# GxP 環境における Teradata Vantage のガイドライン

## 目次

# 概要

このドキュメントでは、GxP 規制環境下での Teradata Vantage の使用を計画されている顧客に透明性を提供します。GxP ガイドラインに準拠するためにテラデータが採用している手順を説明しています。このドキュメントの説明は、電子記録の要件をサポートするために使用できます。規制基準やガイダンスの参照および詳細は、議論の枠組みとして提供するものですが、顧客やその他の事業者に対する法的助言の役割を果たすものではありません。

GxP は、米国ではアメリカ食品医薬品局 (FDA) によって制定され、さまざまな基準を網羅しています。

- G – 「良い」を意味します
- x – アプリケーションによって異なります
- P – 「プラクティス」を意味します

GxP とは、品質に関して世界的に受け入れられている現在の「グッド プラクティス」を指します。GxP には以下が含まれます:

- グッド・マニュファクチャリング・プラクティス(GMP)
- グッド クリニカル プラクティス (GCP)
- グッド ラボラトリー プラクティス (GLP)
- ファーマコビジランス基準 (GPVP)
- グッド エンジニアリング プラクティス (GEP)

テラデータは、GxP ガイドラインによる直接的な規制を受けていませんが、GxP に準拠する必要のある当社の顧客をサポートしています。このドキュメントは、テラデータのクラウドサービスプロバイダー (CSP)、製薬、医療機器、製造業の顧客との経験に基づき作成されたものです。また、テラデータと顧客の間で共有される責任についても説明し、明確にします。

GxPs に加え、テラデータは、ライフサイエンスや製造業の顧客の事業活動が、米国食品医薬品局 (FDA) や欧州医薬品庁 (EMA) など、各国および世界の保健当局の規制を受けていることを認識しています。多くの企業は、Title 21 CFR Part 11 や Annex 11: Computerized Systems Validation などの規制の対象となっています。このような規制は、新しい技術が電子 GxP データの機密性、完全性、可用性をサポートしているかどうかを顧客が評価するための枠組みを提供します。GxP 規制の対象となる顧客は、そのシステムが GxP コンプライアンス、および 21 CFR 11 に準拠していることを評価、運用、検証する責任があります。

# Teradata Vantage

## システムの説明

Teradata Vantage は、エンタープライズ分析に適したコネクテッドマルチクラウドデータプラットフォームです。Vantage は、分析ツール、言語、およびエンジンを統合して、顧客データから洞察を提供します。Vantage を通じて、テラデータはプラットフォームのパフォーマンス、セキュリティ、可用性、および運用を管理します。詳細は CSD (Cloud Service Description: クラウドサービスディスクリプション) に記載されています。このドキュメントでは、Vantage はソフトウェアとテラデータの運用担当者が行う活動の組み合わせと見なしています。運用には、顧客が選択したリージョン内のコンピューティング インスタンス、ストレージ、および追加のクラウドサービスプロバイダー (CSP) リソースの構成と管理が含まれます。Vantage は、テラデータが所有する CSP アカウント内の専用のプライベート仮想ネットワークにデプロイされます。Vantage は、CSP から物理インフラストラクチャとネットワーク セキュリティを受け継いでいます。

| アプリケーション | オプションのアプリケーション |
|---|---|
| Teradata Advanced SQL Engine | Teradata Data Lab |
| Teradata Query Service | Teradata QueryGrid |
| Teradata Data Mover | |
| Teradata Viewpoint | |
| Vantage Analyst | |
| Vantage Editor | |

表 1: Teradata Vantage コンポーネント

# テラデータの組織とガバナンス

テラデータは、品質コンプライアンスの文化を保証する厳格なガバナンス手順を維持しています。これは、エンジニアリングにおける数十年にわたるソフトウェア開発ライフサイクル (SDLC) の一環として取り組んでいます。品質ガバナンスは、ポリシーの文書化、ソフトウェア保証プロセス、品質指標にまでおよびます。これにより、テラデータの内部および外部監査の継続的な成功が容易になり、保証されます。

## サプライチェーンのセキュリティ / レジリエンシー

テラデータは、Vantage のセキュリティ要件を特定するサプライチェーン セキュリティ プロセスを文書化し、実装しています。サプライヤーは、テラデータに販売する製品およびサービスの原産国を明確化する必要があります。Teradata Global Security は、Vantage のセキュリティを危険にさらす可能性のある機能について、サプライヤーの提供内容を確認します。テラデータはまた、サプライヤーにサプライチェーンの配送における潜在的なリスクを明確化することを要求しています。Teradata Global Security では、コンポーネントが予測される範囲で利用可能であることを求めています。これには、予測期間内の交換部品も含まれます。

## 事業継続計画

テラデータには、Vantage 製品に関する事業継続計画 (BCP) を文書化し、実施しています。この計画は、災害後に発生する可能性のある収益や業務統制の喪失のリスクを軽減するものです。BCP は、予期しない災害が発生した場合に、テラデータの復旧プロセスを指示するものです。業務の復旧や重要な業務システムの復旧も対象としています。

