政府 CIO 補佐官等ディスカッションペーパー
2021 年 5 月

政府情報システムに係る

IT 資産管理の必要性について

2021 年 ５月

高橋邦明[1]、 金井孝三[2]、篠田仁太郎[2]、島田篤[2]、田中寿一[2]、田村仁一[2]、
伊藤豪一[1]、 坂本俊輔[1]

要 旨

IT 資産を適切に管理することで、「いつ、いかなる IT 投資をするべきか」、「情報システムの合理化や投資効率の向上をどうすべきか」といった施策を戦略的に推進することが可能となるだけでなく、「セキュリティの強化をどうするのか」について見極めることも容易となる。

これまで、政府においては IT 資産管理に係る各種施策に取り組んできたところであるが、更なる改善と昨今の情報システムを取り巻く環境の変化に対応することが必要となってきている。

本書では、IT 資産等管理の必要性と政府情報システムにおける IT 資産管理に係る課題とその対応策について取りまとめたものである。

本書は、政府 CIO 補佐官等の有識者による検討内容を取りまとめたもので、論点整理、意見・市場動向の情報収集を通じて、オープンで活発な議論を喚起し、結果として議論の練度の向上を目的としています。そのため、ディスカッションペーパーの内容や意見は、掲載時期の検討内容であり、執筆者個人に属しており、内閣官房　情報通信技術（IT）総合戦略室、政府の公式見解を示すものではありません。

---

[1] 政府 CIO 補佐官
[2] 一般社団法人 IT 資産管理評価認定協会

目 次

１　はじめに

１．１　背景と目的

IT 資産を適切に管理することで、「いつ、いかなる IT 投資をするべきか」、「情報システムの合理化や投資効率の向上をどうすべきか」といった施策を戦略的に推進することが可能となるだけでなく、「セキュリティの強化をどうするのか」について見極めることも容易となる。一方で、従来のように年度末における納品物により IT 資産の状況を把握するなどの方法では、投資管理や予算管理のサイクルと整合がとれないという課題がある。

また、政府情報システムは、従来の閉域網内でのオンプレミス型の情報システムからクラウドサービスを用いたオープンなネットワーク環境に移行するよう方向づけられている。さらに情報システムの開発・運用手法もウォーターフォールによるものから、DevSecOps などの継続的改善を行うプロセスに変更するものも出てきている。継続的に改善する情報システムは年度内においても構成情報が変化することや、機能単位でクラウドサービスを契約することがあるため、従前より行われていた IT 資産管理では管理対象や管理プロセスが追随できなくなろうとしている。

本書は、政府情報システムにおける IT 資産管理の必要性とその概要について具体化するとともに、政府情報システムに係る IT 資産管理の課題について明らかにし、その改善の方向性について提言するものである。

１．２　適用対象

本方針の適用対象は、「デジタル・ガバメント推進標準ガイドライン」（平成 31 年２月 25 日各府省情報化統括責任者（CIO）連絡会議（以下「CIO 連絡会議」という。）決定、令和２年３月 30 日に改定版の CIO 連絡会議決定。以下、「標準ガイドライン」という。）が適用される政府情報システムの整備及び管理に関する事項に適用するものとする。ただし、「標準ガイドライン第１編第３章１．適用対象」の規定に基づき適用対象外とされた事項については本方針の全部を適用対象外とする。

また、標準ガイドラインの対象外となる各種 IT サービスを活用した行政サービス、利用者により機能開発が行われる RPA（Robotic Process Automation）なども適用を想定するものとする。

2　IT資産管理の概要

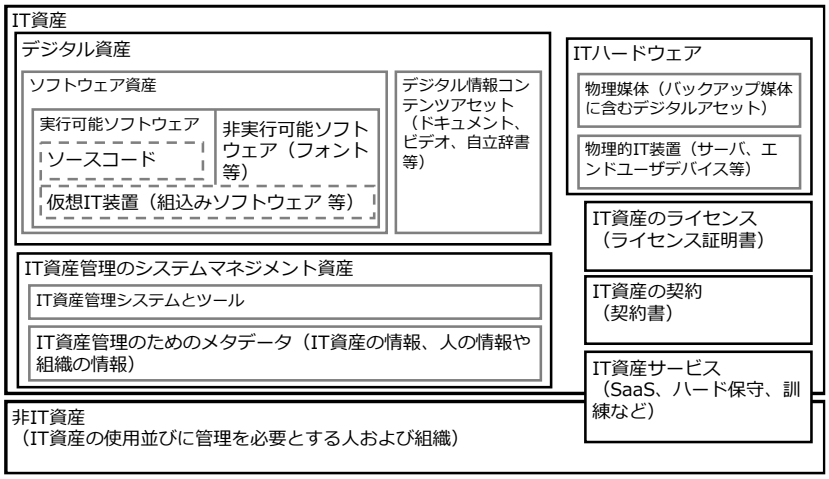
2.1 IT 資産管理の目的と概要

IT 資産管理（JIS　x0164、ISO/IEC　19770 においては「IT アセットマネジメント」）は、IT 資産のライフサイクル、総コスト及びそれらを包含するインフラストラクチャを管理することを目的とした資産管理の一分野として位置付けられている。また、IT 環境のライフサイクル管理及び戦略的意思決定をサポートするために不可欠であるともされている。

政府情報システムに関しては、標準ガイドライン「第２編　ＩＴガバナンス第２章 組織体制　f） 情報資産管理」にて、ＰＭＯは、府省内において、政府情報システムに係る情報資産の状態及び所在を明らかにし、迅速な課題対応等が可能となるよう、主に会計担当部門及び情報セキュリティ担当部門と連携・協力することで、政府情報システムにおける基本情報、情報システム責任者等、システム構成、取扱情報等の情報資産の定期的な棚卸等の管理及びその手順化、情報資産の再利用に関する総合調整及びその手順化を行うこととされている。また、そのために情報システム台帳を整備することとされている。

2.2 IT 資産管理の対象

JIS X 0164-1:2019 において、IT 資産管理の対象は、大きくは IT 資産と非 IT 資産に分類されており、IT 資産の中には、デジタル資産、IT 資産管理のマネジメント資産、IT ハードウェア、IT 資産のライセンス、IT 資産の契約、IT 資産サービスに分類されている。



JIS X 0164-1:2019 より引用し一般社団法人 IT 資産管理評価認定協会作成

図 2.1 IT 資産管理の対象資産

政府情報システムにおける IT 資産は、「サービス・業務の運営に不可欠な電磁的に記録された文書（公文書等）、音楽や映像、書籍等のコンテンツ及びそれらを構成するデータや、システムを構成する IT 環境（サーバやクラウドサービス等）、ソフトウェアや媒体（DVD や USB メモリ等）、それらに関連するライセンスや契約を指す。」とされているところである。IT 資産は、情報資産管理標準シートを用いて、契約額内訳、開発規模、個別開発規模、システム方式、取扱情報、セキュリティ、ハードウェア、ソフトウェア、回線、外部サービス、施設・区域、使用ドメイン、評価指標（目標）、評価指標（実績）、リスク管理表、課題管理表、障害報告を管理することとしている。

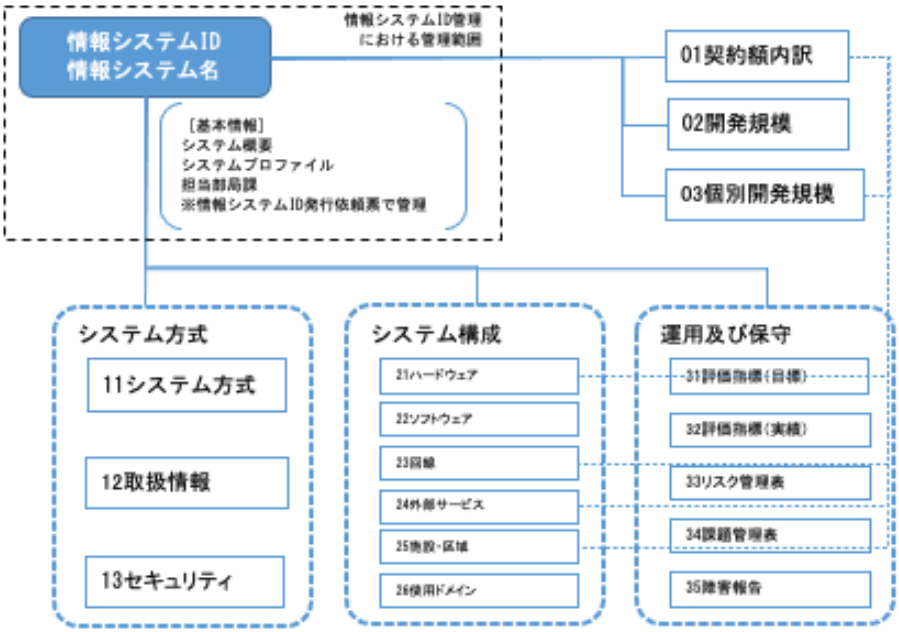


図 2.2 情報資産管理標準シートの全体像

２．３ IT 資産管理のプロセス

IT 資産管理を行うためのプロセスとして、JIS X 0164-1:2019 では、IT 資産の機能に着目した機能的マネジメントプロセスと、ライフサイクルに沿ったライフサイクルマネジメントプロセスが規定されている。

IT 資産管理の機能的マネジメントプロセスは、計画の変更を管理し意図しない変更によって生じた結果をレビューし対応する「変更マネジメント」、IT 資産のデータがライフサイクルに沿って正確に記録される「データマネジメント」、権利に関連すること等がライフサイクルに沿って正確に記録される「ライセンスマネジメント」、IT 資産管理活動で効果的にセキュリティを管理する

