DC セクション 200

SOC2®報告書における受託会社のシステムに係る記述書に関する記述規準

作成者：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SOC2®作業部会

はじめに

.01　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（Assurance Services Executive Committee:ASEC）は、同組織の Trust 情報インテグリティ・タスクフォースの SOC2®ガイド作業部会を通じて、*記述規準*として知られる一連のベンチマークを開発した。この記述規準は、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検証（SOC2®検証）（以下「SOC2®業務」という。）において、受託会社のシステムに係る記述書（以下「記述書」という。）を作成し評価する際に使用されるものである。本文書は、同検証において使用される記述規準を提示する（AICPA の Trust サービス規準は本文書で取り扱わない。[1]それらの規準は SOC2®業務において、記述書において表示されている内部統制が、適用される Trust サービス規準に基づいて受託会社のサービスコミットメント及びシステム要求事項を充足するという合理的な保証を提供するように適切にデザインされ、有効に運用されているかどうか評価する目的で使用される。）。

.02　記述規準の適用には判断が必要となる。そのため、記述規準に加えて、本文書は各規準に対する実施ガイダンスも提示している。実施ガイダンスは、それぞれの規準ごとに、開示の性質及び範囲について判断を下す際に考慮すべき要素を提示している。実務ガイダンスは想定されるあらゆる状況を取り上げているわけではない。そのため、利用者は記述規準を適用する際、受託会社とその環境に関する事実と状況を慎重に検討すべきである。

記述規準の適用可能性と使用

SOC2®業務

.03　本文書に提示されている記述規準は、AICPA ガイド「SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy（SOC2® 受託会社における、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検証についての報告）」（ガイド）に記述されている SOC2®業務と併せて使用されるものとして開発された。SOC2®業務は、AT-C セクション 105「Concepts Common to All Attestation Engagements（全ての証明業務

[1] Trust サービス規準は、「*2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*（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 サービス規準の 2017 年版）」として発行され、TSP セクション 100（AICPA「*Trust サービス規準*」）において体系化されている。TSP セクション 100 のパラグラフ.25～.26 には、受託会社監査人の報告書における同規準の使用に関する経過措置のガイダンスが示されている。

に共通する概念)」及びAT-Cセクション205「Examination Engagements(検証業務)」(AICPA「職業的専門家としての基準及び適用される法令等」)に準拠して実施される。この検証業務において、CPA(受託会社監査人として知られる。)[2]は以下について意見を表明する。

a. 記述書が記述規準に基づいて表示されているかどうか。

b. 内部統制が有効に運用されていれば、適用されるTrustサービス規準に基づいて受託会社のサービスコミットメント及びシステム要求事項が充足するという合理的な保証を提供するように、内部統制が適切にデザインされていたかどうか。

c. タイプ2業務[3]において、適用されるTrustサービス規準[4]に基づいて受託会社のサービスコミットメント及びシステム要求事項が充足するという合理的な保証を提供するように、内部統制が有効に運用されたかどうか。

.04 SOC2®業務では、受託会社のシステムの開発、導入及び運用の最終的な責任を負うのは受託会社の経営者であるため、SOC2®報告書において、受託会社のシステムについての記述書を作成し表示することについても、受託会社の経営者が責任を負っているとの概念に基づいている。受託会社の経営者は、受託会社のシステムに係る記述書を作成する際に本文書の記述規準を使用し、受託会社監査人は記述書が記述規準に基づいて表示されているかどうかを評価する際に同規準を使用する。

記述規準の適合性と可用性

.05 証明基準によれば、適合する規準の特性は以下の通りである。[5]

- 関連性:規準が主題に関連している。
- 客観性:規準に偏向がない。
- 測定可能性:規準により、合理的に一貫した主題の定性的又は定量的測定が可能となる。

---

[2] 証明基準において、証明業務を実施するCPAは通常、*業務実施者*と呼ばれる。しかし、AICPAガイド「*SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*」は受託会社における内部統制に関して報告を行うCPAを業務実施者ではなく*受託会社監査人*と呼称している。そのため、本文書でも*受託会社監査人*という用語を使用する。

[3] SOC2®業務は2種類(タイプ1及びタイプ2)があり、主題は受託会社監査人がどちらの業務を実施するかにより異なる。タイプ1業務の主題は、(*a*) 記述書及び(*b*) 受託会社のサービスコミットメント及びシステム要求事項が、適用されるTrustサービス規準に基づいて充足されることについて、合理的な保証を提供する上での内部統制のデザインの適切性である。タイプ2業務の主題は、(*a*) 記述書、(*b*) 受託会社のサービスコミットメント及びシステム要求事項が適用されるTrustサービス規準に基づいて充足されることについて、合理的な保証を提供する上での内部統制のデザインの適切性及び(*c*) 受託会社のサービスコミットメント及びシステム要求事項が適用されるTrustサービス規準に基づいて充足されることについて、合理的な保証を提供する上での内部統制の運用の有効性である。

[4] この用語は、特定の評価の範囲内に含まれる単一又は複数のカテゴリーに関連するTSPセクション100「*2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*」(AICPA *Trustサービス規準*)におけるTrustサービス規準をいう。

[5] AT-Cセクション105「*Concepts Common to All Attestation Engagements*(全ての証明業務に共通する概念)」(AICPA「*職業的専門家としての基準及び適用される法令等*」)パラグラフ.A42。

・　完全性：規準は、それに基づいて作成された主題が、当該主題に基づく利用者の判断に影響を与えると合理的に予想される関連要素を省略しない場合に充足される。

.06　適合することに加えて、AT-C セクション 105[6]は証明業務に使用される規準を報告書利用者が入手できるべきであると述べている。記述規準の公表は、報告書利用者にその規準を入手可能とする。従って、ASEC は、本文書に提示する記述規準は SOC2®業務での使用に適合しており、入手可能であると結論付けている。

記述規準に基づいた受託会社のシステムに係る記述書の作成及び表示の評価

.07　受託会社の経営者は、委託会社とビジネスパートナーに対する業務の提供に使用されるシステムの内部統制のデザイン、導入及び運用に責任を負う。SOC2®業務において、記述規準に基づいて表示された受託会社のシステムに係る記述書は、委託会社、ビジネスパートナー及び他の SOC2®報告書の想定利用者（集合的に報告書利用者として知られる。）が、受託会社のシステム（当該システムを介したデータと情報の処理及びフローを含む。）を理解できるようにデザインされている。記述書は、受託会社が、受託会社のサービスコミットメント及びシステム要求事項の充足にとって脅威となるリスクを管理する目的で適用している手続及び内部統制を記述する。記述書は、内部統制及びシステム運用の裏付けとなる書類並びに業務を提供する上で用いられるシステム内の方針、プロセス及び手続に関する検討に基づいて、受託会社の経営者により作成される。

