クラウドセキュリティ基本方針

株式会社カーリル

Version 1.0, 2025-11-13

はじめに

カーリルは、クラウドサービス及び関連サービスの提供・利用に必要なセキュリティ水準を維持向上させるため、情報セキュリティ基本方針に加え、以下のクラウドセキュリティ基本方針を策定し、ユーザーの信頼に応えるべく、継続的に各種取り組みを実施する。

本方針は、情報セキュリティ基本方針の下位方針として位置づけられ、クラウドサービス特有のセキュリティ要求事項を定めるものである。　特に、プライバシー保護を最優先とし、セキュリティの維持が必要な場合には、サービスの可用性よりもセキュリティを優先することを基本方針とする。

1. クラウドサービスの設計と実装について

ユーザーからの情報セキュリティ要求事項を勘案した基本方針をここに定め、クラウドサービスの設計及び実装に適用する。サービスごとに責任分担を文書化し、必要に応じてユーザーへ説明する。さらに、各サービスのセキュリティ対策、責任共有モデル、データ保護措置等について、ホワイトペーパーまたは同等の技術文書を整備し、ユーザーへ提供することにより透明性を確保する。

2. 責任範囲の明確化について

クラウドサービスプロバイダとカスタマの責任範囲を明確にし、責任共有モデルに基づいた適切なセキュリティ対策を実施する。

3. クラウドコンピューティング環境の隔離について

クラウドサービスは、仮想化されたマルチテナント環境を利用し、クラウドコンピューティング環境を論理的に隔離する。

4. ユーザー資産へのアクセスについて

サービス提供に必要な範囲（システム保守、障害対応、セキュリティ監視、ユーザーからの要請対応）、および法令に基づく要請を除き、ユーザーの事前許可なくユーザー資産へアクセスしない。当社内部の管理

者アクセスについては、アクセスログを取得し、定期的にレビューする。

5. 管理画面へのアクセス制御について

ユーザー向けの管理画面を提供する場合は、パスキーや多要素認証等の適切な認証方式を整備する。当社が利用するクラウドサービスの管理画面については、多要素認証を含む適切なアクセス制御を実施する。

6. ユーザーへの各種変更通知について

サービスの機能変更、APIの仕様変更、メンテナンス予定等のうち、ユーザーの利用に重要な影響を与える変更については、当社ウェブサイトへの掲載等により原則として事前に通知する。軽微な変更については、変更履歴として公開する。

7. クラウドサービスで扱うデータのアクセスと保護について

責任範囲に基づき、クラウドサービスで扱うデータの適切なアクセス管理と保護（暗号化、定期バックアップ、アクセスログ記録）を実施する。データの保管場所と利用する主要なサブプロセッサ(再委託先)を明示し、関連する法令を遵守する。新たなサブプロセッサを追加する場合は、ユーザーに事前または速やかに通知する。

8. アカウントの管理について

当社の約款に定める場合を除き、アカウント管理はユーザーの責任にて実施いただく。当社が利用するクラウドサービスについては、最小権限の原則に基づき適切に管理する。

9. インシデントの通知と対応について

クラウドサービスの可用性、パフォーマンス、セキュリティ状態を継続的に監視し、ログを適切な期間（最低90日間、セキュリティログは1年間）保管する。インシデントに関する通知および、対応やフォレンジック支援のための情報を共有する。重大インシデントが発生した場合は、可能な限り迅速にユーザーへ通知

する。

10. プライバシーの保護について

図書館の自由に関する宣言に基づき、利用者のプライバシーを保護し、検索履歴等の個人情報を厳格に管理する。

11. データの可搬性について

エクスポート対象となるユーザーデータが存在する場合、サービス利用終了時のデータのエクスポート機能を提供し、ユーザーのデータロックインを防止する。

12. データの完全削除について

サービス利用終了時は、ユーザーデータを完全かつ確実に削除する。

13. 気候変動への配慮について

エネルギー効率の高いクラウドサービスを選択し、不要なリソースを削減することで環境負荷の最小化に努める。

2025年11月13日

株式会社カーリル

代表取締役 吉本龍司

改版履歴

- 2025年11月13日 制定（v1.0）