庁内情報ネットワーク管理運営要領

目次

第１章　総則

（目的）

第１条　この要領は，総務部情報システム課が設置する庁内情報ネットワーク（以下「庁内情報ネットワーク」という。）に係る管理運営について必要な事項を定めることにより，情報通信技術の安定した利用環境を確保するとともに，各種情報資産を様々な脅威から守ることで，行政の円滑な運営と信頼性を確保することを目的とする。

（定義）

第２条　この要領において，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) 庁内情報ネットワーク　電磁的な状態の情報を運搬するための情報通信網であり，総務部情報システム課が設置するものをいう。

(2) 特定通信　通信経路の限定が可能な機器を用いるとともに，アプリケーションプロトコル（ポート番号）による通信の限定によって，あらかじめ許可された目的を達成するために最低限の情報のみが通信されること，およびそのように制御された状態をいう。

(3) マイナンバー利用事務系　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号。以下「番号法」という。）に規定する個人番号利用事務を行うために敷設された庁内情報ネットワークを含む体系であり，特定通信による接続を除き，外界から遮断された状態にあるものをいう。

(4) ＬＧＷＡＮ接続系　総合行政ネットワーク（略称：ＬＧＷＡＮ（Ｌｏｃａｌ　Ｇｏｖｅｒｎｍｅｎｔ　Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔ

ｗｏｒｋ））に接続するために敷設された庁内情報ネットワークを含む体系であり，特定通信による接続を除き，外界から遮断された状態にあるものをいう。

(5) インターネット接続系　インターネットと接続可能な庁内情報ネットワーク体系をいう。

(6) 独立系　他の機器とネットワーク接続されていない状態にあるパーソナルコンピュータ等の情報処理端末または総務部情報システム課が設置した以外の外界から遮断された状態で業務の用に供されている情報ネットワーク体系をいう。

(7) 情報資産　庁内情報ネットワークおよびそれに関する機器または接続する機器等ならびにこれらで取り扱われる情報（入出力帳票を含む）および各種仕様書等の関連ドキュメントをいう。

(8) 情報セキュリティ　情報資産の機密性，完全性および可用性を維持することをいう。

(9) 機密性　許可されていない者が取り扱えないようにする特性をいう。

(10) 完全性　破壊，改ざんまたは消去されていない状態を確保する特性をいう。

(11) 可用性　許可された範囲での取扱いを常に可能とさせる特性をいう。

（利用の範囲）

第３条　庁内情報ネットワークを利用できる機関は，市長，議会，教育委員会，選挙管理委員会，公平委員会，監査委員，農業委員会，固定資産評価審査委員会，公営企業管理者および消防長とする。

第２章　管理組織

（運用管理者）

第４条　情報資産の適正な管理を図るため，運用管理者を置くこととし，総務部情報システム課長をもって充てる。

２　運用管理者は，必要があると認めるときに外部監査人を指定して情報資産の管理に関する監査を実施することができる。

３　運用管理者は，前項の監査を実施した場合であって，外部監査人から監査の結果に関する報告に改善すべき事項が示されたときは，当該事項に対し，速やかに，必要かつ適切な措置を講じなければならない。

（庁内情報ネットワークの利用）

第５条　庁内情報ネットワークを新たに利用しようとする課の長等（当該業務において課長職に相当する職または同等の責務を負うべき者を含む）は，その内容を明らかにした上で，あらかじめ運用管理者に協議または所定の申請手続を行わなければならない。

２　庁内情報ネットワークを利用する業務所管課の長等（以下「利用課の長等」という。）は，当該ネットワークおよびその体系にある情報資産に対して情報セキュリティ上の脅威を与えないよう必要な措置を講じなければならない。

３　利用課の長等は，運用管理者から情報資産の適正な管理を図るために必要な指示を受けた場合，速やかにこれに応じなければならない。

（情報資産の管理および責任）

第６条　運用管理者および利用課の長等は，それぞれが管理する情報資産について，次に掲げる当該情報資産の重要度の区分に応じて適切な運用管理を行わなければならない。

(1) 情報セキュリティが破られることで，住民の生命または財産等に重大な影響があるもの。

(2) 情報セキュリティが破られることで，行政事務の執行等に重大な影響があるもの。

(3) 情報セキュリティが破られることで，行政事務の執行等に一定の影響を与えるもの。

(4) 上記以外のもの。

２　前項の場合において，当該情報資産についてその台帳を常に整備するとともに，適切に管理しなければならない。

第３章　情報セキュリティ対策

（マイナンバー利用事務系）

第７条　運用管理者および利用課の長等は，マイナンバー利用事務系に係る情報資産の適切な管理に当たり，次に掲げる内容を遵守しなければならない。

(1) 番号法において認められる特定通信技術を利用した通信を除き，外界から遮断された状態を保持すること。

(2) 特定通信先においてもインターネットとの通信ができないようにすること。

(3) 情報処理端末へのアクセスについては，ＩＤおよびパスワードのほかに，運用管理者が認めた方法による認証によって二要素認証を行うこととし，そのアクセス権を適正に管理すること。

(4) 情報処理端末の操作記録およびサーバ等の情報資産に対してアクセスした場合におけるその操作記録を残して不正な利用を発見できるようにすること。

(5) ＵＳＢメモリ等の外部記録媒体によって情報処理端末から情報を持ち出せないように設定すること。

(6) やむを得ずその体系を超えてデータの移動が必要な場合は，総務部情報システム課の職員のうち運用管理者があらかじめ指定した者の指示および監視のもとでこれを行うこと。

