公開文書

WINWORKS One クラウドセキュリティホワイトペーパー

文書番号	PUB-CL-002
版数	v1.3
制定日	2026年9月5日
最終改訂日	2026年10月3日
発行	ウィンワークス株式会社

目次

1. はじめに
2. 情報セキュリティのガバナンス
3. 責任分界
4. 準拠法及びデータの所在
5. アカウント及びアクセスの管理
6. 情報の分類及びラベル付け
7. 暗号化
8. ネットワーク及び環境の分離
9. ログの取得、保護及び提供
10. 監視、可用性及びバックアップ
11. 脆弱性管理、開発及び変更管理
12. インシデントの管理及び通知
13. 契約終了時のデータの取扱い
14. 改訂履歴

1. はじめに

1.1 本書の目的

本サービス「WINWORKS One」は、シフト制で勤務する職場における勤務シフトの作成および管理を支援するクラウドサービスです。24時間交代制のように複雑な勤務体系を持つ職場にも対応しており、医療、介護、小売、食品製造をはじめ、業種を問わずご利用いただいています。

本サービスは、従業者の氏名、所属、スキルおよび勤務実績といった個人データをお預かりします。本書は、お預かりしたデータを当社がどのように保護しているかを、ご利用中のお客様および導入をご検討中のお客様にご説明するものです。

以下、ウィンワークス株式会社を「当社」、WINWORKS One を「本サービス」といいます。

1.2 本書の対象範囲

本書は、本サービスおよびその提供に関連する当社の業務を対象とします。当社の情報セキュリティマネジメントシステムの適用範囲は、R&D およびカスタマーサクセスとし、本サービスの開発、運用、保守および顧客支援に係る業務を含みます。

本サービスの稼働基盤として利用するクラウド基盤提供者の管理策については、責任の分担を第3章に示したうえで、当社が確認している範囲において記載します。

1.3 本書の位置づけ

当社は、情報セキュリティ基本方針およびクラウドサービス情報セキュリティ方針を定め、当社ウェブサイトにおいて公開しています。本書は、これらの方針に基づき本サービスにおいて実施している具体的な管理策をご説明するものです。

情報セキュリティ方針： `https://www.win-works.com/security-policy`

個人データの取扱いについては、当社のプライバシーポリシーおよび別表（外国にある第三者への提供）に定めています。

プライバシーポリシー： `https://www.win-works.com/privacy-policy`

別表（外国にある第三者への提供）： `https://www.win-works.com/privacy-policy-appendix`

1.4 本書の改訂

本サービスの機能の変更、当社の管理策の変更、または法令の改正に応じて本書を改訂します。改訂した場合は、版数および最終改訂日を更新のうえ、同一の URL において公開します。改訂の履歴は第14章に記載します。

本書は、作成時点における情報を提供するものであり、契約上の保証を構成するものではありません。記載の内容は予告なく変更されることがあります。本サービスの利用に関する当社とお客様の権利義務は、ＷＩＮＷＯＲＫＳサービス利用約款その他の契約の定めるところによります。

1.5 お問い合わせ

お問い合わせの内容に応じて、次の窓口にて承ります。

技術的なお問い合わせ

本書の内容、本サービスの情報セキュリティに関するご質問、情報セキュリティ事象またはインシデントに関するご連絡、および障害に関するご連絡

`support@win-works.com`

契約に関するお問い合わせ・法的な通知

利用約款に定める通知方法による当社への通知、知的財産権に関するご相談、その他契約に関するお問い合わせ

`administration@win-works.com`
〒100-0014　東京都千代田区永田町2-9-6　十全ビル804
電話：03-3503-5262

利用約款に定めるサポートサービスは、当社から直接ご購入いただいたお客様が別途特定する3名までのご担当者に対して提供します。代理店を通じてご購入いただいた場合は、代理店にお問い合わせください。

2. 情報セキュリティのガバナンス

2.1 情報セキュリティ方針

当社は、情報セキュリティ基本方針およびクラウドサービス情報セキュリティ方針を定めています。

クラウドサービス情報セキュリティ方針では、当社とお客様の責任の分担、お預かりしたデータの取扱い、特権的な権限を用いた操作、お客様への通知といった、クラウドサービスの提供に固有の事項を定めています。

