Vol.2018-EIP-80 No.13
2018/6/1

IT と情報セキュリティに対するガバナンスの経営者のための効果測定

原田要之助†

概要 昨今，あらゆる組織にとって IT は経営の主要なツールとなっている．また，サイバーセキュリティについても組織が軽視出来ないものとなっている．IT に対する取り組みが遅れて企業業績が悪化したり，サイバーセキュリティ対策が後手にまわって，情報漏えいなどのリスクを生じることがある．今までは，これらについては管理層の問題と考えられてきたが，経営に直接の影響を与えることから昨今では，IT ガバナンスや情報セキュリティガバナンスとして経営者層の問題と扱われるようになってきた．すなわち，経営者は IT や情報セキュリティの問題に主体的に取り組むことが求められ，IT ガバナンスや情報セキュリティガバナンスとして認知されるようになった．本稿では．IT ガバナンスの規格 ISO/IEC38500 をベースに経営者が IT ガバナンスを実践するにあたって，これを評価して測定する規格 ISO/IEC38503（現在，新規プロジェクトとして提案中）で検討されている．この規格に検討中の効果測定（Outcome と経営の原則との対応）について MSS をベースとした評価方法について紹介する．

キーワード：IT ガバナンス，情報セキュリティガバナンス，ガバナンスの評価，MSS（マネジメントシステム基準）

Perfomance and Evaluation on Governance of IT and Information Security for Governing body

YONOSUKE HARADA†

1. はじめに

企業などの組織では，IT に伴う投資問題や IT に依存するためのビジネスリスク（例えば，IT が故障してビジネスが正常に実施できない．Web サービスの利用形態が変化して，顧客が古いサービスを利用しなくなるなど）が発生する．また，情報セキュリティのビジネスリスク（例えば，個人情報をデータベースにして利活用を便利にしたが，ネットワークへの不正侵入によりデータが盗まれてカード情報を不正に利用されるなど）の影響は大きい．このように，経営者にとって IT の適正な利活用，情報セキュリティへの考慮は必須のものとなっている．

これらに対して，OECD のコーポレート・ガバナンス原則[1]からのアナロジーで原則（Principle）をベースとした IT ガバナンスの国際規格 ISO/IEC38500（JIS Q38500）[2]が 2008 年に策定され，情報セキュリティガバナンスの国際規格 ISO/IEC27014（JIS Q27014）[3]が 2013 年に策定されている[a]．現在，これらの規格については，JIS 化されたこともあり，日本において広く組織に受け入れられ，活用されている[4]．とくに，経済産業省では，2018 年のシステム管理基準の改定においては，組織が IT に関わるリスクを低減するために IT ガバナンスを確立するという立場を打ち出している[5]．

また，ISO/IEC JTC1 SC40 では，ISO/IEC38500 をベースに IT に関わるガバナンスを様々な分野に広げる規格を策定している．例えば，ビッグデータや個人情報のデータについて，組織が実施すべきガバナンスとして，ISO/IEC38505 [6][b]のデータガバナンスの規格が策定されている．

さらに，ISO では，IT 分野のみならず広く組織のガバナンスを規格化するために 2016 年に TC309（組織のガバナンス）を編成して規格化を進めており，2020 年には，OECD 原則をベースに実務的な規格が発表されるであろう．

IT ガバナンスを経営者が実施する場合，どのように，IT ガバナンスの効果を測定する方法論について述べる．

2. IT・情報セキュリティのガバナンス

2.1 IT ガバナンスのモデル

IT ガバナンスでは，大きく経営者層（英語では，Governing Body）とマネジメント層組織の経営者がマネジメント層に分けたモデルを用いる．

経営者は外部環境から事業圧力や事業必要性を受ける．この外部圧力のもとで，経営者が経営に関わる判断を実施する．なお，IT ガバナンスではとくに IT を利活用したビジネスや内部プロセスに対するものに限っている．この際に経営者が活用する考え方として 6 つの原則がある．原則を

a) 本規格は現在，改訂作業が実施されている．

b) 本規格は 2017 年に策定されたが，JIS にはなっていない．

表 1 に示す．さらに，原則に基づいて IT 利活用のするときの経営者が実施すべきプロセスのモデルを図 1 に示す．図 1 では，プロセスの 3 つの機能である評価，指示，モニタ（3 つを併せた英語の頭文字で EDM モデルと呼ぶ）[2]を示す．

