data --  not included
^rINC        contains no data --  not included
^rINCSAVE    contains no data --  not included
^rINDEXEXT   contains no data --  not included
^rINDEXSQL   contains no data --  not included
^rMACSAVE    contains no data --  not included
9 items selected from
29 available globals
```

i. ^GBLOCKCOPY で、この処理でジャーナリングを無効にするかどうかを尋ねられます。

```
Turn journaling off for this copy? Yes =>
```

既定値の Yes (Yes、Y、y などとすることができます) を入力します。

j. ^GBLOCKCOPY で、データをコピーすることの確認を求められます。

```
Confirm copy? Yes =>
```

既定値の Yes (Yes、Y、y などとすることができます) を入力します。データベースのサイズとプロセッサの処理速度によっては、コピーのステータスが進捗状況に応じて表示される場合があります。完了すると、^GBLOCKCOPY で以下のようなメッセージが表示されます。

```
Copy of data has completed
```

k. ^GBLOCKCOPY で、コピーに関連付けられた統計を保存するかどうかを尋ねられます。既定値の No (No、N、n などとすることができます) を入力します。

```
Do you want to save statistics for later review? No =>
```

コントロールはメイン・プロンプトに戻ります。

5. コピーされたデータが有効かどうかをテストします。このためには、管理ポータルのシステム・エクスプローラで、^GBLOCKCOPY におけるデータのコピー先のデータベースについて、クラス、テーブル、またはグローバルを調査します。
6. データが有効な場合、アクセス不能なキーまたは損傷したキーで暗号化されたデータベースごとに、この手順の 3 と 4 を実行します。
7. 暗号化されていないデータベースにすべての暗号化データベースをコピーしたら、それぞれのデータベースの 2 つ目のコピーを、できればそれぞれの最初のコピーがあるマシンとは別のマシンに作成します。
8. これで、すべての暗号化データベースをディスマウントし、有効なキー (紛失または損傷したキー・ファイルのキー) を無効にできます。この操作は、この時点でのみ可能です。InterSystems IRIS では、すべての暗号化データベースのキーを無効にするには、先にそれらのデータベースをディスマウントする必要があります。

以上で、暗号化されていない 1 つ以上のデータベースにデータがあり、有効なキーが存在しない状態になります。

以前に暗号化されたデータベースを再暗号化するには、以下の手順に従います。

1. "KMIP サーバ上のキーの作成" で説明されている手順に従い、新しいデータベース暗号化キーを作成します。
2. "暗号化データのアクセスにおける偶発的な損失からの保護" で説明されているように、キー・ファイルの新しいバックアップ・コピーを作成します。

   注意　"暗号化データのアクセスにおける偶発的な損失からの保護" の説明にある注意事項が守られていることを確認します。この手順に従わないと、データが永久に失われる場合があります。

3. 新しいキーを使用して、新しい暗号化データベースを 1 つ以上作成します。
4. 前述の手順でエクスポートしたデータを新しい暗号化データベースにインポートします。

これで、正常なキーとそのキーがあるキー・ファイルのバップアップが存在する暗号化データベースにデータが格納されました。

6.2.2 起動時に KMIP サーバが必要で、KMIP サーバにアクセスできない場合

起動時に 1 つ以上のデータベース暗号化キーを使用する必要がある状況では、システムはシングル・ユーザ・モードで起動します。該当する状況は以下のとおりです。

- InterSystems IRIS がインタラクティブに起動または無人起動するように構成されている場合

- 起動時にジャーナル・ファイルまたは IRISTEMP データベースおよび IRISLOCALDATA データベース (あるいはこれらすべて) を暗号化するように指定されている場合、または起動時に暗号化データベースが必要であると指定されている場合
- 必要なデータベース暗号化キーが格納されている KMIP サーバがアクセス不能である場合

6.2.2.1 KMIP サーバへの接続が一時的に利用不可能である場合

ネットワーク障害などの問題が発生している場合や、他の理由で KMIP サーバが一時的に動作していない場合、最も簡単な解決策は、ネットワークやサーバの問題を解決し、必要に応じて InterSystems IRIS を再起動することです。

6.2.2.2 KMIP サーバで長期的な障害が発生している場合

KMIP サーバに長時間接続できない場合は、以下の手順に従います。

1. **messages.log** ファイルの最新エントリにある手順に従い、管理者ターミナル・セッションを開始します。通常、**-B** フラグでターミナル・セッションを開始するように指定されています。

   例えば、“MyIRIS” という InterSystems IRIS インスタンスが既定の場所にインストールされている場合、Windows のコマンド行で次のコマンドを入力します。

   ```
   c:\InterSystems\MyIRIS\bin\irisdb -sc:\InterSystems\MyIRIS\mgr -B
   ```

   オペレーティング・システムのターミナル・ウィンドウで InterSystems IRIS に接続します。このウィンドウのプロンプトは、オペレーティング・システムのプロンプトから InterSystems IRIS の **%SYS** プロンプトに変更されます。

2. 起動時にマウントする必要がある暗号化データベースがある場合、それらに対してこの機能を無効にします。
   a. 管理ポータルのホーム・ページで、**[ローカルデータベース]** ページ (**[システム管理]** > **[構成]** > **[システム構成]** > **[ローカルデータベース]**) に移動します。
