消防団向け災害出動支援クラウド
「コミュたす」

ISO/IEC 27017 ホワイトペーパー

2024/12/01

第 1.1 版

エプソンアヴァシス株式会社

はじめに

JIS Q 27017:2016（ISO/IEC 27017:2015）では、サービスを提供するクラウドサービスプロバイダが実施する情報セキュリティの管理策の内容を、利用されるお客様に向けて情報を提供するよう求めています。
このホワイトペーパー（本書）は、上記の規格に基づき、本サービスが実施している管理策の内容を確認していただくことを目的にしています。

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。また、情報セキュリティを取り巻く環境は日々変化しております。これに対応するための情報セキュリティ対策も変化していますので、最新の情報については、弊社営業までご相談いただくか、下記の本サービスの弊社Webサイトをご確認くださいますようお願いいたします。

URL：https://www.commutas.jp

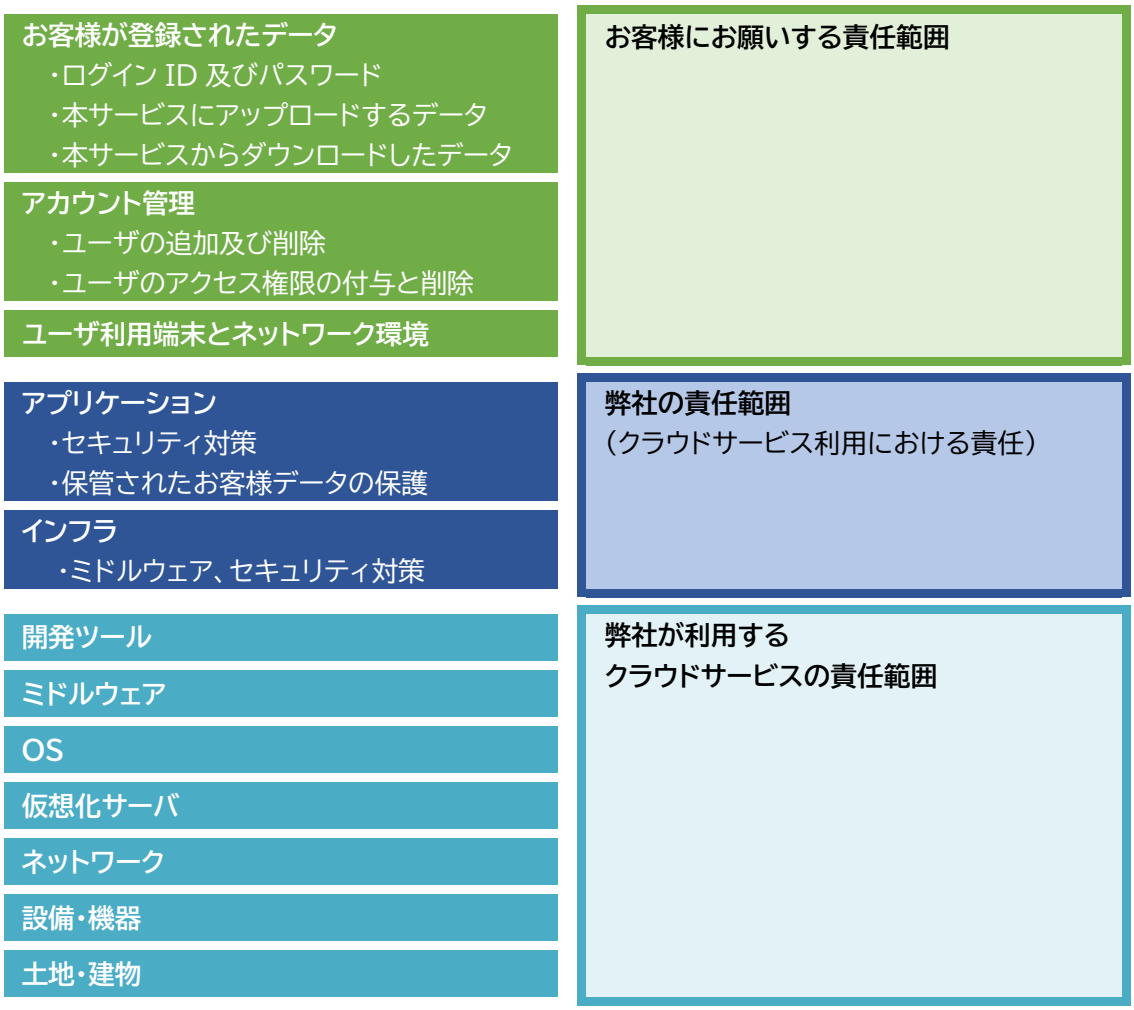
2024/12/01
エプソンアヴァシス株式会社

1.本書の適用範囲

消防団向けクラウドサービス「コミュたす」が本書の適用範囲となります。

2.責任分界点について

本サービスの責任分界点は、以下になります。



3.記載内容について

JIS Q 27017:2016（ISO/IEC 27017:2015）が求める要求事項に対する管理策の項番の順番で本サービスの取り組みを記載いたします。

5.1.1 情報セキュリティのための方針群

本サービスでは、弊社の情報セキュリティ基本方針に従い、下記のクラウドサービス固有の実施の事項を考慮した情報セキュリティ対策を実施しています。

・クラウドサービスの設計及び実装に適用する、最低限の情報セキュリティ要求事項
・認可された内部関係者からのリスク
・マルチテナンシ及びクラウドサービスカスタマの論理的な環境の隔離
・クラウドサービスプロバイダの従業員による、クラウドサービスカスタマの資産へのアクセス管理
・クラウドサービスコンソールへのアクセス制御手順(MFA 認証など)
・変更管理におけるクラウドサービスカスタマへの通知
・仮想化セキュリティ
・クラウドサービスカスタマデータへのアクセス及び保護
・クラウドサービスカスタマのアカウントのライフサイクル管理
・違反の通知、並びに調査及びフォレンジック(forensics)を支援するための情報共有指針

