

# ORACLE ENTERPRISE MANAGER 10<sup>g</sup> DATA MASKING PACK



## おもな機能と利点

Oracle Databaseアプリケーション用  
高性能マスキング・ソリューション

### おもな機能

- 標準で提供されるマスキング・フォーマット
- 包括的なマスキング定義
- 自動参照整合性
- 条件ベースのマスキング
- 複合マスキング
- 統合されたクローン・アンド・マスク
- マスキング前の検証
- マスキング操作を制御する高度なオプション
- 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、さまざまな事業目的のために、常に組織の内外でデータを共有してきました。こうした企業のデータベース管理者 (DBA) は、本番データをステージング環境またはテスト環境にコピーして、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アプリケーション・テストを実行できるようにしています。また、企業は、分析のために販売時点情報 (POS 情報) や治験データを研究者に提供しています。このデータ共有における問題は、多くの場合、政府の規制によってアクセスが制限されている企業の機密情報や慎重な扱いを要する情報、あるいは個人情報の本番データのコピーに含まれている点です。Oracle 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ソリューションを提供し、機密情報が不正に開示されるのを防ぎます。

### データ・マスキングと規制遵守

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従うことであり、あらゆる組織における急務となっています。医療情報のプライバシーからコーポレート・ガバナンスに至るまで、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、J-SOX) などの法律では、企業情報の社内管理に関する標準が強化されています。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) やデータ保護に関する EU 指令 95/46/EC は、個人データのプライバシーを管理する主要な国際法の一部です。クレジット・カードの支払いプロセッサであっても、クレジット・カード情報を処理および共有する場合は、クレジット・カード業界データ・セキュリティ標準 (PCIDSS) を採用する必要があります。

組織は常に、機密情報、個人情報、および慎重な扱いを要する情報を本番データベースに保持しています。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として罰金や罰則が発生してしまいます。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、どの組織もこれらの法に違反したり、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、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遵守できるように支援します。また、逆行できないプロセスを使用して、機密データをマスキング・ルールに基づいてスクラブリ、本物に見えるデータに置き換え、元データの検索やリカバリ、または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を維持するよう努めます。

### 一元管理されたマスキング・フォーマット

組織は、従業員名、顧客住所、またはクレジット・カード番号といった慎重な扱いを要する機密情報や個人情報を、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・マスキングの対象です。今日では、これが組織にとって大きな問題となっています。DBA は、企業データベースのそれぞれでデータをマスクするカスタム・スクリプトを作成して維持する必要があるからです。しかし、この方法には、データベースの数の急増に対応できるスケーラビリティがなく、監査人がスクリプトで提供されるマスキング・プロセスのセキュリティまたは信頼性を監査するための可視性もありません。Oracle Data Masking Pack のフォーマット・ライブラリによって提供される共通マスキング・フォーマットのための中央リポジトリを活用することで、企業はすべての機密データにデータ・プライバシ・ルールを一貫して適用できるため、確実な規制遵守が可能になります。

Oracle Data Masking Pack は、クレジット・カード番号、電話番号、国民識別番号（米国の社会保障番号、英国の国民保険番号）などの各種の機密データに対応するために、標準で提供されるマスキング・フォーマットとともに出荷されます。このマスキング・フォーマットは、マスク・プリミティブと呼ばれる構築ブロックを使用して構築されます。マスク・プリミティブの例としては、乱数、ランダムな桁数、ランダムな日付、定数があります。

