静岡市振込通知オンライン化業務　業務委託仕様書

本仕様書は、静岡市（以下「本市」という。）が郵送にて実施している振込通知をオンラインで実施することを可能とする振込通知オンラインサービス（以下、「サービス」という。）を実施するにあたり、必要な事項を定めるものとする。

１　業務名

令和８年度　会委第３号　静岡市振込通知オンライン化業務

２　目的

現在、本市会計室における「振込通知書」の発行業務は、財務会計システム出力されたデータを専用用紙へ印刷し、専用機による圧着、目視による宛名確認を経て郵送している。その件数は、年間 82,000 件程度となっている。

昨今、地方自治体においては、デジタル技術を積極的に活用し、業務の効率化を進め、本来、職員に求められる企画運営業務等への人的資源の投入が行われているが、本市においても例外ではない。

こうした状況の中で、本市が実施している郵送による「振込通知書」の発行業務について、オンラインで振込内容の確認を可能とすることで、債権者の利便性を向上させるとともに、業務を効率化し、コスト削減、本市職員の負担軽減等を図ることを目的とする。

３　契約期間

本業務の契約期間は、契約を締結した日から令和９年３月 31 日までとする。

サービスの運用開始は令和８年 10 月１日とする。

なお、運用開始までに必要とする項目に関する詳細なスケジュールは、別途、本市と協議の上決定する。

４　履行場所

日本国内

５　業務内容

（１）調達の適用範囲

①オンラインで本市の振込内容を閲覧等することができるシステムにおける本市専用ページの構築（オンライン化に伴う初期設定や登録作業等におけるサポート体制の構築を含む。）

②オンライン化に伴う債権者に対する登録案内通知（11,000 件程度を見込む）

【内容】

ア　サービス開始のお知らせ

イ　利用登録案内

③システムの運用・保守

（２）システム導入後の運用

①本市職員が財務会計システムから抽出したデータ（PDF 又は CSV）を構築されたシステムにアップロードする

②システムが自動で帳票を作成し、債権者にメール等で通知する。債権者はシステムで振込内容を閲覧する

６　機能要件

（１）本市の財務会計システムから出力された CSV データ及び PDF データの両方の取り込みに対応していること

・本市においては、令和９年度から現在使用しているメーカーとは異なるメーカーの財務会計システムの導入を予定している。そのため、取り込みデータ形式の変更（PDF データから CSV データへの変更等）や、新旧システムを利用する期間中に、異なる２種類の帳票レイアウトを併用して運用（アップロード）することとなった場合においても、追加費用が発生することの無いようにすること。

