

CoDMON（コドモン）

クラウドセキュリティホワイトペーパー

---

ISO/IEC 27017に基づくセキュリティ要求事項への取り組み

2024年6月1日 第2版

株式会社コドモン

本書の無断利用・転載等の一切を禁止しています

版数	年月日	内容
1.0	2023年11月1日	新規作成
2.0	2024年6月1日	ISO/IEC 27001:2022 移行による見直し

## 1 目的

本書では、株式会社コドモン（以下、当社）がクラウドサービスプロバイダとして提供する「コドモン（以下、本サービス）」における ISO/IEC 27017（情報-セキュリティ技術-ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）への取り組みを解説し、本サービスにおけるクラウドセキュリティ仕様を明確にします。

## 2 適用範囲

当社の ISO/IEC 27017 におけるクラウドサービスプロバイダの適用範囲は、以下になります。

クラウドサービスプロバイダ	サービスサイト
保育・教育施設向け業務支援システム「コドモン」	<a href="https://www.codmon.com/">https://www.codmon.com/</a>

本サービスは、お客さまからのお申込みに基づき、役務提供しています。

## 3 サービス仕様

### 3.1 利用規約等

文書名	公表先
コドモンサービス共通利用規約 (施設事業者向け)	<a href="https://www.codmon.com/terms/school/">https://www.codmon.com/terms/school/</a>
コドモンサービス利用規約 (保護者向け) :	<a href="https://www.codmon.com/terms/family/">https://www.codmon.com/terms/family/</a>
写真等販売サービス利用特約	<a href="https://www.codmon.com/terms/photo/">https://www.codmon.com/terms/photo/</a>

### 3.2 クラウドサービスのサービス提供時間

サービス時間
24 時間 365 日（計画停止/保守を除く）

セキュリティ対応やシステム稼働に重要な影響がある場合は、緊急メンテナンスを行います。

### 3.3 クラウド品質保証 (SLA)

文書名	公表先
クラウド品質保証 (SLA)	<a href="https://www.codmon.com/terms/sla/">https://www.codmon.com/terms/sla/</a>

### 3.4 動作環境

文書名	公表先
動作確認環境	<a href="https://www.codmon.com/terms/environment/">https://www.codmon.com/terms/environment/</a>

### 3.5 コドモン運営事務局サポートセンター（コドモンヘルプセンター）

対象	公表先
保護者向け	<a href="https://help.codmon.com/parent">https://help.codmon.com/parent</a>
施設向け	<a href="https://help.codmon.com/facility">https://help.codmon.com/facility</a>

### 3.6 クラウドサービスプロバイダの地理的所在地

サービス	場所
AWS	日本国内 (Japan Region)

### 3.7 他社商標について

文書名	公表先
当サイトで使用している 他社商標	<a href="https://www.codmon.com/terms/other-trademark/">https://www.codmon.com/terms/other-trademark/</a>

#### 4 ISO/IEC 27017 に対するセキュリティ取り組み

本書に記載の ISO/IEC 27017 に関する項目は、クラウドサービスプロバイダとしての管理事項およびお客様に公表すべき事項に限定しております、当社のクラウドセキュリティ認証に関わる全ての項目を網羅しているわけではありませんのでご了承ください。

本書は、ISO/IEC 27017:2015 管理策を基準に構成しています。

当社 ISMS の JIS Q 27001:2023 (ISO/IEC 27001:2022) 移行に伴い、ISO/IEC 27017 に対するセキュリティ取り組み（対策内容）に変更及び影響が生じないことを確認しています。  
※各項目タイトル（例：管理策 5.1）の表記は、ISO/IEC 27001:2022 管理策に該当するものです。

##### A.5.1.1 情報セキュリティのための方針群（管理策 5.1）

本サービスでは、弊社の情報セキュリティ基本方針、個人情報保護方針および個人情報の取り扱いについて、クラウドセキュリティ基本方針に従い、情報セキュリティおよび個人情報に関して極めて重要な事項として取り扱い、サービス運営を行います。

文書名	公表先
情報セキュリティ基本方針	<a href="https://www.codmon.co.jp/securitypolicy/">https://www.codmon.co.jp/securitypolicy/</a>
個人情報保護方針	<a href="https://www.codmon.com/terms/privacy-policy/">https://www.codmon.com/terms/privacy-policy/</a>
個人情報の取り扱いについて	<a href="https://www.codmon.com/terms/privacy/">https://www.codmon.com/terms/privacy/</a>
クラウドセキュリティ基本方針	<a href="https://www.codmon.com/terms/cloudsec/">https://www.codmon.com/terms/cloudsec/</a>

##### A.6.1.1 情報セキュリティの役割および責任（管理策 5.2）

本サービスの運用は当社の責任範囲としてサービスの提供範囲に含まれておりますが、利用者情報の登録、変更、削除管理はお客様の責任範囲となります。詳細については各利用規約をご参照願います。

