ユーザ認証基盤関連にかかる情報提供依頼内容の詳細

はじめに

この資料は、三重県（以下、「当県」という。）が実施している「三重県ユーザ認証基盤の構築に係る情報提供依頼」の内、「ユーザ認証基盤関連」にかかる情報提供依頼の内容について、詳細を記載したものです。

三重県ユーザ認証システムにおけるサブシステムの一つである「庁内ドメインシステム」は、Microsoft 社が提供する機能である、ActiveDirectory（以下、「ActiveDirectory」という。）をベースとしてオンプレミス環境にて、構築した認証基盤であり、主に利用者からの認証処理とドメイン内のリソース管理の他、グループポリシー等にてユーザ及びクライアントのセキュリティ管理を行っています。

本資料における**「ユーザ認証基盤」とは、現行の「庁内ドメインシステム」をベースとして機能拡張を行った「庁内ドメインシステム」の後継システム**です。なお、三重県ユーザ認証基盤を構成するサブシステムの一つとして構築予定です。

提案を依頼したい内容については、「１　情報提供を依頼したい内容」を、提案に際して考慮していただきたい項目については、「２　提案に際して考慮いただきたい内容」をご確認ください。

１　情報提供を依頼したい内容

現在利用している庁内ドメインシステムは、平成 16 年度に構築後、機器更新や機能追加等を実施し、現在も運用を行っています。

このシステムは、本県のイントラネット上のオンプレミスの認証基盤として、稼働しているため、特段の理由がない限り、機能を強化したうえで、継続して利用したいと考えています。

そこで、**「現行の「庁内ドメインシステム」の機能を継続しつつ、必要な機能を強化した「ユーザ認証基盤」として使用していくために必要となる作業」と、「それらを実現するために必要となる費用」**等について、**「２　提案に際して考慮いただきたい内容」を踏まえて、情報提供を行っていただくよう**お願いします。

システム名	システムの説明
庁内ドメインシステム	・現行の「三重県行政 WAN ユーザ認証システム」におけるサブシステムの一つ
三重県ユーザ認証基盤	・「三重県行政 WAN ユーザ認証システム」を再構築したもの ・「ユーザ認証基盤」など、複数のサブシステムで構成される
ユーザ認証基盤	・現行の「庁内ドメインシステム」を機能強化した後継システムのこと

表１　本資料内におけるシステムの名称と概要

２　提案に際して考慮いただきたい内容

情報提供を実施いただくに当たり、「（１）現行システムからの継続部分」がベースとなることから、まずは、この部分にかかる提案をいただくようお願いします。そのうえで、「（２）課題解決に何らかの改善提案を要するもの」「（３）新規提案項目」について、可能な範囲で情報提供をいただくようにお願いします。

なお、「（１）現行システムからの継続部分」のみ、又は、その内容の一部のみにかかる提案でも構いません。できる限りの情報提供について御協力をお願いします。

（１）現行システムからの継続部分

現行システムに対して、「ア　現行システムにかかる仕様書」をベースとし、また、「イ　前回調達時の仕様書からの変更点」を踏まえた業務内容に対して提案を行っていただくようお願いします。

なお、現行システム内に、不要な機能や、見直しが必要な機能等があれば、その理由も併せて、提案を行っていただくようお願いします。

ア　現行システムにかかる仕様書

現在利用している「庁内ドメインシステム」の調達にかかる仕様書については、以下の「平成 26 年度三重県行政 WAN ユーザ認証システム設計・機器調達・構築・保守業務委託」における仕様書の内、「庁内ドメインシステム」にかかる記載部分をご確認ください。

現行システム名	左記システムが含まれる業務	仕様書
庁内ドメインシステム	・　平成 26 年度三重県行政 WAN ユーザ認証システム設計・機器調達・構築・保守業務委託	既仕 01～既仕 03

表２　庁内ドメインシステムにかかる仕様書

イ　前回調達時の仕様書からの変更点

前回の調達時から、変更を予定している内容については、以下を参照してください。

- 仕様書内にある、現行システムの概要、機器構成等については、「現シ 01 平成 26 年度三重県行政 WAN ユーザ認証システム設計・機器調達・構築・保守業務委託 基本・詳細・設計書（抜粋）」に記載されている概要、機器構成等に読み替えてください。
- 契約期間として、令和 3 年度中の契約締結、令和 4 年 7 月 1 日からの利用開始、令和 9 年 6 月末日までの保守を行う形を想定してください。
- 利用者として、本県職員数を 6,800 名としてください。

