LINES
学ぶチカラを、未来のチカラに

クラウドセキュリティ
ホワイトペーパー

2 版(2.0)

発行：2025 年 12 月 15 日

目次

1. はじめに 1

1.1 このホワイトペーパーについて 1

1.2 適用範囲 1

1.3 参考文献 1

2. クラウドサービスの管理策 2

2.1 情報セキュリティ方針 2

2.2 責任分界点 2

2.3 ICT サプライチェーン 2

2.4 個人情報保護 3

3. 利用者へのセキュリティの提供 4

3.1 情報資産の管理 4

3.1.1 情報資産のラベル付け 4

3.2 アクセス制御 4

3.2.1 利用者登録 及び 登録削除 4

3.2.2 アカウント管理 及び アクセス権の管理 4

3.3 運用 4

3.3.1 アクセスログ取得 4

3.3.2 操作ログ取得 4

3.3.3 利用状況の確認 5

4. 利用者へのセキュリティ情報の提供 6

4.1 当社の開発や運用における共通方針 6

4.1.1 技術的脆弱性の管理 6

4.1.2 特権的なユーティリティプログラムの使用 6

4.1.3 クロックの同期 6

4.2 当社の開発方針 6

4.2.1 通信の暗号化 6

4.2.2 データの暗号化 6

4.2.3 ネットワーク及び仮想コンピューティング環境における分離 6

4.2.4 仮想マシンの要塞化 6
4.2.5 情報のバックアップ 7
4.3 当社の運用方針 7
4.3.1 アプリケーションのサービスレベル 7
4.3.2 変更管理 8
4.3.3 ネットワークセキュリティ管理の整合 8
4.3.4 情報機器の処分または再利用 8
4.3.5 クラウドサービスカスタマの資産除去 8
4.3.6 容量・能力の提供 8
4.4 情報セキュリティインシデント 8
4.4.1 対象インシデント 8
4.4.2 インシデントの通知内容と方法 9
4.5 コンプライアンス 9
4.5.1 所在地 及び 利用者のデータの保存場所 9
4.5.2 適用法令 9
4.5.3 証拠の収集 9
4.5.4 記録の保護 9
4.5.5 情報セキュリティの独立したレビュー 9
5. 改訂履歴 10

1. はじめに

1.1 このホワイトペーパーについて

この文書は、2025 年 3 月の時点における「安心でんしょばと」の情報セキュリティへの取り組みと、情報セキュリティの観点から利用を検討されている方、または、既にご利用頂いている方に向けて安全にご利用いただくための留意事項をご確認いただくことを目的としています。

1.2 適用範囲

このホワイトペーパーの範囲となる製品は次の通りです。

●安心でんしょばと

1.3 参考文献

●ラインズ株式会社 会社概要
https://www.education.jp/company/profile

●安心でんしょばと(商品ページ)
https://www.education.jp/education03/education03_2/

●安心でんしょばと 利用規約

ご契約者ならびにご契約を検討しているお客様にのみ開示しております。

●安心でんしょばと マニュアル

(本部管理者向け)
https://www.education.jp/cms/lines/data/support/hato/tools/hato_g_manual3.pdf

(教職員向け)

https://www.education.jp/cms/lines/data/support/hato/tools/hato_g_manual4.pdf

●保護者サポートサイト
ご契約者様ならびにユーザー様にのみ開示しております。

2. クラウドサービスの管理策

2.1 情報セキュリティ方針

当社は情報セキュリティポリシーを定め、クラウドサービスカスタマが安心して利用できるように取り組みを行っております。
また、本情報セキュリティ方針及び関連するポリシーや方針群は毎年の ISMS 活動の中で、年に 1 回見直しを行います。

https://www.education.jp/securitypolicy/

2.2 責任分界点

当社は、利用者と当社の情報セキュリティの責任範囲において下記の責任分界点の通り定義しております。

●利用者の責任範囲

»ユーザーの管理データ

・ログイン ID、パスワード

・当社サービスにアップロードするデータ及び当社サービスからダウンロードしたデータ

»サービスの設定内容

»インターネット環境

»ユーザー端末

●当社の責任範囲

»Web アプリケーション

»スマホ向けプッシュ通知型アプリケーション

»保存データ(顧客情報、設定情報、各種ログデータ)

»OS、ミドルウェア

»サーバー、ネットワークのハードウェア

2.3 ICT サプライチェーン

当社は、セコムセキュアデータセンターに設置されたオンプレミスサーバを利用して環境を構築しています。
また、当社の委託先については契約の定めにしたがって管理を行っており、当社と同等の情報セキュリティ水準を要求するように定めています。

