Information Security Management System

ISMS適合性評価制度

JIS Q 27001:2014（ISO/IEC 27001:2013）対応版

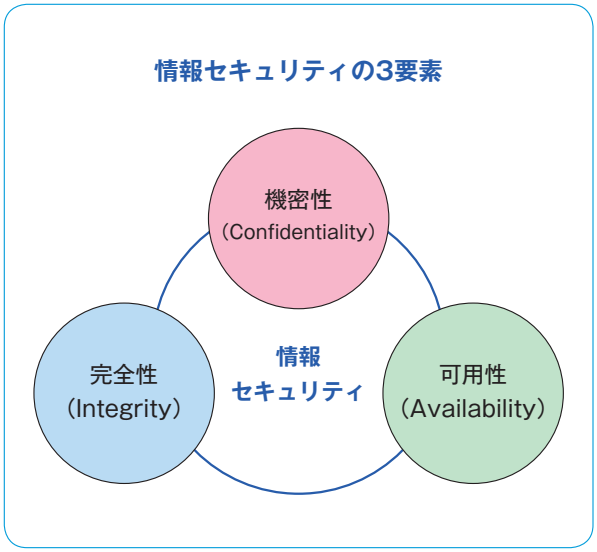
組織の情報セキュリティのための仕組みが
国際規格に適合していることを証明する制度です

一般社団法人
情報マネジメントシステム認定センター
（ISMS-AC）

情報セキュリティマネジメントシステム

ISMSとは

近年、ITシステムやネットワークは社会インフラとして不可欠なものとなっていますが、一方で標的型攻撃やランサムウェアなどによる被害・影響も多発しています。こうした中、組織の情報を保護する有効な手段の1つがISMSです。ISMSとは、Information Security Management System（情報セキュリティマネジメントシステム）の略で、情報のCIA（「機密性（Confidentiality）」、「完全性（Integrity）」、「可用性（Availability）」）を保護するための、体系的な仕組みです。これは、情報が漏えいしないようにし（機密性）、改ざんや誤りがないようにし（完全性）、そして必要なときに必要な人が利用できるようにする（可用性）ということです。ISMSには、技術的対策だけでなく、従業員の教育・訓練、組織体制の整備なども含まれます。



ISMS構築にあたり必要となる

ISMSの国際規格「ISO/IEC 27001（JIS Q 27001）※1」

ISMSを構築するにあたって、必要となるのがISO/IEC 27001（JIS Q 27001）というISMSの国際規格です。この規格には、ISMSをどのように構築、実施、維持、改善すべきなのかが記載されています。また、管理策と呼ばれる情報セキュリティの対策集も記載されています。特に管理策については、ISO/IEC 27002というガイドライン規格があり、管理策を導入する際の参考になります。

ISMSを正しく運用していることを示すための第三者証明

ISMS認証※2

「ISMS認証」とは、第三者であるISMS認証機関が、組織の構築したISMSがISO/IEC 27001に基づいて適切に運用管理されているかを、利害関係のない公平な立場から審査し証明することです。

したがって、「ISMS認証」によって、組織は、ISO/IEC 27001という国際規格に沿って、情報セキュリティを確保するための仕組みをもち、その仕組みを維持し継続的に改善していることを、顧客や取引先に対して客観的に示すことができます。この「ISMS認証」を取得するには、ISMS認証機関に申請し、審査を受ける必要があります。

※1　ISO/IEC 27001とJIS Q 27001

国際規格「ISO/IEC 27001」は、ISO（International Organization for Standardization：国際標準化機構）が発行する国際規格であり、原文は英語です。これを日本国内での使用のために日本語に翻訳し、国内規格として発行したものが「JIS Q 27001」です。翻訳されたJIS Q 27001は、ISO規格と同じ内容であること（IDT：IDENTICAL）が認められています。それぞれの規格の正式名称は次の通りです。

■ISO/IEC 27001：2013 Information technology - Security techniques - Information security management systems - Requirements

