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

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、「セキュリティ対策基盤関連」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「ウィルス対策システム」は、Trendmicro 社のウィルス対策ソフトにより、三重県行政 WAN 内の全庁内端末及び全サーバに対して、ウィルス対策ソフト及びパターンファイルを提供するなど、セキュリティ対策を行うために運用を行っています。

本資料における**「セキュリティ対策基盤」とは、現行の「ウィルス対策システム」の機能に加え、新たなセキュリティ対策を盛り込んだセキュリティ対策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

現在利用しているウィルス対策システムは、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セキュリティ対策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、これまで以上のセキュリティ対策が必要になると考えています。

そこで、「現行の「ウィルス対策システム」だけでは実現できない**新たなセキュリティ対策を実施可能な「セキュリティ対策基盤」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
ウィルス対策システム	・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 ・「セキュリティ対策基盤」など、複数のサブシステムで構成される
セキュリティ対策基盤	・現行の「ウィルス対策システム」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「ウィルス対策システム」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、「ウィルス対策システム」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
ウィルス対策システム	・　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　ウィルス対策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、セキュリティ対策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。
- 現行のウィルス対策システムにおいて、Trendmicro 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、Trendmicro 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、Trendmicro 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。
- セキュリティ対策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

現行のウィルス対策システムに対して、「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　セキュリティ対策基盤に必要とされる構成の想定」を踏まえて、「ウ　マルウェア対策の詳細」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、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、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、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してきたところです。また、三層の対策として、インターネット閲覧用の仮想環境を構築していますが、導入当初から、使い勝手が非常に悪く、業務に支障が出ていました。

・ 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、「現行の「ウィルス対策システム」だけでは対応しきれない新たなセキュリティ対策が実施可能な「セキュリティ対策基盤」について、構築を行う必要があると考えています。

・ なお、新たに構築する「セキュリティ対策基盤」は、現行の「ウィルス対策システム」によるウィルス対策を含め、さまざまな機能をシームレスに提供することが求められることから、新たなシステムとして可能な限り一体的な構築を行うことが望ましいと考えています。

イ　セキュリティ対策基盤に必要な機能の想定

・　「セキュリティ対策基盤」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	・「セキュリティ対策基盤」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）におけるセキュリティ対策を担い、主に、マルウェア対策、EDR（Endpoint Detection and Response）等の機能を提供する。 ・SIEM（Security Information and Event Management）、セキュリティインテリジェンス、CASB（Cloud Access Security Broker）といった、ネットワーク構成に大きく依存する機能については、任意機能とする。 ・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対策については、「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」にて提案を求めているため、そちらを参照されたい。
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３　セキュリティ対策基盤における機能想定

・　以下の機能については、ネットワーク機器等で実施するセキュリティ対策や「資産管理基盤」で提供する機能に含まれると想定しています。そのため、「セキュリティ対策基盤」の必須機能とは考えていませんが、セキュリティ対策の強化を行うため、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
SIEM	・SIEM は、さまざまな機器やソフトウェアのログを収集し、一元的に分析することで、サイバー攻撃やマルウェア等の脅威や被害を検知する機能を提供する。 ・本県では、インターネットとの接続境界に設置済みのファイアウォールにて導入済み。また、三重県自治体情報セキュリティクラウドでも導入されている。ただし、いずれも、UEBA（User and Entity Behavior Analytics）は導入されていない。
セキュリティインテリジェンス	・セキュリティインテリジェンスは、サイバー攻撃やマルウェア等のさまざまな脅威に関する情報を収集し、提供を行うことを指すが、近年では、収集した情報を SIEM や EDR 等と連携させることで、侵入等の痕跡をいち早く検知する機能も提供している。
無害化（メール、Web）	・無害化（メール、Web）は、メールの送受信や Web ブラウジングを実施した際に、パターンマッチングやふるまい検知等により、無害化する機能を提供する。

	・本県では、メール無害化、及び、Web ブラウジング無害化のいずれも導入済み。また、三重県自治体情報セキュリティクラウドでも導入されている。
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。
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。
CASB	・CASB は、利用者と複数のクラウドサービスの間に単一のコントロールポイントを設けて、クラウドサービスの利用状況を可視化・制御する機能を提供する。 ・導入することで、シャドーIT（許可されていないクラウドサービスの利用）を制限したり、一貫性のあるセキュリティポリシーを適用したりすることが可能となる。
脅威ハンティング	・脅威ハンティングは、サイバー攻撃やマルウェア等の被害を受けているエンドポイント等を調査し、抽出を行うこと、または、その仕組みのこと。 ・新たなセキュリティ対策を導入する際は、これまで気づかなかった被害が顕在化することがあるため、導入時等に実施することが望ましい。

表４　その他のサブシステム等における機能想定

ウ　マルウェア対策の詳細

・　マルウェア対策機能における防御方法や仕組みなどの詳細について、提案を行っていただくようお願いします。なお、マルウェア対策にかかる検知率と誤検知率の試験結果（他社比較が望ましい）があれば、併せて説明をいただくようお願いします。

・ EDR の他、他のセキュリティ対策機能を導入することで、マルウェア対策機能を強化できるものがあれば、ご提案をいただくようお願いします。（例えば、セキュリティインテリジェンスや EDR 等と連携することで、パターンファイルでは検知できない脅威に対して、検知が可能になるなどの機能を想定しています。）

