川崎市情報セキュリティ基準

はじめに

川崎市情報セキュリティ基準（以下「本基準」という。）は、川崎市情報セキュリティ基本方針に関する規程（平成１９年川崎市訓令第１号。以下「規程」という。）第５条の規定に基づき規程第３条に規定する情報セキュリティ対策を統一的に行うため、本市で扱う全ての情報資産を安全に管理運用及び利用するに際しての基準となる事項を定めるものとする。

なお、本基準で使用する用語の意義は、規程で定めるところによる。

改正履歴

版数	施行日	文書番号
第１版	平成 14 年 9 月 2 日	14 川総シ企第１２３号
第２版	平成 17 年 5 月 31 日	17 川総シ企第１５６号
第３版	平成 17 年 11 月 10 日	17 川総シ企第５８８号
第４版	平成 19 年 3 月 30 日	18 川総シ企第１３７５号
第５版	平成 20 年 3 月 28 日	19 川総シ企第１５００号
第６版	平成 24 年 3 月 26 日	23 川総行情第１９６６号
第７版	平成 25 年４月 1 日	24 川総行情第１５６３号
第８版	平成 27 年 5 月 13 日	27 川総Ｉ第１６９号
第９版	平成 27 年 12 月 1 日	27 川総Ｉ第７７１号
第 10 版	平成 28 年 3 月 31 日	27 川総Ｉ第１１９２号
第 11 版	令和 2 年 8 月 7 日	2 川総Ｉ第２４７号
第 12 版	令和 5 年 4 月 1 日	4 川総情第２８８７号
第 13 版	令和 6 年 4 月 1 日	5 川総デ第３６０３号

第１章　適用範囲

本基準の適用範囲は、次のとおりとする。

１　適用者

各局(規程第２条第１号)の職員及び本市の情報資産を取り扱う業務に従事する者（以下「職員等」という。）を対象とする。

２　適用する情報資産

各局で所管又は利用する情報資産を対象とする。

第２章　情報セキュリティの管理体制

１　情報管理における役割と責任

規程第４条第１項に定める情報セキュリティ管理体制及びその役割は次による。

（１）情報統括監理者

規程第４条第２項の規定により情報セキュリティ体制を統括する者（ＣＩＳＯ[1]）。

川崎市情報化施策の推進に関する規則（平成１９年川崎市規則第１２号。以下「規則」という。）第５条第１項に規定する情報統括監理者とする（ＣＩＯ[2]）。

（２）情報監理者

情報統括監理者を補佐する者。

規則第５条第３項に規定する情報監理者とする。

情報監理者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、情報統括監理者の指示に従い、情報統括監理者が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権限及び責任を有する。

（３）情報セキュリティ責任者

各局における情報セキュリティ対策の実施に関する権限及び責任を有する者として､情報セキュリティ責任者を置く。

情報セキュリティ責任者は各局の長とする。

（４）情報管理責任者

所管する情報資産を管理運用する者で情報セキュリティ（機密性、完全性及び可用性の保持）及び情報利用者の情報利用（アクセス）の可否判断等を行う。また、必要に応じて情報システム管理者に情報及び情報システムの管理運用を依頼する（原則として業務所管課長とする。）。

（５）情報利用者

情報及び情報システムを利用し、運用、更新等の業務を行う者で、情報管理責任者の指定に基づき、情報資産を利用する。

（６）情報システム管理者

情報管理責任者から情報及び情報システムの管理運用を依頼された者で、情報管理責任者

---

1 CISO: Chief Information Security Officer の略。

2 CIO: Chief Information Officer の略。CISO は、CIO を兼務する。

の依頼に基づき、情報資産を管理運用する（原則として情報システムを管理する課長とする。）。

（７）情報システム利用責任者

情報システムを利用し行う業務に対して責任を有する者で、情報及び情報システムの利用に関して職員を指導する（原則としてシステム利用所管課長とする。）。

（８）統括情報管理責任者

各局の情報セキュリティ責任者を補佐する者で、情報管理責任者及び情報システム管理者を統括する（原則として庶務担当課長とする。）。

（９）情報セキュリティ連絡員

各局の統括情報管理責任者の事務を補佐する者で、庶務担当課職員の中から統括情報管理責任者が選任する。

(10) 情報システムの管理運用が複数の組織にわたる場合

情報システムの管理運用が複数の組織にわたる場合は、管理運用上の役割及び責任を明らかにし、円滑な運用を行うため、各組織の情報管理責任者、情報システム管理者及び情報利用者等で構成する運用協議のための組織を設ける。

(11) 兼務の禁止

ア　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、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、同じ者が兼務してはならない。

イ　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

２　情報セキュリティ管理運営組織

本市の情報セキュリティ管理を運営するための組織は次のとおりとする。

（１）川崎市情報化推進本部

情報セキュリティに関する調整・協議を全庁的に行う。

規則第３条に規定する組織とする。

（２）情報セキュリティ管理会議（ＣＳＩＲＴ[3]）

情報セキュリティ対策を有効に機能させていくため、情報統括監理者を補佐する組織として、情報セキュリティ対策、規定類の立案、職員の研修及び啓発、情報セキュリティ監査等に関する事項を審議する情報セキュリティ管理会議を設置する。

なお、情報セキュリティ管理会議の運営等に関する事項は、情報統括監理者が別に定める。

また、情報セキュリティ管理会議は、情報セキュリティに関連する事故や障害が発生した場合に、統一的な窓口機能を担うほか、必要に応じて国や関係機関など外部の専門組織と連携し、適切な対応を図る。

３　各局におけるセキュリティ管理体制

情報セキュリティ責任者は、所管し、又は利用する情報資産について、本基準本章１に基づき、セキュリティ管理体制を組織し、情報セキュリティ管理会議（ＣＳＩＲＴ）に報告しなければならない。また、組織したセキュリティ管理体制に変更が生じた場合は、その変更につい

[3] CSIRT：Computer Security Incident Response Team の略。

て速やかに情報セキュリティ管理会議（ＣＳＩＲＴ）に報告しなければならない。

４　各局の協力

情報セキュリティ責任者と情報セキュリティ管理会議（ＣＳＩＲＴ）は、情報セキュリティ対策の実施に当たって、相互に緊密な連携を保ち、情報セキュリティ対策を適正かつ円滑に行わなければならない。

５　職員等の遵守事項

職員等は、公職に従事する者としての自覚を持ち、情報セキュリティの重要性について理解し職務に当たる。

（１）本基準及び実施手順の遵守

職員等は、本基準及び実施手順（以下「本基準等」という。）を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報管理責任者に相談し、指示を仰がなければならない。

（２）必要外の情報及び情報システムの利用の禁止

職員等は、自らの業務遂行に必要のない情報や情報システムを利用しない。

（３）情報の機密保持及び保全

ア　職員等は、業務上知り得た情報、情報の管理及び情報システムのアクセスに関する情報（以下「業務上知り得た情報等」という。）を業務目的外に利用しない。また、業務上知り得た情報等を第三者に流出したり改ざんされないよう、情報の保全に努める。

イ　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。また、その後も業務上知り得た情報等を漏らさない。

（４）会計年度任用職員、臨時的任用職員及び特別職非常勤職員への対応

ア　情報管理責任者は、会計年度任用職員、臨時的任用職員及び特別職非常勤職員に対し、採用時に、本基準等のうち守るべき内容を理解させ、また実施及び遵守させる。

イ　情報管理責任者は、会計年度任用職員、臨時的任用職員及び特別職非常勤職員の採用の際、必要に応じ、本基準等を遵守する旨の同意書への署名を求める。

６　情報保全義務の確認及び利用状況の調査

情報管理責任者及び情報システム利用責任者は、守秘義務のみならず、情報を適切に管理する義務（情報保全義務）について職員に説明し、理解させる。情報管理責任者及び情報システム利用責任者は、職員が情報保全義務を遵守しているかどうかを随時確認する。

情報統括監理者は、不正アクセス、不正プログラム等の調査のために、職員が使用している情報資産の利用状況を調査することができる。

７　情報セキュリティに関する情報の収集及び共有

情報管理責任者、情報システム管理者及び情報セキュリティ管理会議（ＣＳＩＲＴ）は、情報セキュリティに関する情報を互いに連携しながら収集し、必要に応じ、関係者間で共有するほか、情報セキュリティに関し、社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じる。

８　情報セキュリティ事故等の対応

（１）緊急時における連絡体制の整備

ア　情報統括監理者は、情報セキュリティ事故など緊急時の円滑な情報共有を図るため、情報監理者、情報セキュリティ責任者、統括情報管理責任者、情報管理責任者、情報システム管理者、情報システム利用責任者及び情報利用者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

イ　情報監理者は、緊急時には情報統括監理者に早急に報告を行うとともに、情報統括監理者が不在の場合には、自らの判断に基づき回復のための対策を講じなければならない。

ウ　情報監理者は、イにより情報統括監理者の不在時に対策を実施した場合は、情報統括監理者に対し事後報告を行う。

（２）事故等の対応

ア　職員は、情報セキュリティに関する事件又は事故が発生し、又は発生したと思料する事象を発見した際は、直ちに情報管理責任者又は情報システム利用責任者に報告し、指示を仰ぐこと。

イ　アにより報告を受けた情報管理責任者又は情報システム利用責任者は、情報統括監理者が別に定める規定により対応すること。

ウ　情報セキュリティ責任者は、情報監理者と協議の上、再発防止策の優先度を考慮し、計画的に対策を実施するものとする。

エ　情報監理者は、情報セキュリティに関する事故、規定の違反等により情報資産への侵害が発生した場合において連絡、調査、報告等を迅速かつ円滑に実施するため、必要な手続を別に定める。

（３）欠陥・脅威への対応

ア　職員は、情報システム若しくは情報システムが提供するサービスのセキュリティに関する欠陥を発見した場合、又は情報セキュリティに関する脅威を発見した場合及び情報セキュリティに関する脅威の疑いがあると判断した場合は、直ちに情報管理責任者又は情報システム利用責任者に報告する。

　報告を受けた情報システム利用責任者は、必要に応じて情報管理責任者及び情報セキュリティ責任者に報告する。また、情報管理責任者は、必要に応じて情報セキュリティ責任者に報告する。

イ　アにより報告を受けた情報管理責任者又は情報システム利用責任者は、関係者と連携し、脅威に対する対応又は欠陥の改修を行う。

９　委託事業者の管理

情報管理責任者は、本市で管理する情報システムの開発若しくは管理運用等の業務又は機密性区分Ⅰ若しくはⅡの情報(第３章２（１）を参照)を取り扱う業務（以下「情報システムの開発又は管理運用等」という。）を外部に委託する場合は、次の管理を行う。

なお、個人情報を取扱う委託業務等（指定管理業務を含む）については、本基準等に定める事項のほか、個人情報の保護に関する法律（平成 15 年法律第 57 号）（以下「個人情報保護法」という。）の規定が適用され、さらに、特定個人情報を取扱う委託業務については、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。）の規定が適用されることに留意する。

（１）委託契約の記載事項等

ア　委託契約書には、必要に応じ次の事項を明記し、契約締結に当たり本市の情報セキュリティに関する遵守事項を再委託事業者も含め説明する。

（ア）本基準等の遵守
（イ）個人情報の取扱いがある場合にはその管理事項
（ウ）委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
（エ）機密保持に関する事項
（オ）再委託の禁止又は制限に関する事項
（カ）指示目的外の使用及び第三者への提供の禁止に関する事項
（キ）情報の複写及び複製の制限に関する事項
（ク）情報の帰属に関する事項
（ケ）情報資産の授受、搬送、保管、返還又は廃棄等の管理事項
（コ）提供されるサービスレベルの保証
（サ）委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
（シ）事故発生時における報告義務等に関する事項
（ス）作業者に対する教育の実施に関する事項
（セ）市による検査に関する事項等
（ソ）本基準等が遵守されなかった場合の規定（損害賠償等）
（タ）その他情報セキュリティの確保に必要な管理事項

