

セキュリティホワイトペーパー
スマートライフパス
Dot to Dot

2024/12/20

第 1.0 版

一般社団法人 UDCK タウンマネジメント

はじめに

当ホワイトペーパー(以下「本書」)は、一般社団法人 UDCK タウンマネジメント(以下「当法人」)が提供するクラウドサービスであるスマートライフパスおよび Dot to Dot(以下「本サービス」)に関する情報セキュリティへの取り組みを記載したものです。

記載内容については、クラウドサービスに関する情報セキュリティの国際規格である ISO/IEC27017:2022 において、クラウドサービス事業者がクラウドサービス利用者に対して開示もしくは公開を求めている事項に基づき構成されています。

なお、各項目の先頭に記載されている数字は、ISO/IEC27017:2022 の該当する項番を表しています。

なお、本書は事前に通知することなく改訂する場合があります。

1. 本書の適用範囲

本書の適用範囲は以下のクラウドサービスとなります。

スマートライフパス (<https://www.dataplatform-portal.jp/>)

Dot to Dot (<https://dot2dot.life/app/m/home>)

2. 責任分界点について

本サービスに関する責任分界点は以下となります。

ユーザデータ(アカウント情報)	お客様の責任範囲
利用端末とネットワーク環境	
コンテンツデータ	当法人の責任範囲
アプリケーション	
ミドルウェア	当法人が利用するクラウドサービスの責任範囲
OS	
仮想サーバ	
仮想化層(ハイパーバイザー)	
物理設備(サーバ、ストレージ、ネットワーク)	
土地・建物	

3. 記載内容について

JIS Q 27017:2023(ISO/IEC 27017:2022)が求める要求事項に対する管理策の項番の順で本サービスの取り組みを記載します。

5.1 情報セキュリティのための方針群

本サービスは、当法人の定めた情報セキュリティ基本方針、並びにクラウドサービス情報セキュリティ方針に従い、サービス運営を行っています。

情報セキュリティ基本方針 (https://www.udcktm.or.jp/security_policy/index.html)

クラウドサービス情報セキュリティ方針 (https://www.udcktm.or.jp/cloud_security/index.html)

5.2 情報セキュリティの役割及び責任

「2.責任分界点について」に記載しております。
本サービスの利用については利用規約をご確認下さい。

5.5 関係当局との連絡

当法人の所在地は、当法人ウェブサイトでご確認下さい。

法人概要 (<https://www.udcktm.or.jp/corporation.html>)

なお、本サービスにて保存されるデータの所在は、Microsoft Azure の日本国内のデータセンターとなります。

5.8 プロジェクトマネジメントにおける情報セキュリティ

当法人は本サービスの情報セキュリティ管理をプロジェクトマネジメントの一環として取り組んでいます。本サービスにおける情報セキュリティ機能に関する情報を本書にて公開します。

5.13 情報のラベル付け

本サービスは、情報資産の分類(クラウドシステム上に保存されたデータ)にご利用頂けるラベル付け機能を保有しています。

所属エリア：お客様の所属エリア情報およびテナントコード

5.16 アイデンティティ管理

本サービスは利用者 ID の登録及び削除機能を提供しています。

5.17 認証情報

本サービスは利用者によるパスワード再発行機能、管理者によるパスワードリセット機能を提供しています。

5.18 アクセス権

本サービスは利用者に対して事前設定された管理機能(アクセス権、機能制限設定等)を提供しており、管理者が設定可能となります。

5.20 供給者との合意におけるセキュリティの取り扱い

本サービスの責任分界点の詳細に関しては「2. 責任分界点について」をご参照下さい。
また、セキュリティ対策についても同「2. 責任分界点について」に記載するサービスの提供範囲において必要なセキュリティ対策を実施しています。

5.24 情報セキュリティインシデント管理計画と準備

本サービスは情報セキュリティインシデント発生における利用者の問い合わせ窓口を設けています。

情報セキュリティインシデントを確認した時点で各所への適切な指示および対応ができるようインシデント対応フローにて定めています。

5.28 証拠の収集

お客様のデータは、本サービスの利用規約に従って適切に管理します。ただし、裁判所からの開示請求など、法律や法令に基づいた正当な開示請求が行われた場合、利用規約の定めに従ってお客様の同意なく開示することがあります。

5.31 法律、法令、規制及び契約上の要求事項

本サービスのご利用に関して、適用される準拠法は日本国の法令です。

5.32 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に関わるご相談は、本サービスの問い合わせ窓口までお問い合わせください。

5.33 記録の保護

本サービスは、サービスを安全に提供するために必要なログ等を1年間保管します。

5.35 情報セキュリティの独立したレビュー

当法人は個人情報の取り扱いについて第三者による審査を受け、プライバシーマークの取得状況を当法人のウェブサイトで公開しています。

当法人は、ISO/IEC 27001 と ISO/IEC 27017 について第三者による審査を受け、認証の取得状況を当社ウェブサイトで公開しています。

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及び責任の共有及び分担

本サービスは、サービスの提供環境における役割及び責任について利用規約に定め、サービスを提供します。

本サービスの責任分界点については、「2. 責任分界点について」をご確認ください。

6.8 情報セキュリティ事象の報告

当法人が確認したセキュリティインシデントがお客様に重大な影響を及ぼす場合、影響有無の確認より3時間以内を目標にお客様へメールにて通知を行います。また、本サービスのサポートサイトへ周知が必要な情報を掲載します。

情報セキュリティ事象に関するお問合せは、サポートセンターでお受けいたします。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

本サービスは利用契約が終了した利用者の情報は速やかに削除します。

但し、法令上等で保管が必要な情報については、利用契約終了後も 3 年間保持します。

8.2 特権アクセス権

本サービスは、二要素認証をはじめとしたお客様のセキュリティに配慮した認証技術を提供しています。

8.8 技術的ぜい弱性の管理

本サービスは、定期的に脆弱性情報を収集し、収集した情報を基にサービスへの影響を評価し、当法人の責任範囲において影響がある場合には、速やかに対応します。

8.13 情報のバックアップ

本サービスは管理対象の情報のバックアップとして日次で7世代を取得/保持しています。

8.15 ログ取得

本サービスは、サービスの維持管理に必要となる適切なログを取得しています。

8.17 クロックの同期

本サービスは、NTP による時刻同期を行っており、日本時間(JST)で管理しています。

8.22 ネットワークの分離

本サービスは、仮想化技術やネットワークセキュリティ技術を利用し、サーバやネットワーク、ストレージを本サービスが稼働する仮想環境ごとに論理的に分離しています。

8.24 暗号の使用

本サービスの利用において保存されるデータは全て暗号化し保管しています。
お客様の利用するサイトでは SSL/TLS による通信の暗号化を使用しています。
なお、輸出規制の対象となる暗号化の利用はありません。

8.25 セキュリティに配慮した開発のライフサイクル

当法人は、本サービスの開発元に開発ライフサイクルを確認した上で本サービスを提供しております。また、第三者による脆弱性診断を定期的の実施し、診断結果を確認しています。

8.32 変更管理

本サービスまたはクラウドサービスプロバイダのサービス変更等により利用者へ影響が発生する場合は、利用者へ事前通知をするとともに、完了時においても通知します。

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、本サービスを構成するシステム環境について、その環境の用途に応じてネットワークを分離しています。

4. 更新履歴

版数	日付	更新内容
第 1.0 版	2024/12/20	初版公開