ＩＴ委員会研究報告第 29 号

個人情報保護に係る内部統制の検証とプライバシーフレームワークの活用

平成 17 年 7 月 20 日
日本公認会計士協会

－目　　次－

Ⅰ　本研究報告の目的

平成 17 年４月１日より個人情報の保護に関する法律（平成 15 年法律第 57 号、以下「個人情報保護法」という。）が全面施行されたことに伴い、個人情報取扱事業者に該当する企業は、個人情報を適正に取扱いかつ安全に保護することが求められるようになった。

このように日本国内では喫緊の課題となっている個人情報保護対策であるが、未だその対策が不十分な企業が多い。欧米諸国においてはこのような過程を既に経験している。公認会計士又は監査法人（以下「公認会計士等」という。）がこのような課題に対応すべく、米国公認会計士協会（以下「AICPA」という。）及びカナダ勅許会計士協会（以下「CICA」という。）が個人情報保護に関する内部統制の助言業務及び検証業務を「プライバシーフレームワーク」として具体的に公表している。

この「プライバシーフレームワーク」は、個人情報保護に関する内部統制がどのように構築されるべきであるか、また公認会計士等はこの個人情報保護に関する内部統制をどのように検証すべきか、ということを解説している。

日本公認会計士協会は、既にこの「プライバシーフレームワーク」の翻訳を研究資料４号として公表している。さらにこの「プライバシーフレームワーク」が求める内部統制が日本の個人情報保護法を遵守するために必要となる対策に十分有効であることを理解し、このような個人情報保護に係る内部統制の助言業務及び検証業務は、客観的かつ独立した立場を有する公認会計士等によって実施されることが最も望ましいものと考える。

本研究報告は、企業の個人情報保護法対応において、「プライバシーフレームワーク」の有効性を示すとともに個人情報保護に係る内部統制の助言業務及び検証業務の有用性を示すことを目的としている。

Ⅱ　定義

① プライバシーフレームワーク

「プライバシーフレームワーク」は、2003 年 11 月に AICPA/CICA が共同で策定したものである。両協会は、学界、法律家を含めて、各業界、大手国際会計事務所、小規模公認会計士事務所をメンバーとして、職業会計人を結集した特別委員会を設立し、公認会計士等がプライバシー問題とリスクについて企業に助言する際の役割の調査に基づき、プライバシー実務のためのベンチマークとして作用するプライバシーフレームワークを開発した。

プライバシーフレームワークは、プライバシーのグローバルスタンダードとしてプライバシーに関する概念を集大成したものである。プライバシーの意義を含んだ概念としての内容と、フライバシーの内部統制に関する原則および規準から構成されている。

プライバシーフレームワークは、プライバシープログラムの導入を支援し、指針を提供するために、プライバシー実務に携わるすべての公認会計士等が利用できるものである。プライバシーフレームワークは、各国の、および国際的な重要なプライバシー法、規則と指針からの概念を含んでいる。

プライバシーフレームワークは、プライバシー実務に携わる公認会計士等およびプライバシー対策を検討する企業の、両者に資するものである。

すなわち、多くの公認会計士等は、種々の企業にも有効なプライバシー実務を導入するのに十分な技能を有しているはずである。公認会計士等は、会計監査に携わっている経験から、内部統制を評価するという観点から、ビジネスプロセスおよび情報が企業の中をどのように流れているかについて理解している。同様に企業がプライバシープログラムをどのように設計すればいいかに関しても、プライバシー法、規制、指針に整合するよう指導し、顧客と企業の間に信頼感を確立しうる適切なプライバシー実務について、広範囲な助言、保証サービスを提供する機会を有している。

本研究報告では、個人情報保護法とプライバシーフレームワークを比較して、プライバシーフレームワークに基づく内部統制の助言業務及び検証業務が、個人情報保護法が求める内部統制の構築及び評価に利用できることを研究した。

② 一般的なプライバシー

プライバシーとは、一般的には「一人にしておいてもらう権利」、あるいは「覗き見もしくは公衆の耳目からの自由」と説明される。

③ プライバシーフレームワークにおけるプライバシー

プライバシーは、個人情報の収集、利用、保持、開示に関する個人及び企業の権利義務である。

④ プライバシーフレームワークにおける個人情報

「個人情報」は、識別可能な個人に関連するか、あるいはそのように推定できる情報である。それは、個人に関連づけられるか、あるいは直接的、間接的に個

人を識別するために利用できるあらゆる情報を含んでいる。企業等によって収集される個人に関する多くの情報は、特定の個人の属性を示しうるのであれば、個人情報として取り扱われる可能性が高い。個人情報のいくつかの例として、以下が挙げられている。

