プライバシーマーク認定取得とISMS認証取得の効果的な使い分け

Effective Use of Acquiring Privacymark Authorization and Acquiring ISMS Scheme

支倉健一* 田上岳夫*
Kenichi Hasekura Takeo Tagami

要　旨

2005年4月に個人情報保護法が全面施行されるなか，組織は個人情報を保護するためにセキュリティ対策を実施することが急務となっています。その対応策として，プライバシーマーク制度とISMS適合性評価制度の認証取得組織数が増加傾向にあります。

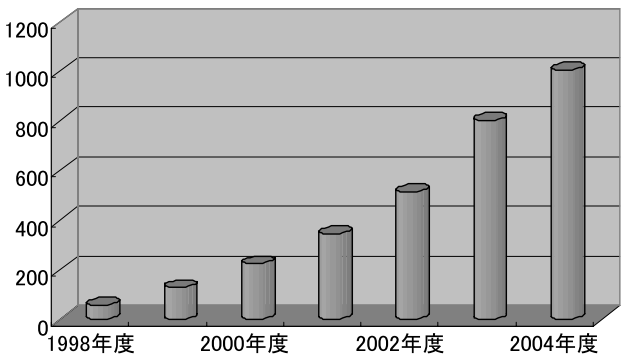
本稿ではセキュリティ対策として代表的なこれらの制度の違いを明確にするとともに，個人情報を保護するためのセキュリティ対策の本質を考えた場合の両制度の使い分けを提案します。

The privacy law will be forced on next April. Each organization has to hurry to build up the security measure for protecting personal information. Recently, organizations acquiring Privacymark authorization and acquiring ISMS scheme have been increasing.

In this paper, differences between both authorized systems are clarified, and the effective use of both authorized systems is proposed.

1．プライバシーマーク制度とISMS適合性評価制度を取り巻く状況

2005年4月，個人情報保護法が全面施行されます。組織は個人情報に対する保護対策を早急に実現しなければなりません。このようななか，個人情報保護対策として，プライバシーマーク制度の認定を取得する動きが活発になっています。プライバシーマーク制度[1]は，平成10年に，財団法人日本情報処理開発協会（JIPDEC）が運用を開始した認定制度です（**図1**）。この制度は，JIS Q15001（個人情報保護に関するコンプライアンス・プログラムの要求事項）[2]に基づき，組織が積極的に推進する自主的な規制，努力にインセンティブを与え，国の個人情報保護をいっそう促進させるための手段として，事業者団体と協調して実施するものです。情報主体である個人は，プライバシーマークによって組織の個人情報の取り扱いが適切であることを容易に判断することが可能になります。また組織にとっては，プライバシーマークを公に示すことによって，消費者から安心と信頼を得ることができ，ビジネスを優位に進められるメリットがあります。



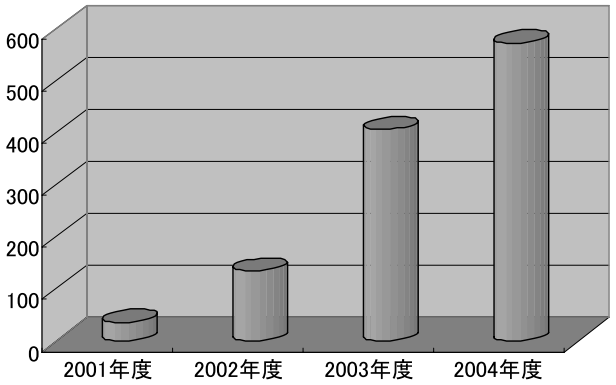
（出展：http://privacymark.jp/pr/20041122.html より一部抜粋し加工）
2004年度は11月22日までの集計

図1　プライバシーマーク制度の認定組織数の推移
Fig.1　Transition of institutional number of Privacymark authorization.

