Lark セキュリティホワイトペーパー

はじめに

「Lark Suite」は、Lark が次世代コラボレーションプラットフォームとして提供しているサービスです。Lark Suite は「モバイルフレンドリー」、「リアルタイム共同編集」、「データの一元管理」といった、お客様の生産性向上や業務・管理コスト削減に役立つ特徴を有しており、効率性やコラボレーション、セキュリティといった面で、お客様のデジタルトランスフォーメーション（DX）を支えることが可能です。

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。

そして、これらの製品、ならびにお客様のデータのライフサイクル全体にわたるセキュリティを保障するため、業界最先端の管理手法や技術ソリューションを採用しております。設計から開発、運用にいたるまで、コンプライアンスや個人情報（プライバシー）保護の要請について十二分に熟慮されており、ネットワークセキュリティや個人情報（プライバシー）、データ保護等に関する法律法規や各種ガイドラインの要件を確実に満たすようにしています。

1. セキュリティチームとその役割

Lark は、SaaS プロバイダーとして、お客様のビジネスとデータセキュリティを最優先課題としてとらえています。インフラフレームワークのセキュリティはもちろん、ユーザーのビジネスやデータセキュリティを維持するための仕組みも整っており、物理層からアプリケーション層、データ層までトータルに守っています。

Lark 社のセキュリティチームは、セキュリティマネジメント、コンプライアンス、ビジネスセキュリティ、データセキュリティ、緊急対応、セキュリティツールの開発など複数の専門チームから構成されています。各々が専門的知見から、製品設計段階におけるセキュリティ評価からコードのセキュリティレビュー、脆弱性スキャン、ペネトレーションテスト、脅威インテリジェンス、侵入検知、緊急対応、データのセキュリティ、セキュリティ・コンプライアンスなど多方面の業務に取り組んでいます。

2. セキュリティ・コンプライアンス認証

Lark は、製品のコンプライアンスを重要視しており、世界トップレベルのコンプライアンス要件をベンチマークしています。これまでに ISO27001、ISO27017、ISO27018、ISO27701、CBPR & PRP、DPTM をはじめとする多数の国際的なコンプライアンス認証のほか、SOC についても SOC 2 Type II や SOC 3 報告書を取得しております。ここからも、Lark が情報セキュリティやプライバシー保護などの面で、標準・規格の求めるレベルを満たしていることが分かると思います。

ISO27001 情報セキュリティマネジメントシステムは、業界で広く認められているセキュリティマネジメントシステム規格です。国際的に最も厳格で、権威ある情報セキュリティ認証規格とされており、世界中で広く受け入れられています。Lark ではデータセンターからマネジメントシステム、研究開発、機能部門がこの認証を取得しております。これはつまり、Lark の情報セキュリティにおけるリスク識別能力・管理能力はすでに世界基準に達しており、世界中どのお客様に対しても信頼性の高いサービスを提供できるということです。

ISO27017 クラウドサービスセキュリティは、クラウドに特化した情報セキュリティ管理体制とその運用について提案するもので、ISO 27002 および ISO 27001 を補完する、いわゆる「アドオン認証」と呼ばれるものです。クラウドサービスプロバイダーの実施すべき情報セキュリティ管理について、詳細に示しています。

ISO27018 パブリッククラウド上における個人情報の保護に関する認証は、パブリック

クラウド上の個人情報保護に特化した、初めての国際規格です。ISO27002 情報セキュリティマネジメントの実践のための規範に基づいて策定されており、パブリッククラウド内の個人情報（Personally Identifiable Information: PII）に適用されるセキュリティ管理体制に対する取り組みを示しています。Lark は法人データの保護、ユーザーの個人情報セキュリティの保障、情報漏えい防止などで、業界でも高いレベルで取り組んでいることが認められ、この認証を取得しております。

ISO27701 プライバシー情報マネジメントシステムは、PDCA サイクルに基づくプライバシー情報マネジメントシステムについて、初めて深く言及された規格です。プライバシー情報マネジメントシステムの確立、実施、維持、継続的改善の各要件について詳しく規定されており、情報セキュリティマネジメントシステムをベースに、個人情報の取り扱いに必要なプライバシー保護策を補完するアドオン認証となっています。Lark はこの認証を 2019 年に国際的な認証機関 BSI（英国規格協会）から取得しており、世界初の認証取得法人に名を連ねました。

