IT委員会研究資料第5号

一般に公正妥当と認められたプライバシー原則

グローバルプライバシーフレームワーク

平成18年6月15日
日本公認会計士協会

2006 年 5 月

発行元：AICPA 保証サービス執行委員会および、CICA 保証サービス開発協議会

目　次

プライバシー－一般に公正妥当と認められたプライバシー原則への序文

はじめに

多くの企業が、国、地域、あるいは、国際的に、プライバシーの管理における困難に直面している。その大部分は運用可能にすべき多くの異なったプライバシー法規制要件に直面している。

重要な内外のプライバシー規制を参照し、ビジネス上の観点から一般に公正妥当と認められたプライバシー原則が策定された。一般に公正妥当と認められたプライバシー原則は、複雑なプライバシー要件を、10 のプライバシー原則によって支えられた単一のプライバシー目標にまとめて運用可能としている。各原則は適合する必要がある、客観的かつ測定可能な規準によって支えられている。規準のサポートとして、モニタリング統制を含むポリシー要件、伝達、内部統制の例示を提供している。

この文書は、いかなる企業もプライバシープログラムの一部として利用できるプライバシー原則を提示している。一般に公正妥当と認められたプライバシー原則は、経営者がプライバシーリスクと遵守義務とビジネス上の機会に対処する有効なプライバシープログラムを作成する補助となるように策定された。この序文は、プライバシーの定義と、プライバシーが単なる準拠性の問題ではなく、ビジネス上の問題である理由の説明を含んでいる。また、企業と顧客の利益のために外部委託をする場合や、起こりうる種類のプライバシー行動計画に、これらの原則をどのように適用できるかということも例示している。

この序文と一般に公正妥当と認められたプライバシー原則と規準は、下記業務の実施担当者にとって有用である。

- プライバシーとセキュリティプログラムの監督およびモニタリング
- 企業へのプライバシーの導入および管理
- 企業へのセキュリティの導入および管理
- 準拠性評価ならびにプライバシーおよびセキュリティプログラムの監査
- プライバシーの規制

プライバシーがビジネス上の問題である理由

プライバシーをよく保護することはビジネスをよくすることである。健全なプライバシー実務は企業統治および説明責任の重要な一部である。今日の重要なビジネス上の緊急課題の 1 つは、個人情報のプライバシーを保持することである。ビジネスシステムとプロセスがますます複雑化し、洗練されるにつれ、ますます多くの個人情報が企業によって収集されつつある。結果として、個人情報が喪失、不正利用、未承認のアクセスおよび開示を含む、様々なリスクに対して脆弱となっている。それらの脆弱性は、企業、政府、一般大衆の懸念を呼び起こしている。

企業は、顧客の個人情報の適切な収集および利用の間のバランスを保とうとしている。政府は公共の利益保護を図る一方で、同時に、市民から収集された個人情報の置き場を管理しようとしている。消費者は、個人情報について非常に心配しており、多くの消費者が、個人情報の制御を失っていると感じている。さらに、社会は、特に金融、医療記録、児童についての情報のような個人情報に対する、なりすましおよび不正アクセスに重大な懸念を有している。

個人は、彼らのプライバシーが尊重され、個人情報が取引した企業によって保護されることを期待する。彼らは最早、企業が彼らのプライバシーを保護できなかったことを大目に見てやったりはしない。それ故に、プライバシーはすべての企業にとってリスク管理上の問題である。

プライバシーポリシーおよび手続が不十分である場合のリスクには下記のようなものがある。

- 企業の風評、ブランド、あるいはビジネス上の関係に与えうる損失
- 法律上の責任と業界に対する信用失墜
- 詐欺的なビジネス実務の告訴
- 顧客あるいは従業員の不信
- ビジネス目的のために個人情報を利用することに対する同意の拒否
- ビジネスの喪失および結果としてもたらされる売上ならびに市場占有率の低下
- 国際的商取引活動の中断

国際的なプライバシーへの配慮

複数の法域で活動する企業において、プライバシーリスクの管理は非常に困難である。

例えば、インターネットとビジネスのグローバルな本質は、1 つの国での規制の動きが世界中のユーザーの権利と義務に影響する場合があることを意味する。国境を越えたデータの流れに関しては、それらの法域内におけるビジネスをしたい場合、企業が対応しなければならない法規制が多くの国にある。データ保護とプライバシーに関する欧州連合の 1995 年および 1997 年の指令はその一つである。したがって、企業は、世界中のプライバシー規制要件の変化に対応する必要がある。さらに、異なった法域には、異なったプライバシー哲学があり、国際的な法令順守を複雑な業務にしている。この証左として、個人情報を収集、保持する場合、いくつかの国が、個人情報を個人に属するとみなして、企業には受託者としての関係があるという立場を取る。それとは別に、他の国では、個人情報はそれを収集する企業に属するとみなしている。

さらに企業は、事業活動を行う各国の最新の規制要件に常に対応する困難に直面している。この文書で提示するような高度な国際基準を遵守することにより、新たに出現する規制への準拠は容易になる。

国際進出が限定的な企業でさえ、他国のデータプライバシー規制要件への準拠の問題にしばしば直面している。これらの企業の多くにとって、より厳しい海外の法規制に対処する方法は明確でない。企業が不注意で、ある国で違反を犯してしまい、当該国によって公表される例となってしまうリスクが増大している。

外部委託とプライバシー

外部委託は、プライバシーに対処する上での複雑性を増大させる。企業は、プライバシーに関する実施責任を含めて、ビジネスプロセスの一部を外部委託することがある。しかしながら、企業はそのビジネスプロセスについて、プライバシーに関する説明責任まで外部委託することはできない。複雑性は、外部委託サービスを実施する企業が異なる国にあるとき増大し、プライバシー法が異なり、プライバシー規制要件を全く適用されない場合もある。そのような状況では、ビジネスプロセスを社外調達する企業は、適切にプライバシー実施責任を管理することを保証する必要がある。

この文書で提示された、一般に公正妥当と認められたプライバシー原則とそれを支える規準は、プライバシーに関する実施責任の一部が移された外部委託を実施する企業のプライバシーポリシー、手続、実務に関して評価(独立した検証を含む)を行う上で、企業を支援することができる。

これらの原則がグローバルに適用できるという事実は、健全なプライバシー実務として認識されており、世界中の様々な法域の多くのプライバシー法規制に含まれる、国際的に知られた適正な情報実務に基づく一貫した尺度を利用したプライバシー評価を外部委託先にも提供することができる。

プライバシーとは何か

プライバシーの定義

一般に公正妥当と認められたプライバシー原則の下では、「プライバシー」は、個人情報の収集、利用、保持、開示に関する個人および企業の権利義務と定義される。

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、個人に関連付けられるか、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。企業によって収集される個人に関する大抵の情報は、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は、下記が挙げられる。

- 名前
- 住所あるいは電子メールアドレス
- 身分証明書番号 (例　社会保障又は社会保険番号)
- 身体的特徴
- 消費者としての購買履歴

ある種の個人情報は「機微な情報」と位置付けられる。法規により、下記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
- 性生活
- 犯罪歴、違反歴を含む情報

機微な個人情報は、一般的に、高い水準の保護および高い注意義務が要求される。例えば、機微な情報には暗黙の同意ではなく、明白な同意が必要とされる。

人に関するある種の情報は、特定の個人と結び付けられてはならない。そのような情報は個人識別不可情報と呼ばれる。これは、個人の識別が不明、あるいは個人との関連が削除された統計上、あるいは要約された個人情報を含んでいる。このような場合、個人の身元は残っている情報から確認できない、なぜなら情報は「個人を識別不可」あるいは「匿名化」されているからである。個人識別不可情報は、個人に関連付けられることができないため、通常個人情報保護の対象とされない。

プライバシーか機密保持か

世界中の多くの国で規則によって定義されている個人の同一性を証明できる情報と異なり、機密情報の広く認められた単一の定義はない。通信および取引業務を処理するに当たり、ビジネスパートナーはしばしば「知る必要がある」(need to know)基準で保持される必要がある情報やデータを交換する。機密保持が要求される対象となる情報の種類の例は下記のようなものである。

- 取引の明細
- 設計図
- 事業計画
- 企業の銀行取引情報
- 在庫の可用性
- 値付、あるいはその依頼
- 価格リスト
- 法的文書
- 顧客や業界からの収入

また、個人情報と異なり、機密情報にその正確性と完全性を保証するアクセス権の明確な定義はない。結果として、機密であると思われることの解釈は、情報は企業間で際立って異なることがあり、たいていの事例で契約の取り決めによって運用される。セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーに関するAICPA/CICA Trustサービス原則と規準及び例示(WebTrustとSysTrustを含む)は、機密保持に関する一連の規準を提供している(www.webtrust.orgを参照)。

一般に公正妥当と認められたプライバシー原則の紹介

一般に公正妥当と認められたプライバシー原則は、プライバシーリスクと事業機会に対処する有効なプライバシープログラムを作成する上で経営者を支援するために策定されている。

一連の、一般に公正妥当と認められたプライバシー原則は、重要な内外のプライバシー法規制、ガイドラインからの主要な概念(付録 B、「国際的なプライバシー概念の比較」を参照)(注 1)と健全なプライバシー実務に立脚している。これらのプライバシー原則を利用することによって、企業はビジネスの観点からプライバシープログラムを確立し、リスク管理をする際に直面する重要な困難に先見的に対処することができる。また、一般に公正妥当と認められたプライバシー原則の利用は複数法域ベースにおけるプライバシーリスクの管理を容易にする。

全般的プライバシー目標

一般に公正妥当と認められたプライバシー原則は、下記のプライバシー目標に立脚している。

個人情報は、企業のプライバシー通知におけるコミットメントおよび AICPA/CICA 一般に公正妥当と認められたプライバシー原則に定められた規準を充足して、収集、利用、保持、開示される。

一般に公正妥当と認められたプライバシー原則

一般に公正妥当と認められたプライバシー原則は、個人情報の適切な保護と管理に欠くことができない。これらのプライバシー原則は、世界中の様々な法域の多くの個人情報保護法規と、認知された健全なプライバシー実務に含まれる国際的に知られた適正な情報実務に基づいている。

下記の事項が、一般に公正妥当と認められたプライバシー10 原則である。

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、開示に関して暗黙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、および個人が暗黙あるいは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および、個人が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を開示する。
8. プライバシーのためのセキュリティ：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リングし、プライバシー関連の苦情と紛争を扱う手続を持っている。

プライバシー10 原則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、内部統制の評価に対して適切、客観的、完全、測定可能な規準がある。「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。

一般に公正妥当と認められたプライバシー原則の利用

一般に公正妥当と認められたプライバシー原則は、下記の目的で企業によって利用される。

- プライバシーポリシーの策定および導入
- パフォーマンス測定
- ベンチマーキング
- プライバシープログラムのモニタリングおよび監査

プライバシープログラムの管理には、下記の活動がついて回る。

- 戦略形成 ― プライバシーの戦略的･事業上の計画策定
- 診断 ― プライバシーのギャップ分析およびリスク分析
- 導入 ― 解決策の策定と組織化
- 維持管理 ― プライバシープログラムのモニタリング活動
- 監査 ― 外部監査人、内部監査人による企業のプライバシープログラムの評価

下記の図表は、企業が事業活動に対処するために一般に公正妥当と認められたプライバシー原則がどのように利用できるかを総括し、例示している。

活動	全般的検討事項	一般に公正妥当と認められたプライバシー原則利用形態
戦略形成	**ビジョン** 企業の戦略は、その企業の長期的な方向性と成功に関係する。ビジョンによってその企業の文化が確認され、さらに顧客や競合他社との関係、法的･社会的･倫理的問題を含む外部環境と企業がどのように交流していくかの方向性が	**ビジョン** 企業のプライバシー対応では、企業が選好を統合し、優先順位に従って目標をランク付けするのも容易になる。 **戦略的計画策定** 企業のプライバシー対応では、一般に公正妥当と認められたプライバシー原則は企業が対処すべき重要な

