乙第２７号証

この資料には、番号制度に係る関係法令に規定された
秘密保持義務を負うべき情報が含まれています。

自治体中間サーバー・プラットフォーム

ASPサービス仕様書

第02.10版

平成29年2月24日

地方公共団体情報システム機構

変更履歴

項	版数	発行日	変更箇所（頁）	変更区分	変更内容
1	01.00	平成27年7月17日	-	-	新規作成
2	02.00	平成28年3月25日	2	更新	「図 1.1 1 ドキュメント体系」を更新
3			7	追加	「表 1.1-1団体業務データ及びVPN装置の役割分担」※2の記載を追加
4			11	更新	「表 3.3 1 サービス提供時間」におけるサービス提供時間を更新
5			12	更新	「図 3.3 1 通常運用スケジュール」における運用スケジュールを更新
6			16	更新	「5.5 災害対策」の記載内容を更新
7			18	追加	「6.2 自治体中間サーバー設定用パラメータ変更」を追加
8			19	更新	「6.4 市町村合併対応等」の目次タイトルを更新 市町村合併対応等の想定パターンを更新
9			20	更新	「7.5 情報保有機関の連絡体制変更時の機構への通知について」の記載内容を更新
10			21	更新	「7.8本サービスの提供に係る相互の連絡調整について」の記載内容を更新
11	02.10	平成29年2月24日	1	更新	「1.1.1 本書の目的」の記載内容を更新
12			2	更新	「図 1.1 1 ドキュメント体系」を更新
13			9	更新	「表 3.1-1 自治体中間サーバー・ソフトウェアの機能概要」の記載内容を更新
14			18	削除	「6.2 自治体中間サーバー設定用パラメータ変更」を削除

目次

1 はじめに

地方公共団体情報システム機構(以下「機構」という。)は、総合行政ネットワーク(以下「LGWAN」という。)におけるASPサービスとして自治体中間サーバー・プラットフォーム ASPサービス(以下「本サービス」という。)の提供を行う。

本サービスは、地方公共団体情報システム機構業務方法書(地方公共団体情報システム機構法(平成25年法律第29号。)第23条第1項の規定に基づき、機構の業務方法について基本的事項を定めるもの。)第7条第2号に定める「中間サーバー・プラットフォームに関するシステムの整備及び運営」を機構が行うものである。

本サービスでは、地方公共団体の経費削減、統一的なセキュリティの強化及び確保、相互バックアップによる災害時の業務継続性強化、運用の安定性の確保等の観点から、自治体中間サーバーの共同化・集約化を図ることとしている。

1.1 本書の目的と位置づけ

1.1.1 本書の目的

本書は、機構が情報保有機関に対して提供する本サービスの内容及び留意事項等について記しているドキュメントであり、提供されるサービスについて情報保有機関による理解を深める事を目的としている。

本書は、番号法附則第1条第5号に掲げる施行期日以降に行われる地方公共団体による情報連携の開始以降に提供されるサービスの内容について記している。本サービス内容については、平成26年12月19日地情機第1157号「中間サーバー・プラットフォームASPサービスの利用申込みについて(通知)」に添付した別添「自治体中間サーバー・プラットフォームASPサービス仕様書」により周知しているところであるが、本書においては現在までに行われた設計結果等を踏まえ、より具体的な説明をしている。第02.10版では、第02.00版配付後に追加された自治体中間サーバー・ソフトウェア機能の追記及び、自治体中間サーバー設定用パラメータ変更の項目を削除している。

なお機構は、自治体中間サーバー・プラットフォームの構築を平成27年度中に行い、平成28年4月からサービス提供を開始しているが、平成28年4月以降から番号法附則第1条第5号に掲げる施行期日までの間の自治体中間サーバー利用時間等、本書と相違する部分については、別途事務連絡等で通知する。なお、本書では「番号法附則第1条第5号に掲げる施行期日」は地方公共団体の情報連携開始日を意図したものとして表記している。

1.1.2 本書の位置づけ

情報保有機関のシステム管理者及び業務担当者は、本サービスを利用するために、ASPサービス利用マニュアル及び自治体中間サーバー・ソフトウェアのマニュアル類等のドキュメントを参照して、サービスを利用することになる。

