Oracleホワイト・ペーパー
2011年12月

Oracle Database VaultによるDBA管理のベスト・プラクティス

ORACLE

はじめに 1
データベース管理タスクの概略 2
一般的なデータベース管理タスク 3
データベース初期化パラメータの管理 3
データベース・ジョブのスケジューリング 4
データベース・ユーザーの管理 5
ユーザーおよびロールの管理 6
Oracle Enterprise Managerによるユーザー管理 6
データベース・オブジェクトの作成および変更 7
データベースのバックアップおよびリカバリ 7
Oracle Data Pump 7
Oracle RMANを使用する場合のセキュリティに関するベスト・プラクティス 9
フラッシュバック表 10
データベース記憶域の構造の管理 10
データベース・レプリケーション 11
Oracle Data Guard 11
Oracle Streams 11
データベース・チューニング 11
EXPLAIN PLAN 11
ANALYZE TABLE 12
索引のメンテナンス 12
データベースへのパッチ適用とアップグレード 13
Oracle Enterprise Manager 14
Oracle Enterprise Managerへの管理者の追加 15
Oracle Database Vaultの管理 16
結論 19

はじめに

Oracle Database Vaultは強力なセキュリティ制御機能を提供することで、アプリケーションや機密データを保護します。また、特権ユーザーによるアプリケーション・データへのアクセスを防止し、非定型のデータベース変更を制限し、アプリケーション・データにアクセスできる手段、時、場所を制御します。さらに、既存のデータベース環境も透過的に保護されるため、コストと時間のかかるアプリケーション変更は不要です。

データへの攻撃の高度化と件数の増加に伴い、データベース内部のセキュリティ制御がこれまで以上に重要になっています。しかしながら、ほとんどの企業はデータベースを管理するDBAの数が少なく、データベースのセキュリティ管理専任の担当者を置く余裕はありません。データベースを統合し、運用効率を向上させれば、さらに少ない人数でもデータベースを管理できるようになります。Oracle Database Vaultの制御機能は柔軟で、DBAが1人しかいなくてもセキュリティを強化することができます。中規模以上のIT部門の場合は、アウトソーシングやオフショアリングに不可欠な保護をOracle Database Vaultの制御機能で適用し、アプリケーション・データへのアクセス権を持たない外部のDBAがデータベースを管理できるようにすることができます。

Oracle Applicationsおよび主要なパートナー・アプリケーションは、Oracle Database Vaultとの連携が保証されています。Oracle Database Vaultの保護機能を利用できるのは、Oracle E-Business Suite、Oracle PeopleSoft、Oracle Siebel、Oracle JD Edwards EnterpriseOne、Oracle Retail、およびOracle Financial Servicesです。また、SAPおよびInfosys FinacleでもOracle Database Vaultの保護機能を利用できます。認定製品に関する詳しい情報、およびカスタム・アプリケーションをOracle Database Vaultで保護する方法については、下に掲載したOracle Database VaultのWebページを参照してください。

本書では、Oracle Database VaultによるDBAのベスト・プラクティスを紹介します。説明するおもなトピックは、一般的なデータベース管理タスク、データベース・ユーザーの管理、データベースのバックアップとリカバリ、データベース・レプリケーション、データベース・チューニング、データベースへのパッチ適用とアップグレード、Oracle Enterprise Managerです。これらのトピックのそれぞれについて、Oracle Database VaultによるDBAのベスト・プラクティスとセキュリティに関する考慮事項を説明します。また、Oracle Database Vaultの管理について説明し、さまざまな企業の使用例を詳しく紹介します。

本書の読了後は、Oracle Database VaultによるOracle Databaseの管理方法が理解できているはずです。

本書は、Oracle Database Vaultの基礎知識を持つ読者を想定して書かれています。Oracle Database Vaultの概要については、次に示すOracle Database VaultのWebページを参照してください。

http://www.oracle.com/technetwork/jp/database/options/database-vault/index.html

データベース管理タスクの概略

次の表に、一般的なデータベース管理タスクをリストし、Oracle Database Vaultによる操作の制御が必要かどうかを示します。

管理タスク	Oracle Database Vaultによる操作の制御の要/不要	コメント
一般的なデータベース管理タスク		
データベースの起動と停止	不要	
データベースの作成	不要	
データベースのネットワーク接続性の構成	不要	
データベース・クローニング	不要	
データベース初期化パラメータの管理	必要	一部のパラメータはALTER SYSTEMのコマンド・ルールにより保護されます。
データベース・ジョブのスケジューリング	必要	このタスクには、適切なOracle Database Vault認可を付与する必要があります。
データベース・ユーザーの管理		
ユーザーおよびロールの管理	必要	本書の関連する項を参照してください。
データベース・オブジェクトの作成および変更	必要	本書の関連する項を参照してください。
データベースのバックアップおよびリカバリ		
Oracle Data Pump	必要	このタスクを実行する前に、適切なOracle Database Vault認可を付与する必要があります。
Oracle RMAN	不要	Oracle RMANのセキュリティに関するベスト・プラクティスは、本書の関連する項を参照してください。
Oracle SQL*Loader	不要	
フラッシュバック	必要	このタスクを実行する前に、適切なOracle Database Vault認可を付与する必要があります。
データベース記憶域の構造の管理	必要	Oracle Data Dictionaryレルムに対する認可が必要です。
データベース・レプリケーション		
Oracle Data Guard	必要	これについては、Support Note 754065.1に記載されている詳しい手順を参照してください。
Oracle Streams	必要	このタスクを実行する前に、適切なOracle Database Vault認可を付与する必要があります。

データベース・チューニング		
DBMS_STATS PL/SQLパッケージ	不要	
データベース・インスタンスのメモリの変更	不要	
自動データベース診断モニター（ADDM）	不要	
アクティブ・セッション履歴（ASH）	不要	
自動ワークロード・リポジトリ（AWR）	不要	
SQLチューニング・アドバイザ	不要	
EXPLAIN PLAN	必要	DBAがPLAN_TABLEにアクセスできる必要があります。
ANALYZE TABLE	必要	DBAがCHAINED_ROWS表にアクセスできる必要があります。
索引のメンテナンス	必要	本書の関連する項を参照してください。
データベースへのパッチ適用とアップグレード		
データベースへのパッチ適用の実行	必要	本書の関連する項を参照してください。
ソフトウェア・アップグレードの実行	不要	
データベース・アップグレードの実行	必要	本書の関連する項を参照してください。
Oracle Enterprise Manager		
Oracle Enterprise Managerの各種設定の構成	不要	
Oracle Enterprise Managerの管理者の追加	必要	本書の関連する項を参照してください。

表1：一般的なDBAアクティビティ概略（操作の制御が必要な場合はコメントを付記）

一般的なデータベース管理タスク

この項では、本書で扱う他の主要トピックに分類されない一般的なデータベース・タスクについて説明します。具体的には、データベース初期化パラメータの管理とデータベース・ジョブのスケジューリングについて、そしてこれらのタスクの実行に必要なOracle Database Vault制御機能について説明します。

