

野々市町情報セキュリティに関する規程

目次

- 第1章 総則（第1条－第3条）
- 第2章 情報セキュリティ基本方針（第4条・第5条）
- 第3章 情報セキュリティ対策基準
 - 第1節 組織体制（第6条－第14条）
 - 第2節 情報資産の分類方法及び管理方法（第15条－第24条）
 - 第3節 物理的セキュリティ対策（第25条－第35条）
 - 第4節 人的セキュリティ対策（第36条－第55条）
 - 第5節 技術的セキュリティ対策（第56条－第92条）
 - 第6節 運用面におけるセキュリティ対策（第93条－第104条）
 - 第7節 知的財産権の管理（第105条）
 - 第8節 評価、見直し等（第106条－第114条）
- 第4章 雑則（第115条）
- 附則

第1章 総則

（趣旨）

第1条 この規程は、本町が保有する情報資産の機密性（利用を許可された者だけが情報の閲覧、更新等を行うことができることをいう。以下同じ。）、完全性（情報源が明らかで、かつ、処理方法が正確になされている状態を完全に維持することをいう。以下同じ。）及び可用性（利用を許可された者が必要なときに情報の閲覧、更新等を行うことができることをいう。以下同じ。）を維持することに関し、必要な事項を定めるものとする。

（定義）

第2条 この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

- （1）個人情報 野々市町個人情報保護条例（平成11年野々市町条例第23号）第2条第1号に規定する個人情報をいう。
- （2）ネットワーク 情報機器（コンピュータ、プリンタ、サーバ、通信制御装置等の機器をいう。以下同じ。）を相互に接続するための通信網並びに当該通信網に接続している情報機器及び記録媒体で構成し情報処理を行う仕組みをいう。
- （3）情報システム 情報機器、ソフトウェア、ネットワーク及び記録媒体で構成されるものであって、これら全体で情報処理を行う仕組みをいう。
- （4）情報系ネットワーク インターネット、総合行政ネットワークシステム、文書管理システム、財務会計システム等を扱うネットワークをいう。
- （5）基幹系ネットワーク 住民情報、税情報、福祉情報等を扱うネットワークをいう。
- （6）電子データ 電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することが

できない方式で作られた記録をいう。以下同じ。)のうち、コンピュータによる処理が可能な状態で記録されているものをいう。

(7) 情報資産 次に掲げるものをいう。

ア ネットワーク及び情報システム並びにこれらに係る機器及び設備

イ 情報システムの設計図書、ネットワーク構成図等(以下「システム関連文書」という。)

ウ 職員等(第3条に規定する職員等をいう。)が業務上作成し、又は取得した電子データ

(8) 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。

(9) セキュリティ障害 次に掲げる事由による情報資産の漏えい、改ざん、消去等により、業務が停止することをいう。

ア 不正アクセス(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)第3条第2項に規定する不正アクセス行為をいう。以下同じ。)、不正プログラム等による情報資産への攻撃又は妨害

イ 情報資産の破壊又は盗難

ウ 情報システムの欠陥又は故障

エ 地震、落雷、火災等の災害

オ この規程その他の遵守すべき事項の違反行為

(不正プログラム:コンピュータウイルス、スパイウェア等のコンピュータに対して意図的に悪影響を及ぼすように作られたプログラム又はソフトウェアのこと。)

(適用範囲)

第3条 この規程は、本町の職員等(特別職に属する職員(常勤の者に限る。)、嘱託職員、臨時に雇用される職員及び労働者派遣契約(事業所等が労働者派遣をすることを約する契約をいう。以下同じ。))により派遣されている者を含み、小学校及び中学校の県費負担教職員を除く。以下同じ。)に適用する。

第2章 情報セキュリティ基本方針

(情報セキュリティ対策等の実施)

第4条 情報セキュリティの維持及びセキュリティ障害の発生を防止するため、組織体制の整備、情報資産の分類及び管理並びに次に掲げる対策(以下「情報セキュリティ対策」という。)を実施する。

(1) 物理的セキュリティ対策 ネットワーク及び情報システムに係る情報機器の設置環境等において必要な措置を講ずること。

(2) 人的セキュリティ対策 職員等及び事業者(情報機器、ソフトウェア等の販売、保守又は改修、通信網の整備、電子データの情報処理等を業務として営む者をいう。以下同じ。)の行動及び作業の制限並びに職員等を対象とする研修及び緊急時に対応するための訓練を実施すること。

(3) 技術的セキュリティ対策 ネットワーク、情報システム等の利用環境の制限、不正アクセスの防止及び不正プログラムの感染防止のための技術的な措置を講ずること。

(4) 運用面におけるセキュリティ対策 情報セキュリティ実施手順(情報セキュリティ対策を実施するための手順をいう。以下同じ。)及び緊急時の対応計画の策定並びに情報システムの利用状況

の監視、コンピュータの利用状況の調査及びこの規程の遵守状況の確認等を実施すること。

(監査及び自己点検の実施)

第5条 情報セキュリティ対策、情報セキュリティ実施手順及びこの規程の遵守状況を検証するため、定期的に又は必要に応じ、監査及び自己点検を実施する。

第3章 情報セキュリティ対策基準

第1節 組織体制

(組織体制)

第6条 本町に、最高情報統括責任者、情報セキュリティ統括責任者、情報セキュリティ総括管理者、情報システム管理者、情報セキュリティ管理者及び情報セキュリティ担当者並びに情報セキュリティ委員会を置く。

(最高情報統括責任者)

第7条 最高情報統括責任者は、副町長をもって充てる。

2 最高情報統括責任者は、本町におけるすべての情報セキュリティ対策に関する最終決定権及び責任を有する。

(情報セキュリティ統括責任者)

第8条 情報セキュリティ統括責任者は、総務部長をもって充てる。

2 情報セキュリティ統括責任者は、最高情報統括責任者を補佐し、情報セキュリティ総括管理者を指導し、及び監督する責任を有する。

(情報セキュリティ総括管理者)

第9条 情報セキュリティ総括管理者は、住民生活部長をもって充てる。

2 情報セキュリティ総括管理者は、本町のすべてのネットワークにおける開発、構築、設定変更、運用、見直し等及び情報セキュリティ対策に関する権限並びに責任を有する。

3 情報セキュリティ総括管理者は、情報システム管理者、情報セキュリティ管理者及び情報セキュリティ担当者に対して、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。

4 情報セキュリティ総括管理者は、セキュリティ障害が発生した場合又は発生するおそれがある場合は、最高情報統括責任者及び情報セキュリティ統括責任者の指示に従い、必要かつ十分な措置を行う権限及び責任を有する。

(情報システム管理者)

第10条 情報システム管理者は、広報情報課長をもって充てる。

2 情報システム管理者は、情報セキュリティ総括管理者の指示に基づき、複数の課に共通する情報資産管理並びに情報セキュリティ実施手順の策定及び管理を行う権限及び責任を有する。

(情報セキュリティ管理者)

第11条 情報セキュリティ管理者は、課長をもって充てる。

2 情報セキュリティ管理者は、次に掲げる事項に関する権限及び責任を有する。

(1) 所管する情報資産の管理

(2) 所管する情報資産の情報セキュリティ対策

(3) 所管する情報システムの開発、構築、設定変更、運用、見直し等

(4) 所管する情報資産に係る情報セキュリティ実施手順の策定及び管理

3 情報セキュリティ管理者は、所管する情報資産に係るセキュリティ障害が発生した場合又は発生するおそれがある場合には、速やかに情報セキュリティ総括管理者に報告し、指示を仰がなければならない。

(情報セキュリティ担当者)

第12条 情報セキュリティ担当者は、文書取扱主任（野々市町処務規程（平成10年野々市町規程第1号）第13条第1項に規定する文書取扱主任をいう。）をもって充てる。

2 情報セキュリティ担当者は、情報システム管理者及び情報セキュリティ管理者の指示に従い、所管する情報システムの開発、構築、設定変更、運用、更新等の作業を行うものとする。

3 情報セキュリティ担当者は、情報セキュリティ管理者の指示に基づき、情報セキュリティ対策を実施する責任を有する。

4 情報セキュリティ担当者は、セキュリティ障害が発生した場合に情報セキュリティ管理者へ報告する責任を有する。

5 情報セキュリティ担当者は、セキュリティ障害が発生した場合には、情報セキュリティ総括管理者及び情報セキュリティ管理者の指示に従い、当該セキュリティ障害への対応を行わなければならない。

(情報セキュリティ委員会)

