# Adabas for Linux, UNIX and Windows

## Adabas のセキュリティ機能

バージョン 6.6

2017 年 10 月

ADABAS & NATURAL

このマニュアルは Adabas for Linux, UNIX and Windows バージョン 6.6 およびそれ以降のすべてのリリースに適用されます。

このマニュアルに記載される仕様は変更される可能性があります。変更は以降のリリースノートまたは新しいマニュアルに記述されます。



**ドキュメント IDは: ADAOS-SECFAC-66-20200619JA**

# 目次

# Adabas のセキュリティ機能

このドキュメントでは、Adabas と Adabas サブシステムが提供するセキュリティ機能について説明します。

次のトピックについて説明します。

- *Adabas 認証*
- *Adabas ユーティリティの認可*
- *Adabas パスワードのセキュリティ（ADASCR）*
- *暗号化*
- *セキュリティの考慮事項*
- *SSXLoginModule コンフィグレーションテンプレート*

# 1

# 表記規則

| 規則 | 説明 |
|---|---|
| 太字 | 画面上の要素を表します。 |
| モノスペースフォント | *folder.subfolder:service* という規則を使用して webMethods Integration Server 上のサービスの保存場所を表します。 |
| 大文字 | キーボードのキーを表します。同時に押す必要があるキーは、プラス記号 (+) で結んで表記されます。 |
| *斜体* | 独自の状況または環境に固有の値を指定する必要がある変数を表します。本文で最初に出現する新しい用語を表します。 |
| モノスペースフォント | 入力する必要があるテキストまたはシステムから表示されるメッセージを表します。Program code. |
| { } | 選択肢のセットを表します。ここから1つ選択する必要があります。中カッコの内側にある情報のみを入力します。{ } 記号は入力しません。 |
| \| | 構文行で相互排他的な2つの選択肢を区切ります。いずれかの選択肢を入力します。\| 記号は入力しません。 |
| [ ] | 1 つ以上のオプションを表します。大カッコの内側にある情報のみを入力します。[ ] 記号は入力しません。 |
| ... | 同じ種類の情報を複数回入力できることを示します。情報だけを入力してください。実際のコードに繰り返し記号 (...) を入力しないでください。 |

# オンライン情報

**Software AG** マニュアルの **Web** サイト

マニュアルは、Software AG マニュアルの Web サイト (**http://documentation.softwareag.com**) で入手できます。このサイトでは Empower クレデンシャルが必要です。Empower クレデンシャルがない場合は、TECHcommunity Web サイトを使用する必要があります。

**Software AG Empower** 製品のサポート **Web** サイト

もしまだEmpowerのアカウントをお持ちでないのなら、こちらへempower@softwareag.com電子メールにて あなたのお名前、会社名、会社の電子メールアドレスをお書きの上、アカウントを請求してください。

いったんアカウントをお持ちになれば、Empower **https://empower.softwareag.com/** のeServiceセクションにてサポートインシデントをオンラインで開くことができます。

製品情報は、Software AG Empower 製品のサポート Web サイト (**https://empower.softwareag.com**) で入手できます。

機能および拡張機能に関するリクエストの送信、製品の可用性に関する情報の取得、製品のダウンロードを実行するには、Products に移動します。

修正に関する情報を取得し、早期警告、技術論文、Knowledge Base の記事を読むには、**Knowledge Center** に移動します。

もしご質問があれは、こちらの**https://empower.softwareag.com/public_directory.asp** グローバルサポート連絡一覧の、あなたの国の電話番号を選んで、わたくし共へご連絡ください。

**Software AG TECHcommunity**

マニュアルおよびその他の技術情報は、Software AG TECHcommunity Web サイト (**http://techcommunity.softwareag.com**) で入手できます。以下の操作を実行できます。

- TECHcommunity クレデンシャルを持っている場合は、製品マニュアルにアクセスできます。TECHcommunity クレデンシャルがない場合は、登録し、関心事の領域として [マニュアル] を指定する必要があります。
- 記事、コードサンプル、デモ、チュートリアルにアクセスする。
- Software AGの専門家によって承認されたオンライン掲示板フォーラムを使用して、質問したり、ベストプラクティスを話し合ったり、他の顧客が Software AG のテクノロジをどのように使用しているかを学んだりすることが可能です。
- オープンスタンダードや Web テクノロジを取り扱う外部 Web サイトにリンクできます。

## データ保護

Software AG製品は、EU一般データ保護規則(GDPR)を尊重した個人データの処理機能を提供します。 該当する場合、適切な手順がそれぞれの管理ドキュメントに記載されています。

# 2 Adabas 認証

認証は、アクセスを許可する前にユーザーが有効なユーザー名と有効なパスワードを入力する方法で、ユーザーを識別します。

Adabas サーバーは、LDAP、Active Directory、オペレーティングシステム、または内部リポジトリなどの外部認証システムのセキュリティ定義に対して資格情報をチェックします。資格情報が一致する場合は、データベースへのアクセス権限がユーザーに付与されます。資格情報が一致しない場合は、認証が失敗し、データベースへのアクセスは拒否されます。

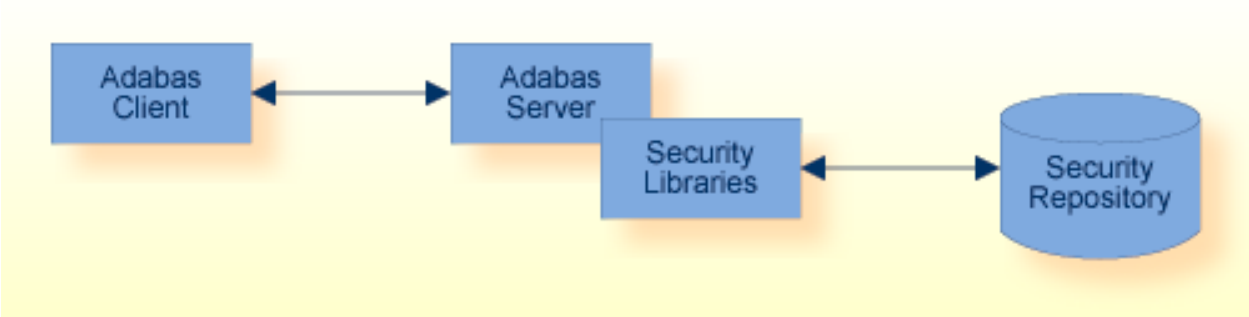
監査証跡には、データベースへの成功したアクセス試行と失敗したアクセス試行の両方が記録されます。

現在のバージョンの場合：

- セキュリティインフラストラクチャは、外部セキュリティシステムへのアクセスを提供するために使用します。
- サポートされている資格情報は、ドメイン、ユーザー ID およびパスワードです。
- 認証は、データベースへの「アクセス可否」を意味します。
- データベースユーティリティは、認証チェックを実行しません。
- 監査証跡は、ADABAS ロギングファイルに書き込まれます。

# 認証の仕組み

アーキテクチャ




認証プロセス

- アプリケーションが資格情報（ユーザー ID とパスワード）を提供します。
- Adabas サーバーは、セキュリティインフラストラクチャを介して資格情報の検証を要求します。
- セキュリティインフラストラクチャは、セキュリティリポジトリに対して資格情報を検証します。

## セキュリティインフラストラクチャ

Adabas サーバーは、セキュリティインフラストラクチャの事前定義されたログインモジュール `SSXLoginModule` を使用して、ユーザー資格情報を認証します。

認証は、LDAP、Active Directory、内部リポジトリ、またはオペレーティングシステムに対して行われます。

`SSXLoginModule` は、Software AG インストーラに付属のセキュリティライブラリの一部です。この機能を使用するには、このコンポーネントをインストールする必要があります。

## 初期セットアップ

**Adabas** のインストール時

Adabas サーバーは、インフラストラクチャセキュリティライブラリを必要とします。これらには、Adabas 認証機能の実装に必要な機能が含まれています。

インフラストラクチャセキュリティライブラリは Software AG インストーラによってインストールされます。GUI インストールで、デフォルトで事前に選択されています。

### 手順 2.1. 認証セキュリティ機能を有効にする

1 ADAINI ユーティリティを使用して、次の操作を実行します。

- 拡張オペレーションデータベースログを定義します。
- 拡張オペレーションアナライザを有効にします。
- 監査証跡機能を有効にします。

  **注意:** これはデータベース固有なので、各データベースに対して実行する必要があります。

- `SSXLoginModule` の使用方法を設定します。
  - 認可タイプ固有のオプション
  - ロギング／診断オプション

2 ADADBM ユーティリティの *SECURITY* 機能を使用して、認証セキュリティ機能を有効にします。

3 データベースを起動します。

### 手順 2.2. レガシーアプリケーションが認証を使用できるようにする

Adabas ニュークリアスユーザー出口 21 は、認証機能を使用するようにレガシーアプリケーションを変更するときに有用なルーチンです。詳細については、「*認証を使用するようにレガシーアプリケーションを変更する*」を参照してください。

