説明資料2－2

# ISMS適合性評価制度の概要

一般財団法人日本情報経済社会推進協会
情報マネジメント推進センター
副センター長　高取　敏夫

2011年9月7日

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

# ISMS適合性評価制度とは

ISMS（Information Security Management System）適合性評価制度（以下、本制度という）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認証制度である。

本制度は、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。

# ISMS適合性評価制度における適合基準


ISO/IEC 17011（JIS Q 17011）
（適合性評価－適合性評価機関の認定を行う機関に対する一般要求事項：
Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies）

ISO/IEC 27006（JIS Q 27006）
（情報技術－セキュリティ技術－ISMSの審査及び認証を行う機関に対する要求事項：
Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems）

ISO/IEC 27001(JIS Q 27001)
（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：
Information technology–Security techniques–Information security management systems–Requirements）

# ISO/IEC 27001の構成

0．1　序文

1　適用範囲　　2　引用規格　　3用語及び定義

4　情報セキュリティマネジメントシステム

- 4．1　一般要求事項
- 4．2　ISMSの確立及び運営管理
- 4．2．1　ISMSの確立
- 4．2．2　ISMSの導入及び運用
- 4．2．3　ISMSの監視及び見直し
- 4．3　文書化に関する要求事項
- 4．3．1　一般
- 4．3．2　文書管理
- 4．3．3　記録の管理
- 4．3．4　ISMSの維持及び管理

