

SAM ユーザーズガイド

—導入のための基礎—

SAM : Software Asset Management
ソフトウェア資産管理

平成 22 年 6 月



財団法人 日本情報処理開発協会



この事業は、競輪の補助金を受けて実施したものです。
<http://ringring-keirin.jp/>

はじめに

本ガイドは、財団法人日本情報処理開発協会が財団法人 JKA の補助金を受けて実施した平成 22 年度情報化推進に関する調査研究等補助事業「IT サービスマネジメントの利活用によるシステム構築・運用環境の改善に向けた調査研究」事業の一環として作成したものである。

近年、ソフトウェアの不正コピーやソフトウェアライセンスの不正利用などの法的問題は、組織の姿勢そのものに疑念を持たれることになり、社会的な信用の失墜につながっている。それらを防止するためにも、組織で利用されている IT 資産、とりわけソフトウェア資産を適切に管理し、利用可能ライセンス数の把握をする必要がある。組織にとって適切なライセンスを把握することで、無駄なライセンス数を購入することがなくなる。また、ソフトウェア資産管理を行うことで利用ソフトウェアのバージョン管理、パッチ適用などのシステム構築・運用環境の改善を図ることができ、オペレーションコストの削減にもつながる。

本ガイドでは、IT サービスマネジメントの利活用の観点から、国際標準の ISO/IEC 19770-1 (Information technology-Software asset management-Part1) に基づいて組織のソフトウェア資産の効果的な管理及び保護のために必要なガイドを策定し、情報セキュリティ強化の促進と適切なソフトウェア資産管理の実現を目的としてとりまとめた。

本調査研究では、組織におけるソフトウェア資産管理の現状の問題点を把握するとともに、国際規格化の動向を調査し、組織が適切にソフトウェア資産管理を構築・運用するためのガイドを提示した。また、IT サービスマネジメントシステム (ITSMS) の一要素として、ソフトウェア資産管理のプロセス (IT サービスの効果的管理のために必要な管理プロセス) があることから、IT サービスマネジメントの品質向上を図るためのガイドも提示した。

本ガイドの作成にあたり、ソフトウェア資産管理評価検討委員会の委員の皆様をはじめ、ご協力頂いた関係各位に対し厚く御礼申し上げます。

平成 22 年 6 月

財団法人 日本情報処理開発協会

目次

はじめに

1. ソフトウェア資産管理の位置づけ	1
1.1. ソフトウェア資産管理（SAM）とは	1
1.1.1. ソフトウェア資産管理とソフトウェアライセンス管理の目的の差異	1
1.1.2. ソフトウェア資産管理開発の背景	1
1.1.3. まとめ	2
1.2. ISO/IEC 19770 と他の規格との関係及びISO/IEC 19770 のロードマップ	2
1.2.1. ISO/IEC 19770 と他の規格の関係	3
1.2.2. ISO/IEC 19770 のロードマップ（2010年1月現在）	3
1.2.2.1. ISO/IEC 19770-0：ソフトウェア資産管理の概説及び定義	3
1.2.2.2. ISO/IEC 19770-2：ソフトウェアタグ	4
1.2.2.3. ISO/IEC 19770-3：ソフトウェアライセンスタグ	4
1.2.2.4. ISO/IEC 19770-4：Tiered Approach	4
1.3. SAMに関連する団体	4
1.3.1. 日本におけるSAMに関連する団体	4
1.3.2. 他国におけるSAMに関連する団体	5
1.4. 本ガイドの活用方法	6
1.4.1. 本ガイドの利用対象者	6
1.4.2. 本ガイドにおけるSAMの基準	6
1.4.2.1. 本ガイドにおける「SAMができている状態」	6
1.4.2.2. SAMの管理台帳について	7
1.4.3. 本ガイドの構成	7
1.4.4. 本ガイドの活用方法	8
2. 用語の解説	9
2.1. ソフトウェア資産管理基準	9
2.2. ソフトウェア資産管理評価規準	9
2.3. 情報セキュリティマネジメントシステム（ISMS）	9
2.4. ITサービスマネジメントシステム（ITSMS）	9
2.5. ITインフラストラクチャーライブラリー（ITIL®）	10
2.6. CMM（Capability Maturity Model）	10

2.7. COBIT	10
2.8. ISO/IEC 19770	10
2.9. ソフトウェア	10
2.10. ライセンス	11
2.11. ハードウェア	11
2.12. ソフトウェア資産	11
2.13. IT資産	11
2.14. IT資産のライフサイクル	11
2.15. ライセンス管理	11
2.16. ソフトウェア資産管理 (SAM)	11
2.17. 使用許諾契約 (使用許諾書)	11
2.18. ソフトウェア資産管理ツール (SAMツール)	11
2.19. インベントリ	12
2.20. 内部監査	12
2.21. 外部監査	12
2.22. 棚卸	12
2.23. ソフトウェアの調達	12
2.24. ソフトウェアの導入	12
2.25. ソフトウェアの削除	12
2.26. ライセンスの利用	12
2.27. ライセンスの保有	13
2.28. ライセンスの廃棄・返却 (又は廃却)	13
2.29. スコープ	13
2.30. ITガバナンス	13
2.31. 導入ソフトウェア台帳	13
2.32. 保有ライセンス台帳	13
2.33. ライセンス関連部材	13
2.34. ライセンス関連部材台帳	13
2.35. ハードウェア台帳	14
2.36. キットティング	14
3. SAMのマネジメントプロセス	15
3.1. SAMのPDCAサイクル	15

3.1.1. Plan（計画立案）	15
3.1.2. Do（導入）	15
3.1.3. Check（監視及びレビュー）	16
3.1.4. Act（継続的改善）	16
3.2. 他のマネジメントシステムとの関連	16
3.2.1. ISMS	16
3.2.2. ITSMS	17
3.2.3. 各マネジメントシステムの比較と相互関係	17
4. IT資産のライフサイクルプロセスとSAM	21
4.1. 取得	21
4.1.1. 取得の定義	21
4.1.2. 取得プロセスの目的と範囲	21
4.1.3. 調達プロセスの内容	22
4.1.4. 調達仕様書の作成	23
4.1.5. 調達コストの最適化	26
4.1.6. ソフトウェア使用許諾条件の順守	27
4.1.7. 発注の処理	27
4.1.8. 納品処理	27
4.1.9. 社内開発によるソフトウェア及び関連資産の取得	28
4.2. 導入	29
4.2.1. ソフトウェアリリース管理プロセス	29
4.2.2. ソフトウェア展開プロセス	29
4.3. 異動	31
4.3.1. 変更管理プロセス	31
4.3.2. ソフトウェア展開プロセス	31
4.3.3. 異動時の留意事項	31
4.4. 廃却	32
4.4.1. 廃却情報の集中化	33
4.4.2. 廃却時のアンインストール	33
4.4.3. 廃却時の情報の更新方法	33
4.5. ISMS／ITSMSにおけるSAMの必要性	33
5. SAMの導入計画	39

5.1. SAMの導入計画の実施手順	39
5.1.1. 現状把握	39
5.1.2. 保有あるいは利用されているソフトウェア資産の概要把握	40
5.1.3. ソフトウェア資産の現状の管理状況の把握	40
5.1.4. ソフトウェアのライフサイクル及びSAMに関わる業務プロセス概要の把握	41
5.1.5. SAM関連のコストの把握	41
5.1.6. ソフトウェア資産に関わるリスクの把握	41
5.2. 体制及び方針決定	44
5.2.1. 現状の整理と利用方針、購入方針などの検討	45
5.2.2. スコープの決定	48
5.2.3. 導入するSAMの枠組みの検討	50
5.2.4. SAM導入方針の策定	51
5.3. 導入計画の策定	52
5.3.1. 作業内容の洗い出し	52
5.3.2. 導入プロジェクト体制の決定	52
5.3.3. 作業スケジュールの作成	53
5.3.4. 導入コストの検討	53
5.4. SAM の成熟度評価	53
5.4.1. SAM のアセスメント	53
5.4.1.1. 成熟度モデル	54
5.4.1.2. 成熟度モデルの考え方	55
5.4.1.3. 成熟度評価	56
5.4.1.4. 成熟度評価方法	57
5.4.1.5. 成熟度評価報告	60
6. SAMの構築	63
6.1. SAMの構築プロセス	63
6.2. 事前準備	63
6.2.1. SAM導入目的の確認	64
6.2.2. 管理対象組織の設定	64
6.2.3. 対象資産の設定	64
6.3. 現状分析	67
6.3.1. 業務プロセスの洗い出し	67

6.3.1.1.	なぜ業務プロセスの洗い出しが必要か	67
6.3.1.2.	現状の業務プロセスの洗い出し方法	70
6.4.	対象資産の調査手順	72
6.4.1.	ハードウェア調査	73
6.4.1.1.	ハードウェア台帳管理項目の設定	74
6.4.1.2.	作業方法の設定	74
6.4.1.3.	作業マニュアルの作成	76
6.4.1.4.	作業方法の講習	77
6.4.1.5.	棚卸の実施	77
6.4.1.6.	データの精査	77
6.4.2.	導入ソフトウェア調査	78
6.4.2.1.	導入ソフトウェア台帳管理項目の設定	79
6.4.2.2.	導入ソフトウェア情報の分析	80
6.4.2.3.	標準・個別導入ソフトウェアの選定	81
6.4.2.4.	未許可ソフトウェアの抽出	82
6.4.3.	ライセンス調査	82
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	83
6.4.3.2.	保有すべきライセンスの確認	84
6.4.3.3.	ボリュームライセンスの調査	85
6.4.3.4.	管理部門が持つライセンスの調査	85
6.4.3.5.	未許可ソフトウェアの調査	86
6.4.3.6.	台帳の関連付け	86
6.4.4.	ライセンス過不足数の是正	88
6.4.4.1	ライセンス過不足数の是正	88
6.5.	問題点の抽出・分析	89
6.5.1.	SAMの業務プロセスに求められる要件の確認	89
6.5.1.1.	SAMに求められる要件	90
6.5.2.	問題点の抽出・分析	91
6.5.2.1.	目標とする管理状態の設定	91
6.5.2.2.	現状の把握結果からの問題点の抽出と解決策の策定	92
6.6.	SAM業務の構築	93
6.6.1.	管理体制の整備	94

6.6.2.	原因の解決方法を策定	96
6.6.3.	改善結果に基づきソフトウェア資産管理規程・使用規則を整備する	97
6.7.	管理規程・手順の策定	97
6.7.1.	管理規程とは	97
6.7.1.1.	管理規程と管理手順書の違い	98
6.7.1.2.	全社規程におけるSAM管理規程の位置づけ	98
6.7.2.	管理方針、管理規程の推奨記載項目	100
6.7.2.1.	ソフトウェア資産管理方針の推奨記載項目	100
6.7.2.2.	ソフトウェア資産管理規程の推奨記載項目	101
6.7.3.	管理手順書の策定例	102
6.7.3.1.	管理手順書の策定手順及び推奨記載項目	102
6.8.	SAMの運用設計	106
6.8.1.	SAM年度計画の策定	106
6.8.1.1.	棚卸	106
6.8.1.2.	監査	108
6.8.1.3.	レビュー	108
6.8.2.	周知	109
6.8.2.1.	管理者への周知	110
6.8.2.2.	全要員への周知	110
7.	SAM運用上のポイント	111
7.1.	SAMを高度化するための改善及び計画策定におけるポイント	111
7.1.1.	コンプライアンスのための計画	111
7.1.2.	コスト削減・合理化のための計画	116
7.2.	SAMを組織へ定着させるためのポイント	119
7.3.	棚卸の実施におけるポイント	122
7.4.	SAM監査におけるポイント	124
7.4.1.	SAM監査計画の策定	125
7.4.2.	SAMの監査実施	128
8.	SAMツール利用のためのポイント	129
8.1.	ツール利用による運用の効率化	129
8.2.	SAMツールとは	129
8.3.	IT資産のライフサイクル管理と関連ツール	130

8.4. SAMツールの機能比較	132
8.4.1. インベントリ収集機能の比較	132
8.4.2. 構成管理機能の比較	137
8.4.3. 台帳管理機能の比較	138
8.4.3.1. 棚卸支援機能の比較	139
8.4.4. その他機能の比較	139
8.5. SAMツールの評価例	139
付録	143
A-1 ソフトウェア資産管理方針	143
A-2 SAMに関連する各種団体・規格・基準・書籍など	145
a) 団体	145
b) 国際規格	145
c) 書籍など	145
d) 基準（ソフトウェア資産管理コンソーシアム：SAMCon（Software Asset Management Consortium））	145
e) ガイド	145

1. ソフトウェア資産管理の位置づけ

1.1. ソフトウェア資産管理 (SAM) とは

ISO/IEC 19770-1 (ソフトウェア資産管理 プロセス) によれば、SAM の目的は、「IT サービスマネジメント全体の有効な支援」とするものであり、「ビジネスリスク管理の促進」、IT サービス及び IT 資産に関する「コスト管理の促進」、IT を有効に活用することによる「競争上の優位性を得ること」としている。

ここから、SAM とは、IT の基盤要素であり、IT 全般に対して重要なマネジメントシステムの一つとして考えられていることがわかる。

1.1.1. ソフトウェア資産管理とソフトウェアライセンス管理の目的の差異

ISO/IEC 19770-1 に SAM について上記のとおり定義されている一方で、ソフトウェア資産管理を単に著作権法、及び使用許諾条件の順守を目的とするもの (以下「ライセンスコンプライアンス」という。) と捉えてしまうことがある。これをここではソフトウェアライセンス管理 (以下「ライセンス管理」という。) とする。

ソフトウェア資産管理とライセンス管理という言葉は、管理対象とする資産も、ハードウェア・利用ソフトウェア及びソフトウェアライセンスと同一であることから、混同して使われやすい。しかし、その目的とするところは異なるため、本来は明確に区別して使用されることが望ましい。

1.1.2. ソフトウェア資産管理開発の背景

そもそも、ライセンス管理は、往々にして、ソフトウェアの著作権者からソフトウェアの利用者に対して求められるものであり、使用許諾契約に定められた使用条件を逸脱しないことを考慮し、実施されることが多い。

その場合、使用許諾契約により認められた利用可能数を実際の利用数が上回らないことにのみ重点が置かれ、結果、過剰なソフトウェアライセンス投資を招いたり、逆に、真に必要なソフトウェアライセンスを調達してもらえず、業務に支障が出ることも起こりうる。

また、ライセンスコンプライアンスといいながらも、その管理の対象は有償のソフトウェアのみに焦点が当てられがちであり、フリーウェアなどの無償ソフトウェアが管理の対象から除外されることも多く (フリーウェアであっても、著作権法の対象となるものであり、一般的には、ソフトウェアごとに使用許諾条件も定められている)、その場合には、ライセンスコンプライアンスの目的も十分に果たされないことになる。

ソフトウェア資産管理は、これらの欠点を解消し、ソフトウェア資産のマネジメントシステムを構築することで、より効果的・効率的な管理を実現するために開発されたものである。

このソフトウェア資産管理の考え方については、日本では「ソフトウェア資産管理基準 Ver. 1.0」がある。この基準は、特定非営利活動法人ソフトウェア資産管理コンソーシアム (以下、「SAMCon」という。) が任意団体だった 2003 年 11 月に、策定され、発表されたものである。SAMCon は、ソフトウェアメーカー、ハードウェアメーカー、管理ツールの開発会社・販売会社、ユーザ、コンサルティング会社など、日本で初めて著作権者以外にも参加した、ソフトウェアを利

用するユーザのための管理指針・管理ガイドを策定し、普及するために設立された団体である（2009年1月に任意団体から特定非営利活動法人に改組した）。そして、SAMConの立ち上げと並行するように、itSMF Japanが設立され、ITIL®¹が日本に普及し始め、そして2006年5月にISO/IEC 19770-1（ソフトウェア資産管理プロセス）が発行され、ソフトウェア資産管理はより広く認知されるようになった。

適切なソフトウェア資産管理を行うことが組織にとって大きなメリットをもたらすことは、この規格が発行されてから、ロシア、ドイツ、スウェーデン、スペインと、次々に国内規格として導入されていることから類推することができる。また、日本でも2010年5月にJIS X 0164-1として制定されている。

1.1.3. まとめ

以上から、ソフトウェア資産管理とライセンス管理の違いをまとめると、表 1-1 のとおりとなる。

表 1-1 ソフトウェア資産管理とライセンス管理の違い

	ソフトウェア資産管理	ライセンス管理
目的	<ul style="list-style-type: none"> ・ ライセンスコンプライアンス ・ 情報セキュリティの維持・向上 ・ IT投資の最適化 	主にライセンスコンプライアンス
対象資産	ハードウェア・利用ソフトウェア・保有ライセンス（有償・無償・自社開発の別はない）を対象とする。	保有ライセンス及び（ハードウェアを根拠としない）利用ソフトウェア（ライセンスについては、特に有償のライセンスを対象とする場合が多い）

また、IT 資産管理とソフトウェア資産管理、ライセンス管理の関係を図で示すと、図 1-1 のとおりとなる。

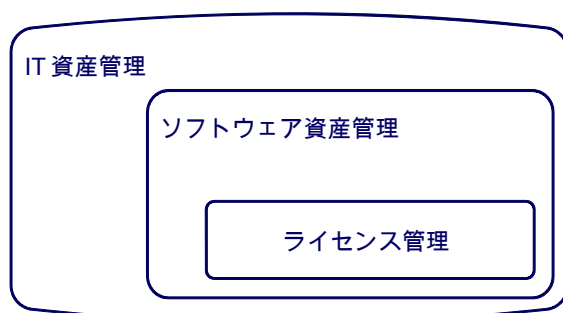


図 1-1 IT 資産管理とソフトウェア資産管理の関係図

1.2. ISO/IEC 19770 と他の規格との関係及び ISO/IEC 19770 のロードマップ

第 1 項で、ソフトウェア資産管理のガイドラインである SAMCon のソフトウェア資産管理基

¹ ITIL®は、英国、欧州連合各国、及び米国における英国政府Office of Government Commerce の登録商標であり、共同体商標です。

準及び、ISO/IEC 19770-1 について触れたが、ソフトウェア資産管理基準は Ver.2.0 を策定する際に、ISO/IEC 19770-1 の要求事項を取り入れて改定している。

ISO/IEC 19770-1 は、ワールドワイドで検討され発行されたソフトウェア資産管理の規格であり、今後もこれを軸にソフトウェア資産管理に関する様々な取り決めがなされていくと思われることから、ここでは、ISO/IEC 19770 について、少し触れておきたい。

1.2.1. ISO/IEC 19770 と他の規格の関係

ISO/IEC 19770 は、ソフトウェア資産管理のための規格であることはこれまで述べてきたとおりだが、ISO/IEC 19770-1 には、SAM の実施が以下のことをもたらすことを期待している。

(1) リスクマネジメント

IT サービス中断のリスク、IT サービスの品質低下のリスク、法的及び規制上のリスクの度合い、これらに起因する社会的信用力の失墜リスクなど、ビジネスリスクの管理の促進

(2) コスト管理

ソフトウェア資産の調達・導入・維持・運用コストなどの最適化及び削減

(3) 競争上の優位性

IT 投資に関する意思決定の迅速化、新たなシステムの速やかな展開、事業ニーズに合った適切なソフトウェアの利用、IT に関連する各種問題の減少に伴う IT 資産の可用性向上などによる競争上の優位性

このことから、ISO/IEC 27000（情報セキュリティ）及び、ISO/IEC 20000（IT サービス）に関連することは類推されるが、実際に、ISO/IEC 19770-1 の「4.6.5 SAM のセキュリティ管理」には、「ISO/IEC 17799 の認証を取得しようとする組織は、ISO/IEC 19770-1 の要求事項を満たすことが望ましい」と記載されており、ISO/IEC 20000 に対しては、序文に「この ISO/IEC 19770 第 1 部は ISO/IEC 20000 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」と記載されている。

このように、他の規格を参照したり、整合したり、又は他の規格に要求したりするような規格はあまり例がないが、切り離せないものだからこそ、規格の中に記載せざるを得なかったものであり、ソフトウェア資産管理が、情報セキュリティ上も IT 全般の運用上も重要であることを示すものである。

1.2.2. ISO/IEC 19770 のロードマップ（2010 年 1 月現在）

ISO/IEC 19770 では、2006 年 5 月に ISO/IEC 19770-1（ソフトウェア資産管理プロセス）を発行した後、現在は、ISO/IEC 19770-0、ISO/IEC 19770-2、ISO/IEC 19770-3、ISO/IEC 19770-4 が検討されている。

それぞれの内容を一言でまとめると以下のとおりとなる。

1.2.2.1. ISO/IEC 19770-0：ソフトウェア資産管理の概説及び定義

IT 資産管理と SAM の関係性から、SAM の必要性を説明し、ISO/IEC 19770 全体の用語やプロセスなどの整合性を保つために、定義しなおすもの。

1.2.2.2. ISO/IEC 19770-2 : ソフトウェアタグ

ソフトウェアの使用者が、ハードウェアに導入されているソフトウェアのベンダー名、バージョン、ソフトウェア名、用途などを容易に認識できるようにするために、ソフトウェアベンダーに対し、ハードウェアにソフトウェアを導入する際の付加情報として含むことを求めるもの。

1.2.2.3. ISO/IEC 19770-3 : ソフトウェアライセンスタグ

ソフトウェアの使用者が、ハードウェアに導入されているソフトウェアが、どのようなソフトウェアライセンスを必要としているかを容易に認識できるようにするために、ソフトウェアベンダーに対し、ハードウェアにソフトウェアを導入する際の付加情報として含むことを求めるもの。

1.2.2.4. ISO/IEC 19770-4 : Tiered Approach

ISO/IEC 19770-1 の要求事項を次の四つの段階に分け、構築していこうとするもの。

- 1) SAMに関し、信頼できる台帳を持っている。
- 2) SAMに関し、実用的な管理が実施できている。
- 3) SAMに関連する各種の運用が統合されている。

ISO/IEC 19770-1に完全適合している。

SAM への取り組みを4段階に分けることにより、導入を容易にし、SAM のメリットを享受しやすくしようとしているもの。

2010年1月現在、ISO/IEC 19770-2 は、2009年11月に正式に国際標準として発行されており、その他のパートについても、2010年以降、順次発行に向け、作業を進めている。

1.3. SAM に関連する団体

SAM については、日本でも幾つかの団体が存在するが、他国においても SAM に対する関心は高く、同じように幾つかの団体が存在している。著作権者による権利保護のための団体ばかりでなく、いかに SAM を運用しやすくするかについて、ベストプラクティスなどを研究している団体もある。また、SAM の知識レベルを認定する民間団体なども存在している。

ここでは、各国の SAM への取り組みを示す一例として、日本だけでなく、海外の SAM に関連する団体を紹介しておく。

1.3.1. 日本における SAM に関連する団体

(1) 特定非営利活動法人ソフトウェア資産管理コンソーシアム (SAMCon)

ソフトウェアベンダー、ツールベンダー、SAM コンサルティング会社が、中心となって設立した団体。SAM の統一的な手法をソフトウェア資産管理に関する管理基準（ソフトウェア資産管理基準）として策定した。また、その成熟度を客観的に評価するための評価規準（ソフトウェア資産管理評価規準）を策定した。ISO/IEC 19770 の日本におけるワーキンググループのミラー団体にもなっている。

(2) 社団法人コンピュータソフトウェア著作権協会 (ACCS)

ソフトウェア著作権の保護と啓蒙・情報モラルの普及などを事業目的として設立された団体。

ソフトウェアベンダーや、弁護士、出版社、ツールベンダーなど約 200 社が会員として参加し、活動している。SAMCon が SAM の手法についての啓蒙をしているのに対し、ACCS は、著作権の適切な保護を啓蒙している。

1.3.2. 他国における SAM に関連する団体

(1) International Association of IT Asset Managers (IAITAM) (米国)

IBM、マイクロソフト、HP、CA、ソニーアメリカなど、700 社を超えるソフトウェアベンダーや IT ベンダー、IT ユーザーが加盟している IT 資産管理のベストプラクティスを研究している団体。ソフトウェア資産管理からハードウェア資産管理及び IT 資産のライフサイクルにおけるあらゆる局面で、それを利用する組織の価値を高めるための手法を研究している。IT 資産管理における、ソフトウェア資産管理、ハードウェア資産管理、交渉、調達、財務管理の各分野のベストプラクティス集を発行しており、各種研修及び研修修了時の修了証の授与などを行っている。

(2) International Business Software Management Association (IBSMA) (米国)

ソフトウェアベンダーや、SAM コンサルティング会社がメンバーとなっている非営利法人。SAM に特化した啓蒙活動や知識認定などを行っている。SAM に関連する書籍の出版及び、「SAM Summit」と称して、毎年定期的に SAM に関する世界的な動向を共有するための大会を開催している。

(3) Software Property-right Council (SPC) (韓国)

韓国の著作権保護団体。警察と連携し、不正コピー抑止、著作権保護の啓蒙活動を行っている。ソフトウェアの利用調査をするための独自ツールを持っており、警察が査察に入る際には、このツールを利用し、ソフトウェアの不正使用の状況を確認している。後述する BSA も韓国にはあるが、BSA の摘発活動についても兼ねており、韓国での BSA の活動は、主に広報だけとなっている。

(4) Business Software Alliance (BSA) (世界各国に支部を持つ団体)

米国に本部を持ち、世界 80 カ国以上で著作権の保護を啓蒙・支援している団体。主なソフトウェアベンダーが所属している。近年は、著作権の保護だけでなく、SAM の啓蒙にも力を入れてきており、日本でも SAM の規程・規則の雛型を公開したり、その利用方法についての研修などを行っている。日本では、SAMCon の管理基準・評価基準をベースとした SAM の成熟度評価も独自に行っている。

(5) itSMF (世界各国に支部を持つ団体)

情報システムの運用管理基準 (ITIL®) の普及を目的に英国で設立され、世界 50 カ国以上に支部を持つ非営利法人。ITIL®は、ISO/IEC 20000 のベースとなっている。日本にも itSMF Japan が設立されており、団体会員数は、277 団体 (2009 年 12 月 15 日現在) となっている。書籍も多数出版しており、SAM に関連する書籍も「アプリケーション管理」として出版している。

これまでも、SAM への取り組み手法や求められる状態については、各国の SAM の団体は、独自の基準を発表してきていたが、ISO/IEC 19770-1 の発行後、各国の SAM の団体は、SAM のプロセスをこの規格に習ってきている。先日発行された ISO/IEC 19770-2(ソフトウェアタグ)も合わせ、各国の SAM に関するプロセスやその取り組みは、今後も ISO/IEC 19770 シリーズをベースとしたものになっていくであろう。

1.4. 本ガイドの活用方法

1.4.1. 本ガイドの利用対象者

本ガイドは、過去に SAM の構築に取り組んだもののうまくいかなかった組織、SAM を運用しているがプロセスがうまく回っていない組織、あるいは、SAM をうまく構築し運用できているが、今後の改善策を検討している組織など、実際に SAM に取り組み、その難しさを多少なりとも経験している組織の管理責任者並びに管理担当者を想定し、まとめている。SAM に関し、全くの初心者が本ガイドをそのまま利用することは想定しておらず、SAM に関する基本的な事項は、説明を省いているところも多い。したがって、SAM に初めて取り組もうとする組織が本ガイドを利用する場合には、より有効に本ガイドを利用いただくために、まず、「ソフトウェア資産管理の基礎と実践」(日本規格協会)で、SAM の概要を把握した後、本ガイドに当たることをお勧めしたい。

1.4.2. 本ガイドにおける SAM の基準

本ガイドによる SAM プロセスは以下のものを基準としている(以下、双方を総称して「SAM の基準」という)。

- ・ ISO/IEC 19770-1
- ・「ソフトウェア資産管理基準 Ver.2.0」(特定非営利活動法人ソフトウェア資産管理コンソーシアム)

1.4.2.1. 本ガイドにおける「SAM ができている状態」

本ガイドを読み進めていただく前に、SAM の構築・運用のレベル感を合わせていただくために、本ガイドが SAM の基準を基にどのような管理体制、運用状況を目指して書いているのかを簡単にまとめておきたい。

なお、以下に記載する SAM の体制や規程類は、組織の SAM の目的を十分に果たすものとして策定されることが求められるものである。

本ガイドが想定している SAM ができている状態とは、

- ・ SAM に関する方針及び体制が定められている。
- ・ SAM に関する規程類が策定されている。
- ・ SAM に関する規程類の定めたとおりに運用されている。
- ・ SAM の状況を内外に示すことができる。

の4点である。

以降の章では、これらについて、どのようにすればそれが確実にできるのかについて詳細にそ

の説明をしている。

1.4.2.2. SAM の管理台帳について

本ガイドでは、SAM を運用していくために、管理台帳としてハードウェア管理台帳、導入ソフトウェア台帳、ライセンス管理台帳、ライセンス関連部材管理台帳の四つの台帳を作成することを前提としているが、一般的な SAM の基準では、実施すべき管理方法について明確に述べられている訳ではない。ただし、管理を実現しようするためには通常これらの四つ台帳が必要となるため、本ガイドではこれらの台帳を利用することを前提として解説を行う。

なお、目指すべき管理は組織によって異なるため、台帳の種類、内容はここに示したものだけでなく、組織の管理目的、目標とそれを達成するための管理方法に合わせたものが望まれるものであり、必ずしもここに挙げているとおりでなければいけないというわけではない。

本書で管理台帳を敢えて管理のベースとして記載しているのは、

- ・ SAM の管理対象資産のライフサイクルが個別に異なること
- ・ 対象資産ごとに管理項目が異なること
- ・ 対象資産ごとに運用のプロセスが異なること

など、対象資産ごとに考慮しなければならない管理の枠組みをわかりやすく解説できると考えたからである。

台帳を作成せずとも、1.4.2.1 の SAM ができている状態を実現できれば、もちろんそれでも構わない。

1.4.3. 本ガイドの構成

本ガイドは、組織において SAM を導入し、運用していくためのプロセスを表 1-2 のように大きく四つに分け、解説している。

表 1-2 SAM のプロセス

SAM のマネジメントプロセス	SAM のマネジメントプロセス
	IT 資産のライフサイクルマネジメントにおける SAM
SAM の導入・構築	SAM の導入計画
	SAM の構築プロセス
SAM の運用	SAM の運用上のポイント
SAM ツールの利用	SAM ツール利用のためのポイント

「SAM のマネジメントプロセス」と「IT 資産のライフサイクルマネジメントにおける SAM」では、SAM を他の IT 資産管理のプロセスと融合させ、マネジメントシステムの一つとして構築していくための意識と知識を高め、取り組みを促進することを目的としている。

そして、「SAM の導入計画」、「SAM の構築プロセス」では、実際に SAM を構築する際の注意点やその手順を理解することを、例示を挙げて詳細に解説している。

「SAM の運用上のポイント」では、SAM の構築後、スムーズな運用を実施すること、及び SAM

のメリットを享受し続けるためのプロセスの改善を目的とし、SAM の構築と同じく、実際の運用をイメージできるレベルで詳述している。

また、付録として、実際の SAM の構築や運用の参考になる規程や規則のひな型や参照とすべき規格、基準、団体などを紹介している。

「SAM ツール利用のためのポイント」では、SAM の運用に欠かすことのできない SAM ツールの機能やその選定方法、利用する際の注意事項などをまとめている。

1.4.4. 本ガイドの活用方法

本ガイドは、日本における SAM の専門家が、その知見を惜しみなく提供するものであり、SAM に関する辞典のように、どの章、項目から参照していただいても良いように構成したつもりである。

SAM に関し、実戦的に利用できるように本ガイドは構成しており、SAM の導入部分から読み始めていただいてもかまわないし、自組織にとって弱いと感じているところ、悩んでいるところをつまみ食いのように読んでいただいてもかまわない。また、SAM の取組みに自信を持たれている組織にも本ガイドを読んでいただき、改善の糸口を見出していただければ幸いである。

更に本ガイドの有効性を高めるために、付録に記載している、参考規格・基準や各種団体を並行して利用することをお勧めする。

本ガイドによって、組織の SAM の取組みが向上するだけでなく、以て IT サービスの改善、IT 統制の基盤の強化が実現できることを願うものである。

なお、本ガイドは、SaaS (Software as a Service) や ASP (Application Service Provider) などのように、サーバベースでソフトウェアの機能をクライアント PC やシンクライアントに提供するものは対象としていない。これは、これらのサービスや技術が緒についたばかりであり、ライセンス体系や提供方法も含め、まだまだそれらのパターンが確立されていないからである。本ガイドをご利用いただく際には、ご留意いただきたい。

2. 用語の解説

この章では、SAM（ソフトウェアアセットマネジメント）で使用される用語に関する知識を深め、SAM の理解を深めるための補助を目的にしている。各用語の詳細について理解を深める際には、関係する本章で理解を深め、ここでは全体の概要を把握することを目的にしている。また、各用語はここで定義している内容以外の広範囲な内容を意味する場合もあるが、ここでは、本ガイドの中で利用されている範囲に限定して、定義を解説している。

2.1. ソフトウェア資産管理基準

ソフトウェア資産管理基準は、組織がどのようなソフトウェア資産管理を行うべきかを検討するための指針を示すために、SAMCon が作成したもので Ver.2.0 の時点では、自社開発ソフトウェアと他者からライセンスを受けたソフトウェア及び関連資産を適正に管理するための基準である。

2.2. ソフトウェア資産管理評価規準

ソフトウェア資産管理評価規準（Ver2.0）は、SAMCon が策定したもので、前述のソフトウェア資産管理基準（Ver2.0）の付属の文書として規定された。ソフトウェア資産管理基準（Ver2.0）に基づく成熟度レベルを策定し、管理レベルを段階分けして判断できるようにすることで、適切に管理状態の把握や目標の設定ができるよう考慮されている。

2.3. 情報セキュリティマネジメントシステム（ISMS）

情報セキュリティマネジメントシステム（ISMS：Information Security Management System）とは、個別の問題ごとの技術対策の他に、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、資源を配分して、システムを運用するための仕組みである。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を ISMS の基本コンセプトとしている。

2.4. IT サービスマネジメントシステム（ITSMS）

IT サービスマネジメントシステム（ITSMS：Information Technology Service Management System）とは、IT サービス提供者が、提供するサービスのマネジメントを効率的、効果的に運営管理するための仕組みである。具体的には次のようなことを行い、顧客満足やサービス品質の向上、若しくは費用対効果の増大などの IT サービス提供に関する運用管理上の要求／期待に対応する。

【対顧客】

サービス提供者は、提供のサービスレベルを顧客と合意し、合意に基づいたサービス品質を管理し、サービスレベル状況を顧客に報告する。

【対サービス提供の関連プロセス】

IT サービスマネジメントは、顧客との合意のサービスレベルを含む各種要求を満たすよう、サービス提供の関連プロセスを統制する。

【対供給者】

サービス提供者は、供給者とサービスレベル（顧客合意のサービスレベルとの整合性が条件）を合意し、監視する。

2.5. IT インフラストラクチャーライブラリー (ITIL®)

IT インフラストラクチャーライブラリー (ITIL®: IT Infrastructure Library) とは、IT サービスマネジメントのベストプラクティスで、IT サービスマネジメントのデファクトスタンダード（事実上の標準）と呼ばれている。1980年代から英国で IT サービスを効率的に管理・運用していくための方法論の模索として整理され、実際の IT サービス運用のノウハウなどが集積されたライブラリーで、一連の書籍群から構成されている。

2.6. CMM (Capability Maturity Model)

企業の情報化、管理プロセス、ソフトウェアなどの状態をレベル1から5までの段階で評価する手法（レベル0から始める場合もある）。もともとは、米国で開発され、それを統合して体系化したものが、CMMI (Capability Maturity Model Integration) と呼ばれている。ISO/IEC 15504では、ソフトウェアの開発手法にこの考え方を取り入れており、前述した SAMCon のソフトウェア資産管理評価規準でも、これをベースとし、策定されている。

2.7. COBIT

米国の ISACA (情報システムコントロール協会: Information Systems Audit and Control Association) と ITGI (IT ガバナンス協会: IT Governance Institute) が発行している IT 管理のベストプラクティス集。IT ガバナンスの成熟度を測るための国際的な規格である。

2.8. ISO/IEC 19770

ISO/IEC 19770 は、ソフトウェア資産管理が、IT サービス全体の有効な支援となるよう開発された規格である。現在は、ISO/IEC 19770-1 (ソフトウェア資産管理プロセス) と ISO/IEC 19770-2 (ソフトウェアタグ) の二つの規格が発行されている。

2.9. ソフトウェア

SAM が対象とするソフトウェアとは、実行可能なソフトウェアと非実行可能なソフトウェアの両方を指す。例えば、実行可能なソフトウェアとは、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、ユーティリティープログラムなどが挙げられる。非実行可能なソフトウェアとは、フォント、グラフィック、音声データ、映像データ、テンプレートやマニュアルなどを含む文書類、辞書類、データなどが挙げられる。ISO/IEC 19770-1 では、自社にて開発されたシステムも対象としている。

2.10. ライセンス

本ガイドで扱われるライセンスとは、ソフトウェアの複製権、使用权、アクセス権を指す。使用許諾契約書又は契約書などには、その使用条件が記載されている。

2.11. ハードウェア

ソフトウェアが稼働する又は、稼働することが可能なプラットフォームをいう。例えば、パソコン、サーバ、プリンタ、ルータなど。

2.12. ソフトウェア資産

ソフトウェア資産は、ソフトウェアとライセンスを総称したものをいう。

2.13. IT 資産

本ガイドでいう IT 資産とは、ライセンス、ライセンスされていることを証明するための部材（以下「ライセンス関連部材」という）、ハードウェア、利用導入されているソフトウェアまでを含んだものをいう。ここでいうハードウェアが何を指すかは、組織によって異なるが、例えば、ネットワークケーブル、ルータ、ハブ、パソコン、サーバ、プリンタやコピー機、ファックスなど考えられる。

2.14. IT 資産のライフサイクル

IT のライフサイクルとは、取得・導入・異動・廃却と定義する。

2.15. ライセンス管理

本ガイドでいうライセンス管理とは、主に著作権法、及び使用許諾条件の順守（ライセンスコンプライアンス）を目的とするものをいう。

2.16. ソフトウェア資産管理（SAM）

ソフトウェア資産管理（SAM：Software Asset Management）とは、ライセンスコンプライアンスに加え、情報セキュリティの維持・向上、IT 投資の最適化を目的とするものであり、ライセンス管理よりも広範としている。

2.17. 使用許諾契約（使用許諾書）

ソフトウェア又はライセンス（複製権、使用权、アクセス権）を使用する際の使用条件を定義した契約を指す。ソフトウェアと同時に配布されるもの、事前に確認されるものなどがある。使用条件を記載したドキュメントを使用許諾契約書（EULA: End User License Agreement）という。一般的に使用許諾契約書は、ライセンス保有を証明するものではなく、ライセンスの使用条件を定義しているものが多い。

2.18. ソフトウェア資産管理ツール（SAM ツール）

SAM ツールとは、ソフトウェア資産管理を実施するに当たって業務を効率化するために使わ

れるツールであり、例えば、IT 資産管理ツールや運用管理ツールなどが挙げられる。

2.19. インベントリ

インベントリとは、ハードウェアのスペックやネットワーク情報、並びに、ハードウェア上で導入されているソフトウェアの情報を総称したものをいう。

2.20. 内部監査

内部監査とは、主に組織内部で独立した部門が、その組織の内部統制が有効かつ効率的であるかどうかの合理性や、法律を順守しているかどうかの合法性などの評価・検証を行い、内部統制の改善に関して助言、勧告することなどの業務を指している。組織外部者が実施する外部監査と対比して内部監査と呼ばれている。

2.21. 外部監査

内部監査と対比して、組織外部の部外者が実施する監査のことを呼ぶ。

2.22. 棚卸

棚卸とは、対象資産の使用状況が管理記録と合致しているかどうかを調査し、合致していない場合には、その差分と差分が発生した原因を明らかにし、是正することをいう。

2.23. ソフトウェアの調達

本ガイドでは、ソフトウェアの調達とは外部からライセンスを購入することを指す。賃借（リース・レンタルなど）した PC 上に導入されるライセンスの調達も含まれるが、ライセンスは原則賃借が認められていない。ライセンスに基づく使用許諾は、最終のユーザに与えられる権利であり、ハードウェアの賃借と管理上の扱いが異なるため、注意が必要になる。各ソフトウェアの使用許諾条件を適切に理解しておく必要がある。

2.24. ソフトウェアの導入

ソフトウェアの導入とは、ソフトウェアをコンピュータ上に導入・複製などをして、ハードウェア上で、ソフトウェアが利用できる状態にすることを指す。例えばインストールなど。アクセス権の導入の場合には、単にアクセスできること又はその環境を作ることが含まれる場合がある。

2.25. ソフトウェアの削除

ハードウェアからソフトウェアを削除すること。使用許諾条件上、ソフトウェアを使用していない状態にすること。例えばアンインストールなど。

2.26. ライセンスの利用

ライセンスの利用とは、使用許諾条件上、ソフトウェアを利用している状態にあることを指す。例えば、インストールなど。

2.27. ライセンスの保有

ライセンスの保有とは、ソフトウェアの使用を許諾されている状態を指し、決められた条件で、複製・使用・アクセスできることを指す。ライセンスの保有は、使用許諾条件によって異なるが、一般的には、ライセンス証書・ソフトウェアを含むメディア・ライセンス購入時のパッケージなどで証明できるものが多い。

2.28. ライセンスの廃棄・返却（又は廃却）

ライセンスの廃却とは、ライセンス関連部材を廃棄・返却することを指す。当然ながら、廃棄・返却されたライセンスで使用を許諾されていたソフトウェアは、ライセンスの廃棄・返却後は、ハードウェア上で使用されることがあってはならない。

2.29. スコープ

スコープとは、SAM が対象とする組織と資産の範囲を指す。組織の範囲とは、例えばひとつの法人全体であるのか、関連会社も含むのか、また、一部除外する組織を作るのかなどをいう。資産の範囲とは、どのようなハードウェア・導入ソフトウェア・ライセンスまでを対象とするのかなどをいう。

2.30. IT ガバナンス

IT ガバナンスとは、主に IT 化により新たに生じるリスクの極小化と、的確な投資判断に基づく経営効率の最大化、すなわちリスクマネジメントとパフォーマンスマネジメントであり、これらを実施するに当たっての、健全性確保のためのコンプライアンスマネジメントの確立である。（日本監査協会 IT ガバナンス委員会引用）

2.31. 導入ソフトウェア台帳

導入ソフトウェア台帳とは、ライセンスがどのハードウェアで利用されているか（場合によって誰が利用しているのか）、またどのコンピュータに導入されているかを管理して、それがどのライセンスに基づいて導入されているかなど管理する台帳のことである。

2.32. 保有ライセンス台帳

保有しているライセンスを管理する台帳をいう。どのようなライセンスをどれくらい保有しているかが判別できる。

2.33. ライセンス関連部材

ライセンスを保有していることを証明するために必要な CD や DVD、ライセンス証書などを指す。

2.34. ライセンス関連部材台帳

ライセンス関連部材を管理するための台帳をいう。ソフトウェアメーカーの正規の媒体（CD/DVD など）や、バックアップ用又は作業用に複製が許されている場合には、その複製媒体

も含む。

2.35. ハードウェア台帳

組織内で保有するハードウェアの情報を登録する台帳である。例えば、コンピュータ・ハードディスクなどのドライブ類・サーバ機器などが挙げられる。

2.36. キットティング

ハードウェアを実際に利用可能な状態にセットアップする作業のことを指す。OS のセットアップやネットワークの設定、個別ユーザの設定などを総称したものを指す。

3. SAM のマネジメントプロセス

本章では SAM の PDCA サイクル、すなわち組織内におけるソフトウェア資産の有効な管理、制御及び保護のために必要なマネジメントプロセスについて解説する。また ISMS (Information Security Management System) や ITSMS (IT Service Management System) など他のマネジメントシステムと SAM の比較分析を試みる。

3.1. SAM の PDCA サイクル

「PDCA サイクル」とは業務を改善するための典型的なマネジメントサイクルの一つであり、Plan (計画立案)、Do (導入)、Check (監視及びレビュー)、Act (継続的改善) のプロセスを順番に実施し、次のサイクルの Plan に戻る。これらのプロセスを循環的かつ螺旋的に実施することで、業務の継続的改善を図ろうとする考え方である。

PDCA サイクルは生産管理や品質管理など様々な分野において、業務を計画どおり円滑に進めるための管理手法として採用されている。また ISO 9000 をはじめとするマネジメントシステムの基本的な考え方でもある。以下の各項では SAM の PDCA サイクルにおける、各プロセスの目的と成果について述べる。

3.1.1. Plan (計画立案)

SAM の計画立案プロセスの目的は、SAM の目的を効果的かつ効率的に達成するために、適切な準備と計画立案を確実に行うことである。そのために組織は、まず「SAM の管理目的」を策定し、取締役会 (又は同等の機関) の承認を受ける必要がある。承認された「SAM の管理目的」は、少なくとも年 1 回は見直すことが望ましい。

続いて SAM を導入し実行するための計画 (以下、「SAM 計画」という。) を立案する。ここではまず管理対象とするソフトウェア及び関連資産などの範囲を明確にした上で、対象資産の管理方針、管理プロセス、管理手順を規定し、文書化する必要がある。SAM の監査手順書、リスク評価手順書、管理状況報告書 (様式)、SAM の導入に必要な予算計画書なども必要となる。SAM の達成度を追跡調査するための「パフォーマンス指標」もあらかじめ定めておくことが望ましい。

