登録第4605292号

ISMSロゴマークは、情報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　ISMS制度推進室
TEL　03-3432-9386　FAX　03-3432-6200
URL　http://www.isms.jipdec.jp/
E-MAIL　info@isms.jipdec.jp

文書番号：JIP-ISMS120-3.2

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.jp/

古紙パルプ配合率100%再生紙を使用
発行年月　2006年3月

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

ISO/IEC 27001:2005　対応版

ISMS

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国際規格化

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6月に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となる予定である。

ISO/IEC 17799:2000は、2002年に国内規格JIS X 5080:2002として発行されている。ISO/IEC 7799:2005は、2006年にJIS Q 27002:2006として発行される予定である。

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年に国内規格JIS Q 27001:2006として発行される予定である。

- ISO/IEC 17799:2005（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。
- 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（ISO/IEC 27001）

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。

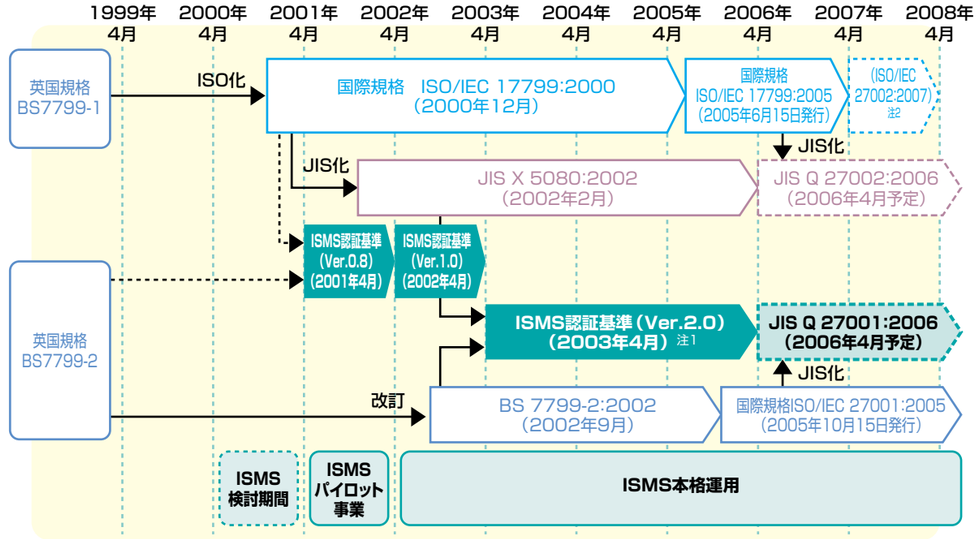
ISMS制度では、国際規格ISO/IEC 17799と英国規格BS7799-2を基にして、2001年4月にISMS認証基準（Ver.0.8）を公表してパイロット事業を開始した。

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が発行されたため、今後はこの規格に移行することとした。具体的には、国内規格JIS Q 27001:2006が発行され次第、JIS Q 27001:2006をISMS認証基準とし、これに基づく認証を開始する。

移行計画では、2007年10月（JIS Q 27001:2006が発行されてから18ヶ月後）までに移行を完了し、その時点でISMS認証基準（Ver.2.0）を廃止するものとする。

ISO規格及びJIS規格制定の経緯

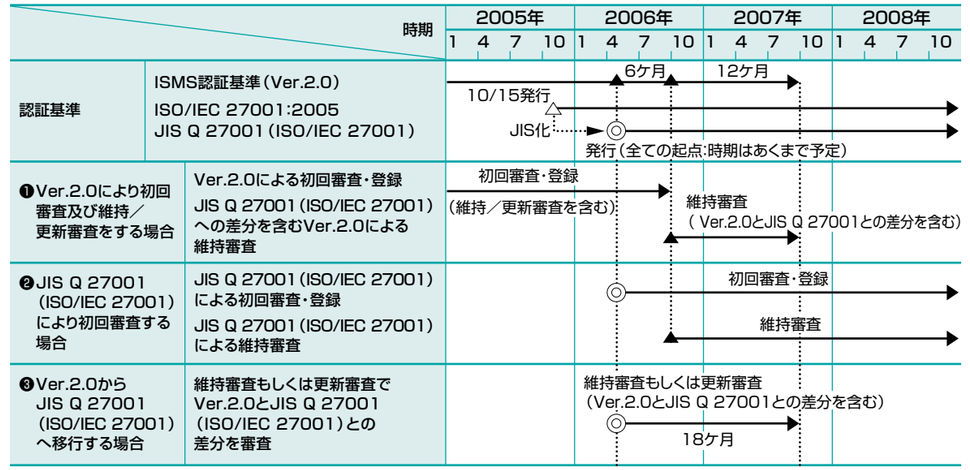


注1:ISMS認証基準（Ver.2.0）は、英国規格BS 7799-2:2002をベースとし、用語、表現についてはJIS X 5080:2002との互換性を確保。
注2:国際規格ISO/IEC 17799:2005の規格番号は、ISO/IEC 27002となる予定（2007年）。
注3:点線部分は、2006年2月時点での予測。
注4:JIS Q 27001の規格名は想定。

