杉並区議会情報セキュリティ対策基準

（令和８年３月19日杉議会第1241号）

目次

第１章　総則

（目的）

第１条　この基準は、杉並区議会情報セキュリティ基本方針（以下「基本方針」という。）に基づき、杉並区議会（以下「議会」という。）が保有する情報資産を適正に管理するために実施すべき情報セキュリティ対策について定めることを目的とする。

（定義）

第２条　この基準において使用する用語の意義は、基本方針及び杉並区電子計算組織の管理運営に関する規則（昭和62年杉並区規則第52号）で使用する用語の例による。

２　前項の規定にかかわらず、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）　情報セキュリティポリシー　基本方針及びこの基準をいう。

（２）　情報セキュリティインシデント　区民の権利が侵害され、又は業務の適確な遂行に重大な支障を及ぼし、情報セキュリティを脅かす事件・事故をいう。

（３）　端末等　パソコン、モバイル端末等のコンピュータ及びそれに付随する装置をいう。

（４） 課　杉並区会計事務規則（昭和39年規則第５号）第２条第１号に規定する課をいう。
（５） 職員等　地方公務員法（昭和25年法律第261号）第３条に規定する一般職の職員及び特別職の職員のうち、議会事務局の職員であって、議会の情報資産を取り扱うものをいう。
（６） 住民情報系　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11項に規定する個人番号利用事務等に係る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。

（対象範囲）

第３条　この基準が適用される機関の範囲は、議会とする。

２　この基準が適用される施設・設備の範囲は、議会において管理する施設・設備とする。ただし、庁内ネットワーク及び庁内ネットワークを利用する端末の維持管理等に関して実施する対策は、区長部局において政策経営部情報システム担当課長（以下「情報システム担当課長」という。）が実施する対策の例による。

３　この基準は、次に掲げる議会の情報資産を対象とする。ただし、議会事務局の職員が職務上作成し、又は取得したものに限る。

（１） 杉並区文書等管理規程（平成15年杉並区訓令甲第30号）第２条第１号に定める文書等
（２） 情報システム及びネットワーク
（３） 情報システム及びネットワークで取り扱う情報並びにこれらを記録した文書等

（組織）

第４条　議会の情報資産の管理及び情報セキュリティ対策を適切に実施するため、電算管理責任者のほか、情報セキュリティ統括責任者及び情報セキュリティ責任を置く。

２　情報セキュリティ統括責任者は、区議会事務局長をもって充てる。

３　情報セキュリティ責任者は、区議会事務局次長をもって充てる。

（情報セキュリティ統括責任者の役割）

第５条　情報セキュリティ統括責任者は、次に掲げる役割を担う。

（１） 情報セキュリティ対策に関する最終的な決定
（２） 情報セキュリティ責任者及び電算管理責任者に対する指導及び助言

（情報セキュリティ責任者の役割）

第６条　情報セキュリティ責任者は、次に掲げる役割を担う。

（１） 情報セキュリティ対策の運用
（２） 情報セキュリティ研修の実施
（３） 情報セキュリティに関する区長部局との連絡調整
（４） 緊急時の情報共有のための連絡体制の整備
（５） 情報セキュリティ実施手順の策定、維持及び管理
（６） 緊急時対応計画の策定、維持及び管理

（兼務の禁止）

第７条　情報セキュリティ対策の実施において、やむを得ない場合を除き、その承認又は許可の申請を行う者とその承認者又は許可者は、兼務してはならない。

第２章　情報資産の分類と管理方法

（情報資産の分類）

第８条　議会の情報資産は、重要度（機密性、完全性及び可用性）により、別表のとおり分類し、分類に応じた取扱制限を行う。

２　別表に基づき分類される情報資産を、次のとおり定義する。

（１） 機密資産　機密性２以上に分類される情報資産
（２） 完全資産　完全性２に分類される情報資産
（３） 可用資産　可用性２に分類される情報資産

（４） 重要資産　機密資産、完全資産又は可用資産のいずれかに該当する情報資産
（５） 最重要資産　機密資産、完全資産及び可用資産の全てに該当する情報資産
（情報資産の管理責任）
第９条　情報セキュリティ責任者は、議会で保有する情報資産（以下「保有情報資産」という。）について管理責任を有する。
２　情報セキュリティ責任者は、保有情報資産を別表の分類に基づき管理しなければならない。また、保有情報資産が複製又は伝送された場合には、複製等された情報資産についても同表の分類に基づき管理しなければならない。
（情報資産目録の作成）
第10条　情報セキュリティ責任者は、情報資産目録を作成しなければならない。
２　情報セキュリティ責任者は、年１回以上は情報資産目録を点検しなければならない。
（情報資産の分類の表示）
第11条　職員等は、最重要資産及び重要資産（以下「重要資産等」という。）について、ラベルの添付等により、当該情報資産の分類及び取扱制限が分かる措置を講じなければならない。
（情報資産の作成）
第12条　職員等は、業務上必要のない情報資産を作成してはならない。
２　情報資産を作成する者は、情報資産の作成時に別表の分類に基づき、当該情報資産の分類と取扱制限を定めなければならない。
３　情報資産を作成する者は、作成途上の情報資産についても、紛失、流出等を防止しなければならない。また、情報資産の作成途上で不要になった場合は、当該情報資産を速やかに消去しなければならない。
（情報資産の入手）
第13条　議会が作成した情報資産を入手した者は、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。
２　議会が作成したものではない情報資産を入手した者は、別表の分類に基づき、速やかに当該情報の分類と取扱制限を定めなければならない。
３　情報資産を入手した者は、入手した情報資産の分類が不明な場合は、情報セキュリティ責任者に報告し、その取扱いについて指示を受けなければならない。
（情報資産の利用）
第14条　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
２　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
３　情報資産を利用する者は、電磁的記録媒体に分類が異なる情報資産が複数記録されている場合は、最も高位の分類に従って、当該電磁的記録媒体を取り扱わなければならない。
（情報資産の保管）
第15条　情報セキュリティ責任者は、別表の分類に従って、情報資産を適切に保管しなければならない。
２　情報セキュリティ責任者は、情報資産を記録した電磁的記録媒体を長期間保管する場合は、書込禁止の措置を講じなければならない。
３　情報セキュリティ責任者は、重要資産等を記録した電磁的記録媒体を保管する場合は、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施錠保管しなければならない。
４　情報セキュリティ責任者は、電磁的記録媒体である最重要資産を長期間保管する場合は、遠隔地等の地震、水害、火災その他の自然災害の影響を受ける可能性が低い場所に保管しなければならない。
（情報の送信）
第16条　外部のネットワークを利用した電子メール等により、機密資産の情報を送信する者

