

ORACLE ENTERPRISE MANAGER 10^g DATA MASKING PACK

ORACLE DATA MASKING PACK

おもな機能

- マスキング・フォーマット
- ユーザー定義マスク・フォーマット
- マスキング定義
- 自動マスクや Related Column Mask を含むアプリケーションの参照整合性
- XMLによる外部化されたマスク・テンプレート
- マスキング前のデータ検証
- 最適化された高パフォーマンスのマスキング・プロセス

企業は常に、組織内および組織外でデータを共有しています。たとえば、社内開発者やオフショア・テスターがアプリケーション開発および実際のデータでアプリケーション・テストを実行できるようにするために、データベース管理者 (DBA) は、ステージング環境で使用可能な本番データのコピーを作成します。このデータ共有アプローチの問題は、多くの場合、本番データのコピーには、アクセスが政府規制によって制限されている企業の機密情報や個人情報が含まれている点です。Oracle Enterprise Manager Data Masking Pack は、内部および外部エンティティと本番データを共有するための包括的な使いやすいつソリューションを提供し、機密情報が不正者に開示されるのを防ぎます。

データ・マスキングと規制順守

本番データを保護し、非本番ユーザーに対する機密情報の漏洩を防ぐことは、データ・プライバシーを管理するさまざまな国際法規制により、あらゆる組織における急務となっています。2002年の米国サーベンス・オクスリー (SOX) 法や日本の金融商品取引法 (FIEL、または J-SOX) は、企業情報の社内管理に関する標準を強化しています。1996年の米国医療保険の相互運用性と説明責任に関する法律 (HIPAA) や EU のデータ保護条例は、個人に関する個人データのプライバシーを管理する国際法の一部です。クレジットカードの支払いプロセスも、クレジットカード情報の使用および共有に関して、クレジットカード業界 (PCI) の標準を採用しています。

組織は常に、機密情報や個人情報を本番データベースに保持しています。このような組織は、この情報の使用や共有を規則に従って保護しなければなりません。保護しなければ、このようなデータのプライバシー法違反に付随する罰金や罰則というリスクを負います。この罰金は、1日に何千ドルにもなる可能性があります。したがって、どのような組織もこのような法に違反したり、不正なデータ侵害が原因で悪い評判を得るリスクを冒したりする余裕はありません。

Oracle Data Masking Pack は、開発環境、テスト環境およびステージング環境で機密情報をマスキングすることによって、組織がプライバシーおよび機密保護法を順守できるように支援します。また、実行できないプロセスを逆に使用して、機密データをマスキング・ルールに基づいてスクラップされた本物に見えるデータに置き換え、オリジナル・データの検索、リカバリおよびリストアができないようにします。Oracle Data Masking Pack は、データをマスキングする一方で、アプリケーションの整合性の維持を支援します。

マスキング・フォーマット

組織は、機密情報や個人情報データベースのさまざまな列に保存しています。これらの情報は多岐に渡りますが、すべてがデータ・マスキングの対象となり得ます。今日では、これが組織にとってのおもな問題点となっています。多くの場合、DBA はおのおののデータベースに対して別個のスキプト・ベースのデータ・マスキング・ソリューションを実装することを選択しているためです。Oracle Data Masking Pack で共通のマスキング・フォーマットに関する定義を一元的に持つことで、企業はすべての本番データにデータ・プライバシー・ルールを一貫して適用できるため、確実な規制順守が可能になります。Oracle Data Masking Pack は、マスキング・フォーマットの使用によってさまざまなデータに対応できます。

Oracle Data Masking Pack は、乱数、ランダムな日付、定数などのさまざまな種類のデータに対して、標準のマスク・プリミティブを提供します。組織は、他の組み込みマスキング・ルーチンも使用でき、1 つの列の値を異なる行に入れ替えるシャッフリングなどを実行できます。これは、列の値の範囲を把握していないことが多い場合や同一の表の値のシャッフリングによって十分なプライバシー保護が提供される場合に有用です。マスキングされた値が現実的でありながらオリジナル・データに基づいていないことが必要な組織に対しては、Oracle Data Masking Pack は名前やアドレスなどのオリジナル・データを、外部のデータソースから抽出した架空の名前やアドレスを含むデータに置き換えることができます。

