

SnowVillage データマネジメント分科会

SnowVillage データマネジメント入門講座 第3回

データガバナンスって結局なに？

2026.7.9



世界水準の知見を、貴社の「最短成功」のエンジンに。

世界が認めるスペシャリスト × 圧倒的な機動力 で提供するエクスチュア価値

喜田 紘介 (Kosuke Kida)



世界が認めるスペシャリスト - Snowflake Data Superheroes

Snowflake によるグローバルでの認定を受けたスペシャリスト

世界100名・日本13名、Snowflakeおよび製品を問わない技術領域へ深い知見を有し、製品の魅力発信、文化の醸成、製品開発チームへ直接フィードバックを行うSnowflakeの「体現者」です。

マルチな技術・文化貢献

深い製品知見だけでなく、コミュニティを通じた文化醸成、最新技術トレンドまで最速でキャッチアップしお客様に提案します。

ビジネス×エンジニアの架け橋

「技術的に可能か」だけでなく「ビジネス価値を生むか」の視点を両立したハイブリッドな対話をお約束します。

「ゼロから1ヶ月」で成果を出す、超高速データ基盤構築

即興型プロトタイピング

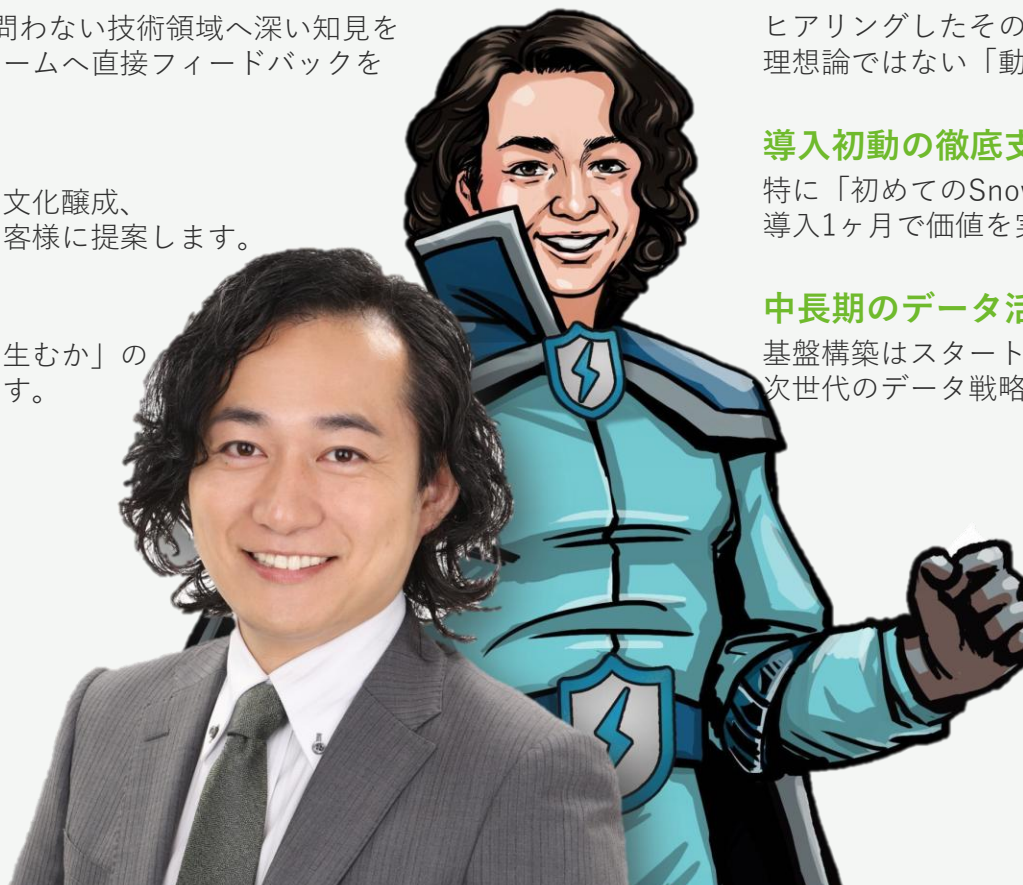
ヒアリングしたその場で、最新機能を用いた解決策を構築・提示、理想論ではない「動くもの」で議論を加速します。

