鹿沼市情報セキュリティ対策基準

第１章　総則

（趣旨）

第１条　本対策基準は、鹿沼市情報セキュリティ基本方針（令和４年１月１７日策定。以下「基本方針」という。）第１０条の規定に基づき、情報セキュリティに関する具体的な判断基準、遵守事項、手続等を定めるものとする。

（定義）

第２条　本対策基準において使用する用語の意義は、基本方針及び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。）において使用する用語の例による。

（適用範囲）

第３条　本対策基準は委員会の所掌に係る情報資産及び職員等に適用し、小中学校委員会の所掌に係る情報資産及び職員等に対しては適用しない。

（対策基準の位置付け）

第４条　本対策基準は、職員等が最低限実施すべき情報セキュリティ対策の基準を定めるものであり、職員等が前項の基準を超えた情報セキュリティ対策を実施することを妨げるものではない。

２　職員等は、本対策基準を理由に、現に実施し、又は実施しようとしている情報セキュリティ対策の水準を低下させてはならない。

第２章　組織体制

第１節　委員会

（委員会の構成）

第５条　委員会の構成は、次のとおりとする。

(1) 委員会は、委員長及び副委員長並びに委員をもって構成する。

(2) 委員長に副市長を、副委員長に行政経営部長を、それぞれ充てるものとする。

(3) 委員は、鹿沼市庁議規程（平成元年４月１日鹿沼市訓令第８号）第３条第４項に掲げる者（市長及び副市長並びに教育長を除く。）をもって充てるものとする。

（委員会の所掌事務）

第６条　委員会は、次に掲げる事務を所掌する。

(1) 基本方針及び本対策基準の制定、改正及び廃止に関すること。

(2) 基本方針第９条に規定する情報セキュリティ監査の実施に関すること。

(3) 個人情報の漏えい、滅失、破損等（以下「セキュリティ侵害」という。）が生じた場合における情報共有、再発防止策及び損害賠償に関すること。

(4) 職員等への研修のうち、特に重要なものの実施に関すること。

(5) 前各号に掲げるもののほか、情報セキュリティ対策の適切な実施及びセキュリティ侵害が発生した場合における対応であって、特に重要なものに関すること。

（会議）

第７条　副市長は、必要に応じて委員会の会議を招集することができる。

２　副市長は、会議に諮る案件の内容、感染症対策、緊急性等を考慮し、持ち回り、Ｗｅｂ会議、グループウェアの回覧機能等により会議を行うことができる。

３　副市長は、会議に諮る案件の適切な審議に必要があると認めるときは、委員以外の者を会議に参加させ、説明をさせ、又は意見を述べさせることができる。

４　前３項に定めるもののほか、委員会の会議に関し必要な事項は、副市長が委員会に諮り、別に定める。

第２節　職員の職責

（ＣＩＳＯの設置）

第８条　本市における全ての情報資産の管理及び情報セキュリティ対策についての最終決定権限及び責任を有する者としてＣＩＳＯを置き、副市長をもって充てる。

２　副市長は、ＣＩＳＯの権限の一部を他の職員に委任し、又は専決させることができる。

（副ＣＩＳＯの設置）

第９条　ＣＩＳＯを補佐し、当該ＣＩＳＯの命を受けて本市の情報セキュリティに関する事務を統括する者として副ＣＩＳＯを置き、行政経営部長をもって充てる。

（統括情報セキュリティ責任者の設置）

第１０条　次に掲げる権限及び責任を有する者として統括情報セキュリティ責任者を置き、デジタル政策課長をもって充てる。

⑴　ＣＩＳＯ及び副ＣＩＳＯを補佐すること。

⑵　本市の全ての情報システムにおける導入、設定、運用、見直し等について、職員等に指導し、又は指示すること。

⑶　本市の全ての情報セキュリティ対策について、職員等に指導し、又は指示すること。

⑷　本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持及び管理を行うこと。

⑸　セキュリティ侵害発生時における円滑な情報共有を図るための緊急連絡体制を整備すること。

⑹　セキュリティ侵害が発生し、又は発生するおそれがある場合において、直ちに、副ＣＩＳＯ及びＣＩＳＯに報告をするとともに、当該報告への指示に基づき、セキュリティ侵害に対する措置を講ずること。

⑺　情報セキュリティに関する規程の課題及び問題点を把握し、必要に応じてＣＩＳＯに報告すること。

⑻　クラウドサービスの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を確立すること。

（情報セキュリティ責任者の設置）

第１１条　次に掲げ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き、部長等（第５条第３号に規定する委員会の委員をいう。以下同じ。）をもって充てる。

(1) その担当する部局等における情報セキュリティ対策を統括すること。

(2) その担当する部局等が所管する情報資産における導入、設定、運用、見直し等を統括すること。

(3) その担当する部局等が所管する情報資産について、セキュリティ侵害発生時における緊急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係る意見の集約及び職員等への教育、訓練、助言及び指示を行うこと。

（情報セキュリティ管理者の設置）

第１２条　次に掲げる権限及び責任を有する者として情報セキュリティ管理者を置き、鹿沼市事務執行規則（平成５年鹿沼市規則第１号）第１０条第２号に規定する課長等をもって充てる。

(1) その担当する課等における情報セキュリティ対策の実施、見直し等に関すること。

(2) 情報セキュリティ対策の実施について、職員等への教育、訓練、助言及び指示を行うこと。

(3) その担当する課等において、セキュリティ侵害が発生し、又は発生するおそれがある場合は、直ちに、情報セキュリティ責任者、統括情報セキュリティ責任者及びＣＩＳＯに報告をするとともに、当該報告への指示に基づき、セキュリティ侵害に対する措置を講ずること。

(4) 前号の課等に所属する職員等に対し、情報セキュリティに関する教育、訓練、助言及び指示を行うこと。

(5) クラウドサービスを利用する際に、外部関係機関・事業者等との必要な連絡体制を構築すること。

２　前項に定めるもののほか、情報システムを所管する情報セキュリティ管理者は、次に掲げる権限及び責任を有するものとする。

(1) その所管する情報システムにおける導入、設定、運用、見直し等を行うこと。

(2) その所管する情報システムにおける情報セキュリティ対策の実施、見直し等に関すること。

(3) その所管する情報システムにおける情報セキュリティ実施手順書の策定及び見直しに関すること。

（取扱担当者の設置）

第１３条　情報システムの導入、設定、運用、見直し等及び情報資産の取扱いを担当する職員（第８条から前条までに規定する職員を除く。）を情報システム担当者として位置付ける。

２　情報セキュリティ管理者は、特定個人情報を取り扱う業務については、情報システム

担当者並びに当該担当者が従事する業務の範囲及び内容を明確にしておかなければならない。

（兼務の禁止）

第１４条　情報セキュリティ対策においては、次に掲げる兼務をしてはならない。ただし、職員等の配置上やむを得ない場合、緊急を要する場合等においては、この限りでない。

(1) 承認者と承認を求める者との兼務

(2) 監査者と被監査者との兼務

（ＣＳＩＲＴの設置）

第１５条　次に掲げる事務を所掌する組織として、鹿沼市ＣＳＩＲＴを設置する。

(1) 本市においてセキュリティ侵害が発生した場合における状況の把握並びに副市長、関係官公庁等への報告及び報道機関への公表を統一的かつ横断的に行うこと。

(2) セキュリティ侵害に係る応急措置及び復旧に係る指示及び助言をすること。

(3) セキュリティ侵害の発生から終息までの対処内容を記録すること。

(4) 平時において、セキュリティ侵害の予防、発生時の対応等について教育啓発を行うこと。

２　前項に定めるもののほか、ＣＳＩＲＴの組織体制、役割分担等は、別に定める。

第3章　情報資産の分類と運用

第1節　情報資産の分類及び取扱制限

第１６条　情報セキュリティ管理者は、情報資産ごとに当該情報資産に求められる機密性、完全性及び可用性の程度に関する分類（以下「程度分類」という。）を行い、程度分類に基づき必要な情報セキュリティ対策を実施するものとする。

２　機密性に関する程度分類及び分類基準は、次の表のとおりとする。

程度分類	分類基準
3	・特定個人情報及び特定個人情報を取り扱う情報資産 ・鹿沼市情報公開条例（平成９年鹿沼市条例第１５号）第６条に規定する非公開情報（この項において「非公開情報」という。）に該当することが明らかな情報資産又は非公開情報に該当するかどうかの判断が困難な情報資産
2	非公開情報に該当しないが、一般への公表を予定していない情報に該当する情報資産
1	機密性の程度分類が３及び２に該当しない情報資産

３　完全性に関する程度分類及び分類基準は、次の表のとおりとする。

程度分類	分類基準

2	その破壊、改ざん又は消去により、住民の権利が侵害され、又は行政事務の遂行に支障（軽微なものを除く。）が生ずるおそれがある情報資産
1	完全性の程度分類が２に該当しない情報資産

４　可用性に関する程度分類及び分類基準は、次の表のとおりとする。

程度分類	分類基準
2	その故障、破壊、消去等により利用が不可能となることで、行政事務の遂行に支障（軽微なものを除く。）が生ずるおそれがある情報資産
1	可用性の程度分類が２に該当しない情報資産

５　情報資産に対する取扱制限は、次のとおりとする。

(1) 機密性の程度分類が２以上の情報資産に対する取扱制限は、次のとおりとする。

ア　機密性の程度分類が３の情報資産にあっては、本市が組織的に導入したパソコン、タブレット等であって、職員等が業務において日常的に操作する端末（以下「端末」という。）以外の機器を用いた作業の禁止

イ　情報資産の複製及び目的外利用並びに外部提供の禁止

ウ　あらかじめ定められた場所以外の場所への保管及び保存の禁止

エ　情報資産を保管し、又は保存する場所への電磁的記録媒体の持込みの禁止

オ　送信、運搬等において、暗号化若しくはパスワードの設定又は施錠可能なケースへの保管をすること。

カ　信頼のできるネットワーク回線を用いて、情報資産の送受信を行うこと。

キ　本市の施設外で情報処理を行う場合において、あらかじめ安全管理措置を定めること。

ク　情報資産を記録した記録媒体を施錠可能な場所に保管し、又は保存すること。

ケ　情報資産を復元不可能な状態で廃棄すること。

(2) 完全性の程度分類が２である情報資産に対する取扱制限は、次のとおりとする。

ア　定期的なバックアップを実施すること。

イ　必要に応じて、電子署名を付与すること。

ウ　本市の施設外で情報処理を行う場合において、あらかじめ安全管理措置を定めること。

エ　情報資産を記録した記録媒体を施錠可能な場所に保管し、又は保存すること。

オ　情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じること。

(3) 可用性の程度分類が２である情報資産に対する取扱制限は、次のとおりとする。

ア　定期的なバックアップを実施すること。

イ　あらかじめ定めた時間内で、バックアップ媒体から情報資産を復元することができる仕組み及び体制を整備すること。

ウ　情報資産を記録した記録媒体を施錠可能な場所に保管し、又は保存すること。

エ　情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じること。

第２節　情報資産の運用

（情報資産の管理）

第１７条　情報セキュリティ管理者は、その所管する業務における情報資産の管理責任を有するものとする。この場合において、情報セキュリティ管理者は、その所管する業務の遂行に不必要な情報が保有されていることを確認したときは、速やかに当該情報を適切な方法で廃棄し、又は返却しなければならない。

２　情報セキュリティ管理者は、複数の情報が保管され、又は保存されている情報資産については、情報セキュリティ対策の実施に支障が生じない場合に限り、当該情報資産を１つの情報資産として程度分類を行うことができる。この場合において、当該程度分類は、それぞれ保存されている情報の中で最も程度が高いもので分類するものとする。

３　情報セキュリティ管理者は、その所管する業務において使用する情報資産の内容、用途等を常に的確に把握し、必要に応じて程度分類を変更するものとする。

４　情報セキュリティ管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報資産台帳を整備しなければならない。

５　情報セキュリティ管理者は、その所管する情報資産の一部又は全部の複製（バックアップを含む。）がされた場合は、当該複製がされた情報資産についても程度分類を行い、必要な情報セキュリティ対策を実施するものとする。

