



# 国際システム審査株式会社

## ISMS 認証サービスご利用のご案内

国際システム審査株式会社

〒450-0003 愛知県名古屋市中村区名駅南一丁目 16 番 30 号

東海ビルディング 7 階

TEL : 052-582-3666

FAX : 052-582-3668

## 目 次

1. はじめに	3
2. 認証活動の全体像	4
3. 認証審査について	5
3.1 認証審査実施にあたってのスタンス	5
3.2 認証審査の種類と目的	6
3.3 アドオン認証 -ISMS クラウドセキュリティ認証-	8
3.3.1 ISMS クラウドセキュリティ認証とは	8
3.3.2 ISMS クラウドセキュリティ認証審査の実施について	9
4 お客様にご準備いただきたい事項と審査の詳細	10
4.1 各審査共通のご準備をお願いする事項	10
4.2 初回認証審査 目的と方法	12
4.2.1 第1段階審査について	12
4.2.2 第2段階審査について	13
4.3 サーベイランス審査 目的と方法	14
4.4 再認証審査 目的と方法	15
5. 各認証審査での指摘の分類と対応の方法	16
5.1 各認証審査での指摘の分類	16
5.2 各認証審査での指摘（不適合）への対応方法	18
6. 認証の表明／認定シンボル・認証マークの利用方法	19
6.1 認証の表明、認定シンボル・認証マーク 用語	19
6.2 認証表明／認定シンボル・認証マークの表示形式	20
6.3 認証の表明、その利用範囲・制限細則	22
6.4 不適切な認証表明／認定シンボル・認証マーク等の使用例	26
6.5 [IAF CERT SEARCH]における登録組織情報の公開に関し	27

## 1. はじめに

このたびは国際システム審査株式会社（以下略称 ISA）の認証サービスをご利用/ご検討いただき誠にありがとうございます。

本案内書には ISA の ISMS 認証サービスをご利用いただくにあたって、お客様にご理解いただきたい事項をまとめております。

マネジメントシステム認証活動は、お客様と認証機関である ISA による相互の協力関係なしには成り立ちません。是非、本案内書をご確認いただき、認証活動の全体像、個々のプロセスについてご理解をいただくとともに、積極的に ISA との協同作業を進めていただければと存じます。

本書をご覧いただく中で、あるいは認証サービスをご利用いただく中で、生じた疑問については、ご遠慮なくご質問を賜ればと存じます。

ご連絡・ご質問受付：

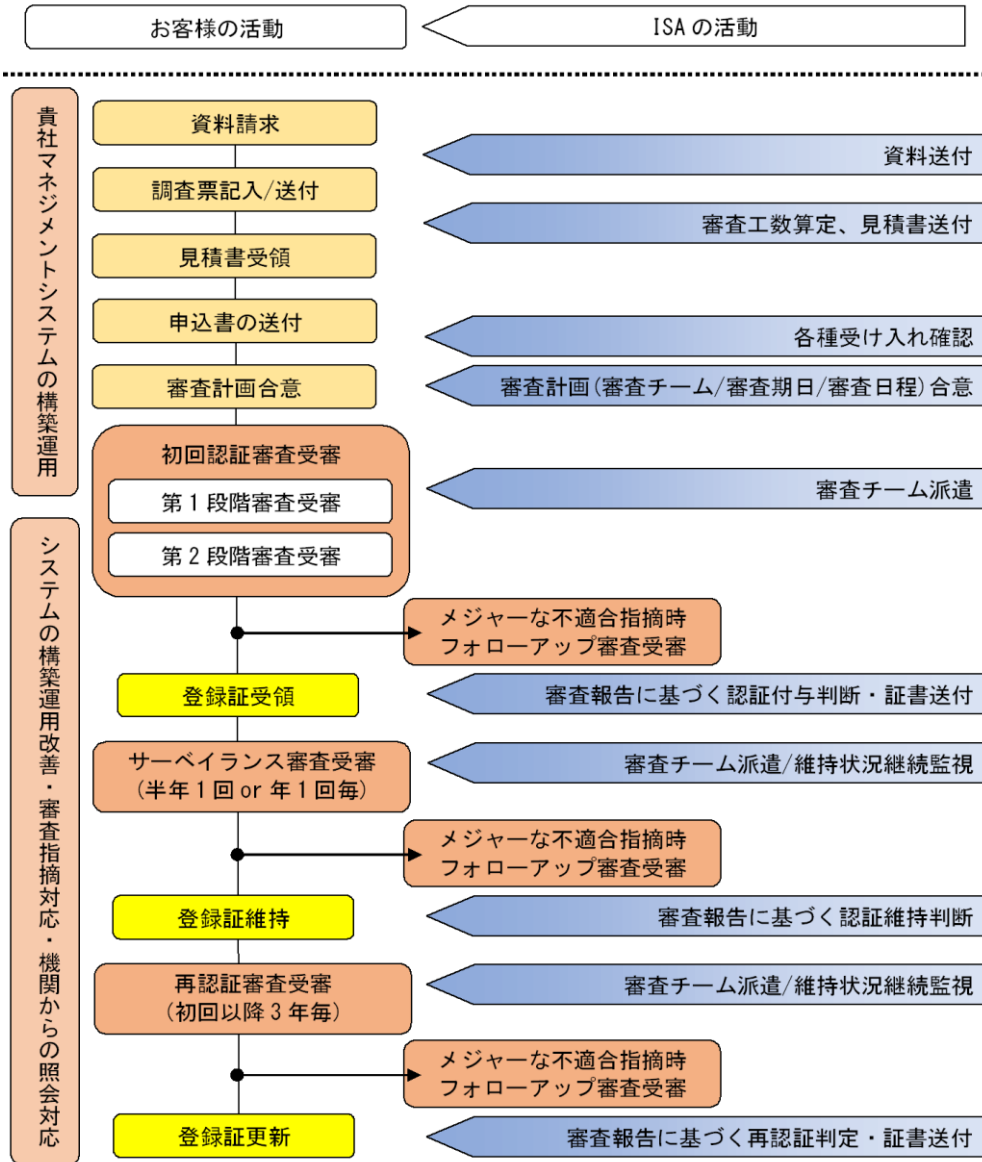
国際システム審査株式会社（略称 ISA）

ISMS 担当

Tel 052-582-3666 Fax 052-582-3668

## 2. 認証活動の全体像

マネジメントシステム認証は、お客様が自らの責任で行う自組織のマネジメントシステム構築・運用・改善活動と、私共 ISA が行う認証審査・登録事務活動の相互連携で成り立つ仕組みです。



私共 ISA は、認証活動の結果、お客様が構築し運用するマネジメントシステムが、認証基準 (ISMS においては [ISO/IEC 27001]) の要求事項に準拠している状況を確認できた場合に、お客様に対して「認証」の付与もしくは維持の決定をします。

また認証を付与/維持されているお客様におかれましては、本書の『6 の認証の表明/認定シンボル・認証マークの利用方法』にある基準に従って、この認証 (マークやロゴあるいは証書や審査報告書などの事) を事業の用に供することができます。

### 3. 認証審査について

ISA の行う認証活動には、お客様のマネジメントシステムの運用改善の状況を継続的に評価する次の活動が含まれます。

- 初回認証審査・サーベイランス審査・再認証審査など ISA から審査員を派遣して、お客様の事業所内で行う「審査」活動
- 審査チームからの報告を踏まえて、認証の付与・維持・再認証あるいは取消し・一時停止等を決定する判定活動
- お客様からのマネジメントシステムの変更申請受付と対応
- お客様に対するマークの使用状況の照会確認
- ISA に寄せられたお客様との間に利害関係を持つ様々な組織・個人からの意見/苦情、又はお客様から当社が受けた社会的責任が問題となる規模の事件・事故発生報告に基づく調査

この中でも多くのお客様にとって一番気がかりなのは、ISA の審査員が直接お客様と面談する「審査」活動かと思います。ここでは認証審査のスタンス、認証審査各段階の目的と方法、そして各段階でお客様にご依頼するご準備事項（どの段階でも共通の準備事項と各段階で異なる準備事項があります）についてお知らせします。

#### 3.1 認証審査実施にあたってのスタンス

認証審査活動は、原則として、お客様の事務所に ISA から指示を受けた審査員が訪問して行います。

審査員は、お客様から提出されたマネジメントシステム文書や記録の閲覧、お客様組織内の役職員の皆さんへのインタビュー、作業や事務現場での活動の観察、手順文書や活動記録、情報処理システムの運用・管理状況等の確認を通じて、規格への合致（適合性）とお客様が確立した方針や目的の達成に向けた活動の進展状況を評価していきます。

