WISE CLOUD SERVICE
audit as a service

セキュリティ
ホワイトペーパー

株式会社エアー

2025 年 11 月 28 日

目次

改訂履歴

日　付	改訂内容	備　考
2023/3/1	初版	
2023/5/15	誤記、表記のゆれを修正	
2023/10/23	P10　23.情報のバックアップ 　バックアップを 1 世代保管→7 世代保管に変更 P10　25.クロックの同期 　時刻同期の方式を NTP→NTP または PTP に変更	
2024/11/01	P9　17. 仮想マシンの要塞化 　設備にアクセス可能な者の限定および作業時のログ取得について追記 P11　27. 技術的ぜい弱性の管理 　ぜい弱性情報を収集しているチームを追加 P13　34. 責任及び手順 　インシデント発生連絡までの目標日数を追記 P14　39. 記録の保護 　記録対象を明確化	
2025/11/28	P8　16. 仮想コンピューティング環境における分離 　シングルテナント構成である旨を記載。 P11　28. ネットワークの分離 　データの分離に関する記載を削除（16. 仮想コンピューティング環境における分離に記載）	

1. このホワイトペーパーの目的

このホワイトペーパー（以下、本書）は、株式会社エアー（以下、当社）が提供するクラウドサービスである WISE Audit as a Service（以下、本サービス）における、セキュリティへの取り組みについて記載したものです。クラウドセキュリティの国際規格 ISO/IEC 27017 の中で、特に利用者に向けて情報開示が求められる事項について、セキュリティへの取り組みをご確認いただくことを目的としています。

ISO/IEC 27017 は、クラウドサービスに関する情報セキュリティ管理策のガイドライン規格です。情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC 27001 の取り組みを ISO/IEC 27017 で強化することで、クラウドサービスにも対応した情報セキュリティ管理体制を構築することができます。

本書では、ISO/IEC 27017「情報セキュリティ管理策の実践の規範」の項番に沿って本サービスの管理策を記載します。

2. 情報セキュリティのための方針群（ISO/IEC27017 項番：5.1.1）

本サービスでは、当社の情報セキュリティ方針に従い、セキュリティに関して極めて重要な事項として取り扱い、サービス運営を行います。

当社の情報セキュリティ方針は https://air.co.jp/profile/security/ をご覧ください。また、クラウドサービス情報セキュリティ方針は https://air.co.jp/profile/cloudsecurity/ をご覧ください。

3. 情報セキュリティの役割及び責任（ISO/IEC27017 項番：6.1.1）

3.1. 当社の責任

当社は、以下のセキュリティ対策を実施します。

- 本サービスのセキュリティ対策
- 本サービスに保管されたお客様データの保護
- 本サービス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

3.2. 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。

- パスワードの適切な管理
- アカウントの適切な管理（登録、削除、管理者権限の付与など）

4. 関係当局との連絡（ISO/IEC27017 項番：6.1.3）

当社の所在地は、当社ウェブサイト https://air.co.jp/ にてご確認ください。

また、本サービスでお客様からお預かりしたデータ（以下、「ユーザーデータ」と言う）は、Azure の東日本リージョンに保管します。

5. クラウドコンピューティング環境における役割及び責任の共有及び分担（ISO/IEC27017 項番：CLD.6.3.1）

本サービスでは、サービスの提供環境における役割及び責任について利用規約に定め、サービスを提供します。

本サービスの責任分界点については、「3.情報セキュリティの役割及び責任」をご参照ください。

6. 情報セキュリティの意識向上、教育及び訓練（ISO/IEC27017 項番：7.2.2）

当社では情報セキュリティ方針（https://air.co.jp/profile/security/）およびクラウドサービス情報セキュリティ方針（https://air.co.jp/profile/cloudsecurity/）を定め、方針に従いサービスを運営しています。また、クラウドサービスカスタマデータ及びクラウドサービス派生データを取り扱う社員に対する定期的な教育を実施しています。

7. 資産目録（ISO/IEC27017 項番：8.1.1）

ユーザーデータと当社がサービスを運営する為の情報は、明確に分離しています。

8. クラウドサービスカスタマの資産の除去（ISO/IEC27017 項番：CLD.8.1.5）

本サービス利用に関する契約が終了した場合、契約終了日翌日から 30 日以内に、ユーザーデータを削除します。

また、正式なプラン申し込みなくトライアルの期間が満了した場合や、本サービスの利用料金の支払いを遅滞するなどして利用停止となった場合には、ユーザーデータを削除します。

