研究ノート

IT ガバナンスに基づくガイドラインの展開に向けた提言
経済産業省「システム監査基準」「システム管理基準」に対する継続的改善

Proposal for Advanced Guidelines Based on IT Governance
Continuous Improvement of “Systems Audit Standards” and “Systems Management Standards” of METI

神橋　基博
Motohiro Kambashi

情報セキュリティ大学院大学　情報セキュリティ研究科
Graduate School of Information Security, Institute of Information Security

概　要

経済産業省は 2018 年 4 月に「システム監査基準」及び「システム管理基準」の改訂版を公開した。

今回の改訂は IT ガバナンスを中核に置き、クラウドサービスやアジャイル開発といった前回 2004 年の改訂後に普及した情報技術及び情報システムの利用に関する変化を取り込むことを主眼とした。IT ガバナンスに関する従来の研究を踏まえ、今回改訂された「システム監査基準」「システム管理基準」について、IT ガバナンスの観点から要点を示し、今後の展開に向けて検討すべき項目を提言する。

キーワード：システム監査基準、システム管理基準、IT ガバナンス、EDM モデル

1．はじめに

経済産業省は、経済・社会に不可欠なものとなっている情報システムに対して、そのリスクを適切にコントロールするための手段の一つとしてシステム監査を位置付け、システム監査を実施する監査人の行為規範及び監査手続の規則を規定した「システム監査基準」、システム監査人の判断の尺度を規定した「システム管理基準」を公表している。

2018 年 4 月 20 日に改訂されたシステム監査基準ではシステム監査を「情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型」[1] とし、IT ガバナンスが対象として含まれることを明確化している。

また、システム管理基準では、「これまで以上に IT ガバナンスの実現に貢献すること」[2] を改訂の主旨に掲げ、IT ガバナンスを実現する際のガイドラインであることを示している。

このように、「システム監査基準」及び「システム管理基準」の改訂において、IT ガバナンスが重要な役割を果たしている一方で、従来の IT ガバナンスに関する研究では、研究者毎に異なる IT ガバナンスの定義、内容が示されている。

本稿は、IT ガバナンスの観点から、2018 年 4 月における「システム監査基準」および「システム管理基準」改訂点を示すと共に、今後の改善に向けた提言を行うことを目的とする。

そのため、本稿では、2 章において、「システム監査基準」及び「システム管理基準」制改訂の経緯を示し、3 章で IT ガバナンスに関する従来の議論、標準化の動向を整理する。その上で、4 章で IT ガバナンスの観点から 2018 年 4 月の改訂内容を示し、5 章で今後の改善に向けた提言を行う。

なお、以降の議論においては、2018 年 4 月の改訂前、改訂後を区別するため、改訂前のシステム監査基準を「旧監査基準」、システム管理基準を「旧管理基準」､改訂後のシステム監査基準を「新監査基準」、システム管理基準を「新管理基準」と表記し、旧監査基準と旧管理基準を纏めて「旧基準」､新監査基準､新管理基準を纏めて「新基準」、新旧区別せずシステム監査基準、システム管理基準を総称する際は「両基準」と表記する。

また、本稿の内容はあくまでも筆者の個人的見解であり、経済産業省、その他の特定の団体の見解

投稿受理日	2018 年 7 月 20 日
再投稿受理日	2018 年 12 月 19 日
査読完了日	2019 年 1 月 30 日

を示すものではない。

2．改訂の経緯

両基準の制改訂の経緯を表 1 に示す。

まず、1985 年 1 月に通商産業省によってシステム監査基準が策定された。当初、システム管理基準は存在しておらず、システム監査基準の「実施基準」として包含されていた。

2004 年 10 月に経済産業省によって二度目のシステム監査基準の改訂が行われた。その際にシステム監査基準からシステム管理に係る項目を抜出し、修正を加えたものとして「システム管理基準」が公開された。

2007 年にシステム管理基準追補版が公開されるものの、財務報告に係る内部統制で求められる IT への対応、いわゆる J-SOX のガイドラインであり、システム管理基準本文の改訂ではない。

2016 年 12 月に、経済産業省は日本システム監査学会、日本システム監査人協会、IT ガバナンス協会、ISACA 東京支部に協力を要請し、事前検討を開始した。事前検討では情報システムの管理者・利用者の立場を代表する様々な団体にヒアリングを行い、システム監査及びシステム管理に対する課題・要望をヒアリングした。また、検討会は 2017 年 8 月に立ち上げられ、改訂内容の具体化について議論した。

これらのヒアリングで寄せられた課題・要望、及び検討会で議論された内容は公開されていないことから、筆者の観点で整理した旧基準の課題を付表 1 に示す。

表 1 両基準における制改訂の経緯
（システム監査学会 30 年史 [3] を基に筆者が作成）

1985 年 1 月	通商産業省「システム監査基準」公開
1996 年 1 月	通商産業省「システム監査基準」改訂
2004 年 10 月	経済産業省「システム監査基準」、「システム管理基準」改訂
2007 年 3 月	「システム管理基準追補版」公開
2016 年 12 月	有志検討会による事前検討開始
2017 年 8 月	システム監査に関する検討会による検討開始
2018 年 4 月	経済産業省「システム監査基準」「システム管理基準」改訂

3．先行研究における IT ガバナンス

本稿で取り扱う IT ガバナンスについて、従来の議論、及び本稿が依拠する国際標準について以下で述べる。

3．1．IT ガバナンスとコーポレートガバナンス

新基準では IT ガバナンスを「経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力である」と定義している。[4] IT ガバナンスの定義は、過去の研究より、複数の観点が存在すると考えられる。

Sambamurthy, V. and R. W. Zmud（1999）は、企業が組織内の調整コストの低減に取り組む中、1980 年代の研究によって、情報システムの管理に関する権限が集中化されるか分散化されるかは、コーポレートガバナンスにおける権限の集中化および分散化のパターンを反映しており、IT ガバナンスとコーポレートガバナンスの関連性を示した。

また、1990 年代には、英国において 1992 年にキャドバリー報告書が公開され、1998 年にはコーポレートガバナンスコードが策定される等、コーポレートガバナンスの原則に関する検討を反映し、ITGI（2003）では、IT ガバナンスを取締役会と役員の責務であり、コーポレートガバナンス内に IT ガバナンスを統合すべきと結論付けた。

一方、Urbach, N., A. Buchwald, and F. Ahlemann（2013）は、IT ガバナンスという用語が研究者に用いられるようになったのは、1990 年代初頭としている。

