荒川区規則第５６号
令和８年４月１日　公布

荒川区情報セキュリティに関する規則

目次

第１章　総則

（目的）

第１条　この規則は、荒川区（以下「区」という。）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ため、区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を目的とする。

（定義）

第２条　この規則において、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）　電子情報システム　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、情報処理を行う仕組みをいう。

（２）　ネットワーク　コンピュータ等を相互に接続するため通信網、その他の構成機器（ハードウェア及びソフトウェア）をいう。

（３）　情報資産　ネットワーク及び電子情報システム並びにこれらに関する設備及び電子的記録媒体、これにより取り扱われる情報（これらを印刷した文書を含む。）並びに電子情報システムの仕様書及びネットワーク図その他のシステム関連文書をいう。

（４）　電子情報処理　電子情報システムを利用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、出力、通信若しくは消去又はこれらに類する処理をいう。

（５）　データ　電子情報処理の対象となる情報又は電子情報処理された情報をいう。

（６）　個人情報　個人情報の保護に関する法律（平成１５年法律第５７号。（以下「保護法」という。）第２条第１項に規定する個人情報をいう。

（７）　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。

（８）　特定個人情報　番号法第２条第９項に規定する特定個人情報をいう。

（９）　職員　地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職の職員及び同条第３項に規定する特別職の職員をいう。

（１０）　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。

（１１）　情報セキュリティポリシー　本規則に基づき別に定める情報セキュリティ対策基準をいう。
（１２）　機密性　別に定めるところにより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。
（１３）　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。
（１４）　可用性　別に定めるところにより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。

（適用範囲）

第３条　本規則は、区長部局、教育委員会、選挙管理委員会、監査委員及び議会事務局に適用し、区の情報資産を対象とする。

第２章　電子情報システムに係る事務の総括

（情報統括責任者）

第４条　政策企画部を担当する副区長を情報統括責任者とする。

２　情報統括責任者は、区における全ての電子情報システム及び情報資産の管理並びに情報セキュリティ対策に関する事務を統括するとともに、その実施等について責任を負う。

（情報統括責任者の補佐）

第４条の２　政策企画部長を情報管理責任者とし、情報統括責任者が行う電子情報システム及び情報資産の管理並びに情報セキュリティ対策に関する事務の統括を補佐し、重要な案件については、必要に応じ、情報統括責任者に報告する。

第３章　電子情報システムの導入等

（新規導入等の申請）

第５条　新たな電子情報システムの導入又は既存の電子情報システムの改修、更改若しくは継続運用（以下「電子情報システムの導入等」という。）を行おうとするときは、政策企画部デジタル推進課（以下「デジタル推進課」という。）が管理するものにあっては政策企画部デジタル推進課長又は当該電子情報システムを利用する部の長が、デジタル推進課以外の課が管理するものにあっては当該電子情報システムを管理する部の長が、次に掲げる基準に該当することを確認した上で、情報管理責任者に申請しなければならない。
（１）　区民サービスの向上に寄与するものであること。
（２）　行財政運営の効率化に寄与するものであること。
（３）　法に定められた事務処理を行う電子情報システムの場合、その内容が法令に適合するものであること。
（４）　保護法に定める個人情報の保護に適合するものであること。

２　前項の規定による申請は、翌年度以降に予定する電子情報システムの導入等について、当該年度中に行うものとする。ただし、法令改正等緊急に行う必要があると認められるときは、この限りでない。

３　前２項に定めるもののほか、申請手続について必要な事項は、情報管理責任者が別に定める。

（付議）

第６条　情報管理責任者は、前条第１項の規定による申請があったときは、必要性、費用、効果、代替手段等の有無に関する資料を徴し、その可否について第７条に規定する電子情

報システム運営委員会に付議しなければならない。
２　情報管理責任者は、前項の規定により付議した案件について電子情報システム運営委員会における可否の決定があったときは、速やかにその結果を、当該申請を行った部長に通知しなければならない。
３　当該申請を行った部長は、申請内容を実施するときは、電子情報システム運営委員会の議を経なければならない。

第４章　電子情報システム運営委員会

（電子情報システム運営委員会の設置）
第７条　電子情報システムの適正かつ効率的な運営を図るため、電子情報システム運営委員会（以下「運営委員会」という。）を設置する。
２　運営委員会に関し必要な事項は、別に定める。

