港区情報安全対策指針

（個人情報等を守るための事務処理指針）

平成１５年（２００３年）８月

港　　区

令和４年（２０２２年）９月改定版

港区平和都市宣言

かけがえのない美しい地球を守り、世界の恒久平和を願う人びとの心は一つであり、いつまでも変わることはありません。

私たちも真の平和を望みながら、文化や伝統を守り、生きがいに満ちたまちづくりに努めています。

このふれあいのある郷土、美しい大地をこれから生まれ育つこどもたちに伝えることは私たちの務めです。

私たちは、我が国が『非核三原則』を堅持することを求めるとともに、ここに広く核兵器の廃絶を訴え、心から平和の願いをこめて港区が平和都市であることを宣言します。

昭和６０年８月１５日

港　　区

港 区 情 報 安 全 対 策 指 針

目　　次

港区情報安全対策基本方針

１　基本的考え方
２　情報安全対策指針の位置付け
３　対象範囲
４　情報セキュリティ対策の実施
５　職員等の義務

港区情報安全対策基準

１　対象範囲
２　管理体制
３　情報の分類と管理
４　人的な情報セキュリティ対策
５　技術的な情報セキュリティ対策
６　物理的な情報セキュリティ対策
７　指定管理者の管理
８　業務委託と外部サービスの利用
９　情報安全対策指針の運用
１０　情報安全対策指針の評価及び見直し

港区情報安全対策基本方針

（平成１５年８月１５日
１５港政情第３１２号）

改正　平成 22 年 3 月 21 日 21 港総情第 2973 号
改正　平成 27 年 6 月 1 日 27 港総情第 1378 号
改正　平成 28 年 4 月 1 日 27 港総情第 6454 号
改正　平成 31 年 4 月 1 日 30 港総情第 4563 号
改正　令和 2 年 4 月 1 日 31 港総情第 4410 号
改正　令和 4 年 9 月 1 日 4 港総情第 1933 号

１　基本的考え方

インターネットに代表される高度情報通信ネットワーク社会の進展は、私たちの生活や仕事、人と人とのコミュニケーションに大きな変化をもたらしています。ネットワーク化の促進によって、誰もが様々な情報にいつでもどこからでも容易にアクセスできるようになり、私たちの暮らしはより便利に、より快適になるものと期待されています。

区は、急速に進歩する情報技術を積極的に活用することにより、区民に様々な行政サービスをスピーディに提供し、区政情報の提供・公開と区民の区政参加を促進するICT（情報通信技術）環境の構築に取り組んでいます。また、国や他の自治体等とのネットワークシステムに参加し、より密接な連携・協力関係のもとで、新たな区民サービスを展開していきます。

行政サービスの高度情報化は、区と区民との新しい関係を創り出し、区民サービスの一層の向上や効率化の促進など大きな効果が期待されます。その反面、情報の改ざん・漏えいを目的とする不正アクセスや、コンピュータの機能を麻痺させるコンピュータウイルスの侵入等、安全で安定した行政サービスを脅かす存在が増加しています。

情報システムの障害はもとより、個人情報の改ざん・漏えい等は絶対にあってはならないことです。区民が安心して行政サービスを利用するためには、個人情報や区の情報システムが安全に管理されていることが不可欠です。

区は、行政サービスの情報化の推進にあたって、個人情報の保護を最優先とした適切な安全管理のもとに、区が収集・蓄積した情報を様々な脅威から守ります。

さらにネットワークシステムの一員として、区民に対してはもちろんのこと、国や他の自治体等へ、ネットワークを通じて脅威を及ぼさないよう適切な措置を講じ、システム全体の社会的信頼の確保に取り組みます。

区は、こうした基本的な考え方に基づいて、体系的、総合的かつ継続的な情報セキュリティ対策を実施し、区が保有する情報資産（情報システム及び情報システムで記録・処理される情報等）及び一定の手続きのもとに区の情報システムに接続する職員個人が所有する携帯情報端末を適切に保護することにより、区民から信頼される安全なICT環境を実現します。

