



● ISMSに関する情報 (JIPDEC) ●

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



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 03-3432-9386 FAX 03-3432-6200

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



ISMS

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

財団法人 日本情報処理開発協会

1 ISMS適合性評価制度創設の趣旨

情報セキュリティマネジメントシステム（Information Security Management System：以下ISMSという）適合性評価制度は、国際的に整合性のとれた情報システムのセキュリティ管理に対する第三者適合性評価制度である。本制度の創設により、わが国の情報セキュリティレベル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。

2 ISMS適合性評価制度の目的

インターネットの急速な普及を背景に、グローバルなネットビジネスが活況を呈しているが、このようなインターネット利用の高度化は、従来に比べ大いに利便性をもたらすと同時に外部ネットワークからの不正アクセス等による被害を発生させる可能性を増大させた。

ネットビジネスにおける取引の安全性、信頼性を確保するためには、国際的にも信頼を得ることができる情報セキュリティ対策を実施することが重要となっている。特に情報セキュリティ対策を有効なものとするためには、技術的なセキュリティ対策だけでは完全に防ぐことは困難であり、人間系の運用・管理面のセキュリティ対策などマネジメントに対する視点から問題を解決する必要がある。

国際的には、「ISO/IEC TR 13335 (GMITS: Guidelines for the Management of IT Security)」や「ISO/IEC 17799 (Code of practice for information security management)」等の情報セキュリティ管理に対する普遍的、包括的なガイドがあり、わが国においても国際標準を踏まえつつ積極的に情報セキュリティ管理を確立する必要がある。

このような状況から、情報セキュリティ管理に関する国際標準化動向を勘案し、わが国はもとより国際的にも信頼を得られる情報システムのセキュリティ管理に対する第三者適合性評価制度を確立し、わが国の情報セキュリティレベル全体の向上を図ることを目的とする。

3 ISMS適合性評価制度について

ISMS適合性評価制度が立脚する規格は、「JIS X 5080:2002 (ISO/IEC 17799:2000) 情報セキュリティマネジメントの実践のための規範」であり、この規格は、組織の規模を問わず情報資産を保護する必要がある場合の情報セキュリティの範囲を明確にする際の枠組みや規範、基準になるべき考え方等をまとめたものであり、情報セキュリティマネジメントに対する普遍的、包括的なガイドを示している。

ISMS制度の概要（対象範囲）

ISMS制度の本格運用ではパイロット事業での対象範囲の制限を外し、業種・業務区分の仕組みを導入することとする。但し、当面は情報技術関連分野（情報処理サービス業を含む）と、それ以外の分野に分け、審査・登録を行う。将来的には、審査・登録の業種・業務区分を明確にしていく。

1 適用する業種・業務区分

「経済活動に関する統計的分類基準」（NACE Rev.1）に基づく業種・業務区分を適用する。

2 背景

以下の理由によりISMSでも業種・業務区分の仕組みを導入する。

① 他のマネジメントシステムとの整合性を確保する。

ISO 9000sやISO 14000s等のマネジメントシステムでは、NACE Rev.1に基づいて審査登録機関の認定・登録、審査員の登録、事業者の審査・登録等を実施している。

② ISMSの対象とする業種範囲が広範である。

ISMSは、情報システム、情報処理関連の業種だけでなく、全ての業種を対象に情報セキュリティに関するマネジメントシステムの認証を行うことが可能である。一方、情報の管理は業務に密着しており、情報資産の洗い出しやリスク評価等に関して審査するには、高度な専門性を有する必要がある。

3 適用方法

評価希望事業者が、原則として適用範囲を考慮した業種・業務区分を申請し審査登録機関とで調整する。審査登録機関、審査員については、それぞれ審査登録機関認定の手順、審査員登録の手順に基づいて適用する。