1 サイト固有の要件を満たすように、サンプルの Adabas ニュークリアスユーザー出口 21 をカスタマイズします。

2 サイト固有のニュークリアスユーザー出口を構築します。

3 ニュークリアスユーザー出口の環境設定を変更します。

4 USEREXITS パラメータを指定してデータベースを起動します。

## 構成

このセクションでは、認証および監査証跡機能を設定する方法について説明します。

- パフォーマンスの考慮事項

## 監査証跡

監査証跡はデータベースログファイルに書き込まれるので、イベントアナライザ（AEO アナライザまたは単にアナライザともいいます）を有効にする必要があります。アナライザは、*ADABAS.INI* コンフィグレーションファイルの NODE_PARAMETER を使って有効にします。そのため、ノード内のすべてのデータベースでアナライザが有効になります。

監査証跡機能はデータベース固有で、*DBnnn.INI* コンフィグレーションファイルを介して構成されます。監査証跡フィルタは、セキュリティイベントを受け取り、データベースログファイルに書き出します。このログファイルで、これらのイベントを解析できます。すべてのアクセス試行を記録することも、セキュリティ違反のみを記録することもできます。

| コンフィグレーションファイル | セクション | サブトピック | 項目 |
|---|---|---|---|
| ADABAS.INI | NODE_PARAMETER | ANALYSER | ACTION |
| | | LOGGING | ACTION<br>LOG_FILE |
| DB*nnn*.INI | DB_PARAMETER | AUDIT_TRAIL | ACTION<br>FILTER |

コンフィグレーションファイルと構文の詳細については、『*拡張オペレーション*』ドキュメントの「*ADABAS.INI*」および「*DBnnn.INI*」の説明を参照してください。

## 認証

認証チェックはデータベース固有で、SSXLoginModule オプションを使用して設定します。これらのオプションは、*DBnnn.INI* に入力します。

| コンフィグレーションファイル | セクション | サブトピック | 項目 |
|---|---|---|---|
| DB*nnn*.INI | DB_PARAMETER | SSX_CONFIGURATION | *SSX コンフィグレーションオプション* |

コンフィグレーションファイルと構文の詳細については、『*拡張オペレーション*』ドキュメントの「*DBnnn.INI*」の説明を参照してください。

SSXLoginModule は、次のような複数の認可タイプ（またはメソッド）をサポートしています。

| AuthType | 説明 |
|---|---|
| TEXT | 認証は、Software AG 内部ユーザーリポジトリにあるセキュリティ定義を使用して実行されます。 |
| LDAP | 認証は、LDAP のセキュリティ定義を使用して実行されます。 |
| ADSI | 認証は、Active Directory のセキュリティ定義を使用して実行されます。 |
| OS | 認証は、オペレーティングシステムのセキュリティ定義を使用して実行されます。 |

さまざまな認可タイプの例とサンプルテンプレートが「*SSXLoginModule コンフィグレーションテンプレート*」セクションにあります。これらのテンプレートは、一部の設定がユーザーに固有であり、必要に応じて変更する必要があるので、完全ではありません。

## パフォーマンスの考慮事項

次のコンフィグレーションオプションはパフォーマンスに悪影響を及ぼすので、注意して使用してください。

| 機能 | オプション | 説明 |
|---|---|---|
| 監査証跡 | LOG_FILE | 同じリソースで複数のデータベースが競合しているとき（同じデータベースログファイルにアクセスしているときなど）に、データベースログファイルに大量のエントリが書き込まれると、パフォーマンスに悪影響を及ぼす可能性があります。 |
| 監査証跡 | FILTER | 大量のユーザーセッションがあると、データベースログファイルに大量のセキュリティエントリが書き込まれます。ユーザーセッション数が増えると、データベースログファイルのサイズが急速に大きくなります。<br><br>デフォルト値：FILTER = ALL。<br><br>推奨される値：FILTER = REJECT。 |
| SSX ロギング／診断 | nativeloglevel | 複数のユーザーセッションが、セキュリティインフラストラクチャログファイルに診断情報を同時に書き込もうとします。<br><br>デフォルト値：None。<br><br>推奨される値：0 または None。 |

# セキュリティモードの有効化

セキュリティモードは、ADADBM ユーティリティの *SECURITY* 機能を使って有効にします。

次のデータベースセキュリティモードを使用できます。

- セキュリティモード ACTIVE により、セキュリティ機能がアクティブになり、認証されたユーザーのみがデータベースにアクセスできるようになります。モード ACTIVE は、変更も無効化もできません。
- セキュリティモード WARN はセキュリティ機能をシミュレートします。これを定義すると、セキュリティ違反が発生した場合に、データベースログファイルに警告が書き込まれますが、データベースへのアクセスは拒否されません。モード WARN は、ACTIVE にのみ変更できます。

**重要:** データベースセキュリティモードは、WARN または ACTIVE のいずれかに設定できます。セキュリティモードをいったん有効にすると、無効にできなくなります。

**ヒント:** セキュリティモードをアクティブにする前に、リカバリ目的でデータベースのバックアップを作成することをお勧めします。

# Adabas 認証に必要なユーティリティ

認証セキュリティ機能の設定と管理に必要なユーティリティは次のとおりです。

- ADADBM - セキュリティモードの有効化
- ADAREP - データベースセキュリティモードの問い合わせ
- ADAINI - セキュリティ機能の設定

## ADADBM - セキュリティモードの有効化

認証および監査機能をアクティブにするには、ADADBM ユーティリティの *SECURITY* 機能を使用します。

**注意:** SECURITY 機能を使用するには、セキュリティ保護するデータベースがオフラインになっている必要があります。

```
adadbm: dbid=nnn
%ADADBM-I-DBOFF, database nnn accessed offline
adadbm: security=active
%ADADBM-I-FUNC, function SECURITY executed
```

### ADAREP - データベースセキュリティモードの問い合わせ

データベースセキュリティモード設定を表示するには、ADAREPユーティリティの*SUMMARY*機能を使用します。

**注意:** セキュリティモード設定は、機能がアクティブになっている場合にのみ表示されます。機能がアクティブになっていない場合は、表示されません。

### ADAINI - セキュリティ機能の設定

セキュリティ機能のコンフィグレーションの設定と変更には、ADAINI ユーティリティを使用します。ADAINI を使用してセキュリティ機能を設定する例を以下に示します。

例 **1**：拡張オペレーションロギングのアクティブ化

```
ADABAS.INI
> adaini   add topic=NODE_PARAMETER topic=LOGGING  ↩
item=LOG_FILE=path_and_name_adabas_log_file
> adaini   add topic=NODE_PARAMETER topic=LOGGING  item=ACTION=YES
> adaini   add topic=NODE_PARAMETER topic=ANALYSER item=ACTION=YES
```

例 **2**：監査証跡のアクティブ化

```
DBnnn.INI
> adaini dbid=nnn add topic=DB_PARAMETER topic=AUDIT_TRAIL item=FILTER=ALL
> adaini dbid=nnn add topic=DB_PARAMETER topic=AUDIT_TRAIL item=ACTION=YES
```

例 **3**：認可タイプ **TEXT** の設定

```
DBnnn.INI
> adaini dbid=nnn add topic=DB_PARAMETER topic=SSX_CONFIGURATION item=authType=TEXT
> adaini dbid=nnn add topic=DB_PARAMETER topic=SSX_CONFIGURATION ↩
item=internalRepository=path_and_name_ssxuser_file
```

例 **4**：セキュリティインフラストラクチャログの設定

```
DBnnn.INI
> adaini dbid=nnn add topic=DB_PARAMETER topic=SSX_CONFIGURATION ↩
item=nativeLogFile=path_and_name_of_ssxlog_file
> adaini dbid=nnn add topic=DB_PARAMETER topic=SSX_CONFIGURATION item=nativeLogLevel=6
```

例 **5**：コンフィグレーション設定の表示

```
ADABAS.INI
> adaini   show topic=NODE_PARAMETER

DBnnn.INI
> adaini dbid=nnn show topic=DB_PARAMETER
```

# アプリケーションの開発



## 認証を使用するようにアプリケーションを開発する

アプリケーションが、データベースセッションのオープン前にユーザーの資格情報を設定します。

クライアントセッションを管理し、資格情報を設定するために次の Adabas クライアント機能が提供されます：

| 手順 | 機能 | 説明 |
|---|---|---|
| 1 | lnk_set_adabas_id() | セッション ID を設定します。 |
| 2 | lnk_set_uid_pw() | 特定のデータベースの認証資格情報を設定します。 |

上記の Adabas クライアント機能の詳細については、『*コマンドリファレンス*』ドキュメントの「*Adabas の呼び出し*」セクションにある「*認証を使用した Adabas の呼び出し*」セクションを参照してください。

## 認証を使用するようにレガシーアプリケーションを変更する

変更を行わないと、レガシーアプリケーションは、セキュリティ保護されたデータベースにアクセスしたときに、ニュークリアスレスポンス 200「セキュリティ違反」を受け取ります。

