【別紙　6】

羽生市情報セキュリティポリシー

平成１５年１０月１０日　策　　定
平成２０年１０月２０日　全部改定
平成２３年　４月２１日　一部改定
平成３０年　７月　９日　全部改定

羽生市

この情報セキュリティポリシーは、情報セキュリティ対策について総合的かつ具体的に取りまとめたものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

【目　　次】

Ⅰ　情報セキュリティ基本方針

1　目的

この基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2　定義

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

(2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

(5) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(6) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

3　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 人による脅威（故意）

不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 人による脅威（過失）

情報の管理不備、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、外部委託管理の不備等の非意図的要因による情報資産の漏えい・破壊・消去等

(3) 災害による脅威

地震、落雷、火災、水害等の災害によるサービス及び業務の停止、情報資産の消失等

(4) 必要資源の不足、故障等による脅威

電力供給・通信・水道供給の途絶等のインフラ障害からの波及、大規模・広範囲にわたる疾病の蔓延による要員不足に伴うシステム運用の機能不全等

4　適用範囲

(1) 行政機関の範囲

この基本方針が適用される行政機関は、市長部局、行政委員会、議会事務局及び消防本部とする。

(2) 情報資産の範囲

この基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

5　職員等の遵守義務

職員、非常勤職員及び臨時職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(5) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6) 運用面におけるセキュリティ

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じ情報セキュリティ監査及び自己点検を実施する。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直し及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

上記６，７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

１０　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

Ⅱ　情報セキュリティ対策基準

１　対象範囲

(1) 行政機関の範囲

この対策基準が適用される行政機関は、市長部局、行政委員会、議会事務局及び消防本部とする。

(2) 情報資産の範囲

この基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

２　組織体制

(1) 組織の構成員と役割

組織・役職名	対象者・構成員	役割・権限等
最高情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）	副市長	1 本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。 2 CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。
統括情報セキュリティ責任者	企画財務部長	1 CISO を補佐する。 2 本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 3 本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。 4 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て、情報セキュリティに関する指導及び助言を行う権限を有する。 5 本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。 6 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策定及び維持・管理を行う権限及び責任を有する。 7 緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。 8 緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければばらない。

情報セキュリティ責任者	各部局長、 行政委員会事務局の長	1 所管する部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。 2 所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。 3 所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。
情報セキュリティ管理者	各課室の長、 出先機関の長	1 所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。 2 情報セキュリティ責任者の指示に従い、所管する対象資産に係る情報セキュリティ実施手順の策定及び更新を行う。 3 所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 4 所管する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、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 へ速やかに報告を行い、指示を仰がなければならない。
情報セキュリティ部会	副市長、 企画財務部長、 各部局の長、 総務課長、 財政課長、 企画課長	本市の情報セキュリティ対策を統一的に行うため、リスク情報の共有、情報セキュリティポリシーの決定等、情報セキュリティに関する重要な事項を決定する。

