

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保証報告書

平成25年7月24日
改正 平成27年10月5日
最終改正 平成29年4月26日
日本公認会計士協会

- 目 次 -

| | 項 番 号 |
|----------------------------------|-------|
| 本実務指針の範囲及び目的 | |
| 1．本実務指針の範囲 | 1 |
| 2．目的 | 5 |
| 3．定義 | 6 |
| 要求事項 | |
| 1．本実務指針の遵守 | 7 |
| 2．職業倫理に関する規定 | 8 |
| 3．品質管理 | 9 |
| 4．経営者及び監査役等 | 10 |
| 5．保証業務契約の新規の締結及び更新 | 11 |
| (1) 保証業務契約書の作成 | 12 |
| (2) 保証業務の契約条件の変更の受諾 | 13 |
| 6．保証業務の計画と実施 | 14 |
| (1) 規準の適切性の評価 | 17 |
| (2) 重要性 | 21 |
| (3) 受託会社のシステムの理解 | 22 |
| 7．証拠の入手 | 23 |
| (1) 記述書に関する証拠の入手 | 24 |
| (2) 内部統制のデザインに関する証拠の入手 | 26 |
| (3) 内部統制の運用状況の有効性に関する証拠の入手 | 27 |
| 8．専門家の業務の利用 | |
| (1) 専門家の業務の利用 | 33 |
| (2) 専門家の業務の理解 | 34 |
| (3) 専門家の業務の評価 | 35 |
| 9．内部監査の利用 | |
| (1) 内部監査機能の理解 | 36 |

| | |
|----------------------------|-----|
| (2) 内部監査の利用の可否及びその利用の程度の判断 | 37 |
| (3) 内部監査人の特定の作業の利用 | 40 |
| (4) 業務実施者の保証報告書に及ぼす影響 | 42 |
| 10. 経営者確認書 | 44 |
| 11. その他の記載内容 | 47 |
| 12. 後発事象 | 49 |
| 13. 調書 | 51 |
| 14. 業務実施者の保証報告書の作成 | 59 |
| (1) 業務実施者の保証報告書の記載内容 | 61 |
| (2) 除外事項付意見 | 63 |
| 15. その他のコミュニケーションの責任 | 65 |
| 適用指針 | |
| 1. 本実務指針の範囲 | A1 |
| 2. 定義 | A4 |
| 3. 職業倫理に関する規定 | A6 |
| 4. 品質管理 | A7 |
| 5. 経営者及び監査役等 | A8 |
| 6. 保証業務契約の新規の締結及び更新 | |
| (1) 保証業務を実施するための能力と適性 | A9 |
| (2) 受託会社確認書 | A10 |
| (3) 受託会社確認書に対する合理的な基礎 | A11 |
| (4) リスクの識別 | A12 |
| (5) 保証業務の契約条件の変更の受諾 | A13 |
| 7. 保証業務の計画と実施 | A16 |
| 8. 規準の適切性の評価 | A21 |
| 9. 重要性 | A24 |
| 10. 受託会社のシステムの理解 | A27 |
| 11. 証拠の入手 | |
| (1) 記述書に関する証拠の入手 | A29 |
| (2) 内部統制のデザインに関する証拠の入手 | A32 |
| (3) 内部統制の運用状況の有効性に関する証拠の入手 | A35 |
| 12. 専門家の業務の利用 | |
| (1) 品質管理手続の整備 | A42 |
| (2) 専門家の業務の理解 | A44 |
| (3) 専門家の業務の評価 | A46 |
| 13. 内部監査人の作業 | |
| (1) 内部監査機能の理解 | A47 |

| | |
|--|-----|
| (2) 内部監査の利用の可否及びその利用の程度の判断..... | A48 |
| (3) 内部監査人の特定の作業の利用..... | A49 |
| (4) 業務実施者の保証報告書に及ぼす影響..... | A50 |
| 14. 経営者確認書 | A52 |
| 15. その他の記載内容 | A54 |
| 16. 調書 | A56 |
| 17. 業務実施者の保証報告書の作成 | |
| (1) 業務実施者の保証報告書の記載内容..... | A57 |
| (2) 業務実施者の保証報告書の想定利用者と目的..... | A58 |
| (3) 運用評価手続の記述 | A59 |
| (4) 除外事項付意見 | A60 |
| 18. その他のコミュニケーションの責任 | A63 |
| 適用 | |
| 付録 1 受託会社確認書の記載例 | |
| 付録 2 業務実施者の保証報告書の文例 | |
| 付録 3 除外事項付意見を表明する場合の業務実施者の保証報告書の文例 | |
| 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 | |

《 本実務指針の範囲及び目的》

《 1 . 本実務指針の範囲》

- 1 . 本実務指針は、公認会計士又は監査法人（以下「公認会計士等」という。）が、委託会社の業務を提供する受託会社の内部統制に関して、委託会社等（想定利用者）が利用するための報告書を提供する保証業務のうち、「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（付録4、以下「原則と規準」という。）」に基づいて内部統制を検証し、報告する保証業務に関する実務上の指針を提供するものである。（A1 項及び A2 項参照）
- 2 . 保証業務において、業務実施者は、保証業務リスクを許容可能な低い水準に抑える必要がある。IT 委員会実務指針第 5 号「IT に係る保証業務等の実務指針（一般指針）」によれば、公認会計士等が業務実施者として行う IT に係る保証業務は、主題に係る業務対象の作成者又は実施者が、一定の規準によって主題を評価又は測定した結果を表明する情報（以下「主題情報」という。）について、又は、主題それ自体について、保証報告書の利用者に対して信頼性を付与するために、業務実施者が自ら入手した証拠に基づき規準に照らして判断した結果を結論として報告する業務である。本実務指針は、合理的な保証を提供する主題情報に対する保証業務で、かつ、結論の報告の様式が直接に主題に対する結論を報告する方式に関する実務上の指針のみを提供している。（第 11 項及び第 61 項(11)参照）
- 3 . 本実務指針は、受託会社が内部統制のデザインの適切性に対する責任を有する場合、又はデザインの適切性に対する責任を有していないものの、それについて主題情報を表明することができる場合のみに適用される。本実務指針は、以下の保証業務を取り扱うものではない。（A3 項参照）
 - (1) 受託会社の内部統制が記載されたとおりに運用されているかどうかに関してのみ報告する保証業務
 - (2) 監査・保証実務委員会実務指針第 86 号「受託業務に係る内部統制の保証報告書」が対象とする保証業務
- 4 . 本実務指針に記載のない事項については、IT 委員会実務指針第 5 号「IT に係る保証業務等の実務指針（一般指針）」に準拠する。

《 2 . 目的》

- 5 . 本実務指針における業務実施者の目的は、以下のとおりである。
 - (1) 「原則と規準」に基づき、以下に関する合理的な保証を得ること。

受託会社のシステムに関する記述書が、特定期間にわたって（又は、タイプ 1 の報告書の場合、基準日現在に）デザインされ業務に適用されているシステムを全ての重要な点において適正に表示していること。

受託会社のシステムに関する記述書に記載された該当する原則とその規準に関連する内部統制が、特定期間にわたって（又は、タイプ 1 の報告書の場

合、基準日現在に)有効に運用されたならば、該当する原則とその規準を充足するよう全ての重要な点において適切にデザインされていること。

タイプ2の報告書の場合、受託会社のシステムに関する記述書に記載された該当する原則とその規準が特定期間にわたって充足されていたという合理的な保証を提供するよう、内部統制が全ての重要な点において該当する原則とその規準を充足するよう有効に運用されていること。

- (2) 業務実施者の発見事項に従って上記(1)の事項について報告すること。

《 3 . 定義》

6 . 本実務指針における用語の定義は、以下のとおりとする。

- (1) 「委託会社」 - 受託会社の提供する業務を利用する会社をいう。
- (2) 「委託会社の相補的な内部統制」 - 受託業務をデザインする段階で、委託会社において整備されることを受託会社が想定する内部統制であり、受託会社のシステムに関する記述書において記載された該当する原則とその規準の充足に必要な内部統制として識別され、記載されるものをいう。
- (3) 「一体方式」 - 受託会社が受託業務の一部を再委託する場合における、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保証報告書(以下「受託会社の内部統制の保証報告書」という。)上での再受託会社の提供する業務の取扱いの方式の一つをいう。一体方式では、受託会社のシステムに関する記述書に再受託会社に再委託している業務の内容が記載され、かつ、再受託会社の該当する原則とその規準及び関連する内部統制が受託会社のシステムに関する記述書及び業務実施者の業務の範囲に含まれる。(A5項参照)
- (4) 「運用評価手続」 - 受託会社のシステムに関する記述書に記載された該当する原則とその規準を充足する内部統制について、その運用状況の有効性を評価するため立案された手続をいう。
- (5) 「該当する原則とその規準」 - 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(付録4)のうち、当該受託会社の経営者によって選択された原則とその規準をいう。
- (6) 「規準」 - 主題を評価又は測定するために使用される規準をいう。規準には、該当する場合、表示と開示に関する規準が含まれる。
- (7) 「業務実施者」 - 受託会社からの依頼に基づき、受託会社の内部統制に関して保証報告書を提供する公認会計士等をいう。
- (8) 「再受託会社」 - 委託会社の内部統制に関連すると思われる業務を委託会社に提供するために、受託会社が受託業務の一部を他の会社に再委託する場合の当該他の会社をいう。
- (9) 「再受託会社の内部統制」 - 該当する原則とその規準の充足を合理的に保証する再受託会社の内部統制をいう。
- (10) 「受託会社」 - 受託業務を委託会社に提供する第三者組織(又はその一部)をいう。
- (11) 「受託会社確認書」 - 第6項(15)、又はタイプ1の報告書の場合、第6項(14)に記載されている受託会社により作成された受託業務に係る内部統制の

確認書をいう。

(12) 「受託会社のシステム」(又は「システム」) - 業務実施者の保証報告書が対象とする業務を委託会社に提供するために、受託会社がデザインし業務に適用するために特定されたインフラ、ソフトウェア、人員、手続、データの五つの重要な構成要素を総称していう。受託会社のシステムに関する記述書には、対象とする業務、記述書が対象とする期間(又はタイプ1の報告書の場合は基準日)該当する原則とその規準、関連する内部統制についての記述が含まれる。

(13) 「受託会社の内部統制」 - 業務実施者の保証報告書の対象となる該当する原則とその規準の充足を合理的に保証する内部統制をいう。(A4項参照)

(14) 「受託会社のシステムのセキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関する記述書(以下「受託会社のシステムに関する記述書」という。)及び内部統制のデザインに関する報告書」(本実務指針では「タイプ1の報告書」と呼称する。)- 以下を含む報告書をいう。

受託会社のシステムに関する記述書

以下の事項に関する受託会社確認書

ア．受託会社のシステムに関する記述書が、適切な規準に基づいて、基準日現在にデザインされ業務に適用されている受託会社のシステムを全ての重要な点において適正に表示していること。

イ．受託会社のシステムに関する記述書に記載された該当する原則とその規準に関連する内部統制が、該当する原則とその規準を充足するよう、基準日現在に全ての重要な点において適切にデザインされていること。

上記 ア及びイに記載された事項について、合理的な保証を提供する業務実施者の保証報告書

(15) 「受託会社のシステムに関する記述書並びに内部統制のデザイン及び運用状況に関する報告書」(本実務指針では「タイプ2の報告書」と呼称する。)- 以下を含む報告書をいう。

受託会社のシステムに関する記述書

以下の事項に関する受託会社確認書

ア．受託会社のシステムに関する記述書が、適切な規準に基づいて、特定期間にわたってデザインされ業務に適用されている受託会社のシステムを全ての重要な点において適正に表示していること。

イ．受託会社のシステムに関する記述書に記載された該当する原則とその規準に関連する内部統制が、該当する原則とその規準を充足するよう、特定期間にわたって全ての重要な点において適切にデザインされていること。

ウ．受託会社のシステムに関する記述書に記載された該当する原則とその規準に関連する内部統制が、該当する原則とその規準を充足するよう、特定期間にわたって全ての重要な点において有効に運用されていること。

以下を含む業務実施者の保証報告書

ア．上記 アからウの事項についての合理的な保証

イ．運用評価手続とその結果に関する記述

(16) 「除外方式」 - 受託会社が受託業務の一部を再委託する場合における、受託会社の内部統制の保証報告書上での再受託会社の提供する業務の取扱いの方式

の一つをいう。除外方式では、受託会社のシステムに関する記述書に再受託会社に再委託している業務の内容が記載されるが、再受託会社の該当する原則とその規準及び関連する内部統制は、受託会社のシステムに関する記述書及び業務実施者の業務の範囲から除かれる。受託会社のシステムに関する記述書及び業務実施者の業務の範囲には、再受託会社の内部統制の有効性をモニタリングする受託会社の内部統制が含まれ、これには、受託会社が再受託会社の内部統制の保証報告書を入手して検討することが含まれることがある。

- (17) 「内部監査機能」 - 受託会社において、確立され、又は提供されている評価活動をいう。当該機能には、内部統制の妥当性及び有効性を検討、評価及びモニタリングすることが含まれる。
- (18) 「内部監査人」 - 内部監査機能の活動に従事する者をいう。内部監査人は内部監査部門又はそれと同様の機能を有する部門に属することがある。
- (19) 「想定利用者」 - 委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局であり、受託会社によって提供される業務の性質、受託会社のシステムの作用、内部統制とその限界、相補的な内部統制の作用及び該当する原則とその規準とその充足を脅かすリスクに関する十分な知識と理解を有すると想定される者をいう。

委託会社は一般的に想定利用者に含まれるが、幾つかの実例(例えば、報告書が受託会社に係る規制当局によって利用される場合)では、委託会社は想定利用者に含まれない場合がある。

なお、受託会社は想定利用者となることはできるが、唯一の想定利用者となることはできない。

《 要求事項》

《 1 . 本実務指針の遵守》

- 7 . 業務実施者は、個々の保証業務に関連する本実務指針の要求事項を全て遵守しなければならない。業務実施者は、それらを全て遵守しない限り、本実務指針に準拠した旨を保証報告書に記載してはならない。

《 2 . 職業倫理に関する規定》

- 8 . 業務実施者は、IT委員会実務指針第5号「ITに係る保証業務等の実務指針(一般指針)」に準拠して、保証業務に関連する職業倫理に関する規定(独立性に関連するものを含む。)を遵守しなければならない。(A6項参照)

《 3 . 品質管理》

- 9 . 業務実施者は、IT委員会実務指針第5号「ITに係る保証業務等の実務指針(一般指針)」に準拠して、品質管理体制を整備し、個々の保証業務に関連する品質管理手続を適用しなければならない。(A7項参照)

《 4 . 経営者及び監査役等 》

10. 業務実施者は、本実務指針に基づき、受託会社に対して質問、経営者確認書の依頼、コミュニケーションを行う場合、受託会社の経営者又は監査役、監査役会若しくは監査等委員会（以下、監査役、監査役会又は監査等委員会を「監査役等」という。）の誰に対して行うのが適切かを判断しなければならない。業務実施者は、確認事項に対する適切な責任と知識を有する者は誰かを考慮して、この判断を行わなければならない。（A8項参照）

《 5 . 保証業務契約の新規の締結及び更新 》

11. 業務実施者は、保証業務契約の新規の締結又は更新の前に、以下を行わなければならない。業務実施者は、以下を実施した結果に満足できない場合には、保証業務契約を新規に締結又は更新してはならない。

