アナウンス音源作成サービス「YUTTE（ゆって）」
ISO/IEC 27017 ホワイトペーパー

JIS Q 27017:2016（ISO/IEC 27017:2015）では、クラウドサービスを提供する事業者（クラウドサービスプロバイダ）が実施する情報セキュリティ管理策について、その内容を利用者に対して適切に情報提供することを求めています。

本書は、上記の規格に基づき、本サービスにおいて当社が実施している情報セキュリティ管理策の内容について、お客様にご理解いただくことを目的として作成した資料です。本サービスのご検討や、情報セキュリティ対策に関する理解を深めていただくための参考資料としてご活用ください。

第 2 版
2026 年 4 月 1 日

TOA 株式会社

本書のご利用にあたって

本書をご利用いただくにあたり、以下の点にご留意ください。

- 本書は、本サービスにおける情報セキュリティ管理策の概要を説明するものであり、本サービスの提供条件、機能、性能、保証内容、または契約上の権利義務のすべてを規定するものではありません。

- 本サービスのご利用にあたっては、利用規約、サービス仕様書、取扱説明書等の関連文書を必ずあわせてご確認ください。これらの文書と本書の内容に相違がある場合は、当該関連文書の定めが優先されます。

- 本書に記載する情報セキュリティ管理策は、本サービスのうち当社が管理・運用する範囲を対象としています。お客様の利用環境および当社が利用するクラウドサービスに関する情報セキュリティ対策については、本書の対象外とします。範囲の詳細については「３．責任分界点について」をご参照ください。

- 本書は、第三者による認証報告書や監査報告書に代わるものではなく、本サービスの特定の基準への適合性や情報セキュリティ上の安全性を保証するものではありません。

- 本書の内容は、予告なく改訂される場合があります。情報セキュリティを取り巻く環境や脅威は日々変化しており、当社は、これに対応するための対策を継続的に見直しています。最新の情報については、当社にお問い合わせいただくか、本サービスのサービス公式 Web サイトをご確認くださいますようお願いいたします。

- 本書の著作権は当社に帰属します。お客様は、本サービスの検討ならびに販売活動を目的とする場合に限り、改変を行わない形で本書を閲覧、複製、配布および引用することが可能です。

改定履歴

版数	改定日	更新内容
第 1 版	2025 年 11 月 1 日	初版
第 2 版	2026 年 4 月 1 日	文言の修正（表現の明確化）

1．本書の適用範囲

当社がサービス提供する、アナウンス音源作成サービス「YUTTE（ゆって）」が本書の適用範囲となります。

2．参照先一覧

本書内の記載事項に対応する参照先 URL を以下に示します。

- YUTTE サービス WEB サイト
  https://yutte.cloud
- 利用規約(PDF ファイル)
  https://yutte.cloud/docs/terms.pdf
- 情報セキュリティ基本方針
  https://www.toa-global.com/ja/securitypolicy
- 当社サポート窓口
  (お問い合わせフォーム)
  https://yutte.cloud/contact/index.html

  (当社事業所一覧)
  https://www.toa-global.com/ja/profile/company/network
- 操作マニュアル
  YUTTE ご利用方法（情報発信基地内）
  https://yutte.cloud/infobase/ta1l-4h2q-soqy-3437

3．責任分界点について

本サービスの責任分界点は、以下になります。

<table>
<tr><th>対象物</th><th>責任範囲</th></tr>
<tr><td>保存されたデータ
・アナウンス
・アップロードしたファイル
・アカウント情報</td><td>お客様にお願いする責任範囲</td></tr>
<tr><td>アプリケーション
・セキュリティ対策
・保管されたお客様データの保護</td><td rowspan="2">当社の責任範囲
（クラウドサービス利用における責任）</td></tr>
<tr><td>インフラ
・ミドルウェア
・セキュリティ対策</td></tr>
<tr><td>ミドルウェア（AWS に付属するもの）</td><td rowspan="5">当社が利用するクラウドサービスの責任範囲

当サービスは、Amazon Web Services（アマゾンウェブサービス：以下 AWS と呼ぶ）を使用しています。</td></tr>
<tr><td>OS</td></tr>
<tr><td>仮想サーバー</td></tr>
<tr><td>物理設備
・サーバー
・ストレージ
・ネットワーク</td></tr>
<tr><td>土地・建物</td></tr>
</table>

