IRCAブリーフィングノート:
ISO/IEC 20000-1:2011

IRCA
INTERNATIONAL
REGISTER OF
CERTIFICATED
AUDITORS

目次

IRCAブリーフィングノート: ISO/IEC 20000-1:2011

序文

国際審査員登録機関（IRCA）は、IRCA登録審査員、IRCA認定トレーニング機関及びその他の関係者の皆様とISO/IEC 20000-1:2011に対するIRCAの理解についてコミュニケーションを図るため、このブリーフィングノートを作成致しました。

本ブリーフィングノートの内容は、善意にてIRCAの意見をご提供するものです。従って、営利目的での複製や使用は望ましくありません。また、IRCA登録審査員及びIRCA認定トレーニング機関の皆様は、ISO/IEC 20000-1:2011規格に精通している必要があります。

2005年に最初の規格が発行されて以来、ITサービスの提供及びその基礎であるサービスマネジメントシステム（SMS）の開発は大幅な成長を続けてきました。業界は社内における情報システムの利用、企業情報システムのアウトソーシングから発展し、今や消費者を取り込んだ一般的かつ実用的なITサービスの提供へと変化しています。このような発展とともにITIL のような慣行及び方法論も生まれています。 同様に、ISO/IEC 20000-1:2011要求事項及び適合性の管理もこのような状況に対応すべく変化しています。

また2011年版への改訂により、他のマネジメントシステム規格、特にISO 9001:2008「品質マネジメントシステム - 要求事項」及びISO/IEC 27001:2005「情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項」との整合性が強化されたことで利便性が向上し、「ビジネスマネジメントシステム」として多分野を統合、プロセスを基礎としたアプローチの実施が可能になりました。

ISO/IEC 20000-1:2011への改訂を相当な変更であると思われる方もいれば既に実施されているグッドプラクティスを主にとらえたものであるとお考えの方もあるでしょう。IRCAは、ISO/IEC 20000-1:2011の発行により、ITサービスマネジメントシステム実施組織及びITサービスマネジメントシステムの審査を実施する必要のある組織に、自らの慣行を再評価し、改善の機会を明確にする機会が与えられると考えております。

概要

ITサービスマネジメントシステム（ITSMS）を実施、または適合性評価を行う際に足かせとなっていたのは、ISO/IEC 20000-1:2005にはいくつの「プロセス」が義務付けられているのかという問題でした。「プロセス」に関する記述は、審査員による解釈や受審側との合意が必要となるような言い回しで表現されているものも多数ありました。

このような「プロセス」の要求事項の多くは、ISO/IEC 20000-1:2011では明確な「文書化された手順」の義務づけという形に全体を通じて置き換えられました。多くの要求事項が簡潔な最低限度の文言で規定され、見直しの際の明確性、意図の理解、適合した実施への支援性が向上しました。適合性要求事項の変更の程度の指標として、以下に注目してみたいと思います。

- ISO/IEC 20000-1:2005には171の‘shall’
- ISO/IEC 20000-1:2011には257の‘shall’（約50%増加）

また今回の改訂により、他のマネジメントシステム規格、特にISO 9001:2008「品質マネジメントシステム」及びISO/IEC 27001:2005「情報セキュリティマネジメントシステム」との整合性が強化されました。これらの規格での経験が豊富な審査員は、共通のテーマや用語を既に熟知していることでしょう。しかし、ISO/IEC 20000-1:2005規格しか経験していない審査員は改訂版規格を入念に見直し、改訂された適合性要求事項を適切に理解しなければならないかもしれません。

レビューの詳細

ISO/IEC 20000-1:2005では、多くの箇条文が（「一般」または「バックグラウンド」という標題の箇条でなくても）その箇条の目的の記述から始まっています。 ISO/IEC 20000-1:2011ではこのような表現は削除されています。

