個人情報保護と情報セキュリティマネジメントシステム（ISMS）

芦田　元之　　武内　春夫
内田　茂

2005年4月の個人情報保護法の全面実施に向けて，企業は数々の情報セキュリティ対策を実施してきた。「五年以内に世界最先端のIT国家となる」ことを目標とした「e-Japan戦略」の基に政府は安心で安全な電子政府・電子自治体の構築を目指し，この五年の間に各種制度やインフラの整備に努めてきた。なかでも個人情報保護を中心とする「情報セキュリティ対策」は目下，最重要テーマといえ，最近では各省庁が連携して対策強化策を打ち出している。今後は，これらの情報セキュリティ対策の有効性が問われることになる。

そこで本稿では情報セキュリティにおける社会環境の動向とこれに伴う必要な情報セキュリティ対策について説明する。

ISMSの標準化動向

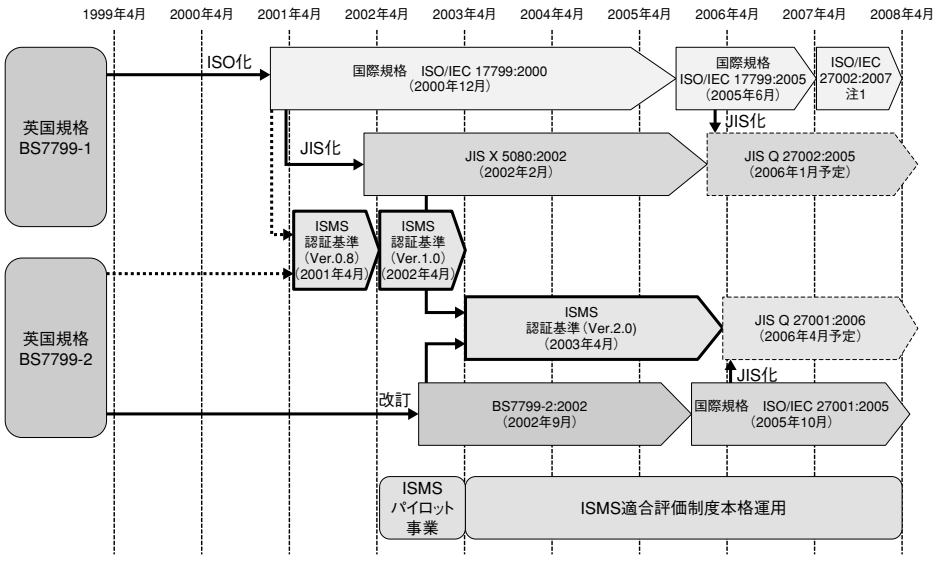
ISMSの原典である英国標準BS7799が，2005年10月に国際規格化された。これまでの標準化の経緯と国際規格化によるISMS認証の影響について説明する。

（1）ISMSの国際規格化

セキュリティポリシーに基づく情報セキュリティマネージメントシステム（ISMS）は，英国標準BS7799が原点である。BS7799は，BS7799-1（実践のための規範）とBS7799-2（ISMS要求仕様）から構成されている。

BS7799-1は，ISMSを実践するためのガイドラインである。BS7799-2は，情報セキュリティ対策を行うために必要な管理策を規定している。したがって，ISMSの認証を取得するためには，BS7799-2で示されている管理策をすべて満足する必要がある。

BS7799，国際規格（ISO/IEC）およびJIS（日本工業規格）との関係を**図1**に示す。BS7799-1は，2000年12月に国際標準ISO/IEC17799:2000に制定されている。これに基づき，日本では，2002年2月にJIS X 5080:2002としてJIS化されている。ISO/IEC 17799:2000は，情報セキュリティ環境の変化に合わせて，2005年6月に改訂され，ISO/IEC 17799:2005となっている。JIS化も2006年1月に行われる予定である。



注1：国際標準規格ISO/IEC17799:2005は、ISO/IEC27002 となる予定（2007年）　　出典：JIPDEC 「ISO/IEC27001への以降計画」

図1　ISO規格およびJIS規格制定動向

国際標準化機構（ISO）は，2003年1月に「情報セキュリティマネジメントシステムに関する国際規格の必要性」について検討した結果，国際規格化することが決められた。認証実績があり，国際的なデファクトスタンダードとして認められているBS7799-2:2002の採用が決まり，国際規格化の作業が本格化した。BS7799-2:2002が改訂され，2005年10月にISO/IEC 27001:2005として国際規格化された。JISとしてもJIS Q 27001:2006として2006年4月に公表される予定である。