SOC（システムおよび組織管理）報告書は、サービスプロバイダーの内部統制について独立した第三者機関（監査法人）が審査して発行する報告書のことです。審査基準は米国公認会計士協会（AICPA）によるものと、国際監査・保証基準審議会（IAASB）によるものがあり、いくつかの主題に分かれています。この種の報告書としては広く認知され、権威性・専門性ともに最も高水準なものでありますが、取得している製品は世界でも多くはありません。SOC の審査をパスしたことで、Lark にはユーザーデータおよびプライバシーの保護を持続的かつ効果的に行う能力があること、セキュリティシステムの構築において今後も高い基準を維持し続けられること、そして効率的で高いセキュリティを有し、信頼性の高いクラウドオフィスサービスを提供できることが示されました。

このうち、SOC 2 (Type Ⅱ) レポートは Lark の体制について説明しており、米国公認会計士協会が定める Trust サービスの基準（TSP セクション 100）のうち、セキュリティ、可用性、機密性、プライバシーについてサービスコミットメントとシステム要件を Lark が満たしていることを示しています。

また、Lark は SOC 3 レポートも取得しています。こちらは、Lark の各ツールの体制について説明するもので、米国公認会計士協会が定める Trust サービスの基準（TSP セクション 100）のうち、セキュリティ、可用性、機密性、プライバシーについてサービスコミットメントとシステム要件を Lark が満たしていることを示しています。

APEC 越境プライバシールールシステム（CBPR) および処理者向けプライバシー認証 (PRP)は、APEC のエコノミーによって構築された認証制度です。個人情報の越境移転

における消費者、法人、管轄機関の信頼を構築することを目的としています。APEC CBPR および PRP の認証は、APEC プライバシーフレームワークと原則に準拠したもので、データ管理者である組織に適用される CBPR と、データ管理者に代わってデータを処理する情報処理者のための PRP という位置づけがなされています。これらの認証を取得することで、APEC エコノミー間における個人情報データの移転についても、プライバシーとセキュリティだけでなく、コンプライアンスの面でもより充実させることができます。

なお、Lark はシンガポールにおいても、同情報通信メディア開発庁（IMDA）よりデータ保護トラストマーク（DPTM）を取得しております。このマークは、シンガポール個人データ保護法（PDPA）や国際基準、ベストプラクティスなどに基づいて制定された規格の認証です。Lark が長年に渡って健全なデータの保護策を講じて実践にあたってきたこと、お客様の個人データ保護に取り組んできたことが、IMDA に認められたことを示しています。

さらに Lark では、製品コンプライアンスに関する国際的な要件についても積極的にキャッチアップしています。提供する製品およびサービスが各種要件を満たすようにするため、セキュリティマネジメントチームやコンプライアンスチームがそれぞれ管轄部門と確認を進めています。Lark にはほかにもプライバシー専門のチームもあります。ユーザー向けのプライバシー規約、製品のプライバシー保護設計、ユーザープライバシーデータの収集・利用についてレビューを行っており、ユーザーのプライバシーデータの適切な取り扱いを徹底することで、ユーザーに対する透明性を維持しています。Lark のプライバシー保護における実践の詳細については、『Lark プライバシーホワイトペーパー』をご参照ください。

3. 社員のセキュリティ

3.1 人事管理プロセス

Lark は、次のように安全な人事管理プロセスを構築しています。

- 新入社員の募集および採用は、人事担当者と採用部門責任者の承認を必要としています。また、新入社員の採用では、プロセスも結果も人事システムに記録されます。
- 新入社員の採用前に、採用職種の重要性に応じて、国の法令等に準拠して身

元調査を人事部が行っています。これはその応募者の採用が Lark の各規則を満たしていることを確認するためです。

- 新入社員に対しては、情報セキュリティに関して負うべき責任と義務について定めた労働契約と機密保持契約の締結を義務付けています。
- 社員や第三者機関に対する機密保持契約の内容については、法務部による確認を年に 1 回以上のペースで行っており、修正の必要があれば更新をしています。更新後は、社員全員・関係者が最新の機密保持契約にアクセスできるよう、社内の知識共有プラットフォームで公開しています。
- 退職については、本人または部門長が人事システムで申請を出し、人事部および他の機能部門の承認を必須としています。退職が決定すると、当該社員のアカウントをすべて抹消するとともに、ハードウェア・ソフトウェア資産の返却を退職前までに行っています（パソコン、作業ドキュメントなど）。

