

# ソフトウェア資産管理対策基準 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/>

## 目次

はじめに .....	6
(1) 目的 .....	6
(2) 組織の対象範囲 .....	6
(3) 対象資産の範囲 .....	6
<b>1. 組織体制及び責任と役割 .....</b>	<b>7</b>
(1) 責任と役割 .....	
(2) 兼務の禁止 .....	9
(3) 連絡体制の整備 .....	9
<b>2. 用語 .....</b>	<b>10</b>
<b>3. ソフトウェアの分類 .....</b>	<b>12</b>
<b>4. 対象資産の調達に関する情報の把握 .....</b>	<b>12</b>
<b>5. ソフトウェアの導入等に関する情報の把握 .....</b>	<b>13</b>
<b>6. 対象資産の管理 .....</b>	<b>13</b>
(1) 対象ソフトウェアの制定 .....	13
(2) 管理台帳の作成 .....	13
(3) 管理台帳の関連性の考慮 .....	14
(4) 管理台帳記載情報の更新 .....	14
(5) ライセンス媒体及び関連記録等の管理 .....	14
<b>7. ソフトウェア等の廃棄・返却 .....</b>	<b>16</b>
(1) ハードウェアの廃棄時 .....	16
(2) リースまたはレンタルしているハードウェアの返却時 .....	16

<b>8. ライセンス情報の入手</b> .....	<b>16</b>
<b>9. 研修</b> .....	<b>17</b>
<b>10. 棚卸</b> .....	<b>17</b>
(1) 棚卸手順の策定 .....	17
(2) 棚卸の実施回数 .....	17
(3) 棚卸結果の報告及び是正措置 .....	17
(4) 保管 .....	17
<b>11. 監査</b> .....	<b>18</b>
(1) 監査の実施 .....	18
(2) 監査結果の報告及び是正措置 .....	18
<b>12. ライセンスコンプライアンスの遵守</b> .....	<b>18</b>
<b>13. ソフトウェア資産管理年度計画の策定</b> .....	<b>18</b>
(1) ソフトウェア資産管理年度計画の策定 .....	18
(2) 年度計画の承認 .....	19
(3) 年度計画の進捗管理 .....	19
<b>14. ソフトウェア資産管理の適合性検証</b> .....	<b>19</b>
<b>15. 本文書の見直し</b> .....	<b>19</b>
(1) 見直し .....	19
(2) 定めのない事項について .....	19
(3) 優先事項 .....	19

16. 違反への対応..... 20

17. 参照資料 ..... 20

## はじめに

### (1) 目的

ソフトウェア資産管理対策基準（以下、「本文書」という）は、〇〇市（以下、「本市」という）におけるソフトウェア（ソフトウェアとは、その機能を利用するためにパーソナルコンピュータやサーバーに導入することができる又は導入されたものをいう。以下同じ。）の使用及び管理の必要事項について定めたものである。

本文書は、本市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且つ有用な使用を推進することを目的とする。

本文書が要求する事項の具体的な実施手順等については、【ソフトウェア資産管理対策手順書】に別途定める。

### (2) 組織の対象範囲

本文書が適用される範囲は、【〇〇市情報セキュリティ対策基準】と同様の範囲とする。

### (3) 対象資産の範囲

本文書が対象とする資産（以下「対象資産」という）は、次の通りとする。

- ① ソフトウェアが稼働する又は稼働する可能性のあるパーソナルコンピュータもしくはサーバー等（以下「ハードウェア」という）。
- ② ソフトウェア
- ③ ソフトウェアを利用するためのライセンス（ライセンスとは、ソフトウェアを利用するために当該ソフトウェアメーカーから正式に取得した使用許諾をいう。以下同じ。）及びライセンス媒体（ライセンス媒体とは、ライセンスされていることを証する部材のすべてをいう。例えば、インストール用DVD、ソフトウェアのパッケージ（外箱）、ライセンス証書、使用許諾契約書、マニュアル等。以下同じ。）。