は、当該情報に対してパスワード等による暗号化を行わなければならない。

（情報資産の持ち出し・運搬）

第17条　重要資産等を庁内から外に持ち出す者は、あらかじめ情報セキュリティ責任者の承認を得なければならない。

２　機密資産を運搬する者は、常に身体に密着させて携行する、施錠可能なケース等に格納する、当該情報が電子データの場合はパスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（情報資産の提供）

第18条　電子データの機密資産を外部に提供する者は、当該情報に対してパスワード等による暗号化を行わなければならない。

（情報資産の公表）

第19条　情報セキュリティ責任者は、公表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。

（情報資産の廃棄）

第20条　機密資産を記録した紙媒体を廃棄する者は、破砕、溶解等し、情報が判別不可能な状態にした上で廃棄しなければならない。

２　機密資産を記録した電磁的記録媒体の廃棄、リース返却等を行う者は、当該電磁的記録媒体に記録される情報を物理的又は論理的に消去し、情報が復元不可能な状態にした上で廃棄又はリース返却等しなければならない。

３　重要資産等の廃棄、リース返却等を行う者は、あらかじめ情報セキュリティ責任者の承認を得なければならない。

４　重要資産等の廃棄を行う者は、行った処理について、情報資産名、日時、廃棄を行った職員等及び処理内容を記録しなければならない。

（取扱いに関する特別の定めがある情報資産）

第21条　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。）を含む情報資産及び住民基本台帳ネットワークシステム（電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成14年総務省告示第334号）第１の１に規定する住民基本台帳ネットワークシステムをいう。）並びに情報提供ネットワークシステム（番号法第２条第15項に規定する情報提供ネットワークシステムをいう。）を構成する情報資産の取扱いに当たっては、第８条から前条までの規定に基づくとともに、法律、条例、規則、要綱及び要領に特別の定めがある場合は、その定めるところによらなければならない。

第３章　情報システム全体の強靭性の向上

（情報のアクセス及び持ち出しにおける対策）

第22条　電算管理責任者は、住民情報系では、情報システムが正規の利用者かどうかを判断する認証手段のうち、「知識」、「所持」又は「存在」を利用する認証手段のうち二つ以上を併用する認証（以下「多要素認証」という。）を利用しなければならない。

第23条　電算管理責任者は、住民情報系では、原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

（住民情報系と接続されるクラウドサービス上での情報システムの扱い）

第24条　電算管理責任者は、住民情報系の端末及びサーバ等と専用回線により接続されるガバメントクラウド等上の情報システムの領域については、住民情報系として扱い、区の他の領域とはネットワークを分離しなければならない。

（住民情報系と接続されるクラウドサービス上での情報資産の取扱い）

第25条　電算管理責任者は、住民情報系の情報システムをガバメントクラウド等において利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。この場合において、暗号は十分な強度を持たなければならない。

２　クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、電算管理責任者は、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

第４章　物理的セキュリティ

第１節　サーバ等の管理

（サーバ等の管理）

第26条　電算管理責任者は、サーバ及びその周辺機器（以下「サーバ等」という。）の取付けを行う場合は、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し、容易に取り外せないよう適切に固定する等、適切な措置を講じなければならない。

（サーバの冗長化）

第27条　電算管理責任者は、サーバ等の冗長化について、必要性を検討し、必要が認められる場合は実施しなければならない。

（機器の電源）

第28条　電算管理責任者は、サーバ等の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間、十分な電力を供給することができる容量を持った予備電源を確保しなければならない。

２　電算管理責任者は、落雷等による過電流に対して、サーバ等を保護するための措置を講じなければならない。

（通信ケーブル等の配線）

第29条　電算管理責任者は、通信ケーブル及び電源ケーブルの損傷等を防止するために、主要な箇所の通信ケーブルの配線に当たっては、配線収納管を使用する等必要な措置を講じなければならない。

２　電算管理責任者は、所管する通信ケーブルのうち、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合は、連携して対応しなければならない。

３　電算管理責任者は、所管する通信ケーブルのネットワーク接続口（ハブのポート等）に、あらかじめ認めた者以外の者が接続することを防ぐための措置を講じなければならない。

４　電算管理責任者は、所管する通信ケーブルの配線を公共の場所に露出しない等、あらかじめ認めた者以外の者による配線の変更又は追加を防ぐための措置を講じなければならない。

（機器の定期保守及び修理）

第30条　電算管理責任者は、重要資産等を扱う機器について定期的に保守しなければならない。

２　電算管理責任者は、機密資産を記録する機器を外部の事業者に修理させる場合は、次に掲げるいずれかの措置を講じなければならない。

（１）　記録されたデータを消去した上で修理させること。

（２）　記録されたデータを消去できない場合は、あらかじめ事業者における安全管理体制を確認するとともに、事業者との間で守秘義務契約を締結した上で修理させること。

（庁外への機器の設置）

第31条　電算管理責任者は、庁外にサーバ等を設置する場合は、杉並区デジタル・セキュリティ部会（杉並区デジタル・セキュリティ部会設置要領（令和５年３月31日杉並第70067号）第１条に規定する部会をいう。以下「部会」という。）の承認を得なければならない。

２　サーバ等で個人情報を取り扱う場合は、前項の手続に加え、杉並区議会個人情報の保護に関する安全管理措置等基準（令和８年３月２日杉議会第1172号。以下「安全管理措置基準」という。）に定める手続を経なければならない。

３　電算管理責任者は、庁外に設置したサーバ等について、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（機器の廃棄等）

第32条　電算管理責任者は、サーバ等を廃棄、リース返却等をする場合は、あらかじめ記録された情報を消去し、情報が復元不可能な状態にしなければならない。

（職員等の業務端末等の管理）

第33条　電算管理責任者は、業務で利用する端末等（以下「業務端末等」という。）について、ワイヤーによる固定、施錠管理等の盗難防止のための物理的措置を講じなければならない。

２　電算管理責任者は、業務端末等に接続する電磁的記録媒体について、情報が保存される必要がなくなった時点で速やかに記録された情報を消去しなければならない。

３　電算管理責任者は、業務端末等に接続する電磁的記録媒体のうち重要資産等を記録するものについて、データ暗号化機能を備える媒体を使用する等、不正利用を防止するための措置を講じなければならない。