3.2 セキュリティ研修と学習

Lark には、研修・学習制度が整っています。新入社員はまず企業風土、規程、情報セキュリティ、賞罰制度などの研修に参加しなければなりません。このほかにも、専門知識・スキルや情報セキュリティ意識向上に関する次のような研修を不定期に行っています。

- 情報セキュリティに関する不定期研修で、社員の情報セキュリティスキル向上をはかる（年 1 回以上）
- 情報セキュリティのアクティビティで、情報セキュリティ意識の周知徹底をはかる（年 1 回以上）
- セキュリティ意識向上に関する宣伝物の作成や、メール・ポスターなどによりセキュリティ意識を浸透させる

3.3 デバイスセキュリティマネジメント

Lark は、社員に対するデバイスセキュリティマネジメントポリシーを定めています。すべてのデバイスにデフォルトで実施されており、このセキュリティ設定を社員自身が削除・編集できなくなっています。社員のパソコンには、アンチウイルスソフトがインストールされており、これを無効化したり、アンインストールしたり、設定を変更したりといった操作をバックエンドで禁止しています。セキュリティ設定ができるのは、アンチウイルスソフトの管理者アカウントを持つ、一部の IT 部の社員に限られ

ています。アンチウイルスソフトは、パターンファイルをリアルタイムに更新しており、定期的に業務用デバイス全体に対するウィルススキャンを実行します。また、Lark では、社員用デバイスのデータやファイルのセキュリティ保護のため、磁気ディスクに対してもディスク全体の暗号化を行っています。業務用デバイスは退職時に返却が必須であり、デバイス内の情報は IT 部によってランダムデータの上書きによって消去されます。

4. アプリセキュリティ

4.1 アプリ実行環境のセキュリティ

Lark アプリは実行環境に対して Root 化や脱獄、デバッグモード、インジェクションなどの検知をはじめ、厳格なチェックを行っています。これはプログラムのハッキングや、悪意あるソフトウェアによって Lark アプリが不正に利用されることを防ぎ、信頼できる環境で Lark アプリを使っていただくことを目的とするものです。

4.2 アプリデータのセキュリティ

Lark アプリは、OS 標準のセキュリティ機構を使ってアプリ間の特権分離を実現しています。また、アプリのローカル情報は暗号化したうえで保存されます。アプリとサーバー間の通信はすべて、HTTPS または WSS で暗号化されます。

Lark は、独自開発したデータセキュリティソリューションをアプリに組み込んでおり、アプリのローカルにあるプライバシーデータをシステムレベルの暗号化能力で守るほか、データとデバイスを完全に一対一で紐づけています。そのため、たとえユーザーデータが盗難されたとしても、データは暗号化されているため、攻撃者が復号して自身のデバイスで使うことは不可能となっています。これにより安全にユーザーデータを扱うバウンダリの大幅拡張とともに、ユーザーデータ漏えいリスクを大きく引き下げています。

4.3 アプリセキュリティの脆弱性防御

Lark には、モバイルセキュリティの脆弱性調査専門チームがあり、Android/iOS/Windows/macOS/Linux などのアプリにセキュリティ評価と脆弱性調査を行っています。それと同時に、アプリのセキュリティを保証するため、利用している

サードパーティー製コンポーネント（ライブラリや SDK）についても脆弱性テストを行って、存在する脆弱性の発見に努めています。さらに、定期的に外部のセキュリティ専門会社に、第三者の立場からペネトレーションテストを実施してもらっており、見つかった問題を適時修復しています。

4.4 製品のセキュリティ能力

Lark は、アカウントセキュリティ、ユーザー権限、データセキュリティなど多方面にわたってセキュリティ能力を有しています。以下にその一例を紹介します。

アカウントセキュリティ：二段階認証、ログイン継続期間の設定、ログイン方法の管理、ログインパスワードの管理、申立て管理など

ユーザー権限：連絡・共同作業権限、外部連絡権限、ファイル操作の権限など

データセキュリティ：秘密度ラベル、透かしの設定、センシティブワードフィルタなど

メールセキュリティ：フィッシング対策、迷惑メール対策、ブラックリスト/ホワイトリスト、データ保護ルールなど

Lark 製品のセキュリティは頻繁に更新されています。最新の機能については、オフィシャルサイトをご覧いただくか、カスタマーサービスへお問合せください。

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、アクセス制御リスト（ACL）によるフェンシングを行っています。社内のネットワーク環境をゲスト、オフィス、開発・テスト環境、本番環境などのエリアに分割しているほか、全社員を Lark のネットワーク境界の外に置いているため、VPN を介さなければ開発・テスト環境、本番環境にアクセスできないようになっています。さらに、アクセスログなどは内部監査部門によってチェックされており、不正な操作記録があれば追跡・処罰の対象となります。