BS7799-2:2002と

ISO/IEC 7001:2005との主たる相違点は以下の2点である。

① 管理策の再編と追加

規定されている情報セキュリティ対策のための管理策は，9項目が削除され、15項目が新しく追加された。この結果、管理策は127項目から133項目となっている。

② 管理策の有効性

情報セキュリティの管理策の有効性を検証するために，管理策の有効性の評価が求められている。

(2) ISMS認証

ISMSの認証活動は，英国を中心とするヨーロッパが先行していた。日本の認証活動は，2001年のパイロット事業としての試行後，2002年4月に「ISMS適合評価制度」として本格運用を開始している。認定機関は、財団法人日本情報処理開発協会（JIPDEC）で，実際の審査は民間機関が行っている。各国の認証はBS7799-2をベースに行われている。日本は当初JIS X 5080:2002（BS7799-1ベース）を基準に認証を行っていたが，BS7799-2:2002の改訂を機にISMS認証基準（Ver.2.0）としてBS7799-2:2002を認証の基準として採用し，各国との整合性が図られた。

2006年4月のJIS Q 27001:2006（ISO/IEC 7001:2005）の発行に伴い，ISMS認証基準（Ver.2.0）は、廃止されるが、2006年10月までの半年間は，どちらの規格でも審査登録できる。その後は，ISMS認証基準（Ver.2.0）での新規登録および既にISMSの認証を取得している企業の継続審査はできなくなる。

このため，ISMS認証基準（Ver.2.0）で認証取得作業を行ってきた企業は、2006年10月までに審査を受けなければならないことになる。既に認証を取得している企業は、いずれの時期にJIS Q 27001:2006に切り替えて継続審査を受けるかを慎重に検討しなければならない。いずれにしろ，2006年10月から日本のISMS認証の基準は，JIS Q 27001:2006（ISO/IEC 7001:2005）に切り替わる。

(3) 情報セキュリティ監査制度

経済産業省は，ISMS適合評価制度とは別に，「情報セキュリティ監査制度」を2003年4月にスタートしている。情報セキュリティ監査制度は，BS7799-2:2002を基準にしているのは，ISMS適合評価制度と同じであるが，対象とする組織および管理策（管理基準）を限定することができ，被監査主体が情報セキュリティ監査を受けやすくしている。監査自体は，民間の監査機関が行う。監査機関の監査のバラつきを防ぐために，情報セキュリティ監査制度は以下の項目を規定している。

- 情報セキュリティ管理基準
- 個別管理基準（監査項目）策定ガイドライン
- 情報セキュリティ監査基準　実施基準ガイドライン
- 情報セキュリティ監査基準　報告基準ガイドライン

