

(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)				2024年8月時点	
No.	種別	サービスレベル項目例	規定内容	測定単位	オプション/利用サービス名
事業者を確認すべき項目		確認すべき項目の内容		事業者を求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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）
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週間前を目途にメール/ホームページにて通知します。
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： 可能な限り2か月以上前にメール/ホームページにて通知します。
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。
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
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。

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション／利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者に求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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、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案内します。
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： データは提供されません。
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
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

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション／利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者を求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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	非公開 ただし、サービス影響のある障害についてはホームページにて障害情報を掲載しております。
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）、メールキュー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： メール／ホームページにて通知します。
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 時間以内を目途にメール／ホームページにて通知します。 ただし、サポートサービス提供時間外の場合は翌営業日の提供時間帯に通知します。
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
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していません。

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション／利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者を求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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	無： ログの閲覧画面は提供されていません。
19	性能	応答時間	処理の応答時間	時間（秒）	定義していません。 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）	定義していません。 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）	定義していません。 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 を変更することができます。 管理画面から設定可能な項目以外のカスタ マイズはできません。
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	無： 連携機能は用意されていません。

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション／利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者に求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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ありません。 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 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。
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 9:00～18:00（電話 / メール / Web フォーム） ※ 祝日および弊社休業日を除く
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 9:00～18:00（電話 / 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、利用者にも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定期的 に取得します。
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	毎日 5 時にシステムバックアップを取得します。

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション／利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者を求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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。
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： HOME利用約款に準じます。
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。
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	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。
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： 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。

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション／利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者に求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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： HOME利用約款に準じます。
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、データの返却はしません。弊社にてデータの削除を行います。
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
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の実施し、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					

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション/利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者を求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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, JIP-ISMS517-1.0(ISO/IEC 27017:2015), SOC2保障報告書Type1
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テラ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。
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： 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。
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。
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： 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。

No.	種別	サービスレベル項目例	規定内容	測定単位	オプション／利用サービス名
		事業者を確認すべき項目	確認すべき項目の内容	事業者を求める回答の単位	HOME type-M 添付ファイルメールセキュリティオプション GUARDIANWALL Mailセキュリティ・クラウド MailConvert on Cloud ベーシック
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。
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。
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。
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「ニフクラ」「AWS」を利用しております。 そのため、「ニフクラ」「AWS」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扱いおよび利用に関する制約条件を把握しております。