資産管理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、「資産管理基盤関連」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「運用管理システム」は、クオリティソフト株式会社の資産管理ソフトにより、三重県行政 WAN 内の全庁内端末にかかるインベントリの収集やプログラムの配信、リモート接続の他、Microsoft 社の WSUS（WindowsServerUpdateServices）によるセキュリティパッチの配布等、資産管理を行うために利用しています。
>
> 本資料における**「資産管理基盤」とは、現行の「運用管理システム」の機能に加え、新たな資産管理対策を盛り込んだ資産管理の基盤となるシステム**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

現在利用している運用管理システムは、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、三重県行政 WAN 内の端末等に対する資産管理等を行うためのシステムとして、オンプレミスにて構築を行いましたが、今後、クラウドサービスの利用や、テレワークの推進などを実施するためには、これまで以上に詳細な資産管理等への対応が必要になると考えています。

そこで、「現行の「運用管理システム」だけでは実現できない**新たな資産管理対策等を実施可能な「資産管理基盤」を構築する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
運用管理システム	・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 ・「資産管理基盤」など、複数のサブシステムで構成される
資産管理基盤	・現行の「運用管理システム」を機能強化し、再構築した新たなシステムのこと

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）現行システムから引き継ぎたい機能」を確認いただき、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）現行システムから引き継ぎたい機能」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）現行システムから引き継ぎたい機能

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「運用管理システム」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、「運用管理システム」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
運用管理システム	・　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　運用管理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、資産管理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。
- 現行の運用管理システムにおいて、クオリティソフト社の製品を指定していますが、他社製品による提案も可とします。なお、クオリティソフト社製品以外のソフトウェアを提案いただく場合は、新規ライセンスの購入費用（具体的には、令和 4 年 7 月 1 日から 1 年間分のソフトウェア使用料）についても費用に含めていただくようお願いします。なお、クオリティソフト社製品の場合であっても、本県が所有するライセンス以外に追加ライセンスが必要となる場合は、同様の対応をお願いします。
- 資産管理基盤にかかるライセンスは、これまでと同様に、毎年度調達を行う予定ですが、詳細仕様書内の年間ライセンス費用の上限については、見直しを予定していることから、提案をいただくソフトウェアにかかる更新費用についても、併せて提案を行っていただくようお願いします。

（２）課題解決に何らかの改善提案を要するもの

現行の運用管理システムに対して、「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　資産管理基盤に必要とされる構成の想定」を踏まえて、「ウ　エンドポイントにおけるインベントリ収集と資産管理の詳細」から「チ　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、<u>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</u>、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。

・ また、新型コロナウィルスにかかる感染対策として、テレワーク環境を構築した他、業務の効率化の観点から、これまで利用を禁止してきた LGWAN 系ネットワークにおける無線 LAN 環境も構築し、運用を行っているところです。

・ しかし、その結果として、<u>βモデルへ移行するための必須要件である EDR（Endpoint Detection and Response）対応のほか、テレワーク等を実施するためのデバイス自身の管理とデバイスに対する脆弱性管理、導入した Apple 社製 iPad や Microsoft 社製 Surface Pro / Surface Go にかかる更新プログラムの反映やデバイス管理、無線 LAN 環境を利用するための認証用証明書の配布、さらには、これらの対策を実施するための人材育成・体制確保など、多くの課題が顕在化</u>してきたところです

・ 以上のことから、<u>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、「現行の「運用管理システム」だけでは対応しきれない新たな資産管理対策等が実施可能な「資産管理基盤」について、構築を行う必要があると考えています。</u>

