EU 一般データ保護規則（GDPR）への対応強化

Oracle Database Security製品の活用

Oracle ホワイト・ペーパー | 2017 年 1 月

著者：データベース・セキュリティ担当主席製品マネージャーDINESH RAJASEKHARAN

目次

免責事項：本書の目的は、企業が Oracle Database Security テクノロジーを活用して EU 一般データ保護規則の特定要件に準拠できるようにする方法の理解を助けることです。Oracle Database Security テクノロジーの中には企業の具体的な環境によっては、関連するものもあれば関連しない場合もあります。オラクルは、必ずユーザーの具体的な環境でセキュリティ・ソリューションを検証することで、確実に性能、可用性、整合性を維持することを推奨しています。

本書の情報は、いかなる法律、規制、規制ガイドラインの内容、解釈、適用に関する法的なアドバイスとして解釈および使用することはできません。顧客（将来の顧客を含む）は、自身で法的助言を求め、個人データの取り扱いに関して（いかなるベンダーの製品やサービスの利用も含めて）適用される可能性のあるあらゆる法律や規制を理解する必要があります。

概要

企業が、プロセスや人、技術的な制御の変更を考慮して新しい欧州連合（EU）の一般データ保護規則の準備をする上で、重要なのは、GDPR による評価、予防、検知の各制御機能の採用を推進するためにオラクル製品をどう役立てるかを検討することです。こうした使いやすいツールによって、GDPR で義務付けられた多くのデータ・セキュリティ原則の導入に関する管理の透明性が確保されます。

このホワイト・ペーパーでは、GDPR の基本的ないくつかの要件について概要を説明し、それを Oracle Data Security の諸機能にマッピングします。GDPR では多くのさまざまなデータ保護、ガバナンス原則、要件（EU 域外へのデータ転送など）が義務付けられていますが、このホワイト・ペーパーでは、主要な GDPR データ保護セキュリティ原則のうち Oracle Data Security の諸機能で対応できるものだけを取り上げます。

一般データ保護規則（GDPR）の概要

欧州連合（EU）がデータ保護標準を導入したのは 20 年前のデータ保護指令 95/46/EC によってでした。加盟国に対する指令では、国内法に導入するときの対応にある程度の柔軟性が許容されたため、ヨーロッパは結局さまざまなプライバシー法からなるつぎはぎの状態になりました。加えて、ここ 20 年にわたるセキュリティ侵害の増加や急速な技術開発、グローバリゼーションによって個人データの保護に関して新たな課題がもたらされました。こうした状況に対処する取り組みの中で、EU が開発したのが一般データ保護規則（GDPR）です。

GDPRの主要なセキュリティ目標

GDPR の主要なセキュリティ目標は以下のとおりです。

目標	説明
基本的な権利としてのデータ・プライバシーの確立	GDPR ではデータ保護は個人の基本的人権と見なされており、個人データの"保護に対する権利"もそのうちの 1 つです。EU に拠点を置くすべての企業または EU 在住者の個人データを扱うか対象とする企業はすべてプロセス、テクノロジー、自動化を取り入れて個人データを効果的に保護する必要があります。
EU 域内のデータ保護に関する責任の明確化	GDPR は、EU 域内に拠点を置く管理者または処理者、または EU 域内に拠点を置かないが、EU 域外から EU 域内のデータ主体に対して製品またはサービスを提供する、または EU 域内のデータ主体の行動を監視する企業に適用されます。
データ保護基準の定義	GDPR では断片化とあいまいさを避けることを目指し、データ保護の基準を設定するために、EU 在住者の個人データを扱うすべての企業に GDPR で策定された要件に従うことを求めています。
データ保護原則の詳述	GDPR では、暗号化は幅広いセキュリティ戦略の構成要素の 1 つにすぎないと考えており、企業に保有する個人データの機密性に基づいて、評価、予防、検知の各制御を検討することが義務付けられています。
執行力の強化	EU は GDPR の順守を徹底する狙いで、コンプライアンス違反に対して年間総売上の最大 4%という多額の罰金を科しています。

GDPRの核となる主体

GDPR では、さまざまな主体を定義してデータ保護の考えと関連する役割が説明されています。

主体	説明
データ主体	識別子によって直接的にまたは間接的に識別されうる者。識別子とは、たとえば、国民識別番号やクレジット・カード番号、ユーザー名、Web Cookie などです。
個人データ	データ主体に関する機密性の高い個人情報を含む、あらゆる個人情報。たとえば、住所、生年月日、氏名、所在地、国籍などです。
管理者	単独でまたは他と共同して、個人データの取扱いの目的および手段を決定する自然人、法人、公的機関、行政機関またはその他の団体。たとえば、管理者として組織や CIO が考えられます。
データ保護オフィサー	データ・プライバシー法と規格に関して幅広い知識を有する管理者または処理者の従業員。データ保護オフィサー（DPO）は管理者や処理者に GDPR に基づく義務を勧告し、その履行を監視するものとします。DPO は、管理者/処理者と監督機関との連絡係の役割を果たします。DPO としては、たとえば最高セキュリティ責任者（CSO）やセキュリティ管理者が挙げられます。
処理者	管理者のために個人データの取扱いを行う自然人、法人、行政機関またはその他の団体。たとえば、開発者やテスター、アナリストなど。処理者にはクラウド・サービス・プロバイダーや外部委託会社も含まれます。
取得者	個人データの開示を受ける自然人、法人、行政機関またはその他の団体。たとえば、個人、税務コンサルタント、保険代理店、行政機関など。
事業者	経済活動に従事している自然人または法人。公共部門か民間部門か、EU 域内か EU 域外かを問わず、基本的にすべての組織が含まれます。
第三者	データ主体、管理者、処理者および管理者または処理者の直接の職権下でデータを取り扱う権限を与えられている者以外の自然人、法人、行政機関またはその他の団体。たとえば、パートナー企業や下請業者など。
監督機関	加盟国によって設立された独立した公的機関（現行の EU データ保護指令に基づく国家データ保護機関）、または裁判所。

架空の事例

さまざまな主体とその役割、相互関係を理解するために、フランスを本拠とする架空の機器メーカーXYZ を検討することにしましょう。XYZ の顧客が同社のウェブ・ポータルを通してオンラインで発注するとします。多国籍ビジネス・モデルの一環として、XYZ は個人情報（"データ主体"）を保存し、取り扱っています。この EU を拠点とする企業は、個人データの取り扱いの目的および方法を決定します（管理者）。開発、テスト、顧客サービスと請求業務はブラジルとインドの外部下請業者（処理者）に外注され、現地の従業員は、たいてい顧客データ（"個人データ"）をローカル・システムにコピーして、それぞれ開発、テスト、処理を行っています。また、XYZ はさまざまな国の決済会社や配送会社（"第三者"）と提携しており、そのパートナー企業に個人データ（"個人データ"）を提供して注文を処理しています。独立した公的機関が、GDPR の適用を監視します（"監督機関"）。