これらの方針は年1回見直し、事業やサービスの内容に変更が生じた場合は改訂します。

2.2 情報セキュリティに関する役割及び責任

当社は、情報セキュリティに関する管理体制を定め、責任者および担当者を任命しています。主要な役割は次のとおりです。

- **情報セキュリティ責任者** — 情報セキュリティマネジメントシステムの運用に関する責任を負い、脆弱性の評価および対応方針の決定、インシデントの重大性の判断、ならびにお客様に影響を及ぼす変更の承認を行います
- **クラウドサービス管理者** — 本サービスの提供に係る技術的な管理を統括します
- **R&D 部門責任者** — 本サービスの変更がお客様に及ぼす影響の有無を判定します

当社とお客様の間の責任の分担については、第3章に記載します。

2.3 従業者に対する教育

当社は、全従業者を対象とする情報セキュリティ教育を実施しています。

本サービスの運営に従事する従業者に対しては、これに加えて、責任の分担、お預かりしたデータの取扱い、障害およびインシデント発生時のお客様への通知、特権的な権限を用いた操作における留意事項について、年1回教育を実施しています。

2.4 第三者による審査

当社は、JIS Q 27001:2023（情報セキュリティマネジメントシステム）および JIP-ISMS517-1.0（ISMS クラウドセキュリティ）の認証取得に向け、認証機関による審査を受けています。

認証を取得した後は、認証範囲、認証規格、登録番号および有効期限を当社ウェブサイトにおいて公開します。

3. 責任分界

3.1 当社とお客様の責任範囲

本サービスの提供および利用にあたり、当社とお客様の責任範囲を次のとおり定めています。

お客様の責任範囲

- アカウントの管理（利用者アカウントの登録・変更・削除、権限の設定、認証情報の管理）
- 提供機能の設定（業務に応じた各種設定、権限体系の設計）
- 提供機能におけるデータの登録および削除（従業者情報、勤務ルール、シフト情報等の入力および保守）

当社の責任範囲

- ソフトウェアの開発（機能の設計、実装および品質の確保）
- サーバーおよびネットワークの設定
- 稼働基盤の管理（物理的な設備はクラウド基盤提供者の責任範囲となります。第3.2節参照）
- 監視・保守（稼働状況の監視、脆弱性への対応、変更の管理）
- 障害対応（障害の検知、原因の調査、復旧およびお客様への通知）

お客様の責任範囲に属する事項について、ご依頼があった場合は、問い合わせ対応の一環として当社が支援を行うことがあります。ただし、当社が独自の判断でお客様のアカウントやデータを操作することはありません。

3.2 クラウド基盤提供者との責任の分担

本サービスは、アマゾン ウェブ サービス（以下「AWS」といいます。）の東京リージョンを稼働基盤として利用しており、次の分担が適用されます。

AWS の責任範囲

データセンターの物理的なセキュリティ、電源および空調等の設備、ハードウェアの調達および保守、記憶媒体の廃棄、仮想化基盤の管理

当社の責任範囲

サーバーおよびネットワークの設定、オペレーティングシステムおよびミドルウェアの管理、アプリケーションの開発および運用、データの暗号化設定、アクセス制御の設定、ログの取得および保管

当社は、AWS が取得している第三者認証（ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 等）および AWS が公開する情報により、AWS の責任範囲における管理の妥当性を確認しています。

3.3 本サービスの提供に利用するクラウドサービス

当社は、**本サービスのシステムに組み込まれて連携して動作し、本サービスの提供に伴いお客様のデータを処理するクラウドサービス**を、ピアクラウドサービスとして特定しています。該当するのは次のとおりです。

- **AWS** — 本サービスの稼働基盤。稼働基盤の全体を同社のサービスにより構成しており、代替の手段を持ちません
- **Sentry** — 本サービスのアプリケーションと連携し、異常を検知します
- **SendGrid** — 本サービスのメール通知機能から呼び出され、同機能をご利用のお客様に対する通知メールを送信します

このうち AWS 以外のサービスは、停止した場合も本サービスの稼働そのものは継続します。

次のクラウドサービスも本サービスに関連して**継続的に**利用していますが、本サービスのシステムとは連携せず、当社のサポート業務等の遂行において利用するものであるため、ピアクラウドサービスとしては特定せず、供給者として個別に管理しています。