これらの文書を含む「SAM 計画」も前述の「SAM の管理目的」と同様、取締役会 (又は同等の機関) の承認を受ける必要がある。承認された「SAM 計画」は、少なくとも年 1 回は見直すことが望ましい。

3.1.2. Do (導入)

SAM の導入プロセスの目的は、前項で定めた「SAM 計画」を確実に実行し、「SAM の管理目的」を達成することである。そのために組織の SAM 管理責任者は、まず SAM 計画に影響する変更や問題及びリスクに関する情報を各部門の SAM 管理責任者から収集するための仕組みを整備する必要がある。そしてこの仕組みは年間を通じて機能するものでなければならない。組織の SAM 管理責任者は SAM 計画の進捗状況については、少なくとも四半期に 1 回は取締役会 (又は同等の機関) に報告することが望ましい。

計画と進捗状況に何らかの不一致があった場合は速やかに追跡調査を実施し、調査結果を文書で報告する。SAM 計画が確実に実施されるように必要な資源を確保し、ツールを導入することも、本プロセスの責任範囲に含まれる。

3.1.3. Check（監視及びレビュー）

本プロセスの目的は、「SAM の管理目的」が達成されていることを定期的を確認することである。そのために、組織の SAM 管理責任者は SAM の施策に対する正式なレビューが少なくとも年 1 回実施されるための仕組みを整備する必要がある。レビューの例は以下のとおりである。

- ① SAM の管理目的及び SAM 計画が達成されているかどうか。
- ② SAM に関して経営陣が承認した方針、プロセス及び手順が、定義された組織の全範囲に周知され、導入されているかどうか。
- ③ 規程に対する違反事項があったかどうか。
- ④ SAM の仕組みを改善する機会があったかどうか。
- ⑤ 継続的なレビューを行う必要性があるかどうか。

組織の SAM 管理責任者は、このレビューに関する報告書を正式に承認し、今後組織が行うべき意思決定と、取るべき行動を文書化し、取締役会（又は同等の機関）に報告する必要がある。また費用対効果が最大になるようにソフトウェア及び関連資産が展開されているかどうかに関しても定期的なレビューと改善勧告が行われるように規定する必要がある。

3.1.4. Act（継続的改善）

本プロセスの目的は、ソフトウェア及び関連資産の使用方法和 SAM プロセスの両方に関して改善の機会を特定し、それが妥当と考えられる場合は確実に改善が実施されるようにすることである。

この目的を達成するために、組織の SAM 管理責任者は、年間を通じてあらゆる発信源から寄せられる SAM の改善案を収集し記録する仕組みを整備する必要がある。そして、改善案が定期的に評価され、優先度が定められ、正式に承認された上で次期の SAM 計画に取り込まれるように規定する必要がある。

3.2. 他のマネジメントシステムとの関連

本項では ISMS や ITSMS など他のマネジメントシステムと SAM の内容を比較分析することで SAM の特徴を明らかにする。

3.2.1. ISMS

ISMS の目的は、組織が保護すべき情報資産について機密性、完全性、可用性をバランスよく維持することである。組織が ISMS を有効に機能させるためには、リスクアセスメントにより保護すべき情報資産ごとに必要なセキュリティレベルを定め、計画的にセキュリティシステムを運営管理する必要がある。

情報セキュリティに関連する組織の様々なプロセスに対して「PDCA サイクル」を適用するこ

とで、情報資産の機密性、完全性、可用性に関する要求事項をバランスよく達成することが可能となる。ISMS における PDCA モデルを以下に示す。

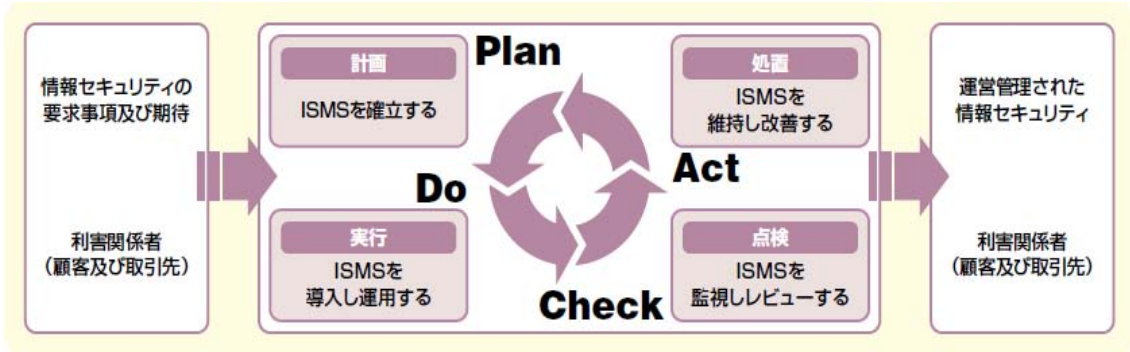


図 3-1 ISMS における PDCA モデル

3.2.2. ITSMS

ITSMS の目的は、組織が提供する IT サービスについて、多様な利害関係者の満足度をバランスよく保ちつつ運営管理することである。組織が ITSMS を有効に機能させるためには、経営陣のコミットメント、各構成員の責任と役割の明確化、プロセスごとのインプットとアウトプットの明確化、各プロセスの重要業績評価指標（KPI）の設定と測定などが必要となる。

IT サービスに関連する組織の様々なプロセスに対して「PDCA サイクル」を適用することで、顧客をはじめとする多様な利害関係者の満足度をバランスよく達成することが可能となる。ITSMS における PDCA モデルを以下に示す。

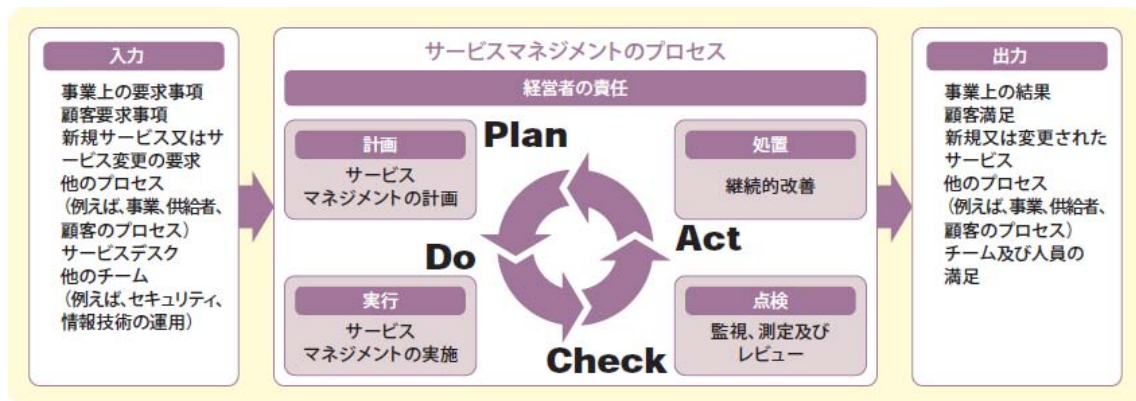


図 3-2 ITSMS における PDCA モデル

3.2.3. 各マネジメントシステムの比較と相互関係

SAM、ISMS、ITSMS の各マネジメントシステムは、基本的には PDCA サイクルに沿った継続的な改善活動であるという点は共通しているが、それぞれの目的、対象資産、利害関係者の範囲、想定されるリスクなどにおいて相応の違いがある。各マネジメントシステムの特徴を明らかにするために、PDCA 比較表（表 3-1）及びインプットアウトプット比較表（表 3-2）を以下に示す。

表 3-1 各マネジメントシステムの PDCA 比較表

	SAM	ISMS	ITSMS
Plan (計画立案)	SAM の管理目的を検討、策定、提案し、取締役会などによる承認を受ける。 管理対象とするソフトウェア及び関連資産の範囲を明確にし、管理方針、管理プロセス、管理手順を規定する。	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。	サービスマネジメントの導入・実施について計画する。
Do (導入)	SAM 計画に影響する情報を収集する仕組みを整備し、計画の進捗状況を取締役会などに報告する。	ISMS 基本方針、管理策、プロセス及び手順を導入し運用する。	サービスマネジメントの目的及び計画を実施する。
Check (監視及びレビュー)	SAM の施策に対するレビューを行い、取締役会などに報告する。また費用対効果が最大となるようにソフトウェア及び関連資産の展開状況に関するレビューも行う。	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。	サービスマネジメントの目的及び計画の達成を、監視、測定及びレビューする。
Act (継続的改善)	ソフトウェア及び関連資産の使用、並びに SAM プロセスの改善機会が特定され、実施されるように、SAM の改善案を収集、記録、評価し、次期計画に取り込む。	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。	サービスの提供及び運営管理の有効性及び効率を改善する。

表 3-2 各マネジメントシステムのインプット、アウトプット比較表

	SAM	ISMS	ITSMS
インプット	取締役会及び取引先（特にソフトウェア購入先）からのソフトウェア資産管理に関する要求事項及び期待	顧客・取引先からの情報セキュリティに関する要求事項及び期待	ITの利用者によるサービス品質に関する要求事項及び期待
アウトプット	適切に運営管理されたソフトウェア資産管理活動による、在庫管理と購買管理の有効性、効率性及び適法性の確保	適切に運営管理された情報セキュリティ活動による、情報資産の機密性、完全性、可用性の確保	適切に運営管理されたITサービスの提供による、顧客、供給者、関連プロセス、関連チーム及び人員の満足度の確保

次に一つの試みとして「経済産業省 システム管理基準（追補版）第IV章」に基づき、IT全般統制に必要な業務範囲を定義し、これに対するSAM、ISMS、ITSMSの各マネジメントシステムのカバー範囲を分析したところ、以下の点が明らかになった。（表 3-3 参照）

- ・ 「経済産業省 システム管理基準（追補版）第IV章」によると、IT全般統制の統制目標は「情報システムのソフトウェアの開発と調達」「システムの運用・管理」「内外からのアクセス管理などのシステムの安全性の確保」「委託先の管理」の4分野、13項目に分類されている。
- ・ 第一の「情報システムのソフトウェアの開発と調達」分野については、SAM、ISMS、ITSMSのいずれも、本領域を主たる領域とするマネジメントシステムではない。（各マネジメントシステム本来の目的達成のため、付随的にソフトウェアの開発と調達に言及した部分は存在する。）したがってこの分野については、組織ごとに定められたシステム開発標準などに依存せざるを得ないと考えられる。
- ・ 第二の「システムの運用・管理」及び第四の「委託先の管理」分野については、ITSMSが主たる領域としてカバーしている。
- ・ 第三の「内外からのアクセス管理などのシステムの安全性の確保」分野については、ISMSが主たる領域としてカバーしている。
- ・ SAMは、ソフトウェア資産に関する調達管理、変更管理、運用管理、構成管理などを部分的にカバーしている。

表 3-3 IT 全般統制に関する「統制目標」の分類

IT全般統制の統制目標の分類 (システム管理基準 追補版 第IV章より)	
3.1 情報システムのソフトウェアの開発・調達	3.1.1 システムの開発・調達
	3.1.2 IT基盤の構築
	3.1.3 変更管理
	3.1.4 テスト
	3.1.5 開発・保守に関する手続の策定と保守
3.2 システムの運用・管理	3.2.1 運用管理
	3.2.2 構成管理
	3.2.3 データ管理
3.3 内外からのアクセス管理等のシステムの安全性の確保	3.3.1 情報セキュリティフレームワーク
	3.3.2 アクセス管理等のセキュリティ対策
	3.3.3 情報セキュリティインシデントの管理
3.4 委託先の管理	3.4.1 委託先との契約
	3.4.2 委託先とのサービスレベルの定義と管理

このように IT 全般統制全体を包括的にカバーするマネジメントシステムは存在しないのだが、昨今の SaaS/PaaS やクラウドコンピューティングの普及を前提に考えると、IT は今後益々「構築するもの」から「利用するもの」へと急速に変貌していくと予想される。このような環境下においては、IT の品質管理手法を提供する ITSMS が統括的マネジメントシステムとしての重要性を高められると思われる。そして ISMS は情報セキュリティ領域において、また SAM はソフトウェア資産管理領域においてそれぞれ ITSMS を適切に補完し、IT サービス全体の品質管理を実現していくことになるであろう (図 3-3)。

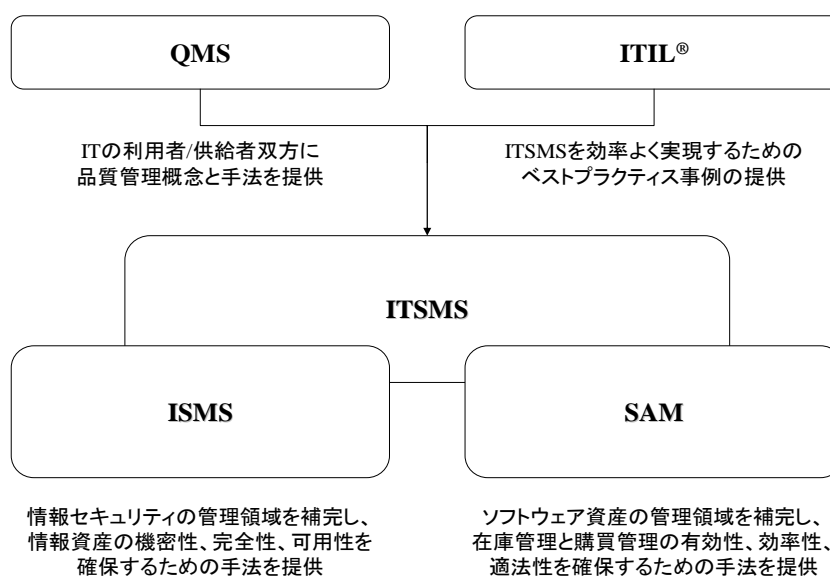


図 3-3 各マネジメントシステムの相互関係

4. IT 資産のライフサイクルプロセスと SAM

本章では、ソフトウェア及び関連資産のライフサイクルプロセスを、取得、導入、異動、廃却の4段階に分けて解説する（表 4-1）。

表 4-1 ソフトウェア及び関連資産のライフサイクルプロセス

段階	名称	本章における定義
1	取得	組織が事業を行うために必要なソフトウェア及び関連資産を購入・賃借などの手段により用意すること、又は社内開発により用意すること。
2	導入	取得したソフトウェア及び関連資産がシステムとして適切に組み込まれ、使用可能な状態になること。
3	異動	導入したソフトウェア及び関連資産の属性（所有者・利用者・設置場所など）が変更されること。
4	廃却	所有していたソフトウェア及び関連資産を不用品として廃棄すること、又は賃借していたソフトウェア及び関連資産を返却すること。

4.1. 取得

4.1.1. 取得の定義

「取得」とは、あるものを入手して利用できる状態にすることである。SAM のライフサイクルプロセスにおける「取得」とは、組織が事業を行うために必要なソフトウェア及び関連資産を、組織の外部から購入・賃借などの手段により用意すること、又は社内開発により用意することを意味する。一方「取得」と似た意味で「調達」という用語も世の中では広く用いられているが（政府調達、調達仕様書など）、いずれも本来は一般用語なので用法の厳密な区別は難しい。

本稿では混乱回避のために、「取得」を一旦「調達」と「社内開発」に分け、ソフトウェア及び関連資産を用意するプロセス全体について述べる場合は「取得」を用い、外部購入について述べる場合は「調達」を用いることとする。またソフトウェア及び関連資産の取得目的については、特に断わった場合を除き「自社使用」のみを検討対象とし、「外部販売用」の仕入れについては検討対象外とする。

4.1.2. 取得プロセスの目的と範囲

ISO/IEC 19770-1 によると、このプロセスは“ソフトウェア及び関連資産が制御された方法で取得され、適正に記録されることを確実にすること”を目的とする。そして、このプロセスの導入によって、組織は以下の成果が期待できる。

- a) ソフトウェアサービスの提供に関する標準アーキテクチャの定義。
- b) 標準ソフトウェア構成の定義。
- c) ソフトウェア及び関連資産の取得要求及び発注に関する方針及び手順の策定と、適正な認可及び発行。
- d) ソフトウェア及び関連資産の受領処理に関する方針及び手順の策定、適正な認可及び発行。

(箇条 4.7.3 「取得プロセス」 参照)

すなわち、本プロセスの導入組織は、ソフトウェアサービスの品質基準が定められることによる安心感が得られ、また標準ソフトウェア構成が定められることによるサポートの省力化やロット購入のメリットを享受することができると考えられる。以下の各項では、取得プロセスの中で特に重要なポイントについて解説する。

4.1.3. 調達プロセスの内容

前述のように、世の中の一般用語としては「取得」より「調達」の方がポピュラーである。本項では、特にソフトウェア及び関連資産の外部購入（「調達」）を対象を絞り、「標準的な調達プロセス」に必要な項目について検討する。

具体例として、「情報システムに係る政府調達の基本方針」（2007年3月1日 各府省情報化統括責任者連絡会議決定。以下、「政府調達基本方針」という。）を取り上げる。この基本方針に従うと、調達プロセスは「企画、入札、契約、実作業、検収」という5段階に分けられる（表 4-2）。

表 4-2 政府調達プロセスの標準構成

段階	業務内容
1. 企画	1.1 調達計画書の作成（必要に応じて情報提供要請（RFI：Request for Information）を行う） 1.2 調達計画書の決定・公表
2. 入札	2.1 調達仕様書案の作成 2.2 意見召集 2.3 調達仕様書の決定 2.4 入札公告 2.5 提案依頼（RFP：Request for Proposal） 2.6 提案受付
3. 契約	3.1 審査 3.2 落札者の決定 3.3 落札者の公告（不落者への通知を含む） 3.4 契約
4. 実作業	
5. 検収	

第1の「企画」段階では、調達計画書を作成し、公表する。第2の「入札」段階では、「調達仕様書」を作成・公表し、入札公告を出し、提案依頼（RFP）を受け付ける。第3の「契約」段階では取引先の審査を行い、落札者を決定し、契約を行う。その後納品（実作業）、検収が行われる。

続いて、調達プロセスの中でも特に重要な「調達仕様書の作成」、「調達コストの最適化」、「仕様許諾条件の確認」、「発注の処理」の各業務における留意事項について考察する。

4.1.4. 調達仕様書の作成

調達仕様書とは入札段階で応札者のために作成する文書であり、調達件名、作業内容、情報システムの要件などを詳しく記載したものである。調達仕様書作成の留意事項は以下のとおりである。(表 4-3「政府調達基本方針 別紙3 調達仕様書に記載する事項」参照)

(1) 提案に不可欠な情報の網羅

現行システムの状況を知っている既存事業者が有利になる可能性を排除するため、提案に不可欠な情報を網羅していること。

(2) 曖昧な要求要件の排除

業務情報を多く知っている事業者には有利な調達仕様書になっていないこと。また一般の事業者が入札に際してリスクを感じないように、具体的な要求要件を第三者にも分かりやすく記載していること。

(3) オープンな標準に基づく要件の記載

業務名称とその詳細、データの入出力及びその関係などを記載していること。また特定技術・製品を前提とした要件になっていないこと。

(4) 技術革新などを踏まえた要件の記載

技術的な制約を与えない内容となっていること。

(5) 調達仕様書の妥当性確認など

CIO 補佐官（民間組織の場合は CIO など）が調達仕様書の妥当性を確認していること。

(6) 電子入札・開札の推進

談合などの不正行為の防止に一定の効果が期待される電子入札システムを活用していること。（民間組織の場合は、本項目は不要。）

表 4-3 「調達仕様書に記載する事項」

章・節のタイトル	内容
表紙	調達件名、年月日、発行元
1. 調達件名	情報システムに係る工程名を記載
2. 作業の概要	
(1) 目的	情報システム導入の目的を入札希望者に理解可能な平易な文章で記載。
(2) 用語の定義	固有の用語、読み手により複数の解釈が可能な専門用語などの意味を記載。
(3) 業務の概要	導入する情報システムに係る業務の全体像（業務一覧な

(4) 情報システム化の範囲 (5) 作業内容・納入成果物	ど) を具体的かつ詳細に記載。 業務のうち、実際に情報システム化する範囲を記載。 受注者側の作業、納入成果物を記載。
3. 情報システムの要件 (1) 機能要件 (2) 画面要件 (3) 帳票要件 (4) 情報・データ要件 (5) 外部インタフェース要件	対象機能の一覧と要求事項を記載。 画面の一覧と要求事項を記載。 帳票の一覧と要求事項を記載。 構築する情報システムで取り扱う情報やデータを蓄積・利用する場合は、その蓄積・利用のイメージ、業務処理要件、タイミングなどを記載。 他の情報システムとの連携（データの入手、データの提供）が必要な場合は、その相手先、やり取りするデータ、受け渡し条件などを記載。
4. 規模・性能要件 (1) 規模要件 (2) 性能要件	構築する情報システムの規模について記載。 構築する情報システムの性能について記載。
5. 信頼性等要件 (1) 信頼性要件 (2) 拡張性要件 (3) 上位互換性要件 (4) システム中立性要件 (5) 事業継続性要件	構築する情報システムに求める信頼性について記載。 構築する情報システムの求める拡張性について記載。 構築する情報システムの求める OS、ミドルウェアなどの上位互換性について記載。 構築する情報システムが提案者などの特定事業者依存しておらず、他の者に引き継ぐことが可能であることの説明を記載。 情報システムの更新時において、データ移行が円滑に実施可能であることの説明を記載。 通常災害時や故障時においても事業を継続することが可能であることの説明を記載。
6. 情報セキュリティ要件 (1) 権限要件 (2) 情報セキュリティ対策要件	利用者、情報システム管理者などの権限を処理機能別に定義。 各組織の情報セキュリティポリシーなどにおいて要求されている事項及び情報資産のリスクを十分に勘案した上で、各情報資産の重要度及びリスクに応じた対策を定義。
7. 情報システム稼働環境 (1) 全体構成 (2) ハードウェア構成	構築する情報システムが稼働するハードウェア、ソフトウェア、ネットワークなどの環境全体の構成図を記載。 構築する情報システムを稼働させるハードウェアについ

(3) ソフトウェア構成	て記載。 構築する情報システムを稼働させるソフトウェアについて記載。
(4) ネットワーク環境	構築する情報システムを稼働させるネットワークについて記載。
(5) アクセシビリティ要件	構築する情報システムに求めるバリアフリー機能、多言語対応などについて記載。
8. テスト要件定義	要求要件に適合しているか検証するためのテストに係る要件を定義。
9. 移行要件定義 (1) 移行に係る要件 (2) 教育に係る要件	次期情報システムへの移行を円滑に遂行するための現行情報資産の継続性を担保するための要件を定義。 業務担当者、運用担当者に対する新業務フロー、情報システムの操作性などの教育訓練に関する要件を定義する。
10. 運用要件定義 (1) 情報システムの操作・監視等要件 (2) データ管理要件 (3) 運用施設・設備要件	情報システムの操作、監視などに係る要件を定義。 電子媒体により管理するデータの要件を定義。 当該情報システムのサーバ、周辺機器などを設置する運用施設の要件を情報資産の重要度に応じて定義。
11. 保守要件定義 (1) ソフトウェア保守要件 (2) ハードウェア保守要件	業務処理ソフトウェア、OS、ミドルウェアなど、ソフトウェアに係る要件を定義。 サーバ、サーバ周辺機器、ネットワーク機器など、ハードウェアに関する保守要件を定義。
12. 作業の体制及び方法 (1) 作業体制 (2) 開発方法 (3) 導入 (4) 瑕疵担保責任	情報システムの開発体制に関する要求事項を記載。(要求する人材の要件、人数、役割など) 情報システムの開発方法に関する要求事項を記載。 開発した情報システムを本稼働させるために必要となる作業について記載。 開発した情報システムの瑕疵担保責任の期間や内容について記載。
13 特記事項	特記事項があれば記載。
14 妥当性証明	本調達仕様書が妥当であることを確認した者の氏名を記載。(民間組織の場合は不要と思われる。)

(出典：「情報システムに係る政府調達の基本方針」を一部改変して転載)

4.1.5. 調達コストの最適化

次に調達コストの最適化について検討する。調達コストの引き下げには、ソフトウェア調達価格の引き下げ、余剰ライセンスコストの削減、管理コストの適正化という三つの方向から総合的に検討することが効果的である。

(1) ソフトウェア調達価格の引き下げ

第一に、ソフトウェアの調達価格そのものを引き下げる方策を検討する。調達価格の引き下げはソフトウェアベンダーとの価格交渉の場で検討されることになるが、その際ユーザー側による「優越的地位の乱用」に当たらないように注意する必要がある。できればユーザー側／ベンダー側双方にメリットが期待できるような施策が最も望ましい。

具体的には、調達窓口の一本化による調達ロットの大口化が考えられる。調達窓口の一本化により、ユーザー側は組織全体の調達実績をタイムリーに把握できるため、その情報に基づきベンダー側と価格交渉に臨むことができる。一方、調達窓口の一本化はベンダー側にとっても営業コストの削減などのメリットが期待できるため、ボリュームディスカウント（割引）などの特典を用意しているベンダーが多い。あるいは年間調達額が一定以上に達したユーザーには調達実績に応じて代金の減額や割戻しを行う場合もある。

これに対して組織内の各部門がそれぞれ調達権限を有し、各部門の調達実績を集約する仕組みがない場合は、組織全体での調達実績がタイムリーに把握することが難しい。そのため複数部門がお互いに知らずに同じソフトウェアを調達し、結果的に余剰ソフトウェアライセンスが増えてしまうという事態を招きやすい。組織全体で調達窓口を一本化することにより、このような事態を回避し、ベンダー側と合法的かつ効果的な価格交渉を行うことができる。

(2) 余剰ライセンスコストの削減

第二に、組織内の余剰ライセンスを合理的に削減する方策を検討する。前述のように、組織内の各部門に調達権限を持たせると、各部門がお互いに知らずに同一ソフトウェアを調達するか、又は各部門がそれぞれ少しずつ余裕を持って在庫を確保するため、組織全体としてはかなりの量の余剰在庫を抱える事態を招きやすい。そこで各部門からのソフトウェア購入申請書を SAM 管理責任部門が一括審査することで、ある部門の余剰ソフトウェアを他部門の不足分に充当することが可能となる。

このように「調達窓口の一本化」は、調達ロットの大口化による価格の引下げと、ライセンスの一元管理による余剰ソフトウェア在庫の抑制という二重の効果が期待できる。しかしながら組織の予算管理体系や組織風土の問題により、調達窓口を一本化できないこともありうる。そのような場合であっても、事後的にソフトウェア購入申請書を SAM 管理責任部門に集約して、せめて余剰ソフトウェアを不足部門に充当できるような仕組みは構築しておくべきである。

(3) 保守契約の絞込み

第三に、ソフトウェア及び関連資産の維持・管理コストを削減する方策を検討する。ソフトウェアベンダーの保守契約はサービス一式のパッケージになっている場合が多い。一方、保守サービスの対象システムには、可用性・サービス継続性要求の高いミッションクリティカルなシステ

ムと、それほどでもない一般的なシステムの両方が混在している。保守契約を締結する際には、ベンダーに任せの方が効果的な業務と自社で実施可能な業務に切り分けて、「本当に必要な保守サービス」に絞り込んで契約を締結することで、維持・管理コストの引き下げが可能となる。

4.1.6. ソフトウェア使用許諾条件の順守

次に、ソフトウェア使用許諾条件の順守について検討する。本件は使用許諾契約に関わる法的要求事項なので、これを順守しないことのリスクは非常に大きい。罰金の支払いによる金銭的被害に止まらず、企業のレピュテーション（世間の評判）を著しく低下させ、最悪の場合は企業の存続そのものが脅かされる危険性すらある。

ISO/IEC 19770-1によると、このプロセスは“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、かつ、契約条件に従って使用することを確実にすること”を目的とする。そして、このプロセスの導入によって、組織は以下の成果が期待できる。

- a) 本プロセスに関する手順の策定と、承認及び発行。
- b) 保有有効ライセンス数と使用許諾契約の照合作業を少なくとも四半期に1回実施。
- c) ここで識別された不一致の適切な記録、原因究明、追跡措置の実行。
- d) 以上の結果として、使用許諾条件に係るコンプライアンスリスクが低減されること。

（箇条 4.5.3「ソフトウェア仕様許諾条件の順守」参照）

4.1.7. 発注の処理

続けて、ソフトウェア及び関連資産の発注の処理について検討するが、基本的に発注処理は各組織の購買管理規程などに基づき適切に処理されるべきである。

なお、購買管理規程を策定する際には、以下の精神に基づくことが望ましい。

- a) 法の順守：関係法令を順守し、その精神を尊重すること。
- b) 経済合理性に基づく公正な取引：自由競争を尊重するとともに、個々の取引は経済合理性に基づいて行うこと。
- c) パートナーシップの構築：取引先との相互理解と信頼関係の維持向上に努めること。また取引先の適格性を定期的に見直すこと。
- d) 資源保護、環境保全などへの配慮：資源保護、環境保全などに十分配慮した発注を行うとともに、取引先の選定においても同様の配慮を求めること。
- e) 機密保持：取引を通じて知り得た取引先の機密などの情報を厳格に管理し、許容された目的以外には使用しないとともに、取引先にも同様の管理を求めること。

4.1.8. 納品処理

続いて受領の処理（納品処理）について検討する。ソフトウェア及び関連資産がベンダーから納品された場合には、「受領物の確認」、「ライセンス証書などの保管」、「複製物の作成と管理」、「ベンダーからの請求への支払い」などの一連の処理が必要となる。各処理に関する留意事項は以下のとおりである。

(1) 受領物の確認

ソフトウェア及び関連資産が納品された場合、まず受領物の内容が発注内容と一致していることを確認する。そのためには、組織内におけるソフトウェアの納品処理が SAM 管理責任部門に一元化されていることが望ましい。この時、ライセンス管理台帳を更新することで、新しいソフトウェアを適切に記録することができる。

(2) 保管

ソフトウェアのインストール完了後は、すべての関連部材（ライセンス証書、マニュアル、インストール媒体など）を安全な保管場所に保管し、委任された一つの部門がこれを適切に管理する。またソフトウェアのインストールを行った場合、導入ソフトウェア管理台帳、ライセンス管理台帳も忘れずに更新する。

(3) 複製物とオリジナルの管理

一般的な商業ソフトウェアの場合、契約及びマニュアルに許諾された範囲で複製物の作成ができる場合がある。ただし、ソフトウェアないしその複製物の全部又は一部について、その名目の如何を問わず、第三者に譲渡、賃貸その他その所有若しくは占有を移転する行為をし、若しくは第三者に使用させてはならないものと定められている場合が多い。また、組織はこの契約上の地位を第三者に譲渡することはできない。

ソフトウェアの複製物は目に見えないため増殖しやすいので注意が必要である。組織は複製物とオリジナルを明確に識別した上で、許諾された条件を厳格に解釈し、適切に管理すべきである。

(4) ベンダーからの請求に対する支払い

請求に対する支払は、各組織の「購買管理規程」などにに基づき適正に処理する。一般に支払処理においては以下の点に留意する必要がある。

- a) 納品：購入物品などが納入されたときには納入された物品が購入仕様を満足しているかどうか契約条件に従い検査を行うこと。
- b) 検収：検査に合格した場合には検収完了とし、代金の請求書を受領し、契約条件に従い支払いを行うこと。
- c) 支払：組織が定めた部署においてのみ支払いを実施する。支払い部署を一元化するか、又は部署ごとに支払うかは、組織のポリシーに従うこと。
- d) 下請法順守：購入先の資本金規模と取引内容が下請代金支払遅延等防止法（下請法）の適用対象となる可能性がある場合は、法の定めるところに従い適切に支払期日を定めること。

4.1.9. 社内開発によるソフトウェア及び関連資産の取得

最後に、ソフトウェア及び関連資産を「社内開発」により取得する場合について検討する。ISO/IEC 19770-1によると、ソフトウェア開発プロセスは、“ソフトウェア及び関連資産が、SAM 要求事項を考慮して開発されることを確実にすること”を目的とする。そして、このプロセスの導入によって、組織は以下の成果が期待できる。

- a) ソフトウェア開発に関する標準アーキテクチャの定義。
- b) 標準ソフトウェア構成の定義。
- c) 使用許諾契約からの制約と依存関係に関する考慮。
- d) 以上を備えた正式なソフトウェア開発プロセスの整備。

(箇条 4.7.4 「ソフトウェア開発プロセス」 参照)

4.2. 導入

「導入」とは、あるものを導き入れて何かを実行することや実現させることである。SAM のライフサイクルプロセスにおける「導入」とは、OS やデバイスドライバなどのソフトウェアやオプションのハードウェアなどの IT 資産をコンピュータに組み込んで使用可能な状態にすることを意味する。

ISO/IEC 19770-1 では、SAM の導入プロセスを「ソフトウェアリリース管理プロセス」と「ソフトウェア展開プロセス」に分けて記述しているため、本稿もこの分類に従う。両プロセスの要求事項並びに実行時の留意事項は以下のとおりである。

4.2.1. ソフトウェアリリース管理プロセス

ISO/IEC 19770-1 によると、このプロセスは“SAM 要求事項を支援するようにしてリリースが計画され、確実に実行されること”を目的とする。そして、このプロセスの導入によって、組織は以下の成果が期待できる。

- a) すべてのリリース案のテスト環境の準備。
- b) (セキュリティパッチを含む) リリースの頻度や種類が、計画され、企業と顧客の間で合意されていること。
- c) 予定のリリース期日や成果物が、関連する変更要求や問題を参照に記録され、インシデント管理に伝達されること。
- d) ソフトウェア及び関連資産のリリースが担当の管理者によって承認されること。
- e) リリースの成否が記録され、定期的なレビューを受けること。
- f) 以上の結果として、正式なリリース管理プロセスが整備されること。

(箇条 4.7.5 「ソフトウェアリリース管理プロセス」 参照)

このプロセスの留意点は、リリース前テストを確実に実施することである。新しいソフトウェアのリリースを行う際には、SAM 管理責任部門がリリースする前に必ずテストを行うことが望ましい。テストを行わないと情報セキュリティ事故や互換性の問題が発生する可能性がある。パッチやウイルス対策ソフトの更新モジュールも同様に扱う必要がある。

4.2.2. ソフトウェア展開プロセス

ISO/IEC 19770-1 によると、このプロセスは“SAM 要求事項を支援するようにして、ソフトウェアの展開及び再展開が実施されることを確実にすること”を目的としている。そして、このプロセスの導入によって、組織は以下の成果が期待できる。

- a) ソフトウェア及び関連資産の配付が担当の管理者によって承認されること。

- b) 展開が成功しない場合、どの展開についてもリリース前の状態に戻す手順又は改善方法があること。
- c) 配付されるソフトウェアへの過大なアクセス及びインストール後を含めた、セキュリティ要求事項が順守されること。
- d) 関連するソフトウェア及び関連資産の状態の変更が、資産の管財権の変更及びこの変更について記録する監査証跡を含めて、正確に、適時に記録されること。(本項目は次項「異動」にも関連する。)
- e) 展開されたものが、展開の認可を得たものと同じであることを検証するための、文書化された管理策があること。
- f) 展開の成否が記録され、定期的にレビューを受けること。
- g) 以上の結果として、組織のソフトウェアの配付及びインストールに関する正式な方針及び手順が策定され、承認され、発行されること。

(箇条 4.7.5 「ソフトウェア展開プロセス」 参照)

ソフトウェアの配付は、業務に支障なく、しかも効率的に行う必要がある。仮に各部門の担当者が各々ばらばらにアプリケーション配付やパッチ適用を行うと、適用ミスや適用漏れが発生する恐れがある。そこであらかじめ全社統一の展開方法を策定し、それに沿ったアプリケーション配付やパッチ適用を行う必要がある。したがって、展開方法を策定する際には以下の点に留意する必要がある。

(1) 統一されたインストールポリシーの適用

ソフトウェアのインストールは一つの部門が社内すべてのソフトウェアの導入を担当し、統一されたインストールポリシーを適用することが望ましい。すべての利用者がこのポリシーを確実に入手できるようにするとともに、違反した場合の罰則規定などを盛り込むことが効果的である。

(2) 業務に支障のない配付計画の立案

業務に支障のない配付を行うために、業務時間外の一斉配付を検討するなど、綿密な展開計画の策定が必要である。

(3) 工数をかけない配付方法の検討

更新対象のシステムがネットワークに接続されていれば、ソフトウェア資産のリアルタイム配付ツールを導入することも効果的である。その際、必要に応じて任意の世代を適用するための「世代管理機能」が備わっていることが望ましい。またソフトウェア資産の配付・適用タイミングを指示する「スケジューリング管理機能」も備わっていれば、なお望ましい。

(4) ソフトウェア資産の一括管理による適用ミス、適用漏れの防止

更新対象のシステムに配付したソフトウェア資産の配付・適用状態を一括管理できることが望ましい。また各システムにおけるインストールの成功/失敗や、インストール状態(転送済み・スケジュール中・適用中・適用完了)が管理可能であることが望ましい。具体的には、配付ツ

ルの GUI 機能などを利用して、各サーバ、各 PC の更新状況、バージョン情報などを把握できるようにする。また更新対象のシステムはグループ化して管理できることが望ましい。

なお、事前に十分な対策を取ったとしてもソフトウェアの適用ミスを中心に防止することは困難である。そこで適用ミスがあった場合に備えて、元の状態に戻す方法、又は修正する方法について、事前に計画しておく必要がある。

4.3. 異動

「異動」とは一般的に、地位や身分、職務、所属部署などが変わることを意味する。SAM のライフサイクルプロセスにおける「異動」とは、導入したソフトウェア及び関連資産の属性（所有者・利用者・設置場所など）が変更されることである。なお、ISO/IEC 19770-1 の中では、SAM の異動プロセスは変更管理プロセスと一部ソフトウェア展開プロセスの中で記述されている。

4.3.1. 変更管理プロセス

ISO/IEC 19770-1 によると、このプロセスは、“SAM に影響するすべての変更が、制御された方法で評価され、承認され、実施され、レビューが行われて、すべての記録保持の要求事項を満たすこと”を目的とする。そして、このプロセスの導入によって、組織は以下の成果が期待できる。

- a) ソフトウェア及び関連資産、サービス、SAM プロセスに影響するすべての変更要求の特定と記録が行われること。
- b) ソフトウェア及び関連資産、サービス、SAM プロセスに影響するすべての変更要求の影響評価と優先付けと正式な承認が行われること。
- c) 正式に承認された変更のみが実施されること。
- d) ソフトウェア及び関連資産、サービス、SAM プロセスに影響するすべての変更が記録されること。
- e) このような変更の成否が文書化され、定期的にレビューされること。
- f) 以上の結果として、正式な変更管理のプロセスが整備されること。

（箇条 4.7.2 「変更管理プロセス」参照）

4.3.2. ソフトウェア展開プロセス

このプロセスの「異動」に関連する部分を再掲する。このプロセスの導入によって、組織は以下の成果が期待できる。

- a) 関連するソフトウェア及び関連資産の状態の変更が、資産の管財権の変更及びこの変更について記録する監査証拠を含めて、正確に、適時に記録されること。

（箇条 4.7.5 「ソフトウェア展開プロセス」参照）

4.3.3. 異動時の留意事項

(1) 所有者・利用者の異動を伴う場合

ソフトウェア及び関連資産の所有者・利用者の異動が発生した場合は、ハードウェア管理台帳と、必要に応じてライセンス管理台帳を更新する。一般にソフトウェアの利用規約は、当該ソフ

トウェアのライセンスの購入者又は利用者とベンダーの間の法律上の強制力のある契約である。そして当該ソフトウェアを電子計算機上で実行することにより、利用者はこの契約書に同意したものとみなされることが多い。したがってソフトウェア利用者の異動が発生した場合は、利用規約を再確認して、その内容を新たなソフトウェア利用者にも同意させておく必要がある。

(2) ハードウェアの異動を伴う場合

一般に、ソフトウェア及び関連資産の実在性を確認する上で最初に取り組むのは、ソフトウェアがインストールされたハードウェア（PC やサーバなど）の所在確認である。ハードウェアの異動が発生した場合は、ハードウェア管理台帳と、必要に応じてライセンス管理台帳を更新する。ソフトウェアの利用規約によっては、インストールされているハードウェアをベンダーへ届け出る必要があるため注意が必要である。更に必要に応じて、ソフトウェアのマニュアルなどの関連書類やパッケージ、インストール媒体の部材一式の保管場所の移動を行う場合もある。

ソフトウェアの利用規約によっては、インストールされたハードウェアの設置場所の地理的条件に制約を加えている場合もある（例えば、「本ソフトウェアをインストールするハードウェアの設置場所は日本国内に限る」など）。ソフトウェア又はソフトウェアをインストールしているハードウェアを海外拠点へ移動する際には、特に注意が必要である。

4.4. 廃却

「廃却」とは廃棄と返却の合成語である。SAM のライフサイクルプロセスにおける「廃却」とは、ソフトウェア及び関連資産を使用できないように撤去することを意味する、当該資産が自社資産の場合は廃棄し、レンタル・リースなどの借用資産の場合は返却することになる。

ISO/IEC 19770-1 によると、このプロセスは“会社の方針に従い、また記録保持についてのすべての要求事項を満たしながら、場合によっては関係資産の再活用も含めて、ソフトウェア及び関連資産を撤去することを確実にすること”を目的としている。そして、このプロセスの導入によって、組織は以下の成果が期待できる。

- a) 撤去するハードウェアからソフトウェアの写しを適切に削除すること。
- b) 再展開可能な使用許諾契約の権利などを、再展開のために特定すること。
- c) 他者に譲渡する資産を、機密保持、仕様許諾条件などの要求事項を踏まえて、適正に譲渡すること。
- d) 再展開不可能な使用許諾契約の権利などが適正に処分されること。
- e) 上記の変更を反映するように記録が更新され、その変更についての監査証跡が維持されること。
- f) 以上の結果として、ソフトウェア又はソフトウェアをインストールしているハードウェアを、セキュリティを確保した状態で撤去するための方針及び手順が策定・承認・発行されること。

（箇条 4.7.9 「廃棄プロセス」 参照）

このプロセスにおける留意事項を以下の各項で述べる。

4.4.1. 廃却情報の集中化

廃却を円滑に進めるためには、廃棄・返却対象となるライセンス又はソフトウェアをインストールしているハードウェアに関する情報を集中化する必要がある。

ここでは、撤去後に再展開可能な使用許諾契約の権利及びその他の資産を再展開のために特定する際の留意点について述べる。ソフトウェア及び関連資産を他者に譲渡する場合は、当該資産を機密保持、使用許諾契約又はその他の契約上の要求事項を踏まえて適正に譲渡する必要がある。

プレインストールのソフトウェアの多くは、当該ハードウェア以外では使用できないという条件が付帯しているものが多い。即ちこれらは再展開不可能な使用許諾契約の権利権であり、ハードウェアとともにソフトウェアも廃棄し、適正に処分されるようにしなければならない。

なお、プレインストールされているソフトウェアのインストール媒体が残っていると、誤って他のハードウェアにインストールされてしまい、コンプライアンス違反を誘発するおそれがあるため、これも確実に廃棄する必要がある。

4.4.2. 廃却時のアンインストール

プレインストールされているソフトウェア以外の場合は、ハードウェア廃却時に、必ずソフトウェアを削除（アンインストール）する必要がある。削除することによって他のハードウェアでの再利用が可能となる。

なお、一般に使用許諾を受けていないソフトウェアについては、これをアンインストールしても使用権についての不備の問題を解決したことにはならないので注意が必要である。これはソフトウェアを使用した時点で既に使用許諾を受ける義務が発生しているからである。この場合は、撤去によって解決するのではなく、インストール又は初めての使用に対する管理をしっかりする必要があり

4.4.3. 廃却時の情報の更新方法

上記変更を反映するように、ハードウェア管理台帳、ライセンス関連部材台帳、導入ソフトウェア管理台帳、ライセンス管理台帳を更新する。また必要に応じて、ソフトウェアのマニュアルなどの関連書類やパッケージ、インストール媒体の部材一式の保管場所についても情報を更新する。

4.5. ISMS/ITSMS における SAM の必要性

SAM と ISMS/ITSMS との関連性については既に 3.2 「他のマネジメントシステムとの関連」で述べたとおりであるが、ここでは逆に組織が ISMS/ITSMS を導入する上で、どの場面で SAM の支援が必要になるのかについて解説する。まず復習を兼ねて、各マネジメントシステムの規格項目の比較表を作成した。(表 4-4)

表 4-4 ISMS、ITSMS、SAM の規格項目比較

名称 分野 規格名	ISMS 情報セキュリティ ISO/IEC 27001	ITSMS IT サービス ISO/IEC 20000-1	SAM ソフトウェア 資産管理 ISO/IEC 19770-1	QMS (参考) 品質管理 ISO 9001
適用範囲	1 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	2 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	3 マネジメント システム要求事項	4. SAM プロセス	4.1 一般要求事項
経営陣の責任	5 経営陣の責任	3.1 経営陣の責任	4.2.2 SAM の企業統 治プロセス	5 経営者の責任
文書管理	4.3 文書化に関する要 求事項	3.2 文書化に関する 要求事項	4.2.5 SAM の能力 (4.2.5.2.a)	4.2 文書化に関する要 求事項
教育訓練	5.2.2 教育・訓練、意識 向上及び力量	3.3 力量、認識及び 教育・訓練	4.2.5 SAM の能力 (4.2.5.2.c)	6.2.2 力量、認識及び 教育・訓練
Plan	4.2.1 ISMS の確立	4.1 サービスマネジ メントの計画	4.3.2 SAM の計画立 案	7.1 製品実現の計画 7.3 設計・開発
Do	4.2.2 ISMS の導入及び 運用	4.2 サービスマネジ メントの実施及びサ ービスの提供	4.3.3 SAM の導入	7.4 購買 7.5 製造及びサービス 提供
Check	4.2.3 ISMS の監視及び レビュー (6. ISMS 内部監査)	4.3 監視、測定及び レビュー	4.3.4 SAM の監視及 びレビュー	8.2 監視及び測定 8.3 不適合製品の管理 8.4 データの分析
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) (8 ISMS の改善)	4.4 継続的改善	4.3.5 SAM の継続的 改善	8.5 改善