ISMS制度 基準・規程・手順・ガイド等

ISMS認証基準	JIS X 5080 (国際規格ISO/IEC 17799 : 2000) 及び英国規格BS7799-2 :1999 (Specification for information security management systems) を参照し、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価するための基準。
ISMSガイド	ISMS認証基準に沿って、解説、例示等を含んで構成されており、審査業務を実施する上での参考ガイド。なお、本書内の例示はあくまでも審査のイメージを伝えることを目的としており審査方法を規定するものではない。
ISMS審査登録機関認定基準	審査登録機関の認定審査及び登録を行う際の認定基準。
ISMS審査登録機関認定の手順	審査登録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。
ISMS審査員研修機関認定基準	審査員向けの研修を行う研修機関の認定審査及び登録を行う際の認定基準。
ISMS審査員研修コース基準	審査員研修コースの内容について、その要求事項等を定めた研修コースの基準。
ISMS審査員研修機関認定の手順	ISMS審査員研修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。
ISMS審査員の資格要件	各審査員（審査員補、審査員、主任審査員）についての資格要件を規定したもの。
ISMS審査員登録の手順	各審査員の資格要件に基づいて評価登録する際の手順を規定したもの。
ISMS認定マーク使用規程	ISMS認定マークを使用する場合の、ISMS認定マークの表示及び適用条件等について規定したもの。

4 ISMSとは

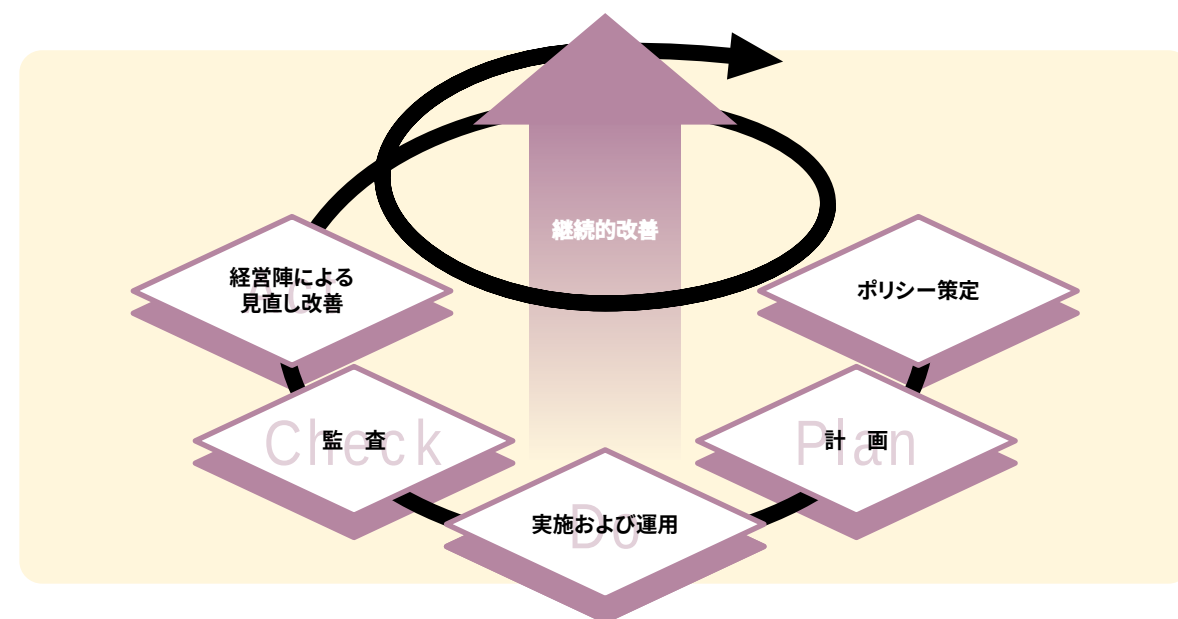
情報セキュリティの問題として、インターネット上のホームページ改ざん、ハードウェア／ソフトウェアのトラブルや関係者による情報の漏洩などが存在しており、それら個別の技術対策は様々であり、それぞれのレベルで実施されていると思われる。