Adabas ニュークリアスユーザー出口 21 を使用し、ADABAS サーバー API 機能を介して認証資格情報を設定することができます。ルーチンは、セッション処理の開始時にコールされます。

このルーチンはできる限り短期間で使用する必要があります。これは、すべてのアプリケーションが Adabas セキュリティの認証機能を使用およびサポートするまでの、移行期間中の使用を目的としています。

詳細については、「*ユーザー出口とハイパー出口*」セクションの「*ニュークリアスユーザー出口 21*」を参照してください。

### SSXLoginModule コンフィグレーションテンプレート

以下のコンフィグレーションオプションを、`DB_PARAMETER` セクションのサブトピック `SSX_CONFIGURATION` にあるコンフィグレーションファイル *DBnnn.INI* に設定する必要があります。

```
DBnnn.INI

[DB_PARAMETER]
  [SSX_CONFIGURATION]
    <option>=<value>
  [SSX_CONFIGURATION-END]
[DB_PARAMETER-END]
```

「*SSXLoginModule コンフィグレーションテンプレート*」には、さまざまな認可タイプ（OS、TEXT、LDAP、ADSI）で使用可能な、追加のコンフィグレーションテンプレートがあります。

# 3 Adabas ユーティリティの認可

Adabasは、役割ベースのアクセス制御（RBAC）のコンセプトを使用して、Adabasユーティリティの認可を実装します。

セキュリティ定義の範囲は、1つのデータベース（モードADABAS）に制限することも、インストールされているすべてのデータベースがあるマシン（モードINI）に制限することもできます。

詳細については、「*Adabas ユーティリティの認可（モード ADABAS）*」または「*Adabas ユーティリティの認可（モード INI）*」を参照してください。

## Adabas 役割ベースのアクセス制御

認可は、選択的なアクセス権限を表す役割をユーザーに割り当てる方法で、データベース上でのAdabas ユーティリティの使用を制限する手段を提供します。

ローカルマシンへのアクセスに使用した資格情報で、ユーザーが識別されます。

Adabasユーティリティは、セキュリティリポジトリのセキュリティ定義に対して、提供された資格情報をチェックします。セキュリティリポジトリは、コンフィグレーション時に選択されたモードによって異なります。詳細については、「コンフィグレーション」を参照してください。

資格情報に役割が割り当てられている場合は、データベースに要求された処理に対するアクセス権限が決定されます。アクセス権限が十分であれば、ユーザーはデータベースでユーティリティを実行できます。アクセス権限が不十分または欠落している場合は、認可が失敗し、ユーティリティの使用が拒否されます。

セキュリティリポジトリは、付与された権限を格納します。特定の処理の拒否はサポートしていません。

監査証跡には、Adabas ユーティリティの使用試行の成功と失敗の両方が記録されます。

現在のバージョンの場合：

- Adabas ユーティリティは、認証チェックを実行しません。
- サポートされている資格情報は、ローカルシステムの資格情報です。
- 認可とは、ユーティリティと、処理が実行されるデータベースの "usage or no usage" を意味します。
- 監査証跡はログファイルに書き込まれます。これは構成できます。
- 認可機能は、次の Adabas ユーティリティでのみ使用できます：ADABCK、ADADBM、ADAELA、ADAFDU、ADAFRM、ADAOPR、ADAORD、ADARBA、ADAREC、ADAREP、ADASCR、ADAULD。


  - データモデル
  - アーキテクチャ

## データモデル

Adabas 役割ベースのアクセス制御は、ユーザーの役割に基づいてデータベースアクセスを制限します。

特定の Adabas ユーティリティを実行する権限が役割に付与され、ユーザーは、割り当てられた役割を通じて Adabas ユーティリティの実行を許可されます。

Adabas RBAC は、オブジェクトタイプ Users、Roles、Actions、および Resources を認識します。Assignments と Privileges は、これらのエンティティ間の関係を表します。

**User**
ユーザー名。

**Role**
役割名グループのアクセス権限。

**Action**
Adabas ユーティリティ。

**Resource**
データベース ID です。現在のデータベースは *DBID.CURRENT* で表されます。

**Assignment**

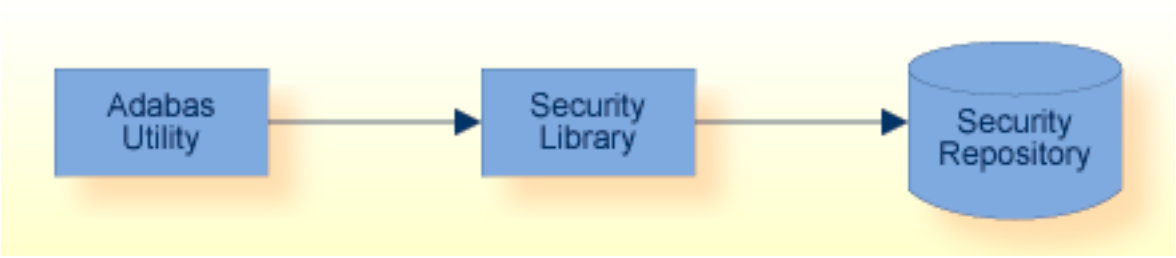
- 1 人のユーザーに複数の役割を割り当てることができます。
- 1 つの役割を複数のユーザーに割り当てることができます。

**Privilege**

- 1 つの役割に複数の権限を付与できます。
- 特定の権限を複数の役割に付与できます。

## アーキテクチャ

セキュリティライブラリは、セキュリティリポジトリに定義されているアクセス権限に対して、Adabas ユーティリティのアクセス要求を検証します。




## 認証

Adabas ユーティリティの認証では、ユーザー認証にログイン資格情報を使用します。

- UNIX：ユーザー ID
- Windows：ドメインおよびユーザー ID

## 認可プロセス

Adabas ユーティリティの認可では、RBAC セキュリティ定義を使用して、指定されたデータベース上での要求された処理を認可します。

セキュリティライブラリは、セキュリティリポジトリに定義されているアクセス権限に対して、アクセス要求を検証します。

一致するアクセス権限が見つかった場合、Adabas ユーティリティは、要求された処理の実行を許可されます。そうでない場合は、要求が拒否されます。

## セキュリティインフラストラクチャ

必要なコンポーネントとコンフィグレーションファイルのインストールは必須です。

## 初期セットアップ

セキュリティインフラストラクチャは、Adabas ユーティリティに必要です。

インストール中に、以下のような初期セキュリティコンフィグレーションが作成されます。

- 監査証跡が事前設定されます。
- 制限のない役割ベースのセキュリティ定義の最小セットがインストールされます。
- 認可はアクティブになりません。

## コンフィグレーションファイル

このセクションでは、認可機能を設定する方法について説明します。

Adabas ユーティリティの認可のコンフィグレーションは、次のファイルに格納されます。

| コンフィグレーションファイル | 説明 |
|---|---|
| `adaauth.ini` | Adabas ユーティリティの認可の設定 |
| `adaaudit.ini` | 監査証跡の構成 |
| `adarbac.ini` | 役割ベースのアクセス制御の定義（MODE=INI） |

これらのファイルは、ローカルマシンを設定し、すべてのデータベースに適用されます。また、マシン上の Adabas バージョン 6.5 以上の、すべての製品のインストールと製品バージョンに適用されます。

コンフィグレーションファイルは ASCII ファイルなので、標準のテキストエディタで編集できます。これらのファイルへのアクセスを制限する必要があります。セクション「*セキュリティの考慮事項*」を参照してください。ここでは、データベースのセキュリティ保護（「強化」）方法について説明しています。

コンフィグレーションファイルの場所は、プラットフォームによって異なります。詳細については、*拡張オペレーション*のドキュメントの「*Adabas ユーティリティの承認のコンフィグレーション*」を参照してください。

## 認可のコンフィグレーション

*adaauth.ini* コンフィグレーションファイルに含まれる情報は、そのマシンとすべてのデータベース、およびマシン上のバージョン 6.5 以上のすべての製品のインストールと製品バージョンに適用されます。

| セクション | 項目 | 説明 |
|---|---|---|
| AUTHZ | AUDIT_FILE | 監査証跡コンフィグレーションファイルの場所 |
| | RBAC_FILE | セキュリティ定義の場所（MODE=INI） |
| | ACTION | Adabas ユーティリティの認可機能を有効にします |
| | MODE | セキュリティ定義のソースを定義します |

**注意:** 現時点では、このファイルによって、Adabas ユーティリティの認可機能の有効／無効が切り替えられます。デフォルト設定は "disabled" です（ACTION = NO）。この設定は、後続の製品バージョンで削除または変更される可能性があります。

このファイルの構文の詳細については、『*拡張オペレーション*』ドキュメントの「*adaauth.ini*」の説明を参照してください。

## 監査証跡のコンフィグレーション

*adaaudit.ini* コンフィグレーションファイルは、監査証跡のレイアウトと場所を定義します。

| セクション | 項目 | 説明 |
|---|---|---|
| AUDIT | LOG_FILE | 監査証跡ログファイルの場所 |
| | FORMAT | ログファイルエントリのレイアウトを決定します<br>■ TEXT（デフォルト）<br>■ CSV |
| | SEPARATOR | CSV レイアウトで使用される区切り文字 |