プライバシーマーク制度は，個人情報を保護するために様々な安全対策を実施します。同じ安全対策を実施する制度に，ISMS適合性評価制度[3]があります。この制度は2002年にJIPDECが運用を開始（パイロット運用は2001年度に開始）した認証制度です。JIS X5080（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）[4]から作成したISMS認証基準[5]に基づき，技術的なセキュリティのほかに，人間系の運用・管理面をバランスよく取り込み，組織として情報セキュリティマネジメントを確立し，セキュリティ水準を向上させることをめざすものです（**図2**）。

一部の組織では，プライバシーマーク制度とISMS適合性評価制度の両方の取得を検討したり，実際に取得したりするケースが増えてきています。そこで本稿では，プライバシーマーク制度とISMS適合性評価制度を比較検討し，

＊ IT基盤システム開発事業部
IT Platform Systems Development Division



（http://j-isms.jp/resume.html の講演資料より一部抜粋し加工）
2004年度は12月16日までの集計

図2　ISMS適合性評価制度の認定取得の推移
Fig.2　Transition of institutional number of ISMS scheme.

効果的な使い分けを考えてみます。

2．プライバシーマーク制度認定取得とISMS認証取得の違い

2.1　スコープ

プライバシーマーク制度とISMS適合性評価制度はともに，そのスコープ（適用範囲）を定めますが，プライバシーマーク制度は組織全体をスコープにすることが原則として定められています。しかしISMS適合性評価制度は，この原則を設けていません。論理的に正しいスコープを設定していれば，認証を取得する組織が独自の判断でスコープを定めることができます（**図3**）。

プライバシーマーク制度では組織の経営陣をトップとしたピラミッド構造をとりますが，ISMS適合性評価制度ではスコープ内のトップが経営陣とみなされます。またプライバシーマーク制度ではプライバシー委員会のような全社横断的な組織を確立するのに対し，ISMS適合性評価制度では部門内セキュリティ連絡会のような組織を確立することになります。

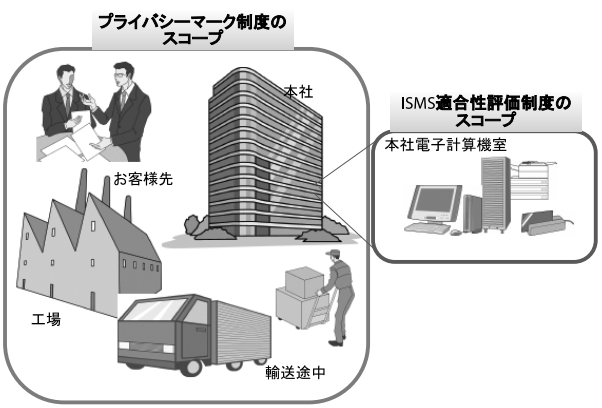


図3　スコープのイメージ
Fig.3　Scope image.

構築面においては，プライバシーマーク制度では全社に分散する個人情報を洗い出し，分析するのに対し，ISMS適合性評価制度ではスコープ内の情報資産について洗い出しを行い，リスクを分析します。資産の洗い出しと分析はマネジメントシステムを構築する土台であり，多くの作業負荷を必要とします。またこの作業は，構築時だけでなく維持時も同様に必要であり，この作業量をいかに少なくするかが全体の作業量を小さくするポイントになります。

双方の制度ではコンプライアンス・プログラム（CP）やセキュリティポリシーを始めとする規程類を作成します。プライバシーマーク制度では全社を対象にした規程となり，ISMS適合性評価制度では既存の全社規程をそのまま参照したり，流用してスコープ内の規程を作成したりします。

スコープが異なれば，おのずと対象人数も異なります。プライバシーマーク制度では全社がスコープであるため，大組織では対象人数が数万人規模になりますが，ISMS適合性評価制度では大組織であっても対象人数が数十人規模となる場合があります。これらに対する教育・研修は，対象人数に応じた作業量が発生します。以上のように，スコープが異なると，構築・維持の作業量に違いが出ます。

