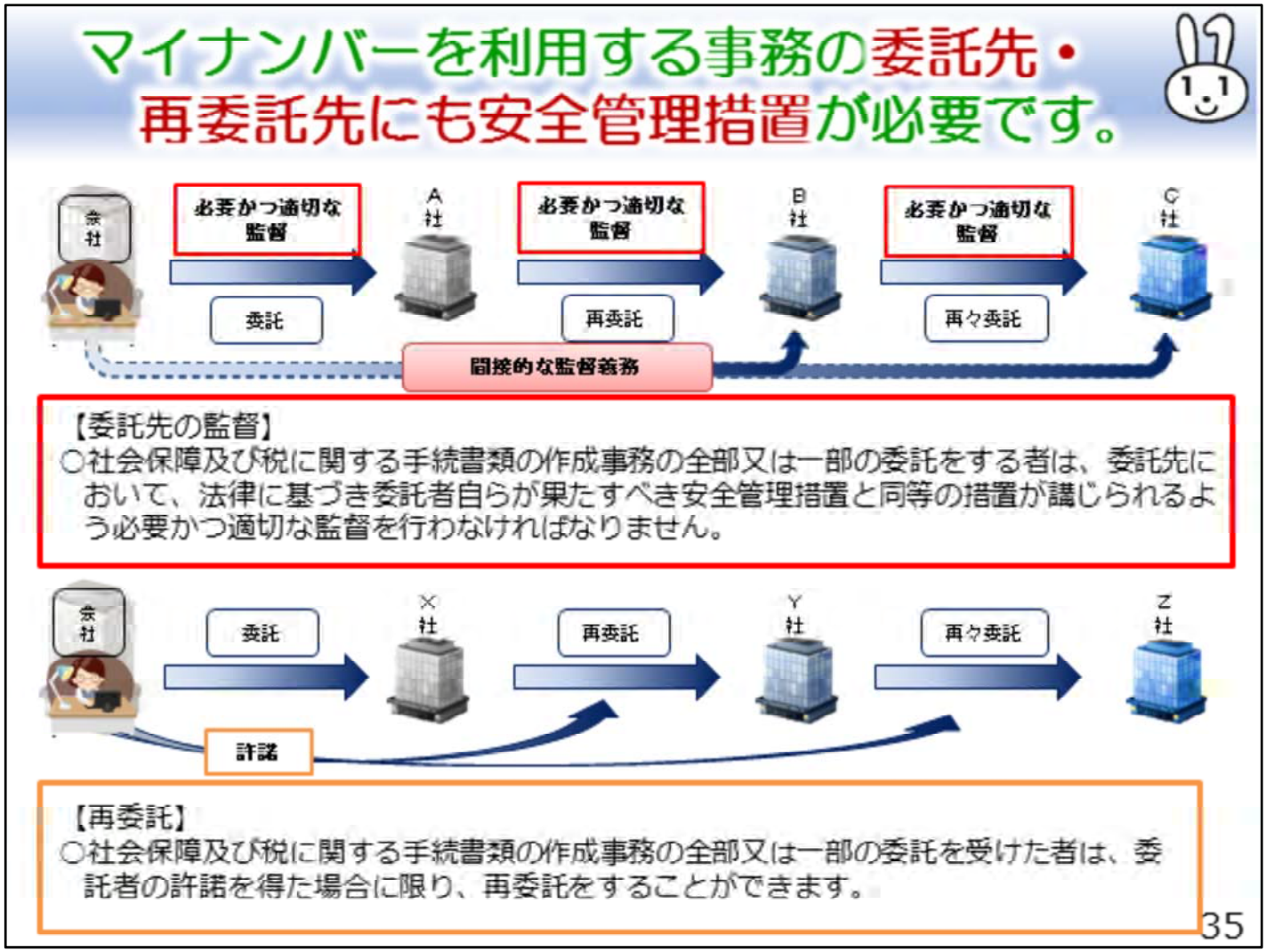


■Safety management measures need to be implemented by parties commissioned (contractors including subcontractor and so on) with administrative tasks that require the use of My Numbers

In the event all or part of administrative document preparation for social security and tax are commissioned to a third party, the consignor must execute appropriate and necessary supervision to ensure that safety management measures equivalent to that of their own are put in place by the consignee.

Specifically, (1) the consignee must be appropriately selected, (2) an agreement must be concluded to ensure that the consignees comply with safety management measures, and (3) the consignor must ascertain the handling of specific personal information by the consignee.

The consignor must check equipment, technical standards, supervision and training of employees and other business environments of the consignee prior to the commissioning of the work.