監査証跡ログファイルの要件は、次のとおりです。

- 監査エントリがログファイルに追加されます。
- そのため、Adabas ユーティリティのユーザーには、ログファイルへの WRITE アクセス権限が必要です。
- ログファイルのサイズを監視し、必要に応じてバックアップまたは移動する必要があります。

**注意:** Adabas ユーティリティの実行を許可されているすべてのユーザーは、LOG_FILE とそれが含まれているディレクトリの両方に対する READ/WRITE アクセス権限を持っている必要があります。

このファイルの構文の詳細については、『*拡張オペレーション*』ドキュメントの「*adaaudit.ini*」の説明を参照してください。

### パフォーマンスの考慮事項

この機能がシステム全体のパフォーマンスに与える影響は最小限に抑えられています。

## Adabas ユーティリティの承認（モード ADABAS）

*adaauth.ini* コンフィグレーションファイルで *MODE=ADABAS* が定義されている場合は、アクセス対象の Adabas データベースがセキュリティ定義のソースです。

- セキュリティ定義
- 初期状態
- 管理マニュアル

### セキュリティ定義

Adabas データベースには、セキュリティ定義を格納する RBAC システムファイルという固有のシステムファイルが含まれています。作成すると、初期定義の基本セットがロードされます。これらのセキュリティ定義は、アプリケーションのニーズに合わせて調整および拡張できます。

このモードの利点は、各認可要求がローカルで決定されることです。そのため、パフォーマンスへの影響は最小限に抑えられています。

このアプローチは、オフラインおよびオンラインでデータベースにアクセスするユーティリティの認可をサポートします。

### 初期状態

モード ADABAS では、初期セキュリティ定義により、すべての Adabas ユーティリティへの無制限アクセスが実装されます。

初期状態では、RBAC システムファイルによってユーザー *PUBLIC* と役割 *PUBLIC* が定義され、役割 *PUBLIC* がユーザー *PUBLIC* に割り当てられています。役割 *PUBLIC* には、すべての Adabas ユーティリティを実行する権限が付与されています。

セキュリティリポジトリにまだ認識されていないすべてのユーザーは、以前のバージョンの Adabas の場合と同様に、無制限にアクセスできるように、ユーザー *PUBLIC* として扱われます。

### 管理マニュアル

認可機能の設定と管理に必要なユーティリティは次のとおりです。

- ADADBM - RBAC システムファイルの作成
- ADAREP - RBAC システムファイルの問い合わせ
- ADARBA - RBAC システムファイルの管理

**ADADBM - RBAC** システムファイルの作成

ADADBM の RBAC_FILE 機能を使用して、RBAC システムファイルを作成します。

**注意:** RBAC_FILE 機能を使用するには、データベースがオフラインになっている必要があります。

**ADAREP - RBAC** システムファイルの問い合わせ

ADAREP の SUMMARY 機能を使用して、データベースシステムファイルを表示します。

**注意:** RBAC システムファイルは、RBAC ファイルが定義されている場合にのみ表示されます。ファイルがロードされていない場合は表示されません。

**ADARBA - RBAC** システムファイルの管理

ADARBA の機能は、セキュリティ定義の作成、読み取り、更新、削除に使用します。

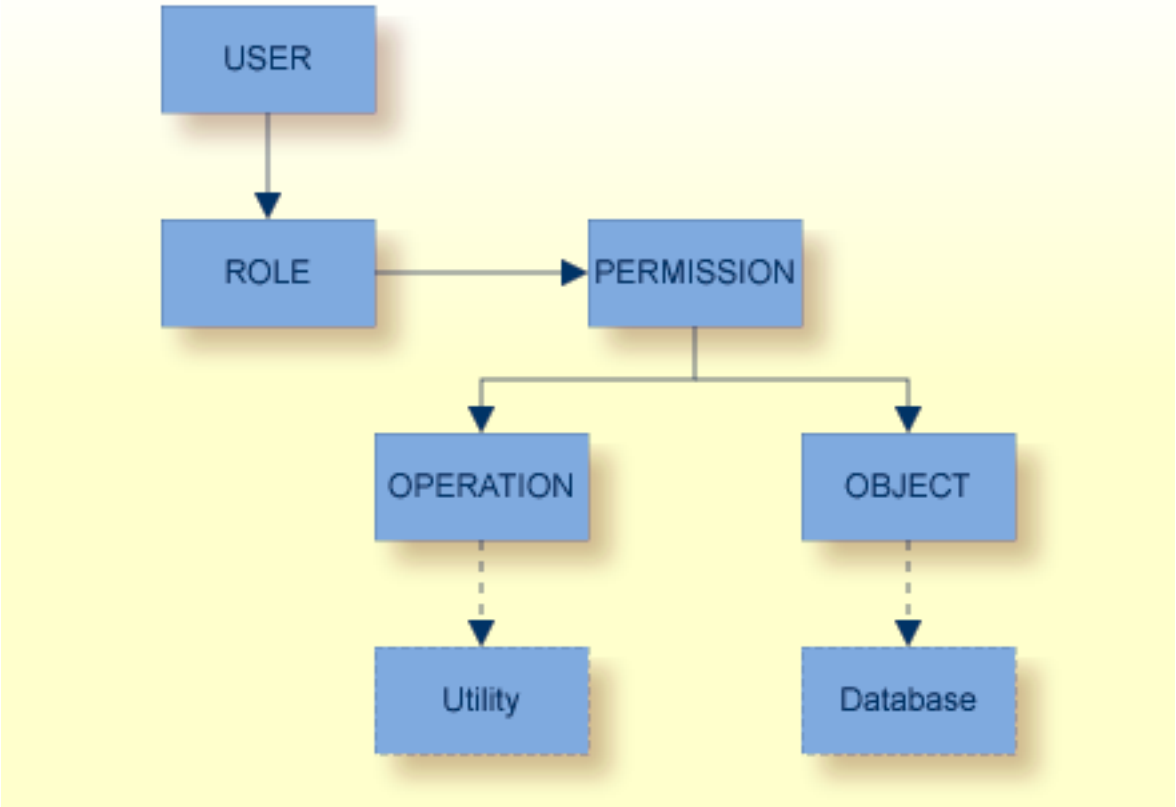
**注意:** ADARBA を使用するには、データベースがオンラインになっている必要があります。

## Adabas ユーティリティの認可（モード INI）

認可モード INI の場合、セキュリティ定義は、マシンおよびすべてのデータベースに適用されます。また、マシン上のバージョン 6.5 以上のすべての製品および製品バージョンに適用されます。

## セキュリティ定義

*adarbac.ini* コンフィグレーションファイルは、役割を定義し、1 つ以上のオブジェクトで一連の処理を実行する権限を割り当てます。ファイル内のエントリ間の関係について、概要を以下に示します。




| セクション | 項目 | 説明 |
|---|---|---|
| USER_ROLE | user_name | ユーザー／役割の割り当て |
| ROLE_PERMISSION | role_name | 役割／権限の割り当て |
| PERMISSIONS | permission_name | 処理／オブジェクトの割り当て |
| OBJECTS | object_name | データベース ID の割り当て |
| OPERATIONS | operation_name | ユーティリティの割り当て |

このファイルの構文の詳細については、『*拡張オペレーション*』ドキュメントの「*adarbac.ini*」の説明を参照してください。

# Adabas ユーティリティの認可の基礎

この*基礎編*では、次のトピックについて説明します。



## 前提条件

Adabas ユーティリティに認可を使用するには、セキュリティインフラストラクチャが必要です。初期のセキュリティコンフィグレーションがインストール時に設定され、この状態では監査証跡が事前設定され、認可はアクティブになっていません。

Adabas の認可では、ログイン資格情報が使用されます。これは、UNIX プラットフォームの場合はユーザー ID、Windows プラットフォームの場合はドメインとユーザー ID です。

Adabas ユーティリティ ADARBA は、RBAC セキュリティ定義の管理、ユーザーおよび役割定義の作成や削除、割り当ておよび特権の許可や取り消しに使用します。

## 構成

このセクションでは、Adabas RBAC システムファイルに格納されている RBAC セキュリティ定義を使用するように、Adabas ユーティリティの認可を設定する方法について説明します。

### 手順 3.1. Adabas ユーティリティの認可のコンフィグレーション方法

1 セキュリティコンフィグレーションファイル *adaauth.ini* のセクション [AUTHZ] で次のように設定します。

- ACTION=YES - Adabas の認可を有効にします
- MODE=ADABAS - 認可モード ADABAS を使用します

設定 RBAC_FILE は、このコンフィグレーションでは使用しません。

この基礎編の場合は、設定 AUDIT_FILE は未変更のままにできます。

2 デモデータベースを作成します。

```
crdemodb 100
```

3 データベース情報を問い合わせます。

```
adarep dbid=100 summary
```

まだ RBAC システムファイルが定義されていないので、MODE=ADABAS を設定した場合でも、この時点では Adabas ユーティリティ ADAREP の実行が許可されます。

