セキュリティホワイトペーパー

「クラウド型医薬品在庫管理システム」の ISO/IEC27017 に基づく セキュリティ要求事項への取り組み

KATABAMI
MANAGEMENT
SERVICE.CO.,Ltd.

カタバミ・マネジメント・サービス株式会社

第１版

2023 年９月１日

はじめに

組織におけるクラウドサービスの利用において、セキュリティへの懸念は必ず取り上げられる問題の１つです。

そのような状況の中、2015 年 12 月にクラウドセキュリティの国際標準規格である ISO/IEC27017 が発行され、クラウドサービスの利用者と事業者が行うべきセキュリティ管理策が定義されました。

本書では、カタバミ・マネジメント・サービスが提供する「クラウド型医薬品在庫管理システム」（以下、「本サービス」）における ISO/IEC27017（以下、「ISO27017」）への取り組みを解説します。

本書で、本サービスにおけるクラウドセキュリティの取り組みを知っていただき、本サービスをご活用いただくことで、今後ますますお客様のお役に立ちたいと考えています。

なお、本書の内容は作成時点での取り組みに基づいて記述しております。内容は変更される場合がございますので、最新の情報は弊社へご確認くださいますようお願い致します。

サービスの概要

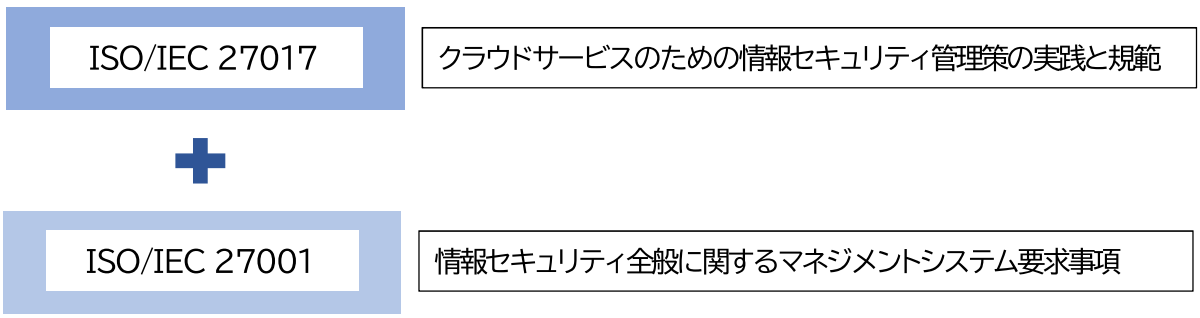
本サービスは、調剤薬局及び医療機関向けの医薬品在庫管理システムです。オンラインによる発注、入荷、患者様の来局予測、薬の有効期限管理、棚卸などにお役立ていただけるサービスです。

ISO27017 の概要

国際標準化機構（ISO）と国際電気標準会議（IEC）が定める情報セキュリティマネジメントの国際規格に ISO/IEC27000 シリーズがあります。

ISO27017 は、このシリーズの1つで、2015 年 12 月に発行されたクラウドサービスにおける情報セキュリティマネジメントのガイドライン規格です。

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である ISO27001 の取り組みを ISO27017 で強化することにより、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することができます。



1. 情報セキュリティのための方針群

1.1.情報セキュリティのための方針群(ISO27017 項番:5.1.1)

弊社の情報セキュリティ方針に従い、本サービスをセキュリティに関してきわめて重要な事項として取り扱い、サービス運用を行います。

弊社の情報セキュリティ基本方針については

https://www.katabami-management.com/security/をご覧ください。

また、クラウドサービスの提供にあたり、お客様の情報セキュリティについての要求を満たすため、次の事項を考慮します。

- クラウドサービスの設計及び実装に適用する情報セキュリティ要求事項
- 認可された内部関係者からのリスク
- マルチテナンシ及びクラウドサービスカスタマ(お客様)の隔離(仮想化を含む。)
- 弊社社員によるクラウドサービスカスタマ(お客様)の資産へのアクセス
- アクセス制御手順
- 変更管理におけるクラウドサービスカスタマ(お客様)への通知
- 仮想化セキュリティ
- クラウドサービスカスタマ(お客様)データへのアクセス及び保護
- クラウドサービスカスタマ(お客様)のアカウントのライフサイクル管理
- 違反の通知、並びに調査及びフォレンジック(forensics)を支援するための情報共有指針