表 1 IT ガバナンスの原則[2]

原則 1：責任（Responsibility）
原則 2：戦略（Strategy）
原則 3：取得（Acquisition）
原則 4：パフォーマンス（Performance）
原則 5：適合性（Conformance）
原則 6：人間行動（Human Behaviour）

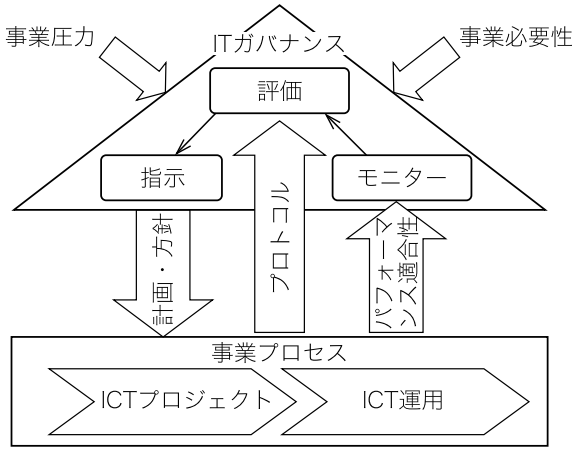

図 1 IT ガバナンスのモデル[2]

2.2 情報セキュリティガバナンスのモデル

情報セキュリティガバナンスのガバナンスのモデルは，ISO/IEC38500 の原則とプロセスモデルを引き継ぐ形で構成されている．情報セキュリティガバナンスは経営者との関係で，対等と扱うべきである．これは，情報セキュリティは情報システムに関わるものの，より，企業の扱う情報の機密性・完全性・可用性に関わるため，経営との関係が強いからである．例えば，企業の重要な顧客の個人情報が漏えいした場合には，経営者がその責任を認め謝罪することが一般的となっているからである．IT の下部概念とすると，経営者の責任が明確に表現出来ないからである．

経営者は外部環境から情報セキュリティについて，顧客のみならず，取引先やステークホルダーから要請を受けることがある．また，米国の SEC では，上場企業に対して情報セキュリティのリスク開示を求めている．すなわち，経営者が事業を進める上でこれらについてきちんと対応することが求められている．

この外部圧力のもとで，経営者が経営に関わる判断を実施する．なお，IT ガバナンスではとくに IT を利活用したビジネスや内部プロセスに対するものに限っている．この際に経営者が活用する考え方として 6 つの原則がある．原則を表 1 に示す．さらに，原則に基づいて IT 利活用のするときの経営者が実施すべきプロセスのモデルを図 1 に示す．図 1 では，プロセスの 3 つの機能である評価，指示，モニタ（3 つを併せた英語の頭文字で EDM モデルと呼ぶ）[2]を示す．

表 2 情報セキュリティガバナンスの原則[3]

原則 1：組織全体の情報セキュリティを確立する
原則 2：リスクに基づく取組みを採用する
原則 3：投資決定の方向性を設定する
原則 4：内部及び外部の要求事項との適合性を確実にする
原則 5：セキュリティに積極的な環境を醸成する
原則 6：事業の結果に関するパフォーマンスをレビューする