Select Format	Data Type	Sample	Description
<input checked="" type="checkbox"/> American Express Credit Card Number	Character	3439864987100000	~10 billion unique American Express credit card numbers
<input type="checkbox"/> Discover Card Credit Card Number	Character	6011007000000000	~10 billion unique Discover Card credit card numbers
<input type="checkbox"/> MasterCard Credit Card Number	Character	5520000000000000	~10 billion unique MasterCard credit card numbers
<input type="checkbox"/> Visa Credit Card Number	Character	4029000000000000	~10 billion unique Visa credit card numbers
<input type="checkbox"/> Generic Credit Card Number	Character	3440000000000000	~10 billion unique generic credit card numbers
<input type="checkbox"/> Generic Credit Card Number Formatted	Character	6011 0244 0000 1020	~10 billion unique generic credit card numbers
<input type="checkbox"/> National Insurance Number Formatted	Character	EE TS 8T 03 D	Generate unique UK National Insurance Numbers
<input type="checkbox"/> Social Insurance Number	Character	672626269	~1 billion unique Canadian Social Insurance Numbers
<input type="checkbox"/> Social Insurance Number Formatted	Character	222-269-964	~1 billion unique Canadian Social Insurance Numbers
<input type="checkbox"/> Social Security Number	Character	000000000	~718 million unique US Social Security Numbers
<input type="checkbox"/> Social Security Number Formatted	Character	270-02-2130	~718 million unique US Social Security Numbers
<input type="checkbox"/> ISBN (Ten Digit)	Character	3445490000	~1 billion unique ISBN numbers
<input type="checkbox"/> ISBN (Ten Digit Formatted)	Character	3-38-494290-1	~1 billion unique ISBN numbers
<input type="checkbox"/> ISBN (Thirteen Digit)	Character	9798213300738	~2 billion unique ISBN numbers
<input type="checkbox"/> ISBN (Thirteen Digit Formatted)	Character	979-8-731406-33-9	~2 billion unique ISBN numbers
<input type="checkbox"/> UPC Number	Character	22580632600	~100 billion UPC numbers
<input type="checkbox"/> UPC Number Formatted	Character	5-28487-48700-9	~100 billion UPC numbers
<input type="checkbox"/> USA Phone Number	Character	300637050	~2.7 billion unique USA phone numbers
<input type="checkbox"/> USA Phone Number Formatted	Character	270-964-0820	~2.7 billion unique USA phone numbers
<input type="checkbox"/> Anglo American First Name	Source Type	Not Generated	Anglo American First Name
<input type="checkbox"/> Anglo American Last Name	Source Type	Not Generated	Anglo American Last Name

図 1: マスキング・フォーマット・ライブラリ

組織は、ほかの組込みマスキング・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元データに基づいていないことが必要な組織に対して、Data Masking Pack は、名前や住所などの元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住所といったデータに置き換えることができます。

組織が国民識別番号や社会保障番号、クレジット・カード番号などの一般的な機密情報に対し、フォーマット・ライブラリにある標準マスキング・フォーマットを維持および適用して、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という適切な企業プラクティスを、オラクルは推奨しています。

### ユーザー定義のマスキング・フォーマット

特殊なマスキング要件をもつ組織は、ユーザー定義のマスキング・フォーマットをマスキング・フォーマットの集合へ追加できます。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もっており、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キング・フォーマットを制限なく作成できます。たとえば、金融機関の多くでは、不正防止のために複雑なアルゴリズムを使用して口座番号を生成しています。ユーザー定義のマスキング・フォーマットを使用すると、これらの金融機関は、口座番号に組み込まれているセキュリティ標準に準拠した状態で、架空の口座番号を生成して元データと置き換えることができます。

### 確定的マスキング

一部の組織では、データベース内およびデータベース間で確定的マスキングと呼ばれる一貫したマスキングを提供することが必要とされます。たとえば、企業は、Siebel のカスタマ・リレーションシップ・マネジメント・アプリケーション、PeopleSoft の財務アプリケーション、およびカスタムのデータウェアハウスで顧客番号を保持することがあります。Oracle Data Masking Pack では、代替マスキング・フォーマットによって、確定的マスキングの標準サポートが提供されます。このマスキング・フォーマットを使用すると、企業は、テスト環境で各顧客番号に対して一貫性のあるマスキングをおこない、マスキングされた一意な値を確実に生成できます。これによって、元の機密データの機密性を確保しながら、テスト・データベース全体でデータ間のリレーションシップを維持することが可能になります。

### 移植可能なマスキング定義

今日のエンタープライズ・アプリケーションには、多くの場合、何百何千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と列を識別し、それらを適切なマスキング・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作業があります。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と列を識別できます。

