

## ○浦安市情報セキュリティ規程

平成24年 6 月22日

訓令第 7 号

浦安市電子計算組織管理運営に係るデータ保護規程（平成元年訓令第 2 号）の全部を改正する。

（目的）

**第 1 条** この規程は、本市が実施する情報セキュリティに係る対策について必要な事項を定めることにより、本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し、もって個人情報（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）第 2 条第 8 項に規定する特定個人情報を含む。）の保護に資するとともに、行政の信頼性を確保することを目的とする。

（平30訓令 9 ・ 一部改正）

（定義）

**第 2 条** この規程において、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) 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維持することをいう。
- (2) 情報 ネットワーク及び情報システムで取り扱う入出力データをいう。
- (3) 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスすることができる状態を確保することをいう。
- (4) 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。
- (5) 可用性 情報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、情報にアクセスすることができる状態を確保することをいう。
- (6) 情報資産 情報、情報システム及び情報システムの仕様書、ネットワーク図等のシステム構成を表す書類をいう。
- (7) ネットワーク コンピュータ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。

- (8) 情報システム コンピュータ、ソフトウェア、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。
- (9) パソコン等 次のいずれかに該当するコンピュータをいう。
- ア サーバ（利用者に対して、特定の機能及び保有するデータを提供するコンピュータをいう。）
  - イ 各課パソコン（総務部情報政策課長が、各課に設置したデスクトップ型のパーソナルコンピュータをいう。）
  - ウ 職員用シンクライアント（総務部情報政策課長が管理し、各職員が使用する、ハードディスクを内蔵しないパーソナルコンピュータをいう。）
  - エ 職員用タブレット型端末（総務部情報政策課長が管理し、各職員が使用するタブレット型のパーソナルコンピュータをいう。）
  - オ 貸出用パソコン（総務部情報政策課長が管理し、各職員に貸し出すノート型又はタブレット型のパーソナルコンピュータをいう。）
  - カ 独自導入パソコン（アからオまでに掲げるもののほか、各課が独自に導入し、及び管理するパーソナルコンピュータをいう。）
- (10) 情報セキュリティポリシー 本規程及び第5条に規定する情報セキュリティ対策基準をいう。
- (11) 個人番号（マイナンバー）利用事務系 個人番号利用事務（社会保障、地方税又は防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。
- (12) LGWAN接続系 LGWAN（地方公共団体を相互に接続する行政専用のネットワークをいう。）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（個人番号（マイナンバー）利用事務系を除く。）をいう。
- (13) インターネット接続系 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。
- (14) 無害化 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状態をいう。

（平28訓令5・令7訓令7・一部改正）

（対象とする脅威及び情報セキュリティ対策の実施）

**第3条** 市長は、情報資産に対する脅威として、次の脅威を想定し、情報セキュリティに係る対策を実施するものとする。

- (1) 不正なアクセス、ウィルス攻撃、サービス不能攻撃（ネットワークに接続されたコンピュータに過剰な負荷をかけてサービスの提供をできないようにする攻撃をいう。）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資産の漏えい、改ざん又は消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持出し、市が許可していないソフトウェアの使用等の規定違反、情報システムの設計又は開発の不備、プログラム上の欠陥、操作又は設定のミス、メンテナンスの不備、監査機能の不備、情報システムの委託管理の不備、マネジメントの欠陥、機器の故障等の非意図的な要因による情報資産の漏えい、破壊、消去等
- (3) 地震、落雷、火災等の災害による情報資産の消去、情報へのアクセスの不能等
- (4) 大規模又は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、通信、水道供給の途絶等のインフラの障害からの波及等  
(平28訓令5・令7訓令7・一部改正)

(情報セキュリティ対策)

**第4条** 前条の情報セキュリティに係る対策は、次のとおりとする。

- (1) 組織体制 本市の保有する情報資産について、情報セキュリティに係る対策を推進するための全庁的な体制及び役割を確立すること。
- (2) 情報資産の分類及び管理 本市の保有する情報資産を、機密性、完全性及び可用性に応じて分類し、当該分類に基づき管理すること。
- (3) 情報システム全体の強靱性の向上 情報セキュリティの強化を目的とし、業務の効率性又は利便性の観点を踏まえ、情報システム全体に対し、次に掲げる区分に応じ、それぞれに定める対策を講じること。

