[® 研究論文]

改正個人情報保護法を意識した要件定義工程の進め方と組織点検及びシステム監査に関する研究－企業２社での実務への適用を通じて－

A Study on the Organizational Inspection and Information Systems Audit of Requirement Definition Process that Considers Revised Personal Information Protection Law
- Survey with the Two Private Enterprises

栗山　孝祐　Takahiro Kuriyama
原　善一郎　Zenichiro Hara

概　要

2015 年 9 月に改正個人情報保護法が成立・公布され、2017 年 5 月に全面施行された。個人情報の保有件数の条件が撤廃され、全企業が改正個人情報保護法の適用対象になる。しかし、2017 年 3 月時点では改正個人情報保護法への対応が進んでいない状況であった。そこで、システム開発の上流工程の中心である要件定義工程で実施すべきプロセスを研究することにした。本論文では、個人情報保護要件検討シートを作り、改正法への対応漏れを防いだ。実践での使用として、企業２社の実際の要件定義工程の組織点検に着目し、既存のプロセスに組込みを行った。さらに、組織点検が適切に行われていることを確認するシステム監査で実施すべき 10 個のプロセスおよび主な監査項目一覧を具体的に整理した。これから改正個人情報保護法をシステム開発段階で適用される企業の参考になろう。

キーワード：個人情報保護法、要件定義工程、システム監査

1　はじめに

1.1　テーマ選定の背景

改正個人情報保護法は全企業が対象であるが、対応準備が遅れている企業が少なくない。

2015 年 9 月に改正個人情報保護法が成立・公布され、2017 年 5 月 30 日に全面施行された。個人情報の保有件数の下限条件が撤廃され、5、000 件以下を保有する場合についてもこの法律が適用されることになり、全企業へ適用が拡大されるとことになった [1)]。2017 年 3 月 10 日の一般財団法人日本情報経済社会推進協会（以下、JIPDEC という）から公表された News Release（以下、News Release という）では、改正個人情報保護法対応について、2017 年春頃までに体制構築対応を予定している企業は 6 割、対応済は 1 割未満であった [2)]。

1.2　企業における課題

企業では、改正個人情報保護法の対応として、自社の規程やルールの見直しの対応をする。そして、規程やルールに従い、業務の見直しを行う。それに合わせ、関連システムの対応も取る。システムの対応をする場合、要件定義工程の役割は重要であるが、システム開発時に個人情報保護法の対応が重点管理されていないことが、改正個人情報保護法対応遅れの原因の一つとなっているケースがある。

この News Release の参加者アンケート結果で法対応の遅れの問題が提示されている。法適用の有無にかかわらず、企業が抱える情報管理実施上の問題点の上位 3 件は、次のとおりである。

・担当できる人材がいない (30.7%)
・管理ルールはあるが社内で徹底されていない (30.7%)
・規程類のルールが定まっていない (26.1%)

上記の問題点がある中、企業のシステム開発時は、改正個人情報保護法の対応以外に数多くのカテゴリー (例：品質、費用、納期、情報セキュリティ)

投稿受理日	2017 年 3 月 30 日
再投稿受理日	2017 年 8 月 21 日
査読完了日	2017 年 9 月 26 日

の対応が必要となる。個人情報を取扱うシステムの開発でも同様となる。実際のシステム開発時は、Quality: 品質、Cost: コスト、Delivery: 納期 (以下、QCD という）の３つの視点が要件定義工程で重要視される。個人情報保護のみの視点で、組織内による点検及び社内の専門部門 (品質管理やシステム管理) による点検 (以下、両方合わせて組織点検と記述) や専用の要件定義プロセス追加を実施することは現実的ではない。なぜならば、個人情報保護の視点の点検を独立させると、これにより、専用規定やルールの作成、人材確保とコスト増になるからである。

肝要なのは、既存の規程やルールの見直しにとどめ、既存の人材を活用し、コストを抑えながら法対応することである。また、システム開発時に、プライバシー・バイ・デザイン (PbD) の基本原則を組み込むタイミングは、要件定義工程である[3]。つまり、「システムを個人情報保護対応済みとすること」は、そのシステム開発の要件定義工程で実施すべきであり、システム開発後に要件実現を組み込むことよりも、コストが低減できる。

1.3　本論文での研究概要

各企業は、従来から要件定義工程のプロセスがあり、組織点検を多様なカテゴリーに関して実施してきた。また、そのことによる内部統制の整備と運用状況を確認する作業をシステム監査として実施してきた。

本論文は、各企業が既に持っている既存のプロセスに、改正個人情報保護法対応に必要な要件定義、組織点検、システム監査を組込むことを提言するものである。

また、改正個人情報保護法対応に必要な要件定義では、3.3.1 で述べる「個人情報保護要件検討シート」を活用して、システムで実現する要件の抽出と要件定義を提言する。