削除したユーザーデータは、当社であっても復旧することができません。

【削除対象となるユーザーデータ】

次のデータを除き、お客様が本サービスに登録した全てのユーザーデータを削除します。

- 本サービスの契約/請求/入金に関するデータ
- 本サービスの窓口責任者・サポート窓口担当者の氏名および連絡先

9. 情報のラベル付け（ISO/IEC27017 項番：8.2.2）

お客様は、ユーザーをお客様自ら追加したグループにグルーピングすることが可能です。

10. 利用者登録および登録削除（ISO/IEC27017 項番：9.2.1）

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・変更・削除を行うことが可能です。登録・変更・削除に必要な手順、情報はマニュアルに記載しています。

11. 利用者アクセスの提供（ISO/IEC27017 項番：9.2.2）

お客様は、ユーザーに対して本サービスの各種管理者権限を自由に付与することができます。 権限設定に必要な手順、情報はマニュアルに記載しています。

12. 特権的アクセス権の管理（ISO/IEC27017 項番：9.2.3）

運用管理ツールへのアクセスに関しては、ID とパスワードの認証に加え、アクセス元 IP アドレスによる制限をする機能を提供しています。また、パスワードポリシー（複雑さ要件）の強制についても機能提供しています。

13. 利用者の秘密認証情報の管理（ISO/IEC27017 項番：9.2.4）

本サービスの運用管理ツールを利用される際のパスワードの変更に必要な手順、情報はマニュアルに記載しています。

14. 情報へのアクセス制限（ISO/IEC27017 項番：9.4.1）

本サービスの管理者権限および権限ごとにアクセス可能な範囲については、マニュアルに記載しています。

15. 特権的なユーティリティプログラムの使用（ISO/IEC27017 項番：9.4.4）

セキュリティ手順を回避し各種サービス機能の利用を可能とするユーティリティプログラムの提供は行っていません。

16. 仮想コンピューティング環境における分離（ISO/IEC27017 項番：CLD.9.5.1）

お客様がアクセスするネットワークと当社運用担当者が利用する管理ネットワークは分離しています。

また、本サービスはシングルテナント構成で提供しており、各社ごとに独立した専用環境であるため、適切にお客様間のデータ分離を制御しています。

17. 仮想マシンの要塞化（ISO/IEC27017 項番：CLD.9.5.2）

設備に対する IP アドレスによるアクセス制限の実施、および不要なポートや常駐プログラムの停止を行っています。

また、設備にアクセスすることが出来るのは、当社運用担当者に限定しています。

さらに本サービスでは、当社の責任範囲において、サービスの維持管理に必要となる作業ログを取得しております。

18. 暗号による管理策の利用方針（ISO/IEC27017 項番：10.1.1）

- 利用者情報

  利用者の各種情報（氏名、メールアドレス等）は、暗号化せずに、適切なアクセス権のもとで保管します。

  パスワードは、暗号化した状態で保管します。

  メールデータについては、暗号化した状態で保管します。

- サービスとの通信

  お客様の端末と本サービスの運用管理ツールとの間のインターネット通信は、TLS 通信によって暗号化します。

19. 装置のセキュリティを保った処分又は再利用（ISO/IEC27017 項番：11.2.7）

当社が利用しているクラウドサービスプロバイダ（Microsoft）に準じます。Microsoft からは、以下の内容が提示されています。

https://www.microsoft.com/ja-jp/trust-center/privacy/data-management#office-ContentAreaHeadingTemplate-gr75fdf

20. 変更管理（ISO/IEC27017 項番：12.1.2）

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、本サービスのサポート担当から、サービス登録時に当社にご提供いただいたメールアドレスに対し、メールにてご連絡します。

21. 容量・能力の管理（ISO/IEC27017 項番：12.1.3）

リソースの利用状況を管理し、安定的にサービスを提供できる仕組みを構築しています。

22. 実務管理者の運用のセキュリティ（ISO/IEC27017 項番：12.1.5）

お客様が利用できる手順書は、本サービスのマニュアルとなります。

23. 情報のバックアップ（ISO/IEC27017 項番：12.3.1）

データベースに保管するお客様の各種情報（氏名、メールアドレス、などのアカウント情報）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 7 世代保管します。

