電気通信事業者のための情報セキュリティマネジメントガイドライン ISO/IEC 27011（ITU-T X.1051）の策定とその影響

中尾　康二　（KDDI 株式会社）

概要　近年，情報セキュリティマネジメントシステム(ISMS)構築，運用の重要性が叫ばれ，多くの組織（企業）が保有する情報資産のセキュリティ確保を目的として ISMS 認証取得・運用の活動を推進している．この環境において，さらに特定のセクタ（金融，電気通信分野など）における情報セキュリティマネジメントのあり方が注目されている．これまで，ISO/IEC 及び ITU-T では，セクタ分野の中で初めて「電気通信事業者のための情報セキュリティマネジメントガイドライン」の国際規格化を ISMS 規格と連携する形で完了した．本稿では，電気通信事業者セクタのための国際規格ガイドライン策定の背景・必要性を述べ，本セクタ規格の概要，及び具体的なガイドライン策定に関わる技法をまとめるとともに，本ガイドラインの業界への影響，及び今後の方向性について言及する．

1. はじめに

情報ネットワークの広域化，分散化，高速化，利便性の向上，及び情報システムの高度化，大容量化，高機能化などを背景に，通信の信頼性はもとより，情報システム及び企業における情報セキュリティ技術の重要性が増している．情報セキュリティ技術の標準化は，多くの分野に関係することもあり，多くの標準化団体によって議論されている． その中で，ISO/IEC JTC1/SC27 は具体的な応用や利用形態に依存しない，汎用性の高い情報セキュリティ技術について，広範囲の検討を進めている．特に組織（企業）において情報セキュリティの確保を実現する手法として，ISMS（情報セキュリティマネジメントシステム）の国際規格化，及び国内制度化の整備が進められており，日本は世界的に ISMS 認証を取得している組織（企業）が最も多い国となっている．

今般，ISO/IEC JTC1/SC27 は ITU-T（国際電気通信連合）と共同して（図 1 参照），セクタ規格では初めて ISMS 関連規格として「電気通信事業者のための情報セキュリティマネジメントガイドライン ISO/IEC 27011（ITU-T X.1051）」の策定を実施した．

本ガイドラインは，電気通信事業者のために情報セキュリティマネジメントの推進に必要となる対策（管理策）の雛形を提供するガイドラインである．本稿では，本ガイドライン策定の背景，セクタ規格としての策定手法など，具体的なガイドライン策定に関わる技法をまとめるとともに，本ガイドラインの業界への影響，及び今後の方向性について言及する．

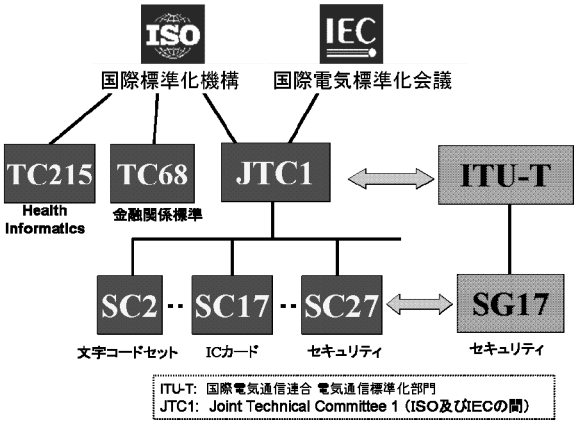

図 1. ISO, ISO/IEC/JTC1 及び ITU-T の関係

2. ガイドライン策定までの背景，及び経緯

2.1 情報セキュリティマネジメントとは

情報セキュリティマネジメントシステム(ISMS)は，組織（企業）の情報セキュリティマネジメントの確保を目的としている．その手法は，組織において保有している重要な情報資産(Asset)を識別し，それらの資産に存在するリスクを脆弱性，脅威，及び影響度により分析しリスクレベル（例えば，５段階表記など）を求め，認識されたリスクレベルのうち，組織が目標とするリスクレベル（許容リスクレベル）を超えていれば，各種セキュリティ対策（管理策と呼ぶ）を用いて許容リスクレベル以下に低減させることを特徴としている．

本 ISMS は, 2005 年に策定された ISO/IEC 27001（ISMS 要求事項）の規格により Requirements（要求事項）が規定されており，ISMS 認証制度については，基本的に本規格に準拠するか否かを認証する. ISO/IEC 27001 に加えて，ISO/IEC 27002（情報セキュリティマネジメントのための実践規範）という重要な規格が存在する．これは，ISMS の構築，運用においてリスク低減を実施するために必要となるセキュリティ対策（管理策）をガイドラインとして規定している．このガイドラインには，多くの分野に跨る管理策が示されており，組織，要員，物理，運用，技術，インシデント対応，事業継続，コンプライアンスなどにおける対策（管理策）がハイレベルな視点からガイドライン化されている. これらの管理策に加え，管理策を実際に実施する場合のガイダンス（実施の手引きと呼ぶ）についても記載されている． ISO/IEC 27002 は，本稿で述べる電気通信事業者向けのガイドラインのベースとなっており, ISMS の実施において雛形とされ，世界中の多くの企業が参照し，基軸としている．