	形成され、決定されていく。 **戦略的計画策定** これは、戦略的な方向付けを含む企業の全体的なマスタープランである。その目的は、すべての企業活動を共通の方向に確実に向かわせることにある。戦略的計画は、プライバシーへの準拠性を確保するための企業の長期的な目標と主要な課題を特定する。 **リソースの配分** このステップでは、戦略的計画、事業計画において設定された目標を達成するために配分される人的および財務的資源が特定される。	構成要素を識別する上で役に立つ。 **リソースの配分** 一般に公正妥当と認められたプライバシー原則を利用して、企業はシステム管理やプライバシーあるいはセキュリティ事項を含む分野で作業しかつ責任を有する人員が確定され、さらにそうした活動のための予算が決定されることもある。 **全社戦略** 戦略的文書には、将来期待される又は意図される将来計画が記述される。一般に公正妥当と認められたプライバシー原則は、検討中のシステム又は企業のプライバシー目標に関する計画を明確化するのを支援する。また、事業計画によって目標達成までのプロセス、マイルストーン、および開発される製品又はサービスが特定される。事業計画はまた、サービス、予算、開発コスト、販促および宣伝活動の詳細を含む重要な導入要素を伝達するメカニズムも提供してくれる。
診断	この段階は一般に評価の段階とされる。すなわち、この段階では企業の弱点や脆弱性および脅威がどこにあるかが特定され、企業環境が徹底的に分析される。企業にとっての初回のプライバシーサービス業務で最も共通しているのは評価である。 評価の目的は、企業のプライバシー目標と目的を評価し、それらを達成するために企業がどの範囲を対象にするかを確認することである。	一般に公正妥当と認められたプライバシー原則は、企業が直面するリスク、機会、ニーズ、プライバシーポリシーや実務、競争圧力、関連する法規制の要件の概要の理解に役に立つ。 一般に公正妥当と認められたプライバシー原則は、企業が望ましい状態と比較して現状はどうかという法規制から中立のベンチマークを提供する。
導入	この段階で、行動計画が実行に移されたり、診断による勧告が実施される。「導入」には、すべての計画されたタスクと行動計画を実行するのに必要なその他タスクの実施が含まれる。また、実施責任を割り当て、スケジュールとマイルストーンを設定して、誰がどのタスクを遂行するかも定義される。さらに、この段階には、プライバシーへの取り組みを策定する企業に対し指針と方向性、方法論、ツールを提供するために計画された一連のプロジェクトの計画と導入が含まれる。	一般に公正妥当と認められたプライバシー原則は、導入目標への合致において企業を支援する。導入段階を完了するとき、企業は下記の成果物を策定すべきである。 ● プライバシー要件に対応して変更されたシステム、手続、プロセス ● プライバシー法令順守のための書式、パンフレット、契約書 ● 社内、社外へのプライバシー周知徹底プログラム
維持管理	維持管理には、是正措置を開始するまでに進捗がどの程度行動計画と食い違っているかを確認するために作業をモニタリングすることも含まれる。モニタリング手続には、企業のプライバシーポリシー、手続への準拠を確保し、正当な注意を行使するための経営者のポリシー、手続、支援技術が含まれる。	企業は、情報へのモニタリング要請に対応する適切な報告規準や、情報を編集するための情報源や、実際に開示された情報を策定するために一般に公正妥当と認められたプライバシー原則を利用できる。また一般に公正妥当と認められたプライバシー原則は、情報開示先である当事者が、情報を受け取る権利を持っていることを確かめるための検証手続を決定することにも利用できる。
プライバシー内部監査	内部監査人は価値を高め、企業の運用を改善するように策定された客観的な保証および助言業務を提供する。彼らは、企業がリスク管理、内部統制、統治手続の有効性を評価し、改善するために系統的で、規律あるアプローチを提供して目標達成を支援する。	内部監査人は、一般に公正妥当と認められたプライバシー原則をベンチマークとして利用し、企業のプライバシープログラムを評価し、経営者に有用な情報を提供し、報告することができる。
プライバシー外部監査	外部監査人(通常、勅許会計士と公認会計士)は、保証サービスを実施できる。一般に、財務、非財務情報の外部監査は、個人、経営者、顧客、ビジネスパートナー、その他の利用者に関する信頼と信用を築き上げる。	外部監査人は、一般に公正妥当と認められたプライバシー原則に準拠して企業のプライバシープログラムを評価し、個人、経営者、顧客、ビジネスパートナー、その他の利用者に有用な報告を提供できる。

一般に公正妥当と認められたプライバシー原則と規準の表示

各原則の下に、規準は 3 列の様式で提示される。最初の列は測定規準を含んでいる。例示と説明を含む 2 番目の列は、規準の理解を深めるように意図される。例示は包括的であることを意図しておらず、また、どの例示も企業に対して規準を満たすために要求されるものでもない。3 番目の列は、健全なプライバシー実務、特定の業界あるいは国に関係がある特定の法規制の選択された要件といった補足的な情報を含む、追加的な留意事項を含んでいる。

これらの原則と規準は、企業の必要性を満たすべきプライバシープログラムを設計、導入、保守、評価することに対して基礎を提供する。

一般に公正妥当と認められたプライバシー原則と規準

管理

管理の規準	規準の例示と説明	追加的な留意事項
1.0 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。		
1.1 ポリシーと伝達		

管理の規準	規準の例示と説明	追加的な留意事項
1.1.0 プライバシーポリシー 企業は下記の側面について、プライバシーポリシーを定義して、文書化する。 • 通知 (2.1.0 参照) • 選択と同意 (3.1.0 参照) • 収集 (4.1.0 参照) • 利用と保持 (5.1.0 参照) • アクセス (6.1.0 参照) • 拡散的な転送と開示 (7.1.0 参照) • セキュリティ (8.1.0 参照) • 品質 (9.1.0 参照) • モニタリングと周知徹底 (10.1.0 参照)	プライバシーポリシーが (書面で) 文書化され、それらを必要とする社内要員と第三者にとって容易に利用可能であるようにする。	
1.1.1 社内要員への伝達 プライバシーポリシーと準拠性違反の顛末は、企業の、個人情報を収集、利用、保持、開示することに実施責任がある社内要員に少なくとも毎年伝達される。 プライバシーポリシーの変更は、変更が承認された後、速やかにこれらの社内要員に伝達される。	企業は、下記を実施する。 • 定期的に社内要員に (例えば、ネットワークあるいは Web サイト上に) 企業のプライバシーポリシーとそのプライバシーポリシーに対する変更についての適切な情報を伝達する。 • 社内要員に対して、企業のプライバシーポリシーに準拠する合意の理解を (採用時、その後定期的に) 確かめる。 • 個人情報にアクセスを持つか、あるいはプライバシーの認識、概念と問題について個人情報のセキュリティに責任を持つ社内要員に対して、(採用時、その後定期的に) 教育し、訓練する。	プライバシーポリシーは、個人情報の保護に関係があるセキュリティポリシーを包摂している。
1.1.2 ポリシーのための実施責任と説明責任 企業のプライバシーポリシーを文書化し、導入し、周知徹底し、モニタリングし、更新することに対して、人あるいはグループに実施責任と説明責任が割り当てられる。このような人あるいはグループの名前と彼らの実施責任は社内要員に伝達される。	企業は、企業プライバシー責任者のような、指名された人 (セキュリティのような、他のポリシーのために割り当てられた実施責任とは異なるプライバシーに関する実施責任を割り当てられた者) にプライバシーポリシーに対する実施責任を割り当てる。 指名された人あるいはグループの権限と説明責任は明確に文書化される。実施責任には下記の事項が含まれる。 • 個人情報の機密度合を分類し、必要とされる保護のレベルを決定するために基準を確立すること • 企業のプライバシーポリシーを定式化して、保持すること • 企業のプライバシーポリシーをモニタリングして、更新すること • 企業のプライバシーポリシーを周知徹底するための権限を委譲すること • ポリシーおよび実務への準拠度合をモニタリングし、訓練あるいは理解度を改善する対策に着手すること 役員会は定期的に、企業統治の定期的レビューにプライバシーを含める。 企業は、ユーザー、経営者、第三者に対して、個人情報のセキュリティと関係があるプライバシーポリシーと手続に従うという理解および合意を (採用時、その後毎年) 確かめる。	プライバシーに対して説明責任があるものとして特定された個人は、企業内部者であるべきである。
1.2 手続と内部統制		
1.2.1 レビューと承認 プライバシーポリシーと手続、それらに対する変更が経営者によってレビューされ、承認される。	プライバシーポリシーと手続は、下記に従う。 • 上級管理職あるいは経営委員会によってレビューされ、承認される。 • 少なくとも毎年レビューされ、必要に応じて更新される。	
1.2.2 プライバシーポリシー手続と法規制との整合性 ポリシーと手続が少なくとも毎年そして関連法規が改正されるつどレビューされ、適用される法規制の要件と比較される。プライバシーポリシーと手続は、適用される法規制の要件を充足するように修正される。	企業の弁護士あるいは法務部は、下記に従う。 • いずれの個人情報保護法規が、企業が操業する法域で適用されるかを確認する。 • 適用される法規と整合していることを保証するために、企業のプライバシーポリシーと手続をレビューする。	
1.2.3 プライバシーポリシーと手続のコミットメントの整合性 企業の要員あるいはアドバイザーが、プライバシーポリシーと手続との整合性および何らかの相違に対処するために契約書をレビューする。	経営者と企業の弁護士あるいは法務部が、企業のプライバシーポリシーと手続との整合のためにすべての契約とサービスレベルアグリーメントをレビューする。	

管理の規準	規準の例示と説明	追加的な留意事項
1.2.4 インフラとシステム管理 企業の要員あるいはアドバイザーが、プライバシーポリシーと手続との整合性および何らかの相違に対処するために、下記に関する設計、取得、導入、設定、管理と変更をレビューする。 • インフラ • システム • アプリケーション • Web サイト • 手続	手続が下記の目的のために採用されている。 • 情報システムの開発、取得、導入、保守に関する統轄、および個人情報の収集、利用、保持、開示、廃棄のために利用される関連技術の統轄。 • 企業のバックアップおよび事業継続管理プロセスがプライバシーポリシーと手続に整合していることを保証する。 • データの機密度合の等級を分類し、それぞれのデータの等級にアクセスしてもよいユーザーの等級を決定する。ユーザーは、個人情報に関与するアクセスの必要性および職務上の責任に基づいてユーザーアクセスプロファイルを割り当てられる。 • プライバシーに対する潜在的な影響に対応して、システムと手続に対する計画された変更を評価する。 • 個人情報を処理するシステムに対する否定的な影響のリスクを最小にするためにシステム構成要素に対する変更をテストする。すべてのテストデータは匿名とされる。 • 個人情報を処理するシステムおよび手続の変更を実施する前に、セキュリティへの影響を含めてプライバシー責任者と業務部門管理者による文書化と承認を要求する。緊急の変更は事後的に文書化、承認されることがある。 情報システム部門は、すべてのソフトウェアおよび適用されているそれぞれのバージョンとパッチのレベルの一覧表を保持する。 承認され、テストされ、文書化された変更のみがシステムに対して行われるという手続が存在する。	
1.2.5 支援のリソース プライバシーポリシーを導入し、支援するためのリソースが企業によって提供される。	経営者は毎年、プライバシープログラムへの要員、予算、その他のリソースの割当てをレビューする。	
1.2.6 要員の資格 企業は、個人情報のプライバシーとセキュリティを保護することに実施責任がある要員の資格を確立して、このような実施責任をこれらの資格を満たしており、必要とされる訓練を受けた要員にだけ割り当てる。	個人情報のプライバシーとセキュリティを保護することに実施責任がある内部要員の資格は下記の手続によって保証される。 • 公式の職務記述書（重要なプライバシー管理職位の実施責任、教育、職業的要件、組織的な報告を含む） • 採用手続（資格証明の包括的検査、経歴調査、対外信用調査を含む） • プライバシーとセキュリティ問題に関連する訓練プログラム • 業績評価（直属の上司によって行われ、人材育成活動の評価を含む）	
1.2.7 ビジネスおよび規制環境の変化 企業が業務を行う法域において、下記の要因の変化のプライバシーに対する影響が識別され、対処される。 • ビジネス運用とプロセス • 人材 • 技術 • 法規 • サービスレベルアグリーメントを含む契約 プライバシーポリシーと手続がこのような変化のために更新される。	企業は、下記の変化がプライバシーに与える影響をモニタリング、評価、対処するための継続的なプロセスを有している。 • ビジネス運用とプロセス • プライバシーとセキュリティ問題に対して実施責任を割り当てられた人材 • 技術（導入前） • 法規制環境 • 第三者とのサービスレベルアグリーメントを含む契約（契約書でのプライバシーとセキュリティ関連の条項を大きく変える変更が、それらが実施される前に、プライバシー責任者あるいは企業の弁護士によってレビューされ、承認される。）	