4 RBAC システムファイルを作成し、初期セキュリティ定義を読み込みます。

```
adadbm db=100 rbac_file=<any_file_number>
```

RBAC システムファイルが定義され、初期定義がロードされたので、この時点で Adabas ユーティリティ ADAREP の実行が許可されます。

5 データベースを起動し、初期セキュリティ定義を表示します（RBAC定義の管理は、データベースがオンラインの場合にのみサポートされます）。

```
adarba db=100 list users
```

初期ユーザー *PUBLIC* が表示されます。

```
adarba db=100 list roles
```

初期役割 *PUBLIC* が表示されます。

```
adarba db=100 list assignments
```

初期割り当て *PUBLIC,PUBLIC* が表示されます。

デフォルトでは、ユーザー *PUBLIC* には役割 *PUBLIC* が付与され、ユーザー PUBLIC には役割 *PUBLIC* に付与されているすべての権限が割り当てられます。

## 認可

初期の RBAC セキュリティデータでは、ログインユーザー ID で、セキュリティが有効になっている Adabas ユーティリティの実行が許可されます。これは、RBAC システムに認識されていないユーザーは、デフォルトで役割 *PUBLIC* が付与されたユーザー *PUBLIC* として承認されることが理由です。

次の手順で、現在のログイン ID の権限を制限します。

### 手順 3.2. 現在のログイン ID の権限を制限する方法

1 新しいユーザーを作成します。

```
adarba db=100 create user=my-login-user
```

ここで、*my-login-user* は現在のユーザー ID です。

2 新しい役割を作成します。

```
adarba db=100 create role=newrole
```

3 新しいユーザーに新しい役割を付与します。

```
adarba db=100 grant assignment role=newrole user= my-login-user
```

4 割り当てを確認します。

```
adarba db=100 list assignments
```

以下が表示されます。

- PUBLIC,PUBLIC（初期割り当て）
- PUBLIC,my-login-user（新しいユーザーのデフォルトの割り当て）
- newrole,my-login-user（新しい割り当て）

5 制限された権限を新しい役割に付与します。

```
adarba db=100 grant privilege action=ada.uti.rba  role=newrole
```

6 権限を確認します。

```
adarba db=100 list privileges
```

以下が表示されます。

- すべてのデフォルト権限
- ada.uti.rba,DBID.CURRENT,newrole

ユーザー *my-login-user* には *PUBLIC* と *newrole* の役割が割り当てられているので、以前のようにすべての処理を実行できます。

7 ユーザー *my-login-user* のアクセス権限を ADARBA に制限します。

```
adarba db=100 revoke assignment role=PUBLIC user= my-login-user
```

8 ADARBA 以外の Adabas ユーティリティを実行します。

```
adarep db=200 sum
```

これにより、「Security violation.Permission denied.（セキュリティ違反。権限が拒否されました。）」が返されます。

アクセス権限を調整またはリストアする場合も、必要に応じて、ADARBA でそれらを定義できます。例を示します。

```
adarba db=100 grant privilege action=ada.uti.rep  role=newrole
```

または

```
adarba db=100 grant assignment role=PUBLIC user= my-login-user
```

# 4 Adabas パスワードのセキュリティ（ADASCR）

# はじめに

Adabas データベースセキュリティユーティリティの ADASCR は Adabas ファイルに対するアクセスおよび更新を制御するための機能を提供しています。

Adabas は、データのアクセス／更新セキュリティの 2 つのクラスをサポートします。ファイル全体を基準にした読み込み／書き込み要求に対するユーザーを制限するクラスと、ファイル内の個々のレコードアクセスに対するユーザーを制限するクラスです。

## ファイルレベルの保護

Adabas ファイルは、ゼロより大きいファイル保護レベルが割り当てられた場合にセキュリティ保護されます。ファイル保護レベルはアクセス（読み込み）と更新に分けて割り当てます。

ユーザーは、ファイル保護レベルと同等かそれ以上の権限レベルのパスワードを入力すると、セキュリティ保護されたファイルに対するアクセス／更新が可能になります。保護レベルおよびパスワードの権限レベルは、セキュリティユーティリティ ADASCR を使用して割り当てます。

保護できるファイル番号は、ASSO1 コンテナファイルのブロックサイズによって制限されます。ブロックサイズが 2 KB の場合、1～2047 の範囲内のファイルだけを保護することができます（3 KB の場合、3071 が制限です）。

## レコードレベルのプロテクション（セキュリティバイバリュー）

セキュリティバイバリューは、ユーザーが、データレコードの 1 つ以上のフィールドの内容に合わせてデータアクセスや更新の制限を別々に定義できるように Adabas ファイル保護レベルセキュリティを拡張します。

セキュリティバイバリューの条件は ADASCR セキュリティユーティリティで定義します。各パスワードに 99 までの Adabas ファイルに対するバリュー条件を含むことができます。

レコードレベルのセキュリティは、セキュリティ保護されたファイルにだけ使用できます。

# ファイル保護レベル

Adabas ファイルは、ゼロより大きいアクセス保護レベルまたは更新保護レベルが割り当てられるとセキュリティ保護されます。

ファイル保護レベルの範囲は 0～15 で、15 が最大保護レベルです。保護レベル 0 は、このファイルに対するアクセス／更新がすべてのユーザーに可能であることを意味します。保護レベルが 15 の場合、このファイルに対するアクセスおよび更新はいかなるユーザーにも許可されません。

保護レベルが割り当てられていない Adabas ファイルには、すべてデフォルトの保護レベル 0 が割り当てられます。このようなファイルに対しては、すべてのユーザーによるアクセスおよび更新が可能です。

| ファイル | 保護レベル番号 | |
|---|---|---|
| | アクセス | Update |
| 10 | 7 | 11 |
| 11 | 2 | 2 |
| 12 | 4 | 4 |

## ユーザーパスワード

各 Adabas ファイルに対して、異なるアクセスレベルおよび更新レベルをパスワードごとに割り当てることができます。パスワードの権限レベルは、0～14 の範囲で割り当てることができます。

| パスワード | FILE 10 ACC/UPD | FILE 11 ACC/UPD | FILE 12 ACC/UPD |
|---|---|---|---|
| PASSWRD1 | 4/0 | 4/0 | 4/0 |
| PASSWRD2 | 2/2 | 2/2 | 2/2 |
| PASSWRD3 | 14/0 | 0/0 | 14/0 |
| PASSWRD4 | 14/14 | 14/14 | 14/14 |
| PASSWRD5 | 7/7 | 0/0 | 7/0 |

パスワードのアクセス／更新権限レベルがファイルのアクセス／更新レベルと同等かそれ以上の場合にパスワードは正しく機能し、目的のファイルに対するアクセス／更新が可能となります。

上記の例のファイル保護レベルおよびパスワード承認レベルを使用する場合、次のようになります。

- PASSWRD1 は、ファイル 11 またはファイル 12 のアクセスに使用できます。
- PASSWRD2 は、ファイル 11 のアクセス／更新に使用できます。
- PASSWRD3 および PASSWRD5 は、ファイル 10 またはファイル 12 のアクセスに使用できます。
- PASSWRD4 は、ファイル 10、ファイル 11、またはファイル 12 のアクセス／更新に使用できます。

# セキュリティバイバリュー条件

各Adabasファイルに対する別々のアクセスと更新の条件をパスワードごとに割り当てることができます。各バリュー条件はAdabasサーチバッファおよび関連するバリューバッファから構成されます。

サーチバッファとバリューバッファは、標準Adabas検索コマンド（非ディスクリプタフィールドおよびマルチプルバリューフィールドの使用を含む）と同じ方法で指定します。ただし、ソフトカップリング、サブディスクリプタ、スーパーディスクリプタ、ハイパーディスクリプタおよびフォネティックディスクリプタは、セキュリティバイバリュー検索条件ではサポートされません。

サーチバッファやバリューバッファの構文および指定の詳細については、『コマンドリファレンスマニュアル』の「Adabasの呼び出し」の「サーチバッファとバリューバッファ」を参照してください。

値のチェックは、Adabasコマンドによって、データストレージが読まれるとき、または更新されるときにだけ行われます。

次の表は、各種の Adabas コマンドに対してテストされる条件を示しています。

| Adabas コマンド | セキュリティバイバリューのチェックを実行 | |
|---|---|---|
| | テスト条件 | テストデータ |
| A1 | Update | ビフォーイメージ |
| E1 | Update | ビフォーイメージ |
| L1～L6 | アクセス | ビフォーイメージ |
| L9 | *（インデックスのアクセスだけで、値のチェックは行われない）* | |
| N1、N2 | Update | アフターイメージ |
| S1(*) | アクセス | ビフォーイメージ |

