Vol.2014-DCC-7 No.3
Vol.2014-EIP-64 No.3
2014/5/14

プロセスアプローチを用いたＩＴ外部委託先管理の研究

河野翔太[†1]　　原田要之助[†2]

IT アウトソーシングは，経営効率の向上や業務の効率化のための手段である．一方で，情報セキュリティの観点から，委託先に対する適切な管理が重要となる．また，IT を取り巻く技術や環境は，劇的に変化する．委託者はそのような変化に対応し，時代に応じた十分な情報セキュリティを確保しなければならない．そのためには，委託先での業務プロセスや自組織における委託先管理の有効性について，適時見直していく必要がある．本稿では，プロセスアプローチを応用した継続的な見直しによって，委託先の管理プロセスの有効性や効率を維持・改善させる仕組みを検討する．

Study on IT Outsourcing Management using process approach

SHOTA KONO[†1]　　YONOSUKE HARADA[†2]

IT Outsourcing is a means to improve efficiency of organization management and business. On the other hand, because of the information security, appropriate management of contractors is important. Also, the environment surrounding IT is changing rapidly. Consignor must correspond to such changes, and ensure enough information security according to era. To that end, it is necessary to review timely about business processes in the contractors and the effectiveness of IT Outsourcing management in the own organization. In this paper, by continuing review of applying the process approach, consider a mechanism to maintain and improve the efficiency and effectiveness of the management process of contractors.

1. はじめに

(1) 研究の背景

現代の企業経営では，選択と集中によって事業のコアコンピタンスが見極められ，利潤の源泉となる事業に対して，経営資源が集中的に投入されている．情報システムは，今や事業を営む組織の事業にとって欠かすことのできない，重要なインフラである．しかし，情報システムの充実・差別化が，必ずしも大きな利益に直結するわけではない．また，技術革新が激しく，次々に新たな技術や製品が登場するため，IT を利活用している組織にとって，IT の技術変化に逐次対応することや相応のスキルを持つ要員を育成・確保することは困難となっている．そこで，組織の多くは，情報システムの構築・運用を専門ベンダにアウトソーシングしたり，IT プロバイダが持つ，高度かつ豊富な資源をサービスとして柔軟に活用することで，技術や環境の変化への対応，コスト削減を実現してきた．

さらに，近年のクラウド・コンピューティング（以下，クラウドという）の広まりは，情報システムの「所有から利用へ」という潮流を生み出している．今後は，自組織で「所有」すべき範囲と，アウトソーシングやクラウドを「利用」すべき範囲を明確にすることで，管理する情報資産のスリム化やコスト削減を図り，経営効率の向上に寄与することが重要になる．

一方で，企業にとって外部リソースの活用が進み過ぎることによる弊害として，情報システムに対する関与が薄くなることで，ベンダやプロバイダに全てを依存する状態になったり，情報システムの内部の技術がブラックボックス化してしまう恐れがある．アウトソーシングした組織の技術力や IT リスクへの関心が低下し，このような結果，情報システムの障害や事故によるサービスの停止，委託情報の漏えいなどのリスクが高まる．2011 年にみずほ銀行の情報システムで発生した大規模システム障害は，情報システムの一部がブラックボックス化していたことが一因とされている [1]．また，2012 年には，委託先のデータセンター内におけるデータ不正取得事件aや，サービスプロバイダが発生させたインシデントにより，データが滅失・漏えいするという事象bが発生した．

(2) 研究の目的

委託先で情報漏えい事故や IT サービスの障害・停止が発生すると，委託元にも多大な影響を及ぼす恐れがある．具体的には，業務の停止による逸失利益や利用者への補償・補填，損害賠償に係る費用などの金銭的被害がある．ただ，これらについては，委託先に対する求償によって補填される可能性もある．一方で，委託元に対する信用や評判が損

†1 情報セキュリティ大学院大学
Institute of Information Security
†2 情報セキュリティ大学院大学
Institute of Information Security

a) 銀行の共同システムを運営するベンダの再委託先の社員が，顧客の取引情報を不正に取得した後，共同センター内のテスト機器を用いてキャッシュカードを偽造し，顧客の預金を引出した事件．
b) レンタルサーバ業者の担当者が，障害対応によるメンテナンス作業のために，独自に作成したプログラムに不具合があったため，約 5,600 ユーザのデータが滅失した事件．滅失データの復旧作業が行なわれたが，復元されたデータには他のユーザのデータが混在しており，情報漏えいに至った．