データベース初期化パラメータの管理

一部のデータベース初期化パラメータは、ALTER SYSTEMのコマンド・ルールにより制御および保護されます。該当するパラメータは、『Oracle Database Vault管理者ガイド』の「デフォルトのルール・セット」の項の、“システム・パラメータのファイングレイン・コントロールを許可”というルール・セットの下に記載されています。DBAがこれらのパラメータを変更できるようにするには、次の要件を満たす必要があります。

1. DBAユーザーはALTER SYSTEM権限を持っている必要があります。

2. ルール・セット“システム・パラメータのファイングレイン・コントロールを許可”にDBAユーザーを追加する必要があります。これを行うには、ルール・セットを編集し、この操作を許可する新しいルールを追加します。下に示されているスクリーンの例では、“Verify user is allowed on ALTER SYSTEM”というルールを追加しています。このルールは、保護されている初期化パラメータの変更を許可する前に、セッション・ユーザーがDBA_JSMITHであることを確認します。ここで使用するルール式は、SYS_CONTEXT (‘USERENV’,’SESSION_USER’) =’DBA_JSMITH’です。

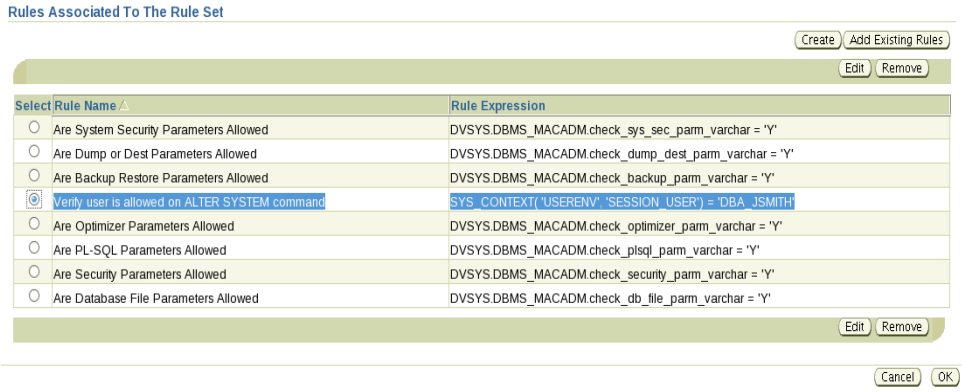

図1：ALTER SYSTEMコマンド・ルールを制御するルール・セットに追加されたルールの例

なお、保護されている初期化パラメータを自社環境内の複数のユーザーまたはロールで変更できるように、独自ルールを1つ以上追加することができます。

3. ルール・セットの評価オプションを“All True”から“Any True”に変更し、「OK」をクリックして変更内容を保存します。

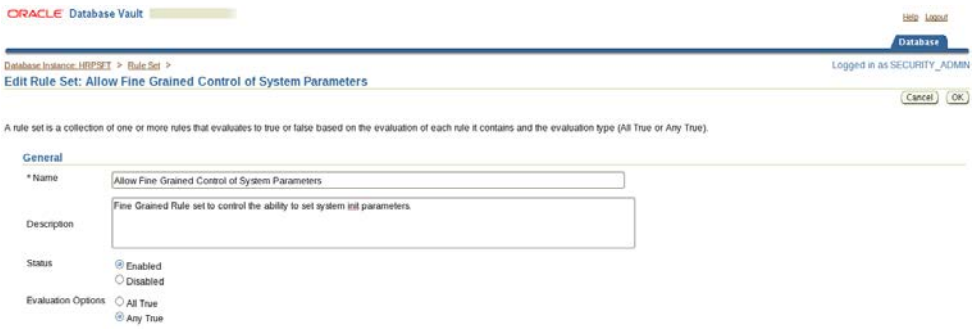

図2：ALTER SYSTEMコマンド・ルールのルール・セットの評価タイプを“Any True”に変更

これで、認可されたDBAは、保護されているものも含めたすべてのデータベース初期化パラメータを変更できます。

データベース・ジョブのスケジューリング

レルムで保護されているスキーマに対してデータベース・ジョブをスケジューリングする操作は、Oracle Database Vaultで制御する必要があります。これには、適切な認可が適用されていることを確認する目的があります。DBAには、スキーマごとにスキーマで、またはデータベース全体でデータベース・ジョブをスケジュールできる権限を付与できます。なお、DBAはこれまでと同様に、データベース・ジョブの実行に必要なCREATE JOB、CREATE ANY JOB、MANAGE SCHEDULERなどの適切なシステム権限も持っている必要があります。

次の例では、レルムで保護されているHRアプリケーションにデータベース・ジョブをスケジュールして実行できる権限をDBAに付与しています。

```
Authorizing DBA_JSMITH to schedule database jobs on the HR application
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('DBA_JSMITH','HR');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図3：レルムで保護されているHRアプリケーションにデータベース・ジョブをスケジュールできる権限をDBA_JSMITHに付与

次のスクリーンは、データベース全体にジョブをスケジュールできる権限をDBAに付与する方法を示しています。

```
Authorizing DBA_JSMITH to schedule database jobs on the entire database
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN>  EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('DBA_JSMITH');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図4：データベース全体にデータベース・ジョブをスケジュールできる権限をDBA_JSMITHに付与

DBAがデータベース全体またはレルムで保護されているスキーマに対してデータベース・ジョブを実行する必要がなくなった場合は、下のスクリーンに示している方法で権限を取り消すことができます。

```
Revoking authorization from DBA_JSIMITH to schedule database jobs on HR application
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('DBA_JSMITH','HR');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図5：DBA_JSMITHがHRアプリケーションにデータベース・ジョブをスケジュールできる権限の取消し

```
Revoking authorization from DBA_JSIMITH to schedule database jobs on the entire database
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('DBA_JSMITH');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図6：DBA_JSMITHがデータベース全体にデータベース・ジョブをスケジュールできる権限の取消し

データベース・ユーザーの管理

Oracle Database Vaultには、ユーザー管理タスクをデータベース・アカウント・マネージャー（DV_ACCTMGR）という別のロールに分離させるオプションがあります。その場合は、DBAがデータベース・ユーザーを作成または管理することがデフォルトではできなくなります。この目的は、非定型のアカウント作成をなくすこと、および監査不適合にならないようにすることです。

ユーザーおよびロールの管理

データベース・アカウント・マネージャーはDV_ACCTMGRロールが付与されているユーザーです。最初のデータベース・アカウント・マネージャーはOracle Database Vaultのインストール時に作成されます。ベスト・プラクティスに従い、専任のデータベース・アカウント・マネージャーを追加作成してDV_ACCTMGRロールを付与する必要があります。