第13条 情報セキュリティ委員会は、情報セキュリティ対策に関する研修計画、監査計画、緊急時対応計画等の重要な事項について調査、審議及び決定を行う。

2 情報セキュリティ委員会は、副町長、部長及び広報情報課長をもって組織する。

(兼務の禁止)

第14条 情報セキュリティ対策の実施において、許可又は承認の申請を行う者は、やむを得ない場合を除き、許可者又は承認者と兼ねることができない。

2 監査を受ける者は、やむを得ない場合を除き、監査を実施する者と兼ねることができない。

第2節 情報資産の分類方法及び管理方法

(情報資産の分類等)

第15条 職員等は、情報資産を次のとおり分類しなければならない。この場合において、他の課から取得した情報資産の分類は、当該他の課による分類を引き継ぐものとする。

分類	重要度	分類基準	取扱制限
S	最重要	セキュリティ障害が発生した場合に市民の生命又は生活への重大な不利益等極めて重大な影響が広範囲に及ぶ情報資産	(1) 複製及び配布の制限又は禁止 (2) 保管場所の制限 (3) 外部記録媒体（記録媒体のうち、情報機器に取付け及び取外しをすることができるものをいう。以下同じ。）等の持出し及び持込みの禁止
A	重要	非公開の情報資産及びセキュリティ障害が発生した場合に複数の課の業務に影響が及ぶ情報資産	(4) 復元不可能な処理による廃棄 (5) 信頼することができる通信回線を選択 (6) 外部で情報処理を行う場合の安全管理措置の規定 (7) 定期的なバックアップの取得
B	標準	公開することができる情報資産のうち、セキュリティ障害が発生した場合に単一の課の業務に影響が及ぶ情報資産	
C	軽易	分類SからBまでの情報資産以外の情報資産	

2 職員等は、分類S及びAの情報資産（以下「重要情報資産」という。）には、その表面、電子データの名前その他見やすい場所にその分類を表示しなければならない。

（バックアップ：コンピュータ、サーバ等に保存されている電子データの複製を別の外部記録媒体に保存すること。）

（重要情報資産の取扱制限）

第16条 職員等は、重要情報資産を取り扱う場合には、必要に応じ、前条第1項の表に定める取扱制限を行わなければならない。

（重要情報資産を取り扱う職員の範囲）

第17条 情報セキュリティ管理者は、重要情報資産を取り扱うことができる職員等の範囲を定めなければならない。

（記録媒体の取扱い）

第18条 職員等は、分類が異なる情報資産が複数記録されている記録媒体を取り扱う場合には、当該情報資産のうち最も重要度の高い分類のものの取扱いに基づき行わなければならない。

(重要情報資産の複製)

第19条 職員等は、重要情報資産を複製する場合には、情報セキュリティ管理者の許可を受けなければならない。

(重要情報資産の提供)

第20条 職員等は、他の課又は外部に重要情報資産を提供する場合には、情報セキュリティ管理者の許可を受けなければならない。

2 職員等は、外部に重要情報資産を提供する場合には、守秘義務を明記した契約を締結しなければならない。

3 職員等は、外部に重要情報資産を提供する場合には、必要に応じ、暗号化又はパスワードの設定その他情報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。

(暗号化：第三者による情報資産の盗聴又は改ざんを防ぐために、決まった規則に従って電子データを変換すること。)

(重要情報資産の運搬)

第21条 職員等は、重要情報資産を運搬する場合には、情報セキュリティ管理者の許可を受けなければならない。

2 職員等は、重要情報資産を運搬する場合には、必要に応じ、暗号化又はパスワードの設定、^{かぎ}鍵付きの入れ物への格納その他情報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。

(情報資産の保管)

第22条 職員等は、情報資産を記録した外部記録媒体を長期間保管する場合には、当該外部記録媒体に情報の書込みを禁止するための措置を講じなければならない。

2 職員等は、重要情報資産を記録した外部記録媒体を保管する場合には、耐火、耐熱、耐水及び耐湿の構造を有し、かつ、施錠することができる場所に保管しなければならない。

(情報資産の公開)

第23条 情報システム管理者及び情報セキュリティ管理者は、情報資産を公開する場合には、当該情報資産の完全性を確保しなければならない。

(情報資産の廃棄)

第24条 職員等は、情報資産を廃棄する場合には、情報セキュリティ管理者の許可を受けなければならない。

2 前項の規定にかかわらず、職員等は、重要情報資産を廃棄する場合には、情報セキュリティ総括管理者及び情報セキュリティ管理者の許可を受けなければならない。

3 職員等は、情報資産を廃棄する場合には、当該情報資産を他に利用されるおそれのない方法により処分しなければならない。

4 前項の場合において、廃棄する情報資産が重要情報資産を記録した外部記録媒体、コンピュータ、サーバ等であるときは、職員等は、重要情報資産廃棄記録簿（様式第1号）に記録した上で、当該

重要情報資産の電磁的記録が残らないよう、当該外部記録媒体、コンピュータ、サーバ等を確実に破壊しなければならない。

第3節 物理的セキュリティ対策

(サーバ等の設置環境)

第25条 サーバその他重要な情報機器（以下「サーバ等」という。）は、原則として、電算室（野々市町庁舎管理規則（平成16年野々市町規則第39号）に規定する電算室をいう。以下同じ。）に設置しなければならない。ただし、やむを得ず電算室以外の場所に設置する場合には、火災、水害、ほこり、電界、磁界、振動、温度、湿度等の影響を受けにくい場所に設置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、サーバ等を設置する場合には、サーバ等の盗難を防止するため、容易に取外しができないよう固定する等必要な措置を講じなければならない。

(サーバ等の二重化)

第26条 情報システム管理者及び情報セキュリティ管理者は、重要情報資産を記録している基幹サーバ等を二重化、ミラーリング等により同一情報を保持するよう努めなければならない。

2 情報システム管理者及び情報セキュリティ管理者は、メインサーバに障害が発生した場合には、速やかにバックアップサーバを起動し、情報システムの運用停止時間を最小限度にするよう努めなければならない。

（基幹サーバ：住民情報、税情報、福祉情報等業務の基幹となる情報を記録しているサーバのこと。）

（ミラーリング：電子データの複製を別の場所にリアルタイムに保存すること。）

（メインサーバ：二重化されたサーバにおいて、通常使用するサーバのこと。）

（バックアップサーバ：メインサーバに障害が発生した場合に備えるための予備用のサーバのこと。）

(サーバ等の電源)

第27条 情報システム管理者及び情報セキュリティ管理者は、サーバ等を設置する場合には、施設の管理者と連携し、次に掲げる措置を講じなければならない。

(1) 停電等により電源供給が停止したときにサーバ等が適切に停止するまでに必要となる電力を供給する予備電源を備え付けること。

(2) 落雷等による過電流からサーバ等を保護するための措置

(通信ケーブル等の管理)

第28条 情報システム管理者及び情報セキュリティ管理者は、施設の管理者と連携し、情報機器に係る通信ケーブル及び電源ケーブルが損傷等を受けないため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、主要な箇所の通信ケーブル及び電源ケーブルの損傷等の有無について、定期的に点検を行わなければならない。

3 情報システム管理者は、第三者がネットワーク接続口にコンピュータを容易に接続することがで

きないよう、ネットワーク接続口を適切に管理しなければならない。

- 4 情報システム管理者は、情報システム管理者又は情報システム管理者が認めた事業者以外の者が配線の変更及び追加をする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。

(サーバ等の保守及び修理)

第29条 情報システム管理者及び情報セキュリティ管理者は、重要情報資産を記録しているサーバ等の継続的な運用を確保するため、当該サーバ等の保守及び管理を行わなければならない。

- 2 情報システム管理者及び情報セキュリティ管理者は、事業者が情報資産を記録しているサーバ等を修理させる場合には、原則として、当該情報資産を消去した状態で修理させなければならない。ただし、当該情報資産を消去することができない場合には、修理する事業者と守秘義務を明記した契約を締結し、秘密保持体制の確認をしたときに限り、当該情報資産を消去しない状態で修理させることができるものとする。

(庁舎外へのサーバ等の設置)

第30条 情報システム管理者及び情報セキュリティ管理者は、庁舎外にサーバ等を設置する場合には、最高情報統括責任者の承認を得なければならない。

- 2 庁舎外に設置したサーバ等の情報セキュリティ対策については、当該サーバ等を情報システム管理者又は情報セキュリティ管理者の責任において定期的に確認しなければならない。

(電算室の管理)

