マイナンバー法と情報セキュリティ

石井　夏生利[1]

概 要

本年 2 月，政府は「行政手続における特定の個人を識別するための番号の利用等に関する法律案」を含む 3 つの法案を閣議決定し，国会に提出した．マイナンバー制度は，複数の機関に存在する個人の情報の同一性を確認する制度であり，同制度には，付番及び連携の正確性，本人確認の確実性，情報の漏えいや不正利用の防止，システムの安全性等，情報セキュリティに関する様々な課題が存在する．そこで，本稿では，情報処理技術の分野で一般に用いられている CIA の要素をもとに，マイナンバー法の具体的規定との関係を考察し，情報セキュリティの観点から課題となり得る事項を明らかにする．

1　はじめに

2012(平成 24)年 2 月 14 日，政府は「行政手続における特定の個人を識別するための番号の利用等に関する法律案」(本原稿執筆時点では法案であるが、本稿では、以下「マイナンバー法」という．)を含む 3 つの法案を閣議決定し，国会に提出した．同法の内容は，2011(平成 23)年 4 月 28 日付「社会保障・税番号要綱」(社会保障・税に関わる番号制度に関する実務検討会)及び同年 6 月 30 日付「社会保障・税番号大綱」(政府・与党社会保障改革検討本部)に基づいている．

マイナンバー制度は，社会保障と税を一体化し，所得を正確に把握した上で適切に所得の再分配を実施し，国民が柔軟できめ細やかな社会保障制度・税額控除制度の恩恵を受けるための社会的基盤を構成する．この制度は，①1 人 1 人の個人に固有の「マイナンバー」を付与し，②当該「マイナンバー」を社会保障分野(年金，医療，介護保険，福祉，労働保険)と税務分野(国税，地方税)で連携させ，③国や地方公共団体，日本年金機構や医療機関などの関係機関等が個別に保有している情報について，同一人の情報であることの確認を行うものである．

マイナンバー制度導入に向けた個人情報保護及び情報連携に関する論点整理は，社会保障・税に関わる番号制度に関する実務検討会及び高度情報通信ネットワーク社会推進戦略本部企画委員会の下に設置された「個人情報保護ワーキンググループ」(座長・堀部政男一橋大学名誉教授)及び「情報連携基盤技術ワーキンググループ」(座長・佐々木良一東京電機大学未来科学部情報メディア学科教授)において，2011 年 2 月から検討が進められてきた．マイナンバー制度は，複数の機関に存

[1] 筑波大学図書館情報メディア系　准教授

情報セキュリティ総合科学 第 4 号　2012 年 11 月、論文受付 2012 年 8 月、同 10 月採録

在する個人の情報の同一性を確認する制度であり，その関係で，付番及び連携の正確性，本人確認の確実性，情報の漏えいや不正利用の防止，システムの安全性等，情報セキュリティに関する様々な課題が存在する．

ところで，「情報セキュリティ」という概念を調べてみると，広辞苑第 6 版には，「情報」は「①あることがらについてのしらせ．②判断を下したり行動を起こしたりするために必要な，種々の媒体を介しての知識．」と説明されている．同じく，「セキュリティ」という用語は，「安全，保安，防犯」といった意味で用いられている．また，「セキュリティ」は，単に「安全」と邦訳されることが多い．

しかし，「情報セキュリティ」と一言で表現すると，固有の概念として用いられることが多く，必ずといってよいほど登場するのは，CIA(Confidentiality, Availability, Integrity)という三要素である．CIA は，経済協力開発機構(Organisation for Economic Co-operation and Development, OECD)が 1992(平成 4)年 11 月 26 日に採択した「情報システムのセキュリティのためのガイドライン」(Guidelines for the Security of Information Systems)で初めて登場した．その中では，「情報システムに依存する者を，可用性，機密性，完全性の欠如に起因する危害から保護すること」，つまり，機密性(Confidentiality)，完全性(Integrity)，可用性(Availability)(以下「CIA」と略称する．)を保つことが情報セキュリティであると定義されている．CIA は，情報処理技術の分野で一般に用いられている．

表 1　CIA の概念

機密性	承認された者だけが情報の開示を受けられること
完全性	情報が正確かつ完全であること
可用性	承認された者が必要に応じて情報にアクセスでき，利用できること

各要素が損なわれるべきケースの典型例は，機密性については情報の不正漏えい，完全性については情報の不正改ざんや情報処理結果の誤り，可用性はシステム障害による利用不能であると説明されている．CIA は，国際標準化機構(International Organization for Standardization, ISO)で国際規格化され，日本工業規格(Japanese Industrial Standards, JIS)でも国内規格化されている(ISO/IEC27001:2005、ISO/IEC27002:2005。前者は JISQ27001:2006、後者は JISQ27002:2006 として国内規格化された)．

CIA 以外にも、国際規格である ISO/IEC TR13335-1 及びその国内規格である JISQ13335-1:2006 では、その対象とする「ICT セキュリティ」を「ICT にかかわる機密性、完全性、可用性、否認防止(Non-repudiation)、責任追跡性(Accountability)、真正性(Authenticity)及び信頼性(Reliability)の定義付け、達成及び維持に関連した全ての側面」である定義している[3]。

表 2　付加的4要素の概念

[3] 岡村久道『情報セキュリティの法律』(商事法務，改訂版，2011 年)4－12 頁．

否認防止	ある活動又は事象が起きたことを、後になって否認されないように証明する能力
責任追跡性	あるエンティティの動作が、その動作主のエンティティまで一意に追跡できることを確実にすること
真正性	ある主体又は資源が、主張通りであることを確実にする特性
信頼性	意図した動作及び結果に一致する属性