4 移行計画

移行計画の起点は、国内規格JIS Q 27001（ISO/IEC 27001と一致している）が発行された時点である。JIS発行日から18ヶ月間で移行を完了させる。ISO/IEC 27001への移行時のケースとしては、❶Ver.2.0により初回審査及び維持／更新審査をする場合、❷JIS Q 27001（ISO/IEC 27001）により初回審査をする場合、❸Ver.2.0からJIS Q 27001（ISO/IEC 27001）へ維持／更新審査により移行する場合がある。

ISO/IEC 27001への移行計画



注1:図中の▲◎の時期は、2006年2月時点での予測。
注2: "Ver.2.0" は "ISMS認証基準（Ver.2.0）" を示す。
注3:JIS Q 27001の規格名は想定。

5 ISMS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が可能となっている。

情報セキュリティの3要素（機密性、完全性、可用性）

ISO/IEC 13335-1:2004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。

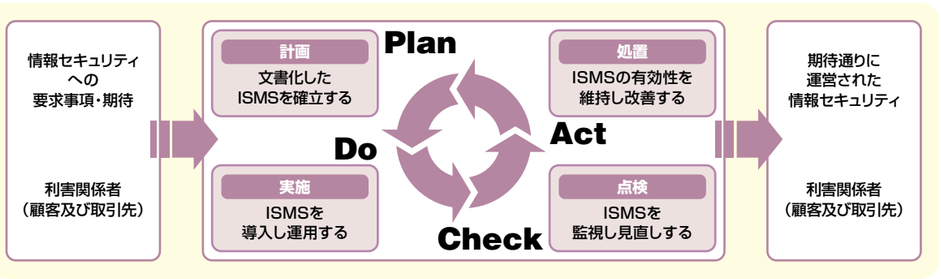
PDCAモデルによるプロセスアプローチ

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。ISO/IEC 27001では、組織においてISMSを確立、導入、運用、監視、維持し、かつそのISMSの有効性を改善する際に、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、その相互関係を把握し、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。

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。

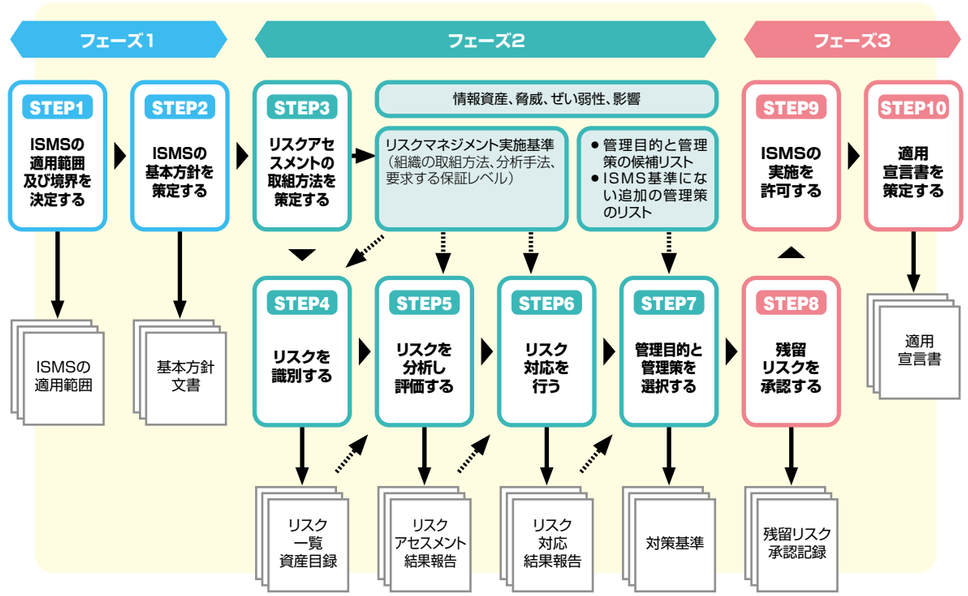


Plan−計画（ISMSの確立）	組織の全般的な基本方針及び目的に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連するISMS基本方針、目的、プロセス及び手順を確立する。
Do−実施（ISMSの導入及び運用）	そのISMS基本方針、管理策、プロセス及び手順を導入し運用する。
Check−点検（ISMSの監視及び見直し）	ISMS基本方針、目的及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。
Act−処置（ISMSの維持及び改善）	ISMSの継続的な改善を達成するために、ISMSの内部監査及びマネジメントレビューの結果やその他関連情報に基づいて是正処置及び予防処置を講ずる。

