江戸川区情報管理安全対策要綱、同基準（江戸川区情報セキュリティポリシー）の適用対象

区に代わり情報資産（※１）を取り扱う業務において、以下の情報システム（※２）を利用する場合を対象とする。

１．区が開発運用する情報システムを利用する場合

（例：各種施設予約システム、図書館システムなど）

指定管理者は、区の情報セキュリティポリシー及び当該情報システムの運用規程等に則して利用することとします。

２．情報システムの開発運用を指定管理者が行う場合（※３）

指定管理者において当該施設の情報セキュリティに関する方針を定め、これに則して情報システム等の開発、運用を行うものとします。方針に定める内容は、区の情報セキュリティポリシーに準じるものとし、協定において規定するものとします。

なお、指定管理者の自主事業及び法人内部の事務処理に係る情報資産、情報システムについては、基本的に、指定管理者自身の情報セキュリティに係る方針等に則して開発、運用するものとします。

※１　情報資産とは、情報システム（※２）の開発と運用に係るすべてのデータ及びそれらで取り扱うすべてのデータをいう。（江戸川区情報管理安全対策要綱第２条（７））

※２　情報システムとは、コンピュータ（ハードウエア及びソフトウエア）、その周辺機器、ネットワーク及び記録媒体の全部又は一部により構成され、これを使用して業務を処理する仕組みをいう。（江戸川区情報管理安全対策要綱第２条（５））

※３　第三者の提供する情報システムを指定管理者が利用する場合を含みます。

江戸川区情報セキュリティポリシー

第１章 情報セキュリティポリシーの位置付け、構成 3

第２章　江戸川区情報管理安全対策要綱 4

（目的等） 4
（定義） 4
（対象範囲） 5
（情報セキュリティ管理体制） 5
（情報資産の分類） 5
（情報セキュリティ対策） 5
（江戸川区情報管理安全対策基準） 6
（情報セキュリティ点検・監査） 6
（違反に対する措置） 6
（見直しの実施） 6
（関係団体等への対応） 6
（指定管理者への対応） 6
（その他） 6
別表第一（第２条関係） 7
別表第二（第２条関係） 7

第３章　江戸川区情報管理安全対策基準 8

（目的） 8
（定義） 8
（情報の分類と管理） 8
（主要な機器、装置の設置場所） 8
（管理区域） 9
（予備電源の整備） 9
（配線等の維持） 9
（職員等の役割と責任） 9
（教育・訓練） １０
（事故、障害に対する報告） １０
（ＩＤ、パスワード及びＩＣカード等の管理） １０
（業務目的外利用の禁止等） １１
（機器構成変更の制限） １１
（ソフトウエア導入の制限） １１
（ソフトウエア等のライセンス管理） １１
（コンピュータ及びネットワークの管理） １１
（アクセス制御） １２

（管理者権限）……１２
（外部からのアクセス）……１２
（開発前のセキュリティ統括者への協議）……１３
（設計時の情報セキュリティ確保）……１３
（開発時のセキュリティ確保）……１３
（外部委託に関するセキュリティ確保）……１３
（コンピュータウイルス対策）……１３
（不正アクセス対策）……１４
（障害時対応手順の策定）……１４
（セキュリティ障害等の対応）……１４
（情報システム運用規程の整備）……１５
（情報セキュリティ対策の遵守状況の確認）……１５
（アクセス記録等の閲覧）……１５
（法令等の遵守）……１６
（情報セキュリティ点検・監査）……１６
（指定管理者に関する措置）……１６
（見直しの実施）……１６
（その他）……１６
（施行期日）……１７
（経過措置）……１７

第１章　情報セキュリティポリシーの位置付け、構成

情報セキュリティポリシーとは、江戸川区が所掌する情報資産について、その機密性、完全性、可用性*を維持するための対策について、総合的、体系的に取りまとめたものである。

江戸川区が所掌する情報資産に係る業務については、情報セキュリティポリシーに即して実施することとし、当該業務に携わる全職員並びに関係団体†の職員及び外部の委託事業者が遵守するよう浸透、普及、定着を図るものとする。

情報セキュリティポリシーは一定の普遍性を備えた部分（江戸川区情報管理安全対策要綱）と情報資産を取り巻く状況の変化に対応する部分（江戸川区情報管理安全対策基準）から構成する。これらに基づき、情報システムごとに具体的な情報セキュリティ対策の実施手順を策定することとする。（下表参照）