## 1. 組織体制及び責任と役割

### (1) 責任と役割

#### ① 最高情報統括責任者

- (ア) 最高情報統括責任者は、【〇〇市情報セキュリティ対策基準】の定める通りに決定する。
- (イ) 最高情報統括責任者は、本文書が定める本市における全ての対象資産の管理及び対策に関する最終決定権限及び責任を有する。
- (ウ) 最高情報統括責任者は、対象範囲内で利用されるすべてのソフトウェアが適正にライセンスを受け、その契約条件に従い利用されているようにしなければならない。
- (エ) 最高情報統括責任者は、必要に応じ、ソフトウェア資産の管理に関する専門的な知識及び経験を有した専門家をアドバイザーとして置くものとする。

#### ② 統括情報セキュリティ責任者

- (ア) 統括情報セキュリティ責任者は、【〇〇市情報セキュリティ対策基準】の定める通りに決定するものとする。
- (イ) 統括情報セキュリティ責任者は、最高情報統括責任者を補佐しなければならない。
- (ウ) 統括情報セキュリティ責任者は、本文書が定める本市の全ての対象資産におけるソフトウェア資産（ソフトウェア資産とは、利用されているソフトウェアと、そのライセンス媒体を総称したものをいう。以下同じ。）の管理に関する設定の変更、運用、見直し等を行う権限及び責任を有する。
- (エ) 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、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、ソフトウェア資産の管理に関する指導及び助言を行う権限を有する。
- (オ) 統括情報セキュリティ責任者は、本市の対象資産に対する侵害が発生した場合又は侵害の恐れがある場合もしくは、本市が利用しているソフトウェア資産の所有者の権利に対し侵害を発生又はその恐れが生じた場合には、最高情報統括責任者の指示に従い、最高情報統括責任者が不在の場合には自らの判断に基づき、必要且つ十分な措置を行う権限及び責任を有する。

- (カ) 統括情報セキュリティ責任者は、本市の対象資産に関するソフトウェア資産管理実施手順の維持・管理を行う権限及び責任を有する。
- (キ) 統括情報セキュリティ責任者は、対象範囲内の職員等（職員、非常勤職員及び臨時職員をいう。以下同じ。）に対する教育、訓練に関する助言及び指示を、情報セキュリティ責任者を通じて行う。
- (ク) 統括情報セキュリティ責任者は、本文書“1. 組織体制及び責任と役割(5)”記載のソフトウェア資産統括管理担当者に対し、ソフトウェア資産管理に関して、自らが秘密であると判断した情報以外は、すべて共有する。

### ③ 情報セキュリティ責任者

- (ア) 情報セキュリティ責任者は、【〇〇市情報セキュリティ対策基準】の定める通りに決定する。
- (イ) 情報セキュリティ責任者は、当該部局等のソフトウェア資産管理対策に関する統括的な権限及び責任を有す。
- (ウ) 情報セキュリティ責任者は、その所管する部門等において保有しているソフトウェア資産に関する設定・利用者等の変更、運用、見直し等を行う統括的な権限及び責任を有する。
- (エ) 情報セキュリティ責任者は、その所管する部門等において保有しているソフトウェア資産について、本文書並びに関連する文書に関する意見の集約及び、統括情報セキュリティ責任者の指示に基づく職員等に対する教育、訓練を行う。

### ④ 情報セキュリティ管理者

- (ア) 情報セキュリティ管理者は、【〇〇市情報セキュリティ対策基準】の定める通りに決定する。
- (イ) 情報セキュリティ管理者は、その所管する課室等のソフトウェア資産の管理に関する権限及び責任を有する。
- (ウ) 情報セキュリティ管理者は、その所管する課室等において、本市の対象資産に対する侵害が発生した場合又は侵害の恐れがある場合もしくは、本市が利用しているソフトウェア資産の所有者の権利に対し侵害が発生又はその恐れが生じた場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び最高情報統括責任者へ速やかに報告を行い、指示を仰がなければならない。

## ⑤ ソフトウェア資産統括管理担当者

- (ア) 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が任命し、ソフトウェア資産管理担当者とともに、対象範囲内の職員等に周知徹底する。(ソフトウェア資産統括管理担当者の人数に定めはないが、統括情報セキュリティ責任者は、本文書が定めるソフトウェア資産管理が適切に行える人数を考慮の上、決定しなければならない。)
- (イ) 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、情報セキュリティ責任者に対し、ソフトウェア資産管理の実施、対策等の指示、依頼等を行う。