なお、規格要求事項の記述方法は規格ごとに多少特徴がある。QMS は「7.1 製品実現の計画」から「8.5 改善」まで本文中に埋め込む形で要求事項が記述されている。ISMS のセキュリティ要求事項は主として附属書 A 「ISMS の管理目的と管理策」に別記されている。また ITSMS も「6 サービス改善プロセス」以降に IT サービスの要求事項を纏めて記述している。

(1) ISMS 管理策に対する SAM の貢献可能性

ISMS 管理策に対して SAM のプロセスが直接的に貢献可能と思われる部分は、附属書 A 「管理目的と管理策」の「A.7 資産の管理」の中の「A.7.1 資産に対する責任」に関する項目である。
(表 4-5)

表 4-5 ISMS 管理策に対する SAM の貢献

箇条	目的と管理策	SAM の貢献ポイント
A.7.1 資産に対する責任	目的：組織の資産を適切に保護し、維持するため。	
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
A.7.1.2 資産の管理責任者	情報及び情報処理施設と関連する資産のすべてについて、組織の中に、その管理責任者を指定しなければならない。	4.4.2 ソフトウェア資産の識別 4.4) 管財人（又は管理責任者）
A.7.1.3 資産利用の許容範囲	情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。	4.4.2 ソフトウェア資産の識別 2.9) ソフトウェア資産に関する、紙及び電子版の両方の契約（契約条件を含む）
A.9.2 装置のセキュリティ	目的：資産の損失、損傷、盗難又は劣化、及び組織の活動に対する妨害を防止するため。	
A.9.2.6 装置の安全な処分又は再利用	記憶媒体を内蔵した装置は、処分する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又は問題が起きないように上書きしていることを確実にするために、すべてを点検しなければならない。	4.7.9 廃棄プロセス 4.7.9.2 成果 a) ソフトウェア、又はソフトウェアをインストールしているハードウェアを、セキュリティを確保して撤去するための方針及び手順の策定、承認、発行
A.9.2.7 資産の移動	装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出してはならない。	4.4.2 ソフトウェア資産の識別 4.3) 場所

まず、A.7.1.1 資産目録に関する要求事項として「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。」と規定している。これに対しては、資産目録の一部として各管理台帳を利用することができる。

また A.7.1.2 資産の管理責任者に関する要求事項として「情報及び情報処理施設と関連する資産のすべてについて、組織の中にその管理責任者を指定しなければならない。」と規定している。これに対しては、資産の管理責任者を指定する上で、各管理台帳の管理責任者欄が利用できる。

更に A.7.1.3 資産利用の許容範囲に関する要求事項として「情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は明確にし、文書化し、実施しなければならない。」と規定している。これに対しては、ソフトウェア資産の利用の許容範囲に関する規則を、紙及び電子版の両方の契約（契約条件を含む）によって明確にすることができる。

この他、A.9.2.6 装置の安全な処分又は再利用に関する要求事項として「記憶媒体を内蔵した装置は、処分する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを

消去していること、又は問題が起きないように上書きしていることを確実にするために、すべてを点検しなければならない。」と規定している。これに対しては、ソフトウェア及び関連資産の廃棄プロセスにおける「ソフトウェア、又はソフトウェアをインストールしているハードウェアを、セキュリティを確保して撤去するための方針及び手順の策定、承認、発行」という要求事項を利用することができる。

最後に、A.9.2.7 資産の移動に関する要求事項として「装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出してはならない。」と規定している。これに対しては、資産台帳の基本情報に「設置場所」を含めることにより、管理対象資産の構外持ち出しに対する一定の抑止力とすることができる。

なおこれとは別に、ISO/IEC 19771-1 の 4.5.4 「ソフトウェア資産セキュリティの順守」については、ISMS の要求事項が大きく貢献しうる。

(2) ITSMS のマネジメントプロセスに対する SAM の貢献可能性

ISO/IEC 19770-1 には、「この規格が定義する SAM のプロセスは、JIS Q 20000 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。(4.1.1 定義及びサービスマネジメントとの関係)。そこで、まず ITSMS 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 (表 4-6)。

表 4-6 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 ISO/IEC 19770-1 の箇条
6. サービス提供プロセス		
6.1. サービスレベル管理	サービスレベルを定義、合意、記録及び管理するため。	4.6.4 サービスレベル管理
6.4. サービスの予算業務及び会計業務	サービス提供費用の予算を管理し、かつ、会計を行うため。	4.6.3 SAM の財務管理
6.6 情報セキュリティ管理	すべてのサービス活動内で、情報セキュリティを効果的に管理するため。	4.6.5 SAM のセキュリティ管理 4.5.4 ソフトウェア資産セキュリティの順守
7. 関係プロセス		
7.2 顧客関係管理	顧客及びその事業推進要因に対する理解に基づき、サービス提供者と顧客の間に良好な関係を確立し、かつ、維持するため。	4.6.2 SAM の関係及び契約管理
7.3 供給者管理	均質なサービスが確実に提供されるように、供給者を管理するため。	4.6.2 SAM の関係及び契約管理

8. 解決プロセス		
8.1 問題管理	インシデントの原因を事前予防的に識別し、かつ、分析することによって、及び問題の終了まで管理することによって、顧客の事業に対する中断を最小限に抑えるため。	4.7.8 問題管理プロセス
8.2 インシデント管理	顧客へ合意したサービスを可能な限り迅速に回復するため、又はサービス要求に対応するため。	4.7.7 インシデント管理プロセス
9. 統合的制御プロセス		
9.1 構成管理	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。	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	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。	4.7.2 変更管理プロセス
10. リリースプロセス		
10.1 リリース管理	リリースにおける一つ以上の変更を、稼働環境に配送し、配付し、かつ、追跡するため。	4.7.5 ソフトウェアリリース管理プロセス

ITSMS のマネジメントプロセスで、SAM のプロセスが最も直接的に貢献可能と思われる部分は「9.1 構成管理」である。(結果的には「9.1 構成管理」とは表裏一体の「9.2 変更管理」にも貢献することになる。)

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 (CI : configuration item) 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。したがって、ITSMS におけるソフトウェア及び関連文書の「構成管理」プロセスは、SAM の「在庫」プロセス (具体的には「ソフトウェア資産の識別」、「ソフトウェア資産の在庫管理」など) と、おおむねオーバーラップすることになる。

このように、構成管理に関する両者の親和性は極めて高いのだが、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。

ITSMS の「構成管理」と SAM の「在庫管理」の対応関係は最も典型的な SAM による ITSMS への貢献可能性であるが、これ以外にも表 4-6 に示したとおり、両者は相互に影響しあい、貢献しうる関係を構築できると思われる。これについては今後の適用事例を待ちたい。

5. SAM の導入計画

導入計画では、どのような SAM を導入するか の 枠組みを決め、具体的に実現するための計画を作成する。

5.1. SAM の導入計画の実施手順

SAM の導入計画フェーズの実施手順は、現状把握、体制及び方針の決定、導入計画の策定大きく三つのステップからなる（図 5-1）。

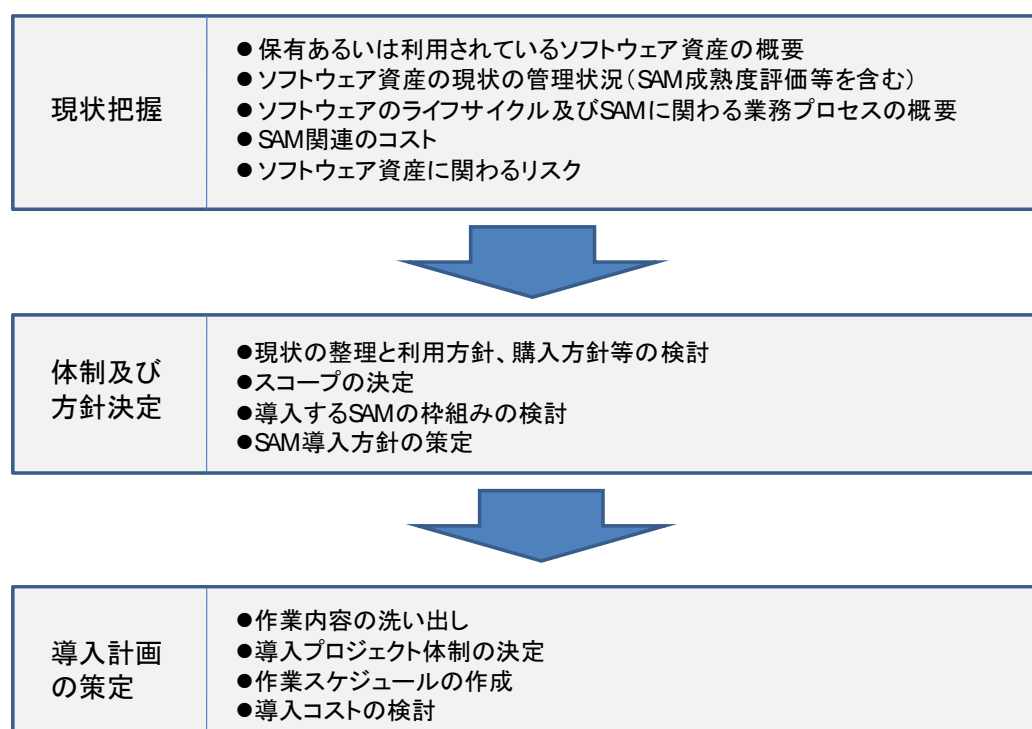


図 5-1 SAM 導入計画のステップ

5.1.1. 現状把握

SAM を導入するに当たって、はじめに実施すべきことは、現状がどのようなものかを把握することである。すなわち、ソフトウェアがどこで、どのようなものが、どのような環境で、利用されているのか、管理の状態はどうか、組織にとってどのようなリスクがあるのかなどを知ることにより、ソフトウェア資産管理にどのように取り組むべきかという、進め方や方針の検討が行えるようになる。

具体的には、次のような点を把握する。

- 保有あるいは利用されているソフトウェア資産の概要
- ソフトウェア資産の現状の管理状況 (SAM成熟度評価などを含む)
- ソフトウェアのライフサイクル及びSAMに関わる業務プロセスの概要
- SAM 関連のコスト

- ソフトウェア資産に関わるリスク

5.1.2. 保有あるいは利用されているソフトウェア資産の概要把握

最初に SAM の対象となるソフトウェアの状態を把握する。対象となるソフトウェアの状態にもとづいて、その他の状況の把握や方針の決定などが実施されることになるので重要なステップとなる。具体的には次のような点を把握することになる。

- どこにどのような種類のソフトウェアが利用されているか（所在、ソフトウェアの種類、名称、数量、契約・ライセンスの形態など）
※ PC、サーバなどのハードウェアの状況含む
- 誰が何に利用しているのか（利用者、利用目的）
- どこの所管か、管理されているか（所有者、管理者、管理状況）

ソフトウェアの状況を確認する場合、PC やサーバなどソフトウェアが導入されているハードウェアの状況を把握したうえで実施しなければならない場合も多いため、ソフトウェアに合わせてハードウェアの状況も把握しておくことが効果的である。

ソフトウェアの状態の把握としては、詳細な棚卸レベルから全体的な状況を把握する概要レベルのものまでが考えられるが、この段階での、ソフトウェアの状態の把握は、方針を検討することが目的のため、通常概要レベルでの把握として実施される。ただし、何らかの形で導入までの段階に詳細な調査は実施されることになるので、対象となる組織の規模や状況に応じ、この段階である程度詳細な棚卸を実施するという事も考えられる。例えば、組織の規模があまり大きくない場合、ソフトウェアの種類や利用形態などの全体の状況が把握されており、複雑ではない場合などであれば、概要レベルと詳細レベルと二度実施するより、この段階で詳細に実施することが効率的となることも考えられる。状況がわからない場合、規模が大きく複雑な場合は、概要レベルである程度把握した後、方針を定め対象や範囲を絞り込んだ形で詳細な棚卸を実施することが効果的と思われる。

なお、詳細な棚卸の方法などについては「6.4. 対象資産の調査手順」に記載している。

概要レベルの把握については、各担当部署などへのヒアリング、あるいは、簡単な調査表を用いたアンケートなどにより実施することが考えられる。

5.1.3. ソフトウェア資産の現状の管理状況の把握

ソフトウェアの状態を把握したら、次にソフトウェア資産の管理状況を把握する。ソフトウェアの管理状況を把握することにより、当該管理のレベルや内容などの状況を踏まえ、SAM 導入の方針や取り組み方を検討していく。

ここでは、ソフトウェア資産管理として、何を実施しているか、何ができていて、何ができていないのかというような点を把握することになる。この段階での把握は、導入に向けて方針などを決定するために実施するものなので、やはり詳細な SAM 監査や SAM 評価というよりは、概要レベルでの把握ということになる。

なお、この管理状況の把握についてソフトウェアの状態の調査に合わせて実施することも考えられる。また、SAM に関連した規程マニュアルなどのドキュメント類などの状況についても確

認しておくことが望まれる。

その他の留意点として、管理状況は、管理する部門や対象ソフトウェアによって状況が異なる場合もあるので、全体の状況が把握できるよう、対象や範囲について留意しておくことが肝要である。

また、現状の管理状況の把握は、SAM の成熟度評価などにより実施することも効果的と考えられる。成熟度評価の詳細な内容については、「5.4. SAM の成熟度評価」を参照のこと。

5.1.4. ソフトウェアのライフサイクル及び SAM に関わる業務プロセス概要の把握

SAM に関連する作業や情報は SAM 業務として独自に存在しているものだけではなく、組織における他の業務プロセスの中で実施されているなど、他のプロセスから情報を入手しなければならないものも多くある。したがって、ソフトウェアを取得してから、廃棄するまでのライフサイクルの中でどのようなプロセスと関わっているのか、ソフトウェア資産の管理としてどこでどのようなことが行われているのかという点を把握し、SAM の構築に向けて、業務プロセスの改善などを含めた SAM の課題などを検討しておくことが効果的である。ここでの業務プロセスの把握についても、詳細な業務プロセスの洗い出しや分析というのではなく、SAM に関連するものとして、どの部署で何をやっているのかというレベルでの把握となる。構築段階では、詳細な業務プロセスの分析、改善などを行うことになるが、その詳細は「6.1. SAM の構築プロセス」を参照のこと。

この段階で、SAM を導入、構築する場合にどの部署が関連し、協力を得る必要があるかが把握されることになり、導入や構築でのプロジェクトの体制を検討するうえでも有用な情報となる。

5.1.5. SAM 関連のコストの把握

SAM の導入に当たり、ソフトウェアの種類や数量のみではなく、ソフトウェアに関連して、何にどれだけのコストがかかっているか (SAM の TCO) という点を把握することは、コスト削減のため、あるいは SAM の方針やスコープを検討するうえでも有用である。

ソフトウェアに関連する費用としては次のようなものがある。

- ソフトウェアの取得費用
 - － ライセンス料
 - － 開発費
 - － 取得に関わる間接費 (契約交渉、資産の調達のための費用 など)
- ソフトウェア運用費用
 - － アップグレード、メンテナンス費用
 - － ソフトウェアサポート費用
 - － ソフトウェアの管理費用
(ライセンス管理、導入、変更、ヘルプデスク、障害対応、教育、監査など)

5.1.6. ソフトウェア資産に関わるリスクの把握

(1) リスク分析評価の必要性

SAM の導入方針などを検討するに当たって、ソフトウェアに関わる上記のような観点での状

況を把握することに加え、ソフトウェア資産に関わるリスクを分析評価しておくことが重要となる。SAM は、ソフトウェア資産に関わるリスクに対応するための管理と捉えることができ、どのような SAM を実現すべきか、何を、どこまで実施すればよいかということから、SAM の枠組みを考える上で、リスクの分析評価が不可欠の要素と考えられる。

(2)ソフトウェア資産に関わるリスク

ソフトウェア資産に関わる一般的なリスクとして、ソフトウェア資産管理基準及び ISO/IEC 19770-1 で挙げられているリスクを示すと次のとおりである。

ソフトウェア資産管理基準 (SAMCon)

- アカウンタビリティ (説明責任) の欠如
- 法的問題の発生
- 社会的信用の失墜
- 余分な費用負担の発生
- ソフトウェア利用サービス提供の中断
- セキュリティ上の問題の発生

ISO/IEC 19770-1 (4.2.3.2 d)参照

- ライセンスに関する非コンプライアンスのリスク
- 不適切なソフトウェア資産管理により生じる IT インフラの問題を原因とする運用障害のリスク
- 不適切なソフトウェア資産管理により生じるライセンス及びその他の IT サポートコストの過度な出費リスク
- ソフトウェア及び関連資産に関する分散管理アプローチや集中管理アプローチに伴うリスク
- 現地のコンプライアンスに関する文化及び実行アプローチを考慮して、異なる国において運用を行う上でのリスク

ソフトウェア資産に関わるリスクは、大きくはおおむね上記のリスクに該当することと思うが、リスクの洗い出し、分析においては、どのような要因から発生するか、どこで発生するかなど様々な観点から検討することが望まれる。リスクの発生要因や影響度などを分析評価することにより、リスクに対してどのような対応を行えばよいかを検討できるようになる。

例えば、ソフトウェアのコンプライアンスに関連する問題であれば、現状のソフトウェアの利用状況や契約形態からどのソフトウェアでどのようなコンプライアンス違反が考えられるのか、その影響はどの程度かなどを分析評価することにより、ソフトウェアの利用を取りやめる、契約形態を見直す、コンプライアンス違反のチェック体制を強化するなどの対応策を検討することができるようになる。あるいは、ソフトウェア利用の中断という観点から、ソフトウェアに関わる障害やバグによるシステムダウンや、開発元が経営悪化しバージョンアップやサポートが受けられなくなるなどのリスクが認識された場合、ソフトウェアの選定時にこのような観点での検討項目を追加しておく、システムダウンなどへの対応が適切に行えるようサポート契約も含め体制整備しておくなども考えられる。

(3) リスク分析評価の手順

リスク分析評価は、次のような手順で実施していくことになる。

表 5-1 リスク分析評価手順

手順	内容
① リスクの洗い出し	ソフトウェア資産管理に関連してどのようなリスクがあるかを洗い出す。
② リスクの評価	リスク洗い出しの調査結果にもとづいて、重要性や影響などから、リスクの評価を行う。リスクの評価は、洗い出しに合わせて実施する場合と、洗い出しの結果に基づいて別に評価を行う場合などが考えられる。
③ リスクの全体的な観点からのレベル調整	リスク評価の結果は、実施の方法によってはばらつきが発生するので、必要に応じ全社レベルでの調整を行っておく。
④ 優先度の検討	評価結果に基づいて、対応の優先度を決定する。
⑤ リスク対応方針の決定	評価結果などに基づいて、どのように対応するか対応の方針を決定する。この段階でリスクを受容する範囲なども決めておく。

リスクの洗い出しについては、詳細なもの、簡易的なもの、あらかじめ分析結果の例を示したもの、例を示さずゼロベースで実施するものなど、様々な方法が考えられる。目的状況に応じた方法で実施することになる。実施方法としては次のような点を検討する。

- 調査対象：どのソフトウェアに対するものかなど
- 調査期間：スケジュールなど
- 調査先：部署、担当者
- 調査方法：アンケート、調査票、ヒアリングなど
- 調査項目：リスクの内容、発生要因、影響、発生可能性、現状の対応策など

なお、リスクの洗い出し、優先度の決定、リスクの対応方針については、必要に応じ経営者の意見などを採り入れ置くことが効果的と考えられるため、経営者層についてのインタビューを実施したり、洗い出しなどの調査の対象とすることも考えられる。

表 5-2 リスク調査シートの例

ソフトウェアに関わるリスク調査シート							
実施日	2009/xx/xx						
調査部署							
調査担当者							
対象となるソフトウェア	リスクの分類	リスクの内容	発生要因	評価についてのコメント	影響度	発生可能性	リスク評価
すべて	法的リスク	ソフトウェアメーカーより損害賠償を求められる	不正コピー	利用数が多いため影響度は大 状況が適切に把握されおらず発生可能性は中	大	中	6
影響度: 大、中、小 発生可能性: 大、中、小 リスク評価: 影響度(大=3、中=2、小=1) × 発生可能性(大=3、中=2、小=1)							

(4) リスクへの対応方針

ソフトウェアに関わるリスクを分析評価した結果に基づいて、その対応を検討することになるが、ここではまず、組織におけるソフトウェア利用の全体をどのような形で管理していくかを検討し方針として定めていく。この方針には、リスクの大きさによる管理の目的、強さあるいは体制構築の優先度などが含まれる。

なお、少なくともソフトウェアがある限り、そのソフトウェアがどのような管理をすべきかが定められている必要がある。また、この方針は、次の 5.2 体制及び方針決定における検討などの過程で必要に応じ適宜修正が行われるものと考えられるので、この点を留意しておくことが望ましい。

表 5-3 対応方針の例

NO	ソフトウェアの分類	全社／部門	コンプライアンスの観点	セキュリティの観点	備考
1	全社共通で利用している有償のソフトウェアのうち主要なソフトウェア	全社共通	○	○	
2	全社共通で利用している有償のソフトウェアのうち1以外のソフトウェア	部門個別	○	○	当初は部門個別とするが、最終的には全体共通管理を目指す。
3	特定の部門でのみ利用している有償のソフトウェア	部門個別	○		
4	無償のソフトウェア	部門個別	○		
5	3、4でセキュリティの観点で管理が必要と思われるソフトウェア	全社共通		○	
6			

5.2. 体制及び方針決定

現状把握ができたところで、次にどのような SAM とするのか、どの範囲で実施するのか、ど

のように取り組んでいくかなどについて導入の方針を検討することになる。ここでの方針は、組織がどのように SAM に取り組んでいくかという観点で重要なものであり、SAM を適切に実現するため、方針の策定段階から経営者の関与が望まれる。具体的には、SAM に関する経営者の理解を得るとともに SAM の方針に経営者の考えを取り入れる。策定した SAM の方針について経営者の承認を得、経営者自らが積極的に推進していくなどが考えられる。

5.2.1. 現状の整理と利用方針、購入方針などの検討

現状を把握した後に実施すべきことは、効果的、効率的に SAM を行うために現状を整理し、変更すべき点、改善すべき点などを洗い出し、ソフトウェアの利用や購入など SAM に関わる基本的事項についての方針を検討することである。

なお、一般にこれらの検討はスコープの検討と合わせて実施することも多いため、実務的には基本的な方針とスコープを合わせて検討することも考えられる。ここでは検討すべき事項を明確にするため分けて記載している。

(1) ソフトウェアの利用方針

現状を把握すると、様々なソフトウェアが、様々な部署で利用されている状況がわかる。多種多様な利用は、管理が煩雑になったり、ファイルの互換性や操作性から利用面で混乱を招いたりするなど管理上望ましくない。そこで、組織全体でソフトウェアをどのように利用していくかを検討しておく必要がある。

具体的には、次のような観点での検討が考えられる。

① 組織として利用すべきソフトウェアか否か

利用されているソフトウェアには、セキュリティ上の問題から利用すべきではないようなソフトウェアや下記の標準化や契約形態の見直しなどで集約した方がよいと思われるソフトウェアがあると考えられる。そこで、組織として利用すべきソフトウェアについての方針（考え方）を明確にしておくことが望まれる。ソフトウェアの中には各部署に管理や購入を任せるといったものもあると思われるが、その場合でも方針に従った利用が行われるよう明確にしておくことが必要となる。個人所有のソフトウェアの利用や個人所有の PC でのソフトウェアの利用などが行われている場合もあるので、それらの対応についても検討しておくことが望ましい。また、利用すべきソフトウェアの検討にはバージョンの統一などの観点も含まれる。検討のポイントとしては次のようなものが考えられる。また、利用すべきでないソフトウェアを明らかにしておくことも望まれる。

- セキュリティ上の観点（情報漏洩、セキュリティパッチ・保守可能性、現状システムとの相性、トラブル状況など含む）
- データの互換性、操作の互換性
- 利用状況（実質的に使われていないもの、業務上不要なものなど）
- コストの観点
- 下記標準化、契約形態の見直しによるもの

② 標準化（ソフト、ハード、業務プロセス）

ソフトウェア、ハードウェアが多種多様なものが利用されている場合、その種類や使われ方に応じた管理が必要になるなど、管理の負荷やコストが大きかったり、部署ごとに異なっている場合など異動すると操作が変わる、あるいはファイルの互換性がないなど利用上の問題が生じる可能性もある。こうした問題に対応するために、標準化を検討することが望まれる。

なお、標準化は、SAM を効率的、効果的に実施するために望ましいものであるが、組織の事業活動への影響についても充分配慮して検討することが必要である。標準化としては、ソフトウェアの標準化、ハードウェアの標準化、SAM 管理手続（業務プロセス）の標準化などが考えられる。

業務の種類、利用部署、場所など幾つかの観点で分類し標準とすべきものを検討する。標準は一つというものではなく、状況に応じ複数の標準が設定される場合もある。ただし、標準のパターンが多すぎると管理が煩雑になるなどの問題が生じるのでバランスを考慮し検討することが必要である。また、標準の設定としては、ソフトウェア、ハードウェア、SAM 管理手続などそれぞれについて行う場合、組み合わせで行う場合が考えられるので状況に応じて適宜設定することが望まれる。

③ 契約等形態

ソフトウェアを利用する場合、例えばパッケージとして購入、プリインストールで購入、ボリュームライセンス契約により購入、インターネットからダウンロード、CD-ROM で提供など、その購入、提供、契約の形態は様々なものがある。こうした状況はやはり、管理上は非効率やコスト負担の増加などを招く可能性があり望ましくない。契約等形態を見直すことで、効率化、法的なリスクの軽減、コストの低減などが可能となる場合も考えられる。そこで現状を踏まえ上記利用方針に合わせ購入、提供、契約の形態などを検討することが望まれる。

④ 利用形態

標準化、契約形態などの検討に合わせて、利用形態自体を見直すなどの検討することも考えられる。利用形態を見直すことにより SAM の管理の効率化、購入コストの削減などが考えられる。具体的には次のような点が挙げられる。

- サーバなどの整理統合
- OA 環境の見直し
- ASP、SaaS、クラウドなどのサービスの利用

(2) 管理体制

この段階で、管理体制についても基本的な事項を検討しておくことが望まれる。

具体的には次のような事項の検討が考えられる。

① 管理責任者、管理部署

SAM を担当する責任者、とりまとめ部署を決め、当該責任者、管理部署を中心に導入検討作業を進めていくことが望まれる。当初より担当する部署を決めておくことにより、運用を踏まえ

た SAM の構築が可能となり、スムーズな導入、運用への移行が行えるようになる。

②集中管理、分散管理

SAM をどのように実施していますかという、各部署に任せていてそれぞれが適切に実施しているはずだと言うような話はよく聞かれることで、その際、集中管理と分散管理という点が取り上げられることがある。集中管理は、一元的に一括して管理するような形態、分散管理は、管理単位を分け管理単位ごとにそれぞれ管理する形態と考えられる。この管理形態は、どちらがいいというものではなく、組織の状況、管理の内容によって適切な形とすべきものである。しかしながら、組織としての管理、ガバナンスという点を考えると、組織として適切に管理を実現している必要がある。分散管理だからそれぞれが実施していればよいということも考えられなくはないが、それぞれが実施していることが組織全体として適切でなければ、全体としては最適ではない可能性もある。したがって、全体的な観点からの調整あるいは管理を行うことが必要となってくる。

SAM を考えた場合も、同様に、組織全体を一括管理できる組織もあれば、個々の部署などで組織の形態や、規模や状況が異なり、一括して管理することは困難な場合も考えられる。一括して管理することが適当でない場合、個々の部門などの管理単位ごとに管理を任せることになる。しかし、組織としては、任せるというのだけではなく、組織全体として適切な SAM が実現できるように、どのような管理を実施すべきかを示すとともに、どのように管理を実施しているかの状況を把握し、個々の管理単位における SAM を統括し、取りまとめ管理する必要がある。

したがって、このような点を踏まえて SAM の管理組織をどのような構成にするかを検討しておくことが重要となる。

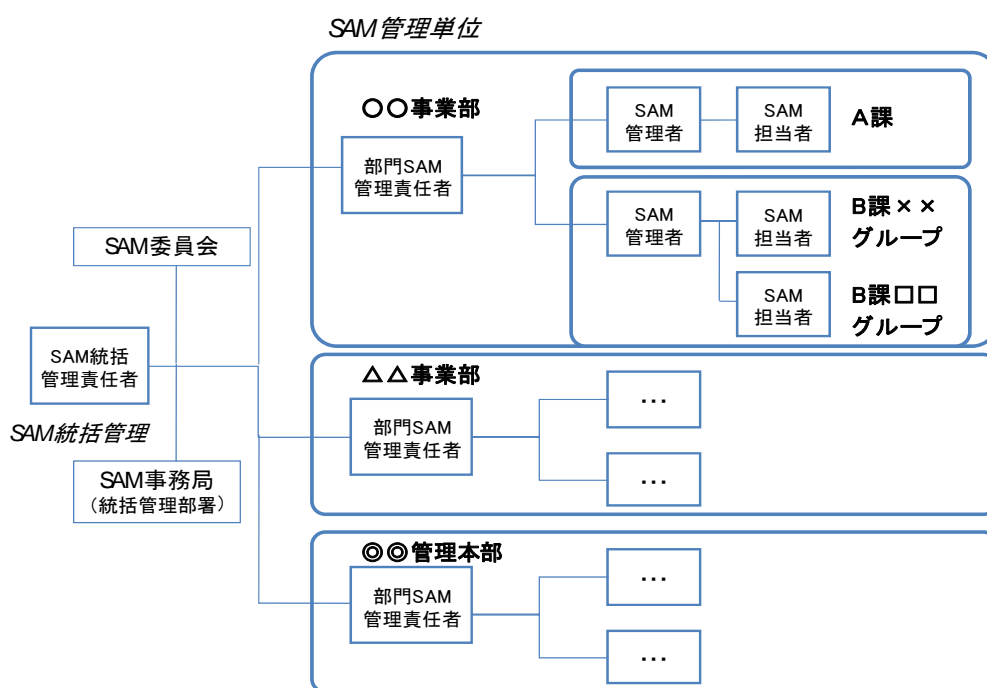


図 5-2 SAM 管理組織の例

③購買手続、窓口の一本化

SAM を検討するうえで、よく購買手続や窓口の一本化ということが課題として取り上げられる。ソフトウェアを適切に管理しようとした場合、まず対象資産の発生時点、すなわちソフトウェアの取得する時点から把握し、管理しておくことが望ましいということによると考えられる。購買は、自社開発などの場合を除きソフトウェアのライフサイクルの一番初めの時点ということになるからである。しかしながら、ソフトウェアを購入する場合、購入時点で SAM が考慮されておらず、手続なども様々となっているケースが多く見受けられる。そうした状況では、管理すべきソフトウェアを把握できず網羅的で適切な管理が困難となる可能性がある。購買手続や窓口を一本化することによりソフトウェアの発生時点から把握し、適切な SAM を実現することが望まれる。なお、一本化としているが、必ずしも一つの必要はなく、効率的に確実に管理可能は手続が検討されればよいと考えられる。

④関連部署との連携

SAM の業務は、組織の中で独立した業務として存在しているのではなく、ソフトウェアのライフサイクルなどを考えると、上記の購買手続と同様に様々な業務と関連を持ち、実現されるところが多いと考えられる。したがって、SAM に関連するすべての部署と適切な連携がとれるような、体制を検討しておくことが必要となる。具体的には SAM の管理組織や連絡体制などとして考慮されることになる。

5.2.2. スコープの決定

SAM を導入する場合、組織全体のすべてのソフトウェアに対して同じレベルで管理を実施することは困難であり、効率的ではない。したがって、把握した現在の状況や対応すべきリスクなどにに基づき、どこで、どのような SAM を実施していくかを決めていく必要がある。そのために、まず、組織、ソフトウェア、ハードウェアなど関連資産の状況を分類整理し対象とする範囲を特定する必要がある。

なお、実際には分類整理した対象範囲ごとに実現すべき SAM の内容を検討し最終的には全組織・全関連資産を対象とすることになる。ここでは導入の優先順位の検討なども含め対象とする範囲を検討するときのポイントを記載する。

(1) 対象とする組織、ソフトウェアなどの検討におけるポイント

SAM 導入の対象とするかを定める場合、現状把握として把握した内容を次のような観点で分類整理し、対象範囲及び取り組み方を検討しく。

- 利用範囲（全体、複数部署、特定部署など）
- 重要性(数量、金額、質、リスクとの関連)
- 利用形態（多種多様・複雑な利用（システム開発部門など）、画一的など）
- 購入形態（ライセンス契約による集中購買、部門個別、ハードとセット（OEM・プリインストール）で購入）

※ライセンス契約がある場合には、契約の範囲なども考慮することが望ましい。

組織あるいはソフトウェアなどの資産を SAM の対象とするか、対象とする場合共通の SAM を導入可能か、共通と個別に分けて検討するか、段階的に導入していくかなどをポイントに、範囲の切り分けと取り組みの仕方を検討する。

一般的には、組織全体で使われているもの、数量や金額が大きいもの、リスクの高いもの、利用形態や購入形態から全体共通的に管理しやすいものから、優先的に共通の SAM を導入していくなどが考えられる。

(2)SAM の対象とする組織や資産の範囲の検討でよく挙げられる事項

ソフトウェア、ハードウェア、その他関連資産について SAM の対象とするかの検討でよく見受けられる検討事項を示すと下記のとおりである。

①組織の範囲

- すべての部門を含めるか、管理部門・事務系部門のみにするか、IT 部門、研究所、工場、作業現場などは除くか
- グループ会社を含めるか、海外の部署・グループ会社を含めるか

②ソフトウェアの範囲

- 実行可能なソフトウェアのみか、非実行可能ソフトウェアも含めるか※
- OS、ユーティリティ、ミドルウェア、アプリケーションなどどれを含むか
- 有料のソフトのみか無償のソフトも含めるか
- ライセンスフリーのソフトなども含めるか
- 自社開発のソフトを含めるか
- 個人所有のソフトウェアなどをどのように取り扱うか

※ ISO/IEC 19770-1 で対象としているソフトウェア

- 実行可能ソフトウェア : OS、アプリケーションプログラム、ユーティリティプログラムなど
- 非実行可能ソフトウェア : フォント、画像、様式、辞書など

③ハードウェアの範囲

- パソコン、サーバ、ホストなどのどの種類のコンピュータを対象とするか
- 対象とするプラットフォームをどうするか、MAC、Linux、Unix などを含めるか
- 常時ネットワークに接続しているもののみ対象とするか、ノート PC など適直接続するものも含めるか、あるいはスタンドアロンのもので含めるか
- 機器などに付属する制御用のマシン、PDA などモバイル製品、アプライアンス製品（専用機器）も対象とするか
- 個人所有のハードウェアの取り扱いをどのようにするか

④その他関連資産の範囲

- ライセンス契約書・証書、購入時証憑など、ライセンスを証明するものとして、どれを対象とするか
- インストール媒体として何を対象とするか（CD、FD、HD 上のイメージなど）
- 配付用の原本、コピー、ビルトなどを対象とするか
- 購入時のパッケージ製品のパッケージ、マニュアルなどを対象とするか

5.2.3. 導入する SAM の枠組みの検討

ここでは、現状把握、基本的な方針やスコープの決定を受け、導入する SAM の基本的な枠組みを検討していくことになる。スコープの検討により、何が対象になるかが特定されているので、それぞれ何を管理するのかなどを検討する。具体的には、ソフトウェアのライフサイクル、SAM の業務から次のような点を検討することになる。

- ソフトウェアの保有状況の管理（購入したソフトウェアライセンス、自己開発したソフトウェアなど組織として保有しているソフトウェアの管理）
- ソフトウェアの導入状況の管理（コンピュータ上に導入されているソフトウェアの管理）
- ソフトウェアの利用状況の管理（利用されているか否か、どの程度利用しているかなど実際の利用状況の管理）
- ソフトウェアの障害状況の管理
- ソフトウェアの購入コスト、予実管理
- ソフトウェアの配付用のイメージ、媒体の管理
- ライセンス証書、契約書の管理
- 法令、ライセンスコンプライアンス状況の管理
- ソフトウェアの棚卸
- 管理状況のモニタリング、監査

この段階では、あくまで導入すべき SAM の枠組みとして基本的な要件のレベルまでを検討するのが適当と考えられる。詳細な要件などの検討は構築の作業として実施される。

ここでは、上記検討すべき点について、何を管理すべきか、そのためにはどのような項目を管理すべきか、またどのような情報が必要となるか、把握した情報をどのように報告あるいは管理するかというようなことを検討していく。

例えば、保有しているソフトウェアの状態を考えた場合、まずソフトウェアを識別するためにどのレベルまで把握しておく必要があるか、種類、名称、バージョン、パッチの状況、バージョンアップどのレベルまで管理するか、また、取得の形態（自己開発、ライセンス購入、プリンストールなど）、ライセンス契約、購入先、使用条件の内容との関連が必要かなどである。また何を管理するかという点で、残高だけでよいか、増減などの受払や異動、履歴の管理などが必要か、証書などとの定期的なチェックが必要かなどを検討する。検討項目、ポイントとして次のようなものが考えられる。

表 5-4 SAM 枠組みの検討項目とポイント

項目	内容又はポイント
対象の識別	どのように対象を識別するか（対象となる資産と関連する実態、契約書、証書、インベントリ情報、媒体など）
管理すべき項目と記録	<p>管理項目の概要</p> <ul style="list-style-type: none"> ● 項目 <ul style="list-style-type: none"> ➢ ソフトウェア：種類、名称、バージョン、パッチの状況、バージョンアップ、期限など、所有状況（ライセンス形態、メーカーなど）、導入状況（導入先、利用者、管理者、利用状況、ライセンスとのひも付け） ➢ ハードウェア：種類、モデル、型番、メーカー、設置場所、利用者など ➢ 購入：予算、購入申請、コスト、購入先、購入部署、担当者、入手形態、契約形態など ➢ 残高、増減（フローとストック）、移動、状態など ➢ 関連する項目（伝票、承認、証憑など）など ● 記録 <ul style="list-style-type: none"> ➢ 申請書、残高台帳、受払台帳、各種管理リスト・報告書など ➢ 履歴管理（過去の状態、記録の保管）、貸出管理、複写管理など ➢ 追跡可能性（監査証跡）、検証可能性など
検証方法	モニタリング、棚卸、監査など
コンプライアンス	違法コピーの有無の状況（導入数と保有ライセンス数の照合など）、ライセンス条件の遵守状況（何をチェックすべきか）など

また、SAM の業務をどのように実現するかという観点で、上記に加え更に次のような点を検討しておく。

- 必要な情報をどのように入手するか（関連業務・システムとのインタフェース）
- 誰がどのような手順で管理するか（ワークフロー）
- 管理の仕組みをどのようにするか（ツールの利用など含む）

5.2.4. SAM 導入方針の策定

ここまで検討してきた、ソフトウェアの利用方針、管理体制、スコープ、SAM の枠組みなどをとりまとめ SAM の導入方針を作成する。SAM の導入方針としては次のような項目が考えられる。

- SAM 目的
- SAM 運用体制

- PDCA
- ソフトウェアの利用方針
- SAM 業務の概要
- SAM ツールの利用
- SAM ワークフロー概要
- 他の業務プロセス（ライフサイクル、財務、人事、購買など）との関連、インターフェース概要

5.3. 導入計画の策定

導入しようとする SAM の方針が決まったところで、次に導入に向けた基本的な計画を策定する。具体的な構築作業なども含めた詳細な計画内容は「6. SAM の構築」の章参照のこと。ここでは、導入に向けた基本的な計画策定のポイントのみ記載しておく。

5.3.1. 作業内容の洗い出し

まず、導入作業として何を実施すべきかの作業項目を洗い出す。この時点での作業項目は大まかなものでよい。

作業項目の洗い出しは、現状と導入しようとする SAM とのギャップ分析、一般的な構築作業の内容手順などにより実施することになる。作業項目には、次のような観点が含まれる。

- 業務の変更（ワークフロー構築など）
- システムの導入、変更（ツール導入、インターフェース構築など）
- 規程、マニュアルなどの整備
- 導入のための教育
- SAM 監査

5.3.2. 導入プロジェクト体制の決定

作業内容の洗い出しとともに導入のためのプロジェクト体制を検討しておく必要がある。導入のプロジェクトは、SAM の運用体制を基本とするが、業務やシステムの変更など実施すべき作業量も大きく、組織全体に関わる作業として実施されることも多いため、実現可能とするための人員や体制とすることが必要である。具体的には、次のような点を考慮しておくことが望まれる。

- プロジェクトの責任者：組織の長など、当該プロジェクトを組織の中で推進していける立場の人とする。
- 事務局の設置：プロジェクトを推進するためのプロジェクトマネジメントを行うもの、運用時での SAM のとりまとめ担当部署が中心となることが望まれる。また、プロジェクトの規模にもよるが、専任の担当者を置くことが望まれる。
- プロジェクトメンバー：関連部署の責任者、担当者などを含める。
- 委員会、ワーキンググループなどの設置：プロジェクトを推進するため、定期的及び随意プロジェクトに関わる意思決定や承認、状況の報告・確認などを行う委員会の設置、個別の作業に応じたワーキンググループの設置などを行うことが望まれる。

5.3.3. 作業スケジュールの作成

導入プロジェクトにおける作業内容と体制が決まったところで、導入に向けてスケジュールを検討する。スケジュールとしては、全体のマスタープランと詳細なスケジュールなどを作成しておくといよい。スケジュールの作成に当たっては次のような点に留意しておくことが望まれる。

- 誰が、いつ、何を実施するか
- 作業の分類やフェーズ分け（具体的な項目は SAM の構築の章参照）
- 実施状況についてのチェックポイント（時点）の設定（委員会開催予定など含む）
- 運用の試行（テストランと確認、SAM の PDCA 一度は回せることが望ましい）
- 段階的に導入する場合はその進め方

5.3.4. 導入コストの検討

作業内容がある程度明らかとなった時点で、導入に関わるコストなどについても見積もっておくことが望まれる。コストの状況によっては SAM の内容自体やスケジュールなどについて見直す必要が出てくる場合もあるので、現状把握、枠組みの検討の段階においても適宜実施しておくことが望まれる。また、導入コストの見積もりは、導入後の投資コストの有効性を検討するためにも有用である。

5.4. SAM の成熟度評価

5.4.1. SAM のアセスメント

組織のソフトウェア資産管理の実施状況がどのようなレベルにあるかを把握する上で、成熟度評価という考え方が利用できる。成熟度評価とは、ある定めた管理基準に対して現在の状況がどの管理レベルに達しているのかを一定の基準で評価することをいう。一般的には管理レベルごとに成熟度を分けて定義し、どの段階まで達しているかをわかりやすく表したものを成熟度モデルと呼んでいる。SAM の場合においても ISO/IEC 19770-1 (JIS X 0164-1) で定義されている内容を基に管理の基準や評価の規準を定義し、それぞれの項目・要素ごとに成熟度を設定して、評価することが行われている。この成熟度モデルにより管理レベルを幾つかの段階に分けることによって、組織における SAM の整備状況、運用状況などの問題点を明らかにし、改善へと繋げて行くことが可能となる。ここでは、SAMCon が策定した「ソフトウェア資産管理 評価規準」を基に SAM の成熟度モデルを定義しているのを例に挙げ、成熟度モデルの考え方、成熟度評価の内容、実際に実施する際の評価方法について記載する。

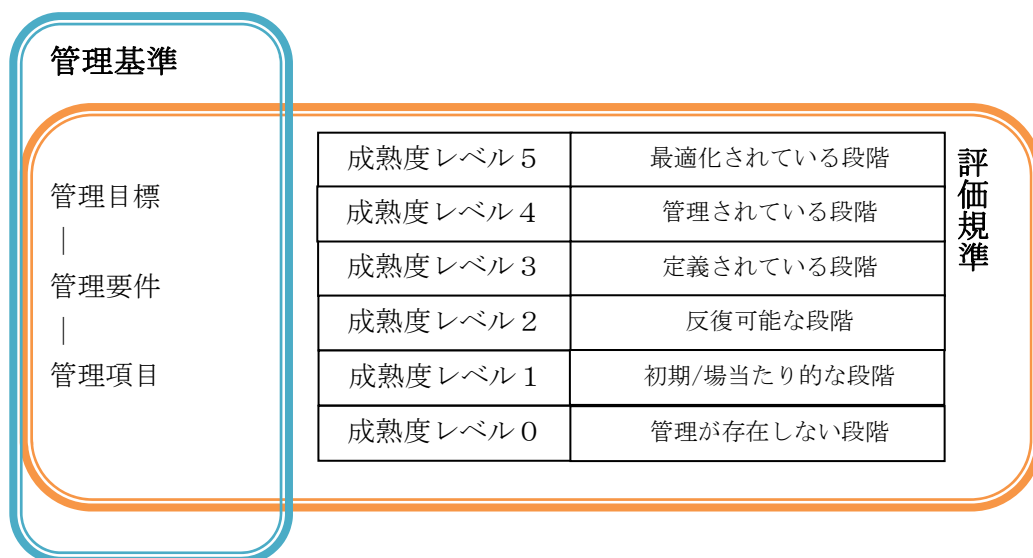


図 5-3 ソフトウェア資産管理基準と評価規準の概念図

ソフトウェア資産管理 評価規準は管理基準に基づく形で存在し、管理基準で定められた管理目標ごとに対応した評価規準が定義されている。また評価を行う場合には対応する管理要件、管理項目を参照し、それぞれの状態を把握することで管理目標ごとの成熟度レベルを判断する。

