ＩＴ委員会研究資料第７号

Trust サービス原則、規準及びその例示

（セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る適合する Trust サービス原則、規準及びその例示の 2009 年版の更新）

平成28年 4 月18日
日本公認会計士協会

セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る適合する Trust サービス原則、規準及びその例示の 2009 年版（TSP セクション 100A）の更新である。プライバシー規準は付録Ｃで提供されている。その規準は、TSP セクション 100A の付録Ｄに詳しく説明されているものと同じ規準である。 現在、プライバシー規準は改訂中である。TSP セクション 100 の規準は、2014 年 12 月 15 日以降終了する期間において適用される。それ以前の適用を妨げない。TSP セクション 100A は 2016 年 3 月 31 日まで更新された文書として有効である。業務実施者は、報告書と確認書に使用した規準のセットがどれであったかを特定する必要がある。

（訳者注：「原則、規準、内部統制及びリスク」において、“management”は「経営者」と翻訳している。利用に際しては、組織の規模、形態や管理手法に応じて、業務実施者が適切に読み替えることを期待する。）

目次

セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る Trust サービス原則及び規準

はじめに

１．AICPA アシュアランスサービス・エグゼクティブコミッティー（ASEC）は、システムのセキュリティ、可用性及び処理のインテグリティ、並びにシステムによって処理される情報の機密保持とプライバシーに関連する内部統制を評価する際に使用する一連の原則と規準（Trust サービス原則と規準）を開発した。本文書では、システムは、経営者の特定した要求事項に従って特定の経営目標（例えば、サービスの提供、製品の生産）を達成するために、デザインされ、導入され、運用される。システム構成要素は、以下の五つのカテゴリーに分類できる。

- システム基盤：物理的構造物、ＩＴ及びその他のハードウェア（例えば、設備、コンピュータ、機器、携帯端末及び通信ネットワーク）
- ソフトウェア：アプリケーション・プログラムとそれをサポートするＩＴシステム・ソフトウェア（オペレーティング・システム、ミドルウエア及びユーティリティ）
- 要員：システムのガバナンス、運用及び利用に関与する要員（開発者、運用担当者、企業ユーザー、外注業者及び管理者）
- プロセス：自動又は手動の手続
- データ：システムにより利用又は処理された、取引の流れ、ファイル、データベース、テーブル及び出力

２．本書は、システムのセキュリティ、可用性及び処理のインテグリティ、並びにシステムによって処理される情報の機密保持とプライバシーに関連する内部統制の有効性を評価する Trust サービス原則と規準を提供する。企業の経営者は、システムの内部統制を評価する際に原則と規準を利用し、又は内部統制に関連する報告やコンサルタント業務の提供を受けるために、公認会計士と契約することができる。

３．証明業務に関する AICPA の基準書（一般に証明基準と言われる。）の下で実行される証明サービスは、検証、レビュー[1]及び合意された手続業務を含んでいる。証明基準では、証明業務を実施する公認会計士は、業務実施者として知られている。検証業務では、特定された一連の規準と関連して、主題又は主題に関する記述書について意

[1] 一般に、レビュー業務は中程度の保証の水準(すなわち、消極的保証)を提供するように設計され、質問と分析的手続の実施から構成される。しかしながら、アシュアランスサービス・エグゼクティブコミッティーは、業務実施者が通常、特定の法律、規制、規則、契約又は助成金の要求事項である企業の内部統制やコンプライアンスについて意味のある分析的手続を実施できていないと考えており、また、レビュー業務を基礎として質問の手続と統合して実施する他の手続を特定できるか不確実である。また、この不確実性のため、業務実施者の手続の性質と範囲に関する誤解により、レビュー報告書のユーザーは、より大きなリスクにさらされる。したがって、Trust サービスに関連するレビュー業務の実現可能性は不確実である。

見を表明する報告書を業務実施者は提供する。例えば、システムの内部統制が処理のインテグリティと機密保持に関する Trust サービス規準を満たすために有効に運用されていたかどうかに関して業務実施者は報告することができる。合意された手続業務では、業務実施者は、意見を表明することなく、特定の関係者と合意した手続を実施し、その結果を報告する。検証業務は、証明基準の AT セクション 101、証明業務に準拠して実施され、そして、合意された手続業務は、AT セクション 201、合意された手続業務に従って実施される（AICPA、職業的基準)。

4．以下は、業務実施者が、Trust サービス原則と規準を使用して検証・報告することができる主題の種類である。

- 一つ又は複数の Trust サービス原則（セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシー）に関する受託会社のシステムの内部統制のデザインと運用の有効性（SOC3 業務)
- 一つ又は複数の Trust サービス原則（セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシー）に関して記載した受託会社のシステムの記述書の表示の適正性。これには、AICPA「受託会社のセキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関する内部統制の報告ガイド」(SOC2）のパラグラフ 1.34 の記述書の規準を、プライバシー原則の場合は更にパラグラフ 1.35 を加えて使用する。タイプ１の報告書は、Trust サービス規準を充足するような内部統制のデザインの適切性。そして、タイプ２の報告書は、Trust サービス規準を充足するように特定の期間における内部統制の運用の有効性（SOC2 業務)。
- 一つ又は複数の Trust サービス原則（セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシー)に関する企業のシステムにおける関連する Trust サービス規準を充足するような内部統制のデザインの適切性（通常、この業務はシステムの導入前に実行される。）

5．個別のユーザー企業に提供する企業のサービスの性質と範囲は、ユーザー企業のニーズに大きく依存するため異なることがある。例えば、毎月のニュースレターのためにウェブサイトを使用する組織のデータセンターホスティングサービスの可用性は、証券会社よりもはるかに限られたニーズである。当該組織は、ニュースレターが利用できない１日の僅かな不便のみを受ける。ところが、証券会社は、システムが 15 分使用できないだけで莫大な赤字を蒙るかもしれない。一般に、そのようなユーザー要求は、契約書、サービスレベルアグリーメント、又は声明書（例えば、プライバシー通知）に基づく経営者の宣言に記述される。これらの経営者の宣言は、Trust サービス原則と規準のコミットメントとして参照される。経営者の経営目標、コミットメント及び義務（例えば、法律や規則）を満たすことを可能にするために、どうシステムが機能すべきかに関する仕様は、Trust サービス原則と規準における要求事項として参照される。例えば、セキュリティ要求事項は、セキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシーに関連する経営者のコミットメントから生じ

るかもしれない。

コミットメントと要求事項は、企業が内部統制を導入する目的であり、その結果、Trust サービス規準の目的でもある。したがって、Trust サービス規準の多くがコミットメントと要求事項を参照する。例えば、「企業は、従業員行動規範を確立し、従業員選考手続（バックグランドチェックを含む。）を導入し、そして[セキュリティ、可用性、処理のインテグリティ又は機密保持のうち該当するものを選択]に関するコミットメントと要求事項を充足する手続を実施する。」。業務実施者がコミットメントと要求事項の遵守か達成について意見を表明する業務では、それらは規準として機能する。

6．経営者は、そのコミットメントと要求事項を遵守し、記録を維持する責任がある。コミットメントと要求事項を特定する際、経営者は、特定の業務のために、何がそのコミットメントと要求事項を構成しているかについて確認書で特定すべきである。例えば、

- 文書による顧客契約に含まれている義務
- 広範な利用者に提供されているサービス以外に、特定の顧客に対してなされた特別なコミットメントに伴うプロセスや、内部統制の追加を除く、全ての顧客に適用される基本となる義務

さらに、Trust サービス業務は、報告対象となる原則について法令、ルール、契約及び合意書に対する企業の遵守状況や遵守に関する内部統制について、業務実施者に報告を求めていない。もし、業務実施者が、企業の内部統制の運用の有効性に関する報告（例えば、SOC3 のプライバシー業務）と併せて、法令、ルール、契約及び合意書の遵守状況の報告に関する契約をした場合、その業務は、AT セクション 601、遵守証明（AICPA、職業的基準）に準拠して実行される。

7．コンサルティング業務には、企業の経営者の意思決定のため検討及び使用される検出事項及び推奨項目の提供が含まれる。業務実施者は、この業務の主題に対して、意見の表明や結論の形成をしない。

一般に、作業はクライアントの利用と便益のためだけに実行される。この業務を提供する業務実施者は、CS セクション 100、コンサルティング業務：定義と基準（AICPA、職業的基準）に従う。

原則、規準、内部統制及びリスク

8．Trust サービス原則は、経営者の目的の達成を支援するシステムの属性を表す。

9．それぞれの原則について、主題を測定し、表示するために利用される、及び業務実施者が主題を評価することに対してベンチマークとして有用で詳細な規準がある。適

切な規準の属性は以下の通りである。

- 客観性：規準に、偏向があってはならない。
- 測定可能性：規準は、主題について、定性的又は定量的に合理的で一貫した尺度を許容せねばならない。
- 完全性：規準は、主題についての意見を覆しかねない関連要因を見逃さないように、十分に完全なものでなければならない。
- 関連性：規準は、主題に関連していなければならない。

10. ASEC は、各原則の Trust サービス規準には、適合する規準の属性の全てを含む共通基準があると結論を下した。適合することに加えて、AT セクション 101 は、業務実施者の報告書の利用者にとって、規準が利用可能であることを示す。原則と規準の公表は、その規準をユーザーにとって利用可能にする。

11. Trust サービス原則と規準は、ユーザーと経営者の目的の達成を可能にするように柔軟に設計されている。したがって、業務実施者は、一つの原則、複数の原則又は全ての原則に関連する業務を実施するかもしれない。

12. システムを運用する環境、すなわちシステムを運用する企業のコミットメント、合意書及び責任は、システム構成の性質と同様に、規準が充足されないリスクをもたらす。有効に作動するならば、規準を充足する合理的な保証を提供するよう適切にデザインされた内部統制の導入を通じて、これらのリスクは対処される。なぜなら、各システムとそれを運用する環境は一意であり、リスクと対応する規準及びリスクに対処するために必要な内部統制の組合せも一意になる。システムのデザインと運用の一部として、企業の経営者は、規準が満たされない特定のリスクとそれらのリスクに対処するために必要な内部統制を特定する必要がある。付録Ｂは、規準を満たすことを妨げるリスク及びそれらのリスクに対処するための内部統制の具体例を提供する。それらの具体例は、どのような企業にも適切であること、規準に対応するリスクやそれらのリスクに対処するために必要な内部統制の全てを含むことを意図していない。

Trust サービス原則

13. Trust サービス原則は以下のとおりある。 [2]
    a. セキュリティ：システムは未承認のアクセス、利用又は変更に対して保護されている。

[2] SysTrust、SysTrust for Service Organizations 及び WebTrust は、Trust サービス原則と規準に基づいて、AICPA 及びカナダ勅許会計士協会（CICA）によって開発された特定の商標を付けられた保証サービスの提供である。業務実施者が、これらの登録されたサービスマークを使用するには、CICA のライセンスを受けなければならない。サービスマークは、適正意見を表明する業務についてのみ発行できる。 ライセンスの詳しい情報に関しては、www.webtrust.org/を参照。
（訳者注）カナダ勅許会計士協会（CICA）は、2013 年４月１日にカナダ国内の他の会計士団体と統合して、カナダ勅許職業会計士協会（Chartered Professional Accountants of Canada）となっている。

セキュリティ原則は、セキュリティ、可用性、処理のインテグリティ及び機密保持に関する経営者のコミットメント及び要求事項の達成を支援するため、論理的及び物理的アクセス管理を通じてシステム資源を保護することを意味する。システムのセキュリティの内部統制は、職務の分離の無効化と回避、システム障害、不正確な処理、データ又はシステム資源の窃取や不正な持ち出し、ソフトウェアの不正使用及び情報への不適切なアクセス、利用、変更、破壊や開示を予防又は発見する。

b. 可用性：システムは、コミット又は合意したとおりに操作でき、かつ利用できる。

可用性原則は、契約、SLA やその他の合意書でコミットした、システム、プロダクト又はサービスのアクセシビリティを意味する。この原則自身は、システム可用性について、最小限受容できるパフォーマンスレベルを設定するものではない。可用性原則は、システム機能性（システムが実施する特定の機能）やシステム・ユーザビリティ（特定のタスク又は問題の処理にシステムの機能を適用するユーザーの能力）は扱わないが、運用、モニタリング及び維持のためのシステムの利用可能性を支援する内部統制を含むかどうかを取り扱う。

c. 処理のインテグリティ：システム処理は完全、正当、正確、タイムリー、かつ承認されている。

処理のインテグリティ原則は、システム処理の完全性、正当性、正確性、適時性と承認について言及する。処理のインテグリティは、そのシステムが存在する目標や目的を達成すること、及び未承認や不注意な操作から解放されて、意図された機能を損なわれないように実行できることを扱う。処理のインテグリティは、システムによって受け取られ、保存された情報が完全に、正当に、正確に、適時に承認されている事を、自動的には示さない。システムは多くの場合、データの入力前にシステム統制により対処することができないリスクがあり、また、そのような誤りを検出することは企業（受託会社）の責任ではない。同様に、システム境界外のユーザーは、処理を開始することに関して責任があるかもしれない。これらの例として、システム処理のインテグリティが保たれても、データが正当でなかったり、不正確だったり、また、そうでなければ不適当であるかもしれない。

d. 機密保持：機密とされた情報が、コミット又は合意したとおりに、保護されている。

機密保持原則は、企業のコミットメント及び要求事項により機密とされた情報を、システムから最終的に廃棄又は除外されるまで保護するシステムの能力について言及する。情報の受託者に、法令、受託者自身の言明、コミットメント又は他の合意書により、アクセス、利用及び保持を限定し、そして、開示は指定された範囲の人員又は組織に制限する義務がある場合（それ以外のシステムの境界内でアクセスを認可された人員等を含む。）、情報は機密となる。情報を機密とする必要性は、多くの異なった理由に起因する。例えば、専有情報、企業の担当者のみを対象とする

情報、パーソナル・インフォメーション、又は漏れたら困る情報などがある。機密保持は、プライバシーとは区別され、(i)プライバシーがパーソナル・インフォメーションに対処するのに対し、機密保持はパーソナル・インフォメーションに制限されないで、より広い範囲について言及し、そして、(ii)プライバシーはパーソナル・インフォメーションの処置、処理及び取扱いの要求事項に対処する。

e. プライバシー：

プライバシー原則はAICPAとカナダ勅許会計士協会（CICA）の発行した、一般に公正妥当と認められたプライバシー原則（GAPP）に記載された規準と、企業のプライバシー通知に準拠したシステムにおけるパーソナル・インフォメーション[3]の収集、利用、保持、開示及び廃棄について言及する（付録C「一般に公正妥当と認められたプライバシー原則」を参照)。GAPPは、Trustサービスのプライバシー原則の測定する規準を含む管理フレームワークである。GAPPは10個の要素から構成される。

i.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。

ii.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、パーソナル・インフォメーションが、収集、利用、保持、開示される目的を特定する。

iii.選択と同意：企業は、個人にとって可能な選択を記述し、パーソナル・インフォメーションの収集、利用、開示に関して黙示又は明示の同意を得る。

iv.収集：企業は、通知で特定した目的のためだけにパーソナル・インフォメーションを収集する。

v.利用、保持及び廃棄：企業は、パーソナル・インフォメーションの利用を通知で特定された目的、及び個人が黙示又は明示の同意をした目的のみに制限する。企業は、これらの目的を満たすため、又は法令によって必要である限りにおいてパーソナル・インフォメーションを保持し、その後、適切に廃棄する。

vi.アクセス：企業は、個人に対して、レビューと更新のためにパーソナル・インフォメーションへのアクセスを提供する。

vii.第三者への開示：企業は、通知で特定された目的及び個人が黙示又は明示の同意をした目的のためだけに、第三者にパーソナル・インフォメーションを開示する。

viii.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パーソナル・インフォメーションを保護する。

ix.品質：企業は、通知で特定された目的のために正確、完全かつ適切なパーソナル・インフォメーションを維持する。

x.モニタリングと徹底：企業は、プライバシーポリシーと手続への準拠性をモニタ

[3] パーソナル・インフォメーションは、個人を識別可能か関連付けることができる情報である。それには顧客、従業員及び他の個人の情報を含むかもしれない。

リングし、プライバシー関連の苦情と紛争を扱う手続を有している。

Trust サービス規準

14. システムを評価するのに使用される規準の多くが全ての原則で共通である。例えば、リスク管理に関連する規準はセキュリティ、可用性、処理のインテグリティ及び機密保持原則に適用される。その結果、セキュリティ、可用性、処理のインテグリティ及び機密保持原則の規準は、(a)全ての四つの原則に対応する規準(共通規準)と、(b)ただ一つの原則だけに対応する規準で構成される。共通規準はセキュリティ原則の規準全体を構成する。

可用性、処理のインテグリティ及び機密保持原則において、規準全体は、共通規準と報告される（一つ以上の）原則に対応する規準から構成される。

共通規準は七つのカテゴリーで構成されている。

a. 組織及び管理：

企業の構造と、企業が導入している業務単位の人員を管理、支援するために実装されたプロセスに関連する規準。これは人員の義務、誠実性、倫理観及び適性を扱う規準、及びそれらが機能する環境を含んでいる。

b. コミュニケーション：

企業が、システムの許可されたユーザーと他の当事者に方針、プロセス、手順、コミットメント及び要求事項を伝えること、それらの当事者とユーザーがシステムを適切に操作する義務に関連する規準

c. リスク管理及び内部統制のデザインと導入：

企業が(i)これらの企業の目的を達成する能力に影響する潜在的リスクを特定し、(ii)それらのリスクを分析し、(iii)内部統制のデザインと導入とその他のリスク緩和策を含むそれらのリスク対応を策定し、そして(iv)リスクとリスク管理プロセスの継続的モニタリングを行うことに関連する規準

d. 内部統制のモニタリング：

企業が、システムの設計及び内部統制のデザインの適合性と運用の有効性を、モニターし、特定された不備へ対応することに関連する規準

e. 論理的及び物理的アクセス管理：

企業が業務で扱われた原則の規準を満たすため、論理的及び物理的なシステムへのアクセスを制限し、これらのアクセス権を付与及び削除し、未承認のアクセスを防ぐことに関連する規準

f. システム運用：

企業が業務で扱われた原則の規準を満たすために、システム手順の実行を管理し、論理的及び物理的なセキュリティの逸脱を含む、処理の逸脱を検出し、緩和することに関連する規準

g. 変更管理：

企業が業務で扱われた原則の規準を満たすために、システム変更の必要性を特定し、統制された変更管理プロセスに従って変更を行い、未承認の変更を防止することに関連する規準

GAPP 管理フレームワークは、規準の構成として共通規準体系を使用しない。GAPP 規準に関しては付録Ｃを参照する。

Trust サービス原則と規準

15.

