KPMG

受託会社の内部統制に係る保証報告書の枠組み

～SOC1（ISAE3402/SSAE16/86号），SOC2（IT7号），
SOC3（SysTrust/WebTrust/IT2号）の
有効活用に向けて～

kpmg.com/jp

あずさ監査法人

はじめに

コアビジネスへの集中、コスト削減、新システムの迅速な開発といった取組みを進める中で、企業（委託会社）はシステム／ビジネスプロセス／データ処理の一部または全てを外部委託業者（受託会社）に委託することを選択し、その数は増加の一途を辿っています。その結果、委託会社は受託会社に対するモニタリングプロセスを構築し、受託会社に対してもリスク管理することが必要となりました。これまで多くの委託会社は、外部に委託した業務の評価のために「財務報告に関わる受託企業の内部統制に係る保証報告書」を利用してきました。しかしながら当該報告書は財務報告に関連するリスクに焦点を当てており、システムの可用性やセキュリティといった財務報告以外の目的には焦点が当てられていませんでした。そこで、米国では、2011年にSOC（Service Organization Controls：受託会社の内部統制）保証報告書の体系をSOC1、SOC2、SOC3の3種類に整理し、また日本ではSOC2に該当する基準として、2013年にIT7号[1]を公表しました。これにより、既存の財務報告に係る内部統制の報告書に加え、受託会社が提供する財務報告以外のサービスに係る内部統制に焦点を当てた保証報告書の提供が可能となり、委託会社のニーズにより広く対応することができるようになりました。

以下では、受託会社の内部統制に係る保証報告書（SOC報告書）の概要と主にSOC2/SOC3報告書の適用に関するガイダンスについて、トピックごとに説明を行います。なお、以下では、日本基準および国際基準における報告書も含めて、SOC1、SOC2、SOC3のカテゴリ区分で総括して説明を行っています。

1　日本公認会計士協会　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・機密保持に係る内部統制の保証報告書」

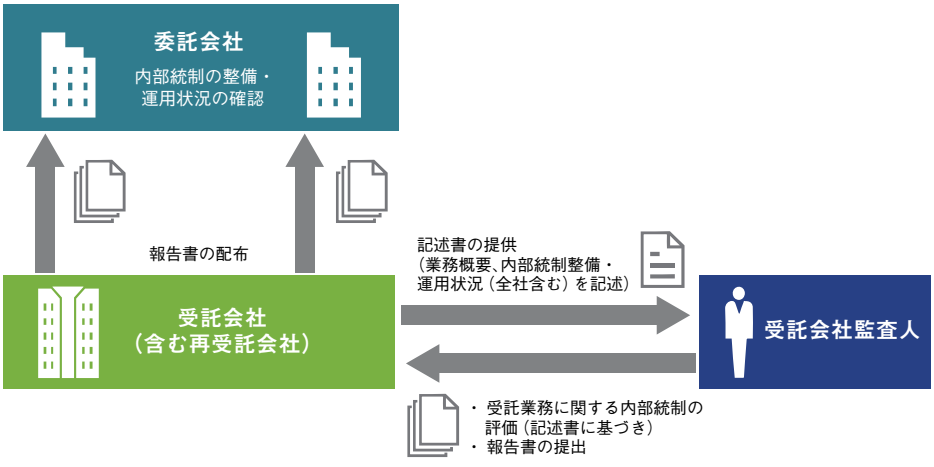
1. 受託会社の内部統制に係る保証報告書（SOC報告書）の概要

（1）　SOC報告書のフレームワーク

SOC報告書は、受託会社が外部に提供しているサービスに係る内部統制を対象とし、受託会社監査人が当該内部統制を評価し、その結果を委託会社等が利用する報告書であり、この業務は、監査法人が行う保証業務の1つとなります。

受託会社監査人は、受託会社が作成した受託業務に関する内部統制の状況を記載した記述書に基づいて、独立的な立場から、その記述が適性に表示されているか、内部統制が重要な点において適切にデザインされ・有効に運用されているかについて評価を行います。なお、監査法人等の意見表明は、財務諸表監査と同様に、合理的な保証となります。