これらの 4 要素は、マイナンバー制度を通じて情報を結びつける場合には重要な役割を果たすと考えられる。例えば、制度の主要な目的である同一人確認を行うためには、完全性のみならず、責任追跡性や信頼性の確保が必須となるほか、社会保障サービスや税の賦課徴収を裏付けるためには、否認防止、真正性が関係してくるものと思われる。他方、ISO/IEC27002:2005、JISQ27002:2006 では、これらの 4 要素は任意の付加事項となっていることや、追加的 4 要素と法制度との関係を整理するにはかなりの紙幅を要することから、本稿では、主たる要素である CIA を中心に取り上げることとする。マイナンバー法に話を戻すと，前記個人情報保護ワーキンググループ及び情報連携基盤技術ワーキンググループでは，必ずしも情報セキュリティを中心に据えた課題整理は行われてこなかった．そこで，本稿では，マイナンバー法の具体的規定を取り上げつつ，情報セキュリティ(CIA)の観点から課題となり得る事項を明らかにすることとしたい．

2 マイナンバー法の概要[4]

2.1 目次

マイナンバー法は，全 8 章，72 条で構成される．

第 1 章 総則(第 1 条－第 3 条)
第 2 章 個人番号(第 4 条－第 13 条)
第 3 章 特定個人情報の保護等
　第 1 節 特定個人情報の保護(第 14 条－第 18 条)
　第 2 節 情報提供ネットワークシステムによる特定個人情報の提供(第 19 条－第 23 条)
　第 3 節 行政機関個人情報保護法等の特例等(第 24 条－第 30 条)
第 4 章 個人番号情報保護委員会
　第 1 節 組織(第 31 条－第 44 条)
　第 2 節 業務(第 45 条－第 50 条)
　第 3 節 雑則(第 51 条)
第 5 章 法人番号(第 52 条－第 55 条)

[4] 本項の説明に際しては、総務省自治行政局住民制度課の許可を得て、「地方公共団体における番号制度の導入ガイドライン(中間とりまとめ)」(2012 年 9 月)の第 1 章「地方公共団体における番号制度の活用について」1-33 頁を参照させていただいた．

第 6 章　個人番号カード(第 56 条)
第 7 章　雑則(第 57 条－第 61 条)
第 8 章　罰則(第 62 条－第 72 条)
附則

2.2　目次

第 1 条は, 次の 4 つの目的を定めている.

表 3　マイナンバー法の目的

目的 1	行政事務処理者において, 個人番号及び法人番号を活用した効率的な情報の管理, 利用を行うこと.
目的 2	他の行政事務を処理する者との間における迅速な情報の授受を行うこと.
目的 3	手続の簡素化による国民の負担の軽減及び本人確認の簡易な手段を得るための事項を定めること.
目的 4	現行の個人情報保護法制の特例を定め, 個人番号その他の特定個人情報の適正な取扱いを確保すること.

第 2 章以下は、目的 1 に対応するために, 個人番号の付番及びその利用を, 目的 2 に対応するために情報連携を, 目的 3 に対応するために個人番号カードを, 目的 4, に対応するために, 特定個人情報の保護や個人番号情報保護委員会をそれぞれ規定している.

第 2 条は,「行政機関」をはじめとする各種定義を定めているが, 最も重要な規定は, 保護対象としての「特定個人情報」である.

「この法律において「特定個人情報」とは, 個人番号(個人番号に対応し, 当該個人番号に代わって用いられる番号, 記号その他の符号であって, 住民票コード以外のものを含む. 第四条, 第五条, 第五十六条第一項及び第六十二条並びに附則第三条第一項, 第二項及び第四項を除き, 以下同じ.)をその内容に含む個人情報をいう. 」(7 項)

特定個人情報を取り扱う事務には, 個人番号利用事務と個人番号関係事務が存在する. 前者は,「行政機関, 地方公共団体, 独立行政法人等その他の行政事務を処理する者が第六条第一項又は第二項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し, 及び管理するために必要な限度で個人番号を利用して処理する事務」をいい, 後者は,「第六条第三項の規定により個人番号利用事務に関して行われる他人の個人番号を利用して行う事務」をいう(9 項, 10 項). 個人番号利用事務を処理する者及び個人番号利用事務の全部又は一部の委託を受けた者は「個人番号利用事務実施者」, 個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託を受けた者は「個人番号関係事務実施者」という(11 項, 12 項).

また, マイナンバー制度では, 情報システムを通じて情報連携を行うための基盤機能として, 情報提供ネットワークシステムが構築される. これは,「行政機関の長等

の使用に係る電子計算機を相互に電気通信回線で接続した電子情報処理組織であって，暗号その他その内容を容易に復元することができない通信の方法を用いて行われる第十七条第七号の規定による特定個人情報の提供を管理するために，第十九条第一項の規定に基づき総務大臣が設置し，及び管理するものをいう．」と定義されている(13 項).

第 3 条の「個人番号及び法人番号を利用する際の基本」では，次の 4 項目が掲げられている.

表 4 個人番号及び法人番号を利用する際の基本

一号	行政事務の処理において，個人又は法人その他の団体に関する情報の管理を一層効率化するとともに，当該事務の対象となる者を特定する簡易な手続を設けることによって，行政運営の効率化及び国民の利便性の向上に資すること.
二号	情報提供ネットワークシステムその他これに準ずる仕組みを利用して迅速かつ安全に情報の授受を行い，情報を共有することによって，社会保障制度，税制その他の行政分野における給付と負担の適切な関係の維持に資すること.
三号	個人又は法人その他の団体から提出された情報については，これと同一の内容の情報の提出を求めることを避け，国民の負担の軽減を図ること.
四号	個人番号を用いて収集され，又は整理された個人情報が法令に定められた範囲を超えて利用され，又は漏えいすることがないよう，その管理の適正を確保すること.

一号は，行政事務の効率化及び国民の利便性向上，二号は，迅速な情報授受・共有による社会保障及び税制等の分野における給付と負担の関係の維持，三号は，国民の負担軽減，四号は，特定個人情報の管理の適正をそれぞれ謳っている．いずれも目的規定を踏まえた理念であるが，特に二号は，マイナンバー制度自体の目的を表していると考えられる.