- 三重県行政 WAN の物理構成図において、IDC2 が IDC1 に統合されています。また、大規模単独地域機関数が 8 拠点から 2 拠点（アスト津、総合教育）に削減され、バックアップ回線は全庁舎から IDC1 に接続されています。
- 三重県行政 WAN の論理構成図において、外部 Firewall からインターネットへの経路上に「三重県自治体情報セキュリティクラウド」が構築されており、各種セキュリティ対策を行っています。
- 三重県行政 WAN のネットワーク構成等について、ユーザ認証基盤を構築するために必須と思われる機能が不足していると判断される場合は、本県の責務により、対応を行うことを想定しています。そのため、三重県行政 WAN にかかる構成等の変更を前提とした提案も可としますが、その場合は、変更内容や変更が必要な理由等についても説明いただくようお願いします。
- ActiveDirectory の構成は、シングルフォレスト・シングルドメインです。また、他システムにより構築されたドメインとの間で信頼関係を結んでいます。サイト構成は、シングルサイトです。

（２）課題解決に何らかの改善提案を要するもの

現行の庁内ドメインシステムに対して、「ア　外部環境の変化に対する対応」が求められています。そのため、「イ　ユーザ認証基盤に必要とされる構成の想定」を踏まえて、「ウ　認証機能の強化」から「タ　グループウェア（庁内メール）との連携」までについての内容を実現するための解決方法や必要となる作業、費用等について提案を行っていただくようお願いします。また、現時点で対応が困難なものや、不可能なもの、条件がそろえば対応可能なものなどについても、可能な範囲で情報提供いただくようご協力をお願いします。

提案を行っていただくうえで必要になるライセンス、サービス等について、その機能や利用料など、できるだけ詳細に示していただくようお願いします。なお、複数のサービスを利用することで値引き等が発生する場合は、可能な範囲で値引き前の価格と値引き後の価格を示していただくようお願いします。

ア　外部環境の変化に対する対応

- 平成 27 年 12 月 25 日付総行情第 77 号の総務大臣通知「新たな自治体情報セキュリティ対策の抜本的対策について」により、各自治体のセキュリティ対策として、いわゆる「三層の対策」への対応が要請されました。その後、「自治体情報セキュリティ強化対策事業」により、都道府県単位における「自治体情報セキュリティクラウド」の導入や、各自治体において、三層の構え（個人情報用ネットワーク、LGWAN 系ネットワーク、インターネット接続系ネットワークを分離すること）が構築されることにより、セキュリティ対策が強化されました。

- しかし、セキュリティ対策を高めた反面、ユーザビリティに大きな影響があったこと、また、政府における「クラウド・バイ・デフォルト原則」を受けた新たなあり方を検討する動きがあったことなどを受け、令和 2 年 5 月「自治体情報セキュリティ対策の見直しのポイント」により、効率性・利便性を向上させた新たな自治体セキュリティ対策のモデルとして、従来のαモデル（三層の対策を施した構成）に対して、βモデル、β’モデル（業務端末をインターネット接続系ネットワークへ設置する構成）が示されたところです。
- そのため、本県においても、現行のセキュリティ対策にかかるサービスレベルを維持したまま、クラウドサービス等をシステム構築の選択肢として検討できるようにするための仕組みづくりや、従来のオンプレミス構成では実現できなかった数々の新たな機能をクラウドサービスとして利用できるようにするため、Cisco 社の WebEX、box 社の box などの試行を行ってきたところです。
- その結果、利用自体はできるようになりましたが、ログインするために毎回 ID とパスワードを入力する必要がある（シングルサインオンが実現できていない）、同一ユーザであってもクラウドサービス毎にユーザ情報を重複管理する必要がある、ライセンス管理や利用者確認などに手間がかかる、などの課題が顕在化してきたところです。
- 以上のことから、上述の外部環境の変化や顕在化してきた課題等に対応するため、既存の庁内ドメインシステムを機能拡張し、新たに「ユーザ認証基盤」として再構築を行う必要があると考えています。なお、既存の庁内ドメインシステムにおいては、これまで、イントラ内のユーザやデバイス等の管理を行っており、また、他のシステムとの間で、ID 連携等、多数の連携実績（シングルサインオンが実現できている）があるため、庁内ドメインシステムの機能は継続させる必要があると考えています。そのため、「ユーザ認証基盤」の構築は、庁内ドメインシステムを機能拡張する形を想定していますので、ご注意ください。