Select	Format	Data Type	Sample	Description	Owner
<input checked="" type="radio"/>	Constant value (in Simplified Chinese)	Character	格式名称	格式说明	SYSMAN
<input type="radio"/>	Anglo-American Last Names	Source Type	Adjani	Realistic but fictitious last names of US or UK origin	SYSMAN
<input type="radio"/>	US National Identifiers (SSN)	Character	111-39-9600	Random social security numbers for US employees	SYSMAN
<input type="radio"/>	Bay Area phone numbers	Character	(415) 555-0100	Dummy phone numbers based on area codes in the Bay Area	SYSMAN
<input type="radio"/>	Visa or Mastercard Credit Card Numbers	Character	5932521262645000	PCI-compliant dummy credit card numbers with checksum	SYSMAN

図 1：さまざまな機密データのマスキング・フォーマット

特殊なマスキング要件を持つ組織は、ユーザー定義のマスク・フォーマットをマスク・フォーマットの集合へ追加することもできます。PL/SQL を使用して定義されたこれらのユーザー定義のフォーマットは柔軟性を持ち、組織が展開するビジネスや業界セグメントに適切なマスク・フォーマットを制限なく作成できます。

情報セキュリティ管理者は、標準フォーマットとユーザー定義のフォーマットのさまざまなマスキング・フォーマットの組み合わせに基づいて複雑な複合マスクを作成できます。たとえば、一般的なクレジットカード番号に対するマスクは 4 または 5 で始まる一意の 16 桁の数字で定義でき、この数字に対してチェックサムが PCI 標準に準拠しているかが検証されます。

適切な企業プラクティスとして、組織は国別識別子や社会保障番号、クレジットカード番号などの通常にマスキングされた機密情報に対して標準マスク・フォーマットを定義し、データ・プライバシー保護プロセスのアプリケーションを統一することをお勧めします。

マスキング定義

今日の企業アプリケーションには、多くの場合、何千何百というデータベース・オブジェクトを含む非常に複雑なデータベース・スキーマがあります。管理者には、機密情報を含むすべての表および列を識別し、それらを適切なマスク・フォーマットへマッピングするという面倒で時間のかかるジョブがあります。Oracle Data Masking Pack は、組込み検索機能によってこのタスクを容易にします。組込み検索機能を使用すると、情報セキュリティ管理者は、データ・ディクショナリ全体に対して問合せを実行し、機密データを含む可能性のある表および列を識別できます。

Masking Definition: Employee mask					
A data masking definition specifies what columns to be masked and the format of masked data.					
Name	Employee mask	Database	Human Resources	Description	
Columns					
Owner	Table Name	Column Name	Format		
HR	EMPLOYEES	EMPLOYEE_ID	99		
Foreign Key Columns					
Owner	Table Name	Column Name	Parent Owner	Parent Table	Parent Column
HR	DEPARTMENTS	MANAGER_ID	HR	EMPLOYEES	EMPLOYEE_ID
HR	EMPLOYEES	MANAGER_ID	HR	EMPLOYEES	EMPLOYEE_ID
HR	JOB_HISTORY	EMPLOYEE_ID	HR	EMPLOYEES	EMPLOYEE_ID
OE	CUSTOMERS	ACCOUNT_MGR_ID	HR	EMPLOYEES	EMPLOYEE_ID
OE	ORDERS	SALES_REP_ID	HR	EMPLOYEES	EMPLOYEE_ID
Dependent Columns					
Owner	Table Name	Column Name	Parent Owner	Parent Table	Parent Column
HR	MANAGERS	MGR_ID	HR	EMPLOYEES	EMPLOYEE_ID