図表1：SOC報告書のフレームワーク



（2）　SOC報告書の種類

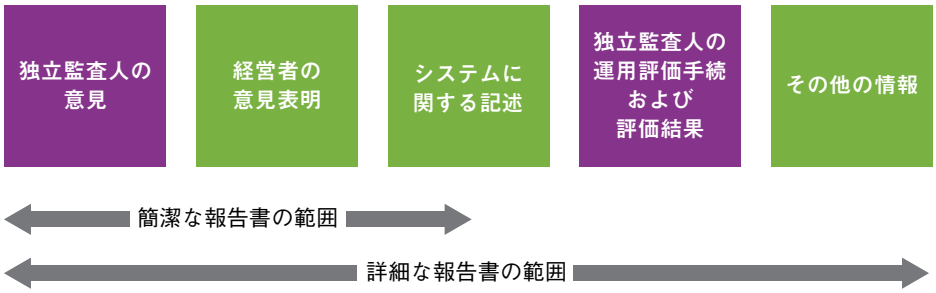
いわゆるSOC1にカテゴリされる受託会社の内部統制に係る保証報告書は、財務諸表監査に関して、委託会社とその監査人を支援することを目的としてきました。現在では、SOC2およびSOC3を加え3つのカテゴリに整理され、セキュリティ、プライバシー、可用性等の、広範囲にわたる委託会社ニーズに対応しています。このことによって、受託会社は自社の統制環境について、より目的にあった保証を受ける方法を検討できることになりました。

図表2：SOC報告書別の概要と適用場面

	財務報告に係る内部統制	財務報告に関連しない領域を含む内部統制	
	SOC1	SOC2	SOC3[2]
概要	委託会社と委託会社監査人のための詳細な報告書	委託会社と委託会社監査人と特定の関係者[3]のための詳細な報告書	一般に配布される簡潔な報告書
適用場面	• 財務報告に関するリスクと受託会社が特定した統制に焦点を当てている • 受託会社が財務取引処理または取引処理システムを支援している場合に、最も適している	• 以下に焦点を当てている - セキュリティ - 可用性 - 処理のインテグリティ - 機密保持 - プライバシー • 幅広いシステムに適している	
実務上の指針[4]	• 日本基準：86号 • 国際基準：ISAE3402 • 米国基準：SSAE16	• 日本基準：IT7号 • 国際基準：ISAE3000 • 米国基準：AT section 101	• 日本基準：IT2号 • 国際基準：ISAE3000 • 米国基準：AT section 101

2 Sys Trust/Web TrustのTrustサービスレポートおよびIT2号報告書がこの種類に該当する。
3 見込客（予定される利用者）、規制当局等を指す。
4 日本基準は、日本公認会計士協会の「監査・保証実務委員会実務指針第86号」、「IT委員会実務指針第7号」、または「IT委員会実務指針第2号」となる。
国際基準は、国際会計士連盟（IFAC）の国際保証業務基準を示している。
米国基準は、米国公認会計士協会の米国保証業務基準（Professional Standard含む）を示している。

図表3：SOC報告書概要イメージ（詳細は図表8を参照）



(3)　SOC報告書のタイプ

SOC報告書は、1年を通じて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、継続的に保証しており、財務報告またはガバナンスの観点からの委託会社の要求を満たしています。対象システムやサービスが通年で運用されない、年次での報告が委託会社のニーズに合致しない時など、場合によっては当該報告書の対象期間を6ヵ月間等に短くすることもあります。また、新システムや新サービスの一時点での評価、またはシステムやサービスの初期の評価のために、内部統制のデザインの適切性のみを対象とする場合もあります。

基準日時点でのデザインの適切性を保証する報告書が“Type1”であるのに対して、一定期間を通じてデザインの適切性と運用状況の有効性を保証する報告書は“Type2”と呼ばれます。例えば、委託会社がセキュリティと特定のシステムの可用性を対象とする一定期間を通じた報告書が必要な場合、受託会社に対してセキュリティおよび可用性を対象としたSOC2のType2報告書を依頼することになります。もし委託会社が特定のシステムの財務報告に係わる内部統制を対象とした報告書が必要な場合は、受託会社に対してSOC1のType2報告書を依頼することになります。

(4)　SOC報告書別の対象範囲の比較

下表ではSOC1とSOC2/SOC3のそれぞれについて、対象となる内部統制、システムに関する記述書の記載内容、対象とする統制項目および標準化のレベルの観点で比較しています。

図表4：SOC報告書別の対象範囲の比較

	SOC1	SOC2	SOC3
対象となる内部統制	財務報告に係る内部統制	財務報告に関連しない領域を含む内部統制	
システムに関する記述の記載内容	• 業務の種類 • 取引の開始から報告書に転記されるまでの手続 • 取引の開始から報告までに使用される会計記録、裏付け情報および特定の勘定 • 取引以外の重要な事象や状況への対応 • 委託会社へのレポート作成プロセス • 統制目的と関連する内部統制 • 委託会社の相補的な内部統制 • 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、情報システムと伝達、統制活動、監視活動	• 業務の種類 • システムの範囲 • システムの構成要素 - インフラ - ソフトウェア - 手続 - 人員 - データ • 重要な事象や状況への対応 • 委託会社へのレポート作成プロセス • 該当する原則と規準および関連する内部統制 • 委託会社の相補的な内部統制 • 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、情報システムと伝達、統制活動、監視活動	• 業務の種類 • システムの範囲 • 該当する原則と規準
対象とする統制項目	• 業務処理統制 • IT全般統制	• セキュリティ • 可用性 • 処理のインテグリティ • 機密保持 • プライバシー	
標準化のレベル	• 統制目的は受託会社により定義されます。 • 統制目的は、提供されるサービスの種類により異なります。	• 原則は受託会社により選定されます。 • あらかじめ定義された特定の基準が使用され、統制目的よりも、記載項目が標準化されています。	