情報セキュリティポリシーの構成

名　　称		内　　容
情報セキュリティポリシー	江戸川区情報管理安全対策要綱	情報セキュリティ対策に関する統一的かつ基本的な方針
	江戸川区情報管理安全対策基準	江戸川区情報管理安全対策要綱を実行に移すためのすべての情報システムに共通の情報セキュリティ対策の基準
各情報システムの運用規程		情報システムごとに定める江戸川区情報管理安全対策基準に基づいた具体的な実施手順

* 機 密 性：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完 全 性：情報及び処理の方法の正確さ並びに完全である状態を安全防護すること。
可 用 性：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

† 関係団体：区が出資その他財政上の援助等を行う法人のうち、財団法人江戸川区環境促進事業団、社団法人江戸川区高齢者事業団、社会福祉法人江戸川区社会福祉協議会をいう。

第２章　江戸川区情報管理安全対策要綱

（目的等）

第１条 この要綱は、区の所掌するあらゆる情報資産及びそれを取り扱う情報システムについて、その情報セキュリティを維持することを目的とする。

２　情報システムの開発、運用及び管理など、区の情報セキュリティに関するすべての施策、規程は、この要綱を基本とする。

（定義）

第２条　この要綱において、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) 課　情報資産とそれを取り扱う情報システムを所掌する課（江戸川区の組織に関する規則（昭和 40 年３月江戸川区規則第８号）第７条に規定する課、室、副参事及び別表第１に定める行政組織並びに江戸川区保健所処務規程（昭和 50 年４月江戸川区訓令甲第３号）第２条に規定する課並びに江戸川区教育委員会事務局処務規則（昭和 46 年９月江戸川区教育委員会規則第２号）第２条に規定する課、室及び別表第２に定める教育組織並びに監査委員事務局、選挙管理委員会事務局及び区議会事務局）をいう。

(2) 課長　前号に規定する課の長をいう。ただし、区議会事務局にあっては次長をいう。

(3) 学校　江戸川区立学校設置条例（昭和 32 年 4 月江戸川区条例第 6 号）別表に掲げる小学校、中学校及び幼稚園をいう。

(4) 学校長　前号に規定する学校の長をいう。

(5) 情報システム　コンピュータ（ハードウェア及びソフトウェア）、その周辺機器、ネットワーク及び記録媒体の全部又は一部により構成され、これを使用して業務を処理する仕組みをいう。

(6) ネットワーク　コンピュータ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）及び記録媒体並びに処理を行う仕組みをいう。

(7) 情報資産　情報システムの開発と運用に係るすべてのデータ及びそれらで取り扱うすべてのデータをいう。

(8) アクセス　情報システムにより情報資産を利用すること。

(9) 情報セキュリティ　情報資産の機密保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(10) 職員等　区の所掌する情報資産及び情報システムに関する業務に携わる正規職員、再任用職員、非常勤職員、臨時職員及び労働者派遣契約に基づき区の業務の処理に従事する派遣労働者をいう。

(11) 情報化推進本部　江戸川区情報化推進本部設置要綱（13 経情エ 1-11 第 1 号平成 13 年 11 月 8 日区長決定）第１条により設置した江戸川区情報化推進本部をいう。

(12) 関係団体　区が出資その他財政上の援助等を行う法人又は団体のうち、財団法人江戸川区環境促進事業団、社団法人江戸川区高齢者事業団、社会福祉法人江戸川区社会福祉協議会及び江戸川区職員厚生会をいう。

(13) 指定管理者　地方自治法（昭和 22 年法律第 67 号）第 244 条の２第３項に定める指

定管理者をいう。

（対象範囲）

第３条　この要綱が対象とする情報資産及び情報システムの範囲は、区長、教育委員会、選挙管理委員会、監査委員、農業委員会、区議会事務局の所掌するものとし、学校における教育のために用いる情報システムは対象外とする。

２　学校における教育のために用いる情報システム等は、この要綱の対象となる情報システムと物理的に分けなければならない。

（情報セキュリティ管理体制）

第４条　区におけるすべての情報資産及び情報システムの情報セキュリティに関する最高責任者として最高情報統括責任者を置き、副区長をもって充てる。

２　情報セキュリティに関する施策を統括し、情報セキュリティ管理者の指導を行わせるため、情報セキュリティ統括者（以下「セキュリティ統括者」という。）を置き、経営企画部長をもって充てる。

３　セキュリティ統括者を補佐し、情報セキュリティ対策を実施するとともに、全庁に関わる情報システムについての情報セキュリティを維持し、その適正な管理並びに効率的な運用を図るため、情報セキュリティ総括管理者（以下「セキュリティ総括管理者」という。）を置き、経営企画部情報政策課長をもって充てる。

