

Information Security Management System

情報セキュリティマネジメントシステム
適合性評価制度の概要

JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応版



ISMS

JIPDEC

財団法人 日本情報処理開発協会

1 ISMS適合性評価制度の目的

ISMS (Information Security Management System) 適合性評価制度 (以下、ISMS制度という) は、国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度である。

ISMS制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としている。

2 ISMS規格の国際規格化及び国内規格化

情報セキュリティマネジメントの国際規格を制定している合同専門委員会ISO/IEC JTC1 (情報技術の委員会) / SC 27 (セキュリティ技術) は、2000年に国際規格ISO/IEC 17799:2000を発行した。その後、改訂作業を進め、2005年にISO/IEC 17799:2005を発行した。なお、この規格は2007年に規格番号が変更になり、ISO/IEC 27002となった。

ISO/IEC 17799:2000は、2002年に国内規格

JIS X 5080:2002として発行され、ISO/IEC 17799:2005は、2006年5月にJIS Q 27002:2006として発行された。

また、英国規格BS 7799-2:2002をベースにしたISMSの国際規格であるISO/IEC 27001:2005も上記委員会より2005年10月に発行された。この規格は2006年5月に国内規格JIS Q 27001:2006として発行された。

- ISO/IEC27002:2005 (Information technology - Code of practice for information security management: 情報技術—情報セキュリティマネジメントの実践のための規範) は、組織の情報セキュリティに責任を持つ人々に向けた効果的なISMSを実施するための規範 (ベストプラクティス—最良の慣行) をまとめた国際規格。ISO/IEC 27002:2005 (2007年7月変更) の旧規格番号はISO/IEC17799。
- BS 7799-2:2002 (Information security management systems - Specification with guidance for use: 情報セキュリティマネジメントシステム—仕様及び利用の手引) は、BS 7799の認証を取得するための英国規格。
- ISO/IEC 27001:2005 (Information technology-Security techniques-Information security management systems-Requirements: 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項) は、組織がISMSを構築するための要求事項をまとめた国際規格。

3 ISMS認証基準の推移

ISMS制度における認証のための基準 (以下、ISMS認証基準という) は、第三者である認証機関が本制度の認証を希望する組織の適合性を評価するための基準である。

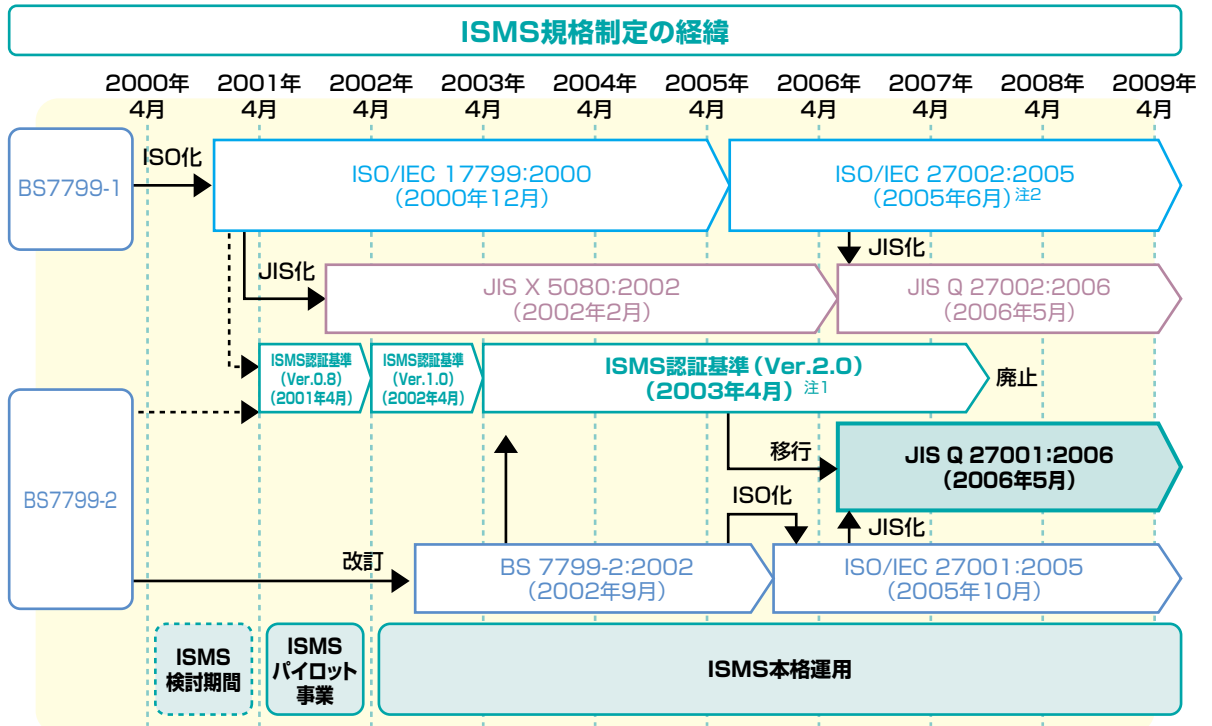
ISMS制度では、国際規格ISO/IEC 17799と英国規格BS7799-2を基にして、2001年4月にISMS認証基準 (Ver.0.8) を公表してパイロット事業を開始した。