6.1.1 情報セキュリティの役割および責任

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

6.1.3 関係当局との連絡

弊社の本社所在地は下記の通りです。サービスの運用拠点も同じです。

長野県上田市下之郷乙 1077-5 上田リサーチパーク内
https://avasys.jp/company/profile/

なお、弊社が提供するクラウドサービスに保存されたデータの所在は Amazon Web Services(アマゾン ウェブ サービス) の日本国内にあるデータセンタに保管されています。

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および責任の共有および分担

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

7.2.2 情報セキュリティの意識向上、教育および訓練

本サービスに携わる当社サービス運営担当者に対し、情報セキュリティ要件やサービスの運用ルール周知徹底と意識向上のための教育・訓練を定期的に実施しています。

また、お客様が本サービスを適切に利用していただけるように、サービスの機能や操作方法に関してわかり易くお伝えするよう取扱説明書の提供や、説明会の開催に努めてまいります。

8.1.1 資産目録

本サービスにお客様が登録するデータと、弊社がサービスを運営するための情報は明確に分離し情報資産管理台帳で管理しています。

CLD.8.1.5 クラウドカスタマの資産の除去

本サービスにお客様が登録・保存したデータ、および本サービスの利用によって生成されたデータの削除は、サービスの解約日から 10 稼働日以内に実施します。バックアップデータについても同様に削除します。ただし、「18.1.3 記録の保護」に記載の通り、お客様の操作ログなどは、サービス解約後も 1 年間はクラウド上に保存されます。

8.2.2 情報のラベル付け

団員情報の「所属」欄と水利管理の「メモ」欄をラベル付け機能としてご利用いただけます。
どちらもお客様の入力画面にて、テキスト入力ができます。

9.2.1 利用者登録および登録削除

本サービスでは利用者のアカウントを登録・削除する管理者機能を提供しています。
本サービス利用時には管理機能から発行したユーザ ID と、LINE の識別子を紐付ける必要があります。登録の詳細はユーザ登録用紙に記載の手順をご参照ください。