データベース・アカウント・マネージャーができることは、ユーザーの新規作成、CONNECTロールの付与、既存ユーザーの管理、Oracle Databaseプロファイルの作成と管理です。なお、セキュリティ上の理由から、データベース・アカウント・マネージャーはOracle Database Vaultの管理者（セキュリティ管理者）のパスワードを変更できません。Oracle Database Vaultの管理者は各自のパスワードのみ変更できます。

ユーザーを作成したら、必要に応じて専任のシニアDBAアカウントでユーザーにシステム権限やロールを付与できます。シニアDBAとは、必要なシステム権限およびロールがADMIN OPTIONで付与されているDBAです。Oracle Database Vaultの制御機能を有効にしている場合は、シニアDBAをOracle Data DictionaryレルムのOWNERとして認可しておかなければ、シニアDBAは他のユーザーにシステム権限やロールを付与できません。

データベース・ロールはOracle Database Vaultのレルムで保護されている場合があります。そのため、付与する側は、該当するロールの管理オプションを持っているだけでなく、それらのロールを保護しているレルムのOWNERとして認可されている必要があります。なお、デフォルトのデータベース・ロールはOracle Data Dictionaryレルムで保護されています。

Oracle Database Vaultに関連するロールを付与できるのは、Oracle Database Vaultのインストール時に作成されたOracle Database Vault管理者のアカウントのみです。同様に、DV_ACCTMGRロールを付与できるのは、Oracle Database Vaultのインストール時に作成されたデータベース・アカウント・マネージャー・アカウントのみです。

Oracle Enterprise Managerによるユーザー管理

データベース・ユーザーは、Oracle Enterprise Managerから管理できます。Oracle Enterprise Managerには、データベース・アカウント・マネージャーのための使いやすいユーザー・インタフェースが用意されています。データベース・アカウント・マネージャーはOracle Database VaultのDV_ACCTMGRロールを持っている必要があります。また、シニアDBAはデータベース・アカウント・マネージャーにSELECT ANY DICTIONARY権限を付与する必要があります。この作業が完了したら、データベース・アカウント・マネージャーはOracle Enterprise Managerにログインできます。ログインするには、「Server」タブ、「Users」リンクの順にクリックします。これが、ユーザー管理スクリーンのある場所です。なお、データベース・アカウント・マネージャーはデータベース・ユーザーとプロファイルは管理できますが、システム権限は付与できません。

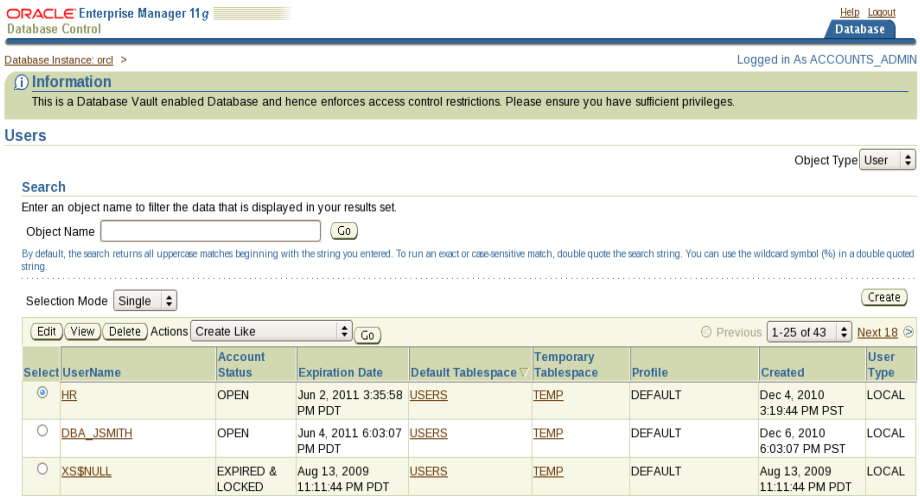

図7：データベース・アカウント・マネージャーがOracle Enterprise Managerからデータベース・ユーザーを管理

データベース・オブジェクトの作成および変更

適切なシステム権限を持つデータベース・ユーザーは、自分自身のスキーマでデータベース・オブジェクトの作成と変更ができます。ただし、ユーザーのスキーマがレルムで保護されている場合は、ユーザーがレルムの所有者として認可されている必要があります。認可されていれば、ユーザーは自分自身のオブジェクトに対してCREATE TABLEやTRUNCATE TABLEなどのデータ定義言語（DDL）SQL文を実行できます。なお、この場合はSELECTやUPDATEなどのデータ操作言語（DML）SQL文への影響はありません。

Oracle Database Vaultのコマンド・ルールも、データベース・ユーザーがデータベース・オブジェクトを作成または変更できるかどうかに影響を与える場合があります。たとえば、セキュリティの強化が必要な場合は、ユーザーがユーザー自身の表を切り捨てられないようにするコマンド・ルールを作成できます。Oracle Database Vaultのコマンド・ルールは、ほぼすべてのOracle Database SQLコマンドに適用できます。Oracle Database Vaultのインストール時にデフォルトのコマンド・ルールのセットが作成されます。これについては、『Oracle Database Vault管理者ガイド』を参照してください。

データベースのバックアップおよびリカバリ

この項では、Oracle Database Vaultを使用するOracle Databaseでのバックアップとリカバリについて説明します。取り上げるのは、Oracle Data Pumpと、Oracle Recovery Manager（Oracle RMAN）を使用する場合のセキュリティに関するベスト・プラクティスです。

Oracle Data Pump

Oracle Database VaultをOracle Databaseでの使用するOracle Data Pumpを使用する場合は、追加の操作制御が要求されます。そのため、権限を持つユーザー以外は非定型のデータ・エクスポートができなくなります。

たとえば、HRアプリケーションはレルムで保護されていますが、DBAは1つの表またはHRアプリケーション全体をエクスポートする必要があるとします。この場合は、Oracle Database Vaultによる操作の制御が要求され、DBAは特定の表またはHRアプリケーション全体をエクスポートできる権限を持っている必要があります。次の図は、Oracle Database Vaultの管理者（SECURITY_ADMIN）がDBA_JSMITHにHR.EMPLOYEES表のエクスポート権限を付与する様子を示しています。

```
Security Administrator authorizes DBA_JSMITH to do Data Pump export of HR schema
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DBA_JSMITH','HR','EMPLOYEES');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図8：HR.EMPLOYEESでOracle Data Pumpエクスポートを実行できる権限をDBA_JSMITHに付与

HRアプリケーション全体をエクスポートできる権限をDBAに付与することができます。

```
Security Administrator authorizes DBA_JSMITH to do Data Pump export of HR schema
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DBA_JSMITH','HR');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図9：HR全体に対してOracle Data Pumpエクスポートを実行できる権限をDBA_JSMITHに付与

