(a)経産省 2010年8月発行 クラウドサービスレベルのチェックリスト（原文そのまま）										
No.	種別	サービスレベル項目例	規定内容	測定単位	サービス名					備考
事業者に確認すべき項目			確認すべき項目の内容	事業者に求める回答の単位	Mailセキュリティ･オンプレミス 添付ファイルダウンロードリンク化オプション	Mailセキュリティ･クラウド プレミアム／ベーシック			Outbound Security for Microsoft 365	
						MailFilter on Cloud	MailConvert on Cloud	MailArchive on Cloud		
アプリケーション運用										
1	可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24時間365日（計画停止／定期保守を除く）	24時間365日（計画停止／定期保守を除く）	24時間365日（計画停止／定期保守を除く）	24時間365日（計画停止／定期保守を除く）	24時間365日（計画停止／定期保守を除く）	
2		計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	有： 2週間前までにメール／サポートサイトにて通知します。	有： 2週間前までにメール／サポートサイトにて通知します。	有： 2週間前までにメール／サポートサイトにて通知します。	有： 2週間前までにメール／サポートサイトにて通知します。	有： 2週間前までにメール／サポートサイトにて通知します。	
3		サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	有： 現時点で予定はしておりませんが、12か月前までにメール／サポートサイトにて通知するよう努力します。	有： 現時点で予定はしておりませんが、12か月前までにメール／サポートサイトにて通知するよう努力します。	有： 現時点で予定はしておりませんが、12か月前までにメール／サポートサイトにて通知するよう努力します。	有： 現時点で予定はしておりませんが、12か月前までにメール／サポートサイトにて通知するよう努力します。	有： 12か月前までにメール／サポートサイトにて通知するよう努力します。	
4		突然のサービス提供停止に対する対処	プログラムや、システム環境の各種設定データの預託等の措置の有無	有無	無： 預託等の措置は行っておりません。	無： 預託等の措置は行っておりません。	無： 預託等の措置は行っておりません。	無： 預託等の措置は行っておりません。	無： 預託等の措置は行っておりません。	
5		サービス稼働率	サービスを利用できる確率（計画サービス時間－停止時間）÷計画サービス時間	稼働率（%）	SLO 99.9% 以上	SLO 99.9% 以上	SLO 99.9% 以上	SLO 99.9% 以上	SLO 99.9% 以上	SLA については定めておりません。
6		ディザスタリカバリ	災害発生時のシステム復旧 サポート体制	有無	無： ディザスタリカバリについてはサービス内容に含まれておりません。	無： ディザスタリカバリについてはサービス内容に含まれておりません。	無： ディザスタリカバリについてはサービス内容に含まれておりません。	無： ディザスタリカバリについてはサービス内容に含まれておりません。	無： ディザスタリカバリについてはサービス内容に含まれておりません。	同一地域内ではありますが、冗長化による可用性の確保については実施いたしております。
7		重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	無： 早期復旧が困難と判断した場合、お客様の業務継続を最優先に考える方法をご案内させていただきます。	無： 早期復旧が困難と判断した場合、当社サービスを一時的に外し、お客様の業務継続を最優先に考える方法をご案内させていただきます。	無： 早期復旧が困難と判断した場合、当社サービスを一時的に外し、お客様の業務継続を最優先に考える方法をご案内させていただきます。	無： 早期復旧が困難と判断した場合、当社サービスを一時的に外し、お客様の業務継続を最優先に考える方法をご案内させていただきます。	無： 早期復旧が困難と判断した場合、当社サービスを一時的に外し、お客様の業務継続を最優先に考える方法をご案内させていただきます。	
8		代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無（ファイル形式）	無： アップロードされた添付ファイル等については確認いただけません。	有： 管理画面にアクセスできる場合には設定情報をテキストファイルで確認いただけます。	有： 管理画面にアクセスできる場合には設定情報をテキストファイルで確認いただけます。	有： 管理画面にアクセスできる場合には「アーカイブデータ」を eml 形式にて確認いただけます。	無： アップロードされた添付ファイル等については確認いただけません。	
