○船橋市情報資産の保護及び管理に関する規程

平成16年３月24日
訓令第２号

船橋市情報資産の保護及び管理に関する規程

（趣旨）

第１条　この訓令は、本市が保有する情報資産の保護を図るため、その適正な管理に関し、必要な事項を定めるものとする。

（定義）

第２条　この訓令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)　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、その構成機器（ハードウェア及びソフトウェア）をいう。

(2)　情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成された情報処理を行う仕組みをいう。

(3)　情報資産　次に掲げるものをいう。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システム並びにこれらに関する設備で取り扱う情報及び電磁的記録媒体で取り扱う情報（当該情報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の図等のシステム関連文書

(4)　機密性　情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(5)　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。

(6)　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、情報にアクセスできる状態を確保することをいう。

(7)　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。

(8)　情報セキュリティ事象　この訓令の違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象をいう。

(9)　情報セキュリティインシデント　望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(10)　情報セキュリティポリシー　この訓令及び第7条に規定する情報セキュリティ対策基準をいう。

（対象とする脅威）

第３条　情報資産に対する脅威は次に掲げるとおりとし、当該脅威を想定し、情報セキュリティ対策を実施する。

(1)　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資産の漏えい・破壊・改ざん・消去、重要情報の詐取及び内部不正等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・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及び機器故障等の非意図的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サービス及び業務の停止
(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
(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

（管理体制）

第４条　市長は、統一的な情報セキュリティを確保するため、全庁的な管理体制を整備する。

（情報資産の分類及び管理）

第５条　職員は、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、情報セキュリティ対策を実施する。

（情報セキュリティ対策）

第６条　市長は、第3条に規定する脅威から情報資産を守るため、次に掲げる対策を講ずるものとする。

(1)　物理的セキュリティ対策（情報システムを設置する施設への不正な立入り、情報資産への損害、情報資産の利用の妨害等から保護するための物理的な対策をいう。）
(2)　人的セキュリティ対策（情報セキュリティに関する権限及び責任並びに遵守すべき事項を明確に定め、職員に対する周知及び徹底を図るとともに、十分な教育研修等を行う対策をいう。）
(3)　技術的セキュリティ対策（情報資産を不正アクセス等から保護するための情報資産へのアクセス制御、ネットワーク管理等の技術的な対策をいう。）
(4)　運用における対策（情報システムの監視、情報セキュリティ対策の遵守状況の確認、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を講じるとともに、情報資産に対する情報セキュリティインシデント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等を行う対策をいう。
(5)　業務委託と外部サービスの利用における対策　次に掲げる場合に応じ、次に定める対策をいう。

ア　業務委託を行う場合　委託事業者を選定し、情報セキュリティ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、措置を講じること。
イ　外部サービスを利用する場合　利用に係る規定を整備し、対策を講じること。
ウ　ソーシャルメディアサービスを利用する場合　ソーシャルメディアサービスの運用手順を定め、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責任者を定めること。

（情報セキュリティ対策基準の策定）

第７条　市長は、情報セキュリティ対策を実施するに当たっての遵守すべき事項及び判断等の統一的な基準として情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

（情報セキュリティ実施手順の策定）

第８条　情報システムを所掌する所属の長は、対策基準に基づき、個々の情報システムについて情報セキュリティ対策を具体的に実施するために、当該情報システムに係る情報セキュリティ実施手順（以下「実施手順」という。）を定めなければならない。

（情報セキュリティ対策の遵守）

第９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。

（情報セキュリティの監査及び自己点検）

第10条　市長は、情報セキュリティ対策が遵守されていることを検証するため、定期的に情報セキュリティの監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図るものとする。

（評価及び見直し）

第11条　市長は、前条の監査及び自己点検の実施の結果により、情報セキュリティ対策の評価を行い、情報セキュリティを取り巻く状況の変化等を踏まえ、情報セキュリティポリシー及び実施手順の見直しを実施するものとする。

附　則

この訓令は、平成16年３月25日から施行する。

附　則（令和元年10月31日訓令第5号）

この訓令は、令和元年11月1日から施行する。

附　則（令和４年９月21日訓令第11号）

この訓令は、令和４年10月１日から施行する。