特定個人情報保護評価書

記載要領と記載ポイント

－自治体編－

平成２７年８月

特定非営利活動法人情報システム監査普及機構

改訂：平成２７年９月１日

はじめに

平成２７年１０月から住民票を有する全ての人に個人番号が付番され、社会保障、税、災害対策の分野で効率的に情報を管理して活用されます。平成２８年１月から各自治体等において、各種の申請手続において個人番号や特定個人情報（個人番号を含む個人情報）が活用されていくことになります。　いわゆる「マイナンバー制度」と呼ばれるものです。　これは、「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（平成２５年法律第２７号）」に基づく制度のことで、マイナンバー制度の導入により、各種手続が便利になる反面、個人情報の漏えいやプライバシーの侵害等、制度の運用に対する懸念にどのように対応するかが課題となります。

そこで、マイナンバー制度では、行政機関や地方公共団体等が特定個人情報ファイル（特定個人情報の集合物）を情報システムにおいて保有しようとする場合、個人のプライバシー等の権利利益に与える影響を予測した上で特定個人情報の漏えいその他の事態を発生させるリスクを分析し、リスクを軽減するための適切な措置を講ずることを宣言する仕組みを構築することになります。この仕組みを「特定個人情報保護評価」といい、これにより「個人のプライバシー等の権利利益の侵害の未然防止」と「国民・住民の信頼の確保」の実現を図ることとしています。

本書は、自治体等が公表にあたり事前に作成された「特定個人情報保護評価書」（以後、「評価書」と言う。）を、特定非営利活動法人情報システム監査普及機構のメンバーにより主要な自治体を選定し、作成上の留意点や指摘事項、改善事項記載を検証したものです。記載にあたっては、できる限り共通的に挙げられる点を討議し、一般化して表現したものです。

記載要領と記載ポイントの総括

総括的にいえますことは、選定し検証した自治体（以後、「自治体」と言う。）が提出されています評価書は全般的に非常に酷似した内容になっています。これは、国が示した記載要項が雛形になって評価書を作成されているからと言えます。また、評価書の内容に具体性が乏しく、どのようにすればよいのか理解できない記載が多々見受けられます。これは、特定個人情報保護の評価書の作成が義務付けられ、とにかく評価書を作成して、提出することに傾注したことによるものと言えます。その反面、特定個人情報保護のためのリスク対策を前向きにとらえ、リスク対策を積極的に推進しようしている自治体の評価書は、内容が誠実に記載されているばかりでなく、具体的な内容も多く記載がなされています。自治体により特定個人情報保護評価制度の受け止め方の温度差を感じます。

リスク対策には、大きく分けて、「リスクの低減」「リスクの保有」「リスクの回避」「リスクの移転」の４つがあります。そこで、重要となるのはリスクの低減で、このリスクの低減のための実効的対策が情報セキュリティ対策であります。

本書は、検証した評価書をもとに、全体をとおして共通的にいえる記載ポイントについて記述していきます。

１．　情報セキュリティ対策のレイヤーと実効性

まず、最初に言えることは、情報セキュリティに対する理解が不足していることです。これは、自治体の首長をはじめＣＩＯ（情報担当役員）等の情報システムに対する理解がなされていないことによります。最も顕著な間違った考え方は、「情報セキュリティは情報システム部署に任して、実施すればよい。」という考え方です。この考え方が組織全体の情報セキュリティに対する理解をなくしてしまい、その結果、実効性のある情報セキュリティの実現は不可能となるでしょう。

下記の表は、情報セキュリティ対策の実効性のある実施の難しさを記載したものです。レベルが上になるほど実効性のある実施は難しくなります。それは、レベルが上位になるほど、「人間の心や考え方」にもとづいて、ひとり一人の個人の行動に依存することになり、情報セキュリティに対する最も難しい側面です。通常、「情報倫理」とも言われ、このレベルまで実行されなければ、実効性の高い情報セキュリティは実現しません。その実現には、組織全体の「情報セキュリティ文化の醸成」が求められます。