(7) 前号において特定個人情報（番号法第２条第８項に規定する特定個人情報をいう。）を外部記録媒体に記録する場合は，別に定める管理簿により管理し，当該外部記録媒体は施錠可能な保管庫等に保管するものとする。

（ＬＧＷＡＮ接続系）

第８条　運用管理者および利用課の長等は，ＬＧＷＡＮ接続系に係る情報資産の適切な管理に当たり，次に掲げる内容を遵守しなければならない。

(1) インターネットにアクセス可能なネットワーク等外部とは接続しないこと。ただし，真にやむを得ない理由で外部通信を行う場合であり，特定通信技術を利用した通信または無害化通信等の手法によ

ってその安全性を確保したもののうち，運用管理者が認めたものを除く。

(2) 情報処理端末へのアクセスについては，ＩＤおよびパスワードのほかに，運用管理者が認めた方法による認証によって二要素認証を行うこととし，そのアクセス権を適正に管理すること。

(3) 情報処理端末の操作記録およびサーバ等の情報資産に対してアクセスした場合におけるその操作記録を残して不正な利用を発見できるようにすること。

(4) ＵＳＢメモリ等の外部記録媒体による情報処理端末から情報を持ち出せないように設定すること。ただし，その利用目的等について，運用管理者が業務上やむを得ないと認めたものを除く。

(5) 前号に基づき認められた媒体の利用に当たっては，運用管理者が指示する方法によって情報セキュリティ対策を図ること。

（インターネット接続系）

第９条　運用管理者は，本市の情報セキュリティ対策として，次に掲げる条件を満たしたインターネット接続系の庁内情報ネットワークを整備するものとする。

(1) インターネット接続系は，マイナンバー利用事務系およびＬＧＷＡＮ接続系から分離すること。

(2) 北海道と協力して自治体情報セキュリティクラウドを構築し，高度な情報セキュリティ対策を講じること。

２　運用管理者および利用課の長等は，前項のネットワークを利用する場合，これに係る情報資産の適切な管理にあたり，次に掲げる内容を遵守しなければならない。

(1) マイナンバー利用事務系およびＬＧＷＡＮ接続系とは接続しないこと。

(2) 情報処理端末へのアクセスについては，ＩＤおよびパスワード等の適切な方法により認証を行うこととし，そのアクセス権を適正に管理すること。

(3) 情報処理端末の操作記録およびサーバ等の情報資産に対してアクセスした場合におけるその操作記録を残して不正な利用を発見できるようにすること。

(4) ＵＳＢメモリ等の外部記録媒体による情報処理端末から情報を持ち出せないように設定すること。ただし，その利用目的等について，運用管理者が業務上やむを得ないと認めたものを除く。

(5) 前号に基づき認められた媒体の利用に当たっては，運用管理者が指示する方法によって情報セキュリティ対策を図ること。

（物理的情報セキュリティ対策）

第10条　運用管理者および利用課の長等は，それぞれが管理する情報資産に対して，次に掲げる物理的な情報セキュリティ対策を講じなければならない。

(1) 盗難，不適切な閲覧または接触ならびに破損または劣化からの保護

(2) 不慮の事故または災害から保護するための必要な措置

(3) 情報資産のうち，記憶装置（機器に内蔵するものを含む）の廃棄および賃貸借契約終了時の返却に当たり，廃棄等の後においても不適切な利用を防止するため，記憶装置から情報を消去の上，物理的または磁気的な破壊に係る措置

(4) 情報資産のうち，サーバ等の機器を取り巻く温度，湿度，電気量および電圧の適正な管理

(5) 情報資産のうち，サーバ等の機器の周囲における埃または静電気等の発生を抑えるほか，その機能維持に必要な環境に対する配慮

（人的情報セキュリティ対策）

第11条　運用管理者および利用課の長等は，それぞれが管理する情報資産に対して，次に掲げる人的な情報セキュリティ対策を講じなければならない。

(1) 必要に応じて情報資産を取り扱う者をあらかじめ指定し，その範囲，責任および作業手順等の明確化

(2) 情報資産に接触する可能性のある全ての者に対する情報セキュリティに係る教育等の実施

(3) 情報セキュリティを脅かす事象または事故が発生した場合における適切な連絡体制の整備およびその周知徹底

（技術的情報セキュリティ対策）

第12条　運用管理者および利用課の長等は，それぞれが管理する情報資産に対して，次に掲げる技術的な情報セキュリティ対策を講じなければならない。

(1) 必要な情報セキュリティ機能の整備およびその仕様書等の適正な管理

(2) 必要に応じてＩＤ，パスワード，生体認証および暗号化等の技術を用いた不正アクセスの防止

(3) 関連機器の障害から情報資産を守るために必要な対策および適切な保守体制の整備

第４章　緊急時対応計画

（緊急時対応方針）

第13条　運用管理者は，庁内情報ネットワークおよびこれに係る情報資産が脅かされた場合またはそのおそれがある場合（以下「緊急時」という。）には，関係者への連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置を迅速かつ適切に実施しなければならない。

（警察機関との連携）

第14条　運用管理者は，緊急時に生じた事案（以下「緊急事態」という。）がサイバーテロその他の犯罪行為による可能性を含む場合には，直ちに警察機関へ報告するものとする。

（緊急事態への対応措置）

第15条　緊急事態を認知した者は，速やかに総務部情報システム課へ報告してその指示を受けるとともに，被害の拡大防止に必要な場合を除き，状況および証拠等の保全に努めなければならない。

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，令和２年３月１７日から施行する。

附　則

この要領は，令和４年１１月２５日から施行する。