全ての原則（セキュリティ、可用性、処理のインテグリティ及び機密保持）に共通する規準	
CC1.0	組織及び管理に関する規準
CC1.1	企業は、 [セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及び要求事項を充足できるようにするシステムの設計、開発、導入、運用、維持及びモニタリングに関して組織構造、指揮命令系統、権限及び責任を明確にしている。
CC1.2	企業のシステム制御に係る設計、開発、導入、運用、維持、モニタリング、承認に関する実施責任及び説明責任は、ポリシー及びほかのシステム要求事項を効果的に業務に広め、実施することを確実にするため、権限とともに企業内の各個人に割り当てられる。
CC1.3	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に影響を与えるシステムの設計、開発、導入、運用、維持、モニタリングに関して責任がある要員は、責任を果たす上で必要な資格と能力を保持している。
CC1.4	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及び要求事項を充足可能とする行動規範を確立し、従業員選考手続（バックグランドチェックを含む。）を導入し、実行手続を行っている。
CC2.0	コミュニケーションに関する共通規準
CC2.1	システムの設計・運用とその境界に関連する情報は、許可された内部及び外部システムユーザーが、システム上の役割とシステム運用の結果を理解できるように用意され、伝達している。

CC2.2	企業の[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]のコミットメントは、適切な方法により外部ユーザーに伝達され、これらのコミットメント及び関連するシステム要求事項は、内部システムユーザーが責任を果たすことができるように伝達されている。
CC2.3	企業は、内外ユーザー及びシステム運用に影響を及ぼす役割があるその他の者に責任を伝達する。
CC2.4	システムの設計、開発、導入、運用、維持及びモニタリングの内部統制に責任がある内部要員と外部要員は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連して、これらの責任を果たすために不可欠な情報を保持している。
CC2.5	内部及び外部のシステムユーザーは、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連する障害、事故、懸念及び他の苦情を適切な担当者に報告する方法についての情報が提供されている。
CC2.6	内部及び外部システムユーザーの責任又は[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]と関連する企業のコミットメント及び要求事項に影響を及ぼすシステム変更は、適時にそれらのユーザーに伝達される。
CC3.0	**リスク管理及び内部統制のデザインと導入に関する共通規準**
CC3.1	企業は、(1)システムの[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及び要求事項を害するおそれのある潜在的脅威を識別し、(2)識別された脅威と関連するリスクの重大性を分析し、(3)それらのリスクに対する軽減方法（内部統制及び他の軽減方法を含む。）を決定する。
CC3.2	企業はリスク軽減方法を実行するため、ポリシーと手続を含む、内部統制を設計、開発、導入する。
CC3.3	企業は、(1)[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]のための内部統制システムに、重大な影響を及ぼし得る変更（例えば、環境、規制及び技術的な変更）を識別・評価し、そして当該変更に基づいてリスクと軽減方法を再評価し、(2)これらの活動の運用とモニタリングに基づいた統制活動のデザインと配置の適合性を再評価し、必要に応じてそれらを更新する。
CC4.0	**内部統制のモニタリングに関する共通規準**
CC4.1	統制のデザインと運用上の有効性は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するコミットメント及び要求事項に対し定期的に検証され、識別された不備に関連する修正及び他に必要となる対応は、適時に実施される。

CC5.0	論理的及び物理的アクセス管理に関する共通規準
CC5.1	論理的なアクセスセキュリティに関するソフトウェア、インフラストラクチャー及びアーキテクチャは、(1)許可されたユーザーの識別及び認証、(2)管理者によって承認された、ハードウェア、データ、ソフトウェア、モバイル機器、出力及びオフライン要素を含む、システム構成要素又はその一部分について許可されたユーザーアクセス制限、(3)未承認のアクセスの防止と発見を支援するために実装される。
CC5.2	新規の内部及び外部システムユーザーは、システム証明書が発行される前に登録・承認されてから、システムにアクセスする権限が与えられる。ユーザーアクセスがもはや承認されないときには、ユーザーシステム証明書は削除される。
CC5.3	内部及び外部システムユーザーは、システム構成要素（例えば、インフラストラクチャー、ソフトウェア及びデータ）にアクセスする場合には、識別され承認される。
CC5.4	データ、ソフトウェア、機能及び他のＩＴ資源へのアクセスは、役割、責任又はシステム設計とそれらへの変更に基づいて、承認され、修正又は削除される。
CC5.5	システムを収容する設備（例えば、データセンター、バックアップ媒体保管庫、これらの所在地にある機密上重要なシステム構成要素のみならず他の機密上重要な所在地）への物理的なアクセスは、承認された人員に制限される。
CC5.6	論理的なアクセスセキュリティ対策を、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するシステム境界の外部要因による脅威から保護するために導入している。
CC5.7	情報の送信、移動及び削除は、許可されたユーザーとプロセスに制限され、そして[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及び要求事項を充足するよう送信、移動及び削除する間は保護される。
CC5.8	未承認又は悪意あるソフトウェアの導入を、防止又は検知し、対処する内部統制が実装されている。
CC6.0	システム運用に関する共通規準
CC6.1	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関して、悪意ある行為、自然災害又はエラーに起因する違反やインシデントについてのシステム構成要素の脆弱性は監視及び評価され、対応策が既知及び新規の脆弱性を補うために実装される。
CC6.2	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの

	組合せで報告対象の原則を挿入]に関して、論理的及び物理的セキュリティ違反、障害、懸念並びに他の苦情を含むインシデントは、確立されたインシデント対応手順に従って識別され、適切な人員に報告され、対処される。
CC7.0	変更管理に関する共通規準
CC7.1	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するコミットメント及び要求事項は、システム構成要素の設計、調達、導入（実装）、設定、テスト、修正及び維持を含んだシステム開発ライフサイクルを通じて対処される。
CC7.2	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するシステムのコミットメント及び要求事項との整合性を保つために、インフラストラクチャー、データ、ソフトウェア及び手続が必要に応じて更新される。
CC7.3	システムの運用中及び監視中に、内部統制のデザイン又は運用の有効性に不備が識別されると、変更管理プロセスが開始される。
CC7.4	システム構成要素への変更は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するコミットメント及び要求事項に準拠して（起案）承認され、設計され、開発され、設定され、文書化され、テストされ、（リリース）承認され、実装される。
可用性に関する追加規準	
A1.1	可用性に関するコミットメント及び要求事項を充足するように、キャパシティ要求を管理し、追加の処理能力の導入を可能にするために、現在の処理能力と使用率が保持され、監視され、評価されている。
A1.2	可用性に関するコミットメント及び要求事項を充足するため、物理的設備対策、ソフトウェア、データのバックアッププロセス、復旧用のインフラストラクチャーが設計され、開発され、実装され、稼働し、保持され、監視されている。
A1.3	可用性に関するコミットメント及び要求事項を充足するため、復旧計画に従ったシステム復旧を支援する手続が定期的にテストされている。
処理のインテグリティに関する追加規準	
PI1.1	処理のインテグリティに関するコミットメント及び要求事項を充足するため、処理エラーを防止し、検出し、是正する手続が存在する。
PI1.2	システム入力は、処理のインテグリティに関するコミットメント及び要求事項に従って、完全に、正確に、適時に測定され、記録される。
PI1.3	データは、処理のインテグリティに関するコミットメント及び要求事項に従って承認されたとおりに、完全に、正確に、適時に処理される。
PI1.4	データは、処理のインテグリティに関するコミットメント及び要求事項に従って、特定された一定期間、完全かつ正確に格納され、保持される。

PI1.5	システム出力は、処理のインテグリティに関するコミットメント及び要求事項に従って、完全で、正確で、配布され、そして保持される。
PI1.6	データの修正は、処理のインテグリティに関するコミットメント及び要求事項に従って、承認された手続により承認される。
機密保持に関する追加規準	
C1.1	機密情報は機密保持に関するコミットメント及び要求事項に従って、システム設計、開発、テスト、実装及び変更プロセスの間、保護されている。
C1.2	システム領域内の機密情報は、機密保持に関するコミットメント及び要求事項に従って入力、処理、保管、出力及び廃棄の間、未承認のアクセス、使用及び開示から保護されている。
C1.3	機密情報へのシステム領域外からのアクセス及び機密情報の開示が、機密保持に関するコミットメント及び要求事項に従って、承認された当事者に制限されている。
C1.4	企業は、システムの一部を構成し、機密情報へのアクセスを持つ製品やサービスを提供するベンダー及び他の第三者から、企業の機密保持要件に整合する機密保持に関するコミットメントを入手している。
C1.5	システムの一部を構成する製品やサービスのベンダー及び他の第三者の機密保持に関するコミットメント及び要求事項の遵守状況が、定期的及び必要に応じて評価され、必要な是正措置が取られる。
C1.6	機密保持のコミットメント及び要求事項の変更が、内部及び外部ユーザー、製品やサービスがシステムの一部を構成するベンダー並びに第三者に伝達される。

プライバシー原則と規準

16. これらの規準は付録Cに詳しく説明される。

発効日

17. Trust サービス原則と規準は、2014 年 12 月 15 日以降終了する期間において適用する。それ以前の適用を妨げない。

付録A　定義

18.

正確性：

実行されたトランザクションに係る主要な情報は、トランザクションの処理を通じて正確さが保持され、トランザクション又はサービスが、意図されたとおりに処理又は実行されていること。

承認(許可)：

処理が、システム処理を管理する方針で定められた必要な承認及び特権に従い、実行されていること。

承認(許可)されたアクセス：

アクセスが、(a)経営者により任命された者により承認され、(b)職務の分離、機密保持コミットメントに抵触しない場合、又は経営者によって承認されたレベルを越えたところまでシステムリスクを増加させない場合（すなわち、アクセスは適切であること。）に限り承認されていること。

システムの境界：

経営者のシステムに関する特定の経営目的を達成するために使用される企業運営の一部の物理的及び論理的な境目のこと。境界は、ベンダーと他の第三者によって提供されたものを含む企業の管理下にあるシステムの全ての構成要素を含んでいる。

プライバシー又は機密保持業務のために、システムの境界は情報の捕捉から始まり、その開示と最終的な廃棄（しばしば、情報ライフサイクルと呼ばれる。）を通した構成要素を含んでいる。システムの境界には、(a)情報の廃棄までにおける収集、利用、保持、開示及び非特定化又は匿名化 、(b)全事業セグメント及び企業全体か単独の特定された事業セグメントに関わるロケーション（例えば、製造事業ではなく小売事業又は企業のウェブサイト若しくは特定のウェブドメイン事業のみ）又は地理的ロケーション（例えば、カナダの事業のみ）が含まれる。

コミットメント：

システムパフォーマンスに関係して経営者が作成する顧客に対する宣言。コミットメントは、個別の契約、標準契約、サービスレベルアグリーメント又は公表された声明書（例えば、セキュリティ実務声明）を通じて伝達される。個々のコミットメントは、一つ以上の原則に関連するかもしれない。業務実施者は、報告する原則に関係するコミットメントのみを検討する必要がある。コミットメントは、以下を含む様々な形式を取るかもしれない。

- 計算に使用されるアルゴリズムの仕様
- システムの利用可能時間について記載した契約上の取決め
- 公表されたパスワード標準
- 保存された顧客データの暗号化に使用される暗号化標準

完全性：

欠落なくトランザクションが処理されるか、又は全てのサービスが実行されること。

物理的設備対策：

企業によって実装された、災害等によるシステムの物理的な損傷のリスクを検出、防止、及び管理する対策 （例えば、火事、洪水、強風、地震、電圧の急変化、又は停電からの保護）

外部ユーザー：

顧客、企業管理者又は他の権限保持者によってシステムに接する権限を与えられたシステム境界外の個人

内部ユーザー：

職務権限によりシステムの人員構成要素のメンバーとなる企業とベンダーの人員

報告書利用者：

AT セクション 101、保証業務（AICPA、職業基準書）に準拠した業務実施者の報告書の想定利用者。報告書利用者は、一般公衆であるか、又は AT セクション 101 のパラグラフ 78 に従った特定の関係者に制限されるかもしれない。

要求事項：

経営者の経営目標、顧客へのコミットメント、及び義務（例えば、法令）にシステムの機能を適合させるための仕様。要求事項は、システムポリシー、システム設計書、顧客との契約及び政府規制でしばしば特定される。

要求事項の例は、

- 政府の銀行規則で確立された従業員の指紋採取と従業員選考手続（バックグランドチェックを含む。）。
- 業務設計書で定義された入力編集
- セキュリティポリシー・マニュアルに文書化された従業員の論理的アクセスの定期的なレビューとしての許容される最大の間隔
- SOAP（Simple Object Access Protocol）のように、他の組織である同業種グループで設定された全てのメタデータ要求事項を含む、データ定義とタグ付け規格
- 規制当局により設定された業務処理規則及び基準。例えば、「医療保険の相互運用性と説明責任に関する法令(HIPAA)」の下のセキュリティ要求事項

セキュリティ要求事項は、セキュリティ、可用性、処理のインテグリティ、又は機密保持に関連する経営コミットメントから生じるかもしれない。例えば、データエントリーとデータ承認の間の職務の分離をプログラムに基づいて実施するコミットメントは、ユーザーアクセス管理に関するシステム要求を作成する。

SOC2 業務：

受託会社の内部統制について、「受託会社のセキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシーに関する内部統制の報告書（SOC2）のガイド」を使用して、デザインの適切性（タイプ１）若しくはデザインの適切性と運用の有効性（タイプ２）を報告する保証業務

SOC3 業務：

一つ以上の Trust サービス原則に関連するシステムに係る企業の内部統制のデザインの適切性及び運用の有効性を報告する保証業務

適時性：

サービスの提供や品物の配達が、コミットメントに記載されたとおりに実施されること

Trust サービス：

システムと関連するデータの運用と保護に関する原則と規準を基に提供される一連の職業的保証業務と助言業務

従業員：

社員、契約社員及びシステムの操作の一部を実施することについて企業が契約したその他の者

付録Ｂ　リスク及び内部統制の例示

19. この付録に示されたリスクと内部統制の例示は、例示的な目的だけのためのものである。それらは仮定している産業で仮定している企業に基づいている。それらは、包括的なリスクと内部統制であること、又は全ての企業にとって適切であることを意図していない。したがって、規準に対するリスクと内部統制のチェックリストとしてそれらを使用するべきではない。業務実施者は、NIST800-53 やクラウド・コントロール・マトリックス（CCM）のような、他のフレームワークの使用を検討すべきである。

規準		リスク	内部統制の例示
全ての原則（セキュリティ、可用性、処理の完全性及び機密保持）に共通する規準			
CC1.0	1.0　組織及び管理に関する規準		
CC1.1	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及び要求事項を充足できるようにするシステムの設計、開発、導入、運用、維持及びモニタリングに関して組織構造、指揮命令系統、権限及び責任を明確にしている。	企業の組織構造が、[セキュリティ、可用性、処理のインテグリティ又は機密保持]の活動を管理するために必要な情報フローを提供していない。	企業が、事業計画プロセスの一部、進行中のリスク評価及び管理プロセスの一部として、その組織構造、指揮命令系統、権限及び責任を評価し、変化するコミットメント及び要求事項を充足するために、必要に応じてそれらを改訂する。
		[セキュリティ、可用性、処理のインテグリティ又は機密保持]の活動についての適切な監督、管理及び監視を実施するための主要な管理者の役割と責任が、十分に	役割と責任は、職務記述書上で定義され、管理者及び上級管理者に伝達される。

		定義されていない。	
			職務記述書は変更が必要かどうか年次で経営者によってレビューされ、職務の変更が生じたときは職務記述書にも必要な変更が行われる。
		指揮命令関係及び組織構造により、上級管理者が[セキュリティ、可用性、処理のインテグリティ又は機密保持]に関する効果的な監督を行うことができない。	指揮命令関係及び組織構造が組織の計画の一部として上級管理者によって定期的にレビューされ、企業のコミットメント及び要求事項が変更される都度、必要に応じて調整される。
		従業員が[セキュリティ、可用性、処理のインテグリティ又は機密保持]に係るコミットメント及び要求事項を満たすだけの責任を与えられていない、又は十分な権限を委譲されていない。	役割及び責任が職務記述書に定義されている。

CC1.2	企業のシステム制御に係る設計、開発、導入、運用、維持、モニタリング、承認に関する実施責任及び説明責任は、ポリシー及びほかのシステム要求事項を効果的に業務に広め、実施することを確実にするため、権限とともに企業内の各個人に割り当てられる。	従業員が、[セキュリティ、可用性、処理のインテグリティ又は機密保持]に係るコミットメント及び要求事項を満たすだけの責任を与えられていない、又は十分な権限を委譲されていない。	役割及び責任が職務記述書に定義されている。
			職務記述書の変更が必要かどうか定期的にレビューされ、変更が識別された場合は更新される。
CC1.3	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に影響を与えるシステムの設計、開発、導入、運用、維持、モニタリングに関して責任がある要員は、責任を果たす上で必要な資格と能力を保持している。	新規雇用者又は異動した従業員が、職務遂行に十分な知識と経験を有していない。	職務要件は職務記述書に文書化され、候補者の能力が職務要件を満たしているかどうか、雇用又は異動の評価プロセスの一部として評価される。
			異動の候補者の経験及び研修は、候補者が職務に就く前に評価される。
		要員が、職務遂行するのに十分な継続的研修を受けていない。	経営者が、従業員へのコミットメント及び要求事項とともにスキルと継続的研修を確立している。
			経営者が、研修の要件

			に準拠しているかをモニタリングしている。
		ツールと情報資源は、割り当てられたタスクを実施するのに不十分である。	経営者は、継続的、定期的なビジネス計画及び予算プロセスの中で、継続的なリスク評価と管理プロセスの一部として、ビジネス目的を達成するために、追加的ツールと資源の必要性を評価する。
CC1.4	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及び要求事項を充足可能とする行動規範を確立し、従業員選考手続（バックグランドチェックを含む。）を導入し、実行手続を行っている。	要員は、行動規範を忠実に守るわけではない。	経営者は、顧客と従業員の苦情のモニタリングを通じて、また、第三者に管理された匿名の倫理ホットラインを利用して、従業員の行動規範の遵守をモニタリングする。
			要員は、採用時に行動規範と機密保持及びプライバシー実務の声明を読んで同意し、その後は正式に年次で再確認を要求される。
		候補者は、企業の経営者によって受け入れ難いとされるバックグランドを持つ。	上級経営者は、従業員候補者が与えられる職位に求められる慎重さやスキルに基づいて採用されることから、排除する特性のリストを策定する。

			要員は、採用される前に企業又は企業の委託を受けている第三者の、賞罰及び財務的な信用のバックグランドチェックを合格しなければならない。
CC2.0	コミュニケーションに関する共通規準		
CC2.1	システム設計・運用とその境界に関連する情報は、許可された内部及び外部システムユーザーが、システム上の役割とシステム運用の結果を理解できるように用意され、伝達している。	ユーザーは、そのスコープ、目的及び設計の理解不足のためにシステムの利用を誤る。	システムの境界を説明し、システムの目的及び設計だけでなく、関係するシステム構成要素を記述するシステム記述は、許可された外部ユーザーが入手できるようになっている。システム記述は、企業の顧客向けウェブサイトを介して許可されたユーザーが入手することができる。
			システム記述は、企業のイントラネット上に置かれ、企業の内部ユーザーが利用できる。この記述はシステムの境界と処理の主要な側面を詳細に説明する。
		ユーザーは主要な組織及びシステムサポート機能、処理並びに役割と責任を自覚していない。	企業の組織構造、システムサポート機能、処理及び組織の役割と責任の記述は、企業のイントラネット上に置かれ、企業の内部ユーザーが利用できる。この記述には、主要なシステム構成要素の設計及び運用の変更に関し実施責任と説明責任を負い、同意

			し、そして伝えられている当事者が説明されている。
		外部ユーザーは、システムの境界外から発生する責任を負うべきリスクに対処していない。	システムの境界を説明し、システムの目的及び設計だけでなく、重要なシステム構成要素を記述するシステム記述は、許可された外部ユーザーが入手できるようになっている。システム記述は、顧客との継続的なコミュニケーション、又は顧客向けウェブサイトを通じて、ユーザーが利用できる。
CC2.2	企業の[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]のコミットメントは、適切な方法により外部ユーザーに伝達され、これらのコミットメント及び関連するシステム要求事項は、内部システムユーザーが責任を果たすことができるように伝達されている。	ユーザーは、[セキュリティ、可用性、処理のインテグリティ又は機密保持]のために提供されるシステムの能力を理解できていない。また、この理解不足に基づき行動をとる。	企業のシステムに関する[セキュリティ、可用性、処理のインテグリティ又は機密保持]コミットメントは、サービス契約及び顧客特定サービスレベルへの同意事項を含んでいる。加えて、これらのコミットメントの要約は企業の顧客向けウェブサイトで利用できる。
		企業のサービスを提供する要員の理解不足のために、企業がそのコミットメントを果たすことができない。	重要なプロセスの方針及び手続文書が、企業のイントラネットで利用できる。
			要員は、年度のセキュリティ、機密保持及びプライバシー研修への参加が要求される。

			要員は、行動規範と機密保持及びプライバシー実務の声明を読んで同意することを、採用時その後は年次で要求される。
			プロセスは、サービスレベルのコミットメント及び合意書への遵守をモニタリングするサービスレベルの管理手続を通じて、モニタリングされている。結果は適切な人物と顧客との間で共有され、コミットメントと合意書が充足されない場合には、行動がとられ、顧客を含む関係者へ伝達される。
CC2.3	企業は、内外ユーザー及びシステム運用に影響を及ぼす役割があるその他の者に責任を伝達する。	システムは、内部ユーザーの責任不履行により、設計されたとおりに機能しない。	システム要件に対処する重要なプロセスの方針及び手続文書が、企業のイントラネットで利用できる。
			要員は、年度のセキュリティ、機密保持及びプライバシー研修への参加が要求される。
			要員は、行動規範と機密保持及びプライバシー実務の声明を読んで同意することを、採用時その後は年次で要求される。
			プロセスは、コミットメント及び要求事項への遵守をモニタリングするサービスレベルの

			管理手続を通じて、モニタリングされている。結果は適切な要員と顧客との間で共有される。
		システムは、外部ユーザーの責任不履行により、設計されたとおりに機能しない。	顧客の責任が、顧客向けウェブサイトとシステム文書に記述されている。
CC2.4	システムの設計、開発、導入、運用、維持及びモニタリングの内部統制に責任がある内部要員と外部要員は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連して、これらの責任を果たすために不可欠な情報を保持している。	内部統制は、これらの内部統制の導入と運用に関する要員の責任部分の理解が誤っているために、結果として[セキュリティ、可用性、処理のインテグリティ又は機密保持]のコミットメント及び要求事項を充足せず、設計された機能が損なわれているか、効果的に運営されていない。	重要なプロセスの方針及び手続文書が、企業のイントラネットで利用できる。
			プロセスは、コミットメント及び要求事項への遵守をモニタリングするサービスレベルの管理手続を通じて、モニタリングされている。結果は、方針に従って共有される。
			顧客の責任が、顧客向けウェブサイトとシステム文書に記述されている。
CC2.5	内部及び外部のシステムユーザーは、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対	システムの異常は内外のユーザーにより検出されるが、障害が適切な要員に報告されないと、結果として[セキュ	運用上の障害、インシデント、システムの問題、事故及びユーザークレームを報告する責任（及び報告のプロセス）