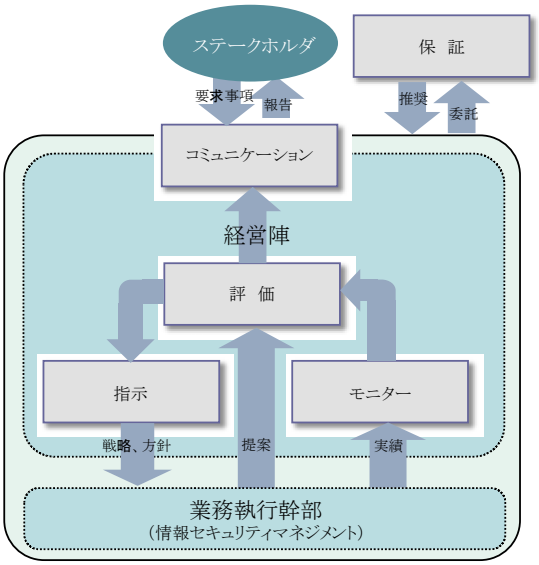

図 2 情報セキュリティガバナンスのモデル[3]

2.3 IT ガバナンスの効果測定（評価方法）について

経営者は， IT ガバナンスとしてマネジメント層に対して EDM に基づいて施策を実施する．これが最終的に組織の活動の結果（以下，Outcome とする）に繋がる．経営者は，原則を活用して EDM プロセスを実施した効果について評価できることが望ましい．これにはさまざまな方法論があり，経営層の EDM とマネジメント層の活動である PDCA を対象結びつけて評価する方法が分かり易い．しかし，PDCA は抽象的なため，(D)→P→D→C→(M)→(E)という流れで検討することになり，原則が複雑に絡み合うため，行き詰まっていた[7]．本稿では，マネジメント層の活動の PDCA モデルが単純過ぎて outcome との関係が明確でないので，

ISO がマネジメントシステムとして導入した MSS がマネジメント活動を表現する粒度として適切で分かり易いことから，これをベースとして検討することにした．

2.4 マネジメントシステム（MSS）について

ISO では，規格を制定する際には“ISO/IEC 専門業務用指針 補足指針”を使うことが義務づけられている． 2012 年 5 月以降に制定・改正された ISO マネジメントシステム規格（Management System Standard:以後，MSS と呼ぶ）[8]は，その構造、要求事項及び用語・定義を共通化することになった．すなわち，附属書 SL には，各 ISO マネジメントシステム規格（MMS）の整合性確保のための MSS 共通基本構造が定められている．これを表 3 に示す．なお，個別分野に適用する場合，MSS だけでは対応できない部分があるため，MSS の意図と矛盾せず，それらの意図を弱めない範囲でのテキストや箇条の追加が認められている．

表３．MSS 共通要求事項の章立て [8]

1.適用範囲
2.引用規格
3.用語及び定義
4.組織の状況
4.1 組織及びその状況の理解
4.2 利害関係者のニーズ及び期待の理解
4.3 XXX マネジメントシステムの適用範囲の決定
4.4 XXX マネジメントシステム
5.リーダーシップ
5.1 リーダーシップ及びコミットメント
5.2 方針
5 3 組織の役割,責任及び権限
6.計画
6.1 リスク及び機会への取り組み
6.2 XXX 目的及びそれを達成するための計画策定
7.支援
7 1 資源
7.2 力量
7.3 認識
7.4 コミュニケーション
7.5 文書化された情報
7.5.1 一般
7.5.2 作成及び更新
7.5.3 文書化された情報の管理
8.運用
8.1 運用の計画及び管理
9.パフォーマンス評価
9.1 監視,測定,分析及び評価
9.2 内部監査
9.3 マネジメントレビュー
10. 改善
10.1 不適合及び是正措置
10.2 継続的改善

MSS は経営者の責任を強く意識しているものの（5 章や 6 章，9 章），多くの章はマネジメントを主体としている．これを実施する主体は図１の事業プロセスにあたり，図２の業務執行幹部に相当する．なお，ISO/IEC38500[2]及び ISO/IEC27014[3]は前提とするマネジメントのモデルは MSS が定義される前の段階の PDCA である．しかし，マネジメントのモデルは規格毎に異なるため，個別に展開することができない．MSS は，経営者とマネジメント層を意識した規格であるので，組織内におけるガバナンスとマネジメントを統合して考察するには，MSS の内容を経営者目線で捉えることが適切である．以下では，MSS をベースに論ずる．

