α’モデル環境におけるセキュリティ監査業務、および、
エンドポイントセキュリティソフト(EPP)更改業務に関する仕様書

１．目的

東彼杵町では、総務省「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」に準拠し、α’モデル（パターン：イ）に基づく庁内 LAN 環境を運用している。次期システム更改にあたっては、DX 推進および業務環境の高度化に対応するため、LGWAN 系およびインターネット系における端末配置や運用形態の柔軟化を段階的に進める方針としている。

前段で示した端末配置および運用形態の見直し等、将来的な運用環境の変化に伴い、情報セキュリティ対策の実効性を維持・向上させる必要があることから、現行システムに対するセキュリティ監査およびリスク評価を実施し、エンドポイントを中心とした技術的および運用的な課題を明確化することを目的とする。あわせて、当該監査およびリスク評価により把握されたリスクや課題に対し、適切な是正および改善措置を講じるものとし、その中核的な対策として、PC 端末およびサーバを対象に、サイバー攻撃に対する防御、検知および対処機能を備えたエンドポイント保護機能（EPP）の導入を、当該監査と連続した取組として実施する。

但し、本業務において実施する情報セキュリティ監査は、現行環境におけるリスクおよび運用上の課題を把握し、今後講ずべき情報セキュリティ対策の方向性および留意点を整理することを目的とするものであり、特定の製品、メーカー又は構成を指定又は推奨することを目的とするものではなく、EPP の導入については本仕様書においてあらかじめ定めた機能要件・運用要件およびシステム要件に基づき実施するものとし、監査結果および助言内容は当該要件の妥当性確認および今後の運用改善に資する参考情報として活用するものとする。

また、三層分離構成の見直し等によるシステム構成および運用環境の変化を踏まえ、管理対象の分散や運用管理の煩雑化を抑制するとともに、管理の効率化および運用負荷の軽減を図る必要がある。このため、EPP の導入にあたってはログ管理および分析を含む運用管理機能を統合的に管理可能な構成とし、単一の管理コンソールによる一元的な監視および運用を可能とすることで、インシデント対応の迅速化、運用管理コストの低減および調達に係る費用の最適化を実現することを目的とする。

２．履行期間

契約締結日から令和９年３月３１日まで

３．既存の環境

現在使用しているエンドポイントセキュリティ（EPP）：ESET

４．監査対象及び監査項目

（１）　監査対象

本町において運用しているα’モデル（行政 LAN/WAN）を対象とする。（個別ネットワークについては、監査対象に含まない。）

（２）　監査項目

適用基準に基づく「情報セキュリティ監査項目」のとおりとする。

（３）　適用基準

本監査において適用する基準は、次のとおりとする。

① 必須とする基準

ア　総務省「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」（令和７年３月２８日公開）

イ　総務省「地方公共団体における情報セキュリティ監査に関するガイドライン」（令和７年３月２８日公開）

② 参考とする基準

ア　東彼杵町情報セキュリティポリシー（令和８年４月１日公開）

５．セキュリティ監査の要件

（１）　業務内容

「地方公共団体における情報セキュリティ監査に関するガイドライン」における「第２章　情報セキュリティ監査手順」で示されている内容に従うものとする。

具体的には以下の手順をもとに監査実施を行うことを想定している。

なお、「外部による確認」を第三者による独立かつ専門的な立場から適正に行うために後述するエンドポイントセキュリティソフト(EPP)の構築業者とは異なる、情報セキュリティサービス基準適合サービスリスト（独立行政法人情報処理推進機構）の情報セキュリティ監査サービス分野に登録されている業者にて監査を実施することが望ましい。

① 監査実施計画書の作成

受託者は監査実施計画書を作成し、町及び受託者の協議により委託業務の詳細内容及び各作業の実施時期を決定するものとする。

監査実施計画書には、監査の目的、監査項目、監査対象、監査手順、実施スケジュール、実施場所、実施体制及び担当者の氏名、本町との役割分担、成果物等を記載すること。

② 監査チェックリストの作成

監査項目ごとに具体的な確認事項となる監査要点を列挙した上で、監査チェックリストを作成すること。

③ 監査の実施

本町の対策に不備がないかどうか、提供するエビデンス類を確認する書面監査を中心に実施することとし、書面監査では確認が不足する事項に対して、関係者へのヒアリング等を実施すること。また、発見された問題点について事実誤認がないか等確認を行うこと。

