飲みきるミカタ　セキュリティ対策に関する情報

2023/08/30 作成

金融庁 「政府機関・地方公共団体等における業務での LINE 利用状況調査を踏まえた今後の LINE サービス等の利用の際の考え方（ガイドライン）」の一部改正について、を参考に作成。 https://www.fsa.go.jp/news/r2/sonota/20210611/20210611.html		
	質問	回答
データの所在・カントリーリスク・責任分界点など		
1	サービス上のデータの所在地は日本国内に限定されているか。	日本国内に限定されています。
2	準拠法・裁判管轄は、日本国内に指定可能か。	日本国内に指定可能です。
3	支援者あるいは患者の登録・入力データ所有権・管理権はどこにあるか。	基本的に患者のデータは患者のものであり、患者のみが削除でき、支援者登録は支援者のみが削除できます。
4	支援者リストの患者について、治療終了などでリストから削除する時、どのような方法が可能か。	支援者リストの整理が必要となった時、患者にデータの連結を外すことをお伝えいただき、飲みきるミカタの患者の設定画面の支援者メールアドレスを削除することで支援者リストから削除できます。
5	保健所からの求めに応じ患者データの消去が可能であるか。	患者の死亡等で患者データの削除を研究所に求める場合、患者のメールアドレスを示して頂き、こちらで削除の作業を行います。
6	システム利用者（患者と支援者）以外が、データの内容を閲覧可能か。（やりとりの内容などを本市以外から確認可能か）	利用している患者とデータが連結されている支援者以外は、観覧不可です。
7	利用に当たって、セキュリティ保護に関する安全管理について、行政などの支援者が責任を負うべき内容は、どこからになるか。	こちらは支援者側の IT システム利用ポリシーで決まるもので、一般には利用可能な範囲が責任範囲になります。 支援者アカウントの運用及びそれによって閲覧可能な情報、ダウンロードデータを支援者側の適切な IT セキュリティポリシーにより活用いただきます。
その他		
8	個人情報を守る方策	飲みきるミカタを利用するにあたり、個人情報となりうるのは、患者名と患者のメールアドレスとなりますので、氏名の登録をニックネームとする、登録するメールアドレスを Gmail 等のフリーメールで作成し、システムの利用終了後は削除するなどの方策も、ご検討ください。

外部サービス選定要件（これまでに回答した要件）		
9	インシデント対処（必須） 情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について整備していること。	開発会社の社内規定で明文化されています。
10	監査等・改善（必須） 情報セキュリティ管理状況その他契約の履行状況を確認する方法（監査の受け入れ、外部監査・認証機関等による報告・認証結果等の公表等）が提示されていること。障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示されていること。	開発会社の社内規定で明文化されています。
11	サービス移行（任意） サービス中断時等の復旧要件・データ移行方法等の検討に必要な情報（目標復旧時間、バックアップサイトへのアクセス手段等）を確保できること。	確保可能です。
12	SLA （Service Level Agreement:サービスの品質や保証．条件等の合意書）（任意） サービスレベルの保証が定められていること。	サービスごとに必要な SLA を締結可能です。
外部サービスにおけるセキュリティ対策		
13	利用者認証（必須） 利用者のログインに関して適切な本人確認が実施できること。 管理者として保守・更新等に係るアクセスをする場合は、不正接続を防止するため認証を徹底すること。（例：ワンタイムパスワードの併用、多要素認証、電子証明書、接続元 IP 制限等）	利用者の本人確認を実施しています。 また、管理業務でアクセスするに際しては、社内ネットワークのみから SSH 接続が可能です。（接続元 IP 制限）

14	アクセス制御（任意、一部必須） データ又は保存領域（アカウント、階層構造等）において、適切な権限管理及びアクセス制御機能が提供されていること。	アクセス制御機能が提供されています。
15	保存データ保護（任意） 機密情報について暗号化等によって適切に保存データを保護できること。	必要に応じて実施可能です。
16	メンテナンス・障害時対処（任意） メンテナンスや障害等、サービスの停止が発生した場合における対処として、サブサイト等の冗長化対応、データのバックアップと復旧方法の整備、及び利用者に対する情報提供方法が確立されている。	メンテナンス・障害時対処方法が確立しています。
17	ログ管理（必須） 外部サービスに係るアクセスログが適切に取得・管理され、侵害発生時に証跡調査等の対応が適切に実施できること。 利用者側が外部サービス提供者に侵害発生時に調査に必要なログを要求できる、調査ツールがある又は調査を要求することが可能であること。	アクセスログが取得され、過去１か月のログが保存されています。
18	不正プログラム対策（必須） マルウェア対策を適切に講じていること。	マルウェア対策を講じています。
19	データ廃棄（必須） データを復元できないように消去を行い、データを消去・廃棄を適切に行った証明書を提示すること。証明書の発行ができない場合、約款において適切なデータ消去処理を宣言し、かつ、外部サービス提供者がデータ消去の規定を含むISMS認証（ISO/IEC 27001）もしくは同等以上の措置・認証（CSゴールドマークやSOC報告書等）を受けていること。	データ消去証明書の発行を行っています。