ActiveDirectryサーバ構築
仕様書

国立研究開発法人
国立循環器病研究センター
令和7年7月

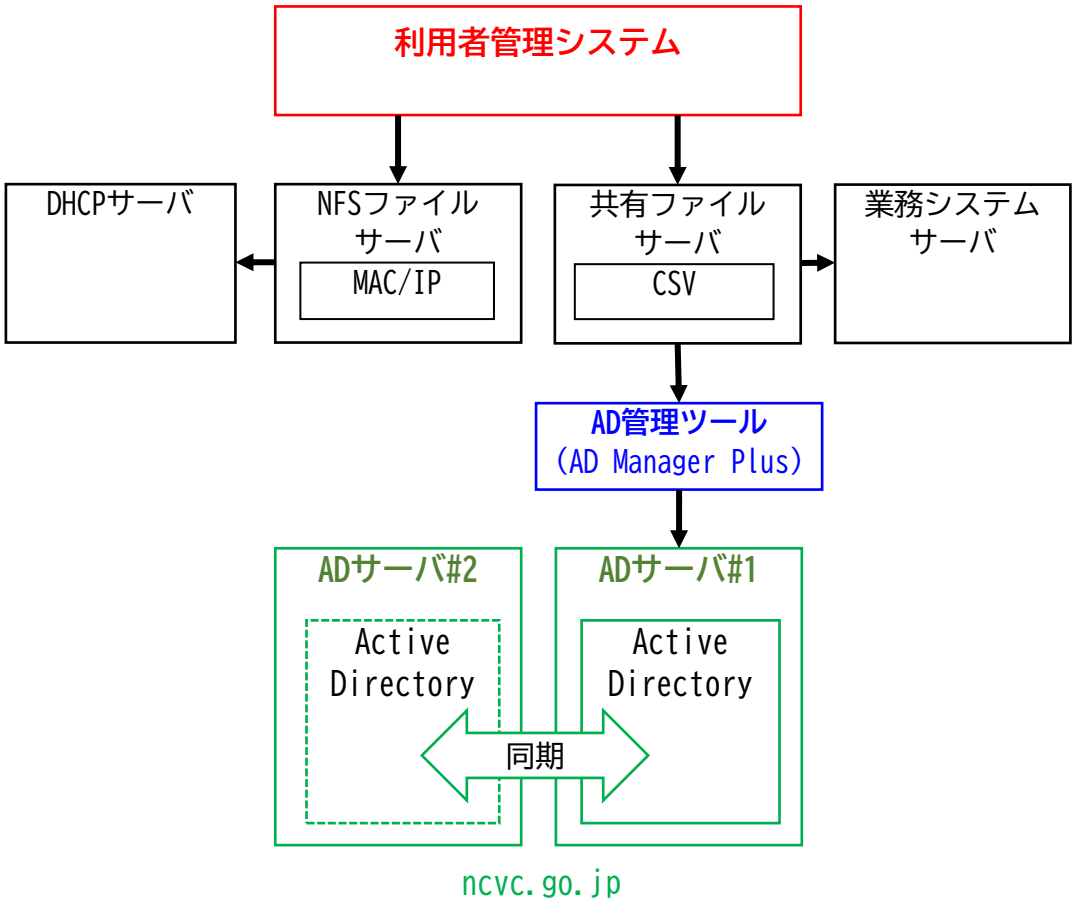
目次

項番	機能要件
A	ActiveDirectryサーバ構築
A.1	基本要件
A.1.1	調達の背景と基本方針
A.1.1.1	国立研究開発法人 国立循環器病研究センター（以下、当センターと称する）は2019年7月の移転を機に更新した情報システム群の多くが2025年12月末を以て契約期間の満了を迎える予定である。本調達対象である利用者管理システムも移転前にMicrosoft365の導入を機に構築したものであるが、現行システムの課題や環境変化に対応したシステムとして新たに構築することとする。
A.1.1.2	認証サーバおよび内部DNSとしてActiveDirectry（以下、AD）を使用しているが、ドメイン変更する必要があり、新しい利用者管理システムと連携するADとして別途新規で構築する。ドメイン変更を機に、M365との連携は停止する。
A.1.1.3	現在のADサーバは当センターが契約するデータセンターにある仮想化基盤で稼働しているが、このデータセンターから撤収する計画があり、新しいADサーバは当センター内のサーバ室の仮想化基盤（以下、当センターの仮想化基盤と称する）に構築を予定している。 なお、当センターの仮想化基盤の仮想化システムはHyper-Vである。
A.1.1.4	ADと別途調達する利用者管理システムおよびAD管理ツールのセットを認証基盤と称する。本調達では認証基盤のうち新ADサーバの構築を対象とする。利用者管理システムからADへの連携はこのAD管理ツールへのcsvファイルの連携にて実現する。全体図を別紙１に示す。なお、AD管理ツールには、ゾーホージャパン株式会社のAD ManagerPlusを採用予定である。
A.1.1.5	この仕様書に定めのない事項が生じた場合、また不明な点が生じた場合等はセンターと受注者で協議し決定することとする。しかし、この仕様書に明記のない場合においても、技術的並びにその性質上当然必要なものについては誠意をもって行うこと。
A.1.1.6	今回調達したものは保守契約を予定している。保守内容は別途協議の上で定めるが、概ね以下を想定している。 ・脆弱性発見時のセキュリティパッチの適用 ・OSやミドルウェアのアップデート ・障害発生時の対応 ・問い合わせ対応
A.1.2	ADサーバ構築要件
A.1.2.1	本調達のシステムは2025年10月末日に納入すること。
A.1.2.2	納入場所は国立研究開発法人 国立循環器病研究センター 大阪府吹田市岸部新町とすること。
A.1.2.3	当センターの仮想化基盤に用意した仮想マシンにOSをインストールし、以下の要件を満たすADを構築すること。なお、本件で構築する仮想Windows Server のOSライセンス(WindowsServer2022)は、当センターが用意する。