注：DBAがOracle Data Pumpを使用できるためには、これまでと同様にEXP_FULL_DATABASEなどの適切な権限が必要です。詳しくは、『Oracle Databaseユーティリティ』マニュアルおよび『Oracle Database Vault管理者ガイド』を参照してください。

データベース全体をエクスポートできる権限をDBAに付与することができます。これには、Oracle Database VaultのスキーマDVSYSとDVFが含まれる場合があります。その場合は、エクスポートを実行できる権限とDV_OWNERロールをDBAに付与する必要があります。下の図は、データベース全体をエクスポートできる権限をDBAに付与する方法を示しています。

```
Security Administrator authorizes DBA_JSMITH to export the entire database
File  Edit  View  Terminal  Tabs  Help
SQL> GRANT DV_OWNER TO DBA_JSMITH;

Grant succeeded.

SQL>
SQL> EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DBA_JSMITH');

PL/SQL procedure successfully completed.

SQL>
```

図10：データベース全体に対してOracle Data Pumpを実行できる権限をDBA_JSMITHに付与

DBAがOracle Data Pumpエクスポートの操作を終了したら、Oracle Database Vaultの管理者は次に示す方法で権限を取り消すことができます。

```
Security Administrator un-authorizes DBA_JSMITH to do Data Pump export of HR schema
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN>  EXECUTE DVSYS.DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('dba_jsmith','hr','employees');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図11：DBA_JSMITHがHR.EMPLOYEESに対してOracle Data Pumpエクスポートを実行できる権限の取消し

```
Security Administrator un-authorizes DBA_JSMITH to do Data Pump export of HR schema
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN>  EXECUTE DVSYS.DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('DBA_JSMITH','HR');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

図12：DBA_JSMITHがHRに対してOracle Data Pumpエクスポートを実行できる権限の取消し

```
Security Administrator revokes authorization from  DBA_JSMITH to export the entire database
File  Edit  View  Terminal  Tabs  Help
SQL> REVOKE DV_OWNER FROM DBA_JSMITH;

Revoke succeeded.

SQL>
SQL> EXECUTE DVSYS.DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('DBA_JSMITH');

PL/SQL procedure successfully completed.

SQL>
```

図13：DBA_JSMITHがデータベース全体に対してOracle Data Pumpエクスポートを実行できる権限の取消し

ベスト・プラクティスに従い、Oracle Advanced Securityを使用してOracle Data Pumpエクスポートを暗号化することを推奨します。Oracle Data Pumpについて詳しくは、『Oracle Databaseユーティリティ』マニュアルを参照してください。

Oracle RMANを使用する場合のセキュリティに関するベスト・プラクティス

Oracle RMANを使用するDBAは、バックアップを実行できるオペレーティング・システム・アクセス権を持っていることと、データベースにSYSDBA権限でログインすることが必要です。セキュリティに関するベスト・プラクティスに従い、Oracle RMANを使用するDBA専用のオペレーティング・システム・アカウントを作成することを推奨します。そうすると、SYS AUDITによるDBA操作の監査が可能になります。また、DBAがOracleソフトウェア所有者アカウントでオペレーティング・システムにログインする必要性も減少します。次の図は、DBA_JSMITHがデータベースのバックアップを実行するためにSYSDBAとしてOracle RMANを使用してデータベースにログインした部分の監査レコードです。

```
dba_jsmith@dbsec-psft:/opt/oracle/admin/HRPSFT/adump
File  Edit  View  Terminal  Tabs  Help
Audit file /opt/oracle/admin/HRPSFT/adump/new_adump/hrpsft_ora_15114_1.aud
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Oracle Label Security and Oracle Database Vault options
ORACLE_HOME = /opt/oracle/product/11.2/db_1
System name:    Linux
Node name:      dbsec-psft.us.oracle.com
Release:        2.6.18-194.3.1.0.2.el5
Version:        #1 SMP Wed May 26 10:20:56 EDT 2010
Machine:        i686
Instance name: HRPSFT
Redo thread mounted by this instance: 1
Oracle process number: 30
Unix process pid: 15114, image: oracle@dbsec-psft.us.oracle.com (TNS V1-V3)

Mon Nov 22 11:20:12 2010 -08:00
LENGTH : '163'
ACTION :[7] 'CONNECT'
DATABASE USER:[1] '/'
PRIVILEGE :[6] 'SYSDBA'
CLIENT USER:[10] 'dba_jsmith'
CLIENT TERMINAL:[5] 'pts/1'
STATUS:[1] '0'
DBID:[9] '614176382'
```

図14：SYSDBAとしてOracle RMANを使用してデータベースにログインしたときのDBA_JSMITHの監査レコード

専用のオペレーティング・システム・アカウントを用意しておくと、DBAがOracle Database Vaultの保護を無効にすることができなくなるメリットもあります。

Oracle RMANを使用する場合のセキュリティに関するもう1つのベスト・プラクティスは、データベースのバックアップをOracle Advanced Securityで暗号化することです。Oracle RMANについて詳しくは、『Oracle Databaseバックアップおよびリカバリ・リファレンス』を参照してください。

フラッシュバック表

古いSCNやタイムスタンプへの表のフラッシュバックは通常どおりに実行できます。ただし、表がOracle Database Vaultのレルムで保護されている場合は、フラッシュバック操作を実行する間、レルムに対する権限をDBAに付与する必要があります。

また、削除した表をフラッシュバックするには、RECYCLEBINを有効にする必要があります。Oracle Database Vaultをインストールすると RECYCLEBINは無効化されます。なぜなら、レルムで保護されている表を削除すると、保護されていないゴミ箱に表が移動されてしまうためです。したがって、削除した表をフラッシュバックできるようRECYCLEBINを明示的に有効にしない限り、削除した表のフラッシュバックは実行できません。なお、これについては今後のリリースでの拡張が検討されています。

データベース記憶域の構造の管理

DBAがデータベース記憶域の構造を管理できるようにする場合は、通常、CREATE TABLESPACE、DROP TABLESPACE、ALTER TABLESPACEなどの権限をDBAに付与します。

Oracle Database Vault環境では、Oracle Data DictionaryレルムのPARTICIPANTまたはOWNERとしての権限もDBAに付与する必要があります。

データベース・レプリケーション

Oracle Database Vault環境では、何も変更しなくてもこれまでと同様にOracle Databaseクローニングを実行できます。ただし、データベースのクローンを作成する場所は常に、Oracle Database Vaultが有効化されているOracle Homeにする必要があります。これは、Oracle Database Vaultによる保護をクローン・データベース環境でも持続させるためです。その他のレプリケーション・アクティビティ（StreamsやData Guardなど）を実行する場合は、適切なOracle Database Vault認可をソース・データベース側で付与する必要があります。ターゲット・データベースに保護を持続させるには、ターゲット・データベースでもOracle Database Vaultを有効にしておく必要があります。

