ISO/IEC27017 ホワイトペーパー

2024 年 1 月

第 1.0 版

株式会社 Quollio Technologies

1. 利用者との責任分解点（6.1.1）

- 当社の責任

  当社は、クラウドサービスのご提供にあたり、以下の事項を実施いたします。

  - クラウドサービスのセキュリティ対策（クラウド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 セキュリティ対策含む）
  - クラウドサービスに保管されたお客様データの保護

  尚、当社のサービスは Amazon AWS を中心とした構成で開発されており、AWS 側の責任については、以下のサイトに公開されています。

  https://aws.amazon.com/jp/compliance/shared-responsibility-model/

- 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
  - クラウドサービスの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）
  - お客様側で行われる作業（各アセットのメタデータ登録など）

2. 関係当局との連絡（6.1.3）

- 当社、株式会社 Quollio Technologies の本社所在地は、当社コーポレートサイトをご参照ください。
- 当社サービスを利用するにあたり、お客様からお預かりしたデータは、AWS 東京リージョンと大阪リージョンに保管されます。

3. 情報のラベル付け（8.2.2）

- 当社は、お客様に対して、情報資産の分類するためのタグ付け機能を提供しています。詳しくはユーザーガイド（https://docs.quollio.com/）のタグ用語集やチュートリアルのメタデータを付与する、をご参照ください。

4. 利用者登録及び登録削除（9.2.1）

- お客様によるクラウドサービスへのアクセスを、お客様が管理するため、当社 は、お客様にアカウントの登録及び削除を行う機能を提供しています。

- お客様は、クラウドサービス上のユーザー管理画面からアカウントの登録を行うことができます。また、お客様は、サービス上のユーザー管理画面からアカウントの停止・削除を行うことができます。詳しくはユーザーガイド（https://docs.quollio.com/）をご参照ください。

5. 利用者アクセスの提供（9.2.2）

- 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。適切な権限グループを設定することで、閲覧・編集を制御することが可能です。詳しくはユーザーガイド（https://docs.quollio.com/）をご参照ください。

6. 特権的アクセス権の管理（9.2.3）

- 当社は、お客様がアクセスする際、ID /パスワード認証の他、ワンタイムパスワードの機能やシングルサインオンの機能を提供しています。また、ご要望に応じて IP アドレスによるアクセス制御も可能です。

7. 利用者の秘密認証情報の管理（9.2.4）

- 管理者ユーザーが、新規ユーザーを追加したと同時に、新規ユーザーのメールアドレスに、初期パス ワードを登録するための、一意の URL を含むメールが送信されます。 新規ユーザーは、その URL にアクセスし、パスワードを入力・設定することで、サービスの利用を開 始できます。

8. 暗号による管理策の利用方針（10.1.1）

- データベースに保管される、お客様サービス利用時の登録・更新情報は、AWS の標準機能により、ディスクレベルでの暗号化が行われます。また、パス ワードは、不可逆暗号化(ハッシュ化)された状態で、データベースに保管されます。

- お客様の端末と、システムとの間のインターネット通信は、TLS/SSL で保護されたネットワークを介します。当社サービス内の通信は、AWS のプライベートネットワーク上を介し、物理レイヤーで自動的に暗号化されます。

- プロパティ機能を利用してアップロードされた画像ファイルは、AWS の標準機能により、ディスクレベルでの暗号化が行われます。プロパティ機能の詳細はユーザーガイド（https://docs.quollio.com/）をご参照ください。

9. 装置のセキュリティを保った処分又は再利用（11.2.7）

- 当社サービス利用に関する契約が終了した場合、お客様の希望に応じて、お客様に関するデータを削除いたします。
- 当社サービスで扱うデータは、全て AWS のリソース上で保管されており、その中で用いられる記憶媒体を内蔵した装置・メディアの破棄方法については、Amazon Web Services, Inc.に従います（https://aws.amazon.com/jp/blogs/news/data_disposal/）。
- 上記理由により、記憶媒体を内蔵した装置・メディアがいつ破棄されたのかについてはわかりかねますが、AWS 上で削除した記録をお客様に提出することは可能です。

10. 変更管理（12.1.2）

- システム変更等、お客様に影響のある変更を行う場合は、約 1 週間前にメールにて通知いたします。

11. 容量・能力の管理（12.1.3）

- 当社サービスは常時監視されており、必要に応じて自動的にリソースが増強されます。

12. 情報のバックアップ（12.3.1）

- 当社サービスの利用にあたり登録した情報は、AWS 東京リージョンで 35 日間のポイントインタイムリカバリ、および AWS 大阪リージョンで 7 日間分のバックアップデータを保存しています。
- お客様によるバックアップデータの復元等に関するご要望がある場合、一度、当社にご相談ください。
- 尚、お客様側では、CSV エクスポートの機能によって、当社サービスに登録した情報（メタデータ）をダウンロードすることができます。