６　情報セキュリティ管理者は、特定個人情報を取り扱う業務（個人番号関係事務を含む。）については、番号法第２８条の規定による個人情報保護評価の実施義務がない場合であっても、同条第１項に規定する評価書を作成しなければならない。

７　職員等は、必要に応じて、情報資産へのラベルの貼付、フォルダ、ファイル又は文書への記載等の方法により程度分類及び取扱制限を明示するものとする。

（情報資産の入手等）

第１８条　職員等は、事務の遂行に必要のない情報資産を入手し、又は作成してはならない。

２　職員等は、情報資産の入手時又は作成時において程度分類及び必要な情報セキュリティ対策を特定しなければならない。この場合において、作成途上の情報資産についても、当該特定をした情報セキュリティ対策を実施するものとする。

（情報資産の庁内共有）

第１９条　職員等は、本市の他の課等又は業務から情報資産の提供を受けた場合は、当該情報資産の提供元が設定した程度分類に応じて、情報セキュリティ対策を実施しなければならない。ただし、情報資産の一部のみを取得したことにより、程度分類の変更が明らかに必要な場合は、この限りでない。

２　職員等は、前項本文に規定する場合において、提供元の程度分類が不明であり、又は疑義があるときは、当該程度分類について自らの所属に係る情報セキュリティ管理者の判断を仰がなければならない。

（情報資産の利用）

第２０条　職員等は、業務の遂行以外の目的で情報資産を利用してはならない。

２　職員等は、情報資産を構成する情報の変更、増減、制度改正等により程度分類の変更が必要と認める場合は、情報セキュリティ管理者の判断を仰ぎ、程度分類を変更しなければならない。

第４章　情報システムの分離等

（個人番号利用事務等を処理する情報システム）

第２１条　個人番号利用事務を処理する情報システムは、マイナンバー利用事務系に係るネットワーク上で構築し、稼働させなければならない。ただし、当該情報システムが、権限のないものによる個人番号へのアクセスを制限する仕組みを備えている場合は、この限りでない。

（マイナンバー利用事務系の分離）

第２２条　マイナンバー利用事務系は、他の情報システムと接続し、通信をさせてはならない。ただし、通信の経路、種類等が適切に限定されている場合は、この限りでない。

２　前項ただし書の規定によりマイナンバー利用事務系と接続された情報システムについても、他の情報システムと接続し、通信させてはならない。ただし、当該接続に係る通信が国等の公的機関が構築した情報システムを相手方とするもの又は無害化通信により十分に安全性が確保されたものである場合は、この限りでない。

３　マイナンバー利用事務系は、原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

４　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。

５　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、暗号化による対策を実施しなければならない。この場合において、暗号は十分な強度を持たなければならない。

６　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は、情報セキュリティ管理者はクラウドサービス事業者が提供するそれらの機能及び内容についての情報を入手し、その機能についての理解に努め、必要な措置を行わなければならない。

（ＬGWAN接続系の分離）

第２３条　ＬGWAN接続系は、インターネット接続系と接続し、通信させてはならない。ただし、無害化通信による接続は、この限りでない。

２　前項ただし書の無害化通信の方法を例示すると、おおむね次のとおりである。

⑴）インターネット接続系で受信した電子メールについて、セキュリティ侵害の要因となるおそれのある添付ファイルを隔離し、本文のみをＬGWAN接続系に転送する方法

⑵）インターネット接続系に設置された端末の画面のみを、ＬGWAN接続系の端末に送信することによりＷｅｂを閲覧する方法

⑶）インターネット接続系で取得したファイルを、コンピューターウィルス、スクリプト、マクロその他セキュリティ侵害の要因を除去する仕組みを経由して、ＬGWAN接続系に取り込む方法

３　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。

（インターネット接続系における対策）

第２４条　本市のインターネット接続系は、栃木県情報セキュリティクラウドを経由してインターネットに接続するものとする。

２　インターネット接続系においては、通信パケットの監視、ふるまい検知その他不正な通信を検出する仕組みを実装しなければならない。

３　統括情報セキュリティ責任者は、インターネット接続系でセキュリティ侵害が発生した場合において、栃木県との緊密な連携の下、迅速な対応をとることができるよう、必要な連絡網、作業手順、実施体制を整備しなければならない。

第５章　物理的セキュリティ

第１節　管理区域

（管理区域の設置）

第２５条　ネットワークの中枢となる通信機器、可用性の高いサーバー、機密性の高いデータその他重要な情報資産を設置し、運用するための区域として管理区域を置く。

２　管理区域は、次の各号に掲げる全ての要件を満たしたものでなければならない。

⑴）２階以上の階に設置されていること。

⑵）外部からの侵入を防ぐため、外壁に窓を設けないこと。

⑶）管理区域への出入口は、最小限の数とすること。

⑷）管理区域への出入口は、施錠が可能なものとすること。

⑸）停電時において非常用発電機による電源供給がなされること。

⑹）管理区域内を一定の温度に保つための空調設備が設置されていること。

⑺）地震による被害を軽減するため、免振装置が設置されていること。

⑻）機器及び電磁的記録媒体に影響のない消火設備を備えていること。

⑼）機器の転倒、落下、盗難等を防止するための措置が講じられていること。

⑽）監視カメラが設置されていること。

（入退室管理）

第２６条　職員等は、管理区域へ入室しようとするときは、あらかじめ統括情報セキュリティ責任者の承認を得なければならない。

２　職員等は、管理区域への入室及び退出について、それぞれ必要事項を入退室管理簿に記載しなければならない。この場合において、入退室管理簿への記載は、電磁的記録媒体への記録をもって替えることができる。

３　管理区域に入室しようとする職員等及び委託事業者は、身分証明書等を携帯しなければならない。この場合において、職員等及び委託事業者は、統括情報セキュリティ責任者又は情報セキュリティ管理者の求めに応じ、当該身分証明書を提示しなければならない。

４　統括情報セキュリティ責任者は、管理区域への入室時において、入室しようとする者が端末、電磁的記録媒体、カメラ、可燃物その他のセキュリティ侵害を誘引し得る物を所持していないかについて確認しなければならない。

５　統括情報セキュリティ責任者は、職員等以外の者に第１項の承認を与える場合は、必要に応じて、職員等の立会、入室時間又は立入区域の制限等の条件を付すものとする。

（搬入及び搬出）

第２７条　職員等は、管理区域にサーバー、通信機器等を搬入し、又は搬出しようとするときは、あらかじめ統括情報セキュリティ責任者の承認（以下この条において「搬入搬出承認」という。）を得なければならない。

２　統括情報セキュリティ責任者は、職員等から搬入搬出承認を求められた場合において、当該職員に対し、搬入又は搬出に係る機器の情報、他の情報システムへの影響等について報告を求めることができる。

３　統括情報セキュリティ責任者は、搬入搬出承認を与える場合において、機器の設置位置、利用する電源の場所、搬入又は搬出の経路及び手順、職員等の立会、留意事項等について条件を付すことができる。

第２節　サーバーの管理

（サーバーの設置）

第２８条　情報セキュリティ管理者は、機密性、完全性又は可用性の程度分類が２以上のサーバーを管理区域内に設置しなければならない。

２　前項の規定にかかわらず、情報セキュリティ管理者は、前項のサーバーを管理区域内に設置することについて著しい支障がある場合は、第２５条第２項に掲げる要件に準じた措置を講じた上で、統括情報セキュリティ責任者の承認を得て、当該サーバーを管理区域以外の区域に設置することができる。

３　統括情報セキュリティ責任者は、外部にサーバ等の機器を設置する場合は、ＣＩＳＯの承認を得なければならない。この場合において統括情報セキュリティ責任者は、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（サーバーの冗長性の確保）

第２９条　情報セキュリティ管理者は、完全性又は可用性の程度分類が２以上であるサーバーについては、次に掲げる措置を講じなければならない。

(1) 必要に応じて、サーバーそのものを冗長化すること。

(2) ハードディスク、ＳＳＤ等の記録領域を冗長化すること。

(3) サーバーに障害が発生した場合において迅速な復旧を可能とするため、正常稼働時におけるサーバー全体の環境をイメージ化して保存すること。

(4) 常時更新されるデータを保存するサーバーにあっては、定期的にデータをバックアップすること。

(5) サーバーの電源ユニットが故障した場合に備え、当該電源ユニットを冗長化すること。

(6) 電源喪失時にサーバーを正常にシャットダウンするための時間を確保するため、無停電電源装置を設置し、適切な設定を行うこと。

(7) 落雷等による過電流からサーバーを保護するための措置を講ずること。

第３節　通信回線の管理

（通信回線の引込み）

第３０条　情報セキュリティ管理者は、施設に通信回線を引き込もうとするときは、あらかじめ統括情報セキュリティ責任者の承認（以下「引込承認」という。）を得なければならない。

２　統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

３　統括情報セキュリティ責任者は、引込承認をするときは、外部ネットワークへの接続を最低限とする観点、外部接続のＬＧＷＡＮへの集約等について慎重に判断しなければななならない。

４　統括情報セキュリティ責任者は、引込承認をする場合において、情報セキュリティ管理者に対し、通信回線の選択、必要となる情報セキュリティ対策等について条件を付すことができる。

（通信機器の設置等）

第３１条　情報セキュリティ管理者は、ネットワークの中枢となる重要な通信機器（第４項において「中枢通信機器」という。）を、それぞれ管理区域内に設置しなければならない。

２　情報セキュリティ管理者は、施設に通信回線を引き込む場合は、当該通信回線を管理区域内において成端しなければならない。

３　情報セキュリティ管理者は、落雷等による過電流から前項の通信機器を保護するための措置を講じなければならない。

４　第２８条第２項の規定は、通信回線の成端及び中枢通信機器の設置について準用す

る。

（通信回線及び通信機器の冗長化）

第３２条　情報セキュリティ管理者は、可用性の程度分類が２である通信回線については、バックアップ回線を敷設し、冗長性を確保するよう努めるものとする。

２　情報セキュリティ管理者は、可用性の程度分類が２である通信機器については、故障時の迅速な復旧を図るため、当該通信機器の２重化、代替機の準備等の措置を講じなければならない。

（通信ケーブル等の敷設及び管理）

第３３条　情報セキュリティ管理者は、通信ケーブル、電源ケーブル等（以下「通信ケーブル等」という。）を敷設しようとするときは、これらの損傷、相互干渉等を防止するため、配線収容管内への敷設、複数の通信ケーブル等に係る離隔の確保、人の手の届かない場所への敷設等必要な措置を講じなければならない。

２　情報セキュリティ管理者は、通信ケーブル等の敷設をしたときは、当該通信ケーブル等の用途、敷設経路、種別、色等について資料を作成しなければならない。

３　施設管理者は、通信ケーブル等の敷設時、損傷等の発生時等において、情報セキュリティ管理者から情報提供、設備の利用、復旧作業等の協力を求められたときは、正当な理由なく当該協力を拒んではならない。

４　情報セキュリティ管理者は、自らが承認を与えた者以外の者が通信ケーブル等の新規敷設又は変更をすることがないよう、通信ケーブル等の管理を適切に行わなければならない。

第４節　取扱区域

（取扱区域の指定等）

第３４条　情報セキュリティ管理者は、機密性の程度分類が３に該当する情報資産（以下「機密情報」という。）を取り扱う区域（管理区域及び書庫を除く。）として、取扱区域を指定するものとする。

（取扱区域における紙文書の取扱い）

第３５条　職員等は、取扱区域において機密情報が記載された紙文書を保管するときは、施錠可能な書架、キャビネット等に保管しなければならない。

２　職員等は、情報システムへの入力、紙台帳への転記等（以下この項において「入力等」という。）のため機密情報の印刷、メモ用紙への記載等をした場合において入力等が完了したときは、直ちに当該機密情報が記録された紙を適切な方法により廃棄しなければならない。

（取扱区域における機器の取扱い）

第３６条　職員等は、取扱区域に設置されたパソコン、外付ハードディスク等の機器（次項において「機器」という。）に機密情報を保存してはならない。ただし、暗号化等の措置を講じ、かつ、情報セキュリティ管理者の承認を得た場合は、この限りでない。