Vol.2014-DCC-7 No.3
Vol.2014-EIP-64 No.3
2014/5/14

なわれた場合には，それらを回復させることは容易ではない．現代の高度に情報化された社会において，情報セキュリティに関わる信頼を損なうことは，顧客の選別に重大な影響を与える可能性がある．

このように，情報システムをアウトソーシングして構築・運用している場合であっても，委託元の社会的地位や事業に関わる損害が発生する恐れはある．したがって，アウトソーシングの程度がどのレベルであっても，情報システムへの関与を失ってはならない．一方で，アウトソーシングの本質は経営効率の向上にある．したがって，運用や管理に係るコスト削減が期待される中で厳格な委託先管理が必要になるというジレンマがある．

そこで，アウトソーシングや委託先管理の現状や課題を調査・整理し，委託先管理の方向性を検討することが，本研究の目的である．

2. IT アウトソーシング

(1) 定義

経済産業省[2]は，アウトソーシングを「企業の事業戦略の達成を支援し，業務の有効性と効率性をより高めるために，外部組織のリソースを活用し，企業内業務の遂行を外部組織に委託すること」と定義している．アウトソーシングは，コスト削減の手法として注目されることが多いが，本来の目的は経営効率を高めることにある．

(2) モデル

経済産業省 [2]は，アウトソーシングを計画，実行・評価，改善の 3 つのフェーズから成る，PDCA によるマネジメントサイクルとしてモデル化している（図 1）．

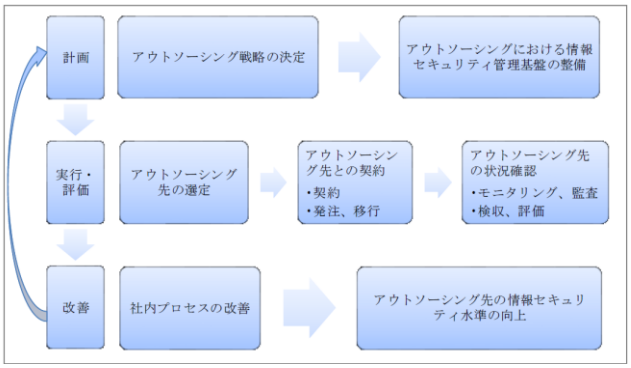

図 1　アウトソーシングのプロセス
（経済産業省 [2] p.9 より，作成）

本研究では，アウトソーシングする業務やビジネスプロセスには着目していない．したがって，アウトソーシングの形態は考慮せず，関口 [3]のいう「組織間での業務の受託と委託の関係」として捉える．その上で，情報システムの開発や運用，保守に外部リソースを活用するものを IT アウトソーシング（以下，ITO という）として，検討を行なう．

3. ITO と情報セキュリティ

(1) 情報漏えい事故の現状

表 1 は，経済産業省が実施している情報処理実態調査[4]をもとに，過去 3 年間の重要情報漏えい事故の発生割合について，原因別に推移をまとめたものである．

表 1　重要情報漏えい事故の発生割合
（経済産業省の調査結果[4]より，作成）

（単位：%）	2009 年	2010 年	2011 年
事故の発生割合（合計）	19.8	20.2	21.3
コンピュータウイルス	1.2	1.0	0.7
不正アクセス	0.3	0.3	0.5
標的型サイバー攻撃	－	0.2	0.1
内部者	1.8	1.8	2.3
委託先	2.0	1.9	1.9
PC や記憶媒体の盗難・紛失	17.4	17.7	18.9

※注：事故の発生割合は，複合的なケースがあるため，単純集計値と合致しない．

表 1 からは．事故が発生した組織の割合は，僅かであるが増加傾向にあり，その原因の大半が，PC や記憶媒体の盗難・紛失によるものであることが分かる．また，委託先による情報漏えいは，内部者による情報漏えいと同水準であり，コンピュータウイルスや不正アクセス，標的型サイバー攻撃を原因とする場合よりも相対的に高い．近年，これらの脅威への対策が注目を集めているが，委託先における情報漏えいのリスクは，それらと同等か上回っていると言える．

(2) 情報セキュリティに対する意識

情報セキュリティ大学院大学・原田研究室では，2013 年に情報セキュリティアンケート調査（以下，2013 年度情報セキュリティ調査という）cを実施した．図 2 は，IT サービスを委託する場合の委託先の選定時に，最も重要とする項目である．

c) 2013 年度情報セキュリティ調査の概要

実施期間	2013 年 7 月 29 日～8 月 23 日
実施方法	郵送
調査方法	P マーク取得企業，ISMS 認証取得企業，公官庁，教育機関など 4,500 組織の情報セキュリティ・システム担当者
有効回答	367（送達確認できた 4,378 組織に対して 8.4%） ※設問により異なる
質問項目	詳細については，原田研究室ホームページを参照 http://lab.iisec.ac.jp/~harada_lab/survey.html

