**要件定義書（Webアプリ & ネイティブアプリ）**

**目次**

[0. 各ドキュメントの目的および位置付け 3](#_Toc162546201)

[「要件定義書」の目的と概要 3](#_Toc162546202)

[「Webアプリ基本設計書」の目的 4](#_Toc162546203)

[「ネイティブアプリ基本設計書」の目的 4](#_Toc162546204)

[1.プロジェクトが解決する課題と提供するソリューション 5](#_Toc162546205)

[1-1. 現状の課題 5](#_Toc162546206)

[1-2. 想定ペルソナ 7](#_Toc162546207)

[1-3. ソリューション 8](#_Toc162546208)

[1-4. プロダクトのUSP 11](#_Toc162546209)

[1-5. プロダクトのステークホルダー 12](#_Toc162546210)

[企業担当者の体験概要 12](#_Toc162546211)

[候補者の体験概要 12](#_Toc162546212)

[2. Webアプリ開発の全体スコープおよび採用技術 14](#_Toc162546213)

[2-1. 開発アプリの全体像と対象となるスコープ 14](#_Toc162546214)

[概要 14](#_Toc162546215)

[システム全体像 15](#_Toc162546216)

[Webアプリ採用技術 15](#_Toc162546217)

[2-2.採用エントリーシステムの対象スコープとなる機能要件 17](#_Toc162546218)

[概要 17](#_Toc162546219)

[機能概要 17](#_Toc162546220)

[2-3.プロセッシングシステムの対象スコープとなる機能要件 18](#_Toc162546221)

[概要 18](#_Toc162546222)

[機能概要 18](#_Toc162546223)

[2-4. 採用マッチングシステムの対象スコープとなる機能要件 19](#_Toc162546224)

[概要 19](#_Toc162546225)

[機能概要 19](#_Toc162546226)

[2-5. 非機能要件 21](#_Toc162546227)

[サポート概要 21](#_Toc162546228)

[サポート環境 21](#_Toc162546229)

[セキュリティ要件概要 21](#_Toc162546230)

[「可用性」「性能・拡張性」「運用・保守性」 21](#_Toc162546231)

[2-6. リスク分析と対応方針 24](#_Toc162546232)

[概要 24](#_Toc162546233)

[成績データの改ざん 24](#_Toc162546234)

[企業情報の漏洩 24](#_Toc162546235)

[2-7. 大規模・商用・社会実装時の対応方針 26](#_Toc162546236)

[3.ネイティブアプリ設計の対象スコープおよび要件 27](#_Toc162546237)

[3-1. ネイティブアプリの設計目的 27](#_Toc162546238)

[目的1: 個人のプライバシー情報を保護するための安全なデータ管理を実現 27](#_Toc162546239)

[目的2: 候補者に対するUI/ UXの提供 28](#_Toc162546240)

[目的3: エントリーシステムの機能の代替 29](#_Toc162546241)

[3-2.ネイティブアプリの全体スコープおよび採用技術 30](#_Toc162546242)

[ネイティブアプリの位置付け 30](#_Toc162546243)

[設計の対象となるスコープとスコープ外 30](#_Toc162546244)

[ネイティブアプリ採用技術 31](#_Toc162546245)

[3-3.ブロックチェーンとRDBを連携した暗号分割管理方式による安全な保存 32](#_Toc162546246)

[技術選定の背景 32](#_Toc162546247)

[機能概要 32](#_Toc162546248)

[3-4.ネイティブアプリの機能要件 34](#_Toc162546249)

[3-5. ネイティブアプリの非機能要件（サポート環境） 35](#_Toc162546250)

[3-6. ネイティブアプリのリスク分析と対応方針 36](#_Toc162546251)

[①秘密鍵管理における法的規制周りのリスク 36](#_Toc162546252)

[②秘密鍵管理における法的規制周りの対応方針 36](#_Toc162546253)

[③秘密鍵への攻撃と盗難のリスク 36](#_Toc162546254)

[④秘密鍵への攻撃と盗難リスクに対するネイティブアプリのセキュリティ特性を生かした対応方針 36](#_Toc162546255)

[⑤内部アルゴリズムの解析リスク 37](#_Toc162546256)

[⑥内部アルゴリズムの解析リスクの対応方針 37](#_Toc162546257)

[3-7. 大規模・商用・社会実装時の対応方針 38](#_Toc162546258)

# 0. 各ドキュメントの目的および位置付け

最初にドキュメント理解の容易性を高めることを目的として、各ドキュメントの目的および位置付けを明確化していく。

ダイアグラム

自動的に生成された説明

本プロジェクトのドキュメントは以下の3つで構成される。各目的に応じたドキュメントを参照されたい。

* **要件定義書（本ドキュメント）**
* Webアプリ基本設計書（別紙参照）
* ネイティブアプリ基本設計書（別紙参照）

### 「要件定義書」の目的と概要

要件定義書は、プロジェクト全体の目的や、各プロダクト仕様の概要レベルでの理解を目的としている。すなわち、要件定義書は最も抽象レベルの高いドキュメントといった位置付けとなる。具体的には、主に以下の要素で構成される。

* ビジネス要件（プロジェクトが解決する課題と解決策）
* 企業向けWebアプリの開発要件の概要（設計の全体像と機能概要）
* 候補者向けネイティブアプリ設計の概要（設計の全体像と機能概要）

前途の通り、要件定義書は概念レベルでの理解を目的としているため、Webアプリやネイティブアプリのシステム要件の説明も概要レベルにとどめており、具体レベルでの仕様詳細に関しては、基本設計書に記載するといった形で、ドキュメントを分離・整理している。

### 「Webアプリ基本設計書」の目的

本ドキュメントは、実証期間中に実際に開発・実装することを目的とした、具体的なシステム要件を記載したドキュメントである。具体的なシステムのアーキテクチャーや、対象とする具体的なデータやロジックを参照する場合に有効。

### 「ネイティブアプリ基本設計書」の目的

本ドキュメントは、Webアプリ基本設計書と同様、ネイティブアプリの具体的なシステム要件を記載したドキュメントである。しかしながら、実証期間中に設計に基づいた開発・実装はしないという点において、Webアプリの設計書とは性質が異なる。

# 1.プロジェクトが解決する課題と提供するソリューション

## 1-1. 現状の課題

「教育市場」と「労働市場」の一体化が進まない。人材は豊富だが教育が不十分な国々（ベトナム等）と、人口減少によって「労働市場」の需要が満たされない国のギャップが存在している。例えば、ベトナムをはじめとした東南アジア諸国は人材が豊富だが、デジタル教育は十分とは言えない現状がある。一方で日本のようにデジタル教育は比較的十分だが、労働市場における人材は人口減少によって不十分になっている。このように国際間の教育および人的リソースのギャップが生じている。

グラフ, バブル チャート

自動的に生成された説明

この両者のギャップを埋める仕組み、すなわち人材な豊富な国に対して教育を提供し、先端デジタル人材を育成し、育成した先端デジタル人材を人材不足の日本企業とマッチングする。この国際間のギャップを埋めることで、労働市場の国際間ギャップの課題を解決するサービスが、今回の人材育成・採用マッチングシステムである。

ダイアグラム

自動的に生成された説明

しかしながら国内企業が海外からデジタル人材を獲得する際、下記のような４つの課題に直面する。

#### 課題1: 最新のデジタル人材教育プログラムの供給が十分ではない & 教育プログラムを受ける予算がない

ベトナムをはじめとした労働人材が豊富な国は、最新のデジタル教育の供給が不十分であるのが現状である。例えば、 ベトナムの国立大学の一つでもあるハノイ貿易大学におけるヒアリングでも、彼らの 予算ではデジタル教育を希望する学生の10分の1程度にしか学生が育つデジタル教育を提供することができない のが現状である。

#### 課題2: 能力が評価できない（標準化されていない）

国内企業が海外からデジタル人材を獲得する際、能力を適切に評価できないと言った課題がある。背景としては、能力データが標準化されておらず、デジタル人材が受講した教育プログラムの難易度の違いなどが反映されていないため、該当国の候補者が、日本の候補者や他諸国の国の候補者と比較した際に、どのくらい優れているのか、などを適切な軸で評価することができない。また、海外の教育内容を日本の多くの企業は知りえないため、レジュメや職務経歴書に記載されている内容が本当に正しいかどうかを判断することができない。

#### 課題3: 個人情報ポータビリティの課題

一般的に、国内企業が海外人材のスクリーニングを行う際の情報利用やデータ移転、持ち出しをする際、個人情報保護方針に対応する必要があり、一般的には煩雑なプロセスを要する。そのため、日本の候補者を採用するケースと比較すると、採用工数およびコストが大きく掛かってしまう。