２　情報セキュリティ管理者は、取扱区域において機密情報を取り扱う機器に対し、必要に応じて盗難防止の措置を講ずるものとする。

３　情報セキュリティ管理者は、取扱区域に設置するパソコンに対し、必要に応じてディスプレイに表示された情報を来庁者が覗き見ることができないよう、必要な措置を講ずるものとする。

４　情報セキュリティ管理者は、取扱区域において機密情報を印刷するプリンターを設置するときは、来庁者の手の届かない場所であって、当該プリンターの印刷物を来庁者が判読することができない場所に設置しなければならない。

第５節　情報資産の取扱い

（機器等の持出し）

第３７条　職員等は、次に掲げる情報資産を、それぞれ当該各号に定める場所から持ち出してはならない。ただし、必要な情報セキュリティ対策を講じた上で、情報セキュリティ管理者の承認を得た場合は、この限りでない。

⑴　管理区域に設置されている機器及び記録媒体　管理区域

⑵　取扱区域に設置されている機器及び記録媒体　取扱区域が置かれている施設

⑶　機密性の程度分類が２である情報が保存されている機器又は記録媒体（前２号に掲げるものを除く。）　当該機器又は記録媒体が設置されている施設

２　前項ただし書の情報セキュリティ対策を例示すると、おおむね次のとおりである。

⑴　機器又は記録媒体に必要最低限の情報のみが保存されていること。

⑵　機器又は記録媒体にパスワードの設定、暗号化等の措置が講じられていること。

⑶　機器又は記録媒体に保存された情報にパスワードの設定、暗号化等の措置が講じられていること。

⑷　機器又は記録媒体の持出し及び返却について、情報セキュリティ上必要な事項が記録されていること。

３　職員等は、機密性の程度分類が２以上である情報資産を運搬するときは、施錠可能なケースへの格納、データの暗号化等の措置を講じなければならない。

（記録媒体の保存）

第３８条　情報セキュリティ管理者は、記録媒体を保存するときは、当該記録媒体に保存された情報又はデータへの追加、修正及び削除を禁止するための措置を講じなければならない。

２　情報セキュリティ管理者は、機密性の程度分類が２以上であり、かつ、完全性又は可用性の程度分類が２である記録媒体を保存するときは、耐火、耐熱、耐水及び耐湿に係る対策を講じた施錠可能な場所に保存しなければならない。

３　情報セキュリティ管理者は、情報システムのバックアップデータを保存するときは、バックアップ元である情報資産が設置されている施設以外の施設に当該バックアップデータを保存するよう努めるものとする。

（情報資産の廃棄又は返却）

第３９条　職員等は、機密性の程度分類が２以上である情報資産が保存年限を満了したときは、情報セキュリティ管理者の承認を得て、速やかに当該情報資産を廃棄しなければならない。

２　職員等は、前項の規定による廃棄において、次に掲げる対策を実施しなければならない。

(1) 誤廃棄の防止についての対策

(2) 集積場所における盗難又は盗み見についての対策

(3) 輸送時における落下、散逸等についての対策

(4) 輸送及び廃棄に他者が関与する場合における盗難又は盗み見についての対策

(5) 日時、担当者、処理内容等の情報セキュリティ上必要な事項の記録

３　職員等は、機器又は記録媒体（以下この項において「機器等」という。）を廃棄し、又は返却しようとするときは、機器等の機密性の程度分類に応じて、あらかじめ次に掲げる対策を実施しなければならない。

(1) 機器等から情報を読み取ることができないよう、機器等を物理的に破壊すること。

(2) 前号の物理的な破壊が適切に行われたことを証するため、職員等による目視確認又は当該破壊の実施者からの証明書を徴取すること。

(3) 第１号の物理的な破壊について職員等が目視確認をすることができないときは、作業者による盗難又は盗み見を防止するため、情報が消去された機器等を作業者に引き渡すこと。

(4) 前号の規定による消去は、本市の施設内において実施し、当該消去について日時、担当者、処理内容の情報セキュリティ上必要な事項を記録すること。

４　クラウドサービス事業者が利用する装置等の廃棄をする者は、セキュリティを確保した対応となっているか、事業者の方針及び手順について確認しなければならない。なお、当該確認にあたっては、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取得している場合には、その監査報告書や認証等を利用できる。

第６章　人的セキュリティ

第１節　職員等の遵守事項

（職員等の一般的遵守事項）

第４０条　職員等は、鹿沼市情報セキュリティポリシー及び情報セキュリティ実施手順書を遵守しなければならない。

２　職員等は、情報セキュリティ対策について、不明な点、不足する点、実施が困難な点等を認めるときは、速やかに情報セキュリティ管理者に相談し、その指示を仰がなければならない。

（業務における情報資産の利用）

第４１条　職員等は、業務以外の目的で情報資産を使用してはならない。

２　職員等は、機密性の程度分類が２以上である情報を個人が所有するパソコン、通信回線、記録媒体等を用いて処理し、又は保存してはならない。ただし、必要な情報セキュリティ対策を講じた上で、情報セキュリティ管理者の承認を得た場合は、この限りでない。

３　職員等は、情報資産に対し、情報セキュリティの維持に係る設定の変更及び個人が所有する機器の接続をしてはならない。ただし、十分な検証をした上で、情報セキュリティ管理者の承認を得た場合は、この限りでない。

４　職員等は、自らが業務で使用するパソコン、記録媒体、紙文書等の情報資産が権限のない者により利用され、又は盗み見られることがないよう、適切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、第２項ただし書及び第３項ただし書の承認をした場合は、当該承認について資料を作成し、適切に保存しなければならない。

６　統括情報セキュリティ責任者は、機密性２以上かつ可用性２かつ完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

７　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

８　情報セキュリティ管理者は、支給のパソコン、モバイル端末及び電磁的記録媒体等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

（異動、退職時等の遵守事項）

第４２条　職員等は、異動、退職等により担当業務が変更となるときは、変更前の担当業務に係る情報資産に対し、次に掲げる措置を講じなければならない。

(1) 貸与を受けていた情報資産に機密性の程度分類が２以上の情報が保存されているときは、当該情報を削除すること。

(2) 貸与を受けていた情報資産を返却すること。

(3) 業務を遂行する上で個人として作成した電子ファイル又は紙文書を削除し、又は廃棄すること。

（セキュリティ侵害発生時の報告）

第４３条　職員等は、セキュリティ侵害について、発生を認め、又は業者、市民等から発生の報告を受けたときは、直ちに、その旨を情報セキュリティ管理者に報告しなければならない。

２　情報セキュリティ管理者は、前項の規定による報告を受けたときは、直ちに当該報告の内容を情報セキュリティ責任者及び統括情報セキュリティ責任者並びに関係機関に報告しなければならない。

３　情報セキュリティ責任者は、前項の規定による報告を受けた場合において当該報告の

内容が重大であると認めるときは、直ちに、その旨をＣＩＳＯに報告しなければならない。この場合において、統括情報セキュリティ責任者は、ＣＩＳＯへの報告について情報セキュリティ責任者に助言し、又は自ら報告することができる。

４　前２項の規定は、情報セキュリティ管理者又は情報セキュリティ責任者が、セキュリティ侵害について自ら発生を認め、又は業者、市民等から報告を受けた場合について準用する。

５　ＣＩＳＯは、セキュリティ侵害について、発生を認め、業者、市民等から発生の報告を受け、又は第３項の規定による報告を受けたときは、当該セキュリティ侵害の程度に応じて、個人情報保護委員会（個人情報の保護に関する法律（平成 15 年法律第 57 号）第 127 条第１項に規定するものをいう。）への報告、記者会見の開催、新聞社への情報提供その他の事実の公表に関する措置を講じなければならない。

（セキュリティ侵害発生時の対応）

第４４条　ＣＳＩＲＴは、情報システム、ネットワーク等の監視及び情報収集を行い、セキュリティ侵害の発生を迅速に把握しなければならない。

２　ＣＳＩＲＴは、セキュリティ侵害の発生を把握したときは、直ちに、その旨をＣＩＳＯ並びに当該セキュリティ侵害に関係する情報セキュリティ責任者及び情報セキュリティ管理者に報告しなければならない。

３　ＣＳＩＲＴは、セキュリティ侵害が発生したときは、当該セキュリティ侵害に関係する情報セキュリティ責任者又は情報セキュリティ管理者に対し、影響を受ける可能性のある本人への連絡、市民等への情報提供、被害の拡大防止を図るための応急措置、復旧等に係る指示をしなければならない。

４　ＣＳＩＲＴは、セキュリティ侵害の原因を明らかにするとともに、発生の経緯、被害の程度及び範囲、講じた応急措置、復旧作業の内容、再発防止策等について資料の作成及び保存をするとともに、当該資料の内容をＣＩＳＯに報告しなければならない。

５　ＣＩＳＯは、前項の規定による報告を受けたときは、当該報告の内容を確認し、再発防止策の修正、実施等について必要な指示をしなければならない。

６　ＣＩＳＯは、セキュリティ侵害による被害の程度が甚大であり、又は類似のセキュリティ侵害の発生を防止するため全庁的な措置が必要と認めるときは、第４項の規定による報告の内容（次項において「再発防止策等」という。）を委員会に報告するものとする。

７　ＣＩＳＯは、前条第５項の規定により事実の公表に関する措置を講じた場合は、必要に応じて、再発防止策等についても同項の公表に関する措置を講ずるものとする。

（情報セキュリティ管理者の責務）

第４５条　情報セキュリティ管理者は、その所管する課室等に所属する職員等に対し、情報セキュリティポリシーの意義、内容等を理解させるとともに、情報セキュリティ対策を適切に実施させなければならない。

２　情報セキュリティ管理者は、特別職非常勤職員、会計年度任用職員その他非常勤の職員（以下「非常勤職員」という。）を任用するときは、必要に応じて、非常勤職員に対し情報セキュリティポリシーの遵守に関する同意書への署名を求めるものとする。

３　情報セキュリティ管理者は、その必要性を十分に検討した上で、非常勤職員による情報システム、電子メール、インターネットへの接続、機密情報等（以下この項において「情報システム等」という。）の取扱いの承認をしなければならない。この場合において、情報セキュリティ管理者は、当該承認の対象とならない非常勤職員が、情報システム等を取り扱うことができないよう、必要な措置を講じなければならない。

４　情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び情報セキュリティ実施手順書を閲覧することができるよう、必要な措置を講じなければならない。

第２節　研修及び訓練

（職員等への研修）

第４６条　ＣＩＳＯは、定期的に、職員等に対する情報セキュリティに関する研修を行わなければならない。

２　統括情報セキュリティ責任者は、定期的に前項の研修（以下「研修」という。）に係る計画を策定し、ＣＩＳＯの承認を得なければならない。この場合において、当該計画に定める研修の内容は、それぞれ職員等の職責、役割、理解度等に応じたものとしなければならない。

３　ＣＩＳＯは、新規採用職員を対象とした研修を行わなければならない。

４　職員等は、正当な理由なく研修の受講を拒んではならない。この場合において、情報セキュリティ管理者は、その所管する課室等に所属する職員等が研修を受講することができるよう、業務分担、スケジュール等の調整をしなければならない。

（研修結果の報告）

第４７条　情報セキュリティ管理者は、その所管する課室等に所属する職員等について、研修の受講状況を把握し、統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

２　統括情報セキュリティ責任者は、定期的に、研修の受講状況について調査、分析及び評価を行い、その結果をＣＩＳＯに報告しなければならない。

３　ＣＩＳＯは、必要に応じて、前項の規定による報告の内容を委員会において周知することができるものとする。

（緊急時対応訓練）

第４８条　ＣＩＳＯは、セキュリティ侵害、システムの障害等の発生を想定した訓練（以下この条において「緊急時対応訓練」という。）について計画を定め、定期的に緊急時対応訓練を実施しなければならない。

２　前項の計画は、情報システム及びネットワークごとに規模、重要度、対象となる脅威

等を考慮するとともに、実施体制、範囲、参加者、実施項目等を定め、緊急時対応訓練が効果的に実施できるものとしなければならない。

３　第４６条第４項の規定は緊急時対応訓練への参加について、前条の規定は緊急時対応訓練結果の報告について、それぞれ準用する。

第３節　認証情報の管理

（認証用カードの取扱い）

第４９条　職員等は、自らが発行を受けた情報システム、入退室管理等において利用者を認証するためのカード（以下この項において「認証用カード」という。）について、次に掲げる事項を遵守しなければならない。

