



COVID-19 学校図書館支援プログラム

株式会社カーリル

Version 1.0, 2020-05-02

プログラムの概要

- インターネットからの蔵書検索と、申し込みを受け付けるための簡易的な仕組みを提供します
- 蔵書情報が外部と共有（公開）されることはありません
- 規模や利用形態にかかわらず、無償でご利用いただけます
- COVID-19に対応するための柔軟なサービス展開を支援します



提供期間

2020年5月～（少なくとも2022年7月末までは安定的にサービスを継続する）

図書館側で必要となる対応

- ISBNを含むテキストファイル（CSV）、または書誌を含むExcel形式（xlsx）の提供
- 予約受付フォームの設定（検索のみの場合は不要）
 フォームに書名、著者名、ISBNなど必要な項目をつくることで書誌情報を自動入力できます

申し込み方法

以下の事項をまとめて contact@calil.jp まで送信してください。3営業日以内にカーリルから蔵書検索URLを発行します。なおタイトルや説明文はサービス開始後に変更することもできます。

- 学校名
- 担当者とメールアドレス
- 予約連携の有無（予約連携する場合はフォームのURL）
- 蔵書データ（添付ファイル）
- 検索画面のタイトル「例:カーリル高校の蔵書検索」
- トップページの説明文（200文字程度まで・なしでも可）

技術的な特徴

- ISBNがある場合は、国立国会図書館とNACSIS-CAT（国立情報学研究所）の書誌情報から自動的に書誌情報が補完されます
- 書名・著者名などの項目が提供データに含まれる場合は上記に加え、ISBNのない本も検索対象となります
- カーリルが連携する公開されたWeb-OPACについても検索対象に含めることができます（図書館が提供するサービスにあわせて公立図書館や提携する大学図書館、電子書籍サービスなどの蔵書をあわせて検索することができます）

予約連携について

- 現時点で提供しているのは、書誌単位での予約連携機能です
- カート機能などが必要な場合はお問い合わせください
- 予約連携先としては「Googleフォーム」を推奨しています（受付時の項目は自由に設定ができます）
- 学校や図書館が作成したフォームや、メールによる送信なども可能です。「Googleフォーム」の利用が難しい場合は、希望する方法をお知らせください。

その他の注意点

- 蔵書情報が外部に広く公開されませんが、URLを知っている人はアクセスできるようになります
ユーザー認証を実施したい場合は希望する方式などについてお知らせください
- アクセス数や蔵書数に制限はありません
- 実際に利用するかどうかの判断は、検索サービス立ち上げ後の判断で構いません
- サービスの利用はいつでも中止できます。中止後は、提供いただいた蔵書データを速やかに破棄します
- プライバシーポリシー(別紙)に基づきパーソナルデータは厳重に保護されます。クッキーやGoogle Analyticsなどによるアクセストラッキングは実施しません
- 書影(本の表紙画像)はopenBDプロジェクトおよびGoogle Booksと連携しています
- データ更新は最新データをメールにてお送りいただくことにより実施します(長期的にはアップロード画面を提供予定)
- 以下のURLでデモサイトを公開しています
<https://private.calil.jp/gk-2002000-3xj40/>

よくある質問と回答

1. 生徒や先生のアクセスに限定できますか

発行するURLを限定した利用者にはしか伝えない運用方法を推奨しています。発行したURLはいつでも再発行(変更)することができます

認証方法の希望があれば技術検討が可能ですのでお知らせください

2. アクセスはどこからでも可能ですか

可能です

3. スマートフォンからの利用は可能ですか

可能です

4. 個人情報の取り扱いはどうなりますか

このプログラムでは、申し込みの連携までの対応であり、予約は原則として図書館に直接送信することを想定しています。ただし、サービスの運用にはプライバシーポリシーを適用します

5. 無償期間が終了した後、有償で継続する可能性はありますか

このプログラムは、カーリルが提供する有償サービスの体験版ではなく、カーリルの技術を迅速なサービス提供に活用することを目的としています。そのため、現時点で有償提供の予定はありませんが、図書館システムの開発会社などと積極的に連携して、発展的なサービス提供に努めます。

6. ほかの学校のデータと一緒に検索できますか

原則として各学校単位の蔵書検索を提供します。蔵書情報が共有されることはありません。ただし、地域やグループなどの運用にあわせて横断的な検索サービスの提供も可能ですのでご相談ください

7. 都道府県や団体などによりとりまとめをしてもいいですか

構いません。ご協力いただくことで円滑で迅速なサービス提供が可能となります

変更履歴

2020/05/02 初版制作



プライバシーポリシー

株式会社カーリル

Version 2.0, 2019-07-24

プライバシーポリシー

基本方針

カーリルは、プライバシーの重要性を認識しています。サービスを継続的に改善し、利便性や収益性を確保するために、特定の個人を識別する情報およびアクセス履歴を含むパーソナルデータ(以下パーソナルデータと呼びます)を収集、保存して分析する場合があります。このようなときは収集範囲と保存期間を明確に定め、必要最小限となるよう努めます。お預かりするパーソナルデータは、その重要性を十分認識し、尊重するとともに、適切に保護し、責任を持って管理します。