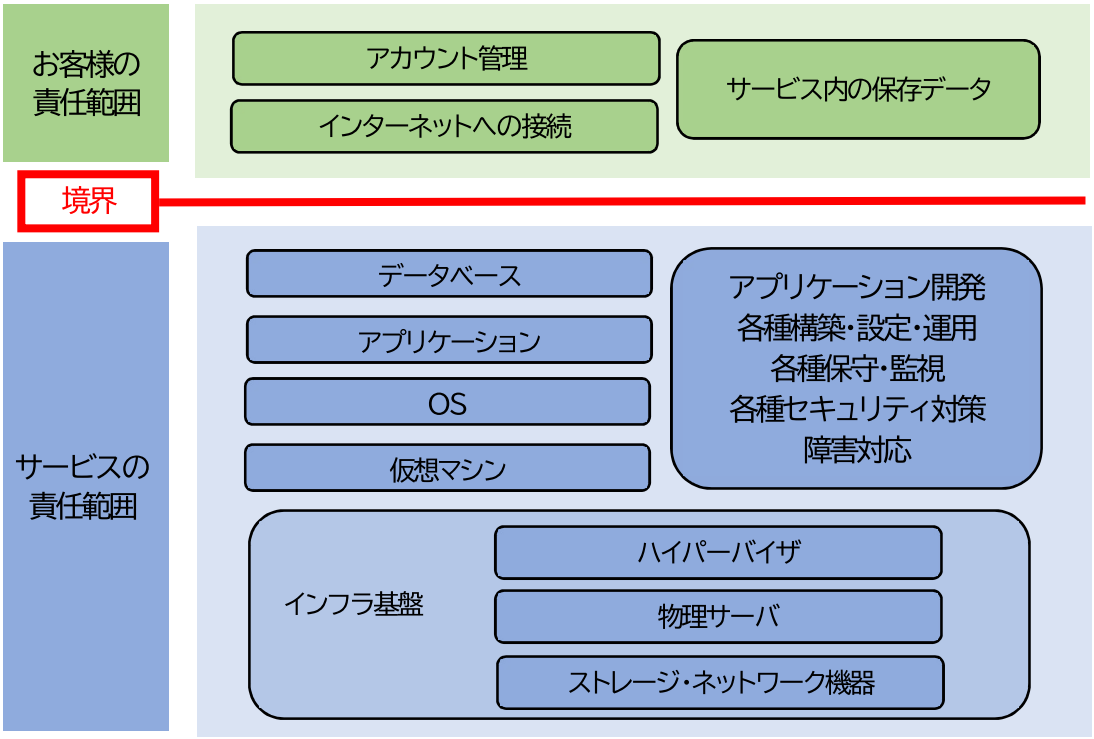
弊社のクラウドセキュリティ基本方針については

https://www.katabami-management.com/cloudsecurity/をご覧ください。

2. 情報セキュリティのための組織

2.1.情報セキュリティの役割及び責任(ISO27017 項番:5.1.1)

本サービスの責任の分界点は、下記の通りとなります。



【お客様の責任】

ご利用者様は、以下のセキュリティ対策を実施する必要があります。

- アカウント(利用ユーザー)の適切な管理(登録、削除、各種管理権限の付与など)
- パスワードの適切な管理
- サービスにアクセスするインターネットへの接続の管理
- サービス内の保存データの適切な管理

【カタバミ・マネジメント・サービス株式会社の責任】

- サービスのインフラ基盤の管理(※1)
- サービスの提供に利用する OS、アプリケーション、データベースの管理
- サービスの提供に利用するアプリケーション開発、各種構築・設定・運用及び各種保守・監視
- サービスの提供に利用する OS、アプリケーション、データベース、その他インフラ等のセキュリティ対策及び障害管理

※1:本サービスのでは、ISO/IEC 20000-1 、ISO/IEC 27001 、ISO/IEC 27017 を適用したマネジメントシステムを構築し、情報セキュリティ対策に取り組んでいる国内データセンターのインフラ基盤を利用しています。インフラ基盤の仕様、運用は、利用するデータセンターに依存しているため、データセンターの保守、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、脅威が生じた場合、サービスに影響が及ぶある場合があります。

本サービスに関するデータセンターについての詳しい情報は、弊社までお問い合わせください。

2.2.関係当局との連絡(ISO27017 項番:6.1.1)

弊社の本店所在地は、長野県松本市双葉 8 番 10 号となります。なお、本サービスに保存された情報の所在は日本国内で、日本法を準拠法として、日本国内においてサービスを提供しています。

2.3.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(ISO27017 項番:CLD.6.3.1)

「クラウド型医薬品在庫管理システム使用契約書」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。また、責任分界点の詳細は、“2.1. 情報セキュリティの役割及び責任”をご参照ください。

3. 人的資源のセキュリティ

3.1.情報セキュリティの意識向上、教育及び訓練(ISO27017 項番:7.2.2)

