所沢市住民基本台帳ネットワークシステム
緊急時対応計画書(不正行為編)

所沢市住民基本台帳ネットワークシステムセキュリティ会議

1 本計画書の目的

本計画書は、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。)のセキュリティを侵犯する不正行為が発生した場合において、不正行為の脅威度に応じて適切な対応を行なうために策定した計画書であり、「電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準」(平成14年6月10日総務省告示第334号)第2-5、「住民基本台帳ネットワークシステムセキュリティ基本方針書－本人確認情報の安全確保措置－」(平成12年9月25日住民基本台帳ネットワークシステム推進協議会決定)」方針10、及び「所沢市住民基本台帳ネットワークシステムセキュリティ規程」(平成14年訓令第15号、以下「規程」という。)第29条に基づいている。

なお、本計画書の運用にあたっては、住民基本台帳ネットワークシステムセキュリティ基本方針書方針5「本人確認情報保護の優先」に基づき、本人確認情報の保護を最優先とした措置を講じるものとする。

2 不正行為の脅威度

本対応計画において、住基ネットのセキュリティを侵犯する不正行為の脅威度については、以下の3つに区分する。

脅威度	事象	事例
レベル1	本人確認情報に脅威を及ぼすおそれのない事象	・住基ネットに関係がある備品がない場所（規程9条1項に規定されていない室）への無権限者※1の侵入
レベル2	本人確認情報に脅威を及ぼすおそれの低い事象	・住基ネットに関係があるが、本人確認情報が記録されていない磁気ディスク、本人確認情報の保護とは関係がないソフトウェア、ドキュメント等のある場所（規程9条1項におけるセキュリティ区分レベル1の室）への無権限者の侵入 ・ファイアウォールを通過しなかった、外部からの不正アクセス ・ウィルス対策ソフトによる、コンピュータウィルス等の検出
レベル3	本人確認情報に脅威を及ぼすおそれの高い事象	・本人確認情報が記録されている磁気ディスク、本人確認情報を保護するうえで重要なソフトウェア、ドキュメント等のある場所（規程9条1項におけるセキュリティ区分レベル2の室）への無権限者の侵入 ・ファイアウォールを通過した、外部からの不正アクセス ・業務端末等の不審な操作の検出 ・コンピュータウィルス等の侵入によるシステムの異常動作 ・本人確認情報保護に関する重大な脆弱性の発見

※1 本計画書において「無権限者」とは、住基ネットの操作権限を持たない者（職員を含む）のうち、入退室の許可を得ていない者をいう。

3 緊急時の対応手順

手順1 状況の把握

各担当者は、本人確認情報に脅威を及ぼすおそれのある事象を発見した場合、いつ(時刻)・どこで(場所)・何を(内容)・どうした等の内容を正確に把握し、システム管理者に報告する。

手順2 緊急措置

システム管理者は、考え得る対応策のうち、サーバの停止、ネットワークの切断など、緊急に実施する必要性が高いものを直ちに着手する。

不正行為の脅威度がレベル2・3に該当する可能性が高い場合は、埼玉県総合政策部市町村課住基ネット担当(以下「市町村課」という。)に通報を行う。また、必要に応じて、関係ベンダーの助言を得る。なお、何らかの理由で市町村課に連絡がつかない場合は、直接、指定情報機関に通報する。

手順3 本人確認情報に重大な脅威を及ぼすおそれの有無の判断

システム管理者は、不正行為の脅威度を判断し、脅威度に応じた対応をとる。

・不正行為の脅威度がレベル1の場合

通報者に脅威がない旨を伝え、緊急時の対応を解く。

・不正行為の脅威度がレベル2・3の場合

直ちに原因の解明を行い、対応策を実施する。

・不正行為の脅威度がレベル3の場合

直ちに原因の解明を行い、対応策を実施する。本人確認情報に重大な脅威があるとシステム管理者が判断した場合には、セキュリティ統括責任者にセキュリティ会議の開催を具申する。

なお、不正行為の脅威度がレベル2であっても、システム管理者が必要と認めるときは、セキュリティ会議の開催を具申することができる。

手順４　セキュリティ会議

セキュリティ統括責任者は、事前に定めた連絡網（別紙）を利用して、セキュリティ会議のメンバーを招集する。

セキュリティ統括責任者は、議長となって以下の項目について決定する。

・緊急時体制の確立

・住民への対応

・関係機関への連絡（警察への通報も含む）

・詳細な被害状況等の把握

・指定情報処理機関への支援要請

・広報

手順５　原因の究明

システム管理者は、被害情報、ログ情報、記録簿及び管理簿等を分析し、不正が行われた時期、場所、方法を究明する。必要に応じて、指定情報機関、市町村課及び関係ベンダーからの支援を得る。

手順6　緊急措置の見直し及び恒久対策の立案

システム管理者は、既に実施した緊急措置を見直し、アクセス権限の設定変更、操作者用ICカードの再発行、サーバの起動及びネットワークの接続等を実施する。また、セキュリティ会議を中心として、恒久対策を立案する。その際、必要に応じて、指定情報機関、市町村課、及び関係ベンダーからの支援を得る。

不正行為の対応手順イメージ図

（所沢市で不正行為が起きた場合）