三重県統合認証管理基盤システム設計・機器調達・構築・運用保守業務に係る意見招請
寄せられた意見と三重県の考え方

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
1	詳細仕様書（案）	P23 3　本システムの詳細な機能要件 （２）統合運用管理システム関連 工　脆弱性管理機能/セキュリティパッチ配布機能 （ア）脆弱性管理機能	【記載内容】 ・取得した脆弱性情報を元に、業務端末における脆弱性の有無について確認し、その結果を定期的に自動収集できること。 【意見】 ・取得した脆弱性情報を元に脆弱性に該当する業務端末が把握可能ですが、こちらの対応でも問題ないでしょうか。	・本要件として、取得した脆弱性情報を元にどの業務端末に当該脆弱性情報が存在するかを定期的、かつ、自動的に確認できることとしていますが、この意図としては、得られた結果を元に対象端末を「最新情報」により的確、かつ、「定期的」に抽出したいと考えているためです。 ・いただいた意見として、「業務端末単位ではなく脆弱性単位での把握」で問題ないか？、また、「定期的に自動収集」ができなくても問題ないか？という意図とお見受けしますが、例えば、月に1回以上（緊急時はその都度、回数は要相談）で、かつ、毎回手動で対象端末単位で脆弱性情報を集計して提出いただければ要件を満たすため、記載内容を以下の内容に変更します。 ・ただし、「業務端末における脆弱性の有無について確認」とは、「脆弱性情報が提供されたソフトウェアがインストールされている業務端末を確認」するだけではなく、「脆弱性情報が提供されたソフトウェアの該当バージョンがインストールされている業務端末を確認」する必要がありますので、ご注意ください。（例えば、Edgeの脆弱性情報が提供された場合は、Edgeがインストールされている端末を確認するということではなく、Edgeのバージョン情報等の詳細情報まで確認し、脆弱性が存在する端末のみを抽出いただく必要があります。） ・また、「業務端末単位で脆弱性を集計して提出」とは、脆弱性単位で得られた対象となる業務端末の情報について、業務端末単位として再集計いただくという形になりますので、ご注意ください。 【変更内容】 ・取得した脆弱性情報を元に、業務端末における脆弱性の有無について確認し、その結果を定期的に自動収集できること。または、取得した脆弱性情報を元に、運用業務として、同様の対応ができること。 ----------【関連項目】---------- ・P38「５　業務詳細（６）運用・保守業務の設計にかかる要件　工　受託事業者が行うもの（オ）脆弱性情報による対象端末の抽出」に記載の「・統合運用管理システムにおける「脆弱性管理機能」により取得した脆弱性情報に基づき、脆弱性が存在する業務端末の抽出を行う。」について、以下の内容に変更します。 【変更内容】 ・統合運用管理システムにおける「脆弱性管理機能」「セキュリティパッチ管理機能」により取得した脆弱性情報及びセキュリティパッチ管理機能に基づき、脆弱性が存在する業務端末及びセキュリティパッチを適用すべき業務端末の抽出を行う。なお、脆弱性情報やセキュリティパッチ情報に基づく業務端末の抽出を、システムではなく手動で実施する場合は、「脆弱性情報やセキュリティパッチが提供されたソフトウェアがインストールされている業務端末を確認」するだけではなく、「脆弱性が提供されたソフトウェアの該当バージョンがインストールされている業務端末を確認」や「セキュリティパッチの対象となるソフトウェアの該当バージョンがインストールされている業務端末を確認」し、抽出した結果を本県に対して報告する。また、業務端末ごとに脆弱性の深刻度を集計して報告する。さらに、本県が指定する業務端末に対して脆弱性情報やセキュリティパッチ情報を集計して報告する。 ----------【関連項目】---------- ・P38「５　業務詳細（６）運用・保守業務の設計にかかる要件　工　受託事業者が行うもの（オ）脆弱性情報による対象端末の抽出」に記載の「・少なくとも月に1回以上、対象となる端末がないかについて、抽出を行うこと。」について、以下の内容に変更します。 【変更内容】 ・少なくとも月に1回以上（回数は要相談）、かつ、緊急の脆弱性情報が提供された場合はその都度、対象となる端末がないかについて、抽出を行う。 ----------【関連項目】---------- ・P39「５　業務詳細（６）運用・保守業務の設計にかかる要件　工　受託事業者が行うもの（カ）セキュリティパッチ配布用タスクの作成」に以下の内容を追記します。 【変更内容】 ・少なくとも月に1回以上（回数は要相談）、かつ、緊急の脆弱性情報が提供された場合はその都度、セキュリティパッチ配布用タスクを作成する。	あり
2	詳細仕様書（案）	P23 3　本システムの詳細な機能要件 （２）統合運用管理システム関連 工　脆弱性管理機能/セキュリティパッチ配布機能 （ア）脆弱性管理機能	【記載内容】 ・資産台帳画面において、脆弱性が確認された各業務端末を脆弱性の深刻度に応じてわかりやすく表示できること。（緊急は赤、警告は黄色、問題なしは青など。） 【意見】 ・資産管理画面において、脆弱性が発見されたソフトウェアを脆弱性の深刻度に応じて分かりやすく色分け表示が可能ですが、こちらの対応でも問題ないでしょうか。	・業務端末には、複数の脆弱性が存在する場合があると想定しているため、本要件として、各業務端末における複数の脆弱性に対して、総合的に深刻度として評価した結果を表示し、業務端末の深刻度を見える化することとしていますが、この意図としては、得られた結果を元に対象端末に対して、迅速、かつ、的確な対応を行いたいと考えているためです。 ・いただいた意見として、「ソフトウェアを色分けして表示」とあるため、「資産管理画面」ではなく、各業務端末の詳細画面（例えばインストールされているソフトウェア一覧画面等）での表示で問題ないか？という意図とお見受けしますが、業務端末の一覧上で確認を行いたいという要件のため、提案いただいた形では、要件を満たしません。 ・ただし、重要な脆弱性（例えばOSやブラウザ等）について、緊急パッチがあたっていないといった状態を深刻度として表示したり、運用での対応として、月に1回以上（緊急時はその都度、回数は要相談）で、かつ、毎回手動で対象端末を抽出し、本県に対して一覧情報として深刻度を提出する、といった対応ができれば要件を満たすため、記載内容を以下の内容に変更します。 【変更内容】 ・資産台帳画面において、脆弱性が確認された各業務端末における脆弱性の深刻度や、重要な脆弱性（例えばOSやブラウザ等）への対応状況に応じてわかりやすく表示（緊急は赤、警告は黄色、問題なしは青など。）できること。または、取得した脆弱性情報を元に、運用業務として、同様の対応ができること。 ----------【関連項目】---------- ・（No1と同じ関連項目を修正する。）	あり
3	詳細仕様書（案）	P23 3　本システムの詳細な機能要件 （２）統合運用管理システム関連 工　脆弱性管理機能/セキュリティパッチ配布機能 （イ）セキュリティパッチ管理機能	【記載内容】 ・各業務端末の詳細画面にて、脆弱性に対応するセキュリティパッチ情報を表示できること。 【意見】 ・脆弱性管理画面の詳細画面にて、脆弱性に対応するセキュリティパッチ情報を表示可能ですが、こちらの対応でも問題ないでしょうか。	・業務端末に複数の脆弱性が存在する場合、全ての脆弱性への対応を行うために複数のセキュリティパッチを適用しなければならない場合があると想定しているため、本要件として、各業務端末において対応が必要なセキュリティパッチの全てを見やすく表示することとしていますが、この意図としては、得られた結果を元に1台ずつの業務端末に対して、対応が必要なセキュリティパッチの全てを迅速、かつ、的確に適用したいと考えているためです。 ・いただいた意見として、「脆弱性管理画面の詳細画面」とあるため、「各業務端末の詳細画面」での表示ではなく、それぞれの脆弱性情報に対するセキュリティパッチ情報を表示させることで問題ないか？という意図とお見受けしますが、業務端末単位でセキュリティパッチの一覧を表示させたいという要件のため、提案いただいた形では、要件を満たしません。 ・ただし、運用での対応として、月に1回以上（緊急時はその都度、回数は要相談）で、かつ、毎回手動で対象となる業務端末における全てのセキュリティパッチ情報を本県に対して一覧情報として提出する、といった対応ができれば要件を満たすため、記載内容を以下の内容に変更します。 【変更内容】 ・各業務端末の詳細画面にて、脆弱性に対応するセキュリティパッチ情報を表示できること。または、取得したセキュリティパッチ情報を元に、運用業務として、同様の対応ができること。 ----------【関連項目】---------- ・（No1と同じ関連項目を修正する。）	あり