2　情報安全対策指針の位置付け

区は、情報セキュリティ対策に関する方針、行動指針等を次のように体系的に整備します。

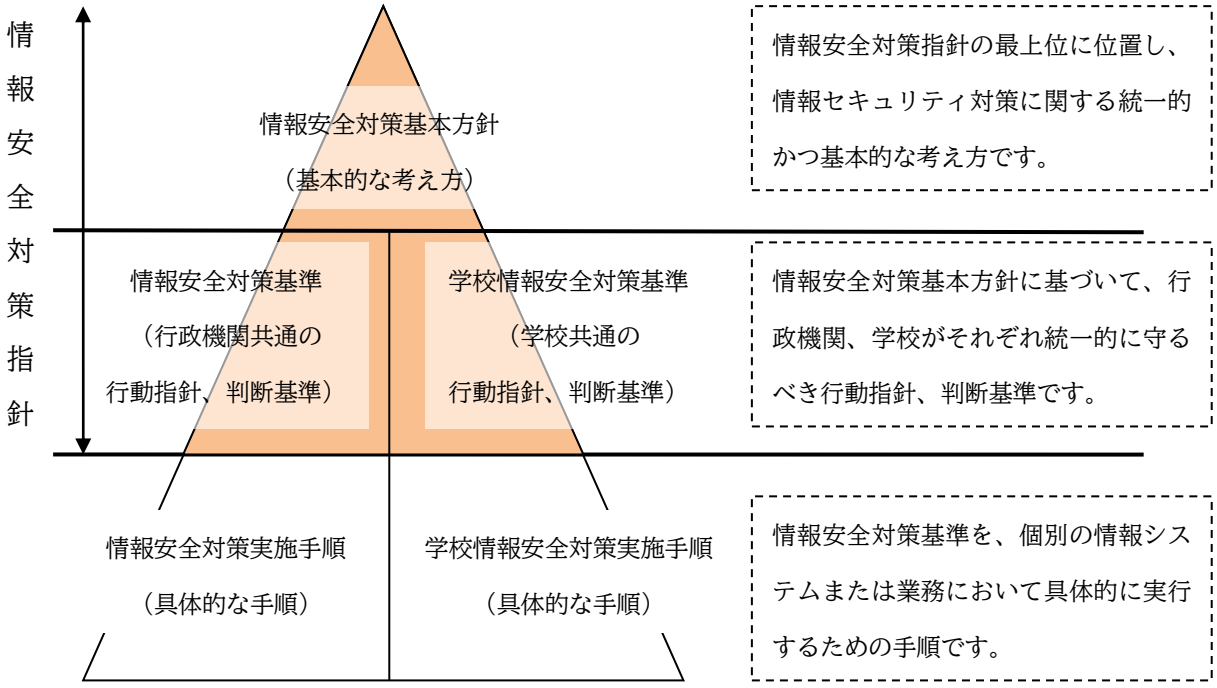

図　情報セキュリティ対策の体系的な整備

3　対象範囲

この方針の対象範囲は、区が保有する情報資産及び建物・関連設備並びに情報資産を取り扱う職員、指定管理者及び受託事業者（以下「職員等」といいます。）とします。

4　情報セキュリティ対策の実施

区は、情報資産を安全に保護するため、全庁的な推進体制を整備し、次のとおりに総合的かつ継続的に情報セキュリティ対策を実施します。

（１）法令等の遵守

個人情報の保護及び情報セキュリティの確保については、法律、条例、規則等を守ります。

（２）脅威の認識

情報資産の不正利用、情報の漏えい等の危険性をもたらす脅威を次のように捉えます。

１）故意による脅威（不正アクセス、情報の改ざん・漏えい等）

２）過失による脅威（誤操作等）

３）故障による脅威（機器の故障等）

４）災害による脅威（地震、火災、水害、落雷等）

（３）総合的な情報セキュリティ対策

様々な脅威から情報資産を保護するため、次の情報セキュリティ対策を実施します。

１）人的な情報セキュリティ対策

職員等の情報セキュリティに関する責任の明確化及び行動指針の遵守による対策

２）技術的な情報セキュリティ対策

情報システムへの不正アクセス、コンピュータウイルス等から保護するための対策

３）物理的な情報セキュリティ対策

情報システムの設置されている場所への不正な立ち入り、機器の損傷等から保護するための対策

（４）監査及び点検

情報安全対策指針の遵守状況を確認するために、監査の体制を明確に定めて、監査及び点検を行います。

（５）評価及び見直し

情報資産を取り巻く環境の変化に適切に対応していくため、情報安全対策指針の評価及び見直しを行います。

５　職員等の義務

職員等は、情報セキュリティの重要性を認識し、業務の遂行にあたって情報安全対策指針を守る義務があります。情報安全対策指針に違反した場合は、法令及び港区職員の懲戒処分に関する指針に基づき、処罰等又は懲戒処分の対象となります。

港区情報安全対策基準

（平成１５年８月１５日
１５港政情第３１２号）

改正　平成17年4月　1日 17港政情第　14号
改正　平成18年3月 22日 17港政情第　703号
改正　平成19年4月　1日 19港総情第　　1号
改正　平成19年6月　1日 19港総情第　616号
改正　平成22年3月 21日 21港総情第 2973号
改正　平成22年4月　1日 22港総情第　308号
改正　平成24年5月　1日 24港総情第 1618号
改正　平成27年6月　1日 27港総情第 1378号
改正　平成28年4月　1日 27港総情第 6454号
改正　平成31年4月　1日 30港総情第 4563号
改正　令和2年4月　1日 31港総情第 4410号
改正　令和4年9月　1日　4港総情第 1933号

港区情報安全対策基準とは、港区情報安全対策基本方針に基づいて、区が保有する情報資産*1を故意、過失、故障及び災害の脅威から保護し、区民から信頼される ICT 環境を実現するための情報セキュリティ対策に関する基準です。