(2) 兼務の禁止

① 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

② 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

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

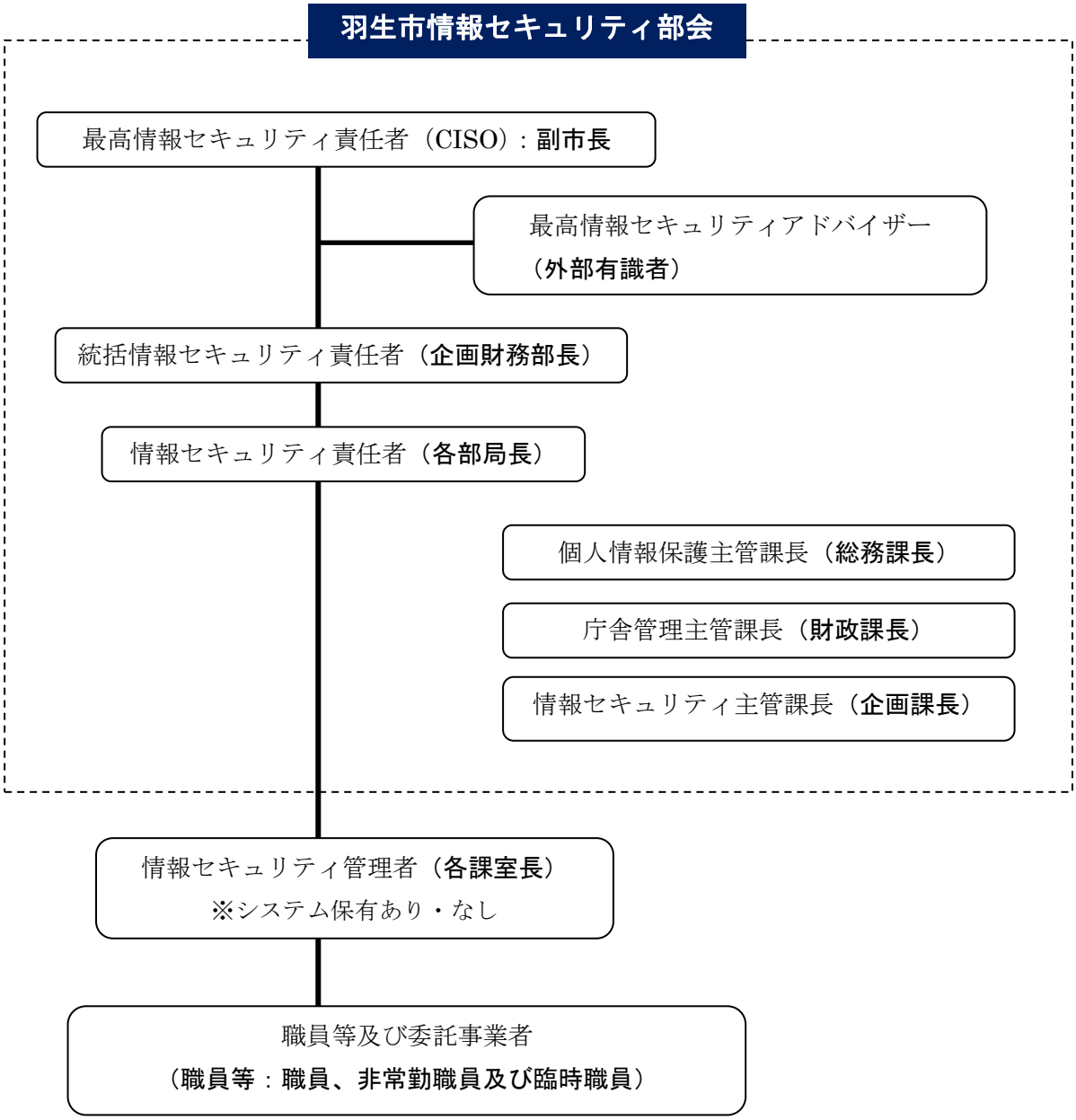
① CISO は、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

② CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

③ 情報セキュリティインシデントを認知した場合には、その重要性や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

④ 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におけるCSIRT の機能を有する部署、外部の事業者等との情報共有を行う。

【組織体制図】



3　情報資産の分類と管理

(1) 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性3	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	分類２に掲げる対策の他、以下に掲げる事項 ・暗号化又はパスワード設定 特定個人情報（個人番号を含む個人情報）においては、上記に掲げる対策のほか、以下に掲げる事項 ・法令で定める以外の事務での取扱いの禁止 ・インターネットに接続したコンピュータへの作成・保管・複製の禁止
機密性2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	・許可された者以外による閲覧の制限 ・必要以上の複製及び配布禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・適切なネットワーク回線の選択 ・電磁的記録媒体の施錠可能な場所への保管
機密性1	上記以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・許可された者以外による編集の制限 ・バックアップの作成・保管 ・電磁的記録媒体の施錠可能な場所への保管
完全性1	上記以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性2	行政事務で取り扱う情報資産のうち、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、住民の権利が侵害される、又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップの作成・保管及び相当時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性1	上記以外の情報資産	

(2) 情報資産の管理

① 管理責任

(ｱ) 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。

(ｲ) 情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき、管理しなければならない。

② 情報の作成及び消去

(ｱ) 職員等は、業務上必要のない情報を作成してはならない。

(ｲ) 情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

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

③ 情報資産の入手

自己以外の者が作成した情報資産を入手した者は、（１）の分類に基づいた取扱いをしなければならない。

④ 情報資産の利用

(ｱ) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(ｲ) 情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

