SCIS 2014 The 31st Symposium on
Cryptography and Information Security
Kagoshima, Japan, Jan. 21- 24, 2014
The Institute of Electronics,
Information and Communication Engineers

IT 外部委託先管理の実効性向上に資する方策の検討
Study on method for improvement of effectiveness in IT Outsourcing Management

河野 翔太* 原田 要之助*
Shota Kono Yonosuke Harada

あらまし IT アウトソーシングを活用する場合、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。委託元は、情報システムを取り巻く技術や環境の目まぐるしい変化に対応し、IT 外部委託先管理の実効性の維持・向上に努めなければならない。本論文では、IT 外部委託先管理をマネジメントシステムとして構築し、プロセスアプローチによって有効性を維持・向上していく仕組みの試案を紹介する。

キーワード アウトソーシング、委託先管理、マネジメントシステム、プロセスアプローチ

1 はじめに

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る。情報システムは、今や事業を営む組織の事業戦略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である。そこで、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）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、情報システム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、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丸投げの状態になったり、ブラックボックス化することなどが考えられる。このような結果、技術力や IT リスクへの関心が低下し、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。

2012 年に発生した、委託先やサービスプロバイダの管理を巡る事件を紹介する。

1.1 再々委託社員による不正データ取得

表 1：事件の時系列
（NTT データの調査結果[1]を元に作成）

日付	内容	備考
2012.6.2	情報取得（1 回目）	
2012.9.10	情報取得（2 回目）	
2012.9.17	ATM で顧客の預金を出金（50 万円）	警察に相談 捜査へ
2012.10.1	情報取得（3 回目）	
2012.11.20	NTT データへ 捜査協力要請	NTT データが 事件を把握
2012.11.27	容疑者逮捕	

(i) 概要

銀行の共同システムを運営するベンダ（NTT データ）の再委託先の社員が、顧客の取引情報を不正に取得。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とされる事件である。

* 情報セキュリティ大学院大学、
〒221-0835 神奈川県横浜市神奈川区,鶴屋町 2-14-1、
Institute of Information Security,
2-14-1 Turuya-cho, Kanagawa-Ku, Yokohama-shi, Kanagawa, 221-0835, Japan

当該共同センターでは、顧客データのうち、口座番号や暗証番号などの重要情報を暗号化またはマスク処理した状態で、データベースに格納している。

そこで、容疑者は、障害時の調査や復旧作業に必要でマスク処理がされていない「システム基本情報」を狙い、自作したツールによって情報を盗取したとされる[2]。

NTT データの調査[1]によると、約半年に渡り少なくとも計 3 回、情報が不正に取得されたとされている。一方で、NTT データが事件を把握したのは、警察から捜査協力依頼された時点である。NTT データが犯行を検知できなかった根本的な原因は、「システム基本情報」のアクセスログが未取得であったことである。また、本件のように、開発担当者が本番データにアクセスする場合には、①必ず複数人で作業を行ない、②実施した作業内容は、その証跡とともに責任者に提出し、チェックを受けるルールが制定されていた。しかし、幾度にも渡る情報の不正取得を許した以上、マネジメントが有効に機能していたとは言えない。

(ii)　責任の所在

共同センター内での管理体制やプロセスが、不十分であったことは言うまでもなく、運営する NTT データの管理責任が問われたことは当然である。一方で、共同センターに参加する銀行の管理責任を追及する報道や見解は、見られなかった。たしかに、本件は銀行の外部に存在するデータセンターでの犯行であり、銀行に過失はないように見える。しかし、共同システムへの参加はあくまで銀行都合によるものである。顧客の属性情報や金融資産情報は特に秘匿性の高い情報であり、それらを銀行の外部で扱う場合には、厳格に管理しなければならない。具体的には、共同センターでの情報セキュリティ対策が有効であるか、内部管理体制に不備がないか、などの点について、継続的にモニタリングや評価を実施する必要がある。

1.2　サービスプロバイダによるデータ滅失漏えい

(i)　概要[3]

ファーストサーバ社（以下、FS 社という）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の不具合により、約 5,600 ユーザのデータが滅失した事件である。

当該作業は、通常定められているメンテナンス作業と異なる手段で行われていた。なお、作業担当者は、10 年もの間マニュアルで定められていない独自の方式でメンテナンス作業を行なっていたが、上長はこれを黙認していた。

