Lark のデータセキュリティへの取り組み

IT 管理者のためのユーザー保護の追求

LARK

目次

はじめに

Lark Technologies は、モバイルに対応し、リアルタイムのコラボレーションをサポートし、シングルアクセスを提供する新世代オフィススイート SaaS である Lark Suite を提供しています。Lark Suite は、ユーザー事業体が効率的かつ連携された形でより安全に情報処理を行う事業に移行できるよう作業効率の向上と生産・管理費の削減を支援します。一方で、当社は、Lark Suite の開発と運営に関連する統制活動の実施をサポートするために、情報技術とアプリケーションシステムを活用してきました。

Lark Suite は、Lark Technologies Pte. Ltd.（「当社」）が創設した企業向け SaaS サービスのオフィススイートで、インスタントメッセージング、クラウドドキュメント、スマートカレンダー、ビデオ会議、オープンプラットフォームなどの機能を備えています。Lark Suite は、例えば、商品とユーザーデータをデータライフサイクルにわたって保護できるよう、業界の先端テクノロジー安全防止策を採用しています。Lark Suite の設計、開発および運営は、コンプライアンスとユーザープライバシー基準に準拠しています。

1. セキュリティチームと機能

当社は、SaaS サービスプロバイダーとして、ユーザーサービスとデータの安全を最優先しています。当社は、徹底したセキュリティインフラとユーザーサービス／データセキュリティ保護システムを備えています。Lark のセキュリティチームは、セキュリティ管理とコンプライアンスチーム、ビジネスセキュリティチーム、データセキュリティチーム、緊急対応チーム、およびセキュリティツール開発チームで構成されています。チームの責任には、商品デザインのセキュリティ評価、コードセキュリティ検証、脆弱性スキャン、侵入テスト、脅威インテリジェンス、侵入検知、緊急対応、データセキュリティ、セキュリティコンプライアンスなどが含まれます。

2. コンプライアンスとプライバシー

当社は商品のコンプライアンスを重要視しており、セキュリティ・コンプライアンス部が国内外の最高基準への準拠を維持する責任を負っています。Lark にはプライバシー専門のチームがあり、同チームは、確実にユーザーデータが正しく使用および処理され、ユーザ

ーが合理的な透明性を有しているよう、ユーザープライバシープロトコル、商品プライバシー保護設計およびユーザーデータの収集と使用を検証します。

当社は、商品コプライアンスの国際要件を積極的に遵守し、商品とサービスが要件を満たしているようにするためさまざまなレベルの規制機関に協力します。

Lark は、業界全体が採用する一連のセキュリティ管理システム規格の ISO 27001 認証を受けています。これは、世界で最も権威ある、厳格な情報セキュリティシステムの認証規格の一つとして認められています。Lark では、データセンター、管理システム、研究開発および機能部門がこの認証を受けており、これは、当社が情報セキュリティ管理の国際規格を満たし、世界中で安全かつ信頼できるカスタマサービスを提供するに十分な情報セキュリティリスク検知と制御能力を有していることを意味します。

Lark は、公共のクラウドにおける個人情報の保護に関する国際規格である ISO 27018 認証を受けています。これは、公共のクラウドで個人を特定可能な情報に対してセキュリティ管理システムの実施を指導するものです。Lark の ISO 27018 認証は、企業データの保護、ユーザー個人情報の保護および情報漏洩の防止で高い基準を達成していることの証拠に他なりません。

Lark は、徹底した PDCA（Plan（計画）、Do（実行）、Check（確認）、Act（見直し））の繰り返しサイクルを有する秘密情報管理システムの規格である ISO 27701 認証を受けています。この規格は 27001 と 27002 の延長線上にあり、プライバシー情報管理システムの設置、実施、維持および継続的な改善の要件を定めています。情報セキュリティ保護の観点から、個人を特定可能な情報の処理に必要なプライバシー保護が考慮されます。Lark は、世界に通用するプライバシーコンプライアンスシステムの構築への長年にわたる取り組みが評価され、この認証を獲得しました。

Lark は、SOC2 タイプ I、SOC2 タイプ II および SOC3 サービス監査報告を受けています。System and Organization Controls（SOC）報告は、米国公認会計士協会の関連するガイドラインに基づき専門の第三者会計事務所が発行する、業務受託会社の内部統制に関する独立第三者による調査報告書です。SOC2 はその一つで、Trust サービス原則（セキュリティ、可用性、処理の整合性、機密性、プライバシー）に基づく顧客データ維持の基準を定義します。Lark は定期的に第三者の監査を受け、商品がこの基準を満たしていることの確認を行っています。これにより、当社システムが信頼でき安全であることが示されます。当社

