3.6.2 「被災者台帳を用いた生活再建システム」における情報セキュリティ保持のための体制・制度の構築

(1) 業務の内容

(a) 業務の目的

首都直下地震の発生による最大 1000 万世帯（2500 万人）に及ぶ膨大な数の被災者に対する公平かつ迅速な生活再建支援の実施のために「被災者台帳を用いた生活再建システム」のプロトタイプを構築する。平成１９年新潟県中越沖地震の際にもっとも甚大な被害を受けた柏崎市で活用されたシステムを基本として、「ひとりの取り残しもない生活再建」を実現するための生活再建支援業務の標準化と、それを実行できる人材の育成手法を検討する。

(b) 平成２３年度業務目的

平成２３年度の業務目的は以下の３点である。

・東京都および実証実験のフィールドとなる区市町村の現行のセキュリティポリシーをもとに生活再建支援システムを活用するためのセキュリティポリシーを策定する。
・実証実験のフィールドで試行的に構築する生活再建支援システムの運用のためのセキュリティーシステムを計画・設計し、その実効性・有効性を検証する。
・情報セキュリティ保持のために獲得すべき能力（コンピテンシー）の同定を実施し、被災者台帳を用いた生活再建システムの研修プログラムを構築する。
・3.6.3 および 3.6.4 と連携し、被災者台帳を用いた生活再建システムの実践利用に向けて、3.6 の研究内容を取りまとめる。

(c) 担当者

所属機関	役職	氏名	メールアドレス
新潟大学危機管理室/災害・復興科学研究所	教授	田村圭子	
新潟大学災害・復興科学研究所	助教	井ノ口宗成	
京都大学防災研究所	教授	林　春男	

(2) 平成２３年度の成果

(a) 業務の要約

・東京都および実証実験のフィールドとなる区市町村の現行のセキュリティポリシーをもとに生活再建支援システムを活用するためのセキュリティポリシーを策定した。
・実証実験のフィールドで試行的に構築する生活再建支援システムの運用のためのセキュリティーシステムを計画・設計し、その実効性・有効性を検証した。
・情報セキュリティ保持のために獲得すべき能力（コンピテンシー）の同定を実施し、被災者台帳を用いた生活再建システムの研修プログラムを構築した。
・3.6.3 および 3.6.4 と連携し、被災者台帳を用いた生活再建システムの実践利用に向けて、3.6 の研究内容を取りまとめた。

(b) 業務の成果

1) 東京都および実証実験のフィールドとなる区市町村の現行のセキュリティポリシーをもとに生活再建支援システムを活用するためのセキュリティポリシーを策定する

「ひとりの取り残しもない生活再建」を実現するためには、生活再建に関わる情報資産を守る手立てについて基本的な考え方を整理し、生活再建支援業務の標準化に向けて、情報セキュリティポリシーを実行できる人材の育成手法を検討する。

情報セキュリティポリシーは、どのような情報資産をどのような脅威から、どのようにして守るかについての基本的な考え方ならびに情報セキュリティを確保するための体制、組織および運用を含めた規定であり、情報セキュリティ基本方針および情報セキュリティ対策標準から構成される。そこで、東京都および実証実験のフィールドとなる区市町村を対象として、標準的なセキュリティポリシーとして検討すべき項目の同定をおこない、要件定義をおこなった。

特に情報セキュリティ対策標準では、自治体ごとに詳細なセキュリティ対策項目と評価基準が設けられており、それらは自治体の実態に依存する。そのため、本研究では情報セキュリティ本方針を対象として、セキュリティポリシーの基本要件を定義した。結果として以下に示す７つの項目を明示化することが要件となり、それらの項目において検討すべき内容を整理した。情報セキュリティポリシーでは、セキュリティ確保および対策を推進するための組織・体制を定め、その果たすべき役割、責任および権限を明確にしなければならない。

a) 組織・体制の確立と維持

自治体が一体となり、恒常的に情報セキュリティ対策を推進するための組織・体制を定め、その果たすべき役割、責任および権限を明確にしなければならない。とくに被災者生活再建支援業務においては、担当する部局が単一である場合もあるものの、複数部局が連携する業務も含まれる。また、業務範囲は事前に規定されるだけにとどまらない。そのため、支援業務が展開するにともなって、業務分析をおこないながら組織・体制の見直しと責任の明確化が求められる。

