多賀町住民基本台帳ネットワークシステム緊急時対応計画

多賀町税務住民課

令和３年６月策定

第１版

第１章　総則

１　目的

この計画は、多賀町住民基本台帳ネットワークシステム管理規程(令和３年多賀町規程第１号)に基づき、住民基本台帳ネットワークシステム(以下「住基ネット」という。)の障害等によりシステムの全部または一部が停止した場合およびセキュリティを侵犯する不正行為等により住民基本台帳データ(以下「住基データ」という。)の漏えいまたは漏えいのおそれがあると認める場合における本町の緊急時対応計画を定める。

２　緊急時の区分

住基ネットに係る緊急時は、以下の２つに区分する。

区分	事象
障害	電子計算機、端末装置の故障その他の事故、電算室の火災その他事故により、住基ネットで使用するハードウェア、ソフトウェアおよびネットワーク機能の正常性が喪失または、そのおそれがある状態をいう。 （例）コミュニケーションサーバ（以下「CS」という。)、端末機器の故障 システムのバグ ネットワーク回線の不通、交換機・ハブの故障
不正行為	電子計算機における不正行為または電子計算機への不正アクセス行為により、住基ネットの目的使用、住基ネットの運用を阻害する行為等、本人確認情報に脅威を及ぼすおそれがある場合をいう。 （例）CS における不正行為 CS への不正アクセス行為 コンピュータウィルスの侵入　等

第２章　機器障害

１　緊急時連絡網

緊急時の初動体制を円滑に行うために、多賀町と滋賀県および指定情報処理機関（以下「全国センター」という。）の緊急時連絡網を整備する。

２　障害の区分に係る緊急時の対応手順

障害の区分に係る緊急時の事象が発生した場合の対応については、以下の手順により行うこととする。

手順１　【障害の特定・原因の究明】

①　障害を発見した職員は、直ちに住基ネット担当者に状況を報告するとともに以下の障害の種類に応じた確認方法により、障害の種類および箇所を特定し原因の究明を行う。また、原因の究明が困難な場合には、必要に応じ保守委託事業者、滋賀県または全国センター等に連絡を行い障害の特定と原因の究明を行う。

障害の種類	事象	確認方法
ハードウェアの障害	故障、停電　等	警告ランプの確認・形状異常の確認　等
ソフトウェアの障害	バグ　等	バグ情報の確認、業務イベントログ解析等
ネットワークの障害	交換機、ハブ故障、庁内回線の切断等	警告ランプの確認 コマンドによる確認・目視チェック　等

②　住基ネット担当者は、必要に応じ保守作業を依頼するとともに、障害の状況・原因・支障の程度等をセキュリティ責任者に報告する。

③　セキュリティ責任者は、障害の状況・原因・支障の程度等をシステム管理者を経て、セキュリティ統括責任者に報告する。

手順２　【サーバ等の動作に関する判断】

①　手順１の③の報告を受けたセキュリティ統括責任者は、直ちにシステム管理者を通じてセキュリティ責任者に対し、データ保護等について必要な指示を行う。

②　セキュリティ統括責任者は、サーバ等が正常に動作しない等、きわめて重大な障害により住基ネットが長時間にわたり停止すると判断したとき、その他必要があると認めるときは、速やかに町長に報告を行うとともに、その対策について協議するため、セキュリティ会議を招集しなければならない。

手順３　【セキュリティ会議】

①　セキュリティ統括責任者は、セキュリティ会議を招集する。

②　セキュリティ責任者は、セキュリティ会議において、障害の状況、原因、支障の程度等を報告するとともに、セキュリティ統括責任者の指示によるデータ保護等の措置については、その承認を得るものとする。

③　セキュリティ会議は、以下の項目について審議し、またセキュリティ統括責任者は、セキュリティ会議の議長となって、その結果について町長に報告する。

決定する項目	内容
機器等への対応	システムの完全停止、機能の一部停止 機器の一部切り離し、ネットワークからの切り離し
関係機関への連絡	全国センター、都道府県管理課、関係市町村　等
技術的支援依頼	全国センター、滋賀県、保守委託事業者　等
緊急体制の確立	役割分担、指揮命令系統の確認
町民への対応	来庁者への対応、問い合わせ対応、苦情処理
広報対応	ホームページ等での告知、情報資料提供、記者発表　等
代替措置の実施	業務ごとに住基ネットが停止した場合の措置を検討し、当該措置を実施する
再開運用の決定	障害復旧状況および本人確認情報の整合性等の報告を受け、運用再開の決定を行う

