参考資料２

鳥取県住民基本台帳ネットワークシステム緊急時対応計画

鳥取県における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。）を構成するハードウェア、ソフトウェア及びネットワークの障害により住民サービスが停止する場合又は不正行為により本人確認情報に脅威を及ぼすおそれがある場合（以下「緊急時」という。）に、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、次のとおり緊急時の対応計画を定める。

第１　総則

１　定義

住基ネットにおける緊急時とは障害と不正行為の２つに区分され、それぞれの定義は次のとおりである。

（１）　障害

障害とは、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機能しなくなることをいう。

（２）　不正行為

不正行為とは、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。

２　緊急時連絡網

緊急時の初動対応を円滑に行うため、住民基本台帳ネットワークシステム全国センター（以下「全国センター」という。）、県及び市町村の緊急時連絡網を整備する。

第２　障害対応編

１　障害の発見

（１）　住基ネット担当者又は県がシステムの運用を委託した事業者（以下「住基ネット担当者等」という。）は、住基ネット運用中は常に機器を監視し、次のような状態が発生したときには障害としての対処を行う。

ア　県サーバの異常通報装置から異常を知らせる電子メールを受信したとき。
イ　県サーバのコンソールに異常を示すログ又はメッセージが表示されたとき。
ウ　県サーバに異常を示すランプが点灯したとき。
エ　県内ネットワーク監視装置に障害検知の表示がされたとき。
オ　業務端末を使用する職員から端末の異常を知らせる連絡があったとき。
カ　市町村又は全国センターから、県サーバ又は県内ネットワークの異常を知らせる連絡があったとき。

（２）　業務端末を使用する職員は、業務端末使用中に、次のような状態が発生した時には、障害としての対処を行う。

ア　業務端末に異常を示すメッセージが表示されたとき。
イ　業務端末が正常に起動又は動作しないとき。

2　障害時の連絡

（1）　住基ネット担当者等が障害を発見したときは、直ちにシステム管理者に状況を報告するとともに、必要に応じ通信事業者又は運用保守委託事業者等に連絡を行う。

なお、システム管理者は、異常により県サーバ、県内ネットワークの業務運用が不可能な場合は、直ちに全国センター及び関係する県の機関、市町村に障害発生、復旧見込みについて連絡する。

（2）　業務端末を使用する職員が異常を発見したときは、業務端末の再起動等の軽易な対応を行った上で、障害が復旧しない場合は、住基ネット担当者に連絡する。

その場合、次の事項について可能な限り把握を行い連絡すること。

ア　障害発生箇所
イ　電源投入又は起動の可否
ウ　画面に表示されているメッセージ等
エ　操作及び直前に行った操作内容
オ　障害メッセージ画面（業務端末画面）の最新状態

3　障害状況の把握

住基ネット担当者等は、障害発生の連絡を受けたときは、直ちに原因を調査し、障害の発生箇所、状況、程度、復旧見込時間等をシステム管理者に報告する。

なお、障害箇所が次の場合は、各担当部署又は事業者に原因の調査及び復旧対応等を依頼する。

項番	障　害　箇　所	担当部署（事業者）
①	住基ネット用専用回線	通信事業者
②	全国ネットワーク	全国センター
③	情報ハイウェイ（県域ＷＡＮ）	該当ネットワーク管理部門
④	住基専用ＬＡＮ	該当ネットワーク管理部門
⑤	住基ネット業務アプリケーション	全国センター
⑥	指定情報処理機関配布ソフトウェア	全国センター
⑦	住基ネット用ファイアウォール	全国センター
⑧	市町村機器	該当市町村

4　重大障害発生時の措置

（1）　システム管理者は、県サーバ、県内ネットワークが正常に作動せず、市町村の住基ネット運用部署又は県の住基ネット利用部署の業務への影響度を把握した上で極めて重大な障害で長期間に渡りシステムを停止する必要があると判断したときは、住民サービスへの影響や広報の必要性が生じる可能性が高いことを踏まえ、セキュリティ統括管理者に報告し、指示を仰ぐ。