	象の原則を挿入]に関連する障害、事故、懸念及び他の苦情を適切な担当者に報告する方法についての情報が提供されている。	リティ、可用性、処理のインテグリティ又は機密保持]に関するコミットメント及び要求をシステムが達成できない。	を含んだ、重要なプロセスに関する方針及び手続文書が公表され、イントラネットで利用できる。
			運用上の障害、インシデント、問題、事故、クレームを報告する責任を含む顧客の責任及び報告のプロセスが、顧客向けウェブサイトとシステム文書に記述されている。
CC2.6	内部及び外部システムユーザーの責任又は[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]と関連する企業のコミットメント及び要求事項に影響を及ぼすシステム変更は、速やかにそれらのユーザーに伝達される。	システム変更に起因して、ユーザーがシステム能力の変更や[セキュリティ、可用性、処理のインテグリティ又は機密保持]の提供に関する自分たちの責任の変化について誤解し、その誤解に基づいた行動をとる。	顧客に影響を与えるシステム変更の提案は、実装のXX日前に顧客向けウェブサイトで公表される。ユーザーは大規模な変更の実装XX日前に、ユーザー受入れテストに参加する機会を与えられる。システムに加えられた変更は、カスタマーケア会議のような継続的なコミュニケーションの仕組みや顧客向けウェブサイトを通じて、顧客に伝達され確認される。
			ビジネス部門の経営者は、変更を承認するまでに、変更を理解していることを確認しなければならない。
			実装されるシステム変更が記載されたシステム変更の日程表は、企業のイントラネットに掲載される。

			更新されたシステム文書が、実装の30日前に顧客向けウェブサイトやイントラネットに掲載される。
			インシデントに起因するシステム変更は、実装プロセスの一部として、電子メールを通じて内外のユーザーに伝達される。
		役割及び責任の変更や、主要な要員の変更が、内外のユーザーへ適時に伝達されない。	役割及び責任の重要な変更や、主要な要員の変更は、変更管理プロセスの一部として、影響を受ける内外のユーザーへ電子メールを通じて伝達される。
CC3.0	リスク管理及び内部統制のデザインと導入に関する共通規準		
CC3.1	企業は、(1)システムの[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及び要求事項を害するおそれのある潜在的脅威を識別し、(2)識別された脅威と関連するリスクの重要性を分析し、(3)それらのリスクに対する軽減方法（内部統制及びほかの軽減方法を含む。）を決定する。	必ずしも全てのシステムの構成要素がリスクマネジメントプロセスに含まれず、その結果、リスクの識別と軽減又は受容ができない。	経営者が使用するための企業のシステム構成要素のマスターリストがメンテナンスされ、追加や削除が明らかにされる。
		リスクマネジメントプロセスに関係する要員が、リスク及び企業のリスク許容度を評価す	企業は、リスク許容度を明確にする正式なリスクマネジメントプロセスや、識別した脅威と

		るための十分な情報を持っていない。	明確化した許容度に基づくリスク評価プロセスを定義している。
		セキュリティ・コントロールにより対処可能で、重要な、そして [セキュリティ、可用性、処理のインテグリティ又は機密保持]に関するコミットメント及び要求の達成を脅かす一つ又は複数の内外のリスクが識別されない。	リスク評価や管理のプロセスを通じて、リスク管理部門の要員は、ビジネス目標、コミットメントと要求事項、内部の運用、ビジネス目標の達成にとって脅威となる外部要因の変化を識別し、システムの目的に対する潜在的な脅威について更新する。
			識別されたリスクは、リスク評価プロセスを使用して評価され、評価結果は経営者によってレビューされる。
			リスク管理グループが、内部統制の有効性と識別されたリスクに合う軽減方法を評価し、その評価に基づき改善を勧告する。
			リスク管理グループによる勧告は、上級経営者によってレビューされ、承認される。
			企業は、主要なシステム構成要素、技術的及びインストールに関する具体的な実装の詳細を把握し、継続的な資産管理やサービス管理に関するコミットメントや要求事項をサポートするための構成管理デー

			タベースや関連プロセスを使用する。
CC3.2	企業はリスク軽減方法を実行するため、ポリシーと手続を含む、内部統制を設計、開発、導入する。	選択、開発及び整備された内部統制や軽減方法が、リスクを適切に軽減しない。	四半期ごとに、現業部門による内部統制の自己評価が実施される。
			年次のリスク評価に基づく内部監査計画に従って、内部監査が実施される。
			事業復旧計画が、年次でテストされる。
			内部や外部の脆弱性チェックが四半期ごとに、又は年ごとに実施され、その頻度は継続かつ変化するコミットメントと要求事項に合わせて調整される。
		整備された内部統制や軽減方法が、評価されていない新たなリスクを生み出す。	CC3.1の内部統制の例示を参照
CC3.3	企業は、(1)[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]のための内部統制システムに、重大な影響を及ぼし得る変更（例えば、環境、規制及び技術的な変更）を識別・評価し、そして、当該変更に基づいてリスクと軽減方法を再	必ずしもシステムに重要な影響を与える全ての変化が識別されず、その結果、関連するリスクが再評価できない。	リスク評価や管理のプロセスを通じて、リスク管理の要員は、ビジネス目標、コミットメントと要求事項、内部の運用、ビジネス目標の達成にとって脅威となる外部要因の変化を識別し、システムの目的に対する潜在的な脅威について更新する。

	評価し、(2)これらの活動の運用とモニタリングに基づいた統制活動のデザインと配置の適合性を再評価し、必要に応じてそれらを更新する。		
		適切に識別されない変更は、リスクマネジメントプロセスを経ていないためにリスクを生み出す。	リスク評価や管理のプロセスを通じて、リスク管理部門の要員は、発生した環境、規制及び技術的な変更を識別する。
CC4.0	内部統制のモニタリングに関する共通規準		
CC4.1	統制のデザインと運用上の有効性は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するコミットメント及び要求事項に対し定期的に検証され、識別された不備に関連する修正及びほかに必要となる対応は、適時に実施される。	内部統制が、適切にデザインされていない、確立した方針に従って構成されていない、又は、効果的に運用されていないことで、結果としてシステムのコミットメントと要求事項を満たさないシステムとなっている。	モニタリングソフトウェアは、継続したシステムパフォーマンス、セキュリティの脅威、リソース利用要求の変化、及び通常でないシステム活動を特定し評価するために利用されている。このソフトウェアはあらかじめ定義された一定の閾値に達した場合に、オペレーションセンターへメッセージを送り、インシデント、問題又は変更管理に関する“チケット”記録を自動的にオープンにする。
			運用とセキュリティ担当者は報告された事象の解決及びエスカレーションのために、定義された手順に従う。
CC5.0	論理的及び物理的アクセス管理に関する共通規準		

CC5.1	論理的なアクセスセキュリティに関するソフトウェア、インフラストラクチャー及びアーキテクチャは、(1)許可されたユーザーの識別及び認証、(2)管理者によって承認されたハードウェア、データ、ソフトウェア、モバイルデバイス、出力及びオフライン要素を含む、システム構成要素又はその一部分について許可されたユーザーアクセス制限、(3)未承認のアクセスの防止と発見を支援するために実装される。	全てのシステム基盤（インフラストラクチャー）又はシステム構成が論理的アクセスセキュリティ対策で保護されておらず、未承認の修正や使用という結果になる。	インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために、確立された企業標準（アクセス管理ソフトウェア、企業設定標準及び標準化されたアクセス統制リストの実装のための要求事項を含む。）がある。
			ネットワークスキャンは、インフラストラクチャー要素と企業標準の不一致を識別するために実行される。
			資産が、ジョブロールに基づいてアクセスを評価する責任があるオーナーに割り当てられる。そのオーナーは、資産が取得され変更される都度、アクセス権を定義し、保管又は受託責任のある資産のために、定期的にアクセスを評価する。
			オンライン・アプリケーションにより、個々のユーザーIDと単一の顧客アカウント番号と照合される。システム記録へのアクセス要求は、最

			初にシステムへのアクセスが許可されるときに、各ユーザーが有する特権リストと顧客アカウント番号との照合を要求する。
		論理的アクセスセキュリティ対策が、ＩＴ構成要素へのアクセスを許可する前に、ユーザーを識別又は認証しない。	インフラストラクチャー構成要素とソフトウェアは、利用可能であるときに、共有ログオン機能を利用するように設定される。共用ログオン機能を利用していないシステムは、ユーザーIDとパスワードの分離送信の実装が要求されている。
			従業員による外部アクセスは、暗号化された仮想プライベートネットワーク（VPN）接続による二要素認証（例えば磁気カードとパスワード）を通じてのみ許可される。
		論理的アクセスセキュリティ対策が、システム設計で要求される職務分離を提供しない。	ロールに基づくセキュリティプロセスは、可能であればロールを利用するように要求される、アクセス管理システムで定義されている。
			資産が、ジョブロールに基づいてアクセスの適切性を評価する責任があるオーナーに割り当てられる。ロールは定期的にレビューされ、資産オーナーとそのリスク管理グループによっ

			て年次で更新される。レビューの結果によるアクセス変更要求は、変更要求記録を経由してセキュリティグループへ提出される。
			ロールベースのセキュリティの利用をサポートしないソフトウェアとインフラストラクチャーのために、役割と関連するアクセス用に分離されたデータベースが管理される。セキュリティグループは、アクセスルールをシステムへ入力するときにこのデータベースを利用する。
		論理的アクセスセキュリティ対策が、システム設定、特権機能、マスターパスワード、強力なユーティリティ、セキュリティデバイス、そしてその他のハイリスク資源へのアクセスを制限していない。	機密性の高い資源への特権アクセスは、定義されたユーザーロールに制限され、これらのロールへのアクセスは最高情報セキュリティ責任者によって承認されなければならない。このアクセスは、最高情報セキュリティ責任者によって設定されるように、定期的に最高情報セキュリティ責任者によって、レビューされる。

CC5.2	新規の内部及び外部システムユーザーは、システム証明書が発行される前に登録・承認されてから、システムにアクセスする権限が与えられる。ユーザーアクセスが最早承認されないときには、ユーザーシステム証明書は削除される。	有効なユーザーIDが、許可されていない人に与えられる。	人事管理システムの人事異動から収集されたユーザーの自動取り込みにより、異動日にアクティブディレクトリとVPNシステムで、ユーザーIDが日次で自動作成又は自動削除される。
			保護された資源への従業員アクセスは、システム資源オーナーからの承認された変更要求に基づいて、セキュリティグループによって、生成又は修正される。
			契約社員とベンダーのIDは、契約社員の部署からの承認された変更要求に基づいて、セキュリティグループによって生成される。これらのIDは、関係の終了予定日又はXX日のいずれか短い期間で有効となる。
			特権顧客アカウントは、指定された顧客窓口からの承認要求書面の記載に基づいて生成される。これらのアカウントはクライアントのユーザーアクセスの生成に使用される。
			システムセキュリティは、初期ログインとXX日ごとに、ユーザーにパスワードを変更することを要求するように設

			定されている。
		既に許可を失ったユーザーが、システム資源へアクセスを続けている。	人事システムは、最終出社日の従業員のアクセスを排除するため、自動取込みをアクティブダイレクトリとVPNに、日次で送信する。そのリストは、アクセス排除のためにセキュリティ要員によって利用される。そのアクセス排除は、セキュリティマネジャーによって確認される。
			週次で、人事システムは、セキュリティグループに退職者リストを、そのアクセスが排除されるようにするため、送信する。そのリストは、セキュリティ要員によってアクセスを排除するために利用される。そのアクセス排除は、セキュリティマネジャーによって確認される。
			週次で、契約社員の管理部署は、セキュリティグループに契約終了ベンダー及び契約社員のリストを、そのアクセスが排除されるように送る。そのリストは、セキュリティ要員によってアクセスを排除するために利用される。そのアクセス排除は、セキュリティマネジャーによっ

			て確認される。
			企業のポリシーは、最高情報セキュリティ責任者の書面による承認なしで、退職者のIDの再活性化又は利用は禁止している。再活性化の要求は、変更管理記録を利用して作成され、その目的とアクセスの正当性（業務上の必要性のため）、再活性化されたそのシステムとアカウントが有効となる期間（XX日間を超えない。）が含まれる必要がある。アカウントは新しいパスワードでリセットされ、要求された期間で活性化される。全てのアカウントの利用は記録され、セキュリティ要員によってレビューされる。
			アカウントの共有は、方針からの逸脱が、アカウント共有の統制される状況、個々の使用の活動ログを提供する「アカウントとパスワードを保管するソフトウェア製品」を使用することが企業によって規定されているとして、最高情報セキュリティ責任者に

			よって認められている場合以外、禁止される。そのほかに、共有アカウントは、低リスクのアプリケーション（例えば、共有 ID によるアクセスが職務の分離を阻害し得ないような情報システム）や、共有 ID の使用がシステム技術上の制約になっている場合（例えば UNIX のルート権限）には認められる。最高情報セキュリティ責任者は、全ての共有アカウントの使用を承認しなければならない。軽減した統制は、可能な場合には実行される（例えば、UNIX のルート権限でのアクセス時の SU の利用）。
CC5.3	内部及び外部システムユーザーは、システム構成要素（例えばインフラストラクチャー、ソフトウェア及びデータ）にアクセスする場合には、識別され承認される。	情報システム構成要素にアクセスするとき、ユーザーは特定されない。	インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために、確立された企業標準（アクセス管理ソフトウェア、企業設定標準及び標準化されたアクセス統制リストの導入のための要求事項を含む。）がある。

			アカウントの共有は、方針からの逸脱が、アカウント共有の統制される状況、個々の使用の活動ログを提供する「アカウントとパスワードを保管するソフトウェア製品」を使用することが企業によって規定されているとして、最高情報セキュリティ責任者によって認められている場合以外、禁止される。 そのほかに、共有アカウントは、低リスクのアプリケーション（例えば共有IDによるアクセスが職務の分離を阻害し得ないような情報システム）や、共有IDの使用がシステム技術上の制約になっている場合（例えばUNIXのルート権限）には認められる。 最高情報セキュリティ責任者は、全ての共有アカウントの使用を承認しなければならない。 軽減した統制は、可能な場合には実行される（例えば、UNIXのルート権限でのアクセス時のSUの利用）。
		無権限者は、システムにアクセスするため、有効なユーザーIDがあるかのように装う。	オンライン・アプリケーションにより、個々のユーザーIDを単一の顧客アカウント番号と照合される。 システム記録へのア

			クセスの要求は、顧客アカウント番号の照合を要求する。
			二要素認証と暗号化されたVPNチャネルの利用は、正当なユーザーのみがＩＴ構成要素にアクセスできることを確実とするのを支援する。
			基盤の構成要素とソフトウェアは、利用できるとき、アクティブディレクトリ共有ログオン機能を使うように構成される。 共有ログオン機能を使っていないシステムは、別々のユーザーIDとパスワードを必要とするように構成される。
		無権限者に権限者の保有する活動ができるようになると、ユーザー・アクセス・クレデンシャルは無駄になる。	ユーザーは、VPN、SSL、その他の暗号化された通信システムの利用を通じてのみ、リモートでそのシステムにアクセスすることができる。
			パスワードの複雑性の標準が、アクセス・コントロール・ソフトウェアのパスワードによる統制を強制するために規定されている。
CC5.4	データ、ソフトウェア、機能及び他のＩＴ資源へのアクセスは、役割、責任又はシステム設計とそれらへの変更に基づいて、承認され、修正又は削除され	正当なユーザーが、システムへの未承認のアクセスを得ることにより、職務の分離の欠如や意図的な悪意のある行為やエラーのリスクが	可能であれば、システムとインフラストラクチャーの構成要素へのアクセスを制限する正式な役割ベースのアクセスコントロールを構

	る。	増大する。	築し、それらはアクセスコントロールシステムによって実施される。 それが可能でないときは、二要素認証された有効なユーザーID が使用される。
			特定の役割のためのユーザーアクセス申請は、ユーザー管理者によって承認され、変更管理記録システムによってセキュリティグループに提出される。
		プロビジョニング・プロセスによって与えられたアクセスが、職務の分離を危うくするか、意図的な悪意のある行為又はエラーのリスクを増大する。	可能であれば、システムとインフラストラクチャーの構成要素へのアクセスを制限する正式な役割ベースのアクセスコントロールを構築し、それらはアクセスコントロールシステムによって実施される。それが可能でないときは、二要素認証された有効なユーザーID が使用される。
			役割は、年次ベースで、資産オーナーとリスク管理グループによって見直され更新される。見直しの結果として、アクセス権の変更申請は、変更申請記録によりセキュリティグループに提出される。

CC5.5	システムを収容する設備（例えばデータセンター、バックアップ媒体保管庫、これらの所在地にある機密上重要なシステム構成要素のみならず他の機密上重要な所在地）への物理的なアクセスは、承認された人員に制限される。	無許可の人のシステム構成要素への物理的アクセスは、構成要素（要員を含む。）へのダメージ、不正、誤った処理、無許可の論理アクセス、情報の毀損を結果としてもたらす。	ID カード（身分証明書）を使用した物理アクセスの管理システムが、施設の周囲、施設の機密区画の入退地点に導入されている。
			従業員の写真付きの ID カード（身分証明書）は、施設への入館時、退館時に常時着用しなければならない。
			ID カード（身分証明書）は、従業員の入社の研修期間中に人事部門によって用意され、全ての必要な調査が完了した後に配布される。ID カード（身分証明書）は、最初は機密でないエリアにのみへのアクセスを提供する。
			機密エリアへのアクセス権限は、機密エリアの所有者が承認したアクセス申請に基づき、必要な調査が実施され、問題が解決された後に、物理アクセス管理者によって ID カード（身分証明書）に追加される。アクセス権限に対する申請と変更は、変更管理記録システムによって、承認され、伝達される。

			契約担当は、ベンダーと契約者のためにIDカード（身分証明書）の発行を申請するかもしれない。IDカード（身分証明書）は、物理セキュリティ管理者により作成される。 申請は、変更管理記録システムによって、承認され、伝達される。
			（入館時に）訪問者は、承認された訪問者であることを特定する一日訪問者識別章が発行される前に、従業員によって（記録簿に）署名されなければならない。
			訪問者識別章は、識別目的のためだけのものであり、施設のセキュアな区画へのアクセスは許可しない。
			全ての訪問者は、機密上重要なシステムとシステム構成要素が維持運用されている施設を訪問するときは、企業の従業員によって付き添われなければならない。
		以前は適切であった物理アクセスが、ユーザーのジョブ責任の変更やシステムの変更により不適切になる。結果として、職務の分離を損ない、又は意図的な悪意のある行為若しくはエラーによるリスクが増大	施設の機密上重要なエリアの所有者は、半年ごとに継続した業務上の必要性について確かめるため、それらのエリアへの物理的アクセスを付与された名前と役割のリストを見直す。変更の申請は、変更管理記

		する。	録システムによってなされる。
		以前は承認されていた要員が、既に権限がなくなった後も、システムリソースに継続的にアクセスする。	設備の機密上重要な領域のオーナーは、半年ごとにそれらの領域へのアクセスをレビューする。変更の申請は、変更管理記録システムによってなされる。
			ベンダーは、半年ごとに ID カードと従業員リストをレビューし、いかなる変更（修正）も申請することが要求される。契約担当部署は、ベンダーレビューに基づいて変更を申請する。
			日次に、雇用の最終日に、人事システムは物理的セキュリティに対して、雇用の最終日である退職従業員のリストを送り、彼らのアクセスは取り消され、彼らの入館証は無効にされる。
		ユーザーが、以前に承認された要員から識別証明と認証証明を入手し、それらを使いシステムに未承認のアクセスをする。	週次に、契約担当部署は、セキュリティグループに対しアクセスを取り消す必要のある契約が終了したベンダーや契約者のリストを送る。
			週次に、人事システムが物理的セキュリティグループに対し、アクセスを取り消す必要のあ

			る退職者リストを送る。
			従業員及び契約者は退職時面接の間に ID カードを返却することが求められ、全ての識別章は退職時面接の前に無効にされる。したがって、従業員と契約者は退職時面接の終了時に組織の施設より物理的に付き添われて退出しなければならない。
			入館証の共有や共連れは、ポリシーにより禁止される。
			マントラップ又は他の物理的装置が、高度に機密上重要な設備のアクセス管理に使われる。
			マントラップを迂回するドアは、マネジメントの指定するメンバーの ID カードによってのみ開けることができる。
CC5.6	論理的なアクセスセキュリティ対策を、[セキュリティ、可用性、処理のインテグリティ、機密性又はそれらの組合せで報告対象の原則を挿入]に関するシステム境界の外部要因による脅威から保護するために導入している。	システムへの脅威は、外部接続ポイントを通じて得られる。	インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために定義された、企業標準（アクセス管理ソフトウェア、企業設定標準及び各ユーザーやシステムアカウントにどの特権を帰属すべきかを定義した標準化されたアクセス統制リストの導入の要求事項を含む。）がある。
			外部接続ポイントは