イ　ユーザ認証基盤に必要な機能の想定

- 「ユーザ認証基盤」に必要な機能の想定は、以下のとおりです。

機能名	機能等の詳細
全体構成	・現行システムにおける「庁内ドメインシステム」（オンプレミス版の ActiveDirectory）を機能強化し、「オンプレミス版の認証基盤」として再構築したうえで、オンプレミス版の認証基盤と ID 連携が可能な「クラウド版の認証基盤」を新たに構築する。（以下、オンプレミス版の認証基盤とクラウド版の認証基盤を併せて「ユーザ認証基盤」という。） ・「ユーザ認証基盤」は、主に、認証機能、ID 連携機能、アクセス制御機能、ID 管理機能を提供する。

認証機能	・オンプレミス版の認証基盤にて、従前と同等の認証機能を提供する。また、クラウド版の認証基盤において、インターネット上からアクセスする利用者向けの認証機能を提供する。 ・認証を行う端末として、本県資産の端末の他、職員所有端末、スマートフォン、タブレット等のモバイル端末等についても、利用があると想定している。
ID 連携機能	・オンプレミス版の認証基盤とクラウド版の認証基盤の間、また、ユーザ認証基盤と各クラウドサービスの間において、認証情報を連携させることができる ID 連携機能を提供する。 ・さらに、複数の方法によるシングルサインオン機能を提供する。（シングルサインオン機能を実現するためには、ユーザ認証基盤にログイン後、認証された ID 情報に紐づく各クラウドサービスのアカウント情報等を、クラウドサービス側に安全に提供できる機能（ID 連携機能）を有する必要があると想定しています。）
アクセス制御機能	・クラウドサービスやアプリケーション等のアカウント情報等を一元管理し、利用可能なクラウドサービスのみをランチャーのような形で利用できるもののみ表示させる機能を提供する。また、各クラウドサービス内における権限等についても一元的に管理し、制御する機能（ActiveDirectory であれば、セキュリティグループと各種システムを連携させて権限等を管理・制御する機能など）を提供する。
ID 管理機能（ID 同期機能）	・オンプレミス版の認証基盤とクラウド版の認証基盤において、ID 情報等にかかる二重管理の手間や間違い等をなくすため、複数の認証基盤上で設定された ID 情報とその ID 情報に紐づくアカウント情報等の一元管理を可能にする ID 管理機能を提供する。また、複数の認証基盤上で ID 情報等を同期させることができる ID 同期機能を提供する。

表３　ユーザ認証基盤における機能想定

ウ　認証機能の強化

・　認証機能として、現在、既存のオンプレミス版の認証基盤で利用している ActiveDirectory は、「Kerberos」認証が利用できるなど高度な認証機能を提供できますが、NAT を超えられない、インターネット上の利用者から利用するのが難しい、等の理由により、イントラ内での利用に限って使用しています。そのため、インターネット上の利用者から利用が可能なクラウド版の認証基盤について、提案を行っていただくようお願いします。