2.3 第 2 章「個人番号」

第 4 条は，個人番号の指定及び通知について，市町村長は，マイナンバー制度導入後に出生などによって新たに住民票に住民票コードを記載したときは，地方公共団体情報システム機構から通知された個人番号を指定し，その者に対し，当該個人番号を書面により通知しなければならないことを定めている(1 項). そのために，第 5 条では，個人番号の生成について，市町村長は，あらかじめ同機構に対し，当該指定しようとする者に係る住民票に記載された住民票コードを通知するとともに，個人番号とすべき番号の生成を求めることとされている(1 項)[5]. 個人番号の変更は，住民票コードと異なり，民間事業者も含め個人番号を利用する者が広範囲に及ぶこと

[5] 制度導入時に既に住民票に住民票コードが記載されている者についてはマイナンバー法附則第 3 条 1 項，施行日にいずれの市町村においても住民基本台帳に記録されていないものについては同法 2 項参照.

から, 個人番号の漏えい等, 一定の要件に該当した場合のみ認められている(第 4 条 2 項). これらの市町村の事務は, 法定受託事務である(第 58 条).

マイナンバー法の特徴の 1 つは, 利用目的が法定されていることにある. 現行の個人情報保護法制上, 利用目的の特定は, 行政機関, 独立行政法人等, 個人情報取扱事業者に委ねられてきたが(行政機関個人情報保護法第 3 条 1 項, 独立行政法人等個人情報保護法第 3 条 1 項, 個人情報保護法第 15 条 1 項), マイナンバー法第 6 条では, ①年金の資格取得・確認, 受給, ②雇用保険等の資格取得・確認, 受給, ハローワーク等の事務, ③医療保険等の保険料徴収等の医療保険者における手続, 福祉分野の給付, 生活保護の実施等低所得者対策の事務, ④国民が税務当局に提出する確定申告書, 届出書, 調書等への記載, 当局の内部事務, ⑤被災者生活再建支援金の支給に関する事務その他地方公共団体の条例で定める事務など, その利用目的が限定されている. これは, 特段の配慮を必要とする特定個人情報が本人の意図とは異なる形で利用されないよう, 侵害を未然に防止する趣旨である.

第 7 条から第 9 条は, 個人番号利用事務等実施者による再委託の制限, 委託先の監督, 安全管理措置, 第 10 条は, 個人番号利用事務実施者による情報共有及びその適切な活用への努力義務, 第 11 条及び第 12 条は, 個人番号利用事務等実施者が事務処理を行う際における個人番号の提供要求, 本人確認措置, 第 13 条は全ての者に対する法定外の個人番号提供要求の禁止を定めている.

第 11 条及び第 12 条について, 個人番号を利用できる個人番号利用事務実施者は, 本人に対し個人番号の提供を求めることが認められており(第 11 条 1 項), この場合, 同実施者は, 本人確認及び個人番号確認のため, 個人番号カードの提示を受けることその他その者が本人であることを確認するための措置をとらなければならない(第 12 条)とされている. これらの規定により, 国の機関や地方公共団体等の個人番号利用事務実施者は, 本人から個人番号カードの提示を受け, 本人確認及び個人番号確認を行った上で, 当該本人の情報を収集し, データベースを構築した上で, 個人番号を利用して個人情報を検索し管理することが想定されている.

第 6 条以下は, 第 2 章「個人番号」の章に属するものであるが, 第 3 章「特定個人情報の保護等」と相まって, 個人番号を含む個人情報の適正な取扱いを図るための規定を含んでいる.

2.4 第 3 章「特定個人情報の保護等」

第 3 章は, 第 1 節「特定個人情報の保護」, 第 2 節「情報提供ネットワークシステムによる特定個人情報の提供」, 第 3 節「行政機関個人情報保護法等の特例等」で構成される. 各節の中に, 特定個人情報の作成, 収集, 利用, 提供, 管理, 開示請求等の規定が置かれており, 概ね次の事項が定められている.

表 5 特定個人情報の保護

第 14 条	個人番号情報保護委員会は, 特定個人情報を適切に管理するために講ずべき措置を定めた指針を作成, 公表する.

第 15 条	行政機関の長等は，特定個人情報保護評価を実施する.
第 16 条	第 17 条十号から十三号に定める場合を除き，特定個人情報ファイルの作成を禁止する.
第 17 条	個人番号利用事務ないしは個人番号関係事務を処理するために必要な場合や，情報提供ネットワークシステムを使用する場合などを除き，特定個人情報の提供は禁止される.
第 18 条	第 17 条各号のいずれかに該当する場合を除き，特定個人情報の収集又は保管を禁止する.

第 15 条の特定個人情報保護評価は，新しい制度である. これは，特定個人情報ファイル(個人番号をその内容に含む個人情報ファイル)が取り扱われる前に，プライバシーや特定個人情報に与える影響を予測・評価し，かかる影響を軽減する措置をあらかじめ講じるという仕組みであり，アメリカ，カナダ，オーストラリア，イギリスに設けられているプライバシー影響評価(Privacy Impact Assessment)に相当するものである.

また，第 17 条七号の定める情報提供ネットワークシステムを用いた情報連携は，マイナンバー制度の主眼となる仕組みである. 同条は，国の機関や地方公共団体等の個人番号利用事務実施者が，個人番号を利用して情報収集し，管理している特定個人情報については，原則的に，他の機関に提供することを禁止している. しかし，同条七号では，マイナンバー法別表第二に掲げられた情報照会者が同表に掲げられた情報提供者に対し，同表の事務を処理するために必要な特定個人情報の提供を求めた場合に，当該情報提供者が情報提供ネットワークシステムを使用して当該特定個人情報を提供することが認められている[6].

