Aurora SMS by メディアSMS

AuroraSMS by メディアSMS サービス

セキュリティホワイトペーパー

第1.0版

株式会社メディア４ｕ

1. はじめに

株式会社メディア4u（以下「当社」といいます）は、情報セキュリティ管理規程および個人情報保護方針に基づき、Aurora SMS サービスの安全性および信頼性の確保に取り組んでいます。

当社は、関連法令および各種ガイドラインを遵守するとともに、情報セキュリティリスクの適切な管理および継続的な改善を実施しています。

本書は、Aurora SMS および関連サービスを対象として、当社が講じているセキュリティ対策について、利用者および導入検討者向けに説明するものです。

2. 適用範囲

本書は、当社が提供する以下のサービスを対象とします。

・Aurora SMS

・Aurora SMS 関連サービス

なお、以下は本書の適用対象外とします。

・他社が提供する外部サービス

・ベータ版または試験提供中の機能

・外部事業者が開発・運用・保守を行うオプション機能

3. 会社情報

会社名：株式会社メディア4u

所在地：東京都港区赤坂1丁目11-30　赤坂一丁目センタービル9F

電気通信事業者番号：A-25-13031

4. 認証

当社は、以下の認証・基準に基づき、情報セキュリティ管理体制を運用しています。

・プライバシーマーク　番号：17001173(07)

