情報区分	D
発　効　日	2025/9/16
版　番　号	Ver.2.0

フレッツ・あずけ～るシリーズの
情報セキュリティに関する文書

ＮＴＴ東日本株式会社

改訂履歴表

版番号	発効年月日	改　訂　内　容
1	2024/11/19	新規制定
2	2025/9/16	商号変更に伴う改正

目次

はじめに

本書の目的

この情報セキュリティに関する文書（以下、本書）は、ISMS クラウドセキュリティ認証の要求事項「JIP-ISMS517-1.0（ISO/IEC27017:2015）」により、クラウドサービスプロバイダが、クラウドサービスカスタマに向けて情報開示を求められている事項について、フレッツ・あずけ～るシリーズにおけるセキュリティの取り組みを確認いただくことを目的としています。

クラウドサービスカスタマデータは、クラウドサービス上で保存、処理されます。クラウドサービス上のデータに対するセキュリティ対策は、主にクラウドサービスプロバイダによって担われることになります。
ISO/IEC27017:2015 では、クラウドサービスプロバイダは、クラウドサービスカスタマが、クラウドサービスにおける情報セキュリティ対策が、自身の情報セキュリティ要求事項を満たすかどうかを検証するために必要な情報を提供することが求められています。
本書は、フレッツ・あずけ～るシリーズのセキュリティの取り組みの理解の促進の一助になるべく策定されました。

なお、ＮＴＴ東日本株式会社（以下、当社）の取り組みは、常に継続的に改善していきますので、最新の情報については、当社営業までご相談いただくか、当社 Web サイトをご確認ください。

【当社 Web サイト】
フレッツ・あずけ～る
https://flets.com/azukeru/azukeru.html
フレッツ・あずけ～る PRO
https://business.ntt-east.co.jp/service/azukerupro/
MS Office Online on あずけ～る
https://business.ntt-east.co.jp/service/azukeru_ms/

本書の適用範囲について

本書の適用範囲は、フレッツ・あずけ～るシリーズ※となります。
※フレッツ・あずけ～る/フレッツ・あずけ～る PRO/ MS Office Online on あずけ～るの 3 種類

本書で使用する用語について

本書で用いる用語及びその定義は、JIP-ISMS517-1.0、ISO/IEC 27017:2015 および JIS Q 27017:2016 によるものとします。また、これらの要求事項や規格で記されている用語については、改変せずに使用しております。

ISO/IEC 27017:2015 とは

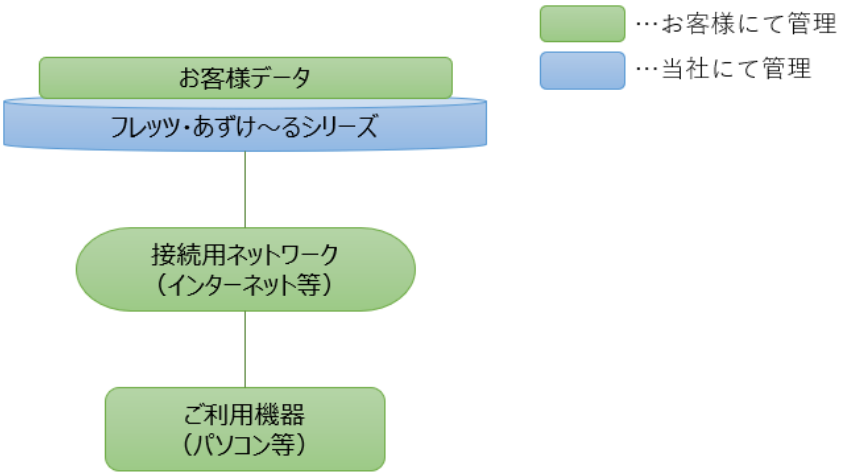
国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定する、情報セキュリティマネジメントに関する国際規格として、ISO/IEC 27000 シリーズがあります。その中で、情報セキュリティマネジメントシステムの要求事項である ISO/IEC27001:2022、情報セキュリティ管理策の実践のための規範である ISO/IEC27002:2013 は、組織が必要とする一般的な情報セキュリティについて規定されています。これらの規格に加えて、ISO/IEC27000 シリーズには、特定の分野固有の情報セキュリティ規格がいくつか策定されています。ISO/IEC27017:2015 は、分野固有の情報セキュリティ規格の一つで、クラウドサービス特有のリスクに対応したクラウド分野固有の情報セキュリティ規格です。ISO/IEC27017:2015 は、ISO/IEC27002:2013 をベースとし、クラウドサービスプロバイダ及びクラウドサービスカスタマの双方に対して、クラウドサービスのための管理策及びクラウドサービスのための実施の手引を規定していることに特長があります。2016 年には、日本規格協会により、ISO/IEC27017:2015 は、JIS Q 27017:2016 として、JIS 化されています。

