Ver202203-01

メルコル　クラウド基盤

（セキュリティガイド）

タワーハートソリューションズ株式会社

■メルコル　サービスセキュリティ項目①　【センター・設備】

本資料は2022年3月時点の情報に基づきます。
本資料は予告なく変更修正されます。

データセンター【Microsoft Azure】

メルコルは、Microsoft社のAzureプラットフォーム上で稼働しており、自社にサービスで利用するサーバは設置しておりません。
下記解答で該当部分にはMicrosoft社のAzure管理内容で解答させて頂いております。

Microsoft Azureのデータセンターや提供サービスに関する情報は、下記公開資料等をもとに作成しております。記載内容の確認や、より詳細な情報確認などは、下記情報等をご確認ください。
『Request for Information (情報提供依頼書) に対する標準的なレスポンス セキュリティおよびプライバシー』
https://www.microsoft.com/ja-jp/download/details.aspx?id=26647
また、金融機関企業様むけには、下記の対応状況資料が公開されています。
『「金融機関等コンピュータ システムの安全対策基準 (第 9 版)」に対する
マイクロソフト クラウド サービス (Microsoft Azure、Office 365、Dynamics 365) の対応状況』
https://cloudblogs.microsoft.com/industry-blog/ja-jp/financial-services/2018/05/11/fisc_v9/

データセンター建屋等		
1	データセンターの所在地はどこですか？	Microsoft Azure　メイン：東日本リージョン（東京・さいたま）　　バックアップ ：西日本リージョン（大阪）
2	データセンター専用建物ですか？ （耐震・免震構造など）	施設の所在地、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、地震活動を含む地域のあらゆる事象の影響を受けにくいように設計されています。影響回避にはラックレベルでの分離による免震も含まれます。
3	給電ルートは冗長化されていますか？	異なる系統からの電源供給が確保されています。
4	無停電電源（UPS）や、非常用電源の用意はありますか？	データ センターには、専用の 24 時間年中無休で稼働する無停電電源装置 (UPS) および緊急電源サポート (発電機など) が装備されています。
5	火災感知・報知システムはありますか？	すべてのデータ センターに火災検知および抑制システムが存在します。また、データ センター内のさまざまな場所に可搬式消火器が設置されています。施設および環境保護機器について、定期的な保守が行われています。
6	不正侵入対策はされていますか？	主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。
データセンター　マシンルーム等		
7	サーバーマシンルームとオペレーションルームが分離されていますでしょうか	適切なアクセスコントロールが保証されるように設計され、実施されます。
8	入退室管理はされていますか？	主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されています。
9	入退室記録は保存されていますか？保管期間は？	記録は保存されています。保管期間は非公開となっています。
10	社員証やバッチなどにより、構内従業者と訪問者の区別は外見から行えるような措置が取られていますか？	職員は常に ID バッジを着用する必要があり、バッジを着用していない人物の身元を確認したり報告を行ったりする必要があります。すべてのゲストは、ゲスト バッジを着用し、権限を与えられた従業員によってエスコートされる必要があります。
11	サーバールーム内を監視するカメラ設備はありますか？	カメラが設置され、記録されます。
12	映像記録の保存期間は？	記録の保管期間は非公開となっています。
13	撮影機能を持つ機器(カメラ付き携帯電話を含む)の持ち込みは禁止または制限されていますか？	ノート PC、携帯電話、携帯情報端末 (PDA) などのポータブルおよびモバイル デバイスの使用が管理者によって承認されている場合を除き、運用環境で使用することはできません。
14	十分な空調設備は備わっていますか？	冷暖房、換気、空調 (HVAC) システム。データ センター内の空間温度と湿度、空間の与圧、外部の空気の取り入れを管理および監視しています。
15	サーバルーム内消火設備はありますか？	すべてのデータ センターに火災検知および抑制システムが存在します。また、データ センター内のさまざまな場所に可搬式消火器が設置されています。施設および環境保護機器について、定期的な保守が行われています。
データセンター　その他		
16	第三者セキュリティ認証は何を取得していますか？	ISO/IEC27001:2013 を取得しております。
17	ユーザ企業の監査の受け入れの可能ですか？	データセンターの立ち入り監査は認められていません。

安全管理措置		
ファイアウォール		
18	インターネットとの境界にファイアウォールが設置されていますか？	Azure　Paas Faasを利用している為、該当しません。
19	必要な通信ポートのみに制限されていますか？	SSL（TLS）通信のみが許可されています。
その他のサーバーシステムのセキュリティ対策		
20	サーバーに対するウィルス対策や不正アクセスなどに対する対策は施されていますか？	Azure Security Center を導入
21	OSのセキュリティパッチの適用を実施していますか？	潜在的な脆弱性と最新のソフトウェア更新プログラムは、自動的に適用されます。