   b. データベースのテーブルでデータベース名をクリックします。そのデータベースの **[編集]** ページが表示されます。
   c. **[編集]** ページで、**[起動時にマウントが必要]** チェック・ボックスのチェックを外します。
   d. **[保存]** をクリックします。
3. ターミナル・プロンプトで、^STURECOV ルーチンを実行します。そのルーチンで、データベース暗号化キーを必要としないように InterSystems IRIS データベースの起動オプションを構成します。これは、**IRISTEMP** データベースおよび **IRISLOCALDATA** データベースとジャーナル・ファイルが適切に動作して、暗号化データベースをマウントできないことを表します。
4. InterSystems IRIS を使用する準備ができたら、^STURECOV を使用してスタートアップ・プロシージャを完了します。マルチ・ユーザ・モードで InterSystems IRIS を起動します。

注意　　″暗号化データのアクセスにおける偶発的な損失からの保護″ で説明されている操作を実行しないと、いずれの形式でもデータを使用できなくなる可能性があります。これは非常に深刻な問題ですが、キーがないと、失われたデータを取得する方法がありません。

7

暗号化に関するその他の情報

ここでは、InterSystems IRIS® データ・プラットフォームでの暗号化に関するその他の情報を紹介します。

7.1 キー・ファイル暗号化情報

データベース暗号化の管理者名は、キー・ファイルに平文で保存されています。データベース暗号化の管理者パスワードは保存されていません。パスワードを入力すると、他のデータと共にそれを使用してキー暗号化キーが生成されます。有効なパスワードを第三者が推測できる場合、そのパスワードのポリシーは脆弱すぎます。キー暗号化キーは、512 ビットの salt と 65,536 回の反復処理を使用する PBKDF2 アルゴリズムを使用して生成され、ディクショナリおよび総当り攻撃を実行不可能にします。

7.2 暗号化とデータベース関連機能

InterSystems IRIS のデータベース暗号化では、データベースのファイルそのものが保護されます。InterSystems IRIS の関連機能は以下のとおりです。

- InterSystems IRIS のオンライン・バックアップは暗号化されません。InterSystems IRIS データベースのバックアップを暗号化するには、InterSystems IRIS を停止し、ファイル・システムのバックアップを実行することをお勧めします ("外部バックアップ" を参照)。
- 暗号化データベースのブロックは、ライト・イメージ・ジャーナル (WIJ) ファイルに暗号化されます。
- **IRISTEMP** データベースおよび **IRISLOCALDATA** データベースは、オプションで暗号化できます。**IRISTEMP** および **IRISLOCALDATA** を暗号化する方法は、"暗号化の起動設定の構成" を参照してください。
- オプションでジャーナル・ファイルを暗号化できます。"暗号化の起動設定の構成" を参照してください。

7.3 暗号化、ハッシュ、およびその他のキー関連操作を実行するための呼び出しについて

InterSystems IRIS では、**%SYSTEM.Encryption** クラスのさまざまなメソッドを使用して、データ暗号化、Base64 エンコーディング、ハッシュ、およびメッセージ認証コードの生成に関連するアクションを実行できます。これには、AES 暗号化、

各種の RSA アルゴリズム、SHA-256 ハッシュ関数などを呼び出すメソッドが含まれます。いくつかの呼び出しを以下に示します。

- $System.Encryption.AESCBCManagedKeyEncrypt および $System.Encryption.AESCBCManagedKeyDecrypt
- $System.Encryption.AESKeyWrap および $System.Encryption.AESKeyUnwrap
- $System.Encryption.Base64Encode および $System.Encryption.Base64Decode
- $System.Encryption.RSASHASign および $System.Encryption.RSASHAVerify
- $System.Encryption.RSAEncrypt および $System.Encryption.RSADecrypt
- $System.Encryption.SHAHash

7.3.1 RSAEncrypt および RSADecrypt の使用例

以下に、RSAEncrypt および RSADecrypt の呼び出しの使用例を示します。これは以下を前提としています。

- コードは Windows で実行されます。
- 使用可能な証明書、秘密鍵、および認証機関 (CA) 証明書があります(この例を試すには、これらを入手する必要があります)。
- これら 3 つのアイテムはすべて C:¥Keys¥ ディレクトリにあります。

処理の詳細は、例の中のコメントを参照してください。

ObjectScript

```
set dir = "C:\Keys\"

// certificate for the instance performing encryption and decryption
// and private key associated with that above certificate
set cert = dir_"test.crt"
set key = dir_"test.key"

// certificate for the CA of the instance
set cacert=dir_"ca.crt"

set data = "data to be encrypted"

// create a local set of X.509 credentials with the
// certificate and private key
set credentials = ##class(%SYS.X509Credentials).%New()
set credentials.Alias="TestCreds"
write credentials.LoadCertificate(cert)
write credentials.LoadPrivateKey(key)
write credentials.Save(),!