- (1) 以下について判断すること。

業務実施者が保証業務を実施する能力と適性を有するかどうか。（A9項参照）

受託会社がシステムに関する記述書を作成する際に適用する規準が、想定利用者にとって適切であり、かつ、利用可能であるかどうか。

保証業務及び受託会社のシステムに関する記述書の範囲が極めて限定されているため、想定利用者にとって有用でない可能性があるかどうか。

保証業務を受嘱又は継続した場合に、保証業務に関連する職業倫理に関する規定又は本実務指針の要求が満たされない結果となる可能性を示す事項があるかどうか。

- (2) 受託会社が以下の責任を有することを認識し理解していることについて受託会社の合意を得ること。

システムに関する記述書及び当該記述書に添付される受託会社確認書を作成すること（記述書と受託会社確認書の記載内容の網羅性、正確性及び表示方法を含む。）。（A10項参照）

システムに関する記述書に添付される受託会社確認書に対する合理的な基礎を得ること。（A11項参照）

システムに関する記述書の作成において使用した規準を受託会社確認書に記載すること。

システムに関する記述書に「原則と規準」のうち選択された該当する原則とその規準を全て記載すること。

システムに関する記述書に記載する原則は、通常、想定利用者からの要請を考慮して受託会社の経営者によって選択される。

システムに関する記述書に記載された該当する原則とその規準の充足を妨げるおそれがあるリスクを識別すること、及び、識別したリスクを低減し、該当する原則とその規準を充足する合理的な保証を提供する内部統制をデザインし、業務に適用すること。（A12項参照）

以下を業務実施者に提供すること。

ア．受託会社がシステムに関する記述書とそれに添付される受託会社確認書

に関連すると認識している記録や証憑書類等の全ての情報。これには、受託会社と委託会社の間で締結した業務契約書が含まれる。

イ．業務実施者が保証業務の目的に関連して受託会社に依頼する、全ての追加的な情報

ウ．業務実施者が証拠を入手するために必要であると判断した、受託会社の構成員への制限のない質問や面談の機会

《(1) 保証業務契約書の作成》

12．業務実施者は、第 11 項で合意した事項を含め、受託会社と合意した保証業務の条件を記載した保証業務契約書を受託会社との間で作成しなければならない。

《(2) 保証業務の契約条件の変更の受諾》

13．業務実施者は、保証業務の終了前に、業務の内容を変更することを受託会社から依頼された場合、その変更に対する正当な理由があるかどうか確かめなければならない。(A13 項から A15 項参照)

《6．保証業務の計画と実施》

14．業務実施者は、保証業務を効果的に実施できるように業務を計画しなければならない。(A16 項から A18 項参照)

15．業務実施者は、記述書の適正な表示、内部統制のデザインの適切性、又はタイプ 2 の報告書の場合、内部統制の運用状況の有効性が損なわれる可能性があることを認識し、職業的専門家としての懐疑心を保持して保証業務を計画し実施しなければならない。(A19 項参照)

16．業務実施者は、前項のリスクを識別し、評価するのに十分で、かつ、追加の証拠収集手続を立案し実施するのに十分なように、受託会社のシステム及びその他の保証業務に影響を及ぼす事項を理解しなければならない。(A20 項参照)

《(1) 規準の適切性の評価》

17．業務実施者は、システムに関する記述書の作成、該当する原則とその規準に関連する内部統制が適切にデザインされているかどうかの評価及びタイプ 2 の報告書の場合、該当する原則とその規準に関連する内部統制が有効に運用されているかどうかの評価において、受託会社が適切な規準を使用しているかどうかを評価しなければならない。

18．業務実施者は、受託会社のシステムに関する記述書を評価する規準の適切性を評価する際、当該規準に少なくとも以下が含まれているかどうかを判断しなければならない。

(1) 記述書に、受託会社のシステムがどのようにデザインされ、業務に適用されているかが記載されているかどうか。これには、該当する場合、以下が含まれる。

提供される業務の種類

業務提供に利用されるシステムの範囲

業務提供に利用されるシステムの構成要素

・ インフラストラクチャー：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、モバイル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やアプリケーションプログラムをサポートするITシステムソフトウェア(オペレーティングシステム、ミドルウェア及びユーティリティ)
- ・ 人員：システムのガバナンス、運用及び利用に携わる人員(開発者、運用担当者、組織のユーザ、ベンダーの担当者及び管理者)
- ・ 手続：自動処理及び手作業の手続
- ・ データ：システムによって利用又は処理されたトランザクション、ファイル、データベース、テーブル及びアウトプット

上記のほか重要な事象や状況を受託会社のシステムにより把握し対応する方法

委託会社向け報告書等を作成するために用いているプロセス

該当する原則とその規準及びそれらを充足するようデザインされた内部統制

内部統制をデザインする段階で想定されている委託会社の相補的な内部統制

受託会社の統制環境、リスク評価プロセス、情報システム(関係する業務プロセスを含む。)と伝達、統制活動、モニタリング活動の側面のうち、受託業務に関連するもの

- (2) タイプ2の報告書の場合、記述書の対象とする期間における受託会社のシステムの変更の内容が記述書に記載されているかどうか。
- (3) 記述書の対象とする受託会社のシステムに関連する情報が省略又は歪曲されていないかどうか。ただし、記述書は広範囲の想定利用者に共通するニーズを満たすために作成される。したがって、個々の想定利用者がその特定の環境において重要と考える受託会社のシステムの全ての側面が含まれているわけではない。
- (4) 報告書がプライバシー原則を対象としている場合、必要により、以下が含まれる。

個人から収集し、又は委託会社や他の組織から入手したパーソナル・インフォメーションの種類、それらの情報の収集方法。委託会社が収集している場合、受託会社による入手方法

ア．委託会社との合意書、法令によりパーソナル・インフォメーションに適用される詳細な要求事項を識別し、イ．それらの要求事項に合致する内部統制と実務を導入するプロセス

受託会社が、パーソナル・インフォメーションを収集、利用、保持、開示及び廃棄又は匿名化している場合、当該個人に提供しているプライバシー通知は、該当する原則とその規準に記載されたプライバシー通知の規準に準拠して作成されている。

受託会社ではなく、委託会社に個人にプライバシー通知を提供する責任が

ある場合、委託会社による個人へのプライバシー通知の方法、委託会社によるプライバシー通知を個人に伝達する責任及び受託会社における自らのプライバシー実務の声明上、委託会社へプライバシー実務を伝達する責任。これらに関する声明には、以下の情報が含まれる。

ア．受託会社とその委託会社間のほとんどの合意に共通した重要なプライバシー及び関連するセキュリティの要求事項並びに受託会社が全て又はほとんどの委託会社に適合する委託会社との合意におけるその他の要求事項の概要

イ．委託会社との合意書に含まれない、受託会社が全て若しくはほとんどの委託会社に適合する法令、業界又は市場から必須となる重要なプライバシー及び関連するセキュリティの要求事項の概要

ウ．委託会社との合意書で認められたパーソナル・インフォメーションの収集目的、利用、開示並びにその合意書で禁じられているパーソナル・インフォメーションの収集目的、利用、開示に関する委託会社によるコミットメント及びこれらの合意書で禁止されていないパーソナル・インフォメーションの収集目的、利用、開示以外のもの

エ．記載された目的若しくは契約要件において必要とされるものを超えない期間若しくは法令で要求される期間で保持される情報に関する声明又はその他の保持実務に関する声明

オ．廃棄される情報の滅失、盗難、誤用又は未承認のアクセスを防止する方法に関する声明

カ．個人が自らの情報を閲覧、更新又は修正するアクセスを得るために、委託会社から認められた手続の受託会社による支援の方法

キ．パーソナル・インフォメーションが正確かつ完全なものであるかを特定する手続及び受託会社が委託会社から許可された修正手続をどのように導入したかに関する記述

ク．個人から（個人から直接又は委託会社を経由して間接かにかかわらず）の自己のパーソナル・インフォメーションに関する問合せ、苦情及び紛争についての受託会社の取扱方法

ケ．文書化されたセキュリティプログラムの存在と、それが業界やその他の基準に基づいている事に関する声明

コ．受託会社が委託会社にとって適切であると考えるプライバシー実務に係るその他の情報

受託会社ではなく、委託会社に個人にプライバシー通知を提供する責任がある場合、受託会社のプライバシー実務の声明

(5) 受託会社が再受託会社を利用している場合、必要により、以下が含まれる。

再受託会社又はその他の者と、情報を提供又は受領する場合

ア．情報の提供又は受領の方法、再受託会社又はその他の者の役割

イ．受託会社のプライバシー実務の声明に準拠して、その情報が保護されている事を特定するために実施される手続

再受託会社が存在し、除外方式を選択している場合

ア．再受託会社が提供するサービスの性質

イ．責任が再受託会社に委任された、パーソナル・インフォメーションライフサイクルのあらゆる側面

ウ．再受託会社単独又は受託会社との組合せの内部統制によって充足するように意図された該当するそれぞれの付録 4 の規準及び除外した再受託会社で実装することが期待されている当該規準を充足する内部統制の種類

エ．再受託会社が、受託会社のプライバシーコミットメントを遵守するために実施が必要となる活動の種類

再受託会社が存在し、一体方式を選択している場合における、再受託会社の内部統制

受託会社及び再受託会社の内部統制で対応していない該当する付録 4 の規準とその理由

19．業務実施者は、内部統制のデザイン及び内部統制の運用状況の有効性を評価する規準の適切性を評価する際、当該規準に該当する原則とその規準が含まれているかどうかを判断しなければならない。

20．タイプ 2 の報告書の場合、業務実施者は、記述書に記載された該当する原則とその規準が充足されるという合理的な保証を提供する内部統制の運用状況の有効性を評価する規準の適切性を評価する際、当該規準が、少なくとも、内部統制が特定期間にわたりデザインされたとおりに一貫して業務に適用されていることを含むかどうかを判断しなければならない。(A21 項から A23 項参照)

《(2) 重要性》

21．業務実施者は、保証業務を計画し実施する際に、記述書の適正な表示、内部統制のデザインの適切性、及びタイプ 2 の報告書の場合、内部統制の運用状況の有効性に関して、重要性を考慮しなければならない。(A24 項から A26 項参照)

《(3) 受託会社のシステムの理解》

22．業務実施者は、保証業務の範囲に含まれる内部統制を含め、受託会社のシステムを理解しなければならない。(A27 項から A28 項参照)

《7．証拠の入手》

23．業務実施者は、合理的な保証を得るため、リスク評価に応じた証拠収集手続の種類、時期及び範囲を決定し、保証業務リスクを許容可能な低い水準に抑える十分かつ適切な証拠を入手しなければならない。それにより、業務実施者は、意見表明の基礎となる結論を導くことができる。

《(1) 記述書に関する証拠の入手》

24．業務実施者は、受託会社のシステムに関する記述書を入手して読み、保証業務の範囲に含まれる記述が適正に表示されているかどうかを評価しなければならない。当該評価には、以下の事項を含めなければならない。(A29 項から A30 項参照)

(1) 受託会社のシステムに関する記述書に記載された該当する原則とその規準が、適切かどうか。

(2) 記述書で識別された内部統制が業務に適用されているかどうか。

(3) 委託会社の相補的な内部統制がある場合、それらが適切に記述されているかど

うか。

- (4) 再受託会社が業務を実施している場合、再受託会社の業務に関して一体方式と除外方式のいずれが採用されているかを含め、再受託会社の実施する業務について適切に記載されているかどうか。

25. 業務実施者は、質問とその他の手続を組み合わせることで実施することにより、受託会社のシステムが業務に適用されているかどうかを判断しなければならない。

その他の手続には、どのように受託会社のシステムが運用され、内部統制が適用されているかについて、観察又は記録や他の文書の閲覧を含めなければならない。
(A31 項参照)

《(2) 内部統制のデザインに関する証拠の入手》

26. 業務実施者は、受託会社のシステムに関する記述書に記載された該当する原則とその規準を充足するために必要となる受託会社の内部統制を判断するとともに、当該内部統制が該当する原則とその規準を充足するよう適切にデザインされているかどうかを評価しなければならない。

この評価には、以下の事項を含めなければならない。(A32項からA34項参照)

- (1) 受託会社のシステムに関する記述書に記載された該当する原則とその規準の充足を妨げるおそれがあるリスクを識別すること。
- (2) 受託会社のシステムに関する記述書において識別された内部統制と当該リスクとの関連性を評価すること。

《(3) 内部統制の運用状況の有効性に関する証拠の入手》

27. 業務実施者は、タイプ2の報告書を提供する場合、受託会社のシステムに関する記述書に記載された該当する原則とその規準の充足に必要であると判断した内部統制の運用評価手続を実施して、期間を通じた当該内部統制の運用状況の有効性を評価しなければならない。過去の期間において内部統制が十分に運用されていたことについて入手した証拠は、たとえ対象期間に入手した証拠によって補完されるとしても、必ずしも運用評価手続の実施を縮小させる根拠にはならない。(A35 項から A38 項参照)

28. 業務実施者は、運用評価手続の立案と実施に当たって、以下の手続を実施しなければならない。

- (1) 以下に関する証拠を入手するために、質問とその他の手続を組み合わせる。

内部統制がどのように運用されていたか。

その運用は一貫していたか。

誰がどのような方法で運用していたか。

- (2) 運用評価手続の対象となる内部統制が他の内部統制(間接的な内部統制)に依存しているかどうか、依存している場合にはこれら間接的な内部統制の運用状況の有効性を裏付ける証拠を入手する必要があるかどうかを判断する。(A39項参照)

- (3) 運用評価手続の対象項目について手続の目的に適う有効な抽出方法を決定する。(A40項からA41項参照)

29. 業務実施者は、運用評価手続の範囲の決定に当たり、少なくとも以下の諸事項を

含め、母集団の特性を考慮しなければならない。

- (1) 内部統制の特性
- (2) 実施頻度（例えば、月次、日次、1日に複数回）
- (3) 予想逸脱率

《サンプリング》

30．業務実施者は、サンプリングを利用する場合、以下を実施しなければならない。
（A40項からA41項参照）

- (1) サンプリングを立案する際、手続の目的と、サンプルを抽出する母集団の特性を考慮する。
- (2) サンプリングリスクを許容可能な低い水準に抑えるために、十分なサンプル数を決定する。
- (3) 母集団の全てのサンプリング単位に抽出の機会が与えられるような方法で、サンプルを抽出する。
- (4) 抽出したサンプルが立案した手続の適用対象として適当でない場合、代替りのサンプルを抽出して手続を実施する。
- (5) 抽出したサンプルに立案した手続又は適切な代替手続を実施できない場合、当該サンプルを逸脱として扱う。

《逸脱の内容と原因》

31．業務実施者は、識別した全ての逸脱の内容と原因を調査して、以下のいずれに該当するかの判断を行わなければならない。

- (1) 識別した逸脱が予想逸脱率の範囲内にあり、許容可能である。したがって、実施した運用評価手続によって、内部統制が特定期間にわたって有効に運用されていると結論付けるための適切な基礎が得られた。
- (2) 特定の該当する原則とその規準に関連する内部統制が特定期間にわたり有効に運用されているかどうかを結論付けるため、当該内部統制又はその他の内部統制に関する追加的な運用評価手続が必要である。（A32項参照）
- (3) 実施された運用評価手続によって、内部統制が特定期間にわたり有効に運用されていなかったと結論付ける適切な基礎が得られた。

32．業務実施者は、サンプルについて発見した逸脱を例外的事象であるとする極めて稀な状況において、該当する原則とその規準が特定期間にわたり充足されていたと結論付けることのできる他の内部統制が識別されないときは、当該逸脱が母集団を代表していないという相当に高い心証を得なければならない。この場合には、業務実施者は、その逸脱が残りの母集団に影響を及ぼさないという十分かつ適切な証拠を入手するための追加的な手続を実施しなければならない。

