2022 年 11 月 01 日

「情報セキュリティマネジメントシステム認証ガイド」の改定のお知らせ

「情報セキュリティマネジメントシステム認証ガイド」を下記の通り改定しましたのでお知らせします。

記

1. 対象文書

GI00001　情報セキュリティマネジメントシステム認証ガイド

2. 版及び改定年月日

版:R33

改定年月日:2022 年 11 月 01 日

3. 主な改定内容の概要

初回審査、サーベイランス審査、再認証審査に於ける、審査報告書（暫定版）の顧客への提出納期変更

変更前：審査終了日

変更後：審査終了後２週間以内

4. 主な改訂理由

審査終了日に審査報告書（暫定版）を提出することが困難なケースに対応するため。

5. 改定内容及び改定理由の詳細

添付の「情報セキュリティマネジメントシステム認証ガイド新旧対照表」(P2/3、P3/3）の通りです。

以　上

頁	新	旧	変更理由
21	**第４章　初回審査** **４．２．２．８　初回１審査報告書の作成** (1)　初回１チーム・リーダーは、初回１終了後、顧客を離れる前に、初回審査・第１段階　審査報告書(暫定版)に関する情報を顧客に提示し、顧客の意見を求めます。審査報告書（暫定版）は、最終会議終了後２週間以内に提出します。 (2)　作成した「懸念領域指摘書／回答書／解決確認書」は、顧客を離れる前に提出します。電子データも同時に配布します。 **４．２．２．９　懸念領域の解決** (1)「懸念領域指摘書／回答書／解決確認書」を受領しましたら、 懸念領域の解決をしていただきます。	**第４章　初回審査** **４．２．２．８　第１段階　審査報告書の作成** (1)　初回１チーム・リーダーは、初回１終了後、顧客を離れる前に、初回審査・第１段階　審査報告書(暫定版)を作成し、顧客に提出し、報告書に対する顧客の意見を求めます。「懸念領域指摘書／回答書／解決確認書」の電子データも同時に配布します。 **４．２．２．９　懸念領域の解決** (1)「審査報告書（暫定版）」を受領しましたら、懸念領域がある場合懸念領域の解決をしていただきます。	前頁４項参照
23	**第４章　初回審査** **４．２．３．５　第２段階　審査報告書の作成** (1)　初回２チーム・リーダーは、初回２終了後、顧客を離れる前に、初回審査　審査報告書(暫定版)に関する情報を顧客に提示し、顧客の意見を求めます。初回審査　審査報告書（暫定版）は、最終会議終了後２週間以内に提出します。 (2)　作成した「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」は、顧客を離れる前に提出します。電子データも同時に配布します。	**第４章　初回審査** **４．２．３．５　第２段階　審査報告書の作成** (1)　初回２チーム・リーダーは、初回２終了後、顧客を離れる前に、初回審査　審査報告書(暫定版)を作成し、顧客に提出し、報告書に対する顧客の意見を求めます。「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」の電子データも同時に配布します。	同上
29	**第５章　サーベイランス審査** **５．２．２．６　サーベイランス審査報告書の作成** (1)　サーベイランス審査チーム・リーダーは、サーベイランス審査終了後、顧客を離れる前に、サーベイランス審査審査報告書(暫定版)に関する情報を顧客に提示し、顧客の意見を求めます。サーベイランス審査　審査報告書(暫定版)は、最終会議終了後２週間以内に提出します。 (2)　作成した「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」は、顧客を離れる前に提出します。電子データも同時に配布します。	**第５章　サーベイランス審査** **５．２．２．６　サーベイランス審査報告書の作成** (1)　サーベイランス審査チーム・リーダーは、サーベイランス審査終了後、顧客を離れる前に、サーベイランス審査審査報告書(暫定版)を作成し、顧客に提出し、報告書に対する顧客の意見を求めます。「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」の電子データも同時に配布します。	同上

頁	新	旧	変更理由
34	**第６章　再認証審査** **６．２．３　再認証審査報告書の作成** (1)　再認証審査チーム・リーダーは、再認証審査終了後、顧客を離れる前に、再認証審査　審査報告書(暫定版)に関する情報を顧客に提示し、顧客の意見を求めます。再認証審査　審査報告書(暫定版)は、最終会議終了後２週間以内に提出します。 (2)「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」は、顧客を離れる前に提出します。電子データも同時に配布します。	**第６章　再認証審査** **６．２．３　再認証審査報告書の作成** (1)　再認証審査チーム・リーダーは、再認証審査終了後、顧客を離れる前に、再認証審査　審査報告書(暫定版)を作成し、顧客に提出し、報告書に対する顧客の意見を求めます。 (2)「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」の電子データも同時に配布します。	同上

情報セキュリティマネジメントシステム
認証ガイド

公益財団法人 防衛基盤整備協会

システム審査センター

＜目　次＞

第１章　総　則

1.１　ガイドの目的

このガイドは、公益財団法人 防衛基盤整備協会 システム審査センター（以下「ＢＳＫ」という。）における下記のマネジメントシステムの認証に関する認証要求事項、認証活動及び審査の手順（プロセス）、並びに顧客（認証提供の依頼者／申請組織／受審組織／被認証組織（共同事業所※を含む））が遵守すべき事項について規定したものです。

※共同事業所：被認証組織内において同一マニュアルで管理される他組織の事業所

① JIS Q 27001　情報セキュリティマネジメントシステム（ISMS）

備考：本ガイドでは、認証機関から見た、認証提供の依頼者、申請組織、受審組織及び被認証組織を、特に必要な場合を除き、顧客と表現します。

1.２　用語の定義

このガイドで使用する用語の定義は、適用される規格に基づいています。

また、必要に応じて、下記の規格を参照してください。

① JIS Q 9000 「品質マネジメントシステムー基本及び用語」
② JIS Q 17000「適合性評価ー用語及び一般原則」
③ JIS Q 19011「品質及び／又は環境マネジメントシステム監査のため指針」
④ JIS Q 27000「情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー用語」

なお、審査工数計算の基礎として使用する「対象従業員数（有効要員数）」、「一時的サイト」については、下記によります。

・経営者、役員を含め、組織の認証範囲の活動に関わる従業員、パートタイム勤務者、派遣社員等の人数（パートタイム勤務者は、勤務時間に応じた人数に減じてよい）
・一時的サイトは、限定された期間内に、特定の業務又はサービスを提供する場所で、常設サイトになることが意図されていないサイトを示します。大規模なプロジェクトマネジメントサイトから小規模なサービス／据付サイトまであり得ます。例えば、以下のサイト（場所）が挙げられます。
　① 現地組立工事、据付工事現場及び工事事務所
　② 現地保守点検、修理作業を行う作業場所
　③ 客先施設のオーバーホール、改造作業場所など

一時的サイトの活動は、全て審査対象とします。従って、現地審査工数を増す場合があります。
一時的サイトの審査（方法等）は、一時的サイトのISMS活動を管理している責任者へのインタビュー、一時的サイト関連文書の確認（例：苦情・事故の有無、管理策、監視・測定などを含むISMS活動全般の確認）等によります。
必要な場合は、一時的サイトへの現地訪問による現地審査を行います。一時的サイトの現地訪問による現地審査は、一時的サイトにおけるISMS活動に関するリスクを考慮して、BSKが決定することになります。

なお、顧客の敷地外に設置されたサイト等の場合、物理的入退管理策やネットワーク管理策など、顧客以外の組織との役割分担等に関連する情報を含め、ISMS活動に関する情報を確認させて頂きます。その情報の範囲や程度等に厳しい開示制限があり、審査の成立が困難と判断される場合には、審査の準備段階（例. 審査計画の立案・調整時等）において、適用範囲からの除外をご検討頂く場合があります。

情報通信技術（ICT）については、下記によります。
情報通信技術（ICT）は、情報の収集、保存、読み出し、処理、分析及び伝送に技術を利用することであり、スマートフォン、携帯端末、ラップトップコンピュータ、デスクトップコンピュータ、ドローン、ビデオカメラ、ウェアラブル技術、人工知能及びその他のソフトウェア及びハードウェアが含まれます。なお、コンピュータを使った審査技法（CAAT）もICTに含まれます。
審査要員が現地審査において、顧客のマネジメントシステムの適合性を評価するための確証を得るために利用するICTが管理の対象となる。
但し、顧客の情報システム（遠隔アクセスを除く／音声又は静止画･動画を含む映像の収集を除く）を利用した情報提供は収集した情報の妥当性及び客観性に影響が無いと考えられ、下記のICTの利用には含まれない（例. 文書管理システム、電子メールによる情報提供等）。
審査要員が審査の確認結果を記録するためにのみ利用するPC等もICTの利用には含まれない。
現地で及び遠隔で行われる審査でICTの利用を希望される場合、事前に申請をお願いします。
ICTを利用した審査工数が現地審査工数の30%を超える場合は、ＩＳＭＳ－ＡＣの事前承認が必要となります
ICTの利用例は次のとおりです。
・音声、映像及びデータ共有を含む、遠隔会議設備を用いた会議
（テレビ会議・電話会議、インターネット会議、双方向インターネット会議等）
・情報への同期（リアルタイム）又は非同期（該当する場合）の遠隔アクセスによる、文書及び記録の認証審査
（マネジメントシステム文書及び/又はマネジメントシステムプロセスへの遠隔電子アクセス等）
・静止画、動画又は音声の記録を用いて情報及び証拠を記録すること
・遠隔地又は危険の可能性があるロケーションへの映像／音声アクセスの提供
（監視カメラ、ビデオカメラ又はドローンによる映像／音声アクセスの提供等）

第２章　マネジメントシステム審査

2.1　審査基準

ＢＳＫは、次に示す適用規格及び適用基準を審査基準として、顧客（共同事業所を含む）のマネジメントシステムの審査を行います。審査の実施は、JIS Q 17021-1「マネジメントシステムの審査及び認証を行う機関に対する要求事項ー第１部：要求事項」に基づいてＢＳＫが設定した審査プロセスに従っています。

次の規格及び基準は、最新版を適用する。
JIS Q 27001　情報セキュリティマネジメントシステム（ISMS）

(1) 適用規格
・JIS Q 27001　情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー要求事項

(2) 適用基準

・JIP-ISAC100　ISMS認証機関認定基準及び指針

上記の適用規格及び適用基準において、次の文書が引用されています。

・ISO 9000　品質マネジメントシステムー基本及び用語
(JIS Q 9000　品質マネジメントシステムー基本及び用語)
・ISO/IEC 17000　適合性評価ー用語及び一般原則
(JIS Q 17000　適合性評価ー用語及び一般原則)
・ISO/IEC17021-1　適合性評価ーマネジメントシステムの審査及び認証を行う機関に対する要求事項ー第１部：要求事項
(JIS Q 17021-1　適合性評価ーマネジメントシステムの審査及び認証を行う機関に対する要求事項ー第１部：要求事項)
・JIS Q 27000　情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー用語
・ISO/IEC 27006　情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項
(JIS Q 27006 情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項)
・JAB NS511:2011　マネジメントシステム認証に関する基本的な考え方
ー故意に虚偽説明を行っていた事実が判明した認証組織に対する　処置
ー　第2版：2011年7月20日
(JAB、ISMS-ACが共同で作成、制定したもの)

２．２　審査及びレビューの種類

ＢＳＫが行う審査及びレビューの種類は次のとおりです。

審査及びレビューの種類（プロセスの視点での分類）

- ＜初めて認証の授与を受ける場合＞
  - [通常審査]
    - (1) 初回審査
    - (2) サーベイランス審査
    - (3) 再認証審査
      - [通常の再認証審査]
      - (4) 繰上げ再認証審査
  - [特別審査]
    - (5) 変更審査
      - [拡大審査]
      - (6) 移行審査
      - [その他の変更審査]
    - (7) 臨時審査
    - [付随的審査]（通常審査、変更審査、臨時審査に付随して行う審査）
      - (8) やり直し審査
      - (9) 追加審査
      - (10) フォローアップ審査
- ＜ＢＳＫ以外の認証機関から授与された認証の登録をＢＳＫに移転する場合＞
  - (11) 認証移転レビュー

審査の種類（実施場所の視点での分類）

- (a) 書類審査
  - ＜受審組織の所在地を訪問せずに実施する場合＞
- (b) 現地審査
  - ＜受審組織の所在地を訪問して実施する場合＞

その他の審査及びレビューの種類

- (ア) 文書レビュー
- (イ) 文書審査　　（二段階方式の主として第１段階）
- [実施審査（本審査）]（二段階方式の主として第２段階）
- (ウ) 組合せ型審査
  - [同時審査]
  - [複合審査]
  - [統合審査]

２．２．１　審査及びレビューの種類(プロセスの視点での分類)

⑴ 初回審査

初回の認証のための審査で、認証範囲に含まれる受審組織の情報セキュリティマネジメントシステムのすべての要求事項に対する適合性及び有効性を確認するための審査です。

初回審査は、第１段階（初回１）及び第２段階（初回２）の二つの段階で実施します。審査の日程を設定する基準とする日付を基準日と呼び、基準日を初回審査の認証日とします。この基準日は、第２回目以降のサーベイランス審査及び再認証審査のスケジュール設定の基準になります。

注、高レベル審査

受審組織の通常審査において、BSKの他のマネジメントシステムを既に３年以上認証されていて、その成熟度が認められた場合、審査工数規定（BSK-MSCC-MS-PO90104）別紙-3 JIS Q 27001情報セキュリティマネジメントシステム（ISMS）BSK標準工数の算定6.⑴高レベル審査適用基準に基づき、⑵高レベル審査におけるBSK審査工数の算定が適用され、初回審査においては、BSK標準初回審査工数の約２／３を下限として低減されます。
初回審査が高レベル審査に該当する場合は、4.1.1⑶の仮見積書を作成して顧客に送付するときにその旨をお伝えいたします。

⑵ サーベイランス審査

被認証組織の認証されたマネジメントシステムが、継続して要求事項に対して適合していることを確認するとともにマネジメントシステムの有効性について評価するための審査です。JIS Q 17021-1に基づき、サーベイランス審査は、少なくとも暦年に1回実施しますが、BSKとしては12か月毎に実施することを基本的な考え方とします。ただし、組織から要望がある場合には、６か月毎に実施することができます。

なお、初回認証に続く最初のサーベイランス審査の期日は、認証の決定をした日から１２か月を超えないものとします。

サーベイランス審査の実施時期は、年１回の場合には基準日を起算日として、原則としてマイナス４か月からマイナス３か月の間、６ヵ月毎の場合には基準日及び初回認証日プラス６か月を起算日として原則としてマイナス４か月からマイナス３か月以内の期間を、ＢＳＫの標準的な審査実施期間としています。

注、高レベル審査

サーベイランス審査においては、BSK標準サーベイランス審査工数の９０%となります。詳細は、初回審査の注2、高レベル審査を参照されたい。
サーベイランス審査が高レベル審査に該当する場合は、5.2.2.1の審査日程及び審査担当審査要員の顧客との合意のときにその旨をお伝えいたします。

⑶ 再認証審査

認証の有効期限に先立って3年目に行う審査です。再認証審査は、被認証組織の情報セキュリティマネジメントシステム全体としての継続的な適合性及び有効性、並びに認証の範囲に対する情報セキュリティマネジメントシステムの継続的な関連性及び適用可能性を確認する審査です。

