カーリル Unitrad API
セキュリティホワイトペーパー

ISO/IEC 27017に基づくセキュリティ要求事項への取り組み

株式会社カーリル

Version 1.0, 2025-11-19

目次

セキュリティホワイトペーパーの目的

このセキュリティホワイトペーパー（以下、「本書」）は、クラウドセキュリティの国際規格である「ISO/IEC 27017：2015」の中で、お客様に向けた情報開示が求められている要求事項に対して、カーリルが提供する「カーリル Unitrad API」（以下、「本サービス」）のクラウドセキュリティに関する取り組みをご理解いただくことを目的としています。

サービスの概要

「カーリル Unitrad API（カーリル・ユニトラッド・エーピーアイ）」は全国の図書館の蔵書情報を統合的に検索できるクラウドベースのAPIサービスです。図書館システムや各種アプリケーションから、あらかじめ設定した横断検索先に対してリアルタイムの蔵書を検索できます。また、オプションサービスとして、オープンソースのユーザーインターフェースである「Unitrad UI」をベースに、各図書館のニーズに合わせたカスタマイズやホスティングを提供する「Unitrad ローカル」も利用可能です。

カーリルのプライバシーポリシー および 図書館の自由に関する宣言 に基づき、エンドユーザーのプライバシー保護を最優先とし、検索履歴などの個人情報は厳格に管理します。提供する機能についての詳細は別途提供する「Unitrad API 技術仕様書」を参照してください。

国際規格のバージョン

- ISO/IEC 27017:2015（JIP-ISMS517-1.0）

サービス利用規約のバージョン

- 2018年4月1日発行

クラウドセキュリティへの対応

1. 情報セキュリティのための方針群

1.1 情報セキュリティのための方針群（ISO27017項番: 5.1.1）

カーリルでは、クラウドサービスを提供するクラウドサービスプロバイダとして、以下のとおりに情報セキュリティに関する方針を定め、ウェブサイトに公開しています。

- 情報セキュリティ基本方針
- クラウドセキュリティ基本方針
- プライバシーポリシー

2. 情報セキュリティのための組織

2.1 情報セキュリティの役割及び責任（ISO27017項番: 6.1.1）

サービス利用規約や技術仕様書においてサービス内容を定義し、サービス提供を実施し、お客様との信頼関係を構築します。責任分界点については「2.3 クラウドコンピューティング環境における役割及び責任の共有及び分担」で明記します。サービス基盤の運用はカーリルの責任範囲としてサービスの提供範囲に含まれています。

2.2 関係当局との連絡（ISO27017項番: 6.1.3）

カーリルの本社所在地は、岐阜県中津川市坂下1645-15です。連絡先に関する最新の情報は 会社概要 から参照できます。本サービスに必要なお客様のデータは日本国内の「ISO/IEC 27001」を取得したデータセンターに保管されます。

2.3 クラウドコンピューティング環境における役割及び責任の共有及び分担（ISO27017項番: CLD.6.3.1）

本サービスは、認証不要の公開型APIとしてSaaS（Software as a Service）形式で提供されます。カーリルがAPIサービス基盤の提供と運用を担い、お客様がAPIの適切な利用とエンドユーザーへのサービス提供を担います。

領域	カーリルの責任	お客様の責任
インフラストラクチャ	クラウド基盤の選定・運用、ネットワークの管理、物理セキュリティの管理	-
プラットフォーム	OS、ミドルウェア、セキュリティパッチ、バックアップ	-
APIサービス	APIの提供、API仕様の管理、サービス品質の監視・維持	適切な利用環境の維持、API利用におけるクライアント側の実装（独自開発する場合）
ユーザーインターフェース	オープンソースUIの提供、セキュリティパッチの適用、最新機能の開発、ホスティング基盤の提供（オプション）	「Unitrad ローカル」の利用または独自開発
データ連携	各図書館との連携維持	横断検索先の決定・管理、システム更新計画や連携エラーの報告
アクセス・監視	サービス監視、ログ管理、セキュリティ監視	アクセス統計の取得
可用性	サービスレベル目標の設定、障害対応・復旧、メンテナンス通知	障害時のエンドユーザーへの情報提供
変更管理	変更の事前通知、APIバージョン管理、後方互換性の考慮	変更への対応、APIバージョンアップへの対応
インシデント対応	インシデント検知、初動対応、お客様への通知	異常の報告