次の章では、従来の個人情報保護法の下での２つの企業の状況を示す。

2　従来の要件定義工程 (進め方、組織点検、システム監査)

SI ベンダー[注1)]A 社及び、製造業 B 社での事例を調査し、これらを比較した。

2.1　SI ベンダー A 社の事例

当事例は、A 社が顧客と契約する作業の事例である。

A 社は顧客のシステム開発を行う標準的な手順の中で、手順の項目について顧客と共同で数多くの点検を行っている。この内容は、QCD が重要視される。特に従来は、開発するシステムで取扱う個人情報の件数が少ないため法適用外であるケースが多く、「個人情報保護法対応は重要な点検ポイントであるという認識」が低いケースが多かった。

2.1.1　開発の手順と点検項目

開発の手順は、国際標準に準じて作成され、これに沿って以下に述べるような点検をしている。独立行政法人情報処理推進機構の「共通フレーム 2013」に於いては、システム開発での要件定義は顧客責任としている[4]が、A 社における実態は、要件定義を顧客と共同作業として進めていることが多い。

A 社は、要件定義工程を、「商談」工程から「要件定義終了」工程までの５つとしている。個人情報の取扱いの確認に着目すると、次の通りとなる。

(1)「商談」工程

・SI ベンダーとして、顧客システムの構築に向けた商談対応の工程で、組織としての商談審査、顧客への見積提示がある。その中で図表－１の①商談審査で、個人情報の取扱いをするシステム商談かどうかの確認をする。

(2)「受注」工程

・顧客と開発システムの契約に関することを進める工程であり、図表－１の②契約前確認にて、個人情報取扱いシステムであるかの確認、及び、個人情報取扱いシステムの場合、A 社は顧客の持つ個人情報を取扱わないように指導する。

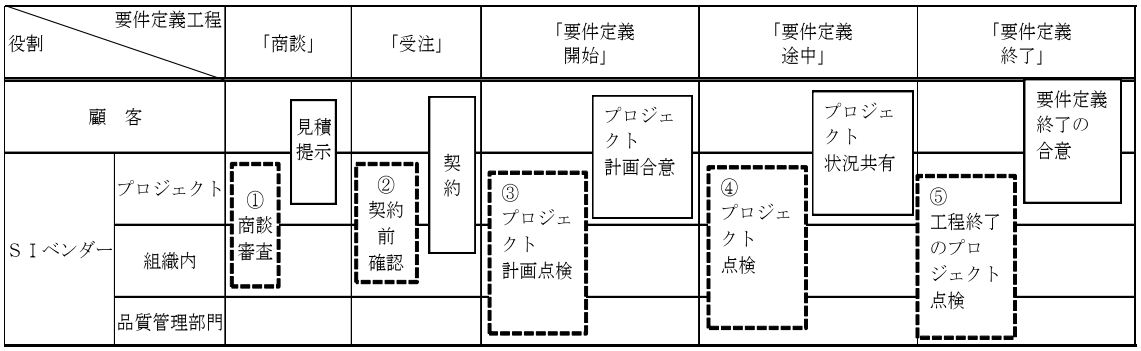
(3)「要件定義開始～途中～終了」の３工程

・要件定義を進める工程であり、開発システムの全体がわかる「システム概要図」も含めた要件定義書の作成を行う。その中で組織として３つの点検を実施している。図表－１の③にて要件定義工程のプロジェクト計画点検を行い、個人情報を取扱うかどうか

を再確認する。そして、システム機能として取扱う場合、要件定義の途中では図表－１の④途中工程のプロジェクト点検、要件定義終了時には図表－１の⑤工程終了のプロジェクト点検で、システム機能での対応範囲の確認を行っている。

Ａ社のシステム開発の場合、5、000 人以上の個人情報を取扱うシステムは、社員情報を管理する人事・給与システムや消費者情報を取扱うシステムであり、これら以外のシステムは法適用外プロジェクトであった。したがって、「個人情報保護対応」は従来も点検項目としてはあったが、余り意識されていなかった。

図表－１　Ａ社での要件定義工程と役割



2.1.2　点検項目の評価の重点

組織点検の中心は、QCD と要員やそのスキル等の人的資源である。

(1)「要件定義開始」時のプロジェクト計画点検 (図表－１の③)

プロジェクト開始時の点検である図表－１の③プロジェクト計画点検では、プロジェクト計画書が出来ていて内容的に問題ないか (一定規模以上のプロジェクトでは、品質管理部門が③の一部として点検する)、作業項目、作業ボリューム、スケジュールの各妥当性、顧客、社内の各体制・要員スキル、品質管理・評価方法の確認、要件定義支援作業のコスト見積の妥当性等が点検され、リスク共有と対策検討が行われる。