再認証審査の実施時期は、3年目の基準日の4ヵ月前から3ヵ月前までの期間を、ＢＳＫの標準的な審査実施期間としています。ただし、再認証審査中に、不適合の事例又は適合性の証拠の不足が特定された場合に修正及び是正処置が認証の有効期限前に実施されるような時間的な余裕を確保するために、再認証審査の実施時期を早めることがあります。

注、高レベル審査

再認証審査においては、BSK標準再認証審査工数の９０%となります。詳細は、初回審査の注2、高レベル審査を参照されたい。

再認証審査が高レベル審査に該当する場合は、6.1.1の申請の準備及び事前協議のときにその旨をお伝えいたします。

⑷ 繰上再認証審査

基準日を変更するために時期を早めて実施する再認証審査を「繰上再認証審査」と呼びます。繰上再認証審査を実施した場合には、繰上再認証審査の再認証日が新しい基準日となります。新しい基準日は、現有効期限内で、繰上再認証審査の現地審査最終日から５か月を超えないものとします。

⑸ 変更審査

認証の内容を変更する場合に行われる審査で、その規模及び内容に応じ、審査項目と審査期間及び審査工数を定めて実施する審査です。この変更には、認証書記載内容の変更（所在地の変更／工場移転を含む）、拡大、縮小、認証書の統合、認証書の分割、適用規格の移行を含みます。変更内容が拡大の場合には、「拡大審査」と呼ぶことがあります。

変更審査は、サーベイランス審査または再認証審査などの他の審査と同時に実施することがあります。

⑹ 移行審査

変更審査の中で、適用規格の移行を対象とする審査を特に「移行審査」と呼びます。適用規格の移行には、同一の規格についての版の移行も含まれます。

移行審査は、サーベイランス審査または再認証審査などの他の審査と同時に実施することがあります。

⑺ 臨時審査

苦情、製品事故、不祥事公表、等の発生により、通常のサーベイランス審査あるいは再認証審査とは別に、被認証組織が認証の要求事項に引き続き適合していることを検証することが必要になった場合

に実施する審査を指します。

⑻ やり直し審査

当初計画した審査が実施の途中で不成立になり、やり直す場合の審査を指します。

⑼ 追加審査

初回審査、サーベイランス審査、再認証審査などの審査で、現地審査を実施した後に審査内容が不十分だったことが判明し、審査の完全性を確実にするために必要となった場合に実施する追加的な審査を指します。

⑽ フォローアップ審査

初回審査、サーベイランス審査、再認証審査などの審査で重大不適合又は不適合が発見され、その是正について再度現地での確認が必要となった場合に実施する審査を指します。これには、認証が一時停止になった被認証組織のフォローアップとして実施する審査も含まれます。

⑾ 認証移転レビュー

認定機関の基準に準拠し、ＩＡＦに属する認定機関から認定を受けている他の認証機関によって授与された、既存の有効な情報セキュリティマネジメンシステム認証を、ＢＳＫの認証として認知し、認証の登録を移転する目的で実施するレビュー（確認）を指します。

２．２．２　審査の種類(実施場所の視点での分類)

(a)　書類審査

現地（受審組織の所在地）を訪問せずに、書類の検証／確認のみで実施する審査を指します。

注. ＢＳＫでは、「マニュアル審査」という用語は廃止されています。この用語は、以前、受審組織の情報セキュリティマニュアルのみを審査する書類審査について使用していたものです。

(b)　現地審査

受審組織の所在地（本拠地及び他サイト）を訪問して実施する審査を指します。

２．２．３　その他の審査及びレビューの種類

⑺ 文書レビュー

初回審査・第１段階などの現地審査に先立って、文書化されている範囲において、審査基準に対するシステムの適合性を判定するために、受審組織の文書をレビューすることを、「文書レビュー」と呼

びます。レビューの対象とする文書には、情報セキュリティマネジメントシステム文書及び記録、並びにこれまでの審査報告書／監査報告書を含めることがあります。

(ｲ) 文書審査

受審組織の情報セキュリティマニュアルを含む情報セキュリティマネジメントシステム文書の審査を指します。文書審査では、対象となる文書一式について、全体として適用規格に適合しているか否かを審査します。

二段階で行う審査の第１段階では、主に文書審査を行います。

(ｳ) 組合せ型審査

組合せ型審査は、複数のマネジメントシステムを有する顧客が、主にマネジメントシステムの運用管理の効率化や審査の効率化（工数削減）などを目的に、複数のマネジメントシステムを同時期に組合せて行う審査であり、顧客のマネジメントシステムの統合されている程度によって統合審査、複合審査、同時審査に類別できます。

統合の程度とは、QMS、EMS、ISMSの各規格書の付属書の対応表を基準として統合可能な規格要求事項の項目の内、統合されている項目（数）、又統合されている程度（手順としての統合された内容）を総合的に評価した程度のことであり、数値化されたものではありません。
組合せ型審査に於ける審査のプロセスは、マネジメントシステムの統合状況に合わせ、同時・シリーズ又は個別に審査を実施し、各マネジメントシステムの規格要求事項を確認します。初回・サーベイランス・再認証審査における審査のプロセスは、原則として通常の審査と同じです。

組合せ型審査の各種類の定義は以下の通りです。

(1) 統合審査

顧客が、同時に二つ以上のマネジメントシステム規格の要求事項を一つのマネジメントシステムに統合して審査される場合を統合審査と呼びます。（JIS Q 17021-1）
統合審査の現地審査では、オープニング・ミーティングからクロージング・ミーティングに至る一連の審査活動を複数のマネジメントシステムについて、その規格要求事項を同時に審査することとなります。

この場合、顧客のマニュアルとしては、例えばQMSの規格要求事項の記述を骨格とし、AQMS、EMS、ISMSの関連する追加要求事項が記述された「統合マネジメントシステムマニュアル」が作成されていることとなります。
審査としては、①初回審査に於ける統合審査、②サーベイランス審査及び再認証審査に於ける統合審査への変更審査（移行審査）などがあります。

二つ以上のマネジメントシステムのサーベイランス審査の周期は、年1回に統一する必要があります。又審査実施日が同期することから「基準日」（基準日の定義は、5.2.1.2項(1)を参照下さい）の前倒しなどの変更が必要となる場合があります。

審査の効率化（審査工数削減）の効果が大きい審査です。
マネジメントシステム毎の審査工数の削減の最大値は、以下の通りです。

① QMS及びEMS審査工数の削減の最大値
JAB MS305-2009「マネジメントシステム認証機関に対する認定の基準についての指針」3.9項に於いてJAB MS305-2009の付属書A（QMS）及び付属書B（EMS）審査工数に対して削減率は「30%を超えることは通常ない」と規定されています。

従って、例えばQMSで設計開発が適用除外となっている場合は、すでに審査工数がJAB MS305-2009の付属書Aの工数に対して20%削減されている場合であり、残り10%削減までが削減工数の最大値となります。

又QMS及びEMSに於いてJAB MS305-2009の付属書A及び付属書B審査工数に対して増減（調整）されている場合も、同様に、削減工数はJAB MS305-2009の付属書A及び付属書Bの審査工数（標準値）に対する削減率は「30%を超えることは通常ない」と規定されています。

② AQMSの審査工数の削減の最大値
AQMS の審査工数は、JAB MS101-2007に於いてQMSに対する追加工数として規定されていますが、増減の規定はなく工数削減の許容はありません。

③ ISMSの審査工数の削減の最大値
審査工数は、JIS Q 27006（ISO/IEC27006）の付属書Bに規定されていますが、削減工数の最大値は30%とされています。従って、30%を超えない範囲で、P090104「審査工数規定」に基づき定められた工数に対して、統合されている規格要求事項の項目数と程度により減じることができます。

⑵ 複合審査

顧客が、同時に二つ以上のマネジメントシステム規格の要求事項に関して審査される場合を複合審査と呼びます。（JIS Q 17021-1）

複合審査の現地審査では、オープニング・ミーティング、クロージング・ミーティング、トップインタビュー及び複数のマネジメントシステムの共通項目（例えば、文書管理、記録の管理、教育・訓練、資源等）などの審査の一部を同時に審査し、非共通項目及び部門審査はマネジメントシステム毎に個別に行う審査となります。

この場合、顧客のマニュアルは、上記の「統合マネジメントシステムマニュアル」が作成されている場合とマネジメントシステム毎に「マネジメントシステムマニュアル」が作成されている場合があります。
審査としては、①初回審査に於ける複合審査、②サーベイランス審査及び再認証審査に於ける複合審査への変更審査（移行審査）などがあります。

二つ以上のマネジメントシステムのサーベイランス審査の周期は、年1回に統一する必要はありませんが、年2回の場合は、審査実施日が他のマネジメントシステムと同期しない時期の審査は、単独の審査（通常の審査）となります。
又複合審査の場合、審査実施日が同期することから「基準日」（基準日の定義は5.2.1.2項(1)を参照下さい）の前倒しなどの変更が必要となる場合があります。

審査の効率化（審査工数削減）の効果は統合審査より少ないですが、通常の審査に比べて審査工数が削減できる審査です。
審査工数の削減率は、統合の程度（共通項目の共通化の程度）によりますが、削減率の最大値は、前述の統合審査と同じ削減率まで可能ですが、一般的には、以下を最大値とします。尚、審査工数の増減がすでに実施されている場合は、その削減分を含めて以下の最大値となります。

① QMSの審査工数標準値に対する削減率：以下の通り。
設計･開発有の場合――最大２０％
設計･開発無の場合――すでに２０%削減されているので０％
② AQMSの審査工数追加分に対する削減：なし
③ EMSの審査工数標準値に対する削減率：最大２０％
④ ISMSの審査工数標準値に対する削減率：最大１０％

⑶ 同時審査

顧客が、二つ以上のマネジメントシステム規格の要求事項に関して、同一期間内で時間を組合せ、認証機関の指名する２つ以上の審査チームにより個々の規格要求事項を審査する場合を同時審査と

呼びます。（複合審査の一種とも言えます）

オープニング・ミーティング、クロージング・ミーティング、トップインタビューなどを同時間内にシリーズに行う審査です。
個々のマネジメントシステムの審査工数が異なる場合、審査期間の短い審査を担当する審査員が、審査期間の長い審査の一部を担当して審査する場合などがあります。この場合、顧客のマニュアルは、マネジメントシステム毎に「マネジメントシステムマニュアル」が作成されています。
審査としては、通常と同じ初回審査、サーベイランス審査及び再認証審査となります。

審査の効率化（審査工数削減）の効果は、通常の審査と同じ工数となるので、審査工数削減の効果は期待できませんが、審査期間が同一期間となり組織の対応期間も同一期間となる点でメリットがあります。審査工数は、マネジメントシステム毎の審査プログラムにて設定された各々の工数となります。

二つ以上のマネジメントシステムのサーベイランス審査の周期は、統一する必要はありませんが、審査実施日が同期することから「基準日」（基準日の定義は5.2.1.2項⑴を参照下さい）の前倒しなどの変更が必要となる場合があります。

２．３　審査チームが実施する業務について

BSKは審査チームが実施すべき次の業務を明確にし、通知します。

⑴ マネジメントシステムに関連する顧客組織の構成、方針、プロセス、手順、記録及び関連する文書を調査し、検証する。

⑵ これらが、対象となっている認証範囲に関連する、全ての要求事項を満たしていることを決定する。特に，JISQ27001の4.3に規定する要求事項を取り扱っていることを確認する。

⑶ 顧客のマネジメントシステムに対する信頼の基礎となるプロセス及び手順が、有効に確立、実施及び維持されていることを決定する。

⑷ 顧客の方針、目的及び目標（該当するマネジメントシステム規格又は他の規準文書の主旨に沿ったもの。）と結果との間にみられるいかなる不一致についても、それに対して行動がとられるよう、顧客に伝える。

第３章　不適合等の取扱い及び是正処置

３．１　不適合

⑴ＪＩＳ Ｑ １７０２１－１の不適合の定義は、次によります。

不適合（ 3.11 ）　　：　要求事項を満たしていないこと。

重大な不適合（ 3.12 ）：　意図した結果を達成するマネジメントシステムの能力に影響を与える不適合。

注記　次の事項は、重大な不適合に分類される可能性がある。

- 効果的なプロセス管理が行われていること又は製品若しくはサービスが規定要求事項を満たすことについての重大な疑い
- 同一の要求事項又は問題に関連する軽微な不適合が幾つかあって、一つのシステムの欠陥であることが実証されることで、重大な不適合となるもの

軽微な不適合（ 3.13 ）：意図した結果を達成するマネジメントシステムの能力に影響を与えない不適合。

⑵ 重大不適合と軽微不適合のより具体的な事例を次に示します。

① 重大不適合：

1) システム又は手順の完全な欠落、もしくは、システム又は手順が完全に機能していない。

2) 意図したアウトプットを達成する依頼者のマネジメントシステムの能力について，重大な疑いを生じさせるような状況である。

3) 類似の不適合がシステム全体に存在し、システムが機能していない。

4) 連続した不適合の指摘

軽微な不適合が指摘され、修正・是正処置等が取られたプロセス、若しくは項目で、次の審査で連続して同様の不適合が指摘された場合は、是正処置の不足として重大不適合と判断されます。

② 軽微不適合：

1) システム又は、手順に若干の欠落。

2) システム又は手順が一部機能していない。（方針及び目的を達成する能力に関して重大な疑いがある場合も含む。）

３．２ 不適合の取扱い

不適合の取扱いは次によります。

⑴ 初回審査・第２段階、サーベイランス審査、再認証審査等において、適用する要求事項から相違した場合、顧客の同意を得て是正処置要求書(CAR)を発行し、不適合の内容を通知します。初回審査・第１段階では適用しません。

⑵ 是正処置要求書(CAR)は、顧客の管理責任者の記名及び是正処置完了予定日を記入していただき、期日までに是正処置完了のうえ、回答していただきます。（回答は原則として３０日以内とします。）

３．３ 修正及び是正処置

⑴ 不適合がある場合は、修正及び是正処置の文書による回答を要求します。

⑵ 回答された修正及び是正処置について、審査チームは提出された是正処置について正しく処置されていることを確認(レビューと容認)します。次回サーベイランス審査又は再認証審査でその有効性を検証することを基本としますが、必要な場合は是正処置確認のためのフォローアップ審査を実施します。

この場合、ＢＳＫは顧客に対し日程の調整をいたします。

⑶ 重大不適合については、全ての修正及び是正処置が実施（設定されそれが正しく処置されていること）され、確認(レビューと容認)されていなければなりません。

⑷ 軽微不適合については、修正及び是正処置が正しく計画されていることの確認(レビューと容認)が終了しなければ、認証の授与の決定と認証書の発行はできません。

⑸ 修正及び是正処置の文書による回答期限は、是正処置要求書(ＣＡＲ)の発行日から原則として３０日以内とします。３０日以内又は合意された期限内に回答がなかった場合や、回答があっても、回答の容認が３０日をこえた場合の処置は次の通りとします。