第31条 電算室におけるすべての管理は、情報システム管理者がその権限及び責任を有する。

- 2 電算室には、第三者に電算室の場所が容易に認識することができるような表示をしてはならない。
- 3 電算室に設置する出入口は1箇所のみとし、当該出入口には鍵、警報装置等により電算室への入室を許可されていない者の入室を防止するための措置を講じなければならない。
- 4 電算室は、出入口以外から容易に入室することができないよう外壁等に囲まれた構造にしなければならない。
- 5 電算室内の情報機器等は、耐震対策を講じた場所に設置するとともに、防火措置等を講じなければならない。
- 6 電算室内のサーバ等の配置は、緊急時に職員等が円滑に避難することができるよう配慮しなければならない。
- 7 電算室を囲む外壁等に開口部が設けられている場合には、それをすべてふさがなければならない。
- 8 電算室に備え付ける消火装置に用いる消火剤は、情報機器に影響を与えるものであってはならない。

(電算室の入退室管理)

第32条 情報システム管理者は、電算室の入退室を管理するため、次に掲げる事項を定めなければならない。

- (1) 入室を常に許可する者の範囲
- (2) 入室を一時的に許可する者の範囲
- (3) 入室を一時的に許可する方法

- 2 情報システム管理者は、電子鍵^{かぎ}により入室を管理する情報システム及び入退室管理簿により、厳重に電算室への入退室を管理しなければならない。
- 3 情報システム管理者は、職員等以外の者が電算室に入室する場合には、その者に身分証明書等を携帯するよう求めなければならない。この場合において、身分証明書等を携帯していないときは、電算室への入室を許可しないことができるものとする。
- 4 情報システム管理者は、電算室への入室を一時的に許可された者が電算室に入室する場合には、電算室への入室を常に許可された職員等を同行させ、その入室する者を監視させなければならない。
- 5 情報システム管理者は、電算室への入室を常に許可された職員等以外の者に対して、電算室に入室する場合及び電算室から退室する場合に入退室管理簿に用件を記入するよう求めなければならない。

(情報機器の搬出入)

第33条 情報システム管理者は、電算室において情報機器の搬出入を行う場合には、電算室への入室を常に許可された職員等を立ち合わせなければならない。

(通信回線及び通信回線装置の管理)

第34条 情報システム管理者は、施設管理者と連携し、庁舎内の通信回線及び通信回線装置（以下「回線等」という。）を適切に管理しなければならない。

- 2 情報システム管理者は、外部ネットワークへの接続を必要最低限に限定しなければならない。
- 3 情報システム管理者は、ネットワークに使用する回線等について、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、送受信される情報の暗号化等の十分な措置を講じなければならない。
- 4 情報システム管理者は、重要情報資産を取り扱う情報システムに回線等を接続する場合には、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対して必要なセキュリティ水準を検討させ、当該セキュリティ水準に適合するよう適切な回線等を選択しなければならない。

(コンピュータ等の接続等)

第35条 情報セキュリティ管理者は、コンピュータ、プリンタ、スキャナ等（以下「コンピュータ等」という。）を新たにネットワークに接続し、又はネットワークに接続しているコンピュータ等を更新する必要がある場合には、情報システム管理者と協議の上、コンピュータ等接続（更新）申請書（様式第2号）を情報セキュリティ総括管理者に提出し、許可を得なければならない。

- 2 情報セキュリティ管理者は、コンピュータ等を設置する場合には、当該コンピュータ等に表示された情報及び出力された情報が当該情報を利用する職員等以外の者にのぞき見られないよう配慮しなければならない。

第4節 人的セキュリティ対策

(職員等の遵守事項)

第36条 職員等は、情報資産を提供し、及び公開してはならない。ただし、提供し、又は公開する

ことが常態であるもの、提供し、又は公開すべきものその他これらに類するものについては、この限りでない。

- 2 職員等は、コンピュータにソフトウェアをインストールしてはならない。ただし、業務上インストールすることが必要な場合において、ソフトウェアインストール申請書（様式第3号）を情報セキュリティ総括管理者に提出し、許可を得たときは、この限りでない。
- 3 職員等は、不正に複製したソフトウェアその他これに類するものを利用してはならない。
- 4 職員等は、コンピュータにインストールされている不正プログラム対策ソフトウェア（不正プログラムの検知、除去等を行うソフトウェアをいう。以下同じ。）の設定を変更してはならない。
- 5 職員等は、外部から取得した電子データをコンピュータに取り入れる場合には、不正プログラム対策ソフトウェアを用いて不正プログラムの有無を確認しなければならない。
- 6 職員等は、電子メールにおいて、差出人が不明なもの又は不審なファイルが添付されているものを受信した場合には、速やかに削除しなければならない。

（目的外利用の禁止）

第37条 職員等は、業務目的以外で情報資産の外部への持出し並びに情報システム、電子メール及びインターネットの利用をしてはならない。

- 2 情報セキュリティ総括責任者は、前項に規定する目的外利用を発見した場合には、目的外利用をした職員等が所属する課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。

（重要情報資産の庁舎外への持出し及び外部における情報処理作業の制限）

第38条 情報セキュリティ総括責任者は、重要情報資産を庁舎外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。

- 2 職員等は、庁舎外に重要情報資産を持ち出す場合又は庁舎外で重要情報資産を用いて情報処理作業を行う場合には、当該重要情報資産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。

（重要情報資産の持出し及び持込みの記録）

第39条 情報セキュリティ管理者は、所管する重要情報資産の持出し又は持込みがあった場合には、重要情報資産持出し（持込み）記録簿（様式第4号）を作成し、保管しなければならない。

（私有コンピュータの庁舎内への持込み及び利用）

第40条 職員等は、庁舎内に私有のコンピュータを持ち込み、当該コンピュータをネットワークに接続してはならない。

- 2 職員等は、いかなる場合においても、私有のコンピュータを利用して業務を行ってはならない。

（セキュリティ機能の設定変更の禁止）

第41条 職員等は、情報システム管理者が設定したコンピュータに係るセキュリティ機能の設定を変更してはならない。

(コンピュータの管理)

第42条 職員等は、コンピュータ及び記録媒体を第三者に利用され、又は閲覧されることがないように、離席時のコンピュータの停止、情報システムからのログアウト、パスワードで保護したスクリーンセーバーの設定等必要な措置を講じなければならない。

(退職時等の遵守事項)

第43条 職員等は、異動、退職等により業務を離れる場合には、当該業務において利用していた情報資産を返却しなければならない。

(嘱託職員等に関する特例)

第44条 情報セキュリティ管理者は、嘱託職員等（職員等のうち嘱託職員、臨時に雇用される職員及び労働者派遣契約により派遣されている者をいう。以下同じ。）を採用した場合には、採用時に当該嘱託職員等に対して、この規程のうち嘱託職員等が遵守すべき事項を理解させ、及び実行させなければならない。

2 情報セキュリティ管理者は、嘱託職員等を採用した場合において、必要と認めるときは、この規程を遵守する旨の書面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、原則として、嘱託職員等に情報資産、電子メール及びインターネットを利用させてはならない。ただし、情報システム管理者と協議の上、嘱託職員等に係る情報資産等利用申請書（様式第5号）を情報セキュリティ総括管理者に提出し、許可を得た場合は、この限りでない。

(業務委託に関する管理)

第45条 情報セキュリティ管理者は、事業者の情報システムの構築等又は個人情報の情報処理等の業務を委託（リース、レンタル等の契約による業務の依頼を含む。以下同じ）する場合には、当該委託に係る情報資産の保護に関し、情報システム管理者と協議しなければならない。この場合において、情報システム管理者は、情報セキュリティ管理者に当該事業者の情報セキュリティに関する体制等を調査させなければならない。

2 情報システム管理者及び情報セキュリティ管理者は、事業者の情報システムの構築の業務を委託する場合には、委託に係る契約書に次に掲げる事項を明記しなければならない。

(1) 業務上知り得た情報の守秘義務に関する事項

(2) 再委託の禁止又は制限に関する事項

(3) 知的財産権の保護に関する事項

(4) 情報資産の目的外利用並びに第三者への提供及び提示の禁止に関する事項

(5) 事故発生時における報告義務に関する事項

(6) 情報資産の複写及び複製の禁止に関する事項

(7) 情報資産保護の状況の検査の実施に関する事項

(8) 契約事項に違反した場合における契約解除、損害賠償等に関する事項

3 情報システム管理者及び情報セキュリティ管理者は、事業者の情報システムの管理、保守等の業務を委託する場合には、委託に係る契約書に次に掲げる事項を明記しなければならない。

