Lark プライバシーホワイトペーパー

はじめに

Lark が提供する次世代コラボレーションプラットフォームは、「モバイルフレンドリー 、リアルタイムな共同作業、データの一元管理」を特徴とし、お客様の作業効率を高め、生産コストおよび管理コストの削減をサポートします。

Lark は優れた機能とサービスを提供しています。メッセンジャー、Docs、ドライブ、カレンダー、音声・ビデオ会議、オープンプラットフォーム、メール、OKR、承認等を含むがこれらに限られません。各プロダクトは、高い拡張性と可用性を備えています。

Lark は、お客様のデータセキュリティおよびユーザーのプライバシー保護を重視しています。プロダクトの設計・開発において、セキュリティならびにプライバシーのコンプライアンスに関する要件に十分配慮し、プライバシー・バイ・デザイン（Privacy by Design）とプライバシー・バイ・デフォルト（Privacy by Default）の考えを貫徹し、世界各国のデータ保護法を満たすことを前提に、透明性、信頼性、安全性、効率性の高いコラボレーション体験をお客様へ提供します。

Lark は、プライバシー保護において様々な構築や考察を進め、大きな成果を上げてきました。このプライバシーホワイトペーパーを通して、この分野における Lark の基本理念・原則とプライバシー保護・管理の実践についてお伝えしたいと思います。

注：本文中の「お客様」とは、許可された自然人により Lark のアカウント登録が行われ、組織構造を構築して管理権限を与えられた法人その他の組織を指します。「ユーザー」とは、お客様が Lark で構築した組織構造にお客様の許可または招待を受けて加入し当サービスを利用する、チーム作成者や管理者などの自然人を指します。

1. Lark が遵守する個人情報処理の基本原則

Lark は、適用すべき法律に基づき個人情報処理の基本原則を確定し、適切な管理および技術的安全管理措置により個人情報処理の際に以下の基本原則を遵守します。

合法性、正当性、透明性

個人情報の処理は、合法性、正当性、透明性の原則を有するものとします。

目的の制限

個人情報の処理は、具体的で、明確な目的を有するものとし、データ処理の当初の目的に反してはなりません。

データの最小化

個人情報の処理は、処理目的の最小限の範囲とし、適切で関連する必要な方法を採用するものとします。

正確性

個人情報の処理は、正確であり、必要に応じて適時更新するものとします。データ処理の目的に基づき、合理的な措置を採用し不正確な個人情報を適時削除または修正します。

保管の制限

個人情報の保管は、処理の目的を実現するために必要な期間を超えてはなりません。

完全性と機密性

個人情報の処理は、適切な管理および技術的安全管理措置を採用し個人情報の安全性を確保するものとし、無許可のアクセス、修正から個人情報を守り、データの破損または紛失を回避します。

責任追跡性

データ処理とプライバシー操作関連のログを残す必要があり、必要に応じて上記原則

の遵守状況を開示することができます。

2. Lark プライバシー保護マネジメントシステム

2.1 プライバシー保護の組織とメンバー

コンプライアンスチーム

Lark は、同じ業務を展開する国家および地域をカバーする法務、セキュリティ等様々なコンプライアンス専門チームを設立し、プライバシー保護を含む各コンプライアンス実践のためにプロフェッショナルなサポートを提供し、責任事項にはデータコンプライアンスマネジメントシステムの構築、実行、最適化ならびに製品化データのコンプライアンス能力およびソリューションの構築等が含むがそれに限られません。Lark がグローバルデータコンプライアンスの法的要件を満たした上で、お客様へよりハイクオリティな製品コンプライアンスの機能およびサービスを提供します。

コンプライアンスの周知徹底と研修

Lark は、様々な形でメンバー全体にコンプライアンスの研修および周知徹底を定期的に実施します。内容は、グローバルデータコンプライアンスの法的要件に基づく教養研修ならびに重要ポジションの社員に対する特別研修が含まれ、社員全体のデータ保護における意識を高めさせ、コンプライアンスリスクを低減させます。

2.2 個人情報処理のライフサイクルマネジメント

データ収集

Lark は、合法性、正当性、透明性、最低限等の原則を厳格に遵守し、サービス提供に必要な個人情報を適切な方法、頻度で収集します。個人情報を収集する前に、プライバシーポリシーの中で収集する個人情報のタイプ、収集の目的および方法等の情報を開示しており、適用する法的要件に準拠し、ユーザーの同意を得ます。同時に、Lark も複数のプライバシー設定機能を提供しており、ユーザーはプライバシー設定項目からまたは Lark チームに連絡することで、付与された同意をいつでも撤回できます。