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、自らのリスク評価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情報セキュリティマネジメントシステム(ISMS)の要求する主要なコンセプトである。

- 機密性: アクセスを認可された者だけが、情報にアクセスできることを確実にすること。
- 完全性: 情報および処理方法が正確であること及び完全であることを保護すること。
- 可用性: 認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

5 ISMSのポイント

PDCAサイクルによるスパイラルアップ



作成したポリシー(方針)を基に

- Plan : 情報セキュリティ対策の具体的計画、方針を策定する。
- Do : 計画に基づいて対策の実施・運用を行う。
- Check: 実施した結果の監査を行う。
- Act : 経営陣による見直しを行い、改善する。

このサイクルを継続的に繰り返し、情報セキュリティレベルの向上を図る。

6 マネジメント枠組みの確立

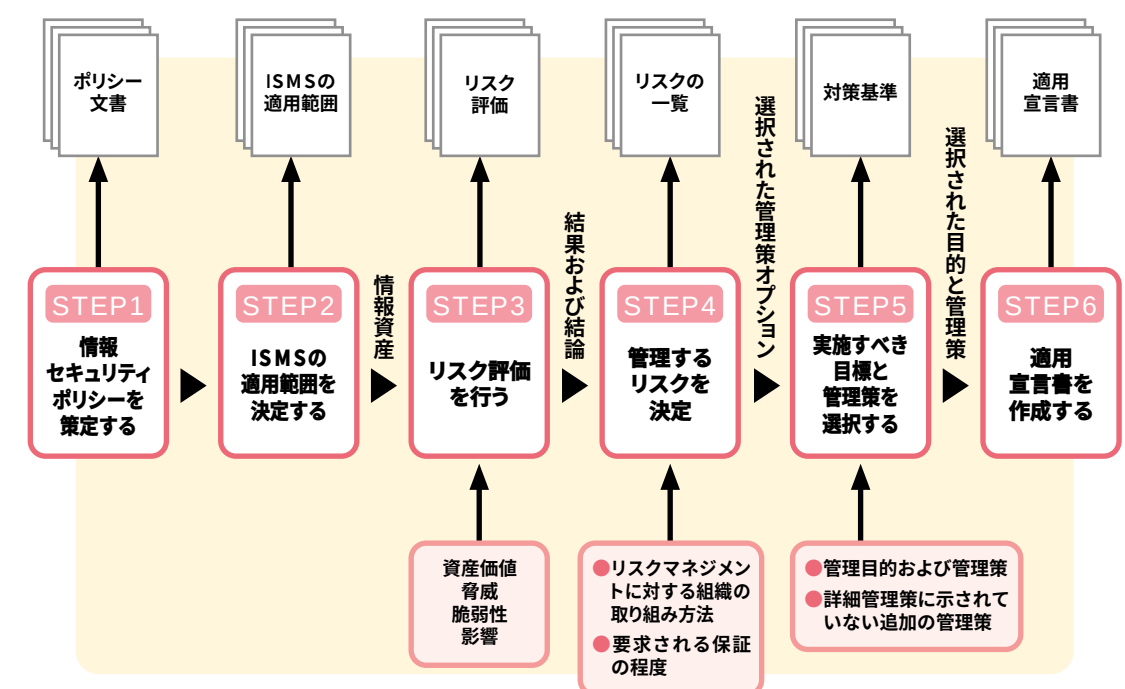
1 マネジメント枠組みに関するISMSの要求事項は、情報セキュリティポリシー、管理目的、管理策、システム運用(実施)、さらには情報セキュリティポリシー文書をはじめとするシステム文書、文書管理及び記録管理に関するものである。

2 この枠組みの確立にあたり情報セキュリティポリシーを策定し(STEP1)、その中でISMSの適用範囲を決定する(STEP2)。策定した情報セキュリティポリシーに基づきリスク評価を実施する(STEP3)。枠組みのもとで管理するリスクを決定する(STEP4)。最適なリスク評価にもとづき、実施すべき管理策を選択する(STEP5)。