Vol.2014-DCC-7 No.3
Vol.2014-EIP-64 No.3
2014/5/14

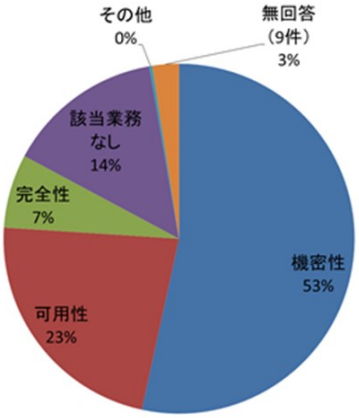

図 2　ITO の委託先選定時に，最も重視する
情報セキュリティ要素（N=367）

図 2 からは. 機密性を最も重視する組織が過半数であることが分かる．委託情報が外部に漏えいするリスクとその影響が，委託元でも認識されていることが伺える.

また，「個人情報の漏えい」または「IT サービスの停止」が発生した際の事業インパクトの比較では,「個人情報の漏えい」がより大きいとする組織が多かった（63%） [5]．したがって，ITO を活用しているか否かに関わらず，情報セキュリティ要素の中では，特に機密性が重視され，委託先に対しても高い機密性を求めている傾向があると推測される.

(3) 形態の複雑化

前述の通り，アウトソーシングの目的は，業務の有効性と効率性をより高めることにある．それらを追及すると，再委託dや複合委託eなどに見られるようにアウトソーシングの形態が複雑化し，委託先管理をより困難にする可能性がある．二段階以上の委託先でインシデント等が発生した場合であっても, 委託元がその責めを負うことは有り得る．例えば，ITO を活用して構築・運用した情報システム上でサービスを利用者に提供する場合，サービス利用者にとってはあくまで委託元の情報システムおよびサービスである．データがその組織内部にあるか，委託先のデータセンター等にあるかといったことは，サービス利用者にとっては関係がないためである．これは，冒頭で紹介した再々委託先の社員によるカード偽造事件にも当てはまることである.

そのような中で，上山[6]は，クラウドの利用やシステム運用・保守のアウトソーシングなどにより，情報のコントロールはユーザ企業から IT ベンダに移っており, 再委託先の責任を明文化することが重要であると述べている. 特に，クラウドに関してはデータセンターが海外にある場合や，詳細な所在地が不明である場合も多い．ITO が多段階になったり，複雑な構成になるほど，委託先企業を直接的に管理することが難しくなる.

4. 委託先管理

(1) 管理の現状（2013 年度情報セキュリティ調査）

2013 年度情報セキュリティ調査では，外部委託している情報システムのセキュリティ管理手法について，図 3 のような回答が得られた.

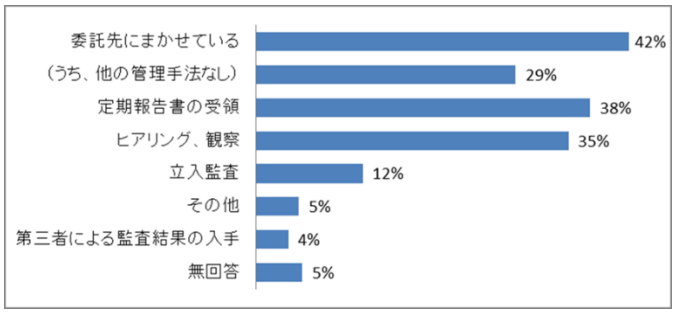

図 3　回答組織に占める委託先管理手法の導入割合
（委託業務が無い先を除く，N=248）

図 3 の回答は，「委託先にまかせている」組織が最も多かった．もっとも，本質問が複数の選択肢を認めるものであったため,「委託先にまかせている」一方で，他の管理手法を取り入れているとの回答もあった．ただし,「委託先にまかせている」と回答した 105 組織のうち，他の管理手法を何ら取り入れず，完全に委託先任せとなっている回答は 73 組織に上った．これは，外部委託業務がないとする組織を除くと，全体の約 30%を占める．このような組織では，委託先での情報セキュリティが，委託先に丸投げの状態となっている可能性が高いと推察される.