情報セキュリティ国際規格化の中心 ISO/IEC JTC1/SC27 で ISMS 規格群を策定

ISO/IEC JTC1/SC27 では，上記２つの重要な規格のほかに，多くのガイドラインを策定している．例えば，ISO/IEC 27003（ISMS 実施のガイドライン）は，ISO/IEC 27001 に従った ISMS 認証の準備段階に具体的な実施内容をガイダンスとしてまとめており，ISO/IEC 27004（情報セキュリティマネジメントの測定）は，ISMS の構築においてその有効性を測定する場合の考え方，事例をまとめている．さらに，ISO/IEC 27005（リスクマネジメントのガイドライン）は前述のリスク分析を行うためのガイドラインをまとめている．これらのガイドラインの位置づけは, ISO/IEC 27002 と同じであるが, ISO/IEC 27002 は体系的な管理策を提示しているのに対し，他のガイドラインは ISMS 認証の流れの中で必要となる個々の手続/手順（リスクの分析手法など）を具体化している（図 2 参照）.

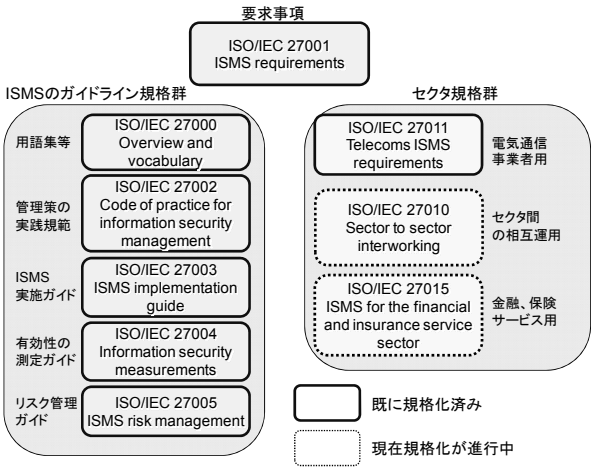

図 2. ISMS ファミリ規格群

2.2 電気通信事業者向けガイドライン策定の背景

2.2.1 我が国における ISMS 認証制度の普及

我が国には，情報処理サービス業のコンピュータシステムが十分な安全対策を実施されているかどうかを認定する制度として，昭和 56 年 7 月 20 日通商産業省告 示 342 号による「情報システム安全対策実施事業所認定制度」（安対制度）が存在した．安対制度は主に技術的な視点を重視した認定制度であったが，組織全体のセキュリティを管理し，要員・組織のセキュリティをも考慮すべきとの声が高まってきた. こうした状況に鑑み，経済産業省では「情報セキュリティ管理に関する国際的なスタンダードの導入および情報処理サービス業情報システム安全対策実施事業所認定制度の改革（平成 12 年 7 月 31 日）」を公表し，従来の安対制度を平成 13 年 3 月 31 日でもって廃止することを決定した．この決定には，2000 年に英国規格 BS 7799（Part2）が ISO/IEC 17799（ISO/IEC 27002 の前身）として国際規格化されたことが大きく影響している．上記の安対制度の廃止，及び国際的な規格化の導入により，時代のニーズに合わせた新しい制度として，情報セキュリティマネジメントシステム（ISMS）適合性評価制度を創設することとなった．本制度における認証の要求事項は，英国規格 BS 7799（Part1）をベースとして，我が国における認証基準を日本情報処理開発協会（JIPDEC）が策定し，それに基づいた ISMS 適合性評価制度が 2001 年に開始された.

2005 年に ISO/IEC JTC1/SC27 では，ISMS 認証の要求事項である ISO/IEC 27001（ISMS 要求事項）を国際規格化したことで，我が国は国際規格をそのままの形で導入することとし, ISO/IEC 27001 の JIS 化を行い, JIS Q 27001 を 2006 年に策定し, ISO/IEC 27001 及び JIS Q 27001 に基づいた ISMS 適合性評価制度へ移行することとなった. その後，図 3 で示すように，世界第 1 位の認証企業数を誇る国に，日本は成長してきた．2010 年 1 月現在で日本の ISMS 取得組織数は 3448 となっており，世界第 2 位の

インドの 484 を大きく引き離している 1)．この成長の背景には，ISMS 認証の取得を実施することによる，「セキュリティ対策済み企業」としてのアピール力強化，ビジネス力の向上，契約数の増加などへの期待が存在する．特に，情報セキュリティマネジメントに関わる「国際規格化」が行われたことにより，認証制度の基軸となる明確な拠り所ができ，国内だけでなく，国際的な相互認証を視野に入れることができたため，特に日本では ISMS 認証が積極的に促進されたと言っても過言ではない．