（2） セキュリティ統括管理者は、４（１）の報告があった場合は、直ちに鳥取県住基ネットセキュリティ会議（以下「セキュリティ会議」という。）を開催する。

（3） セキュリティ統括管理者は、システムの停止（一部切離し、一部停止を含む。）、住民への対応、広報等の重要事項について指示を行う。

5　保守作業の実施

システム管理者は、必要に応じ運用保守委託事業者等に、修理、修復、交換を依頼する。

6　運用の再開

システム管理者は、障害復旧後、直ちに運用を再開する。

ただし、本人確認情報に影響する障害であった場合は、全国センター及び市町村と連携の上、本人確認情報の整合性の確認を行い、必要であれば修復した後に、運用を再開する。

第３　不正行為対応編

1　不正行為の脅威度

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、次の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備品のある場所への無権限者の侵入
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不正アクセス ・　ウイ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への無権限者の侵入 ・　ファイアウォールを通過した不正アクセス ・　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

2　システム管理者

システム管理者は、不正行為に係る情報を集約し、原因の解明、対応策の実施等を行う。

3　状況の把握

住基ネット利用部署等において、住基ネットのセキュリティを侵犯する不正行為を発見した場合、全国センター又は他の地方公共団体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、システム管理者は、状況を把握するため、次の対応を行う。

（1）　不正行為に係る情報は、住基ネット担当者を経由して、システム管理者に集約する。
（2）　運用保守委託事業者等に連絡し、その協力を得て、事象の調査・分析を行う。
（3）　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は、全国センターに通報し、全国センターにおいても状況把握を行うよう要請する。また、必要に応じ、関係する市町村の住基ネット担当部署に通報する。

4　緊急対応策の実施

システム管理者は、把握した状況等を基に、次のとおり運用監視の強化等の緊急措置を実施する。

（1）　緊急措置の実施に当たっては、全国センター、関係する市町村の住基ネット担当部署及び運用保守委託事業者等との協力の下で行う。
（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は、必要に応じて、システムの停止（一部切離し、一部停止を含む。）等の緊急措置を行う。
（3）　全国センター及び他の地方公共団体等が緊急措置を講じる必要がある場合は、当該団体に緊急措置の実施を要請する。

5　不正行為の脅威度の判定

システム管理者は、全国センター、関係する市町村の住基ネット担当部署及び運用保守委託事業者等との協力の下で、当該事象の脅威度の判定を行う。

なお、判定の結果により、次のとおり緊急対応策を行う。

（1）　レベル１の場合

セキュリティ統括管理者に報告を行い、緊急時対応を解く。

（2）　レベル２又は３の場合

直ちに原因の解明を行い、対応策を実施する。

6　重大不正行為発生時の措置

（1）　システム管理者は、不正行為の脅威度がレベル３に該当する場合は、住民サービスへの影響や広報の必要性が生じる可能性が高いことなど、全庁的な対応が求められることから、セキュリティ統括管理者に報告を行う。
（2）　セキュリティ統括管理者は、６（１）の報告があった場合は、直ちにセキュリティ会議を開催する。
（3）　セキュリティ統括管理者は、システムの停止（一部切離し、一部停止を含む。）、住民への対応、広報等の重要事項について指示を行う。

7　原因の解明

システム管理者は、必要に応じて、全国センター、関係する市町村の住基ネット担当部署及び運用保守委託事業者等と協力して、収集したログ等により、原因を解明する。

8　緊急措置の見直し及び恒久対策の立案等
システム管理者は、解明した原因等に基づき、次の対応を行う。

（1） 既に実施した緊急措置を見直し、必要に応じてシステム復旧等を行う。
（2） 恒久対策の立案を行うとともに、セキュリティ統括管理者に報告を行う。
（3） 全国センター、関係する市町村の住基ネット担当部署等に連絡する。

