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

2022年12月28日

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適合するTrustサービス原則、規準及びその例示の2016年版を更新した、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サービス規準である。

Copyright©:2017年　米国公認会計士協会(AICPA)及びカナダ勅許職業会計士協会(CPA Canada) 無断複写複製を禁ずる。

複製は個人的、組織内部用途、又は、教育的な使用にのみ認められる。複製は下記の文言を付さなければ販売、配布、提供してはならない。
“Copyright© 2017 by American Institute of Certified Public Accountants, Inc. and Chartered Professional Accountants of Canada (CPA Canada).Used with permission.”

本「Trustサービス規準」は、AICPA及びCPA Canadaの知的財産である「TSP Section 100 － 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy」を、日本公認会計士協会が日本語に翻訳したものである。
AICPA及びCPA Canadaの文書について、承認された正文は英文である。AICPA及びCPA Canadaは当日本語訳をレビューしておらず内容に関する意見を表明していない。

本「Trustサービス規準」に記載されている規準のうち「Internal Control－Integrated Framework (COSO framework)」より引用された英文の日本語訳は、「COSO内部統制の統合的フレームワーク」(八田進二、箱田順哉監訳、日本内部統制研究学会新COSO研究会訳、日本公認会計士協会出版局発行)から翻訳者の了解を得て引用している。

(訳者注：本翻訳を作成するに当たり、“management”は「経営者」と翻訳している。利用に際しては、組織の規模、形態や管理手法に応じて、業務実施者が適切に読み替えることを期待する。また、“personal information”を「個人情報」とはせずに「パーソナル・インフォメーション」と表記している。これは、AICPAが「Trust サービス原則と規準」を米国、カナダやEU等のプライバシーに関する法令や実務等を参考に作成しており、“personal information”が日本における「個人情報」とは異なる可能性があるため、上記の表記とした。)

目　次

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

読者へ

「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」は、証明業務又はコンサルティング業務において、(a)全社横断的に、(b)子会社、部門又は活動単位のレベルにおいて、(c)組織の運営、報告又はコンプライアンス上の目的に関連する機能に含まれ、又は、(d)組織が使用する特定の種類の情報に対する、情報及びシステムに関するセキュリティ、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係る内部統制を評価し、報告する際に使用できるように、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（ASEC）が策定した内部統制の規準を示している。ASEC は、これらの規準の策定と開発に当たって、一般にコメントを募るための規準案の公開を含むデュープロセスの手続に従った。BL セクション 360、委員会（AICPA、職業的基準）に基づき、ASEC は上級委員会に指定されており、また、AICPA 審議会又は理事会の許可なしに公式声明を行い、測定規準を公表する権限を与えられている。

背景

１．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（ASEC）は、組織、組織の部署又は活動単位において、情報及びシステムのセキュリティ、可用性若しくは処理のインテグリティ、又はシステムによって処理される情報の機密保持若しくはプライバシーに関連する内部統制のデザインの適切性と運用の有効性を評価する際に使用される一連の規準（Trust サービス規準）を開発した。さらに、Trust サービス規準は、組織の一つ若しくは複数のシステム又は組織内部の特定の機能を支援するために用いられる一つ若しくは複数のシステムによって処理される、特定の種類の情報のセキュリティ、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内部統制のデザインと運用の有効性を評価する際に使用される可能性がある。本書は Trust サービス規準を示している。

２．どの内部統制システムでもそうであるように、組織は Trust サービス規準を満たす能力を脅かすリスクに直面する。そのようなリスクは、以下のような要因によって生じる。

- 組織の事業の種類
- 事業運営の環境
- 組織が生成、使用、保存する情報の種類
- 顧客その他の第三者に対して行うコミットメントの種類
- 組織のシステムとプロセスの運用及び維持に伴う責任

・　組織が使用するテクノロジー、接続の種類及び配信チャネル

組織は、有効に運用されている場合に、組織目的の達成の合理的な保証を提供する、適切にデザインされた内部統制の導入を通じて、これらのリスクに対処する。

3．Trust サービス規準を実際の状況に適用するに当たっては判断が求められる。そのため、本書では、Trust サービス規準に加えて、各規準の着眼点も示している。トレッドウェイ委員会支援組織委員会（COSO）は、「内部統制の統合的フレームワーク」（COSO フレームワーク）[1]の中で、着眼点は原則の重要な特性を表していると説明している。COSO フレームワークと同様、本書の着眼点は、経営者が、セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る内部統制をデザイン、導入及び運用するに当たって、役に立つ可能性がある。さらに、これらの着眼点は、経営者と業務実施者が、内部統制が Trust サービス規準を満たすように適切にデザインされ、有効に運用されたかどうかを評価するに当たって、役に立つ可能性がある。

4．着眼点によっては、組織又は実施する業務に適合しない、又は関係しないかもしれない。そのような場合、経営者は特定の着眼点をカスタマイズし、又は組織の具体的な状況に基づき他の特徴を特定し、考慮に含めてもよい。Trust サービス規準の使用によって、各着眼点が対処されているかどうかの判定が必要となるわけではない。使用者は、Trust サービス規準を適用するに当たって、実際の状態の中で組織とその環境に関する事実及び状況を慎重に検討すべきである。

Trust サービス規準の構成

5．本書に示す Trust サービス規準は、COSO の「内部統制の統合的フレームワーク」（2013 年改訂版）の中で示されている 17 の規準（原則として知られる）に合わせて調整されたものである。Trust サービス規準には、これらの 17 の原則に加えて、COSO 原則 12「組織は、期待されていることを明確にした方針および方針を実行するための手続を通じて、統制活動を展開する。」を補完する追加規準が含まれている（補足規準）。補足規準は、業務に関連する組織の目的の達成に適用される規準であり、以下のものから構成される。

・　論理的及び物理的アクセス管理：組織が論理的及び物理的なシステムへのアクセスを制限し、これらのアクセス権を付与及び削除し、未承認のアクセスを防ぐことに関連する規準
・　システム運用：組織がシステムの運用を管理し、論理的及び物理的なセキュリティの逸脱を含む、処理の逸脱を検出し、緩和することに関連する規準
・　変更管理：組織が、システム変更の必要性を識別し、統制された変更管理プロ

[1] ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

セスを使用して変更を行い、未承認の変更を防止することに関連する規準
- リスク軽減策：組織が、ビジネスが中断するおそれ及びベンダーやビジネス・パートナーの使用から生じるリスク軽減活動を識別し、選択し、開発することに関連する規準

6．COSO フレームワークに含まれる 17 の原則に加えて、一部の補足規準は、Trust サービスのカテゴリー（「Trust サービスのカテゴリー」セクションを参照）全てに共通する。例えば、論理的アクセスに関連する規準は、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カテゴリーに適用される。その結果、Trust サービス規準は、以下の規準から構成される。
- Trust サービスの五つのカテゴリー全てに共通する規準（共通規準）
- 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カテゴリーに係る特定の追加規準

7．セキュリティについては、共通規準だけで完全な１組の規準が構成される。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ついては、完全な１組の規準は、共通規準と業務の対象となる特定の Trust サービスの一つ以上のカテゴリーに適用される規準から構成される。業務の対象となる Trust サービスのカテゴリーに係る規準は、そのカテゴリーに関連する全ての規準が業務によって対象とされる場合にのみ、完全であると考えられる。

8．業務実施者は、Trust サービスのカテゴリー（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）を、単独で若しくは一つ又は複数の他の Trust サービスのカテゴリーと組み合わせて報告することができる。業務の対象となるカテゴリーについては、通常は、そのカテゴリーに係る全ての規準に対処する必要がある。しかし、業務の範囲があるシステムに関する報告であり、受託会社が提供するサービスに特定の規準が関連しない場合のような限られた状況において、一つ又は複数の規準を業務に適用できない可能性がある。そのような状況においては、一つ又は複数の規準に対処する必要はない。例えば、受託会社のシステムのプライバシーに関して報告する場合、規準 P3.1「パーソナル・インフォメーションは、プライバシーに関する組織の目的に沿って収集される。」は、データ主体（本人）からパーソナル・インフォメーションを直接に収集しない受託会社には適用されない。さらに、共通規準は、業務範囲に含まれている Trust サービスのカテゴリーを問わず、適用しなくてはならない。

Trust サービスのカテゴリー

9．パラグラフ 24 の表には、Trust サービス規準とそれに関連する着眼点が示されている。その表において、Trust サービス規準は、以下のカテゴリーに分類されて

いる。

a. セキュリティ：情報及びシステムは、未承認のアクセス、未承認の情報の開示、情報又はシステムの可用性、インテグリティ、機密保持及びプライバシーを損ない、組織がその目的を達成するための能力に影響を与えるおそれのあるシステムのダメージに対して保護されている。

セキュリティとは、次の保護をいう。

i. 情報の収集又は生成、使用、処理、送信及び保管中における情報の保護

ii. 組織がその目的を達成できるように電子情報を用いて情報を処理、送信又は移動及び格納するシステムの保護。セキュリティに係る内部統制は、職務の分離の無効化と回避、システム障害、不正確な処理、データ又はシステム資源の窃取や不正な持ち出し、ソフトウェアの不正使用及び情報への不適切なアクセス、使用、変更、破棄や開示を予防又は発見する。

b. 可用性：情報及びシステムは組織の目的を達成するように操作でき、かつ、使用できる。

可用性とは、組織のシステム及び顧客に提供する製品又はサービスが使用する情報のアクセシビリティをいう。可用性の目的は、それ自体では、最小限受容できるパフォーマンスレベルを設定するものではない。可用性の目的は、システム機能性（システムが実施する特定の機能）やシステム・ユーザビリティ（特定のタスク又は問題の処理にシステムの機能を適用するユーザーの能力）は扱わないが、システムが運用、モニタリング及び維持のためのアクセシビリティを支援する内部統制を含むかどうかを取り扱う。

c. 処理のインテグリティ：システム処理は、組織の目的を達成するように、完全、正当、正確、適時であり、かつ、承認されている。

処理のインテグリティとは、システム処理の完全性、正当性、正確性、適時性と承認をいう。処理のインテグリティは、システムが、それ自体が存在する目標や目的を達成すること、そして、誤謬、遅延、脱漏及び未承認や不注意な操作から解放されて、意図された機能を損なわれないように実行できることを取り扱う。組織が多数のシステムを使用することを理由として、処理のインテグリティは通常、システム又は組織の機能レベルにおいてのみ取り扱う。

d. 機密保持：機密とされた情報が、組織の目的を達成するように、保護されている。

機密保持は、経営者の目的に従って、機密とされた情報を、収集又は生成から最終的に廃棄又は組織の管理から除外されるまで保護する組織の能力を取り扱う。情報の管理者（例えば、情報を保持又は格納する組織）がそのアクセス、使用及び保持を制限し、開示を限定された当事者（システムの境界内でアクセスを許可されている者を含む。）に限定する必要がある場合、情報は機密とされる。機

密保持の要求事項は、法令又は顧客その他に対して行われるコミットメントを含む契約や合意に含まれる可能性がある。情報を機密とする必要性は、多くの様々な理由に起因する。例えば、組織の担当者のみを対象とする専有情報が挙げられる。

プライバシーはパーソナル・インフォメーションにのみ適用され、機密保持は様々な機微情報に適用されるという点で、機密保持とプライバシーは区別される。さらに、プライバシーの目的は、パーソナル・インフォメーションの収集、使用、保持、開示、廃棄に関する要求事項に対応している。機密情報には、パーソナル・インフォメーションのみならず、営業秘密や知的財産などのその他の情報が含まれる場合がある。

e. プライバシー：パーソナル・インフォメーションが、組織の目的を達成するように、収集、使用、保持、開示及び廃棄されている。

機密保持は様々な種類の機微情報に適用される一方で、プライバシーはパーソナル・インフォメーションだけに適用される

プライバシー規準の構成は、以下のとおりである。

i. 目的の通知及び伝達：組織は、プライバシーに関連する組織の目的について、データ主体（本人）に通知する。

ii. 選択と同意：組織は、パーソナル・インフォメーションの収集、使用、保持、開示及び廃棄に関する可能な選択を、データ主体（本人）に伝達する。

iii. 収集：組織は、プライバシーに関連する組織の目的を達成するように、パーソナル・インフォメーションを収集する。

iv. 使用、保持及び廃棄：組織は、プライバシーに関連する組織の目的を達成するように、パーソナル・インフォメーションの使用、保持及び破棄を制限する。

v. アクセス：組織は、プライバシーに関連する組織の目的を達成するように、データ主体（本人）が自身のパーソナル・インフォメーションを確認及び訂正（更新を含む。）できるように、データ主体（本人）にアクセス権を付与している。

vi. 開示及び通知：組織は、プライバシーに関連する組織の目的を達成するように、データ主体（本人）の同意を得て、パーソナル・インフォメーションを開示している。違反及び事故の通知は、プライバシーに関連する組織の目的を達成するように、影響を受けるデータ主体(本人)、規制当局等へ行われている。

vii. 品質：組織は、プライバシーに関連する組織の目的を達成するように、正確、最新、完全かつ適切となるパーソナル・インフォメーションを収集し維持する。

viii. モニタリング及び執行：組織は、プライバシーに関連する組織の目的を達成するように、遵守状況をモニタリングする。これには、プライバシーに関連する問合せ、苦情及び紛争に対処する手続も含まれる。

10. 上述のように、Trust サービス規準は、情報及びシステムのセキュリティ、可用性若しくは処理のインテグリティ、又は組織が処理する情報の機密保持若しくはプライバシーに関連する内部統制のデザインの適切性と運用の有効性を評価する際に使用することができる。したがって、組織の内部統制が、単独で又は他のカテゴリーの内部統制と組み合わせて、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のカテゴリーに関連する規準を満たすように有効であるかどうかを評価する際に、Trust サービス規準を使用することができる。