手順４　【保守作業の実施】

セキュリティ責任者は、直ちに修理、復旧その他の措置を実施する。

手順５　【運用の再開】

セキュリティ責任者は、本人確認情報の整合性を確認し、修復後、関係機関への連絡を行い、セキュリティ統括責任者の承認を経て、運用の再開をする。ただし、セキュリティ会議においてシステム停止等の決定を受け、その後運用を再開するときは、セキュリティ会議に対し、障害復旧状況および本人確認情報の整合性等の報告を行い、運用再開の決定を受けなければならない。

３　再発防止策

緊急時の状態が解消された後、再び同様の原因で障害が発生しないように、以下の技術面、運用面からの対策を検討する。

対策の種類	対応内容
技術面の対策	障害監視の強化 技術情報の収集
運用面の対策	定期点検実施時期の見直し オーバーホールの実施 予備装置の確保 教育･研修　等

第３章　不正行為

１　不正行為の区分に係る緊急時の対応手順

(A) 不正行為の脅威度

住基ネットのセキュリティを侵害する不正行為の脅威度について、以下の３つのレベルに区分する。

脅威度	本人確認情報等の脅威	事例
レベル１	本人確認情報等に脅威を及ぼすおそれがない場合	(1)　CS を設置する室または統合端末を設置する場所に無権限者が侵入しようとしたにもかかわらず、当該室または場所に侵入することができなかったもの (2)　レベル２およびレベル３に該当しないもの
レベル２	本人確認情報等に脅威を及ぼすおそれが低い場合	(1)　本人確認情報等が記録されていない磁気ディスクまたは本人確認情報等を保護する上で重要ではないソフトウェアもしくはドキュメント（システム設計書、プログラム説明書、事務説明書、CS および統合端末の操作手引書その他の要領および仕様を記した書類をいう。以下同じ。）等を保管する場所への無権限者の侵入 (2)　ファイアウォールを通過しなかった不正アクセス (3)　コンピューターウィルス対策ソフトウェアによるコンピューターウィルスの検出 (4)　(1)～(3)に該当するもののほか、本人確認情報等に脅威を及ぼすおそれが低いもの
レベル３	本人確認情報等に脅威を及ぼし、または及ぼすおそれが高い場合	(1)　本人確認情報等が記録されている磁気ディスクまたは本人確認情報等を保護する上で重要なソフトウェアもしくはドキュメント等を保管する場所への無権限者の侵入 (2)　ファイアウォールを通過した不正アクセス (3)　正当な権限によるものと確認することができない統合端末等の操作 (4)　コンピューターウィルスの侵入によるシステムの異常動作 (5)　本人確認情報等の不正利用またはそのおそれを生じさせるもの (6)　(1)～(5)に該当するもののほか、本人確認情報等に脅威を及ぼし、または及ぼすおそれが高いもの

(B) 不正行為の対応手順

不正行為の区分に係る緊急時の対応については、以下の手順により行うこととする。

手順１【状況の把握】

①　不正行為を発見した職員は、直ちにセキュリティ責任者に報告を行う。

②　不正行為を発見した場合の報告は、次の項目を正確かつ詳細に把握し行うこととする。

（ア）不正行為を発見した時期および不正行為があったと認められる時期
（イ）不正行為が発生した機器およびその設置場所
（ウ）不正行為および想定される被害等
（エ）報告するまでに行った応急措置等の有無

③　住基ネット担当者は、①の国および滋賀県または全国センターからセキュリティを侵犯する不正行為に係る通報がなされた場合において、情報を把握するために次の措置をとるものとする。
（ア）住基ネット担当者は、不正行為に係る情報を集約する。
（イ）住基ネット担当者は、事象の調査・分析を実施する。
（ウ）不正行為の脅威レベルがレベル２またはレベル３に該当する可能性が高い場合、滋賀県および全国センターと相互に連絡調整を行い、被害状況を把握するための措置等の対応を依頼する。

④　③で情報の把握を行った住基ネット担当者はセキュリティ責任者を通じシステム管理者およびセキュリティ統括責任者に報告する。

手順２【緊急措置の実施】

手順１の④の報告を受けたセキュリティ統括責任者は、町長に報告するとともに直ちにシステム管理者を通じてセキュリティ責任者に対し、データ保護等について必要な指示を行い、当該指示を受けた住基ネット担当者は、次のとおり緊急措置を実施する。

①　緊急措置の実施にあたっては、全国センター、滋賀県、企画課、保守委託事業者等と連絡調整を図り、被害拡大を防止するための措置等、必要な協力を要請する。

②　不正行為の脅威度がレベル３に該当する可能性が高い場合、必要に応じて、システムの停止（機能の一部停止、機器の一部切り離し、ネットワークからの切り離しを含む。）を行う。

