Lightblue

Lightblue クラウドサービス情報セキュリティ方針

情報セキュリティ基本方針

情報セキュリティ基本方針

Lightblue では情報の適切な管理が重要な経営課題であることを認識し、お客さまをはじめとする社会全体の信頼に応え、安心して当社のサービスをご利用いただくために、情報セキュリティに関する当社の取り組みとして「情報セキュリティ基本方針」を宣言し、遵守してまいります。

クラウドサービス情報セキュリティ方針

クラウドサービスを展開するにあたっては、「利便性」と「セキュリティ」がしばしば対立することがあります。しかし、社会や経済の効率性・生産性を高めていくためには、この2つのバランスをうまくとることがとても重要です。

私たちは、利便性を損なうことなく、データのプライバシー保護や情報セキュリティ対策を全社員で徹底し、セキュリティリスクを最小限に抑えます。これにより、安全で安定したサービスの提供を実現していきます。

クラウドサービスプロバイダの情報セキュリティ機能に関する情報

当社は、国際規格（ISO/IEC 27017）に準拠した大手クラウド基盤を利用し、ディスク暗号化・冗長ストレージ・24時間体制の監視を標準装備した環境でサービスを提供しています。データは国内データセンターに保管し、業界標準の強力な暗号化技術を採用しています。

セキュリティに配慮した開発のライフサイクル

当製品で利用される全てのコードは、本番反映前に自動テスト、手動テストおよびソースコードレビューを行い、これらを通過したもののみが、本番環境へと反映されます。

役割と責任の明確化

情報セキュリティ管理体制の構築

当社は、組織を俯瞰した情報セキュリティ対策を推進するため、CTOが最高情報セキュリティ責任者（CISO）を兼任しています。これにより、CTOのリーダーシップのもと、情報セキュリティに関する方針決定を適切に行い、組織全体に対して情報セキュリティ対策を速やかに実施できる体制を構築します。

情報セキュリティ管理責任者の配置

当社は、情報資産の保護および適切な管理、またセキュリティ対策の推進を行うため情報セキュリティ管理責任者を配置します。

利用者の責任範囲

アカウント管理、提供機能の設定、提供機能におけるデータの登録・削除。

事業者の責任範囲

ソフトウェア開発、サーバ・ネットワーク設定、設備機器管理、監視・保守、障害対応。

データの管理と保護

データ保護

クラウドサービスで扱うデータ（個人情報含む）は業界標準のベストプラクティスに基づいて安全管理措置を講じています。

データの保管場所

クラウドサービスプロバイダ内のデータは、日本国内および日本国外のデータセンターに保管しています。データの種類やサービス要件に応じて最適な保管場所を選択し、いずれの場合においても適切なセキュリティ対策の下で管理を行います。

情報のバックアップ

データベースに保管されるイベントデータは、日次でバックアップを取得しています。バックアップは、2世代分保管されます。
但し、お客様によるバックアップデータの復元等に関する要望は、承っておりません。

ログ

アクセス制限、入力作業のログ取得など技術的安全管理を講じています。

データセンターへの通信は全て暗号化

外部からアクセスされたデータセンターへの通信は、ユーザー認証HTTPSによる高度な暗号化等を行っています。

情報のラベル付け

システム上でアシスタントごとに「組織全体公開/ユーザーを限定した公開/個人利用」を選択できるラベル機能を提供し、公開権限を設定することが可能です。

認証・アクセス管理

SSO

シングルサインオン（SSO）を整備し、社内システムへのアクセス時に統一的なセキュリティポリシーに基づいた安全な認証を行います。

認証情報

ワンタイムパスワードでログイン、または、企業でシングルサインオン（SSO）が設定されている場合はいずれかが選択できるようになります。ワンタイムパスワード（6桁の数字）は登録されたメールアドレスに送信されます。

アクセス権

当社は、業務上必要な最小限のアクセス権を付与する原則（最小権限の原則）を遵守します。一般ユーザー招待や権限変更は特権者のみ実行可能とします。

アイデンティティ管理

ユーザー管理機能を提供し、管理画面上からの登録・削除に加え、csvによる一括登録が可能です。これにより、ユーザーのライフサイクル（入社、異動、退職）に応じたアクセス権の管理を容易にし、不要なアクセス権の残存を防止し、情報セキュリティを強化します。

インシデント管理

情報セキュリティインシデント管理計画と準備

- 情報セキュリティ事象やインシデントに関する問合せは、サポートセンターにて対応を行います
- セキュリティインシデントが利用者に重大な影響を及ぼす場合、発生確認より24時間以内を目標にベストエフォートで公表します

ログ

アクセス制限、入力作業のログ取得など技術的安全管理を講じています。

ネットワーク・環境管理

クロックの同期

提供されるログは、UTC（世界標準時）で提供されます。

サービス内の表示に関しては、全て JST（UTC+9）で提供されます。

すべての物理・仮想サーバーの時間同期には、GCP・AWS 等のクラウドベンダーや、NICT 等の公的機関が提供する、信頼性の高い NTP サーバーを使用しています。

ネットワークの分離

当社は、業務ネットワークと管理ネットワークを論理的に分離し、不要な通信を制限します。これにより、内部からの不正アクセスやマルウェアの拡散リスクを低減します。

仮想コンピューティング環境における分離

当社は、仮想化環境において、サービス層認証と希望顧客へはIP制御によりテナント間アクセスを遮断し、データの漏洩や不正アクセスを防止します。また、仮想マシンの要塞化を実施し、不要なポートやサービスを無効化します。

技術的脆弱性・変更管理

定期的な脆弱性診断の実施

外部セキュリティ専門会社による脆弱性診断を年に1回以上実施しています。

変更管理

当サービスは、毎日細かな仕様変更や改善を繰り返しています。その中で重要なものについては、リリースノート等で通知します。

2025年9月16日改定

2025年4月1日制定

株式会社Lightblue

代表取締役 園田 亜斗夢