Trust サービス規準の適用及び利用

11. Trust サービス規準は、様々に異なる主題への適用及び利用に当たって柔軟性を提供できるようにデザインされている。以下は、業務実施者が Trust サービス規準を使用して報告することができる主題の種類である。
- 内部統制の規準としてセキュリティ、可用性及び機密保持に関連する Trust サービス規準を使用したサイバーセキュリティ・リスク管理の検証における、組織のサイバーセキュリティ目的を達成するための、組織のサイバーセキュリティ・リスク管理プログラムに含まれる内部統制の有効性[2]
- タイプ２の SOC2®業務においてセキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシーに係る一つ又は複数の Trust サービス規準を満たすための受託会社のシステムに関する経営者の記述書に含まれている、特定の期間を通じた、これらの規準に関連する内部統制のデザインの適切性と運用の有効性。内部統制の運用の有効性に関する意見を含むタイプ２の SOC2®業務には、当該受託会社監査人が実施した内部統制のテストと、そのテストの結果の詳細な記述も含まれる。タイプ１の SOC2®業務は、タイプ２の SOC2®業務と同じ主題に対処するが、タイプ１の報告書には、内部統制の運用の有効性に関する意見も、当該受託会社監査人が実施した内部統制のテストと、そのテストの結果の詳細な記述も含まれていない。[3]
- 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一つ又は複数の Trust サービス規準に関連するシステムに対する受託会社の、内部統制のデザインの適切性と運用の有効性（SOC3®業務）。SOC3®報告書には、内部統制の運用の有効性に関する意見が含まれているが、当該受託会社監査人が実施した統制のテストと、そのテストの結果の詳細な記述は含まれていない。
- 受託会社以外の組織の一つ又は複数の Trust サービスのカテゴリー（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

[2] AICPA ガイド「組織のサイバーセキュリティ・リスク管理プログラムと内部統制（サイバーセキュリティガイド）」は、業務実施者によるサイバーセキュリティ・リスク管理に関する検証業務の実施と報告のガイドを提供している。

[3] AICPA ガイド「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係る内部統制の報告書」2015 年７月発行には、SOC2®検証業務の実施及び報告のガイドが含まれている。

一つ又は複数のシステムに係る、内部統制のデザインの適切性と運用の適切性

- 関連する Trust サービス規準を満たすための、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係る組織の内部統制のデザインの適切性[4]

12. 業務実施者は一般に、法令、ルール、契約又はグラント・アグリーメントに関する組織の遵守状況又はその遵守のための内部統制の状況について報告するに当たって、Trust サービス規準を使用することはない。業務実施者が、組織の内部統制のデザインと運用の有効性の検証に併せて、法令、ルール、契約又はグラント・アグリーメントへの遵守状況について報告する契約をしている場合（例えば、AT-C セクション 105、「全ての証明業務に共通する概念」及び AT-C セクション 205、「検証業務」に従って実施されるプライバシー業務）[5]、業務のうち、遵守状況に関する部分は、AT-C セクション 105 及び 315、「遵守証明」に従って実施される。

13. Trust サービス規準の多くに、組織の目的を達成するとの文言が含まれている。Trust サービス規準は、様々な異なる種類の業務（パラグラフ 20-23 参照）において、様々な異なる主題（パラグラフ 11 参照）に関連する内部統制を評価するために使用される可能性があることから、この文言の解釈は、業務の具体的な状況によって異なる。したがって、Trust サービス規準を用いる際に、規準で言及されている組織の目的が、特定の業務の主題と範囲によってどのような影響を受けるのかを検討する。

14. 例えば、以下の業務について検討する。

- システムのセキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシーに係る受託会社の内部統制を検証及び報告するために実施される SOC2® 業務では、経営者は顧客へのコミットメントを達成する責任を負う。したがって、SOC2®業務における目的は、顧客へのコミットメントとシステム要求事項を満たすことに関連する。コミットメントとは、一つ又は複数の組織のシステムのパフォーマンスに関して経営者が顧客に行う言明をいう。そのようなコミットメントは一般に、書面による契約、サービスレベルアグリーメント又は公式声明（例えば、プライバシー通知）に含まれる。全ての顧客に適用されるコミットメント（ベースラインコミットメント）が存在する一方で、ベースラインコミットメントを達成するために必要なものに加えて、プロセスや内部統制を導入させる個々の顧客のニーズを満たすようにデザインされたコミットメントも存在する。システム

[4] AT-C セクション 9205、検証業務：セクション 205 の証明解釈指針は、解釈指針第２号「内部統制のデザインに関する報告書」（AICPA、職業的基準、AT-C セクション 9205 パラグラフ.04-.14）にある。この文書は、業務実施者が AT-C セクション 205「証明業務」の下での内部統制のデザインの適切性を調べるかもしれないと記載している。AT-C セクション 205 のパラグラフ 10 は、業務がいまだ実施されていない内部統制を対象としている場合、業務実施者がどのように報告すべきかについての指針を提供する。

[5] 全ての AT-C セクションは、AICPA 職業的基準に記載されている。

要求事項は、顧客に対する組織のコミットメントを達成し、または、関連する法令又はビジネス又は業界団体などの産業別のガイドラインを満たすためにシステムがどのように機能すべきかを指すものである。

・　全社的なサイバーセキュリティ・リスク管理の検証において、組織はサイバーセキュリティ目的を定める。サイバーセキュリティ目的は、サイバーセキュリティ・リスクに影響される目的であるため、組織のコンプライアンス、報告及び運営上の目的の達成に影響を及ぼす。組織のサイバーセキュリティ目的の性質は、組織が事業を運営する環境、組織のミッションとビジョン、経営者が策定する全般的な経営目的及びその他の要因によって異なる。例えば、電気通信事業会社は、重要なインフラストラクチャーとみなされる事業の諸側面が信頼性をもって機能することに関連したサイバーセキュリティ目的を有するかもしれない。一方で、オンラインデート会社は、その事業目的を達成するに当たって、顧客から収集するパーソナル・インフォメーションのプライバシーを重要な要素と考える可能性が高い。[6]

15. 主題及び業務の範囲の違いが、Trust サービス規準の使用にどのように影響するかの例として、次の Trust サービス規準 CC6.4 を検討する。

組織は、その目的を達成するために、設備及び保護された情報資産（例えば、データセンター設備、バックアップ媒体保管庫及び他の機密上重要な場所）への物理的なアクセスを承認された要員に制限する。

16. パラグラフ 14 で取り上げた SOC2®業務の例では、CC6.4 における「その目的を達成するために」との文言は通常、以下のように解釈される。

組織は、受託会社のコミットメントとシステム要求事項を満たすために、施設及び保護された情報資産（データセンター設備、バックアップ媒体保管庫及び他の機密上重要な場所）への物理的アクセスを承認された要員に制限する。

17. また、規準 CC6.4 が適用されるのは、SOC2®業務の範囲に含まれるシステムと関係のある Trust サービスのカテゴリーに係る内部統制に関連する場合に限られる。

18. パラグラフ 14 で取り上げたサイバーセキュリティ・リスク管理の検証の例では、CC6.4 における「組織の目的を達成するために」との文言は通常、以下のように解釈される。:

組織は、そのサイバーセキュリティ目的を達成するために、施設及び保護された情報資産（データセンター設備、バックアップ媒体保管庫及び他の機密上重要

[6] 業務実施者の責任は、SOC1®業務における受託会社監査人において受託会社のシステムに関する経営者の記述書に記載された統制目的が状況に応じて合理的であるかを判断する、AT-C セクション 320「委託会社の財務報告に係る内部統制に関連する受託会社の内部統制の検証報告」の要求事項と同様である。

な場所）への物理的アクセスを承認された要員に制限する。

19. また、規準 CC6.4 は、サイバーセキュリティ・リスク管理の検証範囲に応じて、(a)全社横断的に、(b)子会社、部門又は業務ユニットのレベルにおいて、(c)組織の業務、報告又はコンプライアンス上の目的に関連する機能に含まれ、または、(d)組織が使用する特定の種類の情報に対する、サイバーセキュリティ・リスク管理プログラムに含まれる内部統制に関連する場合に適用される。

Trust サービス規準を使用する業務に関する職業的基準

証明業務

20. AICPA の「証明業務基準」[7]（SSAE 又は証明基準）に基づき、実施される検証業務及び合意された手続業務は、Trust サービス規準を評価規準として用いることができる。証明基準は、検証、レビュー [8]及び合意された手続業務に関連して実施と報告に関するガイダンスを提供する。証明基準において、証明業務を実施する公認会計士は、「業務実施者」とされる。検証業務では、業務実施者は、特定された規準に照らして、主題又は主題に関するアサーションについて意見を表明する報告書を提供する。合意された手続業務では、業務実施者は意見を表明するのではなく、特定の関係者の間で合意された手続を実施し、当該手続の結果を報告する。検証業務は、証明基準の AT-C セクション 105 及び 205 に準拠して実施され、合意された手続業務は、AT-C セクション 105 及び 215 に従って実施される。

21. 証明基準によると、証明業務で使用する規準は、報告書の利用者にとって適切であり、利用可能であることが必要である。適切となる規準の属性は、以下のとおりである。[9]：
- 関連性：規準は、主題に関連していなければならない。
- 客観性：規準に、偏向があってはならない。
- 測定可能性：規準は、主題について、定性的又は定量的に合理的で一貫した測定を可能にしなければならない。
- 完全性：規準は、それに従って作成された主題が、当該主題に基づいて行われる想定された利用者の判断に影響を与えると合理的に見込まれる関連要因を除外することがないように、完全でなければならない。

---

[7] 証明業務基準書 18 号、証明基準：改訂版(AICPA、職業的基準)は、2017 年 5 月 1 日以降の業務責任者の報告書から適用される。

[8] AT-C セクション 305「将来の財務情報」パラグラフ 0.7 において、業務実施者が内部統制のレビューを行うことを禁止している。業務実施者は、Trust サービス規準を使用して、証明基準に従ってレビューエンゲージメントを実行することはできない。

[9] AT-C セクション 105、パラグラフ 25b、「全ての証明業務に共通の概念」

22. 証明業務で用いられる規準は、適切であることに加えて、AT-C セクション 105 により、報告書の利用者にとって利用可能なものでなければならないことが示されている。Trust サービス規準が公表されることにより、当該規準は利用者にとって利用可能なものとなる。よって、ASEC は、Trust サービス規準は、証明基準に従った適切な規準であると結論付けた。

コンサルティング業務

23. 場合により、業務実施者が、組織に一つ又は複数の新たな情報システムを導入するに当たって経営者を支援する準備サービスに、Trust サービス規準が使用されることがある。[10]そのような業務は通常、コンサルティング基準に従って実行される。コンサルティング業務において、業務実施者は、経営者が検討及び使用するための発見事項の提示及び推奨項目の提供をする。業務実施者は、この業務の主題に対して、結論の形成や意見の表明をしない。一般に、コンサルティング業務はクライアントの利用と便益のためだけに実行される。この業務を提供する業務実施者は、CS セクション 100、コンサルティングサービス：定義及び基準（AICPA、職業的基準）に従う。

Trust サービス規準

24. 以下の表は、Trust サービス規準及び関連する着眼点を列挙している。COSO フレームワーク[11]から直接引用されているものは標準フォント、Trust サービス規準を使用する業務に適用するものはイタリック体、そして、Trust サービス規準を使用する業務がシステムレベルで実施される場合のみ適用されるものは、太字のイタリック体で表示されている。

Trust サービス規準と着眼点	
	統制環境
CC1.1	**COSO 原則 1[12]：組織は、誠実性と倫理観に対するコミットメントを表明する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：

[10] 業務実施者が、情報システムの設計、導入又は統合サービスを証明業務のクライアントに提供する場合、業務実施者の独立性への脅威が存在する可能性がある。AICPA 職業行動規範の「情報システム設計、導入又は統合」の解釈は（AICPA、職業的基準、ET セクション 1.295.145）、独立性に対するそのような脅威の影響を評価する業務実施者に指針を提供する。

[11] ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

[12] COSO 原則及び COSO フレームワークに記載されている着眼点の日本語訳については、以下翻訳書から引用している。
「COSO 内部統制の統合的フレームワーク」（八田進二、箱田順哉監訳、日本内部統制研究学会新 COSO 研究会訳、日本公認会計士協会出版局発行）ツール篇 P.27-44

	・　トップの気風の設定―取締役会と事業体のすべての階層の経営者は、内部統制システムの機能を支援する誠実性と倫理観が重要であることを、自らの指示、行動、態度で示している。
	・　行動基準の確立―取締役会および上級経営者が求める誠実性と倫理観は、事業体の行動基準において明確化され、その内容は組織の全階層、外部委託先およびビジネスパートナーに理解されている。
	・　行動基準の遵守状況の評価―事業体が期待する行動基準に照らした、個人およびチームの遵守状況について、評価プロセスを定めている。
	・　行動基準からの逸脱に対する適時の対応―期待される行動基準からの逸脱は適時に一貫性をもって識別され、是正されている。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・　*コミットメントの表明には、契約者及びベンダーの従業員の使用を考慮している。―経営者及び取締役会は、行動基準の確立、基準の遵守状況の評価、基準からの逸脱に対する適時の対応のプロセスにおいて、契約者及びベンダーの従業員の使用を考慮している。*
CC1.2	**COSO 原則２[13]：取締役会は、経営者から独立していることを表明し、かつ、内部統制の整備および運用状況について監督を行う。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：
	・　監督責任の確立―取締役会は、法律および規制上の要件と利害関係者の期待に関して、監督責任を識別し、受け入れている。
	・　関連する専門知識の活用―取締役会は、上級経営者に掘り下げた質問を行い、ふさわしい行動を取るために取締役に必要とされる能力と専門知識を定義し、維持し、定期的に評価している。
	・　独立性の保持―取締役会には、経営者から独立し、客観的な評価と意思決定を行う十分な数のメンバーがいる。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・　*取締役会の専門性の補完―取締役会は、必要に応じて、小委員会又はコンサルタントを利用して、セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る専門知識を補完する。*
CC1.3	**COSO 原則３[14]：経営者は、取締役会の監督の下、内部統制の目的を達成するに当たり、組織構造、報告経路および適切な権限と責任を確立する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：

[13] 脚注 12 に同じ
[14] 脚注 12 に同じ

	・　事業体のすべての構造の検討―経営者と取締役会は、内部統制の目的の達成を支援するため、使用される複数の組織構造（業務単位、法人組織、地域的な分布、外部委託先を含む）に対する検討を行う。
	・　報告経路の確立―経営者は、権限と責任が遂行でき、事業体の活動を管理する情報が伝達できるように、報告経路を組織構造ごとに設計し、評価している。
	・　権限と責任の明確化、付与および制限―経営者と取締役会は、権限を委譲し、責任を明確化しているほか、組織のさまざまな階層で、責任を付与し、必要に応じて職務を分掌するため、適切なプロセスとテクノロジーを利用している。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・　*権限及び責任を定義する際の特有な要件に対する対応―経営者及び取締役会は、権限及び責任を定義する際に、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要件を検討する。*
	・　*組織構造、報告経路、権限及び責任を確立する際に、外部当事者との関わり合いを検討―経営者及び取締役会は、組織構造、報告経路、権限及び責任を確立する際に、外部当事者の活動に関与し、その活動を監視する必要性を検討する。*
CC1.4	**COSO 原則４**[15]**：組織は、内部統制の目的に合わせて、有能な個人を惹きつけ、育成し、かつ、維持することに対するコミットメントを表明する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。：
	COSO フレームワークに記載されている着眼点：
	・　方針と実務の確立―方針と実務は、目的達成を支援するために必要な業務遂行能力への期待を反映している。
	・　能力の評価と能力不足への対応―取締役会および経営者は、組織全体と外部委託先が、確立された方針と実務に照らして業務遂行能力を有しているかを評価し、必要に応じて能力不足に対応している。
	・　個人を惹きつけ、育成し、維持すること―組織は、目的達成を支援するために必要な人数の有能な構成員と外部委託先を惹きつけ、育成し、かつ、維持するために必要な指導と研修を提供している。
	・　後継計画と準備―上級経営者および取締役会は、内部統制に重要な責任を負う構成員の任命に関する代替計画を整備する。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・　*個人のバックグランドの検討―事業体は、潜在的及び既存の構成員、契約者並びにベンダーの従業員を雇用及び維持するかを判断する際に、各個人のバックグランドを検討する。*