5　経営陣の責任

- 5．1　経営陣のコミット
- 5．2　経営資源の運用管理
- 5．2．1　経営資源の提供
- 5．2．2　教育・訓練、意識向上及び力量

6　ISMS内部監査
7　ISMSマネジメントレビュー

- 7．1　一般
- 7．2　レビューへのインプット
- 7．3　レビューからのアウトプット

8　ISMSの改善

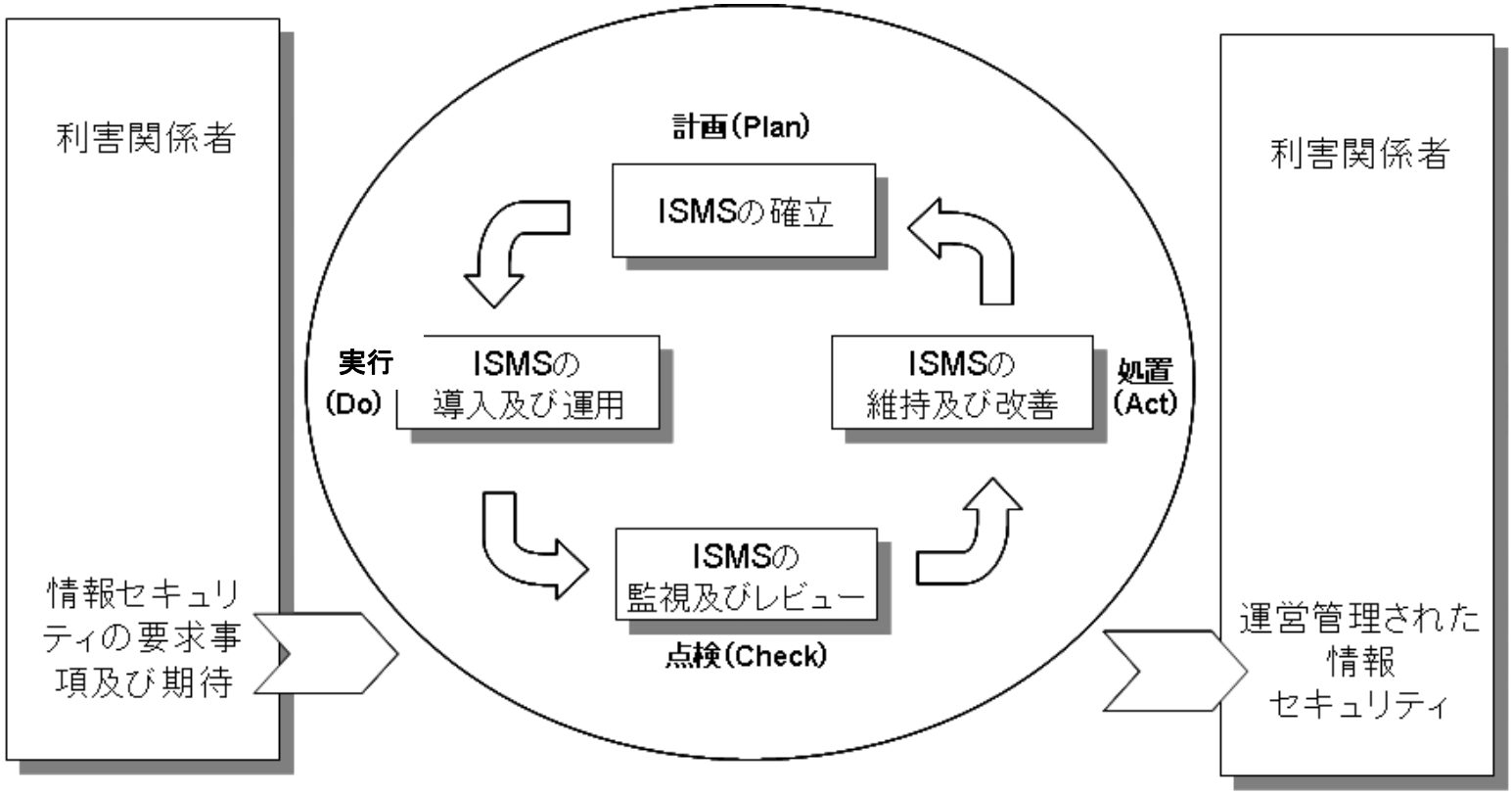
- 8．1　継続的改善
- 8．2　是正処置
- 8．3　予防処置

附属書A（規定）管理目的及び管理策

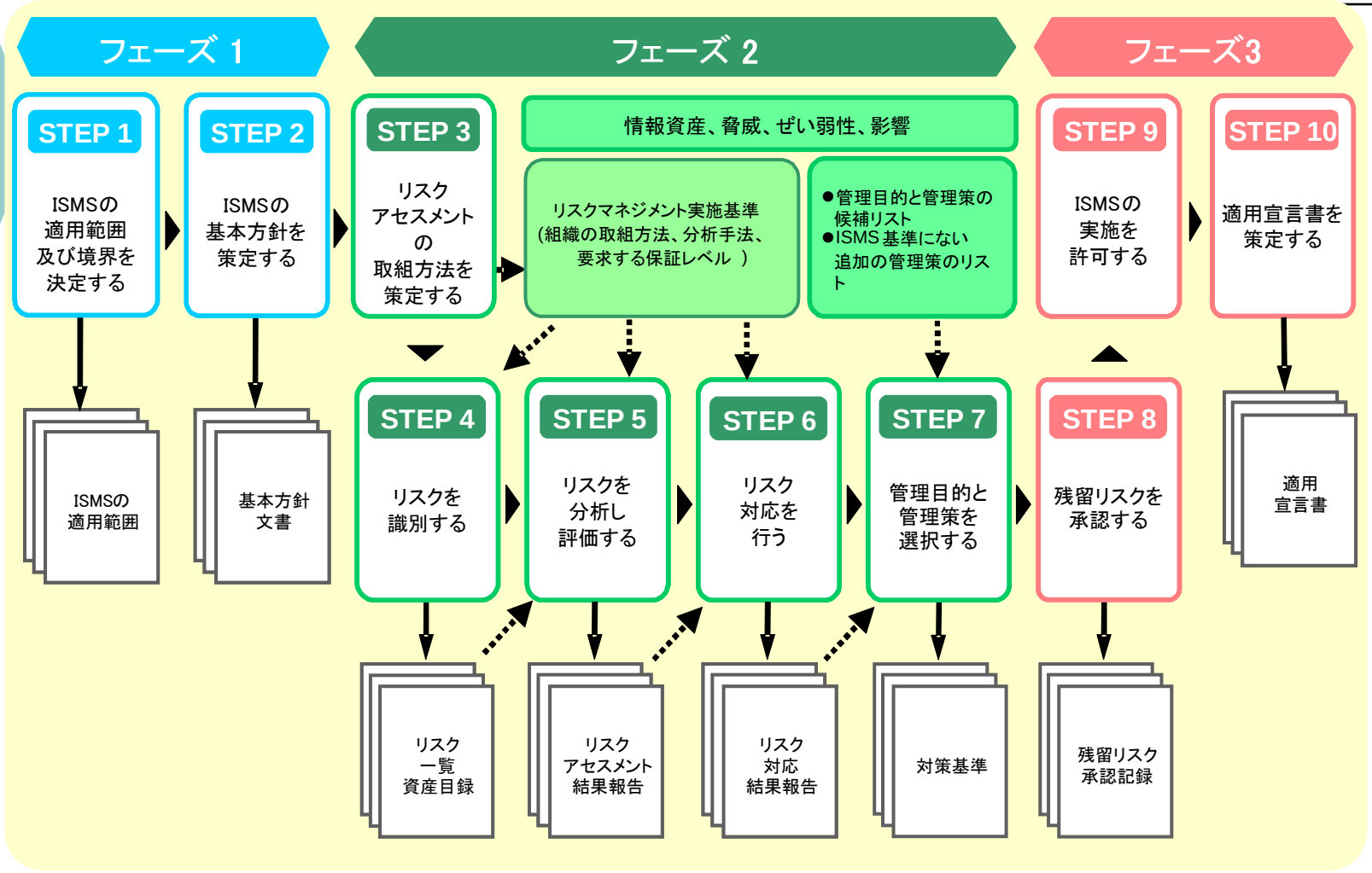
- A.5　セキュリティ基本方針
- A.6　情報セキュリティのための組織
- A.7　資産の管理
- A.8　人的資源のセキュリティ
- A.9　物理的及び環境的セキュリティ
- A.10　情報及び運用管理
- A.11　アクセス制御
- A.12　情報システムの取得、開発及び保守
- A.13　情報セキュリティインシデントの管理
- A.14　事業継続管理
- A.15　順守