#### 課題4: データ管理に関する課題

一般的に就職・転職希望者は、人材紹介会社等に提供した個人情報が、どのように管理されているか知ることができず、不透明なことが一般的である。また、上記の候補者がスキルアップのために受講した認定講座の情報や成績データがどのように管理されるか、あるいはどのように利用されるか等も同様に不透明である。つまり、プラットフォーム主導型の場合は基本的に、個人情報も成績データも、候補者主導で開示許可や削除等はできず、基本的にプラットフォーマーの管理体制に委ねられることとなる。さらに、学習データや講座の認定情報が学習プラットフォームごとに分散しており、個人での管理ができず、また、データの用途がない。

## 1-2. 想定ペルソナ

**採用企業（日本）**

* **基本情報**
  + 業種：金融機関・メーカー
  + 規模：大手上場企業
  + 文化：外国に支店もあり、多様性を重視している
* **採用ニーズ**
  + テクノロジーを活用して事業を推進できるデジタル人材
  + 多様性をもたらせる人材
* **採用における課題**
  + デジタル人材は競争的であり、ニーズのあった人材を獲得することが難しい
  + 多様性をもたらせる外国人材も、彼らが企業風土に合うのか、スキルがマッチするのかなどの判断が難しく採用が進んでいない
  + 外国人の個人情報の取り扱いは煩雑になりがちで対処が難しい

**転職希望者**

* **基本情報**
  + 年齢：20台前半
  + 居住地：ベトナム、ハノイ
  + 教育背景：ハノイ貿易大学、金融・経済専攻（高度人材）
  + 職歴：未経験が大半
* **キャリア志向**
  + 日本での就職意欲がある程度高い（サーベイ（※）で日本で働きたいかどうかを１－５のスケールで調査。「１」が全く働きたくない、「5」がとても働きたい、として調査したところ、「５」の解答が7名、「4」の解答が13名となり、合わせて56%が日本で働きたい、と回答した。「3」は13名であり、36%は中立的）
  + 希望年収は150万円弱（サーベイでの回答から、平均値：140万円；中央値：146万円）である
  + 成長志向がとても強く、簡単には乗り越えられない壁を超えることを誇りとしている
* **職探しにおける課題**
  + 日本における就職プロセスが確立されておらず日本での就職機会は考えたこともない
  + 個人情報がきちんと守られているか心配（31名/36名がサーベイで個人情報保護がきちんと守られているか関心があると回答）

※実証に参加したベトナム人学生・若手社会人合計36名に行った独自サーベイ

## 1-3. ソリューション

本プロジェクトでは以下のようなソリューションを提供することで、前途のような国内企業が海外からデジタル人材を獲得する際のボトルネックを解消しつつ、人材な豊富な国に対して適切な教育を提供し、先端デジタル人材を育成し、育成した先端デジタル人材を、人材不足の日本企業とマッチングする仕組みを構築する。

ダイアグラム

自動的に生成された説明

#### 解決策1: NFTを用いた無償提供の仕組みを構築

教育を受けたい海外人材は、事前無償学習を通じて一定の条件を満たした場合、教育を無償で受ける権利を獲得することができる。（NFTによる無償教育の仕組み、および仕組みを実現するプロダクトに関しては、本要件定義書の開発のスコープ外であるため、詳細な説明は割愛。）

#### 解決策2: 「ESCO基準 × GROW360」をベースとした能力評価の標準化

ESCO（European Skills, Competences, Qualifications and Occupations）とは、職業毎、ポジション毎に必要なスキルを明確に定義したEUにおける能力の基準である。このESCO基準を候補者の評価基準として利用することで、国内企業が海外人材の能力を評価できないといった課題を解決することができる。

GROW360とは、AIを活用した評価補正により、信頼性の高い他者評価を実現した360度能力評価システムおよび、IATと呼ばれる潜在的な傾向チェックにより、隠れたパーソナリティやバイアスを可視化するア セスメントツールである。ESCO基準に加えてGROW360から出力されるデータを能力評価に用いることで、一般的なスキルだけではなく、候補者のソフトスキルといった項目から評価することも可能となる。

#### 解決策3: 個人情報の暗号化および秘密計算によるデータ保護の安全性担保

海外デジタル人材の該当国家、今回のユースケースの場合だとベトナムのレギュレーションに準拠したデータの管理手法を用いるだけではなく、個人情報、能力データ等の適切な手法を用いた暗号化、および能力データを算出する際に、秘密計算（データを暗号化したまま計算する技術）を用いることで各国のレギュレーションに対応しつつ安全な形で、企業に候補者の情報の提供を可能とし、国際間マッチングを実現することが可能となる。

**秘密計算の有用性補足**

以下に今回のユースケースにおいて秘密計算を利用すべき理由を補足する。

今回のユースケースでは、以下のニーズが存在する。

* **ベトナム人学習者（求職者）**： 成績データは個人情報にあたり、特に採用に際して国外企業に提供する際には、個人情報保護規制の問題から、データを秘匿化しておきたい。
* **日本国内の採用企業担当者**： 求職者が自社にマッチしている人材かについて、成績データに企業独自の重みを掛け合わせることで、マッチング度を見たいが、その重み情報は秘匿化しておきたい。

両者のニーズを叶えるために、暗号化された成績データと暗号化された重みを掛け合わせて、能力スコアを算出し、求職者の最低希望年収と合わせて、散布図として表示される。 そして、この散布図から採用企業側は採用したい求職者を選別できるようにする。

この仕組みを構築するためには、暗号化した状態で機密なデータを計算できる秘密計算技術の活用が効果的であり、秘密計算利用により、複数のステークホルダー間でのデータの安全な共有と処理を可能にし、学習者のプライバシーと企業の機密情報を保護する重要な役割を果たしている。

#### 解決策4: 候補者主導でのデータ管理を可能とする仕組みの構築

候補者が自身主導で、個人情報および成績データの開示許可や削除を行えるようにし、プラットフォーム主導ではなく候補者主導でのデータ管理を可能とする仕組みを構築する。加えて、候補者の個人情報を、いつ誰に開示したのか確認できるといったトレーサビリティを担保、透明性を持った仕組みを構築する。さらに個人情報と成績データをパブリックチェーンとリレーショナルデータベースに暗号化、分割保存する仕組みを構築することで、候補者主導の安全なデータ管理を実現する。また、通常学習コンテンツ提供者が保持する成績データなどの精緻な情報を個人で閲覧、提供、削除できるようにすることで、採用マッチングに活用することができる。

## 1-4. プロダクトのUSP

上述の課題と解決策を整理した上での本プロダクトの競合他社にはない、独自の強みとしてのUSP（ユニークセリングポイント）を以下でまとめる。

|  |  |  |
| --- | --- | --- |
| **課題** | **解決策** | **プロダクトのUSP** |
| 最新のデジタル人材教育プログラムの供給が十分ではない & 教育プログラムを受ける予算がない | NFTを用いた無償提供の仕組みを構築 | ・候補者は無償で最新のデジタル教育プログラムを受けることが可能。 |
| 能力が評価できない（標準化されていない） | 「ESCO基準 × GROW360」をベースとした能力評価の標準化 | ・企業担当者は、標準化された客観性の高いデータをもとに候補者をスクリーニングおよびオファーを出すことが可能。  ・企業担当者は、一般的なスキルに加えて能力スコアやソフトスキルといった、マッチング精度に寄与するデータも採用プロセスにおいて活用することが可能。 |
| 個人情報ポータビリティの課題 | 個人情報の暗号化および秘密計算によるデータ保護の安全性担保 | ・企業担当者は、海外人材獲得のための、各国のレギュレーションに準拠しなければならないといった、煩雑なプロセスをなくすことが可能。  ・候補者は国を跨いだ採用エントリーが可能。 |
| データ管理に関する課題 | 候補者主導でのデータ管理を可能とする仕組みの構築 | ・候補者は匿名性が担保されつつ、スキル以外の部分でのPRが可能。 |

## 1-5. プロダクトのステークホルダー

本プロダクトを利用するステークホルダーは大まかに2つに分けられる。

* **「Webアプリ経由」で採用マッチングシステムを利用する「企業担当者」**
* **「ネイティブアプリ経由」で採用マッチングシステムにエントリーする「候補者」**

ダイアグラム

自動的に生成された説明

### 企業担当者の体験概要

実証期間の開発スコープにおける主要ステークホルダーは「企業担当者」である。「企業担当者」とは、海外のデジタル人材を採用したいと考えている、日本の大手企業担当者を指す。企業担当者は、Webアプリを使用して候補者とマッチングを行う。企業担当者は候補者にオファーを送信し、マッチング成立後、候補者とアプリ内でコミュニケーションを取ることができる。彼らは採用プロセスを効率的に管理し、候補者との連絡を取るためにアプリを活用する。

