InterSystems IRIS の基礎：データベース暗号化

Version 2023.1
2024-01-02

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

InterSystems IRIS の基礎 : データベース暗号化
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

InterSystems IRIS の基礎：データベース暗号化

ここでは、InterSystems IRIS® データ・プラットフォームでデータベース暗号化を処理する方法について説明します。これは組織のセキュリティ戦略にとって重要な部分です。

ここでは、データベース暗号化の概要を示し、暗号化されたデータベースの作成に関連するいくつかの初期タスクの手順を説明します。このガイドの完了後には、キー・ファイルを作成し、そのキー・ファイルをアクティブ化し、それを使用してデータベースを暗号化します。これらのアクティビティは、既定の設定と機能のみを使用する設計になっているので、ユーザはトピックの範囲を外れた詳細を扱うことなく、機能の基本部分を十分に理解することができます (ただし実装の実行時には、こうした詳細が重要になる可能性があります)。データベース暗号化の完全なドキュメントは、"暗号化ガイド" を参照してください。

1 データベース暗号化はなぜ重要か

暗号化によって、機密情報や個人情報の不適切または不正な使用や開示を完全に防げるわけではありませんが、保存データの暗号化を確実に行うことで、情報のセキュリティ防御における重要な層が提供されます。データベース・レベルで暗号化を配備すると、情報保護の制御に新たなディメンジョンが追加されます。

さらに、機密情報や個人情報に関する多くの法規制では、データ処理組織に防御の最前線として暗号化の採用を勧告または要求しています。ここには以下のような法規制が含まれます。

- 医療保険の相互運用性と説明責任に関する法律 (米国 HIPAA 法) ― セキュリティ保護された保健情報を読み取り不可、解読不可、復元不可にすることを求めています。
- 米国マサチューセッツ州法 (201 Code of Massachusetts Regulations (CMR) 17.00) ― 送信中と保存済みの個人情報を暗号化することを求めています。
- 米国ニューヨーク州の規制 (New York 23 New York Codes, Rules and Regulations (NYCRR) Part 500) ― 非公開情報を処理する金融機関やその他の関係組織は、データ保護の 1 つの手段として暗号化を利用する必要があります。
- EU 一般データ保護規則 (GDPR) ― 安全保護において暗号化を保護制御として考慮に入れることを求めています。
- イタリアの個人データ保護に関する法律 (PDPC) ― 最低限のデータ・セキュリティ対策に関する技術的な規定のセクション 24 で、健康と性生活を開示するデータの処理を暗号化することを求めています。
- オーストラリアの個人情報保護法 (APP) の Principle 4 ― 強固な暗号化の実装により、個人情報の保護に必要なプライバシー強化テクノロジに取り組みます。
- 日本の経済産業省 (METI) ガイドライン ― 暗号化されていない個人情報または機密情報の侵害が発生した場合、規制調査を実施する必要があります。個人情報の保護に関する法律 (APPI) の第 20 条では、個人情報取扱事業者が情報の漏えい、紛失、またはき損の防止に対する責任を負う規定になっているからです。

こうした規制要件の多くは、急激に一般化している現象であるデータ漏えいに重点を置いていますが、現在のフレームワークは、ロールベースのアクセス、パスワード保護、侵入検出、データ損失防止、ロギング/監査、および暗号化などの適切なセキュリティ制御によってリスクに対処する義務を組織に負わせています。暗号化それだけでは、すべての必須要件が対処されませんが、セキュリティ基盤を提供するものです。データベース・レベルで暗号化を行うと、攻撃者はシ

ステムやファイル領域へのアクセス権だけでなくデータベースへのアクセス権も得る必要が生じるため、保護機能が強化されます。この追加の層によって、組織やその顧客、すべての関係者に保証がもたらされます。

