cybozu.com セキュリティチェックシート

サイボウズ株式会社
東京都中央区日本橋二丁目7番1号
東京日本橋タワー27階

お問い合わせ先　　ISMS事務局

2024年11月6日版

更新日：2024年11月6日

◆本チェックシートは、サイボウズ株式会社が提供する cybozu.com サービスについて、そのセキュリティ対策を記載したものです。

◆サイボウズ株式会社は、下記認証登録範囲の情報セキュリティマネジメントシステムについて
ISO/IEC27001:2013／JIS Q 27001:2014 の要求事項に適合し、認証登録番号 IS577142 を保有しています。
〈認証登録範囲〉
・クラウドサービスの運用基盤の設計、構築及び運用保守
・社内情報システム基盤の設計、構築及び運用保守
・クラウドサービス、オンプレミス製品及び社内システムの開発
2020年7月9日付 適用宣言書 第5版
認証機関：BSIグループジャパン株式会社

◆サイボウズ株式会社は ISO/IEC 27001:2013 に基づく認証されたISMSを保有し、下記登録認証範囲のISMSクラウドセキュリティを ISO/IEC 27017:2015 のガイドラインに沿って運用し、JIP-ISMS517-1.0 に適合し、認証登録番号 CLOUD 715091 を保有しています。
〈認証登録範囲〉
・Garoon、kintone、サイボウズOffice、Mailwise、cybozu.comの提供に係るクラウドサービスプロバイダとしてのシステム運用・保守に係るISMSクラウドセキュリティマネジメントシステム
2020年7月9日付 適用宣言書 第5版
認証機関：BSIグループジャパン株式会社

◆クラウドサービス運用基盤cybozu.com、kintone、Garoonは、ISMAPクラウドサービスリストに登録されています。登録番号 C21-0016-2

◆本チェックシートの項目は、経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版
（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf）を基に、任意で項目の追加削除、及び主客体の解釈を加えて作成したものです。

		確認事項	実施有無	備考
1	情報セキュリティのための方針群			
	1	経営陣によって承認された情報セキュリティに関する基本方針を定めた文書があること。また、該当文書を全従業員及びクラウドサービス利用者に明示すること。	○	経営層に承認されたクラウドサービスに関するセキュリティの基本方針（https://www.cybozu.com/jp/terms/security.html）及び社内セキュリティに関する従業員が遵守すべき社内規程（情報セキュリティ規則等）を定めております。 当方針は、全従業員には、社内規程として周知し、クラウドサービス利用者には、当社ホームページに公開しております。 ▼ISMS基本方針 https://www.cybozu.com/jp/terms/security.html
	2	情報セキュリティに関する基本方針を定めた文書は、定期的またはクラウドサービス提供に関係する重大な変更が生じた場合に、レビューすること。	○	情報セキュリティマネジメントシステム（以下、「ISMS」）を構築し、情報セキュリティ保全活動を効果的に推進するために、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、監査及び見直しを行う仕組みを確立しております。 また、経営層によって承認されたクラウドサービスに関するセキュリティの基本方針は、ISMSにおいて、経営者によって毎年及び重大な変化が発生した場合に見直しております。
2	情報セキュリティのための組織			
	1	内部組織		
	1	経営陣は、情報セキュリティに関する取り組みについての責任及び関与を明示し、組織内におけるセキュリティを積極的に支持・支援を行うこと。	○	当社グループの内部統制についての基本方針にて、経営者、監査役、従業員の行動指針を明らかにし、クラウドサービスに関するセキュリティの基本方針にて、業務に携わる役員、社員が継続的に情報セキュリティ対策を推進することを宣言しております。 ▼内部統制の基本方針 https://cybozu.co.jp/company/internal-control/ ▼ISMS基本方針 https://www.cybozu.com/jp/terms/security.html また、情報セキュリティマネジメントシステム（以下、「ISMS」）を構築し、情報セキュリティ保全活動を効果的に推進するために、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、監査及び見直しを行う仕組みを確立しております。 さらに、当社経営層によって承認されたクラウドサービスに関するセキュリティの基本方針は、ISMSにおいて、経営者によって毎年及び重大な変化が発生した場合に見直しております。
	2	情報セキュリティ責任者とその役割を明確に定めること。またクラウドサービスの情報セキュリティに関する窓口を明確にし、外部に公開すること。	○	セキュリティ対策、手順等について、セキュリティ関係者および関係組織と審議する委員会としてCSM（サイボウズセキュリティミーティング）を設置しております。 委員長は情報セキュリティ管理責任者としております。 クラウドサービスの情報セキュリティに関する窓口は、「脆弱性に対する体制（CSIRT）」を設け、当社ホームページに公開しております。 ▼CSIRT記述書 https://www.cybozu.com/jp/productsecurity/management/cysirt.html
	3	情報セキュリティ対策、設備の認可に対する手順等を明確にし、文書化すること。	○	ISMSマニュアルにて、情報セキュリティ対策（日々の活動や緊急対応、役割別PDCA）を明記しております。
	4	クラウドサービス利用者がクラウドサービスの受け入れを行うために必要な資料を作成し、提供すること。また、提供するクラウドサービスSLA などサービス開始前の合意事項をクラウドサービスの利用を検討する者に明示すること。	○	本チェックシートにて、クラウドサービス利用者に対し、提供するクラウドサービスに関するセキュリティ対策を記載し、提供しております。 サービス開始前の合意は、クラウドサービス利用者に対し、当社ホームページに提供するサービスレベル目標(SLO)を公開しております。 ▼サービスレベル目標(SLO) https://www.cybozu.com/jp/infrastructure/slo.html