■JIS Q 27001：2014　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

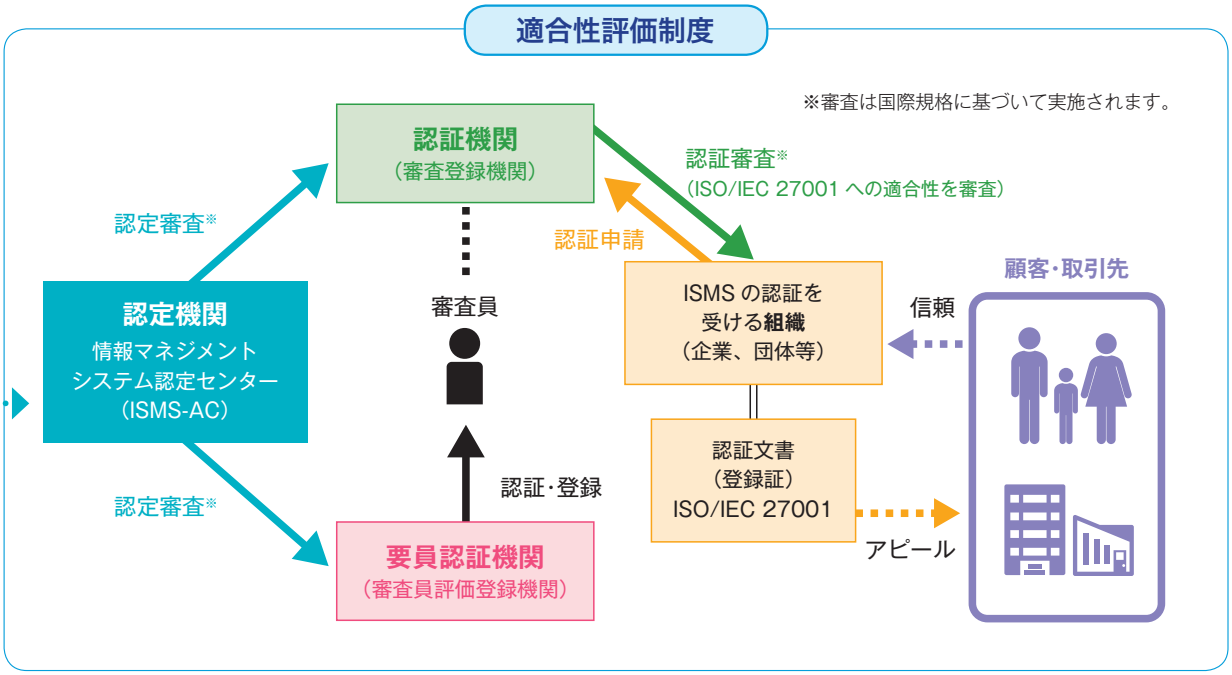
※2　ISMS認証

この「ISMS認証」と同義語として使用されるものに「ISO/IEC 27001認証」「JIS Q 27001認証」があります。上記※1の通り、ISO/IEC 27001とJIS Q 27001の内容は同じものですので、「ISO/IEC 27001認証」「JIS Q 27001認証」も同じ意味です。本書では「ISMS認証」に統一して記載しています。

認証の公平な運用のための国際的な枠組み

ISMS適合性評価制度 ～認定と認証～

認証を公正に運用するために、国際的な枠組みが定められています。これを「適合性評価制度」と呼んでいます。適合性評価制度は「認証機関」「認定機関」「要員認証機関」から構成されます。



認証機関

第三者機関として組織のISMSを審査します。これを「認証審査」といいます。

認定機関

認証機関が適切に認証審査が実施できることを審査し、確認します。これを、「認定審査」といいます。

要員認証機関

認証審査に関する能力をもつ審査員を認証、登録します。

認定機関が、ISMS認証機関を認定する意義

認定機関である情報マネジメントシステム認定センター（ISMS-AC）は、認証機関が適切に審査を実施できる体制・能力をもっているかを、国際規格（ISO/IEC 27006）※に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けたISMS認証機関は、適切なISMS認証審査を実施することのできる、信頼のおける認証機関であることを意味します。要員認証機関についても同様です。

認定シンボル（右）と認証機関マーク（左）が並んだ表示例

認定シンボルと認証機関のマークが２つ並んでいることは、その認証機関が国際規格に従った適切な審査を実施していることを、認定機関であるISMS-ACが保証していることを示します。

※ ISO/IEC 27006 情報技術－セキュリティ技術－情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項