- 名前
- 住所あるいは電子メールアドレス
- 身分証明書番号
- 身体的特徴
- 消費者としての購買履歴

また、個人情報には機微な(sensitive)情報と位置付けられるものが含まれる。多くの国において法規等で、以下の情報は機微な個人情報として定義されている。

- 医療あるいは健康状態の情報
- 家計の情報
- 人種、あるいは民族の起源
- 政治的見解
- 宗教的あるいは哲学的な信念
- 労働組合加入の事実
- 犯罪歴、違反歴を含む情報

Ⅲ　企業にとって重要な個人情報の保護

１．個人情報の保護の重要性

企業にとって個人情報を保護しなければならない理由は、主に次の３つの視点から考えられる。

(1) 個人情報主体の不安の解消

今日の経済・社会においては、ネットワーク化・情報化の進展によって、個人情報を利用した様々なサービスが提供され、生活の利便性は日々向上している。ダイレクトバンキングやインターネットショッピングといった電子商取引などは、個人情報を利用した便利なサービスの例であり、このほかにも多くのサービスが開発・提供されている。反面、漏洩した顧客情報からの不正請求事件など、個人情報の不適切な取扱いによって個人に対して被害を及ぼすおそれがあり、社会問題にまで発展するケースも散見されるようになった。このようなことによって、一般消費者の不安が増大すれば個人情報の提供を躊躇するようになってしまい、ひいては様々なサービスの提供ができなくなる可能性もあり得る。従って、企業にはこのような個人情報主体の不安を取り除く努力が求められている。

(2) 世界的な要請

個人情報の保護は国内だけの問題ではない。個人情報が電子的に処理されるようになってからは、日本に先立って欧米諸国において法制度化が進められて

いる。欧米の企業と取引をするためには、日本の企業も欧米と同レベルの個人情報保護を達成している必要があるため、個人情報の適切な取扱いを実現するための活動が求められている。

(3) 漏洩事件等による損害

個人情報保護法の全面施行以降も頻繁に、企業からの個人情報の漏洩や個人情報の不正な利用に関する事件が報道されている。漏洩事件や個人情報の不正利用を発生させてしまった場合、企業には直接間接双方の損失が発生する可能性がある。個人情報を漏洩してしまった場合のお詫び金や損害賠償は企業にとって大きな負担となる可能性がある。また、個人情報の漏洩等を起こした企業というマイナスイメージによるブランド価値の低下や顧客からの信頼の喪失は、企業にその存続を危うくするほどの影響を与える可能性がある。

以上のことから、企業は個人情報を保護するため及び個人情報の適切な取扱いを行うために有効な内部統制を構築することが重要である。

２．個人情報保護法の内容

個人情報保護法は、高度情報通信社会の進展に伴い、個人情報の利用が著しく拡大していることから、これに対して個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的として制定されたものである。

個人情報保護法は以下のような構成になっている。

第１章　総則
第２章　国及び地方公共団体の責務等
第３章　個人情報の保護に関する施策等
第４章　個人情報取扱業者の義務等
第５章　雑則
第６章　罰則

第１章では、目的および用語の定義そして個人情報は個人の人格尊重の基本理念の下に適正な取扱が図らなければならないという基本理念を説いている。ここで「個人情報」とは、生存する個人に関する情報であり、氏名、生年月日等によって個人を識別できるものとされている。この「個人情報」を体系的にしたものが「個人情報データベース」であり、これを構成する個人情報が「個人データ」である、とされている。「プライバシーフレームワーク」における「個人情報」は、識別可能な個人に関連する、あるいは関連すると推定できる情報であるとされており、プライバシーフレームワークも個人情報保護法もほぼ同じものである。

第２章では、国及び地方公共団体の保有する個人情報についての法制上の措置などについて規定し、第３章では個人情報の保護に関する基本方針、国及び地方公共団体の施策並びに協力について規定している。

第４章は、個人情報取扱業者について利用目的の特定や制限、不正手段による

個人情報の取得禁止、個人情報の取得に際しての利用目的の通知などについて規定している。さらに、個人データを安全に管理するための措置を求め、本人の同意を得ずに個人データを第三者に提供することを禁止し、保有する個人データについて利用目的を明らかにすることを求めている。また、その個人データについて本人から開示や訂正の要請があった場合には遅滞なく対処すべきことも定めている。個人情報の保護を推進するために団体を認定したり、当該認定団体による個人情報保護指針の作成や公表を勧め、主務大臣を定めて関与することも規定している。

第５章の雑則では、個人情報保護の適用を除外する事業者として、報道機関、著述業者、大学等の研究機関、宗教団体、政治団体を示している。これらの事業者は、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、その措置内容を公表するように求められている。