	5	クラウドサービスのサポート窓口、苦情窓口を明確にし、外部に公開すること。	○	お問い合わせについては以下の窓口を用意しております。 お問い合わせ方法：電話、メール 受付時間：月～金 10:00～12:00、13:00～17:30（祝日・年末年始は除く） ▼お問い合わせ https://www.cybozu.com/jp/inquiry/tel/ また、障害発生時のサポート窓口として時間外障害窓口（β サービス）もご提供しております。 ▼cybozu.com時間外障害窓口（β サービス） https://www.cybozu.com/jp/inquiry/em_contact.html
3 人的資源のセキュリティ				
	1 雇用前			
	1	従業員のセキュリティの役割及び責任は、情報セキュリティ基本方針に従って定め、文書化すること。また該当文書を雇用予定の従業員に対して説明し、この文書に対する明確な同意をもって雇用契約を結ぶこと。	○	雇用形態に関わらず、雇用契約書及び、社内規定にて定めております。 経営層に承認されたクラウドサービスに関するセキュリティの基本方針及び社内セキュリティに関する従業員が遵守すべき社内規程（情報セキュリティ規則等）を定めております。また、雇用する従業員とは、雇用契約書を締結し、その中で就業規則及び社内規程の遵守について明確に同意を確認しております。 ▼ISMS基本方針 https://www.cybozu.com/jp/terms/security.html
	2 雇用期間中			
	1	すべての従業員に対して、情報セキュリティに関する意識向上のための教育・訓練を実施すること。	○	雇用する従業員（採用の日から3ヶ月間は試用期間）には、入社オリエンテーションの一環で、コンプライアンス研修を実施しており、社内規程の教育を行っております。ルール違反が発生した場合には個別に再教育を行っております。 ISMSの適用範囲者に対してはPDCAサイクルの一環として年に1度教育を実施しています。 また、社内規程の変更の都度、全従業員に通知し、周知を行っております。 さらに、教育・研修を実施し、セキュリティ、コンプライアンス等に関する教育についても必要に応じて実施しております。
	2	セキュリティ違反を犯した従業員に対する対応手続きを備えること。	○	以下のセキュリティ違反を犯した従業員は、当社就業規則に規定された懲戒の対象となることが、情報セキュリティ規則に明記されております。 － セキュリティ事件・事故を故意に起こそうとした場合 － 情報セキュリティに関する重大な過失を犯した場合 － 情報セキュリティに関する過失を繰り返した場合
	3 雇用の終了又は変更			
	1	従業員の雇用の終了または変更となった場合に、情報資産、アクセス権等の返却・削除・変更の手続きについて明確にすること。	○	従業員の退職・休職時の手続は、以下のとおり情報セキュリティ規則に明記されております。 － 退職時は、全てのシステムのアカウントを削除または使用停止する － アクセス権、リモートアクセス権の変更申請にて削除または使用停止する － 退職者・休職者から業務PC、鍵、カードキー等を回収する
4 資産の管理				
	1	情報資産について明確にし、重要な情報資産の目録及び各情報資産の利用の許容範囲に関する文書を作成し、維持すること。また情報資産について管理責任者を指定すること。	○	情報資産台帳で各資産名、管理責任者、C.I.Aレベル、利用許可範囲、情報コンテナ、保存期間ごとに分類し、記載しております。当台帳はISMSにおいて、定期的に見直し更新しております。
	2	組織に対しての価値、法的要求事項、取り扱いに慎重を要する度合い及び重要性の観点から情報資産を分類すること。	○	
5 物理的及び環境的セキュリティ				
	1	重要な情報資産がある領域を保護するために、物理的セキュリティ境界(例えば、有人受付、カード制御による入口)を用いること。	○	情報資産がある領域（セキュリティエリアは、ワークスペースと入室制限スペース）は、セキュリティカード制御を用いて、フリースペースとの物理的な境界を設けております。 重要な情報資産がある領域(入室制限スペース)は、セキュリティカード制御及び生体認証を用いて物理的な境界を設けております。
	2	重要な情報資産がある領域へ許可された者のみがアクセスできるように入退室等を管理するための手順、管理方法を文書化すること。	○	重要な情報資産がある領域は、情報セキュリティ規則に明記されており、許可された者のみがアクセスできるようにセキュリティカード制御をしております。 入室可能範囲（セキュリティカードのアクセス権の付与）は、以下の基準に基づいて、各本部の本部長が決裁しております。 － 業務上の必要性 － 信頼性の観点 － 抑止力の観点
	3	サーバーが設置されているデータセンターは耐震構造となっていること。	○	1981年6月改正の建築基準法の新耐震基準に従う耐震構造または免振構造です。 東日本データセンターは耐震構造、西日本データセンターは免振構造となっております。
	4	データセンターの落雷対策を確認すること。	○	JIS基準に基づいた避雷設備を設置しており、落雷対策として特高受変電設備に避雷器、誘導雷対策として PDU および PDF に SPD を設けております。 また、誘導雷対策における電圧防護レベルは 1.5kV となります。
	5	データセンターの水害対策を確認すること。	○	津波、高潮、洪水、大雨における対策を実施しております。なお、データセンターはFISCの設備基準を満たしており、JDCCのデータセンターファシリティスタンダードのほぼすべての項目でティア4を満たしております。