ISMS認証取得を受ける際に知っておきたい

ISMS認証について

■ 認証範囲

組織の必要に応じて定めることができます。必ずしも全社を範囲とする必要はありません。

■ 認証を受けるには ～申請から認証取得までの流れ～

①認証機関の選択

認定された認証機関の中から、申請先を選びます。

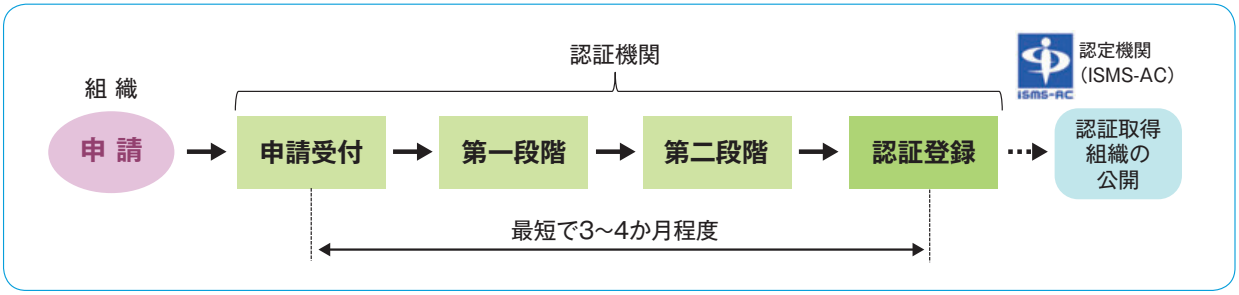
・認証登録に関わる料金は、認証範囲や受審組織の規模等の他、認証機関によって異なります。

・認証機関はISMS認証機関一覧を参照下さい。（参照先：https://isms.jp/lst/isr/）

②申請

選んだ認証機関に申請します。

（ISMS-ACではありませんので、ご注意ください。）



③初回認証審査

申請が受理され、審査に入れる状態になったら、認証機関によって審査が開始されます。審査は原則として第一段階と第二段階の2段階で行われます。

（審査日数や審査工数は、認証範囲、受審組織の規模等によって異なります。）

④認証登録

審査の結果、ISO/IEC 27001（JIS Q 27001）に適合していることが確認されると認証されます。

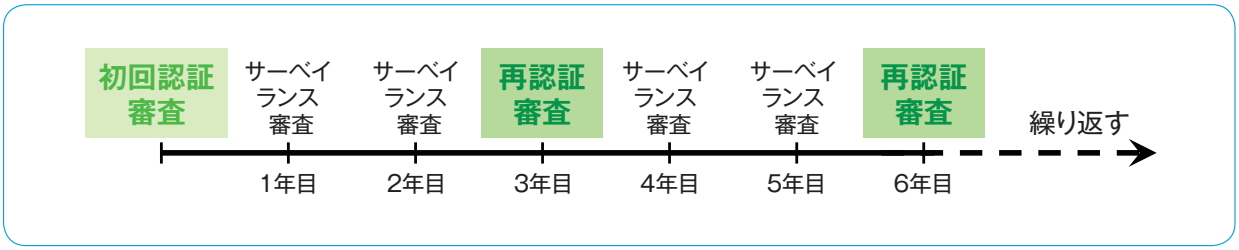
認証の有効期限は3年です。

⑤報告・公開

認証された旨が各認証機関からISMS-ACに報告されましたら、ホームページで公開します。

■ 認証を維持するには ～認証の信頼性を維持するために～

初回審査の後も年に1回以上の中間的な審査（サーベイランス審査）が、そして3年ごとに認証の有効期限を更新するための全面的な審査（再認証審査）が実施され、組織のISMSが引き続き規格に適合し、有効に維持されていることが確認されます。