弊社では情報セキュリティ基本方針

https://www.katabami-management.com/security/

及びクラウドセキュリティ基本方針

https://www.katabami-management.com/cloudsecurity/

を定め、方針に従いサービスを提供しています。

また、クラウドサービスカスタマデータ及びクラウドサービス派生データを取り扱う社員に対する定期的な教育を実施しています。

4. 資産の管理

4.1.資産目録(ISO27017 項番:8.1.1)

お客様の情報資産(お客様にて保存されるデータ)と弊社がサービスを運営する為の情報は、明確に分離しています。

4.2.クラウドサービスカスタマの資産の除去(ISO27017 項番:CLD8.1.5)

本サービスに関するお客様のデータは、契約終了後、180 日以内にデータが復元できない形で削除されます。

4.3.情報のラベル付け(ISO27017 項番:8.2.2)

情報のラベル付け機能の提供は行っていません。

5. アクセス制御

5.1.利用者登録及びネットワークへのアクセス(ISO27017 項番:9.2.1)

お客様専用画面にて、ご利用者様の権限(管理者、一般、制限ユーザー)の登録・変更・停止機能を提供しています。

登録・変更・停止に必要な手順は、「ユーザーマニュアル」に記載しています。

5.2.利用者アクセスの提供(ISO27017 項番:9.2.2)

お客様専用画面は、本サービスのお申込み受理後に発行されたコード、ログイン ID、パスワードでアクセスすることができます。

本サービスに関する利用者権限ごとのアクセス可能範囲及び行使できる権限は、「ユーザーマニュアル」に記載しています。

5.3.特権的アクセス権の管理(ISO27017 項番:9.2.3)

お客様専用画面は、登録者のみが知りえるコード、ログイン ID、パスワードでアクセスできます。

5.4.利用者の秘密認証情報の管理(ISO27017 項番:9.2.4)

お客様専用画面にて、利用される際のパスワードの変更機能を提供しています。

パスワード変更に必要な手順は、「ユーザーマニュアル」に記載しています。

パスワードを忘れた場合は、販売代理店にご連絡ください。

5.5 情報へのアクセス権限(ISO27017 項番:9.4.1)

お客様専用画面は、コード、ログイン ID、パスワードでアクセスできます。

5.6 特権的ユーティリティプログラムの使用(ISO27017 項番:9.4.4)

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ユーティリティプログラムの提供は行っていません。

5.7 仮想コンピューティング環境における分離(ISO27017 項番:CDL.9.5.1)

お客様間のデータの分離は、ソフトウェアにて適切に制御しています。

5.8 仮想マシンの要塞化(ISO27017 項番:CDL.9.5.2)

ファイアウォールによる通信のブロック、不要なポートの閉鎖、アンチウィルスソフトの導入を実施しています。

6. 暗号

6.1.暗号による管理策の利用方針(ISO27017 項番:10.1.1)

・通信

お客様と本サービスとの通信は、暗号化しています。

・保存データ

個人を特定できるデータは、暗号化しています。

7. 物理的及び環境的セキュリティ

7.1.装置のセキュリティを保った処分又は再利用(ISO27017 項番:11.2.7)

本サービスに関する装置を再利用、廃棄する際には適切なプロセスで、保存データの削除や装置の破壊を実施いたします。

8. 運用のセキュリティ

8.1.変更管理(ISO27017 項番:12.1.2)

本サービスに関するサービスのバージョンアップ情報を始めとした、各種変更情報やメンテナンスによる停止に関する情報は、ログイン後の「新着情報」にて閲覧することが可能です。

また、緊急のお知らせ等については、弊社から一斉 FAX にてお客様にご連絡いたします。

8.2.容量・能力の管理(ISO27017 項番:12.1.3)

本サービスに関するリソースの使用量及び稼働状況等を管理し、安定したサービスを提供できる仕組みを構築しています。

8.3.実務管理者の運用のセキュリティ(ISO27017 項番:CLD. 12.1.5)

本サービスに関するサービスの操作手順は、「ユーザーマニュアル」に記載し、提供しています。

8.4.情報のバックアップ(ISO27017 項番:12.3.1)

日次でデータベースのバックアップを実施し、データバックアップ専用ストレージに 2 世代分を保管しています。また、遠隔地に 3 世代保管しています。

8.5.イベントログの取得(ISO27017 項番:12.4.1)

お客様の求めに応じて、操作ログ等を提供することができます。

本サービスに関する操作ログ等についてのお問い合わせは、ログイン後の「サポート」に表示される電話番号までご連絡ください。

8.6.クロックの同期(ISO27017 項番:12.4.4)

本サービスが稼働するサーバの時刻は、国立研究開発法人情報通信研究機構の日本標準時プロジェクトサイトと同期をしております。本サービスに記録される時刻は、すべてこの時刻同期に基づいています。

8.7.クラウドサービスの監視(ISO27017 項番:CDL. 12.4.5)

