荒川区電子情報システムに係る情報セキュリティ対策基準

平成１５年４月１日制定
１５荒総情第７３号
（総務部長決定）
平成２１年１２月１１日一部改正
平成２７年１２月１６日一部改正

１　目的

この基準は、別に定めるもののほか、荒川区電子情報システム管理運営規程（平成１５年訓令甲第６号。以下「管理運営規程」という。）第２７条に基づき、情報セキュリティ対策等を実施するための具体的な事項及び判断基準等を定め、もって荒川区（以下「区」という。）の電子情報システムの適正な管理及び運用に万全を期することを目的とする。

２　定義

この基準で用いる用語の定義は、管理運営規程第２条に定めるとおりとする。

３　対象

(1) 適用範囲

本対策基準が適用される区の機関は、荒川区組織条例（昭和４０年荒川区条例第１号）により設置された部並びに議会事務局、教育委員会事務局、選挙管理委員会事務局及び監査事務局とする。

(2) 情報資産の範囲

本対策基準の対象は、次のとおりとする。

① 電子情報システム及びこれらに関する設備
② 電子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。）
③ 電子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

４　組織体制

(1) 体制の整備

情報統括責任者、システム管理部長及び電子情報システムを利用する部の長は、相互に連携、協働し、それぞれが管理又は利用する電子情報システムに係る情報資産に関し、情報セキュリティ対策を実施するために必要となる組織体制を整備しなければならない。

(2) 全庁的な調整

① 調整等の実施

情報統括責任者は、４－(1)の体制整備及びその見直しに当たり、全庁的な取扱いの統一化や情報セキュリティポリシーの遵守徹底を図る観点から、情報管理責任者をとおして必要な調整等を行う。

② ICT 推進員の活用

情報管理責任者は、４－(2)－①の調整に当たり、荒川区ＩＣＴ推進員設置要綱(平成１７年８月２５日荒総情第１８４号 助役決定)に基づき各所属に配属されたＩＣＴ推進員を活用するものとする。

５　情報資産の分類と管理

(1) 情報資産の分類

情報資産は、各々の機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行う。

① 機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	区の事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・私物パソコンでの作業を禁止する。 ・必要以上の複製及び配付を禁止する。 ・保管場所を制限する。 ・保管場所への必要以上の外部記録媒体等の持ち込みを禁止する。 ・送信、運搬及び提供時には、暗号化又はパスワード設定若しくは鍵付きケースへの格納等を行う。 ・廃棄に当たっては、復元不可能な処理を施す。 ・信頼のできるネットワーク回線を選択する。 ・外部で処理を行う際の安全管理措置を規定する。 ・外部記録媒体を施錠可能な場所へ保管する。
機密性２	区の事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	―

② 完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	区の事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は区の事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップを行う。 ・電子署名付与を行う。 ・外部で処理を行う際の安全管理措置を規定する。 ・外部記録媒体を施錠可能な場所に保管する。
完全性１	完全性２の情報資産以外の情報資産	―

③ 可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	区の事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は区の事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップを行う。 ・指定する時間以内の復旧を行う。 ・外部記録媒体を施錠可能な場所に保管する。
可用性１	可用性２の情報資産以外の情報資産	―

(2) 情報資産の管理又は利用方法

① 情報資産の管理及び取扱い

情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、所管する情報資産について、次のとおり管理及び取扱いを行わなければならない。

(ｱ) 情報資産の分類に従い、それぞれの情報資産についてアクセス権限を定める。

(ｲ) 情報資産が複製又は伝送(外部への送信を除く。)された場合には、複製等された情報資産についても５－(1)の分類に基づき管理する。

(ｳ) 許可なく職員(管理運営規定第２条第１８号の職員をいう。)、人材派遣により従事する者及び受託事業者（当該受諾事業者から再委託を受ける事業者を含む。以下同じ。）（以下、職員から受諾事業者までを一括して「職員等」という。)が情報資産の複製を外部へ持ち出し又は送付しないよう管理すること。

② 情報の作成

(ｱ) 職員等は、業務上必要のない情報を作成してはならない。

(ｲ) 情報を作成する者は、情報の作成時に５－(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ) 情報を作成する職員等は、作成途上の情報についても、紛失や流出等を防止する措置を講じなければならない。又、情報の作成途上で不要となった場合は、当該情報を消去しなければならない。

③ 情報資産を入手した場合の取扱い

(ｱ) 他の職員等が作成した情報資産を入手した職員等は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(ｲ) 職員等以外の者が作成した情報資産を入手した職員等は、５－(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ) 情報資産の分類が不明な情報資産を入手した職員等は、５－(1)の分類に基づき、当該情報の分類と取扱制限を定めるに当たって、情報システム課長又はシステム管理課長若しくは電子情報システムを利用する課の長に判断を仰がなければならない。

④ 情報資産の利用

(ｱ) 職員等は、業務以外の目的に情報資産を利用してはならない。

(ｲ) 情報資産を利用する職員等は、５－(1)の分類に応じ、当該情報資産を適切に取扱わなければならない。

⑤ 情報資産の保管

情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、情報資産の保管について、次の措置を講じなければならない。

(ｱ) ５－(1)の情報資産の分類に従って、情報資産を適切に保管する。

(ｲ) 情報資産を記録媒体により長期保管する場合は、当該記録媒体について書込禁止の措置を講じる。

(ｳ) 使用頻度の低い情報資産や電子情報システム上のデータのバックアップにより取得した情報資産を記録媒体で長期保管する場合は、地震等の自然災害を被る可能性が低い地域に保管する。

(ｴ) 機密性２以上又は完全性２若しくは可用性２に該当する情報を記録した記録媒体は、耐火、耐熱、耐水及び耐湿対策を講じた施錠可能な場所に保管する。

⑥ 情報の送信

情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、情報資産の送信について、次の措置を講じなければならない。