導入初動の徹底支援

特に「初めてのSnowflake/データ基盤」に特化。導入1ヶ月で価値を実感させる独自の最短ルートをレクチャ&伴走します。

中長期のデータ活用へコミット

基盤構築はスタート地点です。AIとデータ活用を現場に普及させ、次世代のデータ戦略の立案まで、ビジネスの成長に継続的に寄り添います。



今日のゴール

脱・曖昧なイメージだけの言葉、データガバナンスとは何か腹落ちさせましょう！

データガバナンスってどんなイメージ？



- ❑ データ基盤PJではいつも出てくる
- ❑ ちゃんとしてなきゃヤバそう
- ❑ 製品発表でもいつも出てくる
- ❑ なんか安心感がありそう



- ❑ 自分の仕事にどう関わるの？
- ❑ 誰が整備するの？
- ❑ 何ができてれば良いの？
- ❑ Snowflakeの機能で言うと結局なんなの？

データガバナンスとは

- 言葉の意味・歴史
- DMBOKとのマッピング
- 実務とのマッピング

ガバナンス腹落ち編 — データベースエンジニアの視点から

- データベースの責務
- 新しく生まれた統制のためのレイヤー

Snowflakeのガバナンス 2026

- 認証
- 行列レベルの制御
- タグと自動分類
- Trust Center
- 新しいガバナンス (Iceberg、Agent)

Chapter 1. データガバナンスとは

まず「ガバナンス」という言葉

ガバナンス＝統治。データガバナンスはコーポレートガバナンスをデータに広げたもの

英語で governance: 統治・統制

- 誰に権限があり、どう意思決定し、誰が説明責任を負うか
- コーポレートガバナンス: 取締役会・監査など、企業を律する仕組み



たくさん稼ぐことを良しとするけど、それよりも、「悪魔に魂を売ってはいけない」を優先ルールとする

データガバナンス: この統治の枠組みを「データという資産」に拡張したもの

- 1970年代～「データ／情報は企業価値を左右する資産」という認識が芽生えた
- 学術的にも「意思決定権と説明責任の枠組み」と説明される (Khatri & Brown, 2010)
- HIPAA (1996)、SOX法 (2002)、EU GDPR (2016)
- Data Governance Institute設立 (2003頃)
- DMBOKによる体系化



データは活用せよ。
誰でもデータを活用できるよ！
でも、目的外利用も操作ミスも許さん。
仕組みで守っているから安心してね！

DMBOKの全体像とデータガバナンスの位置

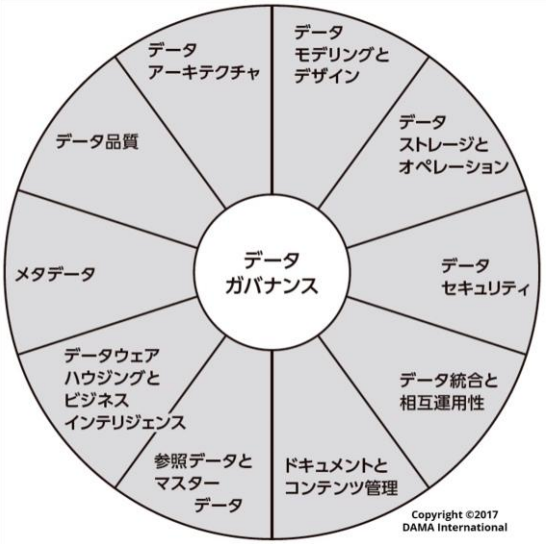
DMBOKではデータガバナンスが車輪の中心（ハブ）に置かれる

DAMAホイール: 中心1 + 周辺10 = 全11の知識領域

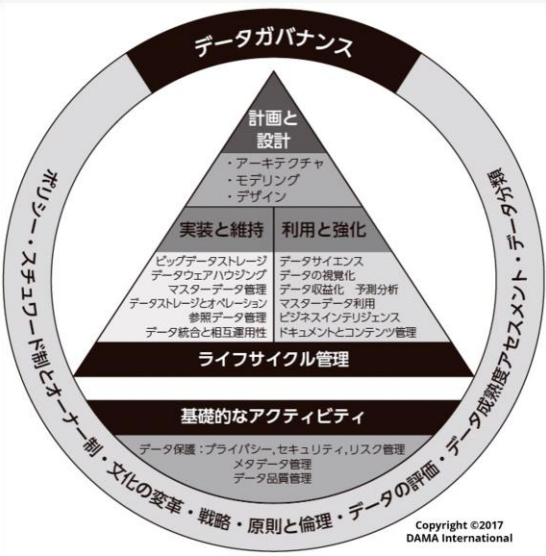
- データガバナンスは中心に位置する
- 全機能を横断的に統制し整合を取る役割だから