さらに、ユーザからの要望に応える形で、滅失した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。

(ii)　問題点

FS 社では、10 年にも渡りマニュアルと異なるメンテナンス作業を継続していた。また、外部媒体へのバックアップもされておらず[3]、情報セキュリティに対して杜撰な取組みがされていたと言える。FS 社はレンタルサーバサービスを提供している。そのサービスを利用する以上、データ保管先において、適切な情報セキュリティ対策のもとで、サーバが運用・管理されている必要がある。佐藤[3]は、パブリッククラウドサービスの事業者の選定時に、ISMS や P マークの認証取得を判断基準とする場合が多いが、ユーザの期待と実際の保証とのギャップが生じていることを指摘している。

第三者認証のみならず、プロバイダそのものやサービスの実態を把握し、事業者を適切に選定、管理しなければならない。

2　IT アウトソーシング

2.1　定義

経済産業省[4]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。

2.2　モデル

経済産業省[4]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捉えている（図 1）。

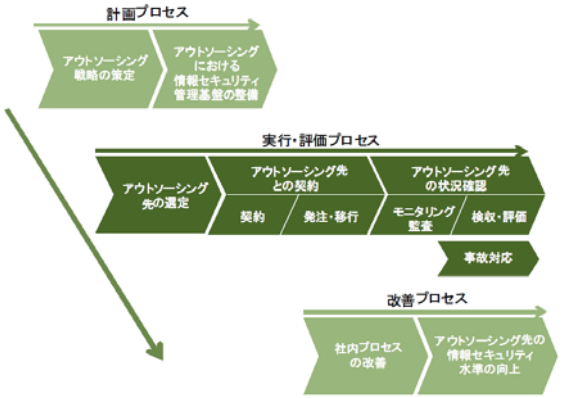

図 1：アウトソーシングのプロセス
（出所：経済産業省[4]、p.9）

本研究もこれに倣い、情報システムを対象とするアウトソーシング（IT Outsourcing、以下 ITO という）における、委託元のプロセスに着目する。その際、アウトソーシングを「組織間での業務の受託と委託の関係」（関口[5]）と捉え、従業員の雇用関係などは考慮しない。

2.3　動向

矢野経済研究所の ITO サービス市場に関する調査結果（2013 年度）[6]から、市場規模の推移を図 2 に示す。

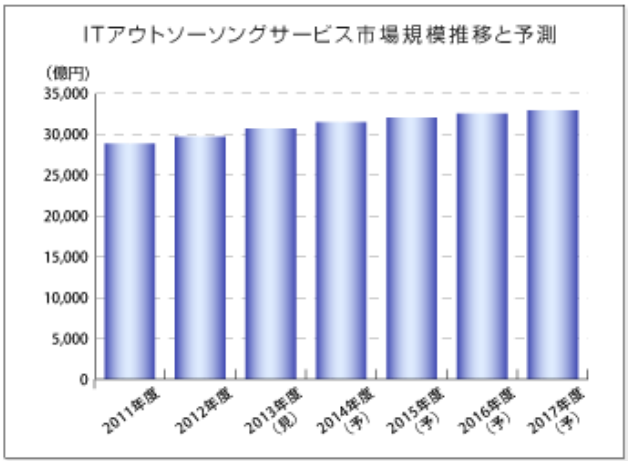

図 2：ITO サービス市場規模推移と予測
（出所：矢野経済研究所[6]）

2013 年度の市場規模は、前年度比 3.5%増の 3 兆 722 億円を見込んでいる。また、データセンターの利用が進むことで、今後も堅調に市場が拡大すると予測している。なお、データセンターの利用が進む要因として、次の 6 つを挙げている。

① データ量の増加
② 情報管理の重要性の高まり
③ 環境対策面からの需要
④ 競争力の確保を目的とした需要
⑤ クラウドコンピューティングの概念の普及
⑥ システム部門の人材不足

IDC Japan[7]は、国内 IT サービス市場における 2012 年～2017 年の年間平均成長率を 1.5%と予測しているが、ITO サービスに関しては、より活発な成長が見込まれる。

2.4　情報セキュリティの現状

(i) 経済産業省による情報処理実態調査[8]