表 6　情報提供ネットワークシステムによる特定個人情報の提供

第 19 条	総務大臣は，個人番号情報保護委員会と協議の上，情報提供ネットワークシステムを設置，管理する.
第 20 条	情報提供者は，第 17 条七号の規定により，情報提供ネットワークシステムを使用して特定個人情報の提供を求められた場合，情報照会者に対し，当該特定個人情報を提供しなければならない.
第 21 条	情報照会者及び情報提供者は，情報提供ネットワークシステムを使用して特定個人情報の提供の求め又は提供があったときは，その記録を保存しなければならない.
第 22 条	総務大臣，情報照会者及び情報提供者は，情報提供等事務に関する秘密について，漏えい防止その他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.
第 23 条	情報提供等事務又は情報提供ネットワークシステムの運営に関する事務に従事する者又は従事していた者は，その業務に関して知り得た当該事務

[6] マイナンバー法別表 2 参照.

	に関する秘密を漏らし，又は盗用してはならない.

表 7 行政機関個人情報保護法等の特例等

第 24 条	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，個人情報保護法の一部規定を適用除外し，他の規定を読み替える.
第 25 条	情報提供等の記録について，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の一部規定を適用除外し，他の規定を読み替える.
第 26 条	地方公共団体等において，特定個人情報の適正な取扱い及び開示，訂正，利用の停止，消去及び提供の停止を実施するために必要な措置を講ずる.
第 27 条～第 30 条	個人番号取扱事業者は，特定個人情報の取扱いの制限や安全管理措置等を講じる義務を負うほか，個人情報保護法と同様の適用除外を受ける.

第 25 条について，社会保障・税番号大綱では，「情報保有機関が保有する自己の「番号」に係る個人情報等を確認できるように，かかる情報を，個人一人ひとりに合わせて表示することができるマイ・ポータルを設けること」とし，それにより「情報保有機関が保有する自己の「番号」に係る個人情報の確認，電子申請，行政機関等からのお知らせの確認」ができると記されている. マイ・ポータルは，2016(平成 28)年 1 月を開始予定としており，この仕組みでは，情報提供ネットワークシステムを介した特定個人情報のやり取りについて，情報照会者及び情報提供者の名称，その日時，特定個人情報の項目等を，本人自ら確認できることが想定されている(第 21 条，第 25 条). そのために，特定個人情報の開示を任意代理人が行えるようにするなど，行政機関の保有する個人情報の保護に関する法律等の特例が設けられている.

2.5 第 4 章から第 7 章

第 4 章「個人番号情報保護委員会」は，第 1 節「組織」，第 2 節「業務」，第 3 節「雑則」にて構成されている. 同委員会は，いわゆる三条委員会として，職権行使の独立性(第 34 条)が保障されており，指導及び助言，勧告及び命令，報告及び立入検査といった監督権限(第 45 条－第 47 条)を付与されている. 個人情報保護に関する独立監視機関が存在しないという問題は，特に，国際的整合性との関係で長年にわたり指摘されてきた[7]. マイナンバー法では，かかる機関を初めて設置することとなり，その実効性が今後の課題となる.

第 5 章は，「法人番号」について，通知等(第 52 条)，情報の提供の求め(第 53 条)，資料の提供(第 54 条)，正確性の確保(第 55 条)を定めている.

第 6 章は，「個人番号カード」について，市町村長による交付，転入届や記載事項変更に伴う市町村長への個人番号カードの提出，同カード紛失時の市町村長への届出，市町村の機関による条例に基づく個人番号カードの利用等を定めている(第

7 堀部政男「プライバシー・個人情報保護の国際的整合性」同編著『プライバシー・個人情報保護の新課題』(商事法務，2010 年)1 頁以下ほか多数.

56 条). マイナンバー制度では, 本人にサービスや給付を行うため, すべての国民が様々な場面で本人確認及び個人番号確認を求められる可能性がある. 個人番号カードは, その確実な確認手段であり, そのために, 原則としてすべての国民に対して提供される. 個人番号カードの交付事務は, 市町村の法定受託事務である(第 58 条).

その他, 第 7 章の「雑則」は, 指定都市の特例や, 事務の区分等を定めている.

2.6 第 8 章

第 8 章は「罰則」を定めている[8].

表 8 個人番号を利用する者に関する罰則(直接罰)

第 62 条	個人番号利用事務等に従事する者又は従事していた者等が, 正当な理由なく, その業務に関して取り扱った個人の秘密に属する事項が記録された特定個人情報ファイルを提供したとき	4 年以下の懲役若しくは 200 万円以下の罰金又は併科
第 63 条	個人番号利用事務等に従事する者又は従事していた者等が, その業務に関して知り得た個人番号を不正な利益を図る目的で提供又は盗用したとき	3 年以下の懲役若しくは 150 万円以下の罰金又は併科
第 64 条	情報提供等事務又は情報提供ネットワークシステム運営事務に従事する者又は従事していた者が, 秘密を漏らし又は盗用したとき	3 年以下の懲役若しくは 150 万円以下の罰金又は併科
第 66 条	国の機関, 地方公共団体の機関等の役員若しくは職員が, 職権を濫用して, 専らその職務の用以外の用に供する目的で個人の秘密に属する特定個人情報が記録された文書等を収集したとき	2 年以下の懲役又は 100 万円以下の罰金

表 9 個人番号等を不正に取得する行為等に対する罰則(直接罰)

第 65 条	何人も, 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, 不正アクセス行為その他の管理侵害行為により, 個人番号を取得したとき	3 年以下の懲役又は 150 万円以下の罰金
第 70 条	何人も, 偽りその他不正の手段により個人番号カードの交付を受けたとき	6 月以下の懲役又は 50 万円以下の罰金

[8] 第 71 条に基づき, 第 62 条から第 67 条までは国外犯処罰規定の対象であり, 第 72 条に基づき, 第 62 条、第 63 条, 第 65 条又は第 68 条から第 70 条までは両罰規定の対象である. 各罰則規定の分類は, 内閣官房社会保障改革担当室の法案説明資料 (http://www.cas.go.jp/jp/seisaku/bangoseido/houansetumei/siryou1.pdf)に基づいた.