**注意:** * 有効なフォーマットバッファを持つ S1 コマンドは、ユーザー ISN 指定の L1 コマンドが後に続く S1 コマンドが発行されたときと同じ方法で処理されます。

要求したファイルの関連セキュリティレベルがゼロの場合、セキュリティバイバリュー条件は無効です。

# Adabas セキュリティ処理

ユーザーが入力したパスワード、およびファイルに対して定義されたファイル保護情報を使用して、Adabas は指定された Adabas ファイルへのアクセス／更新がユーザーに許可されているかどうかをチェックします。ファイルがセキュリティ保護されていない場合、Adabas は入力されたパスワードをすべて無視します。読み込みコマンドと更新コマンドに対する Adabas のセキュリティ処理について、次に説明します。

Adabas は、アクセスまたは更新対象のファイルがセキュリティ保護されているかどうかを判断します。セキュリティ保護されていない場合、セキュリティ処理は停止します。

## セキュリティレスポンスコード

処理対象のファイルがセキュリティ保護されている場合、Adabas は、指定されたパスワードがパスワードテーブル内で定義されているかどうかをチェックします。

パスワードが定義されていない、またはパスワードが指定されない場合、レスポンスコード 201 が返されます。

パスワードが定義されているが、処理対象のファイルに対して有効ではない場合、レスポンスコード 202 が返されます。

パスワードが処理対象のファイルに対して有効である場合、Adabas は、このパスワードに関連付けられている権限レベルとファイルのアクセスまたは更新保護レベルを照合します。レスポンスコード 200 は、パスワード承認レベルがファイルの保護レベルより低い場合に返されます。

承認レベルが充分であれば、現在のファイルに対してさらにセキュリティバイバリュー条件のチェックが、パスワードに対して行われます。指定されたパスワードに対して検索条件が定義された場合、発行された Adabas コマンドによって、データのビフォーイメージまたはアフターイメージでテストされます。セキュリティバイバリューのチェックが正常でない場合、レスポンスコード 200 を返します。正常であれば、最終的にユーザー要求は認められ、Adabas コマンドが処理されます。

次に、Adabas のセキュリティ処理で返されるレスポンスコードの一覧を示します。

**RESPONSE 200**

| | |
|---|---|
| 説明 | セキュリティ違反が検出されました。 |
| ユーザー対処 | 正しいパスワードを指定してください。 |

**RESPONSE 201**

| | |
|---|---|
| 説明 | 指定されたパスワードが見つかりませんでした。 |
| ユーザー対処 | 正しいパスワードを指定してください。 |

**RESPONSE 202**

| | |
|---|---|
| 説明 | ユーザーが権限のないファイルを使用しようとしました。 |
| ユーザー対処 | 正しいパスワードを指定してください。 |

ETロジックユーザーがレスポンスコード200～202を受け取った場合、トランザクションタイムリミット（詳細については『ユーティリティマニュアル』のADANUCのTTパラメータに関する記載箇所を参照）を超えたときと同じように処理を継続します。

セキュリティバイバリューによりセキュリティ違反が発生すると、レスポンスコード200が返されます。

# 5 暗号化

⚠ **重要:** 暗号化機能の実装は、メインフレーム用の Adabas で使用できるものとは異なります。UNIX および Windows の Adabas のサイファコードは静的で、アディション 4 では提供されていません。

UNIX および Windows 用の Adabas での暗号化の目的は、Adabas コンテナファイル（ファイルダンプ、エディタなど）の不正な分析を防止することです。

メインフレームでの暗号化とは異なり、データへの不正アクセスを禁止しません。データベースユーティリティとデータベースアプリケーションのどちらも、サイファコードなしでデータにアクセスできます。

Adabas は、コンテナファイルに格納するデータを暗号化できます。しかし、これはデータストレージに格納されるデータレコードにだけ当てはまり、アソシエータ上のインバーテッドリストに格納されている値には当てはまりません。

暗号化しておけば、Adabas コンテナファイルの内容を権限のないユーザーに見られる心配がなくなります。暗号化が有効であれば（下記参照）、データレコードは Adabas ニュークリアスまたは一括更新ユーティリティ ADAMUP のいずれかを使用してデータベースに格納されるときに暗号化されます。データレコードは、ユーザーまたはアプリケーションから要求されたときに解読されます。つまり、暗号化はユーザーやアプリケーションに対して完全に透過的です。

個々の Adabas ファイルに対して暗号化できます。これを行うには、ADAFDU を使用してファイルを定義するときに `CIPHER/NOCIPHER` オプションを指定します。暗号化プロセスは、セキュリティを最大レベルにするために内部パラメータを使用します。システムによっては、同じ内容のフィールドやレコードがあると、セキュリティ上のリスクが発生することがあります。これは、権限のないユーザーがどちらか一方を解読できる場合、もう一方も解読できることになるからです。しかし、Adabas の暗号化プロセスでは、同一フィールドやレコードは次のように扱われます。

- 1 レコード内の 2 つの同一フィールドは異なるように暗号化されます。
- 1 つの Adabas ファイル内の 2 つの同一レコードは異なるように暗号化されます。

- 同一内容の 2 つの Adabas ファイルは異なるように暗号化されます。

次の例は 1 レコードに 'TEST' という値を含む 2 つのフィールドがある場合を示しています（表示は 16 進）。

```
Record 1  Unciphered=0x54455354  Ciphered=0xDD022537
Record 2  Unciphered=0x54455354  Ciphered=0x55EF0A51
```

**注意:** 上記の暗号化の値はただの例です。実際の暗号化メカニズムを使用して表示されたものではありません。

Adabas の暗号化メカニズムには次の特徴と制限があります。

- システムファイル（チェックポイントファイルおよびセキュリティファイル）は暗号化できません。
- ADAM キーファイルは暗号化できません。
- ユーティリティ ADACMP（圧縮）および ADAULD（アンロード）から作成された出力ファイルは暗号化しません。
- バックアップユーティリティ ADABCKから作成されたファイルに保存されたデータ、およびエクスポートユーティリティ ADAORD から作成された EXPORT ファイルは暗号化します。
- WORK ファイルおよび PLOG ファイルに書き出された再スタートレコードおよびリカバリレコードは暗号化します。
- レポートユーティリティ ADAREP の FILE 機能から作成された出力にはファイルの暗号化に関する情報が含まれます。

# 6 セキュリティの考慮事項

このセクションでは、データベースをセキュリティ保護（「強化」）するために実行が可能な、または実行が必要な手段またはアクションについて説明します。

## UNIX のグループ概念の使用

複数の Adabas ユーザーが異なる UNIX グループに属している場合、このグループに割り当たられたデータベースに Adabas アクセスを制限することができます。

**注意:** この機能は UNIX でのみ使用できます。Windows プラットフォームでは使用できません。

例：

Production と Test の 2 つの UNIX グループがあると仮定します。本番データベース以外のデータベースへのアクセスを許可しないユーザーが Production グループに属しています。また、テストデータベース以外のデータベースへのアクセスを許可しないユーザーが Test グループに属しています。データベースを起動する次の 2 人のユーザーがいると仮定します。

- dbaprod は、Production グループに属し、本番データベースを起動する必要があります。
- dbatest は、Test グループに属し、テストデータベースを起動する必要があります。

特定のデータベースを扱うグループのユーザーに Adabas のアクセスを制限するには、次の条件が必要です。

- Net-Work を使用しない場合でも、2 つの異なる NET_WORK_ID を使用する必要があります。Adabas は、Net-Work サーバーが後で起動されても検出できないため、Net-Work と共通な共有メモリセクションの GDT（グローバルデータベーステーブル）を作成します。GDT へのアクセス権限は、Adabas ニュークリアスが属しているグループに制限されます。したがって、ニュークリアスがアクセスする GDT が、別のグループに属している別のニュークリアスにより使用されている GDT と同じ場合、ニュークリアスの起動が失敗します。

  異なる NET_WORK_ID を使用してニュークリアスを起動すると、NET_WORK_ID ごとに個別の GDT が作成されるため、異なる GDT を使用できます。NET_WORK_ID は環境変数です。この環境変数は、Adabas ニュークリアスの起動時に設定する必要があります。最初の文字が同じ場合、2 つの NET_WORK_ID は同一とみなされます。環境変数 NET_WORK_ID を設定していない場合、空の NET_WORK_ID が使用されます。

  この例では、NET_WORK_ID を P に設定すると Production データベースを起動でき、NET_WORK_ID を T に設定すると Test データベースを起動できます。
- ニュークリアスは、パラメータを ADABAS_ACCESS=GROUP に設定して起動する必要があります。この例では、本番データベースには、ADABAS_ACCESS=GROUP を設定しますが、テストデータベースには ADABAS_ACCESS=ALL（または ADABAS_ACCESS パラメータなし）を設定すると仮定します。この場合、Production のユーザーのみが本番データベースにアクセスできますが、テストデータベースにはすべてのユーザーがアクセスできます。