バックアップデータは、Azure 内の高可用性・高耐久性ストレージにて保管します。

ストレージに保管するユーザーデータは、Azure の機能により多重化しています。

バックアップデータは、サービス全体の復旧を目的としており、個々のお客様データを個別に復旧することはできません。

24. イベントログ取得（ISO/IEC27017 項番：12.4.1）

本サービスでは、過去 90 日分のアクセスログ表示機能を提供しています。

その他のログについては、別途ご相談の上、可能なものについては有償で提供することができます。

25. クロックの同期（ISO/IEC27017 項番：12.4.4）

本サービス内で提供するログは、タイムゾーン JST（UTC+9）で提供します。

ログの時刻は、NTP または PTP による時刻同期に基づいて記録しています。

26. クラウドサービスの監視（ISO/IEC27017 項番：CLD.12.4.5）

本サービスでは、アクセスログ表示機能を提供しています。

また、サービスの常時監視を行っていますが、お客様への公開機能は有していません。

27. 技術的ぜい弱性の管理（ISO/IEC27017 項番：12.6.1）

本サービスの開発チームならびに運用チームは、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、速やかに適用します。

28. ネットワークの分離（ISO/IEC27017 項番：13.1.3）

お客様がアクセスするネットワークと当社運用担当者が利用する管理ネットワークは分離しています。

29. 仮想及び物理ネットワークのセキュリティ管理の整合（ISO/IEC27017 項番：CLD.13.1.4）

当社で提供するクラウドサービスは、全て仮想ネットワークを利用しています。

30. 情報セキュリティ要求事項の分析及び仕様化（ISO/IEC27017 項番：14.1.1）

情報セキュリティ基本方針、本セキュリティホワイトペーパーに定めています。

31. セキュリティに配慮した開発のための方針（ISO/IEC27017 項番：14.2.1）

本サービスの開発は、社内で定めた開発手順に従って実施しています。

32. 供給者との合意におけるセキュリティの取り扱い（ISO/IEC27017 項番：15.1.2）

本サービスは、サービスの提供環境における役割及び責任について利用規約に定め、サービスを提供します。

本サービスの責任分界点については、「3.情報セキュリティの役割及び責任」をご参照ください。

33. ICT サプライチェーン（ISO/IEC27017 項番：15.1.3）

本サービスでは、次に示す機能を運用するために、外部のクラウドサービスを利用しています。当社セキュリティホワイトペーパーに記載されている内容は、以下で示すクラウドサービスにて管理されている範囲には及ばず、また、その内容の遵守を保証するものではありません。

ただし、これらのクラウドサービスはいずれも、セキュリティレベルが十分に高い水準であることを確認して利用しています。

クラウドサービス	機能	運営会社
Azure	インフラ構築、運用	マイクロソフト
SendGrid	メール通知	Twilio

34. 責任及び手順（ISO/IEC27017 項番：16.1.1）

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、検知から 2 営業日以内を目標に、電子メールによりお客様の管理者に連絡します。

35. 情報セキュリティ事象の報告（ISO/IEC27017 項番：16.1.2）

情報セキュリティインシデントに関するお問合せは、サービス利用契約に基づき、サポート担当窓口より受け付けています。

36. 証拠の収集（ISO/IEC27017 項番：16.1.7）

裁判所からの証拠提出命令など、法的に認められた形でユーザーデータの提供を要請された場合、当社は、お客様の許可なく、必要最小限の範囲で、ユーザーデータを外部に提供する可能性があります。

37. 適用法令及び契約上の要求事項の特定（ISO/IEC27017 項番：18.1.1）

お客様と当社との間の契約は、日本法に基づいて解釈されるものとします。

38. 知的財産権（ISO/IEC27017 項番：18.1.2）

本サービスをご利用いただく上で知的財産権に関わるお問い合わせは、サポート担当窓口より受け付けています。

39. 記録の保護（ISO/IEC27017 項番：18.1.3）

お客様から預かったデータを適切に保護することは、当社の責任です。

ログデータを含むユーザーデータは、不正なアクセスや改ざんを防ぐため、運用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します。

また、運用チームのアクセスに関しても、サーバ上での操作はすべて作業ログを記録しているため、万が一改ざんが行われた場合には調査が可能です。

40. 暗号化機能に対する規制（ISO/IEC27017 項番：18.1.5）

輸出規制の対象となる暗号化の利用はありません。

41. 情報セキュリティの独立したレビュー（ISO/IEC27017 項番：18.2.1）

当社は、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 認証を取得しています。（※1）

また、当社は、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も取得しています。（※2）

【ISMS クラウドセキュリティ認証登録範囲】

本サービスの提供に係るクラウドサービスプロバイダとしてシステム開発・運用・保守及び Azure のクラウドサービスカスタマとしての利用に係る ISMS クラウドセキュリティマネジメントシステム

※1 https://isms.jp/lst/ind/CR_JUSE-IR-159.html

※2 https://isms.jp/isms-cls/lst/ind/CR_JUSE-IR-159-CS01.html