情報保有機関が利用するドキュメントの体系と本書の位置づけを以下に示す。

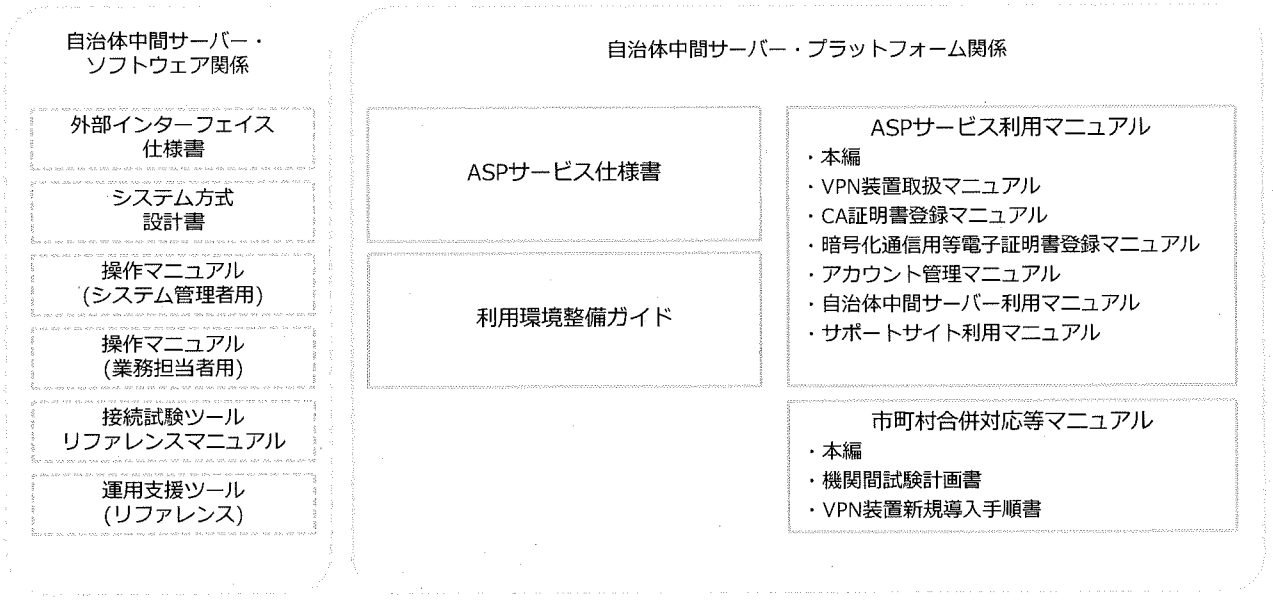

図 1.1-1 ドキュメント体系

1.2 用語の定義

本書で使用する用語の定義を以下に示す。

表 1.2-1用語の定義

項番	用語	説明
1	自治体中間サーバー	「地方公共団体における番号制度の導入ガイドライン第2 章第3 節情報連携のための中間サーバーの構築に係るガイドライン」において、情報連携の対象となる特定個人情報を保有・管理し、情報提供ネットワークシステム(インターフェイスシステム)と既存システムとの情報の授受について、仲介を行う役割を担うものを指す。
2	自治体中間サーバー・プラットフォーム	自治体中間サーバーを構成するために集約設置された機器等を指す。東西2か所のDCに集約し、相互バックアップを実現している。また、自治体中間サーバーの利用に関係するサポートサイト、CA、ヘルプデスク、運用監視を含む。
3	自治体中間サーバー・ソフトウェア	法令(政省令、告示、条例等を含む。)等に基づいて情報保有機関において業務上行われる特定個人情報の照会及び提供それに付随する業務を行うアプリケーション(プログラム)群を指す。ハードウェアを含まない。
4	自治体中間サーバー接続端末	業務担当者が、自治体中間サーバーの機能を使うために接続する端末を指す。
5	情報提供ネットワークシステム	特定個人情報の提供について管理するための電子情報処理組織で総理大臣が設置、管理するものを指す。(番号法第2条第14項)
6	既存システム	各情報保有機関において個人情報を保有・管理するシステム(基幹系システム、システム共通基盤等)を指す。
7	団体内統合宛名システム	既存システムのうち、「地方公共団体における番号制度の導入ガイドライン第2 章第4 節 団体内統合宛名システム等の整備に係るガイドライン」における地方公共団体で業務横断的に宛名、住所、所在地等の情報の保持・管理を行う団体内統合宛名システムを指す。特に明示が無い限り、団体内統合利用番号連携サーバーも含む。
8	住基システム	市区町村で住民票に記載される事項を記録し、住民基本台帳法に基づく業務を行うシステムを指す。
9	認証局(CA)	自治体中間サーバーと自治体中間サーバー接続端末とのSSL通信を実現するためのデジタル証明書発行等を行うルート認証局を指す。
10	自治体中間サーバー用CA証明書	自治体中間サーバー・プラットフォームに構築する認証局(CA)の自己署名証明書を指す。 自治体中間サーバーのサーバ証明書が信頼された認証機関から発行されたことを確認するために用いる。
11	自治体中間サーバー設定用パラメータ	自治体中間サーバーのユーザ登録に関する設定、住基システム又は団体内統合宛名システムと自治体中間サーバーとのシステム間連携に関する設定等、情報保有機関で決定する自治体中間サーバーの構築に必要なパラメータの総称。