(5)　SOC2/SOC3の原則

SOC2とSOC3は、財務報告に係る内部統制を超えた保証を提供するために米国公認会計士協会（AICPA）およびカナダ勅許会計士協会（CICA）が開発した「Trustサービス原則と規準[5]」を利用しています。

この原則および規準では、セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーの5つの原則が定義されています。モジュラー方式となっているため、受託会社と委託会社の要求により、原則を選択して、SOC2またはSOC3報告書に適用することができます。

一方で、SOC1報告書では受託会社に、システム記述書および統制目的とそれに関連する内部統制を定義することが求められています。SOC1報告書では一般的に、財務報告に係わる内部統制の観点から、委託会社の財務報告に関連しないサービスや内部統制を対象とすることはできません。また、災害復旧やプライバシーを評価対象とすることもできません。

図表5：Trustサービスの原則と適用領域

規準	Trustサービスの原則	適用領域
セキュリティ	• システムは（物理、論理双方の）未承認のアクセスに対して保護されている。	• 一般的に要求される基本的な規準です。 • セキュリティに関連する統制は他の統制の基礎となるため、セキュリティの規準は他の原則を包含します。 • セキュリティは委託会社にとって関心の高い領域であり、財務に関係する・しないに関わらず全ての受託会社のシステムに適用可能となります。
可用性	• システムは、コミットまたは合意したとおりに、操作でき、かつ、利用できる。	• セキュリティに次いで要求される規準です。特に標準サービスの一部として災害復旧が提供されている場合に選択します。 • 委託会社がSOC1報告書の一部として評価できない災害復旧だけでなく、システム可用性に関わるSLAを遵守するプロセスの保証が必要な場合にも選択します。
処理のインテグリティ	• システム処理は完全、正当、正確、適時かつ権限付与されている。	• 財務に関連する処理の有無を問わず、システム処理の完全性、正当性、正確性、適時性と承認への保証が必要な場合に選択します。
機密保持	• 機密として指定された情報が、コミットまたは合意したとおりに、保護されている。	• ビジネス上の機密データを保護するために受託会社の業務に関する追加的な保証を委託会社が要求する場合に選択します。
プライバシー	• パーソナル・インフォメーションは、企業のプライバシー通知におけるコミットメントおよび一般に公正妥当と認められるプライバシー原則を充足して、収集、利用、保持、開示および廃棄されている。	• 受託会社が直接エンドユーザとやりとりを行い、パーソナル・インフォメーションを収集する場合に選択します。 • プライバシー・プログラムの統制の有効性を証明する強固なメカニズムを提供します。 ＊日本でいう個人情報とは必ずしも一致しません。

5　Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

(6)　SOC2/SOC3の規準

Trustサービスの規準は、セキュリティ、可用性、処理のインテグリティおよび機密保持に共通する規準、可用性に関する追加規準、処理のインテグリティに関する追加規準、機密保持に関する追加規準、およびプライバシーに関する規準から構成されています。

セキュリティ原則から適用するのが最も実務的なアプローチです。セキュリティの原則はユーザーの関心が最も高い領域であり、他のTrustサービス原則における基礎にもなるため、可用性、処理のインテグリティおよび機密保持に共通する規準として構成されています。

このほかに、委託会社のニーズによって、Trustサービス基準以外であっても、主題情報として追加することができます。例えば、委託会社が金融機関の場合、受託会社に対して、金融検査マニュアルやFISC[6]の安全対策基準を主題情報として追加することを求めるかもしれません。

図表6：Trustサービスの規準

可用性に関する追加規準 (3)	処理のインテグリティに関する追加規準 (6)	機密保持に関する追加規準 (6)

セキュリティ、可用性、処理のインテグリティおよび機密保持に共通する規準 (28)
CC1.0　組織および管理に関する共通規準 (4)
CC2.0　コミュニケーションに関する共通規準 (6)
CC3.0　リスク管理および内部統制の設計と導入に関する共通規準 (3)
CC4.0　内部統制のモニタリングに関する共通規準 (1)
CC5.0　論理的および物理的アクセス管理に関する共通規準 (8)
CC6.0　システム運用に関する共通規準 (2)
CC7.0　変更管理に関する共通規準 (4)