- **Zendesk** — お問い合わせの受付および履歴の管理。返信漏れの防止および返信期限の管理により、サポート業務の正確性を確保するために利用します
- **Anthropic（Claude）** — サポート業務および支援業務において利用。本サービスの稼働には関与しません

Anthropic が提供する Claude については、法人向けプランを利用しており、**同社の商用利用規約により、入力された情報および生成された応答を同社の機械学習に利用しないこととされています。**また、**本サービスのシステムそのものが生成AIを呼び出すことはなく、勤務シフトの計算は数理最適化（数理計画法）によります。**

ピアクラウドサービスおよび上記のサービスについて、第三者認証の取得状況、データの保管場所、お客様データの取扱いに関する規定、可用性、インシデント発生時の通知に関する規定を確認し、水準が維持されていることを年1回確認しています。

当社が外国にある事業者に個人データの取扱いを委託しているものの一覧は、別表（外国にある第三者への提供）に掲げています。本節に掲げるものは、本サービスの提供に関連して継続的に利用するクラウドサービスであり、**別表が掲げる範囲とは目的が異なるため一致しません。**

4. 準拠法及びデータの所在

4.1 準拠法及び管轄

本サービスの利用に関して適用される準拠法は、日本国の法令とします。管轄裁判所は利用約款に定めています。

4.2 本サービスのデータの保管場所

本サービスにおいてお預かりするデータの本体は、AWS の東京リージョンにおいて保管しており、**日本国内のデータセンターに所在します**。他のリージョンへデータを複製する構成は採用していません。

本サービスの提供およびサポートに関連して利用するクラウドサービスにおける保管場所は、次のとおりです。

事業者	サービス	保管国	取り扱う情報
Amazon Web Services, Inc.	Amazon Web Services	日本（東京リージョン）	本サービスにおいてお預かりするデータの全般
Anthropic, PBC	Claude	**アメリカ合衆国（同社が利用する事業者においては、その他の国又は地域において取り扱われることがあります。** **※）**	サポート業務及び支援業務の遂行にあたり入力される情報
Functional Software, Inc.	Sentry	アメリカ合衆国	異常の検知に伴い記録されるエラー情報（保持期間90日）
Zendesk, Inc.	Zendesk	アメリカ合衆国、アイルランド、ドイツ、英国、日本又はオーストラリア	お問い合わせに含まれる情報

（※）Anthropic, PBC が利用する事業者の名称、所在地及び業務の内容は、同社のウェブサイト（ `https://www.anthropic.com/subprocessors` ）において公表されています。

次のサービスは、本サービスのメール通知機能をご利用のお客様についてのみ利用します。同機能をご利用でないお客様の情報が、当該事業者に提供されることはありません。ご利用の有無が不明な場合は、 `support@win-works.com` へお問い合わせください。当社において確認のうえ回答いたします。

事業者	サービス	保管国	取り扱う情報
Twilio Inc.	SendGrid	アメリカ合衆国（送信要求の受付は日本国内で行われ、電子メールアドレス等の保存は米国内で行われます。）	通知メールの送信先の電子メールアドレス及び宛名

「保管国」は、データが物理的に保管される国を示すものであり、事業者が所在する国とは一致しないことがあります。

本表は、本サービスの提供及びサポートに関連して継続的に利用するクラウドサービスを掲げるものです。当社が外国にある事業者に個人データの取扱いを委託しているものの全体は、別表（外国にある第三者への提供）に掲げています。

4.3 知的財産権

本サービスの利用における知的財産権の帰属、および第三者の権利侵害が判明した場合の対応は、利用約款に定めています。

知的財産権に関わるご相談は、第1.5節に記載した契約に関するお問い合わせの窓口にて承ります。

4.4 公的機関からの開示要請

法令に基づき権限を有する公的機関から、適法な手続により情報の開示または提供の要請があった場合、当社は、お客様への通知およびお客様の同意を経ることなく、当該機関に情報を開示します。

本項の取扱いは、2027年1月1日に施行される利用約款第16条第2項において明文化されます。同項は、お預かりしているデータ等を第三者に開示しないことを原則としたうえで、その例外として、法令に基づく場合、当社のプライバシーポリシー第7条第1項に定めるサービス提供事業者に取扱いを委託する場合、および同約款第22条に定める再委託の場合を掲げるものです。