(1) 認証用カードを他人に貸し与え、利用させないこと。

(2) 認証用カードを使用しないときは、機器から取外した上で他人が利用できない状態で保管すること。

(3) 認証用カードを汚損し、破損し、又は紛失したときは、直ちに、その旨を当該認証用カードの発行者（以下この条において「発行者」という。）に報告するとともに、当該発行者の指示に従うこと。

２　発行者は、前項第３号の規定により紛失の報告を受けたときは、直ちに、当該紛失に係る認証用カードを無効化しなければならない。

３　発行者は、予備用の認証用カードを、情報システムの設定、データの未格納等により利用不可能な状態で保管しなければならない。

４　発行者は、認証用カードの汚損、破損等が発生したときは、速やかに当該認証用カードを回収し、次に掲げる措置を講じた上で廃棄しなければならない。

(1) 情報システムから、回収した認証用カードのデータを削除すること。

(2) 回収した認証用カードにデータが保存されており、かつ、当該認証用カードへのアクセスが可能な場合は、当該データを削除すること。

(3) 回収した認証用カードを破砕し、又は粉砕することによりデータの読取りを不可能な状態とすること。

（ＩＤの取扱い）

第５０条　職員等は、自らに付与されたＩＤについて、次に掲げる事項を遵守しなければならない。

(1) ＩＤを貸し与え、教えるなどして、他人に利用させないこと。

(2) 共用ＩＤについては、あらかじめ定められた共用者以外の者に利用させないこと。

（情報セキュリティ管理者によるパスワードの取扱い）

第５１条　情報セキュリティ管理者は、自らが管理する情報システムにおけるパスワードの取扱いについて、次に掲げる事項を遵守しなければならない。ただし、情報システムの機能の不足、経費面の問題等により不可能な場合は、この限りでない。

(1) 情報システムにおいて、パスワードの長さ、必ず使用すべき文字種別の数等を設定

し、パスワードの複雑性を確保すること。

(2) 仮のパスワード（初期パスワードを含む。以下同じ。）を発行した場合は、職員の初回ログオン時に、情報システムが当該仮のパスワードの変更を求めるよう設定すること。

(3) パスワードを秘密とし、本人及び他者からの照会に応じないこと。

（職員等によるパスワードの取扱い）

第５２条　職員等は、自らが利用するパスワードの取扱いについて、次に掲げる事項を遵守しなければならない。

(1) パスワードを他人に知られることのないよう、適切に管理すること。

(2) パソコン、サーバー等の端末にパスワードを記憶させることで、パスワードの入力を省略し、認証することを可能とする設定としないこと。

(3) 長さを十分なものとし、かつ、複数の文字種別を組み合わせるなどしてパスワードの複雑性を確保すること。

(4) 複数のシステムを利用する場合は、システムごとに異なるパスワードを設定するよう努めること。

(5) パスワードが流出し、又はそのおそれがあるときは、直ちに、その旨を情報セキュリティ管理者に報告するとともに、当該パスワードを変更すること。

(6)仮のパスワードは、最初のログオン時点で変更すること。

第7章　技術的セキュリティ

第1節　利用者情報の管理

（利用者の識別等）

第５３条　情報セキュリティ管理者は、ＩＤ、パスワード、カード、生体情報等により利用者を識別するための仕組みを、それぞれ端末及び情報システム（以下この条において「端末等」という。）に実装しなければならない。

２　情報セキュリティ管理者は、必要に応じて、利用者ごとに、利用可能な機能、データ、フォルダ等について、適切な権限設定が可能な仕組みを端末等に実装するものとする。

３　情報セキュリティ管理者は、マイナンバー利用事務系に係る端末等については、第１項の規定による利用者の識別をＩＤ及び生体情報を用いる方法で実装しなければならない。

４　情報セキュリティ管理者は、第１項及び第２項の仕組みを有効に活用するため、利用者の範囲、権限等を定め、端末等の利用承認、ＩＤの発行及び廃止、権限設定等を適切に行わなければならない。

（利用者ＩＤの管理）

第５４条　情報セキュリティ管理者は、情報システムの利用者ＩＤについて、あらかじめ、次に掲げる事項を定め、適切に管理しなければならない。

(1) 登録、変更、削除等に関する手続
(2) 職員等の採用、異動、出向、退職等に伴う処理の内容
(3) 情報セキュリティ管理者の職権による利用者ＩＤの停止、削除等に関する基準

（不要な利用者ＩＤの削除）

第５５条　職員等は、異動、出向、退職、事務分掌の変更等により利用者ＩＤが不要となったときは、情報システムの管理者に対し、当該利用者ＩＤの削除について通知しなければならない。

２　情報セキュリティ管理者は、不要な利用者ＩＤが放置されることがないよう、人事管理部門と連携し、定期的に利用者ＩＤの点検をしなければならない。

（管理者権限を有する利用者ＩＤの管理）

第５６条　統括情報セキュリティ責任者は、情報セキュリティ責任者が指名し、ＣＩＳＯが認めた職員等に付与する利用者ＩＤについてのみ、管理者権限を与えることができる。

２　情報セキュリティ管理者は、前項に定めるもののほか、情報システムを管理するための利用者ＩＤを作成し、管理者権限を付与することができる。この場合において、情報セキュリティ管理者は、当該利用者ＩＤのパスワードの複雑性、入力回数の制限等を通常の利用者ＩＤより高度なものとしなければならない。

３　情報セキュリティ管理者は、管理者権限を有する利用者ＩＤについて、情報システム又はネットワークへの接続回数及び接続時間を必要最小限に制限しなければならない。

４　情報セキュリティ管理者は、管理者権限を有する利用者ＩＤの数を必要最低限にするとともに、当該利用者ＩＤのパスワードが漏えいすることがないよう厳重に管理しなければならない。

５　情報セキュリティ管理者は、管理者権限を与えた利用者ＩＤのパスワード変更を業者にさせてはならない。

（認証情報の保護）

第５７条　情報セキュリティ管理者は、その所管する情報システムに係るパスワード、生体情報、暗号等の認証情報を厳重に管理しなければならない。この場合において、オペレーションシステムが認証情報を不正アクセスから保護するための機能を有している場合は、当該機能を有効化しなければならない。

２　情報セキュリティ管理者は、ＩＤ、パスワード、カード、生体情報その他認証情報の不正利用を防止するため、必要な情報セキュリティ対策を講じなければならない。

（ログオン時の表示）

第５８条　情報セキュリティ管理者は、その所管する情報システム（機密性の程度分類が３であり、かつ、完全性の程度分類が２であるものに限る。）に対し、不正アクセス、情報システムの悪用等を防止するため、次に掲げる機能を実装し、適切に設定しなければならない。

(1) 利用者のログオン時において、管理者が設定したメッセージが表示される機能

(2) ログインの試行回数が一定回数を超えた場合において、その端末からのログイン処理を自動的に停止する機能
(3) 情報システムが一定時間操作されない状態が継続した場合において、自動的に利用者をログオフさせる機能
(4) ログイン及びログアウトに係る時刻を記録し、参照することができる機能

第２節　情報システムの管理

（ファイルサーバーの設定）

第５９条　統括情報セキュリティ責任者は、ファイルサーバに対し部署ごとの容量制限を設定し、その内容を職員等に周知しなければならない。

２　統括情報セキュリティ責任者は、ファイルサーバーにおいて、部、課等の部署単位でフォルダを作成し、それぞれ部署に所属する職員等のみが当該フォルダを利用することができるよう、アクセス権を設定しなければならない。

３　統括情報セキュリティ責任者は、機密情報であって、特定の職員等のみが取り扱うべきデータについては、当該職員のみがデータを利用することができるよう、必要に応じて、当該データのみを保管するフォルダを作成し、アクセス権を設定することができる。

４　統括情報セキュリティ責任者は、第２９条第４号の規定にかかわらず、ファイルサーバーに保管されているデータを定期的にバックアップしなければならない。

（Ｗｅｂサーバーへの情報の保存）

第６０条　情報セキュリティ管理者は、Ｗｅｂサーバーをインターネットに設置する場合は、当該Ｗｅｂサーバーに個人情報、法人運営情報その他機密性の程度分類が２を超える情報を保存してはならない。

（情報システムに関する情報の公開及び取得）

第６１条　情報セキュリティ管理者は、次に掲げる行為をしようとするときは、当該行為が情報セキュリティの低下又はセキュリティ侵害の原因となることがないよう、あらかじめ、当該行為に係る範囲、情報の取扱い等を定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の承認を得なければならない。

(1) 自らが管理する情報システムに関する情報の他者への公開
(2) 他者が管理する情報システムに関する情報の取得

（情報システムの作業記録）

第６２条　情報セキュリティ管理者は、その管理する情報システムにおいて、データの一括更新、処理業者への伝送、年度切替処理その他通常運用における重要作業を実施したときは、当該重要作業の実施者、内容、結果等について作業記録を作成しなければならない。

２　情報セキュリティ管理者は、その所管する情報システムにおいて、バージョンアップ、プログラムの変更、設定の変更その他システム環境の変更に係る作業を実施したと

きは、当該作業の実施者、内容、結果等について作業記録を作成し、適切に保存しなければならない。

３　情報セキュリティ管理者は、前項の作業を実施するときは、次に掲げる事項を遵守しなければならない。

(1) あらかじめ作業内容を確認し、情報セキュリティの維持に必要な指示、助言等を行うこと。

(2) あらかじめ作業実施後に行うテスト項目を定め、作業者に当該テストの実施を命ずること。

(3) 作業は十分な技術及び経験を有する２人以上の者に実施させ、互いに作業の手順、内容等を確認させること。

(4) 作業実施後において作業の実施者、内容、結果等及びテストの実施結果を記載した作業報告書を作業者に提出させること。

（情報システムの仕様等に関する文書の管理）

第６３条　情報セキュリティ管理者は、情報システムの仕様、構成図、設定内容等を記載した文書を作成し、権限のない者による閲覧、紛失等がないよう適切に管理しなければならない。

（ログ等の保存及び分析）

第６４条　情報セキュリティ管理者は、機密性の程度分類が３であり、かつ、完全性又は可用性の程度分類が２である情報システムについて、各種ログ及び情報セキュリティの確保に必要な記録（以下この条において「ログ等」という。）を取得し、一定期間保存しなければならない。

２　情報セキュリティ管理者は、あらかじめログ等について、取得する項目、保存期間、取扱方法、取得できなくなった場合の対応等を定め、適切にログ等を管理しなければならない。

３　情報セキュリティ管理者は、必要に応じて、取得したログ等を定期的に点検し、又は分析する機能又は体制を設け、不正侵入、不正操作等の有無を把握するものとする。

４　クラウドサービス事業者が収集し、保存するログ等についても、ログ管理等に関する対策や機能に関する情報を確認し、ログ等に関する保護が実施されていることを確認しなければならない。

５　情報セキュリティ管理者は、監査及び証拠の保全及び分析に必要となるクラウドサービス事業者の環境内で生成され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。

（システム障害発生時の記録）

第６５条　情報セキュリティ管理者は、その所管する情報システムにおいてシステム障害が発生した場合は、当該障害の内容、原因、復旧策、再発防止策等を記録し、適切に保

存しなければならない。

第３節　ネットワークへの対策

（ネットワークにおける通信の制御）

第６６条　情報セキュリティ管理者は、不正アクセスを防止するため、ネットワークと他のネットワークとの接続点において、アクセス元、アクセス先、通信の種類等を制御するための仕組み（以下「アクセス制御」という。）を実装しなければならない。

２　情報セキュリティ管理者は、必要に応じて、端末とサーバーとの接続点においてもアクセス制御を実装するものとする。

３　情報セキュリティ管理者は、通信機器間において不整合が生ずることがないよう、適切にアクセス制御及びネットワーク経路の設定をしなければならない。

（市民等が利用するネットワークの分離）

第６７条　情報セキュリティ管理者は、市民、業者その他職員以外の者が利用する情報システムについては、必要に応じて、当該情報システムと他の情報システムとを遮断し、又は物理的に分離しなければならない。

