tomoLinks クラウドセキュリティ
ホワイトペーパー

第 1.0 版

コニカミノルタ株式会社
DW-DX 事業本部
DX 開発推進センター

目次

I. 目的

セキュリティホワイトペーパー（以下本書）は、ISMS（情報セキュリティマネジメントシステム）のクラウドセキュリティ認証である「ISO/IEC 27017：2015」で求められている要求事項の中で、コニカミノルタ株式会社 DW-DX 事業本部 DX 開発推進センター(以下、当組織という)がお客様に対し提供しているセキュリティの取組みについて明確にし、ご確認いただくことを目的としています。

●ISO/IEC 27017 について

ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。

クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017 で、情報セキュリティ全般に関するマネジメントシステム規格 ISO/IEC 27001 の取り組みを強化します。これにより、クラウドサービスにも対応した情報セキュリティ管理体制を構築し、その実践を支援します。

II. 適用範囲について

当社の ISO/IEC 27017 の適用範囲は、tomoLinks の提供する 3 つのサービスのうち、先生×AI アシストサービス及び学習支援サービスに対するものです。機能の詳細についてはサービスサイト（https://tomolinks.konicaminolta.jp/）にて確認いただけます。

●tomoLinks の提供する 3 つのサービス

・学習支援サービス

・先生×AI アシストサービス

・授業診断サービス

お問い合わせの窓口

提供時間：月～金 午前 9 時～午後 6 時（日本時間：年末年始・祝日除く）

提供手段：お客様管理者からサポートへの連絡はサービスサイトの「お問い合わせ」フォーム、からお問い合わせいただけます。

お問い合わせには、国民の祝祭日および年末年始休業を除き、1営業日以内に一次回答いたします。

用語について

本書では ISO/IEC 27017:2015 (JIS Q 27017:2016)で記されている用語については、そのまま使用しています。本サービスで利用している用語については、利用規約にてご確認いただけます。

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

以下に ISO/IEC 27017:2015 (JIS Q27017:2016)が求める要求事項に対する管理策を記載します。番号・タイトルは、ISO/IEC 27017 が求める「情報セキュリティ管理策の実践の規範」5～18(17 を除く)の小項目番号・要求事項原文を示しています。

5　情報セキュリティ方針のための方針群

5.1　情報セキュリティのための経営陣の方向性

5.1.1 情報セキュリティのための方針群

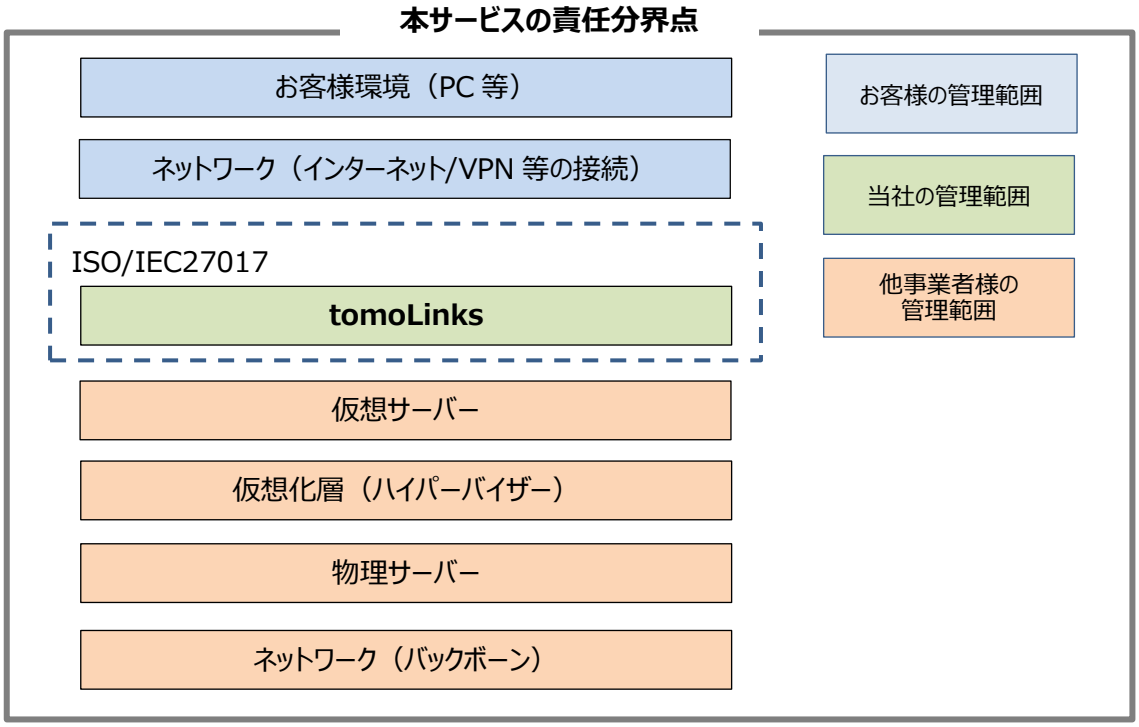
クラウドサービスプロバイダ(CSP)は、 クラウドサービスの提供および利用に取り組むため、情報セキュリティ方針を拡充することが求められています。 本サービスでは、コニカミノルタ情報セキュリティ基本方針及び当組織のクラウドセキュリティ方針に従いサービスを運用しています。

