SchoolStream 職員室コネクトサービス
セキュリティホワイトペーパー

富士電機 IT ソリューション株式会社

2023 年1月28日 第二版

1. はじめに

1.1. ホワイトペーパーの目的

このホワイトペーパー（以下「本ドキュメント」といいます）は、富士電機 IT ソリューション株式会社（以下「弊社」といいます）がサービス提供する SchoolStream 職員室コネクトサービス（以下「本サービス」といいます）を、既にご利用中の方およびご利用を検討される方に向けて、本サービスにおけるセキュリティへの取り組み、または実装されているセキュリティ対策についてご紹介しています。

1.2. 情報セキュリティへの取組

弊社では、情報セキュリティマネジメント体制を客観的に評価していただくために、下記の第三者認証を取得しております。

- ISO/IEC 27001:2013(JIS Q 27001:2014)
- ISO/IEC 27017:2015(JIP-ISMS517-1.0)※
- JIS Q 15001:2017(P マーク)

また「情報セキュリティ基本方針」「クラウドサービス情報セキュリティ基本方針」「個人情報保護基本方針」を定め、すべての従業員に対して、定期的に情報セキュリティ・個人情報保護に関する教育・訓練を実施しております。

情報セキュリティに対する取組は弊社ホームページ上でも公開しております。
情報セキュリティ基本方針：https://www.fujielectric.co.jp/fsl/security/
個人情報保護基本方針：https://www.fujielectric.co.jp/fsl/privacy/
クラウドサービス情報セキュリティ基本方針：https://www.fujielectric.co.jp/fsl/cloud/

※登録活動範囲
クラウドサービスプロバイダとして以下のサービスを提供
・校務支援クラウドサービス「School Stream 職員室コネクトサービス」

クラウドサービスカスタマとして以下のサービスを利用
・クラウドコンピューティングサービス「FJcloud-V、Google Cloud Platform」
・クラウド Web Application Firewall「攻撃遮断くん」
・メール一斉同報配信サービス「SendGrid」
・クラウド環境上へのバックアップサービス「Acronis Cyber Protect Cloud」

2. 本サービスの概要

2.1. 本サービスの構成

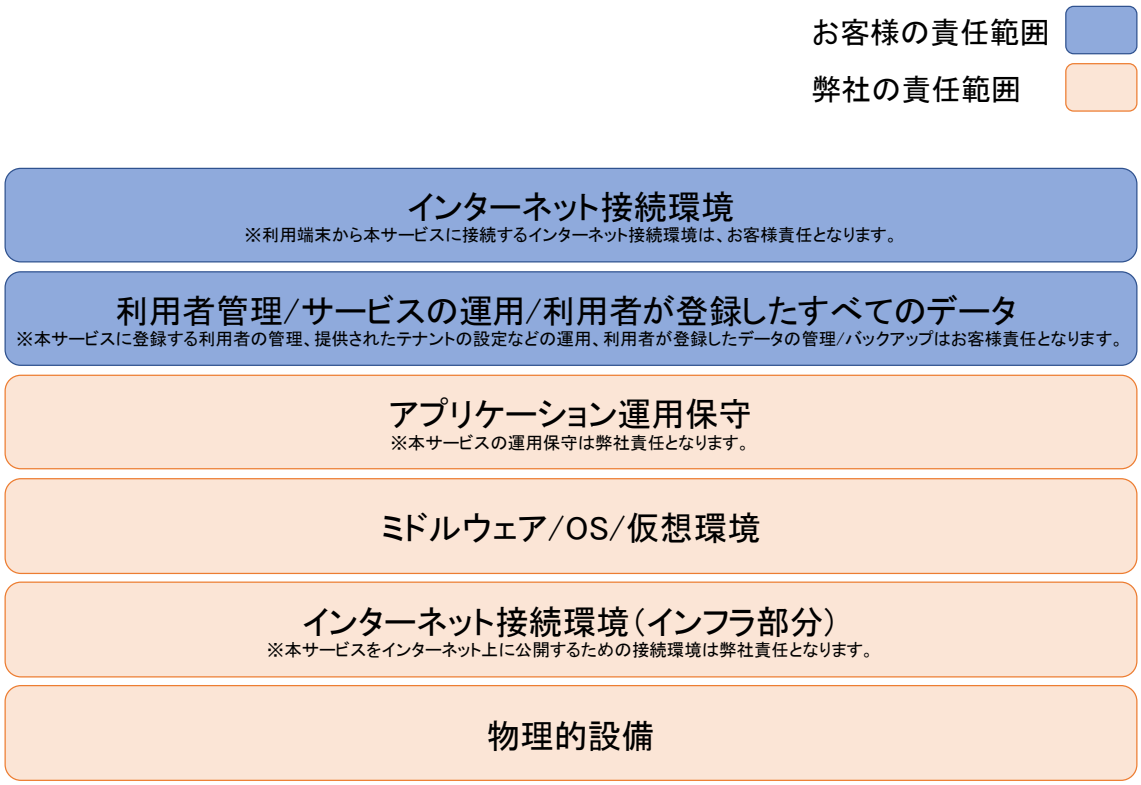
本サービスは、Fjcloud-V（富士通株式会社：提供サービス名「ニフクラ」）の東日本リージョン上に構築されております。詳細な仕様につきましては「職員室コネクトサービスサービス仕様書」および SLA をご参照ください。