（２）PDF 分割機能を有していること

・現行システムから出力される連結された PDF ファイル（数千枚単位）を、ページごとや顧客ごとに自動分割し取り込める機能、または連携アプリを有していること。

（３）振込通知内容について、少なくとも次のとおりとし、本市の都合により取捨選択することが可能であること

①債権者番号（相手方番号）

②債権者名

③振込先口座情報（金融機関名、支店名、種別、口座番号）

④振込日

⑤支払総額

⑥控除金額

⑦振込金額

⑧摘要内容（24 文字以上）

⑨振込元所属

（４）債権者が本市の専用ページから自身の情報についての閲覧及び帳票をダウンロードできること

（５）債権者が過去の振込内容を検索し、閲覧および帳票をダウンロードすることができること

※期間については、直近 12 か月分を表示できる仕様を基本とするが、最終的な決定は本市と協議の上決定する。

（６）帳票発行時、債権者に対してメール等で通知することができること

7　情報セキュリティ及び個人情報保護基本要件

（1）情報セキュリティマネジメントシステム（ISMS）の国際規格「ISO/IEC 27001」の認証を取得していること

（2）個人情報保護マネジメントシステム「プライバシーマーク」の認定を取得していること

（3）データセンターは国内に所在し、データの保存場所も国内であること

（4）サーバー、ネットワーク機器、電源等が冗長化されており、単一障害点でサービスが停止しない構成であること

（5）耐震又は免震構造、自動消火設備、無停電電源装置（UPS）を備えた堅牢なデータセンターで運用されていること

（6）インターネット通信は SSL/TLS（TLS1.2 以上）により暗号化されていること

（7）サーバーへの不正アクセスや情報漏洩の防止、ウイルス対策などが確実に実施されること

（8）プラットフォーム診断及び Web アプリケーション脆弱性診断等を定期的に実施していること

（9）管理者画面へのアクセス元 IP アドレスを制限できる機能を有すること

(10) 債権者側のログインにおいて、セキュリティ強化のための二段階認証等の機能を提供することができること

(11) パスワードの桁数、文字種、有効期限、ロック機能等を管理者が設定できること

(12) 別紙１「静岡市セキュリティポリシー」及び別紙２「個人情報の保護に関する取扱仕様書」を遵守すること

8　サービスレベル及び運用保守要件（SLA 等）

（1）サービス稼働率を 99.9%以上とし、サービス計画停止を除き 24 時間 365 日のサービス提供を行うこと。また、サービス計画停止期間は極力短くすること

（2）計画停止を行う場合は、原則として 30 日前までに通知を行うこと

（3）1 日 1 回以上の頻度で自動バックアップを実施し、遠隔地（または異なる筐体）へ保存すること

（4）バックアップデータは複数世代（4 世代以上等）管理されていること

（5）電話サポート窓口又はメール/Web フォームを開設していること

（6）担当者による導入支援に加え、運用定着後のサポート体制が用意されていること

9　その他

（1）データの流出や流用を防ぐため本契約終了時、本市が受渡したデータ全てを、受託者が適切な方法で削除すること。さらに、データが削除されたことについての証明書等を提出すること。ただし、次年度以降も継続して利用することが見込まれる場合はこの限りではない。

また、本契約終了時に次年度以降の継続利用が見込まれない場合、データの保存方

法等については別途協議し決定するものとする。

（２）受託者は、業務の実施に伴い適用を受ける法令、規程、基準、指針等について、これを遵守しなければならない。

別紙１

静　岡　市

情報セキュリティポリシー

令和８年４月１日

静岡市情報セキュリティ委員会

序　文

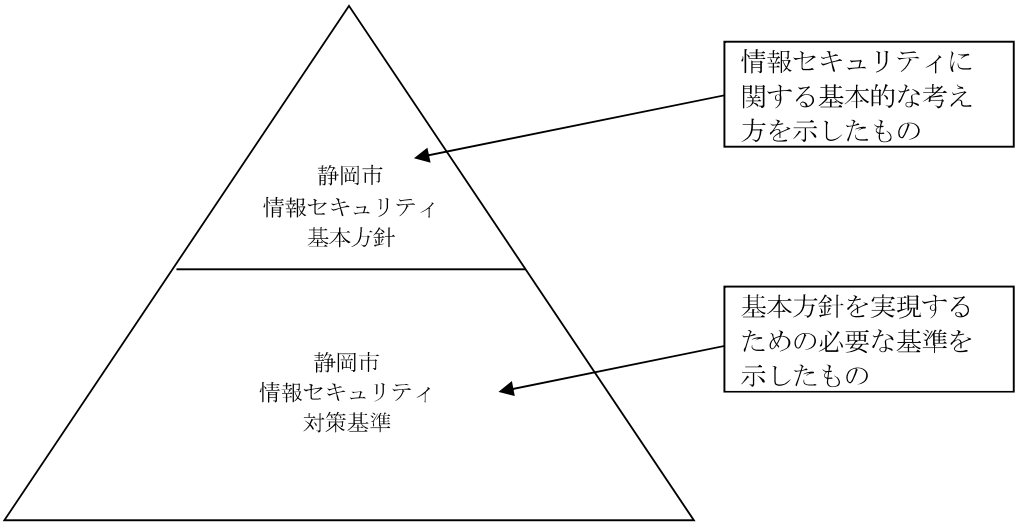
静岡市は、ＩＣＴの高度利用による情報化を推進することにより、電子自治体の実現を目指している。

情報化を推進し、電子自治体を実現するに当たっては、本市の保有する情報を不正なアクセス、情報の漏えい・改ざん等の脅威から防御し、高度な健全性を有した情報システムを構築していかなければならない。

このような状況を踏まえ、静岡市は、保有する情報及び情報システムに関するセキュリティ対策を総合的、体系的かつ具体的に規定した静岡市情報セキュリティポリシーを策定することとした。