通知

通知の規準	規準の例示と説明	追加的な留意事項
2.0 企業は、プライバシーポリシーと手続について通知を提供し、個人情報が、収集、利用、保持、開示される目的を識別する。		
2.1 ポリシーと伝達		
2.1.0 プライバシーポリシー 企業のプライバシーポリシーは、個人に対する通知の提供を扱う。		

通知の規準	規準の例示と説明	追加的な留意事項
2.1.1 個人への伝達 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 (3.1.1 参照) • 収集 (4.1.1 参照) • 利用と保持 (5.1.1 参照) • アクセス (6.1.1 参照) • 拡散的な転送と開示 (7.1.1 参照) • セキュリティ (8.1.1 参照) • 品質 (9.1.1 参照) • モニタリングと周知徹底 (10.1.1 参照) 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。	企業のプライバシー通知は、下記に従う。 • 個人情報が収集される目的を記述する。 • 機微な個人情報を収集する目的が法律上の要件の一部をなすかどうかを示す。 • 様々な方法 (例えば、面談、電話、申込書、アンケート、あるいは電子的) で提供されるかもしれない。書面の通知は望ましい方法である。	下記のような場合、いつ個人情報が開示されるかの条件を通知において記述することがある。 • 公共の安全保障あるいは防衛目的のためのある特定の処理 • 公衆衛生あるいは安全の目的のためのある特定の処理 • 法律によって許され、あるいは必要とされるとき 通知で記述された目的は、個人が合理的に目的を理解することができ、どのように個人情報が利用されるかについて記述すべきである。このような目的は企業のビジネス目的と整合していて、過度に広範囲であるべきではない。 ポリシーのより詳細な部位へのリンクを伴った、概要レベルの通知を提供することに留意すべきである。 「簡略版」プライバシー記述の利用は、ますます一般的になってきている。簡略版プライバシー記述は、それに関連する特定の事業活動における関連する個人情報の範囲、収集、利用、選択、契約の詳細、その他の情報を別個のページに簡潔に要覧するものである。
2.2 手続と内部統制		
2.2.1 通知の提供 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およ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。	プライバシー通知は、下記に従う。 • 個人情報が個人から最初に収集されるとき、既にアクセス可能であり、利用可能である。 • 企業に個人情報を提出すべきかどうか決めることができるようにタイムリーな方法で提供する (それはつまり、情報が収集されるときにおいてあるいはその前に、あるいは実務的範囲でなるべく早くということ)。 • 個人が、企業に個人情報を提出したとき、又は通知を読んだときに、通知の最終更新日が分かるように明確な日付が入っている。 さらに、企業は、下記に従う。 • 企業のプライバシーポリシーと手続の従前のやり取りを記録する。 • 従前に伝達されたプライバシーポリシーに対する変更を個人に情報提供する。例えば、企業の Web サイトに通知を開示する、あるいは郵便で書面の通知を送る、あるいは電子メールを送る。 • プライバシーポリシーと手続への変更が個人に伝達されたことを文書化する。	3.2.2 「新しい目的と利用のための同意」を参照。 ある種の規制要件、プライバシー通知が定期的に (例えば、Gramm-Leach-Bliley 法＜GLBA＞では毎年) 提供されねばならないとしている。

通知の規準	規準の例示と説明	追加的な留意事項
2.2.2 対象とされる企業活動 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。	プライバシー通知は特定の企業、事業領域、事業所、対象となる情報の種類を記述する。例えば、下記のようである。 • (法的、政治的) 運営上の法域 • 事業領域と提携先 • 事業系列(業務内容) • 第三者 (例えば、運送会社と他の種類のサービスプロバイダ) の種類 • 情報 (例えば、顧客および潜在顧客の情報) の種類 • 情報源 (例えば、メールオーダーあるいはオンライン) 企業は、もう企業のプライバシーポリシーと手続の対象とされないとみなしうるとき (例えば、企業の Web サイトに類似した別の Web サイトにリンクを貼るか、または第三者によって提供された企業の紹介サービスの利用)、個人にその旨を知らせる。	
2.2.3 明瞭性と公知性 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。	プライバシー通知は、下記に従う。 • 平易な、単純な言葉で記述される。 • 適切にラベルをはられた、明瞭な、適当な大きさの字で記述する。 • データ収集の個所にリンクされ、Web サイト上に示されている。	複数の通知が異なった子会社あるいは事業部について利用される場合は、類似の様式が、消費者の混乱を避け、どんな相違の理解も明確になされるよう奨励されるべきである。 ある種の、GLBA のような規制が、開示が含んでいなくてはならない特定の情報を含んでいることがある。 例示的な通知は、しばしばある特定の業界と収集、利用、保持と開示の種類のために利用可能である。

選択と同意

選択と同意の規準	規準の例示と説明	追加的な留意事項
3.0 企業は個人にとって可能な選択を記述して、個人情報の収集、利用、開示に関して暗黙あるいは明白な同意を得る。		
3.1 ポリシーと伝達		
3.1.0 プライバシーポリシー 企業のプライバシーポリシーは、個人にとって可能な選択と得られるべき同意を扱う。		
3.1.1 個人への伝達 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	企業のプライバシー通知は、明快かつ、簡潔な方法で記述される。 • 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 • 個人がこれらの選択を行う場合に従うべきプロセス (例えば、販促物を受け取らないために「オプトアウト」ボックスをチェックする。) • 望んでいる連絡方法を変更する個人の能力およびプロセス • 取引またはサービスのために必要な個人情報の提供をしなかった場合の結果 個人は下記について助言を受ける。 • プライバシー通知で識別された目的に不可欠でない個人情報は提供する必要がない。 • 法的あるいは契約上の制限事項および合理的な通知によって、後日、希望が変えられたり、同意が撤回されることもある。 必要とされる同意の種類は個人情報の性質と収集の方法によって異なる (例えば、ニュースレターに加入している個人が、企業から伝達を受けるために暗黙の同意をする)。	ある種の法規 (1988 年豪州プライバシー法セクション 1 原則 11 : 個人情報の開示制限のような) では、個人の同意を得ないことができる企業の特定の義務の免除を提供している。下記に例示する。 • 記録管理者が、合理的な根拠をもって、他の目的のための情報の利用が、個人又は関係者の生命又は健康に対する重大な、差し迫った脅威を防止、軽減できると認めたとき • 他の目的のための情報の利用が法律によって許容ないし認められているとき

選択と同意の規準	規準の例示と説明	追加的な留意事項
3.1.2 同意の拒否又は撤回の結果 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。	企業は、収集に際しては下記について個人に知らせる。 • 個人情報の提供を拒否した場合の結果（例えば、取引が処理されない等） • 同意を拒否又は撤回した場合の結果(例えば、製品やサービスの情報をオプトアウトした場合、販促情報を得られない等) • 最小限要求される以上の個人情報を提供しなかったことにより、情報主体がどのような影響を受け、又は受けないか（例えば、サービスや製品が提供されない等）	
3.2 手続と内部統制		
3.2.1 暗黙あるいは明白な同意 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。	企業は、下記に従う。 • タイムリーな方法で個人の同意を得て、（個人情報が収集されるときあるいはその前、あるいは実務的になるべく早く）文書化する。 • 個人の希望を確認する（書面で、あるいは電子的に）。 • 個人の希望の変更を文書化し、管理する。 • 個人の希望が実行されることを保証する。 • 個人の連絡先に選択肢があることを利用者に通知し、ベンダーに解釈することを要求するプロセスを提供することにより、個人の希望に関して記録の矛盾に対処する。 • 企業内および第三者による個人情報の利用が、個人の希望のとおりであることを保証する。	
3.2.2 新しい目的と利用のための同意 既に収集された情報が従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。	個人情報が従前に指定された以外の目的のために利用されるとき、企業は下記に従う。 • 個人に通知して、新しい目的を文書化する。 • 新しい目的のために個人情報を使うために同意あるいは同意の撤回を得て、文書化する。 • 個人情報が新しい目的のとおりに利用され、同意が撤回された場合は、利用されていないことを保証する。	ポリシーが変更されても、新しい目的あるいは利用を形成しない場合、企業は法律家と相談することが望ましい。
3.2.3 機微な情報のための明白な同意 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。	企業は、個人が明白な同意を提示した場合に限り、機微な情報を収集する。明白な同意は、個人が、ある行動を通して、機微な情報の利用、開示に肯定的に同意することを要求する。明白な同意が個人から直接得られ、文書化される。例えば、個人がボックスをチェックするか、書式に署名するように要求することによって。これは時に「オプトイン」と呼ばれる。	個人情報保護と電子文書法（PIPEDA）スケジュール１ 条項 4.3.6 は、企業が、ある情報が機微であると考えられる場合は、通常は明白な同意を得るよう努めることとしている。 付録 B「プライバシー概念の国際比較」で言及している大抵の法域では、明示的に許諾された場合を除き、機微なデータの収集を禁じている。例えば、欧州連合（EU）加盟国ギリシアの「個人データの処理に関する個人の保護に関する法律」の第 7 章では、「機微なデータの収集および処理は禁止する」としている。しかしながら、機微なデータの収集および処理についての許諾が得られる場合がある。 特定の法域では、政府が発行する個人識別子、例えば社会保障番号または社会保険番号は、機微な情報としてとらえている。

選択と同意の規準	規準の例示と説明	追加的な留意事項
3.2.4 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 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。	企業は、顧客のコンピュータ内に個人情報（クッキー以外の）を保存、書き換え、複写することに対する顧客の許諾を得る。 顧客が、クッキーを望まない意思を企業に示した場合、企業はクッキーが顧客のコンピュータに決して保存されない内部統制を有すべきである。 企業は、許諾を得ることなく個人情報を転送するようなソフトウェアをダウンロードしない。	コンピュータから情報を採取し、抽出して、その後、個人情報の抽出に利用されることを意図したソフトウェア（例　スパイウェア）については、留意すべきである。