1. 適用範囲

このセクションは、サービスマネジメントシステムのライフサイクル全体に本規格を適用できることを確認するためのものです。

1.1 a)からf)に記述されている一般的な使用事例は、ISO/IEC 20000-1:2005の記述を元に発展させたもので、サービス提供者、提供者からのサービスを求めている組織、適合性評価者または審査員のイメージを明確にすることを目的としています。

図 2 の サービスマネジメントシステム図は、ISO/IEC 20000-1:2011の各要素の関係をより確実に見るためのものです。最も特筆すべきは、顧客及び他の利害関係者との関係が追加されたことです。サービスマネジメントシステムの要求事項と新規サービス又はサービス変更の設計及び移行が図に追加され、これらの位置付けやサービス提供プロセス、解決プロセス、関係プロセス及び統合的制御プロセスとの関係が明示されています。また、リリース及び展開管理が統合的制御プロセスのカテゴリーに組み込まれています。

箇条1.2 適用が追加され、適合への要求事項がさらに明確

に文書化されました。ここでは、サービス提供の部分（箇条5から9）は第三者によって提供される可能性があり、そのようなソースからのプロセスガバナンスの証拠も許容されることが認められています。しかし、箇条4に規定されているサービスマネジメントの責任、サービス提供に関与する第三者のガバナンス、文書管理、資源の運用管理及びサービスの確立、改善についてはサービス提供者自身が証拠を示さなければなりません。箇条4の条項の内容で、第三者に委託または請け負わせることができるものはありません。ISO/IEC TR 20000-3には、第三者が運用するプロセスのガバナンスについてのさらに詳細な説明を含め、適用範囲の定義及び適用可能性に関する追加ガイダンスが記載されています。

2. 引用規格

本項には引用規格は何も挙げられていません。つまり、この箇条はISO/IEC 20000-2と箇条番号を一致させる目的で設定されています。

3. 用語及び定義

ISO/IEC 20000-1:2005では15の用語が規定されていたのに対し、ISO/IEC 20000-1:2011では37の用語が規定されています。この技術的改訂に関して予測されていた通り、追加された用語の多くはISO 9000:2005「品質マネジメントシステム - 基本及び用語」、ISO/IEC 27000:2009「情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 概要及び用語」から採用または適用されたものであり、その他の追加用語はITIL v3との整合性を図るために追加されたものです（但し、ISO/IEC 20000-1:2011は他のあらゆる実践規範や規格等の方法論から独立しています）。
例えば、箇条3.11では情報セキュリティは「情報の機密性、完全性及びアクセス性を維持すること」と定義されています。「アクセス性」は「可用性」という用語を用いているISO/IEC 27000:2009規格とは整合していません。しかし、ISO/IEC 20000-1:2011の「アクセス性」は既にこの規格の3.1項に定義されている「（ITサービスの）可用性」 との衝突を避けるために用いられているのです。
他のマネジメントシステム規格の用語との整合性が向上したことにより、複数の分野が統合された、プロセスを基礎としたアプローチがより容易になります。但し、適合性審査の実施に先立ち、規定された用語を詳細に見直し、いくつかの採用された用語の「特質」について確実な共通理解を図るよう配慮する必要があります。