### 3.2 認証審査の種類と目的

認証審査には、段階あるいは時期ごとに異なる名称と目的があります。

名称	実施する段階/時期	目的
初回認証審査	第1段階審査	<ul style="list-style-type: none"> <li>● 御社の情報セキュリティ方針・情報セキュリティ目的・マネジメント文書のレビュー及び御社の事業と適用範囲の確認を通して、御社の事業及び御社の ISMS を審査チームが理解する事</li> <li>● 御社の ISMS 及びその準備状況を確認する事</li> <li>● 第2段階審査の焦点を定める事</li> </ul>
	第2段階審査	<ul style="list-style-type: none"> <li>● 情報セキュリティ目的の設定及びその達成に向けた活動に対するトップマネジメントのコミットメントを確認する事</li> <li>● 情報セキュリティに関連するリスクアセスメントの手順及び結果から、そのアセスメントプロセスが、一貫性及び妥当性があり、かつ比較可能な結果を出すものであるかを確認する事</li> <li>● 御社の情報セキュリティ方針及び情報セキュリティ目的を実現する為の活動が行われており、自ら定めた手順を順守しているかを確認する事</li> <li>● ISMS 規格のすべての要求事項に適合していることを確認する事</li> </ul>
サーベイランス審査 (維持審査)	<p>初回認証審査完了後、再認証審査までの期間、1年毎（ご要望がある場合半年毎）に受けていただきます。</p> <p>有効期限月の前後2か月（有効期限月を含む5か月間）の間に実施いただきますが、初回認証審査後初の審査のみ認証登録日を起点として1年以内に受けていただく必要があります。</p>	<ul style="list-style-type: none"> <li>● 認証された ISMS が引き続き実施されている事を検証する事</li> <li>● 組織運営の変更を踏まえて、ISMS への変更の影響を把握し、かつ認証要求事項の継続的な適合状況を確認する事</li> </ul>
再認証審査	<p>再認証審査は、登録証の有効期限月の3ヶ月前から、有効期限の1ヶ月前までに実施します。</p> <p><b>注）</b> 不適合が出た場合は是正処置の実施に必要な期間を考慮し、通常は有効期限の3ヶ月～2ヶ月前の間に計画させていただきます。</p>	<ul style="list-style-type: none"> <li>● 情報セキュリティ方針、情報セキュリティ目的、手順に従って構築された ISMS が実施されていることを確認する事</li> <li>● ISMS 規格のすべての要求事項に適合していることを確認する事</li> <li>● 御社の ISMS が認証サイクルを通して有効に機能していたかを確認する事</li> <li>● 認証サイクル(3年間)の ISMS の運用実績、審査結果を踏まえ、続く有効期限まで、御社へ認証を継続して付与しうるかを評価する事</li> </ul>

【以下特別な審査】

名称	実施する段階／時期	目的
変更審査 (変更/拡大/縮小)	既に授与した認証範囲を変更する為、定期審査と同時に/又は別の機会に臨時に計画し実施します。  <small>注) 変化の程度に応じ追加工数/費用が発生する場合があります。</small>	<ul style="list-style-type: none"> <li>●御社の ISMS が、変更された適用範囲を含めて確立し運用されていることを評価する事</li> </ul> <p>変更の内容に応じ以下の種別があります。</p> <ul style="list-style-type: none"> <li>・変更：認証対象事業の限定的な変化、拠点の移転</li> <li>・拡大：認証対象事業や拠点の追加拡大</li> <li>・縮小：認証対象事業の中断/中止や拠点の閉鎖、事業や拠点を認証対象から外す</li> <li>・移行：認証対象規格が改定された、組織の適用規格を改定版に移行させる</li> </ul>
フォローアップ審査	初回認証審査の第二段階、変更・拡大・縮小審査、サーベイランス審査、再認証審査でメジャー（重大）な不適合事項が報告された場合に計画し、実施します。  <small>注) 追加の審査となりますので通常の審査とは別料金を徴収致します。</small>	<ul style="list-style-type: none"> <li>●メジャー（重大）な不適合に対して実施された是正処置が適切であり、且つ有効なものであるかを確認し、認証を付与/維持/更新する事に問題がないかを評価する事</li> </ul>
短期予告審査	外部からの苦情や受審組織の社会的責任が問題となる事件・事故の発生に対する調査のため、又は規格の要求事項を継続的に満たすマネジメントシステムの能力に影響を与える可能性のある変更に対して、又は一時停止とした組織のフォローアップとして短期の予告で実施する審査です。  <small>注) 追加の審査となりますので通常の審査とは別料金を徴収致します。</small>	<ul style="list-style-type: none"> <li>●組織の利害関係者や報道機関、組織からの直接の報告等から検知した組織に対する苦情、組織の関わる事件・事故の発生に対し、その要因及び発生後の対応について、マネジメントシステムの運用に問題が無かったかについて評価する事</li> </ul>

### 3.3 アドオン認証 -ISMS クラウドセキュリティ認証-

ISA の提供する ISMS 認証サービスにおいては、お客様のご要望に応じ、従来からの ISMS 認証に追加する形で、クラウドセキュリティに関する国際規格、ISO/IEC27017「ISO/IEC27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」を取り込んだ ISMS クラウドセキュリティ認証審査(以下、クラウド認証)を提供させていただく事が可能です。

#### 3.3.1 ISMS クラウドセキュリティ認証とは

クラウド認証の対象は、クラウドサービスを提供される組織又は利用される組織であり、クラウドサービスの種類(SaaS/PaaS/IaaS 等)は問いません。

クラウドサービス提供者、クラウドサービス利用者それぞれの立場に対して ISO/IEC27017 には管理策のガイドラインがあり、本ガイドラインに沿って ISMS(クラウド認証含む)の認定機関『一般社団法人情報マネジメントシステム認定センター(略称: ISMS-AC)』の定めた認証基準(JIP-ISMS517)に則って審査するのがクラウド認証です。

クラウド認証は、クラウドサービス利用者/クラウドサービス提供者のどちらか一方の立場として、又は提供者と利用者双方の立場として認証審査を受けていただく事ができます。ただし、他社の提供するクラウドサービス上に自社サービスを構築/提供する場合は、利用者 と提供者双方の立場で認証を取得する事が求められます。

またクラウド認証は、ISMS 認証をベースとしたアドオン認証である為、ISMS 認証を取得される事無く単独で取得する事はできません。

既に ISMS 認証を取得されている組織が追加する形、もしくは ISMS 認証とクラウド認証を同時に新規認証される形で審査を受けていただく必要があります。

(クラウド認証の範囲は、ISMS 認証範囲に含まれている事は必須ですが、適用範囲の決定が適切なものであると評価されれば、ISMS 認証範囲の一部でクラウド認証を取得していただく事も可能です。)

クラウド認証の取得は、あくまでお客様が任意で決定いただくものであり、ISMS を取得している組織/ISMS 取得を希望されている組織が、クラウドサービスを利用又は提供されているからといって、必ず取得しなければならないものではありません。

各組織の事業上の必要等からご判断いただき、ご相談いただければと存じます。

### 3.3.2 ISMS クラウドセキュリティ認証審査の実施について

クラウド認証審査の実施形態について以下ご説明させていただきます。

クラウド認証は、ISMS 認証のアドオンである為、基本的に ISMS 認証審査と同時に実施する事となります。

審査の種類等は本書「3.2 認証審査の種類と目的」にある ISMS 認証と同様です。

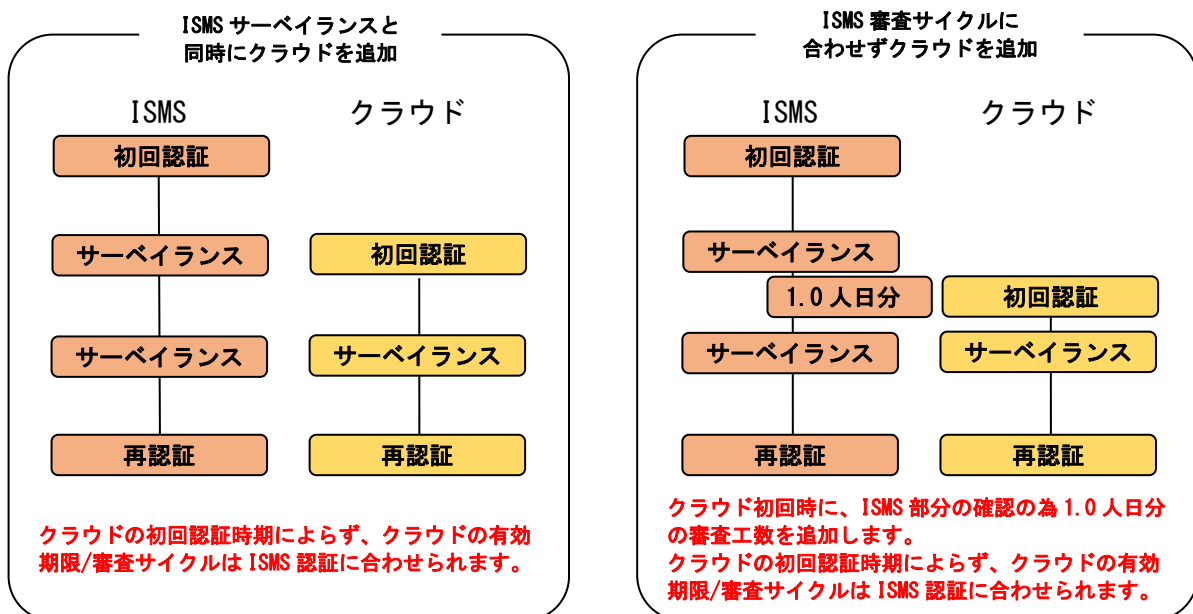
ISMS 認証を既に取得されている組織が初めてクラウド認証を受審される際の審査は、ISMS 認証の審査サイクルの状況によらず、クラウド認証の初回認証審査に必要な審査時間を追加させていただきます。