また別に本サービスでは以下のクラウドサービスを利用しています。

利用サービス名	提供企業名	利用内容
攻撃遮断くん	Cyber Security Clouds 社	WAF
SendGrid	Twilio 社	お知らせ配信時のメール配信中継

2.2. 本サービスにおける責任範囲

下図に本サービスの責任範囲とお客様の責任範囲の概要を記します。



弊社の責任範囲は、物理的設備から OS/ミドルウェア/仮想環境、提供している Saas の運用保守および本サービスをインターネット上に公開するための接続環境を責任範囲として、本サービスを提供いたします。

お客様の責任範囲は、ユーザーID/パスワード等の管理、テナントの管理、利用者が登録したす

べてのデータの管理となります。 また、利用端末から本サービスに接続する環境もすべてお客様の責任範囲となります。 また、お問い合わせ窓口は操作マニュアルに記載しております。

3. 本サービスにおける物理的セキュリティ対策

3.1. 利用しているIaasについて

本サービスは、Fjcloud-V（サービス提供名：ニフクラ）が提供するIaas上に構築しています。また、構築しているリージョンは「東日本」となります。ニフクラの物理的設備などにつきましては、下記をご参照ください。

- ニフクラ　サービス利用規約
  https://pfs.nifcloud.com/term/
- ニフクラ　品質保証制度（SLA）
  https://pfs.nifcloud.com/sla/
- ニフクラ　サービスレベル目標（SLO）
  https://pfs.nifcloud.com/slo/
- ニフクラセキュリティホワイトペーパー
  https://pfs.nifcloud.com/pdf/security_whitepaper.pdf

3.2. 装置の処分又は再利用

ストレージ等廃却の際は、お客様情報が残存せぬよう、適切に処理実施の後、廃棄しております。手順、方法等詳細については非公開情報です。

4. 本サービスのサービス管理

本章では、本サービスの管理について説明いたします。

4.1 運用体制

本サービスでは、サービス提供に携わる要員に対して、スキルの把握を実施し、能力と責任に応じた育成を実施しています。その中には、遵守すべきセキュリティルールや最新のセキュリティ動向・対策等を反映した教育も含まれます。

要員はそれぞれ、テナント管理（テナント作成/削除、テナント管理者作成）、アプリケーション保守（アプリケーション、ミドルウェア、バックアップなど）、インフラ保守（仮想マシン、OS、バックアップ、セキュリティ対策（ウイルス対策、ファイアウォール、WAF など））、監視（サービス監視、死活監視、パフォーマンス監視、リソース監視など）、問合せ対応などの役割を担っています。また、本サービスの運用にあたっては、必要な最低限の権限を各担当の要員に割り当てています。

4.2 テナント管理

本サービスはマルチテナントで管理しております。テナントの作成は、本サービス契約後に配布する「テナント作成ヒアリングシート」（以下、「ヒアリングシート」とします）の情報に従って作成します。

① テナント作成

「ヒアリングシート」の情報に従ってテナントを作成し、テナント管理者のユーザーID と初期パスワードを発行し、通知いたします。パスワードは初回ログイン時に利用者によって変更する必要があります。

② テナント管理

本サービスではテナントを管理するための機能を提供しています。テナントを管理するための機能への通信については TLS の暗号化を使用しています。この機能ではテナントの利用者（教職員権限および保護者権限）を管理する機能などを提供しています。またテナント管理者の権限を有する利用者の登録も可能です。提供機能の詳細につきましては「サービス仕様書」をご参照ください。