「セキュリティマネジメント」、ステイクホルダーを管理し適用範囲内の IT 資産及びサービスの全ての契約を管理する「関係及び契約マネジメント」、IT 資産に関連する費用や価値を監視し、費用対効果を管理する「財務マネジメント」、IT 資産管理に関連するサービスの本質的なレベルの定義、記録、管理を行う「サービスレベルマネジメント」、機能的マネジメントプロセス領域でカバーできないと認識されたリスクを管理する「他のリスクマネジメント」にて構成される。

JIS X 164-1:2019 より抜粋

図 2.3 IT アセット機能的マネジメントプロセス

IT 資産管理のライフサイクルマネジメントプロセスは、IT 資産管理の機能的マネジメントプロセス領域における「変更マネジメント」、「データマネジメント」、「ライセンスマネジメント」、「セキュリティマネジメント」に加え、適用範囲の IT 資産に対して要求事項を適切に要求しデザイン等を行う「仕様」、管理された方法及び適切な記録で取得する「調達」、IT 資産管理の要求事項を満たす方法で開発する「開発」、IT 資産管理の要求事項を支援するように計画・実行する「リリース」、IT 資産を配布及び再展開する「展開」、IT 資産を利用する運用プロセスが IT 資産管理の要求事項に従って実施されるようにする「運用」、現在の使用方針及び全ての記録保持要件に合ったところで再利用やリサイクル及び廃棄を決め、削除する「廃棄」にて構成される。

JIS X 164-1:2019 より抜粋

図 2.4 IT アセットライフサイクルマネジメントプロセス

政府情報システムにおける IT 資産管理のプロセスは、ライフサイクルマネジメントプロセスに沿っており、以下のプロセスにおいて IT 資産管理の業務が行われている。

○予算要求

積算の内訳や IT 資産の対象範囲の明確化を行うとともに目標指標についても具体化している。

○サービス・業務企画

各種指標の状況の把握や情報資産の特定及び分析を行うとしている。

○要件定義

情報システムに求める機能や性能、拡張性などの非機能について具体化することとされている。

○調達

情報資産管理標準シートの提出を求めることとしており、開発や展開、運用において必要な情報を取得することとされている。

○設計・開発

情報システムの構成や管理手法について明らかにするとともに、これらの運用や保守について設計を行うこととしている。

○サービス・業務の運営と改善並びに運用及び保守

情報システムによる効果について把握、評価を行うこととしている。またシステム構成管理を行うだけでなく、毎年度情報システムの現況確認を行うこととされている。

○廃棄

プロジェクトの終結において、情報システムを廃止又は更改する際、当該情報システムを構成するハードウェア、ソフトウェア製品等の利用を停止し、情報セキュリティ等の観点を踏まえ、廃棄又は再利用に取り組むものとされている。

3 IT資産管理の必要性

3．1 概論

標準ガイドラインにおいて、情報システムは単なる事務処理における道具ではなく、ビジネスプロセスの中核を成す基盤とされている。またビジネスモデルや社会構造を変革する強力なツールとなっているとの認識が示されているところである。そのため、情報システムに係る投資判断を適切に行うためにも、情報システムを構成する IT 資産について適切に管理を行う必要があり、以下の点について理解が必要である。

3．2 予算管理上の必要性

IT 資産はイニシャルコストだけでなくランニングコストも必要となるものである。そのため予算上効率の悪い IT 資産を導入することにより業務上の効果はあっても予算が硬直化する、組織の柔軟性が低下する、想定外のランニングコストが発生するなどの課題を抱えることがある。

情報システムにより達成される政策目標や効果に見合ったコスト管理を行うためには、情報システムを構成する IT 資産のコスト構造を適切に把握し、ライフサイクルを通じた管理を行うことが有効である。特に EOL (End of Life)を迎えたソフトウェアや機器等は特別な保守が必要となる場合もあり、ランニングコストが割高になることがある。

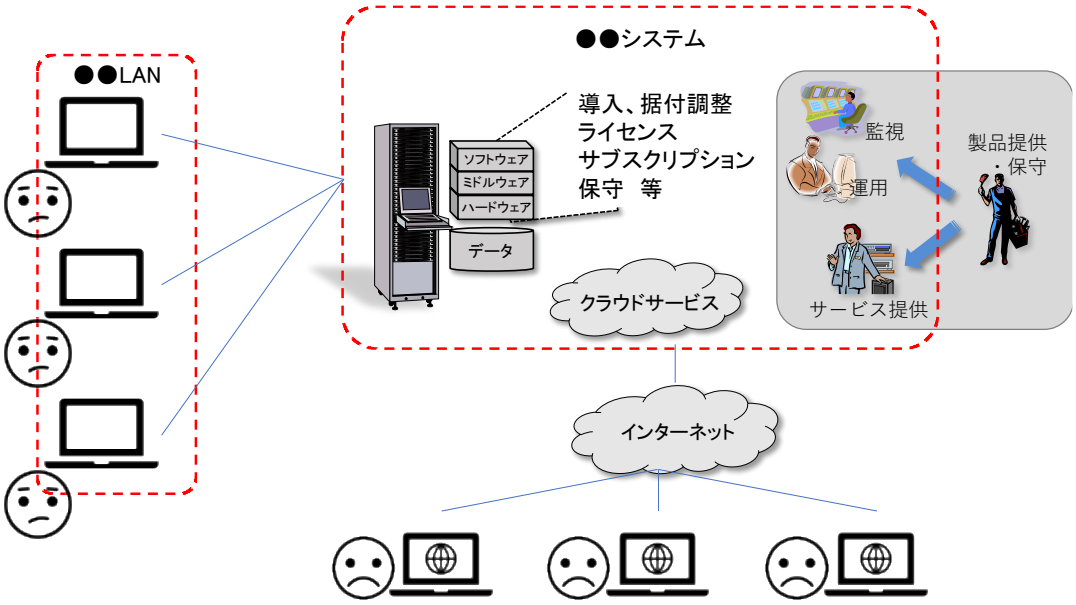


図 3.1 情報システムを構成する IT 資産

また、機器やネットワークの共用化や仮想化によって単一の情報システムやサービスに留まらずに共通サービスとして活用可能な IT 資産の導入も増えてきているところである。

これらを踏まえ、情報システムを構成する IT 資産の導入時期や契約期間などについて、適切な予算管理を行うために、以下の観点から IT 資産管理が必要であると言える。

（1）中長期における予算管理の最適化

機器やサービスの契約期間等を適切に計画し管理することで、いつ機器等の更改が発生するかを把握することが可能となり、限られた予算枠と組織内の様々なシステムの更改に係る投資時期について整合性を確保することが可能となる。

また、情報システム単位で投資判断をしていては、一つの投資の粒度が大きく、予算の振り分けが困難になるため、情報システムを構成する IT 資産に分解し、細かい粒度でライフサイクルを管理することにより、必要なもののみを更改して、経費を効率化するとともに、中長期の予算を平準化することが可能となる。

（2）整備及び更改に係る一次経費の最適化

情報システムを構成する IT 資産においてもそれぞれでライフサイクルが異なるものである。そのため、特定の IT 資産のリース期間や更改時期に応じて全ての IT 資産を一括更改するのではなく、個別の IT 資産の単位でライフサイクルを管理することで、長期に利用可能なものとそうでないものとを精査することが可能となる。

情報システムの整備や更改に必要な IT 資産の範囲を精査し、ハードウェア及びソフトウェアに係る経費の変動を的確に把握することで、整備や更改のために必要な IT 資産への投資を最適化することが可能となる。

（3）冗長構成に伴うコストの最適化

行政サービスの可用性を確保するため、機器やデータセンター等について冗長構成をとることがある。この冗長構成はホットスタンバイ、コールドスタンバイなどの用語があるが、製品を提供する事業者により定義が異なるとともに、課金体系についても区々である。

また、冗長構成をとることで保守作業の対象範囲も広がることから、冗長構成に必要な機器やソフトウェアの構成だけでなく、状態や必要なライセンス及び保守作業についても把握し、管理することが必要である。

（4）機器及びサービス等に係るライフサイクルコストの最適化

情報システム等を構成する機器及びサービスなどの IT 資産について、CPU、メモリ、ストレージ、有線 LAN、無線 LAN 及び WAN 帯域、アカウント

数などの利用状況を把握することにより、運用中の情報システムにおける不要な IT 資産を把握し、場合によってはライフサイクル中においても運用経費を削減することができる。

また、CPU のコア数やアクセス数などによってライセンス料が変化する場合や、利用期間中のライセンス体系に変化が生じる可能性があることにも留意が必要となる。

さらに、クラウドサービスを利用している場合には、不要なリソースやアカウントを削除することで、現状の運用経費を削減することも可能である。

（5）開発したプログラム等の再利用による開発規模の効率化

すでに導入された機器等以外にも、情報システムを構成するプログラムやライブラリ、コンテナ、ソフトウェアライセンス等についても再利用することが可能である。

プログラムやライブラリ、コンテナなどの設計情報は、業務やサービスに係るインプット、プロセス、アウトプットについて具体化されており、加えてデータの項目定義やステイタスなども明確になっている。作成されたプログラム等についても設計に基づいたテスト等がなされており、動作や品質が保証されているものである。

設計書等の IT 資産を活用することで、開発期間の短縮や工数を効率化することが可能となる。また、そのために調達したライセンスは、他の開発やシステムで利用できる可能性もある。

