
令和8年度

次世代エンドポイントセキュリティ対策設定業務委託
仕様書

令和8年10月

目 次

1 章 概要	1-1
1.1 本調達の名称	1-1
1.2 目的	1-1
1.3 契約期間.....	1-1
1.4 納入期限.....	1-1
1.5 納入場所.....	1-1
1.6 発注形態.....	1-1
1.7 基本要件.....	1-2
1.8 適用範囲.....	1-3
1.9 構築スケジュールと作業内容.....	1-3
1.10 作業箇所と範囲.....	1-4
1.11 委託料.....	1-4
1.12 検収	1-4
2 章 導入作業	2-5
2.1 導入要件.....	2-5
2.2 移行要件.....	2-6
3 章 保守運用	3-6
3.1 保守業務.....	3-6
3.1.1 基本方針	3-6
3.1.2 保守条件	3-7
3.1.3 障害受付業務.....	3-7
3.1.4 障害対応業務.....	3-7
4 章 その他	4-1
4.1 その他の要件	4-1

1章 概要

1.1 本調達の内容

本調達の名称は「次世代エンドポイントセキュリティ対策設定業務委託」とする

1.2 目的

本書は、委託者が保有する情報端末を対象として、次世代エンドポイントセキュリティソフトウェアの導入・切り替えに係る調達仕様を定めるものである。

近年、サイバー攻撃の高度化・複雑化に伴い、従来のウイルス対策ソフト（シグネチャベース）のみによる防御では対応が困難な脅威が増加している。本調達により、振る舞い検知・AI 分析・リアルタイム対応を備えた次世代エンドポイントセキュリティ製品を導入し、委託者の情報資産を保護するとともに、安全・安定した行政サービスの継続を図ることを目的とする。

本書の構成を以下に示す。

1.3 契約期間

契約の日から令和9年3月31日までとする

1.4 成果品の納入期限

令和9年3月15日 とする

1.5 納入場所

酒田市本町二丁目2番45号 酒田市企画部デジタル戦略課

1.6 発注形態

本調達は、以下を含む一式とする。

- ・ エンドポイントセキュリティソフトウェアのライセンス・導入設定
- ・ 初年度の運用保守（設定変更、インシデント対応支援等）
- ・ 契約期間（1年間）分のソフトウェアライセンス費用
- ・ 管理コンソール等の利用費用（クラウド型の場合を含む）

なお、初年度の運用保守は本契約に含むものとする。次年度以降の保守については別途契約を締結する予定であるが、この運用保守契約の歳入歳出予算の当該契約金額については現時点で確保されていないため、確約されたものではない。

1.7 基本要件

導入するエンドポイントセキュリティ製品は、従来のウイルス対策ソフト（シグネチャベース）のみによる防御では対応が困難な脅威への対策をする必要があり、以下を基本要件とする。

なお、詳細な機能要件については別紙「機能要件仕様書」の要件を満たすこととする。

表 1.78-1 機能要件概要区分	要 件
エージェント 構成	単一エージェントによりリアルタイム・予約・オンデマンド検索を含むエンドポイント防御機能を統合的に提供できること
マルウェア・ランサムウェア対策	既知マルウェア及びファイルレスマルウェアを検出・防御できること ランサムウェア攻撃を検知し、暗号化されたファイルをロールバック復旧（ボリュームシャドウコピー非依存）できること
	MBR 暗号化やリモート攻撃を含むランサムウェア攻撃を検知・防御できる機能を有すること
	マルウェア検知時にプロセス停止・ファイルクリーンアップを行い、脅威の侵入経路・影響範囲をマッピング表示できること
	既知の攻撃のみならず、AI 分析・振る舞い検知により未知の攻撃やファイルレス攻撃、正規プロセス（PowerShell、WMI 等）を悪用した攻撃も検知・防御できること。
	ランサムウェア攻撃を検知した場合、管理者の操作を介さず自動的に該当プロセスを停止する等の処置を行えること。
Web・ブラウザ 保護	MITB 攻撃の防止、ブラウザ Cookie の保護、URL フィルタリング及びダウンロードファイルのレピュテーション評価機能を有すること
デバイス・アプリケーション制御	外部記憶媒体（USB 等）の接続制御、アプリケーションコントロール及び情報漏えい対策（DLP）機能を有すること
	攻撃を検知した際に保護レベルを自動的に強化し、Safe モード起動時も保護機能を継続できること
管理・運用	一元管理コンソールにより端末の保護状態・アラートを可視化・集中管理でき、月次等のセキュリティレポートを出力できること
	攻撃を検知した場合、その根本原因・影響範囲・時系列での挙動を管理コンソール上で把握できること。