テラデータの事業継続マネジメント (BCM) は、危機から回復するために各機能エリアを統括し、重要なプロセスを復旧する能力を提供します。局所的な危機と重要なプロセスの復旧のリカバリープランは、BCM と機能領域を担当するシニアマネジメントによって策定されます。テラデータ全体に影響を与えるビジネス機能およびシステムの復旧計画は、BCM の責任であり、企業全体の事業継続計画で対処されるものとします。BCM では、ローカルプランの作成を全体的に監督してリーダーシップとガイダンスの実践、さまざまなビジネス依存の間での適切な一貫性と調整の保証、国際標準への準拠が必要となります。

# Vantage プラットフォームのセキュリティ

顧客は、ユーザーアカウントと Vantage インスタンスへのアクセスを管理することで、データへのアクセス を制御します。テラデータが顧客データにアクセスできるのは、顧客が明示的に要求し、許可した場合のみです。Vantage をサポートするインフラへのアクセスはテラデータが管理しています。テラデータは、顧客のデータを機密情報としてあつかいいます。テラデータが共有責任の一部をどのように管理しているかを以下に挙げます。

## アクセス制御

Teradata Cloud の運用およびサポート担当者は、Vantage Cloud インフラストラクチャにアクセスする前に、トレーニングを完了し、セキュリティ契約に署名する必要があります。テラデータは、パスワードの複雑性を適用し、最小および最大の有効期間制限を設けています。パスワードには、保管時および送信時に強力な暗号化処理がされます。テラデータの担当者は、顧客からの指示がない限り、顧客のデータにアクセスしたり、国を超えて転送したりすることは決してありません。

再承認は、標準のセキュリティ プロセスです。これにより、資格情報やアクセス許可の定期的な見直しが行われるようになります。テラデータでは、社員に対して、以下の項目で構成される厳格なセキュリティ再承認プロセスを採用しています。

- リモートデバイスからクラウドへのアクセスは、VPN と多要素認証が必要です。
- システムへのアクセスはログに記録されます。ログは中央のサーバーに送られ、改ざんされないように保護されます。ログ データは常に集計され、分析されます。
- アカウント管理のアクションはレビューと、承認のプロセスを受けます。
- アカウント管理の操作は、不正なアクションに備えて監視されます。
- 非アクティブなアカウントは 90 日後に無効になります。
- Vantage アカウントは、従業員が異動または解雇された場合に無効になります。
- 役割に紐付くアクセスは、従業員の使用状況や知るべきことの要件の変更に連動して更新されます。

## 監視

Vantage のセキュリティ監視プロセスは、関連するセキュリティ ポリシー イベントを収集して集約します。Vantage システムは、ログイン失敗、アカウント作成、アカウント削除、システムポリシー変更、特権アクセス、IPS などのイベントを記録します。セキュリティ情報およびイベント管理システム (SIEM) は、ログファイルを取り込みます。その後、SIEM はそれらをほぼリアルタイムで関連付けて分析します。SIEM のログファイルデータベースは、安全で改ざんされない場所に保存されます。データ イベントは、セキュリティ上重要な機能、新たな脅威、潜在的なセキュリティ インシデントについて監査されます。

## 脆弱性管理

テラデータは、Vantage の運用環境とコードを定期的にスキャンして脆弱性を特定し、是正を図ります。これには、ソフトウェアとオペレーティング システムが含まれます。これは、アプリケーション セキュリティ分析とネットワーク分析を組み合わせたものです。

## 暗号化

Vantage に保存されたすべての顧客データは、CSP のインフラストラクチャ レベルで保存時に暗号化されます。ストレージ ボリュームの暗号化キーは、オプションとして顧客による管理ができます。これには、CSP 提供のハードウェアセキュリティモジュール (HSM) をキーヴォルト アーキテクチャに追加することが含まれます。また、Vantage と接続クライアント間のデータ転送を TLSv1.2 で暗号化するオプションを推奨、提供しています。顧客および CSP のインフラでサポートされている場合、MACsec と IPsec のプロトコルが利用可能です。また、テラデータのパートナー企業による拡張サードパーティ暗号化ソリューションも利用可能です。

| トピック | アクティビティ | テラデータ | 顧客 |
|---|---|---|---|
| **システム セキュリティとアクセス管理** | 暗号化: 移動中の顧客データ | CI | RA |
| | 暗号化: 顧客の保存データ | RA | |
| | ネットワーク セキュリティ、ファイアウォール、侵入検知ソフトウェアの実装と管理 | RA | |
| | ウイルス検出の展開/管理 | RA | |
| | パスワード制御、RBAC、多要素認証、休眠アカウントの無効化 | RA | |
| | Vantage システムの廃止 | RA | CI |
| **オペレーティング システムの管理** | OS のセキュリティ監視 | RA | |
| | OS ボリュームの暗号化 | RA | |
| **ネットワーク管理** | Vantage への受信トラフィックの制限/フィルタリング | RA | |
| **クラウド管理** | Vantage プラットフォームのセキュリティ監視 | RA | |
| | テラデータ担当者のクラウド アクセス管理 | RA | |