上記の観点を踏まえ、情報システムのライフサイクルを通じて、機能追加や設定変更が行われる際には、設計書の修正等が確実に行われることも必要である。

（6）機器等の廃棄に係る経費の効率化

情報システムを廃止又は更改する際だけでなく、保守作業に伴う機器交換においても、機器の撤去に加えデータ消去の作業等が必要となる。これらの作業について期間と工数を適切に見積もり、スケジュールや予算に反映することで、無理なく効率的な実施が可能となる。また、廃止、更改対象となるハードウェアやライセンスの適切な把握によって、流用可能な IT 資産を把握し、一律に廃棄・撤去・返却することなく、新規調達のコストを抑制することも可能となる。そのために、あらかじめ機器等の廃棄の時期を明らかにしていくことが必要である。

３．３ 適切な会計経理の実施上の必要性

情報システムの整備及び管理において、機器やサービス等の調達を行うことが多く発生する。契約相手方により適切に債務が履行されていることを確認するためにも、以下のような観点で IT 資産管理を行うことが必要となる。

（１）契約事務における監督職員の職務上の必要性

情報システムやサービスにおける開発や運用及び保守について、要件定義書や仕様書を作成し、事業者と契約を行うところである。

契約事務取扱規則では、監督職員の一般的職務として仕様書及び設計書に基づき当該契約の履行に必要な細部設計図、原寸図等を作成し、又は契約の相手方が作成したこれらの書類を審査して承認をしなければならない、とされている。

情報システムの開発やサービスの導入においては、適正な履行を確保するために必要な監督をすることから、過不足なく設計や機器等の導入がなされているかを確認することが必要である。この確認を行うためには、機器やサービス等の稼働状況や活用状況についても把握することが必要である。

このように、監督職員として契約の適正な履行を監督するために、利用する機器やサービスの構成情報だけなく、性能やライセンス数、アカウント数などの IT 資産の状況について契約内容との整合性を確認するとともに、設計書や設定内容の適宜の反映、予実管理などが必要である。

（２）契約事務における検査職員の職務上の必要性

会計法において、契約担当官等は契約についてその受ける給付の完了の確認をするために必要な検査をしなければならないとされている。検査は、契約書、仕様書及び設計書その他の関係書類に基づき、かつ、必要に応じ当該契約に係る監督職員の立会いを求め、当該給付の内容について検査を行なわなければならない、とされているところである。

適切な検査を行うためには、導入時や運用期間における設計情報と実際の稼働状況についての整合性チェックや過不足チェックが必要である。

情報システムの開発やサービスの導入時においては、業務やサービスの提供に必要な機能及び性能を満たすライセンス数やアカウント数が充足しているかについて、検査の観点から確認が必要である。

情報システムやサービスの運用及び保守においては、適切な性能等を満たしているか確認することが必要である。

このように、検査職員として、受ける給付の完了を確認するためには、機能、性能、ライセンスやアカウントなどの確認に必要な情報として設計

情報や稼働状況などの IT 資産について把握及びチェックすることが必要である。

（3）予算執行職員の義務及び責任に関わる必要性

予算執行職員等の責任に関する法律において、予算執行職員は、故意又は重大な過失に因り前項の規定に違反して支出等の行為をしたことにより国に損害を与えたときは、弁償の責に任じなければならない、とされている。加えて、会計検査院は、検査又は検定の結果、予算執行職員が故意又は過失に因り予算執行職員等の責任に関する法律第三条第一項の規定に違反して支出等の行為をしたことにより国に損害を与えたと認めるとき、又は国に損害を与えないが故意又は重大な過失に因り同項の規定に違反して支出等の行為をしたと認めるときは、当該職員の任命権者に対し、当該職員の懲戒処分を要求することができる、とされている。

このような中で、過剰な IT 資産を保有し是正措置を行わず、その職責を全うできてないと指摘されることのないよう、IT 資産の把握や管理が適時適切に行われていることが必要である。

３．４情報セキュリティ上の必要性

情報システムは業務や行政サービスの提供を行うために必要な基盤であることから、可用性、機密性、完全性に係るセキュリティについて考慮することが必要である。

セキュリティ対策が不十分なことにより、サービスの停止、重要な情報の漏えいやデータの破壊などが発生し、不便や不利益の生起だけでなく、行政サービスに対する信頼を損なう事態が発生することがある。

セキュリティ対策を適切に施すために、以下のような可用性、機密性、完全性を確保するためにも IT 資産管理について考慮することが必要である。

（1）可用性

○　情報システムの安定稼働

情報システムの利用率が向上するなどしてリソース等が逼迫することによりサービスの遅延や停止が発生することがある。

このような事態を防止するために、利用状況、トランザクション量やリソースの稼働状況などについて把握し、適切なリソース配分を行うことでサービス停止等を回避することが可能となる。

また、可用性を高めるための障害対策として、冗長化（High Availability）構成をとるのが一般的であり、クラウドを利用する場合でもマルチAZ(Multi Availability Zone)、マルチリージョン（multi region）などの対応が検討され、高負荷時における可用性対策として

はアップスケーリング（upscaling）によって対応されることもある。しかしながら、保守作業に伴う機器の入れ替えやサービスのアップデートなどによって設定等が変更されることで、設計当初に想定していた障害時の切り替えが機能せず、サービス停止を招くことがある。そのような事態を防止するため、設計当時の状況だけでなく、設定やマニュアルの継続的な確認が必要である。

なお、リソース等に係る IT 資産管理を運用事業者等に一任する例もあるが、発注者の管理責任や情報システムの運用管理責任者、契約事務に係る職員としての責務を免れることはないことから、運用管理を担当する職員においても当該システムの IT 資産の状況について把握及び管理することは必要である。

さらに、EOL を迎えた機器を利用することにより、障害発生時に適切な保守を受けられないなど、可用性を担保できない恐れもあることから、各機器におけるライフサイクルを把握し、管理することは必要である。

○　情報システムの外部連携における安定性の確保

政府において、開発工数の削減、UX の向上、機能の効率化などの観点から情報システム間のデータ流通や機能の共有を行うようになってきている。一方で、情報システム連携は機能やデータを外部の情報システムに依存することから、外部情報システムの可用性に影響を受けることとなる。さらに、連携先の都合で API の仕様変更がなされることもあるため、利用する API について機能や仕様について把握、管理することが必要である。

○　利用者稼働環境への適時の対応

情報システム利用者のデバイスは多様化しており、OS と WEB ブラウザ、稼働環境などにそれぞれ複数のバージョンが存在してきている。そのため、行政サービスを提供する場合には、このような多様かつ複数バージョンの OS 等について把握し、当該サービスの対応方針を決定することが必要である。

そのためには、情報システムを構成するミドルウェア、サービス、機能などの IT 資産について、OS や WEB ブラウザへの対応状況について把握及び管理する必要がある。

（2）機密性

○ パッチ適用の網羅性の担保

OS やミドルウェアなどのソフトウェアの脆弱性は適宜のパッチ適用により、攻撃者による不正アクセス等を防止してきたところである。

パッチ適用に遅延や漏れがあれば、その箇所が攻撃の起点となることが想定される。

セキュリティ侵害の契機となるゼロデイ攻撃の被害を軽減するために、必要なパッチが配布されていること、必要な端末等に適用されていることを確認することが必要である。

○ EOL を迎えた機器の脆弱性

情報システムに用いる機器等は、製品毎に EOL(End Of Life) と呼ばれる保守サポート終了日が決められている。この終了日を超えて使用することはセキュリティパッチの適用が受けられず、サイバー攻撃などのセキュリティ対策上の脅威となる。フロアスイッチなどの従来はシンプルなものと考えられていた機器が、最近では管理用 Web サーバ機能が実装されるなどの機能が高度化していることもあるため、注意が必要である。

また、同じ契約期間中においてもメーカーや機種により EOL までの期間が異なるため、EOL を迎えた機器を利用し続けることによるリスクについても留意が必要である。

○ データの保管場所としての IT 資産の把握

外部の操作等により意図せず業務で作成されたデータが漏えい、改ざん及び消去されることは、業務上の損害に止まらず、行政サービスへの信用失墜を招きかねない。

一方で、データはサーバ上に保管されるだけでなく外部サービスに保存されている場合や、例えばテレワークに伴う BYOD からアクセスする際の認証情報など、外部から侵入しようとした際に手がかりとなる情報など、履歴などの形で様々な場所に保存されるようになってきている。今や情報システムに保管されるデータの所在場所はオンプレミス環境のデータベースやストレージに限らず、業務用の端末、タブレット、個人のスマートフォンや、クラウドサービスなど利用環境とともに多様化してきている。

情報漏えい等のリスク発生要因を適切に把握して対策を施すためにも、従来のサーバやストレージに限らずに、情報システムに関連する具体的な機器構成や設計情報、アクセス履歴などについても IT 資産として洗い出しを行い、リスク分析を行うことが必要である。

○ 好ましくないソフトウェアの稼働発見

マルウェアとは異なり、利用者によるウェブ閲覧などにより通常のソフトウェアのように振る舞いながらデバイスに取り込まれるアドウェアなどについて稼働を早期に発見するためには、定められた環境に

おいて許可されたソフトウェアが動作している平常状態を日頃から把握し、異常について検知することが必要である。

そのためには、誰が、どこで、どのような目的で、どのようなデバイスを利用しているか、定められたアクセス権限でどのようなソフトウェアやプロセスが稼働し、どの程度の IT リソースを使用しているかについて把握することが必要である。