４　電算管理責任者は、情報システムへのログインについては、ログインパスワード等の認証情報の入力を必要とするよう、住民情報系又は住民情報系を操作する端末へのログインについては、多要素認証を行うよう設定しなければならない。

５　電算管理責任者は、最重要資産を取り扱う業務端末等について、次に掲げる措置を検討し、必要なものを採用しなければならない。

（１）　電源起動時のパスワード（ＢＩＯＳパスワード、ハードディスクパスワード等）の併用

（２）　指紋認証等の二要素認証の併用

（３）　データの暗号化等の機能の有効化

（４）　セキュリティチップが搭載されている場合は、その機能の有効化

第２節　区画の管理

（管理区画）

第34条　管理区画とは、次に掲げる室をいう。

（１）　重要資産等である情報システム及びネットワーク機器を設置し、当該機器等の管理及び運用を行うための室（以下「情報システム室」という。）

（２）　重要資産等が保管される室

（管理区画の構造等）

第35条　情報セキュリティ責任者は、管理区画を定める場合には、当該室に設置又は保管される情報資産の分類に応じて、次に掲げる要件を検討し、必要なものを採用しなければならない。

（１）　地階又は１階に設けないこと。

（２）　外部からの侵入が容易にできないように無窓の外壁にすること。

（３）　外部に通ずる扉は必要最小限とし、鍵、監視カメラ、警報装置等によって許可されていない立入りを防止すること。

（４）　外壁等の床下開口部を塞ぐこと。

２　電算管理責任者は、情報システム室に対する火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除するための措置を講じなければならない。

（管理区画の入退室管理等）

第36条　情報セキュリティ責任者は、管理区画に入室できる者を制限し、ＩＣカード、指紋認証等の生体認証、入退室管理簿の記載等による入退室管理を行わなければならない。

２　管理区画に入室しようとする者は、職員証、身分証明書等を携帯し、求めにより提示しなければならない。

３　情報セキュリティ責任者は、外部からの訪問者が管理区画に入室する場合には、外部か

らの訪問者を外見上職員等と区別できる措置を講じるとともに、必要に応じて職員等の携行、立ち入ることができる区画の制限等を行わなければならない。

４　電算管理責任者は、情報システム室について、当該情報システムに関連しない端末等、通信回線装置、電磁的記録媒体等の持ち込みについて管理しなければならない。

（機器等の搬入出）

第37条　電算管理責任者は、機器等の搬入出のために職員等以外の者が情報システム室に立ち入る場合は、職員等を立ち会わせなければならない。

第３節　通信回線等の管理

（通信回線及び通信回線装置の管理）

第38条　電算管理責任者は、ネットワークに使用する回線について、情報が伝送途上において破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の適切なセキュリティ対策を実施しなければならない。

２　電算管理責任者は、機密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は、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とともに、送受信される情報を暗号化等により適切に保護しなければならない。

３　電算管理責任者は、通信回線装置が動作するために、必要なソフトウェアの状態等を調査し、認識した脆弱(ぜい)性等について対策を講じなければならない。

４　電算管理責任者は、可用資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択するとともに、冗長化等により継続的な運用を確保しなければならない。

第５章　人的セキュリティ

第１節　職員等の遵守事項

（情報セキュリティポリシー等の遵守）

第39条　職員等は、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

２　職員等は、情報セキュリティ対策について疑義等が生じた場合は、速やかに情報セキュリティ責任者に報告し、指示を受けなければならない。

（業務以外の目的での使用の禁止）

第40条　職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（外部における情報処理作業の制限）

第41条　職員等は、在宅勤務型テレワーク（職員が情報通信技術を活用して自宅等で業務を行うものをいう。以下「テレワーク」という。）を行う場合には、情報セキュリティ責任者の許可を得なければならない。

２　テレワークは、内部情報系端末（杉並区庁内ネットワーク等利用要領（平成29年３月24日杉並第63764号）第２条第12号に規定する端末をいう。）を利用して行なわなければならない。

（支給以外の端末の業務利用）

第42条　職員等は、機密資産を取り扱う場合は、業務端末等以外の端末等を利用してはならない。ただし、電算管理責任者が業務上必要と認めるときは、情報システム担当課長が定める手続の例により、情報セキュリティ責任者の許可を得て業務端末等以外の端末等を利用することができる。

（持ち出し及び持込みの記録）

第43条　職員等は、重要資産等の持ち出し及び情報セキュリティ責任者が必要と認める区画への端末等の持ち込みに当たっては、記録を作成し、保管しなければならない。

（業務端末等におけるセキュリティ設定変更の禁止）

第44条　職員等は、業務端末等のソフトウェアに関するセキュリティ機能の設定を当該業務端末等の管理を行う情報セキュリティ責任者の許可なく変更してはならない。

（クリアデスク・クリアスクリーン）

第45条　職員等は、業務端末等及び紙媒体について、第三者に使用されること又は情報セキュリティ責任者の許可なく情報を閲覧されることがないように、適切な措置を講じなければならない。

（退職時等の遵守事項）

第46条　職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。

（情報セキュリティポリシー等の掲示等）

第47条　情報セキュリティ責任者は、情報セキュリティポリシー及び情報セキュリティ実施手順を職員等が常に閲覧できるように掲示等しなければならない。

（外部委託事業者に対する監督）

第48条　情報セキュリティ責任者は、情報資産の取扱いを外部委託事業者に委託する場合は、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守状況について監督しなければならない。