2.2　マネジメントシステムの構築

プライバシーマーク制度で準拠する規格はJIS Q15001であり，個人情報を保護するためにコンプライアンス・プログラムを策定し，実施し，維持しおよび継続的に改善するプライバシーマネジメントシステムの確立を要求しています。ISMS適合性評価制度で準拠する規格はISMS認定基準であり，情報セキュリティの確立のためにPDCA（Plan－Do－Check－Act）モデルである情報セキュリティマネジメントシステム（ISMS）を確立し，導入し，運用し，監視および維持することを要求しています。

このようにプライバシーマーク制度とISMS適合性評価制度とも，PDCAモデルのマネジメントシステムの確立をめざしています。そしてそれぞれは**図4**のような作業工程で構築を行います。両者とも準備，企画，構築，運用，受審フェーズから構成されており，体制の確立，資産の洗い出し・分析，規程類の作成，教育・研修，監査，改善のように作業が進みます。

一般にプライバシーマークはISMS適合性評価制度に比べて，容易に認定を取得できるものととらえられていますが，プライバシーマーク制度の認定を受けるためには，ISMS適合性評価制度の認定を受けるのに必要な作業と同等の，しかも全社的な作業が必要であり，容易に認定を取得できるものではありません。またこれにかかる自社作業コストやコンサルタント依頼コストも同様，ISMS適合性評価制度より安価に対応できるものでもありません。

2.3　規格内容

JIS Q15001は，序文を含め全5章からなり，ISMS認定基準は，序文を含め全8章と付属書の詳細管理策から構成

図4　プライバシーマーク制度とISMS適合性評価制度のマネジメントシステム構築の標準作業フレームワーク

Fig.4　Standard work framework of constructing privacy management system, information security management system.

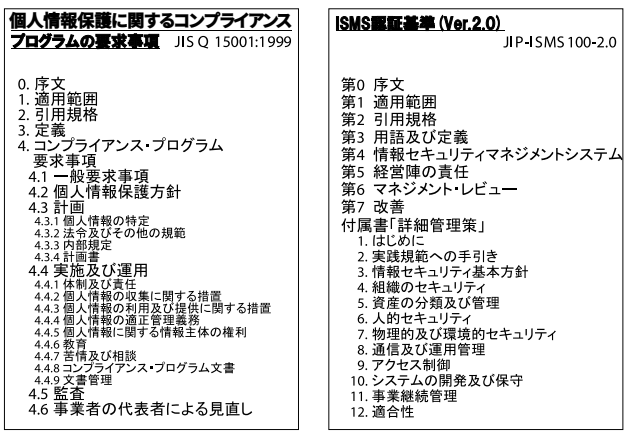


図5　JIS Q15001・ISMS認証基準の目次

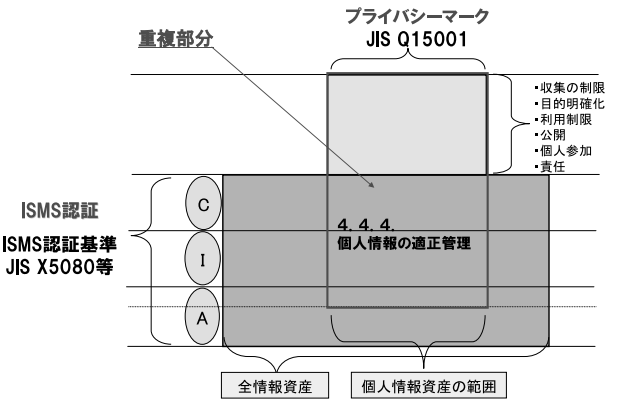
Fig.5　Content of JIS Q15001, JIP-ISMS100.

されています（**図5**）。

プライバシーマーク制度もISMS適合性評価制度も，個人情報や重要な情報資産を脅威から守る（セキュリティ対策を施す）ことには変わりなく，**図6**のようにそれぞれの規格で，セキュリティ対策の部分が重複した内容になっています。JIS Q15001では「4.4.4 個人情報の適正管理義務」で，個人情報に対するセキュリティ対策を要求しています。技術面の対策として，情報システム安全対策基準（平成7年8月29日日通商産業省告示第518号）やコンピュータ不正アクセス対策基準（平成8年8月8日日通商産業省告示第362号）などを参考に安全対策を行うことを求めていますが，現在では実質的にJIS X5080やISMS認証基準を参考にセキュリティ対策を実施することになります。