《 8 ． 専門家の業務の利用 》

《(1) 専門家の業務の利用》

33．業務実施者は、証拠の収集と評価のために業務実施者の事務所内部又は外部の専門家の業務を利用する場合には、保証業務チームと外部の専門家が全体として、受託会社のシステム及び該当する原則とその規準に関して十分かつ適切な証拠を入

手したかどうかを判断するのに十分な専門知識を有していることを確かめなければならない。(A42 項から A43 項参照)

《(2) 専門家の業務の理解》

34. 業務実施者は、表明する意見に対し責任を負うことができるよう、専門家が実施する業務を理解しなければならない。(A44 項から A45 項参照)

《(3) 専門家の業務の評価》

35. 業務実施者は、専門家が実施した業務が保証業務の目的に照らして適切であるという十分かつ適切な証拠を入手しなければならない。(A46項参照)

《 9 . 内部監査の利用》

《(1) 内部監査機能の理解》

36. 業務実施者は、受託会社が内部監査機能を有する場合、内部監査機能が業務実施者の保証業務に関連する可能性があるかどうか判断するため、内部監査機能の責任及び実施する活動の内容について理解しなければならない。なお、独立性に関する重要な阻害要因と考えられるため、本実務指針に基づく保証業務においては、業務実施者が手続を実施するに当たり、内部監査人を直接の補助者として利用してはならない。(A47 項参照)

《(2) 内部監査の利用の可否及びその利用の程度の判断》

37. 業務実施者は、以下の事項を判断しなければならない。

- (1) 内部監査人の作業が業務実施者の保証業務の目的に照らして適切かどうか。
- (2) 内部監査人の作業が適切な場合には、内部監査人の作業が業務実施者の手続の種類、時期又は範囲に及ぼし得る影響

38. 内部監査人の作業が業務実施者の保証業務の目的に照らして適切かどうかを判断するに当たり、業務実施者は以下の事項を評価しなければならない。

- (1) 内部監査機能の客観性
- (2) 内部監査人の専門的能力
- (3) 内部監査人が専門職として正当な注意を払い作業を実施するかどうか。
- (4) 内部監査人と業務実施者との間で有効なコミュニケーションが図れるかどうか。

39. 内部監査人の作業が業務実施者の手続の種類、時期又は範囲に及ぼし得る影響を判断するに当たり、業務実施者は以下の事項を考慮しなければならない。(A48 項参照)

- (1) 内部監査人により実施された又は実施される予定の特定の作業の内容及び範囲
- (2) 業務実施者の結論に対する内部監査人の作業の重要性
- (3) 業務実施者の結論の裏付けとして内部監査人により収集された証拠の評価において、主観的要素が介在する程度

《(3) 内部監査人の特定の作業の利用》

- 40．内部監査人の特定の作業を利用する際に、業務実施者は、業務実施者の目的に照らして適切かどうかを判断するため、当該作業を評価し、それらに対して手続を実施しなければならない。(A49 項参照)
- 41．内部監査人によって実施された特定の作業が業務実施者の目的に照らして適切かどうか判断するために、業務実施者は以下の事項を評価しなければならない。
- (1) 当該作業が、十分な専門的研修を受け、経験を有している内部監査人によって実施されたかどうか。
 - (2) 当該作業が適切に監督、査閲、文書化されたかどうか。
 - (3) 内部監査人が合理的な結論を得るのに十分な証拠を入手したかどうか。
 - (4) 到達した結論がその状況に応じて適切であるかどうか、及び内部監査人により作成された全ての報告書が実施された作業の結果と整合しているかどうか。
 - (5) 業務実施者の保証業務に関連する指摘事項が、内部監査人によって適切に解決されているかどうか。

《(4) 業務実施者の保証報告書に及ぼす影響》

- 42．業務実施者は、内部監査機能を利用した場合に、業務実施者の保証報告書の意見区分において、内部監査人の作業に関して言及してはならない。(A50 項参照)
- 43．タイプ2の報告書において、運用評価手続の実施に際して内部監査人の作業を利用した場合には、業務実施者の保証報告書の運用評価手続及びその結果の記述に、内部監査人の作業及び当該作業に関して業務実施者が実施した手続についての記載を含めなければならない。(A51 項参照)

《10．経営者確認書》

- 44．業務実施者は、受託会社（一体方式の場合、再受託会社を含む。）に、以下の事項について記載した経営者確認書を提出するように要請しなければならない。(A52 項参照)
- (1) システムに関する記述書に添付する受託会社確認書は適正である旨
 - (2) 保証業務契約書で合意したとおり（第11項(2) 参照）受託会社が全ての関連する情報及び情報を入手する機会を業務実施者に提供した旨
 - (3) 以下のいずれかに気付いている場合、それを業務実施者に示した旨
 - 違法行為、不正又は受託会社に起因し委託会社に影響を及ぼす可能性のある未修正の誤謬
 - 内部統制のデザインの不備
 - 内部統制が記述されたとおりに運用されていない事例
- 受託会社のシステムに関する記述書が対象とする期間の翌日から、業務実施者の保証報告書の日付までの間に発生し、基準日現在又は将来の受託会社のシステムに係る内部統制に重要な影響を及ぼす可能性のある全ての事象
- 45．経営者確認書は、業務実施者を宛先とする書簡でなければならない。経営者確認書の日付は、業務実施者の保証報告書の日付より後であってはならず、通常、保証報告書の日付と同一の日付とする。

46. 業務実施者が本実務指針の第 44 項(1)及び(2)に基づき経営者確認書において確認を要請した事項の全部又は一部について、受託会社との協議を行ってもなお受託会社から確認を得られない場合、業務実施者は、意見を表明してはならない。(A53 項参照)

《11. その他の記載内容》

47. 業務実施者は、受託会社のシステムに関する記述書及び業務実施者の保証報告書を含む文書にその他の記載内容が含まれる場合、システムに関する記述書との重要な相違を識別するため、その他の記載内容を通読しなければならない。
業務実施者は、重要な相違を識別するためにその他の記載内容を通読することにより、当該その他の記載内容に関する明らかな事実の虚偽記載に気付くことがある。
48. 業務実施者は、その他の記載内容の重要な相違又は明らかな事実の虚偽記載に気付いた場合、受託会社と当該事項について協議しなければならない。業務実施者は、その他の記載内容に重要な相違又は事実の虚偽記載が存在すると判断したが受託会社がそれを修正することに同意しない場合、適切な措置を講じなければならない。(A54 項から A55 項参照)

《12. 後発事象》

49. 業務実施者は、受託会社のシステムに関する記述書が対象とする基準日又は対象期間の最終日の翌日から業務実施者の保証報告書の日付までの間に、受託会社確認書に重要な影響を及ぼす可能性がある事象に受託会社が気付いたかどうか質問しなければならない。受託会社が当該事象に気が付いているが、当該情報をシステムに関する記述書において開示しない場合、業務実施者の保証報告書で開示しなければならない。
50. 業務実施者は、業務実施者の保証報告書の日付の翌日以降、受託会社のシステムに関する記述、内部統制のデザインの適切性又は運用状況の有効性に関して、いかなる手続を実施する義務も負わない。

《13. 調書》

51. 業務実施者は、経験豊富な業務実施者が、以前に当該保証業務に関与していなくとも以下の事項を理解できるように、調書を作成しなければならない。
- (1) 本実務指針及び適用される法令等に準拠して実施した手続の種類、時期及び範囲
 - (2) 手続を実施した結果及び入手した証拠
 - (3) 保証業務の過程で生じた重要な事項、その結論及びその際になされた職業的専門家としての重要な判断
52. 業務実施者は、実施した手続の種類、時期及び範囲の文書化において、以下の事項を記録しなければならない。
- (1) 運用評価手続を実施した項目又は対象を識別するための特性
 - (2) 手続を実施した者及びその完了日

(3) 査閲をした者、査閲日及び査閲の対象

53. 業務実施者は、内部監査人の特定の作業を利用する場合、内部監査人の作業の適切性の評価に関する結論及び実施した手続を調書に記載しなければならない。
54. 業務実施者は、受託会社及びその他の者と重要な事項について協議した場合には、重要な事項の内容、協議を実施した日及び協議の相手方等について文書化しなければならない。
55. 業務実施者は、重要な事項に関する結論を形成する過程において、矛盾した情報を識別した場合には、業務実施者がどのようにその矛盾した情報に対応したかについて、文書化しなければならない。
56. 業務実施者は、業務実施者の保証報告書日後、適切な期限内に、業務ファイルにおける調書を整理し、業務ファイルの最終的な整理についての事務的な作業を完了しなければならない。(A56 項参照)
57. 業務実施者は、業務ファイルの最終的な整理が完了した後、その保存期間が終了するまで、いかなる調書であっても、削除又は廃棄してはならない。
58. 業務ファイルの最終的な整理が完了した後に、既存の調書の修正又は新たな調書の追加が必要となった場合には、その修正や追加の内容にかかわらず、業務実施者は、以下の事項を文書化しなければならない。
 - (1) 修正又は追加が必要となった具体的理由
 - (2) 修正又は追加を実施した者及び実施日並びにそれらを査閲した者及び査閲日

《14. 業務実施者の保証報告書の作成》

59. 保証報告書作成に当たり、業務実施者は、表明する意見を裏付けるために、十分かつ適切な証拠が入手されたか否かを結論付けなければならない。
60. 保証報告書は文書で作成し、業務実施者の意見を明瞭に示すものでなければならない。

《(1) 業務実施者の保証報告書の記載内容》

61. 業務実施者の保証報告書には、以下の基本的な事項を含めなければならない。(A57 項参照)
 - (1) 独立した業務実施者の保証報告書であることを明瞭に示す表題
 - (2) 宛先
 - (3) 以下についての特定

受託会社のシステムに関する記述書及び受託会社確認書。タイプ2の報告書の場合には第6項(15)に記載されている事項、タイプ1の報告書の場合には第6項(14)に記載されている事項が受託会社確認書に含まれる。

受託会社のシステムに関する記述書のうち、業務実施者の意見の対象でない部分

受託会社の内部統制のデザインの適切性、運用の有効性を評価する、該当する原則とその規準

保証報告書がプライバシー原則を対象としている場合、受託会社のプライバシー実務の声明

記述書に委託会社の相補的な内部統制が必要であることが記載されている場合、業務実施者は委託会社の相補的な内部統制のデザインの適切性や運用状況の有効性を評価していない旨、及び、受託会社の内部統制に加えて委託会社の相補的な内部統制が適切にデザインされている、又は有効に運用されている場合にのみ、受託会社のシステムに関する記述書に記載された、該当する原則とその規準を充足する旨

再受託会社が業務を実施している場合、受託会社のシステムに関する記述書に記載されている再受託会社が実施している業務の内容及び取扱いの方式（一体方式又は除外方式）並びにア及びイ

ア．除外方式の場合、受託会社のシステムに関する記述書から関連する再受託会社の特定の該当する原則とその規準及び関連する内部統制が除外されている旨、及び業務実施者は再受託会社の内部統制について手続を実施していない旨

イ．一体方式の場合、受託会社のシステムに関する記述書に再受託会社の該当する原則とその規準及び関連する内部統制が含まれている旨、及び業務実施者は再受託会社の内部統制に対する手続を実施している旨

- (4) 規準、及び該当する原則とその規準を選択した者（ただし、受託会社が指定している場合は記載を省略できる。）
- (5) 保証報告書及びタイプ2の報告書の場合の運用評価手続の記述は、利用者として、想定利用者のみを想定している旨。また、想定利用者は、該当する原則及びその規準による評価において、委託会社自身が運用する内部統制に関する情報を含めたその他の情報とともに、当該システムを検討するための十分な理解を有していることが想定されている旨（A58項参照）
- (6) 受託会社が以下に対する責任を有する旨

受託会社のシステムに関する記述書及び記述書に添付される受託会社確認書の作成（記述書と受託会社確認書の網羅性、正確性及び表示方法を含む。）

受託会社のシステムに関する記述書が対象とする業務の提供

該当する原則とその規準の記載

受託会社のシステムに関する記述書に記載された該当する原則とその規準を充足するための内部統制のデザインと業務への適用

規準のうち、一部に関連する該当業務がないなどの理由から対応するものがなく、規準の記載を省略する場合にはその理由の記載

保証報告書がプライバシー原則を対象としている場合、プライバシー実務の声明に含まれるか、受託会社のシステムに関する記述書に添付されたコミットメントの遵守

- (7) 業務実施者の責任は、業務実施者が実施した手続に基づいて、受託会社の記述書、記述書に記載された該当する原則とその規準に関連する内部統制のデザイン、及び、タイプ2の報告書の場合、当該内部統制の運用状況の有効性がそれぞれ、該当する原則とその規準を充足していること、また、保証報告書がプライバシー原則を対象としている場合、必要に応じて、プライバシー実務の声明上のコミットメントが遵守されていることに対して意見を表明することにある旨

- (8) 本実務指針に準拠して業務を実施した旨及び本実務指針が、業務実施者に、全ての重要な点において、受託会社のシステムに関する記述書が適正に表示されているかどうか、内部統制が該当する原則とその規準を充足するよう適切にデザインされているかどうか、また、タイプ2の報告書の場合、内部統制が該当する原則とその規準を充足するよう有効に運用されているかどうか、さらに、保証報告書がプライバシー原則を対象としている場合、必要に応じて、プライバシー実務の声明上のコミットメントが遵守されていることについて合理的な保証を得るために手続を計画し実施することを求めている旨
- (9) 合理的な保証を得るための業務実施者の手続の要約、業務実施者が意見表明の基礎となる十分かつ適切な証拠を得たと判断している旨、及び、タイプ1の報告書の場合、業務実施者は、内部統制の運用状況の有効性に関する手続を実施しておらず、したがって、それに対する意見を表明しない旨
- (10) 内部統制の限界の記載及びタイプ2の報告書の場合、将来の期間にわたる内部統制の運用状況に関する有効性の評価の予測に伴うリスク
- (11) 適切な規準に基づいて積極的形式により以下に関して表明される業務実施者の意見

タイプ2の報告書の場合

- ア．記述書が、特定期間にわたりデザインされ業務に適用されていた受託会社のシステムを全ての重要な点において適正に表示しているかどうか。
- イ．受託会社のシステムに関する記述書に記載された該当する原則とその規準に関連する内部統制が、特定期間にわたって、全ての重要な点において該当する原則とその規準を充足するよう適切にデザインされているかどうか。なお、委託会社の相補的な内部統制が該当する原則とその規準の充足に必要な場合は、その条件についても記載する。
- ウ．記述書に記載された該当する原則とその規準の充足について合理的な保証を提供するために必要なものとして運用評価手続を実施した内部統制が、特定期間にわたって、全ての重要な点において該当する原則とその規準を充足するよう有効に運用されているかどうか。なお、委託会社の相補的な内部統制が該当する原則とその規準の充足に必要な場合は、その条件についても記載する。
- エ．保証報告書がプライバシー原則を対象としている場合、必要に応じて、全ての重要な点においてプライバシー実務の声明上のコミットメントが遵守されているかどうか。

タイプ1の報告書の場合

- ア．記述書が、基準日現在でデザインされ業務に適用されている受託会社のシステムを、全ての重要な点において適正に表示しているかどうか。
- イ．受託会社のシステムに関する記述書に記載された該当する原則とその規準に関連する内部統制が、基準日現在で、全ての重要な点において該当する原則とその規準を充足するよう適切にデザインされているかどうか。
- (12) 業務実施者の保証報告書の日付。業務実施者の保証報告書の日付は、業務実施者の意見表明の基礎となる十分かつ適切な証拠を入手した日よりも前の日付としてはならない。
- (13) 業務実施者の名称及び業務実施者の事務所の所在地。ただし、国内のみで流