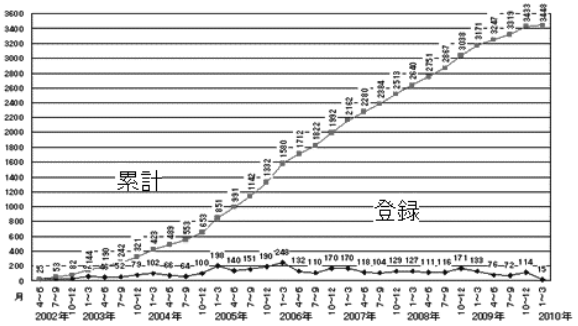

図 3. 日本における ISMS 認証取得企業数の遷移

2.2.2 電気通信事業者向けガイドラインの必要性

情報通信ネットワークは，我が国の社会経済活動を活性化させ，生活をより豊かにするために大いに役立ってきた．また，情報通信ネットワークの安定運用，情報セキュリティの確保については，大手の電気通信事業者を中心に，ISMS 認証取得に向けた活動が目立ってきていた．一方，情報通信ネットワークが我々の日常生活に浸透すればするほど，当該ネットワークの利用者や運用者がウイルス等のマルウェア，DoS 攻撃等の脅威に遭遇する機会が増加するだけでなく，実際にシステム機能不全，またはマルウェア感染の発生により，情報通信ネットワークの安定運用が損なわれる事象が発生していることも事実である．さらに，情報通信ネットワークを運用する側の電気通信事業者においては，通信の秘密の保護，重要通信の優先取扱い，事業者間等の責任分界の明確化など，固有の法令上の要求事項が存在しており，電気通信事業者における情報セキュリティ対策については多くの視点・角度からの検討が必要となってきていた．

以上の状況に鑑みて，情報通信ネットワークの安定性，安全性の確保を担う電気通信事業者には，ISO/IEC 27002 で規定される ISMS に関連した雛形の管理策を用いるだけでなく，上記のネットワーク運用者として想定すべき脅威，電気通信事業者としての特有な法令上の要求事項を十分に加味し，電気通信事業者に適した管理策を導出することが肝要であるとの考えが出てきた．このような検討の必要性の認識の中，総務省では「電気通信分野における情報セキュリティ対策協議会（ISeCT）」（委員長中尾康二（KDDI））を 2006 年に立ち上げ，上記の課題検討の叩き台となる「電気通信事業者のための情報セキュリティマネジメントガイドライン」を策定した．さらに，各重要インフラ事業者（電気，ガス，水道，通信など）に対する「安全基準等」の整備を進める指示が内閣官房情報セキュリティセンターからあったことを受け，本協議会では，技術的視点を中心とした電気通信事業者のため「安全基準等」の策定も実施した．上記２つの本協議会成果物に基づき，本稿の主題である「電気通信事業者のための情報セキュリティマネジメントガイドライン」の国際規格化が開始された．

2.3 国際規格化への経緯

2007 年から ISMS 認証が多くのセクタ（医療，電気通信，IT 業界など）で取得され始めた背景もあり，セクタ向けのガイドライン化の動きが出てきた．一方，電気通信サービスの多くの規格化を担務としている ITU-T では，電気通信事業者向けの情報セキュリティマネジメントの検討を 2003 年より進めており，ISMS 認証を前提とした電気通信事業者向けの情報セキュリティマネジメントのための要求事項（暫定的な要件）として，ITU-T 勧告 X.1051（2004）として規格化を達成していた．

しかしながら，ISO/IEC JTC1/SC27 では，一般的な組織（企業）のための ISMS 要求事項の規格化を 2005 年に ISO/IEC 27001 として完成したため，勧告 X.1051 及び ISO/IEC 27001 の間に不整合が発生した．そのため，ISO/IEC JTC1/SC27 及び ITU-T SG17 は，ISMS 要求事項の枠組みである ISO/IEC 27001 はすべてのセクタに共通とし，電気通信事業者向けの管理策，実施の手引きを拡充していく方向で議論がまとまり，電気通信事業者向けの本ガイドラインを ISO/IEC と ITU-T との共通文書として共同で規格化を進めることとなった（図 1 参照）．一般的に共同規格化は，両方の標準化団体に深く関わっている推進者（本規格では筆者）が必須であり，その推進者における各標準化団体での事前交渉，及び各国からのコメントの調整・対応を円滑に適切に実施していくことが成功の秘訣となろう．

本規格の叩き台の策定段階では，前述の ISeCT の作成した「電気通信事業者のための情報セキュリティマネジメントガイドライン」をベースにドラフトを ITU-T SG17 側で作成したため，多くの管理策，実施の手引きは日本の入力がベースとなった．日本の ISeCT の作成したガイドラインは，ISO/IEC 27002 をほぼ取り込んだ形でまとめ

ていたため，双方の審議で既存規格(ISO/IEC 27002)との冗長性が問題視された．共同審議の結果，できるだけ ISO/IEC 27002 との共通部分は排除し，必要な参照を ISO/IEC 27002 に行い，主に電気通信事業者に特有の管理策，実施の手引きなどの記述を中心に規格をまとめていくこととなった 2)3)．