	6	データセンターの静電気対策を確認すること。	○	サーバエリアの床に静電気対策を実施しております。 また、サーバルーム内の温度、湿度を管理し、静電気の発生を防止しております。
6	運用のセキュリティ・アクセス制御			
	1	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の運用管理の手順について文書化し、維持していくこと。	○	アプリケーション、OS、サーバー、ネットワーク機器の運用管理の手順については文書を作成しています。こちらの文書については操作方法の変更や機材追加・変更が発生する毎に更新しております。 また cybozu.com サービスの操作手順についてはマニュアルを公開しております。 ▼ サイボウズ製品 ヘルプサイト https://jp.cybozu.help/ja/
	2	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の変更について管理すること。またクラウドサービス利用者に影響を及ぼすものは事前に通知すること。	○	cybozu.comへログインした後のトップページにてお知らせしています。 また、弊社お知らせサイトやメールで適時公開を行っております。 ▼サイボウズからのお知らせ(メンテナンス情報) https://cs.cybozu.co.jp/maintenance/
	3	クラウドサービスを利用できるオペレーティングシステムやウェブブラウザの種類とバージョンを明示すること。利用できるOSとブラウザに変更が生じる場合は事前に通知すること。	○	動作環境を公開しております。詳細はWebページにてご確認ください。 ▼動作環境 https://www.cybozu.com/jp/service/requirements.html
	4	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	脆弱性情報について日次で収集するとともにベンダーやセキュリティ 機関(JPCERT等)からの情報を随時受け、影響について確認をしております。またパッチの適用についても手順に則り適用作業を実施しております。
	5	クラウドサービスの資源の利用状況について監視・調整をし、利用状況の予測に基づいて設計した容量・性能等の要求事項について文書化し、維持していくこと。	○	クラウドサービスの利用状況については監視を実施しております。利用状況の推移から増強・増設の計画を立て、その内容については文書を作成しております。
	6	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器について脆弱性診断を行うこと。また、その結果を基に対策を行うこと。	○	弊社担当部門によるレビュー、テストを実施しております。 また、第三者機関による外部セキュリティ監査も実施しております。 プラットフォーム、アプリケーション共に1回/年以上の実施となり、アップデート内容に応じて実施しております。 またその結果に基づき改善等対応作業を実施しております。 ▼安全性への取り組み https://www.cybozu.com/jp/productsecurity/ このほか、脆弱性を報告いただいた方に報奨金をお支払する、「脆弱性報奨金制度」を運営しております。 詳細は以下のホームページをご覧ください。 ▼脆弱性報奨金制度 https://cybozu.co.jp/products/bug-bounty/
	7	モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。また、認可されていないモバイルコードを実行できないようにすることが望ましい。	※	自社で作成し配布するモバイルコードについては、自社内で定められたセキュリティ方針に沿って開発および、試験が行われております。 サービス内で利用されているモバイルコードには、第三者が作成したモバイルコードがございます。 自社で配信する第三者が作成したモバイルコードを管理し、定期的にベンダーが公開するセキュリティ情報を収集し、適切に更新する体制を整えております。 cybozu.com 上で提供されるサービスには、お客様がJavaScriptを読み込む機能を提供するサービスがございます。お客様が安全なJavaScriptコードを作成することを支援することを目的として、「セキュアコーディングガイドライン」を当社ホームページで公開しております。 ▼セキュアコーディング ガイドライン https://cybozu.dev/ja/kintone/docs/guideline/secure-coding-guideline/
	8	クラウドサービス利用者の情報、ソフトウェア及びソフトウェアの設定について定期的にバックアップを取得し、検査すること。	○	お客様のデータは機材故障時のデータ喪失を防ぐため冗長化されたストレージで運用されます。 また、運用事故によるデータ異常や喪失時に備え、日単位でリストア可能なバックアップが14日分復旧用に管理されています。 さらに、災害時への備えとして東西のデータセンター間で復旧用データのレプリケーションも取得されます。 バックアップは運用上生じる可能性のある問題からの復旧用であり、お客様希望によるリストアに対応するものではありません。 ▼データの消失・漏洩対策 https://www.cybozu.com/jp/infrastructure/#infrastructure また、バックアップ時のログにエラーが出力されていないことを日々の業務で確認しています。定期メンテナンス実施日を除き、毎日復元のためのリストアテストを実施しており、きちんと復元できるよう日々の運用でもチェックしています。
	9	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の稼働監視をすること。サービスの停止を検知した場合は、利用者に対して通知すること。	○	稼働状況については監視をしております。 サービスの稼働状況については、cybozu.com 稼働状況サイトにて確認が出来ます。 ▼cybozu.com 稼働状況 https://status.cybozu.com/status/ サービスの停止を検知した場合は、当社のニュースサイトにて連絡を行います。 ▼サイボウズからのお知らせ https://cs.cybozu.co.jp/information/cybozucom/

