《付録４》

受託業務のセキュリティ、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係る内部統制の評価のための原則と規準

－目　　次－

Ⅰ　概要
Ⅱ　原則と規準
１．全ての原則（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）に共通する規準
２．可用性に関する追加規準
３．処理のインテグリティに関する追加規準
４．機密保持に関する追加規準
５．プライバシーに関する追加規準

《Ⅰ　概要》

《１．目的》

１．本付録は、公認会計士等が受託業務のセキュリティ、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係る内部統制を検証し報告する保証業務を提供する場合に適切な規準を提供することを目的としている。

本付録の規準（以下「本規準」という。）は、本実務指針において、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内部統制のデザインの適切性又は運用の有効性を評価する場合に規準として使用する。

《２．本付録の原則と規準》

２．本付録は、原則と規準の二つから構成されている。原則は、保証業務の対象となる内部統制を評価するための目的を表している。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の五つの原則に係る規準は、その原則を達成するために必要な評価の要件である。

３．本付録は、米国公認会計士協会が2016年に公表している「Trust Services Principles and Criteria」を参考にしている。

《３．法令等に関する整合性について》

４．受託会社の経営者には、法令を認識し、遵守する責任がある。「適用される法令、コミットメント、サービスレベルアグリーメント（以下「ＳＬＡ」という。）及びその他の契約の要求事項への整合性」について、規準の中で取り上げられているが、「適用される法令、コミットメント、ＳＬＡ及びその他の契約の要求事項への整合性」と同等な全てのものを識別することは、本規準の適用範囲には含まれない。さらに、本規準は、企業に、適用される法令、コミットメント、ＳＬＡ及びその他の契約の要求事項への法令遵守の統制に関してテスト又は報告することを目的として利用するものではない。

《４．本付録が対象とする原則》

５．本付録では、次の五つの原則について記載している。

(1) セキュリティ：　システムは、受託会社のコミットメント及びシステム要求事項を満たすために、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) 可用性：　システムは、受託会社のコミットメント及びシステム要求事項を満たすために、操作でき、かつ、利用できる。

(3) 処理のインテグリティ：システム処理は、受託会社のコミットメントとシステム要件を満たすために、完全、正当、正確、適時かつ権限付与されている。

(4) 機密保持：　機密として指定された情報が、受託会社のコミットメント及びシステム要求事項を満たすために、保護されている。

(5) プライバシー：　パーソナル・インフォメーションは、受託会社のコミットメント及びシステム要求事項を満たすために、収集、利用、保持、開示及び廃棄される。

《５．各原則の規準の構成》

６．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共通する規準は、次の七つの分類により構成されている。

(1) 組織及び管理

受託会社が、業務の対象とした（一つ以上の）原則の規準を満たすよう、その業務単位の人員を管理、支援するため組織が導入している組織構造とプロセスに関連する規準。これは人員の責任、誠実性、倫理観及び適性を扱う規準並びにそれらが機能する環境を含んでいる。

(2) コミュニケーション

業務で扱われた（一つ以上の）原則の規準を満たすよう、受託会社が、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システム要求事項並びに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を伝達する方法に関する規準

(3) リスク管理及び内部統制のデザインと導入

受託会社が、業務で扱われた（一つ以上の）原則の規準を満たす以下のプロセスを含むリスク管理の方法に関する規準

(ⅰ) 受託会社の目的を達成する能力に影響する潜在的リスクの特定

(ⅱ) それらのリスクの分析

(ⅲ) 内部統制のデザインと導入及び他のリスク緩和策を含むそれらのリスク対応策の策定

(ⅳ) リスクとリスク管理プロセスの継続的モニタリング

(4) 内部統制のモニタリング

受託会社が、業務で扱われた（一つ以上の）原則の規準を満たすよう、内部統制のデザインの適合性と運用の有効性を含めてシステムをモニタリングし、

特定された不備へ対応する方法に関する規準

(5) 論理的及び物理的アクセス管理

受託会社が、業務で扱われた（一つ以上の）原則の規準を満たすよう、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又は削除し、未承認のアクセスを防止する方法に関する規準