5.4.1.1. 成熟度モデル

成熟度モデルとは、一般に企業の経営や情報化、管理プロセスなどの実現レベルを何段階かにモデル化したもので、CMMI (Capability Maturity Model Integration) 「能力成熟度モデル統合」などがある。国際標準化されている ISO/IEC 15504 (JIS X 0145) ではプロセス能力をアセスメントする尺度として下記の 6 段階からなるアセスメントモデルが定義されている。

表 5-5 JIS X 0145 におけるプロセス能力アセスメントモデル

レベル	プロセスの状態
水準 0 : 不完全なプロセス	プロセスを実行していない又はそのプロセスの目的を達成していない。
水準 1 : 実施されたプロセス	実行したプロセスが、そのプロセスの目的を達成している。
水準 2 : 管理されたプロセス	水準 1 の” 実施されたプロセス” を管理された方法 (すなわち、計画し、監視し、調整した方法) で実行しており、その作業生産物も、適切に確立し、制御し、維持している。
水準 3 : 確立されたプロセス	水準 2 の” 管理されたプロセス” は、プロセスの成果を達成することができる、定義されたプロセスを使用して実行している。

水準 4： 予測可能なプロセス	水準 3 の” 確立されたプロセス” は、プロセス成果を達成するために、定義する範囲内で運用している。
水準 5： 最適化しているプロセス	水準 4 の” 予測可能なプロセス” を、関連する現在の事業目標及び計画した事業目標を満たすように絶えず改善している。

※ JIS X 0145-2 情報技術-プロセスアセスメント-第 2 部：アセスメントの実施より抜粋

5.4.1.2. 成熟度モデルの考え方

ソフトウェア資産管理コンソーシアムの評価規準における成熟度モデルの考え方も CMMI の成熟度モデルと同様にソフトウェア資産の管理状態について レベル 0 から レベル 5 までの 6 段階の成熟度で評価している。

SAMCon「ソフトウェア資産管理 評価規準 Ver2.0」における各成熟度についての基本的な考え方は下記のとおりである。

■ **レベル 0: 管理が存在しない段階**

管理を全く実施していない。最も評価（成熟度）が低い。

■ **レベル 1: 初期/場当たりの段階**

組織的ではなく、担当者など個人に依存して、管理を実施している。

■ **レベル 2: 反復可能な段階**

ある程度、組織的な体制があり、継続して管理を実施している。

■ **レベル 3: 定義されている段階**

組織全体の方針・規程、管理体制などが適切に定められており、それらの内容に重大な欠陥はない。※ 方針・規程、管理体制が存在していれば、成熟度レベル 3 ということにはならない。他のレベルも同様となるが求められる状態は、「ソフトウェア資産管理 評価規準」において 13 の管理目標ごとに設定されているので、参照されたい。

■ **レベル 4: 管理されている段階**

定められた方針・規程、管理体制などに従って管理が実施されていることをモニタリングしている。

■ **レベル 5: 最適化されている段階**

ソフトウェア資産管理を取り巻く環境の変化に対応し、最適な管理を実施するため、随時及び定期的に、ソフトウェア資産管理を見直している。最も評価（成熟度）が高い。

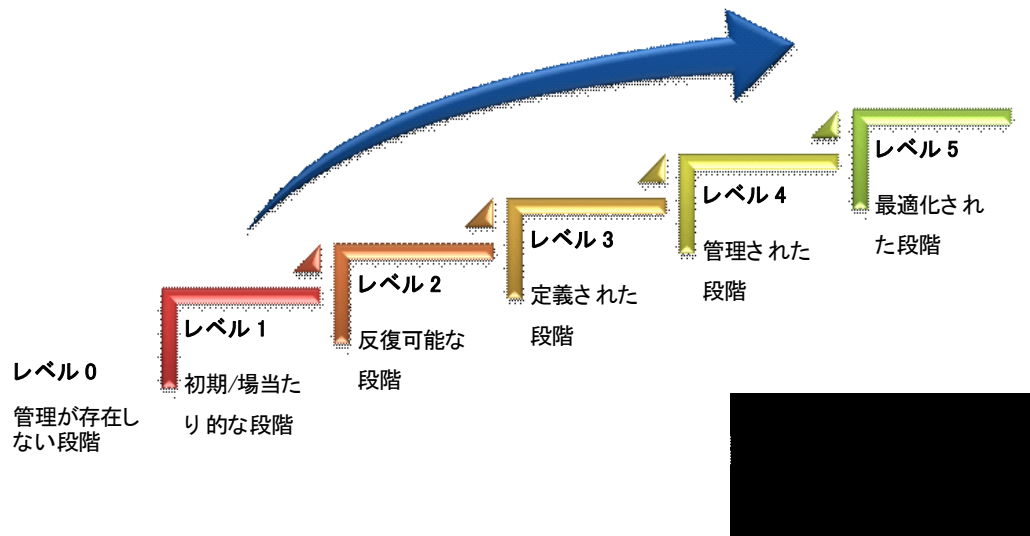


図 5-4 成熟度モデルの概念図

5.4.1.3. 成熟度評価

SAMCon の管理基準並びに評価規準を利用して、実際に SAM の成熟度を評価するに当たっては、管理基準の定める管理要件に従って、現時点の運用上の問題や管理整備状況を確認していく作業を行う。管理基準の定める 13 の管理目標ごとの成熟度レベルを知ること、改善が必要な部分及びその改善策が明確になる。

なお、SAMCon が策定したソフトウェア資産管理基準に基づく評価規準では、以下の 13 の管理目標ごとに 6 段階の成熟度レベルを定義している。

ソフトウェア資産管理基準 管理目標

1. ソフトウェア資産管理の方針・規程の整備
管理目標：自組織に適したソフトウェア資産管理の方針・規程などが作成され、遵守されていること
2. ソフトウェア資産管理体制の整備
管理目標：体制が整備されていること
3. ソフトウェア資産管理の在庫プロセスの枠組み
管理目標：ソフトウェア資産管理におけるインベントリ管理の枠組みを設定する目的は、ソフトウェア及び関連資産の保管場所及び記録を作成して維持し、他のソフトウェア資産管理プロセスにおけるソフトウェア及び関連資産の管理の完全性を確保するためのデータ管理機能を提供すること
4. 所有ライセンスの把握
管理目標：所有ライセンスの種類・数量が把握されていること
5. 導入ソフトウェアの把握
管理目標：どのハードウェアにどのソフトウェアがインストールされているか、また、

そのソフトウェアがどのライセンスに基づいているか把握されていること

6. 所有ライセンスの証明

管理目標：所有ライセンスが証明可能であること

7. ソフトウェア不正使用は不法行為であるとの認識

管理目標：ソフトウェア不正使用は不法行為であるとの認識が浸透していること

8. ライセンス内容の理解

管理目標：ライセンス内容が理解されていること

9. 不正を犯しにくい環境

管理目標：要員が不正使用しにくい環境が構築されていること

10. 購入コストの削減

管理目標：購入コストの削減

11. 管理の効率化、コストの削減

管理目標：管理の効率化、コスト削減

12. セキュリティ上の配慮

管理目標：セキュリティ上の配慮がなされていること

13. 運用管理プロセス

管理目標：ソフトウェア資産管理全体の目的及び便益を達成するための運用管理機能が実行されること

5.4.1.4. 成熟度評価方法

成熟度モデルを用いた評価の方法としては、管理基準ごとの管理目標・管理項目の実態を正確に把握することから始める。

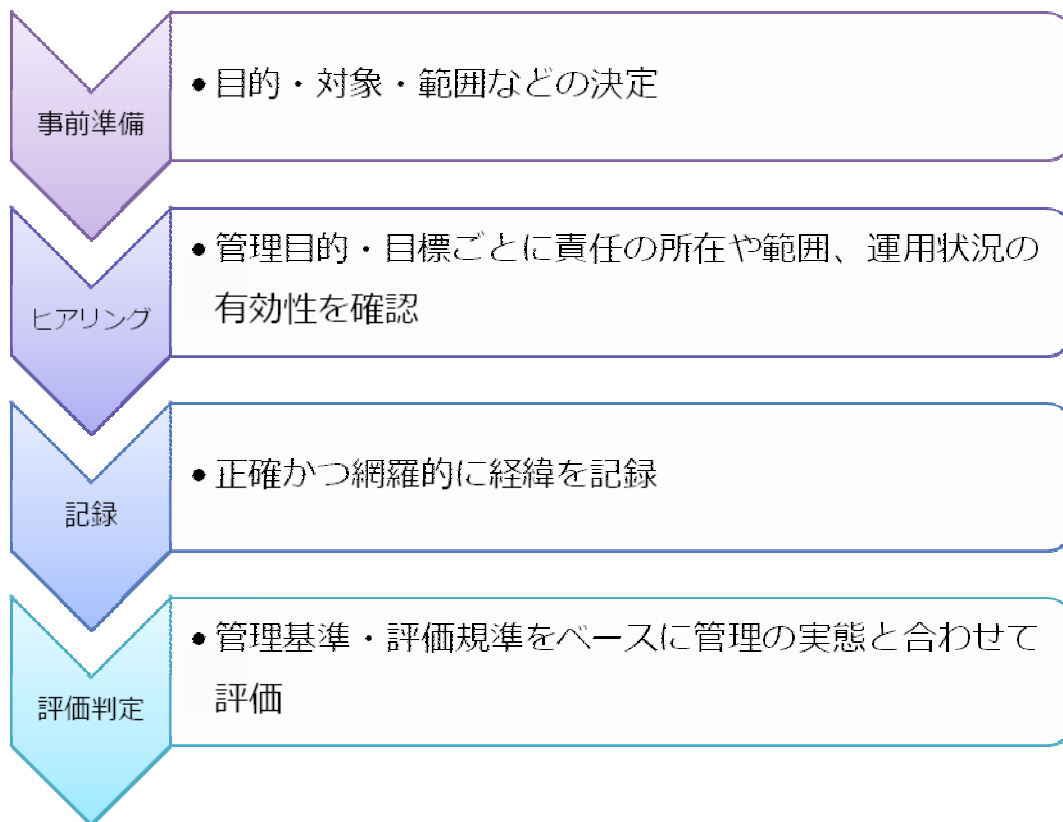


図 5-5 成熟度モデルを用いた評価方法

(1) 事前準備

一般的には管理主体となる組織ごとに、管理対象とする範囲が異なる場合や、管理体制そのものが異なることも多いので、注意を要する。成熟度評価を実施する前に事前に評価の目的・対象・範囲などをあらかじめ決めておくことが望ましい。

(2) ヒアリング

すべての管理項目について特定の人員が詳細まで把握していることは少ないので、項目や内容に応じて適切な管理責任者及び担当者にヒアリングすることが不可欠となる。ヒアリングの具体的項目としては、対象人員数、拠点数、管理対象 PC 台数、管理体制、規程や台帳の整備状況、棚卸の実施状況、社内教育体制、内部監査手順などを順次確認していくこととなるが、大前提として管理の目的、目標をきちんと定めているかどうか重要なポイントとなる。たとえば、管理体制のヒアリングを実施するにあたり、管理体制そのものの存在や、責任の所在や範囲が明確になっているか、管理責任者、管理担当者、統括者などの役割がどのように定められ、任命されているかということを確認していく必要がある。規程類に関してもハードウェア管理規程、ソフトウェア管理規程、導入・廃棄規程など必要な情報の有無だけでなく、その有効性と運用状況についてもヒアリングを通して確認し、場合によっては定められたとおりに実施されているかどうかを現場確認することが必要となってくる。

(3) 記録

ヒアリングと合わせて、評価判定の際に必要な記録を正確に残しておくことが重要である。内部監査で行われる手順などと同様、各項目に沿った調査シートなどを用意しておき、ヒアリングの結果や調査の記録を残しておく。場合によっては複数の担当者に同じ項目についてのヒアリングを実施することや、同様の内容を複数回に分けて調査することがあるので、どのような経緯で導き出された結果なのかをわかるようにしておく必要がある。

(4) 評価判定

担当者からのヒアリングを経て実際の評価判定をする際には、ベースとなる管理基準・評価規準に則していることは言うまでもないが、ヒアリングによって明らかになった情報や評価判定の根拠となった情報についての記録を残し、適切な判断基準に基づく判定が行われたことを証明できるようにしておく。複数の評価者における校正などを実施して、適切な判定を下すことも場合によっては必要になってくるだろう。

その他、すべてのプロセスについて関連することとなるが、組織が定めている規程・規則や体制が、経営層のコミットメントを得られているかどうか成熟度に大きく影響するので、現在の規程・規則がどこまでの承認を得て実施されているものなのかを確認することが重要である。また、ヒアリングによっては管理ができていないように判断できる場合でも、属人的なものでないかどうか、管理意識が先行し机上の論理になっていないかも実際の運用状況と合わせ確認することが望まれる。存在する規程、手続き、体制がもれなく定められ、標準化され、組織として明確に定義・運用された状態にあるかということまで踏み込んで確認・評価して、はじめて適切な成熟度が導き出せる。

SAMCon の評価規準を使って、同管理基準の管理要件を評価項目とした場合の「例」は以下表のとおりである。

1. 方針 ソフトウェア資産管理の方針・規程の整備
管理目標：自組織に適したソフトウェア資産管理の方針・規程などが作成され、遵守されていること
管理目標における成熟度モデル
レベル0 管理が存在しない段階：
ソフトウェア資産管理に関する方針、規程、手続きが全く存在せず、ソフトウェア資産管理を実施していない。
レベル1 初期/場当たりの段階：
ソフトウェア資産管理として取りまとめた方針、規程はなく、実施している手続きは、管理者個人の思いつきであるなど場当たりのものである。あるいは、ソフトウェア資産管理に関わる手続きが、継続的に実施されていない場合がある。
レベル2 反復可能な段階：
ソフトウェア資産管理について、不十分ではあるが、組織として取りまとめられた方針や規

程、手続が存在する。方針に沿って、おおむね一貫性のある規程、手続が作成され、継続的にソフトウェア資産管理が実施されている。しかし、方針や規程の適用範囲は特定の事業所/部署に止まっているなど、組織全体の方針、規程としては不十分であり、事業所/部署によっては組織として望まれるソフトウェア資産管理が実施されていない可能性がある。

レベル 3 定義されている段階：

組織全体を対象としたソフトウェア資産管理の方針、規程、手続が定められ、文書化されている。ソフトウェア資産管理の方針、規程は、ソフトウェア資産に関連するリスク分析結果を踏まえ策定されている。例えば、リスクに応じて詳細に管理するソフトウェアと簡易な管理をするソフトウェアを分けるなど、方針、規程で明らかにしている。それらの方針、規程は、組織の正式なものとして経営者などにより承認されており、手続は、方針及び規程に従ったものとなっている。また、ソフトウェア資産管理が適切に実施されるための体制や仕組み(以下「統制機能」)が整備されている。方針、規程、手続は、ソフトウェア資産管理体制及びソフトウェア資産の取得、利用、異動(移動、ステータスの変更)、廃棄などソフトウェア資産のライフサイクル全般をカバーしており、重大な欠陥はない。

レベル 4 管理されている段階：

定められた方針、規程、手続に従ってソフトウェア資産管理が実施されていることを、ソフトウェア資産管理責任者がモニタリングしている。また、承認手続などの統制機能が有効に働いていることをモニタリングしている。定められた方針、規程、手続が遵守されていない場合、直ちに是正される。

レベル 5 最適化されている段階：

ソフトウェア資産を取り巻く環境の変化に対応し、最適なソフトウェア資産管理を実施するため、随時及び定期的に、ソフトウェア資産管理の方針、規程、手続の見直しを行っている。リスクとの関連を踏まえた見直しを行っており、その結果をソフトウェア資産管理に反映している。

※ SAMCon「ソフトウェア資産管理 評価規準」 Ver2.0 より抜粋

5.4.1.5. 成熟度評価報告

成熟度評価の報告に当たっては、判定した評価結果に基づき「成熟度評価結果報告書」などの成果物を作成する。報告書には SAM の成熟度の結果だけでなく、調査のアプローチ方法や現状の組織における SAM の位置づけに加え、改善点・今後の目標に関する分析事項を提供することが望ましい。

報告書に必要な項目 (例)

評価の概要

- ・評価対象
- ・作業範囲とスケジュール
- ・ヒアリング対象者、評価担当者

成熟度レベル診断基準

成熟度診断結果サマリー

- ・評価結果
- ・総合所見

項目別診断結果 詳細

- ・個別所見
- ・発見・指摘事項

現在の成熟度レベルとその対策

- ・成熟度レベルとその対策

適切なSAM管理体制への改善点

- ・改善提案

今後の目標

- ・次のステップ

評価の概要部分では、今回調査した対象組織のインフラを含む基礎情報（PC 台数、拠点数など）のほか、分析対象・範囲についても明確にし、合わせてヒアリングを実施した対象者の情報、ヒアリング日時など客観的事実を記載しておくといよい。

成熟度レベルの診断基準では、評価の基とした管理基準・評価規準や成熟度を表すレベルを階層ごとに定義し、記載しておく。

診断結果のサマリーについては、全体を通しての総合的な成熟度評価とその判定根拠、現状のリスク及び改善点など総合的な所見を記載する。

個別の診断結果詳細については、管理体制、規程や台帳の整備状況、棚卸の実施状況、社内教育体制、内部監査手順など、評価した各項目を分析した上で、それぞれが方針・体制、コスト、セキュリティなど SAM のどの業務・機能に関わってくるのかを整理しながら、わかりやすい形でまとめ、成熟度を評価すると良いだろう。

その他、評価報告書には結果をわかりやすく見せるためにレーダーチャートのような形式で現在の成熟度レベルと推奨・目標となる成熟度レベルを表すことや、各項目の成熟度レベルに対応した改善対策や次の成熟度レベルを目指すためのアクションについて、分かりやすく記載することも効果的と言える。

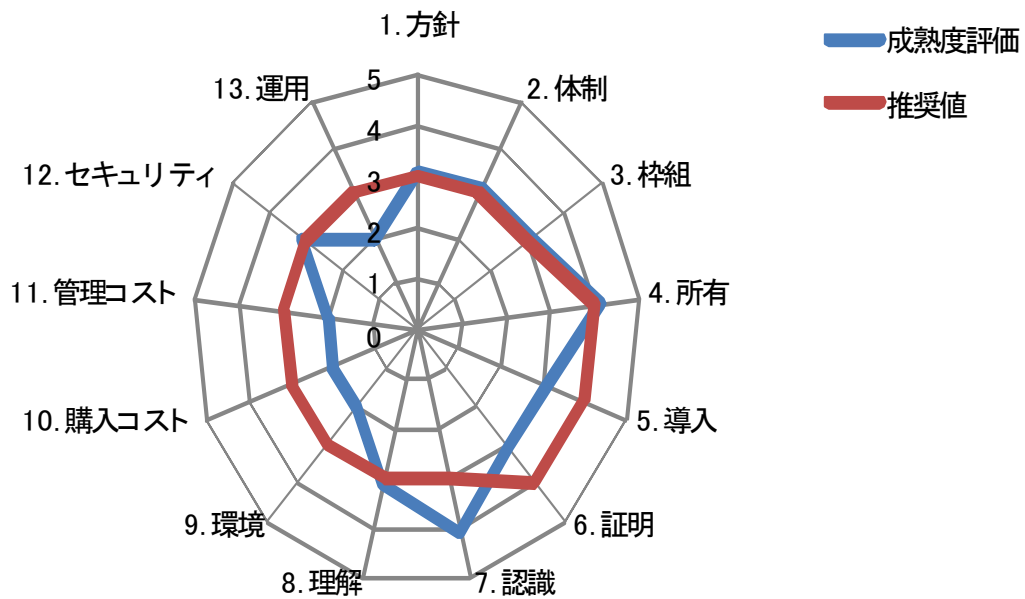


図 5-6 レーダー チャート：サンプル

> 管理目標

自組織に即したソフトウェア資産管理の方針・規程等が策定され、遵守されていること	1
	0.7

> 成熟度レベル：1（初期／場当たりの段階）

ソフトウェア資産管理として取りまとめた方針、規程はなく、実施している手順は、管理者個人の思いつきである等場当たりのものである。あるいは、ソフトウェア資産管理に関わる手順が、継続的に実施されていない場合がある。

> 個別評価

管理要件	成熟度
方針1 全体方針、規程、手順が明確になっており、遵守されていること	1
方針2 定期的にあるいは重要な変更に合わせて、方針・規程、手順の見直しが行われている	1
方針3 ソフトウェア資産についてのリスク管理がされていること	0

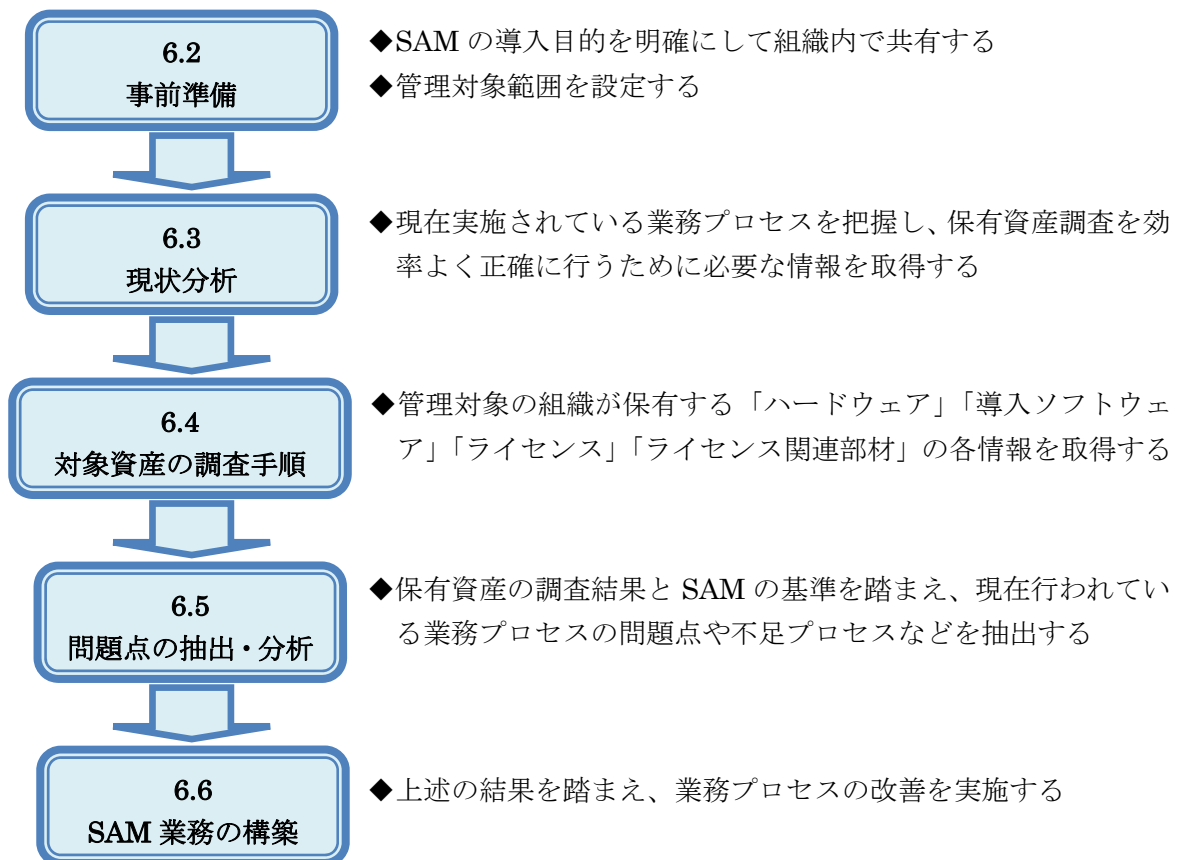
図 5-7 成熟度レベル評価：サンプル

* レーダーチャート、成熟度レベル評価、推奨値などについてはすべてサンプルデータであり、本ガイドが推奨するものではない。

6. SAM の構築

6.1. SAM の構築プロセス

一般的な SAM の構築プロセスの大項目を以下のとおりにまとめる。組織の体制、現在行われている管理により詳細な手順が変わるため、この流れを参考にいただき、組織にあった手順を構築してもらいたい。

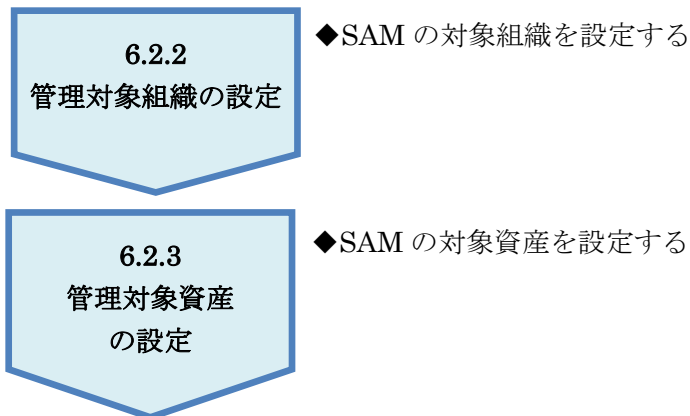


(上記番号は本ガイドブックの項番号を表す)

6.2. 事前準備

<事前準備の流れ>





(上記番号は本ガイドブックの項番号を表す)

6.2.1. SAM 導入目的の確認

まず初めに、組織として、SAM の導入目的を明確にしておくことが望ましい。目的を明確にする理由は、組織として達成すべき目的と目標を共有化するためである。組織としての SAM に対する方針が組織のマネジメントから示されることで、ユーザー部門の理解も得られやすくなる。SAM を実現するためには、SAM 担当の管理者だけでなく、マネジメント層・利用者に至る組織全体の協力が不可欠である。

なぜなら、SAM を実行するためには、SAM 担当者のアサインや、SAM を実行するために必要な予算の確保が求められること、ユーザの協力により SAM の構築・運用がうまくいくことからである。

SAM 導入の目的は、コンプライアンス、セキュリティの維持・向上、コスト削減（コストの最適化）などに分けられるが、目的は複数あっても問題はない。組織の目標や、組織が置かれている環境、状況に応じて設定することを推奨する。

6.2.2. 管理対象組織の設定

通常、SAM は組織全体を対象に実施することが求められるが、そうすることで、SAM の導入に大きな支障や遅延が生じる可能性がある場合、段階を踏んで導入することも考えられる（ただし、最終的には全組織を対象としなければ意味がないことは言うまでもないので、段階的に導入する場合には、全組織までに至るスケジュールまでを想定しておくことが望まれる）。

6.2.3. 対象資産の設定

管理組織の設定後、管理対象資産の設定を行う。管理対象資産として少なくとも考慮しなければならないのは「ハードウェア」、「導入ソフトウェア」、「ライセンス」、「ライセンス関連部材」である。これらの資産については個々人により認識が異なる場合がある為、本ガイドにおける定義を説明したい。

(1) ハードウェア

導入ソフトウェアを漏れなく把握したことを証明するためには、組織で保有するハードウェアを正確に把握することが必要である。

ソフトウェアはハードウェアに導入して利用される為、組織で保有するハードウェアを正確に把握しなければ、同じく、導入されているソフトウェアを正確に把握することはできない。ハードウェア数が把握できていない状態で導入ソフトウェア数を算出しても、その数の根拠となる網羅性を対外的に証明することはできない。

ハードウェア管理の対象資産は、単純に PC やサーバだけではなく、ソフトウェアが導入できるハードウェア、又はライセンスが付属するハードウェアをいう。ただし、ハードウェアのどこまでを管理の対象とするかは、組織によるリスクアセスメントの結果、定められるものである。

表 6-1 ハードウェア

資産名	主な対象資産	管理目的
ハードウェア	<ul style="list-style-type: none">ソフトウェアが実行できる機器 例：PC・サーバ・PDA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">ソフトウェアが導入できるハードウェアを明確にするライセンスが付属するハードウェアを明確にする

(2) 導入ソフトウェア

ライセンスを管理しようとする、保有しているライセンスの数が、導入ソフトウェア数を下回っていないかをいきなり調べる組織があるが、それは順番が違う。

導入しているソフトウェアをまずすべて把握し、それらのソフトウェアを導入するために必要なライセンスは何であるかを把握した上で、それに該当するライセンスをどれだけ保有しているかを調査するプロセスが正しい。こうして初めて、適切なライセンスに基づき、ソフトウェアが導入されていることを証明することができるようになる。導入の定義はベンダー・ソフトウェアにより変わるが、「ソフトウェアがハードウェアに導入（インストールだけを指すものではない。フォントや有償の画像データなどなどのように、単純にハードウェアに置いて使用されるものもある）された状態」を指す場合が多い。導入されたソフトウェアを利用しているか否かは、使用数の判断基準にはならない。

なお、導入ソフトウェア数の算出基準は、ハードウェアへの導入数だけでなく、搭載する CPU 数・利用人数など様々である。判別方法はライセンス証書・使用許諾契約書などに記載されている為、ソフトウェアを導入する前に必ず確認することが望まれる。

また、ソフトウェアの中には、「Web 閲覧履歴などの情報を外部に送信し広告を送ることを許諾する」ような条文が使用許諾条件に含まれているものもあるため、必ず使用許諾条件の事前確認を行い、組織として利用を許可するか確認することが必要である。

表 6-2 導入ソフトウェア

資産名	主な対象資産	管理目的
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

(3) ライセンス

導入ソフトウェアと同様、適切なライセンスに基づき、ソフトウェアが導入されていることを証明するためには、組織が保有するライセンスを管理することが求められる。

ライセンスの証明条件はベンダーやソフトウェアの種類により異なる。一般的に、ボリュームライセンスで購入されたものであればライセンス証書が、パッケージ・プレインストールで購入されたものであれば、購入時に付属してきた部材すべてがそろっていることが求められる。

ライセンス保有の証明条件を独自に判断してしまうと、ライセンス過不足数の判定に誤りが生じるため、独自に判断せず、ベンダーや販売会社、SAM 構築支援会社などに問い合わせ、確認することが望まれる。

表 6-3 ライセンス

資産名	主な対象資産	管理目的
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

(4) ライセンス関連部材

組織内で新規に導入されるソフトウェアを統制するためには、ソフトウェアを導入する為の媒体（ライセンス関連部材）を管理することが必要である。

ライセンス関連部材の対象資産は、ソフトウェアベンダーが定める保有条件を満たすライセンスに付属する媒体や、ライセンスを持たない導入専用の媒体のことをいう。具体的には、導入媒体（DVD や CD など）、ライセンス証書、CD キー、パッケージなどをいう。

手元にあるライセンス関連部材が、使用許諾条件を満たしていない場合には、一般的には、ライセンスの保有を証明することができない。このような状態で使用すれば、ライセンス違反となってしまうので、必要に応じて（下記参考を参照）適正に廃棄する必要がある。ただし、場合によってはベンダーに認められるものもあるので、廃棄する前に、やはりベンダーや、販売会社、SAM 構築支援会社などに問い合わせをしてみるのも良い。

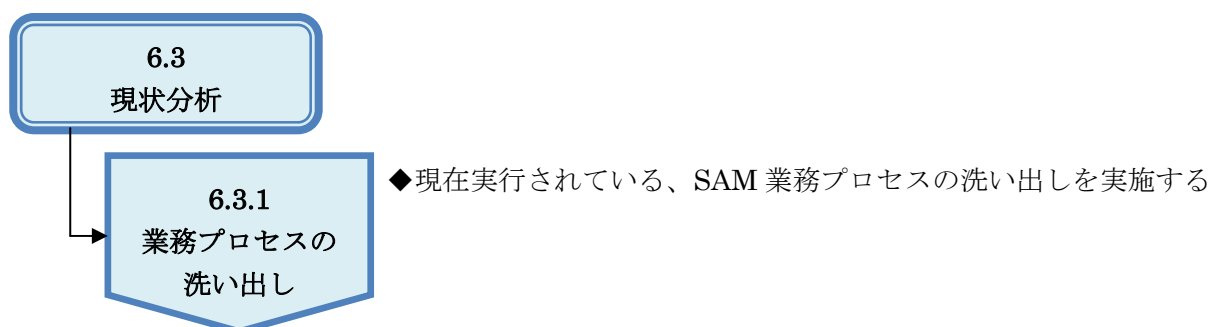
表 6-4 ライセンス関連部材

資産名	主な対象資産	管理目的
ライセンス関連部材	・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）	・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

＜参考：ライセンスの保有条件を満たさないメディアの取り扱いについて＞
 一部ベンダーでは、パッケージ版のメディアをボリュームライセンスの導入メディアとして利用できる場合がある。この場合、組織の判断で導入メディアとして転用ができる。ただし、ボリュームライセンスの導入メディアとして転用できない場合は、ライセンス違反の原因になるため廃棄することを推奨する。

6.3. 現状分析

＜現状分析の流れ＞



（上記番号は本ガイドブックの項番号を表す）

6.3.1. 業務プロセスの洗い出し

6.3.1.1. なぜ業務プロセスの洗い出しが必要か

現状把握で初めて行うべきことは、現在行われている業務プロセスの洗い出しである。

業務プロセスの洗い出しを行う理由は、関連資産の業務プロセスを把握、確認することで、どこにどのような資産があるのかを認識し、現状把握に漏れが出ないようにするためである。現状把握の際の、留意事項などもここで認識できる場合がある。

単に現状把握をするだけなのだから、組織内にある対象資産を単純に洗い出せばよいと考える組織もあるが、それは違う。

例えば、部門によっては、対象資産を他所に預けている場合がある。

また、顧客先に常駐している人員をたくさん抱えている部門がある場合がある。

逆に外部委託の人たちが多く常駐している部門がある。

リース期間が長すぎるので、PC のスペックが足りなくなり、満了前にも関わらず新規で調達したために、古いものを倉庫に大量に保管している場合がある。

以上はほんの一例だが、組織の中で対象資産がどのような状態にあるかを現状把握の前にある程度把握しておくことは、現状把握をより高い精度で実施するために重要であることを理解していただきたい。

また、事前の業務プロセスの洗い出しは、SAM の規程や手順を定める際にも役に立つ。例えば、以下の設問に回答できない場合、何らかの業務プロセスに問題が潜在しているということがわかる。もし、回答ができない設問が1つでもあった場合、一度現在の業務プロセスの見直しをされることを推奨する。

<参考：管理状況を判断する為の設問>

◆ハードウェア関連

- ①組織内で PC を何台保有していますか？
- ②①で回答した保有 PC 台数を証明する台帳を提示することはできますか？
- ③SAM ツールで取得した情報を②の台帳とされた場合、組織内で保有する PC に SAM ツールが漏れなく導入されていることを証明することができますか？
- ④新規に導入される PC を組織全体の管理を統括する担当者が漏れなく把握することができますか？
- ⑤PC が新規に導入されるまでの流れを、組織が認めた資料を利用して第三者に説明することができますか？

◆導入ソフトウェア関連

- ①組織内で利用されているソフトウェアを組織全体の管理を統括する担当者が把握することができますか？
- ②新規に利用するソフトウェアを漏れなく把握することができますか？
- ③ソフトウェアが新規に導入されるまでの流れを、組織が認めた資料を利用して第三者に説明することができますか？
- ④組織内で把握されているすべてのソフトウェアが、ライセンスの裏付けを持って利用されていることを第三者に証明できますか？

◆ライセンス関連

- ①組織全体の管理を統括する担当者が、組織内で保有されているライセンスを把握することができますか？
- ②把握されているライセンスはすべてライセンスの証明条件を満たしていますか？
- ③新規に購入するソフトウェアを漏れなく把握することができますか？
- ④ライセンスが新規に導入されるまでの流れを、組織が認めた資料を利用して第三者に説明することができますか？

<参考：他組織の管理状況>

様々な組織のソフトウェア資産管理状況を見てきた中で、上記設問にすべて回答できる組織は極めて少なかった。そのような組織でも、SAMなど自社のリソースでできて当たり前と考えられるマネジメントが多くみられた。

しかし、SAMを実現するためには、管理部門の努力だけでなく、経営陣からの資金・人的リソースの支援も必要になる。

他組織の状況を知り、自社の管理状況を客観的に判断することは、SAMの改善に役に立つと考える。そのため、本題から少しそれるかもしれないが、ここでは他組織の事例を紹介したい。

◆ハードウェア管理の現状

実際にSAMツールを導入して管理されている組織を対象に、実地棚卸で作業を行った場合、管理者が把握している機器数の1.2倍程度の機器が発見されるケースが多い。(保有機器数が1,000台と申告された組織を対象に棚卸を行った場合、平均で1,200台のPCが検出される) SAMツールはネットワークに接続された機器を対象に情報の取得を行うが、組織内にはスタンドアロンで稼働するPCや予備機、各部署の判断で購入したPCや、各部署で保有する余剰機など、SAMツールで把握できないPCを保有することで発生する。各部門での保有数が1台2台のレベルでも、それが積み重なり、保有機器数の1.2倍の機器数が発見されることになる。これはしかし、単純に2割多く見つかるということではない。顧客の管理台帳を基に、実際に現物と突き合わせをすると、台帳に記載されている中で見つかるものは、平均して60%程度しかない。したがって、正確に把握できているハードウェアの保有数は、わずか50%程度ということになる。

なお、インベントリーツールで自動収集されるハードウェアの数は、これまでの経験値から述べると、保有数の70%程度である。

◆導入ソフトウェア管理の現状

1) 膨大な種類のソフトウェアが検出される

導入ソフトウェアはSAMツールを使えば、情報を収集することはできる。しかし、何も導入制限がかけられていない組織の場合、保有機器数の約2~3倍程度の種類(本数ではない)のソフトウェアが検出される。

(1,000機器保有する組織の場合、2,000~3,000種類のソフトウェアが収集される)

これは、PCにプレインストールされているソフトウェア(ビジネス用のPCでも初期状態で20種類程度のソフトウェアが導入されている)やソフトウェアの関連ツールなど、管理者が意識せず導入されているものや、利用者が個人的に導入したソフトウェアが積み重なり、上記結果になる。

ここでポイントとなるのは、「収集されている=管理されている」ということではないということである。後で述べる現物との突き合わせができて初めて管理の骨組みが完成す

ることになる。

2) 管理者が把握していないソフトウェアが検出される

導入制限がかけられていない組織に対し、導入ソフトウェアの調査を行うと、必ず何かしらの私的導入ソフトウェアが検出される。よく検出されるものとして、スクリーンセーバーや壁紙などがある。それ以外にも、ゴルフや麻雀などのゲームから、ひどいものになるとクリアするまで数十時間プレイしなければならないようなゲームまで検出される場合もある。

◆ライセンス管理の現状

ライセンスは最も管理が難しい資産である。なぜなら、ライセンスといっても、同じソフトウェアでパッケージ・プレインストール・ボリュームライセンスなど種類と使用許諾条件が異なるうえ、一度ソフトウェアを導入してしまえば、ライセンスがなくてもソフトウェアは（コンプライアンスに違反はしていても）現実的に使えてしまうからである。そのため、同じソフトウェアを複数本購入したものの、保管場所がなかったために1本だけパッケージを残し残りは捨ててしまい、ライセンスを保有していることを証明できなくなったというケースも多い。

6.3.1.2. 現状の業務プロセスの洗い出し方法

管理対象資産として「ハードウェア」、「導入ソフトウェア」、「ライセンス」、「ライセンス関連部材」の四つが挙げられる。また、そのライフサイクルプロセスは、「取得」、「導入」、「異動」、「廃却」の四つに分けられる。そのため、図 6-1 のように最低限 16 のプロセスを策定することが求められる。

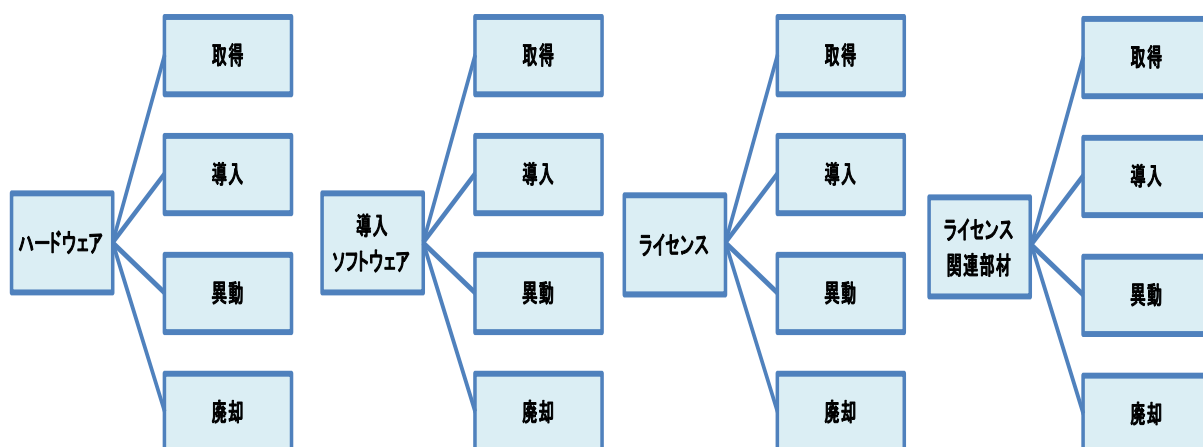


図 6-1 洗い出すべき業務プロセスの種類

業務プロセスを洗い出す方法は、組織の管理状況や業務プロセスに関連する資料の整備状況により異なる。業務プロセスを洗い出す方法として、図 6-2 のような業務フローや、図 6-3 のようなプロセスリストなどをまとめることを推奨する。業務フロー・業務プロセスリスト作成の詳細

手順は、インターネットや各種書籍などで紹介されているので、それらを参照していただきたい。

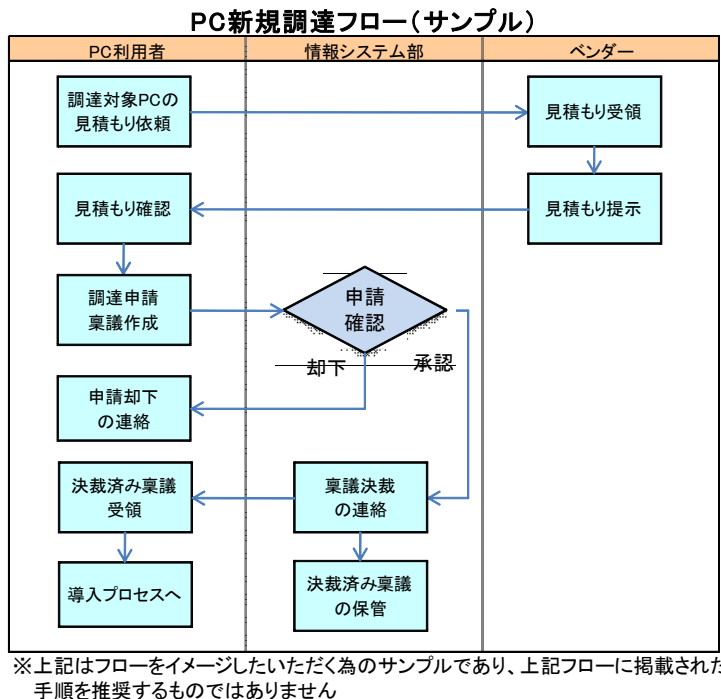


図 6-2 業務フローのイメージ

調 達	
1. ソフトウェアの選定	管理効率と業務効率のバランスを考慮したライセンスプログラムの策定。
2. 調達の妥当性確認	調達するソフトウェアの、そ曳屋ステークホルダーに対する適格性の確認。
	調達しようとするライセンス数の妥当性の確認。
	調達コストを市場価格等、他の調達手段や基準との比較。
	調達先の事業継続性の確認。
3. 調達情報の集中化	すべての対象資産の調達情報一元管理。 決済がSAMの管理部門以外となっている対象資産の調達情報の適時の入手。