22	ソフトウェアのセキュリティパッチの適用を実施していますか？	潜在的な脆弱性と最新のソフトウェア更新プログラムは、自動的に適用されます。
23	不正アクセスに対する防御および監視を実施していますか？	Azure Security Center を導入
24	各種脆弱性攻撃への対策は行っていますか？	Azure DDoS Protectionを導入
25	脆弱性診断を実施していますか？	実施しています。
通信		
26	通信の安全性は実装されていますか？	HTTPS（443）/　SSL（TLS）　通信のみが許可されています。
障害対策（※バックアップについては、　②組織・運用管理　を参照してください。）		
27	システム機器は冗長化されていますか？	すべて冗長化されています。
28	障害を監視していますか？	監視しています。
29	障害発生時に通知はされますか？またその手段は？	障害発生時には迅速に、メールおよび自社WEBページを通じて告知を行います。 （※弊社サポート時間での対応となります。）

■メルコル　サービスセキュリティ項目②　【組織・運用管理】

本資料は2022年3月時点の情報に基づきます。
本資料は予告なく変更修正されます。

安全管理措置		
組織体制・ルール		
1	公的機関による資格や認証を受けていますか？	ISO/IEC27001:2013 を取得しております。
2	情報セキュリティ又は個人情報管理に関する社内規程は制定していますか？	情報セキュリティポリシーや、個人情報保護に関する社内ルールが制定されています。
3	システム運用部門と独立した社内の内部管理部門による監査が定例的に実施されていますか？	実施しています。（年1回、変更時
人的安全管理措置		
4	情報セキュリティに関する責任者は任命されていますか？	任命しております。
5	個人情報管理責任者、個人情報管理担当者は任命されていますか？	任命しております。
6	インシデント発生時の管理組織は存在しますか？	存在します。ISMS事務局
7	ビジネス継続の手順は整備されていますか？	災害復旧手順が整備され、年1回のテストを実施します。
8	就業規則などで、秘密保持義務を規定した条項が設けられていますか？	雇用期間中の秘密情報の扱いや、退職時にも秘密として取り扱う旨を規定しています。
9	従業員に対して、情報セキュリティ及び個人情報管理に関する教育は定期的に実施していますか？	全従業員もれなく、年1回、e-Learningやペーパー資料にて実施しています。
10	情報システム機器に関する、資産管理、持ち出し、持込み管理、廃棄など行われていますか？	情報機器の棚卸、持ち出し可能デバイスの許可承認、紛失時の漏洩対策としてPCパスワード、重要文書の暗号化、情報書類のシュレッダー廃棄、廃棄PCのクリーンナップなどを実施しています。
システム運用・管理体制		
運用組織		
11	運用管理組織は構成されていますか？	本サービスの運用管理を実施する専門チームを設立し、１名以上の運用責任者を設置します。
12	運用管理規程の整備はされていますか？	運用管理規程を作成し、運用責任者、運用担当者は本規程に則って本サービスを運営します。
13	運用管理規程の定期的にみなおされていますか？	運用管理規程は定期的にその有効性を評価し、必要に応じて見直し、改善を実施します。
14	運用管理組織メンバーに対して、専門の教育は実施されていますか？	運用メンバーに対して、年1回運用管理における必要な教育を実施しています。
運用エリア		
15	他の作業エリアと区分けされていますか？	専用のオペレーションルームでの作業となります。
16	入退の制限はされていますか？	施錠ロックにより、許可者のみが入退可能としています。
17	入退可能者リストは管理されていますか？また定期的な見直しはされていますか？	入退出可能リストの定期的な（年間1回および作業員変更時）管理を実施しています。
18	入退室の記録は取得されていますか。また保管期間は決められていますか？	入退室の記録は保存され管理されます。（保管期間3か月）
情報機器		
19	PC端末は専用機ですか？	運用専用端末となります。

