図書クラウドサービス　ホワイトペーパー

第 1.5 版

2021 年 4 月

富士通株式会社

目 次

1 はじめに

1.1 ホワイトペーパーの目的

「図書クラウドサービスホワイトペーパー」(以下、本書)は、クラウドセキュリティの国際規格(ISO/IEC 27017：2015)で求める要求事項に対して、クラウドサービスプロバイダ(CSP)が実施する管理策をご確認いただくことを目的としています。

ISO/IEC 27017 は、情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC 27001 の取り組みを ISO/IEC 27017 で強化した管理策のガイドライン規格になります。本書では、このガイドラインの"情報セキュリティ管理策の実践の規範"箇条 5～18（17 箇条を除く）に沿って管理策を記載しています。

1.2 本書の適用範囲

本書の適用範囲は、以下の図書クラウドサービス（日本国内向けサービス）となります。

- WebiLis …… 公共図書館向けクラウドサービス
- LS@SCHOOL …… 学校図書館向けクラウドサービス
- APSELect …… 図書館 QA サポートサービス

なお、図書クラウドサービスで提供する機能の詳細に関しては、以下サイトを参照下さい。

1) 図書館ポータルサイト
   https://cloud-app-support.fjas.fujitsu.com/
2) 図書館 QA サポートサイト
   https://www.apsel.jp/

2 図書クラウドサービスについて

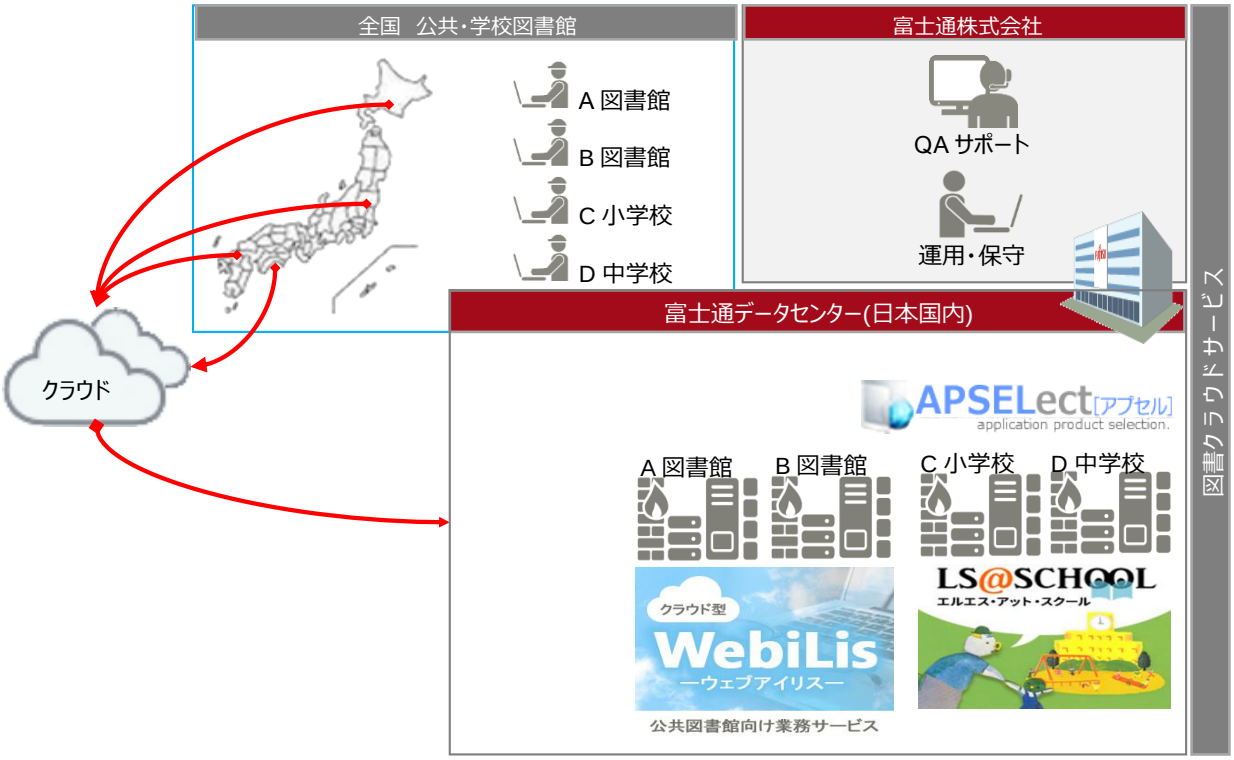
2.1 図書クラウドサービスとは

富士通株式会社が公共・学校向けに図書館業務ソフトウェアを提供する SaaS(Software as a Service)型のクラウドサービスです。サービスでは、「貸出管理」「返却管理」「予約管理」「目録登録」などを行う業務システムや、利用者がインターネットから検索・予約できる OPAC 機能を利用できます。