**注意:** Net-Work を使用する場合は、異なるグループに対して異なる Net-Work サーバーを起動する必要があります。Net-Work 経由では、権限を持たないユーザーにデータベースへのアクセスを許可しないように注意する必要があります。

## コンフィグレーションファイルのセキュリティ保護

このセクションでは、Adabas ユーティリティの認可の設定に使用するコンフィグレーションファイルをセキュリティ保護する方法について説明します。

| ファイル | 説明 |
|---|---|
| adaauth.ini | Adabas ユーティリティの認可の設定 |
| adaaudit.ini | 監査証跡の構成 |
| adarbac.ini | 役割ベースのアクセス制御の定義 |

コンフィグレーションファイルをセキュリティ保護するには、以下を確認します。

- **READ-ACCESS**
  Adabas ユーティリティを実行するすべてのユーザーは、これらのファイルを読み込める必要があります。
- **WRITE-ACCESS**
  ファイルの管理者のみがファイルへの書き込みアクセス権限を持っている必要があります。

コンフィグレーションファイルの場所は、プラットフォームによって異なります。詳細については、*拡張オペレーション*のドキュメントの「*Adabas ユーティリティの承認のコンフィグレーション*」を参照してください。

## 監査証跡ログファイルのセキュリティ保護

このセクションでは、Adabas ユーティリティの認可で使用される監査証跡ログファイルをセキュリティ保護する方法について説明します。

| ファイル | 説明 |
|---|---|
| adaaudit.log | ユーティリティの認可の監査証跡ログファイル |

監査証跡ログファイルをセキュリティ保護するには、以下を確認してください。

- **READ/WRITE-ACCESS**
  Adabas ユーティリティを実行するすべてのユーザーは、監査証跡ログファイルに書き込める必要があります。

監査証跡ログファイの場所は、*adaaudit.ini* コンフィグレーションファイルで LOG_FILE オプションを使って設定します。詳細については、『*拡張オペレーション*』ドキュメントの「*Adabas* ユーティリティの*認可のコンフィグレーション*」を参照してください。

# 7 SSXLoginModule コンフィグレーションテンプレート

次のセクションに、SSXLoginModule のコンフィグレーションテンプレートを示します。これらは認可タイプ別に整理されています。

## 認証タイプ OS

認可タイプOSのセキュリティ定義は、ローカルオペレーティングシステムによって管理されます。

```
[SSX_CONFIGURATION]

# This is a sample properties file for the case
# when authType is OS and the user database is
# the local operating system -
# On Unix Systems it is using PAM authentication
# On Windows a local LogonUser()

# Specifies the authentication type.
# Is Required: Yes
# Valid values: {"OS", "TEXT", "LDAP", "ADSI"}
# Default Value: None

  authType=OS

# Specifies the explicit path of the privileged daemon process.
# Specify this parameter -
# if the sagssxauthd2 executable file is not in the current directory.
# Valid value is the valid path to the sagssxauthd2 module.
# Default Value: None
# Note: UNIX only.

##authDaemonPath

# Specify a default group name here to be returned
# with any of the group results that are returned by the repository manager.
# A valid value is any valid group name.
# Default Value: None
# Optional.

##defaultGroup

# If this parameter is specified, its value is used at authentication time
# when domain name is not specified by the user.
# If a domain name is specified, the value of this parameter is not used.
# A valid value is any valid domain name.
# Default Value: None
# Optional.

##defaultDomain
```

```
# Specifies how to access data.
# Valid values are:
# o true  - Access is under the account of the running process.
# o false - Access is under the impersonated user ID of the logged on user.
# Default Value: FALSE
# Note: Windows only.
# Optional.

##noImpersonation

# Specifies the local machine name (on which the user is authenticated).
# The machine name is added before users and groups;
# for example,machine_name\user.
# Valid values are:
# o true - If set to TRUE (and there is no domain field), you are authenticated ↩
against the local machine only.
# o false - You are authenticated on the domain that you logged on.
# Default Value: FALSE
# Optional.

##unixAddMachineName

# Specifies the log level.
# Is Required: No
# Valid values:
#    0 - No logging
#    Min: 1
#    Max: 6
# Default Value: None

##nativeLogLevel=0

# Specifies the log file.
# Is Required: No
# Valid values:
#    fully qualified file name
# Default Value: None

##nativeLogFile=SAGSSXCLIENTA_SSX.LOG

[SSX_CONFIGURATION-END]
```

# 認可タイプ TEXT

認可タイプ TEXT のセキュリティ定義は、テキストファイルに格納されます。定義は、データベース固有にすることも、複数のデータベースで共有することもできます。

```
[SSX_CONFIGURATION]

# This is a sample properties file for the case
# when authType is TEXT and the user database is
# an SAG Internal User Repository
# created by the ssxtxtpasswd utility

# Specifies the authentication type.
# Is Required: Yes
# Valid values: {"OS", "TEXT", "LDAP", "ADSI"}
# Default Value: None

  authType=TEXT

# Specifies the internal repository file
# which has been created with ssxtxtpasswd utility
# Is Required: No
# Valid values:
#   fully qualified file name
# Default Value: None

  internalRepository=<fullpath>/<filename>.<ext>

# Specifies the log level.
# Is Required: No
# Valid values:
#    0 - No logging
#    Min: 1
#    Max: 6
# Default Value: None

##nativeLogLevel=0

#  Specifies the log file.
#  Is Required: No
#  Valid values:
#   fully qualified file name
#  No default value

##nativeLogFile=SAGSSXCLIENTA_SSX.LOG

[SSX_CONFIGURATION-END]
```

その他の例：

## 内部ユーザーリポジトリファイルの作成

ssxtxtpasswd ツールを使用して、内部ユーザーリポジトリファイルの作成や変更が可能です。

ssxtxtpasswd ツールを起動するには、コマンドプロンプトを使用します。ツールを起動する際に、ユーザー名とパスワードを入力します。これらは暗号化されて（SHA512 および Base64）、結果のテキストファイルに提供されます。このツールは、テキストファイルに新しいユーザー資格情報を追加したり、既存のユーザー資格情報を置き換えたりします。

**注意:** ユーザー名には、数字、アルファベット、および次の文字のみを使用できます：! ( ) - .? [ ] _ ~ .パスワードには、数字、アルファベット、および次の文字のみを使用できます：!"#$%&'()*+,-./:;<=>?[\]^_`{|}~

## 例：ssxtxtpasswd ツールの使用法

```
Tool to create or update an entry in the SSX text file based
user repository.

Usage: ssxtxtpasswd [-f filename] [-c] [-p password] [-d | -e] userId

Use "-c" to create a new file.
      Usually, the file should exist and user entries are
      replaced/added.

Use "-p" to provide the password on the command line instead
      via an extra prompt.

Use "-d" to remove the specified user entry from the text file.

Use "-e" to check, whether the userId is already stored in the text file.

Note: The password usually will be read via a non-echo command input.
      When no filename is specified, a default of "ssx_user" is assumed.
```

### 例：ユーザーとパスワードの追加

```
ssxtxtpasswd -f SAGInternalUserRepository.txt -c -p mypsw myuid

Hash: ↩
bOEOAPEEEJBKv+4zOELiYcFqY7qFhlLZz1ha7Ztf7j/drJHGy2MLOLXEu/kX7TD52Aj7XfwiZ+vpIl9DqRbVkA==
User entry for "myuid" successfully added
```

**SAGInternalUserRepository.txt** の内容

```
*
*
* SAG Internal User Repository
*
version:3.0
*
user:myuid:$6a$bOEOAPEEEJBKv+4zOELiYcFqY7qFhlLZz1ha7Ztf7j/drJHGy2MLOLXEu/kX7TD52Aj7XfwiZ+vpIl9DqRbVkA==
```

