MRS クラウド UI
ホワイトペーパー

第 1.0 版

株式会社ミライコミュニケーションネットワーク

目次

I. 目的

セキュリティホワイトペーパー（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、株式会社ミライコミュニケーションネットワーク(以下、当社という)が利用者に対し提供しているセキュリティの取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

当社の ISO/IEC 27017 の適用範囲は、以下のサービス内容に対するものです。

・MRS クラウド UI（https://mrs.mirai.ad.jp/plan/cloud/）

III. 用語について

本書では ISO/IEC 27017:2015 (JIS Q 27017:2016)で記されている用語については、そのまま使用しています。本サービスで利用している用語については、サービス約款にてご確認いただけます。

IV. 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管理策を記載します。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）の小項目番号・要求事項原文を示しています。

5　情報セキュリティ方針のための方針群

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

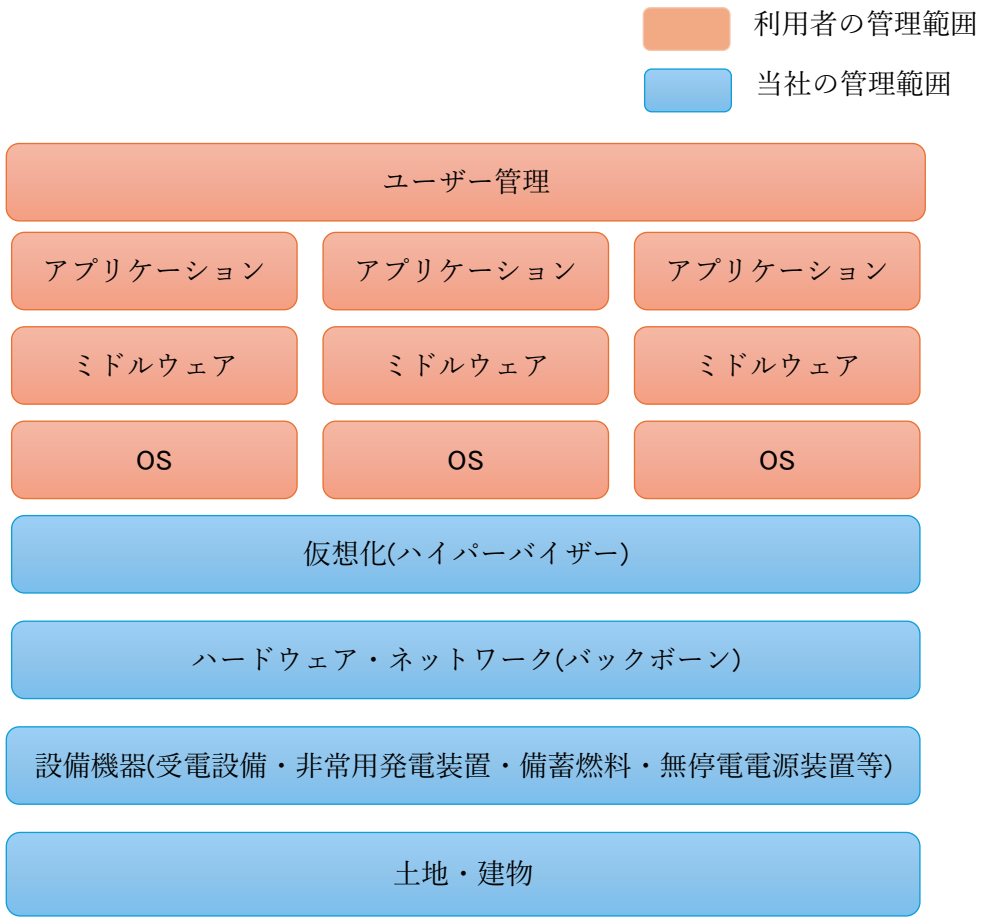
クラウドサービスプロバイダ(CSP)は、 クラウドサービスの提供および利用に取り組むため、情報セキュリティ方針を拡充することが求められています。本サービスでは、当社の情報セキュリティ方針並びにクラウドサービス情報セキュリティ方針に従いサービスを運用しています。