ユーザーの権利尊重

ユーザーからのお問い合わせ、自己情報の開示、修正、補正もしくは消去、または利用もしくは提供の拒否を求められたときは、合理的な範囲で最大限にユーザーの権利を尊重し、これに応じるよう努めます。

パーソナルデータの収集と利用

パーソナルデータをお預かりする場合は、その利用目的を明確にし、その目的を超えた収集や利用はいたしません。また、パーソナルデータの処理を伴う業務を外部へ委託する場合は、秘密の保持、再委託に関する事項、事故時の責任分担、契約終了時の個人情報の返却及び消去等について明確に定め、それに従います。

アクセスログの取り扱い

サーバー上で記録されるアクセスログ(IPアドレスや要求URL)はサーバー設備の運用目的にのみ使用され、原則として6か月以内に削除します。これらのデータは、たとえ個人を特定できないデータであったとしてもパーソナルデータとして取り扱います。

パーソナルデータの保護

パーソナルデータへの不正なアクセス、紛失、漏えい、破壊、改ざんを防止するため、[情報セキュリティ基本方針](#)に基づき必要かつ適切なセキュリティ対策を講じます。

外部とのデータ共有

ユーザーの利便性を向上したり、広告などの収益性を確保するなど明確な目的のために、ユーザーの合意を得たうえで、カーリルが適切にプライバシーポリシーを運用していると認める第三者とパーソナルデータを共有します。共有するデータは必要最小限となるよう努めるとともに、サービスごとにユーザーに分かりやすくお伝えします。また、可能な限りデータの共有を拒否するための手段を提供します。

合意なき第三者への提供

法令に基づき司法機関、行政機関から法的義務を伴う要請（捜索差押令状など）を受けた場合を除き、パーソナルデータをユーザーの合意なく第三者に提供することはありません。また、提供事実については、合理的な範囲で広く公開します。捜査関係事項照会書に基づく要請には原則として対応しません。

法令等の遵守

[個人情報保護に関する法律](#)をはじめとする個人情報の保護に関する法令、ガイドラインおよび本プライバシーポリシーを遵守します。電気通信事業者として[電気通信事業法](#)を遵守し、すべての検閲を排除するとともに、通信の秘密を守ります。図書館サービスの提供者として、[図書館の自由に関する宣言](#)と整合性のあるプライバシーポリシーを運用します。

ポリシーの改定

本プライバシーポリシーは定期的に見直し、よりよいものにしていきます。改定の際は、ウェブサイトにおいて適切に告知し、最終改定日を明記します。特にパーソナルデータの利用実態が大幅に変更となる場合は、再度合意を得るなど適切な対応をします。

お問い合わせ窓口

本プライバシーポリシーに関する問い合わせは[カーリル問い合わせページ](#)で受け付けます。

改版履歴

- 2010年3月10日 制定(v1.0)
- 2019年7月24日 改定(v2.0)



情報セキュリティ基本方針

株式会社カーリル

Version 1.0, 2019-07-09

基本声明

カーリルは、すべての情報資産に対する機密性、完全性、可用性の確保と向上に努め、図書館に求められる社会的要請に応えるため、情報セキュリティ基本方針(セキュリティポリシー)を定める。この方針に基づき情報セキュリティマネジメントシステムを確立し、継続的な情報セキュリティ対策を推進する。役員を含む全従業員がこの方針を理解し、遵守することを宣言する。

2019年7月9日

株式会社カーリル

代表取締役 吉本龍司

情報セキュリティの定義

情報セキュリティとは、機密性、完全性および可用性を確保し維持することをいう。

1. 機密性 (confidentiality): 情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること
2. 完全性 (integrity): 情報が破壊、改ざんまたは消去されていない状態を確保すること
3. 可用性 (availability): 情報へのアクセスを認められた者が、必要時にアクセスできる状態を確保すること

適用範囲

- ウェブサービスの開発、運用およびサポート業務
- APIの開発、コンサルティング、運用およびサポート業務
- 本社施設とネットワーク
- 役員を含むすべての従業員(以下従業員とする)
- すべての情報資産

実施事項

1. 適用範囲の全ての情報資産を脅威(漏えい、不正アクセス、改ざん、紛失、破損、国家権力の濫用など)から保護するための情報セキュリティマネジメントシステムを確立、導入、運用、監視、見直し、維持および改善する。
2. 情報資産の取り扱いは、関係法令および契約上の要求事項を遵守する。
3. 重大な障害または災害により事業活動が中断しないように、予防および回復手順を策定し、定期的な見直しをする。
4. 情報セキュリティの教育・訓練を全従業員に対して定期的実施する。

責任と義務

1. 情報セキュリティの責任は、代表取締役が負う。そのために代表取締役は、従業員が必要とする資源を提供する。
2. 従業員は、情報資産を守る義務がある。
3. 従業員は、本方針を維持するため策定された手順に従わなければならない。
4. 従業員は、情報セキュリティに関する事故および認知した脆弱性を報告する責任がある。
5. 本方針を維持するため策定された手順に故意または重大な過失により違反した従業員は、就業規則に従い処分する。

定期的見直し

情報セキュリティマネジメントシステムの見直しは、環境変化に合わせて定期的実施する。

改版履歴

- 2019年7月9日 制定 (v1.0)