クライアント証明書配布用Webシステム

要件定義書

第0.6版

株式会社システムアイ

目次

[1. 業務要件 1](#_Toc85038510)

[1.1. 背景 1](#_Toc85038511)

[1.2. 用語の定義 1](#_Toc85038512)

[1.3. システム化される業務 1](#_Toc85038513)

[1.3.1. システム化される範囲 2](#_Toc85038514)

[1.3.2. システム化されない範囲 2](#_Toc85038515)

[2. 機能要件 3](#_Toc85038516)

[2.1. 機能一覧 3](#_Toc85038517)

[2.2. 各機能の要件 3](#_Toc85038518)

[2.2.1. 代理店用機能 (クライアント証明書配布システム) 3](#_Toc85038519)

[2.2.2. 管理者用機能 (クライアント証明書管理システム) 4](#_Toc85038520)

[3. 非機能要件 5](#_Toc85038521)

[3.1. システム化方式要件 5](#_Toc85038522)

[3.1.1. システムアーキテクチャ 5](#_Toc85038523)

[3.1.2. アプリケーションアーキテクチャ 5](#_Toc85038524)

[3.1.3. 動作保証ブラウザ 6](#_Toc85038525)

[3.2. 規模要件 6](#_Toc85038526)

[3.2.1. サーバ台数 6](#_Toc85038527)

[3.2.2. ユーザ数 6](#_Toc85038528)

[3.2.3. 同時接続数 6](#_Toc85038529)

[3.2.4. データ量 6](#_Toc85038530)

[3.3. 性能要件 6](#_Toc85038531)

[3.4. 信頼性要件 6](#_Toc85038532)

[3.4.1. 可用性 6](#_Toc85038533)

[3.4.2. 稼働率 7](#_Toc85038534)

[3.4.3. 完全性 7](#_Toc85038535)

[3.5. 拡張性要件 7](#_Toc85038536)

[3.5.1. リソース利用率 7](#_Toc85038537)

[3.5.2. AWS Lambda 7](#_Toc85038538)

[3.5.3. Amazon Aurora 7](#_Toc85038539)

[3.6. 継続性要件 7](#_Toc85038540)

[3.7. 情報セキュリティ要件 7](#_Toc85038541)

[3.8. 監視 7](#_Toc85038542)

[3.9. バックアップ計画 8](#_Toc85038543)

[3.10. 運用要件 8](#_Toc85038544)

[3.10.1. 前提条件 8](#_Toc85038545)

[3.11. 保守要件 8](#_Toc85038546)

[3.11.1. 障害対応 8](#_Toc85038547)

[3.11.2. 連絡先 9](#_Toc85038548)

[3.11.3. 責任範囲 9](#_Toc85038549)

改訂履歴

|  |  |  |
| --- | --- | --- |
| 版数 | 発行日 | 改訂内容 |
| 0.1 | 2021年8月17日 | 新規作成 |
| 0.2 | 2021年8月25日 | 非機能要件追記 |
| 0.3 | 2021年8月27日 | 外部レビュー指摘対応 |
| 0.4 | 2021年8月31日 | 規模要件、運用要件、保守要件追記 |
| 0.5 | 2021年9月25日 | パスワード変更機能追記 |
| 0.6 | 2021年10月13日 | 社名変更対応  動作保証ブラウザ追記 |
|  |  |  |

# 業務要件

## 背景

2021年12月以降、ENEOSの代理店がENEOSの各システムにログインするにあたって、クライアント証明書が必要となる。

当初の計画だと、このクライアント証明書の配布は、証明書をCD化して郵送で実施する予定であったが、ENEOSでんきの20,000強の代理店に対して郵送で証明書を発行するとなると、多大なる時間、あるいは人的コストの消費が予想される。このため、2021年12月までにクライアント証明書の発行サイトを構築し、郵送にまつわるコストの削減を図る。