例えば、Henderson, J.C. and Venkatraman, N.（1993）は、組織にとって必要な I/T 競争力（I/T competence）を選択し、使用するためのメカニズムを I/T governance と定義した。この定義においてコーポレートガバナンスの関連は明確にされていないものの、I/T governance の例として、戦略的アライアンス、ジョイント・ベンチャー、クロスライセンス等を挙げ、経営トップ（top management）による戦略を強調していることから、経営陣の関与を前提としていると考えられる。

3．2．IT ガバナンスの標準化

新基準における、IT ガバナンスの概念は、IT ガバナンスの国内規格である JIS Q 38500:2015 を参照している。

JIS Q 38500:2015 は国際標準である ISO/IEC 38500:2008 の内容に、ISO/IEC 38500:2015 と

して検討中の内容を参考に策定されたものである。また ISO/IEC 38500:2008 はオーストラリアにおける IT ガバナンスの規格である AS 8015-2005 を基に提案されたものである。AS 8015-2005 では IT ガバナンスを経営者の責務とし、6 つの原則と共に、Evaluate、Direct、Monitor の 3 つの職務を定義した。

AS 8015-2005 の定義は ISO/IEC 38500:2015 および JIS Q 38500:2015 にも反映され、JIS Q 38500:2015 では、IT ガバナンスにおける経営者の職務を、図 1 に示す通り、評価、指示、モニタの 3 つで表現する。

なお、以降は図 1 のモデルを AS 8015-2005 の定義における Evaluate、Direct、Monitor の頭文字を取って EDM モデルと呼ぶ。

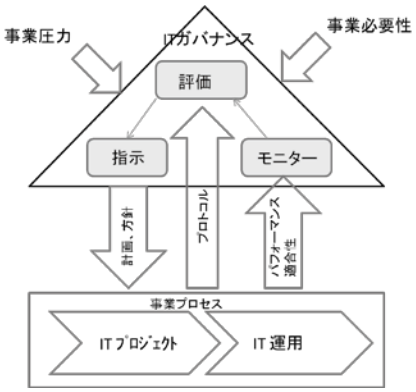

図 1　JIS Q 38500:2015 における
IT ガバナンスのモデル [5]

4．新基準における IT ガバナンス

本章では、付表 1 より新基準における変更点の内、IT ガバナンスの観点を含むものを記載する。各変更点は、(1) 課題認識、(2) 変更箇所として整理した。

4．1．経営陣の観点に基づく構成

(1) 課題認識

新管理基準において、「大企業のみならず中小企業においても情報システム化戦略、情報システム化実践に関わる適切な自己診断及び監査実践を可能にする」および「情報システムにまつわるリスクを適切にコントロールしつつ、これまで以上に IT ガバナンスの実現に貢献する」[6] と記載されているように、組織の規模に関わらず、IT ガバナンスは経営陣の職務であり、両基準はシステム管理者だけでなく、経営陣も活用できるものとすることが望ましい。

しかしながら、旧監査基準では、「Ⅲ．一般基準」、「Ⅳ．実施基準」、「Ⅴ．報告基準」の 3 つの章に 20 項目のガイドラインが箇条書きされており、旧管理基準では、「Ⅰ．情報戦略」から「Ⅵ．共通業務」の 6 つの章に分けて、287 項目のガイドラインが箇条書きされていたものの、各ガイドラインにおいて実施主体は必ずしも明記されていなかった。また、記載内容も簡素であり、IT 及びシステム監査の基礎知識を持たない経営陣にとっては理解が困難なものとなっていた。

(2) 変更点

新基準では、経営陣にとっての判り易さを目的とした構成の変更が行われた。

新監査基準においては、システム監査に馴染みの無い経営陣にも理解しやすくするために、システム監査の流れに即して基準の順序が変更された。また、各基準について、「主旨」にて基準の意図を示し、「解釈指針」にて実践にあたって考慮すべき詳細を記載することで、要点を把握することを容易にしながら、実務に耐えるものとしている。

新管理基準においては、領域毎の章立てとなっていたことから、章立てそのものには大きな変更は行われなかったものの、新監査基準と同様に「主旨」にて意図を、「着眼点」として詳細を記載するよう変更された。

その結果、システム監査基準における基準は 20 項目から 12 項目、システム管理基準では 287 項目から 271 項目に削減されたものの、各基準に対する記載内容が増えたことから、ページ数はシステム監査基準で 4 ページから 38 ページへ、システム管理基準で 12 ページから 116 ページと大幅に増加された。

加えて、従来から両基準を利用していた企業が新基準を継続することを容易にするために、新旧対応表が併せて公開されている。

4．2．IT ガバナンスの明確化

(1) 課題認識

新基準では IT ガバナンスを中核に据えていることから、IT ガバナンスを明確に提示することが望ましい。

しかしながら、旧監査基準では、システム監査を「組織体の情報システムにまつわるリスクに対

するコントロールが適切に整備・運用されていることを担保するための有効な手段」、および「組織体のITガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。」[7]とするものの、システム監査がどのようにITガバナンスの実現に寄与するかは記載されていなかった。
また、旧管理基準では、「ITガバナンスの方針を明確にすること」[8]という基準を定めていたものの、ＩＴガバナンスの方針には何が含まれるべきかについて具体的に記載されていなかった。

(2) 変更箇所

新基準においてはITガバナンスとしてEDMモデルが採用された。
しかしながら、ITガバナンスを明確化するにあたって、JIS Q 38500:2015では、システム管理基準と同等水準まで具体化されたものとはなっていなかった。
一方、旧管理基準では「Ｉ．情報戦略」において「全体最適化」という用語が、「全体最適化の方針」、および「全体最適化計画」という表現で20か所に出現していた。旧管理基準における「最適化」は、各府省CIO連絡会議（2003）におけるシステムの一元化による業務・システムの効率化・合理化を目的とした計画から引用したものであり、一般的にはダウンサイジング等と呼ばれる概念である。また、「最適化」は本来、線形計画法などの規範的決定理論で用いられる概念であり、静的な条件下で方程式を解くような誤解を生じる恐れがある。

一方、組織全体の「方針」および「計画」を示すという点ではEDMモデルの「指示」の一部と見做すことが可能である。そのため、旧管理基準における「Ｉ．情報戦略」を新管理基準では「Ｉ．ITガバナンス」に対応付け、旧基準における「全体最適化」の記載内容をITガバナンスとして読み替えが行われている。