次の図で、上記の各主体の地理的分布例を示します。

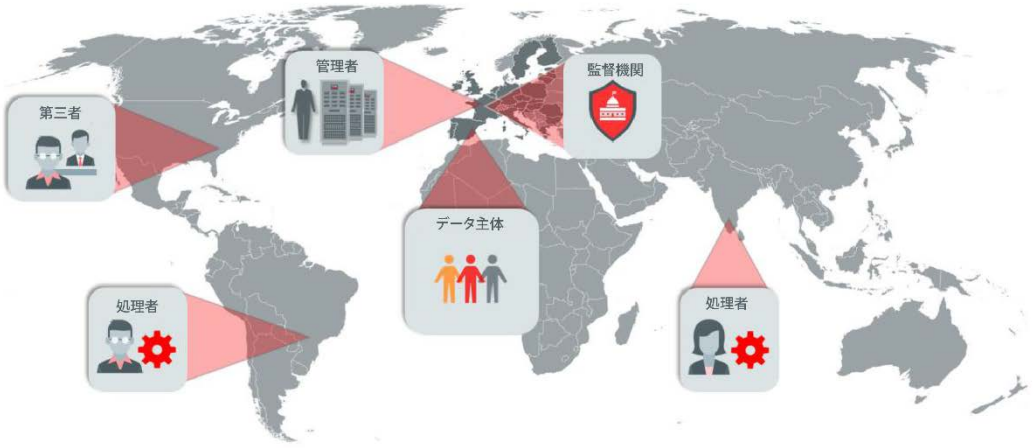

図1：GDPRの主体とEU事業者および管理者

GDPR は、EU 域外であっても EU のデータ主体情報を扱う管理者、処理者、および第三者に適用されます。たとえば、次のような場合です。

» EU 在住者に商品やサービスを提供するオーストラリア企業がアメリカからウェブサイトを運用する場合。

» EU 在住者のプロファイル情報を管理するインド企業（たとえば、ソーシャル・ネットワーキング・サイトや EU 域外のウェブサイトなど）。

» カナダを拠点とするサプライヤー（内部または外部）で EU 域内に"事業所"もサーバーも持たず、クラウド・コンピューティングで EU 在住者にサービスを提供している場合。

» 中国を拠点とする企業が打ち出すマーケティング・キャンペーンで（特に）EU 在住者を対象にさまざまなサービスを提供する場合。

» 直接的にまたは間接的に（クライアントやパートナーを通じて）EU 在住者の個人データを管理する EU 域外を拠点とするクラウド・プロバイダー。

» アメリカに旅行する EU 在住者の情報を保管するアメリカを拠点とするホテル・チェーンや航空会社。

GDPR は、EU 域外に拠点を置くが、EU 域内で製品やサービスを提供する企業または EU 在住者の行動を監視する企業にも適用されます。EU 域内に拠点を置く企業にのみ適用されるわけではありません。

次の図では、管理者は EU 域外ですが、GDPR の対象となります。

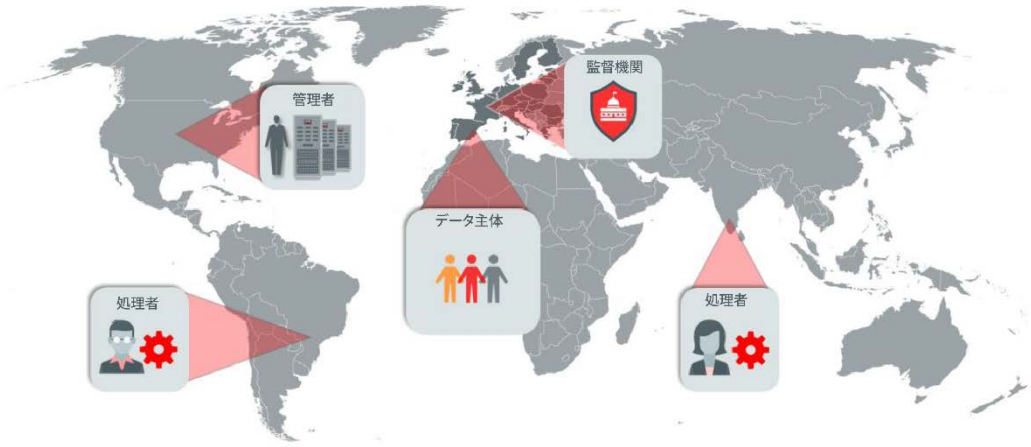

図2：GDPRの主体とEU域外の事業者および管理者

主要なGDPRデータ・セキュリティ要件

主要な GDPR データ・セキュリティ要件は、評価、予防、監視/検知の 3 つに大きく分類できます。また、GDPR では、データ保護の質と厳密さを向上させるため、データ保護原則の順守が求められます。この節では、GDPR で説明されている主要なデータ・セキュリティ要件の概要を紹介します。

セキュリティ上のリスクの評価

GDPR では、個人データのある種の取り扱いが、データ主体にとって"高いリスク"をはらむ可能性があるとき、管理者にデータ保護の影響評価の実施が義務付けられています。この影響評価には、組織による個人データの取り扱い、プロファイリングとこうしたツールによる個人データの保護方法についての体系的かつ詳細な評価を伴う必要があります。

…管理者は、データを取り扱う前に、予定された取り扱い作業の個人データの保護に対する影響評価を実施するものとする。

独立した評価は同様の高いリスクをはらむ同様の一連の取り扱い作業で用いることができる … *-- GDPR 第 35 条*

データ保護影響評価によって侵害防止の基礎を固めるためにギャップとリスクを評価します。

攻撃防止

規定のいろいろな所で GDPR はセキュリティ侵害を防止することの重要性を繰り返し強調しています。GDPR では、次のような複数の攻撃防止技術が推奨されています。

» **暗号化**

GDPR では、暗号化は個人データへのアクセス権限のないすべての人に対してデータを難読化する中核技術の 1 つとみなされています。

…管理者および処理者は、保護レベルをリスクに見合ったものにするため、適切な技術的および組織的対策を実施しなければならない。必要に応じて特に次に掲げる事項を含むものとする。（a）個人データの仮名化および暗号化。 *-- GDPR 第 32 条*

GDPR ではデータ侵害が発生した場合、データが暗号化されデータにアクセスしようとするいかなる人に対しても判読困難になっていれば、管理者によるデータ主体への通知は不要なため、組織にとって通知コストを削減できます。

データ主体への通知は、…要求されない… 個人データの侵害によって影響を受けるデータ、特に暗号化のように、当該個人データにアクセス権限のないあらゆる人に対して個人データが判読できないようにする対策、たとえば暗号化… -- GDPR 第 34 条

» **匿名化と仮名化**

データの匿名化はデータを完全に攪乱して難読化する技術であり、仮名化はデータ・セットとデータ主体の元の身元の間の関連を低減するものです。GDPR では、匿名化技術や仮名化技術を使用すると情報から個人や実体を識別できなくなるため、偶発的または意図的なデータ漏洩のリスクを軽減できるとされています。

… 個人データに仮名化を適用することで関係するデータ主体のリスクを軽減でき、管理者と処理者がデータ保護義務を果たすことができる…

--GDPR 説明事項 28

匿名化された個人データの適用範囲からの除外について：

> *…したがってデータ保護の原則は匿名情報（特定されたまたは特定可能な自然人と無関係な情報）あるいは、データ主体が特定できないかまたはもはや特定できなくなるような方法で匿名化された個人データには適用されないものとする。したがって、この規制では統計的な目的や研究目的も含めてこうした匿名情報の取り扱いは対象としていない。 -- GDPR 説明事項 26*

» **特権ユーザーのアクセス制御**

GDPR では、個人データにアクセスできる特権ユーザーを制御することで内部の人間や侵害されたユーザー・アカウントによる攻撃を防止できることが示されています。

> *… 個人データにアクセスする…管理者やあらゆる人物は…個人データを管理者からの指示以外で取り扱わないものとする… -- GDPR 第 32 条*

» **ファイングレイン・アクセス制御**

特権ユーザー制御に加え、GDPR では個人データへのアクセスを個別の明確な目的に限るためにファイングレイン・アクセス制御手法の採用が推奨されています。このようなファイングレイン・アクセス制御によって組織は個人データに対する不正アクセスを最小化できます。

> *… 管理者は、デフォルトで各具体的取り扱いの目的に必要な個人データのみが取り扱われることを保証するための適切な技術的および組織的対策を実施するものとする。*
>
> *--GDPR 第 25 条*

» **データの最小化**

GGDPR では、個人データの収集と保存を可能な限り最小限に留めることでコンプライアンス境界を縮小することが推奨されています。個人データの収集、取り扱い、共有に際して、管理者と処理者は情報を具体的な作業に必要な量に抑え、必要以上に利用しないことが求められます。

> *個人データは、取り扱われる目的の必要性に照らして、適切であり、関連性があり、必要最小限に限られるものとする（'データの最小化'）。 --GDPR 第 5 条*

