ＩＴ委員会研究資料第９号

Trust サービス原則、規準及びその例示（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2014 年版の更新）

平成29年11月 8 日
日本公認会計士協会

TSP セクション 100 を改訂し、TSP セクション 100A の付録Ｃ「一般に公正妥当と認められたプライバシー原則」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係る適合する Trust サービス原則と規準である。TSP セクション 100 の規準は、2016 年 12 月 15 日以降終了する期間から適用し、早期適用を妨げない。TSP セクション 100A は 2018 年３月 31 日まで更新された文書として有効である。業務実施者は、報告書と確認書に使用した規準のセットがどれであったかを特定する必要がある。

（訳者注：「原則、規準、内部統制及びリスク」において、“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、米国公認会計士協会が「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係る Trust サービス原則及び規準

はじめに

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、システムのセキュリティ、可用性及び処理のインテグリティ、並びにシステムによって処理される情報の機密保持とプライバシーに関連する内部統制を評価する際に使用する一連の原則と規準（Trust サービス原則と規準）を開発した。本書では、システムは、経営者の特定した要求事項に従って特定の経営目標（例えば、サービスの提供、製品の生産）を達成するために、デザインされ、導入され、運用される。システム構成要素は、以下の五つのカテゴリーに分類できる。

- インフラストラクチャー：物理的構造物、ＩＴ及びその他のハードウェア（例えば、設備、コンピュータ、機器、携帯端末及び通信ネットワーク）
- ソフトウェア：アプリケーション・プログラムとそれをサポートするＩＴシステム・ソフトウェア（オペレーティング・システム、ミドルウエア及びユーティリティ）
- 要員：システムのガバナンス、運用及び利用に関与する要員（開発者、運用担当者、企業ユーザー、外注業者及び管理者）
- プロセス：自動又は手動の手続
- データ：システムにより利用又は処理された取引の流れ、ファイル、データベース、テーブル及び出力

２．本書は、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関連する内部統制の有効性を評価する Trust サービス原則と規準を提供する。企業の経営者は、システムの内部統制を評価する際に原則と規準を利用し、又は内部統制に関連する報告やコンサルタント業務の提供を受けるために、公認会計士と契約することができる。

３．証明業務に関する AICPA の基準書[1]（一般に証明基準と言われる。）の下で実施される証明サービスは、検証、レビュー[2] 及び合意された手続業務を含んでいる。証明基

---

[1]本文書作成時点では、AICPA の監査基準委員会（ASB）は、証明業務基準（SSAE 又は証明基準）のクラリティ対応を完了し、SSAE 第 18 号、証明基準：クラリティ版を公表すると見込まれる。
ASB は、SSAE 第 18 号が 2016 年 4 月に入手可能となり、業務実施者の 2017 年 5 月 1 日以降の報告書から有効になると想定している。

[2]一般に、レビュー業務は中程度の保証の水準(すなわち、消極的保証)を提供するように設計され、質問と分析的手続の実施から構成される。しかしながら、アシュアランスサービス・エグゼクティブコミッティーは、業務実施者が通常、特定の法律、規制、規則、契約又は助成金の要求事項である企業の内部統制やコンプライアンスについて意味のある分析的手続を実施できていないと考えており、また、レビュー業務を基礎として質問の手続と統合して実施する他の手続を特定できるか不確実である。また、この不確実性のため、業務実施者の手続の性質と範囲に関する誤解により、レビュー報告書のユーザーは、より大きなリスクにさらされる。したがって、Trust サービスに関連するレビュー業務の実現可能性は不確実である。

準では、証明業務を実施する公認会計士は、業務実施者として知られている。検証業務では、特定された一連の規準と関連して、主題又は主題に関する記述書について意見を表明する報告書を業務実施者は提供する。例えば、システムの内部統制が処理のインテグリティと機密保持に関する Trust サービス規準を満たすために有効に運用されていたかどうかに関して業務実施者は報告することができる。合意された手続業務では、業務実施者は、意見を表明することなく、特定の関係者と合意した手続を実施し、その結果を報告する。検証業務は、証明基準の AT セクション 101、証明業務に準拠して実施され、そして、合意された手続業務は、AT セクション 201、合意された手続業務に従って実施される（AICPA、職業的基準)。

４．以下は、業務実施者が、Trust サービス原則と規準を使用して検証・報告することができる主題の種類である。

・　『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受託会社の内部統制に関する報告（SOC2®)』に関する AICPA ガイド（2015 年７月１日）のパラグラフ 1.26 の記述（及びパラグラフ 1.27 のプライバシーに関する内部統制に関する記述）に関する規準を使用して評価した、一つ又は複数のセキュリティ、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の Trust サービス原則に関して記載した受託会社のシステムの記述書の表示の適正性、関連する Trust サービスの規準を充足する記述書に含まれる内部統制のデザインの適切性及び特定の期間を通じてこれらの Trust サービスの規準を満たす内部統制の運用の有効性（タイプ２SOC 2 業務)。

　内部統制の運用の有効性に関する意見を含むタイプ２SOC 2 業務には、業務実施者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１SOC 2 業務は、タイプ２SOC 2 業務と同じ主題に対処する事になるが、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、業務実施者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。

・　一つ又は複数のセキュリティ、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の Trust サービス原則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、業務実施者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。

・　受託会社以外の企業の一つ又は複数のセキュリティ、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の Trust サービス原則に関連するシステムに対する内部統制のデザインと運用の有効性。

・　一つ又は複数のセキュリティ、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の Trust サービス原則に関連する Trust サービスの規準を充足するシステムに係る企業の内部統制のデザインの適切性（解釈指針第７号、「内部統制のデザインに関する報告」、AT セクション 101、証明業務[AICPA、職業的基準、AT 第 9101 号、パラグラフ 59-69]は、このタイプの業務の背景を説明しており、通常はシス

テムの導入前に実行される)。

5．企業が顧客に提供することが合意されたサービスの詳細（例えば、何を、どのように、いつ提供されるか。）は、書面による契約、サービスレベルアグリーメント、又は声明書（例えば、プライバシー通知）に含まれる。 Trust サービス原則と規準は、そのような合意をコミットメントとして扱う。一部のコミットメントは全ての顧客に適用される（ベースラインコミットメント）一方で、他のコミットメントは、個々の顧客のニーズを満たすように設計されており、ベースラインコミットメントを満たす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。顧客に対する企業のコミットメントを満たすためにシステムがどのように機能すべきか、また関連する法律、規則又は業界団体などの産業別のガイドラインに関係するシステム仕様は、Trust サービスの原則と規準においてシステム要求事項として言及されている。 Trust サービスの規準の多くは、コミットメント及びシステム要求事項について言及している。例えば、

> CC1.4 企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及びシステム要求事項を充足可能とする、行動規範を確立し、従業員選考手続（バックグランドチェックを含む。）を導入し、実行手続を行っている。

経営者は、そのコミットメントを達成し、システム要求事項を満たすことができる方法でシステムを維持し、運用する責任がある。

6．Trust サービス業務は、報告対象となる原則について法令、規則、契約及び合意書に対する企業の遵守状況や遵守に関する内部統制について、業務実施者に報告を求めていない。もし、業務実施者が、企業の内部統制の運用の有効性に関する報告（例えば、AT セクション 101 に従ったプライバシー業務）と併せて、法令、規則、契約及び合意書の遵守状況の報告に関する契約をした場合、その遵守状況に関する業務は、AT セクション 601、遵守証明（AICPA、職業的基準）に準拠して実行される。

7．コンサルティング業務には、企業の経営者の意思決定のため検討及び使用される発見事項及び推奨項目の提供が含まれる。業務実施者は、この業務の主題に対して、意見の表明や結論の形成をしない。一般に、作業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、コンサルティング業務：定義と基準（AICPA、職業的基準）に従う。

原則、規準、内部統制及びリスク

8．Trust サービス原則は、経営者の目的の達成を支援するシステムの属性を表す。

9．それぞれの原則について、主題を測定し、表示するために利用されるとともに業務実施者が主題を評価することに対してベンチマークとして有用で詳細な規準がある。適切な規準の属性は以下のとおりである。

- 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尺度を許容せねばならない。
- 完全性：規準は、主題についての意見を覆しかねない関連要因を見逃さないように、十分に完全なものでなければならない。
- 関連性：規準は、主題に関連していなければならない。

10. ASEC は、各原則の Trust サービスの規準は、共通規準を含め、適切な規準の属性の全てを有すると結論を下した。適切であることに加えて、AT セクション 101 は、業務実施者の報告書の利用者にとって、規準が利用可能であることが必要であると示している。原則と規準の公表は、その規準を利用者にとって利用可能にする。

11. Trust サービス原則と規準は、柔軟かつ利用者と経営者の事業及び保証のニーズを充足するように設計されている。したがって、業務実施者は、一つの原則、複数の原則又は全ての原則に関連する業務を契約するかもしれない。

12. システムの運用環境、顧客及び第三者へのコミットメント、システムの運用及び保守に伴う責任、及びシステムのコンポーネントの性質により、規準が充足されないリスクが生じる。これらのリスクは、効果的に運用されている場合に規準が充足されていることの合理的な保証を提供する適切に設計された内部統制の実施を通じて対処される。各システムとそれが運用される環境は一意なため、リスクに対処するために必要な規準と内部統制を満たすリスクの組合せも一意になる。システムのデザインと運用の一部として、企業の経営者は、規準が満たされない特定のリスクとそれらのリスクに対処するために必要な内部統制を特定する必要がある。付録Ｂ「リスク及び内部統制の例示」は、規準を満たすことを妨げるリスク及びそれらのリスクに対処するための内部統制の具体例を提供する。それらの具体例は、どのような企業にも適切であること、規準に対応するリスクやそれらのリスクに対処するために必要な内部統制の全てを含むことを意図していない。

Trust サービス原則

13. Trust サービス原則は以下のとおりある。 [3]

[3] SysTrust、SysTrust for Service Organizations 及び WebTrust は、Trust サービス原則と規準に基づいて、AICPA 及びカナダ勅許会計士協会（CICA）によって開発された特定の商標を付けられた保証サービスの提供である。業務実施者が、これらの登録されたサービスマークを使用するには、CICA のライセンスを受けなければならない。サービスマークは、適正意見を表明する業務についてのみ発行できる。ライセンスの詳しい情報に関しては、www.webtrust.org/を参照。

a. セキュリティ：システムは、企業のコミットメントやシステム要求事項を満たすように、未承認のアクセス、利用又は変更に対して保護されている。

セキュリティ原則は、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関する企業のコミットメント及びシステム要求事項を企業が満たすように、論理的及び物理的アクセス管理を通じてシステム資源を保護することを意味する。システムのセキュリティの内部統制は、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、利用、変更、破壊や開示を予防又は発見する。

b. 可用性：システムは、企業のコミットメントやシステム要求事項を満たすように、操作でき、かつ利用できる。

可用性原則は、契約、SLA やその他の合意書でコミットした、システム、プロダクト又はサービスのアクセシビリティを意味する。この原則自身は、システム可用性について、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。可用性原則は、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、運用、モニタリング及び維持のためのシステムの利用可能性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、企業のコミットメントやシステム要求事項を満たすように、完全、正当、正確、タイムリー、かつ承認されている。

処理のインテグリティ原則は、システム処理の完全性、正当性、正確性、適時性と承認について言及する。処理のインテグリティは、そのシステムが存在する目標や目的を達成すること、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扱う。処理のインテグリティは、システムによって受け取られ、保存された情報が完全に、正当に、正確に、適時に承認されている事を、自動的には示さない。システムは多くの場合、データの入力前にシステム統制により対処することができないリスクがあり、また、そのような誤りを検出することは企業（受託会社）の責任ではない。同様に、システム境界外のユーザーは、処理を開始することに関して責任があるかもしれない。これらの例として、システム処理のインテグリティが保たれても、データが正当でなかったり、不正確だったり、また、そうでなければ不適当であるかもしれない。

d. 機密保持：機密とされた情報が、企業のコミットメントやシステム要求事項を満たすように、保護されている。

機密保持原則は、経営者のコミットメント及びシステム要求事項に従って、機密

（訳者注）カナダ勅許会計士協会（CICA）は、2013 年４月１日にカナダ国内の他の会計士団体と統合して、カナダ勅許職業会計士協会（Chartered Professional Accountants of Canada）となっている。

とされた情報を、システムから最終的に廃棄又は除外されるまで保護するシステムの能力について言及する。情報の管理者（例えば、情報を保持又は格納する企業）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。そのような要求事項は、法令又はユーザー契約のコミットメントに含まれる可能性がある。情報を機密とする必要性は、多くの異なった理由に起因する。例えば、専有情報、企業の担当者のみを対象とする情報である。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、機密保持原則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、プライバシー原則は、パーソナル・インフォメーションの収集、利用、保持、開示、廃棄に関する要件に対応している。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、企業のコミットメント及びシステム要件を満たすように、収集、利用、保持、開示及び廃棄されている。

機密保持原則は様々な種類の機微情報に適用される一方で、プライバシー原則はパーソナル・インフォメーションだけに適用される。企業がデータ主体（本人）に対し、以下に挙げるカテゴリーの全てを網羅するサービスを提供する直接的な責任を負う場合には、プライバシー原則が適切であるかもしれない。企業が以下に挙げるカテゴリーの重要な部分について直接的な責任を負わないものの、パーソナル・インフォメーションの保護に関する責任も保持する場合は、機密保持原則の方がよりふさわしいかもしれない。

プライバシー原則は、八つのカテゴリーで構成される。

a. コミットメント及びシステム要求事項に関する通知及びコミュニケーション：企業は、企業のプライバシー・コミットメント及びシステム要求事項を満たすように、プライバシー実務についてデータ主体（本人）に通知する。
b. 選択及び同意：企業は、パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関する可能な選択をデータ主体（本人）に伝える。
c. 収集：パーソナル・インフォメーションは企業のプライバシー・コミットメント及びシステム要求事項に従って収集される。
d. 利用、保持及び廃棄：企業は、パーソナル・インフォメーションの利用、保持及び破棄を企業のプライバシー・コミットメント及びシステム要求事項を満たすように、制限する。
e. アクセス：企業は、企業のプライバシー・コミットメント及びシステム要求事項を満たすように、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を確認及び訂正（更新を含む。）できるように、アクセス権を付与している。
f. 開示及び通知：企業は、データ主体（本人）の合意を得て、企業のプライバシ

ーコミットメント及びシステム要求事項を満たすように、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、企業のプライバシー・コミットメント及びシステム要求事項を満たすように、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。

g. 品質：企業は、企業のプライバシー・コミットメント及びシステム要求事項を満たすように、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。

h. モニタリング及び執行：企業は、企業のプライバシーコミットメント及びシステム要求事項を満たすように、遵守状況をモニタリングしている。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。

Trust サービス規準

14. システムを評価するのに使用される規準の多くが全ての原則で共通である。例えば、リスク管理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原則に適用される。その結果、Trust サービス規準は、(1)五つの原則に対応する規準(共通規準)と、(2)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原則に特定された追加規準で構成される。セキュリティ原則については、共通規準が完全な規準を構成する。

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原則において、規準全体は、共通規準と業務の対象となる（一つ以上の）原則に対応する規準から構成される。

業務の対象となる原則に関する規準は、その原則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。

共通規準は七つのカテゴリーで構成されている。

a. 組織及び管理：

業務の対象となる原則の規準を満たすように、企業の構造と、企業が導入している業務単位の人員を管理、支援するために実装されたプロセスに関連する規準。これは人員の義務、誠実性、倫理観及び適性を扱う規準、及びそれらが機能する環境を含んでいる。

b. コミュニケーション：

企業が業務の対象となる原則の規準を満たすように、システムの許可されたユーザーと他の当事者に方針、プロセス、手順、コミットメント及びシステム要求事項を伝えること、それらの当事者とユーザーがシステムを適切に操作する義務に関連する規準

c. リスク管理及び内部統制のデザインと導入：

企業が業務の対象となる原則の規準を満たすように、(i)これらの企業の目的を

達成する能力に影響する潜在的リスクを特定し、(ii)それらのリスクを分析し、(iii)内部統制のデザインと導入とその他のリスク緩和策を含むそれらのリスク対応を策定し、そして(iv)リスクとリスク管理プロセスの継続的モニタリングを行うことに関連する規準

d. 内部統制のモニタリング：

企業が業務の対象となる原則の規準を満たすように、システムの設計及び内部統制のデザインの適合性と運用の有効性を、モニターし、特定された不備へ対応することに関連する規準

e. 論理的及び物理的アクセス管理：

企業が業務の対象となる原則の規準を満たすように、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

f. システム運用：

企業が業務の対象となる原則の規準を満たすように、システム手順の実行を管理し、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

g. 変更管理：

企業が業務の対象となる原則の規準を満たすように、システム変更の必要性を特定し、統制された変更管理プロ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

Trust サービス原則と規準

15. 以下の各 Trust サービスの規準については、括弧でくくられた用語は Trust サービス業務で対象としている特定の原則に合わせて選択する必要がある。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から成る Trust サービス原則は、ある原則が単独で報告されることも、一部の原則又は全部の原則が一緒に報告されることもある。業務で対象としている各原則については、当該原則に関連する全ての規準を対象とされるべきである。さらに、どの Trust サービス原則が業務の対象となっているのかに関係なく、共通規準は適用されるべきである。

全ての原則（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）に共通する規準	
CC1.0	**組織及び管理に関する規準**
CC1.1	企業は、［セキュリティ、可用性、処理のインテグリティ、機密保持若

	しくはプライバシー又はそれらの組み合わせで報告対象の原則を挿入]に関連するコミットメント及びシステム要求事項を充足できるようにするシステムの設計、開発、導入、運用、維持及びモニタリングに関して組織構造、指揮命令系統、権限及び責任を明確にしている。
CC1.2	企業のシステムコントロール及びその他のリスク緩和戦略にかかる設計、開発、導入、運用、維持、モニタリング、承認に関する実施責任及び説明責任は、ポリシー及びほかのシステム要求事項を効果的に広め、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連する企業のコミットメント及びシステム要求事項を満たすように導入され、実施することを確実にするため、権限とともに企業内の各個人に割り当てられる。
CC1.3	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組み合わせで報告対象の原則を挿入]に影響を与えるシステムを設計、開発、導入、運用、維持、モニタリングに関して責任がある要員の適性を評価する手順を確立し、責任を果たす上で必要なリソースを提供している。
CC1.4	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組み合わせで報告対象の原則を挿入]に関連するコミットメント及びシステム要求事項を充足可能とする、行動規範を確立し、従業員選考手続（バックグランドチェックを含む）を導入し、実行手続を行っている。
CC2.0	**コミュニケーションに関する共通規準**
CC2.1	システムの設計・運用とその境界に関連する情報は、許可されたシステムの内部及び外部ユーザーが、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され、伝達している。
CC2.2	企業の[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]のコミットメントは、適切な方法により、外部ユーザーに伝達され、これらのコミットメント及び関連するシステム要求事項は、内部ユーザーが責任を果たすことができるように伝達されている。
CC2.3	内部及び外部ユーザー及びシステム運用に影響を及ぼす役割があるその他の者の責任は、それらの者に伝達されている。
CC2.4	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連して、システムの設計、開発、導入、運用、維持及びモニタリングの内部統制に不可欠な情報は、要員にその責任を果たすために提供される。
CC2.5	内部及び外部ユーザーは、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組み合わせで報告対象の

	原則を挿入]に関連する障害、事故、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。
CC2.6	内部及び外部ユーザーの責任又は[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組み合わせで報告対象の原則を挿入]と関連する企業のコミットメント及びシステム要求事項に影響を及ぼすシステム変更は、適時にそれらのユーザーに伝達される。
CC3.0	**リスク管理及び内部統制のデザインと導入に関する共通規準**
CC3.1	企業は、(1)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あるいはそれらの組み合わせで報告対象の原則を挿入]に関連するコミットメント及びシステム要求事項を害するおそれのある潜在的脅威（システムにアクセスする顧客の人員やその他の者による脅威と同様に、商品及びサービスを提供するベンダー及び他の第三者を利用することによる脅威を含む。）を識別し、(2)識別された脅威と関連するリスクの重大性を分析し、(3)それらのリスクに対する軽減方法（内部統制の導入、商品又はサービスを提供するベンダー及び他の第三者の活動のみならずその評価及びモニタリング、並びに他の軽減方法を含む。）を決定し、(4)内部統制システムに、重大な影響を及ぼし得る変更（例えば、環境、規制及び技術的な変更及び内部統制の評価とモニタリングの結果）を識別・評価し、そして、(5)必要に応じて、識別された変更に基づいて、リスク評価と軽減方法を再評価し、更新する。
CC3.2	企業はリスク軽減方法を実行するため、ポリシーと手続を含む、内部統制を設計、開発、導入、運用し、それらの活動の運用とモニタリングに基づく統制活動の設計及び導入の適合性を再評価し、そして、必要に応じて内部統制を更新する。
CC4.0	**内部統制のモニタリングに関する共通規準**
CC4.1	統制のデザインと運用上の有効性は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組み合わせで報告対象の原則を挿入]に関する企業のコミットメント及びシステム要求事項に対し定期的に検証され、識別された不備に関連する修正及び他に必要となる対応は、適時に実施される。
CC5.0	**論理的及び物理的アクセス管理に関する共通規準**
CC5.1	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は、(1)許可された内部及び外部ユーザーの識別及び認証、(2)管理者によって承認された、ハードウェア、データ、ソフトウェア、モバイル機器、出力及びオフライン要素を含む、システム構成要素又はその一部分について許可された内部及び外部ユーザーアクセス制限、(3)[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすよう未承認のアクセスの