２　委託事業者が情報資産の取扱いを再委託している場合は、前項に規定する監督に加え、再委託先事業者の間接的な監督を行わなければならない。

第２節　研修・訓練

（研修）

第49条　情報セキュリティ責任者は、全ての職員等に少なくとも年１回は研修を受講させなければならない。

２　情報セキュリティ責任者は、新規採用及び雇用の職員等を対象とする研修を当該職員等に受講させなければならない。

３　情報セキュリティ責任者は、職員等の職層、役割、情報セキュリティに関する理解度等に応じた研修を受講させなければならない。

（訓練）

第50条　情報セキュリティ責任者は、年１回、緊急時対応を想定した訓練を実施するよう努めなければならない。

（研修・訓練への参加）

第51条　職員等は、定められた研修・訓練に参加しなければならない。

第３節　アカウント、パスワード等の管理

（アカウントの取扱い）

第52条　職員等は、自己が利用しているアカウントは、他人に利用させてはならない。

２　職員等間で共用アカウントを利用する場合は、共用アカウントの利用者以外に利用させてはならない。

（パスワードの取扱い）

第53条　職員等は、パスワードについて次に掲げる取扱いをしなければならない。

（１）　自己の管理するパスワードは、他人に知られないように管理すること。

（２）　業務端末等にパスワードを記憶させないこと。

（３）　パスワードは、十分な長さで、かつ、容易に類推できない文字列で設定すること。

（４）　仮のパスワードが付与された場合は、最初のログイン時点でパスワードを変更すること。

（５）　パスワードを定期的に変更し、古いパスワードを再利用しないこと。

（６）　複数の情報システムを扱う場合は、同一のパスワードを複数の情報システム間で用いないこと。

２　職員等は、パスワードが流出した可能性がある場合には、情報セキュリティ責任者に速

やかに報告し、パスワードを速やかに変更しなければならない。

（ＩＣカード等の取扱い）

第54条　職員等は、自己の管理するＩＣカード等のうち情報システムの利用に関する認証に用いるもの（以下「認証用媒体」という。）は、他人に利用させてはならない。

２　職員等は、業務上必要のないときは、認証用媒体等をカードリーダ、端末等のスロット等から抜いておかなければならない。

３　職員等は、認証用媒体を紛失した場合には、速やかに情報セキュリティ責任者に報告し、指示に従わなければならない。

４　情報セキュリティ責任者は、前項の報告を受けた場合は、速やかに認証用媒体のアクセス権等を無効にしなければならない。

５　情報セキュリティ責任者は、認証用媒体を切り替える場合は、切替え前の認証用媒体を回収し、破砕等により情報が復元不可能な状態にした上で廃棄しなければならない。

第６章　技術的セキュリティ

第１節　コンピュータ及びネットワークの管理

（ファイルサーバの設定等）

第55条　電算管理責任者は、職員等が使用できるファイルサーバを設置する場合は、次に掲げる措置を講じなければならない。

（１）　ファイルサーバの容量を設定し、職員等に周知すること。

（２）　ファイルサーバを利用するための初期設定として、フォルダを課単位で構成し、職員等が他課のフォルダ及びファイルを閲覧及び使用できないように、アクセス権を設定すること。

（３）　個人情報、人事記録等、特定の職員等しか取り扱えない情報について、別途ディレクトリを作成する等の措置を講じ、同一課であっても、担当職員以外の職員等が閲覧及び使用できないようにすること。

（バックアップの実施）

第56条　電算管理責任者は、サーバ等に記録された情報について、情報資産の分類に応じて定期的にバックアップを実施しなければならない。

２　電算管理責任者は、重要資産等を取り扱うサーバ装置については、原則として、適切な方法でサーバ装置のバックアップを取得しなければならない。

３　電算管理責任者は、重要資産等を取り扱う情報システムを構成する通信回線装置については、原則として、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

（区以外の団体との情報システムに関する重要資産等の交換）

第57条　電算管理責任者は、区以外の団体との間で情報システムに関する情報及びソフトウェアを交換する場合は、その用途等を明確にして目的外利用や紛失、改ざん等が起こらないようにするとともに、これを担保するため、必要に応じて相手方の団体との間で当該内容を明記した合意文書を取り交わす等の対策を取らなければならない。

（システム管理記録及び作業の確認）

第58条　電算管理責任者は、所管する情報システムに対して実施した保守、設定変更等作業について、作業内容を記録しなければならない。

２　電算管理責任者は、前項の記録について、改ざん、紛失等を防止するとともに、業務上必要な者以外が閲覧できないように、適切に管理し、運用及び保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

３　第１項の作業を実施する者は、２名以上の者による作業、チェックリストによる作業確認等作業に誤りがないような措置を講じなければならない。

（情報システム仕様書等の管理）

第59条　電算管理責任者は、所管する情報システムのネットワーク構成図及び情報システム仕様書について、改ざん、紛失等を防止するとともに、業務上必要な者以外の者が閲覧できないように、適切に管理しなければならない。

（ログの取得等）

第60条　電算管理責任者は、所管する情報システムの各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

２　電算管理責任者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

３　電算管理責任者は、取得したログについて、次のいずれかの方法により、不正操作等の有無について確認しなければならない。

（１）　目視により定期的に点検する方法

（２）　情報システムにログを分析する機能を設ける方法

（障害記録）

第61条　電算管理責任者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を障害記録として記録し、適切に管理しなければならない。

（ネットワークの接続制御、経路制御等）

第62条　電算管理責任者は、所管するネットワークに係るフィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

２　電算管理責任者は、不正アクセス等を防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（外部の者が利用できるシステムの分離等）

第63条　電算管理責任者は、所管する情報システムのうち、職員等及び外部委託事業者以外の者が利用できるものについて、当該情報システムに記録される情報資産の重要度に応じ、他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（外部ネットワークとの接続制限等）

第64条　電算管理責任者は、所管する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、部会の承認を得なければならない。

２　接続するネットワークで個人情報を含む情報を伝送する場合は、前項の手続に加え、安全管理措置基準に定める手続を経なければならない。

３　電算管理責任者は、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あらかじめ調査し、区が管理するネットワーク、情報システム等に影響が生じないことを確認しなければならない。

４　電算管理責任者は、外部ネットワークを利用する場合には、外部ネットワークの瑕疵（かし）により業務への影響が生じた場合における、区と当該ネットワークを運用する者間の責任分界点を明確化するとともに、当該事象発生に備え、対応策を定めなければならない。

５　電算管理責任者は、ウェブサーバ等をインターネットに公開する場合は、次のセキュリティ対策を実施しなければならない。

（１）　庁内ネットワークへの侵入を防御するために、外部ネットワークとの境界にファイアウォールを設置する、庁内ネットワークと物理的に分離する等の措置を講じること。

（２）　脆(ぜい)弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用すること。

（３）　ウェブサーバからの不用意な情報漏えいを防止するための措置を講じること。

（４）　ウェブコンテンツの編集作業を行う主体を限定すること。

６　電算管理責任者は、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、情報セキュリティ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との接続を遮断しなければならない。

（プリンタ等のセキュリティ管理）

第65条　電算管理責任者は、プリンタ及び複合機（以下「プリンタ等」という。）を調達する場合は、当該プリンタ等が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を定めなければならない。