ただし、クラウド認証の取得を希望される時期が ISMS 認証審査のサイクルに合わない場合 (ISMS 認証のサーベイランス又は再認証審査と同時に受審しない場合)、ベースとなる ISMS 認証部分の関連事項確認の為、別途 1.0 人日分の審査工数を追加させていただきます。

また ISMS 認証取得済の組織がクラウド認証を取得された場合、クラウド認証の審査サイクル及び有効期限は、クラウド認証の取得時期に関係なく、ベースとなる ISMS 認証の審査サイクルに合わせる事となる事ご留意下さい。

これらクラウド認証審査に係る審査時間/費用については、ベースとなる ISMS 認証分とは別途のお見積りとなります。これは、本認証が ISMS 管理策にクラウドサービス固有の管理策を追加するものである為です。

#### 【ISMS 認証取得済組織がクラウド認証を追加する場合の例】



## 4 お客様にご準備いただきたい事項と審査の詳細

審査までにご準備いただきたい事項と、各段階の審査の詳細をご紹介します。

### 4.1 各審査共通のご準備をお願いする事項

項目	準備期限	準備事項
変更事項の通知	変更時即時	<p>次の適用範囲に関わる事項に変更があった場合、変更時にその概要を ISA へご通知下さい。できる限り電子データでご送付下さい。変更審査の必要性を判断します。 (<u>変更通知様式を巻末に提示します。</u>)</p> <ul style="list-style-type: none"> <li>● 対象事業/業務内容</li> <li>● 対象組織の代表者/所有権/登記に関わる変更</li> <li>● 連絡先窓口</li> <li>● 認証対象事業所の所在地</li> <li>● 対象施設/情報システム等プロセス上の大きな変化</li> </ul> <p>* ) 報告いただいた変更の程度により、審査工数の見直しが発生する場合があります。 審査当日に審査チームへ直接変更内容をご報告いただきましても、その変更の程度/審査への影響の大きさにより、登録情報の更新は不可能な場合があります。 また、変更の結果、確認できないプロセス/事業等があった場合には、認証対象から外す(縮小)処置を取らせていただく場合があります。</p>
審査予定のご確認	「審査日程と審査員のご提案」返信まで	<p>予定されている審査時期が近づいてまいりましたら ISA より「変更調査票」「審査日程と審査員のご提案」(その時点で把握させていただいている貴組織の基本情報と、次回審査日程及び担当する審査員を通知する文書)を FAX 又はメールにより送付させていただきます。</p> <p>通知内容に問題が無い場合(基本情報に間違い/変更がない事をご確認下さい。また審査日程及び担当審査員にご了解いただけるかを確認下さい。)本書にご担当者様のご署名をいただき、FAX 又はメールにてご返送をお願いします。</p> <p>本書返信受領にて、審査予定を確定させていただきますが、通知内容に変更がある場合(審査対象拠点の所在地、要員規模、対象業務内容等)、審査計画(審査工数、日程、担当審査員)を変更する必要がある場合があります。</p> <p>* ) 当社からの予定されている審査に関する確認連絡に対し、返信等をいただけない、又は返信が大きく遅延した場合、御社のご希望時期/実施期限までに審査計画を立てることが困難となります。御社担当者/連絡先の変更等ございました際には速やかにご連絡いただけますようお願い致します。</p>
審査員宿泊先の手配	「審査日程と審査員のご提案」返信まで	<p>ISA から御社に提示する「審査日程と審査員のご提案」に宿泊手配の依頼が提示されている場合、また別段の要件が示されていない場合には、次の要件を満たす宿泊先の手配をお願いしております。また「審査日程と審査員のご提案」への返信時に、ご手配いただきました宿泊先の情報を追記いただき ISA へご通知下さい。</p> <ul style="list-style-type: none"> <li>● 1泊1万5千円以内(消費税別・朝食付 禁煙)</li> <li>● 夕食不要 チェックイン21時</li> </ul>

<p>最新文書の準備</p>	<p>審査日前日まで</p>	<p>次の事項を含め、ISMS 文書記録一式を審査場所で審査員が確認できるように準備してください。紙でも、見読できるデータ資料でも結構です。          事前にご提出いただく必要はありません。</p> <ul style="list-style-type: none"> <li>➢ 情報セキュリティ方針/マニュアル/規定/手順書</li> <li>➢ 適用宣言書</li> <li>➢ リスクアセスメントの記録、リスク対応計画文書及び実施記録</li> <li>➢ 情報セキュリティ目的達成の為に計画文書及び達成結果とその証跡</li> <li>➢ その他計画文書および活動記録</li> </ul>
<p>審査員用部屋の準備</p>	<p>審査日まで</p>	<p>オープニングミーティング、クロージングミーティングおよび、審査員が昼食を頂いたり各種作業を行ったりする部屋をご用意ください。          審査員は審査報告資料作成の為、モバイル PC の持ち込みをさせていただきますので、モバイル PC の持ち込み及び電源の利用許可をお願いします。          ＊) モバイル PC 等の持ち込み及び事業所への入室に際し、事前の申請手続き等の必要がある場合、その手順等についてご連絡をお願いします。</p>
<p>昼食の準備</p>	<p>審査日まで</p>	<p>簡単なもので結構ですので、審査日程に昼食時間を挟む場合、担当審査員人数分の昼食をお客様ご負担でご用意しております。          昼食をいただく際には、審査のまとめ作業や審査チーム内での打ち合わせ等も行わせていただきますので、可能でしたら審査チームのみで食事が取れるようご手配をお願いします。</p>
<p>御社対応要員の確保</p>	<p>審査日まで</p>	<p>オープニングミーティング、クロージングミーティングおよび経営者インタビューの時間には、経営陣のご参加をお願いしております。(通常、オープニングは審査開始後の 30 分間、クロージングは審査終了前の 30 分間で行います)          特にクロージングミーティング時には、経営者様もしくはその代理の方の署名が必要です。          その他審査対象者/部署については、審査日程表にて連絡申し上げます。対応いただける方のスケジュールの確保をお願い致します。          ＊) 対応者の不在、十分な回答をいただけない場合、審査の進行が困難であると判断させていただく場合がございます。</p>
<p>審査のご案内者</p>	<p>審査日まで</p>	<p>案内人(審査場所のご案内/審査対応者との間の調整をしていただける方)をご手配下さい。          案内人には以下の調整をお願い致します。</p> <ul style="list-style-type: none"> <li>➢ 面談のための連絡先及びタイミングを確認していただく。</li> <li>➢ 事業所又は特定部署への訪問の手配をしていただく。</li> <li>➢ 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、審査チームへの周知及び順守を確実にしていただく。</li> <li>➢ 組織を代表して、審査に立ち会っていただく。</li> <li>➢ 審査員から要請があった場合に、不明な点を明らかにし、又は情報を提供していただく。</li> </ul> <p>＊) 適切な場合、審査を受ける方が案内役として対応いただいで結構です。</p>

## 4.2 初回認証審査 目的と方法

### 4.2.1 第1段階審査について

<b>目 的</b> :	<ul style="list-style-type: none"> <li>● 御社の組織及び組織を取り巻く状況を理解すること。</li> <li>● 御社の ISMS とその準備状況理解すること。</li> <li>● 初回第2段階審査に移行できるかを判断し、その審査計画の焦点を定めること。</li> </ul>
<b>実施方法と対象</b> :	<p>主に ISMS 文書や計画文書を中心に評価を進めます。管理責任者・事務局を主たる対象者としますが、各部門の資産およびリスクの状況及び IT 管理所管者や人事総務所管者のセキュリティ管理手続きの整備状況、各部署の役割責任等を審査員が理解する為の情報確認等については、各所管者に説明をお願いする場合があります。</p>
<b>留意事項</b> :	<ul style="list-style-type: none"> <li>● ISMS 運用のため計画が策定されていることを前提に審査を進めます。内部監査・マネジメントレビューについては実施計画が確実に整備されている状況が望ましいです。</li> <li>● 第1段階審査の結果は、審査員がクロージングミーティングの終了時に報告します。</li> <li>● 懸念事項は、第2段階審査までに修正を完了する必要があります。</li> <li>● 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。</li> </ul>