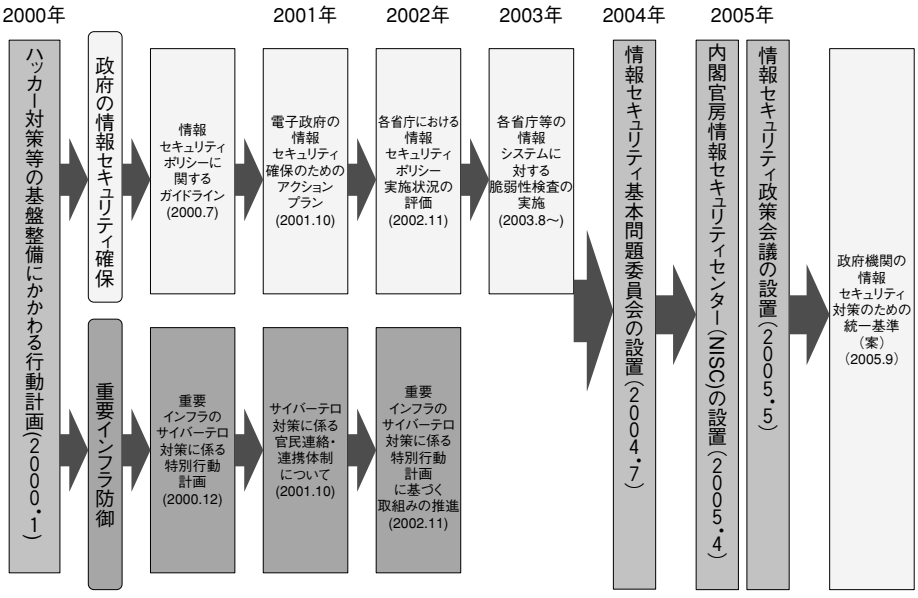


図2　政府における情報セキュリティの取り組み

情報セキュリティ管理基準は，BS7799-2:2002に基づき実施しなければならない管理策を，詳細に規定し，監査する項目を規定している。

個別管理基準（監査項目）策定ガイドラインは，被監査主体が監査を受けるときに，対象とする管理策選定方法を規定している。

情報セキュリティ監査基準実施基準ガイドラインは，（監査機関）が監査を実地するための基準を定めている。

情報セキュリティ監査基準報告基準ガイドラインは，監査機関が監査結果を報告する報告書の作成方法と内容について定

めている。

ISMS適合評価制度は，JIPDECから認証され，公表されるが，情報セキュリティ監査制度では，監査結果を民間の監査機関からを受け取るだけで認証されるわけではない。このため，情報セキュリティ監査のメリットは，民間企業には今ひとつ不明確であり，経済産業省が期待しているほど普及はしていない。民間よりはむしろ公的機関の情報セキュリティ監査に利用されている傾向にある。

政府の動向

本章では、政府における情報セキュリティ政策および地方公共団体に対する取り組みについて述べる。

(1) 政府における情報セキュリティ政策の取り組み

政府は，安全で信頼できる電子政府および電子自治体および世界最先端のIT国家の実現を目標としている「e-Japan戦略」を積極的に推進している。情報セキュリティ対策は，この「e-Japan戦略」で重要な位置付けになるとの認識から，政府は情報セキュリティ対策に取り組んできた。2000年7月に公布された「情報セキュリティポリシーに関するガイドライン」は，各府省庁に対して，情報セキュリティポリシーの策定と運用を指導している。策定されたセキュリティポリシーの実効性を高めるために，政府は積極的に政策を打ち出している（前ページ**図2**参照）。

- 「電子政府の情報セキュリティ対策確保のためのアクションプラン」（2001年10月）
- 「各省庁における情報セキュリティポリシーの実施状況の評価」（2002年11月）
- 「各省庁等の情報システムに対する脆弱性検査の実施」（2003年8月～）

従来，「政府の情報セキュリティ確保」と「重用インフラ防御」は個別に対策が行われてきたが，2004年になり，IT社会の基盤となる情報セキュリティに関する基本的な課題について、優勢順位を付けて検討する母体として「情報セキュリティ基本問題委員会」が設置された。

情報セキュリティ基本問題委員会は，情報セキュリティに取り組む政府の役割・機能の見直しに向けての提言を受け，政府は、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制を整備し，以下の組織を設置した。

- 内閣官房情報セキュリティセンター（NISC）（2005年4月）
- 情報セキュリティ政策会議（2005年5月）

NISCは，以下の機能を持つ。

① 情報セキュリティ政策に関する基本戦略の立案
② 政府機関の総合対策促進
③ 政府機関の事案対処支援
④ 重要インフラの情報セキュリティ対策

情報セキュリティ政策会議は，NISCの活動に対する審議および決定機関である。

NISCは，2005年9月に「政府機関の情報セキュリティ対策のための統一基準」（案）を発表，12月に正式に採用される予定である。各省庁は，2000年に策定された「情報セキュリティポリシーに関するガイドライン」に基づいてセキュリティポリシーを策定したが，省庁間のセキュリティ水準にバラツキが大きいため，情報セキュリティ対策を統一することを目的としている。各省庁は、この統一基準に準拠したセキュリティポリシーの再構築を2006年度に行い，情報セキュリティ水準の向上を行うことになる。この一環として，情報セキュリティ監査も必要になる。**図3**に今後の政府機関の情報セキュリティに対する枠組みを示す。

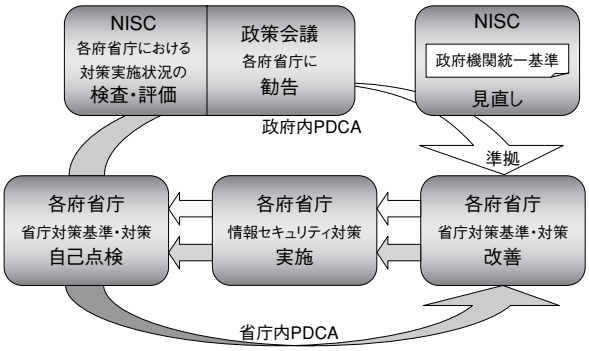


図3　今後の政府機関の情報セキュリティに対する枠組み

(2) 地方公共団体の取り組み

地方公共団体において，本格的な情報セキュリティ対策が開始されたのは，総務省が2001年3月に「地方公共団体における情報セキュリティポリシーに関するガイドラインについて」を公表し，全国の団体に対してセキュリティポリシーの策定を求めたことに端を発している。以来，全国的に取り組みが進められ，2005年7月1日現在，情報セキュリティポリシーの策定状況は，都道府県が100%，市区町村では93.7%と，規定面ではほぼ整備が完了したといえる。しかし，その実状を見ると多くの団体ではポリシー策定に止まり，実際に運用されているところはまだまだ少ないといわざるをえない状況である。住民が安心して利用できる電子自治体を実現するためには，PDCA（Plan：策定・導入，Do：運用，Check：評価，