イ　資産管理基盤に必要な機能の想定

・　「資産管理基盤」に必要と想定される機能は、以下のとおりです。

機能名	機能等の詳細
全体構成	・「資産管理基盤」は、主にエンドポイント（利用者が直接利用するパソコン、モバイル端末等のこと）における資産管理を担い、主に、インベントリ（ハードウェア・ソフトウェア情報）収集と資産管理（HAM　Hardware Asset Management・SAM　Software Asset Management）、MDM（Mobile Device Management）、IT ハイジーン（IT Hygiene）、外部デバイス（USB メモリ）等の利用制限、暗号化管理、操作ログの収集管理、リモートコントロール等の機能を提供する。 ・なお、マルウェア対策、EDR（Endpoint Detection and Response）等のセキュリティ対策にかかる各種機能については、「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」にて提案を求めているため、そちらを参照されたい。
インベントリ収集と資産管理	・エンドポイントにおけるインベントリを収集し、その資産状況について管理する仕組みを提供する。 ・具体的には、定期的、又は、任意のタイミングにて、各エンドポイントからインベントリ情報の収集を実施し、それらを一元的に管理できる仕組みを提供する。 ・ソフトウェア資産を管理するための仕組みを提供し、ライセンス管理を容易にするとともに、ライセンス管理に対する監査等にも対応できる機能を提供する。
MDM	・MDM は、モバイルデバイス自体を管理するための機能の他、モバイルデバイスにインストールされているソフトウェア等にかかる、ライセンス管理、不要なソフトのインストール制限、バージョンや脆弱性情報の一元管理を行う機能等を提供する。 ・また、盗難対策、及び、情報漏洩対策として、モバイルデバイスの現在地把握機能の他、リモートからのロック機能や、データ消去機能等も提供する。 ・なお、MDM を拡張した概念として、EMM（Enterprise Mobility Management）があり、EMM には、MDM の他、モバイルデバイスにかかるアプリケーション管理（MAM Mobile Application Management）、モバイルデバイスにおけるコンテンツ管理（MCM　Mobile Contents Management）が含まれるが、本資料内では、いずれも MDM における機能の一部として記載しているため、留意されたい。

IT ハイジーン	・IT ハイジーンは、エンドポイントにおける「衛生管理」を意味し、各エンドポイントにおける、セキュリティパッチの適用状況や、マルウェア対策ソフトウェアにおけるパターンファイル等の更新状況などを一元管理する機能を提供する。 ・また、対応が不十分なエンドポイントに対して、適正な状態にするための機能（アプリケーションの一斉配布、強制配布、未対応の端末に対する機能制限など）も提供する。
外部デバイス（USB メモリ）等の利用制限	・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を制限する機能を提供する。 ・具体的には、別途調達予定の「ユーザ認証基盤」等と連携し、利用者単位やエンドポイント（デバイス）単位にて、利用の可否（使用可能、読み取りのみ可能、使用不可）等の設定を管理画面等から容易に設定できる機能を提供する。
暗号化管理	・暗号化管理は、エンドポイントや外部デバイス等にかかる情報漏洩対策として実施する暗号化処理等について、各種管理機能を提供する。 ・具体的には、どのエンドポイントや外部デバイスが暗号化状態となっているかを一元的に管理する機能の他、暗号化を行った際のパスワード等の一元管理機能、各種情報を保存する際に強制的に暗号化させる機能、暗号化されていない機器を暗号化するまで利用させない機能等を提供する。
操作ログの収集管理	・操作ログの収集機能は、エンドポイントにおける各種操作ログを収集し、保管する機能を提供する。 ・保管されたログを確認することで、各エンドポイントにおける利用者の操作履歴の他、マルウェア等の動作内容も確認できる。
リモートコントロール	・利用者側のデスクトップ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する。 ・リモートコントロール機能を利用することで、利用者側と画面を共有することができるため、問い合わせ対応や、操作指導等に利用できる他、適正な操作がされているかの確認等に利用できる。

表３　資産管理基盤における機能想定

・ 以下の機能については、「セキュリティ対策基盤」で提供する機能に含まれると想定しています。そのため、「資産管理基盤」の必須機能とは考えていませんが、資産管理にかかる対策を強化するため、必要に応じて情報提供等を行っていただくようお願いします。

機能名	機能等の詳細
マルウェア対策	・エンドポイントにおける、マルウェア（コンピュータウィルス等の悪意ある動作を行うソフトウェア）対策機能として、主に「侵入されないための機能」を提供する。 ・具体的には、パターンファイルやシグネチャ等のパターンマッチングによる検知、ふるまい検知やサンドボックス等の機械学習による検知、マルウェアの遮断（通信遮断、ファイル削除等）等の機能を提供する。
EDR	・EDR は、エンドポイントにおいて、マルウェア等の脅威が侵入した後に「被害を拡大させないための機能」を提供する。 ・具体的には、各エンドポイントから「ログの収集・分析」を実施し、「被害の検知」「不審な通信や動作の遮断」「侵入経路や被害範囲の調査」といった機能を提供する。 ➢ 被害の検知・・・エクスプロイト攻撃や攻撃時における特徴的なふるまい（IOA Indicator Of Attack）の検知の他、感染の痕跡（IOC Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知する。 ➢ 不審な通信や動作の遮断・・・C&C サーバ（Command and Control Server）との通信遮断や特定プロセスの停止等を行う。また、被害があったエンドポイントに対して、被害の拡大を防ぎつつ、迅速な対応を行うため、インシデント対応で利用する通信（例えば、調査を行うためのリモート接続等）以外の通信を全て遮断する。ファイルの削除やレジストリの復旧なども行う。 ➢ 侵入経路や被害範囲の調査・・・収集したログ等の情報からマルウェア等の脅威がどの端末から感染し広がったのか、どれだけの端末に広がっているか、どのような被害（どのファイルがアップロードされたのか、どの管理者権限が奪取されたのかなど）があったのか、などを調査可能な状態に可視化する。