4. サービスマネジメントシステムの一般要求事項

「マネジメントシステムの要求事項」を規定する際に箇条4を利用することで、他のマネジメントシステム、特にISO 9001:2008及びISO/IEC 27001:2005との調整を強化することができます。
本規格の箇条 4 はISO/IEC 20000-1:2005の箇条3及び4を拡張発展させたもので、ISO 9001によって確立された成熟したマネジメントシステム原理が本規格に導入されています。 しかし、これは同一条件の下での適用ではありません。 要求事項及び用語はお馴染みのものかもしれませんが、附属書 Aに概要が示されているように、本規格の箇条4は多くのISO 9001（及び、同様にISO/IEC 27001）の箇条の同等の要素を取り込んだものです。
4.1 経営者の責任はISO/IEC 20000-1:2005の箇条3.1を徹底的に手直ししたもので、多くの追加要求事項が導入されています。経営者のコミットメント、方針の運営管理、責任及び権限が規定され、管理責任者の要求事項がより詳細に規定されています。
供給者管理の箇条については、ISO/IEC 20000-1:2005では、サービス提供を供給者に依存している組織の適合性を審査する際「供給者」という用語について相互の合意が必要でした（「供給者」は規格内では定義されておらず、箇条7.2の図 3は外部供給者のみを考慮することを意図したものでした）。 ISO/IEC 20000-1:2011では箇条4.2 第三者が運用するプロセスのガバナンスを導入し、首尾良いサービス提供への貢献に関与する第三者の範囲を認識、明確化しています（サービス提供者を支援する内部のグループ、外部供給者又は顧客による貢献）。さらに、箇条 1.2の「サービス提供者は、箇条4の要求事項について、第三者が運用するプロセスのガバナンスの証拠のみに依存することができない」という規定を思い出して下さい。規格に適合するめには、サービス提供者は関与しているサービス提供の依存とガバナンスの範囲の両方を実証しなければならないのです。ISO/IEC TR 20000-3では、第三者が運用するプロセスのガバナンスに関するさらなる指針が提供されています。

箇条 4.3 ドキュメンテーション・マネジメント では、SMSのための文書類についてより厳密に規定し、正式な文書及び記録の管理を導入しています。注目すべきは、サービスレベル合意書（SLA）から独立した文書として「サービスの目録」を文書化するという明確な要求事項が追加されたことです。この基本文書は箇条 6.1 サービスレベル管理に規定されたサービス設計及びその目的をサポートするものとして再度登場します。

4.4 資源の運用管理ではSMSにおける「資源」の定義を明確化（箇条2からは削除）して「人、技術、情報及び財務に関する資源」とし、このような資源の決定及び提供の適合性要求事項とともに規定しています。

4.5 SMSの確立及び改善は ISO/IEC 20000-1:2005の箇条4を基に手直しが加えられています。原則及び構造のアウトラインは保持されていますが、多くの曖昧な点及び解釈を全体的に削除し数多くの詳細な要求事項の変更を行った結果、より一貫性のある適用が可能になりました。例えば、サービスマネジメントの計画では ISO/IEC 27001情報セキュリティマネジメントシステム取り消しの要求事項に合わせ、「含むか、参照する」「法令・規制要求事項」「リスク受容基準」といった表現が採用されています。
このような広範囲で詳細な再開発の結果、改訂後の新たな適合性要求事項に精通し、理解するためには箇条4を徹底的にレビューしなければならなくなりました。

5. 新規サービス又はサービス変更の設計及び移行

改訂版規格ではISO/IEC 20000-1:2005の箇条5に規定されている規範及び要求事項に手直しが加えられ、内容が拡張されました。
箇条 5.1 では最初に管理すべきプロセスとして変更管理に再び焦点が当てられています。新規サービス又はサービス変更についての計画立案及び設計活動に関し、提案された変更が却下される可能性があることを認識しつつ、本箇条ではサービス提供者は承認された変更が新規サービス又はサービス変更を効果的に満たしていることを確実にするために「必要な処置を取らなければならない」ことを明確にしています（変更後の有効性の監視及びレビューについての間接的な適合性要求事項は箇条9.2により明確に規定されています）。
箇条 5.2及び 5.3には、新規サービス又はサービス変更の計画取り消し、設計及び開発の要求事項が包括的に列挙されており、「廃止される」（延期、終了又は撤退）サービス及びサービスコンポーネントの提供に貢献する第三者へ

の依存についての考慮に関する具体的な要求事項が含まれています。
5.4 新規サービス又はサービス変更の移行では、サービスを稼働環境に展開し、期待される成果に照らして展開後のレビューを実施するため、サービス提供者に対する展開前のサービス試験の要求事項及び利害関係者との受け入れ基準に関する事前合意、承認された新規サービス又はサービス変更を稼働環境へ展開するために、リリース及び展開管理を使用することについて再度規定されています。

