認証用データ統合プログラムの作成
仕様書

１．目的

日本原子力研究開発機構（以下、「機構」という）では、研究開発業務の遂行のため、情報機器を機構ネットワークに接続して、機構外及び機構内の情報機器間で様々な通信が行われている。機構ネットワークは、情報セキュリティ対策強化及び利便性向上のため、接続する情報機器についてIPアドレス申請システム（以下、「IPDB」という）を用いて申請を行い、申請情報に基づき承認された情報機器のみ接続を許可するための接続認証システムや、利便性を向上させるためのDHCPサーバの運用を行っている。

これらシステムに登録する情報は膨大となるため、手動での作業は不可能であることから都度プログラムを作成してきたが、プログラム毎にコードのばらつきがあることや利用してきたフレームワークの開発が終了したことを受け、老朽化対策及びコードの統一化のため、それらプログラムを統合する。

２．仕様範囲

(1) プログラム設計

本仕様書に基づいて作成要件を取りまとめ、当機構担当者の確認を得てから、本プログラムの設計を行うこと。なお、プログラムは「3.(1)動作環境」に示すサーバにて動作させること。プログラムを作成するにあたっては、現在の環境の言語・フレームワークを利用するか、現環境の動作に仕様が出ないことを前提に、別の言語・フレームワークを利用して設計することも可とする。

(2) プログラム作成

プログラム設計に沿って本プログラムについて作成を行うこと。

(3) DB設計・構築

プログラム設計に沿ってデータベース設計・構築を行うこと。

(4) インストール・動作確認

作成したプログラムを当機構担当者が指示する仮想環境にインストールし、動作確認を行うこと。

(5) 書類の作成

書類として、プログラム設計書及び操作説明書の作成を行うこと。

３．動作環境及びクライアント環境

(1) 動作環境

仮想環境構成

CPU：6CPU

メモリ：16GB

ソフトウェア構成

- OS：Red Hat Enterprise Linux8.1
- DB：PostgreSQL
- Webサーバ：Apache2
- 開発言語：PHP
- フレームワーク：cakePHP

(2) クライアント環境

・本システムは、以下のクライアント環境での動作を想定している。

- OS：Windows11
- WWW ブラウザ： Microsoft Edge、Firefox、Chrome

４．仕様

4.1 管理機能

(1)管理画面

①ログイン画面を用意し、ID 及びパスワードによるログインを可能とすること。また、その際に IP アドレスでのアクセス制限を可能とすること。

②ログイン後のポータル画面を作成し、必要な機能へのリンクを持たせること。

③ポータル画面の機能として、取り込んだデータの確認、データ生成出力の設定、セグメント情報とプロファイル情報の紐づけ設定、取り込み時間の設定、重複情報表示、パスワード変更が可能な画面を作成すること。

④取り込んだデータの確認画面では、指定したホスト数まで表示し、それ以上のホストについては複数のページ形式で表示できるようにすること。なお、指定するホスト数は可変とし、ページ指定も可能なこと。

⑤データ生成出力の設定画面では、4.3 に記述するデータ生成機能ごとにデータの出力順を指定する機能を持つこと。なお、MAC 認証用データについては、取り込む地区に関する情報を指定可能とすること。また、生成するファイルの名称を指定可能なこと。その他、ARP 認証用データに関する指定期日後の削除に関する日数の設定を可能とすること。

⑥セグメント情報とプロファイルの紐づけの設定画面では、4.2 に記述するネットワークセグメント情報とプロファイル情報及び VLAN-ID を紐づけ可能な機能を持つこと。なお、CSV によるインポート、エクスポート機能を持ち一括編集も可能とすること。

⑦取り込み時間の設定画面では、4.2 に記述するデータ取り込み処理の時間及び 1.3 に記述するデータ生成機能ごとにそれぞれ取り込み処理する時間を指定できるようにすること。時間は複数指定可能とすること。

⑧重複情報表示画面では、同一のネットワークセグメント内で重複した有線、無線 LAN 毎に MAC アドレスが存在するかを表示する機能を持つこと。また、地区内に MAC アドレスの重複が存在するかを表示する機能を持つこと。比較に当たり MAC アドレスの表記は異なる場合があることを考慮して処理すること。