4．各管理策への対応について

JIS Q 27017:2016（ISO/IEC 27017:2015）が求める要求事項に対する管理策の項番の順番で本サービスの取り組みを記載いたします。

項番	取り組み内容
5.1.1 情報セキュリティのための方針群	本サービスは、当社の定めた情報セキュリティ基本方針、および、クラウドサービスセキュリティ方針に従い、サービス運営を行います。 情報セキュリティ基本方針は、当社 WEB サイトからご確認いただけます。クラウドサービスセキュリティ方針については、当社サポート窓口までご連絡ください。
6.1.1 情報セキュリティの役割および責任	「３.責任分界点について」 に記載しております。 本サービス利用については利用規約をご確認ください。

6.1.3 関係当局との連絡	当社の本社所在地は次の通りです。 神戸市中央区港島中町 （ホームページ：https://www.toa.co.jp） サービスの運用拠点は次の通りです。 宝塚市高松町１－１０　ナレッジスクエア 当社が提供するクラウドサービスに保存されたデータは、AWS の日本国内にあるデータセンターに保管されています。 本サービスに保存されたデータは、原則として日本国内で管理され、国外へ移転されることはありません。
CLD.6.3.1　クラウドコンピューティング環境における役割および責任の共有および分担	「３.責任分界点について」に記載しております。 本サービス利用については、利用規約をご確認ください。
7.2.2 情報セキュリティの意識向上、教育および訓練	本サービスに携わる当社サービス運営担当者に対し、情報セキュリティ要件や、本サービスの運用ルール周知徹底と意識向上のための教育・訓練を定期的に実施しています。
8.1.1 資産目録	本サービスにお客様が登録するデータと、当社がサービスを運営するための情報は明確に分離しています。
CLD.8.1.5 クラウドカスタマの資産の除去	本サービスにお客様が登録・保存したデータ、および本サービスの利用によって生成されたデータは、サービス契約期間終了後も当社にて保管しており、お客様による退会操作時に削除されます。 ただし、「18.1.3 記録の保護」に記載の通り、お客様の操作ログなどは、退会後もクラウド上に保存されます。
8.2.2 情報のラベル付け	本サービスは、作成したアナウンスやアップロードしたファイルにタイトルを付ける機能を有しており、お客様にて、設定できます。
9.2.1 利用者登録および登録削除	本サービスでは、共同編集者（メンバー）のアカウントを登録・削除する管理者機能を提供しています。管理機能の操作に関しては、操作マニュアルをご参照ください。
9.2.2 利用者アクセスの提供	本サービスでは、ユーザー権限を管理する機能を提供しており、管理者が設定可能となります。 管理機能の操作に関しては、操作マニュアルをご参照ください。
9.2.3 特権的アクセス権の管理	本サービスではメールアドレスとパスワードによる認証に加え、ログイン時のメールアドレスに送付されたワンタイムパスワードを使用した、2 要素認証に対応しております。

9.2.4 利用者の秘密認証情報の管理	本サービスでは、ユーザー登録時に設定いただいたメールアドレスとパスワードで認証を行います。メールアドレスとパスワードは共にアカウント管理画面から変更することができます。
9.4.1 情報へのアクセス制限	共同編集者（メンバー）に対し権限付与をすることができます。管理機能の操作に関しては、操作マニュアルをご参照ください。
9.4.4 特権的なユーティリティプログラムの使用	本サービスにおいて、通常の操作手順またはセキュリティ手順を回避することのできるユーティリティプログラムの提供はありません。
CLD.9.5.1 仮想コンピューティング環境における分離	本サービスでは、仮想化技術を利用し、クラウドシステム環境を利用者団体ごとに論理的に分離しています。
CLD.9.5.2 仮想マシンの要塞化	仮想マシンの要塞化のために、IP/プロトコル/ポートへのアクセス制限などを実施しています。
10.1.1 暗号による管理策の利用方針	お客様よりお預かりしているデータは、すべてクラウドサーバ上で暗号化して管理しています。 また、お客様の利用する Web ページでは SSL/TLS による通信の暗号化を行っています。
11.2.7 装置のセキュリティを保った処分または再利用	機器の老朽化、故障等により交換した機器媒体について、当社が機器媒体の処分を行うことはありません。 本サービスは、AWS のデータセンターを使用しており、サービスを構成する機器として、当社の機器媒体はありません。これら機器媒体の取り扱いについては、AWS の施設、建物、および物理上のセキュリティに基づきます。 AWS クラウドにおける安全なデータの廃棄について https://aws.amazon.com/jp/blogs/news/data_disposal/
12.1.2 変更管理	サービス内容の変更や、メンテナンスを実施する場合、本サービスの WEB ページ内に掲載して事前に通知いたします。
12. 1 .3 容量・能力の管理	当社にて日々のプロセスの中で稼働状態の監視を行っています。システム上で何ら異常を検知した際は、当社システム管理者にメール通知される設計を行っています。
CLD.12.1.5 実務管理者の運用のセキュリティ	本サービスでは、サービスの利用に必要な操作手順を、操作マニュアルとして提供しています。
12.3.1 情報のバックアップ	本サービスでは、サービス提供に用いるシステムデータや預託データのバックアップを、日次で 30 日分を取得／保持しています。バックアップは、サービスのシステム障害や大規模災害発生時を想定し取得するもので、原則、個別の復旧依頼に応じるものではありません。