日本の入力をベースに規格のドラフトを作成

本規格は，ITU-T SG17 及び ISO/IEC JTC1/SC27 の間のジョイントプロジェクトであり，ITU-T SG17 側に上記のベースドキュメント（叩き台）が存在したため，規格立案の NP（新規プロジェクト立案・審査）のフェーズで通常の規格化プロセスとは異なり，加速化プロセスで進めることが合意され，通常のプロセスより多少早く規格完了を実現している（図 4 参照）．しかし，本審議過程においては，ITU-T SG17 及び ISO/IEC JTC1/SC27 の間でコメント処理のやり取りを頻繁に行い，調整を図る必要があったため，作業としてはかなり煩雑となり，お互いのコメントを適切に処理・対応するための調整，及び草案化に多くの時間を割くこととなった．唯一残念なことに，共同文書としてお互いの規格体裁の整備などに多くの時間を要してしまい，発行時期は，通常の発行タイミングより約 1 年遅れの 2009 年となってしまった．

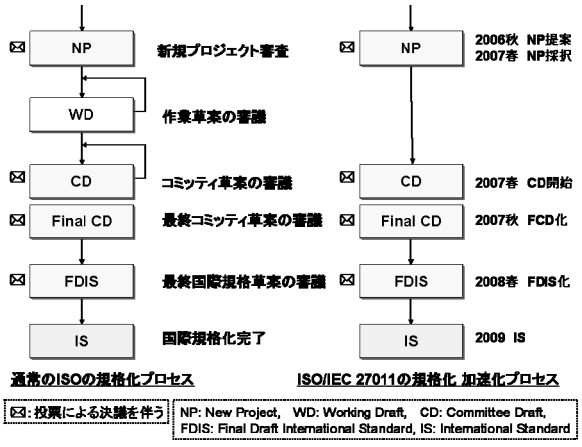

図 4.　規格化プロセス

3. ガイドラインの概要

3.1 ISO/IEC JTC1/SC27 の役割，及び分担

ISO/IEC JTC1/SC27 は特定の応用や業種に限定した技術規格ではなく，一般的に広く適用可能な規格の策定を目指している．本 SC（サブコミッティ）は５つの WG（ワーキンググループ：WG 1 ～WG5）に分かれている．WG1 は情報セキュリティマネジメントシステム(ISMS)に直接的に関連する課題を規格化の対象としている ISO/IEC 27011 は WG1 の課題として策定検討が進められた．また，ISMS に関係する詳細技術に関連する課題については，新しい WG4（セキュリティ制御及びサービス技術，2007 年策定）に委ねられている．その他のワーキンググループは暗号技術(WG2)，セキュリティ評価技術(WG3)，アイデンティティ(Identity)管理及びプライバシー保護技術(WG5)などの審議を実施している．SC27 のワーキンググループ構成を図 5 に示す．

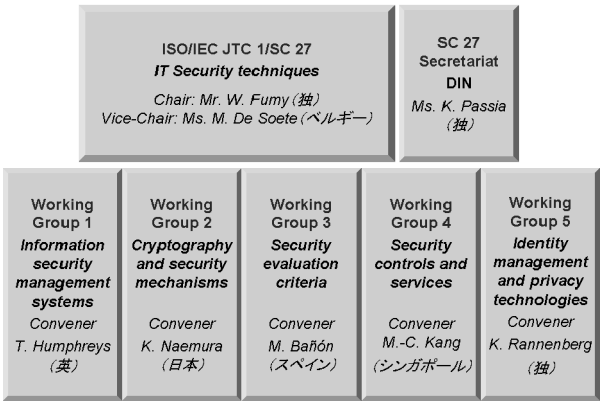

図 5.　ISO/IEC JTC1/SC27 の構成

3.2 ガイドラインの構成

「ISO/IEC 27002 に基づく電気通信事業者のための情報セキュリティマネジメントガイドライン(ISO/IEC 27011(X.1051))」は，ISO/IEC 27002 と同様なフォーマットで構成される（図 6 参照）．具体的には，ISO/IEC 27002 に記載される目的，管理策に追加の情報が不要な場合は，ISO/IEC 27002 への参照のみが記載されており，電気通信分野において特有な管理策，実施の手引きについては，

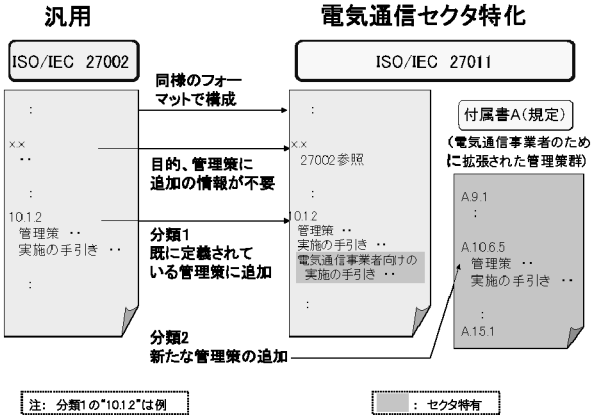

図 6. セクタ規格としての策定手法

付属書 A（規定）に記載される（3.4 節の分類 2）．

さらに，電気通信事業に関連する特定の手引きが必要な管理策の場合は，ISO/IEC 27002 の管理策，及び実施の手引きをそのまま掲載することとし，その後にその管理策に関連する電気通信事業者に特有の手引きを記載する（3.4 節の分類 1）．電気通信分野に特化した実施の手引きや関連情報は，以下の節に含まれており，本稿の 3.4 節で述べる．