	10	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の障害監視をすること。障害を検知した場合は、利用者に対して通知すること。	○	機器の状況については監視をしております。 障害が発生した場合は、ログイン後のトップページや弊社のお知らせサイトにて通知します。影響度に応じてメール配信も実施します。 ▼サイボウズからのお知らせ（障害情報） https://cs.cybozu.co.jp/trouble/ ■通知時間 障害通知の目標時間（登録メールアドレスへの第一報）は、原則として障害検知から1時間以内としています。 ※障害の種類によってはその限りではありません。
	11	システムの運用担当者の作業については記録すること。	○	システムの運用担当者の作業についてはすべて記録を残しております。操作ログは改変不可能なかたちで保管されており、保管期間は5年です。 また作業を実施する際には変更管理に則り、作業内容について責任者の承認を得て、2名体制での相互チェックのもと実行します。
	12	例外処理及びセキュリティ事象を記録した監査ログを取得すること。また該当のログのアラートについては定期確認し、改竄、許可されていないアクセスがないように保護する。	○	監査ログについては、日次で該当ログのアラートについて取得をしております。また該当のログについては改ざんできないように保護されています。
	13	クラウドサービス上で取得する利用者の活動、例外処理及びセキュリティ事象を記録した監査ログについて明示すること。また監査ログの保持する期間、提供方法、提供のタイミングについて明示すること。	○	アプリケーションの監査ログの保存期間や保存形式、閲覧は、ご利用者の管理者アカウントにて管理できるようになっております。 当社サービスへのアクセスログに関しては、法令やガイドラインに準拠した形で保存しております。 ※監査ログ機能で提供している以外のログの提供サービスは行っておりません。
	14	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器については正確な時刻源と同期させること。	○	NTP（ntp.nict.jp）を利用して、オペレーティングシステム、ネットワーク機器等、正確な時刻源と時刻同期を実施しております。
	15	クラウド基盤システムへのアクセスについては、各個人に一意な識別子にし、セキュリティに配慮したログオン手順、認証技術によって制御すること。またアクセス制御方針について文書化すること。	○	システムのアカウントについては当社規定に則り、各個人に一意の識別子を付与しております。またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御しております。アカウントや暗号化方針については当社規定にて定めております。
	16	クラウド基盤システムへのアクセス権限の追加・削除・変更について手順を備えること。また特権の割り当て及び利用は制限し、管理すること。	○	システムへのアクセス権限の追加・削除・変更の方法については手順の文書化を行なっております。特権については利用者をcybozu.comシステムの運用管理担当者のみとしております。
	17	システムの運用担当者が利用するパスワードについては管理し、また良質なパスワードにすること。	○	パスワードについては情報セキュリティ規則、情報システム運用マニュアルに則り、管理しております。
	18	クラウド事業者は、クラウド利用者がネットワークサービスの利用に関する方針を策定できるよう、クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。	○	cybozu.comサービスを利用する際の認証方法、アクセス制限の設定について当社ホームページにて明記しております。 ▼ユーザー管理と認証 https://www.cybozu.com/jp/account/
	19	提供するクラウドサービスにおいてアクセス制御機能を提供すること。	○	BASIC認証(無償)、IPアドレス制限(無償)に加え、クライアント証明書（有償）による追加認証やセキュリティ確認コードを用いた二要素認証を設定可能です。 ▼不正アクセスを防止する機能 https://www.cybozu.com/jp/account/#unauthorized_access_prevention
	20	クラウド事業者は、各クラウド利用者に割り当てたコンピューティング資源に、他のクラウド利用者や許可されていないユーザがアクセスできないように管理し、物理的な設定や移行にかかわらず、仮想環境の分離を確実にすることが望ましい。 ネットワーク若しくはインタフェースの分離がなされていない場合、クラウド事業者は、アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。 クラウド事業者は、クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために、クラウド環境における情報セキュリティについて評価を実施することが望ましい。	○	cybozu.com サービスはマルチテナント構成となっております。 登録されたデータについては利用されているお客様以外アクセスできないようにデータベースおよびネットワークの分離やアクセス制限を行っております。 詳しい分離の仕組みは以下にて公開しております。 ▼cybozu.comのマルチテナント構成における論理的分離について https://www.cybozu.com/jp/support/data/cybozucom_multi_tenant.pdf
	21	提供するクラウドサービスにおいて利用者のID登録・削除機能を提供すること。	○	利用者IDの登録・削除の機能を提供しております。
	22	提供するクラウドサービスにおいて特権の割り当て及び利用制限し、管理する機能を提供すること。	○	特権の割り当て等の管理する機能を提供しております。
	23	提供するクラウドサービスにてパスワード管理ができるような機能を提供すること。また良質なパスワードを確実にする機能があること。	○	パスワードの有効期限や文字数、複雑度等を設定する機能を提供しております。
	24	提供するクラウドサービスで提供している情報セキュリティ対策及び機能を列記し、明示すること。	○	提供しているセキュリティ対策及び機能については、当社ホームページにて公開しております。 ▼ユーザー管理と認証 https://www.cybozu.com/jp/account/
	25	一定の使用中断時間が経過したときには、使用が中断しているセッションを遮断すること。またリスクの高い業務用ソフトウェアについては、接続時間の制限を利用すること。	○	セッションの有効期間を設定可能です。初期値は24時間となっております。 ▼cybozu.com ヘルプ > ログインに関するセキュリティ設定の初期値 https://jp.cybozu.help/general/ja/id/02052.html

