Lumo

セキュリティと安全性について

データ保護・AI/LINE連携を含む安全設計と運用体制

リトルヘルプ・エージェンシー合同会社

発行日：　2026年4月3日
最終更新日：2026年7月18日

目次

1. はじめに

1.1 本書の目的

Lumoは、LINEマーケティングのAIエージェントです。お客さまに安心してご利用いただけるよう、本書ではLumoのセキュリティに関する取り組みを包括的にまとめています。

- **安心してご利用いただくために**
  Lumoが企業水準のセキュリティ基準を満たしていることをお伝えします

- **セキュリティ評価の根拠資料として**
  お客さまの社内セキュリティチェックや第三者評価の際に、エビデンスとしてご活用いただけます

1.2 対象サービス・適用範囲

本書は以下のサービスおよびシステムを対象としています。

- Lumo管理画面（Webアプリケーション）
- Lumo API（管理用API / 公開API）
- AIエージェント機能（マーケティングエージェント / カスタマーエージェント）
- LINE連携機能（Webhook受信 / メッセージ配信 / LINE Login）
- CRM連携機能（HubSpot / Shopify / Klaviyo）
- 決済連携機能（Stripe / Paid）
- 関連するクラウドインフラストラクチャ

1.3 本書がカバーするフレームワーク

本書は、以下の主要なセキュリティフレームワーク・ガイドラインの項目を網羅する形で構成しています。

フレームワーク	発行元	カバー範囲
クラウドサービスレベルのチェックリスト	経済産業省	可用性、信頼性、性能、拡張性、サポート、データ管理、セキュリティの 7カテゴリ
ASP/SaaS情報開示指針	総務省	事業運営、人材、コンプライアンス、サービス特性、ネットワーク等の主要項目
安全なウェブサイトの作り方	IPA（情報処理推進機構）	SQLインジェクション、XSS、CSRF等のWebアプリケーション脆弱性対策
OWASP Top 10 for LLM Applications 2025	OWASP	プロンプトインジェクション、データ漏洩、エージェント制御等のAI固有リスク

各セクションと準拠フレームワークの詳細な対応関係は付録Aをご参照ください。

1.4 用語・表記

用語	説明
GCP	Google Cloud Platform。Lumoが利用するクラウドインフラ基盤
Cloudflare	CDN・DDoS防御・TLS終端等を提供するエッジセキュリティプラットフォーム
VPC	Virtual Private Cloud。仮想プライベートネットワーク
TLS	Transport Layer Security。通信暗号化プロトコル
AES	Advanced Encryption Standard。データ暗号化規格
WAF	Web Application Firewall
RBAC	Role-Based Access Control。ロールベースアクセス制御
LLM	Large Language Model。大規模言語モデル
RAG	Retrieval-Augmented Generation。検索拡張生成

1.5 改訂履歴

バージョン	日付	変更内容
1.0	**2026年4月3日**	初版発行
1.1	**2026年7月16日**	AI処理の実行リージョンに関する記載を明確化
2.0	**2026年7月17日**	実装強化の反映と記載精度の全面改善
2.1	**2026年7月18日**	サポートアクセスの制限・記録に関する記載を追加、記載精度の改善

2. サービス概要と認定・認証

2.1 Lumoの概要

Lumoは、LINEマーケティングのAIエージェントです。使うほどお客さまを理解し、最適化した施策を導き出します。
前身プロダクト「LITTLE HELP CONNECT」で長年培った運用の知見を活かし、LINEおよびHubSpotを熟知したエンジニアリングチームが開発しています。

主な機能:

- **メッセージ配信**: AIによる配信メッセージ生成、セグメント配信、シナリオ配信、A/Bテスト
- **分析**: AIによる顧客属性の分析・提案、配信結果の分析・改善提案
- **自動化**: AIによる自動化設定サポート、ワークフロー管理
- **チャット:** AIによる問い合わせ対応、チャット文自動生成
- **CRM連携**: HubSpot、Shopify、Klaviyo

2.2 運営会社情報

項目	内容
会社名	リトルヘルプ・エージェンシー合同会社
英文名	Little Help Agency LLC
所在地	〒100-0004 東京都千代田区大手町 2-2-1 新大手町ビル3階 xLINK内
設立	2019年1月15日
資本金	500万円
代表者	川野忍（Shinobu Kawano）
事業内容	LINEマーケティングの AIエージェント「Lumo（ルモ）」の開発・運営・提供

2.3 取得認定・認証一覧

Lumoおよび運営会社は、以下の認定・認証を取得しています。

プライバシーマーク（Pマーク）

個人情報の取り扱いについては、第三者機関からの認証を受けています。一般財団法人日本情報経済社会推進協会（JIPDEC）が認定するプライバシーマーク制度の認証を取得しており、JIS Q 15001に基づく個人情報保護マネジメントシステム（PMS）を適切に構築・運用しています。

- 認定番号: 第 25000199 (02) 号
- 認定機関: 一般財団法人日本情報経済社会推進協会（JIPDEC）
- 準拠規格: JIS Q 15001（個人情報保護マネジメントシステム — 要求事項）

2.3 取得認定・認証一覧

LINEヤフー認定テクノロジーパートナー

個人情報の取り扱いについては、第三者機関からの認証を受けています。一般財団法人日本情報経済社会推進協会（JIPDEC）が認定するプライバシーマーク制度の認証を取得しており、JIS Q 15001に基づく個人情報保護マネジメントシステム（PMS）を適切に構築・運用しています。

HubSpot認定テクノロジーパートナー

HubSpot, Inc.のテクノロジーパートナーとして認定されています。HubSpotのセキュリティ・プライバシー基準に準拠したアプリケーションを提供しています。

ISO 27001 / SOC 2 Type IIについて

ISO 27001（ISMS）およびSOC 2 Type IIについては、現時点では未取得です。事業の成長に応じて取得を検討してまいります。現在は、Pマーク認定、外部脆弱性診断の定期実施、および本書に記載する各種セキュリティ対策により、企業水準のセキュリティ体制を維持しています。

2.4 外部セキュリティ評価

外部専門機関による定期的な脆弱性診断

Lumoでは、外部の専門セキュリティ機関による脆弱性診断（セキュリティ診断）を定期的に実施しています。プロダクトの安全性を客観的に検証し、お客さまのデータを守るための重要な投資と位置づけています。