b) 情報の適切な管理責任および方法

生活再建支援業務は、長期にわたる業務の集合体であるとともに、多くの部局が複雑に関わることで実施される。それらの業務は事前からすべてが規定されるわけでなく、生活再建支援過程において新しく発生することも想定され、新しい業務も情報セキュリティの対象としなければならない。そのため、事前・事後において各業務を対象とした業務フローを分析し、情報の発生から整理、蓄積、加工、分析、発信、活用、廃棄といった情報そのものに対する操作を明確化するとともに、それぞれに関わる主体を明らかにしなければならない。情報セキュリティ対策を講じる上で必要となる C.I.A の枠組みの中で、「C：機密性」と「A：可用性」の２つの視点から、それぞれの主体が必要な範囲で情報操作を可能とする一方で、過剰な権限を付与しないことで一定の機密性を確保しなければならない。また「I：完全性」についても同様であり、被災者を確定する過程において「完全性」を担保するための情報処理過程を明確化する必要がある。そのため、情報操作過程においては、それらを記録化することで、情報漏洩や情報改ざんが発覚した際の早急な問題特定と被害波及の軽減を可能とするための対策を講じる必要がある。

c） 物理的セキュリティ

システムの構成によって物理的セキュリティは異なる。SaaS 型であればサーバーは自治体外において一括管理されるが、独立型であれば自治体内でのサーバー管理が求められるため、システムの設置場所についての不正立ち入り、損傷および妨害からの資産保護を目的として、管理区域の設置と物理的対策標準に基づく対策が求められる。また、窓口対応のように、固定的に設置されている情報機器以外のノートパソコンや携帯端末機等をシステム運用時に利用することを想定し、それらの移動可能な端末の管理についても対策を講じておかなければならない。

d） 人的セキュリティ

情報セキュリティを検討する要素である C.I.A のうち「C：機密性」と「A：可用性」は互いにトレードオフの関係にある。可用性を高めれば、情報の流通は進むものの、利用者にその活用方法はゆだねられるため、機密性の確保が難しい。この点において、利用者の範囲を特定するとともに、各々に対する権限および責任を明確化し、ポリシーの内容を周知徹底する、定期的な評価・監査をおこない、十分な教育および啓発が講じられるように、情報セキュリティ対策標準に準じた対策を実施する必要がある。

e） 技術的セキュリティ

情報資産を外部および内部からの不正なアクセス等から適切に保護するため、また、利用範囲外へ被害を拡大させないために、ネットワークおよびハードウェア管理に必要となる対策を講じなければならない。必要に応じて、セキュリティ機器を導入し、アクセス制限を行ない、情報の分類に応じて論理的に異なるネットワークを構築する。各情報機器の通信記録を取得し、一定期間保存し、必要に応じて記録を分析することで、次の対策に活用するという技術的セキュリティ確保に向けたサイクルを運用することが求められる。

f） 情報セキュリティ運用

ポリシーの実効性を確保するため、また、不正利用および不正利用による他システムに対する攻撃に悪用されることを防ぐため、ポリシーの遵守状況の確認、ネットワークの監理といった運用面に関して必要な対策を実施する必要がある。また、緊急事態が発生した際の迅速な対応を可能とするため、緊急時対応計画を規定すること、緊急時においては計画に基づいた対策を実施することを明示化する必要がある。

g）評価・見直し

情報システムは利用過程および技術進展に伴い、対処すべき脅威は変化する。そのため、継続的かつ定期的な対策基準の評価・見直しを実施しなければならない。必要に応じて物理的セキュリティおよび技術的セキュリティの強化、また、人的セキュリティの強化として検収プログラムの見直しを検討しなければならない。定期的な内部監査のみならず、外部監査を実施し、客観的な評価を取り入れ、安定したセキュリティの確保を実現する必要がある。

h）セキュリティポリシーの運用

上記に示すとおり、セキュリティポリシー策定における検討課題は明確化された。しかし、各自治体におけるセキュリティポリシーの運用は、形骸化しているのが実態である。被災者生活再建支援のように「災害が発生した後において初めて実施される業務」を対象とする場合、そのセキュリティポリシーは、平常業務以上に形骸化することが懸念される。