データガバナンスの定義（第3章 データガバナンスより引用）

- データ資産の管理（マネジメント）に対して職務権限を通し統制（コントロール）することである



意訳：デタマネを成功させるための以下の取り組みを「データガバナンス」とする



・出所：『データマネジメント知識体系ガイド 第二版』 DAMA International編著、DAMA日本支部、Metafindコンサルティング株式会社 監訳、日経BP

命綱としてのガバナンス≠アクセスを閉じて自由度を下げるもの

ガバナンスは自由を縛る鎖ではなく、安全を保障することで安心してデータを活用するための命綱

データの目的外利用・不正を防ぎつつ、活用を推進するための取り組み



売上をあげる/ビジネス成果を出すことを
目指す組織に権限を渡す



事故を起こさせないことを目的とする組織
(旧来のセキュリティ部門など) が主導しない



品質・整合性・コンプライアンス確保など
DGOと業務部門で合意して進める

似た意味で使われがちな用語の整理



用語	つまり何？
データガバナンス	セキュリティ対策を正しく実装することも含めた、健全なデータ活用を推進するためのあらゆることを計画して実行。 セキュリティ以外では、それをどういう体制で維持していくのかの組織論や、データ基盤やプロダクトの活用度の測定・監査などが含まれる。
セキュリティ	情報セキュリティのCIA（機密性、完全性、可用性）や業務要件（クレジットカードのPCI規格）のような要求と、それを侵害し得る攻撃手段やリスクを整理し、対策（各プロダクトが備える機能）を駆使して要求を満たすこと。 セキュリティ対策の一環として認証・認可や監査を適切に実装するなど。
認可/権限	データにアクセスしてよし！
認証	ログインしてよし！

実務で見るガバナンスの構成要素マップ

実案件では「発見・分類・保護・品質・監視・統制」に分解できる

機能名と1対1にならない概念も、「問い」に分解すると実装に落ちる
どれか一つではなく、これらの束＝ガバナンス

要素	問い	代表的な機能例
カタログ／発見	どこに何がある？	データカタログ・検索・リネージ
分類	機密度は？	データ分類・タグ付け
アクセス保護	誰が見てよい？	RBAC・行/列制御・マスキング
品質	信頼できる？	データ品質モニタリング
監視／監査	守られている？	アクセス履歴・監査・Trust Center
コンプライアンス	規制に適合？	ポリシー・差分プライバシー

Chapter 2. ガバナンス腹落ち編

— データベースエンジニアの視点から

データベースの根本の責務とは

純粋なDBの責務は「物理最適化・論理抽象・権限制御」の3つ

①物理層の最適化

- テーブルフォーマット、インデックス検索
- CPU/メモリ/ディスクを協調させる低レイヤ技術

②物理を意識させない論理層

- スキーマ・テーブルとSQL（非手続き型）
- 厳格なトランザクションでデータの姿の曖昧さを排除

③権限制御とユーザー／ロール管理

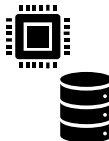
- SQL標準の `GRANT` / `REVOKE`（一般にテーブルへのアクセスまで）



- SQL：アプリ側の言語を問わない汎用インターフェース
- ユーザー認証、権限管理



- 物理層を抽象化するスキーマ/テーブル
- トランザクションによる曖昧さの排除



- データ格納
- データへのアクセス方式
- CPU/メモリ操作

権限管理はSQL標準で定められている

GRANT/REVOKEは1970年代から。行・列単位は比較的新しい

委譲モデルの起源: IBM System R

- Griffiths & Wade (1976) が理論基礎。所有者ベース + GRANT OPTION は今も不変

-- SQL標準の権限制御 (1970年代 から変わらず)

```
GRANT SELECT ON sales TO analyst_role;
```

```
REVOKE SELECT ON sales FROM analyst_role;
```

行・列レベルは標準ではなく、製品固有・後発の機能

- Oracle VPD (8i, 1998) / SQL Server RLS (2016) / PostgreSQL RLS (9.5, 2016)

旧来のシステム開発では1アプリ = 1DB

1システムのための専用DB、DB上の1ユーザーがその業務の多くのテーブルの権限を持つ

Oracle **CREATE SCHEMA**: アプリ用ユーザーとスキーマが1:1の世界観

- 人事管理システムのDBユーザー = スキーマ「hr」
- 受注システムのDBユーザー = スキーマ「oe」

アプリ側でユーザー認証・アプリ内ロール判定

- 個人が各自の権限でデータそのものにアクセスする想定は薄かった（全員がHRユーザー）
- 人事担当者はアプリ内の人事ロールで全部門のデータを確認
- 営業部マネージャーはアプリ内の営業MGRロールで自部門のデータを確認
⇒ **WHERE dept = 'sales'** をアプリ側の責務で実装