第６章は、個人情報を取り扱う事業者が主務大臣の命令に違反したり、虚偽の報告を行った場合などに適用される罰則が規定されている。

個人情報の保護に関する法律施行令には、個人情報を一定の規則に従って目次や索引を付したものも個人情報データベースとなる旨や個人情報データベースに含まれる個人の数が過去６ヶ月以内に５千件を超えなければ個人情報取扱業者とはならない、また、保有個人データから除外されるものとして、当該個人データの存否が明らかになることによって本人や第三者の生命、身体または財産に危害が及んだり違法、不当な行為を助長または誘発したりするおそれがあるもの、さらには国の安全等にかかわるものや犯罪の予防、鎮圧または捜査その他公共の安全と秩序の維持に支障が及ぶおそれがあるものが除外対象となる旨が定められている。

Ⅳ　個人情報保護に係る内部統制とプライバシーフレームワーク

１．プライバシーフレームワークの求める内部統制

公認会計士等は、企業に対してプライバシーの戦略的・ビジネス的計画や、プライバシーのギャップ分析とリスク分析、ベンチマーキング、プライバシーポリシーの設計と導入、パフォーマンス測定、プライバシーに関する内部統制の、独立した立場からの検証を含むあらゆる範疇のサービスを提供することが可能である。

企業においては、プライバシーフレームワークに照らして、内部的な評価を実施することを通じて、企業自らの価値を高めることができる。

プライバシーフレームワークは、Trust サービスやその他のサービスの基準として以下のプライバシーの原則の下に、各国の法律やベストプラクティスから整備したプライバシーに関する規準を示している。

プライバシーの原則: 個人情報は、企業のプライバシー通知でのコミットメント及び AICPA/CICA プライバシー規準を充足して、収集、利用、保持、開示される。

プライバシー規準は以下の 10 の構成要素に区分され策定されている。

表１：プライバシー規準の構成要素と内容

構成要素	内　容
１．管理	企業は、プライバシーポリシーと手続を定義し、文書化し、伝達し、説明責任を割り当てる。
２．通知	企業は、プライバシーポリシーと手続についての通知を提供し、個人情報が、収集、利用、保持、開示される目的を識別する。
３．選択と同意	企業は、個人にとって可能な選択を記述し、個人情報の収集、利用、保持、開示に関して暗黙の、あるいは明白な同意を得る。
４．収集	企業は、通知で識別した目的のためだけに個人情報を収集する。
５．利用と保持	企業は、個人情報の利用を通知で識別された目的、及び個人が暗黙の、明白な同意をした目的のみに制限する。企業は、述べられた目的を満たすために必要である限りにおいて個人情報を保持する。
６．アクセス	企業は、個人に対して、レビューと更新のために個人情報へのアクセスを提供する。
７.第三者への開示	企業は、通知で識別された目的及び、個人が暗黙の、明白な同意をした目的のためだけに第三者に個人情報を開示する。
８．セキュリティ	企業は、（物理的、論理的双方の）未承認のアクセスから個人情報を保護する。
９．品質	企業は、通知で識別された目的のために正確かつ、完全かつ、適切に個人情報を保持する。
10.モニタリングと周知徹底	企業は、プライバシーポリシーと手続への準拠をモニターし、プライバシー関連の問合わせと紛争を扱う手続を持っている。

10 のプライバシー構成要素のそれぞれのために、企業の「プライバシーポリシー」、「伝達」、「手続と内部統制」に対して適切で、客観的、完全な、そして測定可能な規準が掲げられている。

「プライバシーポリシー」は、経営者の意図、目的、要件、実施責任、基準を伝達する書面の記述書である。

「伝達」は、プライバシー通知、コミットメント、その他の適切な情報について個人、社内要員、第三者に企業が行う伝達を意味する。

「手続と内部統制」は、企業が規準を満たすためにとるその他の行動である。

「プライバシーフレームワーク」には、Trust サービスにおいて、本報告のプライバシー規準に基づいてプライバシー検証を実施した場合の検証報告書の例示等も添付されており、公認会計士等が実施するプライバシー実務の具体的支援ツールとしても有用である。

２．プライバシーフレームワークとグローバルな法律等の整合性

プライバシーフレームワークは、AICPA/CICA が個人情報を守るために特別委員会を設置して作成されたものである。

この特別委員会は、大手国際会計事務所、小規模公認会計士事務所のみならず各業界、学会、弁護士等も含まれており、あるべきプライバシー実務のためのベンチマークとしてプライバシーフレームワークを開発した。

このプライバシーフレームワークは、個人情報の適切な保護と管理に欠くことができない 10 のプライバシー構成要素と関連した規準を含んでいる。

これらのプライバシー構成要素と規準は、世界中の様々な管轄区域の多くの個人情報保護法規と、認知された良いプライバシー実務に含まれる国際的に知られた公正な情報実務に基づいている。

重要な国際的なプライバシー法、規則と指針からの概念を含んでいることは、表２：「プライバシー概念の国際比較」に示されている通りである。

従って、プライバシーフレームワークは公認会計士等がプライバシーに関する助言と保証サービスの基礎を提供する知的財産と知識の集合体であり、かつ、グローバルな法律、規則及び指針等に対して整合性を有しているものと考えることができる。