↓

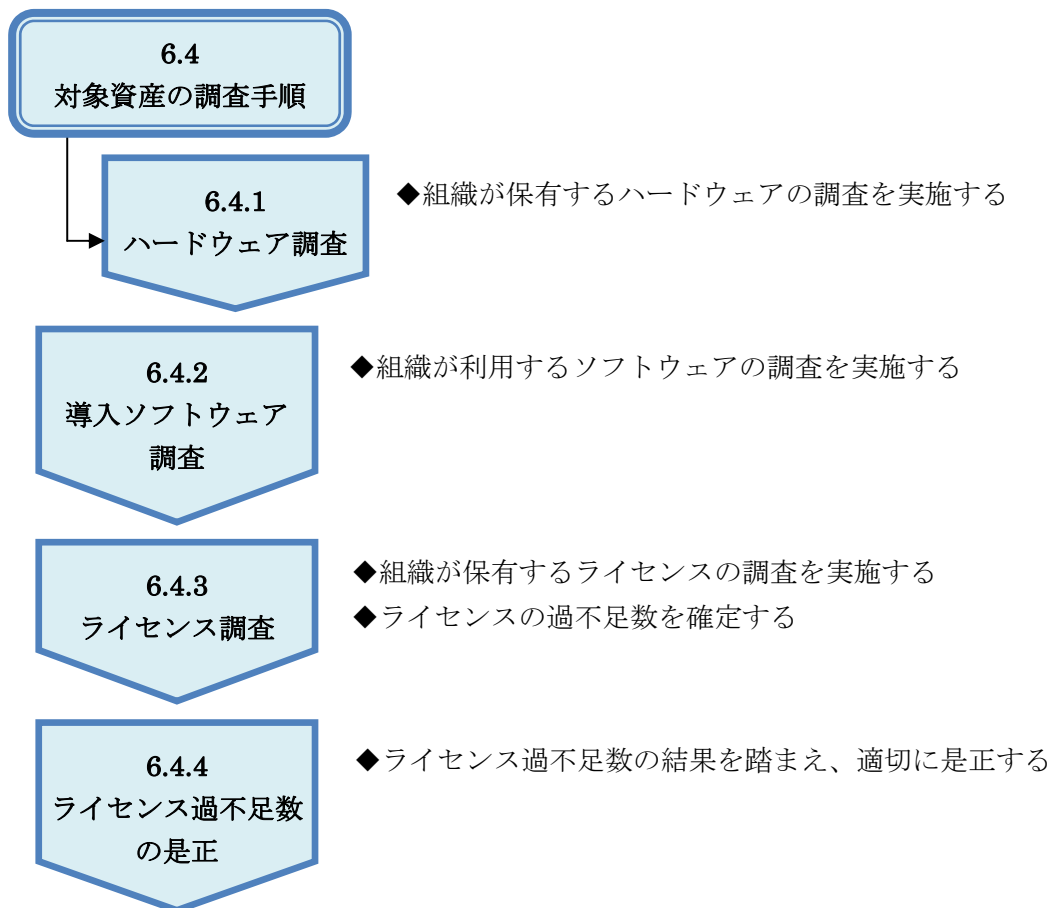
導 入	
1. 導入資産の識別	導入した対象資産を一意に識別する仕組みの構築。
2. 導入資産の記録	適時な記録 対象資産の納品を適時に捉える仕組みの構築。
	適正な記録 SAMの目的を達成するための必要管理項目の網羅。
	適正な記録 正確な情報を記録する仕組みの構築。 更新された情報が適切になされたものであることを確認する仕組みの構築。
3. 使用許諾条件の確認	導入した対象資産を一意に識別する仕組みの構築。

↓

図 6-3 プロセスリストサンプル (BSA P-SAM2009 資料より一部抜粋)

6.4. 対象資産の調査手順

<管理対象資産の把握の手順>



(上記番号は本ガイドブックの項番号を表す)

<参考：管理対象資産の把握手順について>

対象資産の調査を行う場合、①ハードウェア②導入ソフトウェア③ライセンスの順で調査を行うことを推奨する。なぜなら、図 6-4 のとおりはじめにハードウェアの調査を行うことで、他の調査対象の資産を絞り込むことができるからである。

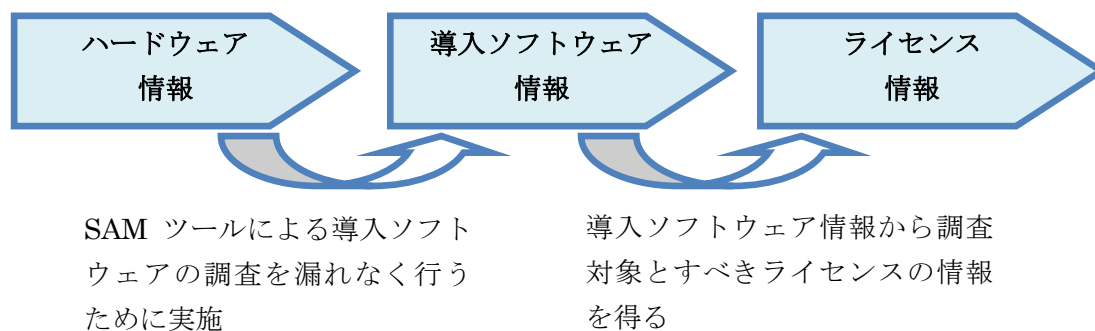
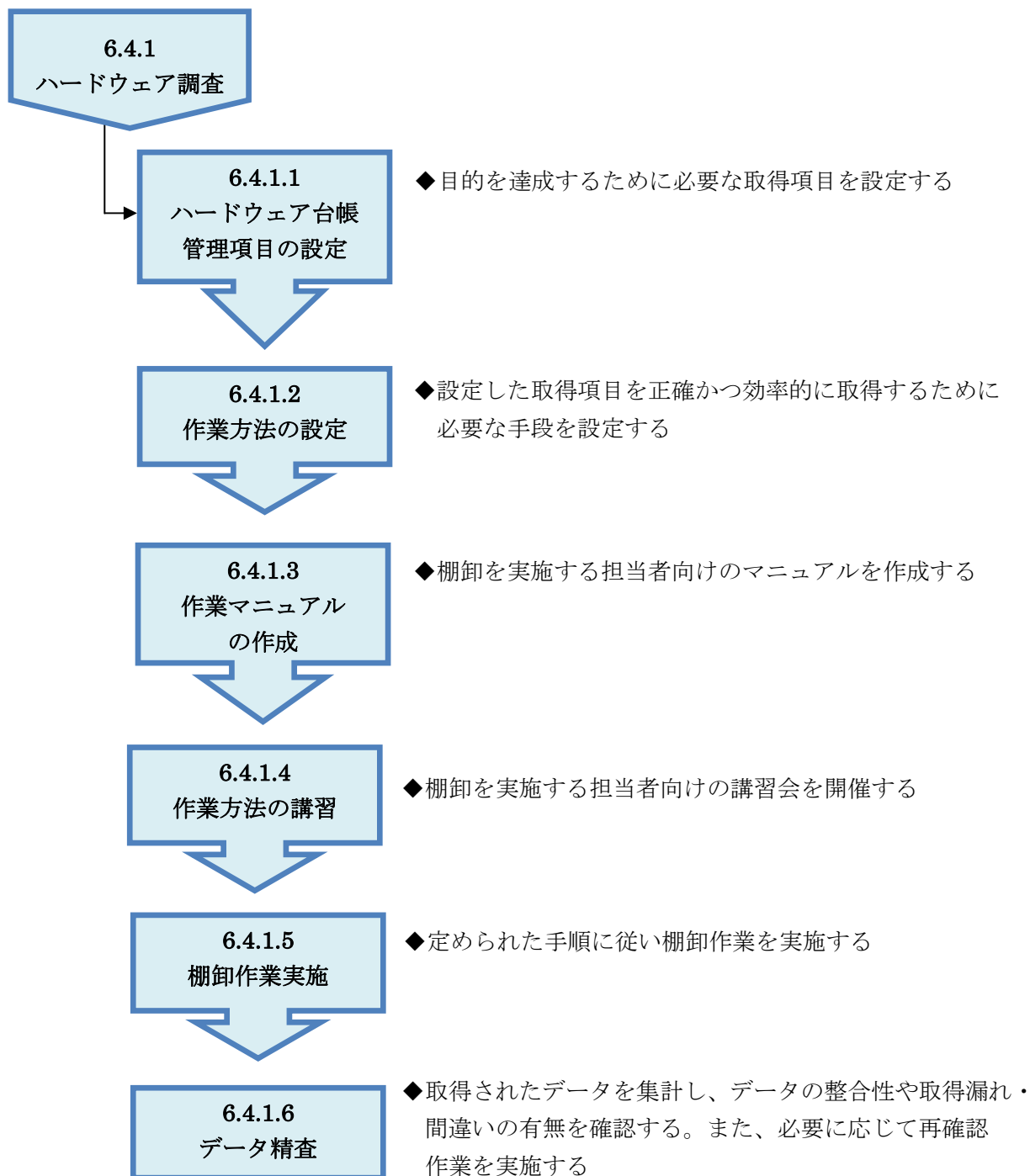


図 6-4 対象資産の調査手順

6.4.1. ハードウェア調査

< 実地棚卸実施の手順（例） >



(上記番号は本ガイドブックの項番号を表す)

表 6-5 ハードウェア調査

項目	詳細
作業を行う上での留意点	<ul style="list-style-type: none"> ・SAM ツールなどを利用してハードウェア情報を取得している場合でも、正確な情報の把握の為、実地棚卸で調査することを推奨する ・管理対象とするハードウェアを明確にした上で作業を行う
成果物	・組織が保有するハードウェアの一覧（ハードウェア台帳）

6.4.1.1. ハードウェア台帳管理項目の設定

管理項目は、表 6-6 ハードウェア台帳の管理項目を参照してほしい（各管理台帳の項目は、管理する資産の種類や、組織の管理方法などにより異なるが、ここでは、各管理台帳のサンプル項目として幾つかを挙げ、説明していく）。これら項目はあくまで、コンプライアンス・セキュリティを目的とした場合に、最低限取得すべき項目である。

実際に項目を設定する場合は、SAM の導入目的や、SAM 以外の IT 資産管理の目的を考慮し、設定した目標を達成するために必要な項目が網羅されていることを確認することが必要である。

表 6-6 <ハードウェア台帳の項目>

管理項目	項目内容
ハードウェア管理番号	当該ハードウェアに貼付する一意の管理番号。バーコードが付属していることが望ましい
機器種別	デスクトップ、ノートブック、プリンタ、サーバ、スキャナなど
ベンダー名	当該ハードウェアのベンダー名
型番	機種番号・タイプと書かれている場合もある、ハードウェアのベンダー区分による種別
シリアル	ベンダーが修理の際、要求する番号。もともと一意とは言い難いものであり、管理番号とすることはできない
利用者	当該ハードウェアの利用者
使用部門	利用者が所属している部署
管理者	当該ハードウェアの管理者。利用者と同一の場合もある
管理部門	管理者が所属している部署。使用部門と同一の場合もある
設置場所	当該ハードウェアが主に使用されている場所
スペック	CPU・CPU 数・メモリ・HDD 容量
前利用者	現利用者の前に当該ハードウェアを使用していた利用者(履歴)
前管理者	現管理者の前に当該ハードウェアを管理していた管理者(履歴)

6.4.1.2. 作業方法の設定

実地棚卸による調査は、組織内の人的・システムのリソースで調査する場合が一般的だが、内部リソースが不足している場合には、外部委託を利用する場合もある（次ページ「参考：管理対象資産の把握について」参照）。いずれの方法で調査を行う場合であれ、現状把握は人的作業によ

るものであり、作業手順を明確にしないと調査結果の精度が低くなることになるため、作業方法を設定する場合には、十分に留意する必要がある。

表 6-7 管理対象資産の把握

<参考：管理対象資産の把握について 1>

◆管理対象資産の調査方法

対象資産の調査方法の 3 パターンの内、どの方法が最適であるかは、組織の管理体制や物理的な設置状況・調査対象拠点の散らばり具合により異なる。いずれにしても、ここで重要になることは、対象資産の情報を正確に調査することである。

棚卸の業務負荷のみを考慮し、棚卸手順を深く検討せず、作業担当者への指示もメールの一斉送信で行ったため、想定していた情報を取得することができず、再度調査を行ったという事例は良くみられる。

そのため、いずれの手段で作業を行う場合でも、作業効率だけでなく、行おうとする手段で漏れなく正確に情報を取得することができるか検討することを推奨する。

調査方法	詳細な手段	メリット・デメリット
すべて組織内の リソースで調査	情報システム部など管理部門の人員のみで調査を行う	<メリット> ・調査作業を行う人員が限られるため、精度の高い調査ができる <デメリット> ・特定の人員に負荷がかかる
	機器の利用者に調査を依頼する	<メリット> ・作業負荷を分散することができる <デメリット> ・調査作業を行う人員が多くなるため、取得情報の精度を保つことが難しくなる
外部委託先を利用して調査	IT 機器の現地調査をサービスとして提供している企業に調査を委託する	<メリット> ・組織内の作業負荷が軽減できる <デメリット> ・委託費用が発生する
組織内・外部委託先で作業を分担	作業拠点や対象機器により組織内のリソースと外部委託先での調査を分担する	<メリット> ・作業負荷とコストを最適化することができる <デメリット> ・作業分担により、作業結果に対する責任があいまいになる可能性がある

<参考：管理対象資産の把握について 2>

◆対象資産の調査手段

対象資産の調査を行うに際し、もうひとつ考慮しなければならないことは、どのような手段で調査を行うかである。一般的な調査手段として、「人手による調査」と「ツールによる調査」の二つが挙げられる。それぞれ調査対象とする資産や項目、作業負荷に差が生じるため、それぞれの特徴を理解した上で最適な調査方法を選択することが求められる。

調査方法	調査に適した資産	メリット・デメリット
人手による調査	<ul style="list-style-type: none">ハードウェアの所在把握ライセンス	<p><メリット></p> <ul style="list-style-type: none">機器の環境、稼動状況に関わらず調査を行うことが可能 <p><デメリット></p> <ul style="list-style-type: none">作業負荷が高い
SAM ツールによる調査	<ul style="list-style-type: none">ハードウェアのスペック（含むネットワーク情報など）把握導入ソフトウェア	<p><メリット></p> <ul style="list-style-type: none">少ない作業負荷で調査をすることが可能 <p><デメリット></p> <ul style="list-style-type: none">機器の環境・稼動状況により調査ができない場合がある調査できる項目が限られる

6.4.1.3. 作業マニュアルの作成

作業マニュアルは、作業者に作業手順を伝える重要なコンテンツである。作業マニュアルのできが悪いと、作業に混乱や間違いが生じ、求める作業結果を得られなくなる。作業者に正確な作業を実施してもらうためには、最低限下記の条件を考慮することを推奨する。

(1) できる限り詳細に作業内容を定義する

どんなに単純な作業内容を記したマニュアルでも、読む人により異なる作業内容を想像する可能性が生じる。また、作業実施時に思いもよらぬ事象が生じる可能性もある。

作業手順をできるだけ詳細に設定することで、作業のばらつきを抑えることができる。考えられる事象を極力マニュアル上に網羅することで、棚卸作業時に生じる作業者による作業レベルの差異を減少させ、網羅性と正確性の担保された作業品質を得ることができる。また、これにより、結果的に管理者の業務負荷を軽減することもできるし、調査内容を対外的に説明することもたやすくなる。

(2) 作業者のレベルに合わせてマニュアルを作成する

同じ組織内でも、IT の知識レベルの差が大きいのが一般的である。作成するにあたり、作成者自身がわかる作業マニュアルではなく、作業をする人が理解できる作業マニュアルを作成しないと、作業内容を正確に伝達することができず、作業内容にばらつきが生じる原因になる。

6.4.1.4. 作業方法の講習

作業方法の講習の目的は、作業者に棚卸実施の目的と作業内容を伝え理解してもらうことである。

作業方法の講習を簡単に行うため、メールで作業内容を一斉送信すれば指示だけ是可以。しかし、作業者が作業内容を理解し、正しく作業を行わなければ意味がないし、メールだけで、作業の意図を明確に伝達することは難しい。そのため、手間はかかるが、できれば対面で説明し、作業目的と内容を正しく理解させることを推奨する。

メールや通達だけで現状把握を実施させて組織の多くは、結局、作業精度の低さから、作業のやり直しを余儀なくされていることをお伝えしておきたい。

6.4.1.5. 棚卸の実施

利用者に作業を依頼して調査を実施する場合、作業期間として 2 週間ぐらいとることを推奨する。1 週間だと利用者が夏休みなどの長期休暇を取っている場合、期間中に作業を行うことができなくなる。調査期間を 2 週間とすることで、作業開始から 1 週間経過した後、作業状況の確認作業を行い、作業未実施者に督促をかけることで作業実施漏れを防ぐことが可能になる。

作業期間中に、作業員から問い合わせを受けた場合、問い合わせ内容とその回答を、組織全体で共有することを推奨する。情報の共有を行うことにより、同様の問い合わせの発生を防ぎ、作業内容を統一することで調査の精度を上げることができるようになる。

6.4.1.6. データの精査

棚卸で取得したデータは、必ず精査することを推奨する。実地棚卸は人が行う作業のため、どんなに注意をしても、間違いが生じる可能性があるからである。どのような条件で精査作業を行うかは、取得項目や取得手段により異なるが、以下に一例を紹介する。

(1) 調査漏れの確認（調査漏れを無くす）

- ・ 調査すべき資産が漏れなく調査されているか
- ・ 調査対象項目が漏れなく調査されているか
- ・ 取得されていない項目は、理由が明確になっているか

(2) データ不整合の確認（同じ情報間の不整合をなくす）

- ・ ベンダー名の日本語・英語表記、フルネーム・略式名など、同じ情報で異なる表記がされていないか

（例：Microsoft やマイクロソフトなど）

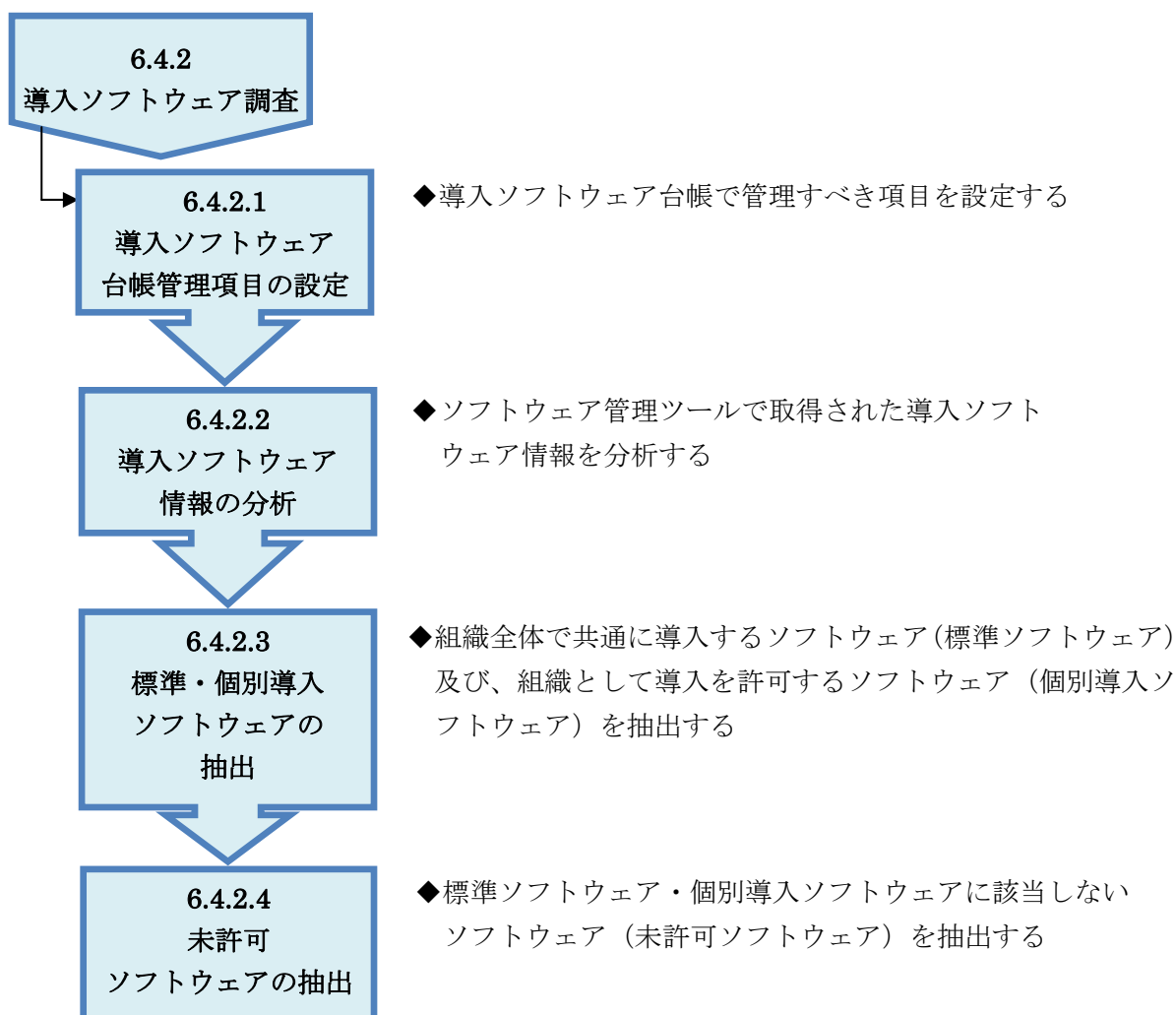
- ・情報の記入漏れにより、他の情報と混在して登録されていないか
(例：AutoCAD LT を AutoCAD として取得。AutoCAD と AutoCAD LT は異なる商品として存在する)

(3) データ不備の確認 (誤った情報を正しい情報に修正する)

- ・指定された項目に、指定以外の情報が記載されていないか (例：型番の記載欄にシリアルが記載されているなど)
- ・取得情報の書き間違いやスペルミスが含まれていないか

6.4.2. 導入ソフトウェア調査

<導入ソフトウェア調査の流れ>



(上記番号は本ガイドブックの項番号を表す)

表 6-8 導入ソフトウェア調査

項目	詳細
成果物	<ul style="list-style-type: none"> ・ 導入ソフトウェア台帳 ・ 標準・個別導入ソフトウェア一覧

6.4.2.1. 導入ソフトウェア台帳管理項目の設定

管理項目は、下記導入ソフトウェア台帳の管理項目を参照してほしい。これら項目はあくまで、コンプライアンスと情報セキュリティの維持・向上を目的とした場合に、最低限取得すべき項目である。

実際に項目を設定する場合は、SAM の導入目的や、SAM 以外の IT 資産管理の目的を考慮し、設定した目標を達成するために必要な項目が網羅されていることを確認することが必要である。

また、SAM ツールで取得された情報のみでは、下記項目を満たすことができないため、必要に応じて個別に情報を追加することが求められる。

表 6-9 <導入ソフトウェア台帳の管理項目>

管理項目	項目内容
ソフトウェア管理番号	当該ソフトウェアをデータ上一意に認識するための番号
ハードウェア管理番号	同左
導入名称	プログラムの追加と削除に表示されているソフトウェアの名称
ベンダー名	当該ソフトウェアのベンダー名(ライセンス台帳と同じ)
ソフトウェア名	当該ソフトウェアの名称(ライセンス台帳と同じ)
エディション	たとえばマイクロソフト Office で言えば、Standard とか Professional をいう(ライセンス台帳と同じ)
バージョン	たとえばマイクロソフト Office で言えば、2003 とか 2007 をいう(ライセンス台帳と同じ)
種別	製品版・フリーウェア・シェアウェア・ドライバなどソフトウェアを利用するために必要になるライセンスの種類を判別するもの
ライセンス管理番号	ライセンスを一意に認識するための番号(ライセンス台帳と同じ)
媒体管理番号	導入するための媒体を一意に認識するための番号
導入元	導入をした際に利用した媒体やイメージの情報
導入日	当該PCに導入された日

※主な使用許諾条件と使用数の集計方法は以下のとおり

使用許諾条件	説明
クライアントライセンス	PCなどのハードウェア1台に対して1ライセンスが消費される
サーバーライセンス	サーバ1台に対して1ライセンスが消費される クライアントライセンスと考え方は同じ
ユーザーライセンス	ソフトウェアを利用する利用者1人に対して1本ライセンスが消費される
CPUライセンス	ソフトウェアが導入されたハードウェアに搭載された物理的なCPU数1個に対して1ライセンスが消費される
クライアントアクセスライセンス (デバイス)	サーバにアクセスする1台のデバイスに対して1ライセンスが消費される
クライアントアクセスライセンス (ユーザー)	サーバにアクセスする利用者1人に対して1ライセンスが消費される
包括ライセンス	契約対象の組織全体で保有するPC台数や従業員数の把握が必要 ※ベンダーとの契約条件により、把握すべき要件が変わる

6.4.2.2. 導入ソフトウェア情報の分析

ハードウェアに導入されているソフトウェアの調査を行う場合、通常、SAMツールを利用する。SAMツールの選定については、7.SAM運用上のポイントで紹介されているため、ここではSAMツールで情報が取得された状態を想定して説明を行いたい。

SAMツールで情報を取得した後、導入ソフトウェア情報の分析を行う。ここでいう分析とは、導入ソフトウェア情報に「ソフトウェアベンダー」、「ソフトウェア種別」情報を追加する作業を指す。

ソフトウェアベンダーの特定とは、SAMツールで検出されたソフトウェアごとにライセンスを許諾するベンダーを特定することである。ベンダーを特定することで、この次のステップで行うライセンス調査の手がかりを得ることができる。

ソフトウェア種別の特定とは、ソフトウェアを例えば、下表のようなカテゴリに分類することである。この分類はその後説明する「標準ソフトウェア」、「個別導入ソフトウェア」、「未許可ソフトウェア」を選別するために利用する（もちろんこの分類は、組織によって別に定められても構わない）。

表 6-10 <主なソフトウェア種別>

分類名	説明
製品版	有償のライセンスを必要とするソフトウェア ※有償のライセンスであれば、その購入形態（パッケージ・ボリュームライセンス・ネット上からダウンロード）は問わない
フリーウェア	無償のライセンスを必要とするソフトウェア
HOTFIX	OS やブラウザ・アプリケーションソフトウェアの修正のためにベンダーから配布されるソフトウェア
その他	下記のいずれかに該当するソフトウェア ・ Exe の説明 ・ β 版 ・ インストーラ ・ サービス提供ソフト ・ サブスクリプション ・ ドライバ ・ マニュアルなど ・ 会員配布 ・ 更新版 ・ 製品の機能 ・ 体験版/評価版/試用版 ・ 周辺機器に付属するソフト
アドウェア	・ Symantec など、ワクチンソフトベンダーの HP に登録がされているソフトウェア ・ オプトメディア（導入後に外部サイトに Web 閲覧履歴などを流すソフトウェア）
不明	種別が特定できなかったソフトウェア

6.4.2.3. 標準・個別導入ソフトウェアの選定

導入ソフトウェア情報の精査完了後、組織として優先的に管理すべきソフトウェアを選定する。ここで重要になるのは、「優先的に管理すべき」というワードである。すべてのソフトウェアを同じ優先順位で管理しようとする、管理が始まるまで膨大な時間を要する。

そのため、表 6-11 のように標準ソフトウェア・個別導入ソフトウェアなど、優先的に管理すべきソフトウェアを設定し、それらソフトウェアの把握・管理が完了した後、管理対象を未許可ソフトウェアに順次拡大することを推奨する。

表 6-11 標準、個別導入ソフトウェアの選定

ソフトウェアの種類	内容
標準ソフトウェア	組織で標準的に利用するソフトウェア。一般的に、SAM の統括管理部門で一括管理されるもの。 例：MS Office, Adobe Reader, 圧縮解凍ソフトウェアなど
個別導入ソフトウェア	組織で標準的に利用しないが、利用者が個別に申請をし、導入が許可されるソフトウェア。一般的に、部門ごとに設定され、管理されるもの。 例：グラフィックソフトなど

未許可ソフトウェア	管理者の導入許可を受けていないソフトウェア 例：スクリーンセーバーなど
禁止ソフトウェア	組織として導入を禁止するソフトウェア 例：P2P ソフトウェア、ゲームソフトなど
パッチ・HOTFIX 類	OS やブラウザなどの修正ソフトウェア

6.4.2.4. 未許可ソフトウェアの抽出

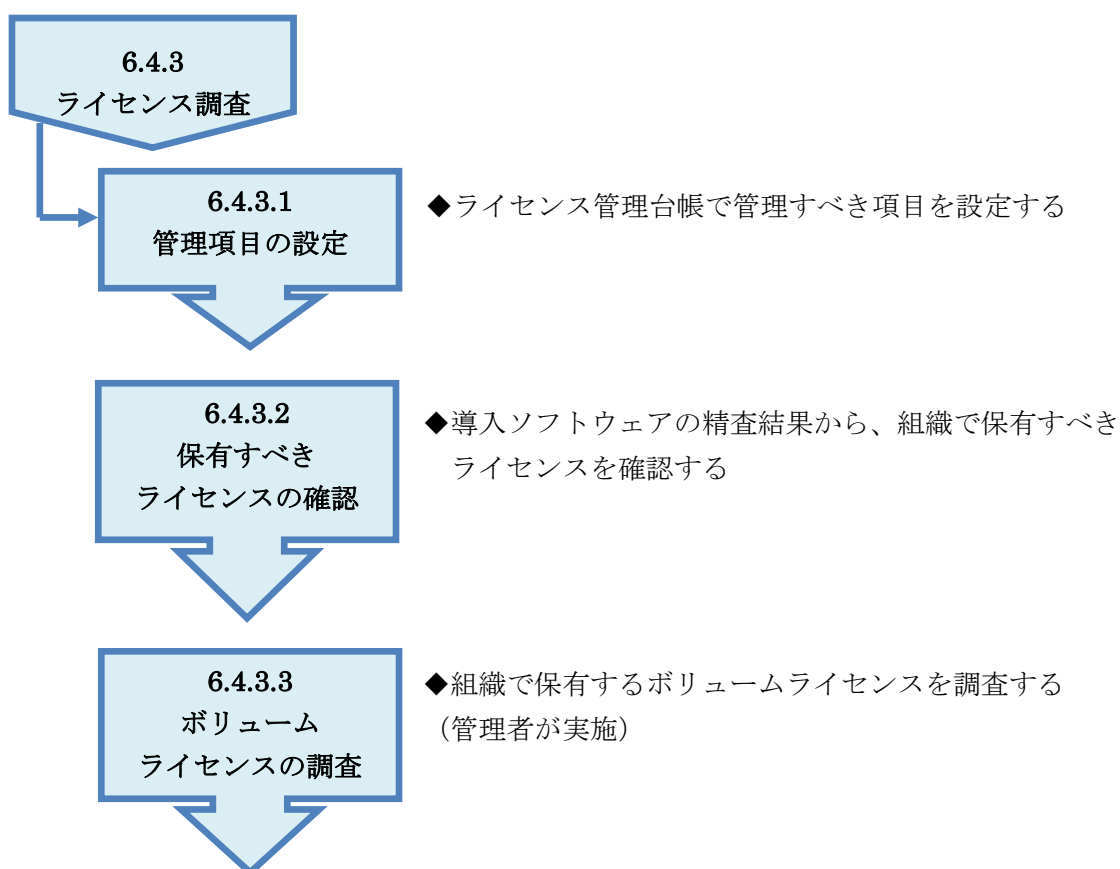
初めて未許可ソフトウェアを設定する場合、導入許可に指定すべきソフトウェアが含まれる可能性もある。そのため、未許可ソフトウェアを、個別導入ソフトウェアに変更する為のプロセスを構築しておくことを推奨する。

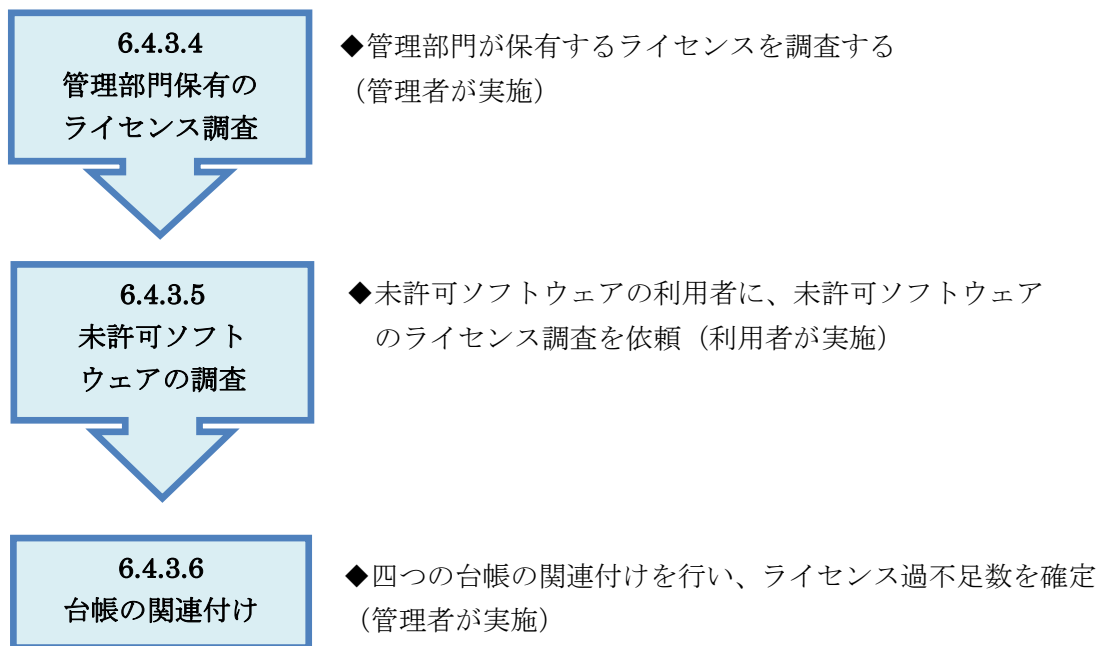
その際に重要なことは、「ソフトウェアの導入目的を明確にする」「申請者にライセンスの保有証明条件を確認させる」ことである。

ソフトウェアの導入目的を明確にするのは、組織としてソフトウェアの要否を判断するためである。また、申請者にライセンスの保有証明条件を確認させるのは、ライセンスに対する意識付けをするため、及び管理者の業務負荷を下げるためである。

6.4.3. ライセンス調査

<ライセンス調査の手順>





(上記番号は本ガイドブックの項番号を表す)

表 6-12 ライセンス調査

項目	詳細
成果物	<ul style="list-style-type: none"> ・ライセンス台帳 ・ライセンス関連部材台帳 ・四つの台帳の関連付け結果 (ライセンス過不足数の算出)

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

管理項目は、表 6-13 ライセンス台帳の管理項目を参照してほしい。ライセンス台帳の管理項目は、ソフトウェアの使用許諾条件や本数など、組織が保有するライセンスの内容・許諾条件・保管場所を特定できる情報とすることが求められる。

表 6-13 <ライセンス台帳の項目>

管理項目	項目内容
ライセンス管理番号	ライセンスを一意に認識するための番号
ベンダー	当該ソフトウェアのベンダー
ソフトウェア名	当該ソフトウェアの名称
エディション	たとえばマイクロソフト Office で言えば、Standard とか Professional をいう
バージョン	たとえばマイクロソフト Office で言えば、2003 とか 2007 をいう
言語	ライセンスで使用が許諾されている言語

購入日	いつからその使用許諾が有効になったのかを把握するもの
購入元	購入の履歴を証明してもらう際の連絡先
購入部門	購入経緯や購入履歴を確認する際に必要なもの
購入者	同上
ライセンス種別	パッケージでの購入か、ボリュームライセンスか？ボリュームライセンスであれば、どのような種類のものか？
ライセンス形態	フルライセンスなのか、アップグレードライセンスなのか？
使用許諾条件	ライセンスの単位。たとえば、クライアントライセンス・ユーザーライセンス・CPUライセンスなど
使用許諾証明	パッケージであれば、パッケージ及び同梱物など、使用許諾を証明する際に必要となる物品・情報
ライセンス証書番号	使用許諾を証する番号
数量	使用許諾されている数量
管理部門	当該ライセンスの管理責任部署
保管場所	当該ライセンスの保管場所
元ライセンス管理番号	当該ライセンスが有効なフルライセンスでない場合に、その基となるライセンス。例えばアップグレードライセンスの元となるフルライセンス
その他付帯条件	サブスクリプション(年間契約)・ダウングレード可否・プラットフォーム(Windows / Mac)など
更新予定日	期限付きライセンス契約の場合の更新日

「ライセンス関連部材台帳」は、ライセンス許諾条件を満たすために必要な部材（媒体など）を管理する為の台帳である。項目として、組織が保有するソフトウェアの媒体・保管場所と、ソフトウェアを導入するために必要な情報（CD キー）などの情報を登録することが求められる。

表 6-14 <ライセンス関連部材台帳の項目>

管理項目	項目内容
ライセンス管理番号	ライセンスを一意に認識するための番号
媒体管理番号	導入するための媒体を一意に認識するための番号
CD キー	ソフトウェアを導入する際に入力求められるキー
管理部門	当該ライセンス付属物の管理責任部署
保管場所	当該ライセンス付属物の保管場所
備考	備考

6.4.3.2. 保有すべきライセンスの確認

ライセンス調査の前に行うべきことは、組織で保有すべきライセンスとその数量を確認するこ

とである。

そのために実施することが、前述した「標準・個別導入ソフトウェアの選定」であり、これによって選定されたソフトウェアを利用するために必要なライセンスを調査することになる。

保有しているライセンスをどれだけ利用しているかではないことに注意してほしい。これでは、一部のライセンスの過不足のみしか把握することができず、コンプライアンスの要件を満たさない。

保有すべきライセンスとその数量を明確にした上で調査を行うことが重要である。

6.4.3.3. ボリュームライセンスの調査

ソフトウェアベンダーに問い合わせをすれば、組織で保有するライセンスの一覧を提出してくれる場合がある。効率的に作業を行う為、組織内の調査を行う前に、導入するソフトウェアのベンダーに問い合わせることを推奨する。

6.4.3.4. 管理部門が持つライセンスの調査

ボリュームライセンスの情報入手後、管理担当部門が持つパッケージ・プレインストールライセンスの調査を行う。

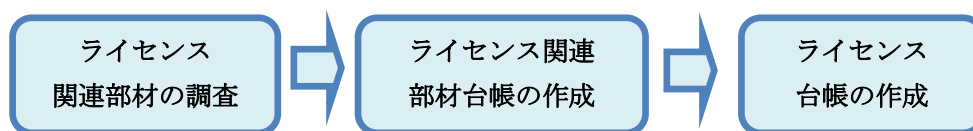
管理担当部門を対象にするのは、一般的に標準ソフトウェアや個別導入ソフトウェアのライセンスが集中して管理されている可能性が高いからである。

<ライセンス調査の手順>

初めてライセンス調査を実施する場合に限り、ライセンスの保有条件を満たしている、いないに関わらず、存在するライセンス関連部材をそのまま調査することを推奨する。

ライセンス関連部材（パッケージ・メディア・証書）が分散してしまっている場合もあり、とりあえず調査の時点では、使用許諾条件に沿っているかどうかは確認せず、すべて把握した後に判断するプロセスを持つことが望ましい。その上で、ライセンス管理台帳を策定する。このようにすることで、図 6-5 のように効率的に台帳を作成することができる。

<効率的なライセンス台帳の作成>



使用許諾条件を満たしてい
るものを抽出

<非効率なライセンス台帳の作成（同じ調査を2回行う必要がある）>

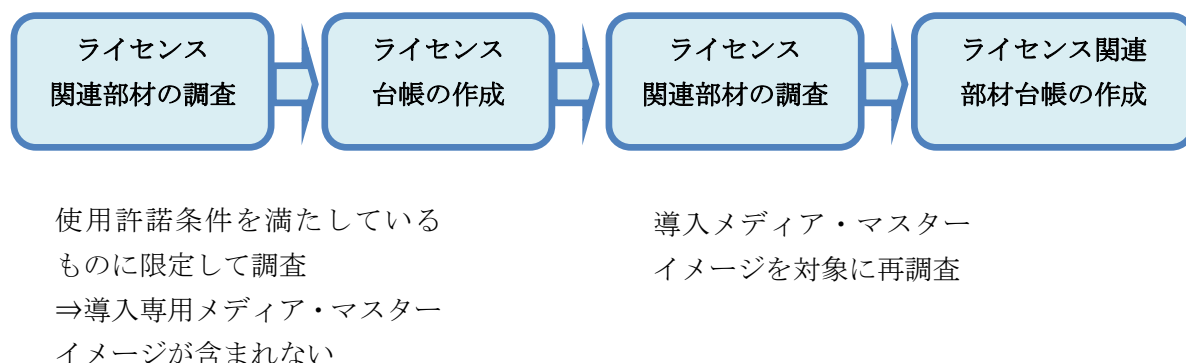


図 6-5 資材の調査結果とライセンス台帳・ライセンス関連部材台帳の関係

6.4.3.5. 未許可ソフトウェアの調査

未許可ソフトウェアの調査は、そのソフトウェアを利用している者に行わせることを推奨する。

これによりソフトウェアが管理されていることを利用者に認識させ、ソフトウェアの無断導入を抑止する効果にもつながる。

もともとが、利用者個人が勝手に導入したソフトウェアであり、これを利用者に調査させることで、管理者の作業負荷軽減にもなる。

6.4.3.6. 台帳の関連付け

ライセンス調査完了後、ライセンスと導入ソフトウェアの比較を行い、ライセンス過不足数を確定させる。ライセンスによっては、ソフトウェアが導入されているハードウェアごとに、ライセンスを関連付けることが求められるもの、利用しているユーザごとにライセンスを関連付けることが求められるものなど、様々なものがある。

ライセンスの過不足は、こういった使用許諾条件を踏まえて算出しなければならない。

ライセンス過不足数算出の方法の一例（図 6-6）を紹介する。この表は Excel 上で作業を行うことができ、かつダウングレードやライセンス種別ごとの管理も行うことができる。

なお、ソフトウェアの名称が、「ソフトウェア名」「エディション」「バージョン」に分解されているが、これは導入ソフトウェア名・ライセンス名を集計しやすくするためと、ダウングレードの調整をしやすくするために設定している。

ソフト名	エディション	バージョン	種別	ライセンス数	インストール数	過不足数	調整	調整番号	最終過不足数
Office	Professional	2007	VL	25	0	25	-25	1	0
			FPP	5	0	5			5
			PIPC	0	24	-24			-24
		2003	VL	0	25	-25	25	1	0
			PIPC	0	7				-7

ライセンスの契約種別を管理

VL : ボリュームライセンス

FPP : パッケージ

PIPC : プレインストール

調整: ダウングレードや同じバージョン内でのライセンスの調整を実施

調整番号: ライセンス過剰・不足の相殺を行った関係を示す番号

ライセンス許諾条件に従い過不足数を算出。

例: FPP が 5 本余っているが、PIPC には適用できないため不足とする

図 6-6 ライセンス過不足数の一覧表

<調整番号 1 が行っている処理>

- ①Office Professional 2007 のボリュームライセンスが 25 本過剰
- ②Office Professional 2003 で 25 本の不足が発生
- ③Office Professional 2007 の過剰ライセンス 25 本をダウングレードし、②の不足と相殺

総数レベルでライセンス過不足数の算出が完了した後、各台帳の関連付けを行う。本ガイドブックに掲載された各台帳の項目が網羅されていれば、図 6-7 に掲載したような関連付けを行うことができる。

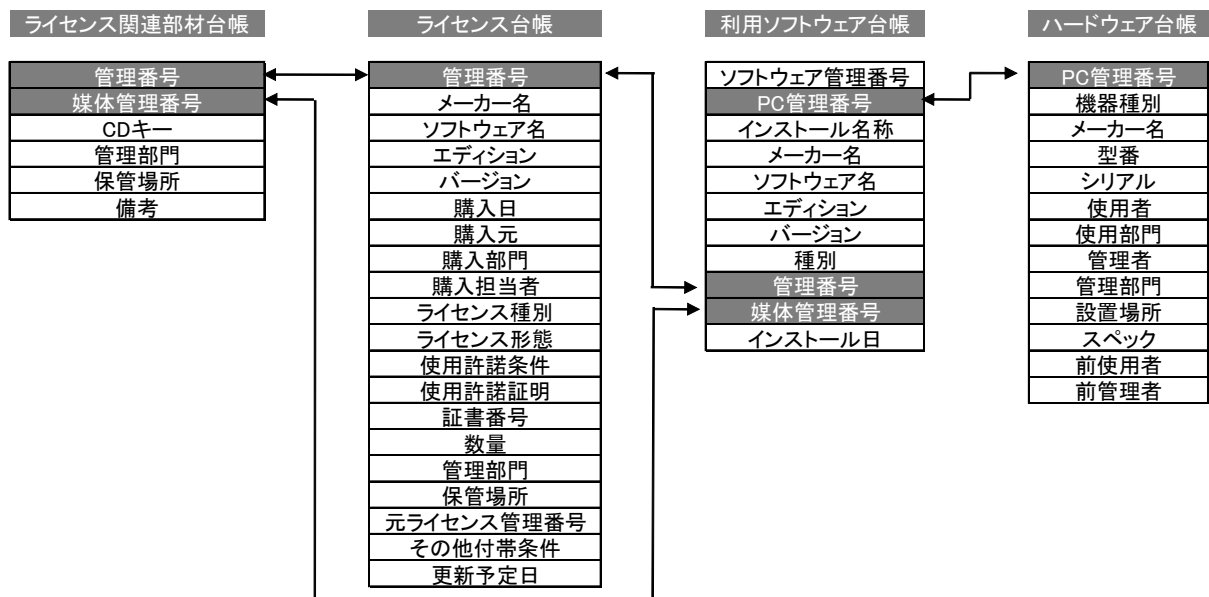
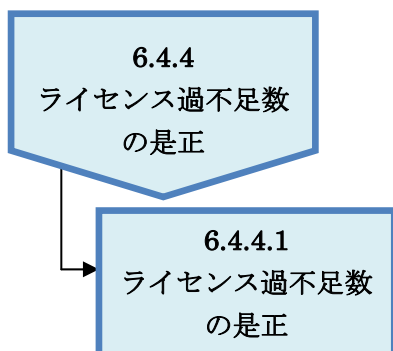