	防止と発見、を支援するために実装される。
CC5.2	企業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は、システム証明書が発行される前に登録・承認されてから、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすようシステムにアクセスする権限が与えられる。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､ユーザーシステム証明書は削除される。
CC5.3	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、内部及び外部ユーザーは、システム構成要素（例えば、インフラストラクチャー、ソフトウェア及びデータ）にアクセスする場合には、識別され承認される。
CC5.4	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、データ、ソフトウェア、機能及び他のＩＴ資源へのアクセスは、役割、責任又は、システム設計と変更に基づいて、承認され、修正又は削除される。
CC5.5	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、システムを収容する設備（例えば、データセンター、バックアップ媒体保管庫、これらの所在地にある機密上重要なシステム構成要素のみならず他の機密上重要な所在地）への物理的なアクセスは、承認された人員に制限される。
CC5.6	企業のコミットメントとシステム要求事項を満たすように、論理的なアクセスセキュリティ対策を、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関するシステム境界の外部要因による脅威から保護するために導入している。
CC5.7	情報の送信、移動及び削除は、許可された内部及び外部ユーザーとプロセスに制限され､そして､[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及びシステム要求事項を満たすよう送信、移動又は削除する間は保護される。
CC5.8	[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又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、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、対処する内部統制が実装されている。
CC6.0	**システム運用に関する共通規準**

CC6.1	［セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組み合わせで報告対象の原則を挿入］に関する企業のコミットメントとシステム要求事項を満たすように、［セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組み合わせで報告対象の原則を挿入］に関して、悪意ある行為、自然災害又はエラーに起因する違反やインシデントについてのシステム構成要素の脆弱性は、識別、監視及び評価され、対応策が既知及び新規に識別された脆弱性を補うために設計、実装及び運用される。
CC6.2	［セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入］に関して、論理的及び物理的セキュリティ違反、障害、識別された脆弱性を含むインシデントは、企業のコミットメントとシステム要求事項を満たすように、確立されたインシデント対応手順に従って、識別され、適切な担当者に報告され、対処される。
CC7.0	**変更管理に関する共通規準**
CC7.1	［セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入］に関する企業のコミットメント及びシステム要求事項は、システム構成要素の設計、調達、導入（実装）、設定、テスト、修正、承認と維持を含んだシステム開発ライフサイクルを通じて対処される。
CC7.2	［セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入］に関する企業のコミットメント及びシステム要求事項との整合性を保つために、インフラストラクチャー、データ、ソフトウェア及びポリシーと手続が必要に応じて更新される。
CC7.3	［セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入］に関する企業のコミットメントとシステム要求事項を満たすように、システムの運用中及び監視中に、内部統制のデザイン又は運用の有効性に不備が識別されると、変更管理プロセスが開始される。
CC7.4	システム構成要素への変更は、企業の［セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入］に関するコミットメント及びシステム要求事項を満たすよう、（起案）承認され、設計され、開発され、設定され、文書化され、テストされ、（リリース）承認され、実装される。
可用性に関する追加規準	
A1.1	企業の可用性に関するコミットメント及びシステム要求事項を満たすように、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、現在の処理能力と使用率が保持され、監視され、評価されている。

A1.2	企業の可用性に関するコミットメント及びシステム要求事項を満たすように、物理的設備対策、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が承認され、設計され、開発され、実装され、稼働し、許可され、保持され、監視されている。
A1.3	企業の可用性に関するコミットメント及びシステム要求事項を満たすように、システム復旧を支援する復旧計画の手続がテストされている。
処理のインテグリティに関する追加規準	
PI1.1	企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、処理エラーを防止し、検出し、是正する手続が存在する。
PI1.2	システム入力は、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、完全に、正確に、適時に測定され、記録される。
PI1.3	データは、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように承認されたとおりに、完全に、正確に、適時に処理される。
PI1.4	データは、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、特定された期間、完全、正確かつ適時に格納され、保持される。
PI1.5	システム出力は、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、完全で、正確で、配布され、そして保持される。
PI1.6	通常の取引処理以外のデータの修正は、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、承認され、処理される。
機密保持に関する追加規準	
C1.1	機密情報は、企業の機密保持に関するコミットメント及びシステム要求事項を満たすように、システム設計、開発、テスト、実装及び変更プロセスの間、保護されている。
C1.2	システム領域内の機密情報は、企業の機密保持に関するコミットメント及びシステム要求事項を満たすように、入力、処理、保管、出力及び廃棄の間、未承認のアクセス、使用及び開示から保護されている。
C1.3	機密情報へのシステム領域外からのアクセス及び機密情報の開示が、企業の機密保持に関するコミットメント及びシステム要求事項を満たすように、承認された当事者に制限されている。
C1.4	企業は、システムの一部として、機密情報へのアクセスを持つ、製品やサービスを提供するベンダー及び他の第三者から、企業の機密保持システム要件に整合する機密保持に関するコミットメントを入手している。

C1.5	システムの一部になる製品やサービスのベンダー及び他の第三者による、企業の機密保持に関するコミットメント及びシステム要求事項の遵守状況が、定期的及び必要に応じて評価され、必要な是正措置が取られる。
C1.6	企業の機密保持のコミットメント及びシステム要求事項の変更が、内部及び外部ユーザー、製品やサービスがシステムの一部となるベンダー並びに第三者に伝達される。
C1.7	企業は、企業の機密保持のコミットメント及びシステム要求事項を満たすように、機密情報を保持する。
C1.8	企業は、企業の機密保持のコミットメント及びシステム要求事項を満たすように、機密情報を廃棄する。
プライバシーに関する追加基準	
P1.0	**コミットメント及びシステム要求事項の通知及びコミュニケーションに関するプライバシー規準**
P1.1	企業は、企業のプライバシー・コミットメント及びシステム要求事項を満たすようにプライバシー実務についてデータ主体（本人）に通知する。 通知は、企業のプライバシー・コミットメント及びシステム要求事項を満たすためにパーソナル・インフォメーションの利用の変更を含む、企業のプライバシー行動の変更に関し適時に更新され、データ主体（本人）に伝えられる。
P1.2	企業のプライバシー･コミットメントが外部ユーザーに適切に通知され、それらのコミットメント及びそれに関連するシステム要求事項が、内部ユーザーがその責任を遂行できるように内部ユーザーに伝えられる。
P2.0	**選択及び同意に関するプライバシー規準**
P2.1	企業は、パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関する可能な選択、各選択の影響をデータ主体（本人）に伝える。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な同意が求められる場合には、データ主体（本人）若しくはその他権限を付与された個人から取得されるが、当該同意は、企業のプライバシー・コミットメント及びシステム要求事項に従って、情報が意図され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、保持及び廃棄に関する黙示的な同意が得られていると判断する企業の根拠は文書化される。
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企業のプライバシー・コミットメント及びシステム要求事項に従って収集される。
P3.2	明示的な同意を求める情報に関し、企業は、そのような同意の必要性のみならずパーソナル・インフォメーションの要請に関し同意しない場合の影響について伝え、企業のプライバシー・コミットメント及びシステム要

	求事項に従って情報を収集する前に同意を取得する。
P4.0	**利用、保持及び廃棄に関するプライバシー規準**
P4.1	企業は、パーソナル・インフォメーションの利用を企業のプライバシー・コミットメント及びシステム要求事項に識別される目的に制限する。
P4.2	企業は、パーソナル・インフォメーションを企業のプライバシー・コミットメント及びシステム要求事項に準拠して保持する。
P4.3	企業は、パーソナル・インフォメーションを企業のプライバシー・コミットメント及びシステム要求事項に準拠して安全に廃棄する。
P5.0	**アクセスに関するプライバシー規準**
P5.1	企業は、識別され認可されたデータ主体（本人）に、レビューのために保管されているパーソナル・インフォメーションにアクセスする能力を付与し、要請がある時点で、当該情報の物理的又は電子的コピーを、データ主体（本人）に企業のプライバシー・コミットメント及びシステム要求事項に従って提供する。もし、アクセスが拒否される場合、企業のプライバシー・コミットメント及びシステム要求事項に準拠し、必要なものとして、データ主体（本人）に拒否及びその理由を通知する。
P5.2	企業は、データ主体（本人）が提供する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、企業のプライバシー・コミットッメント及びシステム要求事項に従って、確約されている又は求められるように、そのような情報を第三者に提供する。訂正要請が拒否された場合には、データ主体（本人）に企業のプライバシー・コミットッメント及びシステム要求事項に準拠して拒否及びその理由を通知する。
P6.0	**開示及び通知に関するプライバシー規準**
P6.1	統制のデザインと運用上の有効性は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及びシステム要求事項に対し定期的に検証され、識別された不備に関連する修正及び他に必要となる対応は、適時に実施される。
P6.2	企業は、企業のプライバシー・コミットメント及びシステム要求事項に準拠して、パーソナル・インフォメーションの承認された開示に関する完全、正確かつ適時の記録を作成、保持する。
P6.3	企業は、企業のプライバシー・コミットメント及びシステム要求事項に準拠して、パーソナル・インフォメーションの未承認の開示（漏洩を含む。）に関する発見若しくは報告の完全、正確かつ適時の記録を、作成、保持する。
P6.4	企業は、ベンダーその他第三者（その製品及びサービスがシステムの一部であり、システムにより処理されたパーソナル・インフォメーションへのアクセスを有する）から、企業のプライバシー・コミットメント及びシステム要求事項に準拠して、プライバシー・コミットメントを取得している。
P6.5	企業は、ベンダーその他第三者（その製品及びサービスがシステムの一

	部であり、システムにより処理されたパーソナル・インフォメーションへのアクセスを有する）の企業のプライバシー・コミットメント及びシステム要求事項の遵守状況を、定期的かつ必要に応じて評価し、必要がある場合には是正措置を講じている。
P6.6	企業は、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又は疑われる場合には、企業に通知をするコミットメントを、システムにより処理されるパーソナル・インフォメーションへのアクセスを有しうるベンダーその他第三者から取得する。当該通知は、企業が策定しているインシデント対応手続き、プライバシー・コミットメント及びシステム要求事項を満たすために、適切な担当者に報告され、対処される。
P6.7	企業はプライバシー･コミットメント及びシステム要求事項に準拠して、漏洩及びインシデントについて、影響を受けるデータ主体（本人）、規制当局その他に通知する。
P6.8	企業は、企業のプライバシー・コミットメント及びシステム要求事項に従って、データ主体（本人）の要求により、保有しているパーソナル・インフォメーション及びデータ主体（本人）のパーソナル・インフォメーションの開示の説明をデータ主体（本人）に提供する。
P7.0	**品質に関するプライバシー規準**
P7.1	企業は、企業のプライバシー・コミットメント及びシステム要件に従って正確、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。
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	企業は、データ主体（本人）及びその他から「の問合せ、苦情及び争議を受け付け、対処、解決及びその解決策を伝えるプロセスを適用し、定期的に企業のプライバシー･コミットメント及びシステム要件への準拠状況、及び識別された不備に関する是正その他必要な措置が適時に講じられていることをモニターする。

発効日

16. Trust サービス原則と規準は、2016 年 12 月 15 日以降終了する期間において適用する。それ以前の適用を妨げない。

付録Ａ　定義

17.

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。

許可されたアクセス：

アクセスが、(a)経営者により任命された者により承認され、(b)職務の分離、機密保持コミットメントに抵触しない場合、又は経営者によって承認されたレベルを越えたところまでシステムリスクを増加させない場合（すなわち、アクセスは適切であること。）に限り承認されていること。

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の原則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。

収集：

パーソナル・インフォメーションを、Web フォームや登録フォームなど個人から直接取得、又はビジネスパートナーなどの別の組織から取得する、いずれかのプロセス。

コミットメント：

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、一つ以上の原則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

同意：

このプライバシー要件は、「公正な情報慣行の原則（FTC 原則)」の一つである。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ある。 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

- 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。 EU データ保護指令によれば、機密情報の処理には明示的な同意が必要です。さらに、データ管理者は、コミュニケーションへの無応答から同意を推論することはできない。

・ 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。

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た個人。

開示：

情報を保持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：

企業が個人のパーソナル・インフォメーション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：

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）によ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措置

外部ユーザー：

顧客、企業管理者又は他の許可された者によりシステムに接する権限を与えられた従業員や要員でない個人

内部ユーザー：

職務権限によりシステムの人員構成要素のメンバーとなる従業員や要員

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。

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管理者の宣言。

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。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

以下はその例示である。

・ 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、(a)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ポリシー及び(b)これらのポリシー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 セクション 101、証明業務（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。報告書利用者は、一般公衆であるか、又は AT セクション 101 のパラグラフ 78 に従った特定の関係者に制限されるかもしれない。

保持：

企業が将来の使用や参照のために情報をどのように格納するかに関するデータライフサイクルの段階。

システム要求事項：

顧客に対する企業のコミットメント、ビジネス又は業界団体などの業界に関連する法規制や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としては、

- 政府の銀行規則で確立された就業者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。

SOC2 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、保証基準及び 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。

SOC3 業務：

一つ以上の Trust サービスの原則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

第三者：

企業とシステムの契約ユーザーとの間の契約の当事者ではないが、当該システムに関与している企業

Trust サービス：

システムと関連するデータの運用と保護に関する一連の原則と規準を基に提供される職業的保証業務と助言業務

就業者：

社員、契約社員及びシステムの操作の一部を実施することについて企業が契約したその他の者

付録Ｂ　リスク及び内部統制の例示

18. 内部統制が各 Trust サービスの規準を満たすように適切にデザインされているかを評価するに当たり、経営者は、評価対象のシステムの規準が満たされないリスクを評価する必要がある。これらのリスクを特定する上で、経営者は以下について検討する

- システムによって提供される製品及びサービス
- 製品及びサービスを提供するために使用されるシステムの構成要素
- システム運用環境
- 企業のシステムの影響を受けるシステムユーザ及び関係者に対するコミットメント
- 以下より派生するシステム要求事項
  - システム機能と製品及びサービスの提供方法に影響する法律及び規制
  - システムの影響を受けるシステムユーザ及び関係者に対するコミットメント
  - 企業の事業目的

以下の例示は、仮に中規模企業がリスク評価中に特定する可能性のあるリスクの例と、そのリスクに対処するために導入され得る内部統制である。業務実施者に、企業が識別するであろうリスクの種類及び規準を満たすようにリスクを軽減

する内部統制を理解することを支援するために提供している。考えられるリスクと内部統制の全てをリストアップすることを意図していない。各企業は、その他のリスクと規準を満たすように、リスクに対処する内部統制を検討する必要がある。また、内部統制のタイプは、ハイレベルで提示され、例えば、統制を行う人の立場、統制が行われる頻度及び 統制がどのように実行され、文書化され、監視されるかのような、適切に設計された内部統制に必要な詳細な記述は含まれていない。

規準		リスクの例示	統制の種類の例示
全ての原則（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）に共通する規準			
CC1.0	**全ての原則に共通する規準**		
CC1.1	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及びシステム要求事項を充足できるようにするシステムの設計、開発、導入、運用、維持及びモニタリングに関して組織構造、指揮命令系統、権限及び責任を明確にしている。	企業の組織構造が、[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]の活動を管理するために必要な組織構造、資源及び情報フローを提供していない。	企業が、事業計画プロセスの一部、進行中のリスク評価及び管理プロセスの一部として、その組織構造、指揮命令系統、権限及び責任を、評価し、変化するコミットメント及びシステム要求事項を満たすように必要に応じて、それらを改訂する。
		[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]の活動についての適切な監督、管理及び監視を実施するための、主要な管理者の役割と責任が十分に定義されていない。	役割と責任は、職務記述書上で定義され、管理者及び上級管理者に伝達される。
			職務記述書は変更が必要かどうか年次で経営者によってレビューされ、職務の変更が生じたときは職務記述書にも必要な変更が行われる。
		指揮命令関係及び組織構造により、上級管理者が[セキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシー]に関する効果的な監督を行うことができない。	指揮命令関係及び組織構造が組織の計画の一部として上級管理者によって定期的にレビューされ、企業のコミットメント及び要求事項が変更される都度、必要に応じて調整される。
		要員が[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]に係るコミ	役割及び責任が職務記述書に定義されている。

規準		リスクの例示	統制の種類の例示
		ットメント及びシステム要求事項を満たすだけの責任を与えられていない、又は十分な権限を委譲されていない。	
		プライバシーとデータ保護に関する実施責任及び説明責任が、企業のリスクとコンプライアンスを管理するために十分な権限を持った要員に割り当てられていない。	プライバシーとデータガバナンスの役割及び責任が、定義され、要員及び第三者に伝達されている。企業は、法律顧問と監査委員会に報告する最高プライバシーオフィサー（CPO）を任命している。CPO は、プライバシーの内部統制を導入、モニタリングの責任をはたすプライバシー・スタッフを監督する。さらに、指名されたプライバシー担当者は、各事業単位に割り当てられ、プライバシー担当者に間接的に報告される。
CC1.2	企業のシステムコントロール及びその他のリスク緩和戦略にかかる設計、開発、導入、運用、維持、モニタリング、承認に関する実施責任及び説明責任は、ポリシー及びほかのシステム要求事項を効果的に広め、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連する企業のコミットメント及びシステム要求事項を満たすように導入され、実施することを確実にするため、権限とともに企業内の各個人に割り当てられる。	要員が[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]に係るコミットメント及びシステム要求事項を満たすだけの責任を与えられていない、又は十分な権限を委譲されていない。	役割及び責任が職務記述書に定義されている。
			職務記述書の変更が必要かどうか定期的にレビューされ、変更が識別された場合は更新される。
		プライバシーとデータ保護の統制に関する実施責任及び説明責任が、企業のリスクとコンプライアンスを管理するために十分な権限を持った要員に割り当てられていない。	CPO は、プライバシーの内部統制を導入し、モニタリングの責任を果たすプライバシー担当者を監督する。さらに、CPO とプライバシー担当者に間接的に報告する指名されたプライバシー担当者は、各事業単位に割り当てられる。プライバシー担当者は、プライバシーの内部統制の導入とモニタリングを確実にす

規準		リスクの例示	統制の種類の例示
			ることを支援する責任を有する。
CC1.3	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に影響を与えるシステムを設計、開発、導入、運用、維持、モニタリングに関して責任がある要員の適性を評価する手順を確立し、責任を果たす上で必要なリソースを提供している。	新規雇用者、新規担当者、又は異動した要員が、職務遂行に十分な知識と経験を有していない。	職務要件は職務記述書に文書化され、候補者の能力が職務要件を満たしているかどうか、雇用、業績評価又は異動の評価プロセスの一部として評価される。
			採用又は任命の候補者の経験及び研修は、候補者が職務に就く前に評価される。
		要員が、職務遂行するのに十分な定期的研修を受けていない。	経営者が、要員に必要なスキルセットを確立し、要員へのコミットメント及び要求事項に関する、継続的研修を提供している。
			経営者が研修の要件に準拠しているかをモニタリングしている。
		テクニカルツールと情報資源は割り当てられたタスクを実施するのに不十分である。	継続的、定期的なビジネス計画及び予算プロセスの中で、経営者は、ビジネス目的を達成するために、追加的ツールと資源の必要性を評価する。
CC1.4	企業は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及びシステム要求事項を充足可能とする、行動規範を確立し、従業員選考手続（バックグランドチェックを含む。）を導入し、実行手続を行っている。	要員は、企業の行動規範を遵守しない。	経営者は、顧客と作業者の苦情のモニタリングを通じて、また、第三者に管理された匿名の倫理ホットラインを利用して、要員の行動規範の遵守をモニタリングする。企業の行動規範は、行動規範に違反した要員の処分方針を含んでいる。処分方針は、行動規範に違反した要員に適用される。
			要員は、採用時に行動規範と機密保持及びプライバシー実務の声明を読んで同意し、その後は正式に年次で再確認を要求される。
		企業の経営者によって受け入れ難いとされるバックグラウドを持つ候補者が、企業により採用される。	上級経営者は、候補者が与えられる職位に求められる慎重さやスキルに基づいて採用されることから排除する特性のリストを、策定する。そのリストは、

規準		リスクの例示	統制の種類の例示
			最終採用決定をする組織内の担当者に提供され、それらの特性は全ての候補者の評価について検討される。
			企業と第三者が契約する前に、第三者の要員は、バックグランドスクリーニングを受ける。バックグランドチェックは、信用、賞罰、薬物及び在籍確認を最低限含んでいる。
			第三者又は再委託先に対する明確に定義された取引条件及び責任を含む、合意書が、第三者又は再委託先と確立される。
			採用に先立ち、要員は「規制チェックデータベース」に対して照合される。
			企業は、要員の倫理行動に関する基準とガイドラインを確立している。
CC2.0	コミュニケーションに関する共通規準		
CC2.1	システムの設計・運用とその境界に関連する情報は、許可されたシステムの内部及び外部ユーザーが、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され、伝達している。	外部ユーザーは、そのスコープ、目的及び設計の理解不足のために、システムの利用を誤る。	システムの境界を説明し、システムの目的及び設計だけでなく、関係するシステム構成要素を記述するシステム記述は、許可された外部ユーザーが入手できるようになっている。システム記述は、企業の顧客向けウェブサイトを介して許可されたユーザーが入手することができる。
			システム記述は企業のイントラネット上に掲載され、企業の内部ユーザーが利用できる。この記述はシステムの境界と処理の主要な側面を詳細に説明する。
		内部ユーザーは主要な組織及びシステムサポート機能、処理、役割及び責任を自覚していない。	企業の組織構造、システムサポート機能、処理及び組織の役割と責任の記述は、企業のイントラネットに掲載され、企業の内部ユーザーが利用できる。この記述には、主要なシステム構成要素の設計及び運用の変更に関し、実施責任を負い、説明責任を負い、同意し、そして伝えられている当事者が説明されている。
		外部ユーザーは、システムの境界外から発生する、責任を負うべきリスクに対処していない。	システムの境界を説明し、システムの目的及び設計だけでなく、重要なシステム構成要素を記述するシステム記述は、許可された外部ユーザーが入手できるようになっている。システム記述は、顧客との継続的なコミュニケーション、又は顧客向けウェブサイトを通じて、外部ユーザーが利用できるようにされ