(ｳ) 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑤ 情報資産の保管

(ｱ) 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

(ｲ) 情報セキュリティ管理者は、電磁的記録媒体を使用して情報資産を長期保存する場合は、書込禁止の措置を講じなければならない。

(ｳ) 情報セキュリティ管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑥ 情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑦ 情報資産の運搬

(ｱ) 車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(ｲ) 機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑧　情報資産の提供・公表

(ｱ) 機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

(ｲ) 機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

(ｳ) 情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑨　情報資産の廃棄

(ｱ) 機密性２以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

(ｲ) 情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

４　物理的セキュリティ

(1) サーバ等の管理

①　機器の取付け

情報セキュリティ管理者は、サーバの機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

②　サーバの冗長化

情報セキュリティ管理者は、所有するサーバに格納している情報の重要性、可用性、停止することによる業務への影響度等を勘案し、必要に応じて冗長化を施し、サービスや業務を停止させないよう努めなければならない。

③　機器の電源

(ｱ) 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、所有するサーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を可能な限り備え付けなければならない。

(ｲ) 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、所有するサーバ等の機器を保護するための措置を講じなければならない。

④　通信ケーブル等の配線

(ｱ) 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、施設管理部門と連携し、所管する通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

(ｲ) 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、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

(ｳ) 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、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

(ｴ) 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、自ら又は操作を認めた者以外の者が、配線を変更、追加できないように必要な措置を施さなければならない。

⑤ 機器の定期保守及び修理

(ｱ) 情報セキュリティ管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

(ｲ) 情報セキュリティ管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報セキュリティ管理者は、外部の業者に故障を修理させるにあたり、修理を委託する事業者との間で守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

⑥ 庁外への機器の設置

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、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、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。

⑦ 機器の廃棄等

情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

(2) 管理区域（電算室等）の管理

① 管理区域の構造等

(ｱ) 管理区域とは、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(以下「電算室」という。）や電磁的記録媒体の保管庫をいう。

(ｲ) 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、施設管理部門と連携して、可能な限り管理区域を地階又は１階に設けてはならない。また、外部からの侵入が容易にできないようにしなければならない。

(ｳ) 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、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

(ｴ) 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、電算室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

(ｵ) 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、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

② 管理区域の入退室管理等

(ｱ) 情報セキュリティ管理者は、管理区域への入退室を許可された者のみに制限し、IC カ

ード又は入退室管理簿の記載による入退室管理を行わなければならない。

(ｲ) 職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

(ｳ) 情報セキュリティ管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等を付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

③ 機器等の搬入出

(ｱ) 情報セキュリティ管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託した業者に確認を行わせなければならない。

(ｲ) 情報セキュリティ管理者は、管理区域の機器等の搬入出について、職員等を立ち会わせなければならない。

(3) 通信回線及び通信回線装置の管理

① 統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

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、行政系のネットワークを総合行政ネットワーク(LGWAN)に集約するように努めなければならない。

④ 統括情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

⑤ 統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑥ 統括情報セキュリティ責任者は、可用性２以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

(4) 職員等のパソコン等の管理

① 情報セキュリティ管理者は、執務室等のパソコン等の端末について、盗難による情報資産の流出を防止するため、ワイヤーによる固定等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

② 情報セキュリティ管理者は、その所有するパソコン等の端末及び情報システムを使用するためには、IC カード、パスワード又はその他の認証方法を組み合わせた複数の認証が必要となるよう設定しなければならない。

５　人的セキュリティ

(1) 職員等の遵守事項

① 職員等の遵守事項

(ｱ) 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

(ｲ) 業務以外の目的での使用の禁止

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

(ｳ) モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

a　職員等は、本市のパソコン、モバイル端末、電磁的記録媒体、情報資産及びソフトウェア等を外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

b　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

c　職員等は、外部で情報処理作業を行う際、本市が管理する以外のパソコンを用いる場合には、情報セキュリティ管理者の許可を得た上で、情報セキュリティ責任者が定めた実施手順を遵守しなければならない。また、機密性３の情報資産については、本市が管理する以外のパソコンによる情報処理を行ってはならない。

(ｴ) 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の業務利用

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原則業務に利用してはならない。ただし、業務上必要な場合で、情報セキュリティ管理者の許可を得た場合はこの限りでない。