初回審査

・30日を超えて3ヶ月以内に回答が容認された場合、認証の可否の判定に進めます。

・回答が、3ヶ月以内に容認されない場合、初回審査を中断します。

・3 ヶ月を超えて 6 ヶ月以内に回答があり、容認できる可能性がある場合は、フォローアップ審査で確認した上で、認証可否の判定に進めます。

・6 ヶ月を超えても回答がなかった場合又は回答が容認されなかった場合は、初回審査は無効とし、新規の申請が必要となります。

サーベイランス審査

・3ヶ月以内の合意された期限までに回答が容認された場合、認証維持の可否の判定に進めます。
・30日以内に回答がなかった場合又は合意された期限までに回答がなかった場合、一時停止となります。
・3ヶ月以内の合意された期限までに回答が容認されない場合、一時停止となります。
・一時停止となり3ヶ月以内に是正が講じられない場合、取消しとします。

再認証審査

・3ヶ月以内の合意された期限までに回答が容認された場合、再認証の可否の判定に進めます。
・30日以内に回答がなかった場合又は合意された期限までに回答がなかった場合、一時停止となります。
・3ヶ月以内の合意された期限までに回答が容認されない場合、一時停止となります。
・有効期限内であっても3ヶ月以内に回答の容認がされない場合、一時停止となります。
・一時停止となり3ヶ月以内に是正が講じられない場合、取消しとします。
・回答がなかった又は回答が容認されなかったために、有効期限までに再認証の決定がされなかった場合、失効となります。

⑹ 修正及び是正処置の回答文書とは別に修正及び是正処置の証拠を審査チームリーダーに提出して頂きます。

３．４　気付事項

気付事項とは、現在不適合ではないが将来不適合となることが懸念される事項、及び不適合ではないが審査中気付いたマネジメントシステムをより良くするための改善の余地がある事項をいいます。

３．５　気付事項の取扱い

気付事項は、審査最終報告書に「気付事項」として添付します。顧客は、気付事項の内容を検討し、処置が必要と判断したものについて対策を行います。（処置の要否は、顧客の判断によります。）
なお、気付事項については、文書による回答は必要としません。ただし、気付事項に対する対応について、次回審査で確認します。

第４章　初回審査

４．１　契約手続き

４．１．１　問合せ及び仮見積書の作成

⑴ 認証取得を希望する場合、ＢＳＫに問合せをお願いします。ＢＳＫの営業担当者が対応します。
⑵ ＢＳＫから認証に係わる費用の見積りを希望する場合、初回認証見積依頼書を送付してください。
初回認証見積依頼書の様式は、ＢＳＫから送付します。ＢＳＫシステム審査センターのホームページからダウンロードすることも可能です。
⑶ ＢＳＫは、初回認証見積依頼書を受領後、仮見積書を作成して顧客に送付します。
⑷ 仮見積書の内容を確認後、ＢＳＫに初回審査の申請をするか否かの決定結果をＢＳＫの営業担当者に連絡してください。

４．１．２　申請の準備及び事前協議

⑴　顧客がＢＳＫに初回審査の申請を行うと決定したことの連絡を受けた後、ＢＳＫは、認証申請に必要な次の資料（以下「申請資料」という。）を顧客に送付します。
尚、組合せ型審査を希望する場合は、「組合せ型認証申請書」を併せて送付しますので、その旨お知らせ下さい。

ア　認証ガイド
イ　認証申請書様式とその電子データ
ウ　認証申請事前調査票様式とその電子データ（認証データシート含む）
エ　認証合意書様式（２通）
オ　審査部門／審査項目対応表様式とその電子データ

⑵　申請資料受領後、申請内容の検討をして申請資料への記入をしていただきます。申請資料への記入について、問合せ、相談がありましたら、連絡をお願いします。認証申請事前調査票は、顧客が認証を受けようとする内容について、事前に希望する認証の内容（被認証組織（共同事業所を含む）の名称、所在地、認証範囲、産業分類、対象従業員数）、適用除外の有無、受審希望時期等の申請に関する情報及び認証に必要な資料の提供をしていただくものです。
次の資料については、認証申請書の添付資料として提供をしていただきます。

① 認証範囲を含む組織のカタログ及び組織図
② 認証範囲及び境界を記載した設備配置図（対象範囲のフロアレイアウト、入退出管理設備、文書庫等及びネットワーク構成）
③ 情報セキュリティマネジメントシステムの実施計画書（認証取得までの計画）

組合せ型審査を希望する場合は、上記ＥＭＳ関係の申請資料だけでなく、組合せ型審査に組み合わせる他のマネジメントシステム認証ガイドに記載の関連資料を提出して頂きます。

⑶　顧客が申請内容等（共同事業所を含む）の詳細について事前協議を希望する場合は、ＢＳＫの顧客（共同事業所を含む）への訪問又は顧客のＢＳＫへの来訪により、協議を行います。

４．１．３　申請及びＢＳＫによる申請のレビュー

⑴　顧客は、送付を受けた認証合意書及び認証ガイドの内容について確認し、同意のうえ、認証申請書及び認証合意書（２通）に申請責任者（経営責任者（経営責任者が指名した者を含む。）又は管理責任者）の記名・押印をしてＢＳＫに返送していただきます。認証合意書は、顧客の代表者（共同事業所を含む）の記名・押印としてください。また、認証申請事前調査票については所要の事項を記入して、併せてＢＳＫ宛に送付していただきます。認証申請書及び認証申請事前調査票については、電子データをメールにてＢＳＫへご送付下さい。尚、組合せ型審査を希望する場合は、上記に併せて「組合せ型認証申請書」の記入及び提出を同様にＢＳＫへご送付下さい。

⑵　ＢＳＫは、申請資料の確認をし、形式的な、書類不備、記入漏れ、情報不足等がありましたら、顧客に連絡します。必要な場合、修正・再提出を依頼しますので、対応をお願いします。

⑶　ＢＳＫは、申請資料の内容について、審査を含む認証活動を行うために必要な包括的なレビュー(申請のレビュー)を行います。申請のレビューにおいて、顧客に問合せ・調整が必要になりましたら連絡しますので対応をお願いします。また、申請のレビューの結果、認証申請書及び認証申請事前調査票について、変更が必要な部分があるとＢＳＫとして判断した場合は、変更案を送付しますので、評価・検討をして、変更申請書の作成・提出をお願いします。

⑷　組合せ型審査の場合、組み合わせる既に認証されているマネジメントシステムの「基準日」（基準日の定義は5.2.1.2項⑴を参照下さい）によっては、基準日の変更等の調整をさせて頂く場合が有

りますので、ご了解下さい。又、統合の程度により統合審査から複合審査又は同時審査、複合審査から同時審査に変更させて頂く場合があります。

４．１．４　契約書類及び申請料

⑴　ＢＳＫは、顧客から送付を受けた認証合意書２通に記名・押印します。認証業務の契約は、顧客から送付を受けた認証合意書２通にＢＳＫが記名・押印した段階で成立します。

⑵　ＢＳＫは、顧客から送付を受けた申請資料に基づき、初回審査に関する費用の見積りを行い、契約書類として、見積書及びＢＳＫが記名・押印した認証合意書（１通）を顧客に送付します。

⑶　前⑵の見積書及び認証合意書の送付に併せて申請料の請求をさせていただきます。また、併せて初回審査に必要な情報セキュリティマネジメントシステム文書の提出を要求します。提出していただく情報セキュリティマネジメントシステム文書は、４．２．２「情報セキュリティマネジメントシステム文書の提出」の通りです。

⑷　契約書類、申請料の請求及びマネジメントシステム文書の提出の要求に対して疑義がある場合はＢＳＫに対して申し出をすることができます。

⑶　申請料の請求に基づき、申請料の支払いをしていただきます。

４．２　初回審査の実施

４．２．１　初回審査概要

４．２．１．１　初回審査の概略プロセス及び目的

⑴　初回審査は、初回審査・第１段階（略称：初回１）及び初回審査・第２段階（略称：初回２）の２段階方式で実施します。初回１では、現地審査の前に文書レビューを実施します。

⑵　文書レビュー、初回１及び初回２の目的及び概要はそれぞれ次の通りです。

＜文書レビュー＞

現地審査に先立って、顧客の情報セキュリティマネジメントシステム文書について、審査基準に対する顧客の情報セキュリティマネジメントシステムの適合性を判定することを目的として実施します。情報セキュリティマニュアル等を提出していただきそれをレビューし、問題点がある場合「文書問題点」として指摘します。これを解決して回答していただくことが初回１へ進む条件となります。

＜初回１＞

顧客（共同事業所を含む）の情報セキュリティマネジメントシステム文書等の審査を行い、初回２のための顧客の準備状況を確認することを目的として実施します。初回２で不適合となる可能性のある事項がある場合「懸念領域」として指摘します。これを解決して回答していただくことが初回２へ進む条件となります。

＜初回２＞

顧客（共同事業所を含む）の情報セキュリティマネジメントシステムの全ての要求事項に対して適合性及び有効性があることを確認することを目的として実施します。要求事項に対して適合していない場合、「不適合」として指摘します。修正及び是正処置について回答していただくことが認証可否の判定へ進む条件となります。

４．２．１．２　審査時期の決定

⑴　初回審査の実施時期は、顧客と調整のうえ決定します。初回１の実施は、原則として次が前提となります。

ア　情報セキュリティマネジメントシステムが確立され、文書化され、実施されていて、必要に応じて該当する記録が確認できること。顧客の情報セキュリティマネジメントシステムが確立されてから記録が確認できるまでの期間は、３か月以上を目安とします。

イ　初回１の現地審査実施前までに、監査対象に全組織、全項目が含まれている内部監査が実施されていて、記録が確認できること。

ウ　初回１の現地審査実施前までに、上記イの監査の結果がインプットに含まれたマネジメントレビューが実施されていて、記録が確認できること。

⑵　初回１と初回２の間は、原則として１か月以上、通常１．５か月～２か月の間隔を取ります。

⑶　初回１実施後、初回２までの期間は原則として６か月以内とします。

ア　６か月以内に懸念領域の解決を完了した場合は、懸念領域の解決確認後、初回２の実施へ進む。

イ　６か月以上１２か月以内に懸念領域の解決を完了した場合は、実施した懸念領域の解決のフォローアップ審査実施後、初回２の実施へ進む。

ウ　１２か月以上経過しても初回２へ進めない場合は、実施済の初回１を無効とし、再度初回１を実施します。

４．２．２　初回審査・第１段階

４．２．２．１　審査日程及び審査担当審査要員の顧客との合意

ＢＳＫは、顧客に審査日程を通知し合意を受けます。同時に、審査担当審査要員の情報(経歴)等を記した「担当審査要員の確認依頼について」を顧客に送付して、異議の有無を確認します。

４．２．２．２　情報セキュリティマネジメントシステム文書の提出

⑴　顧客には、適用規格に適合する情報セキュリティマネジメントシステム（以下「ＩＳＭＳ」という。）を確立し、文書化し、実施していただきます。

⑵　情報セキュリティマネジメントシステムマニュアル（以下"情報セキュリティマニュアル"という。）の作成にあたっては、次の点を考慮してください。

ア　適用範囲（共同事業所を含む）は、認証申請書に記載した認証範囲と整合をとってください。情報セキュリティマニュアルの適用範囲が認証範囲と同じ場合は、認証申請書に記載した認証範囲と同じ表現としてください。この認証範囲の内容がそのまま認証書に記載されます。

イ　JIS Q 27001 付属書Aに規定する管理策を除外した場合には、適用宣言書にその理由を明確に記述して下さい。適用範囲についても、認証申請書に添付した「認証範囲及び境界を記載した設備配置図」と整合をとってください。

ウ　ISMSの運用組織を明記し各運用分担の相互関係を明確にして下さい。

エ　単に規格要求事項を記述するのではなく、受審組織が内部で活用するため、又は内部監査（外部の監査を含む。）がしやすいように、また、説明しやすいように配慮して、プロセスの概要（管理の方法）を記述して下さい。

⑶　文書レビューのために必要な次の文書類を、契約締結後、初回１の２か月前までにＢＳＫに提出して下さい。

なお、再認証審査 及びサーベイランス審査の際は、各審査の１か月前までにＢＳＫに最新版を提出ください。

ア　情報セキュリティマニュアル（含む組織図（共同事業所を含む））　２部

イ　適用宣言書　２部

ウ　情報セキュリティマネジメントシステム文書リスト　２部
（情報セキュリティマニュアルで引用される文書の改定状況を含むリスト）

エ　フロア図（例. 適用範囲、物理的入退管理策箇所を記載した概略図等）　２部

オ　情報システム ネットワーク図（例. ネットワーク概略図等）　２部

カ　既に提出された文書化した情報に変更があればその最新版　２部

キ　ISMS及びその対象となる活動に関わる一般情報　　２部
（ISMSの適用範囲に完全には含まれない，ITサービス，通信システム，
業務機能の外部委託等）

４．２．２．３　文書レビュー前の事前調整(必要に応じ)

初回審査を円滑に進めるため、審査チーム・リーダーが必要に応じ事前調整を行います。また、顧客(主要審査対象部門又は場所)を訪問することもあります。認証範囲の確認及び審査スケジュールなどの細部を調整し、ＢＳＫと顧客との間に生じる理解の違いを解消します。申請書の　申請内容と相違がある場合は、変更申請を提出していただきます。

４．２．２．４　文書レビューの実施

⑴　ＢＳＫは提出していただいた文書のレビューを行います。文書レビューの結果、問題点がある場合は、「文書問題点指摘書／回答書／確認書」の指摘書欄に問題点を記入し、文書レビュー報告書(暫定版)としてまとめ、「文書問題点指摘書／回答書／確認書」の電子データとともに、顧客に送付します。

⑵　文書レビュー報告書(暫定版)を受領しましたら、文書問題点の解決をしていただきます。文書問題点が解決しましたら、ＢＳＫに文書問題点解決の連絡と次の文書の提出をしていただきます。

ア　文書問題点指摘書／回答書／確認書　　１部
（回答書欄に記入し記名した文書及び電子データ）

イ　情報セキュリティマニュアルの改訂版　　２部

ウ　情報セキュリティマネジメントシステム文書リスト(変更がある場合)　２部

⑶　ＢＳＫは、提出していただいた文書を確認し、十分であれば、確認結果を記入した「文書問題点指摘書／回答書／確認書」を付けて「文書レビュー報告書」を作成し顧客に送付します。不十分であれば、その旨顧客に連絡し、⑵を実施していただきます。

４．２．２．５　初回１の事前調整

⑴　ＢＳＫの担当審査要員は、初回１を円滑に進めるため、顧客（共同事業所を含む）を現地訪問し事前調整を実施します。ただし、審査の準備を進める上で支障が無い場合には、現地訪問を省略します。

⑵　事前調整で実施する事項は次の通りです。

ア. 初回１の実施の前提である以下の事項を確認します。

・情報セキュリティマネジメントシステムが確立され実施されていること。(文書の内容及び記録があることを確認します。)

・監査対象に全組織、全項目が含まれている内部監査が実施されていて、記録が確認できること。また，情報セキュリティに関する独立したレビューがある場合は，その記録が確認できること。

・上記の監査の結果がインプットに含まれたマネジメントレビューが実施されていて、記録が確認できること。

イ．認証範囲、場所、審査スケジュールなどの細部を調整し、ＢＳＫと顧客との間に生じる理解の違いを解消します。申請書の申請内容（共同事業所を含む）と相違が有る場合は、変更申請を提出していただきます。