次に，導入率の高い手法は,「定期報告書の受領」である．図 3 に示す 4 つの手法の中でも，最も簡易であると言える．これは，委託先との間で，報告内容や報告書の書式を決定しさえすれば，報告書の作成について委託元の手間は掛からないためである．一方で，報告書を受領したとしても，目を通すことなく，情報システムの機能や管理プロセスの改善に全く役立たないことも有り得るであろう.

次いで導入率の高い手法である「ヒアリングや観察」も，委託先への訪問や面談を通じて行なうという点では,「定期報告書の受領」に比べてコストは掛かるが,「監査の実施」と比べると，その実施は容易であろう.

上述したように，比較的簡易な手法によって，委託先での情報セキュリティ確保が図られる理由には，回答組織に中小規模の組織が多いことがあると考えられる.

d) 委託先が経営効率を高めるために，さらに別の組織のリソースを活用するケース.
e) 一つの業務を複数のアウソーシング先に対して発注する形態．委託先の相互連携が必要となる場合があるため，複雑な委託構造となる可能性がある.

表 2　従業員数と定期報告書の受領の有無のクロス表
（委託業務が無い先を除く，N=248）

(単位:組織)

従業員(4階層)	定期報告書の受領		合計
	実施あり	実施なし	
50人以下	14 (23%)	46 (77%)	60 (100%)
51～300人	35 (33%)	70 (67%)	105 (100%)
301～1,500人	19 (42%)	26 (58%)	45 (100%)
1,501～	25 (66%)	13 (34%)	38 (100%)
合計	93 (38%)	155 (63%)	248 (100%)

表 2 は，回答組織の従業員数（4 階層化）と「定期報告書の受領」の有無をクロス集計した結果である．表 2 からは，従業員数が多い，つまり，規模が大きな組織ほど「定期報告書の受領」の実施率が高いことが分かる．なお，この結果は，1%水準で有意であり（$\chi 2=19.319$），統計的に関連性が強いと言える．

また，リスク分析を行なう際の問題点として，人材の不足を認識している組織は 80%弱に上る [5]．全般的なリスク分析でさえ，人材不足を感じる組織が大半であり，規模の小さな組織では，委託先管理の実施がままならない状況であることが推測される．

(2) 管理の難しさ

委託先管理の手法に関する同様の調査は，高度な情報セキュリティが求められる銀行業界でも行なわれている．日本銀行による 2009 年の調査結果[7]では，打合せや書面を受領している銀行は 9 割を超え，立入監査や監査結果の入手でも 7 割を超えている．図 3 と比べ，極めて高い数値である．一方で，同調査では，委託先管理における悩みとして以下のようなものが多く挙げられている．

- コスト削減を目的とする ITO に管理コストを掛けられない
- ベンダに対して主導権を発揮できる機会が少なく管理が難しい
- IT 委託先管理のスキルを持つ人材がいない

これらの悩みは，委託先管理の必要性に関わるような根本的な問題である．場合によっては，委託先管理が形式だけのものになってしまう恐れがある．委託先管理の実施目的が，管理を実施している証跡を残すこととなり，管理プロセスで作成されるアウトプットさえ残れば良いということになりかねないと危惧される．

5. プロセスアプローチの応用検討

5.1 プロセスアプローチ

(1) 定義

日本規格協会 [8]は，プロセスアプローチを「組織内において，望まれる成果を生み出すために，プロセスfを正確にし,その相互関係を把握し,運用管理することと併せて，一連のプロセスをシステムとして適用すること」と定義している．その目的は，品質マネジメントシステム（QMS : Quality Management System ．以下，QMS という）gの有効性を維持・改善させることにあり，プロセスアプローチの採用は品質マネジメント 8 原則hの一つとなっている．

(2) メリット

プロセスアプローチを採用することによる利点は，以下のようなものがある [8] [9].

- 望まれる成果を出せるようにするためのプロセスの統合及び整合
- プロセスの有効性及び効率において注力する能力
- 顧客及びその他の利害関係者に対する組織の一貫性のあるパフォーマンスについての信頼の付与
- 組織内における運用の透明性
- 資源の効果的な使用による，コストの削減及びサイクルタイムの短縮
- 改善された，一貫性のある，予測可能な結果
- 集中的かつ優先的な改善への取組み機会の供与
- 人々の関与の奨励及びそれらの人々の責任の明確化

4 章 (2) で述べたように,組織における委託先管理では,管理プロセスが形骸化していることが懸念される.そこで,本研究では，委託先管理における個々の管理プロセスについて，プロセスアプローチを応用した継続的な見直しの仕組みを考察する．これは，プロセスアプローチによって，当該プロセスの有効性や効率の維持･改善を図るとともに，委託元が管理プロセスの重要性と責任を自覚し，管理プロセスが形骸化しない仕組みを構築できるからである．

