

WG 2

ISMS/ITSMS との連携の実現性の
調査研究について

平成 24 年 3 月



一般財団法人日本情報経済社会推進協会

本書に記載されている会社名、製品名は、各社の登録商標または商標です。

ISMS/ITSMS との連携の実現性の調査研究について

目次

1.	はじめに.....	1
1.1.	これまでの取り組み.....	1
1.2.	SAM と ISMS/ITSMS の連携	1
2.	マネジメントシステムの比較検証.....	5
2.1.	マネジメントシステムの統合の可能性.....	5
2.2.	ソフトウェア資産管理とサービス管理.....	5
2.2.1.	SAM、ITSMS の定義	5
2.2.2.	SAM、ITSMS のスコープ	7
2.2.3.	SAM、ITSMS の共通項	8
2.2.4.	ISO 19770-1 と ITIL V3 の比較	9
2.2.5.	ISO 19770-1 における「組織」、「顧客」の表現に注意する	11
2.2.6.	SAM と ISMS の類似点	11
2.3.	統合運用.....	12
2.3.1.	統合運用について.....	12
2.3.2.	マネジメントシステム.....	14
2.3.3.	SAM と ITSMS の関係	15
2.3.4.	CI（構成要素）と Asset（資産）の関係	17
2.3.5.	統合運用に向けて.....	21
3.	SAM と ISMS/ITSMS の運用サイクルと管理メッシュ	22
3.1.	企業・組織における ISMS/ITSMS 活動実態	22
4.	マネジメントシステムの管理策の相互依存性.....	23
4.1.	ISMS「資産目録」に関する管理実態	23
4.2.	SAM ができていないことによる ISMS/ITSMS への影響	26
4.2.1.	SAM の要求事項と ISMS/ITSMS との関連性	26
4.2.2.	SAM を実施する上での ISMS の先行実施の有用性	28
4.2.3.	SAM を実施する上での ITSMS の先行実施の有用性	29
5.	結果と考察.....	33

1. はじめに

1.1. これまでの取り組み

わが国では、2005年の個人情報保護法の施行、2007年の金融商品取引法の改正施行等により、企業・組織におけるコンプライアンス意識は全般的に高まって来た。しかし IT 資産、とりわけソフトウェア資産については、依然としてソフトウェアの違法コピーやライセンスの不正利用などの不祥事が続いており、企業・組織の保有資産として適切に管理されているとは言いがたい。このように SAM については“コンプライアンスの暗黒大陸”という状況が続いている。一方、不況の長期化に伴い、企業・組織では IT 資産/ソフトウェア資産についてこれまで以上に効率的な資産運用が求められている。このように、コンプライアンスの観点からは IT 資産/ソフトウェア資産は使用状況に応じたライセンスの購入が求められており、資産効率向上の観点からは不要な IT 資産/ソフトウェア資産の削減が求められる。このような相反する要素を総合的に解決するために、企業・組織が適切なソフトウェア資産管理 (SAM) を行うことはいまや不可欠となっている。JIPDEC では 2009 年度より SAM の普及活動に取り組んでおり、2010 年度の研究成果として以下の文書を発表した。

(図表 1-1) ソフトウェア資産管理 (SAM) に関する文書

名称	発行改訂日
SAM ユーザーズガイドの概説	2010.6.16
JIS X 0164-1 から見た SAM ユーザーズガイド活用方法	2011.6.28
クラウド・コンピューティング時代の SAM の考え方	2011.6.28
SAM ユーザーズガイド - 導入のための基礎 -	2011.7.13

1.2. SAM と ISMS/ITSMS の連携

(1) 目的

前述のように、企業・組織のコンプライアンス及び IT 資産運用効率に直結する SAM への関心は確実に高まっている。加えて、近年 SAM は単にソフトウェア資産の管理対策としてだけでなく、他の IT 系マネジメントシステム (ISMS、ITSMS 等) を下支えするものであることも、次第に理解されてきているように思われる。

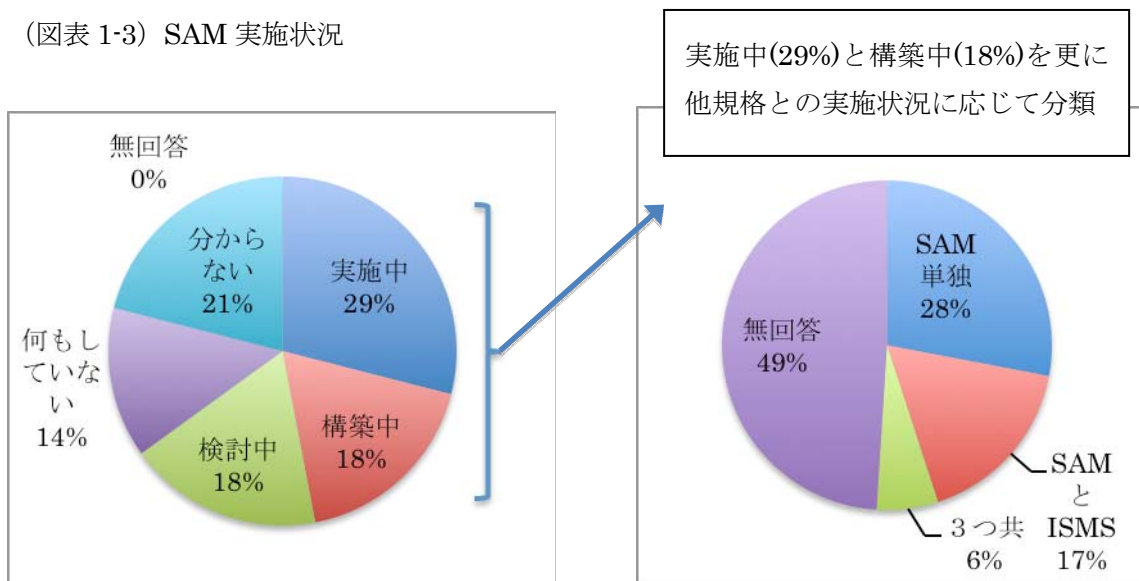
JIPDEC では、2009 年より全国で「ソフトウェア資産管理 (SAM) に関する説明会」を開催している。本説明会におけるアンケート調査では、企業・組織における SAM の実施状況と合わせて、ISMS と ITSMS の実施状況に関する質問を設定している。この質問に対する最近の回答状況は以下の通りである。

(図表 1-2) SAM の実施状況ならびに ISMS、ITSMS との関連

		2011/9/27	2011/10/31	2011/11/18	平均	
SAM実施状況	1.実施中	28%	19%	39%	29%	} 47%
	2.構築中	19%	26%	8%	18%	
	3.検討中	14%	23%	17%	18%	
	4.何もしていない	11%	13%	17%	14%	
	5.分からない	25%	19%	19%	21%	
	6.無回答	3%	0%	0%	1%	
	合計	100%	100%	100%	100%	
SAMとISMS、ITSMS、ITILの関連	1.ISMS取得済み	23%	19%	9%	17%	
	2.ITSMS取得済み	0%	0%	0%	0%	
	3.ISMS,ITSMS取得済み	9%	0%	9%	6%	
	4.ITIL導入済み	0%	0%	0%	0%	
	5.SAM単独導入	23%	43%	17%	28%	
	6.無回答	45%	38%	65%	49%	
	合計	100%	100%	100%	100%	

図表 1-2 に示した通り、2011 年度の開催実績 3 回の平均値では、SAM を実施中あるいは構築中の企業・組織は全体の 47% (29%+18%) を占めている。次に、SAM を実施中あるいは構築中の企業・組織の中で、他のマネジメントシステムとの併用状況については、ISMS の認証を取得した上で SAM を導入しているところが 17%。ISMS と ITSMS の認証を共に取得した上で SAM を導入しているところが 6%、SAM を単独導入しているところが 28%ある。尚、本アンケートでは ITSMS と SAM の組み合わせは 0%となっている。これは ITSMS 認証取得企業・組織には IT サービス会社のデータセンター、アウトソーシング部門が多く含まれており、一般的には ISMS を既に取得しているケースが多いためと思われる。以上の結果を図表 1-3 にまとめた。

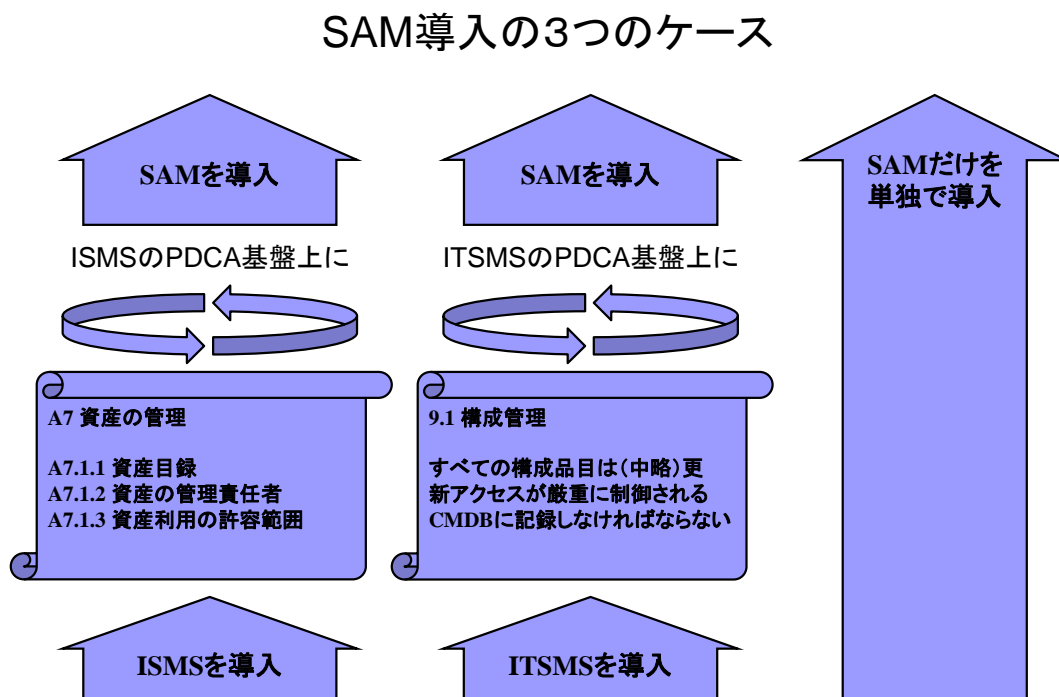
(図表 1-3) SAM 実施状況



上記アンケート結果を勘案すると、企業・組織が SAM を導入する際のパスとして、概ね 3 つのケースが考えられる。(図表 1-4)