なお、欧米の個人情報保護を理解するためには、OECD プライバシーガイドラインとＥＵ指令が参考になる。

＜参考＞

① OECD プライバシーガイドライン

OECD は、1980 年９月に「プライバシー保護と個人データの国際流通に関するガイドライン」を策定し、その第２部の「国内適用のための基本原則」において８原則を挙げている。この８原則は、個人情報保護立法の基本構想を示すものであり、その後法制化された各国の個人情報保護法の参考にされている。

以後、この OECD ガイドラインは、世界の多くの国の立法にその考え方が採用され、個人情報保護の普遍的原理を示すものとなっている。

② EU 指令

1995 年 10 月 24 日制定の EU 指令は、個人情報保護に関する法制度のあり方について大きな影響を与えた。

OECD 勧告は法的拘束力を有しないため、多くの加盟国は異なる形で法制化しているが、EU 指令は「第三国へのデータ提供の原則」について定める 25 条を通して、形式的にも内容的にも個人情報保護法の国際的な統一を促した。

例えば、25 条では次の２つを要請している。
・「個人データの第三国への移転は当該第三国が十分なレベルの保護措置を確保している場合に限り行うことができること」を構成国は定めなければならない。
・「EU 委員会が第三国に十分なレベルの保護を保証していないと認定した場合には、当該第三国へのデータ移転を阻止するための措置」を構成国は講じなければならない。

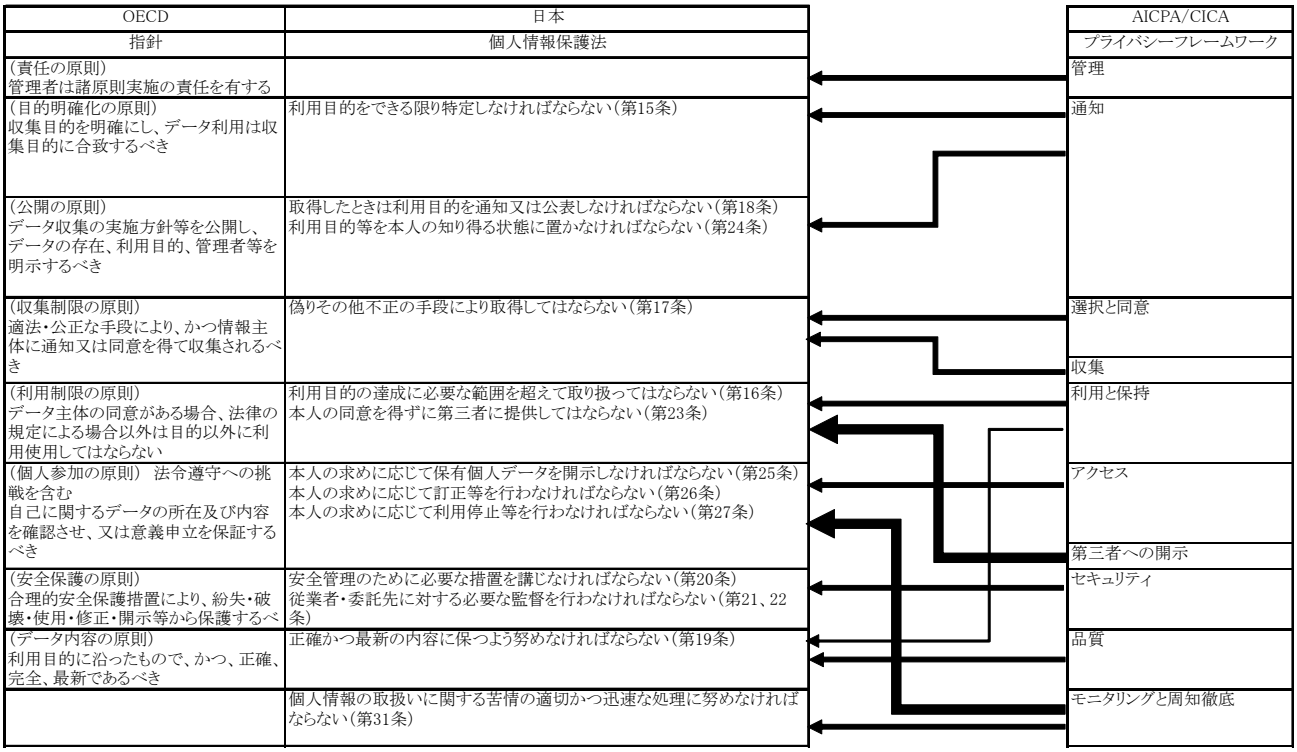
表２：プライバシー概念の国際比較(出典:ＩＴ委員会研究資料第４号「プライバシーフレームワーク」)