・ISMS（ISO/IEC 27001）

・ISMSクラウドセキュリティ（ISO/IEC 27017）

これらの認証は定期的な外部監査を受け、継続的な改善を実施しています。

5. 法令遵守

当社は、日本国の関連法令を遵守し、サービスを提供します。

また、利用規約および本サービスに関する法律関係は、日本法に準拠し、日本法に基づいて解釈されます。

6. 責任分界点

当社の責任範囲

サービス基盤のセキュリティ対策、データ保護、システム運用および監視を実施しています。

主な実施内容は以下の通りです。

・ネットワークおよびサーバ保護

・アクセス制御

・データ保護

・バックアップ運用

・障害監視およびインシデント対応

・ログ管理および監査

また、契約終了後は、所定の手順に基づきお客様データを削除します。

お客様の責任範囲

お客様には、以下の事項について適切な管理をお願いしています。

・ID・パスワード管理

・APIキー管理

・利用端末のセキュリティ管理

・アクセス権限設定

・誤送信防止運用

また、本サービスを利用して取得した情報については、お客様責任のもと管理いただきます。

7. セキュリティ管理体制

当社は情報セキュリティ管理体制を整備し、以下を継続的に実施しています。

・リスクアセスメント

・セキュリティ教育（年1回以上）

・内部監査

・外部監査対応

・インシデント管理

・ PDCAサイクルによる継続的改善

8. 人的セキュリティ

当社では、人的リスクへの対策として以下を実施しています。

・全従業者との秘密保持契約締結

・入社時および定期的なセキュリティ教育

・権限に応じたアクセス制御

・退職・異動時の速やかな権限剥奪

・内部不正防止対策

セキュリティ教育については、入社時教育に加え、年1回以上の継続教育を実施しています。

9. 物理セキュリティ

当社では、国内データセンターを利用し、物理的な安全管理措置を実施しています。

主な対策は以下の通りです。

・入退室管理

・監視カメラによる24時間監視

・耐震対策

・電源冗長化

・空調管理

・重要設備へのアクセス制限

また、サービス運用機器へのアクセスは、許可された担当者のみに限定しています。

10. ネットワークセキュリティ

当社では、多層防御の考え方に基づき、ネットワークセキュリティ対策を実施しています。

ネットワーク構成

・DMZによるネットワーク分離

・管理系ネットワークとサービス系ネットワークの分離

・権限に応じたアクセス制御

主な対策は以下の通りです。

・ファイアウォールによる通信制御

・ IDS/IPSによる不正通信検知

・ WAFによるWebアプリケーション保護

・ VPN接続による管理アクセス制限

・多要素認証（MFA）

・通信監視

・回線冗長化

11. サーバおよびプラットフォームセキュリティ

当社では、最小権限の原則に基づき、サーバおよびプラットフォーム環境の安全管理を実施しています。

主な対策は以下の通りです。

・管理者権限の定期棚卸し

・アクセス制御

・通信制御

・データ暗号化

・パッチ管理

・構成管理

・ログ取得および監査

・セキュリティアップデート適用

また、機器廃棄時には、データ消去または物理破壊を実施し、情報漏えい防止を徹底しています。

12. 開発セキュリティ

当社では、安全なシステム開発および運用を実施するため、開発プロセスにおいて以下の対策を実施しています。

・ソースコード管理

・開発環境・検証環境・本番環境の分離

・レビューおよび承認プロセス

・テスト環境での事前検証

・機密情報の適切な管理

・変更管理運用

・セキュリティを考慮したリリース管理

13. データ保護

データ保管

・データは日本国内のデータセンターに保管

・バックアップは地理的に分散した環境に保管

・お客様データを無断で国外へ移転しません

データ保護対策

・AES-256による暗号化保存

・アクセス制御

・ログ監査

・テナント分離

・不正アクセス防止

10. ネットワークセキュリティ

当社では、多層防御の考え方に基づき、ネットワークセキュリティ対策を実施しています。

ネットワーク構成

・DMZによるネットワーク分離

・管理系ネットワークとサービス系ネットワークの分離

・権限に応じたアクセス制御

主な対策は以下の通りです。

・ファイアウォールによる通信制御

・ IDS/IPSによる不正通信検知

・ WAFによるWebアプリケーション保護

・ VPN接続による管理アクセス制限

・多要素認証（MFA）

・通信監視

・回線冗長化

11. サーバおよびプラットフォームセキュリティ

当社では、最小権限の原則に基づき、サーバおよびプラットフォーム環境の安全管理を実施しています。

主な対策は以下の通りです。

・管理者権限の定期棚卸し

・アクセス制御

・通信制御

・データ暗号化

・パッチ管理

・構成管理

・ログ取得および監査

・セキュリティアップデート適用

また、機器廃棄時には、データ消去または物理破壊を実施し、情報漏えい防止を徹底しています。

14. 通信の暗号化

当社では、通信経路の安全性確保のため、暗号化通信を採用しています。

・HTTPS（TLS1.2以上）を使用

・通信経路上の盗聴・改ざん・なりすましを防止

・推奨されない暗号スイートおよび脆弱なプロトコルを無効化

15. 認証・アクセス管理

認証

・ID・パスワード認証

・多要素認証（MFA）対応

・ログイン失敗回数制限

・ IPアドレス制限

・パスワード複雑性要件

・パスワード再利用制限

・初回ログイン時のパスワード変更

認可

・ロールベースアクセス制御（RBAC）

・最小権限の原則による権限設定

・アカウント管理

・申請・承認によるアカウント発行

・不要アカウントの速やかな削除

・半年ごとのアカウント棚卸し

セッション管理

・一定時間無操作時の自動ログアウト

バックアップ

・日次バックアップ取得

・最大365世代保持

・本番環境と分離して保管

・バックアップデータも暗号化管理

16. マルウェア対策

当社では、マルウェアおよび不正コードへの対策を実施しています。

・アンチマルウェア対策

・EDRによる不審な振る舞い検知

・メールセキュリティ対策

・不正ファイル検知

・不正通信監視

17. サービス提供体制・可用性

当社では、安定したサービス提供のため、継続的な運用管理を実施しています。

サービス提供

・24時間365日でのサービス提供

・計画停止時の事前通知

・障害発生時の通知

・対応サービス終了時の事前通知

可用性対策

・月間稼働率99.99%を目標とした運用

・冗長構成による継続運用

・災害対策の実施

災害復旧（DR）対策

・国内代替拠点の活用

・バックアップ復旧体制

・BCP（事業継続計画）の運用

18. ログ管理・監査

当社では、システム運用状況およびセキュリティイベントを把握するため、各種ログの取得および監査を実施しています。

主な管理内容は以下の通りです。

・ログイン履歴および操作ログの記録

・アクセスログ・システムログ管理

・異常検知のためのログ分析

・インシデント調査時の証跡管理

・ログの適切な保管・管理

ログ保存期間は原則1年間です。

19. 時刻同期

当社では、ログおよび監査証跡の整合性維持のため、各システムで時刻同期を実施しています。

・NTPサーバーによる時刻同期

・時刻ずれの定期監視

・ログ整合性の維持

20. 脆弱性管理

当社では、脆弱性情報の収集、診断、および是正対応を継続的に実施しています。

主な対策は以下の通りです。

・Webアプリケーション脆弱性診断

・プラットフォーム脆弱性診断

・セキュリティパッチ管理

・リスク評価に基づく優先対応

・テスト環境での事前検証

・承認プロセスを経たリリース管理

・サポート期限切れ製品の利用防止

脆弱性診断については、新規構築時、大規模改修時、および定期的に実施しています。

21. 監視・セキュリティ監視

当社では、24時間365日でシステム監視を実施しています。

主な監視対象

・CPU・メモリ・ディスク監視

・Ping監視

・Service Port監視

・プロセス監視

・ネットワーク監視

・ログ監視

・不正アクセス監視

セキュリティ監視

・WAF監視

・IDS/IPS監視

・EDR監視

・メールセキュリティ監視

・Web改ざん検知

・ログ相関分析

異常検知時には、担当者への通知、影響調査、および必要な対策を速やかに実施しています。

22. 冗長性および可用性

当社では、サービス継続性確保のため、冗長化および事業継続対策を実施しています。

・システム冗長構成

・バックアップからの復旧体制

・定期的な復旧テスト

・BCPに基づく継続運用

・災害対策を考慮したデータ分散保管

23. インシデント対応

当社では、情報セキュリティインシデント発生時に迅速かつ適切な対応を実施するため、対応体制および運用手順を整備しています。

インシデント発生時には、影響拡大防止および早期復旧を目的として、状況に応じた対応を実施します。

主な対応内容

・インシデントの検知および初動対応

・影響範囲の調査および特定

・原因分析および暫定対処

・恒久対策および再発防止策の実施

・必要に応じたアクセス制御・遮断対応

・ログ分析および証跡保全

・関係部門へのエスカレーション

・必要に応じた関係機関との連携

・復旧対応およびサービス継続対応

お客様への通知

重大なセキュリティインシデントが発生した場合には、影響範囲、原因、対処状況等を確認のうえ、必要に応じてお客様へ通知を実施します。

また、サービス影響が発生する場合には、状況に応じて継続的な情報共有を行います。

再発防止

インシデント収束後は、原因分析および対応内容をレビューし、必要に応じて以下を実施します。

・運用手順の見直し

・セキュリティ設定の改善

・監視強化

・教育・訓練の実施

・再発防止策の策定

・訓練・改善活動

当社では、インシデント対応能力向上のため、定期的な手順見直しおよび教育・訓練を実施し、継続的な改善に取り組んでいます。

24. サービスレベル

SLAについて

本サービスでは、個別契約を除きSLA（サービス品質保証）は提供していません。

ただし、継続的な可用性向上に努めています。

記載の稼働率は運用目標値です。

可用性

・24時間365日提供

・月間稼働率99.99%を目標として運用

復旧目標

・RTO（復旧目標時間）：2時間

・RPO（データ復旧目標）：1日

障害発生時には、原則として検知後30分以内を目安に初回通知を実施します。

性能

・応答時間1〜2秒を目標として運用

拡張性

・ API連携対応

・負荷状況に応じたリソース拡張

サポート

・営業時間：10時〜19時

・障害情報：適切なタイミングで通知（原則として検知後30分以内を目安）

・定期メンテナンス通知：原則として1か月前までに通知

25.個人情報保護

当社は、個人情報保護方針に基づき、個人情報の適切な取得・利用・保管・廃棄を実施しています。

・利用目的の範囲内で利用

・法令に基づく場合を除き第三者提供を実施しない

・アクセス制御および暗号化による保護

・安全管理措置の継続的改善

26.外部委託・サプライチェーン管理

当社では、外部委託およびサプライチェーン管理に関する基準を整備しています。

業務上必要となる委託先については、適切な評価および管理を実施しています。

主な管理内容は以下の通りです。

・委託先選定基準による評価

・契約管理

・機密保持契約（NDA）締結

・セキュリティ要件確認

・定期的な見直し

・必要に応じた監査

また、委託先に対しては、適切な情報管理および安全管理措置を求めるとともに、必要に応じてお客様への通知を実施します。

27. データ削除

契約終了後、当社所定の手順に従い、お客様データを削除します。

主な対応内容は以下の通りです。

・原則として翌月初に削除

・本サービス上に記録された利用者データを削除対象とする

・データ消去ツールによる上書き消去または暗号化消去を実施

・資産除去時には、必要に応じて物理破壊等を実施

・復元不可能な状態でデータを廃棄

28. 免責事項

本書は、当社における情報セキュリティ対策の概要を説明することを目的としており、特定のセキュリティ要件への適合または完全な安全性を保証するものではありません。

また、本書に記載された内容は、法令改正、サービス仕様変更、セキュリティ対策強化等に伴い、予告なく変更される場合があります。

改訂履歴

版	改訂日	改訂内容
1.0	2026/06/18	初版発行

この資料に関するお問い合わせ

株式会社メディア４ｕ

運営・開発本部　運営グループ

sms-support@media4u.co.jp

別紙１

経済産業省「クラウドサービスレベルのチェックリスト」

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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日提供
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	1か月前までにメールにて事前連絡
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	有り。 サービス終了または大幅な仕様変更の場合、1か月前までにメールにて事前連絡
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	有り。 メインの国内データセンターで復旧不可能なトラブルが発生した場合、代替拠点に保管しているバックアップデータからサービスを復旧させる体制を整えている
5		サービス稼働率	サービスを利用できる確率（計画サービス時間ー停止時間）÷計画サービス時間	稼働率（%）	目標値：99.99%、実績値：約99.99%。 原則としてSLA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	■ 復旧・サポート体制の整備 状況体制の有無: 災害発生時のシステム復旧・サポート体制を整備済み ■ データセンター基盤 施設選定: 災害対策に優れ、物理的セキュリティが整ったデータセンターを利用 ■ BCP（事業継続計画）体制 ◆ 冗長化構成 メインセンター: 日本国内のメインデータセンターを運用 代替拠点: 日本国内の代替拠点データセンターを確保 ◆ 復旧方法バックアップ復旧: 代替拠点に保管したバックアップからのサービス復旧 復旧条件: メインセンターに復旧不可能トラブル発生時に実行 ■ サポート体制 代替サポート: サポート体制も代替拠点を用意
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	有り。 別環境での代替アカウント発行。障害の内容に応じて提案可能な内容があれば提案しますが、SMS以外の代替手段は貴社内での検討を推奨。
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）	代替措置（別環境での代替アカウント発行）における具体的な提供データ形式に関する記載はありません。
9-1		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	■ アップグレード方針の整備状況 方針の有無: パッチ適用やシステム改修の方針を策定済み ■ 脆弱性監視・収集体制 ◆ 継続的診断 毎日診断: Webおよびプラットフォームの脆弱性診断を毎日実施 専門情報収集: セキュリティ専門ベンダから脆弱性情報を収集 迅速対応: 対応すべき脆弱性を可能な限り速やかに解決 ■ パッチ管理方針 ◆ 緊急度別対応 緊急パッチ: セキュリティに直ちに影響する・脅威となる緊急度の高いパッチを速やかに適用 定期パッチ: 緊急性が高くないパッチも定期的なプロセスに従って適用

アプリケーション運用

No.	種別	サービスレベル項目	規定内容	測定単位	設定
9-2	可用性	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	◆ 適用プロセス 統一方針: システム取得・開発・保守における統一的な方針 承認統制: 緊急度判定→対応期日決定→リスク軽減策実施→承認プロセスを経て適切に実施 ■ 製品ライフサイクル管理 サポート切れ対策: サポート切れ製品は使用せず 計画的更新: サポート終了が近い場合はバージョンアップ等を計画・実施 ■ 変更管理・品質保証 ◆ リリース管理 手順書整備: リリース作業手順書を整備 テスト確認: テスト環境での影響確認後に承認を得て実施 ◆ セキュリティテスト 開発時テスト: セキュリティ機能のテストを開発期間中に実施 ■ 報告・管理体制 月次報告: 脆弱性対応状況をセキュリティ管理責任者等に月次報告
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	1時間
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	目標復旧時間(RTO)は2時間。目標復旧時点(RPO)は1日。
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	サービス停止の事故歴はありません
13-1		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	■ システム監視基準の設定状況 基準の有無: システム監視基準を設定し、基準に基づく監視を実施済み ■ 基本システム監視 ◆ 監視項目 ping監視・Service Port監視・プロセス監視・リソース（CPU・Memory・Disk）監視・ログ監視を各サーバに対し実施 ◆ 監視頻度 基本間隔: 5分間隔で実施 ■ セキュリティ監視体制 ◆ 24時間365日監視 不正アクセス監視: IPS/IDS・WAFによる検知・遮断状況を24時間365日監視 即時対応: 不正アクセス発生時即時対応が必要なシステムに対し24時間体制で監視を実施 ◆ 日次監視・分析 イベントログ: 少なくとも日次で監視・分析 FW通信ログ: ファイアウォール通信ログ（遮断ログ）を日次で確認 不正ログイン: WAF・IPS・認証ログ等により監視 ■ 高度な監視・検知システム ◆ 相関分析・統合監視 相関分析: 各種ログを相関的に分析し、セキュリティ機器単体で検知できないサイバー攻撃を検知 可能

アプリケーション運用

No.	種別	サービスレベル項目	規定内容	測定単位	設定
13-2	信頼性	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	◆ 専門的監視システム EDR監視: 不正コード実行や不審な通信の検知・遮断状況をモニタリング 改竄検知: Webサイトの改竄検知システム導入済み メール監視: メールゲートウェイやメールサーバでのウィルス検知状況をモニタリング ■ 運用監査・証跡管理 ◆ 定期監査 ログ監査: サービス提供に必要なインフラに対する外部攻撃や内部不正検知のため、定期的にログや運用証跡を監査 ◆ 監視方針・手順 方針策定: インシデントの兆候確認のため定期的なログ監視方針を策定 手順標準化: ログ確認方法・頻度を検討 ■ 稼働状況監視 サーバ監視: サーバーの稼働状況を監視し、障害・異常を検知可能 ネットワーク監視: ネットワークの稼働状況を監視し、障害・異常を検知可能
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	有り。障害発生時通知は電子メールによる通知。
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	目安として検知後30分以内。
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）	5分間隔。
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	なし
18-1		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	■ 提供可能ログの整備状況 提供の有無: 利用者に提供可能な各種ログを整備済み ■ 利用状況・操作ログ ◆ 基本操作ログ 操作ログ: 5年間保存、利用者自身で管理画面からCSV出力可能 ◆ 詳細操作記録 ログイン履歴・各画面の操作履歴・データ出力履歴を記録 保存期間: アクセス者IDの操作ログを5年間保管 ■ 認証・アクセスログ ◆ ログイン記録記録内容: すべてのユーザーのログイン記録（ログインID、ログイン日時、アクセス元IPアドレス） 保存期間: 1年以上保管 提供方法: アカウントアクティビティ画面からCSV出力可能 ◆ 認証ログ 成功・失敗: 認証成功および認証失敗ログを取得 ID利用記録: ID利用時にシステムに対して行われた操作の記録を取得 セキュリティ調査: 不正アクセスや外部への不審な通信の調査を行えるようログを取得 ■ ファイル操作ログ 記録内容: 操作したユーザー、操作日時、該当ファイル名、アップロード/ダウンロードの別を記録 保存期間: 1年以上保管 提供方法: 利用者（契約者）の画面からの操作により取得（ダウンロード）が可能

アプリケーション運用

No.	種別	サービスレベル項目	規定内容	測定単位	設定
18-2	信頼性	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	■ 通信・送信ログ ◆ SMS送信履歴 送信記録: SMS送信履歴を1年間保存、利用者自身で管理画面からCSV出力可能 ◆ 送信履歴ログ 各種送信: 送信履歴のログを1年間保持 ■ システム管理ログ 管理者操作ログ: システム管理者のログ（メンテナンス作業、特権ID利用時、Domain Adminsグループのログイン履歴）も取得 ■ ログ定義・取得方針 記録要件: 情報システム利用にあたって記録すべき内容を定義し、ログ取得
19	性能	応答時間	処理の応答時間	時間（秒）	1～2秒
20		遅延	処理の応答時間の遅延継続時間	時間（分）	該当する情報が見つかりません
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）	レコード数によって変動する。最大15分
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
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	有り（限定的）。 Microsoft Azureを利用したシングルサインオン(SAML)に対応。APIの暗号化方式はTLS1.2/1.3、認証方式はBasic認証またはアクセストークン。
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）	無制限ですが、「二重ログイン不可」オプションが有効な場合は除きます
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	コンピュータリソース（CPU等）の使用状況を毎日観測し、業務上支障をきたさない十分なキャパシティを確保している

サポート

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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	■ 通信・送信ログ ◆ SMS送信履歴 送信記録: SMS送信履歴を1年間保存、利用者自身で管理画面からCSV出力可能 ◆ 送信履歴ログ 各種送信: 送信履歴のログを1年間保持 ■ システム管理ログ 管理者操作ログ: システム管理者のログ（メンテナンス作業、特権ID利用時、Domain Adminsグループのログイン履歴）も取得 ■ ログ定義・取得方針 記録要件: 情報システム利用にあたって記録すべき内容を定義し、ログ取得
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	一般問い合わせ窓口の営業時間10時～19時です。