マスキング用に列が選択されると、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、選択された表と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、プライマリ列に適用されるマスキング・ルールが、ほかの関連する表および列にも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、データベース管理者は Data Masking Pack の Related Application Column 機能を使用して、関連する表と列を追加できます。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アプリケーション内で維持されている場合でも、アプリケーション・データの一貫性が確保されます。

View Masking Definition: HR Masking Definition

General

Name: HR Masking Definition  
Database: pdb11gR1  
Description:

Columns

Owner	Table Name	Column Name	Column Group	Format
HR\$1	EMPLOYEES	EMPLOYEE_ID		###
HR\$1	EMPLOYEES	FIRST_NAME		###
HR\$1	EMPLOYEES	LAST_NAME		###
HR\$1	EMPLOYEES	PHONE_NUMBER		###
HR\$1	EMPLOYEES	SALARY		###

Foreign Key Columns

Owner	Table Name	Column Name	Parent Owner	Parent Table	Parent Column
HR\$1	DEPARTMENTS	MANAGER_ID	HR\$1	EMPLOYEES	EMPLOYEE_ID
HR\$1	EMPLOYEES	MANAGER_ID	HR\$1	EMPLOYEES	EMPLOYEE_ID
HR\$1	JOB_HISTORY	EMPLOYEE_ID	HR\$1	EMPLOYEES	EMPLOYEE_ID

Dependent Columns

Owner	Table Name	Column Name	Parent Owner	Parent Table	Parent Column
HR\$1	MANAGERS	MGR_ID	HR\$1	EMPLOYEES	EMPLOYEE_ID

Masking Jobs

Job Name	Status	Ended	Elapsed Time (seconds)
MASKING_JOB_146	Succeeded	Feb 1, 2008 7:45:22 PM (UTC-08:00)	56

Data Masking Options

Disable redo log generation during masking

Refresh statistics after masking

Drop temporary tables created during masking

Use parallel execution when possible

Parallel Degree: (Default Value)

図 2 : マスキング定義

データ・プライバシー規制のエンタープライズ・アプリケーションへの適用は、監査人からの法的要件およびビジネス・ユーザーからのアプリケーション要件を反映する複雑な作業になる可能性があります。Oracle Data Masking Pack では、次の 2 つの新しい機能により、これらのルールを簡単に定義して適用できます。

### 条件ベースのマスキング

Oracle Data Masking Pack では、特定の条件に合わせて表の列にある機密データに複数のマスキング・フォーマットを割り当てる機能が提供されます。たとえば、人事管理システム（HRMS）には、世界中の従業員に関するデータが格納されることがあります。ただし、ビジネス・ルールによっては、HRMS 内で各国のプライバシー保護法をその国にいる各従業員に対して実施することが要求される場合があります。Oracle Data Masking Pack を使用すると、企業は、従業員を雇用した国の国民識別番号に合わせて異なるマスキング・ルーチンを指定できるようになります。したがって、米国にいる従業員の国民識別番号は架空の一意な社会保障番号に置き換えられ、また英国にいる従業員の番号は架空の国民保険番号、カナダにいる従業員の番号は架空の社会保障番号に置き換えられます。

### 複合マスキング

特定の種類の機密データは、複数の関連データ要素にまたがっていることがよくあります。たとえば、顧客住所は番地、都市名、州名、郵便番号、国名で構成されています。エンタープライズ・アプリケーションでは、マスキングされた関連データ要素で整合性が維持されることを想定しています。つまり、マスキングされた住所を構成するデータ要素は、有効な住所であることが必要です。Oracle Data Masking Pack の複合マスキング機能では、関連データ要素を別の関連データ要素と一緒にグループとしてマスキングすることが可能になります。これにより、アプリケーション・ロジックの整合性が保証されます。

### Application Masking Template

マスキング定義または表と列のマスキング・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 Masking 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。これによって、管理者は、まったくデータ入力をせずに、事前定義されたアプリケーション・マスキング・テンプレートをデータベースに適用できます。また、マスキング定義が不適切に変更されてしまっている場合は、DBA が元のマスキング定義をリストアすることも可能です。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となります。

