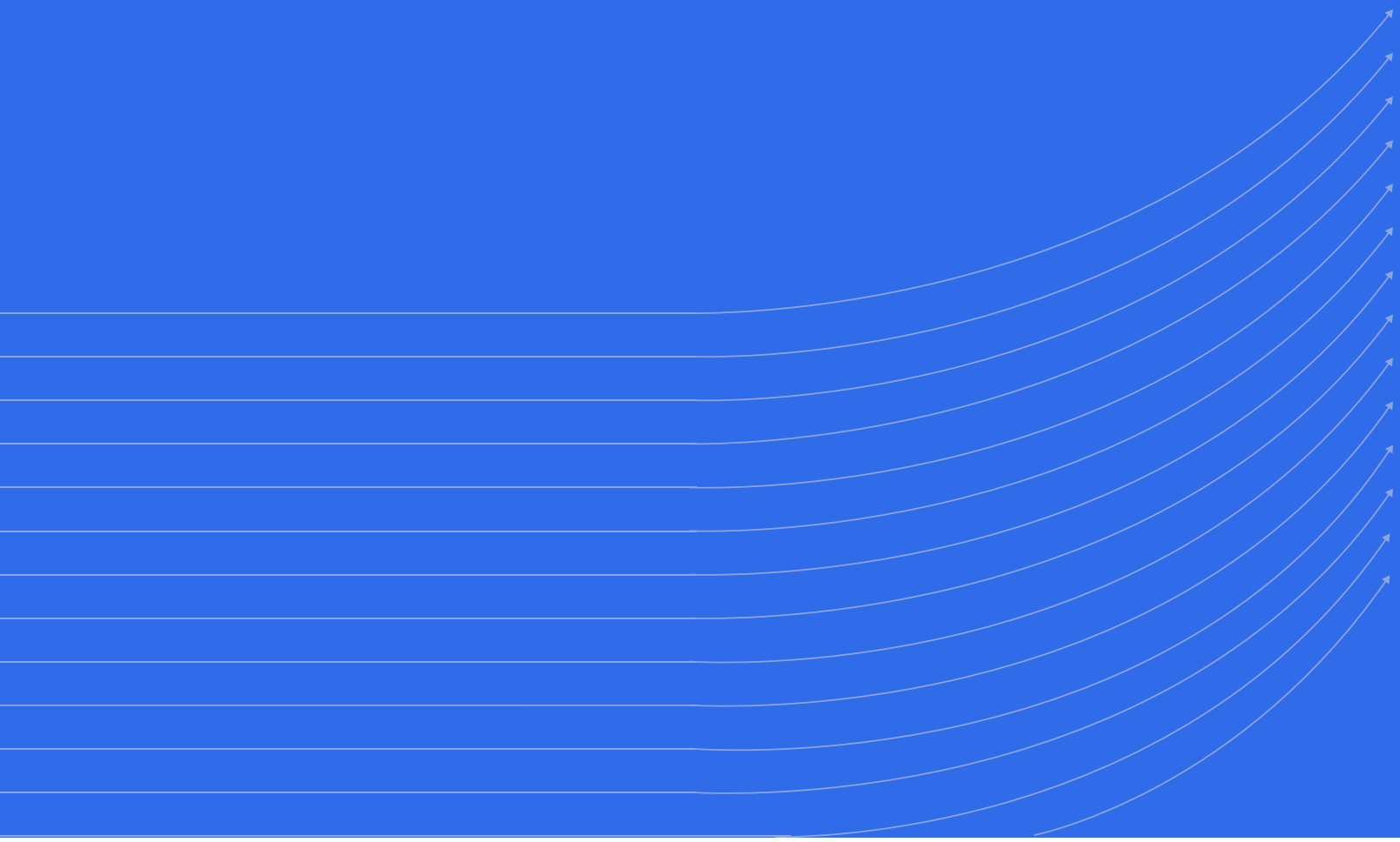
Fivetran

2024年 4月更新

Fivetran セキュリティ ホワイトペーパー



FIVETRAN.COM

目次

はじめに 3

Fivetranセキュリティフレームワーク 4

Fivetran製品のセキュリティとガバナンス 7

データ保護 10

セキュリティプログラム 11

まとめ 15

はじめに

Fivetranは、お客様の組織がデータのセキュリティを重要視していることを理解しており、弊社の各製品およびサービスは、データを保護するように配慮して設計されています。