## 用語の定義

本資料では、便宜上、名称を下記に統一する。

|  |  |
| --- | --- |
| 用語 | 説明 |
| 代理店 | 本システムにおいてクライアント証明書を利用する利用者を指す。 |
| ENEOS | 営業、あるいはカスタマーセンターなど、代理店と接触し、証明書を管理する主体者を指す。ここには、ENEOSと直接契約しているカスタマーセンターのパートナーも含む。 |
| システム管理者 | ENEOSシステムズ、ならびにENEOSシステムズの指揮により本システムの運用を行うパートナーを指す。 |

## システム化される業務

本システムにおいて、システム化される業務を下記とする。

|  |  |  |
| --- | --- | --- |
|  | 業務内容 | システム化される機能 |
| 1 | 代理店からENEOSに向けてのクライアント証明書の利用申請 | * クライアント証明書の利用申請 |
| 2 | ENEOSから代理店に向けてのクライアント証明書の配布手続き | * クライアント証明書のダウンロード |
| 3 | ENEOSから代理店に受けてのルート証明書の配布手続き | * ルート証明書のダウンロード |
| 4 | 代理店からENEOSに向けてのクライアント証明書の再発行申請 | * クライアント証明書の再発行申請 |
| 5 | ENEOSから代理店に向けてのクライアント証明書の失効手続き | * クライアント証明書の失効 |

これらを実施するために、下記の項においてシステム化する範囲、ならびに機能を記載する。

### システム化される範囲

本システム開発において、主にシステム化されるのは以下の範囲となる。

1. 代理店に証明書を配布するシステム
2. 代理店に配布する証明書を管理するシステム

|  |  |  |
| --- | --- | --- |
| システム範囲 | 画面 | 機能 |
| 1. 代理店に証明書を配布するシステム | ログイン画面 | 代理店用ログイン |
| トップページ | 代理店用ログイン維持(セッション保持) |
| 代理店用代理店情報取得 |
| 代理店用クライアント証明書申請 |
| 代理店用クライアント証明書ダウンロード |
| 代理店用ルート証明書ダウンロード |
| パスワード変更画面 | 代理店用パスワード変更 |
| 1. 代理店に配布する証明書を管理するシステム | ログイン画面 | 管理者用ログイン |
| トップページ | 管理者用ログイン維持(セッション保持) |
| ユーザ管理画面 | 管理者用代理店作成 |
| 管理者用代理店情報取得 |
| 管理者用代理店更新 |
| 管理者用代理店削除 |
| 管理者用代理店検索 |
| 管理者用クライアント証明書失効 |

### システム化されない範囲

本システムには、様々な事情により実装できない業務が存在する。現時点で想定される機能について、対応を記載する。

1. ENEOSがクライアント証明書の管理システムにログインするための情報を管理する機能

マスタメンテナンスによってログイン情報を管理する。

1. ENEOS、あるいは管理者が代理店のパスワードを直接閲覧する機能

セキュリティの観点から本機能は実装しない。

1. ENEOS、あるいは管理者が代理店のクライアント証明書を直接取得する機能

セキュリティの観点から本機能は実装しない。

1. 代理店情報を一括情報登録・一括情報管理を行う機能

マスタメンテナンスによって各種情報を一括管理する。

1. 代理店、あるいは管理者に通知を送信する機能

本機能は実装しない。

1. エラーログ以外の各種情報集計

本機能は実装しない。

# 機能要件

## 機能一覧

|  |  |
| --- | --- |
| 機能ID | 機能 |
| AGENCY\_01 | 代理店用ログイン |
| AGENCY\_02 | 代理店用ログイン維持(セッション保持) |
| AGENCY\_03 | 代理店用代理店情報取得 |
| AGENYY\_04 | 代理店用クライアント証明書申請 |
| AGENCY\_05 | 代理店用クライアント証明書ダウンロード |
| AGENCY\_06 | 代理店用ルート証明書ダウンロード |
| AGENCY\_07 | 代理店用パスワード変更 |
| ADMIN\_01 | 管理者用ログイン |
| ADMIN\_02 | 管理者用ログイン維持(セッション保持) |
| ADMIN\_03 | 管理者用代理店作成 |
| ADMIN\_04 | 管理者用代理店情報取得 |
| ADMIN\_05 | 管理者用代理店更新 |
| ADMIN\_06 | 管理者用代理店削除 |
| ADMIN\_07 | 管理者用代理店検索 |
| ADMIN\_08 | 管理者用クライアント証明書失効 |