エ　EDR の詳細

・ EDR におけるログ収集、検知、遮断、調査、事後対応といった各機能や運用方法の詳細について、提案を行っていただくようお願いします。特に、どのようなタイミングで検知がされ、その検知を元に、どのような流れで遮断、調査を行うことになるのかについて、画面等を示して提案を行っていただくようお願いします。（例えば、エクスプロイト攻撃等、通常のマルウェア対策では検知できない脅威に対して、検知、遮断、調査、駆除等にかかる対応の流れを説明いただくようお願いします。）
・ EDR において、詳細画面が英語の場合（日本語化されていない場合）や、各種リスクに対する詳細な解説がない場合、リスクや被害に対する有効な対応方法が示されない場合などにおいて、運用時の負荷が大きくなると想定していますが、そのような場合に必要となる体制やスキル等があれば、説明をいただくようお願いします。なお、本県職員等による運用ではなく、利用可能な運用サービス（例えば SOC（Security Operation Center サービス）を利用した運用の提案も可とします。

オ　セキュリティ対策基盤の必須機能に含めるべき機能

・ セキュリティ対策基盤の必須機能として、「マルウェア対策」「EDR」のみとし、他のセキュリティ対策については、任意機能としていますが、近年のサイバー攻撃やマルウェア等の脅威に対応するため、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。

カ　既存ネットワーク機器との連携

・ 既存ネットワーク機器にて SIEM や無害化処理等のセキュリティ対策を実施していますが、現行の対策を見直したり、別途構築を行ったりすることで、費用対効果の高いセキュリティ対策を実現できるものがあれば、提案をいただくようお願いします。なお、ネットワーク機器を別途調達したり、既存構成を変更したりする必要がある場合は、その費用についても概算でかまいませんので、ご提案をいただくようお願いします。

キ　エージェントソフトウェアのインストール

- マルウェア対策や EDR を実施するためには、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、EDR のエージェントに代わる対策を実施する場合は、その詳細について、説明をいただくようお願いします。

ク　ログ収集と必要回線

- セキュリティ対策基盤にかかる運用を行ううえで、エンドポイント等からのログ収集を行う必要があると想定していますが、ログを収集するために必要となる回線（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）や、ログを収集するために必要なサーバ等のスペック等について、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　監視・分析体制

- セキュリティ対策基盤を運用するうえで、必要となる監視・分析体制について提案を行っていただくようお願いします。なお、現行のウィルス対策システムの運用要員として、ヘルプデスク 4 名が他の業務も実施しながら、対応を行っていますが、増員が必要という場合は、各担当の役割分担や必要となるスキルについても提案をいただくようお願いします。

コ　導入時の対応

・　新たに「セキュリティ対策基盤」を導入し、EDR 機能等を利用した場合、これまでに検知できなかったサイバー攻撃やマルウェア等の脅威に対する被害が顕在化する恐れがあり、また、脅威が顕在化した場合は、迅速な対応が求められると想定しています。
・　そのため、導入時において、顕在化した脅威に対応できる十分な体制を整えるとともに、脅威ハンティング（スレットハンティング）の実施を計画するなど、具体的な体制や必要となる業務量などについて、提案を行っていただくようお願いします。

サ　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、EDR 等によるログの収集・分析の結果として、把握する方法などを想定しています。

シ　テレワーク端末におけるセキュリティ対策

・　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、テレワーク端末として利用している職員所有端末に対するセキュリティ対策について、提案を行っていただくようお願いします。
・　特に情報漏洩対策として、職員が所有する端末やモバイル機器に対して、印刷やスクリーンショットを規制する、ファイルの保存を禁止する、暗号化した領域を作成しそこに保存させる、それらの操作を記録する、などといった対策について、提案を行っていただくようお願いします。なお、被害が顕在化した場合、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から、検知後の対応方法についても併せて説明をいただくようお願いします。
・　逆に、提案いただくセキュリティ対策と連携可能で、かつ、利用が容易なテレワークシステム自体のソリューションがあれば、併せて提案をいただくようお願いします。

ス　無線 LAN 端末の管理方法

・　三層の対策における LGWAN ネットワーク系において、無線 LAN の利用を行っていますが、認証で使用する証明書の安全な配布方法や管理方法の他、各無線 LAN 端末に対する簡単で効果的な管理方法について、提案を行っていただくようお願いします。
・　特に、証明書の全台入れ替えを実施する場合の対応方法や、無線 LAN 端末の廃棄手順等について、セキュリティ対策を踏まえて提案を行っていただくようお願いします。

セ　三層の対策の見直し

- セキュリティ対策基盤を導入することにより、業務端末を LGWAN 系ネットワーク（αモデル）からインターネット接続系ネットワーク（β、β'モデル）へとつなぎ変えるための条件を満たすと想定していますが、他自治体において追加で実施しているセキュリティ対策等があれば、情報提供を行っていただくようお願いします。
- また、αモデルからβ、β'モデルへの移行方法（段階的な移行作業を実施する必要があると想定しています）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。

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、セキュリティ対策基盤として、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、SIEM における UEBA などを想定しています。

タ　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、セキュリティ対策基盤として、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 や IT ハイジーン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。
- 特に IT ハイジーンにより、十分な対策が取られていないことが判明したエンドポイントに対して、重要な情報へのアクセスを禁止したり、脆弱性対応等の必要な対策を促したりする仕組み等があれば、併せて提案を行っていただくようお願いします。（例えば、ファイルサーバへのアクセスを禁止したり、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ようにしたり、といった対策を想定しています。）

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、セキュリティ対策基盤として、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

現行のウィルス対策システムに対して、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。