データ管理

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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	■ バックアップ実施状況 実施の有無: 利用者データのバックアップを実施済み ■ バックアップ内容・頻度 ◆ バックアップ対象 データベース: データベースを全てバックアップ 業務データ: システム障害やランサムウェアに備え、業務データ、プログラム、ドキュメントのバックアップを取得 ◆ 実施頻度・方法 毎日実施: 利用者データのバックアップを毎日実施 自動実行: バックアップは毎日自動で実施される 定期取得: 定期的に取得 ■ バックアップ方式・保存管理 ◆ 保存方式 正副取得: バックアップは正副を取得 分離保存: 本番環境からネットワークが分離された環境で保存 別装置・媒体: 対象データとは別の装置・媒体に保存 ◆ 保存条件定義 方式定義: データ特性やサービスレベルに応じた適切なバックアップ方式、保存サイクル、保存期間を定義 ■ データ保管場所・セキュリティ ◆ 保管場所 国内データセンター: 国内データセンター内のバックアップサーバーに保管 ◆ セキュリティ対策 接続制限: バックアップに使用する装置・媒体はバックアップ時のみ接続 変更防止: バックアップはユーザ権限で変更・削除ができない ■ 利用者データのアクセス権・所有権管理 ◆ アクセス権限 バックアップデータ: バックアップデータへのアクセス権は利用者になし ◆ データ提供・取得 アカウント設定: アカウント設定情報等はCSVでダウンロード可能
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。目標復旧時点(RPO)は1日。
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	1年間
31-1		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	■ データ消去実施状況 実施の有無: サービス解約後のデータ消去を実施済み ■ データ消去のタイミング・方法 ◆ 消去タイミング 契約終了時: 契約終了時に弊社によりアカウント削除実施 データ削除: 原則として契約終了月の翌月月初にサイト上データ削除 ◆ 消去方法・範囲 完全削除: 利用者が本サービスを利用して記録した情報の一切を破棄 ■ データ移行・引き渡し対応 解約時オプション: サービス解約時に、利用者データの引き渡しとその後の完全削除、両方が可能

データ管理

No.	種別	サービスレベル項目	規定内容	測定単位	設定
31-2	データ管理	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	■ 物理媒体の破棄・廃棄 ◆ ハードウェア廃棄 完全削除: ハードウェア等廃棄・返却時、HDD内容を完全削除するか物理的破壊によって内部情報を復元不可能にして廃棄 ◆ 外部媒体管理 手続き管理: 定められた手続きに基づき、外部媒体の廃棄とその管理を実施 ■ 法的根拠・規約 利用規約明記: 利用規約に明記しており、サービス提供終了した時点で利用者が本サービスを利用して記録した情報の一切を破棄
32		バックアップ世代数	保証する世代数	世代数	365世代分を保管
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	■ 暗号化要件の整備状況 要件の有無: データ保護における暗号化要件を整備済み ■ データベース・保管データ暗号化 ◆ データベース暗号化 全データベース: データベースは全てAES-256で暗号化クラウドデータ: クラウド上のデータはデータベース単位で全てAES-256で暗号化 保管データ: 保管されている各種データは全てAES256で暗号化 ◆ バックアップデータ暗号化 バックアップ暗号化: バックアップデータはAES256で暗号化 ランサムウェア対策: ランサムウェア対策としてバックアップデータの暗号化およびアクセス制限を実施 ■ 個人情報・機密データ暗号化 個人情報DB: 個人情報DBは暗号化対策実施済み 電子ファイル: 個人情報が記録された電子ファイル等について、個人情報である旨表示、パスワード設定、暗号化 ■ パスワード・認証情報暗号化 平文禁止: パスワードは平文保存せず ハッシュ暗号化: 乱数と結合してSHA-256以上でハッシュ暗号化 ■ データ転送・出力時暗号化 ◆ ダウンロードデータ パスワード設定: ダウンロードデータにパスワード設定 ◆ 外部媒体暗号化 外部保存: 外部媒体に保存するデータは暗号化（アルゴリズム管理含む）
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	マルチテナントストレージにおけるキー管理要件という直接の記載はありません。テナント分離やアカウント権限設定により、他社データとの混在が生じないよう技術的に制御している。
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	有り。サイバー保険に加入。
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	有り。送信履歴やSMS本文テンプレート等の各種データをCSV形式でダウンロード可能。サービス解約時に、利用者データの引き渡しとその後の完全削除、両方が可能。

データ管理

No.	種別	サービスレベル項目	規定内容	測定単位	設定
37	データ管理	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	有り
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	有り（限定的）。ファイルアップロード機能（有料オプション）があり、ファイルの種類・フォーマットの妥当性やサイズのチェックを実施。

セキュリティ

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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	■ 公的認証取得状況 取得の有無: 情報処理管理に関する公的認証を取得済み ■ プライバシーマーク認証 取得状況: プライバシーマーク取得済み（認証番号：17001173(07), 有効期限：2026年6月3日） ■ ISMS関連認証 ◆ 基本ISMS認証 認証取得: ISMS (JIS Q 27001:2023(ISO/IEC 27001:2022)) 認証取得済み（認証登録番号：JP24/00000114 SGSジャパン株式会社 2024年4月14日取得） ◆ ISMSクラウドセキュリティ認証 クラウド認証: ISMSクラウドセキュリティ (JIP-ISMS517-1.0 (ISO/IEC 27017:2015)) 認証取得済み ■ 業界認定制度 認定取得: 「ASP・SaaS情報開示認定制度」で認定 (2023.03.30 認定) 認定番号：0277-2303
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	有り。 プラットフォーム診断・WEBアプリケーション診断を外部業者提供の専用ツールを利用して実施。システム取得、開発、保守プロセスでも脆弱性診断を実施。 新規構築時、大幅な変更・改修時、大幅な変更・改修がない場合（毎月定期実施）に外部専門業者契約の専用ツールで実施。
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	有り。 サービス運用場所は株式会社メディア4uオフィス内。個人情報を取り扱う業務及びシステムは入退館管理を実施している建物で行われている。外部の人員は許可無く入室できない、監視カメラ設置、映像記録。個人情報を扱う作業場所でのセキュリティ対策（施錠管理、入退室管理、監視カメラ、警備員、入館手続受付、出入り口制限）実施。
42		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 監査報告書は発行しておりませんが、必要な証跡がございましたら個別にご相談可能です。
43		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	有り。 マルチテナント環境におけるクラウドサービス利用者の使用する環境・資源間が分離され、貴社情報が貴社以外のテナント経由で持ち出せないようにしている。

セキュリティ

No.	種別	サービスレベル項目	規定内容	測定単位	設定
44	セキュリティ	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	有り。 担当者の所属・担当業務・職務権限に応じ、必要最小限のデータアクセスや業務処理機能が使用できるように、全てのIDの権限を定めています。本番環境のネットワークには認証された人員2名しかアクセスできません。
45		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	■ 通信暗号化強度の設定状況 設定の有無: システムとやりとりされる通信の暗号化強度を設定済み ■ 基本暗号化プロトコル ◆ 採用プロトコル TLS1.2/1.3: HTTPS 通信(TLS1.2/1.3)で全て暗号化 ◆ プロトコル制限 TLS1.2以上限定: TLS1.2以上のみを許可 ■ 通信種別別暗号化対応 ◆ API通信 API暗号化: APIの暗号化方式や強度はTLS1.2/1.3 ◆ 機器通信 機器-サーバ間: 機器からサーバーへのデータ通信もTLS1.2/1.3で暗号化 ◆ ブラウザアクセス SSL対応: ブラウザ等でサーバーにアクセスする際のSSL対応バージョンは TLS1.2/1.3 ■ 証明書・認証管理 ◆ サーバ証明書 信頼できる機関: SSL/TLSに利用するサーバ証明書は信頼できる機関から発行されたものを使用 ◆ 認証方式制限 匿名認証拒否: 匿名認証（ADH）による暗号化通信を拒否 ■ 通信制御・強制設定 ◆ HTTPS強制 HTTP禁止: 非暗号化通信（http）によるアクセスはできず HTTPS強制: httpsを強制するようにHSTSを設定 ◆ 外部ネットワーク対策 通信データ保護: 外部ネットワークにおける通信データ及び認証情報の漏えいを防止するために、通信データをTLS1.2以上で暗号化
46-1		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	■ トレーサビリティ体制の整備状況 体制の有無: セキュリティインシデント発生時のトレーサビリティを整備済み ■ IDの付与単位・管理 ◆ ID付与方針 個人別付与: ユーザ毎にIDおよびパスワードを発行共用ID禁止: 共用IDの使用を禁止 ◆ ID運用管理 日常点検: IDによるアクセス制限の場合、日常的な運用点検を実施（IDの不正使用点検、棚卸、パスワード定期変更など） ■ ログ検索・取得機能 ◆ ログ取得方法 利用者取得: 利用者（契約者）の画面からの操作により取得（ダウンロード）が可能 アカウント画面: アカウントアクティビティ画面から各種ログを取得可能

セキュリティ

No.	種別	サービスレベル項目	規定内容	測定単位	設定
46-2	セキュリティ	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	■ ログ保存期間・管理 ◆ 保存期間 5年間保管: アクセス者のIDの操作ログは5年間保管 オンライン保管: ログはオンラインで5年間保管 ◆ 保存内容 包括的記録: ログイン履歴、各画面の操作履歴、データ出力履歴を保存 ■ ログ管理・保護体制 ◆ 分離保管 専用サーバ: ログファイルは専用ログサーバに保存し、他のサーバや機器とは論理的または物理的に分離 ◆ セキュリティ対策 暗号化: ログやログのバックアップを暗号化 ■ インシデント対応・分析体制 ◆ 調査対応 不正アクセス調査: 不正アクセスや外部への不審な通信の調査を行えるようログを取得 早期発見: 不正または不適切なアクセスに繋がるログを収集・適時分析し早期発見 ◆ 分析機能 手順整備: ログを確認、分析できるよう手順や仕組みを用意 定期点検: 目的従った頻度でログを点検し、情報システムの安定稼働等を適時分析 ■ 利用者への提供体制 ◆ 提供条件 利用者ログ: 利用者ログはCSV出力可能 運用ログ: 運用担当者/例外処理ログは基本提出不可で個別相談 ◆ トレーサビリティ検証 十分な情報: 各種ログが、セキュリティインシデント発生時に原因究明・影響調査を適切に行うため十分な情報・トレーサビリティを持っていることを検証（ユーザID、種類、日時等を含む）
47		ウイルススキャン	ウイルススキャンの頻度	頻度	毎日。 ウイルス対策ソフト導入あり、毎日定義ファイル更新
48－1		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	■ 二次記憶媒体安全性対策の実施状況 対策の有無: 二次記憶媒体の安全性対策を実施済み ■ バックアップメディア暗号化 ◆ 暗号化保管 常時暗号化: バックアップデータはAES256で暗号化 ◆ 外部媒体暗号化 データ暗号化: 外部媒体に保存するデータは暗号化（アルゴリズム管理含む） ■ 廃棄時データ完全抹消・検証 ◆ 機器廃棄対策 完全削除: 機器廃棄時、HDD内容を完全削除するか物理的破壊によって内部情報を復元不可能にして廃棄 ◆ 書類・媒体廃棄 シュレッダー裁断: 個人情報が記録された書類、記録媒体の廃棄の際に、シュレッダーで裁断手続き管理: 定められた手続きに基づき、外部媒体の廃棄とその管理を実施

