クラウドセキュリティ
ホワイトペーパー

v1.1

2025年 4 月 1 日

東京書籍株式会社

目的

このホワイトペーパーは、ISO/IEC 27017:2015(情報-セキュリティ技術-ISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）に準拠したISMS（情報セキュリティマネジメントシステム）で求められている要求事項の実現のために、東京書籍株式会社（以下「当社」）がお客様に対し提供しているセキュリティ仕様について明確にするものです。

適用範囲

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

・total ID
・マイアセス
・タブドリLive!
・みんなにもっとNIMOT!
・コグトレオンライン
・iFuture

*このホワイトペーパーに記載のISO/IEC 27017に関連する項目は、お客様に公表すべき事項に限定しており、当社の認証にかかわる全ての項目を網羅しているわけではありません。

クラウドセキュリティ基本方針

当社は、お客様に安心、安全、高品質なサービスを提供するため、お客様へホワイトペーパーに定めるクラウドサービスをご提供するにあたり、クラウド環境におけるリスクの特定、および解決に努めるためのマネジメントシステムを整備いたします。

当社の事業活動に必要な情報を適切に管理し活用していくことは、経営上の重要課題であることを認識し、以下の基本方針に従い情報セキュリティ管理に取り組みます。

・お客様からのご要望により、クラウドサービスに適用するセキュリティ要求事項を、セキュリティ上影響のない範囲まで開示いたします。

・内部関係者による不正行為等のリスクに対応するために、適切な教育・訓練を定期的に行ってまいります。

・お客様の環境を確実に分離し、お客様同士でのサービスの混在等が起こらないように努めます。

・クラウドサービス担当者によるお客様の資産へのアクセスは必要最小限に制限いたします。

・仮想化環境におけるセキュリティの構築には、仕様の確認等を含め、未知のリスク等にも積極的に対応いたします。

・違反行為等に対する通知、調査や法的資料の提出等にご協力いたします。

制定日　令和6年4月1日

東京書籍株式会社
代表取締役社長
渡辺　能理夫

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

5.1.1 情報セキュリティのための方針群

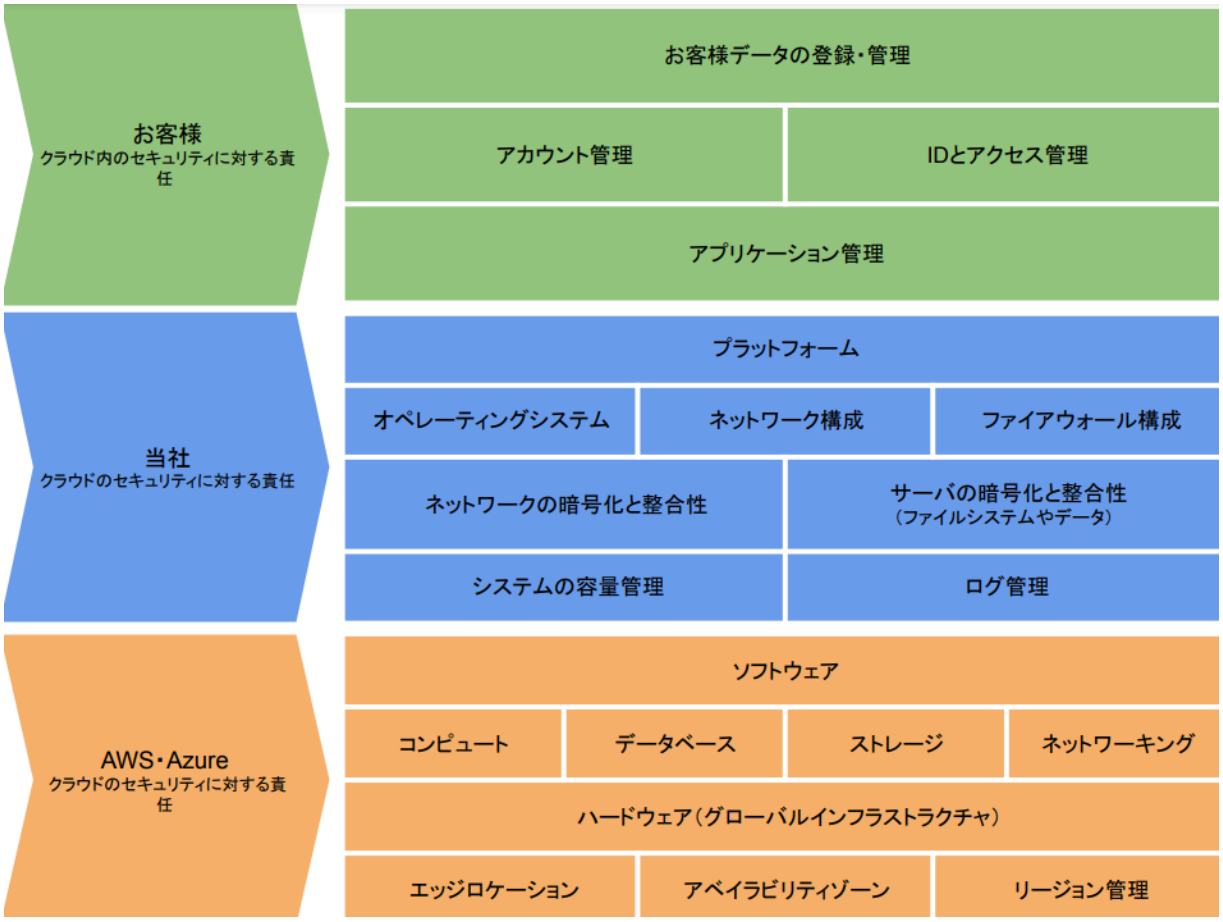
クラウドサービスプロバイダは、クラウドサービスの提供および利用に取り組むため、情報セキュリティ方針を拡充することが求められています。