			複数のファイアウォールの組合せによって保護される。
			ファイアウォールのハードニング（堅牢化）標準は関連する適用可能な技術仕様に基づいており、製品及び業界の推奨実務と対比され、定期的に更新される。
			非公開のサイトへの外部アクセスは、ユーザー認証及びVPN及びSSLなどのメッセージ暗号化システムを通じて制限される。
		システムへの承認された接続が破られ、システムへの不正アクセスを得るために利用される。	ファイアウォールのルールとオンラインシステムは、リモートアクセスが認められる時間を制限し、外部接続により実施される活動及びサービスリクエストのタイプが制限される。
CC5.7	情報の送信、移動及び削除は、許可されたユーザーとプロセスに制限され、そして、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及び要求事項を充足するよう送信、移動及び削除する間は保護される。	非公開情報が、公衆通信網（経路）上を送信中に公開される。	定義された接続ポイントに関し、プロセッシングセンターとカスタマーネットワークの内外からプロセッシングセンターへ接続するユーザーの通信を保護するために、VPN、SSL、セキュアなファイル転送プログラム（SFTP）及び他の暗号技術が使われる。

			企業のポリシーは、機微機密情報をインターネット又は他の公衆通信経路（例えば、電子メール）を通じて送信することを、暗号化している場合を除き禁止している。
			公衆通信経路への外部送信の機微情報をスキャン（検査）するため、DLP ソフトウェア（データ・ロス・プリベンション・ソフトウェア）が使われる。
		ロケーション間の物理的な移動の間にリムーバブルメディア（例えば USB 機器、DVD 又はテープ）が紛失、奪取又は複製される。	バックアップメディアは、生成時に暗号化される。
			ワークステーションと、ラップトップ用のストレージは暗号化される。ワークステーションとラップトップ用のリムーバブルメディアは、ソフトウェアによって自動的に暗号化される。リムーバブルメディアは、組織が所有する他の装置によってのみ読み取れる。
			他のリムーバブルメディアは、データセンターの運用によって作成され、宅配便によって運ばれる。

		リムーバブルメディアは、ソフトウェアの不正な複製を作るために使われ、データはシステムの境界を越えて持ち去られる。	ワークステーションとラップトップ用のストレージは暗号化される。これらの装置のためのリムーバブルメディアは、ソフトウェアによって自動的に暗号化される。リムーバブルメディアは、組織が所有する他の装置によってのみ読み取れる。
			バックアップメディアは、生成時に暗号化される。
CC5.8	未承認又は悪意あるソフトウェアの導入を、防止又は検知し、対処する内部統制が実装されている。	悪意のある又は未承認のコードが、データ送信、リムーバルメディア及びポータブル又はモバイルデバイスを通じて、意図的ないし無意識のうちに、論理的アクセス制御又はシステム機能を侵害する。	ワークステーション及びラップトップへのソフトウェアのインストールは、ＩＴサポート要員に制限される。
			アンチウィルスソフトウェアが、ワークステーション、ラップトップ、当該ソフトウェアをサポートするサーバーにインストールされている。
			アンチウィルスソフトウェアは、少なくとも日次で最新のウィルスパターンを受け取れるように設定されている。ネットワーク・オペレーターは、30 日間更新されていない機器の報告を受け取り、それらの機

			器をフォローアップする。
			システムにソフトウェアをインストールする権限は、変更実施担当者及びシステム管理者に制限されている。
CC6.0	システム運用に関する共通規準		
CC6.1	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関して、悪意ある行為、自然災害又はエラーに起因する違反やインシデントについてのシステム構成要素の脆弱性は、監視及び評価され、対応策が既知及び新規の脆弱性を補うために実装される。	違反やインシデントにつながる脆弱性が、適時に検出されない。	ロギング及びモニタリングソフトウェアは、システムインフラストラクチャー構成要素及びエンドポイントシステムからデータを収集するために使われる。また、システムパフォーマンス、潜在的なセキュリティ脅威及び脆弱性、リソースの利用をモニターするため、及び通常ではないシステム活動又はサービスリクエストを検出するために使われる。このソフトウェアは、運用センター及びセキュリティ部署にメッセージを送り、自動的に優先順位の高いインシデントチケット又はプロブレムチケット及び変更管理システム記録事項をオープンする。

			コールセンター要員が、サポートのため電話及び電子メールのリクエストを受け取る。それらの中には、ユーザーパスワードのリセット又は潜在的な違反やインシデントを企業の担当者に通知するリクエストを含むかもしれない。コールセンター要員は、受け取ったリクエストの記録、解決及びエスカレーションのための定義された手順に従う。
		セキュリティやその他のシステム構成情報が、破損又は破壊され、システムが設計されたとおりに機能しなくなる。	自動システムを用いて、フルシステムのバックアップが毎週、差分バックアップが日々行われる。
CC6.2	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで、報告対象の原則を挿入]に関して、論理的及び物理的セキュリティ違反、障害、懸念及び他の苦情を含むインシデントは、確立されたインシデント対応手順に従って識別され、適切な人員に報告され、対処される。	違反やインシデントが、その影響について、識別、優先順位付け又は評価がされない。	運用担当者が、定められた手順に従って、報告された事象を評価する。セキュリティに関する事象は、評価に向けてセキュリティグループに割り当てられる。
		違反やインシデントに対処する是正措置が、適時、適切に実装されない。	運用及びセキュリティ担当者は、定められた手順に従って、報告された事象を解決、エスカレーションする。

			セキュリティ事象（インシデント又は問題）の解決（策）は、日次及び週次で、運用及びセキュリティのグループ会議でレビューされる。
			内部と外部のシステム利用者は、インシデントについて適時に伝えられ、それぞれの側で行うべき是正措置について助言される。
		是正措置が、有効又は十分でない。	事象の解決（策）は、週次の運用とセキュリティのグループ会議でレビューされる。
			変更管理要求は、恒久的な是正のためオープンされる。
		方針や手続の遵守不足が、制裁や改善措置を通じて対処されず、その結果、将来コンプライアンス違反が増加する。	事象の解決（策）は、週次の運用とセキュリティのグループ会議でレビューされる。ユーザー又は顧客に影響を及ぼす関連する事象は、ユーザー又は顧客対応部署に回される。
			企業の方針は、従業員の不正について、謹慎、停職や解雇を含む懲戒を定めている。
		防止措置が、前の事象が発生した後も実装されず、違反とインシデントが再発する。	変更管理要求は、恒久的な是正のためオープンされる。
CC7.0	変更管理に関する共通規準		

CC7.1	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するコミットメント及び要求事項は、システム構成要素の設計、調達、導入（実装）、設定、テスト、修正と維持を含んだシステム開発ライフサイクルを通じて対処される。	コミットメントと要求事項が、システム開発ライフサイクルの間のいくつかのポイントで対処されず、その結果、システムのコミットメントと要求事項を充足していないシステムがもたらされる。	システム変更要求は、変更が変更管理プロセスを通じてセキュリティ、可用性、処理のインテグリティ、機密保持に関するコミットメントと要求事項への潜在的な影響を明らかにするために評価される。
			システム変更は、小規模に分類されるものを除き、実装する前に、最高情報セキュリティ責任者と運用責任者の承認が必要である。
CC7.2	[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するシステムのコミットメント及び要求事項との整合性を保つために、インフラストラクチャー、データ、ソフトウェア及び手続が必要に応じて更新される。	システム構成要素が、要求事項が変更されても更新されず、その結果、システムのコミットメントと要求事項を充足していないシステムがもたらされる。	継続的なリスク評価プロセスと定期的な計画と予算プロセスの間に、インフラストラクチャー、データ、ソフトウェア及び手続は、必要とされる変更について評価される。変更要求は、識別された必要性を基に作成される。
			深刻度の高いインシデントに関しては、根本的な原因分析が準備され、運用責任者にレビューされる。計画されたインシデント及び問題解決（策）を反映するために、根本的な原因分析を基に変更要求は用意され、企業のリスクマネジ

			メントプロセスと関連するリスクマネジメントデータは更新される。
CC7.3	システムの運用中及び監視中に、内部統制のデザイン又は運用の有効性に不備が識別されると、変更管理プロセスが開始される。	識別された不正、インシデント、その他システムの不具合が、変更管理サイクルの中で考慮されない。	深刻度の高いインシデントに関しては、根本的な原因分析が準備され、運用責任者にレビューされる。計画されたインシデント及び問題解決（策）を反映するために、根本的な原因分析を基に変更要求は用意され、企業のリスクマネジメントプロセスと関連するリスクマネジメントデータは更新される。
CC7.4	システム構成要素への変更は、[セキュリティ、可用性、処理のインテグリティ、機密保持又はそれらの組合せで報告対象の原則を挿入]に関するコミットメント及び要求事項に準拠して(起案)承認され、設計され、開発され、設定され、文書化され、テストされ、（リリース）承認され、実装される。	システムの変更が、システムのデザインと運用に責任を負う者によって承認されず、その結果、システムのコミットメントと要求事項を満たす能力を毀損するシステムの変更がもたらされる。	システム変更要求は、要求された変更作業を開始する前に、インフラストラクチャー又はソフトウェアのオーナーと変更諮問委員会によってレビューされ、承認されなければならない。
		システム変更が意図されたとおりに機能せず、その結果、システムのコミットメントと要求事項を満たさない。	機能及び詳細設計が軽微な変更以外（××時間以上）は用意される。機能設計はアプリケーションオーナー、インフラストラクチャーオーナー及びソフトウェア

			オーナーにレビューされ、承認される。詳細設計は、アプリケーション開発の責任者と変更諮問委員会によって要求された変更又は、開発プロジェクトの作業が開始する前に承認される。
			テスト計画、テストデータは作成され、要求仕様テスト、回帰テストに利用される。テスト計画とテストデータは、テスト管理者によりテスト前とテスト完了時にレビューされ、承認され、新たに開発やソフトウェアの変更は、本番移行前に変更諮問委員会によってレビューされる。セキュリティ脆弱性テストは、関連するアプリケーション、データベース、ネットワーク及びオペレーティング・システムの変更に関して実施されるテストに含まれる。
			システムと回帰テストは、承認されたテスト計画とテストデータを使用して、テスト部門によって準備される。計画された結果からの逸脱は、分析され開発者に提供される。

			コードレビュー又はウォークスルーは、定められた規準（コードレビューとウォークスルーを必須とする。）を充足する大きな影響のある変更に要請され、それらは変更について責務を負わない同レベルのプログラマーによってレビューされる。
			変更は、実装前に変更諮問委員会によりレビュー、承認される。
			インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために、定義された企業標準（アクセス管理ソフトウェア、企業設定標準及び標準化されたアクセス統制リストの導入のための要求事項を含む。）がある。
			ハードニング（堅牢化）標準の変更は、インフラストラクチャー管理担当責任者によりレビュー、承認される。
		未承認の変更がシステムになされ、その結果システムのコミットメント及び要求事項を満たさないシステムがもたらされる。	分離された環境が、開発、テスト及び本番環境で使用される。 開発者は、テスト又は本番環境でのソフトウェアを変更することができない。

			開発、テスト及び本番環境間の移行ができるのは、論理的アクセスコントロール及び変更管理ツールにより、変更配置担当者に制限される。
			変更は、実装前に変更諮問委員会によりレビュー、承認される。
		予見不能なシステム導入の問題により、システムの運用が毀損され、結果としてシステムが設計どおりに機能しない。	運用やバックアウト手順の確認を含む引渡プロセスは、全ての移行に利用される。
			システム変更の作業の確認のためにデザインされた実装後手続は、小規模な変更を除き実装の後１週間実施され、結果は、コミットメント及び要求事項を満たすために必要なものとしてユーザー及び顧客と共有される。
		変更管理プロセスにおける両立しない職務の存在（特に承認者、設計担当者、実装担当者、テスト担当者及び所有者）は、結果として意図した機能と異なるシステムの実装をもたらす。	変更管理プロセスは、下記の役割及びその割当てを定義されている。 ・ 変更要求の承認―オーナー又はビジネスユニット管理者 ・ 開発―アプリケーション設計及びサポート部門 ・ テスト―品質保証部門 ・ 実装―ソフトウェア変更管理グループ

可用性に関する追加規準			
A1.1	可用性に関するコミットメント及び要求事項を充足するように、キャパシティ要求を管理し、追加の処理能力の導入を可能にするために、現在の処理能力と使用率が保持され、監視され、評価されている。	現状の処理能力は、システム構成要素における個々の要素の喪失時に可用性のコミットメント及び要求事項を十分に満たさない。	処理能力は、継続的に監視される。
			重要なインフラストラクチャー構成要素は、重要性の分類によりレビューされ最低限の冗長性が割り当てられる。
		システムのコミットメント及び要求事項に従ってシステムの継続的可用性を提供するために、処理能力の必要に応じた監視、計画及び拡張又は変更がされない。	処理能力の監視は、日次で実施される。
			将来の処理要求は、継続的に予測され、計画された能力と比較される。予測は、上級運用責任者により承認される。変更要求は、承認された予測に基づき必要なものとして提起される。
A1.2	可用性のコミットメント及び要求事項を充足するため、物理的設備対策、ソフトウェア、データのバックアッププロセス、復旧用のインフラストラクチャーが設計され、開発され、実装され、稼働し、保持され、監視されている。	環境上の脆弱性と環境条件変化が識別されない、又は物理的設備対策の利用による対処が行われず、結果としてシステム可用性を喪失する。	物理的設備対策は、下記を含み導入される。 ・ 冷却装置 ・ 電源障害の事故のバックアップとしてのバッテリー及び天然ガス発電機 ・ 通信回線の冗長化 ・ 煙探知機

			・　ドライパイプ式スプリンクラー
		環境上の脆弱性が、監視されず、又は環境上の事象の重要性の増加に対応されない。	運用担当者は、各シフトの間の物理的設備対策の状況を監視する。
			物理的設備対策は、少なくとも年次で保守を受ける。
		処理エラー、意図的行為又は環境上の事象により、ソフトウェア又はデータが喪失又は利用できない。	週次のフルバックアップと日次の差分バックアップが、自動化システムにより実行される。
			バックアップは、自動化システムの利用の失敗について監視され、インシデント管理プロセスが自動的に発動される。
			バックアップは、第三者の保管業者により輸送され外部保管される。
		復旧インフラストラクチャーの不備により、システムの可用性のコミットメント及び要求事項が満たされない。	事業継続及び災害対策計画が作成され、年次で更新される。
			企業は、データセンターの災害時のＩＴ運用の再開を可能にするため、第三者復旧施設と契約を行っている。

			企業は、施設の喪失時に他企業の施設での運用の再開を可能とするため、施設のマルチロケーション戦略を利用する。
A1.3	可用性のコミットメント及び要求事項を充足するため、復旧計画に従ったシステム復旧を支援する手続が定期的にテストされている。	コミットメント及び要求事項に従ったシステム運用の復旧を可能とするための復旧計画が、適切にデザインされていない、又はバックアップが十分でない。	事業継続及び災害復旧計画（バックアップの復元を含む。）は、年次でテストされる。
			テスト結果は、レビューされ、継続計画は修正される。
処理のインテグリティに関する追加規準			
PI1.1	処理のインテグリティに関するコミットメント及び要求事項を充足するため、処理エラーを防止し、検出し、是正する手続が存在する。	処理エラー、意図的行為又は環境上の事象により、ソフトウェア又はデータが喪失又は利用できない。	週次のフルバックアップと日次の差分バックアップが、自動化システムにより実行される。
			バックアップは、自動化システムの利用の失敗について監視され、インシデント管理プロセスが自動的に発動される。
			バックアップは、第三者の保管業者により輸送され外部保管される。
		環境上の脆弱性は、システム可用性の喪失についての物理的設備対策の利用による対処が行われない。	物理的設備対策は、下記を含み導入される。 ・ 冷却装置 ・ 電源障害の事故のバックアップとしてのバッテリー及び天然

			ガス発電機 ・　通信回線の冗長化 ・　煙探知機 ・　ドライパイプ式スプリンクラー
		環境上の脆弱性に関するモニターや、環境的事象の厳密さを向上させる活動が実施されていない。	運用担当者は、各シフトの間の物理的設備対策の状況を監視する。
			物理的設備対策は、少なくとも年次で保守を受ける。
		現在の処理能力は、処理誤りが発生する処理要求に対応していない。	処理能力の監視は、日次で実施される。
			重要なインフラストラクチャー構成要素は、最低限の冗長性を維持している。
PI1.2	システム入力は、処理のインテグリティに関するコミットメント及び要求事項に従って、完全に、正確に、適時に測定され、記録される。	入力が、誤って取り込まれる。	様式チェックは、規定値の範囲に入力を制限する。
			データ準備担当者は、文書を受信した日ごとに一括処理し、日付及びバッチチケットのシートの数を入力する。バッチフォームは、購買イメージシステムでスキャンされる。スキャン処理が完了すると、スキャンされたシートは、スキャン担当者により、バッチチケットごとの数量と

			比較される。
			スキャンされたイメージは、OCR処理される。顧客 ID、顧客名及びレコード種別を含むキーフィールドは、システムによりマスターデータと照合される。
			スキャンシートの自由記入欄の記述は、手作業で入力される。当該情報は、２名の異なる担当者により入力される。その入力情報を比較し、誤りがある記録は、解消のため３人目の担当者に送られる。
		入力が取り込まれないか、完全に取り込まれない。	システムエディットは、必須項目について、レコードが承認される前に、完全であることが要求される。
			データ準備担当者は、文書を受信した日付及びバッチチケットのシートごとに一括処理する。バッチフォームは、購買イメージシステムでスキャンされる。スキャン処理が完了すると、スキャンされたシートは、スキャン担当者によりバッチチケットごとの数量と比較される。

			スキャンされたイメージは、OCR処理される。顧客 ID、顧客名及びレコード種別を含むキーフィールドは、システムによりマスターデータと照合される。
			スキャンシートの自由記入欄の記述は、手作業で入力される。当該情報は、2名の異なる担当者により入力される。その入力情報を比較し、誤りがある記録は、解消のため3人目の担当者に送られる。
			バッチコントロールトータルを含む電子ファイルを受信する。取り込み処理の間、取り込んだデータは、アプリケーションにより自動的にバッチトータルと照合される。
		入力が、適時に取り込まれない。	受信した電子ファイルが、受信した時点で処理される。アプリケーションは、処理が完了せずに終了したファイルを監視し、インシデント管理のためのエラーレコードを作成する。
			手作業のデータ入力フォームは、受領時に一括処理される。バッチは、日次入力監督者により、日次処理のための入力がトレースされ、相違点が調査される。

		入力の最終保管は、正しく処理された事の検証のために、そのソースをトレースできない。そして、処理結果の完全性と正確性を検証するために初期の入力にトレースすることができない。	入力は、ID 番号、登録番号、登録情報又はタイムスタンプを符合することにより、初期の入力から出力及び最終保管、出力から入力源をトレースできる。
PI1.3	データは、処理のインテグリティに関するコミットメント及び要求事項に従って承認されたとおりに完全に、正確に、適時に処理される。	データを、処理の途中に紛失する。	入力レコード数は、入力から最終処理までトレースされる。全ての相違点は調査される。
		データが、処理の途中に不正確に変更される。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			出力値は、先行処理の値と比較される。X%以上の差異は、差異報告書上でフラッグが立ち、インシデント管理システムに記録され、そして、出力担当者により調査される。解決（策）は、インシデント管理システムに文書化される。未解決のインシデントは、運用責任者により日次でレビューされる。
			日次、週次及び月次の趨勢報告書は、異常な傾向を把握するため、運用責任者によりレビューされる。

		新しく作成されたデータが、不正確である。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			システムが、生成された値と許容値を比較する。 許容値外の値は、例外値報告書に記載される。例外値報告書の項目は、日次で、出力担当者によりレビューされる。
		処理が、要求された時間内に完了しない。	スケジュールソフトを、ジョブの投入とジョブ実行のモニタリングの制御に使用する。インシデント管理記録は、プロセスエラーが識別されたときに、自動的に生成される。
PI1.4	データは、処理のインテグリティに関するコミットメント及び要求事項に従って、特定された一定期間、完全かつ正確に格納され、保持される。	データが、コミット又は合意したように、使用できない。	アプリケーションデータファイルのミラーイメージは、夜間に作成され、システムの中断又は停止時に、復旧及び復元に使用するため、セカンドシステムに保存される。
		保存されたデータが、不正確である。	保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
		保存されたデータが、不完全である。	データは、顧客へのコミットメント及び要求事項を充足するため、月次で照合される。

PI1.5	システム出力は、処理のインテグリティに関するコミットメント及び要求事項に従って、完全でかつ正確に配布され、保持される。	システム出力が、完全でない。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			出力値は、先行処理の値と比較される。X%以上の差異は、差異報告書上でフラッグが立ち、インシデント管理システムに記録され、そして、出力担当者により調査される。解決（策）は、インシデント管理システムに文書化される。未解決のインシデントは、運用責任者により日次でレビューされる。
			処理レコード合計は、電子申請、手入力及びOCRシステムでスキャンされたシートによる受領レコード合計と月次で、比較される。
		システム出力が、正確でない。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			出力値は、先行処理の値と比較される。X%以上の差異は、差異報告書上でフラッグが立ち、インシデント管理システムに記録され、そして、出力担当者により調査される。解決（策）は、インシデント管理シス