## 各機能の要件

### 代理店用機能 (クライアント証明書配布システム)

* AGENCY\_01 代理店用ログイン
* 設計によって定める情報を用いて、代理店がクライアント証明書配布システムにログインする。
* 設計書に定める回数、ログインに失敗するとアカウントがロックされる。
* 1度アカウントがロックされた後、設計書に定める期間が経過するとアカウントのロックは解除される。
* AGENCY\_02 代理店用ログイン維持(セッション保持)
* AGENCY\_01によるログイン操作を行った状態を前提とする。
* 設計によって定める一定期間の間、ログイン状態を維持する。
* 一定期間が経過すると、ログイン状態を破棄する。
* AGENCY\_03 代理店用代理店情報取得
* AGENCY\_01と AGENCY\_02 によって、代理店がログインしている状態を前提とする。
* ログイン状態にある代理店の情報を取得する。
* AGENCY\_04 代理店用クライアント証明書申請
* AGENCY\_03 によって、代理店がログインしている代理店の情報を持っていることを前提とする。
* クライアント証明書の発行に必要な証明書の署名リクエスト（CSR）を生成する。
* 生成された CSR を元に、指定された認証局に対してクライアント証明書の申請を行う。
* 代理店が発行されたクライアント証明書をダウンロード可能な状態とする。
* 生成された CSR とダウンロード可能になったクライアント証明書の取り扱いについては、設計にて記載する。
* AGENCY\_05 代理店用クライアント証明書ダウンロード
* AGENCY\_04 によってクライアント証明書がダウンロード可能な状態になっていることを前提とする。
* 設計によって定める手段により、クライアント証明書をダウンロードする。
* AGENCY\_06 代理店用ルート証明書ダウンロード
* AGENCY\_01と AGENCY\_02 によって、代理店がログインしている状態を前提とする。
* 設計によって定める手段により、ルート証明書をダウンロードする。
* AGENCY\_07 代理店用パスワード変更
* AGENCY\_01と AGENCY\_02 によって、代理店がログインしている状態を前提とする。
* 設計によって定める手段により、パスワードを変更する。

### 管理者用機能 (クライアント証明書管理システム)

* ADMIN\_01 管理者用ログイン
* 設計によって定める情報を用いて、ENEOS、あるいはシステム管理者がクライアント証明書管理システムにログインする。
* ログイン可能なPC、あるいはネットワークに対して、設計によって定める制限を与える。
* ADMIN\_02 管理者用ログイン維持(セッション保持)
* ADMIN\_01によるログイン操作を行った状態を前提とする。
* 設計によって定める一定期間の間、ログイン状態を維持する。
* 一定期間が経過すると、ログイン状態を破棄する。
* ADMIN\_03 管理者用代理店作成
* ADMIN\_01と ADMIN\_02 によって、管理者がログインしている状態を前提とする。
* クライアント証明書配布システムで扱える代理店情報を新規に登録する。
* ADMIN\_04 管理者用代理店情報取得
* ADMIN\_01と ADMIN\_02 によって、管理者がログインしている状態を前提とする。
* 設計によって指定される代理店の情報を取得して画面上に表示する。
* ADMIN\_05 管理者用代理店更新
* ADMIN\_01と ADMIN\_02 によって、管理者がログインしている状態を前提とする。
* 設計によって指定される代理店の情報を更新する。
* ADMIN\_06 管理者用代理店削除
* ADMIN\_01と ADMIN\_02 によって、管理者がログインしている状態を前提とする。
* 設計によって指定される代理店の情報を削除する。
* 既に代理店によってクライアント証明書の発行申請が行われていて、かつダウンロード可能な状態である場合、代理店が発行申請を行ったクライアント証明書を強制的に失効する。
* 代理店によってクライアント証明書がダウンロードされていても、この失効処理を行うと利用できなくなる。
* ADMIN\_07 管理者用代理店検索
* ADMIN\_01と ADMIN\_02 によって、管理者がログインしている状態を前提とする。
* 設計によって指定される情報を元に検索を行い、代理店情報の一覧を表示する。
* ADMIN\_08 管理者用クライアント証明書失効
* ADMIN\_01と ADMIN\_02 によって、管理者がログインしている状態を前提とする。
* 代理店によって発行されたクライアント証明書を強制的に失効する。