なお、テナント管理者のユーザーID と初期パスワードを通知後のテナント内の設定はすべてお客様の責任範囲となります。

③ テナント削除

本サービスの契約終了日の翌日よりテナントへはアクセスできなくなります。本サービスに保存されていたデータは契約終了日より 2 か月経過後、すべて破棄されます。

④ その他

本サービスでは、ユーザーの権限に関する管理機能は提供しておりません。

4.3 監視

本サービスでは、安定的にサービスを提供できる仕組みを構築しており、リソースの量および稼働状況を管理しています。管理にあたり下記の監視を行っております。

- 死活監視

  仮想マシンに対する死活監視を行っています。

- リソース監視

  CPU,メモリ、ディスク使用量、ロードバランサーにおけるネットワークトラフィックについて閾値を決めて監視を実施し、閾値を超えると運用担当者にアラートが通知される仕組みを採用しています。これらの情報はお客様には提供しておりません。

- ログ監視

  システムログや WAF におけるセキュリティログなどをサービス提供に関連するログは、運用担当者によって定期的にチェックしています。なお、これらの情報はお客様には提供しておりません。

4.4 バックアップ

本サービスのサービス提供に必要なシステムのバックアップは、定期的かつ厳重に実施されています。

バックアップデータは、システム管理者のみに権限が割り当てられた領域に保存されます。また本サービスのバックアップデータは、本サービスの復旧を目的としたバックアップとなります。そのため、利用者が直接バックアップデータを利用することは出来ません。利用者固有の領域におけるバックアップが必要な場合、お客様にて取得してください。(お客様の責任範囲となります。)

なお、プログラム変更時等は臨時のバックアップを取得しています。バックアップの種別は下記の通りです。

種類	サイクル	保管期間
仮想マシン	月次(フルバックアップ)	60 日
仮想マシン	日次(増分バックアップ)	60 日

4.5 セキュリティ対策

本サービスでは、サービスを構成するシステムに対し、適切なセキュリティ対策を実施しています。

① 暗号化

本サービスを利用のすべての通信は TLS によって暗号化されます。 なお、輸出規制の対象となる暗号化の利用はありません。またお客様にて保存されるデータのうち、アカウント情報は暗号化をしております。情報または通信の保護に暗号化を用いる場合は、CRYPTREC 暗号リストに準じた強度の暗号技術を用いています。

② ネットワーク

本サービスでは、お客様がアクセスするネットワークと弊社運用担当者が利用するネットワークは分離しております。またお客様がアクセスする通信経路には WAF が設置されており、サイバー攻撃などに備えております。また、お客様間のデータ分離は、ソフトウェアにて適切に制御しております。

③ 脆弱性対応

弊社では脆弱性情報を常時収集しております。収集した情報を元に、サービスへの影響を評価し、弊社の責任範囲において影響がある場合については、速やかに対応しております。また、お客様に影響しうるインシデントについても、弊社ホームページやメールにてお伝えしております。

また、本サービスでは、定期的に第三者機関による脆弱性診断を実施しています。診断結果によって脆弱性が報告された場合には、サービスに影響がない範囲で対策を実施しています。

④ 情報へのアクセス制限

ご契約頂きましたサービスをご利用頂く際のサービスへのアクセスの制御に関しては、許可されたお客様のみアクセスできる手段を用いております。

4.6 ログの管理

本サービスでは、弊社の責任範囲において、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。なお、お客様が閲覧できるログの提供はありません。お客様責任範囲における情報セキュリティインシデントに関するログ等の証拠の収集はお客様にて実施頂く範囲となります。

種類	閲覧可能者	保管期間
利用者操作ログ	運用担当者	1 年間
アクセスログ	運用担当者	1 年間
WAF ドロップログ	運用担当者	3 か月あるいは一万件

4.7 時刻同期

本サービスでは、下記の NTP サーバに時刻同期を行っています。

ntp.nict.jp

また、本サービスでは、時刻同期に基づいてログを記録しています。

4.8 開発環境

本サービスへの追加機能などの大規模なバージョンアップについては、中長期のロードマップに基づいた開発を行っています。立案した開発計画は、責任者による確認と承認を行っています。開発用環境を別途用意しており、セキュリティ管理の方針、及び、実装や運用で考慮すべき要件を定めて、設計段階から品質を確保するためのプロセスを実施しています。システム開発に際しては、仕様書に基づいた開発とテストを行っております。

本サービスへの変更は変更管理プロセスに則って変更作業を実施しています。また、定型的変更作業については、作業手順書を整備しています。機能変更時の品質を確保するために、検証用環境にて変更機能に加えて既存機能のテストを実施し、影響度の検証、障害の有無を検証しています。