プライバシーに関する原則と規準 (65)
1.0　管理の規準 (14)
2.0　通知の規準 (4)
3.0　選択と同意の規準 (6)
4.0　収集の規準 (6)
5.0　利用、保持および廃棄の規準 (4)
6.0　アクセスの規準 (7)
7.0　第三者への開示の規準 (6)
8.0　プライバシーのためのセキュリティの規準 (9)
9.0　品質の規準 (3)
10.0　モニタリングと是正措置の規準 (6)

*括弧内の数は項目数を表す。項目数は、各基準のカテゴリごとに示される個別の構成要素に定められた基準数（コントロールの例示が示されているもの）を示す。

プライバシー規準は、プライバシー・プログラムの有効性に関する保証として利用することができます。ただし、注意すべき点として、複数のサービスを提供し、地理的に多様なユーザーを持つ組織においてプライバシー規準は複雑な領域といえます。

よって、プライバシー規準を含むSOC2報告書の作成には、他の規準にもまして、入念な準備が必要です。

6　金融情報システムセンター　The Center for Financial Industry Information Systems

(7)　SOC 2とSOC3の相違点

SOC2とSOC3はどちらもTrustサービスの原則と規準を使用しており、また、受託会社監査人の作業もおおむね同様となります。

しかし、詳細まで記載されているSOC2報告書では、受託会社の内部統制や受託会社監査人の評価手続の結果等の詳しい記述が含まれますが、SOC3報告書では、サマリーレベルの情報のみとなるため、利用のニーズを考慮してその用途が分かれます。図表7では、主要な特徴について対比しています。

図表7：SOC2とSOC3の比較

	SOC2	SOC3
共通点	• 選択された規準に基づき、セキュリティ、可用性、機密性、処理のインテグリティ、プライバシーに関する詳細な評価が実施されます。 • システムに関する記述がSOC報告書に含まれます。	• 経営者による受託会社確認書がSOC報告書に含まれます。 • 再受託会社を利用している場合、受託会社は再受託会社のオペレーションをモニタリングするコントロールを含めることになります。
相違点	• SOC2は、再受託会社によって提供されるサービスについて除外すること[7]（Carve-out）を認めており、SOC3と比べ柔軟性があります。 • SOC2には、受託会社の詳細な内部統制の記述、監査人の監査手続と結果が含まれているため、利用者がより詳細に受託会社の評価を行うことを可能にします。	• SOC3では、受託会社の内部統制の詳細な記述、監査人の監査手続を求めない利用者に対して、受託会社がTrustサービス基準を達成したかどうかの概括的な結論のみを提供できます。
潜在的な弱点	• 利用者はより確かな保証を得るためには、重要な再受託会社から、その活動に関する追加のSOC報告書を入手しなければならない場合があります。 • 利用者は、概括的な結論ではなく詳細な報告書（内部統制、監査手続等）を確認できることを望んでいない場合も想定されます。 • 受託会社は、機密情報（セキュリティコントロールの詳細等）の開示に関しての懸念から、詳細な報告書の提供を望まない場合があります。	• SOC3は、重要な再受託会社の活動に関して除外すること（Carve-out）を認めていません。そのため、再受託会社の活動が、受託会社の評価手続に含まれない場合、SOC3を選択することはできません。

7　除外方式（Carve-out）除外方式では、受託会社のシステム記述書に受託会社が再受託会社に再委託している業務内容を記載するが、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記述書および受託会社監査人の評価範囲から除外される。

(8)　SOC報告書の構成

図表8は、SOC報告書の構造と内容を比較・対照しています。SOC1およびSOC2はどちらも詳細な報告書であり、報告書の構成内容は類似しています。

これらの報告書は、特定の基準日時点（Type1）と特定の期間を通じたデザインの適切性と運用状況の有効性（Type2）のどちらも対象とすることができます。

図表8：報告書の構成内容

項目		SOC 1	SOC2	SOC3
独立監査人の意見		独立監査人の立場として意見表明を行います。		
経営者の意見表明		経営者の意見表明として、「受託会社確認書」が作成されます。		経営者の意見表明として「経営者の記述書」が作成されます。
システムに関する記述	記述方法	システムに関する記述書に、受託会社の概要、サービス概要、詳細な内部統制の状況等が記述されます。		「経営者の記述書」に内部統制を含めて簡略的に記載されます。
	統制目的／評価規準	システムに関する記述書に、設定された財務報告に係る統制目的が記載されます。	システムに関する記述書に、評価規準の個別内容が記載されます。	「経営者の記述書」に準拠する規準名称が示されます。
独立監査人の運用評価手続および評価結果		運用状況の有効性の評価および評価結果が記載されます*。		該当事項なし
その他の情報		その他の情報（該当する場合）		該当事項なし