2.4 個人情報保護

当社は、プライバシーポリシー及び利用約款に記載の通り個人情報を保護しております。

https://www.education.jp/privacy/

3. 利用者へのセキュリティの提供

3.1 情報資産の管理

3.1.1 情報資産のラベル付け

当社は、管理画面で、利用者がグループの名前付けなどでラベル付けを行う機能を提供しています。

詳細は各種マニュアルをご覧下さい。

3.2 アクセス制御

3.2.1 利用者登録 及び 登録削除

管理者のアカウントは当社から発行します。

当社は、管理者がユーザーアカウントを登録及び削除する機能を提供しております。具体的な操作手順は各種マニュアルをご覧下さい。

3.2.2 アカウント管理 及び アクセス権の管理

当社は、管理者アカウントのアクセス保護のための仕組みとして学校コード、ID、パスワードによる認証を提供しています。

アクセス権の管理利用者は次の権限管理機能によりアカウントのアクセス制御を実施頂けます。

製品	権限
安心でんしょばと	・本部管理者 下位の施設・学校の教職員アカウントの登録、削除 下位の施設・学校の生徒・児童アカウントの登録、削除 ・施設管理者 自施設・学校の教職員アカウントの登録、削除、変更 自施設・学校の生徒・児童アカウントの登録、削除、変更

3.3 運用

3.3.1 アクセスログ取得

当社は、利用者のアカウントに対して、リクエストを受け取った時刻、クライアントの IP アドレスなどのアクセスログを取得していますが、閲覧する機能は提供していません。

アクセスログの最低保存期間は 90 日となります。

3.3.2 操作ログ取得

当社は、アプリケーションの操作ログを取得していますが、閲覧する機能は提供していません。

操作ログの最低保存期間は 90 日となります。

3.3.3 利用状況の確認

本部管理者にて、メッセージ送信回数、登録数、ログイン、入退室の状況を把握できます。

4. 利用者へのセキュリティ情報の提供

4.1 当社の開発や運用における共通方針

4.1.1 技術的脆弱性の管理

当社は、開発時やシステムアプデート時などに当社セキュリティポリシーに沿って定期的に脆弱性試験(プラットフォーム診断)を実施しています。

また、脆弱情報を収集するとともに、脆弱性対策を実施しています。

4.1.2 特権的なユーティリティプログラムの使用

当社は、製品の開発や運用において、特権的ユーティリティプログラム及び特権的ユーティリティプログラムを利用する従業員を制限し、定期的にレビューしています。

また、当社製品の利用者には、当社製品の特権的なユーティリティプログラムは提供しておりません。

4.1.3 クロックの同期

当社が提供するクラウドサービス内で提供する時刻情報は、タイムゾーン JST(UTC+9)で取得されます。
ログの時間は、Stratum3 以内の NTP サーバに同期されています。

4.2 当社の開発方針

当社は、社内で定められた開発規程に従ってサービス開発を行っています。

4.2.1 通信の暗号化

当社は、通信内容を暗号化することで、データ漏洩や改ざんを防止しています。利用者の端末と、クラウドサービスプラットフォーム間のインターネット通信を HTTPS により暗号化しています。

4.2.2 データの暗号化

当社は、管理者パスワード、メールアドレスを保存する際に暗号化(AES)またはハッシュ化(bcrypt)しています。

4.2.3 ネットワーク及び仮想コンピューティング環境における分離

当社は、利用者が別の利用者のデータを閲覧することができないよう、また当社の従業員が利用者のデータを必要以上に閲覧することができないように、適切に分離しております。

4.2.4 仮想マシンの要塞化

当社は、クラウドサービスの提供に必要なポート、プロトコル及びサービスのみを提供しております。

また、アンチウイルスソフトによりウイルス対策を実施するとともに、IPS により不正アクセスを含むサイバー攻撃対策を実施しています。

4.2.5 情報のバックアップ

当社は、以下に従い利用者データのバックアップを取得しております。

なお、バックアップデータからの復旧機能はユーザーに提供しておらず、当社がクラウドサービスを運用する中で必要と判断した場合にのみ、バックアップデータから復元を実施します。

製品	バックアップ方針
安心でんしょばと	・データベース バックアップサイクル：1 日 1 回 保管期間：20 日間 バックアップデータの保管場所：日本国内

4.3 当社の運用方針

4.3.1 アプリケーションのサービスレベル

当社は、安心でんしょばとのサービスレベルとして以下の指標として定めています。

項目	設定
サービス時間	・Web 上で提供するサービス：24 時間 365 日 ・サポートサービス： 8:45～17:45(通常窓口) / 8:00～18:30(学童クラブ専用窓口) (土日祝日、年末年始、当社所定の休暇を除く) ※悪天候等で変更の場合があります。
サービス稼働率	99.5%以上 ※(※定期メンテナンス・計画停止を除外)
データセンター	日本国内のデータセンターを利用
外部侵入対策	IPS およびファイアウォールによる
サーバシステム監視	サーバ・ネットワーク機器の死活監視 プロセス監視
システム障害監視間隔	常時(24 時間 365 日)
障害対応時間帯	当社営業時間内 ただし、当社が影響範囲が大きいと判断した障害については当社営業時間によらず至急対応します。
障害復旧時間(目標値)	障害検知から 8 時間以内(当社営業時間内)
端末(IC カードリーダー)監視	IC カードリーダー機器の死活監視
端末障害監視間隔	5:00～22:00：365 日
計画停止	メンテナンスや年次更新などのため、計画停止を行います。 計画停止は可能な限り夜間に行います。但し、合理的な理由から早朝、日中帯で行う可能性もございます。
計画停止予告案内	14 日前までに本サービス内のお知らせ又は当社のホームページに掲示し、案内いたします。
緊急停止	セキュリティ危殆化等のやむを得ない場合は計画停止とは別途の緊急停止がありえます。また、当社は合理的な努力をもって管理を行い欠陥や障害に備えますが、本サービス用設備にやむを得ない故障や欠陥が認められた場合、サービスを停止する場合がございます。