2 InterSystems IRIS によるデータベース暗号化の使用法

データベース操作に関連するアクティビティでは、InterSystems IRIS の暗号化と解読のプロセスはユーザに対して透過的です。エンド・ユーザまたはアプリケーション開発者の視点からは、アプリケーションは単純に通常のアクティビティを実行し、データがディスク上で自動的に暗号化されます。システム管理者の視点からは、データ暗号化が行われたことを確認するいくつかの単純なタスクが存在します。これらのタスクの実行後、再びアクティビティは非表示で実行されます。

さらに、こうしたアクティビティは最小限のプロセッサ時間しか使用しないので、アプリケーションに目立った影響が出ることはほとんどありません。また、当社のデータベースの構築方法により、これらのアクティビティは高度に最適化されています。

暗号化と解読には、米国政府の Advanced Encryption Standard (AES) が Cipher Block Chaining (CBC) モードで使用されています (単純に AES CBC と呼ばれています)。InterSystems IRIS は、AES CBC の 128、192、256 ビットのすべての法定キー・サイズをサポートしています。

InterSystems IRIS は、使用可能な最速の実装を使用して暗号化と解読を実行します。暗号化と解読では、使用可能な場合は常にプロセッサベースの命令セットとそれ本来の効率性が活用されます。最新の Intel および IBM POWER8 プロセッサはこうした命令を装備しています。InterSystems IRIS はこうした命令を自動的に検出して使用するので、ユーザがアクションを起こす必要はありません。Intel プロセッサでは、これは Advanced Encryption Standard New Instructions (AES-NI) に該当します。IBM では AES VMX 命令セットになります。

データベース暗号化キーは、Key Management Interoperability Protocol (KMIP) をサポートするキー管理サーバか、データベース・キーの暗号化コピーを格納するファイル内に保存できます。どちらにも独自の利点があります。

- KMIP は、クライアントがキー管理システムと通信するための OASIS 標準プロトコルです。KMIP サーバは、特殊なハードウェア・アプライアンスか、キー管理ソフトウェアを実行する一般目的のサーバにすることができます。
- データベース暗号化キーのファイル保存時に、インターシステムズは複数層の AES Key Wrap アルゴリズムを使用してキーを暗号化し、個々の管理者のキー暗号化キーは PBKDF2 アルゴリズムを使用して生成されるので、ディクショナリおよび総当り攻撃は実行不可能です。

留意すべき重要な点は、データベース暗号化はセキュリティ戦略に不可欠な部分ではあるものの、それだけではセキュリティの脆弱性に対処できないことです。伝送中のデータ保護など、その他のツールも非常に重要です。データベース暗号化が、InterSystems IRIS でデータ保護のために提供する一連のツールの一部であるのはこのためです。こうしたツールには、以下のものがあります。

- 政府規格のサポート – データベース暗号化に対する FIPS 140-2 (Federal Information Processing Standards) への準拠が検証されたライブラリを使用するように InterSystems IRIS を構成できます。これは Red Hat Linux で使用できます。
- 選択したデータ要素の保護 – データ要素暗号化と呼ばれるこの機能は、レコードの選択した部分 (クレジット・カード番号や社会保障番号など) のみを暗号化できるプログラミング手法を提供します。
- 伝送中のデータ保護 – InterSystems IRIS は、最新バージョンの TLS (Transport-Layer Security) を使用して、伝送中のデータを保護します。TLS は、データ通信を保護するための業界標準のプロトコルです。
- サードパーティ認証のサポート – InterSystems IRIS はサードパーティのサイトのリソースを使用するための認証をサポートします。よく見られるのは、Web 上でサイトを使用するために Facebook や Google を介してログインする方法です。これは Open Authorization Framework バージョン 2.0 (OAuth 2.0) を使用しており、別の層を介した認証 (OpenID Connect) が含まれることもあります。

3 データベース暗号化を試してみる

InterSystems IRIS データベース暗号化は簡単に使用できます。以下の単純な手順によって、暗号化されたデータベースを設定するための基本手順を説明します。