収集

収集の規準	規準の例示と説明	追加的な留意事項
4.0 企業は、通知で識別された目的だけのために個人情報を収集する。		
4.1 ポリシーと伝達		
4.1.0 プライバシーポリシー 企業のプライバシーポリシーは個人情報の収集を扱う。		特定の法域（例えば、欧州の国）では、個人情報を収集する企業に対して、規制当局への登録が要求される。
4.1.1 個人への伝達 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。	企業のプライバシー通知は、収集された個人情報の種類および個人情報の収集方法を開示する。	
4.1.2 収集した個人情報の種類と収集の方法 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。	収集された個人情報の種類の例は、下記のようである。 • 家計（例えば、銀行口座情報） • 健康（例えば、肉体的精神的健康状態あるいは病歴についての情報） • 人口統計的情報（例えば、年齢、所得階層、社会的居住者地域分類） 個人情報の収集方法および第三者情報源は、下記のようである。 • 信用調査機関 • 電話 • インターネットを使った形式、クッキー、あるいは Web ビーコン 企業のプライバシー通知はそれがクッキーと Web ビーコンの利用および利用方法を開示する。通知は、クッキーを拒否した場合の結果も記述する。	特定の法域（例えば、欧州連合）では、個人がクッキーの利用を撤回する機会を持つことが要求される。
4.2 手続と内部統制		
4.2.1 識別された目的に限定された収集 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。	システムと手続が下記の目的のために採用されている。 • 通知において、識別された目的に不可欠な個人情報を指定し、任意の個人情報と区別する。 • 定期的に個人情報を必要とする企業のプログラムあるいはサービスをレビューする（例えば、5 年ごとあるいはプログラムあるいはサービスが変わる度に）。 • 機微な個人情報が収集されるとき、明白な同意を得る（3.2.3「機微な情報の明白な同意」を参照）。 • 個人情報の収集がプライバシー通知において識別された目的に制限されており、すべての任意のデータが識別されていることをモニタリングする。	

収集の規準	規準の例示と説明	追加的な留意事項
4.2.2 公正かつ合法的な手段による収集 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。	企業の弁護士は収集方法とその変更についてレビューする。	下記は詐欺的な実務であると思われるかもしれない。 • 個人に通知せずに個人情報を収集するため、企業の Web サイトに、クッキーと Web ビーコンのような、ツールを使う。 • 個人に通知せずに他のソースの個人情報と個人の Web サイトアクセス時に集めた情報を関連付ける。 • 個人への通知を避けるために情報を収集するため、第三者を使う。 企業が操業している以外の法域における法規制の要求事項について留意するべきである（例えば、カナダの企業がヨーロッパ人についての個人情報を収集する場合、ヨーロッパ特有の法律上の要求事項の適用を受けることがある）。 苦情をレビューすることにより、不公正又は違法な実務の存在を識別するのに役立つことがある。
4.2.3 第三者からの収集 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。	企業は、下記に従う。 • 第三者データプロバイダとの関係を確立する前にデューデリジェンスを実施する。 • 第三者情報源から個人情報を受け取る前に彼らのプライバシーポリシーと収集方法をレビューする。	情報が信頼できる情報源から収集され、公正かつ合法的に収集されることを要求する規定が契約に含まれることがある。 第三者から収集された情報が個人から収集された情報と一緒にされる場合は、個人に通知することに留意すべきである。

利用と保持

利用と保持の規準	規準の例示と説明	追加的な留意事項
5.0 企業は、個人情報の利用を通知で識別された目的、および個人が暗黙あるいは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。		
5.1 ポリシーと伝達		
5.1.0 プライバシーポリシー 企業のプライバシーポリシーは個人情報の利用と保持を扱う。		
5.1.1 個人への伝達 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、および、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。	企業のプライバシー通知は、個人情報の利用を記述する。例えば、下記のようである。 • ビジネス取引の処理（例えば、クレームと保証、給与、税金、特典、ストックオプション、賞与、あるいはその他の報酬スキーム） • 製品あるいはサービスについての問い合わせあるいは苦情の取扱い、又は製品あるいはサービスの販売促進の相互作用 • 製品設計と開発、あるいは製品あるいはサービスを購入すること • 科学的、あるいは医療の研究活動、マーケティング、調査、又はマーケット分析に対する参加 • Web サイトの個人化、あるいはソフトウェアのダウンロード • 法律上の要件 • ダイレクトマーケティング 企業のプライバシー通知は個人情報が述べられた目的を満たすために必要である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と説明する。	
5.2 手続と内部統制		
5.2.1 個人情報の利用 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。	下記を保証するために、システムと手続が個人情報を利用するように採用されている。 • 企業のプライバシー通知で識別された目的に従って利用している。 • 個人から受け取られた同意に沿って利用している。 • 適用される法規制を遵守している。	特定の法規制では、個人情報の利用について特殊な条項を有している。例えば、GLBA、医療保険の携行性および責任法（HIPAA）、児童オンラインプライバシー保護法（COPPA）。

利用と保持の規準	規準の例示と説明	追加的な留意事項
5.2.2 個人情報の保持 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。	企業は、下記に従う。 • 保持ポリシーと処分手続を文書化する。 • 保存方法（例えば、電子媒体、紙）に関係なく、保持ポリシーに従って、記録を消去するか破棄する。 • 保持ポリシーに従って、アーカイブおよびバックアップのコピーを保持して、貯蔵して、処分する。 • 個人情報が、そうする正当なビジネス上の理由がないなら、保持期限を越えて保持されないことを保証する。 • 必要に応じて特定の個人についての個人情報を配置、削除する。例えば、取引終了後にクレジットカード番号を削除するなど。 • 識別された目的を達成するのに必要でなくなった、あるいは法規制によって必要とされなくなった個人情報については定期的かつ体系的に破棄し、消去し、匿名化する。 契約の要件について、保持ポリシーを確立するときに、留意すべきである。	特定の法律では、個人情報の保持期間が特定されている。例えば、HIPAA は、個人情報の作成または最終利用後 6 年の保持期間を定めている。 法規制上の記録保持要件があるかもしれない。例えば、ある特定のデータが課税目的あるいは労基法に従って保持される必要があるかもしれない。

アクセス

アクセスの規準	規準の例示と説明	追加的な留意事項
6.0 企業は、レビューと更新のために個人情報へのアクセスを個人に提供する。		
6.1 ポリシーと伝達		
6.1.0 プライバシーポリシー 企業のプライバシーポリシーが個人情報へのアクセスを個人に提供することを扱う。		
6.1.1 個人への伝達 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。	企業のプライバシー通知は、下記に従う。 • 個人が自身の個人情報にアクセスを得る方法、そのアクセスを得ることについてのコストについて説明する。 • 個人が、自身の個人情報を更新し、修正するための方法を解説する（例えば、書面で、電話で、電子メールで、あるいは企業の Web サイトを利用して）。	
6.2 手続と内部統制		
6.2.1 個人情報への当該個人によるアクセス 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。	下記の手続が採用されている。 • 企業が個人情報を保有又は統制しているかどうかを確認する。 • 当該個人情報にアクセスを得るためにとられる段階を伝達する。 • タイムリーに個人の要請に返答する。 • 個人と企業両方に都合が良い印刷物、あるいは電子媒体で、依頼に応じて、個人情報のコピーを提供する。 • アクセスの否認と未解決の苦情と紛争を含めてのアクセスととられた行動の要請を記録する。	ある種の法規が下記を特定している。 • 個人情報へのアクセス提供条文および要求事項（例えば、HIPAA） • 個人情報へのアクセス依頼は書面で行うという要件
6.2.2 個人の身元の確認 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。	従業員は、下記のアクセス権を与える前に個人の身元を認証するように十分に訓練される。 • 彼らの個人情報にアクセスする。 • 機微な、あるいはその他の個人情報（例えば、住所あるいは銀行明細のような情報を更新するために）を変えることを要請する。 企業は、下記に従う。 • 認証のために政府の発行した識別番号（例えば、社会保障番号あるいは社会保険番号）を利用しない。 • 記録の中の住所に変更依頼の情報を郵送するが、住所変更のケースでは、古い住所、新しい住所の両方に郵送する。 • オンラインでユーザーアカウント情報にアクセスするためにユーザーIDとパスワード（あるいは同等物）が利用されることを要求する。	認証の程度は個人情報の種類と機密度合を考慮して利用可能とする。異なった技術の利用が異なった経路に関して考えられる。 • Web • 対話型の音声応答システム • コールセンター • 対面

アクセスの規準	規準の例示と説明	追加的な留意事項
6.2.3 分かりやすい個人情報、時間、コスト 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。	企業は、下記に従う。 • (例えば、コードとか、番号とか、過度に技術的あるいは専門的な用語ではない) 分かりやすい形式で、個人と企業の双方にとって便利な形式で、個人に個人情報を提供する。 • 要求された個人情報を探すために合理的な努力をし、個人情報が見いだされることができない場合は、合理的な検索がなされたことを明示するため、十分な記録を保持する。 • 開示された情報が、直接、あるいは間接的に、別の人を識別しないことを保証するのに正当な注意を払う。 • 他のビジネス取引のために、あるいは法律によって認められ、要求されるところに従って、企業の通常の応答時間に近似した時間で個人情報へのアクセスを提供する。 • アーカイブ、あるいはバックアップシステムおよびメディアに置かれた個人情報へのアクセスを提供する。 • アクセスを要求した時点あるいは実務上の可能な限り早い時点に、個人に対してアクセスに要するコストを通知する。 • 企業が個人情報へのアクセスを提供するコストを超えない範囲で、個人に対してアクセス料金を従量課金する。 • 個人情報を調査するために適切な物理的空間を提供する。	企業は、情報の品質向上のための機会を得るためだけではなく、ビジネスおよび顧客との関係に利点があるため、個人に対して、彼らの個人情報へのアクセスを提供する場合がある。
6.2.4 アクセスの拒否 個人情報へのアクセスを拒否する企業の正当な権利および、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。	企業は、下記に従う。 • なぜ個人情報へのアクセスが拒否され得るかの理由を記述する。 • すべてのアクセス拒否と未解決の苦情と紛争を記録する。 • 個人情報の一部へのアクセスが正当に拒否された状況では、部分的なアクセスを個人に提供する。 • 個人情報へのアクセスが拒否された理由について、書面での説明を個人に提供する。 • 個人情報へのアクセスが拒否された場合、公式の上申およびレビュープロセスを提供する (6.2.7「苦情および紛争の上申」を参照)。 • 企業の法的な権利と、該当ある場合は、抗弁すべき個人の権利を伝達する。	ある特定の法規制 (例えば、1988 年豪州プライバシー法ポイント 2 原則 5「記録保持者による記録の保持に関する情報」、PIPEDA セクション 8(4)(5)(7)、9、10、28) が、アクセスの拒否できる場合、そのために従うべき (顧客に 30 日以内に書面で拒否について通知するというような) プロセス、違反の場合に課される罰則を明らかにしている。
6.2.5 個人情報の更新あるいは訂正 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。	企業は、下記に従う。 • 個人情報の記録を更新あるいは訂正するために従わなくてはならないプロセス (例えば、書面、電話、電子メール、企業の Web サイトの利用) を記述する。 • (例えば、エディットバリデーションコントロールや必須項目の入力強制により) 個人が更新、あるいは訂正する個人情報の正確性と完全性を検証する。 • 企業の従業員が個人に代わって変更をする場合、変更した日付、時刻、変更した人物の身元を記録する。 • 実施可能であり、合理的であるなら、修正、消去、非開示のため、個人情報が開示された旨を当該第三者に通知する。	特定の法域(例えば、PIPEDA スケジュール 1 条項 4.5.2 と 4.5.3)では、個人情報は企業がそれ以上の処理を停止するのでなければ消去されることができない。
6.2.6 合意未達の記述書 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。	個人と企業が、個人情報が完全で、正確であるかどうかに関して意見を異にする場合は、個人は個人情報が完全で、正確でないということを主張する文書を受諾するように企業に要請することができる。 企業は、下記に従う。 • 個人と企業が、個人情報が完全で、正確であるかどうかに関して意見を異にする場合、その内容を文書化する。 • 抗弁しようとする個人の権利を引用しつつ、個人情報の訂正の要求が拒否された理由について、個人に書面で通知する。 • 個人情報へのアクセスが要求され、あるいはアクセスが実際に提供された場合、合意未達の記述書では、個人によって求められた変更の性質と企業の拒否理由についての情報が含まれるということを個人に通知する。 • 適切である場合は、かつて個人情報を提供した第三者に合意が未達成であることを通知する。	特定の法規 (例えば、HIPAA) が、個人からの要求の拒否および合意未達の取扱いのための特定の要求事項を有している。 個人が抗弁した場合に満足に解決されていないならば、適切であれば、このような抗弁の存在は、問題の情報にアクセス権を有する第三者に伝達される。