(ｱ) 記録媒体を外部へ送付する場合は、区と送付先との間で複製の禁止及び記録媒体の物理的保護に関する協定等を定める。

(ｲ) 機密性２以上の情報を電子メール等により送信する場合は、必要に応じ暗号化又はパスワード設定を行う。

⑦ 情報資産の運搬

職員等は機密性２以上の情報資産を車両等により運搬する場合、次の措置を講じなければなら

ない。
(ｱ) 情報システム課長又はシステム管理課長に許可を得ること。
(ｲ) 必要に応じ、鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正理由を防止するための措置を講じる。

⑧ 情報資産の提供・公表
(ｱ) 職員等は、機密性２以上の情報資産を外部に提供する場合は、事前に情報システム課長又はシステム管理課長の許可を得なければならない。
(ｲ) 職員等は、機密性２以上の情報資産を外部に提供する場合、必要に応じ、暗号化又はパスワードの設定を行わなければならない。
(ｳ) 情報システム課長及びシステム管理課長は、住民に公開する情報資産について、完全性を確保しなければならない。

⑨ 情報資産の廃棄
情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、情報資産が不要となった場合は、次の措置を講じなければならない。
(ｱ) 機密性２以上の情報資産を廃棄する場合、当該情報資産が記録された記録媒体の物理的破壊など情報資産を復元できない措置を行う。
(ｲ) 情報資産の廃棄に当たって実施した措置は、その日時、担当者及び処理内容を記録し、保管する。

６　人的セキュリティ対策

(1) 職員等の義務

職員等は、次の事項について遵守しなければならない。

①職員等は、情報セキュリティポリシーのほか、情報セキュリティポリシーに基づいて情報統括責任者及びシステム管理部長が定めるセキュリティ実施手順、管理運営規程第２１条に規定するセキュリティ委員会の決定事項その他情報資産の保護等に必要な事項を遵守しなければならない。

②職員等は、利用が許された電子情報システム以外のシステムにアクセスしてはならない。

③職員等は、利用する電子情報システムの端末装置や記録媒体について、情報システム課長又はシステム管理課長の許可なく第三者に利用され、又は閲覧されることがないよう、適切な措置を施さなければならない。

④職員等は、情報システム課長又はシステム管理課長の許可なく、情報資産の複写若しくは複製を行ってはならない。

⑤職員等は、情報システム課長又はシステム管理課長の許可なく、情報資産を記録した記録媒体を廃棄してはならない。

⑥職員等は、人事異動や退職等により当該業務への従事の任を解かれた場合には、利用していた情報資産を、情報システム課長又はシステム管理課長に返却しなければならない。又、任を解かれた後も、当該業務上で知り得た情報資産の内容等を秘匿しなければならない。

⑦職員等は、電子情報システムの利用にあたって、次の行為をしてはならない。
(ｱ) 業務目的以外での電子情報システムへのアクセス
(ｲ) 業務目的以外でのインターネットの使用
(ｳ) 業務目的以外での電子メールアドレスの使用
(ｴ) 業務目的以外での情報資産の外部持ち出し
(ｵ) 業務目的以外での標準装備以外のアプリケーションの端末装置へのインストール
(ｶ) アプリケーションの使用許諾契約に違反したアプリケーションの端末装置へのインストール
(ｷ) 情報システム課長又はシステム管理課長の許可なく行う端末の改造及び機器の増設又は交換等
(ｸ) モデム等の機器の増設等による外部ネットワーク環境への接続又は、外部からのアクセスを可能とする仕組みの新設
(ｹ) オンラインショッピング等の電子取引

(ｺ) 電子メールやインターネット等を利用した特定の個人や団体に対する誹謗中傷

⑧職員等は、電子情報システムに対する不正アクセスやコンピュータウィルスの侵入、電子情報システムに係る事故等の緊急に対応が必要な事態を発見した場合又は情報セキュリティポリシーに対する違反行為を発見した場合には、別に定める緊急時対応マニュアルの規定に即し、速やかに報告等を行わなければならない。

⑨職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

(ｱ) 個人利用のＩＤを他人に利用させない。

(ｲ) 共用のＩＤを利用する場合は、当該共用ＩＤの利用者以外に利用させない。

⑩職員等は、パスワードを使用する電子情報システムについて、次の事項を遵守しなければならない。

(ｱ) パスワードを秘密にし、パスワードの照会等には一切応じない。

(ｲ) パスワードは十分な長さとし、文字列は推測しにくいものとする。

(ｳ) パスワードを記載したメモを作成しない。

(ｴ) パスワードが流出した恐れがある場合には、情報システム課長又はシステム管理課長に速やかに報告し、パスワードを速やかに変更する。

(ｵ) パスワードは、定期的若しくはアクセス回数に基づいて変更し、変更前のパスワードの再利用は行わない。

(ｶ) 複数の電子情報システムを扱う職員等は、原則として、複数の電子情報システムで同一のパスワードを使用しない。

(ｷ) 電子情報システムの利用当初に配布された仮のパスワードは、当該電子情報システムへの最初のログイン時点で変更する。

(ｸ) 端末装置のパスワードの記録機能を利用しない。

(ｹ) パスワードを共有せざるを得ない電子情報システムを除き、職員等の間でのパスワード共有は行わない。

⑪職員等は、ＩＣカードや磁気カード(以下「ＩＣカード等」という。)を使用する電子情報システムについて、次の事項を遵守しなければならない。

(ｱ) 業務上必要のないときは、ＩＣカード等をカードリーダ若しくは端末のスロット等から抜いておく。

(ｲ) ＩＣカード等を紛失した場合には、速やかに情報システム課長及びシステム管理課長に通報し、指示を受ける。

⑫職員等は、ウィルス対策として、次の事項を遵守しなければならない。

(ｱ) 外部からデータまたはソフトウェアを取り入れる場合や添付ファイルのある電子メールを送受信する場合は、必ずウィルスチェックを行う。

(ｲ) 差出人が不明のメール又はメールに不自然に添付されたファイルを受信した場合は速やかに削除する。

(ｳ) ウィルスチェックの実行を途中で止めない。

(ｴ) 情報システム課長が提供するウィルス情報を常に確認する。

⑬職員等は、端末装置、記録媒体、情報資産及びソフトウエアを外部に持ち出す場合には、情報システム課長及びシステム管理課長の許可を得なければならない。

⑭職員等は、外部で情報処理業務を行う場合には、当該情報処理を行うパソコン等が私物であるか否かにかかわらず、情報システム課長又はシステム管理課長の許可を得なければならない。