確認項目	主たる確認内容	主たる確認対象
組織の状況	組織及び組織を取り巻く状況の確認。	<ul style="list-style-type: none"> <li>● 組織の事業内容、利害関係者等からの要求事項等</li> <li>● 組織内部、外部の課題</li> </ul>
事業に必要な規制事項の確認	適用規制の概要及び当局との協定/通信内容、責任範囲の確認。	<ul style="list-style-type: none"> <li>● 法規制リストや許可証</li> <li>● 顧客及び供給者との契約書</li> </ul>
適用範囲	適用範囲の業務/組織/物理的区画/論理的区画の確認。	<ul style="list-style-type: none"> <li>● 各プロセスの責任の所在に関する情報</li> <li>● 顧客/外部委託事業者との契約書面</li> <li>● オフィスや IT インフラの状況、ネットワーク構成</li> </ul>
情報セキュリティ方針、情報セキュリティ目的	設定の仕組み、内容。	<ul style="list-style-type: none"> <li>● 情報セキュリティ方針及び情報セキュリティ目的の記述文書</li> </ul>
リスクアセスメントの方法、リスクアセスメント結果	リスクアセスメントの方法と関連様式等の確認。(比較可能性、再現可能性の担保)	<ul style="list-style-type: none"> <li>● リスクアセスメントの方法や基準を定めた文書</li> <li>● リスクアセスメント結果記録</li> </ul>
管理策の導出状況	管理目的管理策の採用/不採用理由の確認。	<ul style="list-style-type: none"> <li>● 適用宣言書の確認による採否の状況とその理由</li> </ul>
リスク対応計画の策定状況 文書化の状況	計画の対象と計画内容の確認。(文書化された要求事項が実現できるか)	<ul style="list-style-type: none"> <li>● リスク対応計画</li> <li>● 各種 ISMS 運用のための文書</li> <li>● 詳細管理策をもとに計画した ISMS 文書</li> </ul>
情報セキュリティ目的及びその達成の為の計画	部門及び階層において確立された情報セキュリティ目的とその達成計画の確認。	<ul style="list-style-type: none"> <li>● 情報セキュリティ目的と目的達成計画の管理文書</li> </ul>
組織的/人的セキュリティ、教育訓練の計画	各種計画の確認。	<ul style="list-style-type: none"> <li>● ISMS 上の役割と責任、組織の情報セキュリティに影響を与える要員に求める力量の決定とそれを持たせる為の活動</li> <li>● 外部組織との関係や契約の状況</li> <li>● 入退職時の手続き、教育訓練手順とその計画など</li> </ul>
事業継続マネジメントにおける情報セキュリティの考慮	事業継続計画の立案状況、ICT 継続の要求事項とその検証活動の確認。	<ul style="list-style-type: none"> <li>● 事業継続のプロセス及び手順に関する文書</li> <li>● ICT 継続の検証計画等</li> </ul>
情報セキュリティパフォーマンス評価の対象と測定方法	ISMS のパフォーマンス及び有効性をどのように測定するか確認。	<ul style="list-style-type: none"> <li>● パフォーマンス評価の対象と方法</li> </ul>
内部監査プログラム/計画	内部監査計画状況確認。(計画及び実施記録確認)	<ul style="list-style-type: none"> <li>● 内部監査の実施計画と実施記録</li> </ul>
マネジメントレビューの計画	マネジメントレビュー計画状況確認。(計画及び実施記録確認)	<ul style="list-style-type: none"> <li>● マネジメントレビューの実施計画と実施記録</li> </ul>
インシデント、セキュリティ違反/苦情への対応状況	インシデント、セキュリティ違反発生時の対応方法確認。	<ul style="list-style-type: none"> <li>● インシデント対応の手順など</li> <li>● 就業規則など</li> </ul>
不適合及び是正処置	計画状況確認。	<ul style="list-style-type: none"> <li>● 是正処置の手順を文書化したものなど</li> </ul>

## 4.2.2 第2段階審査について

目 的 :	<ul style="list-style-type: none"> <li>● 情報セキュリティ方針、情報セキュリティ目的、手順に従って構築された ISMS が有効に実施されているか確認すること。</li> <li>● ISMS 規格のすべての要求事項に適合していること、御社 ISMS が自ら定めた情報セキュリティ方針及び情報セキュリティ目的を実現しつつあることを確認すること。</li> </ul>
実施方法と対象 :	<ul style="list-style-type: none"> <li>● ISMS 文書・運用記録閲覧、組織内の活動や機器の設定状況の観察、各部門/プロセスの従事者への質問を通じて、計画されたマネジメントシステムの運用状況、遵守の状況を確認します。特に次の事項を重点的に確認します。 <ul style="list-style-type: none"> <li>➢ 第1段階審査において提示された「懸念事項」「観察事項」(あった場合)への対応状況</li> <li>➢ 情報セキュリティ方針及び情報セキュリティ目的の確立、ISMS 活動への積極的関与によりトップマネジメントのリーダーシップ及びコミットメントが実証されていること</li> <li>➢ 組織内外の課題・要求事項と、情報セキュリティ方針及び情報セキュリティ目的が、相互に論理的に矛盾なく結び付けられていること</li> <li>➢ 情報セキュリティに関するリスクアセスメントが一貫性/妥当性があり、比較可能な結果を生み出していること</li> <li>➢ リスクアセスメント及びリスク対応プロセスに基づくプロセス及び管理策の選択/導入が適切に行われていること</li> <li>➢ ISMS の意図した成果を達成する為に選択した管理策が有効に機能していること</li> <li>➢ 規格の文書化に関する要求事項が全て満たされていること</li> <li>➢ ISMS のパフォーマンス及び有効性の評価の仕組みが明確であること</li> <li>➢ ISMS 内部監査及びマネジメントレビューが実施されていること</li> <li>➢ ISMS の各プロセスのレビューを通じて、経営陣の決定が裏付けられており、情報セキュリティ方針及び情報セキュリティ目的の達成へ向けた取り組みが行われていること</li> </ul> </li> </ul>
留 意 事 項 :	<ul style="list-style-type: none"> <li>● 内部監査・マネジメントレビューが完了し、マネジメントシステムの運用サイクル(PCDA)が、少なくとも1度回っていることを前提に審査を進めます。</li> <li>● 第2段階審査の結論は、審査員がクロー징ミーティング終了時に通知いたします。</li> <li>● 第2段階審査で提示するマイナーな不適合は、審査完了日から1カ月以内にその完了をISAへ通知しなければなりません。改善が望ましい観察事項については、次回審査時に検討及び対応状況を確認します。</li> <li>● メジャー(重大)な不適合については、再審査となります。その後の対応方法については、ISAからご案内します。</li> <li>● 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。</li> </ul>

確認項目	主たる確認内容	主たる確認対象
組織の状況	内外の期待・課題、要求事項 事業環境の変化点の確認。	<ul style="list-style-type: none"> <li>● マネジメントレビュー/経営者インタビュー</li> <li>● 法規制リストや許可証</li> <li>● 顧客及び供給者との契約書</li> </ul>
情報セキュリティ方針、情報セキュリティ目的	方針・目的の達成の状況と今後の展開。	<ul style="list-style-type: none"> <li>● マネジメントレビュー/経営者インタビュー</li> <li>● 情報セキュリティ方針、情報セキュリティ目文書</li> </ul>
適用範囲	現在の状況及び見直しの状況。	<ul style="list-style-type: none"> <li>● 各プロセスの責任の所在に関する情報</li> <li>● 顧客/外部委託事業者との契約書面</li> <li>● オフィスやITインフラの状況、ネットワーク構成</li> </ul>
リスクアセスメントのプロセス及び結果	実施結果と見直しの状況。	<ul style="list-style-type: none"> <li>● リスクアセスメントの基準やリスクアセスメント結果記録</li> </ul>
管理策の導出状況	現在の状況及び見直しの結果。	<ul style="list-style-type: none"> <li>● 適用宣言書の更新の有無(組織変化との整合)</li> </ul>
リスク対応の状況	リスク対応計画とその進捗状況。 採用管理策の運用状況。	<ul style="list-style-type: none"> <li>● リスク対応計画の結果</li> <li>● 詳細管理策をもとに計画した活動の記録</li> <li>● 各種機器等の設定/運用の状況</li> </ul>
組織的/人的セキュリティ	運用結果の確認。	<ul style="list-style-type: none"> <li>● 組織要員及び外部供給者に対し実施される教育。</li> <li>● 外部提供されるプロセス/製品/サービスの評価結果</li> </ul>
事業継続マネジメントにおける情報セキュリティ	事業継続における要求事項の決定、手順の確立とその検証状況の確認。	<ul style="list-style-type: none"> <li>● 事業継続の計画文書及びその記録</li> <li>● ICT継続の備え及び試験の結果</li> </ul>
ISMS のパフォーマンス及び有効性評価	ISMS のパフォーマンス及び有効性評価の方法と結果を確認。	<ul style="list-style-type: none"> <li>● 監視測定の対象とその評価方法</li> <li>● 監視測定の結果</li> </ul>
内部監査	内部監査の計画と結果を確認。	<ul style="list-style-type: none"> <li>● 内部監査の計画状況とその実施記録</li> </ul>
マネジメントレビュー	マネジメントレビューへの報告事項と評価結果、決定/指示事項の確認。	<ul style="list-style-type: none"> <li>● マネジメントレビュー記録、マネジメントレビューから出た決定/指示事項への対応状況</li> </ul>
インシデント、セキュリティ違反/苦情への対応状況	インシデント発生状況と処置の実施状況の確認。	<ul style="list-style-type: none"> <li>● インシデントの発生実績及び処置の記録</li> </ul>
不適合及び是正処置	発生した不適合の実績と発生時の対応結果の確認。	<ul style="list-style-type: none"> <li>● 不適合及び是正処置の記録</li> </ul>