⑨パスワードの変更画面では、ログインしたユーザごとにパスワードの変更をすることが可能なこと。また、管理者としてユーザ情報の追加を可能とすること。

4.2 データ取り込み機能

(1)IPDB データ取り込み処理

①IPDB にアクセスし、以下のテーブルから、本プログラムに必要な情報を取得し、予め設計・構築したデータベースにデータを格納すること。

・IP アドレス申請情報（約 30,000 レコード）
・IP アドレス申請情報 2（約 600 レコード）
・無線 LAN 情報（約 33,000 レコード）
・DNS 情報（約 20 レコード）
・ゲートウェイ情報（約 600 レコード）

・地区情報（約 50 レコード）

②ゲートウェイ情報を基に CIDR 形式の情報を生成し、データベースに格納すること。また、「4.2 管理処理」に示す CIDR 形式の情報と機構が指定するプロファイル名と紐づけた情報も併せて格納すること。

③②については、「4.3 データ生成機能(1)IG2 用データの生成」における有効なネットワークセグメント情報のフラグを設定可能とすること。

(2)ARP 認証用データ取り込み処理

①ARP 認証用システム（以下、「IG2」という）にアクセスし、IG2 より出力された ARP 認証用ファイル（以下、「IG2 出力データ」という）を取得すること。

4.3 データ生成機能

(1)IG2 用データの生成

①「4.1 管理機能」において指定したデータ生成出力順でデータファイル（以下、「IG2 用ファイル」という）を作成することとし、IG2 出力データと「4.2 データ取り込み機能」で取得したデータ（以下、「IPDB 取り込みデータ」という）を比較し、IG2 から出力されるデータにないもの及び一致するものは新データ（以下、「IG2 取り込みデータ」という）として追加すること。

②①にて IG2 出力データに存在し、IPDB 取り込みデータに存在しない場合は、一時データとして指定した日数保持する必要があるため、IG2 用ファイルに追加すること。なお、「4.2 データ取り込み機能」にて作成したデータベースに当該情報を一時データとして記録し、指定した日数が経過する間に IPDB 取り込みデータに再度出現しない限り、指定した日数が経過後、IG2 取り込みデータから削除すること。

③①にて IG2 出力データと IPDB 取り込みデータを比較する際に、IPDB 取り込みデータに「ネットワーク通信不可フラグ」が有効となっている場合は、IG2 用ファイルに追加しないこと。

④同一ネットワークセグメント内で有線/無線 LAN の MAC アドレスが重複した場合は、登録日時の新しい IPDB 取り込みデータの情報を採用すること。

⑤IG2 セクション情報と一致しないネットワークセグメントの情報は「管理外 IP」としてまとめること。

⑥IG2 用ファイルは CSV 形式で作成すること。

(2)DHCP サーバ用データの生成

①「4.1 管理機能」において指定したデータ生成出力順でネットワークセグメント用データファイル（以下、「DHCP ネットワークセグメントファイル」という）を作成することとし、IPDB 取り込みデータのネットワークセグメント情報をファイルに追加すること。

②「4.1 管理機能」において指定したデータ生成出力順でホスト用データファイル（以下、「DHCP ホストファイル」という）を作成することとし、IPDB 取り込みデータの無線 LAN 申請されたデータのみデータを追加すること。

③DHCP ネットワークセグメントファイルおよび DHCP ホストファイルはそれぞれ CSV 形式で作成すること。

④生成したファイルを指定するサーバの Web 管理画面に Curl 等を用いてアップロードすること。

⑶MAC 認証用データの生成

①「4.1 管理機能」において指定したデータ生成出力順で MAC 認証用データファイル（以下、「MAC 認証データファイル」という）を作成することとし、IPDB 取り込みデータ及びセグメント情報とプロファイルの紐づけ情報に基づき MAC アドレス毎にプロファイル情報を追加すること。

②同一ネットワークセグメント内で有線、無線 LAN の MAC アドレスが重複した場合は、その両方を登録すること。

③MAC 認証データファイルは XML 形式で作成すること。

4.4　インストール

新仮想環境に対し、「３．動作環境及びクライアント環境」を基に必要な環境の構築を行ったうえで、プログラムをインストールすること。

4.5　作業上の留意点

⑴ 本契約に基づく作業を行うに当たっては、当機構と十分に協議を行い、作業内容について当機構の確認を得ること。なお、協議の内容は議事録としてまとめ、協議後 5 営業日以内に提出して当機構の確認を得ること。

⑵ 本仕様要件に含まれていない既存機能に影響が出ないよう十分留意すること。万が一、既存機能に影響が生じた場合は、速やかに既存機能を正常に動作させること。

⑶ 作業等で当機構のネットワークを使用する必要が生じた場合は、事前に当機構の了解を得ること。

⑷ 本作業を実施するにあたり、必要となる資料等がある場合は、その必要となるもの（データ、プログラムソース等）を具体的に提示し、当機構担当者に資料等の提供依頼を行うこと。なお、受注者が求める内容が資料等にまとめられていない場合は自ら調査、確認を行うこと。また、当機構内での調査を必要とする場合は、当機構担当者の了解を事前に得た範囲で受注者自ら調査、確認を行うこと。

