ZOHO

Zohoのセキュリティーとコンプライアンス

Zoho サービスは、

機密性、完全性、可用性を担保した運用体制により

稼働実績月間99.9%を実現。

インシデント脅威から個人情報を守る3つの要素

OECDの情報セキュリティガイドラインでは、情報セキュリティは情報の「機密性」（Confidentiality）、「完全性」（Integrity）、「可用性」（Availability）の3要素からなると定義。ISO/IEC 27001(JIS Q 27001)では、この3要素「CIA」が重視されています。また、ISMS（情報セキュリティマネジメントシステム）も「情報の機密性、完全性及び可用性を維持すること」に留意する必要があるとしています。

機密性（Confidentiality）

顧客情報や製品の開発情報など、企業にとって機密性の高い情報資産には、社内でもできるだけアクセスできる人を減らすことで漏洩や悪用のリスクを減らすことが求められます。
具体的には、データの暗号化、アクセス制御・物理アクセス制御・ログインの要求や閲覧・編集権限の制御、パスワードの定期更新ルールなどが挙げられます。

完全性（Integrity）

情報資産が正しい状態で維持されるために、不正アクセスや内部操作により情報の改ざんを防止する対策が求められます。また、火災や天災によりデータが破損・損失するリスクへの対策も必要です。ここではデータの「読み込み」「書き込み」「保管」「転送」の4つの工程でのリスクと回避策を検討する必要があります。具体的には、データの暗号化や操作ログの記録、データバックアップの保存などが挙げられます。

可用性（Availability）

システムの稼働継続率とも言われ、データをいつでも安全に利用できることが求められます。具体的には、システムダウンや災害時にスピーディーにシステムを復旧させることが求められます。

セキュリティ認証

ISO / IEC 27001（ISMS認証）

ISO / IEC 27001は、最も広く認知された国際セキュリティ規格のひとつです。この認証は、ISOの高い国際基準に準拠する組織団体に付与されます。Zohoは、アプリケーション、システム、人員、技術、プロセスを対象としてISO / IEC 27001：2013認証を取得しています。

ISO/IEC 27701（ISMS認証）

ISO/IEC 27701 は、組織の持つ、個人を特定できる情報の管理のため、既存のISO/IEC27001およびISO/IEC27002規格を拡張したものです。この認証基準は、プライバシー情報管理システム（PIMS）を確立、実装、維持、および継続的に改善するために、追加要件で既存の情報セキュリティ管理システム（ISMS）を強化するよう設計されています。この規格により、組織は世界中のさまざまなプライバシー規制への準拠を証明できます。

ISO / IEC 27017（ISMS認証）

ISO/IEC 27017は、クラウドサービスの提供と利用に適用される情報セキュリティ管理策のガイドラインを提供しており、ISO/IEC 27002に規定される管理策への追加実施ガイダンス、およびクラウドサービスに関連する追加管理策を実施ガイダンスと共に提供しています。Zohoは、このISO/IEC 27017:2015（情報技術 - セキュリティ技術 -ISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）の認証を取得しています。

ISO/IEC27018（ISMS認証）

ISO/IEC 27018は、パブリッククラウドで処理されるPII（Personally Identifiable Information - 個人情報）の保護対策を実施するための、一般的な管理目標、セキュリティ管理策およびそのガイドラインを定めています。その管理策は、ISO/IEC27001およびISO/IEC27002、ISO/IEC27018が拡張されたものであり、クラウドプロバイダーが個人情報（PII）をどのように扱うかに対し関心のある組織にガイダンスを提供します。

SOC 2

ZohoはSOC2Type IIに準拠しています。SOC 2は、AICPAのトラストサービス原則の基準を満たす内部統制の設計および運用の有効性の評価です。

PRIVACY FEEDBACK
Powered by TRUSTe

データ保存先とデータセンター所在国およびその認定状況

アカウントを作成したWebサイトのドメイン	データセンター	認証状況
www.zoho.com/jp/	日本	ISO 27001およびSOC2 Type II
www.zoho.com	アメリカ	SOC1 Type IIおよびSOC2 Type II
www.zoho.eu	EU（オランダ&アイルランド）	ISO 27001
www.zoho.in	インド	ISO 27001