企業担当者向けの要件および設計に関しては、実際に実証期間内に開発を実施し、Webアプリとしてプロトタイプを作成する。

※補足: Webアプリの要件に関しては第2章、詳細に関してはWebアプリ基本設計書を参照

### 候補者の体験概要

「候補者」とは、エントリーシステムを通じてデジタル人材育成のための講座を受講していて、かつ日本企業に就職を検討しているベトナムの学生・若手社会人を指す。候補者はネイティブアプリを利用し、採用マッチングシステムを利用する。候補者はネイティブアプリをスマートフォンにインストールし、マッチングのタブを選択してエントリーを行うことが可能。その後、企業担当者からのオファーを受け取り、オファーを承諾するかしないか、選択が可能である。マッチングが成功（=オファーを承諾）した場合、アプリ内で企業担当者と、テキストメッセージを通じてコミュニケーションをとることができる。

また、本アプリの特徴として、候補者が自身から企業にエントリーする機能は提供されず、代わりに候補者は企業からのオファーに対するアクションを起こすことになる。

※ 補足: ネイティブアプリの要件に関しては第3章、詳細に関してはネイティブアプリ基本設計書を参照

# 2. Webアプリ開発の全体スコープおよび採用技術

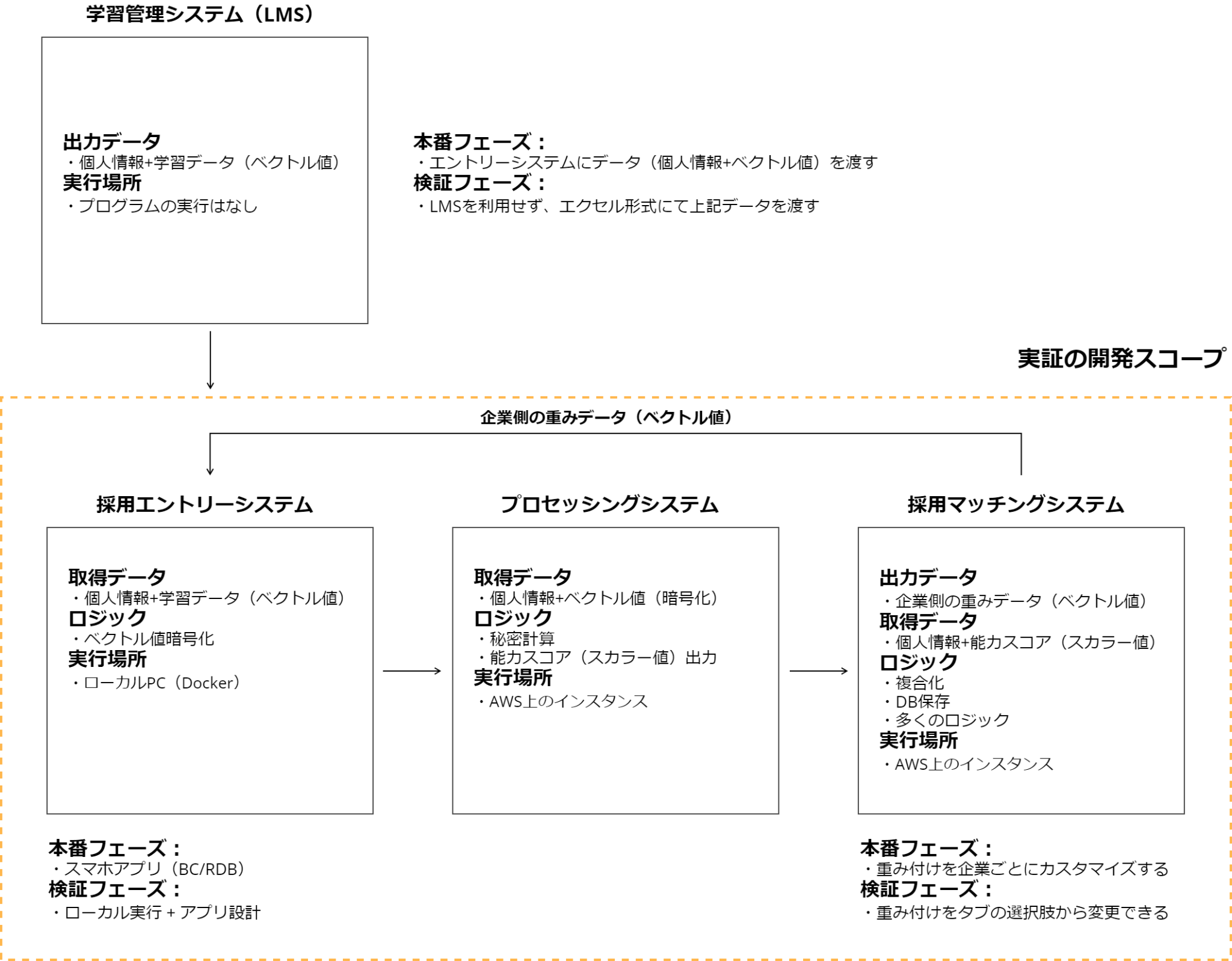
本プロジェクトでは、Webアプリケーションという手段を用いることで、国際間の教育市場および労働市場が抱える課題を効果的に解決していく。今回の開発対象となるアプリケーションは3つのアプリケーションで構成される。3つのアプリケーションとは**「採用エントリーシステム」「プロセッシングシステム」「採用マッチングシステム」**のことを指し、今回の開発対象となるスコープとなる。この3つのシステムが連携することで安全な形で国際間のマッチングを実現することが可能となる。

## 2-1. 開発アプリの全体像と対象となるスコープ

### 概要

* **「採用エントリーシステム」**の責務は、候補者情報の適切な手法を用いた暗号化である。本番リリースをするフェーズではこのシステムはスマホのネイティブアプリで実装されるが、今回の実証においてはローカルPC上でDockerコンテナ等を立てることでアプリを実行する。
* **「プロセッシングシステム」**の責務は、秘密計算を用いて候補者の能力スコア（スカラー値）を求めることである。
* **「採用マッチングシステム」**の責務は、候補者と企業担当者に対して最終的なユーザーインターフェースを提供することである。システムのインターフェースは候補者側と企業担当者それぞれ用意する必要があるが、今回の実証のスコープは企業側のインターフェースのみを対象とし、候補者側のインターフェースは提供しない。

### システム全体像



### Webアプリ採用技術

* Lattigoの選定理由に関しては、Webアプリ基本設計書を参照
* Go言語/ Gin/ AWSの各種コンポーネントに関しては、本技術スタックを採用することでシステム要件を満たすことができ、かつIGSの技術ナレッジが豊富なため、採用に至った

|  |  |  |
| --- | --- | --- |
| **分類** | **採用技術** | **技術概要** |
| サーバーサイド | Go言語 | Googleが開発した汎用のオープンソースプログラミング言語 |
| Gin Web Framework | Golang で書かれた Web フレームワーク |
| Lattigo | 準同型暗号を実装するためのOSSライブラリ |
| フロントエンド | VueJS | WebアプリケーションのUI部分などを開発する際に使われる、オープンソースのJavaScriptフレームワーク |
| インフラ | AWS | アマゾンが提供するクラウドサービスの総称 |
| その他 | Docker | コンテナ型の仮想環境を作成、配布、実行するプラットフォーム |

## 2-2.採用エントリーシステムの対象スコープとなる機能要件

### 概要

* 採用エントリーシステムの目的は候補者のデータ（個人情報と成績データ）を暗号化することである。
* 候補者/採点者はデータ（個人情報と成績データ）をGoogle フォームに入力し、そのベクトル情報を採用エントリーシステムに入力する （プロトタイプではIGSが採用エントリーシステムへの入力を行う）
* プロトタイプにおいてはWebアプリとして開発する。WebアプリはローカルクライアントPCのDockerコンテナで立ち上げ & 実行し、暗号化とデータ送信を行う。
* 候補者の個人情報は暗号化されマッチングシステムに送信される
* 候補者のベクトルデータは”格子暗号”によって暗号化されプロセッシングシステムに送信される