ア 個人番号（マイナンバー）利用事務系 原則として、他の領域との通信をできないようにした上で、端末から情報を持ち出せないようにするとともに、端末への多要素認証（複数の異なる種類の認証を組み合わせ

て行う認証をいう。)を導入すること等により、住民情報の流出を防ぐこと。

イ LGWAN接続系 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とともに、両システム間で通信する場合には、通信を無害化すること。

ウ インターネット接続系 千葉県自治体情報セキュリティクラウド（千葉県及び千葉県内の市町村のインターネットとの通信を集約した上で、不正通信の監視機能の強化等を行うシステムをいう。）の導入等を実施すること。

(4) 物理的セキュリティ サーバ、サーバ室、通信回線及び職員（会計年度任用職員及び非常勤職員を含む。以下同じ。）のパソコン等の管理について、物理的な対策を講じること。

(5) 人的セキュリティ 情報セキュリティに関し、職員が遵守すべき事項及び情報資産に対する事故等が発生した場合の報告等の対処の仕方を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じること。

(6) 技術的セキュリティ コンピュータ等の管理、アクセスの制御、不正なプログラム及び不正なアクセスに係る対策等の技術的な対策を講じること。

(7) 運用等 次に掲げる対策を講じること。

ア 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等情報セキュリティポリシーの運用面の対策

イ 他の部署が所管する情報システム及びデータの利用並びにデータの外部提供に係る対策の策定

ウ 情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するための緊急時対応計画の策定

(8) 業務委託等の利用 次に掲げる区分に応じ、それぞれに定める対策を講じること。

ア 業務委託を行う場合 受託事業者と情報セキュリティに係る要件が定められた契約を締結するとともに、受託事業者が必要な情報セキュリティに係る対策を確保していることを確認する等の措置を講じること。

イ クラウドサービスを利用する場合 利用に係る規定を整備し、情報の機密性に応じたセキュリティレベルを確保するための対策を講じること。

ウ ソーシャルメディアサービス（インターネットを利用し、個人又は法人が情報を発信し、相互に情報のやり取りを行うことができるサービスをいう。）を利用する場合 イに掲げる対策のほか、利用に係る運用手順を定め、発信できる情報を規定し、利用するサービスごとの責任者を定めること。

(9) 評価・見直し 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に係る監査及び自己点検を実施し、運用の改善を行い、情報セキュリティの向上を図ること。この場合において、情報セキュリティポリシーの見直しが必要なときは、その見直しを行うこと。

（令 7 訓令 7 ・全改）

（情報セキュリティ対策基準の策定）

**第 5 条** 市長は、前条の情報セキュリティに係る対策を実施するため、遵守事項、判断基準等を定めた情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

（令 7 訓令 7 ・一部改正）

（情報セキュリティ実施手順の策定）

**第 6 条** 市長は、対策基準に基づき、具体的な手順を定めた情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。

（職員の遵守義務等）

**第 7 条** 職員は、情報セキュリティ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情報セキュリティポリシー及び実施手順を遵守しなければならない。

2 職員は、情報資産を取扱う事務を人材派遣等により職員以外の者に行わせる場合には、当該者から情報セキュリティポリシー及び実施手順の遵守に関する同意を得なければならない。

（令 7 訓令 7 ・一部改正）

（対策基準及び実施手順の非公開）

**第 8 条** 対策基準及び実施手順は、浦安市情報公開条例（平成13年条例第 3 号）第 7 条第 4 号及び第 6 号に掲げる情報が記録されている部分については、非公開とする。

（令 7 訓令 7 ・ 一部改正）

（情報セキュリティに係る監査及び自己点検の実施）

**第 9 条** 情報セキュリティポリシー及び実施手順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に係る監査及び自己点検を実施するものとする。

（令 7 訓令 7 ・ 一部改正）

（情報セキュリティポリシーの見直し）

**第 1 0 条** 情報セキュリティに係る監査及び自己点検の結果、情報セキュリティポリシー及び実施手順の見直しが必要となった場合並びに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、保有する情報資産及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直すものとする。

（令 7 訓令 7 ・ 追加）

#### **附 則**

この訓令は、平成24年 7 月 1 日から施行する。

#### **附 則**（平成28年 5 月30日訓令第 5 号）

この訓令は、平成28年 6 月 1 日から施行する。

#### **附 則**（平成30年 5 月22日訓令第 9 号）

この訓令は、公示の日から施行する。

#### **附 則**（令和 7 年 4 月25日訓令第 7 号）

この訓令は、公示の日から施行する。