表４　その他のサブシステム等における機能想定

ウ　エンドポイントにおけるインベントリ収集と資産管理の詳細

- エンドポイント（利用者が直接利用するパソコン、モバイル端末等のこと）におけるインベントリ収集機能において、収集可能な情報の詳細（ハードウェアの詳細、ソフトウェアの詳細、脆弱性への対応状況、マルウェア対策におけるパターンファイルの更新状況、レジストリの詳細、利用にかかる詳細ログ等）について提案を行っていただくようお願いします。
- 資産管理機能として、収集した情報の管理機能や、ソフトウェアライセンスの導入から廃棄までのライフサイクル全般に関する管理機能（ISO/IEC17990-1 に準拠したソフトウェア資産管理方法）等の詳細について、提案を行っていただくようお願いします。（一覧画面や詳細画面における詳細内容の確認方法、各種条件による抽出や検索方法、MDM やデバイスの利用制限機能等との連携機能の詳細などについて、設定画面等を沿えて説明を行っていただくようお願いします。特に、詳細画面が英語の場合（日本語化されていない場合）は、日本語化マニュアルの有無についても説明を行っていただくようお願いします。
- EDR 等のログ収集機能を他に導入することで、インベントリ収集機能や資産管理機能を強化できるものがあれば、併せて提案をいただくようお願いします。
- インベントリの収集について、実施タイミング（スケジュールによる実施、任意のタイミングによる実施）や、エンドポイントの負荷軽減策等の詳細についても説明を行っていただくようお願いします。

エ　MDM の詳細

- MDM を導入することにより、各エンドポイントに対して利用できる機能の詳細について、提案を行っていただくようお願いします。なお、MDM にとどまらず、MAM や MCM といった EMM に関連する内容についても可能な範囲で提案を行っていただくようお願いします。また、提案いただく MDM で管理が可能なデバイスの詳細（タブレット、スマートフォン、PC（無線 LAN））や、OS の詳細（Andoroid、iOS、Windows 等）についても説明を行っていただくようお願いします。さらに、必要となるライセンスの詳細についても説明を行っていただくようお願いします。
- 盗難対策として利用可能な機能の詳細について、提案を行っていただくようお願いします。具体的には、盗難後に端末の位置を検知するための現在地把握機能、盗難後の端末に対して不正なアクセスや情報漏洩を防ぐため、「リモートで警告を出す」「ロックする（操作を受け付けなくする）」「端末を初期化する」、などといった機能を想定しています。また、初期化後に売却されない機能（Apple 製品であれば、MDM と DEP（DeviceEnrollmentProgram）を連携させることで売却を防ぐことが可能と想定しています）についても提案を行っていただくようお願いします。

- 本県資産のモバイルデバイスについて、利用者が誤った設定等を行うことにより不正なアクセスや情報漏洩等を生じさせないよう、通常の利用用途以外の操作制限（アプリの追加制限、ネットワーク設定への変更制限、シャドーIT の利用制限など）を行うこととしていますが、多数の端末に対して設定変更等の管理が容易で、かつ、十分な制限を実施する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、端末の故障時等においては、管理者権限等により、ロック等の解除ができることが望ましいと考えています。
- 無線 LAN で利用する証明書について、現在は、手作業による設定をそれぞれの端末に対して実施しているところですが、これらの作業について容易に対応でき、また、設定した端末の一元管理ができる方法（導入時だけでなく、継続的に管理ができる方法）について提案を行っていただくようお願いします。また、証明書の一斉変更が必要になった際の配信方法についても提案を行っていただくようお願いします。