### 機能概要

* 以下の表は採用エントリーシステムの機能の概要を項目ごとに整理したものである。
* 詳細な仕様（画面設計および詳細データ）に関しては、基本設計書を参照。

|  |  |  |
| --- | --- | --- |
| **項目** | **機能概要** | **補足事項** |
| **データの暗号化機能** | ・Dockerコンテナ上で、データを格子暗号によって暗号化する  ・データとは候補者の個人データと成績データ（ベクトル値）の両方を指す | 暗号化はGo言語ライブラリのlattigoのCKKSを用いる |
| **個人データ送信機能** | ・暗号化された個人データをマッチングシステムに送信する |  |
| **ベクトルデータ送信機能** | ・暗号化された成績データ（ベクトル値）をプロセッシングシステムに送信する |  |
| **鍵生成機能** | ・秘密鍵と公開鍵のキーペアを作成する |  |

## 2-3.プロセッシングシステムの対象スコープとなる機能要件

### 概要

* プロセッシングシステムの目的は、マッチングシステムによってインプットされた重み情報、採用エントリーシステムによってインプットされた候補者のベクトル情報の2つのデータを用いて、候補者の能力スコアおよびスカラー値を秘密計算によって求めることである。
* 採用エントリーシステムからプロセッシングシステムに送信された候補者のデータは格子暗号によって暗号化されており、IGSはその復号化権限を持たない。つまり鍵管理を行わない
* 採用マッチングシステムからプロセッシングシステムに送信された企業側の重みデータ（UI上のチャート項目に対する重み付けの値）は暗号化されており、IGSはその復号化権限を持たない。つまり鍵管理を行わない

### 機能概要

* 以下の表はプロセッシングシステムの機能の概要を項目ごとに整理したものである。
* 詳細な仕様（画面設計および詳細データ）に関しては、基本設計書を参照。

|  |  |  |
| --- | --- | --- |
| **項目** | **機能概要** | **補足事項** |
| **秘密計算機能** | ・秘密計算を実行する  ・企業側の重みデータベクトルと成績データ（ベクトル値）の2つの変数を用いて掛け算を行う  ・個人の成績データ（ベクトル値）の一部はCKKSにより準同型暗号を用いて暗号化されたまま計算される |  |
| **計算結果保存機能** | ・秘密計算の結果をデータベース、またはストレージに保存する |  |

## 2-4. 採用マッチングシステムの対象スコープとなる機能要件

### 概要

* 採用マッチングシステムの役割は、企業の重み付けの入力および引き渡し、秘密計算の結果を複合化することに加えて、候補者と企業担当者に対して最終的なユーザーインターフェースを提供することである。
* システム管理者はプロフィールのハードスキル、およびソフトスキルを構成する各項目の重み情報をマッチングシステムに入力する。
* 上記重み情報は格子暗号で暗号化されプロセッシングシステムに送信される。
* システムのインターフェースは候補者側と企業担当者それぞれ用意する必要があるが、今回の実証のスコープは企業側のインターフェースのみを対象とし、候補者側のインターフェースは提供しない。

### 機能概要

* 以下の表は採用マッチングシステムの機能の概要を項目ごとに整理したものである。
* 詳細な仕様（画面設計および詳細データ）に関しては、基本設計書を参照。

|  |  |  |
| --- | --- | --- |
| **項目** | **機能概要** | **補足事項** |
| **候補者表示 & 選択機能（散布図形式）** | ・候補者を散布図形式で表示する ・散布図は縦軸の候補者の希望年収、横軸の総合能力スコアで構成される ・企業担当者は散布図から候補者を選択することができる ・散布図上の候補者をクリックすると、プロフィール詳細がモーダル形式で表示される |  |
| **候補者表示 & 選択機能（リスト形式）** | ・候補者をリスト形式で表示する ・リストは候補者の属性情報/スキル/ Like数等で構成される ・企業担当者はリストから候補者を選択することができる ・リスト上の候補者をクリックすると、プロフィール詳細がモーダル形式で表示される | ・ページネーションの仕様は現状なし |
| **候補者ソート機能** | ・企業担当者はリスト上の候補者をソートして表示させることができる ・ソートのクライテリアは「能力スコア」「ハードスキル」「ソフトスキル」「希望年収」「オファー数」 | ・Need要件（可能であれば実装） |
| **候補者プロフィール表示機能** | ・モーダル形式で、候補者のプロフィールが表示される ・プロフィールは「属性情報」「能力スコア合計値（スカラー値）」「個別のハードスキル & ソフトスキル」「Like数などのアプリ内取得情報」で構成される ・「個別のハードスキル & ソフトスキル」に関しては、候補者が表示/ 非表示を決めることができる  ・候補者プロフィールの個別のソフトスキル、ハードスキルの項目に対して、他候補者の平均の値を表示する ・表示形式は、スキルバーの中に、平均値のラインを引く想定 | ・表示データ等の詳細仕様は、基本設計書を参照  ・平均値の表示はNeed要件 |
| **Like送信機能** | ・企業担当者は候補者にLikeを送信することができる ・送信したLike数は、TOPページのリストおよびプロフィール詳細に表示される | ・現状、/Likeを押したとしても候補者に通知は飛ばない |
| **オファー送信機能** | ・企業担当者は候補者にオファーを送信することができる ・オファー送信画面は、TOPページの候補者リストのオファー送信ボタン、またはプロフィール表示画面のタブから「オファー」を選択することで表示可能 ・企業担当者は、自社の連絡先（Emailアドレス）とメッセージを入力することで、オファーを候補者に送信可能。 ・オファーを送信すると、候補者のメールアドレスに直接メッセージが届き、今後のやり取りに関しては、システムは関与しない | ・メール送信機能は、実証のみで利用予定 ・メールの詳細仕様は、基本設計書を参照 ・本番フェーズでは、メールでのやり取りの機能はシステム上のチャットに代替される予定 |

## 2-5. 非機能要件

### サポート概要

* 採用マッチングシステムが対応するハードウェアおよびブラウザは表の通り。
* 基本的に、最新版のGoogle Chrome かつデスクトップが推奨環境。
* デスクトップかつChrome以下のブラウザを利用する場合、利用可能、および非推奨環境。
* モバイルデバイスはサポート外。レスポンシブ対応等も行わない。

### サポート環境

**◎: 推奨環境、○: 利用可、△: 非推奨、×: 非対応**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ブラウザ（国内シェア）** | **Windows**  **（デスクトップ）** | **Mac**  **（デスクトップ）** | **Android**  **（モバイル）** | **iOS**  **（モバイル）** |
| **Chrome（60.7%）** | ◎ | ◎ | **サポート外** | |
| **Edge（22.4%）** | ○ | ○ |
| **Safari（6.2%）** | NONE | ○ |
| **FireFox（7.1%）** | ○ | ○ |
| **IE（2.1%）** | × | × |

### セキュリティ要件概要

* 暗号化および秘密計算部分を除いた一般的なWebアプリケーションのセキュリティ要件が対象。
* プライバシーテック技術を用いた暗号化および鍵管理等の要件に関しては、基本設計書を参照。
* 今回は実証フェーズにおけるプロダクト開発であり、一般のマーケットにリリースされることはない。また、利用想定のステークホルダーも最小限である。従ってセキュリティ要件は堅牢なものではなく一般的なレベルの要件とする。

### 要件

* 常時SSL化（HTTPS化）を実施。
* 検証フェーズにおいては、アカウント登録、およびログイン機能を実装しない。従ってこれらの機能を実装することによって付随するセキュリティリスクに対する対策、例えばセッションハイジャックや CSRF（クロスサイトリクエストフォージェリ）対する対策等は行わない。
* 企業担当者が情報をインプットする部分として、候補者に対してメッセージを送信する部分がある。こちらに関しては、適切なエスケープ処理を行うことで、SQLインジェクションに対する対策を行う。