なお、区立の幼稚園、小学校及び中学校が保有する情報資産については、港区学校情報安全対策基準によります。

１　対象範囲

情報安全対策基準が対象とする行政機関の範囲は、港区総合支所及び部の設置等に関する条例（平成１７年港区条例第６２号）に規定する総合支所及び部並びに防災危機管理室、みなと保健所、会計室、教育委員会事務局、選挙管理委員会事務局、監査事務局及び区議会事務局とします。

２　管理体制

全庁的な情報セキュリティ推進体制は、次のとおりです。

（１）セキュリティ統括責任者

① セキュリティ統括責任者は、情報資産の情報セキュリティ対策を統括する最高責任者とし、副区長（総務部を担任する者）をもって充てます。

② セキュリティ統括責任者は、情報セキュリティ対策に関する責任体制、継続的な監視体制、監査体制を整備し、情報資産の適切な管理に努めます。

（２）セキュリティ副統括責任者

① セキュリティ副統括責任者は、セキュリティ統括責任者を補佐する者とし、総務部長をもって充てます。

*1 情報資産：ハードウェア・ソフトウェア・ネットワークで構成される情報システム、情報システム・外部記録媒体等に記録されたデータ、情報システムで処理された入出力データの総称をいいます。

② セキュリティ副統括責任者は、セキュリティ統括責任者に事故あるときはその職務を代理します。

（３）システム統括管理者

① システム統括管理者は、情報資産の適切な情報セキュリティ対策を実施する者とし、情報政策課長をもって充てます。

② システム統括管理者は、情報資産の情報セキュリティを確保するため、次の事項を実施します。

・庁内の主要なネットワーク*2 の管理運営
・庁内の主要な情報システム*3 の管理運営
・情報セキュリティに関する調査及び研究
・情報セキュリティ確保に関する措置
・情報セキュリティに関する啓発及び研修
・セキュリティ責任者への情報セキュリティに関する指導及び助言
・その他必要な事項

（４）システム管理者

① システム管理者は、情報システムの開発、変更、運用等について責任を有する者とし、その情報システムを設置する課等の長をもって充てます。なお、情報政策課が所管する情報システムについては、システム統括管理者が兼任します。

② システム管理者は、所管する情報システムについて、適切な管理運営を行うため、情報安全対策実施手順等の策定、評価及び見直しを実施します。

（５）セキュリティ責任者

① セキュリティ責任者は、情報資産を利用する課等の長をもって充てます。なお、情報システムを設置する課等においては、システム管理者が兼任します。

② セキュリティ責任者は、システム管理者と相互調整を図り、課等の情報資産の情報セキュリティを確保するため、次の事項を実施します。

・情報安全対策指針、情報安全対策実施手順等の運用状況の確認
・課等に設置する情報システム関連機器の監視
・職員等への啓発及び教育
・情報セキュリティに関する欠陥、事故等の報告
・その他必要な事項

*2 庁内の主要なネットワーク：情報政策課が所管する内部情報系ネットワークをいいます。
*3 庁内の主要な情報システム：内部情報系ネットワークを利用する行政情報システム等をいいます。

（６）兼務の禁止

① 情報セキュリティ対策の実施において、承認又は許可の申請を行う者と承認又は許可をする者は、原則として同じ者が兼務しない体制とします。

（７）港区情報システムセキュリティ会議

① セキュリティ統括責任者は、港区情報システムセキュリティ会議を招集します。

② 港区情報システムセキュリティ会議は、セキュリティ統括責任者、セキュリティ副統括責任者、システム統括管理者及びセキュリティ統括責任者が指名する者をもって組織します。

③ 港区情報システムセキュリティ会議の庶務は、情報政策課が行います。

④ 港区情報システムセキュリティ会議は、情報セキュリティの継続的な確保を図るため、次の事項を決定します。

・情報安全対策指針の評価及び見直し

・情報システムの情報セキュリティ対策の評価及び見直し

・セキュリティ監査の実施

・緊急時における措置

・情報安全対策指針に対する重大な違反に関する調査及び再発防止策

・職員等への計画的な教育など、情報安全対策指針の運用に関する事項

・その他必要な事項

⑤ 港区情報システムセキュリティ会議の決定事項は、庁議等を通じて総合支所長、部長、室長、所長、次長、局長に速やかに伝達します。

（８）情報セキュリティに関する統一的な窓口（ＣＳＩＲＴ：Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。）の設置

① セキュリティ統括責任者は、情報セキュリティに関する欠陥、事故等に対し、ＣＳＩＲＴの機能を有する体制を整備します。

② セキュリティ責任者は、情報セキュリティに関する欠陥、事故等について、その状況をＣＳＩＲＴに報告します。

③ システム統括管理者は、情報セキュリティに関して、必要に応じて関係機関や他の地方公共団体のＣＳＩＲＴの機能を有する部署、外部の事業者等との情報共有、通知・公表等を行います。