項番	用語	説明
12	情報保有機関	番号法別表第二の第1欄に規定される情報照会者及び第3欄に規定される情報提供者を指す。自治体中間サーバー・プラットフォームでは、「都道府県知事」、「市町村長(特別区の区長を含む)」、「都道府県教育委員会」、「市町村教育委員会」及び自治体中間サーバーを利用し情報連携を行う「一部事務組合」、「広域連合(後期高齢者医療広域連合を除く)」を指す。
13	一部事務組合	地方自治法に基づき、普通地方公共団体(都道府県、市町村)や特別区が、事務の一部を共同で処理するために設ける特別地方公共団体。
14	広域連合	地方自治法に基づき、普通地方公共団体(都道府県、市町村)や特別区が、広域にわたり処理することが適当であると認める事務に関し、その事務の一部を広域にわたり総合的かつ計画的に処理するために設ける特別地方公共団体。
15	サポートサイト	自治体中間サーバーに関する各種情報提供、情報保有機関からの各種連絡及び問い合わせ等を受け付けるWebシステムを指す。
16	ヘルプデスク	情報保有機関からの自治体中間サーバーに関する各種問合せを電話、FAX及びメールで受け付ける。また、回答作成のため自治体中間サーバー・プラットフォーム構築・運用事業者内及び当機構をはじめとした各機関とのやり取りを担う者を指す。
17	業務担当者	自治体中間サーバーを利用して業務を行う者の総称。符号に関わる業務、副本に関わる業務、情報照会業務及び情報提供業務等を行う。
18	システム管理者	自治体中間サーバーにおけるシステム利用の管理者を指す。ユーザ管理、権限管理等の管理業務を行う。
19	システム運用者	自治体中間サーバーの運用、監視を行う者を指す。
20	特定個人情報	自治体中間サーバーに副本として保存する個人情報を指す。自治体中間サーバー上には個人を識別可能な情報を保存しないため、個人番号は含まない。
21	符号取得業務	番号法附則第2条に規定する「法律の実施のために必要な準備行為」として実施する、機関別符号(番号法第2条第8項に規定する「個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号」を指す。)の払出しに係る業務を指す。
22	情報照会・提供等業務	情報提供ネットワークシステムから配付される照会許可用照合リスト等の各種マスタファイルの管理業務や情報提供等記録開示システムとの連携に係る業務、情報提供等監視・監督業務を含めた情報照会・提供に係る業務を示す。
23	団体業務データ	自治体中間サーバーにおいて自治体中間サーバー・ソフトウェアを利用し各情報保有機関が主体となり登録・維持管理するデータを指す。
24	生体認証	人間の体の特徴を利用する認証方法。顔、指紋、静脈などを利用して本人確認を行う認証方式を指す。
25	負荷分散	外部から送られてくるデータや処理要求を、同等に機能する複数の装置に振り分けて一台あたりの負荷を抑えることを指す。