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
4	詳細仕様書（案）	P23 3　本システムの詳細な機能要件 （2）統合運用管理システム関連 エ　脆弱性管理機能/セキュリティパッチ配布機能 （イ）セキュリティパッチ管理機能	【記載内容】 ・セキュリティパッチの詳細画面から適用対象の業務端末一覧が表示できること。 【意見】 ・脆弱性が確認されたアプリケーション単位に、該当アプリケーションがインストールされている業務端末の一覧が表示可能ですが、こちらの対応でも問題ないでしょうか。	・セキュリティパッチの中には、複数の脆弱性に対応するためのセキュリティパッチ（累積的なセキュリティパッチ）があるため、本要件として、指定したセキュリティパッチについて、適用対象となる全ての業務端末を見やすく表示することとしていますが、この意図としては、累積的なセキュリティパッチの対象端末として、脆弱性情報から対象となる業務端末を一つ一つ確認するのではなく、対応が必要な業務端末の全てを迅速、かつ、的確に把握したいと考えているためです。 ・いただいた意見として、「セキュリティパッチ」毎の表示ではなく、「アプリケーション単位」で業務端末の一覧を表示させることで問題ないか？という意図とお見受けしますが、セキュリティパッチ単位で対象となる業務端末の一覧を表示させたいという要件のため、提案いただいた形では、要件を満たしません。 ・ただし、運用での対応として、月に1回以上（緊急時はその都度、回数は要相談）で、かつ、毎回手動で対象となるセキュリティパッチにおける全ての業務端末を本県に対して一覧情報として提出する、といった対応ができれば要件を満たすため、記載内容を以下の内容に変更します。 【変更内容】 ・セキュリティパッチの詳細画面から適用対象の業務端末一覧が表示できること。または、運用業務として、同様の対応ができること。 ----------【関連項目】---------- ・（No1と同じ関連項目を修正する。）	あり
5	詳細仕様書（案）	P12 2　本委託業務にて解決したい課題 （2）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題 表　IDaaSに求める機能 機能名　アクセス制御機能	【記載内容】 ・アクセス制御機能とは、外部サービス（クラウドサービス）におけるアクセス権限をIDaaSが管理する機能のこと。 ・この機能を利用することで、IDaaSによるアクセス権設定が可能になり、各外部サービス（クラウドサービス）における多種多様なアクセス権をIDaaSにて一元管理することが可能となる。 ・アクセス制御機能は、各IDaaSにてさまざまな形態により提供されているが、管理しやすく、柔軟な運用ができるアクセス制御機能が利用できる必要がある。 【意見】 ・アクセス制御機能として、クラウドサービス単位の利用可否の制御は可能だが、クラウドサービス内の利用者権限の運用方法は別途ご検討いただけないか。	・「アクセス権限をIDaaSが管理する機能」として、各外部サービス（クラウドサービス）内における複数の権限（例えば、利用者権限や管理者権限等）を、IDaaSが直接管理する「アクセス権管理機能」と、接続してきた利用者やその業務端末における状態（セキュリティパッチが当たっているか、社内からのアクセスか、など）により、アクセスできる範囲を制限したり、追加認証を求めたりする「アクセスコントロール機能」がありますが、表現がわかりにくく、また、現時点で必要とする機能についての記載が漏れていたため、記載内容を以下の内容に変更します。 【変更内容】 ・アクセス制御機能には、外部サービス（クラウドサービス）内における複数の権限（例えば、利用者権限や管理者権限等）を、IDaaSが直接管理する「アクセス権管理機能」と、接続してきた利用者やその業務端末における状態（セキュリティパッチが当たっているか、社内からのアクセスか、など）により、アクセスできる範囲を制限したり、追加認証を求めたりする「アクセスコントロール機能」とがある。 ・これらの機能を利用することで、IDaaSによるアクセス制御が可能になり、各外部サービス（クラウドサービス）における多種多様なアクセス権をIDaaSにて一元管理することが可能となる。 ・しかし、アクセス権管理機能は、IDaaSと各外部サービス（クラウドサービス）間で個別の対応を行う必要があるとともに、アクセスコントロール機能についても、業務端末の状態を把握するためのツール（MDMやEDR等）との連携が必要であるため、現時点で利用できなくとも、将来的にこれらの機能が利用できる必要がある。また、現時点での対応として、IDaaSへの再認証を行うことによる利用者権限の切り替え（アクセス権管理機能の疑似的な実現）や、外部サービス（クラウドサービス）単位の利用可否の切り替え（アクセスコントロール機能の簡易的な実現）については、最低限の対応として、利用できる必要がある。	あり
6	詳細仕様書（案）	P18 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細 表　クラウド認証基盤に求める機能 機能名　アクセス制御機能	【記載内容】 ・各外部サービス（クラウドサービス）内における利用権限等についても一元的に管理でき、同画面で表示できること。 【意見】 ・各外部サービス（クラウドサービス）内における利用権限等についても一元的に管理でき、画面を表示できること、と記載があるが、クラウドサービス単位の利用可否の制御は可能だが、クラウドサービス内の利用者権限の運用方法は別途ご検討いただけないか。	・記載内容を以下の内容に変更します。 【変更内容】 ・各外部サービス（クラウドサービス）内における利用権限等について、IDaaSにおける複数のID/アカウントに対して、個々に紐づけることで一元的に管理できること。また、統合認証基盤への再認証等を経ることで、複数の利用者権限の使い分けが実現できること。（例えば、IDaaSへ「利用者01」としてログイン後、クラウドサービスXに対してuser01（利用者権限）として利用後、IDaaSへ「利用者02」として再ログインし、同サービスに対してuser02（管理者権限等）として利用する、といった使い方が実現できること。）	あり
7	詳細仕様書（案）	P17,18 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細 表　クラウド認証基盤に求める機能 機能名　ID連携機能	【記載内容】 ・外部サービス（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、利用者ID/アカウントと外部サービス（クラウドサービス）における共通アカウントを紐づけてID連携できること。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をActiveDirectoryにおける拡張情報等に設定しておくことで、当該サービスにアクセスする際に、利用者のID/アカウントではなく、共通アカウントで利用する形を想定している。ただし、あくまで統合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の再度認証は不要であること。 ・利用者がID連携機能により、各外部サービス（クラウドサービス）を利用する際、同一利用者が同サービス内に、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、再度の認証なしに、複数のアカウントを切り替えて利用できる機能を持つこと。 【意見】 ・共通アカウントの1:N認証利用）と複数アカウントの再度の認証なしでの切り替え利用の運用方法は別途ご検討いただけないか。	・同一外部サービス（クラウドサービス）内における複数アカウントの切り替えについて、クラウド認証基盤への再認証なしに利用できるのが理想ですが、再認証の実施による切り替えについても仕様を満たす形に変更します。そのため、記載内容を以下の内容に変更します。 【変更内容】 ・外部サービス（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を行う場合もあることから、利用者ID/アカウントと共通アカウントを紐づけてID連携が実現できること。具体的には、同一所属の利用者は、当該サービスにアクセスする際に、利用者のID/アカウントではなく、共通アカウントにて利用できるようにできること。なお、統合認証基盤への認証を利用者単位で実施後、将来的には、共通アカウントへの再認証なしに利用できる必要があるが、当面は、共通アカウントによるクラウド認証基盤への再認証を経て、共通アカウントを利用する形も可とする。 ・利用者がID連携機能により、各外部サービス（クラウドサービス）を利用する際、同一利用者が同サービス内に、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）を利用したい場合が想定されるが、この場合は、別の利用者としてクラウド認証基盤における再認証を行うことで、アカウントを切り替えて利用できること。	あり