6. サービス提供プロセス

本箇条の全体的な構成及び目的に変更はありません。但し、詳細にレビューを実施した結果、ISO/IEC 20000-1:2005での記述を明確化及び改良した多くの適合性要求事項が追加されていることが分かりました。より重大な変更を以下に挙げます。

箇条 6.1 サービスレベル管理には2つの留意すべき変更があります。
まず、各サービスについて一つ以上のSLAの中で規定し、合意し、文書化するというISO/IEC 20000-1:2005での要求事項が更新されました。ISO/IEC 20000-1:2011では、顧客は提供者のITサービスのポートフォリオについて契約を締結する可能性があること、またそれらを「サービスとサービスコンポーネントの依存関係」を含めた顧客向けのサービスの目録の中で規定しなければならないとしています。さらに、「提供する各サービスについて、一つ以上のSLA」が追加されています。
もうひとつの変更は、第三者が運用するプロセスのガバナンス (箇条 4.2)を反映したものです。供給者管理（後出の箇条7.2にて説明）との違いは、箇条6.1の最後のパラグラフは「内部グループ又は顧客が提供するサービスコンポーネント」へのガバナンス要求事項を必須のものとして定めています。

箇条 6.2 サービスの報告も基本的に大幅な変更はありませんが、サービス報告書のコンテキストと内容 についての適合性要求事項がより規定的になりました。

6.3 サービス継続及び可用性管理は拡張され、以下のような明確な適合性要求事項を伴う3つのサブ箇条に論理的な形で再構築されています。

箇条 6.3.1 サービス継続及び可用性取り消し要求事項では、サービス継続及び可用性に対するリスク評価に再度注目し、「顧客」及び他の利害関係者と要求事項について特定及び合意することを最初のステップとしています。但し、様々な顧客に標準化されたサービスを提供しているサービス提供者の適合性を評価する際には、そのサービスの継続及び可用性に対するリスク評価を行い、契約前のサービス仕様の一部としてサービスレベルの目標についてコミットし、SLAが顧客に提供されていることを確認します。また、取り消し契約にはそのような規定されたサービス継続及び可用性へのコミットメントについての顧客の合意が要素として含まれることになります。

6.3.2 サービス継続及び可用性の計画の箇条では、サービス継続及び可用性管理のリスクを基礎とした性質と矛盾するため、以前の「全ての状況において合意された要求事項が満たされることを確実にする」という要求事項がなくなりました。 本箇条には、サービス継続計画及びサービス可用性計画の内容が「これらの計画は1つの文書に統合してもよい」という注記とともに規定されています。

6.3.3 サービス継続及び可用性の監視及び試験の箇条からは、「少なくとも年1回」計画を見直すという要求事項が削除されました。本規格では、計画の試験後又はサービス継続計画の発動後における見直しを義務付けるためのイベント駆動型のアプローチを採用しています。旧版と同様、「サービス環境に重大な変更があった場合、サービス継続及び可用性計画を再度試験」しなければなりません。さらに、継続及び可用性要求事項に照らして試験を実施し、結果を記録及びレビューし、必要な処置を取り、取った処置について報告します。

6.4 サービスの予算業務及び会計業務はほとんど変更されていませんが、レイアウトが改訂され、言い回しが明確になりました。特筆すべきは、「サービスプロセスのための予算業務及び会計業務と、その他の財務管理プロセスとの間に、定義されたインターフェースをもたなければならない」という要求事項が追加されたことです。

同様に、6.5 容量・能力管理 にもわずかな変更点があるものの、基本的には旧版規格が踏襲されています。管理すべき資源の範囲として挙げられているのは「人、技術、情報及び財務に関する資源」です。さらに、要求された結果を満足することを義務付けるような言い回しになるよう、以下のように文言が多少変更されています。

