庁内情報ネットワーク利用基準

（目的）

第１条　この利用基準は，庁内情報ネットワーク管理運営要領に基づき，庁内情報ネットワークを利用するに当たって遵守すべき事項を定めるものである。

（マイナンバー利用事務系への接続）

第２条　マイナンバー利用事務系に電子計算機または情報処理端末等を新たに接続しようとする課の長は，あらかじめ電子計算機管理運営要領第３節第１項および第８節第１項に基づく協議を行わなければならない。

２　前項において接続を許可された機器については，次に掲げる事項を満たさなければならない。

(1) ＩＰアドレスの登録ほか各種ネットワーク設定については，運用管理者の指示どおりに行うこととし，変更または削除しようとする場合には，運用管理者に報告すること。

(2) 運用管理者が指定する生体認証機等を導入することとし，その設定は運用管理者の指示どおりに行うこと。

(3) 運用管理者が指定するウイルス対策ソフトを導入することとし，その設定は運用管理者の指示どおりに行うこと。

(4) 運用管理者が指定する資産管理ソフトを導入することとし，その設定は運用管理者の指示どおりに行うこと。

(5) ＣＤ／ＤＶＤ／ＢＤ等の光学ドライブは，デバイスを使用不可とし，機能しない設定にすること。

(6) 空きＵＳＢポートを使用不可とし，物理的にふさぐこと。

(7) ホストコンピュータ上のシステムをオンラインで利用する場合には，運用管理者が指定したソフトウェアおよび各種ライセンスを導入し，指定したベンダー製の情報処理端末を用いること。

(8) 特定通信によって外部接続を行おうとする場合には，あらかじめ電子計算機管理運営要領に基づく協議を行うこと。ただし，函館市電子計算機処理に係るデータ保護管理規程（平成元年函館市訓令第

１号。以下「規程」という。）第１９条および第１９条の２に基づく協議を行う場合はこの限りでない。

３　マイナンバー利用事務系に接続した機器について，協議した内容が変更となる場合には，あらかじめ運用管理者に協議を行わなければならない。

（ＬＧＷＡＮ接続系への接続）

第３条　ＬＧＷＡＮ接続系に電子計算機または情報処理端末等を接続しようとする課の長は，あらかじめ運用管理者の承認を得なければならない。

２　前項において接続を承認された機器については，次に掲げる事項を満たさなければならない。

(1) ＩＰアドレスの登録ほか各種ネットワーク設定については，運用管理者の指示どおりに行うこととし，変更または削除しようとする場合には，運用管理者に報告すること。

(2) 運用管理者が指定する生体認証機等を導入することとし，その設定は運用管理者の指示どおりに行うこと。

(3) 運用管理者が指定するウイルス対策ソフトを導入することとし，その設定は運用管理者の指示どおりに行うこと。

(4) 運用管理者が指定する資産管理ソフトを導入することとし，その設定は運用管理者の指示どおりに行うこと。

(5) ＣＤ／ＤＶＤ／ＢＤ等の光学ドライブは，業務上やむを得ない場合を除いてデバイスを使用不可とし，機能しない設定にすること。

(6) 業務上やむを得ずＵＳＢメモリ等の外部記録媒体を利用しようとする場合には，あらかじめ運用管理者の承認を得ること。

(7) 必要の無い空きＵＳＢポートを使用不可とし，物理的にふさぐこと。

(8) 特定通信によって外部接続を行おうとする場合には，あらかじめ電子計算機管理運営要領第３節第１項および第８節第１項に準じた協議を行うこと。ただし，規程第１９条および第１９条の２に基づく協議を行う場合はこの限りでない。

（インターネット接続系への接続）

第４条　インターネット接続系に電子計算機または情報処理端末等を接続しようとする課の長は，あらかじめ運用管理者の承認を得なければならない。

２　前項において接続を承認された機器については，次に掲げる事項を満たさなければならない。

(1) ＩＰアドレスの登録ほか各種ネットワーク設定については，運用管理者の指示どおりに行うこととし，変更または削除しようとする場合には，運用管理者に報告すること。

(2) 運用管理者が指定するウイルス対策ソフトを導入することとし，その設定は運用管理者の指示どおりに行うこと。

(3) 運用管理者が指定する資産管理ソフトを導入することとし，その設定は運用管理者の指示どおりに行うこと。

(4) ＣＤ／ＤＶＤ／ＢＤ等の光学ドライブは，業務上やむを得ない場合を除いてデバイスを使用不可とし，機能しない設定にすること。

(5) 業務上やむを得ずＵＳＢメモリ等の外部記録媒体を利用しようとする場合には，あらかじめ運用管理者の承認を得ること。

(6) 必要の無い空きＵＳＢポートを使用不可とし，物理的にふさぐこと。

(7) 特定通信によって外部接続を行おうとする場合には，あらかじめ電子計算機管理運営要領第３節第１項および第８節第１項に準じた協議を行うこと。ただし，規程第１９条および第１９条の２に基づく協議を行う場合はこの限りでない。

（データの移転）

第５条　情報ネットワークに係るそれぞれの系を超えてデータの移転を行う場合には，次に掲げる内容のとおり，ウイルススキャン等の方法により，適切な安全確認を行わなければならない。

(1) ＬＧＷＡＮ接続系から抽出したデータをマイナンバー利用事務系以外の系に移転する場合には，データ受領側の情報処理端末等に接続した運搬用媒体に対して，データを端末へ移転する前に，手動に

よるウイルススキャン（以下「手動スキャン」という。）による安全確認を行うこと。

(2) インターネット接続系から，マイナンバー利用事務を行うものを除く独立系（以下「非番号利用独立系」という。）へ移転またはその逆方向へ移転する場合には，データ移転前および受領側情報処理端末等への媒体接続時の双方で，運搬用媒体に対して手動スキャンによる安全確認を行うこと。

(3) 外部からインターネット接続系または非番号利用独立系へデータ移転を行う場合には，受領側情報処理端末等への媒体接続時において媒体の手動スキャンを行った後，データを移転し，直ちに当該データを移転した保存先フォルダに対して再度，手動スキャンによる安全確認を行うこと。ただし，電子メールによりデータ受信した場合はこの限りでない。

(4) マイナンバー利用事務系に対して他の系から移転する場合またはＬＧＷＡＮ接続系に対してマイナンバー利用事務系以外の系から移転する場合には，運用管理者の指示を受け，指示された安全確認を行うこと。

2　同一系内における別の機器間でデータの移転を行う場合には，次に掲げる方法で行わなければならない。ただし，運搬用媒体を用いずに，運用管理者が認めるデータ共有の仕組みや電子メール等の一般的な通信経路によりデータ移転する場合はこの限りでない。

(1) マイナンバー利用事務系間でのデータ移転は，前項第４号のとおり行うこと。

(2) マイナンバー利用事務系以外においては，前項第２号のとおり行うこと。

3　インターネット接続系からＬＧＷＡＮ接続系へ移転またはその逆方向へ移転する場合には，前２項の規定にかかわらず，運用管理者が用意したメールアドレスあてに，当該データの添付および必要事項等を記入した電子メールによる申請を行うことにより，安全確認行為を省略できるものとする。この場合において，運用管理者は，当該申請に

対する承認を行うとともに，当該データに対して必要な安全確認を行った後，移転先の系においてデータを返送するものとする。

（補則）

第６条　この基準に定めのない事項またはこの基準に関し疑義が生じた場合については，必要に応じ運用管理者と協議するものとする。