（別表） 緊急措置

No.	事　象	事　象　例	緊　急　措　置　の　例
1	不正アクセスの徴候を発見	1－1 全国センターから、不正アクセスの徴候を発見した旨の通報 ・ＩＤＳ及びＦＷ（全国センター管理）のログ解析で執拗な攻撃の痕跡を発見	①　全国センターが行う、不正アクセスの原因となった機器又はネットワークの推定作業に協力 ②　全国センターの要請等を踏まえ、当該機器又はネットワークについて、現地での調査を実施 ③　不正アクセスのパターンが本人確認情報に対する脅威となる場合は、全国センターが行う当該機器又はネットワークの住基ネットからの切離し作業に協力 ④　全国センターと連携して、関連機器のログ解析等を実施し、不正アクセス手段、不正アクセス者等の特定及び防止策の策定
		1－2 県において、不正アクセスの徴候を発見 ・ＦＷ又はデータベース（県の管理）のログ解析で執拗な攻撃の痕跡を発見	①　全国センターの協力を得て、ＦＷログ、データベースのアクセスログの詳細解析等を行い、不正アクセスの原因となった機器又はネットワークを特定（必要に応じ、全国センターのＩＤＳの監視項目増強、ログ解析強化、全国センターサーバデータベースのアクセスログの解析等の強化等を要請） ②　不正アクセスのパターンが本人確認情報に対する脅威となる場合は、全国センターと連携して、当該機器又はネットワークを住基ネットから切離し ③　全国センターと連携して、関連機器のログ解析等を実施し、不正アクセス手段、不正アクセス者等の特定及び防止策の策定
		1－3 全国センターから、県における不審な業務パターンを発見した旨の通報 ・ＩＤＳのログ解析で不審な業務パターンを発見 ・全国センターデータベースのアクセスログ解析で不審な情報提供要求の発見	①　全国センターが行う、不審な業務が行われた団体及びその業務端末等を操作ログ解析等により特定する作業に協力 ②　全国センターの要請等を踏まえ、操作者用ＩＣカードの管理の徹底、操作者用ＩＣカード用パスワードの変更、入退室管理の強化等を実施 ③　全国センターの協力を得て、不正操作者を特定 ※　上記措置の迅速な実施が困難、かつ、本人確認情報への脅威が大きい場合は、全国センターと協議の上、当該部分の住基ネットからの切離し

		1－4 県において、サーバ、業務端末等の不審な操作を発見 ・入退室記録、操作者用ＩＣカード管理簿等の点検による発見 ・県サーバ、業務端末等での操作ログ解析による不審な操作の発見 ・県サーバのデータベースのアクセスログ解析で不審な情報提供要求の発見	①　操作者用ＩＣカードの管理の徹底､操作者用ＩＣカード用パスワードの変更、入退室管理の強化等を実施 ②　全国センターの協力を得て、不正操作者を特定 （必要に応じ、全国センターのＩＤＳの監視項目増強、ログ解析強化、全国センターサーバデータベースのアクセスログの解析の強化等を要請） ※　上記措置の迅速な実施が困難、かつ、本人確認情報への脅威が大きい場合は、全国センターと協議のうえ、当該部分の住基ネットからの切離し
2	セキュリティホールを発見	2－1 全国センターから、誤アクセスを発見した旨の通報 ・ＩＤＳ及びＦＷ（全国センター管理）のログ解析で誤アクセスを発見	①　全国センターが行う､誤アクセス経路となった機器又はネットワークの推定作業に協力 ②　全国センターの要請等を踏まえ､当該機器又はネットワークについて、現地での調査を実施 ③　誤アクセスの原因が、本人確認情報への脅威が大きいセキュリティホールであった場合は､全国センターが行う当該機器又はネットワークの住基ネットからの切離し作業に協力 ④　全国センターと連携し、セキュリティホールの補修を実施
		2－2 県において、誤アクセスを発見 ・ＦＷ（県の管理）のログ解析で誤アクセスを発見	①　全国センターの協力を得て､誤アクセス経路となった機器又はネットワークを特定 ②　誤アクセスの原因が、本人確認情報への脅威が大きいセキュリティホールであった場合は､全国センターと連携して､当該機器又はネットワークを住基ネットから切離し ③　全国センターと連携して、セキュリティホールの補修を実施
		2－3 システム監査等によるセキュリティホール発見の通報 2－4 住基ネットで使用しているハードウェア又はソフトウェアのセキュリティに関する脆弱性情報をベンダー等が公表した旨の通報	①　全国センターと連携して、迅速にセキュリティホールの補修を実施 ②　本人確認情報への脅威が大きいセキュリティホールであった場合は、全国センターと連携して、当該機器又はネットワークを住基ネットから切離し
3	システムじょう乱企図の徴候を発見	3－1 全国センターから、出力される本人確認情報に意味をなさない乱れ、又は他人のものとの交錯がある旨の通報	全国センターが行う、以下の措置に協力 ①　壊れたデータベースを格納している機器を特定し、当該機器の停止及び住基ネットからの切離し ②　各種ログ等の解析により、データベース異常発生の原因が外部からの攻撃等によるものかどうかを調査し、攻撃方法、攻撃者等を特定 ③　データベース復旧を実施