データの使用

Lark は、目的の制限等の原則を厳守し、収集した個人情報はお客様およびユーザーから許可を得た利用目的のみに使用します。Lark 社員は原則として、上記個人データに対するアクセス権限がありません。Lark 社員による操作はすべて厳格に制限および審査されます。

データの共有

Lark 上で取り扱われる個人データの開示は、私どものプライバシーポリシーに従って実施します。Lark がサードパーティーに個人データを共有する必要がある場合、サードパーティーのデータセキュリティの能力と資質を厳正に査定したうえで、Lark の高い基準に基づくデータ保護に努めることをサードパーティーに求めています。

データの保存と処分

私どもは、プライバシーポリシーに記載する目的の実現に必要な期間内においてのみ、お客様の個人データを保持いたします。ただし、法的な義務もしくは要件を遵守するため、法的な訴えの確立や行使や弁護を行うため、合法的な商業目的のため、または法律の規定に準拠するためなどで、長期間の保持が必要な場合を除きます。

2.3 データ主体の権利の保障

ユーザーは、所属法人へデータ主体の権利リクエストを提出でき、Lark による協力が必要な状況に関わる場合、法人はカスタマーサクセスマネージャーを通して協力して処理するよう Lark に連絡することができます。

Lark はコンプライアンス専門チームを配置して、上記データ主体の権利リクエストに対するレスポンスルートの管理運営を行っており、コンプライアンス要件に基づき所定の期間内にレスポンスが行われるよう努めています。

2.4 データレジデンシーと越境移転における管理

Lark は、お客様自身のデータレジデンシーに関するコンプライアンスをサポートするため、複数のデータセンターセンターを設立しました。下表は、データセンターのリージョンおよびサプライヤー関連の情報です。

国家	サプライヤー
シンガポール	Amazon Web Services
日本	Amazon Web Services
米国	Amazon Web Services

個人データの越境移転はすべて、法的およびセキュリティ面に関する厳格なコンプライアンス評価を実施します。このような越境移転については、すでに許可されている法的根拠および例外に依拠し、適用すべき法的要件を遵守しています。同時に、Larkはさらに適切な管理および技術的安全管理措置を採用し、データ伝送の過程におけるセキュリティを保障します。

2.5 プライバシーリスクマネジメント

プライバシー影響評価 (PIA)

Lark は、プライバシー・バイ・デザイン（Privacy by Design）およびプライバシー・バイ・デフォルト（Privacy by Default）の考えを広く徹底し、プライバシー保護の基本原則を製品全体の要件定義と設計、開発、運用プロセスに組み込んでいます。全ての個人データ処理に関する業務の機能またはシーンには、プライバシー影響評価を実施する必要があり、関わる個人情報の種類、処理の目的及び方法、データ主体の権利に生じ得る影響等に対してリスク評価を行います。識別された中および高リスク項目については、定められたリスク軽減措置に従いリスク対策を行い、プライバシーリスクを低減させる必要があります。

コンプライアンスチェック

Lark は、各バージョンのリリース前後に、厳格なコンプライアンスチェックにより、リスクの識別および処置を適時行い、お客様のデータのプライバシーとセキュリティを確保します。

各バージョンをリリースするまでは、アプリの静的解析を行います。バージョンがリリースされたら、モジュールのコンプライアンステストを定期的に実施します。識別された中および高リスクのセキュリティ脆弱性、プライバシーのコンプライアンス等の課題については、期日までに修復および改善をするよう手配します。

2.6 情報漏えい対策とインシデントレスポンス

Lark は、健全な情報セキュリティマネジメントおよびコーポレートガバナンスに関する制度プロセスを構築しており、ID 識別とアクセス管理、データの暗号化、非識別化、コンプライアンスチェック、侵入テスト、セキュリティ情報イベント管理プラットフォーム（SIEM）等の技術的解決手段およびツールを介して、情報漏えい事件の発生をできる限り回避します。

情報漏えい事件が発生した場合、セキュリティとコンプライアンス等のチームがインシデント管理プロセスおよび緊急時対応計画に基づき直ちに対応に当たり、適用する法的要件に基づき監督管理部門へ適時報告し、影響が及ぶ可能性のあるお客様、ユーザーまたは関連当事者へ通知します。また、インシデントの対応が完了した後さらにインシデントのレビューと総括を行い、改善措置を採用して類似的なインシデントの再発を回避します。