（外部ネットワークとの接続手続等）

第６８条　情報セキュリティ管理者は、その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、あらかじめＣＩＳＯ及び統括情報セキュリティ責任者の承認を得なければならない。

２　情報セキュリティ管理者は、前項の承認を求める場合は、次に掲げる事項をＣＩＳＯ及び統括情報セキュリティ責任者に示さなければならない。

(1) 外部ネットワークと接続することの必要性

(2) 接続対象となる外部ネットワークの管理者、用途、利用者等

(3) 外部ネットワークとの接続に係る機器構成、情報セキュリティ対策の内容並びに当該接続に係る本市の情報システム及びネットワークの変更点等

(4) 外部ネットワークとの接続により、本市の情報システム及びネットワークに悪影響が生じないこと。

３　情報セキュリティ管理者は、接続先外部ネットワークの管理者の責に帰すべき事由により、本市の情報が漏えいし、改ざんされ、又は情報システムが停止した場合に備えるため、当該管理者との間で契約を締結し、損害賠償責任について定めなければならない。

４　情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

(1) 庁内ネットワークへの侵入を防御するために、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。

5　情報セキュリティ管理者は、接続先外部ネットワークに起因する問題により、本市の情報資産に対しセキュリティ侵害が生ずるおそれがある場合は、その旨を統括情報セキュリティ責任者に報告するとともに、直ちに外部ネットワークとの接続の停止、ネットワークからのサーバーの分離その他必要な措置を講じなければならない。

6　統括情報セキュリティ責任者は、前項の規定による報告を受けたときは、情報セキュリティ管理者に対し、情報セキュリティの維持について必要な指示をすることができる。この場合において、情報セキュリティ管理者は、正当な理由なく当該指示を拒んではならない。

（通信の暗号化）

第６９条　情報セキュリティ管理者は、次に掲げる場合には、通信の傍受、不正アクセス等を防止するため、通信を暗号化しなければならない。

(1) インターネットその他の不特定多数が接続するネットワークにおいて、個人情報、法人運営情報その他機密性の程度分類が３であり情報を送受信する情報システムを構築する場合

(2) 次条第２項の規定により無線ＬＡＮを利用する場合

（無線ＬＡＮの利用）

第７０条　情報セキュリティ管理者は、マイナンバー利用事務系において無線ＬＡＮを利用してはならない。

2　情報セキュリティ管理者は、ＬGWAN接続系又はインターネット接続系において無線ＬＡＮを利用しようとするときは、あらかじめ統括情報セキュリティ責任者の承認を得なければならない。

3　情報セキュリティ管理者は、前項の承認を得ようとする場合は、統括情報セキュリティ責任者に対し、次に掲げる事項を示さなければならない。

(1) 無線ＬＡＮの必要性

(2) 無線ＬＡＮの利用に関する範囲、接続機器、設定内容等

(3) 無線ＬＡＮの利用に関する情報セキュリティ対策

第４節　情報機器への対策

（端末及び記録媒体への対策）

第７１条　統括情報セキュリティ責任者は、特定個人情報を取り扱う端末におけるＵＳＢメモリ、外付けハードディスクその他の記録媒体へのデータの記録を禁止し、又は承認するため、システムの導入、設定等の技術的措置を講じなければならない。

2　情報セキュリティ管理者は、庁舎外に持ち出して使用する端末、記録媒体等に対し、紛失又は盗難時の情報漏えいを防止するため、パスワードの設定、データの暗号化等の措置を講ずるよう努めるものとする。

3　職員等は、個人番号が記載された紙文書を持ち運ぶ場合は、封緘、個人番号記載部分

への塗潰し又は目隠しシールの貼付その他当該個人番号の漏えいを防止するための措置を講じなければならない。

（複合機に係る情報セキュリティ対策）

第７２条　情報セキュリティ管理者は、複合機について次に掲げる情報セキュリティ対策を講じなければならない。

(1) 複合機を直接インターネット接続系に接続しないこと。

(2) 複合機の記録媒体にデータを保存しないこと。

(3) 複合機を返却し、又は廃棄する場合において、当該複合機に保存されたデータの消去、当該複合機の記録媒体の物理的破壊等を実施すること。

２　情報セキュリティ管理者は、前項に定めるもののほか、複合機に起因するセキュリティ侵害の発生を防止するため、複合機の機能及び用途に応じて必要な情報セキュリティ対策を講ずるものとする。

（ＩｏＴ機器に係る情報セキュリティ対策）

第７３条　情報セキュリティ管理者は、ＩｏＴ機器に個人情報、法人運営情報その他機密性の程度分類が３である情報を保存してはならない。

２　情報セキュリティ管理者は、前項に定めるもののほか、ＩｏＴ機器の機能及び用途に応じて必要な情報セキュリティ対策を講ずるものとする。

第５節　電子メールの取扱い

（電子メールに係る利用者の制限）

第７４条　統括情報セキュリティ責任者は、権限のない者が本市のメールサーバーを踏み台として電子メールを転送することが不可能となるよう、必要な設定をしなければならない。

２　統括情報セキュリティ責任者は、電子メールを利用できる職員、業者等について基準を定めるとともに、当該基準に従って電子メールを適切に運用しなければならない。

３　統括情報セキュリティ責任者は、次の各号に掲げる場合は、それぞれ当該各号に定める者と協議し、電子メールの取扱方法を定めなければならない。

(1) 職員以外の者に電子メールを使わせる場合　当該職員以外の者

(2) 情報システムに対し、一定の条件に合致する場合において業者に電子メールを送信する旨の設定をする場合　当該業者

（スパムメール等に係る対策）

第７５条　統括情報セキュリティ責任者は、外部から受信し、又は内部から送信されるスパムメール、迷惑メール等（次項において「スパムメール等」という。）を検知し、隔離する仕組みを実装しなければならない。

２　統括情報セキュリティ責任者は、本市のメールサーバーから外部に向けたスパムメール等の発信を認めた場合は、直ちに、電子メール送信の停止、メールサーバーの停止その他の必要な措置を講じなければならない。

（電子メールの容量制限等）

第７６条　統括情報セキュリティ責任者は、一定の容量を超えた電子メールの送受信を不可能とするため、それぞれ電子メール１件当たりの容量の上限を定め、電子メールの送受信に係る情報システムに設定しなければならない。

２　統括情報セキュリティ責任者は、保存可能な電子メールの容量を制限するため、あらかじめメールアドレスごとの保存容量の上限を定め、電子メールの受信に係る情報システムに設定しなければならない。この場合において、統括情報セキュリティ責任者は、受信した電子メールの容量が当該上限を超えた場合の対応を利用者に周知しなければならない。

（電子メール等の利用制限）

第７７条　職員等は、業務における電子メール等の利用について、次に掲げる行為をしてはならない。ただし、情報セキュリティ管理者の承認を得た場合は、この限りでない。

(1) 本市のメールアドレス以外のメールアドレスを使って電子メールの送受信を行うこと。

(2) 本市のメールアドレスを宛先として受信した電子メールを、自動転送機能により外部の電子メールアドレスに転送すること。

(3) インターネットで提供されるストレージサービスを用いてファイルを共有し、又は取得すること。

２　前項に定めるもののほか、職員等は、本市のメールアドレスについて、次に掲げる行為をしてはならない。

(1) 業務に必要のない電子メールの送受信に用いること。

(2) 業務に必要のない電子メールを受信するため、情報システム、業者等に対し、本市のメールアドレスを登録し、又は通知すること。

３　職員等は、１通の電子メールを複数の宛先に送信する場合は、受信者が当該宛先となるメールアドレスを知ることができない方法で送信しなければならない。ただし、広く公表されているメールアドレス又は行政機関のメールアドレスのみを宛先とする場合及び受信者に対し宛先となるメールアドレスを周知する必要がある場合は、この限りでない。

（電子メールの誤送信に関する報告）

第７８条　職員等は、送信すべきでない宛先に機密性の程度分類が２以上に該当する情報資産を誤送信した場合は、直ちに、その旨を情報セキュリティ管理者に報告しなければならない。

２　情報セキュリティ管理者は、前項の報告を受けたときは、第４３条第１項のセキュリティ侵害として、当該報告に係る誤送信に対応しなければならない。

（電子署名及び暗号化）

第７９条　職員等は、次に掲げる情報資産を他者に提供する場合は、あらかじめ統括情報

セキュリティ責任者が定めた電子署名、暗号化その他の情報セキュリティの確保に必要な措置を講じなければならない。

(1) 機密情報

(2) 機密性及び完全性の程度分類が２である情報資産

２　統括情報セキュリティ責任者は、前項の措置を定めるに当たり、暗号化に係る鍵、電子署名の正当性を検証するための情報又は手段等の管理及び提供方法についても定めなければならない。

第６節　職員等の遵守事項

（無許可ソフトウェアの利用禁止）

第８０条　職員等は、端末にソフトウェアをインストールしようとするときは、あらかじめ、当該端末の管理者から承認を得なければならない。

２　情報セキュリティ管理者は、その所管する課室等におけるソフトウェアの利用について、次に掲げる措置を講じなければならない。

(1) 不正コピーされたソフトウェアの利用禁止についての周知、監視、是正等

(2) ソフトウェアを利用するためのライセンスの取得数及び利用数の管理

（端末の改造等の禁止）

第８１条　職員等は、端末について、改造並びに部品の増設及び交換をしてはならない。ただし、当該端末の管理者の承認を得た場合は、この限りでない。

（ネットワーク接続の禁止）

第８２条　職員等は、端末をネットワークに接続してはならない。ただし、当該ネットワークの管理者の承認を得た場合は、この限りでない。

２　ネットワークの管理者は、前項の承認を求められた場合は、次に掲げる事項を確認し、全てに該当するときに限り、当該承認をすることができる。

(1) 端末をネットワークに接続することについて、業務上の必要性が認められること。

(2) 接続しようとする端末が本市により組織的に導入されたものであること。

(3) 前号の端末のＯＳ、ソフトウェア等がネットワーク接続に必要な要件を充足していること。

(4) 端末の接続に必要な情報セキュリティ対策が講じられていること。

（業務上必要のないＷｅｂ閲覧の禁止）

第８３条　職員等は、業務上必要のないＷｅｂを閲覧してはならない。

２　統括情報セキュリティ責任者は、職員等による業務上必要のないＷｅｂの閲覧を把握した場合は、その旨を当該職員が所属する課等の長に通知し、是正を求めなければならない。

（職員等による外部からのリモート接続の禁止）

第８４条　職員等は、外部ネットワークを経由した本市の情報システム又はネットワーク（一般に公開されている情報システムを除く。）への接続（以下「リモート接続」とい

う。）をしてはならない。ただし、統括情報セキュリティ責任者の承認を得た場合は、この限りでない。

２　統括情報セキュリティ責任者は、次の各号に掲げる全ての要件を満たす職員等についてのみ、前項ただし書の承認を与えることができる。この場合において、当該承認を与える職員の数は、必要最小限としなければならない。

(1) リモート接続について合理的な理由を有していること。

(2) リモート接続のための情報システムが本人確認に関する機能を有していること。

(3) リモート接続のための情報システム又はネットワークにおいて、通信の傍受に対する暗号化等の対策が講じられていること。

(4) リモート接続に用いる端末において、盗難、紛失等による情報漏えいを防止するための対策が講じられていること。

（持込み端末のネットワーク接続の禁止等）

第８５条　職員等は、外部から持ち込んだ端末を本市のネットワークに接続してはならない。ただし、当該ネットワークの管理者の承認を得た場合は、この限りでない。

２　前項ただし書の承認は、前項の端末が次の各号に掲げる全ての要件を満たす場合にのみすることができる。

(1) 業務の遂行に当たり、端末の持込み及びネットワークへの接続以外の方法を採用することが明らかに困難であること。

(2) コンピューターウィルスに感染していないことが明らかであること。

(3) ＯＳ、ソフトウェア等がネットワーク接続に必要な要件を充足していること。

(4) 情報の漏えい、改ざん等の要因となるソフトウェアがインストールされていないこと。

（公衆通信回線のネットワークへの接続禁止）

第８６条　職員等は、インターネット、公衆無線ＬＡＮ等の公衆通信回線を、本市の情報システム又はネットワーク（以下この項において「本市システム等」という。）に接続してはならない。ただし、統括情報セキュリティ責任者の承認を得た場合は、この限りでない。

