ＩＴ委員会研究資料第６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 2006 年版の更新）

平成25年12月20日
日本公認会計士協会

American Institute of Certified Public Accountants（AICPA）
Technical Practice Aids, TSP section 100
“Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy”, 2009

（訳者注：「原則と規準及び内部統制の例」において、“management”は「経営者」と翻訳しています。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します。）

－目　　次－

はじめに 1

Trust サービス 1

原則、規準及び内部統制の例 2

適用される法令、定義されたコミットメント、サービスレベルアグリーメント及びその他の契約との整合性 3

Trust サービスの構成－Trust サービスの原則と規準 3

発効日 5

原則と規準 5

セキュリティ原則と規準 5

可用性原則と規準 17

処理のインテグリティ原則と規準 34

機密保持原則と規準 56

プライバシー原則と規準 73

付録Ａ　電子商取引システムのための開示例 76

付録Ｂ　システム記述例（電子商取引でないシステム） 84

付録Ｃ　範囲決定及び結論の報告の問題に関する業務責任者への指針 87

付録Ｄ　一般に公正妥当と認められたプライバシー原則 99

TSPセクション100
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、規準及びその例示

はじめに

１．このセクションでは、ＩＴ利用システム[1]（電子商取引システムを含む。）及びプライバシープログラムに関して、保証若しくは助言サービス又は両者を提供する場合の指針を提供している。この指針は、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してサービスを提供する場合に適したものである。

２．この指針は下記のセクションを含んで提供されている。
- Trustサービスの原則と規準
- 当該業務に必要とされるシステム記述の例
- Trustサービス業務のための保証報告書文例

Trust サービス

３．Trustサービスとは、ＩＴ利用システム及びプライバシープログラムのリスクと機会に対処するための中核的な一連の原則と規準に基づく一連の職業的な保証及び助言業務として定義される。Trustサービスの原則と規準は、AICPAの保証業務執行委員会（以下「委員会」という。）によって発行された。

保証業務

４．保証業務には、検証、レビュー[2]及び合意された手続業務が含まれる。検証・レビュー業務では、報告責任者は意見を表明する。例えば、検証業務では、定義されたシステムの内部統制がシステムの信頼性の規準を満たすために有効に運用されたかどうかに関する意見が表明される。合意された手続業務では、業務責任者は意見を表明せず、指定された当事者によって合意された手続を実施して、発見事項を報告する。保証業務はAICPA職業的基準第１巻ＡＴセクション101「証明業務」に準拠して開発された。

---

1 「システム」は、特定の目的を達成するために、組織化された五つの重要な構成要素から成り立つ。五つの構成要素は下記のように分類される。
- システム基盤：システムの物理面又はハードウェアの構成要素（施設、装置とネットワーク）
- ソフトウェア：システムのプログラムと運用ソフトウェア（システム、アプリケーションとユーティリティ）
- 要員：システムの運用及び利用に関与する要員（開発者、運用担当者、ユーザー、管理者）
- 手続：システムの運用に関与するプログラム化された又は手動の手続（自動化された、又は手動の）
- データ：システムにより利用され又はサポートされる情報（取引の流れ、ファイル、データベース、テーブル）

2 業務責任者は、Trust サービスの原則と規準に関連してシステムの内部統制のレビュー業務を受嘱してはならない。

助言業務

５．Trustサービスの内容において、助言業務にはTrustサービス原則及び規準を用いた戦略、診断、導入、維持及び管理などのサービスが含まれている。このようなサービスを提供する業務責任者はコンサルティングサービスのための基準書（AICPA職業的基準第２巻のCSセクション100）を遵守する。こうした業務では、業務責任者による意見の表明はなされない。

原則、規準及び内部統制の例

６．下記の指針では、(1)原則（目的に関する広範囲な文書）及び(2)各原則に合致するために達成されるべき特定の規準、から構成されている。規準は、主題を測定・表示するために利用されるベンチマークであり、業務責任者が主題をそれに照らして評価するものである。適合する規準の属性には、客観性、測定可能性、完全性、関連性がなければならない。委員会は、Trustサービスの規準は適合する規準の全ての属性を持つと結論付けている。さらに、この指針の公表はその規準を利用者に利用可能にしている。Trustサービスの原則は全体的な目標を記述しているが、業務責任者の意見は規準のみに言及するものである。

７．Trustサービスの原則と規準においては、規準は、もし有効に運用されているならばシステムが規準を満たすような内部統制の例示一覧により裏付けられている。これらの例示は、包括的であることを意図しておらず、単なる事例を提供するに過ぎない。企業において実際に適用されている内部統制は、その一覧には含まれていないかもしれないし、また、幾つかの列挙された内部統制は、全てのシステムや状況に適合してはいないかもしれない。業務責任者は、規準を満たすために、企業が採用している関連する内部統制を識別、評価すべきである。これらの内部統制の選択及び数は、企業の経営形態、哲学、規模、業界にも依拠するだろう。

８．Trustサービスの原則と規準を使用して、業務責任者が実施する業務の種類には、以下のようなものがある。

- 企業の対象システムに関する内部統制の有効性に関して報告する。
- 企業の内部統制の有効性及びTrustサービスの原則と規準に関するコミットメントへの当該企業の遵守性に関して報告する。
- Trustサービスの原則と規準を達成するために、企業の対象システムに関する内部統制が有効に運用されるように設計された内部統制のデザインの適合性に関して報告する（この業務は典型的にはシステムの導入前に実施される。）。

業務の主題が、企業のプライバシープログラムである場合、報告書は、コミットメントへの企業の遵守性を対象としなければならない。簡略化のために、このドキュメントは主として、業務責任者がシステムの内部統制の運用の有効性に関してTrustサービス原則と規準を満たしていると報告する業務を記述する。しかしながら、特に断らない限り、本指針は等しくこのパラグラフで記載されたどの主題に関して報告する業務であっても適用可能である。さらに、ＡＴセクション101によれば、業務責任者が主題について又は主題に関する記述書についてのどちらかの報告をすることが認められる（付録Ｃ「経営者の記述書」を参照）。

適用される法令、定義されたコミットメント、サービスレベルアグリーメント及びその他の契約との整合性

９．「適用される法令、定義されたコミットメント、サービスレベルアグリーメント（以下「SLA」という。）及びその他の契約への整合性」については、原則と規準の幾つかの中で参照されている。経営者には、法令を識別し、遵守する責任がある。「適用される法令、定義されたコミットメント、SLA及びその他の契約」について関連する全てのものを識別することは、業務を実施する業務責任者の業務の範囲には含まれない。更に言えば、Trustサービス業務は、企業に、適用される法令、定義されたコミットメント、SLA及びその他の契約への遵守性に関してテスト又は報告することを業務責任者に要求するものではなく、むしろそれらの遵守性に関する企業のモニタリングの有効性について、報告するものである。コミットメントへの遵守性について報告する場合、企業の法令やアグリーメント[3]への遵守性に対して報告することに関する他の職業的基準を参照することが望ましい。

Trust サービスの構成－Trust サービスの原則と規準

10. 下記の原則と関連する規準は、Trustサービス業務[4]の実施において業務責任者が利用するために、AICPA/CICAによって作成された。

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

b. 可用性：　システムは、コミット又は合意したとおりに、操作でき、かつ、利用できる。

c. 処理のインテグリティ：　システム処理は完全、正確、タイムリーかつ承認されている。

d. 機密保持：　機密とされた情報が、コミット又は合意したとおりに、システムにより保護されている。

e. プライバシー：　個人情報[5]は、（付録Ｄ（パラグラフ48）に記載している）企業のプライバシー通知におけるコミットメント及びAICPA/CICAによって発行された一般に公正妥当と認められるプライバシー原則を充足して、収集、利用、保持、開示及び廃棄されている。

11. Trustサービスのセキュリティ、可用性、処理のインテグリティ、機密保持の各原則及び規準は、下記の四つの大分類により構成されている。

a. ポリシー：　企業は、特定の原則に関連するポリシーを定義し、文書化している（ここでは、「ポリシー」という用語は、経営者の意図や、目的、要件、責任と特定の事項に関する基準を伝達する書面に記載されたものをいう。）。

3　AICPA 職業的基準第１巻ＡＴセクション 601「遵守性の証明」を参照

4　WebTrust と SysTrust は、Trust サービスの原則と規準を基礎とした AICPA と CICA によって開発提供された二つの特別な保証業務である。登録されたマークを利用するためには CICA によって認可されたライセンスが必要である。ライセンスに関する追加の情報は www.webtrust.org.に掲載されている。

5　個人情報は個人又は個人に関係付けることができる情報

b. コミュニケーション[6]：　企業は、責任がある当事者や承認されたシステムのユーザーに定義されたポリシーを伝達している。

c. 手続：　企業は、定義されたポリシーに準拠して、その目的を達成するために運用手続を整備している。

d. モニタリング：　企業は、システムをモニターし、定義されたポリシーへの遵守性を維持するために対策を実施している。

12. セキュリティ、可用性、処理のインテグリティ及び機密保持のTrustサービスの原則と規準において、規準の説明のため２列（欄）の様式を使用して記載されている。最初の列はそれぞれの原則の規準を説明し、２番目の列は内部統制の例示を記述している。

13. システム記述は、セキュリティ、可用性、処理のインテグリティ、及び機密保持のTrustサービスの原則と規準で検証の対象となっているシステムの範囲を明確にするために使用される。コミットメントへの企業の遵守性を対象とする業務のために、それらのコミットメントは、システム記述に含まれるか、又はそうでなければ、報告書に添付されることが望ましい。電子商取引及び非電子商取引の両方のシステム記述の例は付録Ａ(45)と付録Ｂ(46)にそれぞれ含まれている。また、付録Ａ(45)は電子商取引システムの特定の原則と規準に関連する開示のサンプルを含んでいる。

14. 信頼できるシステムとは、特定された環境においてある一定期間にわたり、重要なエラー、停止、障害を起こすことなく運用できるシステムである。業務責任者はセキュリティ、可用性、処理のインテグリティに係るTrustサービスの原則と規準が取り扱うシステムの信頼性に関する報告書を提供する。それらの規準は、システムが信頼できるかどうかの評価に利用される。

15. プライバシーのTrustサービスの原則と規準は二つの分野で構成される。

a. ポリシーとコミュニケーション。プライバシーポリシーは、プライバシーに関する経営者の意図、目的、要件、責任及び基準を伝える文書である。コミュニケーションは、プライバシー通知とコミットメント及びその他の関連情報についての個人、職員及び第三者との組織上のコミュニケーションをいう。

b. 手続と内部統制。組織が規準を充足するために取るその他の行動

16. プライバシー業務の範囲は次のとおりである。

(1) 全ての個人情報又は顧客情報や従業員情報のようなある特定された種類の個人情報のみを対象とする。

(2) 企業の全ビジネスセグメントと事業所又は明確に区分されたビジネスセグメント（例えば、小売事業を含み製造事業を含まない、企業のWebサイト又は特定のWebドメインで行われる特定の業務のみ。）、又はある特定の地理的場所（例えば、カナダの業務のみ。）

プライバシー業務の範囲は収集、利用、維持、開示、廃棄、個人識別不能化、匿名化から成る情報ライフサイクルの活動の全てを含むことが望ましい。

6　コミュニケーションはある特定のｅコマースの環境下において、権利、責任、関係者相互の合意、Webサイトにおいてユーザーが取引を完了する際の暗黙の了解としての項目や状況である。このような環境においてのコミュニケーションのカテゴリーは、方針や手続きをそれぞれの企業のWebサイトに公開を望ましいとするコミュニケーションの基準が要請される。各Trustサービス原則のための開示例が付録Ａ(45)に記載されている。

17. プライバシーに係るTrustサービスの原則と規準は、規準の説明を表すために３列（欄）の様式で記載されている。最初の列は、それぞれの原則を測定する規準（企業が原則の達成を示すために満たさなければならない属性）を含んでいる。２番目の列は、統制と手続の例示を提供している。これらは企業が規準を理解しやすいようにデザインされている。これらの説明は、企業が規準を満たすために全てを網羅するとか、どの例示も必要であるということを意図していない。３番目の列は補足説明を含む追加的な説明を記述している。それは例えば、良好なプライバシー実務、又は特定の国や産業において適用される特定の法令や規制から選別された要求事項などのような追加的情報である。

発効日

18. Trustサービス原則と規準は、2009年９月15日より発効する。

原則と規準

セキュリティ原則と規準

19. セキュリティ原則は、物理、論理両方の未承認のアクセスからのシステム構成要素の保護に関連する。システム構成要素へのアクセスを制限することは、潜在的なシステムの不正利用、リソースの盗用、ソフトウェアの誤用、情報への不正アクセス又は不正利用、改竄、破壊、漏洩を防止するのに役立つ。システム構成要素の保護のための重要な要素は、それらの構成要素への承認されたアクセスを許可し、未承認のアクセスを阻止することを含む。

セキュリティ原則と規準の表
20. システムは（物理、論理双方の）未承認のアクセスに対して保護されている。

規準	**内部統制の例**[7]
システムは（物理、論理双方の）未承認のアクセスに対して保護されている。	
1.0　ポリシー：企業は、システムのセキュリティのためにポリシーを定義して、文書化している。	
1.1　企業のセキュリティポリシーは、特定の個人又はグループによって確立され、定期的にレビューされ、承認されている。	ＩＴ及び物理的セキュリティの双方に関わる文書化されたセキュリティポリシーが、ＩＴ基準委員会により承認されており、企業全体に適用されている。 定期的なリスク評価プロセスの一部として、セキュリティ責任者は、新たなアプリケーションやインフラ又はそれらの重要な変更、新たな環境のセキュリティリスク、規制や基準の変更、SLAその他の文書に基づくユーザー要求の変更などに基づいてＩＴリスク評価の変更を識別する。その後、セキュリティ責任者はＩＴリスク評価に基づいて

7　記載されている統制は単なる事例である。これは検証において実際のポリシーや手順を特定するものではない。

規準	内部統制の例[7]
	セキュリティポリシーを更新する。 ＩＴセキュリティポリシーの変更は、適用前にＩＴ基準委員会により承認される。
1.2　セキュリティポリシーは、下記の事項を含むが、それらに制限されない。 a．承認されたユーザーのセキュリティ要件の識別と文書化 b．重要性、機微性（Sensitivity）に基づくデータの分類。分類は保護の必要性、アクセス権限、アクセス制限、維持と廃棄を定義するのに用いられる。 c．定期的なリスク評価 d．未承認のアクセスの防止 e．新規ユーザーの追加、既存ユーザーのアクセスレベルの変更及びアクセスする必要のなくなったユーザーの削除 f．システムセキュリティに対する実施責任と説明責任の割当て g．システム変更と維持管理に対する実施責任と説明責任の割当て h．導入前のシステム構成要素のテスト、評価、承認 i．セキュリティ問題に関連している苦情と要請がどのように解決されるか。 j．セキュリティ違反その他のインシデントを処理するための手続 k．システムセキュリティポリシーをサポートする訓練等に必要な経営資源を配分するための規定 l．システムセキュリティポリシーで明示的に扱われない逸脱事項と状況の取扱いのための規定	（本規準の内部統制の例は、企業の文書化されたセキュリティポリシーであり、左記に列挙された要素を含んでいる。セキュリティポリシーの例示は省略する。）

規準	内部統制の例[7]
m. 適用される法規制、定義されたコミットメント、SLAの識別と一致のための規定 n. 第三者との情報共有の提供	
1.3 企業のシステムセキュリティポリシーの開発・維持及びそれらのポリシーの変更・更新に関わる実施責任と説明責任が割り当てられている。	経営者は最高情報責任者（CIO）の指示の下に、企業のセキュリティポリシーの維持と施行に関する責任をセキュリティ責任者に割り当てている。役員会のＩＴ基準委員会は、役員会のハンドブックに示されたポリシーのレビュー、更新と承認について支援する。
2.0 コミュニケーション：企業は、責任ある当事者と承認されたユーザーに定義されたシステムセキュリティポリシーを伝達している。	
2.1 企業は、システムの記述とその範囲を客観的に定義して、承認されたユーザーに伝達している。	電子商取引システムのために、企業はWebサイト上にシステム記述を開示している。電子商取引システムのためのシステム記述については、付録Ａを参照のこと。 電子商取引でないシステムのために、企業は承認されたユーザーにシステム記述を提供している。電子商取引でないシステムのためのシステム記述については付録Ｂを参照のこと。
2.2 ユーザーのセキュリティ義務と企業のユーザーへのセキュリティコミットメントは、承認されたユーザーに伝達されている。	企業のセキュリティコミットメントと要求されるセキュリティ義務は、顧客及び他の外部ユーザーに対して、企業のWebサイト上に、又は企業の標準サービスアグリーメントの一部として掲示されている。 内部のユーザー（従業員と外部委託先）のために、企業の、セキュリティに関連するポリシーは、オリエンテーションの一部として新しい従業員と外部委託先にレビューされる。ポリシーの重要な項目と従業員への影響については検討される。新しい従業員はそれからポリシーを読んで、理解して、従うことを示している誓約書に署名しなくてはならない。 毎年、彼らのパフォーマンスレビューの一部として、従業員が企業のセキュリティポリシーの理解とそれへの遵守性を再確認しなくてはならない。外部委託先のセキュリティ義務が契約で詳述される。 セキュリティ周知プログラムが、従業員に企業のＩＴセキュリティポリシーを伝達するために実

規準	内部統制の例[7]
	施されている。 企業は、企業のイントラネット上にＩＴセキュリティポリシーを公開する。
2.3　企業のシステムセキュリティポリシーとそれらのポリシーに対する変更・更新のための実施責任と説明責任が、それらを実施することに責任がある企業の要員に伝達されている。	セキュリティ管理チームは、最高情報責任者（CIO）の指揮の下に、企業のセキュリティポリシーの日々の維持について義務と責任があり、そして、CIO及びＩＴ運営委員会に変更について提言する。 文書化された職務記述が定義され、セキュリティ管理チームに伝達されている。 全ての定義されたセキュリティプロセスの文書化されたプロセス及び手続マニュアルが、セキュリティ管理チームの要員に提供される。セキュリティ責任者はセキュリティポリシーの変更に基づいてプロセス及び手続マニュアルを更新する。
2.4　システムセキュリティの違反について、企業に通知し、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	顧客と外部のユーザーが潜在的なセキュリティ違反と他のインシデントを企業に知らせるプロセスは、企業のWebサイト上に開示されるか、又は新規ユーザーの手引書の一部として提供されている。 企業のセキュリティ周知プログラムには、潜在的なセキュリティ違反の識別、セキュリティ管理チームに知らせるプロセスに関する情報が含まれている。 セキュリティ違反その他のインシデントの識別と上申のための文書化された手続が存在している。
2.5　システムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されている。	システム構成要素に対する計画された変更とそれらの変更のスケジューリングは、月次のＩＴ運営委員会のミーティングの一部としてレビューされる。 システムセキュリティに影響を与えるかもしれない変更が、提案された変更の導入前に標準サービスアグリーメントの規定において影響を受ける顧客によってレビューされて、承認される。 顧客及びユーザーと彼らのセキュリティ義務又は企業のセキュリティコミットメントに影響を与えるかもしれない変更が、企業のWebサイト上に強調して掲示される。

規準	内部統制の例[7]
	システムセキュリティに影響を与える要素を含んだシステム構成要素に対する変更は、導入前に管理者及びセキュリティ管理チームの承認を必要とする。 システムセキュリティに影響を与える要素を含む変更の定期的なコミュニケーションがある。 システムセキュリティに影響を与える変更が、企業の進行中のセキュリティ周知プログラムに取り入れられている。
3.0 手続：企業は、定義されたシステムセキュリティポリシーに従って目的を達成するために手続を導入している。	
3.1 (1)システムセキュリティコミットメントを損なうシステム運用の中断の潜在的脅威の識別、(2)識別された脅威に関連するリスクの評価、のための手続が存在する。	リスク評価が定期的に実施される。このプロセスの一部として、セキュリティへの脅威が識別され、これらの脅威から生じるリスクが公式に評価される。 セキュリティ責任者が評価された脅威に基づき、セキュリティプロセスと手続を修正する。
3.2 定義されたシステムへの論理的アクセスを制限するための手続が存在する。下記の事項を含むが、それらに制限されない。	
a. 公にすべきでない情報資源へのアクセスを制限するための論理的アクセスセキュリティ対策	・ 公にすべきでない情報資源への論理的アクセスは、ＯＳ固有のセキュリティ、アプリケーション及び資源固有のセキュリティ、追加的なセキュリティソフトウェアの利用を通じて保護される。 ・ 資源に特有な、又は初期的なアクセスルールは、全ての公にすべきでない資源について定義される。 ・ 資源へのアクセスは、ユーザーの身元に基づいて認証されたユーザーに付与される。
b. ユーザーの識別と認証	・ ユーザーは、関連するパスワードで認証された正しいユーザーＩＤの利用を通じて公にされていない資源にアクセスしようとする場合、企業のネットワークとアプリケーションシステムに対して身元を明らかにしなければならない。 ・ ユニークなユーザーＩＤが個別のユーザーに割り当てられる。 ・ グループ又は共有ＩＤは十分なリスク評価と共有ＩＤを利用するビジネスユニットのマネージャの文書による承認がないと利用できない。

規準	内部統制の例[7]
	・　パスワードは大文字と小文字を区別し、少なくとも８文字で、そのうち１文字は英数字でない文字を含んでいなくてはならない。 ・　セキュリティ設定のパラメータにより、パスワードは90日ごとに更新されるよう強制される。 ・　ログインを３回失敗するとログインできなくなる。
c．新規ユーザーの登録と承認	・　顧客は、企業のWebサイト上で、新規ユーザー情報を提供し、適切なユーザーＩＤとパスワードを選ぶセキュアなセッションの下において自己登録することができる。自己登録された顧客口座と結び付けられた権限及び権限付与が、特定の制限されたシステム機能を提供する。 ・　直属の業務統括者は、従業員と外部委託先のアクセス権変更のリクエストを承認する。制限された資源へのアクセスは資源の所有者（リソース・オーナー）によって承認される。 ・　自己登録の間に与えられたデフォルト権限を超えた顧客アクセス権は、顧客口座管理者か資源の所有者によって承認される。 ・　ユーザーの職務記述書又は役割に基づいて、適切な職務分離が権限を与える際に考慮されている。 ・　ユーザーとユーザーアクセス権限（制限された「顧客口座」としての機能性を除く。）を生成又は修正する権限は、セキュリティ管理チームに限定される。
d．ユーザープロファイルに対する変更と更新のプロセス	・　自己登録の顧客口座に対する変更と更新は、ユーザーが成功裏にシステムにログインした後、企業のWebサイト上でいつでも個々のユーザーによって可能となる。変更は即時に反映される。 ・　使われていない顧客口座（６か月間不使用）がシステムによって排除される。 ・　他のアカウントとプロファイルに対する変更は、セキュリティ管理チームに制限されていて、直属の業務統括者、顧客口座管理者、資源の所有者の承認を要求する。 ・　人事管理システムが新たに退職した従業員のリストを毎週人事部に提供する。このリストはアカウント失効のためにセキュリティ管理チームに送られる。
e．承認されたユーザーに制限されたアウトプット配布	・　コンピュータが処理したアウトプットへのアクセスは、承認された人にだけ、情報の分類に基づいて提供される。

規準	内部統制の例[7]
f．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アクセスの制限 g．システム構成、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とセキュリティ装置（例えば、ファイアウォール）に対するアクセスの制限	・　処理されたアウトプットは、その情報の分類を反映した領域に保存される。 ・　処理されたアウトプットは、情報の分類に基づいたセキュリティポリシーに従って配布される。 ・　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アクセスは、物理的・論理的アクセスコントロールにより、コンピュータ運用スタッフに制限されている。 ・　ハードウェアとオペレーティング・システム設定テーブルは、物理的なアクセス制御、オペレーティング・システム固有のセキュリティ、追加されたセキュリティ機能により適切な要員に制限されている。 ・　アプリケーションソフトウェアの設定テーブルは、承認されたユーザーに制限されており、アプリケーションの変更管理ソフトウェアのコントロール下にある。 ・　データ又はプログラムを、閲覧、追加、変更、削除できるユーティリティプログラムは、承認された技術サービススタッフに制限されている。その使用は、コンピュータ運用の管理者によってログを採取され、モニターされる。 ・　CIO指揮下の情報セキュリティチームは、全ての記憶装置メディアへのアクセスはもちろん、ファイアウォールその他のログへのアクセスも保持する。いかなるアクセスもログを採取されて、企業のＩＴポリシーに従ってレビューされる。 ・　全てのマスターパスワードのリストが暗号化されたデータベースに保存され、副本が企業の金庫に封印された封筒で保持される。
3.3　定義されたシステムへの物理的アクセスを制限する手続が存在する。施設、バックアップ媒体、及びファイアウォール、ルータ、サーバーのような他のシステム構成要素を含むが、それらに制限されない。	企業のＩＴ資源、サーバー及びファイアウォールとルータなどの関連するハードウェアを収容するコンピュータ室への物理的なアクセスが、カードキーシステムによって承認された個人に制限され、ビデオ監視装置によって監視される。 物理的なアクセスカードがビル警備によって管理される。アクセスカードの使用実績が日誌に記録される。記録はビル警備によって保持され、レビューされる。 企業のコンピュータ施設への物理的なアクセス権のリクエストは、コンピュータ運用管理者の承認を必要とする。