.08　SOC2®報告書は、受託会社、それが提供する業務及びそうした業務の提供に用いられるシステム等に関して十分な知識及び理解を有する者により利用されることを意図している。その結果として、記述書を起草する際、受託会社の経営者は利用者がそうした知識や理解を有していると仮定することができる。さらに、利用者がそうした知識や理解を有していない場合、SOC2®報告書の内容、経営者が作成する確認書及び受託会社監査人の意見（これらは全て報告書に含まれる。）を正しく理解できない可能性が高い。そうした理由から、経営者及び受託会社監査人は、報告書の想定利用者（以下「特定当事者」という。）に関して合意すべきである。SOC2®報告書の特定当事者には、受託会社の要員、期間の一部又は全期間にわたってシステムを利用する委託会社、システムとのやり取りにより生じるリスクの対象となるビジネスパートナー、委託会社、ビジネスパートナーに業務を提供する業務実施者、想定される委託会社、ビジネスパートナー及びそうした事項に関する十分な知識と理解を有する規制当局が含まれる可能性がある。

.09　通常、記述書は叙事的であるが、記述書に関して所定の形式はない。記述書に含まれる説明文を補足する目的で、フローチャート、マトリクス表、表、グラフ、コンテキスト・ダイアグラム又はそれらの組合せが使用される場合がある。

.10　さらに、記述書はさまざまな方法で構成される場合がある。例えば、内部統制の構成要素（統制環境、リスク評価、統制活動、情報と伝達、モニタリング活動）ごとに構成される場合がある。別の方法として、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、手続及びデータ）ごとに整理され、受託会社のサービスコミットメント及びシステム要求事項

[6] AT-C セクション 105 パラグラフ.25*b*。

の充足を妨げるリスクの特定と評価並びにそれらに対処するための内部統制のデザイン、導入及び運用に関連する内部統制の構成要素の諸側面に関する開示により補足されることもあり得る。

.11　記述書に含まれる開示の程度は、受託会社とその活動の規模と複雑さに応じて異なる場合がある。加えて、特に、業務の特定の側面が報告書利用者にとって関連性がないか、又はSOC2®業務の対象範囲外である場合、記述書は受託会社のシステム又はシステムにより提供される業務のあらゆる側面を取り上げる必要はない。例えば、委託会社に提供するサービスへの請求に関連する受託会社のプロセスは、報告利用者にとって関連性がある可能性が低い。同様に、記述書には、それによって業務が提供される手作業及び自動化によるシステムでの両方の手続が含まれるが、必ずしもプロセスの全てのステップを開示する必要はない。

.12　通常、SOC2®業務における受託会社のシステムに係る記述書は、(a) 受託会社が業務の提供を目的として導入している（すなわち、運用している。）システムを記述し、(b) 記述されているシステムに関連する範囲において、各記述規準についての情報を含み、かつ(c) 利用者の意思決定に関連する可能性が高い情報を不注意により、意図的に省略又は歪曲しない場合に、記述規準に基づいて表示されている。記述書は各記述規準についての開示を含むべきであるが、そうした開示は、敵対する当事者がセキュリティの脆弱性に付け込み、受託会社がサービスコミットメント及びシステム要求事項を充足する能力を毀損する可能性を高める水準にまで詳細になされることを意図していない。その代わりに、開示では、受託会社が直面するリスクの内容とリスクが顕在した場合の影響を報告書利用者が理解できるようにすることを意図している。

.13　記述書は、(a) 特定のＩＴ構成要素がない場合にそれらがあると声明又は示唆する、(b) 特定のプロセスや内部統制が実施されていない場合にそれらが導入されていると声明又は示唆する、又は(c) 客観的に評価できない声明（誇大広告等）を含む場合、記述規準に基づいて表示されていない。

.14　特定の状況において、記述書を補足する目的で追加的な開示が必要となる場合がある。そうした追加的開示の要否に関する経営者の意思決定及び受託会社監査人による経営者の意思決定に対する評価には、開示が報告書利用者の意思決定にとって関連性が高い情報に影響を与えるかどうかの検討が含まれる。追加的開示には、例えば以下が含まれる可能性がある。

- SOC2®業務の特定の状況での記述規準の適用において行った重要な解釈（例えば、何がセキュリティ事象又はインシデントを構成するのか。）
- 後発事象（内容及び重要性に応じて）

記述書が記述規準に基づいて表示されているかについて、作成及び評価時における重要性の検討事項

.15　パラグラフ.02 で述べたように、記述規準の適用には判断が必要となる。そうした判断の一つに、報告書利用者の情報ニーズが含まれる。SOC2®報告書の大半が、広範な特定当事者を有する。そのため、記述書は特定当事者の共通の情報ニーズを満たすことが意図されており、通常は、個々の報告書利用者それぞれにとって重要とみなされる可能性のあるシステムのあらゆる側面についての情報を含むことはない。しかし、記述書が記述規準に基づいて表示されており、報告

書利用者のニーズを満たす上で十分なものかどうかを判断することにおいて、広範な SOC2®報告書の想定利用者の視点と情報ニーズの理解が必要となる。

.16　記述書が記述規準に基づいているかどうかを評価する際、経営者は記述書内の虚偽表示又は省略が、個別に又は全体として、SOC2®報告書の特定当事者の意思決定に影響を与えることが合理的に予想されるかどうか検討する。例えば、プライバシーに関連性のある内部統制の SOC2®業務において、経営者は、EU 一般データ保護規則の遵守に関わる主要なサービスコミットメントを記述していないことを発見する場合がある。そうした情報は、SOC2®報告書利用者の意思決定に影響を与えると合理的に予想されるため、経営者はそうした情報の省略がそれら利用者の意思決定に影響を与える可能性があると結論付けるかもしれない。その場合、経営者は関連情報を含めることにより記述書を修正することが考えられる。[7]

.17　記述規準は主要な非財務情報の開示を求めているため、ほとんどの記述書は叙事的形式で表示される。そのため、重要性に関する検討は主として定性的な性質を有し、関連情報が省略されている可能性を含め、報告書利用者の意思決定に影響を与えると合理的に予想される情報の中に虚偽表示があるかどうかを中心とする。検討されるべき定性的要因には以下が含まれる。

- 受託会社のシステムに係る記述書に、システム処理の重要な側面が含まれているかどうか。
- 記述書が報告書利用者にとって有意義なものである可能性が高い水準の詳細さで作成されているかどうか。
- パラグラフ.19 にある関連する記述規準がそれぞれ、情報を省略又は歪曲する文言を用いることなく取り上げられているかどうか。
- 記述規準は表示におけるバリエーションを許容しているため、表示の特性が適切かどうか。

SOC2®業務における受託会社のシステムに係る記述書についての記述規準及び関連実施ガイダンス

.18　記述規準に準拠した表示のために、記述書は通常、下表の左欄に示した各要求事項（規準）についての情報を、その規準がシステムに適用され、Trust サービスカテゴリーが検証の対象範囲に含まれる限り、開示する必要がある（重要性に関する検討事項については、パラグラフ.15 から始まる前セクションにて述べられている。）。

.19　下表右欄の実施ガイダンスは、それぞれの規準ごとに、開示の性質及び範囲について判断を下す際に考慮すべき要素を提示している。実施ガイダンスはあらゆる状況に対応しているわけではない。そのため、受託会社の経営者には、SOC2®業務において記述規準を適用する際、受託会社に関する具体的な事実と状況並びに提供される業務の内容を慎重に検討することが推奨される。