アクセスの規準	規準の例示と説明	追加的な留意事項
6.2.7 苦情および紛争の上申 苦情およびその他の紛争は、それらが解決されるまでに、上申される。	企業は、未解決の苦情と紛争を扱う公式の上申プロセスを確立している。 企業は、下記に従う。 • 個人の苦情と紛争処理を取り扱うことに責任がある従業員に対して、上申プロセスに関する研修を行う。 • 未解決の苦情と紛争を文書化する。 • 経営者のレビューのために苦情および紛争について上申する。 • タイムリーに苦情と紛争を解決する。 • 適切であれば、苦情と紛争の解決を支援するために、外部の第三者紛争解決サービス（例えば、調停人）と契約する。	10.1.1「個人への伝達」、10.2.1「苦情処理」、10.2.2「紛争解決及び調停」を参照。 特定の法規（例えば、PIPEDA）では最高裁判所までの法廷システムを通じた上申を認めている。

第三者への開示

第三者への開示の規準	規準の例示と説明	追加的な留意事項
7.0 企業は、通知で識別された目的および、個人が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を開示する。		
7.1 ポリシーと伝達		
7.1.0 プライバシーポリシー 企業のプライバシーポリシーは個人情報の第三者への開示を扱う。		
7.1.1 個人への伝達 法規に別段の定めがない限り、通知で識別された目的および、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。	企業のプライバシー通知は、下記に従う。 • 第三者と個人情報を共有するための実務（該当ある場合は）および情報の共有理由を記述する。 • 個人情報を開示する第三者およびその等級を識別する。 • 個人は、法規に別段の定めがない限り、(1)通知で識別された目的および、(2)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通知される。	企業のプライバシー通知では下記の事項が開示される。 • 第三者に開示された個人情報のプライバシーとセキュリティを保証するために採用されるプロセス • 個人が自身の情報を変更した場合は、第三者と共有された、古く、不正確な個人情報も変更されるようにする、第三者との共有個人情報の更新方法
7.1.2 第三者への伝達 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。	第三者と個人情報を共有するに先立って、企業はプライバシーポリシーを伝達して、当該第三者のデータ保護実務は十分に企業と同程度であるとの書面の記述書を取得する。	
7.2 手続と内部統制		
7.2.1 個人情報の開示 法規に別段の定めがない限り、通知で識別された目的および、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。	下記のシステムと手続が採用されている。 • 個人が開示のために暗黙あるいは明白な同意をしなかった場合、第三者への個人情報の開示は防止される。 • 第三者に開示された個人情報の性質と程度を文書化する。 • 第三者への開示が、企業のプライバシーポリシーと手続、もしくは法規によって明確に許容され、要求される事項を遵守しているかどうかを検証する。 • 法的理由のためのあらゆる第三者への開示を文書化する。	司法あるいは行政機関に対して、種々の法律上のプロセスを通じ、個人情報が開示されることがある。 ある種の法規制においては個人情報開示のために特定の規定が存在する。他の検証可能な同意を要件として、同意なしでの個人情報の開示を認める場合がある。

第三者への開示の規準	規準の例示と説明	追加的な留意事項
7.2.2 個人情報の保護 企業が、企業のプライバシーポリシーの関連箇所に整合して個人情報を保護するよう合意した、第三者のみに対して個人情報が開示される。	下記のシステムと手続が採用されている。 • 情報が第三者（すなわち、契約あるいは協定によって）に提供される場合、企業と同等な個人情報保護のレベルを提供する。 • 例えば、保証（例えば、監査報告）、契約上の義務、あるいは他の誓約（例えば、書面の年次確認書）を得ることによって、第三者による個人情報保護のレベルが、企業のそれと同等であることを誓約する。 • 第三者の個人情報の利用を、契約履行に必要な目的に制限する。 • 第三者に個人の意向を伝達する。 • 企業によって転送された個人情報についてのアクセス又は苦情の要求をするために企業プライバシー責任者を明示する。 • 第三者が企業によって提供された個人情報をいつ、どのように保持するか、あるいは返送するかを明示する。	企業は、第三者に転送された情報を含めて個人情報の保有および保護に関して責任がある。 ある種の規制（例えば、合衆国連邦財務規制当局の通達）が、企業がサービスプロバイダの選定に当たり、適切なデューデリジェンスを実施することによって、適切なサービスプロバイダを監督するための合理的な手続を踏むことを要求する。 欧州のいくつかの国を含む特定の法域では、個人情報を転送しようとする企業は、転送前に規制当局に対して登録することを要求される。 PIPEDA は、個人情報を第三者により処理させる場合は、同等な保護の水準を要求する。 欧州連合指令の第 25 条は、第三者が十分な水準の保護を確約する場合のみ転送が可能であることを要求している。
7.2.3 新しい目的と利用 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。	下記のシステムと手続が採用されている。 • プライバシー通知で識別されていない目的のために、第三者に個人情報を開示する前に、個人に対して通知し、同意を得る。 • 個人に通知し、同意を受けたかどうかを文書化する。 • プライバシー通知で特定された利用においてのみ、第三者に個人情報が提供されていることをモニタリングする。	第三者への拡散的転送には下記のような第三者への転送が含まれる。 • 子会社あるいは関係会社 • 個人によって求められたサービスを提供すること • 司法、行政機関 • 外国および、他の要求事項の適用を受ける可能性のある当事者
7.2.4 第三者による個人情報の誤用 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。	企業は、下記に従う。 • 第三者のいかなる個人情報の誤用の兆候も識別するために苦情をレビューする。 • 企業のプライバシーポリシーと手続あるいは契約上の合意と相違した個人情報を利用、あるいは開示する第三者の了見に対して対応する。 • 実行できる程度に、企業のプライバシーポリシーと手続（例えば、影響を受ける個人に通知し、他人に開示された情報の回復を試み、口座番号を廃止して再発行する）に違反した、第三者の個人情報の利用あるいは開示により起こされた損害を緩和する。 • 第三者が個人情報（例えば、契約の条項が個人情報の誤用のケースを扱う）を誤用した場合、修正行動をとる。	

プライバシーのためのセキュリティ

プライバシーのためのセキュリティの規準	規準の例示と説明	追加的な留意事項
8.0 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。		
8.1 ポリシーと伝達		
8.1.0 プライバシーポリシー 企業のプライバシーポリシーは個人情報のセキュリティを扱う。	プライバシーポリシーは、電子的、紙面、あるいは他の形式であるか否かにかかわらず、個人情報のプライバシーを保護する十分なセキュリティ対策を扱う。セキュリティ対策は、個人情報の機微の程度と整合している。	あらゆる企業の統制下、あるいは企業の統制下であるとみなされる場所での個人情報は保護されなければならない。

プライバシーのためのセキュリティの規準	規準の例示と説明	追加的な留意事項
8.1.1 個人への伝達 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。	企業のプライバシー通知は、例えば下記のように個人情報を保護するために利用されるセキュリティ対策の一般的な種類を記述する。 • 従業員は、職務上の責任に基づいて個人情報にアクセスする権限を与えられる。 • 電子的に保持された個人情報に対する未承認のアクセスを防止するために認証手続が利用される。 • ハードコピー形態で保存された個人情報に対して物理的セキュリティが保持され、インターネット上に送られた個人情報への未承認のアクセスを防止するために暗号化が利用される。 • 機微な情報については、特殊なセキュリティ保護が適用される。	ユーザー、経営者、プロバイダ、その他の当事者は健全なプライバシー実務を開発し、採用すること、セキュリティの必要性を認識して、他者との法的な利害関係を尊重する手立てを促進しようと努力すべきである。 プライバシー通知においては、ユーザーIDとパスワードを秘密にしておくとか、セキュリティ違反を報告するというような、個人のセキュリティ義務を開示することに留意すべきである。 社内のセキュリティが危殆化しないように、詳細なセキュリティ手続の開示を制約することに留意すべきである。
8.2 手続と内部統制		
8.2.1 情報セキュリティプログラム 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。	企業のセキュリティプログラムは下記の個人情報の保護と関係がある事項を扱う。 • 定期的なリスク評価 • 承認されたユーザーのセキュリティ要件の識別と文書化 • アクセスの許可、許可されるアクセスの性質、誰がアクセスを許可するか • 有効な物理的、論理的アクセスコントロールを用いた未承認のアクセスの防止 • 新規ユーザーの追加、既存ユーザーのアクセスレベル変更、アクセスを必要としなくなったユーザーの削除手続 • セキュリティのための実施責任と説明責任の割当て • システム変更と維持管理に対する実施責任と説明責任の割当て • システムソフトウェアの導入、更新、パッチ • 導入前のシステム構成要素の評価、承認、テスト • セキュリティ問題に関する苦情と要求の解決に対処する方法 • エラーと欠落、セキュリティ違反と他の事件を取り扱う手続 • システムへの既遂、未遂の攻撃あるいは侵入を発見する手続および、主体的にセキュリティ手続をテストする手続（例えば、侵入テスト） • そのセキュリティポリシーを支援する訓練その他の資源の配分 • システム処理のインテグリティと関連するシステムセキュリティポリシーにおいて特定されていない例外事項および状況に対応する規定 • 災害復旧計画と関連するテスト • 適用される法規制、定義されたコミットメント、サービスレベルアグリーメントその他の契約の識別および整合性のための規定 • 個人情報のセキュリティに関する企業のプライバシーポリシーおよび手続について（初年度および年次に）ユーザー、経営者、第三者に理解の程度を確認する。 企業のセキュリティプログラムは、企業によって能動的にアクセスされる必要のなくなった、コンピュータ、メディア、紙面の個人情報へのアクセスを防止する（例 コンピュータ、メディア、紙面に保存された情報の売却、あるいは処分）。	採用された保護措置については、企業の運用の規模と複雑性のみならず、データの性質と機微の程度も考慮することがある。例えば、企業は他の情報に適用されるよりも高いレベルで個人情報その他の機微な情報を保護する場合がある。 ある種の規制（例えば、HIPAA）では、特定のセキュリティ対策を考慮し、導入するためのより高いレベルの詳細さを持つ指針を提供している。 ある種のセキュリティ規則（例えば、情報保護に関する GLBA 関連規則）では、下記の事項を要求している。 • 役員会（あるいは委員会、役員会が指名した個人）が、企業の情報セキュリティプログラムを監督承認する。 • 企業が適切なサービスプロバイダの監督において下記の合理的な手順を踏む。 -サービスプロバイダ選定に当たって適切なデューデリジェンスを実施すること。 - 課題となっている個人情報に関して適切な保護措置を導入、保持するようにサービスプロバイダに契約によって要求すること。 ある種のセキュリティ法（例えば、カリフォルニア州 SB1386）では、個人情報の保護が危殆化されたかどうか知らせることを企業に要求する。 支払カード発行者は、セキュリティおよびプライバシー要件を確立している。