Lark では内部リソースへのアクセスも、厳格な社員アクセス制御ポリシーで制限されています。社員であっても内部リソースにアクセスする際には、ID による認証が行われ、その後、デフォルトで必要最小限の権限のみが付与されるのです。別の権限を取

得するには、責任者から承認を受けねばなりませんし、記録に残されます。さらに、権限には有効期限が設けられ、終了後には自動的に回収される仕組みになっています。社員によるオンラインサービスの操作は、すべて要塞ホストを介しており、全操作ログが 180 日間以上保存されるほか、内部監査部門によるチェックも実施されています。

5.2 ネットワークファイアウォール

Lark システムに対する既知のネットワークセキュリティ脆弱性への攻撃は、ネットワークファイアウォールで阻止しています。ネットワークファイアウォールのルールは、コンプライアンス部門の許可されたエンジニアによって、一元的に設定されています。また、ネットワークファイアウォール設定の更新は、自動と手動を組み合わせる手法をとっています。

5.3 DDoS およびサイバー攻撃対策

お客様の Lark サービスへのアクセスは、CDN や動的サイトアクセラレーションを介して接続された後、Lark のロードバランスを経由してバックエンドサービスに到達します。Lark は、業界トップクラスの DDoS 防御サービスを設けており、大量のトラフィックや連続アクセスなども効果的に防御することができます。

5.4 ネットワーク転送の暗号化

Lark の製品は、情報が途中で改ざんや窃取されないよう、内部・外部ネットワーク転送ともに HTTPS、WSS で暗号化して、通信過程のセキュリティを保証しています。

6. サーバーのセキュリティ

Lark は、使用しているサーバーに各種セキュリティマネジメントポリシーを設定して、サーバー稼働のセキュリティを保障しており、ネットワーク上のマルウェア攻撃を効果的に防いでいます。

6.1 サーバーのアクセス制御

Lark は、サーバーアセットのスキャンを定期的に実行しており、不必要なポートやサービスがあれば、随時無効化しています。このように外部への権限を最小化したり、安全ではないサービスをフィルタリングしたりすることで、セキュリティの問題を低

減させます。セキュリティ部門が定期的にウィークパスワードテストを行い、保守運用担当者が脆弱なパスワードの変更を促すことで、暴力的なハッキングを防ぎます。サーバーに対するアクセスはすべて要塞ホストによる審査を介す必要があります。業務サービスへのアクセス元は許可リストで制御されており、信頼できるアクセス元以外はブロックされるようになっています。

6.2 脆弱性スキャン

Lark では定期的に、脆弱性自動スキャンツールによるサーバーの脆弱性テストを行っています。テストの結果はセキュリティ部門で確認を行った後、即座に関係者に連絡して修復作業に移ります。また、サーバーの安定稼働を保障するため、システムの追加・更新作業が保守運用部門によって実施されています。

6.3 侵入検知

Lark の物理サーバーは、HIDS（ホスト型侵入検知システム）を全面的に配置しており、ファイルのベースラインからの変更をリアルタイムでモニタリングしています。ほかにも、異常なプロセスやアクティブな異常接続、トロイなどの異常な挙動を検知し、すぐに対応しています。また、お客様のアプリからのトラフィックは WAF（Web アプリケーションファイアウォール）で攻撃性のチェックと検証が行われ、安全性と合法性が確認されます。もし、悪意のあるリクエストと判断されれば、リアルタイムでブロックされます。さらに、セキュリティチームがセキュリティの稼働状況や最新の攻撃手法にしっかりとキャッチアップすることで、侵入パターンの研究にあたるとともに、防御ポリシーの定期的なアップグレードに努めています。

6.4 異常検知

サーバーに蓄積された大量のマスターログや自己開発した HIDS の収集データは、セキュリティチームがビッグデータや機械学習プラットフォームを活用して、多元的なセキュリティ分析と異常検知モデルの構築を行っています。これにより、サーバー上の高リスク操作や異常なプロセス、悪意のあるネットワーク接続などの異常な挙動をすばやく発見し、すぐに対応できるようにしています。また、セキュリティチームがセキュリティの稼働状況や最新の攻撃手法にしっかりとキャッチアップし、セキュリティアルゴリズムのモデル更新を続けているため、異常な挙動のパターンを最新に保ちつつ、防御ポリシーの定期的なアップグレードも可能となっています。