領域	カーリルの責任	お客様の責任
コンプライアンス	情報セキュリティ基準の遵守、プライバシー保護、図書館の自由宣言を意識したサービス設計	エンドユーザー向けの利用規約の策定、エンドユーザー向けサービス提供における法令遵守

3. 人的資源のセキュリティ

3.1 情報セキュリティの意識向上、教育及び訓練（ISO27017項番: 7.2.2）

カーリルの従業員が、お客様の情報資産を適切に取り扱い、情報セキュリティに関するルールや手順、適用法令及び規制上の考慮事項を順守するために、定期的（年1回以上）もしくは必要に応じて随時、情報セキュリティ教育を実施しています。

4. 資産の管理

4.1 資産目録（ISO27017項番: 8.1.1）

お客様の情報資産と当社がサービスを運営するために必要となる情報資産については、明確に分離し、管理しています。

4.2 クラウドサービスカスタマの資産の除去（ISO27017項番: CLD.8.1.5）

本サービスは公開型APIサービスであり、お客様が本サービスに保存する情報資産は限定的です。お客様に関連するアクセスログなどの情報は、「クラウドセキュリティ基本方針」に基づき最低90日間保管され、「プライバシーポリシー」に従い6か月以内に自動的に削除されます。お客様が本サービスの利用を終了された場合も、同様のポリシーに基づき適切に管理・削除されます。

なお、「Unitrad ローカル」のオプションサービスをご利用の場合、サービス終了時にご希望があれば、カスタマイズされたソースコードやデザイン資産の引き渡しが可能です。引き渡しをご希望される場合は、契約終了前にあらかじめご連絡ください。

5. アクセス制御

5.1 識別情報の管理（ISO27017項番: 9.2.1）

本サービスはオープンAPIとして提供されており、サービス利用にあたってお客様側でのユーザー識別情報の管理は不要です。横断検索先のセットごとに付与されるリージョンIDにより、検索先を識別します。リージョンIDは、検索設定を識別するためのIDであり、機密情報（パスワード等）ではありません。

本サービスを運用・管理するためにカーリルが利用するクラウドサービスおよび社内システムにおいては、情報セキュリティマニュアルに基づき、識別情報を適切に管理しています。

5.2 認証情報（ISO27017項番: 9.2.4）

本サービスはオープンAPIとして提供されており、認証は不要です。

本サービスを運用・管理するためにカーリルが利用するクラウドサービスおよび社内システムにおいては、情報セキュリティマニュアルに基づき、認証情報を適切に管理しています。業務に用いるパスワードは、パスワード管理ツールによって一元管理しており、機密情報が保管されたシステムでは多要素認証またはパスキーの設定を必須としています。

5.3 アクセス権（ISO27017項番: 9.2.2）

本サービスを運用・管理するためにカーリルが利用するクラウドサービスおよび社内システムにおいては、情報セキュリティマニュアルに基づき、アクセス権を適切に管理しています。機密情報は、最小権限の原則に基づいて、必要な人のみにアクセス権限を限定しています。

5.4 特権的アクセス権（ISO27017項番: 9.2.3）

本サービスを運用・管理するためにカーリルが利用するクラウドサービスおよび社内システムにおいては、情報セキュリティマニュアルに基づき、特権的アクセス権を適切に管理しています。各システムには特権管理者を複数名で最小限になるように指定し、特権的な操作の実行には、適切な認証と承認手続きを経て実施しています。

6. 暗号化

6.1 暗号の使用（ISO27017項番: 10.1.1）

サービスの利用において保存されるユーザーデータは原則としてAES256により暗号化して保管し、通信されるデータはTLSにより暗号化しています。輸出規制の対象となる暗号化は行なっていません。仮想環境についてディスクレベル・OSレベルでの暗号化が困難な場合には、リスク評価を実施した上でアプリケーションレベルでの代替手段を講じます。