４　各課及び学校（以下「各課等」という。）の所掌する業務において、情報セキュリティを維持し、情報システムの適正な管理並びに効率的な運用を図るために各課等に情報セキュリティ管理者（以下「セキュリティ管理者」という。）を置き、課長及び学校長をもって充てる。

５　情報セキュリティに係る基本的な方針、計画、重要な施策の決定については情報化推進本部の議を経るものとする。

（情報資産の分類）

第５条　各情報資産については、当該情報を作成した課等においてセキュリティ管理者がそれぞれの重要性、内容に基づいて分類を行い、適正な管理を行うこととする。

（情報セキュリティ対策）

第６条　情報セキュリティの維持を図るため、次の各号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　情報システムを構成する情報機器を損傷、破壊又は盗難等から守り、関係者以外の利用から保護するため、適切な保安設備の設置や機器の運用等の保安対策を実施する。

(2) 人的セキュリティ対策　情報セキュリティ対策に関する権限や責任について定めるとともに、情報資産の保護のために職員等が遵守すべき事項を定めるものとする。また、職員等に対し、適切な情報管理に必要な教育及び啓発が講じられるように必要な対策を講じる。

(3) 技術及び運用におけるセキュリティ対策　情報資産を外部からの不正なアクセス等から適切に保護するため、以下の技術面、運用面の対策を講じるとともに緊急事態が発生した際に迅速な対応を可能とするための対応策を講じるものとする。

ア　利用記録の取得など情報システムの適切な管理

イ　情報資産へのアクセスの制御

ウ　システムの開発、導入、保守等におけるセキュリティ確保

エ　コンピュータウイルス、不正アクセスなどのリスク対応

オ　情報セキュリティに関する規程の遵守状況の確認

（江戸川区情報管理安全対策基準）

第７条　前条の情報セキュリティ対策を講ずるにあたり、遵守すべき行為及び判断等の基準並びに実施に際して必要な事項を明らかにするため、江戸川区情報管理安全対策基準を定めるものとする。

（情報セキュリティ点検・監査）

第８条　情報セキュリティに関する規程の遵守について、定期的に点検・監査を実施するものとする。

（違反に対する措置）

第９条　この要綱及びこれを受けて規定する情報セキュリティに関する規程に違反した者については、当該違反と過失の重大性に応じて、懲戒処分等の対象とする。

（見直しの実施）

第 10 条　この要綱は情報セキュリティ点検・監査の結果及び情報システムを取り巻く状況の変化を踏まえ、必要に応じて見直すものとする。

（関係団体等への対応）

第 11 条　関係団体の所掌する情報資産及び情報システムについて、この要綱の趣旨にのっとり情報セキュリティを確保するため、必要な措置を講ずるよう努めるものとする。

２　関係団体へ情報資産及び情報システムに関わる業務を委託する場合又は関係団体に区の保有する情報システムの利用を認める場合は、当該業務に関するセキュリティ管理者の指定など情報セキュリティに関する協定を締結することとする。

（指定管理者への対応）

第 12 条　指定管理者の実施する業務において、情報資産及び情報システムに関わる業務を実施する場合は、この要綱の趣旨にのっとり情報セキュリティを確保するため、当該指定管理業務に関する協定等において、必要な措置を定めるものとする。

（その他）

第 13 条　この要綱に定めるもののほか、この要綱の施行に関し必要な事項は、別に区長が定める。

付　則

この要綱は、平成 14 年４月１日から施行する。

付　則

この要綱は、平成 15 年５月 19 日から施行する。

付　則

この要綱は、平成 17 年 12 月 26 日から施行する。

付　則

この要綱は、平成 18 年４月１日から施行する。

付　則

この要綱は、平成 19 年４月１日から施行する。

別表第一（第２条関係）

江戸川区希望の家	江戸川区小松川事務所 江戸川区葛西事務所 江戸川区小岩事務所 江戸川区東部事務所 江戸川区鹿骨事務所

別表第二（第２条関係）

江戸川区立中央図書館 江戸川区教育研究所

第３章　江戸川区情報管理安全対策基準

（目的）

第１条　江戸川区情報管理安全対策要綱（以下「対策要綱」という。）第７条の規定に基づき、情報セキュリティ対策を講ずるに当たり遵守すべき行為及び判断等の基準その他必要な事項を定める。

