Security White Paper

Multi-Sigma®（AI解析プラットフォーム）

第1.3版

2025年9月1日

株式会社エイゾス

はじめに

White Paperの目的

Multi-Sigma®は深層学習モデルなどの機械学習モデルをベースにお客様のデータを分析することで、未知の入力データに対する出力の予測や出力に影響を与える要因の分析、望ましい出力を実現するための入力値の最適化などを実現する当社のクラウドサービスです。

本ドキュメントは、Multi-Sigma®の提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMSクラウドセキュリティ認証であるISO/IEC 27017の要求に従う公表を行うことを目的とします。

White Paperの対象

Multi-Sigma®の導入を検討中の方
Multi-Sigma®を利用中の方

クラウドサービス情報セキュリティ方針

当社では、クラウドサービス情報セキュリティの方針を定め、ユーザ様に満足いただける機能的でセキュアなサービスの提供を目指しています。
当社の「クラウドサービス情報セキュリティ方針」は以下のURLからご確認頂けます。
[クラウドサービス情報セキュリティ方針]
https://aizoth.com/cloud-service-information-security-policy/

情報セキュリティ方針

当社では、情報セキュリティ方針を定め、機械学習・データサイエンスの提供企業として、お客様からお預かりする情報資産を守ることを経営の最重要課題と位置づけています。
当社の「情報セキュリティ方針」は以下のURLからご確認頂けます。
[情報セキュリティ方針]
https://aizoth.com/security-policy/

情報セキュリティ組織

当社では、情報セキュリティに関する統括責任者を任命し、情報セキュリティに関する統括責任と権限を与えています。また、情報セキュリティ委員会を設置し、情報セキュリティのマネジメントシステムの運用と継続的改善に取り組んでいます。

組織的管理策

責任範囲（共有Model）

仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。

また、当社は、基盤上に構築したアプリケーションに対して責任を負います。

アプリケーション上のデータについては、ユーザ様の責任において保護していただく必要があります。

当社の責任

・Multi-Sigma®のセキュリティ対策

・Multi-Sigma®に保管されたユーザ様情報の保護

ユーザ様の責任

・利用者アカウントの管理（登録、削除、権限設定、管理者設定、アクセス権の設定など）

・パスワード等の利用者の秘密認証情報の管理

・ユーザ様が取り扱うデータに対してのバックアップ

地理的所在地

当社の所在地は日本国、当社がお客様のデータを保存する国は日本および米国となります。当社が基盤として利用するクラウドサービス（Google Cloud）において、日本および米国以外のリージョンにユーザ様のデータを保存する必要性が生じた場合、ユーザ様に事前に通知したうえで行います。
当社の所在地の詳細については、当社ウェブサイト（https://aizoth.com/）をご確認ください。

資産の管理

情報のラベル付け

Multi-Sigma®は、ディレクトリによるファイル管理機能を提供し、ユーザ様のデータ分類をサポートします。Multi-Sigma®上では、プロジェクトの管理とタスクの管理によって対応します。具体的な使用方法の詳細は「スタートアップガイド」をご参照ください。

資産の分離

Multi-Sigma®の上のお客様の情報資産と当社がサービスを運営するために必要となる情報資産については、明確に分離して管理しています。

サービス利用停止後のデータの扱い

Multi-Sigma®で利用者様が作成・保存した利用者様のデータの除去に関しては、90日以内に消去いたします。バックアップデータ期間を含めると、解約後120日までデータは保持されるものとします。ただし、利用者様のデータを含まないサービス共通のログデータは対象外になります。

アクセス制御

利用者アクセスの管理

Multi-Sigma®は、ユーザ様がストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。お客さまは管理者画面から簡単な操作によりアカウント登録を行うことが出来ます。使用方法の詳細は「スタートアップガイド」をご参照ください。

認証情報の管理

初期のアカウント登録手順は弊社からのご連絡に従ってご対応ください。アカウントの登録時に、画面の指示に従いパスワードの設定を行っていただきます。

パスワードの設定はユーザ様のセキュリティポリシーにもとづいて実施してください。
管理者権限はユーザ様のセキュリティポリシーに従い厳重に管理することをお願いします。

特権的権限

管理者コンソールなどの特権的ユーティリティプログラムは管理者権限に限定して利用可能です。管理者権限を厳重に管理することによりユーティリティプログラムの使用制限につながります。使用方法の詳細は「スタートアップガイド」をご参照ください。

暗号

暗号化

データベースに保管されるユーザ様データは、AES-256暗号化アルゴリズムを使用して、ディスクに書き込む前にすべてのデータを自動的に暗号化します。設定や構成は必要なく、サービスへのアクセス方法を変更する必要もありません。承認済みのユーザーがデータを読み取る際に、データは自動的かつ透過的に復号されます。
Multi-Sigmaとユーザ様との間での通信は、SSL/TLSで暗号化し、情報の盗聴等のリスクに対処しています。

