クラウドセキュリティ ホワイトペーパー

Ver 1.1

◇目的

当ホワイトペーパーは、株式会社ディー・ディー・エス（以下「当社」）が提供するクラウドサービスであるEVECLOUD（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 ISO/IEC 27017:2015 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。
各項目の文頭に記載されているカッコは、ISO/IEC 27017:2015 の該当する項番を表しています。

◇クラウドサービスの管理策

【A.5.1】 情報セキュリティのための方針群

EVECLOUDは、当社の定めた
・情報セキュリティ方針
https://www.dds.co.jp/ja/information-security-policy/
・EVECLOUDサービス規約
https://www.dds.co.jp/wp-content/uploads/2023/06/evecloud-termsofservice_D230350.pdf
に従い、サービス運営を行います。

【A.5.2】 情報セキュリティの役割及び責任

EVECLOUDでは、EVECLOUDサービス利用規約にて契約やサービス内容を定義し、サービス提供を実施しております。 基本的には OS の管理者権限をお渡しするサービスに関してはアカウントレイヤーがお客様の責任範囲となり、アプリケーションレイヤーが当社の責任範囲となります。（図1参照）
これらについては、EVECLOUDの利用開始時に利用規約として同意いただく事項となります。

また、サービスの利用契約が終了した場合、本サービス内に保管されているデータは、速やかに削除します。

本サービスの責任分界点（図1）

【A.5.5】 関係当局との連絡

当社の所在地は、当社ウェブサイトにてご確認下さい。
https://www.dds.co.jp/ja/company/access/
サービス内のデータは、日本国内のデータセンターに保管しています。

【A.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

本サービスでは、当社にてサービスの稼働状況と不正アクセスの監視を行っております。

【A.5.9】 情報やその他の関連資産の許容可能な使用

本サービスでは、お客様の情報資産（お客様が保存されるデータ）と、当社が本サービスを運営するための情報を、明確に分離しています。なお、お客様の情報資産（お客様が保存されるデータ）に関しては、お客様の管理範囲です。

【A.5.13】 情報のラベル付け

本サービスでは、情報のラベル付けに関する機能は提供しておりません。

【A.5.16】 アイデンティティ管理

本サービスは、運用管理担当者、利用者IDの登録及び削除機能を提供しております。
登録や削除の手順は、オンラインマニュアルに記載しております。

【A.5.17】 認証情報

本サービスは、管理者ID、利用者IDの登録やパスワード変更、再発行方法につきましては、オンラインマニュアルに記載しております。

【A.5.18】 アクセス権

本サービスの 初期アカウントの発行は申込時に記載された申込書に沿ってテナント管理者アカウントを発行します。本サービスは、利用者ごとの権限設定によるアクセス制御機能について、利用者登録、変更の機能を提供しております。

【A.5.20】 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、「情報セキュリティの役割及び責任」をご確認ください。

【A.5.21】 ICTサプライチェーンにおける情報セキュリティの管理

本サービスでは、ピアクラウドサービスプロバイダに対して当社の情報セキュリティ方針を示し、それを達成するためのリスクマネジメント活動の実施を要求するよう定めています。

【A.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、当社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、確認より48時間以内を目標にお客様管理者様へメールにて通知を行います。 情報セキュリティインシデントに関する問合せは、サポートセンターでお受けいたします。

【A.5.28】 証拠の収集

本サービスのご利用に関して、お客様責任範囲における情報セキュリティインシデントに関するログなどの証拠の収集はお客様にてご実施いただく範囲となります。弊社責任範囲でのログなどの証拠が必要な場合は、お客様の要望に応じて個別に対応しております。都度、ご相談ください。
また、法令に基づき権限を有する公的機関から適法な手続により、開示または提供の要請があった場合は、クラウドサービスカスタマへの通知および同意を経ることなく、当該機関に情報を開示することについて合意いただく必要があります。

【A.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。
また本サービスはSSL/TLSの暗号化を使用しております。なお、輸出規制の対象となる暗号化の利用はありません。

【A.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、当社までお問い合わせください。

【A.5.33】 記録の保護

本サービスは、クラウドサービスカスタマの契約情報の保護や廃棄については、重要な記録の区分をするとともに、管理基準を定め、適切に管理しております。

【A.5.35】 情報セキュリティの独立したレビュー

当社は、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きます。
（2024年10月時点ではISO/IEC 27017の審査準備中です）

