只見町行政情報セキュリティポリシー
（第３版）

平成 15 年 4 月

（令和 2 年 9 月改正）

（令和 8 年 3 月改正）

只　見　町

目　　次

序　只見町行政情報セキュリティポリシーの構成

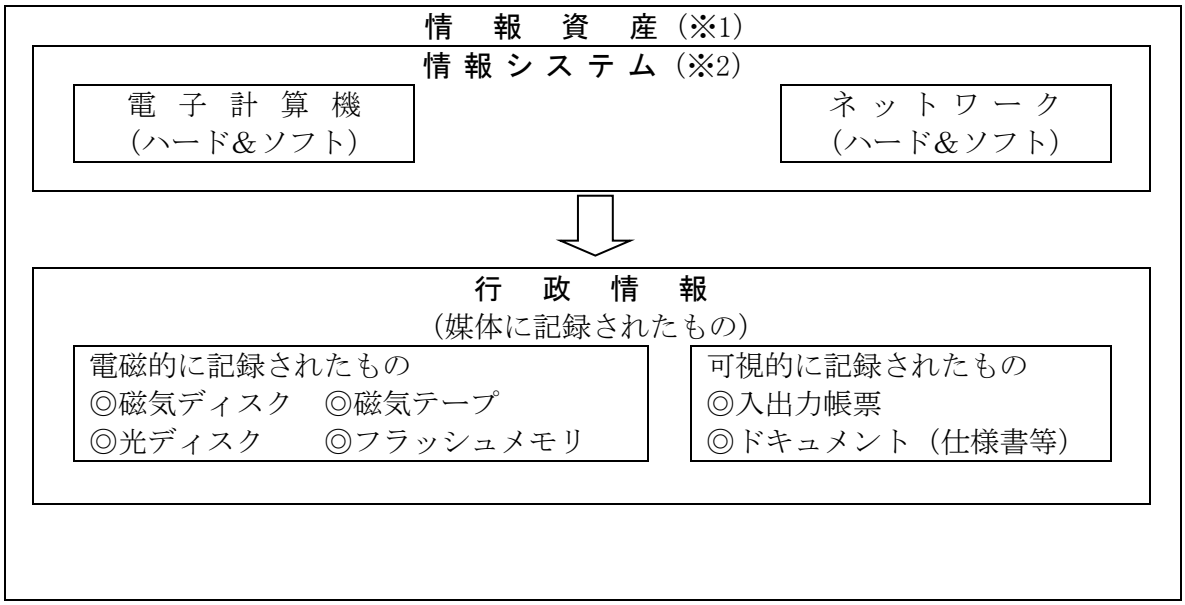
只見町行政情報セキュリティポリシーとは、只見町が保有する情報資産(※1)に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

只見町行政情報セキュリティポリシーは、本町の情報資産を取り扱う全職員に浸透、定着させるものであり、安定的な規範であることが要請される。しかし一方では、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、只見町行政情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層から成るものとして策定することとする。また、情報セキュリティポリシーに基づき、情報システム(※２)毎に、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

只見町行政情報セキュリティポリシーの構成

文　書　名		内　　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報システム毎に定める、情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順。



第１章　情報セキュリティ基本方針

１　目的

本町が取り扱う情報資産には、町民の個人情報を始めとし行政運営上重要な情報など、部外に漏洩等した場合には極めて重大な結果を招く情報が多数含まれており、これらの情報資産を人的脅威や災害、事故等から防御することは、町民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。また、近年のいわゆるＩＴ革命の進展により、電子政府や電子自治体の実現が期待されているところである。本町がこれらに積極的な対応をするためには、本町が管理しているすべての情報システムが高度な安全性を有することが不可欠な前提条件となる。

このため、本町の情報資産の機密性、完全性及び可用性（注）を維持するための対策を整備するため、只見町行政情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

このうち情報セキュリティ基本方針においては、本町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989）

機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）：情報及び処理の方法の正確さ及び完全である状態を完全防護すること。

可用性（availability）：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

（１）課等

只見町の課設置条例（昭和３０年条例第３号）第１条に規定する課及び室並びに教育委員会、公民館、認定こども園・保育所、朝日診療所、保健福祉センター、会計室、議会、農業委員会、選挙管理委員会、只見町ブナセンター、モノとくらしのミュージアムをいう。