⑮職員等は、６－(1)－⑭について、当該情報処理業務の対象が機密性２又は完全性２若しくは可用性２の情報資産である場合は、情報システム課長及びシステム管理課長の許可を得た上で、情報統括責任者が別途定める安全管理措置を遵守し、情報処理を行わなければならない。なお、機密性３の情報資産については、私物パソコンによる情報処理作業を行ってはならない。

⑯職員等は、私物のパソコン又は記録媒体等を庁舎内に持ち込んではならない。ただし、業務上必要な場合は、情報システム課長又はシステム管理課長の許可を得て、これらを持ち込むことができる。なお、私物パソコンの庁内ネットワークへの接続若しくは記録媒体等の庁内ネットワークに接続された端末機器等での利用については、情報システム課長及びシステム管理課長の許可を

得なければならない。
⑰職員等は、端末装置のソフトウエアに関するセキュリティ機能の設定について、情報システム課長又はシステム管理課長の許可なく変更してはならない。
⑱職員等は、端末装置や情報資産を記録する記録媒体又は文書等を第三者に使用させてはならない。又、職員等は情報システム課長又はシステム管理課長の許可なく第三者に情報資産を閲覧されることがないよう、離席時の端末装置のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

(2) 情報システム課長等の責務

①情報システム課長及びシステム管理課長は、ＩＣカード等を使用する電子情報システムについて、次のとおり対応しなければならない。
(ｱ) ＩＣカード等の紛失等の通報があった場合は、当該ＩＣカード等を使用した電子情報システムのアクセス等を速やかに停止する。
(ｲ) ＩＣカード等を切り替える場合は、切り替え前のカードをすべて回収し、破砕するなど復元不可能な処理を行った上で廃棄する。
②情報システム課長は、端末装置等の持出し及び持込みについて、記録を作成し、これを保管しなければならない。
③情報システム課長は、電子情報システムを利用する非常勤職員及び臨時職員に対し、情報セキュリティポリシーやセキュリティ実施手順等のうち、非常勤職員及び臨時職員が守るべき内容を理解させ、又、実施及び遵守させなければならない。
④情報システム課長は、職員等が常に情報セキュリティポリシーやセキュリティ実施手順等を閲覧できるように掲示しなければならない。
⑤情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、電子情報システムの開発、保守等を外部の事業者に委託する場合、情報セキュリティポリシーやセキュリティ実施手順等のうち、当該受託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。
⑥情報システム課長及びシステム管理課長は、６－(1)－⑧により、電子情報システムに係る事故等の緊急に対応が必要な事態の報告があった場合又は情報セキュリティポリシーに対する違反行為の報告で、これが直ちに情報セキュリティ上重大な影響を及ぼす可能性があると判断される場合は、緊急時対応マニュアルに従って適切に対処しなければならない。

(3) 教育及び訓練

①情報システム課長は、情報セキュリティ委員会の指示のもと、定期的又は必要に応じて職員等を対象とする情報セキュリティ対策に関する研修を行わなければならない。
②情報システム課長は、区の幹部職員を含めすべての職員等に対する情報セキュリティに関する研修計画を定期的又は必要に応じて立案しなければならない。

③情報システム課長は、毎年度、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。
④研修は、受講する職員等それぞれの役割や情報セキュリティに関する理解度等に応じたものにしなければならない。
⑤情報統括責任者は、緊急時対応を想定した訓練を定期的又は必要に応じて実施しなければならない。訓練計画は、電子情報システムやネットワークの規模等を考慮し、訓練実施の範囲等を定め、又、効果的に実施できるようにしなければならない。
⑥すべての職員等は、定められた研修及び訓練に参加しなければならない。

(4) 事故、欠陥等の報告

①職員等は、情報セキュリティに関する事故、電子情報システム上の欠陥及び誤動作を発見した場合、速やかに情報システム課が管理するものにあっては情報システム課長に、情報システム課以外の課が管理するものにあってはシステム管理課長に報告しなければならない。

②職員等は、電子情報システム又は情報資産に関する事故、欠陥等について、住民等外部から報告を受けた場合、情報システム課が管理するものにあっては情報システム課長に、情報システム課以外の課が管理するものにあってはシステム管理課長に報告しなければならない。
③職員等は、重要な電子メールを誤送信した場合、速やかに情報システム課長及びシステム管理課長に報告しなければならない。
④情報システム課長及びシステム管理課長は、職員等から事故等の報告を受けた時は、当該事故等について、必要に応じ、情報統括責任者に報告するものとする。
⑤情報統括責任者は、事故等を引き起こした部門のシステム管理課長及び当該電子情報システムを利用する課の長と連携し、当該事故等の原因等を分析するとともに、その記録を保存しなければならない。

7　物理的セキュリティ対策

(1) サーバ等の管理

情報システム課長及びシステム管理課長は、それぞれが管理する電子情報システムで用いるサーバ等について、次のセキュリティ対策を講じなければならない。

① 基幹システムの管理

ホストコンピュータを用いる電子情報システム(以下「基幹システム」という。)については、障害が発生した場合に適切に対応できるようデータを二重化する。

② サーバ等の二重化

基幹システム以外の電子情報システムで用いるサーバのうち、重要情報の格納及び住民サービスを取扱うサーバは、障害が発生した場合に適切に対応できるようサーバを二重化する。そのうえで、メインサーバに障害が発生した場合は、速やかにセカンダリサーバを起動し、電子情報システムの運用停止時間を最小限にする。