ウ. その他必要な事項

⑶　事前調整の結果、審査日程又は審査担当審査要員の変更が必要になった場合は、ＢＳＫから顧客に変更の連絡をします。

４．２．２．６　審査計画書(初回１)の作成

⑴　ＢＳＫは、上記事前調整結果を基に審査計画書を作成し、次の事項を明確にします。

ア　顧客の所在地、代表者

イ　審査の目的

ウ　審査基準及び関連基準文書

エ　審査範囲（共同事業所を含む）

オ　審査の計画

審査チーム及び同行者、使用する言語、審査日時、審査場所（共同事業所を含む）、予定時刻

及び所要時間、審査する組織単位、審査方法、経営者との会議、審査結果について、その他

カ　審査報告書

キ　機密保持

ク　異議申立て

ケ　審査のフォローアップ処置

⑵　初回１の実施場所は、原則として顧客の主要サイト（共同事業所を含む）の現地で実施するものとします。場所及び日程については事前に顧客と合意をとります。

⑶　審査計画書は、必要に応じて顧客と協議・調整をして作成し、顧客に配布します。

４．２．２．７　初回１の実施

⑴　初回１は、審査計画書（初回１）に基づいて実施します。

⑵　初回１では、顧客の情報セキュリティマネジメントシステム文書等の審査を行い、初回２のための顧客の準備状況を確認します。詳細は、次の通りです。

ア　顧客の文書化したマネジメントシステム情報をレビューする。

イ　顧客の事業所固有の条件を評価し、第２段階の準備状況を判定するために顧客の要員と協議する。

ウ　規格の要求事項に関する顧客の状況及び理解を、特にマネジメントシステムの主要なパフォーマンス又は重要な側面、プロセス、目的及び運用の特定に関してレビューする。

エ　次の情報を含むマネジメントシステムの適用範囲に関して、必要な情報を収集する。

－顧客の事業所

－プロセスの使用設備

－確立された管理のレベル（特に複数サイトの顧客の場合）

－適用される法令及び規制要求事項

オ　第２段階のための資源の割当てをレビューし、第２段階の詳細について顧客と合意する。

カ　マネジメントシステム規格又はその他の規準文書に照らして、顧客のマネジメントシステム及び事業所の運用について十分理解することによって、第２段階を計画するうえでの焦点を明確にする。

キ　内部監査及びマネジメントレビューが計画され実施されているかどうかについて評価し、またマネジメントシステムの実施の程度が第２段階のための準備が整っていることを実証するものであることを評価する。

⑶　審査を行った範囲において、このままでは、初回２で不適合となる可能性のある事項がある場合、それを懸念領域として指摘します。懸念領域は、「懸念領域指摘書／回答書／解決確認書」の指摘書欄に記入します。

４．２．２．８　初回１審査報告書の作成

⑴　初回１チーム・リーダーは、初回１終了後、顧客を離れる前に、初回審査・第１段階　審査報告書(暫定版)に関する情報を作成し、顧客に提示提出し、報告書に対する顧客の意見を求めます。審査報告書（暫定版）は、最終会議終了後２週間以内に提出します。

⑵　作成した「懸念領域指摘書／回答書／解決確認書」は、顧客を離れる前に提出します。電子データも同時に配布します。

４．２．２．９　懸念領域の解決

⑴　懸念領域指摘書／回答書／解決確認書を受領しましたら、懸念領域がある場合懸念領域の解決をしていただきます。懸念領域が解決しましたら、初回１チーム・リーダーに懸念領域解決の連絡と次の資料の提出をしていただきます。

ア　懸念領域指摘書／回答書／解決確認書　　１部
（回答書欄に記入し記名した文書及び電子データ）

イ　解決した証拠としての文書又は記録の該当部分　　１部

ウ　情報セキュリティマネジメントシステム文書リスト(変更がある場合)　１部

⑵　ＢＳＫは、提出していただいた文書を確認し、十分であれば、確認結果を記入した「懸念領域指摘書／回答書／解決確認書」を付けて「審査報告書」を作成し顧客に送付します。不十分であれば、その旨顧客に連絡し、⑴を実施していただきます。

⑶　懸念領域が解決されたことを確認後、第２段階が実施可能となります。

４．２．３　初回審査・第２段階

４．２．３．１　審査日程及び審査担当審査要員の顧客との合意

ＢＳＫは、顧客に審査日程を通知し合意を受けます。同時に、審査担当審査要員の情報(経歴)等を記した「担当審査要員の確認依頼について」を顧客に送付して、異議の有無を確認します。

４．２．３．２　初回２の事前調整

⑴　ＢＳＫの審査チーム・リーダーは、初回２を円滑に進めるために必要な場合、顧客と電話等で調整を実施します。また、初回１において顧客と初回２の詳細の合意をしていますが、初回１において訪問していないサイト（共同事業所を含む）があった場合や、初回１から状況の変化があった場合等には、事前調整のために現地訪問が必要となることがあります。その場合は、顧客（共同事業所を含む）と合意を得たうえで現地訪問を行います。現地訪問による事前調整は、顧客の費用負担とさせていただきます。

⑵　事前調整で実施する事項は次の通りです。

ア. 初回２の実施の前提である以下の事項を確認します。
・初回１の懸念事項が解決されていること。

イ. 認証範囲、場所、審査スケジュールなどの細部を調整し、ＢＳＫと顧客との間に生じる理解の違いを解消します。申請書の申請内容（共同事業所を含む）と相違が有る場合は、変更申請を提出していただきます。
なお、マネジメントシステムに影響するような重大な変更（適用範囲の大規模な拡大等）行われる場合、BSKは、第一段階の全て又は一部を繰り返す必要性を考慮する場合があります。

ウ. 顧客において，少なくとも一つの内部監査（認証範囲を対象に含む）及びマネジメントレビューが運用されていること。

エ.　初回２では、詳細な調査のために初回１とは別種の情報及び記録の追加を求める場合があります。

オ. その他必要な事項

⑶　事前調整の結果、審査日程又は審査担当審査要員の変更が必要になった場合は、ＢＳＫから顧客に変更の連絡をします。

４．２．３．３　審査計画書(初回２)の作成

⑴　ＢＳＫは、初回１結果及び事前調整結果を基に審査計画書を作成し、次の事項を明確にします。

ア　顧客の所在地、代表者

イ　審査の目的

ウ　審査基準及び関連基準文書

エ　審査範囲（共同事業所を含む）

オ　審査の計画

審査チーム及び同行者、使用する言語、審査日時、審査場所（共同事業所を含む）、予定時刻及び所要時間、審査する組織単位、審査方法、経営者との会議、審査結果について、その他

カ　審査報告書

キ　機密保持

ク　異議申立て

ケ　審査のフォローアップ処置

⑵　また、審査計画書の審査の計画において、次の項目の予定時刻及び所要時間を明確にします。

ア　オープニング・ミーティング（初日）

審査チーム・リーダーが、認証範囲/基準を確認し、チームメンバーを紹介し、審査の目的及び方法、審査手順の説明等により、審査に必要な事項について合意します。

イ　審査の実施（毎日）

担当審査員、審査対象部署毎の審査項目、予定時刻及び所要時間を決めて審査を実施します。

ウ　審査チーム・ミーティング（最終日を除く毎日レビュー・ミーティング前）

担当審査員が複数の場合、審査チーム内の調整のため審査チーム・ミーティングを計画させていただきます。

エ　レビュー・ミーティング（最終日を除く毎日審査終了後）

当日の実施状況、進捗状況、不適合及び気付事項等を顧客に報告します。特に不適合については、双方の認識に差のないことを確認します。

オ　ブリーフィング（２日目以降毎日審査開始前）

不適合事項等について顧客側の説明があれば受けます。当日の審査計画を確認します。変更事項、追加調査事項、確認文書／記録等のある場合は調整します。

カ　審査チーム・ミーティング（最終）（プリクロージング・ミーティング前）

担当審査員が複数の場合、審査結果について審査チーム内の最終調整のため審査チーム・ミーティングを計画させていただきます。

キ　プリクロージング・ミーティング（最終日）

審査結果の概要について審査チームと顧客側の管理責任者及び事務局と協議し、クロージング・ミーティングの効率的な進行の妨げとなる事項及び審査の成果を損なうような要因をクロージング・ミーティングに先立ち、調整します。

ク　クロージング・ミーティング（最終日）

顧客の経営者出席のもと、審査チーム・リーダーが審査で確認した事項に基づいて、審査の結果（不適合、気付事項及び全般状況等）及び審査後の手順等について説明します。

⑶　初回２の実施場所は、原則として顧客のすべてのサイトの現地で実施するものとします。場所及び日程については事前に申請顧客と合意をとります。また、「経営者の責任」の審査及びクロージン

グ・ミーティングについては、経営者の出席を原則として日時を計画します。

⑷　審査計画書は、必要に応じて顧客と協議・調整をして作成し、顧客に配布します。

４．２．３．４　初回２の実施

⑴　初回２は、審査計画書（初回２）に基づいて実施します。

⑵　初回２では、顧客の情報セキュリティマネジメントシステムの全ての要求事項に対して適合性及び有効性があることを確認することを目的として、情報セキュリティマネジメントシステムの実施状況を含めて審査します。審査においては、次の事項についての評価を行います。

ア　適用される情報セキュリティマネジメントシステム規格又はその他の規準文書の、すべての要求事項に対する適合についての情報及び証拠

イ　主要なパフォーマンスの目的及び目標（適用する情報セキュリティマネジメントシステム規格又はその他の規準文書の主旨に整合した）に対するパフォーマンスの監視、測定、報告及びレビュー

ウ　法的要求事項の順守に関しての、顧客の情報セキュリティマネジメントシステム及びパフォーマンス

エ　顧客のプロセスの運用管理

オ　内部監査及びマネジメントレビュー

カ　顧客の方針に対する経営層の責任

キ　規定要求事項、方針、パフォーマンスの目的及び目標（適用する情報セキュリティマネジメントシステム規格又はその他の規準文書の主旨に整合した）、適用されるすべての法的要求事項、責任、要員の力量、運用、手順、パフォーマンスに関するデータ、及び内部監査の所見・結論の関連

⑶　不適合については、「是正処置要求書（ＣＡＲ）」を発行します。適用規格の要求に不適合ではないが、審査中気付いた情報セキュリティマネジメントシステムをより良くするための改善事項については、気付事項をあげます。

⑷　初回２の現地で、追加審査又はフォローアップ審査が必要と判断した場合は、その旨説明します。

⑸　初回２において、サーベイランス審査の間隔及び次回審査の予定日について顧客の要望を確認し、計画します。（５．２．１．２「サーベイランス審査間隔及び審査時期の決定」参照。）

⑹　審査終了後、情報セキュリティマニュアル１部をシステム審査センター事務所保管用として受領します。（事前に情報セキュリティマニュアルを事務所あて送付いただいている場合は該当しません）。

４．２．３．５　第２段階審査報告書の作成

⑴　初回２チーム・リーダーは、初回２終了後、顧客を離れる前に、初回審査　審査報告書(暫定版)に関する情報を~~作成し、~~顧客に提示提出し、~~報告書に対する~~顧客の意見を求めます。初回審査審査報告書（暫定版）は、最終会議終了後２週間以内に提出します。

⑵　作成した「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」は、顧客を離れる前に提出します。電子データも同時に配布します。

４．２．３．６　不適合の修正及び是正処置

⑴　不適合がある場合、３．３項に基づき不適合の修正及び是正処置を検討していただき、不適合の修正及び是正処置の計画又は実施が完了しましたら、初回２チーム・リーダーに不適合の修正及び是正処置の計画又は実施完了の連絡と次の資料の提出をしていただきます。

ア　是正処置要求書（記入し署名した原紙）　１部

イ　修正・是正処置回答書（記入し記名した原紙及び電子データ）　　１部
ウ　修正及び是正処置の証拠としての文書又は記録の該当部分　　１部
エ　情報セキュリティマネジメントシステム文書リスト(変更がある場合）１部

⑵　ＢＳＫは、提出していただいた資料を確認し、十分であれば、確認結果を記入した「是正処置要求書」及び「修正・是正処置回答書」を付けて「審査報告書」を作成し認証可否の判定に進めます。不十分であれば、その旨顧客に連絡し、⑴を実施していただきます。

⑶　⑴の修正及び是正処置の実施計画及び実施計画に基づく実施は、原則として是正要求書の発行日から３０日以内にＢＳＫにより十分であるとの確認を得られるようにしてください。ただし、JIS Q 27001 情報セキュリティマネジメントシステムにおける軽微不適合ついては、修正及び是正処置の実施計画の確認が十分であれば、４．３項の認証可否の判定を実施します。その際、実施計画に基づく実施の結果は実施期限までに報告してください。

⑷　顧客の修正・是正処置が不十分であり、認証可否の判定に進むことができないと判断した場合には、確認結果（不十分）を連絡し、是正を要求します。必要な場合、初回２のフォローアップ審査が必要であることを顧客に通知します。この場合、修正・是正処置を容認できない旨を記した、「審査報告書」を作成し顧客に配布します。

４．３　認証可否の判定及び通知

⑴　認証可否の判定は、審査報告書等に基づきＢＳＫのマネジメントシステム判定委員会において行われます。

⑵　ＢＳＫは、判定終了後速やかに、判定結果を顧客に文書で通知するとともに、審査報告書を送付します。

４．４　認証書の発行

⑴　ＢＳＫは、判定委員会において合格と判定された場合、顧客が希望する枚数の情報セキュリティマネジメントシステム認証書（以下「認証書」という。）を発行します。認証書には、適用規格、適用基準、認証範囲、認証年月日、有効期限、サイトの名称（共同事業所を含む）等が明記されます。

⑵　ＢＳＫは、ＢＳＫの登録簿（認証リスト）に登録します。

⑶　認証書の有効期間は３年です。（ＢＳＫ以外の認証機関からＢＳＫへ登録移転した場合は、移転前認証書の残り有効期間です。）

⑷　ＢＳＫは、認証書を発行した顧客名、所在地、認証範囲などを含む登録簿を作成し、定期的に公開する権利を保有します。但し顧客の要望で、全部又は一部非公開とすることが可能です。（４．７項参照）

４．５　審査費用の請求と納付

ＢＳＫは、初回２後の判定委員会終了時に顧客に初回審査料を請求します。請求に基づき初回審査料の納付をしていただきます。

４．６　認定シンボル等及び認証書の取扱い

４．６．１　認定シンボル等の使用

ＩＳＭＳ－ＡＣの認定シンボル並びにＢＳＫのマーク（以下「認定シンボル等」という。）を使用する場合の遵守事項及び使用条件等についてはＰ０８０４０１「認証の引用及びマーク使用規定」の定めによります。

ＩＳＭＳ－ＡＣ：情報マネジメントシステム認定センター

４．６．２　認証書の取扱い

４．６．２．１　認証書等の使用禁止

認証を授与された顧客は、次のいずれかに該当する場合、認証書及び認定シンボル等の掲示又は、その他の使用を禁止します。

⑴　認証の失効、一時停止又は取消し時

⑵　顧客が情報セキュリティマネジメントシステムを大幅に変更し、ＢＳＫに変更申請がない場合

４．６．２．２　認証書の誤用

ＢＳＫは、顧客が認証書を不適切に引用又は、誤解を招くような方法で使用した場合は、是正処置の要求又は公表など必要な処置を講ずることがあります。

認証書の管理に関しては、４．６．２項に加え、Ｐ０８０４０１「認証の引用及びマーク使用規定」も確認して下さい。

４．７　ＩＳＭＳ－ＡＣへの登録、登録情報の公開

顧客は、JIS Q 27001の認証取得についてＩＳＭＳ－ＡＣへの登録が義務付けられています。但しＩＳＭＳ－ＡＣ及びＢＳＫのホームページ等での認証の公開については全部又は一部分の非公開を選択することができます。登録時に顧客に事前確認をした上で公開又は非公開とします。