5.2 マネジメントシステム

BSI ジャパン [10]によると,マネジメントシステムは「組織の方針，手段およびプロセスを管理し，継続的に改善するためのフレームワーク」である．継続的な改善を行なうためには，PDCA による見直しを行なう．

本研究では，「委託先の管理プロセスを管理し，継続的に改善するためのフレームワーク」として，ITO マネジメントシステム（ITOMS : ITO Management System）を構築することを提案する.品質マネジメント 8 原則の一つとして，マネジメントへのシステムアプローチがあり，品質を管理するためには，システムとして体系化されたマネジメントの仕組みが必要であることが分かる．そこで，この原則に則り，委託先管理の仕組みをマネジメントシステムとして

f) インプットをアウトプットに変換する，相互に関連するまたは相互に作用する一連の活動 [8].

g) 品質に関して組織を指揮し，管理するためのシステム.
h) ①顧客重視,②リーダーシップ,③人々の参画,④プロセスアプローチ,⑤マネジメントへのシステムアプローチ，⑥継続的改善，⑦意思決定への事実に基づくアプローチ，⑧供給者との互恵関係，の 8 原則．ISO9000:2005（JIS Q 9000:2006）品質マネジメントシステム－基本及び用語に記述されている.

Vol.2014-DCC-7 No.3
Vol.2014-EIP-64 No.3
2014/5/14

構築することで，管理プロセスの品質を管理することを目指す．

なお，経済産業省もアウトソーシングを PDCA によるマネジメントサイクルモデルとして捉えており（図 1），ITOMS の概念は，これに近いと言える．

以下では，マネジメントシステムの中でも本研究に関係が深いものとして，ISMS と QMS の概要を紹介する．その上で，委託先管理について，プロセスアプローチとマネジメントシステムを組み合わせた場合の，フレームワークを示す．

(1) ISMS

JIPDEC [11]は，ISMS を「個別の問題毎の技術対策の他に，組織のマネジメントとして，自らのリスクアセスメントにより 必要なセキュリティレベルを決め，プランを持ち，資源配分して，システムを運用する」ものと定義している．組織が保護すべき情報資産について，機密性，完全性，可用性をバランス良く維持し改善することが，ISMS の基本コンセプトである．図 4 は，PCDA サイクルによる，ISMS における改善活動のモデルである．

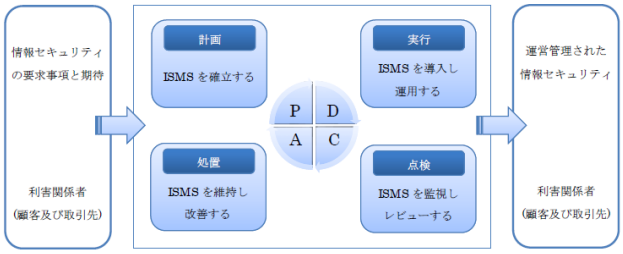

図 4　ISMS の改善活動（JIPDEC [11]より．作成）

なお，ISMS の確立までのプロセスは，以下の 3 フェーズから成る．

- フェーズ 1：ISMS の適用範囲及び基本方針を確立する
- フェーズ 2：リスクアセスメントに基づいて管理策の選択をする
- フェーズ 3：リスクについて適切に対応する計画を策定する

(2) QMS

QMS は，品質に関して組織を指揮し，管理するためのシステムである [12]．組織は，JIS Q 9001:2008 [13]の要求事項に従って，QMS を確立し，文書化し，実施し，かつ，維持しなければならない．また，QMS の有効性を改善する際にプロセスアプローチを採用することで，プロセスを明確にし，その相互関係を把握し，運営管理することと併せて，一連のプロセスをシステムとして適用することが推奨されている [13]．

