

函館市住民基本台帳ネットワークシステムセキュリティ運用要領

(目的)

第1条 この要領は、「函館市電子計算機処理に係るデータ保護管理規程」(以下「規程」という。)に基づき、住民基本台帳ネットワークシステム(以下「住基ネット」という。)のセキュリティ運用について、函館市電子計算機管理運営要領に定めるもののほか、必要な事項を定めるものとする。

(セキュリティ統括責任者)

第2条 住基ネットのセキュリティ対策を総合的に実施するため、セキュリティ統括責任者を置き、総務部長をもって充てる。

(システム管理者)

第3条 住基ネットの適切な管理を行うため、システム管理者を置き、総務部情報システム課長をもって充てる。

(セキュリティ責任者)

第4条 住基ネットを利用する課または支所(以下「住基ネット業務所管課」という。)においてセキュリティ対策を実施するため、セキュリティ責任者を置き、別表1に掲げる者をもって充てる。

(セキュリティ会議)

第5条 セキュリティ統括責任者は、セキュリティ会議を年1回以上招集するとともに、議長を務める。なお、会議の実施については、回付方式の協議によって代えることができることとする。

2 セキュリティ会議は、セキュリティ統括責任者のほか、次に掲げる者をもって組織する。

- (1) システム管理者
- (2) セキュリティ責任者
- (3) その他セキュリティ統括責任者が必要と認めて指名した者

3 セキュリティ会議は、次に掲げる事項を審議する。

- (1) 住基ネットのセキュリティ対策の決定および見直し
- (2) 前号のセキュリティ対策の遵守状況の確認

(3) 監査の実施

(4) 教育・研修の実施

4 議長は、前項のうち重要と認められる事項を審議するときは、函館市個人情報保護運営審議会の意見を聴くものとする。

5 議長は、必要と認められるときは、関係職員の出席を求め、その意見または説明を聴くことができる。

6 セキュリティ会議の庶務は、総務部情報システム課において処理する。

(関係部署の長に対する指示等)

第6条 セキュリティ統括責任者は、セキュリティ会議の結果を踏まえ、関係部署の長に対し指示し、または必要な措置を要請することができる。

(アクセス管理)

第7条 次に掲げる住基ネットの構成機器について、業務アプリケーションに対するアクセス管理を行う。

(1) コミュニケーションサーバ（以下「CS」）

(2) 住基ネットおよび公的個人認証システム受付窓口機能を有する端末（以下「統合端末」）

2 前項のアクセス管理は、静脈等の情報に不可逆演算を施して登録された情報（以下「照合情報」）と認証時に読み取られる情報を照合することにより認証する方法により操作者の正当な権限を確認することおよび操作履歴を記録することにより行うものとする。

(アクセス管理責任者)

第8条 前条のアクセス管理を実施するため、アクセス管理責任者を置き、総務部情報システム課長をもって充てる。

2 アクセス管理責任者は、操作者を識別するためのID（以下「照合ID」）、照合情報および操作権限を識別するためのID（以下「操作者ID」）に関し、次に掲げる事項を実施する。

(1) 照合IDおよび操作者IDの管理方法を定めること

(2) 照合情報の登録および削除の管理方法を定めること

- (3) 操作者 I D の種類ごとの操作者について、住基ネット業務所管課の長と協議して定めること
- (4) 照合 I D および操作者 I D の管理簿を作成すること
(照合 I D, 照合情報および操作者 I D の管理方法)

第 9 条 前条第 2 項の管理方法について、次のとおり定める。

- (1) アクセス管理責任者は、操作者に対し照合 I D を付与し、その操作者が適正に照合情報を登録するように管理する。その上で、照合 I D に対して業務に必要な操作者 I D を付与する。
- (2) アクセス管理責任者は、操作者の退職、人事異動等に際しては、照合情報を削除することにより、照合 I D を無効化する。
- (3) アクセス管理責任者は、照合 I D を付与する際、その有効期限を、付与した日が属する年度の翌年度 6 月 3 0 日までに設定する。
- (4) 操作者は、照合 I D および操作者 I D を他者に利用させない。また、目的外の利用等を行わない。
- (5) アクセス管理責任者は、適正に照合 I D および操作者 I D が利用されているか検査を行う。
- (6) アクセス管理責任者が照合 I D および操作者 I D の利用に関する検査を行った場合には、操作者は協力する義務を負う。