表1　情報セキュリティ対策での「実行に難しさ」のレベルとその脆弱性

レベル	情報セキュリティ対策	事　例	対策の課題
4	法・倫理的対策	法律・条令の厳罰化による規制。規程・規則の強化による規制。コンプライアンス組織の新設、強化等。 「情報倫理」教育による行動規範（「して良いこと」「しては悪いこと」を教える。より低年齢を対象に教育を実施することで効果が上がる）。	一時的にはセキュリティ効果が高められるが、法的な盲点や抜け道をつくる、無視・無謀な行動、組織的な共謀が脆弱性を発生させる。 この効果的実現には、最終的に「セキュリティ文化の醸成」をはかることになる。それには、継続的な教育・啓蒙が重要となる。
3	組織・管理的対策	組織権限の集中化による管理統制の効果をはかる。組織の階層化・牽制機能の強化（二重・三重の検閲等）。情報セキュリティ監査やシステム監査の強化。会議・教育・指導頻度の増加等。	脅威の現実化が起らないとこの対策の実施は縮小することが多い（慣れにより対策を無視される）。また、組織・管理時対策は、共謀に最も弱く、組織の脆弱性環境が増大化する。
2	システム的対策	パスワードの設定・複雑化・長コード化等。データの暗号化、通信の暗号化。携行端末（モバイル、スマートフォン等）からの接続禁止、システムの集中管理（時代の分散化と逆行）、ウイルス対策、自動ログ監視の強化等、論理的なアクセス管理や技術的対策が主である。	システムとの接点で人的な側面の脆弱性とつながってくる。例：パスワードのメモ、ノートへの記載、システム機能を取り外す行為等、情報システムの運用に脆弱性が発生する。可能であれば、対策の自動化が求められる。
1	物理的対策	鍵の設置、ドアの二重化。入口・出口での身体検査。監視カメラの設置。利用できる部屋・人・端末の限定等、入れない・近づけない等のゾーン管理。物理的アクセス管理やセキュリティ機器の活用が主である。	鍵を掛けなかったり、施錠を忘れたりする人間の怠惰や忘却と密接に関連し，脆弱性が発生する。

例えば、レベル１の物理的対策では、鍵をかけたり監視カメラで入室を監視したりする等、物理的に禁止や制限する対策であります。一般に物理的な対策は、機器の投資を強化すれば情報セキュリティはより実効性を高められます。また、システム的対策では、パスワードの設定や暗号化技術の活用で、情報セキュリティ対策の強化を図ることができます。しかし、これらの対策は、情報システムの高度化や情報技術の発展にともなって、情報セキュリティ強度は変化し低下をします。また、情報セキュリティの機能の基本は「難さ：にくさ」（実行することが面倒で難しいこと）であります。部屋に毎日鍵をかけることは面倒でありますが、この面倒くささ（難さ）がセキュリティ機能であります。しかし、人間は、時間の経過や慣れによってこの「難さ」を無視したり否定したりするようになります。ドアの鍵をかけずに開けっ放しにする等典型的な事例です。このことが事故や事件の脅威を誘引する脆弱性を生み出し、潜在化するのです。そして、情報セキュリティのコントロール（統制）が利かなくなった時に、大きな事故や事件が発生し被害がでるのです。

レベル３の組織・管理的対策やレベル４の法・倫理的対策は組織マネジメントや指導・教育に存するところが大きいです。そして、最終的には企業や組織体のなかに、「情報セキュリティ文化の醸成」が必須となります。そのためには、日ごろからの指導や継続的な教育が重要になってきます。情報セキュリティ対策は、一つのことを実施しておけばよいというわけではありません。レベル１の物理的対策からはじまり上位のシステム対策は組織・管理的対策、法・倫理的対策まで、組織の脆弱性を分析して、それに見合った対策を実施することで、必要で実効性の高い情報セキュリティ対策が実現できるのです。

２．担当部署の責任とは：評価書の内容の精査、用語の統一

評価書はそれぞれの事項の担当部署が責任をもって対策案を策定し、記載されたことと考えられます。しかし、多くの評価書では、重要な単語や用語に統一性がなく、それぞれの部署が独自に用語を略したり、慣用語を使ったりしているところが多々見受けられます。重要なことは、担当部署が責任をもって評価書を統合し、統一性を図り内容を精査することです。それには、評価を担当する部署の所属長は、評価書をまとめるだけでなく、用語の統一や略語の使用方法、慣用語の注釈等、あらかじめ統一しておくか、全体の取り纏めるにあたって、統一化を図ることが必要です。担当部署は、特定個人情報保護評価の対象となる事務を担当し、リスクを軽減させるための措置の実施に責任を負うことになります。