7. 物理的及び環境的セキュリティ

7.1 仮想コンピューティング環境における分離（ISO27017項番: CLD.9.5.1）

本サービスは、仮想化されたマルチテナント環境を利用したクラウドサービスとして提供されており、クラウドコンピューティング環境を論理的に隔離しています。利用しているクラウドサービスプロバイダ（Google Cloud、Amazon Web Services、さくらインターネット）は、いずれもISO/IEC 27001およびISO/IEC 27017の認証を取得しており、適切な仮想環境の分離が実施されていることを確認しています。運用基盤の一部としてISO/IEC 27017の認証範囲外のサービス（さくらインターネット・さくらのVPS）を利用していますが、同社が公表しているサービス仕様およびセキュリティアーキテクチャを確認し、カーリルの求める論理的な分離要件（マルチテナント環境における独立性の確保など）に適合していることを評価・確認した上で利用しています。

7.2 仮想及び物理ネットワークのセキュリティ管理の整合（ISO27017項番: CLD.13.1.4）

本サービスは完全にクラウドベースで提供されており、カーリルは物理的なデータセンターを保有していません。利用しているクラウドサービスプロバイダ（Google Cloud、Amazon Web Services、さくらインターネット）が、物理環境と仮想環境のネットワークセキュリティの整合性を確保していることを確認しています。

本サービスを運用・管理するためのシステムにおいては、ゼロトラストの原則に基づき、ネットワークを信頼

せず、サーバーやユーザー単位で認証と暗号化を実施しています。

7.3 ネットワークの分離（ISO27017項番: 13.1.3）

本サービスは、マルチテナント環境において各お客様のデータを論理的に分離しています。お客様間のデータやトラフィックが相互に干渉することはありません。

本サービスを運用・管理するためのシステムにおいては、情報セキュリティマニュアルに基づき、セキュリティレベルに応じたネットワークの分離を実施しています。特に運用管理者のアクセスについては、ユーザーレベルで認証と暗号化を実施しており、ネットワークレベルの認証のみに依存することを禁止しています。

8. 運用のセキュリティ

8.1 情報のラベル付け（ISO27017項番: 8.2.2）

情報資産は、その重要度に応じて「機密」「社外秘」「一般」「公開」の4つに分類し、情報セキュリティマニュアルに基づき適切に管理しています。

8.2 技術的脆弱性の管理（ISO27017項番: 12.6.1）

本サービスを運用・管理するためにカーリルが利用するクラウドサービスおよび社内システムにおいては、情報セキュリティマニュアルに基づき、技術的脆弱性を適切に管理しています。OSやソフトウェアは、常に最新のバージョンを利用することを原則とし、ソフトウェアの脆弱性に関するアラートについては、重要性を評価し、必要に応じて迅速に対応しています。

クラウドセキュリティ基本方針では、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定めており、脆弱性対応においてもこの方針に従っています。セキュリティパッチは自動適用を原則とし、夜間時間帯のメンテナンスにこだわらず、迅速に適用します。なお、適用に際しては複数のデータセンター間での冗長構成を活用し、サービス停止が発生しないようローリングアップデートを用いて実施します。（ただし、緊急性が極めて高い場合はセキュリティ保護を最優先とする場合があります）

8.3 情報のバックアップ（ISO27017項番: 12.3.1）

本サービスを運用・管理するためのデータは、定期的にバックアップを実施し、適切な期間保管しています。

8.4 ログ取得（ISO27017項番: 12.4.1）

本サービスに関連するお客様のアクセスログなどの情報は、「クラウドセキュリティ基本方針」に基づき最低90日間保管され、「プライバシーポリシー」に従い6か月以内に自動的に削除されます。

本サービスを運用・管理するためにカーリルが利用するクラウドサービスおよび社内システムにおいては、

情報セキュリティマニュアルに基づき、ログを適切に取得・管理しています。取得したログデータには、アクセス制御を実施し、ログが消去・改ざんされないようにしています。特に監査ログ（セキュリティログ）については、1年間保持します。

8.5 クロックの同期 (ISO27017項番: 12.4.4)

ログ取得の仕組みにおいては、時刻同期プロトコルを利用して、ログに正確な時刻が記録されるようにしています。

8.6 実務管理者の運用のセキュリティ (ISO27017項番: CLD.12.1.5)