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
AICPA/CICA プライバシーフレームワーク	合衆国 FTC	カナダ PIPEDA	豪州 プライバシー法	合衆国 セーフハーバー原則	EU 指令	OECD 指針	合衆国 HIPAA	合衆国 GLBA	合衆国 COPPA
管理		説明責任			通告	説明責任	管理上の要求事項		
通知	通知	● 目的の識別 ● 開放性	開放性	通知	データサブジェクトに与えられる情報	● 目的の特定 ● 開放性	通知	● プライバシー及びオプトアウト通知 ● 例外事項	通知
選択と同意	選択	同意	利用と開示	選択	● データ処理の適法化 ● データサブジェクトの権利義務	収集制限	● 同意 ● 利用と開示	プライバシー及びオプトアウト通知	保護者の同意
収集		収集の制限	● 収集 ● 機微な情報 ● 匿名性	データのインテグリティ	● データの品質に関する原則 ● 免除及び制限	収集(同意を含む)制限			● 保護者の同意 ● 個人情報の収集への児童の参加に対する禁止
利用と保持		利用、開示、保持の制限	● 識別子 ● 利用と開示	(暗示されているが原則で明確化されていない)	● データ処理の適法化 ● 処理の特殊な領域 ● データの品質に関する原則 ● 免除及び制限 ● データサブジェクトの権利義務	利用の制限(開示の制限を含む)	利用と開示	開示の制限	児童によって提供された個人情報を保護者がレビューする権利
アクセス		個人のアクセス	アクセスと訂正	アクセス	データサブジェクトのデータへのアクセス権	個人の参加	アクセス		児童によって提供された個人情報を保護者がレビューする権利
第三者への開示		利用、開示、保持の制限	● 利用と開示 ● 国境を越えたデータフロー	拡散的な転送	個人データの第三国への転送	利用の制限(開示の制限を含む)	● 利用と開示 ● 開示の説明	開示の制限	保護者の同意
セキュリティ	セキュリティ	安全保護措置	データセキュリティ	セキュリティ	処理の機密保持及びセキュリティ	セキュリティ安全保護措置	セキュリティルール	GLBA セクション 501(b)により強制されたセキュリティ指針	児童から収集された個人情報の機密保持、セキュリティ、インテグリティ
品質	インテグリティ	正確性	データの品質	データのインテグリティ	データの品質に関する原則	データの品質	修正		児童から収集された個人情報の機密保持、セキュリティ、インテグリティ
モニタリングと周知徹底	周知徹底	法令遵守への挑戦	(プライバシーコミッショナー事務局による周知徹底)	周知徹底	● 裁判上の救済 ● 義務及び許可 ● 行動規範 ● 個人データの処理に関する個人を保護する監督機関と調査委員会	個人の参加(法令遵守への挑戦を含む)	(厚生労働省による遵守及び徹底)	(金融サービス産業規制当局、FTC、SEC による徹底)	周知徹底

３．プライバシーフレームワークの内部統制と個人情報保護法の関係

個人情報保護法は、OECD のプライバシーガイドラインとの整合性も図りつつ法制化されているため、OECD 勧告の８原則を満たしている。また、表２のとおり、AICPA/CICA のプライバシーフレームワークは、海外の主要な法律との整合性を図っており、この中に OECD のプライバシーガイドラインも含まれている。このため、個人情報保護法と AICPA/CICA のプライバシーフレームワークは、体系が少し異なるものの基本原則の枠組みにおいて大きな違いはない。AICPA/CICA のプライバシーフレームワークの 10 の構成要素と個人情報保護法の条文との対応を示したものが下図である。

図１：個人情報保護法とプライバシーフレームワークとの関連図



４．10 の構成要素と個人情報保護法の関連

AICPA/CICA のプライバシーフレームワークの 10 の構成要素と個人情報保護法の条文とは、基本的に整合性を持っているが、プライバシー規準と個人情報保護法の条文との関連を示すと次の表になる。ここでは、プライバシー規準と関連のある個人情報保護法の条文に「○」をつけて示している。

例えば、最初の表は、プライバシーフレームワークの「通知」の構成要素に含まれる規準とそれに関連する個人情報保護法の第 15 条、第 18 条及び第 24 条の関係を示している。個人情報保護法では、第 15 条、第 18 条及び第 24 条において、利用目的を特定し、取得に際して利用目的を通知し、保有個人データについては

さらに公表すべき事項を定めている。プライバシーフレームワークでは、2.1.1の規準の中でプライバシーポリシーの通知について述べられているが、この通知には他の構成要素に関連するプライバシーポリシーが含まれている。この表では分りやすくするために、他の構成要素におけるプライバシーポリシーもまとめて示すようにした。このため、最初の表ではプライバシーポリシーの通知または公表に関する事項として整理されている。

