PostgreSQL インサイド

データベースのアクセス制御を簡単に実現

Enterprise Postgres の機密管理支援機能

企業や組織において、情報セキュリティ対策は必要不可欠なものとなっています。例えば、情報漏洩が発生してしまうと、企業イメージの低下による信頼性失墜や多額の損害賠償などの多大なペナルティが発生してしまい、企業の存続にも影響しかねません。このように情報の流出防止は、企業の信頼性確保の重要な鍵となっています。

富士通のデータベース「Fujitsu Enterprise Postgres (以降、 Enterprise Postgres)」は、2016 年のリリース以降、情報漏洩などのセキュリティリスクに対抗する機能を提供してきました。2023 年 4 月にリリースされた、Enterprise Postgres 15 では、データベースのアクセス制御の設定を支援する「機密管理支援機能」が提供され、さらなるセキュリティ強化を実現しています。

ここでは、「機密管理支援機能」の説明を中心に、Enterprise Postgres が提供するセキュリティ機能の狙いやメリットを解説します。

個人情報の取扱いの歴史と現在の課題

個人情報取扱いの歴史

「2025 年の崖」によってクラウド化が加速し、コロナ渦によって社会の環境が劇的に変化したことで、企業の DX(デジタルトランスフォーメーション)推進にますます拍車がかかっています。DX を推進するにあたり、日々、蓄積されていくデータを分析し、どのように活用するかがポイントです。ここでいうデータにはさまざまな種類、情報が含まれており、個人を特定できる「個人情報」も含まれます。

個人情報は、個人のプライバシーにかかわる大切な情報ですが、それらの情報を活用することで、企業が提供するサービスの向上や業務の効率化をもたらします。企業は、個人情報を安全に、効果的に活用する必要があります。

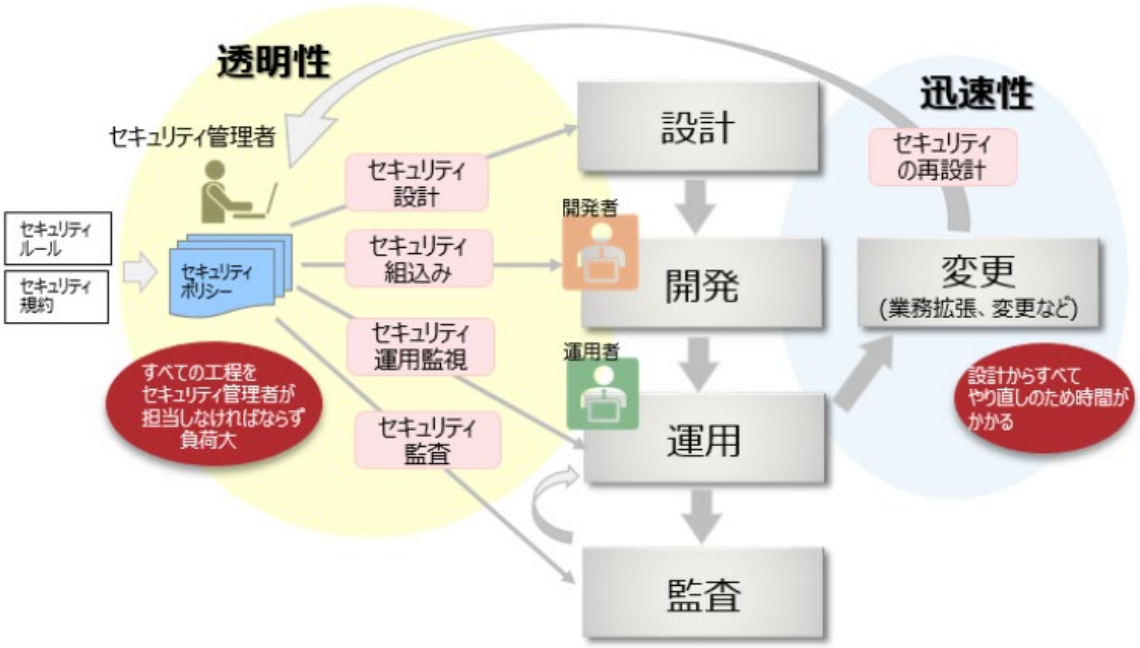
個人情報に関しては、個人の権利や利益を守ることを目的とした「個人情報保護法」がありますが、2003 年に制定以降、3 回の改正が実施されています。2022 年 4 月の改正では、個人データが漏洩された場合に本人への通知が義務化されたり、もともと個人情報の扱いではなかったデータ（個人を識別できない Web 閲覧履歴など）についても個人データとなることが想定される場合は、本人の同意が必要というように、情報の取扱いが年々厳格化しています。