3　情報の分類と管理

（1）情報の分類

① 区が保有する情報は、次の重要性分類に従って分類します。

レベル３	・個人情報 ・法令又は条例の定めにより守秘義務を課されている区政情報（上記個人情報を除きます。） ・法人その他の団体に関する情報であって、公開することにより当該団体の利益を害するおそれのある情報 ・情報システムに関するパスワード及びシステム設定情報
レベル２	公開することにより区の事務事業の執行に重大な影響を及ぼす情報
レベル１	上記以外の区政情報

（2）管理責任

① セキュリティ責任者は、課等で収集及び作成した情報を管理する責任を有します。

（3）アクセス権限の設定

① セキュリティ責任者は、情報の分類に従いアクセス権限を定めます。

② コンピュータ*4 に情報を保存する場合は、アクセス制御された場所に保存します。

③ レベル３及び２の情報について、複製、外部記録媒体*5 を用いた送付、ネットワークを通じた送信を行う場合は、セキュリティ責任者の承認を得たうえで行います。

（4）複製物の管理

① セキュリティ責任者の承認を得て複製した情報は、複製元の情報と同様の管理を実施します。

② 障害や緊急時の発生に備えて、情報のバックアップデータを取得します。なお、バックアップデータは、必要に応じて災害対策を施した場所に保管します。

（5）外部記録媒体の管理

① レベル３及び２の情報を記録した外部記録媒体は、施錠可能な場所に保管します。なお、持ち運びの容易な保管庫等に保管する場合は、保管庫を盗難等から保護します。

② 外部記録媒体の保管状況を記録します。

③ レベル３及び２の情報を記録した外部記録媒体を搬送する場合は、職員等が行うとともに、物理的な保護措置を実施します。また、搬送した日時、搬送先等を記録します。

④ レベル３及び２の情報を記録した外部記録媒体を廃棄する場合は、セキュリティ責任者の承認を得たうえで行います。

*4 コンピュータ：情報を電磁的に処理、蓄積等する機器で、サーバー及びパソコン、携帯情報端末等の端末装置をいいます。

*5 外部記録媒体：磁気テープ、光ディスク、USBメモリ等の記録媒体をいいます。

⑤ 外部記録媒体を廃棄する場合は、初期化処理だけではなく、必ず破壊等を行い、情報漏えいを防ぎます。

（６）入出力データの管理

① レベル３及び２の情報に関する入出力データ（申請書、出力帳票、印刷物等）は、施錠可能な場所に保管します。なお、持ち運びの容易な保管庫等に保管する場合は、保管庫を盗難等から保護します。

② 入出力データの保管状況を記録します。

③ レベル３及び２の情報に関する入出力データを搬送する場合は、職員等が行うとともに、物理的な保護措置を実施します。また、搬送した日時、搬送先等を記録します。

④ レベル３及び２の情報に関する入出力データを廃棄する場合は、セキュリティ責任者の承認を得たうえで、必ず焼却や溶解処分、シュレッダー処理等を行い、情報漏えいを防ぎます。

４　人的な情報セキュリティ対策

（１）職員等の責務

１）情報安全対策指針の遵守

① 情報資産の取り扱いにあたっては、関連法令等を守ります。

② 情報安全対策指針及び情報安全対策実施手順等を守ります。

③ 情報安全対策指針及び情報安全対策実施手順等について不明な点等がある場合は、速やかにセキュリティ責任者に報告し、指示等を仰ぎます。

④ 職務中だけでなく、異動、退職等により職務を離れた場合も、知り得た情報の秘密を守ります。

２）目的外利用の禁止

① 情報資産を職務上の目的だけに使用します。

② 不正アクセス又はそれに類する行為を行いません。

③ 個人の所有するコンピュータ、外部記録媒体等を職務に使用することは、原則禁止とします。ただし、例外的に使用する場合は、システム統括管理者の承認を得ることとします。

３）情報資産の適切な取り扱い

① 第三者による不正使用、盗難等から情報資産を保護します。特に、コンピュータ

等から離れる場合は、情報システムのロック、サインアウト*6 等を行います。

② コンピュータの改造又は機器の増設を行う場合は、システム管理者の承認を得たうえで行います。

③ コンピュータにソフトウェアを導入する場合は、システム管理者の承認を得たうえで行います。

④ 情報資産を庁舎外に持ち出す場合は、セキュリティ責任者の承認を得たうえで行います。なお、庁舎外で作業する場合は、利用する情報資産の管理責任を自らが負うことを自覚し、情報安全対策指針及び情報安全対策実施手順等を遵守します。