その後2002年4月にISMS認証基準 (Ver.1.0) を公表し、これに基づいて本格運用を開始した。更に2002年9月のBS7799-2の改訂に伴い、2003年4

月にISMS認証基準 (Ver.2.0) に改訂し、これに基づいて運用してきた。

2005年10月にISMS認証基準として国際規格ISO/IEC 27001:2005が発行され、これにより国内規格JIS Q 27001:2006が発行されたため、ISMS認証基準をJIS Q 27001:2006とし、これに基づく認証を開始した。

移行計画に従い、2007年11月でJIS Q 27001:2006への移行を完了し、ISMS認証基準 (Ver.2.0) を廃止した。



備考：BSは英国規格、ISO/IECは国際規格、JISは国内規格、ISMS認証基準 (Ver.n) はJIPDEC規格。
 注1：ISMS認証基準 (Ver.2.0) は、BS 7799-2:2002をベースとし、用語、表現についてはJIS X 5080:2002との互換性を確保。
 注2：ISO/IEC 27002:2005 (2007年7月に変更) の旧規格番号は、ISO/IEC 17799。

4 ISMS認証取得の必要性

ISMS制度における認証を取得することは、組織の情報セキュリティ管理体制の整備や社内組織の体質強化につながるだけでなく、対外的にも情報セキュリティの信頼性を向上させることができ、国際的にもアピールすることができる。また、組織が取組

むべきリスクマネジメントを維持し、適切な管理策を実施することによって、情報セキュリティインシデントの発生可能性やインシデントが顕在化したときの損害を減らすことができ、企業価値の向上につながる。

ISMSを構築・運用するメリット

- 技術面及び人間系の運用・管理面の総合的なセキュリティ対策が実現できる。
 - 社員のスキル向上、責任の明確化、緊急事態の対処能力の向上など。
- 総合的マネジメントの視点から、効率的なセキュリティ対策が実施できる。
 - 費用対効果を考えた資産管理、リスクマネジメントの定着など。
 - 上記の活動を継続することにより、セキュリティ意識の向上などの効果が期待される。

ISMS認証を取得するメリット

- 対外的には、情報セキュリティの信頼性を確保できる。
 - 顧客や取引先からのセキュリティに関する要求事項の適合など。
- 内部的には、事業競争力の強化につながる。
 - 入札条件や電子商取引への参加の条件整備など。
 - 特定システムオペレーション企業等認定制度での申請時における必要条件となっている。

5 ISMS導入のポイント

ISMSとは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することである。組織が保護すべき情報資産について、機密性、完全

性、可用性をバランス良く維持し改善することがISMSの基本コンセプトである。ISMSでは、リスクアセスメントにより導入した管理策の有効性を測定することとなっている。

情報セキュリティの3要素（機密性、完全性、可用性）

JIS Q 13335-1:2006では、情報セキュリティの3要素を次のように定義している。

- 機密性：認可されていない個人、エンティティ(団体等)又はプロセスに対して、情報を使用不可又は非公開にする特性。
- 完全性：資産の正確さ及び完全さを保護する特性。
- 可用性：認可されたエンティティ(団体等)が要求したときに、アクセス及び使用が可能である特性。