通することを前提に日本語で作成された保証報告書は、保証報告書に業務実施者の事務所の所在地を記載する必要性は乏しいためその記載を省略することができる。

62. タイプ2の報告書の場合、業務実施者の報告書には、意見の後に別の区分を設け、又は別紙として、実施した運用評価手続及び当該手続の結果を記載しなければならない。業務実施者は、運用評価手続の記述に、以下を明確に記載しなければならない。

- (1) どの内部統制に運用評価手続を実施したか。
- (2) 手続の実施対象が母集団の全項目か又は一部の抽出項目か。
- (3) 運用評価手続の内容。運用評価手続の内容は、当該手続が想定利用者の目的に与える影響を想定利用者が判断できるように十分詳細なものでなければならない。

業務実施者は、逸脱を識別した場合には、逸脱が識別される結果となった運用評価手続の実施範囲（サンプリングを利用した場合にはサンプル数を含む。）及び発見された逸脱の数と内容を記載しなければならない。業務実施者は、実施した運用評価手続に基づき、該当する原則とその規準が充足されていたと結論付けた場合でも、逸脱について報告しなければならない。（A26項及びA59項参照）

《(2) 除外事項付意見》

63. 業務実施者は、以下の状況が存在する場合には、除外事項付意見を表明しなければならない。また、業務実施者の保証報告書において、除外事項付意見の理由について全て明記しなければならない。（A60項からA62項参照）

- (1) 業務実施者の手続実施に以下の事由により制約が存在し、その影響が重要と判断される場合には、その程度に応じて、限定意見を表明するか、又は意見を表明しない。

保証業務リスクを許容可能な低い水準に抑えるために必要な十分かつ適切な証拠を入手できない状況

十分かつ適切な証拠の入手を受託会社が妨げるような状況

- (2) 以下の状況又は事項が存在し、その影響が重要と判断される場合には、その程度に応じて、限定意見を表明するか、又は否定的意見を表明する。

受託会社の記述書が、全ての重要な点においてデザインされ業務に適用されていたとおりに、受託会社のシステムを適正に表示しているとはいえない。

記述書に記載された該当する原則とその規準に関連する内部統制が、全ての重要な点において該当する原則とその規準を充足するよう適切にデザインされているとはいえない。

タイプ2の報告書の場合、受託会社のシステムに関する記述書に記載された該当する原則とその規準の充足について合理的な保証を提供するために必要なものとして運用評価手続を実施した内部統制が、全ての重要な点において該当する原則とその規準を充足するよう有効に運用されているとはいえない。

64. 前項において、除外事項付意見の原因となる状況又は事項の影響が否定的意見を表明するほどではなく、又は意見を表明できないほどではないと判断する場合には、業務実施者は限定意見を表明しなければならない。限定意見は、「(その限定に係

する事項の影響)を除き」と表明される。

《15. その他のコミュニケーションの責任》

65. 業務実施者は、受託会社に起因し、委託会社に影響を及ぼす可能性がある違法行為、不正又は未修正の誤謬で、明らかに僅少ではないものに気付いた場合、当該事項により影響を受ける委託会社に適切に伝達されたかどうか判断しなければならない。当該事項が適切に伝達されておらず、受託会社にその意思がない場合には、業務実施者は適切な措置を講じなければならない。(A63項参照)

《 適用指針 》

《 1 . 本実務指針の範囲 》 (第 1 項及び第 3 項参照)

A1. 本実務指針において、受託会社によって提供される業務の例は以下のとおりである。

- ・ クラウドコンピューティングの業務：自由に構成可能なコンピューティング資源(例えば、ネットワーク、サーバー、記憶装置、アプリケーション、サービス)の共有プールへのオン・デマンドのネットワーク・アクセスを提供すること。
- ・ セキュリティの管理：委託会社のネットワーク及びコンピューティング・システムへのアクセスの管理(システムへのアクセス権を付与し、システムへの侵入を阻止、発見及び極小化すること。)
- ・ 顧客口座サービス：銀行や投資会社の顧客に代わり金融取引を処理すること(インターネットを通じた顧客の証券取引の処理、顧客口座記録の維持、顧客への処理、取引報告の確認等の提供)。
- ・ カスタマー・サポート：委託会社の顧客にオンライン又は電話で販売後の支援及びサービス管理を提供すること(苦情に関する質問、調査、回答等)。
- ・ 営業活動の自動化：営業組織を持っている委託会社のために、ビジネスの手続を自動化するためのソフトウェアを提供し維持すること(注文処理、情報共有、注文追跡、連絡先の管理、顧客管理、販売予測分析、従業員業務評価等)。
- ・ 企業のIT業務の外部委託サービス：委託会社のIT業務を管理、運用し、維持すること(ITデータ・センター、インフラ、アプリケーション・システム及びネットワーク、システム開発、セキュリティ、変更管理、ハードウェア、環境管理活動のようなIT活動の支援等)。

A2. 委託会社の経営者は、財務報告、法令遵守、業務の有効性・効率性と関連する委託会社が直面するリスクを評価し対処する実施責任がある。委託会社が重要なプロセス又は機能を実施するために受託会社と契約する場合、委託会社は受託会社のシステムと関連する追加的なリスクにさらされる。委託会社の経営者は受託会社にタスク又は機能を委託することができるが、委託会社の顧客に提供される製品やサービスに対する実施責任は委託することができない。通常委託会社の経営者は、顧客、株主及び規制当局に対して外部委託された機能に関する有効な内部統制を確立することの実施責任を負うと考えられる。

A3 . 委託会社がデザインしたシステム又は委託会社と受託会社間の契約で規定されているシステムを受託会社が運用している場合、受託会社はシステムのデザインの適切性について受託会社確認書において確認できないことがある。内部統制のデザインの適切性とそれらの運用状況の有効性には切り離せないつながりがある。したがって、業務実施者は、デザインの適切性に関する受託会社の確認が欠如している場合、該当する原則とその規準が充足されていたという合理的な保証を内部統制が提供していると結論付けることができず、内部統制の運用状況の有効性に関する意見を表明できない可能性が高い。

そのような場合、業務実施者は、運用評価手続を合意された手続業務として実施するか、又は、内部統制が記述されたとおりに運用されていたかどうかに関する結論を運用評価手続に基づいて報告する保証業務を実施することを選択する場合があるが、これらの業務はいずれも本実務指針の対象外である。

《 2 . 定義》（第 6 項(3)及び第 6 項(13)参照）

A4 . 「受託会社の内部統制」の定義には、受託会社が保持する委託会社の情報システムとしての側面が含まれる。また、受託会社の内部統制の構成要素のうちの一つ又は複数の側面が含まれることがある。例えば、統制環境、モニタリング活動、統制活動の側面が受託会社の提供する業務に関連する場合、それらは「受託会社の内部統制」に含まれることがある。一方、受託会社のシステムに関する記述書に記載された該当する原則とその規準の充足に関連しない内部統制は、「受託会社の内部統制」には含まれない。例えば、受託会社自身の情報システムに関連する内部統制は、「受託会社の内部統制」には含まれない。

A5 . 一体方式が使用される場合、本実務指針の要求事項は再受託会社に対しても適用される。これには、第 11 項(2) からに記載されている事項について、受託会社のみならず再受託会社の合意を得ることが含まれる。再受託会社で手続を実施する場合には、受託会社、再受託会社及び業務実施者間での調整とコミュニケーションが必要である。一体方式は、一般的に、受託会社と再受託会社間に資本関係がある、又は受託会社と再受託会社間の契約において手続の実施が規定されている場合のみ可能である。

《 3 . 職業倫理に関する規定》（第 8 項参照）

A6 . 業務実施者は、倫理規則及び独立性に関する指針に従う。保証業務に関連する職業倫理に関する規定は、本実務指針に基づく保証業務の実施において、業務実施者が委託会社に対して独立性を保持することを要求していない。

《 4 . 品質管理》（第 9 項参照）

A7 . 個々の業務に関連する品質管理の要素には、品質管理に関する責任、職業倫理及び独立性、契約の新規の締結及び更新、専門要員の採用、教育・訓練、評価及び選任、業務の実施並びに品質管理のシステムのモニタリングが含まれる。

《 5 . 経営者及び監査役等》（第 10 項参照）

A8 . 経営と企業統治の構造は、異なる文化及び法的な背景並びに規模や所有権の特徴等の影響を反映して、国や企業によって様々である。このような多様性が存在するため、業務実施者が特定の事項に関して誰に対してコミュニケーションを行うべきか、本実務指針において、全ての業務に対して規定することは不可能である。例えば、受託会社は、法人の一部門であることもあるが、複数の法人を含むこともある。そのような場合、経営者確認書の要請先として適切な経営者を特定する際には、職業的専門家としての判断を要することがある。

《 6 . 保証業務契約の新規の締結及び更新》

《(1) 保証業務を実施するための能力と適性》（第 11 項(1) 参照）

A9 . 保証業務の実施に関連する能力と適性には、以下のような事項が含まれる。

- ・ 関連する業界の知識
- ・ ITと情報システムの理解
- ・ 「原則と規準」の理解
- ・ 「原則と規準」に係る内部統制の適切なデザインに関連するリスクの評価の経験
- ・ 「原則と規準」に係る内部統制の運用評価手続の立案及び実施並びにその結果の評価の経験

《(2) 受託会社確認書》（第 11 項(2) 参照）

A10 . 業務契約の新規の締結又は更新に関して業務実施者が合意した後、受託会社が受託会社確認書の提供を拒否することは範囲の制約となり、業務実施者が保証業務契約を解除する理由となる。

業務実施者は、保証業務契約を解除することが実務的に困難な場合、意見を表明しない。

《(3) 受託会社確認書に対する合理的な基礎》（第 11 項(2) 参照）

A11 . タイプ 2 の報告書の場合、受託会社確認書には、受託会社のシステムに関する記述書に記載された該当する原則とその規準に関連する内部統制が、特定期間にわたって該当する原則とその規準を充足するよう有効に運用されている旨の記述が含まれる。受託会社のモニタリング活動は、内部統制のデザインの適切性及び運用状況の有効性に関する受託会社確認書を裏付ける証拠を提供することがある。モニタリング活動は、期間を通じて内部統制の有効性を評価するプロセスである。モニタリング活動には、内部統制の有効性の評価を適時に行うこと、不備を識別し受託会社内部の適切な者に報告すること、必要な是正措置を実施することが含まれている。受託会社は、日常的モニタリング活動と独立の評価、又はその組合せを通じて、モニタリング活動を実施する。日常的モニタリング活動の度合いとその有効性が高ければ、独立の評価の必要性は少なくなる。日常的モニタリング活動は、しばしば受託会社の日常の反復継続的な活動の中に組み込まれており、経営者や部門責任者等が通常行う経営管理活動を含むものである。内部監査人又は同様の機能を担う者は、受託会社の活動のモニタリングに貢献していることがある。また、モニタリン

グ活動には、顧客からの苦情や規制当局からの改善勧告等、問題点を指摘し、改善の必要のある点を示唆する外部者からの情報の利用も含まれる。業務実施者が内部統制の運用状況の有効性に関して報告するという事実は、受託会社が受託会社確認書に対する合理的な基礎を得るために自ら実施するプロセスを代替するものではない。

《(4) リスクの識別》（第11項(2) 参照）

A12．第6項(5)の該当する原則とその規準は、内部統制が低減しようとするリスクに関連付けられる。

《(5) 保証業務の契約条件の変更の受諾》（第13項参照）

A13．保証業務の範囲の変更の要請に正当な理由がないことがある。例えば、業務実施者の意見が除外事項付意見となる可能性があるため、特定の該当する原則とその規準を除くことを要請される場合、又は、受託会社確認書が業務実施者に提供されず、本実務指針の対象外となる保証業務を実施することを要請される場合などがある。

A14．一方、保証業務の範囲の変更の要請に正当な理由があることがある。例えば、受託会社が業務実施者による再受託会社へのアクセスについて再受託会社の合意を得られない場合に、保証業務の範囲から再受託会社を除外し、当該再受託会社の提供する業務について一体方式から除外方式に変更する要請を受ける場合などがある。

A15．第13項に記載されている保証業務の内容の変更に関する受託会社からの依頼には、本保証業務を保証業務から非保証業務へ変更する依頼又は合理的保証業務から限定的保証業務へ変更する依頼も含まれる。

《7．保証業務の計画と実施》（第14項から第16項参照）

A16．計画には、保証業務の範囲、重点事項、実施時期及び保証業務実施に関する基本的な方針の策定と、実施する証拠収集手続の種類、時期及び範囲とその決定理由からなる詳細な計画の作成が含まれる。適切な計画は、保証業務を効果的かつ効率的な方法で実施できるように、保証業務の重要な領域に適切に注意を向け、潜在的な問題を適時に識別し、保証業務を適切に組織化して管理することに有用である。適切な計画の策定は、また、業務実施者が保証業務チームのメンバーに適切に作業を割り当てることに役立ち、彼らの指導や監督及び作業の査閲を容易にする。さらに、必要に応じて、専門家等の業務と連携することができる。

A17．計画活動の内容と範囲は、受託会社の規模や複雑さ及び業務実施者と受託会社との過去の経験等の業務環境に応じて異なる。主な検討事項の例は、以下のとおりである。

- (1) 保証業務に係る契約条項
- (2) 主題及び規準の特徴
- (3) 保証業務のプロセスと証拠の情報源
- (4) 受託会社及び受託会社を取り巻く環境（記述書の適正な表示、内部統制のデザ

インの適切性、又はタイプ2の報告書の場合、内部統制の運用状況の有効性が損なわれるリスクを含む。)に関する業務実施者の理解

(5) 想定利用者及びそのニーズの特定並びに重要性及び保証業務リスクの要因の考慮

(6) 専門家の業務の利用の要否及び利用範囲を含む、必要な人員及び専門知識

A18. 保証業務の計画は、業務期間にわたり継続する連続的かつ反復的なプロセスであり、必要に応じ修正すべきものである。予想外の事象の発生、状況の変化及び実施した手続の結果により入手した証拠によっては、基本的な方針及び詳細な計画並びにこれらに基づき計画した手続の種類、時期及び範囲を修正する必要があることがある。

A19. 職業的専門家としての懐疑心を保持することとは、業務実施者が、入手した証拠を鵜呑みにせず、批判的に評価し、かつ、受託会社が作成した資料及び陳述の信頼性に疑念を抱かせる証拠に対して注意を払うことである。

A20. 受託会社のシステム及び業務環境を理解することは、保証業務の計画・実施における必須事項であり、例えば、以下の場合において、業務実施者が職業的専門家としての判断を下す際の枠組みを提供する。

(1) 受託会社のシステムの特徴を考慮する場合

(2) 規準の適切性を評価する場合

(3) 不正の兆候や他の専門家の業務の利用等、特別な検討の必要性を判断する場合

(4) 量的重要性又は質的重要性を考慮する場合

(5) 保証業務リスクを許容可能な低い水準に抑えるために追加的手続の計画を策定し実施する場合

(6) 受託会社による口頭又は文書による陳述の合理性など証拠を評価する場合

受託会社のシステム及び業務環境に関して必要な理解の程度は、業務実施者の職業的専門家としての判断に基づいて決定される。また、自らの理解が、記述書の適正な表示、内部統制のデザインの適切性、又はタイプ2の報告書の場合、内部統制の運用状況の有効性が損なわれるリスクを評価するために十分かどうかを考慮する。ただし、業務実施者の理解の程度は、通常、受託会社の理解の程度よりも低いものとなる。