[15] 脚注 12 に同じ

	・ *個人の技術的な能力の検討—事業体は、潜在的及び既存の構成員、契約者並びにベンダーの従業員を雇用及び維持するかを判断する際に、各個人の技術的な能力を検討する。*
	・ *技術的な能力を維持するための研修の提供—事業体は、既存の構成員、契約者及びベンダーの従業員のスキルセット及び技術的な能力が開発及び維持されることを確実にするために、継続教育訓練などの研修プログラムを提供する。*
CC1.5	**COSO 原則５[16]：組織は、内部統制の目的を達成するに当たり、内部統制に対する責任を個々人に持たせる。**
	COSO フレームワークに記載されている以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ 組織構造、権限および責任を通しての説明責任の履行—経営者および取締役会は、必要な情報が伝達される仕組みを確立し、組織の内部統制に対する責任の履行について個々人に説明責任を持たせ、必要に応じて是正措置を実施している。
	・ 業績尺度、動機づけおよび報奨の制定—経営者および取締役会は、事業体の全階層において責任に応じた業績尺度、動機づけおよびその他の報奨を制定している。業績尺度、動機づけおよび報奨は、業績と期待される行動基準が反映されているほか、短期と長期の目的の達成度を考慮したものとなっている。
	・ 業績尺度、動機づけおよび報奨の継続的適合性の評価—経営者および取締役会は、目的達成における内部統制に対する責任の遂行に見合った動機づけと報奨を決めている。
	・ 過度なプレッシャーの検討—経営者および取締役会は、責任を割り当て、業績尺度を整備し、業績を評価する際に、目的達成に伴うプレッシャーを評価し、調整している。
	・ 業績評価および個人に対する賞罰—経営者および取締役会は、行動基準の遵守と、期待される業務遂行能力のレベルを含め、内部統制に対する責任に関する業績評価を行うほか、必要に応じて賞罰を行っている。
	伝達と情報
CC2.1	**COSO 原則 13[17]：組織は、内部統制が機能することを支援する、関連性のある質の高い情報を入手または作成して利用する。**
	COSO フレームワークに記載されている以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ 必要な情報の識別—内部統制の他の構成要素が機能すること、および事業体の目的達成を支援するために必要な情報を識別するためのプロセ

[16] 脚注 12 に同じ
[17] 脚注 12 に同じ

	スが整備されている。
	・　内部および外部の情報源からのデータの捕捉―情報システムを利用して内部および外部の情報源からデータを捕捉している。
	・　関連するデータの情報への加工―情報システムを利用して関連データを加工し、情報へと変換している。
	・　データ処理過程における品質の維持―情報システムは、適時性、最新性、正確性、完全性、利用可能性をもち、保護されていて、検証可能な、そして保持されるべき情報を作成している。情報は、内部統制の構成要素を支援に当たって関連性をもっているかを評価するためにレビューが行われている。
CC2.2	**COSO 原則 14[18]：組織は、内部統制が機能することを支援するために必要な、内部統制の目的と内部統制に対する責任を含む情報を組織内部に伝達する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：
	・　内部統制に関する情報の伝達―組織内のすべての構成員が各自の内部統制の責任を理解し、遂行するために必要な情報を伝達するプロセスが整備されていること。
	・　取締役会との情報伝達―事業体の目的に関連した職務を遂行する際に必要な情報を共有するため、経営者と取締役会との間で情報伝達が行われていること。
	・　独立した伝達経路の整備―内部通報制度のような独立した伝達経路が整備され、通常の伝達経路が無効になったり有効でなくなった場合でも、それが匿名または秘密の情報伝達ができるように二重の安全装置の役割を果たしていること。
	・　適合性のある伝達方法の選択―伝達の時期、情報の受け手、情報の性質に応じた伝達方法が検討されていること。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・　*責任の伝達―システムコントロールを設計、開発、導入、運用、維持、モニタリングする責任がある事業体の構成員は、各自の職責の変更などを含む責任についての伝達を受け取り、責任を果たすために必要な情報を得ている。*
	・　*障害、インシデント、懸念及びその他の事項の報告に関する情報の伝達―事業体の構成員には、システムに関する障害、インシデント、懸念及びその他の苦情を担当者に報告する方法についての情報が提供されている。*
	・　*目的及び目的の変更の伝達-事業体は、目的及び目的の変更を、適時*

[18] 脚注 12 に同じ

	に構成員に伝達している。
	・ *セキュリティに関する知識及び認識を向上させる情報の伝達―事業体は、セキュリティに関する認識を高める研修プログラムを通じて、構成員がセキュリティに関する知識及び認識を向上させ、また、適切なセキュリティ行動が取れるように情報を伝達している。*
	Trust サービス規準を使用する業務がシステムレベルで実施される場合のみ適用される追加の着眼点：
	・ ***システムの運用及び境界についての情報の伝達―事業体は、システムの設計及び運用とその境界に関連する情報を、承認された構成員が、システム上の役割とシステム運用の結果を理解できるように用意し、伝達している。***
	・ ***システムの目的の伝達―事業体は、構成員が責任を果たすことができるように、その目的を伝達している。***
	・ ***システム変更の伝達―責任又は事業体の目的の達成に影響を及ぼすシステム変更は、適時に伝達されている。***
CC2.3	**COSO 原則 15[19]：組織は、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。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：
	・ 外部の関係者への情報伝達―目的に適する適時な情報を、株主、パートナー、所有者、規制当局、顧客、財務アナリスト等の外部の関係者へ伝達するプロセスが整備されている。
	・ 外部からの情報伝達を可能にする―開かれた伝達経路は、顧客、消費者、供給業者、外部監査人、規制当局、財務アナリスト等の外部の関係者からの情報提供を可能にし、経営者および取締役会に対して目的に適合する情報を提供している。
	・ 取締役会との情報伝達―外部の関係者による評価から得られた目的適合性をもった情報が、取締役会に伝達されている。
	・ 独立した伝達経路の整備―通報制度（ホットライン）のような独立した伝達経路が整備されており、通常の伝達経路が無効または有効でない場合、匿名または秘密の情報伝達を可能にする二重の安全装置の役割を果たしている。
	・ 適合性のある伝達方法の選択―伝達の時期、対象、性質、法律および規則および受託責任に関する要請と期待に応じた伝達方法が検討されている。
	機密保持に係る Trust サービス規準を使用する業務にのみ適用する追加の着眼点：

[19] 脚注 12 に同じ

	・ *機密保持に関する目的及び目的の変更の伝達―事業体は、外部ユーザー、ベンダー、ビジネス・パートナー、その他のシステムの一部になる製品やサービスを提供する者に、機密保持に関する目的及び目的の変更を伝達している。*
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する追加の着眼点:
	・ *プライバシーに関する目的及び目的の変更の伝達–事業体は、外部ユーザー、ベンダー、ビジネス・パートナー、その他のシステムの一部になる製品やサービスを提供する者に、プライバシーに関する目的及び目的の変更を伝達している。*
	Trust サービス規準を使用する業務が、システムレベルで実施される場合のみ適用される追加の着眼点:
	・ ***システムの運用及び境界についての情報の伝達―事業体は、システムの設計及び運用とその境界に関連する情報を、承認された外部ユーザーが、システム上の役割とシステム運用の結果を理解できるように用意し、伝達している。***
	・ ***システムの目的の伝達―事業体は、適切な外部ユーザーに、そのシステムの目的を伝達している。***
	・ ***システムに関する責任の伝達―システムコントロールを設計、開発、導入、運用、維持、モニタリングする責任がある外部ユーザーは、各自の責任についての伝達を受け取り、責任を果たすために必要な情報を得る。***
	・ ***システムに関する障害、インシデント、懸念及びその他の事項の報告に関する情報の伝達―外部ユーザーには、システムに関する障害、インシデント、懸念及び他の苦情を適切な担当者に報告する方法についての情報が提供されている。***
	リスク評価
CC3.1	**COSO 原則 6[20]:組織は、内部統制の目的に関連するリスクの識別と評価ができるように、十分な明確さを備えた内部統制の目的を明示する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点:
	業務目的
	・ 経営者の選択を反映する―業務目的は、組織構造、業界動向、事業体の業績に関する経営者の選択を反映したものとする。
	・ リスク許容度を考慮する―経営者は、業務目的の達成に関連して、許容可能な変動の水準を検討する。
	・ 業務および財務業績の目標を含める―組織は、事業体の業務および財

[20] 脚注 12 に同じ

	務の期待業績値を業務目的に反映させる。
	・　経営資源の配分の基礎を形成する―経営者は、期待される業務および業績を達成するために必要な経営資源を配分するための基礎として業務目的を利用する。
	外部財務報告目的
	・　適用可能な会計基準に準拠する―財務報告目的は、当該事業体に適切かつ利用可能な会計原則と整合するものである。選択された会計原則は、事業体の状況に照らして適切なものである。
	・　重要性を考慮する―経営者は、財務諸表の表示において重要性を考慮する。
	・　事業体の活動を反映する―外部財務報告は、質的特性およびアサーションを示すための基礎となる取引と事象を反映する。
	外部非財務報告目的
	・　外部で設定された基準およびフレームワークを遵守する―経営者は、法律および規則ならびに広く認められた外部組織が設定した基準およびフレームワークを遵守した非財務報告目的を設定する。
	・　求められる精度のレベルを検討する―経営者は、利用者のニーズに適合し、第三者が設定した規準に基づく精度と正確性を非財務報告に反映させる。
	・　事業体の活動を反映する―外部報告は、基礎となる取引と事象を許容可能な範囲で反映する。
	内部報告目的
	・　経営者の選択を反映する―内部報告は、事業体の経営に必要な、経営者の選択肢と情報に関する正確で網羅的な情報を経営者に提供する。
	・　求められる精度のレベルを検討する―経営者は、非財務報告目的における利用者のニーズと財務報告目的における重要性に適合する、求められる精度と正確性の必要なレベルを反映する。
	・　事業体の活動を反映する―内部報告は、基礎となる取引と事象を許容可能な範囲で反映する。
	コンプライアンス目的
	・　法律および規則を反映する―法律および規則は、事業体がコンプライアンス目的に組み込む最低限の行動基準を定めている。
	・　リスク許容度を検討する―経営者は、コンプライアンス目的の達成と関連づけて、許容可能な変動の水準を検討する。
	Trust サービス規準を使用する全ての業務に、特に関連する追加の着眼点：

	・ *目的を支援する下位目的の確立―経営者は、報告、運用及びコンプライアンスに関して、事業体の目的の達成を支援するために、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下位目的を識別する。*
CC3.2	**COSO 原則 7[21]：組織は、自らの目的の達成に関連する事業体全体にわたるリスクを識別し、当該リスクの管理の仕方を決定するための基礎としてリスクを分析する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：
	・ 事業体、子会社、部門、業務単位、機能レベルの包含―組織は、統制目的の達成に関し、事業体、子会社、部門、業務単位、機能レベルごとにリスクを識別し、分析する。
	・ 内部要因と外部要因の分析―リスクの識別においては、内部と外部の両要因と、それらが統制目的の達成に及ぼす影響について検討する。
	・ 適切な階層の経営者の関与―組織は、適切な階層の経営者が関与する有効なリスク評価の仕組みを導入する。
	・ 識別したリスクの重大性の見積り―識別したリスクは、リスクの潜在的な重大性の見積りを含むプロセスを通じて分析される。
	・ リスクへの対応方法の決定―リスク評価では、リスクをどのように管理すべきか、そしてリスクの受容、回避、低減、共有といったリスク対応策の検討が含まれている。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・ *情報資産の重要性の識別・評価及び脅威と脆弱性の特定―事業体がリスクを識別・評価するプロセスには、(1)物理的装置・システム、仮想装置、ソフトウェア、データ・データフロー、外部情報システム及び組織の役割などの情報資産を識別すること、(2)それらの情報資産の重要性を評価すること、(3)意図的（悪意のあるものを含む。）又は意図しないうちに行われる行為及び環境上の事象による資産への脅威を識別すること、(4)識別された資産の脆弱性を特定すること、が含まれる。*
	・ *ベンダー、ビジネス・パートナーなどの当事者に起因する脅威及び脆弱性の分析―事業体のリスク評価のプロセスには、事業体の情報システムにアクセスできるビジネス・パートナーや顧客などに起因する脅威及び脆弱性だけではなく、商品やサービスを提供するベンダーに起因する潜在的な脅威及び脆弱性も分析することが含まれる。*
	・ *リスクの重大性の検討―識別されたリスクの潜在的重大性の検討には、(1)目的の達成における識別された資産の重要度を判断すること、(2)目的の達成において識別された脅威及び脆弱性が及ぼす影響を評価*