同調査では、情報セキュリティトラブルの発生についての質問項目が設けられている。

表 2：重要情報漏えい事故の発生割合（単位：%）
（経済産業省の調査結果[8]を元に加筆修正）

	2009 年	2010 年	2011 年
全体	19.8	20.2	21.3
ｺﾝﾋﾟｭｰﾀｳｲﾙｽ	1.2	1.0	0.7
不正ｱｸｾｽ	0.3	0.3	0.5
標的型ｻｲﾊﾞｰ攻撃	―	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

表 2 は、過去 3 年間の重要情報漏えい事故についての原因別の推移である。委託先による情報漏えいは、コンピュータウイルスや不正アクセスを原因とする情報漏えいよりも多く、内部者による情報漏えいと同水準である。

また、重要情報漏えい事故の発生割合が年々高まっている一方で、その原因がコンピュータウイルスである割合は、減少している。その背景の 1 つとして、ウイルス対策ソフトの進歩が挙げられるのではないか。近年のウイルス対策ソフトのスキャンでは、従来からのパターンファイルとのマッチングに加え、ヒューリスティック技法が取り入れられていること多い。シマンテック[9]によると、最先端のヒューリスティック技法を用いた場合の、未知のウイルス検知率は 70～80%であり、未知の脅威に対する効果は着実に高まっていると言える。

強力な対策によってコンピュータウイルスが抑止されているとしても、委託先での情報漏えい事故の発生割合の方が高くなっている本調査結果は無下にできず、ITO を活用する場合には、委託先に対して厳格な管理を実施しなければならない。さらに、委託業務で個人情報を提供する場合には、個人情報保護法第二十二条により、委託先を必要かつ適切に監督[1]する義務が発生することに、留意する必要がある。

(ii) 情報セキュリティ調査[12]

筆者が所属する情報セキュリティ大学院大学の原田研究室では、毎年 7 月から 8 月に掛けて情報セキュリティ調査を実施している（以下、情報セキュリティ調査という）。

図 3 は、情報セキュリティの 3 要素のうち、ITO の委託元が最も重視する要素についての質問に対する回答を集計したものである。

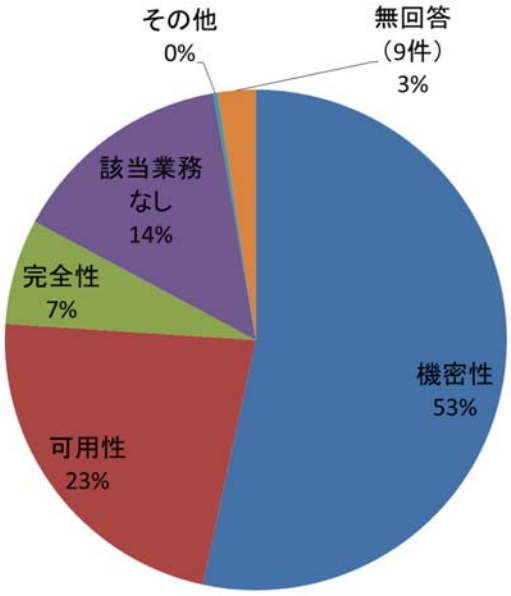

図 3：ITO において委託元が最も重視する
情報セキュリティ要素（N=367）[12]

[1]岡村[10]は、「委託前と同様の安全管理水準を保つために要する監督」であるとする。

機密性を挙げる組織が過半数を占める一方で、可用性、完全性は少ない。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[12]。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。

経済産業省の情報処理実態調査[8]では、システムの停止が発生した組織が 50%を超えている一方で、重要情報の漏えいは 20%前後である。機密性を重視した情報セキュリティ対策が、情報漏えい事故の発生を抑止している可能性があると考えられる。

2.5 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。それらを追及することは、ITO の形態を複雑化させ、委託先管理をより困難にする場合がある。以下にその例を示す。

(i) 再委託

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が起こり得る。これが、再委託である。経済産業省[4]は、単純な直列構造だけでなく、再委託がツリー構造になる場合やネットワーク構造になる場合があるとしている。

(ii) 複合委託

1 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である。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[4]。

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[11]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ある。ITO が多段階になったり、複雑な構成になるほど、委託先を直接的に管理することが難しくなる。

3 委託先管理

3.1 定義

本研究における委託先管理とは、経済産業省の示すアウトソーシングプロセス（図 1）のうち、実行・評価フェーズおよび改善フェーズの各プロセスにおいて、委託先の情報セキュリティを確保するための手法を言う。本章では、実行・評価フェーズのうち、モニタリング・評価プロセスを対象とし、検討を行なう。