例えば、同一の評価書の中に、統一性がなく、さまざまな用語や略語が使われています。以下その事例であります。

・住民基本台帳ネットワークシステム⇒住基ネット、住基ネットワーク、住基システム・・・

・入退出ＩＣカード⇒入退出カード、入退カード、カード、ＩＣカード、キーカード・・・
・標準システムサーバー⇒標準システムのサーバー、サーバーシステム、インフラ・サーバー、システムサーバー
それぞれが、同じ意味の用語と想定されますが、それぞれの事項説明箇所でつかわれています。

さらに、用語はできるだけ、分かりやすく記載することが重要です。なお、専門用語や法律を簡略化したり俗語を用いたりするときには、通常、正式用語を一旦定義し、「以下（以後）〇〇と言う。」ように記載し、以後はその略語等を使用します。

一方、説明内容の深さについても統一されていない場合が多いようです。リスク対策の内容では、「パスワードの設定をして対策を実施しています。」と保護の方法説明をしているだけの内容のものがあれば、パスワードの設定の具体的な設定管理から付与・変更管理まで詳細に記載されているものもあります。その結果、同じ評価書のなかで、統一的な記載内容のレベルまで指示されず、最終的な精査がなされていないままに、作成されていると思われます。これは、担当部署、責任者の評価書作成に対する姿勢の問題です。

３．多様な個人情報の漏洩の原因に対する対策の不足

近年、日本年金機構１２５万件超の漏洩事件、ベネッセの７６０万件の漏洩事件等、有名企業や組織の個人情報漏洩事件が話題になっています。個人情報の漏洩は、しばらく発生していないように思われがちですが、決してそうではありません。公表されています漏洩の事故や事件は少なからず、毎日発生しています。漏洩件数が少なく、話題性がないと判断されて報道で取りあげられていないだけです。そして、大きな事件が発生したときに話題になり、社会的に注意喚起されがちです。

個人情報漏洩がニュースや報道に取り上げられるのは、話題性のある新しい形態の事件であったり、個人情報の漏洩が大量でまた有名企業や組織であったりしたときであります。これまで話題にもならなかった個人情報の漏洩事件、事故を分析すると、その主な要因は、①従業者（派遣社員を含む）の外部持ち出し、②不正アクセス、③パソコンや記録媒体の紛失・盗難、④ウイルスの感染、⑤関係者の不正行為が主であり、その要因をもたらす（誘引する）根本的な脆弱性は、①内部の者への情報セキュリティに対する教育・啓発が徹底されていない、②内部から不正複製による情報の持ち出し、③パソコンやＵＳＢ等の電磁的記録の紛失・置き忘れ、④安易なメールで情報を送信及び誤送信、⑤情報を複製して自宅で業務を行い結果を企業体等に持ち込む、⑥不十分なウイルス対策及びその設定ミス、⑦ネットワークからの侵入（標的型攻撃と標的型攻撃メール）等、徹底されていない情報セキュリティ対策や故意の情報漏洩によるものです。

しかし、評価書のリスク対策の多くは、①パスワードの設定によるアクセス制限、②アクセスログの監視と保管、③通信の暗号化等の記載

が主であります。また、その対策を実施するために、①セキュリティポリシーの制定、②従業者（派遣社員を含む）への教育・指導の徹底が主に記載されてりおり、その上でリスク対策に対する認識は、「十分である」という回答が多々見受けらます。これは、雛形に記載されている標準的な情報セキュリティ対策を記載することで、まずは安全であるという甘い認識によるからです。

情報通信技術が進化し情報システムの高度化が進めば進むほど、その効用に反作用して脆弱性は増大化し、変化します。リスク対応の情報セキュリティ対策は、画一的に実施されるものではなく、情報ネットワークシステムの目的、ネットワークシステムの機能や内容、処理方法等により組織固有の脆弱性の増大化と変化がおこってきます。そこで、脆弱性を抑える（コントロールする）さまざまな情報セキュリティ対策を組み合わせて、変化に対応させていく必要があります。

４．「具体的な内容を記載すること」と指示されているが記載内容に具体性がない：セキュリティ対策の強度の評価が不能

多くの項目には、「具体的な内容を記載すること」となっています。具体的とは、「何時（年月日）」「誰が（主体）」「誰に（対象）」「何を（内容）」「どこで（場所）」「どのようにして（方法）」が示されていることが原則です。例えば、情報セキュリティ教育の実施では、「現場に対して情報セキュリティ教育を定期的に実施していきます。」と言った記載をよく見かけます。この記載では全く具体的な内容が記載されていません。何時（年月日）から、誰が、どのような内容の教育を、誰を対象に、教育を実施していこうとするのかよくわかりません。リスク対策のおいても、「パスワード設定して使用者を制限していきます。」と言った記載があります。不正なアクセスにはパスワードの設定が、最適な方法であり、十分な対策と考える人が多いのです。パスワードの設定はセキュリティ対策に重要な対策であることは否めませんが、パスワードだけで不正なアクセスへの対策には不十分であります。