2 操作者 I D については、別表 2 に示すように操作者 I D の種別ごとに、操作できる業務が限定されているため、セキュリティ責任者は同表を基に、住基ネットを操作する者の業務に応じ、アクセス管理責任者あて各種申請書により、操作者に必要となる操作権限の申請等を行う。

- (1) 照合 I D を新規に付与する場合、セキュリティ責任者は必要となる操作権限を明記のうえ、アクセス管理責任者あてに、「住基ネットワーク登録申請書」(様式第 1 号)を提出する。アクセス管理責任者は、同申請書を基に、操作者に操作者の照合情報と紐付けた新規の照合 I D および操作者 I D を付与する。
- (2) 操作者の退職および人事異動等に際し、操作者のすべての操作権限が不要となった場合、セキュリティ責任者は、付与されている

操作権限を全て明記のうえ、アクセス管理責任者あてに「住基ネットワーク操作者削除申請書」（様式第2号）提出する。アクセス管理責任者は、同申請書を基に、操作権限を返却することで照合情報を削除し、照合IDを無効化する。

(3) 操作者の業務内容が変更となった場合、セキュリティ責任者は変更前および変更後の操作権限を明記のうえ、アクセス管理責任者あてに、「住基ネットワーク操作権限変更申請書」（様式第3号）を提出する。アクセス管理責任者は、同申請書を基に、操作者に必要な操作者IDを付与する。

(4) 照合IDは前項により設定された期間のみ有効となるため、セキュリティ責任者は、有効期限前までに、付与されている操作権限を全て明記のうえ、アクセス管理責任者あてに「住基ネットワーク操作者有効期限更新申請書」（様式第4号）を提出する。アクセス管理責任者は、同申請書を基に、操作者の照合IDの有効期限を、翌年度6月30日までに更新する。

3 アクセス管理責任者は、照合IDおよび操作者IDについて、新規登録、削除、変更および有効期限更新があった場合、「照合IDおよび操作者ID管理簿」（様式第5号）により、操作者の全てのIDを管理する。

（照合情報認証が困難な操作者に対応した補助機能）

第10条 アクセス管理責任者は、操作者において怪我などで照合情報認証に適さない身体状況などが発生した場合など、特に必要と認める場合に限り、照合情報の代わりに認証するための補助機能（以下「操作者照合暗証番号」）を使用することを認める。

2 この操作者照合暗証番号を使用する場合、操作者照合暗証番号が漏えいしないように管理方法を定め、厳重な管理を行わなければならない。

（操作者照合暗証番号の管理方法）

第11条 前条第2項の操作者照合暗証番号の管理方法について、次のとおり定める。

- (1) アクセス管理責任者は、操作者照合暗証番号の有効期限を必要な期間のみに設定し、やむを得ず長期で使用する場合は、適切な周期で定期的に操作者照合暗証番号を再発行する。
- (2) 操作者は、操作者照合暗証番号について、他者への漏えいを防止する手段を講ずるとともに、他者が知り得る状態に置いてはならない。
- (3) 操作者は、操作者照合暗証番号が他者に漏えいした場合は、アクセス管理責任者に報告する。
- (4) アクセス管理責任者は、操作者照合暗証番号が漏えいした場合は、速やかに操作者照合暗証番号を再発行する。

(操作者の責務)

第12条 操作者は、照合ID、照合情報および操作者IDの管理方法を遵守しなければならない。

(操作履歴の記録および管理方法)

第13条 統合端末およびCSにかかる操作履歴について、次のとおり定める。

- (1) アクセス管理責任者は、操作履歴について、7年前までさかのぼって解析できるよう保管するものとする。
- (2) アクセス管理責任者は、ログオンの履歴が記録されるようにシステムを設定するとともに、定期的または必要に応じてその履歴および操作履歴を確認し、不正なアクセスがないか検査する。