暗号化機能に対する規制

Multi-Sigma®において暗号化機能の輸出規制対象になる地域にはサービスを提供していません。

運用のセキュリティ

変更

ユーザ様に影響を与えるMulti-Sigma®の変更は、ご登録頂いたメールアドレス宛に事前通知します。また、各種の変更管理に関する情報は管理者画面より、確認することができます。

バックアップ

システム及びユーザ様データのバックアップは、日次で実行します。バックアップファイルのライフサイクルは30日（最長30日前まではデータベースのフルバックアップ、ストレージファイルの全データを保持、作成から31日目で自動削除）となっています。
ただし、ユーザ様からのバックアップデータの復元等に関するご要望には対応していません。

ログ

Multi-Sigma®の維持管理に必要となる適切なログを取得しています。 ユーザ様が必要となる場合は、Multi-Sigma®内のお問合せフォームからご相談ください。Multi-Sigmaは、基盤として利用するクラウドサービス事業者（Google Cloud）が提供する時刻同期サービスを利用し時刻同期を行っています。ログは協定世界時（UTC）で提供されます。

実務者の運用

Multi-Sigma®の重要な操作手順も含めて、Multi-Sigma®の操作手順については、スタートアップガイドを用意し、提供しています。

クロックの同期

Multi-Sigma® は、基盤として利用するクラウドサービス事業者（Google Cloud）が提供する内部NTP サービスを用いて協定世界時（UTC）と時刻を同期しています。クラウド上の VM／コンテナはデフォルトで同一NTPに同期されています。すべてのログタイムスタンプは UTCで記録・提供されます。時刻源と異なる NTP サーバを併用すると不連続が生じる場合があるため、単一のクロック源への同期を推奨します。

技術的脆弱性の管理

アプリケーションを構築する上で使用するソフトウェアに脆弱性が検知された場合、
Multi-Sigma®のトップ画面等で通知し、速やかに影響調査を行います。
脆弱性情報の収集は以下の手段により行います。
・JPCERTコーディネーションセンターや独立行政法人情報処理推進機構(IPA)、Japan Vulnerability Notes(JVN)から公開される脆弱性情報
・当社関係者による検知
・ユーザ様、基盤を提供するクラウドサービス事業者等の外部からの情報提供

検出した脆弱性については、速やかに影響調査を行い、必要な対策を講じます。対策の状況は随時、Multi-Sigma®のトップ画面にて公表します。

管理者用手順

「スタートアップガイド」等の各種マニュアルの提供に加え、お問い合わせフォームよりQAサポートを提供しています。

クラウドサービスの監視

Multi-Sigma®のウェブアプリ部分が正常に提供されているかに関しては、PaaS事業者の責務で対応を行なっています。Multi-Sigma®のAPIおよび解析コアシステムに関しては、ハードウェア部分はPaaS事業者の責務で対応を行ない、OS部分については最長1日でクリーンな状態に戻るように設計しています。
当社は、Multi-Sigmaが正常に提供され、他社を攻撃する基盤として使用される等不正に使用されていないこと、データの漏洩が発生していないか等の監視を行っています。
監視結果をユーザ様に公開できるサービス機能は有しておりません。監視結果が必要な場合は、Multi-Sigma内のお問合せページからご相談ください。

容量・能力の管理

当社は、サーバリソース、及びネットワークリソースを監視しています。

負荷分散/冗長化

Multi-Sigma®は基盤を提供するクラウドサービス事業者のマネジメントサービスを使用し、複数の仮想サーバに処理を振り分ける、ロードバランシングを採用しています。
また、アプリケーションの構成はマシンイメージとして保存し、即時に複製が可能な状態を整えています。

ブルーグリーンデプロイメント

当社の提供するクラウドサービスは、新バージョンのリリース時に、ブルーグリーンデプロイメントを採用しています。現バージョンの仮想環境（グリーン）と新バージョンの仮想環境（ブルー）を同時に用意し、アクセス先を切り替えることで、瞬時に新バージョンへの移行を可能としています。

装置のセキュリティを保った処分又は再利用

当社は、情報システム管理者に装置の処分又は再利用に関する役割を集中し、従業者による個別対応を排除することで、セキュア且つ確実な装置の処分又は再利用を実現しています。

当社が利用するクラウドサービス事業者のシステム環境におけるストレージデバイス等の装置の処分に関しては、クラウドサービス事業者の廃棄プロセスに基づいて適切に実施されます。

通信のセキュリティ

ネットワーク

Multi-Sigma®では、Virtual　Private　Cloud(VPC)を用いて仮想ネットワークを構築しています。Multi-Sigma®では、他のユーザ様とのネットワーク分離についてはIDによるアクセス資源の論理分離を行っております。ユーザー様と管理用環境は別セグメントで分離されています。