(6) システム運用

受託会社が、業務で扱われた（一つ以上の）原則の規準を満たすよう、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、緩和する方法に関する規準

(7) 変更管理

受託会社が、業務で扱われた（一つ以上の）原則の規準を満たすよう、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を用いて変更を行い、未承認の変更を防止する方法に関する規準

7．プライバシーの規準は、次の８個の要素から構成されている。

(1) コミットメントとシステム要求事項の通知及びコミュニケーション

受託会社は、プライバシー実務に関連するデータ主体（本人）へ、プライバシーコミットメント及びシステム要求事項を通知する。

(2) 選択と同意

受託会社は、データ主体（本人）にパーソナル・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可能な選択を伝達する。

(3) 収集

受託会社は、プライバシーコミットメント及びシステム要求事項を満たすよう、パーソナル・インフォメーションを収集する。

(4) 利用、保持及び廃棄

受託会社は、プライバシーコミットメント及びシステム要求事項を満たす範囲に、パーソナル・インフォメーションの利用、保持及び廃棄を制限する。

(5) アクセス

受託会社は、データ主体（本人）に対して、プライバシーコミットメント及びシステム要求事項を満たすよう、レビューと更新を含む修正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。

(6) 開示と通知

受託会社は、プライバシーコミットメント及びシステム要求事項を満たすよう、データ主体（本人）の同意を得て、パーソナル・インフォメーションを開示する。

漏洩及びインシデントの通知は、プライバシーコミットメント及びシステム要求事項を満たすよう、影響のあるデータ主体（本人）、規制当局及びその他に提供される。

(7) 品質

受託会社は、プライバシーコミットメント及びシステム要求事項を満たすよう、正確かつ、最新かつ、完全かつ、適切なパーソナル・インフォメーションを収集、維持する。

(8) モニタリング及び執行

受託会社は、プライバシー関連の問合せ、苦情及び紛争を扱う手続を含む、プライバシーコミットメント及びシステム要求事項の準拠性をモニタリングする。

8．業務実施者は、受託会社の要請に基づき第６項及び第７項の「原則と規準」に追加して、例えば規制当局の要求事項や業界団体の自主規制等の遵守に関して、本実務指針に準拠して業務を実施することができる。

この場合、業務実施者は、受託会社から追加された主題情報に関する説明、受託会社のシステムに関する記述書の記述の追加及び関連する内部統制等に関する業務実施者の業務の遂行上必要な情報を入手しなければならない。

《II　原則と規準》

《1．全ての原則（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）に共通する規準》

1-1　組織及び管理に関する共通規準
1-1.1　受託会社は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー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システム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。
1-1.2　受託会社のシステムコントロール及びその他のリスク軽減策に係る設計、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、ポリシー及び他のシステム要求事項を効果的に広め、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連する受託会社のコミットメント及びシステム要求事項を充足するために導入され、実施することを確実にするため、権限とともに受託会社内の各個人に割り当てられる。
1-1.3　受託会社は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー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、維持及びモニタリングに関して責任がある要員の適性を評価する手続を確立し、責任を果たす上で必要なリソースを提供している。
1-1.4　受託会社は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー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システム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。）を適用し、実行している。
1-2　コミュニケーションに関する共通規準
1-2.1　システムの設計・運用とその境界に関連する情報は、許可されたシステムの内部及び外部ユーザーが、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、伝達されている。
1-2.2　受託会社の[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー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。
1-2.3　内部及び外部ユーザー並びにシステム運用に影響を及ぼす役割があるその他の者の責任は、それらの者に伝達されている。
1-2.4　[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー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、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不可欠な情報は、要員にその責任を果たすために提供されている。
1-2.5　内部及び外部ユーザーは、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー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要員に報告する方法についての情報が提供されている。
1-2.6　内部及び外部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、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]と関連する受託会社のコミットメント及びシステム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ている。
1-3　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
1-3.1　受託会社は、(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、機密保持若しくはプライバシー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システム要求事項を害するおそれのある潜在的脅威（システムにアクセスする委託会社の要員やその他の者による脅威と同様に、商品及びサービスを提供するベンダー及び他の第三者を利用することによる脅威を含む。）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策（内部統制の導入、商品又はサービスを提供するベンダー及び他の第三者の活動のみならずその評価及びモニタリング、並びに他の軽減策を含む。）を決定し、(4)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及び内部統制の評価とモニタリングの結果）を識別・評価し、そして、(5)必要に応じて、識別された変更に基づいて、リスク評価と軽減策を再評価し、更新する。
1-3.2　受託会社は、リスク軽減策を実行するため、ポリシーと手続を含む、内部統制を設計、開発、導入、運用し、それらの活動の運用とモニタリングに基づく統制活動の設計及び導入の適合性を再評価し、そして、必要に応じて内部統制を更新する。
1-3.3　受託会社は、(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、規制による変更及び技術的な変更）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設計と配置の適合性を再評価し、必要に応じてそれらを更新している。
1-4　内部統制のモニタリングに関する共通規準
1-4.1　内部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、機密保持若しくはプライバシー又はそれらの組合せで報告対