A.1.2.4	新しいADサーバは本番系として2台構築し、冗長化すること。またテスト系を1台構築すること。
A.1.2.5	ADは365日24時間稼働（サービス提供）すること。
A.1.2.6	新ドメインとしてncvc.go.jpドメインを設定すること。 ※ 現在も ncvc.go.jpはグローバルドメインとして存在するが、ローカルドメインもこれを用いるよう見直す。なお、現在のローカルドメインであるncvcnet.localは廃止予定だが、新旧ドメインは並行運用する期間がある。
A.1.2.7	新しいADサーバは各業務システムやファイルサーバーのLDAP認証で使用すること。
A.1.2.8	新しいADサーバはRadius認証のバックエンドとして利用すること。
A.1.2.9	新しいADサーバは、ncvc.go.jpドメインを管理する内部DNSとして動作すること。
A.1.2.10	新しいADサーバは、ncvc.go.jp名を管理する権威DNSとして動作すること。
A.1.2.11	新しいADサーバは、各種クライアントから問い合わせが可能なDNSキャッシュサーバとして動作すること。
A.1.2.12	既存の内部DNSは廃止予定であり、新しいADサーバを内部DNSとして利用する際に既存のncvc.go.jpとの関係を矛盾なく整理する必要がある。当センターが主体で検討するがこれを支援すること。詳細は別紙２を参照のこと。
A.1.2.13	ADオブジェクト（ユーザー、コンピューター、グループ、OU）の登録はAD管理ツールを用いて当センターにて行うが、必要時には支援すること。
A.1.2.14	新ドメインのグループポリシーは当センターにて検討の上、AD管理ツールを用いて当センターにて行うが、必要時には支援すること。
A.1.2.15	WindowsUPDATEおよびそれに伴う再起動は夜間に自動で実施すること。またWindowsUPDATEにより生じるテンポラリーのファイルは定期的に自動削除すること。
A.1.2.16	仮想マシンにOSインストール後は、当センターが貸与するVPNを用いて外部から接続しての作業が可能である。その際には、適切な利用申請と報告を行うこと。
A.1.2.17	ADサーバに導入が必要なソフトウェアは今回の調達に含めること。但し、M365 E3に含まれるソフトウェアは当センターにて用意するため含まないこと。
A.1.2.18	利用するソフトウェアについては、無償のオープンソースソフトウェアを積極的に採用し、コスト削減に努めること。但し、セキュリティの確保には留意すること。（利用や年間の保守に高額な費用が発生する製品の採用は避けること。）
A.1.2.19	ADで設定するOUは、原則は既存のADに準拠するが、別途構築する利用者管理システムの仕様に合わせて見直す可能性がある。
A.1.2.20	仮想マシンのシステムバックアップは当センターにて週次で取得する。
A.2	プロジェクト管理