9		アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	有無	有： 不定期のバージョンアップを行います。 顧客影響のあるバージョンアップとなる場合は事前にユーザー様にメンテナンス予定を通知します。 ただし、OS やサービスに対して緊急を要するメンテナンスが生じた場合、事前の連絡なく実施する場合があります。	有： 不定期のバージョンアップを行います。 顧客影響のあるバージョンアップとなる場合は事前にユーザー様にメンテナンス予定を通知します。 ただし、OS やサービスに対して緊急を要するメンテナンスが生じた場合、事前の連絡なく実施する場合があります。	有： 不定期のバージョンアップを行います。 顧客影響のあるバージョンアップとなる場合は事前にユーザー様にメンテナンス予定を通知します。 ただし、OS やサービスに対して緊急を要するメンテナンスが生じた場合、事前の連絡なく実施する場合があります。	有： 不定期のバージョンアップを行います。 顧客影響のあるバージョンアップとなる場合は事前にユーザー様にメンテナンス予定を通知します。 ただし、OS やサービスに対して緊急を要するメンテナンスが生じた場合、事前の連絡なく実施する場合があります。	有： 不定期のバージョンアップを行います。 顧客影響のあるバージョンアップとなる場合は事前にユーザー様にメンテナンス予定を通知します。 ただし、OS やサービスに対して緊急を要するメンテナンスが生じた場合、事前の連絡なく実施する場合があります。	
10	信頼性	平均復旧時間(MTTR)	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	時間	非公開となります。	非公開となります。	非公開となります。	非公開となります。	非公開となります。	
11		目標復旧時間(RTO)	障害発生後のサービス提供の再開に関して設定された目標時間	時間	非公開となります。	非公開となります。	非公開となります。	非公開となります。	非公開となります。	
12		障害発生件数	1年間に発生した障害件数／1年間に発生した対応に長時間（1日以上）要した障害件数	回	サポートサイトにて過去の障害情報を掲載しておりますのでご参照ください。 https://security-support.canon-its.jp/?site_domain=GUARDIANWALL	サポートサイトにて過去の障害情報を掲載しておりますのでご参照ください。 https://security-support.canon-its.jp/?site_domain=gwc	サポートサイトにて過去の障害情報を掲載しておりますのでご参照ください。 https://security-support.canon-its.jp/?site_domain=gwc	サポートサイトにて過去の障害情報を掲載しておりますのでご参照ください。 https://security-support.canon-its.jp/?site_domain=gwc	サポートサイトにて過去の障害情報を掲載しておりますのでご参照ください。 https://security-support.canon-its.jp/?site_domain=gwc	
13		システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	有： 死活監視（ping 監視･ポート監視･プロセス監視）を行っています。	有： 死活監視（ping 監視･ポート監視･プロセス監視）、メールキュー監視を行っています。	有： 死活監視（ping 監視･ポート監視･プロセス監視）、メールキュー監視を行っています。	有： 死活監視（ping 監視･ポート監視･プロセス監視）、メールキュー監視を行っています。	有： 死活監視（ping 監視･ポート監視･プロセス監視）を行っています。	
14		障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	有無	有： サポートサイトにて障害情報を掲載します。	有： サポートサイトにて障害情報を掲載します。	有： サポートサイトにて障害情報を掲載します。	有： サポートサイトにて障害情報を掲載します。	有： サポートサイトにて障害情報を掲載します。	
15		障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	障害検知後、2時間以内にサポートサイトに掲載します。	障害検知後、2時間以内にサポートサイトに掲載します。	障害検知後、2時間以内にサポートサイトに掲載します。	障害検知後、2時間以内にサポートサイトに掲載します。	障害検知後、2時間以内にサポートサイトに掲載します。	

No.	種別	サービスレベル項目例	規定内容	測定単位	サービス名					備考
事業者に確認すべき項目			確認すべき項目の内容	事業者に求める回答の単位	Mailセキュリティ・オンプレミス 添付ファイルダウンロードリンク化オプション	Mailセキュリティ・クラウド プレミアム／ベーシック			Outbound Security for Microsoft 365	
						MailFilter on Cloud	MailConvert on Cloud	MailArchive on Cloud		