[21] 脚注 12 に同じ

	すること、(3)識別された脅威の発生可能性を評価すること、(4)資産の重要度、脅威の影響度及び発生可能性に基づいて、資産に伴うリスクを判断することが含まれる。
CC3.3	**COSO 原則８[22]：組織は、内部統制の目的の達成に対するリスクの評価において、不正の可能性について検討する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：
	・　さまざまな種類の不正行為の検討―不正の評価では、さまざまな不正および違法行為の結果発生し得る不適切な報告、資産の喪失および汚職について検討する。
	・　動機とプレッシャーの検討―不正リスク評価では、動機およびプレッシャーを検討する。
	・　不正を犯す機会の評価―不正リスク評価では、資産の未承認での取得、使用もしくは廃棄、事業体の報告記録の改ざん、またはその他の不適切な行為を犯す機会を検討する。
	・　姿勢と正当化の評価―不正リスク評価では、経営者およびその他の構成員がどのように不適切な行為に関与する、またはそれを正当化する可能性があるかについて検討する。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・　*ＩＴの利用及び情報へのアクセスに関連するリスクの検討―不正リスクの評価には、特にＩＴの利用及び情報へのアクセスに起因する脅威及び脆弱性の検討が含まれる。*
CC3.4	**COSO 原則９[23]：組織は、内部統制システムに重大な影響を及ぼし得る変化を識別し、評価する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。:
	COSO フレームワークに記載されている着眼点：
	・　外部環境の変化に対する評価―リスクの識別プロセスでは、事業体が業務を運営している規制環境、経済環境および物理的環境の変化を検討する。
	・　ビジネスモデルの変化に対する評価―組織は、新規のビジネスライン、既存のビジネスラインの構成要素の大幅な変更、買収または売却された活動に係る内部統制システム、急速な業績の伸び、海外事業への依存度の変化および新しいテクノロジーの潜在的な影響について検討する。
	・　リーダーシップの変化に対する評価―組織は、経営者の交代と、それに伴う内部統制システムに対する経営者の姿勢および理念の変化を検討

[22] 脚注 12 に同じ
[23] 脚注 12 に同じ

	する。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・ *システム及びテクノロジーの変化の評価―リスクを識別するプロセスでは、事業体のシステムの変更及びテクノロジー環境の変化を検討する。*
	・ *ベンダー及びビジネス・パートナーとの関係の変化の評価―リスクを識別するプロセスでは、ベンダー及びビジネス・パートナーとの関係の変化を検討する。*
	モニタリング活動
CC4.1	**COSO 原則 16[24]：組織は、内部統制の構成要素が存在し，機能していることを確かめるために，日常的評価および/または独立的評価を選択し，整備および運用する。**
	以下の着眼点は、この規準に関する重要な特性を明示している。：
	COSO フレームワークに記載されている着眼点：
	・ 日常的および独立的評価の組合せの検討―経営者は、日常的評価と独立的評価のバランスを検討項目に含めていること。
	・ 変化の速度の検討―経営者は、日常的評価および独立的評価を選択し、整備するにあたり、ビジネスおよびビジネスプロセスの変化の速度を検討していること。
	・ 基準点の確立―内部統制システムの設計と現状を踏まえて、日常的および独立的評価の基準点を確立していること。
	・ 知識豊富な構成員の活用―日常的および独立的評価を実施する評価者は、評価対象を理解する十分な知識を持ち合わせていること。
	・ ビジネスプロセスとの統合―日常的評価は、ビジネスプロセスに組み込まれ、ビジネスプロセスの変更に応じて調整されること。
	・ 範囲と頻度の調整―経営者は、リスクに応じて独立的評価の範囲と頻度を変化させていること。
	・ 客観的な評価―客観的な意見を提供するために、独立的評価を定期的に実施すること。
	Trust サービス規準を使用する全ての業務に特に関連する追加の着眼点：
	・ *様々な種類の継続的評価及び独立的評価の検討―経営者は、侵入テスト、確立された仕様に関する独立した認証（例えば、ISO 認証）、及び内部監査による評価など、様々な種類の継続的評価及び独立的評価を使用する。*
CC4.2	**COSO 原則 17[25]：組織は、適時に内部統制の不備を評価し、必要に応じて、それを適時に上級経営者および取締役会を含む、是正措置を講じる責**

[24] 脚注 12 に同じ
[25] 脚注 12 に同じ

	任を負う者に対して伝達する。
	COSO フレームワークに記載されている以下の着眼点は、この規準に関する重要な特性を明示している。:
	・　結果の評価―経営者および取締役会は、必要に応じて、日常的評価および独立的評価の結果を評価している。
	・　不備の伝達―内部統制の不備が、是正措置の実施に責任を負う関係者および必要な場合には、上級経営者および取締役会へ伝達されている。
	・　是正措置のモニタリング-経営者は、不備が適時に是正されていることを追跡管理している。
	統制活動
CC5.1	**COSO 原則 10[26]：組織は、内部統制の目的に対するリスクを許容可能な水準まで低減するのに役立つ統制活動を選択し、整備する。**
	COSO フレームワークに記載されている以下の着眼点は、この規準に関する重要な特性を明示している。:
	・　リスク評価との統合―統制活動は、リスクに対応し、それを低減するリスク対応が確実に実行されることに役立つ。
	・　事業体特有の要因の検討―経営者は、事業体の業務に係る環境、複雑性、特性ならびに組織特有の性質が、どのように統制活動の選択と整備に影響を与えるかを検討する。
	・　関連性があるビジネスプロセスの決定―経営者は、関連性があるどのビジネスプロセスに統制活動が必要かを決定する。
	・　統制活動の種類の組合せの評価―統制活動には広範かつさまざまな統制が含まれており、また、手作業および自動化された統制の双方ならびに予防的および発見的統制の双方を検討しつつ、リスクを低減するアプローチのバランスを取ることも含まれる場合がある。
	・　適用される活動レベルでの検討―経営者は、事業体のさまざまな階層における統制活動を検討する。
	・　職務分掌への対応―経営者は両立しない職務を分離し、また、分離が実務上難しい場合は、代替的な統制活動を選択し、整備する。
CC5.2	**COSO 原則 11[27]：組織は、内部統制の目的の達成を支援するテクノロジーに関する全般的統制活動を選択し、整備する。**
	COSO フレームワークに記載されている以下の着眼点は、この規準に関する重要な特性を明示している。:
	・　ビジネスプロセスにおけるテクノロジーの利用とテクノロジー全般統制の間の依存関係の決定―経営者は、ビジネスプロセス、自動化された統制活動およびテクノロジー全般統制の依存関係とつながりを理解し、

[26] 脚注 12 に同じ
[27] 脚注 12 に同じ

	決定する。
	・　テクノロジー基盤に係る統制活動の確立―経営者は、テクノロジー処理の網羅性、正確性および可用性の確保を促進するよう設計、適用されたテクノロジー基盤に係る統制活動を選択し、整備する。
	・　セキュリティ管理プロセスに係る統制活動の確立―経営者は、テクノロジーへのアクセス権を、職務上の責任に見合った権限のあるユーザーのみに制限し、外部の脅威から事業体の資産を守るよう設計、適用される統制活動を選択し、整備する。
	・　関連性のあるテクノロジーの取得、開発および保守プロセスに係る統制活動の確立―経営者は、その目的を達成するために、テクノロジーおよびその基盤の取得、開発および保守に係る統制活動を選択し、整備する。
CC5.3	**COSO 原則 12[28]：組織は、期待されていることを明確にした方針および方針を実行するための手続を通じて、統制活動を展開する。**
	COSO フレームワークに記載されている以下の着眼点は、この規準に関する重要な特性を明示している。:
	・　経営者の指示を展開することを支援する方針および手続を明確にする―経営者は、期待されていることを明確にした方針および行動を規定した関連性のある手続を通じて、ビジネスプロセスと日々の従業員の行動に組み込まれる統制活動を設定する。
	・　方針および手続の実行に関する行為責任と説明責任を明確にする―経営者は、関連するリスクが存在するビジネスユニットまたは機能に所属する経営者（または他の指定された者）とともに、統制活動における行為責任と説明責任を明確にする。
	・　適時に実行する―責任者は、方針および手続に示されているとおりに適時に統制活動を実行する。
	・　是正措置を講じる―責任者は、統制活動を実行した結果、識別された問題点について調査し、対応する。
	・　業務遂行能力を有した構成員による実行―十分な権限を有し、業務遂行能力を有する構成員が、勤勉かつ常に集中して統制活動を実行する。
	・　方針および手続を再評価する―経営者は、継続して目的適合性があるかを決定するために統制活動を定期的にレビューし、必要に応じて更新する。
	論理的及び物理的アクセス管理
CC6.1	***組織は、目的の達成のために、論理的なアクセスセキュリティに関するソフトウェア、インフラストラクチャー及びアーキテクチャを導入し、セキュリティ事象から情報資産を保護する。***

[28] 脚注 12 に同じ

	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *情報資産の識別・台帳の作成・管理―事業体は、情報資産を識別し、台帳を作成し、分類し、管理する。*
	・ *論理的なアクセスの制限―ハードウェア、データ（保存中、処理中又は送信中のもの）、ソフトウェア、管理者権限、モバイル機器、出力及びオフラインのシステム構成要素などの情報資産への論理的なアクセスは、アクセス管理ソフトウェアを使用し、かつ、一連の規則に従ったものに制限される。*
	・ *ユーザーの識別及び承認―ローカル又はリモートアクセスのいずれの場合も、情報資産へのアクセスが行われる前に、人、インフラストラクチャー及びソフトウェアは識別され、承認される。*
	・ *ネットワーク分割の検討―ネットワーク分割により、事業体の情報システムにおいて相互関連性のない部分は、互いに分離される。*
	・ *アクセスポイントの管理―外部事業体のアクセスポイント及びアクセスポイントを通過するデータの種類は、識別され、一覧にされ、管理される。各アクセスポイントを利用する個人及びシステムの種類は、識別され、文書化され、管理される。*
	・ *情報資産へのアクセスの制限―情報資産に対するアクセス管理規則は、データ分類、区分されたデータ構造、ポート制限、アクセスプロトコル制限、ユーザー識別及びデジタル証明書を組み合わせて設定される。*
	・ *識別及び認証の管理―事業体の情報、インフラストラクチャー及びソフトウェアにアクセスする個人及びシステムに対して、識別及び認証の要件が確立され、文書化され、管理される。*
	・ *インフラストラクチャー及びソフトウェアに対する資格の管理―新規の内部及び外部のインフラストラクチャー・ソフトウェアは、登録・承認及び文書化を行った後に、アクセス資格が付与され、ネットワーク又はアクセスポイントに導入される。アクセスがもはや必要でない場合、又は、インフラストラクチャー及びソフトウェアがもはや使用されない場合には、資格は削除され、アクセスは無効にする。*
	・ *データ保護のための暗号化―事業体は、リスク評価の結果、データ保護のために適切と考えられる場合には、暗号化により、保存データの保護に用いられている対策を補完する。*
	・ *暗号鍵の保護―生成、保管、使用、破棄時に暗号鍵を保護するためのプロセスが整備されている。*
CC6.2	***組織は、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承認***

	する。組織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 サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *保護された資産へのアクセス資格の管理―情報資産へのアクセス資格は、システム資産のオーナー又は承認された管理者からの許可を得た上で、作成される。*
	・ *保護された資産へのアクセスの適切な削除―個人がもはや必要としないアクセス資格を削除するプロセスが整備されている。*
	・ *アクセス資格の適切性のレビュー―資格の付与が不必要及び不適切な個人がいないか、アクセス資格の適切性を定期的にレビューする。*
CC6.3	***組織は、その目的を達成するために、最小権限の原則及び職務分離を考慮しながら、データ、ソフトウェア、機能及びその他の保護された情報資産へのアクセスを、役割、責任又はシステムデザインと変更に基づいて、承認し、変更又は削除する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *保護された情報資産へのアクセスの作成又は変更―資産のオーナーからの承認に基づいて保護された情報資産へのアクセスを、作成又は変更するプロセスが整備されている。*
	・ *保護された情報資産へのアクセスの削除―個人がもはや必要としない保護された情報資産へのアクセスを削除するためのプロセスが整備されている。*
	・ *役割ベースのアクセス管理の実施―兼務できない職務の分離を支援するために、役割ベースのアクセス管理が実施される。*
CC6.4	***組織は、その目的を達成するために、設備及び保護された情報資産（例えば、データセンター設備、バックアップ媒体保管庫及び他の機密上重要な場所）への物理的なアクセスを承認された要員に制限する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *物理的なアクセスの作成又は変更―システム資産のオーナーからの承認に基づいて、データセンター、事務所、作業領域などの設備への物理的なアクセスを作成又は変更するためのプロセスが整備されている。*
	・ *物理的なアクセスの削除―個人がもはや必要としない物理的資源へのアクセスを削除するためのプロセスが整備されている。*
	・ *物理的なアクセスのレビュー―職責との一貫性を確実にするために、物理的なアクセスを定期的にレビューするためのプロセスが整備されて*

	いる。
CC6.5	***組織は、その目的を達成するために、物理的資産からデータやソフトウェアを読み取り又は復元することをできなくし、もはや必要なくなった場合のみ、その物理的資産に対する論理的及び物理的な保護を中止する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *処分するデータ及びソフトウェアの識別―処分される機器に格納されたデータ及びソフトウェアを識別し、読み取り不能にするための手続が整備されている。*
	・ *データ及びソフトウェアの事業体の統制対象からの削除―事業体の物理的な統制対象から削除される機器に格納されたデータ及びソフトウェアを削除し、読み取り不能にするための手続が整備されている。*
CC6.6	***組織は、論理的なアクセスセキュリティ対策を、システム境界の外部の脅威から保護するために導入している。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *アクセスの制限―通信チャネル（例えば、FTP サイト、ルーターポート）を通じて生じる種類の活動は制限される。*
	・ *識別及び認証資格の保護―識別及び認証資格は、システム境界の外で送信される間、保護される。*
	・ *追加の認証又は資格の要求―システム境界の外部からシステムにアクセスする場合には、追加の認証情報又は資格を要求する。*
	・ *境界保護システムの導入―外部アクセスポイントを攻撃や未承認のアクセスから保護するために、境界保護システム（例えば、ファイアウォール、DMZ 及び侵入検知システム）を導入し、そうした攻撃を検知するために監視する。*
CC6.7	***組織は、その目的を達成するために、情報の送信、移動及び削除を、許可された内部及び外部ユーザーとプロセスに制限し、そして、送信、移動又は削除する間、その情報を保護する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *送信の制限―データ漏洩防止プロセス及び技術を用いて、情報の送信、移動及び削除を承認・実行することを制限する。*
	・ *データ保護のための暗号化技術又は安全な通信チャネルの利用―アクセスポイントの接続を経由したデータ送信などの通信を保護するために、暗号化技術又は安全な通信チャネルが利用される。*
	・ *リムーバブルメディアの保護―必要に応じて、リムーバブルメディア（USB ドライブやバックアップテープなど）に対して、暗号化技術と物*