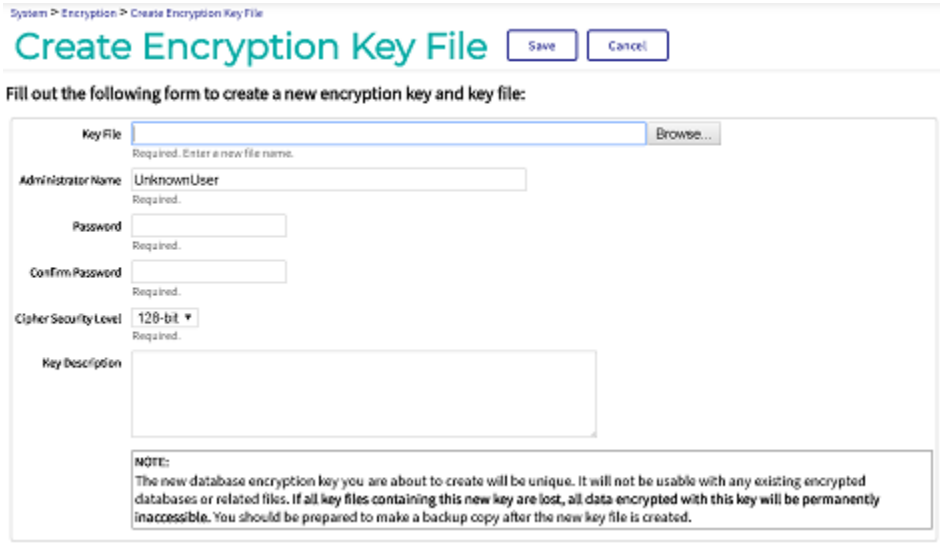
3.1 開始の前に

この手順を使用するには、InterSystems IRIS の稼働中インスタンスが必要です。選択肢としては、いくつかのタイプのライセンス付与されたインスタンスおよび無料の評価版インスタンスがあります。操作を実行するインスタンスをまだ用意できていない場合にインスタンスのタイプ別の導入方法の詳細を確認するには、″InterSystems IRIS の基礎 : IDE の接続″ の ″InterSystems IRIS の導入″ を参照してください。

3.2 暗号化キーの作成

最初にキー・ファイルを作成します。ここでデータベース暗号化キーが自動生成されます。

1. ″InterSystems IRIS の基礎 : IDE の接続″ で説明している該当のインスタンス用の URL を使用して、ブラウザ内でインスタンスの管理ポータルを開きます。
2. **[暗号化キーファイルを作成]** ページ (**[システム管理]** → **[暗号化]** → **[新しい暗号化キーファイルを作成]**) に移動します。



3. **[暗号キー・ファイル作成]** ページで、次の手順を実行します。
   a. **[キー・ファイル]** フィールドに、キー・ファイルの名前とパスを入力します。**[参照]** ボタンをクリックすると、既定でインスタンスの install-dir/**mgr** ディレクトリ (install-dir は InterSystems IRIS のインストール・ディレクトリ) (例えば、**C:¥InterSystems¥IRIS¥mgr¥testkeys.key**) で [ファイル選択] ダイアログが開きます。すべてのタイプのインスタンスでこのディレクトリを使用することも、ホストまたはコンテナのファイル・システム内の別の場所を選択することもできます。
   b. **[管理者名]**、**[パスワード]**、**[パスワード確認]** フィールドに、`testadmin` や `password` などの値を入力します。これは単なる実践例なので、開発環境で使用するパスワードを再利用しないでください。
   c. ページ上部にある **[保存]** ボタンを選択します。

C:¥InterSystems¥directory に testkeys.key というキー・ファイルが作成されました。このファイルにはデータベース暗号化に使用できるキーが含まれています。InterSystems IRIS には、次のように、ファイル内にあるキーを示すメッセージが表示されます。