- **実施頻度**: 年1回以上（重大な機能追加時には随時実施）
- **診断範囲**: Webアプリケーション、API、インフラストラクチャ
- **診断内容**: OWASP Top 10を含む脆弱性スキャン、ペネトレーションテスト
- **対応方針**: 検出された脆弱性は重要度に応じて優先的に対応し、再診断にて改善を確認
- **診断結果の共有**: お客さまのセキュリティ審査において、診断結果のサマリをNDA締結のうえでご共有することが可能です。詳細は当社窓口までお問い合わせください
- 直近では、2026年4月に、外部の専門機関による第三者診断で指摘された12件の事項について、そのすべての是正を完了しています。検出から全件対応・再検証までを迅速に実施する体制を維持しています。

3.　責任共有モデル

クラウドサービスにおけるセキュリティは、サービス提供者とお客さまの間で責任を共有する形で成り立っています。ここでは、それぞれの責任範囲を明確にします。

3.1 Lumo（当社）の責任範囲

Lumoは以下の領域についてセキュリティ責任を負います。

- **アプリケーションセキュリティ**: セキュアなコード開発、脆弱性対策、入力検証、認証・認可の実装
- **データ保護**: 暗号化、バックアップ、テナント分離、データ保持・削除ポリシーの運用
- **インフラ構成管理:** クラウドリソースのセキュアな設定、ネットワーク分離、アクセス制御
- **運用セキュリティ**: 監視、ログ管理、インシデント対応、脆弱性管理
- **AI安全性**: AIモデルの適切な利用、データ取り扱い、出力品質管理
- **コンプライアンス**: 個人情報保護法、Pマーク規程への準拠

3.2 お客さまの責任範囲

お客さまには以下の領域について管理をお願いしています。

- **アカウント管理**: ログイン情報の適切な管理、二要素認証の有効化
- **アクセス権限管理**: ワークスペースメンバーの招待・削除、ロールの適切な設定
- **APIキー管理**: APIキーの安全な保管、不要なキーの削除
- **コンテンツ管理**: 配信コンテンツの適法性、著作権・商標の確認
- **個人データの取り扱い**: LINEユーザー等のエンドユーザーの個人データをLumoで取り扱う場合、お客さまの責任において適切な同意取得やプライバシーポリシーの整備等をお願いしています
- **利用規約の遵守**: 当社サービス利用規約および各連携サービスの利用規約の遵守

3.3 クラウドインフラ事業者の責任範囲

Google Cloud Platform（GCP）

GCPは以下の領域を担保しています。

- **物理セキュリティ**: データセンターの物理的保護、入退室管理、監視
- **ハードウェア**: サーバー、ストレージ、ネットワーク機器のセキュリティ
- **基盤ソフトウェア**: ハイパーバイザー、ホストOS、ネットワーク基盤の管理
- **認証**: SOC 1/2/3、ISO 27001/27017/27018、PCI DSS等の認証を取得

Cloudflare

Cloudflareは、Lumoの公開経路に対して主に以下の役割を担っています。

- **エッジセキュリティ**: DDoS防御、TLS終端
- **ネットワーク**: グローバルCDNネットワークの運用、可用性の確保
- **認証**: SOC 2 Type II、ISO 27001、PCI DSS等の認証を取得

4.　組織的・人的セキュリティ

長年の運用実績に裏打ちされた信頼性の高い体制で、お客さまのデータをお預かりしています。個人情報の取り扱いについては、第三者機関からの認証（Pマーク）を受けています。

4.1 情報セキュリティポリシー

情報セキュリティに関する基本方針を策定し、組織全体で遵守しています。

- **策定状況**: 策定済み（Pマーク認定に基づく個人情報保護方針として運用）
- **見直し頻度**: 2年に1回（Pマークの更新審査に合わせて実施）
- **対象範囲**: 全従業員、業務委託先を含む全関係者
- **基本原則**: 機密性・完全性・可用性の確保、法令遵守、継続的改善

4.2 情報セキュリティ管理体制

- **最高責任者**: 代表社員が情報セキュリティの最終責任を負う
- **個人情報保護管理者**: Pマーク規程に基づき個人情報保護管理者を設置
- **見直し**: 定期的な内部監査を実施し、継続的に改善しています

4.3 従業員のセキュリティ教育・訓練

- **実施頻度**: 年1回以上（入社時研修および定期研修）
- **対象**: 全従業員（正社員、契約社員、業務委託先を含む）
- **内容**:
  - 情報セキュリティポリシーの周知と理解度確認
  - 個人情報の取り扱い（Pマーク規程に基づく）
  - インシデント発生時の報告手順とエスカレーションパス
  - フィッシング・ソーシャルエンジニアリング対策
- **記録管理**: 教育実施記録を保管・管理しています

4.4 秘密保持契約（NDA）

- 全従業員との間で秘密保持条項を含む雇用契約を締結しています
- 業務委託先との間でもNDAを締結し、情報の取り扱いを制限しています
- 退職後も一定期間の秘密保持義務が継続します

4.5 委託先管理

- 業務委託先の選定に際しては、セキュリティ体制を評価しています
- 委託先との間でセキュリティ要件を含む契約を締結しています
- 個人データの取り扱いを第三者に再委託する場合は、お客さまへの事前通知とお客さまの書面による承諾を得たうえで実施します（データ処理規約 第6条）
- 定期的な委託先の管理状況の確認を実施しています

4.6 法令遵守

以下の法令・規格を遵守しています。

- **個人情報の保護に関する法律**（個人情報保護法）
- **JIS Q 15001**（個人情報保護マネジメントシステム — 要求事項）
- **電気通信事業法**（通信の秘密の保護）
- **不正アクセス禁止法**

Pマーク認定（第 25000199 (02) 号）を取得・維持することで、個人情報保護マネジメントシステムの適切な運用を第三者機関から継続的に評価されています。

越境データ移転について

Lumoは一部の外部サービスとの連携において、お客さまのデータの一部が日本国外のサーバーで処理される場合があります。これらのサービスはそれぞれSOC 2 Type II、ISO 27001等の認証を取得しており、適切なデータ保護措置を講じています。外部サービスへの送信データは、各サービスの機能提供に必要な最小限の範囲に限定しています。詳細は12. 外部サービス連携のセキュリティおよび付録Bをご参照ください。

5. インフラストラクチャセキュリティ

Lumoを支えるインフラは、Google Cloud PlatformとCloudflareを中心に構成しています。多層的なセキュリティにより、お客さまのデータを保護しています。

5.1 クラウド基盤（Google Cloud Platform）

LumoはGoogle Cloud Platformで安全に運用しています。

- **利用リージョン**: 東京（日本国内）
- **データ所在地**: 日本国内
- GCPの東京リージョンは、ISO 27001、SOC 2 Type II等の認証を取得した施設で運用されています

