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対応入札仕様書(サンプル)

「渋谷区モデル」導入仕様書

【本資料の前提条件】

本資料は総務省　平成30年9月版「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」に基づき、IT資産管理システム・マルウェア対策システム等のクライアント統合管理システムに関する仕様書サンプルとなります。「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」で求められるすべてのセキュリティポリシーに対応するものではありません。

目次

[1. 概要 3](#_Toc39764586)

[1 本調達の背景と目的 3](#_Toc39764587)

[2 調達物品名及び構成内容等 3](#_Toc39764588)

[2.1 調達物品名及び数量 3](#_Toc39764589)

[2.2 構成内訳 3](#_Toc39764590)

[3 納入期限 4](#_Toc39764591)

[4 納入場所 4](#_Toc39764592)

[2. システム要件 5](#_Toc39764593)

[1 機能要件 5](#_Toc39764594)

[1.1 基本要件 5](#_Toc39764595)

[1.2 資産管理システム 5](#_Toc39764596)

[1.3 不正プログラム対策システム 7](#_Toc39764597)

[1.4 盗難・紛失対策システム（MDM） 7](#_Toc39764598)

[3. システム保守要件 8](#_Toc39764599)

[1 システム保守 8](#_Toc39764600)

[1.1 ソフトウェア保守 8](#_Toc39764601)

[1.2 ハードウェア保守 8](#_Toc39764602)

[4. システム導入要件 8](#_Toc39764603)

[1 システム導入・研修 8](#_Toc39764604)

[1.1 搬入、設定および導入作業 8](#_Toc39764605)

[1.2 導入支援および研修 8](#_Toc39764606)

[5. その他 9](#_Toc39764607)

# 概要

## 本調達の背景と目的

地方公共団体は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、

ほかに代替することができない行政サービスを提供している。

この保有する情報資産の機密性、完全性及び可用性を維持するため、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を元に、本○○（県・市・町などを記入）行政情報ネットワークに接続しているパソコンの管理とセキュアな環境の維持を○○（県・市・町などを記入）〇〇部〇〇課で集中的に一元管理を行なうために必要となる機器及びソフトウェアを調達する。

## 調達物品名及び構成内容等

### 調達物品名及び数量

○○（県・市・町などを記入）クライアント統合管理システム　・・・・・・・・・　1式

※以下、「システム」という。

### 構成内訳

1. ソフトウェア
   1. システム使用に際してのライセンス

※クライアント数を○○（PC台数）とする

* 1. データバックアップソフトウェア

1. ハードウェア
   1. システム管理用サーバー
   2. データバックアップ装置
   3. 無停電電源装置

※すべて付属品を含むものとする

※システム管理用サーバーには、オペレーションシステムを含むものとする

※システム管理用サーバーを複数要する場合は、ディスプレイ、セレクタ、マウス（ポインティングデバイス）、キーボードを添付するものとする

1. ソフトウェア保守
2. ハードウェア保守
   1. システム管理用サーバー保守
   2. データバックアップ装置保守
   3. 無停電電源装置保守
3. 導入及び研修
   1. システム設定設置
   2. 現行システムからのデータ移行
   3. 設計書、マニュアル
   4. システム管理職員への初期研修

## 納入期限

令和○年○月○日（日付を記入）

## 納入場所

○○（納入場所を記入）

# システム要件

## 機能要件

### 基本要件

1. 本システムを提供するにあたって、法令等の定めを十分に理解し遵守すること。
2. 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を十分理解し利便性を損なわない提案をすること。
3. LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすること。
4. セキュリティに対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施すること。
5. インターネット及び外部からの不正侵入対策
6. 意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等の対策
7. 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反による非意図的要因による情報資産の漏えい・破壊・消去等の対策
8. 権限設定によるアクセス可能範囲の限定
9. 位置情報ログ／盗難紛失対策
10. マルウェア対策（ゼロデイ攻撃／事前防御）
11. サーバー、クライアント機器のOS等のセキュリティ対策