ア 前項にかかる検査の観点は、下記の有無とする。

- (a) 業務時間外の操作履歴およびログイン履歴
 - (b) 休暇等を取得しており、不在となっている職員の操作履歴
 - (c) 存在していない端末IDおよび操作者IDの操作履歴
 - (d) 通常と比較して多い、本人確認情報の検索
 - (e) アクセスの失敗
 - (f) 業務アプリケーションの機能エラー
- (3) 前号により、不正なアクセスの可能性のある履歴を発見した場合は、別に定める函館市住民基本台帳ネットワークシステム緊急時

対応計画（以下、「緊急時対応計画」という。）に従い対応する。

（オペレーティングシステムの管理）

第14条 アクセス管理責任者は、第7条のアクセス管理を実施するほか、住基ネットに係る構成機器のオペレーティングシステムについて、必要なセキュリティ対策を実施するものとする。

2 アクセス管理責任者は、前項にかかるオペレーティングシステムのセキュリティ対策状況について、毎年度1回点検することとし、その記録を「年次点検簿」（別表3）に記録すること。

（オペレーティングシステムの管理方法）

第15条 前条のオペレーティングシステムの管理について、CS、電気通信関係装置等のオペレーティングシステムにおけるユーザIDの管理方法を、次のとおり定める。

(1) アクセス管理責任者は、ユーザIDと操作者との対応づけを行い、「オペレーティングシステム操作者名簿」（様式6）によってすべてのユーザIDを管理する。

(2) アクセス管理責任者は、ユーザIDに付与する権限を業務上必要最低限のものとする。

(3) アクセス管理責任者は、操作者が業務に利用するユーザIDについて、業務以外の操作および設定変更を行うことができないよう制限する。

(4) アクセス管理責任者は、ユーザIDおよびその権限について定期的または必要に応じて見直しを行い、不要なユーザIDについては速やかに削除する。

(5) 前号の見直しにかかるユーザIDおよびその権限の管理状況について、毎年度点検することとし、その結果を前条に定める年次点検簿に記録すること。

2 前条のオペレーティングシステムの管理について、CS、電気通信関係装置等のオペレーティングシステムにおけるパスワードの管理方法を、次のとおり定める。

(1) アクセス管理責任者は、パスワードの最低桁数等の制限を設ける。

- (2) アクセス管理責任者は、業務に利用する同一のユーザIDにおいてパスワードを複数回間違えた場合には、ロックアウト（無効）になるよう設定する。
- (3) アクセス管理責任者は、初期設定されているパスワードを、速やかに変更する。
- (4) 操作者は、パスワードについて、権限を与えられたもの以外への漏えいを防止する手段を講ずるとともに、第三者が知り得る状態に置いてはならない。
- (5) 操作者は、パスワードに規則性のある番号または容易に推測可能なものを用いない。
- (6) 操作者は、パスワードを必要に応じて更新する。

3 前条のオペレーティングシステムの管理について、CS、電気通信関係装置等のオペレーティングシステムにおける履歴の確認方法を、次のとおり定める。

- (1) アクセス管理責任者は、定期的または必要に応じてイベントログ等の履歴を確認し、適切に運用されているか検査する。
- (2) アクセス管理責任者は、ログオンの履歴が記録されるようにシステムを設定し、定期的または必要に応じてその履歴を確認し、不正アクセスがないか検査する。
- (3) 本項第1号および第2号の検査について、その検査方法は第13条第1項第2号のとおりとする。

(情報資産の管理責任者)

第16条 住基ネットの情報資産（住基ネットに係る全ての情報ならびにソフトウェア、ハードウェア、ネットワークおよび磁気ディスクをいう。以下同じ。）について、管理責任者を置く。

2 前項の情報資産のうち、本人確認情報、当該本人確認情報が記載されたCSに係る帳票および住民基本台帳カードならびに個人番号カードの管理責任者は、第4条に定めるセキュリティ責任者とし、これら以外の情報資産の管理責任者（以下「情報資産管理責任者」という。）は、総務部情報システム課長をもって充てる。