《 8 . 規準の適切性の評価》 (第 17 項から第 20 項参照)

A21. 規準は、想定利用者にとって利用可能である必要がある。これは、システムに関する記述書の適正な表示、該当する原則とその規準に関連する内部統制のデザインの適切性、及び、タイプ2の報告書の場合、該当する原則とその規準に関連する内部統制の運用状況の有効性に関する受託会社の確認の基礎を、想定利用者が理解できるようにするためである。

A22. 保証業務では、業務実施者は、規準の適切性と主題の適切性を評価することが求められている。主題は、保証報告書の想定利用者の関心の対象となる状況である。

A23. 受託会社が適用した原則の規準の十分性

業務実施者は、受託業務に該当するものとして受託会社が選択した原則の規準が

全て経営者の記述書に含まれることを確認する。

例えば、業務実施者が委託会社の情報セキュリティに関連する受託会社における内部統制のデザイン及び運用状況の有効性について報告する場合、業務実施者は、「該当する原則とその規準」として、セキュリティと関連する規準に関連するリスクを軽減する上で重要な内部統制を示すものが全て記述書に含まれることを確認する。

《 9 . 重要性》（第 21 項及び第 62 項参照）

A24 . 受託会社の内部統制について報告する保証業務において、重要性の概念は、報告対象であるシステムに関係する。業務実施者は、以下の事項を判断するための手続を計画し、実施する。

- ・ 受託会社のシステムに関する記述書が、全ての重要な点において適正に表示されているかどうか。
- ・ 受託会社の内部統制が、全ての重要な点において該当する原則とその規準を充足するよう適切にデザインされているかどうか。
- ・ タイプ 2 の報告書の場合、受託会社の内部統制が、全ての重要な点において該当する原則とその規準を充足するよう有効に運用されているかどうか。

受託会社の保証報告書における重要性の概念では、受託会社のシステムの利用に関する知識を有する広範囲の想定利用者に共通するニーズを満たすように、保証報告書が受託会社のシステムに関する情報を提供することが考慮されている。

A25 . 受託会社のシステムに関する記述書の適正な表示に関する重要性及び内部統制のデザインに関する重要性には、主として質的要因の検討が含まれる。例えば、記述書に重要な取引の処理における重要な側面が含まれているかどうか、記述書において関連する情報が省略又は歪曲されていないかどうか、内部統制のデザインが該当する原則とその規準を充足するという合理的な保証を提供しているかどうか等の検討が含まれる。内部統制の運用状況の有効性に対する業務実施者の意見に関する重要性には、量的要因と質的要因の両方の検討が含まれる。例えば、許容逸脱率と実際の逸脱率（量的要因）、発見した逸脱の性質と原因（質的要因）の検討が含まれる。

A26 . 運用評価手続の記述において、手続実施の結果、識別した逸脱を開示する場合には、重要性の概念は適用しない。これは、業務実施者の意見において逸脱が内部統制の有効な運用を妨げると判断されるかどうかにかかわらず、特定の想定利用者の個別の状況においては、その逸脱が重要性を有することがあるためである。例えば、逸脱が識別された内部統制は、想定利用者の目的に係る特定の状況において重要となる可能性のある誤謬を防止するために特に重要である場合がある。

《 10 . 受託会社のシステムの理解》（第 22 項参照）

A27 . 保証業務の範囲に含まれる受託会社のシステム（内部統制を含む。）を理解することは、業務実施者が以下を行う上で役立つ。

- ・ 受託会社のシステムの対象領域と、他のシステムとのインターフェースの方法の特定
- ・ 受託会社の記述書が、デザインされ業務に適用されているシステムを適正に表

示しているかどうかの評価

- ・ 受託会社のシステムに関する記述書に記載された該当する原則とその規準を充足するために必要となる内部統制の特定
- ・ 内部統制が該当する原則とその規準を充足するよう適切にデザインされているかどうかの評価
- ・ タイプ2の報告書の場合、内部統制が該当する原則とその規準を充足するよう有効に運用されているかどうかの評価

A28．受託会社のシステムを理解するための業務実施者の手続には以下の事項が含まれる。

- ・ 関連する情報を持っている可能性があるため業務実施者が判断する、受託会社の構成員への質問
- ・ 運用状況の観察並びに文書、報告書及び取引の処理に関する紙媒体及び電子媒体による記録の閲覧
- ・ 共通の契約条項を識別するための受託会社と委託会社との間の幾つかの契約書の閲覧
- ・ 統制手続の再実施

《11．証拠の入手》

《(1) 記述書に関する証拠の入手》（第24項から第25項参照）

A29．以下の事項を検討することは、業務実施者が、保証業務の範囲に含まれる受託会社のシステムの記述が全ての重要な点において適正に表示されているかどうかを判断する際に役立つことがある。

- ・ 記述書は、委託会社が受託会社に業務の委嘱を計画する際に広範囲の想定利用者に共通するニーズに関連すると合理的に見込まれる（本保証業務の範囲内の）受託会社が提供する業務の主要な側面を扱っているか。
- ・ 記述書は、広範囲の想定利用者が、受託会社の提供する業務の内部統制の理解を得るために十分な情報を提供すると合理的に見込まれる程度の詳細さで作成されているか。
記述書は、受託会社のプロセスや委託会社に提供される業務の全ての側面を扱う必要はなく、また、受託会社のセキュリティや他の内部統制を脅かすほど詳細である必要もない。
- ・ 記述書は、広範囲の想定利用者の判断に共通するニーズに影響を与える可能性のある情報を省略する又は歪曲するような方法で作成されていないか。例えば、記述書に、業務実施者が気付いた重要な情報の省略や不正確な記述がないか。
- ・ 受託会社のシステムに関する記述書に記載された該当する原則とその規準の一部が業務実施者の業務の範囲から除かれている場合、記述書はその旨を明記しているか。
- ・ 記述書で特定されている内部統制は業務に適用されているか。
- ・ 委託会社の相補的な内部統制がある場合、それらが十分に記述されているか。多くの場合、該当する原則とその規準の記述は、受託会社が業務に適用する内

部統制が有効に運用されていれば、受託会社のみで該当する原則とその規準が充足できるように記載される。一方、場合によっては、委託会社が特定の内部統制を業務に適用することが受託会社のシステムに関する記述書に記載された該当する原則とその規準の充足に必要なため、受託会社のみでは該当する原則とその規準を充足できないことがある。記述書に委託会社の相補的な内部統制が含まれる場合、受託会社のみでは充足できない特定の原則の規準と関連付けて委託会社の相補的な内部統制が受託会社の内部統制とは別に特定される。

- ・ 一体方式の場合、記述書に、受託会社の内部統制と再受託会社の内部統制が区別して特定されているか。除外方式の場合、記述書には、再受託会社の機能が特定されているか。

除外方式の場合、記述書に、再受託会社の具体的なプロセスや内部統制について記載する必要はない。

A30．記述書の適正な表示を評価するための業務実施者の手続には、以下が含まれることがある。

- ・ 例えば、委託会社が規制当局による規制を受ける特定の業界に属しているかどうか等、委託会社の性質及び受託会社の提供する業務が委託会社にどのような影響を与える可能性があるのかの検討
- ・ 受託会社の契約上の義務について理解するため、委託会社との標準的な契約書又は標準的な契約条件を読むこと。
- ・ 受託会社の構成員が実施する手続の観察
- ・ 受託会社の方針や手続に関するマニュアル及びフローチャートや説明書等その他のシステムに関する文書の閲覧

A31．受託会社のシステムが業務に適用されているかどうかを判断するための業務実施者の手続は、システムを理解するための手続と同様である場合があり、その場合、これらの手続は一緒に行われることがある。これらの手続は、受託会社のシステムにより処理される項目の追跡を含むことがあり、また、タイプ2の報告書の場合、期間中に業務に適用されている内部統制の変更に関する特定の質問を含むことがある。想定利用者にとって重要な変更は、受託会社のシステムに関する記述書に記載されることとなる。

《(2) 内部統制のデザインに関する証拠の入手》（第26項及び第31項(2)参照）

A32．想定利用者の観点からは、ある内部統制が十分に遵守された場合に、単独で又は他の幾つかの内部統制との組合せで、該当する原則とその規準を充足するという合理的な保証を提供するのであれば、当該内部統制は適切にデザインされている。しかしながら、受託会社又は業務実施者は、内部統制の逸脱に起因する虚偽表示が委託会社にとって重要であるか否かを判断するための個々の委託会社の事情を認識していない。したがって、業務実施者の観点からは、ある内部統制が十分に遵守された場合に、単独で又は他の幾つかの内部統制との組合せで、受託会社のシステムに関する記述書に記載された該当する原則とその規準を充足するという合理的な保証を提供するのであれば、当該内部統制は適切にデザインされている。

A33．業務実施者は、内部統制のデザインの理解を促進するために、フローチャート、質問書又は意思決定表の利用を検討することがある。

A34．内部統制は、該当する原則とその規準の充足に向けた複数の活動によって構成

されていることがある。その結果、業務実施者は、ある活動が特定の該当する原則とその規準の充足のために有効でないと評価した場合でも、他の活動が存在することによって、該当する原則とその規準に関連する内部統制は適切にデザインされていると結論付けることが可能な場合がある。

《(3) 内部統制の運用状況の有効性に関する証拠の入手》

《運用状況の有効性の評価》(第27項参照)

A35. 想定利用者の観点からは、ある内部統制が、単独で又は他の幾つかの内部統制との組合せにより、該当する原則とその規準を充足するという合理的な保証を提供する場合、当該内部統制は有効に運用されている。しかしながら、受託会社又は業務実施者は、受託会社における内部統制の逸脱が想定利用者にとって重要であるかどうかを判断するための個々の委託会社の事情を認識していない。したがって、業務実施者の観点からは、ある内部統制が、単独で又は他の幾つかの内部統制との組合せにより、受託会社のシステムに関する記述書に記載された該当する原則とその規準を充足するという合理的な保証を提供する場合、当該内部統制は有効に運用されている。また、受託会社又は業務実施者は、発見した内部統制の逸脱が、個々の委託会社の観点から重要であるかどうかを判断できる立場にはない。

A36. 想定利用者にとって有益なものとするため、タイプ2の報告書は、通常、6か月以上の期間を対象とする。対象期間が6か月未満の場合、業務実施者は、業務実施者の保証報告書に対象期間が6か月より短い理由を記載することが適切と考えることがある。以下の場合には、報告書の対象期間が6か月未満になることがある。

- (1) 内部統制に対する報告書を発行する日と保証業務契約締結日が近いため、6か月間より短い期間を対象とした運用評価手続しか実施できない場合
- (2) 受託会社が業務を行っていた期間(又は特定のシステム若しくはアプリケーションが運用されていた期間)が6か月より短い場合
- (3) 内部統制に重要な変更が行われ、かつ、報告書の発行を6か月遅らせること又は変更前と変更後の双方のシステムを対象とした報告書を発行することが実務的に不可能である場合

A37. 一部の内部統制手続は、運用評価手続を後日実施することを可能にする運用状況に関する証拠を残さないことがあり、したがって、業務実施者は、対象期間を通じた様々な時点において、当該内部統制手続の運用評価手続を実施することが必要であると考えられることがある。

A38. 業務実施者は、各対象期間の内部統制の運用状況の有効性に対する意見を提供する。したがって、業務実施者が当該意見を表明するためには、それぞれの対象期間における内部統制の運用状況に関する十分かつ適切な証拠が必要である。なお、過去の期間の業務において逸脱を識別している場合、業務実施者は、対象期間における運用評価手続の範囲を増加させることがある。

《間接的な内部統制の運用評価手続》(第28項(2)参照)

A39. ある状況では、間接的な内部統制の有効な運用状況を裏付ける証拠の入手が必要であることがある。例えば、業務実施者が、システムの障害に関する例外処理報告書の査閲手続の有効性を評価すると決定したときは、その担当者による査閲及びそのフォローアップが、業務実施者に直接的に関連する内部統制であり、例外処理報告書の情報の正確性に関する内部統制が、間接的な内部統制である。

《運用評価手続の実施のための項目の抽出方法》(第28項(3)及び第30項参照)

A40. 業務実施者が利用可能な、運用評価手続の対象項目の抽出方法には、以下のものがある。

(1) 精査（100%の検討）

精査は、四半期ごと等、実施頻度が低い内部統制の場合又は内部統制の適用に関する証拠を全て検討することが効率的である場合には適切なことがある。

(2) 特定項目抽出による試査

特定項目抽出による試査は、実施頻度が低く、サンプリングによる試査を行うほど十分な大きさの母集団とはならない内部統制（例えば、月次又は週次で適用される内部統制）の運用評価手続等、精査が効率的でなく、かつ、サンプリングによる試査が有効でない場合に適切であることがある。

(3) サンプリングによる試査

サンプリングによる試査は、定型的な方法で頻繁に業務に適用され、かつ、運用の証拠が文書で残される内部統制の運用評価手続に対して適切であることがある。

A41．特定項目抽出による試査は、証拠を入手する効率的な方法ではあるが、それはサンプリングによる試査には該当しない。特定項目抽出による試査によって抽出した項目に対して実施した手続の結果からは、母集団全体にわたる一定の特性を推定することはできない。したがって、特定項目抽出による試査は、抽出されない母集団の残余部分に関する証拠を提供しない。他方、サンプリングによる試査は、母集団からその一部の項目を抽出してテストすることによって、母集団全体に関する結論を導き出すことができるようにデザインされている。

《12．専門家の業務の利用》

《(1) 品質管理手続の整備》（第33項参照）

A42．内部の専門家が業務実施者の事務所の社員等や専門職員（非常勤者を含む。）である場合には、事務所の品質管理の方針と手続に従う。一方、内部の専門家がネットワーク・ファームの社員等や専門職員（非常勤者を含む。）である場合があり、事務所はネットワーク・ファームと共通の品質管理の方針及び手続を共有することがある。

A43．外部の専門家は、保証業務チームの一員ではないため、業務実施者の事務所の品質管理の方針と手続は適用されない。

《(2) 専門家の業務の理解》（第34項参照）

A44．業務実施者は、専門家が実施する業務を理解した上で、自らが意見を表明するに当たって必要な専門家の業務を利用する合理的な範囲を判断する。

A45．業務実施者は、専門家と同等の専門知識と技能を有している必要はないが、次の手続が可能となる程度の専門知識が必要になる場合がある。

(1) 専門家に割り当てる業務の目的を定め、当該目的と保証業務の目的との関係を明らかにすること。

(2) 専門家が利用する前提、手法及びデータの合理性を判断すること。

(3) 保証業務の目的と結論に関連して、専門家の指摘事項の合理性を判断すること。

《(3) 専門家の業務の評価》（第35項参照）

A46．業務実施者は、専門家の業務がもたらす証拠の十分性及び適切性を判断するた

めに、次の事項を評価する。

- (1) 専門家が有する適性、能力及び客観性
- (2) 専門家が利用する前提、手法及びデータの合理性
- (3) 保証業務の目的と結論に関連した専門家の指摘事項の合理性と重要性

《13．内部監査人の作業》

《(1) 内部監査機能の理解》（第36項参照）

A47．内部監査機能は、経営者及び監査役等に対して、分析、評価、保証、勧告及びその他の情報提供を行う責任を有する場合がある。受託会社の内部監査機能は、受託会社自体の内部統制システムに係る活動を実施している場合もあれば、受託会社が委託会社に対して提供する業務及びシステム（内部統制を含む。）に係る活動を実施している場合もある。