	26	ネットワークを脅威から保護、またネットワークのセキュリティを維持するためにネットワークを適切に管理し、アクセス制御をすること。	○	セキュリティを維持するためにネットワーク構成の管理、ネットワーク機器監視を実施しております。またアクセス制御についても文書化し、管理・実施しております。
	27	ネットワーク管理者の権限割り当て及び利用は制限し、管理すること。またネットワーク管理者もアクセスを管理するためにセキュリティに配慮したログオン手順、認証技術によって制御すること。	○	ネットワーク管理者の権限については、cybozu.comシステムの運用管理担当者のみとしております。アクセスする際にはVPN網を利用し、またアクセスが許可されていない者がアクセス、ログオンできないように制御しております。アカウントや暗号化方針については当社規定にて定めております。
	28	外部及び内部からの不正なアクセスを防止する装置(ファイアウォール等)を導入すること。また利用することを許可したサービスへのアクセスだけを提供すること。	○	ファイアウォールを導入しております。サービスで利用するポートのみを開放しており、その他のポートについてはアクセスできないように制限しております。
	29	クラウドサービスへの接続方法に応じた認証方法を提供すること。クラウドサービスへの接続方法に応じた認証方法を、クラウドサービスの利用を検討するものに明示すること。	○	提供するクラウドサービスにおいて、提供しているセキュリティ対策及び機能については、当社ホームページにて公開しております。 ▼不正アクセスを防止する機能 https://www.cybozu.com/jp/account/#unauthorized_access_prevention
	30	クラウドサービスの契約が終了した場合にデータが消去されること。消去されるなら、その時期や削除される範囲について確認すること。	○	cybozu.comサービスの契約を終了された場合、契約終了翌日から30日後に、入力データ、ユーザー情報、監査ログを消去します。バックアップデータは各データの消去から2週間程度で完全に消去します。 ただし、契約中の複数サービスのうち一部を解約される場合、解約するサービスの入力データのみを消去します。 ※入力データの暗号化のための暗号鍵は、契約ごとに生成されているものではないため、契約終了翌日から30日後でも消去されません。システム運用担当者による暗号鍵の利用は、顧客データ同様に制限されており、作業内容はすべて記録されているため、不正に利用されることもございません。
	31	クラウドサービスを利用するネットワーク経路が暗号化されていることを確認すること。クラウドサービスで利用する情報がシステム上で暗号化されていること。	○	伝送データおよび入力データは、すべて暗号化しています。 伝送データについては全てSSL通信(TLS1.2、1.3)で暗号化しております。 ▼サービスレベル目標（SLO）セキュリティ https://www.cybozu.com/jp/infrastructure/slo.html 入力データについてはストレージデバイス単位で暗号化されております。 暗号化は、dm-crypt を aes-xts-plain64 方式・512 bit 鍵長で利用しております。 ※入力データの暗号化について、利用者が指定する暗号化方式を採用することや、利用者が独自に暗号化するなどの機能は提供をしていません。また、暗号鍵の管理は弊社責任で実施しており、利用者が暗号鍵の生成・保管・破棄を実施できるような機能は提供しておりません。
7 供給者関係				
	1	外部組織がかかわる業務プロセスから、情報資産に対するリスクを識別し、適切な対策を実施すること。	○	cybozu.com にお客様が登録した情報については、その情報の内容を問わず、最善の注意を持って管理し、別段の定めがある場合を除き、お客様の書面による承諾を得ることなく、本サービス以外の目的のために利用あるいは複製し、または第三者に利用させ、もしくは開示、漏洩いたしません。 なお、当社にて外部組織を利用する場合は、当社規定に則り選定、契約を行います。契約時には、セキュリティ要求事項を含んだ正式な契約書を締結することになっております。 ▼利用規約 15.入力データの取扱い、26.委託 https://www.cybozu.com/jp/terms/ cybozu.com では外部データセンターのハウジングサービスを利用しております。 こちらも上記の規約に則り、正式な契約書を締結しております。
8 情報セキュリティ事象・情報セキュリティインシデント				
	1	すべての従業員は、システムまたはサービスの中で発見したまたは疑いをもったセキュリティ弱点はどのようなものでも記録し、報告するようにすること。	○	情報セキュリティ規則にて、セキュリティ事故の定義、発生時の報告について定めており、またウィルス感染の疑いや利用しているサービスから情報漏えい等の事故があった場合の報告連絡手段、対応手続を定めております。
	2	情報セキュリティインシデントに対する迅速、効果的で毅然とした対応をするために責任体制及び手順書を確立すること。	○	情報セキュリティ規則にて、情報セキュリティインシデントに対応するため、報告連絡手段、対応手続を定めております。 クラウドサービスに関する情報セキュリティインシデントに対応するため、CSIRTを設立しております。 責任体制はISMSマニュアルにて、情報セキュリティ組織を整備しております。インシデントの対応手順は、当社ホームページ上に公開している CSIRT記述書にて、運用体制と活動プロセスを明記し、さらに、ISMSマニュアルにて、システム障害、機密漏洩、被害等、人的誤りを含む情報セキュリティ上のインシデントは、適切な連絡経路を通してできるだけ速やかに報告し、組織全体にわたって管理を行うことを明記しております。 ▼CSIRT記述書 https://www.cybozu.com/jp/productsecurity/management/cysirt.html