関係者へのヒアリング等は原則 Web 会議での開催とし、必要に応じて本町と調整して実施すること。

④ 助言の実施

監査の過程において以下を実施し、本業務における目的の具体的な成果として、今後確認すべき事項の一覧と、それらの内容に対し、事業者の知見及び他自治体/団体の事例をまじえ、具体的なアドバイスを実施すること。

情報セキュリティポリシーの内容を確認し、本町におけるポリシーの適用状況のレビューを行うにおいて確認すべきポイントを一覧化すること。また、改善が望ましい内容があればアドバイスを実施すること。

監査の過程で以下の設計ドキュメントを確認し、リスクが懸念される事項を指摘し、改善ポイントについてアドバイスを実施すること。

【監査項目に含まれるもの】

・ネットワーク設計（セグメント設計、アクセス制御等）
・アカウント管理（AD 含む）
・資産管理
・マルウェア対策
・脆弱性管理
・ログ管理

【監査項目に含まれないが、確認を行うもの】

・バックアップ管理
・システム監視
・実際のログの内容や、各部署で行われている申請処理、起票された帳票等を閲覧し、ランサムウェア等のマルウェアへの感染時に侵入経路、情報の持ち出し等を追跡できるログが取得されているかを確認し、ログの取得方法や取得項目/内容、保管方法や全体としての情報処理の運用等についてアドバイスを実施すること。
・保守委託契約書、定例報告書、議事録の内容確認等からシステム運用の状況を確認し、より効率的かつリスクマネジメントを重視した運用となるようアドバイスを実施すること。
・教育の計画書、報告書、教育資料を確認し、見直すべき項目や追加すべき項目について指摘すること。また、具体的な内容についてアドバイスを実施すること。

・指摘した内容に関して、当町の情報セキュリティポリシーに関する改訂が必要と判断した場合には、その修正ついてアドバイスを実施すること。

（２） 監査調書の作成

監査結果を監査項目ごとに取りまとめた監査調書を作成すること。

（３） 監査成果物の作成

監査報告書及び、地方公共団体情報システム機構が提示した報告様式案（以下、外部監査の実施に係る報告様式と表記する）を作成すること。

監査成果物のうち、「監査報告書、監査調書（監査項目全てについて監査結果がわかるもの)、外部監査の実施に係る報告様式」は地方公共団体情報システム機構へ提出する必要があるため、その点を留意して作成すること。

（４） 監査報告会の実施

監査報告会を実施すること。報告会は原則 Web 会議での開催とし、必要に応じて本町と調整して実施すること。

６．エンドポイントセキュリティソフト(EPP)の要件

（１） 機能要件

EPP の導入にあたっては、ログ管理および分析を含む運用管理機能を統合的に管理可能な構成とし、単一の管理コンソールによる一元的な監視および運用を可能とすることで、インシデント対応の迅速化、運用管理コストの低減および調達に係る費用の最適化を達成することができるものを選定すること。

以下の防御機能をサポートし、別紙.機能要件回答書の要件を満たすこと。

① アンチウイルス対策として、EPP 製品を導入すること。

② LGWAN 系に配置している端末に適用すること。

③ メーカーのサポートサイトからパッチファイルのダウンロードする際は、既存のローカルブレークアウト（以下：LBO）環境を経由して行うこと。なお、LBO 装置の設定は、既存事業者にて行うことを想定しているため、協議のうえ必要な情報を提供すること。なお、設定作業費は、既存事業者と本町との間にて対応するため、今回の提案費用に含める必要はない。

④ クライアントソフトウェアの配布については、東彼杵町にて実施する。

⑤ クライアントソフトウェアは、必要最低限のライセンス数で構成すること。

⑥ オンプレミス環境に管理サーバを設置することなく、管理コンソールが準備できること。

⑦ 管理コンソールについては、日本語対応していること。

⑧ インシデントのリスクイベントを、30 日間、コンソールに表示できること。

⑨ 外部サーバにログを保存する機能を有すること。また、管理コンソールおよびデータの保存場所は、日本国内であること。

⑩ 将来的なセキュリティ管理・インシデント分析を容易にするため、単一のメーカー製品にて、EDR, NDR、リアルタイムのリスク検出とリスクベースの脆弱性管理、ゼロトラスト構成、等が行え、統合管理ができること。