オ　IT ハイジーンの詳細

- IT ハイジーンを導入することにより、各エンドポイントに対して利用できる機能の詳細について、提案を行っていただくようお願いします。
- 具体的な機能として、IT ハイジーンを各端末で実施した結果について、管理画面等により一覧表示する機能や、個々の端末の詳細情報を確認できる機能、対応が不十分な端末に対して「警告」「一部アプリケーションの利用停止」「セキュリティパッチ等の強制配信」等の制限をかける機能、IT ハイジーンを定期的、または、任意のタイミングで実施する機能、テレワークを実施する際にテレワーク元の職員所有端末に対して IT ハイジーンを実施できる機能、といったものを想定しています。
- IT ハイジーンの利用場面の想定は以下のとおりです。

	通常利用時	テレワーク時
対象端末	・本県資産の端末	・職員所有の端末
実施タイミング	・定期的（毎月や毎週）、又は、任意のタイミング	・テレワークを行う前段階（前処理）のタイミング
結果後の対応	・「警告」「一部アプリケーションの利用停止」「セキュリティパッチ等の強制配信」等を実施する	・利用可否の通知 ・利用不可の場合は、必要な対応策を通知する

表５　IT ハイジーンの利用場面

- IT ハイジーンを実行するためには、各種ソフトウェア等に対する最新の脆弱性情報等を取得したうえで、各エンドポイントの対応状況等と比較する必要があると想定していますが、OS（Windows、iOS、Andoroid 等）、導入済みソフトウェア（Office、IE 等）のバージョン、ファームウェア、等にかかる、最新情報の取得可否について説明を行っていただくようお願いします。（例えば、Windows は取得できるが、Office は取得できないなど。また、Windows の脆弱性情報において、個別パッチと累積パッチの親子関係（累積パッチを当てていれば個別パッチは不要となる）などを反映した判断が実施できるかについても説明していただくようお願いします。）
- セキュリティパッチ等の各エンドポイントへの配信方法として、現行システムで利用している運用管理システム（WSUS）を継続利用することも可としますが、Microsoft 社製品以外のセキュリティパッチを配信するための仕組みについては、別途提案を行っていただくようお願いします。
- 配信を行うセキュリティパッチ等の容量が大きい場合、通信回線に大きな負荷をかけずに配信する仕組みについて、提案を行っていただくようお願いします。

カ　外部デバイス等の利用制限の詳細

- 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、提案を行っていただくようお願いします。
- 具体的には、「ユーザ認証基盤」におけるアクセス制御機能と連携し、利用可能なユーザを制限する（管理者権限であれば利用可能、一般権限では利用不可など）、利用可能な端末自体を制限する（A 端末では利用できるが、B 端末では利用できない、総務担当フロアでは利用できないが事業担当フロアでは利用できるなど）、外部デバイスを利用した際の利用ログの保存（例えば、ファイル名の一覧を保存するなど）、といった機能を想定しています。
- また、外部デバイス等にかかる管理を行うため、利用者からの申請に対する申請フロー（例えば、実際に USB メモリを接続した段階で申請許可がポップアップされるなど）、許可した外部デバイスの定期的な管理（定期的な存在確認や更新申請等の受け付けなど）、といった機能についても、提案を行っていただくようお願いします。

キ　暗号化管理の詳細

- 端末の盗難による情報漏洩対策のため、エンドポイントや外部デバイスに対して暗号化を行う必要があると考えていますが、暗号化を行った場合、パスワード等の管理が煩雑になる、故障時等のデータ抽出が困難になる、などの課題があります。そのため、各エンドポイントや外部デバイスに対して、十分な情報漏洩対策を実現することが可能で、かつ、簡単に利用・管理ができる方法について、提案を行っていただくようお願いします。
- 特に、暗号化を実施した際のパスワード等の一元管理機能等について、利便性とセキュリティ強度はトレードオフの関係になることから、費用対効果が高く、実現可能で豊富な実績がある方法を提案いただくようお願いします。

ク　操作ログの収集管理の詳細

- 各エンドポイントにおける情報漏洩対策として、また、セキュリティ事故や悪意ある操作に対する追跡調査を実施できるようにするため、操作ログの収集管理機能により収集が可能な記録の種類や記録形式等について、説明を行っていただくようお願いします。
- 特に、利用者の操作ログだけでなく、マルウェアやシステムにおける特徴的な動作についても記録できることが望ましと考えていますので、具体的な記録内容について、説明をいただくようお願いします。（例えば、ファイルをコピー後、リネームし、メールで送信した、というような操作に対する記録がどのような形で保存されるかについて、説明をお願いします。）
- ログ収集を行うために必要となる回線や、ログ収集に必要なサーバ等のスペック等について、エンドポイント 1 台当たりの必要帯域や 1 日当たりのログの転送容量を踏まえて、提案を行っていただくようお願いします。なお、収集したログをオンプレミスに設置したサーバではなく、クラウドサービス上に送信する必要がある場合は、接続に必要な回線について、必要帯域や転送容量の目安を示していただくようお願いします。
- ログの保存期間を計算するため、1 か月当たりのログ容量の目安についても説明をいただくようお願いします。