《(2) 内部監査の利用の可否及びその利用の程度の判断》（第39項参照）

A48．内部監査人の作業が業務実施者の手続の種類、時期又は範囲に及ぼし得る影響を判断するに当たり、以下の場合には、比較的、必要な手続がより限定的となることがある。

- ・ 内部監査人によって実施された又は実施される予定の特定の作業の内容と範囲が極めて限定されている。
- ・ 内部監査人の作業が、業務実施者の結論に対する重要性が相対的に高くない内部統制に係っている。
- ・ 内部監査人によって実施された又は実施される予定の特定の作業が、主観的又は複雑な判断を必要としない。

《(3) 内部監査人の特定の作業の利用》（第40項参照）

A49．内部監査人の特定の作業について業務実施者が実施する手続の種類、時期及び範囲は、業務実施者の結論に対する内部監査人の作業の重要性についての業務実施者の評価（例えば、運用評価手続の対象とする内部統制が軽減しようとするリスクの重要性）、内部監査機能の評価及び内部監査人の特定の作業に対する評価に依存する。当該手続は以下の手続を含むことがある。

- ・ 内部監査人により既に検討された項目を検討する。
- ・ 内部監査人により検討された項目以外の項目を抽出して検討する。
- ・ 内部監査人により実施される手続を観察する。

《(4) 業務実施者の保証報告書に及ぼす影響》（第42項から第43項参照）

A50．内部監査機能には、その自主性及び客観性の程度にかかわらず、業務実施者が業務を実施する時に求められるような受託会社からの独立性はない。業務実施者は、業務実施者の保証報告書で表明した意見に単独で責任を負うものであり、その責任は、内部監査人の作業を利用したとしても軽減されるものではない。

A51．業務実施者が、内部監査機能によって実施される作業について記述する方法は様々であるが、例えば、以下の方法が挙げられる。

- ・ 運用評価手続の記述の冒頭部分に、内部監査機能の作業の一部を運用評価手続

の実施に際して利用した旨を記載する。

- ・ 個別の運用評価手続の記述部分でそれぞれ記載する。

《14．経営者確認書》（第44項及び第46項参照）

A52．第44項で要求される経営者確認書は、第6項(11)で定義されている受託会社確認書とは別個に追加して要求されるものである。

A53．業務実施者が本実務指針の第44項(3)に基づき経営者確認書において確認を要請した事項の全部又は一部について受託会社から確認を得られない場合、業務実施者は、本実務指針の第63項(1)に従って、除外事項付意見を表明することが適切なことがある。

《15．その他の記載内容》（第48項参照）

A54．業務実施者は、倫理規則等において、以下のような情報であると認識しながら、その作成や開示に関与してはならないことが求められている。

- (1) 重要な虚偽又は誤解を招く記載が含まれる情報
- (2) 業務上必要とされる注意を怠って作成された記載が含まれる情報
- (3) 必要な情報を省略する又は曖昧にする結果、誤解を生じさせるような情報

受託会社のシステムに関する記述書と業務実施者の保証報告書を含む文書に含まれるその他の記載内容に、復旧計画や危機管理計画等の将来情報、業務実施者の保証報告書で識別された逸脱に対処するためのシステムの改善計画及び合理的に実証することができない受託業務の宣伝の性質を有する記述が含まれる場合、業務実施者は、当該情報の削除又は修正を要請することがある。

A55．受託会社がその他の情報の削除又は修正に同意しない場合の適切な追加の措置には、例えば、以下が含まれる。

- ・ 適切な対応について顧問弁護士と相談するよう受託会社に要請すること。
- ・ 重要な相違又は重要な事実の虚偽記載の内容を保証報告書に記載すること。
- ・ 問題が解決するまで保証報告書を発行しないこと。
- ・ 保証業務契約を解除すること。

《16．調書》（第56項参照）

A56．業務実施者の事務所は、保証業務ファイルの最終的な整理に関する方針及び手続を定める。同様に、保証業務ファイルの最終的な整理を完了する期限は、業務実施者の報告書の日付から、通常60日以内となる。

《17．業務実施者の保証報告書の作成》

《(1) 業務実施者の保証報告書の記載内容》（第61項参照）

A57．付録1と付録2は、受託会社確認書の記載例及び業務実施者の保証報告書の文例を示している。

《(2) 業務実施者の保証報告書の想定利用者と目的》（第 61 項(5)参照）

A58．該当する原則とその規準は、以下を理解する想定利用者に対して、内部統制を含む受託会社のシステムに関する情報を提供する目的にのみ適合する。

- ・ 受託会社によって提供される業務の性質
 - ・ 委託会社、再受託会社等と、受託会社のシステムとの相互作用
 - ・ 内部統制とその限界
 - ・ 相補的な委託会社の内部統制と関連する受託会社の内部統制
 - ・ 該当する原則とその規準
 - ・ 該当する原則とその規準の充足を脅かすリスク及びそれらのリスクへの対処
- したがって、その旨が、業務実施者の保証報告書に記載される。

さらに、業務実施者は、想定利用者以外への保証報告書の配布、想定利用者以外の使用又は他の目的での使用を明確に制限する表現を含めることが適切と考えることがある。

《(3) 運用評価手続の記述》（第 62 項参照）

A59．タイプ 2 の報告書における運用評価手続の内容の記述において、業務実施者が以下を記載することは、業務実施者の報告書の利用者にとって有益である。

- ・ 逸脱が識別された全ての運用評価手続の結果（その他の内部統制により該当する原則とその規準が充足されていたと業務実施者が結論付けることのできる場合、又は運用評価手続を実施した内部統制がその後受託会社のシステムに関する記述書から削除された場合も含む。）
- ・ 業務実施者が識別した範囲において、識別した逸脱の原因に関する情報

《(4) 除外事項付意見》（第 63 項から第 64 項参照）

A60．付録 3 は、除外事項付意見を表明する場合の業務実施者の保証報告書の文例を示している。記述書の表示が適正でない場合には、当該除外事項の内容を除外事項付意見の根拠区分に明瞭に記載することとなる。また、内部統制が適切にデザインされていない場合、又は内部統制が有効に運用されていない場合、当該除外事項の内容、期間（タイプ 2 の場合）影響する該当する原則とその規準を除外事項付意見の根拠区分に明瞭に記載することとなる。

A61．業務実施者は、否定的意見を表明する、又は意見を表明しない場合であっても、否定的意見や意見不表明の原因となった事項以外で除外事項付意見の原因となり得る事項について業務実施者が気付いている場合には、当該事項についても全て、除外事項付意見の根拠区分に、その内容及びそれによる影響を記載することが適切な場合がある。

A62．業務範囲の制約のために意見不表明とする場合、通常、実施した手続を記載したり、業務実施者の保証業務の特徴について記載したりすることは適切ではない。これは、意見不表明の事実が不明瞭になるおそれがあるためである。

《18．その他のコミュニケーションの責任》（第 65 項参照）

A63．第 65 項に記載した状況に対応する適切な措置には、以下が含まれる。

- ・ 業務実施者の講じる措置について、法律専門家に助言を求める。

- ・ 受託会社の監査役等とコミュニケーションを行う。
- ・ 何らかの要請がある場合、第三者（例えば、規制当局）とコミュニケーションを行う。
- ・ 業務実施者の保証報告書において、除外事項付意見を表明し、又は「その他の事項」区分を追加する。
- ・ 保証業務契約を解除する。

《 適用》

1．本実務指針は、以下の業務に適用する。

- ・ タイプ1の報告書の場合、平成25年7月24日以後に基準日の到来する業務
- ・ タイプ2の報告書の場合、平成25年7月24日以後に特定期間の開始日の到来する業務

ただし、平成25年7月24日以後に特定期間の終了日の到来する業務（タイプ2の報告書の場合）に適用することができる。

2．平成27年10月5日改正後の本実務指針は、以下の業務から適用する。

- ・ タイプ1の報告書の場合、平成27年10月5日以後に基準日の到来する業務
- ・ タイプ2の報告書の場合、平成27年10月5日以後に特定期間の開始日の到来する業務

ただし、平成27年10月5日以後に特定期間の終了日の到来する業務（タイプ2の報告書の場合）に適用することができる。

3．平成29年4月26日改正後の本実務指針は、以下の業務から適用する。

- ・ タイプ1の報告書の場合、平成29年4月26日以後に基準日の到来する業務
- ・ タイプ2の報告書の場合、平成29年4月26日以後に特定期間の開始日の到来する業務

ただし、平成29年4月26日以後に特定期間の終了日の到来する業務（タイプ2の報告書の場合）に適用することができる。

《付録 1》 (A57 項参照)

この付録は、記載例 1 として、タイプ 2 のセキュリティ、可用性、処理のインテグリティ及び機密保持に関連する受託会社確認書の記載例を示す。記載例 2 として、記載例 1 のケースのタイプ 1 の受託会社確認書の記載例を示す。さらに、記載例 3 として、プライバシーに関連するタイプ 2 の受託会社確認書の記載例を示す。

《受託会社確認書の記載例》

以下は、受託会社確認書の記載例であり、必ずしも全ての状況を網羅するものではなく、また、全ての状況に適用できることを意図したものではない。

《記載例 1：タイプ 2 のセキュリティ、可用性、処理のインテグリティ及び機密保持に関する受託会社確認書》

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（注 1）に関する
受託会社確認書

受託会社名： 株式会社

添付の記述書は、「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」(IT 委員会実務指針第 7 号付録 4) のうち、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その規準(注 2)(以下「該当する原則とその規準」という。)を充足するように意図された内部統制に関する情報を、平成×年×月×日から平成×年×月×日までの期間において受託会社の[受託業務の種類又は名称]システムを使用する委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局(以下「想定利用者」という。)に提供するために作成されています。

想定利用者は、委託会社自身が運用する内部統制に関する情報を含めたその他の情報とともに、記述書を検討するための十分な理解を有することが想定されています。

当社は下記のとおりであることを確認します。

記

1. ××頁から××頁に添付されている記述書には、平成×年×月×日から平成×年×月×日までの全期間にわたり、委託会社の[受託業務の種類又は名称]のシステムが適正に表示されています。この確認に当たって、当社は以下の規準を使用しました。

(1) 添付の記述書が、以下の事項を含め、当社のシステムがどのようにデザインされ、業務に適用されていたかを表示していること。

提供される業務の種類

業務提供に利用されるシステムの範囲

業務提供に利用されるシステムの構成要素

- ・ インフラストラクチャー：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、モバイル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やアプリケーションプログラムをサポートするITシステムソフトウェア（オペレーティングシステム、ミドルウェア及びユーティリティ）
- ・ 人員：システムのガバナンス、運用及び利用に携わる人員（開発者、運用担当者、組織のユーザ、ベンダーの担当者及び管理者）
- ・ 手続：自動処理及び手作業の手続
- ・ データ：システムによって利用又は処理されたトランザクション、ファイル、データベース、テーブル及びアウトプット

上記のほか重要な事象や状況を受託会社のシステムにより把握し対応する方法

委託会社のための報告書等を作成するために用いているプロセス

該当する原則とその規準及びそれらを充足するようデザインされた内部統制

内部統制をデザインする段階で想定されている委託会社の相補的な内部統制

受託会社の統制環境、リスク評価プロセス、情報システム（関係する業務プロセスを含む。）と伝達、統制活動、モニタリング活動の側面のうち、受託業務に関連するもの

(2) 平成×年×月×日から平成×年×月×日までの期間における当社のシステムの変更の内容が表示されていること。

(3) 記述書の対象とした当社のシステムに関連する情報が省略又は歪曲されていないこと（ただし、記述書は広範囲の想定利用者に共通するニーズを満たすために作成され、したがって、個々の想定利用者が、その特定の環境において重要と考えることのある当社のシステムの全ての側面が含まれているわけではないと認識しています。）

2. 添付の記述書に記載された内部統制は、平成×年×月×日から平成×年×月×日までの期間にわたって、適切にデザインされ、有効に運用されています。この確認に当たって、当社は該当する原則とその規準を使用しました。

以 上

- (注1) この表題は、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を選択した文例であり、それ以外の場合は選択した原則のみ記載する。
- (注2) 記載例はセキュリティ、可用性、処理のインテグリティ及び機密保持の原則を選択した文例であり、対象外の原則とその規準について記載しない。
- (注3) 受託会社の要請により、主題情報を追加した場合、当該追加された主題情報についても該当事項を記載する。

《記載例 2：タイプ 1 のセキュリティ、可用性、処理のインテグリティ及び機密保持に関する受託会社確認書》

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（注 1）に関する 受託会社確認書

受託会社名： 株式会社

添付の記述書は、「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」（IT 委員会実務指針第 7 号付録 4）のうち、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その規準（注 2）（以下「該当する原則とその規準」という。）を充足するように意図された内部統制に関する情報を、平成×年×月×日現在において受託会社の〔受託業務の種類又は名称〕システムを使用する委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局（以下「想定利用者」という。）に提供するために作成されています。

想定利用者は、委託会社自身が運用する内部統制に関する情報を含めたその他の情報とともに、記述書を検討するための十分な理解を有することが想定されています。当社は下記のとおりであることを確認します。

記

1. ×× 頁から ×× 頁に添付されている記述書には、平成×年×月×日現在の受託会社の〔受託業務の種類又は名称〕のシステムが適正に表示されています。この確認に当たって、当社は以下の規準を使用しました。

(1) 添付の記述書が、以下の事項を含め、当社のシステムがどのようにデザインされ、業務に適用されていたかを表示していること。

提供される業務の種類

業務提供に利用されるシステムの範囲

業務提供に利用されるシステムの構成要素

- ・ インフラストラクチャー：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、モバイル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やアプリケーションプログラムをサポートする IT システムソフトウェア（オペレーティングシステム、ミドルウェア及びユーティリティ）
- ・ 人員：システムのガバナンス、運用及び利用に携わる人員（開発者、運用担当者、組織のユーザ、ベンダーの担当者及び管理者）

- ・ 手続：自動処理及び手作業の手続
- ・ データ：システムによって利用又は処理されたトランザクション、ファイル、データベース、テーブル及びアウトプット

上記のほか重要な事象や状況を受託会社のシステムにより把握し対応する方法

委託会社のための報告書等を作成するために用いているプロセス

該当する原則とその規準及びそれらを充足するようデザインされた内部統制

内部統制をデザインする段階で想定されている委託会社の相補的な内部統制

受託会社の統制環境、リスク評価プロセス、情報システム（関係する業務プロセスを含む。）と伝達、統制活動、モニタリング活動の側面のうち、受託業務に関連するもの

- (2) 記述書の対象とした当社のシステムに関連する情報が省略又は歪曲されていないこと（ただし、記述書は広範囲の想定利用者に共通するニーズを満たすために作成され、したがって、個々の想定利用者が、その特定の環境において重要と考えることのある当社のシステムの全ての側面が含まれているわけではないと認識しています。）

- 2 . 添付の記述書に記載された内部統制は、平成×年×月×日現在、適切にデザインされています。この確認に当たって、当社は該当する原則とその規準を使用しました。

以 上

(注1) この表題は、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を選択した文例であり、それ以外の場合は選択した原則のみ記載する。

(注2) 記載例はセキュリティ、可用性、処理のインテグリティ及び機密保持の原則を選択した文例であり、対象外の原則とその規準について記載しない。

(注3) 受託会社の要請により、主題情報を追加した場合、当該追加された主題情報についても該当事項を記載する。

《記載例3：タイプ2のプライバシーに関する受託会社確認書》

プライバシーに関する受託会社確認書

受託会社名： 株式会社

添付の記述書は、「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」(IT委員会実務指針第7号付録4)のうち、プライバシー原則とその規準(注1)(以下「該当する原則とその規準」という。)を充足するように意図された内部統制に関する情報を、平成×年×月×日から平成×年×月×日までの期間において受託会社の[受託業務の種類又は名称]システムを使用する委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局(以下「想定利用者」という。)に提供するために作成されています。