16		障害監視間隔	障害インシデントを収集／集計する時間間隔	時間（分）	非公開となります。	非公開となります。	非公開となります。	非公開となります。	非公開となります。	
17		サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	時間	定期的なサービス稼働状況の提供はいたしておりません。 必要に応じて実施します。	定期的なサービス稼働状況の提供はいたしておりません。 必要に応じて実施します。	定期的なサービス稼働状況の提供はいたしておりません。 必要に応じて実施します。	定期的なサービス稼働状況の提供はいたしておりません。 必要に応じて実施します。	定期的なサービス稼働状況の提供はいたしておりません。 必要に応じて実施します。	
18		ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	有： 管理画面より添付ファイルの操作ログを確認いただけます。	有： 管理画面よりメールの送受信ログ／操作ログを確認いただけます。（プレミアムのみ）	有： 管理画面よりメールの送受信ログ／操作ログを確認いただけます。（プレミアムのみ）	有： 管理画面よりメールの送受信ログ／操作ログを確認いただけます。（プレミアムのみ）	無： 送信者は操作画面より添付ファイルダウンロードログを確認いただけます。	Mailセキュリティ・クラウド ベーシックについてはログ提供はございません。
19	性能	応答時間	処理の応答時間	時間（秒）	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	
20		遅延	処理の応答時間の遅延継続時間	時間（分）	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	定義いたしておりません。 ただし、極端なサービス性能の低下がないよう監視・調整を行っております。	
22	拡張性	カスタマイズ性	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	有： 管理画面より添付ファイル変換定義等の設定を変更することが可能です。 管理画面から設定可能な項目以外のカスタマイズは出来かねます。	有： 管理画面よりフィルタリング動作定義等の設定を変更することが可能です。 管理画面から設定可能な項目以外のカスタマイズは出来かねます。	有： 管理画面より添付ファイル変換定義等の設定を変更することが可能です。 管理画面から設定可能な項目以外のカスタマイズは出来かねます。	有： 管理画面よりアーカイブ動作定義等の設定を変更することが可能です。 管理画面から設定可能な項目以外のカスタマイズは出来かねます。	有： 読み込むアドインによって利用可能な機能を変更することが可能です。 アドインで変更できない項目について、カスタマイズは出来かねます。	
23		外部接続性	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（API、開発言語等）	有無	有： GUARDIANWALL Mailセキュリティ・オンプレミスとのみ連携可能な Web API を提供します。	有： 他社ディレクトリサービスサーバーとの連携に対応しております。 本サービス機能として API 等の公開はございません。	有： 他社ディレクトリサービスサーバーとの連携に対応しております。 本サービス機能として API 等の公開はございません。	有： 他社ディレクトリサービスサーバーとの連携に対応しております。 本サービス機能として API 等の公開はございません。	無： 本サービス機能として API 等の公開はございません。	
24		同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無（制約条件）	無： システム上の制約はございません。 ただし、最大同時接続数についてはベストエフォートとなります。	無： システム上の制約はございません。 ただし、最大同時接続数についてはベストエフォートとなります。	無： システム上の制約はございません。 ただし、最大同時接続数についてはベストエフォートとなります。	無： システム上の制約はございません。 ただし、最大同時接続数についてはベストエフォートとなります。	無： システム上の制約はございません。 ただし、最大同時接続数についてはベストエフォートとなります。	
25		提供リソースの上限	ディスク容量の上限／ページビューの上限	処理能力	ログ、リンク化された添付ファイルともに30日の保存期間のみ定めております。	ログの保存期間のみ1年と定めております。	ログ1年、リンク化された添付ファイル30日の保存期間のみ定めております。	ログ、メールアーカイブデータの保存期間のみ1年と定めております。 アーカイブ保管サービス（過去2年以上）はご契約により、保存期間は変動します。	ログ、リンク化された添付ファイルともに30日の保存期間のみ定めております。	ディスク容量、管理画面アクセス数、メール処理能力については定義いたしておりません。
サポート										
