スポテク® ホワイトペーパー

第 1.0 版

株式会社 IST ソフトウェア

目次

1. 目的

ホワイトペーパー（以下本書）は、ISMS（情報セキュリティマネジメントシステム）のクラウドセキュリティ認証である「ISO/IEC 27017：2015」で求められている要求事項の中で、当社がお客様に対し提供しているセキュリティの取組みについて明確にし、ご確認いただくことを目的としています。

ISO/IEC 27017 について

ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。

クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017 で、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 ISO/IEC 27001 の取り組みを強化します。これにより、クラウドサービスにも対応した情報セキュリティ管理体制を構築し、その実践を支援します。

2. 適用範囲について

当社の ISO/IEC 27017 の適用範囲は、以下のサービス内容に対するものです。

- スポテク®

なお、スポテクについては以下サイトをご参照下さい。

- https://portal.spo-tec.com/

お問い合わせの窓口

スポテク お問い合わせフォーム

- https://portal.spo-tec.com/?p=we-page-menu-1-5&category=25014&key=25056&type=contents

3. 用語について

本書では ISO/IEC 27017:2015 (JIS Q 27017:2016)で記されている用語については、そのまま使用しています。スポテクで利用している用語については、スポテク利用規約でご確認いただけます。

なお、本書において、「利用者」は、以下のとおり区分されます。

①「契約者」
スポテク利用契約を当社と締結し、ユーザー管理を行うことができる利用者をいいます。主に小中学校の契約担当者などが該当します。

②「指導者」
契約者からアカウントの提供を受け、アプリを使い、生徒を指導する利用者をいいます。主に小中学校の教師などが該当します。

③「生徒」
契約者からアカウントの提供を受け、アプリを使い、学習支援を受ける利用者をいいます。主に小中学校の生徒などが該当します。

本書において「利用者」と記載しているものは、①「契約者」②「指導者」③「生徒」の全てを対象としています。

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

以下に ISO/IEC 27017:2015 (JIS Q27017:2016)が求める要求事項に対する管理策を記載します。番号・タイトルは、ISO/IEC 27017 が求める「情報セキュリティ管理策の実践の規範」5～18（17 を除く）の小項目番号・要求事項原文を示しています。

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、情報セキュリティ方針を拡充することが求められています。スポテクでは、当社の情報セキュリティ基本方針、クラウドサービス提供における情報セキュリティマニュアルに基づき、サービス提供を行っています。

6.1.1 情報セキュリティの役割および責任

情報セキュリティの役割および責任について利用規約に定め、サービスを提供しています。スポテクにおける責任分界点は下図のとおりです。

お客様環境（PC、スマートフォン等）	■お客様の管理範囲
ネットワーク（インターネットへの接続）	
スポテク アプリケーション	■当社の管理範囲
仮想サーバー	
仮想化層（ハイパーバイザー）	■他事業者様の管理範囲
物理サーバー	
ネットワーク（バックボーン）	

6.1.3 関係当局との連絡

当社所在地は、東京都太田区蒲田５丁目３７番１号 ニッセイ アロマ スクエア １３Ｆとなります。また、クラウドサービスで保存いただくデータの所在は日本国内になります。

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

「6.1.1 情報セキュリティの役割および責任」項の通り、情報セキュリティの役割および責任について利用規約に定め、サービスを提供しています。クラウドコンピューティング環境における責任分界点についても同項に記載されている表をご参照ください。

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。また、個人情報保護・情報セキュリティ・コンプライアンスに関する教育を定期的に行い、プロバイダとしてカスタマデータや派生データを適切に取り扱うための周知事項の共有や実践的な訓練を実施しています。これにより、全ての関係要員がセキュリティポリシーを理解し、お客様の大切な情報資産を保護するための知識と意識を高めています。

8.1.1 資産目録

利用者の情報資産(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います。

CLD.8.1.5 クラウドサービス利用者の資産の除去

利用者がスポテクの利用を停止または終了した場合、当社は利用規約に基づき、利用者がスポテクに登録した情報や、登録した情報等を含む書面及びその複製物を削除サイクルに従って破棄します。バックアップデータについても同様に破棄します。

8.2.2 情報のラベル付け

スポテクは、一部の情報資産に対して分類情報によるラベル付け機能を搭載し、円滑なサービス提供を実現しています。

9.2.1 利用者登録および登録削除

サービス開始時に管理者権限を有する利用者 ID を管理者へ提供しています。この管理者 ID を使用して、利用者のアカウントを登録・更新・削除する機能がご利用いただけます。