### 「可用性」「性能・拡張性」「運用・保守性」

* IPAの非機能要件グレードに基づき上記3つの非機能要件を策定した。
* モデルとして選択したものは「社会的影響が殆ど無いシステム」である。IPAの非機能要件グレードのモデルシステムのグレードによると「社会的影響が殆ど無いシステム」「社会的影響が限定されるシステム」「社会的影響が極めて大きいシステム」の3つに大別されている。
* 今回のシステムは「ごく小規模のインターネット公開システムを想定」していてかつ「システムの機能が低下または利用不可な状態になった場合、利用部門では大きな影響があるが、その他には影響しない」性質を持つことから、本システムは「社会的影響が殆ど無いシステム」をモデルとして選択した。
* 以下の表は選択した重要項目および項目に対するメトリクス指標と対応レベル、運用方針・対策をまとめたものである。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **大項目** | **中項目** | **小項目** | **メトリクス指標** | **対応レベル** | **運用方針・対策** |
| 可用性 | 継続性 | 運用スケジュール | 運用時間（通常） | レベル1 定時内（9時～17時） | クラウドサービスで利用するコンポーネント上、基本的には24時間システム稼働予定であるが、夜間に利用する予定はないため、定時内の運用を想定。 |
| 業務継続性 | 対象業務範囲 | レベル4 外部向けオンライン系業務 | 外部向けオンラインシステムが稼働していることがシステム稼働の条件となることを想定。 |
| 目標復旧水準  （業務停止時） | RTO（目標復旧時間） | レベル1 1営業日以内 | 1営業日以内のシステムの復旧を目指す。 |
| 稼働率 | 稼働率 | レベル2 99% | 1年間で数時間程度の停止を許容。 |
| 性能・拡張性 | 業務処理量 | 通常時業務量 | ユーザー数 | レベル0  特定ユーザーのみ | 候補者20-30名、企業担当者5-10名の利用を想定。 |
| 業務量増大度 | ユーザー数増大率 | レベル5 | 別途社会実装時の対応方針の章を参照。 |
| 運用・保守性 | 運用環境 | 開発用環境の設置 | 開発用環境の設置有無 | レベル1 運用環境の一部に限定した開発環境を設置 | 開発環境と本番環境の2つを管理。開発環境は、コスト削減のため本番環境よりも、グレードを落としたものを利用。 |
| マニュアル準備レベル | マニュアル準備レベル | レベル1 システムの通常運用のマニュアルを提供する | エントリーシステムの操作手順書を用意。 |

## 2-6. リスク分析と対応方針

### 概要

本サービス・アプリを利用するにあたってリスク分析・対応方針の整理を行い、大きく2点の対策を挙げた。なお、今回の対象となるリスクの切り口としては、実証段階おけるリスクに対する対策は限定的となるが、今後の本番リリース時にはより対策方針が強化されると想定される項目を優先的にピックアップした。

### 成績データの改ざん

1点目は候補者の成績データの改ざんが挙げられる。今回の実証のシステム設計では、候補者のデータはCSVで取得し、PCでシステムにアップロードする形式を取る。仮に社内PCに誰かがハッキングした場合、成績データを書き換えてアップロードすることが可能となる。その結果、不正に成績をよく見せる、あるいは不正に悪く見せるといった事案が発生する。その結果、不正基準による企業と候補者のマッチングが行われるだけではなく、サービス提供事業者としての信頼性も損なうことになる。

本リスク、すなわち機密性および完全性に対する対策として、セキュリティが確保された環境、例えば社内PCかつ社内ネットワーク環境でのみシステムを操作できるようにし、かつシステムを実行できる人を限定するなどの対策をすることが挙げられる。また、本番リリースするフェーズでは、成績データのアップロードを個々のユーザースマホのネイティブアプリで代替することで機密性を確保するだけではなく、パブリックチェーンに成績データを暗号化して保存することで、トレーサビリティを担保する。仮に不正操作された場合でも、どこで誰がいつのタイミングでデータを書き換えたのかが追尾可能となる。

### 企業情報の漏洩

2点目は、企業情報の漏洩が挙げられる。今回の実証では企業担当者が、候補者に対してオファーを送る際に、メールアドレス等の企業情報を入力する。そして、その情報は最終的に候補者のメールへと送付される。仮に、候補者の中に悪意を持ったユーザーがいた場合、例えば企業のメールアドレスを取得するためだけに本サービスを利用しているユーザーがいた場合、企業情報を不正に利用されるリスクがある。例えばリスト販売業者への情報売却や営業目的としての利用である。

基本的に、実証におけるサービスとしてサポートするのはシステム上でオファーを出す時までであって、オファー後の行動は企業と候補者間に委ねるといったスタンスではあるが、このような不正があった場合、企業およびサービスの信頼を損なってしまうリスクが存在する。

本リスクに対する対策として、本番フェーズではシステム上に新しい機能としてチャット機能を実装する予定であり、メールの機能は廃止する予定である。今後は、企業がオファーを出したとしても企業のメールアドレスが候補者に行き渡ることはなく、システム上で全てのやり取りが完結する想定となる。

|  |  |  |  |
| --- | --- | --- | --- |
| **サービス利用にかかるリスク** | **発生可能性** | **影響度（CIA）** | **リスクに対する対応方針・攻撃防止の根拠** |
| **成績データの改ざん** | 個人の成績データ（資産）、に対して悪意のあるユーザーがCSVを改ざんしたうえで成績データをWebで挙げること（脅威）があげられる。これはエントリーシステムを実行可能なPCを通じて、不正アクセスを行うことでできてしまう（脆弱性）ため、発生可能性は小~中程度である | 個人の成績データは、完全性と機密性が高く求められるため、影響度は高い。具体的に左記脅威が発生した場合は、不正なマッチングが行われることによる事業者の損失（完全性の欠如）や求職者・事業者に対して、情報が他の方に見られていることによる不安感・プライバシーの毀損（機密性の欠如）を与えることになる | **実証における対策**  エントリーシステムは社内のみからのアクセスに限定するとともに、システムを操作できる人数を限定する。  **本番リリースおける対策**  本番では、候補者のみが実行可能なネイティブアプリをリリースする。 周辺システムである、学習管理システム（LMS）のセキュリティレベルを強化する。 |
| **企業情報（メールアドレス）の漏洩** | 企業のメールアドレス（資産）、に対して悪意のあるユーザーが、企業アドレスを、リスト販売等の不正利用（脅威）するケースが挙げられる。これはマッチングシステムを利用可能な候補者かつオファーを受けた候補者は取得可能なため、発生可能性は小~中程度である | 企業連絡先等は機密性が求められるため、影響度は高い。  具体的には、メールアドレスが不正利用されることによる、不安感・プライバシーの毀損（機密性の欠如）を与えることになる。 | **実証における対策**  ・利用可能な候補者を限定する  ・利用規約で制御する    **本番おける対策**  ・アプリ内にチャット機能を用意することで、個人情報がシステム内で交換されることを防止する。 |

## 2-7. 大規模・商用・社会実装時の対応方針

本事業が大規模に社会実装される際には、負荷増加による大きく二つの課題が考えられる。

* **マッチングシステムの処理速度低下とサーバーダウン**
  + プロセッシングシステムで秘密計算をして計算結果をマッチングシステムに反映している間は、リソースの多くが秘密計算に割かれるため、マッチングシステムのレスポンスタイムが低下

また一時的なイベント等によるユーザーアクセス集中によるダウン

* **プロセッシングシステム（秘密計算場所）の処理速度低下とサーバーダウン**
  + 1ユーザーごとに秘密計算実行する際30秒-1分程度かかり、実行回数が嵩むと処理速度が低下
  + イベント等によるアクセス増長から秘密計算の負荷増加によるダウン

このような課題を引き起こす可能性のある利用規模の想定と、課題に対する現時点でのシステム・運用方針を以下でまとめる。

【**社会実装時に想定する利用規模**】

以下は将来的に社会実装された際の利用想定者およびトラフィックをまとめたものである。また、利用規模の変数は現時点での目標数値や目安となる数値である。変数の精緻化は今後商用利用の戦略を検討する際に詳細に検討する方針である。

**想定アクセス数/日（合計）：**

* 6,140 - 12,280アクセス/日
  + 参加企業: 140 -280アクセスを想定
    - 50（社）x 70% x 4（回）～ 50（社）x 70% x 4（回）x 2
  + ベトナム学生&社会人: 6,000 - 12,000アクセスを想定
    - 3000（人）x 50% x 4（回）～ 3000（人）x 50% x 4（回）x 2

**変数①想定利用ユーザー数（2025年度内における現時点の目標数値）：**

* 採用企業: 50社（学生よりは限定的）
* ベトナム学生＆社会人: 3000人

**変数②アクセス数に影響する仮説：**

* 採用企業のアクティブ率：70％
* 求職者のアクティブ率：50％
* 1ユーザー当たりの平均セッション数：4回/日
* 季節によるアクセス数の変動率：ピーク時で通常の2倍
  + 採用活動は特定の時期（例えば新卒採用のシーズンや年度末）に集中する傾向があり、これを考慮に入れる

**秘密計算実行回数：**

* 300 - 600回/日
  + 3000（人）x 50% x 20% ～ 3000（人）x 50% x 20%x 2

**変数①秘密計算実行回数に影響する仮説**

* 求職者のアクティブ率：50％
* 季節によるアクセス数の変動率：ピーク時で通常の2倍
* アクティブ利用者の内応募する（秘密計算実行する）人の割合：20%

【**課題に対する運用方針**】

上記の利用規模を鑑みた際に、マッチングシステムとプロセッシングシステムの処理速度低下とサーバーダウン双方の課題に対しては、以下の対応方針で対処できると考えている。