想定利用者は、委託会社自身が運用する内部統制に関する情報を含めたその他の情報とともに、記述書を検討するための十分な理解を有することが想定されています。当社は下記のとおりであることを確認します。

記

1. ××頁から××頁に添付されている記述書には、平成×年×月×日から平成×年×月×日までの全期間にわたり、当社の[受託業務の種類又は名称]のシステムが適正に表示されています。この確認に当たって、当社は以下の規準を使用しました。

(1) 添付の記述書が、以下の事項を含め、当社のシステムがどのようにデザインされ、業務に適用されていたかを表示していること。

提供される業務の種類

業務提供に利用されるシステムの範囲

以下の業務提供に利用されるシステムの構成要素

- ・ インフラストラクチャー：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、モバイル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やアプリケーションプログラムをサポートするITシステムソフトウェア（オペレーティングシステム、ミドルウェア及びユーティリティ）
- ・ 人員：システムのガバナンス、運用及び利用に携わる人員（開発者、運用担当者、組織のユーザ、ベンダーの担当者及び管理者）

- ・ 手続：自動処理及び手作業の手続
- ・ データ：システムによって利用又は処理されたトランザクション、ファイル、データベース、テーブル及びアウトプット

記述書に記載されているシステムの境界又は局面。情報のプライバシーに関係するため、少なくとも、パーソナル・インフォメーションライフサイクルを通じてパーソナル・インフォメーションの収集、利用、保持、開示及び廃棄又は匿名化に直接的又は間接的に関係する全てのシステム構成要素が含まれている。

個人から収集し、又は委託会社や他の組織から入手したパーソナル・インフォメーションの種類、それらの情報の収集方法。委託会社が収集している場合、受託会社による入手方法

ア．委託会社との合意書、法令によりパーソナル・インフォメーションに適用される詳細な要求事項を識別し、イ．それらの要求事項に合致する内部統制と実務を導入するプロセス

受託会社が、パーソナル・インフォメーションを収集、利用、保持、開示及び廃棄又は匿名化している場合、当該個人に提供しているプライバシー通知は、該当する原則とその規準に記載されたプライバシー通知の規準に準拠して作成されている。

受託会社ではなく、委託会社に個人にプライバシー通知を提供する責任がある場合、委託会社による個人へのプライバシー通知の方法、委託会社によるプライバシー通知を個人に伝達する責任及び受託会社における自らのプライバシー実務の声明上、委託会社へプライバシー実務を伝達する責任。これらに関する声明には、以下の情報が含まれる。

ア．受託会社とその委託会社間のほとんどの合意に共通した重要なプライバシー及び関連するセキュリティの要求事項並びに受託会社が全て又はほとんどの委託会社に適合する委託会社との合意におけるその他の要求事項の概要

イ．委託会社との合意書に含まれない、受託会社が全て若しくはほとんどの委託会社に適合する法令、業界又は市場から必須となる重要なプライバシー及び関連するセキュリティの要求事項の概要

ウ．委託会社との合意書で認められたパーソナル・インフォメーションの収集目的、利用、開示並びにその合意書で禁じられているパーソナル・インフォメーションの収集目的、利用、開示に関する委託会社によるコミットメント及びこれらの合意書で禁止されていないパーソナル・インフォメーションの収集目的、利用、開示以外のもの

- エ．記載された目的若しくは契約要件において必要とされるものを超えない期間若しくは法令で要求される期間で保持される情報に関する声明又はその他の保持実務に関する声明
- オ．廃棄される情報の滅失、盗難、誤用又は未承認のアクセスを防止する方法に関する声明
- カ．個人が自らの情報を閲覧、更新又は修正するアクセスを得るために、委託会社から認められた手続の受託会社による支援の方法
- キ．パーソナル・インフォメーションが正確かつ完全なものであるかを特定する手続及び受託会社が委託会社から許可された修正手続をどのように導入したかに関する記述
- ク．個人から（個人から直接又は委託会社を経由して間接かにかかわらず）の自己のパーソナル・インフォメーションに関する問合せ、苦情及び紛争についての受託会社の取扱方法
- ケ．文書化されたセキュリティプログラムの存在と、それが業界やその他の基準に基づいている事に関する声明
- コ．受託会社が委託会社にとって適切であると考えるプライバシー実務に係るその他の情報
- 受託会社ではなく、委託会社に個人にプライバシー通知を提供する責任がある場合、受託会社のプライバシー実務の声明
- 重要な事象や状況を受託会社のシステムにより把握し対応する方法
- 委託会社又はその他の関係者に、サービス、報告及びその他の情報を提供するプロセス
- 再受託会社又はその他の者と、情報を提供又は受領する場合
- ア．情報の提供又は受領の方法、再受託会社又はその他の者の役割
- イ．受託会社のプライバシー実務の声明に準拠して、その情報が保護されている事を特定するために実施される手続
- 報告される原則ごとに該当する付録４の規準及びそれらを充足するようデザインされた関連する内部統制（受託会社のシステムのデザインで想定された委託会社の相補的な内部統制を含む。）
- 再受託会社が存在し、除外方式を選択している場合
- ア．再受託会社が提供するサービスの性質
- イ．責任が再受託会社に委任された、パーソナル・インフォメーションライフサイクルのあらゆる側面

ウ．再受託会社単独又は受託会社との組合せの内部統制によって充足するように意図された該当するそれぞれの付録４の規準及び除外した再受託会社で実装することが期待されている当該規準を充足する内部統制の種類

エ．再受託会社が、受託会社のプライバシーコミットメントを遵守するために実施が必要となる活動の種類

受託会社及び再受託会社の内部統制で対応していない該当する付録４の規準とその理由

受託会社の統制環境、リスク評価プロセス、情報、伝達システム及びモニタリング活動の側面のうち、提供されるサービス、パーソナル・インフォメーションライフサイクル及び該当する付録４の規準に関連するその他のもの

(2) 平成×年×月×日から平成×年×月×日までの期間における当社のシステムの変更の内容が表示されていること。

(3) 記述書の対象とした当社のシステム及びパーソナル・インフォメーションライフサイクルに関連する情報が省略又は歪曲されていないこと（ただし、記述書は広範囲の想定利用者に共通するニーズを満たすために作成され、したがって、個々の想定利用者が、その特定のニーズにおいて重要と考える当社のシステム及びパーソナル・インフォメーションライフサイクルの全ての側面が含まれているわけではないと認識しています。）

2．添付の記述書に記載された内部統制は、平成×年×月×日から平成×年×月×日までの期間にわたって、適切にデザインされ、有効に運用されています。この確認に当たって、当社は、該当する原則とその規準を使用しました。

3．プライバシー実務の声明上のコミットメントは、平成×年×月×日から平成×年×月×日までの期間にわたって、全ての重要な点において遵守していました。

以 上

(注１) 受託会社の要請により、主題情報を追加した場合、当該追加された主題情報についても該当事項を記載する。

《付録 2》 (A57 項参照)

《業務実施者の保証報告書の文例》

以下は、報告書の文例であり、必ずしも全ての状況を網羅するものではなく、また、全ての状況に適用できることを意図したものではない。

《文例 1：タイプ 2 のセキュリティ、可用性、処理のインテグリティ及び機密保持に関する業務実施者の保証報告書》

受託会社のシステムに係るセキュリティ、可用性、処理のインテグリティ及び機密保持（注 5）の記述書並びに内部統制のデザイン及び運用状況に関する独立業務実施者の保証報告書

平成×年×月×日

株式会社（受託会社） 御中

| | | |
|--------|-------|---|
| 監査法人 | | |
| 代表社員 | 公認会計士 | 印 |
| 業務執行社員 | | |
| 業務執行社員 | 公認会計士 | 印 |

(注 1)

範囲

当監査法人（注 2）は、××頁から××頁に記載されている、「[平成×年×月×日から平成×年×月×日まで]における 株式会社（以下「受託会社」という。）の[受託業務の種類又は名称]のシステムの記述書」（以下「記述書」という。）及びその記述書に記載された「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」（IT委員会実務指針第 7 号付録 4）のうち、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その規準（注 6）（以下「該当する原則とその規準」という。）を充足するように意図された内部統制のデザイン及び運用状況について報告する業務を実施した。（注 3）

記述書は、受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、受託会社の関連する内部統制に加えて、適切にデザインされており、有効に運用されている場合のみ、記述書に特定された該当する原則とその規準を充足できることを示す。当監査法人（注 2）は、当該相補的な委託会社の内部統制のデザインや運用状況の有効性を評価していない。

受託会社の責任

受託会社の責任は、受託会社確認書及び添付される記述書を作成すること、記述書と受託会社確認書の網羅性、正確性及び表示方法、記述書が対象とする業務を提供すること、該当する原則とその規準を充足する内部統制を記述書に記載すること、該当する原則とその規準を充足するための内部統制をデザインし、業務へ適用し、更に有効に運用することにある。

業務実施者の責任

当監査法人（注 2）の責任は、実施した手続きに基づき、受託会社の記述書及び当

該記述書に記載された該当する原則とその規準に関連する内部統制のデザインと運用状況に対する意見を表明することにある。

当監査法人（注２）は、日本公認会計士協会が公表したＩＴ委員会実務指針第７号「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保証報告書」に準拠して業務を実施した。当該実務指針は、当監査法人（注２）に、関連する職業倫理に関する規定を遵守し、全ての重要な点において、記述書が適正に表示されているかどうか、及び該当する原則とその規準を充足する内部統制が適切にデザインされ、有効に運用されているかどうかについて合理的な保証を得るための手続を計画し実施することを求めている。

受託会社の内部統制の記述書の表示の適正性、デザインの適切性及び運用状況の有効性について報告する保証業務においては、受託会社のシステムに関する記述書の表示の適正性及び内部統制のデザインの適切性と運用状況の有効性について証拠を入手するための手続が実施される。

手続は、業務実施者の判断により、記述書が適正に表示されていないリスク、及び該当する原則とその規準を充足する内部統制が適切にデザインされていない又は有効に運用されていないリスクの評価に基づいて選択及び適用される。

当監査法人（注２）の実施した手続には、記述書に記載された該当する原則とその規準を充足するという合理的な保証を提供するために必要と考える内部統制の運用評価手続が含まれている。また、この保証業務には、記述書の全体的な表示を評価することが含まれる。

当監査法人（注２）は、意見表明の基礎となる十分かつ適切な証拠を得たと判断している。

受託会社の内部統制の限界

受託会社の記述書は、広範囲の想定利用者に共通するニーズを満たすために作成されている。したがって、記述書には、個々の委託会社とその特定の環境において重要と考える受託会社のシステムの全ての側面が含まれているわけではない。

また、受託会社の内部統制は、内部統制の性質及び固有の限界により、必ずしも該当する原則とその規準を充足するように運用されない可能性がある。

さらに、この有効性の評価に基づき将来を予測することには、受託会社の内部統制が不適切になる又は機能しなくなるというリスクが伴う。

意見

当監査法人（注２）の意見は、本保証報告書に記載されている状況を踏まえて形成されている。

当監査法人（注２）が意見形成において使用した規準は、××頁の受託会社確認書に記載されている。

当監査法人（注２）の意見は次のとおりである。

- (1) 記述書は、平成×年×月×日から平成×年×月×日までの期間にわたってデザインされ業務に適用されている〔受託業務の種類又は名称〕システムを、全ての重要な点において適正に表示している。
- (2) 受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、委託会社において平成×年×月×日から平成×年×月×日までの期間にわたって適用されている場合、記述書に記載された受託会社の内部統制は、該当する原則とその規準を充足するように全ての重要な点において適切にデザインされている。

(3) 受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、委託会社において平成×年×月×日から平成×年×月×日までの期間にわたって有効に運用されている場合、記述書に記載された該当する原則とその規準の充足について合理的な保証を提供するために必要なものとして、運用評価手続を実施した受託会社の内部統制は、平成×年×月×日から平成×年×月×日までの期間にわたって、全ての重要な点において有効に運用されている。

運用評価手続の記述

運用評価手続を実施した特定の内部統制と、当該運用評価手続の種類、時期及び結果は、××頁から××頁に記載されている。

想定利用者と目的

本保証報告書及び××頁から××頁に記載された運用評価手続の記述は、利用者として、受託会社並びに、平成×年×月×日から平成×年×月×日までの期間に受託会社の〔受託業務の種類又は名称〕システムを使用する委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局のみを想定している。また、想定利用者は、委託会社自身が運用する内部統制に関する情報を含めたその他の情報とともに、当該システムを検討するための十分な理解を有することが想定されている。

以 上

(注1) 業務契約において業務実施者が特定されている場合又は監査法人の場合において報告書署名者に関する内規がある場合には、これらに応じて代表社員
の肩書を省略するなど、適宜必要な修正を行う。

業務実施者が公認会計士の場合には、以下とする。

公認会計士事務所

公認会計士 印

公認会計士事務所

公認会計士 印

(注2) 業務実施者が公認会計士の場合には、「私」又は「私たち」とする。

(注3) 記述書の一部が業務実施者の業務の範囲に含まれない場合、その旨を保証報告書に明記する。

(注4) 必要と認める場合には、公認会計士法に準じた利害関係の有無に関して、保証報告書の末尾に、例えば以下の記載をすることができる。

利害関係

受託会社と当監査法人又は業務執行社員との間には、公認会計士法の規定に準じて記載すべき利害関係はない。

(注5) この表題は、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を選択した文例であり、それ以外の場合は選択した原則のみ記載する。

(注6) 文例はセキュリティ、可用性、処理のインテグリティ及び機密保持の原則を選択した文例であり、対象外の原則とその規準については記載しない。

(注7) 受託会社の要請により主題情報を追加した場合、範囲及び意見に関する記述は区分して記載する。また、追加された主題情報について業務実施者が実施した追加の検証手続及びその結果についても保証報告書に区分して記載する。

《文例2：タイプ1のセキュリティ、可用性、処理のインテグリティ及び機密保持に関する業務実施者の保証報告書》

受託会社のシステムに係るセキュリティ、可用性、処理のインテグリティ及び機密保持（注5）の記述書並びに内部統制のデザインに関する独立業務実施者の保証報告書

平成×年×月×日

株式会社（受託会社） 御中

監査法人
代表社員 公認会計士 印
業務執行社員
業務執行社員 公認会計士 印
(注1)

範囲

当監査法人（注2）は、××頁から××頁に記載されている「[平成×年×月×日]における 株式会社（以下「受託会社」という。）の [受託業務の種類又は名称] のシステムの記述書」（以下「記述書」という。）及びその記述書に記載された「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」（IT委員会実務指針第7号付録4）のうち、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その規準（注6）（以下「該当する原則とその規準」という。）を充足するように意図された内部統制のデザインについて報告する業務を実施した。（注3）

記述書は、受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、受託会社の関連する内部統制に加えて、適切にデザインされており、有効に運用されている場合のみ、記述書に特定された該当する原則とその規準を充足できることを示す。当監査法人（注2）は、当該相補的な委託会社の内部統制のデザインや運用状況の有効性を評価していない。

当監査法人（注2）は、記述書に含まれる内部統制の運用状況の有効性に関する手続を実施しておらず、したがって、それに対する意見は表明しない。

受託会社の責任

受託会社の責任は、受託会社確認書及び添付される記述書を作成すること、記述書と受託会社確認書の網羅性、正確性及び表示方法、記述書が対象とする業務を提供すること、該当する原則とその規準を充足する内部統制を記述書に記載すること、該当する原則とその規準を充足するための内部統制をデザインし、業務へ適用し、更に有効に運用することである。