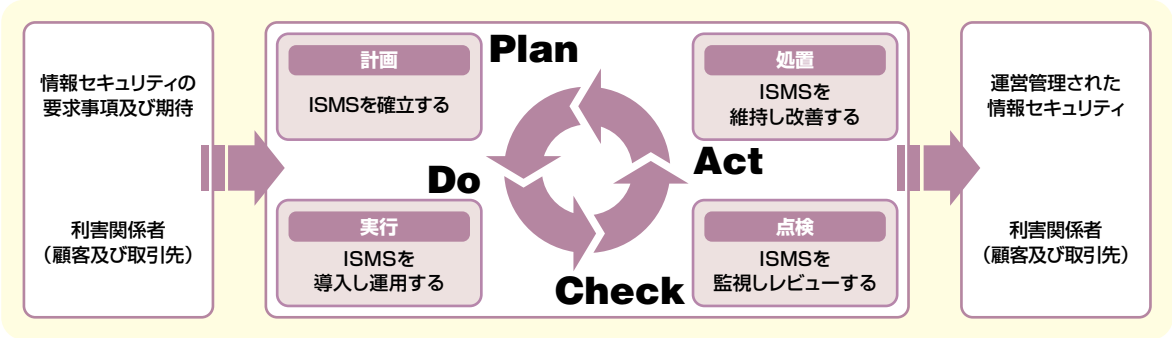
PDCAモデルによるプロセスアプローチ

組織は、ISMSを有効に機能させるために、多くの活動を明確にし、運営管理しなければならない。JIS Q 27001 (ISO/IEC 27001)では、組織においてISMSを確立、導入、運用、監視、レビュー、維持及び改善のために、プロセスアプローチを採用することを奨励している。

プロセスアプローチとは、インプットをアウトプットに変換することを可能にするために、経営資源を使用して運営管理されるあらゆる活動をプロセスとみなし、組織内のプロセスを明確にし相互作用させ、これら一連のプロセスをシステムとして適用して、運営管理することである。

プロセスアプローチを採用するメリットは、個々のプロセス間のつながりを管理し、プロセスの組合せや相互作用を管理することにより、ISMSを有効に機能させることができることである。

JIS Q 27001 (ISO/IEC 27001)では、情報セキュリティに関連するプロセスに対し、「Plan-Do-Check-Act (PDCA)」モデルを適用することで、「利害関係者の情報セキュリティ要求事項および期待」をインプットにこれらの要求事項および期待を満たす情報セキュリティの成果（運用管理された情報セキュリティ）をアウトプットとして生み出すプロセスを継続的に改善していくことがポイントである。



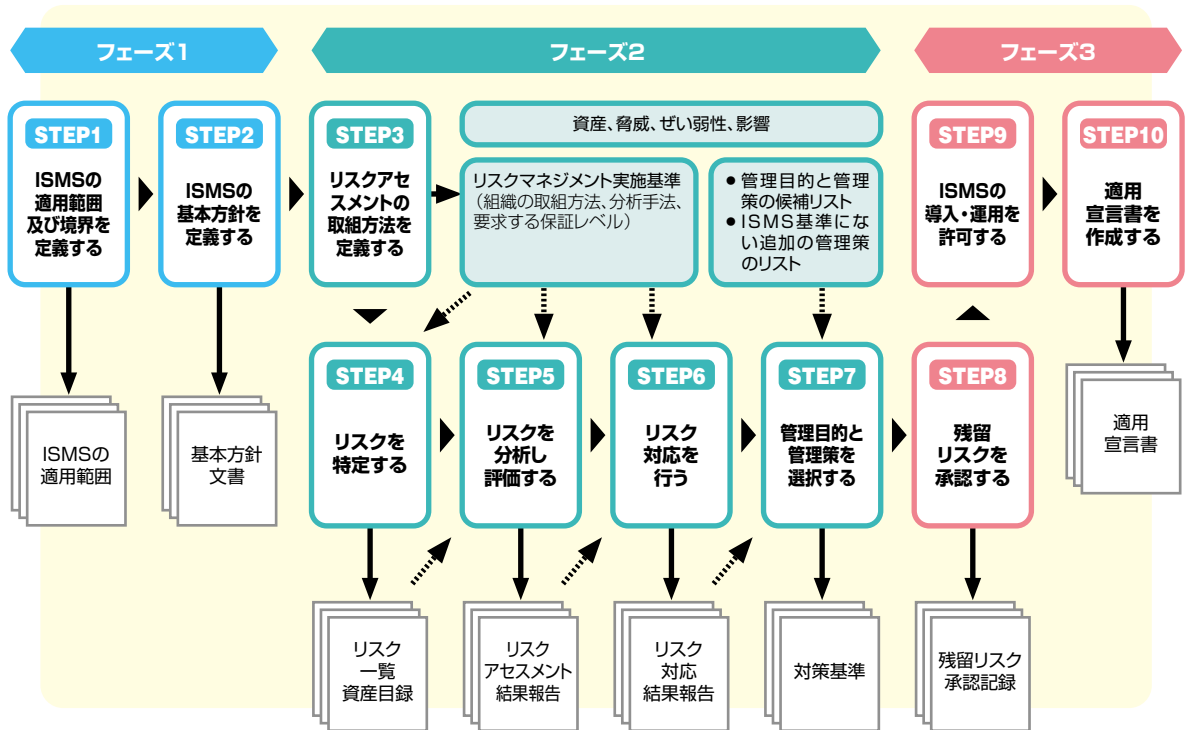
Plan-計画 (ISMSの確立)	組織の全般的な方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS基本方針、目的、プロセス及び手順を確立する。
Do-実行 (ISMSの導入及び運用)	ISMS基本方針、管理策、プロセス及び手順を導入し運用する。
Check-点検 (ISMSの監視及び見直し)	ISMS基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント(可能ならば測定)、及びその結果のレビューのために経営陣に報告する。
Act-処置 (ISMSの維持及び改善)	ISMSの継続的な改善を達成するための、ISMSの内部監査及びマネジメントレビューの結果、又はその他の関連情報に基づいた、是正処置及び予防処置を実施する。