○ 内部からの情報漏えいの発見

マルウェアやアドウェアだけでなく、内部の職員により正規の手続きによりデータにアクセスすることで、情報漏えいが起こることがある。

外部ストレージへのアクセスや大量データのメール添付など、通常と異なる操作について適切に把握することで内部不正を発見することが可能となる。そのため、通常とは異なる CPU やメモリの使用、大量のデータ送信などを検知できるよう IT 資産の管理項目を設定することが必要である。

なお、個人の操作ログを取得する際には同意を得るなどにも留意が必要である。

○ デバイスの廃棄処理

システムの利用に用いる機器等は、サーバ、PC、モバイルを問わず廃棄が必要となる。その際、それぞれのデバイスには、ソフトウェア及びサービスの設定、利用履歴、認証情報、業務上生成されたデータの履歴、データを生成するための基礎となる情報などが保管されている場合がある。

これらの情報がデバイスの廃棄に伴い漏えいすることは、セキュリティ上の問題となるだけでなく、組織への信頼を損なう事態に発展する恐れがある。

そのため、業務上のデータや認証情報がどの利用者や権限に従ってどの機器等に保管され、その機器等はどのような状態にあるかを適切に把握し、廃棄によるリスク度合いを適切に評価するとともに、リスクに応じた確実な破棄やデータ消去を行うことの担保と証跡等による実施状況の確認が必要である。

また、デバイスについては物理的な破壊等による破棄の確認が可能であるものの、当該デバイスが利用していたクラウドサービスのアカウントの削除、データの削除にも留意が必要である。

○ サプライチェーン・リスク対策

情報システムの開発や機器等の製造に係るサプライチェーンの国際

的な分業により、介在する全ての事業者を適切に管理することが困難になっており、情報セキュリティ管理が不適切な事業者がサプライチェーン上に存在することによる情報漏えい等が懸念されている。さらに、サプライチェーンの中には、自国との利益相反が存在する可能性がある他国の政府によって所有、指示又は補助を受けている事業者が存在していることが否定できないことから、そのような事業者による不正行為に起因した情報窃取等が懸念されている。

そのため、懸念のある機器、ソフトウェア、サービスの洗い出しや確認が行えるよう、情報システムに係る構成情報を記録し確認できることが必要である。

（3）完全性

○　機能、サービスの機能処理内容の把握

OS やミドルウェア、クラウドサービスなどのアップデート等により機能やセキュリティ対策の向上が行われるだけでなく、処理仕様について変更され、適切な処理を担保できずデータの不整合や業務上の誤謬が発生することがある。

そのため、OS やミドルウェア、クラウドサービスなどに係る設計・設定情報などの IT 資産について把握し、アップデート等に伴う機能変更の有無についても管理することが必要である。

○　データ品質の管理

利用者の UX 向上のためのワンスオンリーやデータの完全性確保のためにデータ連携が行われるようになった。また、政府の持つデータをオープンデータとして提供することで、事業者によるビジネスモデルの源泉となることもある。

情報システムの処理機能が適切なものであっても、入力されるデータの品質に問題がある場合は、出力される結果も不適切なものとなる。そのため、データ連携を行う情報システムやサービスは、データの発生源とその品質等について把握し、データ品質の低下に伴う影響度についても考慮する必要がある。

このことから、外部参照データ、自らが管理、更新等を行うデータ、外部へ提供するデータの種類や設計情報などについて把握及び管理するとともに、更新頻度や連携タイミングなどについても把握しておくことが必要である。

３．５ コンプライアンス上の必要性

ソフトウェアやサービス等は著作物であることから、これらに係る権利について、発注者及び提供者の間での合意が必要となる。著作物に係る各種権利等の保護の観点から IT 資産管理において以下の観点で考慮することが必要である。

（１）著作権法の遵守

著作権法（昭和 45 年法律第 48 号）において、プログラムやデータベースは保護の対象とされており、これらについて技術的保護手段の回避若しくは技術的利用制限手段の回避を行うことにより、複製物を公衆に譲渡し、若しくは貸与し、公衆への譲渡若しくは貸与の目的をもつて製造し、輸入し、若しくは所持し、若しくは公衆の使用に供し、又は当該プログラムを公衆送信し、若しくは送信可能化する行為は、著作権、出版権又は著作隣接権の侵害となるとされている。

著作権、出版権又は著作隣接権を侵害しているソフトウェアやサービスについて、国が不正使用などをすることにより権利を侵害するようなことはあってはならない。そのため、情報システムを構成するソフトウェア等について著作権侵害の有無を確認するとともに、委託先においても不正使用がなされていないか必要に応じて確認することが必要である。

また、ソフトウェアの著作権等について国が保有する場合においても、利用状況の把握など管理することが必要である。

（２）知的財産基本法の遵守

知的財産基本法（平成 14 年法律第 122 号）における知的財産とは、発明、考案、植物の新品種、意匠、著作物その他の人間の創造的活動により生み出されるものであり、国は、知的財産の創造、保護及び活用に関する施策を策定し、及び実施する責務を有するとされている。

このような責務を有する国において、権利の侵害を防止しているかを確認するため、情報システムにて用いるソフトウェアやサービスにて知的財産の帰属について明らかにするとともに、侵害の有無を確認することが必要である。

（３）産業技術力強化法に基づく事業者の競争力確保

産業技術力強化法（平成 12 年法律第 44 号）第 17 条に規定される日本版バイ・ドール制度に関する規定及び標準ガイドラインにおいて、国の業務に特化した汎用性のないもの及び継続的な機能改修が見込まれるものを除き、受注者側に知的財産権が帰属するものであることに留意することが必要であるとされている。

このことから、請負開発において製造されたプログラムについて、受託者に権利を帰属させうることとなっているため、調達時や納品後に国が安

易にソースコード等を開示することで、受託者の権利を侵害してしまう恐れもある。

産業技術力強化法の規定により、事業者の競争力の源泉として受注者に知的財産権が帰属するものの有無や範囲について明らかにするためにも、設計情報の詳細やソースコードについて管理することが必要である。

（4）使用許諾条件の遵守

ソフトウェアやサービスの利用にあたっては契約事項として、ソフトウェアの開発元とソフトウェアの使用や複製、譲渡などについて契約者に許可あるいは禁止される行為や条件、開発元による保証やサポート、責任の範囲、免責事項などが定められている。また、利用期間中に使用許諾が変更となる場合がある。

政府の情報システムで用いられる様々なソフトウェアやサービスについても使用許諾条件を満たすことが必要である。

利用するソフトウェアやサービスにおいて、使用許諾が適切に遵守されているかを確認するために、ソフトウェアやサービスの稼働環境、利用されるデバイスや利用者数など使用ライセンス数の確認に必要な情報を適切に把握することが必要である。

（5）約款の遵守

ソフトウェアのライセンスだけでなくクラウドサービスの利用においても、利用約款は定められており、利用者の同意なく事後的に変更されることがある。これに伴い、サービス内容が変更になるだけでなく、可用性などのサービスレベルの変更、ライセンス体系の変更による価格の変更、収集される情報の種類などの変更とそれに伴う行政サービスのプライバシーポリシーへの抵触などの影響が発生する。

所管する情報システムにおいても、どのような約款に基づいたサービスを用い、約款の変更とそれに伴う影響度を明らかにするために、これらの情報を管理していくことは必要である。

（6）オープンソースの取扱

オープンソースは、ソースコードについて「再頒布の自由」、「ソースコード」を含んで頒布されていること、「派生ソフトウェア」の頒布を許可すること、元となる「作者のソースコードの完全性」を確保すること、「個人やグループに対する差別の禁止」、「利用する分野に対する差別の禁止」、「ライセンスの分配」により追加的ライセンスに同意することを必要としない、「特定製品でのみ有効なライセンスの禁止」、「他のソフトウェアを制限するライセンスの禁止」、「ライセンスは技術中立的でなければな

らない」とされている[3]。

国の情報システムにおいてもオープンソースプログラムを用いることがあるが、納品時に権利の帰属を求める場合や、改変しても公開しない場合などは、オープンソースの概念に抵触するおそれがある。また、整備した情報システムにおいてオープンソースの著作権及び許諾条件を侵害することの無いよう、適切にオープンソースを用いているかの確認が必要である。また、納品されるソフトウェアのうち商用利用を禁止しているオープンソースソフトウェアが混在することによるライセンス違反や、利用中に使用許諾条件が変更となり利用を停止しなければいけなくなる場合もある。

加えて、オープンソースに係る脆弱性情報や機能改善に係る情報はコミュニティ内で共有されるため、利用者はコミュニティにおける議論の状況やバージョンアップ、セキュリティ対策に係る情報を収集するとともに、独自ビルド、テストなどが必要となる。

このようなオープンソースの特性から、オープンソースの利用時には、ソースコード単位での状況及び、使用許諾条件を把握し、独自に情報を収集しパッチの作成とビルド、テストなどの管理を行うことが必要である。

（7）遵守状況の適時の把握

従来のソフトウェア使用許諾は、パッケージの開封やインストール時点で許諾に同意となったところであるが、人事異動に伴うデバイスの移設によって契約で認められた場所以外に端末が移設される場合や、担当する業務のためにインストールされたソフトウェアを削除しないまま異動先までデバイスを移設してしまうことで、目的外利用の生起や組織内部における予期しない不正コピーと認定されてしまうことがある。また、サービスでは約款の変更などが変更されることで利用条件やセキュリティ設定の変更が生じることもある。