そのため、定期的な研修や訓練でシステム運用をおこないながら、セキュリティ対策の実態を調査し、評価することが必要であると考えられる。

2) 実証実験のフィールドで試行的に構築する生活再建支援システムの運用のためのセキュリティーシステムを計画・設計し、その実効性・有効性を検証する

情報セキュリティーシステムを確実に実装するため、「人的セキュリティ」「物理的セキュリティ」「システムセキュリティ」の３つの視点からシステムを計画・設計した。

「人的セキュリティ」の確保については、実務者の業務運用フローを明らかにするとともに、システムとのインタラクションを整理した。これにより、実務者がシステム内のデータベース操作過程がモデル化され、データベース内の各テーブルに対する「閲覧」「修正」「登録」「削除」の４つの処理を「誰が」「いつ」実施するのかを分析した。この結果から、テーブル自体に対する「操作権限」を整理し、「テーブルを構成する項目の新規設計／変更」、「テーブル自体の削除」を加え、システム運用にかかわる実務者を分類した。これらの整理は、セキュリティを確保するための視点である「C：機密性」「I：完全性」「A：可用性」の３つを軸にした。これらの結果を用いて、システムには「業務（データを活用する生活再建支援業務に加えて、データベースを管理する業務を含む)」「操作（閲覧・修正・登録・削除)」の組み合わせによって各実務者（ユーザー）をマッピングする仕組みを設計し、データベース内に管理用テーブルを構築した。この管理用テーブルをシステムが参照することにより、実務者のシステムへのログイン時に適切な権限を付与することを可能とした。

「物理的セキュリティ」については、行政間のみで閉じたネットワークである LGWAN 上に実装することとした。これにより、外部からの脅威を避けられる。また、LGWAN では、アクセスする端末からはサーバーのアドレス同定も不可能となっているため、各自治体からの直接的なサーバー操作を不可能とした。さらに、LGWAN 内のウィルス・ワーム対策としてファイアウォールを設置するとととともに、TCP/UPD のポートを最小限にとどめた。また、ユーザーからのシステムへ及ぼす脅威を考慮すれば、各自治体がアクセスするデータベースを物理的に分離することがもっともセキュリティを確保できる。しかしながら、サーバー内の空間的制約、費用面の制約、維持・管理上の制約から、１つのサーバーを運用することが現実的であった。そのために、１つのサーバー内に仮想領域を設け、それぞれに仮想稼働環境を整備し、データベース構築・運用することで、１ユーザーが影響を及ぼし得る範囲を当該自治体が管理する領域のみとなるよう制御した。

「システムセキュリティ」については、上記の２つの成果を基盤として、システム内に認証機能を設計・実装した。本機能は、簡易的にユーザーのログイン状況を管理し、業務フロー分析に基づいた操作権限マッピングを参照し、ログインされたユーザーに適切な権限付与を可能とした。サーバー内部ではプロキシを構築することで、ユーザーの操作過程をすべて記録化し、不正操作があった場合に操作過程の追跡を可能とするとともに、不正操作前への復元を可能とした。さらに、ユーザーのログインに関しては、本研究段階では公開鍵を活用した PKI 認証との連携可能性を検討し、ログイン管理機能を切り替えられるようシステム内での機能切り分けをおこなった。PKI 認証への認証に必要な情報を PKI 認証へ提供するとともに、認証結果を処理して操作権限付与へ活用するための機能を設計した。

フィールドで試行的に生活再建支援システムを構築する際には、上記で示した３つの検討内容をもとに、「ひと」「物理的環境」「システム機能」の連携を検討するとともに、各役割を包括的に活用した情報セキュリティーシステムの構築が現実的であることが明らかとなった。