（第 6 節） 情報セキュリティのための組織
（第 7 節） 資産の管理
（第 8 節） 人的資源のセキュリティ
（第 9 節） 物理的及び環境的セキュリティ
（第 10 節） 通信及び運用管理
（第 11 節） アクセス制御
（第 12 節） 情報システムの取得，開発及び保守
（第 13 節） 情報セキュリティインシデントの管理
（第 14 節） 事業継続

3.3 電気通信事業者特有のセキュリティ上の考慮点

本ガイドラインの目的は，電気通信事業者がここに記載される管理策に基づいて適切な管理策を導入することにより，効果的な情報セキュリティを確保することである．これらの管理策は，電気通信事業における電気通信設備，サービス，及び業務用アプリケーションにおいて，確立され，実施され，監視され，レビューされ，及び改善される必要がある．組織のいろいろな利用者によって使用される電気通信設備を保有する電気通信事業者は，個人データ，機微データ，及びビジネスデータなどの情報を処理するために，最大限の注意を払うことが望ましく，適切なレベルの保護を適用することが望ましい．結果的に，電気通信事業者は，適切なセキュリティ管理策が確保されていることを確実にする総合的な ISMS を確立し，継続的に改善することが必要となる．

DoS，スパムなど脅威から電気通信設備，サービス，業務用 AP を守る

本ガイドライン策定において考慮された管理策は，以下の電気通信特有のセキュリティ要件に起因している．

- 大惨事におけるサービス可用性（特に緊急サービス）を含め，提供されるネットワーク及びサービスの信頼性に対する顧客／加入者の要請
- サービスの可用性，公平な競争，及びプライバシー保護を確実にするための，訓令，規制，法令によるセキュリティに対する公的権威者の要請
- 運用・事業利益を保護し，顧客・国民に対する責務を果たすことを目的とした，セキュリティに対するネットワーク運用者及びサービス提供者自身の要請

更に，本ガイドラインにおいては，電気通信事業者が以下のような環境的，及び運用的なセキュリティインシデントを考慮することを推奨している．

- 電気通信サービスは，ルータ，交換機，ドメインネームサーバ，転送リレーシステム，ネットワーク管理システム（NMS）などが相互に連結している設備に強く依存しているため，電気通信におけるセキュリティインシデントは，様々な装置/設備で発生しうるものであり，そのインシデントは，ネットワークを経由して他の装置/設備に瞬く間に伝播する恐れがあること．
- 電気通信設備に加えて，ネットワークプロトコル，及びネットワークトポロジーの脆弱性により，深刻なセキュリティインシデントが生まれる可能性もある．特に，NGN（Next Generation Network）等における有線と無線の融合により，相互運用性を確保できるプロトコルを開発する重要な試みも必要となってくること．
- 電気通信事業者の主要な関心事は，ネットワークの停止を引き起こすセキュリティ侵害の見極めであり，ネットワークの停止は，顧客との関係，収入減，及び復旧コストの観点から極めて高コストとなりうる．国の電気通信インフラの可用性に対する熟考された攻撃は，国家のセキュリティ問題とみなすことが出来ること．
- 電気通信事業者のマネジメントネットワーク及びシステムは，ハッカーの侵入を受けやすい．そのような侵入のための共通な動機は，電気通信サービスを対象とした窃盗行為である．このような窃盗行為は，診断機能を使い，会計記録を改ざんし，プロビジョニング・データベースを改変し，加入者通話を盗聴するなどの様々な方法により，巧みに実装されていること．
- 外部からの侵入に加えて，事業者は，ネットワーク

管理データベースの不正な改ざんや権限の無い人の設定変更などの内部から発生するセキュリティ侵害を懸念すること.

本ガイドラインは，電気通信事業者における情報セキュリティマネジメントの導入において不可欠であるセキュリティ管理策を，上記の電気通信事業特有の考慮点に基づき整理・指針化した.

電気通信事業者に不可欠なセキュリティ管理策を整理・指針化

3.4 電気通信事業者特有の管理策

本ガイドラインで策定した電気通信事業者特有管理策は，ISO/IEC 27002 に基づき，主に以下の 2 種の区分がなされる（図 6 参照）:

- ●分類 1：　ISO/IEC 27002 に既に定義されている管理策に対し，電気通信事業者向けの「実施の手引き」などを追加している管理策.
- ●分類 2：　ISO/IEC 27002 に存在しない新たな管理策.