主なGCPサービスとして、サーバーレスコンテナ実行環境、フルマネージドデータベース、メッセージング基盤、シークレット管理、AI基盤、監視・ログ基盤等を利用しています。

5.2 ネットワークセキュリティ

- **仮想プライベートネットワーク（VPC）**: 独自のVPCを構築し、アプリケーション層とデータベース層をネットワークレベルで分離しています
- **データベースの非公開構成**: データベースはプライベートIPのみで構成し、インターネットから直接アクセスできない設計としています
- **アクセス制限**: データベースへの管理アクセスは、IAP(Identity-Aware Proxy)による認証を経た専用経路に限定しており、インターネットからの直接接続はできません
- **外部通信の制御**: 外部向け通信はNATゲートウェイを経由し、IPアドレスの管理と通信の制御を行っています

5.3 エッジセキュリティ（Cloudflare）

すべての公開サービスはCloudflareを経由しており、以下の保護・制御を実施しています。

機能	説明
DDoS防御	大規模な分散型サービス拒否攻撃を自動検知・緩和
TLS終端	エッジでのTLS終端によりHTTPS通信を保証
公開経路の集約	公開サービスへのトラフィックを Cloudflare経由に集約し、エッジでの制御・監視を容易にしています

5.4 通信の暗号化

すべての通信は暗号化され、保護されています（SSL/TLS）。

- クライアントとの通信はTLS 1.2以上で暗号化しています（エッジは最新のTLS 1.3にも対応）
- エッジの最小TLSバージョン（1.2以上）およびHTTPS強制の設定は、Terraform （Infrastructure as Code）で管理し、構成の変更履歴を追跡できるようにしています
- サービス間の内部通信もすべて暗号化されています
- HTTPでのアクセスは自動的にHTTPSにリダイレクトされます
- 平文（HTTP）での通信は一切許可していません

5.5 コンテナ実行環境

- サンドボックス化されたコンテナ環境で各サービスを実行しています
- 内部サービスへのアクセスはIAM認証で制限し、外部からの直接アクセスを遮断しています
- 負荷に応じた自動スケーリングにより、可用性を確保しています
- 各デプロイは新しいコンテナイメージとして実行され、既存環境を変更しません

6.　データ保護

データは契約単位で管理され、外部AIモデルの再学習には利用されません。お客さまのデータを適切に分類し、それぞれに応じた保護を実施しています。

6.1 データ分類

Lumoでは、取り扱うデータを以下の4段階に分類し、それぞれに応じた保護措置を講じています。

分類	例	保護措置
Critical（最重要）	パスワード、認証トークン、暗号鍵	ハッシュ化またはアプリケーションレベル暗号化、アクセスログ全件記録
High（高）	メールアドレス、電話番号、氏名、LINE情報	アプリケーションレベル暗号化、ワークスペース認証によるアクセス制御
Medium（中）	キャンペーンデータ、配信履歴、セグメント設定	ワークスペースアクセス制御、変更・削除のログ記録
Low（低）	公開設定情報、UIテーマ設定	標準アクセス制御

6.2 保存時の暗号化

データは自動で継続的にバックアップしており、保存時には複数層の暗号化を適用しています。

インフラレベル暗号化

- **データベース**: AES-256による保存時暗号化がGCPによって自動適用されています
- **ファイルストレージ**: AES-256による保存時暗号化がCloudflareによって自動適用されています

アプリケーションレベル暗号化

インフラレベルの暗号化に加え、機密性の高いデータにはアプリケーションレベルの追加暗号化を適用しています。

- **ユーザーパスワード**: 業界標準のハッシュアルゴリズムでハッシュ化。平文での保存は行いません
- **認証トークン・秘密鍵**: AES-256による暗号化
- **外部サービス連携の認証情報**: AES-256による暗号化
- **APIキー**: 一方向ハッシュで保存（平文は保存しません）

6.3 通信時の暗号化

- すべての外部通信はTLS 1.2以上で暗号化しています
- 内部サービス間通信も暗号化しています
- 平文（HTTP）での通信は一切許可していません

6.4 データの保管場所

データ種別	保管場所
データベース	GCP東京リージョン（日本国内）
ファイルストレージ	Cloudflare R2 アジア太平洋リージョン
バックアップ	GCP東京リージョン（日本国内）

お客さまのプライマリデータ（データベース）およびバックアップは日本国内に保管されます。
ファイルストレージ（画像等のアセット）はアジア太平洋リージョンに保管されます。

6.5 バックアップと復旧

自動バックアップ

- **バックアップ頻度**: 週次のフルバックアップに加え、継続的なバックアップ（PITR）を自動で実行しています。
- **ポイントインタイムリカバリ（PITR）**: 継続的なバックアップにより、任意の時点にデータを復旧できます。直近数分前の状態への復旧も可能です
- **複数世代の保持**: 複数世代のバックアップを保持し、障害時の復旧に備えています
- **削除保護**: 本番環境ではデータベースの削除保護機能を有効化し、誤操作による削除を防止しています

復旧目標

指標	目標値
RTO（目標復旧時間）	1時間未満
RPO（目標復旧地点）	5分未満

6.6 データ保持・削除ポリシー

- データ種別ごとに適切な保持期間を設定し、期間経過後にデータを削除しています
- 監査ログは本番環境で1年間保持しています。保持期間はCloud Loggingの保持設定により裏付けています

契約終了時のデータ削除

1. **即時の論理削除:** お申し出を受けた時点で、対象ワークスペースを即時に論理削除状態とし、すべてのアクセスを遮断するとともに、外部サービスとの連携を停止します
2. **30営業日の保全期間:** 誤操作や取り消しのお申し出に備え、30営業日の保全期間を設けます。この期間内であればデータを復旧できます
3. **物理削除:** 保全期間の経過後、データを物理的に削除します
4. **削除証明書の発行:** 物理削除の完了後、削除証明書を発行します。証明書には、対象ワークスペースの識別子、削除日時、削除対象のサマリを記載し、当社の署名を付与します（データ処理規約 第9条）
5. **バックアップからの消去:** 物理削除の後、バックアップに残存するデータも、バックアップの保持期間の経過(最長14週間)をもって完全に消去されます
6. 契約終了前にデータのエクスポートをご希望の場合は、当社窓口までご連絡ください