[7] 記述書が SOC2®報告書利用者の特定のサブグループの情報ニーズを満たす目的で作成されている（及び報告書がそれらの特定の利用者に制限されている。）場合、経営者は虚偽表示（省略を含む。）が報告書利用者の当該特定のサブグループに影響を与えるかどうかを検討する。

記述規準	*実施ガイダンス*
記述書には以下の情報が含まれる。	本規準に関して含める開示の性質及び範囲について判断を下す際には、以下を検討する。
DC 1：提供される業務の種類	受託会社により提供される業務の種類の例は以下の通りである。 ・ *顧客サポート*：委託会社の顧客に、オンライン又は電話でのアフターサービスサポート及び業務管理を提供すること。こうした業務の例として、品質保証に関する問合せや顧客の苦情に関する調査及び対応が挙げられる。 ・ *医療保険請求の管理及び処理*：医療提供者、雇用主、第三者管理機関及び雇用者が保険契約者となる団体保険の契約者に対して、診療記録及び関連する医療保険請求を正確に、安全に、そして秘密に処理できるようにするシステムを提供すること ・ *エンタープライズＩＴアウトソーシング業務*：委託会社のＩＴデータセンター、インフラストラクチャー及びアプリケーションシステム並びにＩＴ活動をサポートする関連機能（ネットワーク、本番環境、セキュリティ、変更管理、ハードウェア、環境上の統制活動等）の管理、運用及び保守 ・ *マネージドセキュリティ*：委託会社向けのネットワークやコンピューターシステムへのアクセス管理（システムへのアクセスの付与、システムへの侵入の防止又は検知及び軽減等） ・ *金融テクノロジー（FinTech）業務*：金融サービス会社に対する、情報技術に基づいた取引処理業務の提供。そうした取引の例としては、ローン処理、P2P融資、支払処理、クラウドファンディング、ビッグデータ解析及び資産運用が挙げられる。
DC 2：主要なサービスコミットメント及びシステム要求事項	内部統制のシステムは、Trustサービス規準を使用し、企業がその業務目的及び下位目的を達成する能力という観点から評価される。受託会社が委託会社に業務を提供する場合、その目的及び下位目的は、主として以下に関係する。 a. 業務の提供に使用されるシステムに関して委託会社に対して行うサービスコミットメントの充足及びそうしたコミットメントの充足に必要なシステム要求事項 b. システムによる業務の提供に関する法令の遵守 c. 受託会社がシステムに関して有する他の目的の達成 これらを受託会社のサービスコミットメント及びシステム要求事項という。 受託会社の経営者は、自らがそのシステムの目的を達成していることについて合理的な保証を提供する内部統制のデザイン、導入及

記述規準	*実施ガイダンス*
	び運用に責任を負うが、経営者が記述書において開示することが求められるのは、次のセクションで述べるように、その主要なサービスコミットメント及びシステム要求事項のみである。 *主要なサービスコミットメント*：主要なサービスコミットメント及びシステム要求事項の開示によって、報告書利用者はシステムを運用する目的と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を評価する上で適用されるTrustサービス規準がどのように利用されたかを理解できる。 サービスコミットメントには、委託会社及びその他（委託会社の顧客等）に対して約束されたコミットメントが、そうしたコミットメントが記述書で取り上げられる単一又は複数のTrustサービスカテゴリーに関係する場合において含まれる。例えば、サービスコミットメントには、米国立標準技術研究所（National Institute of Standards and Technology:NIST）の政府機関及び他の当事者に関するリスク管理枠組みの一部としてのサービスコミットメントも含まれる可能性がある。 受託会社が委託会社及びその他に対して作成するサービスコミットメントは、それらの企業のニーズに基づく。開示されるサービスコミットメントを特定する際、受託会社の経営者は委託会社に対して行ったコミットメントのレビューから着手することができる。サービスコミットメントは、契約、サービス品質保証（Service Level Agreements:SLA）及び公開されたポリシー（例えば、プライバシーポリシー）を通じて等、多くの方法により委託会社に伝達できる。特定の伝達形式は必要とされない。 受託会社は、以下を含め、記述されている業務の多くの異なる側面に関してサービスコミットメントを作成する場合がある。 ・ 計算に使用されるアルゴリズムの仕様 ・ システムが利用可能となる時間 ・ 公開されたパスワード標準 ・ 保存される顧客データの暗号化に使用される暗号化標準 サービスコミットメントは、記述書で取り上げられている一つ以上のTrustサービスカテゴリーについて作成できる。一例として、記述書においてプライバシーに関する内部統制が取り上げられている場合、受託会社は以下のコミットメントを作成できる。 ・ データ主体（本人）の同意を得ることなく情報を処理又は移転しないこと

記述規準	*実施ガイダンス*
	・　６カ月ごとに、又は受託会社の業務ポリシーに変更があった際に顧客にプライバシー通知を行うこと ・　顧客からアクセス要請を受けてから10営業日以内に要請に対応すること 受託会社の経営者はサービスコミットメントを全て開示する必要はなく、開示する必要があるのは広範なSOC2®報告書利用者に関連性のあるもの（すなわち主要なサービスコミットメント）のみである。例えば、記述書で可用性が取り上げられている場合、受託会社は同一のシステム可用性に関するコミットメントをその大多数の委託会社に対して作成できる。委託会社の大半に共通する可用性に関するコミットメントについての情報は、広範なSOC2®報告書利用者に関連性のある可能性が高いため、受託会社の経営者は記述書において主要な可用性に関するコミットメントを記述することになると考えられる。 しかし、他のケースにおいて、受託会社は、他の委託会社よりも高度なシステム可用性を必要とする個別の委託会社に対し、システム可用性に関して異なるコミットメントを作成している場合がある。そうしたコミットメントは広範なSOC2®報告書利用者にとって関連性がある可能性が低いため、通常、受託会社の経営者はそれを開示しないと考えられる。そうしたサービスコミットメントは記述書で開示されないため、当該個別委託会社は、内部統制のデザインの適切性の評価及びタイプ2の検証において、内部統制の運用の有効性の評価が、受託会社によるその主要な（すなわち、大部分の委託会社と共通の）サービスコミットメント及びシステム要求事項の充足に基づいて実施されていると理解する。そのため、当該個別委託会社は受託会社から、その個別の可用性に関するコミットメントの達成に関して追加的情報を取得する必要がある場合がある。 記述書がプライバシーを取り上げている場合、受託会社の経営者は受託会社のプライバシー通知において、又は記述されているシステムに関連性のあるプライバシーポリシーにおいて、特定しているサービスコミットメント及びシステム要求事項を開示する。そうした開示を行う際には、受託会社の経営者が委託会社との合意により認められているパーソナル・インフォメーションの目的、使用方法及び開示を記述していれば、報告書利用者にとって有益である可能性がある。 *主要なシステム要求事項*：システム要求事項とは、システムが以