An agreement must be concluded that includes a clause on confidentiality, the prohibition of the taking of specific personal information outside the office, prohibition of the use of specific personal information for purposes other than specified, the return or destruction of specific personal information after completion of the consignment agreement, the supervision and training of employees, and a report must be submitted to the consignor regarding the status of compliance with the agreement.

The consignor is responsible for supervising the consignee, and also responsible for indirect supervision of re-consigned companies.

The consignee commissioned to conduct all or part of the administrative work for social security and tax may re-consign the work only when consent is obtained from the original consignor.

■Appropriate organizational safety management measures for My Numbers must be put into place

Business operators must implement essential and appropriate safety management measures to prevent leakage, loss or impairment and for other appropriate management of My Numbers and specific personal information, as well as execute essential and appropriate supervision of their employees.

It is important to clarify the range of administrative work that requires the handling My Numbers and specific personal information. The guidelines provide safety management measures that business operators should take. Some of the recommended measures include the establishment of a basic policy, the establishment of rules, and systematic, personnel, physical and technical safety management measures.
A special rule is set for small and medium enterprises with less than 100 employees in consideration of its effect on business operations.
○"Establishment of the basic policy" means that, it is important to clarify fundamental principles for the securing of appropriate handling of specific personal information.

The establishment of a basic policy is not compulsory, however, it has the merit of publicizing the stance of the company and providing training to employees.

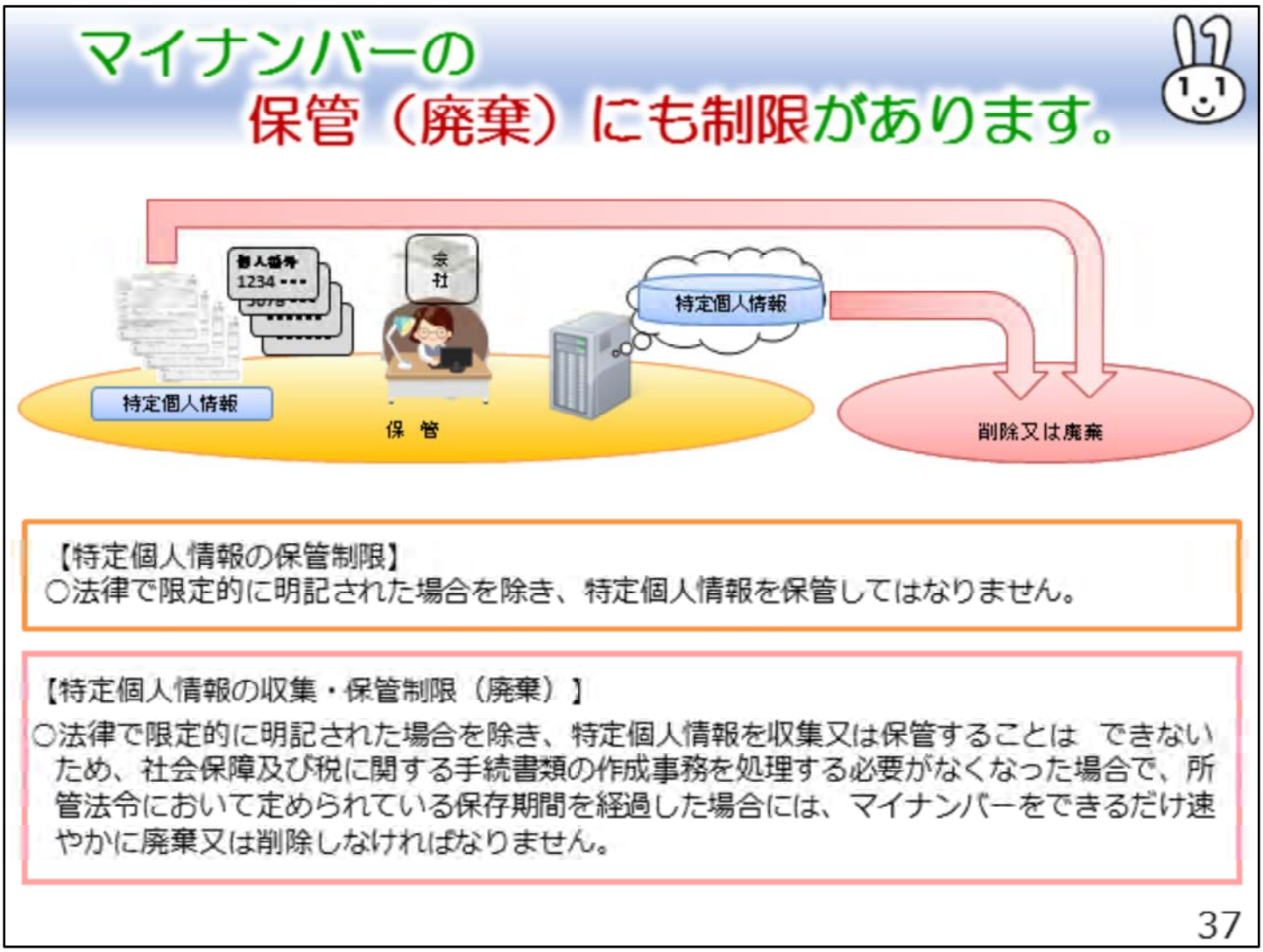
○"Development of official handling rules" means that the establishment of rules that involves the preparation of manuals and documents that show the range of work, organizing the flow of administrative work with clarified range and person in charge of specific individual's personal information and specific handling.