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の適用範囲は、事業、組織、その所在地、資産及び技術の各特徴の観点から定義する。ISMSの基本方針は、事業上及び法的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、リスクマネジメント環境、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の選択をする。（STEP3〜STEP7）

決定したISMSの適用範囲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策定する。リスクの識別では、保護すべき情報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識別する。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度合いを算定し、リスクの評価基準を使用してリスクの受容ができるか、リスク対応が必要かどうか判定する。リスクの受容ができない場合、リスク対応として、管理策の採用、リスク保有、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」のリストから、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。

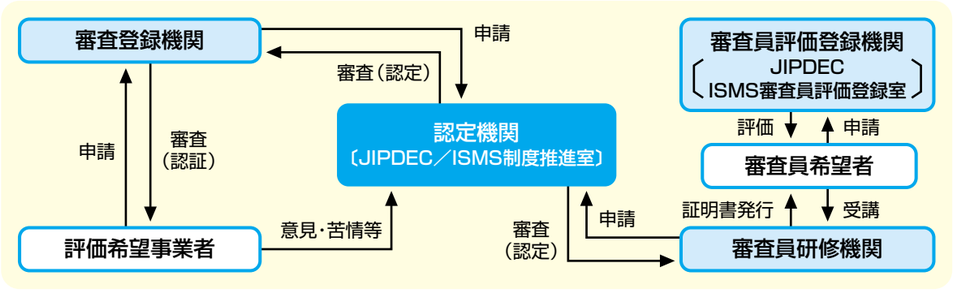
フェーズ3：リスクについて適切に対応する計画を策定する。（STEP8〜STEP10）

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ISO/IEC 27001に適合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」からなる総合的な仕組みである。

今後は、認定機関の認定システムに関する国際規格ISO/IEC 17011:2004及びISO/IEC 17024:2003に適合させるため、審査員評価登録機関業務、審査員研修機関の認定業務を別法人に移管するなど新しい体制への移行を予定している。



ISMS制度の運用体制

■ 認定機関：（財）日本情報処理開発協会（JIPDEC）ISMS制度推進室

- ISMS適合性評価制度の運用と維持管理を行う。
- 審査登録機関の認定と定期的なサーベイランス、3年又は4年毎の更新審査を実施する。
- 審査員研修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。(注)
- 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。

■ 審査登録機関

- ISMS審査登録機関認定基準に基づいて、認定を受ける。
- ISMS認証基準により、評価希望事業者の審査・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年毎の更新審査を行う。

■ 評価希望事業者：ISMS認証取得を希望する事業者

- ISMSの適用範囲及び基本方針を確立する。
- 審査登録機関を選択し申請する。
- ISO/IEC 27001に適合しているかどうか審査（Stage1、Stage2）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、ロゴマークを商業文書に使用することができる。

■ 審査員研修機関(注)

- 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いて、認定を受ける。
- 審査員を養成するため、ISMS審査員研修を実施する。
- 受講者の観察評価、最終試験の結果を総合的に判断し、合否を判定する。

■ 審査員評価登録機関：（財）日本情報処理開発協会（JIPDEC）ISMS審査員評価登録室(注)

- 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。
- ISMS審査員の登録の有効期限は3年間で、3年毎に再登録の評価を実施する。

（注）今後の新しい体制では、別法人に移管する予定。

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。これら委員会活動の詳細は、URL：http://www.isms.jipdec.jp/comm/ を参照のこと。

ISMS制度の基準・規程・手順・ガイド等

ISO/IEC 27001 （ISMS認証基準）	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認証基準である。
ISMSユーザーズガイド	ISMS認証基準（Ver.2.0）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―	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り、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。
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である。
ISMS審査登録機関認定基準に関する指針	ISMS審査登録機関認定基準の要求事項に適用する指針で、EA-7/03に基づいた基準である。
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審査登録機関認定の手引	手引は、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。
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である。
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審査員研修機関認定の手引	手引は、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。
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認定基準である。
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。
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。

備考：上記の他、ISMS適合性評価制度の普及促進のためのガイド等がある。例えば、ISMSを構築するためのポイントを分かり易く説明した解説書や、ISMS認証基準の考え方等を説明した解説書などである。

8 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、リスクの発生可能性やリスク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げることができる。

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満足など。

●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。