カーリル 学校図書館支援プログラム
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 . . . 1
サービスの概要 . . . 1
国際規格のバージョン . . . 1
クラウドセキュリティへの対応 . . . 2
1. 情報セキュリティのための方針群 . . . 2
2. 情報セキュリティのための組織 . . . 3
3. 人的資源のセキュリティ . . . 5
4. 資産の管理 . . . 5
5. アクセス制御 . . . 5
6. 暗号化 . . . 7
7. 物理的及び環境的セキュリティ . . . 7
8. 運用のセキュリティ . . . 9
9. システムの取得、開発及び保守 . . . 12
10. 供給者関係 . . . 13
11. 情報セキュリティインシデント管理 . . . 14
12. 順守 . . . 15
サブプロセッサ . . . 16
クラウドセキュリティ基本方針とISO/IEC 27017の対応表 . . . 18
教育情報セキュリティポリシーに関するガイドラインへの対応について . . . 19
SaaS型パブリッククラウドサービスの利用〔第2編9.1〕との対応関係 . . . 20
SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項〔第2編9.2〕との対応関係 . . . 23
約款による外部サービスの利用との対応関係 . . . 25
改版履歴 . . . 26

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 学校図書館支援プログラム」（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 学校図書館支援プログラム」は学校図書館などを対象にインターネットからの蔵書検索と、簡易的な予約受付の仕組みを無償で提供します。これにより、図書館システムが未導入の図書館や、蔵書検索システム（Web-OPAC）が未整備の場合でも、簡易的なウェブサービスを導入できます。

このプログラムでは、蔵書データをカーリルに送ると、蔵書検索サービスにつながるURLを発行します。生徒や先生にこのURLを通知することで利用者を限定して検索サービスを運用できます。学校のウェブサイト上からリンクすることで広く公開している図書館もあります。データはいつでも更新できます。

「カーリル Unitrad API」を基盤としており、高速で漏れの少ない検索を実現します。国立国会図書館やopenBD（出版社の提供する本の情報）などの公開データを活用することで、Excelや業務システムで管理されている最低限の所蔵データからでも高い検索精度を確保します。また、公共図書館（公立図書館）などの蔵書もあわせて検索するなど、実施するサービスモデルに応じてカーリルが対応する全国の図書館とシームレスに連携できます。

詳細は、サービス紹介ページ（ https://gk.calil.jp/ ）をご参照ください。

国際規格のバージョン

- ISO/IEC 27017:2015（JIP-ISMS517-1.0）

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）

サービスの概要 においてサービス内容を明確に定義します。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「ISO/IEC 27001」を取得したデータセンターに保管されます。また、サービスは日本国内のデータセンターから提供されます。

ただし、蔵書データの受領等に用いる一部の外部サービス（DropboxおよびGoogle Workspace）については、当該サービスの仕様により国外のリージョンにデータが保管される可能性があります。国外リージョンの利用に際しては、ISMAP で要求される管理策に相当するレベルのセキュリティ基準（ISO/IEC 27001、ISO/IEC 27017、CSA-CCM、SOC2 等）を満たしていることを確認した上で利用しています。

DropboxおよびGoogle Workspaceは、データ受領やサポート連絡などの限定的な用途で利用します。ユーザー資産の対象となるのは、蔵書データのみであるため個人情報の越境移転は発生しません。

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、学校図書館向けの検索サービス（SaaS）として提供されます。カーリルが検索システムの構築・運用およびサービス基盤の管理を担い、お客様（導入館）が蔵書データの提供と、利用者（生徒・教職員等）へのサービス提供・案内を担います。学校図書館以外においてもカーリルが認めた場合には、本サービスを利用できます。その場合は、表現を読み替えてください。

領域	カーリルの責任	導入館の責任
検索システム	検索サイトの提供、機能開発、セキュリティ対策、安定稼働の維持、バックアップ	検索サイトの動作確認
蔵書データ	受領したデータの変換・インポート処理、データの安全な保管、外部データ（書影等）の補完、不要になったデータの破棄	蔵書データの作成・抽出・更新データの送付、データ内容の正確性の担保
予約連携	外部フォーム（Googleフォーム、Microsoft Forms等）への遷移機能およびデータ連携機能の提供	連携先フォームの作成・設定、フォームで収集する個人情報の管理・保護
アクセス管理	サービスのアクセス制御（設定に基づく）、アクセスログの保管・監視	検索用URLの適切な管理・配布（生徒・保護者等への周知）、認証連携時のアカウント管理
利用者対応	障害対応、導入館からの問い合わせ対応	生徒・教職員等（エンドユーザー）への利用案内、問い合わせ対応
コンプライアンス	情報セキュリティ基準の遵守、プライバシーポリシーに基づく運用	エンドユーザーに対する利用規約の提示、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。本サービスにおいて「ユーザー資産」とは、導入館より提供される蔵書データ（CSV、Excel 等）を指します。本サービスでは個人情報（生徒・教職員の識別情報、貸出履歴等）は扱わないため、ユーザー資産には含まれません。

