Site24x7 セキュリティチェックシート

・本チェックシートは Zoho Corporation（以下、Zoho）が提供する「Site24x7」について安全・信頼性に係る情報を記載したものです。

・クラウドサービス提供事業者であるZohoの基本情報、組織体制などは、以下サイトにて開示しています。
（https://www.zohocorp.com/）
・本チェックシートは改善のために予告なく変更することがあります。

情報開示項目			内容	事業者回答
1	開示情報の時点	開示情報の日付	開示情報の年月日(西暦)	2021年2月18日
サービス基本特性				
2	契約の終了等		契約終了時等の情報資産（利用者データ等）の返却責任の有無と、受託情報の返還方法・ファイル形式・費用等	無し ※契約終了前に、お客様自身が一部のデータを所定の形式でエクスポート可能
3		情報の返却・削除・廃棄	情報の削除又は廃棄方法の開示の可否と、可能な場合の条件等	開示可 お客様がSite24x7の利用を継続する限り、アカウント内のデータを保持します。 Zohoのユーザーアカウントを削除すると、お客様のデータが、6か月ごとに行われる自動クリーンアップによってZohoのデータベースから削除されます。 データベースから削除されたデータは、3か月後にバックアップからも削除されます。 またお客様のアカウントで支払いのないまま、連続120日間未ログインの場合は、お客様への事前の通知と、データのバックアップオプションを提供し、そのアカウントを削除します。 ▼データの保持と廃棄 https://www.zoho.com/jp/security.html
4			削除又は廃棄したことの証明書等の提供	無し
5	サービス品質	サービス稼働設定値	サービス稼働率の目標値	99.9%
6		認証取得・監査実施	プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1等）の取得	ISO/IEC 27001 ISO/IEC 27017 ISO/IEC 27018 SOC 2 ▼コンプライアンス認証取得状況 https://www.zoho.com/jp/compliance.html
7		脆弱性診断	脆弱性診断の有無	有り 認証を受けたサードパーティのスキャンツールや社内ツールを組み合わせ、セキュリティの脅威をスキャンし、手動/自動による侵入テストを行っています。 ▼脆弱性の管理 https://www.zoho.com/jp/security.html
8		バックアップ対策	利用者データのバックアップ実施インターバル	フルバックアップを週次、差分バックアップを日次で実施しています。 バックアップの復元及び検証は毎週行われ、バックアップデータは3か月間保持されます。 ▼バックアップ https://www.zoho.com/jp/security.html
9		サービス継続	サービスが停止しない仕組み（冗長化、負荷分散等）	エンドポイントレベルでの冗長性を確保するため、複数のスイッチ、ルーター、セキュリティゲートウェイを採用し、単一障害点が生じないようにしています。 ▼ネットワークの冗長性 https://www.zoho.com/jp/security.html
10			DR（ディザスターリカバリー）対策の有無と、「有り」の場合はその概要	有り プライマリデータセンターのデータが、ほぼリアルタイムで、セカンダリデータセンターに複製されます。 プライマリデータセンターに問題が発生した場合、セカンダリデータセンターがアクティブになり、最小限のロスタイムで運用を継続させます。どちらのデータセンターも、複数のISPでインターネット接続をしています。 ▼災害復旧と事業継続 https://www.zoho.com/jp/security.html