象の原則を挿入]に関する受託会社のコミットメント及びシステム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その他必要となる対応は、適時に実施されている。
1-5　論理的及び物理的アクセス管理に関する共通規準
1-5.1　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ーは、(1)許可された内部及び外部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内部及び外部ユーザーアクセス制限、(3)[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するよう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ている。
1-5.2　受託会社によりアクセスを管理される新規の内部及び外部ユーザーは、システム認証情報が発行される前に登録・承認されてから、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するようシステムにアクセスする権限が与えられている。受託会社によりアクセスを管理されるそれらのユーザーに関して、ユーザーアクセスが承認されないときには、システム認証情報は削除されている。
1-5.3　[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するように、内部及び外部ユーザーは、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、承認されている。
1-5.4　[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するように、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変更に基づいて、承認され、修正又は削除されている。
1-5.5　[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するように、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ている。
1-5.6　受託会社のコミットメントとシステム要求事項を充足するように、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、機密保持若しくはプライバシー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。
1-5.7　情報の送信、移動及び削除は、許可された内部及び外部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、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関

する受託会社のコミットメント及びシステム要求事項を充足するよう送信、移動又は削除する間は保護されている。
1-5.8 [セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するように、未承認又は悪意の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適用されている。
1-6 システム運用に関する共通規準
1-6.1 [セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するように、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関して、悪意のある行為、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、識別、モニタリング及び評価され、対応策が既知及び新規に識別された脆弱性を補うために設計、実装及び運用されている。
1-6.2 [セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー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、識別された脆弱性を含むインシデントは、受託会社のコミットメントとシステム要求事項を充足するように、確立されたインシデント対応手順に従って、識別され、適切な要員に報告され、対処されている。
1-7 変更管理に関する共通規準
1-7.1 [セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメント及びシステム要求事項は、システム構成要素の（起案）承認、設計、調達、導入（実装）、設定、テスト、修正、（リリース）承認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ている。
1-7.2 [セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメント及びシステム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、ソフトウェア及びポリシーと手続が必要に応じて更新されている。
1-7.3 [セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメントとシステム要求事項を充足するように、システムの運用中に、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、モニタリングされている。
1-7.4 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、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する受託会社のコミットメント及びシステム要求事項を充足するよう、（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、実装されている。

《２．可用性に関する追加規準》

2-1　可用性に関する追加規準
2-1.1　受託会社の可用性に関するコミットメント及びシステム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、モニタリングされ、評価されている。
2-1.2　受託会社の可用性に関するコミットメント及びシステム要求事項を充足するために、物理的設備対策、ソフトウェア及び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（起案）承認され、設計され、開発され、実装され、稼働し、（リリース）承認され、維持され、モニタリングされている。
2-1.3　受託会社の可用性に関するコミットメント及びシステム要求事項を充足するために、システム復旧を支援する復旧計画の手続がテストされている。