図 6-7 各台帳の関連図

6.4.4. ライセンス過不足数の是正



(上記番号は本ガイドブックの項番号を表す)

6.4.4.1 ライセンス過不足数の是正

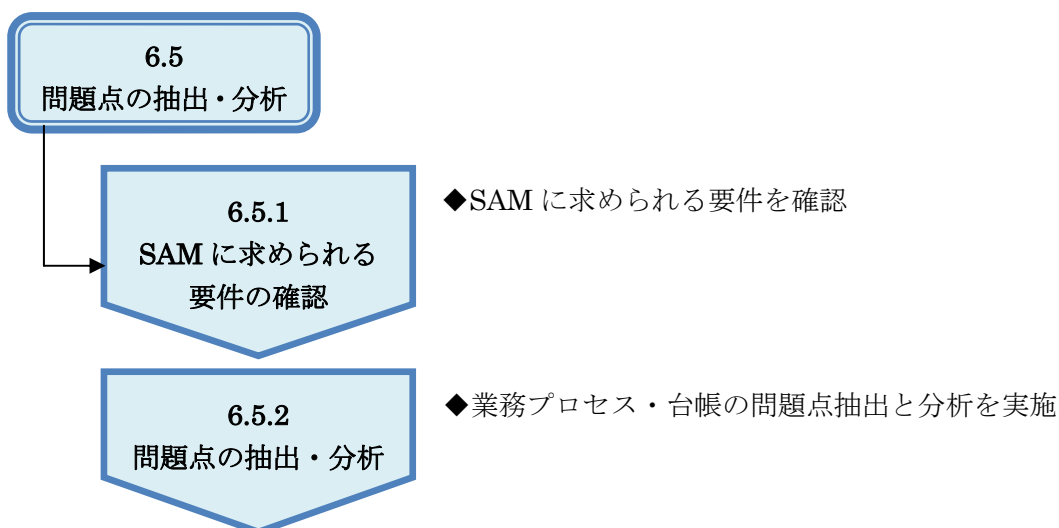
ライセンス過不足数の是正でポイントになるのは、ライセンス不足となったソフトウェアの取り扱いである。製品版の場合、ライセンス不足の解消を目的とした削除を行ってしまうと、証拠隠滅罪（不正に使われているという証拠を消し去ってしまうため）が適用される可能性がある。

表 6-15 <ライセンス過不足数の是正方法例>

ライセンス状況	ソフトウェアの種類	是正の方針例
過剰	標準ソフトウェア	管理部門が過剰ライセンスをプールし、新規導入時に再利用
	個別導入ソフトウェア	
	未許可ソフトウェア	

不足	標準ソフトウェア	管理部門が不足ライセンスを購入
	個別導入ソフトウェア	ソフトウェアを導入する導入者、又は導入者が所属する部門がライセンスを購入
	未許可ソフトウェア	<ul style="list-style-type: none"> ・フリーウェアの場合、使用許諾条件を確認した上で削除 ・製品版の場合、導入者又は導入者が所属する部門がライセンスを購入したうえで、ソフトウェアを削除（ライセンスは管理部門が管理）又は、ベンダーの許可を取った上で削除

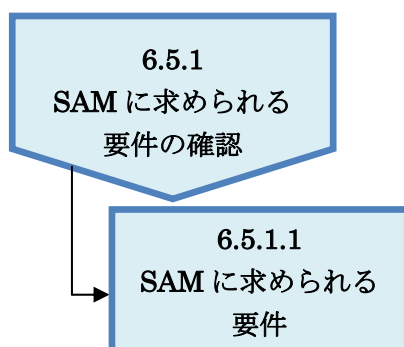
6.5. 問題点の抽出・分析



（上記番号は本ガイドブックの項番号を表す）

6.5.1. SAMの業務プロセスに求められる要件の確認

<SAMの業務プロセスに求められる要件>



（上記番号は本ガイドブックの項番号を表す）

6.5.1.1. SAMに求められる要件

業務プロセスの洗い出し及び現状把握の完了後、業務プロセスの見直しを行う。見直しを行う際のポイントは以下のとおり。

(1) 管理対象の組織・資産の情報が集中されていること

SAMの管理の形としては、集中管理か分散管理又はそのハイブリッドが存在するが、いずれの場合にも、組織全体の管理状況は把握できていることが求められる。

組織により、部門に管理を委任している場合が見られるが、その場合でも部門が持つ情報を管理者に集中し、ハードウェア・導入ソフトウェア・ライセンスすべての資産情報が把握できるプロセスを整備することが求められる。

なぜなら、SAMの問題は、それが発生した場合、その影響が組織全体に及ぶものだからである。

経営者や管理責任部門が、各部門に管理を丸投げしている状態は、分散管理とは言わない。

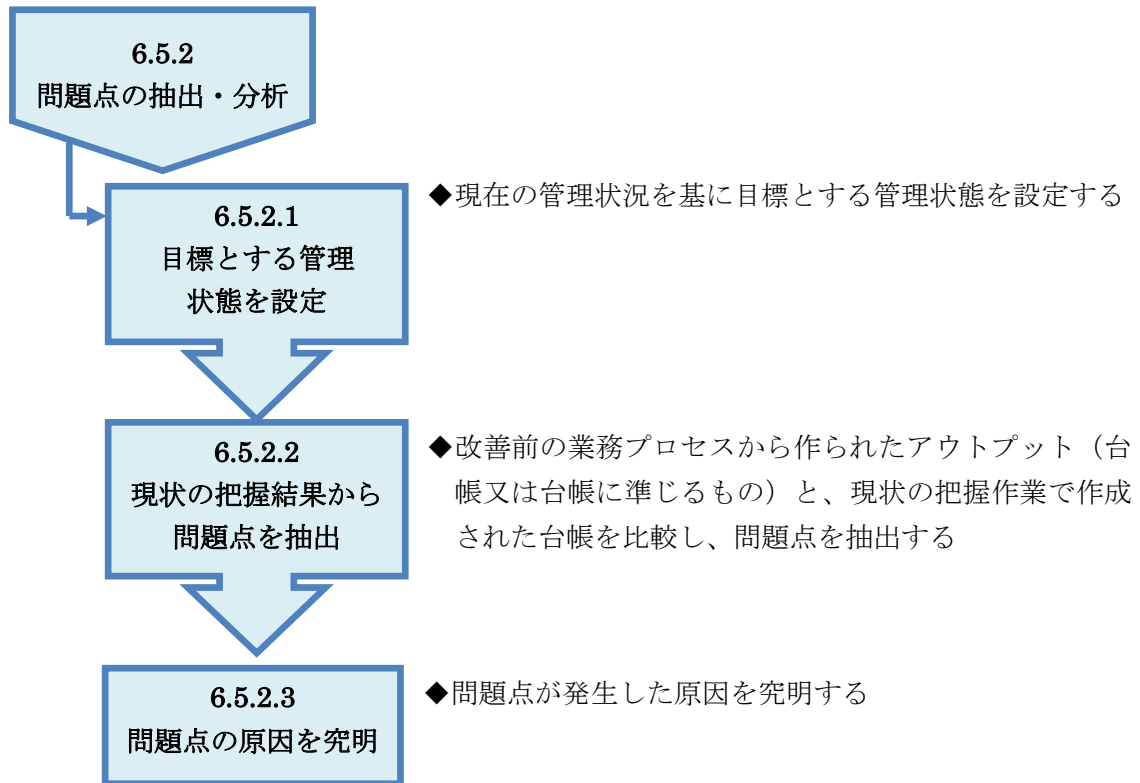
(2) SAMに求められる要件が満たされていること

SAMに求められる要件は、必須要件と推奨要件の二つに分けられる。必須要件は、ベンダーが定めた使用許諾契約条件であり、推奨要件はISO/IEC 19770-1、ソフトウェア資産管理基準などである。

ベンダーが定めたソフトウェア使用許諾条件は、コンプライアンスに関係する為、最低限守ることが求められる。

ISO/IEC 19770-1やソフトウェア資産管理基準は、条件を満たすことを法的に義務付けられてはいないが、これら基準には適切なソフトウェア管理を行う上で満たすべき要件がまとめられており、これを参考に組織の管理方針や体制、規程などを整備することを推奨する。

6.5.2. 問題点の抽出・分析



(上記番号は本ガイドブックの項番号を表す)

6.5.2.1. 目標とする管理状態の設定

すべての情報収集完了後、目標とする管理状態を設定する。目標とする管理状態を設定することで、図 6-8 のように、現在行われている管理体制・業務内容の問題点の抽出ができるようになる。

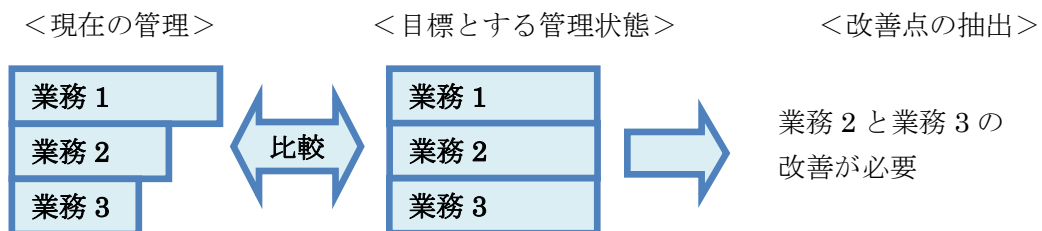


図 6-8 問題点抽出のイメージ

どのレベルを目標にするかは、組織で行うリスクアセスメントにより異なるが、SAM 達成目標として、客観的な指標を利用する場合には、例えば、図 6-9 のように「ソフトウェア資産管理評価規準」を用いて自組織の成熟度診断を行い、組織の目標とすべき成熟度レベルを定めること

も考えられる。

その場合、評価結果がレベル3（定義された段階）以下の場合には、レベル3を目標とするとか、「ソフトウェア資産管理基準」の定める13の目標の内、4、5、6は成熟度レベル4を目指すなど、具体的に定めることができるようになる。

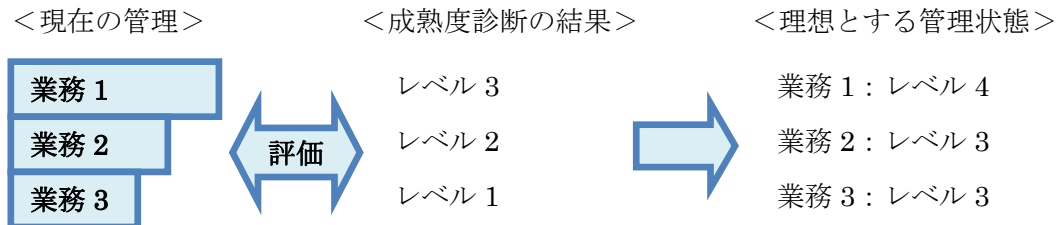


図 6-9 目標とする管理状態の設定イメージ

問題点の抽出を行う場合、あるべき姿と、現状の把握作業で作成された調査結果を比較し、差異を洗い出すことも有効な手段の一つである。

差異が生じる原因として、調査漏れの資産の存在や、必要管理項目の欠如、想定していないプロセスの存在などが考えられる。

6.5.2.2. 現状の把握結果からの問題点の抽出と解決策の策定

問題点は、SAMのあるべき姿と現状把握後の情報との差分から抽出される。このようにして抽出された問題点に関しては、発生する原因の追及とその解決方法を定め、SAMに関する規程や手順に盛り込むことが望まれる。

問題の解決策を導き出す方法としては、「1.管理対象資産・項目・組織に漏れがある」、「2.プロセスが存在しない」、「3.プロセス自体に欠陥がある・正しく機能していない」の3パターンに分類するとわかりやすい。こうすることで各問題に対する改善策を導き出すことも容易になる。

1.管理対象資産・項目・組織に漏れがある

問題点例	考えられる原因例（原因のパターン）
SAMに求められる資産・項目・組織が網羅されていない	<ul style="list-style-type: none"> 対象資産・項目・組織が明確にされていない 対象資産が管理対象から外れている SAMに求められる項目が含まれていない

2.プロセスが存在しない

問題点例	考えられる原因例（原因のパターン）
SAMに足りない台帳が存在する	<ul style="list-style-type: none"> SAMに求められる業務を誤って理解している SAMの認識がない

3.プロセス自体に欠陥がある・正しく機能していない

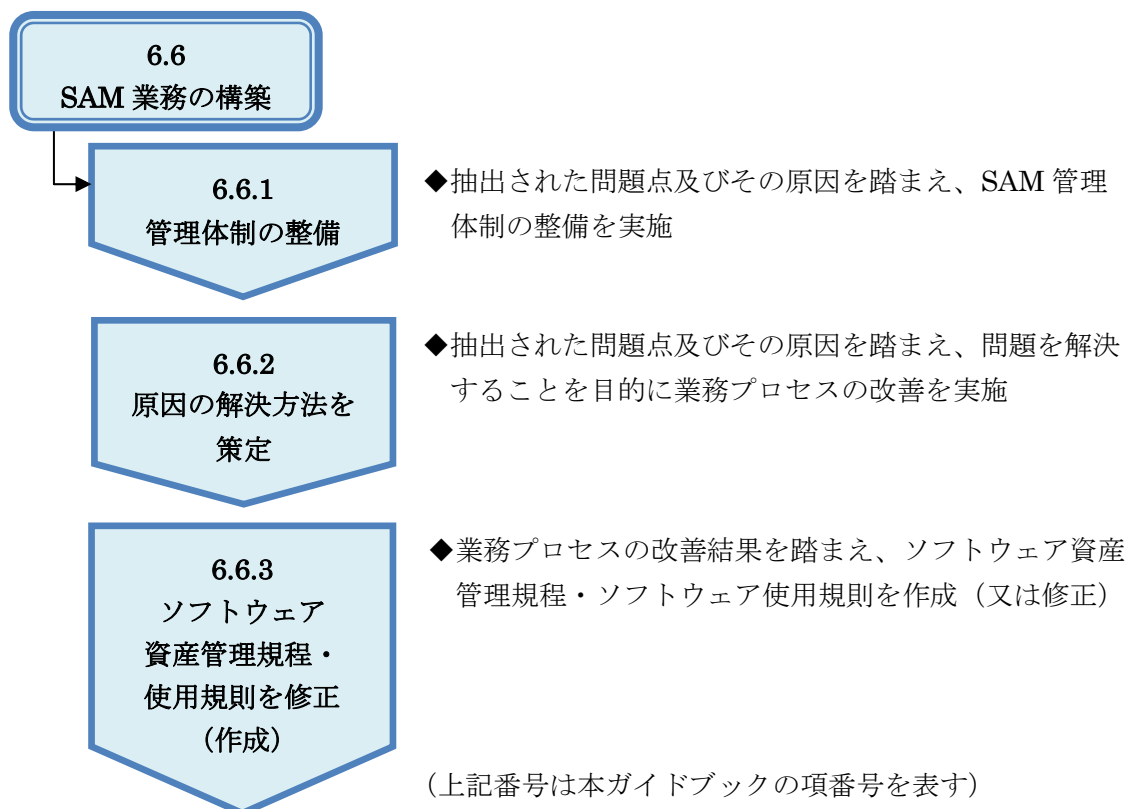
問題点例	考えられる原因例（原因のパターン）
組織全体の管理を統括する部門（統括管理部門）がすべての情報を把握できていない	<ul style="list-style-type: none"> ・管理が部門内で完結しており、統括管理部門に報告するプロセスが存在しない
最新の情報で台帳が維持されていない	<ul style="list-style-type: none"> ・台帳の更新タイミングが定められていない ・導入者のレベルで報告漏れが生じている ・台帳の管理者に更新の報告はされているが、台帳の更新が行われていない ・必要なアウトプットに至るプロセスが設定されていない

問題の原因究明を行う中で、特定の部署や担当者（例：部署・担当者が忙しいためメンテナンスができない）が問題の原因になるケースがある。しかし、特定の部署や担当者を問題の原因としてしまうと、改善策は「部門や担当者を変える」というものになってしまい、本質的な原因を解決することができなくなってしまう。

このような場合は、固有の部門や担当者を原因とするのではなく、更に深い原因（例：担当者の業務負荷が重いいため、SAMに時間を割けない）を究明することが重要である。

6.6. SAM 業務の構築

<SAM 業務の構築手順>



6.6.1. 管理体制の整備

ソフトウェア資産管理を実施するための体制整備を行う。ここでいう体制整備とは、ソフトウェア資産管理を実行するための担当・役割と責任の明確化を指す。

役割と責任を設定するに当たり、図 6-10「集中管理体制」図 6-11「分散管理体制」のいずれかを利用する組織が多い。

管理体制の選定に当たっては、組織内で既に存在する管理体制を活用することを推奨する。SAM が求める管理体制に最も近いものは、一般的には情報セキュリティ体制であると思われる。

ソフトウェア資産管理の管理体制は整っていない組織でも、IT 資産管理やセキュリティなどで管理体制が構築されている場合が多い。既存の管理体制に SAM の役割・責任を当てはめることで、スムーズに導入することができる。

集中管理、分散管理、いずれの体制を選択する場合でも、それぞれ長所短所は存在するため、後述の「集中管理体制・分散管理体制の長所・短所」参考に、組織に適した体制を整備することを推奨する。

(1) 【集中管理体制】

組織全体の管理を統括する部門（統括管理部門）が、被管理部門全体を一括して管理する体制。

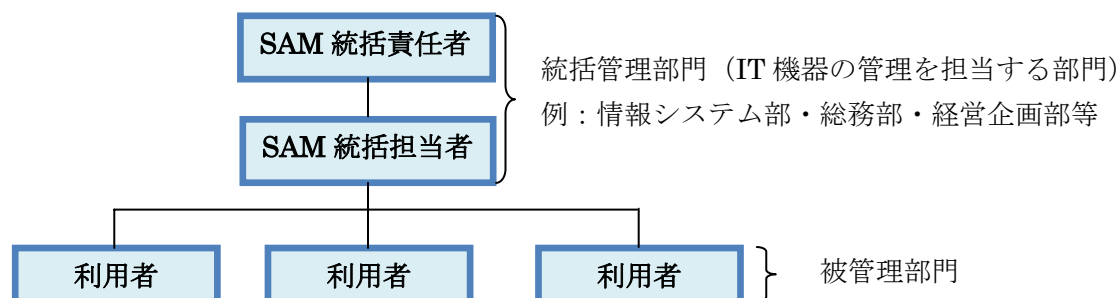


図 6-10 集中管理体制イメージ

(2) 【分散管理体制】

被管理部門内に部門 SAM 管理者を設置し、被管理部門内で行う業務を担当させ、管理業務を分散させる管理体制。

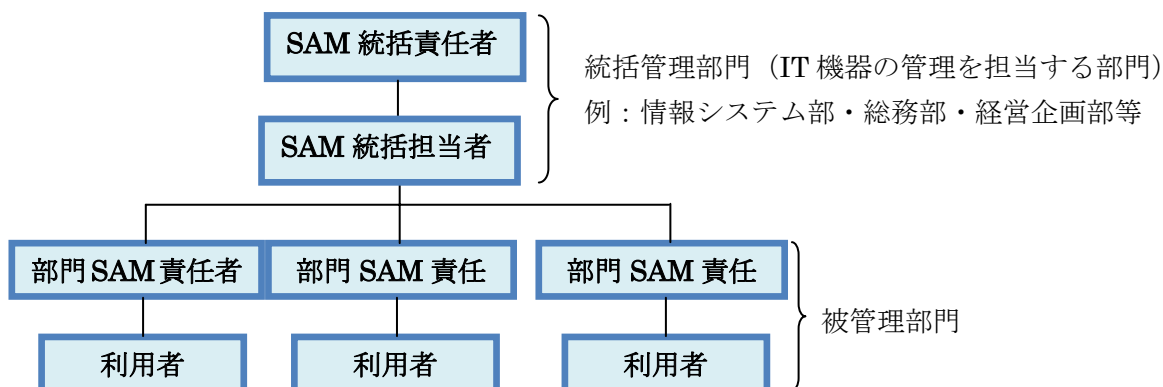


図 6-11 分散管理体制イメージ

(3) 【責任者・担当者の役割】

管理体制構築に際し、任命すべき責任者・担当者は以下のとおりである。下記の役職名については、役割があつていれば名称は各組織で変更しても問題はない。

また、誰にどの役割を割り当てるかについても、既存の役割分担に合わせて変更しても問題はないが、必ず割り当てられた責任者・担当者が職務をこなせるか、職務をこなすための権限を有しているかを考慮することが求められる。

表 6-16 責任者・担当者の役割

部門	役職名	役割	候補者例
統括管理部門	SAM 統括責任者	組織全体の管理責任を負う責任者	CIO・IT 資産を管理する部門の部長
	SAM 統括担当者	組織全体の管理業務を実施する担当者	IT 資産を管理する部門の所属員
被管理部門	部門 SAM 責任者	担当部門の管理責任を負う責任者	部門長

(4) 【集中管理体制・分散管理体制の長所・短所】

表 6-17 長所・短所

	集中管理体制	分散管理体制
長所	<ul style="list-style-type: none"> 情報の伝達がスムーズに行える 管理の精度にばらつきが生じにくい 	<ul style="list-style-type: none"> 統括管理担当者の負荷を分散することができる

短所	・ 統括管理担当者に負荷が集中する	・ 情報の伝達に時間を要する ・ 管理の精度にばらつきが生じやすい
適する組織の例	・ 小規模な組織	・ 大規模な組織 ・ 部門が資産の導入予算を持っている組織

6.6.2. 原因の解決方法を策定

問題の解決方法も問題の原因と同様、組織によりとるべき方法が異なるため、ここでは集約された3パターンを対象に原因の解決方法例を紹介する。

(1) 管理対象資産・項目・組織に漏れがある

目標とすべき台帳・項目・組織（現状の把握作業で設定した条件）と、現在の業務で作成されるアウトプットと比較し、漏れている対象資産・項目・組織を補完。

(2) プロセスが存在しない

上記と同様に「6.3.1.2 現状の業務プロセスの洗い出し方法」で紹介した設定すべきプロセスと、現在存在するプロセスを比較し、足りないプロセスを構築。

(3) プロセス自体に欠陥がある・正しく機能していない

プロセス自体の欠陥が含まれている場合や、正しく機能していない場合の改善策はその原因により異なる。上記二つの改善策と異なり、足りない項目やプロセスなどを補完するのではなく、問題の原因を究明し、個別に解決方法を策定しなければならない。

ここでポイントになることは、どの問題を優先的に解決するかである。優先順位を検討する際には、問題が「6.5.1.1. SAMに求められる要件」で紹介した必須要件、又は推奨要件のどちらに当てはまるかを判断し、リスクアセスメントを行うことを推奨する。

例えば、新規に導入したソフトウェアを把握するプロセスが存在しないという問題の場合、使用許諾条件違反につながるため、必須要件に影響する。しかし、管理の効率が悪く業務負荷が高いという問題の場合、通常必須要件に影響することはない。この場合、必須要件に影響する、新規で導入されたソフトウェアを把握するプロセスがない方を優先的に解決することが求められる。

また、必須要件関わる問題が複数存在する場合は、問題から生じるリスクの大きさに優先順位を判断することを推奨する。上記のように新規に導入したソフトウェアを把握するプロセスが全く存在しない場合、すべてのソフトウェアに影響する。しかし、似たような問題でも、特定部門が新規に購入したソフトウェアを把握するプロセスが存在しないという問題の場合、リスクは特定部門に限定される。

この場合、よりリスクの大きい、新規に導入したソフトウェアを把握するプロセスが存在しないという問題を解決することを優先すべきである。

6.6.3. 改善結果に基づきソフトウェア資産管理規程・使用規則を整備する

改善結果に基づき、ソフトウェア資産管理規程・使用規則を整備する。(規程が既に存在する場合修正を行う)

ソフトウェア資産管理規程・使用規則を整備する目的は、組織が SAM の効率的な計画、運用や制御を確実に実施し、統制のとれた管理が実施できるようにするためである。そのため、ソフトウェア資産管理規程・使用規則という名称でなくても、要件を満たす条項が整備され、文書化されていれば、名称は特に問わない。

また、SAM に関連する規程として考えられるものとして、

- ・情報セキュリティ方針
- ・情報セキュリティ規程
- ・物品調達規程
- ・サービスレベル管理規程
- ・(システムの) リリース管理、展開管理
- ・廃棄・返却規程

など、様々なものがあるが、SAM として策定する規程や規則は、これらの規程などと整合し、又は融合し策定することが望ましい。

ソフトウェア資産管理規程・規則の内容については、次項以降に詳細な説明がされているので、参考にしていただきたい。

6.7. 管理規程・手順の策定

6.7.1. 管理規程とは

SAM に関する管理規程を作成するにあたり、前章の「5.2. 体制及び方針決定」に記述されているとおり、まず、取締役会、又は同等の機関によって正式に承認されたソフトウェア資産管理方針を策定する必要がある。

この管理方針に基づいて、組織のソフトウェアの適切な使用及び管理を通じて、IT ガバナンスと情報セキュリティの組織に対する要求事項を満たし、ソフトウェアの適法、かつ有用な使用を推進することを目的とするものが管理規程である。

次に、管理規程に基づいて、管理規程が要求する事項の具体的な実施手順などについて、詳細な管理手続きを記載したものが管理手順書である。

一般的に、管理規程が SAM 単独で規定されることは稀であり、通常は、IT ガバナンスや情報セキュリティなどの他の管理規程とともに規定されることが多い。

また、管理手順書の策定に当たっては、図 6-12 のとおり、「①全社統一で管理手順書を規定する方法」、若しくは「②管理単位ごとに管理手順書を規定する方法」が想定されるが、いずれの方法を選択しても、適正で、かつ自組織の管理体制と管理規程に沿った管理手順書であれば何ら支障はない。

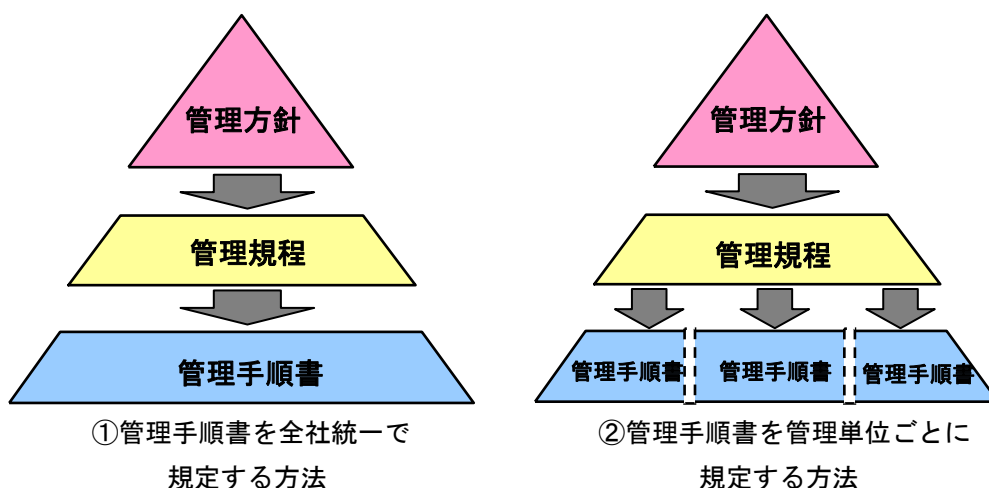


図 6-12 SAM の管理方針・管理規程・管理手順書の関係図

6.7.1.1. 管理規程と管理手順書の違い

管理規程とは、組織の管理方針に基づいて、管理対象スコープ（対象組織、対象資産）や管理プロセス（調達～廃却）などを規定するための組織全体のガイドラインである。

一方、管理手順書は、前述の管理規程に基づいて、SAM を実行するための(1)組織全体、若しくは、(2)管理単位ごとに定められた、具体的かつ詳細な「SAM 運用実施マニュアル」として捉えることができる。

なお、管理手順書の作成にあたっては、管理形態が「分散管理」の場合、下記三つの選択肢が想定されるが、そのいずれかを選択するかについては、組織の規模、ソフトウェア利用の複雑性などに応じて、自組織にとって、より適切に、かつ効率的に管理・運営できる管理手順を検討の上、作成することが望ましい。

- (1) 全社統一の管理手順書を規定する方法
- (2) 全社統一の管理手順と、管理単位独自の管理手順を並存させて規定する方法
- (3) 管理単位ごとに、独自の管理手順書を規定する方法

なお、管理規程は、組織全体の管理ガイドラインという性格上、それほど頻繁に変更されることはないが、管理手順書については、管理対象スコープ（対象組織、対象資産）の変更や管理プロセス（調達～廃却）の見直しなどより、定期的に変更されることが予想されるため、メンテナンス工数などを考慮すると、あらかじめ管理規程とは切り離して作成しておくことが望ましい。

6.7.1.2. 全社規程における SAM 管理規程の位置づけ

組織において、実効性のあるソフトウェア資産管理を構築・運営を行うためには、取締役会、又は同等の機関によって、SAM の管理方針と同様に、管理規程、及び管理手順書が正式に承認されることが望ましい。

また、管理規程の作成方法については、前述のとおり、管理規程が SAM 単独で規定されるこ

とは稀であり、通常は、IT ガバナンスや情報セキュリティなどの他の管理規程とともに規定されることが一般的である。

しかし、組織の管理方針に基づいた管理規程であれば、自組織の事情に応じて、下記のどちらの方法を選択しても構わない。

(1) SAM の管理規程を他の関連する規程類から切り出して独立させる方法

(2) SAM の管理規程を他の関連する規程類の中に含める方法

なお、図 6-13 の例には、(1) のパターンを図示したので参考にして頂きたい。

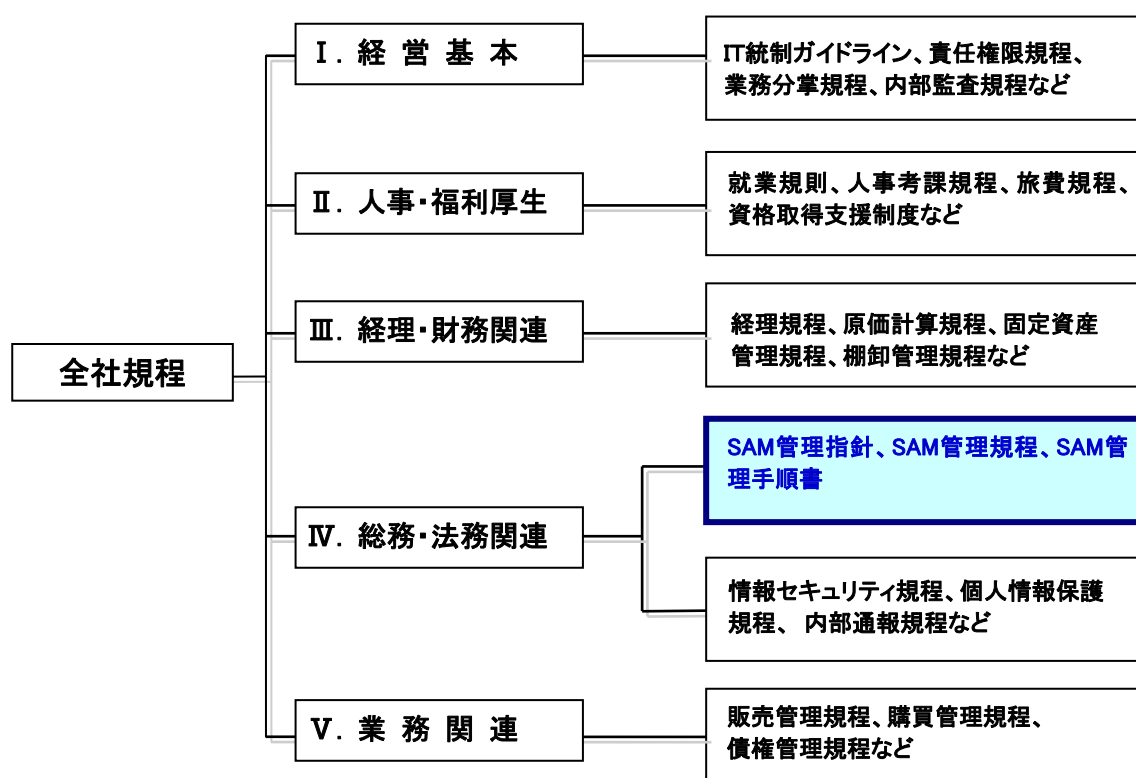


図 6-13 全社規程における SAM 管理規程の位置づけ
(SAM の管理規程を他の関連する規程類から切り出して独立させる方法)

また、組織の SAM に関する管理形態が、下記のいずれを選択しているかによって、その特性から管理規程や管理手順書の作成方法や作成手順も自ずと異なってくる。

(1) 集中管理： SAM 統括部門が組織全体の SAM を一元的に一括管理する形態。

(2) 分散管理： 管理単位を分け、管理単位ごとの管理部門がそれぞれの管理を行い、SAM 統括部門が管理単位ごとの管理部門と連携しながら、組織全体の SAM を統括管理する形態。

したがって、管理形態が「集中管理」の場合、管理規程、及び管理手順書について、組織全体で統一した順守すべき管理項目・管理手順を規定し、取締役会、又は同等の機関による正式承認後、組織全体に周知徹底を図ることが望ましい。

一方、管理形態が「分散管理」の場合、管理規程については「集中管理」と同様、まずは、組織全体で統一した順守すべき管理項目を規定する。

次に管理手順書については、組織全体で順守すべき管理手順のほかに、管理単位ごとに独自の管理手順が存在するのであれば、組織全体で適切、かつ効率的に SAM を実施することができるように、管理単位独自の管理手順を含めた組織全体の管理手順書を規定することが望ましい。

ただし、その場合でも、SAM 統括部門は、管理単位ごとに管理手法や管理レベルの差異が生じることを防ぐために、部門 SAM 管理責任者に対して、組織全体で統一した管理手順書の雛形を提供し、組織として順守すべき管理手順のガイドラインについて指導することを推奨する。

そして最終的には、これら管理規程、及び管理手順書が取締役会、又は同等の機関による正式承認後、組織全体に周知徹底を図ることが望ましい。

なお、管理形態が「分散管理」の場合であっても、管理単位独自の管理手順が存在せずに、組織全体で統一した管理手順に基づいて、SAM を実施しているのであれば、必ずしも管理手順書を管理単位ごとに独自に作成する必要はなく、「集中管理」の場合と同様、組織全体で統一した管理規程、及び管理手順書を規定し、取締役会、又は同等の機関による正式承認後、組織全体に周知徹底を図っていれば何ら問題はない。

6.7.2. 管理方針、管理規程の推奨記載項目

本節では、ISO/IEC 19770-1 で規定されている内容を基に、SAM を実施する上で必要となる管理方針、管理規程の推奨記載項目を紹介する。

これから新たに SAM 規程類を作成する方、若しくは現在 SAM 規程類の見直しを検討されている方が、検討材料の一助として参考にして頂ければ幸いである。

なお本節では、組織が具備すべき SAM の管理方針、管理規程の考え方、枠組みを提供しているが、これらの SAM 規程類を検討する際は、組織の規模、ソフトウェア利用の複雑性など自組織の事情を考慮した上で、必要に応じては SAM の専門家の知見も参考にしながら、自組織に適した管理方針、管理規程を検討の上作成することが望ましい。

6.7.2.1. ソフトウェア資産管理方針の推奨記載項目

ISO/IEC 19770-1 で規定されている内容を基に、SAM を実施する上で必要となるソフトウェア資産管理方針の推奨記載項目を下記のとおり紹介する。

なお、詳細については、表 6-18「ソフトウェア資産管理方針の推奨記載項目」、及び付録「A-1」に「ソフトウェア資産管理方針（サンプル）」を記載しているので参考にして頂きたい。

(推奨記載項目)

- (1) 宣言
- (2) 適用範囲
- (3) リスク管理
- (4) ソフトウェア資産管理者の役割と責任

表 6-18 ソフトウェア資産管理方針の推奨記載項目

推奨記載項目	補足説明及び関連する規格項目
1. 宣言	本管理方針が取締役会、又は同等の機関によって承認されたソフトウェア及び関連資産の文章であること。(4.2.2 a, 4.2.2 b)
2. 適用範囲	(1) 本指針が適用される組織の対象範囲。 (2) 本適用範囲が定期的に毎年、取締役会、又は同等の機関によって見直されること。(4.2.2 c)
3. リスク管理	ソフトウェア及び関連資産を管理する従業員が留意すべきリスクについて規定する。(4.2.2 d) (例：個人のプライバシー順守などの規制を順守しないことのリスクなど)
4. ソフトウェア資産管理者の役割と責任	(1) SAM 管理責任者の役割と責任。 (2) 部門 SAM 管理責任者の役割と責任。(4.2.3)

6.7.2.2. ソフトウェア資産管理規程の推奨記載項目

ISO/IEC 19770-1 で規定されている内容を基に、SAM を実施する上で必要となるソフトウェア資産管理規程の推奨記載項目を下記のとおり紹介する。

なお、詳細については、表 6-19「ソフトウェア資産管理規程の推奨記載項目」を参考にして頂きたい。

(推奨記載項目)

- (1) 文書規程
- (2) SAM 指針
- (3) 要員教育
- (4) 部門 SAM 管理責任者への教育

表 6-19 ソフトウェア資産管理規程の推奨記載項目

推奨項目	補足説明及び関連する規格項目
1. 文書規程	(1)本文書が当該組織の文書管理規程によって発行されること。 (2) ISO/IEC 19770-1 で規定される SAM 管理プロセスと、当該組織の SAM 業務との関連。(4.2.4.2 a, 4.2.4.2 b)
2. SAM 指針	管理方針に対する個人及び企業の責任。(4.2.4.2 c) (例：会社が提供するソフトウェア及び関連資産を私的に利用することを制限するなど)

3. 要員教育	(1)すべての新しい要員には、初めて職務を開始する際に、従来からの要員には、最低年1回、SAM管理責任者が用意する教育を受講すること。 (2) 管理方針及び管理規程は、要員が常に閲覧できるように公開すること。(4.2.4.2 d)
4. 部門 SAM 管理責任者への教育	SAMの責任を負う要員は、下記のような教育訓練を最低年1回受講し、また、その受講証明を受けること。(4.2.5) (1) SAM及び関係する使用許諾権について、初歩的な教育訓練と、年1回の正式な継続教育の両方を受講すること。 (2)使用許諾条件の順守を促すために、ソフトウェアメーカーから製品使用許諾に関する更新情報について最低年1回、確認を行うこと。

6.7.3. 管理手順書の策定例

管理手順書をうまく運用できていないケースの特徴として、自組織の管理プロセスと管理手順書との不整合、管理プロセスの管理手順への記載漏れを挙げることができる。

その原因としては、自組織の管理方針、管理体制、購入形態、管理プロセスなどを十分に考慮せず、インターネットなどで公開されている一般的な管理手順書をそのまま流用して自組織の管理プロセスと異なる管理手順書を作成してしまうことにある。

上記のような方法で作成した管理手順書は当然、自組織の管理プロセスに合致していないので、本手順書に基づいたSAMの運用を実施しようとしても、管理実態に即していないため運用できずに、結果的に有名無実化してしまうことになる。

このような事態を招かないよう管理手順書を作成するに当たっては、自組織で運用している既存の管理プロセスに重大な欠陥がなければ、なるべく既存の管理プロセスを生かす形で、本節で紹介する推奨記載項目をうまく取り入れながら、管理手順書を策定することが望ましい。

本節では、ISO/IEC 19770-1で規定されている内容を基に、SAMを実施する上で必要となる管理手順書の策定手順及び推奨記載項目を下記のとおり紹介する。

6.7.3.1. 管理手順書の策定手順及び推奨記載項目

ISO/IEC 19770-1で規定されている内容を基に、SAMを実施する上で必要となる管理手順書の策定手順及び推奨記載項目を下記のとおり紹介する。

また、管理手順書の推奨記載項目の補足説明と関連する規格項目(一部)を、図6-14に図表にしてまとめているので参考にして頂きたい。

なお、管理手順書を策定する際には、下記ポイントを考慮に入れて検討することが望ましい。

- (1) 管理体制と管理規程に沿った管理プロセスが構築できているか。
- (2) ソフトウェア資産管理の業務効率を低下させるような、非効率なプロセスが存在していないか。

(管理手順書の策定手順)

管理手順書を作成するに当たって、下記手順を参考に策定することが望ましい。

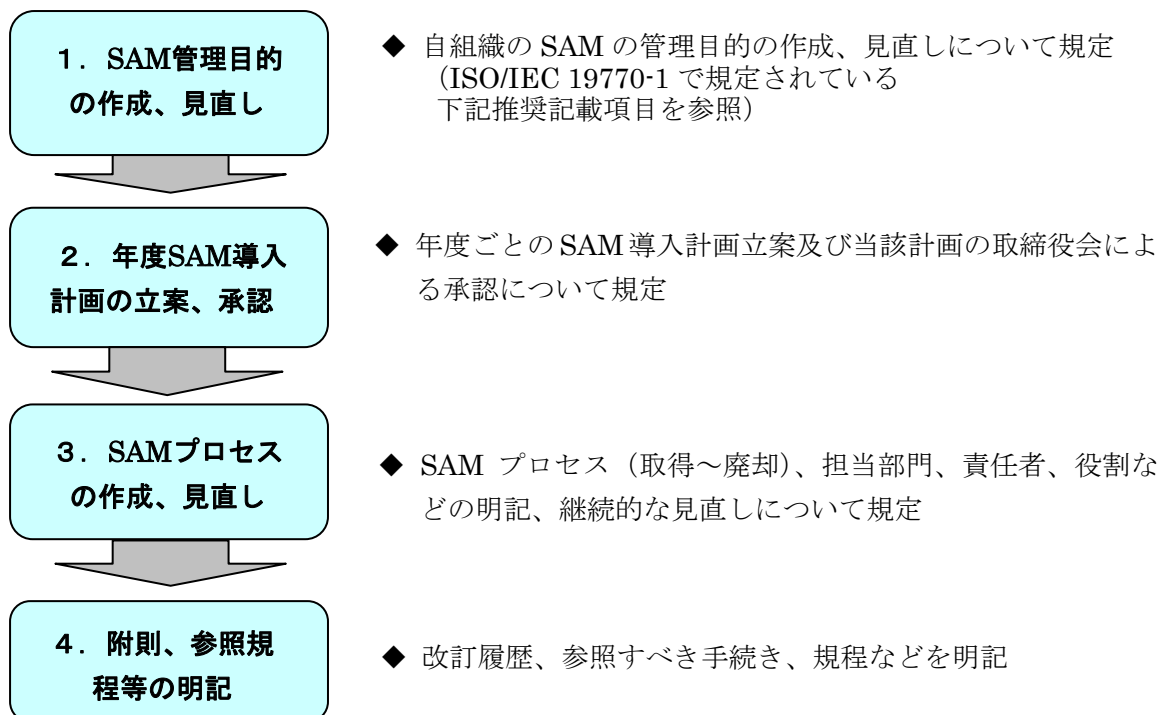


図 6-14 管理手順書の策定手順

管理手順書を作成するに当たって、下記項目を参考に策定することが望ましい。

(推奨記載項目)

(1) SAM の管理目的 (4.3.2.2 a)

下記内容を考慮した SAM の管理目的が記載されており、かつ、本管理目的の見直しが年 1 回、実施されていること。

- ① 組織内におけるソフトウェアの不正コピーの防止
- ② 組織内におけるソフトウェアの購入費用の削減
- ③ ソフトウェア管理コストの削減
- ④ 組織内のソフトウェアの標準化
- ⑤ ソフトウェア導入の迅速化
- ⑥ 最適なソフトウェアの利用

(2) 年度 SAM 導入計画 (4.3.2.2 b 、 4.3.2.2 c)

下記内容を考慮した SAM の導入計画が、毎年、取締役会、又は同等の機関によって承認されていること。

- ① 対象ソフトウェア、及び関連資産の範囲
管理対象項目としては、以下の項目を記載しておくこと。

また管理対象項目のうち、購入形態については、購入形態ごとにソフトウェアの購入及び導入プロセスについて文書化しておくこと。

- (a) 対象ソフトウェア、及び関連資産
- (b) 対象ソフトウェア、及び関連資産に関する説明
- (c) 対象ソフトウェアベンダー名
- (d) 購入形態
- (e) 備考

①-1. SAM 導入計画の実行に必要なリソースの確保

SAM 導入計画を基に、年度計画を確実に実施するための必要なリソース（人、金、ツール）を確保すること。

①-2. 部門 SAM 管理者による自己監査の実施、及び取締役会への定期報告

SAM 管理責任者は、購入責任者からの報告内容を考慮し、部門 SAM 管理者に所管部門の導入状況について自己監査を実施させ、その結果を集計し、4 半期に 1 回、取締役会又は同等の機関に状況報告を行うこと。