7. アプリケーションセキュリティ

7.1 セキュア開発プロセス

Lark はセキュリティリスクについて、脆弱性の大元から制御することを目指しています。そのため、セキュリティに関するカリキュラムを作成し、オンライン・オフラインでの研修を実施しており、開発スタッフ、プロダクトマネージャー全員にセキュリティ研修を義務付けています。これにより、脆弱性の原因やコードなどについて理解を深めています。プロジェクトのスタート時には、セキュリティチームがプロジェクトマネージャーと話し合いを行って、セキュリティニーズやセキュリティテストを計画から織り込むようにしています。さらに製品に使用するサードパーティーのライブラリ、ツール由来の脆弱性が製品に持ち越されないように、セキュリティチームによる評価や脆弱性の確認も行われています。設計や実際のコードについても、製品チームとともにセキュリティチームによるセキュリティレビューが実施され、リリース前にもペネトレーションテストやセキュリティ評価を行うなど、サービスのセキュリティ確保に努めています。

7.2 ユーザーアカウントのセキュリティ

ユーザーによる Lark システムへのアクセスは、パスワードと認証コードによる本人確認が可能です。識別していないデバイスからログイン要求があった場合、リスクコントロールシステムにより、ログイン認証の難易度が引き上げられます。また、アカウントシステムも、異常・不正なログインに対する防御能力を備えています。

Lark は、悪意のあるアカウント作成、クレデンシャルスタッフィング、無理なログインによるハッキングなどに対する防御機能を備えた、自社開発のリスク制御システムとアンチスパムシステムに接続しています。またユーザーサイドでは、パスワードと認証コードの多要素認証によるログインを採用することで、パスワード紛失によるアカウント漏えいリスクの予防につながります。

7.3 脆弱性とセキュリティインシデントのマネジメント

Lark は、内部・外部の脆弱性や脅威インテリジェンスについて、様々な方法でモニタリングを行っています。自社のサービスや OS については、セキュリティチームの自動セキュリティスキャンツールでスキャンし、アプリケーションについても定期的なペネトレーションテストでセキュリティをチェックしています。脆弱性や脅威インテ

リジェンスが認められたら、その危険性に応じてリスクレベルが決定され、すぐさま関係部門に伝えられて修正対応がとられるとともに、Lark が設けている脆弱性ライフサイクル管理ポリシーにのっとって、専門チームが解決までフォローします。

また、Lark のセキュリティチームは、できるだけ多くの脆弱性を発見することを目的に、業界トップクラスの第三者評価企業やホワイトハットコミュニティと密接に連携しており、不定期に報奨金を拠出して、外部企業やホワイトハッカーにペネトレーションテストを依頼したりもしています。

さらに、Lark はインシデント管理フローに基づく 24 時間 365 日の緊急対応ポリシーを実施しています。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がセキュリティ緊急対応計画に基づきインシデントのレベルを迅速に判断し、緊急対応プロセスをスタートして、セキュリティインシデントの拡大を阻止します。対応が完了したら、発生原因や対応の過程と結果、インシデント責任者、フォローアップ措置などの事後レビューを行い、その結果と措置を記録して、インシデントをクローズします。ユーザーやお客様に影響の及ぶセキュリティインシデントであった場合は、インシデント対応プロセスにのっとってユーザーやお客様、その他の関連当事者に適時通知します。

8. データセキュリティ

Lark は、データに対して完全なライフサイクル管理を行っており、データの作成から保存、伝送、使用、廃棄の各段階について明確なプロセスと、それを可能にする技術を備えています。また、データの転送、保存、アクセス、廃棄プロセスのセキュリティについても、相応の管理措置が策定されています。

8.1 データの伝送

Lark は、強力な暗号化プロトコルをサポートするデータ伝送経路をテナントに提供しています。データ受信、本人確認、操作指示などのデータ伝送には、HTTPS を使用して暗号化を行うほか、2048 ビットの RSA キーを使用しています。また、データ送信の暗号化には、WSS プロトコルを、ビデオとチャットには DTLS に基づくエンドポイント-サービスエンドの暗号化を採用しています。