４．８　審査報告書の取扱い

⑴　審査報告書の所有権は、ＢＳＫに帰属します。審査報告書の使用と保管に関して次の事項を守ってください。

1)審査報告書の使用

顧客のお客様／潜在的な（将来お客様になる可能性のある）お客様／監督官庁／ＩＳＭＳ－ＡＣには、審査報告書を提示（閲覧のみ）することができます。但し、審査報告書を提出する場合は、文書（電子メールを含む）によるＢＳＫの同意が必要です。

顧客のお客様／潜在的な（将来お客様になる可能性のある）お客様／監督官庁／ＩＳＭＳ－ＡＣ以外には、文書（電子メールを含む）によるＢＳＫの同意がない限り審査報告書を提示も提出もしてはいけません。

2)審査報告書の保管

審査報告書は、最低限６年間保管してください。

⑵ 顧客は、顧客のお客様等から審査報告書の提出を求められた場合は、次の事項を守って下さい。

1)　使用用途を明確にし、配布管理台帳等で配布管理を適切に行って下さい。
ＢＳＫの同意が必要なものについては、ＢＳＫの同意の証拠（文書（電子メールを含む））を維持、保管してください。

2)　提出は、ＢＳＫから送付されたフルセットを基本とします。審査報告書の一部分を提出することはできません。配布管理台帳等にフルセットであることを記録してください。

3) 顧客がＢＳＫから他認証機関に認証の移転をされる場合、移転先の認証機関からＢＳＫの審査報告書の提出を求められることがありますが、その場合もＢＳＫの同意が必要です。

⑶　ＢＳＫとの同意の要領については、以下を基準とします。

1) 文書（電子メールを含む）による記載内容については以下の例により記載してください

（例１：審査報告書の提出に関する同意の依頼）

【審査報告書の提出に関する同意について（依頼）】

以下のとおり、審査報告書を提出したいので同意を受けたく依頼します。

1　該当報告書名
2　提出先組織の名称
3　提出先組織の区分（該当区分を記入）
□顧客のお客様
□潜在的な（将来お客様になる可能性のある）お客様
□監督官庁
□ＩＳＭＳ－ＡＣ
□その他（上記以外）
4　使用用途（提出理由）
5　提出予定時期
6　必要部数
（提出は、一部分ではなく、ＢＳＫから送付された報告書のフルセットとします。）
7　回答希望年月日

（例２：審査報告書の提示に関する同意の依頼（顧客のお客様／潜在的な（将来お客様になる可能性のある）お客様／監督官庁／ＩＳＭＳ－ＡＣ以外の場合））

【審査報告書の提示に関する同意について（依頼）】

以下のとおり、審査報告書を提示したいので同意を受けたく依頼します。

1　該当報告書名
2　提示先組織の名称
3　提示先組織の区分（その他）
（組織との関係を記述してください。）
4　使用用途（提示理由）
5　提示時期
6　回答希望年月日

2）依頼先

ＢＳＫシステム審査センター　審査業務部長
（連絡担当者：審査業務部　業務第１課長）

第５章　サーベイランス審査

５．１　サーベイランス審査の費用

サーベイランス審査は、初回審査時の契約又は再認証時の契約に基づいて実施します。サーベイランス審査の費用については、原則として見積りはせず、サーベイランス審査終了後に請求します。

５．２　サーベイランス審査の実施

５．２．１　サーベイランス審査概要

５．２．１．１　サーベイランス審査の目的

サーベイランス審査は、被認証組織の認証されたマネジメントシステムが、継続して要求事項に対して適合していること、及び有効性があることを確認することを目的として実施します。

５．２．１．２　サーベイランス審査間隔及び審査時期の決定

⑴　サーベイランス審査は、「基準日」（注記1,2参照）を起算日として１２か月毎に実施することを基本的な考え方とします。但し、顧客から要望がある場合には、６か月毎に実施することができま

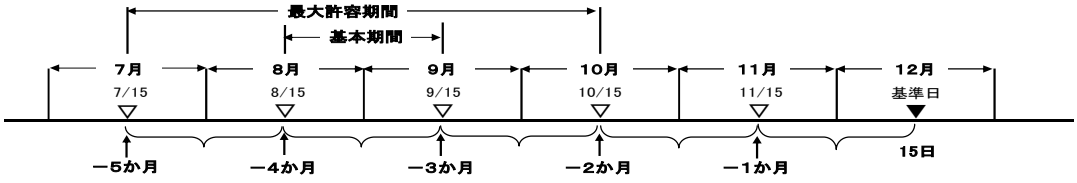
す。なお、初回認証に続く最初のサーベイランス審査の期日は、認証の決定をした日から１２か月を超えないものとします。

注記：「基準日」とは、審査の日程を設定するための基準の日付のことであり、通常は初回審査の認証日です。但し、繰上再認証審査を実施して基準日を変更した場合には、繰上再認証審査の認証日となります。

⑵　サーベイランス審査の実施時期は、「基準日」を起算日とし、次によります。

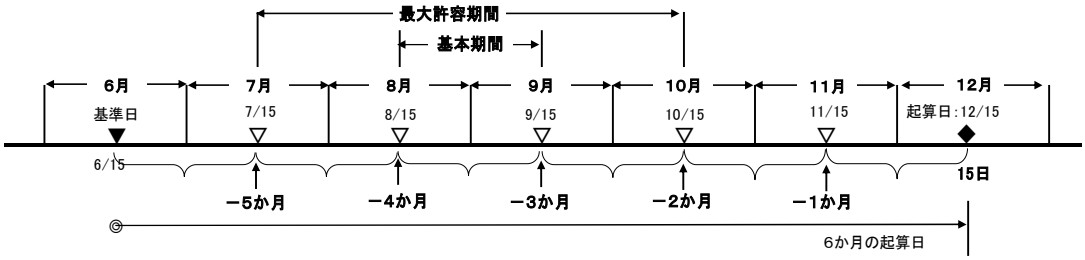
ア　１２か月毎のサーベイランス審査の場合（１年定期）

基準日を起算日として、原則としてマイナス４か月からマイナス３か月の間に実施します。但し、マイナス５か月からマイナス２か月までに実施することを許容します。（下図参照）



イ　６か月毎のサーベイランス審査の場合（６か月定期）

基準日及び初回認証日プラス６か月を起算日として、原則としてマイナス４か月からマイナス３か月以内に実施します。但し、プラス１か月からマイナス３か月以内に実施することを許容します。初回認証日(例：6/15)プラス６か月の場合の審査期間を下図に示します。



５．２．２　サーベイランス審査

５．２．２．１　審査日程及び審査担当審査要員の顧客との合意

ＢＳＫは、審査受審２か月前までに顧客と日程を調整します。ＢＳＫは、顧客に審査日程を通知し合意を受けます。同時に、審査担当審査要員の情報(経歴)等を記した「担当審査要員の確認依頼について」を顧客に送付して、異議の有無を確認します。

サーベイランス審査に於いて、組合せ型審査への変更を希望する場合は、「認証内容変更申請書」と「組合せ型審査申請書」の提出が必要です。詳細は「7.1項の（変更申請及び変更審査）をご参照ください。

組合せ型審査の場合、マネジメントシステム間の「基準日」が異なる時には、基準日の変更等調整をさせて頂く場合が有りますので、ご了解下さい。また、統合の程度により統合審査から複合審査又は同時審査、複合審査から同時審査に変更させて頂く場合があります。

５．２．２．２　情報セキュリティマネジメントシステム文書の提出

最新の審査にて提出頂いた情報セキュリティマネジメントシステム文書の最新版（更新分）を提出ください。（４．２．２．２項 参照）

５．２．２．３　サーベイランス審査の事前調整

⑴　ＢＳＫの審査チーム・リーダーは、顧客に、前回の審査後の変更事項の有無の確認を含めた審査計画の調整を行います。
⑵　変更事項（共同事業所を含む）のある場合、顧客に、「認証内容変更申請書」の提出を求めます。

５．２．２．４　審査計画書（サーベイランス審査）の作成

⑴　ＢＳＫは、事前調整結果を基に審査計画書を作成し、次の事項を明確にします。
ア　顧客の所在地、代表者
イ　審査の目的
ウ　審査基準及び関連基準文書
エ　審査範囲（共同事業所を含む）
オ　審査の計画
審査チーム及び同行者、使用する言語、審査日時、審査場所（共同事業所を含む）、予定時刻及び所要時間、審査する組織単位、審査方法、経営者との会議、審査結果について、その他
カ　審査報告書
キ　機密保持
ク　異議申立て
ケ　審査のフォローアップ処置
⑵　また、審査計画書の審査の計画において、次の項目の予定時刻及び所要時間を明確にします。
ア　オープニング・ミーティング（初日）
審査チーム・リーダーが、認証範囲/基準を確認し、チームメンバーを紹介し、審査の目的及び方法、審査手順の説明等により、審査に必要な事項について合意します。
イ　審査の実施（毎日）
担当審査員、審査対象部署毎の審査項目、予定時刻及び所要時間を決めて審査を実施します。
ウ　審査チーム・ミーティング（最終日を除く毎日レビュー・ミーティング前）
担当審査員が複数の場合、審査チーム内の調整のため審査チーム・ミーティングを計画させていただきます。
エ　レビュー・ミーティング（最終日を除く毎日審査終了後）
当日の実施状況、進捗状況、不適合及び気付事項等を顧客に報告します。特に不適合については、双方の認識に差のないことを確認します。
オ　ブリーフィング（２日目以降毎日審査開始前）
不適合事項等について顧客側の説明があれば受けます。当日の審査計画を確認します。変更事項、追加調査事項、確認文書／記録等のある場合は調整します。
カ　審査チーム・ミーティング（最終）（プリクロージング・ミーティング前）
担当審査員が複数の場合、審査結果について審査チーム内の最終調整のため審査チーム・ミーティングを計画させていただきます。
キ　プリクロージング・ミーティング（最終日）
審査結果の概要について審査チームと顧客側の管理責任者及び事務局と協議し、クロージング・ミーティングの効率的な進行の妨げとなる事項及び審査の成果を損なうような要因をクロージング・ミーティングに先立ち、調整します。
ク　クロージング・ミーティング（最終日）
顧客の経営者出席のもと、審査チーム・リーダーが審査で確認した事項に基づいて、審査の結果（不適合、気付事項及び全般状況等）及び審査後の手順等について説明します。
⑶　サーベイランス審査の実施場所は、初回審査又は再認証審査時に決めます。
⑷　場所及び日程については事前に申請顧客と合意をとります。また、「経営者の責任」の審査及びクロージング・ミーティングについては、経営者の出席を原則として日時を計画します。

⑸　審査計画書は、必要に応じて顧客と協議・調整をして作成し、顧客に概ね１か月前に配布します。

５．２．２．５　サーベイランス審査の実施

⑴　サーベイランス審査は、審査計画書（サーベイランス審査）に基づいて実施します。

⑵　サーベイランス審査では、顧客の認証された情報セキュリティマネジメントシステムが、継続して要求事項に対して適合していること、及び有効性があることを確認することを目的として実施します。審査においては、次の事項についての評価を行います。

ア　内部監査及びマネジメントレビューのプロセス

イ　前回の審査で特定された不適合についてとられた処置の有効性のレビュー

ウ　苦情処理

エ　顧客の目的達成及びマネジメントシステムの意図した結果の達成に関するマネジメントシステムの有効性

オ　継続的改善を狙いとする計画的活動の進捗状況

カ　運用管理に関するマネジメントシステムの有効性

キ　マネジメントシステムの変更の有効性に影響を及ぼすか又は影響する恐れのある変更内容に関する情報

ク　認証書の管理、認定シンボル等の使用及び認証に関する引用

⑶　不適合については、「是正処置要求書（ＣＡＲ）」を発行します。適用規格の要求に不適合ではないが、審査中気付いたＩＳＭＳをより良くするための改善事項については、気付事項をあげます。

⑷　審査終了後、マニュアル１部をシステム審査センター事務所保管用として受領します。（事前に当該マニュアルを事務所あて送付いただいている場合は該当しません）。

５．２．２．６　サーベイランス審査報告書の作成

⑴　サーベイランス審査チーム・リーダーは、サーベイランス審査終了後、顧客を離れる前に、サーベイランス審査　審査報告書(暫定版)に関する情報を作成し、顧客に提示提出し、報告書に対する顧客の意見を求めます。サーベイランス審査　審査報告書(暫定版)は、最終会議終了後２週間以内に提出します。

⑵　作成した「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」は、顧客を離れる前に提出します。電子データも同時に配布します。

５．２．２．７　不適合の修正及び是正処置

⑴　不適合がある場合、３．３項に基づき不適合の修正及び是正処置を検討していただき、不適合の修正及び是正処置の計画又は実施が完了しましたら、サーベイランス審査チーム・リーダーに不適合の修正及び是正処置の計画又は実施完了の連絡と次の資料の提出をしていただきます。

ア　是正処置要求書（記入し署名した原紙）　１部

イ　修正・是正処置回答書（記入し記名した原紙及び電子データ）　１部

ウ　修正及び是正処置の証拠としての文書又は記録の該当部分　１部

エ　情報セキュリティマネジメントシステム文書リスト(変更がある場合)　１部

⑵　ＢＳＫは、提出していただいた資料を確認し、十分であれば、確認結果を記入した「是正処置要求書」及び「修正・是正処置回答書」を付けて「審査報告書」を作成し認証の維持の可否の判定に進めます。不十分であれば、その旨顧客に連絡し、⑴を実施していただきます。

⑶　⑴の修正及び是正処置の実施計画及び実施計画に基づく実施は、原則として是正要求書の発行日から３０日以内にＢＳＫにより十分であるとの確認を得られるようにしてください。ただし、軽微不適合については、修正及び是正処置の実施計画の確認が十分であれば、５．３項の認定維持の可

否の判定を実施します。その際、実施計画に基づく実施の結果は実施期限までに報告してください。

⑷ 顧客の修正・是正処置が不十分であり、認証の維持の可否の判定に進むことができないと判断した場合には、確認結果（不十分）を連絡し、是正を要求します。必要な場合、サーベイランス審査のフォローアップ審査が必要であることを顧客に通知します。この場合、修正・是正処置を容認できない旨を記した、「審査報告書」を作成し顧客に配布します。

５．３ 認証維持の可否の判定及び通知

⑴ 認証維持の可否の判定は、審査報告書等に基づき行います。但し、認証の一時停止又は取消しの可能性がある場合又は変更審査を兼ねて実施した場合は、ＢＳＫのマネジメントシステム判定委員会において判定が行われます。

