

ソフトウェア資産管理対策手順書 Ver.1.0

ビジネスソフトウェアアライアンス 2009.08



—使用許諾条件—

- 1 下記著作権者からの書面による事前の承諾なく、自らの組織にソフトウェア資産管理を導入する目的以外で、この出版物のいかなる部分についても、いかなる形式でも、また写真複製等を含む一切の電子的又は機械的な方法のいずれによっても、複製、利用、転載、アップロードすることを禁止します。
- 2 第三者に対し、有償、無償を問わず、この出版物のいかなる部分についても譲渡又は貸与すること、及び第三者を対象としたセミナー等で紹介することを一切禁止します。
- 3 ビジネスソフトウェアアライアンス (BSA) は、この出版物を利用する組織において、SAM の効果を保証するものではありません。

著作権者 ビジネス ソフトウェア アライアンス (BSA)

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

内容

はじめに	5
(1) 目的	5
(2) 対象範囲	5
(3) 対象資産の範囲	5
1. 用語	5
2. ソフトウェアリストへのソフトウェアの追加及び公表	6
(1) ソフトウェアリストへソフトウェアを追加する際の手続き	6
(2) ソフトウェアリストの作成と更新	7
(3) ソフトウェアリストの版管理	7
(4) 保管	8
3. 管理台帳の管理	8
(1) 管理台帳の項目	8
(2) 管理台帳の利用	8
(3) 管理台帳並びに管理台帳項目の改廃	9
(4) 保管	9
4. 対象資産調達時の手続き	10
(1) ハードウェア	10
(2) 調達先	10
(3) 標準ソフトウェア及び CAL	11
(4) 個別利用ソフトウェア	11
(5) ドライバー・更新プログラム等	12
(6) リース・レンタルによる調達	12

(7) 管理番号の付与.....	13
(8) ライセンス媒体の複製.....	14
(9) 記録.....	15
(10)保管.....	17
5. ソフトウェアの導入・更新手続き.....	18
(1) 標準ソフトウェア.....	18
(2) 個別利用ソフトウェア.....	19
(3) ドライバー・更新プログラム等及びその他.....	19
(4) 記録.....	20
(5) 保管.....	22
6. ソフトウェアの転用手続き.....	22
(1) 標準ソフトウェア.....	22
(2) 個別利用ソフトウェア.....	23
(3) 記録.....	23
7. ソフトウェア資産の削除手続き.....	25
(1) 標準ソフトウェア.....	25
(2) 個別利用ソフトウェア.....	25
(3) ドライバー・更新プログラム等及びその他.....	25
(4) 禁止ソフトウェア.....	26
(5) 記録.....	26
(6)保管.....	267

8. ソフトウェア資産の廃棄手続き	28
(1)ハードウェアの廃棄時	28
(2)ライセンス媒体及び複製物の廃棄	28
(3)記録	28
(4)保管	29
9. ライセンス情報の入手	29
10. 研修	29
(1)研修の実施	28
(2)研修計画の策定	28
(3)研修の種類	28
(4)研修の内容	30
(5)研修結果のレビュー	30
(6)保管	31
11. 検証	31
(1)棚卸	31
(2)監査	33
12. 本文書の見直し	35
13. 違反への対応	35
14. 参照資料	35

はじめに

(1) 目的

ソフトウェア資産管理対策手順書（以下「本文書」という）は、〇〇市（以下「本市」という）において、【ソフトウェア資産管理対策基準】に記載されている目的を満たすために必要となる具体的な手順を定めるものである。

(2) 対象範囲

【ソフトウェア資産管理対策基準】に定める通りとする。

(3) 対象資産の範囲

【ソフトウェア資産管理対策基準】に定める通りとする。

1. 用語

本文書における用語の定義は、以下に記載するもの以外は、【ソフトウェア資産管理対策基準】に記載する用語に拠る。

(1) ソフトウェアリスト

「ソフトウェアリスト」とは、統括情報セキュリティ責任者が対象範囲内に公表する、対象範囲内で利用可能な標準ソフトウェア、個別利用ソフトウェアの一覧をいう。

(2) ライセンスプログラム

「ライセンスプログラム」とは、ソフトウェアメーカーが制定しているソフトウェアの調達の種類をいう。例えば、全社包括契約や、購入ポイントによる調達契約など。

(3) ユーザーライセンス

「ユーザーライセンス」とは、導入されるハードウェアの数ではなく、そのソフトウェアの利用者数に対するライセンスをいう。

(4) CPUライセンス

「CPUライセンス」とは、ソフトウェアを導入するハードウェアのCPU数等に対するライセンスをいう。

(5) ライセンス余剰数

「ライセンス余剰数」とは、保有しているが、まだ導入されていないライセンス数をいう。

(6) 適切なライセンスプログラム

「適切なライセンスプログラム」とは、ライセンスの調達を決定する際に、管理コスト・購入コスト・保守料金などを検討した結果選択されたライセンスプログラムをいう。

2. ソフトウェアリストへのソフトウェアの追加及び公表

(1) ソフトウェアリストへソフトウェアを追加する際の手続き

① 標準ソフトウェア

(ア) 標準ソフトウェアの追加

新たな標準ソフトウェアを追加する際は、統括情報セキュリティ責任者の許可を得なければならない。

(イ) 使用許諾条件の確認

ソフトウェア資産統括管理者は、当該ソフトウェアの使用許諾条件を確認の上、「標準ソフトウェア追加申請書」に必要事項記載の上、「使用許諾条件確認書」を添付し、統括情報セキュリティ責任者の承認を得なければならない。

② 個別利用ソフトウェア

(ア) 個別利用ソフトウェアの追加

新たに個別利用ソフトウェアを追加する際は、情報セキュリティ責任者の承認を得た上で、統括情報セキュリティ責任者に報告しなければならない。

(イ) 使用許諾条件の確認

ソフトウェア資産管理担当者は、当該ソフトウェアの使用許諾条件を確認の上、「個別利用ソフトウェア追加申請書」に必要事項記載の上、「使用許諾条件確認書」を添付し、情報セキュリティ責任者に申請し、承認を得なければならない。承認後は速やかに写しをソフトウェア資産統括管理担当者に提出しなければならない。

③ 使用許諾条件確認書記載内容の確認

(ア) 使用許諾条件確認書の確認日の制限

「標準ソフトウェア追加申請書」もしくは「個別利用ソフトウェア追加申請書」(以下「追加申請書」という)に添付する際は、使用許諾条件の確認日が、追加申請書記載の申請日から数えて3カ月以内でなければならない。