## 認可タイプ LDAP

```
[SSX_CONFIGURATION]

# This is a sample properties file for the case
# when authType is LDAP and the user database is OpenLDAP

# Specifies the authentication type.
# Is Required: Yes
# Valid values: {"OS", "TEXT", "LDAP", "ADSI"}
# Default Value: None

  authType=LDAP

# Specifies which server type will be used.
# Is Required: No
# Valid values: {"ActiveDirectory", "SunOneDirectory", "OpenLdap"}
# Default value: "OpenLdap"

  serverType=OpenLDAP

# Property name that denotes a user entry.
# Is Required: No
# Valid values: (attribute name according to LDAP conventions)
# Default Value: None

  userIdField=cn

# Enumeration of LDAP objectclasses that the user entries use in
# the target LDAP server.
```

```
# Is Required: No
# Valid values: (Comma separated list of objectclass names,
#  according to LDAP conventions)
# Default value - depending on serverType:
#  OpenLdap:
#  "top,person"
#  SunOneDirectory:
#  "top,person,organizationalperson, inetorgperson"
#  ActiveDirectory:
#  "top,person,organizationalPerson,user"

  personObjClass=inetOrgPerson

# Enumeration of LDAP objectclasses that the group entries use in
# the target LDAP server.
# Is Required: No
# Valid values: (Comma separated list of objectclass names,
#  according to LDAP conventions)
# Default value - depending on serverType:
#    OpenLdap:
#    "top,groupOfUniqueNames"
#    SunOneDirectory:
#    "top,groupofuniquenames"
#    ActiveDirectory:
#    "top,group"

  groupObjClass=groupOfUniqueNames

# Property name that denotes a group entry.
# Is Required: No
# Valid values: (attribute name according to LDAP conventions)
# Default value: cn

  groupIdField=cn

# Property name of a user entry that points to the group that
# the user is member of.
# Is Required: No
# Valid values: (attribute name according to LDAP conventions)
# Default value:
#  depending on serverType:
#  OpenLdap:
#  "ou"
#  SunOneDirectory:
#  NULL
#  ActiveDirectory:
#  "memberOf"

  personGrpAttr=ou

# Property name of a group entry that points to users (members)
# Is Required: No
```

```
# Valid values: (attribute name according to LDAP conventions)
# Default value:
#  depending on serverType:
#  OpenLdap:
#  "uniqueMember"
#  SunOneDirectory:
#  "uniqueMember"
#  ActiveDirectory:
#  "member"

  groupPrsAttr=uniqueMember

# Seconds how long auth. user remains in cache.
# Is Required: No
# Valid values:
#  0 - No cache
#  Min: 1, Max: No limit
# Default value: 180

  cacheTime=12

# Specify the max. number of cached users that have been successfully
# authenticated. When the cache overflows, the oldest entry is removed.
# Is Required: No
# Valid values:
#  0 - No cache
#  Min: 1, Max: No limit
# Default value: 300

  cacheSize=4

# Time (in seconds) how long to ignore any further authentication
# requests for a particular User-Id.
# Is Required: No
# Valid values:
#  Min: 1, Max: No limit
# Default value: 100

  denyTime=4

# Number of invalid logon attempts.
# Is Required: No
# Valid values:
#  Min: 1, Max: No limit
# Default value: 3

  denyCount=3

# Specifies an output file for logging.
# Is Required: No
# Valid values: (Valid log file path)
# Default Value: None
```

```
  logCallback=true

# Specifies the log level.
# Is Required: No
# Valid values:
#    0 - No logging
#    Min: 1
#    Max: 6
# Default Value: None

##nativeLogLevel=0

#  Specifies the log file.
#  Is Required: No
#  Valid values:
#   fully qualified file name
#  No default value

##nativeLogFile=SAGSSXCLIENTA_SSX.LOG

# Default group to be automatically included for all requests
# that return any groups
# Is Required: No

##defaultGroup=DefGroup

# BaseBindDN where to find the users.
# Is Required: Yes
# and should contain the most detailed DN to find the users

#  personBindDn=ou=User,o=Org,dc=mycom,dc=com

# BaseBindDN where to find the groups.
# Is Required: Yes
# and should contain the most detailed DN to find the groups

##groupBindDn=ou=Groups,o=Org,dc=mycom,dc=com

# Attribute name of the password.
# Required when changeing the password
# Is Required: Not always
# Default value:
#  depending on serverType:
#  OpenLdap:
#  "userPassword"
#  SunOneDirectory:
#  "userPassword"
#  ActiveDirectory:
#  "unicodePwd"

##passwdField=userPassword
```

```
# Allow to pass a complete BaseBindDN
# via the domain parameter.
# Is Required: No
# Valid values: 0, 1

##allowdomainasbasebinddn=0

# Allow to specify which fields to search for as properties
# of a user entry
# Is Required: No
# Valid values: string, for example: "cn,sn,description"

##personPropAttr

# Allow to specify which fields to search for as properties
# of a group entry
# Is Required: No
# Valid values: string, for example: "cn,description"

##groupPropAttr

# Allow to use the special secure authentication using SASL,
# providing the directory supports this mechanism.
# Is Required: No
# Valid values: 0, 1 (default: 0)

##ldapSaslBind

# Allow to switch from a non-secure connection to a TLS connection,
# providing the directory supports this mechanism.
# of a group entry
# Is Required: No
# Valid values: 0, 1 (default: 0)

##ldapStartTls

# By default, the first "dc=" occurrence within the distinguished name
# name string denotes the domain name.
# If additional abbreviations want to be defined, one can use
# the following 2 parameter.
# Example:  Short="RnD;Admins;board"
#       with ↩
Long="ou=Rnd,ou=user,dc=mycom,dc=com;ou=Administrators,dc=mycom,dc=com;ou=VIP,dc=mycom,dc-com"

##ldapDomainShort
##ldapDomainLong

# If NOT the automatic domain name should be used to compose
# the canonical user id (SSXGetCanonicalUserId_A/W),
# specify this part of the ID here.
```

```
##canonicalDomainName

# Three algorithms are supported to find the groups of a user:
# "ru", recurse up: take the group pointer from the user entry
#                   and continue to search up for all groups
#                   found
# "rd", recurse down: search for all groups that have the
#                     user as member (no recursion)
# "cp", computed property: use a special field in the user
#                          entry to find all groups
#                          --> computedGroupProp retired
# Default: "ru"

##resolveGroups

# If resolveGroup is set to "cp", this parameter must provide
# the field name to look for in the user entry that denotes
# the user groups
# Default: None

##computedGroupProp=

# If the LDAP connection is protected by SSL/TLS, this
# parameter must be set.
# Valid Values: 0, 1
# Default: 0

##ldapSSLConnection=1

[SSX_CONFIGURATION-END]
```

## 認可タイプ ADSI

```
[SSX_CONFIGURATION]

# This is a sample properties file for the case
# when authType is ADSI and the user database is Active Directory

# Specifies the authentication type.
# Is Required: Yes
# Valid values: {"OS", "TEXT", "LDAP", "ADSI"}
# Default Value: None

  authType=ADSI

# Specifies the name of the AD Forest.
# Is Required: No, but should be specified
# Example: "dc=mycom,dc=com"
# (with a possible domain called "dc=eur,dc=mycom,dc=com")
```

```
# Default Value: None

##adsiForestDn

# Seconds how long auth. user remains in cache.
# Is Required: No
# Valid values:
#  0 - No cache
#  Min: 1, Max: No limit
# Default value: 180

  cacheTime=12

# Specify the max. number of cached users that have been successfully
# authenticated. When the cache overflows, the oldest entry is removed.
# Is Required: No
# Valid values:
#  0 - No cache
#  Min: 1, Max: No limit
# Default value: 300

  cacheSize=4

# Time (in seconds) how long to ignore any further authentication
# requests for a particular User-Id.

# Is Required: No
# Valid values:
#  Min: 1, Max: No limit
# Default value: 100

  denyTime=4

# Number of invalid logon attempts.
# Is Required: No
# Valid values:
#  Min: 1, Max: No limit
# Default value: 3

  denyCount=3

# Specifies an output file for logging.
# Is Required: No
# Valid values: (Valid log file path)
# Default Value: None
#   nativeLogFile=SIN_SSX.log

  logCallback=true

# Specifies the log level.
# Is Required: No
# Valid values:
```

```
#    0 - No logging
#    Min: 1
#    Max: 6
# Default Value: None

##nativeLogLevel=0

#  Specifies the log file.
#  Is Required: No
#  Valid values:
#   fully qualified file name
#  No default value

##nativeLogFile=SAGSSXCLIENTA_SSX.LOG

# In case the scope for the node to access users needs to be limited,
# one can specify a particular subtree:
# Example: "ou=user,ou=Rnd,dc=mycom,dc=com"

##adsiPersonBindDn

# In case the scope for the node to access groups needs to be limited,
# one can specify a particular subtree:
# Example: "ou=groups,ou=Rnd,dc=mycom,dc=com"

##adsiGroupBindDn

# By default, the first "dc=" occurrence within the distinguished name
# name string denotes the domain name.
# If additional abbreviations want to be defined, one can use
# the following 2 parameter.
# Example:  Short="RnD;Admins;board"
#       with   ↩
Dn="ou=Rnd,ou=user,dc=mycom,dc=com;ou=Administrators,dc=mycom,dc=com;ou=VIP,dc=mycom,dc-com"

##adsiDomainShort
##adsiDomainDn

# If NOT the automatic domain name should be used to compose
# the canonical user id (SSXGetCanonicalUserId_A/W),
# specify this part of the ID here.

##canonicalDomainName

# Three algorithms are supported to find the groups of a user:
# "ru", recurse up: take the group pointer from the user entry
#                   and continue to search up for all groups
#                   found
# "rd", recurse down: search for all groups that have the
#                     user as member (no recursion)
# "cp", computed property: use a special field in the user
#                          entry to find all groups
```

```
#                            --> computedGroupProp retired
# Default: "ru"

##resolveGroups

# If resolveGroup is set to "cp", this parameter must provide
# the field name to look for in the user entry that denotes
# the user groups
# Default: None

##computedGroupProp=

[SSX_CONFIGURATION-END]
```