(1) この規程及び情報セキュリティ実施手順に基づき、事業者に遵守を求める事項

- (2) 責任者、作業者及び作業場所の特定に関する事項
- (3) 従業員に対する情報セキュリティに関する教育の実施に関する事項
- (4) 事業者に対して提供した情報の目的外利用並びに第三者への提供及び提示の禁止に関する事項
- (5) 業務上知り得た情報の守秘義務に関する事項
- (6) 再委託の禁止又は制限に関する事項
- (7) 委託業務終了後の情報資産の返還、廃棄等に関する事項
- (8) 委託業務の定期報告及び緊急時報告の義務に関する事項
- (9) 委託業務の実施状況の検査の実施に関する事項
- (10) 事故時等の公表に関する事項
- (11) 契約事項に違反した場合における契約解除、損害賠償等に関する事項

4 情報システム管理者及び情報セキュリティ管理者は、必要があると認める場合には、委託に係る契約書に第1項各号及び前項各号に規定する事項のほか、次に掲げる事項を追加するものとする。

- (1) 情報資産の受渡し及び運搬に関する事項
- (2) 事業者における情報資産の保管に関する事項
- (3) その他情報資産の保護に関し必要な事項

(事業者に対する説明)

第46条 情報システム管理者及び情報セキュリティ管理者は、ネットワーク又は情報システムの開発、構築、保守等の業務を委託する場合には、事業者に契約事項を説明し、遵守させなければならない。

2 情報システム管理者及び情報セキュリティ管理者は、事業者が契約に基づき委託業務を再委託する場合には、再委託先の事業者に遵守すべき内容及び機密事項を説明し、遵守させなければならない。

(研修計画の立案及び実施)

第47条 情報セキュリティ総括管理者は、職員等を対象とする情報セキュリティに関する研修を企画立案し、情報セキュリティ委員会の承認を得なければならない。

2 情報セキュリティ総括管理者は、新規採用職員を対象とする情報セキュリティに関する研修を実施しなければならない。

(緊急時対応訓練)

第48条 情報セキュリティ統括責任者は、緊急時に対応するための訓練（以下「緊急時対応訓練」という。）の計画を企画立案し、情報セキュリティ委員会の承認を得なければならない。

2 前項に規定する計画は、ネットワーク及び情報システムの規模等を考慮した上で、訓練実施の範囲等を定め、効果的に実施することができるよう企画立案しなければならない。

3 緊急時対応訓練は、定期的実施するものとする。

(職員等からの事故の報告)

第49条 職員等は、情報セキュリティに関する事故を発見した場合には、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。

- 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場合には、速やかに、情報セキュリティ総括管理者及び情報システム管理者にその内容を報告しなければならない。
- 3 情報セキュリティ総括管理者は、前項の規定による報告を受けた場合には、必要に応じ、最高情報統括責任者又は情報セキュリティ統括責任者にその内容を報告しなければならない。

(住民等外部からの事故の報告)

第50条 職員等は、本町が管理する情報資産に関する事故について、住民等外部から報告を受けた場合には、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場合には、速やかに、情報セキュリティ総括管理者及び情報システム管理者にその内容を報告しなければならない
- 3 情報セキュリティ総括管理者は、前項の規定による報告を受けた場合には、必要に応じ、最高情報統括責任者又は情報セキュリティ統括責任者にその内容を報告しなければならない。
- 4 情報セキュリティ総括責任者は、情報資産に関する事故について、住民等外部から報告を受けるための連絡手段を公表しなければならない。

(事故等の分析及び記録の保存)

第51条 情報セキュリティ総括管理者は、情報セキュリティに関する事故又は情報資産に関する事故に関係する課の情報セキュリティ管理者及び情報セキュリティ担当者と連携し、当該事故を分析し、その記録を保存しなければならない。

(ユーザーIDの管理)

第52条 情報セキュリティ総括管理者は、職員等の採用、異動、出向、退職等に伴うユーザーIDの取扱いを定めなければならない。

- 2 情報セキュリティ総括管理者は、職員等にユーザーIDを付与する場合には、利用権限（情報システムの機能を利用することができる権限をいう。以下同じ）を業務上必要最小限度の範囲としなければならない。
- 3 情報システム管理者は、秘書課長と連携し、利用されていないユーザーIDが放置されないよう点検しなければならない。
- 4 秘書課長は、ユーザーIDが業務上不要となった場合には、当該ユーザーIDを抹消するよう情報システム管理者に通知しなければならない。
- 5 職員等は、ユーザーIDに関し、次に掲げる事項を遵守しなければならない。
 - (1) 自己の保有するユーザーIDを他人に利用させてはならない。
 - (2) 共用ユーザーIDを共有して利用する職員等以外の者に利用させてはならない。

(管理者権限を有するユーザーIDの管理等)

第53条 情報セキュリティ総括管理者は、管理者権限（情報システムのすべての機能を利用することができる権限をいう。以下同じ。）を有するユーザーIDを利用する者の人数を必要最小限度に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、事業者に管理者権限を有するユーザーID及びパスワードの変更を行わせてはならない。

3 管理者権限を有するユーザー I D 及びパスワードは、定期的な変更、入力回数の制限等のセキュリティ機能を管理者権限を有していないパスワードよりも強化しなければならない。

(パスワードの管理)

第 5 4 条 情報システム総括管理者は、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。

2 職員等は、自己の保有するパスワードに関し、次に掲げる事項を遵守しなければならない。

- (1) 照会は一切応じない等パスワードを漏らさないこと。
- (2) パスワードを記録したメモ等を第三者が容易に発見することができる場所に保管しないこと。
- (3) パスワードの設定に当たっては、推測されやすいもの又は解読されやすいものを避けること。
- (4) コンピュータにパスワードを記憶させないこと。
- (5) パスワードが漏れいしたおそれがある場合には、速やかに、情報セキュリティ総括管理者又は情報セキュリティ管理者に報告し、パスワードを変更すること。
- (6) パスワードは、必要に応じ、変更を行うこと。
- (7) 仮のパスワードを付与された場合には、最初のログイン時に当該パスワードを変更すること。
- (8) 職員等の間でパスワード（共用ユーザー I D に係るパスワードを除く。）を共有しないこと。

(I C カードの管理)

第 5 5 条 職員等は、自己の保有する I C カードに関し、次に掲げる事項を遵守しなければならない。

- (1) I C カードを他人に利用させてはならない。
- (2) I C カードを紛失した場合には、速やかに秘書課長に報告し、指示に従わなくてはならない。
(I C カード：半導体集積回路を埋め込み、電子データを記録することができるようにしたカードのこと。)

第 5 節 技術的セキュリティ対策

(ネットワークの構成)

第 5 6 条 本町におけるネットワークは、情報資産の重要性を考慮し、情報系ネットワークと基幹系ネットワークとを分離し、基幹系ネットワークは外部と接続することができない構成とする。

(ファイルサーバの設定及び運用)

第 5 7 条 情報システム管理者は、職員等が利用することができるファイルサーバの容量を設定し、職員等に周知しなければならない。

- 2 ファイルサーバのフォルダは、課単位で構成し、職員等が所属する課のフォルダのみ閲覧し、及び利用することができるよう設定しなければならない。
- 3 職員等は、情報資産のうち電子文書（電子データのうち書式情報（文書の体裁に関する情報をいう。）を含めて記録されているものをいう。）については、ファイルサーバに保存しなければならない。
- 4 前項の規定にかかわらず、職員等は、ファイルサーバの容量を圧迫するような情報資産を保存しないよう努めなければならない。

- 5 住民の個人情報、人事に関する情報等特定の職員等のみが取り扱う情報資産については、当該特定の職員等以外の職員等が閲覧し、及び利用することができないよう設定を行わなければならない。

(バックアップの取得)

第58条 情報システム管理者及び情報セキュリティ管理者は、新たに情報システムを構築する場合には、当該情報システムに係るサーバ等の初期設定情報についてバックアップを取得し、保管しなければならない。

- 2 情報システム管理者は、ファイルサーバに保存された情報について、定期的にバックアップを取得しなければならない。
- 3 情報システム管理者及び情報セキュリティ管理者は、随時更新される情報資産及び情報システムについて、その重要度に応じ期間を定め、定期的にバックアップを取得しなければならない。

(他の団体との情報システムに関する情報等の交換)

第59条 情報システム管理者及び情報セキュリティ管理者は、情報システムに関する情報又はソフトウェアを他の団体と交換する場合には、その取扱いに関する事項を定め、情報セキュリティ総括管理者の許可を得なければならない。

(システム管理記録及び作業の確認)