### 4.3 サーベイランス審査 目的と方法

<b>目 的</b> :	<ul style="list-style-type: none"> <li>● 御社が経営環境の変化を踏まえ、ISMS の必要な見直しを実施している事を確認する。</li> <li>● ISMS が引き続き適切に実施されていること、認証要求事項を満足していることを確認する。</li> </ul>
<b>実施方法と対象</b> :	<ul style="list-style-type: none"> <li>● サーベイランス審査では、次の事項を含む運用状況を審査して、お客様のマネジメントシステムが認証要求事項を満足しているか否か評価します。 <ul style="list-style-type: none"> <li>➢ 内外の課題、要求事項(関連法令規制含む)の変化と変化への対応状況</li> <li>➢ 組織、文書、適用範囲の変更の必要性の検討結果と対応の状況</li> <li>➢ 前回までの「是正処置要求書」(あった場合)への対応状況</li> <li>➢ 前回までの「観察事項」(あった場合)への対応状況</li> <li>➢ その他 ISA からの照会事項(あった場合)への対応状況</li> <li>➢ ISMS の継続的な運用管理状況</li> <li>➢ インシデント(あった場合)への対応状況</li> <li>➢ 不適合、是正処置(あった場合)への対応状況</li> <li>➢ 内部監査実施状況</li> <li>➢ マネジメントレビュー実施状況</li> <li>➢ 登録証/認定・認証マークの使用状況及び認証の表明方法の適切性、「電子清刷」の管理状況</li> <li>➢ 情報セキュリティ方針及び情報セキュリティ目的の達成状況</li> <li>➢ ISMS パフォーマンス及び有効性の評価結果</li> </ul> </li> </ul>
<b>留意事項</b> :	<ul style="list-style-type: none"> <li>● 審査の結論は、審査員がクロージングミーティング終了時に通知いたします。</li> <li>● 審査で提示するマイナーな不適合は、審査完了日から1カ月以内にその完了を ISA へ通知しなければなりません。改善が望ましい観察事項については、次回審査時に検討及び対応状況を確認します。</li> <li>● メジャーな不適合については、再審査となります。その後の対応方法については、ISA からご案内します。</li> <li>● 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。</li> </ul>

確認項目	主たる確認内容	審査員が主に確認する物
組織の状況	内外の期待・課題、要求事項 事業環境の変化点の確認。	<ul style="list-style-type: none"> <li>● マネジメントレビュー/経営者インタビュー</li> <li>● 法規制リストや許可証</li> <li>● 顧客及び供給者との契約書</li> </ul>
情報セキュリティ方針、目的	達成の状況。今後の展開。	<ul style="list-style-type: none"> <li>● マネジメントレビュー/経営者インタビュー</li> <li>● 情報セキュリティ方針、情報セキュリティ目文書</li> </ul>
適用範囲	現在の状況及び見直しの状況。	<ul style="list-style-type: none"> <li>● 各プロセスの責任の所在に関する情報</li> <li>● 顧客/外部委託事業者との契約書面</li> <li>● オフィスや IT インフラの状況</li> <li>● ネットワーク構成を図示した資料</li> </ul>
リスクアセスメントのプロセス及び結果	実施結果と見直しの状況。	<ul style="list-style-type: none"> <li>● リスクアセスメントの基準やリスクアセスメント結果記録</li> </ul>
管理策の導出状況	現在の状況及び見直しの状況。	<ul style="list-style-type: none"> <li>● 適用宣言書の更新の有無(組織変化との整合)</li> </ul>
リスク対応の状況	リスク対応計画とその進捗状況。 採用管理策の運用状況。	<ul style="list-style-type: none"> <li>● リスク対応計画の結果</li> <li>● 詳細管理策をもとに計画した活動の記録</li> <li>● 各種機器等の設定/運用の状況</li> </ul>
組織的/人的セキュリティ	運用結果の確認。	<ul style="list-style-type: none"> <li>● 組織要員及び外部供給者に対し実施される教育。</li> <li>● 外部提供されるプロセス/製品/サービスの評価結果</li> </ul>
事業継続マネジメントにおける情報セキュリティ	事業継続における要求事項の決定、 手順の確立とその検証状況の確認。	<ul style="list-style-type: none"> <li>● 事業継続の計画文書及びその記録</li> <li>● ICT 継続の備え及び試験の結果</li> </ul>
ISMS のパフォーマンス及び有効性評価	ISMS のパフォーマンス及び有効性評価の方法と結果を確認。	<ul style="list-style-type: none"> <li>● 監視測定の対象とその評価方法</li> <li>● 監視測定の結果</li> </ul>
内部監査	内部監査の計画と結果を確認。	<ul style="list-style-type: none"> <li>● 内部監査の計画状況とその実施記録</li> </ul>
マネジメントレビュー	マネジメントレビューへの報告事項 と評価結果、決定/指示事項の確認。	<ul style="list-style-type: none"> <li>● マネジメントレビュー記録、マネジメントレビューから出た決定/指示事項</li> </ul>
インシデント、セキュリティ違反/苦情への対応状況	インシデント発生状況と処置の実施 状況の確認。	<ul style="list-style-type: none"> <li>● インシデントの発生実績及び処置の記録</li> </ul>
不適合及び是正処置	発生した不適合の実績の確認と発生 時の対応結果。	<ul style="list-style-type: none"> <li>● 不適合及び是正処置の記録</li> </ul>

#### 4.4 再認証審査 目的と方法

<b>目的</b>	<ul style="list-style-type: none"> <li>● ISA 登録/更新後の全期間の ISMS の運用実績、審査結果を踏まえ、続く有効期限まで、御社へ認証を継続して付与しうるか</li> <li>● 情報セキュリティ方針、情報セキュリティ目的、手順に従って構築された ISMS が実施されていることを確認する。</li> <li>● 御社 ISMS が有効に機能し、情報セキュリティ目的を実現しつつあることを確認する。</li> </ul>
<b>実施方法と対象</b>	<ul style="list-style-type: none"> <li>● 再認証審査では、過年度のサーベイランス審査報告書の内容、ISA からお客様へ行った照会への対応状況を踏まえ、現地審査で次の事項を含めて評価を進めます。 <ul style="list-style-type: none"> <li>➢ 組織内外の課題・要求事項の変化に対応し、継続して情報セキュリティ方針及び情報セキュリティ目的が確立されていること、認証の適用範囲が妥当であること</li> <li>➢ ISMS 活動への積極的関与により引き続きトップマネジメントのリーダーシップ及びコミットメントが実証されていること</li> <li>➢ 情報セキュリティに関するリスクアセスメント及びリスク対応のプロセスが引き続き一貫性/妥当性があり、環境の変化に対応して適切な結果が生み出されていること</li> <li>➢ ISMS のパフォーマンス及び有効性の評価が行われ、必要に応じ改善の為の対策がとられていること</li> <li>➢ 過去 3 年間の内部監査活動、マネジメントレビューでの評価結果の信頼性</li> <li>➢ 過去 3 年間に発生したインシデントや顧客苦情、不適合事項への対応状況からみた処置の有効性</li> <li>➢ ISA からの指摘事項の処理状況</li> </ul> </li> </ul>
<b>留意事項</b>	<ul style="list-style-type: none"> <li>● 審査の結論は、審査員がクロージングミーティング終了時に通知いたします。</li> <li>● 審査で提示するマイナーな不適合は、審査完了日から 1 ヶ月以内にその完了を ISA へ通知しなければなりません。改善が望ましい観察事項については、次回審査時に検討及び対応状況を確認します。</li> <li>● メジャーな不適合については、再審査となります。その後の対応方法については、ISA からご案内します。</li> <li>● 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。</li> </ul>