表 10 個人番号情報保護委員会に関する罰則(間接罰)

第 67 条	個人番号情報保護委員会の委員長等による秘密の漏えい又は盗用	2 年以下の懲役又は 100 万円以下の罰金
第 68 条	個人番号情報保護委員会の命令に違反したとき	2 年以下の懲役又は 50 万円以下の罰金
第 69 条	個人番号情報保護委員会による報告及び立入検査に対し,虚偽の報告,虚偽の資料提出,検査拒否等を行ったとき	1 年以下の懲役又は 50 万円以下の罰金

3 CIA との関係

3.1 マイナンバー法と CIA

以上をもとに,マイナンバー法のうち,主に,特定個人情報の取扱いを規律する規定を中心に,機密性,完全性,可用性との関係を整理する.

前記のとおり,CIA の各要素が損なわれるべきケースの典型例は,機密性については情報の不正漏えい,完全性については情報の不正改ざんや情報処理結果の誤り,可用性はシステム障害による利用不能であると説明されている.ただし,CIA による区分は相対的でもある.例えば,不正アクセスによってクレジットカード情報が漏えいした場合を考えると,情報漏えいは機密性を侵害するが,その結果,カード番号が悪用されれば完全性を侵害する.また,データの一部毀損は完全性の侵害であるが,大量にデータが毀損すれば,可用性を侵害する.特に,可用性に該当する事項は,原則として完全性にも該当しうることから[9],規定の関係を論じる際は,後者に関わる事項は前者を包含して考えることができる.そして,マイナンバー法には電気通信設備の機能に障害を与えることを禁ずる規定は存在せず,むしろ,可用性の問題は,システムのセキュリティに依存している.なお,コアシステムである情報提供ネットワークシステムについては,第 8 回情報連携基盤技術ワーキンググループの 2012 年 3 月 23 日付資料「情報提供ネットワークシステム等の機能の概要(案)」において,セキュリティ管理機能(他のシステムと送受信するデータの暗号化,機関認証,運用要員管理等により,コアシステムを通じて行われる情報提供に利用される特定個人情報及びその他の情報を保護する機能)を付すことが記されている[10].

そこで,本稿では,主に,機密性と完全性に焦点を当てて,検討を加えることとする.

3.2 CIA 全体を担保する規定

マイナンバー法は,第 3 条の利用の基本の第二号において,情報提供ネットワークシステムその他これに準ずる仕組みを利用して迅速かつ安全に情報の授受を行う

9 岡村・前掲『情報セキュリティの法律』4 頁,170 頁.

10 http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai8/siryou4-2.pdf.

ことを謳っている. これは, 法全体を包含する基本原則である.

この原則を最も直接的に具体化したものは, 安全管理措置の規定である.

同法第 9 条 1 項は,「個人番号利用事務実施者及び個人番号関係事務実施者(以下「個人番号利用事務等実施者」という.)は, 個人番号の漏えい, 滅失又は毀損の防止その他の個人番号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. 」と定めている. 同法第 22 条の「秘密の管理」においても, 情報提供等事務に関する秘密について, 同旨の規定を設けている[11]. 同法は個人情報保護法制の特別法であることから, これらの規定は, 行政機関個人情報保護法第 6 条 1 項, 独立行政法人等個人情報保護法第 7 条 1 項, 個人情報保護法第 20 条の定める各安全管理措置に倣ったものとなっている.

上記文言を CIA に当てはめてみると, 不正漏えい防止は機密性に対応し, 滅失又は毀損の防止は完全性に対応している. ただし,「漏えい, 滅失又は毀損」は例示にすぎず, 少なくとも漏えいが発生すれば機密性が損なわれ, 滅失又は毀損が一部のみに発生すれば完全性が, 多数の部分に発生すれば可用性が損なわれる. したがって, ここにいう「個人番号の適切な管理のために必要な措置」とは, 実質的には CIA の 3 要素全てに関連する概念である[12].

安全保護措置に関しては, 個人情報保護法では個人情報取扱事業者による委託先の監督(第 22 条), 行政機関個人情報保護法及び独立行政法人等個人情報保護法では受託者における安全確保の措置(行政機関個人情報保護法第 6 条 2 項, 独立行政法人等個人情報保護法第 7 条 2 項)が定められている. マイナンバー法では, 個人情報保護法に倣う形で, 委託先の監督(第 8 条)を設けているが, それに加えて, 再委託の制限(第 7 条)を新たに定めている. 第 7 条は, 個人情報利用事務等の委託・再委託が日常的に行われることを踏まえ, 委託元の許諾を得た場合に限り, 個人番号利用事務等の再委託を認めないとする規定である.

第 9 条の定める「個人番号利用事務等実施者」には, 個人番号利用事務ないしは関係事務の受託者が含まれる(第 2 条十一号及び十二号). また, 第 7 条 2 項に基づき, 受託者には再受託者も含まれるため, 全ての受託者は, 第 9 条に基づき安全管理措置を講じなければならない.

以上のほかにも, CIA 全体を担保するための重要な規定が存在する. 利用範囲の法定(第 6 条)[13], 特定個人情報保護評価(第 14 条, 第 15 条), 個人番号情報保護委員会による監督(第 31 条－第 51 条), 同委員会の命令違反, 同委員会への報告義務違反に対する罰則(第 68 条, 第 69 条)である.

---

11 個人番号取扱事業者については, 第 28 条, 第 29 条, 第 30 条 2 項参照.

12 岡村・前掲『情報セキュリティの法律』65 頁.

13 個人番号取扱事業者については第 27 条参照.

