White Paper

Decidim サービスの ISO/IEC27017 に基づくセキュリティ要求事項への取り組み

第 1.2 版

2023 年 8 月 31 日

一般社団法人　コード・フォー・ジャパン

Code for Japan

更新履歴

版数	日付	更新内容
第 1.0 版	2021 年 10 月 7 日	初版
第 1.1 版	2021 年 11 月 30 日	認証取得に伴い、A18.2.1 の記載を変更
第 1.2 版	2023 年 8 月 31 日	問い合わせ先メールアドレスを変更

目次

1. はじめに

1.1. White Paper の目的

本ドキュメントは、Decidim の提供にあたり、当社およびサービスのセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

1.2. White Paper の対象

Decidim の導入を検討中の方、及び Decidim を利用中の方を想定しています。

1.3. ISO/IEC27001,27017 の管理策との対応

各項目の【】内は、ISO/IEC 27001、及び ISO/IEC 27017 の管理策の対応項番を記載しています。

2. 情報セキュリティの組織とサービスの責任範囲

2.1. クラウドコンピューティングのための情報セキュリティ方針【A.5.1.1】

当社では、クラウドコンピューティングに関する情報セキュリティの方針を定め、ユーザ様に満足いただける機能的でセキュアなサービスの提供を目指しています。

クラウドコンピューティングに関する情報セキュリティ方針
当社は、クラウドコンピューティング環境におけるユーザ様の情報資産を情報セキュリティ上の脅威から保護するための措置を講じ、ユーザ様が安心してご利用いただけるセキュアなサービスを提供します。

当社の「情報セキュリティ方針」は以下の URL からご確認頂けます。
https://www.code4japan.org/security

2.2. 情報セキュリティ組織 【A.6.1.1】

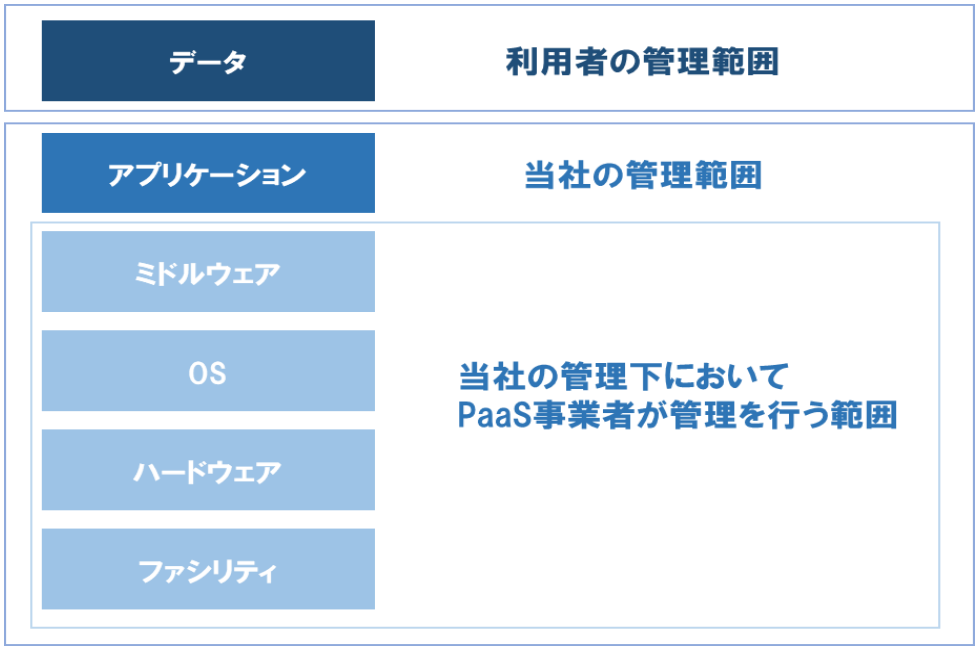
当社では、情報セキュリティに関する統括責任者を任命し、情報セキュリティに関する統括責任と権限を与えています。また、情報セキュリティ委員会を設置し、情報セキュリティのマネジメントシステムの運用と継続的改善に取り組んでいます。