（２） システム要件

① 最新の要件は公式サポートにて随時更新されること。

② 対応 OS は以下に対応すること。

Windows 10/11、Windows Server 2012 以降、macOS、Linux 等

（３） ライセンス要件

① EPP は、LGWAN 系に配置している端末 120 台及びサーバ 30 台を対象として利用可能なライセンスを提供すること。

② 上記ライセンスには、管理コンソールの利用に必要なライセンスを含むこと。

③ ライセンス数は、初期導入時に必要な数量を示すものであり、運用開始後の増減については本町との協議により対応すること。

（４） 運用要件

① アラート管理： 重大なアラートを可視化し、容易に調査を行うことが可能であること。

② ポリシー管理：部署や端末の役割（PC/サーバー）に応じたエンドポイントポリシーテンプレートの作成・適用が可能であること。

③ レポート機能：定期的な脅威検知状況の集約・出力が可能であること。

（５） 製品構成例

以下は、本要件を満たし得る製品構成の一例であり、特定の製品・メーカーを指定するものではない。

同等以上の機能・要件を満たす製品であれば提案可能とする。

- Fortinet FortiEDR(Endpoint Protection / EDR)
- Microsoft Defender for Endpoint
- CrowdStrike Falcon Protect / Insight
- Trend Micro Vision One Endpoint Security
- Palo Alto Networks Cortex XDR

７.実施体制及び構成員に関する要件

（１） ISO/IEC27001（JIS Q 27001）認証またはプライバシーマーク認証を取得していること。

（２） 監査責任者、監査人、監査補助者、監査品質管理者等で構成される監査実施体制を作ること。

（３） 監査チームには、情報セキュリティ監査に必要な知識及び経験を持ち、「ア ネット

ワーク技術分野」の資格を有するもの、「イ 情報セキュリティ監査分野」の資格を有するものがそれぞれ１名以上含まれること。各分野の資格を保有する監査人は同一でも構わない。また監査責任者と兼務でも構わない。

ア　ネットワーク技術分野

・ネットワークスペシャリスト（テクニカルエンジニア(ネットワーク)も可）

・情報処理安全確保支援士

又はこれと同等以上の資格または知識・経験を有する者

イ　情報セキュリティ監査分野

・公認情報セキュリティ主任監査人

・公認情報セキュリティ監査人

・ISMS 主任審査員

・ISMS 審査員

・システム監査技術者

・公認情報システム監査人（CISA）

・公認システム監査人

・情報処理安全確保支援士

（４）　監査チームには、監査の効率と品質の保持のため、次の実務経験を有する専門家がそれぞれ１人以上含まれていること。

ア　過去５年以内に、日本国内の自治体または団体において情報セキュリティ監査の実務経験を有している者

イ　α’モデル採用自治体における外部監査の実務経験を有している者

（５）　監査チームの構成員が、庁内ネットワークの企画、開発、運用、保守等の契約を履行した実績（再委託を含み、現在履行中の契約も含む）を有しない者であること。

（６）　上記要件を満たしていることについて、別添「監査チーム編成表」を記載し、資格の免状等の写しを添付した上で、契約締結後すみやかに本町に提出すること。

８．委託業務における提出物

（１）セキュリティ監査

① 監査実施計画書
② 試験成績表
③ 監査チェックリスト
④ 監査調書
⑤ 監査報告書
⑥ 外部監査の実施に関わる報告様式
⑦ アドバイス一覧
⑧ 議事録

⑨　提案書

再委託先の監査結果に基づく助言内容を整理し、受託者はインシデント対応の迅速化、運用管理コストの低減および調達に係る費用の最適化を達成することを見据えた次期庁内 LAN の暫定的な構想を提示すること。

（２）エンドポイントセキュリティ（EPP）

①　システム構成図

②　システム構成品一覧

③　基本設計書

④　パラメータシート

⑤　試験成績表

（３）納品方法

提出書類はすべて日本語で記載し、原則としてＡ４版で作成すること。

①　紙媒体　　１部

②　電子媒体　１部

９．個人情報

（１）　受託者は、本業務に関わることで知り得た個人情報及び本町から提供された個人情報について、第三者に知らせてはならない。また、本業務終了後も同様とする。

（２）　受託者は、上記個人情報を本業務の目的以外に利用してはならない。ただし、本町が承諾した場合はこの限りではない。

（３）　受託者は、上記個人情報を本町の承諾なしに複写又は複製してはならない。

（４）　受託者は、本業務の成果物の中で、個人情報を使用する場合、その作業、処理等を第三者に委ねてはならない。その管理方法について、本町が適当と判断できない場合は、本町は受託者に対し管理方法の改善を請求できる。