(2)「要件定義工程途中」のプロジェクト点検（図表－１の④）

QCD を重視し、プロジェクトを点検している。(1) と同様に、一定の規模以上のプロジェクトにおいては、Q（Quality: 品質）の客観的な品質評価として、品質管理部門が要件定義ドキュメントの検査を図表－１の④途中工程のプロジェクト点検の一部として行う。

(3)「要件定義工程終了」のプロジェクト点検（図表－１の⑤）

要件定義工程を終了して良いか点検する。この点検で指摘されたことは、プロジェクト内で検討し、必要に応じ顧客とともに協議し、要件定義で対応をとる。「共通フレーム 2013 の概説」も要件定義の重要性を記載している [5]。Ａ社も要件定義の充実度 (システム化業務要件の明確度、システム設計着手の社内基準への適合度) に重点を置いて点検をしている。

2.1.3　システム監査

システム監査は、システム開発を中心にプロジェクトと組織に対し、社内の監査部門が内部監査として、半年ごとに上記 2.1.2 の (1) ～ (3) の実施確認、エビデンス確認を実施している。

2.1.4　個人情報保護対応に対する認識

従来、個人情報を取扱うシステムおよびプロジェクトは、全体システムの一部であり、多くのプロジェクトが非該当であったため、個人情報保護法対応の必要性の認識が薄かった。また、プロジェクトに対し QCD を中心とする多様なカテゴリーで点検しているため、点検時点での項目数は必要最小限に抑えてあった。そして、重要事項は、事前にプロジェクト内の自己チェックや、品質管理部門等の評価を受けていることで、確実な点検となるようにしている。

2.2　製造業Ｂ社での事例

製造業Ｂ社の利用部門が改善のためのシステム検討を行い、SI ベンダーＣ社に提案依頼を行い、発注する事例である。

2.2.1　開発の手順と点検項目

Ｂ社のシステム開発上流工程は「システム化構想」工程から「要件定義・発注」工程までの４つに分けられる (図表－２参照)。

この４つを今回の研究対象で呼ぶ要件定義工程と位置付ける。

(1)「システム化構想」工程

・システムの利用部門が、システム化構想案を「システム化検討書」（業務の現状と問題点、改善後の業務の状態、改善方法のアイディア、業務改善による改善金額、改善活動の時期を記載）という文書で、作成する。

・これを、システム管理部門が図表－２中の「①システム化審査」で、システム化の方向性、計画、システム化検討書の実現可否について審査する。この時、情報担当役員も参加する。

(2)「要件検討」工程

・利用部門が提案依頼書を作成する。但し、利用部門だけで作成できない場合は、社内で関係者会議を立ち上げて作成する。さらに必要に応じ、C社も作成に参画することもある。

・システム管理部門は、図表－２中の「②提案依頼書評価」として、提案依頼書の内容について評価する。

この評価の特徴は、検討するシステムとこれに伴う業務改善が実現した場合、一部門の個別改善事項にとどまるのか、会社全体の新たな仕組みとなり全社の標準と位置付けられ全社の改善につながるものか、これに加えて全社の業務標準自体の継続的な改善を促す仕組みが組込まれた形になるのか、というレベルを評価していることである。これは、後述の金額で評価する投資対効果による評価の仕組みにも反映されている。

・C社に提案依頼書を送付することで、提案依頼と見積依頼を行う。

(3)「提案検討・見積」工程

・C社が提案書と見積を作成し、利用部門へ送付する。

・これらの妥当性確認として、利用部門とシステム管理部門は「③提案・見積内容確認」を実施する。関係者会議を開催する場合もある。

(4)「要件定義・発注」の工程

・利用部門、関係者会議でシステム実現に向けた要件定義書を作成する。この一部として「システム概要図」、「システムリスク確認シート」がある。「システムリスク確認シート」は、個人情報保護要件と関連する５項目 (DB（Data Base)、アクセス管理、入力ミス、影響度確認、遵法性) の確認が用意され実施されている。C社に直接確認がされることもある。

