ACES Meet セキュリティホワイトペーパー

1.0版

株式会社ACES

1　利用者との責任分界点

株式会社ACESの責任

株式会社ACESは、以下のセキュリティ対策を実施します。

- ACES Meetアプリケーションのセキュリティ対策
- ACES Meetアプリケーションに保管されたお客様データの保護
- ACES Meet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
- ACES Meet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）
- ACES Meetの利用にあたり生成、保管されたデータの管理（会議記録(録画・録音データを含む)、個別に入力された情報など）
- ACES Meetの利用にあたり生成されたデータの利用に関する責任
- ACES Meetに登録する個人情報の取扱いに関する適切な管理（利用目的の通知・公表その他の個人情報保護法上必要な対応）

2　データ保管場所

- お客様からお預かりしたデータは、原則としてAWS東京リージョン上の当社管理環境に保管されます。一部のクライアントアプリケーションでは、利便性向上のため端末ローカルにデータが一時保存される場合があります。その場合も、適切なアクセス制御および暗号化等のセキュリティ対策を実施しています。

3　データの削除

- ACES Meet利用に関する契約が終了した場合のデータ削除に関する取り決めはACES Meet 利用規約 第26条に記載しています。
- 削除されるデータの詳細は、ACES Meetセキュリティチェックシートをご確認ください。

4　暗号化の状況

全般

- 当社サービスで取り扱うデータは、その性質および保存形式に応じて暗号化方式を適用しています。保存されるすべてのデータは、AWS Key Management Service（AWS KMS）を利用したサーバーサイド暗号化（

AES-256など）により暗号化された状態で保管されます。また、一部の高機密データについては、適用可能なデータ保存経路において、クライアントサイド暗号化を追加適用したうえで保存されます。パスワードはソルト付加による不可逆ハッシュ方式で安全に管理されています。なお、サービス運用上必要となる氏名・メールアドレス等の構造化データは、暗号化されずにデータベースに保存され、適切なアクセス権のもと管理されます。

- スマートフォンアプリにより、端末内に保存されるデータは、AES方式を用いて暗号化されます。
- 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、SSL/TLSによって暗号化されます。

5　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、下記のリンク先Webページより閲覧することが可能です。
  - サポートサイト　https://support-meet.acesinc.co.jp/
- 一時的な停止を伴うサービスメンテナンスを実施する場合は、原則、メンテナンス予定日より1週間前までに、サポートサイトおよびサービス画面上にてご連絡します。また、メンテナンス終了に伴うご連絡についても、サポートサイトおよびサービス画面上に掲載いたします。ただし、緊急を要するサービス停止を伴うメンテナンスを実施する場合は、その限りではありません。

6　手順書の提供

- サービスにおける機能の詳細説明や手順書は、ご契約者様限定で提供しています。
- 詳細について提供をご希望の場合は、https://meet.acesinc.co.jp/contact/　よりお問い合わせください。なお、セキュリティの観点から、本文書より詳細なセキュリティやシステム情報の提供は原則として行っておらず、より詳細な情報開示の請求についてはお断りさせていただく場合があることをあらかじめご了承ください。

7　バックアップの状況

- データベースに保管される、お客様の各種情報（氏名、メールアドレス、会議情報など）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、30世代保管されます。
- 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。
- ACES　Meetにアップロードされたファイルは、高可用性のクラウドストレージに格納されます。ある箇所でデータが破損しても、冗長データより自動で修復されます。
- 会議情報（文字起こしデータ）はCSVまたはWordまたはTSV形式でダウンロード可能です。また、動画および音声データもダウンロード可能なため、必要に応じて、お客様自身でバックアップを取得してください。な

お、クラウドストレージに格納された録画および音声データについては、当社側での二次的なバックアップは実施しておりません。万が一のデータ消失等に備えた長期的な保存・管理は、ダウンロード機能をご利用の上、お客様の責任において実施いただくようお願いいたします。

8 ログのクロックに関する情報

- ACES Meet内で提供されるログは、タイムゾーンJST (UTC+9) で提供されます。
- ログの時間は、AWSが提供するNTPサービスと同期しています。

9 脆弱性管理に関する情報

- ACES　Meet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。
- 定期的に外部専門業者による脆弱性診断を行っています。

10 開発におけるセキュリティ情報

- ACES Meetの開発は、IPAセキュアコーディングガイドライン、及び、社内コーディング規約に従って実施されます。

11 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(不正アクセス、外部への情報漏洩、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、インシデント発生が発覚してから72時間以内を目標に、ACES Meet利用契約時にご提供頂いたテナント管理者のメールもしくはACES Meetサポートサイトにてご連絡します。
- 情報セキュリティインシデント（知的財産権の侵害を含む）に関する問合せは、本セキュリティホワイトペーパー末尾の「ACES Meetにおけるインシデント対応窓口」より受け付けています。

12 お客様データの保護及び第三者提供について

- お客様からお預かりしたデータを適切に保護することは、株式会社ACES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、株式会社ACES が定める権限に基づき、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ACES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。

13 適用法令等

- お客様と株式会社ACES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。
- 本書は情報提供目的で公開する書面であり、当社サービスの利用規約およびプライバシーポリシーに優先するものではありません。

14 認証

- 株式会社ACES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]を取得しています。

15 セキュリティチェックシート

- セキュリティチェックシートは以下よりダウンロード可能です。
  https://aces-jp.box.com/shared/static/4ijvy1xqj911poggfsegk7mq7xics0ip.zip

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

ACES Meetに関するお問い合わせ

下記Webフォームよりお問い合わせください。

https://meet.acesinc.co.jp/contact/

ACES Meetにおけるインシデント対応窓口

株式会社ACES

担当：ACES Meet インシデント対応窓口

Email：acesmeet-support@acesinc.co.jp

改訂履歴

版	改訂日	改訂内容
1.0	2026/2/27	初版発行