3. IT ガバナンスの MSS を用いた評価について

3.1 MSS と IT ガバナンスの原則との対応

MSS は組織を対象にした要求条件であり，MSS 導入前の PDCA モデルとは一線を画している．すなわち，マネジメント層が独自に判断して実施する項目のみならず，経営者が判断する項目や両者が協力して実施する項目が盛り込まれている．したがって，IT ガバナンスの観点から経営者が主体的に実施する項目，マネジメント層が実施する項目，両者が協力して実施する項目について分類する必要がある．これを表 4 に示す．

表 4．MSS の責任分担について

MSSの項目	経営者	管理層	両者
1.適用範囲			○
2.引用規格		○	
3.用語及び定義		○	
4.組織の状況			
4.1 組織及びその状況の理解	○		
4.2 利害関係者のニーズ及び期待の理解			○
4.3 MS マネジメントシステムの適用範囲の決定			○
4.4 MS マネジメントシステム		○	
5.リーダーシップ			
5.1 リーダーシップ及びコミットメント	○		
5.2 方針	○		
5 3 組織の役割,責任及び権限			○
6.計画			
6.1 リスク及び機会への取り組み	○		
6.2 MS 目的及びそれを達成するための計画策定		○	
7.支援			
7 1 資源			○
7.2 力量			○
7.3 認識			○
7.4 コミュニケーション		○	
7.5 文書化された情報		○	
7.5.1 一般			
7.5.2 作成及び更新			
7.5.3 文書化された情報の管理			○
8.運用			
8.1 運用の計画及び管理		○	
9.パフォーマンス評価			
9.1 監視,測定,分析及び評価		○	
9.2 内部監査		○	
9.3 マネジメントレビュー			○
10. 改善			
10.1 不適合及び是正措置			○
10.2 継続的改善			○

MSS は経営者や管理者の実施する必要な項目を網羅していると考えられるので， 以下では，IT ガバナンスの原則及び EDM タスクとの関係を考えるにあたり，表４をベースに検討する．まず，原則と MSS の関係について表 5 に示す．

表 5. MSS の項目と IT ガバナンスの原則の関係について

MSSの項目	責任	戦略	取得	パフォーマンス	適合性	人間行動
1.適用範囲	○					
2.引用規格						
3.用語及び定義						
4.組織の状況						
4.1 組織及びその状況の理解		○				
4.2 利害関係者のニーズ及び期待の理解		○				
4.3 MS マネジメントシステムの適用範囲の決定	○					
4.4 MS マネジメントシステム						
5.リーダーシップ						
5.1 リーダーシップ及びコミットメント	○					○
5.2 方針		○	○			
5 3 組織の役割,責任及び権限	○					
6.計画						
6.1 リスク及び機会への取り組み					○	
6.2 MS 目的及びそれを達成するための計画策定						
7.支援						
7 1 資源						○
7.2 力量						○
7.3 認識						○
7.4 コミュニケーション						
7.5 文書化された情報						
7.5.1 一般						
7.5.2 作成及び更新						
7.5.3 文書化された情報の管理					○	
8.運用						
8.1 運用の計画及び管理				○		
9.パフォーマンス評価						
9.1 監視,測定,分析及び評価				(○)*		
9.2 内部監査				(○)*		
9.3 マネジメントレビュー				○	○	○
10. 改善						
10.1 不適合及び是正措置	○				○	
10.2 継続的改善	○				○	
(○)*:間接的						