記述規準	*実施ガイダンス*
	下を行うためにどのように機能するかについての仕様である。 ・　委託会社及びその他（委託会社の顧客等）に対する受託会社のサービスコミットメントの充足 ・　ベンダー及びビジネスパートナーに対する受託会社のサービスコミットメントの充足 ・　関連法令及び業界団体（ビジネス団体や事業者団体等）の指針の遵守 ・　記述書に取り上げられているTrustサービスカテゴリーに関連性のある受託会社の他の目的の達成 要求事項は、しばしば受託会社のシステムポリシーと手続、システム設計書、顧客との契約及び政府規制で規定されている。 システム要求事項の例は、以下のとおりである。 ・　政府の銀行規則で設定された従業員の指紋採取とバックグランドチェック ・　設計書で許容された値を制限するシステム編集 ・　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許容される最大の間隔 ・　シンプル・オブジェクト・アクセス・プロトコル（Simple Object Access Protocol:SOAP）のように、業界又は他の組織で設定された関連する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（Health Insurance Portability and Accountability Act:HIPAA）の下のセキュリティ システム要求事項は、一つ以上のTrustサービスカテゴリーに関する受託会社のコミットメントによって生じる場合がある（例えば、データ入力とデータ承認間の職務分掌をプログラムで実施するというコミットメントからは、ユーザーアクセス管理に関するシステム要求事項が生じる。）。 開示する必要がある主要なシステム要求事項とは、記述書で取り上げられる単一又は複数のTrustサービスカテゴリーに関連性があり、広範なSOC2®報告書利用者にとって関連性がある可能性が高い要求事項である。どのシステム要求事項を開示するかを特定する際に、受託会社の経営者は記述されているシステムに関連性のある社

記述規準	*実施ガイダンス*
	内ポリシー、システムの設計と運用において下された主な決定及びシステムに係る他の業務要件を検討できる。例えば、システム関連業務の営業利益に関する社内の要求事項は広範なSOC2®報告書利用者にとって関連性がないため、開示される必要はない。
DC 3：以下を含む、業務の提供に使用されるシステムの構成要素 a.インフラストラクチャー b.ソフトウェア c.人員 d.手続 e.データ	*インフラストラクチャー*：インフラストラクチャー構成要素に関する開示には、受託会社が業務を提供する上で使用する物理環境及び関連構築物、ＩＴ並びに関連ハードウェア（例えば、施設、サーバー、ストレージ、環境モニタリング機器、データ保存機器及び媒体、モバイル機器、社内ネットワーク並びに接続された対外通信用ネットワーク）を含むＩＴ環境全体をサポートする物理的又は仮想的リソースの集成等の事項が含まれる。 *ソフトウェア*：ソフトウェア構成要素に関する開示には、アプリケーションプログラム、そうした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）、使用されるデータベースの種類、外部接続するウェブ・アプリケーションの内容及び社内で開発されたアプリケーションの内容（使用されるアプリケーションが、モバイル・アプリケーションかデスクトップ及びラップトップ・アプリケーションのいずれかについての詳細を含む。）等の事項が含まれる。 *人員*：人員構成要素に関する開示には、システムのガバナンス、管理、運用、セキュリティ及び使用に関与する要員（ビジネスユニットの要員、開発者、運用担当者、委託会社の要員、ベンダーの要員及び管理者）が含まれる。 *手続*：受託会社により実施される自動化された及び手作業による手続に関する開示には、主として業務の提供を通じた手続に関係する。それらには、適宜、業務活動が開始、承認、実施及び伝達される手続並びに作成される報告その他の情報が含まれる。 プロセスは、特定の目標を達成するようデザインされた一連のつながりのある手続で構成される（例えば、サードパーティリスク管理のためのプロセス）。手続は、プロセスを実施する上で実行される特定の活動である（例えば、ベンダーの請求と関与を評価し管理するために整備されている手続）。そうした理由から、受託会社の経営者は手続を、それが一部分を構成するプロセスの文脈の中で記述することが容易であると考える可能性がある。 ポリシーとは、内部統制を有効化する上で何をすべきかに関す

記述規準	*実施ガイダンス*
	る、経営者又は取締役の声明である。そうした声明は、文書化されるか、コミュニケーションの中で明確に表明されるか、又は活動や決定を通じて示唆される場合がある。ポリシーは手続の基礎となる。受託会社は、期待される事項を定めたポリシーと、ポリシーを活動に変換する手続を通じて、内部統制活動を展開する。 受託会社により作成される報告書及びその他の情報も、受託会社により実施された活動の順序を報告書利用者がより理解できるよう、記述書に含める場合がある。 システム構成要素は、受託会社のシステムとシステム境界に関するより明確な理解を形成する具体的な技術用語を使用して記述される場合もある。技術用語は、委託会社に対する受託会社の影響を検討する際に、報告書利用者が受託会社の物理的及び論理的構成要素を理解する上での助けとなる。受託会社にとって、開放型システム間相互接続（Open Systems Interconnect:OSI）7階層モデルの概念を使用してシステム記述書を向上させることが有益な場合がある。例として、受託会社はシステムの特定構成要素がどのように、どの階層で運用されるかを以下のような記述と共に記載することができる。 セキュアシェル（Secure Shell:SSH）を介して、システム利用者をトランスポート層セキュリティ（Transport Layer Security:TLS）標準及びプロトコルに従って動作するセキュアファイル転送プロトコル（Secure File Transfer Protocol:SFTP）サーバーに接続するクライアント仮想プライベートネットワーク（Virtual Private Network:VPN）ハードウェアを使用した受託会社での暗号化接続が行われている。 *データ*：データ構成要素に関する開示には、システムで使用されるデータの種類、取引の流れ、ファイル、データベース、表及びシステムにより使用又は処理された出力が含まれる。 記述書が機密保持又はプライバシーのカテゴリーを取り上げる場合、データ構成要素について開示が検討される可能性があるその他の事項には以下が含まれる。 ・ 受託会社により生成、収集、処理、伝達、利用若しくは保管されるデータの主な種類、並びにデータの収集、保持、開示、処分又は匿名化に使用される手法 ・ 法令又はコミットメントに基づいてセキュリティ、データ保護又は侵害の開示が保証されるパーソナル・インフォメーショ

記述規準	*実施ガイダンス*
	ン（例えば、個人を特定可能な情報、保護された健康情報及びペイメントカード情報） ・　法令又はコミットメントに基づいてセキュリティ、データ保護又は侵害の開示が保証される第三者企業情報（例えば、契約上の守秘義務の対象となる情報） 記述書が機密保持又はプライバシーに関する内部統制について取り上げる場合、経営者は、最低限、明確に定義されたプロセス及び非公式の臨時的な手続の範囲内での、業務を提供する際に使用される機密及びパーソナル・インフォメーションの情報ライフサイクルに関係する、全てのシステム構成要素を取り上げると考えられる。 *システム境界*：受託会社で実施される活動の全てが記述されているシステムの一部というわけではない。システム境界の外部にある機能又はプロセスを見極め、それらを記述書に記述することは、報告書利用者がシステム境界を誤解することを防ぐ上で必要となる場合がある。そのため、特定の機能又はプロセスが記述されているシステムの一部かどうかについて報告書利用者が混乱するリスクがある場合、記述書はどのプロセス又は機能が評価対象に含まれるかを明確化する必要がある。 例えば、以下の受託会社の機能又はプロセスは、記述されているシステム境界の外部にある可能性がある。 ・　受託会社により提供された業務に関して委託会社に請求するために使用されるプロセス ・　新規委託会社の受託会社のシステムへの転換。一部の受託会社に関して、そうした転換は記述されているシステムとは全く異なるシステムにより取り扱われる。 ・　記述されているシステムの外部のソースからのデータの受領。一例として、処理の準備ができた状態で雇用主から情報入力を受け取る給与処理システムがある。これは、受託会社のシステムの責任を、特定の銀行口座に直接銀行預金を生成するために雇用主から提供される入力の処理に制限する。 *第三者アクセス*：ベンダー、ビジネスパートナー及びその他（第三者）はしばしば、機微データを保管、処理及び転送するか、又は他の何らかの方法で受託会社のシステムにアクセスする。これらの第三者は、システムの構成要素を提供する場合がある。受託会社の経営者は、そうした第三者により提供されるシステムの構成要素を記述する必要がある場合がある。そうした開示には、例え