2.3. 地理的所在地【A.6.1.3】

当社の所在地、並びに当社がユーザ様のデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにユーザ様のデータを保存する必要性が生じた場合、ユーザ様に事前に通知したうえで行います。

2.4. 責任範囲（共有 Model）【A.6.1.1, CLD.6.3.1】

仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。
また、当社は、基盤上に構築したアプリケーションに対して責任を負います。
アプリケーション上のデータについては、ユーザ様の責任において保護していただく必要があります。



［当社の責任］

・Decidim のセキュリティ対策

［ユーザ様の責任］

・利用者アカウントの管理（登録、削除、権限設定、管理者設定、アクセス権の設定など）

・パスワード等の利用者の秘密認証情報の管理

・ユーザ様が取扱うデータに対してのバックアップ

2.5. 情報セキュリティの意識向上，教育及び訓練 【A.7.2.2】

当社は、全従業員に対する定期的な情報セキュリティ教育を実施し、情報セキュリティに対する意識向上に努めています。

2.6. 情報セキュリティの独立したレビュー【A.18.2.1】

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。

2.7. インシデント対応プロセス 【A.16.1.1】

当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する手順が文書化され、情報セキュリティ委員会により管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

3. 開発/調達

3.1. 開発プロセス【A.14.2.1】

当社のクラウドサービスは、情報セキュリティについても配慮することを方針として開発し、承認プロセスを経たうえでリリースされます。
また、リリース前のみならず、リリース後も定期的な脆弱性診断を行っています。

3.2. サプライチェーン【A.15.1.3】

当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

4. アプリケーションのセキュリティ機能

4.1. 情報のラベル付け 【A.8.2.2】

Decidim は、コンポーネント機能により、ユーザ様のデータの分類をサポートします。使用方法の詳細は「Decidim マニュアル」をご参照ください。

4.2. 利用者アクセスの管理 【A.9.2.1, A.9.2.2】

Decidim は、ユーザ様がストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。ユーザ様は管理者画面から簡単な操作によりアカウント登録・削除を行い、また利用者に対する権限の割り当てを行うことが出来ます。使用方法の詳細は「Decidim マニュアル」をご参照ください。

4.3. 認証情報の管理 【A.9.2.3, A.9.2.4】

初期のアカウント登録手順は「Decidim マニュアル」をご参照ください。アカウントの登録が完了すると、登録したメールアドレスに対し、アカウント有効化のメールが届きますので、画面の指示に従い有効化を行っていただきます。

パスワードの設定はユーザ様のセキュリティポリシーにもとづいて実施してください。管理者権限はユーザ様のセキュリティポリシーに従い厳重に管理することをお願いします。

4.4. ユーティリティプログラム【A.9.2.3, A.9.4.4】

ユーティリティプログラムは管理者権限に限定して利用可能です。管理者権限を厳重に管理することによりユーティリティプログラムの使用制限につながります。

4.5. 暗号化 【A.10.1.1】

Decidim とユーザ様との間での通信は、SSL/TLS で暗号化し、情報の盗聴等のリスクに対処しています。

データベースに保管されるユーザ様データについては、パスワードはハッシュ化し安全に管理されるとともに、データベースへのアクセス権限を多要素認証を含めたセキュリティグループによって厳格に管理しています。これにより、クラウドサービスカスタマの定めるポリシーと相まって、必要なセキュリティ保護を実施していただくことが可能になっています。

5. 運用

5.1. 変更【A.12.1.2】

ユーザ様に影響を与える Decidim の変更は、ご登録頂いたメールアドレス宛に事前通知します。

5.2. 管理者用手順 【CLD.12.1.5】

「Decidim マニュアル」等の各種マニュアルの提供に加え、ユーザ様からの QA サポートを提供しています。
当社の担当までご相談ください。

5.3. バックアップ【A.12.3.1】

システム及びユーザ様データのバックアップは、日次で 3 世代分のデータを保持します。
ただし、ユーザ様からのバックアップデータの復元等に関するご要望には対応していません。

5.4. ログ【A.12.4.1】

Decidim の維持管理に必要となる適切なログを取得しています。
1 つは管理ダッシュボード上での「管理者アクティビティ」になります。これは Decidim のユーザ情報へのアクセス、その他コンテンツ変更に対するログになります。
もう 1 つは、基盤として利用するクラウドサービス上の各種リソースログ、アクセスログです。