図 2：マスキング中のアプリケーション参照整合性の維持

マスキング用に列が選択されると、Oracle Data Masking Pack は、データ・ディクショナリに保持されている外部キー参照整合性の関係に基づいて、選択された表および列に関連するすべての列を自動的に識別します。これにより、確実にマスキング・ルールがプライマリ列に適用され、他の関連する表および列にもマスキング・ルールが自動的に適用されます。環境によっては、データの参照整合性がデータベースではなくアプリケーション・ロジック内で保持されると、Oracle Data Masking Pack によって、データベース管理者は Related Application Column 機能を使用して関連する表および列を追加できます。これにより、アプリケーションの参照整合性がデータベース内または他の場所で保持されている場合でも、アプリケーション・データの一貫性が維持されます。

マスキング定義または表および列のマスキング・フォーマットへのマッピングが完了すると、管理者やアプリケーション開発者は、Export Mask Definition 機能を使用することにより、この定義を Application Masking Template と呼ばれるポータブル XML フォーマットで保存できます。これにより、管理者は、オリジナルの定義が変更された場合でもマスキング定義をリストアできます。同様のアプリケーション・スキーマを持つデータベースを管理する別個の Oracle Enterprise Manager Grid Control がインストールされている場合、管理者はこれらのマスキング定義を迅速にインポートし、データをマスキングする準備ができます。マスキング・フォーマットが定義され、マスキング定義が完了すると、企業の管理者がマスキング・プロセスを続行する準備ができたことになります。

ORACLE DATA MASKING PACK

おもな利点：

データのプライバシー・ポリシーに準拠した本番データの共有の支援

あらゆる企業データに渡るマスキング・フォーマットの統一アプリケーションを提供

機密データの検出およびマスキングの自動化によるDBAの生産性の向上

関連製品とサービス

関連するOracle製品は次のとおりです。

- Oracle Provisioning Pack for Databases
- Oracle Change Management Pack for Databases
- Oracle Real Application Testing option
- Oracle Database Vault

マスキング・プロセス

マスキング・プロセスを開始する前に、Oracle Data Masking Pack は一連の検証手順を実行し、エラーが発生することなくデータ・マスキング・プロセスが順調に完了するようにします。実行するチェックには、マスキング・フォーマットの検証が含まれます。これは、選択されたマスキング・フォーマットがデータベースおよびアプリケーションの整合性の要件に一致するようにするためのデータ・マスキング・プロセスにおける必要な手順です。これらの要件には、一意性の制約によりマスキングされた列に対する一意の値の作成や、列長またはタイプの要件に一致する値の作成が含まれる場合があります。

Oracle Data Masking Pack では、マスキングされたデータを作成するための非常に効率的で堅牢なメカニズムが使用されています。バルク操作を実行し、オリジナル・データベースの制約、参照整合性、INDEX や PARTITION などの関連するアクセス構造、および GRANT などのアクセス許可を維持しながら、機密データを含む表をマスキングされたデータを含む同一の表へ迅速に置き換ええます。表の更新によってスピードが遅くなる従来のマスキング・プロセスと異なり、Oracle Data Masking Pack はデータベースの組込み最適化を利用してデータベースのロギングと実行の平行処理を無効にし、オリジナル表のマスキングされた置換を迅速に作成します。機密データを含むオリジナル表はデータベースから完全に削除され、アクセスができなくなります。

データベース管理者は、本番データベースがステージング環境にクローンされた直後にマスキング・プロセスが開始されるように、マスキング・プロセスを適切なメンテナンス・ウィンドウで柔軟にスケジューリングできます。高度なDBAには、Oracle Data Masking Pack は、DBA が組織のニーズに合わせてマスキング・プロセスをカスタマイズできるように、マスキング・プロセスをスクリプトとして保存するオプションを提供します。

結論

組織には、アプリケーション・テストなどのさまざまなビジネス目的のために、内部ユーザーおよび外部ユーザーと本番データを共有するニーズがあります。Oracle Data Masking Pack を使用すると、組織は内部およびビジネス・パートナーとセキュアに情報を共有でき、政府規制に準拠できます。情報セキュリティ管理者およびデータベース管理者は、手動のプロセスを排除することによって生産性を改善し、組織に対して情報セキュリティポリシーを一貫して適用できます。

Copyright 2007, Oracle. 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定し、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 は米国 Oracle Corporation 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。