記述規準	*実施ガイダンス*
	ば、受託会社のシステムに対する第三者のアクセスおよび接続の性質が含まれる可能性がある。
DC 4：識別されたシステムインシデントのうち、（a）適切にデザインされなかった若しくは有効に運用されなかった内部統制の結果であるもの、又は（b）記述書の日付時点において（タイプ1の場合）若しくは記述書の対象である期間において（タイプ2の場合）、他の何らかの形で一つ以上のサービスコミットメント及びシステム要求事項の達成における重大な不備を生じさせたものに関する、以下の情報 a. 各インシデントの内容 b. インシデントをめぐる時間的経緯 c. インシデントの範囲（又は影響）及びその処理	インシデントを開示するかどうかを決定する際には判断が必要となる。しかし、記述されているシステムに関係する限りにおいて、以下の事項を検討することは、そうした決定を下す上で有益である場合がある。 ・ インシデントが、一つ以上の内部統制が適切にデザインされていなかった、又は有効に運用されなかったことによって生じたかどうか。 ・ インシデントの結果、受託会社の一つ以上のサービスコミットメント及びシステム要求事項の充足における重大な不備が生じたかどうか。 ・ サイバーセキュリティ関連法規制により、インシデントの公開が必要か（又は必要となる可能性が高いか）どうか。 ・ インシデントが受託会社の財政状態又は業務に重大な影響を与えたかどうか、及び財務諸表の作成にあたり必要な開示事項に重大な影響を与えたかどうか。 ・ インシデントが法規制機関による制裁につながったかどうか。 ・ インシデントが受託会社による重要市場からの撤退又は重要契約の解消につながったかどうか。 識別されたセキュリティインシデントについての開示は、敵対する当事者がセキュリティの脆弱性に付け込み、受託会社のサービスコミットメント及びシステム要求事項を充足する能力を毀損する可能性を高める水準にまで詳細になされることを意図していない。むしろ、開示により、受託会社が直面するリスクの内容とリスクが発現した場合の影響を報告書利用者が理解できるようになることを意図している。 受託会社が、受託会社の一つ以上のサービスコミットメント及びシステム要求事項の充足における不備につながったセキュリティ違反を識別したと仮定する。その違反は、記述書の対象期間の6カ月前に発生したものであるが、記述書の対象期間内において完全に是正されていなかった。この例では、経営者は受託会社が直面するリスクの内容とリスクが発現した場合の影響を報告書利用者が理解できるよう、記述書において同インシデントを開示する必要がある可能性が高いと考えられる。

記述規準	*実施ガイダンス*
	加えて、受託会社の経営者は再受託会社で把握されたインシデントを開示するかどうかを、経営者が一体方式と除外方式のどちらの使用を選択しているかにかかわらず、検討すべきである。
DC 5：適用されるTrustサービス規準、並びに受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供することを目的としてデザインされた関連する内部統制	TSPセクション100「2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy」（AICPA「Trustサービス規準」）は、各Trustサービスカテゴリーにおける規準を提示している。記述書は、統制環境、リスク評価、統制活動、情報と伝達、モニタリング活動等、記述書の対象となる単一又は複数のTrustサービスカテゴリー（適用されるTrustサービス規準）に関連する各規準についての情報を含んでいる場合、この規準に基づいて表示されている。例えば、記述書が可用性を取り上げている場合、経営者はTrustサービス規準内の共通規準及び可用性に関する追加的なTrustサービス規準に対応するために実施している内部統制についての情報を提供すると考えられる。
DC 6：受託会社の経営者が、受託会社のシステムのデザインにおいて、特定の内部統制が委託会社により実施されると仮定しており、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社における内部統制と組み合わせてそうした内部統制が必要である場合、そうした相補的な委託会社の内部統制（Complementary User Entity Controls: CUECs）	相補的な委託会社の内部統制：CUECsは、受託会社の経営者が、システムのデザインにおいて、委託会社により実施されると仮定している内部統制であって、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社における内部統制と組み合わせて必要なものである。 受託会社はそのサービスコミットメント及びシステム要求事項を、自らが責任を負い、合理的に実施可能な事項に限定するため、受託会社は通常、委託会社におけるCUECsの実施に依拠することなく、そのサービスコミットメント及びシステム要求事項を充足できる。以下のTrustサービス規準（CC）6.2を検討すること。 企業は、システム資格を発行し、システムへのアクセスを許可する前に、組織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を登録及び承認する。企業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もはや承認されないときには、ユーザーのシステム資格は削除される。 Trustサービス規準（CC）6.2は、委託会社が受託会社に許可されたユーザーのリストを供給した後、システムがユーザー（委託会社により許可されたユーザーとして身元確認されたユーザー）を登録し、当該ユーザーにシステム認証情報を発行することのみを求めており、そのためこの規準は受託会社の責任を限定している。委託会

記述規準	*実施ガイダンス*
	社は、ユーザーの身元確認及び受託会社への許可されたユーザーのリストの供給に責任を負う。委託会社が不注意により承認されていない従業員を含むリストを提供した場合でも、受託会社は規準を充足している。従って、許可されたユーザーの身元確認及びその情報の受託会社への伝達はCUECsとはみなされない。 CUECsが網羅的に、正確に記述されており、受託会社によるサービスコミットメント及びシステム要求事項の充足にとって関連性がある場合、記述書はこの規準に基づいて表示されている。 委託会社の責任：CUECsに加えて、委託会社はシステムを使用する際に他の責任を負う場合がある。そうした責任は、委託会社が受託会社による業務の利用から意図した便益を得る上で必要となる。例えば、速配サービスのユーザーは完全で正確な受取人情報の提供と適切な梱包材の使用に責任を負う。そうした責任を委託会社の責任という。 Trustサービス規準（CC）2.3は、企業は、内部統制が機能することに影響を及ぼす事項に関して、外部の関係者との間での情報伝達を行うとしている。これには、委託会社の責任の伝達が含まれると考えられる。しかし、委託会社の責任は膨大であり得るため、それらは他の手法により伝達されることが多い（例えば、ユーザーマニュアルに記述する。）。その結果、記述書における委託会社の責任を記述書で開示することは一般に実際的ではない。それに代えて、経営者は通常、記述書において、委託会社の責任について外部ユーザーに行う情報伝達の種類を特定している。そうした情報伝達の形式と内容は受託会社の経営者の責任である。 受託会社の経営者が委託会社の責任を特定の当事者のみに伝達する場合（例えば、委託会社との契約書に含める場合）、経営者は他のSOC2®報告書の想定利用者がそれを誤解する可能性が高いかどうかを検討し、誤解が生じる可能性が高いとき、経営者は報告書の利用をそうした特定当事者に限定すべきである。受託会社の経営者が報告書の利用の限定を希望しない場合、経営者はユーザーによるシステム及び受託会社監査人の報告書の誤解を防ぐために、重要な委託会社の責任を受託会社のシステムに係る記述書に含めることが考えられる。そうしたケースにおいて、報告書は広範なSOC2®報告書利用者にとって適切と考えられる。 受託会社の経営者が記述書に重要な委託会社の責任を含める場合、経営者はそうした開示を、記述書が記述規準に基づいて表示さ