## ⑥ ソフトウェア資産管理担当者

- (ア) ソフトウェア資産管理担当者は、情報セキュリティ責任者もしくは情報セキュリティ管理者によって任命し、統括情報セキュリティ責任者に報告する。情報セキュリティ責任者もしくは情報セキュリティ管理者の指示に従い、対象資産に関する設定の変更、運用、更新等の作業を行う。情報セキュリティ管理者が兼ねることもある。

## ⑦ 監査責任者

- (ア) 監査責任者は、【監査・自己点検実施基準】の定めるとおりに決定する。
- (イ) 監査責任者は、本市が実施するソフトウェア資産管理が、適切に実施され、且つ、継続的な改善が図れるよう、ソフトウェア資産管理の実施状況に関し、監査計画の策定、監査の実施等に関する権限及び責任を有する。

## (2) 兼務の禁止

- ① ソフトウェア資産管理の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
- ② 監査を受けるものとその監査を実施するものは、やむを得ない場合を除き、同じ者が兼務してはならない。

## (3) 連絡体制の整備

統括情報セキュリティ責任者は、ソフトウェア資産に係る問題等の報告について、連絡・報告体制を整備しなければならない。

## 2. 用語

### (1) 標準ソフトウェア

「標準ソフトウェア」とは、統括情報セキュリティ責任者が、動作検証を実施しており、統括情報セキュリティ責任者の責任において制定した、本文書の対象範囲全体で利用することができるソフトウェアをいう。

### (2) 個別利用ソフトウェア

「個別利用ソフトウェア」とは、情報セキュリティ責任者の責任において制定した、情報セキュリティ責任者の権限範囲内でのみ利用することができるソフトウェアをいう。統括情報セキュリティ責任者の動作検証は実施されていない。

### (3) ソフトウェア媒体

「ソフトウェア媒体」とは、ライセンス媒体の内、ソフトウェアを導入するために特に利用する部材（CD-ROMやDVD-ROMなど）をいう。

### (4) Client Access License

「Client Access License」とは、パーソナルコンピューターが、サーバーの機能を利用する際に必要となるライセンスをいう（以下「CAL」という）。例えば、ファイルサーバーやメールサーバーなどの機能をパーソナルコンピューター側で利用する際に、必要とされるものが多い。

### (5) 調達（ソフトウェアに対して使用する場合）

「調達」とは、ソフトウェアメーカーからソフトウェアを利用する許諾を得ることをいう。無償のソフトウェア（フリーウェア）であっても調達の対象となる。

### (6) 導入（ソフトウェアに対して使用する場合）

「導入」とは、ソフトウェアを使用許諾条件に従って、パーソナルコンピューター又はサーバーあるいはその利用者等に割り当て、当該ソフトウェアの機能を利用できる状態にすることをいう。例えばインストールなど。

#### (7) 削除（ソフトウェアに対して使用する場合）

「削除」とは、ソフトウェアをハードウェアから適切に消去することをいう。例えばアンインストールなど。

#### (8) 禁止ソフトウェア

「禁止ソフトウェア」とは、統括情報セキュリティ責任者が、セキュリティ管理上及び事業継続管理上、有害又は、業務に相応しくないと判断し、調達、導入を一切禁止するソフトウェアをいう。

#### (9) ソフトウェアの転用

「転用」とは、ソフトウェアの利用者を他の利用者に変更することをいう。

#### (10) 更新

「更新」とは、ソフトウェアを使用許諾条件上許可された上位のバージョン（アップグレード）または下位のバージョン（ダウングレード）で利用すること、及びセキュリティパッチやドライバーなどの更新プログラムを適用すること（アップデート）をいう。

#### (11) 適切に保管

「適切に保管」とは、ソフトウェア資産及び管理の実施結果並びにその記録を、本文書及び別途定める【ソフトウェア資産管理対策手順書】で定められた手続きに従い保管し、必要に応じて、速やかに提示できるよう状態を保つことをいう。

#### (12) 適切な期間

「適切な期間」とは、特に言及がない限り【公文書管理規程】により定める当該ソフトウェア資産管理に係る文書及び記録等の保存期間をいう。

#### (13) 管理担当者等

「管理担当者等」とは、最高情報統括責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、ソフトウェア資産統括管理担当者、ソフトウェア資産管理担当者を総称していう。