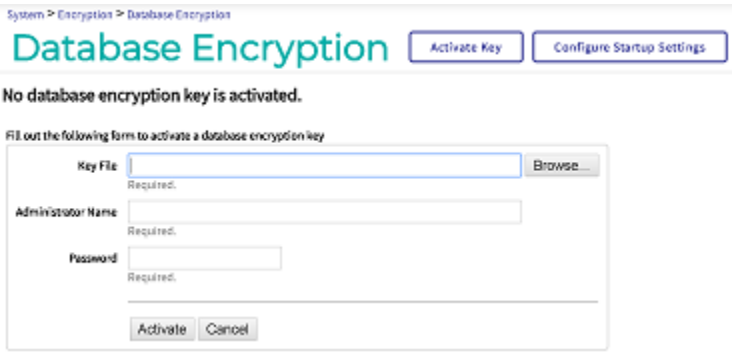
```
New encryption key ID: 46D153E1-F895-42F9-9706-D1236115E45A
```

キー・ファイルおよびその初期キーの作成の詳細は、"キー・ファイルの作成" を参照してください。

3.3 暗号化キーの有効化

次に、作成したキーを有効化します。

1. 管理ポータルで、[**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. [データベース暗号化] ページで、[**キーを有効にする**] ボタンを選択します。



3. [**キー・ファイル**] フィールドに、作成したキー・ファイルの場所を入力します (C:¥InterSystems¥IRIS¥mgr¥testkeys.key など)。
4. [**管理者名**] および [**パスワード**] フィールドに、指定した値を入力します (`testadmin` と `password`)。
5. [**有効化**] ボタンを選択します。