記述規準	*実施ガイダンス*
	れているかどうかについての評価の一環として評価する。
DC 7：受託会社が再受託会社を使用しており、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社の内部統制と組み合わせて、再受託会社の内部統制が必要である場合、以下が含まれる。 a.受託会社の経営者が一体方式の使用を選択する場合： i.再受託会社により提供される業務の内容 ii.受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社の内部統制と組み合わせて必要な、再受託会社の内部統制 iii.再受託会社のインフラストラクチャー、ソフトウェア、人員、手続及びデータのうち、関連する側面 iv.システムのうち、再受託会社の責任に帰すべき部分 b.受託会社の経営者が除外方式の使用を決定する場合： i.再受託会社により提供される業務の内容 ii.再受託会社における内部統制により充足される	*一体方式*：受託会社の経営者が一体方式を選択する場合、再受託会社のインフラストラクチャー、ソフトウェア、人員、手続及びデータの関連する側面は受託会社のシステムの一部とみなされ、受託会社のシステムの記述書に含まれる。関連する側面は受託会社のシステムの一部とみなされるものの、システムの再受託会社の責任に帰すべき部分は記述書で個別に特定されると考えられる。そうした開示には、受託会社によるサービスコミットメント及びシステム要求事項の充足の妨げとなるリスクの特定と評価並びにそれらに対処するための内部統制のデザイン、実施及び運用に関連する内部統制の構成要素の諸側面が含まれる。 記述書は、受託会社における内部統制と再受託会社における内部統制を個別に特定すると考えられる。しかし、両者の区別に関して所定の形式はない。 *除外方式*：受託会社の経営者が除外方式を選択する場合に、再受託会社により提供される業務についての情報を入手し、再受託会社により提供される業務に係る手続の実施を希望する委託会社又はビジネスパートナーにとって、再受託会社の身元についての情報が有益となる可能性がある場合は、こうした情報を開示することが検討される場合がある。 相補的な再受託会社の内部統制（Complementary Subservice Organization Controls:CSOCs）は、受託会社の経営者が、システムのデザインにおいて、再受託会社により実装されると想定された内部統制であって、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社における内部統制と組み合わせて必要なものである。除外方式を使用する場合、記述書は再受託会社が実施していると想定されたCSOCsの種類を特定することになると考えられる。 記述書には、そうしたCSOCsの実施に関する再受託会社の責任も含めるとともに、CSOCsが適切にデザインされ、記述書の対象期間にわたって有効に運用される場合にのみ、関連するサービスコミットメント及びシステム要求事項が充足可能であることを明示することが重要である。 報告利用者にとって意義あるものであるために、経営者は記述されているシステムにより提供される業務に固有のCSOCsのみを含める。CSOCsは、個別の内部統制としてではなく、内部統制の広範なカ

記述規準	*実施ガイダンス*
ことが意図される適用可能な各Trustサービス規準 iii.受託会社の経営者が、受託会社のシステムのデザインにおいて、再受託会社により実施されると仮定している内部統制であって、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社における内部統制と組み合わせて必要なものの種類（一般に相補的な再受託会社の内部統制又はCSOCsと呼ばれる。）	テゴリー又は内部統制の種類として表示される場合がある。 受託会社の経営者は、記述書にサービスコミットメント及びシステム要求事項が受託会社の内部統制のみで充足される場合と、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供する上で受託会社の内部統制とCSOCsとの組み合わせが必要な場合を特定した表を含めることを希望する場合がある。 CSOCsの例には以下が含まれる。 ・　受託会社の代理として行う取引処理の完全性と正確性に関連する内部統制 ・　受託会社に提供され、受託会社が利用する指定報告書の完全性と正確性に関連する内部統制 ・　受託会社のために実施される処理に関連するＩＴ全般統制 ・　無停電電源装置（Uninterruptible Power Supply:UPS）により、データセンターが処理環境への電力供給の途絶から保護されていること CSOCsが完全で、正確に記述されており、受託会社によるサービスコミットメント及び記述されているシステムに関連するシステム要求事項の充足にとって関連性がある場合、記述書はこの規準に基づいて表示されている。 *その他の事項*：複数の再受託会社を使用する受託会社は、１社以上の再受託会社に除外方式を使用し、それ以外の再受託会社に一体方式を使用して記述書を作成する場合がある。 受託会社の経営者が選択する手法にかかわらず、記述書は受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するためにデザインされた内部統制を開示する必要があり、そうした内部統制には、受託会社が再受託会社によって提供される業務をモニタリングする上で使用する内部統制が含まれる。そうしたモニタリング目的の内部統制には以下の組み合わせが含まれる可能性があるが、これらに限らない。 ・　受託会社の内部監査機能のメンバーによる再受託会社における内部統制の評価手続 ・　出力された帳票のレビュー及び照合 ・　再受託会社の人員と定期的な協議を行い、確立されたサービス品質向上の目的及び合意に照らして再受託会社のパフォーマンスを評価すること

記述規準	*実施ガイダンス*
	・　再受託会社に対する現地視察を行うこと ・　再受託会社のシステムに係るタイプ2のSOC2®報告書の閲覧 ・　外部との情報伝達（再受託会社により実施される業務に関連する委託会社からの苦情等）のモニタリング
DC 8：適用されるTrustサービス規準のうち、システムに関連しない特定の規準及びそれが関連しない理由	適用されるTrustサービス規準の一つ以上が記述されているシステムに関連しない場合、受託会社の経営者は記述書にそうした規準が関連しない理由についての説明を含める。例えば、適用されるTrustサービス規準が受託会社により提供される業務に適用されない場合、その規準は関連しない可能性がある。 委託会社（受託会社ではなく）が委託会社の顧客からパーソナル・インフォメーションを収集すると仮定する。記述書がプライバシーに関する内部統制を取り上げている場合、受託会社の経営者は記述書において、委託会社によるパーソナル・インフォメーションの収集に関する内部統制を開示しないと考えられるが、そうした省略についての理由は開示されると考えられる。これに対して、特定の活動を禁じるポリシーの存在は、規準が適用されないとする上で十分ではない。例えば、記述書がプライバシーに関する内部統制を取り上げている場合、受託会社のポリシーが第三者へのパーソナル・インフォメーションの開示を禁じているという事実のみに基づいて、受託会社が記述書において第三者へのパーソナル・インフォメーションの開示を省略することは不適切であると考えられる。その代わりに、記述書には、そうした開示を防止又は検知するポリシー及び関連内部統制が記述されると考えられる。
DC 9：一定期間を対象とする記述書（タイプ2検証）において、当該期間における受託会社のシステム及び内部統制への重要な変更についての関連する詳細であって、受託会社のサービスコミットメント及びシステム要求事項に関連するもの	開示されるべき重要な変更は、広範な報告書利用者にとって関連する可能性が高い変更で構成される。そうした変更の開示には、変更が生じた日付や変更の前後でシステムがどのように変わったか等の適切な水準の詳細が含まれることが想定される。 システムへの重要な変更の例には以下が含まれる。 ・　提供される業務への変更 ・　ＩＴ及びセキュリティ関連要員に関する重要な変更 ・　システムのプロセス、ＩＴアーキテクチャ及びアプリケーション、並びに再受託会社が使用するプロセス及びシステムへの重要な変更 ・　システム要求事項に影響を与える可能性がある法規制上の要求事項への変更 ・　システムに係る内部統制の変更につながる組織構造への変更