⑵ ＢＳＫは、判定終了後速やかに、判定結果を顧客に文書で通知するとともに、審査報告書を送付します。

５．４ 審査費用の請求と納付

ＢＳＫは、認証の維持の可否の判定が行われた後に、顧客にサーベイランス料を請求します。請求に基づきサーベイランス料の納付をしていただきます。

５．５ 認定シンボル等及び認証書の取扱い

４．６項によります。

５．６ ＩＳＭＳ－ＡＣへの登録変更、登録情報の公開

４．７項に準じます。

５．７ 審査報告書の取扱い

４．８項によります。

第６章 再認証審査

６．１ 契約手続き

６．１．１ 申請の準備及び事前協議

⑴ 再認証の審査は３年毎に行われます。この再認証の審査を受けなければ認証は失効します。

⑵ ＢＳＫは、認証有効期限の６か月前迄に、再認証申請に必要な次の資料（以下「申請資料」という。）を顧客に送付し、認証の有効期限４か月前までに所要の事項を記入のうえＢＳＫへの返送を求めます。顧客（共同事業所を含む）の情報セキュリティマネジメントシステムに変更がある場合は、合わせて「認証内容変更申請書」の提出を求めます。認証内容変更申請書の提出にあたっては、ＢＳＫが作成する審査計画書の作成時期等（審査予定日の１か月以前を目途）により認証の有効期限の４か月前より更に前に提出していただく場合もありますのでご理解をいただき速やかな提出をお願いします。

ア 認証申請書様式とその電子データ

イ 認証合意書様式（２通）（新様式（F-P090201-41）により合意をしたものについては以後の認証合意書の提出は不要です。）

再認証審査に於いて、組合せ型審査への変更を希望する場合は、「認証内容変更申請書」と「組合

せ型審査申請書」の提出が必要です。詳細は「7.1項の（変更申請及び変更審査）をご参照ください。

⑶ 申請資料受領後、申請内容の検討をして申請資料への記入をしていただきます。申請資料への記入について、問合せ、相談がありましたら、連絡をお願いします。

⑷ 顧客が申請内容等（共同事業所を含む）の詳細について事前協議を希望する場合は、ＢＳＫの顧客への訪問又は顧客のＢＳＫへの来訪により、協議を行います。

６．１．２ 申請及びＢＳＫによる申請のレビュー

⑴ 顧客は、送付を受けた認証合意書の内容について確認し、同意のうえ、認証申請書及び認証合意書（２通）に申請責任者の記名・押印をしてＢＳＫに返送していただきます。認証合意書は契約書となりますので、申請責任者（共同事業所を含む）は経営責任者（経営責任者が指名した者を含む。）又は管理責任者としてください。また、認証内容変更申請書がある場合は、所要の事項を記入して、併せてＢＳＫ宛に送付していただきます。認証申請書及び認証内容変更申請書については、電子データをメールにてＢＳＫへご送付下さい。

⑵ ＢＳＫは、申請資料の確認をし、形式的な、書類不備、記入漏れ、情報不足等がありましたら、顧客に連絡します。必要な場合、修正・再提出を依頼しますので、対応をお願いします。

⑶ ＢＳＫは、申請資料の内容について、審査を含む認証活動を行うために必要な包括的なレビュー（申請のレビュー）を行います。申請のレビューにおいて、顧客に問合せ・調整が必要になりましたら連絡しますので対応をお願いします。また、申請のレビューの結果、認証申請書及び認証内容変更申請書について、変更が必要な部分があるとＢＳＫとして判断した場合は、変更案を送付しますので、当該変更内容に関する評価・検討をして、変更申請書の作成・提出をお願いします。

６．１．３ 契約書類

⑴ ＢＳＫは、顧客から送付を受けた認証合意書２通に記名・押印します。認証業務の契約は、顧客から送付を受けた認証合意書２通にＢＳＫが記名・押印した段階で成立します。

⑵ ＢＳＫは、顧客から送付を受けた申請資料に基づき、再認証審査に関する費用の見積りを行い、契約書類として、見積書及びＢＳＫが記名・押印した認証合意書（１通）を顧客に送付します。また、最新の該当する認証ガイドを顧客に送付いたします。

⑶ 前⑵の見積書及び認証合意書の送付に併せて再認証審査に必要な情報セキュリティマネジメントシステム文書の提出を要求します。提出していただく情報セキュリティマネジメントシステム文書は、４．２．２．２「情報セキュリティマネジメントシステム文書の提出」の通りです。

⑷ 契約書類及び情報セキュリティマネジメントシステム文書の提出の要求に対して疑義がある場合はＢＳＫに対して申し出をすることができます。

６．２ 再認証審査の実施

６．２．１ 再認証審査概要

６．２．１．１ 再認証審査の目的及び概略プロセス

⑴ 再認証審査の目的は、顧客（共同事業所を含む）の情報セキュリティマネジメントシステム全体としての継続的な適合性、及び有効性、並びに認証の範囲に対する情報セキュリティマネジメントシステムの継続的な関連性及び適用可能性を確認することです。

⑵ 再認証審査は、原則として1段階方式で実施するものとします。但し、情報セキュリティマネジメントシステム、顧客（共同事業所を含む）、又は情報セキュリティマネジメントシステムを運営する状況に重要な変更がある状況において、情報セキュリティマネジメントシステム文書の大幅な変更を伴う様な、変更審査や拡大審査を伴う場合には、必要に応じて初回審査に準じた、再認証審査・第１段階（略称：再認証１）及び再認証審査・第２段階（略称：再認証２）の２段階方式で実

施します。
尚、このような変更は、認証周期中いつでも起こることがあり、1段階方式又は2段階方式による特別審査を必要に応じて実施します。

⑶　再認証審査では、認証の全期間にわたる情報セキュリティマネジメントシステムのパフォーマンスを考慮し、また、それまでのサーベイランス審査報告書のレビューを含むよう実施します。

６．２．１．２　審査時期の決定

⑴　再認証審査は、「基準日」を起算日として３年毎に実施します。 但し、顧客から要望がある場合は、認証書の有効期間を短縮して再認証審査を実施することができます。「基準日」を変更するために時期を早めて実施する再認証審査を「繰上再認証審査」といいます。

注記：「基準日」とは、審査の日程を設定するための基準の日付のことであり、通常は初回審査の認証日です。但し、繰上再認証審査を実施して基準日を変更した場合には、繰上再認証審査の認証日となります。

⑵　再認証審査の実施時期は、「基準日」を起算日とし、次によります。

ア　１段階方式での実施時期は、下記の２つの条件を共に満足する時期とします。

①基準日」を起算日とし、原則としてマイナス４か月からマイナス３か月の間に実施します。但し、マイナス５か月からマイナス２か月までに実施することを許容します。

②再認証審査で指摘された不適合について顧客が実施する是正処置の期間を確保するため、再認証審査の結果報告を予定している判定委員会(原則として毎月２回開催)の開催日よりも１か月以上前とします。

イ　２段階方式での実施時期は、原則として上記アに準じますが、必要に応じて再認証１実施時期の前倒しを許容します。

尚、組合せ型審査の場合、マネジメントシステム間の「基準日」が異なる時には、基準日の変更等の調整をさせて頂く場合が有りますので、ご了解下さい。

６．２．２　再認証審査

⑴　１段階方式の場合は５．２．２項「サーベイランス審査」に準じて、２段階方式の場合は４．２．２項「初回１」及び４．２．３項「初回２」に準じて実施します。また、１段階方式、２段階方式の何れ

の場合においても、同時に過去３年間のマネジメントシステム実施状況と現在の維持状況をレビューします。

⑵　文書レビュー

初回審査と同様に現地審査前に、再認証審査を円滑に進めるために、マニュアル等を提出していただき、それをレビューし、問題点がある場合「文書問題点」として指摘します。
これを解決して回答していただくことが審査へ進む条件となります。（４．２．２．２項 参照）

⑶ 再認証審査においては要求事項の全項目を確認する他、以下のア～ウを確認します。

ア　内部及び外部の変更に対する情報セキュリティマネジメントシステム全体としての有効性、並びに認証の範囲に対する情報セキュリティマネジメントシステムの継続的な関連性及び適用可能性

イ　全体のパフォーマンスを高めるために、情報セキュリティマネジメントシステムの有効性を維持し、改善し続けることに対する実証されたコミットメント

ウ　顧客の目的の達成及び各マネジメントシステムの意図した結果の達成に関するマネジメントシステムの有効性の評価

⑷　ＢＳＫからの顧客（共同事業所を含む）に対する認証要求事項の変更があった場合、顧客の対応状況を検証します。尚、確認の結果、顧客について、認証の要求事項に対する不適合又は不履行があった場合は、適切な是正処置の有無を確認します。未処置の場合、顧客と協議して、合意した期間内に是正を求めます。是正処置が取られない場合は、認証の縮小、一時停止又は取り消すことになります。

６．２．２．１　審査計画書（再認証審査）の作成

⑴　ＢＳＫは、事前調整結果を基に審査計画書を作成し、次の事項を明確にします。

ア　顧客の所在地、代表者

イ　審査の目的

ウ　審査基準及び関連基準文書等

エ　審査範囲（共同事業所を含む）

オ　審査の計画

審査チーム及び同行者、使用する言語、審査日時、審査場所（共同事業所を含む）、予定時刻及び所要時間、審査する組織単位、審査方法、経営者との会議、審査結果について、その他

カ　審査報告書

キ　機密保持

ク　異議申立て

ケ　審査のフォローアップ処置

⑵　また、審査計画書の審査の計画において、次の項目の予定時刻及び所要時間を明確にします。

ア　オープニング・ミーティング（初日）

審査チームリーダーが、認証範囲/基準を確認し、チームメンバーを紹介し、審査の目的及び方法、審査手順の説明等により、審査に必要な事項について合意します。

イ　審査の実施（毎日）

担当審査員、審査対象部署毎の審査項目、予定時刻及び所要時間を決めて審査を実施します。

ウ　審査チーム・ミーティング（最終日を除く毎日レビュー・ミーティング前）

担当審査員が複数の場合、審査チーム内の調整のため審査チーム・ミーティングを計画させていただきます。

エ　レビュー・ミーティング（最終日を除く毎日審査終了後）

当日の実施状況、進捗状況、不適合及び気付事項等を顧客に報告します。特に不適合については、双方の認識に差のないことを確認します。

オ　ブリーフィング（２日目以降毎日審査開始前）

不適合事項等について顧客側の説明があれば受けます。当日の審査計画を確認します。変更事項、追加調査事項、確認文書／記録等のある場合は調整します。

カ　審査チーム・ミーティング（最終）（プリクロージング・ミーティング前）

担当審査員が複数の場合、審査結果について審査チーム内の最終調整のため審査チーム・ミーティングを計画させていただきます。

キ　プリクロージング・ミーティング（最終日）

審査結果の概要について審査チームと顧客側の管理責任者及び事務局と協議し、クロージング・ミーティングの効率的な進行の妨げとなる事項及び審査の成果を損なうような要因をクロージング・ミーティングに先立ち、調整します。

ク　クロージング・ミーティング（最終日）

顧客の経営者出席のもと、審査チームリーダーが審査で確認した事項に基づいて、審査の結果

（不適合、気付事項及び全般状況等）及び審査後の手順等について説明します。

６．２．３　再認証審査報告書の作成

⑴　再認証審査チーム・リーダーは、再認証審査終了後、顧客を離れる前に、再認証審査　審査報告書(暫定版)に関する情報を作成し、顧客に提示提出し、報告書に対する顧客の意見を求めます。
再認証審査　審査報告書(暫定版)は、最終会議終了後２週間以内に提出します。

⑵　「是正処置要求書（ＣＡＲ）」及び「修正・是正処置回答書」は、顧客を離れる前に提出します。電子データも同時に配布します。

６．２．４　不適合の修正及び是正処置

⑴　不適合がある場合、３．３項に基づき不適合の修正及び是正処置を検討していただき、不適合の修正及び是正処置の計画又は実施が完了しましたら、再認証審査チーム・リーダーに不適合の修正及び是正処置の計画又は実施完了の連絡と次の資料の提出をしていただきます。

ア　是正処置要求書
　　（記入し署名した原紙）　１部
イ　修正・是正処置回答書　　（記入し記名した原紙及び電子データ）　１部
ウ　修正及び是正処置の証拠としての文書又は記録の該当部分　１部
エ　情報セキュリティマネジメントシステム文書リスト(変更がある場合)　１部

⑵　ＢＳＫは、提出していただいた資料を確認し、容認出来る場合、確認結果を記入した「是正処置要求書」及び「修正・是正処置回答書」を付けて「審査報告書」を作成し認証可否の判定に進めます。不十分であれば、その旨顧客に連絡し、⑴を実施していただきます。

⑶　⑴の修正及び是正処置の実施計画及び実施計画に基づく実施は、原則として是正要求書の発行日から３０日以内にＢＳＫにより十分であるとの確認を得られるようにしてください。ただし、軽微不適合については、修正及び是正処置の実施計画の確認が十分であれば、期限が認証の有効期限内であることを条件に、４．３項の認証可否の判定を実施します。その際、実施計画に基づく実施の結果は実施期限までに報告してください。

⑷　顧客の修正・是正処置が不十分であり、認証可否の判定に進むことができないと判断した場合には、確認結果（不十分）を連絡し、是正を要求します。必要な場合、再認証審査のフォローアップ審査が必要であることを顧客に通知します。この場合、修正・是正処置を容認できない旨を記した、「審査報告書」を作成し顧客に配布します。

６．３　再認証可否の判定及び通知

４．３項を準用します。

６．４　認証書の発行

４．４項を準用します。

６．５　審査費用の請求と納付

４．５項を準用します。

６．６　認定シンボル等及び認証書の取扱い

４．６項によります。

６．７　ＩＳＭＳ－ＡＣへの登録、登録情報の公開

４．７項によります。

６．８　審査報告書の取扱い

４．８項によります。

第７章　特別審査

７．１　変更申請及び変更審査

７．１．１　顧客による変更申請及びＢＳＫによる申請のレビュー

⑴　顧客は、次の項目に該当した場合、速やかに別に定める認証内容変更申請書を提出して下さい。なお、認証内容変更申請書は、電子データも合わせて提出して下さい。

ア　認証データシート及び／又は認証書への記載事項の変更

①　経営者の役職、氏名

②　対象従業員数

・料金表に定める審査料に影響する従業員数の増加／減少がある場合

③　管理責任者の所属、役職、氏名、所在地、TEL、FAX、E-mail

④　連絡担当者の所属、役職、氏名、所在地、TEL、FAX、E-mail

⑤　被認証組織（共同事業所を含む）の名称、所在地

・名称は、会社名、事業所名、工場名、事業部門名等

・所在地は、市町村合併／住所表記のみの変更を含む

⑥　適用規格・適用基準

・規格の改定による旧版から最新版への移行

⑦　認証範囲

・製品名、サービス名の追加／削除／変更

・活動名（プロセス、製造工程等）の追加／削除／変更

⑧　適用除外

⑨　産業分類

・経済産業分類の追加／削除

⑩　認証に含まれるサイト（共同事業所を含む）の名称、所在地、認証範囲

・サイトの名称、所在地の変更

・サイト毎の製品・サービス名、活動名等の変更

⑪　適用宣言書の名称及び版数

イ　認証書改訂の希望時期

①　速やかな改訂発行を希望する場合、単独の変更審査を実施いたします。

②　次回審査時に改訂発行を希望する場合、次回審査に合わせて変更審査を実施します。

ウ　被認証組織が次を希望する場合

①　認証書の統合

・個別に認証されている２通以上の認証書を統合する

②　認証書の分割

・１通の認証書を２通以上の認証書に分割する

エ　その他

① 被認証組織の情報セキュリティマニュアルの改定
② 被認証組織の情報セキュリティマネジメントシステム文書の大幅な変更
③ 被認証組織の部門の追加又は削除
④ 被認証組織の部門の対象人員数の大幅な増加又は減少