### 資産管理システム

1. 全般
   1. 個人単位でアクセスログ等を取得し、不正利用を防止するとともに権限に応じた利用範囲の制限を行うこと。
   2. 外部メディアへのデータ保存は原則禁止し、指定のUSBメモリからの情報登録のみ許可する仕組みとすること。
   3. 無許可ソフトウェアの導入等を禁止すること。
   4. 無許可でのネットワーク接続を禁止すること。
   5. ISO/IEC、ISO/IEC15408を取得しているメーカーの製品を選択すること。
   6. 保守期間中は、マイナー/メジャーバージョンアップ/後継品を問わず、○○（県・市・町などを記入）と協議の上、事前動作確認を行った上で最新版のプログラム提供を行うこと。
   7. Windows10 pro に対応しているとともに保守契約期間中については、最新OS対応を無償で行うこと。
   8. Windows10 のFeature Updatesに対応する場合でも、クライアントモジュールのバージョンアップのみで対応できること。
   9. ガイドラインに抵触する違反操作が発生した際には、各監督責任者にメール通知と共に、監督責任者毎に、適した閲覧権限での閲覧画面を特別権限として提供すること。
   10. 人事異動を考慮し、セキュリティ上の部門管理責任者に、特別権限をシステム的に与えた際には、集中管理画面にて、特別権限の剥奪、設定が可能なこと

1. 資産管理
   1. クライアント PC から資産情報を自動的に収集し一覧で表示できること。
   2. 特定のファイル名に含まれるキーワードを指定すると、自動で検索が行われ、発見されたファイルに関する情報が一覧形式で確認できること。
   3. 無許可のソフトウェアがインストールされた場合に検知ができるように、新たにソフトウェアがインストールされた際に、アラートを出すことができること。
   4. ソフトウェアのライセンス管理が行えること。尚、インストールされているソフトウェアに対して有償のものなのか無償ものなのかを自動判別を行う、ソフトウェア辞書を提供されており、ソフトウェア辞書は10万件以上のソフトウェアが登録されていること。
   5. 開発元のサポートが終了したOS・ソフトウェアを利用しないように、適用状況が一覧形式やダッシュボード形式で確認できること。
   6. 許可のないPCやモバイル端末がネットワークに接続されないように制限ができること。
2. 操作ログ管理
   1. 情報漏洩リスクを軽減する為、各クライアントパソコンでの以下操作内容の記録を自動収集する仕組み

を用意していること。

・コンピュータ名、ユーザ名、IPアドレスは全てのログに紐づいて取得されるものとする。

・操作内容はウィンドウタイトル名取得、ファイル操作はファイルパスと操作内容（ファイルコピー/移動/作成/削除/名前変更/上書き/閲覧、USB書き込み、Windows標準のライティング機能を利用した

CD/DVDの書込み等）を自動収集する機能を有していること。

* 1. ファイルコピー/移動/ファイル名変更の場合は元、先の変更前、変更元のパス、ファイル名がそれぞれ

取得され、ファイルの追跡が行えること。

* 1. 定期的にログを監視し、違反操作を発見し、即座に対策を打ち問題を未然に防ぐ為、運用上のルール（禁止アプリケーション起動、禁止Webサイトの閲覧、禁止デバイスの使用等）を違反した際に、リアルタイムに本人・指定した管理責任者複数名にそれぞれの管理する違反内容を通知する機能（通知メール）を有していること。

1. Webアクセス制御
   1. 各クライアントパソコンでのWeb閲覧履歴の記録（コンピュータ名、ユーザ名、IPアドレス、アプリケーション名、ウィンドウタイトル、URL等）を自動収集する機能を有していること。
   2. SSLで暗号化されたサイト（HTTPS）に対し、Internet Explorer、Google Chrome、Firefoxでアクセスを行い、WebタイトルとURLが取得できること
   3. 業務外の目的でWebサイトが閲覧できないよう、犯罪、アダルト、出会い等、業務と関係の無いWebサイトについてカテゴリーを指定して閲覧を禁止できる機能を有していること。
   4. Webメールやオンラインストレージサービス等を利用できないように制限できる機能を有していること
2. デバイス制御
   1. データの持ち出し出口を必要最小限にし、情報漏洩リスクを軽減する為、各クライアントパソコンに、CD・USB・フロッピー等の記憶媒体を禁止する機能を有していること。また、読み込みのみ許可する設定が可能なこと。
   2. 使用認可したUSB機器のみを使用可能にする為、特定のシリアルNO、USB名のUSB機器のみを禁止除外する機能を有していること。
   3. SDカードの制御、個体識別による除外登録が可能なこと。また、個体識別の方式としてはファイルをコピーされるリスクも考慮し、個体識別情報を、SDカード内にファイルとして格納しない仕組みであること。SDカードの時間指定による読み込みのみ許可する設定が可能なこと。
   4. 記憶領域をもつデバイスのみを禁止でき、volumeを持つデバイス、またはWPDデバイスといった記憶領域を持つデバイスのみ禁止設定が可能なこと。
   5. 部署ごとにデバイス管理責任者を特別権限として設定し、各部署で購入したデバイスを登録及び利用者を設定できること