侵害検知のための監視

予防的なセキュリティ手段によって組織は攻撃リスクを最小化できるものの、データ侵害の発生の恐れは排除できません。GDPR では、次のような手法によってこうした侵害を検知するための監視とアラート通知が推奨されています。

» **データ監査**

GDPR では、個人データの操作の記録と監査を義務付けているだけでなく、こうした記録を管理者の責任下で一元的に管理するよう推奨しています。つまり、処理者や第三者による監査記録の改ざんや破棄が可能であってはならないのです。簿記に加えて、監査はデータが侵害された場合のフォレンジック分析にも有効です。

> *各管理者....管理下にある取扱い操作の記録を維持管理するものとする。*
>
> *--GDPR 第 30 条*

» **監視とタイムリーなアラート**

個人データの操作を常時監視することは異常を検知する上で非常に重要です。綿密な監視に加えて、GDPR では侵害された場合のタイムリーな通知も義務付けています。

> *個人データの侵害が発生した場合、管理者は、不当な遅滞なしに、可能であれば、侵害に気が付いてから 72 時間以内に、個人データの侵害を監督機関に通知するものとする...* *-- GDPR 第 33 条*

セキュリティ・ガイドラインの 3 つの大きな分類（評価、予防、検知）は組織が脅威に多面的に対処し、不正アクセスからデータを保護するのに有効です。

保護の品質

大企業にとっても中小企業にとっても適切な計画を立てずにデータ・セキュリティを導入、実行しても、日々の IT 業務の妨げになり、結局は管理上の大きなオーバーヘッドになるだけです。適切に計画を立てられず、コストが増大することを言い訳にしてこれまで GDPR などの規定によるセキュリティを導入しなかった事業者もあるかもしれませんが、セキュリティは要件であって選択肢ではありません。こうした課題を解決するために、GDPR では次のことが推奨されており、セキュリティ制御の管理上のオーバーヘッドの軽減と保護品質の向上に役立ちます。設計と初期設定によるデータ保護 GDPR では、データ保護をシステムの中核的な要素にすることを義務付けています。テクノロジー・ライフ・サイクルの初期設計段階でセキュリティを考慮すれば、システムのセキュリティに関する価値が高まり、技術的なセキュリティ制御が期待通りに機能するようになります。

> ***設計と初期設定によるデータ保護***
>
> *... ...管理者は、本規則の要件に合致させるためおよびデータ主体の権利を保護するため、取り扱いの手法を決定する時点および取り扱い時点の両時点において、適切な技術的および組織的対策（たとえば仮名化）を実施するものとし、その対策の意図は、この規定の要件を満たし、データ主体の権利を保護するため、データ保護の原則（たとえばデータ最小化）を効果的な方法で履行すること、および必要な保護措置を取り扱いと統合することにある。* *- GDPR 第 25 条*

» **一元化**

GDPR では複数のアプリケーションやシステムの保護に取り組む場合、一元的な管理が推奨されています。侵害が発生した場合にただちに対処できるからです。また一元管理によって複数のターゲットに対する整合性も徹底でき、個々のターゲットでエラーが発生するおそれを軽減し、事業者全体でベスト・プラクティスを活用できます。

> *EU 域内の管理者の主たる事業所は、EU における一元管理の場所でなければならない... 取り扱いの目的および手段に関して主たる決定を下す管理活動の実効的かつ実質的な遂行を伴うものとする...* *--GDPR 説明事項 36*

» **包括的なセキュリティ**

脅威や攻撃は複数のソースによってもたらされる場合があり、組織は全方面に対する準備が必要です。GDPR では個人データの保護がデータの保存中や送信中といったデータ・ライフサイクルのすべての段階で義務付けられています。

> *適切なレベルのセキュリティの評価において、取り扱いによって生じるリスクを考慮するものとする。特に、転送、格納、またはその他の取り扱いが行われた個人データについて、偶発的または違法な破壊、消失、変更、不正な開示またはアクセスを考慮するものとする。* *--GDPR 第 32 条*

Oracle Database SecurityとGDPR

企業は、通常ファイアウォールや侵入検知システム、適切なネットワーク・セグメント化によってデータベース周りを多層防御することで、攻撃者がデータベースに直接到達できないようにしています。ただし、従来のネットワーク境界が曖昧になり、データベースに直接アクセスするユーザー（管理者、テスターや開発者、パートナー）の数が増えるにつれて、データベースを直接保護することが非常に重要になりつつあります。攻撃対象領域を縮小し、攻撃者がデータベースに到達できる手段の数を減らすためには、可能な限りデータの近くで保護することが極めて重要です。

リスク特性の評価における課題の 1 つは評価対象を特定することです。データベース・アプリケーションには通常、ネットワークやオペレーティング・システム、データベース、さらにはアプリケーション自体からの複数のエントリ・ポイントがあるからです。悪意のある侵入者は、そうしたエントリ・ポイントに必ず存在する弱点を悪用する可能性があります。さらに侵入者は、システムの使用、管理、テスト、保守を担当する従業員や業者を標的にする場合もあります。また組織はクラウド上にある場合も含めてシステムの展開方法やソース・コードがないおそれのあるレガシー・アプリケーションの使用、EU の内外を問わず第三者のテスト・チームや開発チームとの依存関係について検討する必要もあります。

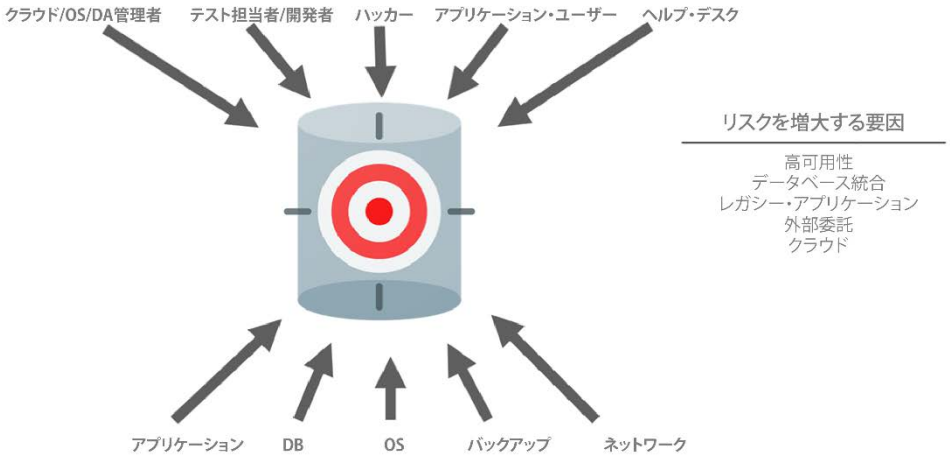

図3：データベースに対する攻撃ベクトルとターゲット

オラクルは、数十年にわたってデータ・セキュリティの分野で誰もが認めるリーダーであり、ここ数年は革新的なデータ・セキュリティ製品を開発してさまざまな脅威ベクトルによる攻撃に組織が対処できるように支援しています。オラクルは、行レベル・セキュリティやファイングレイン監査、透過的データ暗号化、特権ユーザーの機密情報へのアクセス制限、権限分析、データベース・ファイアウォールといった制御技術を最初に導入した企業です。

Oracle Database Security テクノロジーと製品による一連の自動化された、透過的かつ高性能なテクノロジーと製品を利用して課題を解決することで組織の GDPR 順守を促進できます。この節では、Oracle Database Security による制御に GDPR のセキュリティ評価、予防、検知の各要件を取り込む方法をご説明します。

評価	予防	検知
プロセス、プロファイル、データ機密性、リスク	暗号化、仮名化、匿名化、ファイングレイン・アクセス制御、特権アクセス制御、職務分掌	監査、操作監視、アラート、レポート

図4：GDPRの評価、予防、検知の各原則

セキュリティ上のリスクの評価

第 35 条ではある種のデータの取り扱いに対するデータ保護の影響評価が義務付けられています。リスク特性の評価における課題の 1 つは評価対象を特定することです。データベース・アプリケーションには、通常複数のエントリ・ポイントがあり、個人データが複数の列や表に分散し、アクセス制御の定義も厳格ではないからです。