また、利用者向けサービスとして以下オプション機能も合わせてご利用できます。

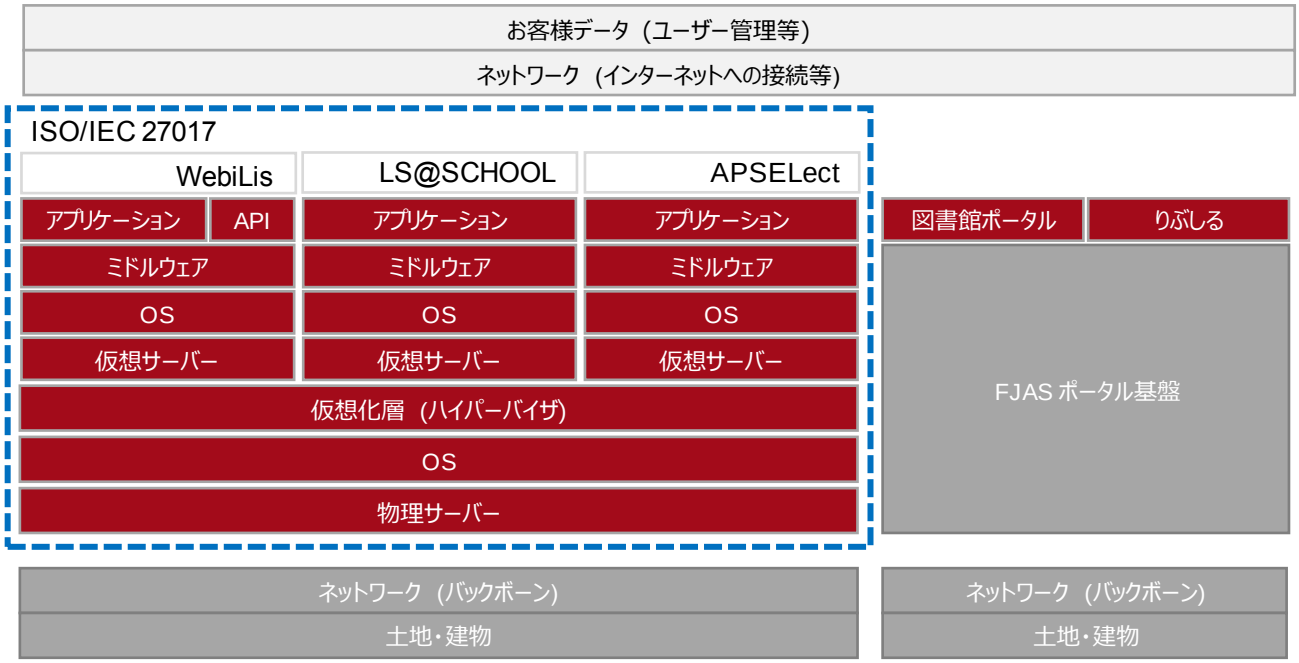
- 読書推進サービス …… 新しい本との出会いを提供する『読書推進サービス』
- ほんナビきっず …… 子供向け読書ナビゲーションサービス

2.1.1 サービス提供イメージ



2.2 責任分界点について

図書クラウドサービスに関する責任分界点は、以下になります。



:お客様、ビジネスパートナー様の管理範囲

:他事業者様の管理範囲

:当社の管理範囲

:ISO/IEC 27017 の認証範囲

3 JIS Q 27017：2016 (ISO/IEC 27017：2015) への対応

3.1 図書クラウドサービスの管理策(3.2 節)に関する見方の説明

3.2 節で、JIS Q 27017:2016(ISO/IEC 27017:2015)が求める要求事項に対する管理策を記載します。「5.1.1 情報セキュリティのための方針群」 などの番号・タイトルは、ISO27017 が求める"情報セキュリティ管理策の実践の規範"箇条 5～18（17 箇条を除く）の小項目番号・要求事項原文を示し、後に続く内容は、図書クラウドサービスの要求事項に対する解釈および管理策になります。