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および責任

情報セキュリティの役割および責任についてサービス約款に定め、サービスを提供しています。本サービスにおける責任分界点は下図のとおりです。



6.1.3 関係当局との連絡

当社所在地は、MRS クラウド UI サービス約款（以下、サービス約款という）に記載しております。また、クラウドサービスカスタマデータを保存する国は、日本国となります。

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および責任の共有および分担

情報セキュリティの役割および責任についてサービス約款に定め、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および責任」をご参照下さい。

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、教育および訓練

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運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練および意識向上の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

利用者の情報資産(保存データ)とサービス提供者が運営するための情報資産は情報資産台帳上で明確に識別の上分離しています。なお、本サービスにおいて利用者が作成・保存する情報資産は、利用者の管理範囲となります。

CLD.8.1.5 クラウドサービス利用者の資産の除去

利用者が本サービスの利用を停止または終了した場合、当社は利用者が本サービスに登録した情報や、登録した情報等を含む書面及びその複製物に対し、利用者の責任において削除いただきます。クラウドサービスカスタマが仮想マシンを含む情報等の削除を行わずに利用を終了された場合は、サービス約款の定めに従い、当社で削除いたします。

8.2 情報の分類

8.2.2 情報のラベル付け

本サービスをご利用いただくにあたり、仮想マシン上に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。管理サイトでは、「プロジェクト名」のラベル付け機能を提供しています。

9 アクセス制御

9.2 利用者アクセスの管理

9.2.1 利用者登録および登録削除

管理サイトの利用者登録及び削除は、当社にて実施します。利用者が作成した仮想マシン上の利用者登録および登録削除は、利用者側での実施となります。

9.2.2 利用者アクセスの提供(provisioning)

本サービスでは、管理サイトへのアクセス権については、契約時に作成したアカウントの管理者がマスターユーザーとなります。機能制限契約時にご提供するクラウドサービスカスタマの作成された仮想マシンへのアクセス権につきましては、クラウドサービスカスタマの定めた規定に従い運用いただくこととなります。

9.2.3 特権的アクセス権の管理

特権的アクセス権は管理者アカウントが該当いたします。当該権限の利用においては、ログイン ID、パスワードによる認証のほか、接続元 IP アドレス制限によってセキュリティを確保しています。アカウントは自己の責任で適切に管理をお願いします。

9.2.4 利用者の秘密認証情報の管理

管理サイトへのログインするための認証情報は、担当よりご案内いたします。この認証情報は、当社で管理しているため利用者側で変更することはできません。

9.4 システム及び業務用ソフトウェアのアクセス制御

9.4.1 情報へのアクセス制限

本サービスのご利用にあたっては、利用者側のアクセスポリシーを適用し、利用者による設定にて情報へのアクセス制限を行うことができます。

9.4.4 特権的なユーティリティプログラムの使用

利用者に対し、セキュリティ手順を回避し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、当社にて運用保守のために保持する特権的ユーティリティプログラムについては、利用者を厳しく限定し、ログによるレビューを実施しております。

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

本サービスでは、利用者ごとにリソースおよびネットワーク領域を分離しており、マルチテナント環境でご利用いただけます。

CLD.9.5.2 仮想マシンの要塞化

構築するすべての仮想化環境は、利用者からサービス申込みの際にご指定いただいた設定でご提供します。また、当社標準の仮想マシン構築手順を整備し、ポート・プロトコルへの制限を実施したうえで仮想マシンを要塞化してご提供します。

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

本サービスでは以下の暗号化を実施しております。

・通信：SSL/TLS（TLS 1.2 対応）を利用

仮想マシン内で扱うデータの暗号化については、利用者にて任意の暗号化を設定いただけます。

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

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、当社内のルールに従って廃棄・再利用しており、廃棄に際しては記録を保持しております。