確認項目	主たる確認内容	審査員が主に確認する物
組織の状況	内外の期待・課題、要求事項 事業環境の変化点の確認。	<ul style="list-style-type: none"> <li>● マネジメントレビュー/経営者インタビュー</li> <li>● 法規制リストや許可証</li> <li>● 顧客及び供給者との契約書</li> </ul>
情報セキュリティ方針、目的	達成の状況。今後の展開。	<ul style="list-style-type: none"> <li>● マネジメントレビュー/経営者インタビュー</li> <li>● 情報セキュリティ方針文書、情報セキュリティ目的に関する文書</li> <li>● 過去 3 年間の活動を通して ISMS の方針/目的の達成に向けた成果の確認</li> </ul>
適用範囲	現在の状況及び見直しの状況。	<ul style="list-style-type: none"> <li>● 各プロセスの責任の所在に関する情報</li> <li>● 顧客/外部委託事業者との契約書面</li> <li>● オフィスや IT インフラの状況</li> <li>● ネットワーク構成を図示した資料</li> </ul>
リスクアセスメントのプロセス及び結果	実施結果と見直しの状況	<ul style="list-style-type: none"> <li>● リスクアセスメントの基準やリスクアセスメント結果記録</li> </ul>
管理策の導出状況	現在の状況及び見直しの状況	<ul style="list-style-type: none"> <li>● 適用宣言書の更新の有無(組織変化との整合)</li> </ul>
リスク対応の状況	リスク対応計画とその進捗状況 採用管理策の運用状況	<ul style="list-style-type: none"> <li>● リスク対応計画の結果</li> <li>● 詳細管理策をもとに計画した活動の記録</li> <li>● 各種機器等の設定/運用の状況</li> </ul>
組織的/人的セキュリティ	運用結果の確認	<ul style="list-style-type: none"> <li>● 組織要員及び外部供給者に対し実施される教育。</li> <li>● 外部提供されるプロセス/製品/サービスの評価結果</li> </ul>
事業継続マネジメントにおける情報セキュリティ	事業継続における要求事項の決定、 手順の確立とその検証状況の確認。	<ul style="list-style-type: none"> <li>● 事業継続の計画文書及びその記録</li> <li>● ICT 継続の備え及び試験の結果</li> </ul>
ISMS のパフォーマンス及び有効性評価	ISMS のパフォーマンス及び有効性評価の方法と結果を確認。	<ul style="list-style-type: none"> <li>● 監視測定の対象とその評価方法</li> <li>● 監視測定の結果</li> </ul>
内部監査	内部監査の計画と結果を確認	<ul style="list-style-type: none"> <li>● 内部監査の計画状況とその実施記録</li> <li>● 過去 3 年間の活動から改善活動の成果が見られるか</li> </ul>
マネジメントレビュー	マネジメントレビューへの報告事項 と評価結果、決定/指示事項の確認	<ul style="list-style-type: none"> <li>● マネジメントレビュー記録、マネジメントレビューから出た決定/指示事項への対応状況</li> </ul>
インシデント、セキュリティ違反/苦情への対応状況	インシデント発生状況と処置の実施 状況の確認	<ul style="list-style-type: none"> <li>● インシデントの発生実績及び処置の記録</li> <li>● 過去 3 年間の活動から改善活動の成果が見られるか</li> </ul>
不適合及び是正処置	発生した不適合の実績の確認と発生 時の対応結果	<ul style="list-style-type: none"> <li>● 不適合及び是正処置の記録</li> <li>● 過去 3 年間の活動から改善活動の成果が見られるか</li> </ul>

## 5. 各認証審査での指摘の分類と対応の方法

各回認証審査では、審査員はお客様のマネジメントシステムについて、次の分類で所見を述べます。「規格要求事項に合致していること＝適合」の場合は、なにも申し上げませんからこの分類には入れていません

それぞれお客様に実施していただく対応方法が異なります。確認をお願いします。

### 5.1 各認証審査での指摘の分類

不適合には2つの区分、観察事項には3つの区分があります。

不適合		
定義	ISMS 規格の要求事項及び、ISMS 規格の要求事項に基づき組織が展開する規定事項が順守されていない状況のことをいいます。	
区分	内容	審査チームからの提示方法
メジャー (重大)	<p>a) システム、又は手順が完全に欠落している状態。システム、又は手順がまったく機能していない状態。</p> <p>例1：文書管理やインシデント管理の仕組みが全くない。 例2：内部監査やマネジメントレビューが実施されていない。</p> <p>b) 類似の不適合がシステム全体に観察され、契約や法規の順守など組織に課せられた責任を果たせない、もしくは情報セキュリティ方針、情報セキュリティ目的の達成に重大な障害を生じうる重大なリスクが放置されている状態。</p> <p>例1：リスクアセスメントの結果、重大なリスクを抱える複数の部門で、インシデント管理の取り組みが実施されていない。</p> <p>c) 前回審査で指摘したマイナーな不適合が是正されていない状態。または是正処置が意図的に守られていない状態。</p> <p>d) 法あるいは契約違反に全く対応していない状態</p> <p>注) 適用される法令を特定し、順守する仕組みがとられていない、監視する仕組みが機能していないといった、マネジメントシステム上の不具合も指摘対象となります。</p>	<p>不適合が発見された場合、審査員はISMS 要求事項の各要素別に「是正処置要求書」を作成します。</p> <ol style="list-style-type: none"> <li>1) ISMS 要求事項の同じ要素についての複数の不適合が一緒になって一つのメジャー是正処置要求が形成される場合、これらの不適合はすべて同じ「是正処置要求書」に記載する場合があります。</li> <li>2) お客様の代表者又はその代理者に対して、不適合の内容を説明し、了承を得て「報告書式」に署名を受けます。</li> <li>3) 「是正処置要求書」の原紙はお客様のもとに置き、コピーを審査員が持ち帰ります。</li> </ol> <p>なお、審査中に不適合を発見した場合、審査員はその場でお客様とともに、状況の確認をおこない、審査チームで審査所見をまとめるときに不適合如何の最終判断をします。是正処置要求は審査チームとして発行します。</p>
マイナー (軽微)	<p>メジャーな不適合以外の不適合のことです。</p> <ol style="list-style-type: none"> <li>a) 単純なシステム上の欠陥、手順の一部欠落</li> <li>b) 単純な過失による一時的な手順上の不適合</li> <li>c) 認証の表明やマーク使用方法の誤り</li> </ol>	

観察事項		
定義	不適合以外で認証審査活動中審査チームが発見した事項	
区分	内容	審査チームからの提示方法
観察事項 A	<p>不適合ではないですが、マネジメントシステムに影響を与える可能性のある発見事項のことです。</p> <p>例：審査範囲外の事項、将来的に不適合になる可能性を持っている事項、対策の必要を検討いただきたい事項など。</p>	<p>検出された場合、審査員は「観察事項シート」に各観察事項を記載し、顧客に提示します。</p> <ol style="list-style-type: none"> <li>お客様代表者に対して、内容を説明し、了承を得ます。</li> <li>「観察事項シート」の原紙は審査員が持ち帰り、コピーをお客様に提供します。</li> </ol> <p>観察事項は、お客様の組織内でご検討いただく事を求めるものです。検討の結果不採用であっても構いません。</p> <p>次回審査で担当審査員が検討結果の内容を確認します。</p>
観察事項 B	<p>特に優れた事項など、今後の運用上さらに充実することで成熟が期待できる事項のことです。</p> <p>(ネガティブな指摘ではありません)</p>	<p>懸念事項が検出された場合、審査員は「観察事項シート」に ISMS 要求事項に対応した懸念事項である事を明示し、お客様に提示します。</p> <ol style="list-style-type: none"> <li>お客様の代表者に対して、内容を説明し、了承を得ます。</li> <li>「観察事項シート」の原紙は審査員が持ち帰り、コピーはお客様に提供します。</li> </ol>
懸念事項	<p><u>初回認証審査の第一段階審査でのみ提示します。</u></p> <p>第二段階審査の折に不適合と判断する可能性が非常に高い事項を「懸念事項」として提示します。</p>	<p>懸念事項が検出された場合、審査員は「観察事項シート」に ISMS 要求事項に対応した懸念事項である事を明示し、お客様に提示します。</p> <ol style="list-style-type: none"> <li>お客様の代表者に対して、内容を説明し、了承を得ます。</li> <li>「観察事項シート」の原紙は審査員が持ち帰り、コピーはお客様に提供します。</li> </ol>

## 5.2 各認証審査での指摘（不適合）への対応方法

3種類の不適合指摘への対応方法は不適合の重大性と審査段階で異なります。

不適合を提示した場合のお客様の対応手順				
区分	初回認証審査	サーベイランス審査	再認証審査	変更（拡大 縮小含む）
メジャー （重大）	お客様は、 <u>是正処置要求後 1ヶ月以内に是正完了を ISA へ書面で報告しなければなりません。</u>	お客様は、 <u>是正処置要求後 1ヶ月以内に是正処置の計画もしくは完了を ISA へ書面で報告しなければなりません。</u>	お客様は、 <u>是正処置要求後 1ヶ月以内に是正完了を ISA へ書面で報告しなければなりません。</u>	お客様は、 <u>是正処置要求後 1ヶ月以内に是正完了を ISA へ書面で報告しなければなりません。</u>
	担当チームリーダーは、フォローアップ審査の日程を、審査実施中にお客様と合意します。 注）再認証審査の場合には、フォローアップ審査による是正処置の完了の確認を、認証有効期限日到来前の ISA 社内判定日程までに実施するように期限設定します。			
	6ヶ月以内に ISA が受審組織を訪問（フォローアップ審査を実施）して是正処置の実施・運用状況を確認します。	2ヶ月以内に ISA が受審組織を訪問（フォローアップ審査を実施）して是正処置の実施・運用状況を確認します。（計画での報告を受けていた場合は完了についても確認）	2ヶ月以内又は有効期限の 2週間前までのいずれか短い方の期間に ISA が受審組織を訪問（フォローアップ審査を実施）して是正処置の実施・運用状況を確認します。	2ヶ月以内に ISA が受審組織を訪問（フォローアップ審査を実施）して是正処置の実施・運用状況を確認します。
マイナー （軽微）	<u>お客様は、是正処置要求後 1ヶ月以内に是正完了の報告を ISA へ書面でしなければなりません。</u>			
	チームリーダーが回答内容の承認如何を判定します。 承認できない場合、承認できると判定できるまで、再度是正の実施を要求します。 <b>（期限内に是正に対し承認の判定ができない場合、認証の一時停止/取消しとなる場合があります）</b>			
	初回認証審査時の場合には、是正完了までが必須です。 サーベイランス審査以降には、是正完了を報告する場合と、是正計画を報告する場合があります。  次回審査訪問時に、是正処置の実施・運用状況を確認します。 維持審査の場合で、計画で報告を受けていた場合は、完了についても確認します。			