これらを防止し、遵守状況について適時の把握を行うためにソフトウェアやサービスの利用状況について適切に把握し管理することが必要である。

自らが使用するソフトウェア等の遵守状況の確認に加え、受託企業や第三者委託先により、不正コピーなどのコンプライアンス違反によるソフトウェア等を用いた行政サービスに係るソフトウェアや情報システムの開発や維持管理がなされることがないよう、契約時に求めるだけでなく、必要に応じて監査を行うなどの確認が必要である。

[3] オープンソースグループ
https://opensource.jp/osd/osd19/

4 IT資産管理における課題

4．1 概要

情報システムの稼働環境は、1960 年代から 70 年代は、汎用機（メインフレーム）が中心であり、1980 年代から 1990 年代はパソコンの普及を受け、クライアント/サーバ型の情報処理が主流となっていった。これらの時代において年度末の設計書や契約において IT 資産は把握されており、稼働後も大きな環境変化がないことから、古い情報を用いても問題は顕在化してこなかった。

2000 年代から 2010 年代にかけてはクラウドコンピューティングが普及しはじめてきたところである。クラウドサービスの適用を前提に設計されたクラウドネイティブと言われる情報システムにおいては、継続的にサービスをリリースできる CI/CD 環境、従来の OS・ミドルウェア等の実行環境なしにアプリケーションを動かすサーバレスアーキテクチャ、複数のクラウドサービス間においても移行可能なコンテナ技術、複数のクラウドサービスを横断的に活用するマルチクラウドなど、従来とは異なる情報システムの運用環境や構築技術が確立されている。また、クラウドサービスにおいては新たなサービスが次々と導入されるなど、基盤技術の変化が加速しており、これらを踏まえたシステム構築・整備が求められるようになっている。

加えてライセンスにおいても従来の永続ライセンス中心から非永続ライセンスへの変更やサブスクリプション契約なども増えてきており、それにあわせて使用許諾条件についても変更されてきている。

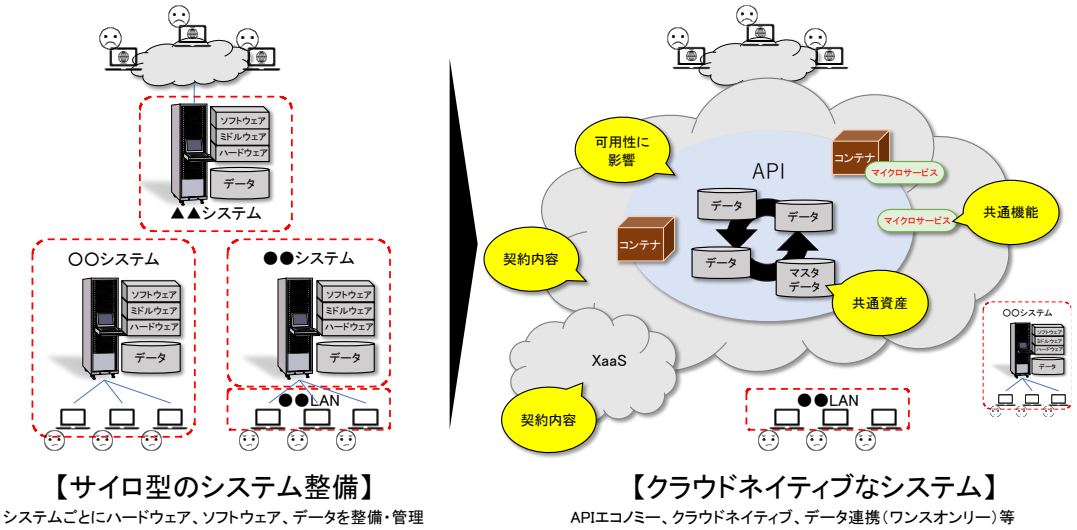


図 4.1 アーキテクチャの変化と IT 資産管理

そのため、従来の年度末に情報システム単位で IT 資産を把握するようなサイクルであっても不十分であったことに加えて、クラウドサービスを活用するにあたっては、機能単位や迅速な変化への対応が必要となってきている。

４．２ 組織面での課題

（１）IT 資産管理に係る組織

政府における IT ガバナンスは、内閣官房及び総務省による政府全体の IT ガバナンス、各府省の PMO による各府省 IT ガバナンスそして PJMO による IT マネジメントに区分される。

この組織の中で、IT 資産の管理は、PMO の機能として位置付けられ、政府情報システムに係る情報資産の状態及び所在を明らかにし、迅速な課題対応等が可能となるよう、主に会計担当部門及び情報セキュリティ担当部門と連携・協力することとされている[4]。

また、組織の在り方として、クラウドサービスの契約、ソフトウェアのサポート切れ、ライセンス管理、ハードウェアの仮想化や保守、データセンター等の調達などについて PMO が一元的に行うことと例示されている[5]。

一方で、例示されるような PMO にて一括契約等を行おうとした場合、各情報システムが必要とするハードウェアやソフトウェアライセンスについてプロビジョニング等を行うことが必要であるが、そのための計画作成や利用状況の把握等についてルールが定められておらず、各府省の PMO に実施の要否も含めて委ねられているところである。

加えて、各情報システムに係る IT 資産管理のための「情報資産管理標準シート」は情報システム ID がキーとなっていることから、共通的なリソースや契約を管理するためには、PMO 横断もしくは政府全体での取組が求められるところである。

（２）IT 資産管理に係るルール

標準ガイドラインにおいて、PMO は、府省内において、政府情報システムに係る情報資産の状態及び所在を明らかにし、迅速な課題対応等が可能となるよう、主に会計担当部門及び情報セキュリティ担当部門と連携・協力するとされている。

従来の IT 資産管理を行う組織は、特定の情報システムに紐付いて設置さ

4　標準ガイドライン　p16 「f）情報資産管理」
5　標準ガイドライン　p20 「表 ２-1　組織の在り方の例」

れており、サーバなどのコンピュータリソースやソフトウェアのライセンスなどはシステム部門により管理され、PC などのデバイスのリースについては契約に基づいて台数等を会計部門で管理することが行われてきた。一方で、端末内にリース契約には含まれないソフトウェアがインストールされることもしばしば発生している。

また、仮想化等によって情報システムの稼働環境の共用化により、基盤とアプリケーションによる運用主体が異なる場合や、府省共通システムなどのアプリケーションの共通化に伴う情報システムの運用主体と業務所管部門が異なるなど、一つの行政サービスを実現するためには複数の主体が関与することで、それぞれの主体間での責任分界が必要となっている。

さらに、クラウドサービスなどの約款によるサービスを導入することで、政府が整備や管理をしていない基盤を活用する業務を遂行する事例も出てきており、異なる PJMO 等の主体間で同じような機能やサービスを契約している場合や、ライセンス数の有効活用や相互融通に支障をきたす場合が生じることがある。加えて、個別の情報システムに紐づくことから、各ライセンス等も情報システムの構成要素になるため、「一式」や「等」の IT 資産として管理対象から外れる場合は、情報システム間を横串にした状況の把握も困難となっている。

４．３ 人的な課題

（１）IT 資産管理に係る教育訓練の不在

IT 資産管理の必要性において述べたように、IT 資産管理を行うためにはリソース管理、ライセンス管理、調達、契約、著作権管理、セキュリティなど多岐に渡る。

政府においては、「政府機関におけるセキュリティ・IT 人材育成総合強化方針」に基づき各府省において「セキュリティ・IT 人材確保・育成計画」を策定し、人材を育成してきているところである。

また、政府におけるセキュリティ・IT 人材の育成において中心的な教育は総務省における情報システム統一研修がある。

情報システム統一研修実施計画[6]に記載される各研修の科目において IT 資産管理に係る科目がなく、また調達管理や運用管理における研修内容に

[6] 政府機関におけるセキュリティ・IT 人材の育成・確保
https://www.e-gov.go.jp/digital-government/HRD/IT-human-resources.html

おいても IT 資産管理は見受けられない。

IT 資産管理の観点や業務について統一的かつ継続的な教育訓練がなされていないことから、各 PMO の個別の取組や PJMO における OJT に依存していることと想定される。さらに、このような状況では政府全体での IT 資産管理の必要性に係る認識の不統一や IT 資産管理に係る業務について個別対応を容認していることとなる。

また、IT リソースのプロビジョニング、ライセンス管理、セキュリティ対応を行うには、知識だけでなく、適時適切な意思決定も必要とされる。IT 資産管理に係る OJT だけでは意思決定に係るケースに偏りが生じる。また、網羅的なケースを習得できる訓練についても、現状は設けられていない。

（2）納品物たる「情報資産管理標準シート」の監督・検査

標準ガイドライン「別紙３　調達仕様書に盛り込むべき情報資産管理標準シートの提出に関する作業内容」の情報資産管理標準シートのうち、契約金額内訳は契約締結後速やかに提出し、開発規模、ハードウェア、ソフトウェア等については、設計・開発実施要領において定める時期、運用及び保守期間におけるハードウェア等の変更や運用及び保守に係る作業実績等について運用実施要領及び保守実施要領にて定める時期にて提出することとされている。

本記述は、仕様書にて記載することからも事業者により記載され、納品物として受領した職員により記載内容の網羅性や正確性について確認や検証されることが前提である。

事業者により納品される情報資産標準管理シートは、記載の粒度について明示されておらず、事業者が記載不要と判断することで記載から漏れている恐れもある。さらにソフトウェアについては、名称だけでなくビルドやバージョンにより機能等が異なるため、適用が必要となるパッチやライセンスも異なることがあるが、それらが管理できるだけの粒度での記載が漏れている恐れもある。