第60条 情報システム管理者及び情報セキュリティ管理者は、情報システムの正常動作の維持のために実施した作業の内容を作業記録簿に記録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、情報システムにおいて、設定変更等の作業を行った場合には、当該作業の内容について記録しなければならない。
- 3 情報システム管理者及び情報セキュリティ管理者は、事業者が情報システムの変更等の作業を行う場合には、当該事業者に対して、原則として2名以上の作業員で作業すること及び作業員が相互に作業の確認を実施することを指示しなければならない。

(システム関連文書の管理)

第61条 情報システム管理者及び情報セキュリティ管理者は、業務上必要とする者以外の者がシステム関連文書を閲覧することができないよう適切に管理しなければならない。

(アクセス記録の取得等)

第62条 情報システム管理者及び情報セキュリティ管理者は、アクセス記録（サーバの利用状況の記録をいう。以下同じ。）その他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。

- 2 情報システム管理者及び情報セキュリティ管理者は、アクセス記録の盗難、改ざん又は消去を防止するために必要な措置を講じなければならない。
- 3 情報システム管理者及び情報セキュリティ管理者は、情報システムから自動出力したアクセス記録等について、必要に応じ、バックアップを取得しなければならない。

(障害記録)

第63条 情報システム管理者及び情報セキュリティ管理者は、情報システムの障害に関する報告、処理結果、課題等を障害記録として記録し、これを保存しなければならない。

(ネットワーク等)

第64条 情報システム管理者及び情報セキュリティ管理者は、ネットワークにおいてフィルタリング及びルーティングが適切に機能するよう、当該ネットワークを構成するスイッチ類（ファイアウォール、ルータ等をいう。）を設定しなければならない。

2 情報セキュリティ管理者及び情報システム管理者は、不正アクセスを防止するため、ネットワークにアクセス制御（利用権限を有さない者が情報システムを利用すること及び許可された利用方法以外の方法により情報システムを利用することができないよう調整することをいう。）を施さなければならない。

（ファイアウォール：インターネット等の外部ネットワークからの侵入を防ぐための機器及びシステムのこと。）

（ルータ：ネットワークの境界に設置され、ネットワーク相互間で電子データを中継し、送信する機器のこと。）

（フィルタリング：送られてきた電子データを検査し、通過させるかどうかを判断する機能のこと。）

（ルーティング：電子データを送信する場合に、最適な通信回線を選択して送信する機能のこと。）

(外部ネットワークとの接続制限等)

第65条 情報システム管理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を外部ネットワーク（インターネット等の本町のネットワーク以外のネットワークをいう。以下同じ。）と接続しようとする場合には、最高情報統括責任者の許可を得なければならない。この場合において、当該許可を得たときは、当該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、庁舎内のすべてのネットワーク及び情報システムに影響が生じないことを確認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、接続した外部ネットワークの^{かし}瑕疵により情報の漏えい、破壊又は改ざん、情報システムのシステムダウンその他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明記した契約を締結するよう努めなければならない。

3 情報システム管理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上に公開する場合には、庁舎内のネットワークへの不正アクセスを防止するために必要な措置を講じなければならない。

4 情報システム管理者は、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、本町においてセキュリティ障害が発生するおそれがある場合には、情報セキュリティ総括管理者の判断に従い、速やかに、当該外部ネットワークとの接続を物理的に遮断しなければならない。

(無線LANネットワークの構築の制限)

第66条 無線LANによるネットワークは、原則として採用しない。ただし、特別な理由により無線LANによるネットワークの構築が必要な場合であつて、情報セキュリティ総括管理者が許可したときは、この限りでない。

2 前項ただし書の規定による許可を得た者は、無線LANによるネットワークを構築する場合には、解読が困難な暗号化及び認証技術を使用しなければならない。

(電子メールの管理)

第67条 情報システム管理者は、利用権限のない者による電子メールの転送及び中継処理が行われることがないように、メールサーバの設定を行わなければならない。

2 情報システム管理者は、大量のスパムメール等の受信又は送信を防止するための措置を講ずるものとし、大量のスパムメール等を検知した場合には、直ちにメールサーバの運用を一時停止する等適正な処置を講じなければならない。

3 情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える容量の電子メールの送受信を不可能にしなければならない。

4 情報システム管理者は、職員等が利用することが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。

5 情報システム管理者は、職員等が電子メールを用いて外部に情報資産を持ち出すことがないように監視しなければならない。

(スパムメール：受信者の都合を無視し、無差別に大量送信される迷惑メールのこと。)

(電子メールボックス：電子メールを保存しておくサーバにおける保存場所のこと。)

(電子メールの利用)

第68条 職員等は、原則として、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。

2 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。

3 職員等は、電子メールを送信する場合には、原則として、上司へカーボンコピーの機能を用いて送信しなければならない。

4 職員等は、複数人に電子メールを送信する場合には、必要があるときを除き、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。

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

6 職員等は、フリーメール、ネットワークストレージサービス等を利用してはならない。

7 職員等は、改姓等の理由により電子メールアドレスを変更する必要がある場合には、秘書課長を通じ、情報セキュリティ総括管理者へ届け出るものとする。

8 情報セキュリティ総括管理者は、情報システムの運用上必要があると認める場合には、電子メールアドレスを変更することができるものとする。

9 情報セキュリティ管理者は、事業ごとに電子メールアドレスを取得することができるものとし、取得をしようとする場合には、電子メールアドレス取得申請書(様式第6号)を情報セキュリティ総括管理者に提出し、許可を得なければならない。

(カーボンコピー：電子メールのソフトウェアのカーボンコピー一覧に入力したメールアドレスに同じ

内容の電子メールが送信される機能のこと。)

(フリーメール：インターネットを介して無料で提供される電子メールサービスのこと。)

(ネットワークストレージサービス：ネットワーク上でファイル保管用のディスクスペースに電子データを保存することができるサービスのこと。)

(電子メールアカウント：電子メールを利用するためのユーザーIDのこと。)

(電子署名)

第69条 職員等は、特に機密性又は完全性の確保に配慮する必要がある情報資産を外部に送信する場合には、電子署名（野々市町処務規程第4条第4号に規定する電子署名をいう。）を行い、送信しなければならない。

(機器の構成変更等の許可)

第70条 情報システム管理者及び情報セキュリティ管理者は、コンピュータの機器構成を変更し、又はコンピュータに周辺機器を接続する必要がある場合には、情報セキュリティ総括管理者の許可を得なければならない。

(外部記録媒体の利用制限)

第71条 情報システム管理者は、基幹系ネットワークで利用するコンピュータ（次項の規定により許可を受けたものを除く。）においては外部記録媒体の利用を不可能とするよう、コンピュータの設定を行わなければならない。

2 情報セキュリティ管理者は、基幹系ネットワークで利用するコンピュータにおいて外部記録媒体を利用しようとする場合には、基幹系ネットワークコンピュータに係る外部記録媒体利用申請書（様式第7号）を情報セキュリティ総括管理者に提出し、許可を得なければならない。

(業務外目的でのインターネット閲覧の制限)

第72条 情報システム管理者は、職員等が業務目的以外でインターネットを閲覧することができないよう、コンテンツフィルタを適用しなければならない。

2 情報システム管理者は、職員等のインターネットの利用について監視するものとし、明らかに業務目的以外でインターネットを利用していることを発見した場合には、情報セキュリティ総括管理者に報告するとともに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。

(コンテンツフィルタ：ホームページの内容をチェックし、有害と思われるものの閲覧を防止する機能のこと。)

(アクセスの制限)

第73条 情報システム管理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又は情報システムごとに利用権限のない職員等が当該ネットワーク又は情報システムを利用することができないよう、システム上制限を実施しなければならない。

(基幹系ネットワークの利用範囲)

第74条 各課における基幹系ネットワークの機能利用範囲は、別表のとおりとする。

2 情報セキュリティ管理者は、別表に定める機能利用範囲を超えて利用しようとする場合には、基幹系ネットワーク機能利用申請書（様式第8号）を利用しようとする情報を所管する情報セキュリティ管理者に提出し、許可を得なければならない。

（職員等による外部からの接続の禁止）

第75条 職員等は、外部ネットワークを通じて本町のネットワークに情報機器を接続してはならない。

（自動識別の設定）

第76条 情報システム管理者は、機器固有情報によって情報機器とネットワークとの接続の可否が自動的に識別される仕組みを構築しなければならない。

（管理者権限による接続時間の制限）

第77条 情報システム管理者は、管理者権限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度にしなければならない。

（情報システムの調達）

第78条 情報システム管理者及び情報セキュリティ管理者は、情報システムを開発し、構築し、又は更新しようとする場合には、情報システム管理者と協議の上、情報システム接続（変更）申請書（様式第9号）を情報セキュリティ総括管理者に提出し、許可を得なければならない。