26	サポート	サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	お問い合わせ受付は平日のみとなりますが、監視体制は夜間・休日も整えております。
27		サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	平日 9:00～17:00（メール / Web フォーム） ※祝日および弊社休業日を除く	
データ管理										
28	データ管理	バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無／内容	有： システム復旧用のシステムバックアップを取得しております。	有： システム復旧用のシステムバックアップを定期的に取得を行います。	有： システム復旧用のシステムバックアップを定期的に取得を行います。	有： システム復旧用のシステムバックアップ、ならびに、アーカイブデータバックアップについて定期的に取得を行います。	有： システム復旧用のシステムバックアップを取得しております。	
29		バックアップデータを取得するタイミング(RPO)	バックアップデータをとり、データを保証する時点	時間	1日1回バックアップを取得します。 なお、詳細は非公開になります。	毎日5時にシステムバックアップを取得します。	毎日5時にシステムバックアップを取得します。	毎日5時にシステムバックアップを取得します。 アーカイブデータバックアップについては前日 23:59 までのデータを日次で取得します。	1日1回バックアップを取得します。 なお、詳細は非公開になります。	
30		バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	システムバックアップは7日間保管します。	システムバックアップは7日間保管します。	システムバックアップは7日間保管します。	システムバックアップは7日間、 アーカイブデータバックアップは1年間保管します。	システムバックアップは7日間保管します。	

No.	種別	サービスレベル項目例	規定内容	測定単位	サービス名					備考
事業者に確認すべき項目			確認すべき項目の内容	事業者に求める回答の単位	Mailセキュリティ・オンプレミス 添付ファイルダウンロードリンク化オプション	Mailセキュリティ・クラウド プレミアム／ベーシック			Outbound Security for Microsoft 365	
						MailFilter on Cloud	MailConvert on Cloud	MailArchive on Cloud		
31		データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	有： 利用約款に準じて削除します。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 利用約款に準じて削除します。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 利用約款に準じて削除します。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 利用約款に準じて削除します。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： サービス解約に伴いデータを削除します。	
32		バックアップ世代数	保証する世代数	世代数	設定バックアップについては7世代保存します。	設定バックアップについては7世代保存します。	設定バックアップについては7世代保存します。	設定バックアップについては7世代保存します。 メールアーカイブデータバックアップについては日次取得で365日分保存します。	設定バックアップについては7世代保存します。	
33		データ保護のための暗号化要件	データを保護するにあたり、暗号化要件の有無	有無	有： ファイルシステム/DB層でデータ暗号化を実施します。	無： データの暗号化は行っておりません。 ただし、管理画面パスワードについては難読化処理を施しています。	無： データの暗号化は行っておりません。 ただし、管理画面パスワードについては難読化処理を施しています。	無： データの暗号化は行っておりません。 ただし、管理画面パスワードや、メールアーカイブデータについては難読化処理を施しています。	有： ファイルシステム/DB層でデータ暗号化を実施します。	
34		マルチテナントストレージにおけるキー管理要件	マルチテナントストレージのキー管理要件の有無、内容	有無／内容	有： 差出人となるユーザーごとにデータを論理的に分離して管理を行っております。 データへアクセスするための Web API 認証キーについてはテナント毎に分離されております。	有： 他テナントとデータを論理的に分離して管理を行っております。 データへアクセスするためのテナント管理者 ID/PW についてはテナント毎に分離されております。	有： 他テナントとデータを論理的に分離して管理を行っております。 データへアクセスするためのテナント管理者 ID/PW についてはテナント毎に分離されております。	有： 他テナントとデータを論理的に分離して管理を行っております。 データへアクセスするためのテナント管理者 ID/PW についてはテナント毎に分離されております。	有： 差出人となるユーザーごとにデータを論理的に分離して管理を行っております。 データにアクセスする際はメーラーから送信されるユーザーを元に表示を行っており、弊社提供アドイン以外からのアクセスはできなくすることで他者から確認ができないようにしています。	