- ① SAM を単独で導入する
- ② ISMS を導入し、資産管理プロセスを始めとする ISMS の PDCA 基盤を構築した上で、SAM 導入に進む
- ③ ITSMS を導入し、構成管理プロセスを構築した上で、SAM 導入に進む

(図表 1-4)



現時点では、上記アンケートからも伺えるように、SAM は単独で導入するケースが多いようである。しかし ISMS と ITSMS は既に IT サービス企業・組織にとっての必修科目となりつつある。従って、本稿において SAM、ISMS、ITSMS という 3 つのマネジメントシステムの共通性を明らかにすることができれば、例えば ISMS の資産管理プロセスを構築した上で SAM を導入する、あるいは ITSMS の構成管理プロセスを構築した上で SAM を導入する企業・組織が増加すると思われる。その結果、企業・組織は IT の総合的なマネジメントシステムを確立し、一層大きな効果を上げることが期待できる。

SAM と ISMS/ITSMS の連携に関する調査研究を行う目的は以上の通りである。

次に、具体的な検討方法について述べる。

(2) 検討方法

本稿では以下の方法で、SAM と ISMS/ITSMS の連携の可能性について検討を行った。
まず第2章では、SAM、ISMS、ITSMS の3つのマネジメントシステムについて、それぞれの定義、スコープ、規格条文等の比較を行い、共通点と相違点を洗い出した。

続く第3章では、SAM、ISMS、ITSMS の運用サイクルと管理メッシュの相違について検討した。既に ISMS と ITSMS の統合運用を試みている企業・組織はいくつか存在する。そこでこれらの先行事例をベースに、更に SAM を加えた、SAM、ISMS、ITSMS の統合運用の可能性について検討した。

第4章では、管理策の相互依存性について検討した。具体的には、ISMS の資産目録管理と、ITSMS の構成管理に着目し、これと SAM の IT 資産管理の共通点と相違点を洗い出した。その上で、ISMS の PDCA 基盤が確立していない場合に、SAM 導入にどのような影響（支障）があるのか、また ITSMS の PDCA 基盤が確立していない場合に、SAM 導入にどのような影響（支障）があるのか、逆に SAM が実施できていない場合に、ISMS/ITSMS の運用にどのような影響（支障）があるのか、などについて検討を加えた。各章の骨子を図表 1-5 にまとめた。

(図表 1-5) 第2章から第4章の骨子

章	項目名	概要
2	マネジメントシステムの比較検証	SAM、ISMS、ITSMS (QMS) のマネジメントプロセス比較表を作成する。
3	運用サイクルと管理メッシュ	SAM と ISMS/ITSMS の運用サイクルと管理メッシュを統合するために、統合運用マニュアル、統合運用年間スケジュール等を提案する。
4	管理策の相互依存性	SAM と ISMS/ITSMS の具体的な管理策を比較検討し、SAM を実施する上で ISMS/ITSMS の先行実施が SAM を実施する上でどのように役立つかを示す。

2. マネジメントシステムの比較検証

2.1. マネジメントシステムの統合の可能性

今日、サービスマネジメント (ITSMS : ISO 20000)、セキュリティマネジメント (ISMS : ISO27001)、ソフトウェア資産管理 (SAM : ISO 19770) など IT マネジメントシステムは、複数の国際標準が存在している。

それぞれの国際標準の内容を吟味すると、それぞれは緊密な連携や依存関係を示しており、完全に独立したマネジメントシステムを構築することを意図していないことがうかがえる。しかし、その一方で、完全に統合され、いずれかのマネジメントシステムが全てを包含すると明示されているわけでもない。

ここでは、各マネジメントシステムを検証し、これらマネジメントシステムの統合の可能性について考察する。

2.2. ソフトウェア資産管理とサービス管理

マネジメントシステムの統合を検討する場合、まずそれぞれのマネジメントシステムのあるべき姿を把握し、全体像を捉え、その共通項と違いを検証することが必要である。

ここでは、ソフトウェア資産管理 (SAM) とサービス管理 (ITSMS) を比較し、統合の可能性を検証する。

2.2.1. SAM、ITSMS の定義

(1) ソフトウェア資産管理の定義 :

「ソフトウェア資産管理とは、組織内のソフトウェア資産の有効な管理、制御及び保護のために、ライフサイクルの全層にわたって必要なインフラストラクチャ、プロセス及び組織としての取り組みをいう」 (ソフトウェア資産管理の基礎と実践 SAM の基礎と実践 編集委員会 編著より引用)

(2) サービス管理の定義 :

「サービスマネジメントとは、顧客に対し、サービスの形で価値を提供する組織の専門能力の集まりである。」 (サービスストラテジ ITIL TSO 出版より引用)

ソフトウェア資産管理については、その管理対象が「ソフトウェア資産」であり、ソフトウェア資産を所有する組織内あるいは、ソフトウェア資産を利用する組織までを対象に、有効な管理、制御及び保護を目的とし、ソフトウェア資産のライフサイクルの全層という範囲を明示し、必要なインフラストラクチャ、プロセス及び組織としての取り組みという具体的な内容までも定義に明示することができる。

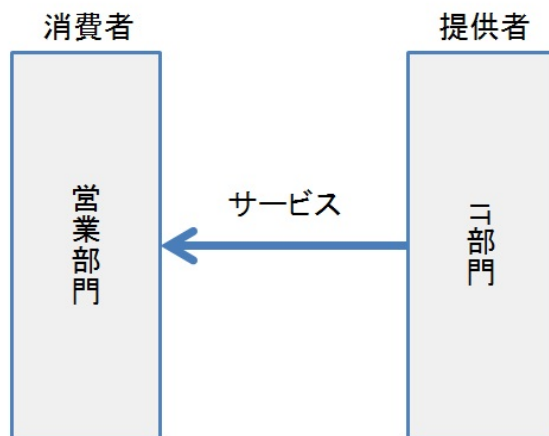
一方で、サービス管理は、サービス管理の定義を明確にするためには、サービスの定義を明確にし、顧客、組織の関係を理解しなければならない。

(3) サービスの定義：

「サービスとは、顧客が特定のコストやリスクを負わずに達成することを望む成果を促進することによって、顧客に価値を提供する手段である。」

サービス管理における顧客とは誰か？ 顧客が IT サービスのユーザーであると考えれば、顧客は「営業部門」のような IT サービスを消費する事業体であり、サービスプロバイダとは「IT 部門」のようにユーザーに IT サービスを提供する立場の部門ということになる。つまり、サービスマネジメントとは、サービス提供者が実施することを意図していると考えられる。

(図表 2-1) サービスの提供



それでは、ソフトウェア資産管理はどうだろうか？ソフトウェア資産管理においては、ソフトウェア資産の所有権が、たとえサービス提供者にあったとしても、ソフトウェアの実際の使用者が営業部門にいれば、営業部門においての使用者に対しての責任が発生する。この責任をも範囲として管理することが、ソフトウェア資産管理では求められる。

ステークホルダー（利害関係者）という観点からいえば、サービス管理においても、ソフトウェア資産管理においても営業部門のユーザーは、ステークホルダーの対象であるが、法的責任や、コンプライアンスの順守という観点からは、ソフトウェア資産管理において営業部門であるユーザーは当事者となる。この点において、サービス管理とソフトウェア

資産管理は異なる。

サービス管理の目的は、ユーザーである顧客が特定のコストやリスクを負わずに達成することを望む成果を提供することにある。しかし、ことソフトウェアの使用にいたっては、例えば、ソフトウェアアプリケーションをサービスとしてユーザーが使用していたとしても、そのリスクを全面的にサービス提供者に転嫁することは不可能なのである。それ故に、サービス管理を実施していたとしても、ソフトウェア資産管理は必要であると言える。

2.2.2. SAM、ITSMS のスコープ

前項では、ソフトウェア資産管理とサービス管理の定義から、その違いの検証を進めた。明らかになったのは、サービス管理において IT 部門は、サービスという製品の製造者であり、提供者であるということ。また、営業部門など事業体は IT サービスを消費する消費者ユーザーであるということ。この場合は、消費者ユーザーは、サービスを消費する一方で、リスクをサービス提供者に転嫁することを目的としていること。そして、ソフトウェア資産管理においては、例えば営業部門がソフトウェアを所有せずに、ソフトウェアアプリケーションサービスを利用していたとしても、ソフトウェアの使用においては、責任が発生することで、そのリスクを全面的にはサービス提供者に転嫁できないということが明らかになった。

もう少し、具体的な例でこれらの関係を考察してみたい。

例えば、サービスモデルの例として、「レンタカー」を考えると。

レンタカーは、レンタカーというサービスを提供する企業が所有する車を、必要な時に、必要なモデルを、必要な時間だけ利用する、サービスモデルである。この場合、利用者は、その利用に応じた料金を支払い、車を所有することに係る責任をサービス提供者に転嫁することができる。車検や保守メンテナンスなど法的義務を遂行する必要はサービスを提供する企業にあり、利用者に法的責任は発生しない。もちろん、サービスの契約内容にもよるが、一般的には利用する時間内に利用者が適当と思える範囲の保険サービスを別途、任意で、サービス提供者と締結し、利用条件に基づいてレンタカーを返却するだけである。利用者は、その目的に応じた車種を選択するという柔軟な選択肢が与えられる。近所でちょっとした送り迎えなら、軽自動車で十分だろうし、引っ越しならトラックを借りることもできる。ニーズに合わせて、そのサービスを選択することができるのだ。もちろん、サービス提供者は、自社以外にもレンタカー会社があるので、できるだけ顧客のニーズを捉え、顧客満足度の高いサービス提供をめざすだろう。

例えば、近所にレンタカー会社が 2 社あり、選択肢がある場合、明らかにサービス料金が高く、しかも、車はいつもドロドロに汚れ、あちこちぶつけた外部の損傷は放置されたまま、車内も臭く、汚れているという車を借りるよりも、サービス料金も抑えられ、車はいつもピカピカに洗車され、目立った損傷もなく、社内も掃除が行き届いていて、どことなく良い香りがする車を借りたいと思うのが、あたりまえだろう。

つまり、サービス管理が目的としているのは、そのような競争環境に置かれるサービス提供者が、どのようにサービスのニーズに応え、競争力を維持、向上していくかにある。

ソフトウェア資産管理においては、少し趣が異なる。それは、ソフトウェア自体の所有権がサービス提供者にはなく、あくまでソフトウェアメーカーが所有するソフトウェアの使用権を、ソフトウェアの利用者が、定められた契約に基づいて、その使用権限の範囲で使用するということが求められるからである。