通知	2.1.1	3.1.1	3.1.2	4.1.1	4.1.2	5.1.1	6.1.1	7.1.1	7.1.2	8.1.1	9.1.1	10.1.1	2.2.1	2.2.2	2.2.3
	個人への伝達	個人への伝達	同意の拒否又は撤回の結果	個人への伝達	収集した個人情報の種類と収集の方法	個人への伝達	個人への伝達	個人への伝達	第三者への伝達	個人への伝達	個人への伝達	個人への伝達	通知の提供	対象とされる企業活動	明瞭性と公知性
	下記のプライバシーポリシーに関して企業から個人に通知を提供する。 ●個人情報を収集する目的 ●選択と同意 ●収集 ●利用と保持 ●アクセス ●拡散的な転送と開示 ●セキュリティ ●品質 ●モニタリングと周知徹底 当該個人以外のソースから情報が収集される場合は、当該ソースは通知で記述される。	下記について企業から個人に通知する。 ●個人情報の収集、利用、開示につき当該個人にとって可能な選択 ●法規に別段の定めがない限り、個人情報の収集、利用、開示に暗黙あるいは明白な同意が要求されること	個人情報が収集されるとき、当該情報の提供を拒否した場合の結果、あるいは当該情報を通知によって識別された目的のために利用することを拒否又は撤回した場合の結果について、企業から個人に通知する。	通知で識別された目的だけのために個人情報が収集されるということを企業から個人に通知する。	収集した個人情報の種類、収集の方法は、クッキーあるいは他の追跡技術の利用を含めて、文書化され、プライバシー通知で記述される。	個人情報が下記のようであるということを企業から個人に通知する。 ●法規に別段の定めがない限り、暗黙あるいは明白な同意があった場合、及び、通知において識別された目的のためのみに利用される。 ●述べられた目的を満たすために必要な期間のみ保持されるか、又は法律あるいは規則によって特に必要とされた期間にわたって保持される。	個人がどのようにその情報をレビューし、更新し、修正するために自身の個人情報にアクセスを得ることができるかについて企業から当該個人に情報提供する。	法規に別段の定めがない限り、通知で識別された目的及び、暗黙あるいは明白な同意をした目的のためだけに第三者に個人情報が開示されることを企業から個人に通知する。開示には、第三者のプライバシー実務及び内部統制に対する何らかの制限が含まれる。そうした開示をしないと、第三者のプライバシー実務及び内部統制が企業のそれに合致するか、上回っていることが示唆される。	プライバシーポリシーは、個人情報が開示される第三者に伝達される。	個人情報を守るために注意がなされることを企業から個人に通知する。	企業は、個人が正確かつ、完全な個人情報を企業に提供すること、及びこのような情報の訂正が必要とされる場合は、連絡を取ることに責任があるということを、当該個人に通知する。	企業は、個人が苦情について、どのように企業と連絡を取るべきかについて、当該個人に通知する。	企業のプライバシーポリシーと手続について個人に提供される通知は、下記に従う。 ●個人情報が収集されるときあるいはその前、あるいは実務的範囲でなるべく早く実施する。 ●企業のプライバシーポリシー及び手続が変更されるときにあるいはその前、あるいは実務的範囲でなるべく早く実施する。 ●個人情報が従前予定されていなかった新しい目的のために利用される前。	プライバシーポリシーと手続によって対象とされた企業活動の客観的な記述が企業のプライバシー通知に含められる。	明瞭かつ、公知された言葉が企業のプライバシー通知で利用される。
第 15 条(利用目的の特定)	○														
第 18 条(取得に際しての利用目的の通知等)	○	○		○		○							○		○
第 24 条(保有個人データに関する事項の公表等)		○	○	○	○	○	○	○	○	○	○	○	○	○	○

選択と同意	3.2.1	3.2.2	3.2.3	3.2.4
	暗黙あるいは明白な同意	新しい目的と利用のための同意	機微な情報のための明白な同意	個人のコンピュータ経由のオンラインデータ転送への同意
	暗黙あるいは明白な同意が、個人情報が収集されるときあるいはその前又は、実務的になるべく早く個人から得られる。個人の同意で表現された希望は確認されて、実行される。	既に収集された情報が前にプライバシー通知で識別された以外の目的のために利用される場合は、新しい目的は文書化され、個人は通知される。さらに、当該個人から暗黙あるいは明白な同意がこのような新しい利用あるいは目的の前に得られる。	法規に別段の定めがない限り、機微な個人情報を収集、利用、開示する場合には、個人から直接、明白な同意を得る。	個人のコンピュータ経由で個人情報が転送される前に、当該個人の同意を得る。
第 17 条(適正な取得)	○	**○:第 16 条に目的の変更について規定されている。**	×:金融機関以外の一般企業では規定なし。 ○:金融機関については、保護法には規定がないが、金融庁のガイドラインでは規定されている。	○:保護法上、個人のコンピュータから取得する場合は、書面で取得する場合と同様であるから、予め本人に利用目的を明示することが必要である(第 18 条)。この利用目的の明示は、本人が確認した記録を残すことが望ましい。