○Systematic safe management measures are maintenance of the organization system, operation based on handling official rules, maintenance of the means to identify the handling situation, maintenance of the system corresponding to the case such as information leakage and grasping and reviewing of the handling situation and safe management.

○Personnel safe management measures are the supervision and training of employees

○Physical safe management measures are management of an area dealing with specific personal information, prevention of theft of apparatus and electronic media and so on, prevention of leaks in the handling of electronic media, deletion of the personal numbers, correspondence about the disposal of apparatus and electronic media. In addition, the disposal and deletion of the personal number, apparatus and electronic media should be performed as promptly as possible when they became needless by the means that cannot be restored to the original state. Also, it is necessary to preserve the record about the deletion or discarded.

○Technical measures are the control of access, identification and authentication of accessing person, prevention of unauthorized access and information leakage and so on.



■Restrictions for the retention (disposal) of My Numbers

Specific personal information that includes My Numbers may not be retained as stipulated by law. Such information can only be retained as required for the execution of administrative processes.

Documents with My Numbers can be retained for the specific period permitted by law.

One example is the retaining of My Numbers of employees in a continuous relationship under an employment agreement for the preparation of certificates of income and tax withholding, health insurance and welfare pension documents expected to be prepared in following years, which makes it possible to retain such personal information.

On the other hand, because the collection and retention of specific personal information is prohibited by law, with exceptions as indicated for a limited extent, when the preparation of documents related to social security and taxation are no longer required and the storage period stipulated by the jurisdiction laws have lapsed, My Numbers must be disposed or deleted as soon as possible.

It is possible to continue holding the document if My Numbers are deleted or masked to an un-restorable level.

In this way, there are restrictions on the retention (disposal) of My Numbers. It is desirable to manage paper documents by year on the assumption that they will eventually be disposed of or deleted, or structure a system on the computer to delete My Numbers that are no longer required.