**対応方針：**

* 上記2つのシステムの処理速度低下に対しては、基本的にはサーバーのスケールアップをすることで対処できると考えている。
* 具体的には、CPUコアを1コアから2コアへといったように増強していく方針である。また左記の利用規模では、対応コストとしても問題ないと考えている。
* さらに、サーバーダウンを引き起こす原因となり得る一時的なアクセス増加に対しては、事前にロードバランサーの暖機申請を行う、インフラの運用体制を強化するといった対策を実施する方針である。

今後の残論点としては、現時点では、商用利用時の戦略は十分に練れておらず、利用規模算出の変数は今後より精緻化し、実際に必要なシステム対応方針を検討する必要がある。

# 3.ネイティブアプリ設計の対象スコープおよび要件

## 3-1. ネイティブアプリの設計目的

### 目的1: 個人のプライバシー情報を保護するための安全なデータ管理を実現

ネイティブアプリ設計の最も重要な命題として「個人のプライバシー情報を保護するための安全なデータ管理を実現すること」がある。個人でのデータ管理を実現するという上では、ブロックチェーンを利用した分散的なデータ管理が有効であるが、一方でブロックチェーン上に記録されたデータは特性上削除することができず、個人にとって保持していることが望ましくない成績データを削除できる権利、いわゆるGDPR（EU一般データ保護規則）における「忘れられる権利」は担保されていない。そのため、個人でデータ管理をしながらも、必要に応じてデータ削除が行える要件を実現するためのデータ管理の方法として、候補者の「個人情報」と「成績データ」を暗号化 & 分割化して、ブロックチェーンとデータベースに保存するといった、分散型システムを設計する。

#### 「忘れられる権利」と「ブロックチェーンの矛盾」とその解決策

GDPRには個人のデータ保護に関する7つの主要な権利が含まれている。これらの権利は以下の通りである。

|  |  |
| --- | --- |
| **権利** | **詳細** |
| **情報へのアクセス権** | 個人は自分に関するデータが収集されているか、どのように使用されているかを知る権利がある。 |
| **訂正の権利** | 不正確な個人データの訂正を求める権利がある。 |
| **削除の権利** | 特定の条件下で自分の個人データの削除を要求する権利がある。  「忘れられる権利」とも呼ばれる |
| **処理の制限の権利** | 特定の条件下でデータの使用を制限する権利がある。 |
| **データの携帯性の権利** | 自分のデータを一つのサービスプロバイダーから別のサービスプロバイダーに移動する権利がある。 |
| **異議申し立ての権利** | 特定の条件下で個人データの処理に異議を唱える権利がある。 |
| **自動決定作成とプロファイリングからの保護** | 自動化された意思決定プロセスやプロファイリングに基づく法的または同様に重要な効果を持つ決定から保護される権利がある。 |

これらの権利の文脈で、ブロックチェーン技術とGDPRの関係には特に注意が必要である。ブロックチェーンはデータの不変性を特徴とし、一度記録されたデータの変更や削除が困難である。これはGDPRの「忘れられる権利」と矛盾する可能性がある。

そのため、ブロックチェーンの透明性を保ちつつGDPRに準拠するシステム設計が重要となる。解決策として、IGSが以前行っていたSTARプロジェクトで実現した暗号化方式およびブロックチェーンと中央管理ストレージサービスを連携したデータ保存形式を利用することで、ブロックチェーンの透明性を保ちつつGDPRに準拠するシステムを実現することが可能となる。

### 目的2: 候補者に対するUI/ UXの提供

実証開発のスコープにおいては、企業担当者に対するUI/UXはWebアプリで提供するが、候補者に対するUI/UXの提供はなかった。そのため、今回のネイティブアプリにおいては、候補者に対するUI/UXを提供することが大きな目的となる。以下は、候補者の体験の概要である。実際のアプリのワイヤーに関しては、ネイティブアプリのUI/UXの章で説明を加えていく。

**体験プロセス概要**

* 候補者は、各自のスマホにネイティブアプリをインストールする。
* 候補者はネイティブアプリのタブ一覧から、マッチングのタブを選択することができる。
* タブを選択すると、採用マッチングシステムにエントリーすることが可能である。
* エントリーが終了すると、企業担当者とのマッチングが自動的に開始される。
* 候補者は、企業担当者からアプリ経由でオファーを受け取ることができる。
* オファーの内容は、オファー金額と自由記載のメッセージの2つで構成される。
* 候補者はオファー内容をもとに、マッチングするかしないかを選択することができる。
* マッチングすると候補者は企業担当者とアプリ内チャットでやり取りを開始する。

### 目的3: エントリーシステムの機能の代替

実証開発のスコープにおいては、候補者が採用マッチングシステムにエントリーする機能は提供しておらず、代替策として以下を行っていた。

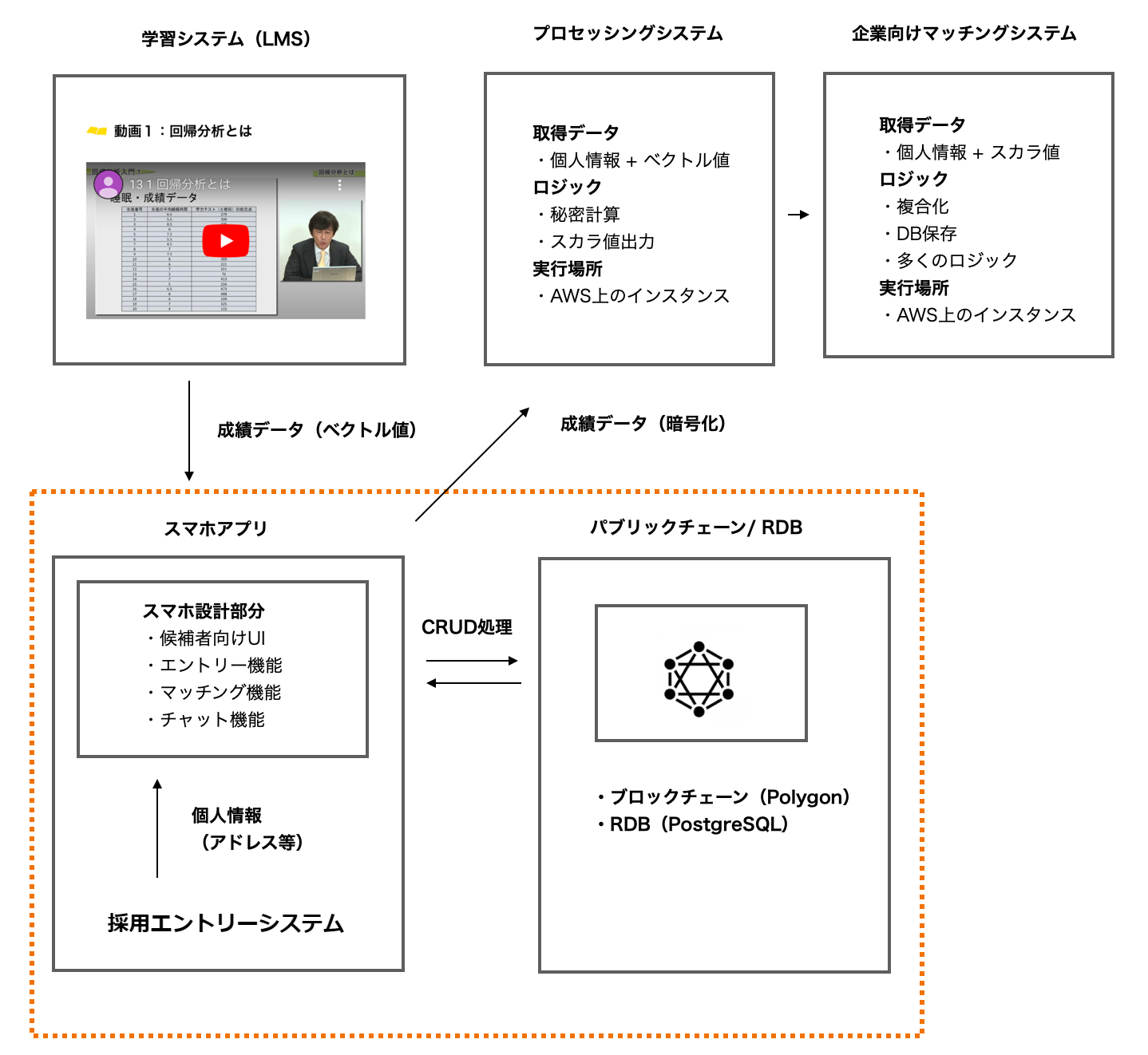
* Webアプリ提供元企業（IGS）が、候補者の個人情報、および成績データ（ベクトル値）を収集。
* 上記データをCSV形式で整理。
* ローカルPCでDockerを用いてエントリーシステムを立ち上げる。
* エントリーシステムに対して、IGSの担当者がCSVをアップロードする。
* 個人情報や成績データが暗号化され、プロセッシングシステムに送信される。

