豊中市
情報セキュリティ対策基準

令和 8 年（2026 年）4 月 1 日

【目次】

第１章　総則

第１節　目的

（目的）

第１条　この基準は、豊中市情報セキュリティ規則（平成 28 年豊中市規則第 83 号。以下「規則」という。）第 12 条に基づき、情報セキュリティ対策を実施するための具体的な遵守事項及び判断基準等を定めることを目的とする。

第２節　用語の定義

（用語の定義）

第２条　この基準に用いる用語の定義は規則に定めるもののほか、次に掲げるとおりとする。

（１）情報セキュリティポリシー　規則及びこの基準のことをいう。

（２）情報セキュリティインシデント　情報セキュリティに関する障害・事故及びシステム上の欠陥のことをいう。

（３）住基ネット　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）に規定する住民基本台帳ネットワークシステムのことをいう。

（４）LGWAN　ミレニアム・プロジェクトについて（平成 11 年 12 月 19 日内閣総理大臣決定）に規定する総合行政ネットワークのことをいう。

（５）業務端末　職員が情報処理を行うために直接操作するサーバ以外の電子計算機のことをいう。

（６）特定個人情報　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 9 項に規定する特定個人情報をいう。

（７）マイナンバー利用事務系　番号法第 2 条第 11 項に規定する個人番号利用事務及び戸籍等の重要な個人情報を扱う情報システムのうち、都市経営部デジタル戦略課長が所管する住民情報を扱う情報システムの通信を専用的に行うためのネットワークに接続された情報システムのことをいう。

（８）LGWAN 接続系　LGWAN に接続された情報システム（マイナンバー利用事務系を除く。）のうち、都市経営部デジタル戦略課長が所管する行政情報を扱う情報システムの通信を専用的に行うためのネットワークに接続された情報システムのことをいう。

（９）インターネット接続系　電子メール、ホームページの管理等に関わるインターネットに接続された情報システムのうち、都市経営部デジタル戦略課長が所管する行政情報を扱う情報

システムの通信を専用的に行うためのネットワークと相互の通信を行う情報システムのことをいう。

(10) MAC アドレス　通信回線に接続された機器や接続口を一意に識別するために物理的に割り当てられた識別番号のことをいう。

(11) IP アドレス　通信回線に接続された電子計算機及び通信機器を識別するために割り振られる識別番号のことをいう。

(12) ポート番号　電子計算機及び通信機器が通信に使用するプログラムを識別するための番号のことをいう。

(13) マルウェア　コンピュータウイルスその他不正プログラムのことをいう。

(14) 複合機　複写機（コピー）、印刷機（プリンター）、画像入力装置（スキャナー）、ファクシミリ等の機能が一つにまとめられている機器のことをいう。

(15) 電子計算機室　ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋のことをいう。

(16) 特定用途機器　特定の用途に使用されるシステム特有の構成機器のうち、通信回線に接続されている又は記録媒体を内蔵しているものをいう。

(17) 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をいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

(18) クラウドサービス　外部サービスのうち、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

(19) ガバメントクラウド　デジタル社会形成基本法（令和 3 年法律第 35 号）第 29 条に規定する、全ての地方公共団体が官民データ活用推進基本法（平成 28 年法律第 103 号）第 2 条第 4 項に規定するクラウド・コンピューティング・サービス関連技術に係るサービスを利用することができるようにするための国による環境の整備として、デジタル庁が整備するものをいう。

(20) 標準準拠システム　地方公共団体情報システムの標準化に関する法律（令和 3 年法律第 40 号）第 6 条第 1 項及び第 7 条第 1 項に規定する標準化基準に適合する基幹業務システムをいう。

第３節　組織体制

（情報セキュリティ統括責任者）

第３条　情報セキュリティ統括責任者は、以下の情報セキュリティ対策の実施のために必要な措置を行う。

（１）部等情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報シス

テム担当者に対する情報セキュリティに関する指導及び助言

（２）本市の情報資産に対する情報セキュリティインシデントが発生した場合又は情報セキュリティインシデントのおそれがある場合の必要かつ十分な措置

（３）緊急時等の円滑な情報共有を図るための緊急連絡網の整備

（４）複数の事業者が存在する場合の責任の所在確認、必要な連絡体制の構築及びクラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制の確立（標準準拠システム・関連システム等の業務システム（以下「標準準拠システム等」という。）をガバメントクラウドにおいて利用する場合に限る。）

（部等情報セキュリティ責任者）

第４条　部等情報セキュリティ責任者は、豊中市事務分掌規則（昭和 37 年豊中市規則第 7 号）第 1 条第 1 項、豊中市消防局組織規則（昭和 41 年豊中市規則第 14 号）第 2 条第 1 項、豊中市上下水道局事務分掌規程（平成 20 年豊中市企業管理規程第 1 号）第 2 条第 1 項及び豊中市議会事務局条例（昭和 27 年豊中市条例第 25 号）第 4 条に規定する課（これらに相当する事務組織を含む。以下同じ。）を所管する部の長又は部に属さない課の所属員を指揮監督する者並びに行政委員会事務局の長をもって充て、所管する部等に係る情報セキュリティ対策の実施を統括管理する。

２　部等情報セキュリティ責任者は、緊急時等における連絡体制の整備並びに情報セキュリティポリシーの遵守に関する教育、訓練、助言及び指示その他部等における情報セキュリティの確保のために必要な措置を行う。

（情報セキュリティ管理者）

第５条　情報セキュリティ管理者は、前条に規定する課の長をもって充て、部等情報セキュリティ責任者の下、その所管に係る情報セキュリティ対策を実施する。

（情報システム管理者）

第６条　情報システム管理者は、情報システムを所管する課等の長をもって充て、部等情報セキュリティ責任者の指示の下、所管する情報システムの管理を行う。

（情報システム担当者）

第７条　情報システム管理者は、自身が管理する情報システムの開発、設定の変更、運用、更新等の作業及び管理を担当する職員を情報システム担当者として指名する。

第４節　セキュリティ会議

（セキュリティ会議の構成）

第８条　規則第４条第３項に規定するセキュリティ会議は、次に掲げる者をもって構成する。

（１）情報セキュリティ統括責任者
（２）総務部長
（３）財務部長
（４）市民協働部長
（５）福祉部長
（６）健康医療部長
（７）こども未来部長
（８）上下水道局経営部長
（９）消防局長
(10) 教育委員会事務局長
(11) 市議会事務局長
(12) デジタル戦略課を担当する都市経営部次長
(13) 都市経営部デジタル戦略課長
(14) 情報セキュリティ統括責任者が指名する部等情報セキュリティ責任者（第２号から第11号の者を除く。）、理事、情報システム管理者及び情報セキュリティ管理者

２　情報セキュリティ統括責任者は、必要があると認めるときは、セキュリティ会議に自らが指名する者を加えることができる。

（セキュリティ会議の所掌事項）

第９条　セキュリティ会議は、次に掲げる事項について調査審議する。

（１）規則及びこの基準の見直しに関すること。
（２）情報セキュリティ対策についての教育・研修の計画及び有効性に関すること。
（３）情報セキュリティ監査（情報セキュリティに関する監査をいう。以下同じ。）の計画及び実施結果に関すること。
（４）情報セキュリティに関する自己点検の計画及び実施結果に関すること。
（５）情報セキュリティインシデントの発生時における対応及び対策について、情報セキュリティ統括責任者が必要と認めたもの。
（６）住基ネット及びLGWANの情報セキュリティ対策の決定及び見直しに関すること。
（７）その他情報セキュリティ統括責任者が必要と認める事項。

（セキュリティ会議の開催）

第10条　セキュリティ会議の議長は、情報セキュリティ統括責任者をもって充て、セキュリティ会議を招集し、職務を総理する。

2　議長に事故があるときは、デジタル戦略課を担当する都市経営部次長がその職務を代理する。

3　議長は、必要があると認めるときは、関係者の出席を求め、その意見を聴くことができる。

4　議長は、セキュリティ会議における審議結果について、情報セキュリティ管理者に通知する。

（セキュリティ会議の庶務）

第11条　セキュリティ会議の庶務は、都市経営部デジタル戦略課において処理する。

（兼職の禁止）

第12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、許可の申請を行う者とその許可者は、同じ者が兼務してはならない。

第５節　CSIRT（シーサート）

（CSIRTの設置及び役割）

第13条　情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを目的としたCSIRT（Computer Security Incident Response Team）は、都市経営部デジタル戦略課長を責任者とし、都市経営部デジタル戦略課に所属する職員をもって充てる。

2　CSIRTは、次に掲げる事項を実施する。

（１）情報セキュリティの統一的な窓口として、市の部局及び市民等外部の関係者から情報セキュリティインシデントについて報告を受けること。

（２）認知した情報セキュリティインシデントについて、状況を確認し、必要に応じて情報セキュリティ統括責任者に報告すること。

（３）認知した情報セキュリティインシデントについて、必要に応じて総務省、大阪府、個人情報保護委員会、その他関係機関へ報告すること。

（４）認知した情報セキュリティインシデントについて、その重要度や影響範囲等を勘案し、広報を担当する課等と協力して、報道機関への通知・公表に対応すること。

（５）情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等と情報を共有すること。

第２章　情報資産の管理

（重要情報資産）

第 14 条　この基準において、次に掲げる判定のいずれかに該当する情報資産を重要情報資産とする。

（１）機密性に基づく判定　個人情報及び法令等の定めにより守秘義務が課されている情報（以下「重要情報」という。）、情報システムに係るパスワード又はシステム設定情報

（２）完全性に基づく判定　改ざん、誤謬、破損等が生じた場合に、市民の権利が侵害される又は業務執行に支障を及ぼすおそれがある情報資産

（３）可用性に基づく判定　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、市民の権利が侵害される又は安定的な業務執行に支障を及ぼすおそれがある情報資産

（情報資産の管理責任）

第 15 条　情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（情報資産管理台帳の作成）

第 16 条　情報セキュリティ管理者は、その所管する情報資産の保管場所や管理状況等について情報資産管理台帳に記載し、情報資産の追加、移設、廃止等が発生した場合は、情報資産管理台帳を更新しなければならない。