4.5 暗号に関する輸出規制

当社が利用している暗号化技術は、公開された標準的な暗号アルゴリズムであり、輸出規制の対象となる暗号化は行っていません。

5. アカウント及びアクセスの管理

5.1 アカウントの発行と管理

サービスの利用開始時、当社は申込書に記載されたメールアドレスに対して、パワーユーザ権限を有する初期アカウントを発行します。

以後のアカウントの追加、変更および削除は、お客様の管理者が管理画面から実施します。**当社がお客様に代わってアカウントを操作することはありません**。ご依頼があった場合は、問い合わせ対応の一環として支援します。

5.2 認証

SSO 認証

本サービスは SAML 2.0 による SSO 認証に対応しています。お客様の ID プロバイダと連携することにより、お客様の認証基盤で要求される多要素認証を、本サービスの認証にも適用できます。

当社は、本サービスの機能として二要素認証を単独では提供していません。多要素認証は、SSO により連携する ID プロバイダ側の機能により実現する構成としており、お客様の組織における認証方針を一元的に適用いただけます。

パスワード認証

SSO を利用されない場合は、利用者IDおよびパスワードによる認証となります。文字数、文字種の組み合わせ、有効期限、初回ログイン時の変更要求を設定でき、お客様の組織のパスワードポリシーに応じた強度を設定いただけます。

導入時は当社のコンサルタントがお客様と協議のうえ設定し、以後の変更はお客様の管理者が行います。**設定されたパスワードは、当社の管理者を含め閲覧できない仕様です。**

5.3 パスワードの再設定

お客様の管理者が、管理画面から利用者のパスワードを再設定できます。

管理者ご自身のパスワードについては、当社への依頼により再設定します。申込書に記載された連絡先との照合により本人性を確認したうえで実施します。

5.4 権限の管理

画面および機能の制限

ユーザーグループを自由に設定し、グループごとに参照できる画面と使用できる機能を指定できます。権限を持たない利用者は、当該画面を表示できません。

登録情報の閲覧制限

利用者の所属（部署、部門等）に応じて、参照できる従業者の情報を制限できます。これにより、お客様の組織内で、自らの管理範囲を超える個人データを参照できない構成としています。

5.5 WebAPI

利用者向けに情報取得用の WebAPI を提供しています。次の仕様により、通常のセキュリティ手順を迂回できない設計としています。

- アクセスできるのは API 権限を付与されたアカウントに限られる
- 当該アカウントはパスワードの設定が必須であり、認証を経ずに利用することはできない
- **提供する機能は情報の読み出しのみで、書き込み操作は提供していない**

なお、オペレーティングシステムやデータベースへ直接アクセスするような特権的なプログラムは、お客様に提供していません。

5.6 当社の要員によるアクセス

当社は、利用約款に明示的に許諾されている場合、お客様の利用に必要な場合、および障害の調査に必要な場合を除き、お客様のデータにアクセス、編集または改変することはありません。

当社の要員がお客様の環境へアクセスする際は、お客様と同一の経路を用い、第8.3節に記載する送信元 IP アドレスの制限の対象となります。

サーバーへの管理接続は AWS の管理サービスを経由しており、SSH をインターネットに公開していません。実行された操作は記録されます。

5.7 操作手順の提供

本サービスの操作手順は、利用者向けマニュアル及び管理者向けマニュアルにより提供します。管理者向けマニュアルには、アカウントの発行及び削除、権限の設定、パスワードの再設定その他の管理操作の手順を記載しています。

6. 情報の分類及びラベル付け

6.1 登録情報のグルーピング

本サービスは、登録された情報を分類するため、次のラベルによるグルーピング機能を提供しています。

- **職員** — スキルによるグルーピング
- **日** — 業務によるグルーピング
- **シフト** — シフトラベルによるグルーピング
- **ルール** — ルールラベルによるグルーピング

6.2 属性情報の付与

職員に対してスキル等の属性情報を付与できます。付与した属性に応じて、参照できる登録情報を制限することもできます。

これにより、お客様の組織の実態に応じた情報の分類と、分類に基づくアクセス制御を適用いただけます。

7. 暗号化

7.1 保存データの暗号化

データベース、ファイルの保管領域およびバックアップを含め、**保存されるすべてのデータを AES-256 により暗号化しています**。暗号鍵は AWS の鍵管理サービスにより管理しています。