２　前項ただし書の承認は、次の各号に掲げる全ての要件を満たす場合にのみすることができる。

(1) 無害化通信又は通信回線の暗号化がされていること。

(2) 本市システム等と公衆通信回線との接続地点において、アクセス制御がされていること。

(3) 公衆通信回線側から本市の情報システムを利用する場合は、当該情報システムにおいて　ＩＤ、パスワード、生体情報、カード等を組み合わせた多要素認証が実装されていること。

（Ｗｅｂ会議サービス利用時の対策）

第８７条　統括情報セキュリティ責任者は、Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。

２　職員等は、前項の利用手順に従い、Ｗｅｂ会議の参加者、取り扱う情報等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　職員等は、Ｗｅｂ会議を主催する場合は、会議に無関係の者が参加できないよう対策を講じなければならない。

第7節　情報システム調達時の措置

（機器等の調達に係る運用規定の整備）

第８８条　統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。

２　統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味し、機器等の納入時の確認及び検査の手続を整備しなければならない。

（機器等及び情報システムの調達）

第８９条　情報セキュリティ管理者は、情報システムの開発、導入、保守等を調達する場合は、これらに必要とされる情報セキュリティ対策に係る機能、技術的要件等を調達仕様書に明記しなければならない。

２　情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、これらの機能及び可用性を入念に調査し、情報セキュリティ上問題のない製品を調達しなければならない。

（情報システムの開発）

第９０条　情報セキュリティ管理者は、情報システムの開発をする場合は、あらかじめ機能要件、情報セキュリティ要件、作業手順、テスト項目、スケジュール等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、情報システムを開発する場合は、あらかじめ、当該開発における責任者及び作業者を特定し、アクセス権限を設定し、これらの者が使用する開発用ＩＤの管理及び開発終了後の削除を適切に行わなければならない。

３　情報セキュリティ管理者は、前項の開発用ＩＤについて、少なくとも次に掲げる措置を講じなければならない。

(1) 開発用ＩＤの利用者、有効期間及び付与する権限を最小限とすること。

(2) 必要に応じて、開発用ＩＤでログイン可能な、サーバー及び端末を限定すること。

(3) 一定の強度を有するパスワードを設定すること。

４　情報セキュリティ管理者は、本市の施設内において、情報システムの開発に使用されるハードウェア及びソフトウェアを特定し、承認しなければならない。

５　情報セキュリティ管理者は、前項のハードウェアにおいて、同項の規定による承認を得ていないソフトウェアが使用されている場合は、当該ソフトウェアの削除、使用停止等の措置を講じなければならない。

６　情報セキュリティ管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

７　情報セキュリティ管理者は、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は、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。

（情報システムにおける実行環境の分離等）

第９１条　情報セキュリティ管理者は、必要に応じて、情報システムの実行環境を次に掲げる環境に分離するものとする。

(1) 情報システムの開発環境

(2) 情報システムのテスト及び利用者の研修に用いる環境

(3) 情報システムの保守環境

(4) 業務における運用環境

２　情報セキュリティ管理者は、前項第１号から第３号までに掲げる環境から同項第４号に掲げる環境への移行に関する手順を、それぞれ開発、導入及び保守に係る計画の策定時に定めなければならない。

３　情報セキュリティ管理者は、前項の移行において、情報システムで用いる情報資産の保存を適切に行い、当該移行に伴う機密性の低下及びデータの破損を防止するとともに、当該情報システムの停止期間を最小限としなければならない。

４　情報セキュリティ管理者は、導入するシステム及びサービスの可用性が確保されていることを確認した上で、当該情報システムを導入しなければならない。

（ネットワーク上で提供される情報システムの選定）

第９２条　情報セキュリティ管理者は、他者がネットワーク上で提供する情報システムを利用する場合は、当該情報システムの機能要件のみならず、接続回線、情報資産の管理及び保守に係る体制及び力量等を十分に満たす情報システムを選定しなければならない。

２　情報セキュリティ管理者は、前項の規定による選定を行う場合は、仮に当該情報システムを構成する情報資産を本市の施設内に設置した場合において、本市が実施しなければならない情報セキュリティ対策に必要な機能、人員、技術、保守体制等を洗い出し、これらの充足の程度を判断基準として選定しなければならない。

（情報システムの導入テスト）

第９３条　情報セキュリティ管理者は、新たな情報システムを導入しようとする場合は、それぞれ次に掲げるテストを実施しなければならない。

(1) 既に本市で稼働している情報システムへの影響を確認するためのテスト

(2) 新たな情報システムにおける操作、機能、処理等に関するテスト

(3) 情報システムの導入において定めた仕様、要件等の達成状況の確認に関するテスト

２　前項第１号に掲げるテストは、新たな情報システムを同号の情報システムに接続する前に行わなければならない。

３　第１項第２号及び第３号に掲げるテストは、それぞれ本市における稼働環境とは別に疑似環境を設けて行わなければならない。

４　情報システムの開発と利用とを別の組織が行う場合における第１項第３号に掲げるテストは、当該開発及び利用に係る組織において、それぞれ行わなければならない。

５　情報セキュリティ管理者は、情報システムのテストにおいて、機密性の程度分類が２以上であるデータを用いてはならない。ただし、そのテストの目的上当該データを使うことが必要であり、かつ、十分な情報セキュリティ対策が講じられている場合は、この限りでない。

６　情報セキュリティ管理者は、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。

（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係る対策）

第９４条　情報セキュリティ管理者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

⑴　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

⑵　情報システムの基盤を管理又は制御するソフトウェアで発生したセキュリティインシデントを認知した際の対処手順

⑶　情報システムが停止した際の復旧手順

２　情報セキュリティ管理者は、利用を認めるソフトウェアについて、バージョン・サポート期限等の定期的な確認による見直しを行わなければならない。

（情報システムの導入等における資料の保存）

第９５条　情報セキュリティ管理者は、情報システムの開発、導入及び保守に関する資料（第９３条第１項に掲げるテストの結果を含む。）を整備し、適切な期間保存しなければならない。また、資料に変更又は追加がある場合には、当該内容について、事前に統括情報セキュリティ責任者に報告しなければならない。

２　情報セキュリティ管理者は、情報システムの開発をした場合は、当該情報システムに係るソースコードを前項の資料として、適切な方法で保存しなければならない。

（情報システムに係る入出力データの正確性の確保）

第９６条　情報セキュリティ管理者は、情報システムを開発し、又は導入する場合は、次に掲げる機能の実装を設計に含めなければならない。

⑴　データの入力における次に掲げる機能

ア　入力されるデータの型、範囲及び妥当性を確認する機能

イ　入力されるデータ間の整合性を確認する機能

ウ　不正な文字列の入力を拒否する機能

(2) 情報の改ざん及び漏えい又はこれらの要因となる行為を検出する機能

２　情報セキュリティ管理者は、ウェブアプリケーション及びウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(1)アプリケーション及びウェブコンテンツの提供方式等の見直し

(2)運用中のアプリケーション及びコンテンツにおける定期的な脆弱性の状況確認

３　情報セキュリティ管理者は、前項第２号において脆弱性が発覚した場合は、必要な措置を講じなければならない。

４　情報セキュリティ管理者は、第１項に規定する場合において、情報システムから出力されるデータに当該情報システムによる処理内容が適正に反映されるよう、当該情報システムを設計しなければならない。

（情報システムの修正等）

第９７条　情報セキュリティ管理者は、情報システム並びに情報システムの開発及び保守に用いるソフトウェアについて、修正、更新、パッチの適用等（以下この条において「修正等」という。）を行おうとする場合は、あらかじめ、修正等による当該情報システム及び他の情報システムへの影響について確認しなければならない。

２　情報セキュリティ管理者は、修正等をした場合は、その理由、内容、実装方法、テスト結果等について資料を整備し、適切な期間保存しなければならない。

（情報システムの導入等における検証等）

第９８条　情報セキュリティ管理者は、情報システムの導入、更新、統合等をしようとする場合は、あらかじめ、リスク管理体制の構築、移行基準の明確化、新たな業務運用体制の構築等について十分に検証し、新たな情報システムを最大限活用するために必要な措置を講じなければならない。

（情報システムについての対策の見直し）

第９９条　情報セキュリティ管理者は、情報システムについてのセキュリティ対策を適切に見直さなければならない。

２　情報セキュリティ管理者は、見直し後の措置を、統括情報セキュリティ責任者へ報告しなければならない。

第８節　不正プログラムへの対策

（システム管理者がとるべき対策）

第１００条　統括情報セキュリティ責任者は、不正プログラムへの対策として、次に掲げる措置を講じなければならない。

(1) 外部ネットワークから受信するデータに対し、本市ネットワークとの接続点において不正プログラムの検知、除去及び隔離をすること。

(2) 外部ネットワークに送信するデータに対し、本市ネットワークとの接続点において不正プログラムの検知、除去及び隔離をすること。

(3) 不正プログラムに関する情報を収集し、必要に応じて、職員等への周知、注意喚起等をすること。

(4) その管理するサーバー及び端末において、不正プログラムへの対策ソフトウェアを常時稼働させるとともに、当該対策ソフトウェア（定義ファイルを含む。次項において同じ。）を常に最新の状態に保つこと。

(5) その管理するサーバー及び端末において、開発元のサポートが終了した製品を使用しないこと。

２　情報セキュリティ管理者は、不正プログラムへの対策として、次に掲げる措置を講じなければならない。ただし、ネットワーク構成、情報システムの利用方法等により、不正プログラムによる脅威が著しく低い場合、他の方法により不正プログラムへの対策が可能な場合等は、この限りでない。

(1) 前項第４号（第３号の情報システムに係るものを除く。）及び第５号に掲げる措置

(2) 不正プログラムへの対策ソフトウェアの管理権限を一括管理するとともに、情報セキュリティ管理者が承認した最小限の職員にのみ与えること。

(3) 不正プログラムへの対策ソフトウェアの更新がネットワーク経由で実施不可能な情報システムについて、不正プログラムへの対策ソフトウェアを常時稼働させるとともに、当該対策ソフトウェアを定期的に最新の状態に保つこと。

(4) 端末等において、不正プログラムへの対策ソフトウェアによる全体確認を定期的に実施すること。

（不正プログラム対策における職員等の遵守事項）

第１０１条　職員等は、不正プログラム対策について、次に掲げる事項を遵守しなければならない。

(1) 統括情報セキュリティ責任者が周知するコンピューターウィルスに関する情報を常に確認し、必要な措置を講ずること。

(2) 端末で動作している不正プログラム対策ソフトウェアの停止及び設定変更をしてはならないこと。

(3) 電磁的記録媒体に保存されたデータ又はソフトウェアをサーバー、端末等に保存する前に、不正プログラム対策ソフトウェアにより当該電磁的記録媒体を確認すること。

(4) 端末において、定期的に、不正プログラム対策ソフトウェアによる当該端末全体の確認を行うこと。

(5) 差出人が不明であり、又は不自然なファイルが添付された電子メールを受信した場合において、当該ファイルを開かず、かつ、速やかに当該電子メールを削除すること。

(6) 電子メールにファイルを添付し、又は電子メールに添付されたファイルを情報システムに保存しようとする場合において、あらかじめ、これらのファイルに対し不正プ

ログラム対策ソフトウェアによる確認をすること。

(7) インターネット接続系から取得したファイルをＬＧＷＡＮ接続系の情報システムに保存しようとする場合は、あらかじめ無害化処理を行うこと。

(8) コンピューターウィルス等の不正プログラムに感染した場合又は感染のおそれがある場合において、情報セキュリティ実施手順書に定められた対応をとること。

（専門家の支援体制）

第１０２条　統括情報セキュリティ責任者は、本市の対策では対処することができない不正プログラムによるセキュリティ侵害が発生した場合を想定し、外部の専門家による支援を受けることができる体制を構築しなければならない。