⑸ 当機構への提出書類（議事録、実施計画書等）及び会議での使用言語は日本語とする。受注者は日本語に精通しコミュニケーション能力に問題がないこと。

⑹ 現在の仮想環境から新仮想環境への切り替えは機構で行う。切り替えに当たり必要な手順を記載した、切替手順書を作成すること。

５．検査

検査は、現地完成検査を当機構の立ち合いのもと実施する。検査の内容・方法等については、以下のとおりである。なお、検査に当たっては、インストールの 2 週間前までに検査要領書を提出し当機構の確認を得てから実施すること。

⑴現地完成検査

現地据付け調整が完了し受注者の自主検査によって、正常動作を確認後、当機構立ち合いのもと予め確認を受けた検査要領書に基づき実施する。

⑵検査項目

検査は、機能検査を行う。なお、機能検査は、検査要領書に基づき「4.仕様」に示すプログラムが正常に動作することを確認する。

６．納期

令和 8 年 2 月 27 日（金）

７．納入場所

茨城県那珂郡東海村白方 2-4

国立研究開発法人日本原子力研究開発機構

原子力科学研究所　情報交流棟南ウィングネットワーク制御室

８．検収条件

「９．提出資料」に示す納入物件がすべて揃っているとともに、検査要領書に基づき 5 項に示す検査に合格すること。

９．提出資料

(1) 12 特記事項(9)に示す資本関係等に関する書類（契約締結後速やかに）1 部
(2) 12 特記事項(10)に示す実施計画書（契約締結後速やかに）　1 部
(3) 検査要領書（インストール 2 週間前）　1 部（要確認）
(4) 検査成績書（納入時）　1 部
(5) プログラム設計書（納入時）　1 部（要確認）
(6) プログラムソース（納入時）　1 本
(7) 操作説明書　（納入時）　1 部
(8) 議事録（会議終了後 5 営業日以内）　1 部（要確認）
(9) その他当機構が必要とする書類（納入時）　1 部

※上記納入物件は印刷物として納入するとともに、電子ファイルでも納入すること。
媒体には CD-ROM 等を用いること。なお、ページ数の多い資料（例 (5)～(7)）は電子ファイルのみでの納入とすること。

１０．保証

検収後、1 年以内に、当機構の取り扱い上の過失に起因しないプログラムミスなどを発見した場合には、受注者の責任において無償で補修、改修すること。

１１．支給品及び貸与品等

(1) 当機構が本業務の実施に必要と判断した情報機器、備品等については当機構が無償貸与し、消耗品については支給することとする。
(2) 当機構が貸与する情報機器などの機構外への持ち出しは不可とする。
(3) 受注者は、当機構担当者と協議の上、本業務を遂行するために必要な当機構の施設を使用できるものとする。

１２．特記事項

(1) 受注者は機構が原子力の研究・開発を行う機関であるため、高い技術力及び信頼性を社会的に求められていることを認識し、当機構の規定等を遵守し安全性に配慮し業務を遂行しうる能力を有する者を従事させること。
(2) 受注者は業務を実施することにより取得した当該業務及び作業に関する各データ、技

術情報、成果その他すべての資料及び情報を当機構の施設外に持ち出して発表もしくは公開し、または特定の第三者に対価をうけ、もしくは無償で提供することはできない。ただし、あらかじめ書面により当機構の承認を受けた場合はこの限りではない。

⑶ 受注者は業務を実施に当たって、次に掲げる関係法令及び当機構の規程等を遵守するものとし、当機構が安全確保の為の指示を行ったときは、その指示に従うものとする。

①労働安全衛生法

②その他、機構が定める規程、規則等

⑷ 受注者は異常事態等が発生した場合、当機構の指示に従い行動するものとする。

⑸ 受注者は、本業務に係わる情報機器の保全について責任を負うものとする。但し、当機構の責任に帰する事項についてはこの限りでない。

⑹ 受注者は、本業務を行うにあたり、対象設備及びその付属設備並びに関連ソフトウェアについて善良な管理者の注意をもって管理を行うこと。

⑺ 本仕様書に記載されている事項及び本仕様書に記載のない事項について疑義が生じた場合は、当機構と協議のうえ、その決定に従うものとする。

⑻ 技術審査時の問い合わせ先の情報として以下の事項を提示すること。

郵便番号、住所、会社名、担当部門名、担当者（氏名、電話、FAX 番号、e-mail アドレス等）

⑼ 受注者は、組織に係る情報として資本の関係・役員の情報及び本契約の実施場所を、従事者に係る情報として従事者の所属・専門性（情報セキュリティに係る資格・研修等）・実績及び国籍についての情報を記した書類を契約締結後速やかに提出すること（別紙 1 及び 2 の作成例を参照のこと）。なお、提出した内容に変更が生じた場合は、その都度提出すること。