読み換えに際して、旧管理基準の内容はEDMモデルを用いて、「評価」「指示」「モニタ」として整理された。例えば、情報システム戦略の評価に関して「経営陣は、経営計画で示した事業の方針及び目標に基づいて、情報システム戦略を評価していること。」[9]、指示に関して「経営陣は、情報システム戦略の策定を情報システム戦略委員会等に、指示していること。」[10]、モニタに関して「経営陣は、情報システム戦略を関係者への周知徹底を指示することと、その結果をモニタすること。」[11]というように、「評価」・「指示」・「モニタ」を意味する動詞を用いて具体化されている。

4．3．アジャイル開発[1]への対応

(1) 課題認識

変化の激しい経営環境において、情報システムも短期間での修正や機能追加が求められる。このような経営からの要請に応える開発手法として近年、アジャイル開発が注目されている。アジャイル開発では利用可能なサービスを短期間でリリースすることを繰り返す（以下、反復開発）ことで、開発プロセスの継続的改善を目指す。

しかしながら、既存の調査においてIPA（2010）は、日本においてアジャイル開発の普及が遅れていることを課題とし、IPA（2012）では、アジャイル開発の認知度が高まるものの、アジャイル開発を導入することで生産性、品質、コストに関する問題が解決するという誤った認識が生じていることが指摘されている。

その一方で、アジャイル開発について、明示的な規格や標準は存在しない。例えば、アジャイルソフトウェア開発宣言（2001）における「アジャイルソフトウェアの12の原則」はアジャイル開発に取り組む際の規範であり、特定の方法論、プロセス、ツールを推奨するものではなく、ウォーターフォール型開発[2]を否定するものでもない。そのため、従来の調査研究におけるアジャイル開発の普及の遅れや誤認識と捉えられている事象はアジャイル開発に対する調査者と調査対象の認識の相違である可能性がある。例えば、あるユーザーがIPA (2013a) において定義される「完全化保守」[3]を準委任契約としてベンダーに委託し、毎月または四半期等で定常的にリリースを行う計画を立てた場合を想定する。この場合、ユーザーは契約した工数の範囲内で要件を調整することとなり、「アジャイルソフトウェアの12の原則」の内、「動くソフ

1 アジャイル開発とは、変化に迅速かつ柔軟に対応するための開発手法であり、利用部門と情報システム部門が一体となってコミュニケーションの頻度と質を高める点に特徴がある。
2 ウォーターフォール型開発とは、早期に品質の作りこみを行うための開発手法であり、段階を経て実施する点に特徴がある。
3 完全化保守とは、業務の改善に伴う機能要件が変わるときに、利用者のために提供するソフトウェアの性能強化や再コーディングを指す。

トウェアを、2-3 週間から 2-3 ヶ月というできるだけ短い時間間隔でリリースします。」及び「ビジネス側の人と開発者は、プロジェクトを通して日々一緒に働かなければなりません」を充足可能である。[12]

一方､ユーザーおよびベンダーの認識は「アジャイル開発」ではなく､「保守」であり、このような形態が一定数存在する場合、既存の調査研究におけるアジャイル開発の普及率は実態よりも低くなっている可能性がある。また､「アジャイル開発」を自社の「保守」とは異なる開発手法と捉えることで､「アジャイル開発」に対する誤った期待を抱くことが懸念される。

一方、旧管理基準においては、システム開発はウォーターフォール型開発を前提としており、保守業務の対象は明確に定義されていない。IPA (2013a) における保守は「完全化保守」以外にも、発見された不具合を修正する是正保守、環境の変化に対応する適応保守、潜在的な不具合が顕在化する前に修復する予防保守が含まれる。これらを「完全化保守」と区別するために､新基準に「アジャイル開発」を追加する際には､旧基準の「保守業務」と別箇に取り扱うことが望ましい。また、旧基準に基づきウォーターフォール型開発を行う利用者の継続性を考慮し、旧基準の「開発業務」とも別箇に取り扱うことが望ましい。

(2) 変更箇所

新管理基準では IPA（2013b）を参考に、「Ⅲ. 開発フェーズ」､「Ⅵ. 保守フェーズ」とは別章として「Ⅳ. アジャイル開発」が追加されている。また、経営陣の理解を容易にするため、反復開発の説明に項が割かれている。

旧管理基準からの利用者にとって、従来の開発手法を維持する場合、「Ⅲ. 開発フェーズ」および「Ⅵ. 保守フェーズ」を、そのまま適用することとなり、継続性が確保されている。

なお、アジャイル開発以外の手法として新管理基準では､パッケージソフトウェア､クラウドサービスが「Ⅱ. 企画フェーズ」､「Ⅲ. 開発フェーズ」､「Ⅵ. 保守サービス」､「Ⅶ. 外部サービス管理」で言及されている。また､インフラはクラウドサービス、アプリケーションはアジャイル開発といった場合にも「一つの開発方針につき、複数の開発手法を組み合わせることが可能」[13] というように複数の開発手法を組み合わせる場合についても、新管理基準で言及されている。

4．4．組織への適合

(1) 課題認識

業種や規模によって、組織は異なる構造を有することから、経営陣が IT ガバナンスの向上を図る上で、組織構造を無視することはできない。例えば、大企業にとっては取締役会といった複数の経営者による会議体を備えていることは前提条件であるものの、小規模事業者にとっては CIO を設置することすら困難であるケースが考えられる。

新管理基準において、組織構造を考慮したものとするためには、業種別・規模別に参照すべき基準を示す方式と、共通の基準を組織に合わせて読み替えさせる方式が考えられる。

業種別・規模別に異なる基準を作成する場合、自組織に適合した基準を参照することが可能となり、経営陣にとっての利便性は高い。しかしながら、組織構造の差異は、業種・規模だけでなく顧客や海外展開の有無といった要因も影響する可能性があり、全ての組合せを網羅した基準を策定することは実質的に不可能である。

一方、組織に応じて、共通の基準を読み替える方式では、各組織において新管理基準を読み替える作業が必要となるものの、汎用性に優れている。

(2) 変更箇所

新管理基準では第二の方式が採用された。

図 2 に示すモデルとなる組織構造を示した上で、新管理基準における記載はモデル組織を前提としたものに統一されている。その上で、自組織に適合させる際の手引きとして「システム管理基準の枠組み」が提供されている。