記述規準	*実施ガイダンス*
	（法人組織に関する変更等）

経過措置ガイダンス

.20　本文書に提示している記述規準（2018 年版記述規準）は、SOC2®報告書において TSP セクション 100「*2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*」に定める 2017 年版 Trust サービス規準と併せて使用されるようデザインされている。2018 年版記述規準は、AICPA「*記述規準*」において DC セクション 200 として体系化されることになる。AICPA ガイド「*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)（セキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシーに関連する受託会社における内部統制に係る報告 (SOC2®)）*」（2015 年版記述規準）のパラグラフ 1.26-.27 に含まれる記述規準は、DC セクション 200A として体系化されることになる。

.21　受託会社のシステムに係る、2018 年 12 月 15 日以前の時点における記述書（タイプ 1 検証）又は 2018 年 12 月 15 日以前の時点で終了する期間についての記述書（タイプ 2 検証）を作成する際には、2018 年版記述規準又は 2015 年版記述規準にいずれかを使用できる（2015 年版記述規準を報告書利用者が入手できるよう、同規準は 2019 年 12 月 31 日まで DC セクション 200A に留まる。）。この移行期間において、経営者は記述書の中で 2018 年版記述規準又は 2015 年版記述規準のいずれを使用したかを特定すべきである。

.22　受託会社のシステムに係る、2018 年 12 月 16 日以後の時点における記述書（タイプ 1 検証）又は同日以後の時点で終了する期間についての記述書（タイプ 2 検証）を作成する際には、2018 年版記述規準を用いるべきである。

付録 – 用語集

.23　本文書の目的に関して、以下の用語は以下に与えられた意味を有する。

適用される Trust サービス規準：特定の検証の対象範囲に含まれる単一又は複数の Trust サービスのカテゴリーに関連する内部統制の評価に使用される、TSP セクション 100「*2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*」及び TSP セクション 100A「*Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*（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）」（AICPA「*Trust サービス規準*」）に体系化されている規準

取締役又は取締役会：受託会社の戦略的方向性を監督する責任と受託会社の説明責任に関連する義務を負う個人。そうした責任は受託会社の性質に応じて、企業では取締役会又は監査委員会、非営利組織では評議員会、行政サービス機関では理事会又は委員会、パートナーシップでは無限責任社員、小規模企業では所有者が負う場合がある。

システム境界：システム境界とは、受託会社の業務の提供に必要な受託会社のインフラストラクチャー、ソフトウェア、人員、手続及びデータの関連する側面である。複数の業務が側面、インフラストラクチャー、ソフトウェア、人員、手続及びデータを共有している場合、システムは重複するが、システム境界は異なる。機密保持又はプライバシー規準について取り上げるSOC2®業務において、システム境界は、最低限として、明確に定義されたプロセス及び非公式の臨時的な手続の範囲内での、機密及びパーソナル・インフォメーションのライフサイクルに関係する、全てのシステム構成要素を対象とする。

ビジネスパートナー：受託会社の事業上の取引に一定程度の関与を有する、若しくは何らかの程度において受託会社との協力に合意しているベンダーを除く個人又は会社（及びその従業員）（例えば、部品を供給する別の会社と協業しているコンピューター製造会社等）

除外方式：再受託会社により提供される業務を取り上げる手法で、受託会社に業務を提供する上で使用される再受託会社のシステムの構成要素は受託会社のシステム記述書及び検証の対象範囲から除外される。ただし、記述書では(1) 再受託会社により実施される業務の内容、(2) 受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、再受託会社において、受託会社における内部統制と組み合わせて実施されることが期待される必要な内部統制の種類及び(3) 再受託会社の内部統制の有効性をモニタリングするために受託会社が使用する内部統制が特定される。

相補的な再受託会社の内部統制：受託会社の経営者が、受託会社のシステムのデザインにおいて、再受託会社により実装されると想定する内部統制であって、受託会社のサービスコミットメント及びシステム要求事項を充足するという合理的な保証を提供するために、受託会社における内部統制と組み合わせて必要なもの

相補的な委託会社の内部統制：受託会社の経営者が、受託会社のシステムのデザインにおいて、委託会社により実装されると想定する内部統制であって、受託会社のサービスコミットメント及びシステム要求事項を充足するという合理的な保証を提供するために、受託会社における内部統制と組み合わせて必要なもの

受託会社における内部統制：受託会社におけるポリシーと手続であって、受託会社の内部統制システムの一部であるもの。内部統制は、５つの内部統制の構成要素（統制環境、リスク評価、統制活動、情報と伝達、モニタリング活動）のそれぞれの中に存在する。内部統制に係る受託会社のシステムの目的は、そのサービスコミットメント及びシステム要求事項が充足されるという合理的な保証を提供することにある。

再受託会社における内部統制：再受託会社におけるポリシー及び手続であって、受託会社による

そのサービスコミットメント及びシステム要求事項の充足に関連するもの

規準：主題の測定又は評価に用いられる標準

外部ユーザー：企業の人員以外のユーザーで、企業の経営者、顧客又は他の承認された者により企業の情報システムとのやり取りを承認された者

一体方式：再受託会社により提供される業務を取り上げる手法で、受託会社のシステムに係る記述書に、(*a*) 再受託会社により提供される業務の内容及び(*b*) 受託会社への業務の提供に使用される再受託会社のシステムの構成要素（受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社における内部統制と組み合わせて必要な再委託会社の内部統制を含む。）が含まれる（一体方式を使用する場合、再受託会社における内部統制は受託会社監査人の検証手続の対象となる。再受託会社のシステム構成要素は記述書に含まれるため、それらの構成要素は検証の対象範囲に含まれる。）。

情報ライフサイクル：明確に定義されたプロセス及び非公式の臨時的な手続の範囲内での、機密若しくはパーソナル・インフォメーションの収集、使用、保持、開示、処分又は匿名化

想定利用者：受託会社が報告書利用者として想定する個人又は企業

内部統制：業務、報告及びコンプライアンスに係る目的の達成に関する合理的な保証の提供を目的としてデザインされ、受託会社の取締役会、経営者その他の人員により実施されるプロセス