（２）職員

地方公務員法第３条に定める、町のすべての職員及び町の会計年度任用職員をいう。

（３）個人情報

只見町個人情報保護条例(平成１４年只見町条例第２３号。)第２条第１号に規定する個人情報をいう。

（４）電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器並びに記録媒体（磁気ディスク等並びに入出力帳票及び情報システム仕様書等）をいう。

（５）記録媒体

電子計算機に使用される磁気ディスク、磁気テープ、光ディスクその他これらに類する記録媒体をいう。

（６）電子計算機室等

電子計算機を運用管理する目的で設置している部屋をいう。

（７）ネットワーク

電子計算機等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

（８）情報システム

電子計算機及びネットワークをいう。

（９）行政情報

本町の行政事務の執行に関わる情報で、かつ情報システムで取扱うものをいう。

（１０）情報資産

情報システム及び行政情報をいう。

（１１）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。

３　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本町の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

４　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は、本町の課等における情報資産及び情報資産に接するすべての職員とする。

５　職員の義務

職員は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用にあたっては情報セキュリティポリシーを遵守するものとする。

６　情報セキュリティ管理体制

本町の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

７　情報資産の分類

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

８　情報資産への脅威

情報セキュリティポリシーを講ずるうえで、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

特に認識すべき脅威は以下のとおりである。

（１）権限外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等

（２）職員及び外部委託者による意図しない操作、故意の不正アクセス又は不正操作 によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏洩等

（３）地震、落雷、火災等の災害や事故、故障等

９　情報セキュリティ対策

本町の情報資産を上記８の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

（１）人的セキュリティ対策

情報資産に接する職員の情報セキュリティに関する権限や責任等を定めるとともに、すべての職員に情報セキュリティポリシーの内容を周知徹底するため、教育・訓練を行う。

（２）物理的セキュリティ対策

電子計算機室等について不正な立入り等から保護するため、入退室や機器管理上の物理的な対策を講ずる。

（３）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策等を実施する。

（４）運用

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、ネットワークの監視等の運用面における必要な措置を講ずる。

また、障害が発生した際の迅速な対応を可能とするため、障害時の対応を講ずる。

１０　情報セキュリティ対策基準の策定

本町の情報資産について、上記９の情報セキュリティ対策を講ずるに当たっては、職員が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。

そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

１１　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、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、公開することにより本町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

１２　評価・見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準の見直しを実施するものとする。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、本町の情報資産に関する情報セキュリティ対策の基準である。

１　管理体制

情報セキュリティの管理については、以下の体制とする。

（１）最高情報総括責任者

- 最高情報総括責任者は、課等における全ての情報システム及び情報資産の情報セキュリティを統括する最高責任者とし、副町長をもってこれに充てる。

（２）総括情報管理者

- 最高情報総括責任者を補佐し、課等の情報セキュリティに関する適正な運用及び管理を監理するため、総括的な権限及び責任を有する総括情報管理者を置き、**総務企画課長**をもってこれに充てる。
- 総括情報管理者は、課等における情報セキュリティポリシーの遵守に関し、職員に対し教育・訓練、助言及び指示を行わなければならない。

（３）情報管理者

- 情報セキュリティの適正な運用及び管理を行うため、情報資産を取り扱う課（これに準ずるものを含む。）に情報セキュリティに関する権限及び責任を有する情報管理者を置き、課等の長をもってこれに充てる。
- 情報管理者は、所管する情報システムの開発、設定の変更、運用、更新等を行う権限及び責任を有する。

・ 情報管理者は、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の作成・維持・管理を行うとともに、定められている事項について職員に実施及び遵守させなければならない。
・ 情報管理者は、使用する情報システムの機器や記録媒体について、第三者に使用させること、又は許可なく情報を閲覧させることがないように、適切な措置を施さなければならない。
・ 情報管理者は、会計年度任用職員の雇用時に必ず情報セキュリティポリシーのうち、職員が守るべき内容を会計年度任用職員に理解させ、また実施及び遵守させなければならない。

２　行政情報の分類と管理

（１）行政情報の分類

対象となるすべての行政情報は、次の重要性分類に従って分類する。

①　重要性分類Ⅰ

・ 只見町個人情報保護条例（平成１４年只見町条例第２３号。）第２条第１号に規定する個人情報。
・ 法令又は条例（以下「法令等」という。）の定めにより守秘義務を課されている行政情報（上記個人情報を除く。）。
・ 法人その他の団体に関する行政情報で漏洩することにより当該団体の利益を害する恐れのあるもの。
・ 漏洩した場合、行政に対する信頼を著しく害するおそれのある行政情報。
・ 滅失し、又はき損した場合、その復元が著しく困難となり、行政の円滑な執行を妨げる恐れのある行政情報。
・ 情報システムに係るパスワード及びシステム設定情報。