２　電算管理責任者は、プリンタ等が備える機能について適切な設定等を行うことによりプリンタ等に対する情報セキュリティインシデントへの対策を講じなければならない。

３　電算管理責任者は、プリンタ等の運用を終了する場合は、プリンタ等に内蔵された電磁的記録媒体の情報を消去し、復元不可能な状態にしなければならない。

（特定用途機器のセキュリティ管理）

第66条　電算管理責任者は、特定用途機器（テレビ会議システム、ＩＰ電話システム及びネットワークカメラシステム等の特定の用途に使用される機器をいう。）について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

（無線ＬＡＮの盗聴対策）

第67条　電算管理責任者は、情報資産を取り扱うために無線ＬＡＮを利用する場合は、暗号化及び認証技術を使用しなければならない。

（電子メールのセキュリティ管理）

第68条　電算管理責任者は、所管する電子メールサーバについて、次に掲げる措置を講じなければならない。

（１）　権限のない利用者により、外部から外部への電子メールの転送（電子メールの中継処理）が行われることを不可能とすること。

（２）　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、所管する電子メールサーバの運用を停止する等の措置を講じること。

（３）　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にすること。

（４）　職員等が使用できる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こと。

（５）　職員等以外の者による電子メール利用について、電子メールを利用する者との間で利用方法を取り決めること。

（電子メールの利用制限）

第69条　職員等は、業務端末等で電子メールを利用する場合は、次に掲げる事項を遵守しなければならない。

（１）　自動転送機能を用いて、外部へ電子メールを転送しないこと。

（２）　業務上必要のない送信先に電子メールを送信しないこと。

（３）　複数人に電子メールを送信する場合は、原則、他の送信先のメールアドレスが分からないようにすること。ただし、他の送信先を知らせる必要がある場合を除く。

（４）　外部に重要資産等を含む電子メールを誤送信した場合は、速やかに情報セキュリティ責任者に報告すること。

（５）　ウェブで利用できるフリーメールを許可なく使用しないこと。また、ストレージサービス（インターネット上でファイルを共有するサービスをいう。）等で、原則として、重要資産等をアップロードしてはならない。

（電子署名・暗号化）

第70条　職員等は、外部にデータを送信するときは、第８条の規定に基づく取扱制限に照らし、機密性又は完全性を確保することが必要と認められる場合は、当該データについて、電子署名、パスワード等による暗号化等の措置を講じた上で送信しなければならない。

（無許可ソフトウェアの導入等の禁止）

第71条　職員等は、業務端末等に無断でソフトウェアを導入してはならない。
２　職員等は、業務上必要な場合は、区長部局の定める手順の例により、情報セキュリティ責任者及び情報システム担当課長の承認を得た上で、業務端末等にソフトウェアを導入することができる。
３　職員等は、不正にコピーしたソフトウェアを利用してはならない。
（ソフトウェアライセンスの管理）
第72条　電算管理責任者は、保有するソフトウェアのライセンスについて、適切に管理しなければならない。
（機器構成の変更の制限）
第73条　職員等は、業務端末等の改造、増設及び交換を行ってはならない。
２　職員等は、業務の執行に当たり、業務端末等の改造、増設又は交換が必要な場合には、あらかじめ電算管理責任者の承認を得なければならない。
３　改造、増設又は交換が必要な業務端末等が情報システム担当課長の所管するものの場合は、あらかじめ情報システム担当課長に承認を得なければならない。
（ネットワーク接続の禁止）
第74条　職員等は、電算管理責任者の許可なく、端末等を当該電算管理責任者の所管するネットワークに接続してはならない。
２　電算管理責任者は、自らが調達した端末について、端末に搭載されたＯＳのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することを検討し、必要が認められる場合は採用しなければならない。
（ウェブ閲覧の禁止）
第75条　職員等は、業務以外の目的でウェブを閲覧してはならない。
２　ウェブ閲覧環境を整備する電算管理責任者は、職員等が、業務に関係のないウェブサイトを閲覧できないよう必要な措置を講じなければならない。
３　ウェブ閲覧環境を整備する電算管理責任者は、職員等が明らかに業務に関係のないウェブサイトを閲覧していることを発見した場合は、情報セキュリティ責任者に通知し、適切な措置を求めなければならない。
（ウェブ会議サービスの利用時の対策）
第76条　職員等は、区長部局の定める利用手順の例により、ウェブ会議（杉並区議会オンライン会議実施要綱（令和３年４月26日杉議会第82号）に定めるオンライン会議を除く。以下同じ。）の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。
２　職員等は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

第２節　アクセス制御

（アクセス制御）
第77条　電算管理責任者は、所管するネットワーク及び情報システムについて、権限のある職員等のみがアクセスできるように、必要最小限の範囲で適切に設定する等、情報システム上制限をするなど必要な措置を講じなければならない。
（利用者アカウントの管理）
第78条　電算管理責任者は、所管する情報システムを利用するためのアカウント（以下「利用者アカウント」という。）の登録、変更、抹消等の情報管理及び利用者アカウントの取扱いの方法を定めなければならない。
２　電算管理責任者は、職員等の異動等により不要になった利用者アカウントについて、速やかに削除しなければならない。
３　電算管理責任者は、利用されていない利用者アカウントが放置されることのないよう、定期的に点検しなければならない。

４　電算管理責任者は、利用者アカウントに不要なアクセス権限が付与されていないか定期的に確認しなければならない。
５　電算管理責任者は、管理者権限等の特権を付与された利用者アカウント（以下「管理者アカウント」という。）を利用する者（以下「管理権限者」という。）を必要最小限にするとともに、管理者アカウントのパスワード（以下「管理者パスワード」という。）の漏えい等が発生しないよう、管理者アカウント及び管理者パスワードを適切に管理しなければならない。
６　電算管理責任者は、管理権限者の範囲が明確になるよう、名簿等を整備しなければならない。
７　電算管理責任者は、管理者パスワードの有効期限、入力回数制限等のセキュリティ機能を、利用者アカウントのパスワードよりも強化する措置を講じなければならない。
８　電算管理責任者は、管理者アカウントを初期設定以外のものに変更しなければならない。ただし、情報システムが固定の管理者アカウントにより運用することが定められている等管理上やむを得ない場合は、この限りではない。

（職員等による区の管理外のネットワークからのアクセスの制限）

第79条　職員等は、区の管理外のネットワークから、区が管理するネットワークにアクセスする場合は、情報システム担当課長の許可を得なければならない。
２　電算管理責任者は、外部からのアクセスに利用する端末等を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。
３　職員等は、持ち込んだ又は外部から持ち帰った端末等を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報システム担当課長が定める手順の例により接続しなければならない。