Oracle Database Security テクノロジーと製品によってこうした課題に対処するためにアプリケーション・データを多面的に評価する次のような機能が提供されています。

» "個人データ"が含まれる表と列の検出機能

» セキュリティ・プロファイル全体を決定するためのデータベース構成機能

» データベースのロールと権限を分析して管理者、処理者、第三者、データ主体および取得者が個人データにアクセスできる方法を決定する機能

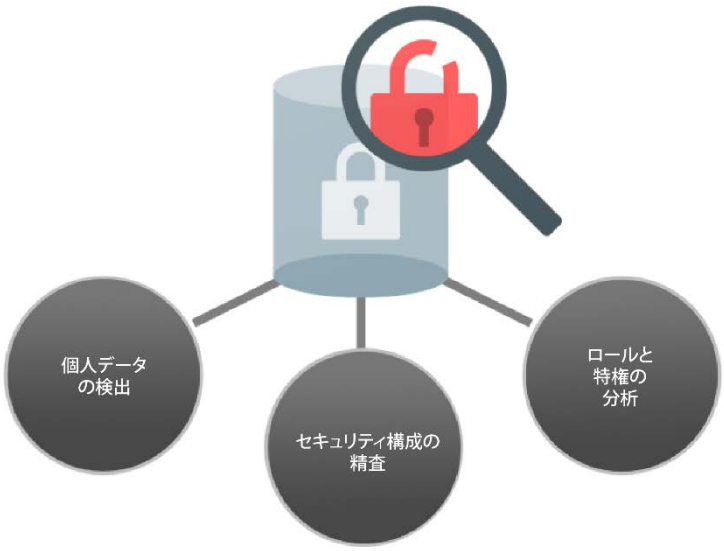

図5：セキュリティ上のリスクの評価

» Oracle Application Data Modeling を使用して機密データ環境を評価する機能

今日の複雑なアプリケーションで個人データを検出することは簡単な作業ではありません。さまざまな識別情報が複数のアプリケーション・スキーマにわたって複数の表に埋め込まれている場合があるからです。Oracle Application Data Modeling では、個人データを含む列と、データベースに定義された該当親子関係が自動的に検出されます。検出プロセスでは、クレジット・カード番号や国民識別番号などの組込みの拡張可能なパターンによって、データのサンプリングと機密性の高い列の識別が行われます。個人データが特定されると、予防型でも発見型でも適切な制御の適用が可能になります。結果として Application Data Model によって機密性の高い列一式とそのリレーション情報が提供され、データ保護制御によるアプリケーションの整合性が確実に維持されます。

» Oracle Database Vault の権限分析を使用して最小権限アクセスを評価する機能

個人データが特定されたら、ユーザー（データ主体、第三者、監督機関、取得者）を特定することが重要になります。ユーザーには特権ユーザーやシステム管理者（管理者、処理者）が含まれますが、これは個人データにアクセスできるだけでなく、処理も可能だからです。アプリケーションの設計や保守過程においては、ユーザーに追加の権限を意図せず認めてしまうことがあります。Oracle Database Vault の権限分析では実行時に実際に使用される権限を認定することでアプリケーションの安全性を向上させています。使用されていないと見なされた権限は廃止対象と評価され、最小権限モデルの実現に有効です。

» **Oracle Database Lifecycle Management Pack を使用してデータベース構成を評価する機能**

データベースはすべて調整可能な構成パラメータを多く備えており、幅広いセキュリティ要件に適合できます。重要なのは、構成が安全であり続け、時間とともにずれることなく、現在の一連のベスト・プラクティスの実践を徹底することです。組織には、デフォルトのアカウント・パスワードやアカウントの状態、アカウント・プロファイルといった非常に多くのセキュリティ関連の設定に関してデータベースを精査することが求められています。Oracle Enterprise Manager の Database Lifecycle Management Pack を使えば、Oracle Database に対して 100 以上の標準ポリシー・チェックを実行し、傾向を見極め、最適設定からのずれを監視できます。また、カスタム構成チェックを定義してオラクル標準のチェックを補完することもできます。

» **Oracle Database Security の評価ツールを使用してデータベース・セキュリティ・プロファイルを評価する機能**

GDPR の第 36 条により、データの機密性にもよりますが、組織は特定の個人情報を取り扱う前に監督機関の承認を得なければならない場合があります。課題は、プライバシーとセキュリティに関する適切な形式の評価レポートをすばやく作成して監督機関に提出することです。Oracle Database Security の評価ツールの分析対象には、構成だけでなく一部のセキュリティ・ポリシーの適用方法も含まれます。そのためユーザーが判読できる構造化された形式で調査結果がまとめられ、監督機関に提出できます。組織としては多くの時間とリソースを費やして Oracle Database のセキュリティ評価に関する調査結果を収集したり分析したりする必要はありません。この情報は、データ保護の影響評価を構築する上で非常に有効です。

攻撃防止

上述した GDPR 推奨の予防技術には暗号化や仮名化、匿名化、特権ユーザー制御などさまざまな技術があります。すべての予防型データ保護制御に関する課題の 1 つが、アプリケーションと日々の IT 業務に関してオーバーヘッドが生じる可能性があることです。このオーバーヘッドはデータ取り扱い方法の変更によって生じる可能性があります。アプリケーションのソース・コードの変更や、テスト、パフォーマンス・オーバーヘッド、さらに拡張性の問題もあります。こうした課題が原因で、既存のアプリケーションに対し予防的なセキュリティ対策の導入に躊躇する組織もあるようです。

こうした懸念も 10 年前なら根拠があったかも知れませんが、今では Oracle Database Security による予防的な制御によってこうした課題に対処しています。この予防的制御は、ほとんどのアプリケーションにとって透過的で、性能や現行の IT 業務への影響は最小限に抑えられています。オラクルの提供する導入が容易な予防型制御スイートによって組織は GDPR が義務付ける暗号化や、仮名化、匿名化、特権ユーザー制御、ファイングレイン・アクセス制御、データの埋込みといった主要な予防技術を実装できます。