3)　情報セキュリティ保持のために獲得すべき能力（コンピテンシー）の同定を実施し、被災者台帳を用いた生活再建システムの研修プログラムを構築する

a)　情報セキュリティ保持のために獲得すべき能力

情報セキュリティ保持のために獲得すべき能力は、被災者台帳の構築からサービス支援台帳の構築に至る過程における以下の７つである（図 1)。

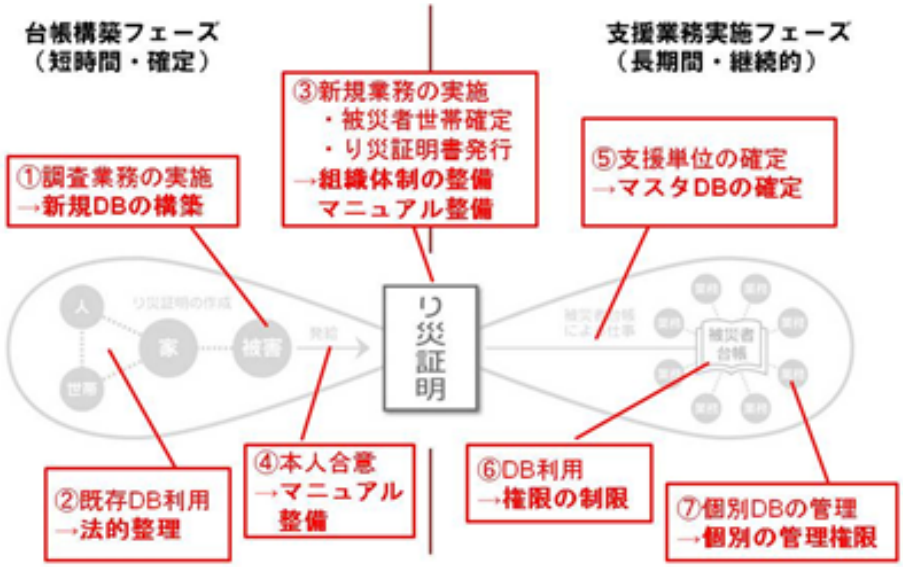

図 1　被災者台帳の構築からサービス支援台帳の構築に至る 7 過程

具体的には、①調査業務実施のための新規データベースの構築に関わるセキュリティの課題を同定できる、②既存データベースの利用の際に、法的な課題の整理ができる、③新規業務を実施する際に、セキュリティを保持するための組織体制やマニュアルを整備することができる、④被災者台帳を構築する際のデータ活用について、被災者本人の同意をとるためのマニュアルや覚え書きなどの整備を実施する、⑤被災者生活再建支援における支援単位を確定し、マスタデータベースを確定する際のセキュリティの保持について検討する、⑦被災者/世帯ごとの個別データベースの管理権限について整備する、に大別できる。

研修プログラムについては、①台帳構築フェーズ、②支援業務実施フェーズ、に分けて構築する。①のフェーズは「短期間」「定型化された業務」の実施期間である。②のフェーズは「長期間」「継続的な業務」の実施期間である。

本システムを構築するに当たり、実際にシステム構築に携わった担当者、受付業務を行った職員などの意見をまとめ、表 1 から表 7 に課題と解決策を業務毎に列挙した。また、今後このようなシステムを構築するに当たり参考となるように、「被災者生活再建支援システムの情報セキュリティ解決チェック表」の作成を行った。表 8 にその結果を示す。

b)「調査業務の実施」の課題と解決策

表 1　「調査業務の実施」の課題と解決策

	課題	解決策
C 機密性	・紙の調査票の管理がずさん	・物理的な管理場所を確保する ・紙調査票の管理体制を整備する
I 完全性	・調査対象物件をすべて調査できているか ・重複したデータ管理がなされていないか	・信頼できる全対象データを整備する ・重複登録を確認する機能（アプリ）を活用する
A 可用性	・調査結果を途中段階であっても利用ニーズが発生する	・調査結果を迅速にデジタル化する仕組みを導入する

