RecoRu

勤怠管理システムのレコル

セキュリティホワイトペーパー

第 1.1 版

中央システム株式会社

目次

1. 目的 3

2. 適用範囲について 3

3. 用語について 3

4. ISO/IEC 27017:2015 (JIS Q 27017:2016) への対応 3

5.1.1 情報セキュリティのための方針群 4
6.1.1 情報セキュリティの役割および責任 4
6.1.3 関係当局との連絡 4
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 4
7.2.2 情報セキュリティの意識向上、教育および訓練 4
8.1.1 資産目録 5
CLD.8.1.5 クラウドサービス利用者の資産の除去 5
8.2.2 情報のラベル付け 5
9.2.1 利用者登録および登録削除 5
9.2.2 利用者アクセスの提供(PROVISIONING) 5
9.2.3 特権的アクセス権の管理 5
9.2.4 利用者の秘密認証情報の管理 5
9.4.1 情報へのアクセス制限 5
9.4.4 特権的なユーティリティプログラムの使用 5
CLD.9.5.1 仮想コンピューティング環境における分離 6
CLD.9.5.2 仮想マシンの要塞化 6
10.1.1 暗号による管理策の利用方針 6
11.2.7 装置のセキュリティを保った処分又は再利用 6
12.1.2 変更管理 6
12.1.3 容量・能力の管理 6
CLD.12.1.5 実務管理者の運用のセキュリティ 6
12.3.1 情報のバックアップ 6
12.4.1 イベントログ取得 7
12.4.4 クロックの同期 7
CLD.12.4.5 クラウドサービスの監視 7
12.6.1 技術的脆弱性の管理 7
13.1.3 ネットワークの分離 7
14.1.1 情報セキュリティ要求事項の分析および仕様化 7
14.2.1 セキュリティに配慮した開発のための方針 7
15.1.2 供給者との合意におけるセキュリティの取扱い 8
15.1.3 ICT サプライチェーン 8
16.1.1 責任および手順 8

16.1.2 情報セキュリティ事象の報告 8
16.1.7 証拠の収集 8
18.1.1 適用法令および契約上の要求事項の特定 8
18.1.2 知的財産権 8
18.1.3 記録の保護 9
18.1.5 暗号化機能に対する規制 9
18.2.1 情報セキュリティの独立したレビュー 9
5. 変更履歴 9

1. 目的

レコルのセキュリティホワイトペーパー（以下本書）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、当社がお客様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。

2. 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。
・レコル

＜お問い合わせの窓口：レコールサポートデスク＞
メール：recoru-contact@smart-works.jp
営業時間：平日 10:00 ～ 17:00（12:00 ～ 13:00 を除く）

3. 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。レコルで利用している用語については、レコル利用規約でご確認いただけます。