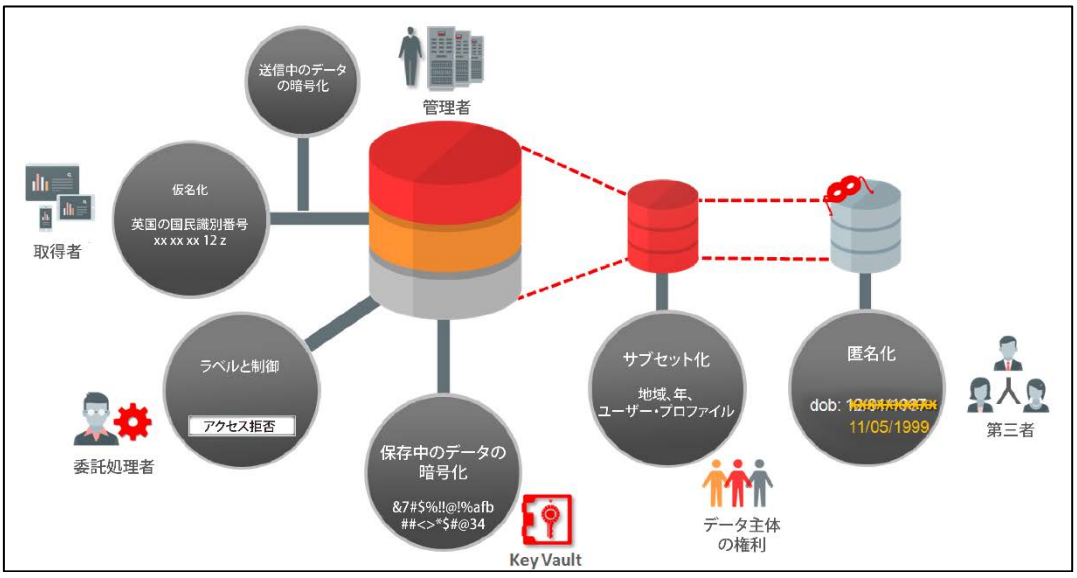

図6：Oracle Database Securityの予防制御

» 透過的データ暗号化を使用した保存データの暗号化

GDPR の第 32 条および説明事項 83 では、データ保護技術の 1 つとして暗号化が推奨されています。データ暗号化を導入する際、組織にとっての課題の 1 つが、暗号化対象に表の個人データだけでなく、バックアップやデータ・ダンプ、ログ・ファイルの個人データまで含めなければならないことです。こうしたすべてのソースから個人データを特定して暗号化する作業はリソースを大きく消費する可能性があります。Oracle Advanced Security の透過的データ暗号化（TDE）は、この課題に対処するためすべてのデータを直接ソース（データベース・レイヤー）内で暗号化します。TDE によってデータは、バックアップやデータ・ダンプ、エクスポート、ログといったストレージに書き込まれるときに自動的に暗号化されます。暗号化されたデータは、同様にストレージから読み出されるときに自動的に復号化されます。このデータベース・レイヤーにおける自動暗号化・復号化機能によって、このソリューションは、データベース・アプリケーションから見て透過的になります。データベース・レイヤーとアプリケーション・レイヤーで実施されるアクセス制御は引き続き有効です。SQL 問合せは不変なので、アプリケーション・コードも構成も変更不要です。Oracle Database には TDE がインストール済みなので簡単に有効化できます。

データを暗号化するときのもう 1 つの懸念は、データベース操作やアプリケーション操作への性能上の影響です。暗号化・復号化プロセスが極めて高速なのは、TDE が Oracle Database のキャッシング最適化機能と、Intel（AES-NI）および Oracle SPARC チップセットで提供される CPU ベースのハードウェア・アクセラレーションを利用しているからです。

» Oracle Key Vault を使用した暗号化キーの一元管理

一元化により、管理者があらゆる部分に同一のセキュリティ制御を適用でき、侵害が発生した場合にも迅速な対応が可能になります。Oracle Key Vault（OKV）では、透過的データ暗号化（TDE）によって暗号化されたデータの一元管理ができます。TDE によって、データ暗号化キーとマスター暗号化キーによる 2 層の暗号化キー管理が実現できます。Oracle[1] {2]Key Vault（OKV）を使用すると、マスター暗号化キーを一元的に制御、管理できます。OKV によってデータの侵害や怪しい挙動が発生した場合にマスター・キーへのアクセスを一時停止し、暗号化データを難読化する機能が提供されます。

Oracle Key Vault はソフトウェア・アプライアンスであり、暗号化キーや Oracle Wallet、Java キーストア、認証情報ファイルを一元管理することで、顧客は暗号化などのセキュリティ・ソリューションをすばやく展開できるようになります。

» Oracle Database のネットワーク暗号化とデータ整合性を使用した送信中のデータの暗号化

送信中の個人データの保護に関する GDPR 第 32 条の要件を満たすために、Oracle Database のネットワーク暗号化とデータ整合性を使用することで、組織と管理者は送信中のデータを暗号化し、データ・スニフィング、データ損失、再生、中間者攻撃を阻止できます。

オラクルでは、ネイティブのネットワーク暗号化と、PKI インフラストラクチャを保持している組織向けの Transport Layer Security（TLS）ベースのネットワーク暗号化の両方を提供します。ネットワーク暗号化とデータ整合性は Oracle Database の標準機能で、デフォルトでインストールされています。オラクルは、AES のような国際的な暗号化アルゴリズムをサポートしています。

» Data Redaction と Database Vault を使用したデータの仮名化

GDPR 第 32 条と説明事項 28 では仮名化が推奨されています。たとえば、表の列に格納された、データ主体を表す属性を編集できます。また、元のデータ主体への関連を形成するのに有用な、複数の属性が格納された表を、結合できないようにして保護し、一方でデータセットとデータ主体の関連を低減しています。

仮名化機能では、アプリケーション画面での偶発的または意図的な機密データの漏洩を防止することで攻撃に対処します。こうした画面は、処理者や第三者によってアプリケーションのサポートや欧州連合域外のコール・センターで使用される可能性があります。仮名化の実装における課題の 1 つが、どうやってアプリケーションからデータベースへの問合せを傍受し、アプリケーションやバックエンドのデータベースに影響を与えずにデータを変換するかです。

Oracle Advanced Security の Data Redaction 機能では、この問題に対処するために、SQL 問合せの結果がアプリケーションに返される前に、結果に含まれる個人データを個別に、動的に編集することで、不正なユーザーがデータを閲覧できないようにしています。この機能によって、同じデータベース情報にアクセスするアプリケーション・モジュールのすべてで、データベース列の一貫した編集が可能になります。Oracle Data Redaction では、アプリケーションに対する変更は最小限に抑えられます。内部データベース・バッファ、キャッシュ、またはストレージにある実際のデータは変更されず、変換したデータをアプリケーションに戻すときに元のデータ型およびデータ書式設定も維持されるからです。Oracle Data Redaction は、バックアップ、リストア、アップグレード、パッチ適用といったデータベースの運用操作や高可用性クラスタに影響を与えることはありません。永続データが変更されないためです。アプリケーションの変更や、プロキシによりデータベースへのアクセスを傍受することが求められるこれまでの手法とは異なり、Oracle Data Redaction のポリシーはデータベース・カーネル内で直接適用されるので、セキュリティが強化され、またパフォーマンスが向上します。また、Oracle Data Redaction によって管理者は実際のデータを正規の取得者に戻すべき条件を指定できます。Oracle Database には Data Redaction がインストール済みなので簡単に有効化できます。

Oracle Database Vault は、権限のあるユーザーに対してのみや特定の環境で、データへのアクセスを保護するレルムを作成できるため、複数の表に格納された機密性の高い属性を保護するのに役立ちます。たとえば、データ主体のすべての属性（複数の表に格納）をアプリケーション・ユーザーが読み取れるようにしながら、データベース管理者などのユーザーだけが親表の主要な属性を確認できるようにし、データ主体への関連付けを困難にできます。

» Oracle Data Masking and Subsetting を使用した匿名化と最小化

匿名化機能を使用してデータ主体の個人データを識別不能にすると、テストや開発のような保護が不十分な環境での個人データの流出を防止できます。たとえば、16 桁のクレジット・カード番号は 5678-0987-4512-1111 のような偽の 16 桁のクレジット・カード番号に匿名化できます。[匿名化の課題の 1 つは、適切に処理されないと、攪乱して識別不能化されたデータはテスターや開発者が使えなくなる場合があることです。さらに、アプリケーションやデータベースのデータ整合性を壊す可能性があります。

Oracle Data Masking and Subsetting ではこうした課題に対処するため、拡張可能な包括的匿名化ライブラリとマスキング・フォーマット、関数/変換、アプリケーション・テンプレートが提供されています。クレジット・カード番号、国民識別番号やその他の個人識別情報（PII）のような個人データやその他の機密情報は、マスキング・フォーマットと匿名化フォーマットの標準ライブラリを使用して簡単にマスクできます。

GDPR 第 5 条では、収集、処理、共有、保持される個人データの量を減らすためデータの最小化が義務付けられています。とはいえ、ほとんどのグローバル企業では 1 つの表に複数の国や地域のデータが混在しており、表の部分ごとに異なるポリシーを適用することは困難です。これが特に厄介になるのは、組織がデータ（個人データを含む）のコピーを EU 域外の特定の国のパートナーのような第三者や処理者に提供する必要のある場合です。GDPR の要件すべてを満たせない場合は、EU 固有のデータを全体から削除し残りを特定の事業目的のために保管するのが最善策となることもあります。Oracle Data Masking and Subsetting では、定義しやすいゴールや国識別子に基づくサブ設定のような条件ベースのサブ設定を利用してこの課題に対処しています。Data Subsetting によって、大規模なデータセットからデータ・サブセットを自動的に指定、削除、抽出する機能が提供されます。Data Subsetting では、削除や抽出処理中にデータ・リレーションシップと依存性が自動的に処理され、データセットの整合性が維持されます。