- クラウド版の認証基盤における「認証」は、インターネット上の利用者からの認証要求を受け付ける形を想定していますが、従来の ID、パスワードによる認証では、パスワードの漏えい等によるなりすましが発生する恐れがあることから、より、高度な認証機能が求められます。そのため、ID、パスワード以外の認証方法として、例えば、「記憶」「所有物」「生体」等の複数の要素による多要素認証、SMS（ショートメッセージングサービス）等を利用した 2 段階認証、パスワード自体を使わない、かつ、インターネット上にパスワードが流れない FIDO2（Fast IDentity Online）などのパスワードレス認証等、について、利用者の利便性とセキュリティ対策を両立できるとともに、運用上、管理者側に過度の負担とならない方法について、情報提供をお願いします。
- 各種クラウドサービスの利用者として、本県職員だけでなく、ゲストユーザとして、市町職員や各種業務における受託事業者、県民の皆様方の利用についても想定されることから、利用者登録時に、なりすましや偽造等による不正な利用者登録を防ぐ仕組みが必要になると想定しています。さらに、利用者登録は、対面ではなく、インターネット経由で実施されるケースが増えてくると想定されることから、インターネット上からの利用者登録申請等に対して、なりすましや偽造等による不正な利用者登録を防ぐための仕組みである eKYC（electronic Know Your Customer）基本認証等の、利用者の利便性を損なわず、かつ、運用上、過度の負担にならない方法について、提案を行っていただくようお願いします。
- 利用者の本人確認方法として、今後、一層の普及が想定されるマイナンバーカードや連携アプリによる「利用者証明サービス」を利用した、さらに厳格な本人確認の方法等について、実現可能な方法があれば、提案を行っていただくようお願いします。

エ　ID 連携機能の強化

- 現在、既存のオンプレミス版の認証基盤は、イントラ内の業務システムと ID 連携を行っており、シングルサインオン機能を実現しています。しかし、既存のオンプレミス版の認証基盤では、インターネット上の各クラウドサービスとの ID 連携やシングルサインオンを実現することができないため、ID 連携等を実現するための方法について提案を行っていただくようお願いします。なお、オンプレミス版の認証基盤において認証を行った利用者だけでなく、「ウ　認証機能の強化」に記載したクラウド版の認証基盤において認証を行った利用者に対しても、同等の ID 連携機能を利用できる形としてください。なお、各種アカウントの管理は、引き続き、オンプレミス版の認証基盤にて実施していく想定のため、ご留意いただくようお願いします。

- クラウドサービスによっては、利用者単位ではなく、所属単位の共通アカウント等での利用が認められている場合もあることから、同一所属内の利用者が共通のアカウントで利用できる機能について提案を行っていただくようお願いします。具体的には、同一所属の利用者は、その所属に割り当てられた共通アカウントにより、各種サービスに対してアクセスするような形を想定しています。ただし、あくまでユーザ認証基盤での認証は、利用者単位で行うものとし、共通アカウントを利用するために、再度認証を実施するような形は避けていただくようお願いします。
- ID 連携実現の方法として、さまざまなクラウドサービスと連携を行えるよう、SAML（Security Assertion Markup Language）、OpenID Connect、フォームによる連携等、さまざまな連携方法に対応しており、かつ、種々のクラウドサービスと連携実績があることが望ましいため、その実例として、3 大クラウドサービス（AWS、Azure、GCP）の他、Microsoft 365、Box、Slack、GoogleWorkSpace 等との連携実績等（逆に、連携していないサービス等があれば連携していない理由等）について、紹介を行っていただくようお願いします。
- 利用者が ID 連携機能により、各クラウドサービスを利用する流れについて、認証機能による認証や、利用可能なクラウドサービスの選択等について、情報提供を行っていただくようお願いします。なお、同一利用者が同じクラウドサービス内に、複数のアカウント（利用者アカウントと管理者アカウント等）を持つ場合が想定されることから、複数のアカウントの切り替え方法についても、併せて情報提供を行っていただくようお願いします。
- ID 連携機能における IdP 機能（ID プロバイダー Identity Provider ID 情報に紐づく各種アカウント情報の一元管理を行う機能）については、オンプレミス版の認証基盤にて対応する形を前提として提案を行っていただくようお願いします。

オ　アクセス制御機能の強化

- 現在、既存のオンプレミス版の認証基盤（ActiveDirectory）の 1 機能である「セキュリティグループ機能」を ID 連携された複数のシステムにおけるアクセス制御機能として利用しています。例えば、Web フィルタリングシステムにおいては、「一般ユーザ」「動画閲覧ユーザ」等のセキュリティグループを権限設定に利用したり、共有ファイルサーバシステムにおいては、三重県の組織を 3 階層モデルとした「部」「所属」「班」単位のセキュリティグループを作成し、同システム内の権限設定に利用したりしています。