⑽ キックオフ会議として第 1 回目の打ち合わせを、契約締結後 1 週間以内に開催すること。なお、キックオフ会議では、実施計画書（作業概要、作業実施方法、作業工程表、作業体制表）を提出し、納期までの想定する実施計画を説明すること。

１３．情報セキュリティの強化

情報セキュリティの強化に係る取り扱いについては、別紙 3「情報セキュリティ強化に係る特約条項」に定められたとおりとする。

１４．グリーン購入法の推進

⑴ 本契約において、グリーン購入法（国等による環境物品等の調達の推進等に関する法律）に適用する環境物品（事務用品、OA 機器等）が発生する場合は、これを採用するものとする。

⑵ 本仕様に定める提出書類（納入印刷物）については、グリーン購入法の基本方針に定める「紙類」の基準を満たしたものであること。

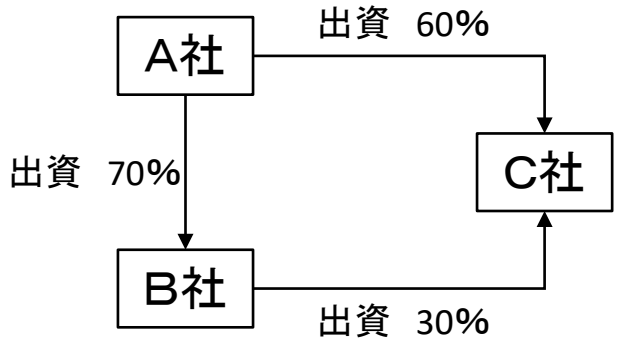
以上

別紙1

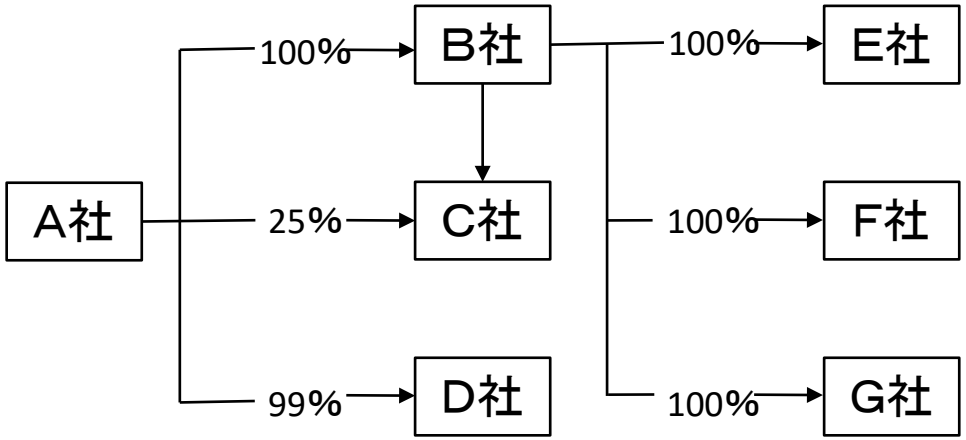
【組織に係る情報の作成例】

資本関係・役員の情報*1・当該契約案件の実施場所を記載のこと。資本関係及び役員の情報についての参考例は下記のとおり。

【資本関係】参考例１



【資本関係】参考例２



【役員の情報】参考例

締役	●●●●	取締役 兼 代表執行役社長
	●●●●	取締役 兼 代表執行役副社長
	●●●●	取締役 兼 ●●●グループ専務執行役員 ●●●●●自動車（株） 取締役社長 ●●●●●（株）執行役員会長
社外取締役	●●●●	社外取締役 ●●●大学●●●●教授 ●●商事（株） 社外監査役 （株）●●●●●社外監査役 （株）●●●●●社外監査役
	●●●●	社外取締役 ●●●●●証券（株）
	●●●●	社外取締役 ●●●●●（株） 代表取締役社長 ●●●●●（株） 社外取締役