表 5 からは，ISO/IEC38500 の 6 つの原則が MSS の活動とどのように対応しているかがよく分かる．今までの PDCA のモデルでは，どこまでが経営者の判断や指示によるものか，両者が相談して決めるかの境界が曖昧であったが，MSS では，4 章や 5 章の経営者が主体的に判断してマネジメント層に指示すべきものとが明確であり，具体的なマネジメントシステムの段階では，マネジメント層の責任で進めていくことが明確に分かる．ただし，取得（Acquisition）については，経営がどこまで主体的に進めるかが曖昧であり，表 5 ではリーダシップでの関係で止めている．昨今では，サプライチェーンのセキュリティ問題が指摘されていることや，また，Unti-primary（賄賂などの不正対策）についても ISO37001 規格が策定されており，これとの関係から経営者のさらなる関与が求まられることが想定されるため，今後，検討が必要であろう．

一方，パフォーマンスについては，マネジメント層が主体的に現場のプロセスを監視・測定して，問題点を把握する．また，全体のプロセスを内部監査するのも一義的にはマネジメント層が実施する[c]．経営者が内部監査を主体的に実施する案も考えられる．ISO/IEC27014 のモデルに Assure の機能が盛り込まれていることからも分かる[d]．ISO/IEC27014 のモデルは組織に対する外部監査を想定しており，外部の監査人が保証型監査を実施する（付録 A には保証型監査が例として参照されている），すなわち，MSS でいう内部監査とは異なる．なお，現在策定中の Assessment of Governance ofIT の標準化においては，評価の主体を経営者層とする案もあり，今後，検討するテーマと考えられる．MSS の 9 章では，パフォーマンス評価として，現状の分析を行い，問題点を内部監査で洗い出して，これをまとめ，マネジメントレビューという形で経営層に報告することが想定されている．したがって，IG ガバナンスでも，経営層は，このマネジメントレビューによる経営層からの報告をうけて，9.1 や 9.2 で明らかになった問題点について理解して，これを分析して（表 5 では，間接的としている），重要な問題点については，早急な指示を行うと考えるのがよいであろう．

c　中立の内部監査部門が実施するのが望ましい

d　Assuure については ISO/IEC38500 には記載がない

3.2 MSS と IT ガバナンスの EDM モデルとの対応

次に，IT ガバナンスの EDM タスクとの関係を検討する．表 5 と同様に，表 4 で経営者が実施する（共通を含む）MSS の項目について，EDM との対応について表 6 に示す．

表 6. MSS の項目と IT ガバナンスの EDM タスクとの関係について

MSSの項目	E	D	M
1.適用範囲		○	
2.引用規格			
3.用語及び定義			
4.組織の状況			
4.1 組織及びその状況の理解	○		
4.2 利害関係者のニーズ及び期待の理解	○		
4.3 MS マネジメントシステムの適用範囲の決定		○	
4.4 MS マネジメントシステム			
5.リーダーシップ			
5.1 リーダーシップ及びコミットメント		○	
5.2 方針		○	
5 3 組織の役割,責任及び権限		○	
6.計画			
6.1 リスク及び機会への取り組み	○		
6.2 MS 目的及びそれを達成するための計画策定			
7.支援			
7 1 資源		○	
7.2 力量		○	
7.3 認識			
7.4 コミュニケーション			○
7.5 文書化された情報			
7.5.1 一般			
7.5.2 作成及び更新			
7.5.3 文書化された情報の管理			○
8.運用			
8.1 運用の計画及び管理			
9.パフォーマンス評価			
9.1 監視,測定,分析及び評価			
9.2 内部監査			
9.3 マネジメントレビュー			○
10. 改善			
10.1 不適合及び是正措置			○
10.2 継続的改善			○