は、顧客データを安全に維持し、当社の顧客の組織の利益とプライバシーを保護することができます。

認証は、より標準化・正規化されたレベルの情報セキュリティ管理、サービス品質管理、IT サービス管理などを達成した Lark の成功の証であり、当社の全体的な品質システムの改善と完全化の強固な基盤となっています。

3. 社員セキュリティ

Lark は、セキュリティ人事管理プロセスを確立しています。

- 新規社員の採用は人事スペシャリストと人材を要請した部門長の承認を受けなければならない。採用プロセスと結果は、人事管理システムに記録される。
- 新規社員を雇用する前に、国の法令等に準拠し、当該社員の職位の重要度に応じて、人事部が身元確認を行い、かかる雇用が当社の規則と規制を満たしているようにする。
- 新規採用社員は、雇用契約と、情報セキュリティに関する当該社員の義務と責任を定める秘密保持契約に署名しなければならない。
- 法務部は、少なくとも年に一度、社員の秘密保持契約と第三者秘密保持契約に含まれる法的条件を見直し、必要に応じて更新し、社内知識共有プラットフォームに更新後の契約を掲載して、全社員と関係者が最新の秘密保持契約にアクセスできるようにする。
- 社員が退職する場合、まず、社員自らまたは部門長が人事管理システムに入力し、その後、人事部、IT 部および他の機能部門の承認を受けて初めて正式に退職となる。

Lark は、包括的な研修・学習システムを確立しています。新規採用社員には、企業文化、規則と規制、情報セキュリティおよび賞罰制度に関する研修への参加が義務付けられています。一方で、当社は、社員の専門知識とスキル、および情報セキュリティ意識の向上のため、非周期でさまざまな方法により下記研修を施します。

- 社員の情報セキュリティスキルを向上させる、情報セキュリティ関連の研修
- 情報セキュリティ意識を高める、情報セキュリティ活動
- セキュリティ意識トピックに関する資料作成と、メールとポスターによる社員への伝達

4. アプリセキュリティ

4.1. 運営環境セキュリティ

Lark アプリは、ルート検知、改造検知、デバッグ検知、インジェクション検知など、実行環境を厳重にテストします。アプリがハッキングされたかマルウェアに感染した場合に、クライアントが安全で信頼できる環境で実行できるようにすることを検査の目的としています。

4.2. データセキュリティ

Lark アプリは、オペレーティングシステムのセキュリティ対策を使って、アプリ間のパーミッションを区別します。クライアント情報は保存のため暗号化されます。クライアントとサーバー間のフルリンク通信は、HTTPS または WSS で暗号化されます。

4.3. セキュリティ脆弱性に対する保護

Lark にはモバイルセキュリティ脆弱性マイニングチームが常設されており、同チームが Android、iOS、Windows、macOS クライアントのセキュリティ評価と脆弱性マイニング、およびクライアントの第三者コンポーネント（ライブラリ、SDK）の脆弱性検知を行い、アプリに内在する脆弱性を可能な限り根絶してクライアントのセキュリティを確保します。

4.4. クライアントセキュリティ戦略

顧客の管理者は、マネジメントコンソールを介してセキュリティ対策をカスタム設定でき、それらを自己のクライアントに適用することができます。

5. ネットワークセキュリティ

5.1. ネットワークアクセス制御

Lark は、Amazon Web Service（AWS）を使って、インフラサービス（サーバールーム、ネットワーク、サーバー、オペレーティングシステムなど）とインフラセキュリティ

サービスを提供しています。AWS に基づき、当社はサーバーへのアクセスのセキュリティ管理を向上させ、サービスはすべて要塞マシンを介して運営・監査されます。

社員が社内リソースにアクセスするには、権限を受けなければなりません。本人確認後、社員には、初期設定で最低限の権限が与えられます。新たな権限を取得するには、担当責任者の承認を受け、同責任者によって記録されなければなりません。権限には期限があり、期限が過ぎると、システムが自動的に権限を回収します。社員によるオンラインサービス作業は要塞マシン経由で行われ、全作業ログは監査を目的として保存されます。

企業ネットワーク外の社員が社内リソースへアクセスするためには、VPN 接続を使う必要があります。Lark の内部監査・管理部がアクセスログを監査し、プロトコル違反の記録を検索し、それに応じた処分を実施します。

5.2. DDoS とサイバー攻撃の防衛

Lark サービスは、世界中の顧客に CDN 経由でのネットワークへのアクセスと、AWS のロードバランシングを用いた動的加速およびバックエンドサービスへのアクセスを提供しています。DDoS が攻撃を受けた場合、例えば AWS や Akamai のネットワーククリーニングサービスを介して攻撃防衛が実施されます。