２　情報セキュリティ管理者は、毎年度１回以上、所管する情報資産と情報資産管理台帳の内容の整合性を確認しなければならない。

３　情報セキュリティ管理者は、情報資産管理台帳の作成にあたっては、都市経営部デジタル戦略課長が整備した様式を使用するものとする。

（情報システム台帳の作成）

第 17 条　情報システム管理者は、所管する情報システムに対して、システム台帳を整備しなければならない。

（複製された情報資産の管理）

第 18 条　情報セキュリティ管理者は、複製又は伝送された情報資産についても、元の情報の重要性に応じて適切に管理しなければならない。

（クラウドサービスにおける情報資産の管理）

第 19 条　標準準拠システム等をガバメントクラウドにおいて利用する場合、情報セキュリティ管理者はクラウドサービスにおける情報資産の管理について、次に掲げる措置を講じなければならない。

（１）クラウドサービスの環境に保存される情報資産の、元の情報の重要性に応じた適切な管理

（２）情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）ごとの取扱いの規定

（３）クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前の文書での提示要求又は公開されている内容の確認

（管理番号等の明示）

第 20 条　情報セキュリティ管理者は、職員による情報資産の不用意な取扱いの防止及び情報資産の紛失等を速やかに発見するため、電子計算機、電磁的記録媒体及び周辺装置又は書面を綴じたファイル等に、管理所属、タイトル、管理番号等を必要に応じて明示し、適切に管理しなければならない。

（作成途上の情報）

第 21 条　情報セキュリティ管理者は、職員が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、当該情報を消去させなければならない。

（電磁的記録媒体の管理）

第 22 条　情報セキュリティ管理者は、重要情報を記録した電磁的記録媒体について、誤って情報を消去することがないように、必要に応じて書込禁止の措置を講じなければならない。

２　情報システム管理者は、災害等により情報システムに使用しているデータが滅失又は破損した場合の復旧に備えるため、必要に応じて情報システムのバックアップで取得したデータが記録された電磁的記録媒体を遠隔地に保管するものとする。

３　情報セキュリティ管理者は、電磁的記録媒体を施錠可能な場所に保管しなければならない。

４　情報セキュリティ管理者は、電磁的記録媒体に記録された情報について、不要になった時点で速やかに消去しなければならない。

（情報資産の搬送）

第 23 条　情報セキュリティ管理者は、重要情報資産を搬送または伝送する場合は、次に掲げる事項を遵守しなければならない。

（１）電磁的記録媒体及び書面については、鍵付き鞄又は容器を利用したりパスワード等による暗号化を行ったりする等、不正利用を防止するための措置を講じること。ただし、大量の印刷物の搬送等、対策が困難な場合を除く。
（２）管理簿により受渡を確認すること。
（３）受け取りの際の数量を確認すること。

（情報資産の持ち出し）

第 24 条　情報セキュリティ管理者は、所管する業務端末、電磁的記録媒体、重要情報が含まれる書面等を外部に持ち出す必要がある場合は、次に掲げる事項を確認した上で許可しなければならない。
（１）対象
（２）目的及び理由
（３）期間
（４）職員名

２　情報セキュリティ管理者は、前項の規定に基づき持ち出しを認める場合は、業務端末、電磁的記録媒体等のパスワード設定、データ又はハードディスクの暗号化を行う等の情報漏えい対策を実施しなければならない。

３　情報セキュリティ管理者は、第１項の規定に基づき持ち出しを認める場合は、持ち出し記録を作成するものとする。

４　情報セキュリティ管理者は、持ち出した業務端末又は電磁的記録媒体を紛失した場合に、記録されている情報を特定できるようにするため、可能な限り、持ち出し時において必要最小限の情報のみを記録し、返却時においては情報の完全削除を行うなどの運用を実施するものとする。

（情報資産の提供・公開）

第 25 条　情報セキュリティ管理者は、重要情報を職員以外の者に提供する場合は、必要に応じてパスワード等による暗号化を行わなければならない。

２　職員は、職員以外の者に重要情報資産を提供する場合は、情報セキュリティ管理者の許可を得なければならない。

３　情報セキュリティ管理者は、市民に対し、ホームページ等で公開するデータについて、誤った情報の公開が起こらないよう慎重に取り扱わなければならない。

４　ホームページ等のシステムを所管する情報システム管理者は、ホームページ等で公開されるデータの改ざん等が起こらないよう対策を講じなければならない。

（書面の廃棄）

第 26 条　情報セキュリティ管理者は、重要情報が含まれる書面を廃棄する場合は、裁断機による裁

断、焼却又は溶解を行わなければならない。

（電磁的記録媒体の廃棄）

第 27 条　情報セキュリティ管理者は、電磁的記録媒体の廃棄を行う場合は、次に掲げる措置を講じなければならない。

（１）特定個人情報が記録されたことがある場合は、物理的破壊又は除去（専用コマンドの使用、復号鍵の消去又は磁気的消去による記憶領域の抹消のことをいう。以下同じ。）の実施

（２）前号以外については、物理的破壊、除去又は専用ソフトウェアによるデータ消去の実施

２　職員は、電磁的記録媒体を廃棄する場合は、情報セキュリティ管理者の許可を得なければならない。

３　情報セキュリティ管理者は、クラウドサービスで利用する全ての重要情報について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

第３章　情報システムの重要性に基づくネットワーク分離等の対策

第１節　マイナンバー利用事務系の対策

（マイナンバー利用事務系と他の領域との分離）

第 28 条　都市経営部デジタル戦略課長は、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。

２　都市経営部デジタル戦略課長は、マイナンバー利用事務系と外部との通信を行う必要がある場合は、通信経路（MAC アドレス又は IP アドレス）及びポート番号の限定を行わなければならない。

３　都市経営部デジタル戦略課長は、前項の規定により外部との通信を行う場合は、インターネット等と接続されている外部接続先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、この限りでない。

４　都市経営部デジタル戦略課長は、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。

（業務端末における対策）

第 29 条　都市経営部デジタル戦略課長は、マイナンバー利用事務系に使用される業務端末へのログインに際しては、知識（パスワード等）、所持（ID カード等）、存在（生体認証等）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。

2　都市経営部デジタル戦略課長は、マイナンバー利用事務系の業務端末について、原則として電磁的記録媒体による情報の持ち出しができないように設定しなければならない。

（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）

第 30 条　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、十分な強度を持つ暗号による対策を実施するよう努めなければならない。

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、必要な措置を講じなければならない。

第２節　LGWAN 接続系の対策

（インターネット接続系との分離）

第 31 条　都市経営部デジタル戦略課長は、LGWAN 接続系の通信環境をインターネット接続系と分離した上で、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。

2　都市経営部デジタル戦略課長は、データをインターネット接続系から LGWAN 接続系に取り込む場合は、次に掲げる方法のいずれかにより、無害化通信（マルウェア等を排除するための措置を行い、安全を確保した通信のことをいう。）を図らなければならない。

（１）インターネット環境で受信した電子メールの本文のみを LGWAN 接続系に転送する方式

（２）インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

（３）ファイルから危険因子を除去し、又は危険因子がファイルに含まれていないことを確認した上で、インターネット接続系から取り込む方式

（ガバメントクラウドにおける LGWAN 接続系の取扱い）

第 32 条　都市経営部デジタル戦略課長は LGWAN 接続系の情報システムをガバメントクラウド上に配置する場合は、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。

第３節　インターネット接続系の対策

（インターネット接続系の対策）

第 33 条　都市経営部デジタル戦略課長は、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速やかな対処が可能となるように、通信データの監視、不正通信の監視等の対策を講じなければならない。

2　都市経営部デジタル戦略課長は、インターネット接続系における通信の安全性を適切かつ効率的に確保するため、大阪府が管理運営する自治体情報セキュリティクラウド（大阪府下の市町村におけるインターネットとの通信を集約し、集中監視と分析を行う監視機能等を有する仕組みのことをいう。）に参加するものとする。ただし、独自の対策により自治体情報セキュリティクラウドと同等の安全性が確保できると認められる場合は、この限りでない。

（インターネット接続系での重要情報の利用）

第 34 条　情報システム管理者は、業務の効率性・利便性の向上を目的として、重要情報を扱う情報システムの業務端末をインターネット接続系に置こうとする場合は、データの保存場所、通信方法、必要なセキュリティ対策等について、情報セキュリティ統括責任者の許可を得なければならない。

2　前項の申し出を受けた情報セキュリティ統括責任者は、セキュリティ会議を招集し、内容について審議するものとする。

第４章　物理的セキュリティ対策

第１節　サーバの管理

（サーバの設置）

第 35 条　情報システム管理者は、所管する情報システムに関してサーバを設置しようとする場合は、次に掲げる対策を講じなければならない。

（１）設置場所における火災、水、埃及び振動等の影響を可能な限り排除すること。

（２）盗難及び転倒を防止するため、設置場所を施錠し、床に固定、又は鎖で固定すること。

2　情報システム管理者は、市の施設以外の場所にサーバを設置してはならない。特段の理由により市の施設以外にサーバを設置しようとする場合は、デジタル戦略課長と協議の上、情報セキュリティ統括責任者の承認を得なければならない。

（サーバの冗長化）

第 36 条　高い業務継続性（可用性）を求められる情報システムを所管する情報システム管理者は、障害発生時におけるデータの滅失及び情報システムの運用停止を回避するため、サーバの冗長化を行うことを検討しなければならない。

（サーバの電源）

第 37 条　情報システム管理者は、所管する情報システムのサーバの電源を適正に管理するため、次に掲げる措置を講じなければならない。

（１）電力供給の停止後、電子計算機が業務を終了するまでの間に適正に動作するための必要な予備電源を備えること。

（２）落雷による過電流からサーバを保護するためのアースを設置すること又はこれと同等の措置を講じること。

（３）電源プラグがコンセントから容易に抜けないよう措置すること。

第２節　配線等の管理

（配線の対策）

第 38 条　情報システム管理者は、所管する情報システムに関する配線について、損傷等を防止するため、床下への配線、保護カバーの取付等の措置を講じなければならない。

２　情報システム管理者は、前項の措置を実施する場合又は所管する情報システムに関する配線に損傷等が発生した場合は、必要に応じて施設管理部署と連携して対応するものとする。

（通信回線の接続口の管理）

第 39 条　情報システム管理者は、通信回線の接続口について、接続を許可した端末以外の機器等が接続されないように必要な措置を講じるよう努めなければならない。

(機器の保守)

第 40 条　情報システム管理者は、重要情報を扱うサーバ等の機器について、保守を実施しなければならない。

第３節　電子計算機等の修理、返却及び廃棄

（電子計算機等の修理）

第 41 条　情報セキュリティ管理者は、委託事業者による電子計算機、複合機等の修理が行われる場合、職員を立ち会わせなければならない。

２　情報セキュリティ管理者は、前項の規定による職員の立ち会いが困難な場合は、修理する電子計算機、複合機等のすべてのデータを消去の上、復元不可能な状態にする措置を講じなければならない。