権限管理の主役はアプリ開発/IT部門（Oracle DBAの責務）

- アプリ内権限はアプリ開発部門の責務
- OracleDBAは認証やDBに対する直接的な不正アクセスの対策



- 人事管理アプリケーション
- アプリ側でログインした人を識別
- ユーザーHRでOracleに接続



- アプリの認証を通ってきた人はすべてHRユーザー
- HRスキーマのテーブルをすべて見れる

現代のデータ基盤：集約と新しい問題

DB集約でサイロは壊れたが、「誰に見せるか」を実態に合わせて適切に管理するには機能不足だった

多数の業務システムがデータソース化し、1つの基盤に集約された

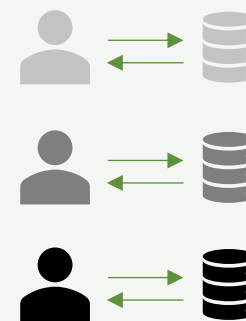
- 利点: サイロ破壊。必要な人が目的に応じて使える

新たな課題: 必要な人は誰か、不要な人には見せない、誰が判断するか

- 権限管理が組織の利害・責任分担にまで発展する

オーナーシップの移動: IT部門 → データを預けた各部門

- 各部門にリテラシーがなく、従来のDB製品にその機能もなかった



- データ基盤にデータを集約
- 各業務部門がデータを所有
- 誰に見せるか、誰に見せないか
- それを制御する人は誰か
- データ基盤で個人を識別

1か所にデータが集まったことで
データベース（データ基盤）に期待する
権限管理のレイヤーが増えた

生まれた新しい層：統制／カタログ層

物理・論理層に加え「統制／カタログ層」が新たに生まれた

データと不可分な「統制/カタログ層」が必要になった

- 簡単・明快なUIを備えリテラシーを要求しない
- 各データオーナー部門が自分のデータを自分で管理できる
- 従来データベースから見るとアプリケーション領域をデータ基盤SaaSがカバーした