6.7 マルチテナントデータ分離

データは契約単位（ワークスペース単位）で厳密に分離されています。

- **データベースレベルの分離制約**: 原則としてすべてのテナントデータにワークスペースの紐付けを必須とし（運用テレメトリ等の明示的な例外を除く）、テナントをまたいだデータ参照を構造的に防止しています
- **CIでの機械的な強制:** すべてのSQLがワークスペース境界を満たしているかを継続的インテグレーション(CI)で自動検査し、スキーマ契約テストと併せてマージの条件としています。テナント分離を損なう変更は、リリース前に機械的に検出・拒否されます
- **自動テストによる検証**: テナント分離ポリシーへの準拠を自動テストで継続的に検証しています

7. 認証・アクセス制御

お客さまのアカウントとデータを守るため、Lumoでは複数の認証方式とアクセス制御を組み合わせています。

7.1 認証方式

認証方式	対象	説明
メール/パスワード	管理画面ユーザー	パスワードは業界標準のアルゴリズムでハッシュ化して保存
Google OAuth	管理画面ユーザー	Googleアカウントを利用したシングルサインオン
二要素認証（2FA）	管理画面ユーザー	ワンタイムパスワード方式による追加認証
APIキー	API利用者	ハッシュ保存、安全な検証方式
LINEログイン	エンドユーザー	LINEアカウントを利用した認証

7.2 多要素認証（2FA）

管理画面ユーザーは、アカウントのセキュリティを強化するために二要素認証を有効化できます。

- **方式**: 時刻ベースのワンタイムパスワード（TOTP、RFC 6238準拠）
- **対応アプリ**: Google Authenticator、Microsoft Authenticator等のTOTP対応アプリ
- **秘密鍵**: 安全な乱数で生成し、暗号化して保存

7.3 パスワードポリシー

- **複雑性要件**: 一定の文字数以上、英字・数字の混在を必須としています
- **保存方式**: 業界標準のハッシュアルゴリズムでハッシュ化。平文での保存は行いません
- **認証保護**: 二要素認証（TOTP）に対応し、ログイン認証では失敗理由の詳細を返さない設計により、認証情報の推測やアカウント列挙のリスクを低減しています

お客さまの社内ポリシーでより高い複雑性要件を求められる場合は、ユーザー側での強いパスワードの設定を推奨します。将来的に管理者側でのパスワードポリシーカスタマイズ機能の提供を検討しています。

7.4 セッション管理

- **トークンベース認証**: 業界標準のトークン形式を使用しています
- **有効期間**: アクセストークンおよびリフレッシュトークンに適切な有効期間を設定しています
- **Cookie保護**: HttpOnly（JavaScript非公開）、Secure（HTTPS限定）、SameSite=Laxを適用し、クロスサイトでの意図しないCookie送信を防止しています
- **多層的なCSRF防御:** SameSite属性に加え、認証にはBearer型トークンを用いるステートレスな方式を採用しています。この多層構成により、クロスサイトリクエストフォージェリ（CSRF）のリスクを低減しています」
- **即時無効化**: トークンの署名検証に加え、サーバー側でのトークン管理により、即時無効化が可能です

7.5 ロールベースアクセス制御（RBAC）

ワークスペース内のユーザーには、以下のロールと権限を設定できます。

ロール	権限
管理者	ワークスペースの全機能を利用できます。メンバーの招待・削除、ロールおよび権限の設定、請求・契約の管理、ワークスペースの削除といった管理操作も行えます
メンバー	管理者が個別に許可した機能のみを利用できます

メンバーに対しては、機能単位でアクセス権限を個別に付与・制限できます。
対象となる主な機能は、チャットフロー、テンプレート、タグ、配信、LINEアカウント、データベース、AIドキュメント、レポート、ワークフロー、チャット、分析などです。加えて、チャット（受信トレイ）については、担当するLINEアカウントの範囲を限定することもできます。なお、メンバーの管理・請求の管理・ワークスペースの削除といった管理操作は管理者ロールに限定されており、メンバーロールでは実行できません。

すべてのAPIリクエストにおいて、リクエストしたユーザーが対象ワークスペースのメンバーであることを検証しています。

7.6 APIキー認証

Lumo公開APIへのアクセスはAPIキーにより認証されます。

- **生成**: 暗号学的に安全な乱数でキーを生成
- **保存**: 一方向ハッシュで保存。平文のAPIキーは保存しません
- **安全な検証**: タイミング攻撃を防止する検証方式を採用しています

7.7 シークレット管理

- **管理基盤**: GCP Secret Managerを使用し、すべてのシークレットを一元管理しています
- **最小権限の原則**: サービスごとに必要最小限の権限のみを付与しています
- **キーレス認証**: デプロイプロセスでは長期間有効な認証キーを保持しない構成としています
- **環境分離**: 開発環境と本番環境で異なるプロジェクト・シークレットを使用しています
- **ローテーション方針**: シークレットは年1回の定期ローテーション、またはインシデント発生時に即時ローテーションを実施する方針としています

7.8 当社担当者によるアクセス制限（サポートアクセス）

お客さまからのお問い合わせ対応等のために、当社の担当者がお客さまのワークスペースへアクセスする場合があります。このアクセスには以下の制限と記録を適用しています。

- **許可リストによる限定:** サポートアクセスが可能な担当者は、許可リストで明示的に指定されたアカウントに限定されています
- **読み取り専用:** サポートアクセスは読み取り専用に制限されており、お客さまのデータの作成・変更・削除はできません。書き込み操作は技術的に拒否されます
- **全アクセスの記録:** サポートアクセスによる操作は、操作者・対象ワークスペース・日時・操作内容を含めてすべてセキュリティログに記録され、事後に追跡できます

8. アプリケーションセキュリティ

Lumoの開発では、セキュリティを開発プロセスのあらゆる段階に組み込んでいます。加えて、外部の専門機関による定期的な脆弱性診断を実施し、安全性を客観的に検証しています。

8.1 セキュア開発ライフサイクル

セキュリティを開発プロセスに組み込んだ開発体制を構築しています。

プロセス	内容
コードレビュー	すべてのコード変更は、リリース前に別の開発者によるセキュリティレビューを実施
静的解析	自動的なコード解析により、品質やセキュリティ上の問題を検出
依存関係管理	利用ライブラリの脆弱性を自動検知し、継続的にセキュリティを維持
自動テスト	リリース前に自動テストおよびビルド検証を実施
環境分離	開発・本番環境を完全に分離し、本番データへの不要なアクセスを防止

