IT委員会研究報告第45号

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」の実施上の留意点

平成26年5月13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>

1. 本研究報告の目的	1
2. Q & A	1
Q 1 IT実7号の保証業務を実施する業務実施者に求められる能力には、どのようなものがありますか。	1
Q 2 IT実7号には、付録4として「原則と規準」がありますが、その利用方法について教えてください。	2
Q 3 付録4の「原則と規準」以外の主題情報を追加する際に留意すべき事項を教えてください。	2
Q 4 受託会社がその業務の一部を外部に再委託している場合、「一体方式」と「除外方式」の留意すべき事項を教えてください。	3
Q 5 受託会社がその業務の一部を外部に再委託している場合の取扱いとして、「一体方式」を採用する場合の保証報告書の記載例を教えてください。	4
Q 6 受託会社がその業務の一部を外部に再委託している場合の取扱いとして、「除外方式」を採用する場合の保証報告書の記載例を教えてください。	5
Q 7 監査・保証実務委員会実務指針第86号とIT実7号を統合した報告書で提供することは可能でしょうか。	7
Q 8 受託会社のシステムの記述書はどのように記載しますか。	8
Q 9 タイプ2の報告書の場合、「実施した運用評価手続及び当該手続の結果」の作成が必要ですが、記載例はないでしょうか。	10
Q 10 保証業務終了時には、保証報告書と同日付で経営者の確認書を入手することになりますが、記載事項について留意すべき事項はありますか。	11
Q 11 いわゆるクラウドサービスに本保証業務を提供する場合の留意点があれば教えてください。	14
Q 12 IT実7号は、報告書の想定利用者を限定していますが、このうち「予想される委託会社」とはどのような関係を想定しているのでしょうか。	15

1. 本研究報告の目的

本研究報告は、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」(以下「IT実7号」という。)の内容について、Q & A方式での具体的な解説を提供し会員の理解が深まることを目的として作成した。

「Q & A」については、IT実7号の項目と対応するように作成しているため、IT実7号と対応させながら読むことを推奨する。

2. Q & A

Q 1 IT実7号の保証業務を実施する業務実施者に求められる能力には、どのようなものがありますか。

A 1 本保証業務は、保証業務及び対象事項に関する十分な知識、適切な技術的研修と経験を持った業務実施者によって行われる必要があります。

業務実施者の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、本保証業務と同様の業務について相当の経験を有していることが必要です(IT実7号 A9 項参照)。

- ・ 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

すなわち、本保証業務の対象には財務報告以外の領域のシステムが含まれますが、システム又はシステムの構成要素は受託会社や受託会社等の属する業界によって異なるため、業務実施者に求められる知識としては、受託会社に関する知識に加えて業界知識や情報技術、内部統制に及びます。

また、業務実施者は、必要とされる専門知識、業務実施のタイミング、専門家の関与の範囲を含めて考慮した上で、本保証業務を効果的に実施できるように業務を計画する必要があります。

なお、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、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ありませんが、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、以下の事項を評価できることが必要です(IT実7号 A46 項)。

(1) 専門家が有する適性、能力及び客観性を判断すること。

- (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) 本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及び重要性を判断すること。

Q 2 IT実7号には、付録4として「原則と規準」がありますが、その利用方法について教えてください。

A 2 付録4は、IT実7号に基づいた保証業務の対象となる内部統制を評価するための目的となる「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」の五つの原則とその規準を提供しています。この原則と規準は、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（IT実7号付録4第3項参照）、国内における実務や実情を考慮して作成されています。

保証業務の対象となる原則は、当該受託会社の経営者によって選択される原則であり、それは単一の原則を対象とする場合と複数の原則を対象とする場合が想定されます。受託会社の経営者は、その想定利用者からの要請や提供するサービスに係る契約内容等を勘案して、適切な原則を選択する必要があります。

また、記載されている規準は対象とする原則を達成するために必要な評価の要件であり、原則に対応して列挙されている規準のうち、一部のみを選択又は除外して用いることは想定されていません。そのため、受託会社の経営者によって選択された原則に対応して記載されている規準については、その全てを評価の対象としなければなりません。ただし、対象となる情報システムの仕様等により、ある規準に関連する内部統制が受託会社において必要ない、又は該当しないという可能性は考えられます。なお、この場合、記述書には、原則に対応する全ての規準を記載した上で、内部統制が受託会社において必要ない、又は該当しない理由について明確にすることが必要です。