イ　個人情報を取り扱う業務を委託する場合には、「個人情報の取扱いに関する情報セキュリティ特記事項」を添付し、個人情報保護法に基づく安全管理措置を講じる。また、委託先が再委託をしようとする場合は、事前に書面により市の許諾を得た場合に限り行えることとし、再々委託以降も同様とする。

ウ　特定個人情報を取り扱う業務を委託する場合には、イに加え、「特定個人情報の取扱いに関する特記仕様書」を添付し、個人情報保護法及び番号法に基づく安全管理措置を講じる。また、委託先が再委託をしようとする場合は、事前に書面により市の許諾を得た場合に限り行えることとし、再々委託以降も同様とする。

エ　情報システム開発及び管理運用等を委託する場合は、委託先の選定要件として、情報セキュリティマネジメントシステム[4]、プライバシーマーク[5]の認定等を考慮して選定する。

オ　委託する業務で機密性区分Ⅰの情報を取り扱う場合は、委託先の責任者や作業者から機密保持等に関する誓約書を提出させる。また、機密性区分Ⅱの情報を取り扱う場合は、業務上の必要に応じて誓約書を提出させる。

（２）委託事業者への確認及び指導

---

[4] 企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組み。コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針（セキュリティポリシー）や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた、トータルなリスクマネジメント体系のことを指す。ISMS（Information Security Management System）の和訳。

[5] 日本情報処理開発協会（JIPDEC）が管理する個人情報取扱いに関する認定制度。有効期間は２年間。

ア　情報管理責任者は、委託事業者に機密性区分Ⅰ又はⅡの情報を貸与する場合は、委託事業者における本基準等の遵守状況を確認する。また、情報漏えい、改ざん等の防止対策について、本基準等の情報セキュリティに関する規定と同等以上の情報セキュリティレベルを確保していることを確認する。

イ　情報システムの開発又は管理運用等を委託する場合は、委託事業者に委託業務遂行過程における安全管理体制及び安全管理方法について、委託前に書面により提出させるとともに、提出した書面に基づき、業務遂行過程においても、遵守状況を把握する。

ウ　情報管理責任者は、委託事業者が受託した業務に関し、機密性区分Ⅰ又はⅡの情報を自ら取得する場合は、委託事業者の情報の保有に関し、本基準等の遵守状況を確認する。また、情報漏えい、改ざん等の防止対策について、本市と同等以上の情報セキュリティレベルを確保していることを確認する。

エ　情報管理責任者は、委託事業者等が所有又は利用する情報システムにおいて機密性区分Ⅰの情報を取扱わせる場合、当該情報システムが、本市と同等以上の情報セキュリティレベルが確保されていることを確認する。

オ　情報管理責任者は、委託事業者に機密性区分Ⅰ又はⅡの情報を貸与する場合は、受渡票等の書類により行う。

カ　情報管理責任者は、委託事業者が受託業務に関し、機密性区分Ⅰ又はⅡの情報を保有している場合は、委託業務終了後速やかに市に返却又は廃棄させなければならない。また、複写及び複製をしていないことを確認し、確実に返却又は廃棄されたことを書面により確認するものとする。

10　指定管理者等[6]に関する留意事項

情報管理責任者は、本市で管理する情報資産の取扱いを伴う事務事業を指定管理者等が実施する場合は、次の管理を行う。

（１）協定の記載事項等

ア　指定管理者等が本市の情報システムを利用して業務を行う場合には、本基準等を遵守する旨明記する。

イ　指定管理者等が機密性区分Ⅰ又はⅡの情報を取り扱う業務を行う場合には、本基準等を遵守する旨明記する。また、機密性区分Ⅰの情報を取り扱う場合は、指定管理者等の責任者や作業者から機密保持等に関する誓約書を提出させる。また、機密性区分Ⅱの情報を取り扱う場合は、業務上の必要に応じて誓約書を提出させる。

ウ　指定管理者等が個人情報を取り扱う業務を行う場合には、「個人情報の取扱いに関する情報セキュリティ特記事項」を添付し、個人情報保護法に基づく安全管理措置を講じる。また、指定管理者等が再委託をしようとする場合は、事前に書面により市の許諾を得た場合に限り行えることとし、再々委託以降も同様とする。

エ　指定管理者等が特定個人情報を取り扱う業務を行う場合には、ウに加え、「特定個人情報の取扱いに関する特記仕様書」を添付し、個人情報保護法及び番号法に基づく安全管理

---

6 地方自治法（昭和２２年法律第６７号）第２４４条の２第３項の規定により市の指定を受けたもの及び公営住宅法（昭和２６年法律第１９３号）第４７条の規定により公営住宅の管理を代わって行うもの

措置を講じる。また、指定管理者等が再委託をしようとする場合は、事前に書面により市の許諾を得た場合に限り行えることとし、再々委託以降も同様とする。

オ　指定管理者等が管理業務の遂行に当たり知り得た秘密を漏らしてはならない旨、及び当該業務以外の目的のために使用しない旨を明記する。また、指定管理者等でなくなった後であっても、同様とする旨を明記する。

カ　上記ア～オについて、情報管理責任者は、指定管理者等に対し、協定締結に当たり本市の情報セキュリティに関する遵守事項を説明する。

（２）指定管理者等への確認及び指導

ア　情報管理責任者は、指定管理者等が本市の情報システムを利用する場合は、本市と同等以上の情報セキュリティレベルが確保されていることを確認する。

イ　情報管理責任者は、指定管理者等が所有する情報システムを業務に利用する場合は、当該情報システムが、本市と同等以上の情報セキュリティレベルが確保されていることを確認する。

ウ　情報管理責任者は、指定管理者等が機密性区分Ⅰ又はⅡの情報を取り扱う場合は、本市と同等以上の情報セキュリティレベルが確保されていることを確認する。

エ　情報管理責任者が指定管理者等に機密性区分Ⅰ又はⅡの情報を貸与する場合は、指定管理者が本基準等を遵守していることを確認する。また、情報漏えい、改ざん等の防止対策について、本市と同等以上の情報セキュリティレベルを確保していることを確認する。

オ　情報管理責任者は、指定管理者等が公の施設の管理に関し、機密性区分Ⅰ又はⅡの情報を自ら取得する場合は、指定管理者等の情報の保有に関し、本基準等の遵守状況を確認する。また、情報漏えい、改ざん等の防止対策について、本市と同等以上の情報セキュリティレベルを確保していることを確認する。

カ　情報管理責任者は、指定管理者等に機密性区分Ⅰ又はⅡの情報を貸与する場合は、受渡票等の書類により行う。

キ　情報管理責任者は、指定管理者等が公の施設の管理に関し、機密性区分Ⅰ又はⅡの情報を保有している場合は、指定管理者等の協定終了後速やかに市に返却又は廃棄させなければならない。また、複写及び複製をしていないことを確認し、確実に返却又は廃棄されたことを書面により確認するものとする。

第３章　情報資産の管理状況の把握

１　情報資産の棚卸し

情報管理責任者は、所管する情報資産について棚卸しを行い、管理状況を把握し、情報資産台帳を作成する。

情報資産台帳の作成については、文書・図画、電磁的記録は作成年度の前年度分までを作成年度の８月３１日までに、情報システム、ハードウェア、ソフトウェア及び可搬媒体については随時、情報セキュリティ対策マニュアルに基づき作成する。

２　情報資産の分類

情報資産のうち、情報及び情報システムについて、機密性、完全性及び可用性の要求レベルを次のとおり評価・分類し、適正な取扱区分を明確にする。

なお、入手した情報資産の分類が不明な場合は、情報管理責任者に判断を仰がなければならない。

（１）機密性区分

情報資産について、個人情報等の保護の観点から、許可された者以外が情報の閲覧等をした場合の影響範囲について、情報セキュリティ関連法令等への準拠及び市民生活、行政運営等への影響度から次の区分を明確にする。

機密性区分	定義
区分Ⅰ	情報の漏えいなど機密性が侵害されることにより、市民の生命、財産、プライバシー又は法人等の競争上の地位や正当な利益に対して著しい影響が予想されるもの 例えば ・個人に関する情報（特定個人情報を含む。） ・公共の安全等に関する情報 ・法令の規定により秘密を守る義務を課されている情報 ・法人に関する情報 などの情報のうち機密性が侵害された場合、市民の生命、財産、プライバシー、又は法人等の競争上の地位や正当な利益に対して支障を及ぼすおそれがある情報
区分Ⅱ	情報の漏えいなど機密性が侵害されることにより、行政事務の執行等に著しい影響が予想されるもの 例えば ・法人等に関する情報 ・審議、検討又は協議に関する情報 ・事務又は事業に関する情報 ・法令等の規定により従う義務を有する国の機関等の指示に関する情報 などの情報のうち機密性が侵害された場合、行政事務の執行等に支障を及ぼすおそれがある情報
区分Ⅲ	区分Ⅰ、Ⅱ以外のもの

（２）完全性区分

情報資産について、破壊や改ざん等の意図しない情報の不備が発生することによる影響範囲について、市民生活、行政運営等への影響度から次の区分を明確にする。

完全性区分	定義
区分Ⅰ	改ざん、誤びゅう又は破壊などにより、市民の生命、財産、プライバシー又は法人等の競争上の地位や正当な利益に対して著しい影響が予想されるもの 例えば ・個人に関する情報（特定個人情報を含む。） ・公共の安全等に関する情報 ・法令の規定により秘密を守る義務を課されている情報 ・法人に関する情報 などの情報のうち完全性が侵害された場合、市民の生命、財産、プライバシー、又は法人等の競争上の地位や正当な利益に対して支障を及ぼすおそれがある情報
区分Ⅱ	改ざん、誤びゅう又は破壊などにより、行政事務の執行等に著しい影響が予想されるもの 例えば ・法人等に関する情報 ・審議、検討又は協議に関する情報 ・事務又は事業に関する情報 ・法令等の規定により従う義務を有する国の機関等の指示に関する情報 ・市民に公開している情報 などの情報のうち完全性が侵害された場合、行政事務の執行等に支障を及ぼすおそれがある情報
区分Ⅲ	区分Ⅰ、Ⅱ以外のもの

（３）可用性区分

情報資産について、許可された利用者が必要な時に情報及び情報システムを利用できない状況になった場合の影響範囲について、市民生活、行政運営等への影響度から次の区分を明確にする。

可用性区分	定義
区分Ⅰ	情報システムの停止など、当該情報資産が利用不可能であることにより、市民の生命、財産又はプライバシーに対して著しい影響が予想されるもの ・利用不可能により、市民の権利、市民の生活に影響を与える情報資産 ・復元が著しく困難である市民の権利、市民の生活に関する情報資産 例えば ・市民生活に影響を与える情報システム ・個人に関する情報（特定個人情報を含む。） など
区分Ⅱ	情報システムの停止など、当該情報資産が利用不可能であることにより、行政事務の執行等に著しい影響が予想されるもの ・利用不可能により、行政事務の執行に支障を与える情報資産 ・復元が困難であり、行政事務に支障を与える情報資産 例えば ・行政内部の執行に支障を与える情報システム ・保存期間未経過の完結文書 など
区分Ⅲ	区分Ⅰ、Ⅱ以外のもの

第４章　情報資産の管理

１　共通事項

情報資産の管理について、共通事項を定める。

（１）管理責任

ア　情報管理責任者は、その所管する情報資産について管理責任を有する。

イ　情報管理責任者は、業務上情報資産を複製した場合には、複製された情報資産も第３章２情報資産の分類に基づき管理しなければならない。

ウ　情報管理責任者は、情報資産の区分及び取扱方法を情報利用者に明示する。

（２）利用資格

ア　情報管理責任者は、アクセス制御ポリシー（情報を利用する利用資格を付与する方針）を作成し、アクセス制御ポリシーに従って情報資産の利用資格を付与する。

イ　情報管理責任者は、異動、休職、退職等による利用資格の停止、変更及び抹消は、速やかに行わなければならない。

ウ　利用資格は、業務上必要な範囲において、原則個人単位で付与する。

エ　利用資格、利用条件、資格の割当状況等は、定期的に見直しをする。

（３）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、情報の作成時に情報管理責任者の指示に従い、第３章２の区分に基づき、当該情報の分類を定めなければならない。