Oracle Data Masking and Subsetting では、データベースからアプリケーション・データの完全コピーまたはサブセットを抽出し、個人データを匿名化した上で最小化することで、データをテスターや開発者、パートナーといった処理者や第三者と安全に共有できます。データベースの整合性が維持され、アプリケーションの継続性が確保されます。

Oracle Data Masking and Subsetting は、Oracle Enterprise Manager にプレインストールされています。統一された Web ベースのマスク用 GUI と、オンプレミスと Oracle Cloud のデータベースのサブセットが提供されます。

また、説明事項 26 には、データ主体を特定できない方法で個人データが匿名化された場合は、データ保護の原則は匿名情報には適用されないことが示されています。本番環境以外でデータをマスクすると、個人データが実際には必要とされない開発環境、テスト環境、その他の環境を GDPR の適用範囲外にするのに役立ちます。

» Oracle Database Vault を使用した特権ユーザーの管理と職務分掌の適用

GDPR 第 32 条で処理者のアクセス制限を推奨しているのは、特権アカウントが、データベース中の機密アプリケーション・データにアクセスするためにもっとも一般に使用されるルートの 1 つだからです。この広範な無制限のアクセスは、データベースのメンテナンスを容易にしますが、大量のデータにアクセスするための攻撃の糸口にもなります。

昔から特権ユーザー（DBA など）の個人データへのアクセス制限は簡単ではありませんでした。こうした制限は、パッチ適用や保守といった日々の業務に支障を来す可能性があります。Oracle Database Vault には、Oracle Database の特権ユーザーのアクセス制御機能が組み込まれており、特権ユーザーによる個人データへのアクセスが制限されています。その一方で DBA は個人データにアクセスすることなく、パッチ適用やインポート、エクスポート、バックアップといった通常の運用操作を実行できます。Oracle Database Vault を使用して、特権ユーザーからだけでなく、データベース・コマンドの使用からも保護する必要のある個人データの領域を明確にします。個人データにアクセスする管理者や処理者、第三者（正規のユーザー）が使う可能性のあるメカニズムやファクタを制御します。

» Oracle Virtual Private Database を使用した選択的データ非表示

GDPR では、選択された個人データを一時的にユーザーが利用できなくするといった、ときどき起こる問題を処理する一時的な予防的技術が取り入れられています。しかし、課題は大規模なデータセットからサブセット値を簡単に抜き出して非表示にすることです。たとえば、ある組織で怪しいアクティビティがあり、イタリア国籍の個人データをすべて一時的に非表示にする必要があるとします。イタリアの国識別子だけをさまざまな国の国識別子を含む膨大な列から抜き出して非表示にするには通常多大なプログラミング作業を要します。

Oracle Virtual Private Database（VPD）ではこの問題に簡単に宣言できる行レベルのセキュリティ（RLS）ポリシーを使って対処します。具体的には、条件または"WHERE"句を計算して入力 SQL 文に自動的に追加することで、表内の行や列へのアクセスを制限します。VPD は Oracle Database にデフォルトでインストールされており、ときどき発生する問題の処理だけでなく通常の操作に対しても不正アクセスからデータベースを保護できます。これにより、ユーザーが自分のデータだけでなく、他のユーザーのデータも閲覧できるようになるプログラム・エラーがある場合に攻撃対象領域が縮小されます。

» Oracle Label Security によるアクセス制御

GDPR では、処理者による個人データへのアクセスが選択的かつ明確な目的によって行われるように組織と管理者が徹底することを推奨しています。Oracle Label Security（OLS）によって組織は、機密性（公開、機密、極秘など）や地域（北米、ヨーロッパ、アジア太平洋など）に基づいてラベルを割り当てることで個人データ要素を分類できます。OLS によってデータ分類に基づいて簡単に宣言できるアクセス制御が提供されます。たとえば、クレジット・カード番号のような機密データ要素を含む行をヨーロッパの最高機密データに分類することで、厳選された処理者またはユーザーのみがこの個人の機密データにアクセスできるようになります。

この簡単に宣言できるアクセス制御によって、OLS ではマルチレベル・セキュリティ（MLS）モデルが簡易化されます。このモデルは多くの政府機関や防衛機関にとっては一般的には必須要件となっています。Oracle Database には Oracle Label Security がインストール済みなので簡単に有効化できます。

» Oracle Real Application Security を使用したエンド・ツー・エンドのアクセス制御の簡易化

GDPR の説明事項 64 によると、管理者はオンライン・サービス絡みで個人データを要求するデータ主体の本人確認を、アクセス権を与える前に実施するものとされています。最新の 3 層アプリケーションでは、ネットワーク環境でのユーザーの身元確認が課題となっています。通常アプリケーションやアプリケーション・サーバーはデータベースに 1 人のデータベース・ユーザーとして接続するため、元のユーザーを追跡することが難しいからです。

Oracle Real Application Security（RAS）ではこの問題に対処するため、ポリシーベースの認証モデルを備え、アプリケーションレベルでデータベース内のユーザー、権限、ロールを認識します。アプリケーションのユーザー・セッション情報を安全にデータベースに伝播する機能が組み込まれているため、RAS を使用すればデータに関するセキュリティ・ポリシーをアプリケーション・ユーザー、ロール、セキュリティ・コンテキストに応じて直接定義できます。ACL によって、個人データにアクセスできるユーザーを RAS で制御できます。Oracle Database には Real Application Security がインストール済みです。

暗号化、仮名化、特権アクセス制御のいずれを問わず、Oracle Database Security の幅広い予防型制御製品ラインアップを使用すると GDPR が義務付けるデータ保護原則の導入と維持の労力を最小化できます。

侵害検知のための監視

従来の境界ファイアウォールは、外部からの不正アクセスに対してデータセンターを保護するために重要な役割を果たしていますが、攻撃はますます高度化し、境界セキュリティをバイパスする、信頼されている中間層を利用する、さらには内部の特権ユーザーを装うなどの手法が使用されるようになってきました。多数のセキュリティ・インシデントの調査から、監査データをタイムリーに審査すれば、不正なアクティビティを早期に検知して結果として生じる経済的な打撃を軽減できることが分かっています。GDPR 第 30 条と第 33 条では、組織は操作の記録を維持することが義務付けられています。これが可能なのは、個人データに対する操作を常に監視、監査する場合だけです。侵害が発生した場合は、このデータを使用してタイムリーに当局へ通知できます。監査とタイムリーな通知を義務付けていることに加えて、GDPR では組織による監査記録の管理も求められています。監査記録を一元管理することで攻撃者や悪意のあるユーザーがローカルの監査記録を削除して自分たちの怪しい挙動の痕跡を隠すことを防ぎます。

Oracle Database Security によって包括的な監査情報収集機能とレポーティング・メカニズムが提供され、GDPR の監視要件を満足します。Oracle Audit Vault and Database Firewall（AVDF）によって提供される次世代型のデータ中心の監査/保護（DCAP）プラットフォームは、Oracle データベースおよび Oracle 以外のデータベースから得られた監査データ、オペレーティング・システム、ファイル・システム、アプリケーション固有の監査データの統合を通じて、包括的で柔軟な監視を実現します。同時に、Oracle Database Firewall はネットワーク防御の最前線として機能し、アプリケーションに期待されている動作を実行して、SQL インジェクション、アプリケーション・バイパスなどの悪意のあるアクティビティがデータベースに到達することを阻止します。Oracle Audit Vault and Database Firewall は、複数のデータベースの監査データを統合し、SQL トラフィックを監視して、不正な SQL 文やポリシー違反の SQL 文を検索、警告して、阻止できます。データ保護オフィサーと管理者は、挙動不審の侵入者を補足するためにアラートをリアルタイムで発行できる条件を指定できます。標準で用意されているさまざまなレポートとカスタム・レポート・インタフェースを組み合わせれば、ネットワーク経由で監視している場合でも、監査ログを調べている場合でも、企業全体のデータベース・アクティビティを総合的に捉えることができます。Oracle AVDF は、Oracle、Microsoft SQL Server、IBM DB2 for LUW、SAP Sybase ASE、Oracle MySQL データベースをサポートしています。