③　また、不正行為の脅威度がレベル３に該当する可能性が高い場合、必要に応じて、関係者からの報告の聴収、関係者への調査等必要な措置を講じる。

④　全国センターから本人確認情報の提供を受けた機関等において、不正行為の発生が認められるときは、当該機関等からの報告の聴収、当該機関等への調査、保有情報の廃棄等必要な緊急措置の実施を要請するとともに、講じた措置について報告を要請する。

手順３　【不正行為の脅威度の判定】

セキュリティ管理者は、全国センター、滋賀県、企画課、保守委託事業者等と連絡調整を図り、当該事象の脅威度を判定し、次のとおり緊急時の対応を行う。

①　不正行為の脅威度がレベル１に該当する場合、庁内で必要な報告を行い、緊急時対応を解除する。

②　不正行為の脅威度がレベル２または３に該当する場合、セキュリティ管理者は、直ちに原因の解明を行い、その対策の実施について、システム管理者を経てセキュリティ統括責任者に報告する。

③　不正行為の脅威度がレベル２に該当する場合、セキュリティ統括責任者は、本人確認情報への脅威が生じる可能性があること等を踏まえ、必要があると認めるときは、セキュリティ会議を召集し、セキュリティ管理者に、不正行為の状況、原因、対応策等を報告させるものとする。

④　不正行為の脅威度がレベル３に該当する場合、セキュリティ統括責任者は、本人確認情報への脅威が生じる可能性が高いと判断したとき、その他必要があると認めるときは、速やかに町長に報告を行うとともに、その対策について協議するため、セキュリティ会議を招集しなければならない。

手順４　【セキュリティ会議】

①　セキュリティ統括責任者は、セキュリティ会議を招集する。

② セキュリティ管理者は、セキュリティ会議において、不正行為の状況、原因、支障の程度等を報告するとともに、セキュリティ統括責任者の指示による緊急の措置等については、その承認を得るものとする。
③ セキュリティ会議は、以下の項目について協議し、またセキュリティ統括責任者は、セキュリティ会議の議長となって、以下の項目について決定し、セキュリティ会議の内容、決定事項について速やかに町長に報告を行う。

決定する項目	内容
システムへの措置	システムの完全停止、機能の一部停止 機器の一部切り離し、ネットワークからの切り離し
関係機関への連絡	全国センター、都道府県管理課、関係市町村　等
技術的支援依頼	全国センター、滋賀県、保守委託事業者　等
緊急体制の確立	役割分担、指揮命令系統の確認
町民への対応	来庁者への対応、問い合わせ対応、苦情処理
広報対応	ホームページ等での告知、情報資料提供、記者発表　等
代替措置の実施	業務ごとに住基ネットが停止した場合の措置を検討し、当該措置を実施する
緊急措置の見直し判断	追加措置 復旧作業等緊急時対応の進捗状況 恒久対策の立案　等
再開運用の決定	障害復旧状況および本人確認情報の整合性等の報告を受け、運用再開の決定を行う

手順５　【原因の究明と復旧措置】

セキュリティ統括責任者は、必要に応じて、全国センター、滋賀県、企画課、保守委託事業者等と協力し、収集したアクセスログ等により原因を究明し、適切な復旧措置を実施する。

手順６　【運用の再開と緊急措置の見直し】

① セキュリティ管理者は、本人確認情報の整合性を確認し、修復した後、セキュリティ統括責任者の承認を経て、運用を再開する。ただし、セキュリティ会議においてシステム停止等の決定を受け、その後運用を再開する時は、セキュリティ会議に対し、障害復旧状況および本人確認情報の整合性等の報告を行い、運用再開の決定を受けなければならない。
② 運用再開に当たっては、必要に応じて、アクセス権限の設定変更、町民サービスの停止解除等を実施する。
③ セキュリティ統括責任者は、町長へ報告を行う。
④ 全国センター、滋賀県、関係する都道府県および市区町村の住基ネットの担当者等へ連絡する。本人確認情報管理責任者は、本町の住基ネットにおいてセキュリティを侵犯する不正行為を発見した場合、または県、他の地方公共団体、指定情報処理機関等からセキュリティを侵犯する不正行為に係る通報がなされた場合等において、次により状況を把握し、緊急措置を行う。

２　恒久対策の実施

緊急時の状態が解消された後に、セキュリティ会議において恒久対策を審議し、それに基づいた対策を実施する。

第４章　その他

１　緊急連絡網

緊急時の連絡先は以下の通りとする。

滋賀県総務部市町振興課　通常業務時
TEL　077―528―3233
滋賀県総務部市町振興課　夜間・休日時
TEL　077―563―3750
指定情報処理機関
TEL　03―5214―0908