ウ　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を適切に廃棄しなければならない。

（４）情報資産の取得

職員等が情報資産を取得した場合には、第３章２の区分に基づき、当該情報の分類を定めなければならない。また、第３章１に基づき情報資産台帳の随時更新を必要とする情報資産を取得した場合は、情報資産台帳を更新する。

（５）情報資産の利用

ア　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。

イ　情報資産を利用する者は、情報資産の取扱区分に応じ、適切な取扱いをしなければならない。

ウ　情報資産を利用する者は、情報資産の取扱区分が異なる情報が複数含まれている情報資産を取り扱う場合、最高度の区分に従って、取り扱わなければならない。

エ　原則として、本市が保有する機密性区分Ⅰ又はⅡの情報資産は、外部に持ち出してはならない。ただし、業務上、機密性区分Ⅰ又はⅡの情報資産を外部に持ち出す場合は、次により対応する。

（ア）持ち出す情報資産は、業務上、必要最小限とする。

（イ）職員は、持ち出す情報資産の内容や持ち出す場所等を明確にして、情報管理責任者又は情報システム利用責任者の許可を得る。

（ウ）情報管理責任者又は情報システム利用責任者は、上記(イ)の許可をした場合は、許可の記録を作成し保管しなければならない。

（エ）職員は、外部に情報資産を持ち出している間、盗難や紛失等に十分注意する。

（オ）職員は、帰庁後速やかに情報管理責任者又は情報システム利用責任者に、情報資産を持ち帰った旨報告する。その際、情報管理責任者又は情報システム利用責任者は、持ち出した情報資産に紛失等がないことを確認する。

オ　職員は、庁舎外で情報処理業務を行う場合には、情報管理責任者の許可を得なければならない。

（６）情報資産の提供・公表

ア　業務上、機密性区分Ⅰ又はⅡの情報資産を外部に提供する場合は、情報管理責任者の許可を得なければならない。

イ　情報管理責任者は、市民に公開している情報について、完全性を確保しなければならない。

（７）情報の保管

ア　情報管理責任者又は情報システム管理者は、情報資産の取扱区分に従って、情報資産を適切に保管しなければならない。

イ　情報管理責任者は、法令及び関連制度の定めに従い所管する情報の保管期間を明確にする。また、法令等の定め以外にも、業務上の必要性、情報の重要度等に応じて保管期間を設定する。

ウ　情報管理責任者は、情報資産の保管場所を定め情報利用者に明示する。

エ　同一保管場所に、情報資産が複数保管されている場合は、最高度の区分に従って、情報セキュリティ対策を行う。

オ　同一保管場所に、複数の部署が機密性区分Ⅰ及びⅡの情報を保管する場合は、保管管理者を定め、保管管理者が情報の出し入れを行うか、入退出管理簿又は利用管理簿等により管理を行う。

カ　職員は、情報を情報管理責任者が指定する保管場所に適正に保管すること。

（８）情報の送信

原則、インターネットを利用する電子メールやＦＡＸなど機密性が確保できない通信手段を利用して機密性区分Ⅰに該当する情報を送信してはならない。

ただし、情報管理責任者が業務上特に必要と認める場合、相手方の送信先情報を送信者と別の人が確認する等誤送信に対する対策を行った上で送信する。また、機密性区分Ⅰ又はⅡに該当する情報を電子メールにより送信する場合は、暗号化[7]やパスワード設定を行って送信する。

（９）情報資産の廃棄

ア　情報資産の廃棄を行う者は、情報管理責任者の許可を得なければならない。

イ　機密性区分Ⅰ又はⅡの情報資産を廃棄する者は、情報を復元できないように処置した上で廃棄しなければならない。

ウ　情報資産の廃棄を行う場合には、廃棄する情報資産の重要度に応じて、行った処理について、日時、担当者及び処理内容を記録し、保存しなければならない。

---

[7] インターネットなどのネットワークを通じて文書や画像などのデジタルデータをやり取りする際に、通信途中で第三者に盗み見られたり改ざんされたりされないよう、決まった規則に従ってデータを変換すること。暗号化、復号には暗号表に当たる「鍵」を使うが、対になる2つの鍵を使う公開鍵暗号と、どちらにも同じ鍵を用いる共通鍵暗号がある。

エ　情報管理責任者は、情報資産が業務上必要なくなった場合かつ組織で保管する必要がなくなった場合は、速やかに廃棄手続を行う。また、第３章１に基づき情報資産台帳の随時更新を必要とする情報資産を廃棄した場合は、情報資産台帳を更新する。

２　文書及び図画の管理

（１）管理

ア　機密性区分Ⅰ又はⅡの文書及び図画(以下「文書等」という。)は、施錠可能な書庫又はロッカーで施錠管理するものとし、情報管理責任者が指定した鍵管理者による鍵の貸出制限により利用制限を行う。

イ　機密性区分Ⅰの文書等は、離席時に保管場所に戻さなければならない。ただし、一時的な離席の場合は、自席の引き出し等に保管することで足りる。

ウ　機密性区分Ⅱの文書等は、離席時に他の職員及び市民の目に触れない場所に一時的に保管しなければならない。

エ　機密性区分Ⅰ又はⅡの文書等は、業務上必要な場合に限り印刷をし、印刷後は、原本及び印刷物を速やかに回収する。

オ　機密性区分Ⅰ又はⅡの文書等を外部に持ち出す場合は、カバン等に入れて持ち運び、必ず手持ち管理を行う。

カ　機密性区分Ⅰの文書等を外部及び他部署に移送する場合は、鍵付きカバン等に入れて移送する。ただし、大量に移送する場合で、自動車により目的地へ直行する場合の移送は、この限りでない。

（２）廃棄

ア　機密性区分Ⅰ又はⅡの文書等を大量に廃棄する場合は、必ず職員が立ち会い、溶解、焼却等の廃棄を行う。

イ　機密性区分Ⅰ又はⅡの文書等を廃棄する場合は、シュレッダー等により、情報を復元できないように処理した上で廃棄する。

３　電磁的記録の管理

（１）管理

ア　機密性区分Ⅰ又はⅡの情報を個別のパソコン内に保存してはならない。

イ　庁内共有ファイルサーバを利用して保存する電磁的記録は、組織として保存する電磁的記録に限る。この場合において、ファイル等の整理・管理により効率的に情報資産台帳が作成できるように利用するものとする。

ウ　庁内共有ファイルサーバに個人情報を保存する場合は、パスワードによる保護等の措置を講ずる。また、必要に応じて、本章１（２）のアクセス制御ポリシーに基づく利用制限の設定を同サーバの管理者に依頼する。

エ　情報管理責任者は、情報利用者が利用するソフトウェアを適正に管理しなければならない。

オ　ソフトウェアを導入する場合は、情報管理責任者又は情報システム管理者の承認を得る。

カ　外部から入手したファイルは、ウィルスチェックを実施する。

キ　離席時には、コンピュータのロックやディスプレイの電源切断等により、ディスプレイに情報が表示されていない状態にする。

（２）廃棄

ア　パソコン、外付け記憶装置、可搬媒体及び庁内共有ファイルサーバに保存している電磁的記録は、定期的に整理を行い、不要な電磁的記録を廃棄しなければならない。

イ　パソコン、外付け記憶装置及び庁内共有ファイルサーバの返却や廃棄を行う場合は、データを完全に判読不能な状態にするため、物理的に破壊、又は専用ソフトウェアにより確実に電磁的記録を消去等した上で返却や廃棄を行う。

４　可搬媒体の管理

（１）管理

ア　原則として、市が所有していない可搬媒体（ＵＳＢメモリ、ＣＤ―ＲＯＭ、ポータブルＨＤＤ等をいう。以下同じ。）は業務で利用してはならない。

イ　ＵＳＢメモリを情報系ネットワークで利用する場合は、情報系ネットワーク接続パーソナルコンピュータ及び周辺機器の運営規約に基づく届出をしなければならない。

ウ　情報管理責任者又は情報システム管理者は、可搬媒体を保管する場合は、保管庫等を設けて所定の場所に保管しなければならない。

エ　情報管理責任者又は情報システム管理者は、情報を記録した可搬媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

オ　情報管理責任者又は情報システム管理者は、利用頻度が低い可搬媒体や情報システムのバックアップで取得したデータを記録する可搬媒体を長期保管する場合は、別個の施設、遠隔地での保管及び自然災害を被る可能性が低い地域に保管することを考慮する。

カ　情報管理責任者又は情報システム管理者は、機密性区分、完全性区分又は可用性区分がⅠの情報を記録した可搬媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な保管庫等に保管し、施錠管理、入退室管理簿等により部屋の入退室管理を行う。

キ　機密性及び完全性区分Ⅱの情報を保存している可搬媒体は、施錠可能な書庫又はロッカー等に保管し、施錠管理、入退室管理簿等により部屋の入退室管理を行う。

ク　機密性及び完全性区分がⅠ又はⅡの情報を保存している可搬媒体は、情報管理責任者が指名した鍵管理者により、利用者のみに利用させるための鍵貸出管理を行う。

ケ　情報管理責任者又は情報システム管理者は、情報技術の変化、可搬媒体の耐用年数等を考慮し、同一又は他の種別の可搬媒体への変換、データ・ファイル形式の変換等の措置を講じなければならない。

コ　機密性区分、完全性区分及び可用性区分がⅠ又はⅡの情報が保存されている可搬媒体（ＵＳＢメモリを除く。）を利用する場合は、利用記録を作成し、貸出返却を確実に行う。

サ　機密性、完全性、可用性の区分に関わらず、ＵＳＢメモリを利用する場合は、利用記録を作成し、貸出返却を確実に行う。

シ　可搬媒体に保存している情報は、必要に応じて定期的なバックアップや毎日の差分バックアップを行う。

ス　離席時には、機密性区分Ⅰの情報が保存されている可搬媒体は元の場所へ返却し、機密性区分Ⅱ又はⅢの情報が保存されている可搬媒体は、他の職員や市民の目に触れない場所に一時的に保管する。

セ　外付け記憶装置は、セキュリティワイヤー等の使用により機器の盗難防止を行う。

ソ　情報管理責任者又は情報システム管理者は、可搬媒体を所定の場所を定めて保管し、職

員に個々に保管させない。

タ　外部から入手した可搬媒体は、ウィルスチェックを実施してから使用する。

チ　可搬媒体に保存された情報が消去されていても、ソフトウェアにより復元できることを認識し、機密性区分Ⅰ又はⅡの電磁的記録を保存した可搬媒体は、適正に管理する。

（２）持ち出し及び移送中の保護

原則として、データ等を記録した可搬媒体の外部への持ち出しはしない。ただし、可搬媒体を外部保管する場合など持ち出す必要がある場合には、情報管理責任者又は情報システム利用責任者の許可を得て、持ち出す内容等を記録、保管し、盗難や紛失等に十分注意し、帰庁後速やかに報告を行うほか、次により取り扱う。

ア　可搬媒体は、移送中の物理的損傷や紛失等から保護するため、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等を行う。

イ　機密性区分Ⅰの情報が保存されている可搬媒体を外部保管又は外部提供する場合は、鍵付ケース等に格納して、職場から目的地へ直行する。

ウ　機密性区分Ⅱの情報が保存されている可搬媒体を外部保管又は外部提供する場合は、必ず手持ち管理を行い、職場から目的地へ直行する。

エ　機密性区分Ⅲの情報が保存されている可搬媒体を外部保管又は外部提供する場合は、必ず手持ち管理を行う。

オ　機密性区分Ⅰ又はⅡの情報を保存していたＵＳＢメモリ等を別の情報の外部提供に利用する場合は、必ず専用ソフトウェアにより完全消去を行った上で、使用する。

（３）廃棄

機密性区分Ⅰ又はⅡの情報を保存している又は保存していた可搬媒体を廃棄する場合は、データを完全に判読不能な状態にするため、物理的に破壊した上で廃棄する。また、廃棄を行う場合は、実施日時、破壊した媒体の数量、残骸の写真等を記録した廃棄記録を作成する。