セキュリティ

No.	種別	サービスレベル項目	規定内容	測定単位	設定
48-2	セキュリティ	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	■ USBポート・データ吸出し制限 ◆ ポート無効化 USBポート無効化: USBポート無効化しており、吸出しを防止 ◆ 出力制御システム書き出し制限: 外部記憶媒体（USB・CD・DVD等）にも書き出しできないよう出力制御あり、専用ツールにて対策済み 原則禁止: 外部媒体への書き出し利用は原則禁止 ■ 検知・監視体制 ◆ 出力検知 検知システム: 外部媒体へ出力が行われた場合にそれを検知する対策（専用ツール、ログ点検）あり ◆ 管理者監視 ログモニタリング: 外部媒体への書き出しログを管理者がモニタリング ■ 予防的セキュリティ対策 ◆ データ保管制限 業務PC禁止: 原則として各自の業務パソコンに保管していない ◆ 自動機能制御 自動再生停止: 外部媒体接続時の自動再生機能を停止
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	把握済み。 データセンター専用建物は日本、関東および北海道に所在。 日本国法を遵守しております。

別紙2

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」

事業所・事業

No.	種別	サービスレベル項目	規定内容	内容
1	事業所等の概要	事業者名	事業者の正式名称（商号）	株式会社メディア４ｕ
2			法人番号	3010001115082
3		設立年月日	事業者の設立年月日（西暦）	2005年11月01日
4		事業所	事業者の本店所在地	株式会社メディア4uオフィス内 東京都港区赤坂1-11-30 赤坂一丁目センタービル9階
			事業者ホームページ	https://www.media4u.co.jp/
5	事業の概要	主な事業の概要	事業者の主な事業概要	SMS（ショートメッセージ）の法人向け送信サービス

人材

No.	種別	サービスレベル項目	規定内容	内容
6	経営者	代表者	代表者氏名	岩館　徹
7		役員	代表者経歴（生年月日、学歴、業務履歴、資格等）	ー
8	従業員	従業員数	正社員数（単独ベース）	32名

財務状況

No.	種別	サービスレベル項目	規定内容	内容
9	財務データ	売上高	事業者の売上高（単独ベース）	岩館　徹
10		経常利益	事業者の経常利益額（単独ベース）	メディア4u単体での決算情報につきましては、開示しておりません。 親会社である株式会社ファブリカホールディングスの決算情報（IR資料）を提出させていただく形となります。 以下のURLより決算資料をご確認ください。 https://www.fabrica-hd.co.jp/ir/library/financialresults
11		資本金	事業者の資本金（単独ベース）	同上
12		自己資本比率	事業者の自己資本の比率（単独ベース）	同上
13		キャッシュフロー対有利子負債比率	事業者のキャッシュフロー対有利子負債比率（単独ベース）	同上
14		インタレスト・カバレッジ・レシオ	事業者のキャッシュフロー対有利子負債比率（単独ベース）	同上
15	財務信頼性	上場の有無	株式上場の有無と、「有り」の場合は市場名	無し
16		財務監査・財務データの状況	該当する財務監査・財務データの状況を、以下より選択する。(1)会計監査人による会計監査、(2)会計参与による計算書類の作成、(3)「中小会計要領」の適用に関するチェックリストの活用、(4)監査役による監査、(5)いずれでもない	(4)
17		決算公告	決算公告の実施の有無	No.10と同じ

資本関係・所属団体

No.	種別	サービスレベル項目	規定内容	内容
18	資本関係	株主構成	大株主の名称（上位5株主程度）、及び各々の株主保有比率	株式会社ファブリカホールディングス　100%
19	所属団体	所属団体	所属している業界団体、経済団体等の名称	JUSA

コンプライアンス

No.	種別	サービスレベル項目	規定内容	内容
20	組織体制	コンプライアンス担当役員	コンプライアンス担当役員の氏名	森　一紘
21		専担の部署・会議体	コンプライアンスを担当する社内の部署・会議体の有無と、「有り」の場合は社内の部署名・会議体	有り 運営グループ
22		情報セキュリティに関する組織体制の状況	情報セキュリティに関する責任者の有無と、「有り」の場合は責任者名・役職	有り 運営グループ部長・早川隆史
			情報セキュリティに関する組織体制の有無	有り
23	個人情報	個人情報の取り扱い	個人情報の取り扱いに関する規定等の有無と、「有り」の場合は記載箇所	■規程の整備状況 - 規程の存在: 個人情報取扱いに関する規程を整備済み - 記載箇所: 「M4u_業務06_個人情報保護規程第２章 安全管理措置」に明記 - 法令遵守: 関係法令・ガイドライン等を遵守する旨を規定 ■管理体制 - 管理責任者: 個人情報保護管理者を設置 - 管理台帳: 個人情報取り扱い台帳（個人情報一覧表）を整備・管理 ■監査・監視体制 ◆日常的な管理 - 継続監視: 個人情報取扱状況の日常的なモニタリングを実施 ■定期的な監査 - 内部監査: 年1回のリスク分析表に基づく定期的な内部監査を実施 - 改善サイクル: 監査結果を踏まえた管理方針・管理規程の見直しを実行 ■継続的改善 - 定期見直し: 年1回の安全管理措置の定期的な見直しを実施 - 社会適応: 個人情報に対する社会通念の変化への対応 技術対応: 情報技術の進歩に応じた管理措置の更新
24	守秘義務	守秘義務契約	守秘義務契約に関わる契約又は条項の有無	無し 必須の場合は別途覚書で対応
			守秘義務違反があった場合のペナルティ条項の有無	無し

コンプライアンス

No.	種別	サービスレベル項目	規定内容	内容
25	従業員教育等	従業員に対するセキュリティ教育の実施状況	従業員に対するセキュリティ教育実施に関する取組状況	■基本的な教育体制 - 実施頻度: 年1回以上の従業員セキュリティ教育を定期実施 - 教育対象: 全従業員を対象とした包括的な実施体制 ■教育内容 ◆個人情報保護教育- 特定個人情報: 特定個人情報等の適正な取扱いに関する従業員教育を実施 - 内部規程周知: 従業員に対する内部規程等の周知・教育・訓練を年1回以上実施 ■脅威対策教育 - ランサムウェア対策: ランサムウェア対策に特化したセキュリティ教育を年1回以上実施 ■情報開示方針 - 基本方針: 従業員教育の取組状況について基本的には非開示 - 例外対応: 必須要件がある場合は個別相談により開示検討
26		従業員に対する守秘義務等の状況	従業員に対する守秘義務対応の取組状況	■ 契約締結状況 実施状況: 従業員に対する秘密保持契約締結済み 契約名称: 従業員等に対して雇用契約時に個人情報等秘密保持に関する契約（名称：「秘密保持契約」）を締結している ■ 情報開示方針 開示可否: 従業員に対する守秘義務対応状況の情報開示の可否と条件：あり
27	委託	委託情報に関する開示	サービス提供に関わる委託先（再委託先）の情報開示の可否と、可能な場合の条件等	再委託は実施しておりません
28		委託先に対する管理状況	自社の個人情報保護指針に対する順守規定の有無	再委託は実施しておりません
			委託先（再委託先）の個人情報保護等の状況に関する情報提供の可否と、可能な場合の条件等	再委託は実施しておりません
			委託先（再委託先）との守秘義務対応状況	再委託は実施しておりません
			委託先（再委託先）の管理方法	再委託は実施しておりません

コンプライアンス

No.	種別	サービスレベル項目	規定内容	内容
29	文書類	情報セキュリティ関する規定等の整備	情報セキュリティに関する基本方針・規定・マニュアル、リスクアセスメント結果等の状況と文書名	■ 文書整備状況 基本文書: 基本方針・規程・マニュアル等の状況と文書名：情報セキュリティ方針 ■ 情報公開・照会対応 照会可否: 規程等の内容に関する照会対応の可否と条件：弊社Webサイトにて照会可能
30		事業継続に関する規定の整備	事業継続に関する基本方針・規定・マニュアル等の有無と、「有り」の場合は文書名	有り（BCP対策を策定） 文書名：情報セキュリティ継続及びICT継続の管理マニュアル
			BCP対応計画及び運用手順等の開示の可否と、可能な場合の条件等	記載なし。BCP対策の概要として、メインの日本国内のデータセンターに復旧不可能のトラブルが発生した場合、日本国内の代替拠点データセンターにて保管しているバックアップからサービスを復旧する体制を整えています。
31		リスク管理に関する規定等の整備	リスク管理に関する基本方針・規定・マニュアル等の有無と、「有り」の場合の文書名	有り 文書名：製品及びサービスの利用に関するリスク管理マニュアル
32		勧誘・販売・係争に関する規定等の整備	勧誘・販売に関する基本方針・規定・マニュアル等の有無と、「有り」の場合は文書名	有り 文書名：利用規約
			係争に関する規定・管轄裁判所等、係争が生じた際の対応に関する情報を含む文書類の有無と、「有り」の場合の文書名	有り 文書名：利用規約
33		ASP・SaaSの苦情対応に関する規定等の整備	ASP・SaaSの苦情処理に関する基本方針・規定・マニュアル等の有無と、「有り」の場合はそれらの文書名	サービス窓口（苦情受付・問合せ）は特定個人情報の取り扱いがないため対象外
			ASP・SaaS事業者の事故責任の範囲と保証範囲が記述された文書の有無と、「有り」の場合は文書名	有り 利用規約にデータ漏えい、破壊時の補償に関する定めを明記
34		利用者による設定不備の抑止・防止に係る規程等の整備	サービス提供の際の利用者による設定不備を起こさせないための基本方針・規程・マニュアル等の有無と「有り」の場合は文書名方針等の文書の作成においては、「クラウドサービス利用・提供における適切な設定のためのガイドライン」における対策項目を参照すると良い。	利用者による設定不備を防止するため、サービス利用マニュアルおよび導入時のサポートを提供しています。また、必要に応じて担当者による設定内容の確認を実施しています。 専用の管理規程は整備しておりませんが、利用者が適切に設定可能となるよう運用支援を実施しています。