規準	内部統制の例[7]
	潜在的セキュリティ違反の識別と上申についての文書化された手続が存在する。 外部保管媒体は安全な施設の中の施錠された保管庫に保存される。これらの保管庫の物理的アクセスはコンピュータ運用管理者の承認された施設担当要員に制限される。
3.4　システム資源への未承認のアクセスから保護するための手続が存在する。	ログインセッションは、３回のログイン失敗の後に終了させられる。 VPN(仮想専用ネットワーク)ソフトウェアが、承認されたユーザーによるリモートアクセスを認めるために使われる。ユーザーが特定の「クライアント」ソフトウェアとユーザーＩＤ及びパスワードを通してVPNサーバーによって認証される。 ファイアウォールが使われて、未承認のアクセスを阻止するために設定される。ファイアウォールの状況はログが採取され、セキュリティ管理者によって毎日レビューされる。 不必要なネットワークサービス（例えば、telnet、ftp、http）は企業のサーバー上で無効とされる。必要とされ承認されたサービスのリストがＩＴ部門によって保持される。このリストは、最新の運用状況における適切性の観点から定常的に企業の管理者によってレビューされる。 企業のネットワークの継続的モニタリングと、潜在的セキュリティ違反の初期段階での識別を提供するために、侵入検知システムが使われる。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。結果と改良のための改善勧告が経営者に報告される。
3.5　コンピュータ・ウィルス、悪意があるコードと未承認のソフトウェアによる感染から保護するための手続が存在する。	他のセキュリティモニタリングに関連して、セキュリティ管理チームは、ユーザー・グループに関与して、コンピュータ・ウィルスに関するサービスに加入する。 送られてくる電子メールメッセージのウィルススキャンを含むアンチウィルスのソフトウェアが備わっている。パターンファイルは都度更新される。

規準	内部統制の例[7]
	発見されたいかなるウィルスもセキュリティチームに報告され、全てのユーザーにそれらの潜在的ウィルス脅威を周知するために警告がなされる。 ＯＳやその他のシステムプログラムをインストール、変更、リプレースする権限は、承認された要員に制限されている。 スーパーユーザー機能及び取扱いに細心の注意を要するシステム機能に対するアクセスは、承認された要員に制限されている。
3.6　インターネット又は他の公衆網上を通過するユーザー認証情報と伝送を保護するため、暗号化又は他の同等のセキュリティ技術が利用される。	企業は、公衆網上でのユーザーＩＤとパスワードを含む個人情報又は機密情報の送信のために、業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を利用する。潜在的セキュリティ問題を回避するためセキュリティ管理チームによってテストされて、使用に当たって承認された最新のバージョンへブラウザを更新するようにユーザーは要求される。 アカウント使用状況はログイン成功後に業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を通して暗号化される。ユーザーは、要求すればすぐに（Webサイト上の「サインアウト」ボタンを選択することによって）、又は10分間使用しないとログアウトされる。
目的達成のために利用される実行及びインシデント管理関連の規準	
3.7　システムセキュリティ違反その他のインシデントを識別して、報告して、行動を起こすための手続が存在する。	ユーザーには、情報セキュリティチームへの潜在的セキュリティ違反を伝達するように指針が提供される。情報セキュリティチームは、顧客ホットラインと電子メールを通して報告されたインシデントを日誌に記録する。 侵入検知システムとその他のツールが、潜在的セキュリティ違反とその他のインシデントを識別し、ログを採取し、報告するために使われる。システムは、進行中の潜在的インシデントについて、電子メールと文書によってネットワーク管理者又は情報セキュリティチームに通知する。 インシデントログが情報セキュリティチームによって毎日モニターされ、評価される。

規準	内部統制の例[7]
	インシデントが発見又は報告された場合、承認された要員により、定義されたインシデント管理プロセスが開始される。定義されたポリシー及び手続に準拠して是正措置が実施される。 手続は、定義されたインシデントの上申プロセス及び通知体制を含んでいる。 全てのインシデントは、解決するまで経営者によって追跡される。 終了したインシデントは、適切な解決のために経営者によりレビューされる。 セキュリティに関連しないインシデントの解決には、インシデントとその解決がセキュリティ要件に与える影響を考慮することが含まれている。
目的達成のために利用されるシステム構成要素関連の規準	
3.8　データ分類のポリシーに従ってデータ分類をし、必要に応じて、それらの分類の定期的なモニタリングと更新を行う手続が存在する。	データオーナーは定義されたセキュリティ要件及びリスク評価に基づいて、データアクセスルールを定期的にレビューし、修正を要求する。 新しいデータが補足又は生成された場合はいつでも、そのデータはセキュリティポリシーに基づいて分類される。 データ分類の適正性は、変更管理プロセスの一部として考慮される。
3.9　セキュリティポリシーへの遵守性違反が直ちに対処され、是正措置がタイムリーに取られる手続が存在する。	全てのインシデントは解決するまで経営者によって追跡される。 終了したインシデントは適切に解決したかを経営者により評価される。 内部監査プロセスは、発見事項に対する行動計画の作成と終了するまでの行動計画の追跡を含んでいる。
3.10　システム基盤とソフトウェアの設計、調達、導入、設定、修正と管理は、承認されたアクセスを可能にして、未承認のアクセスを阻止するために定義されたシステムセキュリティポリシーと整合している。	企業は、コンピュータ化された情報システムの開発、調達、導入、維持及び関連する技術を管理する公式なシステム開発ライフサイクル（SDLC）方法論を適用している。 SDLC方法論は、セキュリティ損失のビジネス影響度の評価に基づいて、確立されたデータ分類と標準的なユーザープロファイルの生成のためのフ

規準	内部統制の例[7]
	レームワークを含んでいる。ユーザーは必要性と職務上の責任に基づいて、標準的なプロファイルを割り当てられる。 セキュリティ管理チームは、新しいシステム開発及び調達について、企業のセキュリティ目的、ポリシー及び基準との整合性を保証するために、アーキテクチャと設計仕様書をレビューして承認する。 セキュリティに影響を与えるかもしれないシステム構成要素に対する変更は、セキュリティ管理チームの承認を必要とする。
3.11　セキュリティに影響を与えているシステムの設計、開発、導入、運用に関して責任がある要員が、彼らの責任を果たす資格と能力を持っていることを規定するための手続が存在する。	企業は、重要な職位のための実施責任と、理論的及び職業的要件を記述した職務記述書を作成している。 雇用手続は、重要な職位の候補者の包括的な審査、及び証明された資格が提案された職位と見合うか否かという検討を含んでいる。新しい要員が、経歴調査と身元調査の対象となることを条件に雇用される。 内部異動を含めた候補者は、職位の提示前に直属の業務統括者によって承認される。 定期的な業績評価が従業員の直属の上司によって行われる、それには人材育成活動の評価とレビューが含まれる。 要員は、システムセキュリティ概念と諸問題に関する訓練と能力開発を受ける。 休暇又は出張の場合に、重要なシステムセキュリティ機能のために代替要員を提供するための手続が備わっている。
システムセキュリティに特有な変更管理関連の規準	
3.12　定義されたシステムセキュリティポリシーと整合した環境設定を含めて、システム構成要素を保持する手続が存在する。	企業経営者が、セキュリティ管理の適切性についての第三者意見を受け取って、企業のシステムとWebサイトをホストしているサービスプロバイダから契約（SLA）に従い受け取るパフォーマンスのレベルを定期的に評価する。 ＩＴ部門は、全てのソフトウェアとそれぞれのレベル、適用されたバージョンとパッチの最新のリストを保持する。

規準	内部統制の例[7]
	システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知らされる。 システム構成は毎年テストされ、企業のセキュリティポリシーと最新のSLAに対して評価される。逸脱事項報告書が作成されるとともに、改善計画が作成され追跡される。
3.13　承認され、テストされ、文書化されたシステム変更だけが行われる手続が存在する。	システム変更の承認、テスト、開発、導入の各職務は、分離されている。 企業の文書化されたシステム開発方法論は、プロセスに埋め込まれた基準と内部統制と同様に、変更着手、ソフトウェア開発と保守及び承認プロセスが含まれる。これらはプログラミング、文書化、テストの基準を含む。 システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況と終了について知らされる。 システム基盤とソフトウェアに対する変更は、本番への導入前に、別の開発・テスト環境で開発され、テストされる。 変更管理ポリシーと手続の一部として、「本番移行」プロセス（例えば、「テスト」から「移行」「本番」まで。）がある。本番への移行に際しては、変更の予算を持つ業務責任者とコンピュータ運用の管理者の承認を必要とする。 変更が重要なシステム構成要素に行われるとき、重要な中断に備えて、作成された「復帰（バックアウト）」計画がある。
3.14　緊急変更が文書化され適時に承認されることを規定するための手続が存在する。	システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知ら

規準	内部統制の例[7]
	される。 標準手続からの逸脱を必要とする緊急変更は、毎日ＩＴ管理者によってログを採取され、レビューされ、直属の業務統括者に報告される。恒久的是正措置は、企業の業務統括者の承認を含む変更管理プロセスに従う。
4.0　モニタリング：企業は、システムをモニターして、定義されたシステムセキュリティポリシーの遵守性を保持するための行動を取る。	
4.1　企業のシステムセキュリティは、定期的にレビューされ、定義されたシステムセキュリティポリシーと比較される。	情報セキュリティチームは、内製の又は一般に利用可能なツールを使ってシステムをモニターし、脆弱性を評価する。潜在的リスクが評価され、SLAと企業のその他の義務と比較される。改善計画が提案され、実施がモニターされる。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。内部監査部門は、年度の監査計画の一部として、システムセキュリティレビューを行う。結果と改善のための提案が経営者に報告される。
4.2　定義されたシステムセキュリティポリシーに従った目的を達成するために、企業の現行の能力の潜在的な劣化を識別して、対処するプロセスがある。	システムセキュリティ目的を達成する企業の能力への潜在的な影響を与えるかもしれない傾向を識別するために、人的又は自動化ツールによってログを分析する。 月次のＩＴスタッフ会議が、システムセキュリティ上の問題と傾向に対処するために開催される。発見事項は年４回の経営会議において検討される。
4.3　環境、規制、技術の変更がモニターされ、それらのシステムセキュリティ上の影響が適時に評価され、その評価に基づきポリシーが更新される。	上級経営者が、年度のＩＴ計画プロセスの一部として、企業のセキュリティポリシー上に適用される法規制の影響と技術開発を考慮する。 企業のＩＴセキュリティグループは、新規技術のセキュリティの影響をモニターする。 ユーザーは、新しい技術の使用を通してシステムセキュリティを改善するために、積極的、主導的に貢献するよう要請される。

可用性原則と規準

21. 可用性原則は、契約、SLA又は他のアグリーメントによって通知又はコミットされるシステム、プロダクト又はサービスへの利用可能性に言及する。この原則自身は、最小限受容できるパフォーマンスレベルをシステム可用性と位置付けないことに注意すべきである。最小パフォーマンスレベルは、当事者間で行われたコミットメン

ト又は相互の合意（契約）によって確定している。

22. システムの可用性、機能性、利用容易性の間には関連があるけれども、可用性原則は、システムの機能性（システムが実施する特定の機能）と利用容易性（システム機能を特定のタスク又は問題に適用するユーザーの能力）を扱わない。システムの可用性は、システムが処理、モニタリング、維持のために、利用可能であるかどうかに関係がある。

可用性原則と規準の表
23. システムは、コミット又は合意したとおりに操作できかつ利用できる。

規準	**内部統制の例**
システムは、コミット又は合意したとおりに操作でき、かつ、利用できる。	
1.0 ポリシー：企業は、システムの可用性のためにポリシーを定義して、文書化している。	
1.1 企業のシステム可用性及び関連するセキュリティポリシーは、特定の個人又はグループによって確立され、定期的にレビューされ、承認されている。	文書化された可用性ポリシーは、ＩＴ基準委員会により承認されており、企業全体に適用されている。 企業の文書化されたシステム開発と調達のプロセスは、システム上の承認されたユーザーと可用性に関連するセキュリティ要件を識別して、文書化するための手続を含んでいる。 ユーザー要件がSLA又はその他の書類で文書化されている。
1.2 企業のシステム可用性及びそれと関連するセキュリティポリシーは、下記の事項を含むが、それらに制限されない。 a. 承認されたユーザーのシステム可用性及びそれと関連するセキュリティ要件の識別と文書化 b. 重要性、機微性（Sensitivity）に基づくデータの分類。分類は保護の必要性、アクセス権限、アクセス制限、維持と廃棄を定義するのに用いられる。 c. 定期的なリスク評価 d. 未承認のアクセスの防止 e. 新規ユーザーの追加、既存ユーザーのアクセスレベルの変更及びアクセスする	（本規準の内部統制の例は、企業の文書化された可用性ポリシーと関連するセキュリティポリシーであり、左記に列挙された要素を含んでいる。可用性とセキュリティポリシーの例示は省略する。）

規準	内部統制の例
必要のなくなったユーザーの削除 f．システム可用性及びそれと関連するセキュリティに対する実施責任と説明責任の割当て g．システム変更と維持管理に対する実施責任と説明責任の割当て h．導入前のシステム構成要素のテスト、評価、承認 i．システム可用性及びそれと関連するセキュリティ問題に関連している苦情と要請がどのように解決されるか。 j．システム可用性及びそれと関連するセキュリティ違反その他のインシデントを処理するための手続 k．システム可用性及びそれと関連するセキュリティポリシーをサポートする訓練等に必要な経営資源を配分するための規定 l．システム可用性及びそれと関連するセキュリティポリシーで明示的に扱われない逸脱事項と状況の取扱いのための規定 m．適用される法規制、定義されたコミットメント、SLAの識別と一致のための規定 n．文書化された顧客コミットメント又はその他の合意に準拠した復旧及びサービスの継続性 o．可用性に関して顧客コミットメント又はその他の合意を達成するためのモニタリングのシステム性能	
1.3　企業のシステム可用性及びそれと関連するセキュリティポリシーの開発・維持及びそれらのポリシーの変更・更新	経営者は最高情報責任者(CIO)に、企業の可用性ポリシーの維持と施行に対する責任を割り当てている。役員会のＩＴ基準委員会は、役員会のハンドブックに示されたポリシーのレビュー、更新と

規準	内部統制の例
に関わる実施責任と説明責任が割り当てられている。	承認について支援する。 重要な情報資源（例えば、データ、プログラムと取引）の所有と管理及び、当該資源の上にシステム可用性及びそれと関連するセキュリティを確立して、維持するための実施責任が定義されている。
2.0 コミュニケーション：企業は、責任ある当事者と承認されたユーザーに定義されたシステム可用性ポリシーを伝達している。	
2.1 企業は、システムの記述とその範囲を客観的に定義して、承認されたユーザーに伝達している。	電子商取引システムのために、企業はWebサイト上にシステム記述を開示している。電子商取引システムのためのシステム記述については、付録Ａを参照のこと。 電子商取引でないシステムのために、企業は承認されたユーザーにシステム記述を提供している。電子商取引でないシステムのためのシステム記述については付録Ｂを参照のこと。
2.2 ユーザーの可用性に関連するセキュリティ義務と、企業のユーザーへの可用性及び関連するセキュリティコミットメントは、承認されたユーザーに伝達されている。	企業は、システム可用性及びそれと関連するセキュリティコミットメントと要求される可用性と関連するセキュリティ義務は、顧客及び他の外部ユーザーに対して、企業のWebサイト上に、又は企業の標準サービスアグリーメントの一部として掲示されている。SLAは毎年顧客にレビューされている。 内部のユーザー（従業員と外部委託先）のために、企業の、システム可用性とセキュリティに関連するポリシーは、オリエンテーションの一部として新しい従業員と外部委託先にレビューされる。ポリシーの重要な項目と従業員への影響については検討される。新しい従業員はポリシーを読んで、理解して、従うことを示している誓約書に署名しなくてはならない。毎年、彼らのパフォーマンスレビューの一部として、従業員がポリシーの理解とそれへの遵守性を再確認しなくてはならない。外部委託先の義務が契約で詳述される。 セキュリティ周知プログラムが、従業員に企業のＩＴセキュリティポリシーを伝達するために実施されている。 企業は、企業のイントラネット上にＩＴセキュリティポリシーを公開する。
2.3 企業のシステム可用性及びそれと関連するセキュリティ	ネットワーク運用チームは、最高情報責任者（CIO）の指揮の下に、企業の可用性ポリシーを実

規準	内部統制の例
ポリシーとそれらのポリシーに対する変更・更新のための実施責任と説明責任が、それらを実施することに責任がある企業の要員に伝達されている。	施することに責任がある。セキュリティ管理チームは、関連するセキュリティポリシーを実施することに責任がある。 ネットワーク運用チームは、企業の可用性ポリシーの日々の維持について義務と責任があり、CIOとＩＴ運営委員会に対する変更について提言する。セキュリティ管理チームは、関連するセキュリティポリシーについて責任がある。 文書化された職務記述が定義され、ネットワーク運用チームとセキュリティ管理チームに伝達されている。 全てのオペレーションとセキュリティプロセスの文書化されたプロセス及び手続マニュアルが、担当者に提供される。指名された担当者は可用性の要求とセキュリティポリシーの変更に基づいてプロセス及び手続マニュアルを更新する。
2.4　システム可用性の問題、システムセキュリティの違反について企業に通知し、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	顧客と外部のユーザーがシステム可用性、潜在的なセキュリティ違反と他のインシデントを企業に知らせるプロセスは、企業のWebサイト上に開示されるか、又は新規ユーザーの手引書の一部として提供されている。 企業のユーザー訓練プログラムは、システム可用性問題、セキュリティ違反その他のインシデントの識別及び報告の対処手順を含んでいる。 企業のセキュリティ周知プログラムには、潜在的なセキュリティ違反の識別、セキュリティ管理チームに知らせるプロセスに関する情報が含まれている。 システム可用性問題、セキュリティ違反その他のインシデントの識別と上申のための文書化された手続が存在している。
2.5　システム可用性とシステムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されている。	システム可用性、顧客及びユーザーと彼らのセキュリティ義務、又は企業のセキュリティコミットメントに影響を与えるかもしれない変更が、企業のWebサイト上に強調される。 システムセキュリティに影響を与えるかもしれない変更が、提案された変更の導入前に、標準サービスアグリーメントの規定において影響を受ける顧客によってレビューされて、承認される。

規準	内部統制の例
	システム構成要素に対する計画された変更とそれらの変更のスケジューリングは、月次のＩＴ運営委員会のミーティングの一部としてレビューされる。 システム構成要素に影響を与える要素を含んだシステム構成要素に対する変更は、導入前に管理者及びセキュリティ管理チームの承認を必要とする。 可用性とシステムセキュリティに影響を与える変更を含むシステム変更の定期的なコミュニケーションがある。
3.0　手続：企業は、定義されたポリシーに従って文書化されたシステム可用性目的を達成するために手続を導入している。	
3.1　(1)システム可用性コミットメントを損なうシステム運用の中断の潜在的脅威の識別、(2)識別された脅威に関連するリスクの評価、のための手続が存在する。	内外の物理的環境のいずれかにおいて、定期的に又は重要な変更が起こるたびに、脅威を識別するリスク評価が実施され、レビューされている。 火災、水害、塵埃、電力停止、過熱、過湿度、労働問題といった脅威が考慮される。
3.2　実務的に可能な場合、リスク評価に対応した、脅威の防止又は低減策が導入されている。	経営者は、定期的なリスク評価に基づいて、環境的要因（例えば、火災、水害、塵埃、電力停止、過熱、過湿度）から保護する対策を維持する。企業が管理している領域は、煙探知器と防火システム両方を利用して火災から保護される。漏水検知器が二重床の中に設置される。 無停電電源装置（UPS）と緊急時電源装置（EPS）両方を利用することによって、企業サイトの処理環境は停電から保護される。この装置は半年ごとにテストされる。 予防的な保守契約と予定された保守手続が、重要なシステムハードウェア構成要素のために備わっている。 ベンダー保証仕様書が準拠され、システムが適切に設定されているかを確認するためにテストされる。 マイナーな処理エラー、停電と記録の破壊に対応するための手続が文書化されている。 問題の識別、文書化、上申、解決、レビューの

規準	内部統制の例
	ための手続が存在する。 物理的、論理的なセキュリティ管理が、システム可用性を害する可能性のある未承認の行動の機会を減らすために導入されている。
3.3　企業の定義されたシステム可用性及びそれと関連するセキュリティポリシーに整合したバックアップ、外部保管、回復、災害復旧を提供するための手続が存在する。	経営者は、ビジネス要件のレビューに基づいて、バックアップ及び回復のための包括的な戦略を導入する。企業のバックアップ手続が文書化されており、それらは冗長サーバー、日次の差分バックアップ及び、週１回の変更の完全バックアップを含んでいる。日次、週次のバックアップが企業のシステム可用性ポリシーに従って外部保管される。 災害復旧計画と緊急時対応計画が、文書化される。 災害復旧計画は役割と責任を定義して、ビジネス影響度分析に基づいて、高い可用性とシステムの信頼性を確かめるために必要な、重要なＩＴアプリケーションプログラム、オペレーティング・システム、要員、データファイル、タイムフレームを識別する。 事業継続計画（BCP）調整者は、毎年、ビジネスの各分野についてのビジネス影響度分析をレビューして更新する。 災害復旧計画と緊急時対応計画が、企業のシステム可用性ポリシーに従って毎年テストされる。テスト結果と変更勧告が企業の経営会議に報告される。 企業の経営会議は災害復旧計画に対する変更をレビューして、承認する。 契約している災害対策施設の能力は、文書化された処理要件と年に一度比較され、必要に応じて修正される。 事業継続計画で識別された重要な要員は、社内及び外部で計画の最新のバージョンを保有している。電子版が外部保管される。
3.4　企業の定義されたシステム可用性及びそれと関連するセキュリティポリシーをサポー	自動化されたバックアッププロセスには、バックアップデータのインテグリティをテストするための手続が含まれる。

規準	内部統制の例
トすることができるように、バックアップデータとシステムのインテグリティを保持する手続が存在する。	バックアップが企業の定義されたバックアップ戦略に従って行われ、バックアップの活用性が少なくとも毎年確かめられる。 利用可能なバックアップの一覧とバックアップの物理的なロケーションは、運用担当者によって維持される。 バックアップシステムとデータが、サードパーティーサービスプロバイダの施設において外部保管される。 サービスプロバイダ契約の要件の下で、企業は、外部保管施設において保存された媒体の年次検証を実施する。検証の一部として、外部保管の場所における媒体が、適切な媒体管理システムと照合される。保管場所は、物理的なアクセスセキュリティとデータファイルと他の項目のセキュリティのために半年に１回視察される。 バックアップシステムとデータが年度の災害復旧テストの一部としてテストされる。
システムの可用性に特有のセキュリティ関連の規準	
3.5　定義されたシステムへの論理的アクセスを制限するための手続が存在する。下記の事項を含むが、それらに制限されない。	
a．公にすべきでない情報資源へのアクセスを制限するための論理的アクセスセキュリティ対策	・　公にすべきでない情報資源への論理的アクセスは、ＯＳ固有のセキュリティ、アプリケーション及び資源固有のセキュリティ、追加的なセキュリティソフトウェアの利用を通じて保護される。 ・　資源に特有な、又は初期的なアクセスルールは、全ての公にすべきでない資源について定義される。 ・　資源へのアクセスは、ユーザープロファイルに基づいて、認証されたユーザーに付与される。
b．ユーザーの識別と認証	・　ユーザーは、関連するパスワードで認証された正しいユーザーＩＤの利用を通じて公にされていない資源にアクセスしようとする場合、企業のネットワークとアプリケーションシステムに対して身元を明らかにしなければならない。 ・　ユニークなユーザーＩＤが個別のユーザーに