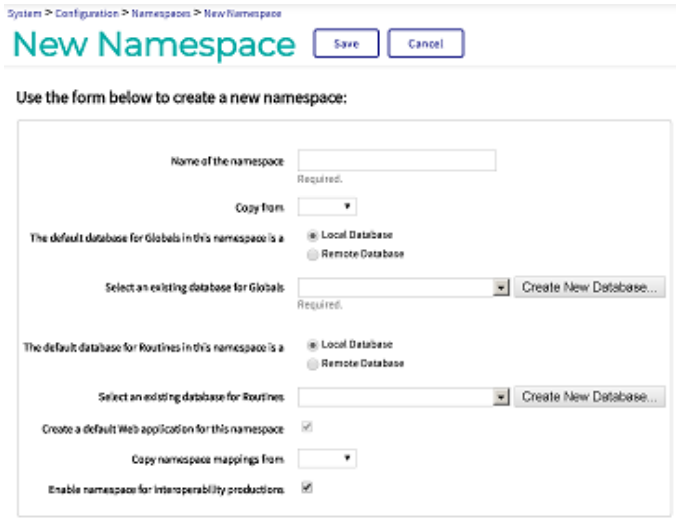
このページにキー ID が表示されます。

キーの有効化の詳細は、"キー・ファイル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。

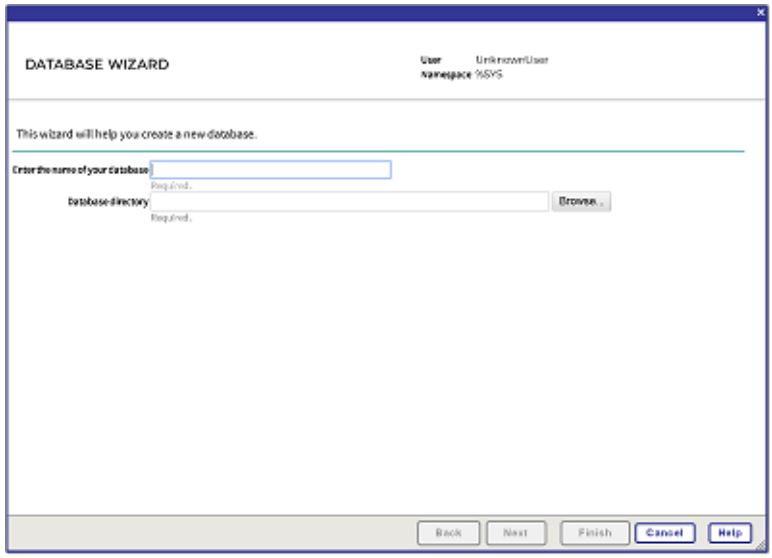
3.4 暗号化データベースの作成

これで、暗号化データベースを作成できるようになりました。

1. 再び管理ポータルで、[**ネームスペース**] ページに移動します ([**システム管理**] → [**構成**] → [**システム構成**] → [**ネームスペース**])。
2. [**ネームスペース**] ページで、[**新規ネームスペース作成**] を選択します。[**新規ネームスペース**] ページが表示されます。



3. [**新規ネームスペース**] ページで、作成する暗号化データベースの名前を入力します (**ENCDB** など)。
4. [**グローバルに既存のデータベースを選択**] ドロップダウン・メニューの横の [**新規データベース作成**] ボタンを選択します。[**データベースウィザード**] が表示されます。



5. [**データベースウィザード**] の最初のページで、[**データベースの名前を入力してください**] フィールドに、作成するデータベースの名前 (**ENCDB** など) を入力します。データベースのディレクトリ (**C:¥InterSystems¥IRIS¥mgr¥ENCDB** など) を入力します。このページで [**次へ**] を選択します。
6. 次のページで、[**暗号化データベース**] の値を `No` から `Yes` に変更します。このページで [**完了**] を選択します。
7. [**新規ネームスペース**] ページに戻り、[**ルーチンに既存のデータベースを選択**] ドロップダウン・メニューで、作成したデータベースを選択します (**ENCDB** など)。
8. ページの上部にある [**保存**] ボタンを選択し、次に、結果のログの末尾の [**閉じる**] を選択します。

これで **ENCDB** という名前の暗号化データベースが作成されました。このデータベースはキー・ファイルの作成時に InterSystems IRIS によって作成されたキーを使用します。このデータベースは、暗号化されていないデータベースと同じように使用できます。InterSystems IRIS では暗号化と解読のすべての機能が非表示で行われるので、ユーザはすべての操作を通常の方法で実行することができます。データはすべて暗号化されます。

ネームスペースとそれに関連するデータベースの詳細は、"InterSystems IRIS システム管理ガイド" の "InterSystems IRIS の構成" の章にある "ネームスペースの作成/変更" を参照してください。背景情報は、"サーバ側プログラミングの入門ガイド" の "ネームスペースとデータベース" を参照してください。

3.5 暗号化されたデータの確認

暗号化データベースの作成後は、その他の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。唯一異なる点は、データの保存方法です。暗号化データベースに保存されたデータと暗号化されていないデータベースに保存されたデータの違いを確認するには、以下の単純なテストを実行できます。

1. "InterSystems IRIS の基礎：IDE の接続" で説明している該当のインスタンスについての手順を使用して、InterSystems IRIS のターミナルを開きます。

2. 以下のコマンドを使用して、暗号化データベースのネームスペースに切り替えます。

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

3. **ENCDB** ネームスペースで、次のコマンドを実行します。

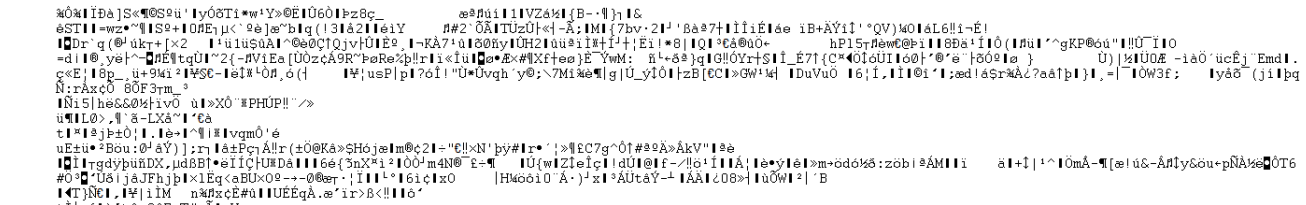
```
ENCDB>for i=1:1:1000 set ^x(i)="This is test number "_i
```

