達人 Cube における ISO/IEC27017
クラウドセキュリティホワイトペーパー

第 1.1 版

株式会社 NTT データ
税務サービスグループ

I. 目的

このホワイトペーパー（以下、本書という）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、株式会社 NTT データ(以下、当社という)の税務サービスグループ(以下、本組織という)がお客様に提供しているセキュリティの取り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

本組織が提供する達人 Cube のアプリケーション機能(「達人」オフィシャルサイト https://www.tatsuzin.info/tos/)のうち、ISO/IEC 27017 の適用範囲は、赤色文字下線で記します。

・達人 Cube
・達人 Cube「クラウドデスクトップ」
・達人 Cube「クラウド AP 仮想化サーバー」
・達人 Cube「クラウドストレ～ジ」
・達人 Cube「報酬請求 Powered by My Komon」
・**達人 Cube「データ収集・配信」**
・達人 Cube「不動産評価」

お問い合わせ窓口：達人インフォメーションセンタ
電話：0120-554-620
受付時間：9:00～12:00 13:00～17:00（土日祝日及び本組織の休業日を除く）

■ 用語について

本書では、ISO/IEC 27017:2015 (JIS Q 27017:2016)で記されている管理策は、頭に「CLD」をつけており、そのまま使用しています。

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本組織の対応状況を記載します。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）の箇条番号・要求事項の原文を示しています。

5 情報セキュリティのための方針群

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及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。

本サービスは、当社の情報セキュリティ方針、並びに本組織の情報セキュリティ方針に従ってサービスを開発、提供しています。

6 情報セキュリティのための組織

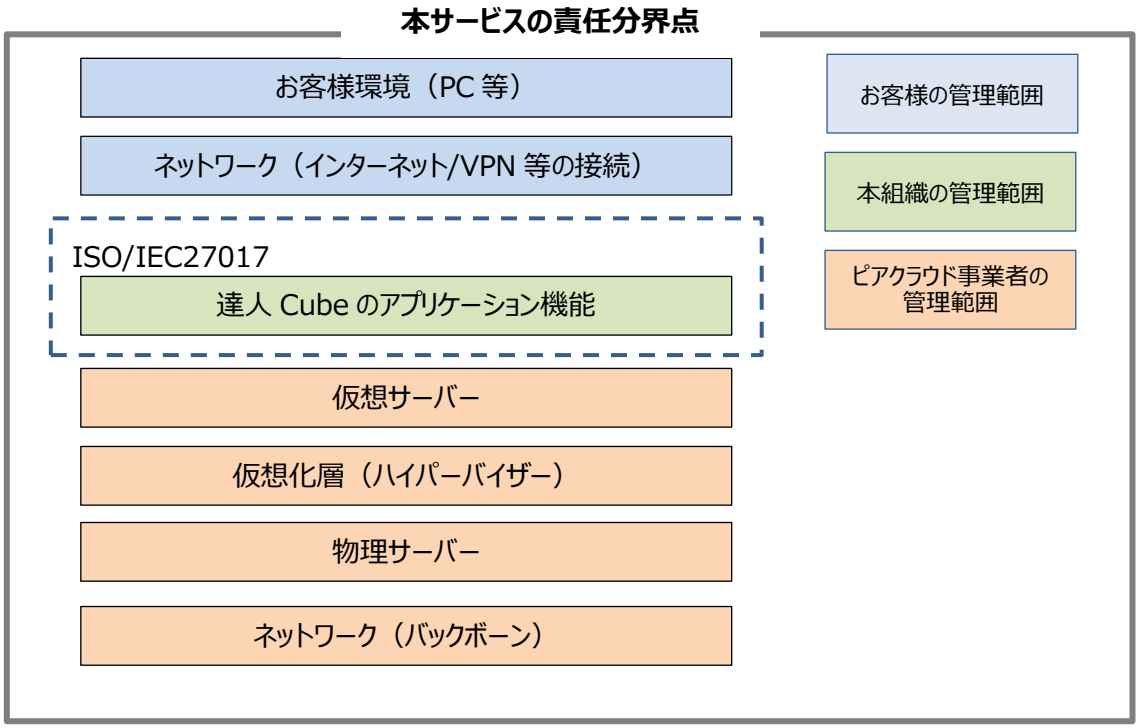
6.1 内部組織

6.1.1 情報セキュリティの役割及び責任

情報セキュリティの役割及び責任については利用規約に定め、サービスを提供しています。

https://www.tatsuzin.info/tos/

本サービスにおける責任分界点は下図の通りです。



6.1.3　関係当局との連絡

本組織所在地は、東京都千代田区です。
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です。

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及び責任の共有及び分担

情報セキュリティの役割及び責任は、利用規約に定めています。
https://www.tatsuzin.info/tos/
本サービスの責任分界点は「6.1.1 情報セキュリティの役割及び責任」をご参照ください。