（電子計算機等の返却・廃棄）

第 42 条　情報セキュリティ管理者は、リース契約等が終了した又は不要になったサーバ及び業務端末については、内蔵された電磁的記録媒体に対して次に掲げる措置を講じなければならない。

（１）特定個人情報が含まれる情報処理に利用されたことがある場合は、物　理的破壊又は除去の実施

（２）前号以外については、物理的破壊、除去又は専用ソフトウェアによるデータ消去の実施

２　情報セキュリティ管理者は、複合機等を返却又は廃棄する場合は、すべてのデータを消去の上、復元不可能な状態にする措置を講じなければならない。

３　情報セキュリティ管理者は、第１項の規定に基づく電子計算機の破壊、除去又はデータ消去について、内部で実施する場合は職員を立ち会わせなければならない。また、作業完了後は職員が破壊、除去又はデータ消去を確認した旨を文書で報告させるとともに、当該報告書を５年間保存しなければならない。

４　情報セキュリティ管理者は、前項の作業について外部で事業者に実施させる場合は、あらかじめ内部で職員にデータ消去を実施させ、結果を目視で確認後に記録を作成させた上で、事業者に引き渡さなければならない。また、作業完了後は事業者に完了証明書を提出させるとともに、当該証明書を５年間保存しなければならない。

５　情報セキュリティ管理者は、電子計算機、複合機等についてリース契約を行う場合は、第１項から第４項の規定に基づいて対応するよう仕様書又は契約書に明記しておかなければならない。

６　標準準拠システム等をガバメントクラウドにおいて利用する場合、情報セキュリティ管理者は、クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）についての方針及び手順が、セキュリティを確保した対応となっているか、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を利用し確認しなければならない。

第４節　管理区域

（管理区域の設定）

第 43 条　情報セキュリティ管理者は、所管する重要情報資産を保管する区域、その他あらかじめ許可された者のみが立ち入ることができる区域を明確に定めなければならない。

2　情報セキュリティ管理者は、前項の区域に対して、許可されていない第三者が立ち入らないように適切に管理しなければならない。

（電子計算機室の入室管理）

第 44 条　情報システム管理者は、電子計算機室について、次に掲げる措置を実施する。

（1）ID カード、生体認証又は入室用パスワードにより入室管理を行うこと。

（2）ID カード又は生体認証を使用する場合は、貸与状況や登録状況を明らかにする管理簿を設けること。

（3）入室用パスワードを使用する場合は、パスワードを定期的に変更すること。

（4）ID カード、生体認証又は入室用パスワードの使用によらない者の入室を許可する場合にあっては、入室を許可した者の氏名、日時、その他入退室に関する必要な事項を記入する入退室管理簿により入室管理を実施すること。

2　情報システム管理者は、電子計算機室に入室する者に対して名札の着用を求めるとともに、必要に応じて身分証明書等により身元の確認を行うものとする。

3　情報システム管理者は、外部からの訪問者が電子計算機室に入室する場合は、必要に応じて立ち入り区域を制限した上で、職員による立ち会いを行わせなければならない。

4　情報システム管理者は、外部からの訪問者による電子計算機室への電磁的記録媒体又は電子計算機の持ち込みを許可する場合は、個人所有である機器等ではないと容易に判別できるよう、持ち込みを許可する電磁的記録媒体又は電子計算機に所属や委託事業者名、許可した日付等を記載したラベルを貼り付けるなどの措置を講じさせなければならない。

（機器等の搬出入）

第 45 条　情報システム管理者は、搬入する機器等を既存の情報システムと連携及び接続する場合に生じる影響について、あらかじめ職員又は委託事業者に確認を行わせなければならない。

2　情報システム管理者は、電子計算機等を搬出入する場合は、職員を立ち会わせなければならない。

第５節　通信回線及び通信回線装置の管理

（施設内の通信回線及び通信回線装置の管理）

第 46 条　情報システム管理者は、所管する通信回線について、施設管理部門と連携して適正に管理するとともに、通信回線敷設図、結線図等を適正に保管しなければならない。

2　情報システム管理者は、所管する通信回線装置について、不正アクセス等のリスクを低減するネットワーク構成とし、当該通信回線装置の提供者が提示する推奨設定や業界標準、ベストプラクティス等を参照し、通信回線装置の各種設定を行う等、適切なセキュリティ対策を実施しなければならない。

（送受信データの保護）

第 47 条　情報システム管理者は、通信回線を用いて重要情報に該当するデータを送信する場合は、当該データが安全かつ確実に送信されるよう通信経路を制限する措置を講じなければならない。ただし、当該措置が講じられない場合にあっては、当該データを暗号化する措置を実施しなければならない。

2　情報システム管理者は、通信回線について、伝送途上にデータの破壊、盗聴、改ざん、消去等が生じないよう必要に応じて不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

3　情報システム管理者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

（通信回線の冗長化）

第 48 条　高い業務継続性（可用性）を求められる情報システムを所管する情報システム管理者は、情報システムの運用停止を回避するため通信回線の冗長化を行うことを検討しなければならない。

第６節　端末等の管理

（執務室等で利用する業務端末の管理）

第 49 条　情報セキュリティ管理者は、執務室等で利用する業務端末を盗難から防止するため、次に掲げるいずれかの措置を講じなければならない。

（１）盗難防止用の鎖による業務端末の固定

（２）施錠できるロッカー等への収納

（３）設置場所の施錠

（業務端末のログイン設定）

第 50 条　情報システム管理者は、情報システムに使用される業務端末へのログインに際し、知識（パスワード等）、所持（ID カード等）、存在（生体認証等）等を利用した認証情報の入力を必要とするように設定しなければならない。

（外部で利用する業務端末の管理）

第 51 条　情報システム管理者は、外部で利用する業務端末について、エンドポイント対策、遠隔消去機能を利用する等の措置を講じるよう努めなければならない。

（業務外ネットワークへの接続の禁止）

第 52 条　情報セキュリティ管理者は、所管する業務端末が異なるネットワークに接続できないように、OS のポリシー設定等により技術的に制限するよう努めなければならない。

（市民が利用する端末等）

第 53 条　情報システム管理者は、市民が利用する端末等について、盗難防止対策、アクセス制御その他の情報セキュリティに必要な措置を講じなければならない。

第５章　人的セキュリティ対策

第１節　職員の責務

（情報セキュリティポリシー等の遵守）

第 54 条　職員は、情報セキュリティポリシー、実施手順及び関連規程に定められている事項を遵守しなければならない。

（業務目的以外の利用等の禁止）

第 55 条　職員は、業務目的以外で情報資産を利用してはならない。

２　職員は、情報セキュリティ管理者の許可なく、情報資産を複製又は外部への持ち出しを行ってはならない。

（情報資産の職場以外での利用）

第 56 条　職員は、業務端末、電磁的記録媒体、重要情報が含まれる書面等を職場以外に持ち出す場合は、情報セキュリティ管理者の許可を得なければならない。

2　職員は、前項の規定により情報資産を持ち出した場合は、移動時において常に当該情報資産を携行する等、紛失、盗難等に厳重に注意しなければならない。

（職場以外での情報処理業務の実施）

第 57 条　職員は、自宅その他、職場以外で情報処理業務を行う場合は、情報セキュリティ管理者の許可を得なければならない。

（支給以外の電子計算機等の利用禁止）

第 58 条　職員は、支給以外の電子計算機、電磁的記録媒体等の情報資産を原則業務に利用してはならない。ただし、情報セキュリティ管理者が業務上特別の理由があると認める場合に限り利用することができる。

2　情報セキュリティ管理者は、前項ただし書の規定により支給以外の情報資産の利用を認める場合であって、当該情報資産を市が管理する通信回線に接続する場合にあっては、都市経営部デジタル戦略課長の許可を得なければならない。

3　職員は、支給以外の電子計算機、電磁的記録媒体等を業務に利用する場合は、次に掲げる事項を遵守しなければならない。

（1）情報セキュリティ管理者の許可を得ること

（2）コンピュータウイルスチェックが実施されていること

（3）無許可で重要情報を記録したり、持ち出したりしないこと

（4）業務に利用する必要がなくなった時点で、支給以外の電子計算機、電磁的記録媒体等から業務に関係する情報を削除すること

4　情報セキュリティ管理者は、第１項及び第２項の規定に基づき、支給以外の情報資産の職場への持ち込みを許可した場合は、記録を作成し、保管しなければならない。

（電子計算機の無断変更、無断接続等の禁止）

第 59 条　電子計算機を利用する職員は、当該電子計算機を所管する情報システム管理者の許可なく、電子計算機のセキュリティ機能の設定の変更又は周辺装置の増設を行ってはならない。

2　電子計算機を利用する職員は、当該電子計算機を所管する情報システム管理者の許可なく、当該電子計算機の接続が認められたネットワーク以外のネットワーク（無線通信による接続を含む。）に接続してはならない。

3　職員は、重要情報に該当するデータを、約款による外部サービス（フリーメール、ファイルスト

レージ、グループウェア等の、市との契約締結を要さず約款に基づきインターネット上で提供される外部サービスのことをいう。）で取り扱ってはならない。ただしWeb会議サービスや、必要なセキュリティ対策について約款内で確認できる場合又は約款外で合意文書を取り交わすことにより確認できる場合については、この限りでない。

（机上の業務端末等の管理）

第60条　職員は、業務端末、電磁的記録媒体又は書面等について、情報セキュリティ管理者の許可なく情報を第三者に使用又は閲覧されることがないように、離席時の業務端末のロック又は電磁的記録媒体及び書面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。

（異動、退職時の対応）

第61条　職員は、異動、退職等により業務を離れる場合は、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を漏らしてはならない。

（遵守すべき事項の掲示）

第62条　情報セキュリティ管理者は、職員が常に留意しておくべき主な情報セキュリティ対策について、職員が常に目にすることができるよう掲示しておくものとする。

（委託事業者に対する説明）

第63条　情報セキュリティ管理者は、情報システムの開発・保守、重要情報を取り扱う業務等を事業者に発注する場合は、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容を説明し、遵守させなければならない。

第２節　研修・訓練

（職員に対する研修）

第64条　情報セキュリティ管理者は、この基準が定める情報セキュリティ対策の適切かつ円滑な運営を行うために、毎年度１回以上、職員の職責及び能力に応じた研修を実施しなければならない。