これにより、`This is test number 22` というようなコンテンツを含む 1,000 個の永続変数が作成されます。

4. 成功したことを確認するには、1 つの変数の値を表示します。

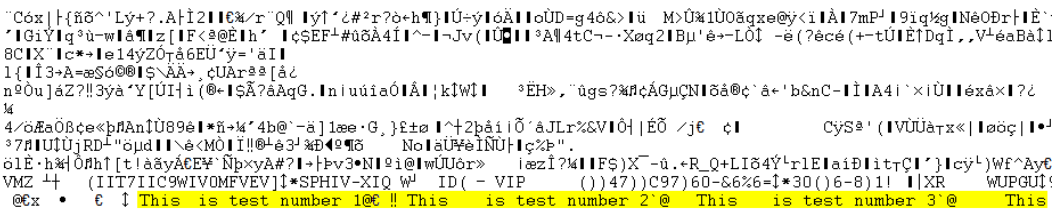
```
ENCDB>w ^x(22)
This is test number 22
ENCDB>
```

5. データベース・ファイルを開くには、前のセクションでこれを作成したディレクトリ (C:¥InterSystems¥IRIS¥mgr¥ENCDB など) に移動して、データベース・ファイル IRIS.DAT を開きます。コンテンツは以下のように表示されます。



6. ファイル内で "This is test number" という文字列を探してみます。文字列は見つかりません。データベースが暗号化されているからです。実際、見つかる唯一の暗号化されていない文字列は、データベースの名前かデータベースの暗号化キーの識別子です。

7. 暗号化されていないデータベースで同じテストを実行した場合、結果のファイルには以下のようなコンテンツが含まれます。



スクリーン・ショットの最後の行に、ターミナルの変数セットの値が含まれています。

3.6 データベース暗号化に関係するその他の機能

InterSystems IRIS にはこの他にも、実装に重要な役割を果たすと思われる重要なデータベース暗号化機能が含まれています。

- KMIP ー InterSystems IRIS では、インスタンスをホストするサーバとは別のサーバにキーを保存できます。こうしたサーバと通信するために、InterSystems IRIS は Key Management Interoperability Protocol (KMIP) をサポートしています。これにより InterSystems IRIS では、KMIP が提供するキー管理に対する標準手法の利点を得ることができます。
- キーの変更と暗号化の追加または削除ー データベースの暗号化キーを簡単に変更できます。必要とあれば、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暗号化されていないコピーの作成も、簡単です。
- ディスク上の関連データの暗号化 ー InterSystems では、最近のトランザクション・レコードを最新に保つ (つまり、ジャーナル・ファイルの) ために使用する一時的なキャッシュ・データベースやその他のディスク上のコンテンツを、簡単に暗号化できます。
- チップベースの暗号化 ー チップにより、アクティビティの一環として暗号化を実行できます。これにより動作が大幅に高速化します。InterSystems IRIS はこうしたチップの使用をサポートしています。チップベースの暗号化の詳細は、次のセクションを参照してください。

4 データベースの暗号化の詳細

インターシステムズでは、データベース暗号化を詳しく学習できるように、多数のリソースを提供しています。

- Encryption Awareness ー インターシステムズの暗号化テクノロジの概念を紹介するインターシステムズのオンライン学習インタラクティブ・コース。
- ″暗号化ガイド″ ー データベースの暗号化および関連機能に関するインターシステムズのドキュメント。
- ″データベース暗号化の FIPS 140-2 準拠″ ー InterSystems IRIS の FIPS 140-2 標準サポートに関するインターシステムズのドキュメント。