REMETIS

セキュリティ管理体制について

1.0版

株式会社 RESTAR
https://www.restar-inc.com/

目的

当ホワイトペーパーは、RESTAR株式会社（以下「当社」）が提供するクラウドサービスである REMETIS - レメティス（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である 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。
なお、各項目の先頭に記載されているカッコは、ISO/IEC 27017:2016 の該当する項番を表しています。

目次

情報セキュリティの取り組み

A.5.1 情報セキュリティのための方針群

REMETISは、当社の定めた情報セキュリティ基本方針（https://www.remetis.jp/）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（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）

REMETISでは、利用規約にて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。利用開始に当たり、管理者権限を有するユーザーを作成いたします。ユーザーアカウント管理・データの管理(リクエスト情報)はお客様の責任範囲となります。こちらについてはREMEITS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。

A.5.5 関係当局との連絡

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。

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本ドキュメントに定め、サービスを提供します。

お客様責任範囲

- アカウント管理
- データ管理

弊社責任範囲

- インフラストラクチャ（サーバー、ミドルウェア）
- アプリケーション開発・保守
- IPアクセス制御

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方針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.5.9 情報及びその他の関連資産の目録

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。

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、要望に応じ速やかに物理的に削除します。

A.5.13 情報のラベル付け

本サービスでは、以下の機能を提供し、ユーザ様のデータ分類をサポートします。
・案件情報へのタグ付け
・ユーザアカウントごとのグループ設定、およびグループを元に案件情報にアクセス権の設定
使用方法の詳細はサービス内の「サービスの使い方」をご参照ください。

A.5.16 識別情報の管理

本サービスは、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、サービス内の「サービスの使い方」をご参照ください。

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書へ記載されたメールアドレスをIDとして、管理者権限を有するユーザーを発行致します。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、ユーザー登録、変更の機能を提供しております。

A.8.2 特権的アクセス権

本サービスでは、IPアドレス制限・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.5.17 認証情報

本サービスは、ユーザーIDの登録やパスワード変更、再発行方法につきましては、サービス内の「サービスの使い方」をご参照ください。

A.8.3 情報へのアクセス制限

本サービスは、管理権限を有するユーザーによって、機能制限を行うことができま

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、アプリケーションレイヤーで論理的に分離しています。

CLD.9.5.2 仮想マシンの要塞化

お客様が利用するサービスの提供に用いる仮想環境は、IP/プロトコル/ポートへのアクセス制限などを実施しています。

A.8.24 暗号の利用

本サービスのご利用において保存されるデータは、「AES-256-XTS」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.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.8.32 変更管理

本サービスの大きなサービスの仕様変更についてはメールなどにて1週間以上前にお伝えいたします。

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。

CLD.12.1.5 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、サポートセンターにてマニュアルなどのドキュメントを提供しています。

A.8.13 情報のバックアップ

本サービスでは、顧客情報を、日次取得し、30世代を取得/保持しています。

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。ログは1年間保管しています。

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などの技術を用いて実施しています。

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。

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.8.22 ネットワークの分離

本サービスの、本番環境のネットワークは、開発環境・テスト環境と分離しています。

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

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、アプリケーションレイヤーでクラウドサービスカスタマごとに論理的に分離しています。

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.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本ドキュメントに定め、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.5.24 情報セキュリティインシデント管理の計画策定及び準備

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、確認次第速やか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.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サポートセンターにて受け付けております。

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。

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。ログは1年間保管しています。

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ます。

改訂履歴

版	日付	概要
1.0	2025-07-02	初版発行