### 不正プログラム対策システム

1. 全般
   1. 所掌するサーバー及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。。
   2. ゼロデイ攻撃に有効であること。
   3. 添付ファイルの無害化や実行を止める等の標的型攻撃／事前防御に有効であること。
2. エンドポイント型マルウェア対策機能
   1. エンドポイント上において、既知/未知のマルウェアを検知・隔離することができること。
   2. ファイル展開後も、システム動作の監視と制限を行い、不正にシステムが変更されるのを検知・防御できること。
   3. パターンファイルを常に最新の状態に保つことが困難な端末があることから、AI等のパターンファイルを利用しない仕組みであること。
   4. 常に最新の状態を保つ必要があることから、クラウド製品であることが望ましい。
   5. ファイルの静的な情報をもとに、不正なプログラムを実行前に止めることができること。
   6. ソフトウェア脆弱性の利用や、実行中のプロセスをエクスプロイトするようなマルウェアについても防御できること。
   7. エンドポイントでのインシデント発生時には操作履歴との連動が出来、発生時のクライアントPC操作の特定ができること。レポート上で、インシデントの発生が組織単位ででき、日々の問題点を把握できること。
   8. メモリ破壊に対して、アラートのみ、呼び出しのブロック、該当のアプリケーションを終了させる事ができること。また、除外設定により許可もできること。
   9. インターネット非接続環境でもエージェントの一斉展開やアップデートが可能なこと。
   10. 脅威を検知、自動隔離した場合に関わらず、また。インターネット接続・非接続に関わらず、検知結果が全て管理者に通知される機能を有していること

### 盗難・紛失対策システム

1. 全般
   1. 紛失時に、最終利用位置情報のログを残し遠隔操作にてデータ消去等の対策を講じること。
   2. ハードディスクードディスク装置を抜き取られても不正利用を防止するために、Bitlockerの暗号化機能を利用する。紛失時はBitlockerをかけた端末を初期化できること。また、管理の観点から暗号鍵が自動取得できる。
   3. 不正利用の観点から、SIMが挿入された端末でSIMが抜き差しされた場合に検知できる仕組みを有すること。
   4. その他有効な対策があれば提案すること。

# システム保守要件

## システム保守

### ソフトウェア保守

1. 本調達により構築したシステムを５年間運用するのに必要なソフトウェア保守ライセンスについては，すべて本調達に含まれるものとする。
2. 保守期間の間であれば最新のバージョンアップモジュールの提供が行えること。
3. 本クライアント管理ソフトは、日本国内のメーカーが開発・サポートしていること。
4. ソフトウェアの保守については、本クライアント管理システムを提供するソフトウェア開発メーカーに直接の電話、E-Mailでの問い合わせが可能であること。また、本クライアント管理ソフトウェア専用のヘルプデスク体制が提供されていること。

### ハードウェア保守

1. システム管理用サーバー、データバックアップ装置及び無停電電源装置について、5年間のオンサイト保守(平日9～17時定額当日訪問修理)を実施すること。
2. 機器の保守拠点が○○（県・市・町などを記入）に存在し、代替保守機材を有する体制がとれること。
3. 機器のオンサイト保守を実施するにあたり、必要な事務手続きを遅滞なく行えること。
4. 機器の定期保守点検を年2回以上行い、報告書を提出すること。定期保守日は○○（県・市・町などを記入）と協議のうえ設定し、保守作業の際はシステムの運用に与える影響は最小限にとどめること。

# システム導入要件

## システム導入・研修

### 搬入、設定および導入作業

1. 保守及びテスト環境とシステム運用環境を分離しなければならない。
2. システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策

定時に手順を明確にすること

1. 移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等

の影響が最小限になるよう配慮すること

1. ソフトウェアの設定を完了させ、可用性が確保されていることを確認し、既に稼働している情報システム等

に影響が無いか十分にテストを行うこと。

1. 搬入、設定及び設置作業を遂行する上で知り得た情報については、秘密の保持に留意し漏洩防止に努めるこ

と。

### 導入支援および研修

1. 必要なエージェントソフトの配付並びに、導入支援を行うこと。
2. システム管理職員への初期研修を1回以上開催すること。
3. 研修のテキストの内容、部数等については○○（県・市・町などを記入）と協議のうえ、必要な部数を準備

し提供すること。

# その他

　・ 提案事業者は、本業務の実施に あたり本 仕様書に記載のない事項または疑義が発生した場合は、速やかに ○○（県・市・町などを記入）と協議を行い、作業を実施すること。