8.2 データの保存

Lark は、安全な暗号鍵を使って、メッセージ、ドキュメントなど、お客様の全データを暗号化して保存しています。

Lark は、データのカテゴリ別・グレード別管理手法を定めており、収集したユーザー情報やバックエンドマネジメントシステム内のテナント情報などに厳格に適用されています。また、システム内に保存しているすべてのセンシティブ情報には暗号化処理を施して、ユーザー情報のセキュリティを保障しています。

暗号化アルゴリズムは各アプリのソースコードに組み込まれ、暗号鍵は暗号鍵マネジメントシステム（以下、「KMS」）で生成され、各アプリから呼び出されます。暗号鍵および重要な設定情報の作成から保存、発行、使用、更新、削除などのライフサイクル管理は、KMS サービスにより実施されます。テナントデータの暗号化に使用するマスター暗号鍵と Lark サービスのその他の重要情報（データベースのアカウント、パスワード等）は、Lark が保守する KMS に記録されており、アクセスするには KMS に接続する必要があり、KMS のルート暗号鍵はハードウェアセキュリティモジュール（HSM）で保守されています。HSM の管理は、複数の役職者が持つ複数の暗号鍵を組み合わせなければできないようになっています。KMS での暗号化/復号は、エンベロープ暗号化の手法がとられています。また、各テナントのマスター暗号鍵は、お互いに隔離して保存されています。

さらに、標準のテナントマスター暗号鍵と AES-256 によるデータとデータ暗号鍵の暗号化保存のほか、独自鍵もサポートしています。これは、KMS でデータ暗号鍵を生成した後、お客様自身のカスタム暗号鍵と指定したアルゴリズムでデータとデータ暗号鍵に対し暗号化することもできます。これにより、暗号化アルゴリズムの選択と、暗号鍵の更新を自身の手でコントロールすることが可能です。

8.3 データのアクセス

ユーザーデータへのアクセスは、厳格な権限分離を行っており、許可されていないユーザー間で互いにアクセスすることはできません。データにアクセスするには、データ所有者が共有操作を行うなどの許可を得る必要があります（例えば、ユーザー A が作成したドキュメントは、他人に閲覧権限を許可しない限り、デフォルトでは A だけが閲覧可能となっています）。

Lark 社員は、お客様やユーザーのデータへアクセスできないようにデフォルト設定されており、社員による操作はすべて厳格に制限され、監査の対象にもなっています。また、不正アクセスや高リスク操作に対しては、自動チェックによるリアルタイム監査とアラートの発出が行われています。

8.4 データの廃棄

個人アカウントは、個人情報の削除請求を申請できます。Lark では、アカウント抹消や個人情報削除の申請の受理後、当該アカウントに関するデータの削除または匿名化処理を行います。

法人テナントの退職社員が個人情報の削除を請求するには、まずテナント管理者にアカウント抹消申請をします。その後、退職社員のアカントが所有していたグループオーナー権限や予定、ドキュメント等のデータ移行について、テナント管理者で確認を行い、Lark のカスタマーサービスに連絡をいただけば、当該アカウントに関するデータの削除または匿名化処理を Lark で行います。

Lark は、ユーザー法人との提携契約を締結する際に、契約終了時のデータ処理について、法的要件に従ってアカウントに関するデータを削除、匿名化等の処理を行うことを取り決めます。

データの削除および匿名化技術は、業界基準や法的要件に合致するものを採用しており、いずれも不可逆的な処理となります。

8.5 データのセキュリティテスト

Lark のオンライン環境にある、すべてのサーバーへのログイン行為、操作、サーバーセキュリティベースラインの変更、アクセス権限の変更、データへのアクセス行為は、すべて記録されます。また、セキュリティチームがユーザー行為のキャプチャや異常行為モデルの構築を実施しており、異常行為の識別、分析、関連付けを実現し、データに対する不正アクセス、悪意あるクローリングおよび高リスク操作、ログイン異常、権限のアップグレード等のような正常ではないデータアク

セス行為をリアルタイムで自動検測し、警告および遮断しています。

9. 物理インフラのセキュリティ

Lark は クラウドサービス「AWS」を利用しており、ハードウェアおよびソフトウェアの操作、マネジメント、制御は AWS が担当しています。AWS は世界トップクラスのクラウドプロバイダーであり、業界トップのセキュリティ能力で、ユーザーインフラのセキュリティを保障しています。AWS が提供するクラウドサービスのインフラ保護に関する詳細情報については、
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf をご覧く