また、管理機能の操作に関しては管理者向けマニュアルをご参照ください。

9.2.2 利用者アクセスの提供

本サービスでは利用者団体ごとに事前設定された機能制限・アクセス権を設定しています。
機能制限やアクセス権は、ユーザの階級や役職によってその範囲が限定されます。
制限の範囲に関しては、利用時に提供する管理者向けマニュアルの表をご覧ください。
またユーザの階級や役職の設定は、お客様側で適宜見直しに努めてください。

9.2.3 特権的アクセス権の管理

本サービスでは、LINE による OpenID Connect（OIDC）による認証の仕組みを提供しています。LINE アプリによる認証は多要素認証にも対応しておりますので、セキュリティ確保にご活用ください。

LINE アプリでの設定：
[LINE アプリ]-[設定]-[アカウント]-[Web ログインの 2 要素認証] を有効にします。

9.2.4 利用者の秘密認証情報の管理

本サービスでは、LINE ログイン認証機能（OIDC）を使用しております。
LINE のパスワードの管理は、利用者自身で努めてください。
また、サービス利用団体の特権ユーザから、サービス利用者アカウントの停止ができます。
サービスアカウントの停止は管理者向けマニュアルをご参照ください。
※本サービスでは、「サービスアカウント」と「LINE アカウント」がログイン連携しており、
サービスアカウントを停止しても、利用者の LINE アカウントには影響を与えません。

LINE アプリでのパスワード設定変更：
[LINE アプリ]-[設定]-[アカウント]-[パスワード] から実施できます。

9.4.1 情報へのアクセス制限

管理者権限を有している利用者によって、各種機能を利用するユーザのアクセスを制限できる機能を提供しています。本サービスにおけるアクセス権は、階級や役割により設定されます。

階級や役割のアクセス権は、利用団体ごとに設定ができるため利用団体内の役割規定などに則った設定が可能です。

9.4.4 特権的なユーティリティプログラムの使用

本サービスにおいて、通常の操作手順または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の提供はありません。

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、仮想化技術を利用し、クラウドシステム環境を利用者団体ごとに論理的に分離しています。マルチテナントの仮想環境で動作しますが、テナント毎に情報資産が分離されているため、別テナントへのアクセス制御が実施されています。

CLD.9.5.2 仮想マシンの要塞化

仮想マシンは、環境構築時に弊社の手順に基づき構築し、構築したシステムのみを利用してサービスを提供しています。環境構築時の自動化や、ログ取得、使用する通信ポートの限定等の要塞化を実施しています。

10.1.1 暗号による管理策の利用方針

お客様よりお預かりしているデータは、すべてクラウドサーバ上で暗号化し管理しています。
また、お客様の利用する Web ページでは SSL/TLS による通信の暗号化を使用しています。

11.2.7 装置のセキュリティを保った処分または再利用

機器の老朽化、故障等により交換した機器媒体については、弊社では機器媒体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。
なおサービスを構成する機器として、弊社の物理的装置はありません。

AWS クラウドにおける安全なデータの廃棄:
https://aws.amazon.com/jp/blogs/news/data_disposal/

12.1.2 変更管理

提供するサービス内容の更新や定期メンテナンスを実施する場合、本サービスの利用者サイトにてお知らせとして事前に通知いたします。
また利用者には、当社サービスサイトでのお知らせ機能に変更内容を通知いたします。

12.1.3 容量・能力の管理

安定的なサービスを提供するために、弊社にてクラウドサービスのリソースを監視し、必要な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

管理者向け機能は、操作マニュアル、FAQなどをサービス開始時に提供しています。

12.3.1 情報のバックアップ

弊社の責任範囲において、本サービスでは、使用するクラウドコンピューティング内にバックアップサーバを設けており、お客様のデータは、更新の度にバックアップし、過去 35 日分のバックアップデータを暗号化して保管しています。

また以下のデータは、お客様自身でバックアップや、リストアできる仕組みを提供しています。

・ユーザ情報
・消防水利情報

12.4.1 イベントログ取得

また、管理者権限を有している利用者向けに下記のようなイベントログを閲覧できる機能を提供しています。ご利用方法は、管理者マニュアルに記載があります。

・各機能の操作ログ
・メール受信ログ
・認証認可ログ
・外部サービスとの送受信ログ

12.4.4 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、システム内部の標準時刻は、世界標準時（UTC）です。画面に表示する際に日本標準時（JST）に変換を行います。