Oracle Data Guard

Oracle Data Guardには、Data Guard Logical Standby、Data Guard Physical Standby、Oracle Active Data Guardの3つのタイプがあります。Data Guard Physical StandbyとOracle Active Data Guardは、両方ともOracle Database Vaultのサポート対象です。Oracle Database Vaultを使用するOracle DatabaseでのOracle Data Guardの構成方法は、Support Note 754065.1に記載されている詳しい手順を参照してください。Oracle Data Guard Logical Standbyは、現在Oracle Database Vaultのサポート対象ではありません。

Oracle Data Guard Logical Standbyは、今後のリリースでサポート対象になる予定です。

Oracle Streams

Oracle Streamsでは、レルムで保護されているスキーマのデータをレプリケートできます。ただし、Oracle Database Vaultの制御機能を使用するには、Oracle Streamsを構成するDBAにDV_STREAMS_ADMINロールを付与する必要があります。こうすると、Oracle StreamsのプロセスをOracle Database Vaultを使用して厳密に管理できるようになりますが、DBAは通常どおりの方法でOracle Streamsを構成できます。

Security Administrator grants DV_STREAMS_ADMIN role to DBA_JSMITH to configuer Oracle Streams

File Edit View Terminal Tabs Help

```
SECURITY_ADMIN> GRANT DV_STREAMS_ADMIN TO DBA_JSMITH;

Grant succeeded.

SECURITY_ADMIN>
```

図15：DBAがOracle Streamsを構成できるようにするために、DV_STREAMS_ADMINロールを付与

データベース・チューニング

この項では、Oracle Databaseをチューニングにするときに DBAが使用するツールやテクニック（EXPLAIN PLANやANALYZE TABLEなど）の一部を紹介し、Oracle Database Vaultで要求される操作の制御について説明します。目標は、DBAによるデータベースのチューニングを許可する一方で、機密性の高いアプリケーション・データを保護することです。

EXPLAIN PLAN

レルムで保護されている表に対してDBAがEXPLAIN PLANを実行できるようにするには、DBAがINSERT権限およびSELECT権限を持っているスキーマにPLAN_TABLEを含める必要があります。下のスクリーンは、レルムで保護されている表に対してDBAが問題なくEXPLAIN PLANコマンドを実行できる様子を示しています。このケースでは、DBA_JSMITHスキーマにPLAN_TABLEを作成したため、DBA_JSMITHはPLAN_TABLEに対するINSERT権限とSELECT権限を持っています。

```
DBA_JSMITH running EXPLAIN PLAN on realm-protected table HR.EMPLOYEES
File  Edit  View  Terminal  Tabs  Help
DBA_JSMITH> run
  1  EXPLAIN PLAN
  2      SET STATEMENT_ID = 'Raise in Tokyo'
  3      INTO PLAN_TABLE
  4      FOR UPDATE HR.EMPLOYEES
  5          SET salary = salary * 1.10
  6          WHERE department_id =
  7             (SELECT department_id FROM HR.DEPARTMENTS
  8*                WHERE location_id = 1200)

Explained.

DBA_JSMITH>
```

図16：DBAはレルムで保護されている表に対して問題なくEXPLAIN PLANを実行

このケースでは、EXPLAIN PLANを実行するDBAにレルムへの権限を付与する必要はなく、したがってレルムで保護されているデータへのアクセス権も付与されません。

ANALYZE TABLE

レルムに対する権限が付与されていなくても、DBAはレルムで保護されている表に対してANALYZE TABLEコマンドを実行できます。ただし、DBAがLIST CHAINED ROWSを実行できるようにするには、DBAがINSERT権限とSELECT権限を持っているスキーマに表CHAINED_ROWSを作成する必要があります。下のスクリーンに示すとおり、DBA_JSMITHはANALYZE TABLEを実行し、CHAINED_ROWS表に連鎖行をリストしていますが、この表は自分のスキーマに自分で作成したものです。そのため、DBA_JSMITHはCHAINED_ROWS表に対するINSERT権限とSELECT権限を持っています。

```
DBA_JSMITH running ANALYZE TABLE  on realm-protected table HR.EMPLOYEES
File  Edit  View  Terminal  Tabs  Help
DBA_JSMITH> ANALYZE TABLE HR.EMPLOYEES
  2  LIST CHAINED ROWS
  3  INTO CHAINED_ROWS;

Table analyzed.

DBA_JSMITH>
```

図17：DBAはレルムで保護されている表に対して問題なくANALYZE TABLEを実行

このケースでは、ANALYZE TABLEを実行するDBAにレルムへの権限を付与する必要はなく、したがってレルムで保護されているデータへのアクセス権も付与されません。

索引のメンテナンス

レルムで保護されている表の索引をDBAがメンテナンスできるようにするには、すべての索引タイプ（Index、Index Partition、およびIndextype）用の独立したレルムを作成する必要があります。また、DBAをこのレルムのOWNERとして認可する必要があります。その実行例を次に示します。

この例では、HRスキーマ全体を保護する“HR Application Protection Realm”の他に、タイプがIndex、Index Partition、およびINDEXTYPEのすべてのHRオブジェクトを保護する“Index Maintenance Realm for HR Application”という2つ目のレルムを作成します。その後、DBA_JSMITHをこのレルムのOWNERとして認可します。