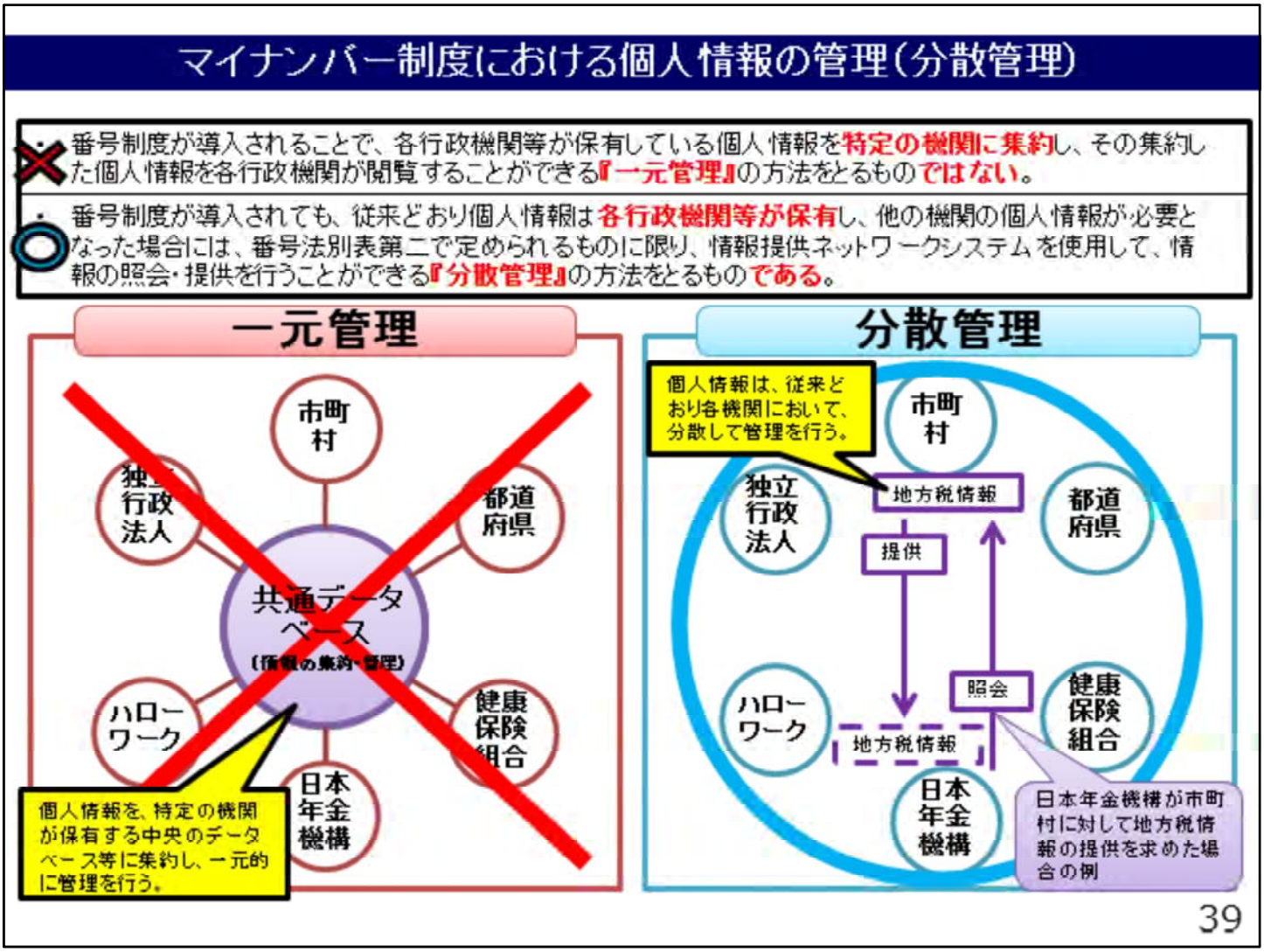
マイナンバー制度における罰則の強化

	行為	マイナンバー法の法定刑	同種法律における類似規定の罰則		
			行政機関個人情報保護法・独立行政法人等個人情報保護法	個人情報保護法	住民基本台帳法
特定の公務員が対象	情報提供ネットワークシステムの事務に従事する者が、情報連機や情報提供ネットワークシステムの業務に関して知り得た秘密を漏らし、または盗用	3年以下の懲役or150万以下の罰金（併科されることあり）	―	―	2年以下の懲役 or 100万以下の罰金
	国、地方公共団体、地方公共団体情報システム機構などの役職員が、職権を濫用して特定個人情報が記録された文書等を収集	2年以下の懲役or100万以下の罰金	1年以下の懲役 or 50万以下の罰金	―	―
番号の取扱者が対象	個人番号利用事務、個人番号関係事務などに従事する者や従事していた者が、正当な理由なく、業務で取り扱う個人の秘密が記録された特定個人情報ファイルを提供	4年以下の懲役or200万以下の罰金（併科されることあり）	2年以下の懲役 or 100万以下の罰金	―	―
	個人番号利用事務、個人番号関係事務などに従事する者や従事していた者が、業務に関して知り得たマイナンバーを自己や第三者の不正な利益を図る目的で提供し、または盗用	3年以下の懲役or150万以下の罰金（併科されることあり）	1年以下の懲役 or 50万以下の罰金	―	2年以下の懲役 or 100万以下の罰金
誰でも対象	人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入等によりマイナンバーを取得	3年以下の懲役or150万以下の罰金	―	―	―
	個人情報保護委員会から命令を受けた者が、個人情報保護委員会の命令に違反	2年以下の懲役or50万以下の罰金	―	6月以下の懲役 or 30万以下の罰金	1年以下の懲役 or 50万以下の罰金
	個人情報保護委員会による検査等に際し、虚偽の報告、虚偽の資料提出をする、検査拒否等	1年以下の懲役or50万以下の罰金	―	30万以下の罰金	30万以下の罰金
	偽りその他不正の手段によりマイナンバーカードを取得	6月以下の懲役or50万以下の罰金	―		30万以下の罰金