規準	内部統制の例
	割り当てられる。 ・　グループ又は共有ＩＤは十分なリスク評価と共有ＩＤを利用するビジネスユニットのマネージャの文書による承認がないと利用できない。 ・　パスワードは大文字と小文字を区別し、少なくとも８文字で、そのうち１文字は英数字でない文字を含んでいなくてはならない。 ・　セキュリティ設定のパラメータにより、パスワードは90日ごとに更新されるよう強制される。 ・　ログインを３回失敗するとログインできなくなる。
c．新規ユーザーの登録と承認	・　顧客は、企業のWebサイト上で、新規ユーザー情報を提供し、適切なユーザーＩＤとパスワードを選ぶセキュアなセッションの下において、自己登録することができる。自己登録された顧客口座と結び付けられた権限及び権限付与が、特定の制限されたシステム機能を提供する。 ・　ユーザーとユーザーアクセス権限（制限された「顧客口座」としての機能性を除く。）を生成又は修正する権限は、セキュリティ管理チームに限定される。 ・　直属の業務統括者は、従業員と外部委託先のアクセス権変更のリクエストを承認する。制限された資源へのアクセスは資源の所有者（リソース・オーナー）によって承認される。 ・　自己登録の間に与えられたデフォルト権限を超えた顧客アクセス権は、顧客口座管理者によって承認される。適切な職務分離が権限を与える際に考慮されている。
d．ユーザープロファイルに対する変更と更新のプロセス	・　自己登録の顧客口座に対する変更と更新は、ユーザーが成功裏にシステムにログインした後、企業のWebサイト上でいつでも個々のユーザーによって可能となる。変更は即時に反映される。 ・　使われていない顧客口座（６か月間不使用）がシステムによって排除される。 ・　他のアカウントとプロファイルに対する変更は、セキュリティ管理チームに制限されていて、直属の業務統括者、顧客口座管理者の承認を要求する。 ・　人事管理システムが新たに退職した従業員のリストを毎週人事部に提供する。このリストはアカウント失効のためにセキュリティ管理チームに送られる。
e．オフラインストレージ、	・　オフラインストレージ、バックアップデー

規準	内部統制の例
バックアップデータ、システムと媒体へのアクセスの制限 f. システム構成、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とセキュリティ装置（例えば、ファイアウォール）に対するアクセスの制限	タ、システムと媒体へのアクセスは、物理的・論理的アクセスコントロールにより、コンピュータ運用スタッフに制限されている。 ・　ハードウェアとオペレーティング・システム設定テーブルは、適切な要員に制限されている。 ・　アプリケーションソフトウェアの設定テーブルは、承認されたユーザーに制限されており、アプリケーションの変更管理ソフトウェアのコントロール下にある。 ・　データ又はプログラムを、閲覧、追加、変更、削除できるユーティリティプログラムは、承認された技術サービススタッフに制限されている。その使用は、コンピュータ運用の管理者によってログを採取され、モニターされる。 ・　CIO指揮下の情報セキュリティチームは、全ての記憶装置メディアへのアクセスはもちろん、ファイアウォールその他のログへのアクセスも保持する。いかなるアクセスもログを採取されて、企業のＩＴポリシーに従ってレビューされる。 ・　全てのマスターパスワードのリストが暗号化されたデータベースに保存され、副本が企業の金庫に封印された封筒で保持される。
3.6　定義されたシステムへの物理的アクセスを制限する手続が存在する。施設、バックアップ媒体、及びファイアウォール、ルータ、サーバーのような他のシステム構成要素を含むが、それらに制限されない。	企業のＩＴ資源、サーバー及びファイアウォールとルータなどの関連するハードウェアを収容するコンピュータ室への物理的なアクセスが、カードキーシステムによって承認された個人に制限され、ビデオ監視装置によって監視される。 物理的アクセスカードがビル警備によって管理される。アクセスカードの使用実績が日誌に記録される。記録はビル警備によって保持され、レビューされる。 企業のコンピュータ施設への物理的なアクセス権のリクエストは、コンピュータ運用管理者の承認を必要とする。 潜在的セキュリティ違反の識別と上申についての文書化された手続が存在する。 外部保管バックアップデータと媒体がサービスプロバイダ施設において保存される。外部保管データと媒体へのアクセスはコンピュータ運用管理者の承認を必要とする。

規準	内部統制の例
3.7　システム資源への未承認のアクセスから保護するための手続が存在する。	ログインセッションは、３回のログイン失敗の後に終了させられる。 VPN(仮想専用ネットワーク)ソフトウェアが、承認されたユーザーによるリモートアクセスを認めるために使われる。ユーザーが特定の「クライアント」ソフトウェアとユーザーＩＤ及びパスワードを通してVPNサーバーによって認証される。 ファイアウォールが使われて、未承認のアクセスを阻止するために設定される。ファイアウォールの状況はログが採取され、セキュリティ管理者によって毎日レビューされる。 不必要なネットワークサービス（例えば、telnet、ftp、http）は企業のサーバー上で無効とされる。必要とされ承認されたサービスのリストがＩＴ部門によって保持される。このリストは、最新の運用状況における適切性の観点から定常的に企業の管理者によってレビューされる。 企業のネットワークの継続的モニタリングと、潜在的セキュリティ違反の初期段階での識別を提供するために侵入検知システムが使われる。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。結果と改良のための改善勧告が経営者に報告される。
3.8　コンピュータ・ウィルス、悪意があるコードと未承認のソフトウェアによる感染から保護するための手続が存在する。	他のセキュリティモニタリングに関連して、セキュリティ管理チームは、ユーザー・グループに関与して、コンピュータ・ウィルスに関するサービスに加入する。 送られてくる電子メールメッセージのウィルススキャンを含むアンチウィルスのソフトウェアが備わっている。パターンファイルは都度更新される。 発見されたいかなるウィルスもセキュリティチームに報告され、全てのユーザーにそれらの潜在的ウィルス脅威を周知するために警告がなされる。 ＯＳやその他のシステムプログラムをインストール、変更、リプレースする権限は、承認された要員に制限されている。

規準	内部統制の例
	スーパーユーザー機能及び取扱いに細心の注意を要するシステム機能に対するアクセスは、承認された要員に制限されている。
3.9　インターネット又は他の公衆網上を通過するユーザー認証情報と伝送を保護するため、暗号化又は他の同等のセキュリティ技術が利用される。	企業は、公衆網上でユーザーＩＤとパスワードを含む個人情報又は機密情報の送信のために、業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を利用する。潜在的セキュリティ問題を回避するためセキュリティ管理チームによってテストされて、使用に当たって承認された最新のバージョンへブラウザを更新するようにユーザーは要求される。 アカウント使用状況はログイン成功後に業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を通して暗号化される。ユーザーは、要求すればすぐに（Webサイト上の「サインアウト」ボタンを選択することによって）、又は10分間使用しないとログアウトされる。
目的達成のために利用される実行及びインシデント管理関連の規準	
3.10　システム可用性上の問題と関連するセキュリティ違反その他のインシデントを識別して、報告して、行動を起こすための手続が存在する。	ユーザーには、システム可用性問題、潜在的セキュリティ違反その他の問題をヘルプデスク又は顧客サービスセンターへ伝達するための指針が提供される。 ヘルプデスクによって解決できないシステム可用性問題と潜在的セキュリティ違反を上申するための文書化された手続が存在する。 ネットワークパフォーマンスとシステム処理が24時間休みなく、社内運用スタッフによって、システムモニタリングツールを使ってモニターされる。パフォーマンス及び処理の可用性問題の上申及び解決のために文書化された手続が存在する。 侵入検知システムとその他のツールが、潜在的セキュリティ違反とその他のインシデントを識別し、ログを採取し、報告するために使われる。システムは、進行中の潜在的インシデントについて、電子メールと文書によってネットワーク管理者と情報セキュリティチームに通知する。 インシデントログが情報セキュリティチームに

規準	内部統制の例
	よって毎日モニターされ、評価される。 文書化されたインシデントの識別と上申手続は経営者によって承認され、定義されたインシデントの上申プロセス及び通知体制を含んでいる。 ネットワークパフォーマンス、システム可用性とセキュリティインシデントの統計と承認された目標との比較の記録が蓄積されて、ＩＴ運営委員会に毎月報告される。 システムパフォーマンスと性能の分析と予測が、ＩＴ計画及び予算編成プロセスの一部として毎年実施される。 システム及びネットワーク運用は運用要員により積極的にモニターされる。 システム中断が発見又は報告された場合、システム及びネットワーク運用要員により、定義されたインシデント管理プロセスが開始される。定義されたポリシー及び手続に準拠して是正措置が実施される。 全てのインシデントは、解決するまで運用管理者によって追跡される。 終了したインシデントは、適切な解決のために運用要員によりレビューされる。
目的達成のために利用されるシステム構成要素関連の規準	
3.11　データ分類のポリシーに従ってデータ分類をし、必要に応じて、それらの分類の定期的なモニタリングと更新を行う手続が存在する。	データオーナーは定義されたセキュリティ要件及びリスク評価に基づいて、データアクセスルールを定期的にレビューし、修正を要求する。 新しいデータが補足又は生成された場合はいつでも、そのデータはセキュリティポリシーに基づいて分類される。 データ分類の適正性は、変更管理プロセスの一部として考慮される。
3.12　システム可用性及びそれと関連するセキュリティポリシーへの遵守性違反が直ちに対処され、是正措置がタイムリーに取られる手続が存在する。	全てのインシデントは解決するまで経営者によって追跡される。 終了したインシデントは適切な解決のために経営者によってレビューされる。

規準	内部統制の例
	内部監査プロセスは、発見事項に対する行動計画の作成と終了するまでの行動計画の追跡を含んでいる。
3.13　システム基盤とソフトウェアの設計、調達、導入、設定、修正と管理は、定義されたシステム可用性及びそれと関連するセキュリティポリシーと整合している。	企業は、コンピュータ化された情報システムの開発、調達、導入、維持及び関連する技術を管理する公式なシステム開発ライフサイクル（SDLC）方法論を適用している。 SDLC方法論は、下記のフレームワークを含んでいる。 ・　ユーザーニーズに基づいて、パフォーマンスレベルとシステム可用性要件を確立すること。 ・　ユーザー要件に従って企業のバックアップと災害復旧計画プロセスを保持すること。 ・　セキュリティ損失のビジネス影響度の評価に基づいて、確立されたデータ分類と標準的なユーザープロファイルの生成に関すること。ユーザーは、必要性と職務上の実施責任に基づいて、標準的なプロファイルを割り当てられる。 ・　システムパフォーマンスと可用性に不利な影響を及ぼすリスクを最小にするために、システム構成要素に対する変更をテストすること。 ・　変更の導入前の復帰（バックアウト）計画の開発 セキュリティ管理チームは、新しいシステム開発及び調達について、企業の関連するセキュリティポリシーとの整合性を保証するために、アーキテクチャと設計仕様書をレビューして承認する。 システム処理パフォーマンス、可用性とセキュリティに影響を与えるかもしれないシステム構成要素に対する変更は、セキュリティ管理チームの承認を必要とする。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。結果と改良のための改善勧告が経営者に報告される。
3.14　可用性とセキュリティに影響を与えているシステムの設計、開発、導入、運用に関して責任がある要員が、彼らの責任を果たす資格と能力を	企業は、重要な職位のための実施責任と、理論的及び職業的要件を記述した職務記述書を作成している。 雇用手続は、重要な職位の候補者の包括的な審

規準	内部統制の例
持っていることを規定するための手続が存在する。	査、及び証明された資格が提案された職位と見合うか否かという検討を含んでいる。新しい要員が、経歴調査と身元調査の対象となることを条件に雇用される。 内部異動を含めた候補者は、職位の提示前に直属の業務統括者によって承認される。 定期的な業績評価が従業員の直属の上司によって行われる、それには人材育成活動の評価とレビューが含まれる。 要員は、システム可用性概念と諸問題に関する訓練と能力開発を受ける。 休暇又は出張の場合に、重要なシステム可用性とセキュリティ機能のために代替要員を提供するための手続が備わっている。
システム可用性に特有な変更管理関連の規準	
3.15　定義されたシステム可用性及びそれと関連するセキュリティポリシーと整合した環境設定を含めて、システム構成要素を保持する手続が存在する。	企業経営者が、セキュリティ管理の適切性についての第三者意見を受け取って、企業のシステムとWebサイトをホストしているサービスプロバイダから契約（SLA）に従い受け取るパフォーマンスのレベルを定期的に評価する。 ＩＴ部門は、全てのソフトウェアとそれぞれのレベル、適用されたバージョンとパッチの最新のリストを保持する。 システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知らされる。 要員確保、システム基盤とソフトウェア要件が定期的に評価され、資源が企業の可用性と関連するセキュリティポリシーに整合して割り当てられる。 システム構成は毎年テストされ、企業の処理パフォーマンス、可用性とセキュリティポリシーと最新のSLAに対して評価される。逸脱事項報告書が作成されるとともに、改善計画が作成され追跡される。

規準	内部統制の例
3.16　承認され、テストされ、文書化されたシステム変更だけが行われる手続が存在する。	システム変更の承認、テスト、開発、導入の各職務は、分離されている。 企業の文書化されたシステム開発方法論は、プロセスに埋め込まれた基準と内部統制と同様に、変更着手、ソフトウェア開発と保守及び承認プロセスが含まれる。これらはプログラミング、文書化、テストの基準を含む。 システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況と終了について知らされる。 システム基盤とソフトウェアに対する変更は、本番への導入前に、別の開発・テスト環境で開発され、テストされる。 変更管理ポリシーと手続の一部として、「本番移行」プロセス（例えば、「テスト」から「移行」「本番」まで。）がある。本番への移行に際しては、変更の予算を持つ業務責任者とコンピュータ運用の管理者の承認を必要とする。 変更が重要なシステム構成要素に行われるとき、重要な中断に備えて、作成された「復帰（バックアウト）」計画がある。
3.17　緊急変更が文書化され承認されること（事後承認を含む。）を規定するための手続が存在する。	システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知らされる。 標準手続からの逸脱を必要とする緊急変更は、毎日ＩＴ管理者によってログを採取されレビューされ、直属の業務統括者に報告される。恒久的是正措置は、企業の業務統括者の承認を含む変更管理プロセスに従う。
4.0　モニタリング：企業は、システムをモニターして、定義されたシステム可用性ポリシー、目的と基準との遵守性を保持するための行動を取る。	
4.1　システム可用性とセキュリティパフォーマンスが定期的にレビューされ、定義された	ネットワークのパフォーマンス及びシステム処理が社内の運用スタッフによって24時間休みなくシステムモニタリングツールを使ってモニターさ

規準	内部統制の例
システム可用性及びそれと関連するセキュリティポリシーと比較される。	れる。ネットワークのパフォーマンス、システム可用性とセキュリティインシデントの統計と承認された目標との比較が、蓄積され、月次のＩＴ運営委員会に報告される。 顧客サービスグループは、システム可用性とそれに関連する顧客の苦情をモニターする。それは改善のための提案と一緒にこのような事項の月次報告書を提供し、それは月次のＩＴ運営委員会のミーティングにおいて考慮され、実行される。 情報セキュリティチームは、内製の又は一般に利用可能なツールを使ってシステムをモニターし、脆弱性を評価する。潜在的リスクが評価され、SLAと企業のその他の義務と比較される。改善計画が提案され、実施がモニターされる。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。内部監査部門は、年度の監査計画の一部として、処理のインテグリティとシステムセキュリティレビューを行う。結果と改善のための提案が経営者に報告される。
4.2　定義されたシステム可用性及びそれと関連するセキュリティポリシーに従った目的を達成するために、企業の現行の能力の潜在的な劣化を識別して、対処するプロセスがある。	ネットワークのパフォーマンス及びシステム処理が社内の運用スタッフによって24時間休みなくシステムモニタリングツールを使ってモニターされる。ネットワークのパフォーマンス、システム可用性とセキュリティインシデントの統計と承認された目標との比較が、蓄積され、月次のＩＴ運営委員会に報告される。 年次ＩＴ計画と予算編成プロセスの一部として、将来のシステム処理のパフォーマンス、可用性と性能要件が見積もられ、分析される。 システムセキュリティ目的を達成する企業の能力への潜在的な影響を与えるかもしれない傾向を識別するために、人的又は自動化ツールによってログを分析する。 月次のＩＴスタッフ会議が、システムのパフォーマンス、可用性、性能、セキュリティ上の問題と傾向に対処するために開催される。発見事項が年４回の経営会議において検討される。
4.3　環境、規制、技術の変更がモニターされ、それらのシス	企業のデータセンター施設は気候と環境のモニタリング装置を含む。最適なパフォーマンス範囲

規準	内部統制の例
テム可用性とセキュリティ上の影響が適時に評価され、その評価に基づきポリシーが更新される。	からの逸脱は上申され、解決される。 上級経営者が、年度のＩＴ計画プロセスの一部として、企業のシステム可用性及びそれに関連するセキュリティポリシー上に適用される法規制の影響と技術開発を考慮する。 企業の顧客サービスグループは、新規技術、顧客要件と競争的な活動の影響をモニターする。

処理のインテグリティ原則と規準

24. 処理のインテグリティ原則は、システム処理の完全性、正確性、正当性、適時性と承認に関係する。もしシステムが、未承認、又は不注意な操作がなく、損なわれない方法で意図された機能を実施するなら、処理のインテグリティは存在している。完全性は、一般に全ての取引とサービスが処理され、又は例外なく実施されることを示している。正当性は全ての取引とサービスが複数回処理されないこと、及びそれらがビジネスの価値と期待に従っていることを示している。正確性は、提出された取引と結び付けられた重要な情報が取引の処理を通じて正確なままであり、又は取引やサービスが意図されたように処理され、又は実施されることを示している。サービスの提供又は商品の引渡しの適時性は、そのような提供のために行われるコミットメントという流れで扱われる。承認は、システム処理を管理しているポリシーによって定義された必要な許可と権限に従って処理が実施されるということを示している。

25. 処理のインテグリティと関連するリスクは、取引を開始した当事者が求められた特定の要求に従って、取引が完結したり、正確にサービスが提供されたりしないということである。適切な処理のインテグリティの内部統制がなければ、買い手は商品を受け取れなかったり、本来依頼した以上の商品又はサービスを受け取ったり、間違った商品又はサービスを受け取るかもしれない。しかしながら、もし適切な処理のインテグリティ管理が存在して有効に運用されているなら、買い手は情報、商品又はサービスを正しい価格・数量・期日で受け取る可能性が高い。処理のインテグリティは業務の主題である製品又はサービスに関連する情報を開始、記録、処理及び報告する手続を含めてシステム構成要素の全てを対象としている。電子商取引システムでのデータ入力の性質は、他のシステムのそれとは顕著に異なっており、多くの場合Webで可能となった入力画面又はフォーム上に直接にユーザーが入力したデータを含んでいる。このデータ入力プロセスの違いのために、電子商取引システムで入力されたデータの完全性と正確性に対する内部統制の性質は、他のシステムとはある面で異なっているかもしれない。下記のパラグラフ27で概説された内部統制の例は、これらの相違の幾つかを識別している。

26. 処理のインテグリティはデータのインテグリティとは違う。処理のインテグリティは自動的にシステムによって保管された情報が完全で、正確で、最新で、承認されていることを意味しない。もしシステムがシステムの境界線の外の源泉からの入力情報を処理するなら、企業は処理のために、提出された情報の完全性、正確性、承認と適時性に対して、限られた内部統制しか確立できない。社外のサイトにおい

て情報及び内部統制手続にもたらされるエラーは、多くの場合企業の内部統制の埒外である。業務を定義するシステム記述において明確に含まれているシステムにより当該情報が保存されている場合でさえ、高いデータインテグリティを示すことなしに当該システムは高い処理のインテグリティを示す可能性がある。例えば、システムに保存された住所がシステムに追加される場合は、全ての適切なエディットチェック及び他の適切なコントロールを通過するが、それはもはや（人又は企業が移転している場合には）最新ではないかもしれないし、（住居番号又は郵送先が住所から漏れている場合には）完全ではないかもしれない。

処理のインテグリティ原則と規準の表
27．システム処理は完全、正確、タイムリーかつ承認されている。

規準	**内部統制の例**
システム処理は完全、正確、タイムリーかつ承認されている。	
1.0　ポリシー：企業は、システムの処理のインテグリティのためにポリシーを定義して、文書化している。	
1.1　企業の処理のインテグリティ及びそれと関連するセキュリティポリシーは、特定の個人又はグループによって確立され、定期的にレビューされ、承認されている。	処理のインテグリティに関する文書化されたポリシーは、経営会議により承認されており、企業全体に適用されている。 定期的なリスク評価プロセスの一部として、経営者は、新たなアプリケーションやインフラ又はそれらの重要な変更、新たな環境のリスク、規制や基準の変更、SLAその他の文書に基づくユーザー要求の変更などに基づいてＩＴリスク評価の変更を識別する。その後、経営者はＩＴリスク評価に基づいてポリシーを更新する。 ユーザー要件がSLA又はその他の書類で文書化されている。 ポリシーの変更は、適用前に経営主導層（leadership）によって承認される。
1.2　企業のシステム処理のインテグリティ及びそれと関連するセキュリティポリシーは、下記の事項を含むが、それらに制限されない。 a．承認されたユーザーのシステム処理のインテグリティと関連したセキュリティ要件の識別と文書化 b．重要性、機微性（Sensitivity）に基づくデータの分類。分類は保護の必要性、アクセス権限、アクセス制限、維持と廃棄	（本規準の内部統制の例は、企業の文書化された処理のインテグリティ及びセキュリティポリシーであり、左記に列挙された要素を含んでいる。処理のインテグリティ及びセキュリティポリシーの例示は省略する。）

規準	内部統制の例
を定義するのに用いられる。 c. 定期的なリスク評価 d. 未承認のアクセスの防止 e. 新規ユーザーの追加、既存ユーザーのアクセスレベルの変更及びアクセスする必要のなくなったユーザーの削除 f. システム処理のインテグリティ及びそれと関連するセキュリティに対する実施責任と説明責任の割当て g. システム変更と維持管理に対する実施責任と説明責任の割当て h. 導入前のシステム構成要素のテスト、評価、承認 i. システム処理のインテグリティ及びそれと関連するセキュリティ問題に関連している苦情と要請がどのように解決されるか。 j. システム処理のインテグリティ及びそれと関連するセキュリティ違反、エラー、欠落その他のインシデントを処理するための手続 k. システム処理のインテグリティ及びそれと関連するシステムセキュリティポリシーをサポートする訓練等に必要な経営資源を配分するための規定 l. システム処理のインテグリティ及びそれと関連するシステムセキュリティポリシーで明示的に扱われない逸脱事項と状況の取扱いのための規定 m. 適用される法規制、定義されたコミットメント、SLAの識別と一致のための規定	
1.3 企業のシステム処理のインテグリティ及びそれと関連す	経営者は、個々の経営メンバーに、企業の処理のインテグリティ及びそれと関連するセキュリテ

規準	内部統制の例
るシステムセキュリティポリシーの開発・維持及びそれらのポリシーの変更・更新に関わる実施責任と説明責任が割り当てられている。	ィポリシーの施行に関する責任を割り当てている。経営会議のうち上記以外の者が、経営会議ハンドブックに示されたポリシーのレビュー、更新と承認について支援する。
2.0　コミュニケーション：企業は、責任ある当事者と承認されたユーザーに文書化されたシステム処理のインテグリティポリシーを伝達している。	
2.1　企業は、システムの記述とその範囲を客観的に定義して、承認されたユーザーに伝達している。 　もしシステムが電子商取引システムであるなら、Webサイト上に提供された追加の情報には下記の事項を含むが、それらに制限されない。 a．該当する場合、提供される商品又はサービスの以下を含む状況の説明 ・　商品の状態（新品か、中古か、修理品か。） ・　サービス（又はサービス契約）の記述 ・　情報源（何処で得られ、どのように変換されたか。） b．電子商取引を行う条件及び要件。下記の事項を含むが、それらに制限されない。 ・　取引（取引とは、商品が販売される場合は注文の履行を、サービスが提供される場合はサービスの提供の履行を意味する。）の完了のためのタイムフレーム ・　注文又はサービス依頼の通常の処理に対する逸脱事項を顧客に通知するタイムフレームとプロセス ・　該当する場合、顧客選択権を含む、通常の商品又はサービスの提供の方法	電子商取引システムのために、企業はWebサイト上にシステム記述を開示している。電子商取引システムのためのシステム記述と追加の開示例については、付録Ａを参照のこと。 　電子商取引でないシステムのために、企業は承認されたユーザーにシステム記述を提供している。電子商取引でないシステムのためのシステム記述については付録Ｂを参照のこと。