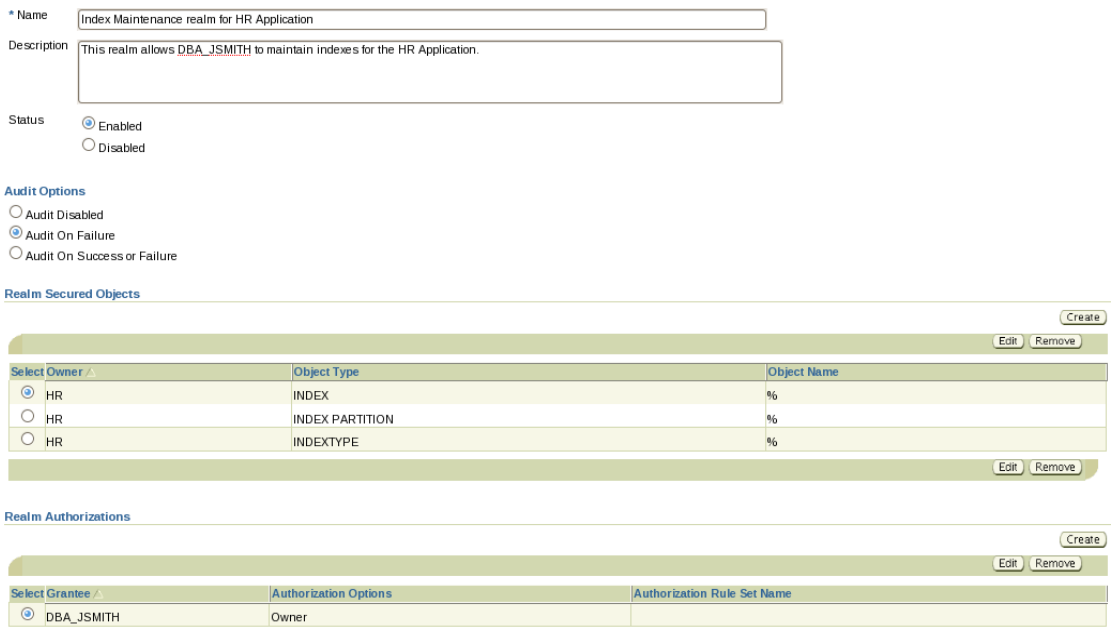

図18：索引は、DBAが索引のメンテナンス権限を持つ独自レルムに分離

下のスクリーンを見て分かるとおり、DBAは保護されている表の索引を再構築できます。

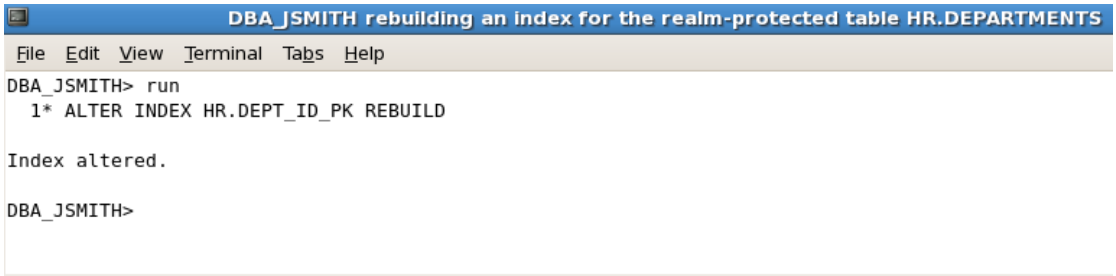

図19："Index Maintenance Realm for HR Application"に認可されているDBAは、HR索引を変更できます

こうすると、アプリケーション・データにアクセスさせずに、DBAに索引のメンテナンスを許可でき、索引をメンテナンスできる人の管理もできます。索引レルムに対する権限をデータベース・ロールに付与し、アプリケーション索引を管理することもできます。

データベースへのパッチ適用とアップグレード

Oracle Database Vaultの保護を無効にしなくても、DBAはデータベースにパッチを適用できます。ただし、あらかじめOracle Database VaultのロールDV_PATCH_ADMINをDBAに付与しておかなければ、データベースにパッチを適用できません。

図20：データベースにパッチを適用できるようにするために、DBA_JSMITHにDV_PATCH_ADMINロールを付与

DBAはSYSDBA権限を持つSYSとしてデータベースにログインしてデータベースにパッチを適用します。Oracle Database Vaultによる保護の効果は、データベースにパッチを適用している間継続します。

DBA_JSMITH can patch the database whithout having access to sensitive data

```
File  Edit  View  Terminal  Tabs  Help
[dba_jsmith@dbsec-psft ~]$ sqlplus DBA_JSMITH AS SYSDBA

SQL*Plus: Release 11.2.0.1.0 Production on Tue Nov 23 14:27:39 2010

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Oracle Label Security and Oracle Database Vault options

SYS> SELECT * FROM HR.EMPLOYEES;
SELECT * FROM HR.EMPLOYEES
                *
ERROR at line 1:
ORA-01031: insufficient privileges


SYS>
```

図21：DBAは、レルムで保護されているアプリケーション・データへのアクセス権なしでデータベースにパッチを適用できます

パッチの適用が完了したら、DV_PATCH_ADMINロールをDBAから取り消す必要があります。

Revoke DV_PATCH_ADMIN from DBA once patching is done

```
File  Edit  View  Terminal  Tabs  Help
SECURITY_ADMIN> REVOKE DV_PATCH_ADMIN FROM DBA_JSMITH;

Revoke succeeded.

SECURITY_ADMIN>
```

図22：データベースへのパッチ適用が完了した後、DV_PATCH_ADMINロールをDBAから取消し

Oracle E-Business Suiteのパッチは、Oracle Database Vaultの保護を無効にしなくても適用できます。E-Business Suite、およびOracle Database Vaultとの連動が保証されているその他のアプリケーションのパッチ適用について詳しくは、Oracle Supportサイトで関連するサーティフィケーション・ノートを参照してください。

ただし、データベースのアップグレードの場合は、アップグレードが終了するまでOracle Database Vaultによる保護を無効にする必要があります。アップグレード中は、データベース監査を使用してすべての保護対象データを監視することを推奨します。アップグレードが完了したら、Oracle Database Vaultによる保護を元の有効な状態に戻し、データベースの監視も通常どおりに戻すことができます。Oracle Databaseの今後のリリースでは、Oracle Database Vaultによる保護を無効にしなくてもデータベース・アップグレードができるようになる予定です。

Oracle Enterprise Manager

Oracle Enterprise Managerのタスクのほとんどは、Oracle Database Vaultによる制御が不要です。この項では、Oracle Enterprise Managerへの管理者の追加について説明します。

Oracle Enterprise Managerへの管理者の追加

Oracle Enterprise Manager Database Controlに管理者を追加する場合は、新しい管理者にSELECT_CATALOG_ROLEを付与することも必要です。このロールはOracle Data Dictionaryレルムで保護されているため、タスクを実行しているユーザーがこのレルムのOWNERとして認可されていなければエラーが発生します。下のスクリーンは、ユーザーSYSMANがDBA_JSMITHを管理者として追加しようとしてエラーが発生した様子を示しています。

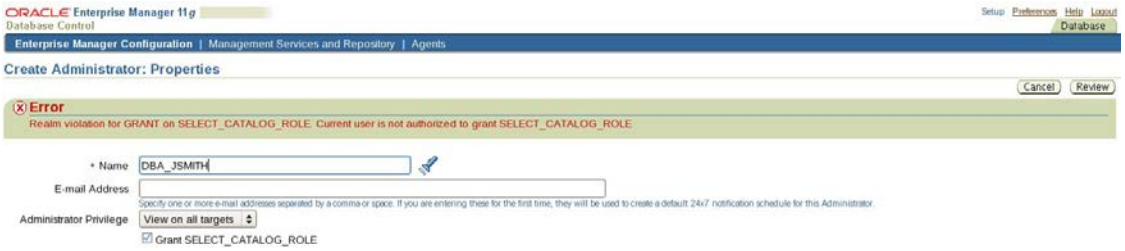

図23：SYSMANでDatabase Controlに管理者を追加しようとしたときのエラー

下のOracle Database Vault Administrationスクリーンでは、SYSMANをOracle Data DictionaryレルムのOWNERとして認可しています。