35		データ漏えい・破壊時の補償／保険	データ漏えい・破壊時の補償／保険の有無	有無	有： 以下サービス利用約款にのっとり、保証の範囲を定めております。 第10条(損害賠償) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 以下サービス利用約款にのっとり、保証の範囲を定めております。 第10条(損害賠償) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 以下サービス利用約款にのっとり、保証の範囲を定めております。 第10条(損害賠償) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 以下サービス利用約款にのっとり、保証の範囲を定めております。 第10条(損害賠償) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	無： 情報の取り扱いには細心の注意を払いますが、以下サービス利用約款にのっとり、免責事項とさせていただいております。 第13条（当社の責任および免責等） https://canon-its.jp/guardian/patch/man/OS365_provision_R1.pdf	
36		解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できていること	有無／内容	有： 解約時についてはデータの返却は実施いたしません。当社内にてデータの削除を実施します。 サービス解約後についてはサービス利用約款に定めております。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 解約時についてはデータの返却は実施いたしません。当社内にてデータの削除を実施します。 サービス解約後についてはサービス利用約款に定めております。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 解約時についてはデータの返却は実施いたしません。当社内にてデータの削除を実施します。 サービス解約後についてはサービス利用約款に定めております。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	有： 解約時についてはデータの返却は実施いたしません。当社内にてデータの削除を実施します。 サービス解約後についてはサービス利用約款に定めております。 第23条(契約終了後の処理) https://canon-its.jp/guardian/patch/man/MSC_ADLOP_Provision_R.pdf	無： 解約時についてはデータの返却は実施いたしません。当社内にてデータの削除を実施します。	
37		預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	有無	非公開となります。	非公開となります。	非公開となります。	非公開となります。	非公開となります。	
38		入力データ形式の制限機能	入力データ形式の制限機能の有無	有無	有： 弊社規定にのっとり、セキュアコーディングを実施しております。 また、脆弱性診断も定期的に実施し、想定外の入力データがシステムに混入しないよう対策を講じております。	有： 弊社規定にのっとり、セキュアコーディングを実施しております。 また、脆弱性診断も定期的に実施し、想定外の入力データがシステムに混入しないよう対策を講じております。	有： 弊社規定にのっとり、セキュアコーディングを実施しております。 また、脆弱性診断も定期的に実施し、想定外の入力データがシステムに混入しないよう対策を講じております。	有： 弊社規定にのっとり、セキュアコーディングを実施しております。 また、脆弱性診断も定期的に実施し、想定外の入力データがシステムに混入しないよう対策を講じております。	有： 弊社規定にのっとり、セキュアコーディングを実施しております。 また、脆弱性診断も定期的に実施し、想定外の入力データがシステムに混入しないよう対策を講じております。	
セキュリティ										