(ｵ) 持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末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。

(ｶ) パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

(ｷ) 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を実施しなければならない。

(ｸ) 退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、業務を離れた後も、業務上知り得た情報を漏らしてはならない。

② 非常勤職員及び臨時職員への対応

(ｱ) 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤職員及び臨時職員に対し採用時に情報セキュリティポリシー等のうち、非常勤職員及び臨時職員が守るべき内容を理解させ、また、実施及び遵守させなければならない。

(ｲ) インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤職員及び臨時職員にパソコン等の端末による作業を行わせる場合は、企画課長に申請しなければならない。

③ 情報セキュリティポリシー等の掲示

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実施手順を閲覧できるように掲示しなければならない。

④ 外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(2) 研修・訓練

CISOは、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。また、職員等は、定められた研修・訓練に参加しなければならない。

① 研修計画の立案及び実施

(ｱ) CISOは、全ての職員等に対する情報セキュリティに関する研修計画を定期的に立案し、情報セキュリティ部会の承認を得なければならない。

(ｲ) 研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

(ｳ) 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

(ｴ) 研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

(ｵ) CISOは、情報セキュリティ部会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

② 緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、かつ、効果的に実施できるようにしなければならない。

(3) 情報セキュリティインシデントの報告

① 庁内からの情報セキュリティインシデントの報告

(ｱ) 職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者に報告しなければならない。

(ｲ) 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者及びCSIRT に報告しなければならない。また、必要に応じて、CISO にも報告しなければならない。

② 住民等外部からの情報セキュリティインシデントの報告

(ｱ) 職員等は、本市が管理するネットワーク及び情報システム等の情報資産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た場合、情報セキュリティ管理者に報告しなければならない。

(ｲ) 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者及びCSIRT に報告しなければならない。また、必要に応じて、CISO にも報告しなければならない。

③ 情報セキュリティインシデント原因の究明・記録、再発防止等

(ｱ) 統括情報セキュリティ責任者は、情報セキュリティインシデントが発生した部門の情報セキュリティ管理者及びCSIRT と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

(ｲ) CISO は、統括情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

(4) ID 及びパスワード等の管理

① IC カード等の取扱い

(ｱ) 職員等は、自己の管理するIC カード等に関し、次の事項を遵守しなければならない。

a 認証に用いるIC カード等を、職員等間で共有してはならない。

b IC カード等を紛失した場合には、速やかに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通報し、指示に従わなければならない。

(ｲ) 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、IC カード等の紛失等の通報があり次第、当該IC カード等を使用したアクセス等を速やかに停止しなければならない。

(ｳ) 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、IC カードを切り替える場合、切替え前のカードを回収し、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。

② ID の取扱い

職員等は、自己の管理するID に関し、次の事項を遵守しなければならない。

(ｱ) 自己が管理しているID は、他人に利用させてはならない。

(ｲ) 共用ID を利用する場合は、共用ID の利用を許可された者以外に利用させてはならない。

③ パスワードの取扱い

職員等は、自己の管理するパスワードに関し次の事項を遵守しなければならない。

(ｱ) 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。

(ｲ) パスワードは秘密にし、パスワードの照会等には一切応じてはならない。

(ｳ) パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

(ｴ) パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

(ｵ) パスワードは定期的に変更し、古いパスワードを再利用してはならない。

(ｶ) 複数の情報システムを扱う職員等は、同一のパスワードを異なる情報システム間で用いてはならない。

(ｷ) 仮のパスワードは、最初のログイン時点で変更しなければならない。

(ｸ) パソコン等の端末にパスワードを記憶させてはならない。

(ｹ) 職員等間でパスワードを共有してはならない。

６　技術的セキュリティ

(1) コンピュータ及びネットワークの管理

① 文書サーバの設定等

(ｱ) 企画課長は、職員等が使用できる文書サーバの容量を設定しなければならない。

(ｲ) 企画課長は、文書サーバを課室等の単位で構成し、職員等が他課室等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。

(ｳ) 企画課長は、住民の個人情報、人事記録等、特定の職員等のみ取扱えるデータについて、アクセス権限をつける等の措置を講じ、同一課室等であっても、担当者以外の職員等が閲覧及び使用できないようにしなければならない。

