

Slack のセキュリティ



データを保護してコンプライアンス要件を満たす、エンタープライズ級のセキュリティ

Slack では、エンタープライズ級のセキュリティがユーザー間のコラボレーションや業務遂行のあらゆる側面に組み込まれています。(ただし、そのために使いやすさが損なわれることはありません!) このため、最大限の価値を引き出しながら、最高の仕事を成し遂げることが可能になります。

これらの企業の皆さまから信頼いただいています



SLACK の社内セキュリティプログラム

業界をリードする Slack のセキュリティプログラムは綿密な多層防御の考え方をベースにしており、あらゆる層で Slack のオーガナイズーションとユーザーのデータを保護します。Slack では今後も、業界の標準セキュリティ規格に準拠する認定を取得し、ユーザー企業の皆さまがコンプライアンス要件を満たせるようさまざまなソリューションを提供していきます。また、ユーザーのデータを安全に保つために、アーキテクチャと運用レベルで厳格な対策を講じていきます。

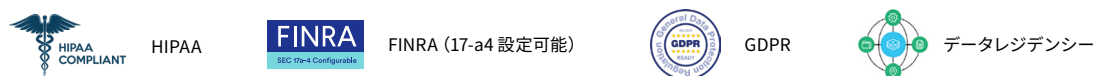
コンプライアンス認定と規制

Slack は業界の標準セキュリティ規格に準拠するだけでなく、さらにそれを超えた水準を実現しており、ユーザー企業の皆さまがそれぞれのコンプライアンス要件を満たすために利用できるソリューションを備えています。

Slack が取得している認定と認証



Slack は、以下によりユーザー企業の皆さまのコンプライアンスをサポートしています。



セキュリティアーキテクチャとプラクティス

Slack の専任セキュリティチームは、業界で認められているベストプラクティスとフレームワークを使って、ユーザー企業の皆さまのデータを安全に保ちます。私たちのセキュリティ対策は、セキュリティガバナンス、リスク管理、コンプライアンスに重点を置いています。これには、保管中と転送中のデータの暗号化、ネットワークセキュリティおよびサーバーのハードニング、管理者のアクセス制御、システムモニタリング、ロギング、警告その他が含まれます。

Slack には、強固なセキュリティとデータ保護機能が組み込まれています。これにより、アジリティを保ちながらセキュリティ上のあらゆる課題をコントロールし、可視化し、柔軟な対応が行えるのです。

ID とデバイス管理

ユーザーのいる場所に関係なく、情報の保護は ID の管理から始まります。Slack では、ユーザーとグループの管理、ID プロバイダを使用した認証の効率的な実施、種別と権限の割り当てができます。Slack では、適切なユーザーと承認されたデバイスだけが企業の Slack 内の情報にアクセスできるようにするソリューションを提供しています。

ID とアクセスコントロール

- SAML ベースのシングルサインオン
- セッションの有効期限
- 2要素認証
- SCIM/JIT によるユーザーとグループのプロビジョニング
- ドメインの申請

デバイス管理

- エンタープライズモビリティ管理 (EMM)*
- 2次認証*
- セッションの管理
- メッセージのコピーとファイルダウンロードのブロック*
- デフォルトブラウザのコントロール*
- ジェイルブレイクまたは root 化されたデバイスのブロック
- アプリの最小バージョン

データの保護

Slack では、基本的なセキュリティコントロールの一環として、保存データと転送中のデータをデフォルトで暗号化しています。また、可視性とコントロールをさらに高めるツールも提供しています。

- Enterprise Key Management (EKM)
- データ損失防止 (DLP) ^
- 監査ログ API
- グリッドワークスペース検出
- アプリとインテグレーションの管理

情報ガバナンス

どんな企業でも、データ漏洩のリスクを軽減するための継続的な戦略が必要です。しかし、規模の異なる企業に 1 つのアプローチで対応することはできません。Slack には、組織のあらゆるニーズを満たす柔軟性を備えたガバナンス機能やリスク管理機能を組み込むことができます。

- グローバル保存ポリシー
- eDiscovery^
- エクスポート (スタンダード/コーポレート)
- カスタムサービス利用規約 (TOS)

* モバイル機能

^ サードパーティのソリューション (Slack の Discovery API がサポートしているもの) が必要