＊1「資本関係・役員の情報」については、貴社で一般に公表している情報（例えば、ホームページに掲載している「会社概要」など）があればその写しでも可。

【従事者に係る情報の作成例】当該契約案件従事者の所属・専門性（情報セキュリティに係る資格・研修等）・実績及び国籍についての情報を記載のこと。

別紙2

従事者	所属	専門性	実績	国籍
A(*2)	●●●●●	【情報セキュリティに係る資格】 令和●年●月：●●●●●取得 令和●年●月：●●●●●取得 【情報セキュリティに係る研修】 令和●年●月：●●●研修受講	令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事	日本
B	●●●●●	【情報セキュリティに係る資格】 令和●年●月：●●●●●取得 令和●年●月：●●●●●取得 【情報セキュリティに係る研修】 令和●年●月：●●●研修受講	令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事	日本
C	●●●●●	【情報セキュリティに係る資格】 令和●年●月：●●●●●取得 令和●年●月：●●●●●取得 【情報セキュリティに係る研修】 令和●年●月：●●●研修受講	令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事	●●
D	●●●●●	【情報セキュリティに係る資格】 令和●年●月：●●●●●取得 令和●年●月：●●●●●取得 【情報セキュリティに係る研修】 令和●年●月：●●●研修受講	令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事 令和●年～●年：●●●業務に従事	●●

＊2氏名の記載は不要

別紙3

情報セキュリティ強化に係る特約条項

受注者（以下「乙」という。）は、本契約の履行に当たり、情報セキュリティの強化のため、契約条項記載の情報セキュリティに係る遵守事項に加え、以下に特約する内容を遵守するものとする。

（情報セキュリティインシデント発生時の対処方法及び報告手順）

第１条 乙は、情報セキュリティインシデントが発生した際の対処方法（受注業務を一時中断することを含む。）及び発注者（以下「甲」という。）に報告する手順について整備しておかなければならない。

（情報セキュリティ強化のための遵守事項）

第２条 乙は、次の各号に掲げる事項を遵守するほか、甲の情報セキュリティ強化のために、甲が必要な指示を行ったときは、その指示に従わなければならない。

(1) この契約の業務を実施する場所を、情報セキュリティを確保できる場所に限定し、それ以外の場所で作業をさせないこと。

(2) 業務担当者に遵守すべき情報セキュリティ対策について教育・訓練等を受講させるとともに、業務担当者には甲の情報セキュリティ確保に不断に取り組み、甲の情報及び情報システムの保護に危険を及ぼす行為をしないよう誓約させること。また、業務担当者の異動・退職等の際には異動・退職後も守秘義務を負うことを誓約させ、これを遵守させること。

(3) 暗号化を要する場合は、「電子政府推奨暗号リスト」に記載された暗号化方式を実装し、暗号鍵を適切に管理すること。

(4) 甲の承諾のない限り、この契約に関して知り得た情報を受注した業務の遂行以外の目的で利用しないこと。

(5) 甲が提供する情報を取り扱う情報システムへの不正アクセスを検知・抑止するために、ログを取得・監視し全ての業務担当者についてシステム操作履歴を取得すること。

(6) 甲が提供する情報を格納する装置、機器、記録媒体及び紙媒体について、業務担当者のみがアクセスできるよう施錠管理や入退室管理を行い、セキュアな記録媒体の使用や使用を想定しないUSBポートの無効化、機器等の廃棄時・再利用時のデータ抹消など想定外の情報利用を防止すること。

(7) 情報システムの変更に係る検知機能やログ解析機能を実装し、外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時には、多要素主体認証を要求するとともに定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時の脆弱性対策を行うこと。

(8) システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施するとともに、システムの欠陥の是正及び脆弱性対策等の情報セキュリティ対策が有効に機能していることの継続的な監視と確認を行うこと。

(9) 委任をし、又は下請負をさせた場合は、当該委任又は下請負を受けた者に対して、業務担当者が遵守すべき情報セキュリティ対策についての教育・訓練等を行うこと。

(10) 契約条項に基づき甲が乙に対して行う情報セキュリティ対策の実施状況についての監査の結果、情報セキュリティ対策の履行が不十分である場合には、甲と協議の上改善を行い、甲の承諾を得ること。

(11) 契約の履行期間を通じて前各号に示す情報セキュリティ対策が適切に実施されたことの報告を含む検収を受けること。また、本契約の履行に関し、甲から提供を受けた情報を含め、本契約において取り扱った情報の返却、廃棄又は抹消を行うこと。