6 情報セキュリティのための組織

6.1 内部組織

6.1.1 情報セキュリティの役割および責任

情報セキュリティの役割および責任について利用規約に定め、サービスを提供しています。本サービスにおける責任分界点は下図のとおりです。



6.1.3 関係当局との連絡

当組織の所在地は、東京都八王子市石川町 2970 と大阪府高槻市桜町1−2になります。また、クラウドサービス上に保存されるデータの所在は日本国内になります。

CLD.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係

CLD.6.3.1 クラウドコンピューティング環境における役割および責任の共有および分担

情報セキュリティの役割および責任について利用規約に定め、サービスを提供しています。本サービスの責任分界点に関しては「6.1.1 情報セキュリティの役割および責任」をご参照下さい。

7 人的資源のセキュリティ

7.2 雇用期間中

7.2.2 情報セキュリティの意識向上、教育および訓練

本サービスのセキュリティ要件及びクラウドサービスの運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練および意識向上の策を実施しています。

8 資産の管理

8.1 資産に対する責任

8.1.1 資産目録

クラウドサービスカスタマー(CSC)の情報資産(保存データ)及び当組織においてサービスを提供者する上で収集することになるクラウドサービス派生データは情報資産台帳上で明確に識別の上分離しています。

なお、本サービス上でカスタマーが作成・保存する情報資産は、カスタマーの管理責任範囲となります。

CLD.8.1.5 クラウドサービス利用者の資産の除去

カスタマーが本サービスの利用を停止または終了した場合、当組織は tomoLinks の利用規約にもとづき、利用終了の申込を頂いた場合や、契約期間終了前の顧客窓口からの確認連絡に 5 営業日返答が無い場合、利用者が本サービスに登録した情報及びその複製物を当組織において契約期間終了日から翌々月末までに削除いたします。

8.2 情報の分類

8.2.2 情報のラベル付け

本サービスをご利用いただくにあたり、カスタマーは以下のようなラベル付けの機能を利用し、情報を整理することができます。

・学校や教室(クラス)の名称
・教材動画データの科目別分類

9 アクセス制御

9.2 利用者アクセスの管理

9.2.1 利用者登録および登録削除

カスタマーは、本サービスの利用者登録及び削除について、「tomoLinks マニュアル」に基づいてユーザの役割に応じて登録・削除・変更をすることができます。

9.2.2 利用者アクセスの提供(provisioning)

カスタマーは、「tomoLinks サービス仕様書」に従い、役割に応じて参照範囲や機能実行範囲を定めるための権限管理をすることができます。

9.2.3 特権的アクセス権の管理

カスタマーは、「tomoLinks サービス仕様書」に従いシステム管理者の機能を特権として利用することができます。当該権限の利用においては、初期パスワードの桁数の差異によりその他の権限と認証の強度を分けています。

9.2.4 利用者の秘密認証情報の管理

お申し込み後の初回利用時の初期パスワードは顧客窓口よりご案内いたします。初期パスワードでログイン後はお客様のパスワードポリシーに従って設定いただくことが可能です。