6

ISMSの確立

ISMSの確立は、3つのフェーズに分けて考えることができる。

- フェーズ1：ISMSの適用範囲及び基本方針を確立する。(STEP1～STEP2)
- フェーズ2：リスクアセスメントに基づいて管理策の選択をする。(STEP3～STEP7)
- フェーズ3：リスクについて適切に対応する計画を策定する。(STEP8～STEP10)



フェーズ1: ISMSの適用範囲及び基本方針を確立する。(STEP1～STEP2)

ISMSの適用範囲及び境界は、事業・組織・所在地・資産及び技術の特徴の見地から定義する。ISMSの基本方針は、事業上及び法令又は規制の要求事項やリスクアセスメントなどから導かれる情報セキュリティに対する要求事項を考慮し、戦略的なリスクマネジメント状況、ISMSを確立し維持する組織環境、情報セキュリティの全般的な方向性及び行動指針を確立する。

フェーズ2: リスクアセスメントに基づいて管理策を選択する。(STEP3～STEP7)

決定したISMSの適用範囲・境界及び基本方針に基づき、リスクアセスメントの取組方法を特定する。リスクの特定では、保護すべき資産に対して機密性、完全性、可用性を喪失させる脅威、ぜい弱性及びそれらが事業に及ぼす潜在的な影響の大きさを特定する。リスクアセスメントでは、セキュリティ障害による事業上の損害及び発生可能性を評価した結果でリスクのレベルを算定し、リスク受容基準を使用して、そのリスクが受容できるか、リスク対応が必要かどうか判定する。リスクを受容できない場合、リスク対応として、管理策の適用、リスク受容、リスク回避、リスク移転の選択をする。リスク対応の結論に従って、附属書A「管理目的及び管理策」の表から、適切な管理目的と管理策を選択する。また、組織の必要に応じて追加の管理目的と管理策を採用することもできる。

フェーズ3: リスクについて適切に対応する計画を策定する。(STEP8～STEP10)

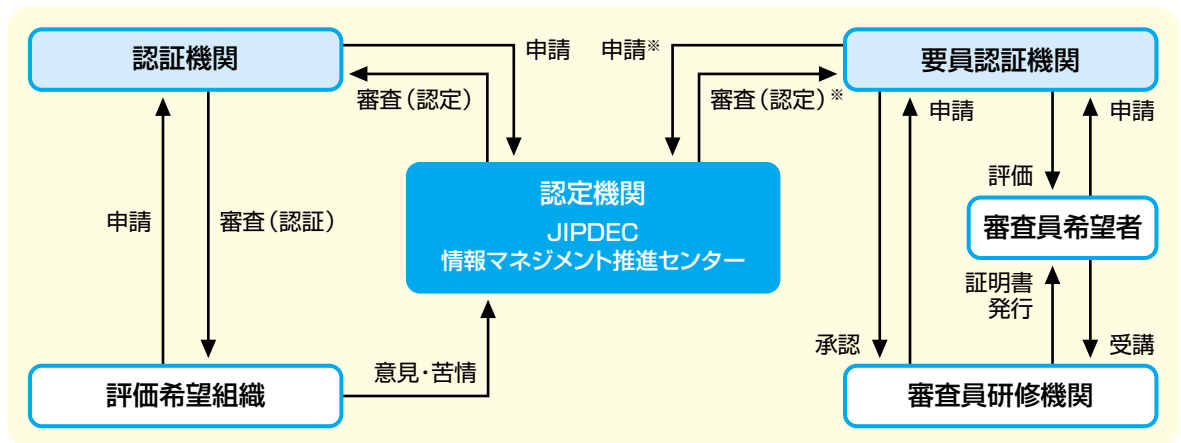
経営陣は、選択した管理目的及び管理策についての残留リスクを承認し、ISMSを実施する許可を与える。選択した管理目的及び管理策並びに選択の理由と除外の理由を記載した適用宣言書を作成する。