このように、エントリーシステムは候補者にとって、サービス利用の起点となる位置付けとなる。しかしながら現状、煩雑なプロセスを要する。このプロセスをネイティブアプリで代替していくのが、アプリ設計の3つ目の目的である。

## 3-2.ネイティブアプリの全体スコープおよび採用技術

### ネイティブアプリの位置付け

 今回設計の対象となるネイティブアプリは、Trusted WebのWebアプリのシステム全体の中の一部のシステムという位置づけになる。



### 設計の対象となるスコープとスコープ外

**ネイティブアプリ設計のスコープ**

* ネイティブアプリで取得する個人情報および成績データ（ベクトル値）に関しては、アプリ上で候補者が入力するのではなく、学習管理システム（LMS）から取得する。このLMSから取得するデータの一連の処理プロセスおよび提供するユーザー体験を明確化していくことが、基本的な設計のスコープとなる。
* 上記システムから取得した個人情報および成績データは、パブリックチェーンおよびDBに保存される。具体的なパブリックチェーンおよびDBの仕様および技術選の背景、処理のユースケース等に関しては、別途基本設計書等を参照。

**設計のスコープ外**

* 会員登録機能やログイン機能といった機能はリリース済みアプリに実装済みであるため、設計上考慮しない。
* 成績データ（ベクトル値）はエントリーシステムを通じてPSに送信され秘密計算が実行されるが、こちらの仕様に関しては別途Web版の要件定義書/ 基本設計書に記載があるため、設計書に含めない。

### ネイティブアプリ採用技術

選定理由に関しては、ネイティブアプリ基本設計書を参照

|  |  |
| --- | --- |
| **採用技術** | **技術概要** |
| Swift | iOS向けのアプリケーションの開発言語 |
| Kotlin | Android向けのアプリケーションの開発言語 |
| Lattigo | 準同型暗号を実装するためのOSSライブラリ（Go言語） |
| gomobile | 上記LattigoをSwift, Kotlin から使えるようにするために使用するバインディングツール |
| polygon | イーサリアムのスケーリングソリューション、そしてレイヤー2として開発されたプロトコル、及びフレームワーク |
| AWS | アマゾンが提供するクラウドサービスの総称 |

## 3-3.ブロックチェーンとRDBを連携した暗号分割管理方式による安全な保存

ブロックチェーンとリレーショナルデータベース（RDB）を連携した暗号分割管理方式を活用し、安全なデータ保管を実現する。この目的は、データの安全保管にとどまらず、オフチェーン情報の正確な取得、データ削除の確実性、第三者への提供証明が含まれる。また、削除要請後に情報漏洩が発生した場合の契約違反を証明する機能も提供する。これらの追跡情報もブロックチェーンに記録される。なお、ブロックチェーンとRDBに個人情報+成績データを暗号分割保存するかどうかは、以下のように、候補者が任意で設定することができる仕様を想定している。

* 個人情報 + 成績データを暗号化および分割化して「ブロックチェーンとRDB」に保存するかどうかは、ユーザーが任意で設定することができる。
* 候補者は「ブロックチェーンとRDB」への保存設定をせずとも、マッチングシステムにエントリー可能
* 候補者は「ブロックチェーンとRDB」への保存設定していない状態で、マッチングシステムを利用する場合、データはLMSとエントリーシステムのDBでCRUD処理される。
* 候補者が「ブロックチェーンとRDB」への保存設定をすると、データは「ブロックチェーンとRDB」に暗号化 & 分割保存され、LMSとエントリーシステムからデータ（個人情報 + 成績データ）は削除される
* 候補者が「ブロックチェーンとRDB」の保存設定をすると、今後のCRUD処理は、BCとRDB経由で実行される。

### 技術選定の背景

設計開始当初は、ブロックチェーンとIPFS（=分散型ストレージ）を用いる予定であった。しかしながら現状のIPFSの仕様上、データを完全に削除することが困難なため、GDPRの「忘れられる権利」に完全に対応することは困難である。そのため、RDB（=リレーショナルデータベース）の選択が望ましいと考えられる。RDBは、データの厳密な管理と削除が可能であり、GDPRの要件を満たすことができる。

しかし、ブロックチェーンの透明性と分散化の利点を活かすためには、削除機能を保証する分散ストレージサービスが将来登場した場合には、RDBからの切り換えが必要である。

※ 技術選定の検討プロセスの詳細に関しては、ネイティブアプリ基本設計書を参照。

### 機能概要

このシステムの主要な機能は、ブロックチェーンとRDBを組み合わせた暗号分割管理方式を用いて、プライバシー情報の安全な取得、保管、提供を行うことに特化している。ここでは、それぞれの機能の概要に焦点を当てて解説する。また、このシステムは、プライバシー情報の管理に関する最新のニーズに応え、運営側とユーザー双方の視点から、データ保護と利便性のバランスを最適化することを目指している。

※ 各機能のシーケンス図および詳細ロジックに関しては、ネイティブアプリ基本設計書を参照。

|  |  |
| --- | --- |
| **機能概要** | **詳細** |
| **1.プライバシー情報の取得** | 最初のステップとして、システムは既存のサーバーからプライバシー情報を取得する。このプロセスでは、情報のセキュリティとプライバシーを保ちながら、必要なデータのみを効率的かつ正確に抽出することが重要である。 |
| **2.ブロックチェーンへの情報格納** | プライバシー情報取得後、それらはブロックチェーンと連携したRDBに安全に格納される。ブロックチェーンの不変性と分散型の特性は、情報の安全性と透明性を高め、データの改ざんや漏洩のリスクを最小限に抑える。 |
| **3.既存サーバーの情報削除** | データがブロックチェーンと連携したストレージに正常に格納された後、原則として既存のサーバーからは該当するプライバシー情報が削除される。これにより、データの重複管理のリスクが軽減され、サーバー側のデータ保護の負担が減少する。 |
| **4.情報の解凍と提供** | ブロックチェーンと連携したRDBに格納された情報は、必要に応じて解凍され、適切な条件下で第三者に提供される。このプロセスは、ユーザーの同意とセキュリティ基準に従って行われ、データのプライバシーを維持しながら、その価値を最大化する。 |
| **5.情報の完全削除** | 最終的に、ブロックチェーンと連携したストレージに保管された情報が不要になった場合、システムはそれを削除する機能を提供する。これは、データのライフサイクル管理を完全に支配し、ユーザーのプライバシー権を尊重する上で不可欠である。 |

## 3-4.ネイティブアプリの機能要件

候補者向けに提供する画面は主に以下の4つの要素で構成される。

* エントリー画面と付随する機能
* オファーおよびマッチング状況のステータス表示画面
* 候補者と企業担当者間のメッセージ機能
* 候補者アカウント設定機能

以下それぞれの要素におけるネイティブアプリの主要な機能の概要について説明をしていく。

※ ワイヤーフレームおよび詳細の詳細に関しては、ネイティブアプリの基本設計書を参照

|  |  |
| --- | --- |
| **機能概要** | **詳細** |
| **エントリー機能** | * 候補者はエントリー機能を起点に、採用マッチングシステムにエントリーすることが可能。 * エントリーするためには、利用規約に同意する必要性がある。 * また、エントリー機能を利用できるのは、エントリーするための条件を満たした候補者のみである。条件を満たさない候補者に対しては「エントリーできません」といった文言のみが表示され、エントリーすることはできない。 |
| **ステータス表示機能** | * 候補者は希望年収、マッチング済み企業、候補者にオファー申請をした企業情報を閲覧することができる。 |
| **マッチング機能** | * 候補者はオファー申請企業リストから企業名をクリックするとオファー画面に推移し、企業名とオファー金額に加えて、メッセージを閲覧することができる。 * 候補者がマッチング許可をすると、マッチング成立画面が表示され、企業担当者とメッセージを開始することができる。 |
| **メッセージ機能** | * メッセージ画面では、マッチング済みの候補者と企業担当者が自由にアプリ上で面談日時や条件のすり合わせなどのやり取りをすることができる |
| **データ設定機能** | * 本機能を通じて、候補者は成績データの企業に対する開示許可の設定をすることができる。 * 本機能を通じて、候補者は成績情報が含まれているコースデータを削除することができる。 |