			テムに文書化される。未解決のインシデントは、運用責任者により日次でレビューされる。
			日次、週次及び月次の趨勢報告書は、異常な傾向を把握するため、運用責任者によりレビューされる。
		システム出力が、未承認の受信者に提供される。	アプリケーションセキュリティ（システム）は、承認されたユーザーIDに出力を制限する。
		システム出力を、許可された受信者が利用できない。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			出力は、マスタースケジュールに従って、システムにより生成される。マスタースケジュールの変更は、変更管理プロセスを通じて管理され、カスタマーサービス執行役により承認される。日次で、自動ルーチンは、出力ファイルをスキャンし、全ての必要な出力が生成されたことを検証する。当該ルーチンは、全ての紛失した出力のインシデントの記録を生成する。インシデントチケットは、インシデント管理プロセスで管理される。

PI1.6	データの修正は、処理のインテグリティに関するコミットメント及び要求事項に従って、承認された手続により承認される。	データが、未承認のプロセス又は手続により修正され、結果として、不正確又は不完全なデータになる。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			データへのアクセスは、アクセス管理ソフトウェアにより承認されたアプリケーションに制限される。アクセスルールは、アプリケーション開発プロセスを通じて、情報セキュリティ要員により作成、更新される。
			アプリケーションレベルのセキュリティは、アクセス制御リストの記録を通してアクセス権を付与されている許可されたユーザーのデータへのアクセス、変更、削除の能力を制限する。アクセス管理記録の生成と変更は、アクセス権提供プロセスを通じて行われる。
		データが、承認を得ずに変更される。	保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
		データが、喪失又は破壊される。	保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
			アプリケーションデータファイルのミラーイメージは、夜間に作成

			され、システムの中断又は停止時に、復旧及び復元に使用するため、セカンドシステムに保存される。
機密保持に関する追加規準			
C1.1	機密情報は機密保持に関するコミットメント及び要求事項に従って、システム設計、開発、テスト、実装及び変更プロセスの間、保護されている。	本番環境以外で使用されるデータは、コミットしたとおりに未承認のアクセスから保護されていない。	企業は、テストデータベースの作成に先行して、機密情報をテスト情報に置き換えるデータマスキングソフトウェアを使用して、テストデータを作成する。
C1.2	システム領域内の機密情報は、機密保持に関するコミットメント及び要求事項に従って、入力、処理、保管、出力及び廃棄の間、未承認のアクセス、使用及び開示から保護されている。	機密情報への未承認のアクセスが、処理の途中に行われる。	データへのアクセスは、アクセス管理ソフトウェアにより承認されたアプリケーションに制限される。アクセスルールは、アプリケーション開発プロセスを通じて、情報セキュリティ要員により作成、更新される。
			承認されたアプリケーション以外からの論理アクセスは、データベース管理システム固有のセキュリティを通じて、管理者に制限される。データベース管理システムのためのアクセス管理記録の生成と変更は、アクセス権提供プロセスを通じて行われる。

			アプリケーションレベルのセキュリティは、アクセス制御リストの記録を通してアクセス権を付与されている許可されたユーザーのデータへのアクセス、変更、削除の能力を制限する。アクセス管理記録の生成と変更は、アクセス権提供プロセスを通じて行われる。
		出力に含まれる機密情報への未承認のアクセスが、処理後に行われる。	アプリケーションセキュリティ（システム）は、承認されたユーザーIDに出力を制限する。
			機微情報を含む出力は、安全な出力機器で印刷され、「機密」と記載される。
			専用用紙は、データ記入後、物理的に安全（な場所）に保管される。物理的なアクセスは、保管担当者に制限される。
C1.3	機密情報へのシステム領域外からのアクセス及び機密情報の開示が、機密保持に関するコミットメント及び要求事項に従って、承認された当事者に制限されている。	システム境界を越える伝送により、機密情報が未承認のユーザー企業の要員に提供される。	アプリケーションセキュリティ（システム）は、承認されたユーザーIDに出力を制限する。
			電子的な出力のシステム境界を越えての伝送は、高度暗号化標準（AES）をサポートする承認されたソフトウェアの利用を通じて行わ

			れる。
			保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
			データは、AES をサポートするソフトウェアを使用して暗号化された形式で保存される。
		機密情報が、機密保持コミットメントに違反して、関連する組織、ベンダー又は他の承認された組織に伝送される。	アプリケーションセキュリティ（システム）は、承認されたユーザーID に出力を制限する。
			電子的な出力のシステム境界を越えての伝送は、高度暗号化標準（AES）をサポートする承認されたソフトウェアの利用を通じて行われる。
C1.4	企業は、システムの一部を構成し、機密情報へのアクセスを持つ、製品やサービスを提供するベンダー及び他の第三者から、企業の機密保持要件に整合する機密保持のコミットメントを入手している。	関係する組織及びベンダーの要員が、企業の機密保持コミットメントを認識していない。	正式な情報共有合意書が関係する組織及びベンダーと締結されている。当該合意書には、当該組織に適用される機密保持コミットメントを含んでいる。合意書の項目には、機密データのマーキングや識別、関係する組織及びベンダーの管理下で機密情報を取り扱う基準並びに不要になった機密情報の返還及び廃棄の要求事項を含んでいる。

		機密情報を取り扱う要求事項が、関係する組織又はベンダーに通知又は合意されていない。	正式な情報共有合意書が関係する組織及びベンダーと締結されている。当該合意書には、当該組織に適用される機密保持コミットメントを含んでいる。
C1.5	システムの一部を構成する製品や、サービスのベンダー及び他の第三者機関の機密保持のコミットメント並びに要求事項の遵守状況が、定期的及び必要に応じて評価され、必要な場合是正措置が取られる。	関係する組織及びベンダーのシステムが、機密保持コミットメントを遵守するよう適切にデザインされていないか、有効に運用されていない。	関係する組織及びベンダーのシステムを、ベンダーリスク管理プロセスの一部として調査の対象とする。可能であれば、保証報告書（SOC2報告書）を入手し、評価する。サイト訪問や他の手続を企業のベンダー管理規準に基づいて実施する。
C1.6	機密保持のコミットメント及び要求事項の変更が、内部及び外部ユーザー、製品やサービスが、システムの一部を構成するベンダー及び第三者機関に伝達される。	機密保持実務及びコミットメントが、ユーザー企業の認識又は同意なしに変更される。	最高情報セキュリティ責任者は、機密保持実務及びコミットメントの変更に責任を有する。ユーザー、関係する組織及びベンダーと、それらの変更についてコミュニケーションをとるために、正式なプロセスが用いられる。
		機密保持実務及びコミットメントが、関係する組織又はベンダーの認識なしに変更され、結果としてシステムが要求される実務を遵守できず、コミットメントを充足しない。	最高情報セキュリティ責任者は、機密保持実務及びコミットメントの変更に責任を有する。ユーザー、関係する組織及びベンダーと、それらの変更についてコミュニケーションをとるために、正式なプロセスが用いられる。

			関係する組織及びベンダーの合意書が、機密保持実務やコミットメントの変更を反映して修正される。
			関係する組織及びベンダーのシステムを、ベンダーリスク管理プロセスの一部として調査の対象とする。可能であれば、保証報告書（SOC2報告書）を入手し、評価する。サイト訪問や他の手続を企業のベンダー管理規準に基づいて実施する。

付録Ｃ　一般に公正妥当と認められたプライバシー原則

20. [利用者への注意喚起：一般に公正妥当と認められたプライバシー原則（GAPP）は、セキュリティ、可用性、処理のインテグリティ及び機密保持の原則とは別に改訂中である。したがって、最新の GAPP が確定するまでは、2009 年度版の GAPP を含めている]

一般に公正妥当と認められたプライバシー原則

2009 年８月

序文

AICPA と CICA は、プライバシーがビジネス上の問題であると、強く考えています。企業が直面しているプライバシーの問題に対処しようとすると、我々は企業が効果的にそのプライバシーリスクを管理するための包括的なフレームワークを有していないことにすぐ気づきました。機関（AICPA と CICA）は、プライバシー要件や期待に影響を受ける全ての関係者ニーズに対処するプライバシーフレームワークを開発することで、多大な貢献を提供することを決定しました。これを受け、機関は「AICPA と CICA の一般に公正妥当と求められたプライバシー原則」を開発しました。機関は、プライバシー問題に対処することに関心がある全ての関係者が広く利用できる「原則と規準」を作成しています。

原則と規準は、両国の現行の国際的プライバシー規制要件とベストプラクティスを検討するボランティアにより開発され、更新されています。原則と規準は、双方の機関の

パブリックコメントのための草案の公開を含むデュープロセス手順に従って発行されている。原則と規準の採用は任意です。

当該原則の基礎となる前提は、「良いプライバシーは、良いビジネスである。」という事です。良いプライバシー実務は、コーポレートガバナンスと説明責任の重要な要素です。今日の重要なビジネスの緊急課題の一つは、企業が収集、保管しているパーソナル・インフォメーションの維持をしていくことです。ビジネスシステムとプロセスが、高度化、精緻化されることに伴い、収集されるパーソナル・インフォメーションの量が増加しています。より多くのデータが収集、保管されるため(電子フォーマットが最も頻繁)、紛失、誤用、未承認のアクセス及び未承認の開示を含む様々な脆弱性のリスクに、パーソナル・インフォメーションがさらされる可能性があります。これらの脆弱性は、企業、政府、個人及び世の中全般に問題を提起します。

複数の法管轄区域で活動する企業では、プライバシーリスクの管理がより重要な課題になります。企業が一般に公正妥当と認められたプライバシー原則を遵守していることは、企業が対象となる全ての法令を遵守していることを保証しません。企業は、事業を展開する全ての法管轄区域の重要なプライバシー要件を認識する必要があります。このフレームワークは、一般的なプライバシーのガイダンスを提供しますが、企業が特有の状況を規定する特定の法令について助言や指導を得るためには顧問弁護士に相談してください。

これらの問題を念頭に置いて、地方、国又は国際的な要件を考慮した方法で、プライバシー管理を支援する運用フレームワークとして、AICPA と CICA は一般に公正妥当と認められたプライバシー原則を開発しました。主要な目的は、プライバシーの遵守と有効なプライバシー管理を促進することです。副次的な目的は、通常プライバシー監査と言われるプライバシー検証業務を実施するための適切な規準を提供することです。

プライバシーリスクの有効な管理を維持する企業を支援し、企業のニーズを認識し、公共の利益を反映した、一般に公正妥当と認められたプライバシー原則は、AICPA と CICA の貢献を表します。 開発の追加的な履歴及び追加的なプライバシーリソースは、以下の URL で参照できます。

www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx

www.cica.ca/privacy

一般に公正妥当と認められたプライバシー原則は、AICPA と CICA のウェブサイトからダウンロードできます。

www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx

www.cica.ca/privacy

プライバシー環境は常時変化しているため、一般に公正妥当と認められたプライバシー原則は、適時に更新される必要があり、したがって、この文書に関してのご意見がありましたら、AICPA (GAPP@aicpa.org)又は CICA (privacy@cica.ca)まで、電子メール

でお寄せください。

AICPA
CICA

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、又は国際的に、プライバシー[4]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令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（以下、「GAPP」という。）が策定された。GAPP は、複雑なプライバシー要件を、10 個のプライバシー構成要素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。

GAPP 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。GAPP 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。GAPP は、ガバナンスと監督の実施に責任がある役員会その他の機関にとっても有用な手段であり得る。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コンプライアンスの問題ではなく、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、起こり得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及びモニタリング
- 企業のプライバシーの導入及び管理
- 企業のセキュリティの導入及び管理
- 企業のリスクとコンプライアンスの監督及びモニタリング
- コンプライアンス評価並びにプライバシー及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

プライバシーを保護することは、ビジネスを良くすることである。健全なプライバシー実務は、企業統治及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

[4] 各用語の初出は付録Ａの用語集でアンダーラインを引かれて、序章の用語集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の表の定義にハイパーリンクしている（訳注、翻訳版ではハイパーリンクはしていない。）。

課題の一つは、パーソナル・インフォメーション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、より多くのパーソナル・インフォメーションが企業によって収集されつつある。結果として、パーソナル・インフォメーションが滅失、不正利用、未承認のアクセス及び開示を含む、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、顧客のパーソナル・インフォメーションの適切な収集及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パーソナル・インフォメーションの置き場を管理しようとしている。消費者は、パーソナル・インフォメーションについて非常に憂慮しており、多くの消費者が、パーソナル・インフォメーションの制御を失っていると感じている。更に社会は、特に金融、医療記録、児童についての情報のようなパーソナル・インフォメーションに対する、なりすまし及び未承認の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、パーソナル・インフォメーションが取引した企業によって保護されることを期待している。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許すことはない。それゆえに、プライバシーは全ての企業にとってリスク管理上の問題として有効に対処する必要がある。

プライバシーポリシー及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、ブランド又はビジネス上の関係に与え得る損失
・　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に対する告訴
・　顧客又は従業員の不信
・　ビジネス目的のためにパーソナル・インフォメーションを利用することに対する同意の拒否
・　ビジネスの喪失並びに結果としてもたらされる売上及び市場占有率の低下
・　国際的商取引活動の中断
・　なりすましによる結果責任

国際的なプライバシーへの配慮

複数の国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、一つの国での規制の動きが世界中の個人ユーザー及び顧客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、企業がそれらの国内におけるビジネスをしたい場合、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（EU）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、国際的なコンプライアンスを複雑な業務にしている。この証左として、パーソナル・インフォメーションを収集、保持する場合、いくつかの国が、パ

ーソナル・インフォメーション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、他の国々では、パーソナル・インフォメーションはそれを収集する企業に属するとみなしている。

更に企業は、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コンプライアンスは容易になる。

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コンプライアンスの問題に多くの場合直面している。これらの企業の多くにとって、多くの場合、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。

その上、多くの法域（都道府県、市区町村など）とヘルスケアや金融などの産業では、一定の規制要求がプライバシーに関連している。

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行責任を含めて、ビジネスプロセスの一部を外部委託する場合がある。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が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外部委託する企業は、適切にプライバシー実行責任を管理することを確保する必要がある。

この文書で提示された、GAPP とそれを支える規準は、プライバシーに関する実行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。

これらの原則及び規準がグローバルに適用できるという事実は、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実施できるということにより、外部委託先にも満足を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、「パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関する個人及び企業の権利義務」と定義される。

パーソナル・インフォメーション

「パーソナル・インフォメーション」（個人を識別できる情報と言われる場合がある。）は、識別できる個人に関連するか、又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、又は直接的、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。この目的において個人とは、企業が関係を有する見込み客、既存

顧客、既往顧客、従業員、その他の者を含んでいる。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得るのであれば、パーソナル・インフォメーションとして取り扱われる可能性が高い。パーソナル・インフォメーションの幾つかの例としては、下記が挙げられる。

・　名前
・　住所又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

ある種のパーソナル・インフォメーションは「機微な情報」と位置付けられる。法令により、下記の情報は機微なパーソナル・インフォメーションとして定義されている。

・　医療又は健康状態の情報
・　財務の情報
・　人種又は民族
・　政治的見解
・　宗教的又は哲学的な信念
・　労働組合加入の事実
・　性生活
・　犯罪歴、違反歴を含む情報

機微なパーソナル・インフォメーションは、一般的に、高い水準の保護及び高い注意義務が要求される。例えば、ある法域においては、機微な情報の収集及び利用には黙示の同意ではなく、明示の同意が必要とされる場合がある。

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「非個人情報（nonpersonal information）」と呼ばれる。これは、個人の識別が不明、又は個人との関連が削除された統計上、又は要約されたパーソナル・インフォメーションを含んでいる。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」又は「匿名化」されているからである。非個人情報は、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。しかしながら、その他の法規制や契約（例えば、医療調査や市場調査）により、非個人情報についても、依然としてある種の法的義務を負わされている企業も存在する。

プライバシーか機密保持か

世界中の多くの国で規制によって定義されているパーソナル・インフォメーションと異なり、機密情報の広く認められた単一の定義はない。通信及び取引業務を処理するに当たり、ビジネスパートナーは多くの場合「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
・　値付又はその依頼
・　価格リスト
・　法的文書
・　顧客や業界からの収入

また、パーソナル・インフォメーションと異なり、機密情報にその正確性と完全性を確保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、大抵の事例で契約の取決めによって運用される。AICPA/CICA「セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関する Trust サービス原則、規準及びその例示」を参照すると、機密保持に関する規準についての追加的な情報が提供されている(www.aicpa.org/TrustServices 又は 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

GAPP 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。

プライバシー原則と規準は、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[5]と健全なプライバシー実務に立脚している。GAPP 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積極的に対処することができる。また、GAPP の利用は多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

プライバシー原則と規準は、下記のプライバシー目標に立脚している。

パーソナル・インフォメーションは、企業の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」に定められた規準を充足して、収集、利用、保持、開示及び廃棄される。

一般に公正妥当と認められたプライバシー原則

プライバシー原則は、パーソナル・インフォメーションの適切な保護と管理に欠くこ

---

5 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越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。これらの国際的なプライバシー概念と一般に公正妥当と認められたプライバシー原則との比較表は、オンライン(www.aicpa.org/privacy)で見ることができる。これらの法令及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。

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令と、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、パーソナル・インフォメーションが、収集、利用、保持及び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、パーソナル・インフォメーションの収集、利用、開示に関して黙示又は明示の同意を得る。
4．収集：企業は、通知で識別した目的のためだけにパーソナル・インフォメーションを収集する。
5．利用、保持及び廃棄：企業は、パーソナル・インフォメーションの利用を通知で識別された目的、及び個人が黙示又は明示の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、又は法規制によって必要である限りにおいてパーソナル・インフォメーションを保持し、その後、適切に廃棄する。
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パーソナル・インフォメーション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黙示又は明示の同意をした目的のためだけに、第三者にパーソナル・インフォメーションを開示する。
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パーソナル・インフォメーションを保護する。
9．品質：企業は、通知で識別された目的のために正確、完全、かつ適切にパーソナル・インフォメーションを保持する。
10．モニタリングと徹底：企業は、プライバシーポリシーと手続への準拠性をモニタリングし、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、内部統制の作成と評価の指針として適切、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、実行責任、基準を伝達する書面である。「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。

GAPP の利用

GAPP 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、導入及び伝達
- プライバシープログラムの確立及び管理
- プライバシープログラムのモニタリング及び監査
- パフォーマンスの測定とベンチマーキング

プライバシープログラムの管理には、下記の活動が含まれる。

・　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及びリスク分析
・　導入　－　パーソナル・インフォメーションに関する内部統制の確立を含む、プログラムの行動計画の策定、文書化、導入、制度化
・　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 GAPP 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、更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、全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、プライバシーへのコンプライアンス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。 [資源の配分] 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及び財務的並びにその他の資源が特定される。	[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」（GAPP）は企業が対処すべき重要な構成要素を識別する上で役に立つ。 [資源の配分]　GAPPを利用して、企業はシステム管理やプライバシー又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、更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。GAPP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、販促及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及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一般的なのは診断評価である。 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決定することである。	GAPP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。 GAPP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、診断による勧告が実施される。導入には、全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、実行責任を割り当て、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組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。	GAPP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するためのシステム、手続及びプロセス □　プライバシーコンプライアンスのために変更された書式、パンフレット及び契約書 □　社内及び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ーすることも含まれる。モニタリングには、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	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GAPPを利用できる。また、GAPP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手続を決定することに

	援技術が含まれる。	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及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、GAPP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、公認会計士と勅許会計士）は、証明及び保証サービス（attestation and assurance services）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、GAPP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、特定の業界又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。

規準の中には、ある種の企業又はプロセスに直接適合しないものもある。規準が適合しないと考えられる場合、企業は将来の評価を支持する意思決定の調整を考慮すべきである。

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		
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。 1．通知（2.1.0参照） 2．選択と同意（3.1.0参照） 3．収集（4.1.0参照） 4．利用、保持及び廃棄（5.1.0参照） 5．アクセス（6.1.0参照） 6．第三者への開示（7.1.0参照） 7．プライバシーのためのセキュリティ（8.1.0参照） 8．品質（9.1.0参照） 9．モニタリングと是正措置（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コンプライアンス違反の顛末は、企業のパーソナル・インフォメーションを収集、利用、保持、開示することに実行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	企業は、下記を実施する。 ・　定期的に社内要員に（例えば、ネットワーク又は ウェブサイト上に）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承認後速やかに伝達する。 ・　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。	（ここでいう）プライバシーポリシーは、パーソナル・インフォメーションの保護に関係があるセキュリティポリシーを含んでいる。

る。		
1.1.2　ポリシーに関する実行責任と説明責任 企業のプライバシーポリシーを文書化し、導入し、是正措置し、モニタリングし、更新することに対して、個人又はグループに実行責任と説明責任が割り当てられる。このような個人又はグループの名前と彼らの実行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行責任とは異なるプライバシーに関する実行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行責任を割り当てる。 指名された人又はグループの権限と説明責任は明確に文書化される。実行責任には下記の事項が含まれる。 ・　パーソナル・インフォメーションの機密度合いを分類し、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 ・　ポリシー及び実務への準拠度合いをモニタリングし、訓練又は理解度を改善する対策に着手すること	プライバシーに対して説明責任がある者として特定された個人は、企業内部者であるべきである。