（定義）

第２条　この基準において用いる用語の意義は、対策要綱において定めるもののほか、次の各号に定めるところによる。

(1) 情報化推進リーダー　情報セキュリティ管理者を補佐し、各課において情報セキュリティ対策、情報政策課との連絡調整を担当する職員

(2) 運用管理者 情報セキュリティ管理者の指定する情報システムの運用管理を担当する職員

(3) ＩＤ　情報システムの利用者を識別するための情報

(4) パスワード　情報システムの利用者を認証するための情報

(5) 端末等　情報システムを構成する機器のうち利用者が情報システムにアクセスするため操作する情報機器をいう。

(6) サーバ等 情報システムを構成する機器のうち、データの管理、端末等の制御など主要な役割を担うコンピュータをいう。

（情報の分類と管理）

第３条　情報システムで取り扱う情報は、当該情報を作成した課において情報セキュリティ管理者（以下「セキュリティ管理者」という。）がそれぞれの重要性、内容に基づき次の各号に定める分類を行う。

(1) 秘密の取り扱いを要する情報（以下「秘密情報」という）

ア　江戸川区行政文書管理規則（平成 18 年 3 月江戸川区規則第 56 号）第 65 条に定める秘密文書に該当する情報

イ　情報システムの運用管理に関する情報で、情報セキュリティを維持するため、秘密の取り扱いを要する情報

(2) その他の情報（以下「一般情報」という）　秘密情報以外の情報

２　セキュリティ管理者は、前項の分類を踏まえ、秘密情報について次の各号に定める適正な管理を行う。

(1) その所掌する秘密情報について、内容ごとにアクセス権限を定めること。

(2) 秘密情報のうち個人情報等特に重要な情報については、記録媒体に複製を作成し、その保管場所には施錠すること

(3) 前号の記録媒体の廃棄にあたっては、情報を復元できないよう処理すること。

（主要な機器、装置の設置場所）

第４条　大型汎用コンピュータ、サーバ用コンピュータ、ネットワーク管理用機器など、情報システムの稼動に重大な影響を与える主要な機器及び装置（以下「主要な機器等」という。）は、防災、防犯等の対策が施されている安全に管理できる区画に設置するもの

とする。セキュリティ管理者は、全装置の記録を作成し、主要な機器等の持ち出しや持ち込みが発生しないように管理しなければならない。

（管理区域）

第５条 前条の区画への入退場は当該区画を管理するセキュリティ管理者に許可を受けなければならない。

２　職員等は身分証明証等を携帯し、求めに応じて提示しなければならない。

３　主要な機器等について、やむを得ず前条の区画以外に設置するときは、機器等の固定、施錠等必要な措置を施すものとする。

（予備電源の整備）

第６条　主要な機器等の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備えていなければならない。また、落雷等による過電流に対してそれらの機器等を保護するための措置を施さなければならない。

（配線等の維持）

第７条　ネットワークを構成する配線及び無線システムは損傷又は傍受等を受けることがないように可能な限り必要な措置を施さなければならない。セキュリティ管理者の指示を受けた運用管理者又は当該業務を委託された外部委託事業者以外の者は配線、機器等を変更、追加してはならない。

（職員等の役割と責任）

第８条　情報セキュリティに関する職員等の権限、役割及び責任は次の各号に定めるとおりとする。

(1) 最高情報統括責任者（以下「最高統括者」という。）　区におけるすべての情報資産の情報セキュリティを総括し、必要に応じ、情報化推進本部の開催を求める。

(2) 情報セキュリティ統括者（以下「セキュリティ統括者」という。）　区における情報セキュリティ対策を統括し、情報セキュリティ管理者に情報システムの使用状況等について報告を求めるとともに、必要な指導及び助言を行う。

(3) 情報セキュリティ管理者（以下「セキュリティ管理者」という。）　その所掌する情報資産に関して次の職務を行う。

ア　情報システムの効率的かつ円滑な運用を図ること。

イ　個人情報などの秘密情報の保護を図ること。

ウ　情報機器等の保護対策を講じること。

エ　災害、過失等による障害、不正アクセス等に備えて、情報システムの適正な管理を行うこと。

オ　システム設計書、プログラム設計書等の資料の作成、整備、管理を行うこと。

カ　各情報システムの運用管理者を定め、その資質の向上に努めること。

キ　職員等に情報セキュリティ対策の内容を理解させ、実践させること。

ク　情報セキュリティ対策について外部委託事業者に遵守させ、責任体制を明確化すること。

(4) 情報セキュリティ総括管理者（以下「セキュリティ総括管理者」という。）　セキュリティ統括者を補佐し、セキュリティ管理者へ助言を行う。また、区の全庁に関わる

情報資産のセキュリティ管理者として、この基準に規定する職務を実施する。区の情報資産に対する侵害又は侵害のおそれのある場合には、セキュリティ統括者の指示に従い、その不在の場合には自らの判断に基づき、必要かつ十分な措置を行う。