規準	内部統制の例
・　該当する場合、顧客選択権を含む支払条件 ・　電子決済実務及びそれに関連する顧客への請求 ・　該当する場合、顧客はどのように請求をキャンセルできるか。 ・　該当する場合、商品返品ポリシー又は責任の制限 c．顧客が購入した商品及びサービスに対する保証、修理サービス、サポートを得ることができるWebサイト上の場所 d．処理のインテグリティに関係している問題の解決のための手続。これらは、製品及びサービスの品質、正確性、完全性と関係がある苦情や、このような苦情の解決の失敗に関連する苦情など、電子商取引のあらゆる部分に関連している。	
2.2　ユーザーの処理のインテグリティ及びそれと関連するセキュリティ義務と、企業のユーザーへの処理のインテグリティ及びそれと関連するセキュリティコミットメントは、承認されたユーザーに伝達されている。	企業の処理のインテグリティに関連するセキュリティコミットメントと要求される処理のインテグリティに関連するセキュリティ義務は、顧客及び他の外部ユーザーに対して、企業のWebサイト上に、又は企業の標準サービスアグリーメントの一部として掲示されている。 内部のユーザー（従業員と外部委託先）のために、企業の、処理のインテグリティに関連するセキュリティポリシーは、オリエンテーションの一部として新しい従業員と外部委託先にレビューされる。ポリシーの重要な項目と従業員への影響は検討される。新しい従業員はポリシーを読んで、理解して、従うことを示している誓約書に署名しなくてはならない。毎年、彼らのパフォーマンスレビューの一部として、従業員が企業の処理のインテグリティとセキュリティポリシーの理解とそれへの遵守性を再確認しなくてはならない。外部委託先の義務が契約で詳述される。 セキュリティ周知プログラムが、従業員に企業の処理のインテグリティ及びそれと関連するセキ

規準	内部統制の例
	ュリティポリシーを伝達するために実施されている。 企業は、企業のイントラネット上にＩＴセキュリティポリシーを公開する。
2.3　企業のシステム処理のインテグリティに関連するセキュリティポリシーとそれらのポリシーに対する変更・更新のための実施責任と説明責任が、それらを実施することに責任がある企業の要員に伝達されている。	経営者が最高運営責任者（COO）に企業の処理のインテグリティポリシーの実施に対する責任を割り当てる。 セキュリティ管理チームは、企業のセキュリティポリシーの日々の維持について義務と責任があり、そして、最高情報責任者（CIO）及びＩＴ運営委員会に変更について提言する。 処理のインテグリティ及びそれに関連するセキュリティコミットメントが、年次のＩＴ計画プロセスの一部として、顧客口座管理者によりレビューされる。 文書化された職務記述が定義され、セキュリティ管理チームに伝達されている。 全ての定義されたセキュリティプロセスの文書化されたプロセス及び手続マニュアルが、セキュリティ管理チームの要員に提供される。セキュリティ責任者はセキュリティポリシーの変更に基づいてプロセス及び手続マニュアルを更新する。
2.4　システム処理のインテグリティ問題、エラーと欠落とシステムセキュリティの違反について、企業に通知し、サポートを受けるプロセス、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	顧客と外部のユーザーが潜在的な処理のインテグリティ問題、セキュリティ違反と他のインシデントを企業に知らせるプロセスは、企業のWebサイト上に開示されるか、又は新規ユーザーの手引書の一部として提供されている。 企業のユーザー訓練とセキュリティ周知プログラムは、処理のインテグリティ問題、潜在的なセキュリティ違反の識別、セキュリティ管理チームに知らせるプロセスに関する情報が含まれている。 システム処理のインテグリティ問題、セキュリティ違反その他のインシデントの識別と上申のための文書化された手続が存在している。
2.5　システム処理のインテグリティとシステムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されてい	システム構成要素に対する計画された変更とそれらの変更のスケジューリングは、月次のＩＴ運営委員会のミーティングの一部としてレビューされる。

規準	内部統制の例
る。	システムセキュリティに影響を与えるかもしれないシステム構成要素に対する変更は、変更の導入前に管理者及びセキュリティ管理チームと変更依頼者の承認を必要とする。 顧客及びユーザーと彼らの処理のインテグリティ及び関連するセキュリティ義務、又は企業の処理のインテグリティ及び関連するセキュリティコミットメントに影響を与えるかもしれない変更が、企業のWebサイト上に強調して掲示される。 処理のインテグリティ及び関連するシステムセキュリティに影響を与えるかもしれない変更が、提案された変更の導入前に標準サービスアグリーメントの規定において影響を受ける顧客によってレビューされて、承認される。 システムセキュリティに影響を与える要素を含む変更の定期的なコミュニケーションがある。 システムセキュリティに影響を与える変更が、企業の進行中のユーザー訓練とセキュリティ周知プログラムに取り入れられている。
3.0 手続：企業は、定義されたシステム処理のインテグリティポリシーに従って文書化されたシステム処理のインテグリティ目的を達成するために手続を導入している。	
3.1 (1)処理のインテグリティのコミットメントを損なうシステム運用の中断の潜在的脅威の識別、(2)識別された脅威に関連するリスクの評価、のための手続が存在する。	リスク評価が定期的に実施される。このプロセスの一部として、処理のインテグリティへの脅威が識別され、これらの脅威から生じるリスクが公式に評価される。 経営者が評価された脅威に基づき、プロセスと手続を修正する。
3.2 入力の完全性、正確性、適時性と承認に関連する手続は、文書化されたシステム処理のインテグリティポリシーと整合している。 もしシステムが電子商取引システムである場合、企業の手続には下記の項目が含まれるが、それらに制限されない。 a. 企業は、正確性と完全性のために、それぞれの要求又は取引をチェックする。	企業は、ユーザー部門が実施すべきデータ作成手続を確立している。 データ入力画面は、フィールド誤謬摘示チェック、リミットチェックを含んでおり、入力フォームはエラーと欠落を減らすように設計されている。 証憑は、入力前に適切な承認のためにレビューされる。 エラーと逸脱事項を発見、報告、修正することを保証するために、データ作成中にエラー取扱手

規準	内部統制の例
b. 積極的な通知が、取引が処理される前に、顧客から受け取られる。	続が準拠される。 原始証憑は、最低７年間、少なくとも法律上の要件を満たすために、データの復旧又は再生を容易にするイメージ管理システム上に保持される。 論理的アクセスコントロールがデータ入力機能を承認された要員に制限する（このセクションの3.6参照）。 顧客口座管理者は、顧客の苦情、注残記録、他の取引分析の定期的なレビューを行う。この情報は顧客サービスアグリーメントと比較される。 企業は、以下を含む多様な手法を用いて、伝送中及び転送中の情報を未承認のアクセス、改竄、誤転送から保護する。 ・　転送情報の暗号化 ・　バッチヘッダー及びコントロールトータル照合調整 ・　メッセージ認証コード及びハッシュトータル ・　承認されたユーザーの接続を専用線又はVPNで行うこと。 ・　相手先固定接続と耐タンパー性のあるパッケージ Webベースの入力の特質のため、規準3.1を達成するための内部統制の性質が、下記のようにある面で異なっていることがある。 ・　成功したログイン後のアカウント使用状況は、業界標準の暗号化ソフトウェアで暗号化されている。 ・　Webスクリプトには無効な入力のエラーチェックが含まれている。 ・　企業の注文処理システムは、処理の前に情報の正確性と完全性をチェックするためのそれぞれの注文に適用される誤謬摘示、検証、リミットチェックを含んでいる。 ・　企業によって取引が処理される前に、意図された注文を確認するように要求を示され、顧客は、「はい、この注文を処理してください」ボタンをクリックするように要求される。 企業は、顧客によって提供された電子メールア

規準	内部統制の例
	ドレスに注文確認の電子メールを出す。注文確認はオンラインの顧客注文追跡サービスとリンクした注文明細、出荷と配送情報とを含んでいる。戻って来た電子メールは顧客サービス係によって調査される。
3.3　システム処理の完全性、正確性、適時性と承認が、エラー訂正とデータベース管理を含めて、文書化されたシステム処理のインテグリティポリシーと整合している。 　もしシステムが電子商取引システムである場合、下記の手続が含まれるが、それらに制限されない。 a．正しい商品が同意された時間内に、正しい数量で出荷され、又は依頼どおりにサービスと情報が顧客に提供される。 b．取引逸脱事項が顧客に即座に伝達される。 c．受信されたメッセージが処理され、正確に、完全に正しいＩＰアドレスに送信される。 d．送信されるメッセージが処理され、正確に、完全にサービスプロバイダ（ＳＰ）のインターネット・アクセスポイントに伝送される。 e．ＳＰのネットワークセグメント内で伝送中である間に、メッセージが変更されることがない。	注文処理、クレジットの適用と現金受領、在庫の保護、ユーザーアカウント管理とデータベース管理に対する責任は分離されている。 企業の文書化されたSDLC方法論は、新規アプリケーションの開発と既存アプリケーションの保守に使われる。方法論は、システム処理のインテグリティ機能の、ユーザー参画、テスト、変換と管理者の承認のため必要とされる手続を含んでいる。 コンピュータ運用とジョブスケジューリング手続が存在し、文書化され、システム処理のインテグリティ目的、ポリシー及び基準に関して運用要員のための手続と指針を含んでいる。逸脱事項は管理者、コンピュータ運用チームの承認を必要とする。 企業のアプリケーションシステムは不完全又は不正確なデータをチェックするために、誤謬摘示・検証ルーチンを含んでいる。エラーは、ログを採取され、調査され、修正され、入力のために再提出される。管理者は、エラーがタイムリーに修正されることを保証するために、毎日エラーログをレビューする。 「日次終了」照合調整手続は、出力記録の数と処理された記録の数と受け入れられた記録の数の照合調整を含んでいる。 企業の電子商取引システムに含まれた追加の内部統制は下記のとおり。 ・　荷札が顧客の受注から作られ、倉庫スタッフによって注文が梱包されるようにチェックされる。 ・　期待された提供スケジュールに確実に合致する運送業者の配送方法が使われる。運送業者のパフォーマンスがモニターされて、定期的に評価される。 ・　サービス提供目標が保持され、提供された実際のサービスが当該目標に対して監視される。

規準	内部統制の例
	・　企業は、サービスの完結又は情報の提供での、顧客満足を確認するために、顧客にフィードバックアンケートを使う。 ・　コンピュータ化された注残記録が保持され、24時間以内に注残の顧客に通知するよう意図される。顧客は、発注をキャンセルするか、又は代替項目が提供されるようにする選択権を与えられる。 ・　モニタリングツールが待ち時間、パケット損失、中継回数及びネットワークパフォーマンスを継続的にモニターするために使われる。 ・　組織はネットワークインテグリティソフトウェアを保持して、ネットワーク管理ポリシーを文書化する。 ・　適切に文書化された上申手続が好ましくないネットワークパフォーマンスに是正措置を起こすために備わっている。
3.4　出力の完全性、正確性、適時性と承認に関連する手続は文書化されたシステム処理のインテグリティポリシーと整合している。 　もしシステムが電子商取引システムである場合、手続には下記の項目が含まれるが、それらに制限されない。 ・　取引を処理する前に、企業は顧客に販売価格と全ての他の経費及び料金を表示する。 ・　取引が同意したように請求され、電子的に決済される。 ・　請求又は決済エラーが即座に修正される。	システム処理のインテグリティ目的、ポリシーと基準に従う出力情報の配布のための文書化された手続が存在する。 　管理作業員が毎日、システム全体及び個別顧客ごとに出力情報件数と取引入力件数のコントロールトータルを照合調整する。逸脱事項はログを採取され、調査され、解決される。 　顧客サービス部門は、顧客の電話と苦情を日誌に記録する。顧客電話の分析、苦情、注残記録その他の取引分析及び企業の処理のインテグリティのポリシーとの比較が月次の経営会議においてレビューされ、必要に応じて行動計画が作成され、実施される。 　企業の電子商取引システムに含まれた追加的内部統制は下記のとおり。 ・　税金、送料、関税、利用通貨を含む全ての経費が顧客に表示される。注文が処理される前に、顧客が「はい」をクリックすることによって、注文を承諾する。 ・　顧客は、注文が処理される前に、将来の検証のために、注文に関する全ての情報（注文された品目、販売価格、経費、売上税、送料など）を詳述した（クレジットカード文書のような）支払記録が付いた「注文確認」を印刷する選択権を有している。

規準	内部統制の例
	・　外貨建取引を行う前に、全ての外国為替レートは顧客に表示される。 ・　請求処理又は決済のエラーが顧客によって報告されてから、24時間以内にフォローアップされ、修正される。
3.5　入力源泉から最終の性質まで情報入力の追跡（逆もまた然り。）を可能にする手続が存在する。	取引の入力においては、システムにより日時が記録され、かつ、入力源泉の識別子（名前、端末、ＩＰアドレス）も記録されている。 各注文には、注文及び、関連した出荷と支払決済情報へのアクセスに使えるユニークな識別子が入っている。この情報には、顧客名と注文、出荷又は請求処理の日付によってもアクセスできる。 企業は、最低10年間、取引履歴を保持する。注文履歴情報が３年間オンラインで保持され、顧客サービス担当者によりすぐにアクセス可能である。３年後に、この情報はオフラインの記憶装置で保持される。 原始証憑は最低７年間、法律上の要件を満たすために、データの復旧又は再生を容易にするため、イメージ管理システム上に保持される。 企業は、外部保管施設において保管されたテープの年次監査を行う。監査の一部として、外部保管の場所におけるテープが適切なテープ管理システムと照合される。
システム処理のインテグリティに特有のセキュリティ関連の規準	
3.6　定義されたシステムの論理的アクセスを制限するための手続が存在する。下記の事項を含むが、それらに制限されない。	
a．公にすべきでない情報に対する論理的アクセスセキュリティ対策	・　公にすべきでない情報資源への論理的アクセスは、ＯＳ固有のセキュリティ、アプリケーション及び資源固有のセキュリティ、追加的なセキュリティソフトウェアの利用を通じて保護される。 ・　資源に特有な、又は初期的なアクセスルールは、全ての公にすべきでない資源について定義される。 ・　資源へのアクセスは、ユーザーの身元に基づいて認証されたユーザーに付与される。
b．承認されたユーザーの識別と認証	・　ユーザーは、関連するパスワードで認証された正しいユーザーＩＤの利用を通じて公にされ

規準	内部統制の例
	ていない資源にアクセスしようとする場合、企業のネットワークとアプリケーションシステムに対して身元を明らかにしなければならない。 ・　ユニークなユーザーＩＤが個別のユーザーに割り当てられる。 ・　グループ又は共有ＩＤは十分なリスク評価と共有ＩＤを利用するビジネスユニットのマネージャの文書による承認がないと利用できない。 ・　パスワードは大文字と小文字を区別し、少なくとも８文字で、そのうち１文字は英数字でない文字を含んでいなくてはならない。 ・　セキュリティ設定のパラメータにより、パスワードは90日ごとに更新されるよう強制される。 ・　ログインを３回失敗するとログインできなくなる。
c．新規ユーザーの登録と承認	・　顧客は、企業のWebサイト上で、新規ユーザー情報を提供し、適切なユーザーＩＤとパスワードを選ぶセキュアなセッションの下において、自己登録することができる。自己登録された顧客口座と結び付けられた権限及び権限付与が、特定の制限されたシステム機能を提供する。 ・　ユーザーとユーザーアクセス権限（制限された「顧客口座」としての機能性を除く。）を生成又は修正する権限は、セキュリティ管理チームに限定される。 ・　直属の業務統括者は、従業員と外部委託先のアクセス権変更のリクエストを承認する。制限された資源へのアクセスは資源の所有者（リソース・オーナー）によって承認される。 ・　自己登録の間に与えられたデフォルト権限を超えた顧客アクセス権は、顧客口座管理者によって承認される。 ・　適切な職務分離が権限を与える際に考慮されている。
d．ユーザープロファイルに対する変更と更新のプロセス	・　自己登録の顧客口座に対する変更と更新は、ユーザーが成功裏にシステムにログインした後、企業のWebサイト上でいつでも個別のユーザーによって可能となる。変更は即時に反映される。 ・　使われていない顧客口座（６か月間不使用）がシステムによって排除される。 ・　他のアカウントとプロファイルに対する変更は、セキュリティ管理チームに制限されていて、直属の業務統括者、顧客口座管理者の承認を要求する。

規準	内部統制の例
e．承認されたユーザーに制限されたアウトプット配布	・　人事管理システムが新たに退職した従業員のリストを毎週人事部に提供する。このリストはアカウント失効のためにセキュリティ管理チームに送られる。 ・　コンピュータが処理したアウトプットへのアクセスは、承認された人にだけ、情報の分類に基づいて提供される。 ・　処理されたアウトプットは、その情報の分類を反映した領域に保存される。
f．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アクセスの制限	・　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アクセスは、コンピュータ運用スタッフに制限される。
g．システム構成、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とセキュリティ装置（例えば、ファイアウォール）に対するアクセスの制限	・　ハードウェアとオペレーティング・システム設定テーブルは、適切な要員に制限されている。 ・　アプリケーションソフトウェアの設定テーブルは、承認されたユーザーに制限されており、アプリケーション変更管理ソフトウェアのコントロール下にある。 ・　データ又はプログラムを、閲覧、追加、変更、削除できるユーティリティプログラムは、承認された技術サービススタッフに制限されている。その使用は、コンピュータ運用の管理者によってログを採取され、モニターされる。 ・　CIO指揮下の情報セキュリティチームは、全ての記憶装置メディアへのアクセスはもちろん、ファイアウォールその他のログへのアクセスも保持する。いかなるアクセスもログを採取されて、企業のＩＴポリシーに従ってレビューされる。 ・　全てのマスターパスワードのリストが暗号化されたデータベースに保存され、副本が企業の金庫に封印された封筒で保持される。
3.7　定義されたシステムへの物理的アクセスを制限するための手続が存在する。施設、オフライン記憶媒体、バックアップ媒体とシステム及びファイアウォール、ルータ、サーバーのような他のシステム構成要素を含むが、それらに制限されない。	企業のＩＴ資源、サーバー及びファイアウォールとルータなどの関連するハードウェアを収容するコンピュータ室への物理的なアクセスが、カードキーシステムによって承認された個人に制限され、ビデオ監視装置によって監視される。 物理的アクセスカードがビル警備によって管理される。アクセスカードの使用実績が日誌に記録される。記録はビル警備によって保持され、レビューされる。 企業のコンピュータ施設への物理的なアクセス

規準	内部統制の例
	権のリクエストは、コンピュータ運用管理者の承認を必要とする。 潜在的セキュリティ違反の識別と上申についての文書化された手続が存在する。 外部保管バックアップデータと媒体がサービスプロバイダ施設において保存される。外部保管データと媒体へのアクセスはコンピュータ運用管理者の承認を必要とする。
3.8　システム資源への未承認のアクセスから保護するための手続が存在する。	ログインセッションは、３回のログイン失敗の後に終了させられる。 VPN（仮想専用ネットワーク）ソフトウェアが、承認されたユーザーによるリモートアクセスを認めるために使われる。ユーザーが特定の「クライアント」ソフトウェアとユーザーＩＤ及びパスワードを通してVPNサーバーによって認証される。 ファイアウォールが使われて、未承認のアクセスを阻止するように設定される。ファイアウォールの状況はログが採取され、セキュリティ管理者によって毎日レビューされる。 不必要なネットワークサービス（例えば、telnet、ftp、http）は企業のサーバー上で無効とされる。必要とされ承認されたサービスのリストがＩＴ部門によって保持される。このリストは、最新の運用状況における適切性の観点から定常的に企業の管理者によってレビューされる。 企業のネットワークの継続的モニタリングと、潜在的セキュリティ違反の初期段階での識別を提供するために侵入検知システムが使われる。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。結果と改良のための改善勧告が経営者に報告される。
3.9　コンピュータ・ウィルス、悪意があるコードと未承認のソフトウェアによる感染から保護するための手続が存在する。	他のセキュリティモニタリングに関連して、セキュリティ管理チームは、ユーザー・グループに関与して、コンピュータ・ウィルスに関するサービスに加入する。 送られてくる電子メールメッセージのウィルススキャンを含むアンチウィルスのソフトウェアが備わっている。パターンファイルは都度更新され

規準	内部統制の例
	る。 発見されたいかなるウィルスもセキュリティチームに報告され、全てのユーザーにそれらの潜在的ウィルス脅威を周知するために警告がなされる。 ＯＳやその他のシステムプログラムをインストール、変更、リプレースする権限は、承認された要員に制限されている。 スーパーユーザー機能及び取扱いに細心の注意を要するシステム機能に対するアクセスは、承認された要員に制限されている。
3.10　インターネット又は他の公衆網上を通過するユーザー認証情報と伝送を保護するため、暗号化又は他の同等のセキュリティ技術が利用される。	企業は、公衆網上でのユーザーＩＤとパスワードを含む個人情報又は機密情報の送信のために、業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を利用する。潜在的セキュリティ問題を回避するためセキュリティ管理チームによってテストされて、使用に当たって承認された最新のバージョンへブラウザを更新するようにユーザーは要求される。 アカウント使用状況はログイン成功後に業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を通して暗号化される。ユーザーは、要求すればすぐに（Webサイト上の「サインアウト」ボタンを選択することによって）、又は10分間使用しないとログアウトされる。
目的達成のために利用される実行及びインシデント管理関連の規準	
3.11　システム処理のインテグリティ問題と関連するセキュリティ違反その他のインシデントを識別して、報告して、行動を起こすための手続が存在する。	ユーザーには、システム処理のインテグリティ問題と潜在的セキュリティ違反をＩＴホットラインへ伝達するための指針が提供される。処理のインテグリティ問題がコンピュータ運用の管理者に上申される。情報セキュリティチームは、顧客ホットラインと電子メールを通して報告されたセキュリティ関連のインシデントを調査する。 本番稼動及び自動化されたバッチジョブスケジューラーのログが毎朝レビューされ、処理上の問題を識別、上申、解決される。 侵入検知システムとその他のツールが潜在的セ

規準	内部統制の例
	キュリティ違反とその他のインシデントを識別し、ログを採取し、報告するために使われる。システムは進行中の潜在的インシデントについて、電子メールと文書によってネットワーク管理者と情報セキュリティチームに通知する。 インシデントログが情報セキュリティチームによって毎日モニターされ、評価される。 インシデントが発見又は報告された場合、承認された要員により、定義されたインシデント管理プロセスが開始される。定義されたポリシー及び手続に準拠して是正措置が実施される。 手続は、定義されたインシデントの上申プロセス及び通知体制を含んでいる。 全てのインシデントは、解決するまで経営者によって追跡される。 終了したインシデントは、適切な解決のために経営者によりレビューされる。 セキュリティに関連しないインシデントの解決には、インシデントとその解決がセキュリティ要件に与える影響を考慮することが含まれている。
目的達成のために利用されるシステム構成要素関連の規準	
3.12　データ分類のポリシーに従ってデータ分類をし、必要に応じて、それらの分類の定期的なモニタリングと更新を行う手続が存在する。	企業にデータの品質保証機能がある。 データ品質保証グループは、データの利用状況をレビューし、検索情報が文書化されていることを確かめる。検索情報は下記の事項を含むが、それに限定されない。 a. 目的 b. 組織内、組織外におけるデータのソース元、所有権 c. 利用者 d. 管理者、責任者 e. 適用される基準 f. セキュリティ、プライバシー目的の分類 g. アクセス権限 h. （検索のための）所在地 i. バージョン j. タイムスタンプ k. 保持、破棄の要件 l. ソース：所有者、責任者、系統、監査証跡

規準	内部統制の例
	m. 保証 新しいデータが補足又は生成された場合はいつでも、そのデータはセキュリティ及び処理のインテグリティポリシーに基づいて分類される。 データ分類の適性性は、変更管理プロセスの一部として考慮される。
3.13 システム処理のインテグリティ及び関連するセキュリティポリシーへの遵守性違反が直ちに対処され、是正措置がタイムリーに取られる手続が存在する。	企業は、手続がポリシーと整合することを要求し、また、手続がポリシーと整合することをチェックするプロセスが存在する。 企業は、ポリシーの変更をモニターし、それらの変更によって影響を受ける手続の変更を即座に行う。 コンピュータ運用チームのミーティングが前日の処理をレビューするため、毎朝開催される。処理の問題については、是正措置を含めて検討され、必要な場合は追加の行動計画が作成され、実行される。 システム処理問題のレビュー、文書化、上申及び解決のための標準手続が存在する。 企業経営者が、定期的に企業のWebサイトを提供するISPから受け取るパフォーマンスレベルを評価する。この評価は、独立の第三者によるISPが有しているセキュリティ統制の評価によってなされるだけでなく、懸念される要因又はオープンな項目についてのISPの管理者のフォローアップも伴う。 処理のインテグリティに関連するセキュリティ問題が記録されて、問題報告が蓄積される。是正措置が経営者によって記録され、モニターされる。 定常的に、処理のインテグリティに関連するセキュリティポリシー、内部統制、手続が内部監査部門によって監査される。このようなテストの結果が経営者によってレビューされ、回答が用意され、改善計画が実行される。
3.14 システム基盤とソフトウェアの設計、調達、導入、設定、修正と管理は、定義された処理のインテグリティ及び	企業は、コンピュータ化された情報システムの開発、調達、導入、維持及び関連する技術を管理する公式なシステム開発ライフサイクル（SDLC）方法論を適用している。