2 情報システム管理者及び情報セキュリティ管理者は、事業者が情報システムの開発、構築、導入、保守等の業務を委託しようとする場合には、当該業務の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。

3 情報システム管理者及び情報セキュリティ管理者は、情報機器及びソフトウェアの調達に当たっては、当該情報機器及びソフトウェアのセキュリティ機能を調査し、情報セキュリティ上支障がないことを確認しなければならない。

（情報システムの開発又は構築）

第79条 情報システム管理者及び情報セキュリティ管理者は、情報システムの開発又は構築に当たっては、職員等から責任者及び作業者を定めなければならない。

2 情報システム管理者及び情報セキュリティ管理者は、前項の責任者及び作業者に開発者用のユーザーIDを付与するものとし、情報システムの開発又は構築が完了した場合には、速やかに、当該開発用のユーザーIDを削除しなければならない。

3 情報システム管理者及び情報セキュリティ管理者は、第1項の責任者及び作業者に開発用のユーザーIDを付与する場合には、利用権限を必要最小限度の範囲としなければならない。

4 情報システム管理者及び情報セキュリティ管理者は、情報システムの開発又は構築のために利用を認めたソフトウェア以外のソフトウェアがインストールされていることを発見した場合には、当該ソフトウェアを情報システムから削除しなければならない。

(情報システムの導入)

第80条 情報セキュリティ管理者は、情報システムを導入する場合には、当該情報システムをネットワーク又は既に稼動している情報システムに接続する前に、既に稼動している情報システムに支障とならないことについて、情報システム管理者と協議の上、十分な運用テスト及び検証を実施しなければならない。

- 2 情報システムの開発、構築、保守及びこれらに係る運用テスト（以下「運用テスト等」という。）を行う場合には、当該運用テスト等の環境と既に稼動している情報システムの環境とを分離しなければならない。
- 3 前項に規定する場合においては、個人情報及び非公開の情報を利用してはならない。ただし、当該個人情報又は非公開の情報を所管する情報システム管理者又は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。
- 4 情報システム管理者及び情報セキュリティ管理者は、情報システムの運用テスト等の環境から運用環境へ移行を行う場合には、当該移行に係る手順を明確にした上で行わなければならない。
- 5 前項に規定する場合においては、既に稼動している情報システムに記録されている情報資産を保存し、当該既に稼動している情報システムの停止等による業務への影響が最小限度となるよう配慮しなければならない。

(情報システムの開発、構築及び保守に関する資料等の保管)

第81条 情報システムの開発、構築及び保守に係るシステム関連文書は、適切な方法で保管しなければならない。

- 2 情報システムの開発、構築及び保守に係る運用テストの結果は、一定期間保管しなければならない。

(情報システムにおける入出力情報の正確性の確保)

第82条 情報システムに入力される情報については、範囲及び妥当性の確認機能並びに不正な文字列等の入力除去する機能を組み込むよう情報システムを設計しなければならない。

- 2 情報システムに入出力される情報について、故意若しくは過失により情報が改ざんされ、又は漏えいするおそれがある場合にこれを検知する機能を組み込むよう、情報システムを設計しなければならない。

(情報システムの変更の管理)

第83条 情報システム管理者及び情報セキュリティ管理者は、情報システムを変更しようとする場合には、情報システム接続（変更）申請書を情報セキュリティ総括管理者に提出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、情報システムを変更した場合には、当該情報システムに係るシステム関連文書の変更履歴を作成し、保管しなければならない。

(開発又は構築及び保守に用いるソフトウェアの更新等)

第84条 情報システム管理者及び情報セキュリティ管理者は、情報システムに係る開発、構築若しくは保守に用いるソフトウェア等を更新し、又は情報システムにセキュリティパッチの適用を行う

場合には、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。

(セキュリティパッチ：ソフトウェアにおけるセキュリティ上の欠陥を修復するためのプログラムのこと。)

(情報システム管理者の措置事項)

第85条 情報システム管理者は、不正プログラム対策及び不正アクセス対策として、次に掲げる事項を行わなければならない。

- (1) 外部から受信するファイル及び外部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不正プログラムの有無の確認を行い、不正プログラムの本町のネットワークへの侵入及び外部への拡散を防止すること。
- (2) サーバ及びコンピュータに不正プログラム対策ソフトウェアを常に機能させること。
- (3) 不正プログラム対策ソフトウェア及び不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つこと。
- (4) すべてのコンピュータに対して、1日1回以上、不正プログラム対策ソフトウェアを用いて不正プログラムの有無の確認を実施すること。
- (5) 使用していないポートを閉鎖すること。
- (6) ホームページの改ざんを検知し、情報システム管理者に通知する等の機能を情報機器及び情報システムに設定すること。

(ゲートウェイ：異なる種類のネットワークを接続する際に、その境界において電子データの変換処理を行う仕組み及び機器のこと。)

(パターンファイル：不正プログラム対策ソフトウェアにおいて不正プログラムを検知するために必要となるファイルのこと。)

(ポート：コンピュータ等において、外部との情報の受け渡しを行うための通信の口。)

(情報セキュリティ管理者の措置事項)

第86条 情報セキュリティ管理者は、情報システムの不正プログラム対策として、次に掲げる事項を行わなければならない。

- (1) サーバ及びコンピュータに不正プログラム対策ソフトウェアを常に機能させること。
- (2) 不正プログラム対策ソフトウェア及び不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つこと。

(不正プログラムに対する措置)

第87条 情報セキュリティ総括管理者は、不正プログラムの情報を収集し、必要に応じ、職員等に対して不正プログラムへの注意を喚起するものとし、職員等は、提供される不正プログラムの情報を常に確認しなければならない。

2 職員等は、コンピュータが不正プログラムに感染した場合には、直ちに、当該コンピュータからLANケーブルを取り外し、情報セキュリティ総括管理者に報告しなければならない。

(専門家の支援体制)

第88条 情報セキュリティ総括管理者は、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。

(攻撃の予告)

第89条 最高情報統括責任者は、サーバ等に攻撃を受けることが明確となった場合には、情報システムの緊急停止その他必要な措置を講じるとともに、警察及び関係機関と連携し、情報の収集に努めなければならない。

(記録の保存)

第90条 最高情報統括責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセスその他犯罪行為の可能性がある場合には、当該攻撃の記録を保存するとともに、警察及び関係機関との連携に努めなければならない。

(攻撃の監視)

第91条 情報セキュリティ統括責任者は、職員等及び事業者が利用しているコンピュータから庁舎内のサーバ等又は外部のホームページ等に対して攻撃することがないように監視しなければならない。

(セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等)

第92条 情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、情報セキュリティ担当者間で当該情報を共有しなければならない。

2 情報システム管理者は、セキュリティホールを発見した場合において、セキュリティ障害の発生を防止するため緊急の必要があると認めるときは、ソフトウェア又は情報機器の更新等の対策を実施しなければならない。

(セキュリティホール：ソフトウェアの設計ミス等により生じたセキュリティ上の欠陥のこと。)

第6節 運用面におけるセキュリティ対策

(情報セキュリティ実施手順の策定)

第93条 情報システム管理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情報セキュリティ実施手順を策定しなければならない。この場合において、新たに導入した情報システムに係る情報セキュリティ実施手順については、当該情報システムの運用を開始するまでに策定しなければならない。

2 情報セキュリティ実施手順には、次に掲げる事項を定めなければならない。

- (1) 情報システムの起動及び停止に係る事項
- (2) 電子データの処理に関する事項
- (3) バックアップの取得に関する事項
- (4) 情報機器及びソフトウェアのメンテナンスに関する事項
- (5) 作業中に発生する障害又は例外事項に対する処置に関する事項
- (6) 情報システムの利用制限に関する事項
- (7) 操作上又は技術上の不測の事態が発生した場合の連絡に関する事項
- (8) 情報システムが故障した場合の再起動又は復旧に関する事項

- 3 情報システム管理者及び情報セキュリティ管理者は、情報セキュリティ実施手順を策定した場合には、情報セキュリティ総括管理者に報告するとともに、情報システムの運用に携わる職員等に対して当該情報セキュリティ実施手順を周知しなければならない。
- 4 情報セキュリティ実施手順は、非公開とする。

(情報システムの監視)

- 第94条 情報セキュリティ総括管理者及び情報システム管理者は、情報システムの正常動作を維持するため、情報システムを常時監視しなければならない。
- 2 情報システム管理者及び情報セキュリティ管理者は、重要なアクセス記録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をするための措置を講じなければならない。
 - 3 情報セキュリティ総括管理者及び情報システム管理者は、ログイン及びログアウトの時刻の表示、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等により、正当な利用権限を有する職員等が利用していることを常時監視しなければならない。
 - 4 情報セキュリティ総括管理者及び情報システム管理者は、外部と常時接続する情報システムを常時監視しなければならない。