(5) 情報化推進リーダー　セキュリティ管理者に情報セキュリティに必要な情報を提供するとともに、その指示によって課内の情報セキュリティ対策を推進する。

(6) 職員等　すべての職員等は、対策要綱、この基準及び第 28 条により定める規程を遵守しなければならない。

（教育・訓練）

第９条　セキュリティ統括者は、必要な説明会、研修等の実施により、すべての職員等が、対策要綱の趣旨とこの基準の内容を理解し、情報セキュリティ対策を実践するよう啓発しなければならない。

２　セキュリティ管理者は、情報化推進リーダーに対し、課内の情報セキュリティ対策の実践・啓発に関して指示することとする。

３　職員等は説明会、研修等に積極的に参加し、情報セキュリティの遵守、実践に努めなければならない。

（事故、障害に対する報告）

第 10 条　職員等は、情報セキュリティに関する事故、情報システムの障害などを発見した場合には、速やかにセキュリティ管理者に報告しなければならない。

２　セキュリティ管理者は、報告のあった事故等について、セキュリティ統括者に報告しなければならない。

３　セキュリティ統括者は、当該事故等について、最高統括責任者に報告するとともに、必要な措置について、セキュリティ管理者に指示するものとする。

４　セキュリティ管理者は、これらの事故等を分析し、再発防止のための情報として記録を保存しなくてはならない。

（ＩＤ、パスワード及びＩＣカード等の管理）

第 11 条　職員等は、自己の保有するＩＤ、パスワード又は課、係等の単位で共有するＩＤ、パスワードに関し、次の各号に掲げる事項を遵守しなければならない。

(1) ＩＤ、パスワードを秘密にし、照会等には応じないこと。

(2) パスワードに職員番号、生年月日など判明しやすい文字列を使用しない こと。また利用者間でパスワードを一致させないこと。

(3) 他者の目に触れる場所にＩＤ、パスワードのメモ等を作らないこと。

(4) 端末等にパスワードを記憶させないこと。

(5) 不正アクセスなどの危険が想定される場合には、パスワードを速やかに変更すること。

２　ＩＣカード等により利用者認証を行う場合、次の各号に掲げる事項を遵守しなければならない。

(1) ＩＣカード等毎に管理する職員を特定すること。

(2) ＩＣカード等を紛失した場合は速やかにセキュリティ管理者に連絡しその指示を受けること。また、連絡があり次第、当該ＩＣカード等によるアクセスを停止すること。

(3) ＩＣカード等はカードリーダ、端末等に常時挿入しないこと。

(業務目的外利用の禁止等)

第 12 条　職員等は、情報システムを利用する際には以下の各号に掲げる事項を遵守しなければならない。

(1) 業務目的以外で情報システムを使用してはならない。

(2) 許可若しくは権利のない情報資産へのアクセスを行ってはならない。

(3) 情報資産を格納した取り出し可能な記録媒体については、適切に管理することとし、複製の作成、課外への持ち出しはその目的を明らかにして、セキュリティ管理者の許可を受けなければならない。

(4) 使用する端末等や記録媒体について、第三者に使用されること、又は許可なく情報を閲覧されることがないように、細心の注意を払わなければならない。

(5) 職員等は秘密情報にアクセス可能とした状態で端末等を長時間にわたって離れてはならない。

(機器構成変更の制限)

第 13 条　職員等は、次項に定める場合を除いて、端末等に対し改造及び機器の増設、交換を行ってはならない。

２　業務を遂行するため、端末等に対し機器の増設、交換を行う必要がある場合は、セキュリティ管理者の許可を受けなければならない。

３　モデム等の機器を介して他のネットワークとの接続若しくは外部からのアクセスを可能とする仕組みを構築する必要がある場合は、セキュリティ総括者の許可を受けなければならない。

(ソフトウエア導入の制限)

第 14 条　職員等が業務上の必要から次の各号に掲げる行為をする場合には、個別にセキュリティ管理者の許可を受けなければならない。

(1) 新たにソフトウエアを端末等へインストールする場合（バージョンアップによるインストールを含む。）

(2) 端末等の各種設定を変更する場合

(ソフトウエア等のライセンス管理)

第 15 条　セキュリティ管理者はその所掌する情報システムにおけるソフトウエアの使用権を適正に管理しなければならない。

２　職員等は、情報システムの利用に際し、ソフトウエア、データの著作権等知的財産権の侵害がないよう注意しなければならない。

(コンピュータ及びネットワークの管理)