(本人確認情報等に係るセキュリティ責任者の業務)

第17条 セキュリティ責任者は、本人確認情報を取り扱うことができる者を指定するとともに、当該本人確認情報の漏えい、滅失およびき損の防止その他当該本人確認情報の適切な管理のための必要な措置を講じなければならない。

2 セキュリティ責任者は、本人確認情報の記録されたCSに係る帳票および住民基本台帳カードの管理方法を定めるものとする。

(情報資産管理責任者の業務)

第18条 情報資産管理責任者は、所管する情報資産の管理方法(操作者の指定を含む。)を定めるものとする。

2 情報資産管理責任者は、前項にかかる情報資産の管理状況について、毎年度1回点検することとし、その記録を第14条に定める年次点検簿に記録すること。

3 情報資産管理責任者は、住基ネット業務所管課の長と協議して、住基ネットのオペレーション計画を定めるものとする。

(特定個人情報等の管理)

第19条 第16条第1項に定める住基ネットの情報資産の管理責任者は、特定個人情報を取り扱うことができる者を指定するとともに、当該特定個人情報の漏えい、滅失およびき損の防止その他当該特定個人情報の適切な管理のための必要な措置を講じなければならない。

2 第16条第1項に定める住基ネットの情報資産の管理責任者は、特定個人情報の記録されたCSに係る帳票および個人番号カードの管理方法を定めるものとする。

(住基ネット緊急時の対応)

第20条 住基ネットにおける緊急時については、緊急時対応計画に従い対応するものとする。

附 則

この要領は、平成14年8月5日から施行する。

附 則

この要領は，平成 15 年 8 月 25 日から施行する。

附 則

この要領は，平成 16 年 12 月 1 日から施行する。

附 則

この要領は，平成 21 年 4 月 1 日から施行する。

附 則

1 この要領は，平成 26 年 4 月 1 日から施行する。

2 平成 26 年 5 月 31 日までの間において，操作者用 I C カードおよびパスワードを継続して使用する必要がある場合には，なお従前の例によることとする。

附 則

この要領は，平成 28 年 1 月 1 日から施行する。

附 則

この要領は，平成 29 年 4 月 1 日から施行する。

附 則

この要領は，平成 29 年 12 月 1 日から施行する。

附 則

この要領は，令和元年 7 月 22 日から施行する。

附 則

この要領は，令和 3 年 4 月 1 日から施行する。

附 則

この要領は，令和 4 年 3 月 10 日から施行する。

附 則

この要領は，令和 4 年 6 月 15 日から施行する。

附 則

この要領は，令和 4 年 11 月 1 日から施行する。

附 則

この要領は，令和 5 年 9 月 16 日から施行する。

附 則

この要領は，令和 5 年 11 月 8 日から施行する。

附 則

この要領は，令和 6 年 4 月 2 2 日から施行する。

様式第 6 号（第 1 5 条関係）

オペレーションシステム操作者名簿

所属	氏名	操作権限	名簿登録日	名簿登録削除日

(例)

情報システム課	○○ ○○○	ファイアウォール	yyyy.mm.dd	yyyy.mm.dd
---------	--------	----------	------------	------------

※ 名簿に登録されている者にのみ、オペレーティングシステムを操作するための ID およびパスワードを公開することとする。

別表1 (第4条および第16条関係)

種別	部局名	業務所管課長
セキュリティ責任者	財務部	税務室市民税担当課長 税務室資産税担当課長 税務室納税担当課長 税務室定額減税調整給付金担当課長
	市民部	国保年金課長 保険料収納担当課長 戸籍住民課長 湯川支所長 銭亀沢支所長 亀田支所長
	保健福祉部	介護保険課長 高齢福祉課長 障がい保健福祉課長 生活支援総務課長 生活支援課長 湯川福祉課長 亀田福祉課長
	子ども未来部	子どもサービス課長 子育て支援課長
	環境部	環境対策課長
	土木部	道路管理課長
	都市建設部	都市整備課長
	戸井支所	市民福祉課長
	恵山支所	市民福祉課長
	楸法華支所	市民福祉課長
	南茅部支所	市民福祉課長
	情報資産管理責任者	総務部