3.3 機密性の保護

3.3.1 機密性と各規定

情報セキュリティとの関係で，マイナンバー法は，機密性を確保するための規定を数多く有している点に特徴を有する．条文中に「漏えい」，「提供の制限」，「秘密保持」という言葉を使う規定には，以下のものがある．

表 11 漏えい関係

第 3 条四号	個人番号の利用の基本
第 4 条 2 項	個人番号通知の際の措置
第 9 条	個人番号利用事務等実施者の責務
第 14 条	個人番号情報保護委員会による指針
第 22 条	情報提供等事務における秘密の管理
第 28 条	個人番号取扱事業者が保有する特定個人情報の保護

表 12 提供制限関係

第 13 条	提供の求めの制限
第 15 条 6 項	特定個人情報保護評価
第 17 条	特定個人情報の提供の制限[14]

表 13 秘密保持関係

第 22 条	秘密の管理
第 23 条	秘密保持義務
第 43 条	秘密保持義務

特定個人情報ファイル，個人番号，秘密等に関する機密性を侵害した場合の罰則は，第 62 条から第 64 条まで及び第 67 条が該当し，個人情報保護法制よりも厳しい法定刑が定められている．

3.3.2 機密性が重視される土壌の形成

日本では，2005(平成 17)年 4 月 1 日に個人情報保護法が全面施行された直後に，対象事業者が個人情報保護法の抵触をおそれて過度に萎縮するという「過剰反応」と呼ばれる事態が生じた．この問題を投げかけたのは，全面施行直後の同年 4 月 25 日に発生した JR 福知山線脱線事故であった．この事故では，JR 西日本や病

[14] なお，マイナンバー法第 21 条は，情報提供ネットワークシステムを通じた特定個人情報の提供等があった場合の記録保存義務を定めている．提供等は機密性に位置づけられるが，第 21 条に関しては，データの消失・紛失を防ぐという意味で，可用性の保護に位置づけることもできる．

院などが，死傷者情報を，個人情報であることを盾にメディアに提供せず，この事態が大きな論議を呼んだ．また，個人情報保護法が脚光を浴びるようになった後，情報漏えい事故がメディアで大きく取り上げられるようになり，企業を中心に，事業者等はとかく漏えい防止に腐心するようになった．

また，個人情報保護ワーキンググループ及び情報連携基盤技術ワーキンググループでは，住民基本台帳ネットワークシステムに関する2008(平成20)年3月6日付最高裁判所判決[15]を十分に踏まえる必要があるとの認識に基づき，検討が進められてきた．同判決は，「憲法 13 条は，国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているものであり，個人の私生活上の自由の一つとして，何人も，個人に関する情報をみだりに第三者に開示又は公表されない自由を有するものと解される…住基ネットのシステム上の欠陥等により外部から不当にアクセスされるなどして本人確認情報が容易に漏えいする具体的な危険はないこと，受領者による本人確認情報の目的外利用又は本人確認情報に関する秘密の漏えい等は，懲戒処分又は刑罰をもって禁止されていること，住基法は，都道府県に本人確認情報の保護に関する審議会を，指定情報処理機関に本人確認情報保護委員会を設置することとして，本人確認情報の適切な取扱いを担保するための制度的措置を講じていること」を合憲性の要件としている．

日本におけるプライバシー権は，東京地方裁判所 1964(昭和 39)年 9 月 28 日の『宴のあと』事件判決[16]以降，「私生活をみだりに公開されないという法的保障ないし権利」であると理解されてきた．最高裁判所は，「プライバシー」という言葉を長年にわたって回避してきたが，他方，1969(昭和 44)年 12 月 24 日付京都府学連事件判決では，「何人も，その承諾なしに，みだりにその容ぼう・姿態(以下「容ぼう等」という．)を撮影されない自由を有する」[17]，1995(平成 7)年 12 月 15 日付外国人指紋押捺拒否事件判決では，「何人もみだりに指紋の押なつを強制されない自由を有する」[18]ことについて，個人の私生活上の自由の一つとして憲法 13 条により保障されると判断した．また，勾留理由開示手続が行われた法廷において，刑事事件の被疑者の容貌・姿態を無断で撮影した行為が問題となった事件ではあるが，2005(平成 17)年 11 月 10 日付最高裁判所判決は，京都府学連事件判決を引用しつつ，「人は，自己の容ぼう等を撮影された写真をみだりに公表されない人格的利益も有すると解するのが相当」である等と述べて不法行為法上の違法性を認めた[19]．

個人に関する情報との関連では，前科照会事件において，最高裁判所は，1981(昭和 56)年 4 月 14 日，「前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有する」[20]ことを認め，1994(平成 6)年 2 月 8 日付『逆

15 最一小判平成 20 年 3 月 6 日判タ 1268 号 110 頁．
16 東京地判昭和 39 年 9 月 28 日下民集 15 巻 9 号 2317 頁．
17 最大判昭和 44 年 12 月 24 日刑集 23 巻 12 号 1625 頁．
18 最三小判平成 7 年 12 月 15 日刑集 49 巻 10 号 842 頁．
19 最一小判平成 17 年 11 月 10 日民集 59 巻 9 号 2428 頁．
20 最三小判昭和 56 年 4 月 14 日民集 35 巻 3 号 620 頁．

転』事件判決では前科照会事件判決を踏襲した[21]. さらには, 2003(平成 15)年 9 月 12 日の早稲田大学講演会名簿提出事件判決[22]において, 最高裁判所は, 氏名, 学籍番号, 住所, 電話番号のような個人識別等のための単純な情報であっても,「本人が, 自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり, そのことへの期待は保護されるべきものである」と述べ,「このようなプライバシーに係る情報は, 取扱い方によっては, 個人の人格的な権利利益を損なうおそれのあるものであるから, 慎重に取り扱われる必要がある」と判示し, 不法行為の成立を認めた. 以上のように, 日本のプライバシー関連訴訟では,「公開」ないしは「開示」の態様によるものが多数を占めてきた[23].

