セキュリティホワイトペーパー

LeySer System

LeySer Plus

LeySer Connect

メシウス株式会社

2025 年 10 月 1 日　Ver 2.0

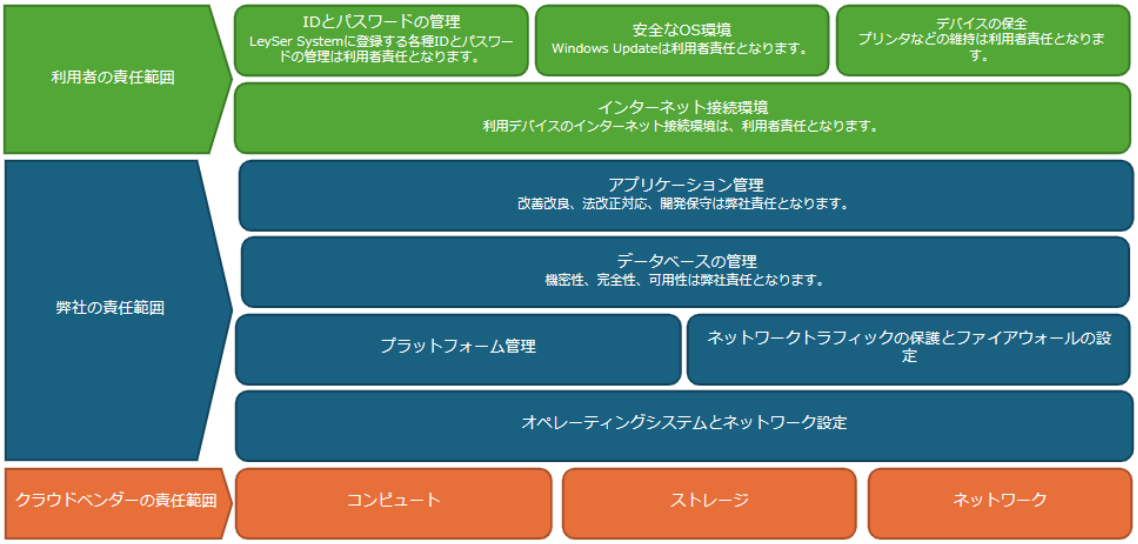
1　はじめに

1.1 ホワイトペーパーの目的

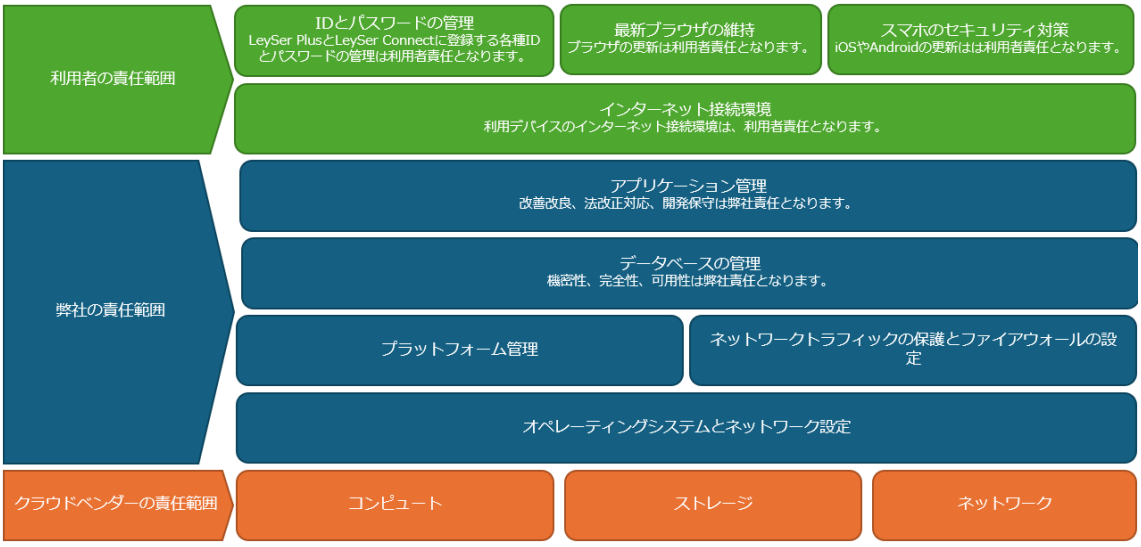
このホワイトペーパー（以下、本書）は、メシウス株式会社（以下、弊社）が提供する「LeySer System、LeySer Plus、LeySer Connect」におけるセキュリティの取り組みを、サービス利用者の方に向けてご確認いただくことを目的としております。