第５章　職員の研修と啓発

情報及び情報システムの取扱いにおける事故や不正な行為を防止するため、職員は自ら情報セキュリティに関する知識の習得や能力の向上に努め、情報管理責任者及び情報システム利用責任者は組織において適切な研修、訓練等を行う。

１　情報及び情報システムを取り扱う職員に必要な能力

職員は、情報及び情報システムの取扱いに際し、情報セキュリティに関する十分な知識を持って当たらなければならない。このため、情報セキュリティのｅラーニング研修の受講や定期的な訓練への参加等を通して、自ら積極的に情報セキュリティに関する知識の習得や能力の向上、情報収集等に努める。

２　規程等の周知

情報管理責任者及び情報システム利用責任者は職員が常に規程及び本基準等を確認できるように常備しなければならない。

３　研修及び訓練

（１）情報監理者は、毎年新規採用の職員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。この場合、任命権者が行う新規採用研修で行う情報セキュリティ研修をもって換えることができる。

（２）情報監理者は、定期的に、ＩＣＴ分野の技術的動向に対応した情報セキュリティに関する研修、訓練等を立案するとともに、集合研修や通年受講可能なｅ ラーニング等を活用し、毎年度１回以上は職員が情報セキュリティに関する研修を受けられるようにし、職員の情報セキュリティの向上を図る。

（３）情報管理責任者は、業務に必要な情報セキュリティに関する研修開催や訓練実施等、職員のセキュリティリテラシーの向上を図る。

（４）職員は、定められた研修、訓練等に参加し、毎年度１回以上は情報セキュリティ研修を受講しなければならない。情報セキュリティの考え方や本基準等に対する理解を深め、情報セキュリティの確保に努める。

第６章　情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じるものとする。

１　マイナンバー利用事務系

（１）マイナンバー利用事務系[8]と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と他の領域との通信をする必要がある場合は、通信経路の限定（ＭＡＣアドレス、ＩＰアドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、ＬＧＷＡＮを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

（２）情報のアクセス及び持ち出しにおける対策

ア　情報のアクセス対策

「知識」、「所持」及び「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（多要素認証）を行うよう設定しなければならない。

イ　情報の持ち出し不可設定

原則として、外付け記憶装置、及びＵＳＢメモリ等の可搬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。

（３）マイナンバー利用事務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

マイナンバー利用事務系の端末・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上の情報システムの領域については、マイナンバー利用事務系として扱い、本市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。

（４）マイナンバー利用事務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

マイナンバー利用事務系の情報システムをガバメントクラウド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。その場合、暗号は十分な強度を持たなければならない。また、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、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。

２　ＬＧＷＡＮ接続系

（１）ＬＧＷＡＮ接続系[9]とインターネット接続系[10]の分割

---

8 個人番号（社会保障、地方税若しくは防災に関する事務）を取り扱う情報システム、共通基盤システムと連携する情報システム及び個人や法人の特定に利用する番号を有する情報システムが存在する領域をいう。

9 マイナンバー利用事務系及びインターネット接続系に属さない、ＬＧＷＡＮに接続可能な情報システムが存在する領域をいう。

10 インターネットメール、ホームページ管理システム等に関わるインターネットに接続された

ＬＧＷＡＮ接続系とインターネット接続系との通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、インターネット接続系からメールや添付ファイル、その他のデータをＬＧＷＡＮ接続系に取り込む場合は、無害化通信[11]を図らなければならない。

（２）ＬＧＷＡＮ接続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

ＬＧＷＡＮ接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をＬＧＷＡＮ接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

３　インターネット接続系

（１）インターネット接続系においては、情報セキュリティインシデントの早期発見と対処等のため、通信パケットの監視、ふるまい検知等の不正通信の監視機能を強化しなければならない。

（２）インターネット接続口を集約する自治体情報セキュリティクラウドに参加するとともに、関係機関と連携しながら、情報セキュリティ対策の推進を図る。

（３）業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、定期的に外部監査を実施しなければならない。

情報システムが存在する領域をいう。

11 インターネットメールの本文のみをテキスト化して転送、端末への画面転送等により、コンピュータウィルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

第７章　物理環境セキュリティ

情報及び情報システムの保管・設置場所は、不正な侵入、不正な利用及び災害等による脅威を排除するための環境的要件を整えるとともに、入退室の制限等の管理を行う。また、情報システムの機器については、設置、移設及び廃棄の各段階において適切な管理を行う。なお、外部サービスについては、別に定める川崎市外部サービスの利用に係るガイドライン（以下「外部サービス利用ガイドライン」という。）に基づき対策する。

１　情報セキュリティ管理エリア

情報管理責任者及び情報システム管理者は、情報及び情報システムを不正な侵入による盗難、不正利用等の脅威及び火災等の災害から保護するために、これらを保管・設置する庁舎及び施設に対して適切な措置を講じる。

（１）情報セキュリティ管理エリア

情報管理責任者又は情報システム利用責任者が定める情報システムの主装置が保管・設置されている場所をいう。

（２）情報セキュリティ管理エリアにおける物理的対策

機密性、完全性区分がⅠ又はⅡの情報システム及びデータ等を取り扱う管理エリアについては、独立した専用の区画とし、地震対策を講じた建物であり、情報システムに影響を与えない消火設備又は消火器を設置すること。ただし、独立した専用の区画が確保できない場合は、専用の鍵付サーバラックによりサーバ[12]等を管理すること。この場合、間仕切り等により一般の人が出入りできない場所に設置すること。

（３）情報セキュリティ管理エリアにおける入退室管理

職員等及び委託事業者は、市の指定する名札の着用を徹底し、部外者と明確に区別するほか、情報セキュリティ管理エリアに入室する場合、身分証明書等を携帯し、求めに応じ提示する。また、情報セキュリティ管理エリアへの入退室は、これを許可された者のみに制限し、ＩＣカード、生体認証や入退室管理簿の記載による入退室管理を行う。

なお、入退出のログの保存期間は、管理の必要に応じて、情報管理責任者が定めるものとするが、ログの保存期間は、公表しないものとする。

（４）機器等の搬入出における留意事項

ア　印刷物、荷物等の受渡しを行う際は、相手方を確認し、必要に応じて搬入物の記録を行う。また、可能な限り情報及び情報システムの保管・設置場所からは離れた場所で受渡しを行う。

イ　情報セキュリティ管理エリアに機器の搬入出を行う場合は、事前に情報管理責任者又は情報システム管理者の許可を得なければならない。また、搬入出について、職員が立ち会わなければならない。

---

12 コンピュータネットワークにおいて、他のコンピュータに対し自身の持っている機能やサービス、データ等を提供するコンピュータのこと。また、そのような機能を持ったソフトウェアのこと。「データベースサーバ」、「Web サーバ」など、提供する機能などの種類を冠して「○○サーバ」と称することが多い。

２　執務室等の管理

（１）機密性区分Ｉの情報資産を取扱う執務室等は、職員以外の者が無断で入室できないよう、受付カウンター、扉、間仕切り等必要な対策を講じる。

（２）執務室内等で委託事業者に情報処理作業を行わせる場合、市の指定する名札の着用を徹底し、部外者と明確に区別する。

３　機器の管理

情報管理責任者は、情報セキュリティ管理エリアに設置される情報システムの機器（サーバ、端末、パソコン、ネットワーク機器、ケーブル等をいう。以下同じ。）を適切に管理するための措置を講じる。

（１）管理責任

業務で職員が共同して利用する情報システムの機器は、共通設備として情報管理責任者又は機器を設置している課の長（これに準ずる者を含む。）が管理責任を持つ。

（２）機器の設置及び台帳等による管理

情報システムの機器は、その重要度に応じて、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エリアに設置し、台帳等により管理する。

（３）機器の冗長化[13]等の対策

情報管理責任者又は機器を設置している課の長（これに準ずる者を含む。）は、可用性区分Ｉ又はⅡのデータを格納している機器については、万が一に備え、業務が継続できるよう冗長化等を行うなど、システムの運用停止時間を最小限にできるように対策を施す。

（４）機器を設置する際の留意事項

ア　電源

（ア）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に十分な電力を供給する容量の予備電源を備え付ける。

（イ）落雷等による過電流に対し、機器を保護するための措置を講じる。

イ　ケーブル

情報システムの接続ケーブル、通信ケーブル等を損傷や切断等の脅威から保護するため、配線収納管を使用する等必要な措置を講じる。また、ネットワークの接続口は、情報利用者以外の者が不正に接続できない場所に設置する。

ウ　その他

新たに機器を搬入する場合は、既存の情報システムに与える影響について、事前に職員又は委託した業者が確認した上で設置する。

（５）機器の移設・廃棄及び修理・保守

ア　台帳等への反映

情報システムの機器を移設・廃棄及び修理・保守する場合は、情報管理責任者又は機器を設置している課の長（これに準ずる者を含む。）の了承を得て行い、結果を台帳等に速やかに反映する。

---

[13] 障害に備えて機材や回線などを複数用意し、並列に使用したり一部をすぐ使える状態で待機させたりする考え方を冗長と呼び、システムをそのように設計・配置することを冗長化という。

イ　機器の廃棄等

（ア）情報システムの記憶装置（ハードディスク）等を処分（廃棄・返却）する場合は、事前に保存されている情報を確実に消去した上で引き渡し、機密性区分等に応じた方法により、保存されている情報を確実に消去、判読不能な状態にする。

（イ）また、委託等により事業者に機器の廃棄を行わせる場合は、処理内容を記録した証明書等を事業者に提出させる。

（ウ）マイナンバー利用事務系の情報又は大量の個人情報が保存された記憶媒体の廃棄を行う場合は、市の管理下で実施し職員が立ち会う等確実な履行を担保する。

ウ　修理・保守時の管理

情報システムの機器の修理・保守に際しては、ハードディスク等に機密性区分Ⅰ又はⅡのデータ等が保存されている場合は、原則事前にバックアップの上、データ消去ソフトなどを使用して保存されている情報を確実に消去し、判読不能な状態にする。消去が困難な場合は、保守契約等において機密保持やデータの保全、機器の破壊処理等に関する事項を明記する又はオンサイト修理[14]を行う。

（６）庁舎外への機器の設置

情報管理責任者又は機器を設置する課の長（これに準ずる者を含む。）は、庁舎外にサーバ等の機器を設置する場合、情報監理者の承認を得るものとする。また、定期的に当該機器に関する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。

（７）機器の持ち出し及び持込み

ア　原則として、本市の情報機器の持ち出しはしない。業務上必要な場合は、情報管理責任者又は情報システム利用責任者の許可を得ること。

イ　情報管理責任者又は情報システム利用責任者は、機密性区分Ⅰ又はⅡの情報システムの管理エリアには、パソコン、モバイル端末、可搬媒体等の情報機器を持ち込ませない。ただし、業務上必要と認める場合は、事前に許可し、機器等を持ち込ませることができる。

ウ　情報管理責任者又は情報システム利用責任者は、許可した情報機器の持ち出しや持込みについて記録を作成し、保管する。

14 製品が故障した際に、技術者が機器の設置場所へ修理しに来る修理方式のこと。

第８章　情報システムの管理運用

情報システムを適正に管理運用するための手続を具体化し、情報システム及びデータ等を漏えい、改ざん、不正アクセス、障害等から保護するため、安全かつ安定的な運用を確保する。

１　情報システムの管理運用手順の整備

情報管理責任者は、次のマニュアル類を整備し、これらに従って情報システム及びデータ等を管理運用する。

（１）情報セキュリティ実施要領等の整備

所管する情報システムの開発、運用、保守管理及び利用に当たっては、情報セキュリティを確保するために遵守すべき手続を具体的に定めた情報セキュリティ実施要領等の実施手順を整備する。

（２）手順書の整備

ア　管理運用手順書[15]（管理運用マニュアル）

データ等の管理方法、情報システムの処理・操作手順、処理の正当性の確認手順等を内容とする管理運用手順書を整備する。

イ　障害対応手順書[16]（障害対応マニュアル）

情報システムの誤動作・機能の停止、不正アクセス、データ等の消失、データ等の漏えい等の情報システムに関する障害及び事故に対し、迅速かつ効果的に対応するための手順等を内容とする障害対応手順書を整備する。