さらに、具体的な記載にも欠如しているために、よく理解できない表現がよくつかわれています。例えば、「特定個人情報ファイルのアクセスできる作業者を最小限にします。」とか、「アクセス管理を行い、不適切な端末操作ができないように抑止する仕組みにします。」といった記載があります。どのようにして作業者を制限するのか、また、どのような方法でアクセス管理をするのか、具体的な記載がなされていない典型的な事例です。このような内容が記載されたならば、評価はできないことになります。

前述のような情報セキュリティ対策の具体的な内容を記載してはじめて、セキュリティ対策に対する強度が評価でき、脆弱性の指摘ができるのです

５．監査の独立・客観性の認識が不足

特定個人情報保護の監査には、個人情報保護監査、システム監査、情報セキュリティ監査等があり、いずれの監査であっても個人情報保護の監査目的は達成できます。しかし、監査をうける組織の長が、監査を実施する責任者となっている自治体があります。これでは、監査の独立・客観性はたもたれず、監査の目的は達成できません。典型的な事例は、情報システム責任者がシステム監査の責任者として兼務しているケースであります。監査は、個人情報を取扱う情報システムをはじめ、その環境・活用・運用等の全体を対象に、安全性・信頼性・効率的の視点で、独立・客観的立場で実施し、首長やＣＩＯ（情報担当責任者）に報告し、場合によっては改善勧告をします。この監査には、助言・勧告をうけることを目標とする「助言・勧告型監査」と、近年、多くなってきました「保証型監査」がありますが、個人情報保護の監査では、自治体の個人情報保護の監査ガイドラインにもとづく「保証型監査」の実施が望まれます。また、監査人は、内部監査人のみならず、外部監査人による実施が有効であります。

評価書では、まず、特定個人情報の取り扱いの適正性について、自己点検の実施が求められていますが、自己点検のツールとなる「自己点検チェックシート」を用いて、具体的なチェックの方法について記載されていません。また、監査についていても、①内部監査か外部監監査、②監査目標、③監査の体制、④監査の頻度等、基本計画レベルの内容すら記載されていないことが多いようです。

６．情報セキュリティ委員会の設置と情報セキュリティ文化の醸成

以上、基本的な評価書の問題点を総括し、情報セキュリティ対策について述べましたが、提示された評価書では、特定個人情報を保護するために総合的な対策強化の方向性が見受けられません。通常実施されているウイルス対策やファイアーウォールといった技術的な対策は、実施されていますが、情報セキュリティは組織全体が真剣に取り組むべきことで、担当部署のみが実施すべきことではありません。また、技術的な対策を実施していれば安心であるといった誤解も多い状況です。特に、組織・管理的対策や法・倫理的対策の継続的強化が求められます。それには、計画的な教育が最も重要ですが、組織全体の情報セキュリティに対する認識の向上が重要です。それには、トップマネジメントをはじめとする情報セキュリティに対する意識改革が必要であります。具体的には「情報セキュリティ委員会」の設置です。情報セキュリティ委員会の設定は、リスクや情報セキュリティに関する情報の共有や課題の討議を行い、日常からの情報セキュリティ指導や啓蒙の実践がおこ

なえます。

そこで、組織全体に実効性の高い情報セキュリティの実践するためには、情報セキュリティ委員長にトップマネジメントが就任し、各現場の実務責任者や担当者から委員を選任し、組織全体の重要委員会に位置づけます。委員会では、①現場で発生する問題への対策討議、②法や規程の改訂情報の共有、③現場への情報セキュリティ対策普及等、トップマネジメントが先頭にたって委員会を推進し、情報セキュリティ意識の改革と文化の醸成をはかることが重要と言えます。

評価書で「情報セキュリティ委員会」の設置について言及している自治体はほとんどありません。従業者に対する教育・啓発に匹敵する重要な対策であります。ましてや日頃の従業者への教育・啓発につながることでもあります。その他のリスク対策に、是非「情報セキュリティ委員会の設置」を盛り込み、情報セキュリティ対策での組織・管理的対策の強化をはかることが必要です。