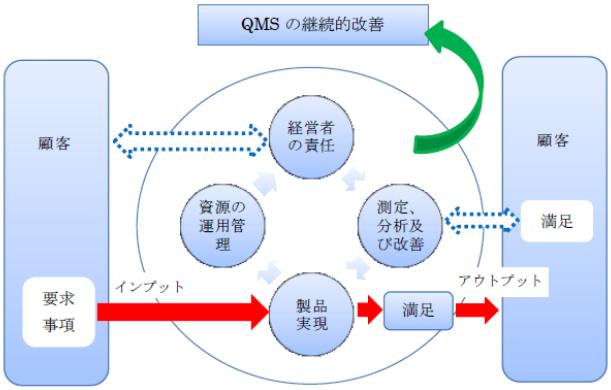

図 5　QMS の改善活動（JISC [12]より，作成）

※ 価値を付加する活動　情報の流れ

なお，QMS の基本にある考え方は，TQM（Total Quality Management：統合的品質管理）i)に通ずるものがある．つまり，QMS の規格である ISO9000 シリーズでは，品質・質についてトップが適切に方針を定め，これを組織的に展開し，個々の現場でそれを確実に実施する活動が規定されている [14]．また，QMS は，当初は物理的な製造物に適用されていたが，1993 年以降 IT を使用した製品やサービスにも広く適用されるようになり [15]，ソフトウェア開発における課題の解決策としての，ソフトウェアプロセス改善（SPI：Software Process Improvement）活動などへも応用されている [14]．

(3) 提案モデル

本研究で検討を行なう ITOMS では，上述した 2 つのマネジメントシステムと同様に，PDCA サイクルによる見直し活動によって，マネジメントシステムの継続的改善を目指す．PDCA によって，委託先の管理プロセスを見直す（図 6）ことで，それらが形骸化することを防ぐとともに，委託元における委託先への強い管理責任を促す．また，個別のプロセスに焦点を当て改善活動を行なうことで，委託先管理の有効性を維持・向上させ，ITOMS の継続的改善を図るとともに，ITO の全体最適の実現を目指す．

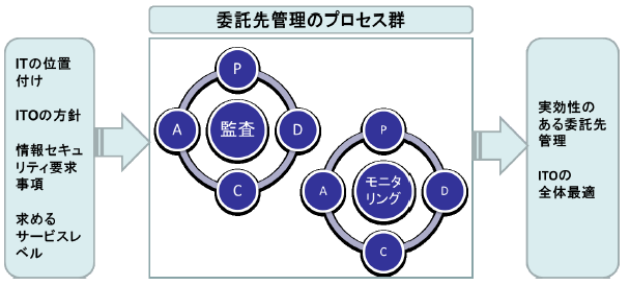

図 6　ITOMS の改善活動

委託先の管理プロセスを必要に応じて，局所的・場当たり的に実施するのではなく，独立したマネジメントシステ

i) トップのリーダーシップのもとに組織が一丸となり，顧客が高度に満足する製品やサービスを提供するための一連の活動．

ムの中で継続的に取り組むことで，委託先管理が定形化して，書類だけをチェックするなど，形骸することを防ぐ．

ITOMS は，より少ないコストと時間で委託先を管理することによって，情報セキュリティの確保やサービスレベルの維持を目指す．IT サービスの品質を管理するという点に，QMS との類似点がある．したがって，ITOMS のモデル化では，主として QMS の概念を取り入れる．

また，ITOMS では，委託先管理のプロセス群に，5.1 節で提案したプロセスアプローチを採用する．これは，プロセスアプローチの利点の一つとして，プロセスの組合せや相互関係とともに，マネジメントシステムにおける個別のプロセス間のつながりを把握・管理できるからである．ITO のプロセス群は，完全に独立しているわけではなく，関連性がある．例えば，監査を行なう場合に，モニタリングで定期的にチェックしている事項を対象に含めることは，非効率な場合がある．また，モニタリングや監査を行なう際に，契約内容を参照する場合もある．このような相互関係を予め把握・管理しておくことで，より効率的な管理を期待できる．そこで，各プロセスを正確かつ明確に定義することが重要となる．

(4) PDCA の内容

ITOMS は委託先管理の個々のプロセスについて，PDCA による見直しを行なう．すなわち，各プロセスを PDCA による見直しの対象とすることが，提案したプロセスアプローチによる PDCA サイクルの特徴である．一方で，同じマネジメントシステムの一つである ISMS では，情報資産に対する情報セキュリティのマネジメントシステムそのものを対象として，PDCA による見直しを行なうため，ITOMS と観点が異なる．この違いを表 3 に示す．