2.7 データセキュリティ

Lark は、お客様のデータセキュリティを重要視しております。「お客様のデータはお客様によってコントロールする」というコンプライアンスの観点を持ち、様々な管理および技術的解決手段によりデータセキュリティを保障します。

データマネジメントプロセスにおいて、データの格付け・分類とデータ暗号化の基準が高い制度を確立し、大規模なデータのラベル付け作業をセットで進め、上記を効果的に実行できるようにしています。技術的解決手段においては、先進的な暗号化技術を採用し、サーバー側の暗号化およびエンドツーエンド暗号化が可能です。暗号化キー管理においては、独自の暗号鍵の持ち込み(BYOK) および第三者の暗号鍵サービス（KMS）の提供が可能です。

データセキュリティの実践に関する詳細内容は、「Lark セキュリティホワイトペーパー」第 8 節「データセキュリティ」をご覧ください。

3. Lark のセキュリティとプライバシーのコンプライアンス認証

Lark は、長年にわたるコンプライアンスおよびプライバシー保護の取り組みが評価され、業界で広く認められているセキュリティとプライバシーのコンプライアンスに関

する国際的に権威ある認証を複数取得しています。

ISO 27001 情報セキュリティマネジメントシステム

ISO 27001 は、業界で広く認められている情報セキュリティ分野の国際的に権威ある認証です。この認証は、Lark が同分野において国際基準のレベルを満たし、当該認証の求めるセキュリティ基準に該当していることを表しています。

ISO 27701 プライバシー情報マネジメントシステム

ISO 27701 は、プライバシー保護領域の国際的に権威ある認証です。情報セキュリティマネジメントシステムを基礎としプライバシー保護の実践を考慮に入れています。この認証は、Lark が当該認証の求めるプライバシー保護基準に該当していることを表しています。

ISO 27018 パブリッククラウド上における個人情報保護に関する認証

ISO 27018 は、PII 処理者としてパブリッククラウド内の PII 保護に焦点を当てた国際認証です。この認証は、Lark がクラウドデータのセキュリティおよび個人情報保護等において国際標準化を実現したことを表しています。

ISO 27017 クラウドサービスセキュリティ

ISO 27017 は、クラウドサービスセキュリティマネジメントの国際認証規格です。この認証は、Lark がクラウドセキュリティ制御機制および実施等において国際標準化を実現したことを表しています。

SOC 2 (Type II) & SOC 3

SOC (System and Organization Controls) レポートは、米国公認会計士協会（AICPA）が定めた審査基準に基づき独立の第三者機関が評価を行った後に作成する組織のコーポレートガバナンスに関する審査レポートです。SOC 2 (Type II) および SOC 3 レポートは、Lark がシステムおよびコーポレートガバナンスにおいて当該基準の求める安全性、可用性、機密性、プライバシーの原則に該当していることを表しています。

DPTM データ保護トラストマーク

DPTM は、データ保護措置が設けられている法人様を認証するために、シンガポール情報通信メディア開発庁（IMDA）から授与されるデータ保護トラストマークであり、その法人のデータコンプライアンスの実践がシンガポール個人情報保護法（PDPA）に準拠していることを証明します。この認証は、Lark が当該認証の求める個人データ保護基準に該当していることを表しています。

APEC CBPR 越境プライバシールールシステム

APEC CBPR（Cross Border Privacy Rules）は、アジア太平洋経済協力（APEC）メンバー国間の個人情報の転送に関する取り決めを規範化するために、APEC により定められました。この認証は、Lark が当該認証の求める個人データ保護基準に該当していることを表しています。

APEC PRP 処理者向けプライバシー認証

APEC PRP（Privacy Recognition for Processors）は、データ処理者に適用され、そのデータ処理者がデータ管理者に協力してプライバシーコンプライアンス義務を履行する能力を有することを証明します。この認証は、Lark が当該認証の求めるプライバシー保護基準に該当していることを表しています。

最後に

Lark は、お客様のグローバル IT 戦略およびグローバル展開のニーズを大切にし、長期的なコミットをしたいと考えています。お客様がデータセキュリティおよびプライバシー保護に求めることを十分に理解した上で、様々なコンプライアンスソリューションを通してお客様の力になれるよう、オープンで複雑なネットワーク環境がもたらすセキュリティチャレンジや日々厳格になるデータのグローバルコンプライアンスおよびプライバシー保護の要件に対応すべくお客様をサポートします。また、より深刻な安全コンプライアンス分野におけるコラボレーションに対して心が開かれています。