Q 3 付録4の「原則と規準」以外の主題情報を追加する際に留意すべき事項を教えてください。

A 3 業務実施者は、受託会社からの要請に基づいて、付録4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、IT実7号に準拠して業務を実施することができます。

この場合、業務実施者は、付録4の「原則と規準」と、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する必要が

あります（IT実7号付録4第8項参照）。

当該情報には以下のものが含まれます。

追加した主題情報に関する受託会社のシステムに関する記述書の補足

追加した主題情報の評価又は測定と表示に利用する規準の説明

規準が内部統制に関係する場合、当該規準に対応する内部統制の説明

追加した主題情報に対する経営者の確認書

また、業務実施者は、追加された主題情報に対して、IT実7号に準拠して当該事項を検証する必要があります。さらに、保証報告書には、範囲及び意見に関する記述は区分して記載し、タイプ2の報告書の場合、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します。

<p>Q 4 受託会社はその業務の一部を外部に再委託している場合、「一体方式」と「除外方式」の留意すべき事項を教えてください。</p>

A 4 受託会社が受託している業務を、再委託している場合の取扱いには、「一体方式」と「除外方式」の二つの方式があります。

受託会社は、「一体方式」と「除外方式」のいずれかの方法を選択することになります。受託会社のシステムに関する記述書には、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においても、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必要があります（IT実7号第24項(4)参照）。

一体方式と除外方式の選択

一体方式と除外方式の選択は、任意ですが、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十分に機能している場合、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ような場合には、除外方式が適しています。

一体方式の留意点

一体方式が採用される場合、IT実7号の要求事項は再受託会社に対しても適用されます。これには、IT実7号第11項(2) から までに記載されている事項（例えば、システムに関する記述書、受託会社確認書、受託会社確認書に対する合理的基礎、経営者確認書等）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ます。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の間での調整とコミュニケーションが必要です。一体方式は、再受託会社の合意が不可欠なため、一体方式の利用は、一般的に、受託会社と再受託会社の間に資本関係がある、又は受託会社と再受託会社の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とされています（IT

実 7 号 A5 項参照)。

除外方式の留意点

- ・ 受託会社の内部統制のデザインで予定された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には、受託会社で行われる再受託会社の業務に対する継続的な評価、受託会社の内部監査部門による定期的な再受託会社の内部統制の有効性検証等が含まれます。
- ・ 除外方式では、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には、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るため、当該内部統制が有効に機能していない場合には、業務実施者の意見が除外事項付意見となる可能性があります。受託会社は、モニタリング活動の結果として、再受託会社の内部統制が有効でないと判断した場合には、是正を促すことになります。

方式の変更

再受託会社に対する取扱いについて、方式（一体方式、除外方式）の変更は、保証業務の範囲の変更になるため、慎重な対応が必要になります。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、受託会社から一体方式から除外方式への変更の要請を受ける場合があります。業務実施者は、その変更に対する正当な理由があるかどうかを確かめなければなりません（IT実7号第13項及びA14項参照）。

Q 5 受託会社はその業務の一部を外部に再委託している場合の取扱いとして、「一体方式」を採用する場合の保証報告書の記載例を教えてください。

A 5 一体方式とは、受託会社が受託業務の一部を再委託する場合において、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方式です（IT実7号第6項(3)参照）。

一体方式の場合の保証報告書の記載は、以下のようになります。

（範囲区分の記載例）

受託会社は、{受託業務の種類又は名称}の運用について、×××株式会社（以下、再受託会社）を利用している。受託会社の該当する原則とその規準を充足する内部統制のうち、再受託会社の運用するシステム要素に関する記述は、受託会社の記述書に含まれている（IT実7号第61項(3)参照）。

（意見区分の記載例 - タイプ2の報告書の場合）

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及び××頁の再受託会社確認書に記載されている。

当監査法人の意見は次のとおりである。

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。

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及び再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。

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及び再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。

(意見区分の記載例 - タイプ1の報告書の場合)

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。

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、記述書に記載された受託会社及び再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。

Q 6 受託会社とその業務の一部を外部に再委託している場合の取扱いとして、「除外方式」を採用する場合の保証報告書の記載例を教えてください。

A 6 除外方式とは、受託会社が受託業務の一部を再委託する場合において、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方式です。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、再受託会社の該

