クラウドセキュリティ

ホワイトペーパー

東京書籍株式会社

2024年 4月 1日

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-ISO27002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、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ISO27017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!
NIMOT!
コグトレオンライン
iFuture
*本文書に記載のISO27017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すべ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

東京書籍株式会社（以下「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

クラウドサービスにおけるセキュリティについて

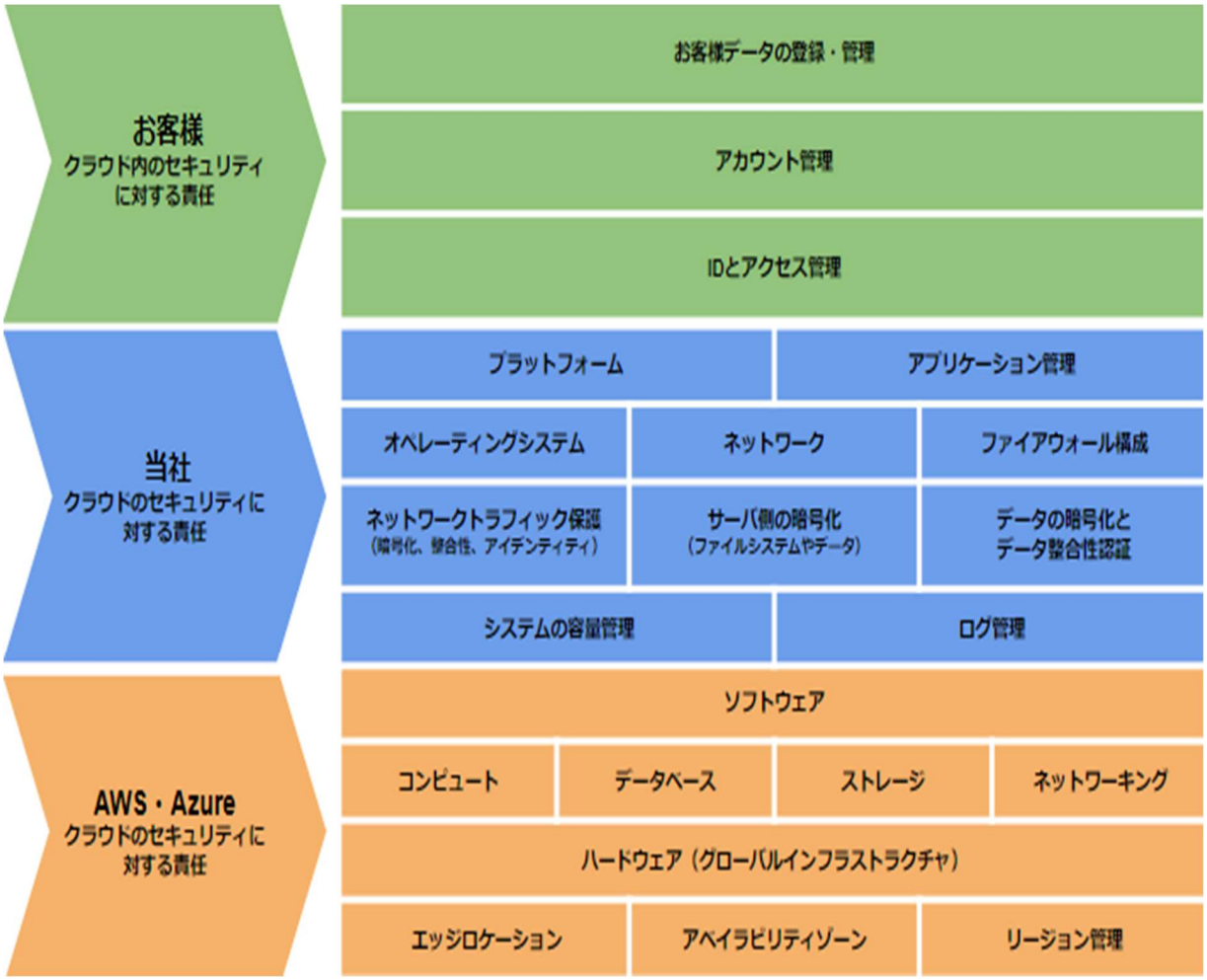
1. クラウドサービスプロバイダの地理的所在地

本社	東京都北区堀船 2-17-1

2. 役割および責任(ISO27017:6.1.1)

