White Paper

伝えるウェブ

第 1.0 版

JIS Q 27001:2023 (ISO/IEC 27001:2022)　×　JIS Q 27017:2016 (ISO/IEC 27017:2015)

2025 年 9 月 1 日

アルファサード株式会社

はじめに

White Paper の目的
伝えるウェブは AI により「やさしい日本語」での情報発信を支援する当社のクラウドサービスです。

本ドキュメントは、伝えるウェブ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。

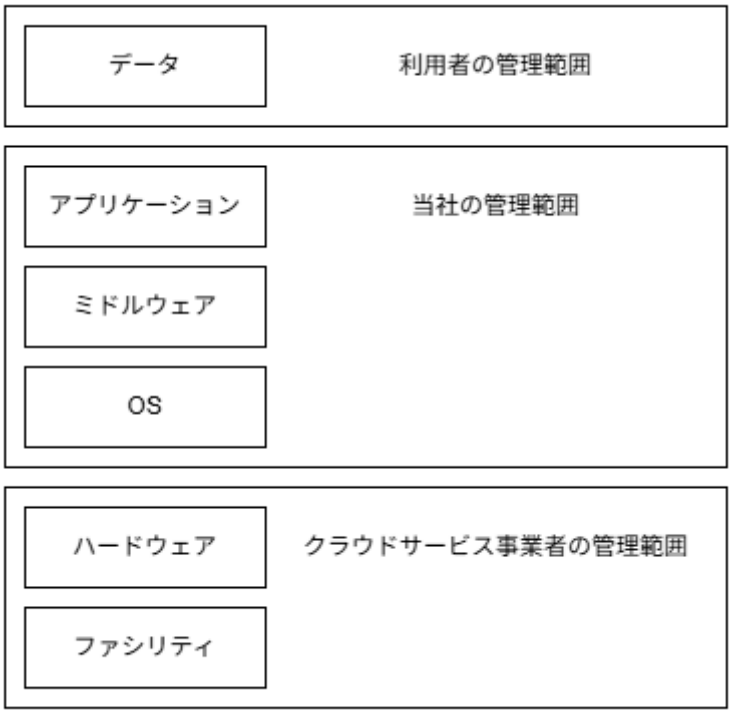
White Paper の対象
伝えるウェブの導入を検討中の方
伝えるウェブを利用中の方

第 3 者認証

ISO/IEC 27001
当社は、全社を認証範囲として 2022 年 11 月 26 日に ISMS（Information Security Management System）の国際規格である ISO/IEC 27001 を取得しています。

情報セキュリティのための組織

責任分界点(A.5.2)（要合意）
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に対して責任を負います。
アプリケーション上のデータについては、利用者の責任において保護していただく必要があります。



当社の責任
- 伝えるウェブのセキュリティ対策
- 伝えるウェブに保管されたユーザー情報の保護

利用者の責任
- 利用者アカウントの管理（ユーザー情報）
- パスワード等の利用者の秘密認証情報の管理
- 利用者が登録し、取扱うデータに対してのバックアップ

地理的所在地(A.5.5)

当社の所在地、並びに当社が利用者のデータを保存する国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において、日本国以外のリージョンに利用者のデータを保存する必要性が生じた場合、利用者に事前に通知したうえで行います。

資産の管理

情報のラベル付け（A.5.13）

伝えるウェブは、カテゴリによるファイル管理機能を提供し、利用者のデータ分類をサポートします。使用方法の詳細は「ユーザーマニュアル」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)（要合意）

伝えるウェブで利用者が作成・保存した利用者のデータの除去に関しては、利用停止から 1 年後の同月末日までに完全に消去いたします。ただし、サービス共通の操作ログデータは対象外になります。

アクセス制御

利用者アクセスの管理(A.5.16)(A.5.18)

伝えるウェブは、本サービスの管理者が本サービス利用者の登録、削除を実施します。
利用プランにより、本サービス利用者を管理者とエディタ利用者に割り当て、エディタ利用者は利用範囲が限定されています。

認証情報の管理(A.8.2)(A.5.17)

管理者から提供されたユーザー情報の変更は利用者側で実施できます。
お客様にて、本サービス利用者のアカウント及び認証情報を適切に管理していただきます。

ユーティリティプログラム

本サービスでは、ユーティリティプログラムの提供は行っておりません。

暗号

暗号化(A.8.24)

データベースのデータの保管場所となるディスク装置やそのバックアップは、AES-256 暗号化アルゴリズムを使用して透過的に暗号化しています。 RDBMS の機能やテーブルでの暗号化は実施していません。
ユーザーのパスワードは、ハッシュ化をしています。
伝えるウェブとユーザーとの間での通信は TLS で暗号化し、情報の盗聴等のリスクに対処しています。

伝えるウェブが稼働する複数サーバー群におけるファイル等のデータ保管場所として、主に個々のサーバー毎の高速なディスクと、それら複数のサーバー群がネットワーク越しに共有する低速・永続的なディスクの 2 つが接続されています。サーバー毎の高速なディスク装置と、そのバックアップは暗号化していません。共有ディスク装置とそのバックアップ

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。

運用のセキュリティ

変更(A.8.32)

利用者に影響を与える伝えるウェブの変更は、ご登録頂いたメールアドレス宛に事前通知します。

バックアップ(A.8.13)