２　前項の規定による研修の実施を支援するため、都市経営部デジタル戦略課長は、総務省、外部機関等が開催する研修の活用を含め、情報セキュリティに関する研修を企画し、情報セキュリティ管理者に提供するものとする。

3　職員は、毎年度１回以上、情報セキュリティに関する研修に参加しなければならない。

（契約相手及び第三者の利用者に対する研修）

第 65 条　情報セキュリティ管理者は、所管の業務に係る契約相手及び第三者の利用者に対し、所管する業務における遵守事項等に関する研修を実施するよう努めなければならない。

2　標準準拠システム等をガバメントクラウドにおいて利用する場合、情報セキュリティ管理者は、委託先を含む関係者について委託先等で研修が行われていることを確認しなければならない。

（未受講者への対応）

第 6 条　情報セキュリティ管理者は、実施した研修の未受講者に対してフォローアップを実施し、確実に全員が研修を受けるように努めなければならない。

（研修の実施結果の記録）

第 67 条　情報セキュリティ管理者は、実施した研修について、日付、内容、受講者等を記録するものとする。

（試験及び訓練の実施）

第 68 条　情報セキュリティ管理者は、災害及び大規模な疾病の流行等に備えて策定された業務継続計画に基づき、特に情報システムが使用不能になった場合などの対応及び復旧について、定期的に試験及び訓練を実施するものとする。

第３節　情報セキュリティインシデント発生時の対応

（情報セキュリティインシデントの報告）

第 69 条　職員は、情報セキュリティインシデントを認知した場合は、直ちに情報セキュリティ管理者に報告しなければならない。

2　前項の報告を受けた情報セキュリティ管理者は、直ちに復旧その他の措置を可能な限り講じるとともに、軽微なものを除き、状況、支障の程度等を、部等情報セキュリティ責任者及び都市経営部デジタル戦略課長に報告するほか、発生した情報セキュリティインシデントに関係する他の情報セキュリティ管理者又は情報システム管理者と相互に連絡調整を行い、被害状況の把握、被害拡大を防止するために可能な措置を講じなければならない。

3　前項の報告を受けた部等情報セキュリティ責任者又は都市経営部デジタル戦略課長は、支障の

程度等を考慮した上で、必要に応じて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。

4　前２項の報告を受けた情報セキュリティ統括責任者又は部等情報セキュリティ責任者は、必要に応じて副市長及び市長に報告を行うものとする。

5　都市経営部デジタル戦略課長は、認知した情報セキュリティインシデントが個人情報・特定個人情報の漏えい等であるときは、必要に応じて個人情報保護委員会に報告しなければならない。

6　都市経営部デジタル戦略課長は、認知した情報セキュリティインシデントが住基ネット又はLGWANに係るものであるときは、別に定める判断基準に従い、軽微なものを除き、大阪府、地方公共団体情報システム機構等と相互に連絡調整を行い、被害状況の把握、被害拡大を防止するための措置その他必要な措置を講じなければならない。

（外部からの報告窓口の設置）

第70条　都市経営部デジタル戦略課長は、市の所管する情報システム、重要情報等に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための連絡先を公表するものとする。

（クラウドサービス事業者が検知した情報セキュリティインシデントの報告）

第71条　標準準拠システム等をガバメントクラウドにおいて利用する場合、情報セキュリティ管理者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

（情報セキュリティインシデントへの対応）

第72条　都市経営部デジタル戦略課長は、認知した情報セキュリティインシデントに関係する情報セキュリティ管理者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示、助言等を行うものとする。また、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示するものとする。

2　情報セキュリティ統括責任者は、情報セキュリティインシデントについて、必要があると認めるときは、セキュリティ会議を招集し、対応及び対策について審議するものとする。

3　前項の規定によりセキュリティ会議で決定された事項に基づき、都市経営部デジタル戦略課長は、直ちに関係する情報セキュリティ管理者に対して必要な対応及び対策に関する指示を行わなければならない。

4　前項の指示を受けた関係する情報セキュリティ管理者は、直ちにデータ保護等の必要な措置及び当該情報セキュリティインシデントに係る所管業務の処理について、適切な措置を講じなければならない。

（情報セキュリティインシデントの記録・再発防止）

第 73 条　情報セキュリティ管理者は、発生した情報セキュリティインシデントについて、対応の内容を記録し、原因の分析及び再発防止策の検討結果と合わせて部等情報セキュリティ責任者及び都市経営部デジタル戦略課長に報告しなければならない。

2　都市経営部デジタル戦略課長は、認知した情報セキュリティインシデントについて、原因及び再発防止策の検討結果を情報セキュリティ統括責任者に報告するものとする。

3　情報セキュリティ統括責任者は、都市経営部デジタル戦略課長に対し、前項の規定により報告を受けた再発防止策を実施するために必要な措置を指示するものとする。

（住基ネットにおける緊急時対応）

第 74 条　前４条に定めるもののほか、住基ネットに係る情報セキュリティインシデント発生時の措置については、豊中市住民基本台帳ネットワークシステム緊急時対応計画に定めるところによる。

第４節　ID・パスワード等の管理

（組織認証用 ID カードの管理）

第 75 条　情報セキュリティ管理者は、組織認証用 ID カード（電子計算機等を操作する職員が所属する部署を識別することができるようにするための ID カードをいう。以下同じ。）を紛失又は破損しないよう、厳重に管理しなければならない。

2　職員は、組織認証用 ID カードを使用する場合は、情報セキュリティ管理者の許可を得なければならない。

3　職員は、業務上必要がないときは、組織認証用 ID カードを ID カード読取装置から取り外しておかなければならない。

4　情報セキュリティ管理者は、組織認証用 ID カードを紛失又は破損した場合は、直ちに組織認証用 ID カードを所管する情報システム管理者に報告しなければならない。

5　前項の規定による報告を受けた情報システム管理者は、当該組織認証用 ID カードを直ちに無効としなければならない。

（個人認証用 ID カードの管理）

第 76 条　個人認証用 ID カード（電子計算機等を操作している者を識別することができるようにするための ID カードをいう。以下同じ。）を貸与された職員は、個人認証用 ID カードを紛失又は破損しないよう厳重に管理しなければならない。

2　職員は、自己の管理する個人認証用 ID カードを他人に使用させてはならない。

3　職員は、業務上必要がないときは、個人認証用 ID カードを ID カード読取装置から取り外しておかなければならない。
4　職員は、個人認証用 ID カードを紛失又は破損した場合は、直ちに情報セキュリティ管理者に報告しなければならない。
5　前項の規定による報告を受けた情報セキュリティ管理者は、直ちに個人認証用 ID カードを所管する情報システム管理者に報告しなければならない。
6　前項の規定による報告を受けた情報システム管理者は、当該個人認証用 ID カードを直ちに無効としなければならない。

（不要となった ID カードの廃棄）

第 77 条　情報システム管理者は、職員の退職、ID カードの切り替え等により使用しなくなった ID カードについては、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（ID の取扱い）

第 78 条　職員は、 自己が利用している個人 ID を他人に利用させてはならない。
2　職員は、 組織での共用が認められている組織 ID を利用する場合であっても、組織 ID の利用が認められている者以外に利用させてはならない。

（パスワードの取扱い）

第79条　職員は、自己の管理するパスワードについて、次に掲げる事項を遵守しなければならない。
（1）パスワードは、他者に知られないように管理しなければならない。
（2）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てはならない。
（3）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（一例としてアルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。
（4）パスワードが流出したおそれがある場合は、情報セキュリティ管理者に直ちに報告し、パスワードを速やかに変更しなければならない。
（5）複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。
（6）仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
（7）サーバ、ネットワーク機器及び職員が共用する業務端末のパスワードについて、ログイン時に入力を省略することを目的に端末等にパスワードを記憶させることをしてはならない。
（8）職員間でパスワードを共有してはならない（ただし共用 ID に対するパスワードは除く）。
（9）共用 ID に対するパスワードは、年１回以上変更しなければならない。
2　前項第４号の規定による報告を受けた情報セキュリティ管理者は、直ちにパスワードを所管する情報システム管理者に報告しなければならない。

3　前項の規定による報告を受けた情報システム管理者は、漏えいしたおそれがあるパスワードを直ちに無効とし、部等情報セキュリティ責任者を経て情報セキュリティ統括責任者に報告するとともに、漏えいの原因を解明して必要な措置を講じた上で、新たなパスワードを設定しなければならない。

第６章　技術的セキュリティ対策

第１節　電子計算機及びネットワークに関するセキュリティ対策

（ファイル保管サーバの管理）

第 80 条　複数の部署が共同でファイルを保管するサーバを所管する情報システム管理者は、部署ごとに使用できるサーバの容量を設定し、当該サーバを利用する情報セキュリティ管理者に通知しなければならない。

2　前項に規定するサーバを所管する情報システム管理者は、職員が他部署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設定しなければならない。

（バックアップの実施）

第 81 条　情報システム管理者は、電子計算機に記録された重要情報について、周期及び保管期間を決定した上でバックアップを行わなければならない。

2　情報システム管理者は、前項のバックアップを行った場合は、その旨を記録しなければならない。

3　情報システム管理者は、重要情報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、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行わなければならない。

4　情報システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、次に掲げる事項を確認しなければならない。

（１）クラウドサービス事業者によるバックアップ機能の仕様

（２）前号の仕様が本市の求める要求事項を満たすこと

5　情報システム管理者は、クラウドサービス事業者からバックアップ機能が提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

（作業の記録及び確認）

第 82 条　情報システム管理者は、所管する情報システム又は情報システムを構成する電子計算機、

通信回線及び通信機器について、増設又は変更を行う場合は、作業内容について記録を作成し、窃取、改ざんされないよう適切に管理し、運用・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。

2　情報システム管理者は、前項に規定する作業については原則２人以上で行い、相互に作業内容の確認を行わなければならない。

（システム仕様書等の管理）

第 83 条　情報システム管理者は、ネットワーク構成図、情報システムの仕様書について、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、適切に管理しなければならない。

（ログの管理）

第 84 条　情報システム管理者は、所管する重要情報を扱う情報システムのログの管理について、次に掲げる措置を講じなければならない。

（１）重要情報へのアクセス、情報システムの設定変更等のログを取得し、一定期間保管すること。

（２）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ること。

（３）電磁的記録媒体等によりログのバックアップを行うこと。

（４）ログが窃取、改ざん及び誤消去されないよう適切に管理すること。

（５）取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

2　情報システム管理者は、標準準拠システム等をガバメントクラウドにおいて利用する場合、クラウドサービス事業者が収集し、保存するログに関する改ざんの防止等、保護の対応について、ログ管理等に関する対策や機能に関する情報を確認し、ログに関する保護が実施されているのか確認しなければならない。