③ 装置の取付け等

電子情報システムを構成する電子情報処理装置は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置するとともに、容易に取り外せないよう固定する又はラックを施錠する等必要な措置を施す。

④ 電源の整備等

(ｱ) 電子情報システムを構成する電子情報処理装置のうち、サーバ等の機器の電源については、停電等による電源供給の停止があった場合でも、機器の適切な停止に必要かつ十分な電力を供給する容量の予備電源を備える。

(ｲ) サーバ等の機器は、落雷等による過電流から機器を保護するための措置を施す。

⑤ 配線の設置等

(ｱ) 情報システム課長又はシステム管理課長若しくは情報システム担当者(情報システム課長又はシステム管理課長から配線の変更等を認められた職員等をいう。)以外の者が配線を変更、追加してはならない。

(ｲ) 主要な配線は、配線収納管を使用する等、損傷等を受けることがないよう必要な措置を施す。又、主要な配線について、損傷等の定期的な点検を実施するとともに、庁舎管理担当など施設管理部門から配線の損傷等の報告があった場合には、施設管理部門と連携して必要な対応を行う。

(ｳ) 主要なネットワーク接続口については、第三者が容易に発見できない場所に設置するよう努める。

⑥ 機器の定期保守及び修理

(ｱ) 可用性２の情報資産を取扱うサーバ等の機器の定期保守を実施するよう努める。

(ｲ) 記録媒体を内蔵する機器の修理を外部の事業者に委託する場合は、記録内容を消去した状態で行わせるよう努める。なお、記録内容を消去できない場合、当該修理業務の受諾事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行うよう努める。

⑦ 庁舎外への機器の設置

庁舎の敷地外の設備等にサーバ等の機器を設置する場合、情報統括責任者の承認を得るとともに、定期的に当該庁舎外機器の情報セキュリティ対策状況について確認する。

⑧ 機器の廃棄等

サーバ等の機器の廃棄又はリース期間満了に伴う返却等をする場合、機器内部の記録装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じる。

(2) 設置場所の管理

情報システム課長及びシステム管理課長は、管理区域（電子情報システムを設置する施設(以下「情報システム室」という。)及び電磁的記録媒体の保管庫をいう。）について、次の対策を講じなければならない。

① 管理区域の設置等

(ｱ) 情報システム室から外部に通ずるドアは１箇所とし、施錠可能なものとする。又、情報システム室には、入口や室内の監視機能を持たせる。

(ｲ) 情報システム室に水害対策を講じるとともに、室内の機器等に転倒や落下防止等の耐震対策のほか、防火対策、防水対策等を講じる。

(ｳ) 管理区域に配置する消火薬剤や消防用設備等は、サーバ等の機器及び記録媒体等に影響を与えないように考慮する。

② 入退室管理

(ｱ) 管理区域への立ち入りは、許可された者のみとし、確実な入退室管理を行う。

(ｲ) 受託事業者を含め、外部の事業者が許可を得て管理区域へ立ち入る場合は、身分証明書等を携帯させ、必要に応じて提示させる。

(ｳ) 外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じる。

(ｴ) 機密性２以上の情報資産を扱う電子情報システムを設置している管理区域について、当該電子情報システムに関連しないコンピュータ、通信回線装置、外部記録媒体等を持ち込ませない。

③ 機器等の搬入出

(ｱ) 管理区域に機器等を搬入する場合は、既存の電子情報システムに与える影響について、あらかじめ職員等に確認を行わせる。

(ｲ) 情報システム室の機器等の搬入出に当たっては、職員を立ち会わせる。

(3) ネットワークの管理

情報システム課長及びシステム管理課長は、ネットワークについて、次の対策を講じなければならない。

① 庁内の通信回線及び通信回線装置を適切に管理する。又、通信回線及び通信回線装置に関連する文書を適切に保管する。

② 外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らすよう努める。

③ 地方公共団体間の通信については、総合行政ネットワーク（ＬＧＷＡＮ）に集約するよう努める。

③ 機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択する。又、必要に応じ、送受信される情報の暗号化を行なう。

④ ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないよう十分なセキュリティ対策を実施する。

(4) 端末装置の管理

情報システム課長及びシステム管理課長は、端末装置について、次の対策を講じなければならない。

① 端末装置は、盗難防止のためワイヤーによる固定等の措置を講じるとともに、許可なく職員等

が外部に持出せないよう管理する。
② 端末装置は、電子情報システムにログインする際にパスワード等の入力を必要とするよう設定する。
③ ７－(4)－②のログイン認証は、可能な限り、パスワード以外に指紋認証等の生体認証を併用するよう努める。

８　技術的セキュリティ対策

(1) 電子情報システムの管理

情報システム課長及びシステム管理課長は、それぞれが管理する電子情報システムについて、次のセキュリティ対策を講じなければならない。

① ネットワークの敷設

ネットワークの敷設については、原則として有線とする。

② アクセス記録の取得等

機密性２以上、完全性２又は可用性２の重要な情報を扱う電子情報システムについて、次の措置を講ずる。

(ｱ) 各種アクセス記録及びその他情報セキュリティの確保に必要な記録を取得し、これらを一定の期間保存する。
(ｲ) アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を施す。
(ｳ) 電子情報システムから自動出力したアクセス記録等は、必要に応じ、外部記録媒体にバックアップする。
(ｴ) アクセス記録等は、定期的又は必要に応じて分析や内容確認等を行う。

③ システム管理記録及び作業の確認

(ｱ) 電子情報システム運用上で実施した作業は、作業記録を作成する。
(ｲ) 電子情報システムの変更等の作業を行った場合は、作業内容について記録を作成し、改ざん、窃取等されないよう適切に管理する。

(ｳ) 情報システム課長又はシステム管理課長から当該電子情報システムの変更等の作業を認められた職員等が電子情報システムの変更等の作業を行う場合は、可能な限り２名以上で作業することとし、互いにその作業を確認する。