ISMS認証基準 詳細管理策(要約)

- | | |
|-----------------|------------------|
| ●セキュリティポリシー | ●通信及び運用管理 |
| ●セキュリティ組織 | ●アクセス制御 |
| ●情報資産の分類及び管理 | ●システムの開発及びメンテナンス |
| ●人的セキュリティ | ●事業継続管理 |
| ●物理的及び環境的セキュリティ | ●準拠 |

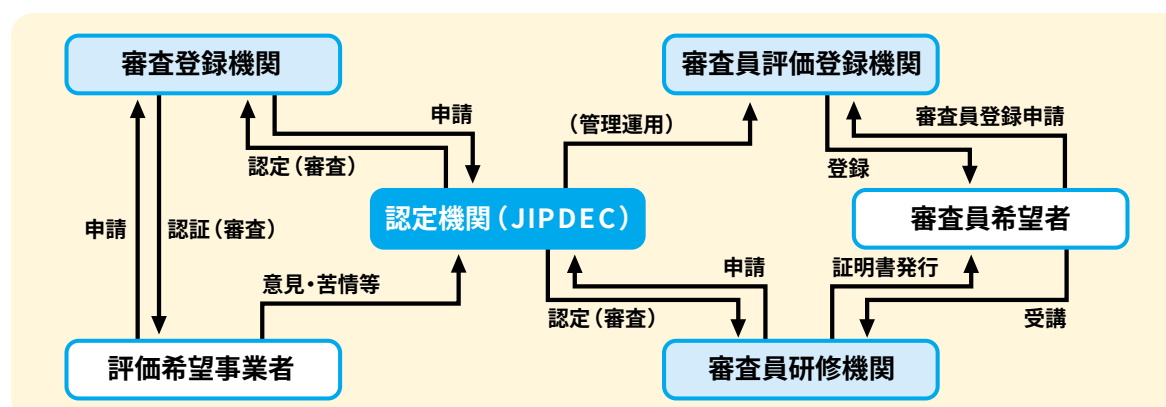
3 「詳細管理策」にある全ての管理策が実施されなければならないわけではなく、リスク評価および要求されるシステムの保証の度合いに基づき管理策を選択して実施できる。特に重要なことは、この選択については適用宣言書で明確に公表する(STEP6)ことにある。また、上記の管理策だけでなく、組織がリスク評価やリスクマネジメントなどを通じて、必要と思われるより良い管理策を追加することができる。





7 ISMS適合性評価制度の運用について

ISMS制度運用体制



■ 認定機関：(財)日本情報処理開発協会（JIPDEC）

- ISMS適合性評価制度の運用と維持管理。
- 審査登録機関の認定と定期的なサーベイランス、3年に1回の更新審査を実施。
- 審査員研修機関の認定と定期的なサーベイランス、3年に1回の更新審査を実施。
- 審査員評価登録機関の管理運用。
- 審査登録、その他制度に対する問い合わせ窓口。

■ 審査登録機関

- ISMS審査登録機関認定基準に基づき、認定機関（JIPDEC）の認定審査を受け、定期的なサーベイランスと、3年に1回の更新審査を受ける。
- ISMS認証基準により、評価希望事業者を審査・登録を行う。
- 登録した事業者の定期的なサーベイランス、3年に1回の更新審査を行う。

■ 評価希望事業者

- 評価希望事業者（ISMS認証取得を希望する事業者）は、申請適用範囲のISMSを確立する。
- 審査登録機関の選択と申請（審査依頼）。
- ISMS認証基準に適合しているか否かについて本審査（Stage1、Stage2）を受審する。
- 審査結果に基づき認証・登録される。
- 登録された場合、ロゴマークを商業文書に使用することが可能。

