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 ····· 14

４．３　サーベイランス審査　目的と方法 ····· 16

４．４　再認証審査　目的と方法 ····· 18

５．　各認証審査での指摘の分類と対応の方法 ····· 20

５．１　各認証審査での指摘の分類 ····· 20

５．２　各認証審査での指摘（不適合）への対応方法 ····· 22

６．　認証の表明／認定シンボル・認証マークの利用方法 ····· 23

６．１　認証の表明、認定シンボル・認証マーク　用語 ····· 23

６．２　認証表明／認定シンボル・認証マークの表示形式 ····· 24

６．３　認証の表明、その利用範囲・制限細則 ····· 26

６．３．１　認定シンボルのデザイン変更に伴う利用の変更に関して ····· 30

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 ····· 31

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。

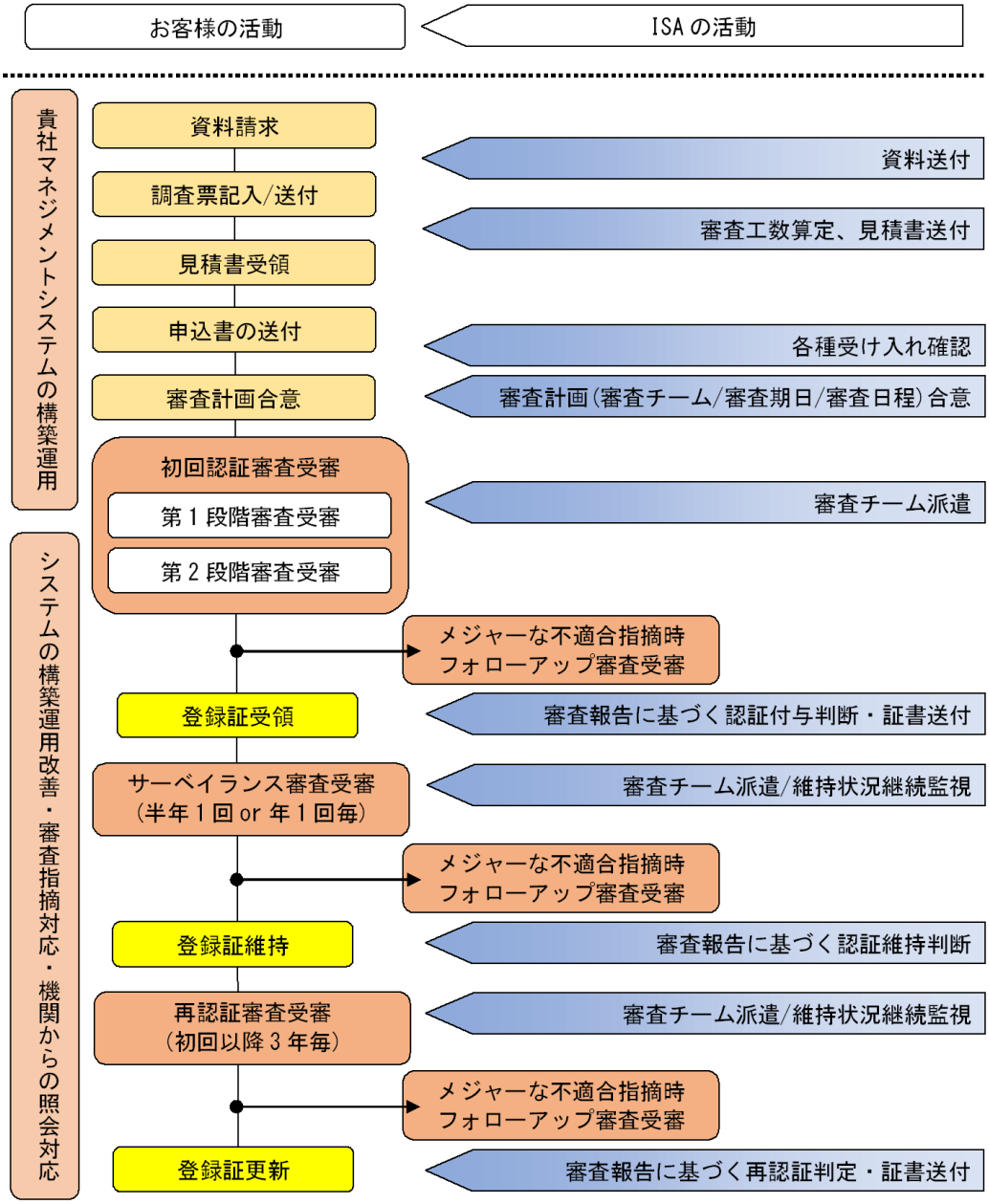
マネジメントシステム認証活動は、お客様と認証機関である ISA による相互の協力関係なしには成り立ちません。是非、本案内書をご確認いただき、認証活動の全体像、個々のプロセスについてご理解をいただくとともに、積極的に ISA との協同作業を進めていただければと存じます。

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-ＩＳＯ規格など-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こと）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・個人からの意見にもとづく照会や確認など

この中でも多くのお客様にとって一番気がかりなところは、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などを通じて、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	初回認証審査は、審査申し込み後初めて受ける審査です。 マネジメントシステムの計画状況の確認の為、文書審査を主体とする第 1 段階審査と、マネジメントシステムの実施状況の確認を行う第 2 段階審査の 2 回に分けて実施します。 第２段階審査は、第１段階審査後、おおよそ２ヶ月程度間をおいて受けていただきます。	● 御社の組織及び組織を取り巻く状況を理解すること。 ● 御社の ISMS 及びその準備状況を理解すること。 ● 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。（どの部門に比重を置いて審査を実施すべきかを定める）
	第２段階審査		● 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こと。 ● 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こと。 ● 御社 ISMS が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。
サーベイランス審査		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。 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。	● 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こと。 ● 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こと。
再認証審査		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。	● ISA 登録後の全期間の 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を評価すること。 ● 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こと。 ● 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こと。 ● 御社 ISMS が有効に機能し、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。

【以下特別な審査】

名称	実施する段階／時期	目的
変更/拡大/縮小審査	既に授与した認証範囲を定期審査とは別の機会に、臨時に登録範囲を変更・拡大・縮小する申請があった場合に実施します 他の審査と同時に行う場合もあります。 注）変更の影響の大きさに応じて、次回審査で確認するか、追加審査を実施するか決定します。	● 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こと。
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。	● 不適合が除去されるとともに、再発防止の計画と対応が完了していることを、原則として現場で確認します。（審査の実施方法は不適合の内容によって異なります。） ● 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します。
短期予告審査	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。	● お客様のマネジメントシステムの重大な問題点を調査し、認証の維持が可能であるか評価することを目的とします。 （ISA に寄せられるお客様に対しての苦情や情報を分析し、実施方法を決定します。審査の方法は目的に応じて異なります。）
移行審査	マネジメントシステムの適用規格を変更する場合に実施する審査です。	● 規格の改訂に伴い、最新版の規格に適合している事（最新版に準拠している事）の確認を目的とします。

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】