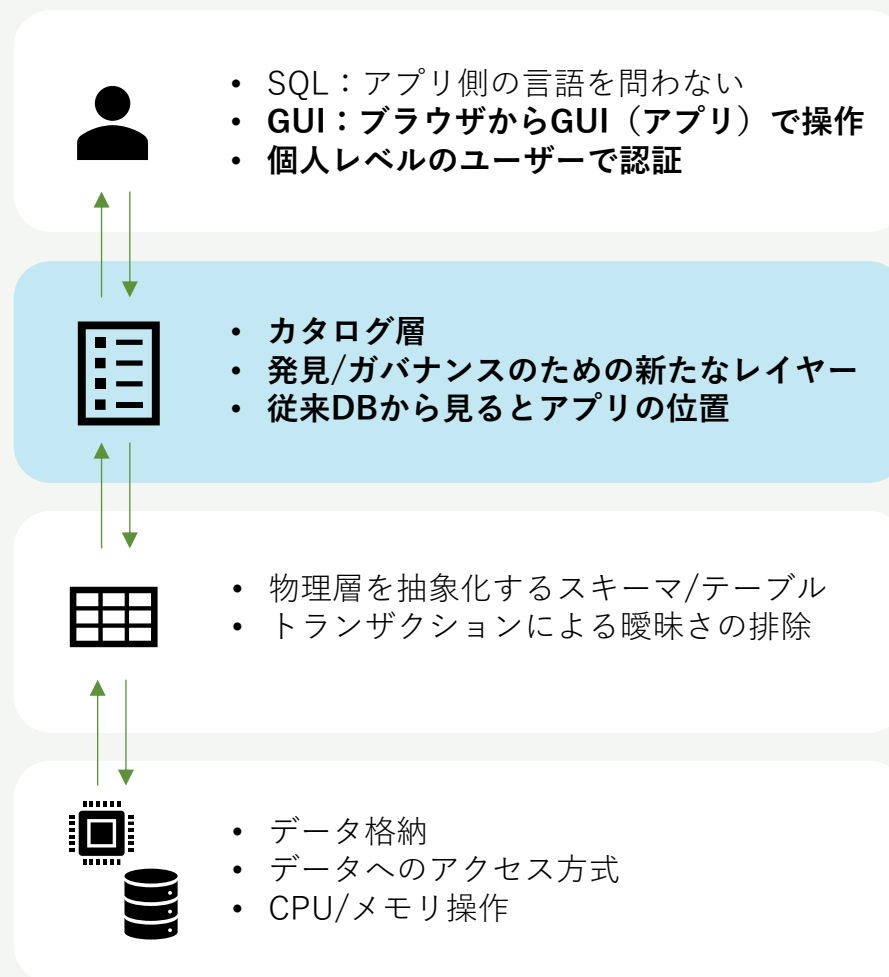
意味が広がり、2つの顔を持つ

- 守るべきものが守られている保証＝「統制（ガバナンス）」
- 見えるべきものはもれなく見える＝「カタログ」

高度な実装例

- **Snowflake Horizon Catalog**：腹持ちしたデータの統制から進化
- **Databricks Unity Catalog**：外部データレイクの接続・発見から進化

※両製品とも、権限管理・発見に加え、リネージ・監査・AIのためのコンテキストなどデータ管理に必要な付加的な情報を一元管理する新たな層として進化



Chapter 3. Snowflakeのガバナンス 2026

Snowflake Horizon Catalog

Horizon Catalogはデータガバナンスの実践のための機能群を包括的に提供する「メタアプリケーション」

データガバナンス実践のためのあらゆるルール適用をアプリではなくデータ基盤側で実行する

- 従来の3層アプリではユーザー権限判定と機能の出し分けはアプリ側の責務
- データベース側でモダンかつ完全な形で提供している
 - ✓モダンな管理対象
 - ✓すべてSQLネイティブに実装（CREATE、POLICY、PROCEDURE、GRANT/REVOKE）
 - ✓ユーザーフレンドリーなUI
AIフレンドリーなAPI/Skillでも定義可能

Snowflake内外のデータ／AI資産を対象

- エンタープライズのユニバーサルAIカタログ（Snowflake Summit 2026）

機能群	例
発見	ユニバーサルサーチ、データリネージ
分類／タグ	データ分類、オブジェクトタグ
保護	RBAC、行アクセス、マスキング
品質	データ品質（DMF：Data Metric Function）
監査／監視	Query History、Trust Center、Global Account
Context	Semantic View、Cortex Sence
App	Viewer URL、Restricted Caller’s Right
AI	AIガードレール・Agent統制

土台：認証・認可とRBAC

認証・認可とRBACがすべての土台（全エディションで標準）

アクセス制御:

- SnowflakeはRBAC（ロールベースアクセス制御）
- 主要なアクセス制御手法には以下があり、管理対象の特性に応じて最適解は異なる
 - DAC：ダイレクトアクセス制御（Googleドライブなど）
 - ABAC：属性ベースアクセス制御（部署、端末による判定）

認証:

- パスワード／SAML(SSO)／OAuth／キーペア／PAT、MFA（パスキー・TOTP）

RBACベストプラクティス:

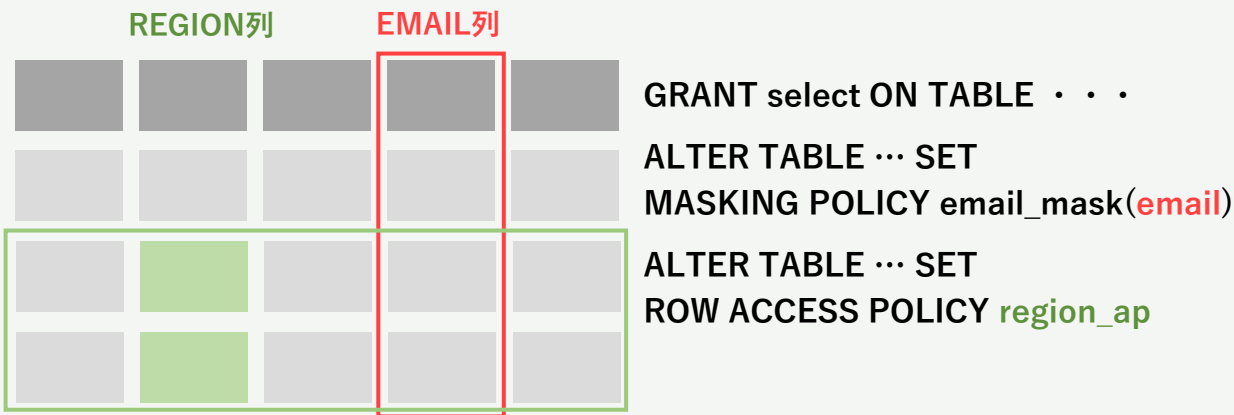
- ドメインのデータプロダクト単位で、同じ粒度のロールを切る
- [Blueprint Manager](#)でベストプラクティス構成をなぞって設計～実装可能