12.4.1 イベントログ取得	当社の責任範囲において、本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。ログが必要な場合は、当社サポート窓口までご連絡ください。
12.4.4 クロックの同期	本サービスは NTP による時刻同期を行っています。システム内部は、世界標準時（UTC)で稼働しており、ユーザー画面上では日本標準時（JST）に変換して表示しています。
CLD.12.4.5 クラウドサービスの監視	本サービスの各種パフォーマンスや攻撃などの監視は、当社が実施しています。 監視結果が必要な場合は、当社サポート窓口までご連絡ください。
12.6. 1 技術的脆弱性の管理	定期的に脆弱性情報の収集と検査を実施し、何らかの対応が必要となった場合は、メンテナンスを実施いたします。サービスの停止が伴うメンテナンスを行う場合は、事前に通知いたします。
13.1.3 ネットワークの分離	当社の社内ネットワークと本サービス側のネットワークとは、物理的に分離されています。
CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合	物理ネットワークと論理ネットワークの整合性がとれるように、設計、構築、管理をしています。
14.1.1 情報セキュリティ要求事項の分析及び仕様化	当社では、クラウドサービスを開発・構築・運用する際の情報セキュリティ要求事項に基づいてセキュリティ要件を決定し、対策を行っています。 主にお客様にお使いいただける情報セキュリティの機能としては、以下の通りです。 ・メールアドレス/パスワードによる認証 ・メールアドレスを用いた 2 要素認証 ・アカウントロック機能 ・パスワードポリシーの適用
14.2.1 セキュリティに配慮した開発のための方針	本サービスでは、以下のガイドラインに沿ったシステム設計・開発を行っております。 ・安全なウェブサイトの作り方(IPA) ・非機能要求グレード(IPA) ・AWS のベストプラクティス また、定期的に脆弱性検査ツールを利用し、セキュリティに配慮したサービスを提供しています。
15.1.2 供給者との合意におけるセキュリティの取扱い	本サービスにおける役割及び責任については、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関しては、「３.責任分界点について」をご参照ください。

15.1.3 ICT サプライチェーン	当社が利用するクラウドサービスプロバイダは、情報セキュリティ水準を確認の上、本サービスの情報セキュリティとの整合性が取れていることを確認しています。
16.1.1 責任及び手順	お客様に影響を及ぼすセキュリティインシデント（データの消失、サービスの停止等）が発生した場合は、当社の定める手順に従い、当社サービスサイト及びメールにて通知いたします。 セキュリティインシデントに関するお問合せは、当社サポート窓口より受け付けています。
16.1.2 情報セキュリティ事象の報告	当社にて確認した情報セキュリティ事象が、お客様に影響を及ぼす可能性がある場合は、サービスサイト及びメールにて通知いたします。お客様から当社に情報セキュリティ事象を連絡いただく場合は、当社サポート窓口より受け付けています。
16.1.7 証拠の収集	お客様のデータは、本サービスの利用規約に従って適切に管理いたします。ただし、法律に基づいた裁判所からの開示請求が行われた場合、利用規約の定めに従ってお客様の同意なく、お客様のデータを当該機関に開示することがあります。
18.1.1 適用法令および契約上の要求事項の特定	本サービスの利用に関して適用される準拠法は、日本国の法令となります。
18.1.2 知的財産権	知的財産権に関わるお問い合わせは、当社サポート窓口までお問い合わせください。
18.1.3 記録の保護	当社の責任範囲において、保存期間を定めログを取得しています。 必要な場合は、当社サポート窓口へお問い合わせください。
18.1.5 暗号化機能に対する規制	本製品は、輸出規制（リスト規制・キャッチオール規制）に該当する暗号化機能を使用していません。
18.2.1 情報セキュリティの独立したレビュー	ISO/IEC 27001 および JIP-ISMS517-1.0（ISO/IEC 27017）について第三者による審査を受け、それぞれの認証を取得しております。