7

ISMS適合性評価制度の運用

ISMS適合性評価制度は、組織が構築したISMSがJIS Q 27001 (ISO/IEC 27001)に適合しているか審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれら各機関がその

業務を行う能力を備えているかをみる「認定機関」からなる総合的な仕組みである。なお、審査員になるために必要な研修を実施する「審査員研修機関」は要員認証機関が承認する。



※2008年に実施予定

ISMS制度の運用体制

■ 認定機関: (財)日本情報処理開発協会 (JIPDEC) 情報マネジメント推進センター

- ISMS適合性評価制度の運用と維持管理を行う。
- 認証機関の認定と定期的なサーベイランス、3年または4年毎の更新審査を実施する。
- 要員認証機関の認定*と定期的なサーベイランス、3年毎の更新審査を実施する。
- ISMS適合性評価制度に関する情報を提供する。
- ISMS適合性評価制度に関する意見や苦情等の受付を行う。

■ 認証機関

- ISMS認証機関認定基準及び指針に基づいて、認定を受ける。
- ISMS認証基準により、評価希望組織の認証・登録を行う。
- 登録した組織の定期的なサーベイランス、3年毎の更新審査を実施する。

■ 評価希望組織: ISMS認証取得を希望する組織

- ISMSの適用範囲及び基本方針を定義する。
- 認証機関を選択し申請する。
- ISMS認証基準に適合しているかどうかの審査 (Stage 1、Stage 2) を受け、審査結果に基づき認証登録される。
- 登録された場合、認定シンボルを認証機関のマークとともに商業文書等に使用できる。

■ 要員認証機関

- ISMS審査員資格基準に基づいて、ISMS審査員 (審査員補、審査員、主任審査員) を評価・登録する。
- 登録したISMS審査員の1年毎の維持手続きと、3年毎の更新登録の評価を実施する。

備考: ISO/IEC 17021 対応により下記用語を使用しているが、() 内の従来の用語を使用する場合がある。
組織 (事業者)、認証機関 (審査登録機関)、要員認証機関 (審査員評価登録機関)

ISMS制度の公平性・透明性・客観性の確保

ISMS適合性評価制度の運営については、その公平性・透明性及び客観性を確保するために、JIPDEC 組織運営機構の中に学識経験者及び業界団体の有識者等から構成される運営委員会及びその下部

組織である技術専門部会を設置している。これらの詳細は、URL: <http://www.isms.jipdec.jp/org/> を参照のこと。

ISMS制度の基準・規定・手順・ガイド等

JIS Q 27001 (ISO/IEC 27001) (ISMS認証基準)	第三者である認証機関が本制度の認証を希望する組織の適合性を評価するための認証基準である。
ISMSユーザーズガイド	JIS Q 27001の要求事項について一定の範囲でその意味するところを説明しているガイドである。
ISMSユーザーズガイド —リスクマネジメント編—	リスクマネジメント編はISMSユーザーズガイドを補足し、リスクマネジメント、とりわけリスクアセスメント及びその結果に基づくリスク対応についての理解を深めるために必要な事項について、例を挙げて解説している。
医療機関向けISMSユーザーズガイド	ISMSユーザーズガイドの医療機関向け版で、医療機関におけるISMSの理解を深めるためのガイドである。
法規適合性に関する ISMSユーザーズガイド	企業がリスクマネジメントを実施する上で、企業の法的リスクを考慮することは重要であり、とりわけ個人情報保護に対応する手段としてISMSの枠組みは極めて有効である。 本書はISMSの枠組みが法的及び規制要求事項に適合させる仕組みであることを理解するためのガイドである。
クレジット産業向け ISMSユーザーズガイド	ISMSユーザーズガイドのクレジット産業向け版で、クレジット産業におけるISMS構築を主眼として、関連する規範とISMS認証基準とのマッピングを示し、ISMSを構築することがこれらの規範を順守する上で非常に有効な手段であることを示したガイドである。
外部委託における ISMS適合性評価制度の活用方法	組織又は企業において情報処理業務の一部又は全てを外部委託する場合に、情報セキュリティ責任者及び担当者が委託先の選定にISMS適合性評価制度を活用するためのガイドである。
ISMS認証機関認定基準及び指針	認証機関の認定審査及び登録を行う際の認定基準及び指針であり、ISO/IEC 27006 (ISO/IEC 17021を含む)に基づいている。
IMS認証機関認定の手順 IMS認証機関認定の手引き	手順は認証機関が認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務について規定したもの、手引きは、申請から登録までと登録維持の標準的な流れと条件を示したものである。
ISMS審査員資格基準	各審査員(審査員補、審査員、主任審査員)についての資格基準を規定したものである。
IMS認定シンボル使用規定	認定シンボルを使用する場合の、認定シンボルの表示及び適用条件等について規定したものである。

