国立市住民基本台帳ネットワークシステム緊急時対応計画

１　目的

本計画書は、国立市住民基本台帳ネットワークシステムの適正な管理に関する条例（平成２３年１２月国立市条例第２２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。）を構成する機器等の障害等によりその稼働が停止した場合、若しくはそのおそれがある場合、又は不正行為により住民基本台帳ネットワークシステムのセキュリティが侵害された場合、若しくはそのおそれがある場合（以下「緊急時」という。）に備えて、被害を未然に防ぎ、又は被害の拡大を防止し早急な復旧を図るため、必要な対応について定めることを目的とする。

２　緊急時対応の責任者

緊急時における情報の集約、原因の解明、対応策の実施等については、住基ネットセキュリティ統括責任者の指示のもと、住基ネット運用管理者が行う。

３　緊急時の区分

住基ネットにおける緊急時は、以下のとおり障害と不正行為の２つに区分し、緊急時対応計画は、それぞれの区分ごとの構成によるものとする。

区分	事象
障害	電子計算機、端末装置の故障その他の事故、電子計算機室の火災その他の事故により、住基ネットで使用するハードウェア、ソフトウェア及びネットワークの機能が正常に動作しない又はそのおそれのある状態をいう。 （例）コミュニケーションサーバ（以下「ＣＳ」という。）や 端末装置の故障 システムのバグ ネットワーク回線の不通、交換機・ハブ故障 等
不正行為	電子計算機における不正行為又は電子計算機への不正アクセス行為により、住基ネットの目的外使用、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 コンピュータウイルスの侵入 等

４　緊急時連絡網

緊急時の初動体制を円滑に行うために、国立市と東京都及び指定情報処理機関（以下「機構」という。）の緊急時連絡網を整備する。

５　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　障害を発見した市民課及び情報管理課の職員は、直ちに住基ネット運用副管理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、障害の種類及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又は東京都、機構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 住基ネット運用副管理者は、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・支障の程度等を住基ネット運用管理者に報告する。

③ 住基ネット運用管理者は、障害の状況・原因・支障の程度等を住基ネットセキュリティ統括副責任者を経て、住基ネット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の報告を受けた住基ネットセキュリティ統括責任者は、直ちに住基ネットセキュリティ統括副責任者を通じて住基ネット運用管理者に対し、データ保護等について必要な指示を行う。

②　住基ネット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、速やかに市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　住基ネット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　住基ネット運用管理者は、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、住基ネット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する。

④　住基ネット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審議し、その結果について市長に報告する。

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	機構・都道府県主管課・関係市町村　等
技術的支援依頼	機構・東京都・保守委託事業者　等
緊急時体制の確立	役割分担、指揮命令系統の確認

市民への対応	来庁者への対応・問合せ対応・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。(例　広域交付発行希望者に対し、発行可能な近隣市の事務所を案内する　等)
運用再開の決定	障害復旧状況及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〕

住基ネット運用管理者は、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〕

住基ネット運用管理者は、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、住基ネット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。

