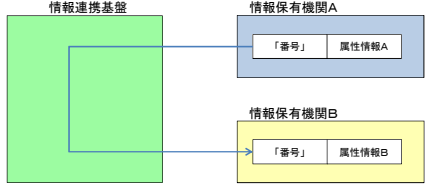
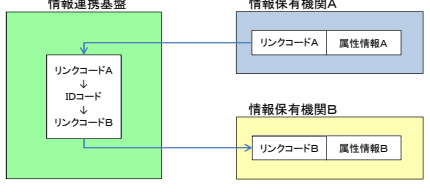
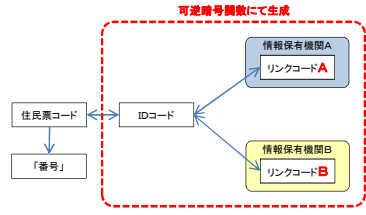
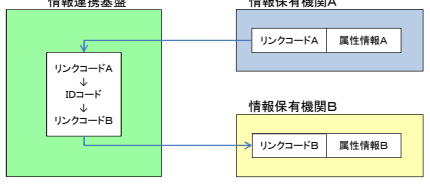
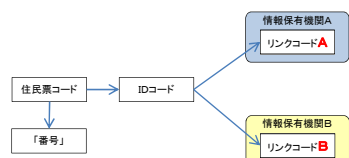
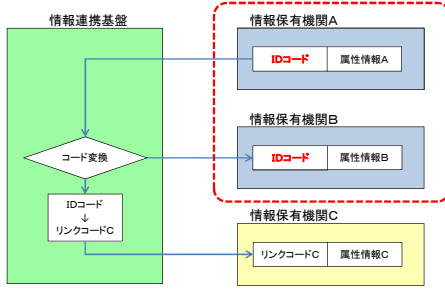
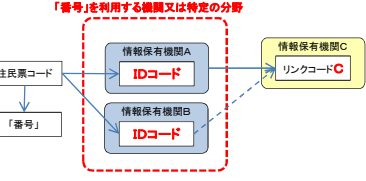
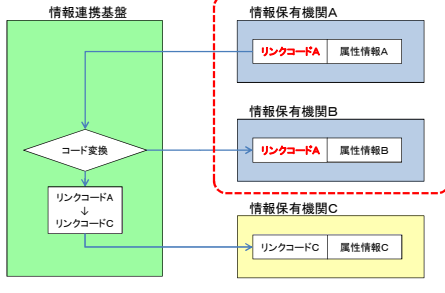
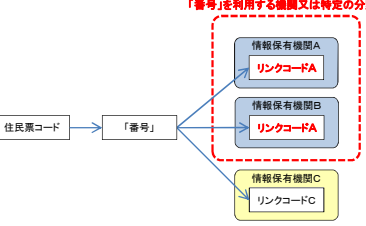


表1 番号連携方式検討表

(第5回情報連携基盤技術WG提出資料(一部修正版))

	連携概要	住民票コード、「番号」及び符号の関係	コストパフォーマンス	連携対象の拡張性	稼働の安定性・運用性	調達の透明・公正性	セキュリティ・プライバシー影響度
案1	 全ての情報保有機関間で「番号」を用いて情報連携を行う方式	 住民票コードから「番号」を生成する	符号(IDコード、リンクコード)を変換するための機能を情報連携基盤に付加せず、情報連携を実現することができるため、コストパフォーマンスは高い。	情報保有機関は保有する個人の情報と「番号」との紐付けを行っていることから、「番号」との紐付けを行っていない機関とは、番号制度に係る情報連携を行うことができない。	情報連携基盤を通じた情報保有機関間の連携において、「番号」を変換した符号を生成し、情報連携に用いる必要がないことから、情報連携基盤における符号(IDコード、リンクコード)の変換処理を要しない点で、他の案よりも情報連携基盤におけるシステム処理上の負荷は低く、システムの安定性は高い。	情報連携基盤におけるコード変換機能が不要である点において、他の案よりも調達の透明性・公平性を確保しやすい。	番号制度において将来的に実現が求められる「民間の機関等との情報連携」においても「番号」で連携を行うことになるが、民間事業者が利用するネットワークは、国・地方公共団体が利用するネットワークとセキュリティ対策が異なる場合も想定され、どこまでセキュリティ要件を求めることができるのか等課題がある。 情報保有機関において、「番号」と「番号」に紐付けられた属性情報を用い不正なマッチングが可能となる危険性があり、また、国が「個人情報を一元的に管理することができる主体」となり得る可能性が懸念される等、プライバシー影響度は非常に大きい。
案2（骨格案）	 各情報保有機関毎に異なるリンクコード割り当て、共通するIDコードを経由して双方を紐付け、情報連携する方式。	 住民票コードから可逆暗号関数(※)にてIDコードを生成し、IDコードから可逆暗号関数にてリンクコードを生成する 「番号」は住民票コードから乱数によるコード変換テーブルにて生成する。	すべての情報連携において、情報連携基盤で可逆暗号方式による符号変換処理(情報保有機関Aが保持するリンクコードAからIDコードへの変換、IDコードから情報保有機関Bが保持するリンクコードBへの変換)が必要となるため、情報連携基盤での変換処理に係るシステム負荷が生じることになる。大量のデータベースの検索を行う必要のあるコード変換テーブル方式を採用する案3と比べ、どの程度のシステム運用面での負荷が生じ、どの程度、コストパフォーマンスに差が出るのか、今後、比較検討する必要がある。	「番号」を利用しない機関に係る情報連携について対応可能である。 将来的な情報連携対象分野の拡大に対応可能である。 (案2、案3、案4、案5は同程度)	すべての情報連携において、情報連携基盤で可逆暗号方式による符号変換処理(情報保有機関Aが保持するリンクコードAからIDコードへの変換、IDコードから情報保有機関Bが保持するリンクコードBへの変換)が必要となるため、情報連携基盤での変換処理に係るシステム負荷が生じることになる。