39	セキュリティ	公的認証取得の要件	JIPDECやJQA等で認定している情報処理管理に関する公的認証 （ISMS、プライバシーマーク等）が取得されていること	有無	有： 下記を取得しております。 ISO/IEC 27001:2013,JISQ 27001:2014	有： 下記を取得しております。 ISO/IEC 27001:2013,JISQ 27001:2014	有： 下記を取得しております。 ISO/IEC 27001:2013,JISQ 27001:2014	有： 下記を取得しております。 ISO/IEC 27001:2013,JISQ 27001:2014	有： 下記を取得しております。 ISO/IEC 27001:2013,JISQ 27001:2014	そのほかサービス基盤で以下を取得しております。 ・FJcloud-V：ISO/IEC 27001:2013，JISQ 27001:2014，JIP-ISMS517-1.0(ISO/IEC 27017:2015)，SOC2保障報告書Type1，ISMAP(登録番号C21-0021-2) ・AWS：ISO/IEC 27001:2022，27017:2015，27018:2019，27701:2019，22301:2019，20000-1:2018，9001:2015，CSA STAR CcM v4.0，SOC1，SOC2，SOC3 ・その他：ISO/IEC 27001:2013，JIP-ISMS517-1.0(ISO/IEC 27017:2015)
40		アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	有無／実施状況	有： 脆弱性対策として第三者であるイエラエセキュリティ社による脆弱性診断 サービスを受け、対策を適宜講じております。	有： 脆弱性対策として第三者であるイエラエセキュリティ社による脆弱性診断 サービスを受け、対策を適宜講じております。	有： 脆弱性対策として第三者であるイエラエセキュリティ社による脆弱性診断 サービスを受け、対策を適宜講じております。	有： 脆弱性対策として第三者であるイエラエセキュリティ社による脆弱性診断 サービスを受け、対策を適宜講じております。	有： 脆弱性対策として第三者であるイエラエセキュリティ社による脆弱性診断 サービスを受け、対策を適宜講じております。	
41		情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること	有無	有： 運用環境へは特定部門の一部の者のみ可能としております。	有： 運用環境へは特定部門の一部の者のみ可能としております。	有： 運用環境へは特定部門の一部の者のみ可能としております。	有： 運用環境へは特定部門の一部の者のみ可能としております。	有： 運用環境へは特定部門の一部の者のみ可能としております。	

No.	種別	サービスレベル項目例	規定内容	測定単位	サービス名					備考
事業者に確認すべき項目			確認すべき項目の内容	事業者に求める回答の単位	Mailセキュリティ・オンプレミス 添付ファイルダウンロードリンク化オプション	Mailセキュリティ・クラウド プレミアム／ベーシック			Outbound Security for Microsoft 365	
						MailFilter on Cloud	MailConvert on Cloud	MailArchive on Cloud		
42		通信の暗号化レベル	システムとやりとりされる通信の暗号化強度	有無	有： Web API と GUARDIANWALL Mailセキュリティ・オンプレミス間の通信は TLS1.2 にて暗号化を行っております。	有： 管理画面へのアクセスは TLS1.2 にて暗号化を行っております。	有： 管理画面へのアクセスは TLS1.2 にて暗号化を行っております。	有： 管理画面へのアクセス、添付ファイルのアップロード、添付ファイルのダウンロードサイトへのアクセスは TLS1.2 にて暗号化を行っております。	有： 添付ファイルのアップロード、添付ファイルのダウンロードサイトへのアクセスは TLS1.2 にて暗号化を行っております。	
43		会計監査報告書における情報セキュリティ関連事項の確認	会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨「最新のSAS70Type2監査報告書」「最新の18号監査報告書」	有無	無： 内部統制に関する監査基準の審査は受けておりません。 詳細は非公開となりますが、弊社内で内部統制は実施しております。	無： 内部統制に関する監査基準の審査は受けておりません。 詳細は非公開となりますが、弊社内で内部統制は実施しております。	無： 内部統制に関する監査基準の審査は受けておりません。 詳細は非公開となりますが、弊社内で内部統制は実施しております。	無： 内部統制に関する監査基準の審査は受けておりません。 詳細は非公開となりますが、弊社内で内部統制は実施しております。	無： 内部統制に関する監査基準の審査は受けておりません。 詳細は非公開となりますが、弊社内で内部統制は実施しております。	
44		マルチテナント下でのセキュリティ対策	異なる利用企業間の情報隔離、障害等の影響の局所化	有無	有： 添付ファイルアップロードサーバー内のデータは送信者のメールアドレスごとに論理的に分離して管理しています。	有： 各テナントごとに論理的に分離して管理し、あわせてユーザーID、パスワードの組み合わせでアカウント情報を付与することでアクセス制御しております。	有： 各テナントごとに論理的に分離して管理し、あわせてユーザーID、パスワードの組み合わせでアカウント情報を付与することでアクセス制御しております。	有： 各テナントごとに論理的に分離して管理し、あわせてユーザーID、パスワードの組み合わせでアカウント情報を付与することでアクセス制御しております。	有： 当サービスは Outlook アドイン型で提供しているため、認証については Microsoft 社基盤に準拠します。 添付ファイルアップロードサーバー内のデータは送信者のメールアドレスごとに論理的に分離して管理しています。	