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、教育及び訓練

本組織では、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利用、提供に関するルールを定め、その確実な遵守を目的にサービス提供に従事する要員を対象とした教育・訓練及び意識向上の施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

本サービスにおいて、お客様が取り扱うデータ(クラウドサービスカスタマデータ)及びお客様が本サービスを利用することに伴って本組織が収集するデータ(クラウドサービス派生データ)は、本組織で管理する情報資産管理台帳にて明確にし、当社分離しています。

なお、本サービスを利用するにあたりお客様が作成、保管、保存する情報資産は、お客様の管理範囲となります。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

お客様が本サービスの利用を停止するまたは終了する場合、お客様が登録、利用、保管、保存した電子ファイル等の情報は、お客様の責任において情報の削除をお願いします。情報の削除は、お客様の責任となります。

お客様における情報の削除漏れによって想定される情報漏えいを防ぐために、本組織では四半期毎に情報の削除状況を確認し、削除処理を行っています。

8.2　情報分類

8.2.2　情報のラベル付け

お客様が本サービスを利用する場合は、お客様はプロダクトコードをラベル付け機能として使用し、対象となるサービスを識別することができます。

9　アクセス制御

9.2　利用者アクセスの管理

9.2.1　利用者登録及び登録削除

本サービスにおいて、お客様が利用できるユーザ区分は、以下の通りです。

・管理者(システム所有者)：契約情報、利用者情報の設定
・管理ユーザ：一般ユーザの登録・変更・削除やアクセス制御の設定

・一般ユーザ：管理ユーザが認可したサービスの一般利用

利用者登録、変更及び削除は管理者(システム所有者)及び管理ユーザのみが行えます。

詳細は「達人 Cube 本体プログラム運用ガイド」をご確認ください。

9.2.2 利用者アクセスの提供(provisioning)

本サービスでは、管理ユーザが一般ユーザを認可し、サービス利用において参照できる範囲や実行できる機能の範囲を定めることができます。

9.2.3 特権的アクセス権の管理

本サービスの特権的アクセス権は、管理者(システム所有者)に割り当てられています。特権的アクセス権の利用は、プロダクトコード、ログイン ID、パスワードにより認証し、セキュリティを確保しています。

9.2.4 利用者の秘密認証情報の管理

本サービス利用開始時の初期パスワードは、本組織より仮パスワードとしてお客様に紙媒体にてご案内します。
受け取られた仮パスワードは、お客様が最初にログインする時のみに使い、これを変更していただきます。
お客様が使用するパスワードは、一定の条件を満たしお客様が定めるパスワードポリシーに従って設定することができます。

9.4 システム及びアプリケーションのアクセス制御

9.4.1 情報へのアクセス制限

本サービスでは、管理ユーザが一般ユーザのアクセスできる範囲や実行できる機能を定め、設定することができます。

9.4.4 特権的なユーティリティプログラムの使用

本組織ではお客様に、本サービスのセキュリティ手順を回避して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、本組織でサービス運用保守するために保有する特権的ユーティリティプログラムについては、運用保守する要員を限定し、厳しく管理しています。

作業発生時は作業の事前申請及び承認、ログの取得、作業内容の確認を行い、妥当性を評価しています。

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、データベースのスキーマ分割及びプロダクトコードによるユーザ識別により、お客様同士及びお客様と本組織の内部環境の資源を分離しています。

CLD.9.5.2 仮想マシンの要塞化

本サービスの提供にあたって構築する仮想化環境は、当社の開発・構築ルールに従ってセキュリティ要件を決定し、ポート・プロトコルの制限、不正アクセス遮断、ログ取得等の要塞化を実装しています。

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

本サービスにおける暗号化の対象と管理策は以下の通りです。

ストレージ：AWS の SSE-S3
データベース：AWS マネージド型キー「aws/ebs」
通信：SSL/TLS（TLS 1.2 対応）

本サービスを利用するためにお客様がログイン時に入力した認証パスワードはハッシュ化して保存されます。
また、お客様が保存した情報は、お客様の暗号化ツールを利用して情報を暗号化することもできます。

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

本サービスの提供に必要な物理インフラの管理は AWS の責任範囲であり、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、本組織が機器を処分、再利用することはありません。AWS の施設、建物、及び物理上のセキュリティ仕様に基づいています。

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

12 運用のセキュリティ

12.1 運用の手順及び責任

12.1.2 変更管理

本サービスのリリースや定期メンテナンス等により、お客様に影響を及ぼす可能性のある作業を実施する場合は、事前に(原則 1 週間前までに)「達人」オフィシャルサイト、達人 Cube ポータルサイト、電子メール等当社が適切と判断する方法にて公表通知させていただきます。

