株式会社マクロミル 標準セキュリティチェックシート

参考資料
ISO/IEC 27001:2022 詳細管理策
総務省「クラウドサービスの安全・信頼性に係る情報開示指針(平成29年3月改訂版)」

株式会社マクロミル 情報セキュリティ部
最終更新日：2024年5月27日

No.	情報開示項目				詳細
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）		2024年5月27日
情報セキュリティにかかわる第三者認証の取得					
2	ISMS認証を取得しているか			○	認証番号：IS 782383 有効期限：2026年06月05日
3	プライバシーマークを取得しているか			○	登録番号：12390042(10) 有効期限：2024年6月30日
情報セキュリティのための方針					
4	情報セキュリティおよび個人情報保護について基本方針を定め、管理層が承認し、それらの方針を組織の内外へ周知しているか。			○	ホームページにて公開している。 プライバシーポリシー：https://www.macromill.com/privacy.html 情報セキュリティポリシー：https://www.macromill.com/security.html
5	情報セキュリティおよび個人情報保護に関する基本方針は、あらかじめ定めた間隔で、及び重大な変化が発生した場合に見直しを行い、組織の状況に応じた最新の情報セキュリティ基本方針として維持しているか。			○	社内規程に則って適宜必要に応じて見直しを行い、組織の状況に応じた最新の状態の情報セキュリティ基本方針として維持されている。
情報セキュリティのための組織					
6	情報セキュリティ管理の責任者を定め、職務範囲や権限、責任について定めているか。			○	社内規程にて定めている。
7	相反する職務と責任を分離し、不注意又は故意による情報資産の不正使用のリスクを軽減しているか。			○	社内規程に職務と責任の分離について定め、対応している。
8	スマートフォンやタブレット端末などモバイル機器の取扱いルールを定め、セキュリティ対策を講じているか。			○	社内規程に定め、対策を講じている。
9	テレワーク（社外での業務）に関するルールを定め、セキュリティ対策を講じているか。			○	社内規程に定め、対策を講じている。
人的資源のセキュリティ					
10	従業員に対して、退職後も有効な秘密保持契約(NDA)を取り交わすなどにより、情報セキュリティに関する就業上の義務を明確にしているか。 また、情報セキュリティに関する方針やルールに違反した従業者に対する懲戒手続が規定されているか。			○	入社時に退職後も加味した誓約書及び従業者個人情報の取扱いについて書面で提出させている。また、違反した場合の懲戒に関しても社内規程により定められている。
11	従業員に対して、情報セキュリティに関する教育や訓練を定期的に実施しているか。			○	入社時研修及び年１回以上の定期研修を実施している。
12	従業員の退職または異動時における、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手順を明確にしているか。			○	社内ルールを定め、ルールに準じて適宜対応を行っている。
情報資産の管理					
13	管理責任者を明確にした情報資産の目録を作成し、定期的に更新を行っているか。また、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しているか。			○	取り扱う情報資産は社内で定めた規定に準じて分類され、ISMSの計画に則って情報資産管理台帳を作成、定期的に更新を行っている。
14	USBや外付けハードディスク等の外部記憶媒体の利用・持ち出し関して、盗難や紛失を想定したセキュリティ対策を含めてルールを定め、取得・使用・移送・廃棄のライフサイクルを通して管理しているか。			○	外部記憶媒体の利用等は社内ルールを定めてルールに準して行われている。取り扱う情報資産も取得～廃棄に関し規程を定められており、規程に準じて対応している。
15	PCや紙媒体の物理的な情報資産が不要になった場合の、処分ルールについて定めているか。			○	社内規程にて定め、規程に準じて処理を行っている。

アクセス制御			
16	顧客情報等の重要な情報へのアクセス権限を設定し、定期的及び、従業員の退職異動時などに見直しを実施しているか。また、ソフトウェアやサービスの利用を管理するためのルールについて定めているか。	○	社内ルールを定め、ルールに準じて適宜対応を行っている。ソフトウェア、サービスの管理ルールも定められている。
17	情報資産（システム、アプリケーション、サービスなど）にアクセスする際の利用者の認証は、セキュリティを保った認証技術及び手順を採用しているか（多要素認証の採用、不正利用を抑止するログオン手続き、利用場所の限定、パスワードルール　など）	○	社内ルールを定め、ルールに準じて対応を行っている。