認定機関の国際的な協力体制

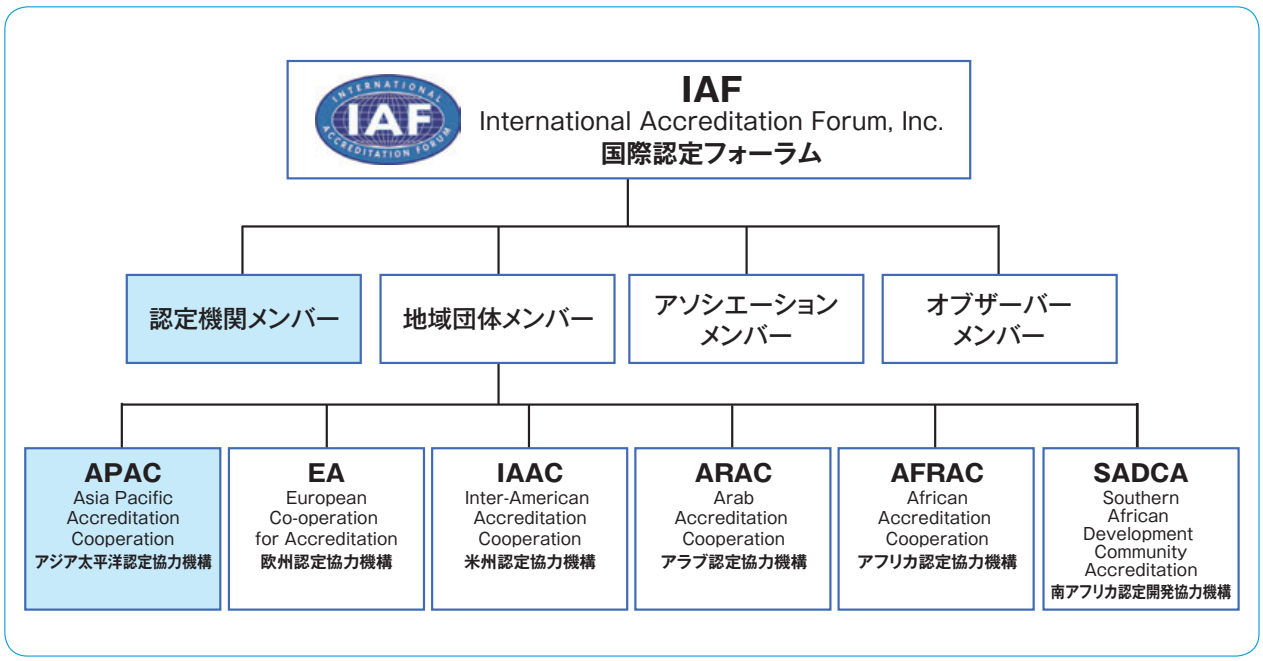
国際認定フォーラム（IAF）への加盟

■ ISMS-ACは国際認定フォーラムに加盟し、国際的な認定機関として貢献しています。

国際認定フォーラム（IAF -International Accreditation Forum, Inc.）は、マネジメントシステム、製品、要員等の適合性評価活動に関わる認定機関、審査機関協議会、各国の産業団体等からなる国際組織です。

IAFの目的の一つは、世界的に整合性のとれた適合性評価プログラムを開発し、認定された認証の信頼性を保証することによって、組織・エンドユーザーのリスクを低減することです。IAFの国際相互承認協定（MLA）に署名した認定機関によって認定された認証機関による認証は、IAFによってその信頼性を保証されます。

ISMS-ACは、2006年にアジア太平洋地域におけるIAFの下部組織であるPAC（現APAC）に、2007年には認定機関メンバーとしてIAFに加盟するとともに、その後新たに発足したISMSのMLAに署名しています。世界的にも多くの認定・認証数の実績をもつISMS-ACは、今後もISMSのMLA運営に対して様々な面から貢献していく考えです。



ISMS認証取得組織へのアンケートより

ISMS導入・ISMS認証取得の効果（メリット）

近年のコンピュータ処理への依存度の高まりやインターネットの爆発的な広がりとともに、それに比例して情報資産への脅威も増大し、システムや人的な脆弱性を突いたセキュリティ事故も件数・規模ともに増加しているため、自社のみならず取引先における情報セキュリティ管理のリスクを把握する重要性についての認識が高まりを見せています。