// encrypt the data using the public key in the certificate, write it
// to the display, and display error information, if there is any
set ciphertext=$System.Encryption.RSAEncrypt(data,credentials.Certificate,cacert)
write ciphertext,!
write $System.Encryption.RSASHA1GetLastError()

// decrypt the data using the private key, write it to the display,
// and display error information, if there is any
write "now decrypting -=-=-=-=-=-=-=-=-=-=-=-",!
set cleartext=$System.Encryption.RSADecrypt(ciphertext,credentials.PrivateKey)
write cleartext,!
write $System.Encryption.RSASHA1GetLastError()
```

A
データベース暗号化の FIPS 140-2 準拠

特定のプラットフォームでは、InterSystems IRIS® データ・プラットフォームは FIPS 140-2 に準拠したデータベース暗号化をサポートします (FIPS 140-2 は Federal Information Processing Standard Publication 140-2 を指します。詳細は、http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf で確認できます)。

このバージョンの InterSystems IRIS は、x86-64 対応の Red Hat Enterprise Linux で、FIPS 140-2 に準拠したデータベース暗号化をサポートしています。Red Hat は、OpenSSL **libcrypto.so** ライブラリおよび **libssl.so** ライブラリの検証証明書を保有しています。FIPS モードでの実行時には、InterSystems IRIS はこれらの証明書ライブラリを使用します。Red Hat Linux のマイナー・バージョンに最新の証明書があるかどうかを確認するには、Red Hat のドキュメントを参照してください。

注釈　FIPS モードが有効な場合の動作:

- Red Hat 7 では TLSv1.0 ～ TLSv1.2 のみがサポートされます。
- Red Hat 8 では TLSv1.2 と TLSv1.3 のみがサポートされます。

政府規格に対する Red Hat のサポートについては、https://access.redhat.com/articles/2918071 を参照してください。

A.1 FIPS サポートの有効化

InterSystems IRIS で、FIPS 140-2 に準拠したデータベース暗号化のサポートを有効にするには、以下を実行します。

1. Red Hat リポジトリから **openssl** パッケージ (rhel-8-server-rpms) をダウンロードしてインストールします。
2. オペレーティング・システムの FIPS モードを有効にします。手順については、Red Hat の Web サイトの記事 "RHEL 6/7/8 を FIPS 140-2 準拠に設定するにはどうすればよいですか?" を参照してください (この記事にアクセスするには、Red Hat のログイン資格情報が必要です)。
3. ディレクトリ **/usr/lib64** で、以下のシンボリック・リンクを確認します。シンボリック・リンクが存在しない場合、作成します。
   - シンボリック・リンク **libssl.so.1.1** は、同じディレクトリ内の適切なファイル (**libssl.so.1.1.1g** ファイルなど) を指している必要があります。
   - シンボリック・リンク **libcrypto.so.1.1** は、同じディレクトリ内の適切なファイル (**libcrypto.so.1.1.1g** ファイルなど) を指している必要があります。
4. InterSystems IRIS で、**FIPSMode** CPF パラメータに **True** (1) を指定します。そのためには、以下の操作を実行します。

a. 管理ポータルを開きます。

b. **[システム管理]→[構成]→[追加設定]→[開始]** を選択します。

FIPSMode の行が表示されます。

c. **FIPSMode** の値を **True** に指定して、変更内容を保存します。

5. InterSystems IRIS を再起動します。
6. "暗号化データベースの使用法" で説明されているように、暗号化データベースを有効化して構成します。

A.2 開始動作と messages.log

InterSystems IRIS の開始時：

- **FIPSMode** が 0 の場合、InterSystems IRIS ネイティブの暗号化が使用されます。Intel AES-NI ハードウェア命令を使用する、最適化されたアセンブリー・コードなどです (CPU がサポートする場合)。このモードでは、InterSystems IRIS は開始時、**messages.log** に以下を書き込みます。

```
FIPS 140-2 compliant cryptography for database encryption is not configured in iris.cpf
```

- **FIPSMode** が 1 の場合、InterSystems IRIS は **/usr/lib64/libcrypto.so** FIPS 検証済みライブラリ内の関数への参照を解決しようとします。その後、FIPS モードでライブラリを初期化しようとします。これらの手順が成功すると、InterSystems IRIS は **messages.log** に以下を書き込みます。

```
FIPS 140-2 compliant cryptography for database encryption is enabled for this instance.
```

- **FIPSMode** が 1 で、ライブラリの初期化が失敗した場合、InterSystems IRIS は開始されません。この場合、**messages.log** には以下のメッセージが書き込まれます。

```
FIPS 140-2 compliant cryptography for database encryption initialization failed. Aborting.
```

- lnxrhx64 以外のプラットフォームでは、**FIPSMode** が 1 の場合、InterSystems IRIS ネイティブの暗号化が使用され、InterSystems IRIS は**messages.log** に以下を書き込みます。

```
FIPS 140-2 compliant cryptography for database encryption is not supported on this platform.
```