8	仕様書（案）	P2 2　事業概要 （2）業務範囲 イ　利用者数、業務端末数、業務端末の詳細	【記載内容】 ・利用者数 約6,800人、業務端末数約10,000台を想定すること。また、ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること。 【意見】 ・「追加等軽微な対応」で軽微なという言葉の基準を具体的に記載していただけますか？	・記載内容を以下の内容に変更します。 【変更内容】 ・利用者数 約6,800人、業務端末数 約10,000台を想定すること。また、ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること。なお、「軽微な対応」に含まれないものとして、物理サーバを1台増設する、新たに高額なパッケージソフトを導入する、など、本県の費用負担が高額になる場合を想定しています。	あり
9	仕様書（案）	P6 2　事業概要 （2）業務範囲 カ　現行システムの概要 表　現行システムにおけるサブシステム一覧 サブシステム名 その他システム	【記載内容】 ・現行システムとは別のシステムとして、「三重県職員アカウント集中管理システム」が構築されており、各職員からの申請・受付・承認機能の他、各サブシステムとの連携機能も有している。 【意見】 ・「三重県職員アカウント集中管理システム」も本委託業務の範囲外と解釈いたしますので、P7　※ 現行システムにおける 庁内メールシステム、ウィルス対策システム、 障害監視システムは、本委託業務とは別の事業で再構築を実施するため、本委託業務の範囲外とする 。 　に、「三重県職員アカウント集中管理システム」も本委託業務の範囲外と明文化していただけますか？	・P6「2　事業概要（2）業務範囲　カ　現行システムの概要」における「※現行システムにおける庁内メールシステム、ウィルス対策システム、障害監視システムは、本委託業務とは別の事業で再構築を実施するため、本委託業務の範囲外とする。」を以下の内容に変更します。 【変更内容】 ※現行システムにおける庁内メールシステム、ウィルス対策システム、障害監視システム、職員アカウント集中管理システムは、本委託業務とは別の事業で再構築を実施するため、本委託業務の範囲外とする。	あり

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
10	仕様書（案）	P2 2　事業概要 （2）業務範囲 イ　利用者数、業務端末数、業務端末の詳細	【記載内容】 ・利用者数 約6,800人、業務端末数 約10,000台を想定すること。また、ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること。 【意見】 ・「ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること」と記載がありますが、追加ライセンス分の費用について本契約の範囲外の認識でよろしいでしょうか。	・お見込みのとおり、ライセンスを追加する場合は、本委託業務の範囲外とし、本県が別途発注する形になります。	なし
11	仕様書（案）	P13 10　調達全般に関する共通要件 （1）プロジェクト管理に関する要件 イ　プロジェクト管理	【記載内容】 ・必要に応じて適宜ミーティング等を実施し、本県に対し報告及び作業内容の説明・協議を行うこと。なお、構築期間においては、週1回以上、運用期間においては、月1回以上の間隔で報告会を開催すること。また、運用期間における年度末の報告会において品質判定会議を開催すること。 【意見】 ・ミーティング及び報告会等についてはリモートでの参加も可能でしょうか。	・特に記載していませんが、本委託業務の実施に支障がない限り、リモートによる参加でも問題ありません。	なし
12	詳細仕様書（案）	P11 2　本委託業務にて解決したい課題 （2）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題 表　IDaaSに求める機能 機能名　認証機能	【記載内容】 ・クラウドサービスとして利用可能なIDaaSでは、外部からのなりすましなどによる攻撃を防ぐため、IDとパスワードの組み合わせによる認証機能だけではなく、二要素認証の他、パスワードレス認証としてFIDO2.0を利用できる必要がある。 【意見】 ・「パスワードレス認証としてFIDO2.0を利用できる必要がある。」と記載がありますが、弊社のサービスでは独自のパスワードレス認証機能を備えています。FIDO2.0への対応は必須でしょうか？	・インターネット上に公開するクラウド認証基盤において、IDとパスワードによる認証だけではセキュリティレベルを維持することが難しいと考えています。そのため、多要素認証やパスワード自体を利用しないパスワードレス認証が必要と考えています。 ・また、本項目は、本県が課題と考えている個所であり、パスワードレス認証としてはFIDO2.0が規格化済みで、かつ、普及が進んでいることから例示として記載しているもののため、変更はなしとします。 ・なお、クラウド認証基盤における詳細な機能要件については、「3　本システムの詳細な機能要件（1）オンプレミス認証基盤/クラウド認証基盤関連　ウ　クラウド認証基盤（イ）各機能詳細」をご確認いただくようお願いします。 【参考　3　本システムの詳細な機能要件（1）オンプレミス認証基盤/クラウド認証基盤関連　ウ　クラウド認証基盤（イ）各機能詳細】 ・二要素認証が実施できること。また、安全性を確保したパスワードレス認証についても実現できること。	なし
13	詳細仕様書（案）	P11 2　本委託業務にて解決したい課題 （2）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題 表　IDaaSに求める機能 機能名　ID連携機能	【記載内容】 ・さらに、IDaaSと別のID/アカウント管理システム（例えば、インントラに設置済みのActiveDirectoryなど）とID連携を行うことで、IDaaSにてパスワード等の機密情報を保持せずに、IDaaSにてID連携機能を提供できるようになる。 【意見】 ・IDaaSにてパスワード等の機密情報を保持せずに」と記載がありますが、弊社製品ではIDaaS内のデータベースにて情報を保持する形になりますが、問題ないでしょうか。	・記載内容を以下の内容に変更します。 【変更内容】 ・IDaaSと別のID/アカウント管理システム（例えば、イントラに設置済みのActiveDirectoryなど）との間において、ID連携を行うことで、IDaaS側にパスワード等の機密情報を保持せずにID連携機能を提供できること。または、ID/アカウント情報についてパスワードも含めて完全に同期することで、同様にID連携機能を提供できること。	あり
14	詳細仕様書（案）	P17 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細 表　クラウド認証基盤に求める機能 機能名　認証機能	【記載内容】 ・クラウド認証基盤のログイン画面にアクセスする際、本県のオンプレミス環境において認証済みの場合は、再度の認証なく、利用できること。 【意見】 ・「オンプレミス環境にて認証済みの場合は、再度の認証なく、利用できること」と記載がありますが、弊社サービスでは、セキュリティ確保の観点から、内部からのアクセスであっても外部からのアクセスと同様に再度のログインを必要としています。 ・また、いずれの場合でも、デバイス証明書を用いたパスワードレス認証が実現できるため、認証にかかる手間は最小限に抑えられると思いますが、再度の認証を必要とする構成では認められないでしょうか。	・記載内容を以下の内容に変更します。 【変更内容】 ・クラウド認証基盤のログイン画面にアクセスする際、本県のオンプレミス環境において認証済みの場合は、再度の認証なく、利用できること。または、セキュリティ対策上、再度認証が必要となる場合は、全ての利用者に対して、安全、かつ、簡易に利用可能な認証方法（ID、パスワードの入力以外の認証方法で、例えばパスワードレス認証等）を提供できること。	あり