④ 障害等の記録

職員等から報告のあった電子情報システムの障害等に対する処理結果又は把握された問題等は、障害等の記録として体系的に記録し、常に活用できるよう保存する。

⑤ バックアップの実施

ファイルサーバ等に記録された情報資産について、二重化措置の有無に関わらず、必要に応じ、当該情報資産の重要度に応じて期間を設定し、定期的にバックアップを実施する。

⑥ 電子メールの設定等

(ｱ) 権限のない利用者により、外部から外部への電子メール転送（メールの中継処理）が行われることを不可能とする等、電子情報システム全般に悪影響を与えないよう設定を施す。
(ｲ) 電子メールの自動転送機能を用いた職場のメールの外部への転送を禁止する。
(ｳ) 機密性２以上又は完全性２若しくは可用性２の重要な情報資産については、原則として電子メールによる外部への送信を禁止する。ただし、外部への電子メールでの送信が不可欠な場合には、暗号化の措置を講ずる。
(ｴ) 複数人に対し電子メールを一括送信する際には、必要がある場合を除き、ＢＣＣ(ブラインドカーボンコピー)を使用し、他の送信先の電子メールアドレスが分からないようにする。
(ｵ) ウェブで利用できるフリーメール、ネットワークストレージサービス等の使用を禁止する。
(ｶ) 大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止する。
(ｷ) 電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能とする。

(ｸ) 職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知する。
(ｹ) 電子情報システムの開発や運用等のため庁舎内に常駐している受託事業者の作業員による電子メールアドレス利用について、受託事業者との間で利用方法を取り決める。

⑦ 職員グループウェアの運用(ファイルサービス関係)

(ｱ) 職員グループウェアのファイルサービスは課単位での利用を原則とし、他課のフォルダ及びファイルを閲覧、使用できないようサーバに設定を施す。
(ｲ) 個人情報や人事記録など特定の職員等に取扱いを限定している情報資産については、職員グループウェアのファイルサービスに別途ディレクトリを作成し、同一課内であっても、担当職員以外の職員等が閲覧及び使用できない設定を施す。
(ｳ) 職員グループウェアのファイルサービスは、職員等が使用できるフォルダの容量を設定し、職員等に周知すること。

⑧ 職員等以外の者が利用できるシステム

職員等以外の外部の者が利用できる電子情報システムについては、必要に応じ他のネットワーク及び電子情報システムと物理的に分離する等、情報セキュリティ対策について特に強固な対策をとる。

⑨ 他団体との情報システムに関する情報等の交換

他の団体との間で電子情報システムに関する情報及びソフトウエアを交換する場合、その取扱いに関する事項をあらかじめ定める。

⑩ 電子情報システム仕様書等の管理

電子情報システム仕様書やネットワーク構成図等は、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう適切に管理する。

⑪ ネットワークの接続制御、経路制御等

(ｱ) フィルタリング及びルーティングの設定の不整合が発生しないよう、ファイアウォールやルータ等の通信ソフトウエア等を設定する。
(ｲ) 不正アクセスを防止するため、ネットワークに適切なアクセス制御を施す。

⑫ 外部ネットワークとの接続制限等

(ｱ) 庁内ネットワークを外部ネットワークと接続しようとする場合には、情報統括責任者の許可を得る。
(ｲ) 接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認する。
(ｳ) 接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保する。
(ｴ) ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するため、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続する。
(ｵ) 接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、情報統括責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑬ 電子署名・暗号化

５－(1)の情報資産の分類により定めた取扱制限に従い、外部に送信する情報資産の機密性又は完全性を確保することが必要な場合には、電子署名、暗号化又はパスワード設定の方法を使用して、送信する。

⑭ 無許可ソフトウエアの導入等の禁止

(ｱ) 端末装置に無断でソフトウェアを導入させないための措置を講じる。
(ｲ) ソフトウェアの新規導入が業務上必要である場合は、情報システム課長の許可を得たうえで導入権限を付与する等の措置を講じる。
(ｳ) 不正にコピーしたソフトウェアを使用させないための措置を講じる。

⑮ 機器構成の変更の制限

(ｱ) パソコン等の端末装置に対し機器の改造及び増設・交換を行わない。
(ｲ) 業務上、パソコン等の端末装置に対し機器の改造及び増設・交換を行う必要がある場合には、情報システム課長の許可を得る。

⑯ 無許可でのネットワーク接続の禁止

情報システム課長の許可なく、職員等が端末装置をネットワークに接続させないための措置を講じる。

⑰ その他

職員等が利用できるプロトコルを、業務上必要最低限のものとする。

(2) アクセス制御

情報システム課長及びシステム管理課長は、それぞれが管理するネットワーク又は電子情報システムについて、次のアクセス制御を講じなければならない。

① 利用者登録

(ｱ) アクセス権限の認められない者が容易に操作できないように、電子情報システムの利用者の登録、変更、抹消及び登録情報の管理並びに異動、荒川区外への出向等の職員等及び退職者における利用者ＩＤの取扱い等について、定められた方法に従って行う。
(ｲ) 業務上必要がなくなった場合は、速やかに利用者登録を抹消する。
(ｳ) 利用されていないＩＤが放置されないよう、人事管理部門と連携し、定期的かつ必要に応じて随時点検を行う。

② 特権を付与されたＩＤの管理等

(ｱ) 管理者権限等の特権を付与されたＩＤを利用する職員等について、対象者を必要最小限にするとともに、パスワード等の漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理する。
(ｲ) 情報システム課長又はシステム管理課長が認めた職員等以外の者には、情報システム課長及びシステム管理課長の特権を代行させない。
(ｳ) 特権を付与されたＩＤ及びパスワードの変更は、情報システム課長又はシステム管理課長が認めた職員が実施することとし、受諾事業者を含め外部の事業者には行わせない。
(ｴ) 特権を付与されたＩＤ及びパスワードは、定期的に変更するほか、誤入力があった場合の入力回数制限等を設ける等、セキュリティ機能を強化すること。