項番	用語	説明
26	冗長化	システムや通信回線の信頼性を高めるために、同じように機能する複数のシステムを用意すること。二重化、多重化ともいう。
27	DC (Data Center)	データセンターの略称。東西にそれぞれ1拠点存在する。
28	LGWAN-ASP	LGWANを介して、利用者である地方公共団体の職員に提供するASPサービスのこと。
29	FW (Firewall)	特定のネットワークとその外部との通信を制御し、内部のコンピュータネットワークの安全を維持することを目的としたソフトウェア(あるいはそのソフトウェアを搭載したハードウェア)を指す。
30	LB (Load Balancer)	外部から送られてくるデータや処理要求を、同等に機能する複数の装置に分散させる装置を指す。
31	VPN (Virtual Private Network)	広域網や公衆回線等に接続している拠点間を認証技術や暗号化を用いて保護し、専用線であるかのような接続を可能とする技術を指す。
32	IPS (Intrusion Prevention System)	ネットワークの境界に設置し、サーバやネットワークへの不正侵入を阻止するシステムを指す。
33	サンドボックス(Sandbox)	保護された領域内でプログラムを動作させることで、その外へ悪影響が及ぶのを防止するセキュリティモデルを指す。
34	SSL (Secure Sockets Layer)	インターネットなどのTCP/IPネットワークでデータを保護するため、暗号化して送受信するプロトコルのうちの一つを指す。
35	DoS攻撃 (Denial of Services attack)	通信ネットワークを通じてコンピュータや通信機器などに行われる攻撃手法の一つで、大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むこと。サービス拒否攻撃ともいう。
36	フィッシング (Phishing)	金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、そのリンクから偽サイト（フィッシングサイト）に誘導し、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為を指す。
37	標的型攻撃	特定の個人や組織、情報を狙ったサイバー攻撃のこと。企業や国家の機密情報の詐取を目的に行われることが多い。

4 セキュリティ対策

機構は、本サービスで扱う特定個人情報を不正アクセスや侵入等の脅威から守るために、以下の対策を実施する。

4.1 利用者の役割ごとのアクセス権限

機構は、自治体中間サーバー・プラットフォームのシステム運用者の役割ごとのアクセス権限を設定する。なお、本サービスを利用する情報保有機関職員の役割ごとのアクセス権限は自治体中間サーバー・ソフトウェアの職員認証・権限管理機能を用いて情報保有機関にて設定を行う。

自治体中間サーバー・プラットフォームのシステム運用者のアクセス権限を以下に示す。

表 4.1-1自治体中間サーバー・プラットフォームのシステム運用者のアクセス権限

項目	概要
アクセス権限	自治体中間サーバー・プラットフォームのシステム運用者に対して、職責や担当業務に応じた利用可能な機能やアクセス範囲を必要最小限に制限することで適切なアクセス権による運用を実施する。
	自治体中間サーバー・プラットフォームのシステム運用者に対して、団体業務データへのアクセス権を付与しないことで、特定個人情報に結びつく情報の漏えいを防止する。
生体認証	運用監視拠点の運用端末は、生体認証による利用制限を行い、不正な端末利用を防止する。
パスワード認証	自治体中間サーバー・プラットフォームのOSの利用にはログオン・パスワードによる認証を行う。ログオン・パスワードは規定の複雑さを必要とし、文字数下限の設定、認証試行回数の制限及び履歴管理による同一パスワードの制限を実施する。
権限分離	自治体中間サーバー・プラットフォームのシステム運用者に対して、単独で実施可能な権限を付与せず、権限分離による対策を実施する。それによりシステム運用者による不正を防止する。

4.2 不正アクセスの検知、証跡ログの取得

機構は、不正アクセスや過剰なアクセスによるシステムダウン等を防止するための対策及び検知を実施する。また、団体業務データへのアクセス等の証跡ログを記録し、不正アクセス監視及び改ざん検知を実施する。不正アクセスの検知及び証跡ログの取得を以下に示す。