運用の有効性（又は有効に運用されている内部統制）内部統制が有効に運用され、適用される Trust サービス規準に基づく受託会社のサービスコミットメント及びシステム要求事項の充足について合理的な保証を提供すること

パーソナル・インフォメーション：特定可能な個人に関する又は関わりがある可能性がある情報

ポリシー：内部統制を有効化する上で何をすべきかに関する経営者又は取締役の声明。そうした声明は、文書化されるか、通信の中で明確に表明されるか、又はアクションや決定を通じて示唆される場合がある。ポリシーは手続の基礎となる。

プライバシー通知：パーソナル・インフォメーションを収集する企業により、パーソナル・インフォメーション収集の対象となった個人に宛てた通信文で、企業の(*a*) 収集する情報の内容及び当該情報の使用、開示、処分又は匿名化の方法に関するポリシー、並びに(*b*) そうしたポリシーの遵守へのコミットメントを説明するもの。プライバシー通知には、情報を収集する目

的、個人がパーソナル・インフォメーションに関して有する選択肢、そうした情報のセキュリティ、並びに個人が自身のパーソナル・インフォメーションに関する問い合わせや苦情及び紛争について企業に連絡を取る方法等の事項についての情報も含まれる。委託会社が個人からパーソナル・インフォメーションを収集する場合、通常、委託会社はそうした個人にプライバシー通知を提供する。

SOC2®報告書の報告利用者（指定利用者又は指定当事者）：本文書において、この用語はSOC2®報告書の利用者を意味する。SOC2®報告書に含まれる受託会社監査人の報告書には、通常、報告書の利用を、報告書を理解する上で受託会社及びシステムについての十分な知識と理解を有する特定当事者に限定する旨の注意書きが含まれる。期待される知識は、以下の事項に関する理解を含む可能性が高い。

- 受託会社により提供される業務の内容
- 受託会社のシステムが委託会社、ビジネスパートナー及び再受託会社その他の当事者とやり取りする方法
- 内部統制及びその限界
- 相補的な委託会社の内部統制及び相補的な再受託会社の内部統制、並びにそれらの内部統制が、受託会社のサービスコミットメント及びシステム要求事項を充足する上で、受託会社における内部統制とどのように相互作用するか。
- 委託会社の責任と、それが委託会社の、受託会社の業務を有効に利用する能力にどのように影響を与える可能性があるか。
- 適用されるTrustサービス規準
- 受託会社のサービスコミットメント及びシステム要求事項の充足を脅かすリスクと、そうしたリスクを管理する方法

そうした知識を有する可能性が高いユーザーには、受託会社のシステムが業務の提供に使用される方法を理解している委託会社及びその従業員、ビジネスパートナー及びその従業員、そうした委託業者及びビジネスパートナーに業務を提供する業務実施者、委託会社及びビジネスパートナーの候補並びに規制当局が含まれる。

受託会社監査人：本文書において、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関連する受託会社のシステム内の内部統制に係るSOC2®業務を実施するCPA。

サービスコミットメント：業務を提供するためのシステムについての、受託会社の経営者による委託会社その他（委託会社の顧客等）への宣言。サービスコミットメントは、個別化した契約書、標準化した契約、サービス品質保証（SLA）又は公式声明（例えば、セキュリティ実践に関する表明において）で伝達できる。

受託会社：委託会社に業務を提供する会社又は会社内のセグメント

SOC2®業務：(*a*) 受託会社のシステムに係る記述書が記述規準に基づいているか、(*b*) 受託会社のサービスコミットメント及びシステム要求事項が適用される Trust サービス規準に基づいて充足されることについて合理的な保証を提供する上で、内部統制が適切にデザインされているか、並びに(*c*) タイプ 2 報告書において、受託会社のサービスコミットメント及びシステム要求事項が適用する Trust サービス規準に基づいて充足されることについて合理的な保証を提供する上で、内部統制が有効に運用されているかに係る報告を目的とした検証業務。SOC2®業務は、証明基準及び AICPA ガイド「*SOC 2® Reporting on an Examination of Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*」に準拠して実施される。

後発事象：業務の対象である特定の期間の後であるが、受託会社監査人の報告書の日付よりも前に生じた事象又は取引であって、受託会社のシステムに係る記述書の表示の評価又はデザインの適切性及び内部統制の運用の有効性の評価に重大な影響を与える可能性のあるもの

再受託会社：受託会社が使用するベンダーで、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社の内部統制と組み合わせて必要な内部統制を実施するベンダー

デザインの適切性（又は適切にデザインされた内部統制）：内部統制は、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供する可能性がある場合、適切にデザインされている。適切にデザインされた内部統制は、内部統制を実施する上で必要な権限と能力を有する者により、デザインされた通りに運用される。

システム：会社の具体的な事業目的（業務の提供や商品の生産等）のうち一つ以上の目的を達成するために、経営者が指定した要件に従って、人々によりデザイン、実装及び運用されるインフラストラクチャー、ソフトウェア、手続及びデータ

システム構成要素：システムの個々の要素を意味し、インフラストラクチャー、ソフトウェア、人員、手続及びデータの５つのカテゴリーに分類できる。

システム事象：運用、業務、機能の消失又は中断につながる可能性があり、結果として受託会社がそのサービスコミットメント及びシステム要求事項を充足できなくなる可能性のある出来事。そうした出来事は、内部若しくは外部当事者による実際の未承認のアクセス、使用又はその試みによって生じる可能性があり、(*a*) 情報若しくはシステムの可用性、インテグリティ又は機密保持を毀損する（又は毀損する可能性がある）、(*b*) 情報その他の資産の不正な開示、盗難、データの破壊又は破損、又は(*c*) システムへの損害の原因となる可能性がある。そうした出来事は、さらにシステムがデータをデザイン通りに処理できないことや、システムが使用するデータの消失、破損又は破壊によって生じる可能性もある。

システムインシデント：システム事象のうち、受託会社によるサービスコミットメント及びシステム要求事項の充足への事象の影響を抑止又は軽減するために、受託会社の経営者の側でのアクションを必要とするもの

システム要求事項：(*a*)委託会社その他（委託会社の顧客等）に対する受託会社のサービスコミットメントの充足、(*b*)ベンダー及びビジネスパートナーに対する受託会社のサービスコミットメントの充足、(*c*)関連法令及び業界団体（事業者または同業者団体）の指針の遵守、及び(*d*)　記述書に取り上げられている Trust サービスカテゴリーに関連性のある他の受託会社の目的の達成のために、システムがどのように機能するべきかについての仕様。要求事項は、しばしば受託会社のシステムポリシーと手続、システム設計書類、顧客との契約及び政府規制で規定されている。

委託会社：受託会社によって提供される業務を利用する企業

ベンダー：受託会社への業務の提供に従事する個人又は事業者（及びその従業員）。ベンダーが提供する業務（例えば、受託会社のサービスコミットメント及びシステム要求事項が充足されることについて合理的な保証を提供するために、受託会社に代わって、受託会社における内部統制と組み合わせて特定の必要な内部統制を運用する場合）によっては、ベンダーは再受託会社でもある可能性がある。

以　上