3.2 図書クラウドサービスの管理策

5.1.1 情報セキュリティのための方針群

クラウドサービスプロバイダ(CSP)は、クラウドサービスの提供および利用に取り組むため、情報セキュリティ基本方針を拡充することが求められています。図書クラウドサービスでは、弊社の情報セキュリティ基本方針に従いサービスを運用しています。

情報セキュリティ基本方針
(https://www.fujitsu.com/jp/about/csr/security/)

6.1.1 情報セキュリティの役割および責任

サービス仕様書にて契約やサービスの内容を定義し、サービス提供を実施しています。また、サービスご利用中に発生する QA 等の問い合わせ対応に関しては、弊社 QA サポートサイト利用時に合意頂いた「APSELect 利用規約」にてサービスの内容を定義し、サービス提供を実施しています。

6.1.3 関係当局との連絡

弊社の本社所在地は、宮城県仙台市青葉区中央 3-2-23 野村不動産仙台青葉通ビルとなります。
なお、図書クラウドサービスで保存頂くデータの所在は、日本国内のデータセンターとなります。

CLD.6.3.1 クラウドコンピューティング環境における役割および責任の共有および分担

サービス仕様書にてサービスの内容を定義し、サービス提供を実施しています。また、サービスに関するお問い合わせ先に関しては、QA サポートサイトにて受付を行っています。
なお、責任分界点に関しては前出の「2.2 責任分界点について」を参照下さい。

7.2.2 情報セキュリティの意識向上、教育および訓練

情報セキュリティ要件の周知徹底とクラウドサービスの運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練および意識向上の策を実施しています。

8.1.1 資産目録

サービス利用者様の情報資産(保存データ)とサービス提供者が運営するための情報資産は明確に分離しております。
なお、図書クラウドサービス上に利用者様が作成・保存する情報資産は、利用者様の管理範囲となります。

CLD.8.1.5 クラウドサービス利用者の資産の除去

図書クラウドサービス上に利用者様が作成・保存したサービス利用者様の情報資産(保存データ)の除去に関しては、サービス仕様書に記載された内容に従って１か月以内に破棄するものとします。但し、サービス利用者様の情報資産を含まないサービス共通ログは対象外とします。

情報資産のバックアップ等が必要となる場合には、サービス仕様書に記載された内容に従って対応を実施して下さい。

8.2.2 情報のラベル付け

ご利用いただく図書クラウドサービスの機能の詳細に関しては、各種マニュアル類も含めてQAサポートサイトにて公開しています。お客様情報資産の分類（一般情報/個人情報/秘密情報の区別、職員別権限設定）にご利用頂ける内容となっております。

9.2.1 利用者登録および登録削除

1) 図書館業務

図書クラウドサービス開始時にご契約いただいた内容に従って、管理者権限を有する利用者IDをご提供致します。提供した利用者IDにて図書館サービス運営に必要となる利用者の登録・更新・削除の機能がご利用頂けます。

提供機能の利用にあたっては、操作マニュアルを参照下さい。

2) QA、各種問い合わせ

QAサポートサイトにてサービス利用者の登録機能を提供しています。

9.2.2 利用者アクセスの提供(provisioning)

図書館業務機能として、利用者の権限管理機能を提供しています。

9.2.3 特権的アクセス権の管理

図書クラウドサービスの利用にあたっては、業務起動制御・利用者ID、パスワード認証による多要素認証技術を利用しています。

9.2.4 利用者の秘密認証情報の管理

図書クラウドサービスの初期利用時には、管理者権限を有する利用者ID・パスワードおよび図書館業務起動の為の手順をメールまたは郵送にてご連絡させて頂いております。

パスワード変更にあたっては、操作マニュアルを参照下さい。

9.4.1 情報へのアクセス制限

図書クラウドサービスのご利用にあたっては、図書館業務の管理権限を有している利用者によって機能制限を行うことができます。

また、図書クラウドサービスは、図書館業務システムのSaaS(Software as a Service)型のクラウドサービスであることから、図書館業務を扱う権限のみを付与します。