20	端末のセキュリティ管理は万全ですか？	ウイルス対策、定期的なシステム更新などを行います。
21	他のエリアからの接続を制限するファイヤーウォールはありますか？	他のエリアからネットワークは分離されております。 また、社外ネットワークとの境界にファイヤーウォールを設置しています。
22	ワイヤレスネットワークは有効ですか？	ワイヤレスネットワークは利用できません。ワイヤレス機能がない端末を利用します。
23	外部記憶装置の利用はありますか？	ありません。USB端子による外部媒体の接続は利用禁止としています。
運用アカウントと特権アカウント管理		
24	運用アカウントの管理ポリシーはありますか？	規定されています。
25	定期的な運用、特権アカウントの棚卸はしていますか？	実施しています。
26	特権アカウントの付与範囲を最小化していますか？	運用管理メンバー利用時には、承認によるパスワード開示が必要です。
27	運用、特権アカウントのパスワードポリシーはありますか？	規定されています。 ※セキュリティ上、ポリシー内容は開示しておりません。
監査		
28	情報管理が適切に実施されていることを、定期的に監査していますか？	ＩＳＯ内部監査委員により、年1回監査を行っています。
29	ユーザ企業の監査の受け入れの可能ですか？	弊社は立ち入り監査には対応しておりません。
運用監視・障害対策		
監視		
30	サーバシステム等の稼働状態を監視していますか。	本サービスの死活監視、パフォーマンス監視、ログ監視を、24時間365日行っています。
ログ管理（システム運用） （※サービス利用に関するログ管理については ③サービス を参照してください。）		
31	顧客の利用者アカウントによる操作を記録していますか？	記録しています。
32	特権・運用アカウントによる操作を記録していますか？	自動的に記録しています。
33	特権・運用アカウントによる操作は、後日追跡できるようになっていますか？	IDの一意性はシステム上確保されています。 アクセスログはIDと紐づけられ、追跡可能です。
34	利用システムのシステムログは記録されていますか？	WAFやIISやSQLなどのシステムコンポーネントのログは自動的に記録されています。
35	取得したログは適切に保護していますか。	ログデータへのアクセスコントロールおよび監視を行っています。
36	ログの信ぴょう性維持のため、サーバーの時刻同期は正しく行われていますか？	データセンター事業者（Microsoft Azure）側にて対応実施しています。
障害・インシデント（事故・事件）対応		
37	障害、事故・事件が発生した場合の報告・連絡体制を整備していますか？	整備しています。
38	障害、事故・事件が発生した場合、迅速に告知されますか？	弊社にて障害発生を確認後、速やかに当社ホームページ、または電子メール等にて通知します。（土曜・日曜・祝日および年末年始を除く）
39	特権・運用アカウントによる操作は、後日追跡できるようになっていますか？	アクセスログは電話発信番号と紐づけられ、追跡可能です。
バックアップ保守 （※データセンター設備の障害対策について ①センター設備 を参照してください。）		
40	データバックアップは行っていますか？	バックアップは日々実施しています。
41	バックアップデータは遠隔地のデータセンターに保管されていますか？	メインサイトの東日本データセンターで取得されたバックアップの複製が西日本データセンターにも保管されます。

■メルコル　サービスセキュリティ項目③　【サービス】

本資料は2022年3月時点の情報に基づきます。
本資料は予告なく変更修正されます。

サービス利用		
利用性		
1	サービス提供時間は？	24時間365日です。（メンテナンス時間は除く）
2	サービス稼働率は？	ＳＬＡ：99.87%以上 （メンテナンス時間は除く） 詳細はＳＬＡに定義しております。 https://www.melucolu.com/kiyaku/SLA.pdf
サポート		
3	問い合わせ対応時間は？	受付窓口設置されているます。 ・フリープラン、スーパーライトプラン：ＷＥＢフォームより受付 ・ビジネスライト、ビジネスプラン、通常のパートナープラン： サービス時間：平日9時～18時、電話にて受付 ・パートナープラン24サービス契約会社：24時間365日、電話にて受付

サービスの終了		
4	サービス終了時する場合の告知体制はどうなっていますか？	サービス終了の３ヶ月前までに、電子メール及び当社Ｗｅｂサイトにて告知いたします。
セキュリティ保護機能		
認証管理		
5	利用者の認証機能はありますか？	ID、パスワードにて認証されます。
6	ログイン失敗時のメッセージや、エラーなどからパスワードが推測されない処置はされていますか？	エラーメッセージにはアカウント名・パスワードおよびそれを推測できる情報は記載されません。
7	ログアウトの忘れなどの防止対策機能はありますか？	ありません。
ログ管理（サービス利用）（システム運用に関するログ管理については　②組織・運用管理　を参照してください。）		
8	ログのアクセス制御はできますか？	ログは当サービスの管理者権限を持つユーザーのみ参照できるよう制限しています。
9	ログは一定期間保管できますか？	ログは過去１年分を保持します。
10	ログの信ぴょう性維持のため、サーバーの時刻同期は正しく行われていますか？	データセンター事業者（Microsoft Azure）側にて対応実施しています。