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　詳細仕様書

令和４年１月

三重県デジタル社会推進局

スマート改革推進課

目　次

１　現行システムの概要

現行システムの概要は以下のとおり。

その他、現行システムの詳細は、資料１「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）」を参照のこと。

（１）完成図書記載時からの変更点

ア　ネットワーク構成の変更

- 現行システムは、三重県行政 WAN 上に構築されているが、利用可能なデータセンターが 2 か所から 1 か所に統合されている。（資料 1 内の表記では、CWJ-IDC と ZTV-IDC の 2 拠点あるが、現在は、津市 IDC に統合され、CWJ-IDC に設置されていた機器は全て津市 IDC に移設されている。）
- これまで、三重県行政 WAN の外部 Firewall からインターネットへ直接接続していたが、現在は、その経路上に「三重県自治体情報セキュリティクラウド」が構築されている。

イ　三層の構えへの対応

- 現行システムの構築時は、三重県行政 WAN は単一のネットワークだったが、三層の構えへの対応として、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、に分離した構成に変更している。
- そのため、ActiveDirectory の構成において、別ドメインとの信頼関係は不要としていたが、LGWAN 系ネットワークに構築された現行システムに対して、個人情報ネットワークとインターネット接続系ネットワークにおいて構築された別ドメインの ActiveDirectory に対して、アカウント情報等を連携させる必要が発生したため、信頼関係を設定している。

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。

（２）庁内ドメインシステム

ア　システム概要

- Microsoft 社製 WindowsServer の ActiveDirectory ドメインを利用したユーザ認証及びリソース管理を行うシステム。
- グループポリシー等にて、ActiveDirectory におけるユーザだけでなく、業務端末のセキュリティ対策も行っている。また、DNS、NTP、DHCP 等の機能も提供している。
- 他の情報システムは、庁内ドメインシステムと連携することで、シングルサインオンなどを実現している。また、職員アカウント集中管理システムは庁内ドメインシステムと連携することで、他の情報システムに対して自動ログオン機能を提供している。

イ　ハードウェア構成・ソフトウェア構成

・ ドメインコントローラの構成は、本庁 3 台, 津市 IDC 4 台の計 7 台構成としている。
・ DNS/NTP は全てのドメインコントローラで提供している。
・ 本庁 3 台、津市 IDC 1 台の計 4 台を物理サーバとし、津市 IDC 3 台は統合サーバ上の仮想マシンで構成している。

No	設置場所	種別	機能				
			FSMO	GC	DNS	NTP	DHCP
1	津市 IDC	物理	○	○	○	○	
2		仮想		○	○	○	○総合庁舎
3		仮想		○	○	○	
4		仮想		○	○	○	○総合庁舎
5	本庁	物理		○	○	○	○本庁
6		物理		○	○	○	○本庁
7		物理		○	○	○	○本庁

表　庁内ドメインシステムの配置表

- FSMO：Flexible Single Master Operation、GC：Global Catalog
- 物理：物理サーバ、仮想：仮想マシン

ウ　機能概要

（ア）Active Directory の構成

・ ActiveDirectory の構成として、シングルフォレスト・シングルドメインを採用しており、また、サイト構成は、シングルサイト、機能レベル Windows Server 2012 R2 としている。
・ 他システムにより構築された ActiveDirectory の別ドメインとの間で主に WSUS を利用するため、信頼関係を構築している。
・ ユーザ、コンピュータともに複数の OU に振り分けを行って管理している。
・ セキュリティグループは、各所属単位の他、各情報システムで必要になる度に作成している。所属単位のセキュリティグループは、部、所属、班の階層にあわせてネスト化（3 階層）して作成し、運用している。

（イ）DHCP

・ 一部のドメインコントローラでは、LGWAN 系ネットワーク上の必要なセグメントに対して、DHCP サービスを提供している。
・ 本庁舎（行政棟、厚生棟、講堂棟、議事堂）、及び、吉田山会館等におけるフロアや建物単位で 13 セグメント、総合庁舎では庁舎単位で 10 セグメントについて、DHCP 機能を提供している。

- DHCP 機能を提供する DHCP サーバは、本庁、及び、津市 IDC に設置した ActiveDirectory 上のドメインコントローラと兼用している。
- 各 DHCP サーバが設置されているセグメントと、DHCP を提供する各セグメントは異なっており、また、DHCP を提供するセグメントが多いため、ネットワーク機器にて DHCP リレーエージェント設定を行うことで、少ないサーバ台数にて対応を行っている。
- DHCP サーバの耐障害性を向上させるため、DHCP フェールオーバー機能による冗長構成としている。

（ウ）DNS

- 全ドメインコントローラにおいて、DNS サービスを提供している。
- ActiveDirectory に必要な前方参照ゾーンとプライベート IP アドレスの逆引きゾーンのみの名前解決を行っている。それ以外の名前解決については、既設の DNS サーバ（BIND 現行システムとは別システムで構築）への転送により解決している。

（エ）NTP

- 全ドメインコントローラにおいて、NTP サービスを提供している。
- 津市 IDC に設置のドメインコントローラのうち 1 台が外部 NTP サービスと時刻同期をし、他のドメインコントローラは、この 1 台と時刻同期を行っている。

（オ）WINS

- 廃止済みのため、サービスを提供していない。（必要な場合は、lmhosts により対応することとしているが、これまでに実績はない。）

（カ）ログオンスクリプト

- ドメインに接続する各業務端末に対し、ログオンスクリプトを使用することで、必要なアプリケーションのインストールや設定変更等が実施できるようにしている。

（キ）CSV インポート機能

- ActiveDirectory におけるユーザの新規追加、有効化、変更、無効化、削除等について、CSV データをインポートすることにより、設定を反映できるよう、VBScript を用意し、運用を行っている。セキュリティグループの登録、メンバ変更、削除も同様に対応している。
- CSV データは、職員アカウント集中管理システムから出力している。

（ク）他システムからの利用

- 庁内ドメインシステムはログイン時におけるユーザ認証だけでなく、他システムからの認証基盤としてシングルサインオンの実現等に利用されている。

（３）庁内メールシステム

ア　システム概要

・ トランスウェア社（現在のクオリティア社）の Active! Mail を利用した LGWAN ネットワーク内に閉じた内部メースシステム。

イ　ハードウェア構成・ソフトウェア構成

・ Web メール用 AP サーバ 4 台、SMTP/IMAP サーバ 2 台、共有ストレージ 2 台（2 コントローラ）、負荷分散装置 2 台、接続用スイッチで構成している。

・ Web メール用 AP サーバ、SMTP/IMAP サーバと共有ストレージの接続は、NFS にて接続している。

・ 共有ストレージには、Web メールの管理データとメールデータを格納している。また、同一ストレージ上の異なる筐体上にバックップデータを格納している。

・ 各サーバは仮想マシンではなく、物理サーバで構築している。

・ Web メール機能はトランスウエア社製（現在のクオリティア社）の「Active! Mail」により構築している。

・ Active! Mail は Web サーバ上に構成する必要があるため、Web サーバは「Apache HTTP Server」で構築している。

・ 共有アドレス帳・個人アドレス帳・シグネチャ等の各種設定は、Active! Mail 上にて管理している。

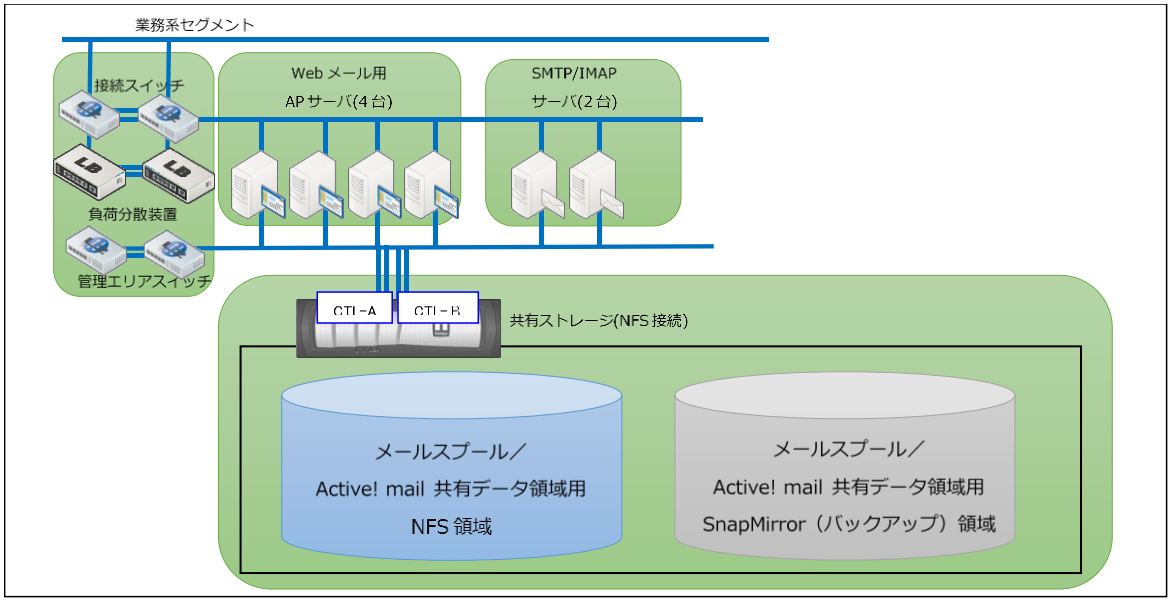

図　庁内メールシステムの構成図

ウ　機能概要

（ア）Web メール機能

・ Active! Mail による Web メール機能を提供している。

（イ）シングルサインオン機能とマルチアカウント機能

・ 庁内ドメインシステムにおける ActiveDirectory と連携し、シングルサインオン機能を構築している。

・ 庁内メールシステムへログオンした後に、複数の庁内メールアカウントを、ログイン/ログアウトを繰り返すことなくアカウントを切り替えることができるマルチアカウント機能を構築している。マルチアカウント機能を実装するために、Acitve! Mail の運用ミドルウェアである Active! Mail　MA（以下、マルチアカウント）を使用している。
・ マルチアカウントを利用するため、ActiveDirectory への属性追加を行う必要があったため、他のアプリケーションとの重複を避けるため、OID（オブジェクト識別子）を取得している。
  ✧ https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers （1.3.6.1.4.1 45856 Mie Prefectural Government）
・ シングルサインオンの概要は、以下のとおり。