8.2 脆弱性診断

外部の専門セキュリティ機関による脆弱性診断を定期的に実施し、プロダクトの安全性を継続的に検証しています。

- **実施頻度:** 年1回以上（重大な機能追加時には随時実施）
- **直近の実施日**: 2026年度実施済み
- **診断種別**: Webアプリケーション診断、API診断、プラットフォーム診断
- **検出時の対応フロー**:
    - 脆弱性の重要度判定（Critical / High / Medium / Low）
    - 重要度に応じた修正期限の設定
    - 修正実施後の再検証
    - 経過の記録・管理
    - 直近の第三者診断では、指摘された12件の事項すべての是正を2026年4月に完了しています。

お客さまのデータを守るための重要な施策の一つとして、継続的に投資しています。

8.3 Webアプリケーション脆弱性対策

IPA「安全なウェブサイトの作り方」およびOWASP Top 10に基づき、以下の脆弱性対策を実施しています。

脆弱性	対策
SQLインジェクション	パラメータバインディングによるクエリ構築。ユーザー入力を直接 SQL文に結合しない設計
クロスサイトスクリプティング（XSS）	JSON APIレスポンス設計、セキュリティヘッダー、フロントエンドフレームワークによる自動エスケープ
クロスサイトリクエストフォージェリ（CSRF）	トークンベースのステートレス認証、Cookie保護属性（Secure、SameSite）の設定
OSコマンドインジェクション	外部コマンドの実行なし。すべての処理をアプリケーション内で完結
パストラバーサル	ファイルパスの直接指定なし。クラウドストレージのオブジェクトキーによる管理
セッション管理不備	暗号学的に安全なトークン生成、適切な有効期限設定、サーバー側でのトークン管理
クリックジャッキング	フレーム表示を拒否するセキュリティヘッダーの設定
アクセス制御の不備	ロールベースアクセス制御（ RBAC）およびワークスペース単位の認可チェック

8.4 入力バリデーション

すべてのユーザー入力に対して、複数層のバリデーションを実施しています。

- **リクエスト検証**: 形式・型のチェック（メール形式、文字数制限、必須項目等）
- **ビジネスルール検証**: プラン上限、リソースの存在確認、権限チェック等
- **データベース制約**: 整合性制約（NOT NULL、外部キー、一意制約等）による最終防御

8.5 Webhook署名検証

外部サービスから受信するすべてのWebhookに対して、送信元の正当性を暗号学的な署名検証または事前共有シークレットの照合により確認しています。

- **LINE**: 署名検証（ワークスペースごとに個別の秘密鍵で管理）
- **HubSpot**: 署名検証（最新方式の署名ではタイムスタンプ検証によるリプレイ攻撃防止を含む）
- **Shopify**: 署名検証（タイミング攻撃に耐性のある比較方式）
- **Stripe**: SDK組み込みの署名検証
- **Klaviyo**: 事前共有シークレットによる検証（タイミング攻撃に耐性のある比較方式）

署名検証に失敗したリクエストは即座に拒否されます。Paidについては、プル型（ポーリング）連携のためWebhookは使用していません。

8.6 負荷制御と可用性保護

- **エッジ保護**: すべての公開エンドポイントをCloudflare経由で公開し、DDoS防御の対象としています
- **非同期処理**: ジョブキューごとの同時実行数およびディスパッチレートを制御し、スパイク時の安定性を確保しています
- **外部API呼び出し**: AI基盤や外部連携先のレート制限に応じて、再試行およびバックオフ制御を実装しています

8.7 セキュリティヘッダー

以下のセキュリティヘッダーを、すべてのレスポンスに明示的に付与しています。

- **HTTP Strict Transport Security（HSTS）:** 常時HTTPS通信を強制します
- **X-Content-Type-Options（nosniff）:** MIMEタイプの推測（スニッフィング）を防止します
- **X-Frame-Options（DENY）:** フレーム内での表示を拒否し、クリックジャッキングを防止します
- **Referrer-Policy:** 外部サイトへのリファラー情報の送出を制御します

加えて、認証情報等の機密データを含むレスポンスには、キャッシュを抑止する制御を適用しています。

8.8 クロスオリジン制御（CORS）

ブラウザからのクロスオリジンアクセスは既定で閉鎖しており、APIは同一オリジン経由での利用を基本としています。

クロスオリジンでの許可が必要となる場合に限り、環境ごとに明示的な許可リストで対象オリジンを開放する構成としています。認証情報付きのクロスオリジン要求は許可していません。

9. AIに関するセキュリティ

AI推論および関連処理は、Google Cloudの企業向けAI基盤上で安全に実行しています。AIエージェントやお客さまのデータも適切に管理しています。本章では、OWASP Top 10 for LLM Applications 2025のフレームワークに基づき、AI/LLMに関するセキュリティ対策を説明します。

9.1 AIの利用方針と透明性

- **利用目的**: マーケティング施策の企画支援・実行・分析、LINE上での自動応答
- **透明性:** AIが生成したコンテンツであることをお客さまが認識できる形で提供します
- **人間による監督**: 重要な操作（メッセージ配信、ワークフロー作成等）にはユーザーの承認を必須としています

9.2.1 利用するAIモデルと実行基盤

LumoのAIエージェント機能は、Google CloudのGemini Enterprise Agent Platform（旧Vertex AI）上のGeminiに一本化されています。

- **プロバイダー**: Google（Gemini / Document AI）
- **モデル**: テキスト生成にはGemini、埋め込み生成にはGeminiのエンベディングモデルを使用しています
- **用途**: テキスト生成、埋め込み生成、文書OCR（ナレッジベース機能のみ。次ページ参照）
- **処理リージョン**: AIエージェントによるテキスト生成および埋め込み生成は、すべてGoogle Cloud東京リージョン（asia-northeast1）で実行します。チャット履歴・LINEユーザー情報・CRM連携データ等が、AI処理のために日本国外へ送信されることはありません
- **データ取り扱い**: Google Cloudの企業向けデータ保護ポリシーおよびデータ処理契約（DPA）に基づく
- **データの閉じた環境**: AI推論および文書OCRを含む関連処理はGoogle Cloudの企業向け基盤内で完結するため、一貫したセキュリティポリシーのもとで保護されています

9.2.2 お客さまが任意で有効化する機能について

以下の機能は、お客さまが明示的に有効化した場合にのみ動作します。既定では無効であり、有効化しない限りこれらの外部通信は発生しません。

- Web検索: AIエージェントが最新の情報を参照するために利用する検索APIです
- 外部エージェント連携（A2A）: お客さまが指定した外部のAIエージェントと連携する機能です