弊社のセキュリティプログラム全体とセキュリティ文化の健全性を確保するため、Fivetranは毎年、SOC 1 Type 2監査、SOC 2 Type 2監査、ISO 27001認証、PCI DSS Level 1検証など、複数の独立したセキュリティ評価を受けています。これらの監査報告書を（NDA締結を前提として）お客様と共有することで、弊社のセキュリティ・プログラムが事業の全部門にわたって堅牢かつインテリジェントに管理されていることを実証しています。

弊社のセキュリティプログラムは、徹底した管理体制を特徴としています。ネットワークやアクセス制御のポリシーは非常に慎重に設計されており、システム内の最小特権の原則に従っています。データパイプラインは、静止状態でも移動中でも、データが常に暗号化されるように設計されています。エフェメラルキーとHSMにバックアップされたカスタマーマスターキーの組み合わせにより、システム内のデータだけでなく、長期保存されるメタデータや設定データも保護します。

また、ログベースの監視と異常検知を導入し、脅威に対してリアルタイムに対応できるようにしています。

最後に、偶発的な漏洩のリスクを減らすために、Fivetranは、パイプラインのデータが移動先に到着した後に決して残らないようにするためのセキュリティプロトコルを導入しています。

データカンパニーとして、我々はセキュリティだけでなく、透明性やデータに裏打ちされた意思決定を強く信じています。

お客様のビジネスにとって、どのように安全で信頼できるパートナーになれるかについて、お客様からの強い信頼を得るためにこの資料を公開しています。

弊社は、第三者認証、最新のセキュリティ文書、標準的なアンケート、よくある質問に対する回答をトラストセンターで管理・掲載しています。Fivetranのトラストセンターには、ISO 27001:2013、SOC 2 Type II、PCI DSS3.2.1、その他多くのセキュリティおよびコンプライアンスに関する文書が掲載されています。
トラストセンターをご覧ください

Fivetranセキュリティフレームワーク

弊社は、製品および社内全体にわたって高レベルのセキュリティを保証するために総合的に設計されています。確立された基準とプロトコルを活用し、クラス最高のセキュリティ管理を実現しています。

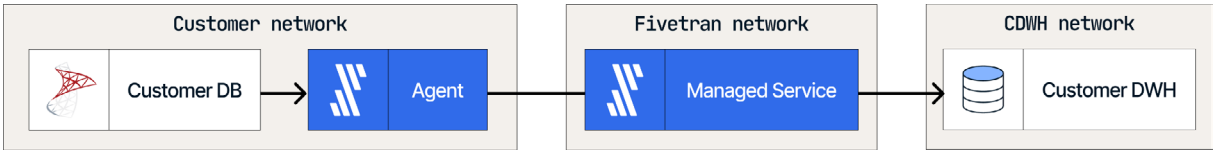
デプロイメント方式

弊社は、お客様のアーキテクチャとデータ処理要件に基づき、複数のデプロイメント方式を提供します。

- **クラウド デプロイメント：** Fivetranは、SaaSアプリケーション、ファイル、データベースからクラウド先への自動化されたスケーラブルで信頼性の高いデータ移動のために、クラウドで完全に管理されています。お客様は、Fivetranをクラウドでホストする地域とデータセンターを選択できます（「データ・レジデンシー」を参照）。

- **セルフホスト デプロイメント：** 機密性の高いデータベース・データをお持ちの方は、Fivetranをダウンロードし、オンプレミスまたは仮想プライベート・クラウドで展開することができます。Fivetran HVRの詳細については、sales@fivetran.comまでお問合せください。

- **ハイブリッド デプロイメント：** Fivetranは、複雑なアーキテクチャやデータ移動のトポロジーに対応するハイブリッドオプションを提供し、クラウドの効率的な利点を提供すると同時に、データの安全性と保護に対する安心感を維持します。



ネットワーク接続

Fivetranのビジネスの中核は、サードパーティのソースからデータを取得して処理し、お客様のデータウェアハウスに移動することです。ソースからFivetranへ、またはFivetranからデータウェアハウスへ、私たちが行うネットワーク接続のひとつひとつが、データの移動のための重要な役割を果たします。

これらのプロセスを注意深く監視し、アルゴリズムの選択と鍵の検証が適切に行われていることを保証しています。また、使用するツール（例：openssl）の脆弱性を積極的に監視し、セキュリティ・インシデントが発生した場合に当社のソフトウェアに速やかにパッチが適用されるようにしています。