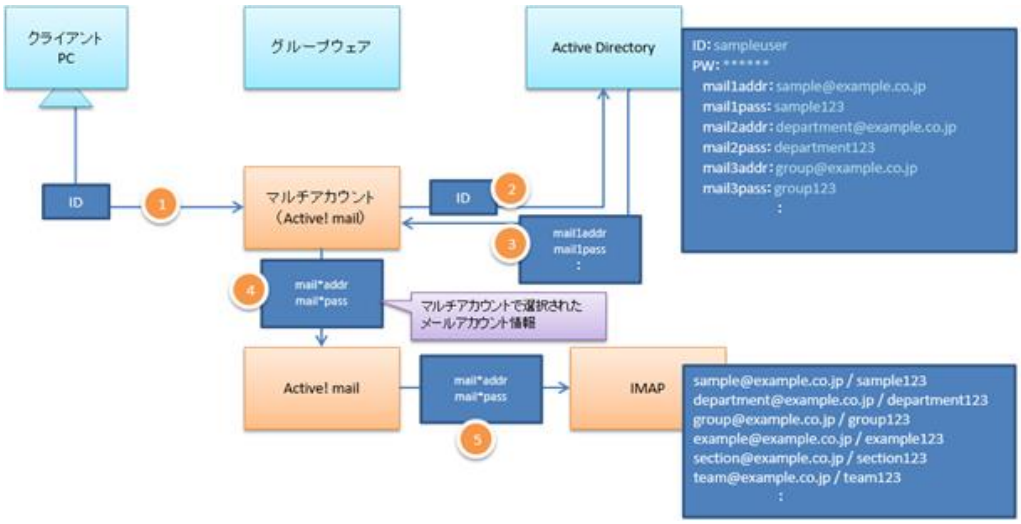

図　庁内メールシステムにおけるシングルサインオンの概要図

(1) クライアント PC からマルチアカウントへの SSO
  ✧ Javascript,ActiveX,WSH を利用して Windows のログインアカウントおよびログイン中のドメインを取得し、マルチアカウントの SSO モジュールをコールする
(2) マルチアカウントの認証（ログインアカウントの有無確認）
  ✧ （1）で取得したログイン中のドメインが正しいものであるか確認する。
  ✧ 正しいドメインだった場合、LDAP 検索により（1）で取得したログインアカウントが ActiveDirectory 上に存在するかを確認する。
  ✧ ログイン中のドメインが正しいものでなかった場合やログインアカウントが ActiveDirectory 上に存在しなかった場合、マルチアカウントのログイン画面を表示し（3）以降は処理しない。

(3) Active! Mail ログイン情報の取得

- ✧ ログインアカウントが ActiveDirectory 上に存在した場合、庁内メールの情報（図の mail1addr）を保有しているかを確認する。
- ✧ 庁内メールの情報を保有している場合は庁内メール利用可能と判断する。
- ✧ 庁内メールの情報を保有していなかった場合、マルチアカウントのログイン画面を表示し（4）以降は処理しない。

(4) Active! Mail へのログイン

- ✧ 庁内メールの情報（図の mail1addr と mail1pass）を使用して、Active! Mail にログインする。
- ✧ Active! Mail は庁内メールの情報（図の mail1addr と mail1pass）により IMAP に認証要求する。

(5) IMAP 認証

- ✧ Active! Mail からの認証要求に対して、IMAP で保持しているアカウント情報を使用して認証する。

（4）ウィルス対策システム

ア　システム概要

- Trendmicro 社の複数のウィルス対策ソフトを用いて三重県行政 WAN 内の全業務端末及び全サーバ機器へのウィルス対策を行うとともに、パターンファイル等の配布、管理を行うシステム。
- 現行のウィルス対策システムにおけるウィルス対策ソフトは、運用期間中において、保守期限が到来したため、後継製品にバージョンアップを行っている。このとき、管理サーバと配信サーバの兼用がサポート対象外となったため、サーバ構成についても見直しを実施している。
- 現在の構成については、「イ　ハードウェア構成・ソフトウェア構成」を参照のこと。

イ　ハードウェア構成・ソフトウェア構成

- インターネットよりパターンファイルをダウンロードするサーバは Proxy セグメントに設置する管理サーバのみとしている。
- 管理サーバから配信サーバにパターンファイルが配信され、その後、配信サーバから各業務端末へパターンファイルが配信される。
- 管理サーバとして、Proxy セグメントに 1 台、LGWAN 系ネットワークに 1 台の構成としており、配信サーバは Proxy セグメントに 1 台、LGWAN 系ネットワークに 3 台の構成としている。
- 別契約にて他のネットワーク（個人情報用ネットワーク、インターネット接続系ネットワーク）に設置された配信サーバについても、現行システムの管理サーバから配信を行っている。

No	設置場所	種別	セグメント	機能	備考
1	津市 IDC	物理	Proxy	管理サーバ	No2,3 へ配信
2	津市 IDC	物理	Proxy	配信サーバ	業務端末へ配信
3	本庁	物理	LGWAN 系	管理サーバ	No4,5,6 へ配信
4	津市 IDC	仮想	LGWAN 系	配信サーバ	業務端末へ配信
5	津市 IDC	仮想	LGWAN 系	配信サーバ	業務端末へ配信
6	津市 IDC	仮想	LGWAN 系	配信サーバ	業務端末へ配信

表　ウィルス対策システムの配置表

- 管理サーバ：配信サーバにパターンファイル等を配信するサーバ
- 配信サーバ：管理サーバからパターンファイル等を受け取り、業務端末へ配布するサーバ

ウ　機能概要

（ア）パターンファイル配信機能

- LGWAN 系ネットワークに接続されている Windows 及び Linux の業務端末やサーバ機器等へウィルス対策ソフトウェア（トレンドマイクロ製 Apex One もしくは Server Protect for Linux）のプログラムやパターンファイルを配布している。

（イ）一元管理機能

- 管理サーバや配信サーバ上で各業務端末に対するパターンファイルや検索エンジンの配布、更新状況やマルウェアの検出状況について、情報を一元的に管理し、画面に表示する機能を提供している。
- 未更新の業務端末に対して Push 型の配信が実施できる機能を提供している。
- マルウェアが発見された場合は、マルウェア名・コンピュータ名・パス名及び対処結果を記載したメールをシステム管理者へ送付している。

（５）運用管理システム（資産管理）

ア　システム概要

- クオリティソフト社製の QND（株式会社大塚商会が販売する QND α Standard）を利用して三重県行政 WAN に接続されている各業務端末に対してインベントリの収集やプログラムの配信を行うためのシステム。
- 各業務端末に対してリモート接続機能も提供している。

イ　ハードウェア構成・ソフトウェア構成

・ 管理サーバとして、マスターサーバ、スレーブサーバを津市 IDC に 1 台ずつ（計 2 台）構築し、それぞれ仮想マシンで構成している。

No	設置場所	種別	セグメント	機能
1	津市 IDC	仮想	LGWAN 系	マスター
2	津市 IDC	仮想	LGWAN 系	スレーブ

表　運用管理システム（資産管理）の配置表

ウ　機能概要

（ア）インベントリ取得・出力機能

・ 毎日、各業務端末のログオン時に QND のインストールチェック（未インストールの場合はインストールを実施する）とインベントリ情報の収集を行っている。

・ 取得している情報は、ハードウェア情報（CPU、メモリ、HDD 容量等）、ウィルス対策ソフト情報（種類、パターンファイル等）、OS 情報（バージョン、適用パッチ等）、アプリケーション情報（インストールされているアプリケーション名）、ソフトウェア情報（保存しているプログラムファイル名等）、レジストリ情報（指定した任意のレジストリ値）、その他（ログオンユーザ名、IP アドレス等）等としている。

（イ）リモート操作機能

・ リモート操作用のコンソールから QND がインストールされた業務端末に対してリモート操作機能を提供している。

・ リモート操作用のコンソールは複数のコンピュータにて起動することができ、複数の操作者による複数の業務端末への同時リモート操作も可能としている。

・ リモート操作時において、業務端末の画面は操作者及び被操作者双方で閲覧及び操作が可能となっている。

（ウ）プログラム配信機能

・ 任意の業務端末に対して、セキュリティパッチ等の任意のプログラムを、任意のタイミングで配信することができる機能を提供している。

（６）運用管理システム（セキュリティパッチ配布）

ア　システム概要

・ Microsoft 社の WSUS を利用し、業務端末に対して任意のセキュリティパッチ、サービスパック等の配信を行うシステム。

イ　ハードウェア構成・ソフトウェア構成

・ WSUS サーバとして、津市 IDC に 1 台、仮想マシンとして、構築している。
・ インターネット上の Windows Update Web サイトと直接同期し、更新プログラムのリストおよび更新プログラム・ファイルにかかる情報を取得している。

No	設置場所	種別	セグメント
1	津市 IDC	仮想	LGWAN 系

表　運用管理システム（セキュリティパッチ配布）の配置表

ウ　機能概要

・ セキュリティパッチ配信機能として、Windows 端末にマイクロソフトのセキュリティパッチやサービスパック等を配信している。また、各業務端末にかかるパッチ適用状況を出力できる。
・ アップストリームサーバとして、他の WSUS サーバ（ダウンストリームサーバ）に対して更新プログラムのリストおよび更新プログラム・ファイルを配信している。

（７）バックアップ・リストアシステム、ログ収集システム

ア　システム概要

・ バックアップ・リストア機能を提供するためのバックアップ・リストアシステム、各サブシステムにおけるログを収集するためのログ収集システムを構築している。

イ　機能概要

・ 庁内メールシステム以外の物理サーバについて、バックアップ・リストアシステムにて、集中バックアップ機能を提供している。
・ ログ収集システムとして、Windows 標準のイベントビューアでは、ログオン及びログアウトの状況が正確に把握できないため、ログオン及びログアウトを行ったユーザやコンピュータの情報を自動取得する仕組みを構築し、提供している。ログオン、ログアウトにかかるログだけでなく、ログオンに失敗したユーザやコンピュータの監査ログについても 1 年以上保存でき、さらに、保存したログを任意に抽出し分析できる仕組みも提供している。