したがって、ユーザーである営業部門は、どこまで行っても、当事者であることに変わりなく、ソフトウェアを使用するにあたり、自らが与えられた権利と法的責任を理解し、それらを行使し、遂行、遵守できる状態でなければならない。

良い例とはならないかもしれないが、例えば、ホリスティックアプローチを提唱する病院において「健康ケアサービス」のようなサービスが存在したとする。「あなたの健康維持、向上のための総合健康サービスです」という謳い文句で提供されるサービスであったとしても、最終的に健康を維持する努力は「自己管理」を含むので、健康ケアサービスで提供されたアドバイスなどを参考に、自己管理に励む必要がある。つまり、ソフトウェア資産管理サービスをアウトソースしたとしても、サービスの消費者であるユーザーがソフトウェアを使用するのであれば、すべての責任やリスクをアウトソーサーであるサービス提供者に転嫁することはできない、ということである。常に、「自己管理」は、求められるのである。

ソフトウェア資産管理とサービス管理のスキームの大きな違いは、この部分にあると言える。サービスの消費者であるユーザー顧客は、サービス管理において提供されるサービスの消費者の立場では、できるだけリスクや責任をサービス提供者に負わせて、自己負担を減らすことに意味がある。もちろんサービスニーズの相互理解などにおいては、ステークホルダーとしてユーザー顧客も参加するのだが、あくまでサービスマーケティングにおける顧客満足度向上のための活動である。責任やリスクはサービス提供者にある。しかし、ソフトウェア資産管理では、ユーザー顧客にも常に責任とリスクが発生しているので、これらを排除することができない。そして、それを継続的に教育し、リスク低減や状態維持を行っていく必要がある。

2.2.3. SAM、ITSMS の共通項

さて、ソフトウェア資産管理とサービス管理においては、視点の違いから完全な統合が困難であることはわかった。それが組織（IT 部門やユーザー事業体）がおかれる立場の違いに起因することも明らかになった。

それでは、どのような共通項をもって統合の可能性を見出すべきなのだろうか？

サービス管理の定義などから、サービスモデルにおいては、ユーザーは特定のコストやリスクを負わずに成果を求め、サービス提供者はそれに応えるサービスの製造と提供を行うことが理解できる。

今まではユーザー部門が所有する IT 資産に対して、技術力というサービスを提供してきた IT 部門は、インフラストラクチャの構築、サーバーアプリケーションの開発、PC プラットフォームの提供、それらの運用管理という技術サービスを中心に、その活動を行ってきた。しかし、サービスモデルでは、基本的な所有はリスク転嫁の目的からサービス提供者の責任となり、サービスの消費者であるユーザーは、あくまでサービスに対しての対価を支払い、できる限りの固定的なコストやリスクを負わないことを期待する。

実際には、そう簡単に今までのモデルからサービスモデルへの転換や変革はスムーズに行われないので、所有権が誰にあるのかを明確に管理し、サービスの具体的な内容と所有権を紐付ながらサービス料金を構成する資産なども管理される必要がある。

しかし、ここではケーススタディとして、サービスモデルに移行した場合のソフトウェア資産管理とサービス管理の統合について考察したいと思う。

例えばある組織（一企業または一事業組織）のユーザー事業体（営業部門）が、今までは PC やサーバーなどハードウェア機器、および PC アプリケーションや、サーバーアプリケーションなどを所有して、その環境構築や運用管理を IT 部門に委託していたとする。IT 部門は、環境構築、運用管理などを実施する技術力をサービスとしてユーザー事業体へと提供していた。

しかし、サーバーの乱立による ROI の低下から、統合が進み、サーバー資源などがプールされ、仮想化され、サーバー資源を複数部門のユーザー事業体において共有する、あるいは、IT 部門の所有資産としてサービス化が進んでいった。

さらに、この組織が、サービスモデルへと変革し、PC アプリケーションを含めるソフトウェアの所有を IT 部門において行い、ユーザー事業体へはアプリケーションサービスとして提供することとなった。

この時点で、ユーザー事業体は IT 資産の所有をしていない。所有に係るリスクをサービス提供者へ転嫁した。

サービス提供者は、ISO 20000、ITIL に則ってサービス管理の実行を行おうとしている。さて、この段階でサービス提供者である IT 部門は、どこまでサービス管理とソフトウェア管理のプロセスを統合することが可能なのだろうか？

2.2.4. ISO 19770-1 と ITIL V3 の比較

ISO 20000 シリーズは歴史的に ITIL をもとに作成された経緯があり、随所に ITIL の影響を認めることができる。プロセスの切り方については若干の差異もあるが、本質的には

ITIL と類似性が高いと考えてよい。また、ISO 19770-1 は、そもそも ISO 20000 との整合を標榜しており、緊密な連携が行われている。それでは、どれほどの類似性あるいは、関連性が認められるのか、実際のプロセスを比較してみる。

ISO 19770-1 と、サービス管理のベストプラクティスで参照されている ITIL のプロセスを比較してみた。ISO 19770-1 の項目への対応は、実際は複数のプロセスをまたがって考慮する必要があり、ITIL V3 においても項目によっては複数のライフサイクル プロセスにおいて考慮する必要が認められる。

具体的に比較してみると、ソフトウェア資産管理はその多くのプロセスにサービス管理との共通性が認められる。従って、サービス管理プロセスの成熟度が高い組織において、ソフトウェアの視点での考慮が盛り込まれており、サービス管理のスコープにサーバーから PC まで、ユーザーへ提供するサービスを構成するすべての資産が構成アイテムとして管理されていれば、すでにソフトウェア資産管理標準が求めるプロセスの多くは実装されているはずである。

サービス管理におけるサービス資産および構成管理、アプリケーション管理、イベント管理、インシデント管理、問題管理、変更管理、知識管理、リリースおよび展開管理、サービスデスク、要求実現などがソフトウェア資産を考慮して実装されていれば、すでに大多数のソフトウェア資産管理プロセスは実装されているべきである。

それでは、サービス管理においてソフトウェア資産管理の標準で要求されるすべてのプロセスが包含されているのだろうかという点、残念ながらすべてが包含されている訳ではない。本来であればインシデント（事件・事故）管理プロセスなどは簡単に統合できそうに思えるが、イベント管理自体がソフトウェア資産管理で独立したシステムとなっている場合が多いため、ソフトウェア資産管理のイベント管理とインシデント管理のつながりがなく、ソフトウェア資産管理のインシデント管理と、サービス管理のインシデント管理の統合が困難となっている。

さらに、通常インシデント管理はサービスデスクの範疇であり、できるかぎり対応はサービスデスクにより実施され、エスカレーションは、ある基準をもって行い、問題管理などの対応から技術チームへのパスが導かれるが、ソフトウェア資産管理においてサービスデスクとの連携がとられていない場合は、ほぼすべての対応においてソフトウェア資産管理チームが対応することとなる。サービスデスクとのインシデント管理における対応の統合や、インシデント管理のシステムの共有化などの検討も必要となる。

しかしこの課題を乗り越えようと、一気に問題管理、変更管理のシステムの共有と統合が見えてくる。重要なのは、サービス管理のマネジメントシステムのチームが、ソフトウェア資産管理の要件もサービス管理のスコープ内であることを認識することと、ソフトウェア資産管理のスコープがサービス管理のスコープに完全に一致しないことを理解し、ソフト

ウェア資産管理チームとの折り合いをつけることである。

2.2.5. ISO 19770-1 における「組織」、「顧客」の表現に注意する

標準の要件を精査した結果、大多数（およそ 80%程度）はサービス管理のスコープに入りそうであることがわかった。もちろんそれは、アプリケーションソフトウェアが、アプリケーションサービスとしてサービス管理におけるサービスカタログに記載されるサービス化されているという前提ではある。

それでは、残りの 20%とは、何があるのだろうか？

ISO 19770-1 を読むと、そこには「組織」という表現と、「顧客」という表現が出現しているのがうかがえる。これこそが、サービス管理との違いを表している部分である。つまり、アプリケーションサービスというサービスは、サービス提供者である IT 部門が、顧客であるユーザー事業体（営業部門など）へサービスとして提供している場合、ユーザー事業体は「顧客」という立場になる。

しかし、それ以外の場合、例えば「4.5.3 ソフトウェア使用許諾条件の順守」などでは、「その組織以外が所有しているが組織で使用するソフトウェア及び関連資産に関係するすべての知的財産について、組織が、適正に使用許諾を受け、・・・」と表記されている。この場合、ユーザー事業体である営業部門は、組織または組織の一部にあたるので（資産の所有権が営業部門にはなく、他の部門または外部の組織にある場合）、当事者である。

したがって、マネジメントシステムにおける当事者として ISO 19770-1 での登場人物を考えると、ソフトウェア資産管理チーム、サービス管理チーム、ユーザー事業体の 3 者に対して、同標準が提示されていると考えることができる。

2.2.6. SAM と ISMS の類似点

SAM と ISMS は、登場人物という点で類似している。なぜなら、どちらもサービス管理チームだけでは完結しないし、ソフトウェア資産管理チームだけ、あるいは情報セキュリティ管理チームだけでも完結しない、さらに、ユーザー事業体が当事者として登場する。この点から、SAM と ISMS の類似点をよく検証し、学べることが多いと考えられる。

ユーザー事業体における体制構築などは、特に酷似するので、ISMS 対応の体制がすでに構築されている場合、この体制をソフトウェア資産管理にも生かすことができる。

いずれにせよ、組織においての IT の全体戦略がサービスモデルへの移行である場合、サービス管理チームは、SAM と ISMS を考慮したサービス管理プロセスを構築する必要がある。SAM チーム、ISMS チームは、ITSMS チームのスコープ外の活動を、ITSMS チームのスコープにおいて共通する部分は ITSMS のマネジメントシステムとの統合を相互協力のもと検討を進め、スコープ外の活動が完全に独立したマネジメントシステムを構築してしまうことがないように ITSMS チームとのコミュニケーションを図り、ITSMS チーム

ムも SAM、ISMS チームの両チームとの連携をより強化し、要求に応えられるような成熟度を目標としてサービス管理戦略を策定する必要がある。

2.3. 統合運用

2.3.1. 統合運用について

本稿では、組織が SAM、ITSMS、ISMS のマネジメントシステムを構築する場合の、統合運用について検討してゆく。

まずは、各 SAM、ITSMS、ISMS のコンセプトを確認しておく。

(1) SAM :