当社においては、情報セキュリティポリシーで定めた管理体制に沿って、データにアクセスできる管理者を制限しています。管理者には情報セキュリティ教育を定期的に実施しています。

また本サービスは「AWS」を基に構築しており、「AWS」の保守・点検・整備・改良・拡張作業・中断またはセキュリティ上のリスクや脅威等が生じた場合、サービスに影響がある場合があります。

##### A.6.1.3 関係当局との連絡（管理策 5.5）

関係当局については、社内文書にて特定・保持しております。お客様に対しては、お問い合わせ窓口として、コドモンヘルプセンターを設置しています。

なお、本サービスに保存された情報の所在は日本国内となります。

**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**  
利用規約にてサービス内容を明示し、サービス提供を実施しています。  
また、責任分界については、6.1.1 を参照ください。

## 7.2.2 情報セキュリティの意識向上、教育および訓練（管理策 6.3）

当社では情報セキュリティ基本方針およびクラウドセキュリティ基本方針を定め、方針に従いサービスを運営しています。  
また、クラウドサービスカスタマデータおよびクラウドサービス派生データを取り扱う社員に対して定期的な教育、訓練を実施しています。  
委託先等にも同様の教育、訓練の実施を要求しています。

### A.8.1.1 資産目録（管理策 5.9）

お客様の登録情報および記録、弊社がサービスを運営するための情報は、資産管理上において明確に分離して管理しています。  
また、クラウドサービスカスタマデータおよびクラウドサービス派生データの識別を実施しています。

### CLD.8.1.5 クラウドサービスカスタマの資産の除去

本サービスの利用契約終了後は、各種データが第三者の利用に供されることのないよう、利用規約に従い、当社にて本サービス内のデータを消去いたします。  
本サービス自体の終息時には、データを完全消去した上でリソースの削除、または停止、廃棄を行います。

### A.8.2.2 情報のラベル付け（管理策 5.13）

お客様の登録情報および記録は、サービスログイン後に確認できます。  
利用方法に関しては、コドモンヘルプセンターをご確認ください。

### A.9.2.1 利用者登録および登録削除（管理策 5.16）

お客様の会社情報の登録、変更、削除は弊社にて登録し提供しています。  
利用方法に関しては、コドモンヘルプセンターをご確認ください。

### A.9.2.2 利用者アクセスの提供（provisioning）（管理策 5.18）

サービスログインは、お申込み受理後に発行されたユーザーID およびお客様が設定したパスワードでアクセスができます。  
利用方法に関しては、コドモンヘルプセンターをご確認ください。