3.2 管理手法

委託先管理の具体的な手法としては、以下の 4 つのような方法が考えられる。

① ヒアリング（打合せ）
② 報告書受領
③ 立入監査
④ 第三者による監査結果の入手

情報セキュリティ調査では、委託先に対する管理手法の導入状況について、図 4 のような回答を得ている。

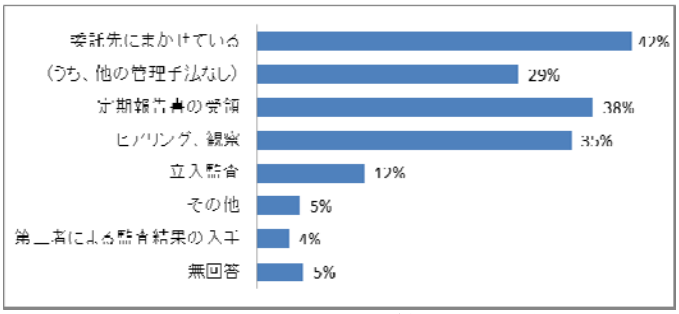

図 4：回答組織に占める委託先管理手法の導入割合（委託業務が無い先を除く、N=248）

回答では、「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」組織もあった。ただ、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、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恐れがあると言える。

この調査結果の背景には、回答組織に売上高や人員から見て中小規模の組織が多いことがあると考えられる。表 3、表 4 は、回答組織の売上高（5 階層に再分類）と、「ヒアリング、観察」および「定期報告書の実施」の実施状況をクロス集計した結果である。

表 3：売上高と「ヒアリング、観察」実施有無のクロス表（N=367）

（単位：組織）

売上高（5階層）	ヒアリング、観察		合計
	実施あり	実施なし	
3億円未満	15 (19%)	65 (81%)	80 (100%)
3億円～10億円未満	16 (21%)	61 (79%)	77 (100%)
10億円～50億円未満	27 (23%)	90 (77%)	117 (100%)
50億円～1,000億円未満	16 (27%)	44 (73%)	60 (100%)
1,000億円～	11 (48%)	12 (52%)	23 (100%)
無回答	3 (30%)	7 (70%)	10 (100%)
合計	88 (24%)	279 (76%)	367 (100%)

表 4：売上高と「定期報告書の受領」実施有無のクロス表（N=367）

（単位：組織）

売上高（5階層）	定期報告書の受領		合計
	実施あり	実施なし	
3億円未満	14 (18%)	66 (82%)	80 (100%)
3億円～10億円未満	15 (20%)	62 (80%)	77 (100%)
10億円～50億円未満	26 (22%)	91 (78%)	117 (100%)
50億円～1,000億円未満	18 (30%)	42 (70%)	60 (100%)
1,000億円～	16 (70%)	7 (30%)	23 (100%)
無回答	5 (50%)	5 (50%)	10 (100%)
合計	94 (26%)	273 (74%)	367 (100%)

表 3、表 4 とも、売上高が高い組織ほど、ヒアリングなどの対策の実施率が、高いことが分かる。同様の傾向は売上高ではなく、従業員数を用いてクロス集計を行なった場合にも確認できた。

また、別の設問によると、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が 80%弱に上っている[12]。規模の小さな組織では、人員の不足などの問題から、委託先管理の実施がままならない状況が分かる。

なお、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。図 5 は、日銀による 2009 年の調査結果である。

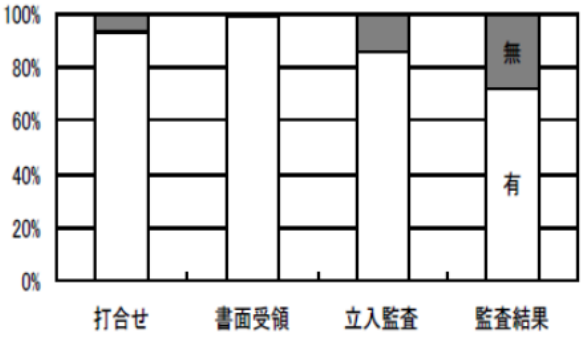

図 5：地方銀行の委託先管理手法の導入状況（出所：日本銀行[13]、p.40）

打合せおよび報告の書面受領の実施率は 90%を超え、立入監査および監査結果の入手でも 70%を超えている。当研究室の調査結果と比べると、極めて高い数値である。

銀行は、顧客の個人情報や金融資産情報などの秘匿性が高い情報を扱っている。また、監督官庁である金融庁は、銀行の業務委託先に対して報告徴求および立入検査を実施することが認められている（銀行法 24 条 2 項、25 条 2 項）。さらに、企業規模でも、当研究室が回答を得た組織を上回ることが、一般的と思われる。