	理的資産の保護対策を行う。
	・ *モバイル機器の保護―情報資産となるモバイル機器（ノートパソコン、スマートフォン、タブレットなど）を保護するためのプロセスが整備されている。*
CC6.8	***組織は、その目的を達成するために、未承認又は悪意あるソフトウェアの導入を防止又は検知し、対処する内部統制を導入する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *アプリケーション及びソフトウェアのインストールの制限―アプリケーション及びソフトウェアのインストールは、許可された個人に制限される。*
	・ *ソフトウェア及び設定パラメーターの未承認の変更の検知―ソフトウェア及び設定パラメーターについて、未承認又は悪意のあるソフトウェアの兆候がある変更を検知するためのプロセスが整備されている。*
	・ *定義された変更管理プロセスの使用―ソフトウェアの導入には、経営者の定義した変更管理プロセスを用いる。*
	・ *アンチウィルス及びアンチマルウェアソフトウェアの使用―アンチウィルス及びアンチマルウェアソフトウェアを導入・運用し、マルウェアを遮断又は検知及び是正する。*
	・ *事業体の外部からの情報資産のマルウェア及び他の未承認ソフトウェアのスキャン―事業体の管理に移された、又は戻された情報資産の、マルウェア及び他の未承認ソフトウェアをスキャンし検出した場合は、ネットワークへの実装前にそれらを削除する手続が整備されている。*
	システム運用
CC7.1	***組織は、その目的を達成するために、(1)新規の脆弱性をもたらす設定の変更及び(2)新たに発見された脆弱性に対する感応度を識別するための検出・監視手続を用いる。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *定義された設定標準の使用―経営者は、設定標準を定義する。*
	・ *インフラストラクチャー及びソフトウェアの監視―事業体は、事業体の目的の達成を脅かす可能性がある設定標準の不遵守について、インフラストラクチャー及びソフトウェアを監視する。*
	・ *変更検知する仕組みの導入―ＩＴシステムは、重要なシステムファイル、設定ファイル又はコンテンツファイルの未承認の変更を、要員に知らせる変更検知する仕組み（例えば、ファイル整合性監視ツール）を含む。*
	・ *未知又は未承認の構成要素の検出―未知又は未承認の構成要素の導入*

	を検出する手続が整備されている。
	・ *脆弱性スキャンの実行―事業体は、潜在的な脆弱性又は誤設定を識別するように設計された脆弱性スキャンを、定期的に又は環境に大きな変化があった時に実行し、適時に識別された不備を是正する。*
CC7.2	***組織は、その目的を達成することに影響するような悪意ある行為、自然災害及びエラーの兆候を示す異常がないか、システムの構成要素及びそれらの運用を監視する。そうした異常は分析され、セキュリティ事象かどうかが判断される。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *検出方針、手続及びツールの導入-システムの運用又は通常でない活動における異常を識別するために、検出方針及び手続を定義・導入し、検出ツールをインフラストラクチャー及びソフトウェアに実装する。手続には、(1)リソースの提供を含む、セキュリティ事象検出・管理のための定義されたガバナンスのプロセス、(2)新たに発見された脅威及び脆弱性を識別するための情報源の使用、及び(3)通常でないシステム活動の記録が含まれる場合がある。*
	・ *検出対策の設計―(1)物理的なバリアへの不正侵入、(2)許可された要員の未承認の行為、(3)識別及び認証資格の不正使用、(4)システム境界の外部からの未承認のアクセス、(5)承認された外部関係者の不正侵入、及び(6)未承認のハードウェア及びソフトウェアの導入又は接続といった行為が実際に行われた、又は試みられたことにより発生する可能性のある異常を識別するための検出対策を設計する。*
	・ *異常を分析するためのフィルターの導入―経営者は、セキュリティ事象を識別するために、異常をフィルターにかけ、要約し、分析する手続を導入する。*
	・ *検出ツールの有効な運用の監視―経営者は、検出ツールの有効性を監視するプロセスを導入する。*
CC7.3	***組織は、セキュリティ事象を評価し、目的を達成することができない原因となり得る、又は原因となったか（すなわちセキュリティ・インシデント）を判断する。もし該当する場合は、防止又は対処する措置を講じる。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *セキュリティ・インシデントへの対応―セキュリティ・インシデントへの対応およびその方針・手順の定期的な有効性評価のための手続が整備されている。*
	・ *検出されたセキュリティ事象の伝達およびレビュー―検出されたセキュリティ事象は、セキュリティプログラムの管理責任を有する関係者に*

	伝達され、レビューされ、必要に応じて、是正措置が講じられる。
	・ *セキュリティ・インシデントを分析するための手続の開発及び導入―セキュリティ・インシデントを分析し、システムへの影響を判断する手続が整備されている。*
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する追加の着眼点：
	・ *パーソナル・インフォメーションへの影響の評価―検出されたセキュリティ事象は、評価され、パーソナル・インフォメーションの未承認の開示又は利用があったか、または、その可能性が判断され、また、関係法令に対する違反がないか判断される。*
	・ *利用又は開示されたパーソナル・インフォメーションの特定―パーソナル・インフォメーションの未承認の利用又は開示があった場合には、それにより影響を受ける情報が識別される。*
CC7.4	***組織は、セキュリティ・インシデントを認識し、抑制し、是正し、伝達するために、定義されたインシデント対応プログラムを実施することにより、識別されたセキュリティ・インシデントに適切に対応する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。：
	・ *役割と責任の割当て―インシデント対応プログラムの設計、導入、維持及び実行に対して、役割と責任が割り当てられる。必要に応じて、外部リソースの利用も含まれる。*
	・ *セキュリティ・インシデントの抑制―事業体の目的に対して脅威となるセキュリティ・インシデントを抑制する手続が整備されている。*
	・ *継続的なセキュリティ・インシデントの軽減―継続的なセキュリティ・インシデントの影響を軽減する手続が整備されている。*
	・ *セキュリティ・インシデントのもたらす脅威の終息―脆弱性の除去、未承認のアクセスの排除及び他の是正措置を通じて、セキュリティ・インシデントのもたらす脅威を終息する手続が整備されている。*
	・ *運用の修復―データ及び業務運用を、事業体の目的の達成を可能にする暫定的な状態まで修復する手続が整備されている。*
	・ *セキュリティ・インシデントに対する伝達手順の開発及び導入―事業体の目的を達成するために、セキュリティ・インシデントの伝達及び影響する当事者へ対処のための手順を開発し、導入する。*
	・ *インシデントの性質の理解及び抑制方針の決定―セキュリティ・インシデントの性質（例えば、インシデントが発生した状況や影響を受けたシステムリソース）及び深刻度を理解し、(1)適切な対応時間枠の決定及び(2)抑制方法の決定と実施などを含む適切な抑制方針の決定を行う。*

	・ *識別された脆弱性の是正―識別された脆弱性は、是正活動の開発及び実行を通じて、対処する。*
	・ *是正活動の伝達―是正活動は、インシデント対応プログラムに従って、文書化され、伝達される。*
	・ *インシデント対応の有効性の評価―インシデントへの対応活動の設計は、その有効性について、定期的に評価される。*
	・ *インシデントの定期的な評価―定期的に、経営者は、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インシデントをレビューし、インシデントのパターン及び根本原因に基づいて、システム変更の必要性を識別する。*
	プライバシーに係るTrustサービス規準を使用する業務にのみ適用する追加の着眼点：
	・ *未承認の利用及び開示の伝達―パーソナル・インフォメーションの未承認の利用又は開示を引き起こした事象は、必要に応じて、データ主体（本人）、規制当局その他に伝達する。*
	・ *制裁措置の適用―個人および組織が、事業体の権限の下で業務を行い、パーソナル・インフォメーションの未承認の利用又は開示に関与した場合には、当該行為は評価され、必要に応じて、事業体の方針及び法令上の要件に従って、制裁措置が課される。*
CC7.5	***組織は、特定されたセキュリティ・インシデントから復旧するための活動を識別、開発及び導入する。***
	Trustサービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。：
	・ *影響を受けた環境の修復―必要に応じて、システムの再構築、ソフトウェアの更新、パッチの適用、設定の変更を行うことにより、影響を受けた環境を、機能的に運用できる状態に修復する。*
	・ *事象に関する情報の伝達―インシデントの性質、復旧のために実施された措置、将来のセキュリティ事象の防止に必要となる活動について、経営者及び、必要に応じて、他の適切な関係者（内部及び外部）に伝達が行われる。*
	・ *事象の根本原因の特定―事象の根本原因が特定される。*
	・ *再発の防止及び検出のための変更の導入―追加のアーキテクチャ又は予防的統制及び発見的統制の変更、又は、その両方が、再発の防止及び検出のために適時に導入される。*
	・ *対応及び復旧のための手続の改善―教訓は分析され、インシデントへの対応計画及びインシデントからの復旧手続が改善される。*

	・ *インシデントからの復旧計画のテストの導入―インシデントからの復旧計画のテストは、定期的に実施される。テストには、(1)脅威の発生可能性、及び重大性に基づいたテストシナリオの開発、(2)可用性を損ない得る事業体全体にわたり関連するシステム構成要素の検討、(3)重要な要員が従事できなくなる可能性を考慮したシナリオ、及び(4)テスト結果に基づいた継続計画およびシステムの修正が含まれる。*
	変更管理
CC8.1	***組織は、その目的を達成するために、インフラストラクチャー、データ、ソフトウェア及び手続の変更を、(起案)承認し、設計し、開発又は取得し、設定し、文書化し、テストし、(リリース)承認し、導入する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *システムのライフサイクルを通した変更の管理―システムの可用性及び処理のインテグリティを支援するために、システム及びその構成要素(インフラストラクチャー、データ、ソフトウェア及び手続)のライフサイクルを通したシステムの変更を管理するプロセスが実施される。*
	・ *変更の承認―開発の前にシステム変更を承認するプロセスが整備されている。*
	・ *変更の設計及び開発―システムの変更を設計し、開発するプロセスが整備されている。*
	・ *変更の文書化―システムの継続的な維持を支援し、また、システムユーザーが各自の責任を果たすことを支援するために、システム変更を文書化するプロセスが整備されている。*
	・ *システム変更の追跡―導入の前に、システム変更を追跡するプロセスが整備されている。*
	・ *ソフトウェアの設定―ソフトウェアの機能管理に使用される設定パラメーターを選択し、導入するプロセスが整備されている。*
	・ *システム変更のテスト-導入の前に、システム変更をテストするプロセスが整備されている。*
	・ *システム変更の承認―導入の前に、システム変更を承認するプロセスが整備されている。*
	・ *システム変更の配置―システム変更を導入するプロセスが整備されている。*
	・ *システム変更の識別及び評価―システム変更の影響を受けた目的は識別され、変更されたシステムの目的を達成する能力はシステム開発ライフサイクルを通じて評価される。*
	・ *インシデントの是正に必要なインフラストラクチャー、データ、ソフトウェア及び手続の変更の識別―継続して目的を達成するために、イン*

	シデントの是正に必要なインフラストラクチャー、データ、ソフトウェア及び手続の変更は識別され、そして、変更プロセスは識別時から開始される。
	・ *ＩＴテクノロジーの設定基準の作成―ＩＴ及び内部統制システムの設定基準は、作成され、維持される。*
	・ *緊急事態に必要となる変更の提供―緊急事態に必要となる変更（すなわち緊急に導入する必要がある変更）を承認し、設計し、テストし、許可し、導入するプロセスが整備されている。*
	機密保持に係る Trust サービス規準を使用する業務にのみ適用する追加の着眼点：
	・ *機密情報の保護―事業体は、機密保持に係る事業体の目的を達成するために、システムの設計、開発、テスト、導入及び変更プロセスの間、機密情報を保護する。*
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する追加の着眼点：
	・ *パーソナル・インフォメーションの保護―事業体は、プライバシーに係る事業体の目的を達成するために、システムの設計、開発、テスト、導入及び変更プロセスの間、パーソナル・インフォメーションを保護する。*
	リスク軽減策
CC9.1	***組織は、潜在的にビジネスが中断することに起因するリスクに対して、リスク軽減活動を識別し、選択し、開発する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *ビジネスの中断に対するリスク軽減策の検討―リスク軽減活動には、計画的な方針、手続、伝達、及び業務を中断するセキュリティ事象に対応し、それを低減し、そこから復旧する代替的な解決処理方法の整備が含まれる。それらの方針及び手続には、対応・低減・復旧への取組の間、事業体の目的を達成するための、監視プロセス、情報と伝達が含まれる。*
	・ *リスクの財務への影響を軽減するための保険利用の検討―リスク管理活動では、事業体が目的を達成することができなくなるような財務上の損失があった場合、それを相殺するために保険を利用することが検討される。*
CC9.2	***組織は、ベンダー及びビジネス・パートナーに関連するリスクを評価し、管理する。***
	Trust サービス規準を使用する全ての業務に特に関連する以下の着眼点は、この規準に関する重要な特性を明示している。:

	・ *ベンダー及びビジネス・パートナーの契約に関する要件の確立―事業体は、ベンダー及びビジネス・パートナーの契約の具体的な要件を確立する。それらの要件には、(1)サービスの範囲と製品仕様書、(2)役割と責任、(3)コンプライアンス要件、(4)サービスレベルが含まれる。*
	・ *ベンダー及びビジネス・パートナーに関連するリスクの評価―事業体は、目的を達成するに当たり、ベンダー及びビジネス・パートナー（それら事業体のベンダー及びビジネス・パートナーを含む。）がもたらすリスクを、定期的に評価する。*
	・ *ベンダー及びビジネス・パートナーの管理に対する実行責任及び説明責任の割当て―事業体は、ベンダー及びビジネス・パートナーに関連するリスクの管理に対して、実行責任及び説明責任を割り当てる。*
	・ *ベンダー及びビジネス・パートナーとの伝達手順の制定―事業体は、ベンダー及びビジネス・パートナーに関連するサービス又は製品の問題に関する、伝達及び解決の手順を制定する。*
	・ *ベンダー及びビジネス・パートナーからの例外処理手続の制定―事業体は、ベンダー及びビジネス・パートナーに関連するサービス又は製品の問題に対して、例外処理手続を制定する。*
	・ *ベンダー及びビジネス・パートナーのパフォーマンスの評価―事業体は、定期的に、ベンダー及びビジネス・パートナーのパフォーマンスを評価する。*
	・ *ベンダー及びビジネス・パートナーの評価時に識別された問題への対処手続の導入―事業体は、ベンダー及びビジネス・パートナーとの関係において識別された問題に対処するための手続を導入する。*
	・ *ベンダー及びビジネス・パートナーとの関係を解消するための手続の導入―事業体は、ベンダー及びビジネス・パートナーとの関係を打ち切るための手続を導入する。*
	機密保持に係る Trust サービス規準を使用する業務にのみ適用する追加の着眼点：
	・ *ベンダー及びビジネス・パートナーからの機密保持コミットメントの入手―事業体は、機密情報にアクセスできるベンダー及びビジネス・パートナーから、事業体の機密保持コミットメント及び要件と整合する機密保持コミットメントを入手する。*
	・ *ベンダー及びビジネス・パートナーの機密保持コミットメントについての遵守状況の評価―事業体は、定期的に、及び必要に応じて、 ベンダー及びビジネス・パートナーによる事業体の機密保持コミットメント及び要件についての遵守状況を評価する。*
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する追加の着眼点：