規準		リスクの例示	統制の種類の例示
			ている。
CC2.2	企業の[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]のコミットメントは、適切な方法により、外部ユーザーに伝達され、これらのコミットメント及び関連するシステム要求事項は、内部ユーザーが責任を果たすことができるように伝達されている。	内部及び外部ユーザーは、[セキュリティ、可能性、処理のインテグリティ、機密保持又はプライバシー]のために提供されるシステムの能力を理解できていない。また、この理解不足に基づき行動をとる。	企業のシステムに関する[セキュリティ、可能性、処理のインテグリティ、機密保持又はプライバシー]コミットメントは、サービス契約及び顧客特定サービスレベルへの同意事項を含んでいる。加えて、これらのコミットメントの要約は企業の顧客向けウェブサイトで利用できるようにされている。プライバシー通知は、全ての企業の公開ウェブサイトとソフトウェアに掲載・表示される。そのプライバシー通知には、企業のプライバシー・コミットメントが記述されている。
			システム要求事項に対処する重要なプロセスのための方針と手順の文書が、イントラネット上で利用可能である。
		企業のサービスを提供する要員の理解不足のために企業がそのコミットメントを果たすことができない。	重要なプロセスの方針及び手続文書が、企業のイントラネット上で利用可能である。
			要員は、年度のセキュリティ、機密保持及びプライバシー研修への参加が要求される。
			要員は、行動規範と機密保持及びプライバシー実務の声明を読んで同意することを、採用時その後は年次で要求される。
			プロセスは、サービスレベルのコミットメント及び合意書への遵守をモニタリングするサービスレベルの管理手続を通じて、月次でモニタリングされている。結果は適切な要員と顧客との間で共有され、コミットメントと合意書が充足されない場合には、行動がとられ、顧客を含む関係者へ伝達される。
CC2.3	内部及び外部ユーザー及びシステム運用に影響を及ぼす役割があるその他の者の責任は、それらの者に伝達されている。	システムは、内部ユーザーの責任不履行により、設計されたとおりに機能しない。	システム要件に対処する重要なプロセスの方針及び手続文書が、企業のイントラネットで利用できる。
			要員は、年度のセキュリティ、機密保持及びプライバシー研修への参加が要求される。
			要員は、行動規範と機密保持及びプライバシー実務の声明を読んで同意することを、採用時その後は年次で要求される。
			プロセスは、コミットメント及

規準		リスクの例示	統制の種類の例示
			び要求事項への遵守をモニタリングするサービスレベルの管理手続を通じて、モニタリングされている。結果は適切な要員と顧客との間で共有される。
		システムは、外部ユーザーの責任不履行により、設計されたとおりに機能しない。	顧客の責任が顧客向けウェブサイトとシステム文書に記述されている。
CC2.4	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連して、システムの設計、開発、導入、運用、維持及びモニタリングの内部統制に不可欠な情報は、要員にその責任を果たすために提供される。	内部統制は、これらの内部統制の導入と運用に関する要員の責任部分の理解が誤っているために、結果として、[セキュリティ、可能性、処理のインテグリティ、機密保持又はプライバシー]のコミットメント及びシステム要求事項を充足せず、設計された機能が損なわれているか、効果的に運営されていない。	重要なプロセスの方針及び手続文書が、企業のイントラネットで利用できる。
			プロセスは、コミットメント及び要求事項への遵守をモニタリングするサービスレベルの管理手続を通じて、モニタリングされている。結果は方針に従って共有される。
			顧客の責任が顧客向けウェブサイトとシステム文書に記述されている。
CC2.5	内部及び外部のユーザーは、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連する障害、事故、懸念及び他の苦情を適切な要員に報告する方法についての情報が提供されている。	システムの異常は内外のユーザーにより検出されるが、障害が適切な要員に報告されないと、結果として[セキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシー]に関するコミットメント及びシステム要求事項をシステムが達成できない。	運用上の障害、インシデント、システムの問題、事故及びユーザークレームを報告する責任（及び報告のプロセス）を含んだ、重要なプロセスに関する方針及び手続文書が公表され、イントラネットで利用できるようにされている。
			運用上の障害、インシデント、問題、事故、クレームを報告する責任を含む顧客の責任、及び報告のプロセスが、顧客向けウェブサイトとシステム文書に記述されている。
CC2.6	内部及び外部ユーザーの責任又は[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれら	システム変更に起因して、内部及び外部ユーザーがシステム能力の変更や[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	顧客に影響を与えるシステム変更の提案は、実装の XX 日前に顧客向けウェブサイトで公表される。内部及び外部ユーザーは大規模な変更の実装 XX 日前にユーザー受け入れテストに参加す

規準		リスクの例示	統制の種類の例示
	の組合せで報告対象の原則を挿入]と関連する企業のコミットメント及びシステム要求事項に影響を及ぼすシステム変更は、適時にそれらのユーザーに伝達される。	イバシー]の提供に関する自分たちの責任の変化について誤解し、その誤解に基づいた行動をとる。	る機会を与えられる。システムに加えられた変更は、カスタマーケア会議のような継続的なコミュニケーションの仕組みや顧客向けウェブサイトを通じて、顧客に伝達され確認される。
			ビジネス部門の経営者は、変更を承認するまでに、変更を理解していることを確認しなければならない。
		内部及び外部ユーザーが、システム変更に気付かない。	実装されるシステム変更が記載されたシステム変更の日程表は、企業のイントラネットに掲載される。
			更新されたシステム文書が、実装の 30 日前に顧客向けウェブサイトやイントラネットに掲載される。
			インシデントに起因するシステム変更は、実装プロセスの一部として、電子メールを通じて内部及び外部ユーザーに伝達される。
		役割及び責任の変更や、主要な要員の変更が、内部及び外部ユーザーへ適時に伝達されない。	役割及び責任の重要な変更や、主要な要員の変更は、変更管理プロセスの一部として、影響を受ける内部及び外部ユーザーへ電子メールを通じて伝達される。
CC3.0	リスク管理及び内部統制のデザインと導入に関する共通規準		
CC3.1	企業は、(1)システムの[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関連するコミットメント及びシステム要求事項を害するおそれのある潜在的脅威（システムにアクセスする顧客の要員やその他の者による脅威と同様に、商品及びサービスを提供するベンダー及び他の第三者を利用することによる脅威を含む。）を識別し、(2)識別された脅威と関連するリスクの重大性を分析し、(3)それらのリスクに対する軽減方法（内部統制の導	必ずしも全てのシステムの構成要素がリスクマネジメントプロセスに含まれず、その結果、リスクの識別と軽減又は受容ができない。	経営者が使用するための企業のシステム構成要素のマスターリストがメンテナンスされ、追加や削除が明らかにされる。

規準		リスクの例示	統制の種類の例示
	入、商品又はサービスを提供するベンダー及び他の第三者の活動のみならずその評価及びモニタリング、並びに他の軽減方法を含む。）を決定し、(4)内部統制システムに、重大な影響を及ぼし得る変更（例えば、環境、規制及び技術的な変更及び内部統制の評価とモニタリングの結果）を識別・評価し、そして、(5)必要に応じて、識別された変更に基づいて、リスク評価と軽減方法を再評価し、更新する。		
		必ずしも全てのシステムに重大な影響を与える変更が識別されず、その結果、関連するリスクを正確に再評価できない。	リスク評価や管理のプロセスを通じて、リスク管理要員は、ビジネス目標、コミットメントと要求事項、内部の運用、ビジネス目標の達成にとって脅威となる外部要因の変化を識別し、システムの目的に対する潜在的な脅威について更新している。識別されたそのリスク対応として、経営者は必要に応じて、方針、手続、プロセス及び内部統制を更新する。
		リスクマネジメントプロセスに関係する要員が、リスク及び企業のリスク許容度を評価するための十分な情報を持っていない。	企業は、リスク許容度を明確にする正式なリスクマネジメントプロセスや、識別した脅威と明確化した許容度に基づくリスク評価プロセスを定義し、導入している。
		セキュリティ・コントロールにより対処可能で、重要な、そして［セキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシー］に関するコミットメント及びシステム要求事項の達成を脅かす、一つ又は複数の内外のリスクが識別されない。	リスク評価や管理のプロセスを通じて、リスク管理部門の要員は、ビジネス目標、コミットメントとシステム要求事項、内部の運用、ビジネス目標の達成にとって脅威となる外部要因の変化を識別し、システムの目的に対する潜在的な脅威について更新している。
			識別されたリスクは、リスク評価プロセスを使用して評価され、評価結果は経営者によってレビューされる。
			企業は、プライバシー特有のリスクや法令順守義務を識別するためにプライバシー影響評価（PIA）を実行し、それらのリス

規準		リスクの例示	統制の種類の例示
			クの発生可能性と潜在的な影響度を評価する。PIA は、パーソナル・インフォメーションを含む新たなプロセスが開発される場合、変更がそのようなプロセスに行われる場合の影響を評価することを伴う。
			リスク管理グループが、内部統制の有効性と識別されたリスクに合う軽減方法を評価し、その評価に基づき改善を勧告する。
			リスク管理グループによる勧告は、上級経営者によってレビューされ承認される。リスク評価による各改善計画に、オーナーが割り当てられる。
			企業は、主要なシステム構成要素、同様に技術的及びインストールに関する具体的な実装の詳細を把握し、継続的な資産管理やサービス管理に関するコミットメントや要求事項をサポートするための構成管理データベースや関連プロセスを使用する。
		適切に識別されていない変更は、リスク管理プロセスを経ても、これらの変更の失敗に起因してリスクを引き起こす。	リスク評価や管理プロセスを通じて、リスク管理要員が、発生した環境規制、及び技術の変化を識別する。識別されたそのリスク対応として、経営者は必要に応じて、方針、手続、プロセス及び内部統制を更新する。
CC3.2	企業はリスク軽減方法を実行するため、ポリシーと手続を含む、内部統制を設計、開発、導入、運用し、それらの活動の運用とモニタリング基づく統制活動の設計及び導入の適合性を再評価し、そして、必要に応じて内部統制を更新する。	選択、開発及び整備された内部統制や軽減方法が、リスクを適切に軽減しない。	四半期ごとに、現業部門による内部統制の自己評価が実施される。
			年次のリスク評価に基づく内部監査計画に従って、内部監査が実施される。
			事業及びシステム復旧計画が年次でテストされる。
			内部や外部の脆弱性チェックが四半期ごとに、又は年ごとに実施され、その頻度は継続かつ変化するコミットメントと要求事項に合わせて調整される。経営者は、脆弱性チェックの結果に基づき措置を講じる。
			リスク管理に関する方針と手順は、開発され、実装され、及び

規準		リスクの例示	統制の種類の例示
			要員に伝達される
		整備された内部統制や軽減方法が、評価されていない新たなリスクを生み出す。	CC3.1の内部統制の例示を参照。
CC4.0	内部統制のモニタリングに関する共通規準		
CC4.1	統制のデザインと運用上の有効性は、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及びシステム要求事項に対し定期的に検証され、識別された不備に関連する修正及びほかに必要となる対応は、適時に実施される。	内部統制が、適切にデザインされていない、確立した方針に従って構成されていない、又は、効果的に運用されていないことで、結果としてコミットメントとシステム要求事項を満たさないシステムとなっている。	内部監査部門は、内部統制の評価を四半期ごとに実施し、監査委員会に是正措置を監視するため、結果を伝達する。
			経営者と内部監査部門は、定期的にインシデントの概要、その根本原因及び是正措置の報告を受ける。内部監査部門は、是正計画の完了を監視する。
			コントロールの自己評価（プライバシーのリスクに対処するコントロールの評価を含む）は、四半期ごとに運用単位で実施され、これらの結果は、追加のコントロール監視目的のために経営者に報告される。
CC5.0	論理的及び物理的アクセス管理に関する共通規準		
CC5.1	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は、(1)許可された内部及び外部ユーザーの識別及び認証、(2)管理者によって承認された、ハードウェア、データ、ソフトウェア、モバイル機器、出力及びオフライン要素を含む、システム構成要素又はその一部分について許可された内部及び外部ユーザーアクセス制限、(3)[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそ	全てのシステム基盤（インフラストラクチャー）又はシステム構成が論理的アクセスセキュリティ対策で保護されておらず、未承認の修正や使用という結果になる。	インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために、確立された企業標準（アクセス管理ソフトウェア、企業設定標準及び標準化されたアクセス統制リストの実装のための要求事項を含む。）がある。

規準		リスクの例示	統制の種類の例示
	れらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように未承認のアクセスの防止と発見を支援するために実装される。		
			ネットワークスキャンはインフラストラクチャー要素と企業標準の不一致を識別するために実行される。静的及び動的コード分析テストは、新しいアプリケーションシステム及び既存システムの変更のソースコードについて、そのシステムが本番環境に導入される事前と事後に実施される。経営者は、スキャン結果に基づいて適切な措置を講じる。
			情報システム資産が、ジョブロールに基づいてアクセスを評価する責任があるオーナーに割り当てられる。そのオーナーは、資産が取得され変更される都度、アクセス権を定義し、保管又は受託責任のある資産のために、定期的にアクセスを評価する。
			オンライン・アプリケーションにより、個々のユーザーIDと単一の顧客アカウント番号と照合される。システム記録へのアクセス要求は、最初にシステムへのアクセスが許可される時に、各ユーザーが有する特権リストと顧客アカウント番号との照合を要求する。
		論理的アクセスセキュリティ対策が、ＩＴ構成要素へのアクセスを許可する前に、内部及び外部ユーザーを識別又は認証しない。	インフラストラクチャー構成要素とソフトウェアは、利用可能であるときに、共有ログオン機能を利用するように設定される。共用ログオン機能を利用していないシステムは、ユーザーIDとパスワードの分離送信の実装が要求されている。
			要員による外部アクセスは、暗号化された仮想プライベートネットワーク（VPN）接続による二要素認証（例えば、磁気カードとパスワード）を通じてのみ許可される。
		論理的アクセスセキュリティ対策が、システム設計で要求される職務分離を提供しない。	ロールに基づくセキュリティプロセスは、可能であればロールを利用するように要求される、アクセス管理システムで定義さ

規準		リスクの例示	統制の種類の例示
			れている。
			資産がジョブロールに基づいて、アクセスの適切性を評価する責任があるオーナーに割り当てられる。ロールは定期的にレビューされ、資産オーナーとそのリスク管理グループによって年次で更新される。レビューの結果によるアクセス変更要求は、変更要求記録を経由してセキュリティグループへ提出される。
			ロールベースのセキュリティの利用をサポートしないソフトウェアとインフラストラクチャーのために、役割と関連するアクセス特権用に分離されたデータベースが管理される。セキュリティグループは、アクセスルールを特定し、システムへ入力する時にこのデータベースを利用する。
		論理的アクセスセキュリティ対策が、システム設定、特権機能、マスターパスワード、強力なユーティリティ、セキュリティデバイス、そしてその他のハイリスク資源へのアクセスを制限していない。	機密性の高い資源への特権アクセスは、定義されたユーザーロールに制限され、これらのロールへの論理アクセスは最高情報セキュリティ責任者によって承認されなければならない。このアクセスは、定期的に最高情報セキュリティ責任者によって、レビューされる。
CC5.2	企業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は、システム証明書が発行される前に登録・承認されてから、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすようにシステムにアクセスする権限が与えられる。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、ユーザーシステム証明書は削除される。	有効なユーザーIDが、許可されていない人に与えられる。	人材管理システムの要員変更から収集された内部及び外部ユーザーの自動取り込みにより、異動日にアクティブディレクトリと VPN システムで、ユーザーIDが日次で自動作成又は自動削除される。
			保護された資源への要員アクセ

規準		リスクの例示	統制の種類の例示
			スは、システム資源オーナーからの承認された変更要求に基づいて、セキュリティグループによって、生成又は修正される。
			契約社員とベンダーの ID は、契約社員の部署からの承認された変更要求に基づいてセキュリティグループによって、生成される。これらの ID は関係の終了予定日又は XX 日のいずれか短い期間で有効となる。
			特権顧客アカウントは、指定された顧客窓口からの承認要求書面の記載に基づいて生成される。これらのアカウントはクライアントのユーザーアクセスアカウント及びそれら関連する特権の生成に使用される。
			システムセキュリティは、初期システムサインインと初期サインイン以降 XX 日毎に、内部及び外部ユーザーにパスワードを変更することを要求するように設定されている。
		既に許可を失ったユーザーがシステム資源へアクセスを続けている。	人事システムは、最終出社日の要員のアクセスを削除するため、自動取り込みをアクティブダイレクトリと VPN に、日次で送信する。そのリストは、アクセス削除のためにセキュリティ要員によって利用される。そのアクセス削除はセキュリティマネジャーによって確認される。
			週次で、人材システムは、セキュリティグループに削除対象者リストを、そのアクセスが削除されるようにするため、送信する。そのリストはセキュリティ要員によってアクセスを削除するために利用される。そのアクセス削除はセキュリティマネジャーによって確認される。
			週次で、契約社員の管理部署はセキュリティグループに契約終了ベンダー及び契約社員のリストを、そのアクセスが排除されるように送る。そのリストはセキュリティ要員によってアクセスを排除するために利用される。そのアクセス排除はセキュリティマネジャーによって確認される。
			企業のポリシーは、最高情報セキュリティ責任者の書面による承認なしで、削除した要員の ID の再活性化又は利用は禁止している。再活性化の要求は、変更

規準		リスクの例示	統制の種類の例示
			管理記録を利用して作成され、その目的とアクセスの正当性（業務上の必要性のため）、再活性化されたそのシステムとアカウントが有効となる期間（XX 日間を超えない）が含まれる必要がある。アカウントは新しいパスワードでリセットされ、要求された期間で活性化される。全てのアカウントの利用は記録され、セキュリティ要員によってレビューされる。
			アカウントの共有は、個々の使用の活動ログ及び使用後のパスワードの再設定により厳しく統制された状況の下でアカウント共有を提供する「アカウントとパスワードを保管するソフトウェア製品」を使用することが企業によって規定されているとして、最高情報セキュリティ責任者によって、方針からの逸脱が認められている場合以外、禁止される。そのほかに、共有アカウントは、低リスクのアプリケーション（例えば、共有 ID によるアクセスが職務の分離を阻害し得ないような情報システム）や共有 ID の使用がシステム技術上の制約になっている場合（例えば、UNIX のルート権限）には、認められる。最高情報セキュリティ責任者は、全ての共有アカウントの使用を承認しなければならない。軽減した統制は、可能な場合には実行される。（例えば、UNIX のルート権限でのアクセス時の SU の利用）。
CC5.3	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、内部及び外部ユーザーは、システム構成要素（例えば、インフラストラクチャー、ソフトウェア及びデータ）にアクセスする場合には、識別され承認される。	情報システム構成要素にアクセスするとき、内部及び外部ユーザーは特定されない。	インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために、確立された企業標準（アクセス管理ソフトウェア、企業設定標準及び標準化されたアクセス統制リストの導入のための要求事項を含む）がある。
			アカウントの共有は、個々の使用の活動ログ及び使用後のパス

規準		リスクの例示	統制の種類の例示
			ワードの再設定により厳しく統制された状況の下でアカウント共有を提供する「アカウントとパスワードを保管するソフトウェア製品」を使用することが企業によって規定されているとして、最高情報セキュリティ責任者によって、方針からの逸脱が認められている場合以外、禁止される。 そのほかに、共有アカウントは、低リスクのアプリケーション（例えば、共有 ID によるアクセスが職務の分離を阻害し得ないような情報システム）や共有 ID の使用がシステム技術上の制約になっている場合（例えば、UNIX のルート権限）には、認められる。 最高情報セキュリティ責任者は、全ての共有アカウントの使用を承認しなければならない。 軽減した統制は、可能な場合には実行される。（例えば、UNIX のルート権限でのアクセス時の SU の利用）
		無権限者は、システムにアクセスするため、有効なユーザーID があるかのように装う。	オンライン・アプリケーションは、入力された個々のユーザーID と単一の顧客アカウント番号の照合により、個々の顧客ユーザーの特権の正当性を認証する。システム記録へのアクセスの要求（例えば、ユーザーのアクセスの試み）は、顧客アカウント番号の照合を要求する。アプリケーションは、ユーザー資格に関する報告機能を提供する。
			二要素認証と暗号化された VPN チャネルの利用は、正当な外部ユーザーのみがＩＴシステム構成要素にリモート及びローカルアクセスできることを確実とするのを支援する。
			基盤の構成要素とソフトウェアは、利用できるとき、アクティブディレクトリ共有ログオン機能を使うように構成される。 共有ログオン機能を使っていないシステムは、別々のユーザーID とパスワードを必要とするように構成される。 アプリケーションは、ユーザー資格に関する報告機能を提供する。
		無権限者に権限者の保有する活動ができるよ	外部ユーザーは、VPN、SSL、その他の暗号化された通信システ

規準		リスクの例示	統制の種類の例示
		うになると、外部ユーザー・アクセス・クレデンシャルは、無駄になる。	ムの利用を通じてのみ、リモートでそのシステムにアクセスすることができる。
			パスワードの複雑性の標準が、アクセス・コントロール・ソフトウェアのパスワードによる統制を強制するために規定されている。
			管理アカウントが設定され、ユーザー管理機能は、特権アカウントを管理するために分離されている。
CC5.4	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、データ、ソフトウェア、機能及び他のＩＴ資源へのアクセスは、役割、責任又は、システム設計と変更に基づいて、承認され、修正又は削除される。	正当な内部及び外部ユーザーが、システムへの未承認のアクセスを得ることにより、職務の分離の欠如や意図的な悪意のある行為やエラーのリスクが増大する。	可能であれば、システムとインフラストラクチャーの構成要素へのアクセスを制限する正式な役割ベースのアクセスコントロールを構築し、アクセスコントロールシステムによって実施される。それが可能でないときは、二要素認証された有効なユーザーIDが使用される。
			特定の役割のためのユーザーアクセス申請は、ユーザー管理者によって承認され、変更管理記録システムによってセキュリティグループに提出される。 職務分離が、アクセス要求、アクセス承認、アクセス権付与及びアクセスレビューする各人の間で存在している。
		プロビジョニング・プロセスによって与えられたアクセスが、職務の分離を危うくするか、意図的な悪意のある行為又はエラーのリスクを増大する。	可能であれば、システムとインフラストラクチャーの構成要素へのアクセスを制限する正式な役割ベースのアクセスコントロールを構築し、アクセスコントロールシステムによって実施される。それが可能でないときは、二要素認証された有効なユーザーIDが使用される。
			役割は、年次ベースで、資産オーナーとリスク管理グループの双方によって見直され更新される。見直しの結果として、アクセス権の変更申請は、変更申請記録によりセキュリティグループに提出される。
CC5.5	[セキュリティ、可用性、処理のインテグリティ、機密保持若しく	無許可の人のシステム構成要素への物理的アクセスは、構成要素（要	IDカード（身分証明書）を使用した物理アクセスの管理システムが、施設の周囲、施設の機密