3　情報システム管理者は、標準準拠システム等をガバメントクラウドにおいて利用する場合、監査及び調査に必要となるログ等の情報について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

（障害記録）

第 85 条　情報システム管理者は、所管する情報システムを構成する電子計算機、通信回線及び通信機器に障害が生じた場合は、障害内容を記録しなければならない。

（ネットワークの接続制御等）

第 86 条　情報システム管理者は、所管する情報システムのネットワークについて、経路制御（ルーティング）、通信データの選別（フィルタリング）等を行う場合は、設定の不整合が発生しないように、通信機器等の設定を適切に行わなければならない。

2　情報システム管理者は、不正アクセスを防止するため、所管する情報システムのネットワークに適正なアクセス制御を施さなければならない。

3　情報システム管理者は、所管する情報システムを他の情報システム管理者が所管するネットワークに接続して運用する場合は、当該ネットワークを所管する情報システム管理者の指示に従わなければならない。

4　自部署以外が利用する情報システムが接続されたネットワークを所管する情報システム管理者は、保守その他の事由によりネットワークの一部又は全部の運用を停止する必要が生じた場合は、可能な限り停止による影響を最小限に止めるように計画するとともに、事前に当該ネットワークに接続された情報システムを利用する情報セキュリティ管理者に通知するものとする。

5　情報システム管理者は、所管するネットワークの設計書、ネットワークに関する設定情報を記載した文書等を整備し、適切に管理しなければならない。

6　情報システム管理者は、所管するネットワークの障害発生に備え、連絡体制及び復旧対応手順を定めなければならない。

7　情報システム管理者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、定期的な確認により見直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 87 条　情報システム管理者は、市民等外部の者が利用できる情報システムについて、市が管理するネットワークへの不正アクセスを防止するための必要な措置を講じなければならない。

（市以外が管理するネットワークとの接続制限）

第 88 条　情報システム管理者は、市が管理するネットワークを市以外のものが管理するネットワークに接続しようとする場合は、書面により情報セキュリティ統括責任者の許可を得なければならない（ただし、LGWAN に接続する場合を除く。）。

2　情報システム管理者は、接続しようとする市以外の者が管理するネットワークの構成及びセキュリティ対策を調査し、市のネットワーク、電子計算機等に影響が生じないことを確認しなければならない。

3　情報システム管理者は、市が管理するネットワーク上のウェブサーバ等をインターネットに公開する場合は、次に掲げる措置を講じなければならない。

（1）庁内ネットワークへの侵入を防御するため、ファイアウォール等を外部ネットワークとの

境界に設置した上で接続すること。

（２）脆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。

４　情報システム管理者は、第１項の規定により接続した市以外のものが管理するネットワークにおいて、データの漏えい、改ざん等が生じるおそれがある場合は、情報セキュリティ統括責任者又は部等情報セキュリティ責任者の判断に基づき、速やかに当該ネットワークを物理的に遮断しなければならない。

（複合機のセキュリティ管理）

第 89 条　情報セキュリティ管理者は、複合機が備える機能、設置環境、重要情報の取扱い等に応じ、適切なセキュリティ対策を講じなければならない。

（特定用途機器のセキュリティ管理）

第 90 条　情報セキュリティ管理者は、特定用途機器について、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しなければならない。

（無線通信回線及びネットワークの盗聴対策）

第 91 条　情報セキュリティ統括責任者は、無線通信回線の利用を認める場合は、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

２　重要情報を取り扱うネットワークを所管する情報システム管理者は、当該ネットワークについて、情報の盗聴等を防ぐため、通信経路を制限する措置又は暗号化の措置を講じなければならない。

３　情報システム管理者は、電子計算機及び周辺機器について、利用を認められた無線通信回線以外の無線通信回線に接続してはならない。

第２節　電子メールに関するセキュリティ対策

（電子メールのセキュリティ管理）

第 92 条　電子メールの送受信に使用する電子計算機を所管する情報システム管理者（以下「メールシステム管理者」という。）は、当該電子計算機が不正に第三者から利用されないよう適切に管理

しなければならない。

2　メールシステム管理者は、電子メールの受信又は送信において異常を検知した場合は、電子メールの送受信に使用する電子計算機の運用を停止しなければならない。

3　メールシステム管理者は、電子メールの送受信容量の上限を設定しなければならない。

4　メールシステム管理者は、利用者ごとの電子メールボックスの容量の上限を設定し、周知しなければならない。

5　メールシステム管理者は、職員が電子メールを利用して情報資産を無断で外部に持ち出すことがないように監視するため、電子メールの送信先に情報セキュリティ管理者を含めなければ送信できない等の措置を講じるものとする。

（電子メールの利用制限）

第 93 条　職員は、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）メールシステム管理者が管理する以外の電子メールを利用してはならない。ただし、都市経営部デジタル戦略課長が承認済み外部サービスとして記録した電子メールサービスについては、この限りでない。

（2）業務上必要のない送信先に電子メールを送信してはならない。

（3）送信先の電子メールアドレスを十分に確認しなければならない。

（4）複数人に同時に電子メールを送信する場合は、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をわからないようにしなければならない。

（5）マルウェア感染や標的型攻撃が疑われるような不審なメールを受信した場合は、添付ファイルの開封または本文中に記載されているリンク先へのアクセス等をせず、直ちに情報セキュリティ管理者を経て、メールシステム管理者に報告し、指示を仰がなければならない。

（電子メールの調査）

第 94 条　メールシステム管理者は、前条の規定に違反することが明らかである場合等においては、所管する電子計算機で送受信される電子メールの内容等を調査することができる。

2　情報セキュリティ管理者は、職員が送信する電子メールの内容を確認しなければならない。

第３節　暗号化・電子署名

（通信の暗号化）

第 95 条　情報システム管理者は、通信の暗号化を行う場合は、技術や計算式等の危殆化により第三者に復号されることのないよう、安全な暗号化通信方式を選択し、情報セキュリティ統括責任者が定めるところにより、暗号のための鍵を管理しなければならない。

（電子署名の利用）

第 96 条　情報システム管理者は、電子署名を利用する場合は、情報セキュリティ統括責任者が定めるところにより、信頼できる機関から発行された電子証明書を使用しなければならない。

第４節　ソフトウェアの管理

（利用するソフトウェアの限定）

第 97 条　情報システム管理者は、所管する情報システムにおいて利用するソフトウェアを定めなければならない。

２　情報セキュリティ管理者は、定められていないソフトウェアを端末等に導入してはならない。ただし、情報システム管理者が、業務上必要があると認めるときは、この限りでない。

（ソフトウェアの管理）

第 98 条　情報システム管理者は、所管する情報システムに関するソフトウェアについて、管理簿を作成し、適切に管理しなければならない。

２　情報システム管理者及び情報セキュリティ管理者は、ソフトウェアの導入について、ライセンス数や使用許諾条件を遵守しなければならない。

（Web 会議サービスの利用時の対策）

第 99 条　情報セキュリティ統括責任者は、Web 会議を適切に利用するための利用手順を策定するものとする。

２　職員は、市の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しなければならない。

３　職員は、Web 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。

４　職員は、外部から Web 会議に招待される場合は、市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

（ソーシャルメディアサービスの利用）

第 100 条　情報セキュリティ管理者は、市が管理するアカウントで電子掲示板や動画共有サイト等のソーシャルメディアサービスを利用する場合は、次に掲げる措置を講じなければならない。

（1）市のアカウントによる情報発信が、実際に市によるものであることを明らかにするために、市のホームページ等の自己管理ウェブ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部署を明示する等の方法でなりすまし対策を実施すること。
（2）パスワード等の認証情報及びこれを記録した媒体（ID カード等）等を適切に管理すること。
（3）重要情報をソーシャルメディアサービスで取り扱わないよう、サービスを利用する職員に周知・徹底すること。
（4）アカウントの乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、市のホームページ等で周知を行うとともに、部等情報セキュリティ責任者及び都市経営部デジタル戦略課長に報告すること。
（5）高い可用性を求められる情報の提供にソーシャルメディアサービスを用いる場合は、自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

第５節　アクセス制御

（アクセス権限の設定）

第 101 条　情報システム管理者は、所管する情報システムのアクセス制御を行うため、次に掲げる措置を講じなければならない。
（1）アクセス権限を管理者権限（情報システムを管理するためのアクセス権限をいう。以下同じ。）及び利用者権限（情報システムを利用するためのアクセス権限をいう。以下同じ。）に区分し、業務に従事する職員に割り当てること。
（2）管理者権限及び利用者権限の割り当てについて、管理簿により適切に管理すること。
（3）管理者権限及び利用者権限の登録、変更又は抹消の方法を定めること。
（4）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すること。
（5）管理者権限の割り当ては、必要最小限の者に限定すること。
（6）情報システムの設定情報、ログ等の情報セキュリティの確保に必要な情報の閲覧は、管理者権限を有する者に限ること。
（7）特権を付与された ID を初期設定以外のものに変更すること。ただし、変更ができない情報システムの場合はこの限りでない。
（8）特権を付与された ID 及びパスワードの変更について、許可なく委託事業者に行わせないこと。

2　情報セキュリティ管理者は、特に必要があると認める場合は、業務端末等の情報処理を前項第１号に規定する職員以外の者に行わせることができる。

（職員による外部からのアクセス等の制限）

第 102 条　情報セキュリティ管理者は、職員に外部から内部の情報システムにアクセスさせる場合は、情報システム管理者の許可を得なければならない。

2　情報システム管理者は、外部からのアクセスを認める場合は、システムを利用する者の本人確認を行う機能を確保しなければならない。

3　情報システム管理者は、外部からのアクセスを認める場合は、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

4　情報システム管理者は、外部からのアクセスに利用する業務端末を職員に貸与する場合は、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。

5　情報セキュリティ管理者は、外部から持ち帰った業務端末を庁内のネットワークに接続する場合は、事前にマルウェアに感染していないこと等を職員に確認させなければならない。

6　情報システム管理者は、所管する情報システムへの外部からのアクセスに利用する通信回線については、閉域網を使用する等、安全な接続方式を採用しなければならない。

（接続機器の制御）

第 103 条　情報システム管理者は、所管する情報システムで使用される電子計算機について、IP アドレス、MAC アドレス等の識別番号、電子証明書による端末認証等を利用して接続の可否を管理しなければならない。