第９節　その他の攻撃への対策

（不正アクセス対策）

第１０３条　情報セキュリティ管理者は、不正アクセス対策について、次に掲げる措置を講じなければならない。

(1) 情報システムにおいて使用しないポートを閉鎖し、又は遮断すること。

(2) サーバー、端末等において、使用しないサービス又は機能の削除又は停止をすること。

(3) Ｗｅｂページの書換えを検出し、管理者に通報する機能をＷｅｂサーバーに実装すること。

(4) ＣＳＩＲＴとの連携により、次に掲げる措置を実施することができる体制及び連絡網を構築すること。

ア　情報システムに対する不正アクセスの監視

イ　不正アクセスを検知した場合の関係者への通知

ウ　不正アクセスが発生した場合における外部窓口への迅速な連絡

エ　不正アクセスが発生した場合における迅速な対応の実施

(5)クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせること。

（外部からの攻撃への対処）

第１０４条　情報セキュリティ管理者は、サービス不能攻撃による情報システムの停止を防止するため、必要に応じて情報システムの可用性の確保に関する措置を講ずるものとする。

２　ＣＩＳＯ及び統括情報セキュリティ責任者は、外部からの情報システムへの攻撃（以下「外部攻撃」という。）を受け、又は受けるおそれがある場合は、直ちに情報システムの停止、ネットワークの遮断その他必要な措置を講じなければならない。

３　統括情報セキュリティ責任者は、平時及び前項に規定する場合において、総務省、栃木県等との連絡を密にし、外部攻撃に関する情報を収集しなければならない。

４　ＣＩＳＯ及び統括情報セキュリティ責任者は、犯罪に該当する可能性がある外部攻撃

を受けた場合は、当該外部攻撃の記録を保存するとともに、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。

（内部からの攻撃への対処）

第１０５条　情報セキュリティ管理者は、本市の施設内において職員等及び外部委託業者が使用している端末について、当該端末による本市又は外部の情報システムへの攻撃を監視しなければならない。

２　統括情報セキュリティ責任者及び情報セキュリティ管理者は、その所管する情報システムにおいて職員等又は外部委託業者による不正アクセスを検知した場合は、当該職員等が所属し、又は当該外部委託業者を監督する課室等の長に対し、その旨を通知し、適切な処処置を求めなければならない。

（標的型攻撃への対処）

第１０６条　情報セキュリティ管理者は、その所管する情報システムへの標的型攻撃による内部への侵入を防止するため、それぞれ次に掲げる措置を講じなければならない。

(1) 情報システムを利用する職員等への教育啓発

(2) 電子メールのテキスト化

(3) 電子メールの添付ファイルに対する無害化処理

(4) 内部への侵入又は攻撃を検知するための機能の実装又は体制の構築

（セキュリティ情報の収集等）

第１０７条　情報セキュリティ管理者は、サーバ、端末、通信機器等におけるセキュリティホールに関する情報を収集し、必要に応じて関係者間で共有しなければならない。この場合において、情報セキュリティ管理者は、セキュリティホールの内容、緊急度等に応じて、パッチの適用、バージョンアップ等の措置を講ずるものとする。

２　情報セキュリティ管理者は、前項に定めるもののほか、不正プログラムその他の情報セキュリティに関する情報を収集し、必要に応じて、当該情報及び対応方法を職員等に周知しなければならない。

３　情報セキュリティ管理者は、情報セキュリティに関する社会、技術等の環境変化により新たな脅威の出現を認めたときは、速やかに、当該脅威に対する情報セキュリティ対策を講じなければならない。

第８章　運用面のセキュリティ

（情報システムの監視及び保守）

第１０８条　情報セキュリティ管理者は、セキュリティ侵害の兆候を検知するため、情報システム及びサーバを常時監視しなければならない。この場合において、外部ネットワークと通信する情報システムについては、外部攻撃、不正アクセス等についても監視するものとする。

２　情報セキュリティ管理者は、情報システムのログにおいて正確な時刻を記録することができるよう、サーバー、端末、通信機器等に対し、時刻同期の設定をし、かつ利用す

るクラウド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ことを確認しなければならない。

3　統括情報セキュリティ責任者は、暗号化された通信を監視するため、必要に応じて、当該通信の複合化及び再暗号化のための機能を実装するものとする。

4　情報セキュリティ管理者は、可用性の程度分類が２であるサーバー、通信機器、システムその他の情報資産については、定期的な状態の確認、障害発生時における修理若しくは交換又はバックアップ媒体からのシステムの復元等について保守体制を構築しなければならない。

5　情報セキュリティ管理者は、前項の保守体制において、記録媒体を外部に持ち出して修理し、又は復元する場合は、あらかじめ当該記録媒体からデータを削除した上で、当該記録媒体を業者に引き渡さなければならない。この場合において、当該データの削除が不可能な場合は、情報セキュリティ管理者は、当該業者に対し、守秘義務に係る契約の締結、秘密保持体制の確認等を行わなければならない。

6　情報セキュリティ管理者は、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は、クラウドサービス事業者が提供するバックアップ機能の仕様を確認し、その仕様が本市の求める要求事項を満たすことを確認しなければならない。

7　情報セキュリティ管理者は、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又は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。

8　情報セキュリティ管理者は、クラウドサービスの利用にあたっては、必要な容量・能力が確保できる事業者を選定するものとする。この場合において、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及び能力を予測し、業務が維持できるように努めなければならない。

9　情報セキュリティ管理者は、第６４条に定める取得するログの内容について、利用するクラウドサービスが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。

（ポリシー等の遵守状況の確認等）

第１０９条　情報セキュリティ管理者は、その所管する課室等において、それぞれ情報セキュリティポリシー及び情報セキュリティ実施手順書（以下「ポリシー等」という。）の遵守状況を確認し、問題があると認める場合は、速やかにＣＩＳＯ及び統括情報セキュリティ責任者に報告しなければならない。

2　ＣＩＳＯは、前項の規定による報告を受けた場合は、速やかに適切な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、情報システムにおけるポリシー等の遵守状況を定期的に

確認し、問題を認める場合は、速やかに適切な措置を講じなければならない。

（利用状況調査）

第１１０条　統括情報セキュリティ責任者は、情報セキュリティ対策を適切に実施するため、端末及び情報システムの利用状況の調査をすることができる。この場合において、職員等は、正当な理由がなければ、当該調査を拒むことができない。

２　ＣＩＳＯ又はその委任を受けた者は、不正アクセス、不正プログラム等の調査のため、サーバー、本市の施設内において職員等又は外部委託業者が使用している端末、電磁的記録媒体、情報システムのログ等を調査することができる。

（緊急時対応計画の策定等）

第１１１条　ＣＩＳＯは、外部攻撃、第１１０条第１項の違反行為等によりセキュリティ侵害が発生し、又は発生するおそれがある場合において、情報共有、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するため、緊急時対応計画を定めなければならない。

２　ＣＩＳＯ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るとともに、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　ＣＩＳＯは、緊急時対応計画において、少なくとも次に掲げる事項を定めなければならない。

(1) 関係者の連絡先

(2) 報告に関する時期、内容、報告者及び被報告者

(3) 発生したセキュリティ侵害への措置

(4) 再発防止策の策定

(5) 自然災害、大規模な感染症等が発生した場合における情報システムの継続計画

４　職員等は、セキュリティ侵害が発生した場合は、緊急時対応計画に従って、適正に対処しなければならない。

５　ＣＩＳＯは、緊急時対応計画と危機管理部門が作成する業務継続計画との整合性を確保しなければならない。

６　ＣＩＳＯは、情報セキュリティを取り巻く社会情勢、本市の施設、組織体制及び情報システム等の変化に対応するため、定期的に緊急時対応計画を見直さなければならない。

（例外措置）

第１１２条　情報セキュリティ管理者は、行政事務を適切に遂行するため、ポリシー等に定める対策を異なる方法で実施する必要がある場合又は当該対策を実施することができない場合は、あらかじめＣＩＳＯの承認を得て、当該異なる方法により対策を実施し、又は当該対策を実施しないこと（以下この条において「例外措置」という。）ができ

る。

２　情報セキュリティ管理者は、前項の規定にかかわらず、行政事務の遂行において緊急を要するため、例外措置をとることが止むを得ない場合は、必要最小限の範囲において例外措置をとることができる。この場合において、情報セキュリティ管理者は、速やかに当該例外措置に係る内容、理由、実施期間等をＣＩＳＯに報告しなければならない。

３　ＣＩＳＯは、例外措置に係る第１項の承認及び前項の報告に関する資料を適切に保存し、定期的に例外措置に係る行政事務、対策の内容、理由等を確認しなければならない。この場合において、ＣＩＳＯは、例外措置の解除が可能であると認めたときは、その旨を当該例外措置を実施している情報セキュリティ管理者に指示しなければならない。

（法令遵守）

第１１３条　職員等は、業務の遂行において使用する情報資産を保護するため、次に掲げる法令等を遵守しなければならない。

⑴　地方公務員法（昭和２５年法律第２６１号）

⑵　著作権法（昭和４５年法律第４８号）

⑶　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）

⑷　個人情報の保護に関する法律（平成１５年法律第５７号）

⑸　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）

⑹　サイバーセキュリティ基本法（平成２６年法律第１０４号）

⑺　鹿沼市個人情報の保護に関する法律施行条例（令和５年鹿沼市条例第１５号）

⑻　前各号に掲げるもののほか、情報資産の保護に関する法令等

２　情報セキュリティ管理者は、クラウド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する場合は、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。

（職員等の報告義務）

第１１４条　職員等は、情報セキュリティポリシーに違反する行為（以下この条において「違反行為」という。）を確認した場合は、直ちに、その旨を違反者が所属する課等の長に通知しなければならない。

２　情報セキュリティ管理者は、前項の規定による通知を受けたときは、直ちに、その旨を情報セキュリティ責任者に通知するとともに、違反者に対し、違反行為の停止、データの削除、設定の変更その他情報資産を保護するための措置を命じ、又は自ら実施しなければならない。

（懲戒処分、是正命令等）

第１１５条　情報セキュリティポリシーに違反した職員等（以下この条において「違反者」という。）及び違反者の監督責任者は、当該違反の重大性、内容、理由等に応じ

て、地方公務員法の規定による懲戒処分の対象とする。

２　情報セキュリティ責任者は、違反者が前条第２項の規定による命令に従わない場合は、当該違反者が情報システム、ネットワーク等を利用することができる権利の剥奪、停止その他情報資産を保護するための措置を講ずることができる。この場合において、情報セキュリティ責任者は、速やかに、当該措置の内容をＣＩＳＯ及び当該違反者が所属する課等の長に通知しなければならない。

第９章　外部委託に係るセキュリティ

第１節　業務委託

（外部委託に係る運用規定の整備）

第１１６条　統括情報セキュリティ責任者は、業務委託に係る次の事項を規定した運用規定を整備しなければならない。

(1) 委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

(2) 委託事業者の選定基準

（業務委託実施時の対策）

第１１７条　情報セキュリティ管理者は、業務委託の実施までに次の事項を実施しなければならない。

(1) 委託する業務内容の特定

(2) 委託事業者の選定条件を含む仕様の策定

(3) 仕様に基づく委託事業者の選定

(4) 情報セキュリティ要件を明記した契約の締結

(5) 委託事業者に重要情報を提供する場合は、秘密保持契約の締結

２　情報セキュリティ管理者は、情報システムの運用、保守その他情報資産の保護が必要となる業務を外部委託する場合は、当該業務の内容に応じて、次に掲げる事項を当該外部委託の契約書に定めなければならない。

(1) ポリシー等の遵守に関すること。

(2) 個人情報漏えいを防止するための技術的安全管理措置に関する取り決め

(3) 委託業務に係る責任者、作業者及び作業内容、作業場所等に関する事項

(4) 外部委託業者が提供するサービスの品質に関する事項

(5) 外部委託業者にアクセスを許可する情報に係る種類、範囲及びアクセス方法の明確化等の、情報のライフサイクル全般での管理方法に関する事項

(6) 外部委託事業者の従業員に対する教育の実施に関する事項

(7) 外部委託業者に提供した情報の目的外利用及び外部提供の禁止に関する事項

(8) 守秘義務に関する事項

(9) 再委託の制限、手続、監督義務等に関する事項

(10) 委託業務終了時における情報資産の返還、廃棄等に関する事項

(11) 委託業務に係る定期報告及びセキュリティ侵害発生時における報告に関する事項
(12) 委託者による調査、提出要請、監査、是正、指示等に関する事項
(13) セキュリティ侵害発生時における委託者による公表に関する事項
(14) 契約違反における契約解除、損害賠償等に関する事項

