Slack の
セキュリティ

本書は、お客様のご参考のために作成された英語版の参考訳であり、可能な限り正確であるように努めていますが、誤りを含む可能性があることをご了承ください。英語版と齟齬がある場合、英語版の定めが優先するものとします。

はじめに

Slack のミッションは、人々のビジネスライフをよりシンプルに、より快適に、より有意義にすることです。お客様のデータを安全に保護する必要があり、それが Slack の最も重要な責務の一つであると信じています。Slack ではセキュリティ対策を公開し、お客様に当社 取り組みを理解してもらえるよう努めています。

組織としてのセキュリティ

業界をリードする Slack のセキュリティプログラムは、組織とデータをあらゆる面で保護する多層防御のコンセプトに基づくものです。このセキュリティプログラムは ISO 27000、AICPA Trust Service Principles、NIST の各標準に準拠しており、ガイダンスの更新や業界の新たなベストプラクティスに合わせて常に進化を続けています。Slack のすべての証明書は**こちら**で確認できます。

Chief Security Officer(CSO) が率いる Slack のセキュリティチームは、セキュリティプログラムの実装と管理を担当します。セキュリティアーキテクチャ、製品セキュリティ、セキュリティエンジニアリングとオペレーション、リスク検知と対応、リスクとコンプライアンスを専門とする Slack のセキュリティチームのメンバーが、CSO の指示の下サポートに当たります。

顧客データの保護

Slack のセキュリティプログラムは、顧客データへの不正なアクセスを防止することに照準を合わせています。そのために、Slack のセキュリティ対策の専門家で構成されるチームは、社員同士が部門の枠を超えて協力し合い、リスクを特定して軽減し、ベストプラクティスを実装し、常に改善の道を切り拓くことに徹底して取り組んでいます。

デザインに基づく安全性

Slack の製品セキュリティチームは、主に当社のオープンソースツール goSDL を利用した、堅牢なセキュア開発ライフサイクルを構築しました。このプロセスについて詳しくは、**こちら**のブログ投稿をお読みください。Slack では、デザインフェーズとテストフェーズのすべての脆弱性を検出するべく尽力していますが、時として不具合も発生します。そのことを想定し、当社では公開バグ報奨金プログラム (**こちら**) を設け、潜在的なセキュリティの脆弱性に関する信頼性の高い開示を促しています。特定されたすべての脆弱性は、正確性が検証され、優先順位付けされて、解決までトラッキングされます。

本書は、お客様のご参考のために作成された英語版の参考訳であり、可能な限り正確であるように努めていますが、誤りを含む可能性があることをご了承ください。英語版と齟齬がある場合、英語版の定めが優先するものとします。

暗号化

- **伝送中のデータ**
  Slack クライアントと Slack サービスの間でデータを伝送する際には、強力な暗号化プロトコルが使用されます。Slack のサービスは、伝送中のすべてのトラフィックを暗号化するために推奨される、最新のセキュアな暗号スイートに対応しています。たとえば、クライアント側でサポートされている場合には必ず TLS 1.2 プロトコル、AES256 暗号化、SHA2 署名を使用します。

- **保管中のデータ**
  Slack のプロダクションネットワークに保管されているデータは、FIPS 140-2 に準拠する暗号化標準を利用して暗号化されています。この暗号化標準は、リレーショナルデータベース、ファイルストレージ、データベースバックアップなど、Slack のシステム内に保管されるあらゆるタイプのデータに適用されます。すべての暗号化キーは、アクセスが厳しく制限される、分離されたネットワーク上のセキュアなサーバーに保管されています。Slack では、秘密情報の保管、検索、廃棄を保護するために、暗号化キーやサービスアカウント認証情報などの適切な安全策を導入しています。

Slack の顧客データは、それぞれ他の顧客データとは論理的に分離された状態で、Slack 社の共有のインフラストラクチャでホストされています。ストレージテクノロジーを組み合わせることで、顧客データをハードウェア障害から保護し、リクエストに応じて即座にデータが返されるようにしています。Slack のサービスは、業界トップのサービスプロバイダーが保守管理するデータセンターでホストされています。これらのデータセンターは、Slack の運用環境を構成するサーバーやインフラに最先端の物理的保護を提供します。Slackは、組織が自身のデータを保存する国やリージョンを選択することを可能とするデータレジデンシー機能も提供します。データセンターは、Slack の運用環境を構成するサーバーやインフラに最先端の物理的保護を提供します。Slackは、組織が自身のデータを保存する国やリージョンを選択することを可能とするデータレジデンシー機能も提供します。