	・ *ベンダー及びビジネス・パートナーからのプライバシー・コミットメントの入手—事業体は、パーソナル・インフォメーションにアクセスできるベンダー及びビジネス・パートナーから、事業体のプライバシー・コミットメント及び要件と整合するプライバシー・コミットメントを入手する。*
	・ *ベンダー及びビジネス・パートナーのプライバシー・コミットメントについての遵守状況の評価—事業体は、定期的に、及び、必要に応じて、 ベンダー及びビジネス・パートナーによる事業体のプライバシー・コミットメント並びに要件についての遵守状況を評価し、必要があれば是正措置を講じる。*
	可用性に関する追加規準
A1.1	***組織は、その目的を達成するように、キャパシティ要求を管理し、追加の処理能力の導入を可能にするために、システム構成要素（インフラストラクチャー、データ及びソフトウェア）の現在の処理能力と使用量を維持し、監視し、評価する。***
	可用性に係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *現在の使用量の測定—システム構成要素の使用量は測定され、キャパシティ管理の基準となる、また、キャパシティ制約により可用性が損なわれるリスクを評価する際に用いる。*
	・ *キャパシティの予測—システム構成要素の使用量の期待される平均及びピークは予測され、システムのキャパシティ及び関連する許容範囲と比較される。予測では、キャパシティの制約によるシステム構成要素の障害が検討される。*
	・ *予測に基づいた変更—システム変更の管理プロセスは、予測使用量がキャパシティの許容範囲を超えた場合に、開始する。*
A1.2	***組織は、その目的を達成するために、環境保護策、ソフトウェア、データのバックアッププロセス、復旧用のインフラストラクチャーを承認し、設計し、開発又は取得し、導入し、稼働させ、許可し、整備し、監視する。***
	可用性に係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *環境上の脅威の識別—リスク評価プロセスの一環として、経営者は、悪天候、環境制御システムの障害、放電、火災及び水害による脅威など、システムの可用性を損なう可能性のある環境上の脅威となる事象を識別する。*
	・ *検出対策の設計—環境上の脅威により発生する可能性がある異常を識別するための検出対策を導入する。*
	・ *環境保護の仕組みの導入及び整備—経営者は、環境上の事象を防止*

	し、軽減するための環境保護の仕組みを導入し、整備する。
	・ *異常を分析するためのアラートの導入―経営者は、環境上の脅威となる事象を識別するために、分析する要員に伝達するアラートを導入する。*
	・ *環境上の脅威となる事象への対応―環境上の脅威となる事象に対応し、それらの方針・手順の有効性を定期的に評価する手続が整備されている。これには、自動化された軽減システム（例えば、無停電電源システムや補助発電サブシステム）も含まれる。*
	・ *検出された環境上の脅威となる事象の伝達及びレビュー―検出された環境上の脅威となる事象は、システムの管理責任者に伝達され、レビューされる。必要に応じて、対応が講じられる。*
	・ *バックアップが必要なデータの決定―データは、バックアップの必要性を判断するために、評価される。*
	・ *データのバックアップの実施―データのバックアップ、バックアップの失敗を検出するための監視、及びそのような失敗の発生時の是正措置を開始する手続が整備されている。*
	・ *外部保管の対処―バックアップデータは、主たる保管場所から十分に離れた場所に保管され、双方のデータがセキュリティ上又は環境上の脅威となる事象から影響を受ける可能性は、適切なレベルに低減される。*
	・ *代替処理インフラストラクチャーの導入―通常処理のインフラストラクチャーが利用できなくなった場合に、代替のインフラストラクチャーの処理に移行するための対策を導入する。*
A1.3	***組織は、その目的を達成するために、システム復旧を支援する復旧計画の手続をテストする。***
	可用性に係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *事業継続計画に対するテストの導入―事業継続計画に対するテストは、定期的に実施される。テストには、(1)脅威の発生可能性及び重大性に基づいたテストシナリオの開発、(2)可用性を損ない得る事業体全体にわたり関連するシステム構成要素の検討、(3)重要な要員が従事できなくなる可能性を考慮したシナリオ、及び(4)テスト結果に基づいた継続計画及びシステムの修正が含まれる。*
	・ *バックアップの整合性及び完全性のテスト―バックアップ情報の整合性及び完全性は、定期的にテストされる。*
	機密保持に関する追加規準
C1.1	***組織は、機密保持に関する組織の目的を達成するように、機密情報を識別し、維持する。***
	機密保持に係る Trust サービス規準を使用する業務にのみ適用する以下の

	着眼点は、この規準に関する重要な特性を明示している。:
	・ *機密情報の識別―機密情報を受領又は作成した際に機密情報として識別及び指定するための手続、及び当該機密情報を保持する期間を決定するための手続が整備されている。*
	・ *機密情報の破棄防止―機密情報が特定の保持期間中に消去又は破棄されることを防ぐための手続が整備されている。*
C1.2	***組織は、機密保持に関する組織の目的を達成するように、機密情報を廃棄する。***
	機密保持に係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *破棄する機密情報の識別―保持期間の満了時に破棄する必要がある機密情報を識別するための手続が整備されている。*
	・ *機密情報の破棄―破棄する必要があると識別された機密情報を消去又は破棄するための手続が整備されている。*
PI1.1	処理のインテグリティに関する追加規準
	組織は、製品及びサービスの使用を支援するため、処理されたデータの定義並びに製品及びサービスの仕様を含む、処理に関する目的に関連する適切かつ良質な情報を取得又は作成し、利用し、伝達する。
	処理のインテグリティに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *情報の仕様を特定―事業体は、製品及びサービスの使用を支援するために必要な情報の仕様を特定している。*
	・ *製品又はサービスの使用を支援するために必要なデータの定義―データが、サービス若しくは製品の一部として提供されている、又は製品若しくはサービスに関連する報告義務の一部として提供されている場合：* *(1) データの定義が当該データの利用者にとって利用可能である。* *(2) データの定義には次の情報が含まれている。:* ・ *データに含まれている事象又は事例の母集団* ・ *データの各要素（例：フィールド）の内容（すなわち、データ要素が関係する事象又は事例。例えば、特定の日における最終取引で XYZ 株式会社の株式を売却するときの取引価格）* ・ *データの入手元* ・ *データ要素（例：フィールド）の測定単位* ・ *測定値の正確性/適切性/精度* ・ *各データ要素及びそれら要素の母集団に内在する不確実性又は信頼区間* ・*データが観察された日又はデータに関連する事象が発生した期間* ・ *上記の日及び期間に加えて、データ要素及び母集団に項目を含め*

	るか含めないかを決定するために使用した要因 *(3) 当該定義は完全かつ正確である。* *(4) データの説明では、データ自体には含まれていないデータの定義及び意図された目的（メタデータ）に整合する方法で、各データ要素及び母集団を理解するのに必要な全ての情報が特定されている。*
PI1.2	***組織は、製品、サービス及び報告が組織の目的を達成するように、完全性及び正確性に対する内部統制を含む、システム入力全般に関する方針及び手続を導入する。***
	処理のインテグリティに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ 入力処理の特性を定義―要件を満たすのに必要な入力処理の特性を定義する。
	・ 入力処理を評価―定義した入力要件への遵守状況について入力処理を評価する。
	・ システム入力の記録を作成及び維持―システム入力活動の記録が、完全、正確かつ適時に作成及び維持される。
PI1.3	***組織は、製品、サービス及び報告が組織の目的を達成するように、システム処理全般に関する方針及び手続を導入する。***
	処理のインテグリティに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ 処理の仕様を定義―製品又はサービス要件を満たすのに必要な処理の仕様を定義する。
	・ 処理活動を定義―要件を満たす製品又はサービスとなるように処理活動を定義する。
	・ 製造上のエラーの検知及び訂正―製造プロセスにおけるエラーは、適時に検知され、訂正される。
	・ システム処理活動を記録―システム処理活動が、完全、正確かつ適時に記録される。
	・ 入力の処理―入力は、定義された処理活動に従い承認されたとおりに、完全、正確かつ適時に処理される。
PI1.4	***組織は、組織の目的を達成する仕様に従い、出力を完全、正確、適時に利用可能にする又は提供するための方針及び手続を導入する。***
	処理のインテグリティに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ 出力の保護―出力は格納若しくは引渡しされる時点又はその両方の時点で仕様の充足を妨げるような出力の窃取、破棄、損傷又は悪化を阻止するように保護される。

	・ *意図された当事者だけに対する出力の配布―出力は意図された当事者だけに配布されるか、又は当該当事者だけが利用可能である。*
	・ *出力の完全かつ正確な配布―配布される出力の完全性、正確性及び適時性を提供するための手続が整備されている。*
	・ *システム出力活動の記録の作成及び維持―システム出力活動の記録が、完全、正確かつ適時に作成及び維持される。*
PI1.5	***組織は、組織の目的を達成するシステム仕様に従い、入力、処理中の項目、及び出力を完全、正確かつ適時に格納する方針及び手続を導入する。***
	処理のインテグリティに係るTrustサービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *格納された項目の保護―格納された項目は、仕様の充足を妨げるような出力の窃取、破棄、損傷又は悪化を阻止するように保護される。*
	・ *システム記録のアーカイブ及び保護―システム記録はアーカイブされ、当該アーカイブされた記録の使用を妨げるような窃取、破棄、損傷又は悪化を阻止するように保護される。*
	・ *データを完全かつ正確に格納―データを完全、正確かつ適時に格納するための手続が整備されている。*
	・ *システムストレージ活動の記録を作成及び維持―システムストレージ活動の記録が、完全、正確及び適時に作成及び維持される。*
	プライバシーに関する追加規準
P1.0	**プライバシーに関する目的の通知及び伝達に関するプライバシー規準**
P1.1	***組織は、プライバシーに関する組織の目的を達成するように、データ主体（本人）にプライバシー実務に関する通知を提示する。当該通知は、プライバシーに関する組織の目的を達成するように、パーソナル・インフォメーションの利用の変更を含む、組織のプライバシー実務の変更に関して、適時に更新され、データ主体（本人）に伝達される。***
	プライバシーに係るTrustサービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *データ主体（本人）への伝達―次に関する通知がデータ主体（本人）へ提示される。:* ・ *パーソナル・インフォメーションを収集する目的* ・ *選択と同意* ・ *収集したパーソナル・インフォメーションの種類* ・ *収集の方法 （例えば、クッキー又は他のトラッキング技法の利用）* ・ *利用、保持及び廃棄* ・ *アクセス* ・ *第三者への開示* ・ *プライバシーのためのセキュリティ*

	・ *品質（品質に関するデータ主体（本人）の責任を含む。）* ・ *モニタリング及び執行* *当該個人以外の情報源からパーソナル・インフォメーションが収集される場合は、当該情報源はプライバシー通知に記述される。*
	・ *データ主体（本人）への通知の提示―データ主体（本人）への通知は、 次のいずれかの時点で提示される。(1)パーソナル・インフォメーションが収集される時点若しくはその前、又はその後の可能な限り早い時点、(2)事業体のプライバシー通知が変更される時点若しくはその前、又はその後可能な限り早い時点、(3)パーソナル・インフォメーションが以前は特定されていなかった新しい目的のために利用される前。*
	・ *事業体及び活動を含む通知―事業体及び活動を含まれる客観的な記述が事業体のプライバシー通知に含まれる。*
	・ *明瞭かつ見やすい言葉の使用―事業体のプライバシー通知は、見やすく、明瞭な言葉を使用する。*
P2.0	**選択と同意に関するプライバシー規準**
P2.1	***組織は、パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関して利用可能な選択並びに各選択による影響があれば当該影響をデータ主体（本人）に伝達する。パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関する明示的同意は、必要な場合には、データ主体（本人）又はその他権限を付与された個人から取得される。当該同意は、プライバシーに関する組織の目的を達成するように、当該インフォメーションの意図した目的のためだけに取得される。パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関する黙示的同意が得られていると判断する組織の根拠は文書化される。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *データ主体（本人）への伝達―データ主体（本人）に、 (a)パーソナル・インフォメーションの収集、利用及び開示についてデータ主体（本人）にとり利用可能な選択、 (b)法令で別段の要求又は容認がなされる場合を除き、パーソナル・インフォメーションの収集、利用、開示をするには黙示的又は明示的同意が必要なことが通知される。*
	・ *同意の拒否又は撤回に伴う結果の伝達―パーソナル・インフォメーションが収集されるとき、データ主体（本人）には、パーソナル・インフォメーションの提供を拒否した場合による影響又は通知に明記された目的のためにパーソナル・インフォメーションを利用することへの同意を拒否若しくは撤回した場合による結果が通知される。*
	・ *黙示的又は明示的同意の取得―黙示的又は明示的同意は、パーソナル・インフォメーションが収集される時点若しくはその前又はその後可*

	能な限り早い時点で、データ主体（本人）から取得される。当該個人の同意で表明された選択は確認され、実行される。
	・ *新しい目的及び利用に係る同意の取得と文書化―以前に収集された情報が、プライバシー通知で以前に識別された目的以外のために利用される場合、新しい目的は文書化され、データ主体（本人）に通知され、当該新しい利用又は目的が開始される前に黙示的又は明示的同意が取得される。*
	・ *機微な情報に係る明示的同意の取得―機微なパーソナル・インフォメーションが収集、利用又は開示される場合には、法令で別段の要求がなされている場合を除き、データ主体（本人）から直接、明示的同意が取得される。*
	・ *データ転送に係る同意の取得―パーソナル・インフォメーションが、個人のコンピューター又は他の類似の機器へ移転される又はそれらから移転される前に、同意が取得される。*
P3.0	**収集に関するプライバシー規準**
P3.1	***パーソナル・インフォメーションは、プライバシーに関する組織の目的に沿って収集される。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *パーソナル・インフォメーションの収集の制限―パーソナル・インフォメーションの収集は、事業体の目的を達成するために必要な範囲に制限される。*
	・ *公正かつ合法的な手段による情報収集―パーソナル・インフォメーションの収集方法は、当該方法を実施するための承認を得る前に、(a)公正であること、脅迫又は騙しがないこと、及び(b)制定法、慣習法を問わず、パーソナル・インフォメーションの収集に関する全ての関連する法律を遵守する合法的なものであることを確認するために、経営者によってレビューされる。*
	・ *信頼できる情報源からの情報収集―経営者は、パーソナル・インフォメーションを第三者から収集する場合には、当該第三者（すなわち当該個人以外の情報源）が、公正かつ合法的に情報を収集する、信頼できる情報源であることを確認する。*
	・ *追加情報が取得される場合におけるデータ主体（本人）への通知―事業体がその利用のためにデータ主体に関する追加情報を作成又は取得する場合には、データ主体（本人）に通知する。*
P3.2	***明示的同意を必要とする情報に関し、組織は、プライバシーに関する組織の目的を達成するように、当該同意の必要性及びパーソナル・インフォメーションの要請に同意しない場合の影響を伝え、当該情報の収集前に同意***