SAM は組織内のソフトウェア資産の有効な管理、制御及び保護を目的としている。IT サービスマネジメントのデファクトスタンダードとして知られる ITIL® では、資産を管理するプロセスとして IT 資産管理を備えている。IT 資産管理は、ITIL V2 および V3 においてプロセスとして存在しているが、SAM は明確な形で扱われていない。

SAM は、ITIL V2 の 7 冊の中核書籍に対する補完書籍という位置付けで、単独の書籍として存在していた。ITIL の SAM 書籍では、ソフトウェア資産管理を次のように定義している。

SAM の定義

SAM (ソフトウェア資産管理) は、組織内のソフトウェア資産のライフサイクル全ステージを通じて、効果的な管理、制御、および保護のために必要なインフラストラクチャとプロセスの全てである。

出典 : ITIL 書籍 『Software Asset Management』 TSO 刊を基に作成

定義における、“管理、制御、および保護”の意味するところは、ソフトウェア資産の持っている特徴を良く表現している。すなわち、ソフトウェア資産を管理する上での重要なテーマの一つであるライセンス管理を想起させる。ライセンス管理を実践することはコンプライアンス(法令遵守)につながることから、ソフトウェア資産をライフサイクルにわたり“管理、制御、および保護”することは必須である。

ITIL V2 のコア書籍においては、IT サービスを顧客/利用者に提供するために必要なプロセス群のベストプラクティス为中心であり、ソフトウェア資産をライフサイクルを通じて“管理、制御、および保護”するためのプロセス群は扱われていない。SAM の定義では、必要なインフラストラクチャも含まれるので、SAM はソフトウェア資産に係るハードウェアとソフトウェア (ライセンスを含んだ) を扱うプロセス群のすべてを指していることになる。規格では SAM のプロセス群を次のように 3 つの領域に分類している。(図表 2-2 参照)

- a) SAM の組織管理プロセス
- b) 中核 SAM プロセス
- c) SAM の主プロセスインタフェース

(図表 2-2) SAM プロセスの枠組み

SAMの組織管理プロセス			
4.2 SAMの統制環境			
SAMの企業統治プロセス	SAMの役割及び責任	SAMの方針、プロセス及び手順	SAMにおける能力
4.3 SAMの計画立案及び導入プロセス			
SAMの計画立案	SAMの導入	SAMの監視及びレビュー	SAMの継続的改善
中核 SAM プロセス			
4.4 SAMの在庫プロセス			
ソフトウェア資産の識別	ソフトウェア資産の在庫管理	ソフトウェア資産の管理	
4.5 SAMの検証及び順守プロセス			
ソフトウェア資産記録の 検証	ソフトウェア使用許諾条件 の順守	ソフトウェア資産セキュリティ の順守	SAMの適合性検証
4.6 SAMの運用管理プロセス及びインタフェース			
SAMの関係及び契約管理	SAMの財務管理	SAMのサービスレベル管理	SAMのセキュリティ管理
SAMの主プロセスインタフェース			
4.7 SAMのライフサイクルプロセスインタフェース			
変更管理プロセス	ソフトウェア開発プロセス	ソフトウェア展開プロセス	問題管理プロセス
取得プロセス	ソフトウェアリリース管理プロセス	事件・事故管理プロセス	廃棄プロセス

(出典：JIS X 0164-1 ソフトウェア資産管理：2010)

(2) ISMS :

ISMSは情報資産(Information Assets)を保護するためにISMSを確立、導入、運用、監視、レビュー、改善するモデルを提供する。情報資産とは、組織内に存在している資産であり、どのような形で存在しているものでもかまわないが、組織が利用している資産を示す。ITSMSの環境では、情報資産は、ITサービスにより利用されるか、一部となりうるだろう。ISMSへの適合を実現するためには、組織はリスクアセスメントプロセスに基づきISMSを実装しなければならない。ISMSでは情報資産へのリスクへ対策として管理策が用意されている。

(3) ITSMS :

サービスマネジメントは、顧客と合意したサービスの要求事項を実現するサービスを計画、開発、移行、提供するサービス提供者の活動とリソースを管理し、制御するのに必要とされる、プロセス群を含んだ、一連の能力である。

規格の要求事項を実現するためには、サービス提供者は広範にわたる特有のプロセス群を実装しなければならない。ITSMS 規格にはインシデント管理、変更管理、問題管理などが含まれなければならない。情報セキュリティ管理はサービスマネジメントプロセスの一つとして捉えられている。

2.3.2. マネジメントシステム

マネジメントシステムとしての SAM、ITSMS、ISMS を見た場合、マネジメントサイクル(PDCA)の確立に関しては、多少の表現の違いこそあれ、同じと考える事が出来る。各規格の PDCA に相当する部分を抜き出したものが図表 2-3 である。

(図表 2-3) 各規格の PDCA

規格名	情報セキュリティ マネジメントシステム ISO/IEC 27001:2005 (JIS Q 27001:2006 を基に作成)	IT サービスマネジメント システム ISO/IEC 20000-1:2011 (ISO/IEC20000-1:2011 英和対訳版を基に作成)	ソフトウェア資産管理 ISO/IEC 19770-1 (JIS X 0164-1:2010 を基に作成)
適用範囲	1 適用範囲	1 適用範囲	1 適用範囲
用語定義	3 用語及び定義	3 用語及び定義	3 用語及び定義
一般要求事項	4.1 一般要求事項	4 サービスマネジメント システムの一般要求事項	4. SAM プロセス
経営陣の責任	5 経営陣の責任	4.1 経営者の責任	4.2.2 SAM の企業統治プロセス
文書管理	4.3 文書化に関する要 求事項	4.3 文書の運用管理	4.2.5 SAM の能力 (4.2.5.2.a)
教育訓練	5.2.2 教育・訓練、意識 向上及び力量	4.4.2 人的資源	4.2.5 SAM の能力 (4.2.5.2.c)
Plan	4.2.1 ISMS の確立	4.5.2 SMS の計画	4.3.2 SAM の計画立案
Do	4.2.2 ISMS の導入及び 運用	4.5.3 SM の導入及び運用	4.3.3 SAM の導入
Check	4.2.3 ISMS の監視及び レビュー (6. ISMS 内部監査)	4.5.4 SMS の監視及びレビュー	4.3.4 SAM の監視及びレビュー
Act	4.2.4 ISMS の維持及び 改善 (7. ISMS のマネジメ ントレビュー)	4.5.5 SMS の維持及び改善	4.3.5 SAM の継続的改善

	(8 ISMS の改善)		
--	--------------	--	--

各規格の特徴(差異)を考えるには、規格の対象範囲(スコープ)を比較してみると理解しやすいだろう。ITSMS のスコープは、サービス提供者が提供している IT サービスのマネジメントである。ISMS は組織の情報資産を保護するための情報セキュリティシステム、SAM は組織におけるソフトウェア資産を対象としている。各規格ではマネジメントシステムを構築し、それぞれの規格の要求事項を満たすプロセス群を構築することを要求される。それぞれの規格におけるスコープの詳細を次にあげておく。

(1) ISMS :

この規格は、あらゆる形態の組織（例えば、営利企業、政府機関、非営利団体）を対象にする。この規格は、その組織の事業リスク全般に対する考慮のもとで、文書化した ISMS (Information security management system) を確立、導入、運用、監視、レビュー、維持及び改善するための要求事項について規定する。この規格は、それぞれの組織又はその組織の一部が、そのニーズに応じて調整したセキュリティ管理策を導入する際の要求事項について規定する。

(2) ITSMS :

この規格は、サービスマネジメントシステム (SMS)の規格である。この規格は、SMS を計画、確立、導入、運用、監視、レビュー、維持及び改善するための、サービス提供者に対する要求事項を規定する。

(3) SAM :

この規格は、ソフトウェア資産管理 (software asset management, SAM) のための統合された一連のプロセスの基準を定める。

2.3.3. SAM と ITSMS の関係

JIS X 0164-1 の序文において、規格の意図が次のように表現されている。

この規格は、JIS Q 20000 規格群と緊密な整合をとり、また、それを支援するように意図されている。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

JIS Q 20000 規格群は ITSMS(IT サービスマネジメントシステム)の国際規格である。読みかえれば、SAM と ITSMS は緊密に整合されていて、SAM は ITSMS を支援するように意図されていることになる。緊密に整合というからには、SAM と ITSMS の中で定義

されているプロセスには、矛盾なく、同一の機能を提供するものが存在していると考えて
良いだろう。規格の箇条 4.1.1 において、次のように上記の序文を補足している。

4.1.1 定義及びサービスマネジメントとの関係

ソフトウェア資産管理とは、組織内のソフトウェア資産の有効な管理、制御及び保護をいう。
この規格が定義する **SAM** のプロセスは、**JIS Q 20000** 規格群が定義している情報技術 (IT)
サービスマネジメントとよく両立するように構成されており、それを適切に支援することを意
図している。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

注：下線部は筆者による

SAM のプロセス群は、JIS Q 20000 規格が定義している IT サービスマネジメントのプロ
セス群とよく両立するように構成されていることになる。

とりわけ、下記の箇条 4.7 の 4.7.1 一般において、SAM 規格の中で定義されている SAM
のライフサイクルプロセスインタフェースは、明示的に JIS Q 20000 のプロセスと整合が
取られているとしている。

4.7 SAM のライフサイクルプロセスインタフェース

4.7.1 一般

“SAM のライフサイクルプロセスインタフェース”は、SAM との関連では、**JIS X 0160** での
主ライフサイクルプロセス及び**JIS Q 20000** 規格群のプロセスとほぼ整合がとられている。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

注：下線部は筆者による

SAM 規格でのライフサイクルプロセスとは、次のプロセス群である。

- a) 変更管理プロセス
- b) 取得プロセス
- c) ソフトウェア開発プロセス
- d) ソフトウェアリリース管理プロセス
- e) ソフトウェア展開プロセス
- f) 事件・事故管理プロセス
- g) 問題管理プロセス
- h) 廃棄プロセス

変更管理、リリース管理、展開、問題管理などのプロセスと JIS Q 20000 で定義される

ITSMSにおける同名のプロセス群が緊密に整合する関係であることは容易に想像できる。

SAM規格はAsset(資産)を扱うことから、ITサービスマネジメントのプロセスの中で最も関連が深いプロセスは構成管理であることは明白だが、SAM規格では構成管理との関係について、次のように述べている。

“SAMの在庫プロセス”は、SAMの基本であるだけでなく、すべての構成管理の基本である。すべてのIT資産(ソフトウェア及び関連資産だけではない。)及びこれらの資産すべての間の関係を対象にする限りにおいて、更に非IT資産も含んでよいことから、構成管理は、SAMの適用される範囲を超える。ITサービスマネジメントのすべてを含むプロジェクトでは、“SAMの在庫管理プロセス”が構成管理の一部とみなされることもある。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