15	詳細仕様書（案）	P17 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細 表　クラウド認証基盤に求める機能 機能名　ID連携機能	【記載内容】 ・外部サービス（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、利用者ID/アカウントと外部サービス（クラウドサービス）における共通アカウントを紐づけてID連携できること。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をActiveDirectoryにおける拡張情報等に設定しておくことで、当該サービスにアクセスする際に、利用者のID/アカウントではなく、共通アカウントで利用する形を想定している。ただし、あくまで統合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の再度認証は不要であること。 ・利用者がID連携機能により、各外部サービス（クラウドサービス）を利用する際、同一利用者が同サービス内に、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、再度の認証なしに、複数のアカウントを切り替えて利用できる機能を持つこと。 【意見】 ・「利用者 ID/ アカウントと外部サービス（クラウドサービス）における共通アカウントを紐づけて ID 連携できること。」と記載がありますが、共有アカウント用のユーザーを作成し、そのユーザーを用いてログイン操作での対応は可能でしょうか。	・同一外部サービス（クラウドサービス）内における複数アカウントの切り替えについて、クラウド認証基盤への再認証なしに利用できるのが理想ですが、再認証の実施による切り替えについても仕様を満たす形に変更します。そのため、記載内容を以下の内容に変更します。 【変更内容】 ・外部サービス（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を行う場合もあることから、利用者ID/アカウントと共通アカウントを紐づけてID連携が実現できること。具体的には、同一所属の利用者は、当該サービスにアクセスする際に、利用者のID/アカウントではなく、共通アカウントにて利用できるようにできること。なお、統合認証基盤への認証を利用者単位で実施後、将来的には、共通アカウントへの再認証なしに利用できる必要があるが、当面は、共通アカウントによるクラウド認証基盤への再認証を経て、共通アカウントを利用する形も可とする。 ・利用者がID連携機能により、各外部サービス（クラウドサービス）を利用する際、同一利用者が同サービス内に、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）を利用したい場合が想定されるが、この場合は、別の利用者としてクラウド認証基盤における再認証を行うことで、アカウントを切り替えて利用できること。	あり

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
16	詳細仕様書（案）	P18 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　アクセス制御機能	【記載内容】 ・各外部サービス（クラウドサービス）内における利用権限等についても一元的に管理でき、同画面で表示できること。 【意見】 ・「各外部サービス（クラウドサービス）内における利用権限等についても一元的に管理でき、同画面で表示できること」と記載がありますが、利用者を切り替えて利用する形での対応は可能でしょうか。	・記載内容を以下の内容に変更します。 【変更内容】 ・各外部サービス（クラウドサービス）内における利用権限等について、IDaaSにおける複数のID/アカウントに対して、個々に紐づけることで一元的に管理できること。また、統合認証基盤への再認証等を経ることで、複数の利用者権限の使い分けが実現できること。（例えば、IDaaSへ「利用者01」としてログイン後、クラウドサービスXに対してuser01（利用者権限）として利用後、IDaaSへ「利用者02」として再ログインし、同サービスに対してuser02（管理者権限等）として利用する、といった使い方が実現できること。）	あり
17	詳細仕様書（案）	P18 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　ID管理機能（ID同期機能）	【記載内容】 ・オンプレミス認証基盤におけるID/アカウントに対して設定されたセキュリティグループや拡張情報等について、クラウド認証基盤上のID管理（ID同期）を行うID/アカウントにかかる付加情報として登録できること。また、その情報をID連携機能やアクセス制御機能で利用できること。 【意見】 ・「オンプレミス認証基盤におけるID/ アカウントに対して設定されたセキュリティグループや拡張情報等について、クラウド認証基盤上の ID 管理（ ID 同期）を行う ID/ アカウントにかかる付加情報として登録できること。」と記載がありますが、別途共通アカウントを利用する形での対応は可能でしょうか。	・本項目における「セキュリティグループ」「拡張情報」については、例示であり、対応が要件となっているものではありません。オンプレミス認証基盤はActiveDirectoryがベースとなるため、ActiveDirectoryで保持可能な情報や設定を、外部サービス（クラウドサービス）のID/アカウント情報として保持する形になると想定しているため、例えば、オンプレミス認証基盤において、user01というアカウントでログオンし、外部サービスAに対してはuser00001などといったアカウントでログオンしたい場合などは、ActiveDirectory上のuser01というアカウントにuser00001という情報を保持しておく必要があると考えていますので、ActiveDirectory上において情報を保持できれば、どのような方式で実現いただいても問題ありません。 ・ただし、別システムでこれらの情報を保持するということであれば、別システムの構築や運用等、本システムを利用するうえで、必要になる経費の全てを本委託業務の範囲内としていただくようお願いします。	なし
18	詳細仕様書（案）	P18 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　ID管理機能（ID同期機能）	【記載内容】 ・オンプレミス認証基盤において利用者の情報を変更した場合、自動的にクラウド認証基盤に同期されること。また、任意のタイミングで同期処理が実行できること。 【意見】 ・「オンプレミス認証基盤において利用者の情報を変更した場合、自動的にクラウド認証基盤に同期されること。また、任意のタイミングで同期処理が実行できること。」と記載がありますが、任意のタイミングでの同期処理はできないため削除頂けないでしょうか。	・同期タイミングとして、定期的に実施できる他、任意のタイミングで実施できる必要があります。そのため、仕様の変更はなしとします。	なし
19	詳細仕様書（案）	P19 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　セキュリティ要件	【記載内容】 ・クラウド認証基盤を提供する事業者は、プライバシーマーク、ISMS認証（ISO27001）などの情報セキュリティの運用に関する第三者機関の認証を取得していること。また、ISMSクラウドセキュリティ認証（ISO27017）を取得していること。 【意見】 「ISMSクラウドセキュリティ認証（ISO27017）を取得していること。」と記載がありますが、IDaaSサービスを提供する事業者においては、ISO27018を取得している場合が一般的と思います。 ISO27017が必須でしょうか。	・記載内容を以下の内容に変更します。 【変更内容】 ・クラウド認証基盤を提供する事業者は、プライバシーマーク、ISMS認証（ISO27001）などの情報セキュリティの運用に関する第三者機関の認証を取得していること。また、クラウドサービス運用・利用に関する情報セキュリティ認証（ISO27017）、クラウドサービス上での個人情報保護・管理認証（ISO27018）を取得、または、取得見込みであること。	あり