	を取得する。
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *機微な情報に係る明示的同意の取得―機微なパーソナル・インフォメーションを収集、利用又は開示する場合には、法令で別段の要求がなされている場合を除き、データ主体（本人）から直接、明示的同意が取得される。*
	・ *情報保持のための明示的同意の文書化―機微なパーソナル・インフォメーションの収集、利用又は開示に係る明示的同意の文書は、プライバシーに関する（事業体）の目的に従い保持される。*
P4.0	利用、保持及び廃棄に関するプライバシー規準
P4.1	***組織は、パーソナル・インフォメーションの利用を、プライバシーに関する組織の目的において識別された利用目的だけに制限する。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *パーソナル・インフォメーションを意図した目的のためだけに利用―パーソナル・インフォメーションは、法令で別段の要求がなされている場合を除き、それが意図された収集目的のためだけに、黙示的又は明示的同意が得られた場合に限り、利用される。*
P4.2	***組織は、プライバシーに関する組織の目的に沿ってパーソナル・インフォメーションを保持する。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *パーソナル・インフォメーションの保持―パーソナル・インフォメーションは、法令で別段の要求がなされている場合を除き、定められた目的を達成するために必要な期間を超えて保持してはならない。*
	・ *パーソナル・インフォメーションの保護―特定された情報保持期間中に、パーソナル・インフォメーションが消去又は破棄されるのを防ぐための方針及び手続が整備されている。*
P4.3	***組織は、プライバシーに関する組織の目的を達成するように、パーソナル・インフォメーションを安全に廃棄する。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *削除要求の把握、識別及びフラグ付け―パーソナル・インフォメーションの削除要求は、プライバシーに関する事業体の目的を達成するように、把握されるとともに、当該要求に関連する情報が破棄のために識別され、フラグ付けられる。*
	・ *パーソナル・インフォメーションの廃棄、破壊及び削除―保持されな*

	くなったパーソナル・インフォメーションは、紛失、盗難、誤用又は未承認のアクセスを防ぐ方法で、匿名化、廃棄又は破壊される。
	・ *パーソナル・インフォメーションの破壊―破棄すると識別されたパーソナル・インフォメーションを消去又は破壊するための方針及び手続が整備されている。*
P5.0	**アクセスに関するプライバシー規準**
P5.1	***組織は、プライバシーに関する組織の目的を達成するように、識別及び認証されたデータ主体（本人）が保存されている自身のパーソナル・インフォメーションをレビューできるようにデータ主体（本人）にアクセス権限を付与し、要求を受けて、当該情報の物理的又は電子的コピーをデータ主体（本人）に提供する。アクセスを拒否する場合、プライバシーに関する組織の目的を達成するように、データ主体（本人）には、要求に応じて、拒否の旨とその理由が通知される。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *データ主体（本人）の身元認証―自身のパーソナル・インフォメーションへのアクセス権を求めるデータ主体（本人）の身元は、当該情報へのアクセス権を付与する前に認証される。*
	・ *データ主体（本人）による自身のパーソナル・インフォメーションへのアクセスの許可―データ主体（本人）は、自身のパーソナル・インフォメーションを事業体が保持するかどうかを決定することができ、かつ要求すれば、自身のパーソナル・インフォメーションへのアクセス権を得ることができる。*
	・ *合理的な期間内に理解可能なパーソナル・インフォメーションを提供―パーソナル・インフォメーションは、理解可能な形式で、合理的な期間内に、（もしあれば）合理的なコストでデータ主体（本人）に提供される。*
	・ *アクセス拒否時のデータ主体（本人）への通知―データ主体（本人）が自身のパーソナル・インフォメーションへのアクセスを拒否される場合、事業体は、法令で禁止されている場合を除き、拒否の旨及び当該拒否の理由を適時にデータ主体（本人）に通知する。*
P5.2	***組織は、プライバシーに関する組織の目的を達成するように、データ主体（本人）により提供された情報を基にパーソナル・インフォメーションを訂正、修正又は追加し、コミット又は要求に応じて、そうした情報を第三者に伝える。訂正要求を拒否する場合、プライバシーに関する組織の目的を達成するように、データ主体（本人）に拒否の旨及びその理由を通知する。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以

	下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *アクセス要求の拒否を伝達―データ主体（本人）に、自身のパーソナル・インフォメーションへのアクセス要求が拒否された理由、該当する場合は、そのアクセスを拒否する事業体の法的権利の根拠、及び当該拒否に抗弁できる個人の権利が法令で特に容認又は要求されている場合には、当該権利について、書面で通知する。*
	・ *データ主体（本人）がパーソナル・インフォメーションを更新又は訂正することの許可―データ主体（本人）は、事業体が保持しているパーソナル・インフォメーションを更新又は訂正することができる。事業体は、プライバシーに関する事業体の目的に沿うように、そのように更新又は訂正された情報を、これまでにデータ主体（本人）のパーソナル・インフォメーションを提供してきた第三者に提供する。*
	・ *訂正要求の拒否を伝達―データ主体（本人）に、パーソナル・インフォメーションの訂正要求が拒否された理由と当該拒否に抗弁できる方法を、書面で通知する。*
P6.0	開示及び通知に関するプライバシー規準
P6.1	***組織は、データ主体（本人）の明示的同意をもって、第三者にパーソナル・インフォメーションを開示する。当該同意は、プライバシーに関する組織の目的を達成するように、開示を行う前に取得される。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *プライバシー・ポリシーを第三者に伝達―パーソナル・インフォメーションの取扱いに関するプライバシー・ポリシー又はその他の特定の指示若しくは要求は、パーソナル・インフォメーションが開示される第三者に伝達される。*
	・ *適切な場合に限りパーソナル・インフォメーションを開示―パーソナル・インフォメーションは、法令で別段の要求がなされている場合を除き、それが収集又は作成された目的のためだけに、データ主体（本人）から黙示的又は明示的同意が得られた場合に限り、第三者に開示される。*
	・ *パーソナル・インフォメーションは適切な第三者に限り開示―パーソナル・インフォメーションは、事業体のプライバシー通知の関連箇所又はその他の具体的な指示若しくは要求に整合した方法でパーソナル・インフォメーションを保護することに事業体と合意した第三者に対してのみ、開示される。事業体は、当該第三者が合意の条件、指示又は要求を満たす有効な内部統制を有していることを評価するための手続が整備されている。*

	・ *新しい目的及び利用のためにパーソナル・インフォメーションを第三者に開示―パーソナル・インフォメーションは、データ主体（本人）から事前の黙示的又は明示的同意がある場合に限り、新しい目的又は利用のために第三者に開示される。*
P6.2	***組織は、プライバシーに関する組織の目的を達成するように、パーソナル・インフォメーションの承認された開示について、完全、正確かつ適時な記録を作成し、保持する。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *承認された開示の記録を作成及び保持する―事業体は、パーソナル・インフォメーションの承認された開示について、完全、正確かつ適時な記録を作成し、保持する。*
P6.3	***組織は、プライバシーに関する組織の目的を達成するように、パーソナル・インフォメーションの発見又は報告された未承認の開示（違反を含む。）について、完全、正確かつ適時な記録を作成し、保持する。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *発見又は報告された未承認の開示に関する記録を作成及び保持―事業体は、発見又は報告されたパーソナル・インフォメーションの未承認の開示について、完全、正確かつ適時な記録を作成し、保持する。*
P6.4	***組織は、プライバシーに関する組織の目的を達成するように、パーソナル・インフォメーションへのアクセス権を有するベンダー及び他の第三者から、プライバシー・コミットメントを取得する。組織は、ベンダー及び他の第三者の遵守状況を定期的かつ必要に応じて評価し、必要な場合は是正措置を講じる。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *パーソナル・インフォメーションは適切な第三者に限り開示―パーソナル・インフォメーションは、事業体のプライバシー通知の関連箇所又はその他の具体的な指示若しくは要求に整合した方法でパーソナル・インフォメーションを保護することに事業体と合意した第三者に対してのみ、開示される。事業体は、当該第三者が合意の条件、指示又は要求を満たす有効な統制を有していることを評価するための手続が整備されている。*
	・ *第三者によるパーソナル・インフォメーションの誤用に対する是正措置―事業体は、事業体からパーソナル・インフォメーションの移転を受けている第三者による当該情報の誤用に対して、是正措置を講じる。*

P6.5	*組織は、パーソナル・インフォメーションへのアクセス権を有するベンダー及び他の第三者から、パーソナル・インフォメーションの未承認の開示が実際に発生した場合又はその発生が疑われる場合には、組織に通知することのコミットメントを取得する。そうした通知は、プライバシーに関する組織の目的を達成するように、確立されたインシデント対応手続に従って、適切な要員に報告され、対処される。*
	プライバシーに係るTrustサービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *第三者によるパーソナル・インフォメーションの誤用に対する是正措置―事業体は、事業体からパーソナル・インフォメーションの移転を受けている第三者による当該情報の誤用に対して、是正措置を講じる。*
	・ *未承認の開示が実際に発生又はその発生が疑われる場合の報告―パーソナル・インフォメーションの未承認の開示が実際に発生した場合又はその発生が疑われる場合には、事業体に報告することのコミットメントをベンダー及びその他の第三者から入手するためのプロセスが存在する。*
P6.6	*組織は、プライバシーに関する組織の目的を達成するように、違反及びインシデントについて、その発生によって影響を受けるデータ主体（本人）、規制当局及びその他に通知する。*
	プライバシーに係るTrustサービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *第三者によるパーソナル・インフォメーションの誤用に対する是正措置―事業体は、事業体からパーソナル・インフォメーションの移転を受けている第三者による当該情報の誤用に対して、是正措置を講じる。*
	・ *違反及びインシデントに関する通知―プライバシーに関する事業体の目的を達成するように、違反及びインシデントについて、その発生により影響を受けるデータ主体（本人）、規制当局及びその他に通知を行うプロセスが事業体に存在する。*
P6.7	*組織は、プライバシーに関する組織の目的を達成するように、データ主体（本人）の要求に応じて、保有しているパーソナル・インフォメーションの記録及び当該データ主体（本人）のパーソナル・インフォメーションが開示された記録を提供する。*
	プライバシーに係るTrustサービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *パーソナル・インフォメーションの種類及び処理プロセスの識別―パーソナル・インフォメーション及び機微なパーソナル・インフォメーションの種類、並びに関連するプロセス、システム及び当該情報の処理に関わる第三者が識別されている。*

	・ *インフォメーションに関する要求の把握、識別及び伝達―保有しているパーソナル・インフォメーションの記録及びデータ主体（本人）のパーソナル・インフォメーションが開示された記録を求めるデータ主体（本人）からの要求は、プライバシーに関する事業体の目的を達成するように、把握され、当該要求に関連する情報が識別され、データ主体（本人）に伝達される。*
P7.0	**品質に関するプライバシー規準**
P7.1	***組織は、プライバシーに関する組織の目的を達成するように、正確、最新、完全かつ適切なパーソナル・インフォメーションを収集し、維持する。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *パーソナル・インフォメーションの正確性及び完全性の確保―パーソナル・インフォメーションは、その利用目的に照らして正確かつ完全である。*
	・ *パーソナル・インフォメーションの適切性の確保―パーソナル・インフォメーションは、その利用目的に照らして適切である。*
P8.0	**モニタリング及び執行に関するプライバシー規準**
P8.1	***組織は、データ主体（本人）及びその他からの問合せ、苦情及び紛争争議を受付し、対処し、解決し、その解決策を伝えるためのプロセスを備えるとともに、プライバシーに関する組織の目的を達成するように遵守状況を定期的にモニターしている。識別された不備に関して訂正及びその他の必要な措置が適時に講じられる。***
	プライバシーに係る Trust サービス規準を使用する業務にのみ適用する以下の着眼点は、この規準に関する重要な特性を明示している。:
	・ *データ主体（本人）への伝達―データ主体（本人）は、問合せ、苦情及び紛争について事業体に連絡する方法を伝えられている。*
	・ *問合せ、苦情及び紛争への対処―問合せ、苦情及び紛争に対処するためのプロセスが整備されている。*
	・ *紛争解決及び解決手段の文書化と伝達―各苦情は対処され、解決策が文書化されるとともに個人に伝えられる。*
	・ *遵守状況のレビュー結果の文書化と報告―プライバシーに関する事業体の目的の遵守状況は、レビュー及び文書化されるとともに、当該レビューの結果は経営者に報告される。問題が識別された場合、是正計画が作成され、実施される。*
	・ *不遵守の場合の文書化及び報告―プライバシーに関する事業体の目的を遵守していない場合は、文書化及び報告されるとともに、必要な場合は、是正措置及び懲戒処分が適時に行われる。*

	・ *継続的モニタリングの実施―パーソナル・インフォメーションに対する内部統制の有効性をモニタリングするため、及び必要な場合は、適時な是正措置を講じるため継続的な手続が実施される。*

経過措置ガイダンス

25. 本書に表示される 2017 年版 Trust サービス規準は、TSP セクション 100 として規定される。2016 年に公表された既存の Trust サービス規準は、2018 年 12 月 15 日まで TSP セクション 100A として利用可能になる。同日以降は、2016 年規準は廃止されたとみなされる。業務実施者は、移行期間中（2017 年４月 15 日から 2018 年 12 月 15 日）、その報告書において 2016 年又は 2017 年どちらの Trust サービス規準が使用されたのか、区別しなければならない。

26. さらに、AICPA は、報告書利用者が確実に参照可能となるようにするために、TSP セクション 100A-1 に規定される 2014 年 Trust サービス規準を 2018 年３月 31 日まで引き続き参照可能とする。この規準は、2016 年 12 月 15 日以降に終了する期間の業務実施者の報告書に関しては更新されているとみなされていた。