アップデート	当社が必要と判断した場合、実施します。

4.3.2 変更管理

機能の変更や廃止、一時的なメンテナンスなど、利用者に影響を与える可能性が生じる場合は、メールやクラウドサービス内の通知機能により 14 日前までに利用者に通知します。

※緊急性の高いメンテナンスについてはこの限りではありません。

4.3.3 ネットワークセキュリティ管理の整合

物理ネットワークと仮想ネットワークの間で整合がとれなくなるような変更作業が行えないようにコントロールを実施しています。

4.3.4 情報機器の処分または再利用

当社は、利用していた情報機器を廃棄及び再利用する際は、当社と機器ベンダーの契約に基づき適切に処理を行っています。

4.3.5 クラウドサービスカスタマの資産除去

当社は、利用者がサービスを終了した場合はサービス上の各種データをダウンロードできなくなります。必要に応じて、解約前にダウンロードして下さい。

利用者がサービスの利用を終了した場合、サービス終了日から 5 営業日以内に利用者に関わる登録データおよび履歴データの一切をサーバーから消去します。消去したデータはいかなる場合でも復旧することはできません。

なお、次の表記載のデータ以外はサービス終了後も設備仕様上、消去できません。

製品	契約終了後に消去する利用者に関するデータ
安心でんしょばと	・施設、学年、クラス名 ・教職員(管理者)情報(氏名、ID、パスワード、メールアドレス) ・児童・生徒情報(氏名、ID、パスワード、保護者連絡用メールアドレス) ・入退室情報 ・メッセージ情報

4.3.6 容量・能力の提供

当社は、サービス提供のために利用している各種リソースについて容量・負荷を常に監視し、必要に応じてリソースを増強します。

4.4 情報セキュリティインシデント

4.4.1 対象インシデント

本項にて対象となるのはインシデントのうち、利用者に大きな影響を与える重大なセキュリティインシデントです。

具体的には次に示すようなものが該当します。

・サービスへの不正アクセスにより、サーバーに保存された情報が外部に流出した。

・サーバーのウイルス感染により、サーバーに保存された情報が外部に流出した。

・外部からの攻撃により、クラウドサービスが利用できない状態となり、その状態が一定時間以上継続した。

4.4.2 インシデントの通知内容と方法

当社で重大な情報セキュリティインシデントを検知した場合は、経過に応じ適切に利用者へ情報提供を行います。

インシデント検知から 5 時間(当社営業時間内)以内を目標に、サービスの通知機能やメールにより利用者へ通知します。

また、情報セキュリティインシデントに関する問合せは、サービス窓口より受け付けています。

4.5 コンプライアンス

4.5.1 所在地 及び 利用者のデータの保存場所

当社は、日本の法人であり、本店所在地は東京都です。クラウドサービスの開発、運営は全て日本国内で行っております。

バックアップデータは、セコムセキュアデータセンター(国内)に設置したサーバーに保管されています。

4.5.2 適用法令

当社と利用者との間の契約における適用法令は利用約款に記載の通り、日本国法を適用しています。

4.5.3 証拠の収集

当社は、サービス内で収集されるデジタル証拠となりうるデータ(ログや契約情報など)を法令により開示を求められた場合、または裁判所・警察などの公的機関から開示を求められた場合に提出することがあります。

4.5.4 記録の保護

利用者データは、不正なアクセスや改ざんを防ぐため、許可された従業員しかアクセスできない、適切に管理されたアクセス権のもとで保管されます。

4.5.5 情報セキュリティの独立したレビュー

当社は、JIS Q27001(ISO/IEC27001) について第三者による審査を受け認証を取得しています。

5. 改訂履歴

版数	日付	主な更新内容
初版(1.0)	2025 年 8 月 25 日	初版発行
2 版(2.0)	2025 年 12 月 15 日	2.1 情報セキュリティ方針に URL を追記 2.2 責任分界点 を更新

■お問い合わせ(ご購入前)

ご購入前のお客様による、資料請求、お見積りやご購入などについてのお問い合わせは下記にて承っております。

https://www.education.jp/education03/contact

■お問い合わせ(ご購入後)

当社製品をご利用中のお客様からのお問い合わせは、お問合わせ窓口(03-6681-5156)から承っております。

※学童クラブのご契約者様専用のコールセンター窓口はご契約者様に個別にご案内しております。