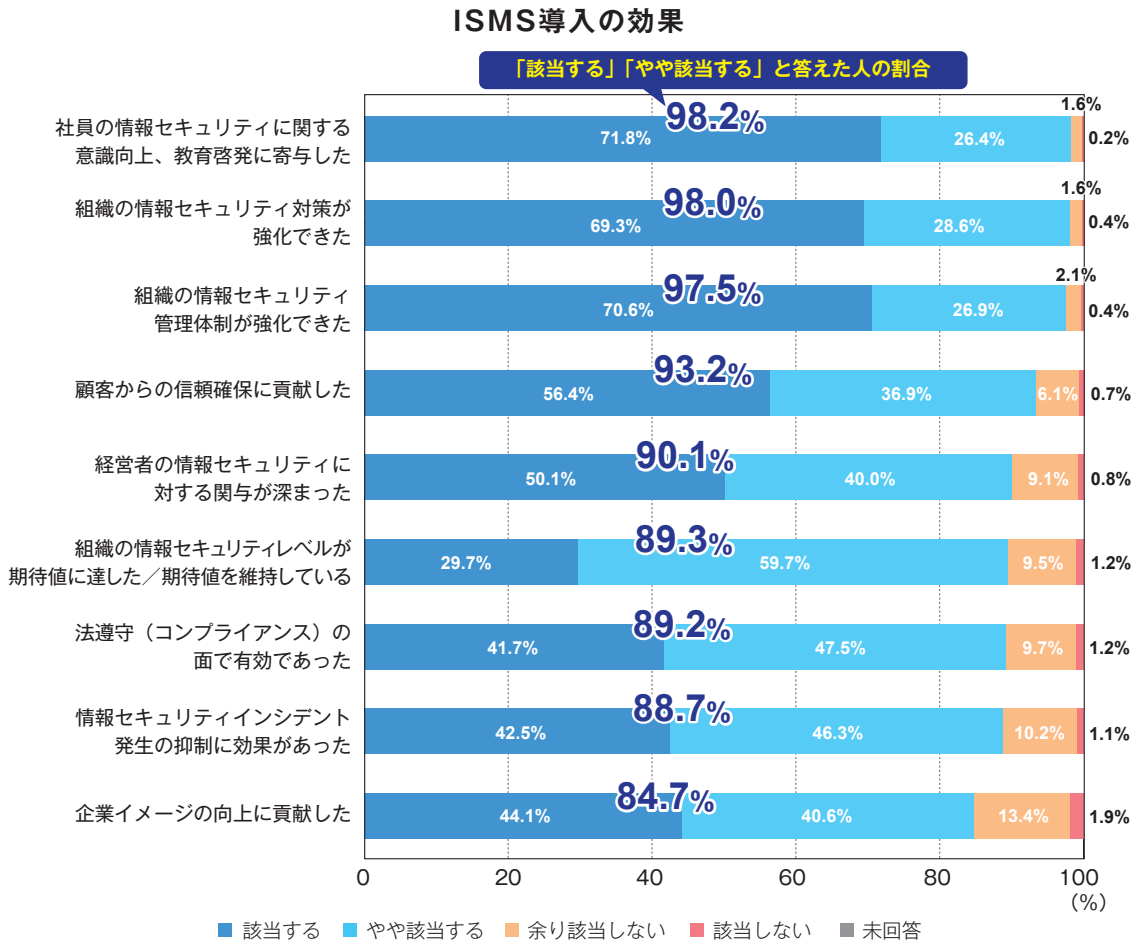
ISMS認証取得組織を対象に「ISMSを導入し、認証を取得された効果」を尋ねたところ、以下のような効果（メリット）が見えてきました。

■ 内部的な効果（メリット）：

- 社員の情報セキュリティに関する意識向上につながる。
- 組織の情報セキュリティ管理体制、情報セキュリティ対策を強化できる。
- 経営者の情報セキュリティに対する関与が深まる。
- 組織の情報セキュリティレベルを向上し、期待レベルを維持できる。 など。

■ 対外的な効果（メリット）：

- 顧客からの信頼確保につながる。
- 企業イメージの向上につながる。 など。



【アンケート調査概要】
- ■調 査 期 間：2018年1月
- ■調 査 対 象：2018年1月時点で、ISMS-AC認定のISMS認証機関からISMS認証を取得した組織のうち、登録情報を公開している5,130組織。
- ■調 査 方 法：郵送でアンケートの案内をし、Web上で質問（選択形式及び記述形式）に回答いただいた。
- ■有効回答数：1,180件
- ■回　収　率：23.0%

クラウドサービスを取り扱う組織には…

ISMSクラウドセキュリティ認証

ISMSクラウドセキュリティ認証とは、ISO/IEC 27001を前提として、その認証範囲内に含まれるクラウドサービスの提供もしくは利用に関して、ISO/IEC 27017※に規定されるクラウドサービス固有の管理策が実施されていることを認証する仕組みです。

ISMSクラウドセキュリティ認証はISO/IEC 27001を前提としていることから、この認証を希望する組織はISO/IEC 27017に沿った対策の実施を要求するJIP-ISMS517-1.0と、ISO/IEC 27001の両方に適合する必要があります。

ISMS-ACでは、クラウドサービスに対する情報セキュリティ認証を求める声を受けて、2016年8月に、ISO/IEC 27017に基づくISMSクラウドセキュリティ認証を開始しました。

■ 認証基準

ISMSクラウドセキュリティ認証の認証基準は、「ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項（JIP-ISMS517-1.0）」です。この認証基準のなかで「ISO/IEC 27001」への適合が求められています。