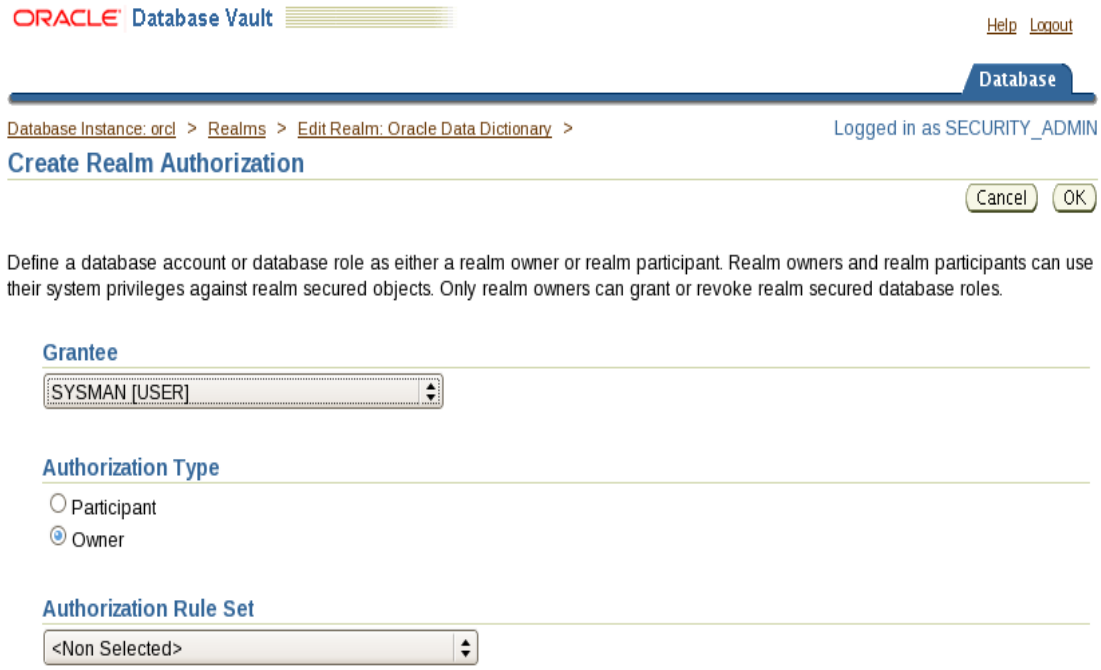

図24：SYSMANをOracle Data DictionaryレルムのOWNERとして追加

これで、SYSMANはOracle Enterprise Managerにログインして新しい管理者をOracle Enterprise ManagerのAdministratorsに追加できます。

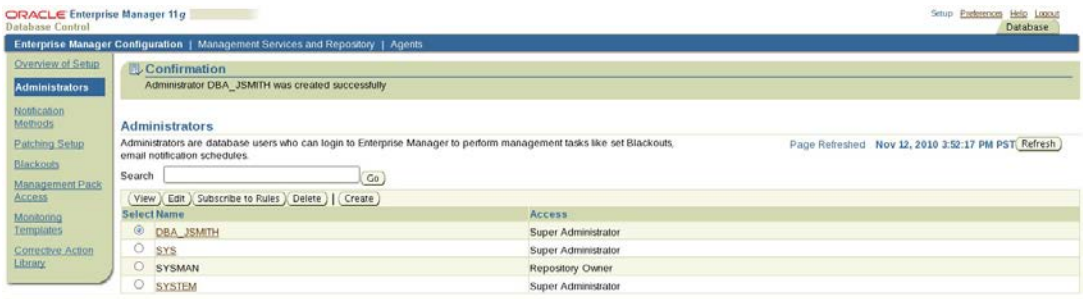

図25：SYSMANはDBA_JSMITHを管理者としてOracle Enterprise ManagerのAdministratorsに追加

Oracle Database Vaultの管理

データへの攻撃の高度化に伴い、データベースに対する操作の制御を強化する必要性がこれまで以上に増しています。ほとんどの企業が少人数のDBAでデータベースを管理している事実を考慮すると、データベース・セキュリティ関連タスクをそれぞれ専用のデータベース・アカウントに分けておくことが非常に重要です。データベースのセキュリティ管理に専用のデータベース・アカウントを作成することは、特権DBAアカウントによるアプリケーション・データへのアクセスの防止、非定型のデータベース変更の制限、アプリケーション・データにアクセスできる手段、時、場所の制御に役立ちます。Oracle Database Vaultを使用すれば、DBAが1人しかいない企業でもセキュリティを強化できます。

1. 特権ユーザーのアカウントを使用したハッカーによるアプリケーション・データの盗難を防止する
2. データベース構造に不正または有害な変更が加えられないように保護する
3. アプリケーション・データにアクセスできる手段、時、場所を制御する
4. 既存のデータベース環境のセキュリティを透過的かつアプリケーションの変更なしに保護する

この項では、Oracle Database Vaultの管理について、異なる企業シナリオに基づいて説明します。これらのシナリオは、さまざまな企業が、企業の規模やデータベースの管理を担当させられる人数に応じて、どのようにOracle Database VaultをIT業務に統合したのかを示しています。下のダイアグラムは一般的なIT部門のおもな職務の概要と、Oracle Database Vaultの管理およびガバナンスがIT全体の構造のどこに該当するかを示しています。