・ そのため、引き続き、セキュリティグループによるさまざまな権限管理を行うことを想定していますが、提案をいただくユーザ認証基盤で利用可能なアクセス制御機能の仕組み（セキュリティグループの他、例えば、各種 ID 情報にかかる属性情報、ロール等）等について、提案を行っていただくとともに、実際の利用例や管理方法等についても情報提供を行っていただくようお願いします。

カ　ID 管理機能の強化

・ クラウドサービスにかかる管理・運用業務として、利用者情報の変更等が発生した場合、その利用者が登録を行っている複数のクラウドサービスに対して変更情報等を反映させる作業が発生すると想定しています。また、利用するクラウドサービスの数が増えるにつれ、管理・運用業務にかかる負荷も大きくなると想定しています。そのため、各クラウドサービスの利用者情報や変更情報を、一元的に管理できる ID 管理機能（SCIM　System for Cross-Domains Identity Management）等について、具体的な操作の流れや画面ショットと共に、提案を行っていただくようお願いします。
・ なお、オンプレミス版の認証基盤として、引き続き、ActiveDirectory を利用する想定ですが、ActiveDirectory の機能を拡張することで、複数のクラウドサービスの情報を保持し、その情報を他のクラウドサービス側に対して簡単な操作で一致させることができる ID 同期機能の他、ID 管理を行うために利用できる、他の機能等について、情報提供をいただくようお願いします。

キ　ユーザ認証基盤の必須機能に含めるべき機能

・ ユーザ認証基盤の必須機能として、「認証機能」「ID 連携機能」「アクセス制御機能」「ID 管理機能（ID 同期機能）」としていますが、クラウドサービス等を利用していくうえで、今後の技術動向等の観点から必須機能に含めるべき機能があれば、提案を行っていただくようお願いします。
・ なお、提案をいただく場合は、その費用対効果についても、併せて説明を行っていただくようお願いします。

ク　年度末移行作業

・　毎年度、三重県職員の 1/3 から 1/5 の職員が異動し、かつ、3 月 31 日の夕刻からから翌 4 月 1 日の業務開始までの限られた時間において、年度末移行作業として、全システムにおける異動情報の反映作業や、権限の再設定作業等を実施しています。また、これらの作業は、限られた時間の中で漏れなく、かつ、正確に実施する必要があるため、管理者側の作業として実施する必要があります。そのため、年度末の移行作業を実施するうえで有効な機能等があれば、提案を行っていただくようお願いします。

ケ　他の認証基盤との連携

・　現在、IDaaS（Identity as a Service）として各社が提供するさまざまなサービスが利用可能であり、また、今後、政府、自治体等の他団体においても、IDaaS 機能を備えた認証基盤の整備が進むと想定しています。その結果、利用者は、複数の認証基盤への利用者登録を行うのではなく、IDaaS 間における ID 連携による利用者登録へとシフトしていくと想定しています。そのため、既存の IDaaS との連携実績や、実際の運用方法等について、提案を行っていただくようお願いします。（例えば、本県が提供するサービス（例えば申請サービス）を利用するために、別の IDaaS（政府や民間のサービス）で認証されている利用者について ID 連携を行うことで、本県側の利用者登録を省略し、サービスが利用できる形を想定しています。また、マイナンバーカードや連携アプリによる「利用者証明サービス」を利用した、さらに厳格な本人確認がされている認証基盤と ID 連携を行うことで、厳格な利用者管理が実現できると期待しています。）

コ　LGWAN との連携

・　クラウドサービスには、インターネット上で提供されるものの他に、LGWAN-ASP にて提供されるものも存在します。そのため、ユーザ認証基盤から連携が可能な LGWAN-ASP 上のクラウドサービスがあれば、提案をいただくようお願いします。
・　また、LGWAN 上のサービスと連携を行う上で、注意点、制限事項等があれば、併せて情報提供を行っていただくようお願いします。

サ　テレワークシステムとの連携

・　本県では、インターネット等を経由して、庁内ネットワークに接続を行うテレワークシステムとして、「モバイルワークシステム」と「在宅勤務システム」を導入していますが、それぞれのシステムを利用する際、ID、パスワード等による認証を行っているところです。また、各システムへのログインの他、VDI 環境の利用、リモートデスクトップの利用、画面転送機能の利用等の場面において、何度も認証を行う必要があります。