（３）情報システムの管理運用記録の整備

管理運用手順書に基づいた情報システムの管理運用が行われている証跡として、オペレーション計画書、オペレーション指示書等を管理運用作業に先立ち作成する。また、管理運用作業終了後、オペレーション実施記録を整備する。

（４）情報システムの障害記録の整備

障害対応手順書に基づいた対応が行われていること及び障害対応手順書が有効に機能していることの証跡として、障害記録書を作成する。

（５）情報システム利用手順書（情報システム操作マニュアル、業務手続）の整備

利用職員における情報システムの操作方法、データ等の管理方法等の情報保全義務に関する手順等を内容とする情報システム利用手順書を整備する。

（６）重要な業務の分散及び相互牽制

手順の整備に当たっては、不注意又は故意による情報システム及びデータ等の誤用や不正使用のリスクを軽減するため、職務と責任の範囲を明確にする。

また、ユーザの登録やシステム設定の変更等の重要な業務が特定の職員に集中することのないよう複数の職員に職務や権限を分散し、職員が相互に重要な業務の操作履歴を確認する等相互牽制の仕組みを組み込む。

---

[15] 管理運用手順書に記述する事項としては、情報の管理、利用者の管理、通常の処理・操作手順、処理の正当性の確認、データ、ソフトウェア等のバックアップ、帳票の管理等がある。

[16] 障害対応手順書に記述する事項については、第 11 章の災害復旧手順書と共通するためそちらを参照。ただし、両者は想定する原因や影響（市民生活や行政運営への影響）の規模が異なるため、具体的な内容のレベルでは、異なるものになることに留意する。

２　コンピュータウィルス対策

情報管理責任者は、情報システムへのコンピュータウィルス等の侵入を防ぎ、感染した場合は、他への被害の拡大を防ぐとともにその駆除を行う。

（１）ウィルス対策ソフトの導入とウィルスチェック

ア　情報システムのサーバ（単体のパソコンを含む。）及びクライアント[17]には、ウィルス対策ソフトを導入し、定期的にウィルスチェックを実施する[18]。

イ　ウィルス対策ソフト及びそのウィルスパターン定義は常に最新の状態に保つ。

ウ　外部から入手したファイル（可搬媒体により外部から入手したファイル、インターネットを経由したダウンロードファイル及び電子メール添付ファイル等）は、ウィルスチェックを実施して安全を確認してから使用する。

（２）未知の不正プログラム対策

パターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動を監視・検出・特定する。情報監理者は、異常な挙動を検出した際には、当該情報システム・端末をネットワークから論理的に隔離する等、必要な措置を講じなければならない。

（３）情報収集、注意喚起等

情報セキュリティ管理会議（ＣＳＩＲＴ）、情報管理責任者、情報システム管理者等は、常にコンピュータウィルスなど情報セキュリティに関する情報の収集に努め、職員に対してウィルスの危険性に関する注意喚起、周知等を行う。

（４）専門家の支援体制

情報統括監理者は、実施している不正プログラム対策を講じてもなお、万一、情報セキュリティ事故等が発生した場合に備え、外部の専門家の支援を受けられるようにする。

３　データのバックアップとログ[19]の取得

情報管理責任者は、情報システム及びデータ等の復旧並びに不正・不当なアクセス活動の検知に備え、データ等のバックアップ、ログの取得・保管等を行う。

（１）データ等のバックアップ

データ等の完全性区分、可用性区分、業務継続の要求レベル等に基づいて情報システムの復旧に必要な要件を明確にし、管理運用手順書、障害対応手順書等に反映させる。この中でデータバックアップの間隔や範囲等についても定め、これに基づいて情報システムの復旧に必要なデータ、ソフトウェア等のバックアップを実施し、必要に応じて復元テストを実施する。

---

17 コンピュータネットワークにおいて、サーバコンピュータの提供する機能やデータを利用するコンピュータのこと。

18 情報システムの設置環境を勘案し、組織全体のメールサーバ、ローカルサーバ及び各クライアントのそれぞれに対して対策を実施することが求められる。

19 ログ：情報システムを利用した場合に記録される履歴情報。例えば、利用者が取り扱った情報とその操作の記録等である。一般的には、情報システムにおいて自動的に取得されるもので、操作記録等の手書きの台帳とは異なる。

（２）ログの取得と保管

ア　ログの取得について

情報管理責任者は、情報システムの操作記録、利用者の活動、正確な日付及び時刻、例外処理及びセキュリティ事象等を記録し、管理する。

イ　ログの保管について

ログの保管に際しては、消去、改ざん等から保護するための措置を講じる。

ウ　ログが取得できなくなった場合の対処等について

情報管理責任者は、ログが取得できなくなった場合の対処等について定め、適切にログを管理するほか、必要に応じて不正アクセス等の有無について点検又は分析を実施する。

エ　ログの保存期間について

ログの保存期間は、関係法令等を確認の上、業務の必要に応じ情報管理責任者が定める。ただし、アクセスログの保存期間は、不正アクセス防止の観点から長期間保存し、保存期間は公表しないものとする。

（３）時刻の正確性の担保

データ等の処理の過程の記録や不正・不当なアクセスの検知等に利用するため、コンピュータの時刻は正確に設定する。

４　可搬媒体の取扱い

情報管理責任者及び情報システム利用責任者は、データ等を記録した可搬媒体について、第４章４の定めに従い取り扱う。

５　データ等の受渡し

情報管理責任者は、本市内部又は外部とのデータ等の受渡しを行う場合には、授受の方法、相手方の確認方法、当事者相互の責任、管理体制、管理方法等を文書で定めて確認する。また、データ等の授受は文書により送受日、送受部署名、送受者、データ名称、数量、媒体の形式等を明らかにし、相互で確認しなければならない。

６　情報システムの利用資格の管理（アクセス制御）

データ等の漏えい、改ざん等の危険性を最小限にするため、情報システム及びデータ等は業務遂行に際して必要な職員のみが利用することを原則とする。

このため、情報管理責任者は、情報システム及びデータ等の利用資格の明確化並びに利用資格の管理を行い、利用を適切に制御する。

なお、ここでは職員の利用資格の管理について記述しているが、本市外部の不特定多数のユーザを対象にサービスを提供する情報システムにおいては、取り扱うデータ等の保護の必要性等に応じて、その利用資格及び利用についても適切に管理する。

（１）利用資格の明確化

業務上のセキュリティ要件並びに情報システム及びデータ等を利用する者の利用資格及び利用条件（アクセス権）を明確にし、管理運用手順書に規定する。

（２）利用資格の管理

ア　利用資格の管理手順

利用資格の付与、停止、変更及び抹消手順を管理運用手順書に規定する。

イ　利用資格の管理

利用資格の付与に際しては、アクセス制御ポリシーに従って利用資格及び利用条件を確認し、条件に合った利用資格を付与する。また、異動、休職、退職等による利用資格の停止、変更及び抹消は速やかに行う。

なお、利用資格の付与に際しユーザＩＤを発行する場合は、利用状況を適切に管理するため、原則として個人単位に発行する。

ウ　定期的な見直し

利用資格、利用条件、資格の割当状況等は定期的に見直す。

（３）特権資格（情報システムの管理者権限）の管理

ア　特権資格の付与

（ア）特権資格を付与する際は、必要最小限の権限を必要最小限の者にのみ与えることとし、特権資格を通常の業務運用には使用しない。

（イ）特権資格を付与する場合は、情報管理責任者又は情報システム管理者の許可を得なければならない。

（ウ）特権資格のパスワードは、職員等のパソコン等の端末のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（エ）情報管理責任者又は情報システム管理者は、特権資格のＩＤを初期設定以外のものに変更しなければならない。

イ　付与状況の記録

特権資格の付与の状況を記録し、管理する。

ウ　特権資格による接続時間の制限

情報管理責任者又は情報システム管理者は、特権資格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制限しなければならない。

（４）ユーザパスワード（利用者が情報システムへアクセスする際のパスワード）の管理

ア　有効なパスワードの設定

ユーザパスワードは十分な長さとし、文字列は想像しにくいものにする。

イ　ユーザパスワードの再発行時の本人確認

ユーザパスワードの再発行は、本人又は所属組織からの正規の申請であることを確認した後に行う。また、その際に古いパスワードを原則再使用しない。

ウ　ユーザパスワードの定期的な変更

ユーザパスワードは定期的に変更する。

また、パスワードの変更をユーザが行える情報システムにおいては、仮パスワード発行後、速やかにパスワード変更を行うとともに、定期的に変更を行う。

エ　多要素認証[20]による対策

マイナンバー利用事務系では、パスワード等の「知識」による認証、ＩＣカード等の「所持」による認証、あるいは生体等の「存在」による認証など、異なる複数の認証要素を組み合わせた多要素認証による対策を施す。

---

20 複数の認証要素を併用して精度を高めたもののこと。認証要素は、大きく分けて、ID/パスワードなど対象者の知識を利用したもの、USB トークンやスマートカードなど対象者の持ち物（所持）を利用したもの、バイオメトリクスなど対象者の身体の特徴（存在）を利用したものの 3 つに分かれる。

オ　パスワード等認証情報の管理

情報管理責任者又は情報システム管理者は、職員等の認証情報を厳重に管理する。また、認証情報ファイルを不正利用から保護するため、認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用する。

7　情報システムの監視

情報管理責任者又は情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

8　情報システム及びネットワークの管理

情報管理責任者は、情報システム及びネットワークへの不正なアクセス、負荷による性能低下等を防ぐため、ネットワーク及び通信機器を適切に管理する。

（1）構成管理

ア　全体構成の把握

ネットワークの全体構成を把握するため、回線、機器等の接続状況を図面化する。

また、構成に変更があった場合は速やかにこれを図面に反映し、常に現況を把握できるようにする。

イ　構成監視

無許可の機器の接続等を監視し、異常を検知して速やかに対処することにより、ネットワークの機密性及び運用の継続性を担保する。

（2）障害管理

ア　潜在的な障害の可能性の把握

情報システム及びネットワークのセキュリティやユーザへのサービスに脅威をもたらすおそれのある潜在的な隘路（ボトルネック）並びに最も負荷の掛かる処理の箇所を明らかにし、業務への支障があると判断される場合は是正する。

イ　障害監視

回線の断線、通信機器の故障等を監視し、異常を検知して速やかに対処することにより、ネットワークの運用の継続性を担保する。

（3）性能管理

可用性区分Ⅰの情報を取り扱う情報システムが接続される通信回線は、継続的な運用を可能とする回線を選択するほか、必要に応じ、回線を冗長構成にする等の措置を講じる。また、ネットワーク及び通信機器のトラフィック[21]、情報システムの負荷状態等を監視し、異常を検知して速やかに対処することにより、ネットワークの運用の継続性を担保する。

（4）機密管理

ア　アクセスログの取得

悪意ある第三者等による不正侵入、不正操作等の事故が発生した際の調査・分析に備えるため、通信機器等（ファイアウォール[22]、WWWサーバ、メールサーバ等を含む。）や特

---

21 通信回線やネットワーク上で送受信される信号やデータのこと。

22 あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこ

に重要なデータ等に関するアクセスログを取得する。

イ　機密監視

悪意ある第三者による不正侵入、不正操作等による被害を防ぐため、定期的にアクセスログの確認を行うとともに不正なプロトコル[23]を監視し、異常を検知して速やかに対処することにより、ネットワークの機密性及び運用の継続性を担保する。

ウ　アクセスログ等の保存

システムから自動出力したアクセスログ等は、一定の期間保存しなければならない。

（５）遠隔管理

ア　遠隔接続ユーザの認証

庁内の情報システムと遠隔地にある本市の情報システムとの間の接続においては、相手方のユーザ及び情報システムの認証[24]を行う。

イ　遠隔監視及び遠隔診断[25]時の留意事項

情報システムの遠隔監視及び遠隔診断を行う場合は、アクセス用の診断ポートを確実に保護する。

（６）不正アクセス対策

ア　措置事項

不正アクセス対策として、以下の事項を措置しなければならない。

（ア）使用されていないポート[26]を閉鎖する。

（イ）使用されていない不要なサービスについて、機能を削除又は停止する。

（ウ）不正アクセスによるウェブページの改ざんを検出した場合には、速やかに情報セキュリティ責任者へ報告する。

（エ）外部から改ざんされる可能性がある重要なシステムの設定を行ったファイル等について、リスクに応じて当該ファイルの改ざんの有無を検査し、情報セキュリティ責任者に報告する。