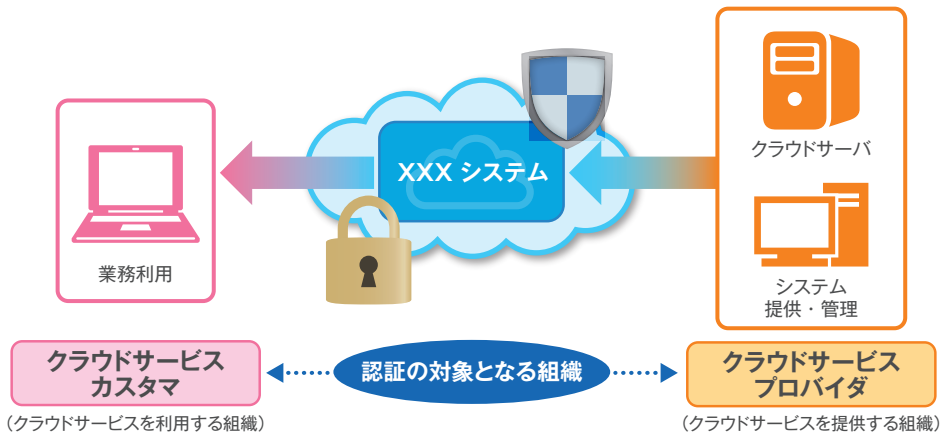
■ ISMSクラウドセキュリティ認証のメリット

ISMS認証に加えて、ISMSクラウドセキュリティ認証を取得することにより、組織はクラウドサービス固有のリスクについて網羅的なアセスメントを実施して必要な管理策を導入していることを、認証機関による審査・認証によって対外的に表明することができます。

また、企業や一般ユーザがクラウドサービスプロバイダ、クラウドサービスカスタマに対して情報を預けることができるかどうかを評価する一つの指標となります。そのため、説明責任が求められている昨今、社会に表明する一つの手段として活用することができます。

■ 認証の対象となる組織

ISMS認証を取得している／取得する組織で、ISO/IEC 27017に従ってクラウドサービスを提供している組織（クラウドサービスプロバイダ）・クラウドサービスを利用している組織（クラウドサービスカスタマ）の両方が対象となります。



※ISO/IEC 27017とは

クラウドサービスに関する情報セキュリティ対策を実施するためのガイドライン規格であり、クラウドサービスを提供する組織と利用する組織の両方を対象としています。なお、内容を変えることなく国内規格化したものとして「JIS Q 27017:2016」があります。正式名称は次の通りです

■ISO/IEC 27017:2015（JIS Q 27017:2016） 情報技術－セキュリティ技術－ISO/IEC 27002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

お問い合わせ先

■ ISMS認証取得に関するお問い合わせ

▶▶▶ 各認証機関にお問い合わせください。

認証機関一覧はこちら https://isms.jp/lst/isr/

■ ISMS適合性評価制度全般に関するお問い合わせ

▶▶▶ 当センターまでお問い合わせください。

情報マネジメントシステム認定センター（ISMS-AC）

TEL 03-5860-7570

当センターでは、次の制度における認定も実施しています。

■ ITSMS適合性評価制度

ITサービスマネジメントシステム（ITSMS）のための制度です。ITSMS認証取得によって、信頼できるITサービスを提供できることを外部に表明できます。また、認証維持のための継続的な審査によって、サービス品質の向上と維持を図ることができます。
https://isms.jp/itsms.html

■ BCMS適合性評価制度

事業継続マネジメントシステム（BCMS）のための制度です。BCMS認証取得によって対外的な信頼性が向上します。また認証審査を受審することによって、より有効なBCMSの構築・運用に向けた改善につなげることができます。
https://isms.jp/bcms.html

■ CSMS適合性評価制度

制御システムセキュリティマネジメントシステム（CSMS）のための制度です。CSMS認証取得によって、サイバー攻撃に対するリスクを低減し、IACS（産業用オートメーション及び制御システム）の運用担当者に対するセキュリティ管理策の行動指針を徹底することができます。
https://isms.jp/csms.html

一般社団法人 情報マネジメントシステム認定センター（ISMS-AC）

〒106-0032 東京都港区六本木一丁目9-9 六本木ファーストビル内
TEL 03-5860-7570　FAX 03-5573-0564
URL https://isms.jp/

文書番号：JIP-ISMS120-6.2 January 2020