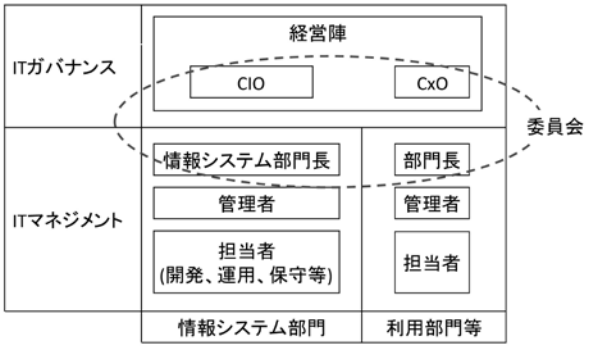

図２　新システム管理基準が想定する組織体制 [14]

新管理基準における読み替えの要点を以下で述べる。

①経営陣

JIS Q 38500:2015 では EDM モデルの担い手を「経営者」としている。しかしながら、多くの組織では取締役会、理事会といった複数名による合議体であること、情報セキュリティ管理基準において「経営陣」という表現が用いられていることから、新管理基準では IT ガバナンスの担い手として「経営陣」が用いられている。

② CIO ／情報システム部門長

新管理基準において、IT マネジメントの担い手は情報システム部門とされている。情報システム部門長が CIO を兼務している場合、CIO は IT ガバナンスまたは IT マネジメントのどちらの担い手かを明確にする必要がある。

一般的には「経営陣の一員として、経営戦略を展開させるための、IT の観点を持った積極的な参加者」[15] というように、CIO は経営陣の一部と見做されている。新管理基準では、CIO を IT ガバナンス、情報システム部門長を IT マネジメントと、役割を明確にするため、別のものとして用いられている。従って、情報システム部門長が CIO を兼任しているケースでは、CIO ／情報システム部門長は経営陣および管理者両方の役割を持つことに留意する必要がある。

③委員会（情報システム戦略委員会，プロジェクト運営委員会等）

組織運営上、組織全体にまたがる利害関係の調整が必要となる意思決定に際しては、複数の部門を含む委員会に検討を委ねることが有用となる。このような委員会は「評価」「指示」「モニタ」に関する経営陣の権限を委譲されており、新管理基準では経営陣の一部と見做されている。

一方、組織内の利害関係の調整が容易、もしくは必要が無い組織において、委員会は必須ではないと考えられる。委員会を設置しない場合は、新管理基準における委員会に関する記述を、経営陣による職務として読み替えることが求められる。

5．今後の改訂を要する箇所

本章では、付表 1 より IT ガバナンスの観点から今後の改訂が望まれる論点について述べる。4 章と同様に（1）課題認識、(2) 今後の改善に向けた提言に分けて整理する。

5．1．IT ガバナンスにおけるシステム監査の位置付け

（1）課題認識

IT ガバナンスに対して、システム監査はどのように貢献するのだろうか。

システム監査は内部監査の一種であり、監査と経営陣の関わりに関しては図 3 に示すような Three Lines of Defense モデル（以降、3LD モデル）が知られている。

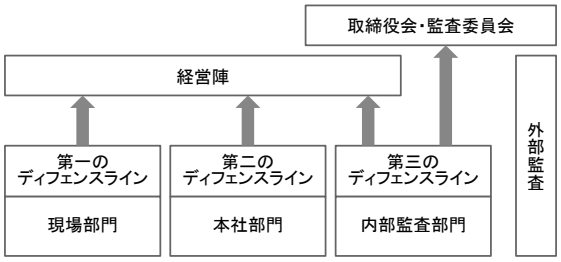

図 3 Three Lines of Defense モデル
参考資料 [16] に基づき筆者が作成

3LD モデルにおいて、システム監査は第 3 のディフェンスラインの位置付けにあり、第 1 および第 2 のディフェンスラインにおける統制状況を経営に報告することを職務とする。

この 3LD モデルに IT ガバナンスを当てはめるためには、2 つのアプローチが考えられる。

第一のアプローチでは、IT ガバナンスに関するシステム監査は EDM モデルの有効性・適切性を検証するものであり、経営陣も監査対象に含まれるとするものである。

第二のアプローチでは、IT ガバナンスに関するシステム監査は EDM モデルそのものではなく、経営陣による「指示」が IT マネジメントに反映されているか、経営陣に対する「モニタ」として報告する内容は IT マネジメントの実態を反映しているかといった適切性に着目する観点であり、経営陣は監査対象に含まれないとするものである。

一般的に内部監査では、対象範囲として「ガバナンス・プロセス、リスク・マネジメントおよびコントロールに関連するすべての経営諸活動を対象範囲としなければならない」[17] と考えられており、第一のアプローチに重点を置いている。一方、内部監査におけるこのような考え方は図 3 に示す通り、執行と監督の分離を前提としたものである。分離が不十分な企業において、監査部門が経営陣

の指揮命令下に置かれる場合、新監査基準で言及されている通り、組織的な独立性が毀損されているとの外観を呈することとなる。[18]

一方、新監査基準では IT ガバナンス監査に対する経営陣のニーズとして、「経営戦略と IT 戦略との整合性、IT 利活用の有効性、企業グループ全体としてみた場合の IT 戦略の合理性についての保証又は助言を提供する」[19] としていることから、第二のアプローチに重点を置いていると言える。

（2）今後の改善に向けた提言

新監査基準ではシステム監査人の独立性に関する基準は定められているものの、内部監査部門の独立性確保に関する基準は含まれていない。そのため、IT ガバナンスの監査において監査対象に経営陣を含めるのであれば、別途、組織的な独立性を確保する方策が必要となる。今後の改善に際しては、日本内部監査協会（2017）等の既存のガイドラインを参考にすることが望ましい。

5．2．アジャイル開発に対する監査手法

（1）課題認識

前章 4.3 では新管理基準におけるアジャイル開発について述べた。

アジャイル開発では、開発チームに大きな権限を委譲することで、迅速なリリースを実現する一方、以下の 2 点に関して従来のシステム監査で取り扱うことが困難と考えられる。

第一に、アジャイル開発においては反復開発の都度、開発プロセスの改善を図るため、システム監査人が監査結果を取り纏める頃には、発見事項が過去のものとなり有効な改善提言とならない可能性がある。

第二に、ウォーターフォール型開発と異なり、アジャイル開発ではドキュメント化を前提としていないため、システム監査人が証跡の提示を求めることで、アジャイル開発のスピードが損なわれる可能性がある。