機密性については、課題として、紙の調査票の管理がずさんなこと、解決策としては、物理的な管理場所を確保する、紙調査票の管理体制を整備することがあげられる。完全性については、課題として、調査対象物件をすべて調査できているか、重複したデータ管理がなされていないか、解決策としては、信頼できる全対象データを整備する、重複登録を確認する金網（アプリ）を活用するがあげられる。可用性については、課題として、調査結果を途中段階であっても利用ニーズが発生する、解決策としては、調査結果を迅速にデジタル化する仕組みを導入するがあげられる。

c)「既存 DB 利用」の課題と解決策

表 2　「既存 DB 利用」の課題と解決策

	課題	解決策
C 機密性	・目的外の利用となるケースが発生する	・事前から法制度を整備する
I 完全性	・既存DB間での整合性がとれない場合がある ・既存DBだけですべての被災者を把握できるわけではない	・既存DBを変更せず，新しいDBを構築する ・被災者・申請者から情報収集を行なう
A 可用性	・目的外利用のケースでは，許可申請手続きに時間を要する ・各DBを統合する主キーが存在しない	・事前から法制度を整備する ・事前から各DBを統合する主キー（住所コード）を整備する

機密性については、課題として、目的外の利用となるケースが発生する、解決策として、事前から法制度を整備するがあげられる。完全性については、課題としては、既存ＤＢ間での整合性がとれない場合がある、既存ＤＢだけですべての被災者を把握できるわけではない、解決策としては、既存ＤＢを変更せず、新しいＤＢを構築する、被災者・申請者か

ら情報収集を行うがあげられる。可用性については、課題として、目的外利用のケースでは､許可申請手続きに時間を要する､各ＤＢを統合する主キーが存在しないがあげられる。可用性については、課題として、目的外利用のケースでは、許可申請手続きに時間を要する、各ＤＢを統合する主キーが存在しないがあげられる、解決策として、事前から法制度を整備する、事前から各ＤＢを統合する主キー（住所コード）を整備するがあげられる。

d)「新規業務の実施」の課題と解決策

表３　「新規業務の実施」の課題と解決策

	課題	解決策
C 機密性	・データ管理責任者･担当者が不明確である ・庁外実施時における情報管理体制が十分に整備できない	・新しく担当組織を設置する ・情報セキュリティポリシーを満たす空間レイアウトを行なう
I 完全性	・どれが正しい判定結果かがわからなくなる ・被災者や被災建物の認定に重複･抜けが発生する	・業務運用マニュアルを整備し，ルールを徹底する ・一元的な情報管理システムを活用する
A 可用性	・その後の支援の基盤となるため，迅速な実施と情報化が求められる ・必要なDBを参照可能な庁外施設に限定される	・業務実施を支援するシステムを導入する ・必要なDBを参照できるネットワークを確保する

機密性については、課題として、データ管理責任者・担当者が不明確である、庁外実施時における情報管理体制が十分に整備できない、解決策として、新しく担当組織を設置する、情報セキュリティポリシーを満たす空間レイアウトを行うがあげられる。完全性については、課題として、どれが正しい判定結果かがわからなくなる、被災者や被災建物の認定に重複・抜けが発生する、解決策として、業務運用マニュアルを整備し、ルールを徹底する、一元的な情報管理システムを活用するがあげられる。可用性については、課題として、その後の支援の基盤となるため、迅速な実施と情報化が求められる、必要なＤＢを参照可能な庁外施設に限定される､解決策として､業務実施を支援するシステムを導入する、必要なＤＢを参照できるネットワークを確保するがあげられる。

e)「本人合意」の課題と解決策

表 4　「本人合意」の課題と解決策

	課題	解決策
C 機密性	• 本人から提示される根拠資料をずさんに管理する	• 資料の管理場所を物理的に確保する • 資料の管理体制を整備する
I 完全性	• 誰から得た合意かが不明確になる	• 本人合意の記録を管理する
A 可用性	• その後の業務展開が不明瞭であるため，利用範囲が分からない	• 本人より生活再建支援全般における情報利用に関する同意を得る

