発　効　日	2022/11/18
版　番　号	Ver.1.0

コワークストレージの
情報セキュリティに関する文書

東日本電信電話株式会社

改訂履歴表

版番号	発効年月日	改　訂　内　容
1	2022/11/18	初版作成

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、コワークストレージにおけるセキュリティの取り組みを記載しております。

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が担います。ISO/IEC27017:2015 では、クラウドサービスプロバイダは、以下の情報をクラウドサービスカスタマに提供することが求めれらています。

・クラウドサービスにおける情報セキュリティ対策が、クラウドカスタマ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

本書は、コワークストレージ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しました。

なお、東日本電信電話株式会社（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、当社営業担当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】

https://business.ntt-east.co.jp/content/coworkstorage/

本書の適用範囲について

本書の適用範囲は、コワークストレージとなります。

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

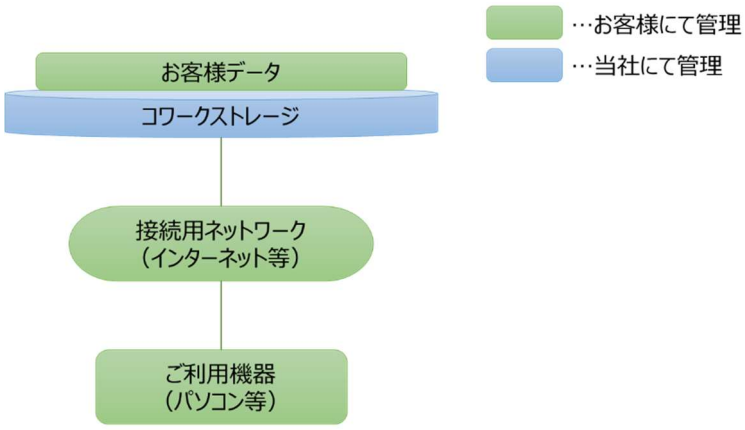
国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定する、情報セキュリティマネジメントに関する国際規格として、ISO/IEC 27000 シリーズがあります。その中で、情報セキュリティマネジメントシステムの要求事項である ISO/IEC27001:2013 や、情報セキュリティ管理策の実践のための規範である ISO/IEC27002:2013 は、組織が必要とする一般的な情報セキュリティについて規定されています。これらの規格に加えて、ISO/IEC27000 シリーズには、特定の分野固有の情報セキュリティ規格がいくつか策定されています。ISO/IEC27017:2015 は、分野固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

コワークストレージに関する責任分界点は、以下のようになります。
コワークストレージ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、およびコワークストレージ上のお客様データ（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、コワークストレージ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。



お客様への通知について

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】
・コワークストレージ　サポート情報
https://business.ntt-east.co.jp/support/coworkstorage
・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『コワークストレージ』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。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

利用規約 第 15 条 (契約者が行う契約の解約)に基づき、データを消去します。消去するデータの詳細については、サポートセンタにお問合せください。

10.1.1 暗号による管理策の利用方針

コワークストレージでは、保管されるデータの全てを自動で暗号化し、データの機密性を強力に保護します。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、コワークストレージ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。

12.1.2 変更管理

クラウドサービスカスタマに何らかの影響が発生する可能性のある変更及びメンテナンスについては、以下の①～④を、事前に当社サイトより通知を行います。

① 変更種別
② 変更予定日及び予定時刻
③ クラウドサービス及びその基礎にあるシステムの変更についての技術的な説明
④ 変更の通知

12.3.1 情報のバックアップ

お客様がコワークストレージにファイルをアップロードした時点で、激甚対策として国内の異なる複数のデータセンターで同時にファイルデータの複製を行います。

また、ファイルを上書き保存すると、1 つ前のファイルがバージョンファイルとして保管されます。バージョンファイルは、7 日間保存されます。バージョンファイルへの入れ替え等については利用マニュアル　操作編　一般ユーザ向け 「Ｗｅｂブラウザ」 10.1 を参照ください。所要時間はファイルサイズに依存します。バージョンファイルについてはダウンロードまたは別ファイルとして保存することも可能なため、ファイルの確認を行うことが可能です。バージョン管理の機能については、コワークストレージをご利用いただき、お試しください。

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、利用規約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等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。

18.2.1 情報セキュリティの独立したレビュー

ISO/IEC 27001 および ISO/IEC 27017 における情報セキュリティに対する取り組みについて、クラウドカスタマの求めに応じて当社にて検討し、開示します。