ISMS クラウドセキュリティ認証とは

ISMS クラウドセキュリティ認証とは、ISMS（ISO/IEC 27001）認証を前提として、クラウドサービスの情報セキュリティ規格（ISO/IEC 27017:2015）を満たしている組織を認証する仕組みです。2016 年 8 月より一般財団法人日本情報経済社会推進協会（JIPDEC）により運用が開始されました。ISMS クラウドセキュリティ認証は、JIPDEC が定める「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項 JIP-ISMS517-1.0」を要求事項とし、ISMS アドオン認証と位置付けられています。

責任分界点について

フレッツ・あずけ～るシリーズに関する責任分界点は、以下のようになります。
フレッツ・あずけ～るシリーズをご利用いただく際に必要となる機器・接続用ネットワーク、およびフレッツ・あずけ～るシリーズ上のお客様データ（保存したファイル、ユーザ情報等）はお客様にて管理をお願いします。
当社では、フレッツ・あずけ～るシリーズにおけるサービス基盤からアプリケーションの管理を行います。



お客様へ通知について

変更管理およびセキュリティインシデント、情報セキュリティ事象等の通知は
当社の下記サイト（以下、当社サイト）にて通知いたします。

＜サイト＞
-フレッツ・あずけ～る　サポート情報
https://flets.com/azukeru/login/news/
-フレッツ・あずけ～る PRO　サポート情報
https://business.ntt-east.co.jp/support/azukerupro/
-MS Office Online on　あずけ～る
https://business.ntt-east.co.jp/support/azukeru_ms/
-サービス　工事故障情報
https://flets.com/customer/const2/

JIP-ISMS517-1.0、ISO/IEC 27017:2015　への対応

JIP-ISMS517-1.0 への対応

4.1　クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定【JIS Q 27001　の 4.3】

認証審査を受けるにあたって、組織は、クラウドサービスを含めた ISMS の適用範囲の決定を行い文書化することが求められています。当社においては、スコープを『フレッツ・あずけ～るシリーズ』と定めています。

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

ISO/IEC 27017 は、ISO/IEC 27002 と共通する管理策については、同じ項番が付与されていますので、ISO/IEC 27001 附属書 A の項番とも一致します。

また、既存の ISO/IEC 27001 附属書 A および ISO/IEC 27002 で想定されていないクラウド特有の拡張された管理策については、「附属書 A（規定）クラウドサービス拡張管理策集」として、頭に『CLD』がつく項番が付与されています。また、頭に『CLD』がつく管理策についても、そのあとに続く番号は、ISO/IEC 27001 附属書 A および ISO/IEC 27002 で定められた番号とも整合がとられています。

本書においては、閲覧時の利便性を考慮し、項番の順番に沿って、クラウドサービスプロバイダとしての取り組みについて解説を行います。

6.1.3 関係当局との連絡

18.1.1 法的及び契約上の要求事項の順守

フレッツ・あずけ～るシリーズでは、安全性・信頼性の高い、日本国内の堅牢で堅固なデータセンターでデータをお預かりします。

10.1.1 暗号による管理策の利用方針

フレッツ・あずけ～るシリーズでは、保管されるデータの全てを自動で暗号化し、データの機密性を協力に保護します。また、通信は全て、SSL/TLS 暗号化による HTTPS 通信です。