（オ）情報管理責任者又は情報システム管理者は、ログイン時におけるメッセージ等により、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ようシステムを設定する。

イ　攻撃への対処

情報セキュリティ責任者は、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。また、関係機関と連絡を密にして情報の収集に努めなければならない。

ウ　記録の保存

サーバ等に攻撃を受け、当該攻撃が犯罪の可能性がある場合には、攻撃の記録を保存す

と。

23 複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。

24 認証の方法としては、ハードウエア・デバイスによるもの（例えば、特定のICカードが差し込まれていない機器はアクセスさせない。）、IPアドレスの確認によるもの等がある。

25 遠隔地から特定のポートを経てアクセスし、情報システムの監視、診断を行うこと。

26 外部とデータを入出力するための、ソフトウェアやハードウェアの末端部分（インターフェース）のこと。

るとともに、警察及び関係機関との緊密な連携に努めなければならない。

エ　職員による不正アクセス

職員による不正アクセスを発見した場合は、当該職員が所属する課の長（これに準ずる者を含む。）に通知し、適切な処置を求める。

オ　標的型攻撃[27]

情報管理責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育、研修等の人的対策を講じる。また、組織内部への侵入を低減する対策（入口対策）並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じる。

カ　サービス不能攻撃

情報管理責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、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る。

（７）セキュリティホール[28]に関する情報の収集・共有及びソフトウェアの更新等

情報管理責任者又は情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有する。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施する。

（８）個人の情報機器等の接続禁止

本市が所有する情報システムには、職員個人が所有するパソコンや所定の手続を経ていない情報機器は接続しない。

（９）通信回線のセキュリティ対策

ア　機密性区分Ⅰ又はⅡ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、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

イ　ネットワークに使用する回線については、伝送途上で情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施する。

（10）無線ＬＡＮ[29]の使用

ア　マイナンバー利用事務系のネットワークでは、無線ＬＡＮを使用しない。

---

27 特定の個人や組織、情報を狙ったサイバー攻撃のこと。例えば、ウィルスメールの件名や本文、偽装された送信元、添付ファイル名などに、対象と関わりのある実在の組織や人物、事業などの名称を記し、対象者の油断を誘って感染させるといった手法がよく用いられる。また、攻撃が発覚しにくいよう痕跡を消去したり、侵入に成功したシステムに長期間潜伏し、繰り返し情報を窃取する場合もある。

28 ソフトウェアの設計ミスなどによって生じた、システムのセキュリティ上の弱点のこと。攻撃を受けると、外部のユーザが本来実行できない操作が可能になるため、Web サーバで公開されている情報が改ざんされたり、機密データが漏洩したり、他のコンピュータへ不正アクセスするための踏み台に利用されたりする。

29 無線でデータの送受信を行う構内通信網（LAN：Local Area Network）のこと。特に、IEEE 802.11 諸規格に準拠した機器で構成されるコンピュータネットワークのことを指す場合が多い。「アクセスポイント」と呼ばれる中継機器（又はその機能を内蔵したルータなど）を中心に、無線通信機能を持ったコンピュータなどが相互に接続され、ネットワークを形成する。

イ　情報管理責任者は、所管するＬＧＷＡＮ接続系及びインターネット接続系のネットワークで無線ＬＡＮを使用しようとする場合は、情報監理者と協議しなければならない。

ウ　イの規定に基づき協議した結果、無線ＬＡＮの利用を認められた場合、情報システムには以下の措置を講じなければならない。

（ア）解読が困難な暗号化方式による無線ＬＡＮ通信の暗号化及び無線ＬＡＮへのアクセス主体の認証等の技術的対策

（イ）アクセスポイント及び接続端末の適切な設定及び管理、機器の脆弱性の適切な管理等の運用による対策

(11) 機器の定期点検

情報管理責任者又は情報システム管理者は、可用性区分Ⅰ又はⅡのネットワークの機器及びサーバ等の機器について、定期保守を実施しなければならない。

(12) ソフトウェアのライセンス管理

ア　情報管理責任者又は情報システム管理者は、情報システムで利用するソフトウェアのライセンスを管理しなければならない。

イ　情報システムで利用するソフトウェアは、本市の他の情報システムに影響を与えないことを確認の上、パッチ[30]やバージョンアップなどを行い、最新の状態にする。

(13) 情報セキュリティに関する情報の収集及び共有

情報管理責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有するほか、情報セキュリティに関し、社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じる。

(14) 他団体との情報システムに関する情報等の交換

情報管理責任者は、他の団体と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、その取扱いに関する事項をあらかじめ定め、情報監理者の許可を得なければならない。

９　フィルタリングソフト等の導入

本市が管理運用する情報システムにおいて、市民等のインターネットの閲覧に供する場合には、違法・有害情報の閲覧防止対策として、フィルタリングソフト等の導入を行うこと。

10　電子メールのセキュリティ対策

情報管理責任者又は情報システム管理者は、電子メールのセキュリティ対策に関し、次の事項を実施・確認する。

（１）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しなければならない。

（２）権限のない利用者による外部から外部への電子メール転送（電子メールの不正中継（踏み台）処理）が行われないよう、電子メールサーバの設定を行わなければならない。

（３）システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員に対して、メールアドレスの付与は行わない。業務上特に必要な場合は、利用範囲等をあらかじめ定めた上で、情報管理責任者及び情報システム管理者の許可を得ること。

---

30 ソフトウェアを修正するための更新プログラムのこと。

第９章　情報システムの利用

情報セキュリティを確保するため、職員は自己の責任を十分に認識し、情報システム及びデータ等を適切に利用する。

１　情報システム及びデータ等の私的利用の禁止

職員は、本市が所有する情報システム及びデータ等（単体のパソコン等を含む。）を業務目的にのみ利用し、個人の趣味、興味本位等の私的な利用は行わない。

また、情報システム及びデータ等に対して不正な行為（不正アクセス、持ち出し、なりすまし、盗み見等）を行わない。

２　インターネット等の利用

職員は、インターネット等の利用に関し、次の事項を遵守する。

（１）電子メールの利用

ア　業務以外の目的で電子メールを利用しない。また、職員としての立場や公序良俗を十分に認識して発信する。

イ　添付ファイルのウィルスチェック及び原則無害化[31]の実施、個人情報の送信の原則禁止、許容される送信容量や添付ファイルの種類等、電子メールの安全かつ適正な運用に必要なものとして定められた事項を遵守する。

ウ　複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

エ　自動転送機能を用いて、電子メールを転送しない。

オ　重要な電子メールを誤送信した場合は、情報管理責任者に報告しなければならない。

（２）ウェブページの利用

ア　業務以外の目的でウェブページを閲覧しない。特別の業務上の必要がない限り、身元が不明なサイトへのアクセスは行わない。また、ファイルをダウンロードする場合は、ウィルスチェックを行い、コンピュータウィルスの感染を防止する。

イ　ウェブで利用できるフリーメール[32]、ネットワークストレージサービス[33]等を利用しない。ただし、情報管理責任者が業務上必要と認める場合は、情報監理者と協議するものとし、さらに機密性区分Ⅰ又はⅡの情報を取り扱う場合は「外部サービス利用ガイドライン」を遵守する。

（３）ソーシャルメディアの利用

ア　ソーシャルメディア[34]には、機密性区分Ⅰ及びⅡの情報は掲載してはならない。

---

31 ファイルを分解し、不正な動作を働くコード等が潜んでいる可能性のある部分を除去した後、ファイルを再構成して原本と同様のファイル形式に復元する処理のこと。サニタイズ処理ともいう。

32 インターネットを通じて無料で提供される e-mail サービスのこと。

33 インターネット上でファイル保管用のディスクスペースにデータを保存することができるサービスのこと。

34 インターネット上で展開される情報メディアのあり方で、個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのこと。

また、ソーシャルメディアは、不正確な情報や不用意な記述が意図しない問題を引き起こし、社会に対し多大な影響を及ぼす等ソーシャルメディアの特性や自ら関わる社会的規範などを十分理解して利用すること。

イ　本市のアカウントによる情報発信が、実際の本市のものであることを示すために、本市のＷｅｂサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

ウ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じること。

（４）業務外ネットワークへの接続の禁止

職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

（５）Ｗｅｂ会議サービスの利用時の対策

ア　職員等は、情報監理者が別途定める利用手順に従い、Ｗｅｂ会議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すること。

イ　職員等は、外部から Ｗｅｂ会議に招待され、これに参加する場合は、情報管理責任者の許可を得なければならない。また、外部の参加者を Ｗｅｂ会議に招待する場合も同様とする。

（６）外部サービスの利用

外部サービスを利用しようとする場合、別に定める外部サービス利用ガイドラインを遵守する。

３　ユーザＩＤ及びパスワードの管理

職員は、ユーザＩＤ及びパスワードの管理に関し、次の事項を遵守する。

（１）個人管理

ア　ユーザＩＤ及びパスワードは、他者に漏えいしないよう職員個々人が責任を持って管理する。また、職員間であっても貸与しない。

イ　パソコン等の端末にパスワードを記憶させない。

ウ　複数の情報システムを扱う職員は、他のシステムであっても同一のパスワードを使用しない。

エ　共用ＩＤを利用する場合は、正当な利用権限を有する利用者以外に利用させない。

（２）パスワードの変更

ア　付与された仮パスワードは、最初に利用する時点で変更する。

イ　パスワードは定期的に変更し、変更の際は、古いパスワードを再使用しない。また、パスワードは、十分な長さとし、文字列は想像しにくいものにする。

（３）パスワードの流失時の対応

パスワードが流失したおそれがある場合には、情報管理責任者に直ちに報告し、パスワードを変更しなければならない。

４　ＩＣカードの管理

（１）職員は、自己管理するＩＣカードに関し、次の事項を遵守しなければならない。

ア　認証に用いるＩＣカードは、職員間で共用してはならない。

イ　業務に必要のないときは、ＩＣカードをカードリーダ若しくはパソコン等の端末のスロット等から抜いておかなければならない。

ウ　ＩＣカードを紛失した場合は、速やかに情報管理責任者又は情報システム管理者に報告し、指示に従わなければならない。

（２）情報管理責任者又は情報システム管理者は、上記ウの報告があった場合、速やかに当該ＩＣカードを使用したアクセスを停止する。

（３）情報管理責任者又は情報システム管理者は、ＩＣカードを切り替える場合、切り替える前のカードを回収し、粉砕するなど復元できないように処置した上で廃棄しなければならない。

（４）組織で共用しているＩＣカードは、情報管理責任者が適正に管理する。

５　離席時等の措置

職員は、離席時等においては次の措置を講じる。

（１）離席時の措置

職員等は、パソコン、モバイル端末、電磁的記録媒体及び文書等について、第三者に使用されること又は情報管理責任者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

（２）不正操作の防止

ソフトウェア（業務用プログラムだけではなく市販のソフトウェアを含む。）を起動している場合は必ずこれを終了させ、また、コンピュータのロックや電源切断等を行い、第三者による不正な操作を防止する。

（３）可搬媒体等の整頓

机上に可搬媒体や文書等を放置せず、所定の保管場所に収納する。

６　ソフトウェアのインストール等

職員は、ソフトウェアのインストール等に関し、次の事項を遵守する。

（１）ソフトウェアのインストール

本市の情報システムに、本市が当該情報システムに必要なものとして認めたもの以外のソフトウェアを無断でインストールしない。なお、本市が既に認めたもの以外のソフトウェアを導入する必要が生じた場合は、情報管理責任者及び情報システム管理者の承認を得てから導入する。