規準	内部統制の例
関連するセキュリティポリシーに整合している。	SDLC方法論は、システムオーナーの割当て、データ分類に関するフレームワークを含む。プロセスオーナーはユーザー仕様書の開発、ソリューションの選択、テスト、変換と導入に関与している。 セキュリティ管理チームは、新しいシステム開発及び／又は調達について、企業の処理のインテグリティ及び関連するセキュリティ目的、ポリシーと基準との整合性を保証するために、アーキテクチャと設計仕様書をレビューして承認する。 プロセス所有者のレビューとテスト結果の承認及び権限付与は変更の導入に必要とされる。 セキュリティに影響を与えるかもしれないシステム構成要素に対する変更は、セキュリティ管理チームの承認を必要とする。
3.15　処理のインテグリティとセキュリティに影響を与えているシステムの設計、開発、導入、運用に関して責任がある要員が、彼らの責任を果たす資格と能力を持っていることを規定するための手続が存在する。	CIOの監督下にある独立のシステム品質保証グループが設置されている。 企業は、重要な職位のための実施責任と、理論的及び職業的要件を記述した職務記述書を作成している。 雇用手続は、重要な職位の候補者の包括的な審査、及び証明された資格が提案された職位と見合うか否かという検討を含んでいる。新しい要員が、経歴調査と身元調査の対象となることを条件に雇用される。 内部異動を含めた候補者は、職位の提示前に直属の業務統括者によって承認される。 要員の資格及び資源の十分性の評価については、外部委託先の活動も含める。 定期的な業績評価が従業員の直属の上司によって行われる、それには人材育成活動の評価とレビューが含まれる。 要員は、コンピュータ運用、システム設計と開発、テスト及びセキュリティ概念と諸問題に関する訓練と能力開発を受ける。

規準	内部統制の例
	休暇又は出張の場合に、重要なシステムセキュリティ機能のために代替要員を提供するための手続が備わっている。 処理のインテグリティ及びそれに関連するセキュリティ要件に適合した、要員の数及びその他の資源の配分のための手続が備わっている。
システム処理のインテグリティに特有の変更管理関連の規準	
3.16　定義されたシステム処理のインテグリティ及び関連するセキュリティポリシーと整合した環境設定を含めて、システム構成要素を保持する手続が存在する。	企業経営者が、セキュリティ管理の適切性についての第三者意見を受け取って、企業のシステムとWebサイトをホストしているサービスプロバイダから契約（SLA）に従い受け取るパフォーマンスのレベルを定期的に評価する。 ＩＴ部門は、全てのソフトウェアとそれぞれのレベル、適用されたバージョンとパッチの最新のリストを保持する。 システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知らされる。 システム構成は毎年テストされ、企業のセキュリティポリシーと最新のSLAに対して評価される。逸脱事項報告書が作成されるとともに、改善計画が作成され追跡される。 企業は、ポリシーの変更をモニターし、それらの変更によって影響を受ける手続の変更を即座に行う。
3.17　承認され、テストされ、文書化されたシステム変更だけが行われる手続が存在する。	企業の文書化されたシステム開発方法論は、プロセスに埋め込まれた基準と内部統制と同様に、変更着手、ソフトウェア開発と保守及び承認プロセスが含まれる。これらはプログラミング、文書化、テストの基準を含む。 システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況と終了について知らされる。

規準	内部統制の例
	システム基盤とソフトウェアに対する変更は、本番への導入前に別の開発・テスト環境で開発され、テストされる。 変更管理ポリシーと手続の一部として、「本番移行」プロセス（例えば、「テスト」から「移行」「本番」まで。）がある。本番への移行に際しては、変更の予算を持つ業務責任者とコンピュータ運用の管理者の承認を必要とする。 変更が重要なシステム構成要素に行われるとき、重要な中断に備えて、作成された「復帰（バックアウト）」計画がある。
3.18　緊急変更が文書化され承認されること（事後承認を含む。）を規定するための手続が存在する。	システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知らされる。 標準手続からの逸脱を必要とする緊急変更は、毎日ＩＴ管理者によってログを採取され、レビューされ、直属の業務統括者に報告される。恒久的是正措置は、企業の業務統括者の承認を含む変更管理プロセスに従う。
システム処理のインテグリティに適用する可用性関連の規準	
3.19　システム処理のインテグリティを害するかもしれない潜在的リスク（例えば、環境のリスク、自然災害、及び日々の操作上のエラーと欠落）に対して、システムを保護するための手続が存在する。	内外の物理的環境のいずれについても、重要な変更が起こるたびに、又は定期的にリスク評価が実施され、レビューされている。火災、水害、塵埃、電力停止、過熱、過湿度、労働問題といった脅威が考慮される。 経営者は、定期的なリスク評価に基づいて、環境的要因（例えば、火災、水害、塵埃、電力停止、過熱、過湿度）から保護する対策を維持する。企業が管理している領域は、煙探知器と防火システム両方を利用して火災から保護される。漏水検知器が二重床の中に設置される。 無停電電源装置（UPS）と緊急時電源装置（EPS）両方を利用することによって、企業サイトの処理環境は停電から保護される。この装置は半年ごとにテストされる。 予防的な保守契約と予定された保守手続が重要なシステムハードウェア構成要素のために備わっ

規準	内部統制の例
	ている。 ベンダー保証仕様書が準拠され、システムが適切に設定されているかを確認するためにテストされる。 マイナーな処理エラー、停電と記録の破壊に対応するための手続が文書化されている。 問題の識別、文書化、上申、解決、レビューのための手続が存在する。 物理的、論理的なセキュリティ管理が、システム処理のインテグリティを害する可能性のある未承認の行動の機会を減らすために導入されている。
3.20　企業の定義されたシステム処理のインテグリティのポリシーに整合したバックアップ、外部保管、回復、災害復旧を提供するための手続が存在する。	経営者は、ビジネス要件のレビューに基づいて、バックアップ及び回復のための包括的な戦略を導入する。企業のバックアップ手続が文書化されており、それらは冗長サーバー、日次の差分バックアップ及び、週１回の変更の完全バックアップを含んでいる。日次、週次のバックアップが企業のシステムポリシーに従って外部保管される。 災害復旧計画と緊急時対応計画が、文書化される。 災害復旧計画は役割と責任を定義して、ビジネス影響度分析に基づいて、高い可用性とシステムの信頼性を確かめるために必要な、重要なＩＴアプリケーションプログラム、オペレーティング・システム、要員、データファイル、タイムフレームを識別する。 事業継続計画（BCP）調整者は、毎年、ビジネスの各分野についてのビジネス影響度分析をレビューして更新する。 災害復旧計画と緊急時対応計画が、企業のシステムポリシーに従って毎年テストされる。テスト結果と変更勧告が企業の経営会議に報告される。 企業の経営会議は災害復旧計画に対する変更をレビューして、承認する。 事業継続計画で識別された重要な要員は、社内

規準	内部統制の例
	及び外部で計画の最新のバージョンを保有している。電子版が外部保管される。
3.21　バックアップのデータとシステムの完全性、正確性、適時性を提供する手続が存在する。	自動化されたバックアッププロセスには、バックアップデータのインテグリティをテストするための手続が含まれる。 バックアップが企業の定義されたバックアップ戦略に従って行われ、バックアップの活用性が少なくとも毎年確かめられる。 バックアップシステムとデータが、サードパーティーサービスプロバイダの施設において外部保管される。 サービスプロバイダ契約の要件の下で、企業は、外部保管施設において保存された媒体の年次検証を実施する。検証の一部として、外部保管の場所における媒体が、適切な媒体管理システムと照合される。保管場所は、物理的なアクセスセキュリティとデータファイルと他の項目のセキュリティのために半年に１回視察される。 バックアップシステムとデータが年度の災害復旧テストの一部としてテストされる。
4.0　モニタリング：企業は、システムをモニターして、定義されたシステム処理のインテグリティポリシーへの遵守性を保持するための行動を取る。	
4.1　システム処理のインテグリティとセキュリティパフォーマンスが定期的にレビューされ、定義されたシステム処理のインテグリティ及び関連するセキュリティポリシーと比較される。	システム処理が社内の運用スタッフによって24時間休みなくシステムモニタリングツールを使ってモニターされる。処理ログ、パフォーマンスとセキュリティインシデントの統計と承認された目標との比較が、運用チームによって毎日レビューされ、蓄積され、月次のＩＴ運営委員会に報告される。 顧客サービスグループは、システム処理に関連する顧客の苦情をモニターする。それは改善のための提案と一緒にこのような事項の月次報告書を提供し、それは月次のＩＴ運営委員会のミーティングにおいて考慮され、実行される。 情報セキュリティチームは、内製の又は一般に利用可能なツールを使ってシステムをモニターし、脆弱性を評価する。潜在的リスクが評価され、SLAと企業のその他の義務と比較される。改善計画が提案され、実施がモニターされる。

規準	内部統制の例
	企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。内部監査部門は、年度の監査計画の一部として、処理のインテグリティとシステムセキュリティレビューを行う。結果と改善のための提案が経営者に報告される。
4.2 定義されたシステム処理のインテグリティ及びそれと関連するセキュリティポリシーに従った目的を達成するために、企業の現行の能力の潜在的な劣化を識別して、対処するプロセスがある。	システム処理が社内の運用スタッフによって24時間休みなくシステムモニタリングツールを使ってモニターされる。処理ログ、パフォーマンスとセキュリティインシデントの統計と承認された目標との比較が、運用チームによって毎日レビューされ、蓄積され、月次のＩＴ運営委員会に報告される。 年次ＩＴ計画と予算編成プロセスの一部として、将来のシステム処理のパフォーマンスと性能要件が見積もられ、分析される。 システム処理のインテグリティに関連するセキュリティ目的を達成する企業の能力への潜在的な影響を与えるかもしれない傾向を識別するために、人的又は自動化ツールによってログを分析する。 月次のＩＴスタッフ会議が、システム処理、性能、セキュリティ上の問題と傾向に対処するために開催される。発見事項が年４回の経営会議において検討される。
4.3 環境、規制、技術の変更がモニターされ、それらのシステム処理のインテグリティとセキュリティ上の影響が適時に評価され、その評価に基づきポリシーが更新される。	企業のデータセンター施設は気候と環境のモニタリング装置を含む。最適なパフォーマンス範囲からの逸脱は上申され、解決される。 上級経営者が、年度のＩＴ計画プロセスの一部として、企業の処理のインテグリティ及びそれに関連するセキュリティポリシー上に適用される法規制の影響と技術開発を考慮する。 企業の顧客サービスグループは、新規技術、顧客要件と競争的な活動の影響をモニターする。

機密保持原則と規準

28. 機密保持原則は、機密として、コミット又は同意された情報を保護するシステムの能力について言及する。世界中の多くの国で規則によって定義され、プライバシー原則（パラグラフ33を参照）の対象となっている個人情報と異なり、機密情報の広く認められた定義はない。通信及び取引業務を処理するに当たり、ビジネスパー

トナーはしばしば機密が保持される必要がある情報を交換する。大抵の事例では、それぞれの当事者は、取引の完了又は取引に伴って生じる疑問を解決するために、アクセスが必要な要員のみが彼らの提供した情報を利用可能であることの保証を望む。ビジネスパートナーの信頼を向上するために、ビジネスパートナーが企業のシステム及び情報の機密保持に関するポリシー、手続及び実務について知らされることは重要である。企業は、システムへの承認されたアクセスの提供と、機密とされた情報の利用・共有についての方法に関するシステム及び情報の機密保持のポリシー、手続及び実務を開示する必要がある。

29. 機密保持の対象とする情報の種類の例
- 取引の明細
- 設計図
- 事業計画
- 企業の銀行取引情報
- 知的財産
- 有効在庫
- 入札価格又は提示価格
- 価格リスト
- 法的文書
- 顧客リスト
- 顧客や業界からの収入

30. 機密であることの解釈は、企業間で際立って異なることがあり、契約の取り決めや規制によって決定される。結果として、取引関係にある当事者ないし潜在的当事者にとって、どんな情報がシステム上で機密として保持されるべきか、必要があれば、どのようなアクセス権が提供されるかを、理解し、合意することが重要である。

31. 取引相手に提供される機密情報は他の当事者のコンピュータシステム上に送信、保管される間に未承認のアクセスにさらされやすい。例えば、ビジネスパートナー属性情報、取引と決済指示が、それらが伝達されている間に、未承認の当事者によって傍受されるかもしれない。暗号化のようなコントロールは送信の間にこの情報の機密保持のために利用できる。ファイアウォールと厳格なアクセスコントロールは、情報がコンピュータシステム上で処理され、保管される間、それを保護するために利用できる。

機密保持原則と規準の表

32. 機密とされた情報がコミット又は合意したとおりにシステムにより保護されている。

規準	**内部統制の例**
機密として設定された情報が、コミット又は合意したとおりに、保護されている。	
1.0　ポリシー：企業は、コミット又は合意されたシステムにより保護される機密情報保護に関連するポリシーを定義し、文書化している。	
1.1　企業の機密保持と関連するセキュリティポリシーは、特定の個人又はグループによって確立され、定期的にレビューされ、承認されている。	ＩＴと物理的セキュリティの双方に関わる文書化された機密保持と関連するセキュリティポリシーが、ＩＴ基準委員会により承認されており、企業全体に適用されている。

規準	内部統制の例
	定期的なリスク評価プロセスの一部として、セキュリティ責任者は下記に基づきＩＴリスク評価への変更を識別する。 ・　新規のアプリケーション、インフラの変更 ・　アプリケーション、インフラの構成要素への重要な変更 ・　新しい環境に基づいた機密保持とセキュリティリスク ・　規制や基準の変更 ・　SLAその他の文書で識別されたユーザー要件への変更 セキュリティ責任者はＩＴリスク評価に基づき機密保持ポリシー及びセキュリティポリシーを更新する。 ＩＴセキュリティポリシーの変更は、適用前にＩＴ基準委員会によって承認される。 機密保持のユーザー要件がSLA、秘密保持契約又はその他の書類で文書化されている。
1.2　企業の、機密情報とセキュリティの保護と関連するポリシーは、下記の事項を含むが、それらに制限されない。 a. 承認されたユーザーの機密保持と関連するセキュリティ要件の識別と文書化 b. 重要性、機微性（Sensitivity）に基づくデータの分類。分類は保護の必要性、アクセス権限、アクセス制限、維持と廃棄を定義するのに用いられる。 c. 定期的なリスク評価 d. 未承認のアクセスの防止 e. 新規ユーザーの追加、既存ユーザーのアクセスレベルの変更及びアクセスする必要のなくなったユーザーの削除 f. 機密保持及びそれと関連するセキュリティに対する実施責任と説明責任の割当て	（本規準の内部統制の例は、企業の文書化された機密保持ポリシーと関連するセキュリティポリシーであり、左記に列挙された要素を含んでいる。機密保持ポリシーとセキュリティポリシーの例示は省略する。）

規準	内部統制の例
g. システム変更と維持管理に対する実施責任と説明責任の割当て h. 導入前のシステム構成要素のテスト、評価、承認 i. 機密保持及びそれと関連するセキュリティ問題に関連している苦情と要請がどのように解決されるか。 j. 機密保持及びそれと関連するセキュリティ違反その他のインシデントを処理するための手続 k. 機密保持及びそれと関連するセキュリティポリシーをサポートする訓練等に必要な経営資源を配分するための規定 l. 機密保持及びそれと関連するセキュリティポリシーで明示的に扱われない逸脱事項と状況の取扱いのための規定 m. 適用される法規制、定義されたコミットメント、SLA、その他契約上の要請の識別と一致のための規定 n. 第三者との情報の共有	
1.3 企業の機密保持及びそれと関連するセキュリティポリシーの開発・維持及びそれらのポリシーの変更・更新に関わる実施責任と説明責任が割り当てられている。	経営者が人事部に、企業の機密保持ポリシーの導入についての実施責任を割り当てている。企業のセキュリティポリシーの導入に対する実施責任が最高情報責任者（CIO）の指示の下に、セキュリティ責任者に割り当てられている。役員会のＩＴ基準委員会は、役員会ハンドブックに示されたポリシーのレビュー、更新と承認について支援する。
2.0 コミュニケーション：企業は、責任ある当事者と承認されたユーザーに、システムによる機密情報保護について定義されたポリシーを伝達している。	
2.1 企業は、システムの記述とその範囲を客観的に定義して、承認されたユーザーに伝達している。	電子商取引システムのために、企業はWebサイト上にシステム記述を開示している。電子商取引システムのためのシステム記述については、付録Ａを参照のこと。 電子商取引でないシステムのために、企業は承認されたユーザーにシステム記述を提供している。電子商取引でないシステムのためのシステム

規準	内部統制の例
	記述については付録Ｂを参照のこと。
2.2　ユーザーの機密保持と関連するセキュリティ義務と、企業のユーザーへの機密保持と関連するセキュリティコミットメントは、機密情報が提供される前に承認されたユーザーに伝達されている。このコミュニケーションは下記の事項を含むが、それらに制限されない。	企業の機密保持と関連するセキュリティコミットメントと要求される機密保持に関連するセキュリティ義務は、顧客及び他の外部ユーザーに対して、企業のWebサイト上に掲示されている。企業の機密保持ポリシーと実務は、契約書、SLA、ベンダー契約規定と条件、標準秘密保持契約で概説することもできる。
a．情報がどのように機密とされ、機密を解除されるか。機密情報の取扱い、廃棄、維持、保存、バックアップ及び配布又は通信	署名された秘密保持契約書が機密とされた情報を第三者と共有する前に必要とされる。契約書、SLA、ベンダー契約がサービス提供の前に交渉される。これらの契約の標準機密保持規定に対する変更には、執行責任者の承認を必要とする。
b．機密情報へのアクセスがどのように承認され、無効にされるのか。	内部のユーザー（従業員と外部委託先）のために、企業の、機密保持と関連するセキュリティポリシーは、オリエンテーションの一部として新しい従業員と外部委託先にレビューされる。ポリシーの重要な項目と従業員への影響については検討される。新しい従業員はポリシーを読んで、理解して、従うことを示している誓約書に署名しなくてはならない。毎年、彼らのパフォーマンスレビューの一部として、従業員がセキュリティポリシーの理解とそれへの遵守性を再確認しなくてはならない。外部委託先の機密保持とセキュリティ義務が契約で詳述される。
c．機密情報がどのように利用されるのか。	セキュリティ周知プログラムが、従業員に企業の機密保持と関連するセキュリティポリシーを伝達するために実施されている。
d．機密情報がどのように共有されるのか。	企業は、企業のイントラネット上に機密保持に関連するセキュリティポリシーを公開する。
e．情報が第三者に提供される場合は、開示に当該第三者の機密保持実務及び内部統制に依拠することによって生じる何らかの制限を受けることを含むべきである。そのような開示をしないならば、企業がその機密保持実務及び内部統制に合致するか、又はそれを超えるような第三者の機密保持実務及び内部統制に依拠していることを示しているこ	署名された秘密保持契約書が機密とされた情報を第三者と共有する前に必要とされる。

規準	内部統制の例
とになる。 f. 機密保持に関して適用される法律と規則に従うための実務	
2.3 企業の機密保持と関連するセキュリティポリシーとそれらのポリシーに対する変更・更新のための実施責任と説明責任が、それらを実施することに責任がある企業の要員に伝達されている。	セキュリティ管理チームは、企業の機密保持に関連するセキュリティポリシーの日々の維持について義務と責任があり、そして、CIO及びＩＴ運営委員会に変更について提言する必要がある。 機密保持に関連するセキュリティコミットメントが年次のＩＴ計画プロセスの一部として顧客口座管理者及び法務部門の代表者によりレビューされる。 文書化された職務記述が定義され、実施責任のある要員に伝達されている。 定義された機密保持プロセスの文書化されたプロセス及び手続マニュアルが、実施責任者に提供される。セキュリティ責任者は機密保持ポリシーの変更に基づいてプロセス及び手続マニュアルを更新する。
2.4 機密保持とシステムセキュリティの違反について企業に通知し、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	顧客と外部のユーザーが潜在的な機密保持又はセキュリティの違反と他のインシデントを企業に知らせるプロセスは、企業のWebサイト上に開示されるか、又は新規ユーザー手引書の一部として提供されているか、又はその両方である。 企業のセキュリティ周知プログラムは、潜在的な機密保持とセキュリティの違反の識別、セキュリティ管理チームに知らせるプロセスに関する情報が含まれている。 潜在的な機密保持又はセキュリティの違反その他のインシデントの識別と上申のための文書化された手続が存在している。
2.5 機密保持とシステムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されている。	システム構成要素に対する計画された変更とそれらの変更のスケジューリングは、月次ＩＴ運営委員会のミーティングの一部としてレビューされる。 システムセキュリティに影響を与えるかもしれないシステム構成要素に対する変更は、導入前にセキュリティ管理者の承認を必要とする。 顧客及びユーザーと彼らの機密保持及び関連す

規準	内部統制の例
	るセキュリティ義務、又は企業の機密保持とセキュリティコミットメントに影響を与えるかもしれない変更が、企業のWebサイト上に強調して掲示される。 機密保持とシステムセキュリティに影響を与えるかもしれない変更が、提案された変更の導入前に標準サービスアグリーメントの規定において影響を受ける顧客によってレビューされて、承認される。 機密保持とシステムセキュリティに影響を与える要素を含む変更の定期的なコミュニケーションがある。 機密保持又はシステムセキュリティに影響を与える変更が、企業の現在のセキュリティ周知プログラムに取り入れられている。
3.0 手続：企業は、定義されたポリシーに従って文書化された機密保持目的を達成するために手続を整備している。	
3.1 (1)システム機密保持コミットメントを損なうシステム運用の中断の潜在的脅威の識別、(2)識別された脅威に関連するリスクの評価、のための手続が存在する。	リスク評価が定期的に実施される。このプロセスの一部として、機密保持への脅威が識別され、これらの脅威から生じるリスクが公式に評価される。 セキュリティ責任者が評価された脅威に基づき、機密保持プロセスと手続を修正する。
3.2 入力の機密保持に関連するシステム手続は文書化された機密保持ポリシーと整合している。	機密保持プロセスは、全ての入力が承認され、処理のために受け入れられ、計上されるのを確実にするために確立される。いかなる喪失した、又は未計上の原始証憑と入力ファイルも識別され、調査される。これらの処理は、特定の期間内でかつデータ処理が発生又は完了する前に、逸脱事項が解決されていることを必要とする。 機密保持プロセスは、入力ルーチンと物理的な入力媒体（未使用及び使用済み）へのアクセスを承認された個人に制限するために導入される。 機密保持プロセスは、承認された個人だけに情報を入力する能力を制限するために存在している。これは運用上又はプロジェクトの特定の役割と責任に基づく制限を含む。 エラーメッセージは承認された者に明らかにされる。エラーメッセージは他人に利用され得る潜

規準	内部統制の例
	在的に害を及ぼす情報を明らかにせず、機微情報（例えば、電子メールの内容や財務情報）はエラーログや関連する管理メッセージにリストされない。
3.3　データ処理の機密保持に関連するシステム手続は文書化された機密保持ポリシーと整合している。	機密保持プロセスは、全ての取引が処理されるのを合理的に保証し、完全に処理されていない取引を特定するために取引ログを使用する。取引の不完全な実行を特定し、見直し、分析し、適切な行動を取るためのプロセスが整備されている。 機密保持プロセスは、データと取引処理に向けられた不適当又は通例でない行為、オーバーライド又は迂回を含む、いかなる目的やデータにアクセスする人の承認レベルを超えた目的のためにデータにアクセスする無権限の試みを、適時にモニターするために存在している。
3.4　出力の機密保持に関連するシステム手続は文書化された機密保持ポリシーと整合している。	経営者は、データの機微性（Sensitivity）と機密保持及び出力データへのユーザーアクセスの適切性を含む報告戦略を策定する。 経営者は、企業の内外での報告その他のコミュニケーションにおいて使用される機密出力データの複製又は作成をモニターするプロセスを整備している。 出力データへのユーザーアクセスは、ユーザーの役割と情報の機密保持に適切に整合する。 レポートへのアクセスはその情報への合理的なビジネスニーズを持ったユーザーに制限される。 ユーザーが、機密情報を含むレポートにアクセスするためには適切な承認が必要である。
3.5　定義された機密保持及び関連するセキュリティポリシーに矛盾しない当事者のみに機密情報を提供する手続が存在する。	従業員が雇用契約の一部として、機密保持合意に署名するように要求される。この合意は、従業員がアクセスを認められた情報及びその他のデータのいかなる開示も禁止する。 論理的アクセスコントロールが職能と必要に基づいて、機密情報へのアクセスを制限するように整備されている。機密データへのアクセス権のリクエストは、データオーナーの承認を必要とする。 ビジネスパートナーは秘密保持契約又はその他の契約の機密保持規定の対象となっている。

