第１章　情報セキュリティ基本方針

１　情報セキュリティの目的

葛尾村（以下「村」という。）が取り扱う情報には、村民の特定個人情報を含む個人情報のみならず行政運営上重要な情報など、部外に漏えいや紛失等が発生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、これらの情報及び情報を取り扱う情報システムを適正に管理し、人的脅威や災害・事故等から防御することは、村民の財産、プライバシー等を守るためにも、また、事務の継続的かつ安全・安定的な運営並びに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。

このため、村民の個人情報を保護し、村の情報資産の重要性を維持し、「特定個人情報の適正な取扱いに関するガイドライン」を網羅した葛尾村情報セキュリティ基本方針、特定個人情報の取扱い基準及び情報セキュリティ対策基準により構成する**葛尾村情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）**を定め、情報セキュリティの確保に最大限に取り組むため基本的な事項を定めることを目的とする。

２　適用範囲

（1）執行機関の範囲

情報セキュリティポリシーが適用される村の執行機関は、村長部局、各行政委員会、議会事務局、及び村長が必要と認めた機関とする。

（2）情報資産の範囲

対象とする情報資産は、次のとおりとする。

① 特定個人情報を含む個人情報、及び行政運営上重要な情報

② ネットワーク及び情報システム並びにこれらに関する設備及び、電磁的記録媒体

③ 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。）

④ 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

３　組織体制・役割　※（　）は、国が定めたガイドラインによる役職名

（1）副村長（CISO：最高情報セキュリティ責任者）

※　CISO：Chief Information Security Officer

① 副村長は、村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 副村長は、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ことができる。

③ 副村長は、情報セキュリティポリシーに定められた自らの担務を、総務課長に担わせることができる。

（2）総務課長（統括情報セキュリティ責任者、監査責任者）

① 総務課長は、副村長を補佐し、副村長が指示した業務を代行する。

② 総務課長は、村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 総務課長は、村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 総務課長は、課長等、係長等、職員等に対して、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 総務課長は、村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、副村長の指示に従い、副村長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実施する権限及び責任を有する。

⑥ 総務課長は、村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・管理を行う権限及び責任を有する。

⑦ 総務課長は、緊急時等の円滑な情報共有を図るため、副村長、課長等、係長等及び職員等を網羅する連絡体制を含めた《**別表1　インシデント対応連絡先一覧**》により緊急連絡網を整備しなければならない。

⑧ 総務課長は、緊急時には副村長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ならない。

⑨ 総務課長は、情報セキュリティ関係規定に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて副村長にその内容を報告しなければならない。

⑩ 監査責任者とし、毎年度及び必要に応じて監査を行わなければならない。

(3) 課長等（情報セキュリティ責任者）

① 課長等は、村長部局の課長等、各行政委員会事務局及び議会事務局の長で、当該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 課長等は、その所掌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、総務課長及び副村長へ速やかに報告を行い、指示を仰がなければならない。

(4) 所管課長等（情報セキュリティ管理者）

① 所管課長等は、所管する課室等において所有する情報システムがある課長等で、その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。

② 所管課長等は、情報セキュリティに関する権限及び責任を有し、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並びに職員等に対する教育、訓練、助言及び指示を行う。

(5) 係長等（情報システム管理者）

① 係長等は、村長部局、各行政委員会事務局及び議会事務局の各係長で、所管する係等における情報セキュリティに関する権限及び責任を有する。

② 係長等は、その所掌する係等において、情報資産に対するセキュリティ侵害が発生した場合は課長等及び総務企画係長へ速やかに報告し、セキュリティ侵害のおそれがある場合には課長等へ速やかに報告を行い、指示を仰がなければならない。

(6) 所管係長等（情報システム担当者）

① 所管係長等は、所管する情報システムを管理する係長等で、システムの開発、設定の変更、運用、見直し等を行う権限及び責任を有し、所管課長等の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。

② 所管係長等は、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、運用しなければならない。

(7) 職員等（職員等）

① 職員等は、村の特定個人情報等を含むすべての情報資産に関する業務に携わる職員、非常勤職員、会計年度任用職員、外部団体職員及び業務受託者の職員をいう。

② 職員等は、インシデントを認知、又は県セキクラ等外部からインシデント発生の通知を受けた場合は、直ちに係長等及び総務企画係長に報告し、所管する情報システムにどのような影響が発生しているのか調査する。

③ 職員等は、本セキュリティポリシーを遵守しなければならない。

(8) 葛尾村電子社会推進本部

① 村の情報セキュリティ対策を統一的に実施するため、「葛尾村電子社会推進本部」において情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

② 葛尾村電子社会推進本部は、必要に応じて、村における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

(9) 総務企画係（CSIRT・PoCを兼務）

※ CSIRT：インシデント緊急即応チーム：Computer Incident Response Team、シーサート
※ PoC：情報セキュリティに関する統一的な窓口：Point Of Contact、ポック

① 「インシデント緊急即応チーム」及び「情報セキュリティに関する統一的な窓口」は総務課総務企画係とし、総務企画係長を責任者とする。

② 総務企画係長は、副村長及び総務課長を補佐し、係内の業務総括及び外部との連携等を行う。

③ 総務企画係長は、副村長及び総務課長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、その内容を関係課室等に提供しなければならない。