(情報システムの停止)

- 第95条 情報システム管理者及び情報セキュリティ管理者は、原則として、情報システムを終日稼働させるものとする。ただし、保守作業等のため必要と認める場合には、職員等に周知した上で、情報システムを停止することができるものとする。
- 2 前項の規定にかかわらず、情報システム管理者は、情報システムに障害が発生した場合には、前項ただし書の規定による周知を行わずに情報システムを緊急停止することができるものとする。

(規程の遵守状況の確認及び対処)

- 第96条 情報システム管理者及び情報セキュリティ管理者は、この規程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、最高情報統括責任者、情報セキュリティ統括責任者及び情報セキュリティ総括管理者に報告しなければならない。
- 2 情報システム管理者は、ネットワーク、サーバ等のシステム設定におけるこの規程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、迅速かつ適切に対処しなければならない。

(コンピュータ、記録媒体等の利用状況調査)

- 第97条 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、不正プログラム等の調査のために、コンピュータ及び記録媒体のアクセス記録、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。

(職員等の報告義務)

- 第98条 職員等は、この規程に違反する行為を発見した場合には、直ちに、情報セキュリティ総括管理者及び情報セキュリティ管理者に報告をしなければならない。

(緊急時対応計画の策定等)

第99条 情報セキュリティ総括管理者は、情報セキュリティに関する事故、職員等の違反行為等によりセキュリティ障害が発生した場合又は発生するおそれがある場合における連絡体制の確保、証拠保全、被害拡大の防止、復旧作業、再発防止等の措置を迅速かつ適切に実施するための計画（以下「緊急時対応計画」という。）を策定しなければならない。

- 2 職員等は、情報セキュリティ障害が発生した場合又は発生するおそれがある場合には、緊急時対応計画に従って適切に対処しなければならない。
- 3 情報セキュリティ総括管理者は、職員等の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判断した場合には、緊急時対応計画に従って適切に対処しなければならない。

(緊急時対応計画に規定する事項)

第100条 緊急時対応計画には、次に掲げる事項を定めなければならない。

- (1) 対応責任者
- (2) 緊急連絡の手順及び連絡の範囲
- (3) セキュリティ障害の影響範囲の確定
- (4) 応急措置の方法
- (5) 代替手段に移行する場合の手順
- (6) 復旧の手順

(委託事業者の選定基準)

第101条 情報セキュリティ総括管理者及び情報セキュリティ管理者は、業務を委託する事業者（以下「委託事業者」という。）の選定に当たり、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。

(委託事業者に対する確認及び措置等)

第102条 情報システム管理者及び情報セキュリティ管理者は、委託事業者において必要な情報セキュリティ対策が確保されていることを確認しなければならない。この場合において、必要な情報セキュリティ対策が確保されていないと認めるときは、情報システム管理者及び情報セキュリティ管理者は、必要に応じ、契約事項に基づき改善要求等の措置を実施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、前項ただし書に規定する改善要求等の措置を実施した場合には、当該改善要求等の内容を情報セキュリティ統括管理者に報告するとともに、その重要度に応じ、最高情報統括責任者に報告しなければならない。

(例外措置の実施)

第103条 情報セキュリティ総括管理者、情報システム管理者及び情報セキュリティ管理者は、業務の適正な遂行を継続するため、最高情報統括責任者の許可を得た場合には、この規程に規定する遵守事項とは異なる方法を採用すること、遵守事項を実施しないこと等の措置（以下「例外措置」という。）を実施することができる。

- 2 前項の規定にかかわらず、情報セキュリティ総括管理者、情報システム管理者及び情報セキュリティ管理者は、業務の遂行上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適当と認

めるときは、同項に規定する許可を得ることなく当該例外措置を実施することができるものとする。

3 前項の場合において、例外措置を実施したときは、情報セキュリティ総括管理者、情報システム管理者及び情報セキュリティ管理者は、速やかに、最高情報統括責任者に報告しなければならない。

(例外措置の履歴の管理)

第104条 情報セキュリティ統括管理者は、例外措置の履歴を適切に保管しなければならない。

第7節 知的財産権の管理

(知的財産権の保護等)

第105条 情報システム管理者及び情報セキュリティ管理者は、ソフトウェア等の電子データに係る著作権、商標権等の知的財産権の保護のため、法的な規制措置を確実に遵守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、ソフトウェア管理簿(様式第10号)を作成し、保管しなければならない。

3 情報システム管理者及び情報セキュリティ管理者は、使用許諾書、マスターディスク、マニュアル等の所有権の証拠書類等を安全かつ確実に保管するものとする。

4 情報システム管理者及び情報セキュリティ管理者は、ソフトウェアを利用する上で許可された利用者の最大数を越えることのないよう管理するものとする。

5 情報システム管理者及び情報セキュリティ管理者は、利用を許可されているソフトウェア及び使用許諾を得ている製品だけがサーバ及びコンピュータにインストールされていることを確認するものとする。

(マスターディスク:ソフトウェアを購入した際にプログラムが記録されているフロッピーディスク、CD-ROM等の外部記録媒体のこと。)

第8節 評価、見直し等

(監査の実施)

第106条 情報セキュリティ委員会は、情報セキュリティ監査統括責任者を指名し、情報セキュリティ対策の実施状況について、定期的に又は必要に応じ、監査を行わせなければならない。

(監査実施計画の立案及び監査の協力)

第107条 情報セキュリティ監査統括責任者は、監査を実施するに当たり、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

2 職員等は、監査の実施に協力しなければならない。

(監査の実施依頼)

第108条 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、当該監査を受ける課が属する部に所属する職員等以外の者で、監査及び情報セキュリティに関する基礎的な知識を有するものに対して、当該監査の実施を依頼しなければならない。

(監査結果の報告)

第109条 情報セキュリティ監査統括責任者は、監査の結果を取りまとめ、情報セキュリティ委員会に報告するものとする。

(監査調書等の保管)

第110条 情報セキュリティ監査統括責任者は、監査の実施を通じて収集した監査証拠及び監査報告書作成のための監査調書を適切に保管しなければならない。

(監査結果への対応)

第111条 情報セキュリティ統括責任者は、監査において指摘事項があった場合には、当該指摘事項に係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て、当該指摘事項への対処を指示しなければならない。この場合において、当該指摘事項に関係していない情報セキュリティ管理者に対しても、同種の問題又は課題がある可能性が高いときは、当該問題又は課題の有無を確認させなければならない。

(自己点検の実施)

第112条 情報セキュリティ総括管理者は、本町が保有する情報資産について、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。

2 情報システム管理者及び情報セキュリティ管理者は、情報セキュリティ総括管理者の指示に従い、情報セキュリティ対策の実施状況について、毎年度又は必要に応じ、自己点検を行わなければならない。

(自己点検結果の報告)

第113条 情報システム管理者及び情報セキュリティ管理者は、自己点検の結果及び当該自己点検の結果に基づく改善策を取りまとめ、情報セキュリティ総括管理者に報告しなければならない。

2 情報セキュリティ総括管理者は、前項の規定により報告があった自己点検の結果を取りまとめ、情報セキュリティ委員会に報告しなければならない。

(自己点検の結果の活用)

第114条 情報セキュリティ総括管理者は、自己点検の結果に基づき、改善が必要であると認める場合には、その改善に必要な措置を講じなければならない。

2 情報セキュリティ委員会は、自己点検の結果をこの規程の見直しその他情報セキュリティ対策の見直しに活用しなければならない。

第4章 雑則

(委任)

第115条 この規程に定めるもののほか、本町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ことに関し必要な事項は、最高情報総括責任者が別に定める。

附 則

この規程は、平成21年7月1日から施行する。

様式第2号（第35条関係）

コンピュータ等接続（更新）申請書

年 月 日

情報セキュリティ総括管理者 あて

課（所、局）長

次のコンピュータ等をネットワークに新たに（更新して）接続したいので申請します。

物品名	
（新規又は更新前の） コンピュータ等の仕様	メーカー 機種・製造番号 使用OS
購入年月日 備品台帳番号	年 月 日
（更新後の） コンピュータ等の仕様	メーカー 機種・製造番号 使用OS
接続（更新）の目的及び理由 （できる限り具体的に記入してください。）	目的 理由
接続するネットワーク	情報系ネットワーク / 基幹系ネットワーク
情報セキュリティ担当者氏名	