**R** – Responsible (責任)　**A** – Accountable (説明責任)　**I** – Informed (通知)　**C** – Consulted (相談)

表 2: 責任の共有: Vantage のセキュリティとアクセス管理

# データベース管理

## データガバナンス

データ ガバナンスは、顧客のビジネス プロセスです。部門のデータ所有者は、データの品質、使いやすさ、一貫性を管理します。データ スチュワードは、データを管理し、対象分野の専門家を特定します。また、スチュワードはデータ カタログやマスター データ管理ツールを導入し、データの監視を強化します。データ ガバナンスは、GxP に不可欠なのは明白です。目標は、データの信頼性を維持し、説明責任を果たすことで、リスクとセキュリティの懸念を軽減することです。データマネジメント ソフトウェアも有効ですが、ガバナンスは事業部門単位で行うものです。

| トピック | アクティビティ | テラデータ | 顧客 |
|---|---|---|---|
| **データベース管理** | データベースのユーザーとオブジェクトの管理 (作成、権限、トラブルシューティング) | | RA |
| | データベース システムのパフォーマンス データの収集 | | RA |
| | 統計の収集と管理 | | RA |
| **データベースのセキュリティ** | セキュリティ ロール、プロファイル、パスワード管理 | | RA |
| | セキュリティアクセス違反の報告、DBQL のデータマネジメント | | RA |
| **データベースの容量とパフォーマンス** | TASM の監視、パフォーマンス データの収集、ワークロードの分類 | | RA |
| | Viewpoint の設定とカナリー クエリを確認して分析し、データベースを監視する | | RA |
| | Viewpoint データベース アラートのカスタマイズと構成 (スペース、CPU、I/O、AWT など) | | RA |
| | パフォーマンス データのレポート | | RA |
| | 性能の調整 | | RA |

**R** – Responsible (責任) **A** – Accountable (説明責任) **I** – Informed (通知) **C** – Consulted (相談)

表 3: 責任の共有: Vantage でのデータベース管理、セキュリティ、パフォーマンス

## データの整合性とアクセス

データの完全性を維持し、顧客データの不正な変更を防止するために、Vantage はさまざまなテクノロジーとプロセスによって保護されています。ハッシュ、チェックサム、巡回冗長検査 (CRC)、ファイル監視、その他関連する管理は、データの入出力を確実に検証するために実施される主要な整合性管理を担います。Vantage は、不正なアクセスから保護するために、安全な認証、役割ベースのアクセス制御による承認ルール、行と列レベルのセキュリティによるきめ細かいアクセス制御、移動中、使用中、保存中のデータの暗号化などのオプションを提供します。これを有効にすると、データは Teradata と接続しているクライアント セッションの間で転送中に暗号化されます。また、クラウドのネットワークセグメントを通過するデータは、顧客が選択したプライベート接続オプションを実装することで、外部への漏えいを防ぎます。

GxP の義務を果たすための十分な仕組みを導入することは、テラデータと GxP 規制対象の顧客との間で共有される責任です。テラデータは、サービス、アプリケーション、データのための安全でコンプライアンスに準拠したプラットフォームを提供します。アクセスの承認、ガバナンスの管理、Vantage のデータの整合性に関連する設定の構成は、顧客の責任であることに留意してください。

| トピック | アクティビティ | テラデータ | 顧客 |
|---|---|---|---|
| データの整合性 | リソースへのアクセスを許可されたユーザーを適切に認証し、アクセスの適切性を継続的に監視している | | RA |
| | データの分類と保持ルールを定義する | | RA |
| | 転送中の顧客データの高度暗号化標準 (AES) またはトランスポート レイヤー セキュリティ (TLS) 暗号化の実施 | | RA |
| | システム ID とパスワードの使用に関する適切な管理体制の構築 | | RA |

**R** – Responsible (責任) **A** – Accountable (説明責任) **I** – Informed (通知) **C** – Consulted (相談)

表 4: 責任の共有: Vantage におけるデータの整合性

## データの可用性と事業継続性

GxP に準拠する顧客は、顧客のインフラやネットワークをサポートするミッションクリティカルなプラットフォーム、アプリケーション、およびサービスの事業継続計画を立てる際に、プラットフォームとデータの可用性に関する要件を考慮する必要があります。Vantage は 99.9% の SLA を設定していますが、CSP の可用性ゾーンまたはリージョンが影響を受ける場合、この SLA は適用されません。Vantage が複数の可用性ゾーンを持つ CSP 地域に導入された場合、テラデータはサービスの一環として、影響を受けていないセカンダリ可用性ゾーンに新しいシステムを導入し、既存のバックアップから影響を受けていないセカンダリ可用性ゾーンにインスタンスをリストアする商業上に合理的な努力を払います。テラデータは、追加のディザスターリカバリーサービス、マルチリージョンの高可用性、マルチクラウド プロバイダ ソリューションを追加料金で提供します。