事業者により提出された「情報資産管理標準シート」について、監督職員や検査職員は承認や検収する責務を有しているものの、その基準や記載する範囲等が仕様書において明示できていないだけでなく、承認や検収の要領についても確立できていないことから、納品に係る確認等も十分に行われていない恐れがある。

４．４ 業務上の課題

（１）予算管理

標準ガイドライン「第３章予算要求」において、PJMO は、予算要求の対象の特定、資料の準備、経費の見積り、府省内での確認、内閣官房及び総務省での確認、プロジェクト計画書の段階的な改定を行うこととされている。

予算管理を適切に行うにあたり、これらのプロセスの中で、必要とされる機能や性能に対して、保有するハードウェア、ソフトウェア、ライセンス等と比較して精査を行い、必要なものについて予算を承認することが有効である。

現状では、情報システムごとに機能や工数等を積算し要求するため、PJMO や省内にある IT 資産の利用状況の精査や遊休 IT 資産の利活用の検討について、省内及び政府全体で予算要求段階の資料に添付することの義務付け等が行われていない。

また、安易な機器やソフトウェアの流用では、利用状況や稼働環境の変化によるライセンス違反が発生しかねないことから、予算要求段階においてライセンス体系やライセンスの種別について確認が必要となるものの、現状においては予算要求資料において IT 資産に係る情報を提示するようにはなっていない。

加えて、ソフトウェアを合同で調達することでボリュームディスカウントが発生することもある。そのような効果を享受するために、調達時期を合わせて基盤環境を集約する調整を予算要求段階ですることが求められるが、府省全体や政府全体での更改スケジュールやライセンス情報を一覧化した情報について予算要求時に精査するなどもされていない。

（２）調達及び契約管理

国による契約は、仕様書や設計書等に基づき予定価格を定め、その価格内において国にとって最も有利な者と契約を行っている。情報システムにおける調達においては、仕様書の他に要件定義書をつけて設計・開発や運用などの役務の範囲等について明らかにするところである。

標準ガイドラインにおける要件定義書記載内容である情報システム稼働環境として、クラウドサービスの構成、ハードウェアの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件等について記載する。なお、稼働環境については、既存の環境を最大限活用し、不要な調達を行わないこと、との記載がなされているところである。

仮に調達府省において利活用可能な IT 資産がある場合には、これを明示することで予定価格の算定も変化が生じるとともに、事業者による提案内

容や入札価格についても低減が見込まれるところである。

稼働環境として種類を列挙するだけでなく、稼働環境のライフサイクル、ライセンスの体系や種類、利活用にあたっての制約事項など応札事業者について参考となる情報についても提供することで入札価格の低減が見込まれる。

また、事業者による提案内容について、過剰な IT 資産を提案している場合などで精査を行うプロセスもなく、加えて総合評価落札方式においては、加点評価した要素についても契約に含めるよう会計検査院による検査報告[7]にて求められた事例もあることから、過剰な IT 資産等により運用経費が高止まることがないよう提案を評価する仕組みについても検討が必要である。

（３）IT 資産の把握

標準ガイドラインでは、ＰＭＯは、府省内において、政府情報システムに係る情報資産の状態及び所在を明らかにし、迅速な課題対応等が可能となるよう、主に会計担当部門及び情報セキュリティ担当部門と連携・協力して行うこととされている。そのために「情報資産管理標準シート」等を活用し、政府情報システムに関する基本情報、担当組織、システム構成、取扱情報等を掲載する情報システム台帳を整備し、適切に維持・管理することとなっている。

この「情報資産管理標準シート」は表計算ソフトのシートを用いて記述されることとなっており、納品物として事業者が記載する場合は、記載の粒度について事業者との個別の調整を行い、年度末や契約終了時に提出されることが想定される。

年度末は府省によってはすでに予算要求プロセスが始まっているだけでなく、次年度の事業者の調達も進んでいる。このため、年度末に納品される最新の IT 資産情報が有効活用されず、古い情報を用いてプロセスが進められる恐れがある。

予算要求や調達時点で新しい IT 資産の情報が得られないことで、契約時のリソースやアカウント数などについて適時に反映できないという課題も生じる。

また、情報資産管理標準シートは事業者によって記載される際に範囲や粒度がまちまちになる恐れを内包しており、加えて各情報システムによる

[7] 普通財産の管理及び処分に係る業務を委託するに当たり、総合評価落札方式により落札者を決定する際に加点評価した提案の内容を確実に契約に反映することにより、会計法の趣旨に沿って国にとって最も有利な内容で契約を締結することとなるよう改善させたもの
https://report.jbaudit.go.jp/org/h26/2014-h26-0141-0.htm

個票であるため、横串にて集計するには不向きなことや、入力から集計までに人手を介すことで多大な集計の工数が発生するだけでなく、誤謬が発生しやすいなどの課題がある。

（4）IT 資産管理に係る評価

IT 資産の年間における利用状況をモニタリング及び評価することで保有するハードウェア、アカウントなどを精査することが可能となる。

情報資産管理標準シートにおいては、保有数等については記載できるものの、利用状況の平均値やピーク値などについて記載するようになっていないことから、利活用状況についてモニタリングできていない。

そのため、情報システムの導入による効果についても、遊休資産などの無駄を内包したままで事務経費が算定されている恐れがある。

また、クラウドサービスを用いてプロビジョニング等を職員自らで行なっている PJMO と、コンピュータリソースを複数年度契約にて固定的に利用している PJMO とでは IT 資産管理に係る知見も大きく異なるものである。

IT 資産管理について、各府省 PMO にて情報システム台帳を整備し、適切に維持・管理することとされているものの、知見や成熟度が異なる PJMO について評価する仕組や、各府省 PMO による IT 資産管理について評価する仕組がなく、政府全体で IT 資産管理業務に係る属人化や個別最適を招きかねない状況となっている。

（5）リスク評価

標準ガイドラインにおいて、プロジェクトに係るリスクは、「プロジェクトの遂行を阻害する可能性のあるリスク」、「設計・開発における作業を阻害する可能性のあるリスク」、「運用における作業を阻害する可能性のあるリスク」及び「保守における作業を阻害する可能性のあるリスク」について記載されている。

IT 資産管理が適切にできていないことで、予算管理上のメリットを享受できないために、運用経費の高止まりによる情報システム関係経費の硬直化が生じる恐れが発生する場合や、過剰な開発規模による整備期間の長期化とそれに伴う効果の発現の遅延、運用経費の高止まりによる予算確保の困難などの理由によるプロジェクト環境を整えられないリスクが発生する恐れがある。

また、IT 資産を適切に管理できていないことにより、過剰な IT 資産を放置して不要な支払が生じる場合や、構造的に放置を容認するなどにより、適切な会計処理がなされていないことや、監督職員や検査職員の職責が適切に履行されていない、との指摘を受けるリスクも存在する。

さらに、利用環境や状況に応じたライセンスを取得している、あるいは

商用利用が許されていないオープンソースを利用していないなど、権利を侵害していないことについて的確に把握できる状態にないことによるリスクも内在している。加えて、著作権を国に帰属させているにもかかわらず、設計書やプログラムが利活用されないことで、同様な機能を複数調達し、莫大な工数や費用をかけて 1 から作り直している恐れもある。

４．５ ツール等の課題

（１）オフィスツールに依存した IT 資産管理

政府における IT 資産管理は、表計算ソフトの 17 のファイルに分かれた情報資産管理標準シートを用いて行われる。このシートへの記載は事業者による手入力等によって行われ、記載された情報資産管理標準シートはメールや電子記録媒体等で納品されたのち、職員の手によって台帳に登録されることになる。この入力内容の正確性や網羅性について検証されていないことが想定される。

仮に特定のソフトウェアで深刻な脆弱性が発見された場合には、各情報システムのそれぞれのシートについて検索をかけることにより該当箇所を特定することになっているものの、実際には各情報システムの膨大なシートやファイルから特定のソフトウェアを抽出することは多大な作業量が必要となるだけでなく、手入力による記載ミスにより、発見できない可能性もある。

また、利活用状況についてリアルタイムだけでなく、年間を通してのピーク値などの変移を見ることができないため、リソースの融通などについても大まかな調整しかできないのが現状である。

さらに、管理コンソールなどにより現状を把握できるものについて、シートへ転記しなければいけない作業が発生することや、個々の端末によってインストールされている環境やソフトが異なる場合などが生じても、手作業による入力に依存した台帳管理だけでは適時・適切な情報は把握できないなどの課題が生じる。

（２）IT 資産の実態把握

納品物である情報資産管理標準シートの納品や情報システム監査などを契機として IT 資産の実態を把握するには、契約書や設計書の記載内容、インベントリツールから取得された情報などが用いられる。この際、IT 資産管理の情報をインベントリツールから取得する場合でも、インベントリツール導入時に管理対象としたものしか情報は取得できないことが多く発生している。

また、クラウドサービスにて、オートスケーリングする場合にはサービス提供中においても適時にリソースの状況が変化する場合や、アカウントを要求に応じて発行する場合など、ライセンスも適時に変化する場合があることから、特定の時期を契機として IT 資産の棚卸をしていては、真の IT 資産に係る実態を把握できず、予算要求や調達において古い情報を元に判断せざるを得なくなってしまう。

４．６データの課題

（１）管理対象

IT 資産を把握するために、情報資産管理標準シートが用いられている。これらのシートはオンプレミス環境で稼働する情報システムを主に想定しているだけでなく、稼働状況等が変化することを想定してない。

一方で、政府においてはクラウドサービスの活用を推進していることやコンプライアンスの関係から、IT 資産毎の特性を考慮して、以下のようなものを管理項目として追加することが必要と考えられる。