（2）今後の改善に向けた提言

第一の課題については、システム監査の目的は開発プロセスの有効性の検証にあり、アジャイル開発における継続的改善はシステム監査の必要性を阻害するものではない。この点については、新監査基準における解釈指針で明確化することが望ましい。

第二の課題については、アジャイル開発独自の監査手法が必要となる。新監査基準ではいくつかの方針を例示するに留まっているものの、今後、アジャイル開発に関する監査事例を蓄積することで、より具体的な監査手法が議論されることが期待される。特に、アジャイル開発では、反復開発の短期化、効率化を進めるため、様々なツールにより、プロジェクト管理やテストの自動化を支援していると考えられる。今後の改善に際しては、主要なツールを対象にシステム監査におけるデータ抽出及び分析手法を具体化することが望ましい。

5．3．新しい技術、サービス、枠組みへの対応

（1）課題認識

2004 年における前回の改訂以降、IoT[4]、AI（人口知能）、ブロックチェーン[5]、DevOps[6] 等の IT に関わる数多くの新しい技術、サービスだけでなく、デジタライゼーション[7] やオープン・イノベーション[8] といった一企業を超えた枠組みが生じている。これらの新しい取組みに対して、経営陣が有効性、適切性を検証するためには、その判断根拠となるガイドラインが提供されることが望ましい。このようなガイドラインは、どのような組織体においても適用できるよう、事例や研究を蓄積から、基本的事項を一般化する作業が必要となる。例えば、新管理基準においてアジャイル開発は、IPA（2013b）を参考にし、組織体が留意すべき基本的事項を一般化している。

しかしながら、IoT、AI、ブロックチェーン、DevOps、デジタライゼーション、オープン・イノベーションについては、一般化できるだけの十分な事例や研究が蓄積されておらず、今回の改訂では基準化が見送られている。

（2）今後の改善に向けた提言

今後も、IT 分野ではイノベーションが継続し、新しい技術、サービス、枠組みが出現することが

4　Internet of Things の略。今までインターネットに接続されていなかったモノをインターネットに接続し、情報交換を行うこと。
5　分散型台帳技術(Distributed Ledger Technology)とも呼ばれ、中心となるサーバー無しに取引を記録するためのデータベース技術。
6　ソフトウェア開発において、開発と運用が協力する開発手法
7　商品・サービスについて、企画・開発から製造・流通までをシステムで連携させること。
8　組織内のイノベーションを促進するため、外部の技術、サービス、データ、知見を組み合わせること。

予想される。現時点では存在しておらず、将来に出現する取組みについても、経営陣の関心が高いものについては、システム管理基準に取り込むことが望ましい。そのためには、新しい取組みに対して、定期的に経営陣のニーズを調査し、事例や研究成果を収集する必要がある。しかしながら、両基準の著作権は経済産業省にあり、予算の単年度主義の原則から、そのような活動を実施するために、今回の改訂のような経済産業省が主体となる専門委員会、作業部会を置くことは困難である。従って、新しい取組みへの対応については、両基準の改訂を目的とした専門委員会及び作業部会とは別に常設的な検討体制を構築する必要がある。このような検討体制は有識者及び実務者による公益性を持った活動として実施されることが望ましい。また、新しい取組みに対する経営陣のニーズは、JIPDEC (2018)、JUAS (2018)、総務省 (2018) 等の継続的に実施される調査結果を活用することが望ましい。

なお、これらの新しい取組みへの対応には政策との整合性を確保することが望ましい為、検討体制にオブザーバーとして参加する等、経済産業省の一定の関与が望ましい。

5．4．標準・規格の制改訂への対応

(1) 課題認識

新管理基準の改訂に際して、参照された国際標準、国内規格、デファクトスタンダード等（以降、標準・規格）は新管理基準の参考文献に掲載されている。これらの標準・規格について、前回の改訂を行った 2004 年から今回の改訂を開始した 2017 年までの間における制改訂を付表２に示す。

ISO では制改訂された標準について５年毎にレビューを実施することから、両基準も５年毎に検討することが望ましい。しかしながら、前節と同様に、経済産業省が主体となって検討を行うことは困難である。

(2) 今後の改善に向けた提言

前節と同様に、従来の両基準の改訂を目的とした専門委員会及び作業部会とは別に常設的な検討体制を構築する必要がある。このような検討体制では、新しい技術、サービスだけでなく、標準化団体や研究組織、業界団体による調査結果、標準・規格の制改訂状況の収集・分析を含めることが望ましい。

5．5．小規模事業者向けガイドラインの提供

(1) 課題認識

両基準は大企業のみならず中小企業においても判断の尺度として用いることを目指している。その一環として、前章 4.4 で述べた通り、新管理基準では組織の規模・組織構造に応じた読替えを提供している。

しかしながら、小規模事業者においては、数名もしくは非専従の担当者によって情報システムの企画・開発・運用・保守を担い、ＣＩＯや情報システム部門長に該当する人材が存在しない可能性が想定される。この場合、新管理基準の読み替えでは、経営陣もしくは担当者への負担が大きくなりすぎる恐れがある。

(2) 今後の改善に向けた提言

新管理基準を小規模事業者にも活用してもらうには、基準そのものを簡略化する必要がある。具体的には、新管理基準から必要最低限の項目を抽出し、小規模事業者に適合できるよう記載内容を調整することになる。

従って、小規模事業者に対しては、新管理基準とは別冊として提供することが望ましい。

5．6．自己診断の提供

(1) 課題認識

両基準は大企業だけでなく、中小企業や小規模事業者においても経営陣がシステム監査の活用を図ることを目的としているものの、経営資源の不足により、組織内でシステム監査人を確保することも、外部監査を利用することも困難であることが懸念される。両基準に準拠したシステム監査が困難である経営陣が、それでもシステム管理の改善を図ろうとする場合、より簡易な手段を選択できることが望ましい。

(2) 今後の改善に向けた提言

より簡易な手段として、内部・外部のシステム監査人による支援を受け、経営陣もしくは管理職自身が自らのシステム管理を評価することが考えられる。これは、内部監査における Self-Assessment に類似するものの、内部監査から独立して実施するという点で ISO/IEC 38503 に向けて検討されている”Facilitated”に近い手法である。Self-Assessment、EDM における「評価」、

および”Facilitated”と区別するため、この手法を「自己診断（Self-Diagnosis）」と名付ける。「自己診断」は経営陣自身または経営陣の指示により実施される場合、IT ガバナンスにおける「評価」の手段となる一方で、システム監査人の専門性・独立性・客観性を要求しないことから、システム監査の代替手段とは成りえない。そのため、「自己診断」に関する実施要領は、システム監査基準とは別に検討する必要がある。また、実施要領は、中小企業や小規模事業者での活用を図るため、報告書のサンプル等、新監査基準よりも具体化されることが望ましい。