（ログインの制限）

第80条　電算管理責任は、外部からアクセス可能な情報システムに対して、ログイン時の試行回数の制限等の不正アクセスを防止のための措置を講じなければならない。

（パスワードに関する情報の管理）

第81条　電算管理責任者は、職員等のパスワードを記録する情報システムを不正アクセス等から保護するため、適切に管理しなければならない。
２　電算管理責任者は、情報システムを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。
３　電算管理責任者は、職員等に対してパスワードを発行する場合には、仮のパスワードを発行し、職員等に対してログイン後直ちに仮のパスワードを変更させなければならない。

（管理者権限等による接続時間の制限）

第82条　電算管理責任者は、管理者アカウントによるネットワーク及び情報システムへの接続時間を必要最小限にするための措置を講じなければならない。

第３節　システム開発、導入、保守等

（情報システムの調達）

第83条　電算管理責任者は、情報システムの調達に当たっては、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しなければならない。
２　電算管理責任者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（情報システムの開発）

第84条　電算管理責任者は、情報システム開発の責任者及び作業者を特定しなければならない。
２　電算管理責任者は、情報システム開発において使用するアカウント（以下「開発用アカウント」という。）を管理し、開発完了後、当該開発用アカウントを削除しなければなら

ない。
3　電算管理責任者は、開発用アカウントのアクセス権限を適切に設定しなければならない。
4　電算管理責任者は、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ェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。
5　電算管理責任者は、情報システムでの利用が認められていないソフトウェアが導入されている場合は、当該ソフトウェアを情報システムから削除しなければならない。
6　電算管理責任者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

（情報システムの導入）

第85条　電算管理責任者は、情報システムにおける、開発、保守及びテスト環境と運用環境の分離について検討し、必要が認められる場合は採用しなければならない。
2　電算管理責任者は、開発、保守及びテスト環境から運用環境へのデータ等の移行方法について、情報システムの開発計画及び保守計画において定めなければならない。
3　電算管理責任者は、前項に規定する移行の際、移行するデータ等のバックアップを行わなければならない。
4　電算管理責任者は、情報システムを導入する場合には、当該情報システムの機密性、完全性及び可用性が確保されていることを確認した上で導入しなければならない。
5　電算管理責任者は、導入する情報システムに必要となる電力、空調、配線等環境を構築することが既存の情報システムに与える影響について、確認した上で導入しなければならない。

（テストの実施）

第86条　電算管理責任者は、新たに情報システムを導入する場合、運用開始前に十分なテストを行わなければならない。
2　電算管理責任者は、実際の事務の内容を考慮した上でテスト計画を策定し、当該計画に基づいたテストを実施しなければならない。
3　電算管理責任者は、前２項に基づくテストを実施するとき、機密資産をテストデータとして使用する場合は、当該機密資産を取り扱うことが認められた者にテストを実施させなければならない。

（システム開発及び保守に関連する資料等の整備及び保管）

第87条　電算管理責任者は、情報システム開発及び保守に関連する資料並びに情報システム関連文書を適切に整備し、かつ、保管しなければならない。
2　電算管理責任者は、前条の規定により実施したテストの結果を一定期間保管しなければならない。
3　電算管理責任者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第88条　電算管理責任者は、情報システムにおいて取り扱う情報資産の重要度に応じ、情報システムにおける入出力データの正確性を確保するため、設計時に次に掲げる機能の必要性を検討し、必要性が認められる場合は採用しなければならない。
（１）　誤入力を防止するためのチェック機能
（２）　出力データにおける内部処理結果を正確に出力する機能
（３）　記録する情報について改ざん又は漏えいをチェックする機能
2　電算管理責任者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。
（１）　利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直すこと。

（２） 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じること。
（３） ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計すること。

（情報システムの変更管理）

第89条 電算管理責任者は、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し、適切に保管しなければならない。

（開発及び保守用のソフトウェアの更新等）

第90条 電算管理責任者は、開発及び保守用のソフトウェア等を更新又はセキュリティパッチを適用する場合は、あらかじめ他の情報システムとの整合性を分析及び検証しなければならない。

（システム更新又は統合時の検証等）

第91条 電算管理責任者は、情報システムを更新又は統合する場合は、あらかじめ情報システムに生じるリスク及び他の情報システムに与える影響を分析及び検証しなければならない。

第４節 不正プログラム対策

（電算管理責任者の措置）

第92条 電算管理責任者は、コンピュータウイルス等の不正プログラム（以下「不正プログラム」という。）への対策として、次に掲げる措置を講じなければならない。
（１） 所管する情報システム及び業務端末等に、不正プログラム対策ソフトウェアをシステムに常駐させること。
（２） 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保つこと。
（３） 不正プログラム対策ソフトウェアは、最新のパターンファイルを更新できる状態に保つこと。
（４） ネットワークに接続していない情報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ェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施すること。
（５） 不正プログラム情報を収集し、必要に応じて職員等に注意喚起すること。
（６） 業務で利用するソフトウェアについては、原則として、開発元のサポートが終了したものを利用してはならない。

（外部ネットワークに接続する情報システムを所管する電算管理責任者の措置）

第93条 外部ネットワークに接続する情報システムを所管する電算管理責任者は、当該情報システムにおいて取り扱う情報資産の重要度に応じ、外部ネットワークのゲートウェイにおいて不正プログラムの侵入を防止する措置を講じなければならない。

（職員等の遵守事項）

第94条 職員等は、不正プログラム対策に関し、次に掲げる事項を遵守しなければならない。
（１） 業務端末等が不正プログラムへの感染又は感染が疑われる場合は、直ちに当該業務端末等をネットワークから切断し、その使用を中止すること。
（２） 業務端末等に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施すること。
（３） 外部からデータを業務端末等に取り入れる場合は、不正プログラム対策ソフトウェアによるチェックを行うこと。
（４） 業務端末等において、不正プログラム対策ソフトウェアの設定を変更しないこと。
（５） 差出人が不明又は不審なファイルが添付された電子メールを受信した場合は、速やかに削除すること。

（６） 電子メールでファイルを送受信する場合は、不正プログラム対策ソフトウェアで当該ファイルをチェックすること。
（７） 情報セキュリティ責任者又は電算管理責任者が提供する不正プログラム対策に関する情報の内容を確認すること。