収集	4.2.1	4.2.2	4.2.3
	識別された目的に限定された収集	公正かつ合法的な手段による収集	第三者からの収集
	個人情報の収集は通知で識別された目的に必要な範囲で限定されている。	個人情報が得られることを確認する前に、個人情報の収集方法が、経営者、弁護士、あるいは両方によってレビューされる。 ●公正であること。 脅迫あるいは騙しがない。 ●合法的であること。 個人情報の収集に関連するすべての関連する法規あるいは慣習法を遵守する。	経営者は、個人情報を収集する第三者(すなわち、個人以外の情報源)が公正かつ合法的に情報を収集する信頼できる情報源であることを確認する。
第 17 条(適正な取得)	○	○	○

利用と保持、第三者への開示	5.2.1	5.2.2	7.2.1	7.2.2	7.2.3	7.2.4
	個人情報の利用	個人情報の保持	個人情報の開示	個人情報の保護	新しい目的と利用	第三者による個人情報の誤用
	法規に別段の定めがない限り、個人情報は、個人が暗黙あるいは明白な同意を提供した場合、又は通知で識別された目的のためにのみ利用される。	法規に別段の定めがない限り、個人情報が、述べられた目的を満たすために必要な期間のみ保持される。 保持する必要のなくなった個人情報が、喪失、誤用、未承認のアクセスを防止するために処分され、破棄されている。	法規に別段の定めがない限り、通知で識別された目的及び、暗黙あるいは明白な同意をした目的のためだけに第三者に個人情報が開示される。	企業が、個人情報を喪失、誤用、未承認のアクセス、開示、改竄、破損から保護するように合意した、第三者のみに対して、個人情報が開示される。	個人の事前の暗黙あるいは明白な同意によってのみ、新しい目的のために、第三者への個人情報の開示がなされる。	企業は、個人情報を転送した第三者による当該情報の誤用に対する修正行動をとる。
第 16 条(利用目的による制限)	○					
第 19 条(データ内容の正確性の確保)		◎:保護法上規定あり。 ○:金融庁の実務指針には明確にそのような定めがある。				
第 23 条(第三者提供の制限)			○	◎:個人情報が提供されるのは、委託契約のある第三者または本人の同意が必要。	○	◎:委託契約のある第三者について

アクセス、モニタリングと周知徹底	6.2.1	6.2.2	6.2.3	6.2.4	6.2.5	6.2.6	6.2.7	10.2.1	10.2.2	10.2.3	10.2.4
	個人情報への当該個人によるアクセス	個人の身元の確認	分かりやすい個人情報、時間、コスト	アクセスの拒否	個人情報の更新あるいは訂正	合意未達の記述書	苦情及び紛争の上申	問合せと苦情処理	紛争解決と調停	準拠性レビュー	準拠性違反の例
	個人は企業が自身の個人情報を保持しているかどうかを確認することができ、依頼によって、自身の個人情報にアクセスを得ることができる。	個人情報にアクセスを求める個人の身元は、彼らがその情報にアクセスを与えられる前に、認証される。	個人情報が、分かりやすい形式、合理的な時間、合理的なコストで個人に提供される。	個人情報へのアクセスを拒否する企業の正当な権利及び、該当ある場合は、法規制で明確に認められ、要求された、拒否に対して抗弁できる個人の権利の根拠などの個人情報へのアクセス要求が拒否された理由を、企業から当該個人に書面で知らせる。	個人は、企業が保持している個人情報を更新あるいは訂正することができる。実務的、経済的に可能である場合は、当該個人情報がかつて提供された第三者に対して、情報の更新あるいは訂正を行う。	個人が個人情報の訂正の要求が拒否された理由と彼らが抗弁できる方法について、書面で、企業から個人に通知する。	苦情及びその他の紛争は、それらが解決されるまでに、上申される。	苦情に対処するプロセスが採用されている。	すべての苦情に対処し、解決が文書化され、企業から個人に伝達される。	プライバシーポリシーと手続、コミットメントと適用される法律、規則、サービスレベルアグリーメントとその他の契約への準拠性がレビューされ、文書化され、レビューの結果は経営者に報告される。問題が識別された場合は、企業のプライバシーポリシーと手続は周知徹底される。	プライバシーポリシーと手続への準拠性違反の例が文書化されて、報告され、必要な場合は、修正処置がタイムリーにとられる。
第 25 条(開示)	○	○	○	○							
第 26 条(訂正等)					○	○					
第 27 条(利用停止等)							○	○			
第 31 条(個人情報取扱事業者による苦情の処理)							○	○	○	**○：点検及び監査については第 20 条で規定されている。**	**○：点検及び監査については第 20 条で規定されている。**