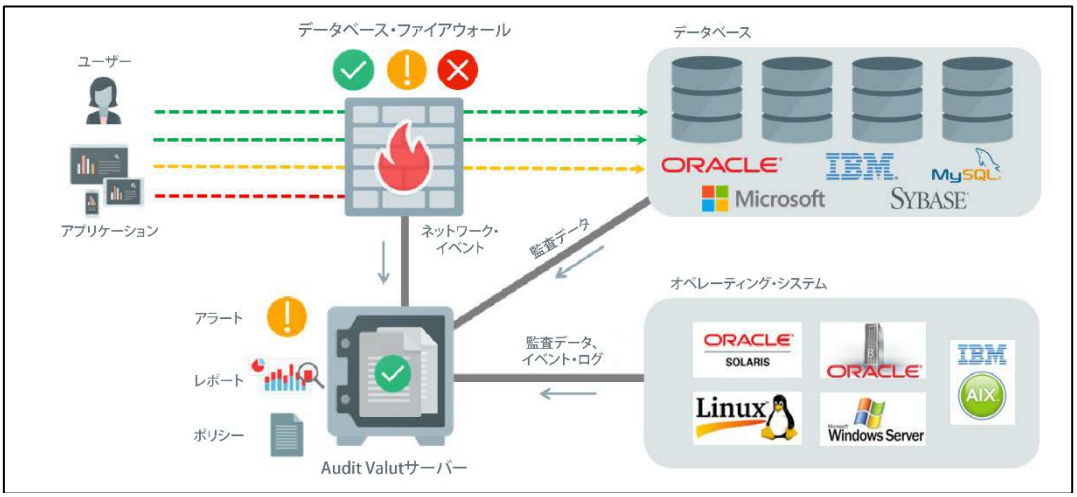

図7：Oracle Database Securityの監視制御

透過性、正確性、性能、拡張性を備えた最大保護

GDPR 第 25 条では、設計と初期設定によるデータ保護の概念が取り入れられています。最新アプリケーションは、Web ゲートウェイ、Web プロキシ、Web サーバー、アプリケーション・サーバー、データベース・サーバーといった複数の基盤となるコンポーネントから構成されています。多層的な環境においてすべてのセキュリティ制御を定義し、実装することは難しい作業です。個別のベンダーからこうしたさまざまなセキュリティ制御や技術をすべて集めることは組織にとって統合、管理する上での課題となります。

Oracle Database Security ではこうした課題に対処するため、制御をデータに近づけ、データベース内で保護を実行します。Oracle が提供するデータ保護制御機能の大半は、Oracle Database に組み込まれています。データを発生元で保護することで設計や展開が容易になるだけでなく、保護の精度が向上し、攻撃対象領域が縮小します。

Oracle Key Vault と Oracle Audit Vault and Database Firewall では制御と管理を一元化することで発生元のデータ保護を補完します。何千もの暗号化鍵や何百万もの監査記録があろうと、セキュリティ・ポリシーの種類がさまざまであろうとも、これらのコンポーネントは一元管理できるため管理に関連する作業が大幅に簡素化されます。Oracle Enterprise Manager（EM）によって、Oracle Database Security コンポーネントを管理するための Web ベースの統合 GUI が提供されます。

特に重要なのは、Oracle Database Security による制御はすべて十分統合されており、個人データをインサイド・アウトベースで保護するということです。次の図でオラクルの Maximum Data Security アーキテクチャによってさまざまな Oracle Database Security 製品を相互に統合して個人データを保護する仕組みを説明します。

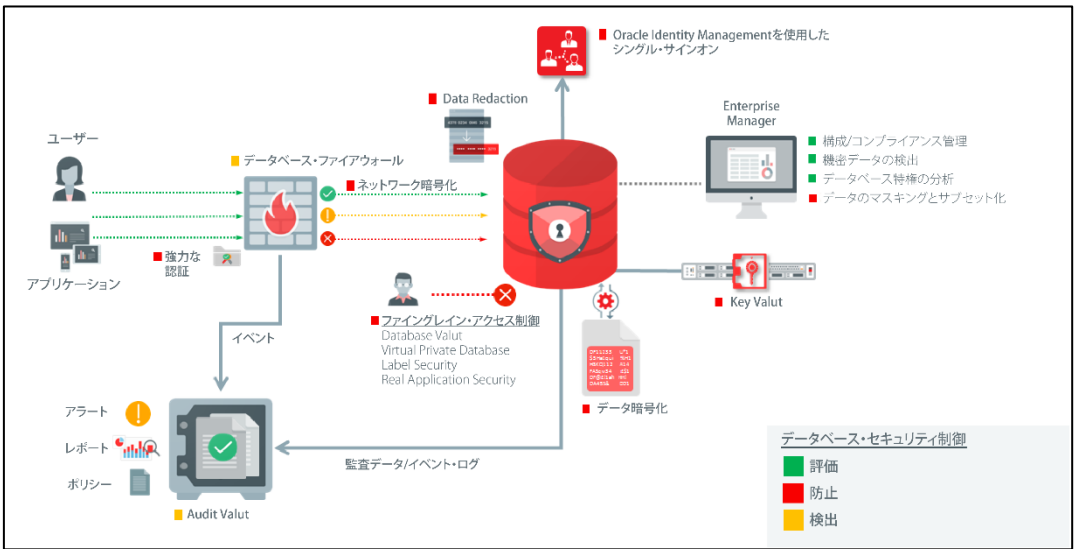

図8：オラクルのMaximum Data Securityアーキテクチャ

架空の事例

これまで GDPR の目的、主体、主要なデータ保護原則について説明してきましたので、ここで、このホワイト・ペーパーの始めに登場した架空のフランスの製造会社 XYZ が Oracle Database Security による制御を利用して、GDPR の主要なデータ保護原則にどうやって適合したかをご紹介しましょう。

» 評価

最初の手順として、XYZ の最高セキュリティ責任者（CSO）の指導により、アプリケーション（APP）グループとデータベース（DB）グループでデータ・セキュリティの現状を評価した結果の概要は次のとおりです。

- Oracle Database Lifecycle Management Pack または Database Security 評価ツールを使用して構成を精査することでデータベースのセキュリティ・プロファイルを評価する。
- Oracle Application Data Modeling を使用してデータ主体の機密データを含む機密性の高いデータベースの列を検出する。
- Oracle 権限分析を使用してユーザーの権限とロールを精査することで機密データへのアクセス方法を評価する。
- 詳細な評価レポートを作成してその調査結果を監査役と監督機関に提出する。

» **予防**

評価結果に基づいて、CSO の指導により DB チームと APP チームが予防的技術を導入することで、外部と内部の攻撃者からアプリケーションを保護できます。概要は次のとおりです。

- Oracle Advanced Security の透過的データ暗号化を使用してデータ主体の個人データを含むデータベースを暗号化する。
- Oracle Key Vault で暗号化キーを一元管理する。
- Oracle Advanced Security の Data Redaction と Oracle Database Vault を使用して顧客サービス・アプリケーションと請求アプリケーションの機密情報を仮名化する。
- Oracle Database のネットワーク暗号化とデータ整合性を使用してデータベースのネットワーク・トラフィックを暗号化する。
- Oracle Data Masking and Subsetting を使用して開発やテストで取り扱う前に個人データを匿名化する。
- Oracle Database Vault を使用して特権ユーザーのアクセス制御と職務分掌を導入する。
- Oracle Virtual Private Database、Oracle Label Security、Oracle Real Application Security を使用してアプリケーションにファイングレイン・アクセス制御を実装する。

» **検知**

最後に CSO の指導で、DB チームと APP チームは検知技術を導入して怪しい挙動がないかアプリケーションとデータベースを監視します。概要は次のとおりです。

- Oracle Database Auditing を使用してデータ主体の情報に対する操作を監査する。
- Oracle Audit Vault を使用して監査記録を一元的に収集、管理する。
- Oracle Database Firewall を使用して怪しい挙動を監視、警告、報告、阻止する。