注：下線部は筆者による

構成管理の適用範囲は“SAM 在庫プロセス”における適用範囲を包含することを述べている。“SAMの在庫プロセス”とは、次のプロセスで構成されている。

- a) ソフトウェア資産の識別
- b) ソフトウェア資産の在庫管理
- c) ソフトウェア資産の管理

つまり、適切に構築されたITSMSの構成管理が適応される範囲はSAMの構成管理の適用範囲を含む事を可能としているのである。

2.3.4. CI(構成要素)とAsset(資産)の関係

ITSMSに於いては、構成管理の対象範囲はCIである。ISMSでは情報資産をSAMではソフトウェア資産を管理・制御の対象としている。マネジメントシステムの統合運用を進めるには、CIと情報資産およびソフトウェア資産の関係を理解しておくことが重要であろう。ここでは、CI、情報資産、ソフトウェア資産の関係を述べる。

ITSMSにおけるCIの定義は、次のようになっている。

3.3 構成品目

CI

サービスの提供のために管理する必要がある要素

出典：ISO/IEC 20000-1：2011 英和対訳版

ISMSは、情報資産を保護し、セキュリティにおける管理策を立てることを目的とするが、情報資産は次のように定義されている。

2.18

情報資産

組織にとって価値をもつ知識あるいはデータ

出典：ISO/IEC 27000：2009 を基に作成

また、ISMS では資産(Asset)を次のように定義している。

2.3

資産

組織にとって価値をもつもの

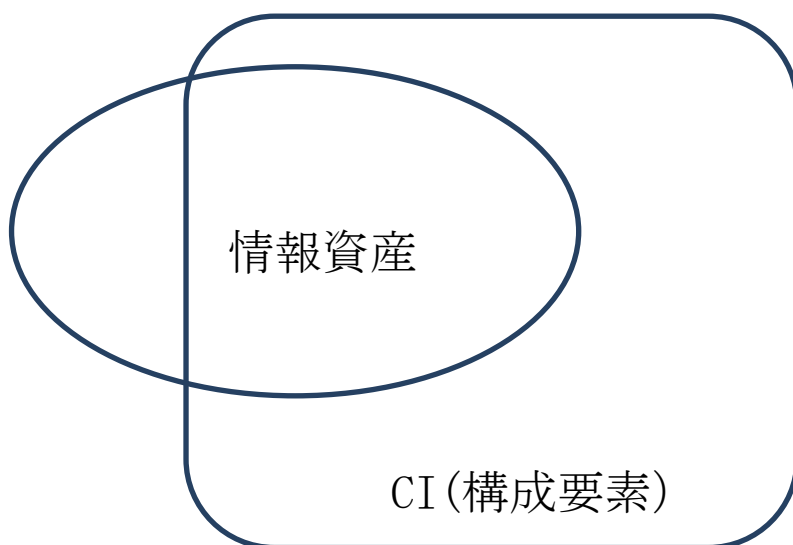
出典：JIS Q 27001：2006

資産としての具体例として、ISO/IEC 27002 において次のように例示されている。

- a) 情報：データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査情報、利用者マニュアル、訓練資料、運用手順又はサポート手順、事業継続計画、代替手段の取決め、監査証拠、保存情報
- b) ソフトウェア資産：業務用ソフトウェア、システムソフトウェア、開発用ツール、ユーティリティソフトウェア
- c) 物理的資産：コンピュータ装置、通信装置、取外し可能な媒体、その他の装置
- d) サービス：計算処理サービス、通信サービス、一般ユーティリティ（例えば、暖房、照明、電源、空調）
- e) 人、保有する資格・技能・経験
- f) 無形資産（例えば、組織の評判・イメージ）

上記のように概観すると、CI は情報資産を含んでいるが、逆は必ずしも成り立たないことが理解できる。情報資産の全てがサービスの提供に必要な CI として定義されるとは限らないからである。例えば、データケーブルを考えた場合、CI の候補にはなりうるが、ISMS の対象とする情報資産にはならないことが理解できる。

ITSMS の CI と ISMS の情報資産の関係を図示すれば、次のようになるであろう。



SAM においては、ソフトウェア資産という用語は定義されていない。SAM は、ソフトウェアの性質に関係なく、すべてのソフトウェア及び関連資産に適用できるとしている。例えば、実行可能なソフトウェアとしてアプリケーションプログラム、オペレーティングシステム、ユーティリティプログラムなどを挙げている。また、非実行可能ソフトウェアとして、フォント、グラフィック、音声、映像、テンプレート、辞書、文書、データなどが挙げられている。SAM におけるソフトウェア資産の適用範囲の定義（この規格適用の範囲に入るソフトウェアの種類）は、“SAM の計画立案”プロセスで開発される SAM 計画の一部として文書化するとしている。

こうして比較してみると、“資産”というものに“情報”、“ソフトウェア”という冠をつけて、それぞれの規格に応じて、資産の範疇を決めたものが ISMS の情報資産であり、SAM におけるソフトウェア資産なのだろう。

規格では CI、情報資産、ソフトウェア資産のいずれにおいても、プロセスが管理してゆく対象として明確にリストアップすることを要求していない。それぞれの規格において、規格に適合した形で、組織が一貫性を持って、設計、構成が可能なのである。

SAM、ITSMS、ISMS 規格における CI と Asset の用語の定義を図表 2-4 に示す。

(図表 2-4) CI と Asset の用語定義

項目	SAM	ITSMS	ISMS
CI (Configuration Item:構成要素)	ハードウェア若しくはその集合体, ソフトウェア若しくはその集合体, 又はこれらの集合体で, 単体として	サービス提供のために管理する必要がある要素	—

	<p>管理するように設計されたもの。</p> <p>注記 構成品目は、複雑さ、規模及び種類の点で多様であり、すべてのハードウェア、ソフトウェア、及び文書を含んだシステム全体から、単独のモジュール又は小規模なハードウェアコンポーネントにまで及ぶ。</p>		
資産 Asset	—	—	<p>組織にとって価値をもつもの。多くの資産のタイプがあり、次を含む</p> <p>a)情報</p> <p>b)ソフトウェア、例えば、コンピュータプログラム</p> <p>c)物理的、例えばコンピュータ</p> <p>d)サービス</p> <p>e)人、その資格、スキル、経験</p> <p>f)不可視なもの、評判とかイメージ</p>
ソフトウェア資産 (Software Asset)	—	—	—
情報資産 (Information Asset)	—	—	<p>組織にとって価値のある知識あるいはデータ</p>

SAM は JIS X 0164-1 : 2010 を参照

ITSMS は ISO/IEC 20000-1 : 2011 を基に作成

ISMS は ISO/IEC 27000 : 2009 を基に作成

ITIL は ITIL V3 用語集 2011 版

2.3.5. 統合運用に向けて

マネジメントシステムという大きな PDCA の枠組みは共通だが、SAM,ITSMS,ISMS には、プロセスで管理、制御してゆく対象が異なる。前述のように、各規格においては、プロセスで管理・制御すべき対象が CI、ソフトウェア資産、情報資産である。どの規格においても、管理の対象とすべきモノをリストアップすることは要求していない。統合運用をすすめてゆく場合には、統合作業において、それぞれの規格に適合した資産(あるいは CI)を、曖昧な形で統合してゆくのではなく、各規格に分類、判別出来るようにするべきである。これらの規格の統合運用を検討する前に、組織が取りうる状態を仮定してみると、次のように分類できるだろう。

- ・ どのマネジメントシステムも構築していない
- ・ どれか一つのマネジメントシステムを構築している
- ・ マネジメントシステムの事務局組織が異なる等の理由により統合運用されていない。

組織が複数のマネジメントシステムの統合運用を考える場合に考慮すべき点は以下の通り。

- ・ 他のマネジメントシステムが利用されているか
- ・ 統合マネジメントシステムの環境での全てのサービスとプロセスの相互関係
- ・ それぞれの規格の要素でマージが可能か、そして、どのようにマージ出来るか
- ・ 分離のままにしておく要素
- ・ 顧客、提供者、他の関係者への統合マネジメントシステムの影響
- ・ 利用している技術への影響
- ・ サービスとサービスマネジメントへの影響あるいはリスク
- ・ 情報セキュリティと情報セキュリティマネジメントへの影響あるいはリスク
- ・ ソフトウェア資産とソフトウェア資産管理への影響あるいはリスク
- ・ 統合マネジメントシステムの教育とトレーニング
- ・ 導入活動の移行段階と順序

統合運用の最初のステップは、マネジメントシステムの統合をし、次いで、管理、制御の対象となる要素を整理することが理に叶っている。プロセスの統合運用に関しては、各プロセスの役割と責任から統合し、次いで機能統合の検討に入るのが良策と考える。

複数の規格を統合運用したいからといっても、各規格の対象を統合しても意味がないことは明らかであろう。複数の規格を統合運用することの目的は、規格の比較をして、どちらが良いとか、正しいという議論をすることではなく、規格への遵守は保ちながら、組織にとって価値のある統合マネジメントシステムを目指すことである。

3. SAM と ISMS/ITSMS の運用サイクルと管理メッシュ

3.1. 企業・組織における ISMS/ITSMS 活動実態

企業・組織における ISMS/ITSMS は、第三者認証制度に基づく活動をベースとしている。これらの認証規格では、内部監査や見直し・レビュー活動を「あらかじめ定められた間隔で」実施することを要求しており、多くの企業・組織が年1回という頻度の運用サイクルを採用している。

ある企業・組織における ISMS、ITSMS、SAM の管理日程を以下に示す。

(図表 3-1)

統合運用 年間スケジュール表

実施事項	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
1. 文書管理												
①関連規程の管理/見直し										←→		
②関連様式の管理/見直し										←→		
2. 教育関連												
①年間教育計画の作成	←→											
②教育テキストの準備			←→									
③教育実施				←→								
④教育実施記録取りまとめ					←→							
⑤教育実施結果の評価						←→						
3. 監査関連												
①年間監査計画の作成	←→											
②監査通知(監査部門→被監査部門)							←→					
③監査実施(適合性評価・運用状況チェック)								←→				
④監査記録(監査報告書、監査チェックリスト)									←→			
⑤監査指摘事項の是正及び予防処置の実施										←→		
4. 資産管理台帳見直し												
①管理台帳の更新状況の確認						←→						
②リスク分析の見直し							←→					
5. 委託先の管理												
①委託先選定基準の見直し		←→										
②委託先の定期的審査(委託先審査票)		←→										
③委託内容の確認			←→									
④新規委託先との覚書締結				←→								
6. SAM, ISMS, ITSMSの定期的運用点検												
①各部門別運用チェックリストによる点検の実施							←→					
②運用点検後の是正処置の実施								←→				
7. 関連法令・規範内容の確認										←→		
8. 情報システム基盤の管理・点検											←→	
9. 外部からの苦情等の受付状況把握												←→
10. セキュリティ事件・事故状況の有無確認												←→
11. 入退管理状況(入退受付表、入退室管理等)												←→
12. マネジメントレビュー										←→		