12.1.3 容量・能力の管理

本サービスをお客様に安定してご利用いただくために、監視対象のリソースを決定し、モニタリングし、計画的または必要に応じて適時リソース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「達人 Cube 本体プログラム運用ガイド」及び「データ収集・配信運用ガイド」として、お客様に提供しています。ガイドを改訂した場合には、達人 Cube ポータルサイトにてお知らせし、改訂版を掲載しています。

12.3 バックアップ

12.3.1 情報のバックアップ

本組織では本サービスを提供するための機器等については「バックアップ・リカバリ設計」に基づきバックアップを行っています。

お客様が必要とする情報のバックアップについては、お客様の責任において保存をお願いします。

お客様にてバックアップできる情報は以下の通りです。

・サービスを利用してアップロードした書類
・事業者情報
・アクセスログ

操作方法は「達人 Cube 本体プログラム運用ガイド」及び「データ収集・配信運用ガイド」をご確認ください。

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、お客様にアクセスログの取得機能を提供しています。取得方法は「達人 Cube 本体プログラム運用ガイド」及び「データ収集・配信運用ガイド」をご確認ください。

12.4.4 クロックの同期

本サービスでは AWS が指定する NTP サーバーを参照することで時刻同期を行っています。

CLD.12.4.5 クラウドサービスの監視

本サービスでは、開発・構築時に監視要件を決定し、実装しています。
お客様は本サービスが提供するアクセスログの取得機能を活用することによってアクセス監視ができます。

12.6 技術的ぜい弱性管理

12.6.1 技術的ぜい弱性の管理

本サービスに関連するぜい弱性は、NTTDATA-CERT 及び本組織内の運用を営む担当にてぜい弱性情報を収集し、評価し、対応しています。

お客様に影響を与える可能性がある場合には、「達人」オフィシャルサイト、達人 Cube ポータルサイト、電子メール等当社が適切と判断する方法にて公表通知いたします。

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のセキュリティ要件を決定し、ネットワーク設計に反映しています。以下のとおり、用途別にネットワークを分離しています。

- ・インターネット公開層：パブリックサブネット
- ・アプリケーション層：プライベートサブネット
- ・データベース層：プライベートサブネット
- ・ジャンプサーバ：パブリックサブネット

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及び仕様化

本組織では、当社の基準に従い、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、実装しています。
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、本書に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

本組織では、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、当社の基準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、ぜい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及び責任」をご参照ください。

15.1.3 ICT サプライチェーン

本組織が利用するクラウド事業者は、本組織と同等以上の情報セキュリティ水準であることを確認しています。

本サービスは、AWS をクラウドベンダとして選定しています。AWS のコンプライアンス状況については下記をご参照ください。

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 責任及び手順

お客様に影響を及ぼすおそれのあ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、影響範囲に応じてインシデントの発生を検知してから 3 営業日を目標に通知いたします。

・影響がお客様全体に及ぶおそれがある場合：「達人」オフィシャルサイト、達人 Cube ポータルサイト、電子メール等当社が適切と判断する方法にて公表通知

・影響が特定のお客様のみに限定されるおそれがある場合：対象となる可能性のあるお客様に電子メール等当社が適切と判断する方法にて通知

情報セキュリティインシデントに関するお問い合わせは、お問い合わせ窓口にて対応いたします。

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予兆と考えられる情報セキュリティ事象を本組織にて検知した場合、「達人」オフィシャルサイト、達人 Cube ポータルサイト、電子メール等当社が適切と判断する方法にて公表通知いたします。

また、お客様において情報セキュリティ事象を検知した場合のご連絡、お問い合わせは、お問い合わせ窓口にて対応いたします。

16.1.7 証拠の収集

本サービスに関して、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、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、本サービスの利用規約をご確認ください。

なお、お客様に重大なインシデント等が発生し、実態調査を目的としたログ情報等が必要な場合は、お問い合わせ窓口にご相談ください。

18　順守

18.1　法的及び契約上の要求事項の順守

18.1.1 適用法令及び契約上の要求事項の特定

本サービスに適用される準拠法は日本国の法令です。

18.1.2 知的財産権

本サービスをご利用いただくにあたり知的財産権に関わるお問い合わせは、お問い合わせ窓口にご相談ください。

18.1.3 記録の保護

本組織では、取り扱う文書や記録等の情報は、管理基準を定めて分類し適切に管理しています。本サービスで収集するお客様の利用ログ等については、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保護しています。

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 暗号による管理策の利用方針」をご参照ください。

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

本組織では、内部監査、マネジメントレビュー、リスクアセスメントの実施に加え、ISO/IEC 27001、JIP-ISMS517-1.0(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。

以上