5．7．グループ会社を跨るシステム監査における守秘義務の取扱い

（1）課題認識

グループ経営を行っている会社群において、グループに属する会社の増加、またはグループ会社の規模の拡大につれて、グループ本社が個々のグループ会社に具体的な指示を出すことが困難となる。その一方で、一つのグループ会社における情報システム開発の遅延やシステム障害、情報漏洩の発生、BCP の失敗等が、他のグループ会社やグループ本社の経営に影響を及ぼす可能性が大きくなる。

グループ本社の経営陣にとっては、グループ本社自身の IT ガバナンスだけでなく、各グループ会社における IT ガバナンスについても、有効性を確認するニーズが生じるものの、グループ会社の全てがシステム監査人材を十分に確保できているとは限らない。従って、グループ本社はグループ会社間でシステム監査人材の効率的な配置を検討する必要がある。グループ会社間でシステム監査人材の共有を図る場合、監査対象となるグループ会社以外のグループ本社やグループ会社とも監査結果を共有する可能性がある。このような状況は、システム監査人としての守秘義務に抵触する可能性があり、監査の目的によって監査結果の開示範囲を検討することが望ましい。そのため、旧監査基準ではシステム監査人の守秘義務を基準としていたが、新監査基準では解釈指針に位置付けを変更されている。

なお、このようなシステム監査人材の共有については、監査対象がグループ本社かグループ会社か、監査人材をグループ本社が出すか、グループ会社が出すかで４通りに類型化することが可能であるものの、グループ会社が自身のシステム監査人材を用いるケースでは、人材の問題が発生しないため、残りの３つの類型について、以下で検討する。

（2）今後の改善に向けた提言

①グループ本社による監査支援

第一の類型として、グループ本社がシステム監査人材の不足しているグループ会社にシステム監査人を派遣し、グループ会社のシステム監査を実施させるパターンが挙げられる。

このようなシステム監査において、対象はグループ会社のシステムであり、監査の依頼者はグループ会社であるものの、グループ本社の経営陣や情報システム部門にも監査調書および監査報告書を参照するニーズがある可能性がある。個々の監査毎に開示の範囲を検討することは却って非効率を招く恐れがあるため、グループ会社全てに適用されるグループポリシー等で、グループ本社からの監査支援を受けた際のシステム監査人の守秘義務の範囲、監査調書、監査報告書の開示の範囲を明確にしておくことが望ましい。

②グループ共通システムの監査

第二の類型として、グループ本社がグループ会社向けに提供するグループ共通システムに対して、グループ本社がシステム監査を実施し、監査調書、監査報告書をグループ会社に提供するパターンが挙げられる。

このようなシステム監査において、対象はグループ本社のシステムであり、監査の依頼者はグループ本社であるものの、グループ会社の経営陣や情報システム部門にも監査調書および監査報告書を提供する必要がある。従って、開示の範囲は対象となるシステムを利用するグループ会社に限定する必要があり、第一の類型のようにグループポリシー等で一律に規定することは望ましくない。個々のシステム監査に対して、システム監査人の守秘義務の範囲、監査調書、監査報告書の開示の範囲を検討する必要がある。

③グループ企業による共同監査

第三の類型として、グループ会社が共同利用しているシステムを対象に、各グループ会社が共同でシステム監査を実施するパターンが挙げられる。

このようなシステム監査では、対象はグループ外のシステムも含まれる。また、直接の監査の依

頼者は共同監査に参加したグループ会社であるものの、共同監査に参加しなかったグループ会社にも監査調書および監査報告書を共有することが求められる可能性がある。ただし、グループ会社数が増えると個々の監査毎に開示の範囲を検討することは非効率を招く恐れがある一方、一律的な開示では共同監査に参加したグループ会社に不公平感が生じることから、持ち回り等で共同監査への参加を強制する、共同監査に参加した会社と不参加の会社で開示範囲に差を付ける等、運用面で対応することが望ましい。

以上、３つの類型について、守秘義務の範囲、開示の範囲を検討したが、具体化にあたては経済産業省（2009）等の既存のガイドラインを参考にすることが望ましい。

５．８．外部委託先による監査報告書の活用

（1）課題認識

前節では、システム監査人材の不足に対して、グループ会社間で共有を図る際の考慮点について考察したが、情報システム部門の人的資源が不足している場合、開発業務や運用業務を外部に委託する選択が可能である。

新管理基準では「Ⅶ．外部サービス管理」において、外部に業務を委託した際の管理に関する基準が記載されている。「Ⅶ．３．１．契約」では、契約書に「再委託の可否（再委託を認める場合は、再委託先が外部委託先と同等の義務を負うこと等責任の所在、再委託時の手続（委託元への届出、委託元の承認等）を明確にすること）」[20]と記載されており、「Ⅶ．３．２．委託先管理」では、「立入監査等では、契約で取り決めた事項に対する遵守状況、情報セキュリティ管理態勢、事故等（サイバーセキュリティ事案を含む）への対応態勢や再委託先（再々委託先以降も含む）の管理状況等を確認すること。」[21]と記載されていることから、外部委託先及びその再委託先、再々委託先が増加するにつれて、委託元による管理負担が増大することが懸念される。

（2）今後の改善に向けた提言

外部委託に対する管理負担の解決策として、外部委託先の管理状況を外部委託先自身に監査させ、委託元に監査報告書を提示する方式が考えられる。このような方式として、STAR 認証[9]やSOC2 報告書[10]といった既存の仕組みを参考にすることが望ましい。

STAR 認証では、セルフアセスメントを実施し、評価レポートを登録した上で、第三者機関による評価を受けるという手順を踏むことから、5.6 で述べた「自己診断」と組み合わせて実施することで効果が期待される。

一方、SOC2 報告書は、大手クラウドサービス事業者が採用したことから利用が広がっているものの、外部委託先に拡大するにあたっては以下の２点を考慮する必要がある。

第一は保証の範囲である。SOC2 報告書はAICPA（2017）が定めた評価の規準に基づいて作成された報告書である。独自項目を追加することが可能であるものの、相応のコストを要することから、中小企業に向けて、委託元のニーズが高い基準に限定することが望ましい。