18	特権的アクセス権の割り当て及び利用は、制限し、管理しているか。	○	特権アクセス権に関しては必要な者のみに限定し、管理されている状態である。
暗号の利用			
19	情報資産保護のための暗号化に関する利用方針を定め、暗号鍵の管理を含むルールを定め、実施しているか。	○	方針を定め、それに準じて実施している。
物理的及び環境的セキュリティ			
20	業務スペースでは、来客者が出入りできるエリアと従業者だけが出入りできるエリアを区別しているか。 また、業務スペースでは、従業者だけが出入りできるエリアに従業者以外が勝手に入ることができないよう、入退管理対策を行っているか。	○	業務スペースは社内規程にて区分について定められており、入退室システムの利用等対策を行っている。
21	ネットワーク機器などの装置は安定した場所に設置する等、破損等の危険性及び災害からのリスクや認可されていないアクセスの機会を低減せるように保護を実施しているか。	○	社内ルールを定め、ルールに則って実施されている。
22	机上は常に整理し、書類や取り外し可能な記憶媒体を放置しないなど、クリアデスクのルールを定め、従業員にルール遵守の徹底を図っているか。	○	社内ルールを定め、ルールに則って実施されている。
23	パスワード付きスクリーンセーバーの設定や手動画面ロックの実施など、クリアスクリーンのルールを定め、従業員にルール遵守の徹底を図っているか。	○	社内ルールを定め、ルールに則って実施されている。
運用のセキュリティ			
24	システムや機器などの操作マニュアルは、必要な情報セキュリティ対策を反映して作成されており、必要とするすべての利用者に対して利用可能な状態となっているか。	○	システム等のマニュアルは、情報セキュリティ対策を反映したものとなっており、利用者がいつでも閲覧ができる状態になっている。
25	ウイルス対策ソフトの自動更新設定や、OS・アプリケーションのアップデートなどのマルウェア対策を実施しているか。	○	社内ルールを定め、ルールに則って実施されている。
26	データバックアップのルールについて定めているか。	○	社内ルールが定められている。
27	アクセスログや操作ログを取得、定期的な確認、適切に管理・保護しているか。	○	社内ルールを定め、ルールに準じて行われている。
通信ネットワークのセキュリティ			
28	重要な情報が通信ネットワークを流れる場合は、ネットワーク経路上での情報漏えいを防止するために、情報の暗号化などの保護措置を実施しているか（SSLによる暗号化　など）	○	社内ルールを定め、ルールに則って実施されている。
29	社外との情報交換に関して、情報保護のための技術的対策及び手順、ルールを定め、従業員に周知徹底を図っているか（電子メール、ファイル交換、チャット　など）	○	社内ルールを定め周知されており、ルールに則った利用が行われている。
システムの取得、開発及び保守			
30	システムの要件定義及び設計、開発の各フェーズにおいて、情報セキュリティに関する要件を含めており、各フェーズごとに要件を満たしていることをテストしているか。	○	社内規程にて定め、規程に準じて処理を行っている。
31	情報セキュリティに配慮した開発方針やコーディング規約は整備されているか。	○	コーティング規約を作成しており、整備されている状態にある。
32	システムに変更に伴う情報セキュリティ上のリスクに対応するために、変更管理手順を定め、実施しているか。	○	手順等定められており、それに則って実施している。
業務委託先の管理			
33	業務委託先の選定における、情報セキュリティに関する選定条件を定め、その選定条件に準じて委託先を選定しているか。 また、委託先を一覧化して管理し、委託先のセキュリティ状況を定期的に確認し、必要な是正措置および改善を指示しているか。	○	社内ルールにて定め、ルールに準じて選定されている。委託先は一覧化され、ISMSの計画に則りセキュリティ状況のチェックを行っている。
34	業務委託先とは、情報セキュリティや秘密保持に関する契約を締結しているか。	○	社内規程に則って秘密保持に関する契約を締結している。
情報セキュリティインシデント管理			
35	情報セキュリティインシデントが発生した場合の、社内および社外に対する報告や公開の手段と手順を定め、関係者に周知しているか。	○	社内規程にて定められ、関係者への周知を行っている。
事業継続マネジメントにおける情報セキュリティ			
36	災害や停電など業務の中断を引き起こし得る事象が発生した場合に備えて、情報セキュリティを考慮した事業継続計画を立案し、定期的に試験・更新を行っているか。	○	規程を定め、それに準じて計画を行っている。立案された計画は定期的にテストを行い、必要と判断されれば適宜改訂を行っている。
遵守			