４）パスワード等の管理

① パスワード、IC カード等を他人に使用されないように各個人が責任を持って管理します。

② IC カードの紛失等があった場合は、当該 IC カードの利用、保管、返却、廃棄等に責任をもつシステム管理者に報告します。

③ パスワードは、英数（大・小文字）、記号等を用いて他人に推測されにくいものを設定し、使い回したり、他人に教えたりしません。

５）欠陥・事故の報告義務

① 情報システムの欠陥、誤動作又は情報安全対策指針に対する違反行為等を発見した場合又は住民等外部からの報告があった場合は、セキュリティ責任者に報告し、指示等を仰ぎます。

（２）教育・訓練

① セキュリティ副統括責任者は、職員等に個人情報の保護及び情報安全対策指針に関する研修を受講させます。

② システム管理者は、情報システムの開発、保守、運用等に携わる職員等に、担当者として必要な研修を受講させます。

③ セキュリティ統括責任者は、情報資産への脅威及び緊急時の対応を想定した訓練を定期的に実施します。

*6 サインアウト：コンピュータや情報システム等にアクセス可能な状態を終了することをいいます。
アクセス可能な状態にすることをサインインといいます。

5　技術的な情報セキュリティ対策

（1）コンピュータの管理

1）担当者の指名

① システム管理者は、コンピュータの運用管理を行う職員等を指名します。

② コンピュータの運用管理を行う職員等は、複数かつ必要最小限とします。

③ セキュリティ責任者は、コンピュータの管理を行う職員等を指名します。

2）機器管理

① システム管理者は、コンピュータに管理番号を付与し、その設置場所等を記録します。

② システム管理者は、コンピュータの設置状況等を定期的に点検します。

（2）ネットワークの管理

1）担当者の指名

① システム管理者は、ネットワークの運用管理を行う職員等を指名します。

② ネットワークの運用管理を行う職員等は、複数かつ必要最小限とします。

2）構成管理

① システム管理者は、最新のネットワーク構成状況を把握します。

② システム管理者は、ネットワーク機器の設置場所及びネットワーク配線の経路を記録します。

③ システム管理者は、ネットワーク機器の設定情報を改ざんされないようにアクセス制御により管理します。

④ システム管理者は、ネットワーク機器の設定情報のバックアップを取得します。

⑤ システム管理者は、ネットワークに通信回線を使用する場合、継続的な運用を可能とする通信回線を選択し、必要に応じて通信回線を冗長構成にする等の措置を講じます。

3）構成変更

① 庁内の主要なネットワークへの新規接続や構成変更を行う場合は、システム統括管理者の承認を得たうえで行います。

4）無線 LAN

① 庁内のネットワークに無線 LAN （Local Area Network）*7 を利用する場合は、解読が困難な暗号化及び認証技術を使用します。

*7 無線LAN（Local Area Network）：ケーブル線の代わりに無線通信を利用してデータの送受信を行う仕組みをいいます。

（３）情報システムの管理

１）担当者の指名

① システム管理者は、情報システムの運用管理を行う職員等を指名します。

② 情報システムの運用管理を行う職員等は、複数かつ必要最小限とします。

２）運用管理

① システム管理者は、情報システムを構成するソフトウェア等のバックアップを取得します。

② システム管理者は、情報システムごとに操作手順書を作成し、常備します。

③ システム管理者は、情報システムごとに操作の承認手続きを定めます。

④ システム管理者は、実施した作業の記録を作成し、適切に保管します。

３）ソフトウェア管理

① システム管理者は、コンピュータへのソフトウェアの導入状況を把握します。

② ソフトウェアを導入する場合は、正規のライセンスを取得します。

③ 導入するソフトウェアは、業務上必要なものに限ります。

④ ソフトウェアを使用する場合は、使用許諾条件等の定められた条件を守ります。

（４）外部とのシステム結合

１）外部ネットワークとの接続

① 庁内の主要なネットワークと外部のネットワークを接続する場合は、港区情報システムセキュリティ会議の承認に基づき実施します。また、庁内の主要なネットワーク以外のネットワークと外部のネットワークを接続する場合は、システム統括管理者の承認に基づき実施します。なお、個人情報を処理する情報システムと外部の情報システムを結合する場合は、港区個人情報保護条例に規定する手続きをとります。

２）総合行政ネットワークとの接続

① 総合行政ネットワークに関する諸規定に基づき、適切に接続及び運用します。

３）住民基本台帳ネットワークシステムとの接続

① 法令等に基づき、適切に接続及び運用します。

（５）アクセス制御

１）コンピュータアクセス制御

① システム管理者は、不正アクセスを防ぐため、コンピュータについて次の事項を実施します。

・起動時にユーザーを認証する機能を設けます。

・利用できるコンピュータ機能を必要最小限にします。

２）ネットワークアクセス制御

① システム管理者は、ネットワークのアクセス経路を制御し、ネットワーク機器の設定を適切に維持・管理します。

② システム管理者は、ネットワーク及びネットワーク機能ごとにアクセス可能な者を定めるとともに、未使用ポートの閉鎖、不要なサービス機能の削除又は停止等、不必要なネットワーク機能へのアクセスを防ぐ対策を実施します。