現在の課題

一方で、DX は、「デジタル技術を活用しながら企業を変革し、企業価値を創出していくこと」を目的としています。例えば、SNS の普及で誰もがインフルエンサーとなって製品やサービスに対する評価を発信しえるため、企業はその評価に対する素早い対応が求められます。変化が著しい社会の中で DX を推進していくためにはスピード感を持った対応が不可欠です。これは、企業内のシステムに当てはめても同様で、DX では、システムの拡張や変更などが頻繁に発生することからシステム開発のスピードが鍵となります。目まぐるしいシステム開発を遂行しながら、個人情報などの情報管理を厳格に確実に行っていくセキュリティの仕組みを取り込まなければいけません。

従来、企業内のシステムは、セキュリティ向上のためのルールや規定をセキュリティポリシーとして言語化し、その後、システム開発の際に、個別のプログラム処理としてセキュリティポリシーを実装していきます。しかし、セキュリティポリシーが正しく講じられているかを判断できるのは、言語化した内容とこれを実装したプログラムの両方を知りえるセキュリティ管理者のみです。また、例えば、業務の変更や拡張などがあった場合、システムごとに設計、構築、運用が必要となるため、セキュリティポリシーをシステムに反映するために多くの時間が必要となります。

DX 推進が加速するなかで、システム開発において今まで以上に確実なセキュリティ対策を実現するためには、セキュリティポリシーが具体化され、だれでも同じ基準でセキュリティポリシーが活用できる**「透明性」**と、それを素早くシステムに反映する**「迅速性」**が重要なポイントであると言えます。



Enterprise Postgres のセキュリティ

そして、企業のシステムにおいて、大事なデータを管理するのがデータベースであり、データベースにも万全のセキュリティ対策を講じる必要があります。すでに、データベースにおいてもさまざまなセキュリティ機能が提供されています。しかし、例えば、情報漏洩抑止につながるアクセス制御や暗号化など、セキュリティの設計や設定には高度なスキルが必要であり、データベースのセキュリティに関しては、すべてセキュリティ管理者が時間をかけて対応するといった現状が少なくありません。スピードが鍵となる DX において、この現状は、とても非効率的な運用です。そこで、Enterprise Postgres 15 では、前述した「透明性」と「迅速性」に着目し、データベースのセキュリティ運用にこれらを加えることで、簡単かつ確実にデータベースセキュリティを実現するしくみ（機密管理支援機能）を実装しました。

以降では、Enterprise Postgres が行ってきたこれまでの取り組みと Enterprise Postgres 15 で提供した「機密管理支援機能」を解説します。

これまでの取り組み

Enterprise Postgres では、情報セキュリティの３要素である「機密性」、「完全性」、「可用性」の維持を念頭におき、データベースのセキュリティ対策に取り組んできました。特に、「機密性」に関しては、セキュリティ脅威の１つである情報漏洩からデータを守ることに注力した以下の機能が提供されています。

透過的データ暗号化

暗号化アルゴリズムに AES を採用しており、アプリケーションの修正をせずにデータを暗号化・復号することができます。また、暗号化する際の暗号化キーについては、ファイルベースのキーストアだけでなく、クラウド鍵管理システムや Key Management Interoperability Protocol (KMIP)に準拠した外部の鍵管理システムを利用することができるため、暗号化キーの運用管理の負荷を軽減することができます。

- 漏えいに備えよ！PostgreSQL で透過的暗号化を実現

データ秘匿化

データ秘匿化は、アプリケーションによって発行された問合せに対して、一部のデータを改訂して参照させる機能です。例えば、従業員データの問合せに対して、8 桁の従業員番号の最後の 4 桁以外を“*”で改訂して参照させる場合などに利用できます。