- ISO/IEC 20000-1:2005では「サービスの容量・能力を監視し、サービスパフォーマンスを調整し、適切な容量・能力を提供するための方法、手順及び技法を明確にしなければならない」と規定されていました。この文言の解釈で議論となったのは、提供者が「適切な容量・能力を提供する」ための「方法、手順及び技法」の使用に実際にコミットすることなしにそのような「方法、手順及び技法」を特定するだけで良いと取られかねない点です。
- ISO/IEC 20000-1:2011は、実に明確に「サービス提供者は、合意した容量・能力及びパフォーマンスの要求事項を満たすために、十分な容量・能力を提供しなければならない」ことを要求しています。

6.6 情報セキュリティ管理には手直しが加えられ、ISO/IEC 27001との整合性が向上しました。情報セキュリティ基本方針、[情報セキュリティ]管理策及び変更とインシデントの管理を網羅した複数の箇条に分割されました。

新しい基本方針及び管理策の要求事項はISO/IEC 27001と比べて少ないように見えますが、ISO/IEC20000規格の2005年版と比べてより規定的になったことで、ISO/IEC 27001に適合した情報セキュリティマネジメントシステムを実施していない組織にとってはハードルの高いものとなりました。
これに比べ、情報セキュリティ管理を既存の変更管理、インシデント管理及び改善プロセスに統合するために全体的に見て2005年版を踏襲しているため、6.6.3 情報セキュリティ変更及びインシデントの箇条はそれほど高いハードルではないようです。

7. 関係プロセス

いくつかの細かい変更はありますが、本箇条の全体的な構成及び内容は変更されていません。

7.1 顧客関係管理はより顧客を重視したものとなり、他の利害関係者との関係については規定が少なくなりました。ISO/IEC 20000-1:2005で規定されていた「毎年のサービスレビュー」は、改訂版では抽象的な「コミュニケーシ

ョンの仕組み」という言い回しに置き換わり、年次レビューから事業上の必要性にマッチした継続的な「需要に応じた」レビュー まで、様々な設定が可能になりました。コミュニケーションの目的は規定されているものの、言い回しは少々抽象的で、「サービスを運用する 事業環境及び新規サービス又はサービス変更に対する要求事項の[相互]理解を促進するため」と解釈するのが妥当でしょう。これにより、例えば以下のようなことが可能になるでしょう。

- サービス供給者が顧客の事業及び事業環境、及び顧客からの変更要求をたゆみなく認識する
- サービス供給者が自らの戦略的及び商業的環境に対応し、多くの顧客に提供している一般的なサービスの要素を改善、調整又は置換する

顧客苦情管理の要求事項に変更はありませんが、顧客満足については2011年版では現実に即した視点からの規定がなされており、「顧客及びサービスの利用者の代表サンプルに基づいた」測定及び分析が可能になりました。

7.2 供給者管理には、供給者との契約に含まれなければならない、または参照されなければならない要素のリストが文書化され規定されています。

ISO/IEC 20000-1:2005に規定されていた毎年の「[供給者との]契約又は正式な合意の主要な見直し」は、改訂版では「あらかじめ定めた間隔で供給者のパフォーマンスを監視する」というより受動的な要求事項に置き換えられました。

特に留意すべきは、2つの「プロセス」要求事項が以下のように変更されたことです。

- 「契約の終了、及び他の関係者へのサービスの移管に関する活動及び責任」について規定又は参照するための供給者との契約の要求事項。移管又は終了の必要性が発生する前に、事前に対応し、文書化することを確実にします。
- 「契約上の紛争を管理するための文書化された手順」の要求事項

8. 解決プロセス

8.1 インシデント及びサービス要求管理では、多くの組織が一つの 顧客向けユニット及び一つの共通プロセスを通じてインシデント報告及びサービス変更要求を処理しているという現在の慣行が認識されています。本規格では、サービス要求の管理は変更管理の箇条から本箇条に移動しています。