本サービスに障害(ネットワーク障害を除く)が発生した場合は、その旨がアクセス画面に表示されます。

8.8.技術的ぜい弱性の管理(ISO27017 項番:12.6.1)

独立行政法人情報処理推進機構(IPA)の脆弱性情報を確認し、重要度や技術情報、影響を検討して、適宜更新プログラムを適用しています。

9. 通信のセキュリティ

9.1.ネットワークの分離(ISO27017 項番:13.1.3)

お客様がアクセスするネットワークと弊社運用担当者が利用するネットワークは分離しています。

また、お客様間のデータの分離は、ソフトウェアにて適切に制御しています。

9.2.仮想及び物理ネットワークのセキュリティ管理の整合(ISO27017 項番:

CDL13.1.4)

仮想ネットワークは利用しておりません。

10. システムの取得、開発及び保守

10.1.情報セキュリティ要求事項の分析及び仕様(ISO27017 項番:14.1.1)

情報セキュリティ基本方針、クラウドセキュリティ基本方針、本ホワイトペーパーに定めています。

10.2.情報セキュリティに配慮した開発のための方針(ISO27017 項番:14.2.1)

IPA「安全な Web サイトの作り方」を参考に、情報セキュリティに配慮した開発を行っています。

11. 供給者関係

11.1.供給者との合意におけるセキュリティの取扱い(ISO27017 項番 15.1.2)

本サービスはクラウドサービスです。責任分界点は、“2.1.情報セキュリティの役割および責任”を参照してください。

また、情報セキュリティ対策については、“2.1.情報セキュリティの役割および責任”の範囲において必要な対策を実施しています。

11.2.ICT サプライチェーン(ISO27017 項番 15.1.3)

本サービスのインフラ基盤は、SO/IEC 20000-1 、ISO/IEC 27001 、ISO/IEC 27017 を適用したマネジメントシステムを構築し、情報セキュリティ対策に取り組んでいる国内データセンターを利用しています。

本サービスに関するデータセンターについての詳しい情報は、弊社までお問い合わせください。

12. 情報セキュリティインシデント管理

12.1.責任及び手順(ISO27017 項番 16.1.1)

弊社の責任範囲である、契約情報やお客様に影響のあるサービス運営上の派生データ等に関する情報セキュリティインシデントが発生した場合には、ログイン後の「新着情報」にて閲覧することが可能です。

また、緊急の障害等については、当社から一斉 FAX にてお客様にご連絡いたします。

本サービスに関するお客様からの事象報告は、ログイン後の「サポート」に表示される電話番号までご連絡ください。

12.2.情報セキュリティ事象の報告(ISO27017 項番 16.1.2)

弊社の責任範囲である、契約情報やお客様に影響のあるサービス運営上の派生データ等に関する情報セキュリティインシデントが発生した場合には、ログイン後の「新着情報」にて閲覧することが可能です。

また、緊急の障害等については、当社から一斉 FAX にてお客様にご連絡いたします。

本サービスに関するお客様からの情報セキュリティ事象の報告は、ログイン後の「サポート」に表示される電話番号までご連絡ください。

12.3.証拠の収集(ISO27017　項番 16.1.7)

情報セキュリティインシデントに関するログ等の証拠の収集は、お客様の要望に応じて個別に対応しております。

本サービスに関する情報セキュリティインシデントに関するログ等のお問い合わせは、ログイン後の「サポート」に表示される電話番号までご連絡ください。

なお、弊社は、業務遂行上知り得た情報やお客様のデータを第三者に開示、提供しません。ただし、法令に基づく場合を除きます。

13. 順守

13.1.適用法令及び契約上の要求事項の特定(ISO27017　項番 18.1.1)

本サービスが稼働する設備は、日本国内に設置しており、日本法を準拠法とします。本サービスのご利用にあたり、弊社と契約者の間で訴訟の必要が生じた場合、被告となる当事者の本店所在地を管轄する地方裁判所を第一審の専属的合意管轄裁判所とします。

13.2.知的財産権(ISO27017　項番 18.1.2)

本サービスに関する知的財産権についてのお問い合わせは、ログイン後の「サポート」に表示される電話番号までご連絡ください。

13.3.記録の保護(ISO27017　項番 18.1.3)

本サービスに関する記録に関するお問い合わせは、ログイン後の「サポート」に表示される電話番号までご連絡ください。

13.4.暗号化機能に対する規制(ISO27017　項番 18.1.5)

本サービスは、日本国内でサービス提供しており、輸出規制の対象となる暗号化の利用はありません。

13.5.情報セキュリティの独立したレビュー(ISO27017　項番 18.2.1)

弊社の組織的な情報セキュリティの取り組みとして、情報セキュリティマネジメントシステムである ISO27001 の認証を取得しています。