## データバックアップと復元

テラデータによる初期設定後、Teradata Console を使用してバックアップジョブを作成・管理する機能を顧客に提供します。データ保護計画では、データ バックアップのスケジュール、頻度、および保持ポリシーを定義します。利用可能なバックアップ ストレージと保持ポリシーは、顧客が Vantage の展開に選択したクラウド プラットフォームによって異なります。

顧客には、適切な完全バックアップが存在することを確認する責任があります。これは、顧客が希望するリカバリーポイントの目標を達成するために、システムプロビジョニング時、または変更要求を介してスケジュールされます。これらのバックアップは、システム停止やデータ破損によりデータベースが使用できなくなった場合に、テラデータがデータや Vantage サービスを復元する目的で使用されます。これを復元するには、完全なデータ バックアップが必要になる場合があります。

| トピック | アクティビティ | テラデータ | 顧客 |
|---|---|---|---|
| **Backup and Restore (BAR) オペレーション** | システムのプロビジョニング時にデフォルトのフルシステム バックアップ ジョブと保持ポリシーを作成し、維持する | RA | CI |
| | 追加のカスタム バックアップ ジョブと保持ポリシーを作成して維持する (オプション) | I | RA |
| | バックアップ ジョブの完了を監視する | I | RA |
| | バックアップジョブの実行状況の提供 | RA | I |
| | ロック解除とブロックされたバックアップ ジョブの中断 | I | RA |
| | 復元ジョブの作成、実行、監視 | RA | CI |
| | 復元ジョブのスケジュールとリクエスト | CI | RA |

**R** – Responsible (責任)　**A** – Accountable (説明責任)　**I** – Informed (通知)　**C** – Consulted (相談)

表 5: 責任の共有: Vantage でのバックアップと復元

## Title 21 CFR Part 11

バイオ医薬品の開発および製造業務には、堅牢な分析アプリケーションが必要です。このようなアプリケーションにより、新薬の発見、開発、生産が円滑化されます。21 CFR Part 11 の厳格な記録と署名の要件は、ここで採用された自動化プロセスのなかで最も重要な要素です。この FDA の規制は、電子記録と電子署名を法的に可能な限り幅広く使用することを認めています。

Vantage データベースが Compliance Implementation Services (CIS)によって独立的に監査された際、テラデータがライフサイエンス企業の Part 11 義務達成を支援できることが独立的に実証されました。CIS はテラデータの設計仕様、ビジネスプロセス、標準業務手順書 (SOP) をレビューしました。CIS は主要な関係者にインタビューを行い、システムのウォークスルーを行いました。CIS は、システム開発、セキュリティ、データ抽出、検証レポートを評価しました。CIS はセキュリティ アクセス属性をテストしました。その他、変更管理、ユーザー受入テスト、トレーニング記録、バックアップ/リカバリー手順などのテストを実施しました。また、CIS は文書やデータの要求に対するテラデータの監査対応についても評価を実施しました。FDA の要求事項への適合性を評価するために、システム制御、文書化、プロセス、手順のレビューを実施しました。

CIS の評価結果: Vantage は、パート 11 の該当するすべての側面に対応しています。Vantage は、豊富なログ機能、アクセス制御、認証方式により、堅牢な柔軟性を提供します。データ収集や解析のアプリケーションを安心して進めることができます。

| 要件 | テラデータのアプローチ |
|---|---|
| **21 CFR § 11.10(a)**<br>システム検証 | Teradata Database は、第三者機関である Compliance Implementation Services によるセキュリティ管理の徹底的な精査を受けています。 |
| **21 CFR § 11.10(b)**<br>記録の正確かつ完全なコピー | Teradata Database は、すべての変更が文書化されていることの徹底と、豊富なログ機能により、変更に対する個人の責任管理を実践することができます。 |
| **21 CFR § 11.10(c)**<br>記録の保護 | Teradata Database は、保持に関して厳密なルールを適用できます。たとえば、選択、作成、修正、削除の権限を個別に割り当てることができます。 |
| **21 CFR § 11.10(d)**<br>システム アクセスの制限 | Teradata Database は、パスワードの複雑さの制限や暗号化された資格情報の交換など、許可された個人のみがデータベースにアクセスできる厳格なログイン セキュリティ制御を実施しています。 |
| **21 CFR § 11.10(e)**<br>監査証跡の生成 | Teradata Database は、選択、書き込み、削除を含むすべてのデータベース・アクセスのログを記録することができます。 |
| **21 CFR § 11.10(f)**<br>運用システムのチェック | Teradata Database は、職務の分離を実施し、ユーザーが適切な SQL 文の実行を許可されているかどうかを確認することができます。 |
| **21 CFR § 11.10(g)**<br>権限チェック | Teradata Database は、許可された個人のみがデータベースにアクセスできるように、厳格なログイン セキュリティ管理を実装しています。 |
| **21 CFR § 11.10(h)**<br>デバイス チェック | Teradata Director Program Identifier は、テラデータ クライアントに個別のホスト識別子を割り当てることができます。これにより、テラデータはユーザー名、パスワード、クライアントのワークステーションでアクセスを制限することができます。 |
| **21 CFR § 11.10(i)**<br>教育・人材育成 | Teradata Database システムには、管理者やエンドユーザーを支援する豊富なドキュメント ライブラリが付属しています。 |
| **21 CFR § 11.10(j)**<br>人事に関する説明責任 | テラデータセキュリティ管理マニュアルは、運用環境全体のセキュリティに関連する健全なセキュリティ実践のためのガイダンスを提供します。 |