適用範囲のサービスでは、当社の情報管理のセキュリティ基本方針およびクラウド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。

6.1.1 情報セキュリティの役割および責任

クラウドサービスを提供するにあたり、お客様と当社、当社が利用するクラウドサービスプロバイダとの役割および責任については、以下に定める責任共有モデルに基づくものといたします。

責任共有モデル



※このホワイトペーパーにおいて、特にことわりがない限り、「お客様」とは、各サービスにおける契約者様と、契約者様が利用権限を付与する利用者様のことをいいます。

※iFutureにおける初期データの登録は当社の責任で実施しますが、データの正当性の確認はお客様の責任となります。

6.1.3 関係当局との連絡

当社の地理的所在地は、東京都北区堀船 2-17-1です。

適用範囲のサービスで保存されるデータの所在は、Amazon Web ServiceおよびMicrosoft Azure上にあり、全て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内の役割分担および責任

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。各サービスの責任の境界に関しては「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

当社は、クラウドサービスカスタマデータおよびクラウドサービス派生データを適切に取り扱うために、従業員に対して、意識向上のための教育および訓練を実施し、委託先等にも同様の教育訓練の実施を要求します。

以下、特にことわりがない限り、「クラウドサービスカスタマデータ」とは、お客様がサービス上に作成・保存するデータのことをいい、「クラウドサービス派生データ」とは、お客様がサービスを利用することによって、サービス上に自動的に保存されるデータのことをいいます。

8.1.1 資産目録

クラウドサービスカスタマデータおよびクラウドサービス派生データは情報資産台帳上で明確に識別して分離しています。

なお、クラウドサービスカスタマデータは、お客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

クラウドサービスの利用終了時には、適切な処理をして、お客様からの要望に応じてデータを完全消去した上でリソースの削除、または停止、廃棄を行います。お客様からの要望がない場合は、保管期間終了の翌年度末までにデータを削除します。詳しくは、「東京書籍教育DX関連事業データ利活用ガイドライン」をご参照ください。

9.2.1 利用者登録及び登録解除

各サービスにおいて、管理者が一般ユーザーのアカウントの登録・削除を行うためのユーザーインターフェース（管理画面）と機能を提供しています。

9.2.2 利用者アクセスの提供(provisioning)

各サービスにおいて、お客様の権限を管理する機能を提供しています。サービスのアクセス制御は、各サービスのマニュアルで公開しています。

9.2.3 特権的アクセス権の管理

お客様は、各サービスのマニュアルに従いシステム管理者の機能を特権として利用することができます。

9.2.4 利用者の秘密認証情報の管理

お申し込み後の利用時パスワードは当社よりご案内いたします。ログイン後はお客様のパスワードポリシーに従って設定いただくことが可能です。

なお、サーバに保持されたパスワード情報は暗号化されて保管されています。

9.4.1 情報へのアクセス制限

お客様は、各サービスのマニュアルに従い、役割に応じて情報の参照範囲や機能実行範囲を定めることができます。また、必要に応じてIPアドレス制限を当社にて設定いたします。

9.4.4 特権的なユーティリティプログラムの使用

お客様に対し、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。

また、運用保守のために保持する特権的ユーティリティプログラムについては、当該プログラムの利用者を厳しく限定し、作業は事前に申請・承認を行い、作業後のレビューを実施しております。

CLD.9.5.1 仮想コンピューティング環境における分離

各サービスは、マルチテナント環境で動作し、データベース内で分割することにより資源の分離を実施しています。

CLD.9.5.2 仮想マシンの要塞化

サービスの仮想化環境は、必要なポート、プロトコル、サービスだけを有効としています。 ファイアウォール機能などにより、ポート・プロトコル・IPアドレス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

各サービスでは、ストレージ、データベース、通信(SSL/TLS)の暗号化を実施しております。

11.2.7 装置のセキュリティを保った処分または再利用

サービスを構成するクラウド事業者に対して、資源のセキュリティを保った処分または再利用のための方針および手順を確認したうえで、利用しています。なお、サービスを構成する機器として、当社の物理的装置はありません。

12.1.2 変更管理

お客様に影響のあるバージョンアップやメンテナンスを実施する場合、次のような事項をサポートサイトまたはメールにて通知します。

・変更種別
・変更予定日および予定時刻
・サービスおよびその基礎にあるシステムの変更についての説明

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、各サーバ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。監視の結果としてシステムの増強が必要と判断された場合には、適切なタイミングにて、システムの増強を実施します。