20	詳細仕様書（案）	P19 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　セキュリティ要件	【記載内容】 ・クラウド認証基盤に利用者の直接登録を行う際、利用者のパスワードポリシーとして、パスワードの最小文字数、最大文字数、パスワードに大文字、小文字、数字、記号を含むよう複雑さの条件、などを設定できること。また、利用者によるパスワードリセット機能を提供できること。 【意見】 ・「利用者によるパスワードリセット機能を提供できること」と記載がありますが、弊社のサービスではID/パスワードのみの認証は推奨していないため利用者側からの操作のみでパスワードをリセットさせる機能を提供していません。また、パスワードレス認証等による認証が利用できるため、パスワードリセット機能を利用する場面が少ないと想定していますが、パスワードリセット機能は必要でしょうか。	・記載内容を以下の内容に変更します。 【変更内容】 ・クラウド認証基盤に利用者のID/アカウント情報を直接登録する際、利用者のパスワードポリシーとして、パスワードの最小文字数、最大文字数、パスワードに大文字、小文字、数字、記号を含むよう複雑さの条件、などを設定できること。また、利用者によるパスワードリセット機能を提供できること。（パスワードレス認証等による認証が実現できている場合は、パスワードリセット機能は不要とする。）	あり
21	詳細仕様書（案）	P19 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　管理者機能	【記載内容】 ・管理用画面における管理者のログインや各種操作、ID管理（ID同期）処理等のログについて閲覧、検索ができること。また、ログの出力ができること。 【意見】 「管理用画面における管理者のログインや各種操作、ID 管理（ID 同期）処理等のログについて閲覧、検索ができること。また、ログの出力ができること。」と記載がありますが、弊社のサービスでは管理者のログではなく、アクセスログを確認する形になりますが、問題ないでしょうか。	・本システムの運用期間中において、インシデント等が発生した際に、管理者ログ等を確認する必要があると考えていますが、その際に必要十分なログが確認できれば問題ありません。そのため、記載内容を以下の内容に変更します。 【変更内容】 ・管理用画面における管理者のログインや各種操作、ID管理（ID同期）処理の他、利用者のアクセスログ等について、運用期間中においてインシデント等が発生した際に必要十分な確認ができること。また、対象となるログの出力ができること。	あり
22	詳細仕様書（案）	P19 3　本システムの詳細な機能要件 （1）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　管理者機能	【記載内容】 ・クラウド認証基盤へのログイン画面について、任意メッセージの掲載など、カスタマイズができること。 【意見】 ・「クラウド認証基盤へのログイン画面について、任意メッセージの掲載など、カスタマイズができること」と記載がありますが、任意のメッセージを画像で表示させる形で問題ないでしょうか。	・画像を変更することで任意のメッセージを表示できれば、問題ありません。	なし

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
23	詳細仕様書（案）	P19 ３　本システムの詳細な機能要件 （１）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細表　クラウド認証基盤に求める機能 機能名　管理者機能	【記載内容】 ・ID管理（ID同期）処理の結果を管理者にメールで通知できること。 【意見】 ・「ID管理（ID同期）処理の結果を管理者にメールで通知できること」とありますが、弊社システムは、数分に一度、同期処理を行っているため、メール通知を行っていません。メール通知は必要でしょうか。	・記載内容を以下の内容に変更します。 【変更内容】 ・ID管理（ID同期）処理の結果を管理者にメールで通知できること。なお、即時同期（数分間に一度の間隔で同期）している場合は、メール通知は不要とする。	あり
24	詳細仕様書（案）	P19 ３　本システムの詳細な機能要件 （１）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （ウ）その他	【記載内容】 ・必要なデータについて、バックアップを行うこと。また、ログの保存機能についても提供すること。 【意見】 ・「ログの保存機能についても提供すること」と記載がありますが、保存期間の指定はありますでしょうか？	・ログの保存期間として、インシデントが発生した際に、遡って調査を行う必要があるため、1年程度と想定しています。ただし、仕様への記載はなしとします。	なし
25	詳細仕様書（案）	P20 ３　本システムの詳細な機能要件 （１）オンプレミス認証基盤/クラウド認証基盤関連 エ　統合認証基盤 （ア）プライベート認証局機能	【記載内容】 ・電子証明書を取得する際、無線LAN接続に必要な情報を管理者が設定しておくことで、利用者が電子証明書を取得する際に、合わせて配布・設定ができる機能を提供すること。 【意見】 ・「電子証明書を取得する際、無線 LAN 接続に必要な情報を管理者が設定しておくことで、利用者が電子証明書を取得する際に、合わせて配布・設定ができる機能を提供すること。」と記載がありますが、IDaaSの機能の他、統合運用管理システムの機能を利用して実現する形でも問題ないでしょうか。	・機能の実現方法について、特に指定はありません。例えば、一部の作業を受託事業者が実施する形であっても問題ありません。ただし、本要件を実現するために必要となる全ての作業等にかかる費用については、本委託業務に含めていただくようお願いします。	なし
26	仕様書（案）	P6 ２　事業概要 （２）業務範囲 カ　現行システムの概要	【記載内容】 ※ 現行システムにおける 庁内メールシステム、ウィルス対策システム、 障害監視システムは、本委託業務とは別の事業で 再構築を実施するため、本委託業務の範囲外とする 。 【意見】 ・障害監視システムが、本件とは別事業で再構築とありますが、本件にて調達されるシステムの監視は、本件受託事業者にて、個別で監視をおこなうという解釈でよろしいでしょうか？	・本県が別途構築を行う障害監視システムを利用可能であるため、このシステムを利用して、運用・保守業務における監視業務を実施いただくようお願いします。なお、このシステムを利用せず、別システムを構築することも可としますが、構築費や運用・保守業務にかかる全ての費用について、本委託業務の範囲内としてください。	なし
27	資料２　統合サーバの利用について	P2 別紙1	【記載内容】 仮想化による統合を行うこととし、仮想化ソフトウェアとして 統合用サーバについては 「 VMware 社製 VMware vSphere 6.7 Update 2 」、 DB 用統合用サーバについては 「 Microsoft Hyper V 7.0 」 を用いている。 【意見】 ・仮想ソフトウェアを分けている理由が三重県様の方で特別な利用がない場合は、VMwareのみまたはHyper-Vのみ、どちらか１つの環境にしても問題は無いでしょうか。	・どちらか1つの環境で問題ありません。なお、通常は、Vmware上でシステム構築を行っていただくこととしています。	なし
28	詳細仕様書（案）	P10 ２ 本委託業務にて解決したい課題 （１）全体の課題 ア 現行システムからの機能引継ぎ	【記載内容】 現行システムにおける「庁内ドメインシステム」「運用管理システム 資産管理 」 「運用管理システム セキュリティパッチ配布 」 「バックアップ・リストアシステム」「ログ収集システム」について、保守契約期限が令和 4 年 6 月 30日 に 迫っているため、それぞれの機能について、 本システムにて 引き続き、提供する必要がある。 【意見】 ・構築及び移行期間において、より安全性を考え、ハードの延長保守を検討しているため、対象機器の、メーカ名、型番、シリアル番号など、ご教示をいただくことは可能でしょうか？	・対象となる機器のメーカ名、型番、シリアル番号については、別紙「納品物一覧」のとおりです。	なし