	管理コンソールより、検知した脅威に対する該当プロセスの停止、マルウェアの検疫、ネットワークからの隔離等の対応を遠隔操作で行えること。また、これらの対応を検知単位で一括して行えること。
	エージェントが収集した情報を任意のキーワードで検索でき、検索結果を CSV 形式（日本語データを含む）で出力できること。
	攻撃を検知した場合、メールにより通知できること。
	誤検知・過剰検知を低減するため、ハッシュ値やファイル名だけでなく、ふるまい単位での検知除外設定ができること。
	管理 UI 及び出力レポート（PDF）は日本語に対応していること。
サポート・ライセンス	日本語対応のテクニカルサポートを有すること。ライセンス形態はユーザーライセンスであること
評価実績	Gartner 等の第三者評価においてリーダーポジションを有し、国内での導入実績があること

1.8 適用範囲

本仕様書は、以下を対象とする。

- ・ 委託者が保有する業務用端末（PC、ノート PC、サーバー等）
- ・ 対象 OS：Windows（主体）
- ・ 対象台数：約 1,720 台（クライアント 1,630 台、サーバー 90 台）
- ・ 管理コンソール（クラウド型又はオンプレミス型）

1.9 構築スケジュールと作業内容

導入スケジュール（予定）を以下に示す。

フェーズ	期間（目安）	主な作業内容
要件確認・設計	契約後 第 1～2 週	既存環境調査、ポリシー設計、展開計画作成
テスト導入	第 3～4 週	パイロット端末へのエージェント導入・動作確認
全端末展開	第 5～8 週	全対象端末へのエージェントインストール・設定適用
切替完了・検収	第 9 週以降	旧製品アンインストール、動作確認、成果物提出・承認

主な作業内容

- (1) 既存環境調査：端末 OS・台数・ネットワーク構成・既存セキュリティ製品の確認
- (2) ポリシー設計：市の運用方針に基づくセキュリティポリシーの設計・文書化

-
- (3) エージェント展開：Active Directory グループポリシー等を活用した一括展開
 - (4) 旧製品撤去：既存ウイルス対策ソフトの安全なアンインストール及び後処理
 - (5) 動作確認・試験：検知・遮断・ログ収集等の機能試験の実施及び報告

1.10 作業箇所と範囲

- (1) 作業実施に当たり、クラウド又は庁舎内サーバへの管理コンソールの展開・初期設定を行うこと。
- (2) 対象全端末へのセキュリティエージェントのインストール・ポリシー適用を行うこと。
- (3) エージェントのインストール後に現行ウイルス対策ソフトのアンインストール作業を実施すること。
- (4) 既存のシステムに影響を及ぼす場合、直ちにポリシーの構成の見直しと適用を行うこと。
- (5) ファイアウォール・プロキシ等の通信要件確認・設定変更支援を行うこと。
- (6) 管理者向けのコンソール操作・アラート対応手順等の説明を実施すること。

1.11 委託料

委託料は、業務完了後に一括で支払うものとする。

1.12 検収

受託者は、試験運用を実施し、エンドポイントセキュリティに係わる検査を実施する。
検収条件として、以下にあげる納入成果物を提出し、委託者の承認を得ること。

表 1.121-1 設計・構築に関する納入成果物

名称	内 容
納入ライセンス一覧表	本調達で手配したソフトウェアライセンス名・数量・有効期限等が記載された一覧表
基本設計書	全体構成図、管理コンソール構成、エージェント設定の概要等を記載したもの
詳細設定書	適用したセキュリティポリシーの詳細設定値を示す書類
端末管理台帳	エージェント導入済み端末の一覧（ホスト名・OS・IP アドレス等）
試験計画書	試験実施スケジュール、試験項目、判定基準等を記載した書類
試験結果報告書	機能試験・検知試験の実施結果を報告する書類

表 1.121-2 設計移行に関する納入成果物

名称	内 容
移行実施計画書	旧製品からの切り替えスケジュール、切り戻し判定基準、リスク対応方針等を定めた計画書 課単位等の作業単位に作成し、職員の同意を得てから作業を実施すること
移行手順書	旧製品アンインストール・新製品導入・設定移行の手順を記載した成果物
移行結果報告書	切り替え作業の結果及び確認事項を報告する書類

表 1.121-3 保守・運用に関する納入成果物

名称	内 容
運用マニュアル	コンソール操作手順、アラート対応手順、インシデント発生時の初動対応等を定めた書類
構成管理書	セキュリティポリシーの設定情報・変更管理に関する書類
保守要綱	ソフトウェアアップデート・ライセンス管理・障害対応の保守実施手順を定めた書類
保守対象一覧	保守対象端末・コンソールの設置情報、担当者・連絡先等を示す書類