9.2.2 利用者アクセスの提供(provisioning)

スポテクでは、契約団体、ならびに利用者別に、サービスの利用権限を管理する機能（機能制限設定等）を提供しており、管理者がこれらの権限設定を行うことで、参照範囲や機能実行範囲を適切に制御することができます。

9.2.3 特権的アクセス権の管理

特権的アクセス権は管理者に付与されます。管理者は、ユーザーID、パスワード認証によりセキュリティを確保しています。マスターユーザーによりログインが行われた際、システム管理者宛へメール通知を行うように設定しており、この機能により、なりすましを検出しています。

9.2.4 利用者の秘密認証情報の管理

スポテクでは、管理者がユーザー管理メニューから利用者の追加を行い、認証情報を提供させていただいております。

9.4.1 情報へのアクセス制限

スポテクのご利用にあたっては、利用者登録時に利用者毎にロール種別が設定され、ロール種別に応じて適切なアクセス制限や機能制限を行っています。

9.4.4 特権的なユーティリティプログラムの使用

利用者に対し、通常の操作手順またはセキュリティ手順を回避することのできる特権的なユーティリティプログラム（API 等）の提供は行っていません。システムの整合性とセキュリティを確保するため、すべての機能は正規の認証・認可プロセスを通じてのみ利用可能としています。

CLD.9.5.1 仮想コンピューティング環境における分離

マルチテナント環境で動作し、ユーザーID に基づく契約団体、ロール種別にてアクセス資源の分離を実施し、各リソースへのアクセス制御を実施しています。

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、マルウェア対策を行った上で、IP アドレス・プロトコル・ポートへのアクセス制限を実施し、不正アクセスの遮断を徹底しています。これにより、セキュリティリスクを最小限に抑え、安全なサービス環境を維持しています。

10.1.1 暗号による管理策の利用方針

スポテクのデータはすべて暗号化を行い、鍵の管理は AWS Key Management Service を利用しています。情報は、暗号化されたストレージのデータベースへ保存しています。お客様パスワードはハッシュ化して保管しています。

スポテクにおいてお客様データをやり取りする通信は SSL/TLS（TLS 1.3 対応）通信を用いて暗号化しています。サービス利用におけるデータ通信の暗号化については、プライバシーポリシーにも記載しています。

11.2.7 装置のセキュリティを保った処分又は再利用

当社は AWS を利用してサービスを提供しているため、物理的な機器を直接所有・管理していません。機器の廃棄や再利用に関しては、AWS のデータ廃棄ポリシーに準拠しています。AWS では NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄することを宣言しており、高いセキュリティ基準でデータ消去が実施されています。

詳細については以下の AWS 公式ブログをご参照ください：
https://aws.amazon.com/jp/blogs/news/data_disposal/

12.1.2 変更管理

提供するサービスの更新や定期メンテナンスなど、利用者へ影響のある変更を実施する場合には、事前にスポテクログイン後のお知らせ、システムの通知機能を通じて利用者に情報を提供いたします。

12.1.3 容量・能力の管理

安定的なサービス提供を行うため、各サーバーの CPU、メモリ、ディスク使用率などのリソース状況について日々稼働監視を行い、適宜増強対応を施しています。AWS CloudWatch などの監視ツールから得られる情報を定期的に確認し、システムの負荷状況を把握することで、必要に応じたキャパシティの増強を実施しています。

CLD.12.1.5 実務管理者の運用のセキュリティ

カスタマ管理者向けに特化した管理操作マニュアルを作成し、システム管理に必要な設定手順や運用方法を詳細に解説しています。

12.3.1 情報のバックアップ

サービス提供に使用している WEB サーバー（1 世代）、DB サーバー（14 世代）のスナップショットを日次で定期取得しています。バックアップデータは暗号化を行い保管しています。（10.1.1 暗号による管理策の利用方針に記載の通りです。）

12.4.1 イベントログ取得

スポテクでは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。利用者向けのログ取得機能は直接提供していませんが、重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には、過去 1 か月分のアクセスログを提供することが可能です。必要な場合は当サービスポータルのお問い合わせフォームまでお問い合わせください。
https://portal.spo-tec.com/?p=we-page-menu-1-5&category=25014&key=25056&type=contents