表 6: テラデータは Part 11 の検証に対応します

# テラデータ品質管理

## 品質システム

テラデータは、次の 5 つの P によって推進される品質システムを遵守しています: Policies (方針)、Procedures (手順)、Processes (プロセス)、People (人材)、Plan (計画) です。ポリシー 品質システムの基本的な「慣習的ルール」を明示化します。手続き は、政策的な指示を遵守することを意味します。プロセス では、品質目標を達成するために必要な一連の作業を明示化します。人材の責任は、役割に適用される手順とプロセス タスクを明確化します。計画と進捗報告書は、品質システムが遵守されていることの証拠となります。

## 品質システム手順

テラデータの品質システムは、業界標準のポリシー、手順、プロセス、計画説明からなる品質マニュアルで管理されており、ハードウェアおよびソフトウェア製品、ソリューションの開発に必要な文書資料が構成されています。また、品質システムが ISO 9001:2015 規格の要求事項をどのように満たしているかを明確にします。

## 品質システム管理レビュー

品質システムおよび品質マニュアルのレビューは、テラデータのエンジニアリング、テラデータのリーダーシップ、主要戦略パートナーのメンバーからなる品質改善チームによって監督されています。このレビューは、上記の品質管理システムのレビュー手順に従って行われます。リーダーシップ チームの幹部は、毎年、品質システムの有効性の検証を実施しています。重大な問題や第三者からの指摘があった場合は、リーダーシップチームが臨時の会議を開催します。その主な責任は、品質管理プロセスの完全性を確保することです。

## 品質システム管理の監査

テラデータは、品質システム プロセスの独立した検査を受けています。認証機関によって、テラデータの品質管理が ISO 9001:2015 に適合していることが確認されました。テラデータの品質管理システムは、1999 年以降、定期的に ISO 9001 の再認証を受けています。

## ソフトウェア開発アプローチ

テラデータは、製品の作成・リリース・廃止のフレームワークである Unified Offering Lifecycle (UOL) を導入しています。UOL は、SAFe 4.6 の原則と慣行を遵守しています。UOL/SAFe 4.6 は、さまざまな種類のソフトウェア、開発、移行、維持に適用されます。これにより、UOL を GMPP (Good Pharmaceutical Medical Practice: 良質な製薬医学のための原則) に調整することができます。

**統一されたオファリングのライフサイクル**
2021 年 2 月現在

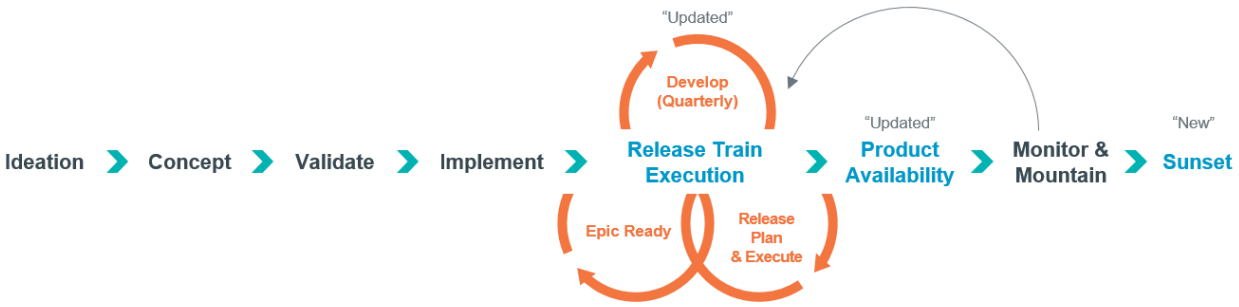


図 1: 統一されたオファリングのライフサイクル

テラデータの製品チームは、Unified Offering Lifecyle の遵守を必須としています。この規格は、準備、開発、アウトソーシング、取得、運用への移行を対象としています。また、運用段階でのソフトウェアの保守・拡張やセキュリティ対応についても対象としています。そのため、テラデータはクラウド上で動作する顧客のアプリケーションに変更を加えることはありません。Vantage の変更は、契約上の合意に基づいてのみ実施されます。