## 3-5. ネイティブアプリの非機能要件（サポート環境）

* IOS要件
  + iPhone（iOS 13.0以降）
  + iPod touch（iOS 13.0以降）
* MAC OS要件
  + Mac（macOS 11.0以降とApple M1以降のチップを搭載したMacが必要）
* Android 要件
  + 9 以上

## 3-6. ネイティブアプリのリスク分析と対応方針

### ①秘密鍵管理における法的規制周りのリスク

ネイティブアプリで行うデータの暗号化と複合化には、秘密鍵の管理が必要である。特に、秘密鍵の用途や運用される国・地域の法律によっては、サーバー上での秘密鍵の管理に「カストディ（Custody）ライセンス」が必要になることがある。これは一般的なデータ管理には関係ないものの、暗号資産や価値が結びついたブロックチェーンのキー管理では、規制が厳しくなる傾向にある。

### ②秘密鍵管理における法的規制周りの対応方針

基本的に本ユースケースでは、秘密鍵の管理はユーザー自身が行うので、カストディライセンスは必要としない。しかしながら、秘密鍵の管理に関わる法的要件を遵守するためには、運用される国や地域の法律を十分に理解し、必要なライセンスを取得することが重要である。そのため、暗号資産やブロックチェーンに関連する特定の規制に精通した法律顧問の協力のもと、定期的にレビューし、必要な対応方針を検討する。

### ③秘密鍵への攻撃と盗難のリスク

秘密鍵への攻撃と盗難は、データ漏洩や不正アクセスなどの大きなリスクをもたらす。本ユースケースでは、秘密鍵で管理している成績データ自体が暗号・分割化して保存することができ、アルゴリズムが特定されなければ、データの公開自体は問題にはならない。しかしながら、不正アクセスによる偽の成績データなどの情報操作は学習者にとって学習歴が改ざんされる大きなリスクとなる。

秘密鍵への主な攻撃手法には以下のようなものがあり、対応方針が必要である。

* ブルートフォース攻撃: 秘密鍵を無作為に試行して解読を試みる。
* ソーシャルエンジニアリング: ユーザーを騙して秘密鍵を明かさせる。
* 物理的盗難: 端末の盗難による秘密鍵の直接的な漏洩。

### ④秘密鍵への攻撃と盗難リスクに対するネイティブアプリのセキュリティ特性を生かした対応方針

#### セキュリティ特性

1. **端末内処理**: 大部分の処理が端末内で完結するため、外部へのデータ露出が少ない。
2. **制御された環境**: スマートフォンOSはアプリの動作を厳格に制御し、一定レベルのセキュリティを提供する。
3. **オフライン利用**: ネットワークに接続していない状態でも機能する。

#### リスク

1. **物理的アクセス**: 端末の紛失や盗難によるデータ漏洩。
2. **マルウェア**: アプリ経由での攻撃。
3. **システムレベル脆弱性**: OSの脆弱性によるセキュリティへの影響。

ネイティブアプリのセキュリティ特性とリスクに基づいた対応方針が以下である。

1. **端末内処理の強化**: 最も信頼性が高い方法は、秘密鍵を端末内にのみ保存し、外部とのデータ交換を最小限に抑える。ただし、Metamaskのような標準的なシステムとの連携には、秘密鍵の共有が必要な場合もあるため、最低限の連携機能は必要と考える。
2. **強化されたセキュリティ管理**: OSレベルでのセキュリティ機能（例：サンドボックス環境、アクセス権限の制御）を利用して、アプリ内の秘密鍵を保護。
3. **オフライン機能の最大化**: ネットワークに依存しない秘密鍵管理機能を提供することで、リモート攻撃のリスクを低減。

ただし、スマートフォンアプリケーションには、アップデートの遅延やプラットフォーム異存という問題も存在し、以下のように対処する方針。

1. **自動アップデートの推進**: ユーザーが常に最新のセキュリティ対策を利用できるよう、アプリの自動アップデートを促進する。
2. **幅広いプラットフォームサポート**: 互換性の問題を防ぐため、多様なOSやデバイスに対応するように、アプリを設計する。

### ⑤内部アルゴリズムの解析リスク

また、ネイティブアプリの内部アルゴリズムが解析されるリスクもある。このリスクは、特にセキュリティに敏感なアプリケーションでは重要な懸念事項である。アプリの内部ロジックやデータ処理方法が露見することで、セキュリティの脆弱性が発見されたり、悪意のある攻撃が計画される可能性がある。

### ⑥内部アルゴリズムの解析リスクの対応方針

**コードの難読化 （Obfuscation）:** ソースコードを解析しにくくするために、変数名、関数名、クラス名を変更したり、プログラムの構造を意図的に複雑にする。難読化はコードの直接的な理解を困難にし、解析作業を手間がかかるものにする。

**バイナリ保護 （Binary Protection）**: 実行ファイル自体を保護する手法で、リバースエンジニアリングやメモリダンプを防止する。これは、アプリがデコンパイルされるのを難しくすることで、内部アルゴリズムの露見を防ぐ。

**動的実行 （Dynamic Execution）**: 一部のコードやアルゴリズムをサーバー上で実行し、その結果のみをアプリに返す方式。これにより、アルゴリズム全体がアプリ内部に存在しないため、解析されるリスクを軽減する。

**セキュリティテストと監視 （Security Testing and Monitoring）**: 定期的なセキュリティテストを行い、アプリの脆弱性を特定して修正する。また、異常な動作や攻撃の兆候を検知するために、実行中のアプリを監視する。

**アップデートとパッチ管理 （Updates and Patch Management）**: セキュリティ上の脆弱性が発見された場合、迅速にアップデートやパッチを適用して修正する。ユーザーに対しても常に最新版を使用するよう促す。

## 3-7. 大規模・商用・社会実装時の対応方針

ネイティブアプリ開発において、大規模なユーザー数を考慮した場合、ネイティブアプリ特有の対応方針は以下のようなものがある。（Webアプリにおける対応方針と重複する部分は割愛。）

* ネイティブ**アプリのキャッシュ機構**
  + ネイティブアプリ開発の際に、使用するライブラリ等を経由してデータの取得などを行う時、キャッシュを活用することでデータの再取得回数を減らし、バックエンドサーバの負荷の軽減やユーザーエクスペリエンスの向上が見込まれる。
* **プッシュ機能の効果的な活用**
  + プッシュ機構を通じて、セグメント分けしたユーザーに対して適切に通知を送信し、ユーザーエクスペリエンスを高めることができる。適切に利用すれば、ユーザーの行動を促し、結果として大規模ユーザーの行動を分散させ、サーバーへの負荷を減らす用途としても活用できる。
* ネイティブ**アプリからDBやストレージへのアクセスの設計についての工夫**
  + ネイティブアプリからバックエンドのDBやストレージからデータを取得する際、ネイティブアプリから直接データを取得する実装方法と、必ずバックエンドサーバを経由する方法が考えられる。両者においてそれぞれメリットやデメリットが存在するため、それらを簡潔に記述する。

|  |  |  |
| --- | --- | --- |
| **アクセス設計** | **メリット** | **デメリット** |
| ネイティブアプリから直接データを取得する実装方法 | 1. **低遅延:**    * 直接データを取得することで、データの転送に関する余分な遅延が発生しにくくなる。 2. **シンプルなアーキテクチャー:**    * バックエンド経由でなく直接ストレージ等にアクセスすることで、アプリのアーキテクチャーがシンプルになる。 | 1. **セキュリティのリスク:**    * 直接データを取得する場合、セキュリティ上の懸念が生じる可能性がある。特に、アプリ内での悪意ある変更や不正なアクセスが検知されない限り、認証なしでデータにアクセスできることになる。 2. **統制が難しい:**    * データの取得がクライアントサイドで行われるため、サーバーサイドでのセキュリティポリシーの変更やアップデートが効果的に適用されにくい。 |
| ネイティブアプリがバックエンドサーバを経由してデータを取得する実装方法 | 1. **セキュリティの確保:**    * データの取得をバックエンド経由にすることで、バックエンドで認証や権限管理を行い、セキュリティを確保しやすくなる。 2. **制御可能なアクセス:**    * バックエンドを介してデータを取得することで、サーバーサイドでの制御が容易になり、アクセス権やポリシーの変更が簡単に適用できる。 | 1. **遅延:**    * クライアントからリクエストがバックエンドを経由するため、データ取得に関する遅延が生じる可能性があり、特に大規模なファイルやネットワーク遅延がある場合に影響が大きくなる。 2. **コストの増加:**    * バックエンドを介してデータを取得する場合、直接取得するよりもコストが高くなる可能性がある。 |

今回、ネイティブアプリは設計にとどまるため、実際の対応方針については開発実装時にプロジェクト全体予算も鑑みながら、上記を考慮して決定するものとする。