資料２

地方公共団体の非識別加工情報の作成・提供に係る効率的な仕組みに係る主な検討項目

４　必要となるセキュリティ基準等

○　作成組織の仕組みに係るセキュリティについては、地方公共団体における情報セキュリティポリシーに関するガイドラインの内容を踏まえつつ、匿名加工情報を取り扱う他の仕組みにおける安全管理措置に照らし、十分な措置を講じることとしてはどうか。

○　作成組織の従事者に対して、取り扱う情報の内容等をみだりに他人に知らせ、又は不当な目的に利用してはならないこと等、行政機関個人情報保護法や条例による非識別加工情報と同等の内容の規律を設けてはどうか。

（1）個人情報等及び非識別加工情報の安全管理措置等について

個人情報保護法及び行政機関個人情報保護法における安全管理措置等に係る規律

	個人情報保護法	行政機関個人情報保護法 （「条例改正のイメージ」も同様）
個人情報等に係る規律	（安全管理措置） 第 20 条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 （従業者の監督） 第 21 条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。 （委託先の監督） 第 22 条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。	（安全確保の措置） 第6条　行政機関の長は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならない。 2　前項の規定は、行政機関から個人情報（行政機関非識別加工情報及び削除情報に該当するものを除く。次条、第 38 条、第 48 条、第 50 条及び第 51 条において同じ。）の取扱いの委託を受けた者が受託した業務を行う場合について準用する。 （従事者の義務） 第７条　個人情報の取扱いに従事する行政機関の職員若しくは職員であった者又は前条第 2 項の受託業務に従事している者若しくは従事していた者は、その業務に関して知り得た個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。

匿名加工情報・非識別加工情報	（匿名加工情報の作成等） 第 36 条　略 2　個人情報取扱事業者は、匿名加工情報を作成したときは、その作成に用いた個人情報から削除した記述等及び個人識別符号並びに前項の規定により行った加工の方法に関する情報の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、これらの情報の安全管理のための措置を講じなければならない。 3～5　略 6　個人情報取扱事業者は、匿名加工情報を作成したときは、当該匿名加工情報の安全管理のために必要かつ適切な措置、当該匿名加工情報の作成その他の取扱いに関する苦情の処理その他の当該匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。	（安全確保の措置） 第 44 条の 15　行政機関の長は、行政機関非識別加工情報、行政機関非識別加工情報の作成に用いた保有個人情報から削除した記述等及び個人識別符号並びに第 44 条の 10 第 1 項の規定により行った加工の方法に関する情報（以下この条及び次条において「行政機関非識別加工情報等」という。）の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、行政機関非識別加工情報等の適切な管理のために必要な措置を講じなければならない。 2　前項の規定は、行政機関から行政機関非識別加工情報等の取扱いの委託を受けた者が受託した業務を行う場合について準用する。 （従事者の義務） 第 44 条の 16　行政機関非識別加工情報等の取扱いに従事する行政機関の職員若しくは職員であった者又は前条第二項の受託業務に従事している者若しくは従事していた者は、その業務に関して知り得た行政機関非識別加工情報等の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。

(2)　作成組織における安全管理措置について

作成組織は、個人情報取扱事業者として、個人情報保護法の規定が適用される前提となるが、地方公共団体から、本人の同意を求めない形で提供を受けた個人情報を取り扱うことを踏まえ、安全管理措置の内容については、行政機関に適用されている規律を踏まえた内容とする必要があるのではないか。具体的には、作成した非識別加工情報に関する安全管理措置の実施を義務とするほか、安全管理措置に係る具体的な内容を法令で規定することも必要か。

（3） 具体的なセキュリティ基準について

①作成組織内部における情報の取扱い

作成組織では、地方公共団体の個人情報について、広域的に取り扱うこと等から、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下、「セキュリティポリシーガイドライン」という。）における現行の地方公共団体のセキュリティ水準（※）を踏まえつつ、十分なセキュリティ対策を実施することが求められる。

具体的には、作成組織において取り扱う情報を、セキュリティポリシーガイドラインにおいて最も高い水準の情報資産として取り扱うこととし、当該情報を取り扱う領域についてインターネットに接続しない等、地方公共団体から個人情報の提供を受けることを踏まえた取扱いとしてはどうか。

②地方公共団体からの個人情報の収集における取扱い

地方公共団体が作成組織に対して提供する個人情報は、セキュリティポリシーガイドラインにおいて、個人番号利用事務系において取扱われる個人情報やLGWAN接続系において取扱われる個人情報であることから、安全性の高い回線により提供することが必要である。

③作成組織からの非識別加工情報の提供における取扱い

作成組織において作成した非識別加工情報は、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないように加工されたものであり、非識別加工情報の提供を受けた者が本人を識別するための照合等を行うことが禁止されているが、地方公共団体から提供を受けた個人情報から作成されることを踏まえ、その民間事業者等への提供については、一定のセキュリティ水準の確保が必要である。

例えば、作成組織による非識別加工情報の提供について、電子媒体等を持ち運ぶ場合の盗難防止対策又はセキュリティ水準の高いネットワークによる提供（専用回線サービス（IP-VPN や SSL-VPN など仮想技術を利用した通信を含む。））等が必要である。