#### (14) 棚卸

「棚卸」とは、管理台帳の記載事項が、使用実態と合致していることを検証するために実施する作業をいう。

#### (15) 管理記録等

「管理記録等」とは、ソフトウェア資産管理を実施するために別途定める対象資産の管理台帳、及びその記載情報を変更するための各種報告書や申請書類をいう。

#### (16) 関連記録等

「関連記録等」とは、使用許諾を正式に得ていることを証するための補助的な証拠となる各種記録をいう。例えば発注書や請求書、領収証など。

#### (17) 監査責任者

「監査責任者」とは別途定められた【監査・自己点検実施基準】に拠る。

#### (18) ソフトウェアの導入等

「ソフトウェアの導入等」とは、導入・更新・削除・転用を含んだものをいう。

### 3. ソフトウェアの分類

統括情報セキュリティ責任者は、ソフトウェアを以下のとおり分類し、ソフトウェアごとの利用可否について定めるものとする。

- (1) 標準ソフトウェア
- (2) 個別利用ソフトウェア
- (3) CAL
- (4) ドライバー・更新プログラム等
- (5) その他

### 4. 対象資産の調達に関する情報の把握

統括情報セキュリティ責任者は、対象範囲内で調達した対象資産を適時に且つ適切に把握する手順を策定し、対象範囲に周知徹底させなければならない。

## 5. ソフトウェアの導入等に関する情報の把握

統括情報セキュリティ責任者は、ソフトウェアの導入・更新・削除・廃棄・転用がある場合には適時に且つ適切に把握できる手順を策定し、対象範囲に周知徹底させなければならない。

## 6. 対象資産の管理

### (1) 対象ソフトウェアの制定

#### ① 標準ソフトウェア

(ア)統括情報セキュリティ責任者は、標準ソフトウェアを制定しなければならない。

(イ)統括情報セキュリティ責任者は、標準ソフトウェアを制定する際には、使用許諾条件及びソフトウェアの性質を確認し、対象範囲並びに社会に対し不利益をもたらさないソフトウェアであることを確認しなければならない。

#### ② 個別利用ソフトウェア

(ア)情報セキュリティ責任者は、所管する部門等からの要請に従い、個別利用ソフトウェアを許可し、適時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。

(イ)情報セキュリティ責任者は、個別利用ソフトウェアを制定する際には、使用許諾条件及びソフトウェアの性質を確認し、対象範囲並びに社会に対し不利益をもたらさないソフトウェアであることを確認しなければならない。

### (2) 管理台帳の作成

統括情報セキュリティ責任者は、対象資産を適正に管理するために、以下の台帳（以下総称して「管理台帳」という）を保有し、整備する体制を構築し、維持しなければならない。

## ① ハードウェア管理台帳

対象範囲内のハードウェアが記載された台帳。ハードウェア1台毎に一意の管理番号が付与され、必要な変更が適時に記録される。

## ② 利用ソフトウェア管理台帳

ハードウェアに導入されているソフトウェアが記載された台帳。ハードウェアとソフトウェアの組み合わせで利用ソフトウェアが識別できるよう、一意の管理番号が付与され、必要な変更が適時に記録される。また、どのライセンスを適用してソフトウェアを利用しているのかが明確になるよう、ソフトウェア毎に、本文書“6. 対象資産の管理(2)④ソフトウェア媒体管理台帳”の一意の番号と紐づくように管理されなければならない。

## ③ ライセンス管理台帳

対象範囲で保有するライセンスがその保有数とともに記載された台帳。調達したライセンス毎に一意の管理番号が付与され、必要な変更が適時に記録される。

## ④ ソフトウェア媒体管理台帳

ソフトウェア媒体が記載された台帳。ソフトウェア媒体毎に一意の管理番号が付与され、必要な変更が適時記録される。ソフトウェア媒体管理台帳は、どのライセンスに紐づくものであるかを明確にするために、ライセンス管理台帳の一意の番号と紐づくように管理されなければならない。必要に応じて、ライセンス証書番号等もソフトウェア媒体の付属情報として記録される。また、使用許諾条件上、導入媒体の複製が許されており、ソフトウェア媒体を複製して利用する場合には、複製されたものであることが判別できるようにした上で、ソフトウェア媒体管理台帳に記載しなければならない。