静岡市情報セキュリティポリシーについては、本市の全職員がその内容を十分理解した上で、各職場において率先して遵守すべきものであるため、安定的な規範であることが要請される一方、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に柔軟に対応できることも必要とされる。

このようなことから、静岡市情報セキュリティポリシーは、情報セキュリティ対策における基本的な考え方を定める「情報セキュリティ基本方針」、この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定める「情報セキュリティ対策基準」により構成するものとする。



※　具体的な確認項目や手順については、運用の手引きのほか、リスクに関するチェックシート及び危機管理に関するマニュアルに示す。

静　岡　市

情報セキュリティ基本方針

令和８年４月１日

静岡市情報セキュリティ委員会

改　版　履　歴

版　数	作　成　日
第１版	平成16年７月13日
第２版	平成17年４月１日
第３版	平成19年４月１日
第４版	平成26年８月４日
第５版	平成27年４月10日
第６版	平成28年４月１日
第７版	平成29年12月15日
第８版	令和４年４月１日
第９版	令和８年４月１日

1　趣旨

情報セキュリティ基本方針（以下「基本方針」という。）は、静岡市（以下「本市」という。）の情報資産の機密性、完全性及び可用性を維持するために必要な対策に関する基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

2　定義

基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（1）情報

文書（メモ等を含む。）、図画及び写真（これらを撮影したマイクロフィルムを含む。）並びに電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）をいう。

（2）行政情報

行政事務の執行に関する情報をいう。

（3）情報システム

コンピュータ、ソフトウェア、ネットワーク及び周辺機器で構成され、情報の処理を行う仕組みをいう。

（4）情報資産

情報及び情報システムをいう。

（5）電子記録媒体

磁気、光学、半導体その他の原理により電磁的記録を保持することを目的とした媒体をいう。

（6）外部記録媒体

電子記録媒体のうち、情報を保持したまま、容易に取り外しが出来るものをいう。

（7）記録媒体

電子記録媒体及び紙媒体をいう。

（8）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（9）機密性

情報にアクセスすることが認可された者だけがアクセスできることを確実にすることをいう。

(10) 完全性

情報及び処理の方法が正確かつ完全である状態を保護することをいう。

(11) 可用性

許可された利用者が必要なときに情報にアクセスできることを確実にすることをいう。

(12) 情報セキュリティインシデント

情報資産の不正使用、業務妨害行為、データの破壊及びそれらに至るための行為等の情報セキュリティに対する脅威及び脆弱性から発生する障害をいう。

(13) 脅威

自然災害、悪意のある行為等情報資産に被害を与える要因をいう。

(14) 脆弱性

情報セキュリティの弱い部分及び情報セキュリティを弱める環境等の脅威を発生しやすくさせる要因をいう。

3　適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、市長事務部局（地方独立行政法人静岡市立静岡病院を除く）、消防局、上下水道局、教育委員会事務局選挙管理委員会事務局、人事委員会事務局、監査委員事務局、農業委員会事務局及び議会事務局とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③　情報システムの仕様書及びネットワーク図等のシステム関連文書

4　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本市の情報資産に関する情報セキュリティ対策の最上位に位置するものである。

5　職員等の責務

職員、非常勤職員及び会計年度任用職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守しなければならない。

6　情報セキュリティ対策

情報資産を脅威から防御し、又は情報資産の脆弱性を解消するため、次の情報セキュリティ対策を講ずるものとする。

（1）情報セキュリティ組織運営対策

対策基準の適用範囲における情報セキュリティの推進及び向上のための組織体制を確立する。

（2）情報資産管理

情報資産の作成及び複製、入手、保管、利用、送信、持出し並びに消去及び廃棄するための取扱いを明確にする。

（3）人的セキュリティ

情報セキュリティの確保を図るため、職員等が服務上遵守すべき事項を明確にする。

（4）物理的セキュリティ

サーバ等のハードウェアの設置環境並びに情報を取り扱う機器及び設備等について、情報セキュリティの確保に必要な対策を講ずる。

（5）IT資産管理

業務で利用するハードウェア、ソフトウェア及びライセンス等のIT資産の適正な運用等について、情報セキュリティの確保及びライセンスコンプライアンスの向上に必要な対策を講ずる。