機密性については、課題として、本人から提示される根拠資料をずさんに管理する、解決策として、資料の管理場所を物理的に確保する、資料の管理体制を整備するがあげられる。完全性については、課題として、誰から得た合意かが不明瞭になる、解決策として、本人合意の記録を管理するがあげられる。可用性について、課題として、その後の業務展開が不明瞭であるため、利用範囲が分からない、解決策として、本人より生活再建支援全般における情報利用に関する同意を得るがあげられる。

f)「支援単位の確定」の課題と解決策

表 5　「支援単位の確定」の課題と解決策

	課題	解決策
C 機密性	• 支援単位確定の責任の所在が不明確である	• 支援単位を確定する責任担当を明確に規定する
I 完全性	• 担当課ごとに支援単位が異なる • 支援単位が一意（世帯×居宅）に決まらず，ばらつきがある • すべての支援単位が確定できているか不明である	• 統一的な支援単位を決定する • 決定された支援単位は変更しない • 抜け・漏れを確認する仕組みを導入する
A 可用性	• 支援確定に時間が取られ，各課の業務展開スピードに追いつかない • 支援確定に必要な情報を柔軟に参照できない	• 業務実施を支援するシステムを導入する • 既存DB，新規DBを相互に閲覧可能な仕組みを整備する

機密性については、課題として、支援単位確定の責任の所在が不明確である、解決策として支援単位を確定する責任担当を明確に規定するがあげられる。完全性については、課題として、担当課ごとに支援単位が異なる、支援単位が一意（世帯×居宅）に決まらず、ばらつきがある、すべての支援単位が確定できているか不明であるがあげられる。解決策としては、統一的な支援単位を決定する、決定された支援単位は変更しない、抜け・漏れ

を確認する仕組みを導入するがあげられる。可用性について、課題として、支援確定に時間が取られ、各課の業務展開スピードに追いつかない、支援確定に必要な情報を柔軟に参照できない、解決策として、業務実施を支援するシステムを導入する、既存 DB・新規 DB を相互に閲覧可能な仕組みを整備するがあげられる。

g)「DB 利用」の課題と解決策

表 6　「DB 利用」の課題と解決策

	課題	解決策
C 機密性	• 統合された全ての情報を一括で閲覧できる	• 利用業務内容に応じて，情報項目ごとに閲覧権限を設定する
I 完全性	• その後の支援で支援単位が変更される • どの時点でのDB利用か不明確になる	• 各課には「編集権限」を与えない • 利用履歴を記録する
A 可用性	• 各課のDBとの整合性がはかられていない • DBを必要とする担当課から容易にDB参照ができない	• 各課のデータと結合可能な主キーを整備する • 全課からアクセス可能なネットワークを整備する

機密性について、課題として、統合された全ての情報を一括で閲覧できる、解決策として、利用業務内容に応じて、情報項目ごとに閲覧権限を設定するがあげられる。完全性について、課題として、その後の支援で支援単位が変更される、どの時点での DB 利用か不明確になる、解決策として、各課には「編集権限」を与えない、利用履歴を記録するがあげられる。可用性については、課題として、各課の DB との整合性がはかられていない、DB を必要とする担当課から容易に DB 参照ができない、解決策として、各課のデータと結合可能な主キーを整備する、全課からアクセス可能なネットワークを整備するがあげられる。

h)「個別 DB の管理」の課題と解決策

表 7　「個別 DB の管理」の課題と解決策

	課題	解決策
C 機密性	• 業務担当課ごとに個別DB利用の目的が規定されている	• 個々の担当課が情報管理責任を担う
I 完全性	• 担当課ごとに支援対象が異なる	• 被災者生活再建支援台帳に基づいて対象を決定する
A 可用性	• 既定の利用目的を超えた柔軟な情報参照は難しい	• 被災者生活再建支援台帳で管理される共通キーを個別DB内で保持する

機密性について､課題として､業務担当課ごとに個別 DB 利用の目的が規定されている、解決策として、個々の担当課が情報管理責任を担うがあげられる。完全性について、課題として、担当課ごとに支援対象が異なる、解決策として、被災者生活再建支援台帳に基づいて対象を決定するがあげられる。可用性について、課題として、規定の利用目的を超えた柔軟な情報参照は難しい、解決策として、被災者生活再建支援台帳で管理される共通キーを個別 DB 内で保持するがあげられる。

i）被災者生活再建支援システムの情報セキュリティ解決チェック表

以上のような分析をもとに、被災者生活再建支援システムの情報セキュリティ解決チェック表を作成した（表 8)。このように各段階において機密性・完全性・可用性に関する解決策があり、これらを包括したような情報セキュリティの取り組みが求められる。