お客様のセキュリティポリシーに合わせたセキュリティ保護を実施されたい場合、フレッツ・あずけ～るシリーズをご利用の上お試しください。

11.2.7 装置のセキュリティを保った処分又は再利用

記憶媒体については、当社の情報セキュリティ規定に沿って処分または再利用を実施します。

12.3.1 情報のバックアップ

フレッツ・あずけ～るシリーズでは、自動バックアップ機能を所持しており、毎日又は週次での周期で自動バックアップを設定することが可能です。バックアップされたファイルは、国内データセンタにて保管されており、お客様にてファイルの削除を実行できます。

また、バックアップ可能容量は、契約ごとに定められておりますので、用途に合った適切な容量を選択ください。

自動バックアップの設定方法については、各種ご利用ガイドにて公開しております。

―フレッツ・あずけ～る

ご利用ガイド 運用編 大容量バックアップ専用ツール編 第 1.2 版

―フレッツ・あずけ～る Pro

ご利用ガイド 運用編 大容量バックアップ専用ツール編 第 1.2 版

解約時は、翌々々月末までデータを保持し、お客様に通知を行わずに削除いたします。

12.4.1　イベントログ取得

フレッツ・あずけ～るでは、操作ログ・アクセスログ・イベントログ等各種ログの提供は行っておりませんので、あらかじめご了承ください。

12.4.4　クロックの同期

フレッツ・あずけ～るシリーズでは、NTP サーバと同期しております。

※NTP サーバ…ネットワーク上で現在時刻を配信するためのサーバ

15.1.2 供給者との合意におけるセキュリティの取扱い

クラウドサービスプロバイダとしてのクラウドサービスの提供に関して、フレッツ・あずけ～る利用規約・IP 通信網サービス契約約款およびプライバシーポリシーを元に当社のクラウドサービスのセキュリティをお客様に説明しております。

なお、責任分界点についての解説は、前出の「責任分界点について」の項を参照ください。

16.1.1 責任及び手順

当社で確認できたセキュリティインシデントについては、該当の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は、当社サイトにて通知いたします。

なお、報告するセキュリティインシデント範囲は、当社サービスをご利用頂くお客様に何らかの異常な影響を及ぼす範囲のみとし、当社の ISO/IEC27001 に準拠したインシデント対応手順にて対応を行い、お客様にその影響範囲と対応策を開示します。当社サイトの通知については目標時間を定めておりませんが、早期に通知するよう努めます。お客様が発見した情報セキュリティ事象の報告や、その他の問い合わせ、報告は、サポートセンタにメールまたは電話にてご連絡が可能です。

16.1.2 情報セキュリティ事象の報告

お客様が発見した情報セキュリティ事象の報告や、その他の問い合わせ、報告は、サポートセンタにメールまたは電話にてご連絡が可能です。また、弊社が発見した情報セキュリティ事象のお客様へのご連絡については当社サイトより通知します。

18.1.3 記録の保護

フレッツ・あずけ～るシリーズをご利用いただくことで発生するデータは、以下のように取り扱います。

＜顧客が保存するデータ＞

・保存方法：データ保存時に自動で暗号化します。

・保存期間：お客様によるデータ削除が可能です。

解約時は翌々々月末までデータを保持し、お客様に通知を行わずに削除いたします。

容量が減少するようなプラン変更をした場合は、翌月末までデータを保持し、

超過分のデータをお客様に通知を行わずに削除いたします。

・保存目的：サービスの完全性を提供するため

＜操作ログ＞

・保存方法：ログ取得時に自動で暗号化します。

・保存期間：過去 2 年分のログを保存しています。
解約時は、解約から 1 年間ログを保持し、お客様に通知を行わずに削除いたします。
・保存目的：監査対応のため