第二は保証の枠組みである。外部委託した開発業務または運用業務で問題が発生した場合、委託元が最終的な責任を負うこととなる。そのため、委託元は報告書を受領しても、管理負担が削減できない恐れがある。一つの案として、外部委託先の管理業務そのものを外部委託することが考えられる。この場合、委託元が説明責任を確保するためには、従来のシステム監査における「可監査性」[11]の概念を拡張し、開発業務や運用業務の外部委託に際して、後の監査に必要となる証跡を確保できるよう、契約や Service Level Agreement 等に明記する必要がある。このような考え方に類似したものとして、金融庁（2017）は監査報告書の価値向上を目的として「監査報告書の透明化」に関する検討内容を公開しており、今後の改善にあたって参照することが望ましい。

６．おわりに

2018 年４月に経済産業省によって更改されたシステム監査基準、システム管理基準では、IT ガバナンスの観点より、内容を大幅な追加・変更が行われた。

9 米国 Cloud Security Alliance(CSA) によって開発された基準を用いてクラウドサービス事業者のセキュリティの成熟度を第三者が評価するサービス
10 外部委託先が受託している業務について、セキュリティ、機密保持、プライバシー等に関連する内部統制を対象として、監査法人が実施した監査手続きの結果と意見表明が記載された報告書
11 システム監査で必要となるログ等の証跡を確保できるよう、システムの開発段階で設計・実装に盛り込んでおくこと。

経営における IT の重要性が高まる中、多くの組織において IT ガバナンスの向上が求められている。改訂された新監査基準、新管理基準は、経営陣が IT ガバナンスの向上を目指す上での判断尺度として寄与するものである。

一方、変化し続ける環境に適応するために、経営陣は自らの組織における IT ガバナンスを継続的に見直す必要がある。従って、その判断尺度となる両基準も新しい技術、サービス、枠組みの取り込み、標準・規格改訂内容の反映を継続する必要がある。

両基準について、前回から今回の改訂まで 14 年近くを要したことから、両基準の継続的改善を図る体制の確立は喫緊の課題である。
本稿における提言が両基準の今後の改善の一助となれば幸甚である。

引用文献

［1］経済産業省（2018），システム監査基準（平成 30 年 4 月 20 日改訂），p.1
［2］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.1
［3］システム監査学会（2017），システム監査学会 30 年史 1987 ～ 2016 年の歩み , pp.87-94
［4］経済産業省 (2018), システム管理基準 (平成 30［年 4 月 20 日改訂），p.2
［5］JIS Q 38500:2015 情報技術 -IT ガバナンス , 図 1
［6］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.1
［7］経済産業省（2004），システム監査基準（平成 16 年 10 月 8 日改訂），p.1
［8］経済産業省（2004），システム管理基準（平成 16 年 10 月 8 日改訂），p.2
［9］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.10
［10］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.9
［11］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.12
［12］https://agilemanifesto.org/iso/ja/principles.html (2018 年 12 月 1 日)
［13］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.25
［14］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.3
［15］https://cio.go.jp/what (2018 年 7 月 18 日)
［16］Federation of European Risk Management Associations, European Confederation of Institutes of Internal Auditing（2006），Implementation Guidance for Senior Management, FERMA, p7
［17］日本内部監査協会（2017），内部監査基準実務指針 6.0 内部監査の対象範囲 , 日本内部監査協会 , p.1
［18］経済産業省（2018），システム監査基準（平成 30 年 4 月 20 日改訂），p.12
［19］経済産業省（2018），システム監査基準（平成 30 年 4 月 20 日改訂），p.9
［20］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.83
［21］経済産業省（2018），システム管理基準（平成 30 年 4 月 20 日改訂），p.85

参考文献

1）AICPA（2017），Trust Services Criteria, American Institute of Certified Public Accountants, Inc.
2）AS 8015-2005, Australian Standard for Corporate Governance of Information and Communication Technology, Standards Australia
3）Henderson, J.C. and Venkatraman, N.（1993），Strategic Alignment: Leveraging Information Technology for Transforming Organizations, IBM SYSTEMS JOURNAL, Vol. 32 No. 1, pp.472-484
4）ISO/IEC 38500:2008, Corporate governance of information technology, International Organization for Standardization
5）ISO/IEC 38500:2015, Information technology -- Governance of IT for the organization, International Organization for Standardization
6）ITGI（2003），Board Briefing on IT Governance, 2nd Edition, IT Governance Institute
5）Sambamurthy, V. and R. W. Zmud（1999），Arrangements for Information Technology Governance: A Theory of Multiple Contingencies, MIS Quarterly Vol. 23 No. 2, pp.261-290
7) Urbach, N., Buchwald, A., Ahlemann, F. (2013), Understanding IT Governance Success And Its Impact: Results From An Interview Study, ECIS 2013 Completed Research. Paper 55
8）IPA（2010），非ウォーターフォール型開発に関する調査報告書，独立行政法人情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター
9）IPA（2012），非ウォーターフォール型開発の 普及

要因と適用領域の拡大に関する調査～非ウォーターフォール型開発の普及要因の調査～ 調査報告書，独立行政法人情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター
11）IPA（2013a），共通フレーム 2013 ～経営者、業務部門とともに取組む「使える」システムの実現～，独立行政法人情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター
10）IPA（2013b），アジャイル型開発におけるプラクティス活用事例調査 調査報告書 ～調査編～，独立行政法人情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター
12）JIS Q 38500:2015, 情報技術– IT ガバナンス，日本規格協会
13）JIPDEC（2018），IT-Report2018 Spring, 日本情報経済社会推進協会
14）JUAS（2018），企業 IT 動向調査報告書 2018, 日本情報システム・ユーザー協会
15）アジャイルソフトウェア開発宣言（2001），
https://agilemanifesto.org/iso/ja/manifesto.html
（2018 年 12 月 1 日）
16）各府省 CIO 連絡会議（2003），業務・システムの最適化，http://www.e-gov.go.jp/doc/optimization/index.html
（2018 年 12 月 1 日）
17）金融庁（2017），「監査報告書の透明化」について
https://www.fsa.go.jp/news/29/sonota/20170626.html
（2018 年 12 月 1 日）
18）経済産業省（2009），情報セキュリティ監査基準 報告基準ガイドライン Ver1.0,
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf
（2018 年 12 月 1 日）
19）日本内部監査協会（2017），内部監査基準実務指針 6.0 内部監査の対象範囲，日本内部監査協会
20）総務省（2018），情報通信白書平成 30 年度版，
http://www.soumu.go.jp/johotsusintokei/whitepaper/h30.html
（2018 年 12 月 1 日）