5.3. ネットワーク通信の暗号化

Lark サービスは、社内外のネットワークで常時 HTTPS と WSS を経由して通信されます。これにより、通信プロセスのセキュリティが確保され、傍受と改ざんが阻止されます。

6. サーバーセキュリティ

Lark は、AWS のクラウドサーバーを使って顧客にサービスを提供しています。

Amazon は、物理的なレイヤから仮想化レイヤまでのクラウドサーバーセキュリティを提供しています。AWS が提供するクラウドサーバーセキュリティの詳細については、Amazon クラウドセキュリティ白書

（https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf）をご覧ください。

7. アプリケーションセキュリティ

Lark は、開発プロセス保護のため適切な対策を講じるものとします。

7.1. セキュリティ開発プロセス

当社は、セキュリティ違反の根源からセキュリティリスクを制御するよう努めています。当社は、セキュリティ講座を実施し、現場とオンラインで研修を施しています。ディベロッパーとプロダクトマネジャーは全員、セキュリティ研修を受け、セキュリティ脆弱性の原因を理解し、コーディングの知識を増強します。プロジェクト開始時にセキュリティチームがプロジェクトマネジャーと連絡をとり合い、プロジェクト計画にセキュリティ要件とセキュリティテストが反映されるようにします。セキュリティチームは同時に、サプライチェーンからもたらされる脆弱性が存在しないよう、商品に使用される第三者ライブラリとツールを評価し、脆弱性を検査します。サービスのセキュリティ確保のため、商品がオンライン化される前に、デプロイメントの侵入評価とセキュリティ評価を実施します。

7.2. ユーザーアカウントセキュリティ

ユーザーが Lark システムにアクセスする際、パスワードと動的認証コードを使った認証が行われます。これにより、パスワード紛失によるアカウント漏洩を効果的に回避します。認識されていないデバイスからログインする場合、リスク管理戦略がユーザーログイン認証の難度を上げます。同時に、アカウント管理システムは異常なログインの試みを防御することができます。リスク管理システムは、悪質な登録の防止、認証情報列挙攻撃防止その他の保護機能を備えています。

7.3. 脆弱性と緊急事態に対する対応

セキュリティチームは、外部から脆弱性の報告を受け、それを検証し、その危害と修正の緊急性を評価します。

当社は、ルーチンスキャンサービスを使ってサービスとオペレーティングシステムをスキャンし、脆弱性が検知された場合に修正を行います。

当社のセキュリティチームは、大手第三者評価会社とホワイトハットコミュニティと密接に協力して定期的に連絡をとり合い、ときに、外部の会社とホワイトハットを報奨付きで招待して、可能な限りセキュリティの脆弱性を発見できるようサービスの侵入テストを実施します。

当社のセキュリティチームは 24 時間年中無休の緊急対応戦略を実施しています。セキュリティインシデントが発生した場合、セキュリティチームは、セキュリティ緊急対策に従って当該事由を迅速に分類し、緊急対応プロセスを開始してセキュリティインシデントの拡大を防ぎます。

8. データセキュリティ

当社は、データのライフサイクル段階（生成、保存、使用、送信、共有および削除を含む）ごとの技術を保証する徹底したデータライフサイクル管理プロセスを備えています。

8.1. データ送信

当社は、安全な暗号化プロトコルをサポートするデータ通信チャンネルをユーザーに提供しています。メッセージプル、本人認証、動作指示などのデータ通信は、HTTPS と 2048 ビットの RSA キーで暗号化されます。メッセージプッシュは、WSS プロトコルを使って通信データを暗号化して保護します。クラウドドキュメントサービスは、対象鍵暗号化アルゴリズム AES256 を使って暗号化され、通信されます。

8.2. データの保存

当社は、キーメカニズムを使って暗号化データ保存をサポートしています。

Lark は、包括的なデータ分類・管理方法を開発済みで、Lark Suite が収集したユーザー情報を厳格に分類しています。Lark は、システムに保存されるセンシティブ情報を暗号化します。これにより、ユーザー情報が効果的に保護されます。

KMS サービスは、キーとセンシティブな設定情報をライフサイクル（生成、保存、配布、使用、更新、削除など）にわたって管理する責任を負っています。Lark ユーザーのデータの暗号化および Lark サービスのその他さまざまなセンシティブ情報（データベースアカウント、パスワードなど）に使用されるマスターキーは KMS システムに保存され、Lark 自らが維持し、それへのアクセスは KMS インターフェース経由で行う必要があります。キーが初期化されると、KMS システムがシャミア秘密分散法を使って 5 つのシェアを生成し、シェアは異なる管理的な役割の機能に配布されます。4 つ以上のシェアがそろった場合にのみ、KMS システムのマスターキーを復元することができます。KMS マスターキーは定期的に更新され、KMS のセキュリティを向上させます。