② バックアップの実施

情報セキュリティ管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

③ 他団体との情報システムに関する情報等の交換

情報セキュリティ管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、必要に応じてその取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者の許可を得なければならない。

④ システム管理記録及び作業の確認

(ｱ) 情報セキュリティ管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

(ｲ) 情報セキュリティ管理者は、所管する情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

(ｳ) 情報セキュリティ管理者は、所管するシステムにおいて、システム変更等の作業を行う場合は、必要に応じて2名以上で作業させ、互いにその作業を確認させなければならない。

⑤　情報システム仕様書等の管理

情報セキュリティ管理者は、所管する情報システムのネットワーク構成図、情報システム仕様書等について、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。

⑥　ログの取得等

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

(ｲ) 情報セキュリティ管理者は、ログ等が窃取、消去又は改ざんされることがないように適切にログを管理しなければならない。

(ｳ) 情報セキュリティ管理者は、所管する情報システムから自動出力したログ等について、必要に応じ、電磁的記録媒体にバックアップしなければならない。

⑦　障害記録

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、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

⑧　ネットワークの接続制御、経路制御等

(ｱ) 統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

(ｲ) 統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑨　外部の者が利用できるシステムの分離等

情報セキュリティ管理者は、所管する情報システムにおいて、電子申請の汎用受付システム等外部の者が利用できる場合、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑩　外部ネットワークとの接続制限等

(ｱ) 情報セキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

(ｲ) 情報セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

(ｳ) 情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

(ｴ) 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、ウェブサーバ等をインターネットに公開する場合、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しなければならない。

(ｵ) 情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認め

られ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑪　複合機のセキュリティ管理

(ｱ) 統括情報セキュリティ責任者は、プリンタ・ファクシミリ・イメージスキャナ・コピー機等の機能が一つにまとめられている機器（以下「複合機」という。）を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

(ｲ) 統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

(ｳ) 統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

⑫　無線LAN 及びネットワークの盗聴対策

(ｱ) 情報セキュリティ責任者は、無線LAN を利用するときは、統括情報セキュリティ責任者の許可を得なければならない。

(ｲ) 統括情報セキュリティ責任者は、無線LAN の利用を認める場合、情報の破壊、盗聴、改ざん、消去等が生じないよう暗号化及び認証技術、その他の十分なセキュリティ対策の実施を義務づけなければならない。

⑬　電子メールのセキュリティ管理

(ｱ) 統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

(ｲ) 統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

(ｳ) 統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

(ｴ) 統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑭　電子メールの利用制限

(ｱ) 職員等は、自動転送機能を用いて、電子メールを転送してはならない。

(ｲ) 職員等は、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。

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

(ｴ) 職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

(ｵ) 職員等は、ウェブで利用できるフリーメールを使用してはならない。

(ｶ) 職員等は、業務上必要な場合を除きウェブで利用できるネットワークストレージサー

ビス等を使用してはならない。

⑮　電子署名・暗号化

職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、暗号化又はパスワード設定等の適切なセキュリティ対策を実施して送信しなければならない。

⑯　無許可ソフトウェアの導入等の禁止

(ｱ) 職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

(ｲ) 職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者はソフトウェアのライセンスを管理しなければならない。

(ｳ) 職員等は、不正にコピー、改ざん等されたソフトウェアを利用してはならない。

⑰　機器構成の変更の制限

(ｱ) 職員等は、パソコン、モバイル端末及びネットワーク機器に対し機器の改造、増設及び交換を行ってはならない。ただし、業務上の必要がある場合は、統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者の許可を得て、これを行うことができる。

⑱　無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

⑲　業務以外の目的でのウェブ閲覧の禁止

(ｱ) 職員等は、業務以外の目的でウェブを閲覧してはならない。

(ｲ) 統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

(2) アクセス制御

①　アクセス制御等

(ｱ) アクセス制御

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は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

