White Paper

Weebum サービス

第 1.0 版

2022 年 5 月 1 日

株式会社ジーティービー

はじめに

White Paper の目的

Weebum サービスは、卒業アルバムのレイアウトや写真の共有や管理などの学校ビジネスに関わるウェブサービスをお客様及びお客様の顧客（学校や写真館）で行うための、AmazonWebService を利用した当社の SaaS(Software as a Service)型のクラウドサービスです。

本ドキュメントは、Weebum サービスの提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

White Paper の対象

Weebum サービスの導入を検討中の方
Weebum サービスを利用中の方

第3者認証

ISO/IEC27001

当社は、2022 年 8 月に ISMS（Information Security Management System）の国際規格である ISO/IEC27001 を取得予定しています。

情報セキュリティのための組織 (A.6)

責任分界点 (A.6.1.1)

仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。

また、当社は、基盤上に構築したアプリケーション及びアプリケーション上のデータについて責任を負います。

当社の責任
・Weebum サービスのセキュリティ対策
・Weebum サービスに保管されたユーザ様情報の保護
ユーザ様の責任
・利用者アカウントの管理（登録、削除、権限設定、アクセス権の設定など）
・パスワード等の利用者の秘密認証情報の管理
・ユーザ様が取扱うデータに対してのバックアップ

地理的所在地（A.6.1.3）
当社の所在地、並びに当社がお客さのデータを保存する国は原則的には日本国となります。当社が基盤として利用するクラウドサービスの仕様上、日本国以外のリージョンにユーザ様のデータを保存される場合があります。

資産の管理 （A.8）

情報のラベル付け（A.8.2.2）
当サービスは、ディレクトリによるファイル管理機能を提供していません。ユーザ管理画面による、アクセス可能ゲートウェイによる管理になります。使用方法の詳細は「ユーザーズマニュアル」をご参照ください。

サービス利用停止後のデータの扱い（CLD.8.1）
Weebum サービスで利用者様から収集したデータの除去に関しては、1 年経過したタイミングで消去いたします。

アクセス制御 （A.9）

利用者アクセスの管理（A.9.2.1）（A.9.2.2）
Weebum サービスは、ユーザ様がストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。お客さまは管理者画面から簡単な操作によりアカウント登録・削除を行い、またユーザのタイプ（写真館・学校など）ごとにユーザ

の権限ごとに割り当てられます。使用方法の詳細は「ユーザーズマニュアル」をご参照ください。

認証情報の管理（A.9.2.3）（A.9.2.4）

初期のアカウント登録を弊社にて行いIDと仮スワードを発行します。登録された仮ワードを使用し、発行されたサービスＵＲＬよりサイトにログインしてください。サインイン後、パスワードの変更（パスワードリセット）を実施してください
ユーザの登録は、ユーザ様のセキュリティポリシーにもとづいて実施してください。
管理者権限はユーザ様のセキュリティポリシーに従い厳重に管理することをお願いします。

アクセス元の地理的制限

ユーザのアクセス元は原則的には日本国のみに制限します。

暗号（A.10）

暗号化（A.10.1.1）

データベースに保管されるユーザ様データは、AES-256 暗号化アルゴリズムを使用して暗号化しています。
ユーザ様のパスワードは、ハッシュ化をしています。
Weebum サービスとユーザ様との間での通信は、SSL/TLS で暗号化し、情報の盗聴等のリスクに対処しています。

運用のセキュリティ（A.12）

変更（A.12.1.2）

ユーザ様に影響を与える Weebum サービスの変更の変更がある場合は電子メール等で通知の上変更を行います。

バックアップ（A12.3.1）

ユーザ様データベースのバックアップは、毎日自動バックを取得しております。自動バックアップは７日間経過したタイミングで自動消去されます。
写真等のデータは原則的に１年４ヶ月のタイミングで消去されます。

上記の期間を経過したデータについては、ユーザ様で必要に応じてデータ保持をお願いします。

ログ（A.12.4.1）（A.12.4.4）

Weebum 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。
ユーザ様が必要となる場合は、当社の Weebum サポート担当までご相談ください。

Weebum サービスは、基盤として利用するクラウドサービス事業者が提供する時刻同期サービスを利用し時刻同期を行っています。
ログは、標準時（UTC）または日本標準時（UTC＋９）で提供されます。

技術的脆弱性の管理（A.12.6.1）

アプリケーションを構築する上で使用するソフトウェアに脆弱性が検知された場合、お客様にメール等で通知し、速やかに影響調査を行います。
脆弱性情報の収集は以下の手段により行います。
・JPCERT コーディネーションセンターから公開される脆弱性情報
・当社関係者による検知
・ユーザ様、基盤を提供するクラウドサービス事業者等の外部からの情報提供

検出した脆弱性については、速やかに影響調査を行い、必要な対策を講じます。対策の状況はメール等でお伝えします。

管理者用手順（CLD12.1.5）

契約書、ユーザーズマニュアルを提供しています。

クラウドサービスの監視（CLD12.4.5）

当社は、Weebum サービスが正常に提供され、他社を攻撃する基盤として使用される等に不正に使用されていないこと、データの漏洩が発生していなか等の監視を行っています。
監視結果をユーザ様に公開できるサービス機能は有しておいません。監視結果が必要な場合は、当社の Weebum サポート担当までご相談ください。