(イ) 使用許諾条件の再確認命令

統括情報セキュリティ責任者もしくは情報セキュリティ責任者は、追加申請書に添付されていた使用許諾条件の確認日が、追加申請書の申請日から数えて3カ月以内だった場合でも、必要に応じて、申請者もしくは報告者に対し、再確認を命じることができる。

(2) ソフトウェアリストの作成と更新

① ソフトウェアリストの更新

ソフトウェア資産統括管理担当者は、毎月1回、追加、削除された標準ソフトウェア及び個別利用ソフトウェアを「ソフトウェアリスト」に反映し、統括情報セキュリティ責任者に報告しなければならない。ただし、追加されたソフトウェアをソフトウェアリストに記載するのは、本文書“4. 対象資産調達時の手続き”によって、当該ソフトウェアの納品が確認できた時点とする。

② ソフトウェアリストの公開

統括情報セキュリティ責任者は、ソフトウェア資産統括セキュリティ担当者から報告された「ソフトウェアリスト」を確認し、速やかに社内掲示板にて、職員等に周知しなければならない。

(3) ソフトウェアリストの版管理

統括情報セキュリティ責任者は、ソフトウェアリストが常に最新のものが公表されるよう、適切にソフトウェアリストの版管理をしなければならない。

(4) 保管

① 「使用許諾条件報告書」及び、追加申請書

(ア) 標準ソフトウェアの場合

統括情報セキュリティ責任者の責任において管理する。紛失、盗難、改ざん等を防止できるよう、当該ソフトウェアがソフトウェアリストから抹消されるまで適切に保管しなければならない。

(イ) 個別利用ソフトウェアの場合

情報セキュリティ責任者の責任において管理する。紛失、盗難、改ざん等を防止できるよう、当該ソフトウェアがソフトウェアリストから抹消されるまで適切に保管しなければならない。

② ソフトウェアリスト

(ア) 最新版原本の保管

統括情報セキュリティ責任者は、ソフトウェアリストに不正な変更、改ざんされないよう、原本を適切に保管しなければならない。

(イ) 旧版ソフトウェアリストの保管

統括情報セキュリティ責任者は、更新前のソフトウェアリストを適切な期間保管しなければならない。

3. 管理台帳の管理

(1) 管理台帳の項目

管理台帳の項目は、別紙「ハードウェア管理台帳」、「利用ソフトウェア管理台帳」、「ライセンス管理台帳」、「ソフトウェア媒体管理台帳」記載の通りとする。

(2) 管理台帳の利用

① 管理台帳の可用性の確保

統括情報セキュリティ責任者は、管理担当者等がそれぞれの管理責任範囲の情報を常に参照し、更新できるようにしなければならない。

② 管理台帳の更新方法

管理台帳の情報は、情報セキュリティ管理者が自らの責任範囲の情報を本文書“4. 対象資産調達時の手続き”、“5. ソフトウェアの導入・更新手続き”、“6. ソフトウェア資産の削除手続き”、“7. ソフトウェア資産の廃棄手続き”に従って更新する。

③ 管理情報の把握

(ア) 対象範囲の全ての情報の把握

統括情報セキュリティ責任者は、必要に応じて、管理台帳から管理情報の全て、又は任意の一部を随時入手することができるようにしなければならない。

(イ) 管理担当者等毎の情報の把握

統括情報セキュリティ責任者は、必要に応じて、管理台帳から各管理担当者等の責任範囲の管理情報を随時入手することができるようにしなければならない。

(ウ) 管理情報の可用性

統括情報セキュリティ責任者は、著作権者からの依頼等、必要に応じて、管理台帳の情報を出力できるようにしなければならない。

(3) 管理台帳並びに管理台帳項目の改廃

管理台帳の改廃、管理項目の修正は、最高情報統括責任者の承認を得なければならない。統括情報セキュリティ責任者は、年1回、定期的に管理台帳の内容を見直し、必要があると判断した場合には、修正案を策定し、最高情報統括責任者に提出しなければならない。なお、管理項目を変更する際の基準は、対象範囲で使用しているソフトウェアの使用許諾条件を順守したものであることを最低条件とする。

(4) 保管

① 管理台帳の保管

統括情報セキュリティ責任者は、管理台帳の完全性、可用性、機密性を確保できるよう、適切に管理しなければならない。また、少なくとも毎月1回、バックアップのために定期的に管理台帳を複製し、それが紛失、盗難、改ざん等の対象とならない環境を構築し、適切に保管しなければならない。

② 管理台帳の複製

(ア) 複製の申請

保管している管理台帳を複製する際は、「管理台帳複製申請書」に必要事項記載の上、統括情報セキュリティ責任者の承認を得なければならない。

(イ) 複製物の明確化

統括情報セキュリティ責任者は、バックアップの目的以外で管理台帳を複製した際は、複製物であることを明確にするために、赤字で複製物である旨の記載をした上で、申請者に渡るようにしなければならない。

4. 対象資産調達時の手続き

(1) ハードウェア

① 調達計画情報の入手

統括情報セキュリティ責任者は、ソフトウェア資産統括管理担当者がソフトウェア資産管理を効果・効率的に行えるよう、【パソコン等取扱規程】に従って調達されるハードウェアの情報が、その計画段階から入手できるようにしなければならない。

② 調達情報の入手

統括情報セキュリティ責任者はハードウェアの対象範囲内への納品情報を速やかに入手できるようにしなければならない。

(2) 調達先

① 仕様書の策定

ソフトウェア資産を調達する際には、調達先から見積を入手するための仕様書を策定し、調達先に提出しなければならない。仕様書には、当該ソフトウェア資産の調達に関し、調達先に求めるサービスレベル（発注から納品までの必要日数、不具合発生時の対応内容等）を含めなければならない。

(ア) 標準ソフトウェア

ソフトウェア資産統括管理担当者が仕様書を策定し、統括情報セキュリティ責任者が確認する。

(イ) 個別利用ソフトウェア

ソフトウェア資産管理担当者が仕様書を策定し、情報セキュリティ責任者が確認する。

② 調達先の選定

調達先の選定は、【物品調達基準】に拠る。

③ 調達先の管理

(ア) サービスレベル管理

仕様書の策定者は、仕様書に記載したサービスレベルの順守状況を確認し、仕様書の確認者に報告しなければならない。また、サービスレベルが順守されていない場合には、調達先とともに改善のための是正措置を策定し、実施しなければならない。