詳細は、データセンター所在マップ（https://www.zoho.com/know-your-datacenter.html ）を参照ください。

情報の可用性を確保するための対策

分散アーキテクチャ	Zohoは、処理や配置などを分散させることで、可用性やスケーラビリティ、パフォーマンスなどを向上させる分散アーキテクチャを採用しています。
電源の冗長化*	Zohoは、電力の供給から配電まで、電源の冗長化を考慮して設定されています。
インターネット接続の冗長化*	Zohoのインターネット接続は、複数のTier-1 ISPを介しており、1つのISP（プロバイダ）に障害や遅延が発生した場合にも安定したデータへのアクセスを確立できます。
ネットワーク機器の冗長化*	Zohoは、内部ネットワークのあらゆるレベルで単一障害点をなくすため、ネットワーク機器（スイッチ、ルーター、セキュリティゲートウェイ）を冗長化しています。
冷却装置/温度制御装置の冗長化*	ZohoのサーバーはN+2冗長構成のHVACシステムと温度管理システムにより保護されています。
ジオミラーリング	すべてのデータは、災害発生時の迅速な復旧と事業継続の目的として、複数の地域でミラーリングされています。
防火対策	データセンターは、業界基準を満たす防火・火災防御システムにより保護されています。
データ保護とデータバックアップ	すべてのデータベースは、複数のサーバーを介して定期的にバックアップされており、障害や災害発生時にも速やかにデータを復旧できます。

*冗長化とは、コンピューターやシステムに何らかの障害が発生したケースに備えて、予備装置を普段から配置、運用しておくことをいいます。

物理的セキュリティ

24時間365日監視	当社のデータセンターは、民間の警備会社による24時間365日の監視体制が置かれています。また、暗視対応の監視カメラにより常に監視されています。
入退室管理	データセンターへの立ち入りは、許可を受けた少人数のみに厳しく制限されており、入室時には生体認証を含む2段階での認証が求められます。
所在の非公開	サーバーの所在地は非公開であり、攻撃の対象とならないよう一般的な外観の施設内部に設置されています。
防弾壁	サーバーは、すべて防弾壁によって外的攻撃から保護されています。

人的セキュリティ

従業員の審査	お客さまサポート対応にあたる当社従業員のうち、機密情報の取り扱いに関する高レベルな資格を保持する者のみがデータセンターのデータベースにアクセスします。また、すべてのアクセスはパスワードによる管理・記録がされています。
アクセス承認	データセンターのデータベースにアクセスできる当社従業員は、サポート対応に必要な場合であり、かつお客さまの承認またはセキュリティ管理責任者が承認した場合にのみお客さまのデータベースにアクセスできるものとし、その他一切のアクセスを禁止しています。
定期監査	データセンターのセキュリティ管理に対し、定期的な監査を実施しています。また、すべての業務プロセスは経営陣による審査を実施しています。

ネットワークセキュリティ

この情報は、ハッキングリスクを回避するため概要のみの公開となります。ネットワークセキュリティに関するご質問は当社まで直接お問い合わせください。（セキュリティの関係上、お伝えできない場合もございます。予めご了承ください。）

通信の暗号化	データベースに送信されるすべての情報はTLS1.2プロトコルを使用し暗号化されており、SHA-254 中間CA証明書により安全性を確保しています。暗号化には、最新かつ強固なAES_CBC / AES_GCM 256ビット/ 128ビットキー、メッセージ認証にはSHA2、キー交換メカニズムにはECDHE_RSAを使用しています。
IDC/IPS	当社ネットワークは、IDS（侵入検知システム）・IPS（侵入防止システム）によって防御・選別されています。
アクセス管理・監視	すべてのデータアクセスはKerberos（ケルベロス）認証により管理・監視されています。また、コンピュータからデータをコピーまたは転送できないよう制御されています。
分散オペレーティングシステム	Zohoサービスは、分散オペレーションシステムを採用しています。分散オペレーションシステムとは、ネットワーク上にあるすべてのコンピューターを仮想的に1つのマシンとしてとらえ、1つのシステムとして運用する手法です。個々のコンピューターが相互に連携して分散処理を行うため、個々の負担も軽減され、効率的な処理が可能となります。
ウィルススキャン	Zohoのサーバーへのアクセスは、最新のウイルススキャンプロトコルにより自動的にスキャンし、有害ウイルスの侵入を防止しています。

本文中に記載されている会社、ロゴ、製品の固有名詞は各社の商号、商標または登録商標です。本ガイドの記載内容は、2021年6月29日現在のものです。記載されている内容は、変更される場合があります。

improve 株式会社インプルーブ

052-228-0624

sales@improve.co.jp

https://improve.co.jp