・システム管理部門による図表－２中の「④発注書 (要件定義書) 検査」を行う。その過程で、「システムリスク確認シート」の点検も実施されている。

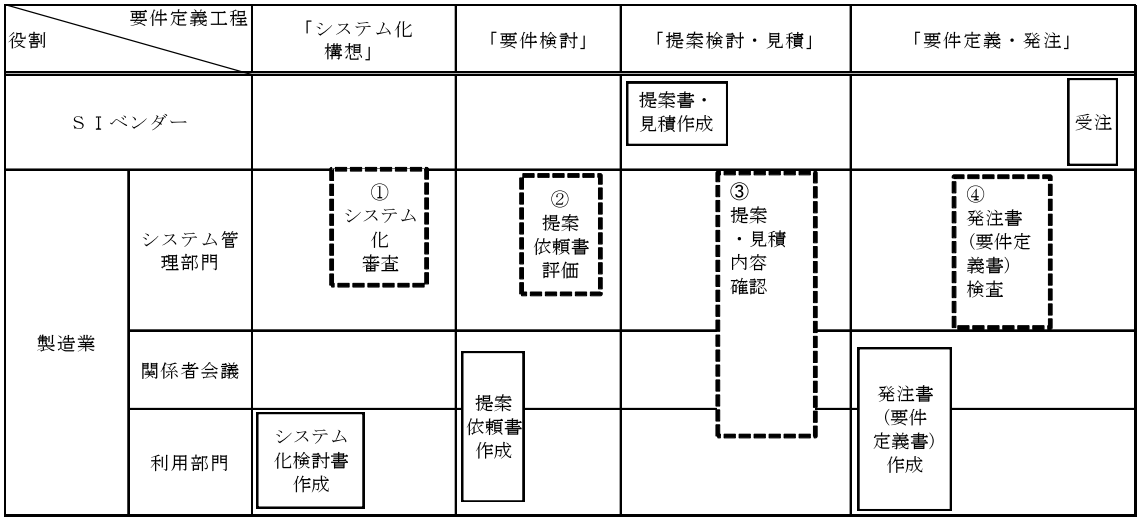
・利用部門が発注を行い、C社が受注する。

2.2.2　点検項目の評価の重点

B社は「システム開発費」、及び、その効果を評価する一定期間の「システム保守費と運用経費」の合計を、「システム投資額」としている。

B社の計画するシステム開発・導入の評価は、投資と効果のバランスが重要視されている。個人情報保護要件が「システム投資額」の増加となった場合は、「定性効果額」に含めて評価されている。評価は、①システム化審査、②提案依頼書評価、③提案・見積内容確認、④発注書（要件定義書）検査に分類される。これらの評価の特徴は、投資

図表－２　B社での要件定義工程と役割



対効果を金額で評価することである。企業であるため、システム投資により最終的には何らかの効果に結び付けなくてはならないからである。

B 社は製造業であるため、あらゆる側面で、金額による評価と原価削減がその評価の中心である。たとえ、売上増に結びつく投資であっても、売上増により原価増になるからである。このシステム投資により増加する原価は、金額で評価される効果により一定期間内に相殺され、さらに、企業としては金額的効果と金額では表現できない定性効果の実現が期待される。効果評価は、３つに分類され、「定量効果額１」（現在の実際に支払っている費用の改善金額）、「定量効果額２」（5 年間の費用増加を想定した場合の改善金額）、「定性効果額」（金額に換算できない効果額を、投資額と同等以下で査定した金額）の合計値が、投資額以下となってはいけないとされている。すなわち、次の式が成立することがシステム開発着手の必要条件となる。

「定量効果額１」＋「定量効果額２」＋
「定性効果額」≧「システム投資額」

さらに、年間に開発するシステムの全体の投資対効果も評価される。年間に開発するシステムの効果額の総合計は、「定量効果額１」と「定量効果額２」それぞれの年間合計を合算した「定量効果額」と「システム投資額」の年間合計を比較している。年間では「定性効果額」を含まないこととし、「定量効果額１」と「定量効果額２」の合計額だけで「システム投資額」を上回っていることを確認する。

「定量効果額１」の年間合計＋「定量効果額２」の年間合計≧「システム投資額」の年間合計

なぜならば、「あるシステムは、他のシステム群の前提システムとなる」という効果も定性効果として評価されるため、重複するからである。この効果評価の仕組みにより、「コンプライアンス対応」などの定性効果のみのシステムも、金額による効果評価の仕組みの中で「必要と判断」が可能となる。

2.2.3　システム監査

システム監査は、利用部門に対し、社内のシステム監査担当部門が内部監査として、半年ごとに上記2.2.2の(1)-(4)の実施確認、エビデンス確認、他の監査項目も含め実施している。

2.3　共通事項と特徴がある事項

ここまで、２つの企業での研究対象である要件定義工程、組織点検、システム監査の現状を見てきた。

2.3.1　共通事項

両方に共通することについて下記にまとめた。

①個人情報保護法対応の必要性の認識が低くかった。
従来は、法適用は個人情報が 5、000 件以上に限定されるとの認識があり、ほとんどのシステムが対象外とされた。

②要件定義書の一部として、開発システムの全体がわかる「システム概要図」を作成していた。

③組織点検は、効率の観点で必要最小限にしている。
組織点検は多種多様なことを要求されるため、実務的には必要事項の一覧性が重要であり、網羅的で各カテゴリー (例 : 品質、費用、納期) は最小限の項目で評価・確認された。