CLD.12.1.5 管理者の運用セキュリティ

提供する機能に関して、操作マニュアル、 FAQ 、利用規約などをサポートサイトへ公開、またはサービス内で提供しています。

12.3.1 情報のバックアップ

サービス提供元としてユーザ情報などを日次でバックアップしていますが、これはサービス障害時の復旧に利用するバックアップです。

お客様の操作(ユーザ削除など)によって生じたデータ消失に関しては、当社による復元は実施いたしませんので、お客様の責任においてバックアップをお願いします。
バックアップ方式や頻度の確認が必要な場合は当社のお問い合わせ窓口にて承ります。

12.4.1 イベントログ取得

当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ログ、お客様の操作ログなどを取得していますが、そのログをお客様が取得する機能は提供していません。
お客様の操作ログなどの確認が必要な場合は当社のお問い合わせ窓口にて承ります。

12.4.4 クロックの同期

システムは NTP による時刻同期を行っており、日本時間(JST)で管理しています。本サービスで記録される時刻は、すべて時刻同期に基づいて記録しています。

CLD.12.4.5 クラウドサービスの監視

各サービスは、監視機能を含むシステム構成としており、サーバの状態監視、システムの死活監視、外部からの攻撃監視、リソース監視を実施しています。
各サービスのパフォーマンスや攻撃などの監視は、当社が実施しておりますが、現在、結果をお客様に公開できるサービス機能は提供しておりません。確認結果についてお客様から求めがあった場合、当社の裁量判断により、お知らせの可否、ならびに、お知らせ可能な事項および範囲を決定いたします。

12.6.1 技術的ぜい弱性の管理

当社では、定期的に技術的ぜい弱性情報を各所から収集しております。
お客様へ共有すべき技術的ぜい弱性情報については、サポートサイトまたはメールで通知いたします。

13.1.3 ネットワークの分離

各サービスでは、開発・構築時にネットワークセキュリティ要件を決定し、用途別にネットワークを分離しており、各サービスのお客様側のネットワーク環境と各サービスの開発ネットワーク環境は分離されています。

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

当社の内部規定を策定し、文書化しています。また、変更管理プロセスにより、物理と仮想での整合が取れなくなるような変更作業を行えないようコントロールを実施しています。

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、およびこのホワイトペーパーに記載しています。セキュリティ機能として以下のような機能を提供しています。

・ウィルス対策のソフトウェアの導入
・ファイアウォールによる制御
・不正侵入検知
・Webアプリケーション保護
・セキュリティログの監視

14.2.1 セキュリティに配慮した開発のための方針

各サービスは、社内で定めるセキュリティ診断を実施後、サービスを提供しています。また、提供中のサービスにおいても年 1 回の定期診断を行い、結果に応じ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

お客様は、サービス契約締結をもってサービス仕様書および利用規約にて定義された事項に合意いただいたものとします。責任の境界に関しては「6.1.1　情報セキュリティの役割および責任」をご参照ください。

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、各サービス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。

https://aws.amazon.com/jp/compliance/
https://learn.microsoft.com/ja-jp/azure/compliance/

16.1.1 責任および手順

当社で確認できた情報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、確認できた情報セキュリティインシデントがお客様に影響を及ぼす可能性がある場合においては、サポートサイトまたはメールにて通知いたします。

16.1.2 情報セキュリティインシデントの報告

お客様からの問い合わせや報告は、当社のお問い合わせ窓口にて承ります。
当社で確認した情報セキュリティインシデントがお客様に影響を及ぼす可能性がある場合には、サポートサイトまたはメールにて通知します。

16.1.7 証拠の収集

お客様は、サービス契約締結をもって、利用規約で定めている通り、クラウドサービスカスタマデータおよびクラウドサービス派生データが、国内外の関係法令に基づき参照、閲覧される可能性があることを承諾されたものとします。

18.1.1 適用法令および契約上の要求事項の特定

利用規約の準拠法および管轄で定めている通り、準拠法は原則として日本法とし、お客様と当社との間の一切の法的紛争は、東京地方裁判所を第一審の専属的管轄裁判所とします。また、当社においての法的準拠については、法務担当を設置し、管理を行っております。

18.1.2 知的財産権

知的財産権などに必要な情報の問い合わせは、当社のお問い合わせ窓口にて承ります。

18.1.3 記録の保護

当社の責任範囲において、お客様の操作ログや契約情報の保護や廃棄については、社内規定に定め、定期的に検査を実施し、適切に管理しております。また、その利用については、当社ホームページの「個人情報の取り扱いについて」にて定めています。

18.1.5 暗号化機能に対する規制

サービスで利用している暗号化機能において、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

プライバシーマーク、ISO/IEC 27001、ISO/IEC 27017にお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ています。

変更履歴

ver.	改訂日	改訂内容
v1.0	2024/04/01	初版公開
v1.1	2025/04/01	ISO/IEC 27017規格項番に準拠した表記に変更

以上