#### A.9.2.3 特権的アクセス権の管理（管理策 8.2）

サービスログインには、強固なパスワードポリシー（大小英数記号混在 10 桁以上）を推奨しています。

#### A.9.2.4 利用者の秘密認証情報の管理（管理策 5.17）

サービスログインに使用されるパスワード変更、削除、再発行方法につきましてはコドモンヘルプセンターをご確認ください。

#### A.9.4.1 情報へのアクセス制限（管理策 8.3）

本サービスでは、アクセス制御機能を提供しています。

利用方法に関しては、コドモンヘルプセンターをご確認ください。

#### A.9.4.4 特権的なユーティリティプログラムの使用（管理策 8.18）

本サービス機能以外の利用を可能とするユーティリティプログラムの提供は行っておりません。

#### CLD.9.5.1 仮想コンピューティング環境における分離

本サービス内のデータはお客さま毎に論理的に分離し、制御しています。

#### CLD.9.5.2 仮想マシンの要塞化

サービスが稼働しているサーバは、不要な設定機能やポートは閉じ、マルウェア対策やログ取得を行っています。

仮想マシンは、導入時に当社基準の要件に基づき、要塞化されたシステムのみを利用しておられます。

#### A.10.1.1 暗号による管理策の利用方針（管理策 8.24）

お客さまの登録情報および記録のデータは SSL 暗号化通信によりサーバまで伝送されています。

詳細は、3-3 クラウド品質保証(SLA)をご確認ください。

#### A.11.2.7 装置のセキュリティを保った処分又は再利用（管理策 7.14）

設備および装置を再利用、廃棄する際には適切なプロセスで、資源の削除や設備および装置の破壊を実施しています。

#### A.12.1.2 変更管理（管理策 8.32）

システム変更およびアップデートを実施する際にお客さま影響がある場合、利用規約に基づき通知します。

#### A.12.1.3 容量・能力の管理（管理策 8.6）

サイトアクセス量を監視し、アクセス量に耐えられない場合はオートスケールにて増強するよう対策しています。

#### CLD.12.1.5 実務管理者の運用のセキュリティ

本サービスの機能別の操作手順は、コドモンヘルプセンターをご確認ください。

#### A.12.3.1 情報のバックアップ（管理策 8.13）

バックアップは1日4回取得しており、各バックアップデータは最低2週間保存されます。

#### A.12.4.1 イベントログ取得（管理策 8.15）

アクセスログ、アプリケーションログ、監査ログを保有しています。

お客様のご要望に応じて、ログ開示を判断します。

#### A.12.4.4 クロックの同期（管理策 8.17）

本サービスはNTPによる時刻同期を行っており、日本時間（JST）で管理しています。

本サービスで記録される時刻は、すべて時刻同期に基づいて記録しています。

#### CLD.12.4.5 クラウドサービスの監視

本サービスに対する不正アクセスについて監視を実施しています。

正常な動作をしていなかったことなど、本サービスに障害がある場合は、お客様に通知の上対応することがあります。

#### A.12.6.1 技術的ぜい弱性の管理（管理策 8.8）

当社では、適宜技術的ぜい弱性情報を各所から収集しております。

本サービスに影響し緊急性が高い場合は、メールで脆弱性情報を含めたりリース情報を公開します。

#### A.13.1.3 ネットワークの分離（管理策 8.22）

お客様のアクセスできる領域は他のお客さまと論理的に分離しています。

#### CLD.13.1.4 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

ネットワークトラブルを防止するため、情報セキュリティ基本方針およびクラウドセキュリティ基本方針に基づき、仮想および物理ネットワークの設定方針を定めています。

#### A.14.1.1 情報セキュリティ要求事項の分析および仕様化（管理策 5.8）

本サービスのご利用に必要となる技術的な仕様、手順についてはお客様とのご契約時にマ

ニュアルなどをご提供しています。

#### A.14.2.1 セキュリティに配慮した開発の方針（管理策 8.25）

情報セキュリティ基本方針およびクラウドセキュリティ基本方針に基づき、変更管理に関するプロセスを定めてサービス開発・運営を実施しています。  
変更管理プロセスでは、弊社内部手順に基づき、サービスリリースしています。  
また、定期的に脆弱性診断を実施する方針を定めています。

#### A.15.1.2 供給者との合意におけるセキュリティの取扱い（管理策 5.20）

本サービスは、AWS を基に構築しており、AWS との契約によって、役割および責任を明確化しています。  
また情報セキュリティ対策も A.6.1.1 の範囲において必要なセキュリティ対策を実施しています。

#### A.15.1.3 ICT サプライチェーン（管理策 5.21）

本サービスでは、ピアクラウドサービスプロバイダは利用していません。

#### A.16.1.1 責任および手順（管理策 5.24）

お客さまに影響のある情報セキュリティインシデントが発生した場合には、お客さま専用の管理画面やサービスサイト上、個別メールなどにて速やかに報告します。

#### A.16.1.2 情報セキュリティ事象の報告（管理策 6.8）

お客さまが本サービス上の情報セキュリティ事象を発見された場合、又は情報セキュリティ事象が発生した場合は、コドモンヘルプセンターからご連絡お願い致します。  
当社が確認した情報セキュリティ事象については、その内容・状況に応じて、コドモンヘルプセンターを通じてお客さまに通知します。

#### A.16.1.7 証拠の収集（管理策 5.28）

情報セキュリティ事象の証拠を保全するため、当社で必要な手順を定めています。  
本サービスにおけるログなどは、原則開示しておりませんが、ご依頼をいただいた場合、内容を精査した上で開示します。

#### A.18.1.1 適用法令および契約上の要求事項の特定（管理策 5.31）

本サービスのサービス設備は日本国内に設置しています。  
当社においての法的準拠については、コンプライアンス担当を設定し、管理を行っております。本サービスをご利用にあたり、当社と契約者の間で訴訟の必要が生じた場合、東京簡易裁判所または東京地方裁判所を第一審の専属的合意管轄裁判所となります。

**A.18.1.2 知的財産権（管理策 5.32）**

本サービスにおける苦情などにおいては、コドモンヘルプセンターをご確認ください。

また、本サービスで使用している他社商標については、3-7 他社商標についてご確認ください。

**A.18.1.3 記録の保護（管理策 5.33）**

お客様の登録情報および記録は、利用規約に基づき保管しています。

**A.18.1.5 暗号化機能に対する規制（管理策 5.31）**

本サービスで利用している暗号情報は、3-3 クラウド品質保証（SLA）をご確認ください。

**A.18.2.1 情報セキュリティの独立したレビュー（管理策 5.35）**

お客様に安心のセキュリティをご提供できるように、組織的な取り組みとして、当社では ISMS および ISMS クラウドセキュリティ認証を取得しており、認証機関からの審査を受審しております。

以上