クラウドセキュリティホワイトペーパー

For ISO/IEC 27017

サイバートラスト株式会社

2024 年 5 月 7 日

目的

本ホワイトペーパーは、ISO/IEC 27017:2015（情報技術－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、当社がクラウドサービスプロバイダとしてお客様にご提供しているクラウドサービスの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対するものです。

認証局アウトソーシングサービス：マネージド PKI ※
本人確認サービス：iTrust 本人確認サービス

※認証局アウトソーシングサービスにおいて一部市販クラウド環境を適用する場合があります。

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（関係当局との連絡）

ISO/IEC 27017:2015 A.6.1.3（ISO/IEC 27001:2022 管理策 5.5）

電子認証センター	日本国内
Amazon Web Services ※市販クラウド環境を適用する場合	アジアパシフィック（東京）リージョン アジアパシフィック（大阪）リージョン
さくらのクラウド ※市販クラウド環境を適用する場合	石狩リージョン 東京リージョン https://manual.sakura.ad.jp/cloud/support/region-zone.html

2. クラウドサービスデータを保存する可能性のある国（関係当局との連絡）

ISO/IEC 27017:2015 A.6.1.3（ISO/IEC 27001:2022 管理策 5.5）

クラウドサービスデータの保存場所は前項の地理的所在地に基づき、日本国内になります。

3.情報セキュリティの意識向上，教育及び訓練

ISO/IEC 27017:2015 A.7.2.2（ISO/IEC 27001:2022 管理策 6.3）

当社は、クラウドサービスカスタマデータ及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、従業員の意識向上、教育及び訓練を提供し、委託先等にも同様の教育訓練の実施を要求します。

4.資産目録

ISO/IEC 27017:2015 A.8.1.1（ISO/IEC 27001:2022 管理策 5.9）

当社は、クラウドサービスデータ及び保存先を資産目録に特定し、クラウドサービスカスタマデータ及びクラウドサービス派生データの識別を行います。

5.クラウドサービスカスタマの資産の除去

ISO/IEC 27017:2015 CLD.8.1.5

当社が提供するクラウドサービスの利用終了時には、サービス利用約款に基づき適切な処理をして、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。

6.仮想コンピューティング環境における分離

ISO/IEC 27017:2015 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、仮想サーバ上で分離されています。

7.仮想マシンの要塞化

ISO/IEC 27017:2015 CLD.9.5.2

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。

8.暗号による管理策の利用方針

ISO/IEC 27017:2015 A.10.1.1（ISO/IEC 27001:2022 管理策 8.24）

当社が提供するクラウドサービス利用時の通信は、規格上暗号化不可のものを除き、すべて暗号化しております。

9.装置のセキュリティを保った処分又は再利用

ISO/IEC 27017:2015 A.11.2.7（ISO/IEC 27001:2022 管理策 7.14）

電子認証センターの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。

10.容量・能力の管理

ISO/IEC 27017:2015 A.12.1.3（ISO/IEC 27001:2022 管理策 8.6）

当社が提供するクラウドサービスの運用には十分な容量・能力を確保しており、電子認証センターにて、下記の監視を実施しています。

・リソース監視
・ログ監視

容量が不足することが予測される場合、適宜増強等を行います。
また、正常動作の確認のため、以下の監視を実施しています。

・サービス監視
・死活監視

クラウドサービスの提供能力に問題があることが確認された場合、適宜修正対応等を行います。

11.情報のバックアップ

ISO/IEC 27017:2015 A.12.3.1（ISO/IEC 27001:2022 管理策 8.13）

当社が提供するクラウドサービスにおけるバックアップに関する情報は、サービス利用約款で定めております。
iTrust 本人確認サービスにおきましては、システムバックアップは四半期に 1 回以上（3 か月以上の保管）、データバックアップは世代管理し 6 世代分保管しています。
また、システム変更時には随時取得しており、フルバックアップは日次で取得しています。前日バックアップ取得時点までの復旧が可能です。

12.クラウドサービスの監視

ISO/IEC 27017:2015 CLD.12.4.5

当社が提供するクラウドサービスは、電子認証センターにて常に以下の監視を行っております。

・不正アクセス監視および遮断
・ファイル改ざん検知

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。

13.技術的ぜい弱性の管理

ISO/IEC 27017:2015 A.12.6.1（ISO/IEC 27001:2022 管理策 8.8）

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、技術的ぜい弱性情報を市販クラウド環境及び専門機関等から適宜収集し、必要に応じて対応しております。

14.仮想及び物理ネットワークのセキュリティ管理の整合

ISO/IEC 27017:2015 CLD.13.1.4

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。

15.情報セキュリティ要求事項の分析及び仕様化

ISO/IEC 27017:2015 A.14.1.1（ISO/IEC 27001:2022 管理策 5.8）

当社が提供するクラウドサービスのセキュリティ要求事項及び仕様は、当社マニュアル及びセキュリティ仕様に準拠しております。要望がある場合は、個別に開示する場合があります。

16.セキュリティに配慮した開発のための方針

ISO/IEC 27017:2015 A.14.2.1（ISO/IEC 27001:2022 管理策 8.25）

当社が提供するクラウドサービスについては、ぜい弱性を埋め込まないためのセキュリティコーディングを実践し、リリース前および、定期的にネットワーク診断等のぜい弱性診断を行うことを方針として定めています。

17.情報セキュリティ事象の報告

ISO/IEC 27017:2015 A.16.1.2（ISO/IEC 27001:2022 管理策 6.8）

当社が提供するクラウドサービス上で検出した情報セキュリティ事象は、必要に応じてお客様へ通知します。
お客様からの問い合わせや報告は、お客様窓口にて承ります。
また、お問い合わせ及び対応の履歴は追跡可能となっております。

18.証拠の収集

ISO/IEC 27017:2015 A.16.1.7（ISO/IEC 27001:2022 管理策 5.28）

当社が提供するクラウドサービスにおけるログ等は、原則開示しておりませんが、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。

19.適用法令及び契約上の要求事項の特定

ISO/IEC 27017:2015 A.18.1.1（ISO/IEC 27001:2022 管理策 5.31）

当社が提供するクラウドサービスの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、コンプライアンス担当を設定し、管理を行っております。

20.知的財産権

ISO/IEC 27017:2015 A.18.1.2（ISO/IEC 27001:2022 管理策 5.32）

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

Web サイトお問い合わせフォーム
https://www.cybertrust.co.jp/contact/ca-security.html
認証・セキュリティ製品・サービスに関するご相談・ご質問
0120-957-975（受付時間：平日 9:00～18:00）

21.情報セキュリティの独立したレビュー

ISO/IEC 27017:2015 A.18.2.1（ISO/IEC 27001:2022 管理策 5.35）

お客様に安心頂けるクラウドサービスをご提供できるように、組織的な取り組みとして、当社では ISMS 及び ISMS クラウドセキュリティ認証を取得しており、認証機関からの審査を毎年受審しております。

本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すべての項目を網羅しているわけではありません。

改訂履歴

版数	年月日	内容
第 1 版	2023 年 6 月 30 日	新規作成
第 2 版	2024 年 5 月 7 日	市販クラウド環境の一部適用及び JIS Q 27001：2023（ISO/IEC 27001：2022）移行による見直し