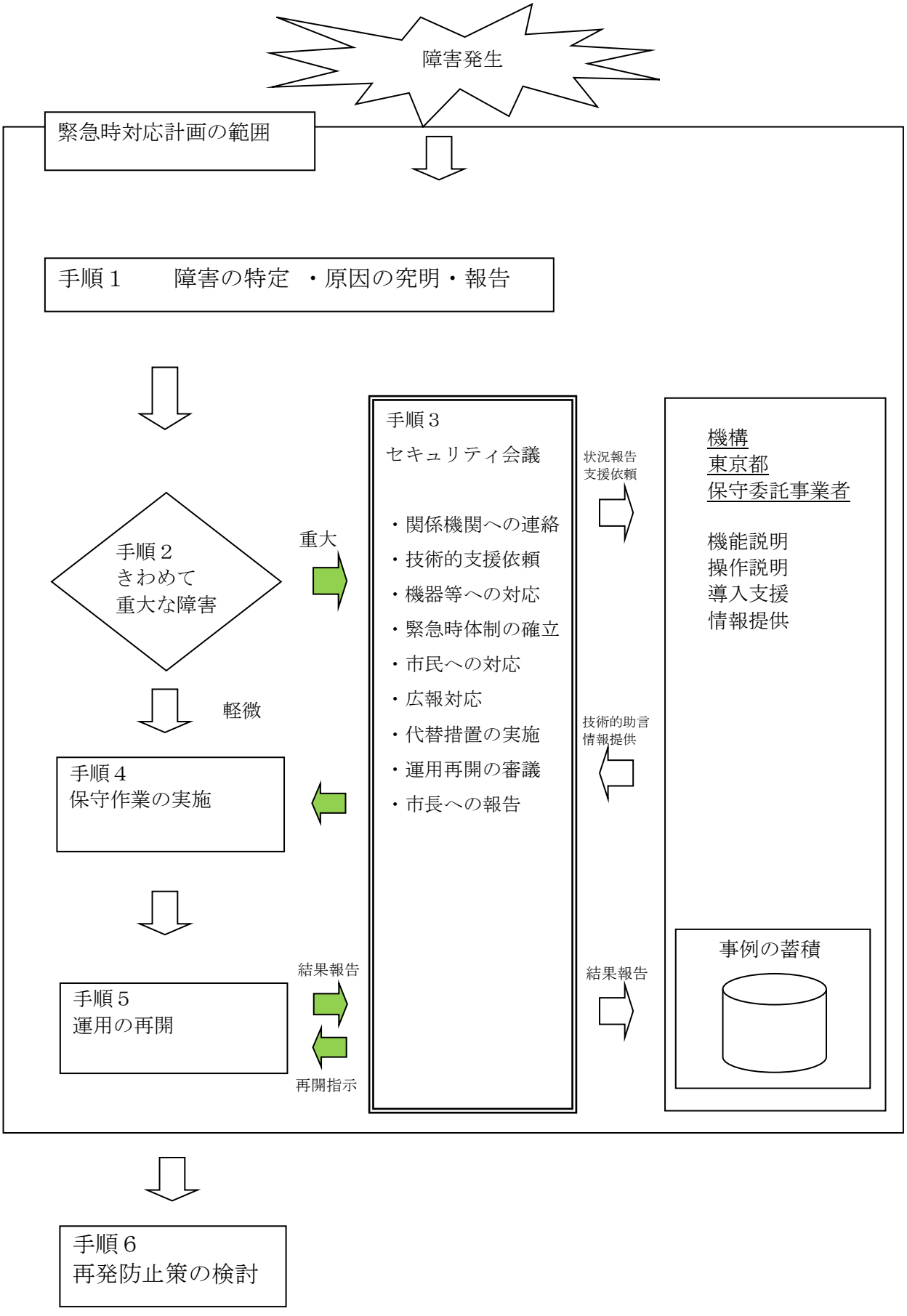
ただし、セキュリティ会議においてシステム停止等の決定を受け、その後運用を再開するときは、セキュリティ会議に対し、障害復旧状況及び本人確認情報の整合性等の報告を行い、運用再開の決定を受けなければならない。

6　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

障害対応のフロー図


障害発生
緊急時対応計画の範囲
手順１　　障害の特定　・原因の究明・報告
手順２
きわめて
重大な障害
重大
軽微
手順３
セキュリティ会議
・関係機関への連絡
・技術的支援依頼
・機器等への対応
・緊急時体制の確立
・市民への対応
・広報対応
・代替措置の実施
・運用再開の審議
・市長への報告
状況報告
支援依頼
技術的助言
情報提供
結果報告
機構
東京都
保守委託事業者
機能説明
操作説明
導入支援
情報提供
事例の蓄積
手順４
保守作業の実施
手順５
運用の再開
結果報告
再開指示
手順６
再発防止策の検討