②　重要性分類Ⅱ

・ 脅威にさらされた場合に実害を受ける危険性は低いが、行政事務の執行において重要性は高いと評価される行政情報（公開されると行政の円滑な執行に著しい障害を生ずる恐れのある行政情報等）。

③　重要性分類Ⅲ

・ 上記以外の行政情報。

（２）行政情報の管理方法

①　行政情報の管理及び取扱い

・ 行政情報の重要性分類に従い、パスワード等によるアクセス制限及び暗号等による通信内容の秘匿を行わなければならない。
・ 重要性分類Ⅰの行政情報の不用意な複製や、送付・送信は行ってはならない。
・ 職員は、業務上必要な場合には、情報管理者の許可を得た上で行政情報の複製・送付・送信を行わなければならない。

② 記録媒体の管理

- 重要性分類Ⅰ・Ⅱの行政情報を記録した取り外し可能な記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない。また、保管状況等を記録しなければならない。
- 重要性分類Ⅰ・Ⅱの行政情報を記録した記録媒体を送る場合は、職員又は守秘義務を明記した契約を締結した外部業者に行わせるとともに、記録媒体の物理的な保護措置を講じなければならない。

③ 記録媒体の処分

- 記録媒体が磨耗等により不要となった場合は、当該媒体に記録されている重要性分類Ⅰ・Ⅱの行政情報をいかなる方法によっても復元できないように消去等を行った上で廃棄しなければならない。
- 重要性分類Ⅰ・Ⅱの行政情報を記録した記録媒体の廃棄は、情報管理者の許可を得ることとし、廃棄を行った日時、担当者及び処理内容を記録しなければならない。

３　人的セキュリティ

（１）職員

- 職員は、情報管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行わなければならない。
- 職員は、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に定めている事項を遵守しなければならない。
- 職員は、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について不明な点、遵守することが困難な点がある場合には、速やかに情報管理者に相談し、指示を仰がなければならない。
- 職員は、使用する情報システムの機器、記録媒体について、第三者に使用されること、または許可なく情報を閲覧されることがないように、適切な措置を施さなければならない。
- 職員は、情報管理者の許可を得ずに、情報システムの機器、記録媒体等を執務室外に持ち出してはならない。
- 職員は、異動等により業務を離れる場合には、知り得た情報を他に漏らしてはならない。

（２）教育・訓練

- 統括情報管理者は、職員に対し情報セキュリティポリシーについて啓発に努めるとともに、職員を対象とした情報セキュリティポリシーに関する研修を設けなければならない。
- 総括情報管理者は、総括情報管理者として必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けなければならない。

・ 情報管理者は、情報管理者として必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けなければならない。
・ 情報システムを所管する情報管理者は、情報システムの運用に支障を来さない範囲において緊急時対応を想定した訓練等を職員に行わせなければならない。
・ 職員は、情報セキュリティポリシーに関する研修を受講し、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理解し、情報セキュリティ上の問題が生じないようにしなければならない。
・ 情報システムの開発・保守・運用管理に携わる職員は、担当者として必要な技術力を習得・維持するための研修を受けなければならない。

（３）外部委託に関する管理

・ 情報システムの開発・保守・運用管理等を外部事業者に委託する場合は、次に掲げる事項を明記した契約を締結し、その遵守を管理しなければならない。ただし、個人情報を取り扱う情報システムの開発・保守・運用管理等を外部事業者に委託しようとする場合には只見町個人情報保護条例第１０条に係る只見町個人情報取扱事務委託基準に定める事項により契約を締結し、その遵守を管理しなければならない。

ア．情報セキュリティポリシーの遵守及び従業員に対する教育に関する事項
イ．秘密保持に関する事項
ウ．目的外への使用及び第三者への提供の禁止に関する事項
エ．データの複写及び複製の禁止に関する事項
オ．再委託の禁止又は制限に関する事項
カ．報告義務に関する事項
キ．監査の実施に関する事項
ク．前各号に掲げる事項に違反した場合における契約の解除等の措置及び損害賠償に関する事項

・ 委託業務主管課の情報管理者は、委託先において事故が発生したときは、速やかにその状況を調査し、必要な措置を講じるとともに、その旨を総括情報管理者に報告しなければならない。