④システム監査の位置付け
システム監査は、内部監査の位置付けで他の監査項目に含めて行っていた。

2.3.2　A 社と B 社に共通しない、各社に特徴がある事項

それぞれに特徴がある事項は次の通りである。

・組織点検は、A 社では顧客との契約履行を重視して、要件定義の品質である充実度 (システム化業務要件の明確度、システム設計着手の社内基準への適合度) に重点が置かれている。B 社では自社のシステムに対するコストの観点を重視して、要件定義工程全般を通じ、システムの投資対効果に重点が置かれている。

3　改正個人情報保護法の対策①（要件定義工程の進め方）

調査を行った企業２社の共通事項と特徴を前提に、研究を行う。

3.1　当研究の特徴

栗山 (2017)[6] は、流通小売業をターゲットに改正個人情報保護法対応を意識したシステム開発における要件定義工程の進め方と要件抽出を模擬適用する研究を行った。業種枠を外し、SI ベンダー

A社と製造業B社へ要件定義工程の進め方、要件抽出(図表－4個人情報保護要件検討シートの活用)、組織点検、システム監査の4つを実際に適用する活動をおこなった研究である。具体的には、図表－3個人情報取り扱いシステム要件定義工程プロセス概要を2つの企業の既存工程(図表－1、図表－2)に組み込んだ。本章では、要件定義工程の進め方、要件抽出(図表－4個人情報保護要件検討シートの活用)を中心に説明する。

3.2　要件定義工程へのプロセス適用

個人情報を取扱うシステムの開発における要件定義工程で組込みを提唱するプロセスは、図表－3に示すように「業務要件の検討」と「個人情報保護要件の策定」の2つのフェーズになり、「業務要件の検討」では、システム化要件全体を検討し、「個人情報保護要件の策定」は、個別の要件定義を示す。

3.2.1　要件定義工程プロセスの詳細

(1)業務要件の検討

業務要件の検討は、下記の4つのステップで行う。従来の要件定義工程で作成する「システム概要図」に「個人情報」に関する情報を記載することになる。

ステップ1：目的および業務の洗い出し

情報システムの「名称」および情報システム導入の「目的」を定める。続いて、目的に合う具体的な「業務」を整理し、業務に関わる人物や情報も整理する。

ステップ2：業務の特徴の整理

改正個人情報保護法、個別法、個人情報保護委員会からの指針、認定個人情報保護団体の情報から遵守事項を確認して対応方針を明確にする[7]。

ステップ3：システム概要図の作成

システム概要図は、他の要件と合わせて作成するため、ここでは「個人情報」に関する情報を記載する。(例：個人情報DB、個人情報の流れ、利用者を表現)

ステップ4：定型設問による業務要件の詳細化

個人情報保護要件の導入に必要なレベルにまで業務要件を詳細化する。「主体」「情報」「利用環境・手段」の3つの視点と、個人情報影響評価(Personal information Impact Assessment)、(以下、PIAという)[注2]の予備評価等で用いられる項目にて業務要件の詳細化を行う。これが「PIAの予備評価情報」となる。PIAの予備評価項目は、個人情報を新規か機能追加として扱うことになったのか、情報に機微情報を含むか、アウトソーシングか、情報取得にあたり利用目的の開示や本人との合意を適切に取って取得しているか等の項目確認である[8]。

(2)個人情報保護要件の策定

個人情報保護要件の策定に関しては、下記の4つのステップで行う。ステップ7を除き、従来の要件策定でも実施されることである。ステップ7は、組織点検の一部として行う詳細の個別確認を改正個人情報保護法対応用にしたものである。

ステップ5：システム対応方針の決定とシステム対応範囲の検討

システムで対応すべき範囲である対応方針を決め、その後、PIAの評価項目単位にシステム対応可否を決める。ステップ2で行った法関連対応の確認も行う。

ステップ6：対策要件の決定

ステップ5の結果に従い、「個人情報保護要件検討シート」にて、システムで対応するとした項目単位に、システム機能概要要件を決定する。

図表－3　個人情報取扱いシステム要件定義工程プロセス概要

業務要件の検討フェーズ

ステップ1	ステップ2	ステップ3	ステップ4
目的及び業務の洗い出し	業務の特徴の整理 (関連法、指針、方針、ガイドライン等の遵守事項の対応整理も含む)	システム概要図の作成	定型設問による業務要件の詳細化