セキュリティ	8.2.1	8.2.2	8.2.3	8.2.4	8.2.5	8.2.6
	情報セキュリティプログラム	論理的アクセスコントロール	物理的アクセスコントロール	環境的保護措置	伝送された個人情報	セキュリティ保護措置のテスト
	セキュリティプログラムは、喪失、誤用、未承認のアクセス、漏洩、改竄、破損から個人情報を保護するための、管理的、技術的、物理的措置を開発、文書化、承認、導入している。	個人情報への論理的アクセスが下記の事項を扱う手続によって制限される。 a.社内要員と個人の権限付与及び登録 b.社内要員と個人の識別及び認証 c.アクセスプロファイルの変更と更新 d.システムアクセス権限と許諾の付与 e.自身の個人的、あるいは機微な情報以外に個人がアクセスすることの防止 f.割り当てられた役割と責任に基づいて承認された社内要員のみへの個人情報へのアクセス制限 g.承認された社内要員のみへの出力帳票配布 h.オフラインストレージ、バックアップデータ、システムとメディアへの論理的アクセス制限 i.システム設定、スーパーユーザー機能性、マスターパスワード、強力なユーティリティー、セキュリティ装置（例えばファイアウォール）へのアクセス制限 j.ウィルス、悪意があるコード、未承認のソフトウェアの導入禁止	個人情報への物理的アクセスが（個人情報を含んでいるか、あるいは保護する企業のシステム構成要素を含めて）どんな形式についても制限される。	すべての形式での個人情報が不法な破壊、予期せざる喪失、自然災害、環境上のリスク要因に対して保護される。	個人情報が、インターネット、公衆回線、メールによって伝達される場合、個人情報の転送、受信のための業界標準の暗号化技術を利用して、保護される。	個人情報を保護している重要な管理的、技術的、物理的保護措置の有効性のテストが少なくとも毎年行われる。
第 20 条（安全管理措置）	○	○	○	○	○	○
第 21 条（従業者の監督）	○	○	○	○	○	○
第 22 条（委託先の監督）	○	○	○	○	○	○

品質	9.2.1	9.2.2
	個人情報の正確性と完全性	個人情報の適切性
	個人情報は、利用される目的に応じて正確かつ、完全である。	個人情報は、それが利用される目的にとって適切である。
第 19 条（データ内容の正確性の確保）	○	○

Ⅴ　個人情報保護のためのプライバシーフレームワークの利用方法

１．個人情報保護のための内部統制の構築支援

平成 17 年４月１日から個人情報保護法が全面施行になったことに伴い、民間企業に個人情報に対する関心が飛躍的に高まっている。また、実際に個人情報の紛失や漏洩事故が絶えないこともあり、主務官庁の監督も厳しさを増している。

個人情報の保護は、個人情報を適正に扱い、個人情報の漏洩等が起こらないように安全に管理することが重要である。これは、個人情報に係るリスク管理、特にそのリスクを低減するために必要な内部統制の導入によって解決されるべきものである。このような観点から、AICPA/CICA では、適正な個人情報の保護のための規準を含むプライバシーフレームワークを開発した。このプライバシーフレームワークは、企業が個人情報の保護を図るために必要な規準を示すとともに必要なコントロールの例示を挙げている。

公認会計士等は、このプライバシー規準及びコントロールの例示を参考にして、企業が必要とする個人情報に係る内部統制の導入を支援することができる。

２．個人情報に係る内部監査支援

個人情報の不適切な取扱いや漏洩事故が企業に大きな損失を与えるため、個人情報がどのように管理されているかという観点から内部監査を実施することが増えている。このような場合に、公認会計士等が内部監査を支援する形で、個人情報に係る内部統制を評価することができる。

内部監査の支援においても、このプライバシー規準及びコントロールの例示を参考にすることができる。

３．個人情報の保護に係る内部統制の検証（合意された手続業務を含む）

AICPA/CICA は、企業の構築した個人情報の保護に係る内部統制がこの規準に照らして有効であるかどうか公認会計士等が検証する業務を開発している。この検証業務は、保証業務基準に準拠して、対象となる内部統制がプライバシー規準に照らして有効であるかどうかについて意見表明をする。

この業務によれば、公認会計士等が作成した検証報告書を第三者に公表することが可能である。また、当事者間のみで報告書を利用するのであれば、双方で合意された手続を実施した報告書を作成することができる。なお、合意された手続の報告書は契約に含まれない第三者に公表することを意図していないことに注意する必要がある

このプライバシー規準に基づいた検証業務は、AICPA/CICA が開発した Trust サービスの検証業務に含まれる形で行うことが義務付けられている。日本公認会計士協会は、AICPA/CICA とのライセンス契約により、この Trust サービスを日本で実施することのライセンスを供与されている。このため、プライバシー規準に基づいた業務を実施するには、Trust サービスに係るサブライセンスを日本公

認会計士協会から受けている公認会計士等に限られている。

以　　上