③ インターネット以外のネットワークにおけるアクセス制御

インターネット以外のネットワークについては、ネットワークごとにアクセスできる職員等を定めること。

④ 経路の制御

インターネット等からの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す。

⑤ 外部アクセスの許可

(ｱ) 外部からのアクセスの許可は、アクセスが必要な合理的理由を有する必要最小限の者に限定する。
(ｲ) 外部アクセス用のサーバに対してのみ接続を許可することとし、原則として、直接内部のネットワークには接続させない。
(ｳ) 外部から持ち込んだ又は持ち帰ったパソコン等の端末装置を庁内のネットワークに接続しようとする場合は、コンピュータウイルスへの感染やセキュリティパッチの適用状況等を確認する。

⑥ 接続時間の制限

特権を付与されたＩＤ及びパスワードによる電子情報システムへの接続時間は、必要最小限に制限する。

⑦ 自動識別の設定

ネットワークで使用する機器は、機器固有の情報により端末装置とネットワークとの接続の可否が自動的に識別されるシステム設定とする。

⑧ ログイン時の表示等

電子情報システムへのログイン時におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン及びログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるシステム設定とする。

⑨ パスワードに関する情報の管理

(ｱ) 職員等のパスワードに関する情報を厳重に管理する。又、パスワードの不正利用を防ぐため、オペレーティングシステム等によるパスワード設定に係るセキュリティ強化機能がある場合は、これを有効に活用する。

(ｲ) 職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させる。

⑩ 外部ネットワークとの接続

外部ネットワークとの接続に当たっては、８－(1)－⑫に規定する措置に加え、８－(2)－①から⑨のアクセス制御のうち必要な措置をとる。

(3) システム開発、導入、保守等

情報システム課長及びシステム管理課長は、電子情報システムの開発、導入、保守等の調達にあたって、次の対策を講じなければならない。

① 電子情報システムの調達

(ｱ) 調達仕様書に必要とする技術的なセキュリティ機能を明記する。

(ｲ) 電子情報処理装置等の機器及びソフトウエアの調達にあたっては、当該製品のセキュリティ機能を調査し、区のセキュリティポリシー上問題のないことを確認する。

② 電子情報システムの開発

(ｱ) 電子情報システム開発の責任者、作業者及び作業場所を特定する。

(ｲ) 電子情報システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、当該開発用ＩＤを削除する。

(ｳ) 電子情報システム開発の責任者及び作業者のアクセス権限を設定する。

(ｴ) 電子情報システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定する。

(ｵ) 電子情報システムの開発に際して利用を認めたソフトウエア以外のソフトウエアが導入されている場合、当該ソフトウエアを当該電子情報システムから削除する。

③ 電子情報システムの導入

(ｱ) 電子情報システム開発や試験のための環境は、運用環境と分離する。

(ｲ) 電子情報システム開発や試験のための環境から運用環境への移行については、当該電子情報システム開発及び保守計画の策定時において手順を明確にする。

(ｳ) 新たな電子情報システムへの移行に際しては、従前の情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮する。

(ｴ) 新たに情報システムを導入する場合、既に稼働している他の電子情報システムに接続する前段階で十分な試験を行う。

(ｵ) 他の電子情報システムへの接続等の試験を行う場合、あらかじめ擬似環境を整備した上で操作等の確認を行う。

(ｶ) 個人情報及び機密性の高い情報資産を、テスト用データとして使用しない。

④ 開発や保守に関連する資料等の保管

(ｱ) 電子情報システム開発や保守等に関連する資料及び文書は、適切な方法で保管する。

(ｲ) 各種のテスト結果は、一定期間保管する。

(ｳ) 電子情報システムに係るソースコードは、適切な方法で保管する。

⑤ 入出力データの正確性の確保

(ｱ) 電子情報システムの設計にあたっては、当該電子情報システムに入力されるデータの範囲や妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むよう努める。

(ｲ) 電子情報システムは、情報処理が正しく反映され、出力されるよう設計する。

⑥ 情報システムの変更管理

電子情報システムを変更した場合は、プログラム仕様書等の変更履歴を作成する。

⑦ 開発・保守用のソフトウエアの更新等

電子情報システムの開発又は保守用のソフトウエア等を更新若しくはパッチの適用を行う場合、事前に他の電子情報システムとの整合性を確認する。

(4) 不正アクセス対策

情報システム課長及びシステム管理課長は、それぞれが管理するネットワーク又は電子情報システムについて、次の不正アクセス対策を講じなければならない。

① 不正アクセスに対して次の事項を実施する。

(ｱ) 使用終了若しくは使用される予定のないポートを閉鎖する。

(ｲ) セキュリティホール等の脆弱性の発見に努め、メーカー等からパッチ等の提供があり次第、速やかにパッチを適用する。

(ｳ) 不正アクセスによるウェブページの改ざんを検出し、情報システム課長又はシステム管理課長へ通報するよう、設定する。

② 攻撃を受けることが明確な場合には、緊急時対応マニュアルの定めるところに従い電子情報システムの停止を含む必要な措置を講ずる。又、各機関との連絡を密にして関連情報の収集に努める。

③ 攻撃を受けることが明確である場合は、データの漏えい、破壊、改ざん又はシステムダウン等により業務に深刻な影響をもたらさないよう備える。

④ 攻撃を受け、当該攻撃が不正アクセス禁止法違反等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や関係機関との緊密な連携に努める。

⑤ 職員等が使用しているパソコン等の端末装置からの不正アクセスや庁内のサーバ等に対する攻撃、外部のサイトに対する攻撃を監視する。又、職員等による不正アクセス等を発見したときは、当該職員等の所属長（受諾事業者の従業員の場合は当該受諾事業者の責任者。以下同じ。）に通知し、適切な処置を求める。