(ｲ) 利用者ID の取扱い

a　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は、所管する情報システムに係る利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ID の取扱い等の方法を定めなければならない。

b　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、当該情報システムを所管する情報セキュリティ管理者に報告しなければならない。

c　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は、所管する情報システ

ムについて、利用されていないID が放置されないよう、人事管理部門と連携し、点検しなければならない。

(ｳ) 特権を付与されたID の管理等

a　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、所管する情報システムに係る管理者権限等の特権を付与されたID を利用する者を必要最小限にし、当該ID のパスワードの漏えい等が発生しないよう、当該ID 及びパスワードを厳重に管理しなければならない。

b　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管理者特権を代行する者は、統括情報セキュリティ責任者若しくは情報セキュリティ管理者が指名し、CISO が認めた者でなければならない。

c　CISO は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、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通知しなければならない。

d　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、特権を付与されたID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

e　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、特権を付与されたID を初期設定以外のものに変更しなければならない。

② 職員等による外部からのアクセス等の制限

(ｱ) 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者の許可を得なければならない。

(ｲ) 統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

(ｳ) 統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

(ｴ) 統括情報セキュリティ責任者は、外部からのアクセスを認める場合、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。

(ｵ) 統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者は、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

(ｶ) 職員等は、持ち込んだ又は外部から持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

③ 自動識別の設定

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、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるよう努めるものとする。

④ ログイン時の表示等

情報セキュリティ管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、

アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

⑤　パスワードに関する情報の管理

(ｱ) 統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

(ｲ) 統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

⑥　特権による接続時間の制限

情報システムを所管する情報セキュリティ管理者は、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。

(3) システム開発、導入、保守等

①　情報システムの調達

(ｱ) 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

(ｲ) 統括情報セキュリティ責任者及び情報システムを所管する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しなければならない。

②　情報システムの開発

(ｱ) システム開発における責任者及び作業者の特定

情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。

(ｲ) システム開発における責任者、作業者のID の管理

ｱ　情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するID を管理し、開発完了後、開発用ID を削除しなければならない。

ｲ　情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

(ｳ) システム開発に用いるハードウェア及びソフトウェアの管理

ｱ　情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

ｲ　情報システムを所管する情報セキュリティ管理者は、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システムから削除しなければならない。

③　情報システムの導入

(ｱ) 開発環境と運用環境の分離及び移行手順の明確化

ｱ　情報システムを所管する情報セキュリティ管理者は、システムの開発・保守並びにテスト環境及びシステム運用環境を分離しなければならない。

ｲ　情報システムを所管する情報セキュリティ管理者は、システムの開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

ｳ　情報システムを所管する情報セキュリティ管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

ｴ　情報システムを所管する情報セキュリティ管理者は、導入するシステムや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導入しなければならない。

(ｲ) テスト

ｱ　情報システムを所管する情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

ｲ　情報システムを所管する情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

ｳ　情報システムを所管する情報セキュリティ管理者は、個人情報及び機密性の高いデータを、テストデータに使用してはならない。

ｴ　情報システムを所管する情報セキュリティ管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

④　システム開発・保守に関連する資料等の整備・保管

(ｱ) 情報システムを所管する情報セキュリティ管理者は、システムの開発・保守に関連する資料及びシステム関連文書を適切な方法で整備・保管しなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

(ｳ) 情報システムを所管する情報セキュリティ管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

⑤　情報システムにおける入出力データの正確性の確保

(ｱ) 情報システムを所管する情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能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。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、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しなければならない。

(ｳ) 情報システムを所管する情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

⑥　情報システムの変更管理

情報システムを所管する情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

⑦　開発・保守用のソフトウェアの更新等

情報システムを所管する情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

⑧　システム更新又は統合時の検証等

情報システムを所管する情報セキュリティ管理者は、システム更新・統合等に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

(4) 不正プログラム対策

①　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

(ｱ) 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

(ｲ) 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

(ｳ) コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

(ｴ) 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

(ｵ) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

(ｶ) 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

(ｷ) 業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

②　情報セキュリティ管理者の措置事項

情報システムを所管する情報セキュリティ管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

(ｱ) 所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

(ｲ) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

(ｳ) 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

③　職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

(ｱ) パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

(ｲ) 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

(ｳ) 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、速やかに削除しなければならない。

(ｴ) 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

(ｵ) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

(ｶ) 統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

(ｷ) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

ｱ　パソコン等の端末の場合

LAN ケーブルの即時取り外しを行わなければならない。

ｲ　モバイル端末の場合

直ちに端末の利用を中止し、通信を行わない設定への変更を行わなければならない。

④　専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム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。