プライバシーのためのセキュリティの規準	規準の例示と説明	追加的な留意事項
8.2.2 論理的アクセスコントロール 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。 • 社内要員と個人の権限付与および登録 • 社内要員と個人の識別および認証 • アクセスプロファイルの変更と更新 • システムアクセス権限と許諾の付与 • 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 • 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 • 承認された社内要員のみへの出力帳票配布 • 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 • 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 • ウイルス、悪意があるコード、未承認のソフトウェアの導入禁止	下記のシステムと手続が採用されている。 • データの機密性と個人情報にアクセスするユーザーの合理的なビジネスの必要性に基づいて、ユーザーへ提供されるアクセスの性質とレベルを確立する。 • 例えば、ユーザー名とパスワード、証明書、外部トークン、バイオメトリクスによって、ユーザーを認証する。 • 個人情報を取り扱うシステムへのアクセス権が与えられる前に、システムによって認証される正当な IDとパスワードを提供するようにユーザーに要求する。 • 追加的、あるいは動的なパスワード、コールバック管理、電子証明書、セキュア ID カード、VPN、適切に構成されたファイアウォールのような、リモートアクセスのために高度化されたセキュリティ対策を要求する。 • 侵入検知およびモニタリングシステムを導入する。	ユーザー認証プロセスにおいて、下記の事項に留意する。 • ストレージのメディアと技術プラットホームのみならず、データがアクセスされる方法（内部あるいは外部ネットワーク） • 個人情報を含む紙およびバックアップメディアへのアクセス • 実際の個人を認証する他の方法がない共有アカウントへのアクセスの拒否
8.2.3 物理的アクセスコントロール 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。	下記のシステムと手続が採用されている。 • ハードコピー、アーカイブ、バックアップコピーを含めて、個人情報への論理的、物理的アクセスを管理する。 • 個人情報へのアクセスログを取得し、モニタリングする。 • 個人情報の未承認もしくは突発的な破壊や喪失を防止する。 • 未承認のアクセスを取得する違反および試行を調査する。 • 適切に任命されたプライバシー担当役員に調査結果を伝達する。 • 個人情報を含む書類の配布を物理的に統制する。 • 機密情報を含むゴミの処分を安全に（例えば、シュレッダーで）行う。	個人情報が処理、保管されている事務所、データセンター、その他の場所へのアクセスを統制するための物理的保護措置には、施錠されたファイルキャビネット、カードアクセスシステム、物理キー、サインオン記録その他の技術を含む。
8.2.4 環境的保護措置 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。	経営者は、リスク評価に基づいて環境的要因（例えば、火災、水害、塵埃、停電、高温、高湿度）から保護する対策を保持する。企業の統制された領域は煙探知器と消火システムの両方を使って火災から保護される。二重床の中に漏水探知器が装備されている。 企業の設備は、無停電電力装置（UPS）と緊急電力装置（EPS）の両方により、処理環境の停電から守られる。この装置は半年ごとにテストされる。	

プライバシーのためのセキュリティの規準	規準の例示と説明	追加的な留意事項
8.2.5 伝送された個人情報 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。	下記のシステムと手続が採用されている。 • 情報の機密保持、伝達、インターネットあるいは他の公衆回線で伝送された個人情報の適切な保護に対処する。 • 暗号化と内部統制の最低レベルを定義する。 • 個人情報の転送、受信に対して業界標準の暗号化技術（例えば、128 ビットの SSL）を利用する。 • 外部のネットワーク接続を承認する。 • メール、運送業者、その他の物理的手段によって送られた情報を保護する。	ある種の規制（例えば、HIPAA）では、健康医療の記録（つまり、標準的な取引に関して）に関する署名の電子的転送および認証のための特別な規定がある。 いくつかのクレジットカード業者は、クレジットカードおよび取引関連データを伝送中、および保管中に暗号化技術の利用の要求を含めて、カード所有者のデータを保護するための最小限度の要求事項を公表している。 技術、市場、規制要件が進展するにつれて、認められる保護レベルに合致するために新しい対策が必要になってきている（例えば、ユーザーIDとパスワードを含む 128 ビットの SSL 暗号）。
8.2.6 セキュリティ保護措置のテスト 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。	下記のシステムと手続が採用されている。 • 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を定期的にテストする。 • 内部、あるいは外部監査人を利用してセキュリティ内部統制の独立した監査を定期的に受ける。 • 少なくとも毎年カードアクセスシステムとその他の物理的セキュリティ装置をテストする。 • 災害復旧および危機管理計画を少なくとも毎年、その現実性を保証するために文書化し、テストする。 • セキュリティ侵入レビューと Web 脆弱性および復元力を含めて、脅威および脆弱性テストを定期的に受ける。 • 実施したテストの結果、新しい、または変化している脅威と脆弱性を考慮して、セキュリティポリシーおよび手続への適切な修正を定期的に行う。	セキュリティ保護措置のテストの頻度および性質は、企業の規模と複雑性、企業活動と個人情報の機密性の性質と範囲により変化する。 ある種の規制（例えば、情報保護に関する GLBA 関連規則）では、企業に対して一定のセキュリティ保護措置を要求する。 • 独立した第三者あるいはセキュリティの開発、維持に当たるスタッフから独立した者によって重要な内部統制、システム、手続を定期的にテストする（あるいは少なくともこれらの独立した当事者がテストの結果をレビューするようにする）。 • 少なくとも毎年、情報セキュリティを評価して、できる限り調整する。

品質

品質の規準	規準の例示と説明	追加的な留意事項
9.0 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。		
9.1 ポリシーと伝達		
9.1.0 プライバシーポリシー 企業のプライバシーポリシーは個人情報の品質を扱う。		
9.1.1 個人への伝達 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、およ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。	企業のプライバシー通知は、個人情報が正確かつ、完全に維持される程度が情報の利用に依存すると説明する。 取引の完了にどの情報の提供が必要であり、どの情報の提供が任意であるかについて個人に知らせるための、正確な指示が企業によって提示される。	
9.2 手続と内部統制		

品質の規準	規準の例示と説明	追加的な留意事項
9.2.1 個人情報の正確性と完全性 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。	下記のシステムと手続が採用されている。 • 個人情報が収集、生成、保管、更新される度に誤謬摘示し、検証する。 • 個人情報の取得、更新日時を記録する。 • 個人情報が失効する時点を特定する。 • 個人情報が更新される方法と時点、更新のための情報源（例えば、保持情報の年次再確認と個人が能動的に個人情報を更新する方法）を特定する。 • 個人から直接、あるいは第三者（4.2.3「第三者からの収集」を参照）を通じて取得され、あるいは第三者（7.2.2「個人情報の保護」を参照）に開示される個人情報の正確性と完全性を確かめる方法を示す。 • 正確である必要性に明確な限界がない限り、利用中である個人情報が、十分に正確かつ、完全であることを保証する。 • 利用される目的を満たすために更新プロセスが必要でない限り、個人情報が定常的には更新されないことを保証する。 企業は、個人情報記録の正確性をチェックし、必要に応じてそれらを修正するための定期的な評価を受ける。	
9.2.2 個人情報の適切性 個人情報は、それが利用される目的にとって適切である。	下記のシステムと手続が採用されている。 • 個人情報が、それが利用される目的に対して十分に適切であり、個人についてビジネス上の意思決定をするのに不適当な情報が利用されるという可能性を最小にすることを保証する。 • 意思決定をする際に不適切なデータの利用の可能性を最小にするために、個人情報記録の適切性を定期的に評価し、必要に応じて修正する。	

モニタリングと周知徹底

モニタリングと周知徹底の規準	規準の例示と説明	追加的な留意事項
10.0 企業は、プライバシーポリシーと手続への準拠をモニタリングし、プライバシー関連の苦情と紛争を扱う手続を持っている。		
10.1 ポリシーと伝達		
10.1.0 プライバシーポリシー 企業のプライバシーポリシーは、プライバシーポリシーと手続のモニタリングと周知徹底を扱う。		
10.1.1 個人への伝達 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通知は、下記に従う。 • 個人が苦情について、どのように企業と連絡を取ることができるか記述する（例えば、企業の Web サイトの電子メールリンクあるいは電話番号）。 • 個人が苦情を提出することができる適切な連絡情報を提供する（例えば、個人または苦情処理に責任がある事務所の名前、電話番号、郵送先、電子メールアドレス）。	
10.2 手続と内部統制		
10.2.1 苦情処理 苦情に対処するプロセスが採用されている。	企業のプライバシー責任者あるいは他の指名された個人が、プライバシー関連の苦情、紛争その他の問題を扱う権限を与えられる。 下記のシステムと手続が採用されている。 • 企業に対する苦情を伝達し、解決するのに従うべき手続 • 苦情が満足に解決されるまで、問題の情報に関してとられるべき行動 • 個人情報の違反について実施可能な補償および当該情報を個人に伝達する方法 • 実施可能な調停および個人に提供可能な調停をレビューし、承認するための公式の上申プロセス • 任命された第三者紛争解決あるいは類似のサービス(提供される場合)に従うべき手続と連絡情報	

モニタリングと周知徹底の規準	規準の例示と説明	追加的な留意事項
10.2.2 紛争解決と調停 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。	企業は下記を行うための公式に文書化されたプロセスを持っている。 • タイムリーにすべての苦情を記録して対応する。 • タイムリーに解決されることを保証するために定期的に未解決の紛争と苦情をレビューする。 • 企業のプライバシーポリシーと手続を変える可能性がある趨勢と必要性を識別する。 • 解決できない苦情に対処する。 • 個人が企業の提案した解決策に満足していない場合、特定の独立した第三者紛争解決サービスあるいは、規制当局によって義務化された他のプロセス、調停を行う第三者からのコミットメントを合わせて利用する。 企業が直接解決できない苦情について第三者紛争解決プロセスを提供する場合は、個人がそのプロセスを使う方法について、説明が提供される。	ある種の規制（例えば、HIPAA および COPPA）が特定の手続と要件を持っている。
10.2.3 準拠性レビュー 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。	下記のシステムと手続が採用されている。 • 毎年、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他の契約への準拠性をレビューする。 • 定期的なレビュー文書、例えば、内部監査計画、監査報告書、準拠性チェックリスト、経営者の署名が、保持される。 • 準拠性レビューの結果と改善勧告を経営者に報告して、改善計画を実施する。 • タイムリー（すなわち、プライバシーポリシーと手続を、必要に応じて修正する）に適切な修正行動がとられることを保証するために、準拠性レビューで発見された問題と脆弱性の解決をモニタリングする。	
10.2.4 準拠性違反の例 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。	下記のシステムと手続が採用されている。 • プライバシー違反とセキュリティ脆弱性を報告する必要のある従業員にタイムリーに通知する。 • セキュリティ脆弱性とプライバシー違反を報告するために適切な従業員に通知する。 • プライバシーポリシーと手続への準拠性違反の例を文書化する。 • セキュリティ脆弱性とプライバシー違反の適切な修正処置がタイムリーにとられることを保証するために、それらの解決をモニターする。 • 企業のプライバシーポリシーおよび手続に違反した第三者による個人情報の利用または開示に起因して発生した損害を、実務的に実施可能な範囲で軽減する（例えば、影響を受ける個人に通知し、他人に開示された情報の回復を試み、口座番号を廃止して再発行する） • プライバシーポリシーと手続に修正を必要とするかもしれない趨勢を識別する。	