(5) 不正プログラム対策

情報システム課長及びシステム管理課長は、それぞれが管理するネットワーク又は電子情報システムについて、次の不正プログラム対策を講じなければならない。

① 外部のネットワークから受信したファイルは、ルータ、ファイアウォール、ゲートウェイサーバ、侵入検知システム、業務用サーバ、端末装置等において２箇所以上ウィルス等の不正プログラムのチェックを行い、電子情報システムへの侵入を防止する。

② 外部のネットワークへ送信するファイルは、８－(5)－①と同様にウィルス等の不正プログラムのチェックを行い、外部へのウィルス拡散を防止する。

③ 不正プログラム対策として次の事項を実施する。

(ｱ) ウィルス等の不正プログラム情報について職員等に対する注意喚起を行う。

(ｲ) 常時ウィルス等の不正プログラムに関する情報収集に努める。

(ｳ) 所掌するサーバ及び端末装置に、ウィルス等の不正プログラム対策ソフトウエアを常駐させる。

(ｴ) 不正プログラム対策ソフトウエアのパターンファイルを最新のものに保つ。

(ｵ) 不正プログラム対策のソフトウエアは、最新の状態に保つ。

(ｶ) インターネットに接続していないシステムにおいても、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウエアを導入し、定期的に当該ソフトウエア及びパターンファイルの更新を実施する。

④ 不正プログラム対策として、職員等に次の事項を遵守させる。

(ｱ) 端末装置に不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更しない。

(ｲ) 外部からデータ又はソフトウエアを取り入れる場合には、必ず不正プログラム対策ソフト

ウエアによるチェックを行う。

(ｳ) 差出人が不明のメール又は不自然に添付されたファイルを受信した場合は、速やかに削除する。

(ｴ) 端末装置に対し、不正プログラム対策ソフトウエアによるフルチェックを定期的に実施する。

(ｵ) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行う。

(ｶ) 情報システム課長が提供するウィルス情報を常に確認する。

(ｷ) ウィルス等の不正プログラムに感染した場合は、ＬＡＮケーブルの即時取り外し又は機器の電源遮断を行う。

(6) セキュリティ情報の収集

情報システム課長及びシステム管理課長は、次のとおりセキュリティ情報の収集を行わなければならない。

① 情報システム課長は、セキュリティに関する情報を収集しこれを取りまとめるとともに、必要に応じてシステム管理課長及びシステム利用課長に通知する。

② システム管理課長は、情報システム課長からの通知及び自らが収集したセキュリティに関する情報をもとに、所管する電子情報システムについて、必要なセキュリティ対策を講じる。

９　運用面におけるセキュリティ対策

(1) 端末装置に保有する情報資産の保護

① 職員等は、原則として、機密性２以上又は完全性２若しくは可用性２に該当する情報資産を端末装置で保存又は管理してはならない。

② 職員等は、合理的かつ止むを得ない理由により、機密性２以上又は完全性２若しくは可用性２に該当する情報資産を端末装置で取扱う場合には、パソコンのログインパスワードの設定、グループウェアのファイリング機能又は指紋認証ユーザログイン認証機能等を活用するものとする。

(2) 電子情報システムの監視

情報統括責任者及びシステム管理部長は、所管する電子情報システムについて、情報システム課長及びシステム管理課長に次の監視を行わせなければならない。

① セキュリティに関する問題等の発生を即時に検知するため、電子情報システムの常時監視を行う。

② 外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、接続している間監視を行う。

③ 重要なアクセスログ等を取得するサーバについて、正確な時刻設定及びサーバ間の時刻同期ができる措置を講じる。

④ 監視により得られた結果については、消去や改ざんを防止するために必要な措置を施すとともに、記録媒体により定期的に安全な場所に保管する。

(3) 情報セキュリティ対策の遵守状況の確認及び対処

① 情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、セキュリティ対策が遵守されているか否か、又、セキュリティに関する問題等が発生していないかについて常に確認を行い、問題が発生している場合には速やかに情報統括責任者に報告しなければならない。

② 情報統括責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

③ 情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、電子情報システムの設定等における情報セキュリティポリシーの遵守状況について定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

(4) 端末装置及び記録媒体等の利用状況調査

情報統括責任者及び情報統括責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末装置、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

(5) 緊急事態への対応

情報システム課長、システム管理課長及び電子情報システムを利用する課の長は、情報資産への侵害若しくは障害が発生した場合、又は侵害若しくは障害の発生が明らかに想定できる場合、緊急時対応マニュアルに基づき、連絡、証拠保全、被害拡大の防止、復旧等、必要な措置を迅速かつ円滑に実施するとともに、再発防止の措置を講じなければならない。

(7) 外部委託

情報システム課長及びシステム管理課長は、電子情報システムの開発や運用等の業務を外部委託する場合には、次の事項に十分留意しなければならない。

① 受諾事業者の選定

(ｱ) 委託内容に応じた情報セキュリティ対策を確実に実施できる事業者を選定する。

(ｲ) 情報セキュリティマネジメントシステムの国際規格の認証取得状況等を参考にして事業者を選定する。

② セキュリティ要件の明記

受諾事業者との契約の締結にあたっては、必要に応じ、契約書又は仕様書若しくはその他契約関係書類に次のセキュリティ要件を明記する。

(ｱ) 区の情報セキュリティポリシー及び情報セキュリティポリシーに基づいて情報統括責任者及びシステム管理部長が定めるセキュリティ実施手順の遵守

(ｲ) 受諾事業者の責任者及び作業者、委託業務の内容や作業場所の特定

(ｳ) 契約に基づいて受諾事業者が提供するサービスレベルの保証

(ｴ) 受託者の従業員に対する教育の実施

(ｵ) 区が提供する情報資産の目的外利用及び受託事業者による第三者への提供の禁止

(ｶ) 業務上知り得た情報の守秘義務

(ｷ) 再委託に関する制限事項の遵守

(ｸ) 委託業務終了時の情報資産の返還、廃棄等

(ｹ) 委託業務の定期報告及び緊急時報告義務

(ｺ) 区による監査、検査

(ｻ) 区による事故時等の公表

(ｼ) 情報セキュリティポリシーが遵守されなかった場合の損害賠償等に関する規定

③ 確認・措置等

契約締結後は、受諾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定期的に確認のうえ、必要に応じて、当該契約に係る契約書条項又は仕様書若しくはその他契約関係の規定に基づき、必要な措置を講じる。