サービス基本特性

No.	種別	サービスレベル項目	規定内容	内容
35	サービス内容	サービス名称	本ASP・SaaSサービス名称	Aurora SMS
36		サービス開始時期	本ASP・SaaSのサービス開始年月（西暦）	2012年2月
			本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と、「有り」の場合は改変年月日（西暦）	無し
37		サービスの内容・範囲	本ASP・SaaSサービスの内容・特徴	SMS配信サービス
			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	利用していません
38		サービス提供時間	サービスの提供時間帯	24時間365日
39		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（契約内容に依存する場合はその旨記述）	有り
40		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（解約内容に依存する場合はその旨記述）	無し
41		マネージド・サービスやコンサルティング・サービスの提供	本サービスのシステム動作環境の設定や運用支援などをマネージド・サービスやコンサルティング・サービスとして提供しているか、または第3者の当該サービスを紹介しているかの有無。「有り」の場合はその概要	有り 本サービスの導入時における設定支援および運用に関する技術サポートを提供しています。ただし、顧客環境の運用代行や常駐型のマネージドサービスは提供していません。
42		ＡＩサービス基本事項（ＡＩポリシー）	ＡＩサービスに対する基本的な考え方。透明性、公平性、安全、セキュリティ、プライバシー保護、倫理など	現時点でSMS配信サービスにおいてAI機能の提供は行っていませんが、今後AIを利用する場合には、透明性、公平性、安全性、セキュリティ、プライバシー保護および倫理性に配慮し、関連法令およびガイドラインに準拠した運用を行います。
43	責任分担	ＡＩ機能に関連する責任分担	人間の判断の有無、ＡＩによる判断に基づく損害賠償責任など責任分担にかかわる事項	現時点でSMS配信サービスにおいてAIによる自動判断機能は提供していません。今後AI機能を提供する場合は、人間による適切な確認・判断を前提とした運用を行い、責任分担についても利用規約等で明確化します。
44	データ及び学習済みモデルの権利	利用	利用者が入力したデータの利用の有無、内容同意の取得方法など	現時点ではAI機能を利用していません。今後AI機能を導入する場合は、利用者データの利用目的や学習利用の有無等を利用規約等に明記し、適切な同意取得および管理を行います。
45		権利関係	利用者データに関する権利（所有権、使用権、著作権、肖像権など）利用者データを使った追加学習後の学習済みモデルの権利	現時点ではAI機能を利用していません。今後AI機能を導入する場合は、利用者データの利用目的や学習利用の有無等を利用規約等に明記し、適切な同意取得および管理を行います。

サービス基本特性

No.	種別	サービスレベル項目	規定内容	内容
46	サービスの変更・終了	サービス名称	利用者への告知時期（事前の告知時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述）	■ 基本告知期間 告知時期: 1か月前 ■ 告知対象・方法 ◆ システムメンテナンス 対象: 定期的な保守等で計画停止がある場合 告知期間・方法: 1か月前までにメールにて事前連絡 ◆ 重要な変更 対象: サービスが終了するまたは大幅な仕様変更がある場合 告知期間・方法: 1か月前までにメールにて事前連絡
			告知方法	電子メール
47		サービス（事業）変更・終了後の対応・代替措置	対応・代替措置の基本方針の有無と、「有り」の場合はその概要	■ BCP（事業継続計画）対策 ◆ データセンター障害対応 主要対策: BCP対策として、メインデータセンターのトラブル時に代替拠点データセンターでバックアップからサービスを復旧する体制 ◆ 災害時対応 復旧方針: 災害発生時のシステム復旧方針およびサポート体制あり ■ 重大障害時の代替措置 代替手段: 重大障害発生時、もし早期復旧が不可能な場合の代替措置として別環境での代替アカウント発行
48	契約の終了等	情報の返却・削除・廃棄	契約終了時の情報資産（利用者のデータ等）の返却責任の有無と、受託情報の変換方法・ファイル形式・費用等	データ引き渡し可能。メディアSMSから出力されるデータ形式はCSV形式が主。費用については記載なし。
			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	■ 情報開示方針 - 開示可否: 情報の削除・廃棄方法の開示が可能 - 開示条件: 特別な条件設定なく開示対応 ■ データ削除・廃棄の体制 ◆ アカウント・サイトデータ削除 - 削除実施: 契約終了時に事業者によりアカウント削除を実施 - 削除時期: 原則として契約終了月の翌月月初にサイト上データを削除 - 一時ファイル: テンポラリーファイル（アップロードファイル等）は1年で自動削除 ◆ ハードウェア・記憶媒体の廃棄 - データ消去: 利用企業のデータ消去を適切に実施 - 記録管理: 廃棄またはリース返却の記録を保管 - 物理的消去: 消磁等による物理的データ消去を実施 ◆ 外部媒体・書類の廃棄 - 外部媒体: 定められた手続きに基づく管理体制 - 書類廃棄: 個人情報が記録された書類・記録媒体はシュレッダーによる裁断処理
			削除又は廃棄したことの証明書等の提供	必要に応じてデータ削除証明書を提供

サービス基本特性

No.	種別	サービスレベル項目	規定内容	内容
49	サービス料金	料金体系	初期費用額	提供内容や契約条件に応じて異なるため、別途担当営業よりご案内します。
			月額利用額	提供内容や契約条件に応じて異なるため、別途担当営業よりご案内します。
			最低利用契約期間	なし
50		解約時違約金支払いの有無	解約時違約金（利用者側）の有無と、「有り」の場合はその額	契約期間内の解約であれば残月分の月額料金を精算して頂く必要があります。
51		利用者からの契約事前受付期限	利用者からのサービス解約の受付時期の有無と、「有り」の場合はその期限（何日・何ヶ月前かを記述）	1ヶ月前
52	サービス品質	サービス稼働設定値	サービス稼働率の目標値	99.99%
			サービス稼働率の実績値	約99.99%
			サービス停止の事故歴	無し
53-1		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と、「有り」の場合は、検知の場所、検知のインターバル、画面の表示チェック等の検知方法	■ 検知体制 検知の有無: システムリソース不足等による応答速度低下の検知体制を整備済み ■ リアルタイム監視 ◆ 監視項目・方法 ping監視・Service Port監視・プロセス監視・リソース（CPU・Memory・Disk）監視・ログ監視を各サーバに対し実施 ◆ 監視インターバル 監視間隔: 5分間隔で実施 ■ 定期分析・観測 ◆ 日次監視 対象・頻度: システムリソース（CPU等）の使用状況を毎日観測 ◆ 月次分析 分析対象: コンピュータリソースの使用状況（システム、サーバ、通信回線装置、通信回線の稼動／負荷状況、メモリやディスクの逼迫、障害の発生／種別）を月1回以上定期的に分析 ■ キャパシティ管理 キャパシティ設定: コンピュータリソースのキャパシティはピーク時の18% - max used by 3 month statistic以下で余裕を持って割り振られている余裕率: 12% - max used by 3 month statistic ■ 障害検知機能 稼働監視: サービス稼働状況は監視しており、障害・異常を検知可能

サービス基本特性

No.	種別	サービスレベル項目	規定内容	内容
53-2	サービス品質	サービスパフォーマンスの管理	ネットワーク・機器等の増強判断基準又は計画の有無、「有り」の場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要	■ 増強判断基準・計画 - 計画の有無: ネットワーク・機器等の増強判断基準・計画を策定済み - 策定方法: コンピュータリソースの使用状況を定期的に分析し計画を策定 ■ 技術的措置の概要 ◆ 冗長構成による可用性確保 - ネットワーク機器: 主要なネットワーク機器の冗長構成 - ストレージ機器: ストレージ機器の冗長構成 - サーバ機器: サーバ機器の冗長構成 - システム全体: システム全体での冗長構成を実現 ◆ サービス継続性対策 - サービス停止防止: サービスが停止しない仕組みを構築 - 負荷分散: 負荷分散による処理能力の向上 - 冗長化: 冗長化によるシステムの可用性確保 ◆ 障害影響最小化対策 - 重要機器の多重化: 障害による影響を小さくするための機器多重化 - データ分散保管: データの分散保管による障害リスクの分散 - 影響範囲限定: 障害発生時の影響範囲を最小限に抑制 ■ 情報開示状況 - 詳細情報: 具体的な判断基準や計画、技術的措置の詳細は非公開 - 基本方針: 基本的な取り組み方針のみ開示
54		認証取得・監査実施	プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1 等）の取得、監査基準委員会報告書第18号（米国監査基準SSAE16、国際監査基準ISAE3402）の作成の有無と、「有り」の場合は認証名又は監査の名称	■ 情報セキュリティ関連認証 ◆ ISMS認証 ●基本認証: JIS Q 27001:2023(ISO/IEC 27001:2022)認証取得済み - 認証登録番号：JP24/00000114 - 認証機関：SGSジャパン株式会社 - 取得日：2024年4月14日 ●クラウド拡張認証: ISMSクラウドセキュリティ認証取得済み - 基準：JIP-ISMS517-1.0 (ISO/IEC 27017:2015) ◆ プライバシー保護認証 ●プライバシーマーク: 取得済み - 認証番号：17001173(07) - 有効期限：2026年6月3日 ◆ 業界認定 ●ASP・SaaS情報開示認定制度: 認定取得済み - 認定日：2023年3月30日 ■ 監査報告書 ◆ 国際監査基準対応 - 18号監査（SAS70）等: 監査報告書作成なし ■ 監査協力体制 ◆ 監査受入れ対応 - Pマーク監査: 監査対応可能 - 情報セキュリティ関連監査: 協力可能 - データセンター監査: 監査対応可能

