調布市情報セキュリティ基本方針

私たちは，インターネットを中心とした情報通信技術（ＩＴ）が飛躍的に変革する中において，全ての市民の方が年齢，性別，情報技術有無に係らず，その恩恵を平等に享受できるよう情報通信技術（ＩＴ）を住民生活や自治体経営に積極的に取り入れ「電子市役所」を形成することで，行政サービスの質を向上させるとともに，サービスに要するコストを低減させ，「みんなが笑顔でつながる・ぬくもりと輝きのまち調布」を目指しています。

情報通信技術（ＩＴ）は豊かな生活環境をもたらしてくれますが，高度化が進む中において次のような課題があります。

１　調布市が保有している住民の個人情報等の機密情報の流出・悪用等の対策

２　インターネットを利用した不正アクセスやコンピュータウイルスへの対策

３　組織内部の者による意図しない操作や不正操作等への対策

情報化の進捗状況に比例して危険性は増大して行きます。

このようなことから，高度情報化通信ネットワーク社会においては，調布市で管理されている住民の個人情報や重要な行政情報等の情報資産の適切な管理が重要な課題であり調布市の責務であります。情報資産の「機密性」，「完全性」及び「可用性」を確保し，「電子市役所」における情報セキュリティ対策を実現するために，「情報セキュリティポリシー」を制定します。この「情報セキュリティポリシー」が有効に機能するよう，情報システムの利用，運用及び開発に関わる全ての職員が，常に意識して行動することを表したものです。

1　目的

調布市情報セキュリティ基本方針（以下「基本方針」という。）は，市が実施する情報セキュリティ対策について基本的な事項を定めることにより，市が保有する情報資産の機密性，完全性及び可用性を維持することを目的とする。

2　用語の定義

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

(1)　情報　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る記録であって電子計算機（演算装置，制御装置，記憶装置及び入出力装置からなる電子情報処理装置をいう。以下同じ。）による情報処理の用に供されるものをいう。

(2)　情報システム　電子計算機及びその周辺機器並びにプログラムにより構成され，情報処理の業務を自動的に処理するものをいう。

(3)　ネットワーク　複数の電子計算機及びその周辺機器等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェアをいう。）をいう。

(4)　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確保することにより脅威から当該情報資産を保護することをいう。

(5)　機密性　情報資産にアクセスすることを認められた者だけが，当該情報資産にアクセスできる状態を確保することをいう。

(6)　完全性　情報資産が破壊，改ざん又は消去をされていない状態を確保することをいう。

(7)　可用性　情報資産にアクセスすることを認められた者が，必要なときに中断されることなく，当該情報資産にアクセスできる状態を確保することをいう。

(8)　端末装置　電子計算機のうち各課に設置され，他の端末装置からの要求に応じて電算処理を行わないものをいう。

(9)　電磁的記録媒体　情報を記録した磁気ディスク，磁気テープ，光磁気ディスク，コンパクトディスク，ＵＳＢメモリ，メモリーカード，フロッピーディスク等をいう。

(10)　個人番号　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。）第２条第５項に規定する個人番号をいう。

(11)　特定個人情報　番号法及び調布市個人番号の利用に関する条例（平成２７年調布市条例第５２号）に定められた事務において，個人番号及び個人番号をその内容に含む個人情報をいう。

(12)　特定個人情報ファイル　番号法第２条第９項に規定する特定個人情報ファイルをいう。

(13) ＬＧＷＡＮ(総合行政ネットワーク)　地方公共団体の組織内ネットワーク（庁内ネットワーク）を相互に接続する行政専用ネットワークをいう。

ＬＧＷＡＮは，インターネットとは切り離された閉域ネットワークとして構築されており，高度なセキュリティを維持した行政専用のネットワークである。

マイナンバーによる情報連携，地方公共団体間におけるメール（ＬＧＷＡＮメール）などに活用される。

(14) マイナンバー利用事務系（個人番号利用事務系）　個人番号利用事務又は戸籍事務等に関わる情報システム及びその情報システムで取り扱うデータをいう。

(15) インターネット接続系　インターネットメール,外部のＷｅｂサイト閲覧等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(16) ＬＧＷＡＮ接続系　庁内ネットワークに接続された情報システム及びその情報システムで取り扱うデータのうち，個人番号利用事務系及びインターネット接続系を除いたものをいう。

グループウェア，文書管理システム，財務会計システムなどの情報システムや，庁内ファイルサーバや端末装置のローカル（デスクトップ等）に保存されたデータなどがＬＧＷＡＮ接続系に該当する。

これらの情報システム及びデータは庁内ネットワークを介して，ＬＧＷＡＮに接続されている。

(17) 通信経路の分割　ＬＧＷＡＮ接続系とインターネット接続系の両環境間の通信環境を分離した上で，安全が確保された通信だけを許可できるようにすることをいう。

(18) 無害化通信　インターネットメール本文のテキスト化や端末への画面転送等により，コンピュータウイルス等の不正プログラムの付着が無い等，安全が確保された通信をいう。