《３．処理のインテグリティに関する追加規準》

3-1　処理のインテグリティに関する追加規準
3-1.1　受託会社の処理のインテグリティに関するコミットメント及びシステム要求事項を充足するために、処理エラーを防止する手続又は検出・是正する手続が存在している。
3-1.2　システム入力は、受託会社の処理のインテグリティに関するコミットメント及びシステム要求事項を充足するために、完全に、正確に、適時に測定され、記録されている。
3-1.3　データは、受託会社の処理のインテグリティに関するコミットメント及びシステム要求事項を充足するために承認されたとおりに、完全に、正確に、適時に処理されている。
3-1.4　データは、受託会社の処理のインテグリティに関するコミットメント及びシステム要求事項を充足するために、特定された期間にわたって、完全、正確かつ適時に格納され、保持されている。
3-1.5　システム出力は、受託会社の処理のインテグリティに関するコミットメント及びシステム要求事項を充足するために、完全で、正確で、適切に配布され、そして保持されている。
3-1.6　通常の取引処理でないデータの修正は、受託会社の処理のインテグリティに関するコミットメント及びシステム要求事項を充足するために、承認され、処理されている。

《４．機密保持に関する追加規準》

4-1　機密保持に関する追加規準
4-1.1　機密情報は、受託会社の機密保持に関するコミットメント及びシステム要求事項を充足するために、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。
4-1.2　システム領域内の機密情報は、受託会社の機密保持に関するコミットメント及びシステム要求事項を充足するために、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。

4-1.3　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、受託会社の機密保持に関するコミットメント及びシステム要求事項を充足するために、承認された当事者に制限されている。
4-1.4　受託会社は、機密情報へアクセスできる、システムの一部になる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、企業の機密保持システム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。
4-1.5　システムの一部になる製品やサービスのベンダー及び他の第三者による、企業の機密保持に関するコミットメント及びシステム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ている。
4-1.6　受託会社の機密保持のコミットメント及びシステム要求事項の変更が、内部及び外部ユーザー、システムの一部となる製品やサービスのベンダー及び第三者に伝達されている。
4-1.7　受託会社は、受託会社の機密保持のコミットメント及びシステム要求事項を充足するように、機密情報を保持している。
4-1.8　受託会社は、受託会社の機密保持のコミットメント及びシステム要求事項を充足するように、機密情報を廃棄している。

《５．プライバシーに関する追加規準》

5-1　コミットメント、システム要求事項の通知及びコミュニケーションに関するプライバシー規準
5-1.1　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項を充足するために、プライバシー実務についてデータ主体（本人）に通知されている。通知は、受託会社のプライバシーコミットメント及びシステム要求事項を充足するために、パーソナル・インフォメーションの利用目的の変更を含む、受託会社のプライバシー実務の変更に関し適時に更新され、データ主体（本人）に伝えられている。
5-1.2　受託会社のプライバシーコミットメントが外部ユーザーに適切に通知され、それらのコミットメント及び関連するシステム要求事項が、内部ユーザーがその責任を遂行できるように伝えられている。
5-2　選択及び同意に関するプライバシー規準
5-2.1　受託会社は、パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関して可能な選択と、各選択の影響をデータ主体（本人）に伝えている。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明示的な同意が求められる場合には、データ主体（本人）又はその他権限を付与された個人から取得されている。当該同意は、受託会社のプライバシーコミットメント及びシステム要求事項に従って、情報が意図された目的のためだけに取得されている。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黙示的な同意が得られていると判断する受託会社の根拠は、文書化されている。
5-3　収集に関するプライバシー規準
5-3.1　パーソナル・インフォメーションは、受託会社のプライバシーコミットメント及びシステム要求事項に従って収集されている。