また，ISMS認証基準の詳細管理策「12（1） 法的要求事項への適用」では，規制や関連法令への準拠を要求しており，JIS Q15001や2005年4月に全面施行される個人情報保護法への準拠を実質的に定めています。

プライバシーマーク制度では組織が保有している個人情報を保護すべき対象としており，ISMS適合性評価制度では組織が保有する個人情報を含むすべての情報資産を保護すべき対象としています。



C：機密性、I：完全性、A：可用性

（出展：(財)日本情報処理開発協会主催プライバシーマークセミナー資料(2002.11.11)より一部抜粋し加筆）

図6　条文内容の重複

Fig.6　Duplication of contents of article.

以上のように，プライバシーマーク制度とISMS適合性評価制度では，マネジメントシステムを構築する上で必要なセキュリティ対策について，規格の条文内容が重複しています。

3．プライバシーマーク制度とISMS適合性評価制度の効果的な使い分け

以上，プライバシーマーク制度とISMS適合性評価制度の比較を中心に述べてきましたが，両者とも組織にとってこれからのビジネス遂行や内部ガバナンスの実践において非常に有益な要素を含んでいることが分かります。しかし組織はセキュリティ対策を無制限に導入できるわけではなく，有限な資産を効率よく活用して導入しなければなりません。

NECは「スリムアプローチ型ISMS構築メソッド」という考え方を持っています。これは，ISMSの短期構築と段階的な精度向上，セキュリティ水準の段階的なレベルアップ，対象範囲の段階的な拡大を行い，スリムにISMSを構築し，維持するメソッドで，組織の有限な資産を効率よく導入できる特長があります。

プライバシーマーク制度とISMS適合性評価制度を導入する際もこの考え方を採用できます。まずは小さい範囲で情報セキュリティマネジメントシステムを確立し，次にそれを段階的に拡大，精度を向上させます。そしてマネジメントシステムが組織内で有機的に機能し始めたことを確認後，全社でプライバシーマーク制度の認定を取得するプランをお勧めします。幸いプライバシーマーク制度とISMS適合性評価制度はマネジメントシステムを構築する点においては同じであり，準拠する規格も部分的に条文が重複しているので，プライバシーマーク制度を認定取得する際，

既存のISMSを効率的に活用してプライバシーマネジメントシステムを構築できます。ただ，現実には組織や業界によって対応方法は異なります。個人情報を多数保有している組織や個人情報を業務の中核としている業界などは，プライバシーマーク制度を優先して取得する方がよい場合があります。

ここで気をつけたいのは，制度ありきで，安易にプライバシーマーク制度やISMS適合性評価制度の認証取得をめざすことです。組織に対するセキュリティ対策を統合的に検討した結果，セキュリティ対策の1つの手段として，これらの制度を効果的に使い分けて認証取得をめざすことをお勧めします。

NECはプライバシーマーク制度認定取得支援コンサルティングサービスとISMS認証取得支援コンサルティングサービスの豊富な実績を有しています。個人情報保護法の全面施行により，その重要性が改めて注目されるなか，NECはお客様の状況を十分加味した両コンサルティングサービスの提供を通して，お客様のマネジメントシステムの構築をトータルにサポートします。

参考文献

1） プライバシーマーク制度
http://privacymark.jp/

2） JIS Q15001（個人情報保護に関するコンプライアンス・プログラムの要求事項）
日本規格協会　http://www.jsa.or.jp/

3） ISMS適合性評価制度
http://www.isms.jipdec.jp/

4） JIS X5080（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）
日本規格協会　http://www.jsa.or.jp/

5） ISMS認証基準
http://www.isms.jipdec.jp/v2/index.html

筆者紹介

Kenichi Hasekura
支倉　健一（はせくら　けんいち）　1991年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターコンサルティングマネージャー。

Takeo Tagami
田上　岳夫（たがみ　たけお）　1995年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター主任。システムズアーキテクト。日本システム監査人協会会員。