様式第3号（第36条関係）

ソフトウェアインストール申請書

年 月 日

情報セキュリティ総括管理者 あて

課（所、局）長

コンピュータに次のソフトウェアをインストールしたいので申請します。

ソフトウェア名称	名称 バージョン
インストールの理由	
ライセンス管理の方法	
インストール対象機器	製造番号 コンピュータ名
情報セキュリティ担当者氏名	

様式第5号（第44条関係）

嘱託職員等に係る情報資産等利用申請書

年 月 日

情報セキュリティ総括管理者 様

課（所、局）長

嘱託職員等にネットワーク及び情報システムを利用させたいので、次のとおり申請します。

利用期間	年 月 日から 年 月 日まで
嘱託職員等氏名	ふりがな 氏 名
利用内容	
利用の目的及び理由 （できる限り具体的に記入してください。）	目的 理由
情報セキュリティ担当者氏名	

様式第6号（第68条関係）

電子メールアカウント取得申請書

年 月 日

情報セキュリティ総括管理者 あて

課（所、局）長

電子メールアカウントを取得したいので、次のとおり申請します。

電子メールアカウント第1希望	@town.nonoichi.lg.jp
電子メールアカウント第2希望	@town.nonoichi.lg.jp
運用期間	年 月 日から 年 月 日まで
メール受信担当者職氏名 及びユーザー名（2名）	職氏名 ユーザー名 職氏名 ユーザー名
事業名	
取得の理由	
情報セキュリティ担当者氏名	

備考

- 1 電子メールアカウントは、4文字以上、12文字以内の英数文字としてください。
- 2 電子メールアカウントには【¥/、;*?"<>|】の文字は使えません。

様式第7号（第71条関係）

基幹系ネットワークコンピュータに係る外部記録媒体利用申請書

年 月 日

情報セキュリティ総括管理者 あて

課（所、局）長

次のコンピュータにおいて外部記録媒体を利用したいので申請します。

基幹系コンピュータ詳細	コンピュータ名 : 備品番号 : 主なコンピュータ使用者 :
外部記録媒体の種別	・FD・USBメモリ・MO・CD-RW/DVD-RW ・その他（ ）
外部記録媒体利用の理由	
情報セキュリティ担当者氏名	

様式第8号（第74条関係）

基幹系ネットワーク機能利用申請書

年 月 日

課（所）長 あて

課（所、局）長

基幹系ネットワークを利用するにあたり、次のとおり機能の利用を希望しますので申請します。

職員等氏名	利用機能名	申請理由

申請担当者

課（所、局） 担当

年 月 日

上記の件について、利用することを許可する。

課（所、局）長

印

備考 許可を得た申請書の写しを情報セキュリティ総括管理者へ提出すること。

付録 用語解説

索引	用語	解説	主な使用箇所
あ	ICカード	半導体集積回路を埋め込み、電子データを記録することができるようにしたカードのこと。大容量の電子データを記録することができ、情報の暗号化も可能であるため、安全性が高い。情報システムを利用する際の認証にも用いられる。	
	アクセス記録	サーバの利用状況（利用者のIPアドレス、利用された日時、利用されたファイル名等）の記録のこと。	
	アクセス制御	利用権限を有さない者が情報システムを利用すること及び許可された利用方法以外の方法により情報システムを利用することができないよう調整すること。	
	暗号化	インターネット等のネットワークを通じて電子データをやり取りする際に、通信途中で第三者に盗聴され、又は改ざんされることのないよう、決まった規則に従って電子データを変換すること。	
か	カーボンコピー	電子メールの機能の1つ。カーボンコピー覧に記入したメールアドレスに同じ内容の電子メールが送信される機能のこと。	
	外部ネットワーク	インターネット等の庁舎外のネットワークのこと。	
	基幹サーバ	住民情報、税情報、福祉情報等業務の基幹となる情報を記録しているサーバのこと。	
	記録媒体	情報を記憶するための媒体（メディア）のこと。ハードディスク、USBメモリ、CD-R、DVD-R等を指す。	
	緊急時対応訓練	実際に情報流出等の事故が発生した場合に即応することができる体制を整えておくための緊急時を想定した訓練のこと。	
	緊急時対応計画	情報資産への侵害が発生した場合等に備えて実施すべき具体的な方法を定めた計画のこと。	
	ゲートウェイ	異なる種類のネットワークを接続する際に、その境界において電子データの変換処理を行う仕組み及び機器のこと。	
	コンテンツフィルタ	ホームページの内容をチェックし、有害と思われるものの閲覧を防止する機能のこと。	
さ	サーバの二重化	サーバが緊急停止した場合でも継続して業務を行うことができるよう、サーバのバックアップシステムを設置すること。	

最高情報統括責任者	本町におけるすべてのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有するものこと。	
時刻同期	サーバ間で時刻設定を自動的に合わせること。	
自己点検	情報セキュリティに関する規程の履行状況等を情報システムを運用する職員等が自ら点検し、及び評価すること。	
システム管理記録	情報システムの状況を正確に把握するため、情報システムに対して行った作業を記録しておくこと。	
システム関連文書	システム設計書、プログラム仕様書等保有する情報システムに関わる文書のこと。	
自動識別	ネットワークに不正な機器の接続を防止するため、機器固有情報によってコンピュータとネットワークとの接続の可否を自動的に識別すること。	
障害記録	システム障害の内容、発生期日等を記録したもの。システム障害への対応時に過去に起きた類似障害を参考とするため、適切に保管する。	
情報資産の分類	機密性、完全性及び可用性の度合いに応じ情報資産の分類を行うこと。	
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。	
情報セキュリティ委員会	情報セキュリティに関する重要な事項を決定する機関のこと。	
情報セキュリティ監査	ネットワーク、情報システム等における情報セキュリティ対策の実施状況について、客観的に専門的見地から評価し、関係者に改善事項等の助言及び勧告を行うこと。	
スパムメール	受信者の都合を無視し、無差別に大量送信される迷惑メールのこと。	
バックアップサーバ	メインサーバに障害が発生した場合に備えるための予備用のサーバのこと。	
セキュリティパッチ	ソフトウェアにおけるセキュリティ上の欠陥を修復するためのプログラムのこと。	
セキュリティホール	ソフトウェアの設計ミス等により生じたセキュリティ上の欠陥のこと。	
総合行政ネットワーク	地方公共団体を相互に接続する行政専用ネットワークのこと。	

た	電子署名	電子文書の正当性を保障するために付けられる署名情報のこと。	
	電子メールアカウント	電子メールを利用するためのユーザーIDのこと。	
	電子メールボックス	電子メールを保存しておくサーバにおける保管場所のこと。	
な	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、その機器構成（情報機器及びソフトウェア）のこと。	
	ネットワークストレージサービス	ネットワーク上でファイル保管用のディスクスペースに電子データを保存することができるサービスのこと。	
は	パスワード	利用者を認証するための暗証番号のこと。	
	パターンファイル	不正プログラム対策ソフトウェアにおいて不正プログラムを検知するために必要となるファイルのこと。	
	バックアップ	コンピュータに保存されたプログラム等の電子データを、破損、コンピュータウイルス感染等の事態に備え、別の外部記録媒体に保存すること。	
	ファイアウォール	インターネット等の外部ネットワークからの侵入を防ぐための機器及びシステムのこと。	
	フィルタリング	ルータ及びファイアウォールが有する機能で、送られてきた電子データを検査し、通過させるかどうかを判断する機能のこと。	
	不正プログラム	コンピュータウイルス、スパイウェア等のコンピュータに対して意図的に悪影響を及ぼすように作られたプログラム又はソフトウェアのこと。	
	フリーメール	インターネットを介して無料で提供される電子メールサービスのこと。	
	ポート	コンピュータ等において、外部との情報の受け渡しを行うための通信の口のこと。	
ま	マスターディスク	ソフトウェアを購入した際にプログラムが記録されているフロッピーディスク、CD-ROM等の外部記録媒体のこと。	
	ミラーリング	電子データの複製を別の場所にリアルタイムに保存すること。	
	無線LAN	無線を使って構築されるLANのこと。	
	メインサーバ	二重化されたサーバにおいて、通常使用するサーバのこと。	
や	予備電源	何らかの要因で電力供給が途絶した場合に、機器が正常に停止するまでの間電力を供給するために設ける予備の電源のこと。	

ら	ルータ	ネットワークの境界に設置され、ネットワーク相互間で電子データを中継し、送信する機器のこと。	
	ルーティング	ルータ及びファイアウォールが有する機能で、電子データを送信する場合に、最適な通信回線を選択して送信する機能のこと。	
英	ID	利用者を識別するための識別符号のこと。	