規準		リスクの例示	統制の種類の例示
	はプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、システムを収容する設備（例えば、データセンター、バックアップ媒体保管庫、これらの所在地にある機密上重要なシステム構成要素のみならず他の機密上重要な所在地）への物理的なアクセスは、承認された要員に制限される。	員を含む。）へのダメージ、不正、誤った処理、無許可の論理アクセス、情報の毀損を結果としてもたらす。	区画の入退地点に導入されている。
			要員の写真付きの ID カード（身分証明書）は、施設への入館時、退館時、常時着用しなければならない。
			ID カード（身分証明書）は、要員のオリエンテーション期間中に人事部門によって用意され、全ての必要な調査が完了した後に配布される。ID カード（身分証明書）は、最初は、機密でないエリアにのみへのアクセスを提供する。
			機密エリアへのアクセス権限は、機密エリアのオーナーが承認したアクセス申請に基づき、必要な調査が実施され、問題が解決された後に、物理アクセス管理者によって ID カード（身分証明書）に追加される。アクセス権限に対する申請と変更は、変更管理記録システムによって、承認され、伝達される。
			契約担当は、ベンダーと契約者のために ID カード（身分証明書）の発行を申請するかもしれない。ID カード（身分証明書）は、承認された管理者による許可に基づき、物理セキュリティ管理者により作成される。申請は、変更管理記録システムによって、承認され、伝達される。
			（入館時に、）訪問者は、承認された訪問者であることを特定する一日訪問者識別章が発行される前に、承認された要員によって（記録簿に）署名されなければならない。
			訪問者バッチは、識別目的のためだけのものであり、施設のセ

規準		リスクの例示	統制の種類の例示
			キュアな区画へのアクセスは許可しない。
			全ての訪問者は、機密上重要なシステムとシステム構成要素が維持運用されている施設を訪問するときは、要員によって付き添われなければならない。
		以前は適切であった物理アクセスが、ユーザーのジョブ責任の変更やシステムの変更により不適切になる。結果として、職務の分離を損ない、又は意図的な悪意のある行為若しくはエラーによるリスクが増大する。	施設の機密上重要なエリアのオーナーは、半年毎に継続した業務上の必要性について確かめるため、それらのエリアへの物理的アクセスを付与された名前と役割のリストを見直す。変更の申請は、変更管理記録システムによってなされる。
		以前は承認されていた要員が、既に権限がなくなった後も、システムリソースに継続的にアクセスする。	設備の機密上重要な領域のオーナーは半年ごとにそれらの領域へのアクセスをレビューする。変更の申請は、変更管理記録システムによってなされる。
			ベンダーは半年ごとに ID カードと要員リストをレビューし、アクセス資格を確認し、及びいかなる変更（修正）も申請することが要求される。契約担当部署はベンダーレビューに基づいて変更を申請する。
			日次に、雇用の最終日に、人事システムは物理的セキュリティに対して、雇用の最終日である退職者のリストを送り、彼らのアクセスは取り消され、彼らの入館証は無効にされる。
		ユーザーが以前に承認された要員から識別証明と認証証明を入手し、それらを使いシステムに未承認のアクセスをする。	週次に、契約担当部署は、セキュリティグループに対しアクセスを取り消す必要のある契約が終了したベンダーや契約者のリストを送る。
			週次又は従業員の退職後直ちに、人事システムが物理的セキュリティグループに対しアクセスを取り消す必要のある退職者リストを送る。
			要員は、退職時面接の間に ID カードを返却することが求められ、全ての識別章は退職時面接の前に無効にされる。したがって、要員は、退職時面接の終了時に組織の施設より物理的に付き添われて退出しなければならない。
			入館証の共有や共連れはポリシーにより禁止される。
			マントラップ又は他の物理的装

規準		リスクの例示	統制の種類の例示
			置が、高度に機密上重要な設備のアクセス管理に使われる。
			マントラップを迂回するドアは、経営者の指定するメンバーの ID カードによってのみ開けることができる。
			監視プロセスが入退ポイントを監視するために存在する。警報システム、監視カメラ、訓練を受けた警備員などの対策（これに限定されない）が採用されている。情報（例えば、ログ、テープなど）が、将来参照するために、定められた期間で維持されている。
CC5.6	企業のコミットメントとシステム要求事項を満たすように、論理的なアクセスセキュリティ対策を、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関するシステム境界の外部要因による脅威から保護するために導入している。	システムへの脅威は、外部接続ポイントを通じて得られる。	インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために、定義された企業標準（アクセス管理ソフトウェア、企業設定標準及び各ユーザーやシステムアカウントにどの特権を帰属すべきかを定義した標準化されたアクセス統制リストの導入の要求事項を含む）がある。
			外部ユーザーによる企業の内部システム及び機器への未承認のアクセスを防止するため、外部接続ポイントは複数のファイアウォール、ネットワーク分割、データ漏洩防止（DLP）及び階層防御の組み合わせによって保護される。
			ファイアウォールのハードニング（堅牢化）標準は関連する適用可能な技術仕様に基づいており、製品及び業界の推奨実務と対比され、定期的に更新される。ファイアウォールのルールはネットワーク、システム及びデータストアのセキュリティ上の脅威リスクの低減のため速やかに更新されるように、セキュリティインシデント及びイベント管理（SIEM）ソフトは、継続してファイアウォールのログを収集し、ビジネスルール及び既知の脅威のシグニチャーを用いてログを分析し、特異な通信又はパケットを識別した場合はセキュリティとネットワーク運用チームへの警告を作成する。

規準		リスクの例示	統制の種類の例示
			非公開のサイトへの外部からのアクセスは、ユーザー認証及びVPN 及び SSL などのメッセージ暗号化システムを通じて制限される。
		システムへの承認された接続が破られ、システムへの不正アクセスを得るために利用される。	ファイアウォールのルールとオンラインシステムは、リモートアクセスが認められる時間を制限し、外部接続により実施される活動及びサービスリクエスト（例えば、コピーアンドペースト又はリモートプリント及びドライブマッピングの禁止）のタイプが制限される。
		通常の場所の外部に一時的に保存されたデータ（例えば、災害復旧テスト中に保存されている。）が、権限のない者によってアクセスされる。	災害復旧施設内のデータ・ストレージ・システムに書き込まれたデータは、施設ベンダーにストレージの管理を引き継ぐのに先立って、ディザスタリカバリのテストの終了時にサニタイズ手続の対象とされる。
CC5.7	情報の送信、移動及び削除は、許可された内部及び外部ユーザーとプロセスに制限され、そして、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及びシステム要求事項を満たすように送信、移動又は削除する間は保護される。	非公開情報が公衆通信網（経路）上を送信中に公開される。	定義された接続ポイントに関し、プロセッシングセンターとカスタマーネットワークの内外からプロセッシングセンターへ接続するユーザーの通信を保護するために、VPN、SSL、セキュアなファイル転送プログラム（SFTP）及び他の暗号技術が使われる。
			企業のポリシーは機微情報をインターネット又は他の公衆通信経路（例えば電子メール）を通じて送信することを、暗号化している場合を除き、禁止している。
			公衆通信経路への外部送信の機微情報をスキャン（検査）するため、ＤＬＰソフトウェアが使われる。制限された情報（例えば、社会保障番号[SSNｓ]、誕生日など）は、外部向け通信から、ブロック又は取り除かれるか、その両方が実施される。
		ロケーション間の物理的な移動の間にリムーバブルメディア（例えば、USB 機器、DVD 又はテープ）が紛失、奪取又は複製される。	バックアップ媒体は生成時に暗号化される。

規準		リスクの例示	統制の種類の例示
			ワークステーションとラップトップ用のストレージは暗号化される。ワークステーションとラップトップ用のリムーバブルメディアはソフトウェアによって自動的に暗号化される。リムーバブルメディアは組織が所有する他の装置によってのみ読み取れる。
			他のリムーバブルメディアはデータセンターの運用によって作成され、宅配便によって運ばれる。
			リムーバブルメディアの使用は、経営者により許可された場合を除き、ポリシーによって禁止されている。
		リムーバブルメディアはソフトウェアの不正な複製を作るために使われ、データはシステムの境界を越えて持ち去られる。	ワークステーションとラップトップ用のストレージは暗号化される。これらの装置のためのリムーバブルメディアはソフトウェアによって自動的に暗号化される。リムーバブルメディアは組織が所有する他の装置によってのみ読み取れる。
			バックアップ媒体は生成時に暗号化される。
CC5.8	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、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、対処する内部統制が実装されている。	悪意のある又は未承認のコードが、データ送信、リムーバルメディア及びポータブル又はモバイルデバイスを通じて、意図的又は無意識のうちに、論理的アクセス制御又はシステム機能を侵害する。	ワークステーション及びラップトップへのソフトウェアのインストールは、ＩＴサポート要員に制限される。
			アンチウィルスソフトウェアがワークステーション、ラップトップ、当該ソフトウェアをサポートするサーバーにインストールされている。アンチウィルスプログラムは、内部及び外部からアクセスすることが出来る、BYOD を含む、いかなるハードウェアもカバーしている。
			アンチウィルスソフトウェアは少なくとも日次で最新のウィルスパターンを受け取れるように設定されている。ネットワーク・オペレーターは 30 日間更新されていない機器の報告を受け取り、それらの機器をフォロー

規準		リスクの例示	統制の種類の例示
			アップする。
		ビジネスオーナーが、適切な承認なしにアプリケーションを入手し、インストールする。	システムにソフトウェアをインストールする権限は、変更実施要員及びシステム管理要員に制限されている。
CC6.0	システム運用に関する共通規準		
CC6.1	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関して、悪意ある行為、自然災害又はエラーに起因する違反やインシデントについてのシステム構成要素の脆弱性は、識別、監視及び評価され、対応策が既知及び新規に識別された脆弱性を補うために設計、実装及び運用される。	違反やインシデントにつながる脆弱性が適時に検出されない。	ロギング及びモニタリングソフトウェアは、システムインフラストラクチャー構成要素及びエンドポイントシステムからデータを収集するために使われる。また、システムパフォーマンス、潜在的なセキュリティ脅威及び脆弱性、リソースの利用をモニターするため、及び通常でないシステム活動又はサービスリクエストを検出するために使われる。このソフトウェアは運用センター及びセキュリティ部署にメッセージを送り、自動的に優先順位の高いインシデントチケット又はプロブレムチケット及び変更管理システム記録事項をオープンする。
			コールセンター要員がサポートのため電話及び電子メールのリクエストを受け取る。それらの中にはユーザーパスワードのリセット又は潜在的な違反やインシデントを企業の要員に通知するリクエストを含むかもしれない。コールセンター要員は受け取ったリクエストの記録、解決及びエスカレーションのための定義された手順に従う。
			脆弱性のモニタリングスキャンが、定期的に行われる。経営者は、スキャン結果に基づいて適切な措置を講じる。
			データ漏洩防止及び検出ツールは、パーソナル・インフォメーションの送信を識別するために、システム境界に設置される。
			脆弱性が検出された場合、データセンター運用要員が文書化された対策戦略を導入する。
		セキュリティやその他のシステム構成情報が	自動化システムを用いて、週次でフルシステムのバックアッ

規準		リスクの例示	統制の種類の例示
		破損又は破壊され、システムが設計されたとおりに機能しなくなる。	プ、日次で差分バックアップが行われる。
CC6.2	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関して、論理的及び物理的セキュリティ違反、障害、識別された脆弱性を含むインシデントは、企業のコミットメントとシステム要求事項を満たすように、確立されたインシデント対応手順に従って、識別され、適切な要員に報告され、対処される。	違反やインシデントが、その影響について、識別、優先順位付け又は評価がされない。	運用要員が、定められた手順に従って、報告された違反又はその他関係するインシデントの兆候のあるシステム事象を評価する。セキュリティに関する事象は、評価に向けてセキュリティグループに割り当てられる。プライバシー・インシデントは、評価のために適切なプライバシー要員に割り当てられる。
		違反やインシデントに対処する是正措置が適時、適切に実装されない。	運用及びセキュリティ要員は、定められた手順に従って、報告された事象を解決、エスカレーションする。これには、必要により経営者にエスカレーションする根本的な原因分析を含む。
			セキュリティ事象（インシデント又は問題）の解決（策）は、日次及び週次で、運用及びセキュリティのグループ会議でレビューされる。
			内部と外部のシステム利用者はインシデントについて適時に伝えられ、それぞれの側で行うべき是正措置について助言される。
		是正措置が、有効又は十分でない。	事象の解決（策）は週次の運用とセキュリティのグループ会議でレビューされる。
			変更管理要求は、恒久的な是正のためオープンされる。
		方針や手続の遵守不足が、制裁や改善措置を通じて対処されず、その結果、将来、コンプライアンス違反が増加する。	事象の解決（策）は週次の運用とセキュリティのグループ会議でレビューされる。内部及び外部ユーザー又は顧客に影響を及ぼす関連する事象は、ユーザー又は顧客対応部署に回される。
			企業の方針に、要員の不正について、謹慎、停職や解雇を含む懲戒が定められている。
		防止措置が前の事象が発生した後も実装されず、違反とインシデントが再発する。	変更管理要求は、恒久的な是正のためオープンされる。
CC7.0	変更管理に関する共通規準		
CC7.1	[セキュリティ、可用	コミットメントとシス	システム変更要求は、変更が変

規準		リスクの例示	統制の種類の例示
	性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及びシステム要求事項は、システム構成要素の設計、調達、導入（実装）、設定、テスト、修正、承認と維持を含んだシステム開発ライフサイクルを通じて対処される。	テム要求事項が、システム開発ライフサイクルの間の幾つかのポイントで対処されず、その結果、コミットメントとシステム要求事項を充足していないシステムがもたらされる。	更管理プロセスを通じて、セキュリティ、可用性、処理のインテグリティ、機密保持に関するコミットメントとシステム要求事項への潜在的な影響を明らかにするために評価される。
			システム変更は、小規模に分類されるものを除き、実装する前に、最高情報セキュリティ責任者と運用責任者の承認が必要である。
CC7.2	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメント及びシステム要求事項との整合性を保つために、インフラストラクチャー、データ、ソフトウェア及びポリシーと手続が必要に応じて更新される。	システム構成要素が、要求事項が変更されても更新されず、その結果、コミットメントとシステム要求事項を充足していないシステムがもたらされる。	継続的なリスク評価プロセスと定期的な計画と予算プロセスの間に、インフラストラクチャー、データ、ソフトウェア及び手続は、必要とされる変更について評価される。変更要求は、識別された必要性を基に作成される。
			深刻度の高いインシデントに関しては、根本的な原因分析が準備され、運用責任者にレビューされる。計画されたインシデント及び問題解決（策）を反映するために、根本的な原因分析を基に、変更要求は用意され、企業のリスクマネジメントプロセスと関連するリスクマネジメントデータは、更新される。
CC7.3	[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関する企業のコミットメントとシステム要求事項を満たすように、システムの運用中及び監視中に、内部統制のデザイン又	識別された不正、インシデント、その他システムの不具合が変更管理サイクルの中で考慮されない	深刻度の高いインシデントに関しては、根本的な原因分析が準備され、運用責任者にレビューされる。計画されたインシデント及び問題解決（策）を反映するために、根本的な原因分析を基に、変更要求は用意され、企業のリスクマネジメントプロセスと関連するリスクマネジメントデータは、更新される。

規準		リスクの例示	統制の種類の例示
	は運用の有効性に不備が識別されると、変更管理プロセスが開始される。		
			緊急の変更を管理するためのプロセスが、存在する。
CC7.4	システム構成要素への変更は、企業の[セキュリティ、可用性、処理のインテグリティ、機密保持若しくはプライバシー又はそれらの組合せで報告対象の原則を挿入]に関するコミットメント及びシステム要求事項を満たすよう、（起案）承認され、設計され、開発され、設定され、文書化され、テストされ、（リリース）承認され、実装される。	システムの変更が、システムの設計と運用に責任を負う者によって承認されず、その結果、コミットメントとシステム要求事項を満たす能力を毀損するシステムの変更がもたらされる。	システム変更要求は、要求された変更作業を開始する前に、インフラストラクチャーもしくはソフトウェアのオーナーと変更諮問委員会によってレビューされ、承認されなければならない。変更を承認と、変更の実施は、異なる要員が責任を負う。
		システム変更が意図されたとおりに機能せず、その結果、コミットメントとシステム要求事項を満たさない。	機能及び詳細設計が軽微な変更以外（××時間以上）は用意される。機能設計はアプリケーションオーナー、インフラストラクチャーオーナー及びソフトウェアオーナーにレビューされ、承認される。詳細設計はアプリケーション開発の責任者と変更諮問委員会によって要求された変更又は、開発プロジェクトの作業が開始する前に承認される。
			テスト計画、テストデータは、作成され、要求仕様テスト、回帰テストに利用される。テスト計画とテストデータはテスト管理者により、テスト前とテスト完了時にレビューされ、承認され、新たな開発やソフトウェアの変更は本番移行前に変更諮問委員会によってレビューされる。セキュリティ脆弱性テストは、関連するアプリケーション、データベース、ネットワーク及びオペレーティング・システムの変更に関して実施されるテストに含まれる。
			システムと回帰テストは、承認されたテスト計画とテストデータを使用して、テスト部門によって準備される。 計画された結果からの逸脱は分析され開発者に提供される。
			静的コード分析ツールを使用し

規準		リスクの例示	統制の種類の例示
			て開発されたソースとオブジェクトコードライブラリのセキュリティ脆弱性スキャンが実行されている。経営者は、重大なセキュリティ上の脆弱性及びコーディングの欠陥を、コンピュータ・プログラムをコンパイルし、本番環境にそれらを統合する前に修復される。
			コードレビュー又はウォークスルーは定められた規準（コードレビューとウォークスルーを必須とする）を充足する大きな影響のある変更に要請される。これらは変更について責務を負わない同レベルのプログラマーによってレビューされる。
			変更は、実行前に変更諮問委員会により、レビュー、承認される。
			インフラストラクチャーとソフトウェアのハードニング（堅牢化）及び設定のために、定義された企業標準（アクセス管理ソフトウェア、企業設定標準及び標準化されたアクセス統制リストの導入のための要求事項を含む）がある。
			ハードニング（堅牢化）標準の変更はインフラストラクチャー管理担当責任者によりレビュー、承認される。
		未承認の変更がシステムになされ、その結果コミットメント及びシステム要求事項を満たさないシステムがもたらされる。	隔離された環境が、開発、テスト及び本番環境で使用される。開発者は、テスト又は本番環境でのソフトウェアを変更することができない。
			論理的アクセスコントロール及び変更管理ツールにより、開発、テスト及び本番環境からの移行能力を変更配置要員に制限する。
			変更は、実装前に変更諮問委員会により、レビュー、承認される。
		予見不能なシステム導入の問題により、システムの運用が毀損され、結果としてシステムが設計どおりに機能しない。	運用やバックアウト手順の確認を含む引渡プロセスは、全ての移行に利用される。
			システム変更の作業の確認のためにデザインされた実装後手続は、小規模な変更を除き実装の後、プロジェクト計画時に決定した明確な期間実施され、結果は、コミットメント及びシステ

規準		リスクの例示	統制の種類の例示
			ム要求事項を満たすために必要なものとして内部及び外部ユーザー又は顧客と共有される。
		変更管理プロセスにおける両立しない職務の存在（特に承認者、設計担当者、実装担当者、テスト担当者及びオーナー）は、結果として意図した機能と異なるシステムの実装をもたらす。	変更管理プロセスは、下記の役割及びその割当を定義されている。 ・ 変更要求の承認－オーナーもしくはビジネスユニット管理者 ・ 開発－アプリケーション設計及びサポート部門 ・ テスト－品質保証部門 ・ 実装－ソフトウェア変更管理グループ
可用性に関する追加規準			
A1.1	企業の可用性に関するコミットメント及びシステム要求事項を満たすように、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、現在の処理能力と使用率が保持され、監視され、評価されている。	現状の処理能力は、システム構成要素における個々の要素の喪失時に可用性のコミットメント及びシステム要求事項を十分に満たさない。	処理能力は、SLA、KPI 及びその他のパフォーマンス関連のパラメーターに従って、継続的に監視される。
			重要なインフラストラクチャー構成要素は、重要性の分類によりレビューされ最低限の冗長性が割当てられる。
		企業のコミットメント及びシステム要求事項を満たすシステムの継続的可用性を提供するよう、処理能力が必要に応じて監視、計画及び拡張又は変更されない。	処理能力の監視は日次で実施される。
			将来の処理要求は、継続的に予測され、計画された能力と比較される。予測は、上級運用責任者により承認される。変更要求は、承認された予測に基づき必要なものとして提起される。
A1.2	企業の可用性に関するコミットメント及びシステム要求事項を満たすように、物理的設備対策、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が承認され、設計され、開発され、実装され、稼働し、許可され、保持され、監視されている。	環境上の脆弱性と環境条件変化が識別されない、又は、物理的設備対策の利用による対処が行われず、結果としてシステム可用性を喪失する。	物理的設備対策は、下記を含み導入される。 ・ 冷却装置 ・ 電源障害の事故のバックアップとしてのバッテリー及び天然ガス発電機 ・ 通信回線の冗長化 ・ 煙探知機 ・ ドライパイプ式スプリンクラー ・ 害獣及び害虫制御
		環境上の脆弱性が、監視	運用要員は、各シフトの間の物

