クラウドセキュリティ
ホワイトペーパー
FOR ISO27017

サイバートラスト株式会社

2023年 6月 30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

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・電子認証センター	日本国内

2. 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。

3. 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(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及びクラウドサービス派生データの識別を行います

5. 資産の除去(ISO27017:CLD 8.1.5)

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(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、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(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。

8. 暗号による管理策の利用方針(ISO27017:10.1.1)

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(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。

10. 容量・能力の管理(ISO27017:12.1.3)

容量・能力については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、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

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. バックアップ(ISO27017:12.3.1)

当社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（ISO27017:CLD12.4.5）

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（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。

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（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。

15. 情報セキュリティ要求事項の分析及び仕様化（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（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の実施や、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。

17. 情報セキュリティ事象の報告（ISO27017:16.1.2）

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（ISO27017:16.1.7）

当社の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(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、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(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)

*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。

初版制定　2023年6月30日