第 16 条　セキュリティ管理者は、情報システムについて、次の各号に掲げる措置を講じるものとする。

(1) 担当する情報システムにおいて行った設定変更等の処理、管理のため実施した作業について、運用管理者に対し、記録を作成させなければならない。

(2) セキュリティ管理者は、ネットワーク構成図、情報システム仕様書など、情報セキュリティの維持に重要な資料については、運用管理者など業務上必要とする者のみに閲

覧を許可するものとする。

2　セキュリティ管理者は、秘密情報を取り扱う情報システムについては、次の各号に掲げる措置を講じるものとする。

(1) 当該情報システムへのアクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存すること。

(2) アクセス記録等が窃取、改ざん、消去されないように必要な措置を講ずること。

(3) 定期的にアクセス記録等を監視、分析すること。

3　セキュリティ管理者は、外部と常時接続する情報システムについては、次の各号に掲げる措置を講じることとする。

(1) ネットワークへの不正アクセスを監視する装置を設置するなど、２４時間監視を行わなければならない。

(2) アクセス記録等が窃取、改ざん、消去されないように必要な措置を講ずる。

(3) 定期的にアクセス記録等を監視、分析する。

4　セキュリティ管理者は、職員等から報告のあった情報及び情報システムの障害に対する処理又は問題等について障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

5　セキュリティ管理者は、サーバ等に記録された情報資産について、重要度に応じて期間を設定し、定期的にバックアップを行わなければならない。

（アクセス制御）

第 17 条　情報システムについては、広く一般の利用に供するためのものを除き、正規の利用者以外の者が情報資産を使用できないよう、ＩＤ、パスワード及びＩＣカードなど、機器もしくは身体、音声、署名等を利用した情報システムなど、利用者と他の者を識別する（以下「利用者認証」という。）ための機能を備えなければならない。

2　利用者認証は利用者ごとに業務上必要な範囲で利用許可範囲を定め、原則として個人単位に登録することとする。なお、業務上、システム構築上やむを得ない場合のみ課、係など組織を単位として登録することができるものとする。

3　セキュリティ管理者は、利用者認証に関し、職員等の新規採用、異動、派遣及び退職に合わせ、登録、変更、抹消などを速やかに実施し、登録情報について適正な管理を行わなければならない。

4　セキュリティ管理者は、パスワードなど利用者認証に関する情報を厳重に管理しなければならない。パスワードは有効期間を定め、定期的に変更するものとする。

（管理者権限）

第 18 条　情報システムの管理者権限は、セキュリティ管理者が有することとし、その権限を代行する者は、運用管理者として当該システムの運用管理に携わる必要最小限の者を指名し、厳重に管理しなければならない。

（外部からのアクセス）

第 19 条　外部から区の情報システムにアクセスする場合は、外部アクセス用のサーバ等に対してのみ接続を許可することとし、直接内部のネットワークにアクセスしてはならない。

（開発前のセキュリティ統括者への協議）

第 20 条　セキュリティ管理者は、情報システムの新たな開発又は更新（以下「開発等」という。）を実施する前に、当該情報システムの情報セキュリティ対策について定め、セキュリティ統括者へ協議するものとする。

（設計時の情報セキュリティ確保）

第 21 条　情報システムの開発等を行う場合には、情報セキュリティの確保を図り、情報の漏洩や不正アクセス等への対策を施すよう設計しなければならない。

２　秘密情報を取り扱う情報システムの開発等を行う場合には、その内容に応じ、アクセス権の制限、ネットワークアクセスを制御する機器の導入、データの暗号化、独立したネットワークの構築など十分なセキュリティ対策を講じることとする。

３　外部のネットワークと接続する情報システムの開発等を行う場合には、外部アクセス用のサーバ、不正アクセスを防止するシステム等を介してのみ接続することとし、直接内部のネットワークに接続してはならない。また、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

４　一般の区民、事業者など職員等以外の者が利用する情報システムの開発等を行う場合は、必要に応じ他の情報システムと物理的に分ける等、情報セキュリティ対策について特に強固な対策を取らなければならない。

（開発時のセキュリティ確保）

第 22 条　情報システムを開発、更新、廃棄した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。

２　情報システムの調達にあたっては、一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

３　情報システムの開発及び保守を行う場合は、事故、不正行為対策のため、データの取り扱い、制限事項などを定めなければならない。

４　新たに情報システムを導入、又は更新する場合は、不具合及び他の情報システムとの相性の確認を行い、既に稼動している情報システム等に接続する前に十分な試験を行わなければならない。