規準		リスクの例示	統制の種類の例示
		されず、又は、環境上の事象の重要性の増加に対応されない。	理的設備対策の状況を監視する。警報装置が、環境上の閾値のいかなる相違も伝達するために設置されている。
			物理的設備対策は、少なくとも年次で保守を受ける。
		処理エラー、意図的行為又は環境上の事象により、ソフトウェア又はデータが喪失又は利用できない。	週次のフルバックアップと日次の差分バックアップが自動化システムにより実行される。
			バックアップは自動化システムの利用の失敗について監視され、インシデント管理プロセスが自動的に発動される。
			バックアップは、承認された配送業者（外部保管の場合）及び暗号化されない場合には同伴者が同行する環境的に管理された状況で、第三者の保管業者により輸送され外部保管される。
		復旧インフラストラクチャーの不備により、可用性のコミットメント及びシステム要求事項が満たされない。	事業継続及び災害対策計画が作成され、更新され、年次でテストされる。
			企業は、データセンターの災害時のＩＴ運用の再開を可能にするため、第三者復旧施設と契約を行っている。
			企業は、施設の喪失時に他企業の施設での運用の再開を可能とするため施設のマルチロケーション戦略を利用する。
A1.3	企業の可用性に関するコミットメント及びシステム要求事項を満たすように、システム復旧を支援する復旧計画の手続がテストされている。	企業のコミットメント及びシステム要求事項を満たすシステム運用の復旧を可能とするための復旧計画が適切にデザインされていない、又は、バックアップが十分でない。	事業継続及び災害復旧計画（バックアップの復元及び緊急時通報システムを含む。）は、年次でテストされる。
			テスト結果は、レビューされ、コンティンジェンシープランは修正される。
処理のインテグリティに関する追加規準			
PI1.1	企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、処理エラーを防止し、検出し、是正する手続が存在する。	処理エラー、意図的行為又は環境上の事象によりソフトウェア又はデータが喪失又は利用できない。	週次のフルバックアップと日次の差分バックアップが自動化システムにより実行される。
			バックアップは自動化システムの利用の失敗について監視され、インシデント管理プロセス

規準		リスクの例示	統制の種類の例示
			が自動的に発動される。
			バックアップは、第三者の保管業者により輸送され外部保管される。
		環境上の脆弱性は、システム可用性の喪失についての物理的設備対策の利用による対処が行われない。	物理的設備対策は、下記を含み導入される。 ・　冷却装置 ・　電源障害の事故のバックアップとしてのバッテリー及び天然ガス発電機 ・　通信回線の冗長化 ・　煙探知機 ・　ドライパイプ式スプリンクラー
		環境上の脆弱性に関する、モニターや環境的事象の厳密さを向上させる活動が実施されていない。	運用要員は、各シフトの間の物理的設備対策の状況を監視する。
			物理的設備対策は、少なくとも年次で保守を受ける。
		現在の処理能力は、処理誤りが発生する処理要求に対応していない。	処理能力の監視は日次で実施される。
			重要なインフラストラクチャー構成要素は、リスクアセスメントに基づいて定義されたレベルの冗長性を維持している。
PI1.2	システム入力は、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、完全に、正確に、適時に測定され、記録される。	入力が誤って取り込まれる。	様式チェックは、規定値の範囲に入力を制限する。
			データ準備担当者は、文書を受信した日ごとに一括処理し、日付及びバッチチケットのシートの数を入力する。バッチフォームは、購入したイメージシステムでスキャンされる。スキャン処理が完了すると、スキャンされたシートは、スキャン担当者により、バッチチケットごとの数量と比較される。
			スキャンされたイメージは、OCR処理される。顧客ID、顧客名及びレコード種別を含むキーフィールドは、システムによりマスターデータと照合される。
			スキャンシートの自由記入欄の記述は、手作業で入力される。当該情報は、２名の異なる担当者により入力される。その入力情報を比較し、誤りがある記録は、解消のため３人目の担当者

規準		リスクの例示	統制の種類の例示
			に送られる。
		入力が取り込まれないか、完全に取り込まれない。	システムエディットは、必須項目について、レコードが承認される前に、完全であることが要求される。
			データ準備担当者は、文書を受信した日付及びバッチチケットのシートごとに一括処理する。バッチフォームは、購入したイメージシステムでスキャンされる。スキャン処理が完了すると、スキャンされたシートは、スキャン担当者によりバッチチケットごとの数量と比較される。
			スキャンされたイメージは、OCR処理される。顧客ID、顧客名及びレコード種別を含むキーフィールドは、システムによりマスターデータと照合される。
			スキャンシートの自由記入欄の記述は、手作業で入力される。当該情報は、２名の異なる担当者により入力される。その入力情報を比較し、誤りがある記録は、解消のため３人目の担当者に送られる。
			バッチコントロールトータルを含む電子ファイルを受信する。取り込み処理の間、取り込んだデータは、アプリケーションにより自動的にバッチトータルと照合される。
		入力が適時に取り込まれない。	受信した電子ファイルが、受信した時点で処理される。 アプリケーションは、処理が完了せずに終了したファイルを監視し、インシデント管理のためのエラーレコードを作成する。
			手作業のデータ入力フォームは、受領時に一括処理される。バッチは、日次入力監督者により、日次処理のための入力がトレースされ、相違点が調査される。
		入力の最終保管は、正しく処理された事の検証のために、そのソースをトレースできなく、そして、処理結果の完全性と正確性を検証するために初期の入力にトレースできない。	入力は、ID番号、登録番号、登録情報又はタイムスタンプを符合することにより、初期の入力から出力及び最終保管、出力から入力源をトレースできる。
PI1.3	データは、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように	データを、処理の途中に紛失する。	入力レコード数は、入力から最終処理までトレースされる。全ての相違点は、調査される。

規準		リスクの例示	統制の種類の例示
	承認されたとおりに、完全に、正確に、適時に処理される。		
		データが、処理の途中に不正確に変更される。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			出力値は、先行処理の値と比較される。X%以上の差異は、差異報告書上でフラッグが立ち、インシデント管理システムに記録され、そして、出力担当者により調査される。解決策は、インシデント管理システムに文書化される。未解決のインシデントは、運用責任者により日次でレビューされる。
			日次、週次及び月次の趨勢報告書は、異常な傾向を把握するため、運用責任者によりレビューされる。
		新しく作成されたデータが、不正確である。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			システムが、生成された値と許容値を比較する。許容値外の値は、例外値報告書に記載される。例外値報告書の項目は、日次で、出力担当者によりレビューされる。
		処理が、要求された時間内に完了しない。	スケジュールソフトを、ジョブの投入とジョブ実行のモニタリングの制御に使用する。インシデント管理記録は、プロセスエラーが識別された時に、サービス管理システムに自動的に生成される。
PI1.4	データは、企業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、特定された期間、完全、正確かつ適時に格納され、保持される。	データが、コミット又は合意したように、使用できない。	アプリケーションデータファイルのミラーイメージは、夜間に作成され、システムの中断又は停止時に、復旧及び復元に使用するため、セカンドシステムに保存される。
		保存されたデータが、不正確である。	保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
		保存されたデータが、不完全である。	データは、前の期間の残高と月次の活動を繰り越した結果と保持されたデータ残高と比較して、月次で照合される。
PI1.5	システム出力は、企業の処理のインテグリティに関するコミットメント及びシステ	システム出力が、完全でない。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。

規準		リスクの例示	統制の種類の例示
	ム要求事項を満たすように、完全で、正確で、配布され、そして保持される。		
			出力値は、先行処理の値と比較される。5%以上の差異は、差異報告書上でフラッグが立ち、インシデント管理システムに記録され、そして、出力担当者により調査される。解決策は、インシデント管理システムに文書化される。未解決のインシデントは、運用責任者により日次でレビューされる。
			処理レコード合計は、電子申請、手入力及び OCR システムでスキャンされたシートによる受領レコード合計と月次で、比較される。
		システム出力が、正確でない。	アプリケーション回帰テストは、変更管理プロセスの中で、アプリケーションの主要なプロセスを検証する。
			出力値は、先行処理の値と比較される。X%以上の差異は、差異報告書上でフラッグが立ち、インシデント管理システムに記録され、そして、出力担当者により調査される。解決策は、インシデント管理システムに文書化される。未解決のインシデントは、運用責任者により日次でレビューされる。
			日次、週次及び月次の趨勢報告書は、異常な傾向を把握するため、運用責任者によりレビューされる。
		システム出力が、未承認の受信者に提供される。	アプリケーションセキュリティ（システム）は、承認されたユーザーID に出力を制限する。
		システム出力を、許可された受信者が利用できない。	出力は、マスタースケジュールに従って、システムにより生成される。マスタースケジュールの変更は、変更管理プロセスを通じて管理され、カスタマーサービス執行役により承認される。日次で、自動ルーチンは、出力ファイルをスキャンし、全ての必要な出力が生成されたことを検証する。当該ルーチンは、全ての紛失した出力のインシデントの記録を、生成する。インシデントチケットは、インシデント管理プロセスで管理される。
PI1.6	通常の取引処理以外のデータの修正は、企	データが、未承認のプロセス又は手続により修	アプリケーション回帰テストは、変更管理プロセスの中で、

規準		リスクの例示	統制の種類の例示
	業の処理のインテグリティに関するコミットメント及びシステム要求事項を満たすように、承認され、処理される。	正され、結果として、不正確又は不完全なデータになる。	アプリケーションの主要なプロセスを検証する。
			データへのアクセスは、アクセス管理ソフトウェアにより承認されたアプリケーションに制限される。アクセスルールは、アプリケーション開発プロセスを通じて、情報セキュリティ要員により、作成、更新される。
			アプリケーションレベルのセキュリティは、アクセス制御リストの記録を通してアクセス権を付与されている許可された内部及び外部ユーザーの、データへのアクセス、変更、削除の能力を制限します。アクセス管理記録の生成と変更は、アクセス権提供プロセスを通じて行われる。
		データが、承認を得ずに、変更される。	保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
		データが、喪失又は破壊される。	保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
			アプリケーションデータファイルのミラーイメージは、夜間に作成され、システムの中断又は停止時に、復旧及び復元に使用するため、セカンドセキュアシステムに保存される。
機密保持に関する追加規準			
C1.1	機密情報は、企業の機密保持に関するコミットメント及びシステム要求事項を満たすように、システム設計、開発、テスト、実装及び変更プロセスの間、保護されている	本番環境以外で使用されるデータは、コミットしたとおりに未承認のアクセスから保護されていない。	企業は、テストデータベースの作成に先行して、機密情報をテスト情報に置き換えるデータマスキングソフトウェアを使用して、テストデータを作成する。
			データオーナーは、本番環境以外の全てのストレージや本番情報の使用を承認する。
C1.2	システム領域内の機密情報は、企業の機密保持に関するコミットメント及びシステム要求事項を満たすように、入力、処理、保管、出力及び廃棄の間、未承認のアクセス、使用及び開示から保護されている。	機密情報への未承認のアクセスが、処理の途中に行われる。	データへのアクセスは、アクセス管理ソフトウェアにより承認されたアプリケーションに制限される。アクセスルールは、アプリケーション開発プロセスを通じて、情報セキュリティ要員により、作成、更新される。

規準		リスクの例示	統制の種類の例示
			承認されたアプリケーション以外からの論理アクセスは、データベース管理システム固有のセキュリティを通じて、管理者に制限される。データベース管理システムのためのアクセス管理記録の生成と変更は、アクセス権提供プロセスを通じて行われる。
			アプリケーションレベルのセキュリティは、アクセス制御リストの記録を通してアクセス権を付与されている許可された内部及び外部ユーザーの、データへのアクセス、変更、削除の能力を制限します。アクセス管理記録の生成と変更は、アクセス権提供プロセスを通じて行われる。
		出力に含まれる機密情報への未承認のアクセスが、処理後に行われる。	アプリケーションセキュリティ（システム）は、承認されたユーザーIDに出力を制限する。
			機微情報を含む出力は、安全な出力機器で印刷され、そして、「機密」と記載される。
			専用用紙は、データ記入後、物理的に厳重に保管される。 物理的なアクセスは、保管担当者に制限される。
			ビジネスプロセス、システム、及び第三者の関与に関連するパーソナル・インフォメーション（パブリック情報及び機微情報の両方）は、データ管理ポリシー及び手順内の重大性及びリスクに基づいて明確に識別及び分類される。 パーソナル・インフォメーションと機微情報の量が特定される。
			意識向上トレーニングは、パーソナル・インフォメーションのポリシーと使用法に関係する要員に提供される。
C1.3	機密情報へのシステム領域外からのアクセス及び機密情報の開示が、企業の機密保持に関するコミットメント及びシステム要求事項を満たすように、承認された当事者に制限されている。	システム境界を越える伝送により機密情報が、未承認のユーザー企業の要員に提供される。	アプリケーションセキュリティ（システム）は、承認されたユーザーIDに出力を制限する。
			電子的な出力のシステム境界を越えての伝送は、高度暗号化標準（AES）をサポートする承認されたソフトウェアの利用を通じ

規準		リスクの例示	統制の種類の例示
			て行われる。
			保存データの論理アクセスは、アプリケーション及びデータベース管理者に制限される。
			データは、AES をサポートするソフトウェアを使用して暗号化された形式で保存される。
			リムーバブルメディアの使用は、経営者により許可された場合を除き、ポリシーによって禁止されている。
		機密情報が、機密保持コミットメントに違反して、関連する組織、ベンダー又は他の承認された組織に伝送される。	アプリケーションセキュリティ（システム）は、承認されたユーザーIDに、出力を制限する。
			電子的な出力のシステム境界を越えての伝送は、AES をサポートする承認されたソフトウェアの利用を通じて行われる。
			機密書類は、保存スケジュールに従って、施錠された保管箱に格納されている。受託会社は、法的な保全要求の場合には、他のクライアントデータに影響を与えることなく、クライアントデータを識別、捕捉、保存及び転送する能力を有している。
			非開示同意書や機密保持同意書は、機密情報へのアクセス権を持つ全ての要員によって署名される。
C1.4	企業は、システムの一部として、機密情報へのアクセスを持つ、製品やサービスを提供するベンダー及び他の第三者から、企業の機密保持システム要件に整合する機密保持に関するコミットメントを入手している。	関係する組織及びベンダーの要員が、企業の機密保持コミットメントを認識していない。	正式な情報共有合意書が関係する組織及びベンダーと締結されている。当該合意書には、当該組織に適用される機密保持コミットメントを含んでいる。合意書の項目には、機密データのマーキングや識別、関係する組織及びベンダーの管理下で機密情報を取扱う基準、及び不要になった機密情報の返還及び廃棄の要求事項を含んでいる。
		機密情報を取り扱う要求事項が、関係する組織又はベンダーに、通知又は合意されていない。	正式な情報共有合意書が関係する組織及びベンダーと締結されている。当該合意書には、当該組織に適用される機密保持コミットメントを含んでいる。
C1.5	システムの一部になる製品やサービスのベンダー及び他の第三者による、企業の機密保持に関するコミットメント及びシステム要求事項の遵守状況が、定期的及び必要に応じて評価され、	関係する組織及びベンダーのシステムが、機密保持コミットメントを遵守するよう適切にデザインされていないか、有効に運用されていない。	関係する組織及びベンダーのシステムを、ベンダーリスク管理プロセスの一部として調査の対象とする。可能であれば、保証報告書（SOC2 報告書）を、入手し、評価する。サイト訪問や他の手続きを企業のベンダー管理ガイドラインに基づいて実施する。

規準		リスクの例示	統制の種類の例示
	必要な是正措置が取られる。		
C1.6	企業の機密保持のコミットメント及びシステム要求事項の変更が、内部及び外部ユーザー、製品やサービスがシステムの一部となるベンダー及び第三者に伝達される。	機密保持実務及びコミットメントが、内部及び外部ユーザーの認識又は同意なしに変更される。	最高情報セキュリティ責任者は、機密保持実務及びコミットメントの変更に責任を有する。内部及び外部ユーザー、関係する組織及びベンダーとそれらの変更についてコミュニケーションをするために、正式なプロセスが用いられる。
		機密保持実務及びコミットメントが、関係する組織又はベンダーの認識なしに変更され、結果として、システムが要求される実務を遵守できず、コミットメントを充足しない。	最高情報セキュリティ責任者は、機密保持実務及びコミットメントの変更に責任を有する。内部及び外部ユーザー、関係する組織及びベンダーとそれらの変更についてコミュニケーションをするために、正式なプロセスが用いられる。
			関係する組織及びベンダーの合意書が、機密保持実務及びコミットメントの変更を反映して修正される。
			関係する組織及びベンダーのシステムを、ベンダーリスク管理プロセスの一部として調査の対象とする。可能であれば、保証報告書（SOC2 報告書）を、入手し、評価する。サイト訪問や他の手続きを企業のベンダー管理ガイドラインに基づいて実施する。
	企業は、企業の機密保持のコミットメント及びシステム要求事項を満たすように、機密情報を保持する。	機密情報が、記載された目的に関連して、記載された目的を達成するために必要な期間以上、又は、企業の機密保持契約及びシステム要求事項で許容される期間以上に保存される。	企業は、その維持する機密情報の保持期間に関連する文書化されたポリシーを確立する。企業は、 ・　特定の保存要件に応じて、機密情報を削除するために、システム・プロセスを自動化している。 ・　定義されたスケジュールに従ってバックアップ情報を削除する。 ・　機密情報が保存期間を超えて保持されるためには承認される必要があり、そして、保持のためにそれらの情報は特別にマークされる。 ・　毎年、保持のためにマークされた情報をレビューする。
	企業は、企業の機密保持のコミットメント及びシステム要求事項を満たすように、機密情報を廃棄する。	機密情報が、機密保持コミットメント及びシステム要求事項に準じて、破壊されない。	企業は、 ・　必要に応じて、特定の機密情報を、検索し、削除又は編集する。 ・　機密保持に関するコミットメント又はシステム要求事項で、特定された目的のためにもはや必要とされない機密情

規準		リスクの例示	統制の種類の例示
			報を定期的かつ手順どおりに破壊、消去又は匿名化する。 ・　保存方法（例えば、電子媒体、光学媒体、又は紙媒体）に関わらず、保持ポリシーに基づいて記録を消去又は破壊する。 ・　オリジナル、アーカイブ、バックアップ及びアドホック又は個人的なコピーは、破壊ポリシーに従って、処分する。 ・　機密情報の廃棄について文書化する。
プライバシーに関する追加規準			
P1.0	コミットメント及びシステム要求事項の通知及びコミュニケーションに関するプライバシー規準		
P1.1	企業は、企業のプライバシー・コミットメント及びシステム要求事項を満たすようにプライバシー実務についてデータ主体（本人）に通知する。 通知は、企業のプライバシー・コミットメント及びシステム要求事項を満たすようにパーソナル・インフォメーションの利用の変更を含む、企業のプライバシー行動の変更に関し適時に更新され、データ主体（本人）に伝えられる。	データ主体（本人）は、パーソナル・インフォメーションの収集、利用及び保持の目的が通知されず、よって規制の遵守違反（例えば、公正情報行動原則（FIPPs）、医療保険の携行性と責任に関する法律（HIPAA）また連邦取引委員会に関して）、また企業の評判の低下の可能性が生じる。	企業は、システムのデータ主体（本人）に企業のプライバシー実務に関する通知を行う（データ収集時、収集の形態ごと、及び企業のプライバシー実務が変更になる時点）。 通知は、 ・　容易に入手可能とし、パーソナル・インフォメーションがデータ主体(本人)から最初に収集される時点で利用可能となるようにする。 ・　データ主体（本人）がパーソナル・インフォメーションを企業に提出すべきか否かを決定できるように適時に提供される（すなわち、パーソナル・インフォメーションが収集される時点又はそれ以前、あるいはその後できる限り速やかに）。 ・　データ主体（本人）が最後に読んだとき、またパーソナル・インフォメーションを企業に最後に提出したとき以降、通知内容が変更になっていないかどうかを判断できるように日付が明確に記載される。 さらに、企業は、 ・　企業のプライバシーに関する通知の履歴を追跡する。 ・　以前のプライバシーに関する通知の変更を（例えば、企業のウェブサイトへの通知の掲載、郵便による通知文の送付、又は電子メールの送付などにより）データ主体（本人）に伝える。 ・　データ主体（本人）に伝達したプライバシー実務の変更

規準		リスクの例示	統制の種類の例示
			を文書化する。
			四半期ごとに CPO とプライバシー担当者は会議を開き、パーソナル・インフォメーション項目の詳細な利用、オプトアウトできる権利、拡張（エンハンスメント）（付加（エンリッチメント））や推測（インファレンス）、共有、開示、アクセス、セキュリティ、保持、及び処分を含む、収集される新たな種類のパーソナル・インフォメーション及びプライバシー実務への影響を議論する。いかなる収集される新たなパーソナル・インフォメーションに関して、通知をデータ主体（本人）に行うためにシステムとプロセスが更新される。
		データ主体（本人）が、以下の一つ又は複数の項目について通知されていない。 ・ パーソナル・インフォメーションの収集又は収集のオプトアウトに対し整備される選択及び同意の仕組み ・ パーソナル・インフォメーションの保持、共有、開示及び処分 ・ パーソナル・インフォメーションに関し、アクセス、変更、又は連絡若しくは問い合わせ出来るよう整備されたプロセス ・ データ主体（主体）が提供する以外に収集されるパーソナル・インフォメーションの追加ソース	企業は、システムのデータ主体（本人）に企業のプライバシー実務に関する通知を行う（データ収集時、収集の形態ごと、及び企業のプライバシー行動が変更になる時点）。CPO は通知をレビューし、通知には以下の開示が含まれることを承認する旨を文書化する。 ・ パーソナル・インフォメーションの収集時及びパーソナル・インフォメーションの目的及び利用の変更時における、パーソナル・インフォメーションの収集及びパーソナル・インフォメーション及び利用に関するオプトアウトの仕組みの通知 ・ パーソナル・インフォメーションの保持、共有、開示及び処分に関する方針 ・ パーソナル・インフォメーションに関し、アクセス、変更、又は連絡若しくは問い合わせが出来る仕組み ・ 収集時にデータ主体（本人）により既に提供されていた（相互参照を通じての）パーソナル・インフォメーションの拡張(エンハンス)、付加(エンリッチ）又は推測（インファレンス）に向けて利用されるパーソナル・インフォメーションの追加ソース
P1.2	企業のプライバシー・コミットメントが外部ユーザーに適切に通知され、それらのコミットメント及び	内部及び外部ユーザーが、能動的及び受動的手段の両方を通じて収集されるパーソナル・インフォメーションについ	企業は、システムのデータ主体（本人）に企業のプライバシー実務に関する通知を行う（電子メール又は通常郵便を通じて、データ収集時、収集の形態ごと、