なお、「ポリシー設定書」「試験計画書」「試験結果報告書」については、管理コンソールの設定画面キャプチャ又は標準テンプレートポリシーからの変更箇所一覧、及びあらかじめ定める標準試験項目（マルウェア検知、ランサムウェア検知（模擬）、通信遮断、ログ収集、管理コンソール連携）に基づく簡易チェックシート（結果一覧を含む）をもって足りるものとし、詳細な仕様書・個別テストケース設計書の別途作成は求めない。

2章 導入作業

ソフトウェアの導入を実施する上で、必要な項目を以下に記載する。

2.1 導入要件

- (1) 契約締結後速やかに委託者と打合せを行い、既存環境の調査及び導入計画を策定すること。
- (2) エージェントの導入に当たっては、パイロット展開を先行して実施し、問題がないことを確認したうえで全端末への展開を行うこと。
- (3) 展開方法は **Active Directory** グループポリシー等の自動配布を推奨するが、環境に応じて適切な方法を提案すること。サイレントインストールに対応すること。対応できない場合は、代替の一括展開方法を提案すること。
- (4) 導入作業中は業務への影響を最小限に抑え、必要に応じて業務時間外に作業を実施すること。
- (5) 導入後は管理コンソールにて全端末の保護状況を確認し、漏れなく適用されていることを

委託者と共に確認すること。

2.2 移行要件

- (1) 現行の端末に導入されているウイルス対策ソフト等のセキュリティ製品を安全にアンインストールし、新製品への切り替えを円滑に実施すること。
- (2) 切り替え作業は段階的に実施し、問題発生時は速やかに旧製品へ切り戻せる体制を整えること。
- (3) 移行期間中、保護されていない状態の端末が生じないよう、新旧製品の切り替えタイミングを管理すること。
- (4) 移行完了後、旧製品のライセンス解除を実施すること。
- (5) 移行結果は移行結果報告書にまとめ、委託者の承認を得ること。
- (6) サーバー側エージェントの移行については下記の作業分担とする。
 - インストーラーの作成：受託者
 - エージェント移行作業：各サーバーメンテナンス業者なお、サーバーエージェントの移行完遂は本業務に含まず、委託者と各サーバーメンテナンス業者が協議のうえ実施するものとする。

3章 保守運用

保守・運用を実施する上で必要な項目を以下に記載する。

3.1 保守業務

エンドポイントセキュリティは、市の情報資産を守る重要な基盤であることから、安定したセキュリティサービスの提供を可能とする保守体制・保守手順を確立し、サービス品質の維持・向上に努めること。

3.1.1 基本方針

- (1) 安定的・効率的な保守基盤を確立すること。
- (2) 障害対応・運用・保守の受付窓口を一元化し、インシデント対応の迅速化を図ること。
- (3) アップデート管理・ポリシー変更・監視を含め、体系化された保守体制を確立すること。
- (4) 連絡体制を明確化し、担当職員及び情報セキュリティ管理責任者への連絡を円滑かつ迅速に行える仕組みとすること。
- (5) 保守体制表（技術担当者の氏名、電話連絡先、電子メールを含む情報）を提出すること。また、保守体制表に変更が生じた場合、内容を提示し委託者の承認を得ること。
- (6) 受託者は、障害連絡を受けてから概ね1時間以内に一次対応（リモート対応可）を行い、最

短時間での復旧に努めること。

- (7) 作業実施手順・ルールを標準化し、マニュアルとして整備すること。
- (8) 調達ソフトウェアのマニュアルを提供すること。マニュアルは可能な限り電子媒体で提供すること。
- (9) 本調達ソフトウェアにセキュリティ上の致命的な欠陥が発見された場合は、必要な情報を提供し、委託者と協議のうえ対処すること。

3.1.2 保守条件

- (1) ソフトウェアのバージョンアップ・パッチ適用を計画的に実施し、常に最新の保護状態を維持すること。
- (2) ライセンスの有効期限を管理し、期限切れが生じないよう事前に委託者へ通知・更新手続きを行うこと。
- (3) 月次又は随時、セキュリティ稼働状況・検知レポートを委託者へ報告すること。
- (4) セキュリティポリシーの変更・追加が必要な場合は、委託者の承認を得てから適用すること。
- (5) 管理サーバのメンテナンス（バージョンアップ作業等）は、ライセンス期間中、回数無制限及び無償で提供すること。

3.1.3 障害受付業務

- (1) インシデント・障害の連絡を一元的に受け付けること。
- (2) 原則として平日、8時30分から17時15分の時間内において受付を行うこと。
- (3) 連絡を受けた場合は速やかに原因の切り分け作業・一次対応（リモートによる調査・隔離等）を行うこと。
- (4) 切り分け結果に応じて現地対応、又は他の保守事業者・ベンダーへの連絡を行うこと。