規準	内部統制の例
3.6　情報が転送される第三者の機密保持ポリシーについて、企業の定義された機密保持と関連するセキュリティポリシーを満たしているという保証又は宣言を得るための手続が存在する。	企業は、技術サポート又はサービスを外部委託して、外部委託したプロバイダにデータを転送する。企業によって提供された情報の機密保持に関するサービスプロバイダの要件は、サービス契約に含められる。法務顧問が企業の機密保持ポリシーとサービスプロバイダの機密保持規定の適合性を評価するために、サードパーティーサービス契約をレビューする。 企業は、外部委託プロバイダによる内部統制について宣言と保証を入手し、外部委託プロバイダの独立した監査人からの当該内部統制の有効性に関する報告書を入手する。
3.7　開示された機密保持実務が中止されるか、又は制限を緩和するために変更される場合、企業は、当該機密情報が受け取られたとき、機密保持実務に従って機密情報を保護するための手続を整備するか、又は顧客の機密情報に関して新しい機密保持実務に従うという顧客の同意を得る。	ビジネスパートナー契約の機密保持規定に対する変更は、ビジネスパートナーと再検討される。 ポリシー制限を緩和する変更がされたとき、企業は新しいポリシーに対して、顧客の同意を得ようと試みる。新しいポリシーに同意しない顧客の機密情報は、システムから取り除かれて、破棄されるか、又は隔離されて、古いポリシーの下で継続的な保護を受ける。
機密保持に特有のシステムセキュリティ関連の規準	
3.8　システムとシステムで維持されている機密情報への論理的アクセスを制限するための手続が存在する。下記の事項を含むが、それらに制限されない。	
a. 公にすべきでない情報資源へのアクセスを制限するための論理的アクセスセキュリティ対策	・　公にすべきでない機密情報資源への論理的アクセスは、ＯＳ固有のセキュリティ、アプリケーション及び資源固有のセキュリティ、追加的なセキュリティソフトウェアの利用を通じて保護される。 ・　資源に特有な、又は初期的なアクセスルールは、全ての公にすべきでない資源について定義される。 ・　資源へのアクセスは、ユーザーの身元に基づいて認証されたユーザーに付与される。
b. 全てのユーザーの識別と認証	・　ユーザーは、関連するパスワードで認証された正しいユーザーＩＤの利用を通じて公にされていない機密情報資源にアクセスしようとする場合、企業のネットワークとアプリケーションシステムに対して身元を明らかにしなければならない。

規準	内部統制の例
c．新規ユーザーの登録と承認	・　ユニークなユーザーＩＤが個別のユーザーに割り当てられる。 ・　グループ又は共有ＩＤは十分なリスク評価と共有ＩＤを利用するビジネスユニットのマネージャの文書による承認がないと利用できない。 ・　パスワードは大文字と小文字を区別し、少なくとも８文字で、そのうち１文字は英数字でない文字を含んでいなくてはならない。 ・　セキュリティ設定のパラメータにより、パスワードは90日ごとに更新されるよう強制される。 ・　ログインを３回失敗するとログインできなくなる。 ・　顧客は、企業のWebサイト上で、新規ユーザー情報を提供し、適切なユーザーＩＤとパスワードを選ぶセキュアなセッションの下において自己登録することができる。自己登録された顧客口座と結び付けられた権限及び権限付与が、特定の制限されたシステム機能を提供する。 ・　ユーザーとユーザーアクセス権限（制限された「顧客口座」としての機能性を除く。）を生成又は修正する権限は、セキュリティ管理チームに限定される。 ・　直属の業務統括者は、従業員と外部委託先のアクセス権変更のリクエストを承認する。制限された資源へのアクセスは資源の所有者（リソース・オーナー）によって承認される。 ・　自己登録の間に与えられたデフォルト権限を超えた顧客アクセス権は、顧客口座管理者によって承認される。 ・　機密性のある適切な職務分離が権限を与える際に考慮されている。
d．ユーザープロファイルに対する変更と更新のプロセス	・　自己登録の顧客口座に対する変更と更新は、ユーザーが成功裏にシステムにログインした後、企業のWebサイト上でいつでも個々のユーザーによって可能となる。変更は即時に反映される。 ・　使われていない顧客口座（６か月間不使用）がシステムによって排除される。 ・　他のアカウントとプロファイルに対する変更は、セキュリティ管理チームに制限されていて、直属の業務統括者、顧客口座管理者の承認を要求する。 ・　人事管理システムが新たに退職した従業員のリストを毎週人事部に提供する。このリストはアカウント失効のためにセキュリティ管理チー

規準	内部統制の例
	ムに送られる。
e．顧客、個人のグループ、又は他の企業が自分自身以外の機密情報にアクセスすることを防止する手続	・　企業顧客にログインプロセスの一部として必要とされるユニークな企業ＩＤを割り当てられる。アクセスソフトウェアが、ログインにおいて使われた企業ＩＤに基づいて、ユーザーアクセスを制限するために使われる。 ・　個々の顧客が彼らのユニークなユーザーＩＤに基づいて、彼ら自身の機密情報資源へのアクセスが制限される。
f．彼らの割り当てられた役割と責任に基づいて、承認された従業員だけに機密情報へのアクセスを制限する手続	・　機密の顧客情報資源へのアクセス権のリクエストは、顧客口座管理者の承認を必要とする。 ・　模擬顧客データがシステム開発とテスト目的のために使われる。機密の顧客情報はこの目的のために使われない。
g．承認されたユーザーに制限されたアウトプット配布	・　コンピュータが処理したアウトプットへのアクセスは、承認された人にだけ、情報の分類に基づいて提供される。 ・　処理されたアウトプットは、その情報の分類を反映した領域に保存される。
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アクセスの制限	・　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アクセスは、物理的・論理的アクセスコントロールにより、コンピュータ運用スタッフに制限されている。
i．システム構成、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とセキュリティ装置（例えば、ファイアウォール）に対するアクセスの制限	・　ハードウェアとオペレーティング・システム設定テーブルは、適切な要員に制限されている。 ・アプリケーションソフトウェアの設定テーブルは、承認されたユーザーに制限されており、アプリケーションの変更管理ソフトウェアのコントロール下にある。 ・　データ又はプログラムを、閲覧、追加、変更、削除できるユーティリティプログラムは、承認された技術サービススタッフに制限されている。その使用は、コンピュータ運用の管理者によってログを採取され、モニターされる。 ・　CIO指揮下の情報セキュリティチームは、全ての記憶装置メディアへのアクセスはもちろん、ファイアウォールその他のログへのアクセスも保持する。そのようなアクセスはログを採取されて、企業のＩＴポリシーに従ってレビューされる。 ・　全てのマスターパスワードのリストが暗号化されたデータベースに保存され、副本が企業の金庫に封印された封筒で保持される。
3.9　定義されたシステムへの物理的アクセスを制限する手続	企業のＩＴ資源、サーバー及びファイアウォールとルータなどの関連するハードウェアを収容す

規準	内部統制の例
が存在する。施設、バックアップ媒体、及びファイアウォール、ルータ、サーバーのような他のシステム構成要素を含むが、それらに制限されない。	るコンピュータ室への物理的なアクセスが、カードキーシステムによって承認された個人に制限され、ビデオ監視装置によって監視される。 物理的なアクセスカードがビル警備によって管理される。アクセスカードの使用実績が日誌に記録される。記録はビル警備によって保持され、レビューされる。 企業のコンピュータ施設への物理的なアクセス権のリクエストは、コンピュータ運用管理者の承認を必要とする。 潜在的セキュリティ違反の識別と上申についての文書化された手続が存在する。 外部保管バックアップデータと媒体がサービスプロバイダ施設において保存される。外部保管データと媒体へのアクセスはコンピュータ運用管理者の承認を必要とする。
3.10　システム資源への未承認のアクセスから保護するための手続が存在する。	ログインセッションは、３回のログイン失敗の後に終了させられる。 VPN（仮想専用ネットワーク）ソフトウェアが、承認されたユーザーによるリモートアクセスを認めるために使われる。ユーザーが特定の「クライアント」ソフトウェアとユーザーＩＤ及びパスワードを通してVPNサーバーによって認証される。 ファイアウォールが使われて、未承認のアクセスを阻止するように設定される。ファイアウォールの状況はログが採取され、セキュリティ管理者によって毎日レビューされる。 不必要なネットワークサービス（例えば、telnet、ftp、http）は企業のサーバー上で無効とされる。必要とされ承認されたサービスのリストがＩＴ部門によって保持される。このリストは、最新の運用状況における適切性の観点から定常的に企業の管理者によってレビューされる。 企業のネットワークの継続的モニタリングと、潜在的セキュリティ違反の初期段階での識別を提供するために侵入検知システムが使われる。 企業は、定期的なセキュリティレビューと脆弱

規準	内部統制の例
	性評価を行うために第三者と契約する。結果と改良のための改善勧告が経営者に報告される。
3.11　コンピュータ・ウィルス、悪意があるコードと未承認のソフトウェアによる感染から保護するための手続が存在する。	他のセキュリティモニタリングに関連して、セキュリティ管理チームは、ユーザー・グループに関与して、コンピュータ・ウィルスに関するサービスに加入する。 送られてくる電子メールメッセージのウィルススキャンを含むアンチウィルスのソフトウェアが備わっている。パターンファイルは都度更新される。 発見されたいかなるウィルスもセキュリティチームに報告され、全てのユーザーにそれらの潜在的ウィルス脅威を周知するために警告がなされる。
3.12　インターネット又は他の公衆網上を通過するユーザー認証と機密情報を保護するため、暗号化又は他の同等のセキュリティ技術が利用される。	企業は、公衆網上でのユーザーＩＤとパスワードを含む個人情報又は機密情報の送信のために、業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を利用する。潜在的セキュリティ問題を回避するためセキュリティ管理チームによってテストされて、使用に当たって承認された最新のバージョンへブラウザを更新するようにユーザーは要求される。 アカウント使用状況はログイン成功後に業界標準の暗号技術、VPNソフトウェア又はその他のセキュアなコミュニケーションシステム（定期的なＩＴリスク評価に沿って）を通して暗号化される。ユーザーは、要求すればすぐに（Webサイト上の「サインアウト」ボタンを選択することによって）、又は10分間使用しないとログアウトされる。 取引相手のエクストラネットを通じて企業に提供される機密情報は、暗号化される。 処理のための独立したサードパーティーサービスプロバイダへの顧客の機密情報の送信は、専用回線でなされる。
目的達成のために利用される実行及びインシデント管理関連の規準	
3.13　機密保持とセキュリティ違反その他のインシデントを識別して、報告して、行動を起こすための手続が存在す	ユーザーには、潜在的機密保持とセキュリティ違反を情報セキュリティチームへ伝達するための指針が提供される。情報セキュリティチームは、顧客ホットラインと電子メールを通して報告され

規準	内部統制の例
る。	たインシデントを記録する。 侵入検知その他のツールが、潜在的セキュリティ違反とその他のインシデントを識別し、ログを採取し、報告するために使われる。システムは進行中の潜在的インシデントについて、電子メールとポケットベルによって情報セキュリティチームとネットワーク管理者に通知する。 インシデントログが情報セキュリティチームによって毎日モニターされ、評価される。 インシデントが発見又は報告された場合、承認された要員により、定義されたインシデント管理プロセスが開始される。定義されたポリシー及び手続に準拠して是正措置が実施される。 手続は、定義されたインシデントの上申プロセス及び通知体制を含んでいる。 全てのインシデントは、解決するまで経営者によって追跡される。 終了したインシデントは、適切な解決のために経営者によってレビューされる。 セキュリティに関連しないインシデントの解決には、インシデントとその解決がセキュリティ要件に与える影響を考慮することが含まれている。
目的達成のために利用されるシステム構成要素関連の規準	
3.14　定義された機密保持及びそれに関連するセキュリティポリシーに従って、システムデータが分類される手続が存在する。	データオーナーは定義されたセキュリティ要件及びリスク評価に基づいて、データアクセスルールを定期的にレビューし、修正を要求する。 新しいデータが補足又は生成された場合はいつでも、そのデータはセキュリティポリシーに基づいて分類される。 データ分類の適性性は、変更管理プロセスの一部として考慮される。
3.15　機密保持及び関連するセキュリティポリシーへの遵守性違反が直ちに対処され、是正措置がタイムリーに取られる手続が存在する。	全てのインシデントは解決するまで経営者によって追跡される。 終了したインシデントは適切な解決のために経営者によってレビューされる。

規準	内部統制の例
	内部監査プロセスは、発見事項に対する行動計画の作成と終了するまでの行動計画の追跡を含んでいる。
3.16　システム基盤とソフトウェアの設計、調達、導入、設定、修正と管理が、定義された機密保持に関連するセキュリティポリシーに整合している。	企業は、コンピュータ化された情報システムの開発、調達、導入と維持及び関連する技術を管理する公式なシステム開発ライフサイクル（SDLC）方法論を適用している。 SDLC方法論は、顧客の機密保持要件を含むデータ分類のフレームワークを含んでいる。顧客の機密保持要件とセキュリティ損失のビジネス影響度の評価に基づいて、標準的なユーザープロファイルが確立される。ユーザーは必要性と職務上の責任に基づいて、標準的なプロファイルを割り当てられる。 内部の情報が分類と使用法に基づいて、所有者に割り当てられる。顧客口座管理者が顧客データの保管者として任命される。内部の情報の所有者及び顧客情報とデータの保管者が機微性（Sensitivity）を分類して、機密保持とセキュリティの適切なレベルを保持するように要求された保護のレベルを決定する。 セキュリティ管理チームは、新しいシステム開発又は調達について、企業の機密保持及び関連するセキュリティポリシーとの整合性を保証するために、アーキテクチャと設計仕様書をレビューして承認する。 セキュリティ又は情報の機密保持に影響を与えるかもしれないシステム構成要素に対する変更は、セキュリティ管理チームの承認を必要とする。 アクセスコントロールとオペレーティング・システム施設は、オプションとパラメータの導入を含めて、企業の機密保持と関連するセキュリティポリシーに従ってアクセスを制限するために導入されている。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。結果と改良のための改善勧告が経営者に報告される。
3.17　機密保持とセキュリティに影響を与えるシステムの設	企業は、重要な職位のための実施責任と、理論的及び職業的要件を記述した職務記述書を作成し

規準	内部統制の例
計、開発、導入との運用に関して責任がある要員が、彼らの責任を果たす資格と能力を持っていることを規定するための手続が存在する。	ている。 雇用手続は、重要な職位の候補者の包括的な審査、及び証明された資格が提案された職位と見合うか否かという検討を含んでいる。新しい要員が、経歴調査と身元調査の対象となることを条件に雇用される。 内部異動を含めた候補者は、職位の提示前に直属の業務統括者によって承認される。 定期的な業績評価が従業員の直属の上司によって行われる、それには人材育成活動の評価とレビューが含まれる。 要員は、システム機密保持及びセキュリティ概念と諸問題に関する訓練と能力開発を受ける。 休暇又は出張の場合に、重要なシステム機密保持及びセキュリティ機能のために代替要員を提供するための手続が備わっている。
機密保持に関連する変更管理関連の規準	
3.18　定義された機密保持及び関連するセキュリティポリシーと整合した環境設定を含めて、システム構成要素を保持する手続が存在する。	企業経営者が、セキュリティ管理の適切性についての第三者意見を受け取って、企業のシステムとWebサイトをホストしているサービスプロバイダから契約（SLA）に従い受け取るパフォーマンスのレベルを定期的に評価する。 ＩＴ部門は、全てのソフトウェアとそれぞれのレベル、適用されたバージョンとパッチの最新のリストを保持する。 システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知らされる。 システム構成は毎年テストされ、企業のセキュリティポリシーと最新のSLAに対して評価される。逸脱事項報告書が作成されるとともに、改善計画が作成され追跡される。
3.19　承認され、テストされ、文書化されたシステム変更だけが行われる手続が存在す	システム変更の承認、テスト、開発、導入の実施責任は分離されている。

規準	内部統制の例
る。	企業の文書化されたシステム開発方法論は、プロセスに埋め込まれた基準と内部統制と同様に、変更着手、ソフトウェア開発と保守及び承認プロセスが含まれる。これらはプログラミング、文書化、テストの基準を含む。 システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況と終了について知らされる。 システム基盤とソフトウェアに対する変更は、本番への導入前に、別の開発・テスト環境で開発され、テストされる。 変更管理ポリシーと手続の一部として、「本番移行」プロセス（例えば、「テスト」から「移行」「本番」まで。）がある。本番への移行に際しては、変更の予算を持つ業務責任者とコンピュータ運用の管理者の承認を必要とする。 変更が重要なシステム構成要素に行われるとき、重要な中断に備えて、作成された「復帰（バックアウト）」計画がある。
3.20　緊急変更が文書化され承認されること（事後承認を含む。）を規定するための手続が存在する。	システムの変更、維持とサプライヤー保守の要件は標準化され、文書化された変更管理手続に従う。変更は分類され、優先順位付けされ、緊急の事項を処理するための手続が備わっている。変更依頼者は、それらの依頼の実施状況について知らされる。 標準手続からの逸脱を必要とする緊急変更は、毎日ＩＴ管理者によってログを採取され、レビューされ、直属の業務統括者に報告される。恒久的是正措置は、企業の業務統括責任者の承認を含む変更管理プロセスに従う。
3.21　定義された機密保持及び関連するセキュリティポリシーに従って、機密情報がシステム開発、テスト、変更プロセスの間保護されるための手続が存在する。	機密とされた情報は、テスト又は開発のシステム及び環境で保存されず、処理されず、維持されない。 機密とされた情報を保持せざるを得ないテスト又は開発システム及び開発環境では、情報の機密保持を保護するためにデータの暗号化、マスキング、浄化技術を使用する。

規準	内部統制の例
4.0　モニタリング：企業は、システムをモニターして、定義された機密保持のポリシーの遵守性を保持するための行動を取る。	
4.1　企業の機密保持とセキュリティのパフォーマンスが定期的にレビューされ、定義された機密保持及び関連するセキュリティポリシーと比較される。	情報セキュリティチームは、内製の又は一般に利用可能なツールを使ってシステムをモニターし、脆弱性を評価する。潜在的リスクが評価され、SLAと企業のその他の義務と比較される。改善計画が提案され、実施がモニターされる。 企業は、定期的なセキュリティレビューと脆弱性評価を行うために第三者と契約する。内部監査部門は、年度の監査計画の一部として、システムセキュリティレビューを行う。結果と改善のための提案が経営者に報告される。
4.2　機密保持及び関連するセキュリティポリシーに従った目的を達成するために、企業の現行の能力の潜在的な劣化を識別して、対処するプロセスがある。	システムセキュリティ目的を達成する企業の能力への潜在的な影響を与えるかもしれない傾向を識別するために、人的又は自動化ツールによってログを分析する。 月次のＩＴスタッフ会議が、システムセキュリティ上の問題と傾向に対処するために開催される。発見事項が年４回の経営会議において検討される。
4.3　環境、規制、技術の変更がモニターされ、それらの機密保持とセキュリティ上の影響が適時に評価され、その評価に基づきポリシーが更新される。	企業のデータセンター施設は気候と環境のモニタリング装置を含む。最適なパフォーマンス範囲からの逸脱は上申され、解決される。 上級経営者が、年度のＩＴ計画プロセスの一部として、企業の機密保持及びそれに関連するセキュリティポリシー上に適用される法規制の影響と技術開発を考慮する。 企業の顧客サービスグループは、新規技術、顧客要件と競争的な活動の影響をモニターする。

プライバシー原則と規準

33. このセクションでは、プライバシーの概念、目標、原則の簡潔な概要を提示している。プライバシー原則の詳細については、付録D（パラグラフ48）の一般に公正妥当と認められたプライバシー原則―グローバルプライバシーフレームワーク（GAPP）を参照されたい。

34. GAPPに含まれるプライバシー原則は、企業（組織）が顧客、従業員その他の個人から取得する個人情報の保護に重点を置いている。一般に公正妥当と認められたプライバシー原則は、国内・海外の個人情報保護法制を参考にしながらビジネスの視点で策定されている。GAPPは、複雑なプライバシー要求事項を、10のプライバシー原則によって支えられた単一のプライバシー目標に集約している。

プライバシーの概念

35. 一般に公正妥当と認められたプライバシー原則の下では、「プライバシー」は、個人情報の収集、利用、保持、開示に関する個人及び企業の権利義務と定義される。

36. 個人情報は、識別可能な個人に関連するか、又はそのように推定できる情報である。それは、個人に関連付けられるか、又は直接的、間接的に個人を識別するために利用できるあらゆる情報を含んでいる。企業によって収集される個人に関する大抵の情報は、特定の個人の属性を示し得るのであれば、個人情報として取り扱われる可能性が高い。個人情報の幾つかの例としては、下記が挙げられる。
- 名前
- 住所又は電子メールアドレス
- 身分証明書番号（例　社会保障又は社会保険番号）
- 身体的特徴
- 消費者としての購買履歴

37. ある種の個人情報は「機微な情報」と位置付けられる。法令等により、下記の情報は機微な個人情報として定義されている。
- 医療又は健康状態の情報
- 家計の情報
- 人種及び民族
- 政治的見解
- 宗教的又は哲学的な信念
- 労働組合加入の事実
- 性生活
- 犯罪歴、違反歴を含む情報

38. 機微な個人情報は、一般的に、高い水準の保護及び高い注意義務が要求される。例えば、機微な情報には暗黙の同意ではなく、明確な同意が必要とされる。

39. 人に関するある種の情報は、特定の個人と結び付けられてはならない。そのような情報は「個人識別不可情報」と呼ばれる。これは、個人の識別が不明又は個人との関連が削除された統計上の又は要約された個人情報を含んでいる。このような場合、個人の身元は残っている情報から確認できない、なぜなら情報は「個人を識別不可」又は「匿名化」されているからである。個人識別不可情報は、個人に関連付けられることができないため、通常個人情報保護の対象とされない。

40. 「プライバシーか機密保持か。」世界中の多くの国で規則によって定義されている個人の同一性を証明できる情報と異なり、機密情報の広く認められた単一の定義はない。通信及び取引業務を処理するに当たり、ビジネスパートナーはしばしば「知る必要がある」（need to know）基準で保持される必要がある情報やデータを交換する。

一般に公正妥当と認められたプライバシー原則

41. 「全般的プライバシー目標」一般に公正妥当と認められたプライバシー原則は、下記のプライバシー目標に立脚している。

個人情報は、企業のプライバシー通知におけるコミットメント及び AICPA/CICA の一般に公正妥当と認められたプライバシー原則に定められた規準を充足して、収集、利用、保持、開示される。

42. 「プライバシー原則」GAPP は、個人情報の適切な保護と管理に欠くことができない。これらのプライバシー原則は、世界中の様々な法域の多くの個人情報保護法規と、認知された健全なプライバシー実務に含まれる国際的に知られた適正な情報実務に基づいている。下記の事項が、GAPP10 原則である。

(1) 管理：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。
(2) 通知：企業は、プライバシーポリシーと手続についての通知を規定し、個人情報が、収集、利用、保持、開示される目的を特定する。
(3) 選択と同意：企業は、個人にとって可能な選択を記述し、個人情報の収集、利用、開示に関して暗黙又は明確な同意を得る。
(4) 収集：企業は、通知で特定した目的のためだけに個人情報を収集する。
(5) 利用と保持：企業は、個人情報の利用を、通知で特定された目的及び個人が暗黙又は明確な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に必要である限りにおいて個人情報を保持する。
(6) アクセス：企業は、個人に対して、レビューと更新のために個人情報へのアクセスを提供する。
(7) 第三者への開示：企業は、通知で特定された目的及び、個人が暗黙又は明確な同意をした目的のためだけに第三者に個人情報を開示する。
(8) プライバシーのためのセキュリティ：企業は、（物理、論理双方の）未承認のアクセスに対して個人情報を保護する。
(9) 品質：企業は、通知で特定された目的のために正確かつ、完全かつ、適切に個人情報を保持する。
(10) モニタリングと周知徹底：企業は、プライバシーポリシーと手続への遵守性をモニタリングし、プライバシー関連の苦情と紛争を扱う手続を持っている。

プライバシー10 原則のそれぞれのために、企業のプライバシーポリシー、伝達、手続、内部統制の評価に対して適切、客観的、完全、測定可能な規準がある。

43. これらの規準は、GAPPとして別途公表されている。

オンラインプライバシー業務

44. プライバシー業務がオンライン領域である場合、企業はプライバシーシールを選択することもできる。これらの業務については、少なくとも企業のオンライン事業領域が含まれている必要がある。追加の留意事項については、付録ＤのGAPPを参照されたい。

付録Ａ　電子商取引システムのための開示例

この付録は、Trustサービスの原則と規準を満たすために、必要とされる電子商取引システムの開示例を示している。開示で要求されている事項は、Trustサービスの原則（セキュリティ、可用性、処理のインテグリティ、機密保持）で個別に特定されている。以下の開示は例示に過ぎず、特定の組織のシステムに応じて修正されるべきである。