29	仕様書（案）	P2 ２　事業概要 （２）業務範囲 イ　利用者数、業務端末数、業務端末の詳細	【記載内容】 ・利用者数 約6,800人、業務端末数 約10,000台を想定すること。また、ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること。 【意見】 ・「利用者数6,800人」は全て庁内ドメインに存在しているという認識ですが、そうで無い場合は、ご明示頂けませんでしょうか。	・利用者数は、正規職員と会計年度任用職員を合わせた職員数のことであり、全職員が庁内ドメインシステムにアカウント登録されています。なお、庁内ドメインシステムには、利用者の他、所属アカウント、システム担当者用アカウントなども登録されているため、アカウント数（CALの数）とは異なります。	なし
30	仕様書（案）	P2 ２　事業概要 （２）業務範囲 イ　利用者数、業務端末数、業務端末の詳細	【記載内容】 ・利用者数 約6,800人、業務端末数 約10,000台を想定すること。また、ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること。 【意見】 ・庁内ドメイン(ActiveDirectory環境)からプロキシーを介してインターネットに接続可能という想定です。 ・(AD→クラウド認証基盤への連携の為、https通信を想定している為、プロキシーの有無、接続可否を確認させてください。)間違いないか確認させて頂きたく。	・お見込みのとおり、オンプレミス認証基盤からクラウド認証基盤に向けて、本県が別途設置しているproxyを経由してアクセスを行う形になります。なお、本県が別途設置しているproxyの上位には、三重県自治体情報セキュリティクラウドのproxyも存在し、こちらも経由しますが、セキュリティクラウドのproxyを経由せず直接インターネットと接続する経路（ローカルブレイクアウト回線）も利用可能です。	なし

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
31	仕様書（案）	P2 ２　事業概要 （２）業務範囲 イ　利用者数、業務端末数、業務端末の詳細	【記載内容】 ・利用者数 約6,800人、業務端末数 約10,000台を想定すること。また、ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること。 【意見】 ・業務端末はWindows端末と読み取れますが、スマートフォンやタブレットでの利用はありますでしょうか。もし利用予定であるようであれば、その内容を明確に提示頂ければと思います。	・タブレット端末として、iPadが183台運用しています。	なし
32	仕様書（案）	P2 ２　事業概要 （２）業務範囲 イ　利用者数、業務端末数、業務端末の詳細	【記載内容】 ・利用者数 約6,800人、業務端末数 約10,000台を想定すること。また、ライセンスの追加等軽微な対応で最大2割程度の利用者、業務端末数の増加に対応できること。 【意見】 ・クラウドサービスを利用する際のご利用ブラウザをご指定頂けますでしょうか。(複数ある場合、可能な限りご回答ください)	・現在、InternetExplorer11を標準ブラウザとして指定していますが、次期標準ブラウザについては、Edge、Chromeのいずれかにすることとはしているものの、未決定です。	なし
33	仕様書（案）	P6 ２　事業概要 （２）業務範囲 カ　本システムで構築するサブシステム	【記載内容】 ・（記載なし） 【意見】 ・クラウド認証基盤で認証し、クラウドサービスをご利用するユーザーは何ユーザー程度でしょうか。 ・「２　事業概要（２）業務範囲　イ　利用者数、業務端末数、業務端末の詳細」の利用者全員が対象でしょうか。ご明示頂きたくお願いします。	・クラウド認証基盤の利用ユーザとして、最大6,800ユーザとしてください。なお、最大2割程度の利用者追加が可能な構成としていただくようお願いします。（追加ライセンスが発生した場合の費用は、本委託業務の範囲外となります。）	なし
34	仕様書（案）	P6 ２　事業概要 （２）業務範囲 カ　本システムで構築するサブシステム	【記載内容】 ・（記載なし） 【意見】 ・クラウド認証基盤で認証し、クラウドサービスをご利用する場所はどこからになるでしょうか？(三重県行政WAN、庁内LAN内など利用環境を明確にご提示いただけますでしょうか)	・クラウド認証基盤を利用する業務端末は、三重県行政WAN内の業務端末（VPNにより外部から接続している場合を含む）と、インターネット上の業務端末を想定しています。	なし
35	詳細仕様書（案）	P11 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題	【記載内容】 ・本県では、外部サービス（クラウドサービス）の利用について、これまで、いくつかのサービスについて、試用を行ってきたが、さまざまな課題が顕在化している。 【意見】 ・利用している外部サービス(クラウドサービス)を明示頂けますでしょうか。また、今後利用される予定のクラウドサービスもあれば明示頂ければと思います。※Microsoft365、GoogleWorkspace、slack 、boxはP.12に記載を確認済ですが、全てご利用中という認識で差支えないでしょうか。例：Office365、box、Salesforce、作りこみのアプリケーション2つ。(AWSに構築。SAMLには対応していない)	・外部サービス（クラウドサービス）として、現在は、slack、box、zoom、webexなどの試行運用を行っていますが、シャドーITを含めてすべての把握は行っていません。 ・全職員が利用可能な外部サービス（クラウドサービス）として、令和4年度から利用可能となるよう、調達準備を進めていますが、実施の可否も含めて、詳細は未定です。	なし
36	詳細仕様書（案）	P11 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題	【記載内容】 ・本県では、外部サービス（クラウドサービス）の利用について、これまで、いくつかのサービスについて、試用を行ってきたが、さまざまな課題が顕在化している。 【意見】 ・利用している外部サービス(クラウドサービス)のID管理はサービスごとに行っていると思いますが、どのようにユーザー登録・修正・削除を行っていますでしょうか。明示頂ければと思います。 例：CSVによる一括インポート、手動、他システムとの連携など	・お見込みの通り、各サービス単位で実施しています。なお、多くの場合は、手作業で対応を行っています。	なし
37	詳細仕様書（案）	P11 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題	【記載内容】 ・本県では、外部サービス（クラウドサービス）の利用について、これまで、いくつかのサービスについて、試用を行ってきたが、さまざまな課題が顕在化している。 【意見】 ・利用している外部サービス(クラウドサービス)のログインはIDとパスワード入力以外のログインをしているサービスはありますか？有る場合はご明示を頂きたくお願いします。	・IDとパスワード以外の認証を実施しているサービスはありません。	なし
38	詳細仕様書（案）	P11 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題 表　IDaaSに求める機能 機能名　認証機能	【記載内容】 ・クラウドサービスとして利用可能なIDaaSでは、外部からのなりすましなどによる攻撃を防ぐため、IDとパスワードの組み合わせによる認証機能だけではなく、二要素認証の他、パスワードレス認証としてFIDO2.0を利用できる必要がある。 【意見】 ・FIDO2.0で連携したい認証デバイスは何になるでしょうか？(検討している製品、連携方式など公開できる情報があればご明示頂きたくお願いします)	・iPhoneなどを想定していますが、詳細は決定していません。	なし
39	詳細仕様書（案）	P11 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題 表　IDaaSに求める機能 機能名　認証機能	【記載内容】 ・クラウドサービスとして利用可能なIDaaSでは、外部からのなりすましなどによる攻撃を防ぐため、IDとパスワードの組み合わせによる認証機能だけではなく、二要素認証の他、パスワードレス認証としてFIDO2.0を利用できる必要がある。 【意見】 ・2要素認証としてお考えの要素は何か想定がございますでしょうか。三重県様として想定があるようでしたらご明示頂きたくお願いします。例：スマートフォンアプリのワンタイムパスワード、eメールやSMSによるワンタイムパスワード、生体認証など	・安全、かつ、簡単に利用できるものとして、本委託業務の契約後、本システムで利用可能な二要素を選定する予定です。（現時点で二要素の指定はありません。）	なし

