情報セキュリティマネジメントシステム（ISMS）

規格に関する

よくある質問集（FAQ）

第 5.0 版　2005 年 5 月

この FAQ 集は、ISO/IEC 17799 の改訂及び ISMS（情報セキュリティマネジメントシステム）規格の作成に関してよせられた、よくある質問をまとめたものです。今後、追加の質問があった際や新たな規格作成作業の実施に応じて定期的に更新されていきます。この FAQ 集及びその更新版は、ISMS インターナショナルユーザーグループのウェブサイトに公開される予定です。メールでのお問い合わせは ISMSIUG@aol.com までお願い致します。

Ted Humphreys
（ISMS インターナショナルユーザーグループ創設者・議長）

出典：http://www.xisec.com/

注意事項：この FAQ 集は、2005 年 5 月に作成されたものであり、内容によっては最新でない情報も含まれています。次の版（第 6.0 版）が発行され次第、この最新版に置き換えられる予定です。

ISO/IEC 17799 *情報セキュリティマネジメントの実践のための規範*

ISO/IEC 17799 改訂版はいつ発行されるのでしょうか？

ISO/IEC 17799 改訂版は 2005 年 6 月に発行される予定です。はっきりとした発行日はまだ確定していません。

ISO/IEC 17799 2000 年版はどうなるのでしょうか？

2005 年版が正式に発行され次第、2000 年版は廃止される予定です。

ISO/IEC 17799 の新版では、新たに管理策が追加されたのでしょうか？

はい。17 の管理策が新たに追加されました。また、現行の管理策のなかには、統合されたり、取り消されたりしたものもあります。結果として、全 133 の管理策となりました。

2005 年版の章構成は、旧版と同じでしょうか？

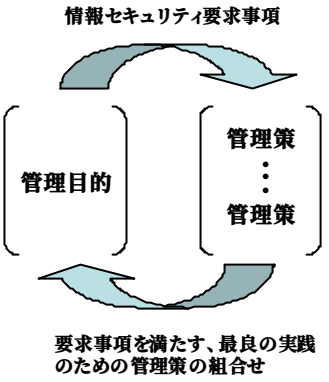
2005 年版の章は、2000 年版より 1 つ多く 11 章あります。また、章の名称も変更されています。下記の図をご参照ください。

他にも ISO/IEC 17799 2005 年版で新しくなったことはありますか？

2005 年版では、様々な事項が取り扱われています。例えば、（これらだけではありませんが）外部関係者によるサービス提供及び外部委託の管理（provisioning of outsourcing）におけるセキュリティ、パッチ管理などといった今日の脅威の取扱い、雇用の前・期間中・終了時のセキュリティ、リスクや事件・事故の取扱いの強化、モバイル通信・遠隔通信・分散通信（mobile, remote and distributed communications）や情報処理の取扱い等について記載されています。

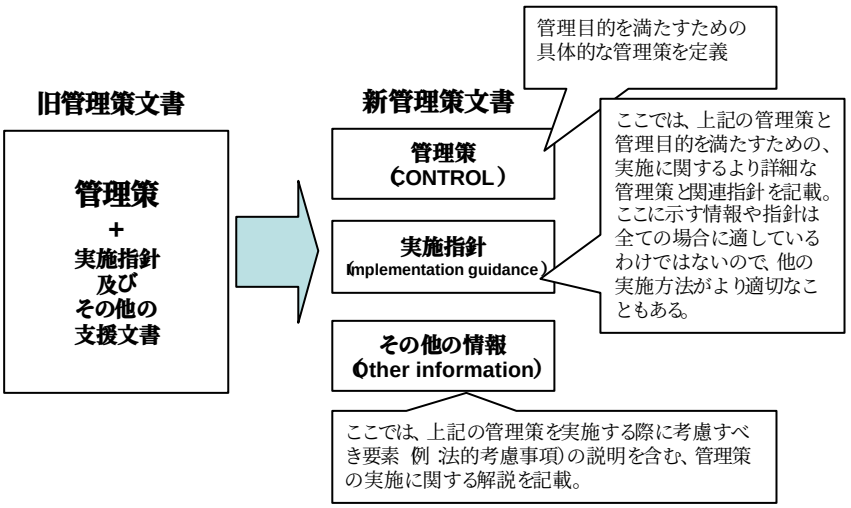
ISO/IEC 17799 2005 年版の管理目的・管理策のモデルは 2000 年版と同じでしょうか？

はい、モデルは 2000 年版と同じで、まず管理目的で要求事項を定義し、続いてその目的を満たすよう設計された管理策を 1 つ又は複数定義しています。



ISO/IEC 17799 2005 年版では、「Look and feel（文書の体裁）」については 2000 年版と同じなのでしょうか？

概して 2005 年版は 2000 年版と同じです。ただ、規格の「使いやすさ」を改善するために修正が加えられ、読者が管理策とその管理策に対する実施指針（implementation guidance）とを区別しやすいようになりました。下記の図は、この「使いやすい」新構造を示しています。