(3) 標準ソフトウェア及びCAL

① 調達時の手続き

(ア) 申請方法

標準ソフトウェアの調達は、ソフトウェア資産統括管理者が「標準ソフトウェア調達申請書兼報告書」に必要事項を記入し、統括情報セキュリティ責任者の承認を得なければならない。

(イ) 事前確認

標準ソフトウェアの調達を申請する際は、コストの抑制も考慮し、対象範囲における全てのライセンスの保有情報と利用状況の確認及び適切なライセンスプログラムの調達をしなければならない。

また、当該ソフトウェアの使用許諾条件についても、変更がないかどうかを確認し、変更があった場合には、【ソフトウェア資産管理対策基準】“15. 本文書の見直し(3)優先事項”の記載に従い、対応しなければならない。

(ウ) 発注方法

発注が必要な場合は、統括情報セキュリティ責任者から承認を得次第、【物品調達基準】に従って発注する。

② 調達時の手続き

(ア) 納品物の確認

申請者は、「使用許諾条件確認書」に記載されているライセンス媒体が全て納品されていることを確認しなければならない。納品物に問題がない場合には、速やかに、承認された「標準ソフトウェア調達申請書兼報告書」に必要事項を追記し、統括情報セキュリティ責任者に提出しなければならない。不足がある場合には、全てのライセンス媒体が揃うまで、調達先に納品物を一旦返却しなければならない。

(4) 個別利用ソフトウェア

① 調達時の手続き

(ア) 申請方法

個別ソフトウェアの調達は、ソフトウェア資産管理者が「個別利用ソフトウェア調達申請書兼報告書」に必要事項を記入し、情報セキュリティ責任者の承認を得た上で、写しを速やかに統括情報セキュリティ責任者に提出しなければならない。

(イ) 事前確認

個別利用ソフトウェアの調達を申請する際は、適切なライセンスプログラムを選択しなければならない。

また、当該ソフトウェアの使用許諾条件についても、変更がないかどうかを確認し、変更があった場合には、統括情報セキュリティ責任者に速やかに報告し、【ソフトウェア資産管理対策基準】“15. 本文書の見直し(3)優先事項”の記載に従い、対応しなければならない。

(ウ) 発注方法

発注が必要な場合は、ソフトウェア資産管理担当者が、情報セキュリティ責任者から承認を得次第、【物品調達基準】に従って発注する。

② 調達時の手続き

(ア) 納品物の確認

申請者は、「使用許諾条件確認書」に記載されているライセンス媒体が全て納品されていることを確認しなければならない。納品物に問題がない場合には、速やかに、承認された「個別利用ソフトウェア調達申請書兼報告書」に必要な事項を追記し、ソフトウェア資産統括管理担当者に提出しなければならない。不足がある場合には、全てのライセンス媒体が揃うまで、調達先に納品物を一旦返却しなければならない。

(5) ドライバー・更新プログラム等

ドライバー・更新プログラム等の調達については、申請者がソフトウェア資産統括管理担当者の場合には、本文書“4. 対象資産調達時の手続き(3)標準ソフトウェア及びCAL”に、ソフトウェア資産管理担当者の場合には、本文書“4. 対象資産調達時の手続き(4)個別利用ソフトウェア”に従う。

(6) リース・レンタルによる調達

ソフトウェア資産のリース・レンタルによる調達は、当然に、使用許諾条件上、許されていることを前提とするが、本市では原則行わないものとする。

(7) 管理番号の付与

① 管理番号の種類

管理番号の種類は、【ソフトウェア資産管理対策基準】“6. 対象資産の管理(2)管理台帳の作成”に拠る。

② 管理番号体系

対象資産毎の管理番号体系は、別紙「管理番号体系一覧」記載の通りとする。

③ 管理番号の付与方法

(ア) 管理番号の管理

発行した管理番号の履歴管理及び発行する管理番号の振り出しは、統括情報セキュリティ責任者が実施する。統括情報セキュリティ責任者は、管理番号を適切に管理するため、「管理番号発行管理簿」を策定しなければならない。

(イ) ハードウェア

統括情報セキュリティ責任者は、納品されたハードウェアに対し、ソフトウェア資産管理のための管理番号（以下「ハードウェア管理番号」という）を付与しなければならない。

ソフトウェア資産統括管理担当者は、速やかに、「管理番号通知書兼報告書」にて、付与された管理番号を情報セキュリティ管理者に伝達しなければならない。

情報セキュリティ管理者は、指示された通りにハードウェアに貼付した上で、「管理番号通知書兼報告書」に必要事項を記入の上、ソフトウェア資産統括管理担当者宛てに提出しなければならない。

(ウ) 標準ソフトウェア及びCAL

統括情報セキュリティ責任者は、納品されたライセンス媒体に対し、ソフトウェア資産管理のための管理番号（以下「ライセンス媒体管理番号」という）を付与しなければならない。

ライセンス媒体管理番号は、受領したライセンス媒体毎に同一の番号を付与する。ただし、本文書4.“対象資産調達時の手続き(8)ライセンス媒体の複製”については、別のライセンス媒体管理番号を付与する。

ライセンス媒体へのライセンス媒体管理番号の貼付の際、DVDやCDなど、直接貼付することで劣化の可能性があるものまたは貼付することで記載内容が確認しにくくなるものについては、それを格納するケース等に貼付する。

(エ) 個別利用ソフトウェア

ソフトウェア資産統括管理担当者は、納品されたライセンス媒体に対し、統括情報セキュリティ責任者の指示に従い、ライセンス媒体管理番号を付与しなければならない。ソフトウェア資産統括管理担当者は、速やかに、「管理番号通知書兼報告書」にて、付与されたライセンス媒体管理番号を情報セキュリティ管理者に伝達しなければならない。

情報セキュリティ管理者は、指示された通りにライセンス媒体に貼付した上で、「管理番号通知書兼報告書」に必要事項を記入の上、ソフトウェア資産統括管理担当者宛てに提出しなければならない。

ライセンス媒体へのライセンス媒体管理番号の貼付の際、DVDやCDなど、直接貼付することで劣化の可能性があるものまたは貼付することで記載内容が確認しにくくなるものについては、それを格納するケース等に貼付する。

(オ) ドライバー・更新プログラム等及びその他

上記ソフトウェア分類に対するライセンス媒体管理番号は、原則付与しない。

(8) ライセンス媒体の複製

使用許諾条件上許される場合には、ライセンス媒体を複製することができる。ライセンス媒体を複製する場合には、以下の手続きに従わなければならない。

① 複製の申請及び報告

(ア) 標準ソフトウェア

ソフトウェア資産統括管理担当者は、ライセンス媒体を複製するために、「ライセンス媒体複製申請書兼報告書」に必要事項を記入し、統括情報セキュリティ責任者の承認を得なければならない。