# Teradata Vantage オペレーション

Vantage では、テラデータが Vantage 環境のプロビジョニング、パッチ適用、アップグレードを管理します。テラデータは、Vantage のすべての顧客を対象に、統合的な保守・サポートサービスを提供しています。含まれているのは、明確に定義されたカバレッジ時間と応答時間です。また、サポート ポータルへのアクセス、Vantage コンソール、およびその他の機能も含まれています。顧客は、サポートポータルから 24 時間 365 日、ケースやサービス・変更依頼を提出することができます。テラデータは、サポート チケットに Infrastructure Technology Information Library (ITIL) のベスト プラクティスを採用しています。

## システムのプロビジョニング

テラデータは、テラデータと GxP 規制対象の顧客が承認したアーキテクチャ設計に従って、Vantage システムのプロビジョニングと構成を行います。テラデータは、Vantage システムを構成して、合意されたネットワーク設計に従って、顧客のネットワーク接続を促進します。テラデータは、Vantage サービスの利用可能日を顧客に通知します。サービス提供開始日以降、顧客は次の責任を負います:

- Teradata Console と同様にサポートポータル、コンソール、サポートロールを使用する登録作業
- DBC パスワードの保持と管理
- 顧客のインフラとネットワークの構成と管理をして Vantage に接続する
- 停止時間の承認と管理を行って移行、評価、ネットワーク テストを実施する

| トピック | アクティビティ | テラデータ | CSP | 顧客 |
|---|---|---|---|---|
| **展開** | プラットフォームのプロビジョニングとカスタマーオンボーディング | RA | I | CI |
| | ネットワーク接続性 | RA | I | RA |
| | プラットフォームでの AES と TLS の暗号化の構成 (PS の関与が必要) | RA | | CI |
| | クライアントで AES と TLS 暗号化を構成する | | | RA |
| **Teradata Advanced SQL Engine** | プロビジョニングとアップグレード | RA | | CI |
| | 可用性の監視とレポート | RA | | I |
| **テラデータのツールとユーティリティ** | クライアントへのインストールとアップグレード | | | RA |
| **Teradata Query Service** | プロビジョニングとアップグレード | RA | | |
| **Teradata Data Mover** | プロビジョニングとアップグレード | RA | | CI |
| | ポートレット (Viewpoint で有効化) | RA | | |
| | Data Mover ジョブの作成 | | | RA |
| | Data Mover 接続の作成<br>(PS の関与が必要) | RA | | CI |
| **Teradata Viewpoint** | プロビジョニングとアップグレード | RA | | CI |
| | ユーザーのセットアップと管理 | | | RA |
| | TASM/TIWM のルール セットの提供 | | | RA |
| | TASM/TIWM の構成とセットアップ | RA | | CI |
| **Vantage Analyst** | プロビジョニングとアップグレード | RA | | |
| **エディター** | プロビジョニングとアップグレード | RA | | |
| **Teradata QueryGrid (オプション)** | プロビジョニングとアップグレード | RA | | CI |
| | ポートレット (Viewpoint で有効化) | RA | | |
| | コネクタ - SQL エンジン ノードへのインストール (PS の関与が必要) | RA | | CI |
| | QueryGrid コネクタ - リモート ノード/システムへのインストール<br>(PS の関与が必要) | RA | | CI |
| | ジョブの作成と管理 | | | RA |
| **Teradata Data Lab (オプション)** | プロビジョニングとアップグレード | RA | | CI |
| | ポートレット (Viewpoint で有効化) | RA | | |
| | ユーザーとラボの作成と管理 | | | RA |

**R** – Responsible (責任) **A** – Accountable (説明責任) **I** – Informed (通知) **C** – Consulted (相談)

表 7: 責任の共有: Vantage での展開と保守

## システム監視

テラデータは、クラウドサービス説明書に定義されたとおり、Vantage 環境のパフォーマンス、セキュリティ、可用性を継続的に監視します。テラデータでは自動イベント管理機能を実装しているため、Vantage の健全性を監視し、サポートケースを作成することができます。

## インシデント管理

テラデータは、Information Technology Infrastructure Library (ITIL) のベストプラクティスに従って、高可用性、コンプライアンス、パフォーマンスの高い Vantage システムを実現しています。テラデータは、顧客の問題、要求、ケースの解決活動を追跡して解決します。Vantage では、5 段階の重大度レベルモデルを実装しています。サポートポータルでケースを開く際、顧客は報告された問題の影響度に基づいて深刻度を選択する必要があります。テラデータは、ビジネスや業務への影響に関連する重大度レベルの説明を提供します。テラデータは、割り当てられた深刻度に基づき、ケースの評価、対応、解決します。場合によっては、顧客の対応が必要となる場合があります。顧客は、「情報待ち」というステータスでケースに対応する必要があります。ケースの解決策が届くと、ステータスは「解決済」になります。その後、顧客は更新内容を確認し、解決策を受け入れるか拒否する必要があります。

| トピック | アクティビティ | テラデータ | 顧客 |
|---|---|---|---|
| インシデント管理 | 自動インシデント作成 | RA | I |
| | ユーザーインシデント作成 | I | RA |
| | 最初の問題のトリアージと RCA | RA | I |
| | Vantage ソフトウェアの問題解決 | RA | I |
| | CSP インフラストラクチャの問題解決 | RA | I |