4. ISO/IEC 27017:2015 (JIS Q 27017:2016）への対応

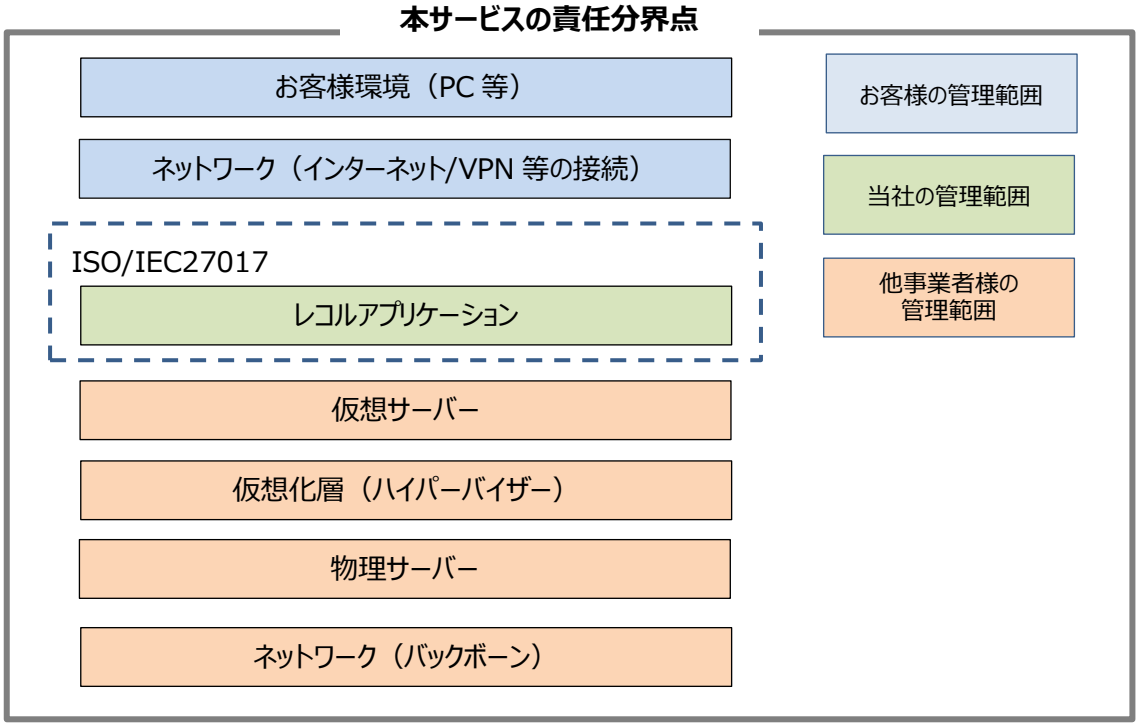
以下に ISO/IEC 27017:2015 (JIS Q27017:2016)が求める要求事項に対する管理策を記載します。番号・タイトルは、ISO/IEC 27017 が求める「情報セキュリティ管理策の実践の規範」 5～18（17 を除く）の小項目番号・要求事項原文を示しています。

5.1.1 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。 レコルでは、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。

6.1.1 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利用規約に定め、サービスを提供しています。レコル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

クラウドサービスで保存いただくデータの所在は日本国内になります。

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

情報セキュリティの役割および責任についてレコル利用規約に定め、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。

7.2.2 情報セキュリティの意識向上、教育および訓練

情報セキュリティ要件の周知徹底と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。

8.1.1 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明確に分離しています。なお、利用者がレコルに作成・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

利用者がレコルの利用を停止または終了した場合、当社は利用者がレコルに登録した情報を消去します。削除については解約日の翌々月 20 日に削除いたします。

8.2.2 情報のラベル付け

レコルは、登録情報に対して ID や各種番号によるラベル付け機能を搭載しており、円滑なサービス提供を実現しています。詳細は、オンラインマニュアルにてご確認頂けます。

9.2.1 利用者登録および登録削除

利用者登録及び削除は、管理者権限を有するログイン ID にて利用者の登録・更新・削除の機能がご利用頂けます。詳細は、オンラインマニュアルにてご確認頂けます。

9.2.2 利用者アクセスの提供(provisioning)

レコルの参照範囲や機能実行範囲を定めるための権限管理機能を提供しています。

9.2.3 特権的アクセス権の管理

特権的アクセス権は、アカウント管理者に付与されます。アカウント管理者は、ログイン ID、パスワード認証により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

レコルのメニューでユーザー登録後、ログイン ID とパスワードを対象者へ通知してください。パスワード変更方法は、オンラインマニュアルをご参照下さい。

9.4.1 情報へのアクセス制限

レコルのご利用にあたっては、利用者管理メニューの権限設定機能により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。
当社においてサービス提供に必要な特権的なユーティリティプログラムについては利用者を厳しく制限し、利用の妥当性を事前に確認し、ログを取得し、レビューを実施しております。

CLD.9.5.1 仮想コンピューティング環境における分離

マルチテナント環境で動作します。テナント毎の ID によるアクセス資源の分離を実施し、別テナントへのアクセス制御を実施しています。

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ポート・プロトコルへの制限を実施し、不正アクセスを遮断して適切にログを保存しています。

10.1.1 暗号による管理策の利用方針

レコルのデータ(アプリケーション及びデータベースのストレージ)は暗号化を行っており、鍵の管理は AWS Key Management Service を利用しています。お客様パスワードはハッシュ化して保管しています。