サービス基本特性

No.	種別	サービスレベル項目	規定内容	内容
55	サービス品質	脆弱性診断	脆弱性診断の有無と、「有り」の場合は、診断の対象（アプリケーション、OS、ハードウェア等）と、対策の概要	■ 診断実施体制- 診断の有無: 脆弱性診断を包括的に実施済み ■ 診断対象・範囲 ◆ 対象システム - プラットフォーム: プラットフォーム診断を実施 - アプリケーション: Webアプリケーション診断を実施 - OS・ミドルウェア: 脆弱性パッチ適用による対策 ◆ 診断手法 - 外部ツール: 外部業者提供の専用ツールを利用 - ペネトレーションテスト: 定期的な侵入テストを実施 ■ 診断頻度・スケジュール ◆ 定期診断 - 毎日実施: Web・プラットフォームの脆弱性診断 - 週次実施: 外部ツールによる診断（週1回） - 月次実施: 大幅変更がない場合の定期診断（毎月） - 年次実施: プラットフォーム・アプリ両方の検査（年1回以上） ◆ 最新実施状況 - 前回診断: 2026年5月実施 ■ 開発・変更時の診断 ◆ 新規構築時 - リリース前診断: 新規構築時はリリース前に必須実施 - 開発期間中: システム開発時のセキュリティ機能テスト実施 ◆ 変更・改修時 - 大幅変更時: 大幅な変更・改修発生時に診断実施 - 継続対応: アプリケーション開発時の包括的診断 ■ 対策の概要 ◆ パッチ管理 - 緊急対応: セキュリティに直ちに影響する高緊急度パッチの速やかな適用 - ベストエフォート: 脅威となるパッチのベストエフォート適用 ◆ 継続的改善 - 定期見直し: 診断結果に基づく継続的なセキュリティ向上 - 予防的対策: 脆弱性の早期発見・対処による予防的セキュリティ管理
56		システム動作環境の設定・診断に係る支援ツール等の提供	システム動作環境の設定や設定値の診断に係る支援ツール等提供の有無。「有り」の場合は、ツールの概要。	いいえ
57		学習コンテンツや学習機会の提供	システム動作環境そのものや設定に係る学習コンテンツもしくは講習会等の学習機会の提供有無。「有り」の場合はその概要	いいえ
58		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	毎日自動で実施される。サービスレベルに合わせて取得タイミングを定め、遠隔地にバックアップを保管。
			世代バックアップ（何世代前までかを記述）	1年（365日）

サービス基本特性

No.	種別	サービスレベル項目	規定内容	内容
59	サービス品質	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）	障害による影響を小さくするため、重要な機器の多重化、データの分散保管等の対策が導入されています。
60			DR（ディザスターリカバリー）対策の有無と、「有り」の場合はその概要	■ DR対策実施状況 対策の有無: ディザスターリカバリー対策を実施済み ■ データセンター基盤 施設選定基準: 災害対策に優れ、物理的セキュリティが整ったデータセンターを利用 ■ BCP（事業継続計画）体制 ◆ 復旧体制 メインセンター・代替拠点: BCP対策として、メインの日本国内のデータセンターに復旧不可能のトラブルが発生した場合、日本国内の代替拠点データセンターにて保管しているバックアップからサービスを復旧する体制 ◆ システム復旧方針復旧方針・サポート体制: 災害発生時のシステム復旧方針およびサポート体制あり ■ バックアップ戦略 ◆ 基本バックアップ 保管場所: バックアップの保管場所は国内データセンター内のバックアップサーバー ◆ 重要データ管理 遠隔地保管: 重要データについては、サービスレベルに合わせて取得タイミングを定め、遠隔地にバックアップを保管している
61		受賞・表彰歴	ASP・SaaSに関連する各種アワード等の受賞歴	ー
62		SLA（サービスレベル・アグリーメント）	本サービスに係るSLAが契約書に添付されるか否か	原則として稼働率に関するSLAは定めておりません。必須の場合は担当営業まで個別にご相談ください。
63	契約者数	契約者数	本ASP・SaaSサービスの契約企業数等	7,500社以上

アプリケーション等

No.	種別	サービスレベル項目	規定内容	内容
64	品質	ＡＩの精度	高い精度は実現するための環境条件など、ＡＩの精度に関わる情報	ー
65		ＡＩの精度向上策	追加学習の有無（有りの場合は時期、頻度、役割分担、料金など）	なし
66		説明可能性のレベル	ＡＩの出力結果の根拠の説明可能性のレベル（ホワイトボックス型／ブラックボックス型）	ー
67	連携	他のサービス・事業との連携状況に関する情報提供	他のサービスや事業との連携の有無と、「有り」の場合は情報提供の条件等	Salesforceやkintoneと連携し、SMS送信アプリを提供
68		ＡＩ関連の連携	ＡＰＩ等による他社のＡＩ機能の活用の有無、フレームワークやライブラリなどオープンソースの利用有無	ー

アプリケーション等

No.	種別	サービスレベル項目	規定内容	内容
69	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	■ 死活監視実施状況 監視の有無: 死活監視を実施済み 監視範囲: 死活監視およびサービスレベル監視として実施 ■ 監視対象・項目 基本監視: ping監視・Service Port監視・プロセス監視・リソース（CPU・Memory・Disk）監視・ログ監視を各サーバに対し実施 ■ 監視実行体制 監視頻度: 5分間隔を基本として実施
70		時刻同期	時刻同期への対応の有無と、「有り」の場合は時刻同期方法	■ 時刻同期実施状況 対応の有無: 時刻同期への対応を実施済み ■ 時刻同期の目的 記録精度: ログの取得にあたって、各イベントの時刻を正確に記録するため ■ 時刻同期方法 ◆ 同期プロトコル 使用プロトコル: NTP（Network Time Protocol）を利用 ◆ 基準時刻 時刻基準: 世界標準時刻（UTC）に合わせている ■ 同期対象機器 対象システム: NTPによってネットワーク上の各種サーバ・機器の時刻同期を実施。サーバやネットワーク機器のシステムクロックを同期
71		ウイルス対策	ウイルス対策の有無	■ ウイルス対策実施状況 対策の有無: ウイルス対策を実施済み ■ ウイルス対策ソフトウェア ◆ 基本機能 検知・駆除: ウイルス対策サービスを導入済み。ウィルス対策ソフトに既知の不正プログラムの検知・駆除、システムの保護を導入未知マルウェア対策: 未知のマルウェア検知対策ソフト（IDSおよびIPS）導入 ■ 定義ファイル・スキャン管理 ◆ 定義ファイル更新 更新頻度: パターンファイルの更新間隔：毎日。ウィルス定義ファイルは毎日自動更新 ◆ スキャン実行 リアルタイムスキャン: リアルタイムスキャンは常時有効 フルスキャン: 定期的にウィルス対策ソフトウェアによるフルスキャンを実施 ■ メールセキュリティ ゲートウェイ・サーバ監視: メールゲートウェイやメールサーバでのウィルス検知状況をモニタリング

アプリケーション等

No.	種別	サービスレベル項目	規定内容	内容
72	セキュリティ	管理者権限の運用管	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	■ 管理手順の整備状況 手順の有無: システム運用部門の管理者権限登録・削除手順を整備済み ■ 情報開示方針 開示対応: 管理者認証に関する情報開示の可否と条件：可能(具体的な開示対象については個別にご相談ください。) ■ 管理者ID管理体制 ◆ ID付与・認証方式 個人別付与: システム管理用IDは個人別に付与、原則多要素認証 ID分離: 管理業務専用IDと日常業務IDは分けている ◆ 共用ID管理 使用者限定・記録: システム管理用IDを複数人で共用する場合は使用者を限定し、使用日時を明確に運用 ■ アカウント登録・削除プロセス ◆ 登録手順 申請ベース: アカウントの発行は申請ルールに基づき、発行され記録されている ◆ 削除手順 担当者交代時: システム担当者交代時、速やかに管理者用個人ID又は管理者権限を削除人事異動・退職対応: 異動または退職になったアカウントは、直ちに削除している
73ー1		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	■基本認証体制 - 2階層権限管理: 管理者権限とユーザー権限の2種類のみ - 個人ID原則: 共有ID使用禁止、ユーザー毎に個別ID・パスワード発行 - システム独自ID: インターネット経由アクセスではシステム特性を考慮した独自ID採用 ■多様な認証方式 - 基本認証: ID・パスワード- 多要素認証: メール認証、アクセストークン、2段階認証 - SSO機能: AzureAD・SAML対応（設定手順書完備） - IPアドレス制限: アクセス許可IP設定による制限 - ワンタイムパスワード: メールによるOTP機能 ■パスワードセキュリティ - 暗号化保存: SHA-256以上のハッシュ暗号化 - 複雑性要件: 8文字以上、数字・大文字・小文字・特殊文字各1文字以上 - 有効期間設定: 10～999日で設定可能 - アカウントロック: 2～10回の失敗でロック機能 ■アカウント管理プロセス - 申請ベース発行: 申請ルールに基づく発行・記録 - 即座削除: 異動・退職時の迅速なアカウント削除 - 定期確認: ID登録状況・権限付与状況の定期的確認手続き - 最小権限原則: 必要最小限の権限付与

アプリケーション等

No.	種別	サービスレベル項目	規定内容	内容
73−2	セキュリティ	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	■セキュリティ機能 - 自動ログアウト: 無操作15分で強制ログアウト - 同時ログイン禁止: 同一IDによる重複ログイン防止（2025年2月対応） - パスワード非表示: 入力時「＊」表示、表示・印刷不可 - アカウント有効期限: 期限設定・自動無効化機能 ■管理機能 - 管理画面提供: アカウントアクティビティ・ユーザーリスト確認機能 - パスワードリセット: 管理者による変更・利用者自身での変更対応 - 技術情報開示: 認証・ポリシー情報の個別相談による開示可能
74		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	■利用者向けログ機能 - SMS送信履歴: 1年間保存、管理画面からCSV出力可能 - 操作ログ: 5年間保存、管理画面からCSV出力可能 - ログイン記録: 1年以上保管（ログインID、日時、IPアドレス記録） - ファイル操作記録: 1年以上保管（操作者、日時、ファイル名、アップロード/ダウンロード区別） - 改ざん防止: すべてのログで改ざん不可の措置を実装 ■システム運用ログ管理 - 保管期間: オンラインで5年間保管 - 保護措置: 専用ログサーバに保存し、論理的・物理的に分離 - 時刻同期: NTPを利用してUTCに同期- 取得対象: アクセスログ、操作ログ、イベントログ、ファイアウォール通信ログ、WAF、IPS/IDS、認証ログ等 ■セキュリティ監視体制 - 24時間365日監視: 不正アクセス検知・遮断を常時監視 - 日次監視: イベントログ、FW通信ログの分析 - 相関分析: 各種ログを統合分析してサイバー攻撃を検知 - Webサイト改竄監視: 自動監視による早期検知 - EDR活用: 不正コード実行や不審な通信の検知・遮断 ■管理者監視 - 特権ID監視: 管理者アクセスを第三者がモニタリング - メンテナンス作業: アクセス管理システムでログ取得・管理 - クラウド連携: クラウド事業者による不正検知・通知機能
			システム運用に関するログの取得の有無と、「有り」の場合は保存期間	有り 5年間保存
			ログの改ざん防止措置の有無	有り ログファイルは専用のログサーバに保存し、他のサーバや機器とは論理的又は物理的に分離