大量のデータベースの検索を行う必要のあるコード変換テーブル方式を採用する案3と比べ、どの程度のシステム運用面での負荷が生ずるか、今後、比較検討する必要がある。	情報連携基盤におけるコード変換機能が必要となり、当該方式と同様の仕組みを採用したシステムは前例がないため、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある。	機関毎に異なるリンクコードにより情報連携を行うこととすることで、情報保有機関間において情報連携基盤が関与しない不当な情報連携が行われることを技術的に回避する。 万が一、情報保有機関AのリンクコードA及び紐付けられている属性情報が漏洩した場合、他の情報保有機関とはリンクコードが異なっていることから、他の情報保有機関が保有する個人情報との不正なマッチングはできず、情報保有機関AのリンクコードAのみを変更することで対処可能であるため、案1、案4、案5よりもプライバシー影響度は低いと思われる。
案3	 各情報保有機関毎に異なるリンクコード割り当て、双方を紐付け、情報連携する方式。IDコードは、リンクコード生成時に使用する。	 住民票コードから「番号」及びIDコードを生成し、IDコードからリンクコードを生成する(いずれも乱数によるコード変換テーブルにて生成する)	すべての情報連携において、コード変換テーブル方式による符号変換処理(情報保有機関Aが保持するリンクコードAから情報保有機関Bが保持するリンクコードBへの変換)が必要となるが、情報連携基盤での変換処理に係るシステム負荷は、案2と比べ、どの程度のシステム運用面での負荷が生じ、どの程度、コストパフォーマンスに差が出るのか、今後比較検討する必要がある。	「番号」を利用しない機関に係る情報連携について対応可能である。 将来的な情報連携対象分野の拡大に対応可能である。 (案2、案3、案4、案5は同程度)	すべての情報連携において、コード変換テーブル方式による符号変換処理(情報保有機関Aが保持するリンクコードAから情報保有機関Bが保持するリンクコードBへの変換)が必要となるが、情報連携基盤での変換処理に係るシステム負荷は、案2と比べ、どの程度のシステム運用面での負荷が生ずるか、今後比較検討する必要がある。	情報連携基盤におけるコード変換機能が必要となり、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある。	機関毎に異なるリンクコードにより情報連携を行うこととすることで、情報保有機関間において情報連携基盤が関与しない不当な情報連携が行われることを技術的に回避する。 万が一、情報保有機関AのリンクコードA及び紐付けられている属性情報が漏洩した場合、案2と同様に、他の情報保有機関とはリンクコードが異なっていることから、他の情報保有機関が保有する個人情報との不正なマッチングはできず、情報保有機関AのリンクコードAのみを変更することで対処可能であるため、案1、案4、案5よりもプライバシー影響度は低いと思われる。
案4	 「番号」を利用する機関又は特定の分野内での情報連携は共通のIDコードを用い、それ以外は機関毎に異なるリンクコードを割り当て、情報連携する方式。	 住民票コードから「番号」及びIDコードを生成し、IDコードからリンクコードを生成する(いずれも乱数によるコード変換テーブルにて生成)	一部の情報連携については、IDコードを用いて情報連携が行われるため、情報連携基盤でリンクコードAからIDコード、IDコードからリンクコードBへの変換をせずに情報連携が行われることから、変換処理に係る情報連携基盤のシステムの負荷は、すべての情報連携においてコード変換処理を行う案2よりも低くなることが見込まれる。 他の案と比べどの程度コストパフォーマンスに差が出るのか、今後比較検討する必要がある。	「番号」を利用しない機関に係る情報連携について対応可能である。 将来的な情報連携対象分野の拡大に対応可能である。 (案2、案3、案4、案5は同程度)	一部の情報連携については、IDコードを用いて情報連携が行われるため、情報連携基盤でリンクコードAからIDコード、IDコードからリンクコードBへの変換をせずに情報連携が行われることから、変換処理に係る情報連携基盤のシステムの負荷は、すべての情報連携においてコード変換処理を行う案2よりも低くなることが見込まれる。	情報連携基盤におけるコード変換機能が必要となり、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある。	IDコードを保持する情報保有機関間において個人情報の不正なマッチングを防ぐことができない点において、共通のIDコードによる情報連携はプライバシー保護の観点から問題がある。 万が一、IDコードによる情報連携を行う情報保有機関のIDコードとIDコードに紐付けられた属性情報が漏洩した場合、同じIDコードにより情報連携を行う複数の情報保有機関が保有する個人情報とのデータマッチングが可能となる危険性があり、該当する複数の情報保有機関においては、IDコードの入れ替えが必要となるため、案2及び案3よりもプライバシー影響度は大きいと思われる(リンクコード漏洩時の影響は、案2と同等である。)
案5	 「番号」を利用する機関又は特定の分野内での情報連携は共通のリンクコードを用い、それ以外は機関毎に異なるリンクコードを割り当て、情報連携する方式。	 住民票コードから生成された「番号」を基にリンクコードを生成する。 (いずれも乱数によるコード変換テーブルにて生成)	一部の情報連携については、共通のリンクコードを用いて情報連携が行われるため、情報連携基盤でリンクコードAからIDコード、IDコードからリンクコードBへの変換をせずに情報連携が行われることから、変換処理に係る情報連携基盤のシステムの負荷は、すべての情報連携においてコード変換処理を行う案2よりも低くなることが見込まれる。 他の案と比べどの程度コストパフォーマンスに差が出るのか、今後比較検討する必要がある。	「番号」を利用しない機関に係る情報連携について対応可能である。 将来的な情報連携対象分野の拡大に対応可能である。 (案2、案3、案4、案5は同程度)	一部の情報連携については、共通のリンクコードを用いて情報連携が行われるため、情報連携基盤でリンクコードAからIDコード、IDコードからリンクコードBへの変換をせずに情報連携が行われることから、変換処理に係る情報連携基盤のシステムの負荷は、すべての情報連携においてコード変換処理を行う案2よりも低くなることが見込まれる。	情報連携基盤におけるコード変換機能が必要となり、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある。	共通のリンクコードを保持する情報保有機関間において個人情報の不正なマッチングを防ぐことができない点において、案5のように共通のリンクコードによる情報連携は、プライバシー保護の観点から問題がある。 万が一、共通のリンクコードによる情報連携を行う情報保有機関のリンクコードとリンクコードに紐付けられた属性情報が漏洩した場合、共通のリンクコードにより情報連携を行う複数の情報保有機関が保有する個人情報とのデータマッチングが可能となる危険性があることから、該当する複数の情報保有機関において、リンクコードの入れ替えが必要となるため、案2及び案3よりもプライバシー影響度は大きいと思われる。

(※)平成22年12月27日開催の「高度情報通信ネットワーク社会推進戦略本部 第8回 電子行政に関するタスクフォース 資料2-1 「国民ID制度における国民IDコードの考え方(その2)」においては、可逆と不可逆の方式について次のように述べられている。
「国民IDコードと利用番号の連携は可逆(相互に検索可)の場合と、不可逆(利用番号から国民IDコードの検索不可)の場合がある。どちらもある分野で利用番号が盗まれた場合でも別分野への不正アクセスや分野横断的な名寄せリスクを限定的なものにすることができるが、不可逆の場合は、分野間の情報連携に当たって、その都度属性情報(氏名、住所、性別、生年月日)等により利用番号間の連携を行う(例:オーストリアのセクトラル方式)ことが想定され、その場合は効率性や安全性に課題があると考えられる。」