付録 A 用語集

関係会社	他の企業を統制する企業、統制される企業、あるいは共通の統制の下に置かれる企業。
機密保持	個人情報以外の情報やデータを未承認の開示から保護すること。
同意	企業が、プライバシー通知に従って、個人情報を収集、利用、開示するための個人による合意。このような合意は明白、あるいは暗黙であり得る。明白な同意は、口頭であるいは書面で与えられて、あいまいでなくて、同意を求めている企業の一部に推論を必要としない。暗黙の同意は、合理的に個人の作為あるいは不作為から推定されるかもしれない（オプトインおよびオプトアウトについては下記を参照）。
クッキー	クッキーは、Web サーバによって生成され、将来のアクセスに備えて、ユーザーのコンピュータに保存される小さな情報である。この情報は、ユーザーが Web サイトに戻ってきたとき、Web コンテンツの個人履歴を示し、過去の購買履歴に基づいて可能性がある興味の項目を提案するために利用することができる。ある特定の広告主は、クッキーを含めて、サイトを通じてパターンと経路を分析する追跡方法を使う。
企業	個人情報を収集、利用、保持して、開示する組織。
個人	収集される個人情報の対象となる人（時に、データサブジェクト）。
社内要員	従業員、委託先、代理人、および企業およびその関係会社のために行動している他の人たち。
オプトイン	個人の明白な同意なしでは、個人情報が企業によって収集、利用、保持、開示されないとすること。
オプトアウト	個人が明白に許諾を拒否しないなら、個人情報を収集、利用、保持、開示するために企業に暗黙の同意があるとみなすこと。
外部委託	企業のためにビジネス上の機能を発揮する第三者による、個人情報の利用および取扱い。
個人情報	個人の同一性を識別できる情報あるいはそうでありうる情報。
ポリシー	経営者の意図、目標、要求事項、実施責任あるいは基準を伝達する書面の記述書。
プライバシー	個人情報の収集、利用、開示、保持に関する個人および企業の権利義務。
プライバシー違反	企業のポリシーや適用されるプライバシー法規の規定に準拠しない方法で個人情報が収集、保持、アクセス、利用、開示される場合にプライバシー違反は起こる。
プライバシープログラム	一般に公正妥当と認められた プライバシー原則と規準に準拠して、個人情報を管理し、保護するために採用されたポリシー、伝達、手続、内部統制。
目的	個人情報が企業によって収集される理由。
機微な個人情報	例えば、医療あるいは健康状態、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、性生活、犯罪歴、違反歴を含む情報のような、高い水準の保護、高い注意義務を要求される個人情報。
第三者	個人情報を収集する企業と提携していない企業、あるいは企業のプライバシー通知の対象となっていない提携先企業。
Web ビーコン	Web ビーコンは、Web バグとしても知られていて、データを転送するために、Web ページあるいは電子メールメッセージで写実的なイメージを配信するための方法を提供するコードの小さいストリングである。企業では、サイトトラフィック報告、ユニークなビジターカウント、広告および電子メールの監査報告と個人化を含めて、多くの目的のために Web ビーコンを使う。例えば、Web ビーコンがユーザーの IP アドレス、リファラーを収集し、ユーザーが訪問したサイトを追跡することができる。

付録 B　プライバシー概念の国際比較

下記の表は、一般に公正妥当と認められたプライバシー原則に関わる、国際的なプライバシー規制、法律、指針で提示されたプライバシー概念の比較を提供する。これは、例示が目的であって、包括的であることを意図しない。最初の列は、一般に公正妥当と認められたプライバシー原則の 10 原則である。2～9 番目の列は、特定の法規制において検討される重要な原則である。次頁（各列のキーワードについての出典）には、比較される各法律や規則の情報源を識別している。

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Generally Accepted Privacy Principles	Australia Privacy Act	Canada PIPEDA	E.U. Directive	OECD Guidelines	U.S. FTC	U.S. Safe Harbor	U.S. HIPAA	U.S. GLBA
Management		Accountability	Notification	Accountability			Administrative requirements	
Notice	Openness	Identifying Purposes, Openness	Information to be Given to the Data Subject	Purpose Specification, Openness	Notice	Notice	Notice	Privacy and Opt Out Notices, Exceptions
Choice and Consent	Use and Disclosure	Consent	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Collection Limitation	Choice	Choice	Consent, Uses and Disclosures	Privacy and Opt Out Notices
Collection	Collection, Sensitive Information, Anonymity	Limiting Collection	Principles Relating to Data Quality, Exemptions and Restrictions	Collection (including consent) Limitation		Data Integrity		
Use and Retention	Identifiers, Use and Disclosure	Limiting Use, Disclosure, and Retention	Making Data Processing Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object	Use Limitation (including disclosure limitation)		(implied but not specified in the principles)	Uses and Disclosures	Limits on Disclosures
Access	Access and Correction	Individual Access	The Data Subject's Right of Access to Data	Individual Participation		Access	Access	
Disclosure to Third Parties	Use and Disclosure, Transborder Data Flows	Limiting Use, Disclosure, and Retention	Transfer of Personal Data to Third Countries	Use Limitation (including disclosure limitation)		Onward Transfer	Uses and Disclosures, Accounting of Disclosures	Limits on Disclosures
Security for Privacy	Data Security	Safeguards	Confidentiality and Security of Processing	Security Safeguards	Security	Security	Security Rule	Security Guidelines mandated by section 501(b) of GLBA
Quality	Data Quality	Accuracy	Principles Relating to Data Quality	Data Quality	Integrity	Data Integrity	Amendment	
Monitoring and Enforcement	Enforcement by the Office of the Privacy Commissioner	Challenging Compliance	Judicial Remedies, Liability and Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data	Individual Participation (including challenging compliance)	Enforcement	Enforcement	Compliance and Enforcement by the Department of Health and Human Services	Enforcement by financial services industry regulators, the FTC and SEC

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
一般に公正妥当と認められたプライバシー原則	豪州 プライバシー法	カナダ PIPEDA	EU 指令	OECD 指針	合衆国 FTC	合衆国 セーフハーバー原則	合衆国 HIPAA	合衆国 GLBA
管理		説明責任	通告	説明責任			管理上の要求事項	
通知	公開	● 目的の識別 ● 公開	データサブジェクトに与えられる情報	● 目的の特定 ● 公開	通知	通知	通知	● プライバシーおよびオプトアウト通知 ● 例外事項
選択と同意	利用と開示	同意	● 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	選択	選択	● 同意 ● 利用と開示	プライバシーおよびオプトアウト通知
収集	● 収集 ● 機微な情報 ● 匿名性	収集の制限	● データの品質に関する原則 ● 免除および制限	収集（同意を含む）制限		データのインテグリティ		
利用と保持	● 識別子 ● 利用と開示	利用、開示、保持の制限	● 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 ● 免除および制限 ● 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）		（暗示されているが原則で明確化されていない）	利用と開示	開示の制限
アクセス	アクセスと訂正	個人のアクセス	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	アクセス	
第三者への開示	● 利用と開示 ● 国境を越えたデータフロー	利用、開示、保持の制限	● 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）		拡散的な転送	● 利用と開示 ● 開示の説明	開示の制限
プライバシーのためのセキュリティ	データセキュリティ	安全保護措置	処理の機密保持およびセキュリティ	セキュリティ安全保護措置	セキュリティ	セキュリティ	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
品質	データの品質	正確性	データの品質に関する原則	データの品質	インテグリティ	データのインテグリティ	修正	
モニタリングと周知徹底	プライバシーコミッショナー事務局による周知徹底	法令遵守の難しさ	● 裁判上の救済 ● 義務および許可 ● 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（法令遵守の難しさを含む）	周知徹底	周知徹底	保険福祉省による遵守および徹底	金融サービス産業規制当局、FTC、SEC による周知徹底

各列のキーワードについての出典
(1) AICPA/CICA Generally Accepted Privacy Principles, May 2006.
(2) Australia Privacy Act 1988, Privacy Act 1988, as amended, effective December 21, 2001.
(3) Canada Personal Information Protection and Electronic Documents Act (PIPEDA), also referred to as. Bill C-6, Second Session, Thirty-sixth Parliament, 48-49 Elizabeth II, 1999-2000, assented to April 13, 2000, effective January 1, 2001.
(4) EU Directive, European Union (EU), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, October 24, 1995, effective October 25, 1998, as implemented in EU country specific laws and regulations.
(5) OECD Guidelines, Organization for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, September 23, 1980.
(6) U.S. FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, United States (U.S.) Federal Trade Commission (FTC), May 2000.
(7) U.S. Safe Harbor, an agreement between the U.S. Department of Commerce and the European Commission's Internal Market Directorate, approved by the European Commission July 27, 2000, open for use November 1, 2000.
(8) U.S. United States Health Insurance Portability and Accountability Act of 1996 (HIPAA), Privacy Rule (compliance deadline April 16, 2003), Security Rule (compliance deadline April 21, 2005).
(9) U.S. Financial Services Modernization Act, also referred to as the Gramm-Leach-Bliley Act (GLBA), Title V – Privacy, Subtitle A, enacted November 12, 1999, effective November 13, 2000, Compliance by July 1, 2001. The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision (collectively, the Agencies) published final Guidelines establishing standards for safeguarding customer information that implement sections 501 and 505(b) of GLBA.

付録 C 一般に公正妥当と認められたプライバシー原則を利用した公認会計士の検証責任者サービス

この付録は、一般に公正妥当と認められたプライバシー原則を利用することでハイレベルな公共実務における公認会計士(検証責任者)が提供できるサービスの概要を提供する。「プライバシーサービスの理解と導入－公認会計士のリソース」における詳細な指針は、特別委員会によって開発され、AICPA と CICA の両方から利用可能である(www.aicpa.org/privacy と www.cica.ca を参照)。この詳細な指針は、この付録で検討したサービスを提供する検証責任者にとって、不可欠のリソースである。

プライバシー助言業務

検証責任者は、一般に公正妥当と認められたプライバシー原則の規準を利用することで、戦略策定、診断、導入、維持管理を含む多様な助言サービスを提供できる。これらのサービスには、ベンチマークとして一般に公正妥当と認められたプライバシー原則の規準を利用した、例えば、システムの弱点に関するクライアントへの助言、リスク評価、活動計画に対する改善勧告等を含む。

そのような助言サービスを提供する合衆国の検証責任者は、コンサルティングサービスの基準、すなわちコンサルティングサービス基準書に従う。定義と基準(AICPA 職業的基準第 2 号、CS セクション 100)である。

プライバシー保証業務

プライバシー保証業務は、定義されたプライバシー関連の主題または記述書に関して検証責任者が行う下記のサービスを含んでいる。

- (検証)意見の表明。
- レビューの実施。
- 合衆国では、合意された手続の実施。

プライバシー検証業務

証明業務関連の米国基準は、証明サービス基準書に含まれている。プライバシー保証業務は、この基準の中で定義されている。検証責任者が関連する職業的基準によって確立された要件を意識していることが期待されている。

保証業務では、検証責任者は高水準だが、絶対的でない水準の保証を、主題または記述書に提供する。その目的で、検証責任者は、検証責任者の専門的な判断力で検証責任者が不適切な結論に達するリスクを低水準に減少させる検証手続を開発する。プライバシー検証報告書の文例は付録 D に示されている。

下記の主要な概念が、プライバシー保証業務（注 2）に適用される。

- 通常、プライバシー保証報告書は 10 原則全てを対象とする。無限定報告書（注 3）（注 4）を発行するためには、検証対象期間を通じて、当該関連規準のすべてに適合している必要がある。
- 作業は、保証の最高水準である「検証」もしくは同等の水準で実施されるべきである。
- 業務の範囲は、(1) すべての個人情報でもよいし、特定の種類の顧客情報または従業員情報などの個人情報でもよく、(2)企業全体の事業領域・所在地でもよいし、特定の事業領域(小売活動を指す。製造活動または企業の Web サイトで生成される小売活動だけでは不可)、もしくは、地理的な場所(カナダの活動のみなどの)でもよい。

さらに下記の概念が適用される。
o 一般に、業務の範囲がプライバシー通知で対象とされる企業および活動の記述と一致しているべきであり、(規準 2.2.2 を参照) 関連するプライバシー通知で対象としたものより狭い場合が多く、通常広くなることはない。
o 業務の範囲は、「情報サイクル」の関連する個人情報のための活動のすべてを含むべきである。これらには収集、利用、保持、開示、廃棄、個人識別不能化、匿名化を含むべきである。検証報告書の利用者にとって、この全体のサイクルを含んでいない領域を定義することは判断を誤らせることになりやすい。
o 業務の範囲にないが、検証の範囲に含まれていた特定の個人情報が混ざっている場合、プライバシー保証業務は、混ざっていた情報のすべての内部統制を対象とする必要がある。
o 通常、検証報告書は特定期間対象(少なくとも 2 カ月)であるべきだが、検証責任者の初度報告書は特定時点対象報告書とすることができる。