(8) 例外措置

① 例外措置の許可

情報システム課長及びシステム管理課長は、情報セキュリティポリシー等のセキュリティ関係規定を遵守することが困難な状況にある場合において、区の事務の適正な遂行を継続するため、遵守事項とは異なる方法等を採用し又は規定された遵守事項を実施しないことについて合理的な理由がある場合には、情報統括責任者の許可を得たうえで、例外措置を取ることができる。

② 緊急時の例外措置

情報システム課長及びシステム管理課長は、区の事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、これを実施し、事後速やかに情報統括責任者に報告するものとする。

③ 例外措置の申請書の管理

情報統括責任者は、例外的な措置に係る情報システム課長又はシステム管理課長からの申請書及び審査結果並びに事後報告等を適切に保管しなければならない。

(9) 違反への対応等

① 懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じ、地方公務員法による懲戒処分の対象とする。

② 違反時の措置

情報システム課長又はシステム管理課長は、職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

(ｱ) 違反を確認した場合、当該職員等の所属長に通知し、適切な措置を求める。

(ｲ) 所属長の指導によっても改善されない場合は、必要に応じて、当該職員等の電子情報システムを使用する権利を停止又は剥奪する。権利の停止又は剥奪の措置を行った場合は、その旨を情報統括責任者及び当該所属長に通知する。

１０　法令遵守

職員等は、職務の遂行において使用する情報資産を保護するため、次に揚げる法令その他関係する法令等を遵守し、これに従わなければならない。

①刑法（明治４５年法律第１５３号）
②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）
③著作権法（昭和４５年法律第４８号）
④地方公務員法（昭和２５年法律第２６１号）
⑤個人情報の保護に関する法律（平成１５年法律第５７号）
⑥行政機関の保有する個人情報の保護に関する法律（平成１５年法律第５８号）
⑦住民基本台帳法(昭和４２年法律第８１号)
⑧荒川区個人情報保護条例(平成８年条例第２８号)
⑨荒川区住民基本台帳ネットワークシステムの適正管理等に関する条例(平成１５年条例第２号)
⑩荒川区住民基本台帳ネットワークシステム運営規程（平成１４４年訓令甲第９号）
⑪荒川区電子情報システム管理運営規定(平成１５年訓令甲第６号)
⑫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）

１１　評価・見直し

(1) 監査の実施

① セキュリティ委員会（管理運営規定第 20 条の情報セキュリティ委員会をいう。）は、情報セキュリティポリシーの遵守状況を検証するため、電子情報システムに係るセキュリティ対策について監査を実施する。

② １１－(1)－①のセキュリティ対策に係る監査（以下、「セキュリティ監査」という。）は、実施計画を策定のうえ、定期的に又は必要に応じ、対象となる電子情報システムを指定して行うものとする。

③ 指定された電子情報システムを管理する情報システム課長及びシステム管理課長並びに当該電子情報システムを利用する課の長は、セキュリティ監査の実施に協力しなければならない。

④ セキュリティ委員会は、原則として、指定した電子情報システムを管理又は利用する部課等から独立した者にセキュリティ監査の実施を依頼する。

⑤ セキュリティ監査の範囲は、受託事業者に委託している場合、受託事業者が再委託した事業者も含めるものとする。

⑥ セキュリティ委員会は、監査結果を踏まえ、情報システム課長又はシステム管理課長若しくは電子情報システムを利用する課の長に対し、指摘事項を通知するとともに、当該指摘事項への

対処を指示する。又、当該指摘事項について、他の電子情報システムにおいても同種の課題及び問題点が生じる可能性が高いなどと認められる場合には、当該指摘事項の対象となっていないシステム管理課長又は電子情報システムを利用する課の長に対しても、当該課題及び問題点の有無を確認させるものとする。

⑦ セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用する。

⑧ セキュリティ委員会は、セキュリティ監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書等を、紛失等がないよう適切に保管しなければならない。

(2) 自己点検の実施

① 情報システム課長及びシステム管理課長並びに電子情報システムを利用する課の長は、情報セキュリティポリシーの遵守状況を検証するため、電子情報システムに係るセキュリティ対策について、定期的に又は必要に応じて自己点検を実施する。

③ 情報システム課長及びシステム管理課長並びに電子情報システムを利用する課の長は、１１－（2）－①のセキュリティ対策に係る自己点検（以下、「セキュリティ自己点検」という。）を実施した時は、その結果及び結果に基づく改善策を取りまとめ、セキュリティ委員会に報告しなければならない。

③ 情報システム課長及びシステム管理課長並びに電子情報システムを利用する課の長は、セキュリティ自己点検に基づく改善策の具体化を図るとともに、職員等に対し、それぞれの権限の範囲内で改善や工夫等を行うよう働きかけるものとする。

④ セキュリティ委員会は、セキュリティ自己点検の結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用する。

(3) 情報セキュリティ対策の更新

セキュリティ委員会は、セキュリティ監査やセキュリティ自己点検の結果、又は新たな情報セキュリティ対策の必要性が生じた場合は、それまでのセキュリティ対策の実効性を評価し、その内容の見直し等を行い、セキュリティ対策を更新しなければならない。

１２　実施手順

情報統括責任者及びシステム管理部長は、より具体的な情報セキュリティ対策に関する基準を定める必要がある場合には、それぞれの電子情報システムに応じたセキュリティ実施手順を個別に定めることができる。

１３　施行

この基準は、平成２７年１２月１６日から施行する。