*注記: Type 2の報告書のみに適用される。

図表9：SOC1およびSOC2報告書の監査人の評価手続および評価結果のイメージ

SOC1

統制目的1：XXXXXXXX

内部統制	評価手続	評価結果
XXXXX	・XXXXXX ・XXXXXX	XXXXX
XXXXX	・XXXXXX ・XXXXXX	XXXXX

統制目的2：XXXXXXXX

内部統制	評価手続	評価結果
XXXXX	・XXXXXX ・XXXXXX	XXXXX
XXXXX	・XXXXXX ・XXXXXX	XXXXX

統制目的3：XXXXXXXX

内部統制	評価手続	評価結果
XXXXX	・XXXXXX ・XXXXXX	XXXXX
XXXXX	・XXXXXX ・XXXXXX	XXXXX

SOC2

セキュリティの原則：システムは（物理、論理双方の）未承認のアクセスに対して保護されている。

CC1.0 組織および管理に関する共通規準

規準	内部統制	評価手続	評価結果
XXXXX	XXXXX	・XXXXXX ・XXXXXX	XXXXX

CC2.0 コミュニケーションに関する共通規準

規準	内部統制	評価手続	評価結果
XXXXX	XXXXX	・XXXXXX ・XXXXXX	XXXXX

CC3.0 リスク管理および内部統制の設計と導入に関する共通規準

規準	内部統制	評価手続	評価結果
XXXXX	XXXXX	・XXXXXX ・XXXXXX	XXXXX

CC4.0 内部統制のモニタリングに関する共通規準

規準	内部統制	評価手続	評価結果
XXXXX	XXXXX	・XXXXXX ・XXXXXX	XXXXX

2. SOC2/SOC3報告書の適用に関するガイダンス

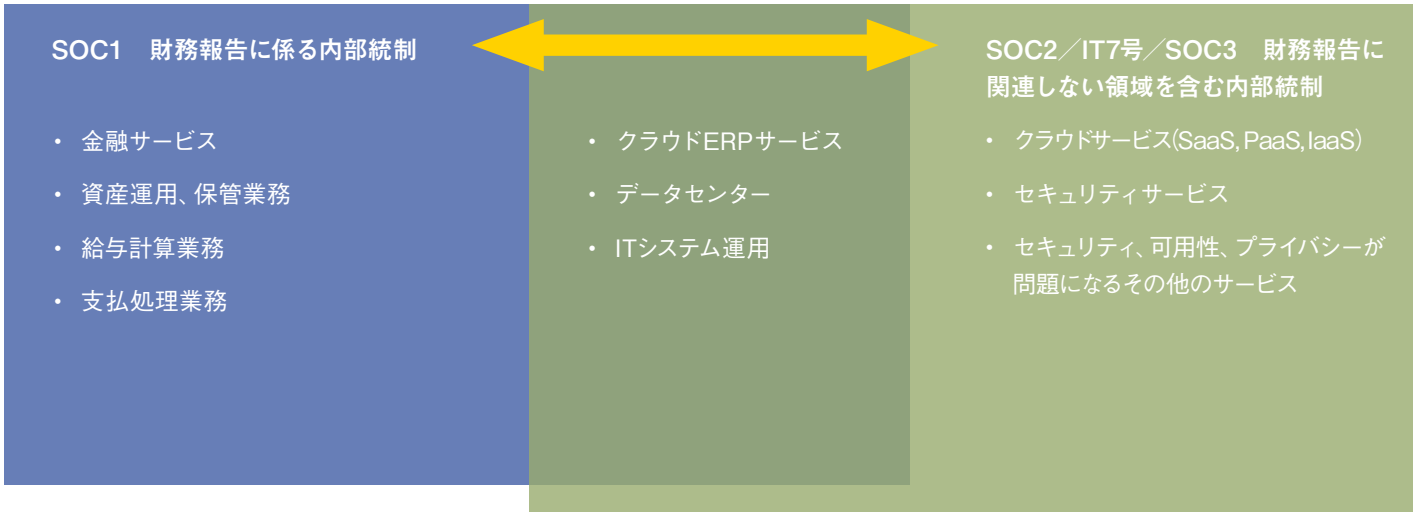
(1)　コントロールとサービスによる報告書の選択

図表10は、コントロールとサービスにおいて、どの種類の報告書が適切かについて、参考情報としてまとめたものです。図表10において左端にあるのは、財務報告関連サービスであり、委託会社のニーズとして、SOC1報告書が求められる領域です。これらについて対象となる受託会社のサービスについては、例えば、財務サービス、保険給付支払、給与計算と給与支払等の処理が挙げられます。