### マスクの検証と実行

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。実行するチェックの1つでは、マスキング・フォーマットが検証されます。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を満たす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を満たす値の作成が含まれる場合があります。

妥当性チェックが正常に完了すると、Oracle Data Masking Pack によって PL/SQL ベースのマスキング・スクリプトが生成されます。このスクリプトは、実行するためにターゲット・データベースに転送されます。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、元の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並列処理を無効にし、元の表のマスキングされた置換を迅速に作成します。機密データを含む元の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。

### セキュアなクローン・アンド・マスク・ワークフロー

現在、Oracle Data Masking Pack は、Oracle Enterprise Manager のデータベース・クローニング機能に統合されています。スタンドアロンのマスキング・プロセスに加えて、データベース・クローン・プロセスにデータ・マスキングを追加できる柔軟性が、データベース管理者に提供されるようになりました。これは、本番データベースをステージング環境に指定し、クローニング後に実行する必要があるマスキング定義を指定することで実現します。クローン・プロセスが完了すると、Oracle Data Masking Pack は、管理以外の目的でデータベースにアクセスすることを防止するために、クローン・データベースを RESTRICTED モードに移行し、マスキング・プロセスを実行します。そのあとでデータベースを開き、マスキング・プロセスが正常に完了することを検証する目的に限り、制限なしで使用できるようにします。

## 関連製品とサービス

### 主な利点

- 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 and Patch Automation Pack for Databases
- Oracle Change Management Pack for Databases
- Oracle Real Application Testing
- Oracle Application Testing Suite
- Oracle Database Vault

## 高度なマスキング・オプション

Oracle Data Masking Pack を使用することで、管理者はマスキング・プロセスをさらに制御できるようになり、またマスキング・プロセスの整合性を配置の前にテストし、検証できるようになります。以下のオプションがあります。

- **REDO ログの生成**: 特定のマスクを試してみたい一部の管理者の要望に応えて、Oracle Data Masking Pack ではマスキングの試験中に REDO ログを生成する機能がサポートされています。選択したマスキング・フォーマットで問題が発生した場合、管理者は Oracle データベースのフラッシュバック・テクノロジーを使用して、データベースをマスキング前の状態にリストアし、マスキング定義を修正してマスキングを再試行できます。
- **マッピング表**: ビジネス・ユーザーは、アプリケーション・データの整合性を検証するために、マスキングしたデータから元の機密データへ逆方向のマッピングができる必要があります。試験中に、管理者はマスキング・プロセスの間に生成されたマッピング表を保持するオプションを指定することで、マスキングされたデータの検証をビジネス・ユーザーに許可できます。
- **統計収集と並列度**: 大規模で複雑なデータベース環境をサポートするために、Oracle Data Masking Pack では、統計収集を無効にするオプション、またはマスキング・プロセスの並列度をカスタマイズするオプションが提供されます。これらのオプションによって、管理者はマスキング・プロセスを高速化できます。

コマンドラインをベースにした環境では、Oracle Data Masking Pack によって、外部スクリプトに PL/SQL ベースのマスキング・スクリプトを追加するオプションが提供されます。このマスキング・スクリプトは、DBA が組織のニーズに応じて独自のカスタム・クローン・アンド・マスク・プロセスを実行できるようにスケジューラから呼び出すことができます。

## 結論

組織では、アプリケーション・テストまたは製品研究や市場調査といった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の間で本番データを共有することへのニーズが高まっています。Oracle Data Masking Pack を使用することで、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、政府の規制に準拠できます。Oracle Data Masking Pack の強力で豊富な機能は、今日の複雑なエンタープライズ・アプリケーションをサポートするために設計されています。これによって、手動プロセスが排除されて管理者の生産性が大幅に向上し、組織全体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るようになります。



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

Copyright © 2009, 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、その内容に誤りがないことを保証するものではなく、また、口頭による明示的保証や法律による黙示的保証を含め、商品性ないし特定目的適合性に関する黙示的保証および条件などのいかなる保証および条件も提供するものではありません。オラクル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 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。0109