上記①、②、③の取扱いを中心に、引き続きセキュリティ基準の具体的な項目・内容等について検討する必要がある。

（別紙2）作成組織におけるセキュリティに関する対応のイメージ

（別紙3）「地方公共団体における情報セキュリティポリシーに関するガイドライン」の全体像

（参考）医療分野の研究開発に資するための匿名加工医療情報に関する法律施行規則
（平成 30 年内閣府・文部科学省・厚生労働省・経済産業省令第1号）

第6条 法第八条第三項第三号及び法第二十条の主務省令で定める措置は、次のとおりとする。

一～三 （略）

四 技術的安全管理措置

イ～ハ （略）

ニ 認定事業医療情報等を電気通信により送受信するとき、又は移送し、若しくは移送を受けるときは、次に掲げる措置を講じていること。

(1) 外部の者との送受信の用に供する電気通信回線として、専用線等（IP―VPNサービス（電気通信事業報告規則（昭和六十三年郵政省令第四十六号）第一条第二項第十五号に掲げるIP―VPNサービスをいう。）に用いられる仮想専用線その他のこれと同等の安全性が確保されると認められる仮想専用線を含む。）を用いること。

(2) (1)に規定する電気通信回線に接続されるサーバ用の電子計算機のうち、医療情報取扱事業者からの医療情報の受信に用いるものについては、外部への送信機能を具備させないこと。

(3) (1)に規定する電気通信回線に接続されるサーバ用の電子計算機のうち、匿名加工医療情報取扱事業者への匿名加工医療情報の送信に用いるものについては、外部からの受信機能を具備させないこと。また、(2)又はホに規定する電子計算機以外のサーバ用の電子計算機を用いること。

(4) (1)から(3)までに掲げるもののほか、認定事業医療情報等を適切に移送し、又は移送を受けるために、暗号化等必要な措置を講ずること。

ホ 匿名加工医療情報の作成の用に供する医療情報の管理は、ニ(2)及び(3)の電子計算機以外のサーバ用の電子計算機を用いることとし、ニ(2)及び(3)に規定する電子計算機を経由する以外の方法による外部へのネットワーク接続を行わないこと。また、ニ(2)及び(3)に規定する電子計算機との接続においては、専用線を用いること。

(4) 非識別加工情報の識別行為の禁止について

非識別加工情報に関して、行政機関個人情報保護法等や条例においては、識別行為に係る禁止は設けていないところであるが、これは、行政課題の解決等のために提供元の行政機関において照合行為を行う必要性が生じることがあり得ることも想定され、照合禁止義務を課した場合、行政事務の適正かつ円滑な遂行に支障が生じるおそれがあるためである。

作成組織の役割は、非識別加工情報を作成し提供することに限定されるものであり、上記のように照合行為を行う必要性も認められないと考えられるため、非識別加工情報に係る識別行為の禁止を課すこととしてはどうか。

(5) 従業者等の義務について

行政機関個人情報保護法等においては、個人情報及び行政機関非識別加工情報等の取扱いに従事する者等について、 業務に関して知り得た行政機関非識別加工情報等の内容をみだりに他人に知らせ、又は不当な目的に利用してはならないとの義務が課されている。

作成組織の従業者又はこれらであった者に対して、非識別加工情報の作成事業に関して知り得た個人情報等又は非識別加工情報の内容等をみだりに他人に知らせ、又は不当な目的に利用してはならないことを内容とする義務を課してはどうか。