4.9 インシデント管理

本サービスにおいて、弊社の責任範囲に対して情報セキュリティインシデントが発生した場合には、お客様に対して弊社ホームページまたはメールにて速やかに報告いたします。なお、お客様が情報セキュリティインシデントを検知した際の報告先は弊社問い合わせ窓口となります。弊社問い合わせ窓口については「サービス仕様書」をご確認ください。

また、責任範囲について当ドキュメントの「サービスの責任範囲」の記述を、免責事項については「SchoolStream 職員室コネクトサービス 利用規約」をご参照ください。

4.10 契約終了後の措置

本サービスの契約終了時に弊社サービスに残存したお客様の情報資産はすべて消去いたします。データ消去に関してはサービス仕様書に記載をしておりますのでご参照ください

なお、以下の本サービスの利用にあたって作成された派生データについては、個別のユーザー情報を分離することができないため、保管期限まで情報が保有されます。

・ バックアップ（仮想マシン、データベース）
・ ログ（操作ログ、アクセスログ、WAF ドロップログ）

4.11 準拠法、合意管轄

本サービスは「SchoolStream 職員室コネクトサービス 利用規約」において、準拠法を日本法とし、専属的合意管轄裁判所を東京地方裁判所としています。本サービスは電気通信事業法、個人情報保護法、GDPR 、不正アクセス禁止法等の情報セキュリティに関する法令、規範及びガイドラインを順守し運営しています。またお客様が本サービスに保管したデータについても同様の法令等の順守が求められ、お客様自身での管理が必要となります。なお、本サービスに保存いただくデータの所在は日本国内となります。

4.12 メンテナンスおよび通知

本サービスでは、利用者向けの情報としてメンテナンス・障害情報などの情報、および変更管理に関する通知を当社ウェブサイトまたはメールにてご連絡いたします。定期的なメンテナンスに関する通知は、2 週間前を目安としています。なお障害発生時の緊急メンテナンスなど、「SchoolStream 職員室コネクトサービス利用規約」に定める本サービスの一時中断に該当する事由の場合は通知いたしません。詳細につきましては「SchoolStream 職員室コネクトサービス利用規約」をご参照ください。

また、仮想サーバの定期メンテナンスのため、下記時間帯において数分程度アクセスできない時間があります。

対象時間帯	停止時間
毎月：第 4 日曜日 22:00～翌日 4:00 までの間	数分程度

5. お客様に提供される機能

本章では、本サービスにて、お客様に提供している機能について説明いたします。

5.1. ログイン ID およびパスワード

本サービスのテナント(学校)管理者画面へログインする際には、ユーザーID 及びパスワードが必要です。また、本サービスを利用するためには、ユーザー1 名に対して、ユーザーID 及びパスワードが発行されます。発行されたユーザー ID およびパスワードは、ユーザー自身で適切に管理してください。

パスワードは以下の条件にて変更が可能です。

なお、すべてのパスワードを入力する機会おいて、パスワードが表示されないようにしています。

5.1.1 パスワードポリシー

パスワードポリシーは以下となります。

- パスワードの文字数:8 文字以上 12 文字以内
- パスワードの複雑さ:英語大文字/小文字、数字、記号のうち 3 種類以上
- パスワードの有効期限:なし
- パスワード履歴:旧パスワードと同じパスワードは設定不可

5.1.2 アカウントロック

本サービスでは、以下の条件にてテナント管理者/教職員/保護者権限のユーザーのアカウントのロック/ロック解除を行います。

① 認証失敗 5 回でアカウントをロックする

② アカウントロック後、1 時間経過でアカウントロックを自動解除する。

自動解除を待たずにアカウントロックを希望する場合、テナント管理者へご依頼ください。

5.1.3 パスワード初期化

パスワードを忘れてしまった場合には、操作マニュアルに従ってパスワードの再設定をしてください。具体的な操作方法については操作マニュアルをご参照ください。

5.2 情報のラベル付け

本サービスでは、ユーザーが個別にクラウド上に保存している情報資産の分類、ラベル付け等の管理機能は提供していません。ユーザーは、自身の責任で情報資産を分類、ラベル付け等を実施して、適切な情報管理・漏洩対策を実施してください。

5.3 操作マニュアル

本サービスをご利用頂くにあたり、必要な操作手順はご利用の手引き(操作マニュアル)として文

書化し提供しております。

6. 改編履歴

2022/09/07 初版作成
2023/01/28 ISO/IEC 27017:2015(JIP-ISMS517-1.0)取得にともない 1.2 節に追記

以上