（業務委託実施期間中の対策）

第１１８条　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、次の対策を実施しなければならない。

(1) 委託判断基準に従った委託事業者への重要情報の提供
(2) 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
(3) 統括情報セキュリティ管理者へ措置内容の報告
(4) 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若しくは情報の目的外利用等が発覚した場合における、契約に基づく対処の要求

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、必要に応じて、次の対策の実施を委託事業者に求めなければならない。

(1) 情報の適正な取扱いのための情報セキュリティ対策
(2) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
(3) 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又は情報の目的外利用等を認知した場合における委託業務の一次中断などの必要な措置を含む対処

（業務委託終了時の対策）

第１１９条　情報セキュリティ管理者は、業務委託の終了に際し、次の対策を実施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確認を含む検収
(2) 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

２　情報セキュリティ管理者は、業務委託の終了に際し、次の対策の実施を委託事業者に求めなければならない。

(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

（情報システムの構築を業務委託する場合の対策）

第１２０条　情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、次の対策の実施を委託事業者に求めなければならない。

(1) 情報システムのセキュリティ要件の適切な実装
(2) 情報セキュリティの観点に基づく試験の実施
(3) 情報システムの開発環境及び開発工程における情報セキュリティ対策

（情報システムの運用・保守を業務委託する場合の対策）

第１２１条　情報セキュリティ管理者は、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ための要件について、契約に基づき、委託事業者に実施を求めなければならない。

２　情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

第3節　クラウドサービスの利用

（クラウドサービスの運用規程の整備）

第１２２条　統括情報セキュリティ責任者はクラウドサービスの選定にあたっては、当該サービスで用いる情報資産の程度分類が機密性２以上の場合、次の規定を含む運用規程を整備しなくてはならない。

(1) クラウド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
(2) クラウドサービス提供者の選定基準
(3) クラウドサービス利用申請の許可権限者と利用手続
(4) 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確認

２　統括情報セキュリティ責任者は、クラウドサービスの利用について、機密性２以上の情報を取り扱う場合は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、次の規定を含む運用規程を整備しなければならない。

(1) 導入・構築段階におけるセキュリティ対策方針
　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
(2) 運用・保守段階におけるセキュリティ対策方針
　ア　クラウドサービスの利用方針の規定
　イ　クラウド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　クラウドサービス内の通信の制御

キ　設計・設定時の誤りの防止

ク　クラウドサービスを利用した情報システムの事業継続

(3) 利用終了段階におけるセキュリティ対策方針

ア　クラウドサービスの利用終了時における対策

イ　クラウドサービスで取り扱った情報の廃棄

ウ　クラウドサービスの利用のために作成したアカウントの廃棄

３　統括情報セキュリティ責任者は、機密性２以上の情報を取り扱わない場合、次の規定を含む運用規程を整備しなければならない。

(1) クラウドサービスを利用可能な業務の範囲

(2) クラウドサービスの利用申請の許可権限者と利用手続

(3) 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

(4) クラウドサービスの利用の運用手順

（クラウドサービスの選定）

第１２３条　情報セキュリティ管理者は、クラウドサービスを導入しようとする場合は、当該クラウドサービスで用いる情報資産の程度分類及び取扱制限を念頭に、前条の運用規程に従って、業務に係る影響度等を検討した上でクラウドサービスの利用・選定を検討しなければならない。

２　クラウドサービスの選定における要件は、次に掲げるとおりとする。

(1) データーセンター、サーバー等が国外に設置されていないこと。

(2) クラウドサービスが中断し、又は終了した場合において、当該クラウドサービスで使用していた情報資産を他のクラウドサービス、情報システム等に円滑に移行できること。

(3) クラウドサービスで使用する情報資産が、日本国以外の国の法令が適用される場所において閲覧され、利用され、監視され、又は保守されることがないこと。

(4) 当該クラウドサービスで処理する情報資産の程度分類に応じた情報セキュリティ対策が適切に実施されること。

(5) 外部サービス提供者がその役務内容の一部を再委託する場合は、再委託先においても、情報資産の程度分類に応じた情報セキュリティ対策が適切に実施されるとともに、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が本市に提供されること。

(6) 当該クラウドサービスに対し、情報セキュリティに関する監査が実施されており、かつ、当該監査に係る報告書の内容、認定又は認証の取得状況等から、当該クラウドサービスにおける情報セキュリティ面の信頼性が十分なものであると総合的かつ客観的に判断できること。

（クラウドサービスの利用に係る調達及び契約）

第１２４条　情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウド

サービス提供者の選定基準及び選定条件並びにクラウド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、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを確認し、契約までに統括情報セキュリティ責任者の利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。

３　情報セキュリティ管理者は、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、クラウドサービス事業者に情報を求め、本市の業務及び保有するデータへの影響について特定し、クラウドサービス事業者における脆弱性管理の手順について確認しなければならない。

４　統括情報セキュリティ責任者は、クラウドサービスの利用を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。

（クラウドサービスを利用した情報システムの導入及び構築時の対策）

第１２５条　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報資産台帳に記載し、その内容を統括情報セキュリティ責任者へ報告しなければならない。

２　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービス運用開始前までに以下の全ての実施手順を整備しなければならない。

(1) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

(2) 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する手順

ア　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

イ　クラウドサービス利用の終了手順

ウ　バックアップ及び復旧

(3) クラウドサービスを利用した情報システムの運用・監視中における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

(4) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

（クラウドサービスを利用した情報システムの運用及び保守時の対策）

第１２６条　クラウドサービス管理者は、クラウドサービスの運用・保守時に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等で修正又は変更等が発生した場合、情報資産台帳及び関連文書を更新又は修正し、統括情報セキュリティ責任者へ報告しなければならない。

２　クラウドサービス管理者は、クラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

（クラウド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１２７条　クラウドサービス管理者は、クラウドサービスの利用終了時に、第１２２条に規定する運用規程に従って、情報の廃棄等が適切に実施されたことを確認及び記録しなければならない。

第１０章　ソーシャルネットワークサービスの利用

第１２８条　職員等は、業務中にソーシャルネットワークサービス（以下この条において「ＳＮＳ」という。）を利用してはならない。ただし、本市の行政情報を組織的に発信し、又は職員間において情報を共有するものとして、情報セキュリティ管理者の承認を受けたものについては、この限りでない。

２　情報セキュリティ管理者は、情報発信に係るＳＮＳを導入しようとする場合は、次に掲げる措置を講じなければならない。

(1) 本市のアカウントによる情報発信であることを明らかにするため、次に掲げる措置を講ずること。

ア　本市のホームページに、本市が情報発信に用いるＳＮＳ及びアカウントの名称を掲載すること。

イ　本市のアカウントに係るプロフィール欄、自由記述欄その他ＳＮＳの利用者が参照可能な場所に、本市の名称、運用組織の名称等を掲載すること。

(2) 情報発信に用いるアカウント及びパスワードを適切に管理すること。

(3) 情報発信の手続、責任者、担当者等を定めること。

(4) 機密性の程度分類が２以上の情報、誤った情報、古い情報等を発信することがないよう、情報発信における操作手順、チェック体制等を定めること。

(5) 権限のない他者により、本市のＳＮＳアカウントを不正に用いて情報発信がされた場合を想定し、あらかじめ、被害を最小限に抑えるための対策、手続、周知方法等を定めること。

３　情報セキュリティ管理者は、職員等の情報共有に係るＳＮＳを導入しようとする場合は、次に掲げる措置を講じなければならない。

(1) 権限のない者がＳＮＳを利用することができないよう、適切な方法により利用者の制限を行うこと。

(2) ＳＮＳを利用する権限を失った利用者を随時把握し、直ちに当該利用者によるＳＮＳの利用を停止すること。

(3) 当該ＳＮＳが利用不可能な場合における代替措置を定めておくこと。

第１１章　評価及び見直し

（監査の実施）

第１２９条　ＣＩＳＯは、本市が保有する情報資産に対する情報セキュリティ対策の実施状況について、少なくとも毎年度１回、監査を実施しなければならない。

２　ＣＩＳＯは、前項に定めるもののほか、次に掲げる場合は、監査を実施することができる。

⑴ 本市においてセキュリティ侵害が発生した場合であって、他部署において同様のセキュリティ侵害の発生を防止するため監査の実施が必要と認めるとき。

⑵ セキュリティ侵害が発生した部署に対し、更なるセキュリティ侵害の発生を防止するため監査の実施が必要と認める場合

⑶ 他の地方公共団体、企業等において重大なセキュリティ侵害が発生した場合であって、本市においても当該セキュリティ侵害の発生を防止するため監査の実施が必要と認めるとき。

⑷ 前３号に掲げる場合のほか、本市において情報セキュリティ対策を適切に実施するため、監査の実施が必要と認めるとき。

（監査の実施体制）

第１３０条　ＣＩＳＯは、監査を実施する場合は、被監査部署に所属せず、客観的に監査を実施することができる職員のうちから、情報セキュリティ監査統括責任者を指名しなければならない。

２　情報セキュリティ監査統括責任者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

３　情報セキュリティ監査統括責任者は、監査の実施について、あらかじめ情報セキュリティ監査計画を立案し、委員会の承認を得なければならない。

４　情報セキュリティ監査統括責任者は、外部委託業者及びその下請け業者（次項において「外部委託業者等」という。）についても、監査を定期的又は必要に応じて行わなければならない。

５　被監査部署は、監査の実施及び外部委託業者等への監査に協力しなければならない。

６　クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的又は必要に応じて監査を行わなければならない。クラウドサービス事業者にその証拠の提示を求める場合、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることができる。

７　前各項に定めるもののほか、監査の実施について必要な事項は、委員会が別に定める。

（監査結果の報告及び保存）

第１３１条　情報セキュリティ監査統括責任者は、監査結果について監査結果報告書を作成し、委員会に報告しなければならない。

２　情報セキュリティ監査統括責任者は、監査において収集した資料、監査報告書等を適切に保存しなければならない。

（監査結果に基づく見直し）

第１３２条　ＣＩＳＯは、監査結果に基づき、それぞれ次に掲げる措置を講じなければならない。

⑴　指摘事項に係る情報セキュリティ管理者に対し、当該指摘事項の解消を指示すること。

⑵　指摘事項に対する措置が完了していない場合は、定期的に進捗状況の報告を指示すること。

⑶　指摘事項に係る問題又は課題が他の部署においても存在する可能性が高い場合は、当該他の部署を所管する情報セキュリティ管理者に対し、当該問題又は課題の有無を確認させること。

⑷　本市において横断的に改善が必要な事項について、統括情報セキュリティ責任者及び情報セキュリティ管理者に対し、当該改善の実施を指示すること。

２　委員会は、監査結果をポリシー等、監査の実施方法その他情報セキュリティ対策の見直しにおける基礎資料として活用しなければならない。

（自己点検の実施等）

第１３３条　情報セキュリティ責任者は、その所管する情報資産に対する情報セキュリティ対策の実施状況について、統括情報セキュリティ責任者と共同して、少なくとも毎年度１回、自己点検を実施しなければならない。

２　情報セキュリティ責任者は、自己点検の結果及び改善策について資料を作成し、ＣＩＳＯに報告するとともに、当該資料を適切に保存しなければならない。

３　情報セキュリティ責任者は、改善策に係る情報資産を所管する情報セキュリティ管理者に対し、当該改善策の実施を指示しなければならない。

４　前条第２項の規定は、情報セキュリティ責任者による自己点検の結果の活用について準用する。

（ポリシー等の見直し）

第１３４条　委員会は、監査及び自己点検の結果、新たな脅威の発生、情報セキュリティに関する状況の変化等に対し、ポリシー等の規程が十分なものであるかどうかを毎年度検証し、必要に応じて、ポリシー等の見直しを行うものとする。

第１２章　補則

第１３５条　本対策基準に定めるもののほか、情報セキュリティ対策の実施に関し必要な事項は、委員会が別に定める。

附　則

この対策基準は、令和４年４月１日から施行する。

附　則

この対策基準は、令和５年４月１日から施行する。

附　則

この対策基準は、令和８年４月１日から施行する。