統括情報セキュリティ責任者は、ライセンス媒体の複製物のために、ライセンス媒体管理番号を付与しなければならない。その際、複製元となるライセンス媒体のライセンス媒体管理番号を同時に伝達しなければならない。

ライセンス媒体へのライセンス媒体管理番号の貼付の際、DVDやCDなど、直接貼付することで劣化の可能性があるものまたは貼付することで記載内容が確認しにくくなるものについては、それを格納するケース等に貼付する。

(イ) 個別利用ソフトウェア

ソフトウェア資産管理担当者は、ライセンス媒体を複製するために、「ライセンス媒体複製申請書兼報告書」に必要事項を記入し、情報セキュリティ責任者の承認を得た上で、ソフトウェア資産統括管理担当者に提出しなければならない。

ソフトウェア資産統括管理担当者は、統括情報セキュリティ責任者の指示に従い、ライセンス媒体の複製物のために、ライセンス媒体管理番号を付与しなければならない。

ソフトウェア資産統括管理担当者は、速やかに、「管理番号通知書兼報告書」にて、付与されたライセンス媒体管理番号並びに複製元となるライセンス媒体のライセンス媒体管理番号を情報セキュリティ管理者に伝達しなければならない。

情報セキュリティ管理者は、指示された通りにライセンス媒体に貼付した上で、「管理番号通知書兼報告書」に必要事項を記入の上、ソフトウェア資産統括管理担当者宛てに提出しなければならない。

ライセンス媒体へのライセンス媒体管理番号の貼付の際、DVDやCDなど、直接貼付することで劣化の可能性があるものまたは貼付することで記載内容が確認しにくくなるものについては、それを格納するケース等に貼付する。

(9) 記録

① 管理番号の記録

(ア) 記録の実施

統括情報セキュリティ責任者は、管理番号を付与する際には、ソフトウェア資産統括管理担当者に指示し、「管理番号発行管理簿」に記録させなければならない。

(イ) 記録の確認

記録された内容は、統括情報セキュリティ責任者が、速やかに誤りのないことを確認しなければならない。

② 管理台帳への登録

(ア) ハードウェア

ソフトウェア資産統括管理担当者は、納品された情報を入手次第、「ハードウェア管理台帳」に記録しなければならない。記録した内容は、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認しなければならない。

確認の結果、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

(イ) 標準ソフトウェア

ソフトウェア資産統括管理担当者は、ライセンス媒体管理番号が付与され次第、「ライセンス管理台帳」及び「ソフトウェア媒体管理台帳」に記録しなければならない。

記録した内容は、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認しなければならない。

確認の結果、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

(ウ) CAL

ソフトウェア資産統括管理担当者は、納品を確認次第、「ライセンス管理台帳」に記録しなければならない。

記録した内容は、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認しなければならない。

確認の結果、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

(エ) 個別利用ソフトウェア

ソフトウェア資産管理担当者は、情報セキュリティ管理者から、ライセンス媒体管理番号が付与され次第、「ライセンス管理台帳」及び「ソフトウェア媒体管理台帳」に記録しなければならない。

記録した内容は、別のソフトウェア資産管理担当者もしくは情報セキュリティ管理者が確認しなければならない。

確認の結果、不備が発見された場合には、記録したソフトウェア資産管理担当者に指示し、速やかに修正させなければならない。

(オ) 複製物の記録

当該ライセンス媒体を一意に管理するために、複製元と同様に当該ライセンス媒体の複製元のライセンス媒体管理番号を「ソフトウェア媒体管理台帳」に記録しなければならない。

(カ) アップグレード

アップグレードライセンスを調達した際は、当該ライセンス媒体のライセンス媒体管理番号に加え、アップグレード元となるライセンスのライセンス媒体管理番号を「ライセンス管理台帳」に登録しなければならない。

(10) 保管

下記ものは、指定された管理担当者等が、紛失、盗難、改ざん等を防止できるような環境下で、【公文書保存規程】に従い、適切に保管し管理しなければならない。

- ① 仕様書及び調達先との契約書等
仕様書の確認者が管理する。
- ② 標準ソフトウェア調達申請書兼報告書
統括情報セキュリティ責任者が管理する。
- ③ 個別利用ソフトウェア調達申請書兼報告書
情報セキュリティ責任者が管理する。
- ④ 管理番号体系一覧
統括情報セキュリティ責任者が管理する。
- ⑤ 管理番号発行管理簿
統括情報セキュリティ責任者が管理する。
- ⑥ 管理番号通知書兼報告書
統括情報セキュリティ責任者が管理する。
- ⑦ ライセンス媒体複製申請書兼報告書
 - (ア) 標準ソフトウェア
統括情報セキュリティ責任者が管理する。
 - (イ) 個別利用ソフトウェア
情報セキュリティ責任者が管理する。

- ⑧ ライセンス媒体
 - (ア) 標準ソフトウェア
統括情報セキュリティ責任者が管理する。
 - (イ) 個別利用ソフトウェア
情報セキュリティ責任者が管理する。

5. ソフトウェアの導入・更新手続き

(1) 標準ソフトウェア

① 導入・更新の申請

申請者は「標準ソフトウェア導入／変更申請書兼報告書」に必要事項を記入し、統括情報セキュリティ責任者の承認を得なければならない。

② 導入・更新可能ライセンスの確認

統括情報セキュリティ責任者は、申請されたソフトウェアのライセンス利用状況及び使用条件を「使用許諾条件確認書」及び、「利用ソフトウェア管理台帳」、「ライセンス管理台帳」にて確認し、申請の可否を判断する。

③ ソフトウェア導入・更新の実施

申請者は、承認されたソフトウェアの導入・更新を速やかに実施し、実施後、「標準ソフトウェア導入／変更申請書兼報告書」に必要事項を記入の上、統括情報セキュリティ責任者に提出する。

④ 一括導入・一括更新の実施

対象範囲内での標準ソフトの変更や、ハードウェアの大規模な調達等により、申請者からの要請なく標準ソフトウェアを導入・更新する場合は、統括情報セキュリティ責任者は、「一括導入／更新計画書」を策定し、最高情報統括責任者の承認を得なければならない。