8.3. データアクセス

ユーザーデータアクセスは、権限で厳格に区別されます。ユーザーは、許可なくお互いのアカウントにアクセスすることはできません。データへのアクセス（共有など）は、データ所有者が明示的に同意したうえで行われなければなりません。

当社社員によるユーザーデータへのアクセスは、厳格に制限および監査されており、社員はユーザーデータにアクセスできるようデフォルト設定されていません。特別なアクセスをする場合、ユーザーの明示的な許可を受け、また、厳格な社内承認プロセスを経て、一時的なアクセス権を得なければなりません。この場合、権限は作業完了後直ちに回収されます。Lark のオンライン環境内の全サーバーのログインログ、作業ログ、サーバーセキュリティベースラインファイル変更およびアクセス権限変更ログが記録されます。不正アクセスと危険な作業は、自動検知によりリアルタイムで監査され、アラームが生成されます。Lark はデータの活動ログを詳細に記録しており、オペレーターの役割が区別され、それに応じて異なる権限が与えられます。作業は承認と監査を要します。

当社と Lark は、当社または Lark がユーザーの同意を得ない限り、当該ユーザーの情報を開示しません。ただし、法令等、強制的な行政または司法要求によりユーザーデータが求められた場合、当社または Lark は、開示要求された種類のユーザーの個人情報を、開示要求された方法で、規制・法執行機関または司法機関に開示します。当社が開示要求を受けた場合、当社は法令等で許容される範囲で、法令等に対応する法的文書を発行しなければなりません。当社は、特別な調査を目的としてデータを取得する

法的権利を有する法執行機関に限り、データを提供します。法令等に服することを条件に、当社が開示する文書は暗号化手段によって保護されます。

8.4. データの処分

ユーザーへのサービスを終了する際、Lark 管理者は当該ユーザーのアカウント情報を削除し、現地法令等を遵守して当該ユーザーデータを恒久的に削除します。未実装のディスクは、ドライブに情報が残存しないよう消磁および破壊されます。

ユーザー事業体を退職した従業員は、テナント管理者にアカウント閉鎖を申し込むことができます。かかる退職した従業員のアカウント内のグループオーナー、スケージュール、ドキュメントその他のデータが移転されたことを確認した後、テナント管理者は Lark のカスタマーサービス機能から当社に連絡します。当社は、テナント管理者からの申請に応じて、要請を受けたアカウントのデータとドキュメントを匿名化します。

当社がユーザー事業体とサービス契約を締結する場合、かかる契約にはサービス終了時、対応するデータはユーザー事業体の要求に応じて処分されることが規定されます。

ユーザー事業体のテナントのユーザーに加え、Lark Suite は個人ユーザーも対象としています。個人ユーザーがアカウントの閉鎖を要する場合、当社に連絡します。当社は、Lark カスタマーサービス機能経由で、アカウント閉鎖機能を含む Lark Suite インストールパッケージを提供します。インストール後、ユーザーはかかるソフトウェア上でアカウント閉鎖を申請することができ、Lark Suite は要請を受けたアカウントのバックエンドデータベース内のデータとドキュメントを匿名化します。

8.5. データセキュリティ検知

Lark オンライン環境内の全サーバーのログイン挙動、作業挙動、サーバーセキュリティベースラインファイル変更、アクセス権変更およびデータアクセス挙動が記録されます。セキュリティチームは、ユーザーの挙動ポートレートと異常な挙動モデルを構築することで異常な挙動を監視および分析し、データへの不正アクセス、悪意あるデータクローリング、異常なログイン、特権昇格などさまざまな異常なデータアクセス

行為を自動的に検知します。セキュリティ装置は、特異な挙動を自動的に警告し、阻止します。

9. 物理的なインフラセキュリティ

Lark は、Amazon Web Service と Akamai を使って、世界各地の顧客にサービスを提供しています。

9.1. Amazon Web Service（AWS）インフラセキュリティ

AWS は、Lark のクラウドサービスプロバイダーの一つとしてクラウドサーバーなどのサービスを提供しています。AWS 自ら、物理的なレイヤから仮想化レイヤまで、自己のハードウェアおよびソフトウェアを運営、管理および制御しています。Amazon は、世界大手のクラウドサービスプロバイダーとして、ユーザーにインフラセキュリティを提供する業界最高のセキュリティ能力を有しています。AWS が提供するクラウドサービスインフラの保護に関する詳細については、AWS セキュリティ白書（https://d0.awsstatic.com/whitepapers/Security/AWS_Security _Whitepaper.pdf）をご覧ください。