⑵ ＢＳＫは、認証内容変更申請書の確認をし、形式的な、書類不備、記入漏れ、情報不足等がありましたら、顧客に連絡します。必要な場合、修正・再提出を依頼しますので、対応をお願いします。

⑶ ＢＳＫは、認証内容変更申請書の内容について、審査を含む認証活動を行うために必要な包括的なレビュー(申請のレビュー)を行います。申請のレビューにおいて、顧客（共同事業所を含む）に問合せ・調整が必要になりましたら連絡しますので対応をお願いします。また、申請のレビューの結果、認証内容変更申請書について、変更が必要な部分があるとＢＳＫとして判断した場合は、変更案を送付しますので、当該変更内容に関する評価・検討をして、変更申請書の作成・提出をお願いします。

⑷ 組合せ型審査への変更を希望する場合は、「認証内容変更申請書」と併せて「組合せ型認証申請書」の提出が必要になります。
組合せ型審査の場合、マネジメントシステム間の「基準日」が異なる時には、基準日の変更等の調整をさせて頂く場合が有りますので、ご了解下さい。
又、統合の程度により統合審査から複合審査又は同時審査、複合審査から同時審査に変更させて頂く場合があります。

７．１．２　契約手続き

⑴ ＢＳＫは、顧客から認証内容変更申請書が提出された場合、現地審査の要否を連絡します。また、現地審査要の場合は、次の何れで行うかを連絡します。

・サーベイランス審査又は再認証審査とは独立した変更審査（書類審査又は現地審査）
・サーベイランス審査兼変更審査
・再認証審査兼変更審査

⑵ サーベイランス審査又は再認証審査とは独立した変更審査の場合、ＢＳＫは見積書(変更審査用)を顧客に送付します。サーベイランス審査兼変更審査で工数が増える場合には、別途見積りを送付します。再認証審査兼変更審査の場合、再認証審査の見積時に再認証審査兼変更審査として見積ります。

⑶ 現地審査にかかった費用は、審査終了後別途請求します。

７．１．３　変更審査の実施

⑴ 変更審査は、変更に係わる全項目を原則として実施します。

⑵ 再認証審査に準じて実施します。

７．１．４　臨時審査報告書の作成、不適合の修正及び是正処置

再認証審査に準じて実施します。

７．１．５　認証維持の可否の判定及び通知

再認証審査に準じて実施します。

７．１．６　審査費用の請求と納付

ＢＳＫは、判定委員会の判定結果のいかんに係わらず、審査に伴う経費等については、原則として顧客に請求します。請求に基づき審査料の納付をしていただきます。

７．２　臨時審査

７．２．１　臨時審査の通知

⑴　顧客（共同事業所を含む）の情報セキュリティ事故、不祥事公表、苦情等（以下「情報セキュリティ事故等」という。）の発生により、通常のサーベイランス又は再認証審査とは別に、認証登録した顧客（共同事業所を含む）の情報セキュリティマネジメントシステムが認証要求事項に引き続き適合していることを検証することが必要となった場合に、臨時審査を実施します。
特に、法令違反に係る不適合の疑い(情報漏洩等)の場合は、その内容が公表されたあと速やかに臨時審査を実施します。

⑵　ＢＳＫは、臨時審査の必要理由及び審査時期等を記して、事前に顧客に臨時審査を行うことを通知します。なお、ＢＳＫは、悪質と判断される内容の苦情の審査、内部告発に対応の審査の場合、予告なしに臨時審査を行うことがあります。
この場合、審査に要した審査工数（人･日）に基づく審査料を、別途申し受けます。

⑶　ＢＳＫは、審査日程及び審査担当審査要員を顧客に通知します。

⑷　ＢＳＫは、審査計画書を作成し顧客に通知します。

７．２．２　臨時審査の実施

臨時審査は、審査計画書(臨時審査)に基づいて、４．２．３．４「初回２の実施」に準じて実施します。

７．２．３　臨時審査報告書の作成、不適合の修正及び是正処置

⑴　ＢＳＫは、４．２．３．５「第２段階審査報告書の作成」に準じて臨時審査報告書を作成して顧客に配布します。

⑵　不適合がある場合、４．２．３．６「不適合の修正及び是正処置」に準じて、不適合の修正及び是正処置の手続きをとります。

７．２．４　認証維持の可否の判定及び通知

⑴　チーム・リーダーは審査報告書及びその他の資料をもって審査結果について、判定委員会に報告します。

⑵　判定委員会の判定結果により、認証の取消し又は一時停止になった場合はその結果を顧客に通知するとともに、既発行の認証書を返却していただきます。また、一時停止になった場合は、その理由及び一時停止の解除条件など、その後の計画プロセス等を顧客に通知するとともに必要な是正処置を要求します。

７．２．５　審査費用の請求と納付

ＢＳＫは、判定委員会の判定結果のいかんに係わらず、審査に伴う経費等については、原則として顧客に請求します。請求に基づき審査料の納付をしていただきます。

７．３　付随的審査

７．３．１　付随的審査の目的及び審査の種類

付随的審査は、初回審査、サーベイランス審査、再認証審査、変更審査又は臨時審査の中で重大不適合が発見された場合、又は審査が不十分となった場合に、認証の要求事項に適合していることを検証できなかった内容を改めて検証するために再度審査を必要とする審査であり、フォローアップ審査、追加審査及びやり直し審査があります。

７．３．２　付随的審査の実施

⑴　審査項目は、フォローアップ等に至った審査において確認できなかった要求事項とします。

⑵　ＢＳＫは、顧客と調整した内容を基に「審査計画書」を作成し、顧客に送付します。

⑶　初回審査、サーベイランス審査、再認証審査、変更審査又は臨時審査に準じて実施します。

７．３．３　付随的審査の審査報告書の作成

初回審査、サーベイランス審査、再認証審査、変更審査又は臨時審査に準じて実施します。

７．３．４　不適合の修正及び是正処置

初回審査、サーベイランス審査、再認証審査、変更審査又は臨時審査に準じて実施します。

７．３．５　認証維持の可否の判定及び通知

初回審査、サーベイランス審査、再認証審査、変更審査又は臨時審査の一環として実施します。

７．３．６　審査費用の請求と納付

費用の請求は、審査の実施が必要になった理由に基づきます。

- 審査の実施が必要になった理由が、顧客（共同事業所を含む）の責の場合、審査費用を請求します。請求に基づき審査料の納付をしていただきます。
- ＢＳＫの責の場合*）、費用を請求しません。

　＊）　ＢＳＫが認定機関から不適合の指摘を受けその修正として審査を実施する場合等が相当します。

第８章　認証の一時停止、取消し及び復帰等

８．１　認証の一時停止

⑴　ＢＳＫは、次のいずれかに該当する場合、認証書の有効期限内にあっても、認証を一時停止することがあります。この場合、認証は一時無効となります。

ア　顧客（共同事業所を含む）の認証されたマネジメントシステムが、その有効性に関する要求事項を含む認証要求事項に対し、常態化した不適合 (注ア-1) 、又は深刻な不適合 (注ア-2) があった場合。

(注ア-1) 常態化した不適合の事例

1)　規制当局等より不適合が指摘され、当該不適合に関わる修正・是正処置が計画され承認され実施されているにも関わらず、認証範囲において同種のあるいは類似の不適合が繰り返し発生している状態。

2)　認証組織が不適合状態にあることを認識しながらその状態を継続していたこと（時期）がある場合も含む。

(注ア-2) 深刻な不適合の事例

1)　不適合の内容に組織的な悪質性が認められ経営者や部門長の経営層が直接関与している場合

2) 認証されたマネジメントシステムに於いて、社会の信頼及び信用に反するような法令違反に関する事象（情報漏洩等に関する行政処分、業務改善命令等）が発生した場合

イ 顧客（共同事業所を含む）が、マネジメントシステムとして要求された頻度でのサーベイランス又は再認証審査の実施を受け入れない場合。

ウ 顧客（共同事業所を含む）が下記に示す認証（の地位）を不適切に引用、又は認証文書やマークを不適切な使用（不正使用、誤用を含む）、又は誤解を招く使用を行った場合。

a) 顧客が認証の地位をインターネット、パンフレット 又は広告、若しくは他の文書等のコミュニケーション媒体に当センターの要求事項に適合しない不適切な引用を行った場合。

b) 顧客が認証に関連して誤解を招く表明を行ったり、他の組織に認証に関連した表明を許したりした場合。

ｃ）顧客が認証文書又はその一部に誤解を招く誤った方法で使用した場合。また顧客が他の組織がその認証文書を使用することを許した場合。

d) 認証、及びマーク（認定シンボル等）が製品（サービスを含む）又はプロセスを認証機関が認証したと受け取られる方法で、使用された場合。

e) 認証が認証範囲外の活動にも及んで使用されている場合。

f) 顧客が認証機関及び／又は認証システムの評価を損ない，又は社会的信用を失墜させる方法で認証を用いた場合。

エ 料金の支払いが定められた支払い期限を越えて滞った等、ＢＳＫとの契約の不履行があった場合。

オ 顧客が認証を維持できないため、自発的に一時停止を要請した場合。

カ 認証審査において認証の判定に重大な影響を与えるような故意の虚偽説明があったと判断された場合。

注：故意の虚偽説明とは：

認証機関が実施する認証審査の過程での、組織による審査のための文書と記録類の提供、審査員の質問に対する回答及び自主的な説明において、認証の判定に重大な影響を与える事実について、真実と異なる情報を、それと知りながら殊更に提供、回答し若しくは説明し又は真実の情報が存在するにもかかわらず殊更にそれを提供、回答若しくは説明しないことをいう。

キ その他上記各項に準じ、当センターが認証の一時停止が相当と判断した場合。

⑵ 認証の一時停止の手続きは次の通りです。

ア ＢＳＫは、上記ア～キに該当する案件が発生した場合、認証の一時停止を判定委員会に上程します。

イ 判定委員会において認証の一時停止が確定された場合、一時停止の旨を文書で通知します。文書には、一時停止の根拠並びに一時停止の解除条件及び方法を明示します。

ウ 顧客は認証が一時停止となった場合、認証の引用を含む広告宣伝（ウェブサイト等を含む。）はできません。

エ ＢＳＫは、ホームページに顧客の認証が一時停止状態であることを公表します。

⑶ 一時停止の解除条件は、上記ア～エの一時停止事由が解消され再発防止が十分講じられることです。

⑷ 一時停止の解除の手続きは次の通りです。

ア 一時停止事由が解消され再発防止が十分講じられましたら、一時停止事由が解消され再発防止が十分講じられたことを示した是正処置報告書等を添付し、一時停止の解除申請書を提出してください。

イ ＢＳＫは、是正処置報告書等の書類を確認した結果、一時停止の要因が確実に除去されていると

判断できる場合には、一時停止の解除を判定委員会に上程します。

また、是正処置報告書等の書類を確認した結果、及び常態化した不適合や深刻な不適合の未解決等の一時停止の要因の内容によって、フォローアップが必要であると判断される場合には、臨時審査を計画し、実施します。臨時審査の結果、一時停止の要因が確実に除去されていると判断できる場合には、一時停止の解除を判定委員会に上程します。

ウ　認証の一時停止は、判定委員会の判定によって解除が確定した後、解除されます。解除が確定された場合は、一時停止の解除の旨を文書で通知するとともに、認証書を再発行します。

８．２　認証の取消し

⑴　ＢＳＫは、次のいずれかに該当する場合は、認証を取消すことができます。

ア　前記８．１項において、一時停止の原因となった問題を合意された期限内(最大　６ヶ月以内)に解決できない場合。

イ　顧客（共同事業所を含む）による意図的、又は重大な過失によって、マネジメントシステム認証の要求事項を遵守しなかった場合。

ウ　顧客（共同事業所を含む）による意図的、又は重大な過失によって、当センターとの契約の不履行があった場合。

エ　顧客（共同事業所を含む）において、意図的、又は重大な過失による法律違反等の不適切な活動があり、マネジメントシステム認証制度に対する信用を著しく失墜させる事実があった場合。

オ　顧客から当センターによる認証登録を取り止める旨の申し出があった場合

カ　認証審査において認証の判定に重大な影響を与えるような広範囲にわたる故意の虚偽説明があったと判断された場合。

（故意の虚偽説明は前述8.1(1)カに示す。）

キ　被認証組織において、破産法に基づく破産手続き開始の申し立てを行った場合、会社法による会社解散・私的会社整理が開始された場合、又は特別清算手続きが開始された場合。

ク　その他上記各項に準じ、当センターが認証の取り消しが相当と判断した場合。

⑵　認証の取消しが決定した場合、ＢＳＫは直ちに認証書及び認定シンボル等原版を回収し、登録簿から登録を削除します。

⑶　顧客（共同事業所を含む）は認証が取消された場合、認証が引用されている全ての広告物の使用を中止していただきます。

⑷　顧客は、認証取消し後、改めて認証を希望する場合は、新規認証申請書を再提出し新規の初回審査を受けていただきます。但し、制限がある場合、初回審査を受けられない場合があります。

初回審査を受けられない場合：ー

例；故意の虚偽説明によって認証を取消された場合

ア 認証取り消し後1年間又は新たに認証されたことが確認されるまでの間のいずれか短い期間公表します。

イ 認証取消し事由を解消し再発防止が十分行われるまで、認証申請を受理しません。　申請を受理しない期間は、通常1年間必要としますが、実際に必要とする期間は個別事象ごとに異なるため具体的な期間設定はＢＳＫが判断を行います。

８．３　認証書の返却

⑴　認証書の改定又は再認証により新認証書を受領した場合は、旧認証書をＢＳＫへ返却していただきます。

⑵　認証の一時停止又は取消しを受けた場合は、認証を引用している全ての宣伝・広告を中止し、ＢＳＫへ認証書を返却していただきます。

８．４　認証の復帰

⑴　認証の復帰とは、認証の有効期限が過ぎることにより認証が失効した後、失効状態から認証状態に戻すことです。認証の復帰は一時停止の解除とは異なります。

⑵　認証の復帰に関する方針は次の通りです。

認証が失効した後、⑶項の認証の復帰の条件を満たせば、認証を復帰することができます。BSKは、認証の復帰について顧客に通知し、希望について打診し、希望する場合は認証の復帰の申請を要請します。希望しない場合は、認証の取消しのプロセスに入ります。

⑶　認証の有効期限が過ぎることにより認証が失効した後、次のいずれかの条件に該当する場合、認証を復帰することができます。

ア　未完了だった再認証活動が有効期限から６か月以内に完了した場合。

この条件のケースとして、次の内容が考えられます。

・再認証審査を有効期限前に実施したが、不適合の修正及び是正処置が完了していないため、不適合の修正及び是正処置を完了させ、有効期限から６か月以内に判定委員会を行う。

・大震災等の非常事態又は特殊の状況を含むなんらかの理由で再認証審査の実施を有効期限後に実施したが、有効期限から６か月以内に判定委員会を行う。

イ　未完了だった再認証活動が有効期限から６か月以内に完了しない場合、第２段階を実施し再認証活動が完了した場合。

再認証審査を有効期限前に実施したか、有効期限後に実施したかに関わらず、有効期限から６か月以内に判定委員会を行えなかった場合が相当します。この場合、BSKは、初回審査第２段階の審査工数で、１段階審査方式の再認証審査を行い、判定委員会を行います。