結論

オラクルは、数十年にわたりデータ・セキュリティにおいて誰もが認めるリーダーであり続けています。ここ数年は革新的なデータ・セキュリティ製品を開発してさまざまな脅威ベクトルによる攻撃に組織が対処できるように支援してきました。世界中の組織が GDPR の要件への対応を強化するために Oracle Database Security の評価、予防、検知制御を利用することで、オーバーヘッドを最小化し、透明性を高め、展開の複雑度を下げることができます。

重要なのは、GDPR の要件への対応方法の計画を今から始めることです。Oracle Database Security 製品を利用することで、組織は最短で制御機能の導入を開始できます。その目的は、GDPR への対応強化だけでなく、機密性の高い個人データとビジネス・データに対する強固なセキュリティを実現することです。

参考資料

以下のウェブサイトに Oracle Database Security 製品と EU の GDPR に関する詳細情報が掲載されています。

» EU GDPR：http://ec.europa.eu/justice/data-protection/reform/index_en.htm

» Oracle Database Security 製品に関するデータ・シート、ホワイト・ペーパー、FAQ、文書、参考資料、ブログ、フォーラム、デモを集めた Oracle Technology Network：

http://www.oracle.com/technetwork/jp/database/security/index.html

» Oracle Database Lifecycle Management Pack：
http://www.oracle.com/technetwork/jp/oem/lifecycle-mgmt/index.html

» Oracle Database のセキュリティアセスメントツール(Oracle Database Security Assessment Tool)：
http://go.oracle.com/LP=38340

付録：Oracle Database Security製品とGDPRの対応表

	参考資料	GDPR ガイドライン	Oracle Database の推奨事項
評価	第 35 条	データ保護の影響評価："...管理者は、データを取り扱う前に、予定された取り扱い作業の個人データの保護に対する影響評価を実施するものとする。独立した評価は同様の高いリスクをはらむ同様の一連の取り扱い作業で用いることができる"	» Oracle Enterprise Manager の Application Data Modeling を使用して機密情報を含むデータベース列を精査し機密データ環境を評価する。 » Oracle Database Vault の権限分析を使用して Oracle Database のロールと権限を精査することで機密データへのアクセス方法を評価する。 » Oracle Enterprise Manager の Database Lifecycle Management Pack を使用して構成を精査し Oracle Databases のセキュリティ・プロファイルを評価する。 » Oracle Database Security の評価ツールを使用してデータベースのセキュリティ構成、適用されたセキュリティ・ポリシー、ユーザーやロール、権限認可の状態を評価する。
	説明事項 84	"...データ取り扱い業務が個人の権利と自由に高いリスクをもたらす可能性が高い場合、管理者は特にこのリスクの原因、特質、特殊性、重要度を評価するためデータ保護の影響評価を実施する責任を負うものとする..."	
予防	第 6 条	"…4.）個人データの取り扱いが、収集された目的以外で、データ主体の同意に基づいていない場合...管理者は、目的外の取り扱いが個人データが当初収集された際の目的と合致することを確保するため、特に次に掲げる項目を考慮するものとする。 4.e.）暗号化または仮名化を含めた適切な保護措置の存在…"	» Oracle Advanced Security の Transparent Data Encryption を使用してデータを暗号化する。 » Oracle Advanced Security の Data Redaction を使用して本番アプリケーションのデータを仮名化する。 » Oracle Data Masking and Subsetting を使用して本番以外のアプリケーションのデータを匿名化する。
	第 32 条	"...管理者および取扱者は、保護レベルをリスクに見合ったものにするため、適切な技術的および組織的対策を実施しなければならない。必要に応じて特に次に掲げる事項を含むものとする。個人データの仮名化および暗号化..."	
	説明事項 28	"個人データに仮名化を適用することで関係するデータ主体のリスクを軽減でき、管理者と処理者がデータ保護義務を果たすことができる"	
	説明事項 83	"セキュリティを維持し、この規制に違反した取り扱いを防止するため、管理者または処理者は、データの取り扱いに伴うリスクを評価し、暗号化などのリスク軽減策を導入するものとする"	» Oracle Data Masking and Subsetting を使用して本番環境以外のデータをマスクするか匿名化する。
	説明事項 26	"…したがってデータ保護の原則は匿名情報（特定されたまたは特定可能な自然人と無関係な情報）あるいは、データ主体が特定できないかまたはもはや特定できなくなるような方法で匿名化されたデータには適用されないものとする。したがって、この規制では統計的な目的や研究目的も含めてこうした匿名情報の取り扱いは対象としていない"	» Oracle Data Masking and Subsetting を使用して本番環境以外のデータをマスクするか匿名化する。
	第 5 条	"個人データは、取り扱われる目的の必要性に照らして、適切であり、関連性があり、必要最小限に限られるものとする（'データの最小化'）"	» Oracle Data Masking and Subsetting によりデータの削除や別の場所へのデータの抽出を行うことでデータのサブセットを生成する。

予防	第 29 条	"個人データにアクセスする、処理者または管理者や処理者の権限下で行動する人物は、管理者からの指示以外で個人データを取り扱わないものとする…"	» Oracle Virtual Private Database によりファイングレイン・アクセス制御を実施する。 » Oracle Label Security によりデータ集別ラベルを機密情報に割り当てる。 » Oracle Label Security によりデータ集別に基づいてアクセスを制御する。 » Oracle Database Vault により処理者などの特権ユーザーのアクセスを制御する。
	第 32 条	"… 4）管理者と処理者は、個人データにアクセスする管理者または処理者の権限化で行動する自然人が、管理者からの指示以外で個人データを取り扱うことがないように対策を講じるものとする…"	
	説明事項 64	"… 管理者はあらゆる合理的な手段を利用してアクセスを要求するデータ主体の身元を確認するものとする（特にオンライン・サービスやオンライン識別子に関連する場合）"	» Real Application Security（RAS）とともに SSL や Kerberos のような強力な認証技術を使用して、機密情報にアクセスするデータベース・ユーザーやアプリケーション・ユーザーの身元を確認する。
検知	第 30 条	"各管理者、該当する場合、管理者の代理人は、管理下にある取り扱い操作の記録を維持管理するものとする。"	» Oracle Database Auditing を使用してデータ取り扱い記録（監査記録）を維持管理して利用可能にする。 » Oracle のファイングレイン監査機能を使用して機密データに対する SELECT のような特定のユーザー操作を記録または監査する。 » Oracle Audit Vault and Database Firewall を使用して、データ取り扱い記録を一元的に保存、管理する。 » Oracle Audit Vault and Database Firewall を使用して、怪しい挙動を監視しタイムリーにアラートを送信する。
	第 33 条	"個人データの侵害が発生した場合、管理者は、不当な遅滞なしに、可能であれば、侵害に気が付いてから 72 時間以内に、個人データの侵害を監督機関に通知するものとする..."	
	第 34 条	個人データの侵害が発生した場合、管理者は、不当な遅滞なしに、可能であれば、侵害に気が付いてから 72 時間以内に、個人データの侵害を監督機関に通知するものとする...	
最大保護	第 25 条	"... 管理者は、本規則の要件に合致させるためおよびデータ主体の権利を保護するため、取り扱いの手法を決定する時点および取り扱い時点の両時点において、適切な技術的および組織的対策（たとえば仮名化）を実施するものとし、その対策の意図は、この規定の要件を満たし、データ主体の権利を保護するため、データ保護の原則（たとえばデータ最小化）を効果的な方法で履行すること、および必要な保護措置を取り扱いと統合することにある。"	» Oracle Database Security の最大保護アーキテクチャを利用してインサイド・アウトのデータを保護するため評価、予防、検知の各制御を導入する。
	第 32 条	"適切なレベルのセキュリティの評価において、...転送、格納、またはその他の取り扱いが行われた個人データについて、偶発的または違法な破壊、消失、変更、不正な開示またはアクセスを考慮するものとする"	

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

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

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Hardware and Software, Engineered to Work Together