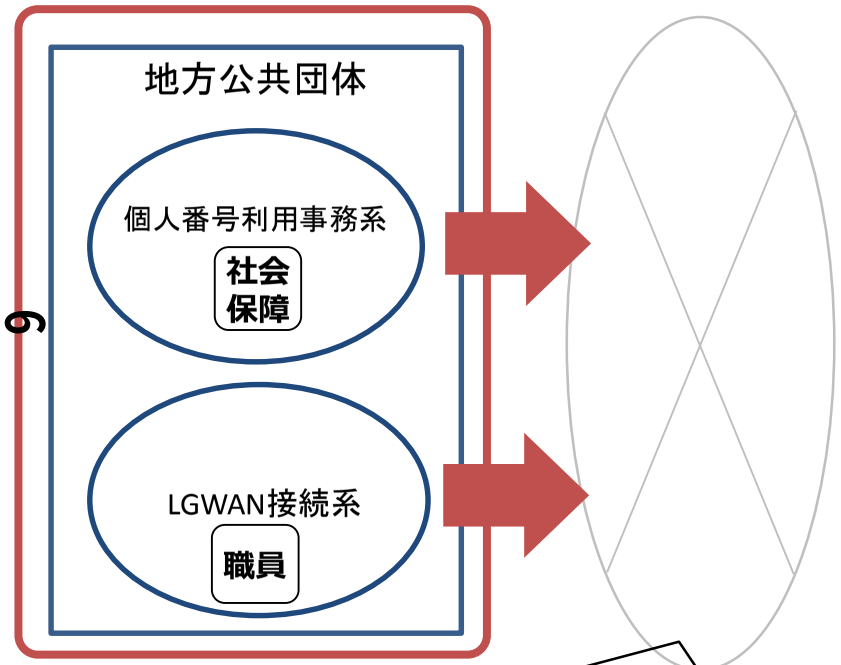
作成組織におけるセキュリティに関する対応のイメージ

別紙２

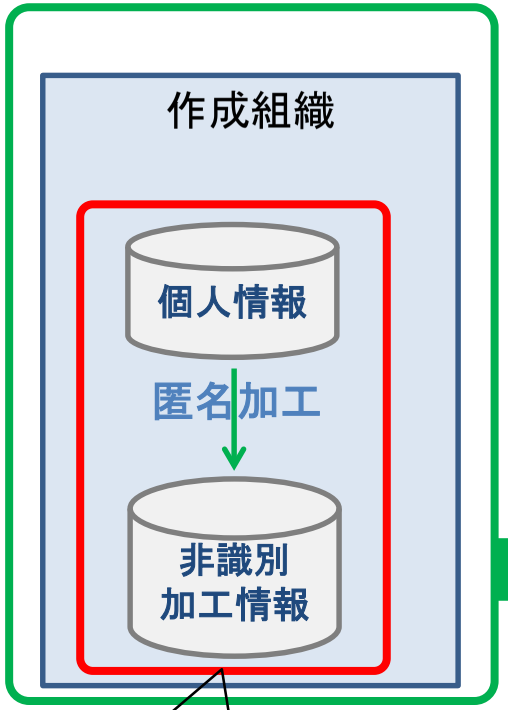
● 地方公共団体における情報セキュリティポリシーに関するガイドラインを踏まえ、①地方公共団体からの個人情報の提供や②作成組織内部における情報の取扱い、③作成組織から民間事業者等への非識別加工情報の提供におけるセキュリティ基準の在り方について検討が必要となる。

①地方公共団体

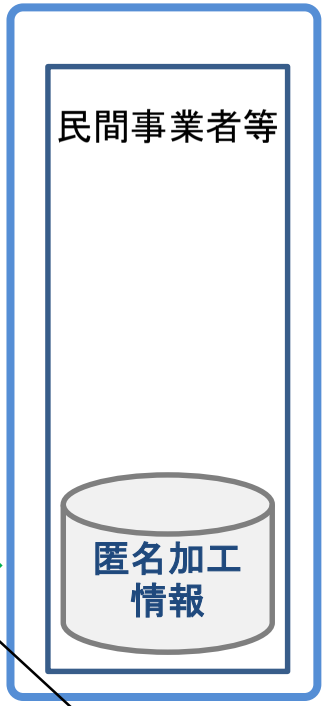
・地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）



②作成組織



③利活用する民間事業者等



①→②　地方公共団体から作成組織への個人情報の提供

→地方公共団体からは、個人番号利用事務系及びＬＧＷＡＮ接続系に分類される個人情報が提供されることから、安全性の高い回線により提供することが必要ではないか。（※）

②　作成組織内部における情報の取扱

→作成組織内の個人情報を扱う領域とインターネットに接続された情報系ネットワークとの分離が必要ではないか。（※）

②→③　作成組織から民間事業者等への非識別加工情報の提供

→匿名加工された情報の取扱いについても、電子媒体等を持ち運ぶ場合の盗難防止対策又はセキュリティ水準の高いネットワークによる提供等が必要ではないか。（※）

（※）その他、具体的な項目・内容については、引き続き検討を行う。

地方公共団体における情報セキュリティポリシーに関するガイドライン　概要

別紙３

項目	内容
目的	地方公共団体が保有する情報資産の機密性、完全性及び可用性を維持するため、地方公共団体が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。
職員等の遵守基準	地方公共団体の職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。
組織体制	地方公共団体の保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。
情報資産の分類と管理	地方公共団体の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。
情報システム全体の強靭性の向上	情報システム全体に対し、次の三段階の対策を講じる。 ①個人番号利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

※地方公共団体における情報セキュリティポリシーに関するガイドライン（平成30年9月版）から作成

地方公共団体における情報セキュリティポリシーに関するガイドライン　概要②

項目		内容
物理的セキュリティ		サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。
	サーバの管理	情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。
	情報システム室等での管理	情報システム管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。
	通信回線等の管理	機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
	職員等のパソコン等の管理	情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。
技術的セキュリティ		コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
	ログの取得等	各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存した上で、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。
	不正アクセス対策	サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。

※地方公共団体における情報セキュリティポリシーに関するガイドライン（平成30年9月版）から作成

地方公共団体における情報セキュリティポリシーに関するガイドライン　概要③

項目	内容
人的セキュリティ	情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
運用	情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
外部サービスの利用	外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。 約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。
評価・見直し	情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。
情報セキュリティ監査及び自己点検の実施	情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。
情報セキュリティポリシーの見直し	情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

※地方公共団体における情報セキュリティポリシーに関するガイドライン（平成30年9月版）から作成