② SAM の管理体制

SAM 管理責任者、部門 SAM 管理者、購入責任者など SAM を適正、かつ効率的に運営するための管理体制を明確化しておくこと。

(3) SAM プロセス（取得～廃却）

取得～廃却までの業務手続きと、担当部門、責任者、役割、などを定義しておくこと。

(4) 附則

改訂履歴などについて明記しておくこと。

(5) その他

すべての項目において、参照すべき手続、規定などについて明記しておくこと。

表 6-20 管理手順書の推奨記載項目

推奨項目	補足説明及び関連する規格項目
1. SAM の管理目的	<p>当該組織の SAM の管理目的が定義され、本管理目的が年 1 回、見直しが実施されていること。(4.3.2.2 a)</p> <p>(例)</p> <ul style="list-style-type: none"> ・組織内におけるソフトウェアの不正コピーの禁止 ・組織内におけるソフトウェアの購入費用の削減 ・ソフトウェア管理コストの削減 など
2. 年度 SAM 導入計画	<p>本導入計画が、毎年、取締役会、又は同等の機関によって承認されること。(4.3.2.2 b 、 4.3.2.2 c)</p> <p>(1) 対象ソフトウェア、及び関連資産の範囲</p> <p>管理対象項目としては、①対象ソフトウェア、及び関連資産、 ②「対象ソフトウェア、及び関連資産」の説明、 ③ソフトウェアベンダー名、④購入形態などを明確にすること。</p> <p>(1)-1. SAM 導入計画の実行に必要なリソースの確保</p> <p>SAM 導入計画を基に、年度計画を確実に実施するための必要なリソース（人、金、ツール）を確保すること。</p> <p>(1)-2. 部門 SAM 管理者による自己監査の実施、及び取締役会への定期報告</p> <p>SAM 管理責任者は、購入管理者の報告内容を検討し、部門 SAM 管理者に所管部門の導入状況を監査させ、当該監査結果を分析集計し、取締役会、又は同等の機関に 4 半期に 1 回、報告されること。</p> <p>(2) SAM の管理体制</p> <p>SAM の管理体制を明確にすること。</p> <p>(例) SAM 管理責任者、部門 SAM 管理者など</p>
3. SAM プロセス (取得～廃却)	<ul style="list-style-type: none"> ・取得： 購入申請～発注までのプロセスと、担当部門、責任者、役割などを明記。 ・導入： 検収～保管管理、支払までのプロセスと、担当部門、責任者、役割などを明記。 ・異動： IT 資産の異動（利用者、設置場所の異動）に関するプロセスと、担当部門、責任者、役割などを明記。 ・廃却： IT 資産及びインストール媒体の廃却に関するプロセスと、担当部門、責任者、役割などを明記。
4. 附則	改訂履歴などについて明記。
5. その他	すべての項目において、参照すべき手続、規定を明記。

6.8. SAMの運用設計

6.8.1. SAM 年度計画の策定

2006年5月、SAMプロセスに関する国際規格（ISO/IEC 19770-1）が発行し、ソフトウェア資産が有する経済的価値、及び組織運営に対する影響度が高まり、組織において、ソフトウェア資産管理の重要性が再認識され、実効性のあるソフトウェア資産管理の構築に向けた取り組みが求められている。

すなわち、SAMを「計画（Plan）－実行（Do）－評価（Check）－改善（Act）」というPDCAサイクルに基づくマネジメントシステムとして、構築・運用していくことが肝要であり、特に、SAMの年度計画を策定することは、その実行を担保する上で、最も重要なタスクの一つである。

したがって、SAM管理責任者は、SAMの管理、棚卸、監査、レビュー、教育の実施方法、実施予定などを定めたSAM年度計画を年1回、策定するとともに、策定した年度計画を取締役会、又は同等の機関に報告し、承認を得ることが望ましい。

本節では、SAM年度計画の中でも、特に重要となる「棚卸」、「監査」、「レビュー」について説明を行いたい。

6.8.1.1. 棚卸

棚卸の目的は、ソフトウェア資産及び関連資産の現物の状態を確認するとともに、管理台帳などの記録と照合し、実態面から管理状態を確認することにある。

SAM管理責任者は、管理規程に基づいて組織全体に対して、ソフトウェア資産、及び関連資産の現物と関連する管理台帳の記録との照合を指示し、不整合があれば、発生原因を調査の上、再発防止策を検討するとともに、棚卸結果に基づいて、速やかに是正処置を実施する必要がある。

棚卸の実施に当たっては、「①手作業によって実施する方法」、「②SAMツールを利用して実施する方法」があるが、管理の効率化、及び管理コストの削減を考慮すると、SAMツールを導入し、有効利用することが望ましい。

管理手順書の棚卸手順は、下記事項を参考に策定することが望ましい。

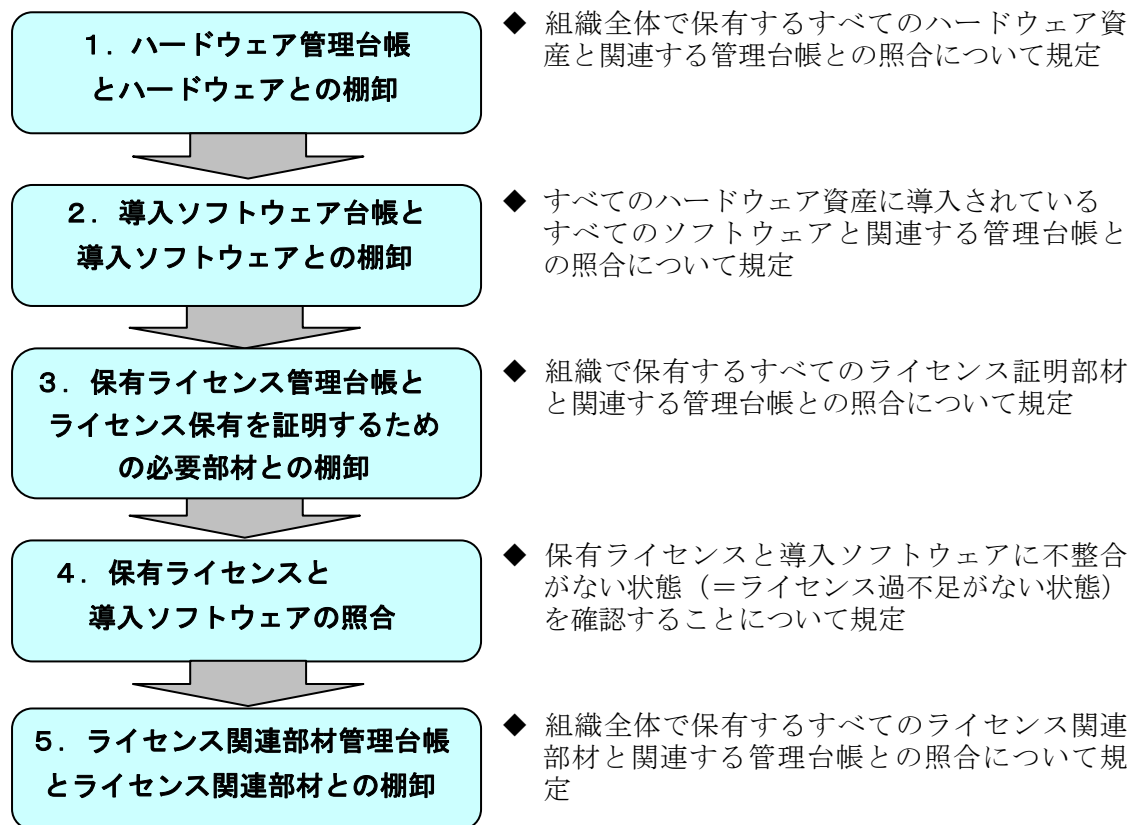


図 6-15 管理手順書（棚卸）の策定手順

(1) ハードウェア管理台帳とハードウェアとの棚卸

ハードウェアの棚卸を実施する場合には、実際に使用している PC、サーバなどだけでなく、現在使用していない PC、サーバなどを含めたすべてのハードウェア資産についても調査対象として、組織全体で保有するハードウェア資産を把握した後、その棚卸結果を関連する管理台帳の記録と照合を行うことが望ましい。

(2) 導入ソフトウェア台帳と導入ソフトウェアとの棚卸

上記ハードウェアの棚卸で判明した組織で保有するすべてのハードウェア資産に導入されているすべてのソフトウェアの調査を行った後、その棚卸結果を関連する管理台帳の記録と照合を行うことが望ましい。

(3) 保有ライセンス管理台帳とライセンス保有を証明するための必要部材との棚卸

保有ライセンス数の調査を行う際には、購入方法によって、ライセンスを証明するための必要部材（Proof of License）が異なるので注意が必要である。

本作業の実施に当たっては、組織が保有しているライセンス保有を証明するために必要な部材を調査し、当該調査が完了した後、その調査結果を関連する管理台帳の記録と照合を行うことが望ましい。

またライセンス保有を証明するために必要な部材は、ソフトウェアメーカーごと、購入方法ごと、及び製品ごとに異なるので、詳細については、ソフトウェアメーカー、若しくは、SAM 構築支援会社に確認することが望ましい。

(4) 保有ライセンスと導入ソフトウェアの照合

現物調査の結果に基づいて、保有ライセンスと導入ソフトウェアに不整合がないこと（＝ライセンスの過不足がないこと）を確認する。

(5) ライセンス関連部材管理台帳とライセンス関連部材との棚卸

組織で保有するすべてのライセンス関連部材の調査を行った後、その棚卸結果を関連する管理台帳の記録と照合を行うことが望ましい。

6.8.1.2. 監査

監査責任者は、下記内容に沿った「監査計画」を策定し、取締役会又は同等の機関の承認を得た上で、部門 SAM 管理者などに周知することが望ましい。

(監査計画の内容)

- (1) 実施スケジュール
- (2) 監査の種別（内部監査・外部監査）
- (3) 監査方法
- (4) 監査の実施対象範囲（実施対象スコープ）

また SAM の監査は通常、整備状況、及び運用状況について実施される。

(1) 整備状況の監査

整備状況の監査は、監査対象において、次の事項が適切に実施されているかといった観点から実施されることが望ましい。

- (a) SAM の機能設計及び運用設計が適切になされているか
- (b) 上記を取り巻く運用体制及び運用手続きが適切に設定されているか

(2) 運用状況の監査

運用状況の監査は、監査対象において、SAM として整備されている管理の仕組みが適切に機能しているかどうかといった観点から実施されることが望ましい。

6.8.1.3. レビュー

SAM 管理責任者は、年度 SAM 導入計画のレビューを下記目的のために、最低年 1 回実施し、SAM の管理目的が確実に達成させるようにすることが望ましい。

- (1) SAM の管理目的、及び SAM 計画が達成されているかどうかの評価
- (2) SAM に関して、経営陣が承認した方針、プロセス及び手順が定義された組織の全範囲に効果的に周知され、導入されているか
- (3) 識別された違反事項の要約
- (4) SAM についての改善機会の特定
- (5) 継続的なレビューを行う必要性の有無

また、SAM 管理責任者は、年度 SAM 導入計画の進捗管理を把握し、その結果として取るべき措置を取締役会又は同等の機関に報告を行うことが望ましい。加えて、SAM 管理責任者は、最も費用対効果が上がるように、ソフトウェア及び関連資産がどのように展開されているかに関して、定期的なレビュー（最低年1回）を実施し、改善に向けた勧告が行われるように管理することを推奨する。

6.8.2. 周知

管理規程や管理手順書を策定しても、組織全体に対してこれらを周知徹底し、順守されることができなければ、まさに絵に描いた餅であり、何の意味もなさない。

そこで、組織全体に対して、管理規程や管理手順書を周知徹底し順守させるために次の3点を活動ポイントとして推進することが望ましい。

- (1) 目的・問題意識の共有
- (2) 報告・連絡体制の整備
- (3) SAMに関する理解、及び教育研修の定期実施

表 6-21 管理規程の周知に向けた活動ポイント

項目	活動ポイント
1. 目的・問題意識の共有	・管理方針、管理規程、管理手順書の徹底
	・管理方針、管理規程、管理手順書の目的の明確化
	・管理体制の確立
	・責任と役割の明確化
	・トップマネジメントの理解とリーダーシップ
2. 報告・連絡体制の整備、	・コンプライエンスの順守
	・管理方針、管理規程、管理手順書の公開・伝達 (ポータルサイトなどツールを利用した仕組みの構築)
3. SAMに関する理解、及び教育研修の定期実施	・SAM 管理責任者と部門 SAM 管理者などとの定例ミーティングの開催、及び改善に向けた情報交換の実施
	・褒章と罰則規程の策定
	・内部監査の定期実施
	・部門 SAM 管理責任者、管理担当者の役割、責任の明確化と SAM に関する理解の徹底
	・ソフトウェア利用者の責任と SAM に関する理解の徹底
3. SAMに関する理解、及び教育研修の定期実施	・部門 SAM 管理者、部門 SAM 担当者への SAM 教育研修などの定期的な実施
	・全要員への著作権やソフトウェア利用上の教育研修などの定期的な実施

また、対象者によって周知すべき内容が異なるので、ここでは、「管理者」と「全要員」に分けて、周知内容を紹介したい。

6.8.2.1. 管理者への周知

部門 SAM 責任者、及び部門 SAM 担当者など、SAM の責任を負う要員は、SAM をマネジメントシステムとして運営・管理していくために、下記のような教育訓練を最低年 1 回受講し、またその受講証明を受けることが望ましい。

- (1) SAM 及び関係する使用許諾権について、初歩的な教育訓練と、年 1 回の正式な継続教育の両方を受講すること。
- (2) 使用許諾条件の順守を促すため、ソフトウェアメーカーから製品使用許諾に関する更新情報について最低年 1 回、確認を行うこと。

6.8.2.2. 全要員への周知

ソフトウェア利用者などの要員は、SAM をマネジメントシステムとして運営・管理していくために、下記のような教育訓練を最低年 1 回受講し、またその受講証明を受けることが望ましい。

- (1) すべての新しい要員には、初めて職務を開始する際に、従来からの要員には、最低年 1 回、SAM 管理責任者が用意する教育を受講すること。
- (2) 管理方針、管理規程及び管理手順書は、要員が常に閲覧できるように公開され、伝達されていること。

なお、教育訓練を実施するに当たっては、SAM やソフトウェア利用に関する e ラーニングコースなどを提供する企業も存在しており、研修実施を検討する際には、自社独自で実施した場合と、これら外部業者が提供するサービスを利用した場合の費用対効果を比較検討の上、実施することが望ましい。

7. SAM 運用上のポイント

前章で構築した SAM の体制や規程・手順書などをベースに SAM を運用していくわけであるが、SAM が効果的かつ効率的に運用されるためには、運用上の不備を是正するとともに、継続的に改善することが欠かせない。日本における多くの組織では、台帳の整備や SAM ツールの導入だけで「SAM」が完結したとしている状況が散見されるが、「コンプライアンス」や「コスト削減・合理化」といった根本的な経営課題の解決につながることで、はじめて経営における SAM の価値が創造され、実施することの意義が産まれてくる。本章では、形ばかりの「SAM」にならないようにするための SAM 運用上のポイントを、継続的改善の観点から、

- ① SAM を高度化するための改善及び計画策定におけるポイント（7. 1）
- ② SAM を組織へ定着させるためのポイント（7. 2）
- ③ 棚卸の実施におけるポイント（7. 3）
- ④ SAM 監査におけるポイント（7. 4）

の四つに分けて解説する。なお、本章は前章で設計し策定された SAM 運用プロセスにより、PDCA サイクルが一度回っていることを前提としている。

7.1. SAM を高度化するための改善及び計画策定におけるポイント

多くの組織では SAM は IT インフラの一つとして整備されることが多く、SAM の計画も IT 計画に含まれることが多い。一般的に IT インフラは投資対効果が見えにくく IT 計画における優先度は低くなりがちであるが、更に資産管理とあってはほとんど IT 計画の俎上に上がってこないのが実情であろう。しかし、「SAM」が IT インフラを支える基盤だけでなく、「コンプライアンス」、「コスト削減・合理化」という経営からの要請に応える有効なツールとして活用できることから、計画的に取り組むことで SAM の効果を最大限に引き出したい。

では具体的にどのような取組みを計画立てればよいのだろうか？ここでは、SAM の管理目的のうち、「ライセンスコンプライアンス（法的リスクの回避）」、「コスト削減・合理化（TCO の削減）」の観点から説明していく。

7.1.1. コンプライアンスのための計画

(1) 管理対象ソフトウェアの見直しにおけるポイント

SAM を構築した段階では、組織が保有しているすべてのソフトウェアが管理対象になっていないかもしれない。コンプライアンスにおける最大の留意点は例外が認められないことにある。SAM においては、組織が保有しているソフトウェアライセンスに関連する法令・契約はすべて順守しなければならない。

ただし、初めからすべてについて管理するには莫大な時間とリソースが必要となり現実的

でない場合もありうる。また、無料ソフトウェアによっては特別に管理を実施しなくとも、コンプライアンス上の問題が発生しないことも考えられる。これは、組織においてどのようなソフトウェアが利用されているのかについて網羅的に把握した上で管理対象を絞るということであり、初めから管理対象ソフトウェアありきではないことに留意いただきたい。管理対象範囲の決定については、5章で説明したように、リスクの大きいものから順に対応する「リスクアプローチ」を取ることが多い。

コンプライアンスの観点からは、既に管理しているソフトウェアから、更により広範囲のソフトウェアを対象にしていくことが望まれる。管理対象となるソフトウェアを拡大することによって管理負担も増えていくことになるが、ソフトウェアの標準化(7.1.2 ポイント(1))や利用禁止ソフトウェアなどを併せて見直すことにより効率的かつ実効的な管理を行うことも望まれる。

ソフトウェアが利用されるハードウェア資産や利用者などについても、漏れなく管理対象として定めておく必要があることに留意したい。デバイスに紐付くソフトウェアライセンスの場合は、ある特定のハードウェア上で当該ソフトウェアが利用されている場合、ハードウェアの所在がソフトウェア利用状況の確定に必要な情報となるからである。利用者に紐付くソフトウェアライセンスについても同様であり、当該ソフトウェアを利用する利用者を漏れなく管理しておく必要がある。

(2) 正確な情報の確保と可視化におけるポイント

コンプライアンスの観点からは、管理対象として決定されたソフトウェアに関して、そのライセンスの保有状況と使用状況について常に正確な状態を保持し、適時に管理状況を見える状態(見える化・可視化)にしておくことが望まれる。このことにより、組織がコンプライアンスに対して説明責任を果たすことが可能となる。このために必要となる施策について、以下に解説する。

① 管理台帳に関する管理手続の整備

正確性の確保に関してはデータベースの基本機能である CRUD(Create: 新規作成、Read: 読み出し、Update: 更新、Delete: 削除)に留意して、各手続きと管理台帳への操作を漏れ無く行えるよう整備しておきたい。特に「資産の登録」は重要であり、ここが漏れてしまうと保有資産として認識されないため、適正な管理を行うことができない。「資産の登録」以外にもデータベースに操作が加わる管理業務については、その管理手続を確実に整備しておきたい。

表 7-1 ライフサイクルにおける管理台帳への操作

	新規作成	読み出し	更新	削除
調達時の参照		○		
資産の登録	○			
資産の利用			○	
資産の異動			○	
資産の棚卸		○	○	○
資産の処分				○

管理対象の拡大により管理対象となるソフトウェア関連資産が増えた場合は、その管理対象についての管理が適正に行われなければならないため、管理手続や管理台帳についても必要に応じて見直すことが望まれる。特に部門で独自に管理する場合には、その手法や管理レベルが疎かになりがちであるため、SAM を担当する部門が適切に指導に当たることが重要である。

② 棚卸の実施計画

資産管理において、管理手続を整備し、そのとおりに運用したとしても、例外的な取り扱いによる手続きの漏れや、不正な利用、資産の紛失・盗難などによる減損などにより、本来はあってはならないことであるが現状と管理台帳上の情報は次第に乖離していく。定期的に棚卸を実施し、管理台帳上の情報を現物に一致させることにより、乖離している状況をなるべく最低限にすることができ、コンプライアンス違反を能動的かつ、速やかに是正することができるようになる。また、乖離が起きた原因を調査し、その芽を摘む施策を打つことで SAM の改善にも資することになる。棚卸が説明責任を果たすことにつながることもについても留意しておきたい。棚卸の実施におけるポイントは「7. 3 棚卸の実施におけるポイント」で解説する。

棚卸の実施間隔は、本質的には管理対象の量や管理台帳に対する統制のレベルによって適正な期間を設定すべきである。管理手続が整備され運用も適切に回っている場合は乖離が起これにくいことから実施期間はある程度長くすることが可能であるが、逆の場合は頻繁に棚卸を実施しなければ管理台帳は実態を示すものではなくなる。

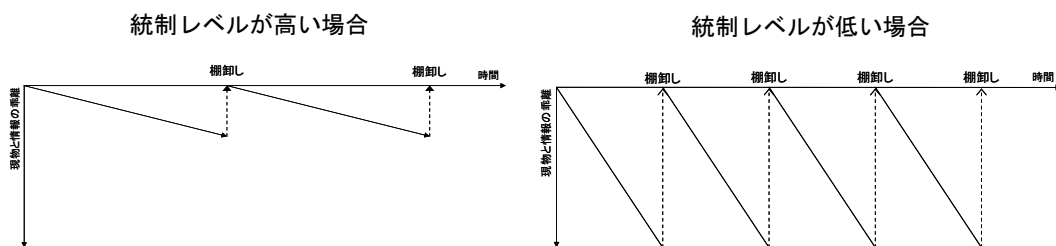


図 7-1 統制レベルによる乖離度合の違い

棚卸についてもリスクアプローチを適用し、ソフトウェアのリスクに応じて棚卸の実施間隔を変えることによりリソースを最適配分することが可能であり有効である。なお、ISO/IEC 19770-1 で推奨されている棚卸の実施間隔は下表のとおりであり、参考にするによい。統制のレベルや対象となるソフトウェアのリスクを考慮しながら、管理対象に対しては確実に棚卸を実施することが望まれる。

表 7-2 棚卸実施間隔の推奨値 (ISO/IEC 19770-1 を基に作成)

実施間隔	実施対象
3ヶ月に1回以上	インストール済みのソフトウェアとインストール申請手続きなど証跡との照合
	保有ライセンスと使用ライセンスの確認と調整
6ヶ月に1回以上	ハードウェア資産の所在確認
	ソフトウェアが記録された媒体の所在確認
年に1回以上	ソフトウェアライセンス証書や契約文書の所在確認 (真正性、完全性の確認を含む)
	保有するライセンスの数量の確認

③ ソフトウェアの不正利用に対する統制の見直し

上記でも示したとおり、現状と管理情報が乖離する一因として不正インストールなどによるソフトウェアの不正利用がある。過失か故意であるかを問わず、ソフトウェアを利用している事実が管理台帳に反映されない場合は、ソフトウェアライセンスの利用状況が現状と乖離し、やがてソフトウェアライセンスの違反につながる事となる。

ソフトウェアの不正利用に対する技術的な統制としては、「インストール権限の剥奪」や「外部記憶デバイス（特に CD-ROM ドライブ）を使用不可にする」などの対策が多く見られる。ただし、業務利用目的などによってはこれらの対策を講じることにより業務効率の低下などを招く場合もあるため、予防・発見、技術的・人的による統制の組み合わせに

より、組織に適した対策を実装していくとよいだろう。言うまでもなく、技術的なソフトウェアの不正利用に対する予防統制を取り入れていない場合は、導入ソフトウェアの棚卸し実施間隔を短くし発見統制を強めることも必要であろう。

なお、インストール権限を与えていないから棚卸は不要であるという考え方は、大きな間違いである。インストールが不要なソフトウェアがあることはもちろんのこと、ハードウェアの移動及び異動の確認、ライセンス関連部材の实在の確認も必要であり、スタンドアロンのように、現場で管理者権限を持って利用している場合もある。したがって、いかなる場合であっても棚卸という行為は必要である。

表 7-3 ソフトウェアの不正利用に対する統制例

	技術的	人的
予防	<ul style="list-style-type: none"> ・ インストール権限の剥奪 ・ CD-ROM ドライブの使用禁止設定 ・ ファイルサーバへのアクセス制御 	<ul style="list-style-type: none"> ・ ソフトウェア利用申請手続き ・ 教育や罰則の設定
発見	<ul style="list-style-type: none"> ・ インベントリツールによる情報収集 	<ul style="list-style-type: none"> ・ 手作業による導入ソフトウェア情報の収集

④ 従業員への教育や周知の徹底

従業員によるソフトウェアの不正利用に対しては、コンプライアンス教育を実施することによる抑止効果が期待できる。著作権の重要性を教育した上で、ソフトウェアの不正利用による法的な制裁や、組織における罰則を知らしめることにより、不正利用を行う動機は相当に減少すると考えられる。しかし、利用者たる従業員に教育するだけでは充分ではない。SAM に従事する者、特にソフトウェアの利用手続に関与する管理者及び担当者に対しては、より強いコンプライアンスと管理手続遵守の意識を植え付けなければ、管理手続は序々にほころび始めるであろう。

ソフトウェアライセンスの体系や条件などについて教育を実施することもライセンス違反を防止する上で有効であり、SAM に従事する者に対してはもちろんのこと、従業員に対してもソフトウェアライセンスに関する基本的な知識を身に付けるための教育の実施が望まれる。

教育の実施を計画する上では、従業員と SAM に従事する者として教育や周知の内容、頻度を変えることにより、最適なりソースで効果的な統制効果を生み出すことが期待できる。

以上、コンプライアンスのための計画のポイントを解説したが、やみくもにコストをかけて SAM を実施しても、SAM の効果を最大限享受できたとはいいがたい。ソフトウェア関連資産の管理や調達にかかるコストを合理化し、最低限のコストで最大限の効果を上げることが、経

営のためのツールとしての「SAM」に求められる。コスト削減・合理化のための施策には何があるのか、次項にて解説する。

7.1.2. コスト削減・合理化のための計画

(1) 標準化（統一化）におけるポイント

IT システムの増強や従業員数の増加などに伴い、組織が保有するソフトウェア関連資産は増加する傾向にある。更に、前項で解説した管理対象の拡大と合わさることにより、管理対象となるソフトウェア関連資産は増加の一途を辿ることになる。SAM の管理対象の増加は、管理台帳の更新や棚卸、ソフトウェアのアップデート、セキュリティパッチ、問い合わせ対応といった業務量の増加に直接的に影響し、IT コスト中の SAM にかかるコストの比率が高まることになるが、前述したとおり通常は SAM に対して十分な予算が割り当てられることは少ない。このような状況に対して、「標準化」の施策は管理対象を効果的に減少させる有効な方法である。

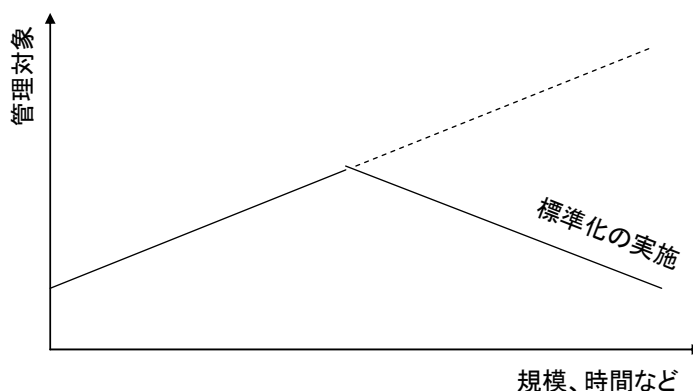


図 7-2 標準化の実施による管理対象の減少

SAM における標準化の対象としてソフトウェア関連資産（ソフトウェア・ハードウェア）と業務プロセスが該当する。以下にそれぞれの標準化の施策と便益について解説する。

① デスクトップ環境の標準化

一般の企業組織は、デスクトップ環境（パソコンなど）とシステム環境（サーバなど）を有し、企業によっては開発や研究、生産、流通、計測などの特殊環境を有している。大部分はデスクトップ環境が占めていると考えられる。仮にパレートの法則が適用できるとすれば、組織内で利用されている上位 20% のソフトウェアが、組織全体の 8 割で使用されていると考えられるが、大概の組織で該当するのではないだろうか。もしそうであれば、デスクトップ環境だけでも標準化を積極的に採用することにより、相当な管理コストの削減が期待できる。

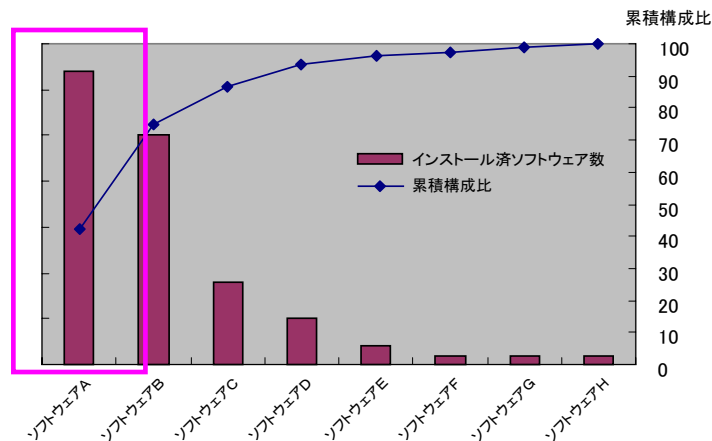


図 7-3 組織で利用されるソフトウェアの状況例

具体的には、デスクトップ環境のソフトウェア（OSやオフィスアプリケーション、その他共通して利用されるアプリケーション）を標準化することにより、セキュリティパッチやバージョンアップ、バグや問い合わせに対する情報収集量が減り、管理側の負担が大きく軽減される。また、セキュリティパッチやバージョンアップの適用を自動に行うためのツールを導入することにより、現場も含めた業務効率の向上が期待できる。

副次的な効果としては、

- ・ クライアント側のアプリケーションのバージョンが同一となることから、システムを構築する際の要件がシンプルになり、開発コストを抑制することができる
- ・ 大量発注することができ、ボリュームディスカウントのメリットを得ることができる
- ・ 問い合わせ対応の品質（回答内容やレスポンス）が向上する

などが挙げられる。ソフトウェアだけでなくハードウェアについても標準化することによるメリットは大きく、ソフトウェアの場合と同等のメリットを得ることができる。

ただし、標準化することによるリスクも同時に存在する。特定のソフトウェアやハードウェアに依存することになるため、初期不良や重大な不具合、未知のウイルス、ベンダーの倒産などに直面した場合、事業継続上の問題につながりかねない。このようなことから、1種類ではなく、2種類以上の標準環境を順次展開している組織が多く見られる。特にデスクトップ環境における端末数が多い企業においては、計画的に標準環境を導入しその裏で次期標準環境のテストを実施する態勢を整えておくことが肝要である。

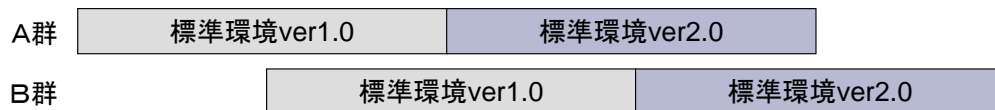


図 7-4 標準環境の順次展開

② 業務プロセスの標準化

事業部制を敷いている企業や、中央官庁及び自治体など、事業部や部局に管理責任をおき自治を尊重する風土が根付いている組織では、各事業部あるいは各部局でそれぞれ資産管理を実施しているところが多い。これ自体は否定することではないが、このような組織の多くは管理手続や管理台帳を独自で作成し管理している。このことにより、

- ・ 管理手続や管理台帳を独自で作成するため、ムダなコストが発生している
- ・ 管理手続や管理台帳に実効性がなく有効な管理が行えていない（意味のないムダな管理を行っている）
- ・ 管理台帳のフォーマットが標準化されていないため、情報を集約して組織全体の管理状況を可視化するためにムダな作業が必要となる

など、SAM に関して多くのムダが生ずることとなる。各事業部あるいは各部局でそれぞれ資産管理を実施することを選択する組織においては、可能な限りにおいて管理手続や管理台帳は標準化したものを共通的に各事業部や各部局で利用させることが望ましく、これにより組織全体の SAM に関するコスト削減につながることを期待できる。

そもそも、各部門に管理を一任し、その管理レベルも管理状況も把握していない状態は、SAM においては分散管理とは言わない。分散管理とは、組織全体の管理目標や管理レベルを示し、かつ、その管理状態を把握できている状況をいうものである。

分散管理を採用する場合は、管理規程を統一した上で管理マニュアルの雛型を用意し、部門によって管理手法や管理レベルに差異が生じない仕組みを導入する必要がある。

(2) 業務プロセスの見直しにおけるポイント

① ソフトウェアライセンス調達における助言機能の設置

SAM に関するコスト削減の実現において、ソフトウェアの調達コストを抑えることは有効な策である。特に、規模が大きい組織においては、その効果は顕著となる。直接的にソフトウェアの購入費用を抑えるには、コストメリットのある買い方ができるかどうかが決め手となる。

ソフトウェアライセンスの条件や購入方法に精通し、ソフトウェアライセンスの調達に当たって助言ができる担当者を組織内に設置することが望ましい。ソフトウェアの調達プロセスを集中化している組織においては、ソフトウェアを調達する部門内に設置するとよいだろう。調達を各現場で行っている組織においては、各現場に前述のような担当者を設

置ることが難しい場合もあるため、各現場から問い合わせができるような仕組みを整備することで同等のメリットを享受することが可能である。

ソフトウェアライセンスの調達に当たって助言ができる担当者にはソフトウェアライセンスに精通していることが要件として求められる。したがって、ソフトウェアベンダーとの情報交換を密に行い、ソフトウェアライセンスの条件や購入方法、それらに変更が加わった場合はその変更点などについて、十分な情報収集を継続的に行うことが求められる点についても付記しておく。

② 資産情報の集約化

ソフトウェア関連資産に関する情報が集約されることにより、適時にソフトウェア関連資産の状態を把握することが可能となり、

- ・ 調達時に遊休状態にあるソフトウェアライセンスやハードウェア資産を把握できるため、二重買いの防止や資産の有効利用が可能となり、調達にかかるコストを削減することができる
- ・ 財務管理や契約管理など、他の管理システムとの連携が可能となり、全社的な管理効率が向上する

などのメリットを享受することが可能となる。

資産情報を集約する方法としては、管理台帳を一元化し集中管理することが考えられるが、分散管理においても各現場の情報が適時に収集し情報集約できる仕組みを整備することにより同等のメリットを享受することが可能である。ただし、各現場でスプレッドシートを用いて管理している場合は、組織全体としての資産情報を迅速に把握することが困難な場合が多いため、SAM ツールの導入の検討が望まれる。

7.2. SAM を組織へ定着させるためのポイント

前節で述べたように、SAM に関して様々な計画を立てて実施していくべきであるが、その中でも教育や周知活動については、最新情報の提供だけでなく、教育対象の漏れや意識の風化を防ぐ観点からも毎年実施することが望ましい。情報セキュリティやコンプライアンスについての教育及び周知活動は、既に多くの組織において取組まれているところであるが、ソフトウェアライセンスやソフトウェア資産管理に関する教育や周知活動を実施しているところはまだまだ多くないのが実情である。SAM を組織に定着させるためには何を教育・周知させればよいのだろうか？

ポイント①：著作権、契約順守などの重要性の理解

「ソフトウェア」は目に見えない無形物であることに加え、わが国の風土や歴史的背景から契約の法的拘束力に関して意識に乏しいことが、ソフトウェアライセンス違反の原因と言

われて久しい。国内の著作権保護団体の様々な活動により、ソフトウェアライセンス違反が発覚した場合の金銭的ペナルティや風評被害についてはよく知られるようになったが、罰則の理解がコンプライアンスの理解ではない。ソフトウェアライセンス順守を受身ではなく前向きに取り組むためには、著作権や契約順守の重要性を説くことが何よりも重要である。著作権保護の重要性に関しては、国内の著作権保護団体のサイトを参考にするとよいだろう。

- ・文化庁

<http://www.bunka.go.jp/> ※文化庁サイト内「著作権に関する教材、資料など」

- ・社団法人コンピュータソフトウェア著作権協会（ACCS）

<http://www2.accsjp.or.jp/>

- ・ビジネスソフトウェアアライアンス（BSA）

<http://www.bsa.or.jp/>

また、ソフトウェアを利用する際に使用許諾条件を確認することもコンプライアンスだけでなくセキュリティの観点からも重要である。例えば、ソフトウェアの中には、「Web 閲覧履歴などの情報を外部に送信し広告を送ることを許諾する」ような条文が使用許諾条件に含まれているものもある。組織の方針にそぐわないソフトウェアを誤って導入しないためにも、使用許諾条件の事前確認について、ソフトウェアを利用する全員に対して周知徹底を図ることが望まれる。

ポイント②：ソフトウェアの利用に関する手続きの周知徹底

組織が従業員や役職員にソフトウェアを利用させるに当たって、どのような手続きを定めているかを周知し、手続きの実施を徹底させることがソフトウェアに関するコンプライアンスにつながる。

特にソフトウェアの利用に関する手続きの周知は重要であり、ソフトウェアの不正利用防止の要となる。また、利用だけでなく利用の終了（アンインストールなど）や廃却などについての周知も重要である。不要なソフトウェアや使い終わったソフトウェアはすぐにアンインストールや削除を行うことにより、ソフトウェアライセンス違反が起こりにくくなるだけでなく、他のパソコンで利用することによりソフトウェアライセンスを有効に活用することもできる。単なる手続きの伝達に終始せず、その必要性やメリットなどを併せて伝えることによって効果的な周知につなげることが重要である。

ポイント③：ソフトウェアの調達に関する手続きの周知徹底

ソフトウェアの調達手続きについても周知徹底を図っておきたい。ソフトウェアをどのように調達するかによって、調達にかかるコストを削減できる場合もあればムダに支払ってしまうこともある。ソフトウェアを各部門で購入している組織においては、ディスカウントを受けられることができる有利なソフトウェアライセンスの購入方法があるにもかかわらず、パッケージ単品を購入してしまうなどがよく起こりうる。このようなことが組織全体で日常的に行われていれば、相当なムダが生じることになる。こういったムダを防ぐためにも、ソフト

ウェアを購入する場合の手続きや、リースを利用する場合の手続きなどについて、ソフトウェアの調達担当者に周知しておくことが望まれる。

更には、どのようにソフトウェアを調達するとコストメリットがあるのかをノウハウとして伝えることにより、コスト削減の効果が期待できる。ソフトウェアライセンスの条件や購入方法、リースの方法などについて、ソフトウェアの調達担当者に対し定期的な勉強会を開くことも有効である。

ポイント④：罰則の周知

「なぜやるのか」、「どうやるのか」の後は、「やらないとどうなるのか」の周知である。利用者たる従業員や役職員に対して罰則を周知することは必要ではあるが、多くのルールを順守しなければならない中で意識を高めることは容易ではない。むしろ、管理レベルの向上に伴い、管理者や担当者に対して罰則の周知を図るほうが効果的である。特に SAM 従事者がソフトウェアの不正利用に加担するようなことがあれば、コンプライアンスに対する統制は意味をなさなくなる。このようなことが起こらないためにも、ソフトウェアの利用者だけでなく、SAM 従事者に対しても罰則の設定と周知が重要である。

ポイント⑤：網羅的な教育

あらゆる階層に対して必要な教育を提供することが、教育の有効性を高めるためにも重要なポイントである。SAM に関しても同様に、経営層、管理職、従業員、SAM 従事者といったそれぞれの役割に対して必要な教育を施すことにより、組織全体のソフトウェアに関するリテラシーが向上する。下表のようなマトリックスを作成し、漏れなく計画的に教育を実施することを心がけたい。

表 7-4 教育内容と対象のマトリックス例

教育内容	教育の対象（○必須、△任意、－対象外）			
	経営層	管理職	SAM 従事者	従業員、 派遣社員
著作権や契約に関するコンプライアンス	○	○	○	○
ソフトウェアにまつわる事故やその対応に関する動向	○	○	○	○
ソフトウェア資産管理に関する他社事例、動向、ベストプラクティス	△	△	○	－
ソフトウェア資産管理の方針と罰則	○	○	○	○
自社におけるソフトウェア資産管理態勢（方針、組織体制、活動内容など）	○	○	○	△
ソフトウェア資産管理における手続き	△	○	○	○

7.3. 棚卸の実施におけるポイント

棚卸作業とは、簡単に言えば管理台帳上の情報と現状の差異を検出し、あるべき状態に修正することである。台帳管理の手続きが有効に機能していることを確認することにより、ライセンスコンプライアンスの説明責任を果たすことができる。更に、コスト削減・合理化を達成するに当たっては管理台帳上の情報が正確であることが前提であり、棚卸作業は SAM の効果を左右する重要な作業の一つである。

前述したように、棚卸作業を定期的実施することで、管理台帳上の情報の正確性を保つことができる。管理台帳上の情報の正確性をより高いレベルで維持するためには、なるべく頻繁に棚卸をすることが求められるが、そのためには棚卸作業にかかるコストを考慮し効率的に実施することが望まれる。以下に、棚卸を実施する際に留意すべきポイントを解説する。

ポイント①：ハードウェア資産の網羅的な把握

ソフトウェアライセンスを適切に管理するためには、組織が保有するハードウェア資産を「網羅的に」把握することが何よりも重要である。管理対象であるハードウェア資産が管理台帳上の情報どおりに存在するかを確認するだけでなく、管理から漏れているハードウェア資産の存在についても確認することが必要である。更に、ハードウェア資産を正確かつ網羅的に把握するために、納品書などの購入履歴といった証憑を併せて実在性を確認することも検討する。

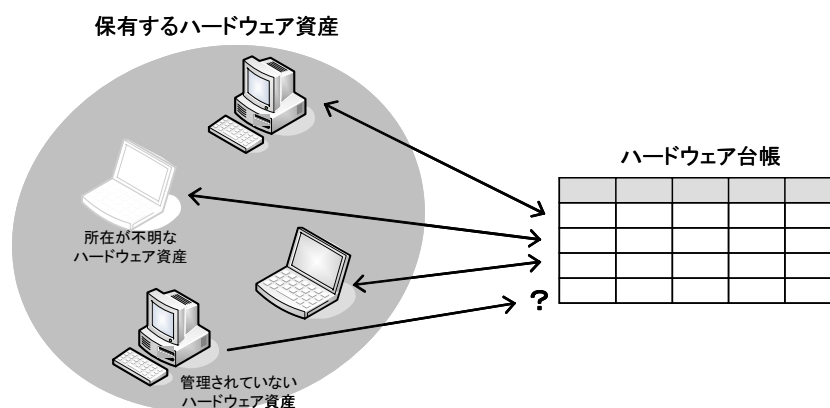


図 7-5 ハードウェア資産の網羅的な把握

インベントリ収集ツールなどを用いるなど IT を活用することにより棚卸作業の効率化を図ることも検討したいポイントである。インベントリ収集ツールなどを用いる場合は、ネットワークに接続されていないスタンドアロン PC や予備機、電源が入っていないハードウェア資産や修理中のハードウェア資産などを見落としやすいため、棚卸の手續策定において留意しておく必要がある。

なお、自動収集するだけでは、現物とツールによる収集情報を紐付けることは容易ではないことから、現物との紐付けを容易にするための確認作業は別途必要であることを忘れてはならない。

ポイント②：利用されているソフトウェアの正確な把握

次に棚卸において重要なポイントは、ハードウェア資産が網羅的に洗い出された後、そのハードウェア資産上で利用されているソフトウェアを正確に把握することである。ハードウェア資産上で利用されているソフトウェアが台帳上の情報と一致しているかどうかを確認する。なお、利用されているソフトウェア情報を取得する際は、保有するソフトウェアライセンスとの照合を考慮し、ソフトウェア名称だけでなく、必要に応じてバージョン情報なども取得しておく。

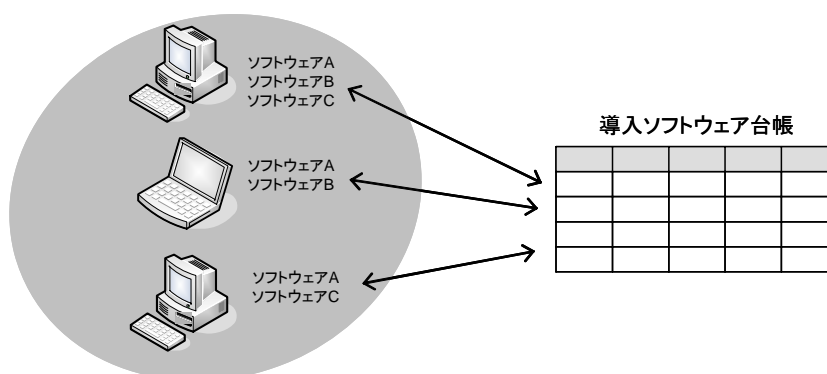


図 7-6 導入されているソフトウェアの把握

収集方法は、インベントリ収集ツールを用いる方法や、WindowsOS であればレジストリ情報をコマンドで取得する方法、「アプリケーションの追加削除」を確認する方法などがある。インベントリ収集ツールを利用しない場合は、調査票ベースで従業員や管理者、あるいは外部業者などに調査させることになるが、現場に負担を強いることは組織全体の生産効率低下が懸念され、外部に任せる場合はコストがかかること、また、正確性も担保できないことから、SAM ツールを導入することが望ましい。

ポイント③：保有するソフトウェアライセンス関連部材の確認

ソフトウェアライセンスを組織が保有していることを証明できなければ、そのソフトウェアの利用がライセンス違反として捉えられてしまう可能性が高い。そのため、ソフトウェアライセンスを保有していることを証明するための証拠となる関連部材は確実に管理しておきたい。また、ソフトウェアベンダーによってその証拠能力の捉え方が異なることから、ソフトウェアを調達する段階でソフトウェアベンダーに問い合わせしておくことも重要である。(6.8.1.1. 棚卸 (3) を参照)。

ソフトウェアライセンスの関連部材は一式が揃っていないとソフトウェアライセンスを保有していると見做されない場合もあるため、同梱されるライセンス関連部材にシールなどで付番し管理することが望ましい。