1.2 責任分界点

「LeySer System、LeySer Plus、LeySer Connect」は、国内クラウドベンダーを基盤にシステムを構築しております。「LeySer System」に関する責任分界点は以下の通りとなります。



「LeySer Plus、LeySer Connect」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、JIP-ISMS517-1.0（ISO/IEC 27001:2013及び ISO/IEC 27001:2015）を取得しました。2025年7月にISO/IEC 27001:2022／JIS Q 27001:2023、JIP-ISMS517-1.0 を登録更新しております。「LeySer System、LeySer Plus、LeySer Connect」が保有する情報資産を機密性、完全性、可用性の観点から維持・改善するために、事業内におけるセキュリティルールを確立し、継続的に運用、監視、改善を行っております。

2.2 クラウドコンピューティング環境

「LeySer System、LeySer Plus、LeySer Connect」は、クラウドコンピューティング環境として国内クラウドベンダーを採用しております。国内クラウドベンダーは、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、ISO/IEC 27017:2023 の認定を受けており、国内クラウドベンダーが「LeySer System、LeySer Plus、LeySer Connect」の基盤として適切であると判断し、利用しております。

2.3 アカウント管理

「LeySer System、LeySer Plus、LeySer Connect」は、サービス固有のアカウントで利用します。サービス利用者は、「LeySer System、LeySer Plus、LeySer Connect」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

「LeySer System、LeySer Plus、LeySer Connect」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、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

「LeySer System、LeySer Plus、LeySer Connect」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、国内クラウドベンダーの日本国内リージョンに保管しております。

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

契約が終了した場合、お客様が「LeySer System、LeySer Plus、LeySer Connect」に保存したデータは契約終了日から直ちに消去されます。以降、お客様のデータを復元することができないようになっております。なお、データ削除の証明書に類する書類は発行しておりません。

2.9 アクセスコントロール

「LeySer System、LeySer Plus、LeySer Connect」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、「LeySer System、LeySer Plus、LeySer Connect」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

「LeySer System、LeySer Plus、LeySer Connect」のデータは、一般に公開される利用サービスの通信は TLS 1.2 方式により暗号化されます。

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データは、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、7 世代（7 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

「LeySer System、LeySer Plus、LeySer Connect」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

「LeySer System、LeySer Plus、LeySer Connect」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

「LeySer System、LeySer Plus、LeySer Connect」は、マルチテナント方式でサービス提供を行い、各テナントはネットワークを共有して利用しております。ネットワークの分離は行っておりませんが、データベース層で論理的に切り離すように構築しているため、テナント間のデータアクセスができない構成になっております。

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「メーカーからのお知らせ」にてご連絡いたします。

2.17 開発におけるセキュリティ情報

「LeySer System、LeySer Plus、LeySer Connect」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するとともに、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不定期に実施しております。

2.18 インシデント発生時の対応

「メーカーからのお知らせ」や「https://s.leyser.jp/info」へ障害状況を掲載し、通知します。
また、影響度に応じてご契約者様・追加連絡先へのメール配信も行います。
なお、お客様からの情報セキュリティインシデントに関するご質問は、メールで Lsupport@mescius.com までお問い合わせください。

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。Azure 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	2025/4/1	制定
2.0	2025/10/1	登録更新に伴う修正