③ システム管理者は、庁内のネットワークと外部のネットワークの間には、ファイアウォール*8 を設置するなど、必要な対策を実施します。

④ 庁内のネットワークと外部のネットワークの接続点の数は、必要最小限にします。

３）情報システムアクセス制御

① セキュリティ責任者は、情報及び情報システムに対する職員等のアクセス権限を定めます。

② システム管理者は、情報システムにユーザーを認証する機能を設け、サインイン手順を定めます。

③ システム管理者は、情報システムごとにユーザー登録、抹消等の手続きを定めます。

④ システム管理者は、セキュリティ責任者からユーザー登録、変更等の申請を受けた場合は、直ちに情報システムに反映します。

⑤ システム管理者は、必要なアクセス制限を行うとともに、例外的な使用を行う場合の申請・承認の手続きを定めます。

⑥ 職員等がテレワークにより外部から情報システムを利用又は情報を閲覧する場合は、人事課が定めるテレワークの諸規定に則り実施します。

４）システム上の管理者権限*9

① システム管理者は、情報システム、ネットワーク機器及びサーバー等について、システム上の管理者権限の付与、変更等の手続きを定めます。

② システム上の管理者権限の変更があった場合は、パスワード等を直ちに変更します。

*8 ファイアウォール：庁内のコンピュータやネットワークが外部から侵入されることを防ぐための仕組みをいいます。

*9 システム上の管理者権限：情報システム、ネットワーク機器及びサーバー等において、システム上の設定を行うことのできる管理者用の権限をいいます。

５）パスワードの管理

① システム管理者は、情報システムで使用するユーザーID・パスワードを厳重に管理します。

６）IC カードの管理

① システム管理者は、IC カードの利用、保管、返却、廃棄等における取扱方法を定め、厳重に管理します。

② システム管理者は、IC カードの紛失等の報告があった場合は、当該 IC カードを使用した情報システムへのアクセス等をただちに停止します。

７）アクセスログ*10 の取得・分析

① システム管理者は、アクセスログを取得すべき情報システム等を定め、記録機能を設けます。

② システム管理者は、アクセスログを一定期間保存するとともに、改ざん、漏えい等の防止策を実施します。

③ システム管理者は、不正アクセス等の状況を調査するため、アクセスログを必要に応じて分析します。

（６）不正アクセス対策

① システム管理者は、内部及び外部への不正アクセスを防ぐため、技術的な検査を実施します。

② システム管理者は、重要な情報システムの設定に関するファイル、インターネットに公開しているファイル等について、その改ざんの有無を確認します。

③ システム管理者は、セキュリティホール*11 等、情報セキュリティ対策に関する情報の収集に努め、速やかに必要な対応を実施します。

④ システム管理者は、標的型攻撃*12 による内部への侵入防止及び侵入した攻撃を早期検知するため、情報セキュリティ教育及び技術的対策を実施します。

⑤ インターネットに公開するウェブサイトにおいては、転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を実施します。

*10 アクセスログ：情報システム等にアクセスした者、日時、処理内容等を記録したものをいいます。
*11 セキュリティホール：コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことをいいます。
*12 標的型攻撃：機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃のことをいいます。

（７）コンピュータウイルス*13 対策

１）コンピュータウイルスの検査

① システム管理者は、ウイルス対策を必要とするコンピュータにウイルス対策ソフトを導入し、ウイルス検査を実施します。また、ウイルス対策ソフトを適切に更新します。

② システム統括管理者は、庁内の主要なネットワークにつながるコンピュータにおいて外部記録媒体の利用を制限します。

③ システム統括管理者は、インターネットとの接続点にウイルス対策ソフトを導入し、ウイルス検査を実施します。

④ 職員等は、外部からデータ又はソフトウェアを取り入れる場合は、必ずウイルス検査を実施します。また、電子メール等で送付元が不明なファイル等、不審なメールを受信した場合は、速やかに削除します。なお、不審なメールの受信状況はシステム管理者に報告します。

