tetoru セキュリティホワイトペーパー

Ver 1.0（2025年5月1日）

Classi株式会社

改訂履歴

版	改訂日	改訂内容
1.0	2025/05/01	初版発行

1.目的

このホワイトペーパーは、tetoruの利用を検討されている方、すでに利用いただいている方に向けて、お預かりしたお客様の個人データ（以下「お客様データ」）に関して、tetoruの関係法令・ガイドライン等の遵守状況、tetoruのセキュリティへの取り組みtetoruへの質問及び苦情処理の窓口を確認いただくとともに、tetoruをセキュアに利用いただくための留意事項を確認いただくことを目的としています。

2.Classiと利用者との責任分担

Classi株式会社の責任

Classi株式会社は、以下のセキュリティ対策を実施します。

- お客様データの保護
- サービス提供のために当社が設計・開発するソフトウェアのセキュリティ対策
- サービス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（自治体・学校等の契約団体、保護者）の責任

お客様は、tetoruをご利用するにあたり、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
- 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）
- サービス内に登録・保管するデータのバックアップ
- 利用する端末等の適切な管理（インターネット回線、OS・ブラウザ等の最新版利用など）

3.データ保管場所

- tetoruのデータベース上のデータは、日本国内のデータセンターに保管されます。

4.自治体・学校等契約団体の判断で解約された際のデータの取扱い

- tetoruに保存したデータが必要な場合は、自己の責任と費用負担においてダウンロードしてください。
- それまで利用していたユーザーからはアクセスできなくなります。

5.教職員の退職や異動、児童生徒の卒業や転校などに伴い利用停止になったデータの取扱い

教職員の退職や異動に伴う利用停止になったデータの取扱い

- 利用停止となった教職員については、ログインができなくなり、データの閲覧・更新等ができなくなります。
- 管理者や他の教職員からは、利用停止になった教職員の氏名や過去の投稿データなどは引き続き参照可能です。

児童生徒の卒業や転校などに伴う利用停止になったデータの取扱い

- tetoruに保存したデータが必要な場合は、自己の責任と費用負担においてダウンロードしてください。
- 利用停止になったデータは児童生徒の保護者から読み取り・更新をすることができなくなります。教職員においても基本は同様ですが、業務に必要な範囲で卒業後も読み取りが可能なデータがあります。

6.パスワードの通知方法

自治体・学校等の契約団体

- 初期パスワードは、tetoruから自治体・学校等の契約団体の管理者へ通知されます。契約団体の管理者は、各教職員のアカウントを作成し、各教職員へパスワードを通知します。
- 初期パスワードは、初回ログイン時に変更が必要です。
- 管理者がパスワードを忘れた場合は、ヘルプセンターよりtetoruへお問合せください。
- 各教職員がパスワードを忘れた場合は、契約団体の管理者へ依頼することで、パスワードの再設定を行うことが可能です。
- 管理者による各教職員のパスワード変更の詳細な手順はtetoruヘルプページより確認いただけます。

保護者

- 初期パスワードは、アカウント作成時にご自身で設定いただきます。
- パスワードを忘れた場合は、ユーザ自らサービス画面よりパスワードの再設定を行うことが可能です。
- パスワード変更の詳細な手順はtetoruヘルプページより確認いただけます。

7.暗号化の状況

- データベースに保管される、お客様データは、内容に応じての暗号化されるほか、適切なアクセス権のもとで保管されます。
- 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、SSL/TLSプロトコル（TLS1.2以上）により暗号化されたhttps通信が用いられます。

8.仕様の変更管理

- バージョンアップをはじめとする、各種のサービスの仕様の変更に関する情報は、「tetoruからのお知らせ」より通知いたします。
- サービスのメンテナンスを行う際は、事前に「tetoruからのお知らせ」より通知いたします。また、お客様の利用に大きな影響があるメンテナンスを実施する場合は、お客様の管理者に対してメール等にてご連絡します。

9.手順書の提供

- tetoruの仕様や操作方法については、Web上のヘルプページや利用ガイドにて確認が可能です。

10. バックアップの状況

- データベースに保管される、お客様データは、日次でバックアップを取得しています。
- ただし、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。

11. 脆弱性管理

- 脆弱性診断サービスを利用して定期的に脆弱性診断を実施しています。
- 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はセキュリティの専門家が収集、確認し、対応可否を判断しています。

12. 開発におけるセキュリティ

- tetoruのシステムの開発は、情報セキュリティに関する要件を含んだ開発ルールに従って実施されます。

13. 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（データの消失・漏洩、長時間のシステム停止等）が発生した場合には、発生を確認し次第、遅くとも2営業日以内にお客様の管理者へメール、Webサイトの告知、tetoruからのお知らせ等にてご連絡します。

- 情報セキュリティインシデントに関するご報告は、以下の窓口より承ります。
    - お問い合わせ窓口：privacy@classi.jp

14. ログの時刻同期について

- ログの時間は、Amazon Web Servicesが提供するマネージドサービスである Amazon Time Sync Serviceを利用しています。

15. ログの保管

tetoruの機能を通して提供されるログは、以下の表に従った期間で保管されます。

ログの種類	保管期間
操作ログ	5年間
ログインログ	5年間

- 利用者からのログの提出要求に関しては、原則応じることはできませんので、あらかじめご了承ください。

16. 連携サービス

- tetoruは、以下のURLに記載する校務支援サービス（連携サービス）との児童生徒名簿や欠席情報等のAPI連携ができます。（別途C4thオプション利用の場合）
    - https://www.educom.co.jp/service/c4th

- 連携サービスの機密性、完全性、可用性については、お客様の責任にて判断するものとします。
- 連携サービスを利用することにより生じた問題等について、お客様から直接、連携サービスを提供する会社にお問い合わせいただくものとします。必要に応じて、連携サービス提供会社と連携の上、Classi株式会社も問題解決に取り組みます。

17. 適用法令

- お客様とClassi株式会社との間の契約は、日本法に基づいて解釈されるものとします。

18. 情報セキュリティの独立したレビュー

- 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。
- 当社は、定期的に監査を実施しています。監査では、社内の独立した立場の監査員もしくは専門組織等の監査員によって、当文書を含む社内のポリシーに、当サービスが適合しているかのチェックが実施されており、問題が見つかった場合には、速やかに改善を行っています。

19. その他の情報安全管理措置

- お客様データの取得・保存から利用、消去等における取扱方法等についての規律・マニュアルを整備しています。
- 就業規則において、従業員に、お客様データを含めた機密情報につき機密保持義務を課すとともに入社時に従業員より、情報管理に関する誓約書を取得しています。
- お客様データの取り扱いにおいて、権限を有しない者による閲覧を防止する措置を実施しています

この資料に関するお問い合わせ

Classi株式会社
東京都新宿区西新宿2丁目1-1 新宿三井ビルディング 14階
Email：privacy@classi.jp