当する原則とその規準及び関連する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ます。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入手して検討することが含まれることがあります（IT実7号第6項(16)参照）。

除外方式の場合、受託会社のシステムに関する記述書には、再受託会社の機能が特定されていることが必要ですが、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ありません（IT実7号A29項参照）。

除外方式の場合の保証報告書の記載は、以下のようになります。

（範囲区分の記載例）

受託会社は、{受託業務の種類又は名称}の運用について、×××株式会社（以下、再受託会社）を利用している。記述書には、再受託会社の内部統制が有効に運用されている場合のみ、該当する原則とその規準を充足することが記載されているが、記述書には、該当する原則とその規準を充足する内部統制の導入、運用について記載していない。当監査法人は、当該再受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。（IT実7号第61項(3)参照）

（意見区分の記載例 - タイプ2の報告書の場合）

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次のとおりである。

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。

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、及び、再受託会社において、受託会社の内部統制のデザインで予定された再受託会社の内部統制が平成×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。

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、及び、受託会社の内部統制のデザインで予定された再受託会社の内部統制が平成×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。

(意見区分の記載例 - タイプ1の報告書の場合)

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。

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、及び、再受託会社において、受託会社の内部統制のデザインで予定された再受託会社の内部統制が平成×年×月×日現在におい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。

Q7 監査・保証実務委員会実務指針第86号とIT実7号を統合した報告書で提供することは可能でしょうか。

A7 本保証業務は、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」(以下「監保実86号」という。)が対象とする保証業務を取り扱うものではありません。監保実86号は、委託会社の財務報告に関連する業務を提供する受託会社の内部統制の評価を実施し報告するものです。これに対し、IT実7号はその第1項に記載のとおり、委託会社の業務を提供す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・機密保持に係る内部統制を検証し報告する保証業務です。

また、保証報告書の利用者は、監保実86号が「委託会社とその監査人」を想定しているのに対して、IT実7号第6項(19)「想定利用者」では、「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」を利用者としており、利用者の範囲も異なります。

両者は異なる観点から検証を実施するもので、それぞれ個別に契約されるべきものです。また、クライアントから同時に両方の業務を依頼された場合であっても、利用者の範囲が異なるため、保証報告書は別々に作成されなければなりません。

ただし、業務の同時提供が禁じられているわけではありません。また、双方の業務に共通の証拠を入手して利用できるときには、業務を効率的に実施できることがあります。

Q 8 受託会社のシステムの記述書はどのように記載しますか。

A 8 受託会社のシステムの記述書は、IT実7号第6項(12)で、「「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。」とされています。

また、IT実7号第18項(1)で、含まれるべき内容として以下の事項を挙げています。

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

さらに、同項(2)で、「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。」、同項(3)では、「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。」とされています。

以上のように、システムの記述書には、システムの内部統制を含む広範囲かつ複雑な内容が記載されるため、想定される利用者の利便性を考慮して、フロー図、内部統制と規準のチャートや業務の流れをストーリー的なまとめ方をするなど、受託会社の創意工夫が求められています。

受託会社のシステムに関する記述書（例）

1．システム概要

- (ア) 提供される業務の種類
- (イ) 業務提供に利用されるシステムの範囲
- (ウ) 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

ソフトウェア

人員

手続

データ

- (エ) 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

2．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

3．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

（「実施した運用評価手続及び当該手続の結果」の欄を参照する方法が合理的）

4．委託会社の相補的な内部統制

5．受託業務に関連する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

(ア) 統制環境

経営理念

セキュリティ管理

セキュリティポリシー

(イ) リスク評価プロセス

(ウ) 情報システムと伝達

(エ) 統制活動

(オ) モニタリング活動

以 上

Q9 タイプ2の報告書の場合、「実施した運用評価手続及び当該手続の結果」の作成が必要ですが、記載例はないでしょうか。

A9 「実施した運用評価手続及び当該手続の結果」は、業務実施者が個々の業務で必要と判断して実施した運用評価手続とその結果を記載するものです。したがって、以下に記載した「手続と結果」は単なる記載例で、当該手続の妥当性等については保証するものではありません。