# 非機能要件

## システム化方式要件

### システムアーキテクチャ

クラウド基盤「AWS」上に構築し、PaaSを積極的に採用する。

システムの全体構成は別紙の「システム構成図(クライアント証明書配布用Webサイト)」を参照のこと。

### アプリケーションアーキテクチャ

本システムではアプリケーションを以下に従って新規開発する。

|  |  |  |  |
| --- | --- | --- | --- |
| 種別 | 言語 | フレームワーク | 備考 |
| フロントエンド | HTML |  |  |
| CSS |  |  |
| TypeScript | React |  |
| バックエンド | TypeScript | Node.js | バージョンは14とする |
| SQL |  |  |

### 動作保証ブラウザ

本システムの動作保証ブラウザは以下の通りとする。

* 代理店用機能

Windows10：Microsoft Edge、Google Chrome、Firefox、Internet Explorer11

MacOS：Safari

Android：Google Chrome

iOS：Safari

* 管理者用機能

Windows10：Microsoft Edge、Internet Explorer11

※ 動作確認バージョンは2021年10月1日時点の最新バージョン

## 規模要件

### サーバ台数

クラウド基盤を使用するため、サーバ台数等の機器数は定義しない。

ただし、冗長化は考慮した構成とする。

### ユーザ数

利用者数は4万代理店を見込む。

（既存代理店の約2倍）

### 同時接続数

4万代理店が同時にアクセスしても表示に遅延が発生したりシステムが利用不可にならないよう、Webサイト及びクライアント証明書を発行できるシステム基盤とする。

本システムではWebサイトを表示するアーキテクチャに1秒間あたり250,000リクエストまで受けることが可能であるAWSマネージドサービスのCloudFrontを採用する。

### データ量

データ量は4万代理店の情報を格納可能な容量を確保する。

クラウド製品を使用しデータ容量は容易に追加可能なため、明確なデータ容量を定義せず必要に応じた容量を都度、追加する。

## 性能要件

目標値は以下とする。

* 通常時のレスポンスタイム：3秒以内

## 信頼性要件

### 可用性

障害が発生した場合にも本システムを稼働し続けられるよう、冗長構成をとり待機系への切り替えを実施するなどシステムを停止させない構成とする。

### 稼働率

目標とする稼働率は「99.9%」と定める。

ただし、本システムで利用するAWS製品自体の稼働率は公表値に準拠する。

### 完全性

データの改変や損失を防止するため、以下のような対策を行う。

* 機器の故障によるデータ損失を防ぐため、データベースを冗長化させる等の対策を講じる。
* 異常なデータ処理によるデータ改変を防ぐため、入力チェック等の対策を講じる。
* データの紛失や改ざんを検知した際に復旧できるようにバックアップを定期的に取得する。