（ログインの制御）

第 104 条　情報システム管理者は、ログイン試行回数の制限、アクセスタイムアウトの設定等、情報システムが保有する機能に応じ、権限を持たない者からのアクセスを防止するための必要な設定を行うものとする。

（特権による接続時間の制限）

第 105 条　情報システム管理者は、特権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。

（インターネット閲覧の制限）

第 106 条　インターネットが利用できる情報システムを所管する情報システム管理者は、業務目的以外にインターネットが利用されないよう、アクセス可能なウェブサイトを制限する等、必要な措置を講じなければならない。

第６節　情報システムの開発・導入・保守等

（機器等の調達に係る仕様）

第 107 条　情報システム管理者は、ネットワークの基幹機器及び重要な情報システムにかかる機器等を調達する際は、品質保証体制及び設置時や保守時のサポート体制が確立していること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できることを調達仕様に定めなければならない。

（情報システム導入等の協議）

第 108 条　情報システム管理者は、情報システムを導入又は変更しようとするときは、目的、機器構成、安全管理措置等について、情報システム機器の管理運営に関する規程（昭和 61 年 11 月 1 日訓令第 1 号）第 8 条に基づき、あらかじめ都市経営部デジタル戦略課長と協議しなければならない。

２　情報システム管理者は、情報システムの導入又は変更の完了後速やかに、都市経営部デジタル戦略課長に報告しなければならない。

３　情報システム管理者は、所管する情報システムの運用に関し、関係する情報システム管理者又は情報セキュリティ管理者に対し必要な調整を行うことができる。

（情報システムの開発・導入等）

第 109 条　情報システム管理者は、情報システムの開発、導入及び変更並びに保守（以下「開発等」という。）を行う場合は、次に掲げる措置を講じなければならない。

（１）責任者及び監督者を定めること。

（２）作業者及び作業範囲を明確にすること。

（３）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とともに、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を明記すること。

（４）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、情報セキュリティ上問題のないことを確認すること。

（５）開発等を行うために使用する ID を管理し、開発等が完了後直ちに抹消すること。

（６）開発等の責任者及び作業者のアクセス権限を明確にすること。

（７）開発等の責任者及び作業者が使用する電子計算機及びソフトウェアを特定すること。

（８）利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアを削除すること。

（９）ウェブアプリケーションの開発においては、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ること。

（10）開発を行う環境をシステム運用環境及び他の情報システムから分離すること。

（11）開発等に関する手順を明確にすること。

（12）作業記録をとること。

（13）電子計算機に記録されているデータの保存を確実に行い、情報システムの移行に伴う影響を最小限とすること。

（14）必要な可用性が確保されていることを確認した上で情報システムの導入又は変更を行うこと。

（15）保守を行う場合は、セキュリティ上問題となるおそれがあるソフトウェアを使用しないこと。

（16）電子計算機に初期設定されているパスワードを変更すること。

（テストの実施）

第 110 条　情報システム管理者は、情報システムを導入又は変更する場合は、運用を開始する前に十分なテストを行わなければならない。

２　情報システム管理者は、システム運用環境に保存された個人情報をテストに使用してはならない。

３　情報システム管理者は、開発した情報システムの受け入れテストを行う場合は、開発した組織と導入する組織のそれぞれが独立したテストを行うよう努めなければならない。

４　情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

（機器等の納入時又は情報システムの受入れ時）

第 111 条　情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

２　情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（情報システムの基盤を管理又は制御するソフトウェアにおける対策）

第 112 条　情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを利用する場合は、ソフトウェアの特性を踏まえ、情報システム全体に影響を及ぼすような重要な操作及び、情報セキュリティに関する設定や構成を変更する際の手順を整備しなければならない。

2　情報システム管理者は、当該ソフトウェアで情報セキュリティインシデントが発生した際、利用するソフトウェアの権限を用いて他の情報システムに対して不正なアクセスがなされないよう、情報セキュリティインシデントを認知した際の対処手順を整備しなければならない。
3　情報システム管理者は、利用を認める当該ソフトウェアについて、ソフトウェアのバージョンやサポート期限など、定期的な確認による見直しを行わなければならない。

（開発等に関連する資料等の整備・保管）

第 113 条　情報システム管理者は、情報システムの開発等に関連する資料及び情報システムの運用に関連する文書を適切に整備・保管しなければならない。
2　情報システム管理者は、情報システムの導入又は変更に関するテスト結果について、一定期間保管しなければならない。

（入出力データの正確性の確保）

第 114 条　情報システム管理者は、入力されるデータの範囲、妥当性をチェックする機能を組み込むように情報システムを設計しなければならない。
2　情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次に掲げる措置を講じなければならない。
（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。
3　情報システム管理者は、情報の処理が正しく反映されたデータが出力されるように情報システムを設計しなければならない。
4　情報セキュリティ管理者は、重要情報に関する情報処理を行う場合は、入出力されるデータの正確性を確保するため、処理結果について複数人で確認するようにしなければならない。

（情報システムの変更管理）

第 115 条　情報システム管理者は、所管する情報システムの設定の変更、電子計算機の構成の変更等を行った場合は、設定及び構成の履歴を記録しなければならない。

（ソフトウェアの更新）

第 116 条　情報システム管理者は、ソフトウェアを更新する場合は、情報システムに与える影響を検証しなければならない。ただし、ソフトウェアを更新しないことにより情報セキュリティインシデントが発生するおそれがある場合その他の緊急を要する場合はこの限りでない。

（情報システムについての対策の見直し）

第 117 条　情報システム管理者は、必要に応じて情報システムの情報セキュリティ対策を適切に見直さなければならない。

2　情報セキュリティ統括責任者は、本市における情報システムの情報セキュリティ対策について横断的な改善が必要となる場合は、情報システム管理者に情報セキュリティ対策の見直しについて改善指示を行うものとする。

3　情報システム管理者は、前項の指示を受けた場合は、措置の結果について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。

第７節　マルウェア・不正アクセス対策

（マルウェア対策における措置事項）

第 118 条　情報システム管理者は、マルウェア対策として、次に掲げる措置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について、内部のネットワークとの接続ポイントにおいてチェックを行い、内部の情報システムへのマルウェアの侵入を防止すること。

（２）外部のネットワークに送信するファイルについて、内部のネットワークとの接続ポイントにおいてチェックを行い、マルウェアの外部への拡散を防止すること。

（３）マルウェアの情報を収集し、必要に応じ職員に情報提供し、注意喚起すること。

（４）所管に係る電子計算機にマルウェア対策のソフトウェアの導入を行い、常に最新の状態に更新すること。

（５）不具合の修正やバージョンアップ等のサポートが終了したソフトウェアを利用しないこと。また、ソフトウェアの利用を予定している期間中に、当該サポートが終了する予定がないことを確認すること。

（６）仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びクラウドサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施すること。SaaS 型を利用する場合は、これらの対応がクラウドサービス事業者側でされているのか、クラウドサービスを利用する前に確認すること。

（７）クラウドサービスを利用している状況下では、前号のセキュリティ対策が適切にされてい

るのか定期的にクラウドサービス事業者に報告を求めること。(標準準拠システム等をガバメントクラウドにおいて利用する場合に限る。)

（８）スタンドアロン（インターネット等の一切のネットワークや他の機器に接続せず、単独で機能する環境をいう。）の電子計算機について、当該機器で重要情報を扱う場合は、マルウェア対策のソフトウェアの導入を行い、定期的に最新の状態に更新すること。

（職員によるマルウェア対策）

第 119 条　職員は、マルウェア対策を行うため、次に掲げる事項を遵守しなければならない。

（１）マルウェア対策ソフトウェアの設定を変えないこと。

（２）外部から入手したデータ又はソフトウェアを取り込む場合は、マルウェア対策ソフトウェアによるチェックを行うこと。

（３）差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除すること。

（４）緊急の場合を除き、マルウェア対策ソフトウェアによるチェックを途中で止めないこと。

（５）情報システム管理者から提供されるマルウェアに関する情報を確認すること。

（マルウェアを発見した時の対応）

第 120 条　職員は、マルウェアが発見された場合又は感染が疑われる場合は、直ちに電子計算機の利用を中止し、電源を切らずに通信回線から切り離さなければならない。

２　前項の場合においては、直ちに情報セキュリティ管理者を経て、情報システム管理者に報告しなければならない。

３　情報セキュリティ統括責任者は、マルウェアが発見された場合に適切かつ迅速に対応することを目的とした手順を策定するものとする。

（支給以外の電子計算機等の対策）

第 121 条　情報システム管理者は、業務上市の支給以外の電子計算機等を所管する機器又はネットワークに接続する必要がある場合は、当該電子計算機等の情報セキュリティ対策を確認し、マルウェア感染等のリスクに細心の注意を払わなければならない。

（専門家の支援）

第 122 条　情報セキュリティ統括責任者は、実施しているマルウェア対策では不十分な事態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しておかなければならない。

（不正アクセス対策における措置事項）

第 123 条　情報システム管理者は、不正アクセス対策として、次に掲げる措置を講じなければならない。

（１）使用されていないポート番号を利用した通信を閉鎖すること。

（２）不要なサービスを削除又は停止すること。

（３）標準準拠システム等をガバメントクラウドにおいて利用する場合、情報セキュリティポリシーにおけるアクセス制御に関する事項が、クラウドサービス又はクラウドサービス事業者の提供機能等により実現できるか、利用前にクラウドサービス事業者に確認すること。

（４）標準準拠システム等をガバメントクラウドにおいて利用する場合、パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が情報セキュリティポリシーを満たすことを確認すること。

（５）不正アクセスによる攻撃を受けた場合は、攻撃の記録を保存すること。

（６）職員及び委託事業者が使用している電子計算機等から庁内のサーバに対する攻撃や、外部に対する攻撃を監視すること。

（７）サービス不能攻撃によるサービス利用の停止を防止するため、情報システムの可用性を確保する対策を行うこと。

（８）標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じること。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や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、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）を講じること。

第８節　セキュリティ情報の収集

（セキュリティに関する情報の収集・通知等）

第 124 条　都市経営部デジタル戦略課長は、情報セキュリティ技術の向上や情報セキュリティ対策に関する情報を収集し、必要に応じて情報セキュリティ管理者に通知しなければならない。