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）

前述のとおり、本サービスにおけるユーザー資産は蔵書データのみです。お客様が本サービスの利用終了を希望される場合は、当社担当窓口（メール等）へご連絡いただくことで、いつでも利用を終了できます。利用終了のお申し出を受領後、当社は提供された蔵書データおよびサーバー上の検索用インデックスデータを速やかに完全に削除（破棄）します。

また、サービス利用に伴い生成されたアクセスログなどの履歴情報は、「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」に従い一定期間（最大6ヶ月）経過後に自動的に削除されます。

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、原則としてユーザー登録やログインが不要なオープンな検索サービスとして設計されています。そのため、本サービスの利用にあたって、お客様（導入館）側で生徒・教職員等のユーザーID（識別情報）を管理する必要はありません。各図書館の検索サイトは「リージョンID」によって識別されますが、これは設定を呼び出すための公開識別子であり、認証を伴う機密情報ではありません。

なお、オプション機能として「Google Workspace for Education」等による認証連携を利用する場合でも、識別情報は外部の認証基盤（IdP）側で管理され、本サービス側では認証のための一時的な識別子（トークン等）のみを利用します。

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、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、検索用URLを知っている利用者がアクセスできる方式（URLベースのアクセス制御方式）を基本としており、パスワード等の認証情報の入力は不要です。オプション機能でユーザー認証（Google Workspace for Education連携等）を利用する場合も、認証プロセスはGoogle等の外部IdPに委任するため、本サービス側でパスワード等の認証情報を保持・管理することはありません。

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、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）

お客様（導入館）の管理者向けに提供される専用の管理画面（Webインターフェース）は原則として存在しません。蔵書データの更新や設定変更は、事前に登録された担当者からのメール等による申請ベースで実施されるため、お客様側での複雑なアクセス権限管理は発生しません。

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、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。さくらインターネットについては、一部ISO/IEC 27017の認証範囲外のサービス（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。提供された「蔵書目録」のデータについてはカーリル社内において「機密」データとして扱います。

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。

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、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。このサービスでは基盤に「カーリル Unitrad API」を利用しているため、このサービスの運用状況についても参考にしてください。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。

データ保管場所については、セキュリティホワイトペーパー 2.2項をご参照ください。（原則国内ですが、一部例外についての記載があります）

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	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	ISO/IEC 27001, ISO/IEC 27017, ISMAP
Elasticsearch B.V. (Elastic Cloud)	ミドルウェアの管理	日本国内	ISO/IEC 27001, ISO/IEC 27017
Google Workspace (Gmail)	サポートメールの送受信	グローバル	ISO/IEC 27001, ISO/IEC 27017, ISMAP, SOC2/3
Dropbox, Inc.	受領データの保管（AES-256による暗号化）	日本国内、米国	ISO/IEC 27001, ISO/IEC 27017, ISMAP, SOC2/3
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。

DropboxおよびGoogle Workspaceは、データ受領やサポート連絡などの限定

> 的な用途で利用します。ユーザー資産の対象となるのは、蔵書データのみであるため個人情報の越境移転は発生しません。

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）	

教育情報セキュリティポリシーに関するガイドラインへの対応について

本サービスの設計・運用にあたっては「教育情報セキュリティポリシーに関するガイドライン（令和7年3月）」を参照しています。教育委員会や学校長へ提出する「外部サービス利用申請書」や「セキュリティチェックシート」を作成する場合、以下の整理が可能です。

情報資産の種類	重要性分類	情報資産の分類
蔵書目録	**IV（公開情報相当）** ※貸出履歴や生徒個人情報は扱わない	**機密性1**（公開を前提とした情報資産） または **機密性2A**（直ちに一般に公表することを前提としていないが、児童生徒がアクセスすることを想定している情報資産）