システム全体のバックアップは日次で 35 世代分、利用者が作成したデータのバックアップは、日次で 7 世代分のデータを保持します。
ただし、利用者からのバックアップデータの復元等に関するご要望には対応していません。

ログ(A.8.15)(A.8.17)

伝えるウェブの維持管理に必要となる適切な操作ログを取得しています。利用者は閲覧できません。

また、伝えるウェブの下記の各機能に関する利用状況を記録したアクティビティログを取得しています。ご利用方法は、「伝えるウェブ 管理画面操作マニュアル」に記載があります。

- やさしい日本語
- ルビ
- 読み上げ
- 書き換え支援
- 非同期

伝えるウェブは、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、日本標準時（UTC＋９）で提供されます。

技術的脆弱性の管理(A.8.8)

脆弱性情報の収集と定期的な検査を実施し、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は、速やかに対応を実施いたします。システムを停止しての対応を伴う際には事前にメールにて情報を通知いたします。
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
- 利用者、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

管理者用手順(CLD12.1.5)

「伝えるウェブ 管理画面操作マニュアル」の提供に加え、メールによるサポートを提供しています。

クラウドサービスの監視(CLD12.4.5)

当社は、伝えるウェブが正常に提供され、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いか等の監視を行っています。
監視結果を利用者に公開するサービス機能は有しておりません。監視結果が必要な場合は、当社の伝えるウェブお問い合わせまでご相談ください。

容量・能力の管理

当社は、サーバーリソース、及びネットワークリソースを監視しています。またリソースの増減は GUI から瞬時に実行することができます。サーバーリソースはインスタンスの構成を変更せずにスケールアップによることを原則としていますが、将来的なニーズに照らして、必要があればスケールアウトによる対応も行います。

負荷分散/冗長化

伝えるウェブは基盤を提供するクラウドサービス事業者のマネジメントサービスを使用し、複数の仮想サーバーに処理を振り分ける、ロードバランシングを採用しています。
また、アプリケーションの構成は即時に複製が可能な状態を整えています。

装置のセキュリティを保った処分又は再利用

サービスを構成する機器として、弊社の物理的装置はありません。
そのため装置の処分や再利用を弊社で行うことはありません。AWS の方針に基づきます。

通信のセキュリティ

ネットワーク(A.8.22)

伝えるウェブ専用の仮想ネットワークを構築し、サービスとして必要なポート番号の TCP/IP 接続のみ入口として許可することによりセキュリティを確保しています。

また、伝えるウェブが稼働するクラウドコンピューティング環境と、当社の管理用環境を別セグメントとして分離しています。

システムの取得、開発および保守

情報セキュリティ機能(A.5.8)

主に利用者が検討す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/IEC 27017 の管理策）	本ホワイトペーパーの記述
5.16　識別情報の管理	利用者アクセスの管理
5.17　認証情報	認証情報の管理
5.18　アクセス権	利用者アクセスの管理
8.2　特権的アクセス権	認証情報の管理
8.3　情報へのアクセス制限	利用者アクセスの管理
8.13　情報のバックアップ	バックアップ
8.15　ログ取得	ログ
8.24　暗号の使用	暗号化
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.8.25)

当社のクラウドサービスの開発は、機能性とユーザー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。
また、リリース後も定期的な脆弱性診断を行っています。

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、およ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

インシデント対応プロセス(A.5.24)

当社では、ISO/IEC 27001 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

伝えるウェブ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、伝えるウェブ用ウィジェット・辞書の改ざん等の利用者に大きな影響を及ぼす可能性のある情報セキュ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利用者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 72 時間以内を目標に通知します。
通知手順	ご登録のメールアドレス宛及び管理画面 （必要に応じて電話等の手段を使用する場合もあります。）
問い合わせ窓口	伝えるウェブお問い合わせ
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利用者に影響があるものは、あらゆる手段で対処します。

また、利用者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、伝えるウェブ内のお問い合わせページ、又は当社伝えるウェブお問い合わせからご連絡ください。

順守

適用法令及び契約上の要求事項(A.5.31)

利用契約に関する準拠法は、日本法とします。別途、「利用規約」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伝えるウェブ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。合意について別途、「利用規約」をご参照ください。

知的財産権

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、「利用規約」をご参照ください。

記録の保護(A.5.33)

本サービスのご利用状況に関するアクティビティログは利用者にて管理して頂く必要があります。当社は管理画面における利用者の操作ログを取得しています。アクセス制限を実施しており、利用者は閲覧できません。

暗号化機能に対する規制(A.5.31)

伝えるウェブにおいては、輸出規制の対象となる暗号化の利用はありません。

情報セキュリティのパフォーマンス評価(A.5.35)

当社では、ISO/IEC 27001 (JIS Q 27001)に基づく ISMS 認証を得ており、当サービスの開発・運用・保守業務に関しても管理策に基づいた情報セキュリティ対策を実施しています。

また、定期的な内部監査及び、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。

伝えるウェブに関するお問い合わせ

伝えるウェブお問い合わせ
https://tsutaeru.cloud/contact/contact_us.html
フォームをご利用いただけない場合は、
info@tsutaeru.cloud
宛てにメールでご連絡ください。