また、委託会社にとってセキュリティ、可用性に関する詳細な情報が必要なケースがあります。その場合、受託会社は財務報告に係る内部統制のためにSOC1報告書を提供している場合でも、委託会社によるセキュリティ監査に対応するための要求が高いなどで、セキュリティ・可用性に関する保証の提供が必要な場合、SOC2/SOC3報告書が利用されます。

図表10の中央にある領域は、上記の2つのカテゴリに明確に分類できないサービスであり、提供されるサービスの性質と委託会社のニーズにより、SOC1またはSOC2、ないしは両方が適している領域になります。

図表10：各報告書の対象領域



- **クラウドERPサービス**は、委託会社に対して重要な財務報告に係るサービスを提供している場合、SOC1報告書（IASE3402/SSAE16/86号報告書）を提供しています。しかし、クラウドサービスを利用する委託会社のニーズにより、セキュリティ・可用性に関するSOC2またはSOC3報告書を提供する必要があるかもしれません。
- **データセンター（コロケーション）**の提供者は、物理的・環境的なセキュリティに限定したSOC報告書の提供を行ってきました。しかし、ほとんどのデータセンターは、委託会社の財務に関連するシステム以外のサーバも運用しています。その結果、一部のデータセンターはセキュリティを対象としたSOC2報告書へと移行を始めているほか、サービスの性質によって可用性の原則を追加しています。
- **ITシステム運用**は、一連の顧客に対して一般的なITサービスを提供することもあれば、特定の顧客に対してカスタマイズされたサービス提供することがあり、委託会社の保証報告書のニーズが財務報告に係る内部統制監査なのか、セキュリティ／可用性なのかによって、SOC1/SOC2報告書を選択する必要があります。

極端な例では、運用に関する技術に特化したサービスで、ユーザーの財務報告に係る内部統制に直接的な関係がないか、間接的な関係しかないサービスがあります。

例えば、これらの外部委託されたサービスは、上場企業の内部統制監査のスコープに含まれることはないとします。当該サービスの委託会社は一般的にデータのセキュリティ、システムの可用性にもっとも関心があり、それに対してはセキュリティと可用性を対象とするSOC2、SOC3報告書により対応することができます。また、適切な場合、SOC2/SOC3報告書は処理のインテグリティ、機密保持のほか、プライバシーも同様にカバーすることができます。さらにSOC2は、第三者の機密データを保管、処理するすべての組織に対して適用できる可能性があります。

情報を保護するために、効果的なセキュリティ・機密保持のコントロールが存在することを、第三者に対して証明したいとき、SOC2/SOC3は有用となります。報告書のシステム記述を通じて、受託会社はシステムの境界を明確に記述することができ、そしてあらかじめ定められたTrustサービスの規準に基づいた評価が行われます。

(2)　委託会社がSOC2/SOC3を採用する際の進め方

委託会社は、リスクマネジメントやビジネスの観点から、主要なベンダーがもつ自社に対する影響、SOC2/SOC3報告書を入手することによる利益を検討する必要があります。主要なアクティビティは次のようなものです。

図表11：導入にあたっての主要なアクティビティ

主要なアクティビティ	説明
ベンダーとの関係のリストアップ	• 使用しているベンダーについて、どのような業務を委託しているか、将来保証報告書を必要とするかといった関係を整理し、リスト化します。
ベンダーのリスク評価	• 重要なベンダーに関連する自社の主要なリスクを評価します。（例えば、セキュリティ、可用性、他のリスク）
関連するレポートの識別	• 過去、SOC報告書やその他報告書を入手しているか確認します。 • 今後、SOC1報告書を入手すべきか検討します。 • 重要なベンダーについて、SOC2報告書とSOC3報告書のどちらを要求すべきか、検討します。同様に、SOC2/SOC3報告書において、どの原則（例えば、セキュリティ、可用性、または他の原則）がカバーされるべきか、検討します。
契約上の条項	• 契約により、特殊な監査報告書を要求しているか確認します。また、監査権があるかについても確認します。 • 契約によりSOC2/SOC3報告書を要求すべきか検討します。