ISO/IEC 17799 新版は、2000 年版と同じく実践規範なのでしょうか？

はい。ISO/IEC 17799 新版は、2000 年版と同じく最良の実践のための管理策を定めた、実践規範です。この規格では、以前と同様に全管理策において「～が望ましい（should）」という表現のみが使用されており、管理策の選択とその導入は全く組織の判断に委ねられています。これと対照的に、BS 7799 Part2（ISO/IEC 27001 ともいう。下記参照）は要求仕様です。BS 7799 Part2 の管理策では「しなければならない（shall）」という表現が使用されており、この規格を認証目的に利用することができるようになっています。

ISMS（*情報セキュリティマネジメントシステム*）規格

BS7799-2:2002 についてですが､ISO/IEC 17799 改訂に基づく附属書 A を盛り込むために BS 7799-2 の 2005 年版が発行されるのでしょうか？

いいえ。ISO/IEC JTC 1/SC 27（ISO/IEC17799 も取り扱っている標準化委員会）では、ISMS（情報セキュリティマネジメントシステム）要求事項規格の作成が進められています。この作業が終了してこの規格が ISO/IEC 規格として発行された後（発行予定日は 2005 年末を目指しています）、BS 7799 Part2:2002 は廃止となり、この ISO/IEC 規格に置き換えられる予定です。

ISMS 規格の（ISO）番号はどうなるのでしょうか？

他のマネジメントシステム規格（ISO 9000 や ISO 14000 シリーズなど）の先例に従って､ISO/IEC JTC 1/SC 27 は、ISMS（情報セキュリティマネジメントシステム）規格に関するものとして 27000 シリーズに着手しました。従って、新 ISMS（情報セキュリティマネジメントシステム）規格の番号と表題は、ISO/IEC 27001 Information security management systems –Requirements （情報セキュリティマネジメントシステム ― 要求事項）となる予定です。

ISO/IEC 27001 は、やはり ISO/IEC 17799:2005 と関連したものとなるのでしょうか？

はい。この 2 つの規格は関連したものとなる予定です。ISO/IEC 27001 Information security management systems –Requirements （情報セキュリティマネジメントシステム ― 要求事項）には附属書 A があり、BS 7799 Part2: 2002 と同じく、この附属書に ISO/IEC 17799 の管理策が記載される予定です。

ISO/IEC 27000 シリーズのなかには、他にも ISMS 規格があるのでしょうか？

はい。ISO/IEC 27001 Information security management systems –Requirements （情報セキュリティマネジメントシステム ― 要求事項）の作成と同様に、ISMS 実施状況（プロセス及び管理策）の*有効性*の測定方法を取り扱うことを目的とした、ISO/IEC 27004 'Information security management metrics and measurement'（情報セキュリティマネジメントの評価尺度及び測定法）についても現在作成作業が進められています。

また、その他にも ISO/IEC 27001 の利用及び導入を支援するための規格やガイドライン作成に関する提案もあり、現在検討が進められています。そのような提案には、例えば、ISO/IEC 27001 に規定するプロセス及び管理策の実施に対し、よりいっそうの支援や追加のガイダンスを提供することを目指した、'ISMS Implementation guidance'（ISMS 実施指針）規格の作成などがあります。

ISO/IEC 17799:2005 と ISO/IEC 27000 シリーズの関連についてはどうなるのでしょうか？

ISO/IEC 17799:2005 Code of practice for information security management （情報セキュリティマネジメントの実践のための規範）の番号は、当面は変更されず現行のままの予定です。しかしながら、ISO/IEC 17799 に対し、2007 年 4 月に ISO/IEC 27002 という番号を割り当てることが提案されています。こうした期間をおくことにより、この新しいシリーズ番号が自然に市場になじむことができると思われます。

ISO/IEC 27001 は、どの程度 BS 7799 Part2 と違うのでしょうか。

ISO/IEC 27001:2005 と BS7799 Part2:2002 の違いは、それ程大きくはならないと予想されます。現在改訂作業は、この 2 つの規格の互換性（backwards compatibility)、整合性、そして移行の容易さを念頭に置いて進められています。ISO/IEC 27001 と BS7799 Part2:2002 の違いは、BS7799 Part2:2002 とその旧版である BS7799 Part2:1999 間の違いと比べるとはるかに小さいです。

（認定された認証機関の行う）ISMS 認証についてはどうですか？

現在、組織の ISMS 認証審査は、認証に関する要求事項である BS7799 Part2:2002 に沿って行われています。ISO/IEC 27001 が発行され、BS7799 Part2 が廃止された後は、認証作業（例えば、新規の認証、既存の認証取得事業者のサーベイランス審査及び認証の更新）については、この ISO 規格を使用したものに移行することができます。組織とその認証機関が BS7799 Part2:2002 から ISO/IEC 27001 への移行に必要とする期間については、その詳細を記載した Certification Transition Statement（「認証の移行手順書」）を、このプロセスにかかわる各国の認定機関（National Accreditation Body）が公開する予定です。この「認証の移行手順書」の公開は、ISO/IEC 27001 の発行前に実施される予定です。

世界 ISMS 認証取得事業者リストはどうなるのでしょうか？

現在の世界 ISMS 認証取得事業者リストについては、ISMS 認証事業者を登録する目的で引き続き世界リストとして維持・機能していきます。各国の認証機関は、新規の認証と既存の認証の更新の詳細を含めた事業者リストを、現在と同じ通知プロセスを通して引き続き提供をお願いします。