【A.6.3】 情報セキュリティの意識向上、教育及び訓練

本サービスでは、サービス運営担当者に対し、当社が定めたセキュリティ教育に加え、クラウドサービス情報セキュリティポリシーに定めた管理事項の運営に必要な教育を実施しています。

【A.6.8】 情報セキュリティ事象の報告

情報セキュリティ事故が発生した場合には、メールなどにて速やかに報告いたします。また、お客様からの事象報告はお問い合わせ窓口にて受け付けております。

【A.7.14】 装置のセキュリティを保った処分又は再利用

本サービスは、サービスの提供に関連する機材の故障などにより交換した記憶媒体の再利用、廃棄に際し、適切なプロセスでデータの削除や設備の破壊を行います。

【A.8.2】 特権的アクセス権の管理

本サービスでは、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。

【A.8.3】 情報へのアクセス制限

本サービスは、管理権限を有する利用者によって、機能制限を行うことができます。

【A.8.6】 容量・能力の管理

本サービスでは、安定的にサービスを提供するため、日々の稼働監視を実施しています。 監視・分析の結果、必要と判断された場合、適切なタイミングにてシステムメンテナンスを実施します。

【A.8.8】 技術的ぜい弱性の管理

本サービスでは、ぜい弱性情報を収集し、収集した情報を元にサービスへの影響を評価し、当社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。

【A.8.13】 情報のバックアップ

本サービスでは、バックアップデータは日次で取得し、35世代分を保持しています。またバックアップデータが問題なく取得できていることを月次で監視しています。インシデント発生の際のリストア手順を定めており、年1回リストア試験を行なっています。

【A.8.15】 ログ取得

本サービスでは、サービスの維持管理に必要となる適切なログを取得し、サービスの提供に関わる作業及び結果を記録し、レビューを実施しています。
また、管理権限を有している利用者へエンドユーザーのサービス利用に関わるログの確認機能を提供しています。

【A.8.17】 クロックの同期

本サービスでは、サービス提供に必要なシステムのクロック同期を、NTP 技術を用いて実施しています。

【A.8.18】 特権的なユーティリティプログラムの使用

本サービスでは、使用者の特権的なユーティリティプログラム、セキュリティ手順を回避することのできるユーティリティプログラムは提供しておりません。ユーティリティプログラムのアクセス権限を定期的に点検しています。

【A.8.22】 ネットワークの分離

本サービスでは、論理的にネットワークを分離し、サービス運営で必要となる管理ネットワークに関しても、お客様のネットワークと分離しています。

【A.8.24】 暗号の使用

本サービスのご利用において保存されるデータは、「AES-256」で暗号化され保管されます。 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。

【A.8.25】 セキュリティに配慮した開発のライフサイクル

本サービスは、当社にて定めた規約に則ったセキュリティに配慮した開発を行っています。
また、開発を外部に委託する際も、これに準じた契約のもと開発が行われます。

【A.8.32】 変更管理

本サービスは、サービスの仕様変更について利用規約に定め、サービスを提供します。

【CLD6.3.1】 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。

【CLD.8.1.5】 クラウドサービスカスタマの資産の除去

サービスの利用契約が終了した場合、サービス内に保管されているデータは、速やかに物理的に削除します。

【CLD.9.5.1】 仮想コンピューティング環境における分離

本サービスでは、仮想化技術やネットワークセキュリティ技術を利用し、データベースのテーブル単位でお客様ごとに分離しています。

【CLD12.1.5】 実務管理者の運用のセキュリティ

本サービスでは、サービスの利用に必要な操作手順を、オンラインマニュアルなどのドキュメントとして提供しています。

【CLD.12.4.5】 クラウドサービスの監視

本サービスでは、サービスの提供に必要なシステムおよびログの監視を行っています。
また、エンドユーザーの利用できるサービスを確認する機能を提供しています。

改版履歴

Ver	日付	改訂内容
1.0	2024.10.15	初版作成
1.1	2024.10.30	【A.5.1】 情報セキュリティのための方針群：条文の誤記修正 【A.5.5】 関係当局との連絡：当社所在地追記 【A.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：条文の変更 【A.8.13】 情報のバックアップ：項目追加 【CLD12.1.5】 実務管理者の運用のセキュリティ：条文の変更