ネットワークセキュリティとサーバーの強化

Slack では、システムを個別のネットワークに分散させ、機密データの保護を強化しています。テストや開発活動をサポートするシステムは、Slack のプロダクションインフラをサポートするシステムとは別のネットワークでホストされています。Slack のプロダクションフリート内のすべてのサーバーは、不要なポートの無効化や、デフォルトパスワードの削除などにより強化され、環境内での一貫性を保つために基本構成イメージが適用されます。

オープンなパブリックネットワーク (インターネット) からの Slack のプロダクション環境へのネットワークアクセスは制限されており、インターネットからアクセスできるプロダクションサーバーはごくわずかです。Slack の領域内で公開されているのは、Slack サービスをユーザーに提供するために不可欠なネットワークプロトコルのみであり、DDoS (distributed denial of service) 攻撃に対する防衛策がネットワーク境界上に実装されています。さらに Slack では、ホストベースの侵入を検知し予防するアクティビティと

して、すべてのシステムコールをロギング、モニタリング、監査しており、侵入の可能性を示すシステムコールに対するアラートを配備しています。

エンドポイントのセキュリティ

Slack のスタッフに支給されるすべてのワークステーションは、Slack自身 により、当社のセキュリティ基準を満たすように構成されています。これらのセキュリティ基準では、すべてのワークステーションが Slack のエンドポイント管理ソリューションによって適切に構成、更新、トラッキング、モニタリングされることが必須とされています。Slack のデフォルト構成では、保管中のデータを暗号化し、強力なパスワードを設定し、アイドル時にはロックするようにワークステーションがセットアップされます。ワークステーションでは、最新のモニタリングソフトウェアを実行して、潜在的なマルウェア、未許可のソフトウェアやモバイルストレージ端末が報告されるようになっています。Slack の業務で使用するモバイル端末は、Slack のセキュリティ標準を確実に満たすよう、該当するモバイル端末管理システムに登録する必要があります。

アクセスコントロール

- **プロビジョニング**
  Slack ではデータ漏洩のリスクを最小限に抑えるため、アクセスを与える際には、最小権限および役割ベースの権限の原則に従っています。従業員は、現在の職責を果たすために合理的に必要と認められるデータにのみアクセスする権限が与えられます。すべてのプロダクションアクセスは、四半期に 1 回以上審査を受けます。

- **認証**
  Slack では、データへの不正アクセスのリスクをさらに軽減するため、顧客データを格納するプロダクション環境も含め、機密データを収めるシステムへのすべてのアクセスに対して多要素認証を適用しています。また、そうした個々のデバイスにおける多要素認証に加えて、可能な限り秘密鍵を使った認証を行っています

- **パスワード管理**
  Slack では、承認済みのパスワードマネージャーを使うことをスタッフに義務付けています。パスワードマネージャーは一意の複雑なパスワードを生成、保管、入力することで、パスワードの再利用、フィッシング、その他パスワード関連のリスクを防ぎます

システムのモニタリング、ロギング、アラート

Slack ではサーバー、ワークステーション、モバイル端末をモニタリングし、企業インフラとプロダクションインフラにおけるセキュリティ状態を総合的に確認し、分析しています。Slack のプロダクションネットワークの全サーバーで行われた、管理権限によるアクセス、特権コマンドの使用、システムコールはロギングされ、最低 2 年間保存されます。ログ分析は、潜在的な問題検出に関して実用的な範囲まで自動化され、

本書は、お客様のご参考のために作成された英語版の参考訳であり、可能な限り正確であるように努めていますが、誤りを含む可能性があることをご了承ください。英語版と齟齬がある場合、英語版の定めが優先するものとします。

責任者にアラートを出します。すべてのプロダクションログは、関係するセキュリティ担当者のみにアクセスが制限された、別個のネットワークに保存されます。

データの保存と廃棄

顧客データは、エンドユーザーが削除した時点、または顧客管理者が設定したメッセージの保存期限が切れた時点で、速やかに削除されます。Slack は現在実行中のプロダクションシステムからすべての情報 (チーム名、Web サーバーのアクセスログの URL に埋め込まれた検索条件を除く) を物理的に削除します。また、バックアップは 14 日間以内に廃棄されます。

