情報セキュリティとプライバシーに関する
ホワイトペーパー

株式会社Ｗｅｌｂｙ

Ver.1.0
2021年8月

情報セキュリティとプライバシーに対する方針・ポリシー

Welby が提供しているのは、個人やご家族が自ら医療情報の記録・保存を行い、医療関係者と共有する、PHR（Personal Health Record）プラットフォームです。この PHR プラットフォームに蓄積される情報があらゆる脅威から守られ適切に管理された状態を維持することは、Welby における最重要課題と認識し、サービスの利用者様が大切なデータをお預けいただき、安心してサービスを利用いただけるよう対策を行うことは Welby の使命と考えています。

Welby はテクノロジーとデータで個人中心の医療の実現に貢献することを目指し、情報セキュリティ、データプライバシー、および品質管理対策に真摯に取り組んでいます。各種法令を遵守することはもちろんのこと、最新の脅威・対策状況を把握し適用するよう努めています。

概要

本ホワイトペーパーは、Welby の提供する各種サービスにおける情報セキュリティとプライバシー、品質管理を実現するために Welby が行っている取り組みについて説明するものです。Welby がサービスの利用者様のデータを保護するために行っている組織的および技術的な管理の詳細な対策について説明します。

役割と責任

1）開発部門

このグループの責任者は、後述の保守・運用部門も合わせて統括し、Welby が提供するアプリケーションを含む各種サービスの技術実装、開発後の円滑な運用に対する責任を負っており、開発及び、リリース後の保守・運用を範囲とし、実装におけるアプリケーションの管理・監督を行います。クライアントのシステム要件のレビュー、事前評価及び、監査要求への確実な対応にも責任を負います。

このグループのメンバーは、前述の責任者の指示のもと、Welby の提供する各種サービスを構成するハードウェア、ソフトウェア及び、インフラストラクチャに関する導入計画、設計、実装、テスト及び、運用開始後の構成変更及び、新規機能の実装を担当しています。

2）保守・運用部門

このグループのメンバーは Welby の提供する各種サービスの継続動作の保証、その

ために必要な各種施策の検討・実施、サービスの監視及び、障害発生時の迅速な復旧を担当しています。

3）情報セキュリティ部門

このグループは情報セキュリティ責任者が統括し、情報セキュリティ、プライバシー及び、Welby の提供する各種システムが適切に管理され、品質が安定的に維持されるよう、広く普及している各種標準、規制、及びフレームワークに則ったポリシーの策定と管理策の実装を担当しています。

第三者認証、および独立機関による証明

1）ISO27001（ISMS）

Welby は各サービスを通し利用者様よりお預かりする情報および、自社の情報資産を脅威・リスクのレベルに応じ、適切に管理される仕組みを構築・運用しております。第三者認証機関による ISO27001(ISMS)の認証を受けています。

2）ISO27017

Welby の提供する各種サービスの提供基盤として利用している AWS（アマゾン ウェブサービス）のクラウドサービスカスタマとして、また、「Welby マイカルテ」はクラウドサービスプロバイダとして、第三者認証機関による ISO27017 の認証を受けています。

各種レギュレーション対応

Welby の提供する各種サービス・機能において求められるレベルを維持するため、情報セキュリティ、データプライバシー、および品質管理対策に関係する各種省令・ガイドライン・指針等のレギュレーション※を特定し、それらを参考とした自社 SOP を作成、適切な運用が実施されるよう従業員への教育を行なっています。

なお、発出後、対応を開始するため、一部整備、適用途中のものがあります。

※個人情報保護法、3 省 2 ガイドライン、民間 PHR 事業者による健診等情報の取扱いに関する基本的指針、GDPR 等

各レギュレーションの概要については、巻末「参考情報：各種レギュレーションの概要」を参照ください。

人的セキュリティ

Welby は入社時に社員との間で機密情報等を私的に利用しないこと、外部に漏洩させないこと等を盛り込んだ機密保持契約書を締結しており、不正行為を未然に防止するよう対策を行なっております。
また、入社時及び、入社後四半期毎のセキュリティ教育、週次での利用環境に関する全社員への脆弱性情報の共有・対策を実施しており、継続的に社員のセキュリティに対する意識レベルの向上を図っております。

物理的セキュリティ

Welby の提供サービスにおける各種システムは AWS 環境にて稼働しています。
AWS では、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しており、データセンターへのアクセスを必要とするすべての担当者は、厳格な申請と承認のプロセスにより業務上の正当性が認められた場合に限り、最少権限の原則に基づき許可がなされます。AWS のセキュリティコントロールの詳細については以下を参照ください。
AWS のコントロール（https://aws.amazon.com/jp/compliance/data-center/controls/）

ネットワークセキュリティ

サービスの利用者様の端末と、システムとの間のインターネット通信は、SSL 通信（SHA256)によってデータ転送の暗号化がなされています。

アプリケーションセキュリティ

Welby の提供する各種サービスへのユーザアクセスは、WAF（ウェブアプリケーションファイアウォール）を経由させることで、アプリケーションの脆弱性を狙う攻撃から保護しています。WAF を適切に設定することで、ユーザからのリクエストやコンテンツへのアクセスのコントロールを行なっています。

データベースセキュリティ

サービスの利用者様の各種情報（氏名、メールアドレス、各機能で利用するデータなど）が格納されるデータベースは暗号化ストレージを利用しています。利用者の認証に用いるパスワード情報は、不可逆暗号化(ハッシュ化)された状態で、データベースに保管されています。