管理メッシュについては、規格の違いよりも組織の管理体制に依存するところが大きく、成熟度の高い組織がマネジメントシステムを構築すれば、SAM、ISMS/ITSMS の管理メッシュも自ずと整合されていく可能性が高い。但し現状では ITSMS の管理対象は主として IT サービス提供基盤であるデータセンター及びサーバー群に偏向することが多く、一方 SAM の管理対象は主としてエンドユーザのリテラシーに左右される PC 周りのソフトウェアライセンス管理に偏向することが多いのもまた事実である。

今後、企業・組織にとって SAM の位置づけが上がれば、ISMS/ITSMS の基盤の上に SAM を構築する事例が増加し、3つの規格の統合運用が進展するものと考えられる。

4. マネジメントシステムの管理策の相互依存性

4.1. ISMS「資産目録」に関する管理実態

JIS Q 27001:2006 附属書 A「管理目的及び管理策」の「A7.1.1 資産目録」（以下「ISMS 附属書 A7.1.1 資産目録」と略す）に関する管理策では、「すべての資産は、明確に識別しなければならない。また、重要な資産すべての目録を作成し、維持しなければならない」と規定されており、ISMS の管理策では、「SAM ができている」という前提である。そこで、ISMS 認証取得企業における「ISMS 附属書 A7.1.1 資産目録」の管理実態について紹介したい。

ISMS においては、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）に対して、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システムの実践のための規範）が発行されている。JIS Q 27002:2006 では、具体的な取り組みが紹介されており、本稿の目的にも適うと考え、JIS Q 27002:2006 を例として採用した。

JIS Q 27002:2006 では、組織の ISMS 適用範囲における資産の保有状況を確認するために資産目録を作成することを、「7.1.1 資産目録」で推奨している。

実施の手引（JIS Q 27002:2006 7.1.1 資産目録より引用）

組織は、すべての資産を識別し、それら資産の重要度を記録することが望ましい。資産目録には、資産の種類、形式、バックアップ情報、ライセンス情報及び業務上の価値を含め、災害から復旧するために必要なすべての情報を記載することが望ましい。目録は、他の目録と不必要に重複しないことが望ましく、その記載内容が他の目録と整合していることを確実にしていることが望ましい。

さらに、各々の資産の管理責任者(7.1.2 参照)及び情報の分類(7.2 参照)について合意し文書化することが望ましい。資産の重要度に応じた保護のレベルは、資産の重要度、業務上の価値及びセキュリティ上の分類に基づいて決めることが望ましい。(資産の重要度を表すための評価手法については、TR X 0036-3 参照)。

資産の洗い出しの結果、資産目録の望ましい例として、下記のような項目が記載されている。

- ・資産の管理責任者（資産の所有者、管理者名）
- ・資産の形態
- ・保管形態
- ・保管場所

- ・ 保管期間
- ・ 廃棄方法
- ・ 用途
- ・ 利用者の範囲（+業務プロセス）
- ・ 他のプロセスとの依存性

また、JIS Q 27002:2006 の「7.1.1 資産目録」には、資産の例示がされている。

(図表 4-1) 資産の例示

資産の種類	例示
情報	データベース及びデータファイル, 契約書及び同意書, システムに関する文書, 調査情報, 利用者マニュアル, 訓練資料, 運用手順又はサポート手順, 事業継続計画, 代替手段の取決め, 監査証跡, 保存情報
ソフトウェア資産	業務用ソフトウェア, システムソフトウェア, 開発用ツール, ユーティリティソフトウェア
物理的資産	コンピュータ装置, 通信装置, 取外し可能な媒体, その他の装置
サービス	計算処理サービス, 通信サービス, 一般ユーティリティ (例えば, 暖房, 照明, 電源, 空調)
人	保有する資格・技能・経験
無形資産	例えば, 組織の評判・イメージ

ISMS における資産の洗い出しを行う目的は、ISMS の適用対象全体で適切なセキュリティ対策を決定することにある。従って、組織のすべての資産を網羅し、個々の資産の属性を明記した詳細な管理台帳を作成することが必ずしも重要ではない。

一方、SAM では、コンプライアンス上の要求事項を満たすという目的のために、SAM ユーザーズガイド「6. SAM の構築」で説明されている通り、対象資産の属性に応じて、下記の4つの管理台帳を作成することが望ましい。

- (1) ハードウェア
- (2) 導入ソフトウェア
- (3) ライセンス
- (4) ライセンス関連部材

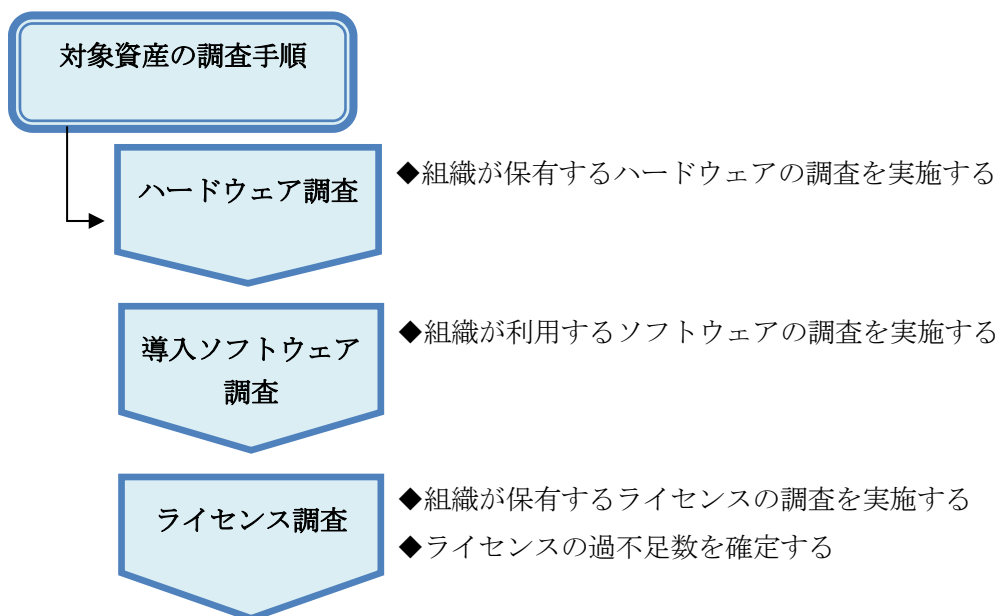
(図表 4-2) SAM における対象資産と管理目的

資産名	主な対象資産	管理目的
ハードウェア	・ ソフトウェアが実行できる機器 例：PC・サーバー・PDA	・ ソフトウェアが導入できるハードウェアを明確にする

	<ul style="list-style-type: none"> ・ライセンスがバンドルされている機器 例：PC・HDD・DVDなどのドライブ 	<ul style="list-style-type: none"> ・ライセンスが付属するハードウェアを明確にする
導入ソフトウェア	<ul style="list-style-type: none"> ・ハードウェアに導入された実行可能なソフトウェア 例：OS・アプリケーション・ユーティリティ 	<ul style="list-style-type: none"> ・ハードウェアに導入されたソフトウェアを明確にする
ライセンス	<ul style="list-style-type: none"> 外部から購入したソフトのライセンス 例：パッケージソフトウェア 	<ul style="list-style-type: none"> ・組織で保有するライセンス数を明確にする
ライセンス関連部材	<ul style="list-style-type: none"> ・使用許諾条件を満たすために必要な部材（導入用DVD/ライセンス証書・データが格納されたDVD・パッケージなど） 	<ul style="list-style-type: none"> ・使用許諾条件を逸脱しない、又は適正にソフトウェアが導入される環境を維持するため

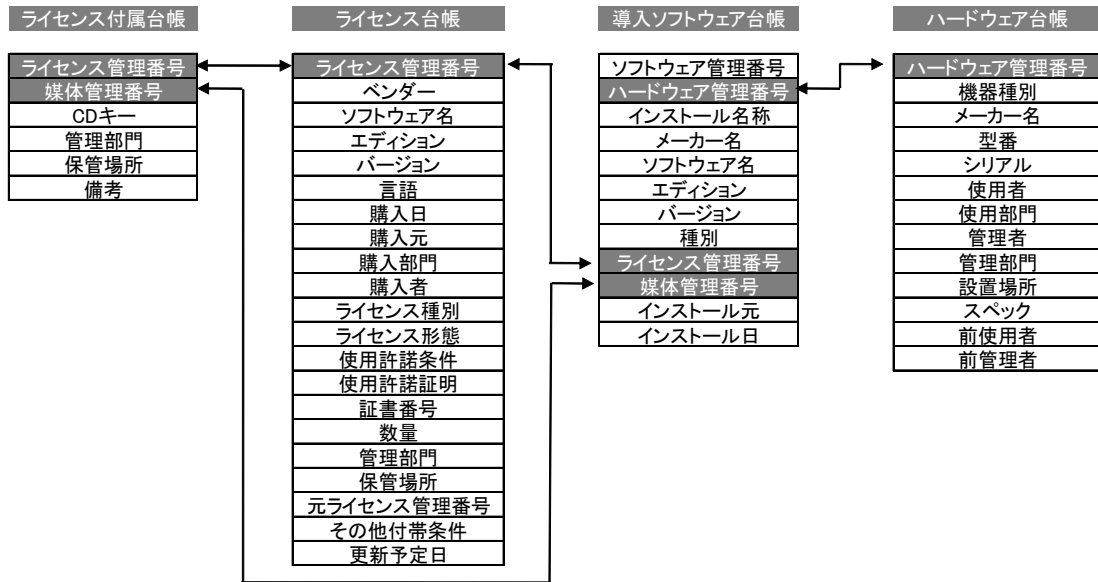
また、SAMでは、図表4-3「管理対象資産の把握の手順」の通り、当該組織が保有、ないしは、利用するハードウェア、ソフトウェア、ライセンスの調査を実施したうえで、ライセンスの過不足数を確定する必要がある。