システム記述

電子商取引でないシステムを記述するために使われるシステム構成要素を記述するよりは、組織は以下のようにシステムの機能を記述したほうが良い。

システム記述の例

弊社のサイト（abc-xyz.org）は起業家と小規模事業主がabc-xyz.orgの一連の事業サービスを利用して、オンライン店舗（myABC-xyz.org）を生成し、管理することを可能にしています。それはまた、abc-xyz.org上に作られた顧客サイトからの注文と弊社のサイトに関連した様々なサービスを提供するサードパーティーサービスプロバイダの利用を容易にするために、abc-xyz.orgに統合された履行と決済システムを対象範囲に含んでいます。

この記述では、ユーザーが自分自身のオンライン店舗を生成し、管理する機能を対象範囲に含んでいます。abc-xyz.orgに統合された、顧客サイトからの注文をabc-xyz.orgに生成できるようにするための履行と決済システムを対象範囲に含んでいます。

特定の原則と規準に関連する開示

以下の表は、電子商取引システムのための開示例を記述している。

セキュリティ

規準	開示例
2.2　ユーザーのセキュリティ義務と企業のユーザーへのセキュリティコミットメントは、承認されたユーザーに伝達されている。	弊社はあなたがABC.comを通じて提供する情報を保護するよう努めておりますが、インターネット上のデータ伝送が100%安全であることは保証できません。結果として、弊社は、弊社のWebサイトとオンライン・サービスを通して、あなたから送信された、又はあなたが弊社から受け取るどんな情報のセキュリティも保証又は担保することができません。 弊社は、定期的に弊社のセキュリティポリシーをレビューし、必要に応じて変更しています。毎年ＩＴ部門による厳格なレビューを行います。これらの定義されたセキュリティポリシーは、アクセス権、情報収集の必要性、説明責任とその他の事項を詳述しています。文書化されたシステムセキュリティ目的、ポリシー及び基準は契約上、法律上、その他のSLAで定義されたシステムセキュリティ要件と整合しています。例えば、ABC社内の承認された個人からなるグループだけがユーザー情

規準	開示例
	報にアクセスする権限を持ちます。アクセス、スクリプティング、更新、リモートアクセスに関して詳述している完全なポリシーは、組織の中で資格を持った要員によるレビューがなされるようになっており、一般の利用には供しておりません。 ABC.comはパスワードで保護された安全なデータネットワークで運用されており、一般には利用できません。あなたとABC.comの間で情報を伝送するとき、データセキュリティは、Secured Sockets Layer（SSL）と呼ばれるセキュリティプロトコルを通じて処理されます。SSLはデータ暗号化とWebサーバー認証を使うインターネットセキュリティ規格です。 暗号化の強度は、データを暗号化するために、使われた鍵の長さによって測定されます。すなわち、鍵がより長いと、それだけ暗号化が有効です。SSLプロトコルを使って、あなたとABC.comサーバーの間のデータ伝送が業界標準の暗号化強度において行われます。
2.4　システムセキュリティの違反について、企業に通知し、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	このサイトにセキュリティ違反があったと感じられましたら、(800)XXX-XXXXに電話してすぐに弊社と連絡を取ってください。
2.5　システムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されている。	サイトのユーザーに影響を与えるような、弊社のWebサイトのセキュリティに影響を与えるいかなる変更も、弊社のセキュリティポリシー及び重要な内部統制を要約するWebページに概要を表示して伝達します。

可用性

規準	開示例
2.2　ユーザーの可用性に関連するセキュリティ義務と、企業のユーザーへの可用性及び関連するセキュリティコミットメントは、承認されたユーザーに伝達されている。	ファイル保持とバックアップに十分な時間を割り当てるため、弊社のネットワークは最長で毎日22時間利用可能です。災害又は他の長期のサービス中断が生じたとき、弊社は、代替サービスサイトを使用して、24時間内に全面ビジネス再開を可能にするように手配しています。 弊社は、アクセス権、情報収集の必要性、説明責任その他の事項を詳述しているセキュリティポリシーを定義しています。それはレビューされて、年４回の経営会議において更新され、毎年ＩＴ部門による厳格なレビューを行っています。文

規準	開示例
	書化されたシステムセキュリティ目的、ポリシー及び基準は契約上、法律上、その他のSLAで定義されたシステムセキュリティ要件と整合しています。例えば、現在のポリシーではＩＤの共有を禁止しています。各サポート要員は、ログオンしてネットワーク装置を保守するための各自のユニークなＩＤを持っています。アクセス、スクリプティング、更新、リモートアクセスに関して詳述している完全なポリシーは、組織の中で資格を持った要員によるレビューがなされるようになっており、一般の利用には供しておりません。
2.4　システム可用性の問題、システムセキュリティの違反について企業に通知し、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	経営者は、サイトのセキュリティとシステムの可用性に関してお客様にどんなコメントでも、苦情又は懸念でも、電話をかけられる消費者ホットラインを持っています。もしこのサイトにアクセスすることが不可能なら、(800)XXX-XXXX宛てに弊社のお客様サポート要員と連絡を取ってください。このサイトにセキュリティ違反があったと感じられましたら、(800)XXX-XXXXに電話してすぐに弊社と連絡を取ってください。
2.5　システム可用性とシステムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されている。	サイトユーザーとしてのあなたに影響を与えるような、弊社のWebサイトのセキュリティとシステムの可用性に影響を与えるどんな変更でも、その概要を予測された変更の７日前に電子メールによってあなたに伝達します。その変更は弊社の可用性とセキュリティポリシーを要約するWebページに概要を表示します。

処理のインテグリティ

規準	開示例
2.1　企業は、システムの記述とその範囲を客観的に定義して、承認されたユーザーに伝達している。 もしシステムが電子商取引システムであるなら、Webサイト上に提供された追加の情報には下記の事項を含むが、それらに制限されない。 a. 該当する場合、提供される商品又はサービスの以下を含む状況の説明 ・　商品の状態（新品か、中古か、修理品か。） ・　サービス（又はサービス契約）の記述	あなたは、弊社のサイトにおいて新しい本又は古本を購入することができます；古本にはその旨を明示しています。 弊社があなたの仲介取引のために得る抵当利息（Mortgage Rate）情報は毎日、12の異なる貸付機関から収集されます。ここをクリックすれば、これらの貸付機関の全リストを見ることができます。 ABCオンラインRFQブローカレージ社は、注文部品の注文依頼書（RFQ）のためのオンラインの仲介業者です。弊社のユニークなサービスを通して、部品を探している製造業者（OEM）は、受注を探している契約製造業者と引き合わされます。

規準	開示例
・　情報源（何処で得られ、どのように変換されたか。） b. 電子商取引を行う条件及び要件。下記の事項を含むが、それらに制限されない。 ・　取引（取引とは、商品が販売される場合は注文の履行を、サービスが提供される場合はサービスの提供の履行を意味する。）の完了のためのタイムフレーム ・　注文又はサービス依頼の通常の処理に対する逸脱事項を顧客に通知するタイムフレームとプロセス ・　該当する場合、顧客選択権を含む、通常の商品又はサービスの提供の方法 ・　該当する場合、顧客選択権を含む支払条件 ・　電子決済実務及びそれに関連する顧客への請求 ・　該当する場合、顧客はどのように請求をキャンセルできるか。 ・　該当する場合、商品返品ポリシー又は責任の制限 c. 顧客が購入した商品及びサービスに対する保証、修理サービス、サポートを得ることができるWebサイト上の場所 d. 処理のインテグリティに関係している問題の解決のための手続。これらは、製品及びサービスの品質、正確性、完全性と関係がある苦情や、このような苦情の解決の失敗に関連する苦情など、電子商取引のあらゆ	弊社のオンラインの仲介業者が発行したRFQは、契約製造業者が見積書を作成するために、必要な全ての情報を受け取ることを保証する集中的なレビュープロセスを経ています。ABC社の訓練された要員は、彼らの不安を緩和するためにアウトソーシング市場の新規OEM製造業者と密接に共同作業をします。 RFQ入札プロセスに参加している契約製造業者は、ABC社のBizTrustプログラムの会員です。新しい会員は、RFQを入札する資格を持っていることを保証するために、クレジット審査のようなチェックと照会チェックの各種の組み合わせを受けなければなりません。これらのチェックの結果は、ABC社の全ての会員が容易に読め、かつ入手可能なBizTrust報告書に集約されます。 全国的な調査は、報酬リサーチ会社であるDowden社によって行われ、全ての規模の会社、全ての産業グループ、全ての合衆国地域を含む900以上の情報システム専門業の雇用主から集めた20X2年の報酬データを示しています。調査は20X1年７月に完了しました。 弊社は、お客様に承認された注文を受けてから１週間以内に注文された品を出荷することにしています。弊社の経験では注文の90パーセント以上が48時間以内に送られ、残りは１週間以内に送られています。 もしあなたが指定した日時までに弊社が注文を履行できないときは、弊社は24時間以内に電子メールであなたに通知し、あなたは追加義務なしに注文を解除できます。注文された品が出荷されるまではあなたは請求されることはありません。 あなたは、求められた情報を今ダウンロードするか、又は弊社がUPS２日便又はフェデラル・エクスプレス翌日配送便によってCD-ROMであなたに送るかの選択権を有しています。 クレジット承認が出荷前に必要とされます。全ての商品は、弊社の決済（正味30日）又は代替的契約条項が採用されているところに従って出荷をもって請求されます。

規準	開示例
る部分に関連している。	弊社は、取引の終わりに料金と経費の電子資金移動を必要とします。新しいお客様の場合は、預託金が必要とされることがあります。 あなたの月次のサービス料金をキャンセルするために、Subscriber@ABC.com宛てに電子メールを送るか、又は(800)XXX-XXXX宛てにお電話ください。あなたの口座番号を必ず入力してください。又はお電話の際にはお手元にご準備ください。 発注について、出荷受領後30日間以内に返品することで全額の返金を受けることができます。返品承認番号を受け取るために、フリーダイヤル又は電子メールをいただき、返品する商品の外装に明記するようお願いします。 保証その他のサービスは、このWebサイト上にリストアップした弊社の世界中の249拠点のどこでも受けることができます。これらの拠点のリストも弊社の全ての製品とともに配送されます。 このサイトでの取引は、弊社指定の調停人（XXX法律事務所）を通して行われた制限的調停の対象となります。彼らとはwww.name.orgにおいて、又はフリーダイヤル(800)XXX-XXXXにアクセスできます。調停の条項と条件の詳細については、ここをクリックしてください。 弊社の、消費者紛争解決のプロセスは、あなたがフリーダイヤル(800)XXX-XXXX宛てに弊社のお客様ホットラインと連絡を取るか、又はcusthelp@ourcompany.com宛てに電子メールによって弊社と連絡を取ることが必要です。もしあなたの問題が満足に解決されなかったなら、あなたは、サイバー苦情処理調停協会に連絡することもできます。協会には標準営業時間（中部標準時間で午前８時から午後５時）の間にwww.ccomplaint.comのWebサイトによって又は(877)XXX-XXXXに連絡できます。 調停の条項と条件の詳細については、ここをクリックしてください。 弊社のお客様であるあなたがこのサイトでの質問又は苦情に対するフォローアップないし回答を要求する場合、あなたはwww.xxxquestions.org宛

規準	開示例
	てに弊社と連絡を取ることができます。もしあなたへのフォローアップや苦情処理に不満がある場合は、あなたはこの国の電子商取引において消費者苦情を取り扱う電子商取引オンブズマンと連絡を取るべきです。オンブズマンとはwww.ecommercombud.orgで連絡を取ることができ、又は(800)XXX-XXXX で連絡できます。
2.2　ユーザーの処理のインテグリティ及びそれと関連するセキュリティ義務と、企業のユーザーへの処理のインテグリティ及びそれと関連するセキュリティコミットメントは、承認されたユーザーに伝達されている。	弊社の処理のインテグリティポリシーを定義した、関連したセキュリティポリシーが全ての企業の承認されたユーザーに伝達されます。セキュリティポリシーでは、アクセス権限、情報収集の必要性、責任その他の事項を規定しています。それはレビューされて、年４回の経営会議において更新され、毎年ＩＴ部門によって厳格なレビューを経ています。文書化されたシステムセキュリティ目的、ポリシー及び基準は契約上、法律上その他のSLAで定義されたシステムセキュリティ要件と整合しています。例えば、現行のポリシーは、ＩＤの共有を禁止しています。それぞれのサポート要員がログオンして、ネットワーク装置を保持するために、自身のユニークなＩＤを持っています。アクセス、スクリプティング、更新、リモートアクセスに関係して詳述している完全なポリシーが資格を持った要員によるレビューがなされるようになっており、一般の利用には供しておりません。
2.4　システム処理のインテグリティ問題、エラーと欠落とシステムセキュリティの違反について、企業に通知し、サポートを受けるプロセス、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	サービスその他の情報については、午前７時から午後８時（中部標準時間）の間に(800)XXX-XXXXでお客様サービス担当に連絡してください。又は、下記の宛先に郵送してください。 顧客サービス部 ABC㈱ 〒600-00　イリノイ州某市某通り1234番地 又はCustServ@ABC.com このサイトのインテグリティ又はセキュリティに違反があったと感じられたなら、直ちに(800)XXX-XXXXに電話して弊社と連絡を取ってください。
2.5　システム処理のインテグリティとシステムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されている。	サイトユーザーとしてのあなたに影響を与えるような、弊社のWebサイトのセキュリティとシステムの処理のインテグリティに影響を与えるどんな変更でも、その概要を予測された変更の７日前に電子メールによってあなたに伝達します。その変更は弊社の処理のインテグリティとセキュリティ

規準	開示例
	ポリシーを要約するWebページに概要を表示します。

機密保持

規準	開示例
2.2　ユーザーの機密保持と関連するセキュリティ義務と、企業のユーザーへの機密保持と関連するセキュリティコミットメントは、機密情報が提供される前に承認されたユーザーに伝達されている。このコミュニケーションは下記の事項を含むが、それらに制限されない。	XYZ - manufacturing.comは高品質な電子部品の注文製造業者です。お客様及び潜在的なお客様は弊社のWebサイト又は電子メールを通して設計図、仕様書、製造見積価格の依頼を提出することができます。
a. 情報がどのように機密とされ、機密を解除されるか。機密情報の取扱い、廃棄、維持、保存、バックアップ及び配布又は通信	あなたの情報へのアクセスは、弊社の従業員又は弊社が弊社の見積り作成において利用することに決めるかもしれない第三者に制限されます。弊社は、見積価格と以後の製造以外の目的のために、あなたが提供する情報を利用しませんし、あなたの代理として注文を履行しません。しかしながら、召喚令状、裁判所命令、適用される法律と規則に従うための法的手続又は他の場合に提供する必要があるかもしれません。
b. 機密情報へのアクセスがどのように承認され、無効にされるのか。	弊社の暗号化ソフトウェアを利用して、あなたは「機密取扱い」ボックスをチェックすることによって、機密の情報を指定することもできます。このソフトウェアは弊社のサイトからダウンロードでき、ほとんどのフォーマットで情報を受け入れます。このような情報は自動的にインターネット上への送信前に弊社の公開鍵を使って暗号化されます。あなたは、弊社のWebサイトを通して又は電子メールによって弊社にこのような情報を伝達することもできます。
c. 機密情報がどのように利用されるのか。	「機密」とされた情報へのアクセスは、弊社の知る必要のある従業員にのみ制限されます。弊社は、あなたの事前の許諾なしで第三者にこのような情報を提供しません。
d. 機密情報がどのように共有されるのか。	弊社が第三者に情報を提供するとき、弊社は貴社名を提供しません。しかしながら、弊社は第三者のこのような情報の機密の取扱いについてはいかなる誓約も行いません。
e. 情報が第三者に提供される場合は、開示に当該第三者の機密保持実務及び内部統制に依拠することによっ	弊社の機密保護の期間は２年間であり、２年間の経過後はどの機密情報も依頼によりあなたに返還されるか、廃棄されます。

規準	開示例
て生じる何らかの制限を受けることを含むべきである。そのような開示をしないならば、企業がその機密保持実務及び内部統制に合致するか、又はそれを超えるような第三者の機密保持実務及び内部統制に依拠していることを示していることになる。 f. 機密保持に関して適用される法律と規則に従うための実務	このような情報を提供する時点であなたがまだ弊社のお客様ではなかったなら、あなたにはアカウント番号とパスワードが提供されます。あなたは、あなたが提出した情報、関連して弊社に提供された価格見積情報にアクセスするために、このアカウント番号とパスワードを使うことができます。あなたは、あなたの組織の他の構成員がこの情報にアクセスすることができるように、追加の10のサブアカウントとパスワードを設定することもできます。 弊社のサービス及び機密情報の保護は第三者紛争解決の対象となります。このプロセスは、弊社のWebサイト上の「調停手続」に記述されています。
2.4 機密保持とシステムセキュリティの違反について企業に通知し、苦情を申し立てるプロセスは、承認されたユーザーに伝達されている。	このサイトにおいて述べられている、機密保持ポリシー、弊社の組織についての質問がございましたら、CustServ@XYZ-manufacturing.comに連絡してください。 このサイトにセキュリティ違反があったと感じられましたら、(800)XXX-XXXXに電話してすぐに弊社と連絡を取ってください。
2.5 機密保持とシステムセキュリティに影響を与えるかもしれない変更が、経営者と影響を受けるユーザーに伝達されている。	200X年１月から、弊社は、情報の「秘密」カテゴリーを廃止しました。このような秘密カテゴリーの下で提出された情報は、弊社のコミットメントに従って保護を継続します。

プライバシー

関連する規準については、付録DのGAPPを参照されたい。

付録Ｂ　システム記述例（電子商取引でないシステム）

システム記述の目的は、保証報告書の経営者の記述書又は保証報告書の主題によって対象とされたシステムの境界線を明らかにすることである（この事例では年金処理サービス）。システム記述は、業務責任者の保証の対象となっている特定の原則に関連するポリシーについての企業による伝達の一体化された部分であるべきである。システム記述は保証報告書に常に添付するべきである。

背景

XYZ年金サービス社（XPS社）はニューヨーク州のニューヨークに本拠地を置いて、北アメリカ各地に事業所を有し、XPS社のサービス提供先である年金制度スポンサーのために、年金管理システム（PAS）を管理・運用している。年金制度加入者は年金制度に登録されるXPS社のサービス提供先の従業員である。XPS社は年金関連の活動の記録保持のためにPASを利用する。

システム基盤

PASは専有のクライアントソフトウェア、アプリケーションサーバーとデータベースサーバーを含む３層のアーキテクチャを利用する。

テープカートリッジサイロ、ディスク・ドライブ、レーザー及びインパクトプリンターのような多様な周辺機器が利用されている。

ソフトウェア

PASアプリケーションは、XITD（XYZ社のＩＴ部門）のシステム開発とアプリケーションサポートの区域でプログラムスタッフによって開発された。PASは年金規定に基づいて、加入者の年金拠出及び退職給付の処理を可能にする。PASは加入者、制度スポンサー、税務当局のために、全ての必要とされる報告書を作成する。PASは投資及び関連する取引（購入、販売、配当、利息及びその他の取引）を記録する機能も提供する。取引のバッチ処理が夜間に行われる。

PASはオンラインのデータ入力と報告のリクエストのための機能を提供する。さらに、PASはデジタル、磁気媒体又はファイル伝送で制度スポンサーからの通信基盤を通じた入力を受け入れる。

要員

XPS社は、以下の機能分野における約200名の従業員スタッフを有している。

- 年金管理部門は、年金規定の策定、マスターファイルの保守、PASに対する拠出処理、制度スポンサー及び加入者への報告、制度加入者からの質問対応の専門家チームを含む。
- 財務運用部門は、給付処理、拠出の預託、投資会計に責任がある。
- 信託会計部門は、銀行照合調整に責任がある。
- 投資サービス部門は、株式、債券、預金証書その他の金融商品の購入処理に責任がある。

XITDは、以下の機能分野における約50名のPAS及び関連するシステム基盤に専任するスタッフを有している。

- ヘルプデスクは、制度スポンサーはもちろん、PAS及びその他のシステム基盤

のユーザー技術支援を提供する。
・　システム開発及び管理支援は、PASの改良と修正のためのアプリケーションソフトウェア開発及びテストを提供する。
・　製品サポート専門家は、文書化されたマニュアルと訓練資料を作成する。
・　品質保証は、基準への遵守性をモニターして、変更執行プロセスを管理統制する。
・　情報セキュリティ及びリスクは、セキュリティ管理、侵入検知、セキュリティモニタリング、ビジネス復旧計画に責任がある。
・　運用サービスは、サーバー及び関連する周辺機器の日々の運用を実施する。
・　システムソフトウェアサービスは、システムソフトウェアリリースを導入、テストし、システムパフォーマンスを毎日モニターし、システムソフトウェアの問題を解決する。
・　技術提供サービスは、PAS処理環境に対するジョブスケジューリングを保持し、ソフトウェアの提供を報告し、セキュリティ管理を統括し、ポリシー及び手続マニュアルを維持する。
・　音声及びデータ伝達は、伝達上の問題の解決及びネットワーク計画における伝達環境を保持し、ネットワークを監視し、ユーザー及び制度スポンサーに対する支援を提供する。

手続

このシステム記述によって対象とされる年金管理サービスは以下を含む。
・　年金マスターファイルのメンテナンス
・　拠出
・　給付
・　投資会計
・　加入者への報告

これらのサービスはXYZ社のＩＴ部門（XITD）によって年中無休でサポートされる。XITDによって提供される重要なサポートサービスは以下を含む。
・　システム開発と保守
・　セキュリティ管理と監査
・　侵入検知とインシデント対応
・　データセンター運用とパフォーマンスモニタリング
・　変更管理
・　ビジネス復旧計画

データ

PASにおいて定義されたデータは以下により構成される。
・　マスターファイルデータ
・　取引データ
・　エラー、サスペンスログ
・　出力帳票
・　伝送記録
・　システム及びセキュリティファイル

取引処理は紙の書類、電子媒体又はXYZ社のコールセンターへの電話による受付によって始められる。取引データはオンライン処理ないしバッチ処理のいずれかでPASによって処理され、そしてマスターファイルを更新するために使われる。出力帳票は、職能に基づいて、承認されたユーザーにより、ハードコピーないし報告書閲覧

機能を通じて利用可能である。年金記述書と取引報告書が制度スポンサーと加入者に郵送される。

付録Ｃ　範囲決定及び結論の報告の問題に関する業務責任者への指針

この付録は、Trustサービスの原則と規準を用いた業務の計画、実施、結論の報告に関する問題を取り扱う。このセクションでは、下記の領域を取り扱う。

- 業務の要素
- 保証報告書
- レビュー業務
- 合意された手続業務
- その他の事項

Trustサービス業務は、AICPA証明業務基準書の下で実施される保証業務である。

業務の要素

Trust サービス原則

Trustサービスは、五つの異なる原則（セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシー）を利用した個別適用アプローチを提供している。業務責任者は単一又は複数の原則を結合させて対象としてTrustサービス検証を実施することが可能である。それぞれの原則は、システムの属性（例えば、可用性）を記述しており、当該属性に関してシステムを評価するための規準が続いている。

Trust サービス規準

規準は、主題を測定し表示するために利用される指標である。業務責任者はこれら規準に基づいて主題を評価する。

AICPA職業的基準第１巻ＡＴセクション101「証明業務」[8]では、適合する規準は下記の属性を有しなければならない。

- 客観性：規準に、偏向があってはならない。
- 測定可能性：規準は、主題について、定性的又は定量的に合理的で一貫した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。

Trustサービスの規準は、適合する規準の要件を満たし、かつ、公開されており、意見聴取プロセスを経て作られている。

経営者の記述書

ＡＴセクション101では、通常業務責任者は、経営者から、書面の記述書[9]を入手しなければならず、さもなければ業務責任者は、報告書[10]を修正するように要求されている。具体的には、経営者は、報告書の対象期間にAICPA/CICA Trustサービス規準に基づいて、対象となるTrustサービス原則と規準を充足するように検証対象シス

8　AICPA 職業的基準第１巻ＡＴセクション 101「証明業務」のパラグラフ 24 を参照
9　ＡＴセクション 101 のパラグラフ９を参照
10　書面の記述書が得られなかった場合の業務責任者の記述については、ＡＴセクション101のパラグラフ58を参照

テムに対して、有効な内部統制を保持していることを記述する。特定の原則のみを対象とする業務では、経営者の記述書は業務の対象となる原則のみに対処すべきである。また、企業のコミットメントへの遵守性を対象とする業務では、報告書で対象とされるコミットメントは、経営者の記述書において特定すべきである。

ＡＴセクション101では、業務責任者は、経営者の記述書に対して、又は業務の主題に対してのどちらについて結論を報告してもよい。業務責任者が記述書に対して、結論を報告するときは、経営者の記述書は保証報告書に添付するか、又は保証報告書の第一段落に含められるべきである[11]。業務責任者が主題に対して結論を報告するときは、業務責任者は、経営者に対して、保証報告書の利用者のために利用可能な経営者の記述書を作成することを求めてもよい。単一又はより多くの規準からの逸脱がある場合は、業務責任者は、保証報告書を修正すべきである。修正した保証報告書を発行する場合、業務責任者は、経営者の記述書に対してよりも、主題に対して直接の結論の報告を行うべきである[12]。