２　情報システム管理者は、前項の規定による通知等に限らず、所管する情報システムに係る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よう努めなければならない。

３　都市経営部デジタル戦略課長は、緊急度が高い情報セキュリティに関する情報について、直ちに情報セキュリティ統括責任者及び部等情報セキュリティ責任者に報告しなければならない。

４　前項の規定による報告を受けた部等情報セキュリティ責任者及び都市経営部デジタル戦略課長は、所管に係る情報システムの適正管理その他の情報セキュリティ対策について、必要な措置を講じなければならない。

５　情報システム管理者は、標準準拠システム等をガバメントクラウドにおいて利用する場合、ク

ラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定し、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

第７章　運用

第１節　情報システムの監視

（情報システムの監視）

第 125 条　情報システム管理者は、情報セキュリティインシデントを検知するため、所管する情報システムについて、次に掲げる監視を行うよう努めなければならない。

（１）重要情報に該当するデータの改ざんを検知するための監視

（２）電子計算機への不正侵入を検知するための監視

（３）急激な通信量の増大を検知するための監視

（４）電子計算機の処理能力及び記憶容量の限界到達を検知するための監視

２　情報システム管理者は、正確な監視結果を得るため、電子計算機における正確な時刻設定及び機器間の時刻同期ができる措置を実施するか、１ヶ月ごとに電子計算機の時刻を設定するよう努めなければならない。また、利用する外部サービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

３　情報システム管理者は、標準準拠システム等をガバメントクラウドにおいて利用する場合、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

４　情報システム管理者は、標準準拠システム等をガバメントクラウドにおいて利用する場合、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

５　情報システム管理者は、標準準拠システム等をガバメントクラウドにおいて利用する場合、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（１）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（２）クラウドサービス利用の終了手順

（３）バックアップ及び復旧

6　情報システム管理者は、新たな脅威の出現、運用、監視等の状況等を踏まえ、所管する情報システムにおける監視の対象や手法の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。

（調査及び閲覧）

第 126 条　情報セキュリティ統括責任者及び情報セキュリティ統括責任者が指名した者は、不正アクセス等の情報セキュリティインシデントの発生の防止及び調査のため、情報システムのログ及びデータの更新内容を閲覧することができる。

第２節　違反への対応

（違反の報告）

第 127 条　職員は、情報セキュリティポリシーに対する違反行為又は情報システムの運用を妨げるおそれのある行為を発見した場合は、直ちに情報セキュリティ管理者に報告しなければならない。

2　前項の規定による報告を受けた情報セキュリティ管理者は、当該行為を中止させるとともに、当該行為により業務等に重大な影響が生じるおそれがあると判断した場合は、部等情報セキュリティ責任者に報告しなければならない。

3　前項の規定により報告を受けた部等情報セキュリティ責任者は、情報セキュリティ管理者に対し、違反を起こした職員への改善指導や再発防止策の実施など適正な措置を求めなければならない。

4　情報セキュリティ管理者の指導によっても違反行為が改善されない場合、情報セキュリティ管理者は情報システム管理者に報告して当該職員のネットワーク又は情報システムを使用する権限を停止し、速やかに部等情報セキュリティ責任者に報告しなければならない。

5　前項の規定により報告を受けた部等情報セキュリティ責任者は、違反が改善されなかったことにより職員の権限を停止した旨を、都市経営部デジタル戦略課長を通じて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。

第３節　情報漏えい発生時の対応等

（情報漏えい発生時の対応手順の策定）

第 128 条　情報セキュリティ統括責任者は、重要情報に係る情報漏えいが発生した場合における対応を適切かつ迅速に実施するために、次に掲げる事項を記載した情報漏えい発生時の対応手順を策定するものとする。

（１）報告手順及び報告内容に関する事項

（２）事案の調査内容に関する事項
（３）セキュリティ会議における措置に関する事項
（４）公表及び本人への連絡に関する事項
（５）原因の分析及び再発防止策に関する事項
（６）情報漏えいに関与した職員の処分及び告訴に関する事項

2　標準準拠システム等をガバメントクラウドにおいて利用する場合、情報セキュリティ統括責任者は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

3　情報セキュリティ統括責任者は、前各項の規定により策定した手順及び計画について、組織体制の変化等、必要に応じて見直しを行うものとする。

第４節　例外措置

（例外措置の許可）

第 129 条　情報セキュリティ管理者及び情報システム管理者は、情報セキュリティポリシー等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には、情報セキュリティ統括責任者の許可を得て、例外措置を講じることができる。

（緊急時の例外措置）

第 130 条　情報セキュリティ管理者及び情報システム管理者は、行政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、事後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。

（例外措置の申請書の管理）

第 131 条　情報セキュリティ統括責任者は、例外措置の申請書及び審査結果を適正に保管させなければならない。

第５節　法令遵守、懲戒処分

（法令遵守）

第 132 条　職員は、職務の遂行において使用する情報資産を保護するために、次に掲げる法令のほか関係法令を遵守し、これに従わなければならない。

（１）地方公務員法(昭和 25 年法律第 261 号)

（２）著作権法（昭和 45 年法律第 48 号）

（３）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）

（４）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）

（５）サイバーセキュリティ基本法（平成 26 年法律第 104 号）

（６）個人情報の保護に関する法律（平成 15 年法律第 57 号）

（７）豊中市個人情報の保護に関する法律施行条例（令和 4 年豊中市条例第 44 号）

２　情報システム管理者は、外部サービスに商用ライセンスのあるソフトウェアをインストール又は IaaS 等でアプリケーションを構築する場合は、そのソフトウェアのライセンス条項への違反を引き起こさないよう、利用するソフトウェアにおけるライセンス規定に従わなければならない。

（懲戒処分）

第 133 条　情報セキュリティポリシーに違反した職員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て、地方公務員法による懲戒処分の対象とする。

第８章　業務委託、外部サービス

第１節　業務委託

（委託事業者の選定）

第 134 条　情報セキュリティ管理者は、委託事業者の選定にあたり、情報セキュリティに関する国際規格の認証取得状況等を参考にして、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（業務委託契約項目）

第 135 条　重要情報を取り扱う業務又は情報システムの導入、運用、保守、機器の廃棄その他情報処理に係る業務を委託しようとする場合は、業務委託の実施までに、委託内容に応じて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の遵守に関する事項
（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事項
（３）委託事業者の責任者、作業内容、作業者の所属、作業場所の特定（制限を含む。）に関する事項
（４）前号に規定する事項の変更に関する事項
（５）提供されるサービスレベルの保証に関する事項
（６）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に関する事項
（７）委託事業者の従業員に対する教育の実施に関する事項
（８）情報資産の目的外の使用、複製・複写及び委託事業者以外の者への提供の禁止に関する事項
（９）業務上知り得た情報の守秘義務に関する事項
(10) 再委託に関する制限事項の遵守に関する事項
(11) 情報資産の保管、返還及び廃棄に関する事項
(12) 委託業務の定期報告及び緊急時報告義務に関する事項
(13) 市による監査、検査の権利に関する事項
(14) 委託業務に係る情報セキュリティインシデント発生時における市による公表に関する事項
(15) 知的所有権及び著作権の権利の帰属に関する事項
(16) 前各号に違反した場合における契約解除の措置及び損害賠償に関する事項

（業務委託実施期間中の対策）

第 136 条　情報セキュリティ管理者は、委託した業務において、情報セキュリティインシデントの発生もしくは情報の目的外利用等を認知した場合は、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求を行わなければならない。

２　情報セキュリティ管理者は、業務委託の実施期間において、委託事業者に情報の適正な取扱いのための情報セキュリティ対策およびその履行状況の定期的な報告の実施を求めなければならない。

（業務委託終了時の対策）

第 137 条　情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めたうえで、適切に実施されたことを確認しなければならない。

（１）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
（２）提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

第２節　情報システムに関する業務委託

（情報システムに関する業務委託における委託事業者の選定）

第 138 条　情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図しない変更が加えられないようにするため、次に掲げる内容を含む情報セキュリティ対策を実施することを選定条件に加えるとともに、仕様を策定するよう努めなければならない。

（１）委託事業者もしくはその従業員、再委託先又はその他の者によって、情報システムに当市の意図しない変更が加えられないための管理体制

（２）委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

（３）情報システムの開発工程において、当市の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること及び当該品質保証体制が書類等で確認できること

（４）情報システムに当市の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、当市と委託事業者が連携して原因を調査・排除できる体制を整備していること及び当該体制が書類等で確認できること

（情報システムの構築を業務委託する場合の対策）

第 139 条　情報システム管理者は、情報システムの構築を業務委託する場合は、次に掲げる内容を含む対策の実施を、契約に基づき委託事業者に求めるよう努めなければならない。

（１）情報システムに関連する脆弱性についての対策要件として定めるセキュリティ要件を適切に実装すること

（２）試験を実施する際は、運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離し、試験項目及び試験方法を定めたうえで実施し、実施記録を保存すること

（３）開発工程においては、ソースコードが不正に変更・消去されることを防ぐために、ソースコードの管理を適切に行うこと

（４）セキュリティ機能が適切に実装されていることを確認するため、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること

（情報システムの運用・保守を業務委託する場合の対策）

第 140 条　情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるようにするため、次に掲げる要件について、契約に基づき、委託事業者に実施を求めるよう努めなければならない。

（１）情報システムの運用環境に課せられるべき条件の整備

（２）情報システムのセキュリティ監視を行う場合の監視手順や連絡方法
（３）情報システムの保守における情報セキュリティ対策
（４）運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策
（５）情報セキュリティ対策の実施により、情報システムに変更が生じた場合の報告

（情報システムに関する再委託）

第 141 条　前 7 条の規定は、再委託をする場合に準用する。

第３節　外部サービスの利用（重要情報を取り扱う場合）

（外部サービスの選定に係る規定の整備）

第 142 条　情報セキュリティ統括責任者は、次に掲げる事項を記載した外部サービス（重要情報を取り扱う場合）の選定に関する規定を整備しなければならない。
（１）外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「外部サービス利用判断基準」という。）
（２）外部サービス提供者の選定基準
（３）外部サービスの利用申請の許可権限者と利用手続
（４）外部サービス管理者の指名と外部サービスの利用状況の管理
（５）標準準拠システム等をガバメントクラウドにおいて利用する場合のクラウドサービス管理者の指名とクラウドサービスの利用状況の管理