「一括導入／更新計画書」には、少なくとも以下のことを記載しなければならない。

- ・ 導入／更新ソフトウェアの動作検証方法及び検証結果
- ・ 導入／更新対象ハードウェアのバックアップの範囲及び方法
- ・ バックアップスケジュール
- ・ 導入／更新方法を記載したマニュアル
- ・ 導入／更新スケジュール
- ・ 導入／更新が失敗した際のバックアップによる復元方法及びその検証

(2) 個別利用ソフトウェア

① 導入・更新申請

申請者は「個別利用ソフトウェア導入／変更申請書兼報告書」に必要事項を記入し、情報セキュリティ責任者の承認を得た上で写しを統括情報セキュリティ責任者に提出しなければならない。

② 導入・更新可能ライセンスの確認

情報セキュリティ責任者は、申請されたソフトウェアのライセンス利用状況を「利用ソフトウェア管理台帳」及び「ライセンス管理台帳」にて確認し、自らの管理範囲内で余剰がある場合には、申請を承認する。

③ ソフトウェアの導入・更新

申請者は、承認されたソフトウェアの導入・更新を速やかに実施し、導入・更新実施後、「個別利用ソフトウェア導入／変更申請書兼報告書」に必要事項を記入の上、統括情報セキュリティ責任者に提出する。

(3) ドライバー・更新プログラム等及びその他

① 導入・更新申請及びその実施

申請者は「ドライバー等導入／変更申請書兼報告書」に必要事項を記入し、情報セキュリティ責任者の承認を得た上で写しを統括情報セキュリティ責任者に提出し速やかに導入・更新しなければならない。

② 一括導入・一括更新

セキュリティ管理や内部システム管理のために、統括情報セキュリティ責任者が、導入・更新しなければならないと判断したドライバー・更新プログラム等及びその他を導入・更新する場合は、統括情報セキュリティ責任者は、「一括導入／更新計画書」を策定し、最高情報統括責任者の承認を得なければならない。

「一括導入／更新計画書」には、少なくとも以下のことを記載しなければならない。

- ・ 導入ソフトウェアの動作検証方法及び検証結果
- ・ 導入対象ハードウェアのバックアップの範囲及び方法
- ・ バックアップスケジュール
- ・ 導入方法を記載したマニュアル
- ・ 導入スケジュール
- ・ 導入が失敗した際のバックアップによる復元方法及びその検証

(4) 記録

① ライセンスの利用予約

(ア) 標準ソフトウェア

統括情報セキュリティ責任者は、導入・更新申請の承認後速やかに、ソフトウェア資産統括管理担当者に指示し、承認したライセンス数を利用予定のライセンスとして「ライセンス管理台帳」に記載し、ライセンス余剰数を減じなければならない。

記録した内容は、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認し、その結果、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

(イ) 個別利用ソフトウェア

情報セキュリティ責任者は、導入・更新申請の承認後速やかに、ソフトウェア資産管理担当者に指示し、承認したライセンス数を利用予定のライセンスとしてライセンス管理台帳に記載し、ライセンス余剰数を減じなければならない。

記録した内容は、別のソフトウェア資産管理担当者もしくは情報セキュリティ管理者が確認し、その結果、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

② 管理台帳の更新

(ア) 標準ソフトウェア

統括情報セキュリティ責任者は、ソフトウェア資産統括管理担当者に指示し、ソフトウェアの導入・更新時に、「ハードウェア管理台帳」、「利用ソフトウェア管理台帳」、「ライセンス管理台帳」、「ソフトウェア媒体管理台帳」の記載情報を更新しなければならない。

更新した内容は、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認し、その結果、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

(イ) 個別利用ソフトウェア

統括情報セキュリティ責任者は、ソフトウェア資産統括管理担当者に指示し、ソフトウェアの導入・更新時に、「ハードウェア管理台帳」、「利用ソフトウェア管理台帳」、「ライセンス管理台帳」、「ソフトウェア媒体管理台帳」の記載情報を更新しなければならない。

更新した内容は、別のソフトウェア資産管理担当者もしくは情報セキュリティ管理者が確認し、その結果、不備が発見された場合には、記録したソフトウェア資産管理担当者に指示し、速やかに修正させなければならない。

(ウ) CAL

導入・更新のための変更はない。

(エ) ドライバー・更新プログラム等及びその他

管理台帳には記載しない。

(オ) ダウングレード

ソフトウェアをダウングレードして更新した際は、当該ライセンス媒体のライセンス媒体管理番号に加え、ダウングレード元となるライセンスのソフトウェア媒体管理番号を「ライセンス管理台帳」に登録しなければならない。

③ ライセンス媒体貸出簿

ソフトウェアの導入・更新に伴う、ライセンス媒体の入出庫を管理するために、「ライセンス媒体貸出簿」を策定しなければならない。

ライセンス媒体貸出簿には、以下の項目を含まなければならない。

- ・ライセンス媒体管理番号
- ・ソフトウェア名
- ・標準ソフトウェア導入申請書兼報告書管理番号
- ・貸出日
- ・貸出者
- ・借出者
- ・返却予定日
- ・返却確認日
- ・返却確認者

(ア) 標準ソフトウェア

統括情報セキュリティ責任者が、「ライセンス媒体貸出簿」を策定しなければならない。

(イ) 個別利用ソフトウェア

情報セキュリティ責任者が「ライセンス媒体貸出簿」を策定しなければならない。

(5) 保管

下記のものは、指定された管理担当者等が、紛失、盗難、改ざん等を防止できるような環境下で、【公文書保存規程】に従い、適切に保管し管理しなければならない。

- ① 標準ソフトウェア導入／変更申請書兼報告書
統括情報セキュリティ責任者が管理する。
- ② 個別利用ソフトウェア導入／変更申請書兼報告書
情報セキュリティ責任者が管理する。
- ③ ドライバー等導入／変更申請書兼報告書
統括情報セキュリティ責任者が管理する。
- ④ 一括導入計画書
統括情報セキュリティ責任者が管理する。
- ⑤ ライセンス媒体貸出簿
 - (ア) 標準ソフトウェア
統括情報セキュリティ責任者が管理する。
 - (イ) 個別利用ソフトウェア
情報セキュリティ責任者が管理する。

6. ソフトウェアの転用手続き

(1) 標準ソフトウェア

- ① 転用申請
使用許諾条件がユーザーライセンスのものについて使用者を変更する場合には、申請者は「標準ソフトウェア導入／変更申請書兼報告書」に必要事項を記入し、統括情報セキュリティ責任者の承認を得なければならない。
- ② 転用可能ライセンスの確認
統括情報セキュリティ責任者は、申請されたソフトウェアのライセンス利用状況及び使用条件を「使用許諾条件確認書」及び、「利用ソフトウェア管理台帳」、「ラ