クラウドサービスを提供するにあたり、当社とお客様、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



3. クラウドサービスデータを保存する可能性のある国(ISO27017:6.1.3)

クラウドサービスデータの保存場所は日本国内になります。

AWSおよびMicrosoft Azureをそれぞれ日本国内リージョンにて運用しております。

4. 教育(ISO27017:7.2.2)

当社は、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、意識向上、教育および訓練を提供し、委託先等にも同様の教育訓練の実施を要求します。

5. 資産目録(ISO27017:8.1.1)

当社は、資産目録の管理を行うにあたり、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の識別を行います。

6. 資産の除去(ISO27017:CLD 8.1.5)

クラウドサービスの利用終了時には、適切な処理をして、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。

7. 仮想コンピューティング環境における分離(ISO27017:CLD 9.5.1)

仮想環境における仮想マシンは、お客様環境の混在を防ぐため、AWSおよびMicrosoft Azure上で分離されています。

8. 仮想マシンの要塞化(ISO27017:CLD9.5.2)

仮想マシンは、導入時に当社基準の要塞化手順に基づき、要塞化されたシステムのみを利用しております。

9. 暗号による管理策の利用方針(ISO27017:10.1.1)

クラウドサービス上の情報は、AWSおよびMicrosoft Azureにより暗号化しております。

暗号化の範囲：本番環境内の各リソースおよび個人情報は全て暗号化しております。

暗号の方式：データの保存先はS3、ネットワークはhttps(TLS)を使用しております。

10. 装置のセキュリティを保った処分又は再利用(ISO27017:11.2.7)

装置を処分する場合は、情報を完全に消去したうえで処分いたします。

11. 容量・能力の管理(ISO27017:12.1.3)

容量・能力についてはクラウドサービスを運用するのに十分な容量・能力を確保しております。

不足することが予測される場合、適宜増強等を行います。

12. バックアップ(ISO27017:12.3.1)

メンテナンス時にスナップショットおよびAMI(AWS限定)を取得しております。

また、システム停止のリスクを予防するため、パッチの適用前後でのバックアップも行っております。

13. イベントログ(ISO27017:12.4.1)

システム内のログについては、12ヶ月間保管しております。
ログの直接的開示は行いませんが、お客様からの要望に応じて、ログの解析等の結果をお知らせいたします。

14. クラウドサービスの監視(ISO27017:CLD12.4.5)

サービスは、下記の対象に対し常に監視を行っております。

・total ID
・マイアセス
・タブドリLive!
・NIMOT!
・コグトレオンライン
・iFuture

正常な動作をしていなかったことを検出した場合は、お客様に通知の上、対応することがあります。

15. 技術的ぜい弱性の管理(ISO27017:12.6.1)

弊社とお客様で共有すべき技術的ぜい弱性情報については、適宜ご提供しております。
また、弊社では、適宜技術的ぜい弱性情報を各所から収集しております。

16. 仮想および物理ネットワークのセキュリティ管理の整合(ISO27017:CLD13.1.4)

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。

17. 情報セキュリティ要求事項の分析および仕様化(ISO27017:14.1.1)

当社のクラウドサービスにおけるセキュリティ要求事項および仕様は、AWSおよびMicrosoft Azureの基準に準拠した上で導入しており、次の内容になります。

・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
・改ざん検知
・セキュリティログの監視

18. セキュリティに配慮した開発のための方針(ISO27017:14.2.1)

当社のクラウドサービスについては、リリース前および定期的なぜい弱性診断を実施すること、並びに、定期的なネットワーク診断を行うことを、方針として定めています。

19. 情報セキュリティ事象の報告(ISO27017:16.1.2)

お客様からの問合せや報告は、お問合せ窓口およびコールセンターにて承ります。
情報セキュリティに関する事件、事故の可能性がある場合はお知らせください。

20. 証拠の収集(ISO27017:16.1.7)

当社のクラウドサービスにおけるログ等は、ご依頼をいただいた場合、内容を精査した上で開示します。

21. 適用法令および契約上の要求事項の特定(ISO27017:18.1.1)

当社のクラウドサービスにおける準拠法は日本法と定めております。
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。

22. 知的財産権(ISO27017:18.1.2)

知的財産権に関する苦情・相談等があった場合は、当社のお問合せ窓口までお問い合わせください。

以上