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、お客様からの要請対応）、および法令に基づく要請を除き、お客様の事前許可なくお客様の情報資産にアクセスしません。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、定期的にレビューしています。

8.7 クラウドサービスの監視 (ISO27017項番: CLD.12.4.5)

本サービスで必要となる各サーバーやサービスについて、監視ツールによりリソースをリアルタイムに監視しています。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ています。

なお、サービスのリアルタイムな稼働状況やメンテナンス情報、障害発生時の状況については、カーリルヘルプデスク にて公開しています。

オープンAPIの特性上、サービスの可用性を維持するため、異常なトラフィックを検知・遮断するレートリミット（流量制限）機構を導入しています。

8.8 変更管理 (ISO27017項番: 12.1.2)

サービスの機能変更、APIの仕様変更、メンテナンス予定などのうち、お客様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などにより原則として事前に通知します。軽微な変更については、変更履歴として公開します。特に影響の大きいAPI仕様の変更については、後方互換性を考慮し、既存のお客様の利用に影響が出ないように配慮しています。

本サービスを運用・管理するためのシステムにおいては、情報セキュリティマニュアルに基づき、変更を適切に管理しています。

9. システムの取得、開発及び保守

9.1 プロジェクトマネジメントにおける情報セキュリティ（ISO27017項番: 6.1.5）

新しいシステムの導入や、既存のシステムの改修を行うときは、事前にリスクアセスメントを実施し、情報セキュリティが確実に確保されるようにしています。

9.2 セキュリティに配慮した開発のライフサイクル（ISO27017項番: 14.2.1）

本サービスを運用・管理するためのソフトウェア開発においては、情報セキュリティマニュアルに基づき、セキュリティに配慮した開発を実施しています。一般的な開発におけるセキュリティ対策（認証と認可、セッション管理、入力値の検証など）については、すべてのシステム開発において適用しています。

開発環境・試験環境・運用環境は、原則分離しており、開発環境には本番環境のデータを持ち込まないこととしています。

10. 供給者関係

10.1 供給者との合意における情報セキュリティの取扱い（ISO27017項番: 15.1.2）

供給者との契約の内容には、「機密保持に関する内容」および「情報漏洩が発生した場合の報告に関する取り決め」を含めています。供給者に対しては、委託した業務の再委託を原則禁止としており、やむを得ず再委託を実施する場合は、再委託先にも同等のセキュリティレベルが確保できるようにしています。

機密情報を扱うクラウドサービスを利用する場合は、データが保管される国を明らかにし、その国固有の法令や規制に自社のデータが悪影響を受けないかを確認しています。

サービス利用終了時のデータのエクスポートが可能であるかを確認しています。新たなサブプロセッサ（再委託先）を追加する場合は、お客様に事前または速やかに通知します。

11. 情報セキュリティインシデント管理

11.1 情報セキュリティインシデント管理の計画策定及び準備（ISO27017項番: 16.1.1）

情報セキュリティインシデントに対する対応手順を整備し、インシデント発生時に迅速に対応できる体制を構築しています。

情報セキュリティインシデントは、以下の原則に従って対応を行います:

1. 重大なインシデントについては、速やかに経営層へ報告する
2. インシデントの原因分析と同時に、被害の拡大防止および二次被害を防止するための対応を実施する
3. 個人情報の漏洩を伴う場合には、関係当局に報告する

重大インシデントが発生した場合は、可能な限り迅速にお客様へ通知します。通知は カーリルヘルプデスク に掲載します。このページでは、メールアドレスを登録することで掲載時にメールで自動通知することが可能です。

11.2 情報セキュリティ事象の報告（ISO27017項番: 16.1.2）

情報セキュリティに関する報告を受けた場合は、責任者に相談し、インシデントレベルを決定します。従業者が情報セキュリティインシデント（もしくはその疑い）を発見した場合は、速やかに報告する体制を整備しています。

11.3 証拠の収集（ISO27017項番: 16.1.7）

情報セキュリティインシデントに対する対応の結果や、インシデントの証拠となるログは、記録して保管しています。ログは適切な期間保管し、インシデント対応やフォレンジック支援のための情報を共有できるようにしています。