## 6. 認証の表明／認定シンボル・認証マークの利用方法

ISA からマネジメントシステムの認証を受けると、本紙に従い登録証、認定・認証マークを用いる等により認証の表明をしていただくことが出来ます。

但し、これら認証の表明及び認定・認証マークの使い方には以下の制限があります。

ここでは皆様に認証の表明/認定シンボル・認証マークを正しくご利用いただくためのガイダンスを提示します。

### 6.1 認証の表明、認定シンボル・認証マーク 用語

- 「認定シンボル」

認定機関: ISMS-AC から、ISA が認定を受けていることを示すマークです。

[ISMS 認証]



[クラウドセキュリティ認証]



- 「認証マーク」

ISA が御社へ認証を付与していることを示すマークです。

[ISMS 認証]



[クラウドセキュリティ認証]



- 「認証番号」

組織が認証を受けているマネジメントシステムごとに ISA が付与する固有の番号です。登録証に記載されます。

- 「登録証」

ISA が認定の条件に従って御社へ発行する登録証で、御社への認証を表明する書面です。登録させていただき組織へ送付させていただきますが、登録証の所有権は ISA に帰属します。

## 6.2 認証表明／認定シンボル・認証マークの表示形式

認定シンボル・認証マークで認証を受けた組織が利用できるのは、次の形式だけとなります。

### ① ISA の認証マーク（ISA のマークに規格番号の入ったもの）を単独で使用

[ISMS 認証]



[クラウドセキュリティ認証]



### ② 認定機関（ISMS-AC）の認定シンボルと ISA 認証マークを並べて使用

[ISMS 認証]



[クラウドセキュリティ認証]

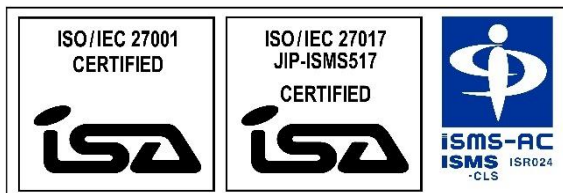


※注記：「認定シンボル」のみの単体使用はできません。「認定シンボル」を使用する場合は、必ず「認証マーク」を並べたものを使用しなければなりません。送付させていただく電子データの配置のまま使用してください。（縦横比率を維持した上での拡大／縮小を除き、データの加工はしないで下さい）

### ③ クラウドセキュリティ認証取得組織における特別な表示例

ISMS 認証に追加してクラウドセキュリティ認証を取得している組織が、ISMS の認証マーク及びクラウドセキュリティの認証マークを同時に（一箇所）で使用する場合、クラウドセキュリティ認証用の認定シンボルのみを使用する事ができます。（ISMS 認証マークとクラウドセキュリティ認定シンボルのみの組み合わせは許容されません）

[ISMS 認証とクラウドセキュリティ認証]

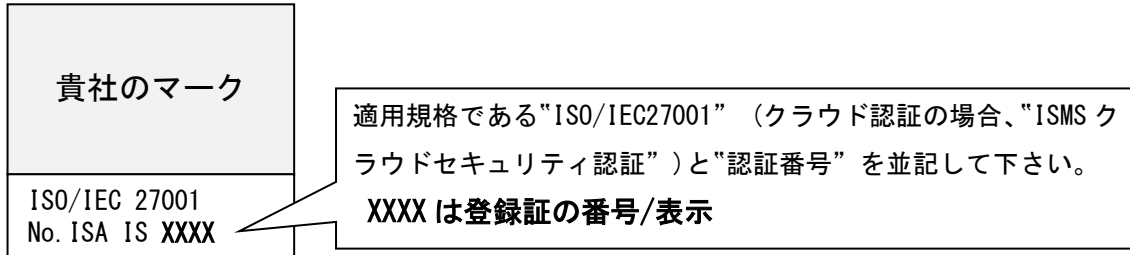


※注記：この表示形式において、ISMS 認証の認証範囲とクラウドセキュリティ認証の認証範囲が異なる場合は、それぞれの認証範囲が異なる事を示す表記（説明等）を付記してください。

●認定シンボル・認証マークを使用せず認証の表明を行う場合

認定シンボル・認証マークを使わずに認証を受けていることを表明することもできます。

①シンボル・マーク非利用：御社のマークを利用して認証を受けていることを表す方法



②シンボル・マーク非利用：言葉のみの表現で認証を受けていることを表す方法

マークを使用せず「ISO/IEC27001 認証取得」「ISMSクラウドセキュリティ認証取得」などの言葉のみの表現で認証を受けていることを表す場合、認証番号などで ISA にて認証を受けていることを示して下さい。

ISO/IEC 27001 認証取得 No. ISA IS XXXX

ISMSクラウドセキュリティ認証取得 No. ISA ISC XXXX

●登録証の使用

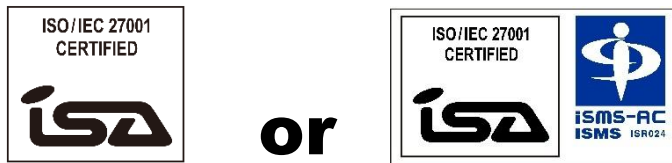
登録証の掲示、コピーや電子データ化しての利用などに際しては、以下の点にご注意ください。

- ・登録証は汚損、紛失等がないよう管理してください。登録証の所有権はISAに帰属します。汚損、紛失の場合、再発行する事となりますが有償となります。
- ・コピーは鮮明なものを使用し、原本の写しであることを明確にするため「写し」である事を意味する文字を追加したものを利用ください。
- ・掲示/配布/提供に際しては、登録証と付属する場合には付属書を対にして扱ってください。

## 6.3 認証の表明、その利用範囲・制限細則

### 【使用できる範囲】

- 認定シンボル・認証マーク（下記イメージは ISMS 認証の例）



これらのシンボル・マークは、登録された情報セキュリティマネジメントシステムに関する説明書、宣伝用資料、封筒、レターヘッド、名刺等の印刷物及びウェブサイト等に使用することが出来ます。

なお、認証マークと認定シンボルを並べて表示する場合、これらマークが同一のマネジメントシステムに基づくものであることを示すために両方を枠で囲んで下さい。

- 認証マーク（下記イメージは ISMS 認証の例）



このマークは、上記のほか組織の旗、看板、車両等にも用いることが出来ます。

### 【認証の表明にあたっての制限/注意事項】

- 認証の表明/認定シンボル・認証マークは個々の製品が認証されたと誤解されるのを防ぐため、製品それ自体、あるいは梱包に使用しないでください。
- 認証の対象範囲は、登録証に記載された範囲です。そこに記載されていない組織や活動に使用しないでください。認証を受けた範囲と受けていない範囲とが誤解されない方法で使用してください。認証範囲が組織の一部に限定される場合の認証の表明においては、対象になった組織（事業所、部署）・活動（業務）についてのみ利用でき、限定された範囲を示す情報を表明文書・マークと一緒に表記する必要があります。  
名刺に使用する場合、認証範囲外の要員が認証の表明/マークの利用のある名刺を使用する事はできません。
- 認証されたことを広告や出版物に載せるときは ISA によって認証されたことを記述してください。

- 認定シンボル・認証マークを含む媒体(当社より提供するCD)の管理について
  - ・送付した媒体及びその内容物は、保護及び漏洩防止のため、管理を確実にしてください。(目的外の使用防止、不正使用防止、紛失・盗難の防止等)
  - ・当該媒体を提供した下請負業者に、媒体の保護及び情報漏洩防止のための適切な管理を要求し、必要に応じて媒体を提供した下請負業者の一覧表を作成してください。  
(認定シンボル・認証マークのデータを使用して説明書、宣伝用資料、名刺等の作成を依頼した印刷業者等にデータの確実な管理を要求し、依頼した印刷業者等の一覧表を作成すること。協力会社一覧などに掲載されていれば結構です。)
- 電子データの利用について
  - ・認定シンボル・認証マークの電子データは、原則として「印刷用」—ビットマップ(BMP)形式、「ウェブサイト用」—JPEG形式で配布されます。印刷用は印刷に、ウェブサイト用はウェブサイトで使用してください。
  - ・解像度を低くしないで使用してください。
  - ・電子データは保存形式を変更しないでください。
- WEBサイトでマーク等を利用する場合の特別な注意
  - ・「ウェブサイト用」—JPEG形式を使用し、加工・編集しないでください。配布したウェブサイト用データをそのまま使用し、加工や編集をしないでください。
  - ・解像度を低くしないで使用してください。電子データの保存形式を変更しないでください。
  - ・同一のページ内で、認定シンボル(ISMS-ACマーク)、認証マーク(ISAマーク)を使用してください。
  - ・認証範囲が全社でなく、社内の特定の部門/事業に限定されている場合、認証の表明/マークの下もしくは隣接する範囲に「特定の部門/事業で認証取得された」旨の記述をしてください。