付表 1 システム監査基準・システム管理基準 (平成 16 年 10 月 8 日改訂) における主な課題と対応状況

課題			ITガバナンスとの関連	対応状況		本文中の参照箇所
				新監査基準にて対応	新管理基準にて対応	
基準の位置付け・範囲に関する課題	1	国の経済産業政策や経済・企業の動きと協調可能な内容とする。	○	－	×	5.3
	2	情報セキュリティ監査基準、情報セキュリティ管理基準の位置付けを明確にする。	－	○	○	－
	3	各種管理（リスク管理、構成管理、変更管理等）を追加する。	－	－	○	－
	4	ITガバナンスの定義を明確にする。	○	○	○	4.2
基準が対象とする組織体制に関する課題	5	対象とする組織の業態・規模等に合わせてカスタマイズ可能にする。	○	－	○	4.4
	6	組織における責任・権限・役割等を明確にする。	○	－	○	4.4
	7	情報システムに関して組織内に必要となる機能について、実際の部門として構成するための解説を加える。	○	－	○	4.4
	8	利害関係者について、役割と責任を明確に示す。	○	－	○	4.4
基準の書式・記載ルールに関する課題	9	参考文献、参照箇所を明確に示す。	－	－	○	－
	10	作業上の留意点の列挙を見直し、経営者・管理者からの観点で整理する。	○	○	○	4.1
	11	主語と目的語を明確に表現する。	○	－	○	4.1, 4.4
システム監査基準に関する課題	12	監査調書の記載事項、特に監査手続に関する具体例を示す。	－	△	－	－
	13	システム監査の自動化・機械化に関する実証実験を行う。	－	×	－	－
	14	専門の監査人を擁しない小規模事業者でも使えるようなチェックリスト方式にする。	○	×	－	5.5
	15	外部委託先による保証型監査によって、委託元による委託先管理を簡略化する仕組みを導入する。	○	×	－	5.8
	16	ITサービスの提供元による監査実施状況を参照できる仕組みを導入する。	○	×	－	5.8
システム管理基準に関する課題	17	クラウドサービスに対する管理項目を追加する。	－	○	－	－
	18	IoT、AI等の新しい技術領域に対する管理項目を追加する。	○	－	×	5.3
	19	デジタルイノベーション、オープンイノベーションに対する管理項目を追加する。	○	－	×	5.3
	20	サプライチェーンに対する管理項目を追加する。	○	－	×	5.7
	21	サービスマネジメントに対する管理項目を追加する。	○	－	○	－
	22	アジャイル開発やDevOpsに対する管理項目を追加する。	○	△	○	4.3、5.2
基準の維持管理に関する課題	23	旧監査基準・管理基準の利用者に対する緩和措置を用意する。	－	○	○	－
	24	新しい技術、サービス、リスクが発生した際に、必要となる基準を追加可能にする。	○	×	×	5.3
	25	継続的に内容の改善を図ることが可能な仕組みを構築する。	○	×	×	5.3, 5.4
	26	標準、規格、デファクトスタンダードの見直しに合わせ、改訂を実施可能とする。	○	×	×	5.4

付表２ システム管理基準（平成 30 年４月 20 日改訂）が参照した標準・規格・デファクトスタンダード、及び関連する標準・規格を含めた制改訂（平成 16 年 10 月～平成 30 年４月）

標準・規格・ デファクトスタンダード	関連する標準・規格を含めた制改訂(2004年10月～2018年4月)
経済産業省 情報セキュリティ監査基準	2009年 情報セキュリティ監査手続ガイドライン
経済産業省 情報セキュリティ管理基準	2005年 ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management 2006年 JIS Q 27001:2006 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 JIS Q 27002:2006 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の実践のための規範 2008年 情報セキュリティ管理基準(平成20年改正版) 2013年 ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls 2014年 JIS Q 27001:2014 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 JIS Q 27002:2014 情報技術 - セキュリティ技術 - 情報セキュリティ管理策の実践のための規範 2016年 情報セキュリティ管理基準(平成28年改正版)
独立行政法人情報処理推進機構(IPA) 共通フレーム	2004年 ISO/IEC 12207:1995/Amd2:2004 2007年 JIS X 0160 追補1:2007 ソフトウェアライフサイクルプロセス（追補1） 2007年 共通フレーム2007 2008年 ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes 2012年 JIS X 0160:2012 ソフトウェアライフサイクルプロセス 2013年 共通フレーム2013 2017年 ISO/IEC/IEEE 12207:2017 Systems and software engineering -- Software life cycle processes
ISACA COBIT 5	2005年 COBIT 4 2007年 COBIR 4.1 2012年 COBIT 5
JIS Q 38500	2005年 AS 8015-2005 Australian Standard for Corporate Governance of Information and Communication Technology 2008年 ISO/IEC 38500:2008 Corporate governance of information technology 2015年 ISO/IEC 38500:2015 Information technology -- Governance of IT for the organization 2015年 JIS Q 38500:2015 情報技術 - ITガバナンス
JIS Q 22301	2012年 ISO/IEC 22301:2012 Societal security -- Business continuity management systems -- Requirements 2013年 JIS Q 22301:2013 社会セキュリティ - 事業継続マネジメントシステム - 要求事項
JIS X 0161	2006年 ISO/IEC 14764:2006 Software Engineering -- Software Life Cycle Processes -- Maintenance 2008年 JIS X 0161:2008 ソフトウェア技術 - ソフトウェアライフサイクルプロセス - 保守
JIS Q 20000-1	2005年 ISO/IEC 20000-1:2005 Information technology -- Service management -- Part 1: Specification 2007年 JIS Q 20000-1:2007 情報技術 - サービスマネジメント - 第1部：仕様 2011年 ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements 2012年 JIS Q 20000-1:2012 情報技術 - サービスマネジメント - 第1部：サービスマネジメントシステム要求事項
JIS Q 20000-2	2005年 ISO/IEC 20000-2:2005 Information technology -- Service management -- Part 2: Code of practice 2007年 JIS Q 20000-2:2007 情報技術 - サービスマネジメント - 第2部：実践のための規範 2012年 ISO/IEC 20000-2:2012 Information technology -- Service management -- Part 2: Guidance on the application of service management systems 2013年 JIS Q 20000-2:2013 情報技術 - サービスマネジメント - 第2部：サービスマネジメントシステムの適用の手引