マルウェア対策

Welby 社員が業務において利用する端末には、マルウェア対策ソフトをインストールし、最新の定義ファイルが自動的に適用される状態としております。

管理者権限・管理者アクセス

1）管理者権限

サービス提供において使用する各種システムの特権アクセスが可能な管理者権限は、適格性を評価した上で権限の付与を行なっております。また、権限所持者の退社時の速やかな権限剥奪及び、月次にて管理者権限保持者の棚卸し、定期見直しを実施しております。

2）管理者アクセス

サービス提供において使用する各種システムの設定変更を行うために利用する管理コンソールへの管理者アクセスについては、二要素認証を用い本人認証を行なっております。また、利用者様の各種情報（氏名、メールアドレス、各機能で利用するデータなど）が格納されるデータベースへのアクセスについては、証明書を用いた認証を行なっております。

モニタリング

1）リソース監視

Welby の提供する各種サービスを構成するハードウェア（CPU、メモリ、データ容量等)、ソフトウェア及び、インフラストラクチャに関するリソースの監視を行なっております。

それぞれ適切な閾値を設定しており、閾値を超えた場合、保守・運用部門にアラートが発報され必要となる対応を行っています。

2）エラー監視

Welby の提供する各種サービスのシステムにおけるエラー監視（プログラム不具合等）を行なっており、それぞれ予め設定された適切な閾値を超えた場合、保守・運用部門にアラートが発報され必要となる対応を行っています。

3）ログ監査

Welby の提供する各種サービスのシステムから出力される各種ログ（イベントログ、操作ログ、認証ログ等）は、それぞれ予め設定された閾値を超えた場合、保守・運用部門にアラートが発報され必要となる対応を行っています。

4）脅威検知

Welby の提供する各種サービスのシステム内における脅威検知のため、マネージド型脅威検知サービスを利用しており、各システム内のネットワークアクティビティ、データアクセスパターン及び、アカウント動作を継続的にモニタリングし脅威を特定しています。

構成管理

Welby の提供する各種サービスのシステムにおける構成変更は、予め定められた変更管理プロセスに則り、計画の事前レビュー、テスト、承認が適切になされた場合にのみ実行されます。利用者様への影響を最小限に抑えるため、変更時には事前の通知をシステム上で行なっています。このプロセスは緊急時にも同様の方法にて実施されています。

インシデント管理

インシデント発生時に迅速に対応することが可能となるよう対応フローを作成し、フローに基づいた対応を行なっております。発生事象・影響範囲等よりレベル判定を行い、判定結果に応じた対応を実施、有効と考えられる再発防止策を立てた上で収束するよう情報セキュリティ部門で管理をしております。

脆弱性対応

1）ペネトレーション診断・脆弱性診断

新規システム開発時及び、新機能開発時にはリリース前に第三者によるペネトレーション診断を実施しています。また、リリース後は定期的にサービス提供において使用する WebAPI に対し、診断ツールを用いた脆弱性診断を実施しています。

2）脆弱性パッチ対応

システムで利用している OS、ミドルウェア等に関する脆弱性情報を定期的に収集し、随時適用しています。システムで利用しているコンポーネントに対する緊急性が高い脆弱性パッチが公開された場合は、速やかに適用しています。

BCP

1）データの保管場所

提供サービスにて利用者様からお預かりしたデータは、AWS 東京リージョン内においてマルチ AZ（アベイラビリティゾーン）構成にて保管され、複数の AZ にまたがってシステムの配置を行っております。万が一、インフラストラクチャ障害が発生した場合でも AZ 間で自動的にフェイルオーバーすることで、中断することなくサービスの継続提供が可能となっております。

AWS はデータセンターの場所を選択する前に、洪水、異常気象、地震活動などの環境リスクを軽減するために環境評価および地理的評価を実施した上でデータセンターの場所を慎重に選択しています。前述の AZ 間は物理的に分離されており、相互に独立して構築されています。

2）データのバックアップ

データベースに保管される、利用者様の各種情報（氏名、メールアドレス、各機能で利用するデータなど）は、日次でバックアップを取得しています。バックアップは、35 世代分保管されております。

3）BCP 訓練

稼働している提供サービスより毎年対象を選定し、取得したバックアップからのリストアを含めた BCP 訓練を年次で実施しております。

内部監査

Welby は社内で内部監査人を任命し、ISO27001(ISMS)及び、ISO27017 運営において提供する各種サービスを含む内部監査を年次で実施しています。

参考情報：各種レギュレーションの概要

3省2ガイドライン

医療情報システムの構築・運用を行う医療機関等や医療機関等から医療情報を受託管理する事業者・団体向けに医療情報の安全管理策を示した厚生労働省、総務省、経済産業省の3省が発行するガイドライン

民間 PHR 事業者による健診等情報の取扱いに関する基本的指針

配慮を要する個人情報である健診等情報を取り扱うこととなる民間事業者が遵守すべき事項について、項目別に詳細を提示した厚生労働省、総務省、経済産業省の3省が発行する指針

GDPR

EU 一般データ保護規則（General Data Protection Regulation の略）は、データ主体のプライバシーに関する基本的な権利を保護し、個人データの保護を強化するための個人データの処理と移転について定めた欧州連合（EU）の法律