ケ　リモートコントロールの詳細

- リモートコントロールを行う操作者側が、利用者側の操作画面を確認でき、かつ、操作を行うことができるリモートコントロール機能の詳細について、提案を行っていただくようお願いします。
- 機能の詳細として、同時接続数や利用可能な OS の種別等の他、利用者側の端末にてインシデントが発生した際に、リモートコントロール以外の通信を制限する機能（リモートコントロールのみを実現する機能）等についても説明を行っていただくようお願いします。

コ　資産管理基盤の必須機能に含めるべき機能

・ 資産管理基盤の必須機能として、「インベントリ収集と資産管理」「MDM」「IT ハイジーン」「外部デバイス（USB メモリ）等の利用制限」「暗号化管理」「操作ログの収集管理」「リモートコントロール」としていますが、近年のサイバー攻撃やマルウェア等の脅威へ対応するため、費用対効果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。

サ　エージェントソフトウェアのインストール

・ 資産管理基盤を運用していくためには、各エンドポイントに対して、エージェントソフトウェアのインストールを行う必要があると想定しています。そのため、全てのエンドポイントへ漏れなく確実にエージェントをインストール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。
・ エンドポイントとして、本県資産の端末やモバイル端末の他、テレワークシステム等を利用するため職員が所有する端末やモバイル機器も想定していますが、これらの機器に対するエージェントの配信方法についても提案をいただくようお願いします。（イントラ内の端末に対しては、これまでグループポリシーやログインスクリプト、インストール用実行ファイルの送付等により、強制的に配布を行っていましたが、職員が所有する機器に対してエージェントを強制的にインストールさせるための方法等について、提案をいただくようお願いします。）
・ 職員が所有する端末やモバイル端末について、資産管理基盤におけるエージェントソフトウェアに代わる対策（例えば、アクセスする都度、エンドポイントの情報を収集するためのツールが自動実行されるなど）を実施する場合は、その詳細について、説明をいただくようお願いします。

シ　導入時の対応

・ 新たに「資産管理基盤」を導入し、IT ハイジーン機能等を利用した場合、対応が不十分な端末が大量に顕在化する恐れがあります。そのため、導入時に優先して対応すべき作業や手順等があれば、提案をいただくようお願いします。
・ なお、大量の対応を行う場合は、セキュリティパッチ等の配信のため、大量のトラフィックが流れることになると想定していることから、通信回線に負荷をかけない方法についても提案をいただくようお願いします。

ス　シャドーIT 対策

・　シャドーIT（許可されていないクラウドサービス等の利用）への対応として、シャドーIT の把握方法について、提案を行っていただくようお願いします。なお、操作ログの収集・分析の結果として、把握する方法などを想定しています。

セ　テレワーク端末における資産管理

・　三重県行政 WAN に対して、種々の方法により、テレワークを行っていますが、テレワークを実施する端末に対する資産管理方法について、提案を行っていただくようお願いします。
・　なお、職員が所有する端末やモバイル機器は、相当数が見込まれるとともに、頻繁に更新されると想定されるため、全ての機器に対する管理や把握は難しいと思われること、さらに、職員の所有端末に対しては、端末の初期化や保存内容の全開示などの対応が困難と想定されることなどから、全ての操作記録を保存するといった方法の他、あらかじめ、端末側へのファイル保存を禁止する、システム側に操作記録を残す、などといった職員所有端末の資産管理を実施せずに実現できる対策等があれば、提案をいただくようお願いします。

ソ　ユーザ認証基盤との連携

・　「依頼内容 01　ユーザ認証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、ユーザ認証基盤にかかる内容について、資産管理基盤として、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。
・　例えば、外部デバイスにおけるユーザ単位の利用制限連携などを想定しています。

タ　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、セキュリティ対策基盤にかかる内容について、資産管理基盤として、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。
・　例えば、IT ハイジーン機能において対策が不十分なエンドポイントに対して、自動的にスキャンを実施したり、ログ収集機能で連携を行ったりする機能などを想定しています。

チ　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、資産管理基盤として、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。

（３）新規提案項目

現行の運用管理システムに対して、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。