主要なアクティビティ	説明
ベンダーモニタリング	• 重要なベンダーの評価頻度を検討します。 • SOC報告書の入手と評価、懸念事項に関する対応を含めたベンダーモニタリングプロセスを構築します。
ベンダー評価	• ベンダーの評価プロセスの一部として、関連するSOC報告書の入手を要求するか検討します。
コミュニケーション計画	• 報告書の利用が望ましい場合、ベンダーに報告すべき主な論点は以下となります。 - カバーされているシステム（記述）の範囲 - 提供されている報告書の種類（SOC1,SOC2/SOC3) - 提供されている報告書のTypeと基準日または評価期間 - カバーしている統制項目 （SOC1：統制目的、SOC2/SOC3：原則と規準） - 再受託会社の有無 - 報告書の提供時期

(3)　委託会社による保証報告書の評価時における主要な観点

委託会社は受託会社から入手した保証報告書を評価する際に、以下の項目について確認する必要があります。

図表12：報告書入手時の確認項目

項目	確認内容
報告書の種類	• 入手した報告書がSOC1、SOC2、SOC3、それ以外の報告書のいずれかを確認する。
評価対象期間	• 入手した報告書がType1、Type2かを確かめ、基準日または評価対象期間が自らの評価すべき期間と合っているかを確認する。
意見	• 受託会社が受けている意見が適性意見なのか、限定意見なのかを確認する。 • 限定意見に対する影響を検討する。
受託会社監査人	• 受託会社監査人が報告書を提供するに足る評判・能力を有しているか確認する。
範囲	• 評価したい業務、場所が報告書の範囲に含まれているかどうか、システム記述書および意見の内容から確認する。
再受託会社	• 再受託会社の有無、再受託会社がある場合に、一体方式[8]（Inclusive）か除外方式[9]（Carve-out）かを、システム記述書および意見の内容から確認する。
規準、統制目的	• 入手した報告書がSOC1ならば統制目的、SOC2/SOC3ならば選択された原則と規準が、自らの利用目的・要求とあっているか確認する。
委託会社の相補的な内部統制	• 識別された委託会社の相補的な内部統制を通読し、自社に適用可能な手続が存在しているか確認する。
統制活動の記述	• SOC1およびSOC2の場合、統制活動の記述内容を通読し、記載レベルが十分に理解できるレベルとなっているか確認する。
評価手続	• SOC1およびSOC2の場合、受託会社監査人の評価手続を通読し、十分な評価手続が実施されているか確認する。
評価結果	• SOC1およびSOC2の場合、もし例外事項があれば、例外事項の内容と会社の回答を通読し、自社における影響と追加手続の必要性について検討する。
対象期間中の変更	• システム、再受託会社および統制の重要な変更の有無と変更による自社への影響を検討する。

8　一体方式（Inclusive）受託会社のシステム記述書に受託会社が再受託会社に再委託している業務内容を記載され、かつ、再受託会社の該当する原則とその規準および関連する内部統制は、受託会社のシステム記述書および受託会社監査人の評価範囲に含まれる。

9　4と同じ。

(4)　受託会社がSOC2/SOC3を採用する際の進め方

SOC2/SOC3報告書に対する市場認知の高まりにより、委託会社は保証報告書に対する自身のニーズを見極め、契約条項の変更を検討し、受託会社のリスク管理プロセスを強化するために、契約更新の際にそれらの要求事項について受託会社に交渉を求めることが想定されます。多くの業界内の会議や、クライアントとの議論によれば、委託会社がセキュリティ／可用性／プライバシーについて関心をもっている状況において、SOC2/SOC3報告書に対する肯定的な反応が見られています。よって、受託会社はSOC2/SOC3報告書に対する委託会社のニーズを検討し、必要に応じてSOC2/SOC3へ移行／提供するための計画を進めることが重要です。

SOC2/SOC3報告書に対応するための主なトピックは、以下の通りです。

図表13：移行／提供にあたっての検討事項

トピック	検討内容
現在の要求事項のリスト化	• 過去に保証報告書を提供したことのある委託会社をリストアップします。 • 保証報告書の提供を定めた契約をリストアップします。 • 委託会社または見込客からの最近の要求事項についてリストアップします（例：セキュリティ質問書への対応 等）。
今後の要求事項の決定	• 委託会社または見込客の要望として、財務目的とガバナンス／オペレーション評価／セキュリティ目的のいずれの要望が強いのか検討します。 • 現在提供中のサービス、計画中のサービスの組み合わせと、それらに関連づけられる委託会社のリスクを評価します。 • 委託会社や、見込客の要望に最も適した報告書の種類を決めます。
新しい基準への対応	• ISAE3402/SOC1報告書に対する要求事項を確認するため、既存報告書の範囲を再評価します。 • SOC2へ移行する報告書については、どの原則を選択すべきか検討します。 • 識別された統制（過去のSOC1報告書、あるいはその他の統制に関するドキュメントを参照して）から、SOC2/SOC3の要求へ対応付けを行い、ギャップを識別します。 • ギャップ分析の結果に基づき、SOC2/SOC3提供のためのスケジュールを決めます。例えば、セキュリティについては当年度に対応し、他の原則については翌年以降に遅らせることが有意義なケースがあります。 • 識別されたギャップに対応するための計画を作り、正式なSOC2/SOC3評価の準備をします。
コミュニケーションの計画	• 主要な委託会社へ、当年度の報告書提供に関する計画を伝達するための計画を定めます。 • FAQ／論点のリストを作成し、社内の関連部署（顧客サービス、営業、マーケティング、IT、他）が自社の提供計画を説明し、委託会社からの質問に効果的に答えることができるようにします。