MSS と IT ガバナンスの EDM タスクとの関係は，表 5 よりも関係が明確である．経営者が実施すべきことは，経営の観点から経営資源を考慮にいれて戦略を決め，それに整合するように，予算やリソースの配分を検討する．さらに，マネジメント層に計画を策定させて，内容を承認して，権限委譲を行う．ここでは，マイケルポーターのいう企業の競争戦略よりも，ジェイ・バーニーのいう自分のリソースを正確に判断して，何ができるのか，また，何が出来ないのかをきちんと分析して，優先度付けを行うことが望まれる．責任の委譲，リソースの配分を行うことが望まれる．また，リスクやプロジェクトの優先度については，一次的な分析は経営層が実施するが，経営層は，その結果をを受けて，ポートフォリオなどを作成して，考え方をマネジメントに示す必要がある．

とくに，MSS と ISO31000 の導入では，リスクをとってより事業を拡大する戦略も採用できるようになった．そのため，経営者は，今までのように経営層にリスク分析の報告のみを求めるだけではなく，より，リスクをとって，企業の戦略的優位に立てるかの分析が望まれている．これについては，リスクの高い事業について機会損失を分析する方法論が未熟なため，評価方法がない．

3.3 MSS の Outcome について

表 4～表 6 をベースに IT ガバナンスと MSS を組合わせてうまく運用することで期待できる Outcome（成果）を考える．ここでは，MSS を用いたときの観点で何が経営者やマネジメント層にプラスとなるかの観点で考察する．MSS の各項目について，経営者，マネジメント，共通の 3 つについて検討した結果を表 7 に示す．

例えば，経営者には，MSS の 5.1 節で「リーダシップ及びコミットメント」が要請される．これについては経営層は自組織の持っているリソースを評価し，競争優位に立つ経営を考えて，企業の方針を定め，マネジメント層に指示することになり．ここでの Outcome は，経営能力の向上に繋がる．また，経営方針自体も成果となる．同様に，7.1 節の「資源」については，マネジメント層がリソースをさらにブレークダウンして，必要な機会を購入して生産性を上げるなどに繋がる．

表 7. MSS の項目と IT ガバナンスの EDM タスクとの関係について

MSSの項目	経営者	管理者	両者
1.適用範囲			理解度
2.引用規格			
3.用語及び定義			
4.組織の状況			
4.1 組織及びその状況の理解			
4.2 利害関係者のニーズ及び期待の理解			ニーズの特定
4.3 MS マネジメントシステムの適用範囲の決定			範囲
4.4 MS マネジメントシステム		方法論	
5.リーダーシップ			
5.1 リーダーシップ及びコミットメント	経営能力向上		
5.2 方針	経営指針		
5 3 組織の役割,責任及び権限			責任範囲
6.計画			
6.1 リスク及び機会への取り組み	リスク認識	リスク低減	
6.2 MS 目的及びそれを達成するための計画策定		管理能力向上	
7.支援			
7 1 資源		生産能力	
7.2 力量			生産性
7.3 認識			品質
7.4 コミュニケーション		企業文化	
7.5 文書化された情報		マニュアル	
7.5.1 一般			
7.5.2 作成及び更新			
7.5.3 文書化された情報の管理			内部統制
8.運用			
8.1 運用の計画及び管理		生産性	
9.パフォーマンス評価			
9.1 監視,測定,分析及び評価		品質	
9.2 内部監査		問題点分析	
9.3 マネジメントレビュー			原因分析
10. 改善			
10.1 不適合及び是正措置			是正措置
10.2 継続的改善			改善活動

表 7 は，MSS の各項目の要求条件として想定される Outcome の一例を示しているが，これは，国，業種，規模，従業員の特性など具体的なマネジメントの状況で異なる．表 7 では，「生産性向上」としているが，例えば，ソフトウェア開発能力が単位時間あたり 15%向上したとか，バグ工数が減少して品質が向上したなどと結びつけられると考えられる（この例は，品質としているがセキュリティ向上で生産性があがったなども想定できると考えられる）．また，経営の最終目標である売上が 10%向上したというのも Outcome と考えてもよいであろう．