（４）パスワード等の管理

・ 職員は、自己の保有するパスワードについて、不用意にもらしたりメモを作ったりしないようにするなど、パスワードの秘密保持に努めなければならない。

（５）接続時間の制限

・ 職員は、情報システムへの接続については、必要最小限の接続時間で行うように努めるものとする。

４　物理的セキュリティ

（１）入退室の管理

- 情報管理者は、重要性分類Ⅰ・Ⅱの行政情報の記録されている媒体保管場所及びそれを取り扱う情報機器の設置場所への入退室の管理について必要な措置を講じなければならない。

（２）電子計算機室等

- 総括情報管理者は電子計算機室を管理し、電子計算機室への入室は、鍵等により許可されていない立入りを防止しなければならない。
- 電子計算機室内は、空調、耐震等の対策を講じるとともに、機器及び記録媒体に影響を与えない防火措置を施さなければならない。なお、電子計算機室内の機器類の配置は、緊急時に職員が円滑に非難できるように配慮しなければならない。
- 電子計算機室の入退室する場合は、必ず入退室管理簿に記載し、外部委託事業者は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。
- 電子計算機室等へ機器等を搬入・搬出する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、職員による確認を行い、機器等の搬入・搬出には、職員が立ち会う等の必要な措置を講じなければならない。

（３）職員の情報システムの機器管理

- 職員は執務室に職員が不在となる場合には、施錠するなど部外者の侵入を防ぐ措置を講じなければならない。

（４）電源

- 停電及び電圧異常等によりデータ等が破壊され、業務処理に支障を来す恐れのある情報システム等の機器の電源は、当該機器を適切に停止するまでの間に必要な電力を供給する容量の予備電源を備え付ける等の措置を講じなければならない。

（５）配線

- 配線は、傍受又は損傷等を受けることがないよう可能な限り必要な措置を施さなければならない。
- 主要な箇所の配線は、損傷等についての定期的な点検を行わなければならない。

５　技術的セキュリティ

（１）情報システムの管理

①　情報システム管理記録の作成と管理

- 情報管理者は、所管する情報システムにおいて行ったシステムの変更作業を記録し、適切に管理しなければならない。

②　情報システム仕様書の管理

- 情報管理者は、仕様書を最新の状態にしなければならない。また、システムの仕様変更等の処理を行った場合は、その記録を作成しなければならない。
- 情報管理者は、仕様書を業務上必要とする者のみが閲覧できる場所に保管しなけ

ればならない。

③　アクセス記録の取得

- 情報管理者は、情報システムの各種アクセス記録及びセキュリティ確保に必要な記録を可能な限り取得し、一定の期間保存しなければならない。
- 情報管理者は、情報システムのアクセス記録が、窃取、改ざん又は消去されないように必要な措置を講じなければならない。
- 情報管理者は、情報システムのアクセス記録を可能な限り分析し、監視しなければならない。

④　障害記録の作成

- 総括情報管理者は、職員等から報告のあった情報、システムの障害に対する処理または問題等は障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

⑤　バックアップの取得

- 情報管理者は、情報システムの重要性分類Ⅰ・Ⅱの行政情報については、外部媒体へのバックアップを取り、施錠等のできる安全な場所へ保管しなければならない。

⑥　ソフトウェアの導入に関する注意

- 職員は、新たにソフトウェアを導入する場合は、総括情報管理者の許可を得なければならない。
- 職員は、正規のライセンスのないソフトウェアを導入してはならない。
- 職員は、業務上不必要なソフトウェア及び出所不明なソフトウェア等安全性が確認されないソフトウェアをインストールしてはならない。
- 職員は、導入されているソフトウェアを適切に運用管理しなければならない。

⑦　メールの送受信等

- 職員は、メールの自動転送機能を用いて、業務上不必要な者へ職場のメールを転送してはならない。
- 職員は、不審なメールを転送してはならない。
- 職員は、重要性分類Ⅱの行政情報に該当する添付ファイルのあるメールを送信する必要がある場合には、事前に情報管理者の承認を受けなければならない。
- 職員は、外部からソフトウェアを取り入れる場合は、事前に情報管理者の承認を受けなければならない。
- 職員は、差出人が不明な、又は不自然なファイルが添付されたメールを受信した場合は、情報管理者に報告するとともに、直ちに廃棄しなければならない。