## ⑤ ライセンス媒体貸出簿

ソフトウェアを調達した際に取得したライセンス媒体及び許可された複製物の貸出しを適正に記録し、管理するための台帳。ライセンス媒体の所在が把握できるように記載しなければならない。

### (3) 管理台帳の関連性の考慮

管理台帳は、以下を考慮して作成されなければならない。

#### ① ハードウェア管理台帳

利用ソフトウェア管理台帳と紐づき、利用ソフトウェア管理台帳を介して、ライセンス管理台帳、ソフトウェア媒体管理台帳とも紐づくこと。また、ハードウェアの利用者及びCPU(中央演算処理装置)数を含めた性能情報も併せて記載すること。

#### ② 利用ソフトウェア管理台帳

ハードウェア管理台帳、ライセンス管理台帳、ソフトウェア媒体管理台帳と紐づくこと。

#### ③ ライセンス管理台帳

利用ソフトウェア管理台帳、ソフトウェア媒体管理台帳と紐づくこと。

#### ④ ソフトウェア媒体管理台帳

ライセンス管理台帳、利用ソフトウェア台帳と紐づくこと。

#### ⑤ その他

全ての管理台帳項目は、調達したあるいはこれから調達しようとするソフトウェア資産の使用許諾条件を満たすものであること。

### (4) 管理台帳記載情報の更新

統括情報セキュリティ責任者は、すべての管理台帳に記載されている情報が、適時に且つ適切に更新されるよう手順を定め、それを対象範囲に周知徹底させなければならない。

### (5) ライセンス媒体及び関連記録等の管理

#### ① ライセンス媒体及び関連記録等の保管

統括情報セキュリティ責任者は、ライセンス媒体並びに関連記録等を適切に保管する手順を定め、対象範囲に周知徹底させなければならない。

#### ② ライセンス媒体及び関連記録等の保管場所

統括情報セキュリティ責任者は、ライセンス媒体並びに関連記録等を施錠できる場所に保管し、無断使用の防止ができる手順を策定し、対象範囲に周知徹底させなければならない。

### ③ ライセンス媒体の貸出し

統括情報セキュリティ責任者は、ソフトウェアの導入に際し、ライセンス媒体が必要な場合には、ライセンス媒体を貸し出すための手順を策定し、対象範囲に周知徹底させなければならない。

### ④ ライセンス媒体の複製

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を作成する際の手順を定め、対象範囲に周知徹底させなければならない。

## 7. ソフトウェア等の廃棄・返却

### (1) ハードウェアの廃棄時

統括情報セキュリティ責任者は、ハードウェアの廃棄時に、当該ハードウェアに導入されているソフトウェアが確実に削除される手順を定め、対象範囲に周知徹底させなければならない。

### (2) リース又はレンタルしているハードウェアの返却時

統括情報セキュリティ責任者は、リース又はレンタルしているハードウェアの返却時に、当該ハードウェアに導入されているソフトウェアが確実に削除される手順を定め、対象範囲に周知徹底させなければならない。

## 8. ライセンス情報の入手

統括情報セキュリティ責任者は、現在の管理手順が適切であるかどうかを確認するために、標準ソフトウェアの使用許諾条件に関し、年1回定期的に、ソフトウェアメーカーから最新情報を入手する仕組みを構築し、維持しなければならない。

## 9. 研修

統括情報セキュリティ責任者は、全ての職員等に対して、ソフトウェア資産の管理を促進することを目的とした研修を実施する仕組みを構築し、維持しなければならない。

## 10. 棚卸

### (1) 棚卸手順の策定

統括情報セキュリティ責任者は、対象資産に対する棚卸の手順を策定し、周知徹底させなければならない。

### (2) 棚卸の実施回数

棚卸は定期的実施し、その実施回数は、次の通りとしなければならない。

#### ① ハードウェアの棚卸

6か月に1回以上実施しなければならない。

#### ② 導入の許可を得たソフトウェアと実際に導入しているソフトウェアの棚卸

四半期に1回以上実施しなければならない。

#### ③ ライセンス媒体の棚卸

年1回以上実施しなければならない。

#### ④ 保有ライセンス数と利用ソフトウェア数の棚卸

四半期に1回以上実施しなければならない。

### (3) 棚卸結果の報告及び是正措置

統括情報セキュリティ責任者は、棚卸結果をとりまとめ、明らかになった課題の是正措置及び再発防止策を記載した「棚卸結果報告書」を策定し、最高情報統括責任者へ報告しなければならない。また是正措置の実施状況をモニタリングし、定期的に報告しなければならない。