２　本委託業務にて解決したい課題

本委託業務により、解決したい課題は以下のとおり。なお、それぞれの課題に対応した各サブシステムにおける必要な機能要件については、「３　本システムの詳細な機能要件」を参照すること。

（１）全体の課題

ア　現行システムからの機能引継ぎ

- 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。
- 現行システムの内、「庁内メールシステム」については、令和 4 年度に再構築を予定しているが、当面は、既存システムを保守延長し、利用を継続することから、「庁内メールシステム」におけるシングルサインオン機能、マルチアカウント機能について、継続して利用可能な状態にする必要がある。なお、「庁内メールシステム」の保守延長にかかる業務については、現行システムにかかる受託事業者が担当することから、本委託業務の範囲外とする。
- 現行システムの内、「ウィルス対策システム」については、本県が令和 4 年 1 月に契約締結予定の「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務」にて、機能を引き継ぐことを予定しているが、マルウェア対策/EDR 用のソフトウェアへの入れ替えが完了するまでは、既存のウィルス対策システムを継続して運用する必要がある。なお、「ウィルス対策システム」の保守延長にかかる業務については、現行システムにかかる受託事業者が担当することから、本委託業務の範囲外とする。

イ　セキュリティポリシーガイドラインへの対応

- 本県は、現在、αモデル（業務端末を LGWAN 系ネットワークに接続して利用するモデル）による運用を行っているが、効率性・利便性を向上させるため、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）による運用に移行したいと考えている。そのため、令和 2 年 5 月に総務省から公表された「地方公共団体における情報セキュリティポリシーに関するガイドライン」において、β‘モデルで求められている要件について、対応を行なっていく必要がある。さらに、「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」において、令和 3 年度中にも同ガイドラインの改定が予定されていることから、新たなガイドラインについても、対応を行っていく必要がある。
- そのため、今後のセキュリティ対策の方向性を見据え、少なくとも今後数年の変化に耐えられる環境を構築していく必要がある。

（２）庁内ドメインシステムおける課題

ア　外部サービス（クラウドサービス）の利用にかかる課題

- 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。
- 特に、ID/アカウント管理について、サービスに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）、サービス毎にユーザ情報の管理を行う必要がある（アカウントの重複管理）、ライセンス管理や利用者確認などに手間がかかる（管理負荷の増大）、などの課題が顕在化している。さらに、今後、利用するサービスの種類や利用するユーザ数が増大した場合、現行の運用体制では、対応できなくなると考えている。
- 以上のことから、外部サービス（クラウドサービス）にかかる ID/アカウントを一元的、かつ、効率的に管理するため、IDaaS（Identity as a Service）機能を導入する必要がある。
- なお、IDaaS を導入することで、利用したい機能は、以下のとおり。

機能名	機能詳細
認証機能	・認証機能とは、正しい利用者かどうかを確認するための機能のこと。 ・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。 ・この機能を利用することで、低コストで利用しやすく、かつ、高いセキュリティ機能を持った認証が実現できる。
ID 連携機能	・ID 連携機能とは、外部サービス（クラウドサービス）と IDaaS の認証情報を連携させることで、IDaaS の認証を受ければ、外部サービスの再認証を受けることなく利用できるようになる機能のこと。 ・この機能を利用することで、シングルサインオンを実現できる。 ・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。 ・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。

アクセス制御機能	・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。
ID 管理機能（ID 同期機能）	・ID 管理機能とは、外部サービス（クラウドサービス）における ID/アカウント情報について、IDaaS での変更内容を自動的に反映させることができる機能のこと。 ・この機能を利用することで、通常であれば、利用者情報の変更があった場合、それぞれの外部サービス（クラウドサービス）にて個別に利用者情報の変更を実施する必要があるが、IDaaS への変更だけで対応を完了でき、管理者の作業負荷を軽減できる。 ・さらに、IDaaS 自体の ID/アカウント情報についても、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）と同期を行うことで、IDaaS における ID 管理についても省力化が実現できる。 ・ID 管理機能は、それぞれの IDaaS において、一つ一つの外部サービス（クラウドサービス）に対して提供されるものであるため、IDaaS によって、ID 管理機能が利用できる外部サービス（クラウドサービス）に差異があるのが現状だが、利用が多い外部サービス（クラウドサービス）として、Microsoft365 や GoogleWorkspace、slack、box などにおいて、ID 管理機能が利用できる必要がある。

表　IDaaS に求める機能

イ　ActiveDirectory（オンプレミス版の認証基盤）と IDaaS（クラウド上の認証基盤）

- 本県において、各種 ID/アカウントの管理は、庁内ドメインシステム（ActiveDirectory）にて実施しており、また、グループポリシーを利用することで、各種デバイスの管理も行っているため、IDaaS の導入後も各種 ID/アカウント管理は、ActiveDirectory により一元的に実施したいと考えている。
- そのため、ActiveDirectory をオンプレミス版の認証基盤、IDaaS をクラウド版の認証基盤としてそれぞれ、ID/アカウント管理できるような形で構築し、ActiveDirectory 上で ID/アカウント管理を行うことで外部サービス（クラウドサービス）の ID/アカウントについて、一元的に管理が実施できるようにする必要がある。
- 特に、現時点で、本県が利用を行う外部サービス（クラウドサービス）は、決定しておらず、また、将来的には、利用したい外部サービス（クラウドサービス）を、オンデマンド（利用したいサービスを利用したい時に利用したいだけ）で利用する形を想定しているため、ActiveDirectory における ID/アカウント情報の管理方法として、ActiveDirectory の拡張情報と連携する方法やセキュリティグループと連携する方法が利用できる必要がある。
- なお、ActiveDirectory と IDaaS 間の通信が途絶した場合でも、一定期間、利用者に IDaaS 機能を継続して提供するため、パスワード以外の情報を ActiveDirectory から IDaaS に同期し、認証のみを ID 連携にて、IDaaS から ActiveDirectory に対して実施する形を実現できる必要がある。

ウ　セキュリティ対策の強化

- IDaaS に対して、インターネット上からのさまざまな攻撃が想定されるため、セキュリティ対策の強化を行う必要がある。具体的には、許可されないデバイスからのアクセスを拒否できる必要がある。
- 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。

エ　無線 LAN 用の電子証明書

- 本県では、LGWAN 系ネットワークにおいて、無線 LAN 環境を構築し、運用を行っているが、接続可能なデバイスを判定するため、電子証明書による端末認証を行っている。
- しかし、セキュリティポリシーガイドラインの見直し議論において、個々のデバイスに対して、利用者や用途を確認するとともに、端末毎の電子証明書発行や、安全に配布する仕組みなどの構築が求められているため、業務負荷の軽減に配慮しながら、これらのセキュリティ対策を実現する必要がある。

（３）運用管理システム関連

ア　業務端末における脆弱性管理

・ 現行システム導入当初は、業務端末に対するセキュリティ対策の向上を目指して、セキュリティパッチの適用状況を収集し、管理を行ってきたが、年々セキュリティパッチの種類や量が増え、全端末の管理が困難になりつつある。さらに、セキュリティパッチの適用状況を把握するだけでは、脅威度の判定を行うことができないため、結果として、優先的に対応すべき業務端末を把握できず、効果的なセキュリティ対策を実施できなくなってきている。

・ そのため、これまで実施してきたセキュリティパッチの適用状況に加えて、脆弱性の有無についても情報収集し、その結果から各業務端末における脅威度の判定や、脅威度が高い業務端末に対して強制的なセキュリティパッチ配布の他、通信を制限するなどの対応を行うなど、さらなるセキュリティ対策を実現可能にする必要がある。

・ 特に、Microsoft 社製ソフトウェア（OS、Office、IE 等）、Adobe 社製ソフトウェアについては、影響が大きいため、対応していく必要がある。

イ　セキュリティパッチの配布時における課題

・ 現行システムで利用している運用管理システム（セキュリティパッチ配布）では、大容量のファイルを効率良く配信する仕組みがなかったため、大容量ファイルを媒体で配布したり、職場の代表者がコピーし、他の業務端末等へコピーしたり、といった手作業が必要になり、効率性や確実性に課題があった。

・ そのため、大容量のセキュリティパッチの配布や実行について、漏れなく、かつ、効率的に実施していくために、ネットワークに負荷をかけずに配信できる仕組みを備えたセキュリティパッチ配布機能を構築する必要がある。

・ さらに、これまでの運用管理システム（セキュリティパッチ配布）では、Microsoft 社以外のセキュリティパッチ等を配信できなかったが、「ア　業務端末における脆弱性管理」への対応により Microsoft 社以外の脆弱性情報についても取得する形になることから、影響が大きいソフトウェアにについて、脆弱性管理からセキュリティパッチ配布までをシームレスに効率よく実施できるようにする必要がある。

ウ　外部デバイス等の利用制限

・ これまで、情報漏洩対策として、USB メモリや CD/DVD など、大量の情報を外部へ持ち出すことが可能な外部デバイス等に対する利用制限機能について、運用による対応を行い、特段のシステム化はしていなかった。しかし、将来的なセキュリティ対策として、今後、必要になると考えられることから、外部デバイス等に対する利用制限機能を構築する必要がある。

・ なお、実際に外部デバイスの利用制限を行う際は、ユーザ権限や業務端末の種別等による柔軟な制限が可能で、かつ、許可した外部デバイスを 1 年に 1 度棚卸する機能や、利用者からの申請機能、承認機能等についても構築する必要がある。

３　本システムの詳細な機能要件

「２　本委託業務にて解決したい課題」への対応を行うため、本委託業務において、構築するサブシステムの詳細な機能要件は以下のとおり。なお、全ての機能を実現する必要があり、代替機能での実現や機能自体の削減は原則として認めないが、合理的な理由があり、かつ、その理由を本県に説明したうえで、本県が承認した場合に限り、代替機能等により構築を行うことができる。