住基ネット判決に基づく考慮事項のうち,「何人も, 個人に関する情報をみだりに第三者に開示又は公表されない自由」との判旨部分は, 京都府学連事件判決を引き継いでおり, その後の一連の流れを汲んだ最高裁判所の考え方が示されているといえる.

以上のように, 日本のプライバシー・個人情報保護は, 個人に関する情報を明らかにされることからの保護であるという認識が浸透しており, その認識を定着させる土壌が存在していたと考えられる. マイナンバー法に機密性を保護するための多くの規定が存在するのは, 機密性を重視する起草者の認識が現れているとも考えられる.

3.3.3 収集・作成の制限等

機密性は, 裏を返せば他者による情報収集の制限であり, マイナンバー法には, 公開や漏えい以外に, 収集ないしは作成を制限する規定が存在する. 同法は, 第 17 条の提供制限の次に,「何人も, 前条各号のいずれかに該当する場合を除き, 特定個人情報(他人の個人番号を含むものに限る.)を収集し, 又は保管してはならない」旨を定めている(第 18 条). 第 17 条の関係では, 同条の第十号から第十三号に該当する場合を除き, 個人番号利用事務等の従事者に対して, 特定個人情報ファイルの作成を制限する規定が設けられている(第 16 条). 管理侵害行為等による個人番号の取得及び職権濫用等による特定個人情報の収集に対しては, 前記の罰則が置かれている(第 65 条, 第 66 条).

さらに, マイナンバー法は, 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, 個人情報保護法の特例を設け, 個人番号利用事務等実施者に対し, 特定個人情報の開示を義務づけている. 特定個人情報は, 本来的には個人番号利用事務等以外の目的による開示を許されるべきではないが, 本人は, 機密性にいう「アクセスを許可された者」に該当することから, 開示が認められている(第 24 条のうち, 開示にかかわる特例[24]). また, 第 11 条は, 個人番号利用事務等実施者による個人

---

21 最三小判平成 6 年 2 月 8 日民集第 48 巻第 2 号 149 頁.

22 最二小判平成 15 年 9 月 12 日民集 57 巻 8 号 973 頁.

23 プライバシーを人格権に含め、これに基づく差止請求の存在を認容した判決として,『石に泳ぐ魚』事件判決(最三小判平成 14 年 9 月 24 日判タ 1106 号 72 頁)参照.

24 第 25 条の情報提供等の記録に関する特例も同様である.

番号の提供要求を認めているが，この場合，個人番号利用事務等実施者が「アクセスを許可された者」に該当することとなる．

3.4 完全性の保護

「完全性」は，情報が正確かつ完全であることをいう．情報の完全性は，作成名義の同一性と情報内容の完全性に大別することができる．前者の典型例は，「偽造」「成りすまし」であり，後者の典型例は「変造」「改ざん」である[25]．

マイナンバー法第 1 条は，「…特定の個人及び法人その他の団体を識別する機能を活用して…本人確認の簡易な手段を得られるようにする」ことを目的に置いており，正確性の確保は法の主目的である．日本では，2006(平成 18)年 6 月に約 5,000 万件の年金記録が未統合である事実が明るみに出て社会問題化したほか，社会保険庁(当時)が組織的に改ざんに関与する事態も発生し，メディアで大きく取り上げられた．マイナンバー制度は，こうした問題の再発を防ぐための制度でもある．

作成名義の同一性との関係では，第 12 条において，個人番号利用事務等実施者が本人から個人番号の提供を受けるときの本人確認措置が定められている．第 70 条は，偽りその他不正の手段により個人番号カードの交付を受ける行為に対する罰則が置かれている．

情報内容の正確性について，第 23 条の秘密保持義務が盗用を禁止するほか，個人番号カードについて，記載事項に変更があったときの 14 日以内の届出義務，個人番号カードを紛失したときの届出義務，有効期間満了時における個人番号カードの返納義務(第 56 条 4 項－6 項)が定められている．

特定個人情報の正確性自体には，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，個人情報保護法の各規定が適用される．前 2 つの法律は，「利用目的の達成に必要な範囲内」で，保有個人情報が「過去又は現在の事実と合致」するよう「努めなければならない」と定めており，個人情報保護法は，「利用目的の達成に必要な範囲内」において，個人データを「正確かつ最新の内容に保つ」よう「努めなければならない」と定めている(行政機関個人情報保護法第 5 条，独立行政法人等個人情報保護法第 6 条，個人情報保護法第 19 条)．行政機関及び独立行政法人等に関する各個人情報保護法は，過去又は現在の事実への合致となっており，個人情報保護法は，正確かつ最新の内容を保つことが求められている点で異なるが，「利用目的達成に必要な範囲内」の「努力義務」にとどまる点は共通する[26]．

マイナンバー法では，法遵守の担保措置として，個人番号情報保護委員会の監督(第 31 条以下)及び罰則(第 62 条以下)の各制度を設けている．他方，一般法である個人情報保護法を見ると，正確性の確保は主務大臣の勧告対象ではなく，命令，間接罰の対象にもならない．行政機関個人情報保護法にも独立行政法人等個人情報保護法にも，正確性の確保に違反した場合の罰則は存在しない．

これに対し，マイナンバー法第 46 条 1 項は，「委員会は，特定個人情報の取扱い

---

25 岡村・前掲『情報セキュリティの法律』170-171 頁．

26 法人番号に関しては，マイナンバー法第 55 条参照．

に関して法令の規定に違反する行為が行われた場合において，特定個人情報の適正な取扱いの確保のために必要があると認めるときは，当該違反行為をした者に対し，期限を定めて，当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる」と定めており，勧告の対象を限定していない．しかし，努力義務は，これに違反する行為を違法・無効とするものではなく，当事者の自主的履行を促す趣旨の規定である．したがって，特定個人情報であったとしても，個人番号情報保護委員会の監督権限は及ばず，間接罰も及ばないと考えられる．