9.2.3 文書OCR（Document AI）の処理リージョンについて

AI関連の処理のうち、日本国外で処理が行われるのは本機能のみです。

- **対象機能**: ナレッジベース機能にお客さまがPDF資料を登録した場合の文書OCR（テキスト抽出）に限られます
- **処理リージョン**: 現時点ではGoogle Cloud Document AIの米国リージョンで処理しています。日本リージョンが利用可能になり次第、移行する予定です
- **送信されるデータ**: OCRの対象は、お客さまがナレッジベースに登録したPDFファイルの内容のみです。LINEユーザーの個人データ・チャット履歴・CRM連携データ等が本処理のために国外へ送信されることはありません
- **データの取り扱い**: OCR実行時に一時的に処理されるのみで、お客さまのデータがAIモデルの学習に利用されることはありません（Google Cloudの企業向けデータ保護ポリシーおよびDPAに基づく）
- **利用しない場合**: ナレッジベース機能にPDF資料を登録しない場合、本処理は一切発生しません。PDF以外の形式（テキスト、Markdown、CSV、Word文書、Webページ）の取り込みは、日本国内の自社処理基盤で完結します

9.3 顧客データの取り扱い

データは契約単位で管理され、外部AIモデルの再学習には利用されません。

- お客さまのデータは、AIモデルの学習・ファインチューニングには一切使用しません
- AIモデルへの入力は、対象ワークスペースのデータに限定されます
- AIの処理結果は対象ワークスペース内にのみ保存されます

9.4 テナント単位のデータ分離

- **ベクトル検索（RAG）のテナント分離**: 検索クエリにはワークスペース単位のフィルターを必ず適用し、他テナントのデータが検索結果に含まれないことを保証しています
- **ドキュメントストレージの分離**: アップロードされたドキュメントはワークスペースごとに分離して格納されます
- **会話履歴の分離**: AIエージェントとの会話履歴はワークスペース単位で分離されています

9.5.1 AIエージェントの安全設計

Human-in-the-Loop（人間による承認フロー）

AIエージェントが影響の大きい操作を行う場合、ユーザーの明示的な承認を必須としています。

承認が必要な操作の例:

- LINE配信メッセージの作成・スケジュール
- セグメントの作成・変更
- ワークフローの作成・有効化
- A/Bテストの作成

これらの操作はリスクレベルに応じて分類され、高リスク操作は必ずユーザーのプレビューと承認を経てから実行されます。

9.5.2 AIエージェントの安全設計

エージェントの権限制限

- 各AIエージェントが利用できる操作は明示的に定義されており、定義外の操作は実行できません
- カスタマーエージェントの操作は必要最小限に限定されています
- 会話のターン数に上限を設定し、無限ループを防止しています

自律度の制御（信頼スコア）

低リスクの操作に限り、実績に基づく信頼スコアに応じて自動実行の範囲を調整します。

メッセージ配信の送信およびワークフローの有効化は、信頼スコアの高低にかかわらず、常にユーザーの承認を必須としています。この不変条件が信頼スコアによって緩和されることはありません。

9.6 プロンプトインジェクション対策

- **システム指示とユーザー入力の分離**: システム指示とユーザーメッセージは構造的に分離し、ユーザー入力がシステム指示に干渉しない設計としています
- **操作パラメータの検証**: AIが出力した操作パラメータは、実行前にバリデーションを通過する必要があります
- **構造化された応答**: 操作結果は構造化データとして処理され、自由形式のテキストが直接操作に影響を与えません

9.7 出力の検証と品質管理

- **操作結果の構造化**: AIが行う操作の結果は、構造化データとして処理されます
- **LINE出力の安全な変換**: LINE配信用コンテンツは専用のフォーマッターを通じて安全な形式に変換されます
- **カスタマーエージェントの安全弁**: 自動応答の停止フラグにより、お客さまがいつでもAI自動応答を無効化できます

9.8 レート制限とリソース管理

- **外部APIレート制限対応**: AI基盤のAPI呼び出しに対して、自動的なリトライと流量制御を実装しています
- **会話ターン制限**: エージェントの会話ターン数に上限を設定し、リソースの過剰消費を防止しています
- **タイムアウト制御:** 外部通信には適切なタイムアウトを設定しています

9.9 AIの品質・安全性の観測

- AIエージェントの品質・安全性に関するテレメトリは、Google Cloud内（Cloud Trace）で完結する設計としています
- 品質評価のために会話の本文を収集しない設計とし、外部の観測サービスへ会話内容を送信することはありません

10. LINE連携のセキュリティ

LumoはLINEマーケティングツールとして、LINE公式アカウントとの連携がサービスの中核を担っています。LINEヤフー認定テクノロジーパートナーとして、LINEプラットフォームのセキュリティ要件を満たした安全な連携を実現しています。

10.1 LINEヤフー認定テクノロジーパートナー

LINEヤフー株式会社より、LINE公式アカウントの技術パートナーとして認定されています。認定にあたっては、LINEプラットフォームのセキュリティ要件および技術審査を通過しています。LINE Developersが提供するセキュリティチェックリストに準拠した実装を行っています。

10.2 Webhook受信の安全性

LINE PlatformからのWebhookは暗号学的な署名検証により、不正なリクエストを拒否しています。

- **署名検証**: すべてのWebhookリクエストに対して署名検証を実施し、LINE Platform以外からの不正なリクエストを排除
- **チャネルシークレットの分離管理**: ワークスペースごとに個別のチャネルシークレットを使用し、暗号化して保存しています。あるワークスペースのシークレットが他のワークスペースの検証に使用されることはありません

10.3 LINEユーザーデータの保護

- **LINE IDの管理**: LINEユーザーIDはワークスペース単位で管理され、テナント分離が適用されています
- **プロフィール情報**: LINEから取得したプロフィール情報（表示名、アイコン等）はワークスペース内でのみアクセス可能です
- **アクセストークン管理**: LINEチャネルアクセストークンは暗号化して保存しています
- **エンドユーザーのデータ削除対応:** LINEユーザー（エンドユーザー）の個人データについて、削除のご要望に対応する機能を備えています

10.4 メッセージ配信の安全性

- **配信前の承認フロー**: AIエージェントが作成した配信メッセージは、ユーザーがプレビューし承認するまで送信されません
- **セグメント配信の検証**: 配信対象のセグメント条件はワークスペース内のデータのみを参照し、他テナントのユーザーに配信されることはありません
- **配信コンテンツの安全な変換**: 配信コンテンツは専用のフォーマッターを通じてLINEの仕様に適合する安全な形式に変換されます