(5) 不正アクセス対策

①　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

(ｱ) 使用されていないポートを閉鎖しなければならない。

(ｲ) 不要なサービスについて、機能を削除又は停止しなければならない。

(ｳ) 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出するよう設定しなければならない。

(ｴ) 統括情報セキュリティ責任者は、CSIRT と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

②　攻撃の予告

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

③　記録の保存

CISO及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、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。

④　内部からの攻撃

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

⑤　職員等による不正アクセス

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

⑥　サービス不能攻撃

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

⑦　標的型攻撃

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

(6) セキュリティ情報の収集

①　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

②　不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

③　情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7　運用面におけるセキュリティ

(1) 情報システムの監視

① 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

② 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる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及び情報システムを所管する情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。

(2) 情報セキュリティポリシーの遵守状況の確認

① 遵守状況の確認及び対処

(ｱ) 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、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、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。

(ｲ) CISO は、発生した問題について、適切かつ速やかに対処しなければならない。

(ｳ) 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

② パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO 及びCISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体のログ、電子メールの送受信記録等の利用状況を調査することができる。

③ 職員等の報告義務

(ｱ) 職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに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報告を行わなければならない。

(ｲ) 違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合は、適切に対処しなければならない。

(3) 侵害時の対応

① 緊急時対応計画の策定

CISO 又は情報セキュリティ部会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

② 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

(ｱ) 関係者の連絡先

(ｲ) 発生した事案に係る報告すべき事項

(ｳ) 発生した事案への対応措置

(ｴ) 再発防止措置の策定

③ 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ部会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

④ 緊急時対応計画の見直し

CISO 又は情報セキュリティ部会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

(4) 例外措置

① 例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係規定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、CISO の許可を得て、例外措置を取ることができる。

② 緊急時の例外措置

情報セキュリティ管理者は、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CISO に報告しなければならない。

③ 例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適切に保管しなければならない。

(5) 法令遵守

職員等は、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、次の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 個人情報の保護に関する法律（平成１５年法律第５７号）

⑤ 行政手続き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）

⑥ 羽生市個人情報保護条例（平成１３年条例第３号）

(6) 懲戒処分等

① 懲戒処分

情報セキュリティポリシーに違反した職員等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。

② 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

(ｱ) 統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

(ｳ) 情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止又は剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止又は剥奪した旨をCISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

8 外部サービスの利用

(1) 外部委託

① 外部委託事業者の選定基準

(ｱ) 情報セキュリティ管理者は、外部委託事業者の選定にあたり、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。

(ｲ) 情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

(ｳ) 情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

② 契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・外部委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・外部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
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等

・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

③　確認・措置等

情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、②の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCISO に報告しなければならない。

(2) 約款による外部サービスの利用

①　約款による外部サービスの利用に係る規定の整備

情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性２以上の情報が取り扱われないように既定しなければならない。

(ｱ) 約款によるサービスの利用可能な範囲
(ｲ) 業務により利用する約款による外部サービス
(ｳ) 利用手続及び運用手順

②　約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

(3) ソーシャルメディアサービスの利用

①　情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めるなど、情報セキュリティ対策を講じることとする。

(ｱ) 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市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己記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。
(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

②　機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

③　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

９　評価・見直し

(1) 監査

① 実施方法

情報セキュリティ部会は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行わせなければならない。

② 監査を行う者の要件

(ｱ) 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

(ｲ) 監査を行う者は、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 監査実施計画の立案及び実施への協力

(ｱ) 情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ部会の承認を得なければならない。

(ｲ) 被監査部門は、監査の実施に協力しなければならない。

④ 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

⑤ 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ部会に報告する。

⑥ 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

⑦ 監査結果への対応

CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

⑧ 情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ部会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

(2) 自己点検

① 実施方法

(ｱ) 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、所管するネットワーク及び情報システムについて、定期的に又は必要に応じ自己点検を実施しなければならない。

(ｲ) 情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局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、定期的又は必要に応じ自己点検を行わなければならない。

② 報告

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は、自己点検結果及び自己点検結果に基づく改善策を取りまとめ、情報セキュリティ部会に報告しなければならない。

③ 自己点検結果の活用

(ｱ) 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

(ｲ) 情報セキュリティ部会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

(3) 情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ部会は、情報セキュリティポリシー監査、自己点検の結果及び情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。