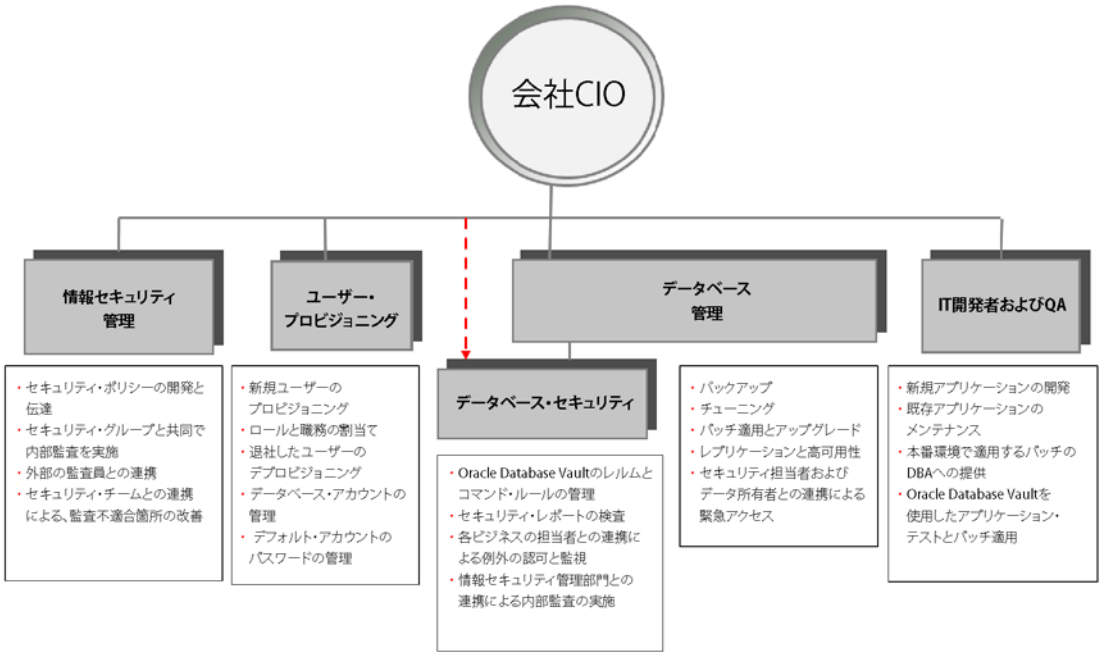

図26：ITのおもな職務をOracle Database Vaultの管理と統合

上のダイアグラムから分かるとおり、ITのおもな職務は情報セキュリティ管理、ユーザー・プロビジョニング、データベース管理、データベース・セキュリティ、開発とQAです。ほとんどの企業でIT部門の規模が小さいという事実を踏まえると、ITスタッフの大半は複数の職務を兼任していると考えられます。では、最初にこうしたITの職務を1つずつ見ていきましょう。

1. 情報セキュリティ管理
   - 会社全体の内部セキュリティ・ポリシーの開発と伝達
   - 内部セキュリティ・ポリシーおよび業界規則へのコンプライアンス確保を目的とした内部監査をセキュリティ担当と連携して定期的に実施
   - 外部の監査員との連携
   - セキュリティ担当との連携による、監査不適合箇所の改善
2. ユーザー・プロビジョニング
   - 新規ユーザーのプロビジョニング
   - 新規および既存ユーザーへのロールと職務の割当て
   - 退社したユーザーのデプロビジョニング
   - データベース・アカウントの管理
   - デフォルト・アカウントのパスワードの管理（Oracle Database Vaultのデフォルトのアカウント管理者およびセキュリティ管理者を含む）
3. データベース・セキュリティ
   - Oracle Database Vaultの管理：レルム、コマンド・ルール、およびファクタの作成と、それらの認可の管理
   - データベース・セキュリティ・レポートの検査

- 各ビジネスの担当者との連携による例外の認可と監視の有効化
- 情報セキュリティ管理部門との緊密な連携による内部監査の実施と監査不適合箇所の改善

4. データベース管理
   - データベース・バックアップ
   - データベース・チューニング
   - データベースへのパッチ適用とデータベース・アップグレード
   - データベース・レプリケーションと高可用性
   - セキュリティ担当者およびデータ所有者との緊密な連携による例外対処と緊急アクセスの取得
5. IT開発および品質保証（QA）
   - アプリケーションの開発とテスト
   - 既存アプリケーションのメンテナンス
   - 本番環境で適用するパッチのDBAへの提供
   - Oracle Database Vaultを使用したアプリケーション・テストとパッチ適用

では、IT部門の規模（小、中、大）が異なる3つの企業のシナリオを説明し、それぞれの企業でのOracle Database Vaultの管理方法を確認します。

セキュリティに関する手続きが進化しつつある小規模のIT部門の場合は、同じ人が異なる職務を兼任する必要がある可能性があります。たとえば、同じITスタッフがデータベースを管理しながら開発とQAも担当していたり、このスタッフがセキュリティの管理とデータベースの管理を同時に行っていたりする場合があります。その場合は、それぞれの職務に専用の独立したアカウントを作成することを推奨します。たとえば、John Smithがセキュリティの管理とデータベースの管理を同時に担当する必要がある場合は、異なるパスワードを設定した別々の2つのデータベース・アカウント（データベース管理用としてDBA_JSMITH、データベース・セキュリティ管理用としてSEC_ADMIN_JSMITH）をJohn Smithに付与する必要があります。彼専用のオペレーティング・システム・アカウントとは別に、これを行います。このようにしておくと、各アカウントによる操作を記録し、コンプライアンスや監査に役立てることができます。また、外部のハッカーに特権データベース・アカウントを巧みに乗っ取られた場合でも、アプリケーション・データへのアクセスを防止できます。

中規模のIT部門では、セキュリティの専任にできるのは少数のスタッフで、その場合も通常は複数の職務を兼任します。たとえば、セキュリティ担当者がユーザー・プロビジョニングも兼任している場合があります。DBAが開発やシステム管理をいくらか行っている場合や、開発者が開発やテストといった本来の職務の他にデータベース管理を行っている場合もあります。Oracle Database Vaultを使用すれば、特権データベース・アカウントを乗っ取ったハッカーによる攻撃から機密性の高いデータを保護できます。また、有害/不正な変更から本番環境を保護できます。

大規模なIT部門では、異なる職務に別々のスタッフを割り当てることができるため、先ほどのダイアグラムに示したおもな領域のそれぞれには専任スタッフが置かれます。この場合は、データベース・アカウントの管理がユーザー・プロビジョニングの一部となり、データベース・セキュリティ担当は情報セキュリティ担当およびDBAの両方と緊密に連携します。Oracle Database Vaultを使用すると、DBAがOracle Database内で実行できるアクティビティをデータベース・セキュリティ担当が管理できます。これは、アウトソーシングを行う局面で、社外のDBAに特権データベース・アカウントを付与する必要はあるものの機密性の高いデータへのアクセスは禁止する場合に特に効果的です。

結論

データへの攻撃の高度化と件数の増加に伴い、データベース内部の厳しいセキュリティ制御の実現がこれまで以上に重要になっています。Oracle Database Vaultには、アプリケーションや機密データを保護するための強力かつ柔軟なセキュリティ制御機能が用意されています。Oracle Database Vaultレルム、複数ファクタによる認可、およびコマンド・ルールを個別に、または組み合わせて使用することで、操作の制御が可能になり、データ侵害を防止できます。Oracle Database Vaultの制御機能を使用すれば、DBAが1人の企業でもセキュリティを強化できます。Oracle Database Vaultの制御は、IT組織やデータ・ガバナンス・モデルの進化に合わせ、新しいポリシーや手続きに合致するようにカスタマイズすることができます。Oracle Database Vaultのポリシーは、Oracle PeopleSoft、Oracle E-Business Suite、Oracle Siebel、SAPなど、オラクルおよびパートナーの主要なアプリケーションで使用できます。

ホワイト・ペーパー タイトル
2012年12月著者：Kamal Tbeileh

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

海外からのお問い合わせ窓口：
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2012, Oracle and/or its affiliates.All rights reserved.
本文書は情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社は本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクル社の書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはOracleおよびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

AMD、Opteron、AMDロゴおよびAMD Opteronロゴは、Advanced Micro Devicesの商標または登録商標です。IntelおよびIntel XeonはIntel Corporationの商標または登録商標です。すべてのSPARC商標はライセンスに基づいて使用されるSPARC International, Inc.の商標または登録商標です。UNIXはX/Open Company, Ltd.によってライセンス提供された登録商標です。0110

Hardware and Software, Engineered to Work Together