	役員会は定期的に、企業統治の通常レビューにプライバシーを含める。	
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。 ・　上級管理職又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と手続の法令との整合性 ポリシーと手続が少なくとも毎年そして関連法令が改正される都度レビューされ、適用される法令の要件と比較される。プライバシーポリシーと手続は、適用される法令の要件を充足するように修正される。	企業の弁護士又は法務部は、下記に従う。 ・　いずれの個人情報保護法令が、企業が操業する法域で適用されるかを確認する。 ・　企業に適用されるその他の基準を識別する。 ・　適用される法令と適切な基準と整合していることを確保するために、企業のプライバシーポリシーと手続をレビューする。	法令の要件に加えて、企業によっては国際標準化機構（ISO）の基準への準拠を選択し、又は事業を行う条件としてカード業界の基準等に準拠することを要求される場合がある。企業は、このプロセスにそうした基準を含める場合がある。
1.2.3　パーソナル・インフォメーションの識別と分類 パーソナル・インフォメーションと機密情報の種類、それらの情報の取扱いに係る関連するプロセス、システム、第三者が特定されている。それ	企業は、下記を含む情報分類ポリシーとプロセスを有している。 ・　分類のプロセス（それは、情報を以下のカテゴリーの一つ以上に識別して、分類する）。 －ビジネス上の機密情報 －パーソナル・インフォメーション（機微その他のパー	

らの情報は、企業のプライバシーポリシー、関連するセキュリティポリシー及び手続の対象となっている。	ソナル・インフォメーション） －ビジネス一般の情報 －公知の情報 ・　パーソナル・インフォメーションを取り扱うプロセス、システム、第三者の識別 ・　それぞれの情報カテゴリーに適用される特定のセキュリティ及びプライバシーポリシー	
1.2.4　リスク評価 リスク評価プロセスは、リスクベースラインを確立し、少なくとも年に１回、新しい又は変化したパーソナル・インフォメーションのリスクを識別し、当該リスクへの対応を策定し、更新するのに使用される。	定期的に企業のパーソナル・インフォメーションのリスクを識別するためにプロセスが整備されている。そのようなリスクは、社外（業者による情報の滅失又は法的な要求事項に従わないことなど）にも社内（保護のない機密情報のメール送信など）にもある場合がある。新しい又は変化したリスクを識別したときに、プライバシーリスク評価と対応戦略を更新する。それらのプロセスは、プライバシーインシデント管理、苦情・紛争解決プロセス、モニタリング活動等の実務のような要因を考慮する。	理想的には、プライバシーリスク評価は、セキュリティリスク評価に統合され、企業の総合的ERMプログラムの一部であるべきである。役員会はプライバシーリスク評価の監督・レビューを行うべきである。
1.2.5　プライバシーポリシーと手続のコミットメントへの整合性 社内要員又は企業のアドバイザーが、プライバシーポリシー及び手続と契約書の整合性をレビューし、何らかの不整合に対応する。	経営者と企業の弁護士又は法務部が、企業のプライバシーポリシーと手続との整合のために全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。	

1.2.6　インフラストラクチャーとシステム管理 新しい個人情報取扱プロセスが導入される場合及び当該プロセス（第三者又は委託先に外部委託された活動を含む。）に変更がなされる場合に、潜在的なプライバシーに対する影響が評価され、プライバシーポリシーに準拠して、パーソナル・インフォメーションの保護が継続される。この目的のために、個人情報取扱プロセスは、下記に関する設計、取得、導入、設定、管理、変更を含む。 ・　インフラストラクチャー ・　システム ・　アプリケーション ・　ウェブサイト ・　手続 ・　製品とサービス ・　データベース及び情報リポジトリ ・　モバイルコンピューティング又はその他の類似した電子機器 企業のプライバシーに関するポリシーと手続に基づき、情報が匿名化されない場合、又は保護されない場合、処理及びシステム・テスト並びに開	下記の手続がプライバシーへの影響に対処するために採用されている。 ・　経営者は、新しい又は著しく変更された製品、サービス、ビジネス実務、インフラストラクチャーのプライバシーへの影響を評価する。 ・　企業は、パーソナル・インフォメーションを収集、利用、保持、開示及び廃棄するために利用される全ての情報システム及び関連する技術（手作業の手続、アプリケーション・プログラム、技術インフラストラクチャー、組織構造、ユーザー及びシステム人員の実行責任を含む。）のために文書化されたシステム開発及び変更管理プロセスを利用する。 ・　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。 ・　パーソナル・インフォメーション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。全てのテストデータは、匿名化される。統制されたテストデータベースが、一つのプログラムに対する変更が他のパーソナル・インフォメーションを処理するプログラムに不利な影響を及ぼさないようにする完全復帰テストを維持す	ある法域では、匿名化しないか、本番情報並みのポリシーで求められるレベルの保護をしない場合、個人情報のテスト及び開発への利用を禁止している。

発におけるパーソナル・インフォメーションの使用は禁止される。	る。 ・　旧システムから新システム又は変更されたシステムへの移行時には、パーソナル・インフォメーションのインテグリティ及び保護を確保する手続が維持されている。 ・　パーソナル・インフォメーションを処理するシステム及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、セキュリティ責任者、業務部門管理者及びＩＴ管理者による文書化と承認を要求する。同水準のパーソナル・インフォメーションの保護のために、緊急の変更は文書化される必要があるが、その文書化、承認は事後的でもよい。 情報システム部門は、パーソナル・インフォメーションを処理する全てのソフトウェア及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維持する。 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。 コンピュータ化されたシステムが関わるところでは、パーソナル・インフォメーションへのアクセスが適切に制限されるのを確保するために開発、テスト、本番ライブラリの使用の分離などのような適切な手続	

	に準拠している。 新しいシステムと変更、導入に責任がある人員、及び新しい又は変更されたプロセスと、アプリケーションのユーザーにプライバシーに関連する研修や訓練を提供する。個々の役割と責任はプライバシーと関連して割り当てられる。	
1.2.7 プライバシーインシデントと違反の管理 文書化されたプライバシーインシデントや違反の管理プログラムは下記を含むが、それに制限されない。 ・ プライバシーインシデントや違反の識別、管理、解決のための手続 ・ 定義された責任 ・ インシデントの深刻度を識別するプロセス及び必要な行動を決定するプロセス及び上申手続 ・ 必要により、利害関係者への違反通知を含む、違反した法令に従うプロセス ・ インシデントや違反に実行責任がある従業員や第三者の復旧・処罰・懲戒などの説明責任のプロセス ・ 下記に基づく必要なプログラム変更を識別	公式かつ包括的なプライバシーインシデントと違反（以下を特定する）管理プログラムが実装されている。 ・ プライバシーインシデントと違反であるかどうかを評価する違反対応チームのメンバーに報告されるか、関連するセキュリティ、プライバシーとセキュリティに責任がある要員により、インシデントの深刻度を分類し、必要な行動を開始して、必要な関与を決定する。 ・ プライバシー管理最高責任者（CPO）は、プログラムのために総合的な責任を持って、プライバシーとセキュリティ運営委員会によってサポートされ、違反対応チームによって補助される。パーソナル・インフォメーションを含まないインシデントと違反は、CIOの責任である。 ・ 企業にはプライバシー違反通知ポリシーがある。ポリシーは(a)違反で影響を受けるデータ主体に関連する他の適切な法域における社内の通知と関連する要件を識別	企業によっては、それらが作動する全ての法域内に一貫した違反通知ポリシーを採る場合がある。最小限で、必要に迫られて、そのようなポリシーはどの法域でも包括的な法的要件に基づく。

するための実際のインシデントの定期的レビュー（少なくとも年一度）プロセス －インシデントのパターン、根本原因 －内部統制環境又は外部の要件（法令）における変化 ・　定期的なテスト又はウォークスルー（少なくとも年一度）プロセスと関連する必要な復旧プログラム	するためのプロセス、(b)法令やポリシーによって要求される場合、利害関係者の通知への違反に求められる評価のプロセス、(c)適時に通知を提供するためのプロセスによってサポートされる。企業は、通知プロセスと必要なら信用モニタリングサービスを管理するための第三者との合意を有している。 ・　プログラムは、インシデントの種類、深刻度又は両方に基づいて、経営者、顧問弁護士、役員会までの明確な上申プロセスを含む。 ・　プログラムは必要なとき、司法当局、行政当局又はその他の当局に連絡するためのプロセスについて詳しく説明している。 ・　新規採用者とチームメンバーのためのプログラムの訓練、及び一般スタッフのための周知訓練が、毎年及び重要なプログラムの変更が導入される時と大きなインシデントの後に行われる。プライバシーインシデント・違反管理プログラムは、下記についても特定する。 ・　主要なプライバシーインシデントの後、正式なコンプライアンス評価が内部監査又は社外コンサルタントによって行われる。 ・　実際のインシデントの四半期レビューが行われ、必要なプログラム更新が下記に基	

	づいて識別される。 ―インシデントの根本原因 ―インシデントのパターン ―内部統制環境と法令環境における変化。 ・　四半期レビューの結果が毎年プライバシー運営委員会と監査委員会に報告される。 ・　重要な指標が定義され、追跡され、四半期で上級経営層に対し報告される。 ・　プログラムは、少なくとも６か月ごと、及び重要なシステム又は手続上の変更の実施後に直ちにレビューされる。	
1.2.8　支援のための資源 プライバシーポリシーを導入し、支援するための資源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。	
1.2.9　要員の資格 企業は、パーソナル・インフォメーションのプライバシーと、セキュリティを保護することに実行責任がある要員の資格を確立して、このような実行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。	パーソナル・インフォメーションのプライバシーと、セキュリティを保護することに実行責任がある内部要員の資格は、下記の手続によって確保される。 ・　公式の職務記述書（重要なプライバシー管理職位の実行責任、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。）並びに公式の雇用契約及び機密保持契約 ・　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。）	
1.2.10　プライバシーの意識向上と訓練 役割と実行責任に応じて選抜された要員に対して、企業のプライバシーポリシー及び関連事項に関するプライバシー意識向上プログラムが提供される。	双方向的なプライバシー及びセキュリティのオンライン意識向上コースが、全ての従業員に毎年要求される。新入社員、契約者その他の者は、採用後１か月目以内にこのコースを完了しなければならない。プライバシー、関連するセキュリティポリシー、手続、法令の問題、インシデント対応、関連する話題を含む徹底的な訓練を提供する。当該訓練は下記の要領で行う。 ・　パーソナル・インフォメーションに接近する手段を持っているか、又はパーソナル・インフォメーションの保護に責任がある全社員に毎年必要である。 ・　従業員の仕事の責任に適合する。 ・　外部の訓練と会議によって補われる。 企業のプライバシー訓練と意識向上コースの出席はモニターされる。 現在の法令、産業、企業ポリシー及び手続要件を反映するために訓練と意識向上コースを見直し、更新する。	

1.2.11　規制及びビジネス要件の変化 企業が業務を行う法管轄区域において、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。 ―法令 ―SLAを含む契約 ―業界の要件 ―ビジネス運用とプロセス ―人員、役割と責任 ―技術 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。 ・　法令環境 ・　業界の要件（通販協など） ・　第三者とのSLA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又は顧問弁護士によってレビューされ、承認される。） ・　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行責任を割り当てられた人員 ・　技術（導入前）	理想的には、これらの手続はリスク評価プロセスと調整されるべきである。企業はまた、何も要求されない法域での違反通知のような、最新の健全な実務を考慮すべきである。

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、パーソナル・インフォメーションが、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。		
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。 a．パーソナル・インフォ	企業のプライバシー通知は、下記に従う。 ・　収集されるパーソナル・インフォメーション、当該情報の情報源、当該情報が収集される目的を記述する。	下記のような場合、パーソナル・インフォメーションが開示される条件を通知において記述する場合がある。 ・　公共の安全保障又は防

メーションを収集する目的 b．選択と同意（3.1.1参照） c．収集（4.1.1参照） d．利用、保持及び廃棄（廃棄）（5.1.1参照） e．アクセス（6.1.1参照） f．第三者への開示（7.1.1参照） g．プライバシーのためのセキュリティ（8.1.1参照） h．品質（9.1.1参照） i．モニタリングと是正措置（10.1.1参照） 当該個人以外の情報源から情報が収集される場合は、当該情報源は通知で記述される。	・　機微なパーソナル・インフォメーションを収集する目的、それが法律上の要件の一部をなすかどうかを示す。 ・　求められた情報を提供しなかった場合の結果を記述する。 ・　購買パターンなどのような一定の情報が作成される場合があることを示す。 ・　様々な方法（例えば、面談、電話、申込書、アンケート、又は電子的に）で提供されるかもしれない。しかしながら、書面の通知は望ましい方法である。	衛目的のためのある特定の処理 ・　公衆衛生又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、又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、どのようにパーソナル・インフォメーション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セクション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。
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、(a)パーソナル・インフォメーションが収集されるとき若しくはその前、又は実務的範囲でなるべく早く、(b)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若しくはその前、又は実務的範囲でなるべく早く、(c)パーソナル・インフォメ	プライバシー通知は、下記に従う。 ・　パーソナル・インフォメーション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。 ・　企業にパーソナル・インフォメーションを提出すべきかどうか決めることができるように適時な方法で提供する（それはつまり、情報が収集されるときにおいて若しくははその前に、又は実務的範囲でなるべく早くということ）。	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。

ーション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に実施される。	・　個人が、企業にパーソナル・インフォメーション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、企業のウェブサイトに通知を開示する、又は郵便で書面の通知を送る、若しく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。	
2.2.2　対象とされる企業の活動 プライバシーポリシーと手続によって、対象とされた企業の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 ・　事業領域と関係会社 ・　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、顧客及び潜在顧客の情報）の種類 ・　情報源（例えば、メールオーダー又はオンライン） 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得るとき（例	

	えば、企業のウェブサイトに類似した別のウェブサイトにリンクを貼るか、又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、かつ公知された用語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。 ・　平易で、単純な用語で記述される。 ・　適切にラベルを貼られた、明瞭で、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、ウェブサイト上に示されている。	異なった子会社又は事業領域について複数の通知を利用する場合は、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場合がある。 例示的な通知は、多くの場合、ある特定の業界と収集、利用、保持、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、パーソナル・インフォメーションの収集、利用、開示に関して黙示又は明示の同意を得る。		
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 (a)パーソナル・インフォメーションの収集、利用、開示につき当該個人にとって可能な選択、(b)法令に別段の定めがない限り、パーソナル・インフォメーションの収集、利用、開示に黙示又は明示の同意が要求されることについて企業から個人に通知する。	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。 ・　パーソナル・インフォメーションの収集、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及びプロセス ・　取引又はサービスのために必要なパーソナル・インフォメーション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パーソナル・インフォメーションは、提供する必要がない。 ・　法的又は契約上の制限事項及び合理的な通知によって、後日、希望が変更されたり、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パーソナル・インフォメーションの性質と収集の方法によって異なる（例えば、ニュースレ	ある種の法令（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、かつ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、法律によって許容又は認められているとき。

	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。）。	
3.1.2　同意の拒否又は撤回の結果 パーソナル・インフォメーションが収集されるとき、当該情報の提供を拒否した場合の結果又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。 ・　パーソナル・インフォメーション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パーソナル・インフォメーション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る、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　黙示又は明示の同意 黙示又は明示の同意が、パーソナル・インフォメーションが収集されるとき若しくはその前、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要望は確認されて、実行される。	企業は、下記に従う。 ・　適時な方法で個人の同意を得て、（パーソナル・インフォメーションが収集されるとき若しくはその前、又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（書面で又は電子的に）。 ・　個人の希望の変更を文書化し、管理する。 ・　個人の希望が適時に実行されることを確保する。	

	・　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。 ・　企業内及び第三者によるパーソナル・インフォメーションの利用が、個人の希望のとおりであることを確保する。	
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、当該個人から黙示又は明示の同意がこのような新しい利用又は目的の前に得られる。	パーソナル・インフォメーション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パーソナル・インフォメーションを利用するために同意又は同意の撤回を得て、文書化する。 ・　パーソナル・インフォメーション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確保する。	
3.2.3　機微な情報のための明示の同意 法令に別段の定めがない限り、機微なパーソナル・インフォメーションを収集、利用、開示する場合には、個人から直接、明示の同意を得る。	企業は、個人が明示の同意を提示した場合に限り、機微な情報を収集する。「明示の同意」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。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、明示の同意が個人から直接得られ、文書化される。これはとき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、通常は明示の同意を得るよう努めることとしている。 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

		する個人の保護の法律」の第７章では、「機微なデータの収集及び処理は禁止する」としている。しかしながら、機微なデータの収集及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又は社会保険番号は、機微な情報として捉えている。
3.2.4　個人のコンピュータ又は他の類似の電子機器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その他類似の機器経由でパーソナル・インフォメーションが転送される前に、当該個人の同意を得る。	企業は、顧客のコンピュータその他類似の電子機器内にパーソナル・インフォメーション（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その他類似の電子機器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パーソナル・インフォメーションを転送するようなソフトウェアをダウンロードしない。	コンピュータその他類似の電子機器から情報を採取し、抽出して、その後、パーソナル・インフォメーション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パーソナル・インフォメーションを収集する。		
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		特定の法域（例えば、欧州の国）では、パーソナル・インフォメーションを収集する企業に対して、規

ポリシーはパーソナル・インフォメーションの収集を扱う。		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、パーソナル・インフォメーション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、収集されたパーソナル・インフォメーションの種類及びパーソナル・インフォメーションの収集方法、購買パターンのような個人に関する情報が作成又は要求されるかどうかを開示する。	
4.1.2　収集したパーソナル・インフォメーションの種類と収集の方法 収集したパーソナル・インフォメーションの種類、収集の方法は、クッキー又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。	収集されたパーソナル・インフォメーションの種類の例は、下記のようなものである。 ・　財務（例えば、銀行口座情報） ・　健康（例えば、肉体的精神的健康状態又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） パーソナル・インフォメーションの収集方法及び第三者情報源は、下記のようなものである。 ・　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、又はウェブビーコン 企業のプライバシー通知はクッキーとウェブビーコンの利用及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（EU））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 パーソナル・インフォメーションの収集は、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パーソナル・インフォメーションを指定し、任意のパーソナル・インフォメーションと区別する。 ・　定期的にパーソナル・インフォメーションを必要とする企業のプログラム又はサービスをレビューする（例えば、５年ごと又はプログラム若しくはサービスが変わる度に）。 ・　機微なパーソナル・インフォメーションが収集されるとき、明示の同意を得る（3.2.3「機微な情報のための明示の同意」を参照）。 ・　パーソナル・インフォメーション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、全ての任意のデータが識別されていることをモニターする。	
4.2.2　公正かつ合法的な手段による収集 パーソナル・インフォメーションが得られることを確認する前に、パーソナル・インフォメーションの収集方法が、(a)公正であること、脅迫又は騙しがないこと、(b)合法的であること、パーソナル・インフォメーションの収集に関連する全ての関連する法令又は慣習法を遵守し	企業の経営者、プライバシー責任者、法務委員会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。 ・　個人に通知せずにパーソナル･インフォメーションを収集するため､企業のウェブサイトに､クッキーとウェブビーコンのようなツールを使う。 ・　個人に通知せずに､他のソースのパーソナル･インフォメーションと個人のウェブサイトアクセス時に集めた情

ていることについて、経営者によってレビューされる。		報をリンクする。 ・　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令の要求事項について留意すべきである（例えば、カナダの企業がヨーロッパ人についてのパーソナル・インフォメーションを収集する場合、ヨーロッパ特有の法律上の要求事項の適用を受ける場合がある。）。 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場合がある。
4.2.3　第三者からの収集 経営者は、パーソナル・インフォメーションを収集する第三者（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。 ・　第三者情報源からパーソナル・インフォメーション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と同意の種類をレビューする。	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。
4.2.4　個人について作成される情報 個人は、企業がその利用のために個人に関する追加の情報を作成又は取得する場合に通知される。	企業のプライバシーポリシーは、第三者ソース、ウェブ訪問履歴、クレジット、購買履歴などの個人に関する情報を作成又は要求する場合があることを通知する。	