Fivetranは、お客様の特定のデータ移動要件を満たすために、多くのプライベートネットワーク接続オプションを提供しています。

- **SSHトンネル -** 追加のセキュリティ層として、Fivetran がデータベースポートにアクセスするためのトンネル接続を設定します。
- **リバースSSHトンネル -** ポートへの直接アクセスを提供できない場合、Fivetran トンネルサーバーをセットアップして、お客様のIPから入ってくるトラフィックをリッスンすることができます。
- **VPNトンネル -** 高度な暗号化、認証、完全性をサポートするIPSec VPNトンネルです。
- **プロキシ -** お客様のデータベースとFivetran間のセキュアなアウトバウンドのみの通信を可能にします。
- **プライベート・ネットワーク -** Fivetranとお客様のクラウド・サービスが、トラフィックを公衆網に公開することなく通信できる、最も安全な接続方法です。
    - **AWS PrivateLink**
    - **Azure Private Link**
    - **Google Private Service Connect**

データの移動

エンドツーエンドの暗号化 - Fivetranは、送信元から送信先までエンドツーエンドで暗号化し、転送中のデータを保護します。移動中のデータのセキュリティ対策については、**ネットワーク接続**オプションをご覧ください。

ロード後にデータパージ - Fivetranは、同期を成功させるために必要な期間だけデータを保持します。顧客データは、デスティネーション（連携先）へのロードに成功するとすぐにパージされます。データ保持の詳細については、**ドキュメント**をご覧ください。

データレジデンシー

Fivetranのデータ処理する場所は、規制遵守やその他のデータ保存要件に応じて選択できます。

Geography	GCP regions	AWS regions	Azure regions
US	us-east4 (N.Virginia)* us-west1 (Oregon) us-central1 (Iowa)	us-east4 (N.Virginia)* us-east2 (Ohio) us-west2 (Oregon) us-gov-west-1 (GovCloud US West)	us-east4 (N.Virginia)* us-west1 (Oregon) us-central1 (Iowa)
UK	europe-west2 (London)	eu-west-2 (London)	uksouth (London)
EU	europe-west3 (Frankfurt)	eu-central-1 (Drankurt)* eu-west-1 (Dublin)	westeurope (Netherlands)
Canada	northamerica-northeast1 (Montréal)	ca-central-1 (Montréal)	canadacentral (Toronto)
Austalia	australia-southeast-1 (Sydney)	ap-southeast-2 (Sydney)	australiaeast (Sydney)
Singapore	asia-southeast1 (Singapore)	ap-southeast-1 (Singapore)	southeastasia (Singapore)
India	asia-south1 (Mumbai) centralindia (Central India)	ap-south-1 (Mumbai)	centralindia (Pune)
Japan	asia-northeast1 (Tokyo)	ap-northeast-1 (Tokyo)	japaneast (Tokyo)
Indonesia	asia-southeast2 (Jakarta)		
Middle East			uaenorth (Dubai)

弊社は定期的に対応するリージョナルのデータセンターを追加しており、最新情報は**ドキュメント**で参照することができます。

Fivetran製品のセキュリティとガバナンス

お客様のセキュリティチームは、コンプライアンスを維持し、安全に拡張するために、ビジネスと顧客データを保護する必要があります。弊社のセキュアなプラットフォームは、安全なデータの取り扱いを保証するために必要な機能を提供します。

お客様の法務およびセキュリティチームが貴社のデータ移動戦略に自信を持ち、データ実務が社内外のセキュリティ要件およびガバナンスポリシーを満たすことを保証します。

アクセス制御

データ資産へのアクセスを制御することは、データ、顧客、会社を保護するために不可欠です。

Fivetranは、様々なアクセスコントロール機能を提供し、ユーザーを過剰に許可することなく、不正アクセスのリスクを制限します。

SAMLによるシングルサインオン

FivetranはSAMLベースのログインをサポートしており、ユーザーに対して多要素認証を強制することを推奨しています。

ロールベース アクセス制御

Fivetranに登録されたお客様の組織のユーザーとFivetranの運用スタッフのみが、お客様の組織のFivetranダッシュボードにアクセスすることができます。