9.4 システム及び業務用ソフトウェアのアクセス制御

9.4.1 情報へのアクセス制限

カスタマーは、「tomoLinks サービス仕様書」に従い、役割に応じて情報の参照範囲や機能実行範囲を定めることができます。

9.4.4 特権的なユーティリティプログラムの使用

カスタマーに対し、セキュリティ手順を回避し各種サービス機能の利用を可能とする API 等のユーティリティプログラムの提供は行っておりません。

また、当組織にて運用保守のために保持する特権的ユーティリティプログラムについては、当該プログラムの利用者を厳しく限定し、作業は事前に申請・承認を行い、ログによる事後のレビューを実施しております。

なお、同じ組織内の複数人でダブルチェックと並行して行った作業であれば、事後のログレビューによる検証は不要としております。また、承認者が申請者を兼ねる場合は申請を省略可としております。

CLD.9.5 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御

CLD.9.5.1 仮想コンピューティング環境における分離

本サービスは、マルチテナント環境で動作し、データベース内で分割することにより資源の分離を実施しています。

CLD.9.5.2 仮想マシンの要塞化

本サービスにおける仮想化環境は、社内の「製品セキュリティ実施要領」にもとづいて脅威分析を行い、セキュリティ要件を決定し、ポート・プロトコルへの制限、不正アクセス遮断、ログ取得等の要塞化を実施しています。

10 暗号

10.1 暗号による管理策

10.1.1 暗号による管理策の利用方針

本サービスではストレージ、データベース、通信(TLS1.2 対応)の暗号化を実施しております。

11 物理的及び環境的セキュリティ

11.2 装置

11.2.7 装置のセキュリティを保った処分又は再利用

機器の老朽化、故障等により交換した機器媒体の処理については、当社では直接装置の処分を行うことはありません。AWS の施設、建物、および物理上のセキュリティに基づきます。

https://aws.amazon.com/jp/blogs/news/data_disposal/

12 運用のセキュリテイ

12.1 運用の手順及び責任

12.1.2 変更管理

本サービスにおいて、バージョンアップやメンテナンスを実施する場合、1週間前を目安にサービスサイトに掲示し、通知いたします。

12.1.3 容量・能力の管理

安定的なサービス提供を行うため、各サーバーのリソースを監視し、必要に応じてキャパシティの増強を行っています。

CLD.12.1.5 実務管理者の運用のセキュリティ

本サービス操作方法は、オンラインマニュアルを作成し、カスタマーにご案内しており、サービス側の更新に合わせて都度改訂しています。

12.3 バックアップ

12.3.1 情報のバックアップ

本サービスでは、AWS 上にバックアップ領域を設けており、バックアップデータは日次で 1 週間分を暗号化して保管しています。

12.4 ログ取得及び監視

12.4.1 イベントログ取得

本サービスでは、ご契約されている機能に応じて、例えば児童生徒の欠席の記録や児童生徒の日ごとのこころの状態等の記録を取ることができます。また、サービスへのアクセスログにつきましては、利用者側での不正操作等の検出を目的とした場合、12 ヵ月前の記録まで、お問い合わせに応じて都度対応させていただきます。

12.4.4 クロックの同期

本サービスでは AWS が提供する Time Sync Service を基準に時刻を同期しています。

CLD.12.4.5 クラウドサービスの監視

本サービスでは、監視機能を含むシステム構成としており、サーバの状態監視、システムの死活監視、外部からの攻撃監視、リソース監視を実施しています。

12.6 技術的脆弱性管理

12.6.1 技術的脆弱性の管理

また、本サービスに関する脆弱性情報を収集し、評価し、対応しております。お客様への影響がある脆弱性情報については、サービスサイトにてお知らせします。

13 通信のセキュリティ

13.1 ネットワークセキュリティ管理

13.1.3 ネットワークの分離

本サービスでは、開発・構築時にネットワークセキュリティ要件を決定し、用途別にネットワークを分離しており、tomoLinks のカスタマ側のネットワーク環境と tomoLinks のネットワーク環境は分離されています。