7　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	○住基ネットに直接関係のない場所への無権限者の侵入 ○住基ネットに直接関係があるが認証等セキュリティ対策が施されている機器等に対する無権限者の接触でチェックがかかり侵入できなかったもの
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、ドキュメント等への無権限者の接触 ○外部からのファイアウォールを通過しなかった不正アクセス ○ウィルス対策ソフトによる、コンピュータウイルス等の検出
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上で重要なソフトウェア、ドキュメント等（以下「重要度の高い情報資産」という。）のある場所への無権限者の侵入 ○重要度の高い情報資産の盗難 ○住基ネット機器への直接的な毀損、破壊 ○外部からのファイアウォールを通過した不正アクセス（本人確認情報の盗取、改ざんを含む。） ○コンピュータウイルスによる住基ネットの異常動作及び破壊
		○業務端末等の不審な操作の検出 ○内部又は外部からの、住基ネットにおける本人確認情報の盗取、漏えい等、不正行為の事実の発見（それらが生じたと思われる事実の発見を含む） ○本人確認情報保護に関する重大な脆弱性の発見

(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市民課職員は、直ちに住基ネット運用管理者に報告を行う。

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及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及びその設置場所

（ウ）不正行為の内容及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　住基ネット運用管理者は、①の報告及び東京都又は機構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、情報を把握するために次の対応を取るものとする。

（ア）住基ネット運用管理者は、不正行為に係る情報を集約する。

（イ）住基ネット運用管理者は、システム担当者に指示を行い、事象の調査・分析を実施する。

（ウ）不正行為の脅威度がレベル２又は３に該当する可能性が高い場合、東京都及び機構

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運用管理者は、データ保護等に支障が生じ、又は生じるおそれがあるときは、不正行為の状況、支障の程度等を、住基ネットセキュリティ統括副責任者を経て住基ネット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の報告を受けた住基ネットセキュリティ統括責任者は、市長に報告するとともに直ちに住基ネットセキュリティ統括副責任者を通じて住基ネット運用管理者に対し、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運用管理者は、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、機構、東京都、情報管理課、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徴収、関係者への調査等必要な措置を講じる。

④　機構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徴収、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〕

住基ネット運用管理者は、機構、東京都、情報管理課、保守委託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又は３に該当する場合、住基ネット運用管理者は、直ちに原因の解明を行い、その対策の実施について、住基ネットセキュリティ統括副責任者を経て住基ネット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、住基ネット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、住基ネット運用管理者に、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、住基ネット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、速やかに市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　住基ネット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　住基ネット運用管理者は、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、住基ネット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する。
④　住基ネット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する
⑤　住基ネットセキュリティ統括責任者は、セキュリティ会議の内容、決定事項について速やかに市長に報告を行う。

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	機構 都道府県主管課、関係市町村　等
技術的支援依頼	機構 東京都、保守委託事業者　等
緊急時体制の確立	役割分担、指揮命令系統の確認
市民への対応	被害者への連絡・通知対応 問合せ対応・苦情処理
広報対応	情報資料提供・ホームページ等での告知 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
運用再開の決定	障害復旧状況及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〕

住基ネットセキュリティ統括責任者は、必要に応じて、機構、東京都、情報管理課、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　住基ネット運用管理者は、本人確認情報の整合性を確認し、修復した後、住基ネット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、障害復旧状況及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、操作者識別カードの再発行、市民サービスの停止解除等を実施する。
③　市長へ報告を行う。
④　機構、東京都、関係する道府県及び市区町村の住基ネットの担当者等へ連絡する。