分類 1 に属する管理策は，図 7 の「10.1.2　変更管理」（斜体字）の例に示されるように，「電気通信事業者向けの実施の手引き」が ISO/IEC 27002 の実施の手引きに追加されている．分類 2 に属する管理策は，本ガイドラインの付属書 A（電気通信事業者のために拡張された管理策群：規定）に記載され，図 8 の「A.10.6.5 DoS/DDoS 攻撃対応」の例に示すとおり，ISO/IEC 27002 には規定されない電気通信事業者向けの新たな管理策である.

図 8 のような付属書 A（規定）に記載される電気通信事業者特有の管理策は，以下に示す分野に跨る:

A.9.1 セキュリティを保つべき領域
　A.9.1.7 通信センターの安全確保
　A.9.1.8　電気通信設備室における安全確保
　A.9.1.9　物理的に隔離された運用区画
A.9.3　自社の管理外の場所に設置する設備のセキュリティ
　A.9.3.1　他の電気通信事業者の領域に設置する設備
　A.9.3.2　電気通信サービス加入者の領域に設置する設備
A.9.3.3　相互接続の電気通信サービス
A.10.6 ネットワークセキュリティ管理
　A.10.6.3　電気通信サービス提供におけるセキュリ

10.1.2 変更管理
管理策
情報処理設備及びシステムの変更は，管理することが望ましい.
実施の手引
運用システム及び業務用ソフトウェアは，厳格な変更管理の下に置くことが望ましい.
特に，次を考慮するのが望ましい.
a)　重要な変更の特定及び記録
b)　変更作業の計画策定及びテスト実施
c)　そのような変更の潜在的な影響（セキュリティ上の影響を含む.）のアセスメント
d)　変更の申出を正式に承認する手順
e)　すべての関係者への変更に関する詳細事項の通知
f)　うまくいかない変更及び予期できない変更を，中止すること及び復旧させることに対する手順及び責任を含む，代替手順
装置，ソフトウェア，又は手順に対するあらゆる変更の十分な管理を確実にするためには，正式な責任体制及び手順を備えていることが望ましい．変更がなされたときには，変更にかかわるすべての関連情報を含んだ監査ログを保持することが望ましい.
電気通信事業者向けの実施の手引き
電気通信事業者は，施設の新設，移転，及び撤去の手順及び記録を考慮することが望ましい.

図 7. 分類 1 の事例（変更管理）

A.10.6.5 DoS/DDoS攻撃対応
管理策
電気通信事業者は，電気通信サービスのために良好な環境の整備を図るために，DoS/DDoS攻撃への対応方針を定め，適切な対策を実施することが望ましい.
実施の手引き
電気通信事業者がDoS/DDoS攻撃の存在を認識した場合は，電気通信事業者は，電気通信設備の安定運用継続のため，適切な対策を講じることが望ましい.
必要とされる具体的な対策については，DoS/DDoS攻撃の種別によって異なるが，以下のような対策を考慮することが望ましい.
攻撃時の対象被害サイトへのパケットのフィルタリング
DoS/DDoS攻撃で使用される通信ポートの制限
対象となる電気通信設備の縮退運転，又は運転一時停止
DoS/DDoS攻撃の発信者が自社の電気通信サービス加入者であることが判明した場合は，電気通信設備に対するDoS/DDoS攻撃を阻止するために，電気通信事業者は，当該発信者への電気通信サービスを一時停止することが望ましい.
電気通信設備を相互に接続している他の電気通信事業者経由のDoS/DDoS攻撃がある場合，当該他の事業者に対しDoS/DDoS攻撃を停止するための必要な措置を要請することが望ましい. また，要請を受けた事業者は，その要請に対し適切な対応を実施することが望ましい.
DoS/DDoS攻撃への対策の効果をあげるため，電気通信事業者は，他の電気通信事業者，及び国内外のサイバー攻撃対策組織との協力を密に行うことが望ましい.

図 8. 分類 2 の事例（Dos/DDoS 攻撃対応）

ティ管理
A.10.6.4 スパムメール対応
A.10.6.5 DoS/DDoS 攻撃対応
A.11.4 ネットワークアクセス制御
A.11.4.8 電気通信サービス利用者による電気通信事業者の識別及び認証
A.15.1 法的要求事項の順守
A.15.1.7 通信の秘密
A.15.1.8 重要通信の確保
A.15.1.9 緊急時対応の適合性確保

3.5 ガイドラインの活用方法，及び影響

本ガイドラインの利用者は ISP 事業者，データセンタ事業者，ASP 事業者，モバイル通信事業者などの広義の電気通信事業者を想定している．ISMS の運用・構築を考慮している各電気通信事業者は, ISO/IEC 27001 にある ISMS 要求事項に順守した形でマネジメントプロセス（PDCA）をまわす．具体的な管理策の選択･適用については，始めに ISO/IEC 27002 に基づく一般的な管理策を考慮・検討することとなるが，各電気通信事業者に特有の管理策の実施を考慮するにあたり，本ガイドライン ISO/IEC 27011 を用いて, 更なる管理策及び実施の手引きの適用・選択を検討するアプローチをとることが望ましい．特に，本ガイドラインの付属書 A は，ISO/IEC27001 に適合することを意図した ISMS の運用の中で，これらの電気通信事業者特有の管理策を実施することを推奨しており，また，この附属書に規定された管理策を組織の適用宣言書に含め, 拡張することが望ましいとしている．