CLD.12.4.5 クラウドサービスの監視

サービスの各種パフォーマンスや攻撃などの監視は、弊社が実施しておりますが、監視結果をお客様に公開するサービス機能は提供していません。確認結果が必要となる場合には、サポート窓口までお問い合わせください。

12.6.1 技術的脆弱性の管理

定期的に脆弱性情報の収集と検査を実施し、何らかの対応が必要となった場合には、定期または緊急メンテナンスにて対応を実施いたします。システムを停止しての対応を伴う際には事前に情報を通知いたします。

13.1.3 ネットワークの分離

本サービスでは、弊社の社内ネットワークと本サービス側のネットワークとは、物理的に分離されています。

CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合

物理ネットワークと論理ネットワークの整合性がとれるように設計、構築、管理をしています。

また、弊社が利用するクラウドサービスプロバイダに関しては ISO/IEC27017 の認証有無を確認の上、開発をしています。

14.1.1 情報セキュリティ要求事項の分析及び仕様化

弊社での、クラウドサービスを開発・構築・運用する際の情報セキュリティ要求事項に基づき、セキュリティ要件を決定し対策をしています。主にお客様にお使いいただける情報セキュリティの機能としては、以下の通りです。

・9.2.1 利用者登録および登録削除
・9.2.2 利用者アクセスの提供
・9.2.3 特権的アクセス権の管理
・9.2.4 利用者の秘密認証情報の管理
・10.1.1 暗号による管理策の利用方針
・12.3.1 情報のバックアップ
・12.4.1 イベントログ取得

14.2.1 セキュリティに配慮した開発のための方針

本サービスでは、弊社で定めた規約（静的解析、セキュリティ対策が入ったライブラリの使用等）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、定期的に脆弱性検査ツールを利用し、セキュリティに配慮したサービスを提供しています。

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、「2.責任分界点について」をご参照ください。

15.1.3 ICTサプライチェーン

弊社が利用するクラウドサービスプロバイダは、外部認証有無などで、情報セキュリティ水準を確認の上、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。

16.1.1 責任及び手順

お客様に大きな影響を与える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、当社サービスサイト及びメールにて通知いたします。
また、セキュリティインシデントに関するお問合せは、当社サポート窓口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

弊社にて確認した情報セキュリティ事象が、お客様に影響を及ぼす可能性がある場合は、サービスサイト及びメールにて通知いたします。 また、お客様から弊社に情報セキュリティ事象を連絡いただく場合は、当社サポート窓口より受け付けています。

16.1.7 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いたします。ただし、法律に基づいた裁判所からの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、お客様のデータを当該機関に開示することがあります。

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、日本国の法令となります。

18.1.2 知的財産権

知的財産権に関わるお問い合わせは、弊社サポート窓口までお問い合わせください。

18.1.3 記録の保護

本サービスのご利用において、蓄積されたお客様の操作ログ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。またログデータは 1 年間以上保存しています。

18.1.5 暗号化機能に対する規制

本サービスでは、キャッチオール規制等の輸出規制の対象となる暗号化の利用はありません。

18.2.1 情報セキュリティの独立したレビュー

弊社は、ISO/IEC 27001（JIS Q 27001）に基づく ISMS 認証を得ており、当クラウドサービスの開発・運用・保守業務に関しても管理策に基づき情報セキュリティ対策を実施しています。

また、クラウドサービス固有の情報セキュリティ対策については、「ISO/IEC27017:2015 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）」に従い、情報セキュリティ対策を実施し、実施状況を定期的に内部監査にて確認しております。

コミュたすサポート窓口連絡先：
commutas-support@exc.epson.co.jp

改版履歴

版数	日付	更新内容
第1.0 版	2024/7/1	初版公開
第1.1 版	2024/12/1	2.責任分界点について　弊社責任内容の明確化を実施 -アプリケーションのセキュリティ事項、データ保護を追加 -インフラ関連の項目全体を追加