（１）オンプレミス認証基盤/クラウド認証基盤

ア　全体構成

- 現行システムにおける「庁内ドメインシステム」（ActiveDirectory）について、その機能を引き継ぐとともに必要な機能を強化した「オンプレミス認証基盤」として再構築を行うこと。また、IDaaS（インターネット上の認証基盤）として、「クラウド認証基盤」を新たに構築すること。（以下、オンプレミス認証基盤とクラウド認証基盤を合わせて「統合認証基盤」という。）
- さらなるセキュリティ対策を行うために必要となるプライベート認証局を、統合認証基盤内に構築すること。また、同機能を利用した無線 LAN デバイス認証機能を構築すること。

イ　オンプレミス認証基盤

（ア）基本機能

- 現行システムにおける庁内ドメインシステムの機能を引き継ぐ形でオンプレミス認証基盤として、再構築を行うこと。構築するドメインコントローラの台数（物理サーバと仮想サーバの台数）についても原則として、引き継ぐこと。
- 庁内ドメインシステムで提供していた、DNS/NTP/DHCP サービスについて、それぞれの機能を引き継ぐこと。
- ドメインコントローラの IP アドレスは可能な限り現行ドメインコントローラのものを引き継ぐこと。また、IP アドレスが変更となる場合は、その影響範囲及び対応策を本県に説明のうえ、了承を得ること。
- 更新に際して Active Directory の構成等を変更する必要がある場合は、その影響範囲及び対応策を本県に説明のうえ、了承を得ること。
- 同一セグメント上の業務端末から、ログオン時において、ユーザ名とパスワードをドメインコントローラに送信してから、応答するまでにかかる時間が 5 秒以内となるよう、必要なハードウェアにかかるサーバスペックを決定すること。
- 現行システムにおいて、仮想マシンで提供されている機能の内、現行システムにかかる保守契約期限到来後も継続して機能を提供することができるものについては、そのままの構成にて当面の間、機能提供を行うことも可能とする。ただし、Windows Server 2012 R2 など、契約期間内にサポートが切れるソフトウェアの利用を継続する場合は、本委託業務の契約期間内にバージョンアップ等を行うこと。

（イ）クラウド認証基盤との情報連携

- オンプレミス認証基盤の ID/アカウントについて、クラウド認証基盤に対して、パスワード情報以外の情報を同期できること。また、クラウド認証基盤からの ID 連携要求に対応できること。
- 外部サービス（クラウドサービス）の ID/アカウントを管理できること。なお、管理方法として、セキュリティグループや拡張情報による方法を想定しているが、実現方法は問わないこととする。ただし、20 以上の外部サービス（クラウドサービス）の情報を保持でき、かつ、保持している情報について、CSV 情報の取り込みによる一括情報修正が可能なこと。
- 管理する外部サービス（クラウドサービス）の ID/アカウントは、オンプレミス認証基盤における登録済みの ID/アカウントに紐づけて管理ができること。
- 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。
- オンプレミス認証基盤とクラウド認証基盤間において、ID 管理や ID 連携を実現するために連携用プログラム等が必要になる場合は、当該プログラムを利用するために必要となるサーバ等の構築も合わせて行うとともに、安定的な運用ができるよう、運用・保守業務を行うこと。また、メンテナンス時や故障時を考慮して、冗長構成とすること。

（ウ）他システム連携

- 現行システムにおける庁内メールシステムの他、LGWAN 系ネットワーク内で構築している各種システムは、現行システムにおける ActiveDirectory の機能にて、ID 連携を行い、シングルサインオン機能などを実現しているため、引き続き、利用できること。
- 職員アカウント集中管理システムにより、ActiveDirectory にかかる ID/アカウントの新規、変更、削除申請にかかる受付や承認処理を行っているが、承認処理時に出力される CSV ファイルを用いて、現行システムと同様に、一括修正等ができること。なお、外部サービス（クラウドサービス）にかかる利用者情報等についても、職員アカウント集中管理システムにて管理を行う予定のため、取り込み用の vbs スクリプトについて、更新を行うこと。（現行システムで利用している vbs スクリプトについては、契約後に提示する。）

ウ　クラウド認証基盤

（ア）基本機能

- 外部サービス（クラウドサービス）にかかるID/アカウント管理等を行うため、クラウド認証基盤としてIDaaSをクラウドサービスとして提供すること。
- クラウド認証基盤については、「（イ）クラウド認証基盤における機能要件」を満たすとともに、全ての機能が24時間/365日利用できるものを選定すること。また、クラウド認証基盤にかかるサービスを提供するデータセンターの所在地は日本国内とし、問題が発生した場合に、国内法が適用できること。

（イ）クラウド認証基盤における機能要件

機能名	機能詳細
認証機能	・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。 ・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。
ID連携機能	・外部サービス（クラウドサービス）に対して、ID連携機能が提供できること。 ・SAML連携が可能な外部サービス（クラウドサービス）に対して、シングルサインオンが実現できること。 ・クラウド認証基盤からオンプレミス認証基盤へのID連携を実施している場合、クラウド認証基盤側において、キャッシュ機能等を有することで、オンプレミス認証基盤と通信ができない状態でも一定条件の元、ID連携機能を提供できること。 ・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。 ・最初に外部サービス（クラウドサービス）にアクセスしてからのシングルサインオン（SP Initiated SSO）、及び、クラウド認証基盤にアクセスしてからのシングルサインオン（IdP Initiated SSO）に対応していること。
アクセス制御機能	・統合認証基盤での認証後、利用可能な外部サービス（クラウドサービス）を一覧で表示できる画面を提供できること。（利用できないサービスは非表示、グレー表示等ができること。） ・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。）
ID 管理機能（ID 同期機能）	・オンプレミス認証基盤（ActiveDirectory）とクラウド認証基盤との間で ID 管理（ID 同期）が実施でき、オンプレミス認証基盤のパスワード以外の ID/アカウント情報について、クラウド認証基盤の ID/アカウントとして登録できること。 ・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で ID 管理（ID 同期）を行っている ID/アカウントの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。 ・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。 ・オンプレミス認証基盤とクラウド認証基盤間において、ID 管理や ID 連携を実現するために連携用プログラム等が必要になる場合は、当該プログラムを利用するために必要となるサーバ等の構築も合わせて行うとともに、安定的な運用ができるよう、運用・保守業務を行うこと。また、メンテナンス時や故障時を考慮して、冗長構成とすること。

	・クラウド認証基盤においても、オンプレミス認証基盤と同様に、ID/アカウント情報を登録できること。
セキュリティ要件	・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。 ・クラウド認証基盤において、定期的な脆弱性の検査や対策を行うなど、セキュリティ対策を実施していること。 ・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。 ・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。） ・クラウド認証基盤に直接登録している利用者に対して、連続でログインが失敗した際、自動でロックできること。 ・24 時間 365 日、システム監視を実施していること。 ・E メールによる問い合わせ受付が提供されており、障害時等の問い合わせが可能なこと。
管理者機能	・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。 ・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。 ・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。 ・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。

	・ID/アカウントについて、管理者側の操作で情報の一括登録、更新、削除等ができること。 ・オンプレミス認証基盤とクラウド認証基盤のそれぞれで登録したID/アカウントについて、管理画面等で一元的に管理できること。

表　クラウド認証基盤に求める機能

（ウ）その他

- クラウド認証基盤について、操作マニュアルやその他の関連文書について、日本語で提供すること。
- 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。

エ　統合認証基盤

（ア）プライベート認証局機能

- 統合認証基盤において、プライベート認証局機能を構築し、X.509 v3 証明書を発行できる機能を提供すること。また、CRL（Certificate Revocation List）及び OCSP（Online Certificate Status Protocol）に対応し、他の電子証明書にかかる失効情報の把握や、発行した電子証明書の失効状態の提供ができること。
- 統合認証基盤における 1 利用者あたり、5 枚以上の電子証明書の発行ができること。また、電子証明書の有効期限を任意に設定できること。なお、デバイス用に電子証明書を発行することを想定している。
- 電子証明書の発行を行う際の利用者側における作業として、電子証明書を発行するデバイスの準備、当該デバイス上での鍵ペア生成、電子証明書の発行申請、(管理者側での電子証明書にかかる承認処理)、電子証明書の取得、といった一連の操作を想定しているが、これらの操作が安全かつ簡単に行える機能を提供すること。
- 発行された、電子証明書や秘密鍵について、盗難や悪用（他のデバイスへの流用）などがされないような機能が提供できること。
- 電子証明書の発行申請時における必須情報として、利用者情報の他、導入を予定しているデバイスの情報（OS、コンピュータ名、ドメイン名等）を必須項目として入力させることができること、もしくは、電子証明書の発行時にデバイスの情報を自動で収集できること。
- 発行済み電子証明書について、効率的に管理できること。
- 構築したプライベート認証局に対して、信頼する認証局を登録することにより、外部の認証局で発行された電子証明書についても認証できること。
- 電子証明書の更新処理について、利用者側の操作のみで完了できること。

・ 不要となった複数の電子証明書について、管理者が任意のタイミングで一括して失効処理ができること。
・ 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。
・ 別途用意された CSR（証明書署名要求）ファイルをインポートすることで、サーバ用電子証明書を発行できること。また、電子証明書の発行時に秘密鍵入りの PKCS#12 形式や PEM 形式で発行できること。
・ 統合認証基盤とは別に、プライベート認証局機能を構築することも可とするが、その場合は、統合認証基盤における ID/アカウント情報と電子証明書の情報を紐づけるなど、関連付けを行うことにより、一元的な管理ができること。

（イ）無線 LAN デバイス認証機能

・ 無線 LAN におけるデバイス認証方式として、IEEE802.1X 認証における EAP-TLS により、認証ができること。
・ EAP-TLS を利用するために必要となる RADIUS サーバの構築も合わせて行うとともに、安定的な運用ができるよう、運用・保守業務を行うこと。また、メンテナンス時や故障時を考慮して、冗長構成とすること。
・ EAP-TLS における認証で利用する各業務端末の電子証明書として、統合認証基盤のプライベート認証局機能により発行した電子証明書を利用できること。
・ RADIUS の認証方式として、EAP-TLS、EAP-TTLS、PAP に対応していること。
・ RADIUS サーバの無線 LAN における認証ログについて、管理者から容易に閲覧できること。

（２）統合運用管理システム

ア　全体構成

・ 現行システムにおける「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）」について、その機能を引き継ぐとともに必要な機能を強化した「統合運用管理システム」として再構築を行うこと。
・ 統合運用管理システムは、各業務端末にインストールするエージェントソフトウェアと、エージェントソフトウェアから情報を集約して管理を行う管理サーバで構成すること。