ださい。

10. ディザスタリカバリ（DR）と事業継続性

10.1 バックアップとディザスタリカバリ

Lark は、データベースのバックアップポリシー、バックアップデータの保管、リストアテストなどについて標準化した規程を定めています。業務データベースは、定期的にスナップショットとバックアップを作成しており、そのデータを 2 拠点で 3 つ保存しています。さらに、バックアップ状況をモニタリングする仕組みもあり、バックアップの完全性を確保しつつ、定期的なリストアテストを実施しています。

週に 1 度の全データバックアップのほか、随時、追加データの自動バックアップも行われています。Lark のバックアップモニタリングは、バックアップタスクのエラー時もデータベース管理者にアラートをプッシュ送信できるため、管理者による原因の確認と対応が可能です。

バックアップデータの抽出とリストアテストは毎日実施しています。データベース運用保守プラットフォームから研究開発メンバーによるリストアリクエストが出されると、担当者の承認後にデータベース管理者によるリストアが実施され、研究開発メンバーがバックアップデータの可用性を検証するという流れになっています。

10.2 事業継続性の保障

業務システムへの接続は、インフラサービスプロバイダーが提供するパブリックゲートウェイという、可用性の高い方法を介して接続しています。バックエンドはサービスの信頼性保障のため、複数のインスタンスを接続して構成されています。トラフィックや障害については細かなモニタリングを行っており、トラフィックの急増や障害の発生時には、ダウングレードモードで運用するなどして、事業における可用性を保障します。

Lark は、業務の中断を招き得るシナリオについて緊急対応と復旧措置を定めています。年に一度、業務影響分析およびリスクアセスメントを実施しており、重要な業務プロセスおよび Lark の業務・リソースの中断にいたる恐れのある脅威の識別、最大許容中断時間・復旧時間目標・最低サービスレベルなどの指標の定義、業務中断シナリオごとの対応ポリシーの策定などを行っています。

10.3 緊急対応シミュレーション

Lark は、緊急対応シミュレーションを整備しており、定期的に演習を行うことで、障害発生に備えています。この演習には業務チーム、セキュリティチーム、保守運用チームなどが参加しており、年に 1 回以上の頻度で業務中断シナリオに関する DR 演習を行って、データの可用性を保障しています。

11. 変更制御

11.1 プログラムの変更

Lark はプログラムの変更管理規程を定めており、変更案の立案、承認、実施など変更管理の要件やプロセスを明確化しています。オンラインサービスの安定性、可用性、安全性に対して影響のあることが既知である、またはその恐れがある操作は、オンライン変更の範囲に含めています。Lark の製品開発では、厳格な変更管理が行われており、変更がサービスの安定性に影響を及ぼさないようにしています。オンライン操作には指示書を必須としており、許可のない状態では実行できないようになっています。各製品に関するアプリには開発、テスト、生産用の独立環境を設けており、ダークローンチによるリリースが遵守されています。リリースは、サービスの安定性およびセキュリティを確保するために、負荷テストを実施しなければできないようになっています。

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定めており、研究開発メンバーは自分の所属チームが扱うリポジトリしかアクセス・管理できません。リポジトリ内部にあるプロジェクトリポジトリは、リポジトリ担当者を設定しています。チーム外のリポジトリのアクセス権限が必要な場合、リポジトリ内で申請を提出して、その部門責任者と当該リポジトリの担当者の承認を得る必要があります。

11.3 インフラの変更

Lark は、パブリックネットワークの境界にアクセス制御リスト（ACL）を配置して、ネットワークアクセスを制御しています。ACL 設定ベースラインやネットワークのアクセス制御リストに変更の必要が生じた場合、保守運用メンバーが所定のプラットフ

ォームから申請を提出し、専門エンジニアによって変更が合理的であると判断されなければ、変更はできなくなっています。また、ネットワークアクセス設定の変更操作の権限は、許可を得たエンジニアだけに限られています。

11.4 変更モニタリング

Lark は毎年、内部統制として内部監査システムの実施状況をチェックしております。そのなかには変更管理の有効性チェックも含まれており、内部監査報告書にまとめられます。異常が認められたら、内部監査部門と担当チームに連絡して是正を行い、その結果をフォローまで行います。開発、テスト、承認、リリース、モニタリングなど変更管理で兼任すべきではない職務は、きちんと分離されています。