<タイプ2の報告書の「実施した運用評価手続及び当該手続の結果」記載例>

1-2 コミュニケーションに関する共通規準

規準	内部統制	実施した運用評価手続	運用評価手続の結果
1-2.1 (省略)	省略	省略	省略
1-2.2 受託会社のセキュリティ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。	<p>年次のセキュリティ研修を実施するとともに、四半期ごとのアップデート研修も実施している。</p> <p>受託会社は、標準的なサービス及び委託会社ごとの固有のコミットメントを含む正規のサービス契約を締結している。</p> <p>委託会社ごとの固有のコミットメントは、受託会社の法務部の契約担当部署がデータベースに記録している。</p>	<p>年次研修及び四半期の研修について日ごとの出席者のリストに基づき、出席者を抽出して入手し、出席簿のサインと照合した。</p> <p>対象期間内に契約が締結された新規顧客及び既存顧客の契約書を抽出して閲覧し、コミットメントの伝達を確認した。</p> <p>抽出したサンプルのうち、委託会社固有のコミットメントが検出された契約について、契約担当部署の管理するデータベースと照合した。</p>	<p>例外事項なし。</p> <p>例外事項なし。</p>
1-2.3 内部及	受託会社のIT要員は、年	IT要員のリストに基	50 サンプル

規準	内部統制	実施した運用評価手続	運用評価手続の結果
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。	次のセキュリティポリシーの理解に関する確認書に署名している。	づき確認書を抽出して閲覧し、IT要員の署名があることを確かめた。	のうち、1名の署名がなかった。
	受託会社の新入社員は入社オリエンテーションに関連するセキュリティポリシーを通読し、確認書に署名している。	新入社員のリストに基づき確認書を抽出して閲覧し、新入社員の署名があることを確かめた。	例外事項なし。
	業務に係るセキュリティコミットメント及び義務は、受託会社のウェブサイトに掲示されている。	受託会社のウェブサイトを閲覧し、セキュリティコミットメント及び義務の表示を確かめた。	例外事項なし。

Q10 保証業務終了時には、保証報告書と同日付で経営者の確認書を入手することになりますが、記載事項について留意すべき事項はありますか。

A10 IT実7号では、その第44項で以下のような項目の記載を求めています。

- (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

また、業務の遂行上必要に応じて項目を追加することになりますが、具体的には以下のような項目が想定されます。

システムに関する記述書とその他の記載内容の間に識別されている重要な相違

システムに関する記述書及び受託会社確認書に影響を与える規制当局や他の者からの通知が業務実施者に開示されていること

認識されている経営者又は受託会社の従業員による、以下に悪影響を及ぼす可能性のある全ての意図的な行為に関する事実、疑い又は通報

(a) システムに関する記述書の表示の適正性

(b) 該当する Trust サービス規準の充足性

経営者の確認書には、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関する責任が、受託会社にあることを記載します。

なお、以下に記載例を例示しますが、業務実施者が必要に応じて加筆修正を行う事を前提としています。

		平成×年×月×日
監査法人		
代表社員		
業務執行社員 公認会計士	殿(注1)	
	株式会社	
	代表取締役	(署名)
		(又は記名捺印)
	担当取締役	(署名)
		(又は記名捺印)
		(注2)
<p>本確認書は、当社の「平成×年×月×日から平成×年×月×日までの[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(以下「該当する原則とその規準」という。)(注3)を充足するように意図された内部</p>		

統制のデザイン及び運用状況について、貴監査法人が意見を表明するに際して提出するものです。私たちは、下記のとおりであることを確認します。

記

記述書及び受託会社の確認書

1. 私たちは、平成×年×月×日付の保証業務契約書で合意したとおり、受託会社確認書に準拠して記述書を作成する責任を果たしました。私たちの作成した記述書及び受託会社の確認書は適正に表示しております。
2. 不正又は誤謬による重要な虚偽表示のない記述書及び受託会社確認書を作成し、記述書に記載したシステムを適切に運用するために経営者が必要と判断する内部統制を整備及び運用する責任は経営者にあることを承知しております。
3. 受託会社確認書に記載した記述書を作成するための規準は、該当する原則とその規準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関して適切であると判断しております。
4. 保証対象期間終了後、本確認書の日付までに発生した記述書及び受託会社確認書に重要な影響を及ぼす事象は、全て適正に記載されております。
5. その他、業務実施者が記載することが適切であると判断したその他の確認事項