（外部委託に関するセキュリティ確保）

第 23 条　情報システムの開発、導入又は保守等を外部の事業者に委託する場合、秘密情報の守秘義務及び情報セキュリティを確保するために受託事業者が遵守すべき事項を明らかにして契約を締結しなければならない。また、損害賠償等それらが遵守されなかった場合の規定を定めなければならない。

２　記憶媒体に秘密情報が記録された機器について外部の事業者に修理又は廃棄させる場合は、その情報が完全に消去された状態で行わなければならない。また、故障を外部の事業者に修理させる際、情報を消去することが難しい場合は、修理を委託する事業者に対して守秘義務に関する事項を明らかにして契約を締結しなければならない。

（コンピュータウイルス対策）

第 24 条セキュリティ総括者は、セキュリティ管理者、情報化推進リーダーを通じ、次の各号に掲げるコンピュータウイルス（以下「ウイルス」という。）対策を実施する。

(1) ウイルスの発生する可能性のあるすべての情報システムにウイルス対策ソフトウエアを導入し、ウイルスの検出と駆除を図る。

(2) ウイルスに関する最新の情報を収集し、速やかに職員等への周知に努める。

(3) サーバ及び端末において、定期的にウイルスチェックを行うよう職員等を指導する。

(4) ウイルス対策ソフトウェアのデータを、常に最新のものに保つよう職員等を指導する。

2　職員等は、情報システムへのウイルスの侵入とその拡散を防止するため次の各号に掲げる事項を遵守しなければならない。

(1) 外部から取得したファイル及び外部へ配布するファイルについて、すべてウイルスチェックを行うこと。

(2) 作成者、差出人が不明なファイル又は電子メールなどに不自然に添付されたファイルは速やかに削除すること。

(3) 最新のウイルス情報を常に確認すること。

(4) 添付ファイルのある電子メールを送受信する場合は、ウイルスチェックを行うこと。

(不正アクセス対策)

第25条　セキュリティ管理者は情報システムの不正アクセスの原因となるセキュリティ上のかし、不備の発見に努めるとともに、その改修を実施しなければならない。

2　セキュリティ統括者は、区の情報システムへ不正アクセスによる侵入などの攻撃を受けることが明確な場合には、情報システムの停止を含む必要な措置を講じなければならない。また、関係機関との連絡を密にして情報の収集に努めなければならない。

3　セキュリティ統括者は、攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号。以下「不正アクセス禁止法」という。）に違反するなど犯罪の可能性がある場合には、記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

4　職員等による不正アクセスがあった場合、セキュリティ統括者は当該職員等が所属する課、関係団体のセキュリティ管理者に通知し、適切な処置を求めなければならない。

(障害時対応手順の策定)

第26条　セキュリティ管理者は、障害が生じた場合、区民生活、事務運営に多大な影響が生じると思われる情報システムについて、業務ごとに代替措置を含めて、障害時の対応手順を定めるものとする。

(セキュリティ障害等の対応)

第27条　セキュリティ管理者は、その所掌する情報システムが稼動不能となる重大な障害若しくは情報システムへの不正アクセス等の侵害行為（以下「セキュリティ障害等」という。）が生じた場合、次の各号に掲げる措置を講じなければならない。

(1) 情報システムについてセキュリティ障害等を認めた場合、次の各号に掲げる事項について、可及的速やかにセキュリティ統括者に報告し、指示を受けること。

ア　セキュリティ障害等の内容

イ　セキュリティ障害等が発生した原因として、想定される行為

ウ　確認した被害・影響範囲

(2) 次の各号に掲げるセキュリティ障害等が発生した時は情報資産の防護のためにネットワークの切断、情報システムの停止など必要な措置を運用管理者に命じること。ただし、緊急を要する等、やむを得ない場合には、運用管理者の判断で切断、停止し、セキュリティ管理者への事後報告とすることができる。

ア　異常なアクセスが継続しているとき、又は不正アクセスが判明した場合

イ　情報システムの運用に著しい支障を来す攻撃が継続している場合

ウ　ウイルス等不正プログラムがネットワーク経由で拡大している場合

エ　その他情報資産に係る重大な被害が想定される場合

(3) セキュリティ障害等を認めた場合、次の記録を保存するものとする。

ア　セキュリティ障害等に係るアクセス記録等

イ　セキュリティ障害等への対処した経過

(4) 前号の証拠保全の実施を完了した後、当該セキュリティ障害等の発生した情報システムに再発防止の暫定措置を講じ、復旧すること。

(5) 当該セキュリティ障害等の原因調査を実施し、セキュリティ統括者と協議のうえ、情報セキュリティ対策の改善に係る再発防止策を作成し、最高情報統括責任者へ報告する。