備考：上記の他、ISMS適合性評価制度の普及促進のための文書として構築事例集や、認証基準相互の比較表などがある。

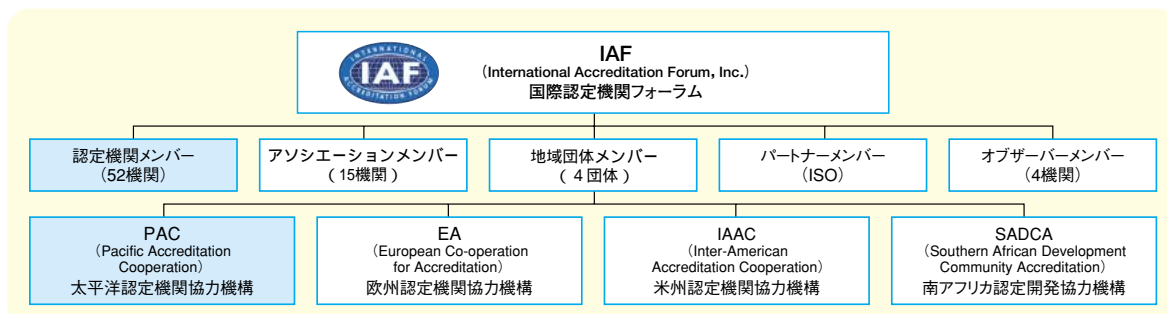
8

IAF (国際認定機関フォーラム) への加盟

IAF (International Accreditation Forum, Inc.) は、マネジメントシステム、製品、サービス、要員等の適合性評価プログラムに関わる、適合性評価認定機関及び関連する機関によって構成され、現在約50の認定機関メンバーを中心に、地域団体メンバー (PAC、EA、IAAC、SADCA)、アソシエーションメンバー (審査機関の協議会等、各国の産業団体)、パートナーメンバー、オブザーバーメンバーの、総勢70以上の機関が加盟している。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、また国際規格に則して認定機関の能力を確実なものとし、認定された認証の信頼性及び有効性を向上させることによって、事業者及びエンドユーザーのリスクを低減することである。また、「Certified once, accepted everywhere」

をモットーに国際相互承認を推進し、その結果経済地域間の技術的貿易障壁を除去することにより貿易の促進を目指している。IAFの国際相互承認協定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がその信頼性を保証することにより世界中の顧客から信頼を得ることができる。JIPDEC情報マネジメント推進センターは、第21回IAF/ILAC年次総会において正式にマネジメントシステムの認定機関メンバーとして加盟を承認された。なお、アジア太平洋地域におけるIAFの下部組織であるPACについては、第14回PAC年次総会においてフルメンバー (正会員) として既に加盟を承認されている。

今後はISMSの国際相互承認の体制作りに向けて、積極的に国際貢献していく考えである。



2008年1月現在



本シンボルは、情報やセキュリティは人によって守られることをイメージしています。

● ISMS制度に関する問合せ先 ●

〒105-0011 東京都港区芝公園3-5-8 機械振興会館内
財団法人 日本情報処理開発協会 情報マネジメント推進センター

TEL 03-3432-9386 FAX 03-3432-6200

URL <http://www.isms.jipdec.jp/>

文書番号：JIP-ISMS120-4.0



財団法人 日本情報処理開発協会

〒105-0011 東京都港区芝公園3丁目5番8号 機械振興会館内

TEL 03-3432-9371 FAX 03-3432-9379

URL <http://www.jipdec.or.jp/>



古紙/OLP配合率100%再生紙を使用
発行年月 2008年1月