■ 審査員研修機関

- ISMS審査員研修機関認定基準、ISMS審査員研修コース基準に基づき、認定機関（JIPDEC）の認定審査を受け、定期的なサーベイランスと、3年に1回の更新審査を受ける。
- 審査員を養成するため、情報セキュリティマネジメントシステムに関する研修・試験を行う。
- 受講者の観察評価、試験結果を総合的に判断し、可否を判定する。

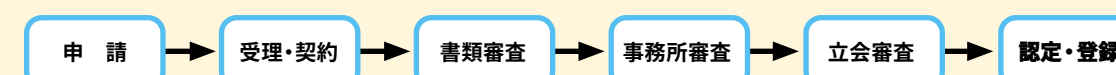
■ 審査員評価登録機関

- ISMS審査員の評価・登録を行う。
- ISMS審査員（審査員補、審査員、主任審査員）の資格要件に基づき評価・登録する。
- 審査員補、審査員及び主任審査員の登録の有効期限は3年間で、3年毎に再登録のための評価を受ける。

※認定されたISMS審査員研修の合格証明書が有効である。

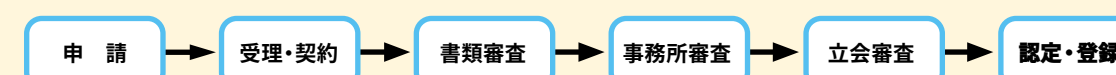
ISMS適合性評価制度は、組織が構築したISMSが要求事項に合致しているか審査し登録する「審査登録機関」、その審査員になるために必要な研修を実施する「審査員研修機関」及び審査員の資格を付与する「審査員評価登録機関」、そしてこれら各機関がその業務を行う能力を備えているかをみる「認定機関：(財)日本情報処理開発協会（JIPDEC）」からなる総合的な仕組みである。

審査登録機関の認定の流れ



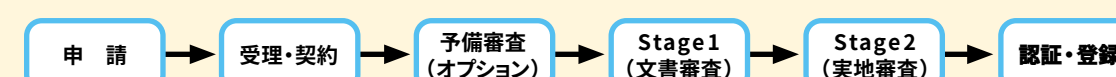
- 認定審査に用いられる基準は、ISMS審査登録機関認定基準。
- 申請時に必要な条件や手順はISMS審査登録機関認定の手順に示す。
- 各審査項目においては是正が必要な指摘事項があった場合には、その是正処置または必要に応じて是正計画を提出し、妥当性が確認された後に認定取得となる。
- 認定を受けた審査登録機関の情報はJIPDECまでお問い合わせください。

審査員研修機関の認定の流れ



- 認定審査に用いられる基準は、ISMS審査員研修機関認定基準。
- 申請時に必要な条件や手順はISMS審査員研修機関認定の手順に示す。
- 各審査項目においては是正が必要な指摘事項があった場合には、その是正処置または必要に応じて是正計画を提出し、妥当性が確認された後に認定取得となる。
- 認定を受けた審査員研修機関の情報はJIPDECまでお問い合わせください。

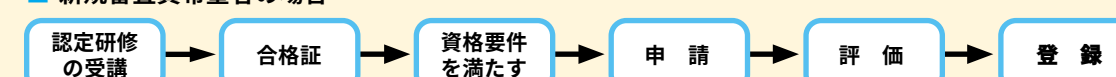
評価希望事業者の認証・登録の流れ



- 認証審査に用いられる基準は、ISMS認証基準。
- 申請時に必要な条件や審査手順は各審査登録機関により異なる場合がある。
- ISMS認証審査・登録に関する詳細は各審査登録機関にお問い合わせください。

審査員評価登録の流れ

■ 新規審査員希望者の場合



■ 既に審査員補、審査員の場合（資格の変更）



- 認定審査に用いられる基準は、ISMS審査員資格要件。
- 申請時に必要な条件や評価手順はISMS審査員登録の手順に示す。