(図表 4-3) 管理対象資産の把握の手順



なお、各管理台帳の項目例、および、各管理台帳の関連図については、図表 4-4「各台帳の関連図」を参考にして頂きたい。

(図表 4-4) 各台帳の関連図



従って、ISMS で作成した資産目録は、SAM を実施するために必要となる管理項目が網羅されていない、ライセンス過不足状況が把握できていないなど、コンプライアンス上の要求事項を満していないため、ISMS 認証取得しているからといって、ISMS の管理策の前提である「SAM ができている状態」とは言えないのである。

4.2. SAM ができていないことによる ISMS/ITSMS への影響

4.2.1. SAM の要求事項と ISMS/ITSMS との関連性

ISMS、ITSMS の先行実施が SAM を実施するうえで、どのように役立つかを検証するために、JIS X 0164-1 の要求事項を整理し、ISMS、ITSMS の要求事項との関連性を整理した比較表を作成した。(図表 4-5)

この比較表では、SAM プロセスに関わる個別の要求事項に記載されている 4.2 から 4.7 の項目について、関連する ISMS、ITSMS の要求事項の項番を記載している。

SAMプロセス		項番	内容	ISMSの 該当項番	ITSMSの 該当項番	
SAMの統制環境	SAMの企業統治プロセス	4.2.2.2.a	組織の範囲及びその中の責任者の明確化	4.2.1 a, 5.1 c, 4.3.1 b	4.1 a, 4.1 d	
		4.2.2.2.b	SAMの企業統治責任の最高意思決定機関による認識	4.2.1 b 5), 5.1	3.1	
		4.2.2.2.c	ソフトウェア資産の使用に関する規制や方針の文書化及びレビュー	4.3.1 a, 4.3.2 b	3.2 a, 3.2 d	
		4.2.2.2.d	SAMIに関連する資産に対するリスクアセスメントの実施と最高意思決定機関による承認とレビュー	4.2.1 g, 5.1 h, 7.1	4.1 f, 4.2 d, 3.1 f	
		4.2.2.2.e	SAMの管理目的に対する最高意思決定機関による承認	5.1 b	3.1 a	
	SAMの役割及び責任	4.2.3.2.a	SAM管理責任者の役割の明確化と最高意思決定機関による承認	5.1 c	3.1 d, 4.1 d	
		4.2.3.2.b	SAMIに対する部門管理者の役割及び責任の明確化	5.1 c	4.1 d	
		4.2.3.2.c	対象組織におけるSAM管理責任者及び部門管理者の役割及び責任の周知	5.2.2 d	4.1 d, 3.3	
	SAMの方針、プロセス及び手順	4.2.4.2.a	SAMIに関係する方針、プロセス、手順及び関連文書の作成とその承認、発行、管理方法の明確化	4.3.1, 4.3.2, 4.3.3	3.2 a, c	
		4.2.4.2.b	規格の要求事項に応じた上記の方針、プロセス、及び手順関係文書の分類と相互参照性の構築	4.3.3	3.2	
		4.2.4.2.c	規格の要求事項に応じた方針の策定、承認、公表	4.2.1 b2, 4.2.1 b5	3.2	
		4.2.4.2.d	これらの方針及び手順の全対象者に対する伝達、及び全対象者の閲覧可能状態の維持	4.3.3	3.2	
	SAMIにおける能力	4.2.5.2.a	教育訓練の可用性、及びそのレビュー	5.2.2	3.3	
		4.2.5.2.b	ライセンスの証拠のレビュー	N/A	N/A	
		4.2.5.2.c	SAMの管理責任を負う要員への教育訓練の実施	5.2.2 b, 4.2.2 e	3.3	
		4.2.5.2.d	ソフトウェアベンダーからの新しいライセンス情報の入手	N/A	N/A	
	SAMの計画立案及び導入プロセス	SAMの計画立案	4.3.2.2.a	SAMの管理目的の定期的な更新、修正とその承認の実施	4.2.1 b1, 4.2.1 b5	4.1 b
			4.3.2.2.b	SAM計画の定期的な立案	7.1, 8.1	4.4.3
			4.3.2.2.c	SAM計画の最高意思決定機関による承認	4.2.1 b5, 4.2.1	4.1
		SAMの導入	4.3.3.2.a	SAM計画に対するインシデント及びリスクに対するフィードバック	4.2.2 h, 4.2.3 a	4.2 d
			4.3.3.2.b	SAM計画の進捗状況報告書の作成	4.2.2 d, 5.1 b, 4.2.3 c	4.2 h
			4.3.3.2.c	是正項目のフォローアップ	4.2.2 h, 8.2, 4.2.3 a	4.4.2 a
		SAMの監視及びレビュー	4.3.4.2.a	定期的なSAM実施のレビュー	4.2.3 b, 7.1	4.3
4.3.4.2.b			最高意思決定機関によるSAMの実施事項に関する承認	5.1	3.1 g	
4.3.4.2.c			定期的なSAMの改善のためのレビュー	8.1, 5.2.1 e	4.3	
SAMの継続的改善		4.3.5.2.a	SAMの改善案の収集システム	8.1, 8.3	4.4.2	
		4.3.5.2.b	SAMの改善案の実行システム	8.2, 5.2.1 f	4.4.3	
SAMの在庫プロセス		ソフトウェア資産の識別	4.4.2.2.a	管理すべき資産の種類及び付随する情報の定義	A.7.1.1, A.7.1.2	9.1
	4.4.2.2.b		管理すべき資産の保管先及び在庫リストの作成	A.7.1.1, A.7.1.2	9.1, 3.2 d	
	ソフトウェア資産の在庫管理	4.4.3.2.a	在庫管理のための方針、及び手続きの策定	4.3.1 a, A.7.1.1	9.1, 3.2 a, c	
		4.4.3.2.b	ハードウェア、インストールソフトウェア及びライセンスの在庫リスト	A.7.1.1	9.1, 3.2 d	
		4.4.3.2.c	ソフトウェア原本、及び契約書類の在庫リスト	A.7.1.1	9.1, 3.2 d	
		4.4.3.2.d	インストールして利用されるソフトウェア	A.7.1.1	9.1, 3.2 d	
		4.4.3.2.e	管理すべき資産の継続可用性の確保	N/A	9.2	
		4.4.3.2.f	在庫報告書への目的、及びデータソースの詳細の記述	N/A	9.1	
	ソフトウェア資産の管理	4.4.4.2.a	管理すべき資産の情報変更に関する監査証拠の維持	6	9.1	
		4.4.4.2.b	ソフトウェアのバージョン管理に関する方針、及び手続き	N/A	9.1	
		4.4.4.2.c	ソフトウェアの実展開の基準に関する方針、及び手続き	N/A	10.1	
	SAMの検証、及び順守プロセス	ソフトウェア資産記録の検証	4.5.2.2.a	管理すべき資産の記録を検証する方針、及び手続き	N/A	9.1
			4.5.3.2.a	ソフトウェア使用許諾条件の順守に関する方針、及び手続き	A.15.1.2	9.1
ソフトウェア資産セキュリティの順守		4.5.4.2.a	SAMIに関するセキュリティポリシーの実践	4.3.1 a, 4.2.1 g	6.6	
		4.5.4.2.b	不備に関する是正措置の実施	4.2.2 h, 8.2	6.6	
SAMの適合性検証		4.5.5.2.a	規格の要求事項に対する順守と検証の方針及び手続き	4.3.3	3.1	
		4.5.5.2.b	規格の要求事項に対する順守と検証の実施	4.3.3	3.1	

SAMプロセス		項番	内容	ISMSの 該当項番	ITSMSの 該当項番
SAMの運用管理プロセス、及びインターフェイス	SAMの関係及び契約管理	4.6.2	SAMの関係及び契約管理	N/A	7.2, 7.3
	SAMの財務管理	4.6.3	SAMの財務管理	N/A	6.4
	SAMのサービスレベル管理	4.6.4	SAMのサービスレベル管理	A.10.2	6.1
	SAMのセキュリティ管理	4.6.5	SAMのセキュリティ管理	4.2.2 h, 4.2.1 e	6.6
SAMのライフサイクルプロセスインターフェイス	変更管理プロセス	4.7.2	変更管理プロセス	A.9.2.7	9.2
	取得プロセス	4.7.3	取得プロセス	A.7.1.1	9.1
	ソフトウェア開発プロセス	4.7.4	ソフトウェア開発プロセス	N/A	9.1
	ソフトウェアリリース管理プロセス	4.7.5	ソフトウェアリリース管理プロセス	N/A	10.1
	ソフトウェア展開プロセス	4.7.6	ソフトウェア展開プロセス	N/A	9.1, 10.1
	インシデント管理プロセス	4.7.7	インシデント管理プロセス	4.2.2h, 4.2.3a	8.2
	問題管理プロセス	4.7.8	問題管理プロセス	4.2.3 b	8.1
	廃棄プロセス	4.7.9	廃棄プロセス	A.9.2.6	9.1

(図表 4-5) SAM、ISMS、ITSMS の要求事項における関連性の比較表

上記の調査結果からも分かる通り、ISMS、ITSMS の先行実施が SAM を実施するうえで有用であることが分かる。

SAM、ISMS、ITSMS は、マネジメントシステムであり、基本的には、PDCA サイクルは存在し、それを支えるための統制環境も存在する。

そこで、SAM に関連が強い、ISMS については、「資産目録」、ITSMS については、「構成管理」、「変更管理」の3点に絞って、SAM を実施するうえで、ISMS、ITSMS の先行実施がどのように役立つかについて説明したい。

4.2.2. SAM を実施する上での ISMS の先行実施の有用性

資産目録：

ISMS を先行実施することによって、SAM で必要となる管理台帳のもととなる資産目録を作成することになるので、ISMS で作成した資産目録をもとに、SAM を実施するために必要となる項目を充足させ、保有ライセンス管理台帳、導入ソフトウェア管理台帳、ハードウェア管理台帳、ライセンス関連部材管理台帳の各管理台帳を整備すればよい。

また ISMS 附属書「A7.1.1 資産目録」の管理策に対して、SAM の貢献ポイントとして考えられる部分として、JIS X 0164-1 の「4.4.2 ソフトウェア資産の識別」に関する要求事項を挙げるができる。

(図表 4-6) ISMS の管理策に対する SAM の貢献

箇条	管理策	SAM の貢献ポイント
A.7.1.1 資産目録	すべての資産は、明確に識別しなければならない。また、重要な資産すべての目録を、作成し、維持しなければならない。	4.4.2 ソフトウェア資産の識別