⑷　認証の復帰の処理プロセスは次の通りです。

ア　復帰の申請の実施

BSKは、認証の復帰について顧客に通知し、希望について打診し、希望する場合は認証の復帰の申請を要請します。復帰を希望する場合、有効期限内に認証できなかった理由及び⑶のア、イのどの条件で復帰するのかを記載して、復帰の申請をしていただきます。書式は自由です。

イ　認証の復帰の申請の受領と復帰のための活動

BSKは、認証の復帰の申請を受領した場合、入手資料を基に調査検討を行い、認証の復帰の条件に照らし、認証の復帰に必要な調査活動や現地審査等を実施します。

ウ　ホームページへの掲載

BSKは、認証の有効期限がきれた場合、認証の失効の状態とし、ホームページに認証の失効の状態である旨を記述し、公表を行います。

エ　判定委員会での決定

BSKは、認証の復帰の条件を満たした場合、判定委員会に上程し、復帰の可否を判定します。

オ　認証書の発行

BSKは、認証の復帰の決定を受けて、認証書を発行します。再認証日は，再認証決定日（判定委員会実施日）とし、有効期限は前の認証の周期に基づき、前の認証の有効

期限の３年後の日付とします。また、認証書には復帰による再認証であることを記載します。

カ　新認証書の送付と旧認証書の返却

BSKは、顧客に対して認証の復帰の旨を文書で通知します。BSKは新認証書を送付しますので、旧認証書を返却してください。

キ　ホームページへの掲載

BSKは、ホームページに当該被認証組織の認証が復帰になった旨を記述し、公表を行います。

第９章　審査に対する権利及び義務

９．１　受審組織の権利及び義務

９．１．１　受審組織の権利

受審組織には、「異議及び苦情の申し立て」の権利があります。
詳細は第１０章を参照下さい。

９．１．２　認証の引用及びマークの使用に関する制約事項の順守義務

インターネット、パンフレット、広告、その他の文書などのコミュニケーション媒体に認証の地位を引用する場合、及びＢＳＫマーク、ＩＳＭＳ－ＡＣ認定シンボルを使用する場合は次の事項を順守して頂きます。詳細は「認証の引用及びマークの使用規定」（Ｐ０８０４０１）を参照下さい。

ア　認証に関連して誤解を招く表明を、自ら行わず、他者による表明も行われないよう注意して下さい。

イ　認証文書又はその一部を、誤解を招く方法で自ら使用せず、他者による使用もされないよう注意して下さい。

ウ　認証が取消しになった場合、認証の引用を含む全ての広告物の使用を中止して下さい。

エ　認証範囲が縮小された場合，全ての広告物を修正して下さい。

オ　製品（サービスを含む）又はプロセスをＢＳＫが認証したと受け取られる方法で，マネジメントシステム認証を引用しないで下さい。

カ　認証範囲外の活動及び事業所にも認証が及んでいると受け取られないようにして下さい。

キ　ＢＳＫ及び／又は認証システムの評価を損ない又は社会的信用を失墜させる方法でその認証を用いないで下さい。

９．１．３　審査に対する協力義務

⑴　ＢＳＫの審査を受審するにあたり、審査チームリーダーと受審組織との間でほかに合意がある場合を除き案内役が同行しなければなりません。審査を円滑に進めるために、審査チームに案内役を割り当てていただきます。適切な場合、審査される者が案内役として行動してもよいです。
案内役は次の責任を含みます。

ア　面談のための連絡先及びタイミングを確認する。

イ　事業所又は組織の特定の部署への訪問を手配する。

ウ　事業所の安全に関する規則及びセキュリティ手順について、審査チームメンバーへの周知及び順守を確実にする。

エ　必要に応じて審査に立ち会う。

オ　審査員から要請があった場合に、不明な点を明らかにし又は情報を提供する。

⑵　顧客（共同事業所を含む）はＢＳＫの審査員に対し、初回審査、サーベイランス審査、再認証審査、変更審査及び特別審査並びに苦情理解を目的としたすべてのプロセス、領域（設備を含む。）、記録及び要員へのアクセス、文書の調査についての提示、立ち入り及び閲覧を許可していただきます。

⑶　顧客は，現地での認証審査前に少なくとも次の情報を提供しなければならない。

a) ISMS及びその対象となる活動に関わる一般情報

b) JIS Q 27001で要求されるISMS文書の写し及び要求のある場合には関連文書一式

⑷　ＩＳＭＳ－ＡＣの認定に関わる認証書を希望する顧客又は既に認証を有する顧客は、ＩＳＭＳ－ＡＣの認定審査員（訓練中を含む。）がＢＳＫを審査する目的でＢＳＫ審査チームに同行して顧客（共同事業所を含む）に立ち入る場合があります。顧客（共同事業所を含む）は、このＩＳＭＳ－ＡＣ認定審査員の立ち入りを受入れる義務があります。

この場合、ＢＳＫは事前に顧客に対し書面で申入れを行います。

⑸　前⑷の申し入れが拒絶された場合は、ＢＳＫはその事実をＩＳＭＳ－ＡＣに通知します。

この場合、ＩＳＭＳ－ＡＣが正当と認める理由がある場合を除き、組織審査立会の受け入れを拒絶する組織に認証書を発行しないものとします。

⑹　顧客が、ＩＳＭＳ－ＡＣの組織審査立会を回避するために審査を依頼する機関を変更又は他の機関に認証を移転した場合、ＩＳＭＳ－ＡＣは、当該組織名称を、ＩＳＭＳ－ＡＣに認定された機関及びＩＡＦメンバー認定機関に通知します。ＩＳＭＳ－ＡＣに認定された機関は、当該組織にＩＳＭＳ－ＡＣ認定シンボル付き認証書を発行しないものとします。ＩＡＦメンバー認定機関は、自機関が認定した機関に対し、このような組織に認定シンボル付き認証書を発行しないように求めることがあります。

９．１．４　事故等発生時の通知義務

⑴　顧客は、７．２の臨時審査が必要と判断されるＩＳＭＳに関連する情報セキュリティ事故等が発生した時は、速やかにＢＳＫに対して通知していただきます。

⑵　前⑴の情報セキュリティ事故等には、マスコミ報道、規制当局の公表、関係者からの通報・告発・苦情等に関する意図的な法令違反を含みます。

⑶　ＢＳＫは、事実確認を行うため、必要により顧客を訪問することがあります。

９．１．５　苦情の記録の閲覧

顧客（共同事業所を含む）は、外部から受けたすべての苦情について、適切な是正処置による対策を確立し、その結果及び効果を記録し管理しなければなりません。ＢＳＫの審査員が審査時に必要に応じてそれらの記録を利用できるよう準備をお願いします。

９．１．６　法令及び規制の順守

法令及び規制を順守し、その順守状況を評価するのは顧客の責任です。

９．２　ＢＳＫの権利及び義務

９．２．１　ＢＳＫの権利

認証機関であるＢＳＫは、以下の権利を有します。

⑴　ＢＳＫは、顧客（共同事業所を含む）の認証の授与、一時停止又は取消しについての情報を、ホーム

ページで公表します。

⑵ ＢＳＫは、関係者からの要請があった場合、顧客(被認証組織)（共同事業所を含む）の認証の有効性を確認する手段を提供します。

⑶ 認証書とマークの所有権

⑷ ＢＳＫは、顧客から提供された情報及び文書をＢＳＫの認証業務に係わる要員が使用する権利を有します。必要に応じてデータ／文書の複製を行う権利を有します。なお、これらの情報／文書の取扱は、ＢＳＫと顧客との間で合意する機密保持の取決めに従います。

⑸ ＢＳＫは、審査員又は技術専門家の指名をする権利を有します。顧客は、これに異議を唱えることができ、その異議が正当であるとＢＳＫが認めた場合には、ＢＳＫはチームを再編成します。

⑹ 審査報告書の所有権はＢＳＫにあります。

⑺ 短期予告審査(臨時審査及び付随的審査)を実施する権利、及び顧客（共同事業所を含む）が審査を拒否した場合には認証の一時停止や取り消しを行う権利。

⑻ 記録を維持する権利

ＢＳＫは、申請を提出したすべての組織、及び審査された組織、認証された組織、又は認証の一時停止若しくは取消しを受けた組織を含む、すべての顧客に対する審査及び他の認証活動についての記録を維持します。

⑼ ＢＳＫは、必要に応じて、情報通信技術（ICT）を利用します。

９．２．２　ＢＳＫの義務

認証機関であるＢＳＫは、以下の義務を有します。

⑴ ＢＳＫは、顧客への認証活動の提供に関し、法的に拘束力のある合意書として、認証合意書を結びます。さらに、顧客が複数の事業所をもつ場合、ＢＳＫは法的な拘束力のある合意が、ＢＳＫと認証範囲に含まれるすべての事業所（共同事業所を含む）との間で結ばれることを確実にします。

⑵ ＢＳＫは、審査プロセス及び認証の授与、維持、拡大、更新、縮小、一時停止又は取消しに関する認証プロセスを記述した情報、並びに認証にかかわる活動、マネジメントシステムの種類及びＢＳＫが活動する地域の情報を維持し、公にアクセス可能にするか、又は要請に応じて提供します。

⑶ ＢＳＫは、公開の対象にしようとしている情報を、事前に顧客に知らせます。他のすべての情報は、顧客によって公開されている情報を除いて、機密情報とみなします。

⑷ 顧客又は個人に関する情報は、この認証ガイドにおける記載事項を除き、関係する顧客又は個人の書面による同意なく第三者へ開示しません。ＢＳＫが法律によって機密情報を第三者へ提供することを要求された場合、関係する顧客又は個人は、法律によって規制されない限り、当該情報の提供について事前に通知します。

⑸ ＢＳＫは、顧客以外（例えば、苦情申立者、規制当局）から入手した顧客に関する情報を機密として取り扱います。

（注、顧客に対しても開示しません。）

⑹ ＢＳＫの委員会メンバー、契約者、外部機関の要員又はＢＳＫを代行して活動する個人を含む要員は、ＢＳＫの活動の実施の過程で得られた又は生成された情報について機密を保持します。

⑺ ＢＳＫは、認定機関の認定審査（サーベイランス審査、更新審査等）における事務所審査を受審する場合、認定審査に関わる機密情報の提示又は閲覧を認定機関に対し許可します。

但し、認定審査以外の目的で、他の機関（例えば、認定機関、同等性評価スキームの合意グループ）が機密情報の利用を必要とする場合、ＢＳＫは事前に顧客に対し、文書で通知します。

⑻ ＢＳＫは、認証に関する要求事項が変更になった場合、いかなる変更についても、顧客に対し適切に通知をします。その場合、ＢＳＫは、顧客が新しい要求事項に適合していることを検証します。

⑼ ＢＳＫは、ＢＳＫ保有のICTを利用する場合、審査前に、その利用について顧客と合意するとともに、ＢＳＫ規定に従ってICTに関する情報セキュリティ及びデータ保護の対策を実施します。
なお、顧客が自ら保有するICTの利用を申請頂いた場合は、必要に応じて、顧客の規定に従い、そのICTに関する情報セキュリティ及びデータ保護の対策を実施頂きます。
審査の確認結果を記録するためにのみ利用するＢＳＫ保有の機材（ＰＣ等）は前述のICTに含めませんが、ＢＳＫ規定に従って、情報セキュリティ及びデータ保護の対策を実施するとともに、審査当日はその持ち込み、利用条件等について顧客の指示に従って対応します。

⑽ 異議申し立てに関連する義務
ＢＳＫは、異議申立ての処理の手順についての情報及び更新した情報を顧客に提供します。異議申立ての提出及び調査並びに異議申立てに関する決定が、申立者に対する差別的行動につながらないようにします。ＢＳＫは、申立者に対し異議申立ての受領を通知し、進捗状況報告及び異議申立ての結果を提供します。ＢＳＫは、異議申立て処理プロセスの終了を申立者に対し正式に通知します。

⑾ 苦情に関連する義務
ＢＳＫは、苦情の処理の手順についての情報を顧客に提供します。苦情が顧客に関連するものである場合、苦情の調査では認証されたマネジメントシステムの有効性を考慮します。顧客に対するいかなる苦情も、ＢＳＫが当該の顧客に対して、処理を進めるために、適切な時期に照会します。ＢＳＫは、苦情の内容及びその決着内容を公表するかどうか、また、公表する場合にはどの範囲とするかについて顧客及び苦情申立者と調整します。

第１０章　異議及び苦情の申立て

１０．１　異議申立て

⑴ 顧客が希望する認証に関して、ＢＳＫが行った不利な決定について、次に該当する場合、異議等申立てができます。
ア　申請受理の拒否
イ　審査段階に進むことの拒否
ウ　是正処置の要求
エ　認証範囲（共同事業所を含む）の変更
オ　認証の拒否、一時停止又は取消しに関する決定
カ　その他認証取得を阻む行為

⑵ 異議申立てにあたっては、申立て案件が発生してから３０営業日以内に書面でＢＳＫ宛にご提出下さい。ＢＳＫの規定により公平かつ客観的に処理します。
（営業日とは、ＢＳＫの出勤日をいいます。）

⑶ 異議申立ての処理については、受領、進捗状況及び異議申立ての結果の情報を提供します。また、異議申立ての処理が終了した場合、処理終了を正式に申立て者に通知します。

１０．２　苦情申立て

⑴ 苦情とは、ＢＳＫの認証活動の利用者が、ＢＳＫの活動又はＢＳＫに認証された顧客（共同事業所

を含む）に関係ある事項に対する不満足等に対するＢＳＫの決定に同意できないことをＢＳＫに対して原則として文書で申立てをすることをいいます。

⑵ 苦情の申立ては、申立て案件が発生してから３０営業日以内に書面でＢＳＫ宛に提出され、ＢＳＫの規定により公平かつ客観的に処理されます。

⑶ 苦情申立ての処理にあたり、顧客（共同事業所を含む）に関係する事項の場合、必要に応じて顧客から情報を提供していただく場合があります。

１０．３ 規定の公開

「異議申立処理規定」及び「苦情処理規定」については、ホームページで公開します。

第１１章 その他

１１．１ 認証要求事項の変更

⑴ ＢＳＫは、認証の要求事項に影響を及ぼすような本ガイドの重大な変更を行う場合には十分な期間をおいて、その内容を文書で予告いたします。

⑵ 顧客（共同事業所を含む）は、公表の後その変更が顧客の情報セキュリティマネジメントシステムに影響を及ぼす場合、情報セキュリティマネジメントシステム文書の必要な改訂を行い、ＢＳＫが公表時に指定した期日内に「認証内容変更申請書」を提出して下さい。

１１．２ 手順に関する情報

申請された認証範囲が特定のプログラムに関係する場合(例えば、立入申請が必要な審査を行う場合、審査の見学がある場合)は、顧客に対して必要な説明を行います。また、要求があれば、申請に関する追加情報を提供します。

１１．３ 審査後のアンケート

現地審査終了後に、別途、審査に関するアンケート調査を実施しますので、ご協力をお願いします。

尚、ご回答に際しては、経営者又は管理責任者の方によるアンケート回答の内容についてご確認をお願いします。

お知らせ

当センターが発行するマネジメントシステム認証ガイドについては、当センターのホームページ（http://www.bsk-z.or.jp）に掲載しています。