9.4.4 特権的なユーティリティプログラムの使用

全てのサービス利用においては、認証が必要となっており、セキュリティ手順を回避し各種サービス機能の利用を可能とするユーティリティプログラムの提供は行っておりません。

CLD.9.5.1 仮想コンピューティング環境における分離

1) シングルテナント環境の場合

仮想化環境を利用し、アプリケーション・オペレーティングシステム・ストレージおよびネットワーク論理的分離を実施しています。

2) マルチテナント環境の場合

マルチテナント環境では、ユーザーID によるアクセス資源の分離を実施し、別テナントへの不正アクセスを抑止しています。

CLD.9.5.2 仮想マシンの要塞化

構築するすべての仮想化環境は、ポート・プロトコル・IP アドレスへの制限を実施しています。

10.1.1 暗号による管理策の利用方針

図書館業務のお客様パスワードはハッシュ化しています。図書クラウドサービスにてお客様データをやり取りする通信は SSL/TLS 通信を用いています。

11.2.7 装置のセキュリティを保った処分又は再利用

機器の老朽化、故障等により交換した機器媒体の処理については、富士通の廃棄規定に基づき適切に廃棄処理を行っています。

12.1.2 変更管理

提供するサービスの変更を実施する場合、影響のあるお客様に変更内容を、QA サポートサイト、メーリングリストを通じて連絡を行います。

提供サービスに変更が及ばない、定期メンテナンスの場合も連絡を行います。

12.1.3 容量・能力の管理

安定的にサービスを提供するため、各テナントのキャパシティを明確にし、日々の運用プロセスの中で稼働監視を行っています。監視の結果として必要と判断された場合には、適切なタイミングにて、システムメンテナンスを実施します。

CLD.12.1.5 管理者の運用セキュリティ

ご利用いただく図書クラウドサービスの操作方法に関しては、各種マニュアル類も含めて QA サポートサイトにて公開しています。

12.3.1 情報のバックアップ

サービス利用者様が実施可能なバックアップ機能は、提供しておりません。システムおよびお客様情報資産のバックアップに関しては、対象データ・周期・方法にて弊社が日々の運用プロセスとして実施しています。世代管理は３世代、障害復旧時点は前日バックアップ取得時点となります。

12.4.1 イベントログ取得

弊社の責任範囲において、クラウドサービスの維持管理に必要となる適切なログを取得しています。必要な場合は、弊社問い合わせ窓口（QA サポートサイト）までご連絡下さい。

12.4.4 クロックの同期

図書クラウドサービスで利用する、物理・仮想サーバーは富士通提供の日本国内 NTP サーバーを参照することで時刻を同期（日本標準時）します。

CLD.12.4.5 クラウドサービスの監視

ネットワークのトラフィックおよび、CPU・メモリ・ディスクアクセスの使用率増加を検知する監視は、弊社が実施しております。現在、結果をサービス利用者様に公開できるサービス機能は有しておりません。監視結果が必要となる場合においては、弊社問い合わせ窓口（QA サポートサイト）までご連絡下さい。

12.6.1 技術的ぜい弱性の管理

定期的にぜい弱性情報の収集を実施し、サービス利用者で対応が必要となるぜい弱性情報があった場合には、QA サポートサイトまたはメーリングリストにて通知連絡致します。

図書クラウドサービス側での対応が必要になった場合には、定期・緊急メンテナンスにて対応を実施し、メンテナンス前後で対応内容および対策後結果を随時連絡致します。

13.1.3 ネットワークの分離

ネットワークの仮想化技術を利用し、他のサービス利用者様とのネットワークの分離を適切に行っています。

また、サービス提供者の社内ネットワークと図書クラウドサービス側のネットワークとは、物理的に分離されています。

CLD.13.1.4 仮想および物理ネットワークのためのセキュリティ管理の整合

物理ネットワークと論理ネットワークの整合性がとれるように設計、構築、管理を徹底しています。

14.1.1 情報セキュリティ要求事項の分析および仕様化

情報セキュリティに関しましては、情報セキュリティ基本方針および、サービス仕様書、当ホワイトペーパーに記載しています。

下記に主なセキュリティ機能を記載します。詳細は当ホワイトペーパー該当項番をご参照下さい。

- アクセス制限機能（9.4.1 情報へのアクセス制限、CLD.9.5.2 仮想マシンの要塞化）
- 通信暗号化機能（10.1.1 暗号による管理策の利用方針）
- バックアップ機能（12.3.1 情報のバックアップ）
- ログ取得機能（12.4.1 イベントログ取得）