#### (4) 保管

統括情報セキュリティ責任者は、棚卸に係る文書、棚卸結果及びその記録等を適切な期間保管する手順を策定し、周知徹底させなければならない。

### 1 1. 監査

#### (1) 監査の実施

監査責任者は、対象範囲内のソフトウェア資産管理に関する内部監査を年1回以上実施する仕組みを構築し、維持しなければならない。また、2年に1回以上は、外部監査を利用した、対象範囲のソフトウェア資産管理の状態に対する成熟度評価を行わなければならない。

#### (2) 監査結果の報告及び是正措置

監査責任者は、監査結果をとりまとめ、最高情報統括責任者に報告しなければならない。監査責任者は、最高情報統括責任者への監査報告後、統括情報セキュリティ責任者に対し、明らかになった課題の是正措置及び再発防止策の策定を指示し、是正措置の実施状況をモニタリングの上、その結果を最高情報統括責任者へ報告しなければならない。

### 1 2. ライセンスコンプライアンスの遵守

棚卸や監査に限らず、保有ライセンスと利用ソフトウェアに関し、管理記録等と実際の状態との差分が発見された場合には、統括情報セキュリティ責任者は、その原因を調査し、適切な処理及び再発防止策を立案した上で、最高情報統括責任者の承認を受け、速やかに是正しなければならない。

この差分を発見した職員等は、直ち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。

### 1 3. ソフトウェア資産管理年度計画の策定

#### (1) ソフトウェア資産管理年度計画（以下「年度計画」という）の策定

統括情報セキュリティ責任者は、ソフトウェア資産管理の管理・監査・改善の実施方法・活動予定などを定めた年度計画を年1回、策定しなければならない。

#### (2) 年度計画の承認

統括情報セキュリティ責任者は、策定した年度計画を最高情報統括責任者に回付し、承認を得なければならない。

#### (3) 年度計画の進捗管理

統括情報セキュリティ責任者は、年度計画の進捗状況を把握し、その結果を最高情報統括責任者に四半期に一回、報告しなければならない。計画通りに進捗していない場合には、統括情報セキュリティ責任者は、その原因を究明し、解決策を策定しなければならない。

### 1 4. ソフトウェア資産管理の適合性検証

統括情報セキュリティ責任者は、本文書及びこれに基づく文書で規定するソフトウェア資産管理に関して定められている事項が、本文書“1 7. 参照資料(1)準拠、参照する基準等”に整合し、適切に実施されているかについて、年1回定期的に検証し、その結果を最高情報統括責任者に報告しなければならない。

### 1 5. 本文書の見直し

#### (1) 見直し

本文書は、本文書“1 7. 参照資料”記載の準拠、参照する基準等に整合しない場合、最高情報統括責任者は、本文書の見直しを統括情報セキュリティ責任者に指示しなければならない。

#### (2) 定めのない事項について

本文書及び【ソフトウェア資産管理対策手順書】に定めのない事項については、著作権法及びその他の法令並びに、各ソフトウェアの使用許諾契約に従わなければならない。

### (3) 優先事項

著作権法その他関連する法令及び使用許諾契約の記載内容（以下「法的要求事項」という）が、本文書の記載事項と異なる場合には、法的要求事項が本文書に優先し、本文書に定める手続きに従って本文書は速やかに修正されなければならない。

## 16. 違反への対応

本文書及びこれに基づく文書に違反した場合の対応については、別途定める【罰則基準】に拠る。

## 17. 参照資料

### (1) 準拠、参照する基準等

- ① ○○市情報セキュリティ対策基準
- ② ○○市情報セキュリティポリシー
- ③ 公文書管理規程
- ④ 監査・自己点検実施基準
- ⑤ パソコン等取扱規程
- ⑥ 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）
- ⑦ ISO/IEC19770-1