セキュリティホワイトペーパー
SERVE システム

メシウス株式会社

2026 年 8 月 1 日　Ver 1.0

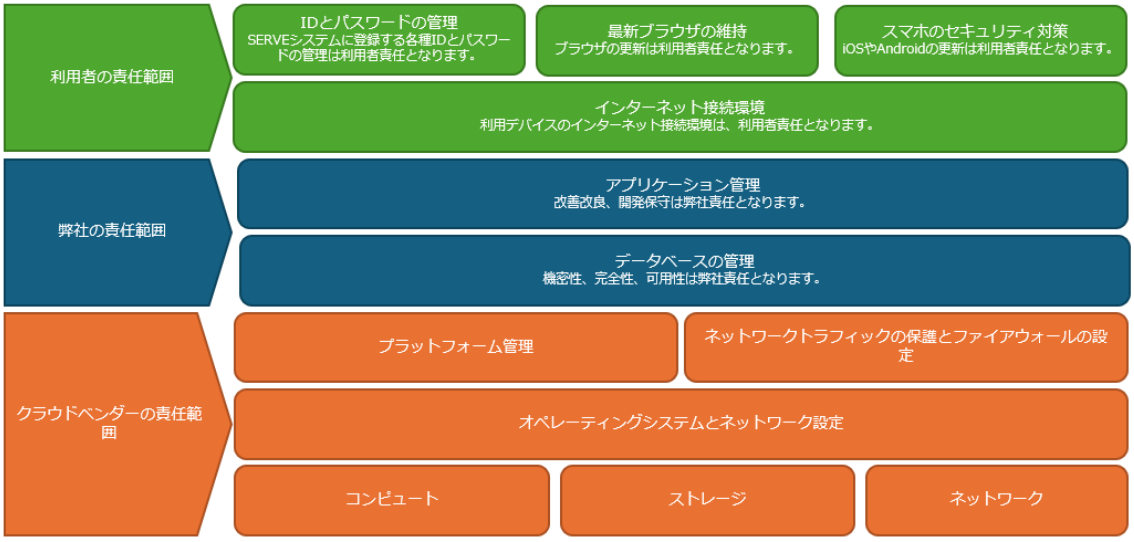
1　はじめに

1.1 ホワイトペーパーの目的

このホワイトペーパー（以下、本書）は、メシウス株式会社（以下、弊社）が提供する SERVE システムにおけるセキュリティの取り組みを、サービス利用者の方に向けてご確認いただくことを目的としております。

1.2 責任分界点

SERVE システムは、Amazon Web Services（以下、AWS）を基盤にシステムを構築しております。SERVE システムに関する責任分界点は以下の通りとなります。



2　セキュリティへの取り組み

2.1 ISO/IEC 27001、JIP-ISMS517-1.0（ISO/IEC 27017）

弊社は、2022 年 7 月に情報セキュリティマネジメントシステム（ISMS）の国際規格である ISO/IEC 27001:2013／JIS Q 27001:2014 の認証を取得しました。

あわせて、クラウドサービスに関する情報セキュリティ管理策の認証である JIP-ISMS517-1.0（ISO/IEC 27017）を取得しております。

その後、2025 年 7 月に ISO/IEC 27001:2022／JIS Q 27001:2023 への移行を含む登録更新を行い、JIP-ISMS517-1.0 についても登録を更新しております。

弊社では、これらの認証に基づく情報セキュリティマネジメントの枠組みに従い、SERVE システムに関連する情報資産について、

機密性、完全性、可用性の維持・向上を図るため、事業内のセキュリティルールを整備し、継続的な運用、監視および改善に取り組んでおります。

2.2 クラウドコンピューティング環境

SERVE システムは、クラウドコンピューティング環境として AWS を採用しております。AWS は、クラウドシステム運用の多くの実績があり、そのノウハウやサービスの継続的な改善や機能追加にも力を入れております。また、ISO/IEC 27001:2022、27017:2015、27018:2019、27701:2019、22301:2019、20000-1:2018、9001:2015、CSA STAR CCM v4.0 の認証を受けており、AWS が SERVE システムの基盤として適切であると判断し、利用しております。