容量・能力の管理

AWS 側で、サーバリソース、及びネットワークリソースを監視しています。サーバー処理能力向上のために自動スケールアップ対策が講じられています。

負荷分散/冗長化

Weebum サービスは基盤を提供する AmazonWebService のマネジメントサービスを使用します。

装置のセキュリティを保った処分又は再利用

VPN 等のクラウド環境の再利用はしていません。

通信のセキュリティ（A.13）

ネットワーク（A.13.1.3）

Weebum サービスは、AWS を利用して、他のユーザ様とのネットワークの分離を適切に行っています。

システムの取得、開発及び保守（A.14）

情報セキュリティ機能（A.14.1.1）

主にユーザ様が検討される情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

機能（ISO/IEC27017 の管理策）	本ホワイトペーパーの記述
A.9.2.1 利用者登録及び登録削除	利用者アクセスの管理
A.9.2.2 利用者アクセスの提供	利用者アクセスの管理
A.9.2.3 特権的アクセス権の管理	認証情報の管理
A.9.2.4 利用者の秘密認証情報の管理	認証情報の管理
A.9.4.1 情報へのアクセス制限	利用者アクセスの管理
A.10.1.1 暗号による管理策の利用方針	暗号化
A.12.3.1 情報のバックアップ	バックアップ
A.12.4.1 イベントログ取得	ログ
CLD.12.4.5 クラウドサービスの監視	クラウドサービスの監視

開発プロセス（A.14.2.1）

当社のクラウドサービスの開発は、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発は非機能要件としてのセキュリティ要件を定義し、厳格な承認プロセスを得たうえで実施されます。セキュリティ機能に関するソースコードはレビューされ、テストプロセスを経たうえでデプロイされます。

ブルーグリーンデプロイメント
当社の提供するクラウドサービスは、新バージョンのリリース時に、ブルーグリーンデプロイメントを採用しています。現バージョンの仮想環境（グリーン）と新バージョンの仮想環境（ブルー）を同時に用意し、アクセス先を切り替えることで、瞬時に新バージョンへの移行を可能としています。

サプライチェーン
当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

情報セキュリティインシデントの管理 （A.16）

インシデント対応プロセス（A.16.1.1）
当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する全ての手順が文書化され、情報セキュリティ委員会により一元的に管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

インシデント対応
Weebum サービスに関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

項目	内容
報告する範囲	データの消失、長時間のシステム停止等のユーザ様に大きな影響を及ぼす可能性のある情報セキィリティインシデント
対応の開示レベル	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、すべて同等のレベルで対処します。
通知を行う目標時間	検知から 3 営業日以内を目標に通知します。
通知手順	お知らせ等は電子メール等で通知 （必用に応じて電話等の手段を使用する場合もあります。）

問合せ窓口	Weebum サポート担当
適用可能な対処	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、あらゆる手段を講じて対処します。

また、ユーザ様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、当社 Weebum サポート担当までご連絡ください。

順守 (A.18)

適用法令及び契約上の要求事項 (A.18.1.1)

利用契約に関する準拠法は、日本法とします。別途、「契約書」をご参照ください。

証拠の収集

法令また権限のある官公庁からの要求により Weebum サービス上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。

知的財産権

本製品、当社ウェブサイト及び本サービスに関する特許権、実用新案権、意匠権、著作権、ノウハウその他一切の知的財産権は、全て当社、当社にライセンスを許諾している者、当社が本製品及び本サービスに関連して業務提携するその他の事業者に帰属しており、本規約に基づく本サービスの利用許諾は、本製品、当社ウェブサイト又は本サービスに関する当社又は当社にライセンスを許諾している者、その他の事業者の知的財産権のユーザへの移転又はユーザ以外の第三者への利用許諾を意味するものではありません本サービスを構成する有形または無形の構成物（プログラム、データベース、画像、マニュアル等の関連ドキュメントを含むがこれらに限られない）に関する著作権を含む一切の知的財産権その他の権利は当社に帰属します。別途、「契約書」をご参照ください。

記録の保護 (A.18.1.3)

当社は、アクセスログのみ 7 日間記録しています。アプリケーションにおけるデータ操作等のログはユーザ様にて保護して頂く必要があります。

暗号化機能に対する規制 (A.18.1.5)

Weebum サービスにおいて暗号化の規制対象になる地域にはサービスを提供していません。

情報セキュリティのパフォーマンス評価（A.18.2.1）

当社では、定期的（最低でも年に一回）に情報セキュリティに関する内部監査を実施しています。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化にあわせて、独立した内部監査を行っています。

当サービスに関するお問い合わせ

株式会社ジーティービー　　Weebum サポート担当　事業
TEL：078-265-5385
FAX：078-265-5389
問い合わせフォーム：　https://www.jp.gtb.co.jp/weebum