付録Ａ　用語集

パーソナル・インフォメーションへのアクセス権：

組織が保持するパーソナル・インフォメーションを閲覧する権利。この権利は、情報を更新又は修正する権利によって補足される。アクセス権は、ID とデータの関係を定義する。すなわち、誰がどのデータに何ができるのか。アクセス権は「公正な情報慣行の原則（FTC 原則）」の一つである。個人は、企業がどのようなパーソナル・インフォメーションを持っているのか、その情報がどのように使われているかを知ることができなければならない。個人は、そのような記録内の誤った情報を訂正することができなければならない。

アーキテクチャ：

論理的構成要素を含むシステム構成のデザイン、及びコンピューター、そのオペレーティング・システム、ネットワーク、その他の要素の論理的相互関係

認証：

ある実体（利用者、プロセス又はデバイス）から主張される若しくは想定される身元又はその他の属性を検証するプロセス、若しくはデータのソース及びインテグリティを検証するプロセス

承認：

アクセス権を付与する権限を有している人が、利用者、プログラム又はプロセス

にアクセス権を付与するプロセス

理事会又は取締役会：

企業の戦略的方向性の監視の責任及び企業の説明責任に関する義務を負う個人（による会議体）。企業の性質にもよるが、そうした責任は、法人の場合には取締役会又は監督機関、非営利法人の場合には評議会、政府系機関は理事会又は委員会、パートナーシップの場合には無限責任社員、中小企業の場合はオーナーが担う可能性がある。

ビジネス・パートナー：

単なるベンダーではなく、企業の事業の取引に一定程度の関与を持ち、企業といかなる度合いにおいても協力することに同意する個人又は事業体（及びその従業員、例えば、パーツを提供する別の企業と協力するコンピューター・メーカーなど）。

収集：

（例えば、インターネット上の書式又は登録フォームの提出を介して）個人から直接取得又はビジネス・パートナーなど別の当事者から、パーソナル・インフォメーションを取得するプロセス

コミットメント：

一つ以上のシステムパフォーマンスに関係して経営者が作成する顧客に対する宣言。コミットメントは、個別の契約、標準契約、サービスレベルアグリーメント又は公表された声明書（例えば、セキュリティ実務声明）を通じて伝達される。個々のコミットメントは、一つ以上の Trust サービス・カテゴリーに関連するかもしれない。業務実施者は、報告する原則に関係するコミットメントのみを検討する必要がある。コミットメントは、以下を含む様々な形式を取るかもしれない。

- 計算に使用されるアルゴリズムの仕様
- システムを利用できる時間
- 公表されたパスワード標準
- 保存された顧客データの暗号化に使用される暗号化標準

構成要素：

統制環境、リスク評価、統制活動、情報と伝達及びモニタリング活動を含む、内部統制の五要素の一つ。

コンプロマイス（不正侵入、不正使用）：

結果として生じる(1)システムの処理上のインテグリティ又は可用性若しくは(2)システム入出力のインテグリティ又は可用性の毀損を含む、情報の機密保持、インテグリティ又は可用性の喪失を指す。

契約者：

契約条件に従って企業にサービスを提供することに従事する、従業員以外の個人

統制：

内部統制の一環となる方針又は手続。次の五つの COSO 内部統制構成要素のそれぞれに統制は存在する。統制環境、リスク評価、統制活動、情報と伝達及びモニタリング活動である。

統制活動：

目的達成のリスクを低減する経営者の指令が確実に実行されるようにするための方針及び手続を通じて定められる行為

同意：

このプライバシー要件は、公正な情報慣行の目的の一つです。法的に要求されない限り、個人は個人データの収集を防止することができなければならない。個人が自分の情報の使用又は開示について選択権を有する場合、同意は個人が使用又は開示の許可を与える方法です。同意は明示的（例えば、オプトイン）又は黙示的（例えばオプトアウトしていない。）である可能性がある。

同意の二つのタイプ

(1) 明示的同意

当事者間の積極的なコミュニケーションによって、個人とデータ管理者の承諾を「表明する」という要件

(2) 黙示的同意

同意が合理的に個人の行為又は不作為から推定される場合

COSO：

トレッドウェイ委員会支援組織委員会(Committee of Sponsoring Organizations of the Treadway Commission)。COSO は、五つの民間部門組織の共同イニシアティブであり、企業のリスク管理、内部統制及び不正抑止に関するフレームワーク及びガイダンスの開発を通じてソートリーダーシップを提供する。(www.coso.org 参照)

サイバーセキュリティ目的：

企業の全体的な事業目的の達成に影響を及ぼすサイバーセキュリティのリスクに対処する目的（コンプライアンス、報告及びオペレーション上の目的を含む。）

サイバーセキュリティ・リスク管理検証業務：

(a)企業のサイバーセキュリティ・リスク管理プログラムに関する経営者の記述が記載規準に従って表示されているか否か、(b)当該プログラムの内部統制がコン

トロール規準に基づいて企業のサイバーセキュリティ目的を達成するために有効か否かに関する報告を行う検証業務。サイバーセキュリティ・リスク管理検証業務は、証明基準及びAICPAのサイバーセキュリティ・ガイドに従って実施される。

デザイン：

COSOの内部統制の定義に用いられるように、内部統制システム設計は、企業の目的を達成に合理的な保証を与えることを意図されている。

データ主体（本人）：

パーソナル・インフォメーションを収集される個人

開示：

情報を保有している企業以外への情報の公表、転送、アクセスの提供又は他の方法で明かすこと。開示は、しばしば、共有及び転送（onward transfer）という用語と互換的に用いられる。

廃棄：

企業がデータ若しくは情報を削除又は破棄する方法に関するデータライフサイクルの段階

環境保護策：

情報システムの物理的な部分（例えば、火災、洪水、風、地震、電力サージ又は停電からの保護）に対する損害のリスクを検出、防止、及び管理するために企業が実施する内部統制及びその他の活動

組織/事業体：

特定の目的に向けて設立されたいかなる規模の法人組織又はビジネスモデル。法人組織には例えば、企業、非営利組織、政府機関又は学術機関などが挙げられる。ビジネスモデルは、地理的市場による業績のさらなる区分又は合算を伴う、製品やサービス別、部門又は営業活動単位が基になり得る。

全社的：

事業体組織全体を通して適用される活動として、全社的統制が最も一般的

外部ユーザー：

情報システムに接することを、企業経営者が承認した企業の職員以外の利用者、顧客又はその他の個人

情報及びシステム：

その利用、処理、伝達、保存の間の電子的な形式の情報（電子情報）及び情報を利用、処理、送信又は転送及び保存するシステムを指す。

情報資産：

データ及び、それに関連するソフトウェア及びインフラストラクチャーで情報を処理、伝達及び保存するのに利用するもの

インフラストラクチャー：

サーバー、ストレージ及びネットワーク要素を始めとする、全体的なＩＴ環境を支える物理的又は仮想的な資源の集合体

固有の限界：

全ての内部統制システムに関する限界。限界は、内部統制の前提条件、組織/事業体の統制の及ばない外部事象、人間の判断の限界、機能しなくなるという現実及び経営者による無効化及び共謀の可能性に関係する。

内部統制：

業務、報告及びコンプライアンスに関する目的の達成に関し合理的な保証を与えるために整備された取締役会、経営者及びその他の要員が実施するプロセス

経営者による無効化：

個人的な利益、また、事業体の財務状態又はコンプライアンス状況をよく見せようと不適切な目的で、規定されているポリシー又は手続を経営者が無効にすること

外部委託サービス・プロバイダー：

企業の目的を達成するために特定のビジネスプロセス、オペレーション又はコントロールが必要になるときに、企業の代わりにそのビジネスプロセス、オペレーション又はコントロールを実施するサービス・プロバイダー・ベンダー

パーソナル・インフォメーション：

識別可能な個人に関する、又は関連する情報若しくは成り得る情報

方針：

統制を有効にするために何をすべきかに関する経営者又は取締役会構成員の声明。そうした声明は文書化され、コミュニケーションにおいて明示的に述べられ、又はその他の行為及び決定を通じて黙示的に示される。方針ポリシーが手続の基礎になる。

プライバシー・コミットメント：

パーソナル・インフォメーションを処理するシステムのパフォーマンスに関する経営者の宣言。プライバシー・コミットメントは、書面による同意書、標準化された契約書、サービスレベルアグリーメント又は公表された声明書（例えば、プライバシー実務声明）を通じて伝達される。さらに、プライバシー・コミットメントは、提供されているサービスの様々な側面について、以下を含むことがある。

- システムによって処理される情報の種類
- 従業員、第三者及び情報にアクセスできる他の人
- 同意なしに情報を処理できる条件

以下は、プライバシー・コミットメントの例示である。

- 組織は、データ主体（本人）の同意を得ずに情報を処理又は転送しない。
- 組織は、６か月に１回、又は組織のビジネスポリシーに変更があったときに、顧客にプライバシー通知を提供する。
- 組織は、顧客からの要求を受けてから 10 営業日以内にアクセス要求に応答する。

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から個人への、(1)収集する情報の性質とその情報をどのように使用、保持、開示、廃棄又は匿名化するかに関する方針及び(2)これらの方針に従うことをコミットする、書面による伝達。プライバシー通知には、情報収集の目的、個人がパーソナル・インフォメーションに関連して保持している選択肢、当該情報の安全性、個人のパーソナル・インフォメーションに関する照会、苦情、紛争に関する企業への連絡方法などの情報も含まれる。ユーザー企業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、当該個人にプライバシー通知が提供される。

報告書利用者：

AT-C セクション 205、検証業務（AICPA、職業的基準書）に準拠した業務実施者の報告書の想定利用者。一般目的報告書では幅広い報告書利用者が存在するが、AT-C セクション 205 パラグラフ 64 にしたがって制限される報告書に関しては、限られた特定の当事者のみが存在する。

保持：

企業が将来の使用や参照のために、情報をどのくらいの期間格納するかに関するデータライフサイクルの段階

リスク：

ある事象が発生し目的の達成に悪影響を及ぼす可能性

リスク対応：

リスクを受容する、回避する、低減する、又は共有する決定

リスク許容度：

目的達成に向けたパフォーマンスに対応して受容可能な変化の度合

セキュリティ事象：

内部又は外部の当事者による、不正アクセス又は不正利用の既遂又は未遂から生じる出来事で、情報又はシステムの可用性、インテグリティ又は機密保持を損なう、また、損なう可能性があり、その結果、情報の許可されない開示又は窃盗につながる、又はシステムに損傷をもたらす可能性があるもの。セキュリティ・インシデントは、情報資産及びリソースを保護するために企業側での措置が求められるセキュリティ事象である。

セキュリティ・インシデント：

情報資産及びリソースを保護するために、組織側で措置が求められるセキュリティ事象

上級経営者：

最高経営責任者又はそれに相当する組織のリーダー及び上級経営陣

サービス・プロバイダー：

組織にサービスを提供する契約を結ぶ（サービス組織などの）ベンダー。サービス・プロバイダーには外部委託サービス・プロバイダー並びに庶務、法律及び監査サービスなどのビジネス機能も含まれる。

SOC 2®業務：

受託会社のシステムに関する経営者の記述書の適正性、記述書に含まれている内部統制の設計の適合性、タイプ２の業務では、それらのコントロールの運用上の有効性を報告する検証業務。この業務は、証明基準及び AICPA のガイド「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、機密保持及びプライバシーに関連する内部統制の報告（SOC2®）」に従って実施される。

SOC 3®業務：

一つ以上の Trust サービス・カテゴリーに関連するシステムに対する企業の内部統制のデザインと運用の有効性を報告する保証業務

利害関係者：

株主、事業体が事業活動を行う地域社会、従業員、顧客及びサプライヤーなど、事業により影響を受ける当事者

システム：

経営者の特定の要求事項に従って、一つ以上の特定の事業目的（例えばサービス提供又は製品の製造）を達成するために、一体で稼働するようデザイン、実装、運用されるインフラストラクチャー、ソフトウェア、人、プロセス及びデータを指す。

システムの境界：

機能を実行し、サービスを提供するために必要な、企業のインフラストラクチャー、ソフトウェア、要員、手順及びデータの特定の側面。複数の機能又はサービスのシステムが、その側面、インフラストラクチャー、ソフトウェア、要員、手順及びデータを共有する場合、システムは一部重複するが、各サービスのシステムの境界は異なる。機密保持とプライバシー規準に関係する業務において、システムの境界は、明確に定義されたプロセスと非公式の一時的な手順の中で機密情報とパーソナル・インフォメーションのライフサイクルに関連する全てのシステム構成要素を最低限カバーしている。

システム構成要素：

システムの個々の要素を指す。システム構成要素は以下の五つのカテゴリーに区分される。インフラストラクチュアー、ソフトウェア、要員、手順及びデータである。

システム要求事項：

顧客に対する企業のコミットメント、法規制やビジネス又は業界団体などの業界に関連する産業別のガイドラインを充足するために、システムがどのように機能すべきかに関する仕様。要求事項は、しばしば企業のシステムポリシーと手続、システム設計文書、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、下記のとおりである。

- 政府の銀行規則で確立された従業員の指紋採取とバックグランドチェック
- 業務設計書で定義されたシステム入力における認められた値に制限された入力編集
- セキュリティポリシー・マニュアルに文書化された就業者の論理的アクセスの定期的なレビューとしての許容される最大の間隔
- SOAP（Simple Object Access Protocol）のように、業界又は他の組織で設定された全ての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(HIPAA)」の下のセキュリティ要求事項

システム要求事項は、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企業のコミットメントから生ずるかもしれない。例えば、データエントリーとデータ承認の間の職務の分離をプログラムに基づいて実施す

るコミットメントは、ユーザーアクセス管理に関するシステム要求を作成する。

第三者：

事業体とその従業員以外の個人又は組織。顧客、ベンダー、ビジネス・パートナーやその他も第三者となることがある。

Trust サービス：

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わる一連の規準を基に提供される職業的保証業務と助言業務

未承認のアクセス：

情報又はシステム構成要素への、(a)経営者に指定された要員による承認がなされていないアクセス、及び(b)業務分掌、守秘義務のコミットメントを無視した、若しくは経営者が承認したレベル以上に情報又はシステム構成要素に対するリスクを高めることになる、その他の意に反したアクセス（すなわち、アクセスは不適切）

ベンダー：

事業体への財又はサービスの提供を依頼される個人又は事業（及びその従業員）。ベンダーが提供するサービスに応じて（例えば、企業のサイバーセキュリティ目的を達成するのに必要となる一定の統制を企業に代わり実施する場合）、それはまた、サービス・プロバイダーになる場合もある。

以　上