イセンス管理台帳」にて確認し、申請の可否を判断する。

③ ソフトウェアの転用

申請者は、承認されたソフトウェアの転用を速やかに実施し、実施後、「標準ソフトウェア導入／変更申請書兼報告書」に必要事項を記入の上、統括情報セキュリティ責任者に提出する。

(2) 個別利用ソフトウェア

① 転用申請

申請者は「個別利用ソフトウェア導入／変更申請書兼報告書」に必要事項を記入し、情報セキュリティ責任者の承認を得た上で写しを統括情報セキュリティ責任者に提出しなければならない。

② 転用可能ライセンスの確認

情報セキュリティ責任者は、申請されたソフトウェアのライセンス利用状況及び使用条件を「使用許諾条件確認書」及び、「利用ソフトウェア管理台帳」、「ライセンス管理台帳」にて確認し、申請の可否を判断する。

③ ソフトウェアの転用

申請者は、承認されたソフトウェアの転用を速やかに実施し、実施後、「個別利用ソフトウェア導入／変更申請書兼報告書」に必要事項を記入の上、統括情報セキュリティ責任者に提出する。

(3) 記録

① 管理台帳の更新

(ア) 標準ソフトウェア

統括情報セキュリティ責任者は、ソフトウェア資産統括管理担当者に指示し、ソフトウェアの転用時に必要に応じて、「ハードウェア管理台帳」、「利用ソフトウェア管理台帳」、「ライセンス管理台帳」、「ソフトウェア媒体管理台帳」の記載情報を更新しなければならない。

更新した内容は、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認し、その結果、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

(イ) 個別利用ソフトウェア

情報セキュリティ責任者は、ソフトウェア資産管理担当者に指示し、ソフトウェアの転用時に必要に応じて「ハードウェア管理台帳」、「利用ソフトウェア管理台帳」、「ライセンス管理台帳」、「ソフトウェア媒体管理台帳」の記載情報を更新しなければならない。

更新した内容は、別のソフトウェア資産管理担当者もしくは情報セキュリティ管理者が確認し、その結果、不備が発見された場合には、記録したソフトウェア資産管理担当者に指示し、速やかに修正させなければならない。

(ウ) ダウングレード

ソフトウェアをダウングレードして転用した際は、当該ライセンス媒体のライセンス媒体管理番号に加え、ダウングレード元となるライセンスのソフトウェア媒体管理番号を「ライセンス管理台帳」に登録しなければならない。

② ライセンス媒体貸出簿

必要に応じて、ソフトウェアの転用・導入・更新に伴うライセンス媒体の入出庫を管理するために、「ライセンス媒体貸出簿」を策定しなければならない。

ライセンス媒体貸出簿には、以下の項目を含まなければならない。

- ・ライセンス媒体管理番号
- ・ソフトウェア名
- ・標準ソフトウェア導入申請書兼報告書管理番号
- ・貸出日
- ・貸出者
- ・借出者
- ・返却予定日
- ・返却確認日
- ・返却確認者

(ア) 標準ソフトウェア

統括情報セキュリティ責任者が、「ライセンス媒体貸出簿」を策定しなければならない。

(イ) 個別利用ソフトウェア

情報セキュリティ責任者が「ライセンス媒体貸出簿」を策定しなければならない。

7. ソフトウェア資産の削除手続き

(1) 標準ソフトウェア

① 通常の削除時の手続き

標準ソフトウェアを削除する場合には、「標準ソフトウェア削除申請書兼報告書」に必要事項を記入し、統括情報セキュリティ責任者の承認を得なければならない。

② 一括削除の手続き

標準ソフトウェアを一括して削除する際には、「標準ソフトウェア一括削除申請書兼報告書」に必要事項を記入し、通常削除時の手続きと同様に承認を得なければならない。

③ 削除報告

申請者はソフトウェアの削除が完了次第、承認された「標準ソフトウェア削除申請書兼報告書」もしくは「標準ソフトウェア一括削除申請書兼報告書」に削除が完了した旨の追記をし、統括情報セキュリティ責任者に報告しなければならない。

(2) 個別利用ソフトウェア

① 削除時の手続き

個別利用ソフトウェアを削除する場合には、「個別利用ソフトウェア削除申請書兼報告書」に必要事項を記入し、情報セキュリティ責任者の承認を得なければならない。

② 削除報告

申請者はソフトウェアの削除が完了次第、承認された「個別利用ソフトウェア削除申請書兼報告書」に削除が完了した旨の追記をし、情報セキュリティ管理者並びに統括情報セキュリティ責任者に報告しなければならない。

(3) ドライバー・更新プログラム等及びその他

① 削除時の手続き

ドライバー・更新プログラム等及びその他を削除する場合には、「ドライバー等削除申請書兼報告書」に必要事項を記入し、統括情報セキュリティ責任者の承認を得なければならない。

(4) 禁止ソフトウェア

禁止ソフトウェアを導入又は導入していることを発見した場合には、以下の手順に従う。

- ① インターネットを含め、ネットワークに接続されている場合には、接続を解除する。
- ② 禁止ソフトウェアを導入又は導入していることを発見した職員等は、統括情報セキュリティ責任者もしくは最高情報統括責任者に報告する。
- ③ 統括情報セキュリティ責任者は、原因を究明し、是正措置を実施する。

(5) 記録

① 標準ソフトウェア

統括情報セキュリティ責任者は、「標準ソフトウェア削除申請書兼報告書」もしくは「標準ソフトウェア一括削除申請書兼報告書」にて、削除の報告を受領次第、ソフトウェア資産統括管理担当者に指示し、「利用ソフトウェア管理台帳」を変更しなければならない。

変更した内容は、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認しなければならない。

確認の結果不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

② 個別利用ソフトウェア

ソフトウェア資産管理担当者は、「個別利用ソフトウェア削除申請書兼報告書」にて申請したソフトウェアを削除次第、削除申請をした「個別利用ソフトウェア削除申請書兼報告書」に必要事項を記入し、情報セキュリティ管理者に報告しなければならない。情報セキュリティ管理者は報告を受領次第、ソフトウェア資産管理担当者に指示し、「利用ソフトウェア管理台帳」を変更しなければならない。