規準		リスクの例示	統制の種類の例示
	関連するシステム要求事項が、内部ユーザーがその責任を遂行できるように伝えられる。	て通知されていない、又は認識していない。	及び企業のプライバシー実務が変更になる時点で行う)。
		プライバシー・コミットメント及びシステム要求事項が、パーソナル・インフォメーションが、収集される前に、又は収集後できる限り速やかに、内部及び外部ユーザーに伝えられていない。	パーソナル・インフォメーションが収集される前に、企業は、パーソナル・インフォメーションの詳細な利用方法、オプトアウトできる権利、拡張（エンハンスメント）(付加（エンリッチメント))、推測（インファレンス)、共有、開示、アクセス、セキュリティ、保持及び処分を含む、パーソナル・インフォメーションの収集目的及び利用を内部及び外部ユーザーに伝える。
		パーソナル・インフォメーションの収集又は利用のオプトアウトのため、内部及び外部ユーザーに情報の利用に関するプライバシー・コミットメント又はシステム要求事項の変更が、適時に通知されない。	変更がなされる前に、企業は、パーソナル・インフォメーションの詳細な利用、オプトアウトできる権利、拡張（エンハンスメント）(付加（エンリッチメント))、推測（インファレンス)、共有、開示、アクセス、セキュリティ、保持及び処分を含む、パーソナル・インフォメーションの目的及び利用の変更を内部及び外部ユーザーに伝える。
		内部及び外部ユーザーに、企業のパーソナル・インフォメーションの利用の性質及び範囲に関し十分な情報が与えられない。	パーソナル・インフォメーションが収集される前に、企業は、パーソナル・インフォメーションの詳細な利用方法、オプトアウトできる権利、拡張（エンハンスメント）(付加（エンリッチメント))、推測（インファレンス)、共有、開示、アクセス、セキュリティ、保持及び処分を含む、パーソナル・インフォメーションの収集の目的及び利用を内部及び外部ユーザーに伝える。
P2.0	選択及び同意に関するプライバシー規準		
P2.1	企業は、パーソナル・インフォメーションの収集、利用、保持、開示及び廃棄に関する可能な選択、各選択の影響をデータ主体（本人）に伝える。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な同意が求められる場合には、データ主体（本人）又はその他権限を付与された個人	同意の方針及び手続が、選択及び同意に関するオプションについて述べていない。データ主体（本人）が、アクティブ・コミュニケーションの存在を示す同意を「表明」していない。	選択及び同意に関するオプションについての情報を含む、方針及び手続は以下を含む。 ・ 同意は、パーソナル・インフォメーションを処理又は取り扱う前に、取得される。 ・ 同意が自由に与えられる事を確保できるよう、同意の要求は、虚偽による強要がない、又は、同意を与えないことが、結果として著しい悪影響につながると示唆することがないように設計される。 ・ 許可が必要な場合（明示的な同意)、当該許可は文書で得

規準		リスクの例示	統制の種類の例示
	から取得されるが、当該同意は、企業のプライバシー・コミットメント及びシステム要求事項に従って、情報が意図され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、保持及び廃棄に関する黙示的な同意が得られていると判断する企業の根拠は文書化される。		るものとする。 ・　黙示的な同意には、データ主体（本人）がオプトアウトする方法について、明確な手段がある。 ・　有効な同意とするためのデータ主体（本人）による行為 ・　同意の要求は、データ主体（本人）の年齢や能力及び特定の状況にふさわしいものとなるように設計される。
		パーソナル・インフォメーションの収集に関し、黙示的又は明示的な同意が適切であるかを判断するためのプロセスが整備されていない。	年次でプライバシー担当者が収集プロセスをレビューし、取得された同意が適切かどうかを判断する（具体的には、黙示的又は明示的な同意が、収集プロセスに応じて適切に収集されているかを判断する。）。
		データ主体（本人）が、パーソナル・インフォメーションの収集、利用や開示に関し可能な選択について通知されていない。	年次で、プライバシー担当者が、通知が内部及び外部の利用者に提供されていること、利用者にとって通知が明確、包括的及び明瞭であること、及び通知は、パーソナル・インフォメーションの詳細な利用、同意、オプトアウトできる権利、認可、共有、開示、アクセス、セキュリティ、保持、及び処分について網羅しており、収集されたパーソナル・インフォメーションの目的及び意図される利用について含んでいることを確認する。
		特定の法令により、いつの時点で同意が求められるかについての理解が不足している。	プライバシー担当者が四半期ごとに、関連するプライバシー法令をレビューし、当該法令により企業は同意を取得しなければならないのか否かを判断し、企業の方針をレビューし、法令の要求事項に適合するように更新する。
		同意の拒否又は撤回が認識されていない、又は管理されていない。	年次で企業は、現在の選択を伝える通知文をデータ主体（本人）に送付し、データ主体（本人）が従前に与えた同意を確認する、又は撤回する、のいずれかを選択できるようにする。同意の拒否又は撤回は、プライバシー担当者がさらなる処理に向けて追跡する。
		明示的な同意又はオプトアウトの同意が求められる場合に、黙示的な同意に依拠してしまう。	プライバシー担当者は、黙示的な同意、又は明示的な同意のいずれが適用されるのかを判断するために要求事項を取得及び評価し、当該要求事項と用いられ

規準		リスクの例示	統制の種類の例示
			た同意とを比較する。
		オプトアウトの同意が、その選択が利用者に及ぼす影響について伝えることなく、利用される。	データ主体（本人）がオプトアウトする選択を与えられる場合、解説情報が提供される。
		機密性の高いパーソナル・インフォメーションが、法的根拠なく、そして明示的な同意も得ることなく収集される。	プライバシー担当者が、受領されるパーソナル・インフォメーションが明示的な同意を要求されるかを判断するため、収集される情報の性質を評価する手続をレビューする。
			プライバシー担当者が四半期ごとに、関連するプライバシー法令をレビューし、当該法令が、企業に同意の取得を要求しているか、又は企業がデータの処理を可能にする他の法的根拠を有しているかを判断する。また、プライバシー・スタッフは、企業の方針をレビューし、要求事項に適合するように更新する。
		いずれのパーソナル・インフォメーションが「機密性が高い」パーソナル・インフォメーションと考えられるかに関し、企業に明確な定義が存在しない。	年次で CPO が、方針をレビューし、「機密性の高い」パーソナル・インフォメーションの定義が適切に表現され、要員に伝えられるようにする。
			企業は、何がパーソナル・インフォメーションを構成し、いずれのパーソナル・インフォメーションが「機密性が高い」と考えられるかを明確にすることを含む、要員に対するアップデート研修や意識向上を行う。
		新たな目的及び利用に関して要求される同意が取得されない。	プライバシー部門が、新しい製品、ソフトウェア、リレーションシップ及び取引に関し、同意を取得し記録する必要性について評価する手続を策定する。
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企業のプライバシー・コミットメント及びシステム要求事項に従って収集される。	パーソナル・インフォメーションが、企業のプライバシー・コミットメント及びシステム要求事項に整合しない方法で収集され、以下のような事態が生じる可能性がある。 ・ 企業が不公正及び虚偽取引行動に関する規制上のクレームの対象になる。 ・ 企業がデータ主体（本人）又は集団の訴訟にさらされる。	プライバシー担当者は、企業が、データ主体（本人）からデータを収集する法的根拠を有しており、かかる法的根拠が収集前に文書化されていることを検証する。さらにプライバシー担当者は、同意が求められる場合、企業がデータ主体（本人）に明示的な同意文書を要求し、それを受領していることを試査によって検証する。

規準		リスクの例示	統制の種類の例示
		・　ネガティブな報道により企業の評判に傷がつく。 ・　競合他社がこうした事態を利用してマーケット・シェアを拡大する。	
			プライバシー関連の苦情は毎月、不公正又は違法行動のインシデントの有無を識別するために調査される。
		企業は、サービスの提供に向けて必要となる情報を収集するための明示的又は黙示的同意を有していない。	プライバシー担当者は、企業が、データ主体（本人）からデータを収集する法的根拠を有しており、かかる法的根拠は収集前に文書化されていることを検証する。さらにプライバシー担当者は、同意が求められる場合、企業がデータ主体（本人）に明示的な同意文書を要求し、それを受領していることを試査によって検証する。
			プライバシー関連の苦情は受けるたびに、不公正又は違法行動のインシデントの有無を識別するために調査される。
		パーソナル・インフォメーションが、プライバシー・コミットメント及びシステム要求事項に従ってサービスを提供するのに必要とされる最低限の情報を超えて収集される。	プライバシー担当者は、パーソナル・インフォメーションがプライバシーに関する通知に特定される目的のためだけに収集されており、事業目的を達成するのに最低限必要とされるパーソナル・インフォメーションのみが収集されているかを判断するために、以下を実施する。 ・　システム変更にパーソナル・インフォメーションの利用又は新たなパーソナル・インフォメーションの収集が含まれる場合、システム変更依頼をレビューし承認する。 ・　契約を締結する前に第三者のプライバシーポリシー及びパーソナル・インフォメーションの収集方法をレビューする。 ・　契約をレビューし、パーソナル・インフォメーションは、強要又は虚偽なしに公正に取得されること、及び全ての関連する法令を適法に遵守することを定める条項が含まれているかどうかを確認する。
			プライバシー関連の苦情は隔週で、不公正又は違法行動のインシデントの有無を識別するために調査される。

規準		リスクの例示	統制の種類の例示
		システム変更により結果として、プライバシー・コミットメント及びシステム要求事項以上の、またそれらに整合しないパーソナル・インフォメーションが収集される。	システム変更がプライバシーに及ぼす影響を評価できるようにPIA（プライバシー影響調査）を実施する。システム変更を行う権限を与えられる要員は、PIAを適切に実施できるように適正な訓練を受ける。法律顧問が、プライバシーに影響を及ぼすシステム変更をレビューする。
		経営者が、企業が第三者からパーソナル・インフォメーションを収集していることを認識しておらず、パーソナル・インフォメーションの種類、パーソナル・インフォメーションが収集された手段や方法を認識していない。	第三者との新規の各契約又は合意書に関し、プライバシー担当者は、パーソナル・インフォメーションがプライバシーに関する通知に特定される目的のためだけに収集されており、事業目的を達成するのに最低限必要とされるパーソナル・インフォメーションのみが収集されるかを判断するために、以下を実施する。 ・　システム変更にパーソナル・インフォメーションの利用又は新たなパーソナル・インフォメーションの収集が含まれる場合、システム変更依頼をレビューし承認する。 ・　契約を締結する前に第三者のプライバシーポリシー及びパーソナル・インフォメーション収集方法をレビューする。 ・　契約をレビューし、パーソナル・インフォメーションは、強要又は虚偽なしに公正に取得され、全ての関連する法令を適法に遵守することを定める条項が含まれるかどうかを確認する。
		企業は、追加のパーソナル・インフォメーションを収集したこと又は収集することをデータ主体（本人）に伝えておらず、したがってデータ主体（本人）は、企業のプライバシーに関する通知に説明される以上に企業がパーソナル・インフォメーションを有していることを認識していない。	企業は、(データ収集時、各収集の形態に関し、及び企業のプライバシー実務が変更になる時点で）企業のプライバシー実務に関する通知をシステムのデータ主体（本人）に提供する。当該通知は、 ・　容易に入手可能とし、パーソナル・インフォメーションがデータ主体（本人）から最初に収集される時点で利用可能となるようにする。 ・　データ主体（本人）がパーソナル・インフォメーションを企業に提出すべきか否かを決定できるように適時に提供される（すなわち、パーソナル・インフォメーションが収集される時点又はそれ以前、

規準		リスクの例示	統制の種類の例示
			あるいはその後できる限り速やかに)。 ・ データ主体（本人）が最後に読んだとき、またパーソナル・インフォメーションを企業に最後に提出したとき以降、通知が変更になっていないかどうかを判断できるように日付が明確に記載される。
P3.2	明示的な同意を求める情報に関し、企業は、そのような同意の必要性のみならずパーソナル・インフォメーションの要求に関し同意しない場合の影響について伝え、企業のプライバシー・コミットメント及びシステム要求事項に従って情報を収集する前に同意を取得する。	企業は、センシティブ・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、明示的な同意をデータ主体（本人）から直接取得していない。	企業の変更管理方針は、求められる場合にはシステム・プロセスにより、明示的な同意を取得すると定めている。CPO の担当者が、実施する前に方針の準拠に向けて全てのシステム変更をレビューし承認する。
		データ主体（本人）のコンピュータその他同様の電子機器への、又はそれらからのオンラインデータ転送に関する同意が取得されない。	企業のアプリケーションに、データ主体（本人）が情報を提出する前にデータ主体（本人）の同意を取り、記録するクリック・ボタンの付いたユーザー・インターフェイス（UI）画面を設ける。
P4.0	**利用、保持及び廃棄に関するプライバシー規準**		
P4.1	企業は、パーソナル・インフォメーションの利用を企業のプライバシー・コミットメント及びシステム要求事項に識別される目的に制限する。	パーソナル・インフォメーションが、プライバシー・コミットメント及びシステム要求事項で識別されていないため同意が取得されていない目的、及び許可されない目的又は適用される法令に準拠していない目的に利用される。	企業は、許容される利用及び開示のシナリオを定義する方針及び手続を維持する。パーソナル・インフォメーションの潜在的な利用及び開示を伴う企業運営を担当する管理者が、それらの方針を受領し理解していることを正式に認める。
			年次ベースで、企業はプライバシー方針及び手続をレビューし、パーソナル・インフォメーションが確実に以下の形で利用されるようにする。 ・ 企業のプライバシーに関する通知で識別される目的に整合する。 ・ データ主体（本人）から受領される同意に整合する。 ・ 適用される法令に準拠する。
P4.2	企業は、パーソナル・インフォメーションを企業のプライバシー・コミットメント及びシステム要求事項に準拠して保持する。	パーソナル・インフォメーションが、明記されている目的に関連する情報以上に、明記される目的を達成するのに必要とされる期間以上に、ま	企業は、維持する情報の種類ごとに保持期間に関する文書による方針を定める。企業は以下を実施する。 ・ 自動化されたシステム・プロセスを整備し、特定の保持

規準		リスクの例示	統制の種類の例示
		た法令に定められる期間以上に保持されており、したがって法令違反の可能性を生み出し、データ流出リスクが高まる。	要件に従って情報を削除する。 ・　規定されたスケジュールに従ってバックアップ情報を削除する。 ・　保持期間を越えて保持される情報に関し CPO による承認を求め、保持するそうした情報に具体的な印を付す。 ・　毎年、保持のため印が付された情報をレビューする。
		パーソナル・インフォメーションの保管場所が識別追跡されておらず、データ流出のリスクが高まる。	組織のデータ・インベントリーのレビューを毎年実施し、文書が最新の状態になっており、データの場所、データの内容及び特定のデータオーナーが記載されていることを検証する。
		パーソナル・インフォメーションが適用される法令に違反する方法で保持されている。	企業は、パーソナル・インフォメーションの保持に関する方針及び手続を文書化しており、当該文書は適用される法令との整合性について（内部又は外部の）法律専門家によって少なくとも年１回レビューされる。パーソナル・インフォメーションの保持に関する法令は、新規又は改正された、適用法令の有無について、プライバシー・スタッフ・メンバー及び（内部又は外部の）法律専門家によって少なくとも年１回レビューされる。企業の保持に関する方針及び手続は、適用される法令との整合性についてレビューされる。現在の適用される法令に整合しないパーソナル・インフォメーションの保持の方針及び手続は、是正（例えば、必要に応じての企業の方針及び手続の更新）に向けて経営者に上申される。
P4.3	企業は、パーソナル・インフォメーションを企業のプライバシー・コミットメント及びシステム要求事項に準拠して安全に廃棄する。	パーソナル・インフォメーションが、企業のプライバシー・コミットメント及びシステム要求事項並びに適用される法令を満たす形で破棄されておらず、したがって、法令違反の可能性及びデータ漏洩リスクが高まる。	週次ベースでセンター要員が、企業が以下を実施していることを示すチェックリストの記入を行う。 ・　（企業が）保管の方法（例えば、電子、光学媒体又は紙ベース）を問わず、保持方針に従って記録を消去又は破棄している。 ・　（企業が）記録の原本、アーカイブ、バックアップ又は一時的なコピー、若しくは個人用コピーを廃棄方針に従って処分している。 ・　（企業が）パーソナル・インフォメーションの処分を文書化している。

規準		リスクの例示	統制の種類の例示
			・　（企業が）技術的限界の範囲内で求められるように、データ主体（本人）についての特定のパーソナル・インフォメーションの場所を特定し、除去又は編集する（例えば、取引完了後のクレジット・カード番号の除去）。 ・　（企業が）プライバシー・コミットメントにおいて特定される、又は法令で求められる目的にとって、もはや必要とされないパーソナル・インフォメーションを破棄、消去又は匿名化する。 データセンター要員が破棄手続に従って上記の項目を完了し、これらの手続の実施状況に関する書類をチェックリストに添付する。CPO の担当者が四半期ごとに、サンプルとして抽出したビジネスユニットの法令遵守状況を評価し、チェックリスト及び関連する文書をレビューすることによりプライバシー及びセキュリティ方針への準拠を検証する。
P5.0	アクセスに関するプライバシー規準		
P5.1	企業は、識別され認可されたデータ主体（本人）に、レビューのために保管されているパーソナル・インフォメーションにアクセスする能力を付与し、要求がある時点で、当該情報の物理的又は電子的コピーを、データ主体（本人）に企業のプライバシー・コミットメント及びシステム要求事項に従って提供する。もし、アクセスが拒否される場合、企業のプライバシー・コミットメント及びシステム要求事項に準拠し、必要なものとして、データ主体（本人）に拒否及びその理由を通知する。	データ主体（本人）が、パーソナル・インフォメーションへのアクセス又はその写しの要求に関するプロセスを認識できず、コンプライアンス違反やデータの完全性に関する問題が生じる可能性がある。	プライバシー担当者は毎年、データ主体（本人）との直接的なコミュニケーション、オンライン通知、プライバシーに関する声明、郵送物、担当者向け研修及び啓蒙プログラムが関係するプロセスをレビューする。当該レビューでは、担当者はそれらが、データ主体（本人）のパーソナル・インフォメーションへのアクセスの提供、及びかかる情報の更新に関するプロセスに対応しているか判断する。CPO が、アクセス方針、手続及び行動に変更が生じた場合にデータ主体（本人）へのコミュニケーションを更新する手続を明文化する。
			データ主体（本人）に対するパーソナル・インフォメーションへのアクセスの提供及び情報の更新について説明する企業のプライバシー通知は、サービス契

規準		リスクの例示	統制の種類の例示
			約が締結される時点でデータ主体（本人）が入手できるとともに、企業のウェブサイトでも確認できるようにする。
			CPO は、企業の要員が、データ主体（本人）によるパーソナル・インフォメーションへのアクセスへの要求にいかにして応じるかを定めるプライバシー方針及び手続を明文化する。
		アクセス権の付与に先行する認証を受けていない未承認の個人にアクセス権が与えられる。	CPO は、データ主体（本人）がパーソナル・インフォメーションへのアクセスを付与される前のデータ主体（本人）の認証状況を追跡しモニターするための手続を明文化する。
		データ主体（本人）に提供される情報が、不完全、不正確である、又は適時に受領されない。	CPO は毎年、パーソナル・インフォメーションを提供する際の対応時間、企業が負担する関連費用、及びデータ主体（本人）への請求費用についてまとめている報告書をレビューする。データ主体（本人）に提供される情報の様式の分りやすさを、プライバシー担当者が毎年評価する。
		データ主体（本人）がアクセスを拒否されたとき、データ主体（本人）に、企業のプライバシー・コミットメント及びシステム要求事項に従って拒否の理由を通知されない。	CPO は毎年、アクセスを拒否されたデータ主体（本人）への対応時間及び拒否の理由、並びに説明の求めに関し行われたコミュニケーション内容についてまとめている報告書をレビューする。
P5.2	企業は、データ主体（本人）が提供する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、企業のプライバシー・コミットッメント及びシステム要求事項に従って、確約されている又は求められるように、そのような情報を第三者に提供する。訂正要求が拒否された場合には、データ主体（本人）に企業のプライバシー・コミットッメント及びシステム要求事項に準拠して拒否及びその理由を通知する。	訂正、修正又は追加に関し受け取られた要求が、企業のプライバシー・コミットッメント及びシステム要求事項に従って正確、適時に、又は、権限を与えられたデータ主体（本人）により処理されない。	CPO は、企業が保有するパーソナル・インフォメーションをどのように更新し、是正するかをデータ主体（本人）に一貫性をもって一律に通知する方針及び手続文書を策定する。
			CPO は、データ更新及び訂正要求を追跡し、かかるデータの正確性及び網羅性を検証する手続