・ 現行システムにおける管理サーバは、「運用管理システム（資産管理）」で 2 台、「運用管理システム（セキュリティパッチ配布）」で 1 台の計 3 台で構成されているが、統合運用管理システムでは仮想マシンで、かつ、サーバ台数が 1 台の構成で構築を行うこと。なお、複数台で構築しても、種々の機能を一元的に管理できる場合や、合理的な理由により物理サーバによる構築が必要な場合は、本県に説明後、承認を受けたうえで、受託事業者が提案する構成で構築を行うことができる。なお、物理サーバを導入した場合は、安定的な運用ができるよう、運用・保守業務を行うこと。また、メンテナンス時や故障時を考慮して、冗長構成とすること。
・ 本県では、令和 4 年 1 月契約締結予定の別契約にて、EDR を導入する予定のため、統合運用管理システムにおける EDR 機能（または、EDR 機能を前提として提供可能となる各種機能）については、利用する予定がないため、注意すること。

イ　エージェントソフトウェアの配布と削除

・ エージェントソフトウェアを業務端末へ効率的、かつ、漏れなく配布するために必要となる、インストールパッケージの作成や、配布状況の進捗管理機能等について、利用できること。
・ 各業務端末からエージェントソフトウェアを削除するためのインストールパッケージも作成できること。
・ エージェントソフトウェアは、利用者の操作で許可なくアンインストール等ができないようパスワード等で保護できること。
・ 現行システムのエージェントソフトウェアとして、クオリティソフト社製の QND（株式会社大塚商会が販売する QND α Standard）を利用しているが、エージェントソフトウェアが変更になる場合は、変更後のエージェントソフトウェアの導入後、既存のエージェントソフトウェアのアンインストールを実施すること。なお、既存のエージェントソフトウェアにかかるアンインストール用のプログラムについては、本県から提供する。

ウ　資産管理機能

（ア）基本機能

・ 各業務端末やサーバ機器（WindowsOS に限る）にエージェントソフトウェアを導入することで、資産管理機能が利用できること。
・ 管理サーバにおいて、収集した情報を一覧表示できる画面（資産台帳画面）が利用でき、同画面にて収集した情報の一元管理ができること。また、各機能が統一されたユーザインターフェースで利用できること。

（イ）インベントリ収集機能/資産台帳画面

- 各業務端末から以下のハードウェア情報、ソフトウェア情報などのインベントリ情報を収集できること。
  - ✧ 「プログラムの追加と削除」に登録されているアプリケーション情報
  - ✧ Microsoft 社が提供するセキュリティパッチ等の適用状況
  - ✧ 本県が指定する任意の INI、レジストリの値
- 業務端末のインベントリ情報について、定期的、又は、任意のタイミングにて、情報を収集できること。
- 何らかの理由により、業務端末からインベントリ情報の取得が出来なかった場合、自動的に再送処理が実施できること。
- 業務端末に接続した USB メモリ等の外部デバイスにかかる情報を取得できること。
- インベントリ情報の収集がスムーズに実施できるよう、エージェントソフトウェアから管理サーバに対する十分な同時接続に対応できること。
- 収集したインベントリ情報について、資産台帳画面にて一覧表示ができ、また、個々の業務端末の詳細画面にて全てのインベントリ情報の表示ができること。
- 資産台帳画面において、任意の列を追加でき、画面上での修正や CSV データ等の取り込み等による一括編集ができること。
- 資産台帳画面において、フィルター機能を有し、条件を入力することで、表示される情報を抽出できること。フィルター条件として、「○○を含む/含まない」「○○と一致する/一致しない」「○○で始まる/始まらない」など、の設定ができること。
- 資産台帳画面において、任意の条件で絞り込んだ情報を CSV 等で外部に出力できること。
- 資産台帳画面にて、各業務端末の状態を視覚的にわかりやすく表示できること。

（ウ）ライセンス管理機能

- 各業務端末におけるソフトウェアのインストール状況の管理ができること。
- 管理するソフトウェアについて、エディションやバージョン等の細かな違いにより、ソフトウェア名が一致しないソフトウェアについてもまとめて管理できること。
- 管理するソフトウェアについて、ライセンスの取得状況や割り当て数、インストール済の端末数等の管理ができること。

エ　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

- 各ソフトウェアに対する脆弱性情報について、主なメーカーや情報提供サイト等から自動的に最新情報を取得し、管理できること。特に、Microsoft 社製品と Adobe 社製品にかかる脆弱性情報を取得し、管理できること。
- 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。
- 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。
- 資産台帳画面にて、各業務端末で確認されたそれぞれの脆弱性に対して、検索や抽出ができること。なお、抽出条件として、キーワードや深刻度などが利用できること。

（イ）セキュリティパッチ管理機能

- 「（ア）脆弱性管理機能」にて取得したそれぞれの脆弱性情報について、対応するセキュリティパッチ情報を自動的に取得し、管理できること。特に、Microsoft 社製品と Adobe 社製品にかかるセキュリティパッチ情報を取得し、管理できること。
- 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。
- 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。

（ウ）セキュリティパッチ配布機能

- 脆弱性が存在し、かつ、その脆弱性に対応したセキュリティパッチが存在する業務端末について、セキュリティパッチを安定的、かつ、効率的に配布できること。
- セキュリティパッチを配布する際に、必要となる詳細情報として、対象端末、配布実施日時、配布するセキュリティパッチの詳細、等を指定する必要があるが、これらの詳細情報をまとめて「タスク」として管理ができること。
- 作成したタスクにより対象となる業務端末への一斉配信や任意のタイミングでの配信、任意の業務端末への配信等、安定的なセキュリティパッチ配布が実施できること。
- タスクの作成や管理は、GUI 画面により実施できること。

- タスクとして、脆弱性に対するセキュリティパッチ配布以外に任意の情報やレジストリ情報の取得や編集、任意のプログラムの実行などが、実施できること。
- ログオンしているユーザの権限に依存せずにセキュリティパッチの配布が実施できること。
- セキュリティパッチ配布の実行結果について、成功、失敗、中止、未実施など、各業務端末における実施状況を把握し、管理できること。また、成功しなかった業務端末に対し、再度のセキュリティパッチ配布が用意に実施できること。
- 大容量のセキュリティパッチにかかる各業務端末への配信の際に、ネットワークや業務端末に大きな負荷がかからないような負荷軽減機能（利用帯域の制限、代表端末から再配布、プログラムの分散配布など）が利用できること。

（エ）MicrosoftUpdate における QU と FU

- Microsoft 社から提供される更新プログラムとして、毎月配信される QU（Quality Update）と年 2 回配信される FU（Feature Update）があるが、QU、FU のいずれについても最新情報の取得ができること。
- QU、及び、FU の情報取得後、速やかに適用タスクの作成ができること。
- 資産台帳画面から業務端末を指定して WindowsUpdate のスケジュール実行または即時実行を実施できること。
- 取得した QU と FU のいずれについても、各業務端末への配信の際に、ネットワークや業務端末に大きな負荷がかからないような負荷軽減機能（利用待機の制限、代表端末から再配布、プログラムの分散配布など）が利用できること。
- 業務端末に対して、Windows Update の有効/無効の設定が資産台帳画面から実施できること。

オ　外部デバイス（USB メモリ）等の利用制限機能

- USB メモリや CD/DVD ドライブ等の外部デバイス等に対して、利用の可否にかかる設定（使用可能、読み取りのみ可能、使用不可）を資産台帳画面等から容易に設定できること。また、統合認証基盤等と連携し、利用者単位や業務端末単位においても、利用の可否等の設定を同様に設定できること。
- 使用禁止のデバイス接続時にメッセージを表示できること。
- 業務端末から外部デバイスの制御設定の変更を申請できること。
- 相当数の利用希望に日々、対応していくために、利用者が未許可の USB メモリを接続した後、申請画面等によりデバイスの利用申請をスムーズに実施できること。また、申請後、管理者側で承認処理等を行うなどにより利用できるようになるなど、スムーズな承認処理が実施できること。

・ 許可した外部デバイスに対する棚卸機能として、利用者側から存在確認を行えるような仕組みを利用できること。また、存在確認が実施されない外部デバイスに対して、当該外部デバイスが利用された業務端末やログインユーザ等から利用していた可能性が高い利用者等について、確認ができること。
・ カードリーダーや内蔵ドライブ等に関わらず、メディア個体を識別して制御可能であること。（製造番号等が取得できないものなどについては、識別不要。）
・ 業務端末にて検知した外部デバイスについて、自動的に情報を取得し、管理できること。
・ 外部デバイス（USB メモリ）に格納されているファイルの一覧を取得できること。

カ　リモートコントロール機能

・ 利用者側のデスクトップ画面を管理者側から操作できる、リモートコントロール機能を提供できること。
・ 管理者側から同時に別々の業務端末へリモート接続が実施できること。このとき 20 台までの同時接続に対応すること。
・ リモートコントロール機能により、利用者側と管理者側で画面を共有することができ、問い合わせ対応や、操作指導等に利用できること。

キ　業務端末に対する利用制限

・ 業務端末のデスクトップ上にハードウェア情報や任意の文字列（メッセージ）を表示できること。
・ 業務端末における任意のファイルを検索できること。検索後、ファイル名の他、ファイル作成日時やファイルパス、容量等により抽出等ができること。
・ 業務端末に対して、特定の宛先以外への通信を制限するなどの通信制限ができること。

ク　不正端末検知機能

・ エージェントソフトウェアが未導入の機器（未インストールの業務端末の他、悪意ある端末等）を検知し、資産台帳画面に自動登録できること。このとき、業務端末以外の確認済みの機器（ネットワーク機器等）については、グループ分けや非表示設定等、業務端末と視覚的にわかりやすく分けて表示ができること。