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
40	詳細仕様書（案）	P11 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題 表　IDaaSに求める機能 機能名　ID連携機能	【記載内容】 ・現在、多くの外部サービス（クラウドサービス）にて、ID連携機能が利用可能になっているが、特に、IDaaSとして、SAML（Security Assertion Markup Language）によるID連携機能が利用できる必要がある。 【意見】 ・連携予定の外部サービス(クラウドサービス)の中でSAML対応していないサービスはございますでしょうか。 ・仕様上必要かと思いますのでご明示頂きたくお願いします。	・現時点で連携予定の外部サービス（クラウドサービス）は確定していません。そのため、その中に、SAML連携に対応していないサービスがあるかどうかは確認できません。（今後、そのようなサービスを利用する可能性はあります。） ・なお、本システムとID連携を行う外部サービス（クラウドサービス）は、SAML対応が条件となります。	なし
41	詳細仕様書（案）	P12 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ア　外部サービス（クラウドサービス）の利用にかかる課題 表　IDaaSに求める機能 機能名　ID管理機能（ID同期機能）	【記載内容】 （該当する記載内容なし） 【意見】 ・庁内ドメインに存在しないユーザーを今回の認証基盤側で管理する想定はございますでしょうか。	・庁内ドメインに存在しない利用者として、各外部サービス（クラウドサービス）の管理者ユーザなどを統合認証基盤で管理する予定です。	なし
42	詳細仕様書（案）	P13 ２　本委託業務にて解決したい課題 （２）庁内ドメインシステムにおける課題 ウ　セキュリティ対策の強化	【記載内容】 ・なお、アクセス拒否の方法として、電子証明書で判定する方法やMDM（Mobile Device Management）などの管理ツールの有無により判定する方法などがあるが、管理者の負荷が少なく、現実的に運用が可能な方法である必要がある。 【意見】 ・ご利用のMDM製品または導入を検討しているMDM製品はございますでしょうか。※クラウド認証基盤での端末認証の連携に想定しているMDM製品があれば教えてください。	・現時点でMDM製品の導入については未定です。	なし
43	詳細仕様書（案）	P18 ３　本システムの詳細な機能要件 （１）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細 表　クラウド認証基盤に求める機能 機能名　認証機能	【記載内容】 ・クラウド認証基盤のログイン画面にアクセスする際、本県のオンプレミス環境において認証済みの場合は、再度の認証なく、利用できること。 【意見】 ・「本県のオンプレミス環境において認証済みの場合、再度認証なく、利用できること」とあるが、これはオンプレミス環境でWindowsの業務端末でドメインにログインした状態を意味しているという認識で間違いありませんでしょうか。 ・具体的に記載頂けると助かります。	・お見込みのとおり、オンプレミス認証基盤へのログイン後にクラウド認証基盤へアクセスし、その後、外部サービス（クラウドサービス）を利用する流れを想定しています。	なし
44	詳細仕様書（案）	P18 ３　本システムの詳細な機能要件 （１）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細 表　クラウド認証基盤に求める機能 機能名　セキュリティ要件	【記載内容】 ・クラウド認証基盤のログイン画面にアクセスするための通信について、TLS等により暗号化できること。また、アクセス用の電子証明書の有無により、電子証明書が確認できないアクセスについては、アクセスを拒否できること。 【意見】 ・[アクセス用の電子証明書の有無により、電子証明書が確認できないアクセスについては、アクセスを拒否できること」との記載があるが、電子証明書のみでしょうか？(MDM製品との連携でもご提案としては許容されるでしょうか？)	・MDMとの連携によるアクセス拒否についても本要件を満たしますが、MDMにより管理する情報には電子証明書の有無に関する情報も含まれていると想定しているため、仕様の変更はなしとします。	なし
45	詳細仕様書（案）	P19 ３　本システムの詳細な機能要件 （１）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （イ）各機能詳細 表　クラウド認証基盤に求める機能 機能名　管理者機能	【記載内容】 ・クラウド認証基盤の操作を実施するため、管理用画面を用意し、管理者が安全に利用できること。また、管理画面が、Webで提供され、日本語で表記できること。 【意見】 ・クラウド認証基盤の管理Web画が日本語であること、との記載があるが日本語以外(英語のみ)のクラウド認証基盤は許容されるでしょうか？	・本要件は、本県職員において、クラウド認証基盤の管理画面から各種操作を実施する際の条件となるため、日本語表記が出来ない場合は、受託事業者が代わりに作業を実施する形となります。そのため、記載内容を以下の内容に変更します。 【変更内容】 ・クラウド認証基盤の操作を実施するため、管理用画面を用意し、管理者が安全に利用できること。また、管理画面が、Webで提供され、日本語で表記できること。（日本語で表記できない場合は、受託事業者が全ての運用・保守業務にかかる作業を実施することになるため、注意すること。）	あり
46	詳細仕様書（案）	P19 ３　本システムの詳細な機能要件 （１）オンプレミス認証基盤/クラウド認証基盤関連 ウ　クラウド認証基盤 （ウ）その他	【記載内容】 ・必要なデータについて、バックアップを行うこと。また、ログの保存機能についても提供すること。 【意見】 ・現行のログ保存機能はどのような形で保存しているでしょうか？ご提示頂けますと構成確認が進みますのでご提示頂ければと思います。	・現在、クラウド認証基盤は存在しないため、ログは存在しません。なお、庁内ドメインシステムにおけるログはログ収集システムにより保管しています。	なし
47	詳細仕様書（案）	P26 ３　本システムの詳細な機能要件 （３）バックアップ・リストアシステム	【記載内容】 バックアップは、数世代分を取得することとし、必要に応じて任意のバックアップからファイル単位でリストアができること。 【意見】 ・「バックアップは、数世代分を取得することとし」とありますが、何世代分が必要でしょうか。 既にお決まりなっているようでしたらご教示頂きたくお願いします。	・バックアップの世代数については、指定はありません。バックアップを行うデータの重要度等に応じて、取得する世代数について設計をいただくことになります。	なし

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
48	詳細仕様書（案）	P26 ３　本システムの詳細な機能要件 （３）バックアップ・リストアシステム	【記載内容】 現行システムにおける「バックアップ・リストアシステム」にて実現していた、「庁内メールシステム」以外の物理サーバに対するバックアップ・リストア機能について、本システムにおける物理サーバに対するバックアップ・リストア機能として、利用できること。 【意見】 ・バックアップ対象のディスク容量は、「13_仕様書_資料1」に記載されています既存システムの容量をベースとして想定することでよいでしょうか？（既に三重県様で想定されていますディスク容量がございましたらご教示ください） また、現行システムのバックアップされていますファイル容量をご教示ください。	・本システムにおけるディスク容量や、バックアップ方式、世代数等については、本委託業務における設計段階にて確定するものと考えているため、想定している容量はありません。 ・現行システムにおける庁内メールシステム以外のバックアップとして、毎週約600GByte程度の容量をバックアップしています。なお、バックアップ・リストアシステムにおける現在のバックアップ容量は約1.1TByteです。（毎週テープ交換を行いながら運用を行っています。）	なし