9.2. Akamai インフラセキュリティ

Akamai は世界一の CDN サービスプロバイダーで、世界中で顧客に長期的な信頼性と安定した加速サービスを提供しています。Lark は、Akamai を介して海外顧客に加速化されたアクセスを提供しています。Akamai のセキュリティに関する詳細については、Akamai セキュリティ白書（https://www.akamai.com/cn/zh/about/ourthinking/white-papers.jsp）をご覧ください。

10. 災害復旧とサービスの継続

10.1. バックアップと災害復旧

当社は、Lark Suite のバックアップ戦略、バックアップデータの保存および復旧テスト方法などを標準化するため、データバックアップ・復旧管理ポリシーを確立していま

す。ビジネスデータベースは定期的にスナップショットとバックアップがなされ、データは 3 つのリザーブを備えた 2 か所に保存されます。同時に、当社は、データバックアップの完全性を確保するため、バックアップ性能監視体制を敷いています。Lark のチームは、定期的にバックアップデータ復旧テストを実施します。

10.2. サービス継続保証

サービスシステムアクセスレイヤには、高可用性モードで、Lark が提供する公共のゲートウェイサービスを介してアクセスします。バックエンドは、サービスの信頼性を確保するため、マルチインスタンスアクセスを利用します。詳細なモニタリングにより、トラフィックのバーストや障害が発生した場合、劣化オペレーションモードを使ってサービス可用性を確保します。

Lark は、事業の混乱を引き起こしうるシナリオを想定して、緊急対応と復旧対策のガイドラインを定めた計画を確立しています。Lark は年に一度、重要なビジネスプロセスと当社事業およびリソースに混乱を招きうる脅威を特定するためのビジネスインパクト分析とリスク評価を行い、最大許容停止時間、復旧時間目標および最低限のサービスレベルなどの指標を定義し、異なる業種の混乱シナリオごとに対応戦略を立てます。

10.3. 防災訓練

当社は、徹底した防災訓練体制を備え、開発チーム、セキュリティチーム、オペレーションおよびメンテナンスチームなどが参加する障害訓練を定期的に実施しています。

11. 変更管理

11.1. プログラムの変更

当社は、変更管理の条件と手順（変更計画の構築、変更承認および変更の実施などを含む）を定める変更管理規則を定めています。変更は、オンラインサービスの安定性、可用性およびセキュリティに危険をもたらす可能性があります。Lark が開発したシステムは、サービスのバランスに影響をもたらすことのないよう切替時に厳格に制御します。オンライン作業は作業承認を得ていなければならず、承認を得た上でのみ

作業することができます。サービスの安定性とセキュリティを確保するため、リリースを低トラフィックでテストする必要があります。

11.2. ソースコードの管理

Lark は厳格なソースコード管理プロセスを確立しており、ディベロッパーは自己のチームに対応するコードウェアハウスにのみアクセスでき、それを管理することができます。研究開発要員は、自己のグループに帰属するコードウェアハウスにのみアクセスすることができます。研究開発要員が他のチームに帰属するコードウェアハウスへのアクセスを申し込む場合、かかる申込は当該コードウェアハウスに提出します。申込者のチームリーダーと申込先のコードウェアハウスのオーナーの承認を受けた後、当該コードウェアハウスは申込者に自動的にアクセスを許可します。

11.3. IT インフラの変更

Lark は、公共ネットワーク境界上にアクセス制御リスト（Access Control List、ACL）を設けてネットワークアクセスを管理します。ACL 設定ベースラインとネットワーク制御方針を変更しなければならない場合、作業要員はシステムワークフロープラットフォームに申請します。システム部のエンジニアが、変更リクエストの合理性を評価した後、変更を実施します。システム部の授権エンジニアに限り、ネットワークアクセス設定を変更するためのアクセスが付与されます。

11.4. モニタリングの変更

Lark チームが毎年内部監査を行い、当社の内部統制システム（変更管理に関する統制を含む）の運用有効性を評価します。監査結果は、内部監査報告書にまとめられます。例外が特定された場合、内部監査・内部統制部が、改善対策を講じて改善状況を追跡するよう担当チームに通知します。変更管理プロセス（変更開発、テスト、承認、マイグレーションおよびモニタリングを含む）において、非対応の役割は分離されます。

larksuite.com

LARK