（２）システム設定情報の変更禁止

情報管理責任者及び情報システム管理者の許可なく、情報システムの設定情報を変更しない。

（３）不正コピー及びライセンス違反の禁止

ソフトウェアの不正コピーやライセンス違反を行わない。

７　コンピュータウィルス対策

職員は、コンピュータウィルス対策に関し、次の事項を遵守する。

（１）ウィルスチェック及び無害化

定期的に最新のウィルス対策ソフト及びウィルスパターン定義により、パソコン等のフル

スキャンによるウィルスチェックを実施する。また、外部から入手したファイル（可搬媒体により外部から入手したファイル、インターネットを経由したダウンロードファイル等）は、ウィルスチェックを実施し、安全を確認してから使用する。

（２）ウィルス発見時の対処

コンピュータウィルスを発見した際は、パソコン等の端末にあっては直ちにＬＡＮケーブルを取り外し（無線ＬＡＮは接続を無効に設定し）、ネットワークから切断する等の措置を講じ、速やかに情報管理責任者に連絡する。

８　その他の措置

職員は、情報セキュリティを確保するため、上記以外にも次の事項を遵守する。

（１）機器の盗難防止等

パソコン、モバイル端末、外付け記憶装置等は、セキュリティワイヤーの使用、施錠可能な所定の保管場所への収納等の措置を講じ、盗難から保護する。また、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した情報を消去する。

（２）プリンター出力物の取扱い

業務上必要のないプリンター出力は行わず、出力した場合は、放置せず速やかに回収し、適切に管理する。また、重要データ等が含まれる出力物を廃棄する場合は、シュレッダーによる裁断等、判読不能な状態にしてから廃棄する。

（３）ディスプレイの向き

パソコン等の端末のディスプレイは、必要な職員以外には見られないように配置する。

（４）暗号化等機能の利用

パソコン等の端末におけるデータの暗号化等の機能を必要に応じて利用する。また、可搬媒体についても、同様に必要に応じてデータ暗号化機能を備える媒体を使用する。

（５）情報機器の持ち出し及び外部における情報処理の制限

原則として、本市の情報機器の持ち出しはしない。業務上必要な場合は、情報管理責任者又は情報システム利用責任者の許可を得る。また、外部で情報処理を行う場合、情報管理責任者又は情報システム利用責任者の許可を得た上で、適切に管理する。情報管理責任者又は情報システム利用責任者は、本市の情報機器の持ち出しについて記録を作成し、保管する。

（６）機器構成の変更の制限

パソコン等の端末やプリンター等の情報機器に対し、メモリ増設等の変更を行ってはならない。業務上必要がある場合、情報管理責任者は、情報監理者と協議しなければならない。

（７）記憶装置の適正な処分

情報システムの固定記憶装置（ハードディスク）を処分（廃棄・返却）する場合は、必ず事前に保存されているデータ等をデータ消去ソフト等により確実に消去し、判読不能な状態にする。

（８）職員等が所有するパソコン及び可搬媒体等の業務利用

原則として、職員等が所有するパソコン及び可搬媒体等は業務では利用しない。業務上必要な場合には、情報管理責任者又は情報システム利用責任者の許可を得た上で、適切に利用する。ただし、業務利用が許可された情報機器であっても、本市の情報システムへ接続してはならず、また、機密性区分Ⅰの情報資産については、処理を行ってはならない。

（９）モバイル端末等の利用

情報システム管理者又は情報管理責任者は、モバイル端末を庁外での業務に利用させる場合、遠隔消去機能を利用する等の措置を講じなければならない。その他、モバイル端末の利用規定については、情報統括監理者が別に定める。

第１０章　情報システムの調達時等における情報セキュリティ

情報システムの調達に際しては、情報セキュリティの検討及び要件の明確化を調達の手順に組み込むとともに、情報セキュリティ要件を実現するために必要な機能の実装、アクセス制御等を検討する。また、開発環境を適切に管理する。

さらに、ネットワークの接続は、ネットワーク内部における機器の接続や他のネットワークとの接続に必要な要件を定めて行う。

１　情報システムの企画及び設計

情報管理責任者は、情報システムの開発及び既存のシステムの改善に際し、企画及び設計の段階においては次の事項を実施・検討する。

（１）情報セキュリティの検討の手順化

情報セキュリティの検討をその内容に含めた開発手順書を整備し、これに従って開発・改善を行う。

（２）情報セキュリティの検討体制

情報セキュリティの検討を十分に行い、情報セキュリティ要件を明らかにする。検討に際しては、情報セキュリティ管理会議（ＣＳＩＲＴ）、運用部門、ユーザ部門等、関連を持つ部門との協議及び確認を十分に行う。

（３）情報セキュリティの検討内容

情報セキュリティの検討内容には、本章の内容に加え、次の事項を含む。

ア　管理運用に関する事項

本基準第２章、第３章及び第８章に示す事項について必要な検討を行う。

イ　物理環境セキュリティに関する事項

本基準第７章に示す事項について必要な検討を行う。

ウ　災害復旧に関する事項

本基準第１１章に示す事項について必要な検討を行う。

エ　教育・研修等に関する事項

新しい情報システムの操作・使用についての教育・研修等の検討を行う。

オ　法的準拠等に関する事項

本基準第１２章に示す事項について必要な検討を行う。

カ　その他の検討事項

（ア）適正性能の確保

情報システムの過負荷のリスクを軽減するために、将来の通信量や情報量等の伸びを予測し対処する。

（イ）暗号技術の導入

極めて重要なデータ等の保護に関しては、暗号化、デジタル署名[35]等の暗号技術の導入を検討するとともに、その暗号鍵の生成、保管等の管理に関する安全性・実用性につ

[35] デジタル文書の真正性を保証するために付けられる暗号化された署名情報。また、そのような署名を行うための技術及び一連の手順のこと。公開鍵暗号を応用したもので、文書の送信者を証明し、かつその文書が改ざんされていないことを保証する。

いても考慮する。

（ウ）入出力データの正確性の確保

情報システムに入力されるデータについて、範囲、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及び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。また、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計する。

（エ）ウェブサイトの常時ＳＳＬ／ＴＬＳ[36]化

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行う。

（オ）二重化[37]

サービスの停止が市民生活や行政運営に大きな影響を与える情報システムについては、情報システム及びデータ等及びネットワークの二重化を考慮する。

（４）情報セキュリティ機能等の評価及び調整依頼

情報管理責任者又は情報システム管理者は、本項（１）～（３）及び次項２について検討の上、「情報システムの導入等に係る事務手続要綱」に基づき、情報システム導入計画書の評価及び調整の依頼をする。また、外部サービスを利用する場合は、外部サービス利用ガイドラインを遵守する。

２　セキュリティ実現機能の実装

情報管理責任者は、情報システムの開発及び既存のシステムの改善に際し、情報セキュリティ要件を実現するために必要な機能（以下「セキュリティ実現機能」という。）を情報システムに実装するよう検討する。また、検討に際しては、庁内に共通的に提供される情報環境基盤を利用することにより、機能が効果的に実現される場合があること等も視野に入れ、有効性・合理性を考慮する。

なお、検討すべきセキュリティ実現機能とは次のようなものである。

（１）認証機能
（２）ウィルス検出機能
（３）プログラム改ざん検出機能
（４）不正アクセス監視機能
（５）改ざんデータ検出機能
（６）端末識別機能
（７）ログ取得機能

---

[36] SSL（Secure Socket Layer）、TLS（Transport Layer Security）は、インターネット等でデータを暗号化して送受信する方法のひとつで、通信途中でのデータの傍受、なりすまし又は改ざんを防ぐための手段。TLS は SSL の後継規格であり現在は SSL ではなく TLS が使用されているが、SSL という名称が広く定着しているため、ここでは SSL／TLS と併記する。

[37] システムの耐障害性を高める手法の一つで、同じ構成の機器や回線などを二系統用意すること。普段から二系統を同時に使用して、障害時には半分の能力で処理を継続する方式（コンピュータシステムの場合は「デュアルシステム」と呼ばれる）と、普段は片方のみを使用して、障害発生時に即座にもう片方に切り替えて処理を継続する方式（デュプレックスシステム）がある。

（８）バックアップ自動取得機能
（９）なりすまし防止機能

３　セキュリティ実現機能の定期的な確認

情報管理責任者は、情報システムのセキュリティ実現機能が有効に機能していることを定期的に確認する。

４　情報システムの調達

情報管理責任者は、情報システムの調達に際し、次の事項を実施・確認する。

（１）調達仕様書の確認

調達仕様書が情報セキュリティ要件を満たしていることを確認する。また、これらの事項の確認には、必要に応じて情報管理部門の支援を得る。

（２）開発ドキュメント[38]の納品

開発されたソフトウェアの納品に当たっては、開発ドキュメント等についても成果品として納品の対象とする。

（３）製品の選定要件

ハードウェア及びソフトウェアを選定する際は、当該製品が情報セキュリティ上の問題を生じさせないよう、情報セキュリティ要件を満たしていること、サポート体制が充実していること、信頼性の高い技術を採用していること、信頼できる製造元であること等を考慮する。

また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

これらの事項の確認には、必要に応じて情報管理部門の支援を得る。

５　不要サービスの機能停止

（１）不要ソフト及びサービスの実装禁止

情報管理責任者は、情報システムの動作に必要のないソフトウェアやサービスを実装しない。

（２）不要ソフト及びサービスの機能停止

情報管理責任者は、不要なソフトウェアやサービスがオペレーティングシステム[39]等にあらかじめ実装されている場合は、その機能を停止させるための措置を講じる。

６　ソースコード[40]による納品

情報管理責任者は、ソフトウェアの開発においては、コードの確認が行えるようソースコー

---

38 一般的にシステム開発時に作成される書類全般を意味する。

39 ソフトウェアの種類の一つで、機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェアのこと。OS（Operating System）の和訳。OS の機能を利用し、OS の上で動作するソフトウェアをアプリケーションソフト（application software、応用ソフト）という。

40 人間が読み取り可能なコンピュータ言語を用いて記述された、一連のコンピュータ命令のこと。ソースコードを実行可能な形式に変換する等することにより、コンピュータ上で動くプログラムとなる。

ドの提出を求める。

7　アクセス制御

（1）情報管理責任者は、職員及び外部利用者が利用を認められた範囲内で情報及びサービスの利用ができるようにアクセス制御を行う。

（2）情報管理責任者は、外部の者が利用できるシステムについて、必要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る。

8　ネットワーク接続要件

情報管理責任者は、ネットワーク接続に関し、必要な要件及び手続を定めるとともに、アクセスを適切に制御するための措置を講じる。また、必要に応じて情報管理部門の支援を得る。

（1）ネットワーク構成

ア　区分された構成及び接続要件の明確化

本市のネットワークは、機密度に応じて論理的又は物理的に区分する。このため、区分されたネットワーク間の接続にはゲートウェイ[41]の設置等を行い、ネットワーク全体の安全性を確保する。また、ネットワーク内部における機器の接続又は他のネットワークとの接続に必要な要件及び手続を定め、これに基づいて接続する。

イ　ネットワーク間の制御技術[42]の導入における留意事項

ネットワーク間の制御技術の導入においては、データ通過パフォーマンス等の性能を考慮する。

（2）外部ネットワークとの接続

ア　原則として、個々の情報システムは外部ネットワーク（インターネットや外部機関のネットワーク）と直接接続しない。

イ　情報管理責任者は、所管する情報システムを外部ネットワークと接続しようとする場合は、情報監理者と協議しなければならない（ただし、川崎市行政基盤ネットワーク運営規約により外部ネットワークと接続する場合は除く。）。情報監理者は、協議内容について、本市の接続設備の機器構成及び相手先のネットワーク構成、機器構成、セキュリティレベル等を評価し、本市の情報システムに影響を与えないことを確認する。

ウ　情報システム管理者は、川崎市行政基盤ネットワーク運営規約により承諾を与えた場合は、情報監理者に報告すること。

エ　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、情報管理責任者又は情報システム利用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する。なお、明らかに情報資産に脅威が発生している場合には、直ちに当該外部ネットワークを物理的に遮断し、速やかに情報セキュリティ責任者へ報告する。