組織内の管理者は、Fivetranアカウントとデータ ウェアハウスにアクセスできるユーザーを制御できます。

管理者はデータをロードできるコネクタを制限することもできます。

標準ロールは、新しいコネクタの作成と編集、変換の作成、および新規ユーザーの追加を行えるユーザーを定義するのに役立ちます。

ロールの詳細は**ドキュメントを参照**してください。

Fivetranダッシュボードは、各コネクタのステータスと各統合のメタデータへの可視性を提供し、

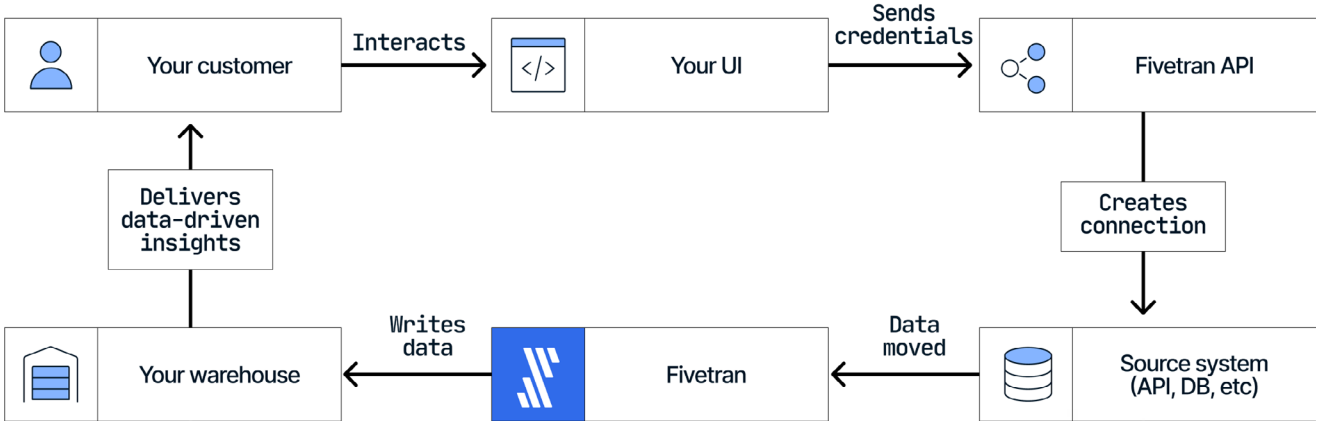
コネクターを一時停止または削除する機能を提供します（ただし、お客様のデータを削除することはできません）。大規模なユーザーグループに対してアクセス許可を拡張する場合、グループレベルのアクセス許可を作成することができます。関連するチームメンバーに適用することができる特定のアクセス許可を持つグループを設定します。一括アクションはFivetran APIによるプログラムコントロールを介して適用することができます。スケーラブルなアクセス許可は、アクセスを適用する際のヒューマンエラーのリスクを低減します。

クロスドメインID管理システム（SCIM）

OktaまたはAzure ActiveDirectoryと統合して、ユーザーライフサイクルをより簡単に管理することも、権限付与を拡張するための選択肢の1つです。ITチームがユーザーのオンボーディング、変更、オフボーディングを自動化できるようにします。事前に定義された役割と権限を持つチームを設定することで、各新規ユーザーを適切なアクセスレベルで簡単にオンボーディングできます。

コネクト・カード

お客様のユースケースによっては、あなたの顧客がFivetranでそれらをプロビジョニングせずに、あなたの製品に自分のデータを同期させたい場合があります。このような場合、コネクト・カード（埋め込み可能なFivetranのポップアップ）を使用することができます。これにより、あなたの顧客は、お客様が提供するユーザーインターフェースを利用して、完全に自分自身で、データソースへの接続を認証することができます。



透明性

Fivetranは、プロセスに透明性をもたらす複数のツールをお客様に提供しています。

ログ

コネクタ、ダッシュボードのユーザーアクション、およびFivetran APIコールから構造化されたログイベントを生成します。ログは、各コネクター内で発生した操作の内部ビューを提供します。ログ情報には以下の方法でアクセスすることができます。