12.4.4 クロックの同期

スポテクでは NTP サーバーを参照することで時刻を同期（日本標準時）しています。

CLD.12.4.5 クラウドサービスの監視

外部からの攻撃や不正アクセスを常時監視し、システムの安全性を確保しています。また、サーバーの状態監視やシステムの死活監視を実施することで、サービスの可用性を維持しています。

12.6.1 技術的脆弱性の管理

初期リリース時に脆弱性診断を実施しています。また、日々脆弱性情報の収集を行い、当社の責任の範囲で対応が必要となった場合には、定期または緊急メンテナンスにて対応を実施します。対策時に生じるメンテナンス等の利用者へ影響する情報は、システムの通知機能にて案内を行っています。

13.1.3 ネットワークの分離

スポテクはマルチテナント環境の共用型サービスであるため、利用者間のネットワーク分離は行っておりません。なお、当社社内ネットワークと当サービスのネットワークは、物理的に分離して構成しています。

14.1.1 情報セキュリティ要求事項の分析および仕様化

当社では、情報セキュリティ方針の下で、お客様が要求される情報セキュリティを維持、提供しています。

主にお客様が検討される情報セキュリティの機能の仕様として、当ホワイトペーパーは以下の項目を記載しています。

- 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

当社では、セキュリティに配慮した開発方針として、開発時点からセキュリティに関するリスク対応、脆弱性対応を行い、初期リリース時に第三者による脆弱性診断を行っています。

15.1.2 供給者との合意におけるセキュリティの取扱い

スポテクにおける役割及び責任については、利用規約に定め、サービスを提供します。本サービスの責任分界点に関しては「6.1.1 情報セキュリティの役割および責任」をご参照下さい。

15.1.3 ICT サプライチェーン

当社が利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、スポテクの情報セキュリティとの整合性が取れていることを確認しています。

スポテクは、AWS をクラウドサービスプロバイダとして運用しています。AWS のコンプライアンス状況については下記をご参照下さい

https://aws.amazon.com/jp/compliance/

16.1.1 責任および手順

当社で確認したセキュリティインシデントについては、当社情報セキュリティ基本方針に則り迅速に対応を行います。利用者へ重大な影響を及ぼす可能性がある事象（データの消失、長時間のシステム停止等）が発生した場合は、サービスポータルサイト、メール、システム通知機能等により、適切に通知を行います。

セキュリティインシデントに関するお問合せについては、当サービスポータルのお問い合わせフォームより受付けています。

https://portal.spo-tec.com/?p=we-page-menu-1-5&category=25014&key=25056&type=contents

16.1.2 情報セキュリティ事象の報告

情報セキュリティ事象が発生した場合は、サービスポータルサイト、メール、システム通知機能等により、通知を行います。

また個別のお問い合わせについては、当サービスポータルのお問い合わせフォームより受付けています。

https://portal.spo-tec.com/?p=we-page-menu-1-5&category=25014&key=25056&type=contents

16.1.7 証拠の収集

裁判所からの開示請求など、法令に基づいた正当な開示請求が行われた場合、利用者への通知または同意を経ることなく、利用者のデータを該当機関へ開示することがあります。これらの開示に関する詳細は、スポテク利用規約およびプライバシーポリシーに定義しておりますので、ご確認ください。

18.1.1 適用法令および契約上の要求事項の特定

スポテクの利用に関して、適用される「準拠法」は「日本法」となります。これは本サービスの利用規約に明記しております。

18.1.2 知的財産権

スポテクをご利用いただく上で知的財産権に関わる情報の取り扱いについては、本サービスの利用規約、プライバシーポリシー内に示された取り決めに従います。また、知的財産権に関するお問い合わせについては、当サービスポータルのお問い合わせフォームより受付けています。
https://portal.spo-tec.com/?p=we-page-menu-1-5&category=25014&key=25056&type=contents

18.1.3 記録の保護

本サービスご利用にて蓄積された記録に対しては不正アクセス・改ざんを防ぐため、利用者のロール種別や契約団体に基づいてアクセス制限を実施しています。

18.1.5 暗号化機能に対する規制

スポテクでは「10.1.1 暗号による管理策の利用方針」項に記載の通り、SSL/TLS（TLS 1.3 対応）による通信の暗号化をはじめとする各種暗号化機能を利用しています。

18.2.1 情報セキュリティの独立したレビュー

当社では、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 および JIP-ISMS517-1.0（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していることで、情報セキュリティに対する取り組みの証憑とし、安全なセキュリティレベルを確保します。

5. 変更履歴

版	日付	改訂内容
第 1.0 版	2025/3/14	初版作成