本サービスはユーザー登録やログイン機能を排除した設計（URLベースのアクセス制御方式）となっており、「生徒の個人情報」や「貸出履歴」といった要配慮個人情報をクラウド上に一切保存しない仕様です 。そのため、万が一URLが流出した場合でも、漏えいするのは「学校にどの本があるか」という情報のみであり、個人情報の漏えい事故には繋がりません

SaaS型パブリッククラウドサービスの利用〔第2編9.1〕との対応関係

ガイドラインに例示されている各要求事項と本サービスの対応関係は以下のとおりです。

文部科学省ガイドライン項目〔第2編9.1〕	ホワイトペーパー対応箇所	適合状況の概要
(1) 利用者認証 ・適切な本人確認 ・認証機能の提供 ・管理者権限IDの管理	5.1 識別情報の管理 5.2 認証情報	**【適合・代替措置】** 本サービスは*ユーザー登録やログイン機能を提供しておらず、生徒等のID・パスワードの管理自体が不要な設計です。
(2) アクセス制御 ・アクセス権限の制限機能 ・利用者ごとの環境設定	2.3 責任分界点 5.3 アクセス権	**【適合】** 導入館（学校）側での複雑な権限管理は発生しません（メール申請ベースでの運用）。利用者（生徒）へのアクセス制御は、URLの通知範囲によってコントロールする仕様です。
(3) クラウドに保管するデータの暗号化 ・保管データの暗号化 ・保護措置の確認	12.1 法令・規制 サブプロセッサー一覧	**【適合】** データはISO/IEC 27001取得のデータセンターに保管されます。これらのプロバイダは、保存データの暗号化機能を提供しています。
(4) マルチテナント環境の管理 ・テナント間の干渉防止	7.1 仮想環境の分離 7.3 ネットワーク分離	**【適合】** マルチテナント環境において各顧客データは論理的に分離されており、相互干渉しない設計となっています。
(5) 外部脅威対策 ・監視、検知 ・境界防御	8.7 監視 サブプロセッサー一覧	**【適合】** リソースはリアルタイムに監視されており、異常トラフィックを検知・遮断するレートリミット機構が導入されています。アプリケーションレベルでのエラー検知・監視も実施しています。

文部科学省ガイドライン項目〔第2編9.1〕	ホワイトペーパー対応箇所	適合状況の概要
(6) 通信経路のセキュリティ ・通信の暗号化（TLS等）	6.1 暗号の使用	**【適合】** APIおよびウェブサービスはすべて*TLS1.2以上*で暗号化されており、通信経路の盗聴・改ざんを防止しています。
(7) 物理的セキュリティ ・データセンターの堅牢性 ・廃棄時の措置	7. 物理的・環境的 12.1 法令・規制	**【適合】** 物理データセンターは保有せず、ISO/IEC 27001/27017認証取得済みのクラウド事業者を利用することで、物理的セキュリティを担保しています。サービス基盤のデータ保管は日本国内です。
(8) 運用管理 ・サービス停止等の通知 ・冗長化、バックアップ ・ログ取得	8.3 バックアップ 8.4 ログ取得 8.8 変更管理	**【適合】** 重要な変更はウェブで事前通知されます。データは定期的にバックアップされ、アクセスログは最低90日間保管されます。
(9) マルウェア感染対策 ・サーバ等の対策 ・侵入検知	8.2 脆弱性管理	**【適合】** OSやソフトウェアは常に最新版を利用し、セキュリティパッチは自動適用を原則として迅速に対応する方針が定められています。
(10) 利用者側のセキュリティ ・端末保護 ・教育	2.3 責任分界点	〔利用者の責任を確認〕 検索用URLの適切な管理・配布や、エンドユーザー（生徒等）への利用案内は、導入館（学校）の責任範囲として定義されています。
(11) 人的セキュリティ ・従業員教育 ・守秘義務	3.1 教育及び訓練	**【適合】** 従業員に対して定期的（年1回以上）な情報セキュリティ教育を実施し、ルール遵守を徹底しています。

文部科学省ガイドライン項目〔第2編9.1〕	ホワイトペーパー対応箇所	適合状況の概要
(12) データの廃棄等 ・利用終了時の完全削除 ・アカウント抹消	4.2 資産の除去	**【適合】** 利用終了の申し出により、提供された蔵書データおよびサーバー上のインデックスデータは速やかに*完全に削除（破棄）*されます。ログも一定期間経過後に自動削除されます。
(13) ネットワーク設計 ・要件基準の確認	12.1 法令・規制 8.7 監視	**【適合】** サービスの可用性を維持するための流量制限等が設けられており、これに基づいた利用が前提となります。

SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項〔第2編9.2〕との対応関係

ガイドラインに例示されている各要求事項と本サービスの対応関係は以下のとおりです。

文部科学省ガイドライン項目〔第2編9.2〕	ホワイトペーパー対応箇所	適合・対応状況の概要
(1) 守秘義務、目的外利用及び第三者への提供の禁止 ・守秘義務契約 ・目的外利用の禁止	10.1 供給者との合意 12.1 法令、規制	**【適合】** プライバシーポリシーおよび供給者（サブプロセッサ）との契約において機密保持や情報漏洩時の報告を取り決めています。また、従業員教育（3.1）により徹底されています。
(2) 準拠する法令、情報セキュリティポリシー等の確認 ・準拠規範の開示 ・整合性の確認	1.1 情報セキュリティのための方針群 12.1 法令、規制	**【適合】** 「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」等をWeb公開し、準拠する国際規格（ISO/IEC 27017:2015）や法令遵守の姿勢を明示しています。
(3) クラウド事業者の管理体制 ・責任者の設置 ・組織体制の確認	2.1 情報セキュリティの役割及び責任 会社概要（Web参照）	**【適合】** サービスの提供範囲と責任を明確化し、サービス基盤の運用責任をカーリルが負うことを明記しています。
(4) クラウド事業者従業員への教育 ・教育・訓練の実施 ・意識向上	3.1 情報セキュリティの意識向上、教育及び訓練	**【適合】** 従業員に対し、定期的（年1回以上）または必要に応じた情報セキュリティ教育を実施しています。
(5) 情報セキュリティに関する役割の範囲、責任分界点 ・責任分界点の明示 ・整合性の確認	2.3 役割及び責任の共有及び分担	**【適合】** 「検索システム」「蔵書データ」「アクセス管理」等の領域ごとに、カーリルと導入館（学校）の責任分界を詳細な表形式で定義しています。

文部科学省ガイドライン項目〔第2編9.2〕	ホワイトペーパー対応箇所	適合・対応状況の概要
(6) 監査 ・監査状況の開示 ・安全性確認	12.4 情報セキュリティの独立したレビュー サブプロセッサー一覧	**【適合】** 第三者機関による審査（ISO/IEC 27001, ISO/IEC 27017）を受け、認証を取得・維持することで、セキュリティ対策の有効性を客観的に証明しています。
(7) 情報インシデント管理及び対応フローの合意 ・責任範囲とフロー ・連絡体制	11.1 インシデント管理の計画策定 11.2 事象の報告	**【適合】** インシデント対応手順を整備し、重大なインシデント発生時には「カーリルヘルプデスク」等を通じて迅速に通知する体制を構築しています。
(8) クラウドサービスの提供水準及び品質保証 ・SLA/SLOの確認 ・要求水準との適合	8.7 クラウドサービスの監視 サービスの概要	**【適合】** リアルタイムの稼働状況を公開しています。
(9) クラウド事業者の再委託先等との合意事項 ・再委託先の管理 ・サプライチェーンリスク	10.1 供給者との合意 サブプロセッサー一覧	**【適合】** 主要な再委託先（サブプロセッサ）をリスト化し、各社の認証取得状況（ISMAP, ISO/IEC 27001等）やデータ保管地域を確認・公開しています。
(10) その他留意事項 ・事業継続性 ・データ移行/返却 ・準拠法/管轄裁判所 ・個人情報保護	4.2 資産の除去 12.1 法令、規制 5.1 識別情報の管理	**【適合】** **データ移行:** 利用終了時は申し出によりデータを完全に削除します。 **準拠法:** 主要なデータは日本国内のデータセンターを利用し、国内法令を遵守します。 **個人情報:** 本サービスは「個人情報を扱わない」設計（URL認証、ログイン不要）であるため、個人情報保護に関する特段のリスク対応は「該当なし（リスク低）」となります。

約款による外部サービスの利用との対応関係

本サービスは、サービス概要ページ に記載した事項を約款に代替しており、「約款による外部サービスの利用」に整理されます。サービスの概要ページからダウンロードできる「印刷用資料」は履歴管理されており、変更内容についても分かりやすく提示しています。

また、セキュリティチェックリストなどへの回答が必要な場合にはサポート窓口にて対応します。

改版履歴

- 2025年11月19日 初版発行（v1.0）