37	情報セキュリティに関連する法令・規制・ガイドライン等を特定し、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、最新に保っているか。	○	関連する法令・規制・ガイドライン等は特定され、ISMSの計画に則り定期的に最新の状態になるよう更新を行っている。

サービス基本特性				詳細		
				OpenMill/QuickMill	OrderMill	AIRsMEMBERS/Myリスト
38	サービス内容	サービス名称	本ASP・SaaSのサービス名称	QuickMill・OpenMill	OrderMill	AIRsMEMBERS/Myリスト
39		サービス開始時期	本ASP・SaaSのサービス開始年月日（西暦）	2000年8月	2003年 6月	2009年2月24日
			サービス開始から申請時までの間の大規模な改変等の有無	有り（2006年3月）	有り（2015年4月）	インフラ基盤の刷新（2017年1月）
40		サービスの内容・範囲	本ASP・SaaSのサービスの内容・特徴	インターネットリサーチサービス	インターネットリサーチサービス	セルフアンケートツール
			他の事業者との間で行っているサービス連携の有無と、「有り」の場合はその内容	有り（サービス事業者とパネル情報等の連携を行っている）	有り（サービス事業者とパネル情報等の連携を行っている）	有り（サービス事業者との連携等を行っている）
41		サービス提供時間	サービスの提供時間帯	24時間365日(定期メンテナンス等の計画停止を除く)	24時間365日(定期メンテナンス等の計画停止を除く)	24時間365日(定期メンテナンス等の計画停止を除く)
42		サービスのカスタマイズ範囲	アプリケーションのカスタマイズの範囲	不可	契約内容に依存	不可
43		移行支援	本サービスを利用する際における既存システムからの移行支援の有無 （契約内容に依存する場合はその旨記述）	無し	無し	無し
44	契約の終了等	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	情報の削除は可能（一定期間で自動削除）	情報の削除は可能（要望に応じる）	データベースをドロップ、環境を物理削除
			削除又は廃棄したことの証明書等の提供	廃棄証明書を提供（オプション）	廃棄証明書を提供（オプション）	廃棄証明書を提供（オプション）
45	サービス品質	サービスパフォーマンスの管理	システムリソース不足等による応答速度の低下の検知の有無	サービスレスポンス速度などのパフォーマンスと、 システムインフラのキャパシティ管理を行っている。	サービスレスポンス速度などのパフォーマンスと、 システムインフラのキャパシティ管理を行っている。	サービスレスポンス速度などのパフォーマンスと、 システムインフラのキャパシティ管理を行っている。
46		脆弱性診断	脆弱性診断の有無	有り（アプリケーション診断・プラットフォーム診断）	有り（アプリケーション診断・プラットフォーム診断）	有り（アプリケーション診断・プラットフォーム診断）
47		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	利用者データをサービス特性にあわせて複数世代バックアップしている。	利用者データをサービス特性にあわせて複数世代バックアップしている。	利用者データをサービス特性にあわせて複数世代バックアップしている。
48		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）	サービスの特性にあわせてシステムの冗長化と負荷分散を行っている。	サービスの特性にあわせてシステムの冗長化と負荷分散を行っている。	サービスの特性にあわせてシステムの冗長化と負荷分散を行っている。
49	セキュリティ	死活監視	死活監視の有無と、「有り」の場合は死活監視の対象	有り（サーバー・DB・URL）	有り（サーバー・DB・URL）	有り（サーバー・DB・URL）
50		時刻同期	時刻同期への対応の有無	有り（NTP）	有り（NTP）	有り（NTP）
51		ウイルス対策	ウイルス対策の有無	有り	有り	有り
52		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	有り	有り
53		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	有り	有り	有り
54		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、その保存期間及び利用者への提供可否	利用者の利用状況およびシステム運用に関するログを記録している。ログの改ざん防止措置を行っている。 ※保管期間1年、利用者への提供は不可	利用者の利用状況およびシステム運用に関するログを記録している。ログの改ざん防止措置を行っている。 ※保管期間1年、利用者への提供は不可	利用者の利用状況およびシステム運用に関するログを記録している。ログの改ざん防止措置を行っている。 ※保管期間1年、利用者への提供は不可