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

提供するサービスの更新や定期メンテナンスを実施する場合、原則 2 週間前までにログイン後のポータルにて通知させていただきます。

12.1.3 容量・能力の管理

安定的なサービス提供を行うため、各サーバーのリソースを監視し、必要に応じて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

本サービス操作方法は、「管理画面操作手順書」にて利用者にご案内しており、改訂された場合には都度お知らせいたします。

12.3 バックアップ

12.3.1 情報のバックアップ

本サービスではバックアップ機能は提供しておらず、利用者の責任でデータエクスポートを行う等で実施いただきます。なお、本サービスでは、複数ノードによる運用によって可用性を向上させるほか、複数ノードの冗長構成により、システムの一部に障害が発生しても、他のノードが機能を維持するほか、複数のノードにデータを複製することで、データの損失を防ぎ、システムの信頼性を向上させています。

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、利用者に仮想化基盤へのログイン/ログアウトおよび操作ログを取得しており過去 30 日分までご提供可能です。ログについては、アクセス制御されたログ管理サーバーで保存しております。なお、当社側でアクセスログの追跡はできかねますので、利用者ご自身で管理をお願い致します。

12.4.4 クロックの同期

本サービスでは、NTP サーバーを参照することで時刻を同期しています。

CLD.12.4.5 クラウドサービスの監視

本サービスでは、開発・構築時に監視要件を決定し、実装しております。利用者においては、リソース使用状況を監視することができます

12.6 技術的脆弱性管理

12.6.1 技術的脆弱性の管理

本サービスでは、脆弱性情報を常時収集・評価し、対応しております。利用者へ影響がある場合には、メールで通知いたします。

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セキュリティ要件を決定し、用途別にネットワークを分離しております。

CLD13.1.4 仮想および物理ネットワークのセキュリティ管理の整合

本サービスにおける物理ネットワークおよび仮想ネットワークは、それぞれ管理表に基づいて当社内部ネットワーク領域と利用者ネットワークの割り当てを管理することで整合性を確保しています。

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および仕様化

当社では、当社内の基準に従い、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、実装しております。主に利用者が検討される情報セキュリティの機能の仕様として、当ホワイトペーパー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

当社では、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、当社内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、脆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、サービス約款に定め、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「6.1.1 情報セキュリティの役割および責任」をご参照下さい。

15.1.3 ICT サプライチェーン

本サービスは、当社のデータセンターにて環境を構築しております。当社からの委託先については、契約・約款の定めに従い管理を行っています。また、現時点においてクラウドサービスプロバイダは存在しません。今後利用する場合には、同等の情報セキュリティ水準を要求することとしています。合わせて、サプライチェーンでクラウドサービスを提供する場合は、供給者に対して情報セキュリティ目的を示し、それを達成するためのリスクマネジメント活動を要求することとしています。

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 責任および手順

利用者に大きな影響を与え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、インシデントの発生を確認してから 3 営業日を目標に、メール、電話、当社 Web サイトへの掲載により通知いたします。情報セキュリティインシデントに関する問合せは、お問い合わせ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

情報セキュリティ事象が発生した場合には、メールで通知いたします。また個別のお問い合わせは、お問い合わせ窓口にて受け付けています。

16.1.7 証拠の収集

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、利用者の同意なく、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、本サービス約款をご確認ください。なお、利用者に重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には、お問い合わせ窓口までお問い合わせください。

18 順守

18.1 法的及び契約上の要求事項の順守目的

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「日本法」となります。本サービス運用に関連する各種法令に関しては法規制管理台帳を作成し、準拠するように努めています。

18.1.2 知的財産権

本サービスをご利用いただく上で知的財産権に関わるお問い合わせは、お問い合わせ窓口までお問い合わせ下さい。

18.1.3 記録の保護

利用者の本サービスご利用に関して蓄積された記録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。

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 参照）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

当社では、社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001、ISO/IEC27017 に基づく第三者による認証審査を控えており、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。

V. 変更履歴

版	日付	改訂内容
第 1.0 版	2024/10/30	制定

以上