	3	情報セキュリティインシデントの報告をまとめ、定期的にクラウド利用者に明示すること。	○	CSIRTを設け、窓口・対応・関係者への連絡を実施しております。但し、定期的な明示はしておりません。脆弱性が発見された場合は、その都度公的機関(JPCERT)、自社Webページなどを利用してクラウド利用者に情報を明示しています。 cybozu.com や各サービスのメンテナンスやアップデート、インシデント情報を、「cybozu.com お知らせ一覧」に公開しています。 ▼サイボウズからのお知らせ https://cs.cybozu.co.jp/cybozucom/ また、cybozu.com 共通管理者及びサイボウズドットコムストア管理者のメールアドレスにも一部の情報をお知らせしています。配信内容に関しましては製品ヘルプページをご覧ください。 ▼cybozu.com ヘルプ > メール配信の内容 https://jp.cybozu.help/s/ja/id/050106.html
9 事業継続マネジメントにおける情報セキュリティの側面				
	1	業務プロセスの中断を引き起こし得る事象は、中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに特定すること。	○	事業継続計画書の中で事業継続リスク分析及びビジネスインパクト分析をおこなっております。その中で各業務プロセスの中断発生確率、復旧許容時間から優先度を定め、要求されたレベルで時間で復旧できるように事業継続計画書・事業継続計画手順書を作成しております。
	2	クラウド事業者は，クラウドサービスを提供するシステムの冗長化を図るとともに、クラウドサービスの冗長化の状況を、クラウドサービスの利用を検討する者に明示することが望ましい。	○	全てのサーバー、ネットワーク、ストレージ、データについて冗長化を実施しております。
	3	事業継続計画については定期的に試験・更新すること。	○	事業継続計画書を作成し、定期的に試験及び見直しを行なっております。
	4	クラウドサービス提供に用いる機材は、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	○	クラウドサービス提供に用いる機材は全てデータセンターに設置しており、停電・電力障害が発生した場合も電力が供給されるようになっております。
	5	クラウドサービス提供に用いる機材を設置する部屋には、火災検知・通報システム及び消火設備を用意すること。	○	クラウドサービス提供に用いる機材は全てデータセンターに設置しており、火災検知・通報システム及び消火設備を用意しております。
10 順守				
	1	関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取り組み方を明確に定め、文書化し、維持すること。また重要な記録については消失、破壊及び改ざんから保護し、適切に管理すること。	○	ISMSに影響を及ぼす可能性のある変更(関連する法令、国の定める指針その他の規範と改正状況を反映した資源、組織、規定、規格の変更)は、ISMSの中で、確認されることになっております。 ISMSに作成・利用される文書・記録は、文書ごとに、管理者、承認者、保管期間を定め、適切に管理しております。
	2	クラウド事業者は，クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及び クラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項を明示することが望ましい。	○	cybozu.comサービスは東日本のデータセンターで運用し、西日本のデータセンターにバックアップデータを保管しています。 また当社ホームページ上に公開している利用規約において、準拠法および裁判管轄について定めております。 ▼利用規約27.準拠法・裁判管轄 https://www.cybozu.com/jp/terms/