表 3　ISMS とプロセスアプローチ（ITOMS）における PDCA の違い

	ISMS[11]	プロセスアプローチ（ITOMS）[16]を参考に作成
Plan（計画）	【ISMS の確立】 組織の全般的な方針及び目的に従った結果を出すための，リスクマネジメント及び情報セキュリティの改善に関連した，ISMS 基本方針，目的，プロセス及び手順を確立する．	【プロセスの計画】 プロセスを定義し，その相互関係を明確にする．その上で，プロセスを計画し，実行に必要となる資源を準備する．可能な場合は，目標を定数化する． ※ISMS よりも対象範囲が広い．
Do（実行）	【ISMS の導入及び運用】 ISMS の基本方針，管理策，プロセス及び手順を導入し運用する．	【プロセスの実施】 計画に沿って，必要となる資源や情報を利用可能な状態にし，プロセスを実行．運用・監視及び測定を行なう．
Check（点検）	【ISMS の監視及びレビュー】 ISMS 基本方針，目的及び実際の経験に照らした，プロセスのパフォーマンスのアセスメント（可能ならば測定），及びその結果のレビューのために経営陣に報告する．	【プロセスのレビュー】 プロセスの実行結果及び実施状況を分析する．必要に応じて，関係部署や経営陣に報告する． ※情報資産に特化しないため，関連するプロセスをチェックすることになる．
Act（改善）	【ISMS の維持及び改善】 ISMS の継続的な改善を達成するための，ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた，是正処置及び予防処置を実施する．	【プロセスの改善】 プロセスの計画達成のための処置と継続的改善の実施．

5.3 期待される効果とプロセス

本項では，委託先の管理プロセスのうち監査とモニタリングについて，プロセスアプローチによる PDCA サイクルを実践した場合に期待される効果とプロセスを検討する．なお，ここで言う監査やモニタリングは，委託先管理としての PDCA の C（点検）を指すのではない．監査やモニタリングを個別のプロセスとして定義して，各々のプロセスで PDCA を実施させるものである（図 6）．例えば，監査については，P（監査計画）－D（監査実施）－C（監査評価）－A（結果のフィードバック）といった形で検討を行なう．

(1) 監査

監査では，監査計画を作成した上で監査を実施し，結果のレビューを行なう．監査で通常言うところの改善は，監査意見を受けた上でのシステムの性能やセキュリティの向上である．それだけではなく，委託先へ監査を行なった際の計画や実施内容，結果のレビューについて見直しを行ない，今後の改善に繋げていくことが ITOMS による監査である．それにより，監査の形骸化や監査項目の内容の不足を防ぐことができる．

また，監査はその目的や対象，評価の視点から大きくシステム監査と情報セキュリティ監査に分けることができる j．まず，システム監査については，その対象が情報システムとなるため，技術的な内容（情報システムの開発プロセス．受入れ試験など）にも踏み込む必要がある．システム監査は，情報システムのライフサイクル（情報戦略の策定から，企画，開発，運用，保守）の適切性に関する監査 [17] でもあり，情報システムの安全性や信頼性，効率性を評価することになる．つまり，ライフサイクルに関する委託先での内部プロセスだけでなく，性能の評価や使用されている技術が適切かどうかといった判断も必要となる．したがって，例えば監査ごとに技術テーマを設定・変更することで，委託元の監査人もスキルや最新動向に精通していなければならず，委託元の技術力の保全を図ることも可能であると言える．

一方で，セキュリティ監査については，情報資産を対象としているため技術的な内容に踏み込むことは多くない．情報資産の管理方法や体制が主となるため，監査が定形化し，形式的なものとなる可能性は高い．したがって，委託元の方針や規程などの見直しも念頭に，監査プロセスを PDCA によって実施していく必要がある．このような場合，委託先が作成した言明書k に沿って監査を行なうことで，改善活動における尺度を明確にすることができる．

(2) モニタリング

委託先のモニタリングには，定期的なものとトラブル等の発生に伴う随時的なものがある．前者については，PDCA のサイクルが極めて遅くなり，C（点検）のフェーズのみが形式的に繰り返され，P（計画）や A（改善）といったフェーズに入らないことが考えられる．また，後者については，突発的に発生することが多いと言え，当該トラブル等の収束にのみ注力され A（改善）に活かされない可能性がある．

定期的なモニタリングについては，PDCA サイクルを定例的に回す仕組みが必要となる．そのためには，P（計画）を見直すタイミングを決めておいたり（例えば月 1 回），エラー件数などの定量的な管理指標が設定値に達した場合に，行動に移るよう委託先との間で取り決めをしておくことが必要となる．そうすることで，PDCA によって適切なタイミングで継続的に，モニタリングのプロセスを見直す仕組みを構築することが期待できる．

j) 日本システム監査人協会の資料 [17]より作成

	システム監査	セキュリティ監査
目的	IT ガバナンスの実現に寄与	情報資産の適切な管理・活用
対象	情報システム	情報資産
評価の視点	安全性．信頼性．効率性	機密性．完全性．可用性 ≒情報システムの安全性

k) 情報セキュリティに関するリスクマネジメントが効果的に実施されるよう．リスクアセスメントに基づいて適切なコントロール（管理策）を整備し運用している」旨の経営陣による確認書．（公認情報セキュリティ監査人研修テキスト．p.80 より）