別表 2 (第 9 条関係)

1 操作者 ID の種別と役割

項番	分類	操作者 ID 種別 (操作権限)	操作端末	役割 (可能な業務)	備考
1		市町村業務管理者	CS / 統合端末	<ul style="list-style-type: none"> ・ 本人確認 ・ 本人確認情報検索 ・ 本人確認情報更新 ・ 転入転出 (全般) ・ 広域交付 (全般) ・ 統計処理 ・ 住民票コード管理 ・ 本人確認情報整合 ・ 本人確認情報提供状況開示 ・ 文字コード管理 ・ 公的個人認証連携 ・ 戸籍附票 ・ イベント通知 (インジケータ) ・ 送付先メニュー ・ 通知カード・個人番号通知書管理メニュー ・ 附票 	住民基本台帳カード発行管理業務および個人番号カード管理を除く、住基ネット業務を行うことができる職員。
2	通常業務	広域交付	統合端末	<ul style="list-style-type: none"> ・ 本人確認 ・ 本人確認情報検索 ・ 広域交付 (全般) ・ イベント通知 (インジケータ) 	広域交付業務を行う職員。
3		転入転出	統合端末	<ul style="list-style-type: none"> ・ 本人確認 ・ 本人確認情報検索 ・ 転入転出 (全般) ・ 戸籍附票 ・ イベント通知 (インジケータ) ・ 附票 	転入転出業務を行う職員。
4		業務窓口	統合端末	<ul style="list-style-type: none"> ・ 本人確認 ・ 本人確認情報検索 ・ 転入転出 (全般) ・ 広域交付 (全般) ・ 公的個人認証連携 ・ 戸籍附票 ・ イベント通知 (インジケータ) ・ 送付先メニュー ・ 通知カード・個人番号通知書管理メニュー ・ 附票 	広域交付, 転入転出を行うことができる職員。 窓口数の少ない支所等で使用する。
5		カード発行業務	カード発行管理全般	統合端末	<ul style="list-style-type: none"> ・ 本人確認 ・ 本人確認情報検索 ・ 住基カード発行管理 (窓口) ・ 住基カード発行管理 (データ書込・印刷)
6		カード発行窓口	統合端末	<ul style="list-style-type: none"> ・ 本人確認 ・ 本人確認情報検索 ・ 住基カード発行管理 (窓口) 	窓口で行う, 申請登録, 交付, 一時停止, 廃止などの「データ書込・印刷」以外の業務を行う職員。

別表 2 (第 9 条関係)

項番	分類	操作者 I D 種別 (操作権限)	操作端末	役割 (可能な業務)	備考
7	個人番号 カード管理	個人番号カード管理全般	統合端末	<ul style="list-style-type: none"> ・本人確認 ・本人確認情報検索 ・住基カード発行管理 (窓口) ・個人番号カード管理 (全般) ・個人番号カード管理 (交付前設定) ・通知カード・個人番号通知書管理メニュー 	個人番号カード発行管理全般を行う職員。
8		個人番号カード交付前設定	統合端末	<ul style="list-style-type: none"> ・個人番号カード管理 (交付前設定) 	個人番号カード交付前設定業務を行う職員。
9		個人番号カード交付全般	統合端末	<ul style="list-style-type: none"> ・本人確認 ・本人確認情報検索 ・住基カード発行管理 (窓口) ・個人番号カード管理 (全般) ・個人番号カード管理 (交付前設定) ・公的個人認証連携 ・通知カード・個人番号通知書管理メニュー 	個人番号カード発行管理業務全般と公的個人認証連携業務を行う職員。
10	通知カード・個人番号通知書管理	カード有効性管理全般	統合端末	<ul style="list-style-type: none"> ・通知カード・個人番号通知書管理メニュー 	通知カード状況管理および通知カード・個人番号カードの偽変造情報管理を行う職員。
11	他業務	市町村他業務	統合端末 (他部署に設置)	<ul style="list-style-type: none"> ・本人確認情報検索 ・情報提供アプリケーション 	住基法別表第二または第四の事務による利用および道が制定する事務処理特例条例により事務を移譲された市町村における別表第三、第五または第六の事務ならびに道が制定した条例による事務を行う職員。
12		公的個人認証	統合端末	<ul style="list-style-type: none"> ・公的個人認証連携 	公的個人認証連携業務を行う職員。
13		市町村窓口業務本人確認	統合端末 (他部署に設置)	<ul style="list-style-type: none"> ・市町村窓口業務本人確認 (住基カード, 個人番号カード) 	市の判断により, 住基カードを利用して本人確認を行う統合端末を設置した部署の職員。
14	附票	附票業務	統合端末	<ul style="list-style-type: none"> ・情報提供アプリケーション ・附票 	附票業務および住基事務による情報提供の業務を実施可能な職員。
15	操作者管理業務	操作者管理	統合端末	<ul style="list-style-type: none"> ・操作者登録 ・操作者権限追加/返却 ・操作者変更/削除 ・照合情報再登録 ・操作者有効期限変更 ・操作者 I D 無効化 ・操作者個別状況照会 ・操作者権限状況照会 ・操作者権限委譲履歴照会 ・操作者権限委譲状況一覧表出力 ・操作者管理帳票出力 ・操作者照合暗証番号発行 ・操作者権限設定 ・端末間暗号設定ツール 	市全体の操作者の管理を行う職員。