JIS X 0164-1 の「4.4.2 ソフトウェア資産の識別」では、ソフトウェア資産のライフサイクル全体を通じ、効率的な SAM を実現するため、対象となるソフトウェア資産を適切に定義、分類されるように、次のような事項が要求されている。

- ・管理対象となる資産の種類、及び必要とされる管理項目が定義されていること
- ・対象資産について種類が特定され、必要な情報が把握管理されること
- ・個々の対象資産が管理可能、追跡可能であるように一意に識別できること
- ・何がどこに保管されているか把握管理するため、台帳が作成されること
- ・対象資産の複製については、複製元を特定できるように管理されること

従って、本要求事項に沿った各管理台帳を整備するためにも、JIPDEC が発表している「SAM ユーザーズガイド —導入のための基礎—」を参照し、導入計画を立案し、構築を行っていくことが望ましい。

具体的には、対象資産の定義や分類については、「5.2.2 SAM のスコープの検討」、「6.2.3 対象資産の設定」に記載されており、管理項目については、「5.2.3 導入する SAM の枠組みの検討」、「6.4.1.1 ハードウェア台帳管理項目の設定」、「6.4.2.1 導入ソフトウェア台帳管理項目の設定」、「6.4.3.1 ライセンス台帳・ライセンス関連部材台帳の管理項目の設定」に記載されている。また、対象資産の調査手順については、「6.4 対象資産の調査手順」に記載されているので参考にして頂きたい。

4.2.3. SAM を実施する上での ITSMS の先行実施の有用性

JIS X 0164-1 には、「この規格が定義する SAM のプロセスは、JIS Q 20000 規格群が定義している情報技術 (IT) サービスマネジメントとよく両立するように構成されており、それを適切に支援することを意図している。」と記述されている。

ITSMS のマネジメントプロセスで、SAM のプロセスに対して、最も直接的に貢献可能と思われる部分は「構成管理」と「変更管理」である。

そこで、ITSMS のマネジメントプロセスの中から、「9.1 構成管理」と「9.2 変更管理」のマネジメントプロセスに対応する SAM のプロセスを抽出した。

(図表 4-7) ITSMS のマネジメントプロセスに対する SAM の貢献

ISO/IEC 20000-1 の箇条	プロセスの目的	対応する JISX 0164-1 の箇条
9. 統合的制御プロセス		
9.1 構成管理	CMDB は更新アクセスの制御を含め、その信頼性及び正確性を確実にするために管	4.4.2 ソフトウェア資産の識別 4.4.3 ソフトウェア資産の

	理しなければならない。各 CI の種類の定義について文書化しなければならない。	在庫管理 4.4.4 ソフトウェア資産の管理 4.5.2 ソフトウェア資産記録の検証
9.2 変更管理	変更管理方針を確立し、次を定義しなければならない。 a) 変更管理が制御している CI b) サービス又は顧客に重大な影響を及ぼす可能性のある変更を判断する基準	4.7.2 変更管理プロセス

(1) 構成管理：

ITSMS における構成管理プロセスの骨子は、サービス及びインフラストラクチャのコンポーネントを定義し、制御し、かつ、正確な構成情報を維持するために、以下の活動を実施することである。

- ・ 構成管理の計画及び導入
- ・ 構成識別
- ・ 構成コントロール
- ・ 構成ステータスの説明及び報告
- ・ 構成の検証及び監査

構成品目の例としては、ソフトウェアと関連する文書（要求仕様書、設計書、リリース文書）など、標準ハードウェアやセキュリティコンポーネント（ファイアーウォール）など、サービス関連文書（SLA、契約書）などが挙げられる。

従って、ITSMS におけるソフトウェア及び関連文書などの「構成管理」プロセスは、「SAM の在庫プロセス（JIS X 0164-1 4.4）」とおおむねオーバーラップしている。

（SAM の在庫プロセスは、「ソフトウェア資産の識別」、「ソフトウェア資産の在庫管理」、「ソフトウェア資産の管理」の3つから構成されている。）

このように、構成管理に関する両者の親和性は極めて高く、ITSMS を先行実施することで、SAM をスムーズに実施することが可能になるが、以下の点には注意する必要がある。

- ・ 構成管理の適用範囲について

ITSMS の適用範囲は、多くの場合「システム運用管理部門」に限定される。これに対し

て、SAM は（コンプライアンス上の要求事項を満たすという目的のために）組織全体を適用範囲とすることが多い。したがって、ある組織が（運用管理部門で）ITSMS を導入し、構成管理プロセスを適正に運用しているからといって、その組織全体が SAM に関するコンプライアンスを達成していることにはならない。

- ・ 構成品目の識別メッシュについて

SAM の「ソフトウェア資産の識別」において管理すべき項目には、ソフトウェアの原本と写しのほか、使用許諾契約に係る文書類など、コンプライアンス上の要求事項を満たすため、在庫管理プロセスにおける構成品目の識別メッシュが非常に細かくなっている。これに対して、ITSMS の構成管理においては、基本的に「ビジネスが必要とする」レベルで構成品目を識別すれば十分とも考えられ、総じて SAM と比較して ITSMS の方が構成品目の識別メッシュは粗いことが多い。

（2）変更管理

ITSMS における変更管理プロセスの骨子は、すべての変更を、制御された方法で、アセスメント、承認、実装及びレビューすることを確実にするために、以下の活動を実施することである。

- ・ 変更要求の記録（変更要求の登録とフィルタリング）
- ・ 変更要求の分類（優先度の割り当て、変更のカテゴリ化）
- ・ 変更要求の評価
- ・ 変更の認可
- ・ 変更の実装の監視（変更の構築、テスト、実装）
- ・ 変更のレビュー

「SAM の変更管理プロセス（JIS X 0164-1 4.7.2）」では、ソフトウェア及び関連資産に関連するすべての「変更」について、管理することを求めている。ソフトウェア及び関連資産に関連するすべての「変更」とは、ソフトウェア資産管理全体のプロセスに影響する事項すべてと規定されている。この管理は、制御された管理であることが重要で、発生毎に検討するのではなく、定義されて、承認を得ており、実際に実行され、レビューされて、すべての記録保持の確認もされている状態としている。これは、ソフトウェアの特性として、「変更」が表面化しにくい要素があるため、そうした特性を配慮して検討しておくことが必要となる。

また、「SAM の変更管理プロセス（JIS X 0164-1 4.7.2）」では、変更管理プロセスの導入で、実現できる項目を下記のように定義している。

- ・ ソフトウェア及び関連資産のすべての「変更」の特定。これは、サービスや SAM プロセスに影響する項目も含み、それらすべての「変更」の事前の特定と、特定された内容の

記録。

- ・ソフトウェア及び関連資産の「変更」が影響する範囲の評価と優先度の特定。また、担当管理者によって、優先度等承認されている状態。

- ・承認された変更要求の実施プロセスは、承認に従って実施されている状態。
- ・ソフトウェア及び関連資産のすべての「変更」が記録されている状態。
- ・ソフトウェア及び関連資産のすべての「変更」実施の成否の文書情報と定期的レビュー

従って、ITSMSにおけるソフトウェア及び関連文書などの「変更管理」プロセスは、「SAMの変更管理プロセス（JIS X 0164-1 4.7.2）」とおおむねオーバーラップしている。このように、変更管理に関する両者の親和性は極めて高く、ITSMSの先行実施することで、SAMをスムーズに実施することが可能になる。

総括すると、総合的にSAMをスムーズに実施するためには、ISMS/ITSMSによる管理基盤を先行整備することが望ましく、その結果、組織としてのリソースの有効活用につながることになる。

5. 結果と考察

最後に、本稿各章における検討の結果と考察について述べる。

第2章ではマネジメントシステムの比較検証を行い、以下の結論を得た。

- ① SAM と ITSMS は多くのプロセスにおいて共通性が認められるが、SAM の要求プロセスが全て ITSMS に包含されている訳ではない
- ② 成熟度の高い組織が ITSMS を構築すれば、SAM の要求するプロセスの 80%以上は実装されているはずである。
- ③ ITSMS の管理対象として、PC からサーバーまでサービス提供基盤を全て含めることが、SAM と親和性の高い ITSMS を構築するポイントである。
- ④ マネジメントシステムの骨格については SAM と ISMS/ITSMS には大きな矛盾はないが、各規格の目的が異なる以上、要求事項の詳細については違いも多く、実運用においてはその差をふまえて実施していく必要がある。

第3章では SAM と ISMS/ITSMS の統合運用スケジュールを検討し、以下の結論を得た。

- ① 運用サイクルについては、例えば年度予算編成時期、内部監査時期等と整合させることで、統合運用を進められる可能性が高い。
- ② 管理メッシュについては、マネジメントシステム毎に粒度が違うために、運用担当者間でギャップが生じてしまう可能性がある。
- ③ 事務局を統合することで、SAM と ISMS/ITSMS の運用負荷は大きく軽減され、統合運用の意義は大きい。

第4章では SAM と ISMS/ITSMS の管理策を比較検討した結果、以下の結論を得た。

- ① SAM を実施する上で ISMS の先行実施が役立つポイントは、「資産目録」の整備と運用である。
- ② SAM を実施する上で、ITSMS の先行実施が最も直接的に貢献すると思われる部分は「構成管理」と「変更管理」である。
- ③ 総合的に SAM をスムーズに実施するためには、ISMS/ITSMS による管理基盤を先行整備することが望ましく、組織としてのリソースの有効活用につながる。

以上の検討は SAM の啓発・導入促進に繋がることを目的としており、本稿が企業・組織において SAM に対する取り組みを検討する上での一助となることを期待している。

平成 23 年度ソフトウェア資産管理評価検討委員会

(敬称略)

氏名	所属	WG
篠田 仁太郎 (委員長)	(株)クロスビート	
今田 英顕	日本電気(株)	WG3
片岡 伸吉	オートデスク(株)	WG3
薩摩 貴人	公認情報システム監査人/公認内部監査人	WG3 リーダー
塩田 貞夫	日本ヒューレット・パッカード(株)	WG2
島田 篤	ダイヤモンドレンタルシステム(株)	WG1
高橋 快昇	富士通(株)	WG1
武内 烈	国際 IT 資産管理者協会	WG2
田村 仁一	有限責任監査法人トーマツ	WG1 リーダー
手島 伸行	日本マイクロソフト(株)	WG1
中村 大造	ウチダスペクトラム(株)	WG2
中村 究	(株)シルクロード テクノロジー	WG2 リーダー
川崎 紘	石川県	WG3
新城 裕也	沖縄県	WG3