- **Fivetranダッシュボード -** コネクタレベルのログは、ツール内のユーザーアクションの履歴と一緒に、Fivetranダッシュボード内で利用可能です。より高度なユースケースのために、Fivetranは、AWSCloudwatchやGoogle Stackdriverなどのサービスへのログの完全なエクスポートを提供しています。
- **Fivetran Platform Connector -** Fivetran Platform Connector は、ログとアカウントのメタデータをデスティネーション（連携先）のスキーマに配信します。このメタデータには、Fivetranの詳細な利用情報が含まれます。
- **外部ログサービス -** Fivetranは、外部サービス（エンタープライズまたはビジネスクリティカルプラン）にログを送信することができます。サポートされている外部ログツールの情報はドキュメントを参照してください。デスティネーションごとに1つのログサービスと接続できます。

メタデータ共有

Fivetranは、データスチュワードにデータ観測可能範囲を拡大する権限を与え、メタデータを共有する力を提供します。

Fivetranのメタデータをデータカタログにフィードすることで、データスチュワードは組織データの全体像を一元的に把握することができます。

コア・データ・チームがデータの流れを把握することで、PIIや機密データをどのように扱うべきかなど、内部ガバナンス・ポリシーを適用することができます。

これにより、GDPR、CCPA、およびその他の規制に準拠し、データに関連する社内の法的要件やセキュリティ要件を満たすことができます。

Fivetranは、Alation、Atlan、Collibra、data.worldと連携し、さらに多くのパートナーとの連携が継続的に追加されています。

データ保護

企業がFivetranのようなマネージド・クラウド・データ移動プラットフォームの利用を検討する際、多くの場合、データ・セキュリティが最重要課題となります。多くのセキュリティチーム、特に金融サービスやヘルスケア業界では、機密データ資産を保護するために完全なコントロールを維持する必要があります。

ブロックとハッシュ化

Fivetranは、機密データをウェアハウスに送信しないようにすることができます。ブロックとハッシュ化機能は、個人特定項目（PII）を排除し、GDPRへの準拠を促進するのに役立ちます。

- **カラムブロック** により、特定のカラムを完全にウェアハウスに入れないようにすることができます。
- **カラムのハッシュ化**により、分析価値を維持したままウェアハウス内のデータを匿名化できます。データウェアハウスに機密データを持ち込むことなく、データセット間で結合できます。

サポートへのアクセス許可

Fivetranの24時間365日のカスタマーサポートチームは、お客様のデータパイプラインで発生する可能性のあるあらゆる問題に対応することができます。

トラブルシューティングには、本番環境で直接対応することが最速または最善の方法である場合があります。FivetranのGrant Support Access（GSA）と呼ばれる機能は、お客様がFivetranに権限を与えることで、お客様の環境内でのトラブルシューティングを支援します。

- 顧客データは、お客様の明示的な承認なしにアクセスされることはありません。
- Fivetranの従業員は、SAML統合を介してシングルサインオンを使用する必要があります。
- セッションの持続時間は、最近のMFA認証を確実にするために12時間に制限されています。
- 監査により、お客様は誰がいつ何にアクセスしたかを確実に把握できます。
- アクセスはいつでも取り消すことができ、本番データを安全に保つことができます。

カスタマー・マネージド・キー

カスタマー・マネージド・キーは、データおよびクレデンシャルの暗号化に使用されるマスター・キーの管理を可能にし、いつでもアクセスを制限することができます。ボタンを押すだけで、セキュリティチームはキーへのアクセスを無効にし、Fivetranによるデータの同期を停止できます。

ボタンを押すだけで、セキュリティチームはキーへのアクセスを無効にし、Fivetranのデータ同期を停止することができます。キーはいつでも再有効化して同期を再開できます。

暗号化に使用されるマスターキーを所有し管理することで、データパイプラインで使用される機密情報を完全にコントロールすることができます。これは、データ侵害やその他のセキュリティ・イベントが発生した場合に、セキュリティ・チームが「緊急ボタン」を押す必要がある場合に重要です。カスタマー・マネージド・キーはいつでも無効にすることができ、Fivetranの全操作を停止させることができます。Fivetranは機密情報の暗号化を解除することはできません。

セキュリティプログラム

セキュリティ運用

弊社は、ツール、プロセス、および技術がFivetranサービスの安全な開発と運用を促進することを保証するために、セキュリティ運用プログラムを実装しています。

このプログラムは、以下を提供することにより、リスクを軽減し、お客様のビジネスをサポートすることを目的としています。

- ソフトウェア開発ライフサイクル（SDLC）全体にわたるセキュリティステップ
- CI/CDツールチェインの強化
- 静的テストとコードレビュー
- コンテナの安全性と不変性
- クラウド構成監査およびコンプライアンス監査
- エンジニアリング・デザイン・レビューと脅威のモデリング