別表2 (第9条関係)

2 操作者IDの種別と操作可能な業務の対応表 (操作者管理業務を除く)

業務	本人確認※1	本人確認情報検索※1	本人確認情報更新※2	転入転出(全般)	広域交付(全般)	統計処理	住民票コード管理	本人確認情報整合	本人確認情報提供状況開示	文字コード管理	住基カード発行管理(窓口)	住基カード発行管理(データ書込・印刷)	個人番号カード管理(全般)	個人番号カード管理(交付前設定)	公的個人認証連携	市町村窓口業務本人確認(住基カード, 個人番号カード)※3	戸籍附票	イベント通知(インジケータ)	情報提供アプリケーション	送付先メニュー	通知カード・個人番号通知書管理メニュー	附票	操作者ID種別 (操作権限)	
																							市町村業務管理者	通常業務
市町村業務管理者	○	○	○	○	○	○	○	○	○	○	×※4	×	×※5	×	○	×	○	○	×	○	○	○	○	市町村業務管理者
広域交付	○	○	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	通常業務
転入転出	○	○	×	○	×	×	×	×	×	×	×※4	×	×※5	×	×	×	○	○	×	×	×	×	○	通常業務
業務窓口	○	○	×	○	○	×	×	×	×	×	×※4	×	×※5	×	○	×	○	○	×	○	○	○	○	通常業務
カード発行管理全般	○	○	×	×	×	×	×	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×	×	カード発行管理全般
カード発行窓口	○	○	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	カード発行管理全般
個人番号カード管理全般	○	○	×	×	×	×	×	×	×	×	○	○	○	○	×	×	×	×	×	×	○	×	×	個人番号カード管理全般
個人番号カード交付前設定	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	個人番号カード管理全般
個人番号カード交付全般	○	○	×	×	×	×	×	×	×	×	○	○	○	○	○※6	×	×	×	×	×	○	×	×	個人番号カード管理全般
通知カード・個人番号管理	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	通知カード・個人番号管理
市町村他業務	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	市町村他業務
公的個人認証	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	市町村他業務
市町村窓口業務本人確認	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	市町村他業務
附票業務	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○※7	×	×	○	×	附票業務