⑧　暗号化

- 暗号化については、統括情報管理者が定める方法を用いなければならない。
- 暗号のための鍵は、重要性分類Ⅰの行政情報として厳重に管理しなければならない。

⑨　職員以外の者が利用できる情報システム

・ 情報管理者は、職員以外の者が利用できる情報システムについては、情報セキュリティ対策について特に強固な対策を取らなければならない。

⑩　情報システムの入出力データ

・ 情報管理者は、情報システムの入力されるデータの適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

・ 情報管理者は、情報システムから出力されるデータの処理が正しく行われていることを確認しなければならない

⑪　業務目的以外の使用の禁止

・ 職員は、業務目的以外での情報システムへのアクセス及びメールの使用を行ってはならない。

（２）情報システムアクセス制御

①　利用者登録

・ 情報管理者は、情報システムの利用者の登録、変更、抹消等については、情報システム毎に定められた方法に従って行わなければならない。

・ 利用者登録、変更等は、情報システムを所管する情報管理者に対する申請により行わなければならない。

②　マイナンバー利用事務系へのアクセス制御

・ 原則として他の領域と通信できないようにした上で、端末からの情報持ち出し規制設定や端末への多要素認証の導入により、住民情報の流失防止の措置を講じなければならない。

③　LGWAN 接続系へのアクセス制御

・ LGWAN 通信を要する業務用システムとインターネット接続系のシステムの通信経路を分割し、両システム間での通信する際には無害化通信を実施する。

④　インターネット接続系へのアクセス制御

・ 不正通信監視機能の強化等の情報セキュリティ対策を講じる。都道府県及び市区町村の通信を集約し、自治体情報セキュリティクラウドの導入等を実施する。

⑤　インターネット以外のネットワークへのアクセス制御

・ 総括情報管理者は、不必要なネットワークサービスにアクセスできないよう必要な措置を講じなければならない。

⑥　外部からのアクセス

・ 外部からのアクセスの許可は、必要最低限にしなければならない。

⑦　外部ネットワーク（クラウドサービス等）との接続

・ 外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成及び情報セキュリティレベル等を詳細に検討し、本町の情報資産に影響が生じないことを明確に確認したうえで、最高情報総括責任者の許可に基づき接続しなければならない。

- 総括情報管理者は、外部ネットワークとの接続を行うことで内部ネットワークの安全性が脅かされることの無いようにセキュリティ対策に努めなければならない。
- 接続した外部ネットワークの情報セキュリティに問題が認められた場合には、総括情報管理者は、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。
- 内部ネットワークの情報セキュリティに問題が認められた場合には、総括情報管理者は速やかに当該内部ネットワークを、外部ネットワークから遮断しなければならない。
- クラウドサービスを導入する場合には、利用ガイドラインを整備し対策を講じる。
- ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

⑧　パスワード等の管理

- 情報管理者は、情報システムのＩＤ、パスワードを厳重に管理しなければならない。
- 情報管理者は、情報システムのネットワーク並びにネットワーク上で利用する各種サービスのＩＤ、パスワードを適切に管理しなければならない。

（３）情報システムの開発・導入・保守

①　情報システムの開発・導入

- 情報管理者は、情報システムのソフトウェアを開発・導入する場合は、情報セキュリティ上問題にならないかどうか確認しなければならない。
- 情報管理者は、情報システムのソフトウェアを開発する場合は、ソフトウェアの仕様書、ネットワーク構成図等を整備しなければならない。
- 情報管理者は、開発したソフトウェアを情報システムに取り入れる場合は、既に稼動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。

②　情報システムの変更管理

- 情報管理者は、重要な情報システムを追加、変更、廃棄等した場合は、その際の設定・構成等の履歴を記録・保存し、必要な場合には復旧できるようにしなければならない。

③　ソフトウェアの保守及び更新

- 情報管理者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切な保守が行われるようにし、その不具合については、速やかに修正等の対応を行わなければならない。
- 情報管理者は、情報システムのソフトウェアの更新等については、計画的に実施しなければならない。

④　機器の修理及び廃棄

・ 記録媒体の含まれる機器を、外部の業者に修理させる場合又は貸借期限終了等により廃棄する場合は、可能な範囲でバックアップを取り、記録媒体内のすべての行政情報を消去しなければならない。なお、故障を外部の業者に修理させる際、行政情報を消去することが難しい場合は、修理を委託する業者と守秘義務を明記した契約を締結しなければならない。