5-3.2　受託会社のプライバシーコミットメント及びシステム要求事項に従って、明示的な同意を求める情報に関し、受託会社は、そのような同意の必要性のみならずパーソナル・インフォメーションの要請に関し同意しない場合の影響について伝え、情報を収集する前に同意を取得している。
5-4　利用、保持及び廃棄に関するプライバシー規準
5-4.1　受託会社は、パーソナル・インフォメーションの利用を受託会社のプライバシーコミットメント及びシステム要求事項において特定された目的に制限している。
5-4.2　受託会社は、パーソナル・インフォメーションを受託会社のプライバシーコミットメント及びシステム要求事項に準拠して保持している。
5-4.3　受託会社は、パーソナル・インフォメーションを受託会社のプライバシーコミットメント及びシステム要求事項に準拠して確実に廃棄している。
5-5　アクセスに関するプライバシー規準
5-5.1　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項に従って、識別され認可されたデータ主体（本人）に、レビューのために、保管されている自身のパーソナル・インフォメーションにアクセスする能力を付与し、要請がある時点で、当該情報の物理的又は電子的コピーを、データ主体（本人）に提供している。もし、アクセスを拒否する場合、受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項に準拠し、データ主体（本人）に拒否及びその理由を通知している。
5-5.2　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項に従って、データ主体（本人）が提供する情報を基にパーソナル・インフォメーションを訂正、修正又は追加し、コミットされ又は要求されているように、そのような情報を第三者に提供している。訂正要請を拒否する場合には、受託会社は、データ主体（本人）に受託会社のプライバシーコミットメント及びシステム要求事項に準拠して拒否及びその理由を通知している。
5-6　開示及び通知に関するプライバシー規準
5-6.1　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項を充足するために、データ主体（本人）の明示的な同意を得て、パーソナル・インフォメーションを第三者に開示している。なお、受託会社は、当該同意を開示の前に取得している。
5-6.2　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項に準拠して、パーソナル・インフォメーションの承認された開示に関する完全、正確かつ適時の記録を作成、保持している。
5-6.3　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項に準拠して、発見若しくは報告されたパーソナル・インフォメーションの未承認の開示（漏洩を含む。）に関する完全、正確かつ適時の記録を、作成、保持している。
5-6.4　受託会社は、ベンダーその他第三者（その製品及びサービスがシステムの一部であり、システムにより処理されたパーソナル・インフォメーションへのアクセスを有する。）から、受託会社のプライバシーコミットメント及びシステム要求事項に準拠して、プライバシーコミットメントを取得している。
5-6.5　受託会社は、ベンダーその他第三者（その製品及びサービスがシステムの一

部であり、システムにより処理されたパーソナル・インフォメーションへのアクセスを有する。）の受託会社のプライバシーコミットメント及びシステム要求事項の遵守状況を、定期的かつ必要に応じて評価し、必要がある場合には是正措置を講じている。
5-6.6　受託会社は、パーソナル・インフォメーションの未承認の開示が実際に発生又は疑われる場合には、受託会社に通知をすることを含むコミットメントを、システムにより処理されるパーソナル・インフォメーションへのアクセスを有し得るベンダーその他第三者から取得している。当該通知は、受託会社が策定しているインシデント対応手続、プライバシーコミットメント及びシステム要求事項を充足するために、適切な要員に報告され、対処している。
5-6.7　受託会社は、プライバシーコミットメント及びシステム要求事項に準拠して、漏洩及びインシデントについて、影響を受けるデータ主体（本人）、規制当局その他に通知している。
5-6.8　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項に従って、データ主体（本人）の要求により、保有しているパーソナル・インフォメーション及びデータ主体（本人）のパーソナル・インフォメーションの開示の説明をデータ主体（本人）に提供している。
5-7　品質に関するプライバシー規準
5-7.1　受託会社は、受託会社のプライバシーコミットメント及びシステム要求事項に従って正確、最新、完全かつ適切なパーソナル・インフォメーションを収集し維持している。
5-8　モニタリング及び執行に関するプライバシー規準
5-8.1　受託会社は、データ主体（本人）及びその他からの問合せ、苦情及び紛争を受け付け、対処し、解決し及びその解決策を伝えるプロセスを適用し、定期的に受託会社のプライバシーコミットメント及びシステム要求事項への準拠状況、及び識別された不備に関する是正その他必要な措置が適時に講じられていることをモニタリングしている。

以　上