3.1.4 障害対応業務

- (1) 受付結果に応じて、必要に応じて現地に出向き、障害箇所の特特定・リカバリ作業・設定修正等を行うこと。
- (2) 対応時は進捗報告・対応（復旧）報告を実施すること。
- (3) 平日受付時間外に重大なインシデントが発生した場合は、翌営業日以内に一次対応又は関係者への連絡・対処を行うこと。なお、ランサムウェア等の重大インシデントについては時間外対応の可否・手順についても事前に取り決めること。

4章 その他

4.1 その他の要件

- (1) 本仕様書に定めのない事項および疑義を生じた事項については、委託者と受託者が協議し、その解決にあたること。
- (2) 受託者は本調達に当たり、関係法令および酒田市の条例、規則、要綱を遵守して業務にあたること。
- (3) 受託者は委託者が定める「酒田市情報セキュリティポリシー」を遵守して業務にあたること。
- (4) 受注者及びその作業者は、本業務に関して知り得た一切の事項について、第三者に漏らしてはならない。上記内容は本業務終了後も同様とする。
- (5) 受注者及びその作業者は、本業務に係わる全ての個人情報の保管・管理について当市個人情報保護条例、及び電子計算機処理に係わるデータ保護管理規定に従うこと。また、当該データの漏洩、消滅、棄損等の事故発生を防止すること。
- (6) 目的外使用の禁止について、受託者は、委託者が保有する情報媒体（磁気ディスク、磁気テープ、光磁気ディスク、フロッピーディスク等）を本業務の目的外に使用し、または第三者に提供してはならない
- (7) 複写及び複製の禁止について、受託者は、委託者が保有する情報媒体等を委託者に無断で複写し、または複製してはならない。委託者の許可を受けて複写及び複製したときは、本業務終了後直ちに個人情報を消去し、再生又は再利用ができない状態にしなければならない。
- (8) 事故発生時における報告義務について、受託者は、事故が生じたときは、直ちに委託者に対して報告するとともに、遅滞なくその状況を委託者に通知し、委託者の指示に従いその解決に努めなければならない。
- (9) 受託者における個人情報の保管及び廃棄について、受託者は、本業務に係わる個人情報の保管及び管理について、善良な管理者の注意をもって当り、個人情報の消滅、毀損等の事故を防止しなければならない。
- (10) 受託者は、本業務を終了したときは個人情報を消去し、再生または、再利用ができない状態にしなければならない。また、委託者が請求したとき、受託者はその保有する本業務に係わる個人情報を直ちに委託者に返還しなければならない。

別紙1 機能要件仕様書

■セキュリティ対策ソフト仕様

	要件
1	単一エージェントでエンドポイント防御機能を提供できること。
2	リアルタイム検索機能を有すること。
3	予約検索機能を有すること。
4	オンデマンド検索機能を有すること。
5	既知マルウェアを検出・ブロックできる機能を有すること。
6	AMSI（Microsoft Antimalware Scan Interface）を利用した防御機能を有すること。
7	ファイルレスマルウェアに対応した防御機能を有すること。
8	ランサムウェア攻撃を検知し、ロールバックできる機能を有すること。
9	ランサムウェアにより暗号化されたファイルを復旧させる際にボリュームシャドウコピーを利用せずに復元できること。
10	マスターブートレコードを暗号化するランサムウェア攻撃を検知・ブロックできる機能を有すること。
11	リモートからのランサムウェア攻撃に対する防御機能を有すること。
12	ブラウザに存在する脆弱性を攻撃してWebブラウザに感染するMITB（Man-in-the-Browser）攻撃を防止する機能を有すること。
13	ブラウザのCookieを保護する機能を有すること。
14	マルウェア検知時にプロセスの停止やファイルのクリーンアップ機能を有すること。
15	脅威を駆除した後に脅威の侵入経路及びファイルに対する影響範囲（発生日時、アプリケーションなど）などをマッピングして表示する機能を有すること。
16	デバイスへの攻撃と思われる検知が確認された場合に、Safeモードの再起動を防止するなどといった形で保護レベルが自動的に高くなる機能を有すること。
17	Safeモードで起動しても保護機能を保持し続けること。
18	URLフィルタリング機能を有すること。
19	ダウンロードしたファイルを評価するレピュテーション機能を有すること。
20	USBメモリやMTP/PTP接続デバイスといった、外部機器の接続に対して制御する機能を有すること。
21	アプリケーションコントロール機能を有すること。
22	情報漏えい対策（DLP）機能を有すること。
23	ベンダーが有するテクニカルサポートセンターを利用することができること。
24	テクニカルサポートが日本語対応できること。
25	海外拠点で利用する場合、ライセンス調達場所に依存せず、海外のテクニカルサポートを利用することができること。
26	PCへのインストールは、デバイスライセンスではなくユーザーライセンスであること。
27	Gartnerなどの第三者評価でリーダーのポジションであること。
28	国内で導入実績があること。