第５節　不正アクセス対策

（電算管理責任者の措置事項）
第95条　電算管理責任者は、不正アクセス対策として、次に掲げる事項を措置しなければならない。
（１） 使用されていないポートを閉鎖すること。
（２） 不要なサービスについて、機能を削除又は停止すること。
（３） 外部公開用ウェブページを設置する情報システムには、データ書換え検出、検知時の通報設定等の改ざん防止対策を講じること。
（攻撃への対処）
第96条　電算管理責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、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。
（記録の保存）
第97条　電算管理責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存しなければならない。
（職員等による不正アクセス）
第98条　電算管理責任者は、所管する情報システムへの職員等による不正アクセスを発見した場合は、情報セキュリティ責任者に通知し、適切な処置を求めなければならない。
（サービス不能攻撃）
第99条　電算管理責任者は、所管する情報システムが外部からアクセスできる場合は、第三者からのサービス不能攻撃等により、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。
（標的型攻撃）
第100条　電算管理責任者は、所管する情報システムへの標的型攻撃による内部への侵入を防止する対策として、次に掲げる措置を講じなければならない。
（１） 標的型攻撃に関する職員への指導及び情報共有
（２） 自動再生無効化等の入口対策
（３） 内部への侵入を早期検知して対処するための通信チェック等の対策
（セキュリティ情報の収集及び周知）
第101条　情報セキュリティ責任者は、脆弱性や不正プログラム等のセキュリティ情報を収集し、必要に応じて電算管理責任者に周知しなければならない。
２　電算管理責任者は、前項により周知された脆弱性、不正プログラム等が所管する情報システムに与える影響について分析し、必要に応じてセキュリティ侵害を防止するための措置を講じなければならない。

第７章　運用

（情報システムの運用及び保守時の対策）
第102条　電算管理責任者は、情報システムの運用及び保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。
２　電算管理責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。
３　電算管理責任者は、重要資産等を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。
（情報システムの監視）
第103条　電算管理責任者は、セキュリティ侵害を検知するため、情報システムを監視しな

ければならない。
２　電算管理責任者は、重要なログ等を取得するサーバ等の正確な時刻設定及び他サーバ等との時刻同期ができる措置を講じなければならない。
（情報セキュリティポリシーの遵守状況の確認）
第104条　情報セキュリティ責任者は、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、問題を認めた場合には、速やかに情報セキュリティ統括責任者に報告しなければならない。
２　電算管理責任者は、所管する情報システム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、問題を認めた場合には、速やかに対応しなければならない。
（業務端末等の利用状況調査）
第105条　情報セキュリティ責任者は、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業務端末等のログ、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。
（職員等の報告義務）
第106条　職員等は、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は、直ちに情報セキュリティ責任者に報告しなければならない。
２　情報セキュリティ責任者は、前項の違反行為が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認められる場合は、速やかに緊急時対応計画に基づき対応しなければならない。
（緊急時対応計画の策定）
第107条　情報セキュリティ責任者は、情報セキュリティポリシーの違反等により情報セキュリティインシデントが発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。
２　緊急時対応計画には、次に掲げる事項を定めなければならない。
（１）　関係者の連絡先
（２）　発生した事案に係る報告すべき事項
（３）　発生した事案への対応措置
（４）　再発防止措置の策定
３　情報セキュリティ責任者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に対応するため、定期的に緊急時対応計画を見直さなければならない。
（例外措置）
第108条　情報セキュリティ責任者は、情報セキュリティポリシーを遵守することが困難な状況で、遵守事項とは異なる方法（以下「例外措置」という。）を採用し又は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、情報セキュリティ統括責任者の承認を得て、例外措置を実施することができる。
２　情報セキュリティ責任者は、業務の遂行に緊急を要する等の場合であって、情報セキュリティ統括責任者に承認を得るいとまがない場合は、例外措置を実施することができる。ただし、例外措置を実施後、直ちに情報セキュリティ統括責任者に報告しなければならない。
（法令遵守）
第109条　職員等は、情報資産を適切に保護するために、地方公務員法、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）、番号法、杉並区議会個人情報の保護に関する条例（令和７年杉並区条例第50号）その他情報資産を管理する上で必要な法令等を遵守しなければならない。
（違反時の対応）

第110条　電算管理責任者は、所管する情報システムにおいて、職員等の情報セキュリティポリシー違反を確認した場合は、速やかに情報セキュリティ責任者及び情報セキュリティ統括責任者に通知し、適切な措置を求めなければならない。
２　電算管理責任者は、前項の通知後も、情報セキュリティポリシー違反の是正が認められない場合には、所管する情報システムについて、情報セキュリティを確保するための必要な措置を講じることができる。

第８章　外部サービスの利用

第１節　外部委託

（委託事業者の選定基準）
第111条　情報セキュリティ責任者は、情報資産を取り扱う業務を外部に委託する場合は、委託で取り扱う情報資産の重要度に応じた情報セキュリティ対策が確保されるようにするため、委託事業者の選定に関する選定基準等を定めなければならない。
２　情報セキュリティ責任者は、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、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。
（契約項目）
第112条　情報セキュリティ責任者は、情報資産を取り扱う業務を外部に委託する場合には、委託事業者が取り扱う情報の重要度に応じて、委託事業者との間で次に掲げる情報セキュリティ等に係る要件を明記した契約を締結しなければならない。
（１）　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
（２）　個人情報漏えい防止のための技術的安全管理措置に関する取り決め
（３）　外部委託事業者の責任者、委託内容、作業者及び作業場所の特定
（４）　提供されるサービスレベルの保証
（５）　外部委託事業者にアクセスを許可する情報の種類、範囲及びアクセス方法
（６）　外部委託事業者の従業員に対する教育の実施
（７）　提供された情報の目的外利用及び受託者以外の者への提供の禁止
（８）　業務上知り得た情報の守秘義務
（９）　再委託に関する制限事項の遵守
(10)　委託業務終了時の情報資産の返還、廃棄等
(11)　委託業務の定期報告及び緊急時報告義務
(12)　区による監査、検査
(13)　区による情報セキュリティインシデント発生時の公表
(14)　情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）
２　個人情報を取り扱う業務を外部委託する場合には、前項に掲げるものに加え、外部委託事業者との間で個人情報に係る外部委託契約特記仕様書のガイドライン（平成18年11月30日杉並第58465号）に基づく個人情報保護措置要件を明記した契約を締結しなければならない。
（実施状況の確認）
第113条　情報セキュリティ責任者は、外部委託事業者において前条に規定する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しなければならない。