今後の雛形となる ISMS 初のセクタ規格

具体的には，各電気通信事業者におけるリスク評価の過程で，例えば DoS やスパムに関する脅威，及びシステムへの影響が大きいとの分析がなされたと仮定する．これまでの ISO/IEC 27002 の管理策においては，上記のような脅威，リスクに対して直接的に有効な管理策の記述はなく, 一般的なシステムのトラブルとして扱っていた．本ガイドラインには，このように電気通信事業者にとって特に考慮すべき管理策，実施の手引きが推奨されており，これらの管理策，実施の手引きを積極的に活用することにより，電気通信事業者の情報セキュリティレベルの大きな向上，情報ネットワークの安定運用に資することができると考える．すなわち，本ガイドラインの適用により，電気通信事業者において想定される特有のリスクに対する対策がより具現化され，事業者にとって必要となる管理策の実施に向けた活動か容易になるといった利点が挙げられる．

ISMS 認証の取得・運用はコストがかかり過ぎ，その有効性が不透明であるなど問題点も多いが，現状の通信ネットワークに関わる脅威，リスクに対する十分な対策の実施は, 特に電気通信事業者にとっては生命線であり，的確なリスク分析，及び適切な管理策の選択・実施が最重要課題のひとつと言えよう．本ガイドラインは，2009 年の規格化であるため，現在のところ十分な通信事業者への定着は見られない．しかし，本規格が日本発で規格内容・背景を熟知しているという強みを活かせば，規格活用のためのユーザガイドや適用事例を国内規格（TTC など）として充実させることにより，特に日本国内の電気通信事業者のネットワーク安定運用/情報セキュリティ強化に資することができると考える．

これまで個々の電気通信事業者が独自で進めていた脅威分析，セキュリティ対策の実施には限界があり，今後は電気通信事業者間の対策連携（インシデント情報等の共有）などの施策も重要となる．その意味で，本ガイドラインは電気通信事業者間の連携施策をも視野に入れており，ISMS 認証取得・運用の目的に限らず，多くの電気通信事業者にとって共通に活用できる国際規格として策定した．また，ISMS 関連規格で特定セクタ向けとしては初めての ISO ガイドライン化を実現し，今後の他セクタにおける検討の雛形を与えたことは，電気通信分野だけでなく，多くのセクタ分野へインパクトを与えたと言えよう．

4. 今後の規格化の進展と展開

4.1 規格化作業の今後

4.1.1 認証審査の基準との連携

現状の ISO/IEC 27011 は，ISO/IEC 27002 と同様に「ガイドライン」としての位置づけとなっており，ISO/IEC 27011 に記載される管理策については, ISMS 認証審査の対象にはなっていない. 従って, 電気通信事業者が ISMS の認証取得・運用を推進する際，これらの新しい管理策がない状態でも, ISMS 認証取得，または ISMS 更新を行うことが可能となる．本ガイドラインは電気通信事業者に必要とされる管理策（通信の秘密など）などが記載されているため，「ガイドライン」より多少なりとも「要求事項」に近い位置づけにシフトされることが望ましい．

具体的な方法論としては，ISO/IEC 27001 の付属書 A を拡張して ISO/IEC 27011 の付属書 A を取り込む方法や，電気通信事業者セクタの標準化機関である ITU-T においてより要求事項に近い形で本ガイドラインの付属書 A を位置づけるなどの方法が考えられる．幾つかの方法論からの選択については，今後規格化がなされていく他セクタ（銀行，医療など）との歩調を合わせることにより，電気通信事業者のためのセキュリティ確保に向けた基準化がなされていくことが望ましい．

ガイドラインから要求事項へのシフトが望まれる

4.1.2 ISO/IEC 27011 の定期見直し

ISO/IEC JTC1/SC27 では，すべての規格に対して定期的（5 年を目処）な見直しを実施している．ISO/IEC 27011 は 2009 年に規格として発行されたため，その 4 年後（2013 年）からその見直し作業の検討を開始し，見直しの必要性が合意された場合は，2014 年から見直しの作業に入ることとなる．一方，ISO/IEC 27011 のベースとなっている ISO/IEC 27002 の見直しを現在（2009 年）進めているが，かなり大きな変更が余儀なくされる状態になっている．従って，今後，ISO/IEC 27011 の保守を進めるにあたり，これまでと策定方法が変わらないと仮定すると，新たな ISO/IEC 27002 改訂版をベースとした見直し作業を実施する必要がでてくる．ただし，今後の ISO/IEC 27011 の規格化の方向としては，別の規格への依存度を極力低くし，電気通信事業者のための管理策のみに特化した規格をわかりやすい形で作っていく必要があると考える．