⑤　機器構成の変更

・ 職員は、情報システムの機器について改造又は機器の増設・交換を行ってはならない。
・ 職員は、情報システムの機器について業務を遂行するため機器の増設・交換を行う必要がある場合には、情報管理者の許可を得なければならない。

（４）コンピュータウイルス対策

①　総括情報管理者は、次の事項を実施しなければならない。

・ 情報システムのサーバ及び必要な機器にウイルス対策ソフトを導入すること。
・ ウイルスチェック用のパターンファイルは常に最新のものに保つこと。
・ 定期的に新種のウイルスに関する情報収集や情報システム内部の感染状況等について情報収集をすること。
・ コンピュータウイルス情報について、職員に対する注意喚起を行うこと。
・ コンピュータウイルスについて、職員に対して必要な啓発活動を行うこと。

②　職員は、次の事項を遵守しなければならない。

・ 外部からデータ又はソフトウェアを取り入れる場合、及び外部に持ち出す場合には、必ずウイルスチェックを行うこと。
・ ウイルスチェックの実行を途中で止めないこと。
・ 添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行うこと。
・ 総括情報管理者が提供するコンピュータウイルス情報を常に確認すること。

（５）不正アクセス対策

・ 総括情報管理者は、セキュリティホール等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録・保存しなければならない。
・ 総括情報管理者は、本町ネットワークに不正な侵入や利用があった場合に探知等できるよう、適切な対策に努めなければならない。
・ 総括情報管理者は、本町ネットワークに攻撃を受けていることが明らかな場合には、ネットワークの停止を含め必要な措置を講じなければならない。
・ 職員により本町ネットワークに対して不正なアクセスがあった場合は、総括情報管理者は当該職員が所属する情報管理者に通知し、適切な処置を求めなければならない。
・ 総括情報管理者は、外部ネットワークより不正アクセスがあった場合は、最高情

報総括責任者に報告し、適切な措置を講じなければならない。

（６）セキュリティ情報の収集

- 情報管理者は、重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。
- 総括情報管理者は、セキュリティに関する情報について、国及び関係団体、民間事業者等から適宜情報を収集し、職員に対して必要な啓発活動を行わなければならない。

６　運用

（１） 情報システムの監視

- 情報管理者は、情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

（２） 情報セキュリティポリシーの遵守状況の確認

- 総括情報管理者は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じていないかについて確認を行わなければならない。

（３） セキュリティ障害時の対応

- セキュリティ障害が発生した場合には、総括情報管理者及び情報管理者はすみやかに対応するとともに、再発防止の措置を講じなければならない。

①　障害拡大の防止措置

- 総括情報管理者は、故意の不正アクセス又は不正操作により、情報システムに障害を及ぼすことが明らかな場合には、情報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。
- 総括情報管理者は、情報システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。

②　障害の調査

- 情報管理者は、セキュリティ障害が発生した場合、障害の発生を速やかに最高情報総括責任者へ報告するとともに、次の項目について調査をしなければならない。
  ア．障害の内容
  イ．障害が発生した原因
  ウ．確認した被害、影響範囲
- 調査した内容は速やかに最高情報総括責任者へ報告しなければならない。ただし、障害の程度が軽微なものについては報告を要しないものとする。

③　障害への対応

- 情報管理者は、総括情報管理者の指示の下に速やかにセキュリティ障害を復旧し、その措置について最高情報総括責任者に報告しなければならない。

・ 障害が外部に重大な影響を及ぼすおそれがある場合には、情報管理者は速やかに最高情報総括責任者に報告のうえ必要な指示を仰がなければならない。

④ 再発防止の措置

・ 情報管理者は、必要な再発防止の措置を講じるとともに、その結果を最高情報統括責任者に報告しなければならない

7 法令等遵守

・ 職員は、使用する情報資産について、次の法令等を遵守しなければならない。

１．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）

２．著作権法（昭和４５年法律第４８号）

３．行政機関の保有する個人情報の保護に関する法律（平成１５年法律第９５号）

４．只見町個人情報保護条例（平成１４年只見町条例第２３号）

また、マナーと倫理をもって情報システムを利用しなければならない。

8 評価・見直し等

・ 情報管理者は、当該部署の情報セキュリティが確保されていることを確認するため、自主点検を行い、必要に応じ改善措置を講じなければならない。

・ 統括情報管理者は、評価及び見直しが必要となる事象が発生した場合には、「只見町電子自治体推進本部」に諮り必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。