アプリケーション等

No.	種別	サービスレベル項目	規定内容	内容
75	セキュリティ	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	■脆弱性監視・収集体制 - 毎日の診断実施: Web・プラットフォームの脆弱性診断を日次で実行 - 専門情報収集: セキュリティ専門ベンダからの脆弱性情報を継続収集 - 迅速対応原則: 対応すべき脆弱性は可能な限り速やかに解決 ■パッチ適用方針 ◆緊急度別対応 - 高緊急度: セキュリティに直ちに影響する脅威はベストエフォートで速やかに適用 - 通常緊急度: 定期的なパッチ適用プロセス（月1回程度）に従って適用 ■適用プロセス - 緊急度判定: 脅威レベルの評価・分類 - 対応期日決定: 適用スケジュールの策定 - リスク軽減策: 設定変更・WAF/IPSによる仮想パッチ実施 - 承認取得: 対象資産の重要性に応じた適切な承認 - 適用実施: パッチ適用・システム改修の実行 ■品質管理・記録保持 - テスト環境確認: パッチ適用前の影響確認を徹底 - 手順書整備: リリース作業手順書（申請・体制・戻し手順含む）を完備 - 変更記録: パッチ適用内容を記録し1年間保管 - 承認プロセス: 手順書に従った適用承認の実施 ■製品ライフサイクル管理 - サポート切れ対策: サポート終了製品は使用禁止、またはリスク評価・軽減策を策定 - 計画的移行: サポート終了予定製品の速やかなバージョンアップ・移行実施 - 最新バージョン維持: ソフトウェアの適切な管理による最新状態の維持 ■報告・管理体制 - 月次報告: 脆弱性対応状況をセキュリティ管理責任者へ定期報告 - 未適用管理: 緊急性評価・判明日・適用予定日の詳細報告 - 継続監視: 適用状況の継続的な追跡・管理
76-1		暗号化対策	暗号化措置（データベース）への対応の有無と、「有り」の場合はその概要	有り ■ 基本暗号化仕様 暗号化アルゴリズム: AES-256を利用 適用範囲: データベース全てAES-256で暗号化 保管データ: 各種データ全てAES256で暗号化 ■ 対象データ別の暗号化対応 ◆ 個人情報 個人情報DB: 暗号化対策実施済み 電子ファイル: 個人情報表示・パスワード設定・暗号化 特定個人情報: 該当無し ◆ システムデータ パスワード: 平文保存せず、ハッシュ値保存、ソルティング実施 バックアップデータ: AES256で暗号化

アプリケーション等

No.	種別	サービスレベル項目	規定内容	内容
76-2	セキュリティ	暗号化対策	暗号化措置（データベース）への対応の有無と、「有り」の場合はその概要	有り ■ 暗号鍵管理体制 管理: 手順・責任を文書化、アクセス権限制限、安全保管 ■ 法的準拠 日本国法遵守
77		設定不備防止対策	申請したサービスが該当する「クラウドサービス利用・提供における適切な設定のためのガイドライン」における「【評価項目】 a. クラウドにおけるセキュリティ設定項目の類型と対策」それぞれに対する設定不備防止対策の有無。「有り」の場合は、該当項目と設定不備防止対策の概要	いいえ
78		ＡＩ関連セキュリティ対策	ＡＩに特化したセキュリティ対策の有無	未利用のため対象外
79	性能	ＡＩ性能	推論時間等（利用者の操作に係わるもの）、（利用者が学習を行う場合は）学習時間	未利用のため対象外

ネットワーク

No.	種別	サービスレベル項目	規定内容	内容
80	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	グローバル専有ネットワーク
81		帯域	データ通信速度の範囲、帯域保証の有無	500 Mbit/sec
82	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	■ ファイアウォール導入体制 基本導入: ファイアウォール導入済み 多層防御: ネットワークへの不正アクセス防止対策（ファイアウォール、IPS等）を導入 ■ ネットワーク構成・境界防御 DMZ構成: インターネットとDMZの境界、及びDMZと内部セグメントの境界の各々にファイアウォールを導入 ■ 通信制御・アクセス管理 ◆ 内部通信制御 ユーザ端末間通信遮断: ファイアウォールのアクセス制御機能でユーザ端末間通信を遮断し、運用管理に必要な通信のみ許可 ◆ 外部通信制御 プロキシ経由限定: インターネット閲覧は組織内プロキシ通信のみ許可するよう、内部から外部へのフィルタリングルールを設計・設定 ■ 運用管理体制 定期的棚卸: ファイアウォールルールの定期的棚卸を実施不要ルール除去: ネットワーク機器の通信ルール棚卸を定期的に行い、不要フィルタリングルールがないか確認

ネットワーク

No.	種別	サービスレベル項目	規定内容	内容
83	セキュリティ	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と、「有り」の場合は対応方法	有り ■ 多層防御システム構成 IDS（侵入検知システム）: 不正侵入検知・早期検知により被害発生・拡大を防止 IPS（侵入防止システム）: 重要情報を大量保有し漏洩時影響が甚大なシステムに導入 WAF（Web Application Firewall）: 重要情報を大量保有し漏洩時影響が甚大なシステムに導入 ■ 導入方針・対象システム 基本防御: IDSとWAFによるネットワーク保護を実施 包括的対応: 不正アクセスを防止・発見できる仕組みとしてWAF,IDS,IPSを導入済み ■ 運用・監視体制 24時間365日監視: IPS/IDS, WAFによる不正アクセス検知・遮断状況を24時間／365日監視 ■ 最新化管理 定義ファイル更新: IPS等のセキュリティ機器に最新の定義ファイルが適用されている
84		ネットワーク監視	事業者とエンドユーザとの間のネットワーク（専用線等）において障害が発生した際の通報時間	死活監視を5分間隔で実施。サーバの稼働状況、ネットワークの稼働状況について監視を行い、障害・異常を検知可能です。
85-1		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	■認証方式 ◆基本認証 - ID・パスワード認証: 個人別ID原則、共有ID禁止 - システム独自ID: インターネット経由アクセス用の独自ID採用 ◆多要素認証 - 2段階認証: メール認証によるOTP機能 - アクセストークン: トークンベース認証 - IPアドレス制限: 許可されたIPからのアクセスのみ許可 - SSO機能: AzureAD・SAML対応（設定手順書完備） ■場所・装置からの接続制御 ◆ネットワークレベル制御 - IPアドレス制限: L3レベルでのアクセス制限、グローバルIPによる接続元制限 - リスクベース認証: アクセス元IPアドレスによる制限機能 ◆端末・システム制御 - 認証単位: ホスト・サーバシステム単位での個別認証 - 同時ログイン禁止: 同一IDでの重複ログイン防止（2025年2月対応） ■セキュリティ機能 ◆自動セキュリティ - 自動ログアウト: 無操作15分で強制ログアウト - アカウントロック: 誤入力許容回数設定によるロック機能 - 有効期限管理: アカウント有効期限設定・自動無効化

ネットワーク

No.	種別	サービスレベル項目	規定内容	内容
85-2	セキュリティ	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	◆パスワードセキュリティ - 強化機能: 複雑性・文字数・有効期間の設定可能- 暗号化保存: 全パスワードの暗号化保存 - 表示制限: パスワード表示・印刷不可、入力時「＊」表示 ■権限管理体制 ◆最小権限原則 - 顧客情報アクセス: 担当者の所属・業務・職務権限に応じた必要最小限付与- 特権ID管理: 管理ポリシーによる権限最小化、不用意な配布・拡散防止 - 開発用ID: 本番データ・プログラムへのアクセス制限 ◆ID管理プロセス - 申請ベース: 文書化されたルール・手順、承認・記録保存 - 定期棚卸: ID登録状況・権限付与状況の定期確認、不要アカウント削除 - 利用制限: 特権IDの申請・承認、使用期間制限 ◆監査・監視機能 - 操作ログ: アカウントアクティビティ画面での確認・CSV出力 - 不正利用検知: 特権IDの不正利用検知機能 - 管理画面: ユーザーリスト・アカウント状況の一覧確認 ◆運用管理 - 技術情報提供: 認証に係る技術情報の個別相談対応 - パスワードリセット: 管理者・利用者双方による変更機能 - システム管理用ID: 個人別付与、原則多要素認証、交代時の適切な権限削除
86		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	■ 基本暗号化仕様 暗号化プロトコル: TLS1.2/1.3を全面採用 通信方式: HTTPS通信(TLS1.2/1.3)で全て暗号化 対応範囲: TLS1.2以上のプロトコルをサポート ■ 通信種別別の暗号化対応 ◆ Webアクセス ブラウザアクセス: TLS1.2/1.3によるSSL対応 API通信: TLS1.2/1.3で暗号化、Basic認証またはアクセストークン ◆ データ通信 機器-サーバ間: TLS1.2/1.3で暗号化 個人情報送信: インターネット・無線LAN等で暗号化 FTPS: 利用なし ■ セキュリティ強化設定 ◆ プロトコル制限 TLS1.2以上限定: TLS1.2以上のみ許可 非暗号化通信拒否: 非暗号化通信(http)によるアクセスできない、HTTPS強制(HSTS設定) 匿名認証拒否: 匿名認証(ADH)による暗号化通信を拒否 ◆ 証明書管理 信頼できる証明書: SSL/TLSサーバ証明書は信頼できる機関から発行されたもののみ使用

ネットワーク

No.	種別	サービスレベル項目	規定内容	内容
87	セキュリティ	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と、「有り」の場合は認証の方法	有り Microsoft Azureを使用したシングルサインオン（SAML）をサポートしています。API暗号化方式：TLS 1.2/1.3。認証方式：基本認証またはアクセストークン
88		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）	■ネットワーク攻撃対策 ◆DDoS攻撃対策 - DOS/DDos攻撃対策: 専用の攻撃対策を実装 ◆不正アクセス対策 - 多層防御システム: WAF・IDS・IPSを統合導入 - 包括的防御: 不正アクセスの防止・発見を同時実現 ■ランサムウェア対策 ◆システム対策 - バックアップ暗号化: バックアップデータのAES暗号化 - アクセス制限: バックアップデータへの厳格なアクセス制御 ◆物理対策 - 物理的分離: バックアップデータの物理的隔離保管 ◆人的対策 - セキュリティ教育: 年1回以上の定期的なセキュリティ教育実施 ◆データ流出防止対策 - オンラインストレージ制御: ネットワーク機器によるインターネットストレージ接続制御 - アップロード制限: 不正なデータ流出を防止する接続制御 ■メールセキュリティ対策 ◆攻撃対策 - スパム対策: 不正メール・スパムメールの遮断 - DoS攻撃対策: メールを利用したDoS攻撃への対応 ◆認証対策 - 受信メール認証: SPF・DKIM・DMARC等による送信元検証 - 送信メール認証: 自社メールの正当性証明 ◆ファイル・内容対策 - 添付ファイル対策: 不審ファイルの自動ドロップ・暗号化 - メール無害化: 危険な要素の除去・無害化処理 ◆運用管理対策 - 上長承認: メール送信時の承認プロセス - モニタリング: メール通信の監視・記録 - 自動転送禁止: 意図しないメール転送の防止
89	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	無し
			ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲	無し
90		推奨帯域	推奨帯域の有無と、「有り」の場合はそのデータ通信速度の範囲	無し