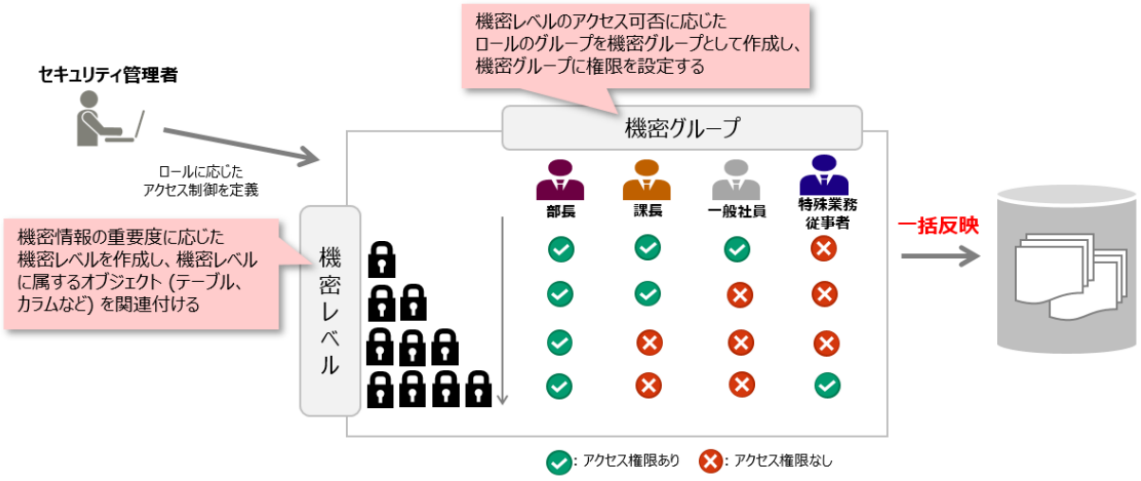
監査ログ

Enterprise Postgres の監査ログは、OSS の pgaudit を拡張した機能であり、データベースアクセスに関するより詳細な情報を監査ログとして取得することができます。また、監査ログは、専用ログファイルまたはサーバログに出力できます。これにより 効率的かつ正確なログ監視が可能になります。データベースに対する不正アクセスや権限濫用などのセキュリティの脅威に対抗できます。

- PostgreSQL の監査ログ ～セキュリティ対策は万全! 監査ログで情報漏えいを検知～

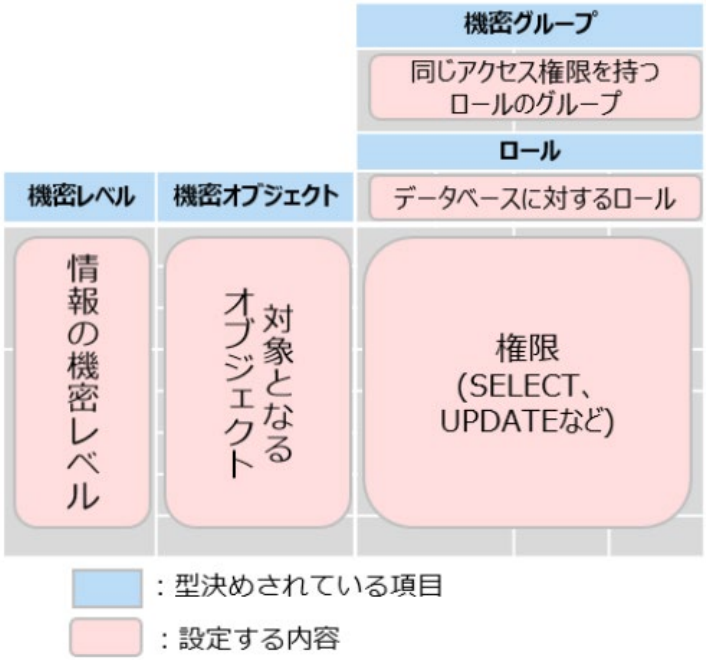
機密管理支援機能を解説

Enterprise Postgres 15 で提供された「機密管理支援機能」は、誰がどのデータをどのようにアクセス可能とするのかといったデータベースへのアクセス制御の設定や運用を支援する機能です。機密管理支援機能を利用することで、あらかじめ、機密情報の重要度に応じた機密レベルと、データベースのロールがどの機密レベルにアクセス可能かを示す機密グループの組み合わせを定義します。その定義に基づいて、データベースに一括してアクセス制御を設定し、また設定した内容を一括管理できます。



通常、このようなアクセス制御は、セキュリティ管理者が 1 件 1 件設定していく必要があり、設定する際もデータベースのセキュリティに関する高度なスキルが必要となります。機密管理支援機能は、企業内でのセキュリティ管理を実現するうえで、「情報の機密性のレベル」や「誰がどの情報をどのようにアクセスできるのか」といったセキュリティポリシーを型決めされたマトリクスの形式で表現できるようにしています。そのマトリクスをデータベースのオブジェクト(テーブル、カラムなど)に関連付けるだけで簡単にデータのアクセス制御が行えます。