これらの理由から、委託先に対して様々な手法を用いて管理に努めている様子が伺える。

3.3 再委託

2. 4 節で述べた通り、ITO の形態が複雑化する理由の 1 つに再委託の問題がある。上山[11]は、受託先が再委託を行なう場合は、事前に委託元の承諾を得ることを原則とし、再委託先で問題が発生した場合には、その委託元である一次委託先が責任を負う契約内容にすべきであると述べている。

また、再委託の禁止を契約内容に盛り込むことも考えられる。情報セキュリティ調査[12]では、ITO を利用する組織の約 30%が、再委託を禁止している。

再委託の制限や禁止によって、委託先管理の実効性が飛躍的に向上するわけではない。また、制限や禁止が設けられていないことが、直ちに問題となるわけではない。しかし、再々委託社員によるカード事件に見られるように、組織は、二段階以上の委託によるリスクについて、十分に留意しておく必要がある。

4 マネジメントシステム

BSI ジャパン[14]は、マネジメントシステムを「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」と説明している。

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、情報セキュリティマネジメントシステム（ISMS）と品質管理マネジメントシステム（QMS）を紹介する。その上で、委託先管理をマネジメントシステムとして構築する事の必要性・有用性を検討し、具体的なフレームワークを示す。

4.1 ISMS

JIPDEC[15]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 6 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 6：ISMS の改善活動（出所：JIPDEC[15]）

4.2 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[16]。組織は、JIS Q 9001:2008[17]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[17]。

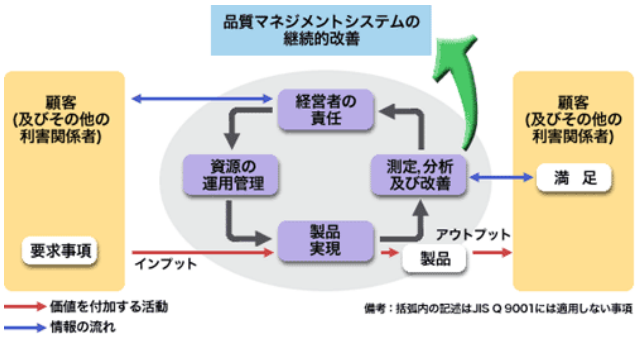

図 7：QMS の改善活動（出所：JISC[16]）

4.3 委託先管理への応用

委託先における情報セキュリティの重要性・困難性に鑑み、PDCA サイクルによって委託先管理の有用性を継続的に見直す仕組みが必要である。このような仕組み自体は目新しいものではなく、経済産業省の示すモデル（図 1）が、一般的である。本稿では、このモデルを IT 外部委託先マネジメントシステム（ITOMS：IT Outsourcing Management System）と呼ぶ。

5 提案モデル

5.1 概要

ITOMS を構築する際の前提条件は、ITO の全般的な「方針」が策定されていることである。これは、ISMS や QMS と同様である。

その上で、ITOMS では、委託先管理に関する個々のプロセスについて、PDCA サイクルによる継続的な改善を図る（図 8）。

図 8：ITOMS の改善活動

各プロセスに対する継続的な改善活動の結果、委託先管理の実効性が向上し、ITO の全体最適の実現に繋がる。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、マネジメントシステムの中で継続的に取り組むことが、本モデルの特徴である。

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。

ITOMS では、委託先管理のプロセス群に着目したプロセスアプローチを採用する。プロセスアプローチの利点の 1 つに、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・管理できること[17]がある。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。