（3）バックアップ・リストアシステム

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。

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。

（４）ログ収集システム

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。

４　ハードウェア・ソフトウェアにかかる要件

（１）基本的な考え方

本システムの設計、構築、導入及び運用に伴い必要となる全てのハードウェア、ソフトウェア等の物品（以下、納入物品という。）の取得、設定に関することを業務範囲とする。

納入物品の設置に伴って必然的に必要となる物品（ラック取り付け金具や、ケーブル等の接続部品等）についても提供すること。

落札決定後速やかに業務計画書の一部として納入物品の一覧を提出することとするが、納入時点での製品状況が業務計画書提出時点より変わった場合は、本県の承認を得たうえで最新の製品状況に従い最適な物品を納入すること。

納入物品は、買い取りで提供すること。また、中古品であってはならない。

納入物品等に伴うマニュアル、技術資料等については、必要部数を提供すること。

納入に際して、梱包材、本県が不要と判断する付属品、マニュアル等を撤去すること。

バックアップ及びクリーニングに必要な外部媒体等がある場合は、委託期間内において必要な量を見積り、確保するとともに、本県の要請に応じ納入すること。

運用期間終了後、本委託業務範囲に係る物品（本委託業務で導入したハードウェア等）については、本県が指示するものを除き、受託事業者側で撤去（データの完全な消去を含む）を行うこととし、データの消去と機器の廃棄を証明する書類を提出すること。

納入したソフトウェアは業務終了後も本県にて利用できるものとすること。

納入物品のすべてを保守対象とし、一つの窓口で対応すること。

（２）ハードウェア要件

各サブシステムにかかるサーバの設置場所等については、下表のとおりを想定しているが、性能要件、設置要件等を踏まえたうえで、サーバ構成を決定すること。

統合サーバについての仕様等の詳細については、資料２「統合サーバの利用について」を参照のこと。なお、本県が提示する構成にて、スペックが不足する場合は、追加割り当てが可能である。

物理サーバとして納入するハードウェアについて、性能要件を満たすよう、受託事業者においてサイジングを行うこと。なお、性能要件を満たさない場合は、ハードウェア等の増強を行うこととし、増強するために必要となるハードウェアの調達、設定、保守も本委託業務の範囲に含むものとする。

１ 台のサーバで複数のサブシステムを兼用させないこととするが、合理的な理由がある場合は、本県に説明後、承認を得たうえで、受託事業者が提案する構成で構築を行うことができる。

物理サーバを設置する場合、安定的な運用ができるよう、運用・保守業務を行うこと。また、メンテナンス時や故障時を考慮して、冗長構成とすること。

バックアップ・リストアシステムは、ストレージが必要になると想定しているため、運用要件を考慮し、適切な製品選定を行うこと。

ディスプレイはラックマウントタイプとすること。

No	サブシステム	設置場所	種別	セグメント	備考
1	オンプレミス認証基盤	津市 IDC	物理	LGWAN 系	
2		津市 IDC	仮想	LGWAN 系	
3		津市 IDC	仮想	LGWAN 系	
4		津市 IDC	仮想	LGWAN 系	
5		本庁	物理	LGWAN 系	本庁に仮想環境なし
6		本庁	物理	LGWAN 系	
7		本庁	物理	LGWAN 系	
8	統合認証基盤（連携用）	津市 IDC	仮想	LGWAN 系	冗長構成
9		津市 IDC	仮想	LGWAN 系	
10	統合認証基盤（RADIUS）	津市 IDC	仮想	LGWAN 系	冗長構成
11		津市 IDC	仮想	LGWAN 系	
12	統合運用管理システム	津市 IDC	仮想	LGWAN 系	
13	バックアップ・リストアシステム	津市 IDC	物理	LGWAN 系	ストレージ別途
14	ログ収集システム	津市 IDC	仮想	LGWAN 系	

表　運用管理システム（セキュリティパッチ配布）の配置表

（3）ソフトウェア要件

新規に納入するソフトウェアは、契約時における最新バージョンの使用権を確保すること。なお、最新バージョンを使用しない場合は、最新バージョンの使用権を確保したままダウングレードを行うこと。

使用するソフトウェアはシステムへの影響がない限り、最新のセキュリティパッチの適用を行ったうえで納入すること。

使用ソフトウェアとして、要件を満たすソフトウェアを選定し、納入すること。

（4）ハードウェア設置要件

ア　共通要件

- 機器の導入にあたり、各機器の搬入、設置、設定作業は基本的にすべて受託事業者が行うこと。
- サーバのディスプレイ、キーボード等に関しては複数サーバ間で共用するなどの省スペースに配慮した構成とすること。
- ラックに機器をマウントする際には、空調・ファンの稼動など、ラック内の温度に考慮した設置を行うこと。
- ラックの設置位置においては、ブランクパネル等を使用し通気通路を考慮すること。
- ラックにマウントできない機器に関しては耐震バンド等により耐震・免震措置を施すこと。

・ 機器・ラック・分電盤・電源ケーブル・通信ケーブルにラベル表記すること。
・ 通信ケーブルに負荷の掛からないケーブリングを施すこと。
・ 設置場所への納入および設置作業、電源工事、配線工事ならびにネットワークへの接続作業の実施においては、必要に応じて実施日時を本県と調整すること。また、搬入時は各設置スペース管理者が指示する搬入口やエレベータ等を使用し、設備、器物破損を防止するための措置を講じること。

イ　本庁 7 階サーバルーム

・ サーバ及びその付属機器は全て、本県が指定する 19 インチラック（1 ラック以内）に搭載すること。なお、現行機器が設置されているラックは本システム用のラックとは別ラックであり、新旧機器の併設が可能である。
・ ラック単位に無停電電源装置を設置し、同一ラック内のサーバ等の機器へ電源供給を行うこと。
・ 現行システムの機器の一部は非常用電源に接続されているため、機器更新後はこの非常用電源への接続を行うこと。
・ ラックの規格は H2,000mm×W600mm×D1,000mm（41U）である。
・ 本県が準備するスイッチのポートからの UTP ケーブル敷設作業および接続作業を行うこと。なお、スイッチと本システムのサーバは別ラックである。
・ 本庁のラックは本県が用意する。

ウ　津市 IDC

・ サーバ及びその付属機器は全て、本県が指定する 19 インチラック（1 ラック以内）に搭載すること。なお、現行機器が設置されているラックは本システム用のラックとは別ラックであり、新旧機器の併設が可能である。
・ ラックの規格は H2,000mm×W700mm×D1,000mm（42U）である。ただし、各ラックにパッチ盤及び電源盤が設置されているため、実質的に利用できるのは 35U 程度である。
・ 同一ラック内のパッチ盤までの UTP ケーブル配線及びラック内の UTP ケーブル敷設、接続作業を受託事業者の作業とする。なお、ラック間配線については本県が必要な対応を行うが、ラック間配線には、2 週間程度を要するため、余裕をもって設置計画を立てること。

エ　受託事業者が利用するデータセンター

・ 物理サーバ等の設置場所として、本庁 7 階サーバルーム、及び、津市 IDC 以外のデータセンター（以下、「受託事業者が利用するデータセンター」という。）を利用する場合は、ラックの利用料やラック配線、通信回線にかかる費用等、全ての費用について、本委託業務の範囲内とし受託事業者が負担すること。
・ 受託事業者が利用するデータセンターとして津市 IDC 以外のデータセンターを利用する場合、当該データセンターについては、以下の要件を満たすこと。

（ア）基本要件

- 受託事業者の入退館及び館内作業が可能であること。
- 受託事業者による機器設置室内での作業は、土日祝日を含めた 24 時間 365 日可能であること。
- 計画的な定期保守点検などによる設置機器のサービス停止がないこと。
- データセンター事業者は、5 年以上の運用実績を有すること。
- データセンターファシリティスタンダードのティア 3 相当以上のティアレベルに準拠していること。なお、設備に関するその他の要件については「（イ）設備要件」を参照すること。

（イ）設備要件

要件	詳細
情報セキュリティマネジメントシステム	・JIS Q 27001 又は ISO/IEC 27001 に基づく認証を取得している組織によって運用されていること。
立地	・国内に設置された施設を利用することとし、データ保管場所が特定できる場所であること。 ・データセンターは活断層上に建設・設置されていないこと。
地震対策	・建物は、震度 6 強の地震に対して建物の仕上げ及び設備に損傷を与えない設計の耐震構造の建築物であること。
火災対策	・火災の予兆を検知できるシステムが設置されており、ガス消化設備を有していること。
災害発生時の避難対策	・建物は、非常口、非常照明設備及び避難誘導標識等が設置されており、保守作業員が災害時に円滑な避難ができること。
落雷対策	・建物には、落雷の被害を受けない対策がなされていること。
防水対策	・建物には、水害の被害を受けないような防水対策を施していること。ただし、河川、高潮、津波の氾濫想定水位に対し、データセンタービルの 1 階床標高が上回っている場合はその限りではない。
防犯対策	・建物への入館、機器設置室への入退室、建物からの退館において、入室者を識別及び記録できる複数段階のセキュリティ設備（IC カード等）により許可されたもののみ入退室が可能なこと。 ・入退館管理は、24 時間 365 日行っていること。 ・主要な出入口は、監視カメラ等により映像を記録すること。

電源対策	・2 系統以上で、冗長性を確保していること。 ・建物の電源設備の法定点検及び工事の際においても、機器の停電時対策をとる必要のないこと。 ・停電時にシステムを運用するために十分な電源容量を持つ非常用自家発電装置を備えていること。 ・停電時に自家発電装置が安定的に起動するまでの間、瞬断することなくシステムに十分な電力供給が可能な無停電電源装置を設置していること。無停電電源装置は冗長構成がとられていること。
空調設備	・機器設置室は空調設備からの漏水対策を行っていること。または空冷式の空調機を採用していること。 ・機器設置室の主要な空調設備機器については、予備機が設置されており、主要機器が故障の場合でも必要な冷却能力を確保できること。

表　データセンターの設備要件

５　業務詳細

（１）設計業務全体にかかる基本方針

本システムの安定した稼動、業務の継続性を第一とし、構築期間、移行期間、運用期間を通じて、安全で確実な運用が可能となるような設計とすること。

設定変更等の作業を実施する場合は、サービス設定ミス等に起因するリスクや、作業に伴うサービス停止時間の短縮を考慮し、原則として、作業手順書を作成し、各作業に対するテストやリハーサルが可能となるようにすること。