	3	クラウド事業者は、自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知することが望ましい	○	当社ホームページ上に公開している利用規約において、知的財産権について利用を許諾する範囲を定めております。 ▼利用規約22.知的財産権等 https://www.cybozu.com/jp/terms/
	4	認可されていない目的のための情報処理施設の利用は阻止すること。	○	情報セキュリティ規則にて、物理的境界及びその他の各境界へのアクセスが許可される者について定めており、アクセス許可がされていない者はアクセスできないように制限をかけております。またアクセス許可判断方針についても定めております。
	5	個人データ及び個人情報は、関連する法令、規制、及び適用がある場合には、契約事項の中の要求にしたがって確実に保護すること。	○	当社ホームページ上に公開している利用規約に従って取り扱っております。 ▼利用規約 https://www.cybozu.com/jp/terms/
	6	クラウド事業者は、独立したレビュー及び評価（例えば、内部／外部監査、認証、脆弱性、ペネトレーションテストなど）を定期的に実施し、情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。 また、クラウド事業者は、クラウド利用者の個別の監査要求に応える代わりに、クラウド利用者との合意に基づき、 独立したレビュー及び評価の結果を提供することが望ましい。	○	弊社担当部門によるレビュー、テストを実施しております。 また、第三者機関による外部セキュリティ監査も実施しております。 プラットフォーム、アプリケーション共に1回/年以上の実施となり、アップデート内容に応じて実施しております。 脆弱性の監査結果は、当社ホームページにて公開しております。 ▼安全性への取り組み https://www.cybozu.com/jp/productsecurity/ お客様自身での脆弱性検証も可能です。 検証用環境をご提供いたしておりますのでそちらをご活用ください。 詳しくは、以下の当社ホームページをご確認ください。 ▼脆弱性検証環境提供プログラム https://cybozu.co.jp/products/testing-environment/ ※本番環境での脆弱性検証は他のお客様に影響が出る恐れがありますので、お控えください。
11 その他				
	1	記録媒体(書類、記録メディア)の保管管理については適切に行うこと。また廃棄する際には記録された情報を復元できないように安全に処分すること。また再利用の際には機密情報の漏えい等につながらないように対処すること。	○	情報セキュリティ規則にて、記録媒体の情報取扱方法（保管、廃棄）を定め、適切に取り扱っております。
	2	重要な情報資産については、机の上に放置せず安全な場所に保管すること（クリアデスク）。また離席時には情報を盗み見られないように情報端末の画面をロックすること(クリアスクリーン)。	○	情報セキュリティ規則にて、クリアデスク（重要な情報資産は、作業終了時には、施錠されたキャビネット、引出しに保管）と離席する場合は、第三者が容易に操作及び閲覧ができないようスクリーンロック等の対策を講じるよう定め、実施しております。