5.2 プロセスアプローチの実施ステップ

図 9 は、QMS の一般要求事項として、実施が求められる事項である。

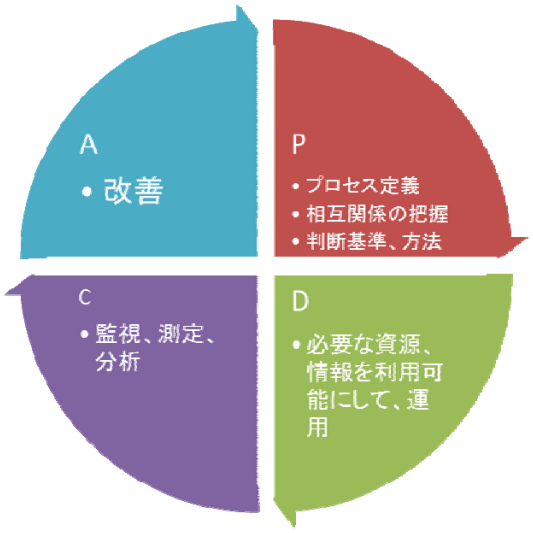

図 9：一般要求事項の各項目と PDCA（出所：沖本[18]）

組織は、各プロセスを QMS 規格の要求事項に従って、運営管理しなければならない。また、プロセスをアウトソースした場合には、組織の QMS の中で管理の方式および程度を定め、該当プロセスに関して管理を確実に実施することが求められている。

プロセスアプローチを実践する際には、図 9 に示す要求事項を満たすための具体的な手法を、事前に確定しておくべきである。副田[19]は、日本規格協会（JSA）が公開する手引[20]を元に、独自の実施ステップを作成している（表 5）。本モデルでは、このステップに沿って、各プロセスの解析・整理を行なう。

表 5：プロセスアプローチの実施ステップ
（出所：副田[19]）

ステップ	No.	手順
ステップ 1 プロセスの特定	1.1	組織の目的とアウトプットを明確にする
	1.2	組織の方針及び目標を明確にする
	1.3	組織のプロセスを明確にする
	1.4	プロセスのつながりを決定する
	1.5	プロセスの所有者を明確にする
	1.6	プロセスの文書化ニーズを明確にする
ステップ 2 プロセスの計画	2.1	プロセスの目的・目標を明確にする
	2.2	プロセスに必要な資源を明確にする
	2.3	プロセス内の活動を明確にする
	2.2	プロセスの測定事項を明確にする
	2.4	意図した目的に対してプロセスを検証する
ステップ 3 プロセスの実施及び測定	3.1	活動の実施
	3.2	活動の測定・管理
ステップ 4 プロセスの分析	4.1	パフォーマンスの把握
	4.2	パフォーマンスと要求との比較
	4.3	改善の機会の明確化
	4.4	トップへの報告
ステップ 5 プロセスの是正処置及び改善	5.1	是正処置方法の決定
	5.2	是正処置の実行と検証
	5.3	継続的改善の実施
	5.4	改善効果の検証
	5.5	潜在的問題の明確化と予防処置

5.3 タートル図

プロセスアプローチを実践する際のツールとして、図 10 のようなタートル図を採用する。

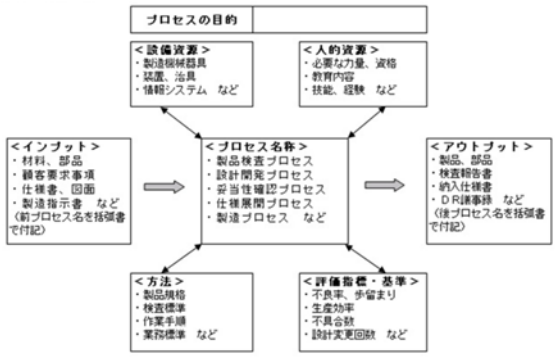

図 10：ISO9001 でのタートル図の運用
（出所：Mottai-Navi[21]）

タートル図は、その名が示す通り「亀」のような形の図である。甲羅にあたる中心部分にプロセスを据え、関連する要素を整理することで、ポイントとなる項目を漏れなくリストアップするためのツールである。

図 10 のように、プロセス、インプット、アウトプットの他に、設備資源、人的資源、方法、評価指標・基準を項目とすることが一般的である。本モデルでは、IT が技術革新の激しい分野であることに鑑み、プロセスに影響を与える技術などの「環境」の変化を、項目に加える。

タートル図を用いることで、そのプロセスにおいて、何が重要であるかを視覚的に把握することができ、効率的かつ漏れなく、プロセスを実施・改善することが期待できる。また、プロセスごとに整理することで、プロセス間の相互関係の把握に繋げることができる。