変更した内容は、別のソフトウェア資産管理担当者もしくは情報セキュリティ管理者が確認しなければならない。

確認の結果不備が発見された場合には、記録したソフトウェア資産管理担当者に指示し、速やかに修正させなければならない。

また、変更が完了次第、統括情報セキュリティ責任者へ削除が完了した旨を報告しなければならない。

- ③ ドライバー・更新プログラム等及びその他
ドライバー・更新プログラム等及びその他の削除の記録は、「ドライバー等削除申請書兼報告書」にのみ実施する。
- ④ 禁止ソフトウェア
統括情報セキュリティ責任者は、禁止ソフトウェアの導入が発見された場合、以下の情報を記録した「禁止ソフトウェア発見／対応報告書」を作成し、最高情報統括責任者に報告しなければならない。
- ・ソフトウェア名称
 - ・発見者
 - ・発見日時
 - ・削除日時
 - ・削除者
 - ・削除確認者
 - ・禁止ソフトウェアの導入理由
 - ・是正措置

(6) 保管

下記のものは、指定された管理担当者等が、紛失、盗難、改ざん等を防止できるような環境下で、【公文書保存規程】に従い、適切に保管し管理しなければならない。

- ① 標準ソフトウェア削除申請書兼報告書
統括情報セキュリティ責任者が管理する。
- ② 標準ソフトウェア一括削除申請書兼報告書
統括情報セキュリティ責任者が管理する。
- ③ 個別利用ソフトウェア削除申請書兼報告書
情報セキュリティ責任者が管理する。
- ④ ドライバー等削除申請書兼報告書
申請者がソフトウェア資産統括管理担当者の場合には、統括情報セキュリティ責任者が、ソフトウェア資産管理担当者の場合には情報セキュリティ責任者が管理する。
- ⑤ 禁止ソフトウェア発見／対応報告書
統括情報セキュリティ責任者が管理する。

8. ソフトウェア資産の廃棄手続き

(1) ハードウェアの廃棄時

ハードウェアを廃棄する際は、本文書“7. ソフトウェア資産の削除手続き”に従ってソフトウェア資産を削除しなければならない。

(2) ライセンス媒体及び複製物の廃棄

① 廃棄時の手続き

(ア) 事前削除

ライセンス媒体及び複製物を廃棄する際には、本文書“7. ソフトウェア資産の削除手続き”に従って、廃棄申請前に、導入されている廃棄対象ソフトウェアを全て削除しなければならない。

(イ) 廃棄申請

ライセンス媒体及び複製物を廃棄する場合には、申請者が「ソフトウェア媒体廃棄申請書兼報告書」に必要事項を記入し、統括情報セキュリティ責任者の承認を得なければならない。

② 廃棄の実施及び確認

ライセンス媒体及び複製物の廃棄は、ソフトウェア資産統括管理担当者が実施し、統括情報セキュリティ責任者が確認する。

(3) 記録

統括情報セキュリティ責任者は、「ソフトウェア媒体廃棄申請書兼報告書」にて廃棄の報告を受領し、実際に廃棄を確認次第、ソフトウェア資産統括管理担当者に指示し、「ライセンス管理台帳」及び「ソフトウェア媒体管理台帳」「利用ソフトウェア管理台帳」を変更しなければならない。

また、「ライセンス媒体管理簿」に削除した旨、記入しなければならない。

変更した内容及び記入した内容については、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認し、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

(4) 保管

下記のものは、指定された管理担当者等が、紛失、盗難、改ざん等を防止できるような環境下で、【公文書保存規程】に従い、適切に保管し管理しなければならない。

- ① ソフトウェア媒体廃棄申請書兼報告書
統括情報セキュリティ責任者が管理する。

9. ライセンス情報の入手

ライセンス情報の入手は、【ソフトウェア資産管理対策基準】“8. ライセンス情報の入手”に拠る。

10. 研修

(1) 研修の実施

研修の実施は、【ソフトウェア資産管理対策基準】“9. 研修”に拠る。なお本研修は単独で実施せず、情報セキュリティ研修など他の研修に含んで実施しても良い。

(2) 研修計画の策定

統括情報セキュリティ責任者は、以下の内容を含めた「研修年度計画」を策定し、最高情報統括責任者に提出しなければならない。

- ① 実施する予定の研修の種類
- ② 実施する予定の研修内容
- ③ 実施予定スケジュール
- ④ 期待する効果

(3) 研修の種類

研修は、職員等が初めて職務に着く際に実施する導入研修と、年1回、定期的を実施する継続研修があり、さらに管理担当者等に実施するものと、管理担当者等を除く職員等に実施するものに分ける。

- ① 導入研修
 - (ア) 管理担当者等
 - (イ) 管理担当者等を除く職員等

② 継続研修

- (ア) 管理担当者等
- (イ) 管理担当者等を除く職員等

(4) 研修の内容

研修には、ソフトウェア資産管理全般の知識及び使用許諾条件の種類やその内容、本文書並びに【ソフトウェア資産管理対策基準】の内容を次の通り含まなければならない。

① 導入研修の内容

- (ア) 管理担当者等
 - ・ 使用許諾条件の種類やその内容
 - ・ 本文書並びに【ソフトウェア資産管理対策基準】の内容
- (イ) 管理担当者等を除く職員等
 - ・ 本文書並びに【ソフトウェア資産管理対策基準】の内容

② 継続研修

- (ア) 管理担当者等
 - ・ ソフトウェア資産管理の重要性
 - ・ 使用許諾条件の種類やその内容
 - ・ 使用許諾条件やライセンス形態に関する最新情報
 - ・ 本文書並びに【ソフトウェア資産管理対策基準】
- (イ) 管理担当者等を除く職員等
 - ・ ソフトウェア資産管理の重要性
 - ・ 本文書並びに【ソフトウェア資産管理対策基準】の内容

(5) 研修結果のレビュー

① 実施の完全性の確保

導入研修、継続研修ともに、対象となる職員等の全てが受講できるようにしなければならない。

② 理解度の確認

研修実施後に、参加者に対し研修の内容に関する理解度確認のためのテストを実施しなければならない。

③ 定期的なレビューの実施

統括情報セキュリティ責任者は、毎年1回定期的に、次の項目を含む研修結果の報告書（以下「研修結果報告書」という）を策定し、最高情報統括責任者に報告しなければならない。