5.5. クロックの同期 【A.12.4.4】

Decidim は、基盤として利用するクラウドサービス事業者が提供する時刻同期サービスを利用し同期を行っています。
ログは、日本標準時（UTC+9）で提供されます。

5.6. クラウドサービスの監視 【A.12.4.5】

Decidim の運用状況（登録者数、コメント状況、アクセスログ）に関する報告をユーザ様に定期的に提供します。

5.7. 技術的脆弱性の管理 【A.12.6.1】

脆弱性情報は、Decidim 本家をはじめ、構成するソフトウェアそれぞれのコミュニティ情報を収集しています。基盤として利用するクラウドサービスによるパッケージ管理がされているものについては、当該クラウドサービスが対応しています。

5.8. ネットワーク 【A.13.1.3】

Decidim は、ネットワークの仮想化技術を利用して、他のユーザ様とのネットワークの分離を適切に行っています。

また、ユーザ様に提供するクラウドコンピューティング環境と、当社の管理用環境を別セグメントとして分離しています。

5.9. 容量・能力の管理【A.12.1.3】

当社は、サーバリソース、及びネットワークリソースを監視しています。またリソースの増減は GUI から瞬時に実行することができます。サーバリソースはインスタンスの構成を変更せずにスケールアップによることを原則としていますが、将来的なニーズに照らして、必要があればスケールアウトによる対応も行います。

5.10. 負荷分散/冗長化【A.17.2.1】

Decidim は基盤を提供するクラウドサービス事業者のマネジメントサービスを使用し、複数の仮想サーバに処理を振り分ける、ロードバランバランシングを採用しています。
また、アプリケーションの構成はマシンイメージとして保存し、即時に複製が可能な状態を整えています。

5.11. インシデント対応 【A.16.1.1】

Decidim に関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

項目	内容
報告する範囲	データの消失、長時間のシステム停止等のユーザ様に大きな影響を及ぼす可能性のある情報セキュリティインシデント
対応の開示レベル	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、すべて同等のレベルで対処します。
通知を行う目標時間	検知から 72 時間以内を目標に通知します。
通知手順	ご登録頂いたメールアドレス宛 （必用に応じて電話等の手段を使用する場合もあります。）
問合せ窓口	当社の担当
適用可能な対処	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、あらゆる手段を講じて対処します。

また、ユーザ様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、Decidim の当社の担当にご連絡ください。

5.12. サービス利用停止後のデータの扱い【CLD.8.1.5】

Decidim で利用者様が作成・保存した利用者様のデータの除去に関しては、年１回３月末に完全に消去いたします。また、個別の契約で定める事も可能性です。ただし、利用者様のデータを含まないサービス共通のログデータは消去の対象外になります。

5.13. 装置のセキュリティを保った処分又は再利用【A.11.2.7】

装置の処分又は再利用については、当社の管理下で基盤として利用するクラウドサービス事業者の対応によります。

6. その他

6.1. 証拠の収集【A.16.1.7】

法令また権限のある官公庁からの要求により Decidim 上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。合意について別途、利用規約をご参照ください。

6.2. 適用法令及び契約上の要求事項【A.18.1.1】

利用契約に関する準拠法は、日本法とします。別途、利用規約をご参照ください。

6.3. 知的財産権【A.18.1.2】

Decidim のソフトウェアのライセンスは、AGPLv3、画像やフォント等については CC BY-SA 4.0、Decidim コミュニティで集めたデータのライセンスは Open Data Commons Open Database License に該当します。

Decidim のデータベース上の知的財産権の詳細については、個別の契約・利用規約をご参照ください。

6.4. 記録の保護 【A.18.1.3】

アプリケーションにおけるデータ操作等のログはユーザ様にて保護して頂く必要があります。当社は、仮想ネットワークへのアクセスに関するログ、及びサービスのバージョンアップに関する内部要員による作業ログを一定期間保存します。

6.5. 暗号化機能に対する規制 【A.18.1.5】

Decidim において暗号化の規制対象になる地域にはサービスを提供していません。

7. Decidim に関するお問い合わせ

以下までお問い合わせください。

問い合わせ窓口：decidim@code4japan.org

以　上