12. 順守

12.1 法令、規制及び契約上の要求事項（ISO27017項番: 18.1.1）

自社に関連する法令や規制を洗い出し、適切に管理しています。すべての事業活動は「プライバシーポリシー」に基づいて実施するとともに、主要なサービスにおいては個別に追加プライバシーポリシーを制定しています。

法律や規制により、一定期間の保管が求められる文書は、滅失や改ざんを防ぐため、適切なアクセス権のもとで、所定の期間、保管しています。

本サービスに必要なお客様のデータは日本国内の「ISO/IEC 27001」を取得したデータセンターに保管されます。

12.2 知的財産権（ISO27017項番: 18.1.2）

ソフトウェアを利用する場合は、事前に利用規約やライセンスを確認し、規約に違反する利用を行わないようにしています。ソースコードを公開する場合は、ライセンスを明確にするとともに依存するライブラリのライセンスも確認しています。

12.3 記録の保護（ISO27017項番: 18.1.3）

法律や規制により、一定期間の保管が求められる文書は、滅失や改ざんを防ぐため、適切なアクセス権のもとで、所定の期間、保管しています。情報資産には保管期限を定めており、保管期間を終えた資産は、速やかに削除を行っています。

12.4 情報セキュリティの独立したレビュー（ISO27017項番: 18.2.1）

定期的に内部監査を実施し、当社の情報セキュリティマネジメントシステムの状況をレビューしています。ISO/IEC 27001およびISO/IEC 27017について、第三者による審査を受け、それぞれの認証を取得、維持、更新することにより、情報セキュリティに対する取り組みの証拠としています。

サブプロセッサ

本サービスの提供にあたり、以下のクラウドサービスプロバイダおよび関連サービスをサブプロセッサとして利用しています。これらのサブプロセッサは、ISO/IEC 27001 または同等のセキュリティ基準に基づく管理体制を備えていることを確認しています。

サブプロセッサ名	利用用途	データ保管地域	認証状況
Google Cloud	サービス基盤、データ処理	日本国内 AES256・暗号化	ISO/IEC 27001, ISO/IEC 27017, ISMAP
さくらインターネット	サービス基盤、データ処理	日本国内	ISO/IEC 27001
Amazon Web Services	CDN、UIホスティング	日本国内 AES256・暗号化	ISO/IEC 27001, ISO/IEC 27017, ISMAP
Sentry, Inc.	APIサーバーのエラーの検知・分析・監視	米国	ISO/IEC 27001, SOC2 Type II

本サービスでは、Sentry に送信される例外情報・ログについて、個人情報（検索語、IP アドレス、その他識別子）が含まれないよう、ログマスク機能を設定しています。これにより、Sentry に送信される個人情報を最小化しています。

クラウドセキュリティ基本方針とISO/IEC 27017の対応表

基本方針項番	クラウドセキュリティ基本方針	ISO27017項番	ホワイトペーパーセクション
1	クラウドサービスの設計と実装	5.1.1, CLD.6.3.1	1.1, 2.3
2	責任範囲の明確化	6.1.1, CLD.6.3.1	2.1, 2.3
3	クラウドコンピューティング環境の隔離	CLD.9.5.1	7.1
4	ユーザー資産へのアクセス	CLD.12.1.5	8.6
5	管理画面へのアクセス制御	9.2.1, 9.2.4, 9.2.2, 9.2.3	5.1, 5.2, 5.3, 5.4
6	ユーザーへの各種変更通知	12.1.2	8.8
7	クラウドサービスで扱うデータのアクセスと保護	12.3.1, 12.4.1, 10.1.1, 15.1.2	8.3, 8.4, 6.1, 10.1
8	アカウントの管理	9.2.1, 9.2.4, 9.2.2	5.1, 5.2, 5.3
9	インシデントの通知と対応	16.1.1, 16.1.2, 16.1.7, CLD.12.4.5	11.1, 11.2, 11.3, 8.7
10	プライバシーの保護	18.1.1	12.1
11	データの可搬性	15.1.2	10.1
12	データの完全削除	CLD.8.1.5	4.2
13	気候変動への配慮	（ISO/IEC 27017対象外）	

改版履歴

- 2025年11月19日 初版発行（v1.0）