10.5 LINE Login

- **OAuth 2.0 / OpenID Connect準拠**: LINE Loginは標準的なOAuth 2.0 / OpenID Connectフローで実装しています
- **エンドユーザーの同意**: LINE Loginの利用時には、エンドユーザーに情報提供の同意画面が表示されます
- **取得情報の最小化**: LINE Loginで取得する情報はサービスの提供に必要な最小限の範囲に限定しています

11. 監視・ログ・インシデント対応

Lumoでは、サービスの安定運用とセキュリティ維持のために、継続的な監視体制を整えています。万が一のインシデント発生時にも、迅速に対応できる体制を構築しています。

11.1 ログ管理と監査証跡

- **構造化ログ**: JSON形式の構造化ログをクラウドログ管理基盤に集約しています
- **標準フィールド**: リクエストID、ユーザーID、ワークスペースID等を自動的に記録しています
- **分散トレーシング**: リクエストの処理経路を追跡し、問題の迅速な特定を可能にしています
- **個人情報の保護**: ログにはメールアドレス等の個人情報を直接記録せず、内部IDのみを記録しています
- **監査ログの保持**: 本番環境で1年間保持しています。保持期間はCloud Loggingの保持設定（Infrastructure as Codeで管理）により裏付けています
- **データアクセス監査ログ**: シークレット管理（Secret Manager）、アクセス管理（IAM）、データベース（AlloyDB）に対するデータアクセス監査ログを有効化し、特権的な操作の証跡を記録しています

11.2 監視・アラート

- **アプリケーション監視**: ダッシュボード、メトリクス、アラートによる継続監視
- **ログ監視**: エラーログの検知、ログベースアラート
- **分散トレーシング**: リクエスト処理経路の可視化、レイテンシ分析
- **稼働監視**: 公開サービスに対するHTTPヘルスチェック

11.3 インシデント対応手順

セキュリティインシデント発生時には、以下の手順に従って対応します。

フェーズ	内容
1. 検知・報告	監視アラートまたは担当者からの報告によりインシデントを認識。発見者はセキュリティ責任者に即時報告
2. 初動対応	影響範囲の特定、必要に応じたサービスの隔離・停止判断
3. 調査・分析	原因の特定、影響を受けたデータ・ユーザーの範囲確認
4. 復旧	システムの正常化、データの復旧
5. 通知	影響を受けたお客さまへの通知、法令に基づく報告（詳細は 11.4参照）
6. 再発防止	原因の根本対策、プロセスの見直し、対応記録の保管

11.4 セキュリティイベント通知

- セキュリティに影響するインシデントが発生した場合、影響を受けるお客さまに**72時間以内**に第一報を通知します
- 個人情報の漏洩等が発生した場合、個人情報保護委員会への報告を法令に基づき実施します（速報: 事態認知後3〜5日以内、確報: 法令の定める期限内「原則30日以内、不正アクセス等の事案は60日以内」）
- 通知方法: メール、管理画面上の通知、またはその両方
- インシデントの概要、影響範囲、お客さま側で推奨される対応を含む通知を行います

12. 可用性・事業継続

データは自動で継続的にバックアップしています。Lumoの安定したサービス提供のため、冗長構成と災害復旧の仕組みを整えています。

12.1 サービス稼働率（SLA）

- **目標稼働率**: 99.9%（月間）
- **サービス提供時間**: 24時間365日
- **稼働率の計算対象**: 計画メンテナンス時間を除く

12.2 冗長構成とオートスケーリング

- 主要サービスは常時複数インスタンスで稼働し、単一障害点を排除しています
- トラフィック増加時にはインスタンスが自動的にスケールアウトします
- 最小インスタンス数の設定により、コールドスタートの影響を最小化しています

12.3 バックアップと災害復旧（DR）

- **自動バックアップ**: 週次のフルバックアップ+継続バックアップ（PITR）により任意の時点への復旧が可能
- **本番環境の削除保護**: データベースの削除保護機能を有効化し、誤操作による削除を防止
- **RTO**: 1時間未満
- **RPO**: 5分未満

12.4 計画メンテナンス

- 計画メンテナンスが必要な場合は、事前にお客さまに通知します
- **通知期間**: 原則5営業日前まで（緊急の場合は可能な限り事前に通知）
- 可能な限りサービス停止を伴わないローリングデプロイを実施しています

13. 外部サービス連携のセキュリティ

Lumoは、LINE公式アカウントのほか、HubSpot、Shopify、Klaviyo、Stripe、Paidと接続し、お客さまのマーケティング活動を支援しています。各連携先との通信はすべて暗号化され、認証情報も安全に管理しています。LINE連携のセキュリティについては10. LINE連携のセキュリティをご参照ください。

13.1 利用する外部サービス一覧

カテゴリ	サービス	用途
メッセージング	LINE Platform	メッセージ配信、Webhook受信、LINE Login（詳細は10章参照）
CRM	HubSpot	コンタクト同期、ワークフロー連携
EC	Shopify	顧客・注文データ同期
マーケティング	Klaviyo	セグメント・キャンペーン連携
決済（カード）	Stripe	クレジットカード決済、サブスクリプション管理
決済（銀行振込）	Paid	銀行振込（請求書払い）決済
メール	SendGrid	トランザクションメール配信
AI	Google Cloud AI（Gemini Enterprise Agent Platform / Document AI）	テキスト生成、埋め込み生成、文書 OCR（OCRはナレッジベース機能のPDF資料のみ。詳細は 9章参照）
ヘルプ	Zendesk	ヘルプセンター連携

13.2 CRM連携（HubSpot / Shopify / Klaviyo）

- **OAuth 2.0認証**: 各CRMサービスとの認証にはOAuth 2.0を使用し、アクセストークンを安全に管理
- **トークンの暗号化保存**: OAuthトークンはアプリケーションレベルで暗号化して保存
- **Webhook署名検証**: 各サービスからのWebhookに対して署名検証を実施
- **HubSpot認定テクノロジーパートナー**: HubSpotのセキュリティ・プライバシー基準に準拠
- **GDPR Webhook対応**: HubSpotおよびShopifyからの必須GDPR Webhook（顧客データ削除要求等）に対応しています
- **連携トークンの再認証ガード**: 外部サービスの認可トークンの失効を検知した場合、該当の連携を安全に停止し、お客さまに再認証（再連携）を求めます。失効したトークンのまま処理が継続することを防ぎます