**R** – Responsible (責任)　**A** – Accountable (説明責任)　**I** – Informed (通知)　**C** – Consulted (相談)

表 8: 責任の共有: Vantage でのインシデント管理

## 変更管理

テラデータは、新しいバージョンがリリースされると、Vantage を更新します。最新バージョンには、新機能やセキュリティ問題を軽減するパッチが含まれている場合があります。中断を最小限に抑えるため、テラデータは GxP の顧客と協力してアップグレードのスケジュールを調整します。テラデータでは、メジャーバージョンアップを最低 4 ヶ月前に通知しています。これにより、顧客はアプリケーションの互換性をテストし、新しいバージョンを検証できます。アップグレードは、顧客が承認した時間枠に合わせてスケジュールされます。

| トピック | アクティビティ | テラデータ | CSP | 顧客 |
|---|---|---|---|---|
| 変更管理 | Teradata Vantage コンポーネントと OS へのアップグレード | RA | | CI |
| | CSP インフラストラクチャの最新性を維持するアップグレード | RA | I | I |
| | ネットワークとファイアウォールの変更 | R | I | RA |
| | アップグレード後の顧客のアプリケーション、ワークロード、プロセスのテスト | | | RA |
| | ETL やレポートを含む顧客ワークロードとプロセスの作成、開発、推進、バックアップ | | | RA |

**R** – Responsible (責任)　**A** – Accountable (説明責任)　**I** – Informed (通知)　**C** – Consulted (相談)

表 9: 責任の共有: Vantage での変更管理

## GxP 検証の運用モデル

データおよび分析プラットフォームに関する GxP コンプライアンスは、顧客の責任となります。そのため、テラデータの顧客には、Vantage の使用経験やクラウドインスタンスの管理経験が必要となります。法規制への対応は、顧客の企業の品質方針と適用される県境組織と連携して実施する必要があります。

テラデータとそのコンプライアンス パートナーは、Vantage の評価、設計、実装、検証を支援する体勢が整っています。私たちは連携して取り組むことで、Part 11 やその他の規制要件への準拠を徹底しています。テラデータとライフサイエンスおよび製造業の顧客は、GxP 検証に向けた多くの運用モデルを導入することができます。

- **モデル 1**: ライフサイエンスや製造業の企業は、ビジネスや技術的な移行に加え、GxP アプリケーションの検証にも責任を負います。その統括管理は、品質管理システム (QMS) です。

- **モデル 2**: ライフサイエンス企業や製造業は事業責任を保持します。第三者に依頼し、自社の QMS を使用して GxP アプリケーションの検証を支援します。技術パートナーは、その管理ツールを使用して「論理的な」工場を作成します。工場は、実際の実行ステップを計画し、調整します。また、アプリケーションやデータベースの移行や検証もこの工場で実施します。

- **モデル 3**: GxP への準拠に対する責任は、ライフサイエンスおよび製造業の顧客にあります。責任共有モデルは、顧客によるリソースの割り当てに役立ちます。これにより、必要な労力を軽減できます。また、このモデルは、顧客が直面する事務的・技術的な負担の軽減にも役立ちます。Vantage インフラストラクチャのセキュリティは、一般的にテラデータが担当します。顧客の責任において、データの安全性を確保する必要があります。

## まとめ

Teradata Vantage は、ライフ サイエンスおよび製造業の顧客に、クラス最高のセキュリティ、データマネジメント、監査レポートなどの幅広い機能を提供します。これにより、FDA 21 CFR Part 11 要件への準拠が可能になります。Vantage は、一連の試行錯誤を重ねたアクセス、セキュリティ、プライバシー制御により、安全で一貫性のある信頼性の高いパフォーマンスを維持します。これらのプロセスや管理は、資格のある第三者の認可された評価者によって継続的に監査・検証されます。同様に重要なのは、ライフサイエンスや製造業の顧客が、検証やガバナンス戦略を定義する際に実施する必要のある管理であり、これによって GxP コンテンツの完全性が保証されます。協力して取り組むことで、コンプライアンス、コスト削減、効率化、イノベーションを実現することができます。

## 業界/規制ガイダンス基準


参考文献 [1] **ISO/IEC 27001:2013 情報技術 – セキュリティ技術 – 情報セキュリティ管理システム – 要件**

参考文献 [2] **ISO 9001:2015 品質管理システム – 要求事項**

参考文献 [3] **PCI DSS クイック リファレンス ガイド: クレジット カード業界のデータ セキュリティ基準を理解するバージョン 3.2.1**

参考文献 [4]**財務報告に関するユーザーエンティティの内部統制 (ICFR) に関連するサービス組織における統制に関するレポート**

参考文献 [5]**規則 (EU) 2016/679 (一般データ保護規則)**

参考文献 [6]**現行の最終医薬品の適正製造基準 (Title 21 CFR Part 11)**

参考文献 [7]**米国 FDA、連邦規則集、Title 21 Part 11、電子記録、電子署名**

参考文献 [8] **米国 FDA、業界向けガイダンス - Part 11、電子記録、電子署名 – 範囲と適用、2003 年 8 月**

参考文献 [9]**米国 FDA、21 CFR Part 11 -- 質疑応答 (ガイダンス案)、2017 年 6 月に基づく臨床調査における電子記録および電子署名の使用**