7.2 通信データの暗号化

ブラウザおよび WebAPI からのアクセス、当社の要員による運用操作を含め、**すべての通信を HTTPS（SSL/TLS）により暗号化しています。**

HTTP でのアクセスは HTTPS へリダイレクトされ、利用可能な TLS バージョンは 1.2 以上に制限しています。

8. ネットワーク及び環境の分離

8.1 環境の分離

本番環境は、当社が利用する開発環境、運用保守環境およびデモ環境と分離しています。

開発環境 — 本番環境とは独立した環境であり、開発環境において本番環境のデータを使用することはありません。

運用保守環境 — バージョンアップ内容の事前確認や調査依頼への対応のため、本番環境から複製したデータを保持することがあります。このため本番環境と同等の安全管理措置を適用したうえ、**接続できる通信元を当社の環境に限定し、アクセスできる要員を限定しています**。お客様が検証にご参加いただく期間に限り、当該お客様の通信元を追加して許可します。

デモ環境 — 架空のデータのみを保持し、お客様のデータを保持しません。

8.2 環境間及びテナントの分離

本番環境は、他の環境とネットワーク（VPC）を分けて構築し、環境間の通信を業務上必要な範囲に限定しています。

お客様ごとのテナントは論理的に分離しており、**お客様が他のテナントのデータへアクセスすることはできません。**

8.3 外部からのアクセスの制限

データベースはインターネットから直接到達できない領域に配置し、外部との通信は業務上必要な範囲に限定しています。許可していない通信はすべて遮断する構成です。

お客様ごとに、許可する送信元 IP アドレスを設定する機能を備えています。固定の IP アドレスを保有されるお客様については、当該お客様の環境へアクセスできる通信元を、指定された範囲に限定します。

固定の IP アドレスを保有されないお客様にはこの制限を適用していませんが、利用者の認証、通信の暗号化および次項の防御は他のお客様と同一に適用されます。

これらのネットワークの構成およびアクセス制御の設定は、変更履歴を追跡できる形で管理し、年1回内容を確認しています。

8.4 攻撃への防御

WAF（Web Application Firewall）により、一般的な攻撃パターンを検知・遮断しています。

9. ログの取得、保護及び提供

9.1 お客様が参照できる操作ログ

本サービスは、利用者による**主な操作**を「操作ログ」として記録しています。すべての操作が記録の対象となるわけではなく、記録の対象とする操作の一覧はマニュアルに記載しています。

記録する内容は、日時、操作したユーザー、操作した機能、操作の内容および操作の対象です。

操作ログの閲覧権限を付与された利用者が、管理画面から期間やユーザーを指定して出力できます。**お客様が参照できる範囲は直近1年分です。**

9.2 当社が保管するログ

アプリケーションのエラーログ、サーバーのログおよびアクセスログを、**1年間保管しています。**

これらのログは保存時に暗号化され、当社の要員のうち権限を付与された者のみが参照できます。

なお、異常の検知に用いる外部サービス（第3.3節に記載する Sentry）に記録されるエラー情報の保持期間は90日です。同期間の経過により当該サービス上のエラー情報は削除されますが、当社が保管する上記のログはこれと別に保管されます。

9.3 調査及び証拠の提供

お客様の利用範囲におけるログの調査は、原則として「操作ログ」機能によりお客様自身に実施していただきます。

事象が重大であると判断された場合は、当社が保管するログの内容を確認のうえ、お客様へ提出することを検討します。

公的機関からの開示要請への対応については、第4.4節に記載のとおりです。

9.4 時刻の同期

本サービスを構成するサーバーの時刻は、クラウド基盤提供者が提供する時刻同期サービスにより同期しています。

10. 監視、可用性及びバックアップ

10.1 稼働状況の監視

本サービスの稼働状況および応答性能を継続的に監視しています。**異常を検知した場合に当社の要員へ通知される仕組み**としており、通知を受けた要員が原因を確認し、必要に応じて障害対応の手続に移行します。

対応の手順および判断基準は、当社の障害対応手順に定めています。

10.2 処理能力の確保

データベースは負荷に応じて処理能力が自動的に増減する構成を採用しています。利用者の増加に対しては、サーバーの追加により対応します。

10.3 バックアップ

データベースのバックアップを**日次で取得**しており、**35日前までの任意の時点に復元できます**。バックアップの取得は、クラウド基盤提供者の機能により自動的に実行されます。