プライバシーレビュー業務

職業的基準の下では、レビュー業務は保証業務の一形態である。しかしながら、「プライバシーレビュー」という用語は、プライバシー診断業務のような、プライバシー検証、または、ある種のプライバシー助言業務の意味としてしばしば誤用されている。職業的基準で定義されるレビュー業務は、第三者利用者に誤解されやすいため、プライバシー特別委員会は、当該用語の使用を推奨しない。

合意された手続業務

合意された手続業務では、検証責任者は、当事者（注 5）によって合意された手続を実施して、当該当事者の調査結果を報告する。検証責任者は、記述書または主題の検証やレビューを実施せず、意見を述べず、または記述書や主題に関する消極的保証を提供しない。検証報告書は、手続と調査結果の記述の様式である。一般に公正妥当と認められたプライバシー原則が当該業務に利用される場合がある。この種の業務は、保証報告書に導くのではなく、むしろ合意された手続と対応する調査結果を提示する報告書に導く。企業のシステムの一部分に比例して一般に公正妥当と認められたプライバシー原則の一部分に関して合意された手続を受嘱することができる。例えば、企業は、検証責任者が一般に公正妥当と認められたプライバシー原則の一部分を利用することで、合意された手続を完了し、調査結果を報告することを依頼する場合がある。

利用者ニーズのばらつきが大きいため、合意された手続の性質、タイミング、範囲は異なる場合がある。その結果、彼らが自身の必要性を特に理解しているため、報告書の当事者(合意された利用者とクライアント)は手続の十分性に対する責任を負う。当該報告書の利用は手続に合意した特定の当事者に制限される。

一般に公正妥当と認められたプライバシー原則と Trust サービス原則と規準との関係

一般に公正妥当と認められたプライバシー原則は、AICPA/CICA Trust サービス原則と規準（共通のフレームワーク(すなわち、原則と規準のコアセット)に基づく一連の職業的保証および助言サービス）の一部である。Trust サービスの原則と規準は米国公認会計士協会(AICPA)とカナダ勅許会計士協会(CICA)の無償の特別委員会によって策定された。AICPA と CICA は本研究資料では「協会」と呼ばれる。その他の Trust サービスの原則と規準は下記のとおりである。

- **セキュリティ**：システムが（物理的、論理的双方の）未承認のアクセスから保護されている。

- **可用性**：システムは、約束あるいは合意したとおりに、運用、利用のために利用可能である。
- **処理のインテグリティ**：システム処理は完全で、正確で、タイムリーで、承認されている。
- **機密保持**：機密と指定された情報が、約束あるいは合意したとおりに、保護されている。

上記は、http://www.webtrust.org で、より詳細に検討されている。「Trust サービスの理解、導入」という Trust サービスに関する追加情報が一連の指針となっている。(AICPA と CICA から利用可能)。

オンラインプライバシー業務

オンライン領域に関わるプライバシー業務の場合、企業は、WebTrust オンラインプライバシーシールの表示を選択してもよい。これらの業務については、下記のようである必要がある。

- 業務の範囲として、企業のオンラインビジネス領域が含まれており、それに限定されないこと。WebTrust シールの利用は、オンラインビジネス領域が検証責任者の検証範囲に含まれている場合に限って許容される。
- WebTrust シールが商標登録され、サービスマーク登録された画像イメージであり、それらの利用は Trust サービスのライセンス合意の対象であること。Trust サービスプログラムのために確立されたライセンス合意及び指針は、クライアントの Web サイト上に表示されるイメージを許可しており、下記の要件に従う。
  - 検証責任者が、Trust サービスライセンス合意において、ライセンスを受けなければならないこと
  - 企業が、検証責任者から限定や範囲の限定を含まない報告書を収受せねばならないこと
  - 企業が、(通常、検証責任者の契約書に含まれる) WebTrust シールの使用法を規定する条項に合意しなければならないこと
  - シールが、AICPA/CICA のプロセスを通じて発行され、協会のサーバに置かれなければならないこと
  - シール利用料が、Trust サービスライセンス合意で確立されたとおりに協会に支払われること

WebTrust シールを利用する場合、特別委員会は、検証報告書に下記のような文言を含めることを推奨する。「WebTrust オンラインプライバシーシールは、独立した検証責任者の報告書の内容を象徴的に表示しているのであり、報告書を更新し、あるいは何らかの追加的な保証を提供するように解釈されるべきではない」。

付録 D　プライバシー検証報告書の文例

以下の付録には、職業的報告基準の下での検証報告書の文例が含まれている。

AICPA 証明基準が適用される場合
文例 1－AICPA 証明基準の下での主題に対する直接意見表明
文例 2－AICPA 証明基準の下での経営者記述書に対する意見表明
経営者の記述書の文例

文例 1－AICPA 証明基準の下での主題に対する直接意見表明

独立した検証責任者のプライバシー検証報告書

ABC社　代表取締役　殿

当監査法人は、2006年○月○日から2006年○月○日の間のABC社の、(1)プライバシー通知におけるコミットメント及びAICPA/CICA　一般に公正妥当と認められたプライバシー原則に定められた規準に基づいて、個人情報が収集、利用、保持、開示されているという合理的な保証を提供するための○○事業（例えば「メールオーダーカタログ販売事業」というように対象とする企業及び活動を記述）に関する内部統制の有効性を検証し、(2)当該事業に関するプライバシー通知におけるコミットメントへの準拠性を検証した。これらの内部統制の有効性及び当該コミットメントへの準拠性はABC社の経営者の責任である。当監査法人の責任は当監査法人の検証に基づいて、意見を表明することである。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に従って行われた。それには、(1) ABC社の個人情報のプライバシーに関する内部統制についての理解 (2) 内部統制の運用状況の有効性についてのテスト及び評価 (3) プライバシー通知における企業のコミットメントへの準拠性についてのテスト(4)当監査法人が状況に応じて必要と認めたその他の手続の実施が含まれる。当監査法人は当監査法人の検証が当監査法人の意見に合理的な基礎を提供すると信じる。

当監査法人の意見では、2006年○月○日から2006年○月○日の間にABC社は、(1)プライバシー通知及び一般に公正妥当と認められたプライバシー原則に定められた規準におけるコミットメントに基づいて、個人情報が収集、利用、保持、開示されているという合理的な保証を提供するための当該事業に関する有効な内部統制を保持していた。(2)プライバシー通知におけるコミットメントに準拠していた。

内部統制の固有の限界のため、誤り又は不正が発生し、それらが発見されないことがある。さらに、当監査法人の発見事項に基づいたどんな結論の予測でも、将来の時期にはシステムもしくは内部統制に対する変更、必要な変更のの懈怠、内部統制の有効性程度の悪化により、当該結論の正当性が変更される可能性がある。

［監査法人名］
○○○○監査法人
［住所］
［日付］

文例 2－AICPA 証明基準の下での経営者記述書に対する意見表明

独立した検証責任者のプライバシー検証報告書

ABC社　代表取締役　殿

当監査法人は2006年○月○日から2006年○月○日の間のABC社の経営者記述書の下記の事項について検証した。

- プライバシー通知及びAICPA/CICA　一般に公正妥当と認められたプライバシー原則に定められた規準及び事業に関連するコミットメントに基づいて、個人情報が収集、利用、保持、開示されているという合理的な保証を提供するための○○事業（例えば「メールオーダーカタログ販売事業」というように対象とする企業及び活動を記述）に関する有効な内部統制が保持されていた。
- プライバシー通知におけるコミットメントに準拠していた。

この記述書はABC社の経営者の責任である。当監査法人の責任は当監査法人の検証に基づいて、意見を表明することである。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に従って行われた。それには(1) ABC社の個人情報のプライバシーに関する内部統制についての理解 (2) 内部統制の運用状況の有効性についてのテスト及び評価 (3) プライバシー通知における企業のコミットメントへの準拠性についてのテスト(4)当監査法人が状況に応じて必要と認めたその他の手続の実施が含まれる。当監査法人は当監査法人の検証が当監査法人の意見に合理的な基礎を提供すると信じる。

当監査法人の意見では、2006年○月○日から2006年○月○日の間にABC社の経営者の記述書は、下記の事項について、すべての重要な点において適正に表示しているものと認める。

- 事業に関連するプライバシー通知におけるコミットメント及びAICPA/CICA　一般に公正妥当と認められたプライバシー原則に定められた規準に基づいて、個人情報が収集、利用、保持、開示されているという合理的な保証を提供するための当該事業に関する有効な内部統制を保持していた。
- プライバシー通知におけるコミットメントに準拠していた。

又は

当監査法人の意見では、上記のABC社の経営者の記述書は、ABC社のプライバシー通知及びAICPA/CICA　一般に公正妥当と認められたプライバシー原則に定められた規準に基づいて、すべての重要な点において適正に表示しているものと認める。

内部統制の固有の限界のため、誤り又は不正が発生し、それらが発見されないことがある。さらに、当監査法人の発見事項に基づいたどんな結論の予測でも、将来の時期にはシステムもしくは内部統制に対する変更、必要な変更の懈怠、内部統制の有効性の程度の悪化により、当該結論の正当性が変更される可能性がある。

［監査法人名］

○○○○監査法人
［住所］
［日付］

経営者記述書の文例

2006 年○月○日から 2006 年○月○日の間に、ABC 社は、すべての重要な側面において下記の事項を実施した。

- 事業に関連するプライバシー通知におけるコミットメント及びAICPA/CICA 一般に公正妥当と認められたプライバシー原則に定められた規準に基づいて、個人情報が収集、利用、保持、開示されているという合理的な保証を提供するための○○事業（例えば「メールオーダーカタログ販売事業」というように対象とする企業及び活動を記述）に関する有効な内部統制を保持していた。
- プライバシー通知におけるコミットメントに準拠していた。

注 1 例えば、経済協力開発機構（OECD）は個人データのプライバシー保護と国境を超えた個人データ交換指針、欧州連合(EU)はデータプライバシー指令（指令 95/46/EC）を示した。さらに、合衆国は Gramm-Leach-Bliley 法（GLBA）、医療保険の携行性と責任に関する法律（HIPAA）と児童オンラインプライバシー保護法（COPPA）を制定した。カナダは個人情報保護と電子文書法（PIPEDA）を、豪州は 1988 年の豪州プライバシー法を制定し、2001 年に改正した。これらのプライバシー法規の Web サイト URL は、付録 B に提示している。これらの法規および一般に公正妥当と認められたプライバシー原則と規準への準拠性は、適用されるプライバシー法規制への準拠を結果としてもたらす必要は必ずしもないため、企業は法規制に対する法令順守に関して適切な法律的助言を求めてもよい。

注 2.「プライバシーサービスの理解と実施－CPA のリソース」という AICPA 指針の第 10 章「今日のプライバシー問題のための解決策」には、プライバシー保証業務を実施する際の指針が含まれている。

注 3. 付録 D 「プライバシー検証報告書の文例」を参照。

注 4. 特定の状況（TPSP に関する意見表明のような）では、10 のプライバシー原則の幾つかを対象とする特殊目的のプライバシー報告書が発行される場合がある。プライバシー特別委員会は、当該報告書において、対象としていないプライバシー原則がプライバシー全般にわたって不可欠であり、「利用を制限」されているといった文言を含めることを推奨する。

注 5. 特定された報告書利用者と検証責任者は、検証責任者によって実施される手続に合意する。