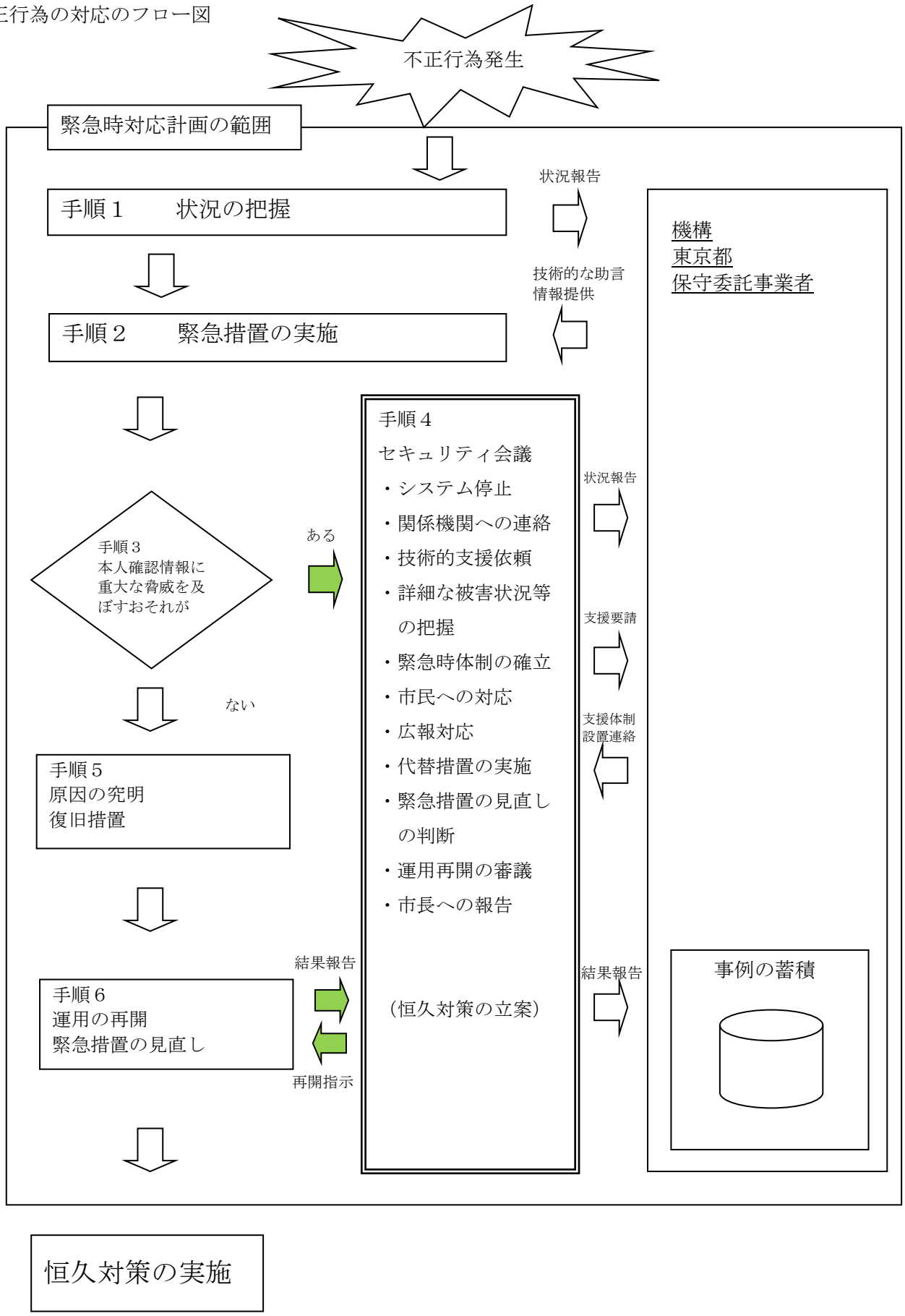
８　恒久対策の実施

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。

9　緊急措置

緊急時に講ずべき緊急措置は、当該事象の様態等に応じ、別表のとおりとする。

不正行為の対応のフロー図



恒久対策の実施