２）コンピュータウイルス発見時の対応

① 職員等は、ウイルス検査によりコンピュータウイルス感染を検知した場合は、システム管理者に直ちに報告します。

② システム管理者は、ＣＳＩＲＴへ状況を報告するとともに、被害状況に応じて、感染経路の特定、被害拡大の防止、修復措置等を実施します。

（８）情報システム構築・保守等の対策

１）情報システムの開発・導入・変更

① システム管理者は、情報システムの開発、導入、変更を行う場合は、情報セキュリティ対策及び稼動中の情報システムへの影響を十分に検証します。

② システム管理者は、情報システムを変更する場合は、必要なときに変更前の状態に復旧できるようにします。

③ システム管理者は、システム障害を防止するため、作業内容について記録を作成し、適切に保管します。

④ システム管理者は、ソフトウェア等を購入する場合は、次の事項を満たす製品を選定します。

・港区情報安全対策指針に定める運用が可能であり､情報セキュリティ上問題がないこと

・購入先又は開発元の事業者の連絡先が明らかなものであること

*13 コンピュータウイルス：コンピュータのソフトウェアに侵入し、その中のデータやプログラムを破壊する悪意をもって作られたプログラムをいいます。

・製品に関する更新情報の提供が受けられバージョンアップ等の対応が可能であること

2）情報システムの保守

① システム管理者は、情報システムの保守を適切に行い、情報セキュリティに重大な影響を及ぼす内容を発見したときは、速やかに対応します。

② システム管理者は、情報システムの保守を行う場合は、不具合及び他の情報システムへの影響を十分に検証したうえで作業を実施します。

3）設計書等の管理

① システム管理者は、情報システムの開発、変更等に関する記録（設計書等）を作成します。

② システム管理者は、設計書等を適切に管理し、最新の状態を保ちます。また、閲覧を制限します。

（9）障害対応

① 必要に応じて情報システムの可用性を確保するため、情報システムを多重化する等の対策を実施します。

② 情報システムには、障害等の発生を検知できる機能を必要に応じて設けます。

③ システム管理者は、情報システムごとに障害発生時の対応手順を定めます。

④ システム管理者は、障害発生時において、その発生原因及び対応の記録を作成し、保管します。また、再発防止策を検討及び実施します。

（１０）電子メールの利用制限

① セキュリティ責任者は、情報資産の不正な持ち出しを防止するため、電子メールの利用及びセキュリティ管理について、必要な手続きを定めます。

（１１）Web 会議サービス*14 の利用時の対策

① システム統括管理者は、Web 会議を適切に利用するための必要な手続きを定めます。

（１２）ソーシャルメディアサービスの利用

① 港区が管理するアカウントでソーシャルメディアサービスを利用する場合、セキュリティ責任者はソーシャルメディアサービス運用にあたっての手順等を定めます。

*14 Web会議サービス：専用のアプリケーションやWebブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいいます。

6　物理的な情報セキュリティ対策

（1）入退管理

① システム統括管理者は、管理区域*15 に許可した者以外が立ち入らないよう入退管理を実施します。

② システム管理者は、事務室や管理区域に許可したもの以外が立ち入らないよう入退管理を実施します。

（2）搬入出物の管理

① 事務室や管理区域への搬入出物については、業務上必要なものに制限し、事務室や管理区域のセキュリティ責任者の承認を得たうえで搬入出します。

（3）作業の監視

① システム統括管理者が指定する管理区域には、監視カメラを設置し、監視を行います。

② 職員等以外の者が事務室や管理区域へ立ち入る場合は、事務室や管理区域のセキュリティ責任者の承認を得たうえで行います。

③ 職員等以外の者が管理区域で作業を行う場合は、職員等が立会うなど、必要な対策を実施します。

（4）不正行為の防止

① システム管理者は、コンピュータやネットワーク機器について、盗難等を防ぐための対策を実施します。

② システム管理者は、ネットワーク配線について、傍受又は損傷等を防ぐための対策を実施します。

③ 職員等以外の者が利用できる情報システムのコンピュータについては、その設置環境に応じて盗難防止策や不正使用防止策を実施します。

（5）災害対策

① セキュリティ統括責任者は、管理区域の構造や内装について、その状況に応じて災害対策を実施します。

② システム管理者は、コンピュータやネットワーク機器について、その設置環境に応じて災害対策を実施します。

（6）電源の確保

① システム管理者は、コンピュータやネットワーク機器について、停電等による影響を受けないように予備電源を確保するなど、必要な対策を実施します。

*15 管理区域：コンピュータや重要なネットワーク機器等の設置場所のことをいいます。

（７）機器の保守

① システム管理者は、コンピュータやネットワーク機器の保守を実施します。

② コンピュータ等の機器を修理等のために庁舎外に搬出する場合は、情報漏えいを防ぐ措置を実施します。

（８）機器の廃棄

① コンピュータ等の機器を廃棄やリース返却等する場合は、機器内部の記憶装置の初期化処理だけではなく、必ず記録領域の消磁や記憶装置の物理破壊等によるデータ復元が不可能な措置を行い、情報漏えいを防ぎます。

７　指定管理者の管理

（１）選定

① 港区情報安全対策指針を遵守できる指定管理者を選択します。

（２）協定

① 指定管理業務の業務主管課のセキュリティ責任者は、指定管理者と協定を締結する際、守秘義務、情報安全対策指針の遵守義務、違反時の措置等を明記します。

（３）指定管理業務に関する情報資産の保護措置

① 指定管理業務の業務主管課のセキュリティ責任者は、指定管理業務に関する情報資産について、情報セキュリティを確保するために必要な人的、技術的、物理的対策を、指定管理者に実施させます。