38

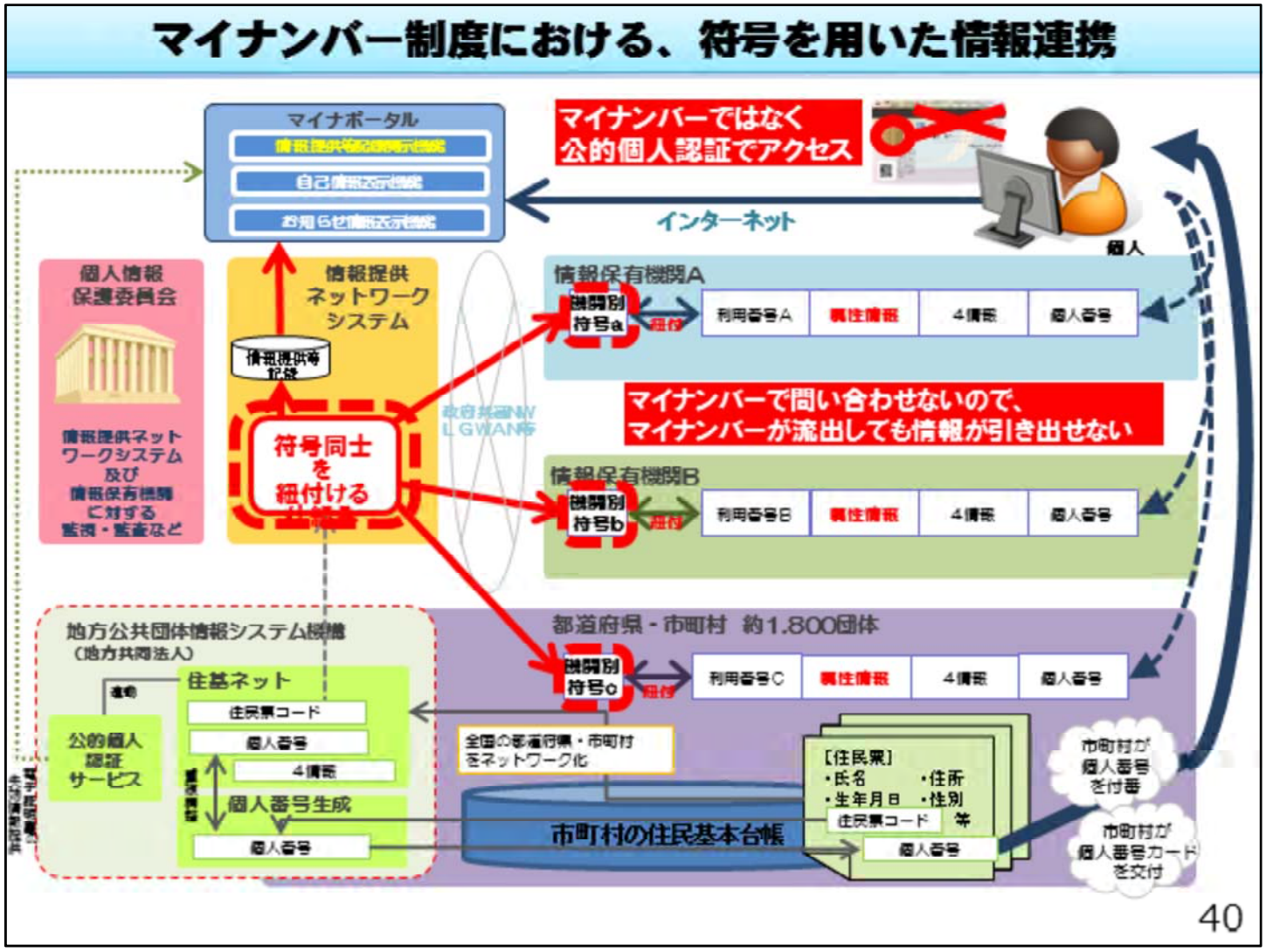
■Punishments were strengthened

Punishments related to My Number System are more strengthened than other punishments of similar provisions in the same type of law.



■Personal information is retained under the decentralized management

In the My Number System, personal Information is de-centrally retained in governmental agents such as regional municipalities and health insurance societies, and “de-centralized management” method, in which the information is exchanged as needed, is adopted utilizing the information-sharing through network system.



■With information sharing, My Number itself is not used

With information sharing, we do not use My Number directly but use a code specifically written to every information possession organization, so that the system prevents leaking out the information one after another and works in safer environment.

Also, through the function “exchange history” of the website “Mynaportal” which is accessible by logging-in using My Number Card, the user will able to check when and between which agencies one’s information was exchanged.