AWS のセキュリティ対策については、下記 URL をご参照ください。

AWS クラウドセキュリティ：https://aws.amazon.com/jp/security/

2.3 アカウント管理

SERVE システムを利用するためのサービス固有のアカウントはあります。サービス利用者は、SERVE システムの機能を利用する際にアカウント ID とパスワードを登録して使用します。

2.4 サービス内におけるアクセス制限

SERVE システムは管理権限を持つユーザーが各アカウントに権限を付与することで、サービスごとのアクセスを制限することが可能です。

2.5 特権的なユーティリティプログラムの使用

SERVE システムを利用するためのサービス固有の特権ユーザーは存在しません。このため、特権を使用してユーティリティプログラムや API を操作することはありません。

2.6 データの保管場所

お客様のデータ並びにバックアップは、AWS の日本国内リージョンに保管されます。

2.7 データの利用

法律上必要な場合を除き、保存されているお客様のデータを弊社が利用することはありません。

2.8 データの削除

契約終了時のデータ取扱いは契約条件および当社所定の手続きに従います。

2.9 アクセスコントロール

SERVE システムは、弊社内外問わず悪意のあるユーザーからの攻撃を防ぐために、必要最小限のポート開放を行っており、故意・過失による不正アクセスの可能性を抑制しております。また、SERVE システムの機能を利用する際にはアカウントによる認証を行っております。

2.10 暗号化の状況

SERVE システムにおける利用者端末とサービス間の通信は、TLS 1.3 により暗号化されています。

2.11 バックアップの状況

データベースに保管されるお客様の設定情報は、日次でバックアップを取得しております。バックアップは、30 日分保管されます。

2.12 クロック

システムで使用しているクラウドサービスのクロックは NTP（Network Time Protocol）サーバを使用して時刻同期を行っており、タイムゾーンは UTC です 。

2.13 ログに関する情報

SERVE システムは、情報セキュリティポリシーに従い、最低 6 か月間のシステムログを保存し、監視を行っております。収集したログは、サービス利用状況の把握、障害発生時の原因調査などの目的で使用します。

2.14 情報のラベル付け

SERVE システムは、保存されたデータに対してラベル付けを行う機能は提供しておりません。

2.15 ネットワークの分離

SERVE システムはマルチテナント方式でサービスを提供しており、共通のクラウド基盤上で運用されています。テナント間のデータはデータベース層で論理的に分離され、他テナントのデータへアクセスできない構成としています。

2.16 サービスのバージョンアップ

サービスのバージョンアップは、実施前に以下にてお知らせをしております。

・SERVE システム

システム稼働状況のお知らせページ（https://serve.jp/support/）

SERVE システムのトップページ（https://en.serve-system.jp/）

・SERVE〈保護者アプリ〉

マイページ ＞ メーカーからのお知らせ

2.17 開発におけるセキュリティ情報

SERVE システムのシステム開発は、脆弱性を作りこまないよう、 IPA Web Security CheckList V7 などの一般的なセキュリティ対策基準に従って実施されます。また、第三者セキュリティ専門家によるセキュリティ脆弱性診断を重要変更時に実施しております。

2.18 インシデント発生時の対応

インシデント発生時は、運用規則に沿って以下にて障害状況を通知いたします。

・SERVE システム

システム稼働状況のお知らせページ（https://serve.jp/support/）

SERVE システムのトップページ（https://en.serve-system.jp/）

・SERVE〈保護者アプリ〉

マイページ ＞ メーカーからのお知らせ

掲載できない場合は SERVE のホームページのお知らせに障害状況について掲載します。

2.19 適用法令

お客様と弊社との間の契約は、日本法に基づいて解釈されるものとします。AWS に適用される法域については、準拠法は日本法で、裁判所は東京地裁になります。

【改訂履歴】

本書の改訂履歴は以下の通りです。

Ver.	発行日	改訂内容
1.0	2026/8/1	制定