Fivetranサービスの安全な開発および運用を促進するツール、プロセス、および技術を確保するために、セキュリティ運用プログラムを導入しています。

このプログラムは、リスクを低減し、お客様のビジネスをサポートすることを目的としています。

監視とアラート

Fivetranは、クラウド構成と監査イベント、ホストレベルのシステム/プロセス/ネットワーク情報、およびコンテナイメージの脆弱性を継続的に収集し、通常の期待される動作のベースラインを確立する異常ベースのセキュリティ監視システムを導入しています。

通常の動作から逸脱した場合は、SecOps にアラートが送信され、さらなる調査が行われます。

FivetranのWebポータルはWAFによって保護されており、OWASPトップ10攻撃に対する追加の保護だけでなく、アカウントのセキュリティと潜在的なWebの脆弱性に対する可視性を提供します。

リスクおよび脆弱性の管理

Fivetranは、脆弱性をタイムリーに検出し、修復するための脆弱性管理プログラムを導入しています。脆弱性は、Fivetranの環境全体で発見、特定され、リスク評価され、修復の優先順位が付けられます。脆弱性は、パッチの適用、コードやインフラストラクチャの変更、手順やユーザーの行動の変更によって修復・改善されます。正当なビジネス上の理由で脆弱性を是正できない場合は、代わりとなる措置を講じるか、正式なリスク受容書を取得されます。すべての修復活動は、元の脆弱性が解決されたことを確認するために検証されます。

すべての上位レベルのプログラムリスクとアーキテクチャリスクは、リスク登録簿に定期的に登録され、リスクは頻繁にレビューされ、評価され、優先順位付けされます。

その後、各リスクを分析し、処置、終結、容認、移管といった最良の対応策を決定します。

- ホストレベルの脆弱性は、頻繁なスキャンによって特定され、優先順位が付けられます。
- サービスおよびWebアプリケーションの脆弱性は、社内のSAST、SCA、DASTテストによって特定されます。
- 新機能と既存のアーキテクチャのリスクは、正式な設計レビューと脅威モデリングによって特定されます。
- FivetranのWebアプリケーション、サービス、および基礎となるインフラストラクチャに対して、定期的な評価を実施するために、サードパーティーのペネトレーションファームと契約しています。
- 発見された脆弱性を報告するセキュリティ・リサーチャーのための責任ある開示ポリシーを維持しています。

インシデント対応

弊社とその顧客に影響を与えるセキュリティ・インシデントに効果的に対応するためのポリシー、手順、トレーニング、およびサポートをFivetranの従業員に確実に提供するため、インシデント対応プログラムを実施しています。

このプログラムの目的は、Fivetranのインフラストラクチャーおよび/または顧客データが関係する予期せぬ事象に対してインシデントレスポンスを提供することにより、セキュリティインシデントが収益、評判および業務遂行能力に与える影響を防止または軽減することです。

Fivetranの社員は、あらゆるインシデントをも抑制、軽減、解決するために適切な措置を講じます。

インシデント対応の方針と手順は、セキュリティ・インシデントに協調的かつ効果的に対応するために策定されました。

これらのポリシーと手順は、すべての対応活動の一環として、また年1回の机上でのシナリオテストを通じて、継続的に改善されています。

弊社は全体的なリスク削減戦略の一環として、業界標準のサイバーセキュリティ賠償責任保険に加入しています。

コンプライアンス

弊社は確立されたセキュリティ業界標準へのコンプライアンスの維持に努めています。SOC 2 Type 2、ISO 27001、PCI DSS、EU94/95プライバシー規則、GDPR、HIPAA基準への準拠を維持しています。

弊社は毎年、独立したSOC 2 (Type 2)レビューを受けており、監査報告書はNDAを前提として、ご要望に応じてすべての既存および見込み顧客に提供されます。この報告書は、Google CloudおよびAmazon Web Services（AWS）のコンプライアンスプログラムの利点を補完するものです。

さらに弊社は、すべてのサブスクリプション・レベルでISO 27001認証を取得し、プレミアム・プランではPCI DSS Level 1の検証も受けました。これらの基準は、グローバルなセキュリティ基準への準拠を示すものであり、当社のSOC 2監査を補完するものです。