本委託業務を実施する中で、障害等の発生により作業が中断した場合を考慮し、可能な限り、切り戻し手順についても設計を行うこと。

本県の担当職員が実施しなければならない作業がある場合は、作業時間を考慮し、余裕をもって依頼を行うこと。

関係する受託事業者等に対して、作業の依頼等を行う場合は、拘束時間を短くするなど、負担が極力少なくなるよう留意すること。

作成した設計書、手順書等については、作成の都度、本県に対して説明を行い、承認を得ること。

（２）事前調査にかかる要件

本県が本委託業務の契約締結後に提供する、既存システム（現行システムを含む）や既存ネットワーク等に関する資料について、内容を確認し、既存システムや既存ネットワーク等に関する詳細を把握すること。

確認した内容等について、確認が必要な点がある場合は、既存事業者との協議を行い、詳細を確認すること。

本システムの構築時において想定される、現行システム等の受託事業者等に対する設定変更依頼等にかかる実施可否の詳細について確認すること。

（３）全体構成と機能要件

ア　全体構成

- 本システムにおける全体構成については、本県に対して詳細な説明を行い、承認を得たうえで設計を行うこと。
- 障害時等の業務継続性や冗長構成等についても設計に盛り込むこと。

イ　機能要件

- 本システムにおける機能要件の設計においては、「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　仕様書」の他、「３　本システムの詳細な機能要件」「４　ハードウェア・ソフトウェアにかかる要件」を踏まえて実施すること。
- 本システムにおける各サブシステムの他、本委託業務で構築を行う全ての機能について、本県に対して詳細な説明を行い、本県の承認を得たうえで設計を行うこと。

・ 本システムの構築により利用可能となる各種機能について、「サービス定義書」に反映し、作成したサービス定義書について、本県に対して報告し、承認を得ること。

（４）構築業務等の設計にかかる要件

ア　構築設計

・ 本システムを構築するために必要となる全ての設計として、構築設計を行うこと。
・ 構築設計にあたっては、現行システムをはじめ、既存システムや既存ネットワークなどの設定及び構成を踏まえたうえで、実現可能で、かつ、既存の構成等にできるだけ影響を与えないように設計すること。
・ 「（３）全体構成と機能要件」にて策定した「サービス定義書」に定義した機能を提供するために必要となる全ての構築業務について設計を行うこと。
・ 本システムの構築後、提供される各機能に対して、稼働試験が実施できるよう、試験内容についても設計を行うこと。
・ 運用期間における機器の不具合や障害の発生を想定し、監視設計を行うこと。また、監視や検知の動作確認方法やアラート通知等にかかる試験についても設計を行うこと。
・ 本システムにおける各機能において、冗長化された部分がある場合（例えば、Active/Standby 構成の機器や通信経路の切り替えなど)、切り替え作業にかかる試験、及び、切り戻し試験についても設計を行うこと。
・ 全ての構築作業及び各種試験が完了した段階で、構築された本システムが、機能面、運用面等において要求仕様を満たし、かつ、正常に稼動していることを最終的に判断することができるような試験についても設計を行うこと。

イ　経路設計

・ 本システムは、LGWAN 系ネットワーク上に構築することとしているが、インターネットを含む、物理的、論理的に分割された他のネットワークと通信を行う必要がある場合は、経路設計として、通信経路や利用ポートなどの設計を行うこと。
・ 経路設計にあたっては、既存ネットワークの受託事業者や運用管理担当者と調整を行い、可能な限り、シンプルな構成となるよう留意すること。

ウ　データセンターの利用にかかる詳細設計

・ 本システムを構築するうえで、本庁 7 階サーバルーム、津市 IDC、受託事業者が利用するデータセンター等を物理サーバ等の設置場所として利用することを想定しているが、「４（４）ハードウェア設置要件」を満たしたうえで、ラック構成図やラック内配線等、必要な設計を行うこと。

・ 本システムを導入することにより、インターネットへの通信に大きな負荷をかける場合は、セキュリティクラウドにおけるローカルブレイクアウト回線を利用する構成として設計を行うこと。（通信容量が、おおよそ 10Mbps 未満の場合は、セキュリティクラウドにおける通常の通信経路を利用する。）

（５）導入業務等の設計にかかる要件

ア　導入設計

・ 本システムを導入するために必要となる全ての設計として、導入設計を行うこと。
・ 導入設計にあたっては、現行システムをはじめ、既存システムや既存ネットワークなどの設定及び構成を踏まえたうえで、実現可能で、かつ、既存の構成等にできるだけ影響を与えないように設計すること。
・ 本システムにおける全ての機能にかかる導入業務について漏れなく設計を行うこと。
・ 本システムの導入後、提供される各機能に対して、稼働試験が実施できるよう、試験内容についても設計を行うこと。
・ 全ての導入作業及び各種試験が完了した段階で、導入された本システムが、機能面、運用面等において要求仕様を満たし、かつ、正常に稼動していることを最終的に判断することができる試験内容についても設計を行うこと。
・ 作成した導入設計について、可能な限り、リハーサルを実施することとし、その結果について、本県に対して説明し、承認を得ること。

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。

ウ　エージェントソフトウェア導入設計にかかる要件

- 本委託業務を実施するために、各業務端末に対してエージェントソフトウェアの導入を行う必要があるが、各業務端末に対して既存のエージェントソフトウェアから本システムが配布するエージェントソフトウェアへ入れ替えを行う作業について、エージェントソフトウェア導入設計を行うこと。
- エージェントソフトウェア導入設計にあたっては、本県、及び、運用管理担当者が、既存エージェントソフトウェアの活用やログオンスクリプトの利用などにより、実施する形を想定し、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エージェントソフトウェア導入が実施できるよう設計を行うこと。
- 作成したエージェントソフトウェア導入設計について、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。
- エージェントソフトウェア導入作業の実施当日において、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。
- エージェントソフトウェアの導入にかかる進捗状況を管理するための設計も併せて行うこと。なお、進捗管理として、エージェントソフトウェアの入れ替え状況を把握するだけではなく、未導入の業務端末への配布方法の他、新たに導入された機能を用いた展開作業等についても設計に含めること。

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。

オ　導入計画書

- 導入業務の実施に向けて、導入設計の内容に沿って、具体的な日時や担当者、作業時間等を決定した導入計画書を作成すること。
- 導入計画書は、作成次第、本県に向けて説明し、承認を得ること。

・ 導入業務により、現行システムや本システム等にて提供される各種機能について、大きく変更や制限される場合は、土日祝日や夜間作業を基本とすること。なお、各種機能に大きな影響がないと認められる場合は平日日勤帯での作業も可とするが、必ず本県の承認を得ること。また、土日祝日、夜間の作業であってもサービス停止時間を極力短縮するよう努めること。

（６）運用・保守業務の設計にかかる要件

ア　基本的な考え方

・ 本システムを安定的に稼働させるために必要となる、運用・保守業務について、運用・保守設計を行うこと。
・ 納入した全てのハードウェア、及び、ソフトウェア等、本システムのすべてを運用・保守業務の対象として設計を行うこと。
・ 運用・保守業務に必要となる全てのハードウェア、及び、ソフトウェア等の準備は全て本委託業務の範囲内とする。
・ 運用・保守設計にあたっては、運用・保守業務を実施するために必要となる役割分担や運用・保守体制についても設計に含めること。
・ 運用・保守業務にかかる対応窓口はできる限り一つとすること。
・ 運用・保守業務には、リモート保守環境の利用を可能とするため、必要に応じて、適宜、利用を行うこと。詳細は、資料３「リモート保守環境の利用について」を参照すること。

イ　運用・保守業務にかかる役割分担

・ 本システムの安定稼働後は、本システムにかかる運用・保守業務の一部を運用管理担当者にて担当させることができるが、運用管理担当者による業務を開始するまでに、本県、及び、運用管理担当者に対し、運用管理担当者に実施させる運用・保守業務について説明を行い、承認を得る必要があるため、注意すること。
・ 運用管理担当者にて実施可能な運用・保守業務の想定は以下のとおりだが、詳細な業務内容と役割分担について設計を行うこと。なお、運用管理担当者が対応する業務であっても、なんらかの理由により、対応ができない場合は、受託事業者が対応を行なう必要があるため、注意すること。
・ 運用管理担当者が実際に業務を実施する前に、それぞれの業務に対するマニュアル等の作成や、各業務に対する引継ぎや研修等を行う必要があるため、留意すること。

作業内容	運用管理担当者	受託事業者
日常の設定作業	（ア）	
バックアップデータの管理	（イ）	
バックアップ・リストア	（ウ）	
稼働監視	（エ）	
性能・構成管理	（オ）	
ログ管理	（カ）	
日常運用業務に対する支援、提案		（ア）
パッチによる影響等の情報提供		（イ）
パッチインストール	（キ）	
バージョンアップによる影響等の情報提供		（ウ）
バージョンアップ作業		（エ）
脆弱性情報等による対象端末の抽出		（オ）
セキュリティパッチ配布用タスクの作成		（カ）
業務端末へのセキュリティパッチの配布	（ク）	
庁舎停電対応	（ケ）	
障害一次切り分け	（コ）	
障害対応		（キ）
障害後是正措置・予防措置		（ク）
運用マニュアルの改訂		（ケ）
外部サービス（クラウドサービス）導入支援		（コ）
既存システムとのシステム連携支援		（サ）

表　運用管理システム（セキュリティパッチ配布）の配置表

ウ　運用管理担当者が行うもの

・ 以下の業務については、運用管理担当者が担当することを想定しているため、詳細な業務内容について、設計を行うこと。
・ なお、業務内容にかかるマニュアルについては受託事業者にて作成し、運用管理担当者に業務の説明を行う必要があるため、注意すること。

（ア）日常の設定作業

・ アカウントの登録、削除等、運用マニュアルに基づき日常の設定作業を行う。

（イ）バックアップデータの管理

・ バックアップデータの管理を行う。

（ウ）バックアップ・リストア

・ システムに変更を加える際に必要に応じてバックアップを取得する。
・ また、必要に応じてデータのリストアを行う。

（エ）稼働監視

- 本県が別途構築している障害監視システムにより、各サーバの死活監視及びリソース監視を行う。

（オ）性能・構成管理

- サーバのリソースについて、不足がないか定期的にチェックを行う。
- 本システムにて導入される、ハードウェア及びソフトウェアの構成を管理する。

（カ）ログ管理

- 各種ログ（ログオン、DHCP 等）について異常がないかチェックし、定期的に報告する。

（キ）パッチインストール

- 受託事業者により本システムへの影響がないと判断されたパッチのインストールを行う。

（ク）業務端末へのセキュリティパッチの配布

- 受託事業者により作成されたセキュリティパッチ配布用タスクにより、業務端末に対するセキュリティパッチの配布を行う。
- Microsoft 社から提供される Quality Update について、業務への影響がないことを確認次第、速やかに実施する。