項番	機能要件
A.2.1	プロジェクト管理
A.2.1.1	開札後、2週間以内にキックオフ会議を開き、プロジェクト計画書を提示すること。
A.2.1.2	週に1回は当センターに対し進捗報告および課題の共有を行うこと。対面でもWEB会議でも構わない。
A.2.1.3	システムテスト計画書を作成し、テスト開始までに当センターの承認を得ること。
A.2.1.4	システムテスト結果報告書を作成し、検出された不具合と対応および品質評価を報告すること。
A.2.1.5	本番稼働後の不具合（初期障害）については障害管理を行い、重障害については経緯、原因、対処、根本対策を当センターに報告すること。 ※ 安定稼働後は保守契約に基づく管理とする。
A.2.1.6	納品されたドキュメント、システムは当センターが著作権を留保する。
A.2.2	情報セキュリティ管理
A.2.2.1	「政府機関の情報セキュリティ対策のための統一基準」の最新版及び当センターの情報セキュリティポリシーに準拠していること。なお、当センターの情報セキュリティポリシーが原則的に優先するが、統一基準にある記載内容を考慮したものであることが必要である。
A.2.2.2	受託者は、導入及び保守の期間を通じて、受託業務の実施にあたって計画している情報セキュリティ対策を「情報セキュリティ管理計画書」としてまとめること。本書は契約締結後2週間以内に作成し、当センターの承認を受けること。なお、プロジェクト実施計画書・体制図等の一部としても差し支えない。情報セキュリティ管理計画書には、以下の内容を記載すること。 （必須項目） ・従事者の所属、専門性(情報セキュリティに係る資格・研修実績等)、国籍等 ・従事者が利用するPCの管理方法 ・授受した情報・電子ファイルの管理・廃棄ルール、目的外利用の禁止 ・本受託業務の実施場所 ・インシデント発生時の対応フロー・連絡先 （参考文献） ・「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」 (SBD(Security by Design)) ・「IT製品の調達におけるセキュリティ要件リスト」 ・「ITセキュリティ評価及び認証制度(JISEC)」
A.2.2.3	ソフトウェアの選定に当たっては、サプライチェーン・リスクに配慮すること。調達後新たなサプライチェーン上の脅威が発見された場合には、受注者は当センターに対しかかる脅威についての情報提供を行うこと。 （参考文献） ・「IT製品の調達におけるセキュリティ要件リスト」 ・「ITセキュリティ評価及び認証制度(JISEC)」
A.2.2.4	受注者の資本関係・役員等の情報について情報提供を行うこと。
A.2.2.5	作業の一部又は全部を再委託する場合は、契約前に当センターに許可を求めること。
A.2.2.6	本業務の実施に当たり、成果物に対して意図しない変更が加えられないための管理、および機密情報の窃取等が行われないための管理がされていること。
A.2.2.7	本調達の役務内容を一部再委託する場合は、再委託先に対しても情報セキュリティ管理計画書に準拠した情報セキュリティ対策を実施すること。また再委託先と秘密保持契約を締結すること
A.2.2.8	本業務において、情報セキュリティインシデントの発生または情報の目的外利用等を認知した場合は、速やかに当センターに報告すること
A.2.2.9	情報セキュリティ対策に関する履行状況を再委託先含めて定期的に確認し、当センターへ報告すること
A.2.2.10	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、速やかに改善策を提出し、当センターの承認を受けた上で実施すること
A.2.2.11	当センターが求めた場合に、速やかに情報セキュリティ監査を受け入れること。
A.2.2.12	当センターから要保護情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。
A.2.2.13	当センターから受領する要保護情報、又は当センターのデータが国内法以外の法令及び規制が適用される環境に保存される場合は当センターの承認を受けること。
A.2.2.14	当センターから受領した要保護情報が不要になった場合は、これを確実に返却、または抹消し、書面にて報告すること。
A.2.2.15	当センターが提供する情報(資料等)は、情報セキュリティ管理体制の下、第三者への漏えいや目的外利用が行われないよう、適切に管理すること。
A.2.2.16	納品物に含む運用手順書には、情報セキュリティ水準の維持に関する手順や情報セキュリティインシデントを認知した際の対処手順など情報セキュリティ対策を実施するために必要な手順を含むこと。
A.2.2.17	納品物には、システム構成情報、取り扱う情報の内容、接続するセンター外通信回線の種別、委託先情報を含めること。
A.2.2.18	リモートメンテナンスが必要となる場合は、原則として当センターが提供するVPN環境で接続すること。当センターVPN環境が利用できない場合は、接続方法について当センター情報統括部と協議の上、決定すること。
A.2.2.19	独自のネットワーク（無線LANも含む）を構築しないこと。その必要がある場合は、理由など必要な資料を提示し、当センター情報統括部長の判断を求めること。
A.2.2.20	ネットワークカードの２枚挿しやルータの導入によるネットワーク分離が必須である場合は、その理由や構成図を示して情報統括部長の判断をあおぐこと。