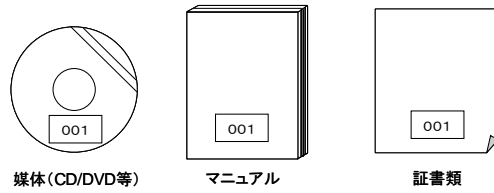


図 7-7 同梱されるライセンス関連部材の付番による管理

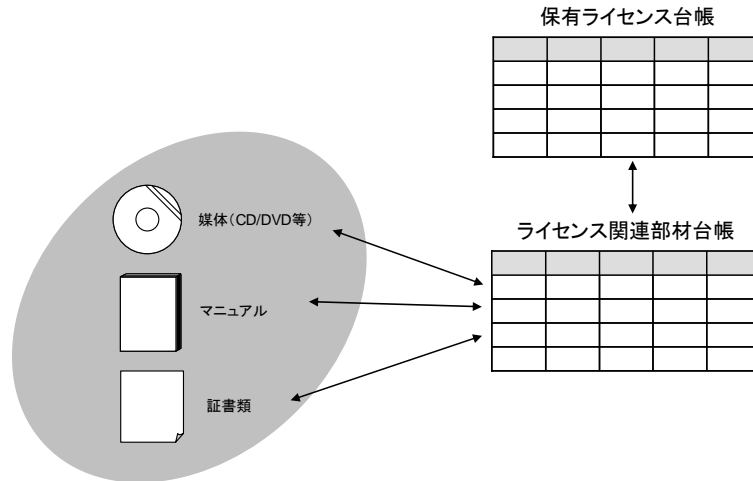


図 7-8 ライセンス関連部材の把握

ポイント④：差異分析と再発防止のための改善

管理台帳上の情報と現状とを照合し、その間に差異が認められた場合は、その差異が発生した原因を分析し、再発防止につなげることが SAM の改善において重要なポイントである。管理台帳上の情報に差異が発生する要因として、

- ・管理台帳への登録・更新・削除に関する手続上の不備
- ・管理台帳への登録・更新・削除に関する運用上の不備
- ・ソフトウェア関連資産の紛失や盗難、誤廃棄
- ・ソフトウェアの不正利用
- ・管理台帳上の情報に対する不正操作

など様々に考えられるが、故意、過失のいずれの場合においても、再発防止のための改善策を講じておくことが望まれる。

7.4. SAM 監査におけるポイント

SAM を是正し継続的に改善させるためには、SAM を定期的にモニタリングすることが欠かせない。SAM が設計したとおりに適切に運用されているか、また設計された SAM 自体に不備はないかを確認し、SAM を是正し改善させるための計画策定につなげるのが SAM におけるモニタリングの役割である。本節では、SAM をモニタリングする手段としての「SAM 監査」を

効率的かつ効果的に実施するために考慮すべきポイントについて解説する。

7.4.1. SAM 監査計画の策定

ポイント①：監査目的の決定におけるポイント

監査目的については、SAM の管理目的に照らして決定するのがよい。「ライセンスコンプライアンス（法的リスクの回避）」を例にとると、

1. ライセンス違反を起こさないための方針や統制のための手続きが適切に整備されていることの確認
2. ライセンス違反を起こらないための統制が適切に運用されていることの確認
3. ライセンス違反が発生していないことの確認

を実施するとよいだろう。ライセンスコンプライアンスだけでなく、コスト削減・合理化の観点からもモニタリングすべきであるが、監査資源によっては監査テーマを絞りこむことも必要である。リスクや SAM に関する動向、経営からの要請などにより、時宜にあった適切な監査を実施したい。

表 7-5 監査の概要（テーマ・目的）と監査対象の一覧例

SAM 監査テーマ	監査の目的	監査対象部門
ライセンス コンプライアンス (法的リスクの削減)	<ul style="list-style-type: none"> ・ ライセンス違反を起こさないための方針や統制のための手続きが適切に整備されていることの確認 ・ ライセンス違反を起こらないための統制が適切に運用されていることの確認 ・ ライセンス違反が発生していないことの確認 	情報システム部 研究開発部 総務部 ……
TCO の削減 (購入コスト)	<ul style="list-style-type: none"> ・ コストに配慮したソフトウェアの購入方針と手続きが適切に整備されていることの確認 ・ ソフトウェアの購入手続きが適切に運用されていることの確認 	情報システム部 調達部 財務経理部 ……
TCO の削減 (管理コスト)	<ul style="list-style-type: none"> ・ 業務や手続、申請書など、簡素化や共通化ができる要素について、その実現可能性と効果に対する確認 ・ 業務や管理対象など、標準化や統一化ができる要素について、その実現可能性と効果に対する確認 ・ 業務や情報など、一元化や集中化ができる要素について、その実現可能性と効果に対する確認 	情報システム部 総務部 財務経理部 ……

ポイント②：監査対象の決定におけるポイント

SAM の特性として、業務横断的、組織横断的、管理目的が複数存在する、などが挙げられるが、SAM を監査する上でもその特性は考慮しておく必要がある。SAM の監査の実施は任意であり、監査資源（監査人・予算・時間など）は潤沢に確保できないことも多い。したがって、監査資源の制約の中で監査目的を達成できるように、何をどこまで監査するのかを吟味することが必要である。

監査対象は、リスクアプローチにより決定することが有効である。管理対象のソフトウェア関連資産や組織範囲のすべてを対象に監査を実施することは監査資源との兼ね合いから現実的でないことも多い。リスクアプローチにより、例えばライセンスコンプライアンスにおけるリスクやコストにおける影響度が高いと判断されたソフトウェア関連資産や部署に対して、監査資源が許す範囲で効果的な監査を実施することができる。

また、監査対象を決定する際は、下記のような環境の変化や動向などにも留意したい。監査資源の制約により単年度で監査できない場合は、複数年度にわたって計画を策定し、例えば監査対象のソフトウェアや部署をローテーションして監査するなど、監査対象が網羅的に監査されることが望まれる。

表 7-6 環境の変化や動向などの例

外部環境	<ul style="list-style-type: none">・ ソフトウェアライセンスの違反に関する事件や動向・ ソフトウェアの利用におけるシステム停止などの事故や動向・ ソフトウェアベンダーによるライセンス条件や契約などの変更など
内部環境	<ul style="list-style-type: none">・ SAM に関する組織や手続きの変更・ 部署の新設、統合、引越など・ 利用形態の追加（自宅利用、海外への持ち出し、他）など

ポイント③：評価基準の選定と監査手続の作成

監査を実施するに当たっては、監査目的を達成するために、何をどのように確認すればよいのかを明らかにするための監査手続を事前に作成しておく必要がある。監査手続を作成するに当たっては、SAM の整備状況と運用状況を確認するための手続を整備すべきである。

整備状況の確認のためには拠り所となる基準が必要となるが、SAM においては次の基準を利用することをお勧めする。

- ・ ISO/IEC 19770-1 (JIS X 0164-1)
- ・ 「ソフトウェア資産管理基準」(SAMCon)
- ・ 「ソフトウェア資産管理評価規準」(SAMCon)

ここでは、「ソフトウェア資産管理基準 Ver2.0」を例にとり説明する。「ソフトウェア資産管理基準 Ver2.0」では、各管理要件に対して管理目的が関連づけられている。例えば、ライセンスコンプライアンスに関して監査をする場合であれば、「法的リスクの回避」に○がついている管理要件を抽出し、その管理要件を確認するための具体的な手続をまとめていけばよい。例えば、「不正使用についての教育を実施している（図 7-9、点線枠内）」を確認するためには、

- ・不正使用についての教育を実施するための規定が存在することを確認（整備状況）
- ・実際に不正使用についての教育を実施したことの証跡を確認（運用状況）

をすることになる。関連する管理要件について個別に監査手続を検討し、一覧表にまとめておくとよい。

管理要件	認識	不正使用について警告、教育がされていること	管理目的との関連			
			アカウンタビリティ	法的リスクの回避	TCOの削減	セキュリティ
管理項目						
①不正使用についての警告をしている				○		
②不正使用についての教育を実施している				○		

図 7-9 ソフトウェア資産管理基準 Ver2.0（抜粋）（出典：SAM コンソーシアム）

表 7-7. SAM の監査手続例

要求事項	監査手続	
	整備状況	運用状況
...		
不正使用についての教育を実施している	<ol style="list-style-type: none"> ソフトウェアライセンスの不正使用について教育を実施する旨が管理規程上に規定されていることを確認する。 ソフトウェアライセンスの不正使用に関する教育の手順が規定されていることを確認する。 	<ol style="list-style-type: none"> ソフトウェアライセンスの不正使用に関する教育計画が策定され、SAM の責任者により承認されていることを確認する。 ソフトウェアライセンスの不正使用に関する教育の受講履歴を確認し、教育対象の全員が受講していることを確認する。 ソフトウェアライセンスの不正使用に関する教育の受講履歴がSAM の責任者により承認を受けていることを確認する。
...		

7.4.2. SAM の監査実施

①監査の効率化におけるポイント

SAM を適切に運用するためには多くの管理手続を整備する必要があるが、管理手続の数に応じて証拠が増えることにもなり、監査にかかる工数は増加することになる。限られた監査資源において、監査工数の増加は監査品質の低下につながる。したがって、なるべく監査を効率的に進められるよう環境整備しておきたい。

特に、効果が高いのが IT の活用である。インベントリ情報の収集や、保有ソフトウェアライセンスと使用ソフトウェアライセンスの照合が可能なツールの導入や、申請手続きのワークフロー化などにより確認のための工数を大きく軽減することが可能となる。同じ監査資源で精緻な監査を実施することにより、監査の効果を高めることができる。

また、管理の集中レベルが監査の負荷に対して影響を与えることに留意しておきたい。集中管理している場合はリスクも集中するため、監査資源を集中的に投下することができる。これにより監査にかかる工数が軽減されることになるだけでなく、少数の部署に対する監査で組織全体の SAM に関するリスクをある程度捕捉することができる。

コスト削減・合理化のための施策がモニタリングにまで効果が及ぶことを念頭に SAM を改善していくことも肝要である。

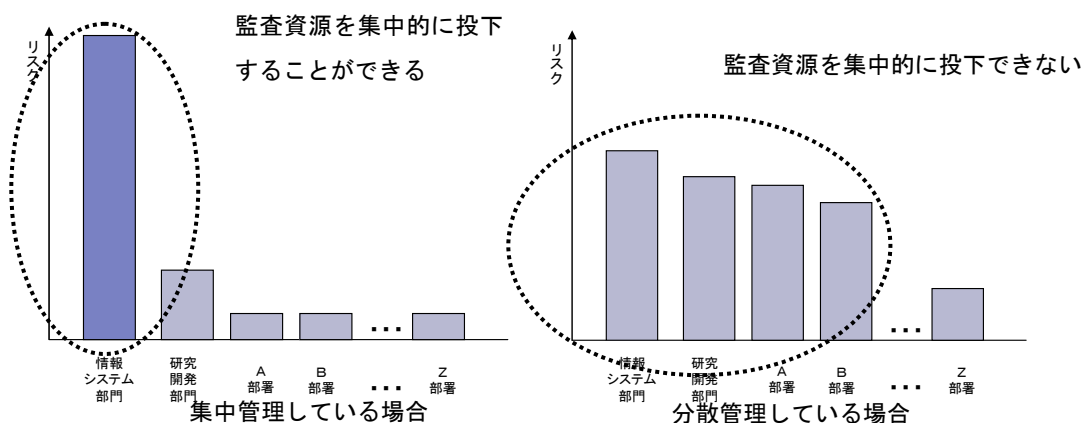


図 7-10 管理の集中度合とリスクの分布

8. SAM ツール利用のためのポイント

8.1. ツール利用による運用の効率化

SAM の運用を効率化するためには、ツールを利用することが望ましい。

ツールを利用することで、夜間のビジネス利用されていない時間帯に自動採取することができたり、ネットワーク回線経由でインベントリ情報を送信することにより、遠隔地にあるマシンからのインベントリ収集も容易に行えるなど、さまざまな効率化のポイントがある。

ツールの他の活用例として収集したインベントリの結果分析により、収集できていない PC や私有 PC の不許可接続、また、禁止ソフトウェアの検出も行うことができる。また、これら検出結果を自動的に管理者や利用者宛に送付することができるツールであれば機器の故障、ネットワーク接続の不備、不正な IT 資産利用のチェックといった機能を持つツールもある。

しかしながら、ツールですべての情報が自動収集でき、管理できるわけではない。ネットワークにつながっていないもの、また、ツールが動作しない OS などがあるためである。

また、前節でも述べたように、ツールだけで自動収集した場合には、どの現物の情報が収集されていて、どの現物の情報が収集されていないのかを判別することは容易ではない。したがって、ツールを利用したとしても、最終的には人的管理により管理台帳とつき合わせて棚卸を実施するなどの措置が肝要である。

8.2. SAM ツールとは

本ガイドは、SAM の運用についてまとめたものであり、その運用を支援するツールを、SAM ツールとして定義する。

「1.ソフトウェア資産管理(SAM)の位置づけ」で説明されているとおり、SAM ツールは、ハードウェア、利用ソフトウェア、保有ライセンスの管理を支援するための製品である。

ただし、一般的に販売されているソフトウェア製品で、SAM の支援だけに特化した製品はほとんどなく、より広い機能範囲をカバーする統合運用管理製品、IT 資産管理ツール、セキュリティ製品などにその機能範囲が含まれて製品提供されているものが多い。SAM ツールは、その出自として、次の五つに大別される。

① インベントリ管理を目的とするツール

人手で行ってきた棚卸作業をソフトウェアで実現したもの。ハードウェア、ソフトウェアの IT 資産情報の収集、棚卸確認、契約情報管理、管理台帳の帳票出力といった機能が実装されたもの。

② セキュリティパッチやソフトウェアの配付を目的とするツール

従来からある配布機能をもつ製品が、インベントリ収集機能を機能追加することで SAM ツールとしての機能を実装したもの。

③ 不正接続や使用禁止ソフトの検知などを目的とするツール

セキュリティ製品が、パッチ管理の対象を一般的なソフトウェアに拡張し、SAM ツールの機能を実装したもの。

④ ログ管理を目的とするツール

ログ管理製品が機能拡張し、SAM ツール機能を実装したもの。

⑤ IT 資産全般の運用管理を目的とするツール

統合運用管理製品の一部として SAM ツール機能が提供されるもの。

上述のような製品の成り立ちにより、それぞれの製品の長所/短所は異なっており、SAM ツールと一口に言っても、それぞれのツールが対応している範囲及び機能の詳細は異なっていることが多い。

これら各種製品を SAM の対象資産や目的又は、導入済み他製品との関連、自組織のシステム環境など、さまざまな観点で評価し、製品の導入を検討する必要がある。

8.3. IT 資産のライフサイクル管理と関連ツール

IT 資産のライフサイクル管理を行うにあたり、次の五つのステップを考える必要がある。

それは、「計画」「調達」「導入,展開」「運用,保守」「廃棄,返却」である。それぞれのステップにおいて、利便性を補助するツールが存在し、SAM を行う上で、これらツールの利用を検討し、それらのツールが提供する機能を利用することは運用上、欠かせない。

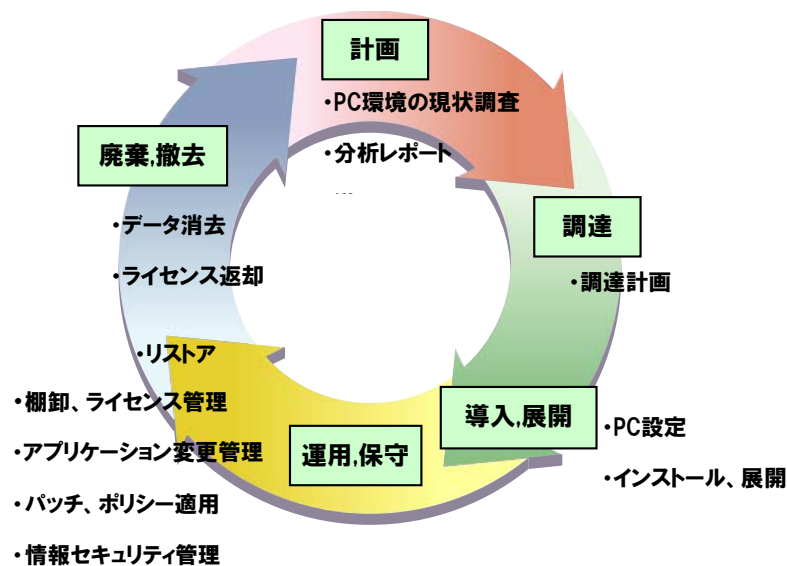


図 8-1 IT 資産のライフサイクル管理

具体的な活用フェーズとしては、次のようにまとめられる。

表 8-1 PC ライフサイクル管理活用フェーズ

ステップ	項目内容
計画	PC 環境の現状調査、調査レポート
調達	調達計画
導入、展開	PC 設定
	インストール、展開
運用、保守	ハードウェア管理、アプリケーションの稼動管理、障害・通報管理
	ソフトウェアライセンス管理、契約管理、指定アプリケーション管理
	禁止ソフトウェア管理
	アプリケーション制御
	利用ソフトウェアのメータリング
	パッチ適用・配布、ウイルス定義配布
	操作ログ管理
	デバイス制御機能
	ポリシー管理
	障害復旧
	リモートコントロール
廃棄、撤去 返却	データ消去 ライセンス返却

上記ステップで用いられるツールとしては、次のようなものがあげられる。

- ① 計画：
 - PC 環境の現状を把握するため、「SAM ツール」が用いられる。
- ② 調達：
 - 明示的に用いられるツールはないが、購入プロセスと連携した「ワークフローツール」の利用が考えられる。
- ③ 導入、展開：
 - 大規模環境への展開では、同一ソフトウェア環境を簡易に作成するため、マスタ PC を作成し、そのクローンを展開するといった作業が行われていることが多い。こうした作業を支援するツールとして、「PC キットティングツール」と呼ばれる、ネットワーク経由あるいは CD-ROM などを用いて PC の設定(ネットワーク設定、ソフトウェアのインストール)を自動的に配信し設定することが可能なツールが用いられる。なお、PC キットティングツールを利用する際には、OS やソフトウェアの使用許諾条件を確認し、使用許諾に反した作業(クローンマシンの作成など)を行うなどの不正行為をしない

いように注意する必要がある。また、マスタ PC 導入後に、一律のソフトウェア環境を実現するために「配布ツール」が用いられることが多い。

④ 運用、保守：

- 半期に一度の棚卸や、インベントリ管理として「SAM ツール」が用いられる。不正なソフトウェア利用の検出、不許可 PC のネットワーク接続などのセキュリティリスク管理として、「セキュリティ対策ソフトウェア」が用いられる。パッチ管理、配布などで「配布ツール」が用いられる。障害対応などで遠隔地の PC を操作するための「リモートコントロールツール」などが用いられる。

⑤ 廃棄、撤去：

- 廃棄 PC からソフトウェアを削除するための「データ消去ツール」が用いられる。消去されたソフトウェア情報と紐づいていたライセンス返却を実行するために「SAM ツール」が用いられる。

8.4. SAM ツールの機能比較

SAM ツールの機能比較としては、前項に記した機能内容と、導入にあたり必要とされる機能とのマッピングを行い、製品間の優劣を検討するのが、効果的である。

ここでは、SAM を行う観点でのツール選択を行うための観点として、重要となるインベントリ収集機能、構成管理機能、台帳管理機能の三つに焦点をあて、以下比較のポイントについて説明する。

8.4.1. インベントリ収集機能の比較

(1) 収集方法

(ア) 自動収集

- ① エージェントインストールあり
- ② エージェントインストールなし

(イ) 手動収集

- ① インベントリ収集ツールの実行 (USB メモリなどに仕込んで実行するほか、ログインスクリプトなどに追加し、半自動的に実施させることができるものもある)
- ② インベントリ情報ファイル(テキストファイル、XML ファイル、Excel ファイルなど)
- ③ 管理画面からの入力

インベントリの収集方法としては、管理対象機器にプログラム(一般的に、「エージェント」と呼ばれている)をインストールし、このエージェントモジュールがレジストリ、ファイルなど参照し、情報収集することで、資産管理対象より自動収集する方法と、データファイル、管理コンソールからの入力などで、手動収集する二つの方法に大別される。

自動収集する方法では、更に、エージェントをインストールし、情報採取するタイプと、ネットワーク機器や IT 機器を制御、管理する通信プロトコル(SNMP,WMI など)を活用して、

エージェントレスで、インベントリ収集を行う二つに大別される。長所/短所は、それぞれがクロスする関係にあり、導入するユーザー環境に応じて、適切なタイプを選択する必要がある。

表 8-2 組織の環境によるエージェント利用の組み合わせ

組織の環境	特性	利用タイプ	
		長所	短所
通常会社	エージェントのインストール可能	エージェントタイプ (各 PC へのインストールあり)	
		詳細なインベントリ情報の入手が可能 パッチ配布も可能 夜間の集約処理可能 (バッチ管理など)	大量マシンへの展開に時間がかかる 既存のソフトウェア資産との動作組み合わせで問題が起きる可能性がある。
病院	24 時間のコンピュータ/ネットワーク稼動が必要 インベントリ情報の収集の負荷制御が必要(ネットワークへの負荷軽減) 夜間バッチ処理不可	エージェントタイプ (各 PC へのインストールあり)	
		詳細なインベントリ情報の入手が可能 パッチ配布も可能	インベントリ収集時、パッチ配布時にネットワーク負荷の軽減要 PC・ネットワークの停止不可
データセンター (ホスティングサービス)	ホスティング資産へのインストール不可	エージェントレスタイプ (各 PC へのインストールなし)	
		リモート環境を展開する時間が不要 管理対象のソフトウェア資産への影響なし	取得できるインベントリ情報が限られる パッチ配布は不可

例えば、自社オフィスに導入し、ネットワークに接続された大量の PC についての資産管理を行う場合は、エージェントインストールありのタイプを選択するのが望ましいと考えられる。

また、エージェントインストールありのタイプの選択が可能であるが、病院などでは、PC、ネットワークの 24 時間稼動という観点より、インベントリ収集やパッチ配布時にネットワーク上を流れるデータ量の負荷制御や、PC やネットワークの停止不可といった制約が追加され、これらも考慮できる製品を選択するのが望ましいと考えられる。

一方、データセンターなどでホスティングしている顧客資産に対しての資産管理であれば、

勝手にエージェントをインストールすることはできないため、後者のエージェントインストールなしのタイプを選択するのがベストであると考えられる。

また、管理対象として両者がミックスされた環境を管理する場合など、複数の収集方法を総合的に管理できれば、そういう機能を持つ製品を選択することが最善と考えられる。

手動でインベントリを収集する場合は、収集できるバリエーションがあるほうがよりよいと思われる。

手動でインベントリ情報を収集するケースとしては、次の三つのシーンが考えられる。

一つ目は、エージェントをインストールして、インベントリ情報を採取することが物理的に不可能な資産を管理する場合である。この場合は、直接 SAM ツールの管理コンソールから、ライセンス関連部材についての資産情報入力が可能で、かつ大量にデータがある場合は、ファイルなどにデータを記載し、インポート処理を実施する機能により、一括登録できる機能がある製品を選択すべきである。

二つ目には、エージェントをインストールできても、スタンドアロンのマシンなどでネットワークに直接接続していない機器からのインベントリ情報収集の場合がある。たとえば、工場などに設置している機器など、物理的にネットワーク接続がない場合、また、古いコンピュータで、ウイルス対策パッチが対応されなくなり、セキュリティ上の問題で、接続できない場合などである。このような場合、インベントリ情報を収集するエージェント及び採取データを USB メモリなどの手段で可搬に持ち込める形態で動作するツールが提供されている製品を選択することが望ましい。

三つ目には、既に別の製品を使っていて、そこから違う製品に乗り換える場合、既存にインベントリ情報が集まっていて、それを再利用するというケースも考えられる。この場合は、直接データベースに登録されているデータをそのまま移行するのは、それぞれの製品間でのテーブル定義が異なるため、一旦、テキストファイルなどにデータを出力し、その出力されたデータを移行製品のテーブル定義にあわせて編集し、インポートするというのが一般的な運用である。これら、他社製品からの移行を簡易にする仕組みを持つ製品を選ぶと移行作業が省力化できるので、この点も製品選択時の検討項目になると考えられる。

なお、自動でインベントリを収集する場合、最終収集日が一定期間以上更新されない情報を洗い出す機能があることが望ましい。ネットワーク接続されているはずのハードウェアが、例えば2週間以上に亘ってインベントリデータが収集されないというのは、廃棄・返却したのに、その手続がなされていない場合や、紛失している場合が考えられるためであり、こういった事象を定期的に把握する仕組みを持つことは、ツールを利用する場合に、重要なポイントの一つである

(2) 収集可能な資産

表 8-3 管理可能な IT 資産

コンピュータ	ネットワーク機器	その他 IT 機器	インベントリ 以外の情報
Windows Linux UNIX(HP-UX,Solaris,AIX..) Macintosh メインフレーム PDA	ルータ スイッチ プリンタ	マウス キーボード Etc.	インストール媒体、 ライセンス証書 (契約書など)

収集可能な資産は、種類が多ければ多いほどよいが、かといって、管理用途で不要な機能を持ち、それにより、価格が高い製品を選ぶとコストパフォーマンスが悪い場合もある。

実際にインベントリ管理必要な資産を管理できる製品、また、直接管理できなくても、他ツールで収集した結果をインポートできる機能で補完できる製品など複数製品を組み合わせた総合力でも検討する必要がある。

(3) ソフトウェアライセンス管理

SAM ツールの機能の一つに、購入したライセンスと導入ソフトウェアとの紐付け管理を行う機能がある。

紐付けの際には、ユーザがアプリケーションの追加と削除から取得された構成情報などと確認を行い、手動で紐付けを行う方法が一般的である。

なお、Office 製品などで、市場シェアの高いものについては、ソフトウェア辞書という形式で、ある特定の構成管理情報が登録された場合に、インベントリ情報として採取されるレジストリ情報をこのソフトウェア辞書情報と照らし合わせることで、製品名を特定し、自動的にライセンスとの紐付けを行える製品もある。

ただし、ソフトウェア辞書がカバーできる範囲は、市販の製品 5,000 から 6,000 種のうち 1,000 程度であり、対応できている範囲は、ごく一部の有名製品に限られてしまうこと、また、バージョンアップなどで製品仕様が変更になれば、ソフトウェア辞書の修正も必要になるので、その効果は限定的となってしまう。

よって、ソフトウェア辞書の有効性については、管理対象のソフトウェアが、辞書で十分対応されているかなど、SAM 管理者側で効果を正確に見積もる必要がある。

今後は ISO/IEC 19770-2 で策定中のソフトウェアタグ仕様から、各製品提供ベンダー、若しくは販売ベンダーにより適正な製品名が、統一化されたタグ情報として、記録されたものが、ソフトウェア辞書として利用されることも想定されるが、現時点においては、ソフトウェアとライセンスの自動紐付けの実現は将来課題のままである。

(4) メータリング

SAM ツールの機能の一つにソフトウェアメータリングと呼ばれ、ユーザが使用しているソフトウェアの使用状況(利用回数、使用時間など)を監視する機能がある。

前述したインベントリ収集では、使用/不使用を問わず、PC上に存在したソフトウェアの情報を採取するが、その場合、実際に使用されていないソフトウェアも計上してしまうことになる。

メータリング機能が利用できれば、利用していないソフトウェアを検出可能となり、導入ソフトウェアの要/不要を確認できる。これにより、無駄なソフトウェアを削除し、転用可能なライセンス数を増やすことができる。

(5) 収集結果の分析・警告メッセージ送信

SAM ツールの機能の一つに、収集したインベントリ情報の内容を分析し、ユーザが指定した設定値を超えた場合に、対象資産の管理者及び使用者に対して、警告メッセージを送信できる機能をもつ製品がある。

例えば、購入したライセンス数を超えて使用されている場合や、業務外使用の疑いのあるソフトウェアの検出、未許可 PC のネットワーク接続の検出といった不正使用防止に用いることができる。

インベントリ収集の対象数が増加した場合、人的管理だけで、こうした情報を見つけ出すことは難しく、こうした支援機能を持つ製品であれば、効率化の一つのポイントとなる。

(6) 変化への対応

本章の冒頭で説明したように、IT 資産 100 台以上の環境では、人手のみでは管理に膨大なコストが必要とされるため、SAM ツールの導入を検討する価値がある。また、導入後に様々な変化が予想され、ツールを選択する際には、こうした変化に対して柔軟に対応できる製品であることも検討のひとつとなる。

① 管理対象の増加

SAM の対象資産がどれくらい増加する可能性があるかという点について考慮する必要がある。

管理対象範囲を広げていく場合には、例えば、当初数百の IT 資産ではじめたものが、数万まで増加することが考えられる。こういう事態に対応できるかどうかをあらかじめ確認しておく必要がある。

ソフトウェアとして単に対応可能というだけでなく、シームレスにシステム拡張が可能か(サーバの増強、メモリ増設といったハードウェアを更新、追加するだけで済むのか、それとも、管理対象の増加により、管理システム全体(ソフトウェア、ハードウェア、管理方式含む)を見直さなければいけないのか)といったものをツールの導入前に検討しておく必要がある。

② 新規資産への対応

新たな IT 資産(新 OS、新ハードウェアなど)に対する対応体制の確認が挙げら

れる。新製品により、インベントリ収集対象が変わっても、それに対する対処(修正パッチの提供や任意項目での補完対応など)が速やかに行えるベンダーであり、製品であることが望ましい。単に現在の製品が持つ機能だけでなく、今後の保守、パッチ適用体制も含めてツール提供ベンダーの選定をする必要がある。

8.4.2. 構成管理機能の比較

(1) 構成管理項目の画面上の視認性

インベントリ情報により、採取された各種項目が、管理コンソール上でユーザの視認性よく配置され、ユーザが管理しやすい製品が選択される必要がある。視認性については、単に機能の有無だけでは判断しにくいところがあり、実際に使って判断するほうがよいと思われる。この場合、お試し利用が可能な製品を選択すれば、ユーザ主観に応じた製品を選択できるものと思われる。

(2) カスタマイズ機能

ユーザが管理したい資産情報は、それぞれのユーザにより千差万別であり、それぞれが管理しやすいよう項目の追加、削除が行える製品を選択するのが望ましい。この場合、ユーザがあとから任意の項目を追加し、それらについても製品ベンダー提供済みの既存項目と同じレベルで管理できる製品であれば更にその選択はよいものと思われる。

(3) 多様な管理方法の提供(利用シーンにあわせて)

ユーザの利用シーンとして、直接情報システム部門のみで管理する場合、複数拠点からリモートで管理ツールを操作する場合、また、夜間のバッチ処理などで、自動化をしたい場合などの利用シーンがあると考えられる。

この場合、SAM ツールの管理コンソール及びコマンドなどでこれらの利用シーンに応えられる製品を選択するのが望ましい。

(4) 検索機能

採取されたインベントリ情報を活用し、企業システムで管理されている情報を有効活用できる機能として、未適用セキュリティパッチがあるマシンの検索など、検索機能が提供されている製品を選択することが望ましいと考えられる。

検索項目としては、製品ベンダーが提供するテンプレート以外に、ユーザがそれぞれの目的に応じた任意の検索項目をカスタマイズ可能な製品であれば、更に望ましい。

(5) 異動(移動)管理

構成管理は、異動に伴う部門間での資産移動にも、対応できる必要がある。半期ごとの組織改変などで、部門が変更になった際も、組織の変更管理や、部門異動に対応したライセンス割当の変更などができる機能を持つ製品が望ましい。

ソフトウェアのライセンスとしては、次の種類があり、会社単位で購入される全社包括ライセンス以外は、部門異動により、資産移動管理を行う必要があるものもある。

表 8-4 ライセンス種別表

使用許諾条件	必要ライセンス数の集計方法
クライアントライセンス	PC などのデバイス 1 台に対して 1 ライセンスが消費される
サーバーライセンス	サーバ 1 台に対して 1 ライセンスが消費される クライアントライセンスと考え方は同じ
ユーザーライセンス	ソフトウェアを利用する使用者 1 人に対して 1 本ライセンスを消費
CPU ライセンス	ソフトウェアが導入されたハードウェアに搭載された CPU の数だけライセンスを消費
クライアントアクセス ライセンス (デバイス)	サーバにアクセスするデバイスの数だけライセンスを消費
クライアントアクセス ライセンス (ユーザー)	サーバにアクセスする利用者の数だけライセンスを消費
全社包括ライセンス	契約対象の組織全体で保有する PC 台数や従業員数の把握が必要 ※ベンダーとの契約条件により、把握すべき要件が変わる

8.4.3. 台帳管理機能の比較

SAM の運用において、IT 資産を台帳管理する必要がある。主な台帳としては、ハードウェア管理台帳、導入ソフトウェア台帳、ライセンス管理台帳、ライセンス関連部材台帳といったものがあげられる。

それぞれの台帳項目については、「6.SAM の構築」に記載があるので、詳細は、そちらを参照されたい。

管理台帳の作成は、

- ① 対象となる資産及びライセンスの調査
- ② 台帳の作成

というステップで行われる。

SAM ツールの中には、これらの台帳作成を支援するものとして、自動収集した IT 資産のインベントリデータまた、システム管理者により手動入力されたライセンス情報などを台帳形式にまとめ、画面表示や帳票印刷を行える機能を持つ製品がある。また、直接印刷機能は持たなくても、適切な書式でデータを出力できる製品というものもある。

SAM ツールで管理される IT 資産のインベントリデータは、データベースなどに登録されており、それぞれのテーブル間で連携するデータ、例えば PC 管理番号といった共通項目が、IT 資産の変更に伴い自動的に各テーブルへ反映されるといった効用がある。

なお、SAM ツールが提供するインベントリデータは、あくまで収集時点のツールにより取得更新した最新情報のみを示すものであり、それだけで完全なインベントリデータを作成できたわけではないことを念頭に置く必要がある。人的管理をした紙の台帳と付き合わせを行い、収集した

インベントリデータの不足、誤りを補った上で、正しいデータとする必要がある。

8.4.3.1. 棚卸支援機能の比較

棚卸支援機能としては、管理者によるものと、ユーザ個人単位での現況確認があり、そのどちらにも対応していることが望ましいと考えられる。

管理者による入力においては、一括登録など、大量データを扱う際の考慮がされていることが望ましい。

また、棚卸作業においては、現品確認を誰がいつどこで行ったか、また、その結果を誰が承認確認したかの情報が必要であり、IT 内部統制の観点より、証跡管理が行える製品であることが望ましい。

8.4.4. その他機能の比較

ソフトウェア資産管理機能の範囲を超えるが、IT 資産管理の観点では、次の機能も重要であり、それらについて説明する。

(1) ソフトウェアの配布機能

多くの統合運用管理製品、IT 資産管理ツール、セキュリティ製品では、現時点のソフトウェアのインベントリ管理をする以外に、アップデートプログラムの配布、セキュリティパッチの展開といった観点で、ソフトウェアの配布の機能を持つ製品が多く、製品選択において、この機能の検討も必要である。

製品としては、どういった種類のソフトウェアが配布できるのか？といった配布対象が多いことが望ましい。

また、配布した後に、資産管理、構成管理と連携して、配布したソフトウェアのバージョン管理ができることが望ましい。

スケジュール管理と組み合わせて、夜間のバッチ配布や配布に伴うネットワーク負荷を軽減する機能、更に配布失敗時のリトライ、前回のしかかり中から再送できる機能といった様々な機能を持つ製品であることが望ましい。

(2) 拡張機能の比較

- ・ リモートコントロール
- ・ ログ収集

不正なライセンス状態、ソフトウェア構成にある状態を正す機能として、リモートコントロール機能が実装されているツールもある。

また、資産管理を行う上で、証跡情報をきちんと管理することが必要であり、これら証跡情報をログ収集という形で管理することも考えられる。

8.5. SAM ツールの評価例

SAM ツールを評価するには、管理対象の資産がどのように構成されているか？また、検討して

いる SAM ツールがどのような機能を持っているか、費用がいくらかかるかを、表にまとめ、相対評価を行うとよいと思われる。

例えば、次の三つの製品について検討を行ったとする。それぞれは、次の点で特長がある。

- 製品 A は、総合的な IT 資産管理製品で、Windows、UNIX などマルチプラットフォーム対応し、クライアント、サーバを問わずに資産管理が行える製品である。ライセンスはサーバーライセンス方式で、CPU 数でカウントされます。大規模環境の管理をする場合、1 台あたりの管理単価が安くなる。
- 製品 B は、UNIX には対応していないが、Windows については、Windows95 からの古いものも対応している製品である。導入したクライアント PC 単位でライセンスがカウントされる。管理対象の IT 資産数が少ない場合、割安になる。
- 製品 C は、Macintosh に対応し、DTP などへの対応をしている点に特長がある製品である。また、ライセンスはユーザライセンスになっており、ひとりのユーザが複数のマシンを利用する環境では、割安になる。

単に特長を見ただけでは、検討が難しいが、表 8-5 にまとめると、それぞれの特長が明確になり、合理的に判断を行うことができるようになると思われる。

下記にツール比較のための表の一例を記載する。

表 8-5 SAM ツール比較表

		製品 A	製品 B	製品 C
サポート OS	クライアントPC	Windows 7 Windows Vista Windows XP Windows2000	Windows 7 Windows Vista Windows XP Windows2000 Windows98 Windows95	Windows 7 Windows Vista Windows XP Windows2000 Macintosh X
	サーバ	Windows2008 Windows2003 Windows2000 RHEL HP-UX Solaris AIX	Windows2008 Windows2003 Windows2000 WindowsNT4.0	Windows2008 Windows2003 Windows2000
	収集サーバ	Windows2008 Windows2003 Windows2000 RHEL HP-UX Solaris AIX	Windows2008 Windows2003 Windows2000	Windows2008 Windows2003 Windows2000
台帳	導入ソフトウェア台帳	○	○	○
	ライセンス管理台帳	○	○	○
	ライセンス関連部材台帳	○	—	○
	ハードウェア管理台帳	○	○	○
登録設定	各項目、台帳の一括登録の可否	○	○	○
	スタンドアロンの登録	—	○	○
	ツールを利用できない機器情報の登録可否	○	—	○
	購入情報の登録可否	—	○	○
	指定レジストリの収集	—	○	—
	ユーザ入力項目の設定	○	○	○
更新	各登録内容の一括更新の可否	○	○	—
	部署更新方法	—	○	—

エージェント	エージェントレス	○	—	—
	エージェントあり	○	○	○
	ネットワーク負荷	大	中	小
辞書	ソフトウェア辞書の有無	—	○	○
	対象機器メーカー	—	メーカー- A、B、D	メーカーA、B、D
	対象ソフトウェア種類	—	OS,Office,開発 支援	OS,DTP,Office
	辞書の更新方法	—	Web配信	メディア配布
	ライセンス管理台帳と導入ソフトウェア台帳との紐付け方法	×	○	△
その他	ファイル配信	○	○	×
	禁止ソフトの登録	-	○	○
	メータリング	○	○	—
	監査ログの収集	○	—	—
購入	ライセンス体系	サーバーライセンス(CPU)	クライアントライセンス	ユーザーライセンス
	ライセンス費用	5,000,000	2,000,000	3,500,000
	初期費用	15,000	200,000	150,000
	保守料金	100,000	300,000	50,000
	24H サポート費用	150,000	—	—

比較表でまとめた○×の数を集計し、単純に○が多い製品を選択するという方法もあるが、より適切な製品を選択するには、項目表の中で優先度が高い項目について考察することが望ましい。

例えば、これから IT 資産の管理を行う環境が Windows、UNIX などが混合した環境であり、管理対象の台数が多い場合は、サポート OS の一覧を注視し、対応した製品が多い製品を選択する方が望ましいと考えられる。この例の場合、製品 A を選ぶのが望ましいと考えられる。

また、管理対象の製品が Windows のみで、Windows95 などの古い OS についてもあわせて管理したいという場合は、同様にサポート OS の一覧より、Windows 製品を広くカバーしている製品 B を選ぶのが望ましいと考えられる。

IT 資産の管理を行う環境は千差万別であり、また、費用面の問題など、様々な評価観点がある。導入を検討している環境で、どういった項目を重視しているかをあらかじめリストアップし、適切な評価表を作成することが、SAM ツールの導入を適切に行う上で重要であると考えられる。

付録

A-1 ソフトウェア資産管理方針

ソフトウェア資産管理方針【ソフトウェア資産管理方針 サンプル】

ソフトウェア資産管理方針（日本語版）¹

1. 宣言（4.2.2 a）,4.2.2b）²

本管理方針は、取締役会により認証されたソフトウェア及び関連資産の管理方針を定める。

2. 適用範囲（4.2.2c）

本方針の適用される組織の範囲は、以下のとおりである。

- ・ _____
- ・ _____
- ・ _____
- ・ _____
- ・ _____

本適用範囲は、毎年4月の取締役会において見直す。

3. リスク認識（4.2.2d）

ソフトウェア及び関連資産を管理する従業員は以下のリスクを留意して行動する。

- ・ 個人のプライバシーの順守などの規制を順守しないことのリスク。
- ・ 使用許諾条件を順守しないことのリスク。
- ・ 不適切な SAM に起因する IT 基盤の問題による運用中断のリスク。
- ・ 不適切な SAM によるライセンスの取得及びその他の IT サポート費に対する過剰な出費のリスク。
- ・ ソフトウェア及び関連資産に対する分散管理手法対集中管理手法に付随するリスク。
- ・ 各国の法令・規制の順守についてのリスク。

4. ソフトウェア資産管理者の役割と責任（4.2.3）

(1) SAM 管理責任者の役割と責任

SAM 管理責任者の役割と責任を以下に規定する。

- ・ SAM の管理目的の提案。
- ・ SAM 計画策定の監督。
- ・ 承認された SAM 計画を実施するための資源の確保。

¹ 通常これらの方針や規程、手順等は、企業内の LAN で WEB に公開されている。

² 表題の（）内の番号は、分かり易くするために ISO/IEC 19770-1 で規定されている章番号を示している。

- ・ SAM 計画に対する結果の伝達。
- ・ すべての部門 SAM 管理責任者がその責任を適正に果たすこと。
- ・ 組織のすべての部門が，SAM 管理責任者又は部門 SAM 管理責任者によって，矛盾を起こすような重複がなく管理されること。

(2) 部門 SAM 管理責任者の役割と責任

部門 SAM 管理責任者の役割と責任を以下に規定する。

- ・ SAM 計画を実施するための資源の確保。
- ・ SAM 計画に対する結果の伝達。
- ・ 必要な方針，プロセス及び手順の採用及び導入。
- ・ ソフトウェア及び関連資産の正確な記録の維持。
- ・ ソフトウェア資産の調達，展開及び管理に，管理面及び技術面からの承認が必要になることを確実にすること。
- ・ 契約，供給者との関係，及び内部顧客との関係の管理。
- ・ 必要改善点の特定と実施。

これらの情報は，関連各組織に周知徹底する。

A-2 SAMに関連する各種団体・規格・基準・書籍など

a) 団体

■ 日本

- ・ 特定非営利活動法人ソフトウェア資産管理コンソーシアム
- ・ 社団法人コンピュータソフトウェア著作権協会

■ 海外

- ・ itSMF (IT Service Management Forum)
- ・ IAITAM(International Association of Information Technology Asset Managers, Inc.)
- ・ IBSMA(International Business Software Managers Association)
- ・ BSA(Business Software Alliance)

b) 国際規格

- ISO/IEC 19770-1:2006 Information technology -- Software asset management -- Part 1: Processes

- ISO/IEC 19770-2:2009 Information technology -- Software asset management -- Part 2: Software identification tag

管理規程サンプル

http://www.iso.org/iso/catalogue_detail?csnumber=33908

c) 書籍など

- 実務者のためのソフトウェア資産管理 / 中央コーパス・アンド・ライブランドコンサルティング. -- コンピュータ・エージ社, 1993.4
- 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. -- 日本規格協会, 2009.6
- ソフトウェアライセンス管理 / ソフトウェアライセンス研究会. -- クオリティ, 1995.5
- ソフトウェアライセンスの基礎知識 / 可知豊. -- ソフトバンククリエイティブ, 2008.9
- IAITAM Best Practice Library – IBPL (IAITAM)
- アプリケーション管理 (itSMF)

d) 基準 (ソフトウェア資産管理コンソーシアム : SAMCon (Software Asset Management Consortium))

- ソフトウェア資産管理基準 (参考資料 I に引用)
- ソフトウェア資産管理評価規準

<http://www.samconsortium.org/>

e) ガイド

- ソフトウェア管理ガイドライン (経済産業省)

<http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanri-guide.htm>

■ 企業向けソフトウェア管理支援ポータル (BSA : Business Software Alliance)

<http://www.bsa.or.jp/index.html>

※掲載 URL は、2010 年 1 月 1 日現在のもの。

ソフトウェア資産管理評価検討委員会

(敬称略)

氏名	所属
篠田 仁太郎 (委員長)	(株)クロスビート
岩下 健久	日本電気(株)
片岡 伸吉	オートデスク(株)
薩摩 貴人	あずさ監査法人
島田 篤	ダイヤモンドレンタルシステム(株)
高橋 快昇	富士通(株)
田村 仁一	有限責任監査法人トーマツ
手島 伸行	マイクロソフト(株)
中村 大造	ウチダスペクトラム(株)
中村 究	エヌシーアイ総合システム(株)
塩田 貞夫 (オブザーバー)	日本ヒューレット・パッカード(株)