個人情報保護要件の策定フェーズ

ステップ5	ステップ6	ステップ7	ステップ8
システム対応方針の決定と対応範囲の検討 (ステップ2の法関連対応の確認含む)	対策要件の決定	個人情報影響評価(PIA)の実施とその評価の反映	要件定義書への反映

ステップ７：PIA の実施とその評価の反映
改正個人情報保護法の普及段階では、有識者による評価を行い、指摘事項を機能要件の見直しに活用する。具体的な評価対象としては、業務要件の検討で作成した「システム概要図」、ステップ４で実施した「PIA の予備評価情報」、および、ステップ６で作成した「個人情報保護要件シート」である。
ステップ８：要件定義書への反映
ステップ７で決定したことを要件定義書に反映させる。

3.3　要件抽出に個人情報保護要件検討シートを活用

栗山 (2017)[6] 掲載の個人情報保護要件検討シートを他業種で適用できるように拡張している。

3.3.1 「個人情報保護要件検討シート」のＡ社、Ｂ社への適用

本論文では、栗山 (2017)[6] 掲載の個人情報保護要件検討シートに凡例を追記した。

図表－４では、評価の大項目を提示し、a) で評価項目単位にシステム化要件にて対応/非対応(システム以外で対応) を、b) でシステムにて実現する場合の検討すべき補足説明等を、c) でシステム機能要件例を記載した。例えば、大項目①目的明確化は、目的を明確化すること自体はシステムでは実現できないため、a) は非対応とした。b) は①の目的外利用の防止をシステムで実現する場合、検討が必要であること、及び、機微情報について、システムで区別して管理する場合、検討が必要であることを記載した。A 社及び B 社は、当シートを活用し、改正個人情報保護法に関する要件を数プロジェクトにて抽出した。その結果、活用したシステムでは、改正個人情報保護法の要求事項のシステム要件漏れを防ぐことができている。

4　改正個人情報保護法の対策②（要件定義工程での組織点検とシステム監査）

改正個人情報保護法がシステム開発の要件定義工程から意識されていることを、組織点検で確認することと、組織点検の妥当性を確認するシステム監査で確認することが望まれる。４章では、２企業の組織点検の組込みと、今後予定されるシステム監査について説明する。

4.1　要件定義工程での組織点検

2.3 の共通事項にあるように、それぞれの企業において既に確立された組織点検プロセスがあり、効率的に実施されている。そのため、各企業が既に持っている点検に改正個人情報保護法の視点を組込む。具体的には、図表－１の①②③④⑤、図表－２の①②③④の活動に組込んだ。

改正個人情報保護法対応として、組織点検の段階では、法適用が必要なシステムであるかの確認や、該当する場合、有識者や専門部門の事前確認が実施済であるかの確認が重要である。

そのため、組織点検の前に、有識者や専門部門で、改正個人情報保護法について熟知し、かつ、自社での影響を把握できる要員の判定や確認が必須である。対応者の候補としては、社内のシステム監査スキル保有者やプライバシーマーク制度推進者、同制度の審査員の知識を有する者などの活用が有効である。さらに、特定個人情報 (マイナンバー) 対応経験者の活用も有効であると考える。点検時の組込みカテゴリーとしては、現実的には品質管理の項目として組込むのが良く、事例の２つの企業も品質のカテゴリーとして組込んだ。ISO（国際標準機構 International Organization for Standardization の略。ここでは、国際標準機構が出版した国際規格を示す）では QMS（品質管理システムの国際規格 Quality Management System ISO9001）と ISMS（情報セキュリティマネジメントシステムの国際規格 Information Security Management System）で一部共通化の動きはあるが[10]、実際の現場では両方合わせて対応・点検する意識が強い。そのため、情報セキュリティ対策も品質のカテゴリーに加えて考えた方が良く、今回の個人情報保護対応も含めるのが良いと判断する。

発生するコストについては、要件定義工程で定義して設計時に対策をする場合と比較して、開発時の対策は 6.5 倍、運用時に至っては 100 倍と評価している調査結果がある[8]。

