Ai Workforceセキュリティホワイトペーパー

1.1版

株式会社 LayerX

1　お客様との責任分界点

株式会社LayerXの責任

株式会社LayerXは、以下のセキュリティ対策を実施します。

- Ai Workforceアプリケーションのセキュリティ対策
- Ai Workforceアプリケーションに保管されたお客様のデータの保護
- Ai Workforceアプリケーションの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策

お客様の責任

お客様は、以下のセキュリティ対策を実施する必要があります。

- 各利用者に付与されたパスワードの適切な管理
- Ai Workforceアカウントの適切な管理（登録、削除、組織管理者権限の付与など）
- ユーザーコンテンツ（お客様がアップロードした情報）、生成コンテンツ（ユーザーコンテンツを本サービスにアップロードしたことによってAi Workforceによって生成された情報）の管理

※ただし、上記は当社が提供している環境においてサービスを提供している場合に限ります。お客様環境においてサービスを提供する場合は、別途定めた契約に準ずるものとします。

2　データ保管場所

- お客様からお預かりしたデータは、日本国内に保管されます。

3　データの削除

- Ai　Workforce利用に関する契約が終了した場合、契約終了から90日以内に、お客様からお預かりしたデータは完全に消去されます。

4　ラベル付け機能

全般

- お客様は、一部を除き各種設定や登録においてラベルを付けることが可能です。
    - （例：ワークフローを識別するため、作成したワークフローに任意の名称を設定することができます）

5　利用者登録および削除

- お客様は、契約の範囲内において、いつでも自由にユーザーの登録・削除を行うことが可能です。

6　アクセス権の管理

- お客様は、登録したユーザーの権限を、自由に切り替えることが出来ます。組織管理者権限を付与することで、各種機能の管理画面にアクセスすることが可能です。

7　パスワードの配布方法

- ユーザーの認証情報は、Ai Workforceとの連携が可能なIdPで管理できます。

8　暗号化の状況

全般

- データベースに保存されるお客様のデータのストレージ暗号化には、FIPS 140-2 認証済みの暗号モジュールが使用されます。 データ (バックアップを含む) は、クエリの実行中に作成される一時ファイルも含めて、ディスク上で暗号化されます。このサービスでは、Azure ストレージ暗号化に含まれる AES 256 ビット暗号が使用され、キーはシステムによって管理されます。ストレージの暗号化は常にオンになっており、無効にできません。
- お客様の端末とシステム間のインターネット通信は、TLSによって暗号化されます。なお、対応しているTLSは、TLSv1.2 以降であり、安全な暗号アルゴリズムを選定して利用しています。
- データベース以外のストレージの暗号化では、サーバ側暗号化(SSE)を使用してクラウドに永続化されるときにデータを自動的に暗号化します。暗号化方式にはAES 256 ビット暗号を利用しています。

9　変更管理

- サービスのバージョンアップ情報を始めとした、各種の変更に関する情報は、LayerX窓口担当者から、サービス登録時にご提供いただいた連絡先宛にご連絡します。

10 手順書の提供

- お客様が利用できる手順書は、ご契約時に所定の方法にてご提供します。

11 バックアップの状況

全般

- データベースに保管される、お客様の各種情報は、日次でバックアップを取得しています。バックアップは、35日分保管されます。但し、お客様によるバックアップデータの復元等に関する要望は、承っておりません。

12 ログのクロックに関する情報

- Ai Workforceサービス内で提供されるログは、日本標準時(UTC+9)をタイムゾーンとして採用しています。
- サービスを提供するサーバーは、NTPを用いて時刻同期を実施しています。

13 脆弱性管理に関する情報

- Ai Workforce開発チームは、システムで利用しているOS、ミドルウェア等に関する脆弱性情報を、定期的に収集しています。
- システムで利用しているコンポーネントに対する脆弱性パッチが公開された場合は、テスト環境での検証を経た後、速やかに適用されます。

14 開発におけるセキュリティ情報

- Ai Workforceシステムの開発では、利用している言語の業界標準やベストプラクティス、および株式会社LayerX AI・LLM事業部のセキュア開発ガイドラインに沿って開発を行っています。

15 インシデント発生時の対応

- お客様に大きな影響を与えるセキュリティインシデント(データの消失、長時間のシステム停止等）が発生した場合は、インシデント発生してから72時間以内を目標に、Ai Workforce利用契約時にご提供頂いた組織管理者のメールもしくは電話にご連絡します。

- 情報セキュリティインシデントに関する問合せは、お客様ごとにご案内しております「Ai　Workforce担当者」の連絡先（メールアドレス）宛にご連絡ください。

16　お客様のデータの保護及び第三者提供について

- お客様から預かったデータを適切に保護することは、株式会社LayerXの責任です。ログデータを含むお客様のデータは、不正なアクセスや改ざんを防ぐため、Ai　Workforce開発チームの一部の人間しかアクセスできない、限られたアクセス権のもとで保管されます。
- 但し、裁判所からの証拠提出命令など、法的に認められた形でお客様のデータの提供を要請された場合、株式会社LayerXは、お客様の許可なく、必要最小限の範囲で、お客様情報を外部に提供する可能性があります。

17　適用法令

- お客様と株式会社LayerXとの間の契約は、日本法に基づいて解釈されるものとします。

18　独立したレビュー

- Webアプリケーションの脆弱性診断を定期的(年1回)に外部ベンダーに依頼し、実施しています。
- 株式会社LayerXは、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS適合性評価制度における、ISMS認証[1]を取得しており、内部監査および外部審査を定期的(年1回)に実施しています。
- 株式会社LayerXは、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS適合性評価制度における、ISMSクラウドセキュリティ認証[2]の取得準備をしています。

19　外部クラウドサービスの利用

- Ai　Workforceではサービスの提供にあたり、外部のクラウドサービスを利用しています。詳細は「外部送信規律（https://layerx.co.jp/privacy/thirdparties/）」に記載の“「Ai　Workforce」に関する公表事項“を参照してください。
- 本サービスにおいて一部の機能を利用する際に、お客様のデータ処理において、以下に記載の海外のリー

[1] https://isms.jp/lst/ind/

[2] https://isms.jp/isms-cls/lst/ind/

ジョンのシステムを利用する場合があります。

- Azure OpenAI
- Azure Container Apps Dynamic Sessions
- （これらのシステムへお客様のデータを送信する場合がありますが、保管はされず、通信も公衆ネットワークを介さない仕組みとなっています）

20 Ai Workforceにおける物理的な機器の廃棄及び再利用時のセキュリティ

- 当社クラウドサービスのインフラストラクチャとして Azureを利用しています。
- サーバなどの装置は、Microsoft　Corporationにより適切に管理され、不要になった場合は、安全な方法で廃棄が行われています。

より詳細な情報は、以下からご確認ください。

Azure インフラストラクチャのセキュリティ

https://learn.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure

改訂履歴

版	改訂日	改訂内容
1.0	2025/05/19	初版発行
1.1	2025/06/12	「20. Ai Workforceにおける物理的な機器の廃棄及び再利用時のセキュリティ」を追加

この資料に関するお問い合わせ

株式会社LayerX
問合せ窓口：https://layerx.co.jp/contact/