（外部サービスの利用に係る規定の整備）

第 143 条　情報セキュリティ統括責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、外部サービス（重要情報を取り扱う場合）を利用して情報システムを導入・構築、運用・保守、利用終了する際のセキュリティ対策に関する規定を整備しなければならない。

（外部サービスの選定）

第 144 条　情報セキュリティ管理者は、重要情報の取扱いの有無、求められる可用性等を考慮した上で、外部サービス利用判断基準に従って、業務に係る影響度等を検討した上で外部サービスの利用を検討しなければならない。

２　情報セキュリティ管理者は、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めなければならない。
（１）外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利

用の禁止

（2）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

（3）外部サービスの提供にあたり、外部サービス提供者もしくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

（4）外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（5）情報セキュリティインシデントへの対処方法

（6）情報セキュリティ対策その他の契約の履行状況の確認方法

（7）情報セキュリティ対策の履行が不十分な場合の対処方法

3　情報セキュリティ管理者は、前項の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービスが、情報セキュリティポリシーを満たしているか否かを評価しなければならない。

4　情報セキュリティ管理者は、外部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、外部サービス提供者の選定条件に含めなければならない。

5　標準準拠システム等をガバメントクラウドにおいて利用する場合、部等情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認しなければならない。

6　情報セキュリティ管理者は、外部サービス上での重要情報の取扱いの有無、求められる可用性等を考慮した上で、必要に応じて以下の内容を外部サービス提供者の選定条件に含めなければならない。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

7　情報セキュリティ管理者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制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、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

8　情報セキュリティ管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めなければならない。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

9　情報セキュリティ管理者は、外部サービスの特性を考慮した上で、外部サービスが提供する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、情報セキュリティに関する役割及び責任の範囲を踏まえて、次に掲げる事項をすべて含むセキュリティ要件を定めなければならない。

（1）外部サービスに求める情報セキュリティ対策

（２）外部サービスで取り扱う情報が保存される国・地域及び廃棄の方法
（３）外部サービスに求めるサービスレベル

１０　情報セキュリティ統括責任者は、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、外部サービス提供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。

（外部サービスの利用に係る調達・契約）

第 145 条　情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

２　情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

（外部サービスの利用承認）

第 146 条　情報セキュリティ管理者は、外部サービスを利用する場合には、都市経営部デジタル戦略課長へ外部サービスの利用申請を行わなければならない。

２　都市経営部デジタル戦略課長は、前項の規定による利用申請を審査し、利用の可否を決定しなければならない。

３　都市経営部デジタル戦略課長は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、申請ごとに外部サービス管理者を指名しなければならない。

（外部サービスを利用した情報システムの導入・構築時の対策）

第 147 条　情報セキュリティ統括責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（ウ）開発時におけるセキュリティ対策
（エ）設計・設定時の誤りの防止
（オ）クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

２　外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

３　標準準拠システム等をガバメントクラウドにおいて利用する場合、クラウドサービス管理者は、前各項の規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウ

ドサービス事業者に情報を求め、実施状況を確認及び記録しなければならない。

（外部サービスを利用した情報システムの運用・保守時の対策）

第 148 条　情報セキュリティ統括責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

（ア）外部サービス利用方針の規定
（イ）外部サービス利用に必要な教育
（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）外部サービス内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）外部サービスを利用した情報システムの事業継続
（ケ）設計・設定変更時の情報や変更履歴の管理

2　外部サービス管理者は、外部サービスの運用・保守時において、情報セキュリティ対策を実施するために必要となる項目に変更が発生した場合、都市経営部デジタル戦略課長へ外部サービスの利用変更申請を行わなければならない。

3　都市経営部デジタル戦略課長は、前項の規定による利用変更申請を審査し、利用の可否を決定しなければならない。

4　外部サービス管理者は、クラウドサービス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。

5　情報セキュリティ管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

6　外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

7　標準準拠システム等をガバメントクラウドにおいて利用する場合、クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録しなければならない。

（外部サービスを利用した情報システムの更改・廃棄時の対策）

第 149 条　情報セキュリティ統括責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定しなければならない。

（ア）外部サービスの利用終了時における対策
（イ）外部サービスで取り扱った情報の廃棄
（ウ）外部サービスの利用のために作成したアカウントの廃棄

2　外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に都市経営部デジタル戦略課長へ外部サービス利用終了届の提出をしなければならない。

3　標準準拠システム等をガバメントクラウドにおいて利用する場合、クラウドサービス管理者は、情報資産を破棄する際に、データ消去の方法の一つとして、データ記録時に使用した暗号鍵を削除するなどの方法により、その情報資産を復元困難な状態としなければならない。

第４節　外部サービスの利用（重要情報を取り扱わない場合）

（外部サービスの利用に係る規定の整備）

第 150 条　情報セキュリティ統括責任者は、以下を含む外部サービス（重要情報を取り扱わない場合）の利用に関する規定を整備しなければならない。

（ア）外部サービスを利用可能な業務の範囲

（イ）外部サービスの利用申請の許可権限者と利用手続

（ウ）外部サービス管理者の指名と外部サービスの利用状況の管理

（エ）外部サービスの利用の運用手順

（外部サービスの利用承認（重要情報を取り扱わない場合））

第 151 条　情報セキュリティ管理者は、外部サービス（重要情報を取り扱わない場合に限る）を利用する場合には、都市経営部デジタル戦略課長へ外部サービスの利用申請を行わなければならない。

2　都市経営部デジタル戦略課長は、前項の規定による利用申請を審査し、利用の可否を決定しなければならない。

第９章　評価・改善、雑則

第１節　情報セキュリティ監査

（情報セキュリティ監査の実施）

第 152 条　情報セキュリティ統括責任者は、情報セキュリティ監査を実施するための実施手順を策定するものとする。

第２節　自己点検

（自己点検の実施・報告）

第 153 条　情報セキュリティ管理者は、所管する情報資産及び情報システムにおける情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行い、不備等が発見された場合は、必要な改善を図らなければならない。

２　情報セキュリティ管理者は、前項に基づく点検の結果を部等情報セキュリティ責任者及び都市経営部デジタル戦略課長に報告しなければならない。

３　都市経営部デジタル戦略課長は、有効かつ効率的な自己点検が実施されるよう、自己点検に関する様式を整備するものとする。

（自己点検結果の共有・活用）

第 154 条　都市経営部デジタル戦略課長は、情報セキュリティ管理者により実施された自己点検の結果を取りまとめ、セキュリティ会議に報告するとともに、必要に応じて、情報セキュリティポリシー及び関係規程等の見直しに活用するものとする。

第３節　是正処置

（是正処置の実施）

第 155 条　情報セキュリティ管理者は、次に掲げる事項に該当した場合、是正処置を実施しなければならない。

（１）情報セキュリティインシデントの発生により情報セキュリティ対策の不備等が検出されたとき

（２）自己点検により情報セキュリティ対策の不備等が発見されたとき

（３）情報セキュリティ監査の指摘等により、放置しておくと情報セキュリティインシデントが発生するおそれを把握したとき

（４）セキュリティ会議により、是正処置の必要性を指摘されたとき

（５）その他、情報セキュリティインシデントの発生に繋がるような事象が発見されたとき

２　情報セキュリティ管理者は、情報セキュリティインシデントの発生に基づき是正処置を実施する場合は、次に掲げる手順で行うものとする。

（１）発生した情報セキュリティインシデントの事象を正確に把握する。

（２）前号の事象に対する直接的な原因及びその原因を作り出した根幹的な原因を追及する。

（３）第１号の事象を防止するために講じる具体的な処置の計画を立てる。

（４）第１号の事象と講じる処置内容を照らし合わせ、実施の必要性及び処置内容の妥当性を評価し、実施するか否かを決定する。

３　都市経営部デジタル戦略課長は、是正処置が適切に実施されるよう、是正処置に関する様式を整備するものとする。

（是正処置の報告）

第 156 条　情報セキュリティ管理者は、前条の規定により是正処置を実施した場合は、部等情報セキュリティ責任者及び都市経営部デジタル戦略課長に報告しなければならない。

２　都市経営部デジタル戦略課長は、前項の規定により報告を受けた是正処置及び自らが実施した是正処置について、軽微なものを除き、セキュリティ会議に報告するものとする。

第４節　実施手順

（実施手順の策定）

第 157 条　情報システム管理者は、情報処理における情報セキュリティを確保するため、所管する情報システムに関する実施手順を策定する。

２　前項に規定する実施手順においては、この基準に基づき情報セキュリティ対策を具体に実施するための手順のほか、次に掲げる事項について記載しなければならない。

（１）情報システムの概要

（２）機器・ソフトウェア一覧

（３）機器・ネットワーク構成図

（４）障害・事故等発生時連絡網

３　都市経営部デジタル戦略課長は、第１項に規定する実施手順が適切に策定されるよう、実施手順の記入例等を提示するものとする。

４　情報セキュリティ管理者は、第１項に規定する実施手順のほか、情報セキュリティの管理運営について、必要に応じて実施手順を策定するものとする。

（実施手順の点検）

第 158 条　情報システム管理者及び情報セキュリティ管理者は、前条に基づき策定した実施手順の内容を、毎年度点検しなければならない。

附則

この基準は、平成 15 年８月１日から実施する。

附則

この基準は、平成 17 年 4 月 1 日から実施する。
附則
この基準は、平成 17 年 8 月 1 日から実施する。
附則
この基準は、平成 17 年 12 月 16 日から実施する。
附則
この基準は、平成 18 年 4 月 1 日から実施する。
附則
この基準は、平成 19 年 4 月 1 日から実施する。
附則
この基準は、平成 20 年 4 月 1 日から実施する。
附則
この基準は、平成 21 年 6 月 1 日から実施する。
附則
この基準は、平成 22 年 4 月 1 日から実施する。
附則
この基準は、平成 23 年 4 月 1 日から実施する。
附則
この基準は、平成 24 年 6 月 1 日から実施する。
附則
この基準は、平成 28 年 5 月 31 日から実施する
附則
この基準は、平成 31 年 4 月 1 日から実施する。
附則
この基準は、令和 2 年 3 月 1 日から実施する。
附則
この基準は、令和 2 年 10 月 1 日から実施する。
附則
この基準は、令和 3 年 9 月 30 日から実施する。
附則
この基準は、令和 4 年 9 月 30 日から実施する。
附則
この基準は、令和 5 年 4 月 1 日から実施する。
附則
この基準は、令和 5 年 8 月 31 日から実施する。
附則
この基準は、令和 7 年 9 月 1 日から実施する。
附則

この基準は、令和８年４月１日から実施する。