第５章　情報セキュリティ委員会

（情報セキュリティ委員会の設置）
第８条　情報セキュリティの確保を図るため、情報セキュリティ委員会（以下「セキュリティ委員会」という。）を設置する。
２　セキュリティ委員会に関し必要な事項は、別に定める。

第６章　情報セキュリティ対策等

（職員等の遵守義務）
第９条　第３条の機関に所属する職員等（以下「職員等」という。）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、業務の執行に当たって情報セキュリティポリシーを遵守しなければならない。
（対象とする脅威）
第１０条　情報セキュリティ対策は、次に掲げる事象を想定し、これに対処するために定めるものとする。
（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃その他のサイバー攻撃、部外者の侵入その他の意図的な行為又は内部不正により、情報資産の漏えい、破壊、改ざん、若しくは消去又は重要情報の詐取が生じること。
（２）　情報資産の無断持出し、無許可ソフトウェアの使用その他の規定違反、設計又は開発の不備、プログラム上の欠陥、操作又は設定の誤り、保守管理の不備、内部監査機能又は外部監査機能の不備、マネジメントの欠陥若しくは機器故障その他の非意図的な要因により、情報資産の漏えい、破壊若しくは消去が生じること。
（３）　地震、落雷、火災その他の災害により、サービス又は業務の停止等が生じること。
（４）　大規模又は広範囲にわたる疾病により要員不足が生じ、システム運用の機能不全等が生じること。
（５）　電力供給の途絶、通信の途絶、水道供給の途絶その他の社会インフラの障害により、業務に支障が生じること。
（情報セキュリティ対策）
第１１条　前条の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講じる。
（１）　情報セキュリティ対策を推進するため、全庁的な組織体制を確立すること。

（２）　荒川区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、当該分類に基づき情報セキュリティ対策を実施する。
（３）　情報セキュリティの強化を図るとともに、業務の効率性及び利便性に配慮し、電子情報システム全体について次に掲げる対策を講じること。
ア　マイナンバー利用事務系電子情報システムにおいては、原則として、他のネットワークとの通信をできないようにした上で、端末からの情報資産持出しができないようにする設定及び端末への多要素認証の導入その他の対策により、住民情報の流出を防止すること。
イ　ＬＧＷＡＮ接続系電子情報システムにおいては、ＬＧＷＡＮと接続する業務用システムとインターネット接続系電子情報システムとの通信経路を分割し、これらのシステム間で通信する場合は、無害化通信を実施すること。
ウ　インターネット接続系電子情報システムにおいては、情報セキュリティクラウドその他の仕組みにより、不正通信の監視機能の強化その他の高度な情報セキュリティ対策を実施すること。
（４）　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ことその他の人的な対策を講じること。
（５）　サーバ、情報システム室、通信回線及び職員等の端末その他の情報機器の管理について、物理的な対策を講じること。
（６）　コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策その他の技術的対策を講じること。
（７）　電子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その他の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、緊急時対応計画を策定すること。
（８）　業務委託を行う場合にあっては、委託事業者を選定、情報セキュリティ要件を明記した契約を締結、委託事業者における必要なセキュリティ対策の確保の確認その他必要な措置を講じること。
（９）　外部サービス（クラウドサービス等を含む）を利用する場合にあっては、利用に係る規定を整備し、必要な対策を講じること。
（１０）　ソーシャルメディアサービスを利用する場合にあっては、運用手順を定め、発信できる情報を規定するとともに、利用するソーシャルメディアサービスごとに責任者を定めること。
（１１）　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し、運用改善を行うとともに、必要があると認めるときは、情報セキュリティポリシーの見直しを行うこと。

第７章　情報セキュリティ対策基準等

（情報セキュリティ対策基準の策定）
第１２条　前条に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。
２　前項の情報セキュリティ対策基準は、非公開とする。

（情報セキュリティ実施手順の策定）

第１３条　各課長は、情報セキュリティ対策基準に基づき、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。

２　前項に規定する情報セキュリティ実施手順は、非公開とする。

第８章　雑則

（処分の方針）

第１４条　情報セキュリティ対策に違反した職員については、事案の状況等に応じて懲戒処分等の対象として取り扱うものとする。

（委任）

第１５条　この規則の施行について必要な事項は、区長が別に定める。

附　則

この規則は、公布の日から施行する。