レコルにおいてお客様データをやり取りする通信は SSL/TLS（TLS 1.2/ TLS 1.3 対応） 通信を用いて暗号化しています。

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、当社では直接装置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。

https://aws.amazon.com/jp/blogs/news/data_disposal/

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、HP 及びレコルログイン後のお知らせとメールで事前に通知いたします。

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

レコルの操作方法は、レコルログイン後のオンラインマニュアルページにて各種マニュアルを提供しています。

12.3.1 情報のバックアップ

システムおよびお客様情報資産のバックアップは 35 日間、差分バックアップにて保持しています。バックアップからのリストアテストを定期的に実施しています。バックアップデータは暗号化を行い保管しています。(10.1.1 暗号による管理策の利用方針に記載の通りです。)

12.4.1 イベントログ取得

レコルの維持管理に必要となる適切なログを取得しています。ユーザはレコルへログイン後、過去5 年分の打刻ログおよび勤務編集ログを確認することができます。
また、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、過去 5 年分のアクセスログから調査を実施しますので、レコルサポートデスクまでお問い合わせください。

12.4.4 クロックの同期

レコルでは NTP サーバーを参照することで時刻を同期（日本標準時）しています。

CLD.12.4.5 クラウドサービスの監視

WAF や IDS を用いることで、不正に利用されていないことを常に監視しています。また、CPU・メモリ・ディスクの使用率等のシステムに関するリソース状況も監視しています。

12.6.1 技術的脆弱性の管理

定期的に脆弱性情報の収集を実施し、当社の責任の範囲で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します。
メンテナンス情報は HP 及びレコルログイン後のお知らせとメールで通知いたします。
当社では、より一層のセキュリティ確保のため、上流でセキュリティ要件を定め、テストを実施した上でリリースしています。

13.1.3 ネットワークの分離

インターネット回線を利用してレコルへ接続し、契約 ID とログイン ID により論理的にセキュリティを確保しています。レコル管理者は、VPN を利用し他の利用者のネットワークと分離しています。

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、情報セキュリティ方針の下で、お客様が要求される情報セキュリティを維持、提供しています。
主にお客様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）
- バックアップ機能（12.3.1 情報のバックアップ）
- ログ取得機能（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

当社では、セキュリティに配慮した開発方針として、開発時点からセキュリティに関するリスク対応、脆弱性対応を行い、初期リリース時及び大幅な変更を伴うメンテナンス時に第三者による脆弱性診断、及びネットワーク診断を行っています。

15.1.2 供給者との合意におけるセキュリティの取扱い

レコルにおける役割及び責任については、レコル利用規約に定め、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「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

当社が利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、レコル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。

レコルは、AWS をクラウドサービスプロバイダとして運用しています。AWS のコンプライアンス状況については下記をご参照下さい

https://aws.amazon.com/jp/compliance/

16.1.1 責任および手順

利用者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、サービスレベルに基づきメールで通知いたします。サービスレベルについて詳細はレコル利用規約をご確認ください。
セキュリティインシデントに関する問合せは、レコルサポートデスク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

HP 及びレコルログイン後のお知らせ、またはメールで通知いたします。
また個別のお問い合わせは、レコルサポートデスクより受付けています。

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、レコル利用規約をご確認ください。
なお、お客様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レコルサポートデスクまでお問い合わせください。

18.1.1 適用法令および契約上の要求事項の特定

レコルの利用に関して、適用される「準拠法」は「日本法」となります。
レコル運用に関連する各種法令に関しては関連法規管理要領に従い、法的準拠するように努めています。

18.1.2 知的財産権

レコル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、レコルサポートデスクまでお問い合わせ下さい。

18.1.3 記録の保護

利用者のレコル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

レコルでは SSL/TLS （TLS 1.2/TLS 1.3 対応）による通信の暗号化を使用しています。なお、輸出規制の対象となる暗号化の利用はありません。

18.2.1 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受け、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。

（2023 年 6 月 ISO/IEC27017 認証取得）

5. 変更履歴

版	改訂日	改訂内容
1.0	2023/2/1	初版作成
1.1	2023/6/27	ISO/IEC27017 認証取得に伴い修正