（４）検査

① セキュリティ統括責任者は、指定管理者に対して、港区情報安全対策指針が遵守されていることを点検します。

（５）指定管理者の情報システムの利用

① システム統括管理者は、指定管理者が指定管理業務遂行のために指定管理者の情報システムを用いる場合は、次の事項を確認した上で承認します。

・港区が所管するコンピュータ、ネットワークと接続しないこと。

・港区情報安全対策指針が遵守できること。

（６）指定管理者の情報資産の受入れ

① システム統括管理者は、指定管理者が指定管理業務と直接関係のない指定管理者のコンピュータ等の情報資産を指定管理施設内に持ち込む場合は、次の事項を確認した上で承認します。

・港区情報安全対策指針が遵守できること。

8　業務委託と外部サービスの管理

（１）委託先の選定

① 港区情報安全対策指針を遵守できる委託事業者を選択します。

（２）委託先との契約

① システム管理者は、情報システムの開発、保守、運用等を業務委託する場合は、守秘義務、情報安全対策指針の遵守義務、違反時の措置等を明記した契約を締結します。

（３）委託業務に関する情報資産の保護措置

① システム管理者は、委託業務に関する情報資産について、情報セキュリティを確保するために必要な人的、技術的、物理的対策を実施します。

（４）委託先に関する検査

① システム管理者は、委託先において港区情報安全対策指針が遵守されていることを点検します。

（５）指定管理業務の委託先の管理

① 指定管理者が、指定管理業務の一部を外部委託する際は、８業務委託と外部サービスの利用の第１項から第４項までを準用します。

（６）外部サービス[*16]の利用（レベル２以上）

① システム管理者は、次の事項を確認した上で外部サービスの利用可否を判断します。

・バックアップを含め、必要なサービスレベルを保証させる契約が締結可能であること

・監査等に必要な各種ログ等の情報提供が可能なこと

・外部サービス及び外部サービス提供者の信頼性が、運用実績や各種認定および認証制度の適用状況等から確認できること

② システム管理者は、外部サービスで取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外部サービス提供者を選定します。

③ システム管理者は、外部サービスを利用する際は、外部サービスの利用開始から利用終了（バックアップ期間満了）まで、最新のセキュリティ対策を講じた上で利用します。

*16 外部サービス：事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するもの（ソフトウェアやデータ等を、インターネットを通じ必要に応じて利用者に提供するクラウドサービス等）をいいます。

（７）外部サービスの利用（レベル１）

① システム管理者は、利用するサービスの約款、その他提供条件において、港区情報安全対策指針が遵守されていることを確認した上で外部サービスの利用可否を判断します。

９　情報安全対策指針の運用

（１）監査の実施

① セキュリティ統括責任者は、情報安全対策指針の遵守状況について監査を実施します。なお、セキュリティ監査に関する具体的な実施事項は、システム統括管理者が定めます。

② セキュリティ統括責任者は、専門知識を有する者が監査を実施する体制とします。

③ 監査を受ける者とその監査を実施する者は、原則として同じ者が兼務しない体制とします。

④ セキュリティ統括責任者は、システム統括管理者の報告を受けて、評価、指摘、改善します。

⑤ システム統括管理者は、セキュリティ監査に関して、次の事項を実施します。

・監査計画書の作成
・監査の実施
・監査報告書の作成
・改善計画書の作成
・改善計画書の実施

⑥ セキュリティ責任者は、セキュリティ統括責任者によるセキュリティ監査の評価結果、指摘事項に関して、速やかに改善します。

（２）点検の実施

① セキュリティ責任者は、課等における情報安全対策指針及び情報安全対策実施手順等の遵守状況を点検し、その結果に応じて改善します。

（３）情報資産の利用状況等調査の実施

① セキュリティ統括責任者及びセキュリティ統括責任者が指名した者は、情報資産の保護及び不正な取り扱いの防止を目的とする場合は、その運用管理状況や利用状況を調査することができます。

② 調査は、ログの取得、分析、送受信中のデータ取得、分析、記録の確認等の手段

により行います。

（４）緊急時対応

① セキュリティ統括責任者は、緊急時の連絡体制を整備します。

② ＣＳＩＲＴは、情報資産への侵害が発生した場合は、速やかに発生原因を調査し、対応します。状況により、セキュリティ統括責任者は、港区情報システムセキュリティ会議を招集し、再発防止策を検討及び実施します。

③ システム統括管理者は、情報資産への侵害が発生した場合は、ネットワークを物理的に遮断するなど、被害拡大の防止策を実施します。

④ 情報資産への侵害があった場合は、国や他の自治体等と連携し、適切に対応します。また、犯罪のおそれがある場合は、速やかに警察に通報します。

（５）港区情報安全対策指針の掲示

① セキュリティ統括責任者は、職員等が常に港区情報安全対策指針を閲覧できるように掲示します。

１０　情報安全対策指針の評価及び見直し

セキュリティ統括責任者は、情報資産を取り巻く環境の変化やセキュリティ監査の指摘に応じて、継続的に必要な評価及び見直しを行い、区民から信頼される ICT 環境を実現するための情報セキュリティ対策を実施します。