凡例 ○:可 ×:不可

- ※1: 「本人確認」には、操作権限名「個人番号カード管理全般」および「個人番号カード交付全般」を除き、条例利用による本人確認を含む。
- ※2: 「本人確認情報更新」には、本人確認情報メンテナンスなども含む。
- ※3: 「市長村窓口業務本人確認(住基カード, 個人番号カード)」の検索範囲は自市長村のCSのみ。
- ※4: 住民基本台帳カード発行管理業務のうち、「カード廃止情報入力」, 「カード回収情報入力」, 「カード暗証番号初期化」, 「カード発行履歴照会」, 「カード継続利用」, 「カード券面事項更新」および「カード券面事項照会」業務のみ実施可能。
- ※5: 個人番号カード管理業務のうち、「個人番号カード券面事項更新」, 「個人番号カード廃止情報入力」, 「個人番号カード回収情報入力」, 「個人番号カード暗証番号初期化」および「個人番号カード継続利用」業務のみ実施可能。
- ※6: 「個人番号カード交付処理」の署名用電子証明書破棄を行う場合において、「個人番号カード管理業務」から「公的個人認証連携業務」へ遷移する際の操作者のログオフおよびログオンが不要。
- ※7: 情報提供アプリケーションのうち、「ファイル転送メニュー」のみ実施可能。

別表 2 (第 9 条関係)

3 操作者 I D の種別と操作可能な業務の対応表 (操作者管理業務)

操作者 I D 種別 (操作権限)		業務													
		操作者登録	操作権限追加／返却	操作者変更／削除	照合情報再登録	操作者有効期限変更	操作者 I D 無効化	操作者個別状況照会	操作権限別状況照会	操作権限委譲履歴照会	操作権限委譲状況一覧表出力	操作管理帳票出力	操作者照合暗証番号発行	操作権限設定	端末間暗号設定ツール
通常業務	操作者管理	○	○	○	○	○	○	○	○	○	○	○	○	○	○

凡例 ○ : 可 × : 不可

別表3 (第14条および第18条関係)

年次点検簿

(例)

1	CSおよび統合端末のOSログイン画面にて、複数回パスワードの入力を間違えた場合、ロックアウトされる設定となっている。 (ただし、Administratorを除く)	各機器のOS上の設定を確認する。	○	mm. dd	印	
---	--	------------------	---	--------	---	--

項番	点検項目	点検方法	結果	実施日	実施者	備考
1	CSおよび統合端末のOSログイン画面にて、複数回パスワードの入力を間違えた場合、ロックアウトされる設定となっている。 (ただし、Administratorを除く)	各機器のOS上の設定を確認する。				
2	CS、統合端末およびファイアウォール(市)のOSに対して、不正なログイン記録が無い。	資産管理ソフトによって確認する。				
3	CSおよび統合端末にて、不要なフォルダの共有がされない設定となっている。	各機器のOS上の設定を確認する。				
4	CSおよび統合端末にて、不要なプログラムが起動しない設定となっている。	各機器のOS上の設定を確認する。				
5	CSおよび統合端末にて、定められたソフトウェア以外がインストールされていない。	各機器のOS上の設定または資産管理ソフトによって確認する。				
6	情報資産管理簿が適時更新され、現況と一致している。	管理簿と現況および担当者への聞き取り調査等で確認する。				
7	オペレーティングシステム操作者名簿が適時更新され、不要なユーザーID等が登録されていない。	名簿と現況を確認する。				
8	ファイアウォール(市)設定表が適時更新され、現況と一致している。	設定表と現況および担当者への聞き取り調査等で確認する。				

別表3 (第14条および第18条関係)

9	CSおよび統合端末からインターネット通信が行えない。	ブラウザを起動して確認する。				
10	照合IDが適切な操作者に利用されており、ログイン時の操作者有効期限設定の判定が有効である。	CSの操作者管理環境設定画面の設定を確認する。				
11	目的外利用等の不正な操作や業務上必要のない検索または抽出が行われていない。	操作ログおよび担当者への聞き取り調査等により確認する。				
12	ネットワーク構成図, 配線図, ポート収容図が現況と一致している。	現況および担当者への聞き取り調査等により確認する。				
13	磁気ディスクのラベリングが適切である。	現況を確認する。				
14	バックアップ運用管理表が適正に記載されている。	バックアップ運用管理表を確認する。				
15	ファイアウォール(市)のログの中に不正アクセスの可能性のあるログがない。	アクセスログを確認する。				
16	ファイアウォール(市)のアクセスログは、定められた通りに保管されている。	現況を確認する。				