ISO/IEC 27001 は、ベンダーに以下の内容を要求しています。

- 脅威、脆弱性、影響を考慮して、情報セキュリティリスクを体系的に検討すること。
- 容認できないと判断されたリスクに対処するために、一貫性のある包括的な一連の情報セキュリティ管理策および／または他の形態のリスク処置を設計し、実施すること。
- 情報セキュリティ管理策が継続的に情報セキュリティのニーズを満たし続けることを確実にするための包括的な管理プロセスを採用すること。

Payment Card Industry Data Security Standard（PCI DSS）では、年間600万件以上の取引を処理する企業を「レベル1」と定義しています。これはPCI DSSのレベルの中で最も高く、最も厳しいものです。

データ・サブプロセッサーとしての潜在的な役割において、FivetranはEU 94/95プライバシー規則およびGDPR規則の原則を遵守します。Fivetranは、米国/EUプライバシーシールドプログラムに登録されています。

弊社は、保護されるべき健康情報（PHI）に対するHIPAA要件を遵守し、HIPAA義務の対象となる顧客（通常は、HIPAA対象事業体）と業務提携契約（BAA）を締結します。

Fivetranは、HIPAA規則の対象事業体ではないため、「HIPAAに準拠」することはできません。HIPAA自体が対象事業体（つまり、HHSによる規制の対象となる事業体）に適用されるからです。Fivetranはデータパイプラインとして機能し、Fivetran環境を通過するPHIが永久に保存されることはありません。すべてのデータ通信は、業界のベストプラクティス（現時点ではTLS 1.2以上）を使用して暗号化されます。一時的な保存は、送信されるデータ量がリアルタイム処理の容量を超え、短期的なキャッシュが必要になった場合に発生することがあります。このような一時保管は暗号化され、デスティネーション（連携先）に到着するまでFivetranのシステム内に保存されます。

Fivetranは、少なくとも年1回、その環境とプラットフォームに対する侵入テストを実施するために、資格のある第三者に依頼しています。

ベンダーとサブプロセッサー

弊社は、データの分類と取り扱い、ネットワークアクセスなどに関する具体的なポリシーを含む、包括的なセキュリティおよびリスク管理プログラムに従っています。

すべてのベンダーとサブプロセッサーは、定期的にリスク評価を受けています。新しいソフトウェアやベンダーの要請には、IT、法務、財務、セキュリティチームの承認が必要です。

開発者とカスタマーサポートの従業員は、開発環境にアクセスするためにOktaによる認証が必要です。さらに、アクセスに関するすべてのリクエストは、管理者とセキュリティチームの承認が必要です。

Oktaへのアクセスには、チーム全体で多要素の要件が適用されます。

Oktaのパスワードや多要素のリセット要求には、本人確認として電話や同僚による認証が必要です。

Fivetranは、安全なソフトウェア開発ライフサイクルのベストプラクティスに従っています。

物理的および環境的なセキュリティ

FivetranはGoogle Cloud、AWS、Azureに依存しているため、物理的および環境的なセキュリティはすべてこれらのプロバイダーによって処理されます。

これらのプロバイダーは、SOC1/2-3、PCI-DSS、ISO27001など、コンプライアンスと規制に関する広範な保証を提供しています。

より詳細な情報については、**Google Cloudのコンプライアンス**と**セキュリティに関する文書**、および**Amazonのコンプライアンス**と**セキュリティに関する文書**をご覧ください。

まとめ

Fivetranは、私たちの組織がデータにアクセスするために毎日使用しています。弊社のプラットフォームが安全であり続けることは、私たち自身のデータだけでなく、お客様の情報を保護するためにも不可欠です。これは弊社の最優先事項です。

自動データ統合製品のリーダーとして、Fivetranの使いやすさを維持しながら、データセキュリティを最優先に考えています。Fivetranについてもっとお知りになりたい方は、弊社営業チーム（**sales@fivetran.com**）までご連絡ください。

セキュリティに関する問題を報告いただくには、**security@fivetran.com**までご連絡ください。

Fivetran is the global leader in modern data integration. Our mission is to make access to data as simple and reliable as electricity. Built for the cloud, Fivetran enables data teams to effortlessly centralize and transform data from hundreds of SaaS and on-prem data sources into high-performance cloud destinations. Fast-moving startups to the world's largest companies use Fivetran to accelerate modern analytics and operational efficiency, fueling data-driven business growth. For more info, visit **Fivetran.com**.