規準		リスクの例示	統制の種類の例示
			文書を策定する。CPO は毎年、更新及び訂正要求並びに記録を更新するまでの対応時間に関する報告書をレビューする。 セルフサービス機能をデータ主体（本人）が利用可能な場合、パーソナル・インフォメーションの更新又は修正の責任を担う許可されたデータ主体（本人）が指定される。
		訂正、修正又は追加されたパーソナル・インフォメーションが、企業のプライバシー・コミットメント及びシステム要求事項に従って当該パーソナル・インフォメーションを従前に受け取っていたベンダーその他第三者に伝えらない。	CPO は、従前にデータ主体（本人）のパーソナル・インフォメーションを受領していたベンダーその他第三者に更新情報が一貫性をもって一律に伝えられる手続文書を策定する。 関連するベンダーその他第三者に情報の更新を提供しないことについて、正当性を示す文書が保管される。
		パーソナル・インフォメーションの訂正、修正又は追加への要求が企業のプライバシー・コミットッメント及びシステム要求事項に従って、拒否されていること又はその理由が、データ主体（本人）に通知されていない。	CPO は、パーソナル・インフォメーションの訂正要求がなぜ拒否されたのか、その理由及びどのようにしたら訂正を要求することができるかを文書にてデータ主体（本人）に通知する際の適切な視点を説明する方針及び手続文書を策定する。
			CPO は毎年、拒否状況をレビューし、パーソナル・インフォメーションの訂正要求の拒否の正当性が適切に文書化され、根拠付けられているかを検証する。
			CPO は毎年、パーソナル・インフォメーションの正確性及び網羅性に関し見解の不一致が見られるケースをレビューし、適切な正当性及び根拠資料が保持されていることを検証する。
P6.0	開示及び通知に関するプライバシー規準		
P6.1	企業は、企業のプライバシー・コミットメント及びシステム要求事項を満たすように、データ主体（本人）の明示的な同意を得て、パーソナル・インフォメーションを第三者に開示する。なお、当該同意は開示の前に取得する。	許可される利用及び開示のシナリオが定義されておらず文書化されていない。	ビジネスユニット・リーダーは、その事業分野に関連して許可されるパーソナル・インフォメーションの利用と開示を識別し文書化する。年次ベースで利用と開示をプライバシー担当者がレビューし承認する。
			新しい種類のパーソナル・インフォメーションの開示及び新たな第三者受領者への開示については PIA（プライバシー影響調

規準		リスクの例示	統制の種類の例示
			査）が記入される。評価の一環としてプライバシー担当者は、開示が、通知、同意及びプライバシー・コミットメント及びシステム要求事項に準拠しているかを判断する。
			変更管理プロセスの一環としてCPO が、第三者への新たな自動開示及び送信、並びに既存の自動開示及び送信の変更をレビューし承認する。
		パーソナル・インフォメーションがデータ主体（本人）の明示的な同意を取得することなしにベンダーその他第三者に開示され、企業のプライバシー・コミットメント及びシステム要求事項が充足されない。	明示的な同意が求められる場合にはビジネスユニットの要員が明示的な同意を取得するプロセスを実施する。同意プロセスの更新は、CPO がレビューし承認する。
			開示要求は、処理する前に、ビジネスユニットの要員により記録され、事前に承認されている種類の開示と比較される。求められる場合にはデータ主体（本人）の同意を処理する前に取得される。
			明示的な同意が求められる場合は、承認を受けたデータ主体(本人）の要求及び一時的な要求であっても、(明示的な）同意が受領されていない場合には拒否される。拒否されたものは、リポジトリに記録される。
P6.2	企業は、企業のプライバシー・コミットメント及びシステム要求事項に準拠して、パーソナル・インフォメーションの承認された開示に関する完全、正確かつ適時の記録を作成、保持する。	未承認の開示がなされることによって、データ流出の可能性が生じる。	パーソナル・インフォメーションの開示が明示的な同意を求める時は、自動化されたプロセスを通じて開示される情報は、開示の前に同意について確認するため、同意の記録と比較される。
		企業は実施された開示の目的を追跡するための記録を維持していない。	自動化された開示は、企業のプライバシー・コミットメント及びシステム要求事項に従って保持される開示データベースに記録される。承認された開示は、企業のプライバシー・コミットメント及びシステム要求事項に従って記録され保持される。
			開示要求は、処理の前にビジネスユニットの要員により記録され、事前に承認されている開示の種類と比較される。事前に承認されている開示の種類に一致しない要求は、プライバシー・

規準		リスクの例示	統制の種類の例示
			オフィサーとの協議によってその適切性について評価される。必要な場合には、処理の前にデータ主体（本人）の明示的な同意が取得される。
		データ主体（本人）によりなされた開示要求が記録されていない。	開示要求は、要求に関する受領日及び具体的な詳細（例えば、要求された情報、要求者の氏名、要求された期限）を含み、ビジネスユニットの要員により記録される。プライバシー担当者が、未処理の要求及び通常でない活動に関し週次ベースで、データ主体（本人）の記録及び一時的な開示の要求をレビューする。未処理の要求については調査が行われ、通常でない要求は、正式な調査及び解決に向けてインシデント管理システムに記録される。
P6.3	企業は、企業のプライバシー・コミットメント及びシステム要求事項に準拠して、パーソナル・インフォメーションの未承認の開示（漏洩を含む。）に関する発見又は報告の完全、正確かつ適時の記録を、作成、保持する。	インシデント管理の一環として識別された、又はデータ主体（本人）その他外部当事者により報告された開示が、プライバシー・インシデントとして識別されていない。	インシデント管理プロセスの一環で発見される未承認の開示及びその可能性のある開示を伝える自動化されたメッセージがプライバシー部門に送られる。プライバシー上問題としてフラグ付けが行われる全てのインシデントの解決は、記録が閉じる前にプライバシー担当者により承認されなければならない。
			インシデント管理手続には、インシデントの疑いのある事象を情報セキュリティ・チームに、そして必要な場合には、プライバシー部門又は法務部門に、エスカレートする方法についての詳細なインストラクションも含まれる。企業は、各インシデントについて記入しなければならない標準的なインシデント・テンプレートを整備する。インシデント管理手続及びテンプレートは、パーソナル・インフォメーションを取り扱う要員に伝えられる。
P6.4	企業は、ベンダーその他第三者（その製品及びサービスがシステムの一部であり、システムにより処理されたパーソナル・インフォメーションへのアクセスを有する）から、受託会社のプライバシー・コミットメント及びシステム要求	契約上の合意が、企業とパーソナル・インフォメーションの処理に関与するベンダーその他第三者との間で整備されていない。	買掛金システムに、ベンダーその他第三者を設定するには、ベンダーその他第三者との契約が求められる。プライバシー担当者は年次ベースで、支払いが行われるベンダーその他第三者の一覧を取得し、パーソナル・インフォメーションを処理するベンダーその他第三者を識別する。プライバシー担当者はまた、企業のプライバシー及びセキュ

規準		リスクの例示	統制の種類の例示
	事項に準拠して、プライバシー・コミットメントを取得している。		リティに関するコミットメントに準拠するプライバシー及びセキュリティに関するコミットメント及びシステム要求事項が契約に含まれているかを判断するために、ベンダーその他第三者との契約をレビューする。
		ベンダーその他第三者が、企業のプライバシー・コミットメント及びシステム要求事項に従った実務を導入していない。	ベンダーその他第三者は、企業が当該当事者と契約を結ぶ前に、企業が実施するプライバシー及びセキュリティに関する評価を受け、そしてその後（毎年又は半年ごとに）管理、技術及び物理的なセーフガードが企業のコミットメント及びシステム要求事項に準拠し整備されていることを確認することを求められる。代わりに、ベンダーその他第三者は、プライバシーに関する SOC2 報告書を提供することができる。SOC2 報告書が提供される場合、プライバシー担当者は報告書をレビューし、適切な規制上の要求事項が含まれ、満たされていることを検証する。プライバシー担当者は、提出された評価結果又は SOC2 報告書をレビューし、改善が必要になるプライバシー又はセキュリティに関するリスクの有無を判断する。プライバシー部門が、必要とされる改善が適時に完了するかどうかをモニターする。
			企業は、企業の改正後のプライバシー、セキュリティポリシー及び手続との継続的な整合性を確認するため、定期的に契約をレビューする。
		企業とベンダーその他第三者との間の契約が、パーソナル・インフォメーションを扱うためのインストラクション、要求事項又はコミットメントを定めていない。	パーソナル・インフォメーションが関連する契約には標準的な契約テンプレートが用いられる。契約には、パーソナル・インフォメーションの承認された取扱いに関するインストラクションが含まれる。標準的テンプレートからの乖離は CPO からの承認を要する。契約テンプレートは、定期的にレビューされ、システム要求事項（たとえば、パーソナル・インフォメーションの取扱いに関する規制上の要求事項又はコミットメント）の変更の結果、テンプレートの変更が必要かどうかを判断する。
P6.5	企業は、ベンダーその他第三者（その製品及びサービスがシステ	ベンダーその他第三者は、契約上のコミットメントに準拠する適切な	パーソナル・インフォメーションが関連する契約には、独立第三者の評価又はベンダーその他

規準		リスクの例示	統制の種類の例示
	ムの一部であり、システムにより処理されたパーソナル・インフォメーションへのアクセスを有する）の受託会社のプライバシー・コミットメント及びシステム要求事項の遵守状況を、定期的かつ必要に応じて評価し、必要がある場合には是正措置を講じている。	プライバシー及びセキュリティ能力を有していない。	の第三者を監査する権利に関する要求事項を定める標準的契約テンプレートが用いられる。標準的テンプレートからの乖離はCPOの承認を必要とする。
			ベンダーその他第三者は、企業が当該当事者と契約を結ぶ前に、プライバシー及びセキュリティに関する評価を受け、そしてその後は毎年、企業の管理、技術及び物理的なセーフガードに準拠する手段が整備されていることを確認することを求められる。代わりに、ベンダーその他第三者は、プライバシーに関する SOC2 報告書を提供することもできる。プライバシー担当者は評価結果又は SOC2 報告書をレビューし、改善が必要になるプライバシー又はセキュリティに関するリスクの有無を判断する。
		ベンダーその他第三者のプライバシーに関する手続又は内部統制の変更が、ベンダーその他第三者によるパーソナル・インフォメーションの処理に有害な影響を及ぼす。	パーソナル・インフォメーションが関連する契約には、ベンダーその他第三者に、パーソナル・インフォメーションの処理に影響を及ぼすベンダーその他第三者のプライバシーに関する手続又は内部統制の変更を企業に伝えることを求める要求事項を定める標準的契約テンプレートが用いられる。標準的テンプレートからの乖離は、CPO の承認を要する。企業は四半期ごとに当該第三者と会議を開き、パーソナル・インフォメーションの処理に影響を及ぼす、ベンダーその他第三者のプライバシー手続及び内部統制の変更について議論する。
		契約終了時点で、パーソナル・インフォメーションの返却又は破棄を確認するための保証がベンダーその他第三者から取得されていない。	パーソナル・インフォメーションが関連する契約には、ベンダーその他第三者に、パーソナル・インフォメーションは契約の要求事項に従って適切に返却された、また破棄されたことを確認する文書を提供することを求める要求事項を定める標準的契約テンプレートが用いられ

規準		リスクの例示	統制の種類の例示
			る。標準テンプレートからの乖離は CPO の承認を必要とする。ベンダーその他第三者とのリレーションシップ・マネージャーはポリシーにより、かかる保証を取得し、プライバシー担当者に裏付け文書を提供することを求められる。契約の終了を決定した場合、企業は、、情報の返却又は破棄に関し実行すべき手続のチェックリスト及び手続の完了を文書で証明するテンプレートをベンダーその他第三者に提供する。
P6.6	企業は、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又は疑われる場合には、企業に通知をするコミットメントを、システムにより処理されるパーソナル・インフォメーションへのアクセスを有しうるベンダーその他第三者から取得する。当該通知は、企業が策定しているインシデント対応手続き、プライバシー・コミットメント及びシステム要求事項を満たすように、適切な要員に報告され、対処される。	ベンダーその他の第三者は、コミットメント又は要求事項により、パーソナル・インフォメーションの流出若しくは未承認の開示について企業に適時に通知する義務を負っていない。	パーソナル・インフォメーションが関連する契約に関しては、パーソナル・インフォメーションの流出若しくは未承認の開示について企業に通知する要求事項を定める標準的契約テンプレートが用いられる。標準的テンプレートからの乖離は、CPO の承認を要する。
		ベンダーその他の第三者にはインシデント対応手続が存在しない。	ベンダーその他の第三者と契約を結ぶ前に、ベンダーその他の第三者はインシデント対応手続の写しを提供することを求められる。ベンダーその他の第三者は、プライバシー又はセキュリティに関するインシデントが発生した場合には、誰に連絡し、そしていつまでに通知すべきかについて具体的なインストラクションを与えられる。
P6.7	企業はプライバシー・コミットメント及びシステム要求事項に準拠して、漏えい及びインシデントについて、影響を受けるデータ主体（本人）、規制当局その他に通知する。	未承認の利用及び開示について、それが流出に該当するかどうか判断するための評価がなされない。	インシデント管理プロセスの間に識別されるプライバシー関連の開示及び潜在的な開示は、プライバシー担当者により事前に策定されている評価ガイドラインを用いて評価される。評価は、インシデント管理システムに記録される。不適切に利用又は開示されるパーソナル・インフォメーションの種類、機微性、価値及び量を基に流出と判断され

規準		リスクの例示	統制の種類の例示
			る、未承認の利用及び開示は、別個のリポジトリに記録される。
		未承認の利用及び開示が流出として適切に識別されない。	未承認の利用及び開示の例、インシデントが流出に該当するかを判断するガイドラインも定めている包括的なインシデント識別及び流出対応手続が文書化されている。当該手続は、パーソナル・インフォメーションを取り扱う要員に伝えられる。
		識別された流出及びインシデントが、企業のプライバシー・コミットメント及びシステム要求事項に従って記録されていない。	不適切に利用又は開示されるパーソナル・インフォメーションの種類、機微性、価値及び量を基に流出と判断される、未承認の利用及び開示は、別個のリポジトリに記録される。流出及びインシデントは CPO によりレビューされる。
		流出及びインシデントの通知が、コミットメント及びシステム要求事項にしたがって完了しない。	流出の通知手続は定期的にレビューされ、手続がコミットメント及びシステム要求事項に整合しているかが判断される。流出の通知活動は、流出の通知手続に照らし合わせてレビューされ、通知は CPO により承認される。
P6.8	企業は、企業のプライバシー・コミットメント及びシステム要求事項に従って、データ主体（本人）の請求により、保有しているパーソナル・インフォメーション及びデータ主体（本人）のパーソナル・インフォメーションの開示の説明をデータ主体（本人）に提供する。	開示の説明請求が処理されない。	開示の説明請求はリポジトリに記録される。請求の処理完了日及び説明書作成担当者がリポジトリに記録される。
		開示の説明が未承認の人に提供される。	請求者識別手続が、処理請求の手続に定義される。実施された識別の種類は、リポジトリに記録される。
		開示の説明が不完全又は不正確である。	開示の各記録に関し、事前に定義されたクエリーが定められている。請求リポジトリには、照会すべき各システムアプリケーションのチェックリストが含まれる。クエリーは、事前に定義された様式でプロセッサーのワークステーションに自動的に返送される。プロセッサーは、各クエリーの結果をリポジトリに保存する。完了した時点でプロセッサーは、リポジトリからの開示報告書の生成を要求する。

規準		リスクの例示	統制の種類の例示
		開示の説明に他のデータ主体（本人）のパーソナル・インフォメーションが含まれる。	全てのクエリーは、特定の請求を行うデータ主体（本人）の固有の識別番号を基に行われる。一つの識別番号ごとに、処理される。
P7.0	品質に関するプライバシー規準		
P7.1	企業は、企業のプライバシー・コミットメント及びシステム要求事項に従って正確、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。	収集されるパーソナル・インフォメーションが不正確又は不完全である。	パーソナル・インフォメーションが収集される時点で自動のエディット・チェック機能により、データ・エントリー・フィールドが適正に入力される（例えば、SSN が入力される場合には 9 桁しか受け付けられない）。
			パーソナル・インフォメーションが収集される時点で、利用者は、情報を企業に提出する前に情報が正確であることを確認するように依頼される。
		収集されたパーソナル・インフォメーションが不正確に変更される。	ＩＴシステム内のパーソナル・インフォメーションが変更される場合、企業内でそれを識別し通知を行う自動制御が存在する。当該変更は、記録が最終確定される前にオペレーション要員によりレビュー及び承認されなければならない。
			ＩＴシステム内のパーソナル・インフォメーションが変更される場合、通知がデータ主体（本人）に送られる。企業は、不正確な箇所については 30 日以内に知らせるようにデータ主体（本人）に要求する。
		意図的か否かに関わらず、パーソナル・インフォメーションが企業内で変更され、それがもはや正確かつ完全でなくなる。	ＩＴシステム内のパーソナル・インフォメーションが変更される場合、企業内でそれを識別し通知を行う自動制御が存在する。当該変更は、記録が最終確定される前にオペレーション要員によりレビュー及び承認されなければならない。
		目的と関連のない情報が収集される。情報がデータ主体（本人）に開示されていない目的ために収集され利用される。	収集されたパーソナル・インフォメーション及び意図された収集の目的が、完全性及び正確性に関してプライバシー通知と比較される。
			企業は、ビジネスユニットが定期的な更新を行うことを求められている最新のデータ・インベントリーを維持する。CPO は定期的にインベントリーをレビューする。
			パーソナル・インフォメーションが収集される方法及び情報が利用される目的の変更は、企業内のガバナンスを担う適切な個

規準		リスクの例示	統制の種類の例示
			人に伝えられる。当該個人は、変更を評価し、その適切性を判断し、必要がある場合にはプライバシー通知を変更する。
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	企業は、データ主体（本人）及びその他から「の問合せ、苦情及び争議を受け付け、対処、解決及びその解決策を伝えるプロセスを適用し、定期的に企業のプライバシー・コミットメント及びシステム要求事項への準拠状況、及び識別された不備に関する訂正その他必要な措置が適時に講じられていることをモニターする。	データ主体（本人）は、問合、苦情及び争議に関する企業への連絡方法を伝えられていない。	企業は、プライバシー統制の状況及び顧客のパーソナル・インフォメーションのプライバシーの保護に関し企業の顧客及びデータ主体（本人）へのコミットメントの遵守をモニターし、問合、苦情及び争議に関し企業への連絡方法についての情報を顧客及びデータ主体（本人）に提供する。
		苦情を提出することができず、データ主体（本人）は、苦情を規制当局に報告する必要が生じる。	企業は、顧客のプライバシーに関する懸念及び問題点を捕捉し追跡するための、自動化され機密性のある顧客プライバシー苦情システムを提供する。
			苦情追跡システムにより捕捉される顧客のプライバシーに関する懸念は、取締役会及び法令により求められる場合には関連する監視機関又は規制当局に報告される。
		流出又は不適切なアクセスにより、正式な報告又は是正措置計画など、アクションが求められるか否かを判断するために、苦情を評価することができない。	企業は、企業のプライバシー方針及び手続の遵守状況のモニターを担当するシニア・サービス・エンティティ・チームリーダーで構成するデータ・プライバシー・タスク・フォースを創設する。データ・プライバシー・タスク・フォースは、顧客のプライバシーに関する懸念及び苦情の評価、改善措置に関する喫緊の報告が求められるか否かの判断、及びかかる懸念及び苦情に対処するために講じられた措置の顧客への直接の対応を行う責任を担う。
		問題の再発を防止する是正措置計画が策定又はモニターされていない。	プライバシー担当者は、プライバシー統制に影響を及ぼし得る識別された又は疑わしいプライバシー・インシデント及び関連するデータ処理上の問題点に対処するために策定される是正措置計画の策定及び執行状況をモニターする。
		方針及び手続が古くなっており、現在の規制、	プライバシー担当者は、プライバシーに関する規制、合意及び

規準		リスクの例示	統制の種類の例示
		合意若しくは契約に対応できない。	契約に関する企業の方針及び手続の継続的な適合性及び適用可能性をモニターする。
		モニタリング又は監査に関する活動の文書の欠如が、プログラムが有効ではないとみなされることがある。	CPO は、企業のプライバシーに関する内部統制及び企業のプライバシー方針及び手続、法令その他の要求事項の遵守状況をモニターする方針及び手続文書を策定する。モニターされる内部統制の選択及びモニターが実施される頻度は、リスク評価に基づき決定される。毎年、遵守状況のモニタリング結果及び改善措置が、プライバシー部門により分析され、経営者に提供される。
		文書化された措置計画の欠如が、プログラムが有効ではないとみなされることがある。	経営者は文書化された措置計画を用いて、企業のプライバシー・プログラムがプライバシーに関連する懸念事項の識別、モニタリング及び対処に有効に運用されるようにする。

付録C　「Trust サービス原則と規準」と「一般に公正妥当と認められたプライバシー原則」の対比表

19.