バックアップは保存時に暗号化され、本体のデータと同一のリージョン内に保持されます。

当社は、自動バックアップが有効であること及び復元可能な時点の範囲が設定どおりであることを、月次で確認しています。

10.4 復旧の手順

復旧の手順および判断基準は、当社の障害対応手順に定めています。バックアップからの復元については、実施する項目と確認する事項を手順書において定めています。

本番環境の稼働への影響を避けるため、復元を伴う確認は運用保守環境において実施します。

10.5 サービスの一時的な中断

利用約款に定める場合、すなわち臨時の保守点検が必要となったとき、通信回線や電力の供給が中断されたとき、不可抗力によりサービスを提供できないとき、または外部からの不正アクセス等により一時的な中断が必要となったときは、事前の連絡なくサービスの提供を中断することがあります。緊急を要する脆弱性への対処も同様です。

この場合は、中断の事実および理由を、実施後速やかに第12.3節に記載する方法により通知します。

定期的な保守点検については、第11.3節に記載するとおり事前に通知します。

11. 脆弱性管理、開発及び変更管理

11.1 脆弱性への対応

当社は、クラウド基盤提供者からのセキュリティ情報および公的機関の公表情報により、本サービスに影響を及ぼす可能性のある脆弱性情報を収集しています。

収集した情報は、本サービスにおける該当箇所の有無、影響範囲および深刻度により評価し、対応の要否と緊急度を判断します。評価および対応方針の決定は情報セキュリティ責任者が行います。

対応を要すると判断した場合は、修正プログラムの適用、設定変更または代替措置により速やかに是正します。

お客様への通知は、お客様に影響が生じた場合、またはお客様側での対処が必要となる場合に行います。当社の責任範囲内で是正が完結し、お客様に影響が及ばない場合は、個別の通知は行いません。

11.2 セキュリティに配慮した開発

環境の分離 — 第8.1節に記載のとおり、本番環境と開発環境を分離し、開発環境において本番環境のデータを使用しません。

変更の管理 — ソースコードの変更は、レビューによる承認を経ずに本番環境へ反映できない仕組みとしています。レビューでは、認証情報等の機密情報が含まれていないこと、記録すべき操作がログに残ることを確認します。

11.3 変更の事前通知

本サービスの変更によりお客様に影響が生じる場合は、次の区分に従い事前に通知します。

区分	通知の時期
計画的な保守作業に伴いサービスが一時停止する場合	1週間前まで
仕様変更に伴いお客様へ大きな影響を及ぼす場合	1ヶ月前まで
サービスを廃止する場合	6ヶ月前まで

通知する内容は、変更の内容、実施の日時、お客様への影響の範囲、およびお客様側で必要となる対応の有無です。通知の方法は第12.3節のとおりです。

お客様の設定、操作および出力に変化を生じない変更（内部処理の改善、不具合の修正等）については、個別の通知を行いません。

お客様への影響の有無および区分の判定は、R&D 部門責任者が行い、情報セキュリティ責任者が承認します。

11.4 変更の実施及び完了時の通知

変更の実施後、完了した旨を同一の方法により通知します。サービスの一時停止を伴う変更については、サービスの再開を確認したうえで完了を通知します。

12. インシデントの管理及び通知

12.1 問合せの受付

情報セキュリティ事象およびインシデントに関する問合せは、第1.5節に記載した技術的なお問い合わせの窓口（ support@win-works.com ）にて受け付けます。

12.2 重大なインシデントの通知

セキュリティインシデントがお客様に重大な影響を及ぼす場合、**当社が発生を確認した時点から1営業日以内を目標に**、登録された連絡先へ電子メールにて通知します。重大性の判断は情報セキュリティ責任者が行います。

本書において「営業日」とは、土曜日、日曜日および国民の祝日に関する法律に規定する休日を除く日をいいます。

インシデントが長期にわたる可能性がある場合は、調査および復旧の進捗に応じて、随時、電子メールにより続報を通知します。

12.3 通知の方法

通知は、利用約款に定める通知方法により、申込書に記載された電子メールアドレス宛の電子メールまたは書面により行います。

本サービスのお客様は契約に基づく法人に限られ、連絡先が特定されているため、**登録された連絡先への個別の通知により確実に到達させる方法を採用しています。**

13. 契約終了時のデータの取扱い

13.1 削除の方法

本サービスは、一つのデータベースに複数のお客様のデータを収容する方式です。このため、**特定のお客様のデータのみを記憶媒体ごと物理的に消去することはできず、データベース上での削除により対応します。**