(5)　受託会社へ提供するサービス

これまでに監査を受けたことがない受託会社にとって、報告書を提供するためには「SOC2/SOC3の準備を進める」、「評価を完了させる」の、2段階のプロセスがあります。図表14には、初めて報告書を取得する受託会社向けてKPMGが提供するサービス内容をまとめています。KPMGは、はじめに事前診断サービスを提供します。事前診断サービスでは、受託会社と協力し、評価のための準備に必要なサポートを提供します。評価サービスは、事前診断サービスで確立した受託会社のアーキテクチャや内部統制への理解を前提として、効率的に実施します。

図表14：受託会社へ提供するサービス

事前診断サービス

- 評価の範囲と、全体のプロジェクトタイムラインの決定を支援します。
- 経営者とのディスカッション、あるいは、ドキュメントのレビューを通じた既存、または必要な統制を理解します。
- 事前レビューを実施し、経営者の注意が必要なギャップを識別します。
- 識別されたギャップに対応するため、優先付けされた対応方法の検討を支援します。
- 打合せを通じて、代替案や、改善計画について助言します。
- 正式な評価が始まる前に、ギャップが解消されたことを確認します。
- 受託会社への外部からの要求に答えるため、もっとも効果的な評価、報告の方針の決定を支援します。

評価サービス

- 全体的な評価計画を提示します。
- 評価プロセスを効率的に進めるため、現地作業の前に事前確認を実施します。
- 現地のヒアリングや評価手続を実施します。
- 収集した情報に対してオフサイトで分析を実施します。
- 進捗状況や、論点があれば報告します。
- 経営者によるレビューのための報告書のドラフト、最終報告書を提供します。
- 経営者向け／内部向けに、所見や要検討事項を含んだ報告を実施します。

3. まとめ

受託会社のサービスを利用する多くの委託会社がSOC1報告書を依頼しています。SAS70報告書[10]／18号[11]報告書を利用していた当時は、当該報告書の目的が「委託会社や委託会社監査人が、委託会社の財務諸表監査や内部統制監査において、受託会社の内部統制に依拠するため」と知りつつも、セキュリティ、可用性、プライバシーといった領域に関心を持った委託会社は、受託会社に対して、SAS70報告書／18号報告書を要求してきました。

2011年、SAS70報告書／18号報告書がSOC1報告書へ移行したことに伴い、新たにこれらの領域をサポートするSOC2/IT7号、SOC3報告書が登場し、委託会社は自らの目的に合わせて報告書を選択することが可能となりました。

例えば、基幹となる財務報告サービス（給与計算、トランザクション処理、資産管理、他）を提供する受託会社は、SOC1報告書を提供しています。財務報告システムに直接的な影響がない、あるいは間接的な影響しかないITサービスプロバイダーは、SOC2報告書の提供を始めています。SOC3報告書は、幅広いユーザーに対して、詳細な統制内容や、テスト結果を開示せずに保証のレベルを伝えるために使われています。いくつかの会社は、異なる顧客層に適合するため、SOC2/SOC3を統合した評価を受けて2つの報告書を用意するかもしれません。

SOC報告書は、サービスが財務報告に関連する・しないにかかわらず、幅広く保証可能となり、委託会社と受託会社の間をより良く繋ぐツールとなりました。これらの報告書を適切に選択し利用することは、実務的にも国際的にも認識されたソリューションであり、貴社の継続的な成長を支えるものとなります。

10 米国公認会計士協会（AICPA）の米国監査基準書第70号 Statement on Auditing Standard No.70

11 日本公認会計士協会の監査基準委員会報告第18号「委託業務に係る統制リスクの評価」

有限責任 あずさ監査法人
東京事務所 IT監査部

TEL:03-3548-5315

パートナー
河西　正之
masayuki.kawanishi@jp.kpmg.com

パートナー
小松　博明
hiroaki.komatsu@jp.kpmg.com

マネジャー
鈴木　雅之
masayuki.b.suzuki@jp.kpmg.com

kpmg.com/jp