12. オープンプラットフォームのセキュリティ

Lark は、SaaS の多様な体験でさまざまな法人のニーズを満たせるよう、安全で信頼性の高いアプリ用エコシステムのプラットフォームづくりに取り組んでいます。このようなモデルでは、Lark プラットフォーム、デベロッパー、お客様・ユーザーなど多数の責任主体が関わることになります。Lark は、サービスベンダーの参入、開発アプリのリリース審査、権限のカテゴリ分け・グレード分けと承認、定期的なセキュリティチェックなど多方面から確認を行っており、アプリのセキュリティやプラットフォームの健全性、ユーザーのプライバシー保護に努めています。

12.1 ベンダーの承認

Lark は、ユーザーデータのセキュリティを保障できないベンダーを防ぐため、独立系ソフトウェアベンダー（ISV）に対して、厳格な参入承認制度を構築しています。例えば、法人設立から一定年数経過している、製品がすでに定着して事業化されている、お客様の数が一定数を超過している、などの条件があります。

Lark は、ISV の参入時に一律で資格審査を行っています。審査内容には、会社の資格、研究開発力、コアメンバー、過去の実績、顧客層、社会的信用などが含まれています。

12.2 開発アプリのリリース審査

Lark は、ISV が高いセキュリティと信頼性をもって開発できるよう、開発者用のドキュメントを詳細に記述して、開発段階からセキュリティとコンプライアンス性を満た

したアプリを開発するよう指導しています。ストアアプリのリリース段階において、Lark は、アプリ全体に対してデプロイ環境、セキュリティ、コンプライアンスとプライバシー、セキュリティ製品など多岐にわたる検収を行うほか、サプライヤーへのアンケート、実機テストなどでアプリのコンプライアンスを確認しています。

アプリのリリース前には、Lark による厳格な審査が行われます。まず、サードパーティーアプリを、アプリが取得する権限、使用するテナントまたはユーザーの数といったリスクに応じて 3 つのグレードに分類します。グレードごとにデプロイ環境、セキュリティ、コンプライアンスとプライバシー、セキュリティ製品など、複数の審査項目が定められています。

- P0：ベースライン要件：すべてのアプリリリースに適用されます。
- P1：セキュリティ強化要件：センシティブな権限および使用量の多いアプリに適用されます。
- P2：推奨セキュリティ措置：トップアプリに推奨されます。

12.3 権限のカテゴリ分け・グレード分けと承認

ユーザーおよびお客様のデータのセキュリティを考慮し、権限と関連するオープン機能を利用するには、Lark のオープンプラットフォームから申請を提出し、Lark のオープンプラットフォームまたはテナント管理者の承認を受けねばなりません。Lark の権限は、一般権限と高度な権限に分けられます。

- 一般権限：データの重要度が通常程度である権限。ユーザー ID の取得、アプリの ID によるメッセージ送信、等。
- 高度な権限：アクセスするデータの重要度が高い権限。ユーザー企業の組織構造情報の取得、カレンダー・予定および繁忙状況情報等の取得、等。

法人のカスタムアプリ及びストアアプリについては、グレードごとに権限申請と承認ポリシーを策定しており、操作に必要不可欠で合理性のある権限のみを承認します。このうち、ストアアプリの権限操作はすべて、リリース時のオープンプラットフォームによる審査と、インストール・バージョン更新時のテナント管理者による審査という、両方の審査が必須となっています。テナント管理者は、自身の実際のデータニーズによっては、承認不要ルールを設定して、審査の負担を減らすことも可能です。

法律や OS の要請によって、ユーザーの位置情報やマイクアクセスなど、一部のセンシティブな個人情報やシステム権限の利用には、ユーザーが個別に許可する必要が生

じる場合もあります。

12.4 セキュリティのモニタリングスキャン

Lark は、サードパーティーアプリに対し、脆弱性自動スキャンを行っています。サーバーに脆弱性がある、またはサーバーが攻撃されやすいサービスを利用していないかなどを確認するとともに、継続的にリスクアラートを出したり、脆弱性テストを行ったりといった取り組みもしています。

Lark のセキュリティチームによる、サードパーティーのアプリに対するセキュリティテストも不定期で実施されています。クラッカーの挙動を模して、ストアアプリに対して高度なセキュリティ評価を行うことで、クラッカーに先んじてサードパーティーアプリのリスクを発見できるようサポートしています。