インシデント及びサービス要求の管理プロセスについては、記録作成から終了に至るまで、インシデント及びサービス要求のライフサイクル管理を2つの別々の手順書で規定することが規格で要求されています。また、リリース及び展開管理プロセスからの情報を含め、プロセスを実施する要員が情報を入手できなければならないとされています。

最後のパラグラフには、文書化された手順を用いて重大なインシデントを管理する方法が規定されています。

8.2 問題管理 はほとんど変更されていませんが、レイアウトが改訂され、言い回しが明確になりました。特筆すべき改善の一つは、全ての問題が恒久的に解決可能なわけではないということ、そして商業的、技術的又は外部からの制約によりその発生を防げる可能性を明確に認めていることです。 改訂版の箇条には「根本原因が特定されたが、問題が恒久的に解決されていない場合、サービス提供者はその問題がサービスに及ぼす影響を低減又は除去するための処置を特定しなければならない」と記述されています。

9. 統合的制御プロセス

構成及び変更管理の箇条は、2011年版ではより明確に規定されています。

9.1 構成管理の要求事項については、以下が変更されました。

- CMDB内の各CIについての最小限必要な情報フィールド
- 資産 - リスクを基礎とした制御を考慮した、CIの版を記録、制御及び追跡するための文書化された手順
- CMDBに記録されているCIの原本は、構成記録が参照している、セキュリティが保たれた物理的又は電子的な格納庫に収納しなければならない
- CMDBに保管されている記録のあらかじめ定められた間隔での監査

9.2 変更管理 の要求事項については、以下が変更されました。

- 最小限の変更管理方針の内容
- サービスの削除又は移管は、重大な影響を及ぼす可能性のあるサービス変更として分類されなければならない
- 変更要求を記録し、分類し、承認する文書化された手順
- 緊急変更を管理する文書化された手順

変更要求管理の要求事項は、以下の通りより厳格なものになりました。

- 「サービス又は顧客に重大な影響を及ぼす可能性があるとして分類された変更要求は、新規サービス又はサービス変更のプロセスの設計又は移行を用いて管理しなければならない。変更管理方針で定義された、CIに対する他のすべての変更要求は、変更管理プロセスを用いて管理しなければならない。」
- 「サービス提供者及び利害関係者は、変更要求の受け入れについて決定しなければならない」
- 失敗した変更を元に戻す、又は修正するために必要な活動を計画し、可能な場合は試験しなければならない」
- 「サービス提供者は、有効性について変更をレビューし」（ISO/IEC 20000-1:2005では単に「成功のためには変更をレビューしなければならない」と規定されています）

9.3 リリース及び展開管理は、改訂版では制御プロセスの一つとして認識されており、全体的な目的及び内容に変更は無いものの、いくつかの細かい変更がなされています。特筆すべき追加要求事項は以下の通りです。
改訂版では変更管理プロセスを用いて展開計画を調整するための明確な要求事項が規定されており、関連する変更要求、既知の誤り及びリリースによって終了する問題を含めなければならないとしています。また、計画の立案には各リリースの展開の日付、成果物及び展開方法を含めなければならないとしています。
緊急のリリースの定義は文書化し、リリースは緊急変更手順とのインターフェースが図られている文書化された手順に従って管理されなければなりません。
各リリースの受け入れ基準について、顧客及び利害関係者と合意しなければなりません。展開前に、リリースは合意した受け入れ基準に従って検証し、承認しなければなりません。受け入れ基準を満たしていない場合には、顧客及び利害関係者は進捗に必要な処置の決定に関与しなければなりません。