- (ア) 研修受講者のリスト
- (イ) 研修内容の要約
- (ウ) 研修受講者の理解度の要約
- (エ) 課題・問題点の要約
- (オ) 次回のポイント

(6) 保管

下記のは、指定された管理担当者等が、紛失、盗難、改ざん等を防止できるような環境下で、【公文書保存規程】に従い、適切に保管し管理しなければならない。

① 研修結果報告書

統括情報セキュリティ責任者が管理する。

② 研修年度計画

統括情報セキュリティ責任者が管理する。

1 1 . 検証

(1) 棚卸

① 棚卸計画

(ア) 棚卸計画の内容

統括情報セキュリティ責任者は、以下の内容を含む「棚卸年度計画」を策定し、管理担当者等に周知しなければならない。

- ・実施回数
- ・実施時期
- ・対象資産
- ・棚卸方法

(イ) 対象資産毎の棚卸実施回数

【ソフトウェア資産管理対策基準】“1 0 . 棚卸(2)棚卸の実施回数”に拠る。

② 棚卸の実施

(ア) 棚卸の依頼

統括情報セキュリティ責任者は、情報セキュリティ責任者に対し、棚卸の実施依頼をし、情報セキュリティ責任者は、依頼に基づき、自らの責任範囲において棚卸を実施しなければならない。

(イ) 棚卸用データの提供

統括情報セキュリティ責任者は、情報セキュリティ責任者が棚卸を実施する際に利用する「棚卸用データ」並びに棚卸の手順をまとめた「棚卸手順書」を準備し、提供しなければならない。

(ウ) 棚卸の実施

情報セキュリティ責任者は、統括情報セキュリティ責任者の指示に基づく方法で、棚卸の結果を「棚卸実施結果」として取りまとめなければならない。

(エ) 棚卸期限の順守

情報セキュリティ責任者は、統括情報セキュリティ責任者の指示に基づく方法で棚卸を実施し、「棚卸実施結果」を、定められた期間内に統括情報セキュリティ責任者に報告しなければならない。

(オ) 棚卸結果の妥当性の検証

統括情報セキュリティ責任者は、ソフトウェア資産統括管理担当者に指示し、情報セキュリティ責任者からの「棚卸実施結果」の妥当性を管理記録等及び関連記録等を元に検証する。

検証の結果、疑義が生じたものについては、ソフトウェア資産統括管理担当者から情報セキュリティ責任者に確認し、情報セキュリティ責任者は速やかに調査の上、回答しなければならない。

③ 棚卸結果の報告及び是正措置

【ソフトウェア資産管理対策基準】 10. 棚卸(3)棚卸結果の報告及び是正措置に拠る。

④ 記録

統括情報セキュリティ責任者は、棚卸により発見された管理台帳との不一致を是正するため、ソフトウェア資産統括管理担当者に指示し、必要に応じて管理台帳の情報を変更させなければならない。

変更した内容については、別のソフトウェア資産統括管理担当者もしくは統括情報セキュリティ責任者が確認し、不備が発見された場合には、記録したソフトウェア資産統括管理担当者に指示し、速やかに修正させなければならない。

⑤ 保管

下記のものは、指定された管理担当者等が、紛失、盗難、改ざん等を防止できるような環境下で、【公文書保存規程】に従い、適切に保管し管理しなければならない。

(ア) 棚卸年度計画

統括情報セキュリティ責任者が管理する。

(イ) 棚卸用データ

統括情報セキュリティ責任者が、原本を保管し管理する。

(ウ) 棚卸手順書

統括情報セキュリティ責任者が管理する。

(エ) 棚卸実施結果

統括情報セキュリティ責任者が管理する。

(オ) 棚卸結果報告書

統括情報セキュリティ責任者が管理する。

(2) 監査

① 監査計画

監査責任者は、以下の内容を含む「監査年度計画」を策定し、最高情報統括責任者の承認を得た上で、管理担当者等に周知しなければならない。

- ・実施スケジュール
- ・監査の種別（内部監査／外部監査）
- ・監査の方法
- ・監査の対象範囲

② 内部監査の内容

内部監査は、以下の内容を含んで実施しなければならない。

- ・対象資産の利用状況と管理台帳との差分の有無
- ・管理記録等の管理状況
- ・ソフトウェア媒体及び関連記録等の管理状況
- ・本文書及び【ソフトウェア資産管理対策基準】の認識と理解
- ・ソフトウェア資産管理の必要性の認識と理解

③ 内部監査報告等

内部監査に関する監査実施方法及び「監査報告」等の詳細については、【監査・自己点検実施基準】に拠る。

④ 外部監査による成熟度評価

外部監査は、対象範囲のソフトウェア資産管理に関する「成熟度評価」を目的に実施する。成熟度評価では、以下の監査基準を参考に、内部監査の内容に加え、本文書並びに【ソフトウェア資産管理対策基準】に定める内容についても評価の対象としなければならない。

- ・ソフトウェア資産管理基準
- ・ソフトウェア資産管理評価規準
(ともにNPO法人ソフトウェア資産管理コンソーシアム策定)
- ・ISO/IEC19770-1

⑤ 外部監査委託先の能力

ソフトウェア資産管理の成熟度評価の能力の有無を図る際の「監査委託仕様書」の策定に当たっては、以下の団体の意見を参考にする。

- ・ビジネスソフトウェアアライアンス
- ・NPO法人ソフトウェア資産管理コンソーシアム

⑥ 監査結果の報告及び是正措置

【ソフトウェア資産管理対策基準】 1 1. 監査(2)監査結果の報告及び是正措置に拠る。

⑦ 保管

下記のものは、指定された管理担当者等が、紛失、盗難、改ざん等を防止できるような環境下で、【公文書保存規程】に従い、適切に保管し管理しなければならない。

(ア) 監査年度計画

監査責任者が管理する。

(イ) 監査報告

監査責任者と統括情報セキュリティ責任者のそれぞれが、原本を保管し管理する。

(ウ) 成熟度評価

監査責任者と統括情報セキュリティ責任者のそれぞれが、原本を保管し管理する。

(エ) 監査委託仕様書

監査責任者が管理する。

1 2. 本文書の見直し

【ソフトウェア資産管理対策基準】“1 5. 本文書の見直し”に拠る。

1 3. 違反への対応

【ソフトウェア資産管理対策基準】“1 6. 違反への対応”に拠る。

1 4. 参照資料

(1) 準拠、参照する基準等

(ア)〇〇市情報セキュリティ対策基準

(イ)〇〇市情報セキュリティポリシー

(ウ)公文書保存規程

(エ)パソコン等取扱規程

(オ)物品調達基準

(カ)監査・自己点検実施基準

(キ)ソフトウェア資産管理対策基準

(ク)ソフトウェア資産管理基準（NPO法人ソフトウェア資産管理コンソーシアム）

(ケ)ISO/IEC19770-1