（ケ）庁舎停電対応

- 本庁舎及び総合庁舎について、電気設備点検等で停電が発生する際、必要に応じて機器の停止・起動の設定を行う。

（コ）障害一次切り分け

- 障害が発生した場合、運用マニュアルに基づき、障害の一次切り分けを行う。

エ　受託事業者が行うもの

- 以下の業務については、受託事業者が担当することを想定しているため、詳細な業務内容について、設計を行うこと。

（ア）日常運用業務に対する支援、提案

- 運用管理担当者による本システムの運用業務全般を実施するための技術支援を行う。定常運用に伴う技術支援についても実施する。
- 必要に応じて性能を改善するための計画や対策を策定し、本県に対して提案を行う。また、運用を効率的に行うためのスクリプト等にかかる作成支援についても実施する。
- 運用管理担当者が各種報告を行うための各種支援についても実施する。

（イ）パッチによる影響等の情報提供

- 本システムで使用するソフトウェア製品に関するバグフィックス、セキュリティ対応等のパッチがリリースされた場合、速やかにその内容の調査を行い、適用の可否を本県に報告する。また、適用できない場合は、適用するためのシステム改修の内容を本県に報告する。

- パッチがリリースされてから情報の提供までの期間は Microsoft 社のパッチは 2 開庁日以内、その他の製品のパッチは 1 週間以内とする。
- 本システムに影響を及ぼす恐れのあるパッチが提供された場合、運用管理担当者が影響の有無についての確認作業を短時間に行えるように支援を行う。もしくは受託事業者がパッチ適用に立ち会い、本システムへの影響の有無を確認する。
- パッチの適用作業は運用管理担当者が行うものとするが、パッチ適用による障害が発生した場合は、受託事業者にて障害対応を行う。

（ウ）バージョンアップによる影響等の情報提供

- 本システムで使用するすべてのソフトウェア製品のバージョンアップ製品がリリースされた場合、その内容の調査、本システムに対する影響の調査、適用の検討、本システムの改修が必要な場合はその内容に係る情報の提供を行う。

（エ）バージョンアップ作業

- 契約期間中に本システムで利用しているソフトウェアのバージョンのサポートが終了する場合、速やかにバージョンアップ版ソフトウェアの取得を行い、継続してサポートが受けられるように対応を行う。その際に発生する全ての作業については受託事業者の業務範囲とする。
- また、サポート切れとなるソフトウェアのバージョンアップに伴い、他のソフトウェアのバージョンアップが必要となる場合は、そのソフトウェアのバージョンアップ版の取得及びバージョンアップ作業も本委託業務の範囲とする。
- なお、ソフトウェア製品に対してパッチが適用されない、または、セキュリティホールの有無をそのソフトウェア開発業者が確認しなくなった時点でサポートの終了とする。

（オ）脆弱性情報等による対象端末の抽出

- 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」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。

- 対応すべき脆弱性が多岐に渡り、短期間で全ての対応を行うことが困難な場合は、各業務端末における深刻度が高いものから優先して抽出するなど、計画的な対応を行う。
- マニュアルや考え方などを整備したうえで、運用管理担当者に対して引継ぎ等を実施し、業務移管についての了承を得た場合には、運用管理担当者による対応も可とする。
- 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。

（カ）セキュリティパッチ配布用タスクの作成

- 統合運用管理システムにおける「セキュリティパッチ配布機能」により各業務端末に対するセキュリティパッチ配布を行うために必要となるタスクを作成する。
- マニュアルや考え方などを整備したうえで、運用管理担当者に対して引継ぎ等を実施し、業務移管についての了承を得た場合には、運用管理担当者による対応も可とする。
- 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。

（キ）障害対応

- 運用管理担当者にて障害の発生原因の切り分けが困難である場合は、本県もしくは運用管理担当者からの連絡に基づき、障害の切り分け支援を行う。
- 必要に応じて障害発生拠点へ駆けつけ、不良部位の切り分け及び修理・修正・交換を行う。
- 障害によりソフトウェア、データが破損した場合、バックアップデータ等から速やかに復旧を行う。また、必要に応じて、システムの再セットアップを行う。

（ク）障害後是正措置・予防措置

- 障害が発生した場合、障害に関する情報を収集したうえで、その障害情報をもとに原因を分析し、同様の障害が発生しないように是正措置・予防措置を講じる。また、直ちに障害原因が判明しない場合は、本県の了承を得たうえで、継続して調査を行い、障害原因の特定に努める。
- 障害情報、是正措置・予防措置の内容は障害記録として体系的に記録し、常に活用できるように保存する。

（ケ）運用マニュアルの改訂

- 運用作業により、ドキュメント等の修正が発生した場合には履歴管理を行った上で速やかに各種ドキュメントを修正する。尚、ドキュメントの修正にあたっては本県の承認を得ること。

（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。

オ　運用・保守体制

（ア）保守対応時間

- 保守対応時間として、24 時間 365 日とし、メール及び電話による障害連絡を 24 時間受け入れられること。

（イ）障害対応要件

- 保守対応時間内において、対応依頼から初期対応を開始するまでの時間として、概ね 30 分以内として設計を行うこと。なお、大規模災害発生時においては可能な限り当該時間を目標にして設計を行うこと。なお、初期対応とは、障害発生箇所・原因の確認作業への着手、本県などの関係者への連絡等を指す。
- 駆けつける必要があると判断してから、駆けつけ完了までの時間を開庁日の 8 時 30 分から 17 時 15 分までは 2 時間以内、上記以外の時間帯は 4 時間以内として設計を行うこと。大規模災害発生時においては可能な限り当該時間を目標として設計を行うこと。
- 復旧方法が明らかになり、かつ復旧作業が必要な場所へ到着してから、復旧するまでの時間として概ね 2 時間以内となるように設計を行うこと。なお、2 時間以内の復旧が困難と判明した場合における対応等についても設計を行うこと。
- 障害が発生した場合でも、ハードウェア等が冗長化されており、機能提供に影響がないと判断される場合や、特段の機能停止が発生しないと確認できた場合は、翌開庁日の 7 時 30 分からの対応も可とするため、必要に応じて設計に盛り込むこと。

（ウ）保守部品・消耗品

- オンサイトでの保守対応が不可能な部位がある場合を想定し、予備品の保有等についても設計を行うこと。
- 常時保有すべき保守部品（付属品、ソフトウェアを含む。）がある場合は、必要数の確保について設計に盛り込むこと。なお、履行期間中において、製造中止等に伴い保守部品の入手が困難になった場合は、本県の承認を得たうえで、代替品による対応も可とする。
- 運用・保守業務を実施するうえで、必要になる消耗品がある場合は、履行期間中における必要数について、設計を行うこと。なお、履行期間中における消耗品の納入についても、本委託業務の範囲内とする。

（７）本システムの構築にかかる要件

本システムの構築作業として、「サービス定義書」に定義した各種サービスを提供するために必要となる全ての構築作業を行うこと。

構築作業は、先に作成した「構築設計」に従い、確実に実施すること。

構築作業終了後、構築設計に従い、各種試験を実施し、その結果を本県に対して報告し、承認を得ること。

津市 IDC での作業を実施する際は、入館申請が必要となるため、注意すること。なお、機器搬入等を行う際は、津市 IDC が指定する搬入口及びエレベータを使用し、設備、器物破損を防止するための処置を講じること。また、搬入にあたり発生した不要物（梱包材）は速やかに回収し、受託事業者の責任、負担において、安全に破棄すること。

既存システムやネットワーク等との接続時には、各受託事業者と綿密な連絡を取りながら、既存システムやネットワークへの影響を与えないよう、細心の注意を払うこと。

障害発生等の理由により、作業を中断、中止、切り戻し等を行う必要がある場合は、速やかに本県の担当者宛連絡を行うこと。また、速やかに、構築設計を修正し、本県に対して説明を行い、承認を得ること。

構築作業に伴い、重大な事故・障害が発生した場合は、遅滞なく本県に報告を行うとともに、直ちに切り戻し作業を行い、被害が最小限になるよう、一次対応を行うこと。その後、速やかに、事故・障害発生状況、影響範囲、根本解決策等について本県に報告を行うこと。

全ての構築作業が完了後、「稼働判定基準」に基づき試験を実施し、その結果について、本県に対して説明を行い、承認を得ること。

（８）導入業務にかかる要件

導入設計に沿って導入作業を行うこと。特に、外部サービス（クラウドサービス）の導入作業や、エージェントソフトウェアの導入作業、既存システムとのシステム連携がスムーズに実施できるよう、留意すること。

既存ネットワークや既存システムが設置されている施設で作業を実施する際は、本県の指示に従い、事前連絡、入館申請等の対応を行うこと。

各種試験の結果については、導入作業の進捗状況に応じて、速やかに本県へと報告を行うこと。

導入作業に伴い、重大な事故・障害が発生した場合は、遅滞なく本県に報告を行うとともに、直ちに切り戻し作業を行い、被害が最小限になるよう、一次対応を行うこと。その後、速やかに、事故・障害発生状況、影響範囲、根本解決策等について本県に報告を行うこと。

予定していた全ての導入作業が完了後、本県に対して説明を行い、承認を得ること。

（９）運用・保守業務にかかる要件

本システムの安定的な運用を行うため、運用・保守業務を行うこと。

運用・保守業務は、先に作成した「運用・保守設計」に従い、確実に実施すること。

運用・保守設計の内容については、本県の組織改正等に応じて、適宜修正すること。

運用・保守業務を実施する保守要員に変更がある場合は、引継ぎ作業として、「運用・保守設計」の内容だけでなく、必要に応じて、現地確認等についても実施し、サービスレベルを低下させないよう、留意すること。

（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。