以下は、機密管理支援機能が提供する、型決めされたマトリクス(機密マトリクスと呼びます)です。



セキュリティポリシーが変更となった場合は、マトリクスの設定内容を変更すればよく、業務追加などで新たにセキュリティ設定が必要となった場合は、他のシステムのマトリクスを再利用することで、その実績を即座に展開することができます。また自システムとのポリシーの違いをデータベース機能レベルで確認することができます。このように、マトリクスを再利用して容易なセキュリティ設定が可能です。

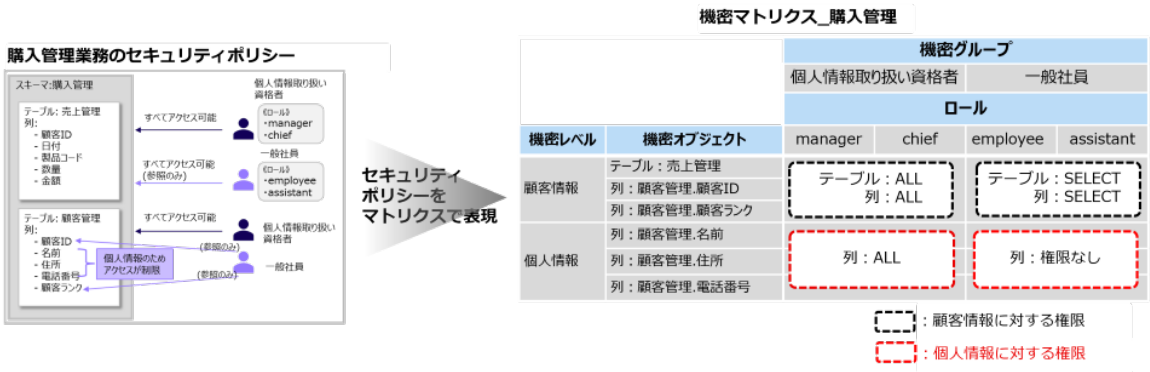
機密管理支援機能は、セキュリティポリシーの設定をマトリクスの形で見える化することで、誰もが同じ基準で簡単に扱える**「透明性」**と、業務変更や追加に対するセキュリティの設定変更に、柔軟かつ素早く対応できる**「迅速性」**を持ち合わせている機能であるといえます。

機密管理支援機能の利用例

ある企業において、商品の購入管理を扱う業務を想定し、機密管理支援機能の利用イメージを示します。

下図の「購入管理業務のセキュリティポリシー」では、業務で扱うテーブルの構成とデータのアクセス可否の関係を示しています。個人が特定できる情報に関しては、アクセスできる人物を限定することで情報漏洩のリスクを最小限に抑えなければなりません。「顧客管理テーブル」の「名前」、「住所」、「電話番号」は、個人が特定可能なため個人情報となります。これに該当する機密度の高い情報を意味する「個人情報」とそれ以外の情報を「顧客情報」として、２つの機密レベルを用意します。また、個人情報は、個人情報をアクセスするための資格を持つロールである「manager」、「chief」がアクセス可能です。「employee」、「assistant」は個人情報を扱うことができないロールであり個人情報以外の情報について参照のみができます。

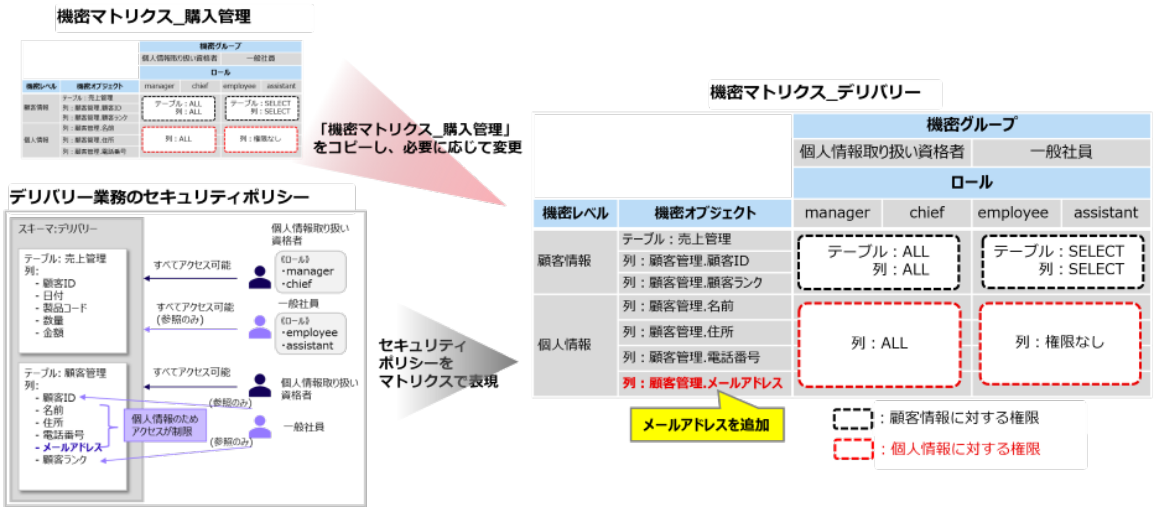
このセキュリティポリシーをマトリクスに当てはめて、データベースのオブジェクトを反映したものが下図の「機密マトリクス_購入管理」です。この機密マトリクスを利用することで、テーブル単位または列単位のアクセス権限が柔軟に設定できます。また、購入管理業務のアクセス制御が一括管理でき、適切な権限を維持することができます。