提供する情報

6. 貴監査法人に、保証業務契約書で合意したとおり以下を提供いたしました。
 - (1) 記録、文書及びその他の事項等、記述書及び受託会社の確認書の作成に関連すると認識している全ての情報
 - (2) 記述書に記載したシステムに関連する重要な議事録、稟議書又は決裁書類
 - (3) 貴監査法人から要請のあった意見を表明するための追加的な情報
 - (4) 証拠を入手するために必要であると貴監査法人が判断した、当社の役員及び従業員への制限のない質問や面談の機会
 - (5) 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
 - (6) 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
 - (7) 内部統制のデザインの不備に関する情報
 - (8) システムに関する記述書とその他の記載内容の間に識別されている重要な相違
 - (9) 内部統制が記述されたとおりに運用されていない事例

- (10) 記述書及び受託会社確認書に影響を与える規制当局やその他の者からの通知
(11) 認識されている経営者又は受託会社の従業員による以下に悪影響を及ぼす可能性のある全ての意図的な行為に関する事実、疑い又は通報
- システムに関する記述書の表示の適正性
 - 該当する Trust サービス規準の充足性
7. 全ての関連する事項は記述書又は受託会社確認書に反映されております。

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

公認会計士事務所

公認会計士

- (注2) 確認者は、保証対象システムのサービス内容に応じた適切な組織の責任者とする。
- (注3) この規準は、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。

Q11 いわゆるクラウドサービスに本保証業務を提供する場合の留意点があれば教えてください。

A11 クラウドサービスは、自由に構成可能なIT資源(例えば、ネットワーク、サーバー、記憶装置、アプリケーション又はサービス)の共有プールが、必要に応じて、必要なだけネットワーク経由で利用できることに特徴があります。

クラウドサービスを実現するための技術は、一般に標準化された技術だけではなく、クラウド事業者によって開発された先進的な技術によりサービスが構築、提供されている場合もあります。

また、クラウドサービスを利用する際のリスクは、ユーザー自らの責任になるにもかかわらず、自らが管理できない環境上の脅威及び脆弱性により発生することが少なくありません。これは、クラウドサービスが、クラウド事業者が管理主体となってネットワーク上に様々なリソースを配置していることに起因しています。また、これらのリソースが外国に所在し、当該国の政治体制や法律の影響下にある場合もあります。

さらに、クラウドサービスは、例えば、以下のような多様なシステムと技術、サービスの提供方法があります。

クラウドのリソースの管理主体が複数存在することがある。

サービスの提供方法としてのパブリック、プライベート、コミュニティ及びハイブリッドの構造がある。

サービスの階層としての、SaaS、PaaS、IaaS 等の内容がある。

以上のようなクラウドサービスの特性を理解することが重要であり、保証業務を実施するに当たっては、保証対象範囲の特定、必要な内部統制の特定、証拠を含む内部統制の検証方法の選定等に留意することが必要です。

Q12 IT実7号は、報告書の想定利用者を限定していますが、このうち「予想される委託会社」とはどのような関係を想定しているのでしょうか。

A12 IT実7号第6項(19)で、報告書の「想定利用者」を「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」に限定しています。

この想定利用者に含まれる「予想される委託会社」については、全ての潜在的顧客を想定している訳ではなく、一定の関係を受託会社と構築しつつある潜在的顧客を想定しています。

一定の関係については、客観的な指標を定義することは困難ですが、例えば、以下のような関係と考えられます。

入札条件としてセキュリティ等に関する報告書等の提出が必要になった。

秘密保持契約を締結して詳細な内部情報のやり取りを開始した。

その他、報告書の開示が有用と判断できる状況となった。

なお、報告書は、監査法人又は公認会計士の作成する保証報告書のほか、「受託会社確認書」、「受託会社のシステムに関する記述書」、さらに、タイプ2の報告書の場合には「運用評価手続とその結果に関する記述」のような受託会社の詳細な内部情報も含まれます（IT実7号第6項(14)(15)参照）。

このように報告書の内容が受託会社のビジネス、システムの作用や内部統制の記述等多岐にわたり、かつ、複雑と考えられるため、報告書の提供の可否については、受託会社において慎重に判断するよう求めることが望ましいと考えられます。

以 上