		3 - 2 出力される本人確認情報に意味をなさない乱れ、又は他人のものとの交錯があることを発見	全国センターの協力を得て、以下の措置を実施 ① 壊れたデータベースを格納している機器を特定し、当該機器の停止及び住基ネットからの切離し ② 各種ログ等の解析により、データベース異常発生の原因が外部からの攻撃等によるものかどうかを調査し、攻撃方法、攻撃者等を特定 ③ データベース復旧を実施
		3 - 3 全国センターから、予期せぬシステムの機能停止又は電文遅延が発生した旨の通報	全国センターが行う、以下の措置に協力 ① 異常が生じた装置を特定し、当該装置の住基ネットからの切離し ② 機能停止又は電文遅延の原因が外部からのＤＯＳ攻撃等によるものかどうかを調査するとともに、同様の問題が他の装置に発生する可能性についても分析し、攻撃方法、攻撃者等を特定 ③ 切り離された装置の住基ネットへの再組込み
		3 - 4 県において、予期せぬシステムの機能停止又は電文遅延が発生	全国センターの協力を得て、以下の措置を実施 ① 異常が生じた装置を特定し、当該装置の住基ネットからの切離し ② 機能停止又は電文遅延の原因が外部からのDOS攻撃等によるものかどうかを調査するとともに、同様の問題が他の装置に発生する可能性についても分析し、攻撃方法、攻撃者等を特定 ③ 切り離された装置の住基ネットへの再組込み
4	コンピュータウィルス等、自動的に実行される不正プログラムの発見	4 - 1 全国センターから、ウィルス等チェックプログラムにより、ウィルス等が検出･駆除された旨のメッセージ出力があった旨の通報	全国センターが行う、以下の措置に協力 ① ウィルスが混入したのと同じ機種全てについて、最新のパターンファイルに更新されていることを確認 ② ウィルス混入経路及び混入源となった機器を特定 ③ 当該機器の運用管理の強化
		4 - 2 県において、ウィルス等チェックプログラムにより、ウィルス等が検出･駆除された旨のメッセージ出力	全国センターの協力を得て、以下の措置を実施 ① ウィルスが混入したのと同じ機種全てについて、最新のパターンファイルに更新されていることを確認 ② ウィルス混入経路及び混入源となった機器を特定 ③ 当該機器の運用管理の強化
		4 - 3 全国センターから、ウィルス感染を発見した旨の通報	全国センターが行う、以下の措置に協力 ① ウィルス感染範囲及び症状を調査 ② 当該機器のネットワーク（直近のＬＡＮ、通信回線等）からの切離し及びウィルスの駆除 ③ 未知のウィルスであれば、駆除方法等を調査したうえで対処
		4 - 4 県において、ウィルス感染を発見	① 全国センターに対し、パターンファイルの提供を要請 ② 当該機器のネットワーク（直近のＬＡＮ、通信回線等）からの切離し及びウィルスの駆除 ③ 未知のウィルスであれば、全国センターの協力を得て、駆除方法等を調査

附　則

1　この計画は、平成１８年３月３日から施行する。