機密マトリクスの再利用によりセキュリティ管理者の負荷を軽減

DX の過程では、新しいシステムの在り方を模索するために業務の変更や追加が激しく起こりえます。今後はこのような変化が当然のものとなっていくでしょう。例えば、企業が新たな業務を追加する場合、従来は、セキュリティ管理者が初期設定時と同様に、オブジェクトやロールに対して、セキュリティポリシーに則って 1 件 1 件アクセス制御を設定していました。しかし、企業内のセキュリティポリシーは変わらないため、例えば、個人情報に対する扱いは同等であると考えられます。このような場合、機密管理支援機能で作成した機密マトリクスを再利用し、追加業務にあわせてオブジェクトやロール、権限を変更するだけで簡単にセキュリティ設定が行えます。

上記の企業が、新たにデリバリー業務を追加したと仮定します。このとき、デリバリー業務では、顧客の情報として、メールアドレスが必要なので、顧客管理テーブルに「メールアドレス」の列が追加されています。メールアドレスは個人情報であり、アクセス可能なロールが限定されています。デリバリー業務は、購入管理業務と同じセキュリティポリシーなので、購入管理業務で作成した機密マトリクス_購入管理をコピーして、機密レベル「個人情報」に対するオブジェクトとして「メールアドレス」を追加するだけで、デリバリー業務に関するアクセス制御が設定できます。



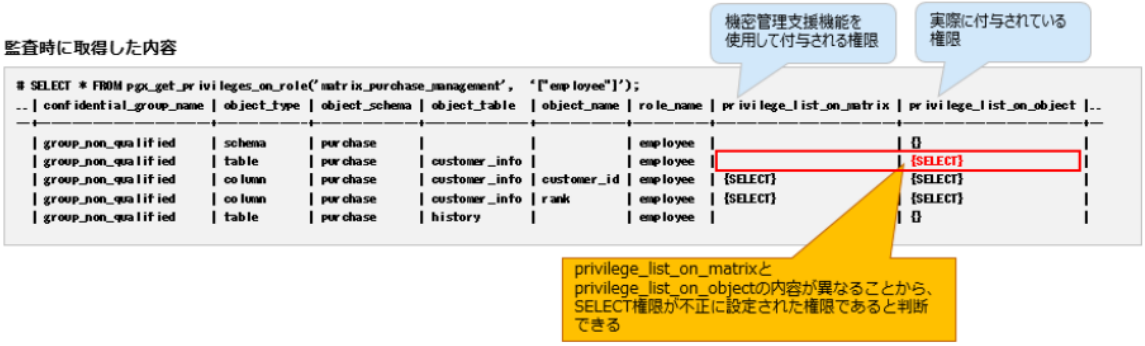
セキュリティ監査の負荷軽減

企業はセキュリティ対策を講じて企業活動を行いますが、意図したとおりに安全にシステムが運用されているかを保証するため、定期的にセキュリティ監査を行う必要があります。その際、監査対象のリソースやロールの数が増えるほどに関係が複雑化し、アクセス制御がセキュリティポリシーに沿っているかの判断も難しくなり、結果として監査のコストがかさんでしまいます。その反面、機密管理支援機能で設定したアクセス制御は、セキュリティポリシーが機密マトリクスに設定されているので、機密マトリクスの内容とデータベースに反映されている実際の設定とを比較することで監査が実施できます。また、機密管理支援機能を使用せずにアクセス権限が設定されてしまった場合も機密マトリクスを利用して不正を検出できます。これらは、機密管理支援機能が提供する関数を使用して実施できるため、セキュリティ監査の負荷が軽減できます。