附属書 A
ISO 9001及び ISO/IEC 27001と比較したサービスマネジメントシステムの一般要求事項

ISO/IEC 20000:2011	ISO 9001:2008	ISO/IEC 27001:2005
4.1 経営者の責任	5 経営者の責任	5 経営陣の責任
4.1.1 経営者のコミットメント	5.1 経営者のコミットメント	5.1 経営陣のコミットメント
4.1.2 サービスマネジメント方針	5.3 品質方針	4.2.1 b) ISMS基本方針を定義する...
4.1.3 権限、責任及びコミュニケーション	5.5 責任、権限及びコミュニケーション	5.1 c) 情報セキュリティのための役割及び責任を確立、及び附属書 Aの管理策 A.6.1.2 (おおよその相関)
4.1.4 管理責任者	5.5.2 管理責任者	5.1 c) 情報セキュリティのための役割及び責任を確立、及び附属書 Aの管理策1 A.6.1.1 & A.6.1.2 (おおよその相関)
4.2 第三者が運用するプロセスのガバナンス	7.4 購買 (おおよその相関)	複数の附属書Aの管理策1, 特に A.6.1.2 ~ A.6.1.6 及びA.6.2 (おおよその相関)
4.3 ドキュメンテーション・マネジメント	4.2 文書化に関する要求事項	4.3 文書化に関する要求事項
4.3.1 文書の作成及び維持	4.2.1 一般	4.3.1 一般
4.3.2 文書管理	4.2.3 文書の管理	4.3.2 文書管理
4.3.3 記録の管理	4.2.4 記録の管理	4.3.3 記録の管理
4.4 資源の運用管理	6 資源の運用管理	5.2 経営資源の運用管理
4.4.1 資源の提供	6.1 資源の提供	5.2.1 経営資源の提供
4.4.2 人的資源	6.2 人的資源	5.2.2 教育・訓練、意識向上及び力量
4.5 SMSの確立及び改善	複数の引用（以下の通り）	4.2 ISMSの確立及び運営管理
4.5.1 適用範囲の定義	4.2.2 a) 品質マニュアル – QMS の適用範囲の定義	4.2.1 a) ISMSの適用範囲及び境界を定義する
4.5.2 SMSの計画 (Plan)	5.4.2 品質マネジメントシステムの計画	4.2.1 b) ISMS基本方針の定義~j) 適用宣言書の作成 (おおよその相関)
4.5.3 SMSの導入及び運用 (Do)	4.1 一般要求事項 (おおよその相関)	4.2.2 ISMSの導入及び運用
4.5.4 SMSの監視及びレビュー (Check)	5.6 マネジメントレビュー	4.2.3 ISMSの監視及びレビュー
4.5.4.1 一般	8.1 測定、分析及び改善 - 一般	4.2.3 ISMSの監視及びレビュー
4.5.4.2 内部監査	8.2.2 内部監査	6 ISMS内部監査
4.5.4.3 マネジメントレビュー	5.6 マネジメントレビュー	7 ISMSのマネジメントレビュー
4.5.5 SMSの維持及び改善 (Act)	8.5 改善	8 ISMSの改善
4.5.5.1 一般	8.5.1 継続的改善	8.1 継続的改善
4.5.5.2 改善の管理	5.6 マネジメントレビュー	7 ISMSのマネジメントレビュー　4.2.1 d) リスクの特定~ i) 経営陣の許可の取得により補足 (おおよその相関)

1. ISO/IEC 27001:2005に適合するためには規格の附属書Aの全ての目的及び管理策を実施する必要はありません。なぜなら目的及び管理策は情報セキュリティマネジメントシステムの規定された適用範囲に基づいて選択されるからです。但し、A.6.1の管理目的及び管理策の除外が正当化されることはほとんどありません。

International Register of Certificated Auditors (IRCA)
2nd Floor North
Chancery Exchange
10 Furnival Street
London EC4A 1AB
United Kingdom

Email: irca@irca.org
Tel: +44 (0) 20 7245 6833
Fax: +44 (0) 20 7245 6755

IRCA
INTERNATIONAL REGISTER OF CERTIFICATED AUDITORS