55		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	セキュリティパッチに含まれる脆弱性のリスク度合いと緊急度を評価し、計画的にパッチ適用を行っている。	セキュリティパッチに含まれる脆弱性のリスク度合いと緊急度を評価し、計画的にパッチ適用を行っている。	セキュリティパッチに含まれる脆弱性のリスク度合いと緊急度を評価し、計画的にパッチ適用を行っている。
ネットワーク				**OpenMill/QuickMill**	**OrderMill**	**AIRsMEMBERS/Myリスト**
56	センター側ネットワーク	回線	専用線（VPNを含む）、インターネット等の回線の種類	インターネット回線	インターネット回線	インターネット回線
57	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	有り	有り
58		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	有（対応は非開示）	有（対応は非開示）	有（対応は非開示）
59		ユーザ認証	ユーザ（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	ID/パスワードによる認証	ID/パスワードによる認証	ID/パスワードによる認証
60		なりすまし対策（事業者サイド）	第三者によるなりすましサイトに関する対策の実施の有無	有り（方法は非開示）	有り（方法は非開示）	有り（方法は非開示）
61		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（SSL暗号化）	有り（SSL暗号化）	有り（SSL暗号化）
62		その他セキュリティ対策	その他特筆すべきセキュリティ対策を記述（情報漏洩対策等）	ISMS（ISO/IEC27001:2022)に基づき、 組織的・人的・物理的・技術的な管理策を網羅的に実施している。	ISMS（ISO/IEC27001:2022)に基づき、 組織的・人的・物理的・技術的な管理策を網羅的に実施している。	ISMS（ISO/IEC27001:2022)に基づき、 組織的・人的・物理的・技術的な管理策を網羅的に実施している。
63	ＰＣ側ネットワーク	推奨回線	専用線（VPNを含む）、インターネット等の回線の種類	インターネット回線	インターネット回線	インターネット回線
端末				**OpenMill/QuickMill**	**OrderMill**	**AIRsMEMBERS/Myリスト**
64	ＰＣ等（操作端末）	推奨端末	パソコン、スマホ、タブレット、シンクライアント等の端末の種類、OS等	推奨環境については、下記のURLを参照。 https://www.macromill.com/requirements.html	推奨環境については、下記のURLを参照 https://www.macromill.com/requirements.html	推奨環境については、下記のURLを参照 https://www.net-research.jp/enq/recommendationBrowser.html
サービスサポート				**OpenMill/QuickMill**	**OrderMill**	**AIRsMEMBERS/Myリスト**
65	サービス通知・報告 インシデント対応	メンテナンス等の一時的サービス停止時の事前告知	利用者への告知時期（1ヵ月前、3ヵ月前、6ヵ月前、12ヵ月前等の単位で記述）	2か月前	2か月前	2か月前
			告知方法	メール	メール	メール
66		障害・災害発生時の通知	障害発生時通知の有無と、「有り」の場合は通知方法及び利用者への通知時間	有り（状況に応じて弊社営業からメールにて通知）	有り（状況に応じて弊社営業からメールにて通知）	有り（状況に応じて弊社営業からメールにて通知）
67		セキュリティ・インシデント対応	セキュリティに関するインシデントが発生した場合の対応 （通知、被害の拡大防止、暫定対処、本格対処など）	弊社の社内規程である情報セキュリティインシデント細則に沿って対応を行い、影響のあったお客様や関係者へ通知を行い、必要な対処に関して連携を行う	弊社の社内規程である情報セキュリティインシデント細則に沿って対応を行い、影響のあったお客様や関係者へ通知を行い、必要な対処に関して連携を行う	弊社の社内規程である情報セキュリティインシデント細則に沿って対応を行い、影響のあったお客様や関係者へ通知を行い、必要な対処に関して連携を行う