13. イベントログ取得（12.4.1）

- 当社の責任範囲において、クラウドサービスの維持管理に必要となる適切なログを取得しています。必要な場合は、当社問い合わせフォームまでご連絡下さい。

14. クロックの同期（12.4.4）

- クラウドサービスは、Amazon Time Sync Service を利用して同期（UTC[世界標準時]）しています。

15. 技術的ぜい弱性の管理（12.6.1）

- 当社開発チームは、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、検証環境での検証を経た後、速やかに適用されます。
- お客様側で対応が必要となるようなぜい弱性情報があった場合には、個別にメールにて通知連絡いたします。

16. ネットワークの分離（13.1.3）

- 各テナントを論理的に分離しているため、他のテナントとの内部通信は行えない仕組みになっています。

17. 情報セキュリティ要求事項の分析および仕様化（14.1.1）

- 情報セキュリティに関しましては、情報セキュリティ基本方針および、当ホワイト ペーパーに記載しています。

18. セキュリティに考慮した開発のための方針（14.2.1）

- 本サービスの環境は、開発・検証・本番の 3 環境に分かれており、本番リリースまでのプロセス（ソフトウェア開発ライフサイクル）を定めてサービス開発・運営を実施しております。

19. 供給者との合意におけるセキュリティの取り扱い（15.1.2）

- 本サービスは、SaaS（Software as a Service）型のクラウドサービスとなり、責任分解点に関しては、「1. 利用者との責任分解点」をご参照ください。
- セキュリティ対策に関しても「1. 利用者との責任分解点」に記載する弊社サービスの提供範囲において必要なセキュリティ対策を実施しています。

20. 責任及び手順（16.1.1）

- 当社で確認できたセキュリティインシデントに関しては、情報セキュリティ方針に則り、適切に対応しております。
- また、確認できた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可能性がある場合においては、検知から 1 営業日を目標に個別にメール通知致します。

21. 情報セキュリティ事象の報告（16.1.2）

- お客様がセキュリティインシデント事象を発見したとき、当社にお問い合わせ・通知する機能として、コーポレートサイトにお問い合わせフォームをご提供しております。

22. 証拠の収集（16.1.7）

- 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。ログデータを含むお客様データは、不正なアクセスや改ざんを防ぐため、当社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、当社は、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。

23. 適用法令および契約上の要求事項の特定（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。

24. 知的財産権（18.1.2）

- 当社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、コーポレートサイトのお問い合わせフォームからお問い合わせください。

25. 記録の保護（18.1.3）

- 当社の責任範囲において、お客様アクセスログを取得しています。必要な場合は、当社コーポレートサイトの問い合わせフォームをご利用ください。
- 尚、保存期間は 12 ヵ月間となります。

26. 暗号化機能に対する規制（18.1.5）

- 「8. 暗号による管理策の利用方針」をご参照ください。
- 尚、輸出規制の対象となる暗号化の利用はありません。

27. 情報セキュリティの独立したレビュー（18.2.1）

- 社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001、ISO/IEC27017 の ISMS 認証取得において第 3 者による審査を受け、情報セキュリティに対する取り組みを行うことで、常に安全なセキュリティレベルを確保しています。

28. 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（CLD.6.3.1）

- 「1. 利用者との責任分解点」をご参照ください。

29. クラウドサービスカスタマの資産の除去（CLD.8.1.5）

- 「9. 装置のセキュリティを保った処分又は再利用」をご参照ください。

30. 仮想コンピューティング環境における分離（CLD.9.5.1）

- テナント ID によるアクセス資源の分離を実施し、別テナントへの不正アクセスを抑止しています。

31. 実務管理者の運用のセキュリティ（CLD.12.1.5）

- ご利用いただく当社サービスの操作方法に関しては、ユーザーガイド（https://docs.quollio.com）をご参照ください。

32. クラウドサービスの監視（CLD.12.4.5）

- システムリソース監視は AWS サービスを利用し当社で実施しております。
- 現在、当社サービス内やコーポレートサイト上など、監視結果をお客様に公開する機能を有しておりません。

改訂履歴

版	改訂日	改訂内容
1.0	2023/01/05	初版発行