参考文献 [10]**ホワイトペーパー: AWS で GxP 規制ワークロードの強固な基盤を構築する**

参考文献 [11] **Microsoft 365 GxP ガイドライン、2020 年 4 月公開**

# 付録 - テラデータ認定

テラデータは、規制機関や監査法人から多くの認証や証明書を取得しています。これらは、テラデータのコンプライアンスとセキュリティの実現に向けた取り組みを裏付けるものです。Vantage は、以下の規制基準への準拠について、定期的に監査を受けています。

**ISO 9001:2015** では、組織内で効果的な品質管理を実現するために必要な構造、責任、手順を文書化し、レビューするためのプロセス指向のアプローチを概説しています。規格の特定のセクションには、次のようなトピックに関する情報が含まれています:

- ドキュメントを含む品質管理システムの要件
- マネジメントの責任
- 人的資源および組織の作業環境などのリソース管理
- 内部監査による QMS の測定、分析、改善

**ISO/IEC 27001:2013** は、情報セキュリティマネジメント基準 (ISMS) の規格です。ここでは、情報セキュリティマネジメントの要求事項を定義しています。この規格では、情報には、データ、文書、通信、会話、メッセージ、録音、写真が含まれます。これには、デジタル データや電子メールから、ファックスや電話での会話まで、あらゆるものが含まれます。

**SOC 1** レポートは、財務監査に関連するサービス組織での管理に焦点を当てています。Teradata SOC 1 レポートは、財務監査を扱っています。また、セキュリティ組織、従業員のユーザーアクセス、論理セキュリティ、安全なデータ処理、物理セキュリティ、変更管理、データの完全性、可用性、インシデント処理についても説明しています。

**SOC 2** レポートは、米国公認会計士協会 (AICPA) によって定義された管理を評価します。これらの原則では、セキュリティ、可用性、処理の整合性、機密性、プライバシーの制御を定義しています。これらは、テラデータなどのサービス組織に適用されます。SOC 2 Type 2 レポートは、セキュリティ、可用性、機密性サービスに関連するテラデータの制御の概要を示しています。この SOC 2 レポートは、GxP コンプライアンスに直接的に関係しています。

## PCI-DSS 3.2.1

PCI データセキュリティ基準は、ブランド化されたクレジットカード所有者のデータを保護するために設計された要件です。この基準は、カード所有者のデータを保存、処理、伝送するすべての事業者に適用されます。コンプライアンスは PCI 協議会 (American Express、Discover Financial Services、JCB、MasterCard、Visa Inc.) により実施されます。Vantage は、カード所有者データの取り扱いに直接関与していません。テラデータでは世界中の銀行が PCI-DSS 3.2.1 に準拠するための製品とサービスを提供しています。

## 1996 年に制定された HIPAA (Health Insurance Portability and Accountability Act: 医療保険の携行性と責任に関する法律)

テラデータのコンサルタントは、HIPAA セキュリティ ルールを満たすために必要なコントロールの評価を行います。また、2009 年に制定された HITECH (Health Information Technology for Economic and Clinical Health: 経済的および臨床的健全性のための医療情報技術) 法の侵害通知規則も評価します。この具体的な目的には次が含まれます:

- HIPAA のセキュリティと侵害通知規則の要件に従った ePHI 環境のセキュリティ態勢の評価
- 必要とされ、対処可能な管理的、技術的、物理的な保障措置の要件に関するギャップの特定

## CSA CAIQ

クラウド セキュリティ アライアンス (CSA) の コンセンサス アセスメント イニシアティブ アンケート (CAIQ) は、クラウド事業者のセキュリティ管理およびプロセスの透明性を提供する一般公開されたドキュメントです。そのため、顧客はこのレポートを利用して、どのコントロールがサービスの一部として完全に活用されているか、または共有されているかを評価し、サービスプロバイダーのセキュリティコントロールについてより良く理解することができます。テラデータでは、任意の CSA 自己評価を実施しており、CSA が公表しているベストプラクティスに準拠していることを文書化しています。テラデータは、完成した CSA CAIQ を要求に応じて顧客に提供します。

## CCPA と GDPR

テラデータは、業界で認められた独立した監査人を使用して、Vantage を毎年監査しています。定期的な監査によって、顧客が個人情報保護に関する責任を果たすことができます。年次監査結果は、CCPA および GDPR の顧客レビューで確認できます

17095 Via Del Campo, San Diego, CA 92127 **Teradata.jp**