14.2.1 セキュリティに配慮した開発のための方針

図書クラウドサービスは、IPA が発行する「安全なウェブサイトの作り方」を参考に開発し、第三者によるセキュリティ問診・診断（富士通として必須のセキュリティ要件）を実施後にサービスを提供しています。また、提供中サービスにおいても年 1 回の定期診断にてセキュリティ対策を実施しています。

15.1.2 供給者との合意におけるセキュリティの取扱い

図書クラウドサービスは、SaaS(Software as a Service)型のクラウドサービスとなり、責任分界点の詳細に関しては前出の「2.2 責任分界点について」を参照下さい。

また、図書クラウドサービスのセキュリティ対策に関しても「2.2 責任分岐点について」に記載する弊社サービスの提供範囲において必要なセキュリティ対策を実施しています。

15.1.3 ICT サプライチェーン

他のクラウドサービスの供給は受けておりません。図書クラウドサービスの提供に必要となる構成要素(データセンターや機器等)の供給については、弊社セキュリティ方針を満たすようリスク管理を実施しています。

16.1.1 責任および手順

弊社で確認できたセキュリティインシデントに関しては、情報セキュリティ基本方針に則り、適切に対応しております。

また、確認できたセキュリティインシデントがお客様に重大な影響を及ぼす可能性がある場合においては、検知から 7 営業日を目標に QA サポートサイトにて通知致します。

16.1.2 情報セキュリティ事象の報告

QA サポートサイトのお問合せにて、双方向での情報のやり取りを可能とする仕組みをご提供しています。

尚、ご利用にあたってはサイトの利用規約を参照下さい。

16.1.7 証拠の収集

裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、利用者の同意なく、利用者のデータを第三者に開示することがあります。

18.1.1 適用法令および契約上の要求事項の特定

図書クラウドサービスの利用に関して、適用される「準拠法」は「日本法」となります。

18.1.2 知的財産権

図書クラウドサービス上でサービスをご利用いただく上で知的財産権に関わるお問い合わせは、QA サポートサイトからお問い合わせ下さい。

18.1.3 記録の保護

弊社の責任範囲において、お客様アクセスログを取得しています。必要な場合は、弊社問い合わせ窓口（QA サポートサイト）までご連絡下さい。

尚、保存期間は 6 ヵ月間となります。

18.1.5 暗号化機能に対する規制

サービス利用者様が利用するサイトでは SSL/TLS による通信の暗号化を使用しています。なお、輸出規制の対象となる暗号化の利用はありません

18.2.1 情報セキュリティの独立したレビュー

社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001、ISO/IEC27017 の ISMS 認証取得、プライバシーマークの取得において第 3 者による審査を受け、情報セキュリティに対する取り組みを行うことで、常に安全なセキュリティレベルを確保しています。

4 更新履歴

版数	日付	更新内容
第 1.0 版	2018/08/01	初版公開
第 1.1 版	2018/10/31	8.2.2 情報のラベル付けに具体例を追加 12.4.4 クロックの同期について日本標準時であることを追記 14.1.1 情報セキュリティ要求事項の分析および仕様化の具体例を追加 16.1.1 重大なセキュリティインシデント通知の目標時間を追記
第 1.2 版	2019/01/15	2.2, 18.2.1 ISO/IEC 27017 認証取得による表記変更（取得予定を削除）
第 1.3 版	2019/09/02	1.2 URL の更新（http→https） 5.1.1 URL の更新（http→https） CLD.8.1.5 サービス共通ログの取り扱いについて明記
第 1.4 版	2020/10/09	1.2 本書の適用範囲 日本国内向けサービスである文言を追記 5.1.1 情報セキュリティのための方針群 情報セキュリティ基本方針 URL の変更
第 1.5 版	2021/04/01	富士通グループのフォーメーション再編に伴う社名変更