49	詳細仕様書（案）	P26 ３　本システムの詳細な機能要件 （３）バックアップ・リストアシステム	【記載内容】 現行システムにおける「バックアップ・リストアシステム」にて実現していた、「庁内メールシステム」以外の物理サーバに対するバックアップ・リストア機能について、本システムにおける物理サーバに対するバックアップ・リストア機能として、利用できること。 【意見】 ・バックアップ対象のファイル容量は年率何%の増加率を見込んでおられますでしょうか？ その見込がある場合は、明示頂きたくお願いできますでしょうか。	・増加率について、特に見込みはありません。（増減するかについては、設計によるところが大きいと考えています。	なし
50	詳細仕様書（案）	P26 ３　本システムの詳細な機能要件 （３）バックアップ・リストアシステム	【記載内容】 現行システムにおける「バックアップ・リストアシステム」にて実現していた、「庁内メールシステム」以外の物理サーバに対するバックアップ・リストア機能について、本システムにおける物理サーバに対するバックアップ・リストア機能として、利用できること。 【意見】 ・テープへのバックアップは必須でしょうか？リストア等の時間を考えますと、ディスク装置へのバックアップが主流になっているかと存じまして、効率的かと考えています。	・必須とはしていませんが、現行システムと同等の信頼性が実現できる構成としてください。	なし
51	詳細仕様書（案）	P26 ３　本システムの詳細な機能要件 （３）バックアップ・リストアシステム	【記載内容】 現行システムにおける「バックアップ・リストアシステム」にて実現していた、「庁内メールシステム」以外の物理サーバに対するバックアップ・リストア機能について、本システムにおける物理サーバに対するバックアップ・リストア機能として、利用できること。 【意見】 ・バックアップシステムの別場所への設置は必要でしょうか？ ・そのお考えがあるならご明示頂きたくお願いします。	・必須とはしていませんが、現行システムと同等の信頼性が実現できる構成としてください。	なし
52	詳細仕様書（案）	P26 ３　本システムの詳細な機能要件 （４）ログ収集システム	【記載内容】 現行システムにおける「ログ収集システム」にて実現していたログ収集機能について、本システムでも利用できるようにすること。 取得したログを任意に抽出し、分析できる仕組みも提供すること。 取得したログは1年分以上、保存できること。 【意見】 ・現行システムで収集されているログのファイル容量はどのくらいでしょうか？ ・ご提示いただいたサーバスペックの容量のみで足りていると考えていて宜しいでしょうか。 ・仕様確認上必要ですのでご提示頂けばと思います。	・本システムにおいて収集するログについて、その詳細やローテーション方法等については、本委託業務における設計段階にて確定するものと考えているため、想定している容量はありません。 ・現行システムにおけるログとして、毎月約250GByte程度の容量となっています。なお、ログ収集システムにおける現在のログ容量は約1.0TByteです。（容量が一杯になる前にNAS等へ退避しています。）	なし
53	詳細仕様書（案）	P1 １　現行システムの概要 （１）完成図書記載時からの変更点	【記載内容】 ウ　障害監視システムの停止 ・現行システムでは、障害監視システムを構築し、運用を行っていたが、本県が別契約で構築した新たな障害監視システム（zabbix）にて、現行システムにおける障害監視の対象機器についても監視を行う形に変更している。 【意見】 ・障害監視システムは現行システムでは構築していません。	・記載内容を以下の内容に変更します。 【変更内容】 ウ　障害監視システムの変更 ・現行システムの運用当初は、本県が別途構築を行った障害監視システム（crane）を利用して運用を行っていたが、現在は、本県が新たに構築した障害監視システム（zabbix）にて、現行システムにおける障害監視対象機器にかかる監視を行っている。	あり
54	詳細仕様書（案）	P36、P39 ５　業務詳細 （６）運用・保守業務の設計にかかる要件 エ　受託事業者が行うもの	【記載内容】 ・（なし） 【意見】 ・「外部サービス（クラウドサービス）導入支援」「既存システムとのシステム連携支援」にかかる仕様の追加。	・「（コ）外部サービス（クラウドサービス）導入支援」「（サ）既存システムとのシステム連携支援」として、以下の内容を追記します。 【追記内容】 （コ）外部サービス（クラウドサービス）導入支援 ・新たに外部サービス（クラウドサービス）を利用する際に、本システムとの連携等において必要となる作業等について、導入支援作業を行う。 （サ）既存システムとのシステム連携支援 ・新たにオンプレミスの業務システムと本システム間でID連携等を行うために必要となる作業等について、導入支援作業を行う。	あり

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
55	詳細仕様書（案）	P33 5　業務詳細 （４）構築業務等の設計にかかる要件	【記載内容】 ・（なし） 【意見】 ・「外部サービス（クラウドサービス）導入設計にかかる要件」「既存システムとのシステム連携設計にかかる要件」にかかる仕様の追加。	・「イ　外部サービス（クラウドサービス）導入設計にかかる要件」「エ　既存システムとのシステム連携設計にかかる要件」として、以下の内容を追記します。 【追記内容】 イ　外部サービス（クラウドサービス）導入設計にかかる要件 ・本委託業務で導入するクラウド認証基盤において、本県が指定する各外部サービス（クラウドーサービス）との間でID連携等が実施できるようにする必要があるが、クラウド認証基盤がIDaaSとして提供可能な各種機能について利用できるようにするために必要となる各種作業について、外部サービス（クラウドサービス）導入設計を行うこと。 ・外部サービス（クラウドサービス）導入設計にあたっては、本県、及び、運用管理担当者が、当該外部サービス（クラウドサービス）用のID/アカウント情報について、オンプレミス認証基盤上で一元管理ができるよう、クラウド認証基盤へのID同期の他、クラウド認証基盤と外部サービス（クラウドサービス）間の連携実現方法についても設計を行うこと。 ・作成した外部サービス（クラウドサービス）導入設計について、可能な限り本番稼働機にてリハーサルを実施し、その結果について本県に対して説明し、承認を得ること。 ・外部サービス（クラウドサービス）導入にあたっては、障害発生等により作業が中断した場合に備えて、あらかじめ、障害原因の調査方法などについて、準備しておくこと。 エ　既存システムとのシステム連携設計にかかる要件 ・現行システムにおける庁内ドメインシステムにおいて、ActiveDirectoryの標準機能を利用して、既存システムとの連携を行っていたため、現行システムと同様に既存システムとのシステム連携が実現できるよう、既存システムとのシステム連携設計を行うこと。 ・既存システムとのシステム連携設計にあたっては、既存システムとの連携にかかる詳細を確認し、業務への影響や作業負担を最小限に抑え、かつ、安全で確実に実施可能な設計を行うこと。 ・作成した既存システムとのシステム連携設計について、可能な限り本番稼働機にてリハーサルを実施し、その結果について本県に対して説明し、承認を得ること。 ・既存システムとのシステム連携の実施にあたっては、障害発生等により作業が中断した場合に備えて、あらかじめ、障害原因の調査方法などについて、準備しておくこと。	あり
56	詳細仕様書（案）	P40 5　業務詳細 （６）運用・保守業務の設計にかかる要件	【記載内容】 カ　機器撤去 ・履行期間終了時において、受託事業者が納入したハードウェアの内、本県が指定したものの撤去について、設計を行うこと。 ・機器撤去時期については、契約終了年度にて、本県と調整を行うことになるので、留意すること。 ・機器撤去において、機器内のデータ全消去を行ったうえで、データの消去、機器の廃棄が証明できるような仕組みについて設計に盛り込むこと。 【意見】 ・記載場所を変更する。	・機器撤去の設計に関する要件として記載されている、P40「５　業務詳細（６）運用・保守業務の設計にかかる要件」を削除し、機器撤去の実施にかかる業務詳細として、「５　業務詳細（10）機器撤去」に以下の内容を追記します。 【追記内容】 （10）機器撤去 運用期間終了時において、受託事業者が納入したハードウェアの内、本県が指定したものの撤去を行うこと。 機器撤去時期については、契約終了年度にて、本県と調整を行うことになるので、留意すること。 機器撤去において、機器内のデータ全消去を行ったうえで、データの消去、機器の廃棄が証明できる書類を提出すること。	あり
57	－	－	・誤字・脱字等の修正	・仕様書（案）、詳細仕様書（案）の赤字部分が修正部分です。	あり