表 4.2-1 不正アクセスの検知及び証跡ログの取得

項目	概要
侵入防止	FWにより情報保有機関と本サービスの通信を制御し、不正な通信を遮断する。
標的型攻撃対策	LGWANから不正プログラムを送り込む脅威及び自治体中間サーバー・プラットフォームから不正プログラムを送り込む脅威に対して、サンドボックスによる解析を実施する。

項目	概要
	IPSで通信中に含まれる不正アクセス(Dos攻撃等)に関するパケットを遮断する。
監視・追跡	団体業務データへのアクセスを証跡として記録する。
	不正アクセス監視及び改ざん検知を実施する。
	データセンターや運用監視拠点等の監視カメラの映像及び入退室の記録を証跡として記録する。

4.3 サーバ認証等によるなりすまし防止

機構は、サーバ認証等によるなりすまし防止を実施する。なりすまし防止を以下に示す。

表 4.3-1 サーバ認証等によるなりすまし防止

項目	概要
なりすまし防止	証明書を使ったサーバ認証によりフィッシング等の偽装サイトへの接続を防止する。

4.4 マルウェア対策

機構は、ウィルスやワーム等の悪意のあるソフトウェアによる脅威に備えるためマルウェア対策を実施する。マルウェア対策を以下に示す。

表 4.4-1 マルウェア対策

項目	概要
マルウェア対策	マルウェア(ウィルス、ワーム、ボット等)による脅威に備えるため、マルウェア対策機能を導入する。また、感染経路の制限による感染予防及びウィルス対策機能による感染の予防・検知・通知・適切な除去を実施する。

4.5 暗号化によるデータ保護

機構は、通信、データベース及びバックアップデータを暗号化することによりデータ保護を実施する。暗号化によるデータ保護を以下に示す。

表 4.5-1 暗号化によるデータ保護

項目	概要
通信の暗号化	VPN装置で情報保有機関と本サービスの通信を情報保有機関ごとに分離するとともに、通信を暗号化することでデータ保護を行う。
	東西データセンター拠点間及び運用監視拠点と東西データセンター拠点間の通信を暗号化することでデータ保護を行う。

項目	概要
データベースの暗号化	特定個人情報を保管するデータベースの情報は、情報保有機関ごとに異なる暗号化を実施しデータを保護する。
バックアップデータの暗号化	特定個人情報を含む業務データのバックアップデータは暗号化を実施しデータを保護する。

4.6 物理対策

機構は、運用監視拠点及び東西データセンター拠点の入退室時における不正な侵入を防止する対策を実施する。また、東西データセンター拠点及び運用監視拠点の各拠点間通信は、専用回線を用いて閉域性を確保し、第三者によるアクセスを遮断する。物理対策を以下に示す。

表 4.6-1 物理対策

項目	概要
入退室管理	運用監視拠点の入退室時は、生体認証により不正な侵入を防止する。
	データセンターの入退室時の2要素認証及び監視カメラによる24時間常時監視を行うことで、不正な侵入を防止する。
拠点間通信	東西データセンター拠点間及び運用監視拠点と東西データセンター拠点間の通信回線は、専用回線を用いて閉域性を確保し、第三者によるアクセスを遮断する。

4.7 情報セキュリティ監査

機構は、本サービスにおける情報セキュリティを維持・管理する仕組みが適切に整備・運用されているかを点検・評価するために、外部によるセキュリティ監査実施者(以下、監査実施者という。)による情報セキュリティ監査を年1回実施する。

また、監査の結果に基づき情報セキュリティ上の問題点の指摘と改善の方向性の提言をまとめ、必要な改善を行う。

実施する情報セキュリティ監査を以下に示す。

表 4.7-1 情報セキュリティ監査

項目	概要
監査対象	自治体中間サーバー・プラットフォーム及び運用業務を対象とする。
監査方法	機構は、年度ごとに外部の監査実施者による監査を受ける。
監査結果の公開	機構は、監査結果を適切な範囲で情報保有機関へ公開する。