3　対象とする脅威

情報資産に対する脅威として，以下の脅威を想定し，情報セキュリティ対策を実施する。

(1)　情報システムに対する不正アクセス，ウイルス攻撃，サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報の漏えい，破壊，改ざん，消去及び重要情報の詐取，内部不正等

(2)　情報の無断持ち出し，無許可ソフトウェアの使用等の規定違反，情報システムの設計，開発の不備，プログラム上の欠陥，操作及び設定ミス，メンテナンス不備，内部又は外部監査機能の不備，委託管理の不備，マネジメントの欠陥，機器故障等の非意図的要因による情報の漏えい，破壊及び消去等

(3)　地震，落雷，火災等の災害によるサービス及び業務の停止等

(4)　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
(5)　電力供給の途絶，通信の途絶，水道供給の途絶等のインフラの障害からの波及等

4　適用範囲

この基本方針の適用範囲は，次に定めるところによる。

(1)　職員の範囲

この基本方針が適用される職員は，市長，議会，教育委員会，選挙管理委員会，農業委員会,監査委員及び固定資産評価審査委員会の所管に属する部門に勤務する者とする。

(2)　情報資産の範囲

この基本方針が対象とする情報資産は，次のとおりとする。

ア　ネットワーク，情報システム，これらに関する設備，電磁的記録媒体

イ　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。）

ウ　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

5　調布市情報セキュリティ対策基準の策定

この基本方針に基づき，市における情報セキュリティ対策の具体的な遵守事項及び判断基準等を，調布市情報セキュリティ対策基準（以下「対策基準」という。）として策定しなければならない。

6　情報セキュリティ実施手順の策定

この基本方針及び対策基準（この基本方針において「情報セキュリティポリシー」という。）に従い，情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお，情報セキュリティ実施手順は，公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

7　職員等の義務

職員，非常勤職員及び臨時職員（以下「職員等」という。）は，情報セキュリティ対策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は，この基本方針及び対策基準並びに実施手順を遵守しなければならない。

8　情報セキュリティ対策

脅威から情報資産を保護するために，以下の情報セキュリティ対策を実施するものとする。

(1)　組織体制

市の情報資産についての情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2)　情報資産の分類と管理

市の保有する情報資産をその重要度に応じて区分し，その区分に応じた情報セキュリティ対策を実施するものとする。

(3)　情報システム全体の強じん性の向上

情報セキュリティの強化を目的とし，業務の効率性・利便性の観点を踏まえ，情報システム全体に対し，次の三段階の対策を講じる。

ア　マイナンバー利用事務系においては，原則として，他の領域（ＬＧＷＡＮ接続系及びインターネット接続系）との通信をできないようにした上で，端末からの情報持ち出し不可設定や端末への多要素認証の導入等により，住民情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系においては，ＬＧＷＡＮと接続する業務用システムとインターネット接続系の情報システムとの通信経路を分割する。なお，両システム間で通信する場合には，無害化通信を実施する。

ウ　インターネット接続系においては，不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として，東京都及び市区町村のインターネットとの通信を集約した上で，自治体情報セキュリティクラウドの導入等を実施する。

(4)　物理的セキュリティ対策

サーバ，情報システムを設置する施設，通信回線及び職員等の端末装置の管理について物理的な対策を講じる。

(5)　人的セキュリティ対策

情報セキュリティに関し，職員等が遵守すべき事項を定めるとともに，十分な教育及び啓発を行う等の人的な対策を講じる。

(6)　技術的セキュリティ対策

情報システムの誤操作，不正アクセス等から情報資産を保護するために，情報資産へのアクセス制御等の技術的な対策を講ずる。

(7)　運用

ネットワーク障害，不正アクセス等から情報資産を保護するために，ネットワークの可用性確保，ネットワーク監視等の必要な対策を講ずる。

(8)　業務委託と外部サービスの利用

業務委託する場合には，情報セキュリティに関する要件を明記した契約を締結し，委託事業者において必要なセキュリティ対策が確保されていることを確認し，必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には，利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には，ソーシャルメディアサービスの

運用ポリシーを定め，ソーシャルメディアサービスで発信できる情報を規定し，利用するソーシャルメディアサービスごとのアカウント管理者を定める。

9　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため，定期的に，又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

10　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果，情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には，情報セキュリティポリシーを見直さなければならない。

附　則

この基本方針は，平成２７年４月１日から施行する。

附　則

この基本方針は，平成２９年４月２０日から施行する。

附　則

この基本方針は，平成３１年４月１日から施行する。

附　則

この基本方針は，令和３年５月３１日から施行する。

附　則

この基本方針は，令和４年７月１５日から施行する。