5.4 他のマネジメントシステムとの統合

組織が、ISMS や QMS など、複数のマネジメントシステムを導入している場合、それらを個別に運営管理することは非効率である。委託先管理および ITOMS は、あくまで委託元組織における情報セキュリティ対策の一環であるため、特に ISMS との統合性は高いと言える。このように、複数のマネジメントシステムを統合して導入する場合を、統合マネジメントシステム（IMS：Integrated Management System）と呼ぶ[2]。
医療現場における ISMS と QMS との統合事例[22]など、様々な導入事例があり、IMS に対する認証審査サービスも提供されている。

6 まとめと今後の方向性

本稿では、組織の情報セキュリティにおける委託先管理の重要性を検証した。そして、タートル図によるプロセスアプローチを活用することで、より少ないコストと時間で実効性のある委託先管理を実施すること。また、マネジメントシステムの仕組みを取り入れることで、継続的な改善活動を実施することを提案した。

今後は、個別のプロセスをモデルに当てはめて分析・検討を行ない、有効性や問題点を確認しつつ、さらに詳細なモデル化を進める予定である。

参考文献

[1] NTT データ,“キャッシュカード取引情報の不正取得に関する調査結果および再発防止等について”,http://www.nttdata.com/jp/ja/news/release/2013/011700.html,2013 年 12 月 15 日アクセス

[2] 小笠原啓,“動かないコンピュータ「最大 1068 口座の情報を不正取得　システム監視体制に三つの不備」”,日経コンピュータ　No.830,2013 年 3 月,p.20-22

[3] 佐藤栄城・原田要之助,“クラウドサービス利用における第三者認証制度の考察”,情報処理学会研究報告,vol.2013-EIP-59 No.1,2013 年 2 月

[4] 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

[5] 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

[6] 矢野経済研究所,“IT アウトソーシングサービス市場に関する調査結果 2013（サマリー）”,http://www.yano.co.jp/press/press.php/001106,2013 年 12 月 12 日アクセス

[2] ISO/IEC27013 は、ISO/IEC20000-1（ITSMS）と ISMS の統合認証のためのガイドラインである。

[7] ITmedia,“国内サービス市場は低成長ながらも拡大－IDC 予測”, http://www.itmedia.co.jp/enterprise/articles/1310/30/news136.html,2013 年 12 月 12 日アクセス
[8] 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
[9] シマンテック, “ヒューリスティック手法詳説：シマンテックの Bloodhound 技術”, http://www.symantec.com/region/jp/avcenter/reference/heuristc.pdf,2013 年 12 月 6 日アクセス
[10] 岡村久道,「個人情報保護法の知識＜第 2 版＞」,日本経済新聞出版社,2010 年 1 月,p.163
[11] 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
[12] 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”,2013 年 暗号と情報セキュリティシンポジウム（SCIS2013）,2014 年 1 月
[13] 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－”,リスク管理と金融機関経営に関する調査論文,2009 年 6 月
[14] 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
[15] 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（JIS Q 27001:2006 対応版)”, http://www.isms.jipdec.or.jp/doc/ismspanf.pdf, 2013 年 12 月 13 日アクセス
[16] JISC, “ISO9000 ファミリーについて, ” http://www.jisc.go.jp/mss/qms-9000.html, 2013 年 12 月 14 日アクセス
[17] 日本工業規格, “JIS Q 9001:2008「品質マネジメントシステム－要求事項」”,2008 年 12 月
[18] 沖本一宏,「タートルチャート活用によるプロセスアプローチの実践」,日科技連出版社,2010 年 4 月
[19] 副田武夫, “プロセスアプローチの QMS への実装理論と事例”, 標準化研究 7(1), 標準化研究学会,21-31, 2009
[20] JSA, “ISO9000 導入・支援パッケージ”, http:www.jsa.or.jp/stdz/iso/pdf/process2.pdf, 2013 年 12 月 14 日アクセス
[21] Mottai-Navi, “【品質管理テーマ】ISO9001 での「タートル図」の運用”, http://www.mottai-navi.com/Contents/QCEcoLaw/Op_Turtle_Cht.html,2013 年 9 月 15 日アクセス
[22] 田中宏明, “医療分野における「ISO9001 と ISO27001 の統合と運営管理」(<特集>ISO 統合マネジメントシステムの運営管理) ” “, 品質 40(3), 日本品質管理学会,261-265, 2010-07-15
[23] 中村翰太郎, “ISO 品質マネジメントシステム規格におけるプロセスアプローチに関する考察(<特集>プロジェクト時代の品質マネジメント) ”,プロジェクトマネジメント学会誌 5(5),3-8, 2003-10-15