14 システムの取得、開発及び保守

14.1 情報システムのセキュリティ要求事項

14.1.1 情報セキュリティ要求事項の分析および仕様化

当組織では、製品セキュリティ実施細則に従い、サービスの設計・開発・構築時にセキュリティ要件を決定し、実装しております。

主にお客様が検討される情報セキュリティの機能の仕様として、当ホワイトペーパーは以下の項目を記載しています。

- アクセス制限機能（9.4.1 情報へのアクセス制限、CLD.9.5.2 仮想マシンの要塞化）
- 通信暗号化機能（10.1.1 暗号による管理策の利用方針）
- ログ取得機能（12.4.1 イベントログ取得）

14.2 開発及びサポートプロセスにおけるセキュリティ

14.2.1 セキュリティに配慮した開発のための方針

当社では、セキュリティに配慮した開発方針として「セキュリティ・バイ・デザイン」の原則に則り、製品セキュリティ実施細則に従って開発時点からセキュリティに関するリスク対応、脆弱性対応を行っています。

15 供給者関係

15.1 供給者関係における情報セキュリティ

15.1.2 供給者との合意におけるセキュリティの取扱い

本サービスにおける役割及び責任については、利用規約に定め、サービスを提供します。本サービスの責任分界点に関しては「6.1.1 情報セキュリティの役割および責任」をご参照下さい。

15.1.3 ICT サプライチェーン

当社が利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、本サービスの情報セキュリティとの整合性が取れていることを確認しています。

本サービスは、AWS をクラウドサービスプロバイダとして運用しています。AWS のコンプライアンス状況については下記をご参照下さい

https://aws.amazon.com/jp/compliance/

16 情報セキュリティインシデント管理

16.1 情報セキュリティインシデントの管理及びその改善

16.1.1 責任および手順

カスタマーの業務に影響を与える情報セキュリティインシデント(データの消失、長時間のシステム停止等)が発生した場合は、インシデントの発生を検知してから 3 営業日を目標に、全体的なインシデントの場合には、サービスサイトまたはメールで通知いたします。特定のお客様に生じたインシデントの場合には、メールなどにより通知いたします。

セキュリティインシデントに関する問合せは、本サービスお問い合わせサポートより受け付けています。

16.1.2 情報セキュリティ事象の報告

本サービスにおいて、情報セキュリティインシデントの兆候となる事象を検知した場合、サービスサイトでのお知らせ、またはメールで通知いたします。また個別のお問い合わせは、本サービスお問い合わせサポートより受付けています。

16.1.7 証拠の収集

本サービスにおいて、お客様のデータは「tomoLinks 利用規約」に従って適切に管理いたします。ただ、裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、「tomoLinks 利用規約」の定めに従ってお客様の同意なく、利用者のデータを当該機関に開示することがあります。詳細は、本サービス利用規約をご確認ください。なお、お客様に重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には本サービスお問い合わせサポートまでお問い合わせください。

18 順守

18.1 法的及び契約上の要求事項の順守目的

18.1.1 適用法令および契約上の要求事項の特定

本サービスの利用に関して適用される「準拠法」は「日本法」となります。本サービス運用に関連する各種法令に関しては法規制管理台帳を作成し、準拠するように努めています。

18.1.2 知的財産権

本サービスをご利用いただく上での知的財産権は「tomoLinks 利用規約」の取り決めに従います。お問い合わせは、本サービスお問い合わせサポート窓口にて受け付けております。

18.1.3 記録の保護

利用者の本サービスご利用に関して蓄積された記録に対しては不正アクセス・改ざんなどを防ぐためアクセス制限を実施しています。

18.1.5 暗号化機能に対する規制

本サービスでは 各種暗号化機能を利用しています。（10.1.1 参照）なお、輸出規制の対象となる暗号化の利用はありません。

18.2 情報セキュリティのレビュー

18.2.1 情報セキュリティの独立したレビュー

当社では、社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001、ISO/IEC27017 に基づく第三者による認証審査を受け、情報セキュリティに対する取り組みを行うことで、安全なセキュリティレベルを確保します。（初回認証審査は 2023 年 10 月 31 日、11 月 1 日）

IV. 変更履歴

版	日付	改訂内容
第 1.0 版	2023/10/13	初版作成

以上