項番	機能要件
A.2.2.21	納入候補となるソフトウェア等については予め当センターにリストを提出すること。当センターがサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、提案の見直しを図ること。
A.2.2.22	情報システムに当センターの意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、当センターと連携して原因を調査し、排除するための手順及び体制(例えばシステムの操作ログや作業履歴等を記録し、要求された場合には提出できるなど)を整備していること。これらの手順書、体制について資料を提出すること。
A.2.2.23	データベース内に格納するデータは暗号化することが望ましい。
A.2.2.24	データベースの管理者アカウントは、情報システム管理者との区別、データへのアクセス要否、委託先を含む管理者権限付与の適切性等を勘案した上で、適正に設定管理すること
A.2.2.25	データベースの操作ログには操作対象データや操作内容を含むこと。
A.2.2.26	主体認証のパスワードは英大文字（26種類）小文字（26種類）＋数字（10種類）＋記号（26種類）の計88種類の文字をランダムに使って10桁以上とすること。また、運用保守段階へ移行するに当たっては利用可能なアカウントやアクセス可能な範囲の見直しを行うこと。不可能な場合はその理由を明確にし、代わりとなる措置をリスク低減策として提案すること。
A.2.2.27	アカウントロックの機能を実装すること。アカウントロックされた場合、管理者へ通知ができ、システム管理者によるロック解除か、一定時間経過でのロック解除を設定可能なこと。不可能な場合はその理由を明確にし、不正な主体認証の試行に対抗するための代替措置をリスク低減策として提案すること。
A.2.2.28	一定回数以上のログイン試行を管理者に通知する仕組みを実装すること。不可能な場合はその理由を明確にし、不正な主体認証の試行に対抗するための代替措置をリスク低減策として提案すること。
A.2.2.29	通信要件を明確にし、OSのファイアウォール機能等を使って、それ以外を使用できないように設定すること。具体的には、通信目的（アプリケーション名）、送信元、送信先、通信プロトコル（ポート番号）を文書で示すこと。
A.2.2.30	情報システムのサーバや端末のOS、その他の端末上で稼動させるソフトウェアは、本稼動時点で最新の修正プログラムやセキュリティパッチを適用の上でシステム動作試験を行い、正常に動作することを検証すること。
A.2.2.31	情報セキュリティ上の問題が発生した際に確認するため、導入するサーバOS及びアプリケーションについてのログを取得すること。
A.2.2.32	システムや機器の納入時に、情報セキュリティ対策の実装状況について確認し、確認結果について情報統括部長への承認を求めること。チェック項目については仕様書にもとづき、構築開始時点で協議により決定する。
A.2.3	納品
A.2.3.1	以下のドキュメントを納品すること。 ・情報セキュリティ管理計画書 ・システム構成図 ・仮想サーバパラメータシート(設計書) ・システムテスト計画書 ・システムテスト結果報告書
A.2.3.2	ドキュメントはMicrosoft 365アプリ(Excel、Word等)で作成できること。
A.2.3.3	ドキュメントおよびスクリプト類をCD-R・DVD-Rまたはオンラインストレージ等を使用し電子媒体で納品すること。

別紙１：認証基盤


利用者管理システム
DHCPサーバ
NFSファイル
サーバ
MAC/IP
共有ファイル
サーバ
CSV
業務システム
サーバ
AD管理ツール
(AD Manager Plus)
ADサーバ#2
Active
Directory
ADサーバ#1
Active
Directory
同期
ncvc.go.jp

別紙２：DNS設定

以下の観点から新旧DNSの相互連携は段階的な切替や切断が必要と考えている。

- 各種新システム/クライアントは、新ADに対しDNSとして問い合わせることになるが、旧DNSに未更新システム分・先行更新システム分・継続システム分が含まれることなどからncvc.go.jpドメイン名は全て引き継ぎが必要と考えている。
- 旧DNSとしては、ncvc.go.jpの他、his.localやncvcnet.local、his.localを更新した新hisドメイン、外部配置のncvc.go.jpの権威DNS、がそれぞれ別サーバとして存在しており、フォワード等が必要となる。

別紙３：現状説明

現在のADの使用状況を以下に示す。規模感などを掴むための概要として取り扱うこと。

- 現在、ADに登録されているユーザー数は約7,000である。
  うち、約1,000は停止中である。

- 現在、ADに登録されている機器は約13,000台ある。
  これらはAD上はオブジェクトクラスをユーザーとして登録されている。
  その際にMACアドレスをcnとしており約20,000件が登録されている。

- 現状でDNSを利用する端末はサーバー、クライアント合わせて同時接続数で約5,500台である。