Act：見直し）サイクルに則って定期的に情報セキュリティ対策の改善を図り，地方公共団体の情報セキュリティレベルを高く維持することが求められている。セキュリティ対策の実効性を評価するために，2003年12月に「地方公共団体情報セキュリティ監査ガイドライン」を公表し，外部監査の導入を推進しているが，実際には，外部監査の導入は進んでいない。

表1　情報セキュリティ監査の実施状況

実施状況		都道府県	市町村
実施している		26（55.3%）	504（20.8%）
	内部監査の実施	10	344
	外部監査の実施	12	108
	内部/外部監査実施	4	52
検討中		21（44.7%）	1,231（50.9%）
未実施		0	683
合計		47	2,418

出展：地方自治情報管理概要「地方公共団体における行政情報化の推進状況調査（平成17年4月1日現在）の取りまとめ結果」（総務省）

表1は，地方公共団体における情報セキュリティ監査の実施状況を示している。「情報セキュリティ監査を実施している」のは，都道府県が26団体（55.3%），市区町村が594団体（20.8%）となっている。このうち12の都道府県，170の市区町村が「外部監査」まで実施しているが，その監査内容のほとんどは「情報システムの脆弱性診断」に止まっており，対策の改善・向上を促すという本来の意味での情報セキュリティ監査は，進んでいない。2005年8月，総務省が発表した「平成十八年度ICT政策大綱」に，電子自治体推進における地方公共団体の情報セキュリティ水準の向上策が盛り込まれている。ここでは，地方公共団体の具体的なアクションプランとして，

① 個人情報保護条例の充実
② 情報セキュリティポリシーに基づく対策
③ 情報セキュリティ監査の推進

などを挙げている。

この結果，地方公共団体の情報セキュリティ監査は加速されると推測される。

沖電気グループの取り組み

「安全で安心なeソリューションの提供」を行っている沖電気グループは，情報セキュリティ対策は最重要項目であり，積極的に取り組んできている。特に，セキュリティ対策の有効性を確認するために，第三者評価であるISMS認証取得を推進している。現在までに，以下の部門と関連企業でISMS認証を取得している。

- 情報企画部（2003年2月取得）
- 沖電気システムセンター（2003年8月取得）
- 社会情報ソリューション本部（2004年12月取得）
- 沖電気カスタマアドテック（OCA）（2004年1月取得）
- 日本ビジネスオペレーションズ（JBO）（2004年1月取得）
- 沖通信システム（OTS）（2005年7月）
- 運輸流通ソリューション本部（作業中：2006年春予定）
- 沖電気ネットワークインテグレーション（作業中）

個人情報保護対策として，プライバシーマークの認証については以下の関連企業が取得または審査中である。

- 沖ヒューマンネットワーク（OHN）（2005年9月）
- 沖ソフトウェア（OSK）（審査中）
- オキアルファクリエイト（OAC）（審査中）

ISMSおよびプライバシーマークの認証取得は，沖コンサルティングソリューションズ（OCS）のコンサルティングで行われている。OCSは，ISMS認証取得，情報セキュリティ監査およびプライバシーマーク認証取得等の情報セキュリティに関するコンサルティングを積極的に展開しており，豊富な実績と経験を有している。OCS自体は個人情報や情報処理を行っていないが，ISMS認証取得の作業を行っている。

ま と め

情報セキュリティ対策は，導入するだけでなく，実質的な有効性が求められる時期に来ている。政府，公共団体および企業を含めて，情報セキュリティ対策の評価・見直しを行い，情報セキュリティレベルの更なる向上が必要である。

特に，政府および地方公共団体では，情報セキュリティ監査の実施が求められることになる。 ◆◆

●筆者紹介

芦田元之：Asanobu Ashida. 沖コンサルティングソリューションズ株式会社
武内春夫：Haruo Takeuchi. 沖コンサルティングソリューションズ株式会社
内田茂：Shigeru Uchida. 沖コンサルティングソリューションズ株式会社