端末

No.	種別	サービスレベル項目	規定内容	内容
91	ＰＣ等（操作端末）	推奨端末	パソコン、携帯電話等の端末の種類、OS等	■ リモートアクセス端末管理 ◆ 端末使用制限 使用可能端末: 会社支給端末のみ使用許可 個人端末禁止: 個人所有PC等の使用を禁止 要件定義: リモートアクセス利用端末の種類と要件（ウィルス対策、パスコード設定、無線LAN利用条件等）を定める ■ 社外持ち出し端末のセキュリティ対策 ◆ 高度セキュリティ機能 EDR・セキュアウェブゲートウェイ・統合アカウント管理・デバイス管理システムを導入 ◆ アクセス制御・認証 パスコードロック: 無操作10分でロック 権限制限: ローカル管理者権限不許可 多要素認証: 多要素認証実装 ◆ データ保護機能 暗号化: 重要データ暗号化・暗号鍵管理 遠隔制御: 端末紛失時の遠隔消去・追跡可能 業務継続防止: 紛失モード・アカウント無効化による業務継続不可 ■ 端末管理統制 ◆ 持ち出し制限・管理端末管理簿: 重要データ保持 端末は「端末管理簿」で管理 持ち出し記録: 社外持ち出しは記載、責任者が管理 ◆ 在高管理 突合せチェック: 端末管理簿と端末現物の突合せ確認
92			利用するブラウザの種類	Chrome/Safari/firefox/Edge の最新版

ハウジング（サーバ設置場所）

No.	種別	サービスレベル項目	規定内容	内容
93	施設建築物	建物形態	データセンター専用建物か否か	データセンター専用建物 データセンターファシリティスタンダード（日本データセンター協会）においてTier3相当のデータセンターを利用
94		所在地	国名、日本の場合は地域ブロック名（例：関東、東北）	日本、関東および北海道
			特筆すべき立地上の優位性があれば記述（例：標高、地盤等）	物理的セキュリティが整ったデータセンターを利用。耐火・対水害・対落雷など各種災害対策実装。事前にハザードマップにより所在地周辺の想定リスクを確認した上で、対策をとっています。
95	耐震・免震構造	耐震・免震構造	耐震数値	耐震性能 II 類相当。耐震度数 震度7（新耐震基準）

ハウジング（サーバ設置場所）

No.	種別	サービスレベル項目	規定内容	内容
96	施設建築物	耐震・免震構造	免震構造や制震構造の有無	■ 耐震構造実施状況 構造の有無: 制震・耐震・免震構造実施済み ■ 免震システム ◆ 免震装置 免震構造: 免震装置の地震時の応答に対応 ◆ 免震床システム免震床: 免震床設置 ■ 機器固定・転倒防止対策 コンピュータ機器・什器: コンピュータ機器及び什器などが移動、転倒しないよう固定、各種機器の床固定 ■ 建物・設備保護措置 落下防止対策: 地震による天井・壁・照明器具等の落下・損壊の防止措置 影響防止措置: 建物、設備、コンピュータ等への影響を防止する措置を実施
97	非常用電源設備	無停電電源	無停電電源装置（UPS）の有無と、「有り」の場合は電力供給時間	有り 5分間。停電に備え、UPS（無停電電源装置）を設置しています。
98		給電ルート	異なる変電所を経由した給電ルート（系統）で２ルート以上が確保されているか否か（自家発電機、UPSを除く）	異なる変電所を経由した給電ルートで2ルート以上確保
99		非常用電源	非常用電源（自家発電機）の有無と、「有り」の場合は連続稼働時間の数値	有り 無給油48時間。停電に備え、ガスタービン自家発電装置を設置しています。
100	消火設備	サーバルーム内消火設備	自動消火設備の有無と、「有り」の場合はガス系消火設備か否か	有り データセンターで防火、耐火対策を実施しています（ガス消火器設置を含む）。
101		火災感知・報知システム	火災検知システムの有無	有り データセンターで火災検知システム設置
102	避雷対策設備	直撃雷対策	直撃雷対策の有無	有り 耐火・対水害・対落雷など各種災害対策実装
103		誘導雷対策	誘導雷対策の有無	有り
104	空調設備	空調設備	空調設備（床吹き上げ空調、コンピュータ専用個別空調等）の内容	直接外気冷房方式もしくは間接外気冷房方式
105	セキュリティ	入退室管理等	入退室記録の有無と、「有り」の場合はその保存期間	有り 5年間。データセンターで入退室記録の確保と保存が行われています。重要データにアクセスできる区画の入退室記録を取得・保管
			監視カメラの有無	有り 重要データにアクセスできる区画に入退室を監視する防犯カメラ設置
			個人認証システムの有無	有り 生体認証有り。データセンターの入退管理設備には磁気カード・IDカード・指紋照合装置等による個人認証システムが含まれます。
106		媒体の保管	紙、磁気テープ、光メディア等の媒体の保管のための鍵付きキャビネットの有無	有り 外部媒体の保管：機密情報が記載された外部媒体は施錠保管されています。
			保管管理手順書の有無	有り 外部媒体等の作成・保管・廃棄に関するルールが決められています。

ハウジング（サーバ設置場所）

No.	種別	サービスレベル項目	規定内容	内容
108	セキュリティ	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（破壊侵入防止対策、防犯監視対策等）	■データセンター物理セキュリティ ◆建物・防犯対策 - 建物構造: 堅固な建物の利用 - 監視体制: 監視カメラ設置・警備員配置による24時間監視 - 入館管理: 入館手続受付窓口設置・出入り口制限による入館統制 ◆入退管理システム - 事前登録制: システム事前登録人員のみ入館可能 - リアルタイム監視: 入館者状況のリアルタイム確認 - 権限管理: 入退館資格付与・権限削除の適切な管理 ◆重要エリア・設備のセキュリティ - 出入口限定: データセンター・コンピュータ室等の出入口を1カ所に限定 - 入退管理設備: 入退管理設備・防犯設備の設置 - 認証システム: 磁気カード・IDカード・指紋照合装置による多重認証 - 外部者管理: 識別・本人確認・同行義務付け・私物持込制限 ◆サーバルーム特別対策 - アクセス制限: 顧客・決済情報保管サーバルームへの物理アクセス区画限定 - 要員最小化: 入室要員の最小限化- 持込・持出管理: 金属探知機・警備員による端末・外部媒体等の管理 - 施錠管理: サーバラック・ネットワーク機器ラックの施錠・鍵貸出記録 ◆防犯・防災対策 - 防犯監視: 警備員巡回・監視カメラ・非常通報装置・開閉感知センサー・振動感知器 - 防火対策: 自動火災報知設備・スプリンクラー・ガス消火器・耐火保管庫 - 防災組織: 組織整備・社員教育・訓練実施 - 地震対策: 免震装置・機器固定・床固定措置 ◆個人情報保護対策 - 作業環境: 入退館管理建物での業務実施・監視カメラによる監視 - 情報管理: 個人情報記録媒体の表示・分離保管・持出完全禁止 - 出力制御: 外部記憶媒体への書き出し防止・検知システム・ログ点検 - データ保護: ファイルパスワード設定・有効期限設定・DB暗号化 ◆システムセキュリティ - 外部脅威対策: セキュリティソフト・ファイアウォール・標的型攻撃対策 - ウイルス対策: 定義ファイル更新・脆弱性パッチ適用 - 利用統制: 離席時対策・フリーソフト制限・リモート接続禁止 ◆廃棄・処分セキュリティ - 物理的消去: ハードウェア・記憶媒体廃棄時の消磁等データ消去・記録保管 - 書類廃棄: 個人情報記録書類のシュレッダー処理

サービスサポート

No.	種別	サービスレベル項目	規定内容	内容
109	サービス窓口（苦情受付・問合せ）	連絡先	電話／FAX、Web、電子メール等の連絡先	問い合わせ窓口が設置されています。サービス窓口（苦情受付・問合せ）は特定個人情報の取り扱いはないため対象外
			代理店連絡先の有無と、「有り」の場合は代理店名称、代理店の本店の所在地と連絡先	無し
110		営業日・時間	営業曜日、営業時間（受付時間）	問い合わせ窓口の営業日・時間、サポートダイヤル、Mailアドレスが明記されています。
111		サポート範囲・手段	サポート範囲	管理画面操作やAPI連携について対応
			サポート手段（電話、電子メールの返信等）	電話もしくは電子メール
112	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）	定期的な保守等で計画停止がある場合は1か月前までにメールにて事前連絡
			告知方法	メールにて事前連絡
113		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 通知方法：電子メールによる通知。 利用者への通知時間：目安として検知後30分以内。
114		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）	■インシデント発生時の通知・対応体制 ◆利用者への通知体制 - 連絡方法: メールによる連絡体制 - 通知内容: 発生事実・原因・被害状況の速やかな報告 - 詳細報告: 可能な限り詳細なアナウンスメールによる情報提供 - SLA: 原則としてSLA（サービスレベル合意）は締結していない ◆ログ監視・検知体制 - 監視方針: インシデント兆候確認のための定期的ログ監視方針を策定 - 証跡保全: セキュリティインシデント調査に必要な証跡をログで取得 - 検知システム: インシデント検知・対応トリガーとなるツール・プロセスを整備 ◆24時間監視・対応 - 即時対応: 不正アクセス発生時の即時対応が必要なシステムを24時間体制で監視 - EDR活用: 不正コード実行・不審通信の検知・遮断状況をモニタリング - 定例手順: 検知時の定められた手順による対応実施 ◆調査・分析基盤 - トレーサビリティ: インシデント時の原因究明・影響調査に十分な情報・トレーサビリティを検証 - 調査基盤: IoC（侵害指標）から不正ファイル・不正通信の調査が可能な仕組み構築 - 脅威確認: 外部入手IoC等による自社システム内脅威の確認 - 相関分析: 各種ログの相関分析によるセキュリティ機器単体では検知困難なサイバー攻撃の検知

サービスサポート

No.	種別	サービスレベル項目	規定内容	内容
114−2	サービス窓口（苦情受付・問合せ）	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）	◆障害対応・復旧措置 - 代替措置: 重大障害時・早期復旧困難時の別環境での代替アカウント発行 - サービス復旧: 目標復旧時間（RTO）を定めた範囲での復旧実施 - 復旧目標: 目標復旧時点（RPO）1日、目標復旧時間（RTO）2時間 ◆開発段階対策 - セキュリティテスト: 開発期間中のセキュリティ機能テスト実施
115		定期報告	利用者への定期報告の有無（アプリケーション、サーバ、プラットフォーム、その他機器の監視結果、サービス稼働率、SLAの実施結果等）	無し