アプリケーション等				
11	セキュリティ	死活監視	死活監視の有無	有り ▼Site24x7の可用性ステータス https://status.site24x7.com/
12		時刻同期	時刻同期への対応の有無	有り
13		ウイルス対策	ウイルス対策の有無	有り すべてのユーザーのファイルを、マルウェアの拡散防止するよう設計された独自の自動スキャンシステムを用いてスキャンしています。独自のアンチマルウェアエンジンが、外部の複数の脅威情報ソースから定期的に情報を受け取り、ブラックリストに挙げられた署名や悪意のあるパターンに対してファイルをスキャンします。さらに、機械学習技術が組み込まれた独自の検出エンジンにより、マルウェアから顧客データを保護しています。 ▼マルウェアと迷惑メール対策 https://www.zoho.com/jp/security.html
14		管理者権限の運用管理	システム運用部門の管理者権限の登録・登録削除の手順の有無	有り 技術的なアクセス制御と内部ポリシーにより、従業員が恣意的にユーザーデータにアクセスすることを禁じています。データ漏洩リスクを低減するため、最小権限の原則とロールベースのアクセス制御の原則に従っています。 実稼働環境へのアクセスは、中央ディレクトリで管理され、強力なパスワード、2段階認証、パスフレーズで保護されたSSH鍵を組み合わせた認証を行っており、厳しい規則によってセキュリティ強化された端末で別ネットワーク経由して行われます。さらにすべての操作を記録し、定期的に監査しています。 ▼管理的アクセス https://www.zoho.com/jp/security.html
15		ID・パスワードの運用管理	事業者側にて、利用者のID・PWを付与する場合におけるIDやパスワードの運用管理方法の規程の状況	Zohoの統合ID・アクセス管理（IAM）サービスで管理しております。 ▼シングルサインオン（SSO） https://www.zoho.com/jp/security.html
16		記録（ログ等）	利用者の利用状況の記録（ログ等）取得の状況と、利用者への提供可否	監査ログをご利用いただけます。 ▼ログとモニタリング https://www.zoho.com/jp/security.html
17			システム運用に関するログの取得の有無	有り サービス、Zohoネットワーク内で収集された情報をモニタリングし分析しています。この情報をイベントログ、監査ログ、障害ログ、管理者ログ、オペレーターログの形式で記録しています。 ▼ログとモニタリング https://www.zoho.com/jp/security.html
18		セキュリティパッチ管理	パッチ管理の状況とパッチ更新間隔等、パッチ適用方針	修正を必要とする脆弱性を確認した場合、それを記録し、重要度に基づいて優先順位を設定して担当者に割り当てます。また関連リスクを確認し、システムへのパッチ適用または、管理策の適用を行い、クローズするまで、脆弱性をトラッキングします。 ▼脆弱性の管理 https://www.zoho.com/jp/security.html
19		暗号化対策	暗号化措置（データベース）への対応の有無と、「有り」の場合はその概要	有り お客様のデータ保存時に、256ビット高度暗号化標準（AES）で暗号化しています。Zohoはその鍵を社内の鍵管理サービス（KMS）を使用して管理しています。マスター鍵を使ってデータ暗号化鍵を暗号化し、セキュリティレイヤーを追加します。マスター鍵とデータ暗号化鍵は、物理的に分離されており、アクセスが制限された別々のサーバーに保管しています。 ▼暗号化 https://www.zoho.com/jp/security.html

ネットワーク				
20	セキュリティ	ファイアウォール	ファイアウォール設置等の不正アクセスを防止する措置の有無	有り ファイアウォールを使用して、Zohoネットワークへの不正アクセスや望ましくないトラフィックから保護しています。 ▼ネットワークセキュリティ https://www.zoho.com/jp/security.html
21		不正侵入検知	不正パケット、非権限者による不正なサーバ侵入に対 する検知等の有無と、「有り」の場合は対応方法	有り Zohoの侵入検知システムは、各端末のホストベースのシグナルと、Zohoサーバー内のモニタリングポイントからのネットワークベースのシグナルを記録しています。Zohoの実稼働ネットワークに存在するすべてのサーバーの管理的アクセス、特権コマンドの使用、システムコールを記録し、セキュリティエンジニアにインシデント警告を送ります。 ▼侵入検知および防止 https://www.zoho.com/jp/security.html
22		ユーザー認証	ユーザー（利用者）のアクセスを管理するための認証方法、特定の場所及び装置からの接続を認証する方法 等	シングルサインオンや多要素認証などをサポートしております。 ▼シングルサインオン（SSO）、多要素認証 https://www.zoho.com/jp/security.html
23		暗号化対策	暗号化措置（ネットワーク）への対応の有無と、「有り」の場合はその概要	有り Zohoへの送信データは強力な暗号化プロトコルで保護されています。Zohoサーバーへのすべての通信（Webアクセス、APIアクセス、モバイルアプリ、IMAP/POP/SMTPメールクライアントアクセスなど）に対して、TLS 1.2/1.3の使用を義務付けています。 Zohoは、Perfect Forward Secrecy（PFS）をフルサポートしているため、以前の通信内容が復号化される可能性はありません。Zohoは、すべてのWeb通信に対してHTTP Strict Transport Security（HSTS）を有効にすることで、Zohoへの接続をすべて暗号化通信に限定します。 ▼暗号化 https://www.zoho.com/jp/security.html
ハウジング（サーバー設置場所）				
24	サーバー設置場所	所在地	国名、日本の場合は地域ブロック名（例：関東、東北）	米国、ヨーロッパ、インド、オーストラリア 日本のお客様データは、基本的には米国のデータセンターに記録されます。
25		非常用電源	非常用電源の有無	有り ▼災害復旧と事業継続 https://status.site24x7.com/
26		火災対策	火災対策の有無	有り
27		空調設備	空調設備の有無	有り
28	セキュリティ	入退室管理等	入退室記録の有無	有り CCTV（監視）カメラを通じて、Zohoのすべてのビジネスセンターおよびデータセンターへの入退出を監視しています。映像のバックアップは、現地の要件に従って所定の期間保管されます。 ▼監視 https://www.zoho.com/jp/security.html
29			監視カメラの有無	有り
30			個人認証システムの有無	有り アクセスカードを使用してZohoのリソース（建物、インフラストラクチャー、施設）へのアクセスを管理しています。従業員、請負業者、ベンダーおよび訪問者に対し異なるアクセスカードを支給し、それぞれの目的に応じたアクセスのみが許可されるようにしています。 ▼ワークスペース https://www.zoho.com/jp/security.html