記事
Mihoko Iijima · 2020年12月28日 3m read

データベースの暗号化手順について

これは InterSystems FAQ サイトの記事です。

データベース暗号化は、ディスクへの書き込みまたはディスクからの読み取りで暗号化と復号が実行されるため、アプリケーションのロジックに手を加える必要はありません。

この機能のドキュメントについては、以下ご参照ください。

マネージド・キー暗号化【IRIS】

マネージド・キー暗号化

暗号化データベース作成までの流れは、以下の通りです。

(1) 暗号化キーの作成

- (a) 管理者 ユーザ名/パスワード
- (b) 暗号化キーファイル

(2) 暗号化キーの有効化

(3) 暗号化されたデータベースの作成

暗号化データベース作成後の運用のための設定は以下の通りです。

○ データベース暗号化の起動設定（暗号化キーの有効化をどのように行うか）

暗号化されたデータベースは、"暗号化キーの有効" が行われてアクセスできるようになります。
既定の設定では、"暗号化キーの有効"を行いませんので、以下3種類の方法から選択します。

① キーを有効化しない起動の構成

既定の設定のまま、インスタンス起動時に "暗号化キーの有効" が行われません。
暗号化されたデータベースをマウントする前に管理ポータルなどから "暗号化キーの有効"
を行う必要があります。

以下の場合、この運用は適応できません。

- 起動時に暗号化データベースのマウントが必要な場合
- 暗号化されたジャーナル・ファイルを利用している場合

- 監査ログが暗号化されている場合

② インタラクティブ（対話式）にキーを有効化する起動の構成

インスタンス起動時に、インタラクティブに "暗号化キーの有効" を行います。

③ 無人でキーを有効化する起動の構成

インスタンス起動時に、自動的に "暗号化キーの有効" を行います。

セキュリティの強度については、①および②の運用の方が、③よりも強度が高くなります。詳細は、下記ドキュメントページをご確認ください。

データベース暗号化の起動設定の構成【IRIS】
データベース暗号化の起動設定の構成

○暗号化キーファイル および 管理者とパスワードの管理方法(管理をどうするか)

暗号化キーの有効化するには以下の 2 つの情報が必要です。

(a) 管理者 ユーザ名/パスワード
(b) 暗号化キーファイル

これらに関して、ファイルの損失、管理者のユーザ名/パスワードの失念や漏えい等から防ぐ方法については、以下のドキュメントページをご確認ください。

データ損失に対する保護【IRIS】
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

○ 緊急事態(緊急事態の対処方法)

緊急事態として以下の場合の対処については下記ページをご確認ください。

緊急事態への対処【IRIS】
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【IRIS】
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【IRIS】

緊急事態
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
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

#システム管理 #セキュリティ #暗号化 #Caché #Ensemble #InterSystems IRIS #InterSystems IRIS for Health

ソースURL:
https://jp.community.intersystems.com/post/%E3%83%87%E3%83%BC%E3%82%BF%E3%83%99%E3%83%BC%E3%82%B9%E3%81%AE%E6%9A%97%E5%8F%B7%E5%8C%96%E6%89%8B%E9%A0%86%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6