（５）　個人情報の漏洩により本町が損害を被った場合、本町は受託者に対しその損害に対する費用を諸求できる。ただし、個人情報の漏洩が受託者の責に帰すると判断できない場合は、この限りではない。

10. セキュリティ対策等

（１）　本システムを構成する機器について、必要となる全てに対しアンチウィルスソフトウェアを導入すること。リモートメンテナンスを含む全てのネットワーク通信について、通信傍受及び不正侵入等に対するセキュリティ対策を講ずること。

（２）　情報セキュリティ確保の観点から、受託者は情報セキュリティマネジメントシステム認証（ISO/IEC27001、JISQ27001）取得に相当する取り組みを実施していること。

※委託会社にて取得している場合は可とする。

11. その他事項

（1） 受託者は、本業務の責任者を選定し、業務従事者の指揮監督を行うこと。

（2） 本業務の遂行に当たっては、本町と十分に協議を行い、本町の指示に従うこと。また、本町の施設内で作業を行う際は、本町の指示に従うこと。

（3） 受託者は、設定、動作確認等の作業の際、他の業者と関連する場合には、相互に協調し作業の便宜を図ること。

（4） 本契約の履行中に知り得た情報を他に漏らさないこと。

（5） 本仕様書に明記していない事項であっても、本システムの運用及び機能上当然具備すべき事項は、これを充足すること。

（6） 受託者は、本業務の一部を下請会社に代行させるときは、事前に本町に通知し承諾を得ること。

（7） 本業務の実施に当たり建造物及び機器等に損傷を与えた場合は、速やかに協議のうえ、受託者の負担で復旧すること。

（8） 本業務の完成に際しては、作業現場の後片付け及び清掃を十分に行うこと。

12. その他

（1） 前述のソフトウェア要件に提示したソフトウェアを適切に設定し導入すること。

（2） 既存端末に、追加のソフトウェアの導入や、その他設定が必要となる場合は、既存端末の OS に応じた手順書を作成し提出すること。

（3） 状況に応じ、東彼杵町内で確認が必要な場合は、現地確認を行い本見積に含めること。

機能要件回答書（共通フォーマット）

No	機能カテゴリ	機能要件	区分	回答	備考
1	マルウェア対策	ファイルの入出力をリアルタイムに監視し、マルウェアを検知・隔離・削除等が可能であること	必須（EPP）		
2	マルウェア対策	既知および未知の脅威を、振る舞い検知や機械学習等によりリアルタイムに検知・対応可能であること	必須（EPP）		
3	マルウェア対策	クラウド上の最新セキュリティ情報を参照して検知を行えること	必須（EPP）		
4	侵害防止	プロセスやシステム挙動を監視し、不正な変更や侵害行為を検知・防御できること	必須（EPP）		
5	侵害防止	正規機能（PowerShell、WMI 等）を悪用した攻撃を検知可能であること	必須（EPP）		
6	ランサム対策	不正な暗号化や改ざん行為を検知・防御するランサムウェア対策機能を有すること	必須（EPP）		
7	通信監視	C&C サーバ等の不正な外部通信を検知し、通信元端末を特定可能であること	推奨（EDR）		
8	挙動分析	端末の通信・挙動情報を基に侵害兆候を検知・可視化できること	推奨（EDR）		
9	管理機能	管理コンソールにより端末の状態、検出イベントを一元的に確認できること	必須（運用）		
10	管理機能	管理コンソールが日本語に対応していること	必須（運用）		
11	管理機能	インシデントやリスクイベントを一定期間（30 日以上）確認可能であること	必須（運用）		
12	管理機能	誤検知時に例外（ファイル／プロセス等）設定が可能であること	必須（運用）		
13	ログ管理	セキュリティログを外部サーバに保存可能であること	必須（運用）		
14	ログ管理	ログ検索結果を CSV または Excel 形式で出力可能であること	必須（運用）		
15	レポート	レポートをスケジュール出力し、PDF 等の形式で出力可能であること	必須（運用）		
16	構成	オンプレミスに管理サーバを設置せず、クラウド型で運用可能であること	必須（構成）		
17	将来拡張	EDR、NDR、脆弱性管理、ゼロトラスト等へ将来的に拡張・統合管理が可能であること	将来要件		

本要件における将来拡張項目については、導入時点での実装を必須とするものではなく、同一メーカー製品との連携や拡張により段階的に実現可能であることを求めるものとする。