45		情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること 利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	有無／設定状況	有： 原則として利用者のデータに対してアクセスできないように制限されています。ただし、利用者からの依頼を得たうえでアクセスする場合があります。 なお、その場合でも運用環境を操作できる者は運用部門内でも限定されております。	有： 原則として利用者のデータに対してアクセスできないように制限されています。ただし、利用者からの依頼を得たうえでアクセスする場合があります。 なお、その場合でも運用環境を操作できる者は運用部門内でも限定されております。	有： 原則として利用者のデータに対してアクセスできないように制限されています。ただし、利用者からの依頼を得たうえでアクセスする場合があります。 なお、その場合でも運用環境を操作できる者は運用部門内でも限定されております。	有： 原則として利用者のデータに対してアクセスできないように制限されています。ただし、利用者からの依頼を得たうえでアクセスする場合があります。 なお、その場合でも運用環境を操作できる者は運用部門内でも限定されております。	有： 原則として利用者のデータに対してアクセスできないように制限されています。ただし、利用者からの依頼を得たうえでアクセスする場合があります。 なお、その場合でも運用環境を操作できる者は運用部門内でも限定されております。	
46		セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	設定状況	ログ情報の提供は行ってはおりませんが、保管しているログ情報より、調査可能となっております。	ログ情報の提供は行ってはおりませんが、保管しているログ情報より、調査可能となっております。	ログ情報の提供は行ってはおりませんが、保管しているログ情報より、調査可能となっております。	ログ情報の提供は行ってはおりませんが、保管しているログ情報より、調査可能となっております。	ログ情報の提供は行ってはおりませんが、保管しているログ情報より、調査可能となっております。	
47		ウイルススキャン	ウイルススキャンの頻度	頻度	ウイルススキャンは実施しておりませんが他の対策を複数行っており非公開となります。	ウイルススキャンは実施しておりませんが他の対策を複数行っており非公開となります。	ウイルススキャンは実施しておりませんが他の対策を複数行っており非公開となります。	ウイルススキャンは実施しておりませんが他の対策を複数行っており非公開となります。	ウイルススキャンは実施しておりませんが他の対策を複数行っており非公開となります。	
48		二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管していること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること	有無	有： 二次記憶媒体を含む、インフラ環境は「AWS」を利用しております。 そのため、「AWS」での安全性対策に準拠します。	有： 二次記憶媒体を含む、インフラ環境は「FJcloud-V」を利用しております。 そのため、「FJcloud-V」での安全性対策に準拠します。	有： 二次記憶媒体を含む、インフラ環境は「FJcloud-V」「AWS」を利用しております。 そのため、「FJcloud-V」「AWS」での安全性対策に準拠します。	有： 二次記憶媒体を含む、インフラ環境は「FJcloud-V」を利用しております。 そのため、「FJcloud-V」での安全性対策に準拠します。	有： 二次記憶媒体を含む、インフラ環境は「AWS」を利用しております。 そのため、「AWS」での安全性対策に準拠します。	
49		データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	把握状況	インフラ環境は「日本国内」リージョンで運用しているため、日本の各種法制度の下におけるデータ取り扱いおよび利用に関する制約条件を把握しております。	インフラ環境は「日本国内」リージョンで運用しているため、日本の各種法制度の下におけるデータ取り扱いおよび利用に関する制約条件を把握しております。	インフラ環境は「日本国内」リージョンで運用しているため、日本の各種法制度の下におけるデータ取り扱いおよび利用に関する制約条件を把握しております。	インフラ環境は「日本国内」リージョンで運用しているため、日本の各種法制度の下におけるデータ取り扱いおよび利用に関する制約条件を把握しております。	インフラ環境は「日本国内」リージョンで運用しているため、日本の各種法制度の下におけるデータ取り扱いおよび利用に関する制約条件を把握しております。	