（3）通信事業者の通信回線

サーバとクライアント端末の接続等、本市の情報システムで通信事業者の通信回線を利用

---

41 ネットワーク間等の通信を中継する機器や、それを実現するソフトウェアのこと。

42 ネットワークを流れるデータの流れの方向や通過量を制御する技術で、ルータ、ハブ（スイッチングハブ）による流れの方向制御、ゲートウェイ（主としてファイアウォール）によるフィルタリングや監視ソフトによる通過情報の監視等を指す。

する場合は、取り扱う情報の機密性、完全性及び可用性に応じて利用する回線の種別を選択する。

（４）ネットワークサービスの利用

インターネット環境を利用して他組織の保有するサーバにアクセスし処理を行うネットワークサービスの利用に際しては、相手先のネットワーク構成、機器構成及びセキュリティレベル等を評価し、本市の情報及び情報システムに影響を与えないことを確認する。

９　複合機等のセキュリティ対策

（１）情報管理責任者は、複合機を調達する場合、当該複合機が備える機能、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、データの暗号化やＩＣカード等による認証など適切なセキュリティ要件を策定する。

（２）情報管理責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティ事故等への対策を講じる。

（３）情報管理責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録の全てを抹消又は再利用できないようにする対策を講じる。

（４）情報管理責任者は、ＩＰ電話システム[43]、ネットワークカメラシステムその他特定の用途に使用される機器について、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する。

10　開発環境

情報管理責任者は、情報システムの開発環境を本番環境から分離するとともに、資源を適切に管理する。

（１）開発環境と本番環境との分離

現在運用中（本番環境）のデータやソフトウェアの安全を確保するため、情報システムの開発環境は、テスト段階も含めて本番環境から分離する。

（２）システム開発における責任者、作業者のＩＤの管理

ア　情報管理責任者又は情報システム管理者は、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、開発用ＩＤを削除しなければならない。

イ　情報管理責任者又は情報システム管理者は、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しなければならならない。

（３）開発テスト

ア　情報管理責任者又は情報システム管理者は、新たに情報システムを導入する場合、既に稼動している情報システムに接続する前に十分なテストを行わなければならない。

イ　情報管理責任者又は情報システム管理者は、運用テストを行う場合、あらかじめ疑似環境による操作確認を行わなければならない。

ウ　情報管理責任者又は情報システム管理者は、テスト結果を一定期間保管しなければならない。

---

[43] 電話回線ではなく、インターネット回線等のネットワークを利用して提供される電話サービスのこと。

エ　原則として、本番環境で使用しているデータをテストデータに使用してはならない。使用する場合は、個人が特定できるデータについて、マスキング[44]などを施す。

オ　開発したシステムの受入れテストを行う場合、開発した組織と利用する組織が連携してテストを行う。

（４）本番環境への移行

ア　情報管理責任者又は情報システム管理者は、システム開発、保守及びテスト環境からシステム運用環境への移行について、システム開発、保守計画の策定時に手順を明確にしなければならない。

イ　情報管理責任者又は情報システム管理者は、移行の際、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しなければならない。

ウ　情報管理責任者又は情報システム管理者は、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。

（５）開発用資源の管理

ア　改ざん等からの保護

開発段階において使用されるデータ等の資源を、悪用、改ざん等から保護するための措置を講じる。

イ　テストデータ等の管理

原則として、本番環境のデータを開発テストには利用しない。ただし、情報管理責任者が必要を認めた場合はコピーファイルを使用し、本番環境データと同等の情報セキュリティ管理策を講じる。この場合、個人情報等の部分については可能な限り消去することとし、テスト終了後はデータを確実に消去・破棄し、情報管理責任者に報告する。

ウ　本番環境への移行時の措置

開発環境から本番環境への移行に際しては、開発環境で使用したライブラリのバックアップ、ユーザＩＤ及びパスワードの抹消等を行う。

11　システム保守

システム又はネットワークの保守、重要な機器の設定変更、システム変更及び変更したプログラムの本番への移行に当たっては、本章の定めに従うほか、次に掲げる内容について留意する。

（１）変更したプログラムによる既存システムへの影響範囲の明確化

変更したプログラムを組み込むことによる影響範囲を、企画時及び設計時に調査分析し、変更したプログラムの本番移行による障害発生を予防する。

（２）本番環境と同一環境によるテスト

本番環境と同一レベルのソフトウェア、ハードウェア及びデータの環境において、変更したプログラムの移行テスト及び稼動確認を実施する。

（３）移行計画の作成と移行作業中の障害発生時における緊急対策手順の整備

本番移行スケジュール及び移行手順を含む移行計画を作成する。また、あらかじめ移行テストを行い、移行計画が有効に機能することを確認する。

---

44 文字列等について、伏字にする等により元の情報を判別・利用できないようにすること。

移行計画実施中の不測の事態等による情報システムの停止やデータの破損に備え、緊急対策手順を用意する。

（４）保守作業

ア　保守、システム変更等の作業を開始する前に、提案の詳細について情報管理責任者又は情報システム管理者の承認を得ること。

イ　保守、システム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認すること。

ウ　情報管理責任者又は情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成する。

12　システムドキュメントの管理

（１）情報管理責任者は、システム設計書、コード体系表、プログラム仕様書、ソースコード等のシステムドキュメントを整備し、あらかじめ定められた場所に適切な方法で保管する。

（２）保管されるシステムドキュメントの閲覧、貸与、ドキュメントの加筆及び修正等を行う場合は、情報管理責任者の承認を得なければならない。この場合、情報管理責任者は、記録の作成などによりシステムドキュメントのアクセス管理を行う。

（３）障害発生時の対策実施手順を定めること。

第１１章　情報システムの災害復旧

災害等による情報システムの機能の停止等が市民生活や行政運営に及ぼす影響を評価し、これに応じた対応・復旧の手順を定め、迅速かつ効果的に対応できるよう対策を講じる。また、手順の検証及び見直しを行い、実効性を維持する。

１　手順の策定及び改訂

情報管理責任者は、業務継続計画との整合性を図りつつ、所管する情報システムについて、災害等による大規模な障害及び事故に対し、迅速かつ効果的に対応・復旧を行うため、災害復旧手順書を整備するとともに、その改訂及び実効性の検証を行う。

（１）災害復旧手順書の整備

災害復旧手順書に記述する事項には次のものを含む。

ア　体制

状況判断及び指示を行う者、対応に関与すべき者等

イ　代替運用

業務の代替運用の方法等

ウ　対応と連絡

取るべき措置、連絡先等

エ　テスト

情報システムの正常復帰を確認するためのテストの内容及び手順

オ　再開の手続

正常業務に復帰するための措置、手順等

カ　教育

災害復旧手順書を理解し、実行するために必要な教育の内容等

（２）手順の改訂

定期的又は情報システムの更新時に、リスクの把握･分析を行い、災害復旧手順書を見直し、必要に応じて改訂を行う。

（３）アウトソーシングにおける代替運用対策

アウトソーシングサービスにおける代替運用対策は、原則として、契約に定める範囲で、アウトソーシング先の責任範囲とする。

（４）手順の検証

災害復旧手順書の策定時及び改訂時には、手順に基づくテスト及び訓練を実施し、実効性を検証する。

２　影響等の調査

情報管理責任者は、障害や事故が発生した場合、情報セキュリティ管理会議（ＣＳＩＲＴ）と連携し、速やかに内容、原因、被害、影響範囲等を調査・把握するとともに、情報セキュリティ責任者及び情報統括監理者（ＣＩＳＯ）に報告する。

３　再発防止の措置

情報管理責任者は、情報システム管理者及び情報セキュリティ管理会議（ＣＳＩＲＴ）と連携し、発生した障害や事故に関する分析を行って再発防止の措置を講じるとともに、必要に応じて災害復旧手順書の改訂を行う。また、情報統括監理者（ＣＩＳＯ）は、規程及び本基準の改善につながる案がある場合は、必要な措置を指示する。

第１２章　法的準拠等

情報及び情報システムの管理運用及び利用に際しては、関連する法律、条例等を遵守する。また、情報セキュリティ対策が正しく運用されていることを点検する。

１　法律等の遵守

職員は、情報及び情報システムの管理運用及び利用に際し、関連する法律、条例等を遵守する。

（１）遵守すべき法律等

遵守すべき法律等には次のようなものがある。

ア　地方公務員法（昭和 25 年法律第 261 号）
イ　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）
ウ　著作権法（昭和 45 年法律第 48 号）
エ　電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）
オ　個人情報の保護に関する法律（平成 15 年法律第 57 号）
カ　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）
キ　サイバーセキュリティ基本法（平成 26 年法律第 104 号）
ク　その他業務の遂行に関連する法律等

（２）遵守すべき条例等

遵守すべき条例等には次のようなものがある。

ア　川崎市情報公開条例（平成 13 年川崎市条例第 1 号）
イ　川崎市個人情報の保護に関する法律施行条例（令和 4 年川崎市条例第 76 号）
ウ　川崎市職員の保有個人情報の取扱い等に関する規則（平成 17 年川崎市規則第 72 号）
エ　川崎市公文書管理規則（平成 13 年川崎市規則第 20 号）
オ　川崎市公文書管理規程（昭和 36 年川崎市訓令第 2 号）
カ　川崎市情報化施策の推進に関する規則(平成１９年川崎市規則第１２号)
キ　川崎市情報セキュリティ基本方針に関する規程(平成１９年川崎市訓令第１号)
ク　その他業務の遂行に関連する条例、規則、規程等
ケ　本市の情報システム及びネットワークと接続する外部ネットワーク等において定められたセキュリティに関する規定

（３）知的所有権

知的所有権に関わる物件及びソフトウェア製品の使用については、法的制限事項を確認し、遵守する。

２　本基準等への準拠

（１）情報管理責任者は、定期的に、所管する情報システムが技術面や運用手順面で本基準等に準拠していることを確認する。

（２）情報管理責任者又は情報システム管理者は、情報セキュリティ関係規程を遵守することが困難な状況で、行政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は、情報監理者との協議を

経て、情報統括監理者の承認を得れば、例外措置を取ることができる。

３　違反時の対応

本基準に違反した職員等は、その重大性、発生した事案の状況等に応じて、懲戒処分等の対象とする。

４　自己点検の実施

（１）情報資産の自己点検

情報管理責任者及び情報システム管理者は、毎年度及び必要に応じて、情報資産の管理について、自己点検を行う。

（２）職員の自己点検

職員は、本基準等の遵守状況について、毎年度自己点検を行う。

５　局点検

情報セキュリティ責任者は、規程第６条第３項に基づき、情報セキュリティ対策の実施状況を確認するために、情報管理責任者及び職員が行った自己点検の実施状況を確認する。必要に応じ、情報管理責任者に改善の実施に関し指示するとともに、点検結果について情報監理者へ報告する。

６　情報セキュリティ監査の実施

情報統括監理者は、規程第７条の規定に基づき、情報セキュリティ対策を行う部署が規程及び本基準等により、情報セキュリティ対策を適正に運用しているかを検証するため、情報セキュリティ監査を実施する。

なお、情報セキュリティ監査を行うために必要な事項については、情報統括監理者が別に定める。

７　情報セキュリティ内部検査の実施

情報統括監理者は、規程第７条の規定に基づく情報セキュリティ監査を補完するため、情報セキュリティ対策を行う部署の情報セキュリティ対策の実施状況を確認する情報セキュリティ内部検査を実施する。

なお、情報セキュリティ内部検査を行うために必要な事項については、情報統括監理者が別に定める。

８　改善計画の策定

情報管理責任者及び情報システム利用責任者は、自己点検、局点検、情報セキュリティ監査又は情報セキュリティ内部検査により改善の必要性が確認された場合は、速やかに改善計画を策定し、情報セキュリティ責任者の承認を得て改善を行う。

９　本基準の見直し

情報統括監理者は、本基準について情報セキュリティ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、必要があると認めた場合、その見直しを行う。

10　情報セキュリティ実施手順の取扱い

規程第６条第２項の規定に基づく情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから原則非公開とする。

11　優先事項

市民の生命や財産を最優先に考え、災害発生時等緊急の必要性がある場合には、他の措置を情報セキュリティに関する措置に優先して扱うことができるものとする。

川崎市情報セキュリティ基準

（第１３版）

令和６年４月

川崎市　総務企画局　デジタル化施策推進室