13.3 決済連携（Stripe / Paid）

Stripe（クレジットカード決済）

- **PCI DSS準拠**: カード情報はStripeが直接処理し、当社システムを経由しません
- **Webhook署名検証**: SDK組み込みの署名検証機能を使用
- **シークレット管理**: 認証情報はGCP Secret Managerで管理

Paid（銀行振込/請求書決済）

- **認証情報管理**: GCP Secret Managerで管理された認証情報を使用
- **通信暗号化**: すべてのAPI通信はHTTPS/TLSで暗号化
- **テナント分離**: 決済データはワークスペース紐付きの請求契約を通じてテナント分離を確保

13.4 外部サービスとの通信セキュリティ

- **すべての通信のTLS暗号化**: 外部サービスとの通信はすべてTLS 1.2以上で暗号化
- **シークレットの一元管理**: すべての外部サービスの認証情報はGCP Secret Managerで管理
- **キーレス認証**: デプロイプロセスでは長期キーを使用しない構成
- **イベント駆動アーキテクチャ**: 外部サービスからのイベントは受信と処理を分離し、外部サービスの障害がシステム全体に波及することを防止

14. お客さま向けセキュリティ機能

Lumoでは、お客さまご自身でセキュリティ設定をカスタマイズしていただけます。

14.1 利用可能なセキュリティ設定

管理画面から設定できるセキュリティ機能は以下の通りです。

機能	説明
二要素認証（2FA）	アカウントごとにワンタイムパスワード方式の二要素認証を有効化できます
メンバー権限管理	ワークスペースメンバーごとにロール（管理者　/ メンバー）と詳細権限を設定できます
APIキー管理	APIキーの発行・無効化を管理画面から実行できます
AI自動応答の制御	カスタマーエージェントの自動応答をユーザー単位で停止できます
AIエージェント操作の承認	マーケティングエージェントの高リスク操作は実行前に承認を求められます

14.2 推奨セキュリティ設定

Lumoをより安全にご利用いただくために、以下の設定を推奨します。

1. **二要素認証の有効化**: すべてのユーザーに対して二要素認証を有効化してください
2. **最小権限の原則**: メンバーには業務に必要な最小限の権限のみを付与してください
3. **APIキーの定期的な更新**: 定期的にAPIキーをローテーションしてください
4. **不要なメンバーの削除**: 退職・異動等で不要になったメンバーは速やかに削除してください
5. **パスワードの定期変更**: 定期的なパスワード変更を推奨します

付録A. 準拠フレームワーク対応表

経済産業省「クラウドサービスレベルのチェックリスト」

カテゴリ	対応セクション
可用性	12.1 サービス稼働率、12.2 冗長構成
信頼性	6.5 バックアップと復旧、11.3 インシデント対応
性能	12.2 冗長構成とオートスケーリング
拡張性	12.2 冗長構成とオートスケーリング
サポート	11.3 インシデント対応、11.4 セキュリティイベント通知
データ管理	6.1〜6.7 データ保護全般
セキュリティ	2.3 認定・認証、2.4 外部評価、5〜9 各セキュリティセクション

総務省「ASP/SaaS情報開示指針」

カテゴリ	対応セクション
事業運営	2.2 運営会社情報
人材	4.3 セキュリティ教育
コンプライアンス	4.6 法令遵守
サービス特性	2.1 サービス概要
アプリケーション	8. アプリケーションセキュリティ
ネットワーク	5.2 ネットワークセキュリティ、5.3 エッジセキュリティ
データセンター	5.1 クラウド基盤
サービスサポート	11.3 インシデント対応、12.4 計画メンテナンス
AI関連	9. AIに関するセキュリティ

IPA「安全なウェブサイトの作り方」

脆弱性カテゴリ	対応セクション
SQLインジェクション	8.3
OSコマンドインジェクション	8.3
パストラバーサル	8.3
セッション管理不備	7.4、8.3
XSS	8.3
CSRF	8.3
HTTPヘッダインジェクション	8.3
クリックジャッキング	8.3、8.7
アクセス制御の不備	7.5、8.3

OWASP Top 10 for LLM Applications 2025

項目	対応セクション
LLM01: プロンプトインジェクション	9.6
LLM02: 機密情報の漏洩	9.3、9.4
LLM03: サプライチェーン	9.2
LLM04: データ汚染	9.3、9.4
LLM05: 不適切な出力処理	9.7
LLM06: 過剰なエージェンシー	9.5
LLM07: システムプロンプト漏洩	9.6
LLM08: ベクトル/埋め込みの脆弱性	9.4
LLM09: 誤情報	9.7
LLM10: 制御されない消費	9.8

付録B. 利用外部クラウドサービス一覧

付録B. 利用外部クラウドサービス一覧

サービス	提供元	用途	データ所在地
Google Cloud Platform	Google LLC	アプリケーション基盤、データベース、AI基盤（Gemini Enterprise Agent Platform）、文書OCR	日本（東京リージョン）。ナレッジベース機能のPDF資料の文書OCR（Document AI）のみ米国（9.2.3参照）
Cloudflare	Cloudflare, Inc.	CDN、DDoS防御、TLS終端、ファイルストレージ	グローバル（エッジ）/ アジア太平洋（ストレージ）
LINE Platform	LINEヤフー株式会社	メッセージング連携	日本
HubSpot	HubSpot, Inc.	CRM連携	米国
Shopify	Shopify Inc.	EC連携	カナダ / 米国
Klaviyo	Klaviyo, Inc.	マーケティング連携	米国

付録B. 利用外部クラウドサービス一覧

サービス	提供元	用途	データ所在地
Stripe	Stripe, Inc.	クレジットカード決済	米国
Paid	株式会社ラクーンフィナンシャル	銀行振込決済	日本
SendGrid	Twilio Inc.	メール配信	米国
Zendesk	Zendesk, Inc.	ヘルプセンター	米国

付録C. お問い合わせ先

付録C. お問い合わせ先

セキュリティに関するお問い合わせは、以下までご連絡ください。

項目	内容
窓口	セキュリティ窓口（リトルヘルプ・エージェンシー合同会社）
メールアドレス	hq@littlehelp.co.jp
対応時間	平日 10:00〜18:00（日本時間）

脆弱性の報告やセキュリティインシデントに関するご連絡も、上記窓口で受け付けています。

関連文書

- Lumo利用規約
- データ処理規約（個人情報の取り扱いに関する契約）
- プライバシーポリシー

LITTLE HELP AGENCY

リトルヘルプ・エージェンシー合同会社

〒100-0004 東京都千代田区大手町2-2-1 新大手町ビル3階 xLINK内

https://www.littlehelp.co.jp