6. まとめと課題

ITO を活用していく中で，情報システムの高度な信頼性・安定性を確保していくためには，情報システムへの関与を薄めず，自組織が有する技術力の低下を防ぐことが必要となる．そこで，本研究では，IT 外部委託先管理を独立したマネジメントシステムを構築・運用することで，IT を取り巻く技術や環境の変化への対応を行ない，自組織の技術力を維持する仕組み（ITOMS）を提案した．

今後の課題として，プロセスアプローチの実施ステップに沿った，具体的な当てはめが必要となる．現時点では抽象的であり，具体的な情報システムを想定のもとで，モデルへの実際の当てはめを行なうことで，その有効性を示さなければならない．

その上で，実組織において運用することの有用性やメリットを，客観的な数値等によって検証する必要がある．

謝辞 本研究を進めるにあたり，様々なアドバイスを頂いた情報セキュリティ大学院大学・原田研究室の皆様に感謝致します．また，アンケートのデータ入力に多大なご協力を頂いた．神奈川県内特別支援学校の皆様に深く感謝致します．

参考文献

[1] 日経コンピュータ, システム障害はなぜ二度起きたか, 図書印刷,2011 年.

[2] 経済産業省, アウトソーシングに関する情報セキュリティガイダンス, 2009 年 6 月.

[3] 関口和代, “アウトソーシング・ビジネスの現状と課題 ―ビジネス・プロセス・アウトソーシング（BPO）を中心に―,” 東京経大学会誌 第 270 号, 2011 年.

[4] 経済産業省, “情報処理実態調査結果（平成 22 年～24 年）,” http://www.meti.go.jp/statistics/zyo/zyouhou/result-2.html. 2013 年 12 月 12 日アクセス

[5] 佐々木崇裕・原田要之助・福島健二・河野翔太・久保知裕・渡邉晴方・佐藤栄城・新原功一, “企業・組織における情報

セキュリティ調査," 2014 年 暗号と情報セキュリティシンポジウム（SCIS2014）, 2014 年.

[6] 上山浩, "クラウド時代の IT 法務（第 4 回）「個人情報の漏洩リスクを考慮 再委託先の管理責任も明文化",日経コンピュータ No.802,2012 年 2 月 16 日,p.104-107

[7] 日本銀行, "金融機関におけるシステム共同化の現状と課題－地域銀行 108 行へのアンケート調査結果からー," リスク管理と金融機関経営に関する調査論文,2009 年.

[8] 日本規格協会, "マネジメントシステムのためのプロセスアプローチの概念及び利用に関する手引,"
http://www.jsa.or.jp/stdz/iso/pdf/process2.pdf.
2014 年 3 月 2 日アクセス.

[9] 日本規格協会, "品質マネジメントの原則,"
http://www.jsa.or.jp/stdz/iso/pdf/qmp.pdf. 2014 年 3 月 2 日アクセス.

[10] BSI ジャパン, "マネジメントシステムとは,"
http://www.bsigroup.jp/ja-jp/assessmentandcertification/managementsystem/ataglance/whatisms/. 2013 年 12 月 13 日アクセス.

[11] JIPDEC, "情報セキュリティマネジメントシステム適合性評価制度の概要（JISQ 27001:2006 対応版）,"
http://www.isms.jipdec.or.jp/doc/ismspanf.pdf.
2013 年 12 月 13 日アクセス.

[12] JISC, "ISO9000 ファミリーについて,"
http://www.jisc.go.jp/mss/qms-9000.html. 2013 年 12 月 13 日アクセス.

[13] 日本工業規格, "JISQ 9001:2008「品質マネジメントシステムー要求事項」," 2008 年 12 月.

[14] 小笠原秀人, "特集『我が国のソフトウェア品質技術の潮流』ソフトウェアプロセス改善," 品質, vol42, No.4, pp. 22-27, 2012 年 10 月.

[15] 赤林隆仁, "IT 内部統制に関する考察－ISO27001 ISO9001 の活用ー," 埼玉学園大学紀要（経営学部篇）第 7 号, pp.177-187, 2007 年 12 月.

[16] 岩波好夫, 図解 ISO9000 よくわかるプロセスアプローチ, 日科技連出版社, 2009.

[17] 日本システム監査人協会, "システム監査と情報セキュリティ監査の違い Q&A,"
http://www.saaj.or.jp/team_for10years/QandA10_201002.pdf.
2014 年 3 月 2 日アクセス.