## 拡張性要件

### リソース利用率

リソース利用率が常時、80%以上（※）となった場合、メモリ/CPUなどのリソース追加を行う。

* リソース設定を変更する目安となる閾値については、申込PWAにて実施しているデータベースCPU使用率監視の設定値に準拠する。

### AWS Lambda

Lambdaに設定するメモリの値は512MB（※）を指定する。

※ 「ＥＮＥＯＳでんきWEBアプリ」の設定値と同値

### Amazon Aurora

本システムのデータベースは申込PWAで利用しているAmazon Auroraに専用のスキーマを作成するが、システムリリース時にインスタンススペックの変更は実施しない。システム運用保守開始後、性能不足によるインスタンススペック変更を実施する場合、申込PWAの運用保守状況を考慮した上で対応する。

## 継続性要件

「ＥＮＥＯＳでんきWEBアプリ」に準ずる。

『ENEOSでんき既存客向けアプリ要件定義書（1.0版）』を参照のこと。

## 情報セキュリティ要件

本システムの利用ユーザはID、パスワードによる認証方法を用いる。

利用ユーザのパスワードは不可逆暗号化した上でCognitoに保存することとする。

その他の要件については「ＥＮＥＯＳでんきWEBアプリ」に準ずる。

『ENEOSでんき既存客向けアプリ要件定義書（1.0版）』を参照のこと。

## 監視

本システムと申込PWA環境で利用する同一リソースについては、既に申込PWA運用保守で監視を実施しているため、既存の設定箇所への監視設定は追加しない。

新規リソース及び設定箇所については、要否を確認した上で、監視設定を追加する。

システムの致命的な不具合や障害を検知するためログを取得し、要否を確認した上で、監視設定を追加する。

## バックアップ計画

本システムで採用するデータベースについては、申込PWAで利用中のAmazon Auroraであるため、自動で定期バックアップ（1日１回、9世代分）を取得するよう設定済みであり、バックアップ取得に関する設定追加は実施しない。

## 運用要件

### 前提条件

本システムの運用にかかわる前提条件を下記に記す。

|  |  |
| --- | --- |
| 項目 | 定義内容 |
| システム稼働時間(AWS環境) | 24時間365日 ※ただしAWSの障害により、アクセス不可となる可能性がある。 |
| システム稼働時間(クライアント証明書配布用Webシステム) | 24時間365日（計画停止時間帯を除く） |
| 運用作業範囲 | システムで利用するクラウド基盤全般 |
| 運用作業 | システム監視業務  システム定例作業全般  システム障害対応に関する業務全般  構成、変更管理などの管理業務全般 |

本システムの運用にかかわる内容については、上記のような条件を基に、設計工程にて以下を具体的に検討・調整し、運用保守設計書にまとめる。運用計画については基本設計以降に策定する。

|  |  |
| --- | --- |
| 項目 | 定義内容 |
| システム運用時間(クライアント証明書発行Webシステム) | システムリリース後、安定稼働をしてからの運用業務を実施する時間帯 |
| システム利用可能時間(クライアント証明書発行Webシステム) | 代理店がクライアント証明書発行Webシステムにアクセスして証明書を発行できる時間帯 |

また、下記にその他条件を述べる。

システム運用者は、瑕疵等について本システムにて問題が発生した際には、速やかに原因の究明を行い、提供サービスに支障が起こらないよう、協力と支援を行うこと。その他、瑕疵一般については、契約書に準拠する。

システム運用者は、秘密保持について本業務で知り得た秘密事項などを第三者に開示もしくは漏洩しないものとし、秘密事項の扱いには十分な注意と配慮を行うこと。

## 保守要件

### 障害対応

ＥＮＥＯＳでんきWEBアプリの開発時と障害発生時の対応に変更が無いため、『ENEOSでんき既存客向けアプリ要件定義書（1.0版）』に準ずる。

### 連絡先

障害を確認した場合、監視担当者は速やかに運用担当者及び責任者に連絡すること。

なお、担当者については設計工程以降で詳細を決定する。

### 責任範囲

ＥＮＥＯＳでんきWEBアプリの開発時とAWSを利用する際の責任分界点に変更が無いため、『ENEOSでんき既存客向けアプリ要件定義書（1.0版）』に準ずる。