対象期間

ＡＴセクション101では、経営者の記述書及び保証報告書は、経営者の記述書及び保証報告書の対象期間をそれぞれ特定すべきである。業務責任者は、特定期間又は特定日対象の報告書を発行することができる。適切な期間の決定は、業務責任者及び企業の判断によるべきである。

保証報告書の対象期間を決定するために留意すべき要因は以下のとおり。

- 保証報告書の想定利用者及びそれらのニーズ
- 保証報告書の対象期間の連続性に関する必要性
- 各システム構成要素の変更の程度及び頻度
- システムにおける処理の循環的特質
- システムに関する履歴情報

保証報告書

委員会は、Trust サービスの原則及び規準に基づいて結論を報告する場合、業務責任者は下記の項目を考慮してもよいとしている。

複数の原則に関する結論の報告

ほとんどのケースでは、業務責任者は、五つの原則全てについてではなく、一つ又はそれ以上のTrustサービス原則について、結論を報告するように依頼されるだろう。業務責任者は、保証報告書の最初の段落において業務範囲に含まれる原則を特定すべきである。

個別又は結合報告書

複数原則について、Trustサービス検証を実施するときは、業務責任者は、クライアントのニーズに基づき、各原則について、個別に報告書を発行することもできるし、又は結合報告書を発行することもできる。この検討の目的としては、業務責任者がクライアントからセキュリティ、プライバシー、機密保持という三つの一連の原則と規準への準拠性について、結論を報告するように依頼されたと仮定しよう。

11　ＡＴセクション 101 のパラグラフ 64 を参照
12　ＡＴセクション 101 のパラグラフ 66 を参照

最初の問題は、(1)三つの原則について一つの業務とするか、(2)個々の原則ごとに三つの業務とするか、を決定することである。これについては、一つの保証報告書を発行するか、複数の保証報告書を発行するか、及び経営者の確認書の数と内容、契約書、その他の事項が影響してくるだろう。どちらのケースでも、保証報告書には業務の範囲及び性格を明確に伝達すべきである。

規準への適合の失敗

もし一つ又はそれ以上の規準に適合しなかった場合、業務責任者は、肯定的結論報告書を発行することができない。ＡＴセクション101では、修正された保証報告書を発行する場合、業務責任者は経営者の記述書に対してよりも主題に対して直接結論を報告すべきである[13]。

異なる検証期間

企業が二つ以上の原則について、検証を依頼した場合、様々な理由により、原則の報告対象期間が異なってくる（報告対象期間の長さや、対象期間の開始日が違うであるなど）こともあり得る。理想的には、業務責任者にとってはそのような期間が一致することが効率的である。異なる期間の保証報告書が存在する場合、業務責任者は、分離して報告するか結合して報告するかを考慮することができる。分離された原則を対象とする分離された保証報告書は、結合された保証報告書よりも複雑性が少ない。結合された保証報告書が発行される場合、異なる報告期間を確実に強調するため、保証報告書の冒頭及び結論の段落に詳述する必要がある。

TPSP(サードパーティーサービスプロバイダ)の利用

業務責任者は、検証対象の企業が、Trustサービス規準の幾つかを達成するために、サードパーティーサービスプロバイダを利用しているという状況に直面することがある。AICPA/CICAの「WebTrust又は類似業務におけるサードパーティーサービスプロバイダの影響」は、当該状況に適用できる指針を提供しており、www.webtrust.orgからダウンロードできる。

他の原則に関連する規準からの逸脱を伝達する実施責任

Trustサービスの検証を行っている間に、例えば当該業務の範囲外の原則と規準に関する準拠性違反や内部統制の欠陥などの、規準からの逸脱についての情報が業務責任者の目にとまるかもしれない。例えば、セキュリティ原則に関連した内部統制に関する結論の報告にしか従事していない場合でも、業務責任者が、企業がWebサイトに掲載したプライバシーポリシーを遵守していない（例えば、個人情報を選定された第三者に提供しているなど）ことに気付くかもしれない。業務責任者は、検証範囲を超えて規準からの逸脱についての情報を発見する責任はないが、そのような情報を探知した場合は、それが重要かどうか（それがシステムの利用者を誤らせるほどに重要か）を評価すべきである。

もし業務責任者がそのような逸脱が重要であると判断した場合、経営者に対して、書面で伝達すべきである。経営者は、その欠陥又は遵守性違反を是正（この場合、第三者への情報提供をやめる。）するか、実際の実務を適切に開示して利用者が実際のポリシーを知ることができるようにすべきである（この場合、プライバシーステートメントについて、情報を第三者に提供している事実を反映するように改訂す

13　ＡＴセクション 101 のパラグラフ 66 を参照

る。）。

もし業務責任者が、この情報の内容の欠落が重要であると結論付け、かつ経営者が逸脱を是正することにもその情報を開示することにも消極的であったら、業務責任者は、業務の解約を検討してもよい。

後発事象

保証報告書で対象とする特定期間又は特定日後保証報告書日の前に、主題や経営者の記述書に重要な影響を与え、そのため主題や経営者の記述書の表示において修正ないしは開示することが必要な事象や取引が、発生することがある。こうした発生の事実は、「後発事象」と呼ばれる。保証業務を実施する際には、業務責任者は、判明し得た後発事象についての情報に留意すべきである。業務責任者が留意しなければならない後発事象には２種類ある。

第一のタイプは、保証報告書で対象とする特定期間又は特定日に存在していた、追加的な情報を提供する事象である。この情報は、後発事象が規準への準拠性において表示されているかどうか、主題、経営者の記述書、保証報告書に影響を与えるかどうかを業務責任者が考慮する際に利用すべきである。

第二のタイプは、保証報告書で対象とする特定期間又は特定日後に発生した、その性質や重要性が主題を誤らせないようにするため開示が必要となる情報を提供する事象である。この種の情報は、適切に開示されていれば、普通は保証報告書に影響を与えない。

業務責任者は、後発事象を検出する責任はないものの、保証報告書日までに主題又は経営者の記述書に対する重要な効果を持つ後発事象に気が付いているかどうかについて、責任ある当事者（クライアントが責任ある当事者でない場合、その関係先）に照会すべきである[14]。経営者確認書は通常、後発事象に関する確認事項を含む。

業務責任者は、保証報告書日後の事象について、逐次情報を得る責任を有していない。しかしながら、もし業務責任者がそれに気付いていたなら、業務責任者は、保証報告書日後に、影響を与えるかもしれないその日付において存在した状態に気付くかもしれない。このような状況では、業務責任者は、AICPA職業的基準第１巻ＡＵセクション561「監査報告書日に存在した事実の事後発見」に留意することが望ましい[15]。

レビュー業務

証明業務基準書に従って実施されるレビュー業務は、業務責任者が、彼らの実施した業務に基づいて、主題が規準に基づいていない（準拠していない）こと又は経営者の記述書が全ての重要な点において規準に基づいて表示されていない（適正に表示されていない）ことを示唆していると思われる情報があったかどうかを報告する保証業務の一つである。一般に、そのようなレビュー業務は、質問と分析的レビュー手続に制限される。そのため、委員会は Trust サービスの原則と規準に従ってシステムの内

14　ある証明基準は業務責任者の後発事象に関する考慮要件を含んでいる。例えば、ＡＴセクション 601 のパラグラフ 50 から 51 とパラグラフ 129 から 134 を参照

15　ＡＴ101 のパラグラフ 95 から 99 を参照

部統制に関して報告する場合、レビュー業務を実施すべきでないと決定した。

合意された手続業務

クライアントは、業務責任者が Trust サービスの原則と規準に関して、合意された手続業務を行うことを要請することがある。このような業務では、業務責任者は、特定の当事者[16]によって合意された特定の手続を行って、発見事項を報告する。当事者のニーズは多様であるかもしれないので、合意された手続の性質、タイミング、範囲も同様に多様である。その結果、特定の当事者が最も良く彼ら自身のニーズを理解しているので、手続の十分性に対して責任を有することが想定される。合意された手続業務では、業務責任者は、経営者の記述書又は主題の検証を実施しない、又は経営者の記述書若しくは主題に対して意見を表明しない。業務責任者の合意された手続についての報告には、手続と発見事項が記載される[17]。合意された手続報告書の利用は、手続について合意した特定の当事者に限定される。

保証報告書の文例

下記は、Trust サービス検証業務のための保証報告書の文例である。文例１から３は、業務責任者が経営者の記述書に対して結論を報告する場合の報告書の例である。文例４及び５は、業務責任者が主題に対して直接結論を報告する場合の報告書の例である。保証報告書の最初のパラグラフは、業務責任者が経営者の記述書に対して、又は、主題に対して直接結論を報告するかどうかを示している。

システムの信頼性のための Trust サービスの原則と規準は、可用性、セキュリティ、処理のインテグリティを含む。さらに、業務責任者が報告をすることのできる四つ目の原則及び一連の規準として機密保持もある。

可用性、処理のインテグリティ、機密保持に関連する Trust サービスの原則と規準は顧客に対して企業が行うコミットメントに関する規準を含む。それらの原則と規準については、クライアントは業務責任者に対して、以下について依頼してもよい。

(1) （コミットメントへの特別の言及を行わない場合の）コミットメントに関する内部統制に関する結論の報告
(2) （文例３で記載するように、コミットメントへの言及を行う場合の）当該コミットメントに対する意見表明及び当該コミットメントに対する企業の遵守性に対する結論の報告

クライアントは結論の報告の対象となっている原則と規準に関連するシステムと内部統制の一覧を含めてもよい。そのような結論の報告に関する保証報告書の文例は、文例５によって示されている。

これらの保証報告書は、例示を目的とするものなので、特定の業務の事実と状況を担保するべく、適用される専門的な基準に従って修正されるべきである。

16　業務責任者が実施すべき手続は特定のユーザーと業務責任者が合意する。
17　合意された手続業務は、AICPA 職業的基準ＡＴセクション 201「合意された手続業務」の下で行われる。

文例１－四つの原則（可用性、セキュリティ、処理のインテグリティ、機密保持）に関連する内部統制の有効性に関する経営者の記述書に対するTrustサービス保証報告書（特定期間対象報告書）

独立した業務責任者のTrustサービス保証報告書

ABC社　代表取締役　殿

当監査法人は、AICPA/CICAのTrustサービスの可用性、セキュリティ、処理のインテグリティ、機密保持の規準に基づいて、×年×月×日から×年×月×日までの期間において、ABC社の○○システム（検証対象システム）が、AICPA/CICAのTrustサービスの可用性、セキュリティ、処理のインテグリティ、機密保持の規準に基づき、下記について合理的な保証を提供するための有効な内部統制を維持していることについて記載された経営者の記述書について検証を行った。

- システムがコミット又は合意されたとおりに運用・利用のために利用可能であったこと。
- システムが（物理、論理双方の）未承認のアクセスに対して保護されていたこと。
- システム処理が完全、正確、タイムリーかつ承認されていたこと。
- 機密とされた情報がコミット又は合意されたとおりにシステムにより保護されていたこと。

この経営者の記述書の作成責任はABC社の経営者にある。当監査法人の責任は当監査法人の実施した手続に基づいて結論を報告することにある。経営者の記述書が対象とする、○○システム（検証対象システム）の各側面に対するシステム記述は添付されている。当監査法人はこのシステム記述について検証しておらず、したがって当監査法人はそれらに対する意見を表明しない。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に準拠して実施され、(1)ABC社の○○システム（検証対象システム）の可用性、セキュリティ、処理のインテグリティ及び機密保持に関する内部統制を理解し、(2)内部統制の有効な運用をテストし評価し、(3)当監査法人が状況により必要と認めたその他の手続を実施したこと、を含んでいる。当監査法人は検証の結果として結論を報告するための合理的な基礎を得たと判断している。

内部統制の固有の限界のため、誤り又は不正、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反が発生し、それらが発見されないことがある。当監査法人の結論から将来を予想することにはリスクがある。

当監査法人は、上記の経営者の記述書がAICPA/CICAのTrustサービスのセキュリティ、可用性、処理のインテグリティ、機密保持の規準に基づいて、全ての重要な点において適正に表示しているものと認める。

［監査法人名］
○○○○監査法人
［住所］
［日付］
［AICPA基準の下で作成されるべき保証報告書文例については注記を参照のこと。］

文例２－システムの信頼性（可用性、セキュリティ、処理のインテグリティ）に関連する内部統制の有効性に関する経営者の記述書に対するTrustサービス保証報告書（特定期間対象報告書）

独立した業務責任者のシステムの信頼性についてのTrustサービス保証報告書

ABC社　代表取締役　殿

当監査法人は、AICPA/CICAのTrustサービスのシステムの信頼性のための可用性、セキュリティ、処理のインテグリティの規準に基づいて、×年×月×日から×年×月×日までの期間において、ABC社の○○システム（検証対象システム）の信頼性に関する内部統制について記載された経営者の記述書について検証を行った。信頼できるシステムは、特定の環境で特定の期間、重要なエラー、失敗、障害なしに運用できるシステムである。経営者の記述書は、「○○システム（検証対象システム）に係る内部統制の有効性に関するABC社の記述書」と題する添付書類に含まれており、下記について記述している。

×年×月×日から×年×月×日までの期間において、ABC社がAICPA/CICAのTrustサービスのシステムの信頼性のための可用性、セキュリティ、処理のインテグリティの規準に基づいて、○○システム（検証対象システム）の可用性、セキュリティ、処理のインテグリティに関して、下記について合理的な保証を提供する有効な内部統制を維持していた。

- システムがコミット又は合意されたとおりに運用・利用のために利用可能であったこと。
- システムが（物理、論理双方の）未承認のアクセスに対して保護されていたこと。
- システム処理が完全、正確、タイムリーかつ承認されていたこと。

添付されたABC社の○○システム（検証対象システム）のシステム記述は、経営者の記述書が対象としている○○システム（検証対象システム）の各側面を識別している。

この経営者の記述書の作成責任はABC社の経営者にある。当監査法人の責任は当監査法人の実施した手続に基づいて結論を報告することにある。経営者の記述書が対象とする、○○システム（検証対象システム）の各側面に対するシステム記述は添付されている。当監査法人はこのシステム記述について検証しておらず、したがって当監査法人はそれらに対する意見を表明しない。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に準拠して実施され、(1)ABC社の○○システム（検証対象システム）の可用性、セキュリティ、処理のインテグリティに関する内部統制を理解し、(2)内部統制の有効な運用をテストし評価し、(3)当監査法人が状況により必要と認めたその他の手続を実施したこと、を含んでいる。当監査法人は検証の結果として結論を報告するための合理的な基礎を得たと判断している。

内部統制の固有の限界のため、誤り又は不正、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反が発生し、それらが発見されないことがある。当監査法人の結論から将来を予想することにはリスクがある。

当監査法人は、上記の経営者の記述書がAICPA/CICAのTrustサービスのシステムの信頼性のための可用性、セキュリティ、処理のインテグリティの規準に基づいて、全ての重要な点において適正に表示しているものと認める。

［監査法人名］
○○○○監査法人
［住所］
［日付］
［AICPA基準の下で作成されるべき保証報告書文例については注記を参照のこと。］

文例３－単一の原則（機密保持）への内部統制の有効性及び遵守性に関する経営者の記述書に対するTrustサービス保証報告書（特定日対象報告書）

独立した業務責任者のTrustサービス保証報告書

ABC社　代表取締役　殿

当監査法人は、AICPA/CICAのTrustサービスの機密保持の規準に基づいて、×年×月×日において、ABC社の○○システム（検証対象システム）が、機密とされる情報をコミット又は合意されたとおりに保護しており、機密とされる情報の保護に関するコミットメントを遵守していたという合理的な保証を提供するための有効な内部統制を維持していることについて記載された経営者の記述書について検証を行った。

この経営者の記述書の作成責任はABC社の経営者にある。当監査法人の責任は当監査法人の実施した手続に基づいて結論を報告することにある。経営者の記述書が対象とする、○○システム（検証対象システム）の各側面に対するシステム記述は添付されている。当監査法人はこのシステム記述について検証しておらず、したがって当監査法人はそれらに対する意見を表明しない。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に準拠して実施され、(1)ABC社の○○システム（検証対象システム）における機密とされた情報の保護に関する内部統制を理解し、(2)内部統制の有効な運用をテストし評価し、(3)機密とされた情報の保護に関するABC社のコミットメントへの遵守性について、テストし、(4)当監査法人が状況により必要と認めたその他の手続を実施したこと、を含んでいる。当監査法人は検証の結果として結論を報告するための合理的な基礎を得たと判断している。

内部統制の固有の限界のため、誤り又は不正、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反が発生し、それらが発見されないことがある。当監査法人の結論から将来を予想することにはリスクがある。

当監査法人は、上記の経営者の記述書がAICPA/CICAのTrustサービスの機密保持の規準に基づいて、全ての重要な点において適正に表示しているものと認める。

［監査法人名］
○○○○監査法人
［住所］
［日付］
［AICPA基準の下で作成されるべき保証報告書文例については注記を参照のこと。］

文例４－システムの信頼性（可用性、セキュリティ、処理のインテグリティ）のためのTrustサービス保証報告書－主題に対する直接の結論の報告（特定期間対象報告書）

独立した業務責任者のシステムの信頼性についてのTrustサービス保証報告書

ABC社　代表取締役　殿

当監査法人は、AICPA/CICAのTrustサービスのシステムの信頼性のための可用性、セキュリティ、処理のインテグリティの規準に基づいて、×年×月×日から×年×月×日までの期間において、ABC社の○○システム（検証対象システム）の内部統制の信頼性に関する内部統制の有効性について検証を行った。信頼できるシステムは、特定の環境で特定の期間、重要なエラー、失敗、障害なしに運用できるシステムである。この内部統制の有効性に係る責任はABC社の経営者にある。当監査法人の責任は、当監査法人の実施した手続に基づいて結論を報告することにある。

添付された経営者の記述書により対象とされたABC社の○○システム（検証対象システム）のシステム記述は、○○システム（検証対象システム）の各側面を識別している。当監査法人はこのシステム記述について検証しておらず、したがって当監査法人はそれらに対する意見を表明しない。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に準拠して実施され、(1)ABC社の○○システム（検証対象システム）の可用性、セキュリティ、処理のインテグリティに関する内部統制を理解し、(2)内部統制の有効な運用をテストし評価し、(3)当監査法人が状況により必要と認めたその他の手続を実施したこと、を含んでいる。当監査法人は検証の結果として結論を報告するための合理的な基礎を得たと判断している。

内部統制の固有の限界のため、誤り又は不正、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反が発生し、それらが発見されないことがある。当監査法人の結論から将来を予想することにはリスクがある。

当監査法人は、ABC社がAICPA/CICAのTrustサービスのシステムの信頼性のための可用性、セキュリティ、処理のインテグリティ規準に基づいて、○○システム（検証対象システム）の信頼性に関して、全ての重要な点において、下記について合理的な保証を提供する有効な内部統制を維持していたものと認める。

- システムがコミット又は合意されたとおりに運用・利用のために利用可能であったこと。
- システムが（物理、論理双方の）未承認のアクセスに対して保護されていたこと。
- ×年×月×日から×年×月×日までの期間において、システム処理が完全、正確、タイムリーかつ承認されていたこと。

［監査法人名］
○○○○監査法人
［住所］
［日付］
［AICPA基準の下で作成されるべき保証報告書文例については注記を参照のこと。］

文例５－単一の原則(セキュリティ)に関する内部統制の有効性に係るTrustサービス保証報告書－主題に対する直接の結論の報告（内部統制を記述した明細書を含む特定期間対象報告書）

独立した業務責任者のTrustサービス保証報告書

ABC社　代表取締役　殿

当監査法人は、AICPA/CICAのTrustサービスのセキュリティの規準に基づいて、×年×月×日から×年×月×日までの期間において、ABC社の○○システム（検証対象システム）の明細書Ｘに記載された内部統制の有効性について検証を行った。この内部統制の有効性に係る責任はABC社の経営者にある。当監査法人の責任は、当監査法人の実施した手続に基づいて結論を報告することにある。

添付された経営者の記述書により対象とされたABC社の○○システム（検証対象システム）のシステム記述は、○○システム（検証対象システム）の各側面を識別している。当監査法人はこのシステム記述について検証しておらず、したがって当監査法人はそれらに対する意見を表明しない。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に準拠して実施され、(1)ABC社の○○システム（検証対象システム）のセキュリティに関する内部統制を理解し、(2)内部統制の有効な運用をテストし評価し、(3)当監査法人が状況により必要と認めたその他の手続を実施したこと、を含んでいる。当監査法人は検証の結果として結論を報告するための合理的な基礎を得たと判断している。

内部統制の固有の限界のため、誤り又は不正、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反が発生し、それらが発見されないことがある。当監査法人の結論から将来を予想することにはリスクがある。

当監査法人は、×年×月×日から×年×月×日までの期間において、AICPA/CICAのTrustサービスのセキュリティ規準に基づいて、ABC社の○○システム（検証対象システム）が（物理、論理双方の）未承認のアクセスに対して保護されていたという合理的な保証を提供するABC社の○○システム（検証対象システム）に関する明細書Ｘで記述された有効な内部統制を全ての重要な点において維持していたものと認める。

［監査法人名］
○○○○監査法人
［住所］
［日付］
［AICPA基準の下で作成されるべき保証報告書文例については注記を参照のこと。］

明細書Ｘ（AICPA/CICAのTrustサービスのセキュリティ規準により検証されるABC社の○○システムのセキュリティに関する内部統制）

システムは（物理、論理双方の）未承認のアクセスに対して保護されている。	
1.0　ポリシー：企業は、システムのセキュリティのためにポリシーを定義して、文書化している。	**内部統制**
1.1　企業のセキュリティポリシーは、特定の個人又はグループによって確立され、定期的にレビューされ、承認されている。	企業の文書化されたシステム開発と調達のプロセスは、システム上の承認されたユーザーとセキュリティ要件を識別して、文書化するための手続を含んでいる。 ユーザー要件がSLA又は他の書類で文書化されている。 セキュリティ責任者は毎年セキュリティポリシーをレビューしている。提案された変更が、ＩＴ基準委員会による承認を必要とされるため、同委員会に提出されている。
1.2　セキュリティポリシーは、下記の事項を含むが、それらに制限されない。 a. 承認されたユーザーのセキュリティ要件の識別と文書化 b. 重要性、機微性（Sensitivity）に基づくデータの分類。分類は保護の必要性、アクセス権限、アクセス制限、維持と廃棄を定義するのに用いられる。 c. 定期的なリスク評価 d. 未承認のアクセスの防止 e. 新規ユーザーの追加、既存ユーザーのアクセスレベルの変更及びアクセスする必要のなくなったユーザーの削除 f. システムセキュリティに対する実施責任と説明責任の割当て g. システム変更と維持管理に対する実施責任と説明責任の割当て h. 導入前のシステム構成要素のテスト、評価、承認 i. セキュリティ問題に関連している苦情と要請がどのように解決されるか。 j. セキュリティ違反その他のインシデントを処理するための手	企業の文書化されたセキュリティポリシーは、左記に列挙された要素を含んでいる。

続 k. システムセキュリティポリシーをサポートする訓練等に必要な経営資源を配分するための規定 l. システムセキュリティポリシーで明示的に扱われない逸脱事項と状況の取扱いのための規定 m. 適用される法規制、定義されたコミットメント、SLAの識別と一致のための規定 n. 第三者との情報共有の提供	
1.3 企業のシステムセキュリティポリシー及びそれらのポリシーの変更・更新に関わる実施責任と説明責任が割り当てられている。	経営者は最高情報責任者(CIO)に、企業のセキュリティポリシーの維持と施行に関する責任を割り当てている。役員会の他の人たちが、役員会のハンドブックに示されたポリシーのレビュー、更新と承認について支援する。 重要な情報資源（例えば、データ、プログラムと取引）の所有と管理及び、当該資源の上にセキュリティを確立して、維持するための実施責任が定義されている。

この明細書は、例示のみが目的であり、セキュリティ原則の全ての規準を含んでいない。業務責任者が二つ以上の原則について、結論を報告するときは、適切な規準及び内部統制を明確にするため類似の様式を用いることになる。業務責任者は、必ずしもこの様式の形式に拘束されず、他の代替的な形式によってもよい。

付録D　一般に公正妥当と認められたプライバシー原則

この文書が公表された時点では、一般に公正妥当と認められたプライバシー原則（GAPP）は改訂中である。GAPP の最新のバージョンをダウンロードするには、以下を参照

http://www.infotech.aicpa.org/Resources/Privacy/Genelrally+Accepted+Privacy+Principles/

以　上