システムの取得、開発及び保守

情報セキュリティ機能

主にユーザ様が検討される情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

機能（ISO/IEC27017の管理策）	本ホワイトペーパーの記述
5.16　識別情報の管理	利用者アクセスの管理
5.17　認証情報	認証情報の管理
5.18　アクセス権	利用者アクセスの管理
8.2　特権的アクセス権	認証情報の管理
8.3　情報へのアクセス制限	利用者アクセスの管理
8.13　情報のバックアップ	バックアップ
8.15　ログ取得	ログ
8.24　暗号の使用	暗号化
CLD.12.4.5クラウドサービスの監視	クラウドサービスの監視

開発プロセス

当社のクラウドサービスの開発は、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発時には、開発環境におけるテストにより、コードの潜在的なバグやパフォーマンスの問題、安全でないコーディングパターンの検出に努めています。また、第三者による脆弱性診断を実施することで、リリース前のみならず、リリース後も定期的な脆弱性診断を行っています。

ブルーグリーンデプロイメント

当社の提供するクラウドサービスは、新バージョンのリリース時に、ブルーグリーンデプロイメントを採用しています。現バージョンの仮想環境（グリーン）と新バージョンの仮想環境（ブルー）を同時に用意し、アクセス先を切り替えることで、瞬時に新バージョンへの移行を可能としています。

サプライチェーン

当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

情報セキュリティインシデントの管理

インシデント対応プロセス

当社では、ISO/IEC27001に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する全ての手順が文書化され、情報セキュリティ委員会により一元的に管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

インシデント対応

Multi-Sigma®に関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

項目	内容
報告する範囲	データの消失、長時間のシステム停止等のユーザ様に大きな影響を及ぼす可能性のある情報セキュリティインシデント
対応の開示レベル	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、すべて同等のレベルで対処します。
通知を行う目標時間	検知から72時間以内を目標に通知します。
通知手順	ご登録頂いたメールアドレス宛、管理者画面

	（必用に応じて電話等の手段を使用する場合もあります。）
問合せ窓口	Multi-Sigmaサポート（ご契約者様専用）
適用可能な対処	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、あらゆる手段を講じて対処します。

また、ユーザ様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、Multi-Sigma®内のお問合せフォームからご連絡ください。

インシデント報告

Multi-Sigma®に関連した情報セキュリティインシデントが発生した場合、上記インシデント対応に記載の方法で通知するとともに、当社のウェブサイト上でも公表を行います。なお、これまでMulti-Sigma®に関連した情報セキュリティインシデントの発生はありません。

順守

適用法令及び契約上の要求事項

利用契約に関する準拠法は、日本法とします。別途、「利用規約」をご参照ください。

証拠の収集

法令また権限のある官公庁からの要求によりMulti-Sigma®上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。それら機関から適法な要請を受けた場合は、法的妥当性の審査を行い、許される場合には事前通知を行い、最小限の範囲での開示を行います。開示が禁止されている期間が満了した後は、可能な範囲で顧客に通知します。合意について別途、「利用規約」をご参照ください。

知的財産権

本サービスを構成する有形または無形の構成物（プログラム、データベース、画像、マニュアル等の関連ドキュメントを含むがこれらに限らない）に関する著作権を含む一切の知的財産権その他の権利は当社に帰属します。別途、「利用規約」をご参照ください。
知的財産権に関する苦情・相談等があった場合は、当社の問合せ窓口までお問い合わせください。

記録の保護

アプリケーションにおけるデータ操作等のログはユーザ様にて保護して頂く必要があります。当社は、仮想ネットワークへのアクセスに関するログ、及びサービスのバージョンアップに関する内部要員による作業ログを一定期間保存します。

情報セキュリティのパフォーマンス評価

当社では、定期的（最低でも年に一回）に情報セキュリティに関する内部監査を実施しています。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化にあわせて、独立した内部監査を行っています。

内部監査結果の開示

当社は、既存または見込みの顧客等からの要請に応じ、監査結果のサマリーを提供可能です。本ホワイトペーパーにてその旨を周知し、以下の手順で開示します。サマリーには、監査実施期間や対象範囲、監査方法、是正計画の有無等が含まれます。

[手順]

申請：以下の窓口に「内部監査結果サマリー開示希望」として連絡

- 連絡先：info@aizoth.com

適格性確認：利害関係の有無を確認し、必要に応じて秘密保持契約（NDA）を締結

作成：最新の監査結果に基づきサマリーを作成（必要に応じてマスキング）

提供：PDF等で提供

情報セキュリティの意識向上，教育及び訓練

当社は、全従業員に対する定期的な情報セキュリティ教育を実施し、情報セキュリティに対する意識向上に努めています。また、クラウドコンピューティングに関する契約相手に対しても、同等レベルの教育を求めています。

セキュリティの責任範囲

Multi-Sigma®の責任分界点の詳細は、組織的管理策の責任範囲をご参照ください。

稼働状況・インシデントに関する情報の公開

当社は、Multi-Sigma®の稼働状況、計画停止、インシデント発生状況について、ウェブサイト上で公開しています。(https://aizoth.com/status-page/)

Multi-Sigma®に関するお問い合わせ

[Multi-Sigma®の問合せ窓口]

TEL：050-3557-9379

メール： info@aizoth.com