④ 総務企画係長は、情報セキュリティインシデントについて外部並びに課室等より報告を受け、又はインシデントを認知した場合には、その状況を確認し、総務課長、副村長、重要度が高い場合は県、総務省、特定個人情報の漏えい等で《**第2章4－3　個人情報保護委員会への報告**》、《**第2章4－4　本人への通知**》に該当する場合は個人情報保護委員会及び本人へ報告しなければならない。

⑤ 総務企画係長は、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表などの対応を行わなければならない。

⑥ 情報セキュリティに関して、関係機関や他の地方公共団体のPoC並びに委託事業者等との情報共有を行わなければならない。

(10) 兼務の禁止

① 情報セキュリティ対策の実施において、止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 情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

４ 遵守事項

４－１ 職員等の遵守義務

(1) 法令、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は次に掲げる法令等、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。

- 番号法等関係法令
- 地方公務員法(昭和25年法律第261号)
- 著作権法(昭和45年法律第48号)
- 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)
- 個人情報の保護に関する法律(平成15年法律第57号)
- サイバーセキュリティ基本法(平成26年法律第104号)
- 葛尾村個人情報保護条例等関係条例
- 地方公共団体における個人情報保護対策について(平成15年6月16日総行情第91号総務省政策統括官通知)等の関連通知
- 特定個人情報の適正な取扱いに関するガイドライン
- 特定個人情報保護評価を実施した事務については、その内容
- 接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置等

(2) 特定個人情報の適切な管理

個人番号利用事務等実施者は、個人番号(生存する個人のものだけでなく死者のものも含む。)の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。また、村は、保有個人情報である特定個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報である特定個人情報の適切な管理のために必要な措置を講じなければならない。

４－２ 懲戒処分等

(1) 懲戒処分の対象

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。

① 職員等が違反を確認した場合は、速やかに課長等及び総務課長に通知し、適切な措置を求めなければならない。

② 課長等が違反を確認した場合は、速やかに総務課長及び当該職員等の監督責任者に通知し、当該職員等への指導など必要かつ適切な措置を講じさせ、違反の事実関係について報告を求めなければならない。

③ 総務課長は、事実関係の報告及び事情聴取等により、当該職員等の故意又は重大な過失による違反であることを確認した場合又は監督責任者等の指導によっても改善されないと判断できる場合は、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あるいは剥奪することができる。その後、総務課長は、速やかに職員等の権利を停止あるいは剥奪した旨を副村長、全ての課長等及び当該職員等の監督責任者に通知しなければならない。

4－3　罰則の強化

番号法第48条から第55条の3まで〔罰則〕においては、「行政機関の保有する個人情報の保護に関する法律」、「独立行政法人等の保有する個人情報の保護に関する法律」及び「住民基本台帳法」における類似の刑の上限が引き上げられている等、《**表1　罰則一覧表**》のとおり罰則が強化されている。

また、番号法第56条〔罰則〕により項番①から⑤までは、日本国外においてこれらの罪を犯した者にも適用される。

表1　罰則一覧表

項番	行　　為	番号法	同種法律における類似規定の罰則	
			行政機関 個人情報保護法	住民基本台帳法
①	個人番号利用事務等に従事する者又は従事していた者が、正当な理由なく、特定個人情報ファイルを提供	4年以下の懲役若しくは200万円以下の罰金又は併科 （第48条）	2年以下の懲役又は100万円以下の罰金 （第53条）	―
②	上記の者が、不正な利益を図る目的で、個人番号を提供又は盗用	3年以下の懲役若しくは150万円以下の罰金又は併科 （第49条）	1年以下の懲役又は50万円以下の罰金 （第54条）	2年以下の懲役又は100万円以下の罰金 （第42条）
③	情報提供ネットワークシステムの事務に従事する者又は従事していた者が、情報提供ネットワークシステムに関する秘密を漏えい又は盗用	同上 （第50条）	―	同上 （第42条）
④	人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入、不正アクセス等により個人番号を取得	3年以下の懲役又は150万円以下の罰金 （第51条）	―	―
⑤	国の機関の職員が、職権を濫用して、専らその職務の用以外の用に供する目的で、特定個人情報が記録された文書等を収集	2年以下の懲役又は100万円以下の罰金 （第52条）	1年以下の懲役又は50万円以下の罰金 （第55条）	―
⑥	個人情報保護委員会から命令を受けた者が、個人情報保護委員会の命令に違反	2年以下の懲役又は50万円以下の罰金 （第53条）	―	1年以下の懲役又は50万円以下の罰金 （第43条）
⑦	個人情報保護委員会に対する、虚偽の報告、虚偽の資料提出、検査拒否等	1年以下の懲役又は50万円以下の罰金 （第54条）	―	30万円以下の罰金 （第46条、第47条）
⑧	偽りその他不正の手段により個人番号カード等を取得	6月以下の懲役又は50万円以下の罰金 （第55条）	―	30万円以下の罰金 （第46条）

５　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て情報セキュリティ監査及び自己点検を実施する。

６　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が必要となった場合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。

７　情報セキュリティ対策基準の策定

情報セキュリティポリシーを実施するために、具体的な遵守事項及び判断基準等を《**第2章　特定個人情報の取扱い**》及び《**第3章　情報セキュリティ対策基準**》のとおり定める。

８　情報セキュリティ実施手順の策定

各情報システムの担当係長は、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村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。