	3	従業員のパソコンにウィルス対策を行うこと。また技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	情報セキュリティ規則にて、クライアントPCに関する利用者の遵守事項（ウィルス対策等）を定め、遵守しております。 技術的脆弱性に関する情報は、ウィルス、スパイウエア、技術的脆弱性等への対策について、情報収集と情報周知を実施しております。
	4	サービス提供を終了する場合は、利用者に対して事前に通知を行うこと。	○	当該廃止予定日より3ヶ月以上前に、弊社が提供する手段により通知するものとします。 ▼利用規約18.サービスの廃止 https://www.cybozu.com/jp/terms/
	5	サービス提供にあたって役割分担および責任範囲を明示していること。	○	cybozu.com提供の各サービスに関する責任分界点については、以下をご確認ください。 ▼cybozu.comに関する責任分界点 https://www.cybozu.com/jp/support/data/cybozucom_boundary.pdf
	6	情報のラベル付けをする機能が提供されていること。	○	各サービスの機能詳細に関しては、マニュアルを公開しています。 ▼サイボウズ　マニュアルサイト https://manual.cybozu.co.jp/ 情報ごとにタイトルを付与したり、アクセス権を設定するなど、お客様の情報資産の分類にご利用いただける機能となっております。
	7	IPv6の対応についての情報が提供されていること。	※	IPv6には対応しておりません。