附属書B（参考）　OECD原則とこの規格
附属書C(参考）　ISO 9001：2000、ISO 14001：2004及びこの規格の対応

# ISMSにおけるPDCAモデル



# ISMSの確立



# ISMS認証取得組織の年度別推移

| 年度 | 2003年3月 | 2004年3月 | 2005年3月 | 2006年3月 | 2007年3月 | 2008年3月 | 2009年5月 | 2010年5月 | 2011年5月 |
|---|---|---|---|---|---|---|---|---|---|
| 認証取得組織数 | 143 | 275 | 423 | 720 | 568 | 497 | 556 | 404 | 210 |
| 認証取得組織数累計 | 143 | 418 | 841 | 1,561 | 2,129 | 2,626 | 3,182 | 3,586 | 3,796 |
| 認定された認証機関数累計 | 6 | 9 | 18 | 19 | 23 | 23 | 24 | 25 | 25 |

2011年5月　現在

# 各国（地域）毎のISMS登録証発行数

出典：http://www.iso27001certificates.com/
2011年7月現在

| | | | | | |
|---|---|---|---|---|---|
| 日本 | 3840 | スロベニア | 18 | マカオ | 3 |
| インド | 526 | オランダ | 15 | カタール | 3 |
| 中国 | 497 | フィリピン | 15 | アルバニア | 2 |
| 英国 | 471 | イラン | 14 | アルゼンチン | 2 |
| 台湾 | 420 | パキスタン | 14 | ベルギー | 2 |
| ドイツ | 170 | ベトナム | 14 | ボスニアヘルツェゴビナ | 2 |
| 韓国 | 106 | アイスランド | 13 | キプロス | 2 |
| チェコ共和国 | 101 | インドネシア | 13 | マン島 | 2 |
| 米国 | 100 | サウジアラビア | 13 | カザフスタン | 2 |
| スペイン | 73 | コロンビア | 11 | ルクセンブルク | 2 |
| ハンガリー | 68 | クェート | 11 | マケドニア | 2 |
| イタリア | 67 | ノルウェー | 10 | マルタ | 2 |
| ポーランド | 58 | ポルトガル | 10 | ウクライナ | 2 |
| マレーシア | 55 | ロシア連邦 | 10 | モーリシャス | 2 |
| アイルランド | 41 | スウェーデン | 9 | アルメニア | 1 |
| タイ | 40 | バーレーン | 8 | バングラデシュ | 1 |
| オーストリア | 38 | カナダ | 8 | ベラルーシ | 1 |
| ルーマニア | 35 | クロアチア | 7 | デンマーク | 1 |
| 香港 | 32 | スイス | 7 | エクアドル | 1 |
| ギリシャ | 30 | エジプト | 5 | ジャージー | 1 |
| オーストラリア | 29 | オマーン | 5 | キルギスタン | 1 |
| シンガポール | 29 | ペルー | 5 | レバノン | 1 |
| フランス | 25 | 南アフリカ共和国 | 5 | モルドバ | 1 |
| メキシコ | 24 | スリランカ | 5 | ニュージーランド | 1 |
| トルコ | 24 | ドミニカ共和国 | 4 | スーダン | 1 |
| ブラジル | 23 | リトアニア | 4 | ウルグアイ | 1 |
| スロバキア | 23 | モロッコ | 4 | イエメン | 1 |
| アラブ首長国連邦 | 20 | チリ | 3 | | |
| ブルガリア | 18 | ジブラルタル | 3 | Total | 7279 |

# ISMSユーザーズガイド一覧表

| | |
|---|---|
| ISMSユーザーズガイド<br>-JIS Q 27001:2006(ISO/IEC 27001:2005)対応- | ISMS認証基準(JIS Q 27001:2006)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。主な読者は、ISMS認証取得を検討もしくは着手している組織において、実際にISMSの構築に携わっている方及び責任者を想定している。 |
| ISMSユーザーズガイド<br>-JIS Q 27001:2006(ISO/IEC 27001:2005)対応-<br>-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。事例を付録として追加している。 |
| 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。このガイドは、医療機関関係者にISMSを理解してもらうことを目的としている。 |
| クレジット産業向け“PCI DSS”/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。 |
| 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、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法等の法規順守については重要な課題となっている。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してもらうことを目的としたガイドである。 |

# ご清聴ありがとうございました

(一財)日本情報経済社会推進協会
情報マネジメント推進センター
Tel:　03-3432-9386
FAX:　03-3432-6200
Web: http://www.isms.jipdec.or.jp/