

# Vertica Accelerator セキュリティステートメント

このセキュリティステートメントは、Vertica Accelerator に適用可能な、Vertica によって実装される情報セキュリティ管理システムに関する情報を提供することを目的としています。

## 情報セキュリティ管理システム(ISMS)

Vertica は、お客様の情報の保護に取り組んでいます。この目標を達成するために、Vertica は ISO/IEC 27001:2013 に準拠した情報セキュリティ管理システム (ISMS) を導入しています。

Vertica ISMS を覆う包括的なフレームワークは、情報セキュリティポリシーの Micro Focus セットである Micro Focus Information Security Policy Framework (ISPF) です。これは、企業および顧客の情報を保護するための一連のセキュリティ要件で構成されています。

## Vertica Accelerator の概要:

### お客様の権限を活用:

- Vertica Accelerator は Amazon Web Services (AWS) 内でホスティングされます。お客様の AWS アカウントで稼働します。
- このアプローチにより、すべてのデータとコンピューティングリソースを自社の安全なクラウドに保持し、AWS の優先価格と柔軟性を維持できます。
- Vertica Accelerator のデプロイおよび管理には、お客様の AWS アカウントにクロスアカウントロールが必要ですが、これらのロールの構築には最小特権の原則を使用しています。

### クラウドネイティブアーキテクチャ:

- Vertica Accelerator は、実績のあるクラウドネイティブな Vertica アーキテクチャに基づいて構築されており、分析ユースケースごとに適切なレベルのリソース、管理、および制御を必要とする組織に、ハイパフォーマンスでスケラブルな分析とエンドツーエンドのインデックス機械学習を提供します。

### サービスとしての高度な分析:

- Vertica Accelerator は、組織の環境の管理、クエリのチューニング、データの所有権など、組織の透明性と管理性を大幅に向上させます。また、クラウドに最適化された実。

績のあるアーキテクチャを採用しており、予測可能で透過的な価格設定により、大規模なスケールで最高レベルのパフォーマンスを実現します

Vertica は Micro Focus 製品グループです。Micro Focus は、フォーチュン 100 社のうち 98 社を含む、世界中の 40,000 社の経営と変革を支援しています。

Micro Focus は、世界をリードするセキュリティ製品を開発しています。Vertica と Micro Focus の情報セキュリティ担当者は合わせて 400 人を超え、比類のないセキュリティ経験と専門知識をお客様に提供しています。

詳細については [Micro Focus Product Security Page](#) を参照してください。

## 情報セキュリティポリシー

Vertica は、経営陣によって定義および承認され、公開され、従業員および関連する外部関係者に伝達される、情報セキュリティに関する一連のポリシーを実装しました。

## 情報セキュリティの組織

Vertica は、適切な職務分離を伴う情報セキュリティ責任を定義し、割り当てています。

## 人事セキュリティ

Vertica は、すべての従業員の経歴確認を行い、情報セキュリティに対する責任を認識することを求めています。

Vertica の従業員は、職務に関連するセキュリティ教育・訓練を受け、組織のポリシーと手順の定期的な更新を受けます。



## 資産管理

Vertica は、所有者が割り当てられた資産目録を管理しています。Vertica の従業員は、情報および情報処理施設に関連する資産の適切な使用方法について訓練を受けています。

## アクセス制御

Vertica は、ユーザーの登録と登録解除を制御するアクセス制御ポリシーと手順を確立しています。情報およびアプリケーションシステム機能へのアクセスは、アクセス制御ポリシーに従って制限されます。

## 暗号化

情報を保護するための暗号制御の使用に関するポリシーと手順が策定され、実装されています。鍵管理システムは、暗号鍵の使用、保護、およびライフサイクルを導くために利用されます。

お問い合わせ先:  
[www.vertica.com](http://www.vertica.com)

この記事が気に入っていただけましたか？共有してください。



### 物理的および環境的なセキュリティ

Vertica のオフィスは、業界をリードする物理的および環境的管理によって保護されています。

### 運用のセキュリティ

Vertica では、運用の指針となるプレイブックを文書化しています。開発環境、テスト環境、運用環境が別々に用意されています。

バックアップ、変更管理、ロギング、マルウェアおよび脆弱性管理に対する制御が確立されています。

### コミュニケーションのセキュリティ

ネットワークは、システムおよびアプリケーション内の情報を保護するために管理および制御されます。

### システムの調達、開発、および保守

情報セキュリティ関連の要件は、新しい情報システムまたは既存の情報システムの拡張に対して規定されています。

Vertica では、開発の全段階でセキュリティとプライバシーを考慮した安全な開発ライフサイクルを採用しています。

### サプライヤーとの関わり

組織の資産へのサプライヤーのアクセスに関連するリスクを軽減するための情報セキュリティ要件は、サプライヤーと合意され、文書化されています。

### 情報セキュリティインシデント管理

Vertica には、情報セキュリティインシデントへの迅速、効果的、かつ秩序ある対応を保証するための確立されたインシデント管理プロセスがあります。

### 事業継続管理における情報セキュリティ方針

Vertica には、文書化された事業継続と災害復旧計画があります。冗長化された資産とデータのレプリケーションを設定し、継続性と回復性を確保しています。

### コンプライアンス

関連するすべての法律、法定、規制、および契約上の要件は、各情報システムおよび組織について明示的に識別、文書化され、最新の状態に保たれます。

プライバシーの管理と個人を特定できる情報の保護が実装されています。

Vertica では、情報セキュリティ管理システムを常に最先端のものにしていきたいと考えています。そのために、私たちは弊社の情報セキュリティマネジメントシステムの ISO 27001 監査を受けました。2022 年 1 月までには認証を取得できる見込みです。

Vertica ISMS には買収した Full 360 の ISMS も統合されており、Full 360 は [有効な ISO 27001 認証](#) (2024 年 6 月まで有効) を取得しています。