表 8　被災者生活再建支援システムの情報セキュリティ解決チェック表

	C（機密性）	I（完全性）	A（可用性）
① 調査業務の実施	□ 調査票の管理場所が確保できている □ 調査票の管理責任者が確保できている	□ 調査対象の全体が把握できている □ 重複･もれを確認する仕組みが導入されている	□ 調査結果を迅速にデジタル化する仕組みを導入する
② 既存DB利用	□ DB利用の法制度が整理できている	□ 新しくDBを構築する □ 申請者から情報収集する環境が整備できている	□ 各DBを統合する主キー（住所コード）が整備されている
③ 新規業務の実施	□ 新しく担当組織が設置されている □ 情報セキュリティポリシーを満たす空間レイアウトが行なわれている	□ マニュアルが整備されている □ ルールが徹底されている □ 一元的な情報管理システムが活用されている	□ 業務実施を支援するシステムが導入されている □ 必要なDBを参照できるネットワークが確保されている
④ 本人合意	□ 合意資料の管理場所が確保できている □ 合意資料の管理責任者が確保できている	□ 本人合意が確実に記録されている	□ 本人より生活再建支援全般における情報利用に関する同意を得ている
⑤ 支援単位の確定	□ 支援単位を確定する責任担当が明確に規定されている	□ 統一的な支援単位が決定されている □ 支援単位が一意になっている □ 重複･漏れを確認する仕組みが導入されている	□ 支援単位確定を支援するシステムが導入されている □ 既存DB，新規DBの相互の閲覧を可能とする仕組みが整備されている
⑥ DB利用	□ 情報項目ごとに閲覧権限が設定されている	□ 各課には「編集権限」が与えられていない □ DBの利用履歴が記録されている	□ 各課のデータと結合可能な主キーが整備されている □ 全課からアクセス可能なネットワークが確保されている
⑦ 個別DBの管理	□ 個々の担当課が情報管理責任を担う体制がとられている	□ 被災者生活再建支援台帳に基づいて支援対象が決定されている	□ 被災者生活再建支援台帳で管理される共通キーが個別DB内で保持されている

(c) 結論ならびに今後の課題

本研究では、東京都および実証実験のフィールドとなる区市町村の現行のセキュリティポリシーをもとに生活再建支援システムを活用するためのセキュリティポリシーを策定した。実証実験のフィールドで試行的に構築する生活再建支援システムの運用のためのセキュリティーシステムを計画・設計し、その実効性・有効性を検証した。次に、情報セキュ

リティ保持のために獲得すべき能力（コンピテンシー）の同定を実施し、被災者台帳を用いた生活再建システムの研修プログラムを構築した。また、3.6.3 および 3.6.4 と連携し、被災者台帳を用いた生活再建システムの実践利用に向けて、3.6 の研究内容を取りまとめた。

本研究では、生活再建支援システムを活用するためのセキュリティポリシーについて課題を分析・導出し、その解決策を提案することができた。今後は、これらを包括したような情報セキュリティーシステムの実現化および実装化が求められる。現在、岩手県において支援ベースで生活再建支援システムの提供を行っている。既に被災市町村の一部で活用され、生活再建支援業務の整理・統合・実施において実際に活用されている。これらの運用におけるセキュリティ問題なども分析・導出しながら、セキュリティーシステムの精緻化・高度化を図っていきたい。

(d) 引用文献

なし

(e) 学会等発表実績

学会等における口頭・ポスター発表

なし

学会誌・雑誌等における論文掲載

なし

マスコミ等における報道・掲載

なし

(f) 特許出願，ソフトウエア開発，仕様・標準等の策定

1)特許出願

なし

2)ソフトウエア開発

名称	機能
被災者生活再建支援サービス台帳ベータ版～情報セキュリティ対応版	被災者の生活再建支援業務を被災者台帳の基盤部分を用いて実施する。

3) 仕様・標準等の策定

なし