（6）技術的セキュリティ

情報システム等のログの管理、バックアップ等について、必要となる技術的なセキュリティ対策を講ずる。

（7）情報システム開発、導入、保守等

情報システムに係る審査、情報システムの調達、開発、導入、保守等について、情報セキュリティの確保に必要な対策を講ずる。

（8）外部サービス利用

事務事業を外部委託事業者又は指定管理者に実施させる場合若しくは約款による外部サービス、ソーシャルメディア又はクラウドサービス等を利用する場合において、情報セキュリティの確保のために必要な対策を講ずる。

（9）情報セキュリティインシデント対応

情報セキュリティインシデントが発生した場合において、迅速かつ適切な対応を行うための手順等を明確にする。

(10) 情報セキュリティ対策評価

情報資産のリスク管理体制をより適切かつ効果的にするために行う監査、点検及び調査を明確にする。

(11) 情報セキュリティポリシー運用

静岡市情報セキュリティポリシーの遵守違反が発生したときの調査、違反行為者等に対する指示、情報セキュリティポリシーの例外措置等について、必要な対策を講ずるものとする。

7　情報セキュリティ対策基準の策定

５の情報セキュリティ対策において規定された事項について、職員等が遵守すべき範囲を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定する。

8　情報セキュリティポリシーの公開

情報セキュリティポリシーには、本市のセキュリティ上の脆弱性に関する内容が含まれるため、情報セキュリティの確保の観点から、基本方針及び対策基準の概要についてのみ公開するものとし、対策基準の全文については業務上必要がある場合に限り公開するものとする。

9　保健福祉長寿局清水病院及び学校の情報セキュリティ対策基準の策定等

保健福祉長寿局清水病院及び学校は、この基本方針に準拠した独自の情報セキュリティ対策基準を策定し、及び運用する。

別紙２（第●条関係）

個人情報の保護に関する取扱仕様書

１　個人情報保護の基本原則

乙は、この契約に基づく業務（以下「業務」という。）の実施に当たり、個人情報（個人に関する情報であって、特定の個人を識別できるものをいう。以下同じ。）について、その保護の重要性を認識し、個人の権利利益を侵害することのないよう、適正に取り扱わなければならない。

２　個人情報の漏えい等の禁止

乙は、業務に関して、知り得た個人情報を他人に漏らしてはならない。この業務が終了し、又は契約が解除された後においても同様とする。

３　使用者への周知

乙は、その使用する者に対し、在職中及び退職後において、業務に関して知り得た個人情報を他人に知らせ、又は契約の目的以外に利用してはならないこと等の個人情報の保護の徹底に関する事項を周知しなければならない。

４　適正な管理

乙は、業務に係る個人情報の漏えい、滅失、改ざん又は毀損の防止を図るため、管理責任者を選任し、個人情報の適切な管理を行わせる等個人情報の適正な管理について必要な措置を講じなければならない。

５　収集の制限

乙は、業務において個人情報を収集するときは、当該業務を実施するために必要な範囲内で、本人から直接収集しなければならない。

６　利用及び提供の制限

乙は、甲の指示又は承諾があるときを除き、業務に係る個人情報を当該業務の目的以外に利用し、又は提供してはならない。この業務が終了し、又は契約が解除された後においても同様とする。

７　複写及び複製の禁止

乙は、甲の指示又は承諾があるときを除き、業務の実施に当たり甲から提供された個人情報が記録された資料等を複写し、又は複製してはならない。

８　資料等の返還

乙は、業務の実施に当たり甲から提供され、又は乙が収集し、若しくは作成した個人情報が記録された資料等を、業務の終了後直ちに甲に返還し、又は引き渡すものとする。ただし、甲が別に指示したときは、その指示に従うものとする。

９　再委託等における個人情報の取扱い

乙は、契約書第●条第１項ただし書の規定により甲の承認を受けて業務を再委託する場合は、再委託を受けた者との間で締結する契約書等に、この契約書の個人情報の保護に関する規定を準用する旨を明記しなければならない。この場合において、乙は、当該契約書等の締結後、速やかにその写しを甲に提出するものとする。

10　事故発生時における報告

乙は、業務の実施において、この仕様書に違反する事態が生じ、又は生ずるおそれがあることを知ったときは、直ちに甲に報告し、甲の指示に従うものとする。業務が終了し、又は契約が解除された後においても同様とする。