以下に監査の例を示します。

1) 機密管理支援機能を使用せずに権限付与が行われている場合

機密管理支援機能を使用せずに GRANT 文で権限が付与されてしまった場合は、pgx_get_privilege_on_role()関数を使用することで不正な権限が付与されたことを確認できます。以下の例では、機密管理支援機能を使用して付与される権限と実際に付与されている権限が異なることから、SELECT 権限が不正に付与されたことがわかります。



また、機密管理支援機能を使用せずに、不正な権限の変更などセキュリティ設定に関する操作が行われた場合は、Enterprise Postgres の監査ログ機能を使用することで不正を検知することもできます。

2) 機密管理支援機能を使用して不適切な権限付与が行われた場合

pgx_get_privileges_on_matrix()関数を使用することで、設定されている権限を出力することができます。これを利用して初期設定時の機密マトリクスの内容と現在、データベースに設定されている内容を比較します。以下の例では、初期設定時に設定されていなかった SELECT 権限が付与されていることがわかります。

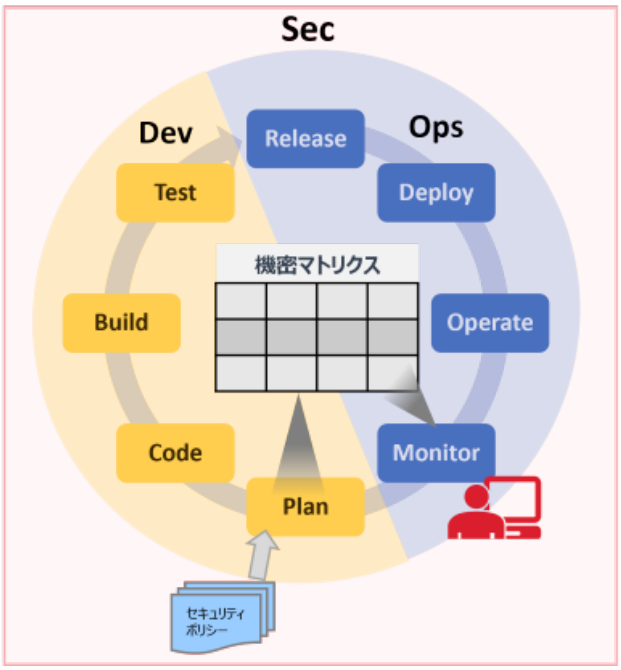
DevSecOps での機密管理支援機能の利用

DX が急務となっている昨今、システムをスピーディーにかつ安全に開発/運用していくことが必須要件となっています。最近では、その要件を満たすためのシステム開発手法として、「開発」、「運用」、「セキュリティ」を融合させた DevSecOps が注目されています。DevSecOps の成功のポイントとして、開発、運用、セキュリティのそれぞれのチーム間の連携を密にし、情報や責任を共有する組織形成が挙げられます。開発のスピードを低下させないために、セキュリティを組織内で内製化することも重要です。

- 【DevSecOps とは？】入門者向けにメリットなどの概要をわかりやすく解説

Enterprise Postgres の機密管理支援機能を DevSecOps で利用することで、この機能の「透明性」により、セキュリティポリシーが組織内で共有でき、「迅速性」により短期間でのセキュリティ対策が実現できます。

例えば、開発工程(Dev)の Plan 工程で機密管理支援機能を利用してセキュリティポリシーを機密マトリクスとして設定します。この機密マトリクスの情報は、機密管理支援機能のシステムテーブルとして管理されています。開発、運用、セキュリティチーム内で共有することで、SQL で設定情報を簡単に参照できます。また、運用工程(Ops)では、機密マトリクスの情報を Monitor 工程で利用する監視ツールの入力として利用することで、不正な権限設定などを検知することが可能です。



DX は、デジタル技術を活用した企業の変革により多くの価値をもたらします。一方で、クラウドの活用やシステム開発の短期化などビジネス環境が変化しており、それに伴うセキュリティリスクも大きくなっています。このような環境下での DevSecOps の適用はとても効果的です。DevSecOps を進めていく中で Enterprise Postgres のセキュリティ機能を活用することで、万全なセキュリティ対策を講じながら迅速なシステム開発が可能となります。DX を成功させる鍵として、DevSecOps にも最適な Enterprise Postgres の利用をぜひご検討ください。

2023 年 4 月 21 日