Slack のホスティングプロバイダーは、ディスクを再利用する前に、そのディスクからデータが義務付けられた方法で削除されていることを確認する責任を負います

災害復旧と事業継続プラン

Slack では、ホスティングプロバイダーが導入した、プロダクション環境を４ヶ所の物理的に分散された拠点で運用するサービスを利用しています。

これら 4 つの拠点は同じ地理的地域にありますが、通信環境や電源設備が損なわれた場合や、その他の一般的な拠点特有の障害が発生した際に、Slack サービスを保護します。プロダクションでのトランザクションはこれらの分散された運用環境間で複製され、いずれかの拠点で災害などの障害が発生したとしても、Slack のサービスが停止しないよう保護します。Slack では、プロダクションデータの完全なバックアップコピーを一次運用環境から大きく離れた場所に保持することも行っています。この遠隔拠点に、少なくとも 1 日に 1 回完全なバックアップが保存され、トランザクションは継続的に保存されています。Slack は少なくとも四半期ごとにバックアップをテストして、正常に復元できることを確認します。

セキュリティの不具合への対応

Slack では、潜在的なセキュリティの不具合に対応するためのポリシーと手順 (ランブック(run book)とも呼ばれる) を確立しています。すべてのセキュリティ上の不具合は、Slack のリスク検知と対応を専門とするDetection and Responseチームによって管理されます。ランブックでは、問題対応プロセスを通じて管理する必要があるイベントのタイプが定義され、重大度に基づいて分類されています。不具合の発生時には、影響を受けるお客様にカスタマーエクスペリエンスチームからメールで通知されます。問題対応手順は、少なくとも年に 1 回テストされ、更新されます。

本書は、お客様のご参考のために作成された英語版の参考訳であり、可能な限り正確であるように努めていますが、誤りを含む可能性があることをご了承ください。英語版と齟齬がある場合、英語版の定めが優先するものとします。

ベンダーの管理

Slack では運用を効率化するために、下請けのサービス企業を利用しています。このような下請けサービス企業が Slack のプロダクション環境のセキュリティに影響を及ぼす可能性がある場合、Slack では、当社のセキュリティ体制を確実に維持するために必要な措置を取ります。そのため、Slack のお客様に対する機密保護の取り組みを遵守することを求める契約を、サービス企業と結んでいます。Slack では、すべてのサービス企業を利用する前に、年に 1 回以上の審査を実施し、企業の情報保護の効果的な運用をモニタリングします。Slack の下請けサービス企業については、**こちら**でご確認ください。

第三者機関による検証

- **セキュリティコンプライアンス監査**
  Slack では、自社のセキュリティ対策の設計と運用の効率性を絶えずモニタリングし、監査し、改善しています。こうしたアクティビティは、資格を有する第三者の監査機関と、Slack 社内のリスク・コンプライアンスチームの両者により定期的に実施されています。監査結果は経営陣に報告され、すべての調査結果について解決まで随時トラッキングされます。Slack の証明書一式については、**こちら**でご確認ください。

- **ペネトレーションテスト**
  Slack では、コンプライアンス監査に加えて、年に 1 回以上アプリケーションレベルとインフラレベルでペネトレーションテストを実施する独立組織と契約しています。こうしたテストの結果は経営陣に報告され、選別され、優先順位が付けられて、随時是正されます。お客様は、こうしたアクティビティの事業計画を、担当のアカウントエグゼクティブを通じてリクエストして受け取ることもできます。

- **顧客主導の監査とペネトレーションテスト**
  Slack では、お客様が Slack の環境でセキュリティコントロール審査やペネトレーションテストを実施することを歓迎しています。これらいずれかのアクティビティの手配の仕方については、担当のアカウントエグゼクティブにお問い合わせください。

最後に

Slack は、お客様のデータを守ることを非常に大切にしています。すべてのユーザー、チーム、組織のデータは、安全に保護されて機密性が守られるべきであり、そう扱われることが期待されます。Slack はお客様のデータを保護する重要な役割を担い、その信頼を維持するために常に最善を尽くします。ご質問やご心配な点については、担当のアカウントエグゼクティブまでお問い合わせください。