利用、保持及び廃棄

利用、保持及び廃棄の規準	規準の例示と説明	追加的な留意事項
5.0 企業は、パーソナル･インフォメーションの利用を通知で識別された目的、及び個人が黙示又は明示の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、又は法令によって必要である限りにおいて、パーソナル･インフォメーションを保持し、その後、適切に廃棄する。		
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パーソナル・インフォメーションの利用、保持及び廃棄を扱う。		
5.1.1 個人への伝達 パーソナル・インフォメーションが、(a)法令に別段の定めがない限り、黙示又は明示の同意があった場合、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、(b)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、又は法令によって特に必要とされた期間にわたって保持され、(c)滅失、盗難、誤用、未承認のアクセスを防止しつつ廃棄される、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、パーソナル・インフォメーションの利用を記述する。例えば、下記のようなものである。 ・ ビジネス取引の処理（例えば、クレームと製品保証、給与、税金、特典、ストックオプション、賞与又はその他の報酬スキーム） ・ 製品又はサービスについての問合せ若しくは苦情の取扱い、又は製品若しくはサービスの販売促進の相互作用 ・ 製品設計と開発又は製品若しくはサービスを購入すること ・ 科学的若しくは医療の研究活動、マーケティング、調査又はマーケット分析に対する参加 ・ ウェブサイトの個人化、又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、パーソナル・インフォメーション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令によって特に必要とされた期間にわたって保持され、その後、セキュアに廃棄されるか、又はいかなる個人も識別できないように匿名化されると説明する。	
5.2 手続と内部統制		
5.2.1　パーソナル・インフォメーションの利用 法令に別段の定めがない限り、パーソナル・インフォメーションは、個人が黙示又は明示の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。	下記を確保するために、システムと手続がパーソナル・インフォメーション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。 ・　適用される法令を遵守している。	特定の規制では、パーソナル・インフォメーションの利用について特殊な条項を有している。例えば、GLBA、医療保険の携行性及び責任法（HIPAA）、児童オンラインプライバシー保護法（COPPA）。
5.2.2　パーソナル・インフォメーションの保持 法令に別段の定めがない限り、パーソナル・インフォメーションが、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。	企業は、下記に従う。 ・　保持ポリシーと廃棄手続を文書化する。 ・　保持ポリシーに準拠して、アーカイブ及びバックアップコピーを保持し、消去し、廃棄する。 ・　パーソナル・インフォメーションが、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確保する。	特定の法律では、パーソナル・インフォメーションの保持期間が特定されている。例えば、HIPAAは、パーソナル・インフォメーションの作成又は最終利用後、電子医療情報については３年、紙の医療情報については６年の保持期間を定めている。法令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又は

	契約の要件について、通常のポリシーへの例外があるとき、保持ポリシーを確立するときに、留意すべきである。	労基法に従って保持される必要があるかもしれない。
5.2.3 パーソナル・インフォメーションの廃棄、破壊、編集 保有する必要のなくなったパーソナル・インフォメーションは、滅失、盗難、誤用、未承認のアクセスを防ぐ方法で匿名化されるか、廃棄される又は無効にされる。	企業は下記に従う。 ・ 保管方法（電子的、光学的媒体、紙ベース）に関係なく、保持ポリシーに従って記録を消去し、廃棄する。 ・ 廃棄ポリシーに従って、オリジナルの、アーカイブ、バックアップ、臨時の又は個人的なコピー記録を廃棄する。 ・ パーソナル・インフォメーションの廃棄を記録する。 ・ 技術の限界の中で必要に応じて、例えば、取引終了後にクレジットカード番号を削除するように、個人に関して指定されたパーソナル・インフォメーションを探索し、削除する又は編集する。 ・ 必要に応じて法令で特定された目的を実現させるために、匿名化を必要としないパーソナル・インフォメーションを定期的、かつ系統的に廃棄又は消去する。 契約の要件について、通常のポリシーへの例外があるとき、廃棄、破壊、編集実務を確立するときに留意すべきである。	パーソナル･インフォメーションのセキュアな破棄サービスを提供する業者のサービスを､利用することに対して留意すべきである。これらの業者は、廃棄証明書を必要に応じて提供している。DVD､CD､マイクロフィルム､マイクロフィッシュなどの格納技術は､そのような媒体に含まれた全体のデータベースを破壊しなければ、個々の記録の消去ができない場合がある。

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パーソナル・インフォメーション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は、パーソナル・インフォメーション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パーソナル・インフォメーション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。 ・　個人が自身のパーソナル・インフォメーション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、自身のパーソナル・インフォメーションを更新し、修正するための方法を解説する（例えば、書面で、電話で、電子メールで又は企業のウェブサイトを利用して）。 ・　パーソナル・インフォメーションに関する不同意がどう解決されるかを説明する。	
6.2 手続と内部統制		
6.2.1　パーソナル・インフォメーションへの当該個人によるアクセス 個人は、企業が自身のパーソナル・インフォメーション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パーソナル・インフォメーシ	下記の手続が採用されている。 ・　企業がパーソナル・インフォメーションを保有又は統制しているかどうかを評価する。 ・　当該パーソナル・インフォメーションにアクセスを得るためにとられる段階を伝達する。 ・　適時に、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又は電子媒体で、依頼に応じて、パーソナル・インフォ	ある種の法令が下記を特定している。 ・　パーソナル・インフォメーションへのアクセス提供条文及び要求事項（例えば、HIPAA） ・　パーソナル・インフォメーションへのアクセス依頼は書面で行うという要件

ョンにアクセスを得ることができる。	メーション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。	
6.2.2　個人の身元の確認 パーソナル・インフォメーション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。 ・　彼らのパーソナル・インフォメーションにアクセスする。 ・　機微な、又はその他のパーソナル・インフォメーション（例えば、住所又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、社会保障番号又は社会保険番号）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（又は同等物）が利用されることを要求する。	認証の程度は、パーソナル・インフォメーションの種類と機密度合い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。 ・　ウェブサイト ・　対話型の音声応答システム ・　コールセンター ・　対面
6.2.3　分かりやすいパーソナル・インフォメーション、時間枠、コスト パーソナル・インフォメーションが、分かりやすい形式、合理的	企業は、下記に従う。 ・　（例えば、コード、番号、過度に技術的又は専門的な用語ではない）分かりやすい形式かつ、個人と企業の双方にとって便利な形式で、個人にパーソナル・インフォメーションを提供する。	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、ビジネス及び顧客との関係に利点があるため、個人に対して、彼らのパーソナル・インフォメーションへのアクセスを提供

な時間、合理的なコストで個人に提供される。	・　要求されたパーソナル・インフォメーションを探すために合理的な努力をし、パーソナル・インフォメーション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、直接又は間接的に、別の人を識別しないことを確保するのに正当な注意を払う。 ・　他のビジネス取引のために、又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、パーソナル・インフォメーションへのアクセスを提供する。 ・　アーカイブ又はバックアップシステム及び媒体に置かれたパーソナル・インフォメーションへのアクセスを提供する。 ・　アクセスを要求した時点又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。 ・　企業がパーソナル・インフォメーション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。 ・　パーソナル・インフォメーションを調査するために、適切な物理的空間を提供する。	する場合がある。
6.2.4　アクセスの拒否 パーソナル・インフ	企業は、下記に従う。 ・　なぜパーソナル・インフォメーションへのアクセスが拒否され得るかの理由を記述する。	ある特定の法令（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

ォメーションへのアクセス要求を拒否する理由、該当する場合には、そのアクセスを拒否する企業の法的根拠について、もしあれば、当該拒否に抗弁できる法令による具体的な許可や要求に関する個人の権利について、当該個人に書面で通知される。	・　全てのアクセス拒否と未解決の苦情と紛争を記録する。 ・　パーソナル・インフォメーション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。 ・　パーソナル・インフォメーション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。 ・　パーソナル・インフォメーションへのアクセスが拒否された場合、公式の苦情提起プロセスを提供する。 ・　企業の法的な権利と該当する場合は、抗弁できる個人の権利を伝達する。	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　パーソナル・インフォメーションの更新又は訂正 個人は、企業が保持しているパーソナル・インフォメーションを更新又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、企業は、当該パーソナル・インフォメーションがかつて提供された第三者に対して、情報の更新又は訂正を行う。	企業は、下記に従う。 ・　パーソナル・インフォメーションの記録を更新又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、企業のウェブサイトの利用）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）個人が更新又は訂正するパーソナル・インフォメーションの正確性と完全性を立証する。 ・　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、パーソナル・インフォメーション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、パーソナル・インフォメーションは企業がそれ以上の処理を停止するのでなければ、消去することができない。

6.2.6　合意未達の文書 個人がパーソナル・インフォメーション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、パーソナル・インフォメーションが完全、かつ正確であるかどうかに関して意見を異にする場合は、個人はパーソナル・インフォメーションが完全で、正確でないということを記述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、パーソナル・インフォメーションが完全、かつ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、パーソナル・インフォメーション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。 ・　パーソナル・インフォメーションへのアクセスが要求され、又はアクセスが実際に提供された場合、合意未達の文書では、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、かつてパーソナル・インフォメーション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。	10.1.1「個人への伝達」、10.2.1「問合せ、苦情及び紛争処理」、10.2.2「紛争解決と調停」を参照。 特定の規制（例えば、HIPAA）が、個人からの要求の拒否及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。

第三者への開示

2009(完成版)		
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及び、個人が黙示又は明示の同意をした目的のためだけに第三者にパーソナル・インフォメーションを開示する。		
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パーソナル･インフォメーションの第三者への開示を扱う。		
7.1.1　個人への伝達 法令に別段の定めがない限り､通知で識別された目的及び､黙示又は明示の同意をした目的のためだけに､第三者にパーソナル･インフォメーション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。 ・　第三者とパーソナル・インフォメーションを共有するための実務（該当ある場合は）及び情報の共有理由を記述する。 ・　パーソナル・インフォメーションを開示する第三者及びその等級を識別する。 ・　個人は、法令に別段の定めがない限り、(a)通知で識別された目的及び(b)黙示又は明示の同意をした目的のためだけに、第三者にパーソナル・インフォメーション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パーソナル・インフォメーション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、不正確なパーソナル・インフォメーションも変更されるようにする、第三者との共有パーソナル・インフォメーションの更新方法
7.1.2　第三者への伝達 パーソナル･インフォメーションの取扱いに要求されるプライバシーポリシーその他の特定の指示、要求事項は、パーソナル･インフォメーションが開示される第三者に伝達される。	第三者とパーソナル・インフォメーションを共有するに先立って、企業は、パーソナル・インフォメーションの取扱いに要求されるプライバシーポリシーその他の特定の指示、要求事項を伝達して、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合意書を取得する。	
7.2 手続と内部統制		

7.2.1　パーソナル・インフォメーションの開示 法令に別段の定めがない限り、通知で識別された目的及び黙示又は明示の同意をした目的のためだけに第三者に、パーソナル・インフォメーションが開示される。	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黙示又は明示の同意をしなかった場合、第三者へのパーソナル・インフォメーションの開示は防止される。 ・　第三者に開示されたパーソナル・インフォメーションの性質と程度（範囲）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又は法令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テストする。 ・　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。	司法又は行政機関に対して、種々の法律上のプロセスを通じ、パーソナル・インフォメーションが開示される場合がある。 ある種の法令においては、パーソナル・インフォメーション開示のために特定の規定が存在する。他の立証可能な同意を要件として、同意なしでのパーソナル・インフォメーションの開示を認める場合がある。
7.2.2　パーソナル・インフォメーションの保護 企業が、企業のプライバシーポリシーの関連箇所、その他の特定の指示又は要求事項に整合して、パーソナル・インフォメーションを保護するよう合意した第三者のみに対して、パーソナル・インフォメーションが開示される。企業は、第三者がその合意、指示、要求事項に沿って有効な内部統制を有していることについて評価する手続を有している。	パーソナル・インフォメーションを第三者に提供する場合、企業は、第三者に提供された情報に、企業と同等な個人情報保護のレベルを要求する第三者と契約関係に入る。企業は下記を行う。 ・　第三者のパーソナル・インフォメーションの利用を、契約履行に必要な目的に制限する。 ・　第三者に個人の意向（同意）を伝達する。 ・　企業によって転送された、パーソナル・インフォメーション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のような指名されたプライバシー担当役員を明示する。 ・　第三者が企業によって提供されたパーソナル・インフォメーションをいつ、どのように保持する、又は返送するかを明示す	企業は、第三者に転送された情報を含めてパーソナル・インフォメーションの保有及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。 ヨーロッパの幾つかの国を含む特定の法域では、パーソナル・インフォメーションを転送しようとする企業は、転送前に規制当局に対し

	る。 企業は、リスク評価に依拠するより高いレベルの保証を得るために、下記のアプローチの一つ以上を用いて契約への遵守性を評価する。 ・　第三者は、それらの実務に関する質問書に回答する。 ・　第三者は、実務が内部監査報告書その他の手続に基づく企業の要件を満たすことを自己証明する。 ・　企業は、第三者の実地評価を実行する。 ・　企業は、独立監査人によって提供された監査又は同様の報告書を受け取る。	て登録することを要求される。 PIPEDAは、パーソナル・インフォメーション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（EU）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 個人の事前の黙示又は明示の同意によってのみ､新しい目的のために､第三者へのパーソナル･インフォメーションの開示がなされる。	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、第三者にパーソナル・インフォメーションを開示する前に、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、第三者にパーソナル・インフォメーションが提供されていることをモニターする。	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。 ・　子会社又は関係会社 ・　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 ・　外国及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 第三者によるパーソナル･インフォメーションの誤用 企業は､パーソナル・インフォメーションを転送した第三者による	企業は、下記に従う。 ・　第三者のいかなるパーソナル・インフォメーション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又は契約上の合意と相違	

当該情報の誤用に対する修正行動をとる。	したパーソナル・インフォメーションを利用、又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、第三者のパーソナル・インフォメーションの利用又は開示により起こされた損害を緩和する。 ・ 第三者がパーソナル・インフォメーション（例えば、契約の条項がパーソナル・インフォメーション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

2009(完成版)		
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パーソナル・インフォメーションを保護する。		
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(関連するセキュリティポリシーを含む。）は、パーソナル・インフォメーションのセキュリティを扱う。	プライバシーポリシーは、電子的、紙面又は他の形式であるか否かにかかわらず、パーソナル・インフォメーション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、パーソナル・インフォメーションの機微の程度と整合している。	あらゆる企業の統制下又は企業の統制下であるとみなされる場所でのパーソナル・インフォメーションは、保護されなければならない。

8.1.1　個人への伝達 パーソナル･インフォメーションを守るために予防策が実施されることを､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、下記のようにパーソナル・インフォメーション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パーソナル・インフォメーションにアクセスする権限を与えられる。 ・　電子的に保持されたパーソナル・インフォメーション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パーソナル・インフォメーションに対して物理的セキュリティが維持され、インターネット上に送られたパーソナル・インフォメーション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、追加的なセキュリティ保護が適用される。	ユーザー、経営者、プロバイダー、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又は、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を危険にさらさないように、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、滅失、誤用、未承認のアクセス、漏洩、改竄､破損からパーソナル･インフォメーションを保護するための､管理的、技術的、物理的措置を開発、文書化、承認、導入をしている｡セキュリティプログラムは､少	企業のセキュリティプログラムは、下記のパーソナル・インフォメーションの保護と関係がある事項を扱う。 ・　定期的なリスク評価 ・　あらゆる種類のパーソナル・インフォメーション、パーソナル・インフォメーションを取り扱うのに関与する関連プロセス、システム、第三者の識別 ・　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	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場合がある。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

なくともパーソナル･インフォメーションのセキュリティに関する下記の領域[6]に対処すべきであるが､それに制限されない。 a．リスクの評価と対応(1.2.4) b．セキュリティポリシー(8.1.0) c．情報セキュリティ管理体制(セクション１、７、10) d．資産管理（セクション１） e．人的セキュリティ（セクション１） f．物理的、環境的セキュリティ（8.2.3と8.2.4） g．伝達と運用の管理(セクション１、７、10) h．アクセスコントロール(セクション１、8.2、10) i．情報システムの取得､開発､保守(1.2.6) j．情報セキュリティインシデント管理(1.2.7) k．事業継続管理(セクション8.2)	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行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行責任と説明責任の割当て ・　ＯＳ、ネットワークソフトウェア、システムファイルの保護 ・　暗号化ツール、情報の保護 ・　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インシデントを取り扱う手続 ・　システムへの既遂、未遂の攻撃又は侵入を発見する手続及び、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	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（又は委員会、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。 ―課題となっているパーソナル・インフォメーション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。

[6] ISO/IEC27002:2005（情報技術及びセキュリティ技術）情報セキュリティ管理実務規約から、これらの情報は得られる。ライセンスは国際標準化機構(ISO)を代表して米国規格協会(ANSI)によって与えられる。http://webstore.ansi.org/で合衆国とカナダのANSIから､www.standardsstore.ca/eSpecs/index.jspで、カナダ規格審査会からISO/IEC27002のコピーを購入できる。一般に公正妥当と認められたプライバシー原則の規準8.2.1を満たすために、ISO/IEC27002:2005の規準の全てに適合することは必要でない。各領域に関連しているリファレンスは、この目的のために最も関連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の規準を示す。

1．コンプライアンス (セクション１、10)	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及び状況に対応する規定 ・　事業継続管理と災害復旧計画と関連するテスト ・　適用される法令、定義されたコミットメント、SLAその他の契約の識別及び整合性のための規定 ・　パーソナル・インフォメーションのセキュリティに関する企業のプライバシーポリシー及び手続について（初年度及び年次に）ユーザー、経営者、第三者に理解の程度を確認する。 ・　人員が退職した場合、権限を削除し、パーソナル・インフォメーションにアクセス又は保存しているコンピュータその他の機器の返却を確保する手続 企業のセキュリティプログラムは、組織によって利用する必要がなくなったコンピュータ、媒体、紙面のパーソナル・インフォメーションへのアクセスを防止する（例　コンピュータ、媒体、紙面の情報の保存、売却又は廃棄）。	カード業界は、特定ブランドからカード保持者情報のためのセキュリティ及びプライバシー要件を確立している。
8.2.2　論理的アクセスコントロール パーソナル･インフォメーション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。	下記のシステムと手続が採用されている。 ・　データの機微の程度とパーソナル・インフォメーション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。	ユーザー認証プロセスにおいて、下記の事項に留意する。 ・　ストレージの媒体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（内部又は外部ネッ

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．ＩＴインフラ構成要素とパーソナル･インフォメーションへのアクセス権限と許諾の付与 e．自身のパーソナル・インフォメーション又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実行責任に基づいて承認された社内要員のみへのパーソナル･インフォメーションへのアクセス制限 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､システムと媒体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､マスターパスワード､強力なユーティリティー､セキュリティデバイス（例えば、ファイアウォール）へのアクセス制限 j．ウイルス、悪意のあ	・　パーソナル・インフォメーションを取扱うシステムへのアクセス権限を付与する前に、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。 ・　追加的又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。 ・　侵入検知及びモニタリングシステムを導入する。	トワーク） ・　パーソナル・インフォメーションを含む紙及びバックアップ媒体へのアクセス ・　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 特定の法域では、保存されていたデータを暗号化その他の方法で不明瞭化することを求めている。

るコード､未承認のソフトウェアの導入禁止		
8.2.3　物理的アクセスコントロール パーソナル･インフォメーションへの物理的アクセスが（パーソナル･インフォメーションを含んでいるか､又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、パーソナル・インフォメーションへの論理的、物理的アクセスを管理する。 ・　パーソナル・インフォメーションへのアクセスログを取得し、モニターする。 ・　パーソナル・インフォメーションの未承認又は突発的な破壊や滅失を防止する。 ・　未承認のアクセスを取得する違反及び試行を調査する。 ・　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。 ・　パーソナル・インフォメーション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破棄をセキュアに（例えば、シュレッダーで）行う。	パーソナル・インフォメーションが処理、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 全ての形態でのパーソナル･インフォメーションが、自然災害、環境上のリスク要因による不測の開示から保護される。	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維持する。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。 それに加えて企業は、環境的なインシデントによりパーソナル・	欧州連合（EU）指令のようなある種の規制では、パーソナル・インフォメーションが、不意の漏洩に加えて、不法な破壊、不意の毀損、自然災害、環境的脅威からも保護されることを求めている。

	インフォメーションの不意の漏洩が起こるのを防止するために、物理的その他の安全保護措置を講じる。	
8.2.5　伝送されたパーソナル･インフォメーション パーソナル･インフォメーションがメールその他の物理的手段による伝送時に保護される。パーソナル･インフォメーションが､インターネット､公衆回線､その他のセキュアでないネットワーク､無線ネットワークによって収集､伝送される場合、パーソナル･インフォメーションの転送､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。 ・　暗号化と内部統制の最低レベルを定義する。 ・　パーソナル・インフォメーションの転送、受信に対して業界標準の暗号化技術（例えば、128ビットのトランスポート・レイヤー･セキュリティ（TLS）､VPN）を利用する。 ・　外部のネットワーク接続を承認する。 ・　ハードコピー及びメールの電子的形式、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。 ・　無線で収集され、伝送されるパーソナル・インフォメーションを暗号化し、無線ネットワークを未承認のアクセスから保護する。	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及び認証のための特別な規定がある。 幾つかのクレジットカード業者は、クレジットカード及び取引関連データを伝送中、並びに保管中に暗号化技術の利用の要求を含めて、カード所持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ビットのセキュアTLS）。 パーソナル・インフォメーションの無線機器（例えば、携帯電話）からの音声伝送は暗号化されない場合がある。