第２節　ソーシャルメディアサービス

（ソーシャルメディアサービスの利用に係る規定の整備）
第114条　職員等は、区長部局の定めるソーシャルメディアサービスの利用に係る規定の例により、ソーシャルメディアサービスを利用しなければならない。

第３節　クラウドサービス

（クラウドサービスの利用）
第115条　職員等は、区長部局の定めるクラウドサービスの利用に係る規定の例により、ク

ラウドサービスを利用しなければならない。
2　情報セキュリティ責任者は、クラウドサービスを利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報資産の取扱いを委ねることの可否を判断しなければならない。
3　情報セキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。
4　情報セキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件としなければならない。
5　情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。
6　情報セキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
7　職員等は、約款への同意及びアカウントの登録等により、当該約款の範囲内で利用可能なクラウドサービス（電子メール、ファイルストレージ、グループウェア等（国、都道府県その他公的機関から提供される公的サービスを除く。））においては、機密資産を取り扱ってはならない。

第９章　評価・見直し

第１節　監査

（監査を行う者の要件）
第116条　情報セキュリティ責任者は、監査を実施する場合には、被監査部門から独立した者を監査人として指名しなければならない。
2　情報セキュリティ責任者は、監査人の指名に当たり、監査及び情報セキュリティに関する知識の習熟度等を考慮した上で、指名しなければならない。
3　被監査部門は、監査の実施に協力しなければならない。
（外部委託を行っている被監査部門に対する監査）
第117条　情報セキュリティ責任者は、被監査部門が情報資産の取扱いを外部委託している場合には、被監査部門における次に掲げる事項の実施状況を監査しなければならない。
（１）　委託事業者等が契約に基づき実施する情報セキュリティポリシー及び契約情報の遵守状況の監督
（２）　委託事業者等が情報資産の取扱いを再委託している場合は、再委託先事業者への間接的な監督
（監査証跡等の保管）
第118条　情報セキュリティ責任者は、監査報告に係る調書及び監査の実施を通して収集した資料等を適切に保管しなければならない。
（監査結果への対応）
第119条　情報セキュリティ統括責任者は、監査結果を踏まえ、被監査部門の情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。
2　情報セキュリティ責任者は、前項の指摘事項について、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点を周知するとともに、その有無を確認させなければならない。
（監査結果の活用）
第120条　情報セキュリティ責任者は、監査結果を情報セキュリティポリシー及び関係規程

等の見直し時に活用するものとする。

第２節　自己点検

（自己点検の実施）

第121条　情報セキュリティ責任者は、情報セキュリティ対策の状況について、毎年度及び必要に応じて自己点検を実施しなければならない。

（自己点検結果の活用）

第122条　情報セキュリティ責任者は、自己点検結果に基づき、情報セキュリティ対策の適切な改善を図らなければならない。

２　情報セキュリティ責任者は、自己点検結果を情報セキュリティポリシー及び関係規程等の見直し時に活用しなければならない。

第３節　情報セキュリティポリシー等の見直し

（情報セキュリティポリシー及び関係規程等の見直し）

第123条　情報セキュリティ責任者は、監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生したときは、評価を行うものとし、必要が認められる場合は、見直さなければならない。

第10章　雑則

（委任）

第124条　対策基準に定めるもののほか、情報セキュリティ運用等の細目については、区長部局の定める次の要領の例による。

（１）　杉並区庁内ネットワーク等利用要領　庁内のネットワーク運用等に係る細目

（２）　杉並区外部ネットワーク等利用要領　外部のネットワーク運用等に係る細目

２　前項の規定に加え、この基準の施行に関し必要な事項は、情報セキュリティ責任者が別に定める。

附　則

この基準は、令和８年４月１日から施行する。

別表（第８条、第９条、第12条、第13条、第15条関係）

機密性による情報資産の分類

分類	分類基準	取扱制限の例
機密性３A	議会の事務で取り扱う情報資産のうち、秘密保全の必要が高く、その漏えいが国の安全 、利益に損害を与えるおそれのある情報を含む行政文書 （例）「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）の秘密文書に相当する文書	・施錠可能な場所への保管 ・業務上必要のない複製及び配布禁止 ・復元不可能な処理を施しての廃棄 ・保管場所への許可を得ない電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時におけるパスワード等による暗号化設定 ・データ持ち出し制限や上長承認の実施 ・許可された端末以外での作業の禁止 ・信頼のできるネットワーク回線の選択 ・適切なアクセス権設定 ・外部で情報処理を行う際の安全管理措置の規定 ・クラウドサービスで取り扱う場合には、「杉並区クラウドサービス利用
機密性３B	議会の事務で取り扱う情報資産のうち、機密性３Aに相当する機密性は有しないが、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、取扱いに非常に留意すべき情報資産 （例）保有個人情報（特定個人情報を含む）	
機密性３C	議会の事務で取り扱う情報資産のうち、機密性３Bに相当する機密性は有しないが、公表を前提としていない情報で、取扱いに留意すべき情報資産 （例）職員情報	

	入札予定価格等の非公開情報	ガイドライン」に基づく措置の実施
機密性２	議会の事務で取り扱う情報資産のうち、機密性３以上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 （例）政策検討等に関する情報	・特定個人情報を含む場合には、「杉並区特定個人情報取扱指針」に基づく措置の実施
機密性１	機密性２の情報資産以外の情報資産	・情報セキュリティ管理者があらかじめ定めた手順による取扱制限の実施

完全性による情報資産の分類

分類	分類基準	取扱制限の例
完全性２	議会の事務で取り扱う情報資産のうち、下記の性質をもつ情報資産 ・改ざん、誤びゅう又は破損により、区民の権利が侵害される又は業務の適確な遂行に重大な支障を及ぼすおそれがあるもの	・施錠可能な場所への保管 ・許可を得ない複製及び配付禁止 ・バックアップの実施 ・電子署名付与
完全性１	完全性２の情報資産以外の情報資産	・情報セキュリティ管理者があらかじめ定めた手順による取扱制限の実施

可用性による情報資産の分類

分類	分類基準	取扱制限の例
可用性２	議会の事務で取り扱う情報資産のうち、下記の性質をもつ情報資産 ・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、区民の権利が侵害される又は業務の適確な遂行に重大な支障を及ぼすおそれがあるもの	・施錠可能な場所への保管 ・バックアップの実施 ・指定する時間以内のシステム復旧の補償
可用性１	可用性２の情報資産以外の情報資産	・情報セキュリティ管理者があらかじめ定めた手順による取扱制限の実施