また，本人は，自らの情報が不正確な場合には，行政機関及び独立行政法人等に対し，それぞれを規律する個人情報保護法に基づき，訂正請求権を行使することが認められており，その前提となる開示請求権も，手続とともに制度化されている(行政機関個人番号情報保護法第 12 条以下，独立行政法人等個人番号情報保護法第 12 条以下，マイナンバー法第 24 条による読み替え)．しかし，個人情報取扱事業者に対する開示の「求め」は，裁判に訴え出ることのできる具体的権利ではないという判決が下されており[27]，この結論は，訂正等や利用停止等の制度にも同様の解釈を及ぼすこととなる．

4 おわりに

以上見てきたとおり，マイナンバー法は，完全性・可用性と比較すると，機密性に関する規定をはるかに多く有しており，違反した場合の法定刑も厳格である．これは，1 つには，個人情報保護法施行直後に過剰反応が発生し，その後も情報漏えいが社会的に注目を集めてきたことや，プライバシー侵害訴訟が「開示」，「公開」型を中心に争われてきたという日本特有の事情が影響していると考えられる．他方、プライバシー権の提唱国であるアメリカでは、様々な侵害類型による多数の裁判例が蓄積されてきている。不法行為の場面では、いわゆるプロッサーの 4 類型である「不法侵入」、「私的事実の公開」、「公衆の誤認」、「盗用」の類型に基づく訴訟が提起され、憲法に関わる場面では「通信の秘密」の侵害、「無令状捜索・差押え」、「自己決定権」の侵害、「私的事実の公開」という類型で多様な類型の訴訟が提起されてきた。

しかし，「公開」、「開示」型を中心とする日本特有の議論方法では、マイナンバーのもたらす問題には対処できないと考えられる。前記のとおり，マイナンバー制度の目的は，個人番号を用いた本人確認を正確に行うことである．したがって，同制度との関連では，完全性の確保がその本質であり，機密性は，その手段に位置づけられるはずである．また，情報セキュリティの全体的な向上には，CIA をバランス良く機能させることが重要であることから，マイナンバー法が機密性を重視することに対しては，規定のバランスや法執行の実効性の点において，課題が生じるであろうと考えられる．

---

[27] 開示請求権の有無が争われた事例につき，東京地判平成 19 年 6 月 27 日判時 1978 号 27 頁．鈴木正朝「個人情報保護法とプライバシーの権利 －「開示等の求め」の法的性質－」堀部・前掲『プライバシー・個人情報保護の新課題』61 頁以下．

マイナンバー制度は，法制度とシステムの安全性が車の両輪の関係に立ち，適切な形で機能させなければならない．法制度及びシステムの双方にかかる新たな仕組みとしては，特定個人情報保護評価やマイ・ポータルの仕組みが存在する[28]．これらの仕組みを有効活用しながら，全体的なセキュリティレベルの担保を図っていくことが求められる．

参考/引用文献

[1] 岡村久道『情報セキュリティの法律』(商事法務，改訂版，2011 年)
[2] 佐々木良一監修・手塚悟編著『情報セキュリティの基礎』(共立出版，2011 年)
[3] 堀部政男編著『プライバシー・個人情報保護の新課題』(商事法務，2010 年)
[4] 名和小太郎『情報セキュリティ―理念と歴史』(みすず書房，2005 年)
[5] 政府・与党社会保障改革検討本部 2011 年 6 月 30 日決定「社会保障・税番号大綱」(http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110630/honbun.pdf)
[6] 社会保障・税に関わる番号制度に関する実務検討会 2011 年 4 月 28 日付「社会保障・税番号要綱」(http://www.cas.go.jp/jp/seisaku/bangoseido/youkou_honbun.pdf)
[7] 政府・与党社会保障改革検討本部 2011 年 1 月 31 日決定「社会保障・税に関わる番号制度についての基本方針―主権者たる国民の視点に立った番号制度の構築―」(http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110131/honbun.pdf)
[8] 個人情報保護ワーキンググループ 2011 年 6 月 22 日付「社会保障・税番号制度における個人情報保護方策について大綱に盛り込むべき事項」(http://www.cas.go.jp/jp/seisaku/jouhouwg/taiko.pdf)
[9] 個人情報保護ワーキンググループ 2011 年 6 月 23 日付「個人情報保護ワーキンググループ報告書」(http://www.cas.go.jp/jp/seisaku/jouhouwg/houkokusho.pdf)
[10] 情報連携基盤技術ワーキンググループ 2011 年 7 月 28 日付「中間とりまとめ」(http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/cyukan/cyukan.pdf)
情報保護評価サブワーキンググループ 2012 年 3 月 13 日付「特定個人 情報保護評価 情報保護評価 情報保護評価 情報保護評価 指針 素案(中間整理) 行政機関・独立行政法人等・機構・情報提供ネットワークシステムを使用する事業者向け」(http://www.cas.go.jp/jp/seisaku/jouhouwg/hyoka/pdf/sisin.pdf)
[11] 総務省自治行政局住民制度課「地方公共団体における番号制度の導入ガイドライン(中間とりまとめ)」

[28] 特定個人情報保護評価は、特定個人情報ファイル(マイナンバーを含む個人情報ファイル)の保有・変更にあたり、プライバシーや特定個人情報へ及ぼす影響を事前に評価し、その保護のための措置を講じる仕組みであり、マイナンバー法第 14 条以下に定められている。マイ・ポータルは、国民 1 人 1 人が、自己情報・情報提供ネットワークシステムを通じた特定個人情報へのアクセス記録を確認できる仕組みであり、マイ・ポータルを通じたプッシュ型・ワンストップサービスなども予定されている。マイナンバー法上では、情報提供等の記録及び保存の義務(第 21 条)、開示・訂正・利用停止等の請求に関する行政機関個人情報保護法等の特例(第 25 条)などにおいて関連する規定が置かれている。