業務実施者の責任

当監査法人（注2）の責任は、実施した手続に基づき、受託会社の記述書及び当該記述書に記載された該当する原則とその規準に関連する内部統制のデザインに対する意見を表明することにある。

当監査法人（注2）は、日本公認会計士協会が公表したIT委員会実務指針第7号「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保証報告書」に準拠して業務を実施した。当該実務指針は、当監査法人（注２）に、関連する職業倫理に関する規定を遵守し、全ての重要な点において、記述書が適正に表示されているかどうか、及び該当する原則とその規準を充足する内部統制が適切にデザインされているかどうかについて合理的な保証を得るための手続を計画し実施することを求めている。

受託会社の内部統制の記述書の表示の適正性、デザインの適切性について報告する保証業務においては、受託会社のシステムに関する記述書の表示の適正性及び内部統制のデザインの適切性について証拠を入手するための手続が実施される。

手続は、業務実施者の判断により、記述書が適正に表示されていないリスク、及び該当する原則とその規準を充足する内部統制が適切にデザインされていないリスクの評価に基づいて選択及び適用される。また、この保証業務には、記述書の全体的な表示を評価することが含まれる。

上述のとおり、当監査法人（注２）は、記述書に含まれる内部統制の運用状況の有効性に関する手続を実施しておらず、したがって、それに対する意見は表明しない。

当監査法人（注２）は、意見表明の基礎となる十分かつ適切な証拠を得たと判断している。

受託会社の内部統制の限界

受託会社の記述書は、広範囲の想定利用者に共通するニーズを満たすために作成されている。したがって、記述書には、個々の委託会社とその特定の環境において重要と考える受託会社のシステムの全ての側面が含まれているわけではない。

また、受託会社の内部統制は、内部統制の性質及び固有の限界により、必ずしも該当する原則とその規準を充足するように運用されない可能性がある。

意見

当監査法人（注２）の意見は、本保証報告書に記載されている状況を踏まえて形成されている。

当監査法人（注２）が意見形成において使用した規準は、××頁の受託会社確認書に記載されている。

当監査法人（注２）の意見は次のとおりである。

- (1) 記述書は、平成×年×月×日現在においてデザインされ業務に適用されている [受託業務の種類又は名称] システムを、全ての重要な点において適正に表示している。
- (2) 受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、委託会社において平成×年×月×日現在において適用されている場合には、記述書に記載された受託会社の内部統制は、該当する原則とその規準の充足について全ての重要な点において適切にデザインされている。

想定利用者と目的

本保証報告書は、利用者として、受託会社並びに、平成×年×月×日において受託会社の [受託業務の種類又は名称] システムを使用する委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局のみを想定している。また、想定利用者は、委託会社自身が運用する内部統制に関

する情報を含めたその他の情報とともに、当該システムを検討するための十分な理解を有することが想定されている。

以 上

- (注1) 業務契約において業務実施者が特定されている場合又は監査法人の場合において報告書署名者に関する内規がある場合には、これらに応じて代表社員の肩書を省略するなど、適宜必要な修正を行う。

業務実施者が公認会計士の場合には、以下とする。

公認会計士事務所

公認会計士 印

公認会計士事務所

公認会計士 印

- (注2) 業務実施者が公認会計士の場合には、「私」又は「私たち」とする。
(注3) 記述書の一部が業務実施者の業務の範囲に含まれない場合、その旨を保証報告書に明記する。
(注4) 必要と認める場合には、公認会計士法に準じた利害関係の有無に関して、保証報告書の末尾に、例えば以下の記載をすることができる。

利害関係

受託会社と当監査法人又は業務執行社員との間には、公認会計士法の規定に準じて記載すべき利害関係はない。

- (注5) この表題は、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を選択した文例であり、それ以外の場合は選択した原則のみ記載する。
(注6) 文例はセキュリティ、可用性、処理のインテグリティ及び機密保持の原則を選択した文例であり、対象外の原則とその規準については記載しない。
(注7) 受託会社の要請により主題情報を追加した場合、範囲及び意見に関する記述は区分して記載する。また、追加された主題情報について業務実施者が実施した追加の検証手続及びその結果についても報告書に区分して記載する。

《文例3：タイプ2のプライバシーに関する業務実施者の保証報告書》

受託会社のシステムに係るプライバシーの記述書並びに内部統制のデザイン及び運用状況に関する独立業務実施者の保証報告書

平成×年×月×日

株式会社（受託会社） 御中

監査法人
代表社員 公認会計士 印
業務執行社員
業務執行社員 公認会計士 印
(注1)

範囲

当監査法人（注2）は、××頁から××頁に記載されている「[平成×年×月×日]における株式会社（以下「受託会社」という。）の[受託業務の種類又は名称]のシステムの記述書」（以下「記述書」という。）及びその記述書に記載された「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」（IT委員会実務指針第7号付録4）のうち、プライバシー原則とその規準（以下「該当する原則とその規準」という。）を充足するように意図された内部統制のデザイン及び運用状況について報告する業務を実施した。（注3）

当監査法人の業務は、平成×年×月×日から平成×年×月×日までの期間における、受託会社のプライバシーに関する法令の遵守に関する法的判断を提供しない。

記述書は、受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、受託会社の関連する内部統制に加えて、適切にデザインされており、有効に運用されている場合のみ、記述書に特定された該当する原則とその規準を充足できることを示す。当監査法人（注2）は、当該相補的な委託会社の内部統制のデザインや運用状況の有効性を評価していない。

受託会社の責任

受託会社の責任は、受託会社確認書及び添付される記述書を作成すること、記述書と受託会社確認書の網羅性、正確性及び表示方法、記述書が対象とする業務を提供すること、該当する原則とその規準を充足する内部統制を記述書に記載すること、該当する原則とその規準を充足するための内部統制をデザインし、業務へ適用し、更に有効に運用することにある。

業務実施者の責任

当監査法人（注2）の責任は、実施した手続に基づき、受託会社の記述書及び当該記述書に記載された該当する原則とその規準に関連する内部統制のデザインと運用状況に対する意見を表明することにある。

当監査法人（注2）は、日本公認会計士協会が公表したIT委員会実務指針第7号「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保証報告書」に準拠して業務を実施した。当該実務指針は、当監査法人（注2）に、関連する職業倫理に関する規定を遵守し、全ての重要

な点において、記述書が適正に表示されているかどうか、及び該当する原則とその規準を充足する内部統制が適切にデザインされ、有効に運用されているかどうかについて合理的な保証を得るための手続を計画し実施することを求めている。

受託会社の内部統制の記述書の表示の適正性、デザインの適切性及び運用状況の有効性について報告する保証業務においては、受託会社のシステムに関する記述書の表示の適正性及び内部統制のデザインの適切性と運用状況の有効性について証拠を入手するための手続が実施される。

手続は、業務実施者の判断により、記述書が適正に表示されていないリスク、及び該当する原則とその規準を充足する内部統制が適切にデザインされていない又は有効に運用されていないリスクの評価に基づいて選択及び適用される。当監査法人(注2)の実施した手続には、記述書に記載された該当する原則とその規準を充足するという合理的な保証を提供するために必要と考える内部統制の運用評価手続が含まれている。また、本保証業務には、記述書の全体的な表示を評価することが含まれる。

当監査法人(注2)は、意見表明の基礎となる十分かつ適切な証拠を得たと判断している。

受託会社の内部統制の限界

受託会社の記述書は、広範囲の想定利用者に共通するニーズを満たすために作成されている。したがって、記述書には、個々の委託会社とその特定の環境において重要と考える受託会社のシステムの全ての側面が含まれているわけではない。

また、受託会社の内部統制は、内部統制の性質及び固有の限界により、必ずしも該当する原則とその規準を充足するように運用されない可能性があり、パーソナル・インフォメーションの未承認のアクセスや使用、法令が遵守されない可能性がある。例えば、パーソナル・インフォメーションの不正や未承認のアクセス又は承認された要員による未承認の使用や開示が発見又は防止されない可能性がある。

さらに、この有効性の評価に基づき将来を予測することには、受託会社の内部統制が不適切になる又は機能しなくなるというリスクが伴う。

意見

当監査法人(注2)の意見は、本保証報告書に記載されている状況を踏まえて形成されている。

当監査法人(注2)が意見形成において使用した規準は、××頁の受託会社確認書に記載されている。

当監査法人(注2)の意見は次のとおりである。

- (1) 記述書は、平成×年×月×日から平成×年×月×日までの期間にわたってデザインされ業務に適用されている[受託業務の種類又は名称]システム及びプライバシー実務を、全ての重要な点において適正に表示している。
- (2) 受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、委託会社において平成×年×月×日から平成×年×月×日までの期間にわたって適用されている場合、記述書に記載された受託会社の内部統制は、該当する原則とその規準を充足するように全ての重要な点において適切にデザインされている。
- (3) 受託会社の内部統制のデザインで考慮された相補的な委託会社の内部統制が、委託会社において平成×年×月×日から平成×年×月×日までの期間にわたっ

て有効に運用されている場合、記述書に記載された該当する原則とその規準の充足について合理的な保証を提供するために必要なものとして、運用評価手続を実施した受託会社の内部統制は、平成×年×月×日から平成×年×月×日までの期間にわたって、全ての重要な点において有効に運用されている。

運用評価手続の記述

運用評価手続を実施した特定の内部統制と、当該運用評価手続の種類、時期及び結果は、××頁から××頁に記載されている。

想定利用者と目的

本保証報告書及び××頁から××頁に記載された内部統制の運用評価手続の記述は、利用者として、受託会社並びに平成×年×月×日から平成×年×月×日までの期間に受託会社の〔受託業務の種類又は名称〕システムを使用する委託会社、予想される委託会社、委託会社の監査人・業務実施者及び委託会社又は受託会社に係る規制当局のみを想定している。また、想定利用者は、委託会社自身が運用する内部統制に関する情報を含めたその他の情報とともに、当該システム及びプライバシー実務を検討するための十分な理解を有することが想定されている。

以 上

(注1) 業務契約において業務実施者が特定されている場合又は監査法人の場合において報告書署名者に関する内規がある場合には、これらに応じて代表社員の肩書を省略するなど、適宜必要な修正を行う。

業務実施者が公認会計士の場合には、以下とする。

公認会計士事務所

公認会計士 印

公認会計士事務所

公認会計士 印

(注2) 業務実施者が公認会計士の場合には、「私」又は「私たち」とする。

(注3) 記述書の一部が業務実施者の業務の範囲に含まれない場合、その旨を保証報告書に明記する。

(注4) 必要と認める場合には、公認会計士法に準じた利害関係の有無に関して、保証報告書の末尾に、例えば以下の記載をすることができる。

利害関係

受託会社と当監査法人又は業務執行社員との間には、公認会計士法の規定に準じて記載すべき利害関係はない。

(注5) 受託会社の要請により主題情報を追加した場合、範囲及び意見に関する記述は区分して記載する。また、追加された主題情報について業務実施者が実施した追加の検証手続及びその結果についても報告書に区分して記載する。

《付録 3》 (A60 項参照)

《除外事項付意見を表明する場合の業務実施者の保証報告書の文例》

以下は、限定意見を表明する場合の業務実施者の保証報告書の文例であり、付録 2 の報告書の文例からの変更点のみを示している。これらは、必ずしも全ての状況を網羅するものではなく、また、全ての状況に適用できることを意図したものではない。

《文例 1：限定意見 受託会社のシステムに関する記述書が適正に表示されていない場合》

...

受託会社監査人の責任

...

当監査法人は、限定意見表明の基礎となる十分かつ適切な証拠を得たと判断している。

限定意見の根拠

添付の記述書の××頁には、受託会社が、アプリケーションに対する未承認のアクセスを防止するため、オペレーターのIDとパスワードによる管理について記載されている。

当監査法人が実施した受託会社の職員に対する質問及び活動状況の観察等の手続に基づき、当監査法人は、オペレーターのIDとパスワードによる管理がアプリケーションAとBでは採用されているが、アプリケーションCとDでは採用されていないと判断した。

限定意見

当監査法人の意見は、本保証報告書に記載されている状況を踏まえて形成されている。当監査法人が意見形成において使用した規準は、××頁の受託会社確認書に記載されている。

当監査法人の意見は、「限定意見の根拠」に記載した事項を除き、次のとおりである。

(1) ...

《文例 2：限定意見 内部統制が適切にデザインされていない場合》

…

受託会社監査人の責任

…

当監査法人は、限定意見表明の基礎となる十分かつ適切な証拠を得たと判断している。

限定意見の根拠

受託会社は、記述書において、「セキュリティポリシーへの遵守性違反を識別しその是正措置をタイムリーに行うための手続がある」と記載している。

しかしながら、セキュリティポリシーへの遵守性違反を識別する内部統制が整備されていなかった。

限定意見

当監査法人の意見は、本保証報告書に記載されている状況を踏まえて形成されている。当監査法人が意見形成において使用した規準は、××頁の受託会社確認書に記載されている。

当監査法人の意見は、「限定意見の根拠」に記載した事項を除き、次のとおりである。

(1) …

《文例3：限定意見 内部統制が有効に運用されていない場合（タイプ2の報告書）》

…
受託会社監査人の責任

…
当監査法人は、限定意見表明の基礎となる十分かつ適切な証拠を得たと判断している。

限定意見の根拠

受託会社は、記述書において、「セキュリティポリシーへの遵守性違反を識別しその是正措置をタイムリーに行うための手続がある」と記載している。

しかしながら、「内部統制のテストの記述及びその結果」の××頁に記載されているとおり、セキュリティポリシーへの遵守性違反を十分に識別されていなかった。

したがって、平成×年×月×日から平成×年×月×日までの期間において、「内部統制が、セキュリティポリシーへの遵守性違反を識別しその是正措置をタイムリーに行うための手続がある」という合理的な保証を提供しているという規準を充足していなかった。

受託会社は、平成×年×月×日に、セキュリティに係る内部統制を業務に適用しており、当監査法人の運用評価手続は、平成×年×月×日から平成×年×月×日までの期間、当該内部統制が有効に運用されていたことを示している。

限定意見

当監査法人の意見は、本保証報告書に記載されている状況を踏まえて形成されている。当監査法人が意見形成において使用した規準は、××頁の受託会社確認書に記載されている。

当監査法人の意見は、「限定意見の根拠」に記載した事項を除き、次のとおりである。

…

《文例４：限定意見 業務実施者が十分かつ適切な証拠を入手できない場合》

…

受託会社監査人の責任

…

当監査法人は、限定意見表明の基礎となる十分かつ適切な証拠を得たと判断している。

限定意見の根拠

受託会社は、記述書の××頁において、「セキュリティポリシーへの遵守性違反を識別しその是正措置をタイムリーに行うための手続がある」と記載している。

しかしながら、「内部統制のテストの記述及びその結果」の××頁に記載されているとおり、準守性違反を識別するための記録が事故により平成×年×月×日以降のデータが消滅し、当監査法人はセキュリティポリシーへの遵守性違反を識別するための内部統制について十分な証拠を得ることができなかった。

したがって、当監査法人は、内部統制が平成×年×月×日から×月×日までの期間、セキュリティポリシーへの遵守性違反を識別しその是正措置をタイムリーに行うための手続が有効に運用されているかどうか判断することができなかった。

限定意見

当監査法人の意見は、本保証報告書に記載されている状況を踏まえて形成されている。当監査法人が意見形成において使用した規準は、××頁の受託会社確認書に記載されている。

当監査法人の意見は、「限定意見の根拠」に記載された事項を除き、次のとおりである。

(1) …