RBACの発展：テーブル単位よりさらに細かい行・列レベルの権限管理をポリシーで定義

行・列レベルの制御がポリシー/タグを組み合わせることで「もれなく」適用できる（Enterprise以上）

動的データマスキング:

- クエリ時にロール／コンテキストを判定
 - ✓ 特別なコンテキストを持たなければマスク
 - ✓ バイパス設定（CASE）に当てはまる場合のみ平文
- 保存データは不変。External Tokenization も選択可



行アクセスポリシー:

- 行ごとの可視性を SELECT/UPDATE 等で判定
- マッピングテーブルに詳細な条件を定義
 - ✓ entitlementsテーブルには、どのロールがどのリージョンを見れるか定義している
 - ✓ 列内の値のパターンと強く紐づくため、タグベースでの自動適用は現時点では不可
- 保存データは不変。

```
-- 列マスキング：ロールに応じて出し分け
CREATE MASKING POLICY email_mask AS (val STRING)
RETURNS STRING ->
CASE WHEN CURRENT_ROLE() = 'PII_READER' THEN val
ELSE '***MASKED***' END;

-- 行アクセス：担当リージョンの行だけ見せる
CREATE ROW ACCESS POLICY region_ap AS (region STRING)
RETURNS BOOLEAN ->
EXISTS (SELECT 1 FROM entitlements
WHERE role = CURRENT_ROLE() AND allowed_region = region);
```

タグベースでデータベース内のすべての同種の列に効かせる

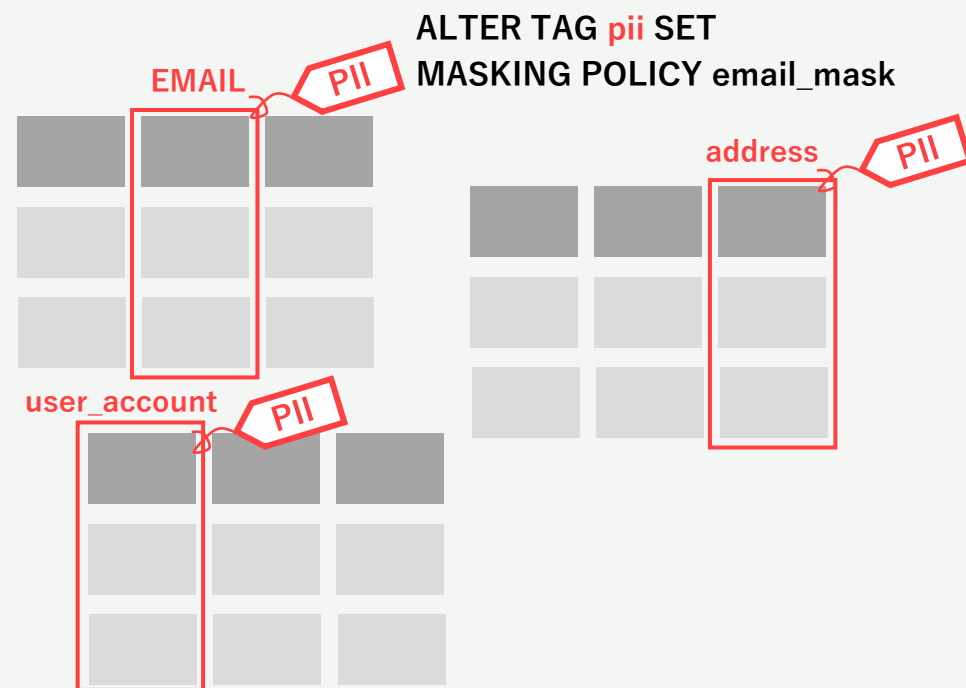
タグにポリシーを紐づけ、一度の設計を多数へ自動適用

タグベースマスキング:

- マスキングをタグに割り当て → タグ付与で型一致の列を自動保護
- 「一度書いて一度割り当てる」で大規模運用 (Enterprise)

タグ使用状況の可視化:

- ACCOUNT_USAGE のビューで継承・自動伝播も追跡できる



```
-- タグにマスキングポリシーを割り当て
ALTER TAG governance.pii SET MASKING POLICY email_mask;

-- 列にタグを付けるだけで保護が伝播する
ALTER TABLE customers MODIFY COLUMN email
SET TAG governance.pii = 'EMAIL';

-- タグの使用状況を確認
SELECT * FROM SNOWFLAKE.ACCOUNT_USAGE.TAG_REFERENCES;
```