●既存 IT 資産における利用状況：情報資産管理標準シートにおいては、調達時点に保有する IT 資産の情報についてしか把握できていない。IT リソースを共用する場合には、ピーク量や時期を把握することで遊休資産を他の情報システムにて活用することが可能となる。またこの把握の間隔は分単位、時間単位、日単位など、IT リソースのプロビジョニングに係る時間とも整合を取ることが必要である。一方で、IT 資産を柔軟に活用することで契約外での流用やライセンス違反の惹起などの恐れがあるため、併せて契約内容の確認も必要である、

●アカウント：SaaS の利用などにおいて、管理者アカウントと一般ユーザアカウントでは利用権限が異なるだけでなく、価格体系なども異なることがある。これらについて人事異動などに伴い管理が適切に行われていない場合、不必要な費用が発生するだけでなく、不要なアクセス権を付与してしまうことで不正アクセスや情報漏えいのおそれが生じる。

また、アカウント種別に応じた権限はクラウドサービス側のアップデートにより変更も生じることから、アカウント種別に応じた発行状況だけでなく、アカウントの権限の状況についても管理が必要である。

●約款（SLA 含む）：クラウドサービスは、サービスレベルやデータ消去、格納されるデータへのアクセスなどについて記載される約款に基づいてサービスが提供されている。約款はサービス提供者が不特定の者に

対して結ぶ契約事項であり、サービス提供者の都合で改訂されることもあることから、約款の記載事項と変更のタイミング、効力の発生時期なども管理することが必要である。

●セキュリティレポート：利用する基盤としてセキュリティ対応状況についても確認が必要である。そのためには関連する脆弱性情報や SOC レポートなどのセキュリティ対応状況についても継続的に把握することが必要である。

●ソースコード：ソースコードは、情報システムの機能を実現するためのプログラムを記述するものであり、開発・保守を行う際には必要となるものである。政府情報システムとして開発され納品された情報システムについてソースコードを把握することで、不正処理や非効率な処理などの内部ロジックについて検証を行うことや、ベンダーロックインの回避が可能となるものの、必ずしも納品物には位置付けられていないのが現状である。

また、政府情報システムのソースプログラムを公開する場合やオープンソースを活用する場合など、国民や民間事業者、コミュニティなどとソースコードを共有する場合がある。コミュニティの場などでソースコードに対して脆弱性やバグが発見された場合、対応が必要となることがある。公開されている関連したソースコードについてもモニタリングし、適切な対応がなされることが必要である。

●コンテナ：マルチクラウドサービス環境下において動作できるよう、コンテナ技術を用いて情報システムを構成することがある。コンテナ技術を用いる場合には、コンテナに係るソースだけでなく、ビルド方法やコンテナ用のライセンスの要否も含めて管理する必要がある。

●API：外部システムとの連携や情報システム内連携に API を用いることがある。その際に、OS やフレームワークのアップデートによって動作が変わることもあるとともに、外部システムの都合により仕様が変更されることもある。

API の仕様変更に伴い、担当する情報システムのサービス停止や機能変更なども生じることがあることから、関連する API の動作環境や稼働状況についても把握しておくことが必要である。あわせて、変更の影響度把握のために、API 相互の関連性などを表したサービスメッシュなどの全体像について把握することも必要である。

●外部データ：ワンスオンリーや API 連携により外部情報システムのデータの活用の増加が想定される。またベースレジストリなどのマスタデータを外部に依存することも想定される。そのため、外部システム

等の都合によりコードの意味やデータの桁数などの変更、データの更新履歴のポリシー変更などが生じた場合には、担当する情報システムのデータの持ち方や管理方法にも影響が生じる。これらに適切に対応するためにも、外部データの状況について把握し、適時に確認することが必要である。

国が提供しているオープンデータについても同様に、国民等にとっては外部データに当たることから、利用状況やデータの鮮度等について適切な管理を行うことが必要である。

●設計書・パラメータシート：納品物となっているものの、受入テストや検収において設計書どおりに情報システムが動作しているかの確認や、保守等による適宜の最新化がなされているかなどの管理がなされていない場合がある。保守作業によって生じた設計書の差分情報のみが納品されている場合などは情報システムの全体像が不明確になり、監督職員や検査職員に負担を強いることとなる。納品される設計書について監督業務、検査業務における活用方法や IT 資産における現況把握のための根拠となるよう、取扱要領について具体化が必要である。

また、設計情報を活用することでシステム更改や同様の機能に係る開発について費用や工数を削減することができることから、設計書を政府内で共有するなどの仕組みについても検討が必要である。

さらに、近年はソフトウェアパッケージやクラウドサービスの活用により、開発は伴わないものの、設定情報を活用することで効率化することが可能であることから、パラメータシート等の設定情報についても設計書と同様に活用する仕組づくりが必要である。

●BYOD：テレワーク等が進むことにより個人デバイスの業務利用の増加が想定される。その際に格納されるデータや認証情報などが漏えいすることにより不正アクセス等を招きかねない。一方で個人デバイスについて組織としてどこまで制限や管理すべきか、それに伴う動作保証や通信帯域の確保について具体化することが必要である。

●RPA やローコードツール等：近年の技術の進歩により、業務の利便性向上のために情報システムの整備とは別に、業務担当者等により RPA やローコードツールなどを用いて独自にサービスを構築することができるようになった。これらのツールの活用により、サービスやデータ処理は多様化することから、情報システムではないもののツール活用によって作成されたプロセスの管理も必要である。

●著作権：政府情報システムにおいては、発注者への著作権帰属や、著作者人格権を行使しないこととしているものの帰属された権利につい

て管理されていない。そのため、納品した事業者によって他機関等へ設計情報、プログラムの再利用などがなされた場合についても把握していないのが現状である。すでに国に帰属している著作権については、国の資産として有効活用することで、開発機能や工数を削減できることもあるため、設計情報やソースコードに係る権利の管理や活用策についても検討が必要である。

また、事業者に著作権がある場合や日本版バイドールにより事業者に権利行使を認めている場合において、設計情報やソースコードを公開しないことは事業者の権利を保護する上で必要なことである。

（2）データの信頼性

情報資産管理標準シートは事業者の手作業による入力である場合に、ライセンス証書とは異なるソフトウェア名称などが用いられることがある。また同じソフトウェア名称でも版数やビルドにより機能や構成が変わることがある。仮に保有する IT 資産について横串で確認しようとしても、表記揺れや版数の未記載に伴う集計漏れ等が発生し、全体像を掴めないなどの恐れがある。

また、表計算ソフトのファイルの版管理ができていないことにより、メール添付やフォルダ格納時に古いファイルと混在してしまうなどのヒューマンエラーも生起しかねない。

さらに、運用を自動化している場合など、情報資産管理標準シートを記載した時点と実際に運用されている OS やミドルウェア、サーバ数、メモリ数などが異なる場合がある。

加えて、情報資産管理標準シートに記載されている内容について、情報システムの担当職員が検証する仕組みがないため、記載事項について信頼性を担保することができていない恐れがある。

（3）データ利活用

調達時において保有する IT 資産を仕様書にて提示することで、応札者は活用できるライセンス等を知ることができ、提案する情報システムの構成等に反映し、入札価格や運用経費を削減することも可能となる。応札者にとって必要となる IT 資産に係る情報についても具体化することが必要である。

また、保有する IT 資産について各 PJMO により個別に更新がなされている。政府全体で情報を共有されることで、ボリュームディスカウントの機会が得られるにもかかわらず、予算の効率的な執行ができていないことも課題である。

４．７その他の課題

（１）財産としての管理

民間企業においては、取得した IT 資産について財産登録を行うことや、業務ノウハウの蓄積として管理しているところもある。政府においては情報システムや IT 資産について著作権の帰属や業務ノウハウ等が含まれていながら、財産として管理される対象とはなっていない。

そのため、業務ノウハウの継承や無形財産として省庁や部局間において設計情報やプログラムが役立てられていないだけでなく、業務フローやチェックロジックなどの業務の引継において活用可能なものであっても廃棄されている恐れがある。

（２）情報開示

過去の IT 資産に係る情報化基本調査、電子政府基本調査などにおいては、その調査結果が統計資料として共有されていたところである。また、政府の情報システムに係る状況については IT ダッシュボード[8]にて公表されているところである。

一方で、政府調達の透明性を重んじるあまり、運用している現行情報システムの構成情報を公開することによって、ゼロデイ攻撃の対象となりやすくなるリスクが内在することについても留意することが必要である。

保有する IT 資産の状況に係る統計分析や情報開示の方法について具体化を検討することが必要である。

（３）IT 資産管理業務に係る改善

政府情報システムのアーキテクチャはオンプレミスからクラウド・バイ・デフォルト、今後は Gov-Cloud の導入などさらなる変化が想定され、開発手法ではウォーターフォールからアジャイル開発、DevSecOps へと変化することが想定される。

政府における IT 資産管理業務は、行政情報化の進展に伴い調査や棚卸しをしてきたところである。

このような変化を踏まえ、継続的に IT 資産の対象やサイクルも変化できる仕組みが必要である。

（４）開発環境における IT 資産の管理

情報システムを開発する場合、開発事業者においても必要な OS やミドル

[8] IT ダッシュボード
https://www.itdashboard.go.jp/

ウェアを取得し、開発環境を整備しているところである。この開発環境について発注のなかで整備しているのであれば、発注した国にライセンスが帰属するなど納品物や契約面での調整が必要である。