そのため、このような情報をシステム開発にかかわる者に浸透させ、組織点検は、要件定義工程ですることが大切である。

4.2　個人情報保護要件検討シートの活用に対する組織点検

図表－４の「個人情報保護要件検討シート」の

図表－４　個人情報保護要件検討シート

大項目	評価項目	システム化要件での対応判断と検討すべきシステム機能要件例
	凡例	a)は、システム化機能要件で対応/非対応(システム以外で対応)の区分を記載。 b)は、システム化機能要件時の補足説明等 c)は、該当時のシステム機能要件例
①目的明確化	利用目的/個人情報の特定 機微情報	a)非対応(システム以外で対応) b)左記目的外の利用を防止する等をシステムで実現する場合、検討要。 b)機微情報の取扱いについて、システムで区別して管理する場合、検討が必要。
②利用制限	目的外利用・変更 第三者提供、共同利用	a)非対応(システム以外で対応) b)但し、利用目的変更/第三者提供/共同利用時等でシステムを利用して お客様に同意を取る場合等は、機能の検討が必要。
③収集	本人の同意	a)非対応(システム以外で対応) b)システムで対応する場合、画面等での同意機能の検討が必要。
④データ内容	データの正確性	a)対応 b)随時、定期等、個人情報をメンテナンスできる機能の検討が必要。 c)例1 お客様から連絡を受けてメンテナンスできる機能。 例2 インターネットシステムでは、お客様が変更できる機能。
⑤安全保護	1)プライバシー保護機能	a)対応 c)システム管理者以外の第三者が見れないようにする機能。 c)利用者が利用履歴等を確認できる機能。
	2)脆弱性対策	a)対応　　b)悪意に対する対策 c)利用システムに対し、セキュリティパッチ等を定期的に行う機能。 c)インターネット接続されている場合のファィアウォール機能
	3)データの消去	a)対応 c)データの完全消去機能とその確認機能。
	4)識別認証	a)対応 c)ID、パスワード管理(期限管理機能、安易なパスワード防止機能　等)機能。
	5)通信の保護	a)対応 c)データ転送する際の盗聴/改ざん防止機能。
	6)アクセス制御	a)対応 c)アクセス権限、機能区分、一定時間退席時の対応等 c)外部からのサーバ監視は、できる限りサーバへログインしない方法を検討する。注3)　9)
	7)監査	a)非対応(システム以外で対応)　b)但し、下記の様な対応の検討必要 c)監査できるように各種ログを取得する機能
	8)安全管理措置	a)対応 c)バックアップ/リカバリ機能、システム運用作業者ログ取得機能 又、当件は、サーバ設置場所確認が必要(サーバは国内法が及ぶ範囲か)
	9)ミス防止	a)対応 c)印刷時の関係者外秘印刷、外部媒体出力時、注意画面表示等
⑥公開	個人情報保護方針	a)非対応(システム以外で対応)　b)直接のシステム化機能要件ではないが、下記の様な検討が必要。 c)システム対応の場合、会社ポータル上、インターネットサービス上、 お客様利用画面等での掲載。
⑦個人参加	情報開示、訂正、利用停止 第三者提供の停止	a)対応 c)お客様からの左記依頼に対し、情報検索、開示、訂正、停止、削除、 第三者提供停止をできる機能。

活用方法とプロセスについて下記に示す。概要は、有識者や専門部門のチェックを受け、組織点検で実施の有無を確認する。

①抽出した要件一覧を社内の改正個人情報保護法の有識者や専門部門がチェックする。
改正個人情報保護法について熟知し、自社での影響を把握できる要員が実施する。

②上記の①を実施したことを、確認項目の一覧に含め、組織点検する。
具体的には、図表―１の「A社での要件定義工程と役割」では⑤終了工程のプロジェクト点検、図表―２の「B社での要件定義工程と役割」では「④発注書（要件定義書）検査」で実施する。
要件定義工程での「組織点検」についてまとめると、要件定義工程での組織点検概要図となる（図表－５）。

4.3　要件定義工程でのシステム監査

図表－５は、見方を変えると、改正個人情報保護法を意識したシステム監査対象を表す表となる。すなわち、図表－５に示す①～⑩がシステム監査の対象を表すことになる。

さらに、この概要表にもとづきプロセス①～⑩に対する主な監査項目は、図表―６に示した。監査項目として特徴的なところは、④要件検討と⑤最終確認である。つまり④要件検討では、図表－３のステップ２、４、５、６の実施確認、図表－４の「個人情報保護要件検討シート」の実施と内容確認である。⑤最終確認では、図表－３のステッ

図表－５　要件定義工程での組織点検概要（システム監査対象）

役割＼時点	要件定義開始	要件定義途中	要件定義終了
組織の審査	③開始審査	（必要時）途中審査	⑦終了審査
有識者 / 専門部門	②法対応有無判定	（必要時）支援、途中確認	⑤最終確認
利用部門、プロジェクト	①法対応有無検討	④要件検討	⑥要件定義書完成
教育	⑧関係者の底上げ教育		
	⑨専門部門の育成教育		
⑩全体プロセス作成・実施・改善			