2　セキュリティ統括者は、前項第１号の報告を受けた場合、当該セキュリティ障害等の調査を開始するとともに、最高情報統括責任者へ報告し、関係する他のセキュリティ管理者へ通知するものとする。

3　最高情報統括責任者は、前項の報告を受けた場合、必要に応じ、情報化推進本部へ報告するとともに、当該セキュリティ障害等による影響が生じると思われる庁外の個人及び法人並びに関係行政機関へ速やかに通知するものとする。

（情報システム運用規程の整備）

第 28 条　セキュリティ管理者はその所管する情報システムについて情報セキュリティ対策の具体的な実施手順（以下「運用規程」という）を、対策要綱及びこの基準に即し、セキュリティ総括者と協議のうえ定めることとする。

（情報セキュリティ対策の遵守状況の確認）

第 29 条　セキュリティ管理者は、運用規程に即して情報セキュリティ対策実施の有無又は問題発生の有無について常に確認を行い、問題が発生した場合には速やかにセキュリティ統括者に報告しなければならない。

2　セキュリティ統括者は、報告を受けた問題への対応について、セキュリティ管理者に助言又は指導するものとする。

（アクセス記録等の閲覧）

第 30 条　セキュリティ管理者は、前条の目的を達成するため、その所掌する情報システムの職員等へのアクセスの記録、電子メール等を閲覧できるものとする。

2　セキュリティ管理者は、前項の権限を実施する職員を指名することとし、その人数は必要最低限の数とする。

3　前項により指名された職員は、第１項による閲覧をセキュリティ管理者の指示のもと実施することとし、その実施状況についてセキュリティ管理者へ報告するものとする。

（法令等の遵守）

第 31 条　すべての職員等は、情報システムの運用にあたって、著作権法（昭和 45 年法律第 48 号)、不正アクセス行禁止法及び江戸川区個人情報保護条例（平成６年江戸川区条例第１号）の規定を遵守しなければならない。

（情報セキュリティ点検・監査）

第 32 条　セキュリティ管理者は情報セキュリティ対策の実施状況について定期的に点検を行い、セキュリティ統括者に報告しなければならない。

２　セキュリティ統括者は外部の専門的知識を有するものに委託し、主要な情報システムのセキュリティ機能、管理体制について定期的に監査を実施するものとする。

３　セキュリティ統括者は点検及び監査の結果をとりまとめ、最高情報統括責任者に報告するものとする。

４　最高情報統括責任者は前項の報告を情報化推進本部へ報告するものとする。

（指定管理者に関する措置）

第 33 条　指定管理者の業務における情報セキュリティを確保するため、対策要綱第 12 条に基づき、指定管理業務に関する協定等に定める措置は次のとおりとする。

(1) 指定管理者が実施する業務に、区が開発運用する情報システムを利用する場合、対策要綱及び対策基準に則して対策を実施すること。

(2) 指定管理者が、区に代わって実施する業務（以下「管理業務」という。）に、指定管理者が開発運用する情報システムを利用する場合（第三者が提供する情報サービスを利用する場合を含む。)、対策要綱及び対策基準に準じた情報セキュリティに関する方針を定め、これに即して情報システムの開発、運用を行うこと。

(3) 前２号に規定する業務において、指定管理者は情報セキュリティ対策の実施状況について定期的に点検を行い、区に報告を行うこと。

(4) 区は必要に応じて主要な情報システムのセキュリティ対策、管理体制について点検を行うことができること。

(5) 指定管理者が実施する管理業務以外の事業（以下「自主事業」という）及び法人内部の事務処理に係る業務に、指定管理者が開発運用する情報システムを利用する場合（第三者が提供する情報サービスを乙が利用する場合を含む。)、個人情報保護法その他関係法令に即した対応を図ること。

(6) 指定管理者の管理する情報システムにおいて、重大な障害若しくは不正アクセス等の侵害行為が生じた場合、速やかに区へ報告すること。

（見直しの実施）

第 34 条　この基準は､対策要綱の改正､情報セキュリティに関する技術的進展等を踏まえ、必要に応じて見直すものとする。

（その他）

第 35 条　この基準に定めるもののほか、この基準の実施に必要な事項は最高情報統括責任者が別に定める。

付　則

（施行期日）

1　この基準は、平成 14 年４月１日から施行する。

（経過措置）

2　この基準の適用開始日において、稼動済みの情報システムについて、この基準に適合しない事項がある場合は、１年以内に対応を図るものとする。

付　則

この基準は、平成 17 年 12 月 22 日から施行する

付　則

この基準は、平成 19 年４月 1 日から施行する