[サンプル] (下記イメージは ISMS 認証の例)



認証範囲：本社と A 営業所  
事務機器の修理と販売

- マークデータを含む媒体を汚損、紛失された場合の再発行については有償となります。

### 【認定シンボルの表示制限】

ISMS-ACの認定シンボルには次の表示制限があります。ISAが認定シンボル単独のデータをお客様へ配布することはありません。この注意は、デザインの都合などで、AI形式ファイルを必要とするお客様へ向けた特別の記述となります。

- 認定シンボルの構成  
組織が認定シンボルを表示する場合は「認定番号」(ISAを意味する“ISR024”)とともに表示する。
- 認定シンボルの縮小または拡大  
認定シンボルを縮小または拡大して表示する場合、縦横比を変更しない。縮小する場合の最小サイズは、各部が明瞭に識別できる範囲とする。
- 認定シンボルを並べて表示する場合  
ISAにより登録を受けた組織が認定シンボルを表示する場合は、ISAの認証マークと共に表示する。認定シンボルのみを単独で表示することは出来ない。ISAの認証マークと認定シンボルの関係が明確で、かつ両者が明確に識別できなければならない。認証のマークと認定シンボルを並べて表示する場合、両者が同一のマネジメントシステムに基づくものであることを示す為、両者を枠で囲むこと。
- 認定シンボルの形態、色調



ISMS-AC発行の認定シンボル使用規定抜粋：

認定シンボルを印刷物に表示する場合の色は原則として下記指定色とする。

プロセスカラーの場合：(C100%+M70%)

特殊印刷色の場合：(DIC220) 1色

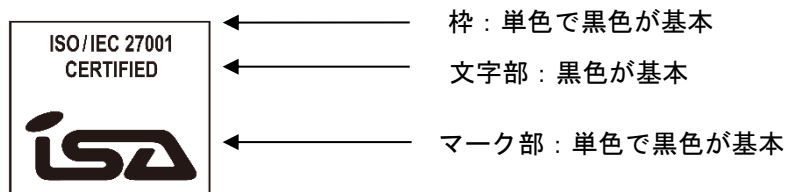
ホームページや電子情報に表示する場合の色指定は原則として下記とする。

WEB カラースライダーで指定の場合：(003399)

RGB カラーで指定の場合：(R=000, G=051, B=153)

### 【認証マークの表示制限】

- ISA ISMS 認証マークの形態、色調



地色、文字色各々、単一色に統一して利用ください。  
認証を示す文字が識別できない配色はご遠慮願います。

#### 【認証の表明/マーク利用の中止】

- 有効期限を過ぎた場合、あるいは登録が取り消された場合、認証の一時停止となった場合には、直ちに認証の表明、マークの利用を中止してください。また、認証の表明、マークの利用をしている文書等については、表明/マークを抹消して使用するか、使用を停止してください。
- 組織が認証範囲の縮小を実施された場合、認証範囲外となった範囲に関連する認証の表明、マークの利用は速やかに中止してください。認証範囲外となった要員による名刺の利用も直ちに中止してください。
- 認証の取下げ、取消し、一時停止等により認証登録の効力が無くなる場合、登録証及びマークデータを含む媒体は、返却又は廃棄を依頼します。

#### 【違反に対する処置】

- 認証の表明について、本手順に違反する使用をした場合、審査にて不適合として指摘し、是正処置を要求します。  
一定期間を経ても是正されない場合、認証実施規定に従い、認証の一時停止、取消し、及び違反の公表等の処置をとります。  
違反の程度に応じ、場合によっては、損害賠償が求められる事があります。

## 6.4 不適切な認証表明/認定シンボル・認証マーク等の使用例

(お客様が間違いやすい不適切な使用例)

認定シンボル (ISMS-AC) の「単独」表示：

単独使用はできません。



※ISMS-AC の認定シンボルは、単独では使用できません。ISA マークは、単独でも使用できます。

看板、門表、ドア、車両等の表示：

認定シンボル (ISMS-AC) は使用できません。

※ISA マーク単独の場合には、組織の旗、看板、門表、ドア、車両にも用いることが出来ません。

広告物・印刷物へのマーク表示：

会社案内、宣伝・広告資料、カレンダー、名刺、封筒・レターヘッド、ウェブサイト等に使用できますが、製品そのものへのマーク表示はできません。また、製品自体が適合していると誤解を与えるような使用はできません。また、マークを縮小しすぎて、ロゴ内の文字が明瞭に確認できない使用はできません。

※製品・製品の梱包・製品証明書等は製品への適合と誤解を与える為使用できません。

認証範囲以外の「業務」又は「事業所」が記載されている資料への表示：

何の注記も記載しないで認証の表明/マークを使用して、記載された「業務」又は「事業所」の全てが認証を受けているかのような誤解を招く使用はできません。

※登録された「事業所名」及び登録証に記載された「登録範囲」の文言を記載すること、又は、その事が明確に判別できる措置があれば構いません。

※名刺に使用する場合は、登録範囲の対象組織（事業所、部署）及び登録範囲の業務に従事する者のみが使用できます。

限定した認証範囲の場合の表示：

認証範囲が全社でなく、社内の特定期間/事業等に限定されている時には、認証の表明/マークの下又は隣接する範囲に「特定部門/事業で認証取得された記述」が必要です。

※名刺に利用する場合、認証対象外の要員の名刺には使用できません。

他の認証と並記した表示：

他機関での認証、ISA で取得した他規格認証との区別にご注意ください。

※当社の ISMS 認証は ISMS-AC 認定の認証サービスですが、当社で受審される QMS/EMS 認証は JAB 認定の認証サービスです。認証機関が異なりますので、マークの使用/配置において、混在しないようにしてください。(データ加工禁止です。)

「文言」での認証取得表現：

「ISA IS \*\*\*\*」という認証番号を併記する等により、ISA(国際システム審査)から認証を取得した事を明示してください。



QMS 認証は ISMS-AC 認定ではありません。認定シンボルには ISA 認定番号を含みます。

## 6.5 [IAF CERT SEARCH]における登録組織情報の公開に関し

世界各国の認定機関（ISMS 認証の認定機関である ISMS-AC 含む）が加盟する IAF（国際認定フォーラム）は、世界中のあらゆる経済圏からの個々の認定された認証をリアルタイムで検証可能とするため、「IAF Cert Search」というシステムを立ち上げました。

本システムは、

- ・ IAF から収集した認定機関データ
- ・ 認定機関から収集した認証機関データ
- ・ 認証機関から収集した認証データ

をまとめ、世界中のユーザが、IAF MLA に加盟する認定機関メンバーが認定した認証機関によって認証された組織が保有する個々の認証の有効性を検証する事をできるようにし、不正な認証表明を防止し、また世界の産業界及び規制当局を支援する事を目的としています。

上記目的を達成する為、IAF は「MD23:2023 IAF データベースにおけるデータのアップロード及び維持に関する IAF 必須文書」を作成し、認定機関及び認証機関に対する必須要求事項としての認証情報の登録を求めています。

本登録においては、（いままでの認定機関にて運用/公開されていたデータベースでは許容されていた）「全部又は一部の組織情報の非公開」について、上記目的を達成する為に厳しい制限が設けられており、以下の事例に該当する場合を除き、原則認証情報の登録及び公開を要求しています。以下事項に該当しない場合については、情報の登録/公開を回避する事はできない事となりますのでご了解の程宜しくお願い致します。

[認証情報の登録/公開の回避が認められる事例]

- ・ 認証された組織が、国家安全保障に関連する活動について認証されている場合
- ・ 認証活動の所在地、又は適用範囲の公表が、認証組織、その従業員又は認証された組織の顧客に対して重大な安全上のリスクをもたらす可能性が合理的に考えられる場合
- ・ 政府又は規制による要求事項により、そのような情報を機密として扱う要求がある場合

注) 認証機関が、認証された組織の情報の全部又は一部を登録できない場合、認定機関に対しその正当な理由を文書で提出する義務があり、認定機関による承認を得る必要があります。



国際システム審査(株) ISMS 担当宛

ISMS 認証範囲の変更通知

通知年月日： 年 月 日

[変更通知組織]

組織名	
組織代表者の役職 代表者ご芳名	役職
本紙記入者の役職 記入者ご芳名	役職

[変更内容の詳細] 欄中に記載できない場合は、別添説明書を同送してください。

対象変更内容	現在（新）	変更前（旧）	別添説明書（有/無と書名）
対象事業/業務			
対象組織の代表者/所有権			
連絡先窓口 (役職氏名、TEL/FAX 番号、メールアドレス等)			
認証対象事業所の所在地			
対象施設/情報システム等プロセス上の大きな変化			

以上