UIで簡単・高度に：分類とタグ管理

データ分類とタグ管理はSnowsightのUIから高度に行える

データ自動分類（Automatic Classification）：各列に2種のカテゴリを付与

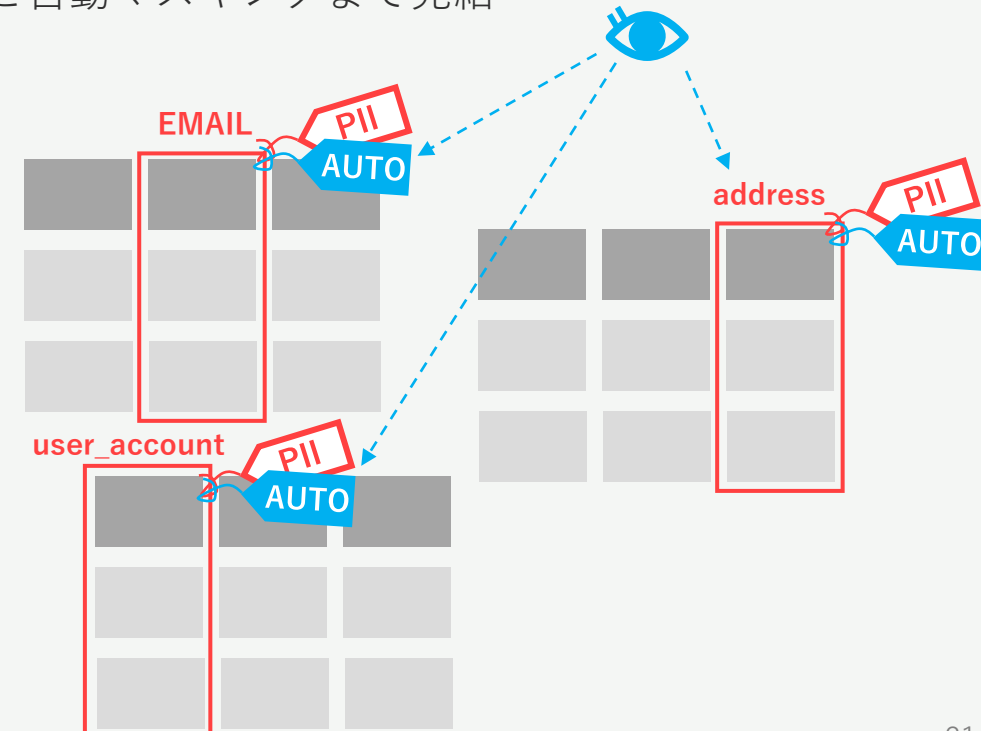
- スキーマ指定ですべてのテーブル/列を検査し、センシティブかどうかを判定
- SEMANTIC_CATEGORY（氏名・住所など"種類"）と PRIVACY_CATEGORY（"機密度"）
- 自動分類に加え、正規表現でカスタム分類も定義できる（Enterprise）
- 自動分類タグをユーザー定義のマスキング用タグにマッピングすると自動マスキングまで完結

タグ管理:

- 付与・継承・自動伝播をUIとビューで一元把握
（1オブジェクト最大50タグ）

意義:

- データオーナー部門が、SQLを書かずに自分のデータを統制できる



守られている保証：Trust Center

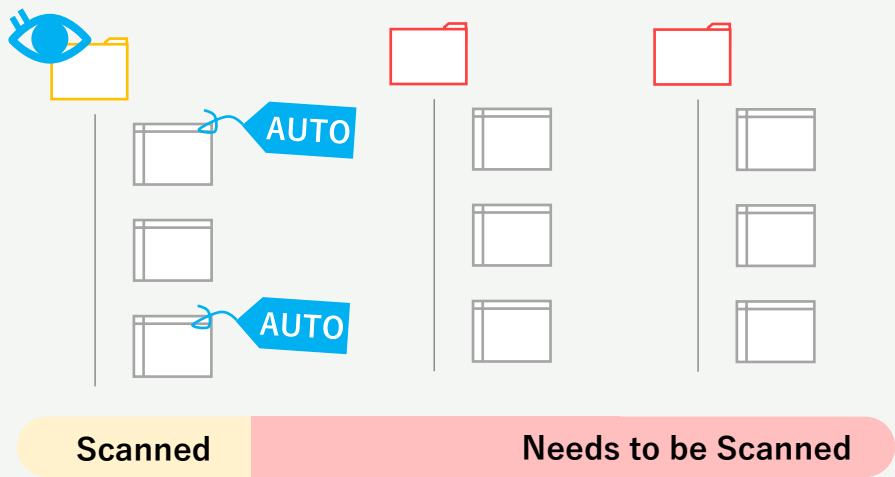
Trust Centerで「守られていること」を継続的に監視する

リスクを評価・監視・低減し、findings を継続生成（違反／検知）

- Snowsight「Governance & security ≧ Trust Center」から確認でき、SQLは不要

2026年の動き：

- Data Security が GA（2026-04）



- Summit 26で AI Security Posture Management (PuPr)

スキャナ	内容	状態
Security Essentials	MFA／ネットワーク等の推奨	GA（既定）
CIS Benchmarks	CIS基準による評価	GA
Threat Intelligence	ログイン異常・リスク検知	GA
Data Security	機密データの自動分類・保護状況	GA（2026-04）
AI Security	AI／エージェントの姿勢監視	Public Preview

広がるガバナンス①：外部データ（Iceberg／Lakehouse）

外部データ（Open Table Format）にも統制を広げる

Iceberg などのオープンテーブルにも Horizon のガバナンスを適用

- 認証・ロール・行/列ポリシーを保ったまま、外部エンジンに開放

Polaris（Apache, Iceberg REST）＝オープンな技術カタログ、そのマネージドが Open Catalog

- 「Enterprise Lakehouse」構想:
- 単一データコピーで安全にアクセス

項目	内容	時期
Iceberg V3	行リネージ等に対応	GA 2026-05
外部エンジン読取	Spark等からHorizon経由で	GA 2026-02
Open Catalog	Apache Polarisのマネージド	提供中

広がるガバナンス②：Agenticエンタープライズ

Agentic時代は、エージェント自体を統制の対象にする

原則: エージェントはログインユーザーのIDと権限を継承し、それを越えられない

- 行／列／マスキングが全操作に自動適用される（既存RBACを再利用）

3層セキュリティフレームワーク: データ層／モデル層／エージェント層

- Cortex Guard／AI Guardrailsで有害応答・プロンプトインジェクションを防止

Agent Identity（検証可能なIDと監査）

- Agent情報をセッションコンテキストに埋め込み可能になる（**CURRENT_XXX()**にAgent情報が入る）
- マスキングポリシーの定義内にPerson/Agentの分岐を入れて結果を出し分ける

今日のゴール

脱・曖昧なイメージだけの言葉、データガバナンスとは何か腹落ちさせましょう！

データガバナンスってどんなイメージ？



□ データ基盤PJではいつも出てくる

- ✓ コーポレートガバナンスとか、コンプライアンスとかと同列データの世界でやるべきことをやろう！

□ ちゃんとしてなきゃヤバそう

- ✓ DMBOKに沿ってやり切るハードルはかなり高い
- ✓ DMBOKに沿わずとも製品機能を知り最低限の設定をしよう

□ 製品発表でもいつも出てくる

- ✓ 現代のデータ基盤の最上位で見るべき機能群、当然！

□ なんか安心感がありそう

- ✓ 製品マーケでは理想を語るの、これだけで安心感がすごい
- ✓ 実運用をやりきるのは大変だけど、ひと昔前と比べたら充実



□ 自分の仕事にどう関わるの？

- ✓ Snowflakeに関わる全てのエンジニア、ユーザーが関わっている

□ 誰が整備するの？

- ✓ 教科書的には責任者を置き組織運用でやりきる！
- ✓ 実態はSnowflakeに詳しいデータエンジニアが救世主となるか

□ 何ができてれば良いの？

- ✓ 最低ラインは実態にあわせたロール設計～運用
- ✓ 個人情報を扱うならカスタム分類など便利機能をまずやる

□ Snowflakeの機能で言うと結局なんなの？

- ✓ UIで提供されるほとんど全部がガバナンスの活動につながる

- DMBOK: DAMA-DMBOK2 (damadmbok.org)、Snowflakeのdama-dmbok解説
- 用語史・定義: DATAVERSITY／EWSolutions、Khatri & Brown (2010)
- DB技術史: Codd (1970)、Griffiths & Wade (1976)、Oracle／Microsoft／PostgreSQL公式史
- Snowflake: docs.snowflake.com (Horizon／Trust Center／Classification／Iceberg／Cortex)
- Summit 2026プレスリリース

Data to the People

すべての人にデータを