削除したデータが保存されていた記憶媒体の再利用および廃棄は、クラウド基盤提供者の責任範囲であり、NIST SP 800-88（記憶媒体のサニタイズに関するガイドライン）に定める手法により処理されます。

13.2 契約終了時の削除

サービス利用契約が終了した場合、**終了の日から3ヶ月以内に**、当該契約に対応するデータを、これに紐づく利用者情報および業務データとあわせてデータベース上から削除します。

削除の処理を行った後、当該データを復元することはできません。

なお、利用者アカウントが削除された場合、当該アカウントに係るデータは速やかに削除します。

13.3 バックアップに含まれるデータ

バックアップに保存されたデータは、保持期間（35日）の経過に伴い順次消失します。

当該期間中は削除前の時点への復元が技術的に可能ですが、復元は障害対応の手続に基づく場合に限り、情報セキュリティ責任者の承認を得て実施します。

13.4 ログ及び問合せの記録の取扱い

アプリケーションのログおよびアクセスログは、時系列に蓄積されるものであり、お客様ごとに区分して抽出することができません。このため、**契約の終了に伴う個別の削除は行いません**。これらは第9.2節に記載する保持期間（1年）の経過により削除されます。

お問い合わせの記録および当社との間の電子メールについては、対応品質の維持および製品の改善のため、契約の終了後も保持します。これらへのアクセスは、サポート業務に従事する要員に限定しています。

14. 改訂履歴

版数	日付	改訂内容
v1.0	2026年9月5日	制定
v1.1	2026年9月27日	**プライバシーポリシー、別表（外国にある第三者への提供）および利用約款の改定（2026年10月1日公開）にあわせて改訂した。**（1）第1.3節に、プライバシーポリシーおよび別表の URL を加えた。（2）第1.4節に、本書が契約上の保証を構成しない旨を加えた。（3）第3.3節に「継続的に」を補い、本節が掲げる範囲と別表が掲げる範囲とが目的を異にするため一致しない旨を明記した。（4）第4.2節の Anthropic, PBC の保管国に、同社が利用する事業者においてはその他の国又は地域において取り扱われることがある旨および副処理者一覧の URL を加えた。**従前の「アメリカ合衆国」のみの記載は、別表の記載より狭いものであった。**（5）第4.4節に、本項の取扱いが2027年1月1日に施行される利用約款第16条第2項において明文化される旨を加えた。（6）認証の取得状況に関する記載（第2.4節）は変更していない。
v1.2	**2026年9月27日**	**ISMS クラウドセキュリティのベースライン分析（WINWORKS One（CSP））との突合により改訂した。**（1）**第5.7節（操作手順の提供）を新設した。**ベースラインの **CLD.12.1.5（実務管理者の運用のセキュリティ）**に対応する記述が本書になかったためである。（2）**第9.1節の操作ログについて、お客様が参照できる範囲を「直近3ヶ月分」から「直近1年分」に訂正した。実際の稼働は1年分であり、従前の記載が誤りであった。**ベースラインの **A.8.15（ログ取得）**と一致する。（3）**第10.3節に、自動バックアップが有効であること及び復元可能な時点の範囲が設定どおりであることを月次で確認している旨を加えた。**ベースラインの **A.8.13（情報のバックアップ）**に対応する。確認は月次点検 **M21** による。（4）第8章及び第10.4節において、本番環境以外の環境の呼称を「運用保守環境」に改め、第8.2節の記述を改めた
v1.3	**2026年10月3日**	**内部監査の結果を受け、第3.3節のピアクラウドサービスの特定の基準を改めた。**従前の「本サービスの中核をなす機能を担い、その停止が本サービスの停止に直結するもの」を「本サービスのシステムに組み込まれて連携して動作し、本サービスの提供に伴いお客様のデータを処理するもの」に改め、**Sentry 及び SendGrid をピアクラウドサービスとして特定した。**Zendesk 及び Anthropic（Claude）は、本サービスのシステムとは連携せず、当社のサポート業務等の遂行において利用するものであるため、特定していない。

ウィンワークス株式会社

〒100-0014　東京都千代田区永田町2-9-6　十全ビル804

本書に関するお問い合わせ： support@win-works.com

以上