3.4 ガバナンスの効果測定について

表 5～7 は， MSS の要求条件をベースとしているので，全ての項目で，「実施出来ている」ことが認証を受ける最低条件となる．すなわち，効果について，次の「実施できていない」，「ベースライン達成」，「改善の効果確認」，「良好」4 つの段階で評価すればよいと考えられる．MSS の要求条件が求めるレベルの Outcome が実施できていない場合には，経営者はマネジメントにベースラインを達成するための施策を要請することになる．「ベースライン達成」したときは，最低限のレベルであり，維持するための施策が必要となる．ベースラインを超えた段階（「改善の効果確認」）では，経営者はマネジメントに管理を委譲する．なお，マネジメントレビューや内部監査でレベルが「ベースライン」に低下したときには，直ぐに改善施策をマネジメントに要請することになる．レベルが良好なときにはマネジメントが継続的にモニタリングすればよい効果測定レベルと必要なアクションを表 8 に示す．

表 8. Outocome の評価について

-1：効果なし	実施できていない（改善が必要要）
0：最低限	ベースライン達成（継続監視）
1：改善効果	効果確認（項目の管理を委譲）
2：良好	マネジメントが管理

4. まとめ

2017 年 10 月以降，ISO/IEC SC40WG1 で原則ベースのガイドラインを採用したときのガバナンスについてどのように評価するのが検討されている．まず，IT ガバナンスの規格は原則ベースで，6 つの視点で責任，戦略，調達などがあり，経営者がどのように理解して，マネジメント層に指示する．これについて評価が必要となる．今までは，経営層のモデルに PDCA を前提としていたため，結果としての Outcome との関係が難しく，評価が抽象的なものとなりがちであった[8]．本稿では，マネジメントのモデルとして，ISO が策定した共通マネジメントシステムを定義しており，これがマネジメントと経営の両方の視点で規定されており，組織に求められるガバナンス＋マネジメント層の行動内容としても網羅性が高い．

そこで，本稿では，ISO の MSS をマネジメントの中核として，IT ガバナンスの原則及び EDM モデルと対比することで Outcome との関係性がより高まり，評価がやりやすくなることを示した．

謝辞

本研究は，ISO/IEC38503 Assessment of Governance ofIT の標準化において検討するテーマであり，かつ，原則ベースの規格を実践するにあたって，ガバナンスの実施母体である経営者とマネジメント層がどのように業務を分担して効率のよい経営を実践できるかを評価することにフォーカスしている．検討にあたり，この機会を頂いた ISO/IECSC40 国際・国内委員会に感謝します．さらに，このテーマを検討するにあたり，さまざまなコメントや異見をいただいたシステム監査学会，NPO 公認システム監査人協会に感謝します．

さらに貴重なコメントをいただいた本学の教授・准教授の皆様，原田研究室の博士後期課程・前期過程の学生諸氏，客員研究員に感謝いたします．

参考文献

[1] OECD, G20/OECD Principles of Corporate Governance,2015
[2]ISO/IEC38500, Governance of IT, 2015, (JIS Q 38500:2015 情報技術-IT ガバナンス - 日本工業規格)
[3] ISO/IEC27014, Governance of Information Security, 2013, (JIS Q 27014:2015 情報技術-情報セキュリティガバナンス - 日本工業規格)
[4] 原田，企業に求められる IT ガバナンスの新しいモデル，InfoCom Review，vol,47,2009
[5] 経済産業省，（改訂）システム管理基準，http://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kanri_h30.pdf（アクセス 2018 年 4 月 24 日），2018 年 4 月
[6] ISO/IEC38505, Governance of IT, Governance of Data, 2017
[7] 原田，IT ガバナンスの評価について，第 80 回情報処理学会全国大会予稿集，2018 年 3 月
[8]ISO,Directive Part II, Annex SL(MSS 共通テキスト・定義・上位構造)（ISO 業務指針の補足指針の付属書 SL）、2016
[9]ISO/IEC38503 NWIP draft, Assessment of Governance of IT, 2018