4.2 今後の展開

ISO/IEC JTC1/SC27 WG1 では，ISMS 関連規格の審議を進めており，電気通信事業者向けの ISO/IEC 27011 だけでなく，以下に示すセクタに向けた規格化審議を現在（2009 年秋）進めている．いずれの審議も作業文書（Working Draft）の段階であり，まだ検討の緒についたばかりである（図 2 参照）．

- ISO/IEC 27010：Sector to sector interworking and communications for industry and government
- ISO/IEC 27015：ISMS for the financial and insurance service sector

一方，医療セクタについては，ISO/IEC 27011 の検討以前に ISO TC215（Health informatics）において検討が開始されており（図 1 参照），ISO/IEC 27011 と同様に ISO/IEC 17799（ISO/IEC 27002 の前身）を参考としたセキュリティマネジメントの規格 ISO 27799（ISO/IEC 17799 を用いた医療におけるセキュリティマネジメント）が策定された．本医療の国際規格は，日本の財団法人医療情報システム開発センタ（MEDIS-DC）の支援で策定されたが，ISO/IEC 27011 とは大きく異なり，医療セクタの要求事項，ガイドラインの両方が混在している規格となっている．

今後の展開としては，汎用性のある ISMS 関連基準・ガイドラインだけではなく，特定のセクタにおけるより具体的な管理策，実施のガイドラインなどの規格化がさらに重要となってくると考える．本稿で述べた電気通信事業者セクタの規格である ISO/IEC 27011 は，ISO/IEC JTC1/SC27 におけるセクタ規格の第 1 号であり，ISO/IEC 27002 の活用方法，セクタ要件を加味した実施の手引きの記載方法，新しい管理策の策定方法など，今後のセクタ規格ドキュメント策定の雛形として評価されており，その意味でも日本が主導で策定した ISO/IEC 27011 の価値は高いと判断する．

ISO/IEC 27011 に関連する今後のアプローチとしては，早々な国内規格化（JIS/TTC）を進め，電気通信事業者での活用方法としてのユーザガイド，さらには ISMS 認証との関係を整理していく必要があると考える．一例としては，英国にある T-SCHEME がセクタレベルの認証を既に実現しているが，我が国を取り巻く環境（参考となるベストプラクティス）などを十分考慮し，今後の施策としてベストの道を探求すべきであろう．

5. おわりに

ISO/IEC JTC1/SC27 及び ITU-T において共同で策定された電気通信事業者のための情報セキュリティマネジメントガイドライン（ISO/IEC 27011）の規格化作業について概観した．近年の IT 社会の浸透により，セキュリティ技術はすべての分野，領域に深く関連している状況にある．その中で，セキュリティ基盤としての暗号・認証技術，製品のセキュリティ評価技術，ネットワーク/アプリケーションのセキュリティ技術などの検討・規格化は重要であると位置づけられているが，企業（特にセクタ事業者）の視点からみた情報セキュリティマネジメント技術は今後の情報セキュリティを推進するために最も重要な技術であると言える． 特に，本稿で述べた電気通信事業者に特有のセキュリティガイドラインは，通信事業者に対して管理策，実施の手引きとして影響があるだけではなく，

他セクタ（金融など）に対してもガイドライン策定方法のベストプラクティスとして影響が大きいと言えよう．ISO/IEC JTC1/SC27 は，情報セキュリティマネジメント技術の規格化を推進している最も活性化した組織であるが，日本としても積極的な ISMS 関連規格化への引き続きの貢献が多く期待されるところである．

引き続き日本の積極的な規格化への貢献を期待

謝辞 本ガイドライン国際規格化にご協力をいただいた，ISO SC27 国内委員会メンバに感謝します．

参考文献

1) http://www.iso27001certificates.com
2) Koji Nakao: Standardization Overview on Information Security Management Guidelines for telecommunications, ISO SC27 INDUSTRY SEMINOR (Oct. 2007).
3) Koji Nakao: Overview of Information Security Management Activities Undertaken within ITU-T SG 17 and ISO/IEC JTC1/SC 27, Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (Aug. 2007).

中尾 康二（正会員）
E-mail：ko-nakao@kddi.com
著者略歴： 1979 年 早稲田大学卒業後，国際電信電話（株）に入社．KDD 研究所を経て，現在 KDDI（株）情報セキュリティフェロー，及び独立法人 情報通信研究機構（NICT）セキュリティセンター インシデント分析 G リーダー兼務．ネットワーク及びシステムを中心とした情報セキュリティ技術に関わる技術開発に従事．電子情報通信学会，情報処理学会などの会員．2002 年より早稲田大学非常勤講師．情報処理学会研究賞，経済産業省大臣賞，文部科学大臣賞等を受賞．

投稿受付：2010 年 1 月 18 日
採録決定：2010 年 2 月 8 日
メンタ：安信千津子（日立コンサルティング）