またクラウドサービスを利用する場合においては、開発事業者がクラウドサービスの管理アカウントを持つことで、他の事業者による保守等の参入ができなくなるなどベンダーロックインを誘引することがある。そのため、開発終了時に管理アカウントを国に移管するなどの処置にも留意が必要である。

５ IT資産管理における課題への対策

５．１ 概要

政府においては、IT 資産管理への取組を行なってきたところであるが、より充実した IT 資産管理を行うための課題が明らかになったところである。これらの課題に対応するため、以下の方策について検討することが必要である。

５．２ 個別の課題への対応

（１）組織面での課題への対応

○ IT 資産管理に係る組織の確立

省庁横断で IT 資産管理を行うために、統括的組織が必要となるところである。一方で統括的な組織が細部まで管理することは管理工数が膨大となるだけでなく、業務の変化への柔軟かつ迅速な対応が難しくなるおそれがある。政府全体、各府省、各 PJMO などの管理階層に応じた役割と責任を明確にするとともに、職責に応じた権限を付与することにも留意が必要である。

○ IT 資産管理に係るルールの策定

それぞれの管理階層に応じて分化しつつも、効果的かつ効率的な IT 投資を行うために必要な IT 資産管理を行うには、IT 資産管理に係る目的の明確化、計画の策定、ルールの確立などが必要である。なお、ルールを確立するにあたっては、既に標準となっている JIS X 0164-1 などを基に政府としての管理の基準を持つことが必要である。

○ 「クラウド・バイ・デフォルト原則」への追随

「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（(平成 30 年６月７日 CIO 連絡会議決定、令和２年３月 30 日に改定版の CIO 連絡会議決定。）に記載された「クラウド・バイ・デフォルト原則」に沿って、政府の関係するすべての組織において、IT システムが大きく変化することが想定される。アーキテクチャや IT インフラの変更に伴って IT 資産管理についても常に変化が求められることから、継続的に管理方法やルールを適切に変化させることができるようにすることが必要である。

（２）人的な課題への対応

○ IT 資産管理に係る教育訓練の実施

IT 資産管理に係る組織を構成し、ルールを実現するための人の教育訓練が必要である。セキュリティ・IT 人材に必要な素養として情報システム統一研修においても IT 資産管理の科目を設けるとともに、調達

や運用の科目においても教育を行うことが必要である。

そのためには、役割に応じた IT 資産管理に必要な人物像を具体化し、職務や権限に応じたスキルを具体化することが必要である。これらに基づき、カリキュラムを作成することが必要である。

○ 納品物の監督・検査チェックシート、マニュアルの作成

監督職員及び検査職員に任命された職員は、必ずしも IT に知見のある職員とは限らない。一方で、IT 資産に係る監督及び検査を行う必要があり、職責を全うできていないことにより国に損失を与える恐れもある。そのために、まずは、IT 資産管理の観点から、納品物に求める要件について具体化を行ない、IT に知見のない職員においても IT 資産に係る監督・検査ができるようにチェックシートやマニュアル等を準備するとともに受託者に求める要件についても具体化することも必要である。

（3）業務上の課題への対応

○ 予算管理

合同調達を行うなどを計画するためには、予算要求の段階で保有する IT 資産について棚卸しがなされており、それぞれのライフサイクルに応じた更新時期を考慮した計画を立案することで効率的な予算編成が可能となる。

そのため、予算要求段階で IT 資産に係る中長期計画の策定を求め、その内容を元に予算査定を行うなどの予算要求プロセスを確立することが必要である。その際、予算査定を行う側においても IT 資産管理の観点から、チェックができるようにすることにも留意が必要である。

○ 調達及び契約管理

入札公告時に IT 資産の保有状況や活用状況について開示することで効果的な調達を行うことができる。そのために、仕様書等において記載すべき IT 資産の情報等について明確にすることが必要である。

また、IT 資産管理を効率的に行うためには、契約時や納品時に求める IT 資産に係る情報について具体化し、適切なインプット情報とすることが必要である。そのため、仕様書において契約時や検収時にて必要とする IT 資産に係る情報についても具体化することが必要である。その際、機器やライセンスの数に加え、利用目的や使用許諾条件などについても確認することに留意が必要である。

さらに、総合評価落札の提案書評価において過剰な IT 資産の提案を加点評価しないなどの抑制策についても検討が必要である。

○ IT 資産管理の業務

政府全体、府省単位、部局単位、情報システムの運用・管理を担任する課室等の異なる IT マネジメントの管理階層に応じて必要とされる情報は異なるものである。また、情報システムのライフサイクルや会計事務におけるプロセスにおいてもそれぞれで必要となる情報の粒度も異なる。

必要な情報が必要な時に得られない、もしくは鮮度の古い情報をもとに意思決定を行うことがないよう、情報集積のサイクルやプロセスについても整合が必要である。

そのためには、IT 資産管理に必要な情報の発生源にはどのようなものがあり、それらの情報をどのように集積して、各ステイクホルダーに応じたビューがどのようなものがあるかについてユースケースを踏まえた分析が必要である。

管理方法についても、台帳ベースで管理する場合とリアルタイムで収集する場合とで意思決定のプロセスや粒度も異なることがある。加えて情報システムの規模や基盤環境（オンプレミス、仮想環境、クラウドサービス等）や管理する組織の成熟度に応じても IT 資産管理に係る業務プロセスや管理の粒度が異なる。このような状況が混在する場合に、一律で IT 資産管理のプロセスを定めることは過剰な作業を発生させてしまう恐れや、従来の管理レベルより落とした業務を強要することで非効率が発生してしまうなどの弊害が発生する恐れがある。

そのため、ベースとなる IT 資産管理の項目を定めるとともに、成熟度等に応じた管理レベルを設けるなどの工夫が必要である。

○ IT 資産管理に係る評価

IT 資産が有効に活用されているかについて、ある特定の時期だけでなく年間の業務上の繁閑期や利用者の動向などとあわせて評価することが必要である。そのため、IT 資産について「いつ」、「いかなる視点」で評価をすることが必要かについて明確化が必要である。

また成熟度に応じた IT 資産管理を行う場合、省庁単位ではなく、PJMO 単位などで成熟度を評価するなどの仕組が必要である。

○ リスク評価

予算環境や会計経理、コンプライアンスなどに係るリスク発生を防止するために必要なインプットやプロセス、アウトプットについて整理し、プロジェクト計画やプロジェクト実施のモニタリング・コントロールに活かすことが必要である。

そのために、IT 資産を起因としたリスク要因について洗い出しを行うとともに、影響度や対応策についてのユースケースについて立案す

ることが必要である。

（4）ツール等の導入

現状の表計算ソフトウェアなどのオフィスツールに依存した IT 資産管理は、更新頻度が低下して実態が把握できなくなるだけでなく、手作業による入力が発生するために誤入力や漏れが発生するなどのデータ品質の低下を誘引し、記載内容の検証にも多大な作業量が必要となる。このような課題に対応するためインベントリツールや台帳ツールなどの IT 資産管理ソフトを利用することも有用であると考えられる。

しかしながら、IT 資産管理ソフトは種類が異なると取得できる情報や管理可能な項目は異なる。IT 資産管理の目的に照らし合わせ、必要なデータ項目を精査し、必要があれば追加のインターフェースや管理項目を設けることを検討する必要がある。

（5）データの課題への対応

〇管理対象の精査

IT 資産として現状では管理できていない項目について多数存在するところである。それらについて政府情報システムの動向等を踏まえ管理対象として取り組むことが必要である。

その際、管理対象を選定するにとどまらず、管理対象の情報をどのように収集し、手作業や台帳を用いずに自動化する手段などについても検討することが必要である。

〇データの信頼性の向上

手作業により入力された台帳をもって管理されている現状において、IT 資産に係るデータの品質が低下している恐れがある。

台帳に記載されているデータに関する検証要領やデータ品質の基準を設けるとともに、品質基準を満たしていないデータについて品質向上策を立案することも必要である。その際、点検や修正を手作業で行うことにより誤修正が発生するなどのリスクも生じることから、信頼性向上施策についても属人化の排除や必要な自動化などを考慮することが必要である。

〇データの利活用

政府内及び入札公告などにおいて保有する IT 資産について情報共有できることで、予算を効率化することが可能である。このための管理項目を具体化するとともに共有のための仕組や手順を構築することが必要である。

（6）その他の課題

政府として IT 資産を財産として管理する制度や業務、IT 資産に係る情

報開示の方法などについては、課題としての認知もされていないのが現状である。管理プロセスなどだけでなく、管理していないことのリスクや管理することにより生じる課題についても具体化が必要である。

また、各種課題を解消しつつ、今後の政府情報システムの整備や IT 資産の活用状況に応じた IT 資産管理業務に係る状況の把握や継続的な改善についても枠組みを構築することが必要である。

５．３ 政府情報システムに係る IT 資産管理の目的の確立

個別の課題に対して各個に対応することは可能であるものの、職員の作業量に係る制約や IT 資産管理のための環境の整備などの投資も必要となるところである。あわせて、IT 資産管理業務を適切に行うための人材育成には時間が必要となるところである。

政府として IT 資産管理を行うことの目的や期待する効果について具体化し、そのために必要な体制や業務、管理項目などについて明らかにすることが必要である。

一方で、その時々におけるトピックに従って IT 資産管理を行なっていては管理項目やプロセスの一貫性が損なわれ、場当たり的な対応となってしまう恐れがある。そのため、目的に則って IT 資産管理を行う枠組みや手法などを、既に業界において標準とされている JIS 等の IT 資産管理に関する規格や基準を基に体系化し、具体化及び詳細化することも必要である。