・ そのため、ユーザ認証基盤と連携可能で、かつ、シングルサインオンが可能なテレワークシステムがあれば、提案をいただくようお願いします。

シ　利用者情報にかかる申請管理

・ ActiveDirectory には、各種アカウントに対する、新規・変更・停止（削除）等の申請を管理するための機能（申請管理機能）が提供されていないため、本県では、「三重県職員アカウント集中管理システム」という各種アカウント管理を行うためのシステムをフルスクラッチで構築しています。
・ 管理を行うアカウントには、ActiveDirectory におけるアカウントの他、パソコン、プリンタ等のデバイス、職員アカウント、所属等の共通アカウント、グループウェアやメール等の各種システム等アカウント等があり、また、これらのアカウントを一元的に管理し、かつ、各種アカウントに対する「申請受付」「審査・承認」「各システムへの反映指示」「利用者へのお知らせ」等の機能も提供しています。さらに、システムによっては、フォーム連携機能によるシングルサインオン機能が利用可能になっているため、多くのシステムが三重県職員アカウント集中管理システムにてアカウント管理を行っています。
・ そのため、引き続き、当該システムの利用を予定していますが、今後、新たに管理を行うことになると想定される各クラウドサービスにかかるアカウント情報等について、三重県職員アカウント集中管理システムに代わる管理方法があれば、提案をいただくようお願いします。

ス　管理者権限の委譲

・ ユーザ認証基盤にて認証を行う利用者として、本県職員だけでなく、外部受託事業者や、県民の皆様についても対象とする想定をしていますが、例えば、特定のサービスを利用するためだけの利用者登録を行う場合、そのサービスを所管する所属にて登録を実施したいというニーズが出てくると想定しています。
・ そのため、上記のニーズに対応するための運用方法等について、提案を行っていただくようお願いします。（具体的には、利用者登録の承認権限、サービス利用の承認権限など、様々な承認権限を複数の管理者ユーザに柔軟に設定（委譲）できるような形を想定しています。）

セ　セキュリティ対策基盤との連携

・ 「依頼内容 02　セキュリティ対策基盤関連にかかる情報提供依頼内容の詳細」に記載されている、各種セキュリティ対策にかかる内容について、ユーザ認証基盤として、関連する内容があれば、提案を行っていただくようお願いします。

・ 特に、攻撃や不審な挙動を検知した後、被害を最小限に食い止めるため、利用者の権限を制限したり、システムの利用を一時停止したりする機能について、提案を行っていただくようお願いします。

ソ　資産管理基盤との連携

・ 「依頼内容 03　資産管理基盤関連にかかる情報提供依頼内容の詳細」に記載されている、資産管理基盤関連について、ユーザ認証基盤として、関連する内容があれば、提案を行っていただくようお願いします。
・ 特に、職員が所有する端末や、スマートフォン、タブレット等のモバイル端末等に対する運用管理を行っていくための MDM（モバイルデバイス管理）等と一元管理を行うことによる業務の効率化等について、提案を行っていただくようお願いします。
・ テレワーク端末等、外部からアクセスを行う機器に対して IT ハイジーン（デバイスに対する衛生管理）を実施する必要があると考えていますが、IT ハイジーンにより、十分な対策が取られていないデバイスに対して、利用可能な機能を制限したりすることができる機能について、提案を行っていただくようお願いします。（例えば、セキュリティパッチの適用等のみが実施できるセグメントにしかアクセスできない、などの機能を想定しています。）

タ　グループウェア（庁内メール）との連携

・ 「依頼内容 04　グループウェア（庁内メール）関連にかかる情報提供依頼内容の詳細」に記載されている、グループウェア（庁内メール）にかかる内容について、ユーザ認証基盤として、関連する内容があれば、提案を行っていただくようお願いします。
・ 特に、職員録やアドレス帳等、グループウェアや庁内メールを管理・運用していくうえで、必要な情報をスムーズに連携できる機能について提案を行っていただくようお願いします。

（３）新規提案項目

現行の庁内ドメインシステムに対して、上述の「（２）課題解決に何らかの改善提案を要するもの」だけでなく、新規の提案として、機能改善、業務量の改善、使いやすさの改善等が実現できるものがあれば、提案を行っていただくようお願いします。