「Trust サービス原則と規準」と「一般に公正妥当と認められたプライバシー原則」(GAPP)の対比表

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
CC1.1	1	**管理の規準**	**管理の規準：企業は、プライバシーポリシーと手続を定義し、文書化し、伝達し、説明責任を割り当てる。**
CC1.1	1.1.0	プライバシーポリシー	企業は下記の側面について、プライバシーポリシーを定義して、文書化する。
			1. 通知（2.1.0 参照）
			2. 選択と同意（3.1.0 参照）
			3. 収集（4.1.0 参照）
			4. 利用、保持及び廃棄（5.1.0 参照）
			5. アクセス（6.1.0 参照）
			6. 第三者への開示（7.1.0 参照）
			7. プライバシーのためのセキュリティ（8.1.0 参照）
			8. 品質（9.1.0 参照）
			9. モニタリングと是正措置（10.1.0 参照）

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
CC2.2, CC1.4, CC2.6	1.1.1	社内要員への伝達	プライバシーポリシーとコンプライアンス違反の顛末は、企業のパーソナル・インフォメーションを収集、利用、保持、開示することに実行責任がある社内要員に少なくとも毎年伝達される。プライバシーポリシーの変更は、変更が承認された後、速やかにこれらの社内要員に伝達される。
CC1.1, CC1.2, CC3.2, CC4.1	1.1.2	ポリシーに関する実行責任と説明責任	企業のプライバシーポリシーを文書化し、導入し、是正措置し、モニタリングし、更新することに対して、個人又はグループに実行責任と説明責任が割り当てられる。このような個人又はグループの名前と彼らの実行責任は社内要員に伝達される。
CC1.2	1.2.1	レビューと承認	プライバシーポリシーと手続、それらに対する変更が経営者によってレビューされ、承認される。
CC1.1, CC1.2	1.2.2	プライバシーポリシーと手続の法令との整合性	ポリシーと手続が少なくとも毎年そして関連法令が改正される都度レビューされ、適用される法令の要件と比較される。 プライバシーポリシーと手続は、適用される法令の要件を充足するように修正される。
CC3.1	1.2.3	パーソナル・インフォメーションの識別と分類	パーソナル・インフォメーションと機密情報の種類、それらの情報の取扱いに係る関連するプロセス、システム、第三者が特定されている。それらの情報は、企業のプライバシーポリシー、関連するセキュリティポリシー及び手続の対象となっている。
CC3.1	1.2.4	リスク評価	リスク評価プロセスは、リスクベースラインを確立し、少なくとも年に１回、新しい又は変化したパーソナル・インフォメーションのリスクを識別し、当該リスクへの 対応を策定し、更新するのに使用される。
CC1.1, CC1.2, CC3.1	1.2.5	プライバシーポリシーと手続のコミットメントへの整合性	社内要員又は企業のアドバイザーが、プライバシーポリシー及び手続と契約書の整合性をレビューし、何らかの不整合に対応する。
CC7.1, CC7.4, C1.1	1.2.6	インフラストラクチャーとシステム管理	新しい個人情報取扱プロセスが導入される場合及び当該プロセス（第三者又は委託先に外部委託された活動を含む。）に変更がなされる場合に、潜在的なプライバシーに対する影響が評価され、プライバシーポリシーに準拠して、パーソナル・インフォメーションの保護が継続される。この目的のために、個人情報取扱プロセスは、下記に関する設計、取得、導入、設定、管理、変更を含む。

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
			・ インフラストラクチャー
			・ システム
			・ アプリケーション
			・ ウェブサイト
			・ 手続
			・ 製品とサービス
			・ データベース及び情報リポジトリ
			・ モバイルコンピューティング又はその他の類似した電子機器
CC2.5, CC6.2, P6.6	1.2.7	プライバシー・インシデントと違反の管理	文書化されたプライバシー・インシデントや違反の管理プログラムは下記を含むが、それに制限されない。
			・ プライバシー・インシデントや違反の識別、管理、解決のための手続
			・ 定義された責任
			・ インシデントの深刻度を識別するプロセス及び必要な行動を決定するプロセス及び上申手続
			・ 必要により、利害関係者への違反通知を含む、違反した法令に従うプロセス
			・ インシデントや違反に実行責任がある従業員や第三者の復旧・処罰・懲戒などの説明責任のプロセス
			・ 下記に基づく必要なプログラム変更を識別するための実際のインシデントの定期的レビュー（少なくとも年一度）プロセス
			—インシデントのパターン,根本原因
			—内部統制環境又は外部の要件（法令）における変化
			・ 定期的なテスト又はウォークスルー（少なくとも年一度）プロセスと関連する必要な復旧プログラム
CC1.3	1.2.8	支援のための資源	プライバシーポリシーを導入し、支援するための資源が企業によって提供される。
CC1.3, CC1.4	1.2.9	要員の資格	企業は、パーソナル・インフォメーションのプライバシーと、セキュリティを保護することに実行責任がある要員の資格を確立して、このような実行責任をこれらの資格を満たしており、必要とされる訓練を受けた要員にだけ割り当てる。
CC2.3	1.2.10	プライバシーの意識向上と訓練	役割と実行責任に応じて選抜された要員に対して、企業のプライバシーポリシー及び関連事項に関するプライバシー意識向上プログラムが提供される。
CC1.1, CC1.2, CC3.1	1.2.11	規制及びビジネス要件の変化	企業が業務を行う法管轄区域において、下記の要因の変化のプライバシーに対する影響が識別され、対処される。
			—法令
			—SLA を含む契約
			—業界の要件
			—ビジネス運用とプロセス
			—人員、役割と責任
			—技術

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
			プライバシーポリシーと手続がこのような変化のために更新される。
	2	**通知の規準**	**通知の規準：企業は、プライバシーポリシーと手続について通知を提供し、パーソナル・インフォメーションが、収集、利用、保持、開示される目的を識別する。**
CC1.1, CC1.2, P1.2	2.1.0	プライバシーポリシー	企業のプライバシーポリシーは、個人に対する通知の提供を扱う。
P1.1, P1.2	2.1.1	個人への伝達	下記のプライバシーポリシーに関して企業から個人に通知を提供する。
			a. パーソナル・インフォメーションを収集する目的
			b. 選択と同意（3.1.1 参照）
			c. 収集（4.1.1 参照）
			d. 利用、保持及び廃棄（廃棄）（5.1.1 参照）
			e. アクセス（6.1.1 参照）
			f. 第三者への開示（7.1.1 参照）
			g. プライバシーのためのセキュリティ（8.1.1 参照）
			h. 品質（9.1.1 参照）
			i. モニタリングと是正措置（10.1.1 参照）
			当該個人以外の情報源から情報が収集される場合は、当該情報源は通知で記述される。
P1.1	2.2.1	通知の提供	企業のプライバシーポリシーと手続について個人に提供される通知は、(a)パーソナル・インフォメーションが収集されるとき若しくはその前、又は実務的範囲でなるべく早く、(b)企業のプライバシーポリシー及び手続が変更されるきに若しくはその前、又は実務的範囲でなるべく早く、(c)パーソナル・インフォメーションが従前予定されていなかった新しい目的のために利用される前に実施される。
P1.1, P1.2	2.2.2	対象とされる企業の活動	プライバシーポリシーと手続によって、対象とされた企業の活動の客観的な記述が、企業のプライバシー通知に含められる。
P1.1, P1.2, P2.2	2.2.3	明瞭性と公知性	明瞭、かつ公知された用語が企業のプライバシー通知で利用される。
P2.1	3	**選択と同意の規準**	**選択と同意の規準：企業は個人にとって可能な選択を記述して、パーソナル・インフォメーションの収集、利用、開示に関して黙示又は明示の同意を得る。**
CC1.1, CC1.2, P1.1, P1.2	3.1.0	プライバシーポリシー	企業のプライバシーポリシーは、個人にとって可能な選択と得られるべき同意を扱う。
P1.1	3.1.1	個人への伝達	(a)パーソナル・インフォメーションの収集、利用、開示につき当該個人にとって可能な選択、(b)法令に別段の定めがない限り、パーソナル・インフォメーションの収集、利用、開示に黙示又は明示の同意が要求されることについて企業から個人に通知する。

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
P2.1	3.1.2	同意の拒否又は撤回の結果	パーソナル・インフォメーションが収集されるとき、当該情報の提供を拒否した場合の結果又は当該情報を通知によって識別された目的のために利用することを拒否又は撤回した場合の結果について、企業から個人に通知する。
P2.1	3.2.1	黙示又は明示の同意	黙示又は明示の同意が、パーソナル・インフォメーションが収集されるとき若しくはその前、又は実務的になるべく早く個人から得られる。個人の同意で表現された要望は確認されて、実行される。
P2.1	3.2.2	新しい目的と利用のための同意	既に収集された情報が従前にプライバシー通知で識別された以外の目的のために利用される場合は、新しい目的は文書化され、個人は通知される。 さらに、当該個人から黙示又は明示の同意がこのような新しい利用又は目的の前に得られる。
P2.1	3.2.3	機微な情報のための明示の同意	法令に別段の定めがない限り、機微なパーソナル・インフォメーションを収集、利用、開示する場合には、個人から直接、明示の同意を得る。
P2.1	3.2.4	個人のコンピュータ又は他の類似の電子機器経由のオンラインデータ転送への同意	個人のコンピュータその他類似の機器経由でパーソナル・インフォメーションが転送される前に、当該個人の同意を得る。
	4	**収集原則と規準**	**収集原則：企業は、通知で識別された目的だけのためにパーソナル・インフォメーションを収集する。**
CC1.1, CC1.2, P1.2	4.1.0	プライバシーポリシー	企業のプライバシーポリシーはパーソナル・インフォメーションの収集を扱う。
P1.1, P2.1	4.1.1	個人への伝達	通知で識別された目的だけのために、パーソナル・インフォメーションが収集されるということを、企業から個人に通知する。
P1.1, P1.2, P2.1	4.1.2	収集したパーソナル・インフォメーションの種類と収集の方法	収集したパーソナル・インフォメーションの種類、収集の方法は、クッキー又は他の追跡技術の利用を含めて文書化され、プライバシー通知で記述される。

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
P3.1	4.2.1	識別された目的に限定された収集	パーソナル・インフォメーションの収集は、通知で識別された目的に必要な範囲で限定されている。
CC3.1, CC3.2, CC4.1, P8.1, P3.1	4.2.2	公正かつ合法的な手段による収集	パーソナル・インフォメーションが得られることを確認する前に、パーソナル・インフォメーションの収集方法が、(a)公正であること、脅迫又は騙しがないこと、(b)合法的であること、パーソナル・インフォメーションの収集に関連する全ての関連する法令又は慣習法を遵守していることについて、経営者によってレビューされる。
CC1.0, P1.1, P3.1	4.2.3	第三者からの収集	経営者は、パーソナル・インフォメーションを収集する第三者（すなわち、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。
P1.1, P2.1	4.2.4	個人について作成される情報	個人は、企業がその利用のために個人に関する追加の情報を作成又は取得する場合に通知される。
	5	**利用、保持及び廃棄原則と規準**	**利用、保持及び廃棄原則：企業は、パーソナル・インフォメーションの利用を通知で識別された目的、及び個人が黙示又は明示の同意をした目的のみに制限する。企業は、述べられた目的を満たすため、又は法令によって必要である限りにおいて、パーソナル・インフォメーションを保持し、その後、適切に廃棄する。**
CC1.1, CC1.2, CC2.1, CC2.2, CC2.4, P1.2	5.1.0	プライバシーポリシー	企業のプライバシーポリシーはパーソナル・インフォメーションの利用、保持及び廃棄を扱う。
P1.1	5.1.1	個人への伝達	パーソナル・インフォメーションが、(a)法令に別段の定めがない限り、黙示又は明示の同意があった場合、及び通知において識別された目的のためのみに利用され、(b)述べられた目的を満たすために必要な期間のみ保持されるか、又は法令によって特に必要とされた期間にわたって保持され、(c)滅失、盗難、誤用、未承認のアクセスを防止しつつ廃棄される、ということを企業から個人に通知する。
P4.1	5.2.1	パーソナル・インフォメーションの利用	法令に別段の定めがない限り、パーソナル・インフォメーションは、個人が黙示又は明示の同意を提供した場合、又は通知で識別された目的のためにのみ利用される。
P4.2	5.2.2	パーソナル・インフォメーションの保持	法令に別段の定めがない限り、パーソナル・インフォメーションが、述べられた目的を満たすために必要な期間のみ保持される。

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
P4.2, P4.3	5.2.3	パーソナル・インフォメーションの廃棄、破壊、編集	保有する必要のなくなったパーソナル・インフォメーションは、滅失、盗難、誤用、未承認のアクセスを防ぐ方法で匿名化されるか、廃棄される又は無効にされる。
	6	**アクセス原則と規準**	**アクセス原則：企業は、レビューと更新のためにパーソナル・インフォメーションへのアクセスを個人に提供する。**
	6.1.0	プライバシーポリシー	企業のプライバシーポリシーは、パーソナル・インフォメーションへのアクセスを個人に提供することを扱う。
CC1.1, CC1.2, P1.2, P5.1	6.1.1	個人への伝達	個人が、どのようにその情報をレビューし、更新し、修正するために自身のパーソナル・インフォメーションにアクセスを得ることができるかについて企業から当該個人に情報提供する。
P2.1, P5.1	6.2.1	パーソナル・インフォメーションへの当該個人によるアクセス	個人は、企業が自身のパーソナル・インフォメーションを保持しているかどうかを確認することができ、依頼によって自身のパーソナル・インフォメーションにアクセスを得ることができる。
P5.1, P6.2	6.2.2	個人の身元の確認	パーソナル・インフォメーションにアクセスを求める個人の身元は、彼らがその情報にアクセスを与えられる前に認証される。
P5.1	6.2.3	分かりやすいパーソナル・インフォメーション、時間枠、コスト	パーソナル・インフォメーションが、分かりやすい形式、合理的な時間、合理的なコストで個人に提供される。
P5.1, P5.2	6.2.4	アクセスの拒否	パーソナル・インフォメーションへのアクセス要求を拒否する理由、該当する場合には、そのアクセスを拒否する企業の法的根拠について、もしあれば、当該拒否に抗弁できる法令による具体的な許可や要求に関する個人の権利について、当該個人に書面で通知され。
P5.2	6.2.5	パーソナル・インフォメーションの更新又は訂正	個人は、企業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。実務的、経済的に可能である場合は、企業は、当該パーソナル・インフォメーションがかつて提供された第三者に対して、情報の更新又は訂正を行う。
P5.2	6.2.6	合意未達の文書	個人がパーソナル・インフォメーションの訂正の要求が拒否された理由と、彼らが抗弁できる方法について、書面で、企業から個人に通知する。

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
	7	**第三者への開示原則と規準**	**第三者への開示原則：企業は、通知で識別された目的及び、個人が黙示又は明示の同意をした目的のためだけに第三者にパーソナル・インフォメーションを開示する。**
CC1.1, CC1.2, P1.2	7.1.0	プライバシーポリシー	法令に別段の定めがない限り、通知で識別された目的及び、黙示又は明示の同意をした目的のためだけに、第三者にパーソナル・インフォメーションが開示されることを、企業から個人に通知する。
P1.1, P6.1, P6.2	7.1.1	個人への伝達	企業のプライバシーポリシーはパーソナル・インフォメーションの第三者への開示を扱う。
P1.2	7.1.2	第三者への伝達	パーソナル・インフォメーションの取扱いに要求されるプライバシーポリシーその他の特定の指示、要求事項は、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。
P1.1, P6.1	7.2.1	パーソナル・インフォメーションの開示	法令に別段の定めがない限り、通知で識別された目的及び黙示又は明示の同意をした目的のためだけに第三者に、パーソナル・インフォメーションが開示される。
P6.4, P6.5	7.2.2	パーソナル・インフォメーションの保護	企業が、企業のプライバシーポリシーの関連箇所、その他の特定の指示又は要求事項に整合して、パーソナル・インフォメーションを保護するよう合意した第三者のみに対して、パーソナル・インフォメーションが開示される。企業は、第三者がその合意、指示、要求事項に沿って有効な内部統制を有していることについて評価する手続を有している。
P3.1, P6.1, P6.4	7.2.3	新しい目的と利用	個人の事前の黙示又は明示の同意によってのみ、新しい目的のために、第三者へのパーソナル・インフォメーションの開示がなされる。
P6.7, P6.8	7.2.4	第三者によるパーソナル・インフォメーションの誤用	企業は、パーソナル・インフォメーションを転送した第三者による当該情報の誤用に対する修正行動をとる。
	8	**プライバシーのためのセキュリティ原則と規準**	**プライバシーのためのセキュリティ原則:企業は、(物理的、論理的双方の) 未承認のアクセスからパーソナル・インフォメーションを保護する。**
CC1.1, CC1.2, P1.2, CC5.1-CC5.8	8.1.0	プライバシーポリシー	企業のプライバシーポリシー（関連するセキュリティポリシーを含む。）は、パーソナル・インフォメーションのセキュリティを扱う。

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
P1.1	8.1.1	個人への伝達	パーソナル・インフォメーションを守るために予防策が実施されることを、企業から個人に通知する。
CC3.1, CC3.2, CC5.1- CC5.8, P6.5, P8.1	8.2.1	情報セキュリティプログラム	セキュリティプログラムは、滅失、誤用、未承認のアクセス、漏洩、改竄、破損からパーソナル・インフォメーションを保護するための、管理的、技術的、物理的措置を開発、文書化、承認、導入をしている。セキュリティプログラムは、少なくともパーソナル・インフォメーションのセキュリティに関する下記の領域 6 に対処すべきであるが、それに制限されない。
			a. リスクの評価と対応(1.2.4)
			b. セキュリティポリシー(8.1.0)
			c. 情報セキュリティ管理体制(セクション１、７、10)
			d. 資産管理（セクション１）
			e. 人的セキュリティ（セクション１）
			f. 物理的、環境的セキュリティ（8.2.3 と 8.2.4)
			g. 伝達と運用の管理(セクション１、７、10)
			h. アクセスコントロール(セクション１、8.2、10)
			i. 情報システムの取得、開発、保守(1.2.6)
			j. 情報セキュリティインシデント管理(1.2.7)
			k. 事業継続管理(セクション 8.2)
			l. コンプライアンス(セクション１、10)
CC5.0, CC5.2- CC5.4, CC5.6- CC5.8	8.2.2	論理的アクセスコントロール	パーソナル・インフォ メーションへの論理的 アクセスが、下記の事項を扱う手続によって制限される。
			a. 社内要員と個人の権限付与及び登録
			b. 社内要員と個人の識別及び認証
			c. アクセスプロファイルの変更と更新
			d. ＩＴインフラ構成要素とパーソナル・インフォメーションへのアクセス権限と許諾の付与
			e. 自身のパーソナル・インフォメーション又は機微な情報以外に個人がアクセスすることの防止
			f. 割り当てられた役割と実行責任に基づいて承認された社内要員のみへのパーソナル・インフォメーションへのアクセス制限
			g. 承認された社内要員のみへの出力帳票配布
			h. オフラインストレージ、バックアップデータ、システムと媒体への論理的アクセス制限
			i. システム設定、スーパーユーザー機能、マスターパスワード、強力なユーティリティー、セキュリティデバイス（例えば、ファイアウォール）へのアクセス制限
			j. ウイルス、悪意のあるコード、未承認のソフトウェアの導入禁止

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
CC5.5	8.2.3	物理的アクセスコントロール	パーソナル・インフォメーションへの物理的アクセスが（パーソナル・インフォメーションを含んでいるか、又は保護する企業のシステム構成要素を含めて）どんな形式についても制限される。
CC6.1	8.2.4	環境的保護措置	全ての形態でのパーソナル・インフォメーションが、自然災害、環境上のリスク要因による不測の開示から保護される。
CC5.7	8.2.5	伝送されたパーソナル・インフォメーション	パーソナル・インフォメーションがメールその他の物理的手段による伝送時に保護される。 パーソナル・インフォメーションが、インターネット、公衆回線、その他のセキュアでないネットワーク、無線ネットワークによって収集、伝送される場合、パーソナル・インフォメーションの転送、受信のための業界標準の暗号化技術を利用して、保護される。
CC5.1, CC5.4	8.2.6	ポータブルメディア上のパーソナル・インフォメーション	ポータブルメディアに保存されたパーソナル・インフォメーションが、未承認のアクセスから保護される。
CC4.1, P8.1	8.2.7	セキュリティ保護措置のテスト	パーソナル・インフォメーションを保護している重要な管理的、技術的、物理的保護措置の有効性のテストが、少なくとも毎年行われる。
	9	**品質原則と規準**	**品質原則：企業は、通知で識別された目的のために正確かつ、完全かつ、適切にパーソナル・インフォメーションを保持する。**
CC1.1, CC1.2, P1.2	9.1.0	プライバシーポリシー	企業のプライバシーポリシーはパーソナル・インフォメーションの品質を扱う
P1.1	9.1.1	個人への伝達	企業は、個人が正確かつ、完全なパーソナル・インフォメーションを企業に提供すること、及びこのような情報の訂正が必要とされる場合は、連絡を取ることに責任があるということを、当該個人に通知する。
P5.2, P7.1, P8.1	9.2.1	パーソナル・インフォメーションの正確性と完全性	パーソナル・インフォメーションは、利用される目的に応じて正確かつ、完全である。
P4.1	9.2.2	パーソナル・インフォメーションの適切性	パーソナル・インフォメーションは、それが利用される目的にとって適切である。
	10	**モニタリングと是正措置原則と規準**	**モニタリングと是正措置原則：企業は、プライバシーポリシーと手続への準拠性をモニタリングし、プライバシーに関連する問合せ、苦情及び紛争を扱う手続を持っている。**
CC1.1, CC1.2, P1.2	10.1.0	プライバシーポリシー	企業のプライバシーポリシーは、プライバシーポリシーと手続のモニタリングと是正措置を扱う。

TSPC	*Ref*	*Title*	*Extant GAPP Criterion*
P1.1, P5.1, P5.2	10.1.1	個人への伝達	企業は、個人が問合せ、苦情及び紛争について、どのように企業と連絡を取るべきかについて、当該個人に通知する。
CC6.1, CC6.2, CC5.1, CC5.2, P8.1	10.2.1	問合せ、苦情及び紛争処理	問合せ、苦情及び紛争に対処するプロセスが採用されている。
CC6.1, CC6.2, CC5.1, CC5.2, P8.1	10.2.2	紛争解決と調停	全ての苦情に対処し、解決が文書化され、企業から個人に伝達される。
C3.2, CC4.1, P8.1	10.2.3	コンプライアンスレビュー	プライバシーポリシーと手続、コミットメントと適用される法律、規則、SLA とその他の契約へのコンプライアンスがレビューされ、文書化され、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は、企業の是正計画が策定、導入される。
CC6.2, P8.1	10.2.4	コンプライアンス違反への対応	プライバシーポリシーと手続へのコンプライアンス違反の例が文書化されて、報告され、必要な場合は、是正及び懲戒処分の対策が適時にとられる。
CC4.1, P8.1	10.2.5	継続的モニタリング	リスク評価(1.2.4)に基づくパーソナル・インフォメーションの内部統制の有効性をモニタリングして、必要に応じて適時な是正行動をとるために継続的モニタリングが実施される。

以　上