8.2.6　ポータブルメディア上のパーソナル･インフォメーション ポータブルメディアに保存されたパーソナル･インフォメーションが､未承認のアクセスから保護される。	ポリシー及び手続により、ビジネス上の要請が存在するか、保管が経営者によって承認されていない限り、パーソナル・インフォメーションをポータブルメディアその他の機器に保管することが禁止されている。 下記を使用するなどでアクセスされる、又は保存されたパーソナル・インフォメーションを保護するためのポリシー、システム、手続が整備されている。 ・　ラップトップコンピュータ、PDA、スマートフォン、類似機器 ・　例えば、在宅勤務や出張している間に従業員によって使用されたコンピュータその他の装置 ・　USBドライブ、CD、DVD、磁気テープ、その他の携帯用の媒体 企業のアクセス、保有、廃棄ポリシーの対象となる当該情報が暗号化され、パスワードは物理的に保護される。 バックアップと復旧に使用されるパーソナル・インフォメーションを含む媒体の作成、転送、保管、廃棄について内部統制が存在する。 パーソナル・インフォメーションを含む媒体の滅失、潜在的誤用を報告するための手続が存在する。 従業員又は契約社員の退職のときに、パーソナル・インフォメーションにアクセスし、保存するのに使用されるポータブルメディアと機器、印刷された他のコピーのような情報の返却又は廃棄に備え	例えば、規制当局と監査人に提供されたパーソナル・インフォメーションにも必要である保護に対して考慮を払うべきである。

	る手続が存在する。	
8.2.7　セキュリティ保護措置のテスト パーソナル･インフォメーション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。 ・　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、又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機器をテストする。 ・　災害復旧及び危機管理計画を少なくとも毎年、実行可能性を確保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ウェブ脆弱性及び復旧能力を含めて、脅威及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、新規及び変化した脅威と脆弱性を考慮して、セキュリティポリシー及び手続を定期的に適切に改定する。 ・　セキュリティテストの結果を定期的に経営者に報告する。	セキュリティ保護措置のテストの頻度及び性質は、企業の規模と複雑性、企業活動とパーソナル・インフォメーションの機微の度合いの性質と範囲により変化する。 ある種のセキュリティ規制（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。 ・　独立した第三者又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（又は少なくとも、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

2009(完成版)		
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、適切にパーソナル・インフォメーションを保持する。		
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パーソナル･インフォメーションの品質を扱う。		
9.1.1　個人への伝達 企業は､個人が正確かつ､完全なパーソナル・インフォメーション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。	企業のプライバシー通知は、個人が企業と継続的な関係を持つとき、パーソナル・インフォメーションが正確かつ、完全に維持される必要があると説明する。	
9.2 手続と内部統制		
9.2.1　パーソナル・インフォメーションの正確性と完全性 パーソナル･インフォメーションは､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。 ・　パーソナル・インフォメーションが収集、生成、保管、更新される度に誤謬摘示し、確認する。 ・　パーソナル・インフォメーションの取得、更新日時を記録する。 ・　パーソナル・インフォメーションが失効する時点を特定する。 ・　パーソナル・インフォメーション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パーソナル・インフォメーションを更新する方法）を特定する。 ・　個人から直接、又は第三者（4.2.3「第三者からの収集」を参照）を通じて取得され、又は第三者（7.2.2「パーソナル・インフォメーションの保護」を参照）に開示されるパーソナル・インフォメーション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、利用中であるパーソナル・インフォメーションが、十分に正確かつ、完全であることを確保する。 ・　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、パーソナル・インフォメーションが定常的には更新されないことを確保する。 企業は、述べられた（定められた）目的を達成するために、パーソナル・インフォメーション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実施する。	
9.2.2　パーソナル・インフォメーションの適切性 パーソナル･インフォメーションは､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。 ・　パーソナル・インフォメーションが、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ため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確保する。	

	・　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、パーソナル・インフォメーション記録の適切性を定期的に評価し、必要に応じて修正する。	

モニタリングと是正措置

モニタリングと是正措置の規準	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性をモニタリングし、プライバシーに関連する問合せ、苦情及び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是正措置を扱う。		
10.1.1　個人への伝達 企業は、個人が問合せ、苦情及び紛争について、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、企業のウェブサイトの電子メールリンク又は電話番号）。 ・　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、個人又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　問合せ、苦情及び紛争処理	企業のプライバシー責任者又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	

問合せ、苦情及び紛争に対処するプロセスが採用されている。	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 ・ パーソナル・インフォメーションの違反について実施可能な救済策及び当該情報を個人に伝達する方法 ・ 実施可能な調停及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又は類似のサービス（提供される場合）に従うべき手続と連絡情報	
10.2.2 紛争解決と調停 全ての苦情に対処し、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。 ・ 個人の苦情や紛争の解決、上申プロセスの取扱いを担当する従業員を訓練する。 ・ 適時に全ての苦情を文書化して対応する。 ・ 適時に解決されることを確保するために、定期的に未解決の紛争と苦情をレビューする。 ・ 未解決の苦情と紛争を経営者によるレビューのために上申する。 ・ 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。 ・ 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	ある種の規制（例えば、HIPAA及びCOPPA）が特定の手続と要件を持っている。 ある種の法律（例えば、PIPEDA）が裁判システムを通じた最高裁までの苦情提起を許容している。

	独立した第三者紛争解決サービス又は、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。	
10.2.3　コンプライアンスレビュー 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、SLAとその他の契約へのコンプライアンスがレビューされ、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、企業の是正計画が策定、導入される。	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、SLA と他の契約へのコンプライアンスをレビューする。例えば、内部監査計画、監査報告書、コンプライアンスチェックリスト等の文書を定期的にレビューし、経営者が署名する。 ・　コンプライアンス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。 ・　適時（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。）に適切な是正行動がとられることを確保するために、コンプライアンスレビューで発見された問題と脆弱性の解決をモニターする。	法令及び契約上の要件に加えて、企業によっては国際標準化機構（ISO）の基準への準拠を選択し、又は事業を行う条件としてカード業界の基準等に準拠することを要求される場合がある。
10.2.4　コンプライアンス違反への対応 プライバシーポリシーと手続へのコンプライアンス違反の例が文書化されて、報告され、	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適時に通知する。 ・　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、	

必要な場合は、是正及び懲戒処分の対策が適時にとられる。	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コンプライアンス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是正対策が適時にとられることを確保するために、それらの解決をモニターする。 ・　プライバシーインシデントや違反を引き起こした従業員その他の者を適切に処分する。 ・　企業のプライバシーポリシー及び手続に違反した第三者によるパーソナル・インフォメーションの利用又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。	
10.2.5 継続的モニタリング リスク評価(1.2.4)に基づくパーソナル・インフォメーションの内部統制の有効性をモニタリングして、必要に応じて適時な是正行動をとるために継続的モニタリングが実施される。	企業は下記を利用する。 ・　内部統制報告書 ・　傾向変動分析 ・　訓練出席及び評価 ・　苦情解決 ・　定期的な社内レビュー ・　内部監査報告書 ・　受託会社の内部統制を対象とする独立監査報告書 ・　内部統制の有効性に関するその他の証拠 モニターされる内部統制の選定、モニターされる頻度は、情報	「内部統制システムのモニタリング指針」は、COSO（米国トレッドウェイ委員会の後援組織委員会）によって発行されており、内部統制の有効性をモニターするための有用な指針を提供する。

	の機微の度合いと情報の潜在的漏洩リスクに基づいている。 内部統制の例は下記のとおりである。 ・　ポリシーは、全社員が採用後30 日以内に初回プライバシー訓練を受けることを必要とする。継続的モニタリングは、コース完了の適切な証拠を持っていることを確認するために選択された従業員の人事ファイルのレビューを含む。 ・　従業員が職務責任を交代するか、退職するときは、ポリシーは、退職してから 24 時間以内に従業員のパーソナル・インフォメーションへのアクセスが適切に変更されたかをレビューすることを要求する。これはアクセスの自動終了を避けるための管理者の操作を必要とする、従業員状態変更報告を作成する人事システムの自動化されたプロセスで制御される。これは、報告に関連する管理者の操作のコピーを受け取るセキュリティグループによってモニターされる。 ・　ポリシーは、72 時間以内にプライバシー関連の苦情の確認を苦情提起者に提供し、10 営業日以内に解決しない場合、問題をCPO に報告することを記述する。内部統制は、苦情提起日を含むプライバシーの苦情と解決を終えた後の活動を記録するのに使用されるログである。モニタリング活動は、このポリシーの一貫性のためのログの毎月のレビ	

	ューである。	

付録Ａ　用語集

関係会社：他の企業を統制する企業、統制される企業又は共通の統制の下に置かれる企業

匿名化：特定の個人を識別するのに利用され得る個人に関連する情報を消去すること

機密保持：パーソナル・インフォメーション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、パーソナル・インフォメーションを収集、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示又は黙示であり得る。「明示の同意」は、口頭で、電子的に、又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。「黙示の同意」は、「オプトアウト」されていない、又は取引を完了するためにクレジットカード情報を提供するなどの、合理的に個人の作為又は不作為から推定されるかもしれない（オプトイン及びオプトアウトについては別掲）。

クッキー：クッキーは、ウェブサーバーによって生成され、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、ユーザーがウェブサイトに戻ってきたとき、ウェブコンテンツの個人履歴を示し、過去の購買習慣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。

暗号化：復号化するための特別な鍵を保有する当事者以外には、情報を変換して読み取れなくするためのプロセス

企業：パーソナル・インフォメーションを収集、利用、保持して、開示する組織

個人：収集されるパーソナル・インフォメーションの対象となる人（時に、データサブジェクト）

社内要員：従業員、委託先、代理人並びに企業及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：個人の明示の同意なしでは、パーソナル・インフォメーション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：個人が明示的に許諾を拒否しないなら、パーソナル・インフォメーションを収集、利用、保持、開示するために企業に黙示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、パーソナル・インフォメーションの利用及び取扱い。

パーソナル・インフォメーション：個人の同一性を識別できる情報又はそうであり得る情報

個人情報サイクル：パーソナル・インフォメーションの収集、利用、保持、開示、廃棄、匿名化

ポリシー： 経営者の意図、目標、要求事項、実行責任又は基準を伝達する書面

プライバシー： パーソナル・インフォメーションの収集、利用、開示、保持、破棄に関する個人及び企業の権利義務

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、パーソナル・インフォメーションが収集、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、パーソナル・インフォメーションを管理し、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： パーソナル・インフォメーションが、企業によって収集される理由

編集： パーソナル・インフォメーションを文書又はファイルから抹消又はマスキングすること。

機微なパーソナル・インフォメーション： 例えば、医療又は健康状態、人種又は民族、政治的見解、宗教的又は哲学的な信念、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、高水準の保護、高い注意義務を要求されるパーソナル・インフォメーション

第三者： パーソナル・インフォメーションを収集する企業と提携していない企業、又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

ウェブビーコン：ウェブビーコンは、ウェブバグとしても知られていて、データを転送するために、ウェブページ又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、広告及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ウェブビーコンを使う。例えば、ウェブ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　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業務実施者サービス

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（GAPP）を利用することで公共の実務における公認会計士（業務実施者）が提供できるサービスのハイレベルな

概要を提供する。業務実施者のための追加的な指針は、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)。

プライバシー助言業務

業務実施者は、GAPP 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 GAPP の規準を利用した、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業務実施者は、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の CS セクション 100：定義と基準（AICPA 職業的基準第２号）に従う。

プライバシー証明業務 （Privacy Attestation and Assurance Engagements）

業務実施者は、第三者による使用のための報告書を通常もたらす彼らのクライアントに対する証明サービスを提供するのに GAPP を使用できる。それぞれのために発行される報告書のサービスの本質、関連する職業的基準及び種類は以下で説明する。

プライバシー検証業務 （Privacy Examination and Audit Engagements）

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。プライバシー証明業務は、この基準の中で定義されている。業務実施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。

証明業務（Examination and audit engagements）では、業務実施者は高水準だが、絶対的でない水準の保証（assurance）を、主題又は記述書に提供する。その目的で、業務実施者は、業務実施者の専門的な判断力で業務実施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（develops audit procedures）する。プライバシー保証報告書の文例は付録Ｃに示されている。

下記の主要な概念が、プライバシー検証業務に適用される。

- 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[78]を発行するためには、検証対象期間を通じて、当該関連規準の全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」又は同等の水準で実施されるべきである。

---

[7] 付録Ｃ「プライバシー保証報告書の文例」を参照

[8] 特定の状況（TPSP に関する結論の報告のような）では、10 のプライバシー原則の幾つかを対象とする特定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」報告書といった文言を含めることを推奨する。

・　業務の範囲は、(1)全てのパーソナル・インフォメーションでもよいし、特定の種類の顧客情報又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。製造活動又は企業のウェブサイトで生成される小売活動だけでは不可）、又は地理的な場所（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。

— プライバシー通知は、(1)保証報告書が利用者にとって利用可能であり、経営者の記述書及び報告書で明確に記述されているべきであり、また、(2)経営者の記述書及び保証報告書を添付するべきである。

— 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及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。

— 業務の範囲は、情報サイクルの関連するパーソナル・インフォメーションのための活動の全てを含むべきである。これらには収集、利用、保持、開示、廃棄、匿名化を含むべきである。保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。

— 業務の範囲にないが、検証の範囲に含まれていた特定のパーソナル・インフォメーションが混ざっている場合、業務の範囲は、混ざっていた情報の全ての内部統制を対象とする必要がある。

— 通常、保証報告書は特定期間対象（少なくとも２か月）であるべきだが、業務実施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。

経営者の記述書

AICPA 証明基準の下では、検証業務では、通常、業務実施者は書面の記述書を得るべきである。経営者が書面の記述書を業務実施者に提供しない場合でも、業務実施者は主題に関して結論を報告することができるが、状況[9]によっては、報告書の様式が異なる場合がある。

AICPA 基準の下では、業務実施者は、経営者の記述書か主題のどちらかに関して結論を報告する場合がある。業務実施者が記述書に関して結論を報告する場合、記述書[10]は、保証報告書に添付するか、又は報告書の第一節に記述書の内容を入れるべきである。業務実施者が主題に関して結論を報告する際に、業務実施者は、経営者の記述書が保証報告書の利用者にとって利用可能になるよう要求する場合がある。

プライバシー検証に関しては、記述書ベースの業務が直接主題に関して結論を報告する業務より適切であることは間違いない。記述書を第三者に提供することにより、経営者は記述書に記述された実行責任を明示的に了承する。

---

9 書面による記述書が得られない場合の業務実施者の結論の記述については、証明業務（AICPA 職業的基準第１号）AT セクション 101 パラグラフ 58 を参照

10 AT セクション 101 パラグラフ 64 を参照

プライバシーレビュー業務（Privacy Review Engagements）

レビュー業務は証明業務の一種である （A review engagement is a type of attestation or assurance engagement.）。しかしながら、プライバシーレビューという用語は、プライバシー業務に言及する場合、ある種のプライバシー診断業務、プライバシーに関する発見事項や、改善提案事項を作成する業務などのプライバシーのアドバイザリー業務に誤用されることが多い。業務実施者とクライアントのどちらかが、相手へのニーズや期待を誤解するリスクを軽減させるため、業務実施者は、クライアントに実施するサービスの詳細と発行する報告書の種類に関して、理解を確立すべきである。

職業的基準で定義されるレビュー業務は、業務実施者が実施した作業に基づいて、何らかの情報に関心を持つに至ったのかどうかについて、保証報告書に示す検証業務の一種である。その関心とは、主題が規準に基づいて、全ての重要な点において、主題が規準に基づいていない（又は、規準に適合していない）、又は、表示されていない（又は、適正に表示されていない）ことを示すものである。一般に、業務実施者のレビュー業務報告書の基礎を提供するために実施された手続は、質問、分析的レビュー手続、検討に制限される。AICPA/CICA プライバシータスクフォースの視点では、これらの手続とレビュー業務から提供された限定的保証は、レビューを実施する当事者が、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を示すことが期待される場合には、プライバシー要件と期待に影響を受けるほとんどの当事者のニーズを満たすのに適切でない。したがって、プライバシーレビュー業務の実施については指針を提供しない。

合意された手続業務

合意された手続業務では、業務実施者は、当事者[11]によって合意された手続を実施して、当該当事者の発見事項を報告する。業務実施者は、記述書又は主題[12]の検証やレビューを実施せず、結論を報告せず、又は記述書や主題に関する消極的保証を提供しない。この種の業務では、保証報告書は、手続と発見事項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と規準が、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発見事項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、業務実施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、発見事項を報告することを依頼する場合が

11 特定された報告書利用者と業務実施者は、業務実施者によって実施される手続に合意する。

12 合衆国では、合意された手続業務は、AT セクション 201 パラグラフ.15 合意された手続業務（AICPA 職業的基準第 1 号）の下で実施される。指定された手続業務において、指定された手続を適用する結果を特定のユーザーに報告するために業務実施者は業務を実施する。そのような手続を適用する際に、必ず高水準の保証を提供するのに業務実施者の判断で必要な手続の全てを実施するわけではないので、業務実施者は主題に関する結論を表明しない。むしろ、報告書は発見された例外事項も含めて、適用された手続の事実上の結果を記述する。

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、特定された利用者とクライアントは、自分自身のニーズを最もよく理解しているため、手続の十分性に対する実行責任を負う。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及び助言サービス）の一部である。Trust サービス原則と規準[13]は、AICPA と CICA の無報酬の特別委員会によって策定された。その他の Trust サービス原則と規準は下記のとおりである。

セキュリティ：システムは、（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、コミット又は合意したとおりに、運用、かつ利用できる。

処理のインテグリティ：システム処理は完全、正確、タイムリー、かつ承認されている。

機密保持：機密として設定された情報が、コミット又は合意したとおりに保護されている。

上記は、http://www.aicpa.org/TrustServices で、より詳細に検討されている。

付録Ｃ　プライバシー保証報告書の文例

以下の付録には、AICPA 又は CICA の報告基準の下での保証報告書の文例が含まれている（訳注：CICA の例示は省略）。

AICPA 証明基準が適用される場合

文例１ －AICPA 証明基準の下での経営者記述書に対する結論の報告

－文例１に対する経営者記述書の文例

文例２ －AICPA 証明基準の下での主題に対する直接の結論の報告

文例１－AICPA 証明基準の下での経営者記述書に対する結論の報告

[13] WebTrust と SysTrust は、Trust サービス原則と規準に基づく AICPA と CICA によって開発された二つの特定の検証サービス業務である。業務実施者は、WebTrust か SysTrust シールのいずれかの使用を CICA によって許諾されなければならない。プライバシー業務がオンライン領域を組み込んで、企業が限定事項か範囲の制限を含まない保証報告書を受け取ったとき、企業は、WebTrust オンラインプライバシーシールを表示することを選ぶことができる。業務実施者のライセンスに関する詳しい情報とオンラインプライバシー業務に関しては、www.webtrust.org を参照。

独立した業務実施者のプライバシー保証報告書

ABC 社　代表取締役　殿

当監査法人は 2009 年○月○日から 2009 年○月○日までの期間の 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、パーソナル・インフォメーションが収集、利用、保持、開示及び廃棄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維持されていた。
- 2009 年○月○日付の、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、結論を報告することである。

当監査法人の検証は、米国公認会計士協会によって作成された証明基準に従って行われた。それには(1)ABC 社のパーソナル・インフォメーション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、当監査法人の結論に合理的な基礎を提供するのに十分かつ適切であると判断している。

当監査法人の結論では、2009 年○月○日から 2009 年○月○日までの間に ABC 社の経営者の記述書は、下記の事項について、全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、パーソナル・インフォメーションが収集、利用、保持、開示及び廃棄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維持していた。
- 上記の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、

当監査法人の結論では、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、全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及び性質のため、前述の規準及びプライバシー通知におけるコミットメントへの適合において、ABC 社は影響される場合がある。例えば、システム及び情報に対する不正、未承認のアクセス、社内及び社外のポリシーや規制要件へのコンプライアンス違反が防止又は発見されない場合がある。さらに、当監査法人の発見事項

に基づいて結論を予測することには、将来の変更又は事象により、当該結論の正当性が変更されるリスクがある。
［監査法人名］
○○○○監査法人
［住所］
［日付］

文例１に対する経営者記述書の文例

2009 年○月○日から 2009 年○月○日までの期間に、ABC 社は、全ての重要な点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、パーソナル・インフォメーションが収集、利用、保持、開示及び廃棄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維持していた。
- 2009 年○月○日付の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。

文例２－AICPA 証明基準の下での主題に対する直接の結論の報告

独立した業務実施者のプライバシー保証報告書

ABC 社　代表取締役　殿

当監査法人は、2009 年○月○日から 2009 年○月○日までの期間に 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、パーソナル・インフォメーションが収集、利用、保持、開示及び廃棄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、結論を報告することである。

当監査法人の検証は、米国公認会計士協会によって作成された証明基準に従って行われた。それには、(1)ABC 社のパーソナル・インフォメーション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結論に合理的な基礎を提供するのに十分かつ適

切であると判断している。

当監査法人の結論では、2009 年○月○日から 2009 年○月○日までの間に 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、パーソナル・インフォメーションが収集、利用、保持、開示及び廃棄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維持していた。(2)上記の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及び性質のため、前述の規準及びプライバシー通知におけるコミットメントへの適合において、ABC 社は影響される場合がある。例えば、システム及び情報に対する不正、未承認のアクセス、社内及び社外のポリシーや規制要件へのコンプライアンス違反が防止又は発見されない場合がある。さらに、当監査法人の発見事項に基づいて結論を予測することには、将来の変更又は事象により、当該結論の正当性が変更されるリスクがある。

［監査法人名］

○○○○監査法人

［住所］

［日付］

以　上