プ７の実施確認、図表－４の「個人情報保護要件検討シート」の利用網羅性の確認である。

５　おわりに

本論文では、栗山 (2017[6]) での提言を基に、要件定義工程で実施すべきプロセスと個人情報保護要件検討シートを作り、必要要件候補を一覧にした。さらに、企業２社の実際の要件定義工程の組織点検に着目し、既存のプロセスにこれらの組込みを行った。加えて、システム監査項目一覧を具体的に整理した。これから適用される企業の参考になろう。

なお、本研究は、改正個人情報保護法の全面施行前という時期による実践であったので、この研究をさらに発展させるには、研究実践後の評価と反映があると認識する。

特に、現実のシステム開発プロセスでは、他の管理項目と合わせて適用するため、全体での位置づけ、実施タイミングなどの評価とブラシュアップが必要である。

今後、上記の課題について少しずつではあるが、実際のシステム開発の現場や特定非営利活動法人日本システム監査人協会での活動、システム監査学会での活動を通じ、継続してシステム監査に関する研究を進めていきたい。

注

注 1）顧客の業務内容を分析し、問題に合わせた

図表－６　要件定義工程での主なシステム監査項目一覧

プロセス	主な監査項目（太字は、今回の特徴的な項目）
①法対応有無検討	・個人情報保護法対応の必要性有無は検討されているか
②法対応有無判定	・法対応有無判定は実施されているか ・対応有無判定は正しいか
③開始審査	・審査項目に含め、法対応有無は判定されているか
④要件検討	・要件検討はされているか 特に、図表－３　ステップ2、4、5、6の実施状況確認 ・漏れなく検討はされているか 図表－４　個人情報保護要件シートの項目実施状況と内容確認
⑤最終確認	・最終確認はされているか 特に、図表－３　ステップ7の実施状況確認 ・漏れなく確認・評価されているか 図表－４個人情報保護要件シート活用による確認
⑥要件定義書完成	・最終確認はされているか ・指摘は反映済みか
⑦終了審査	・審査項目に含め、実施されているか
⑧関係者の底上げ教育	・計画されている、実施されているか ・効果は出ているか
⑨専門部門の育成教育	・計画されているか、実施されているか ・効果は出ているか
⑩全体プロセス	・文書化されているか ・実施されているか ・改善、見直しをされているか

情報システムの企画、構築、運用などの業務を一括して請け負う企業のこと。IT 用語辞典 e-Words より

注 2）瀬戸洋一著「実践的プライバシーリスク評価技法」近代科学社　2014 年を参考にして本論文では「PIA」を次のように捉えることとする。

日本における民間利用の PIA は、「個人情報影響評価」、法律で規定されたマイナンバーに関する PIA は、「特定個人情報保護評価」とする。上記の両方の英文表記は、「Personal information Impact Assessment」とする。

注 3）サーバ等へログインしない方法で監視機により監視する方法の実現性は、実証実験が実施されている。「IoT を利用した遠隔監視機」により、サーバにログインしない方法で、「サーバ等の異常検出と短いサイクルの分析」を実現している [9]。

参考文献

1) 個人情報保護委員会「個人情報保護法について」 https://www.ppc.go.jp/personalinfo/　参照日：2017.07.19

2）一般財団法人日本情報経済社会推進協会 (JIPDEC)「News Release」2017 年 3 月 10 日 https://www.jipdec.or.jp/topics/news/u71kba00000075b5-att/20170310.pdf-

3）堀部政男 / 一般財団法人日本情報経済社会推進協会 (JIPDEC) 編
Privacy by Design: アン・カブキアン著、JIPDEC 訳
「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」
日経 BP 社　2012 年

4）独立行政法人情報処理推進機構 (IPA) 技術本部 ソフトウェア・高信頼化センター (SEC)「共通フレーム 2013」 2013 年 12 月

5）室谷隆著「共通フレーム 2013 の概説」
独立行政法人情報処理推進機構 (IPA) 技術本部 ソフトウェア・エンジニアリング・センター (SEC)　2013 年

6）栗山孝祐著 「個人情報取扱いシステムにおける要件定義工程の提言－流通小売業システムでの模擬適用を通じて－」
大阪市立大学大学院　創造都市研究科　修士学位論文　2017 年 3 月

7) 岡村久道著「個人情報保護法の知識 < 第 3 版 >」日本経済新聞出版社　2016 年

8）瀬戸洋一著「実践的プライバシーリスク評価技法」 近代科学社　2014 年

9）原善一郎、石井成美 :"IoT 時代における光信号の遠隔監視の実証研究 "、日本生産管理学会第 45 回全国大会講演論文集、pp.47-50

10）NPO 法人日本システム監査人協会監修『6 ヶ月で構築する個人情報保護マネジメントシステム　実施ハンドブック』同文舘版　2014 年